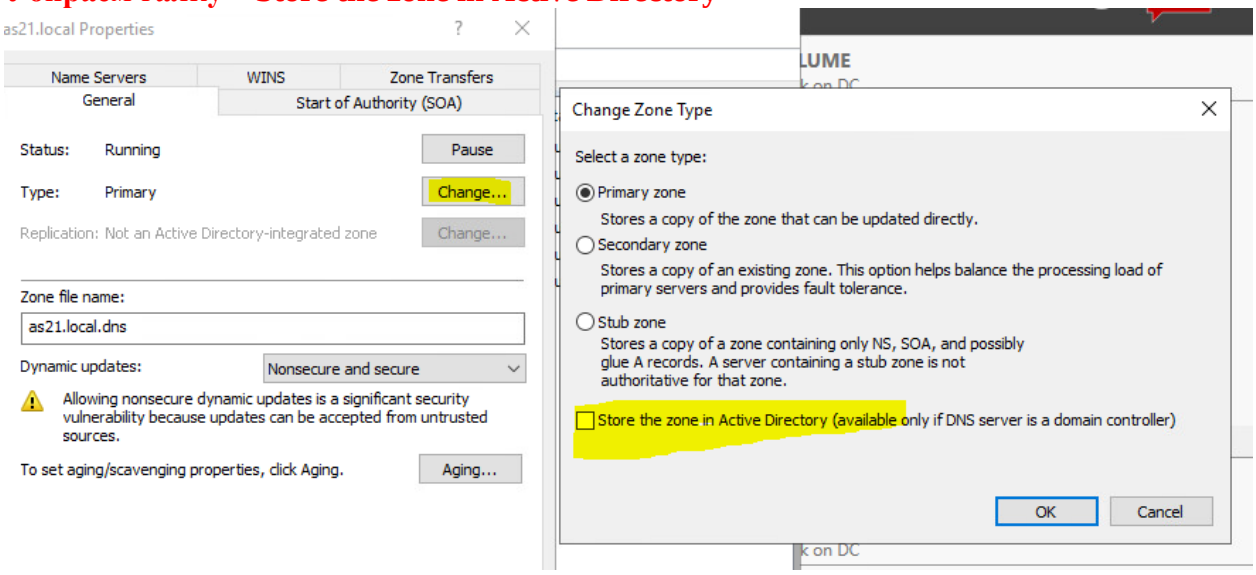
AtomSkills 2021

ПОСЛЕ СОЗДАНИЯ ДОМЕНА AS21.LOCAL

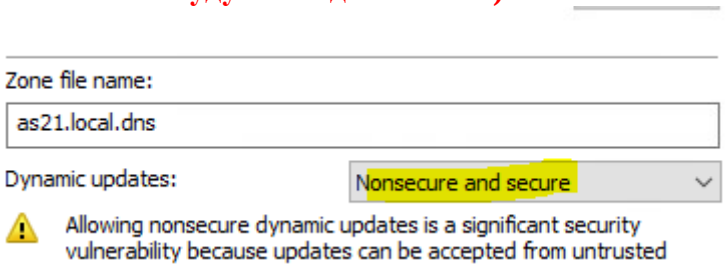
Сделайте сервер DC контроллером домена AS21.local.

Настройка сервиса DNS для переноса на WINSRV1

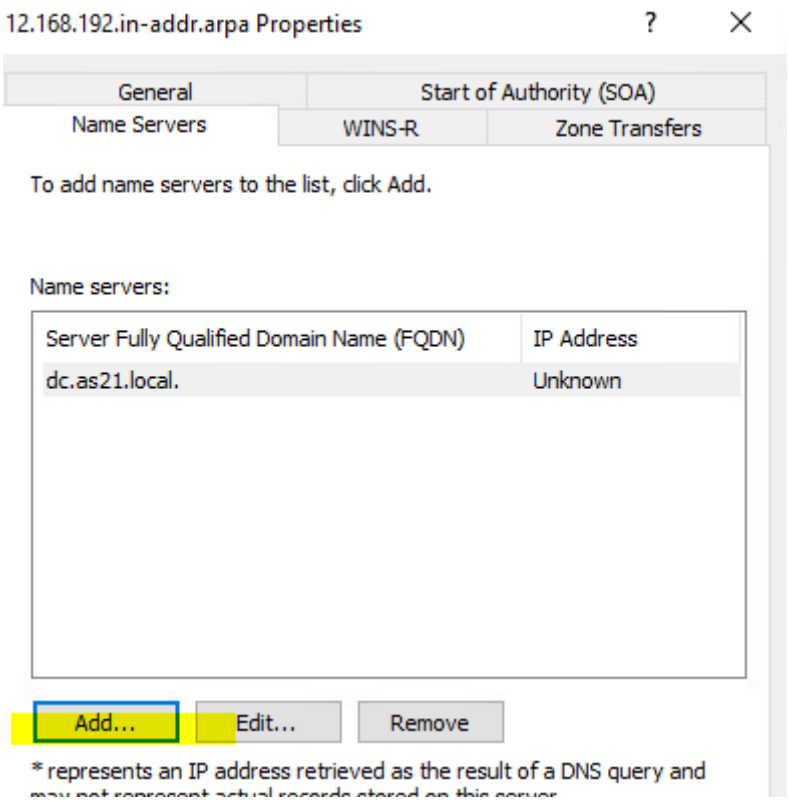
Для начала на DC: Отключаем интеграцию всех зон в домене (прямых и обратных). Убираем галку – Store the zone in Active Directory

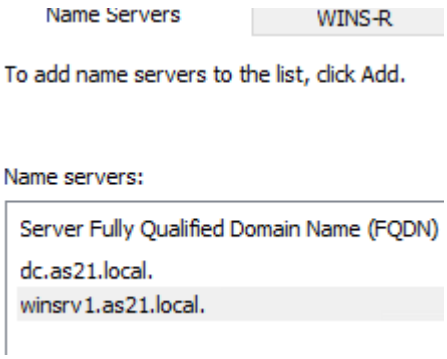


На всех зонах включить Dynamic updates: Nonsecure and secure (иначе компы Windows не будут попадать в DNS)

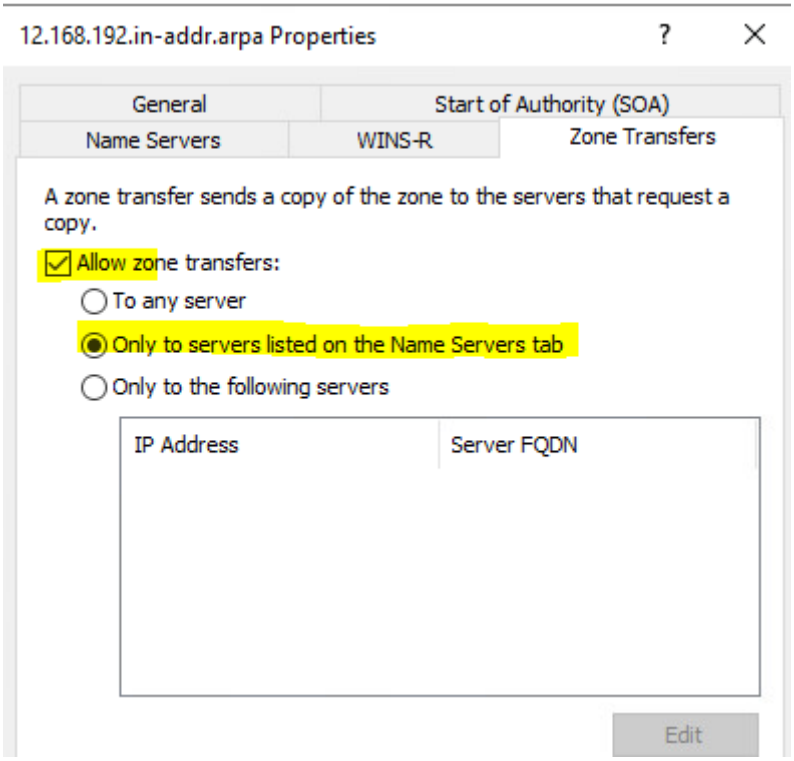


Разрешить передачу зоны на сервер winsrv1 всех зон. Для каждой делаем:





Разрешить передачу зоны на сервера, указанные ранее

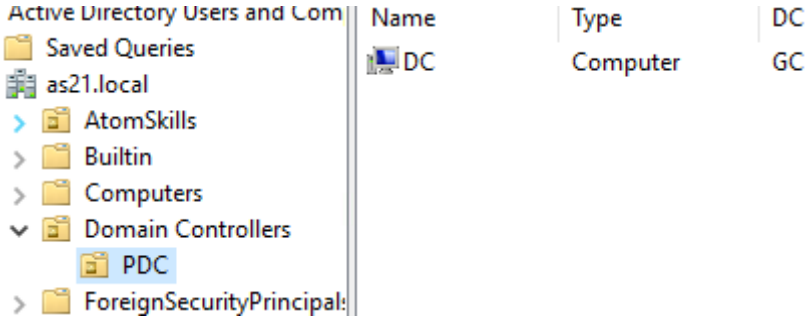


Учетная запись доменного администратора должна иметь логин Administrator и пароль P@ssw0rd; других доменных администраторов быть не должно;

LOGON BANNER

ii. На контроллере домена перед окном ввода пользовательских реквизитов должен находиться баннер с надписью "Warning! Property of RosAtom!".

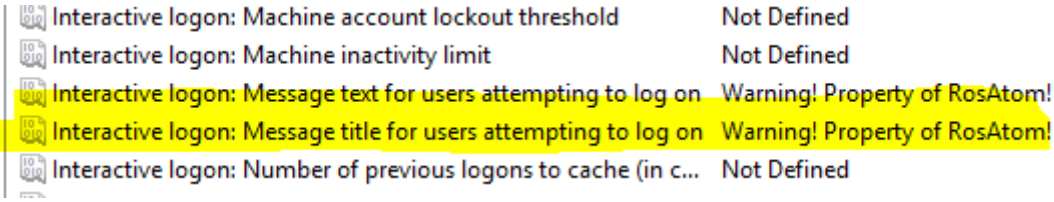
Поместите контроллер домена DC в отдельную OU



GPO на контроллер домена DC:

Computer Configuration > Policies > Windows Settings> Security Settings > Local Policies > Security Options > Interactive logon:Message text for users attempting to log on-> Warning! Property of RosAtom!

Computer Configuration > Policies > Windows Settings> Security Settings > Local Policies > Security Options > Interactive logon:Message title for users attempting to log on-> Warning! Property of RosAtom!



НАСТРОЙКА WINCLI1 и WINCLI2

2. Сделайте компьютеры WINCLI1 и WINCLI2 членами домена AS21.local.

i. Учетная запись локального администратора на WINCLI1 и WINCLI2 должна иметь логин Administrator и пароль P@ssw0rd; других локальных администраторов быть не должно.

ВАЖНО!!! При использовании “визарда” Windows 10, он создает дополнительных администраторов. Не забыть удалить и разблокировать УЗ Administrator. Проверить!

ПРИВЕТСТВЕННАЯ АНИМАЦИЯ

ii. Приветственная анимация при входе новых пользователей должна быть отключена.

GPO на домен: Computer Configuration > Administrative Templates > System > Logon > Show First Sign-In Animation -> Disabled

Do not enumerate connected users on domain-joined com...	Not configured	No
Show first sign-in animation	Disabled	No
Enumerate local users on domain-joined computers	Not configured	No

TEXT.TXT ПРИ ПЕРВОМ ВХОДЕ ПОЛЬЗОВАТЕЛЕЙ

При первом локальном входе пользователя на компьютер WINCLI1 на рабочем столе должен находиться файл. Test.txt со следующим содержанием "It is a first login".

Под локальным администратором до ввода в домен создать на рабочем столе файл Test.txt (аккуратнее с расширением) с содержанием It is a first login, затем скопировать его в C:\Users\Default\Desktop

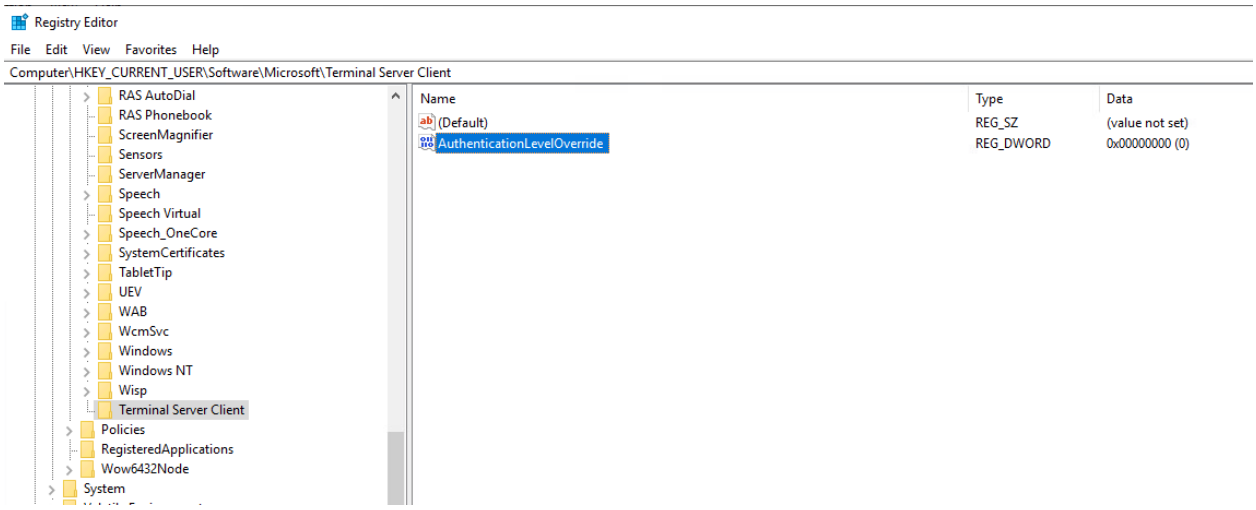
RDP ПОДКЛЮЧЕНИЕ ПО СЕРТИФИКАТАМ

На клиентах и серверах домена включите возможность подключения к ним с использованием утилиты Remote Desktop Connection с защитой подключения с помощью сертификатов, выданных сервером SubCA (данная настройка должна автоматически применяться для любых новых клиентов домена). При подключении должна быть возможность использовать: на клиентах - канонические и короткие имена компьютеров, а на серверах - канонические и короткие имена компьютеров, а также ip-адреса (при этом не должно возникать никаких ошибок и предупреждений)

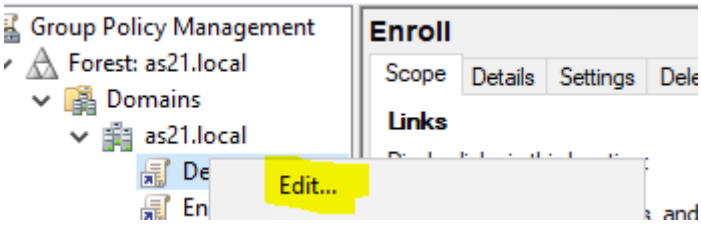
Настройка серверов для работы по ip

На DC заходим в реестр (regedit)

HKEY_CURRENT_USER > Software > Microsoft создаем ключ Terminal Server Client и DWORD значение AuthenticationLevelOverride = 0



Редактируем Default domain policy



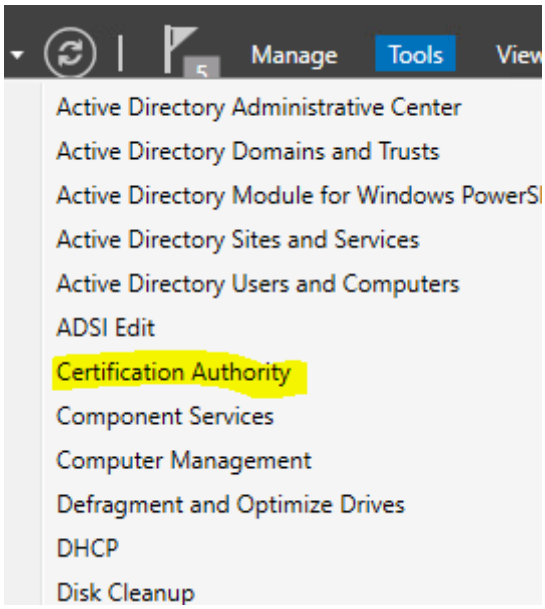
User Configuration > Preferences > Windows Settings > Registry -> New -> Registry Wizard

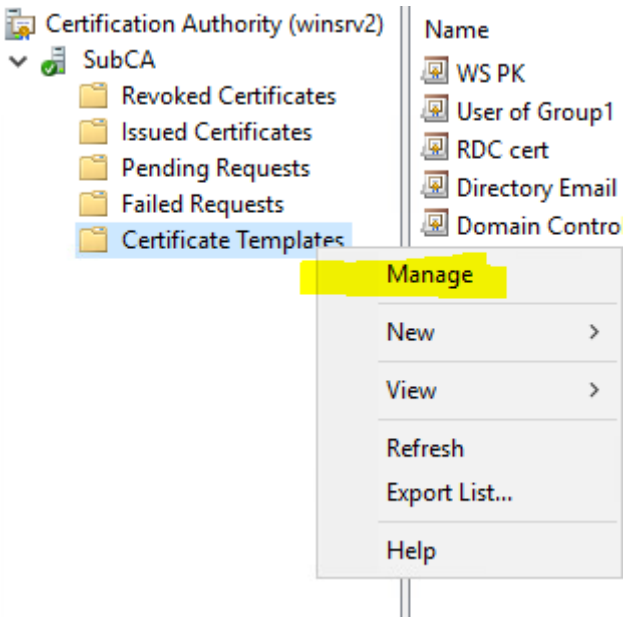
Создать «визардом» новую запись Local Computer выбираем ветку
HKEY_CURRENT_USER > Software > Microsoft > Terminal Server Client

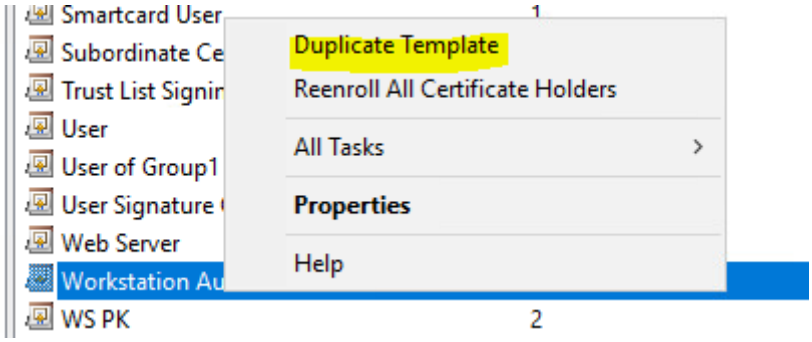
Выбираем все параметры оттуда

Настройка шаблона выдачи сертификатов

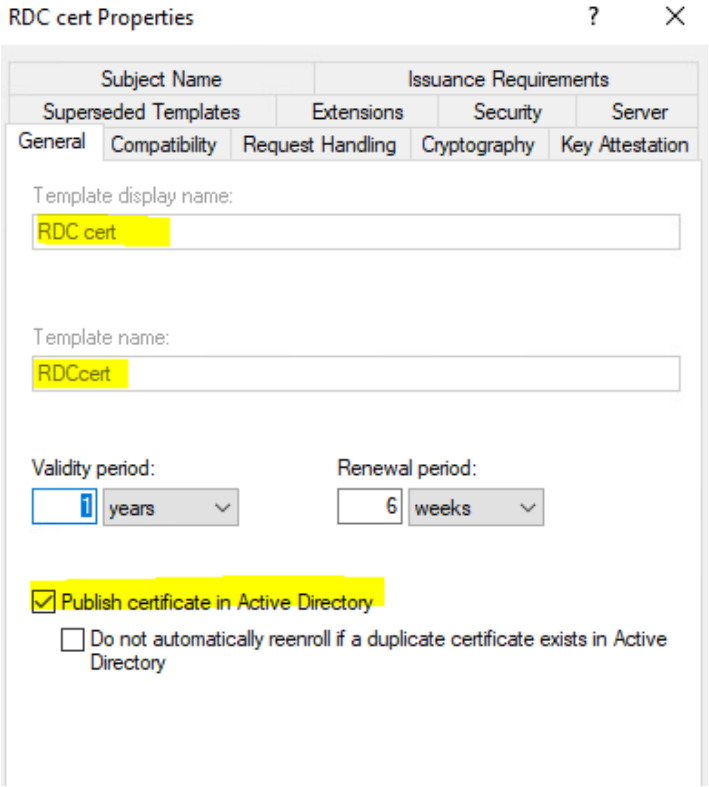
Настроим выдачу нужного сертификата на WINSRV2



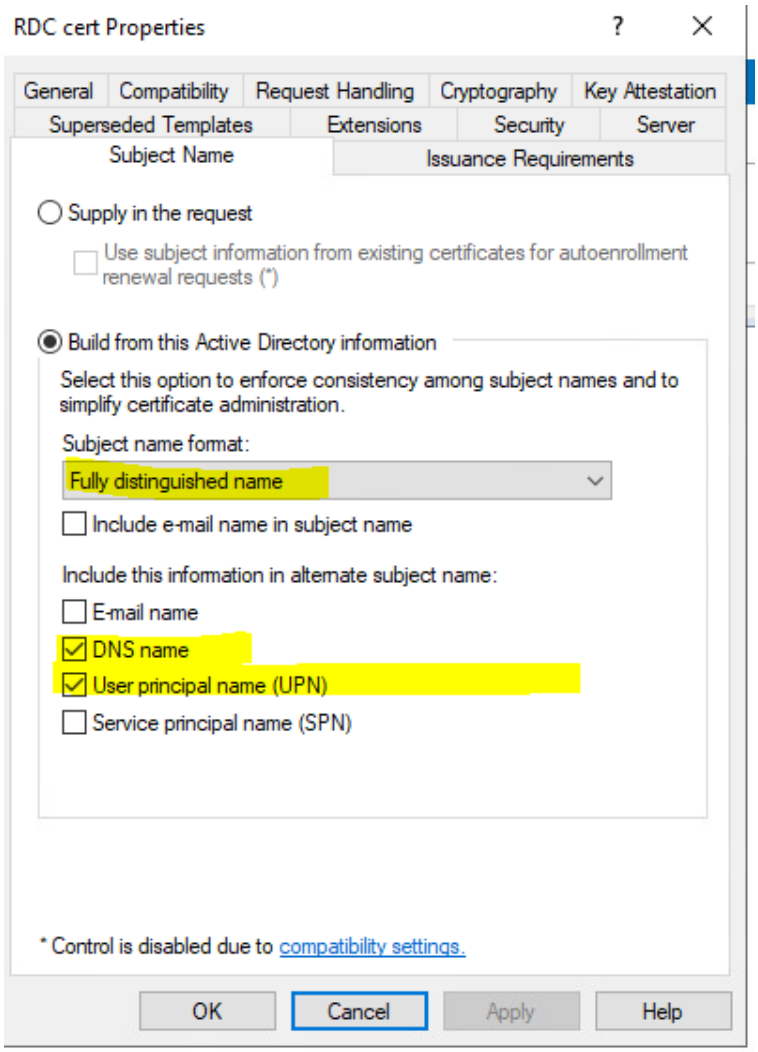




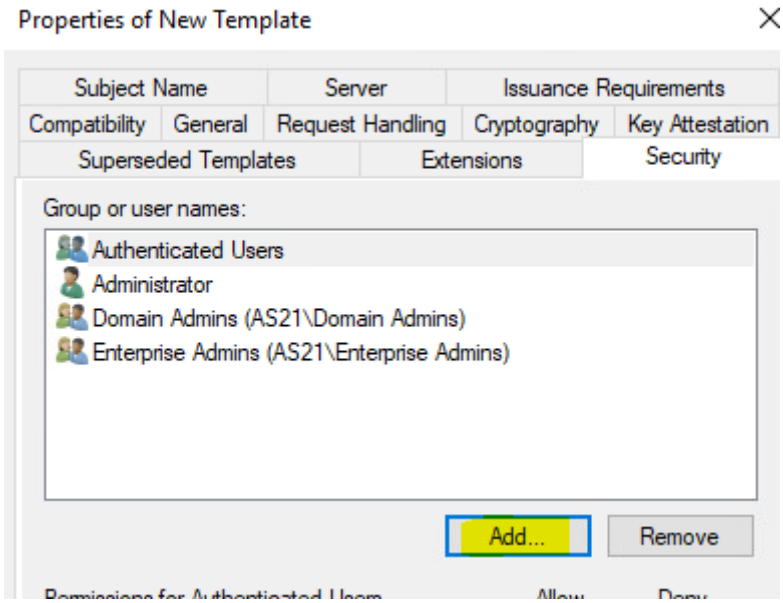
Вводим имя нового шаблона. Включаем публикацию в Active Directory



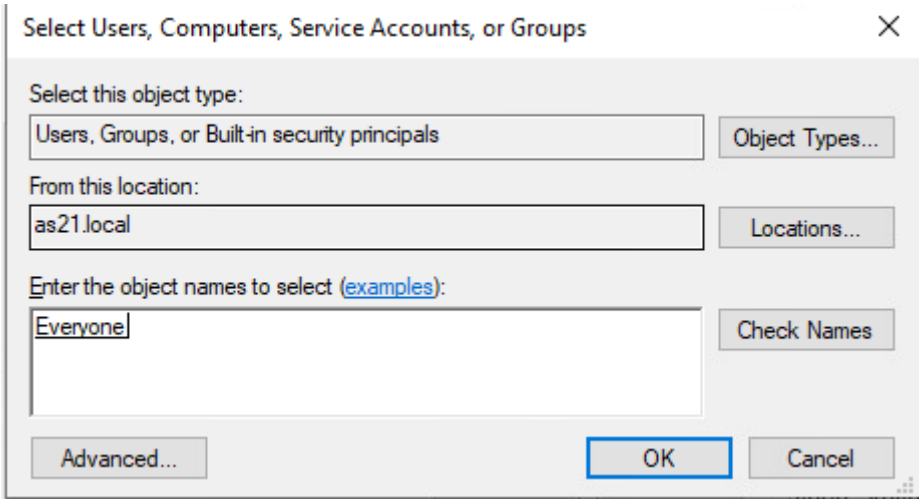
Убираем из шаблона все упоминания о e-mail, ибо у нас его нет

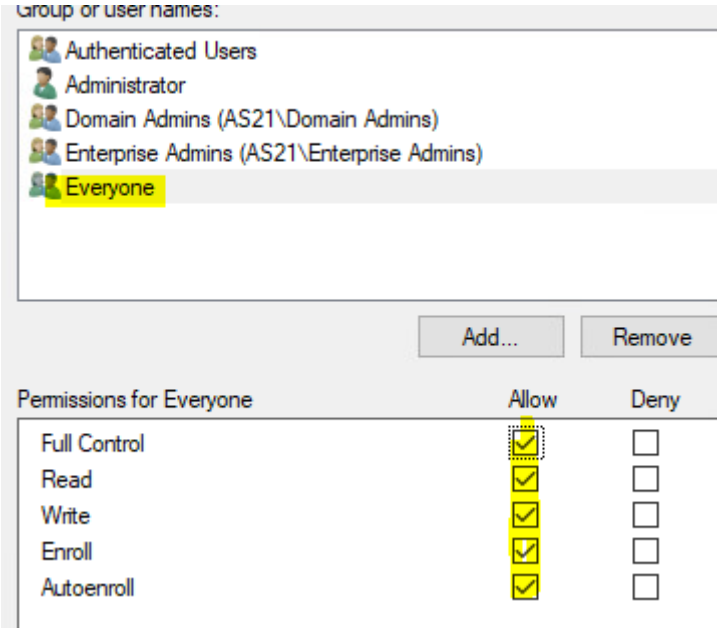


Нужно добавить возможность выпуска сертификата любой машиной

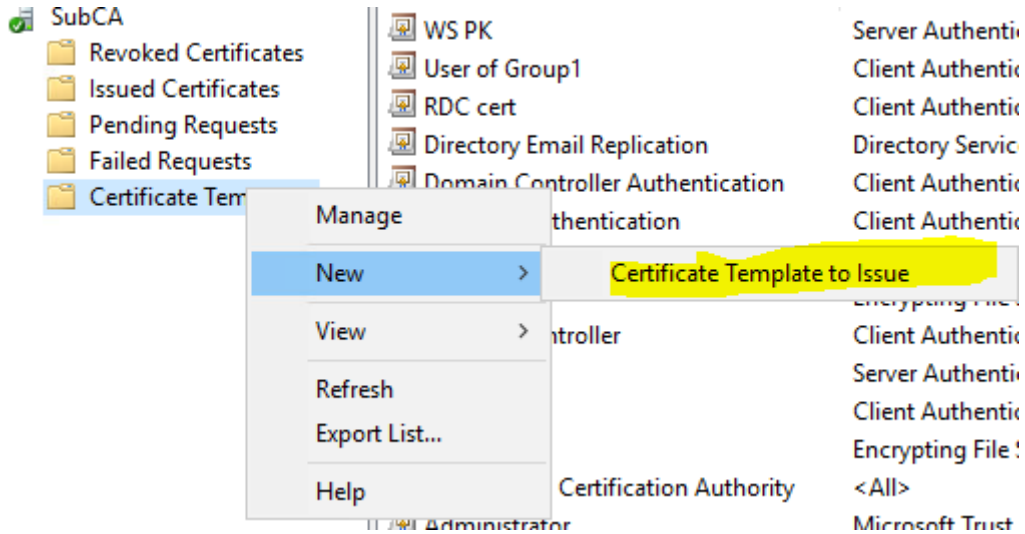


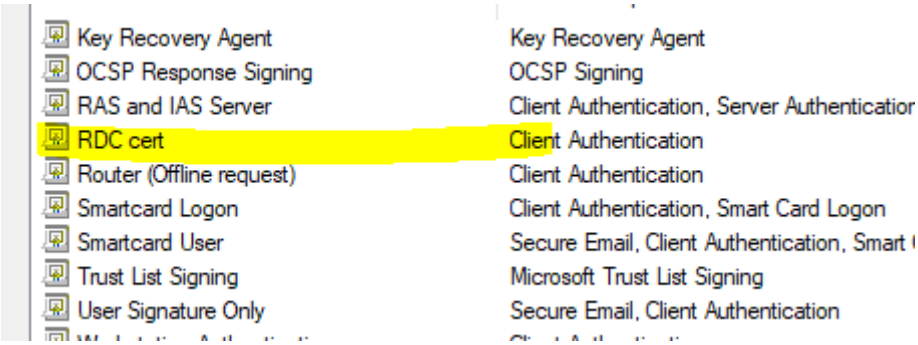
Даем всем права на выпуск сертификата группе Everyone





Публикуем сертификат в Active Directory

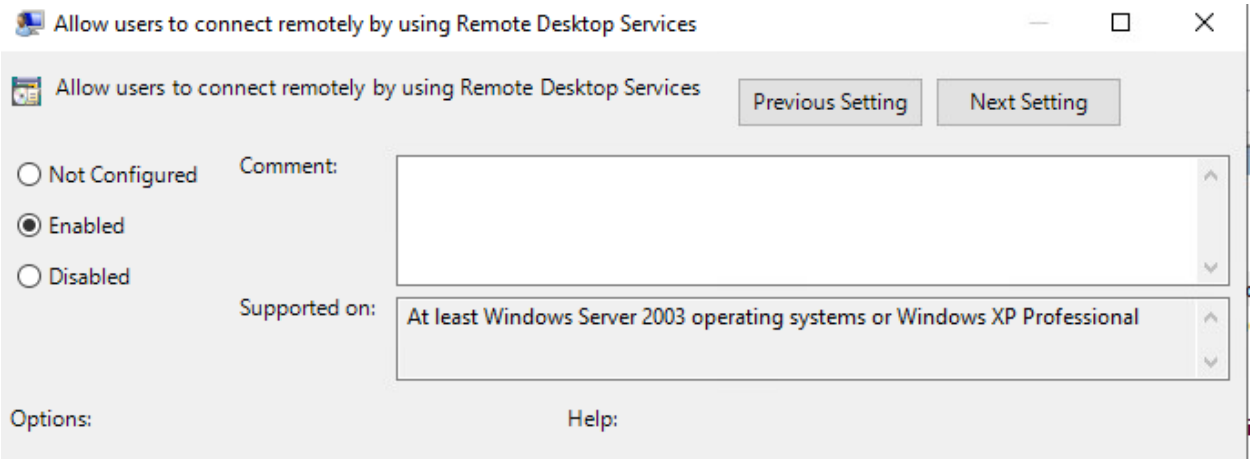




Настройки GPO для RDP

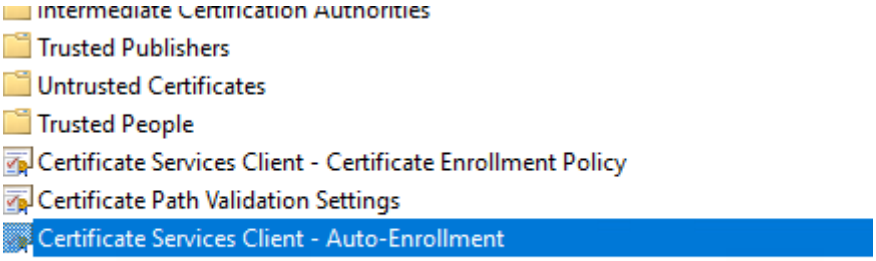
Разрешаем через GPO использование Remote Desktop Connection

GPO на домен: Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services -> Remote Desktop Session Host > Connections > Allow users to connect remotely using Remote Desktop Services -> Enabled

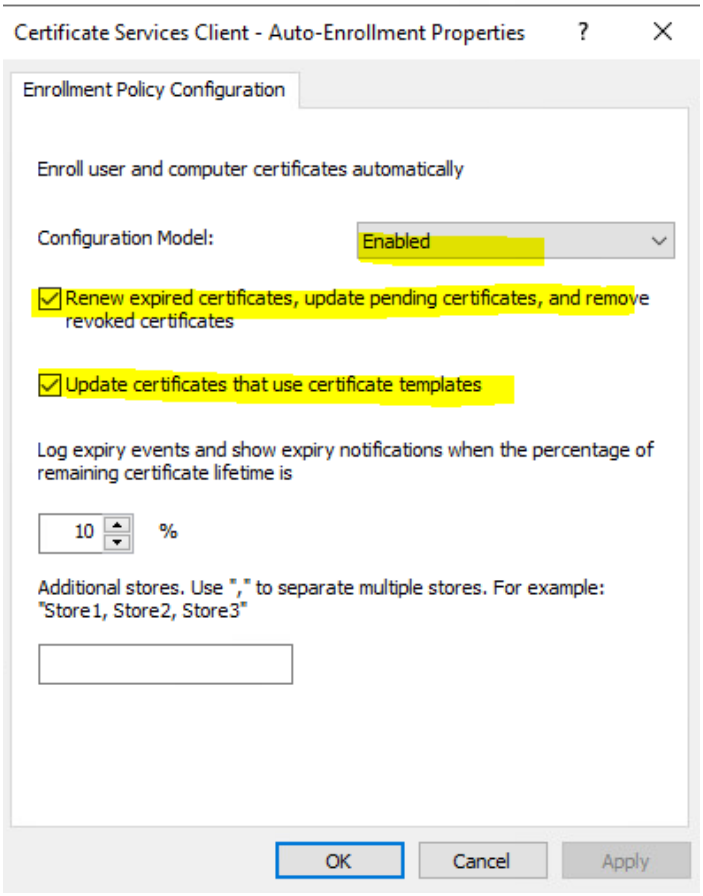


Включаем авто выдачу сертификатов всем устройствам домена

GPO на домен: Computer Configuration > Policies > Windows Settings> Security Settings > Public Key Policies > Certificate Service Client – Auto-Enrollment -> Enabled

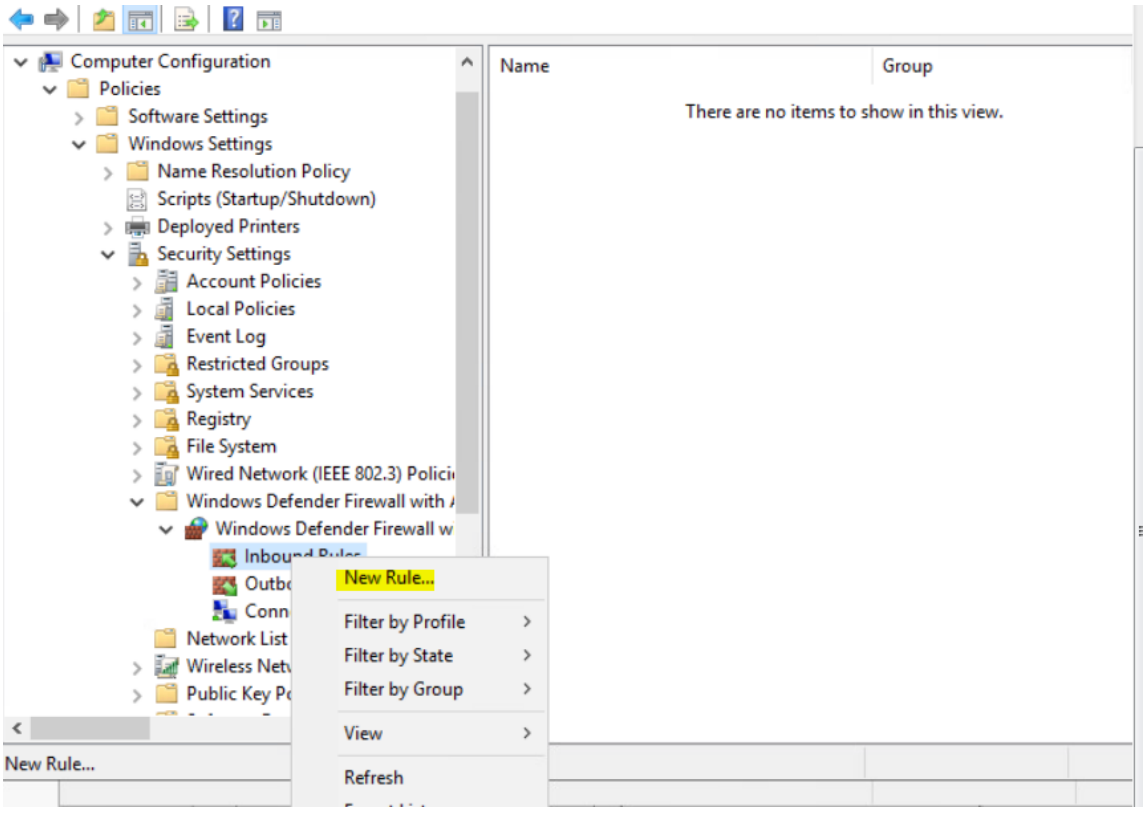


Включаем общую настройку выдачи и выбираем 2 конфигурации

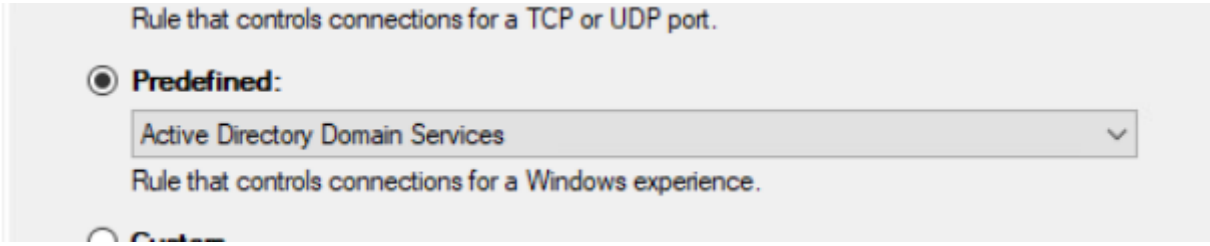


Разрешаем подключение по RDP компьютерам домена

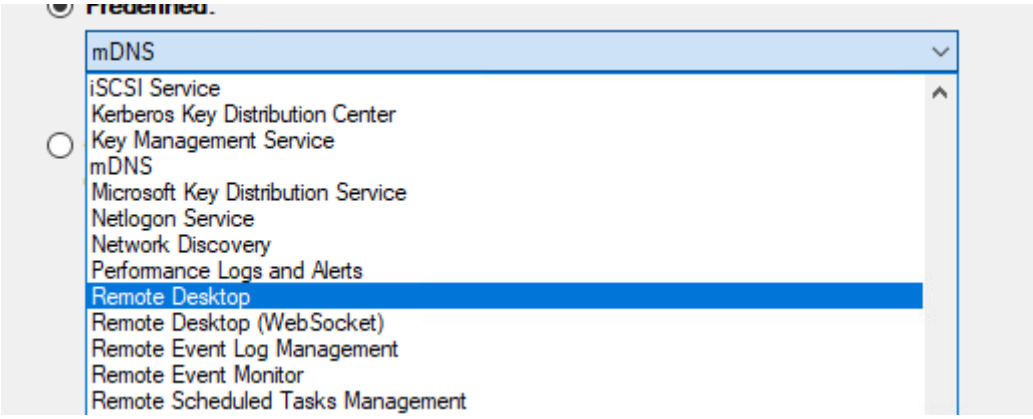
Computer Configuration > Policies > Windows Settings > Security Settings >Windows Defender Firewall and Advanced Security > Inbound Rules -> New Rule

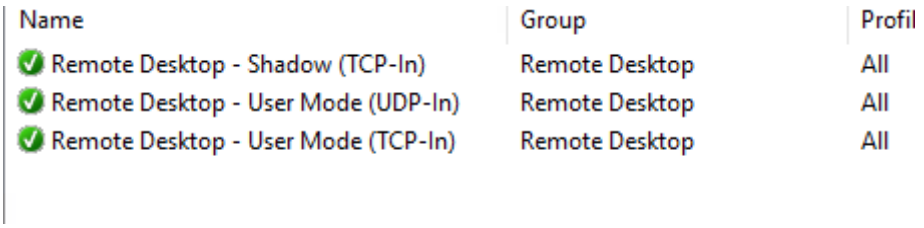


Выбираем предопределенные (Predefined)



Выбираем Remote Desktop





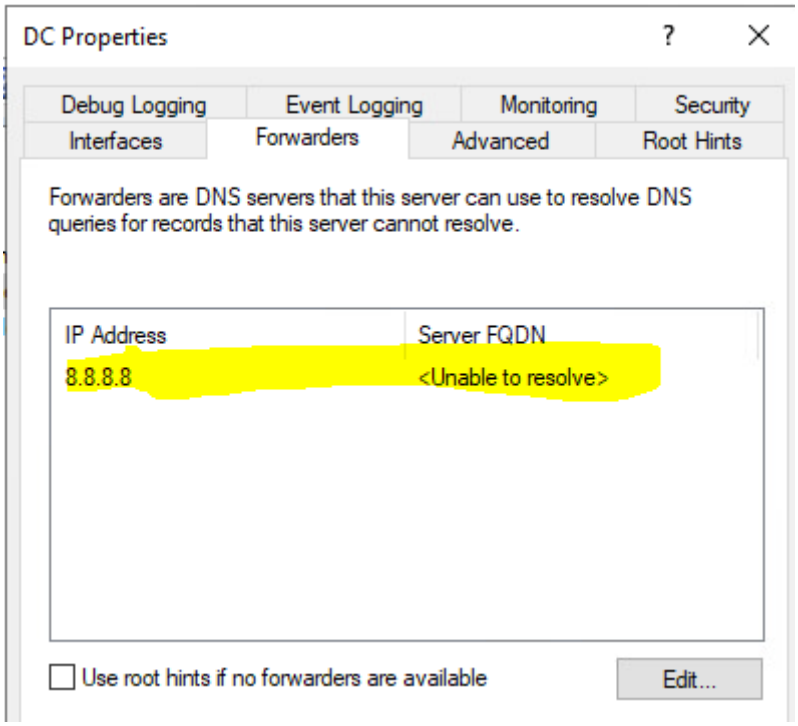
РАБОТОСПОСОБНОСТЬ DNS

Настройка Forwarders

Обеспечьте работоспособность службы DNS на DC.

Должна быть настроена переадресация запросов для имен, не связанных с внутренним доменом, на сервер Moogle.

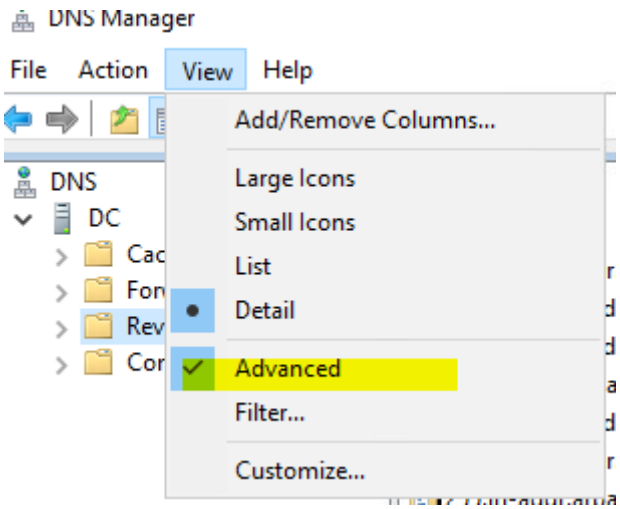
В свойствах DNS сервера прописать Forwarders на 8.8.8.8. Остальные можно удалить



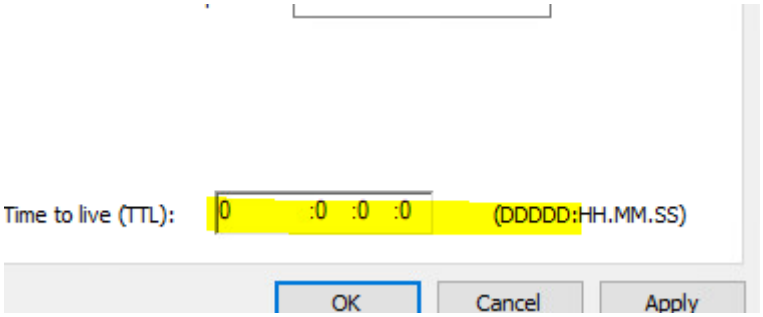
Настройка Round Robin

Для имеющихся в основной доменной зоне записей с одинаковыми именами, но разными адресами должна работать балансировка по алгоритму round-robin, при этом не должно быть повышения нагрузки на DNS-сервер из-за слишком частого обновления зон.

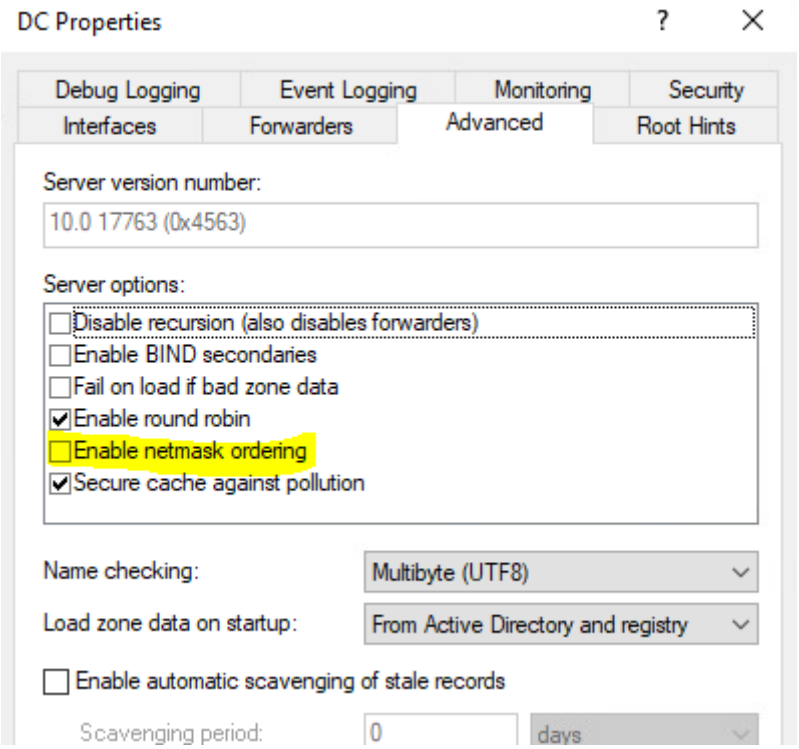
Включить DNS Manager > View > Advanced



Установить TTL для одинаковых A записей = 0



В свойствах DNS сервера в Advanced убрать галку на Enable netmask ordering



НАСТРОЙКА DHCP

Обеспечьте работоспособность службы DHCP на DC.

Все клиенты в сети центрального офиса должны иметь возможность получать корректные адреса в своих подсетях с DC.

ВАЖНО!!! 3 опции на каждую зону: dns, domain name, router.

Option Name	Vendor	Value	Policy Name
003 Router	Standard	192.168.11.254	None
006 DNS Servers	Standard	10.0.3.1, 192.168.12.1	None
015 DNS Domain Name	Standard	as21.local	None

5.

ФАЙЛОВЫЕ СЛУЖБЫ НА DC (File Restrictions)

Проверьте работоспособность файловых служб на DC.

Члены группы Engineers должны иметь полный доступ к общей папке Work.

Члены группы Projects должны иметь доступ к общей папке Work только для чтения.

ВАЖНО!!!

Папку создаем C:\Work, «расшариваем» её с Shared Permissions – Everyone Full Access

Убрать наследования и убрать пользователей AS21\Users из ACL!

Создайте в домене при необходимости указанные выше группы, в каждой группе создайте по одному

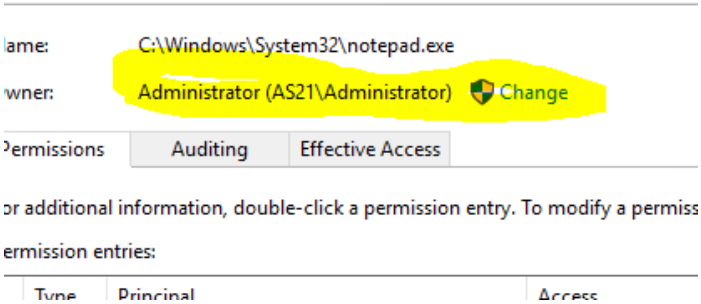
пользователю Engineer1/P@ssw0rd и Projects1/P@ssw0rd соответственно.

ВАЖНО!!! Имена кривые, следите и делайте четко по тексту

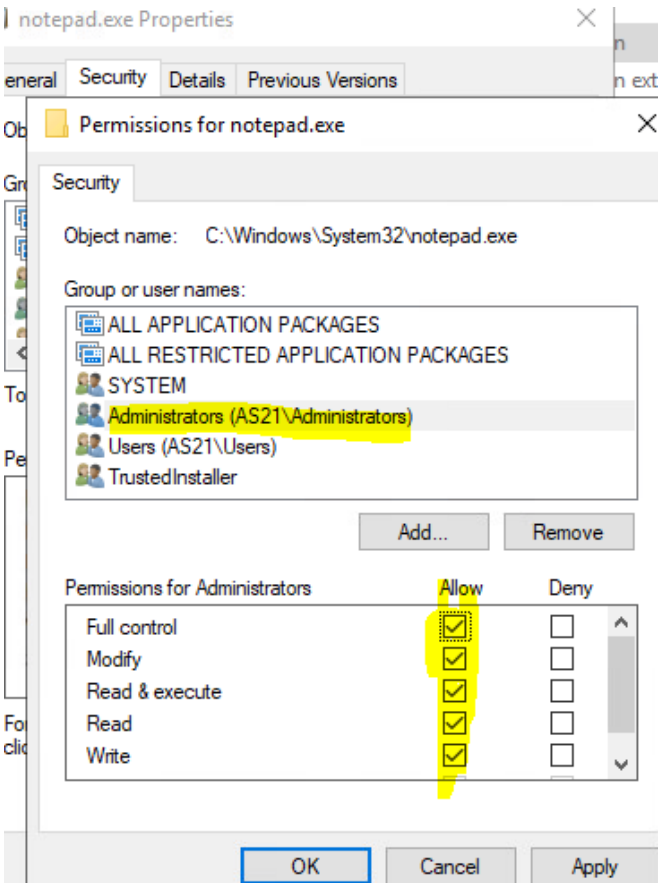
Переместите в общую папку Work исполняемый файл notepad.exe; обеспечьте возможность запуска notepad.exe из общей папки Work, но учтите, что никакие другие исполняемые файлы не должны запускаться из этой папки.

GPO на домен (OU=PDC,OU=Domain Controllers,DC=AS21,DC=local)

Notepad.exe переносим!!! Чтобы это сделать, забираем у Trusted Installer владельца



Группе AS21\Administrators даем полные права на файл



Создать политику на домен:

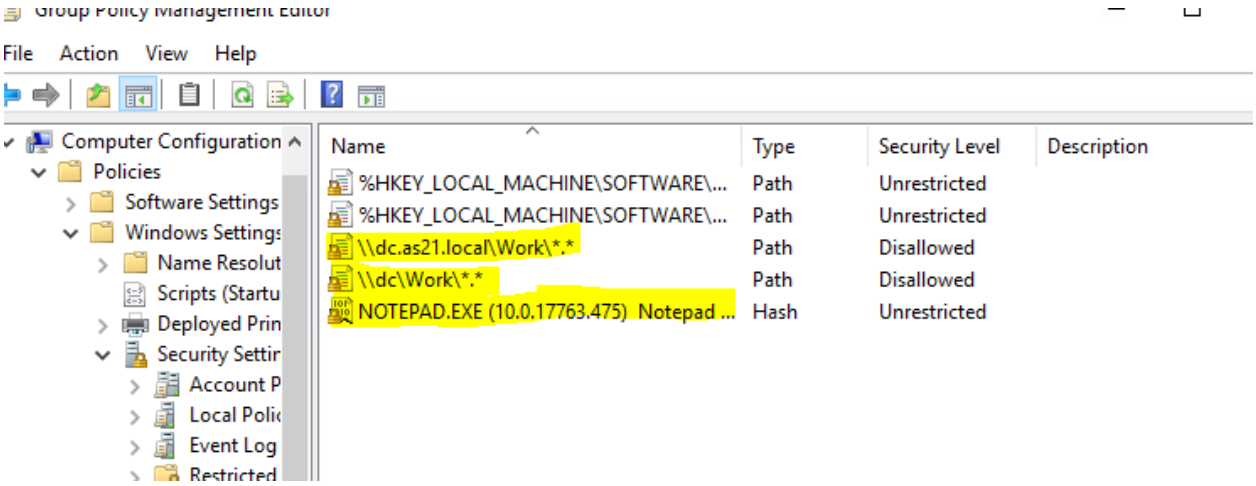
Computer Configuration > Policies > Windows Settings> Security Settings > Software Restriction Policies и прописать Additional Rules:

Path Rule (Disallowed):

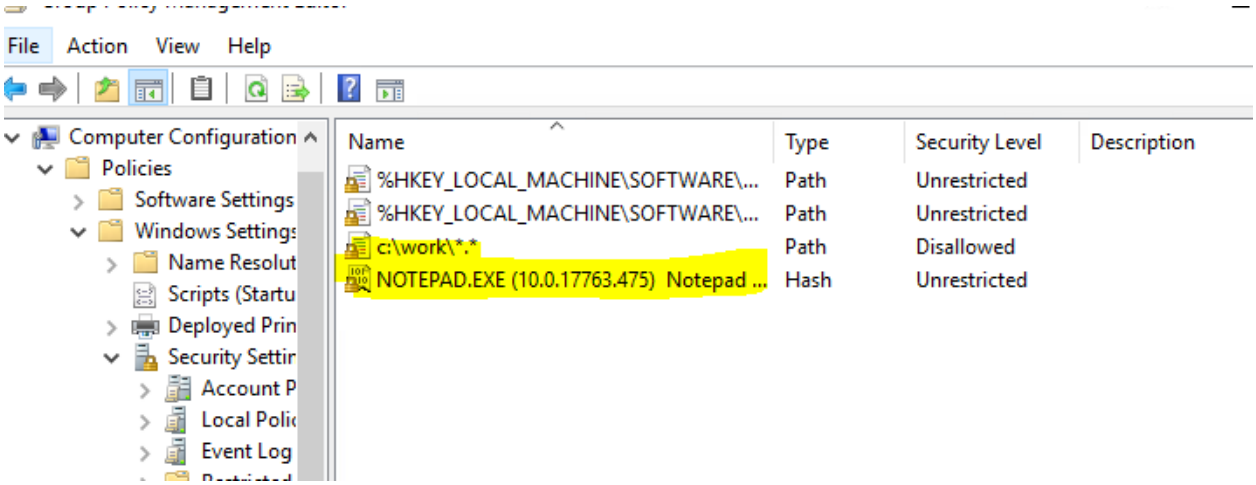
\\dc.as21.local\Work*.*

\\dc\Work*.*

Hash Rule (Unrestricted): выбрать файл c:\work\notepad.exe



GPO на OU с DC (OU=PDC,OU=Domain Controllers,DC=AS21,DC=local), ибо DC наш PDC



Computer Configuration > Policies > Windows Settings> Security Settings > Software Restriction Policies и прописать Additional Rules:

Path Rule (Disallowed): C:\Work*.*

Hash Rule (Unrestricted): выбрать файл c:\work\notepad.exe

Для проверки – Log off

СЛУЖБА ВРЕМЕНИ (NTP)

Проверьте работоспособность служб времени на DC и в домене в целом.

Настройка DC на получение времени с Moogle

Контроллер домена должен быть настроен для синхронизации системного времени с сервером Moogle.

GPO на OU с DC (OU=PDC,OU=Domain Controllers,DC=AS21,DC=local), ибо DC наш PDC

Computer Configuration > Policies > Administrative Templates > System > Windows Time Service > Time providers > Configure Windows NTP Client ->

NtpServer	8.8.8.8,0x9
Type	NTP
CrossSiteSyncFlags	2
ResolvePeerBackoffMinutes	15
ResolvePeerBackoffMaxTimes	7
SpecialPollInterval	1024
EventLogFlags	0

Computer Configuration > Policies > Administrative Templates > System > Windows Time Service > Time providers > Enable Windows NTP Server -> Enabled

Computer Configuration > Policies > Administrative Templates > System > Windows Time Service > Time providers > Enable Windows NTP Client -> Enabled

ion.	Setting	State	Comment
	Configure Windows NTP Client	Enabled	No
	Enable Windows NTP Client	Enabled	No
	Enable Windows NTP Server	Enabled	No

Настройка клиентов на получение времени с DC

Все компьютеры в домене должны синхронизировать время с контроллером домена DC.

GPO на домен: Computer Configuration > Policies > Administrative Templates > System > Windows Time Service > Time providers > Configure Windows NTP Client ->

NtpServer	dc.as21.local,0x9
Type	NT5DS
CrossSiteSyncFlags	2
ResolvePeerBackoffMinutes	15
ResolvePeerBackoffMaxTimes	7
SpecialPollInterval	1024
EventLogFlags	0

Computer Configuration > Policies > Administrative Templates > System > Windows Time Service > Time providers > Enable Windows NTP Client -> Enabled

Setting	State	Comment
Configure Windows NTP Client	Enabled	No
Enable Windows NTP Client	Enabled	No
Enable Windows NTP Server	Not configured	No

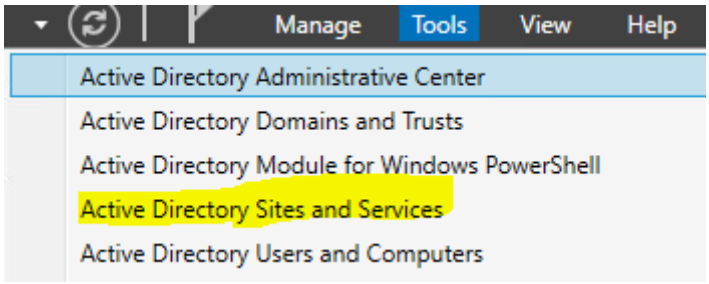
Настройте сервера WINNET и WINDMZ на получение времени контроллера домена

w32tm /config /syncfromflags:manual /manualpeerlist:dc.as21.local /reliable:yes

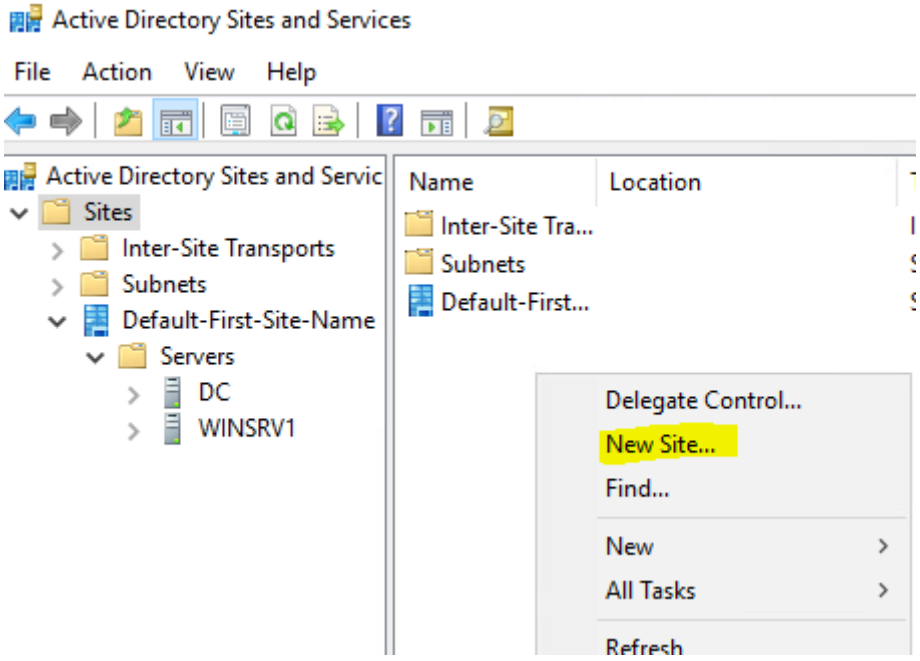
w32tm /resync /rediscover

Настройка временной зоны

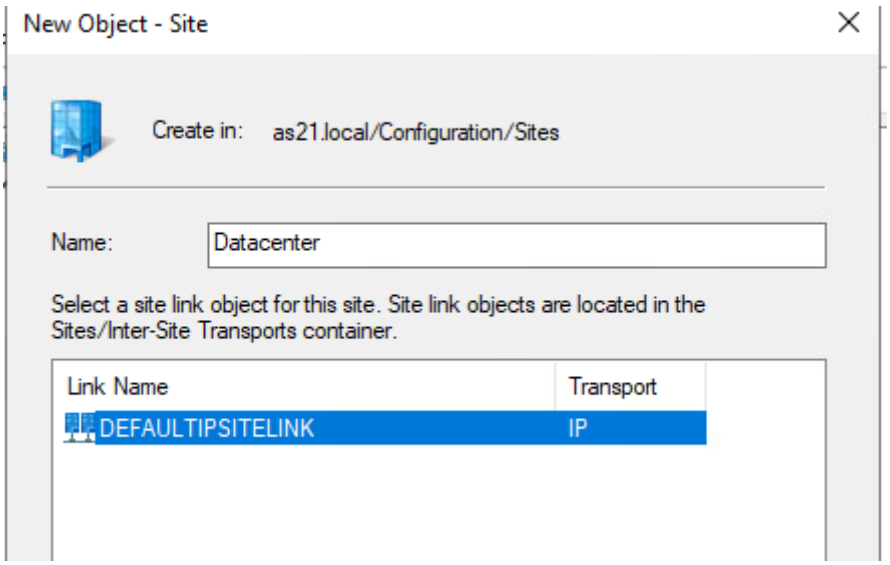
Создаем сайт – Datacenter
Открываем на DC оснастку Active Directory Sites and Services



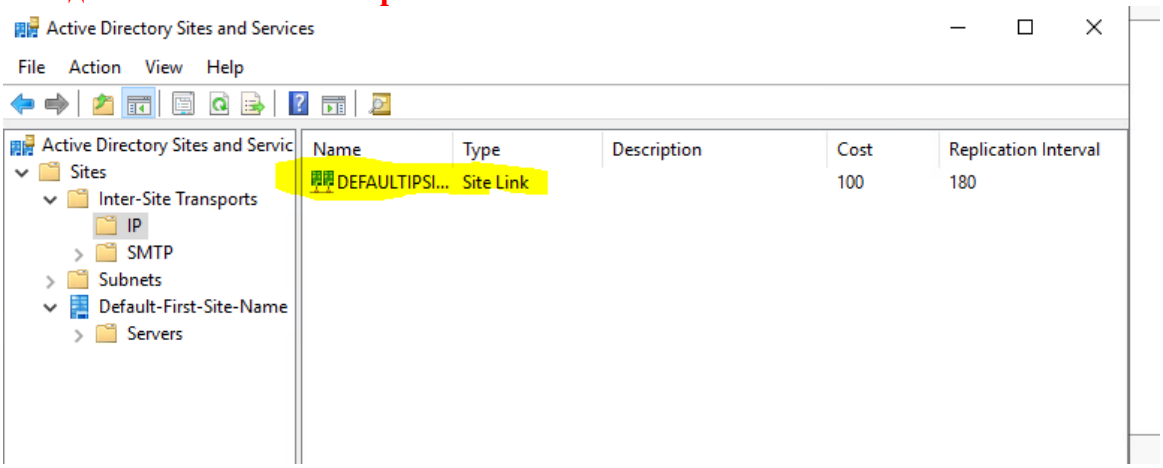
В разделе Sites создаем новый сайт – New Site



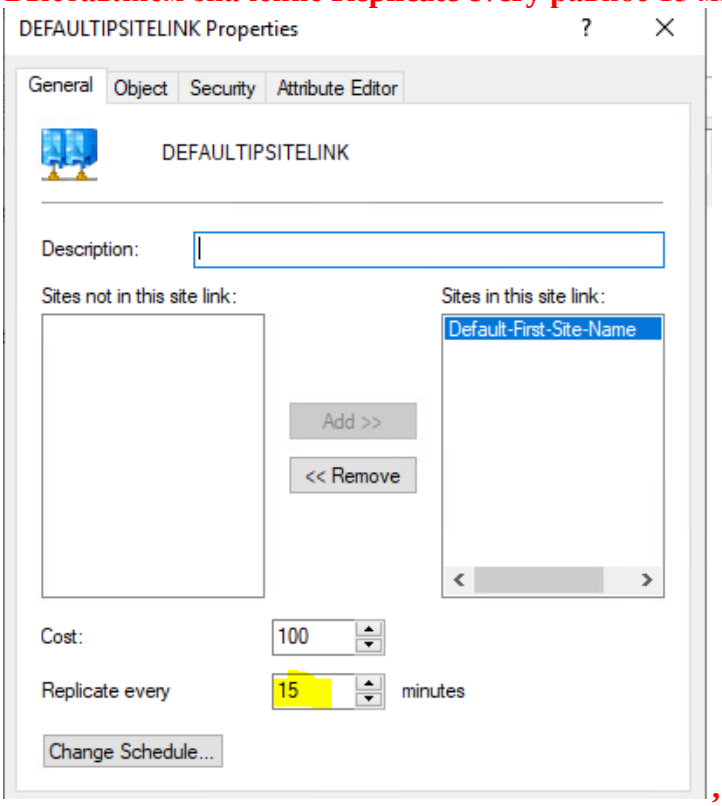
Выбираем для него соединение между сайтами по умолчанию



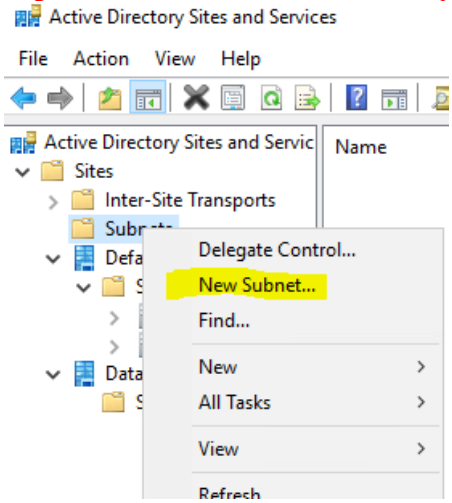
Настроим наименьшую периодичность репликации – 15 минут
Заходим в Inter-Site Transports > IP и вызываем свойство DEFAULTSITELINK



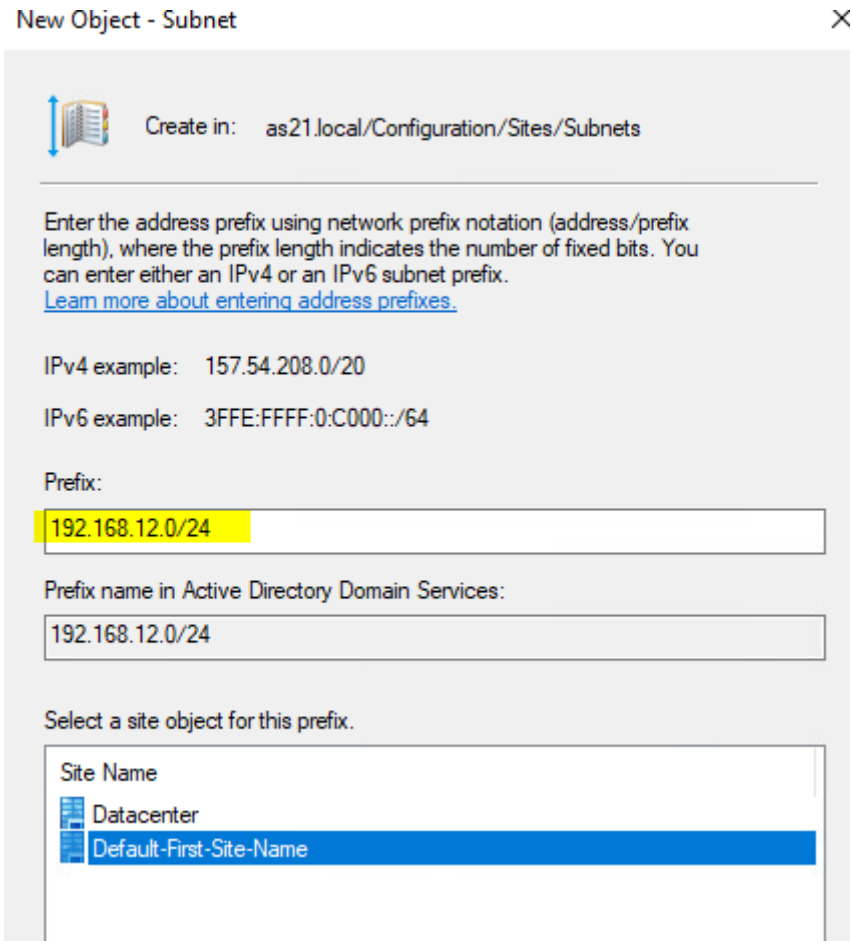
Выставляем значение Replicate every равное 15 минутам



Создаем и закрепляем подсети за сайтами (все)
В разделе Subnets создаем новую подсеть - New Subnet



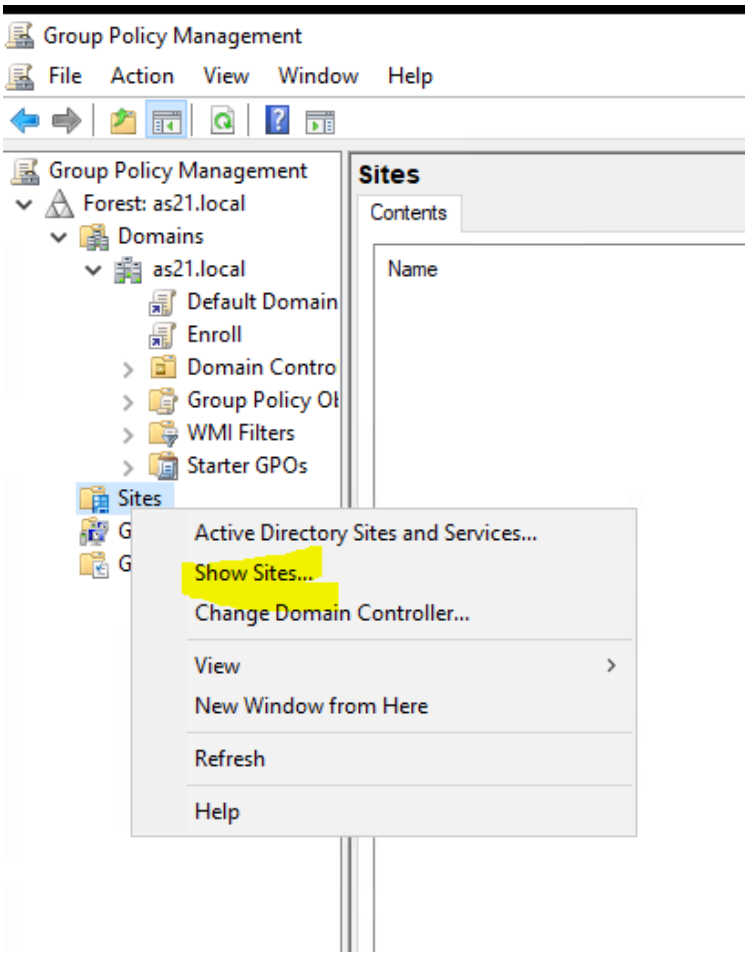
Пишем наименование сети формата сеть/маска. Назначаем её соответствующий сайт



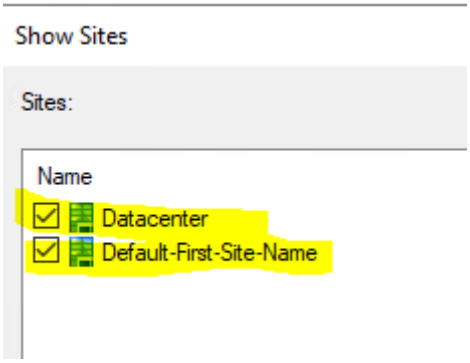
На всех компьютерах домена в ЦОД должна быть установлена зона "Moscow Standard Time"; эта настройка должна действовать всегда, в том числе, после перезагрузки.

Устанавливаем на DC зону Moscow Standard Time +3.

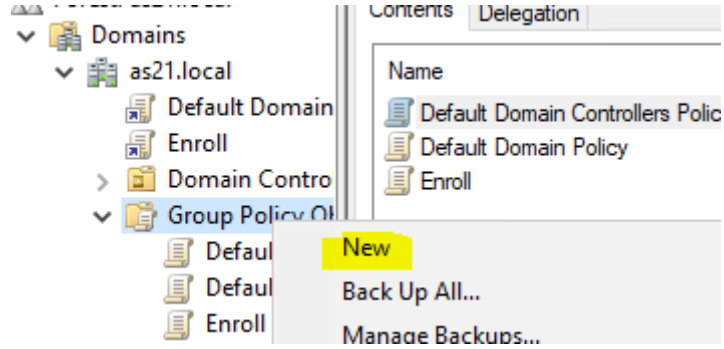
В оснастке Group Policy Management правой кнопкой по Sites и выбираем Show Sites



Выбираем оба сайта



Правой кнопку по разделу Group Policy Objects

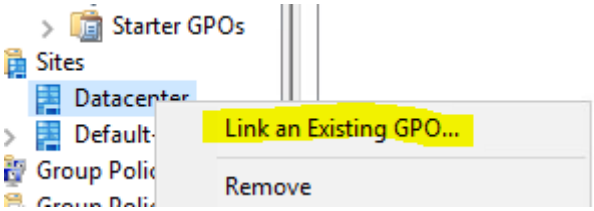


Создаем GPO для ЦОД (Datacenter): **Computer Configuration > Preferences > Windows Settings > Registry ->** **New -> Registry Wizard**

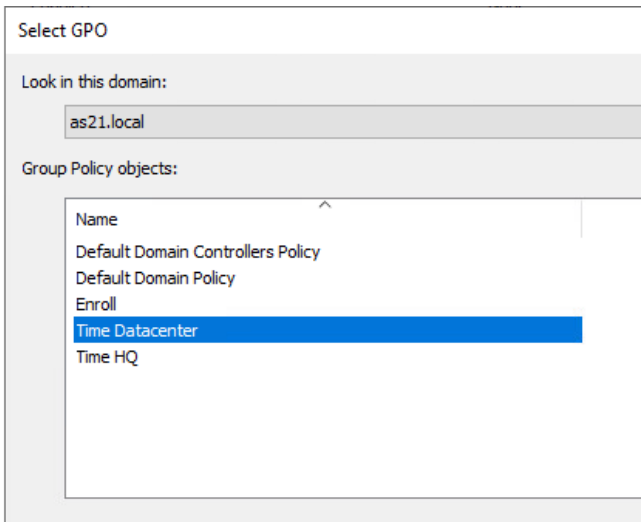
Создать «визардом» новую запись Local Computer выбираем ветку HKLM\System\CurrentControlSet\Control\TimeZoneInformation

Выбираем все параметры оттуда

Чтобы привязать GPO, правой кнопкой по сайту Datacenter и нажимаем Link an Existing GPO



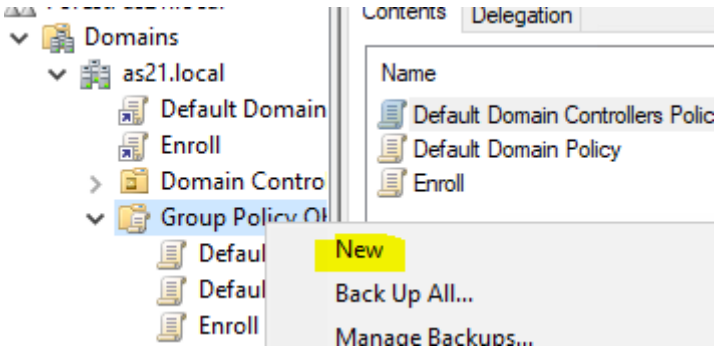
Выбираем наше GPO для ЦОД, созданное ранее



На всех компьютерах домена должна быть установлена зона "Ekaterinburg Standard Time"; эта настройка должна действовать всегда, в том числе, после перезагрузки.

Устанавливаем на DC нужную зону Ekaterinburg Standard Time +5.

Правой кнопку по разделу Group Policy Objects

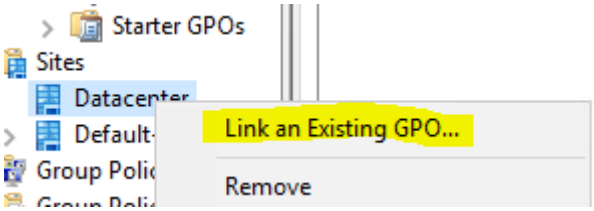


Создаем GPO для центрального офиса (Default-First-Site-Name): Computer Configuration > Preferences > Windows Settings > Registry -> New -> Registry Wizard

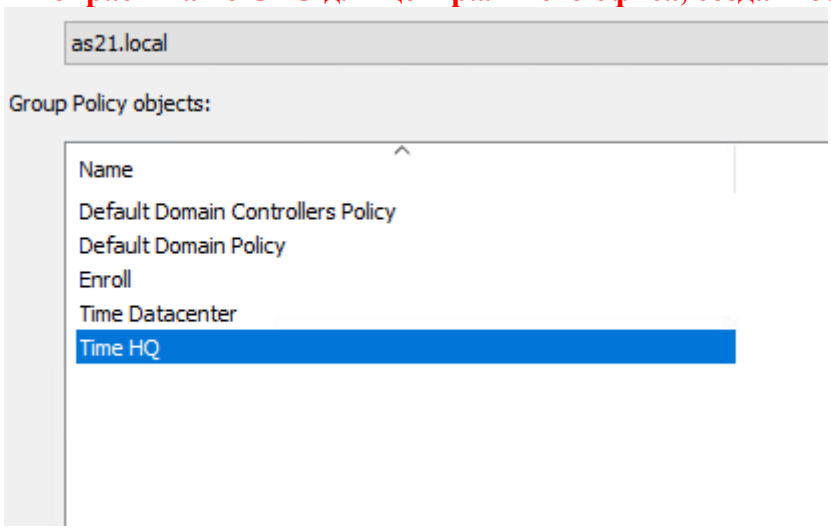
Создать «визардом» новую запись Local Computer выбираем ветку HKLM\System\CurrentControlSet\Control\TimeZoneInformation

Выбираем все параметры оттуда

Чтобы привязать GPO, правой кнопкой по сайту Default-First-Site-Name и нажимаем Link an Existing GPO



Выбираем наше GPO для центрального офиса, созданное ранее



СОЗДАНИЕ ПОЛЬЗОВАТЕЛЕЙ ДОМЕНА

Создайте подразделения, группы безопасности и пользователей на контроллере домена DC

Создайте подразделение Office.

В подразделении Office создайте три группы Group1, Group2, Group3.

В подразделении Office создайте 150 пользователей User1 - User150. Имя входа в домен, например, User1@AS21.local (для остальных пользователей аналогично). Пароль для входа в домен P@ssw0rd (для всех создаваемых пользователей). Первые 50 пользователей должны быть членами группы Group1, следующие 50 пользователей - членами группы Group2, оставшиеся 50 пользователей - членами группы Group3. Все созданные аккаунты должны быть включены.

```
for ($i=1; $i -le 50; $i++){

   $name=("User" + $i)
```

$pass="P@ssw0rd"

New-ADuser -name $name -path "OU=Office,DC=as21,dc=local" -AccountPassword(ConvertTo-SecureString($pass) -AsPlainText -Force) -Enabled $true -CannotChangePassword $true

Add-AdGroupMember -Members $name -Identity "Group1"

} – далее только меняем переменную $i и Identity группы

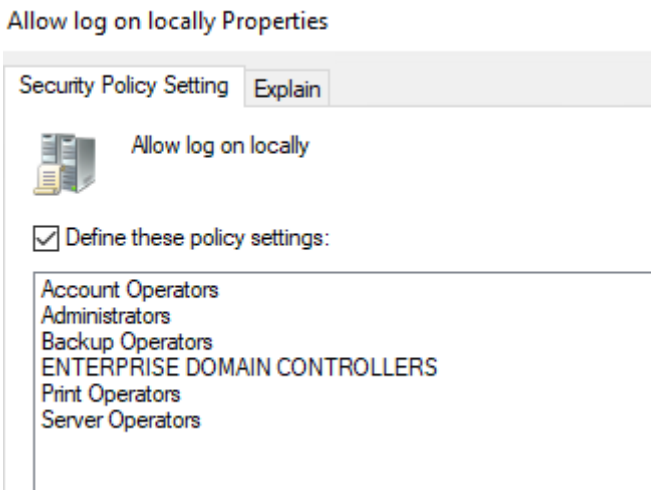
РАЗРЕШИТЬ GROUP3 ЗАХОДИТЬ НА DC

Разрешите членам группы Group3 локальный вход на контроллер домена DC.

Открываем политику Default Domain Controllers Policy

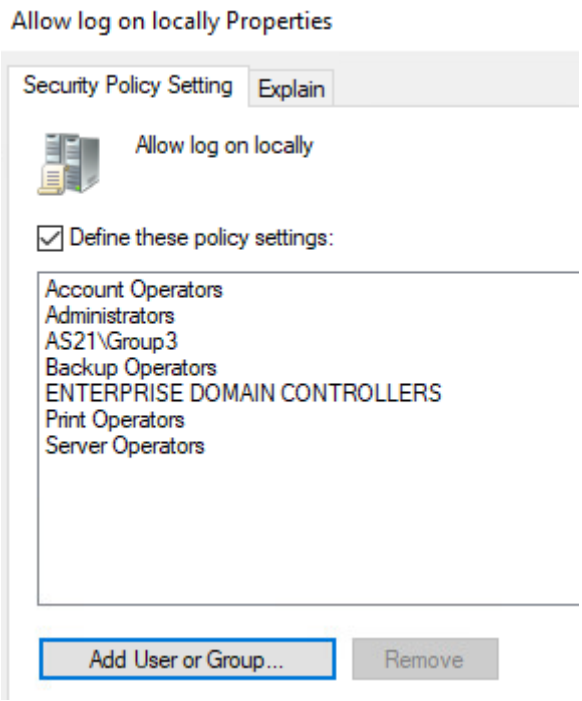
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Right Assignment -> Allow log on locally (открыли и он нам нужен)

Можно вырезать Ножницами (Snipping Tool)



GPO на OU с DC (OU=PDC,OU=Domain Controllers,DC=AS21,DC=local)

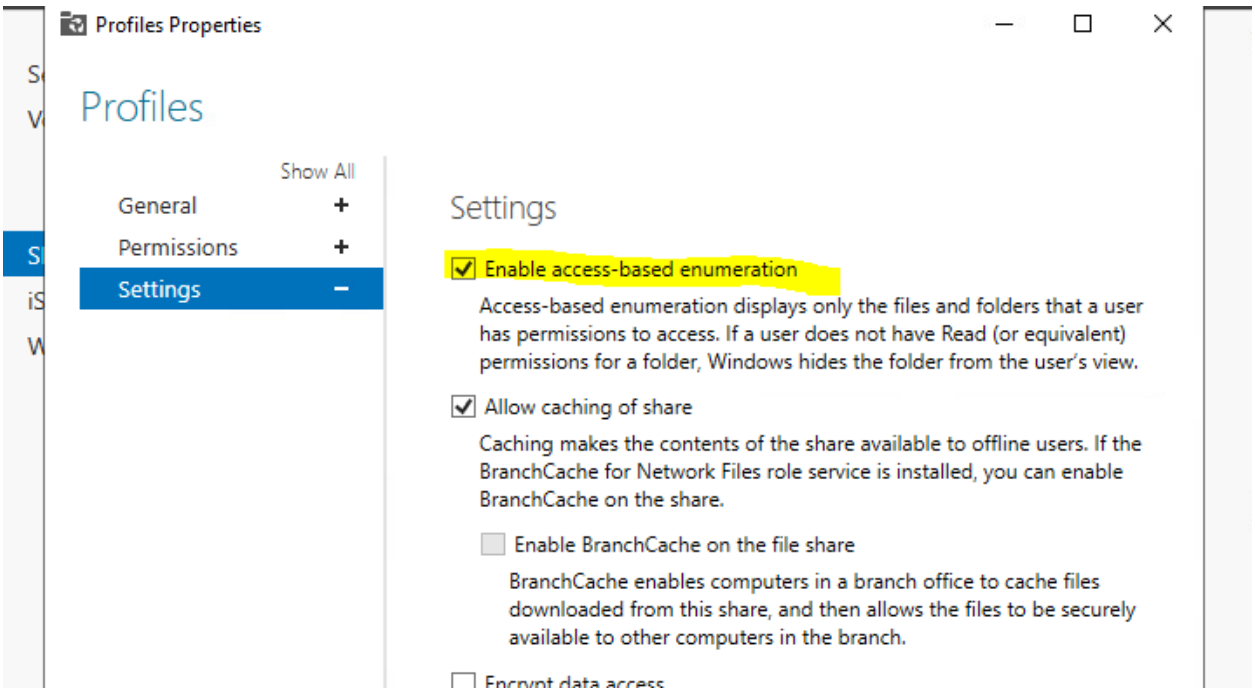
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Right Assignment -> Allow log on locally перебиваем туда все группы из пункта выше + добавляем Group3



ROAMING PROFILES

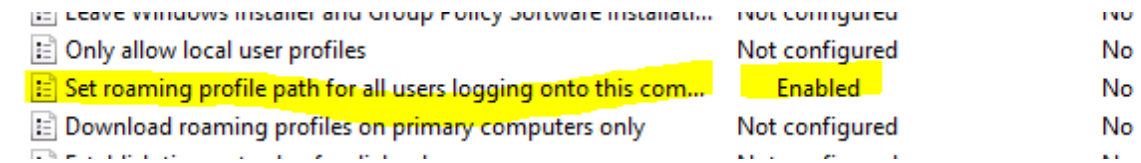
Для членов группы Group3 настройте использование перемещаемых профилей (место хранения профилей выберите самостоятельно); каждый пользователь должен иметь доступ только к папке своего профиля, в том числе при обращении к папке по сети через файловый менеджер.

Папку создаем на DC по пути C:\Profiles, «расшариваем» её с Shared Permissions – Everyone Full Access, включаем Access Based Enumeration и разрешаем Group3 Write&Modify.

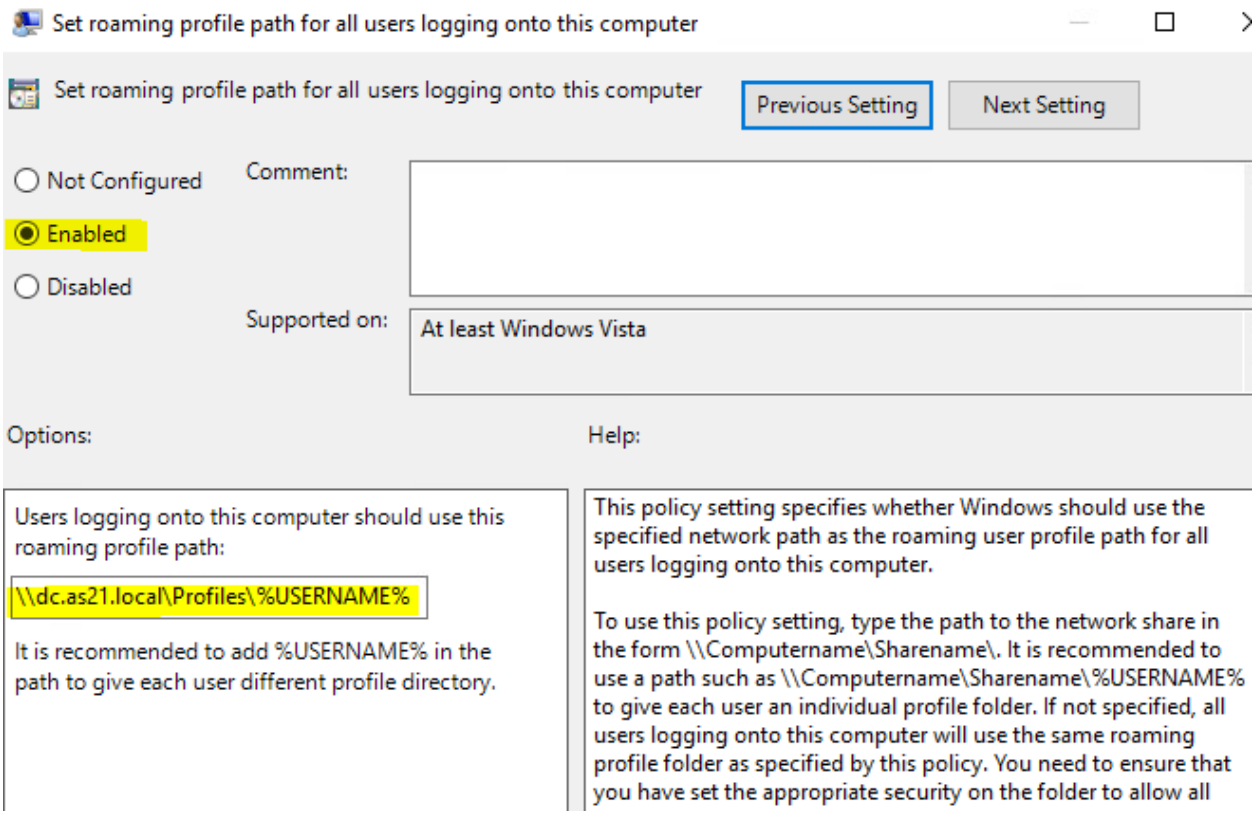


План А

GPO на домен: Computer Configuration > Policies > Administrative Templates > System > User Profiles > Set roaming profile path for all users logging onto this computer -> Enabled



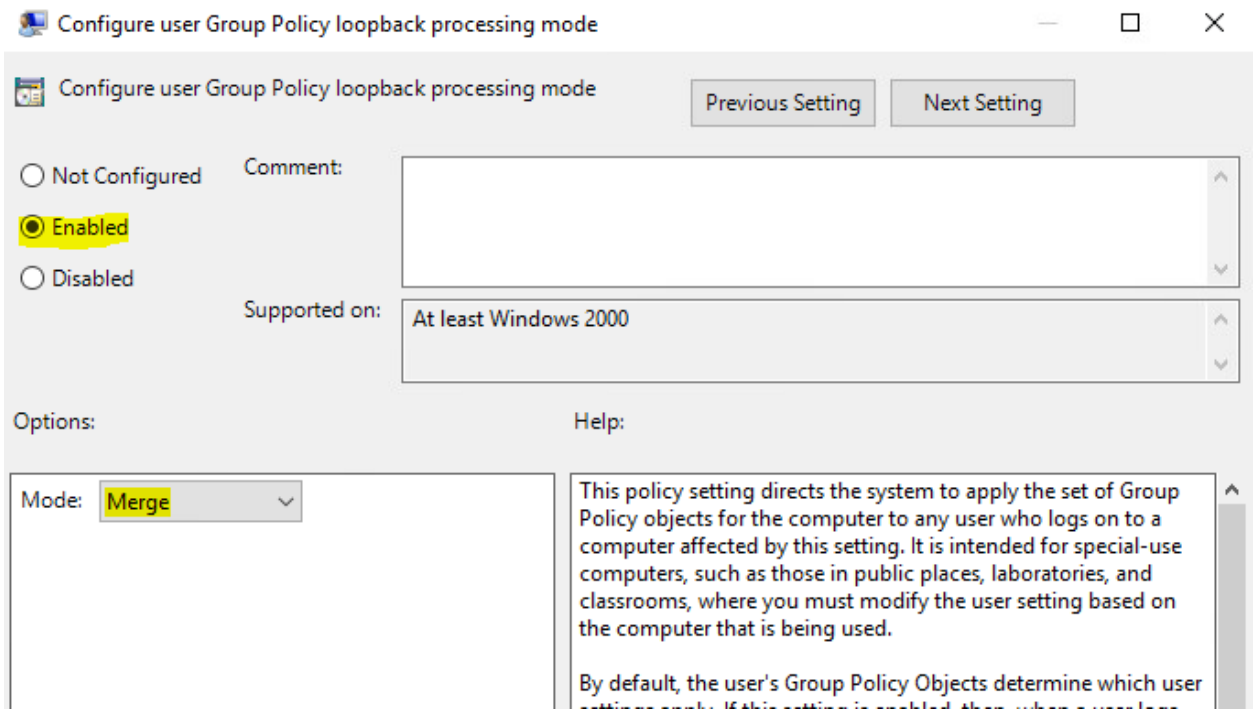
Пишем путь \\dc.as21.local\Profiles\%USERNAME%

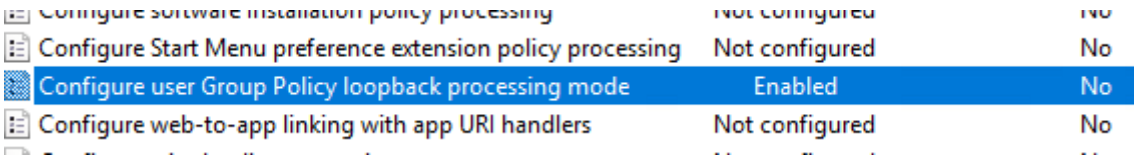


Идем сюда:

Computer Configuration > Policies > Administrative Tempates > System > Group Policy > Configure user Group Policy loopback processing mode -> Enabled

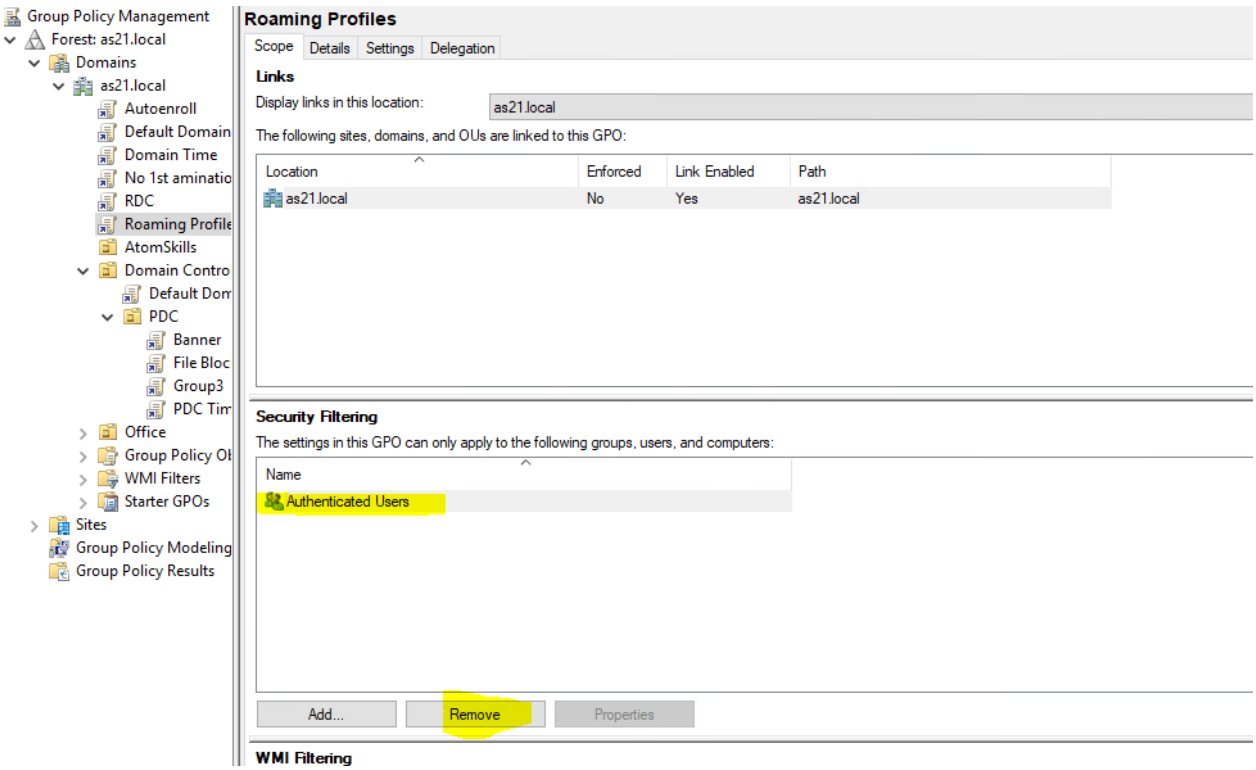
Ставим параметр Merge



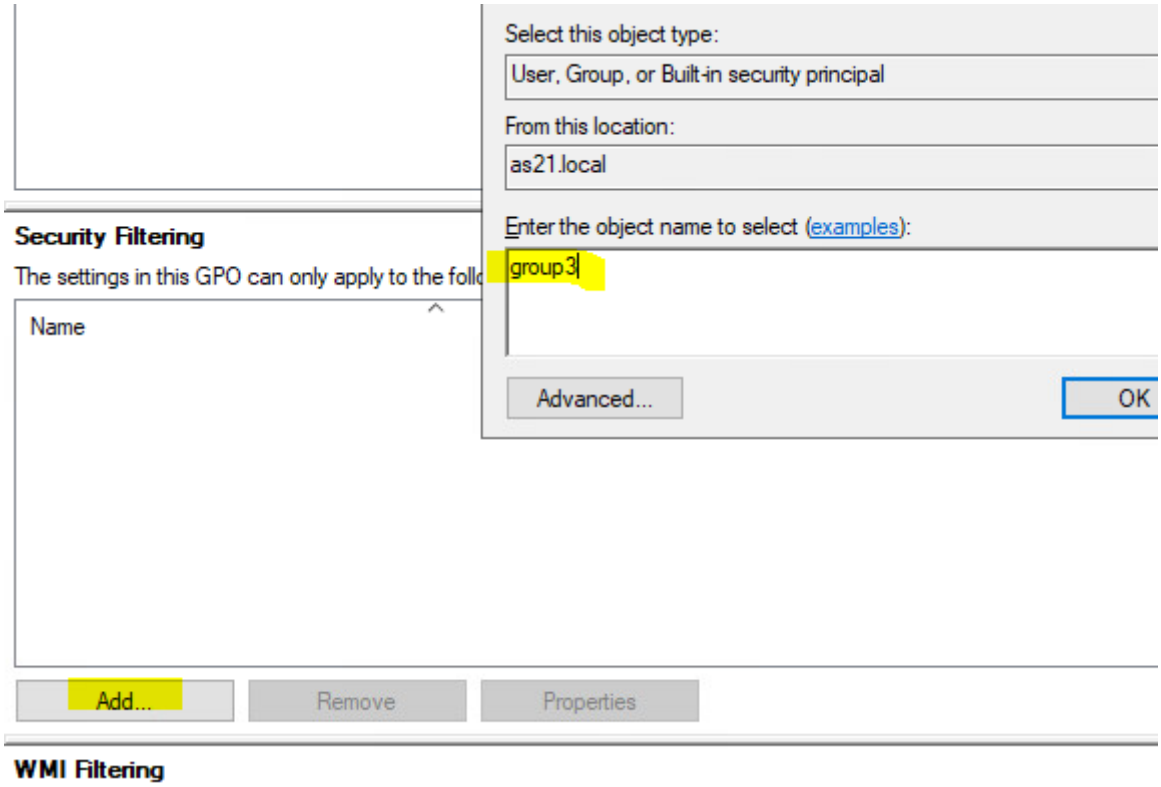


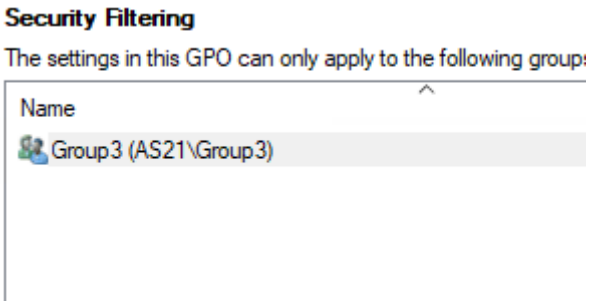
Теперь нужно ограничить распространение данной политики группой Group3

Выделяем политику и в окне Scope удаляем Authenticated Users

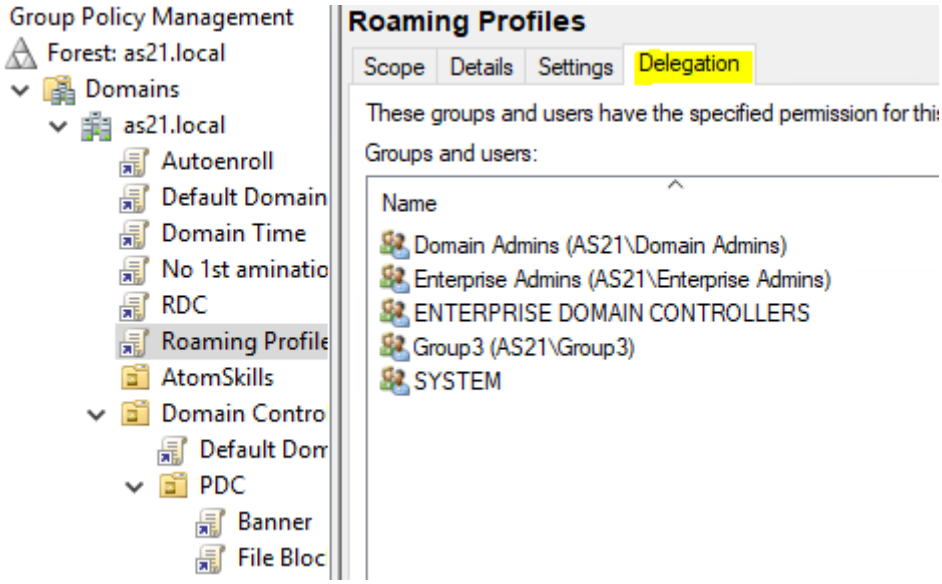


И добавляем Group3

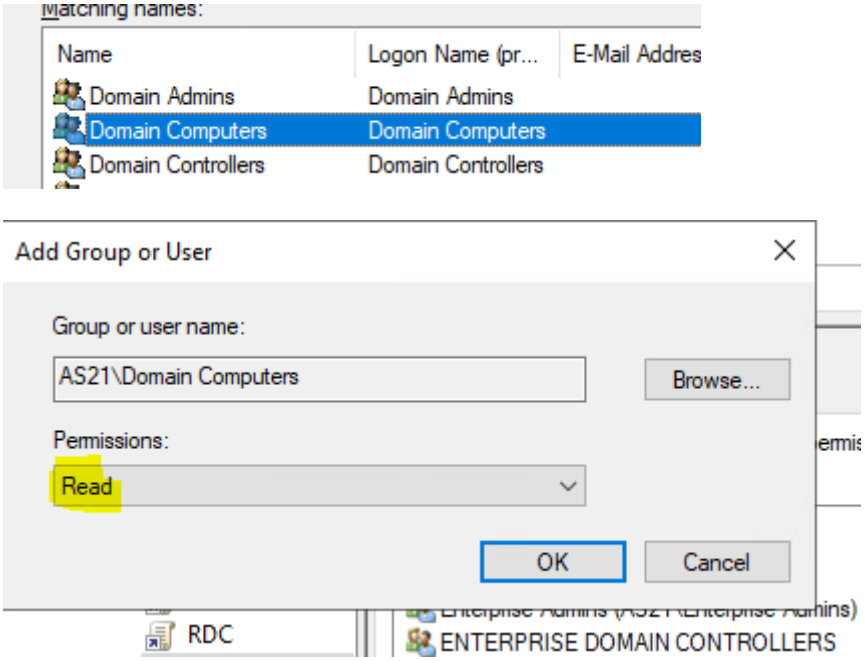




Переходим во вкладку Delegation



Добавляем Domain Computers с правами Read

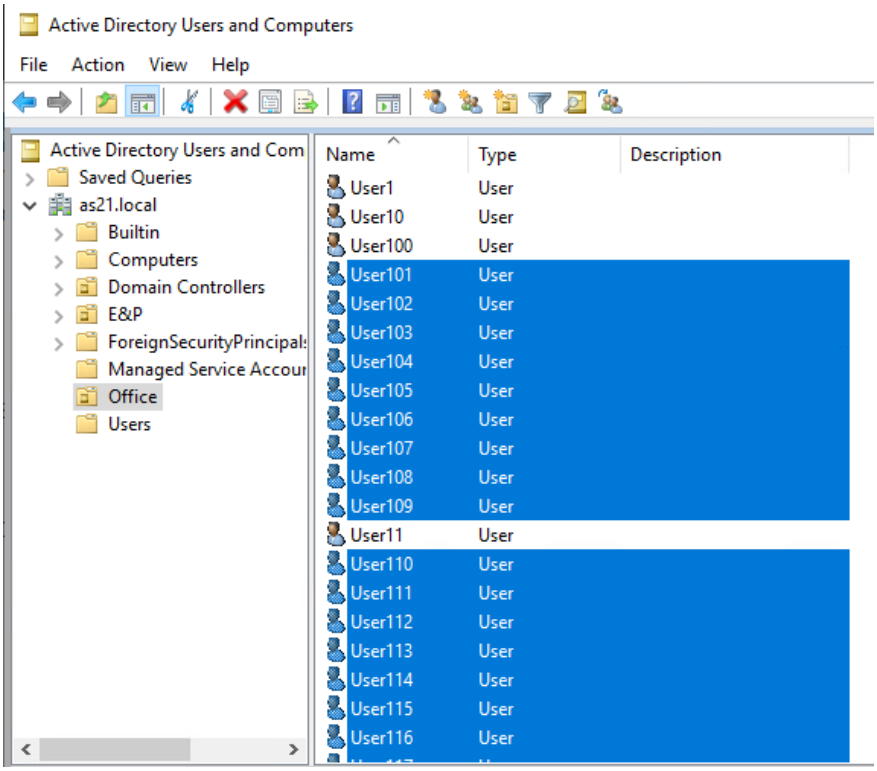


План Б

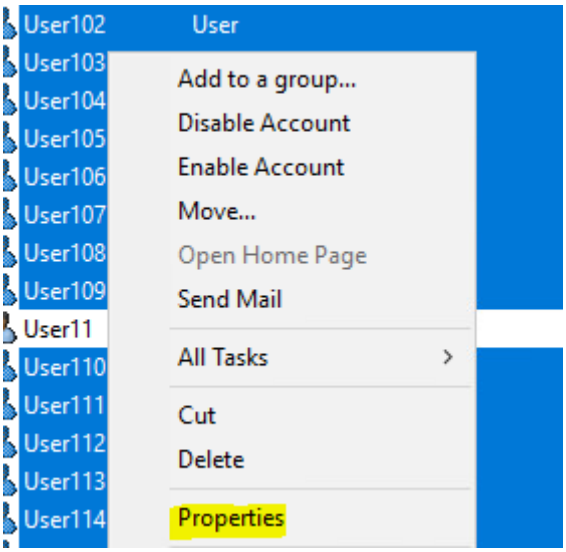
Если план А не завелся

Удаляем GPO с плана А

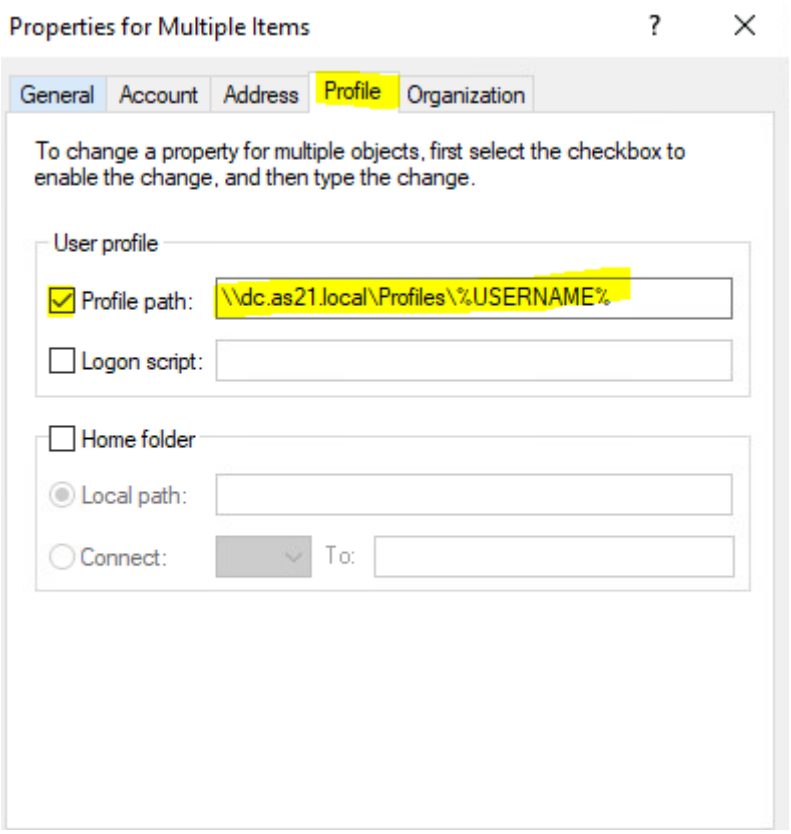
Идем в Active Directory Users and Computers. Выделяем пользователей группы Group3



Вызываем их свойство



В разделе Profile прописываем путь к профилям (Profile path) - \\dc.as21.local\Profiles\%USERNAME%

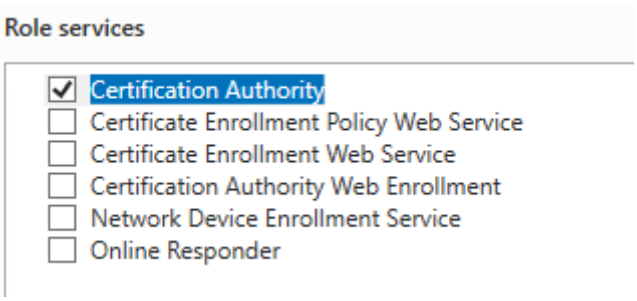


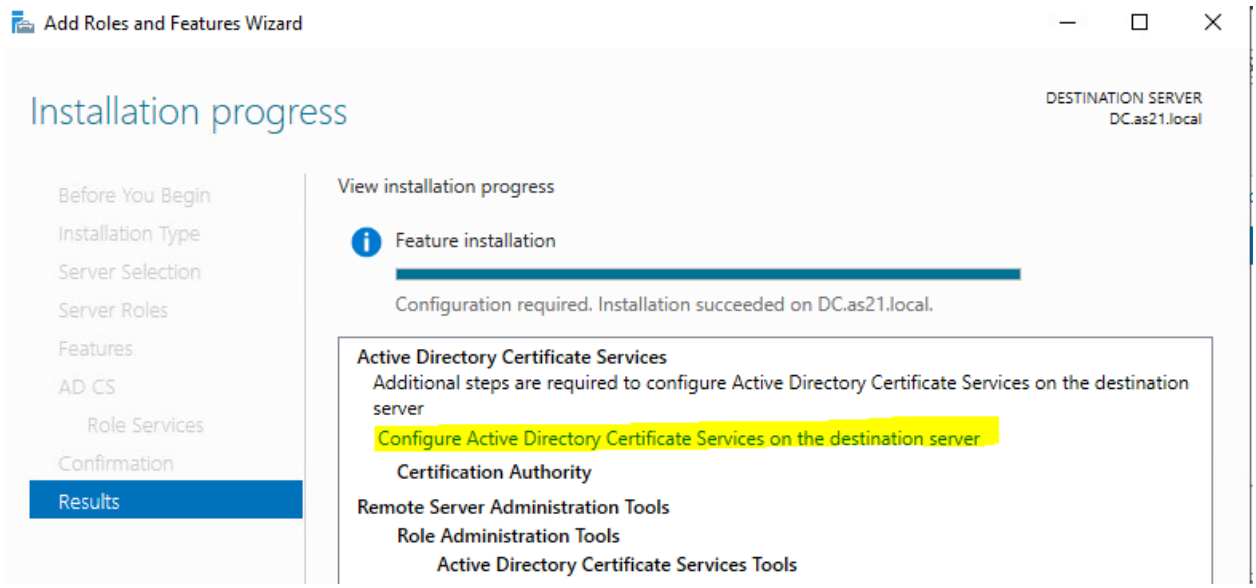
ROOT CA

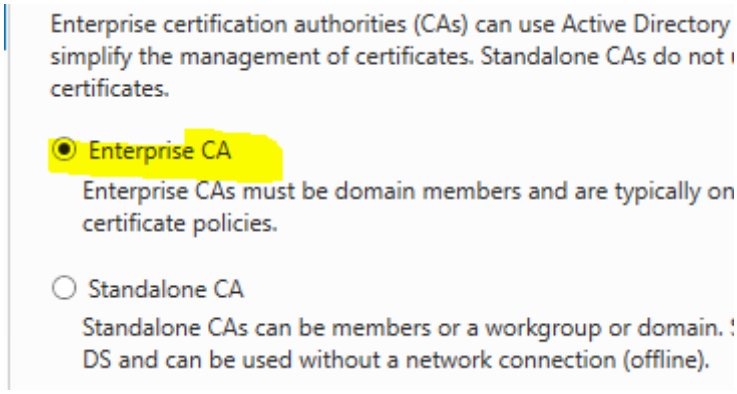
Настройте корневой центр сертификации на контроллере домена DC

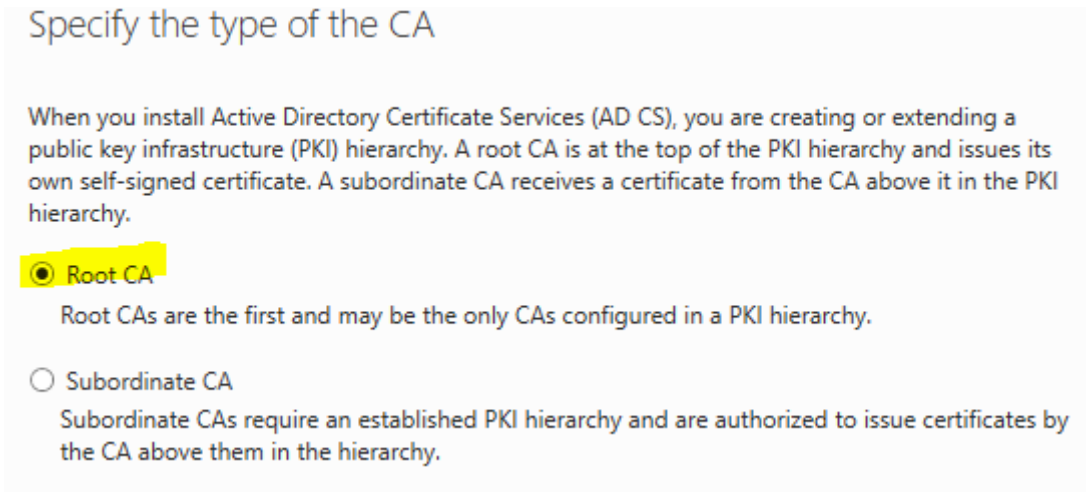
Базовая настройка RootCA

ВАЖНО!!! СА делать после того как будет закончена настройка времени

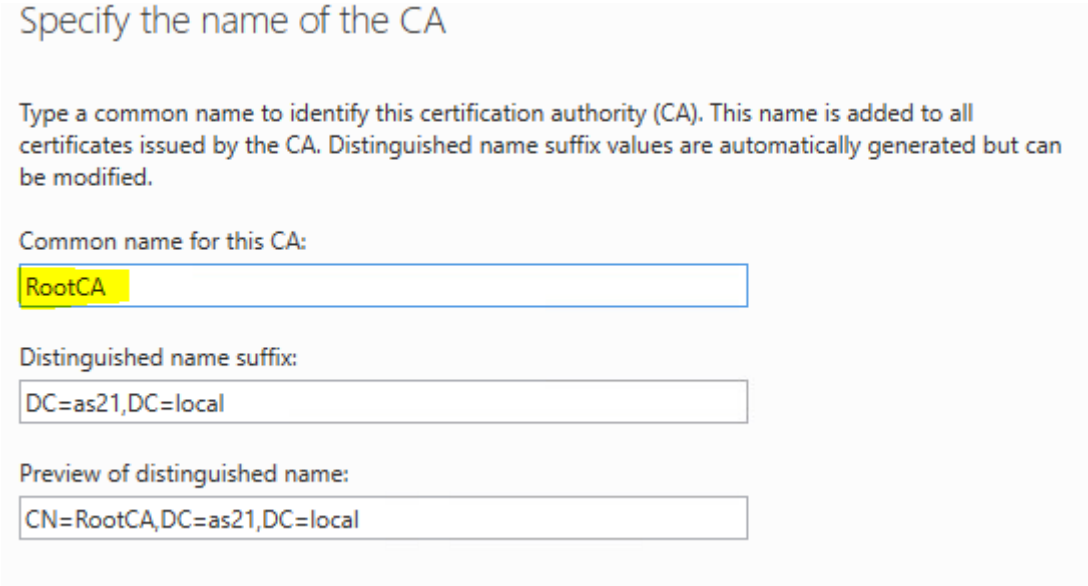




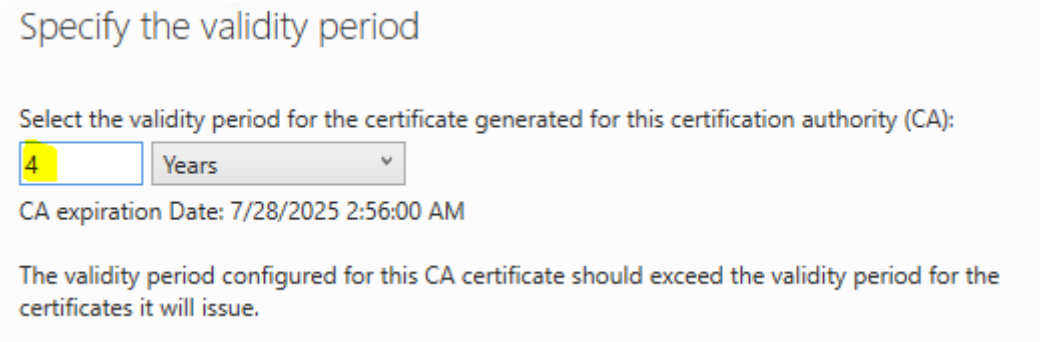




i. Имя настраиваемого центра сертификации - RootCA.



ii. Срок действия сертификата - 4 года.



Обеспечьте доверие данному центру сертификации на всех компьютерах и устройствах в соответствии с настоящим конкурсным заданием.

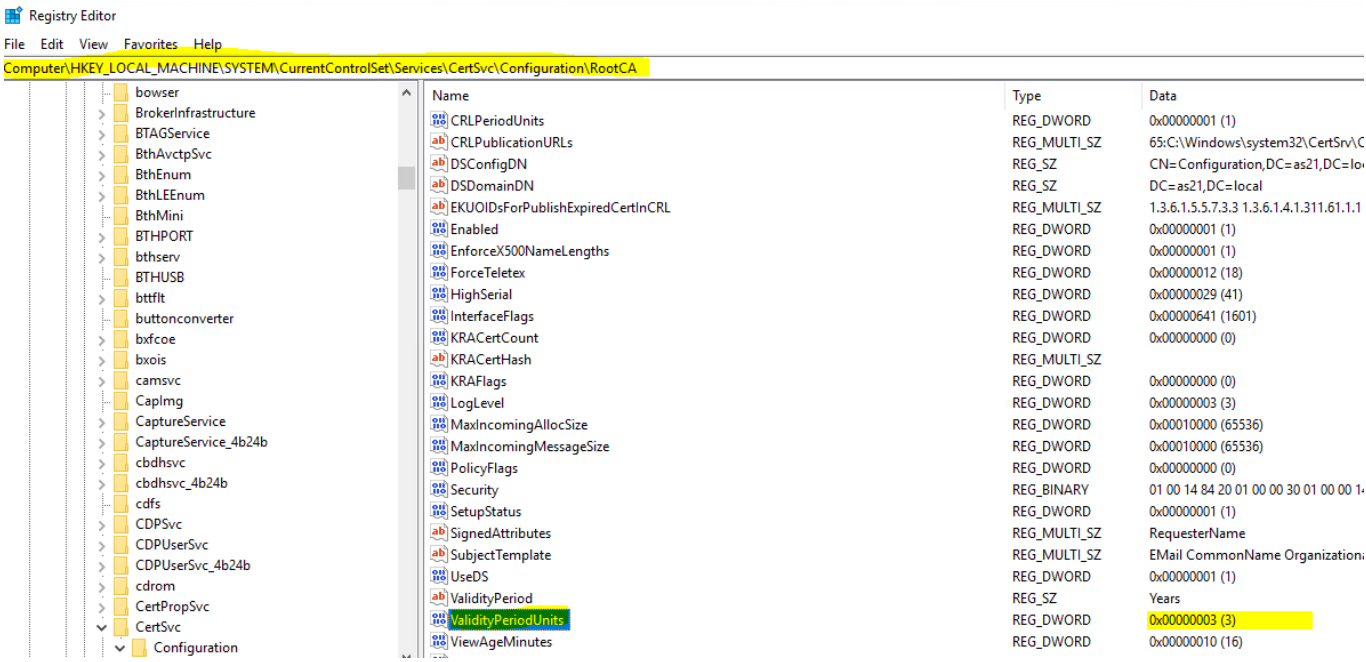
Нужно прописать сертификат на всех не доменных устройствах, в которых нужно по заданию

Подготовка RootCA для выпуска сертификата SubCA

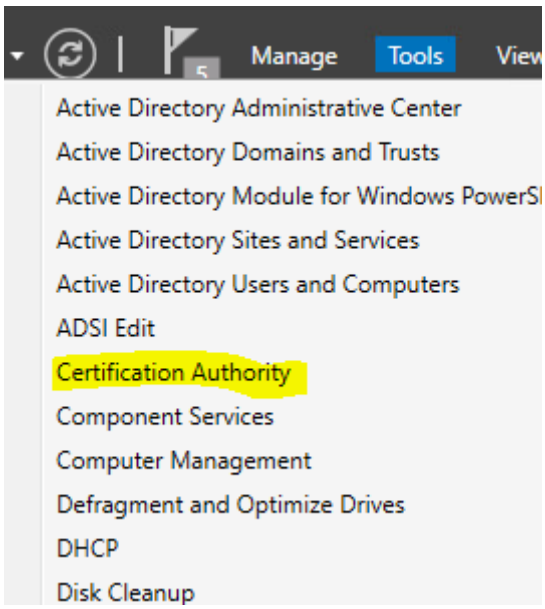
На DC запускаем редактор реестра (regedit)

Переходим в раздел HKLM > SYSTEM > CurrentControlSet > Services > CertSvc > Configuration > RootCA

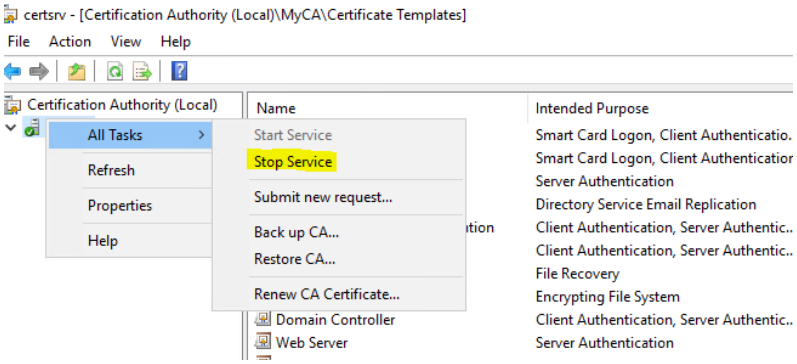
Меняем значение ValidityPeriodUnits на 3



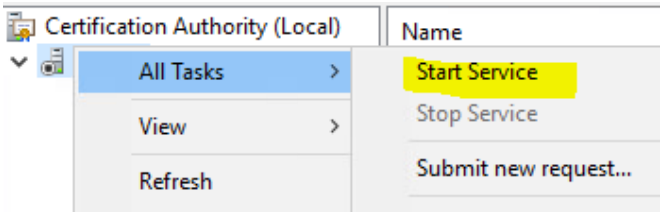
Идем в оснастку Certification Authority



Правую кнопку по названию центра сертификации RootCA > All Tasks -> Stop Service



Правую кнопку по названию центра сертификации RootCA > All Tasks -> Start Service



На всех компьютерах под управлением ОС Microsoft Windows обеспечьте функционирование Defender Firewall. При этом работоспособность настроенных ранее сервисов не должна нарушиться.

Настройка компонентов ОС Microsoft Windows в ЦОД

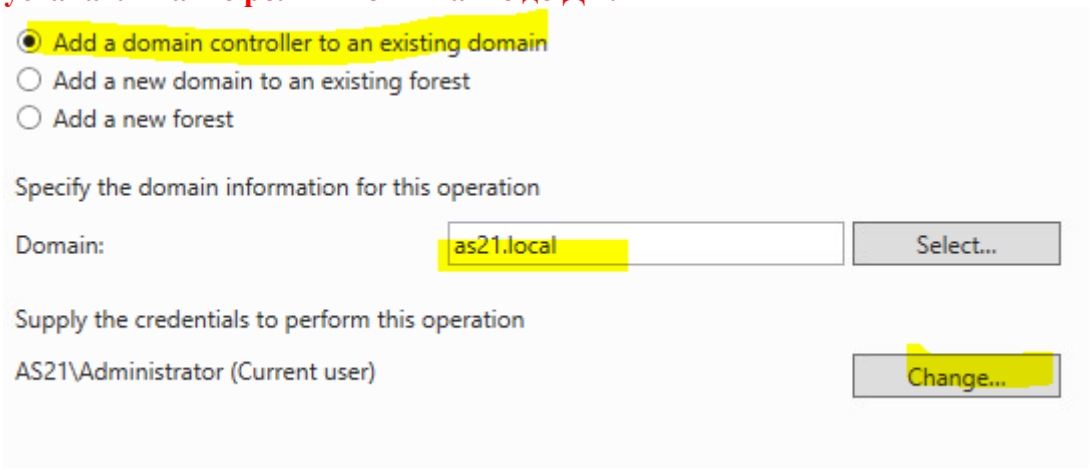
1. На WINSRV1 настройте дополнительный контроллер домена AS21.local.
1. Данный дополнительный контроллер домена должен быть контроллером только для чтения.

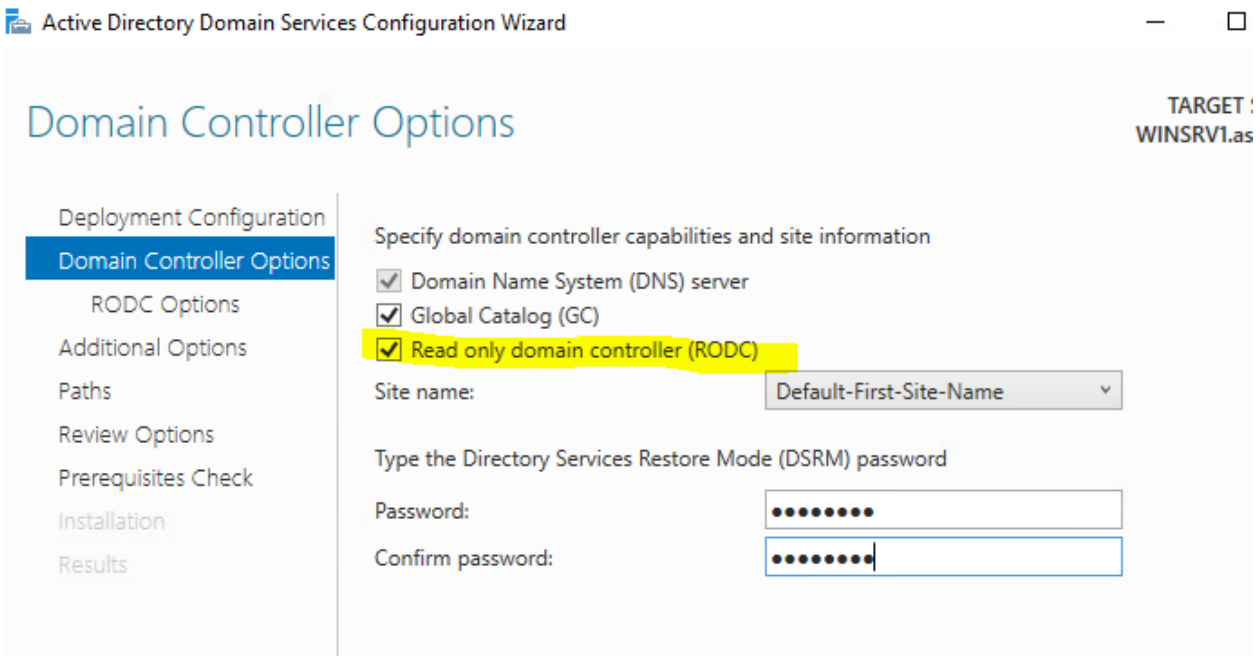
НАСТРОЙКА RODC

Установка контроллера домена

ВАЖНО!!! Сначала делаем RDS и DFS!!!

Перед тем как сделать его ДК, сначала введите его в домен as21.local, затем устанавливайте роль и повышайте до ДК.



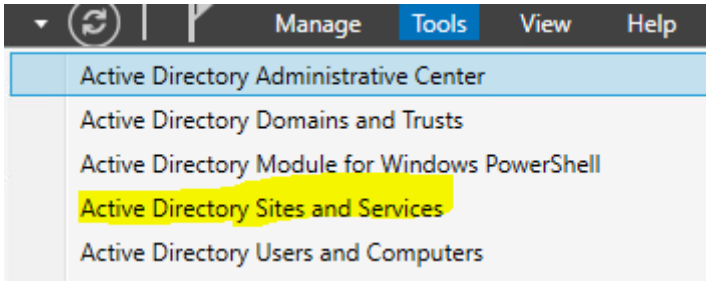


Настройка сайтов

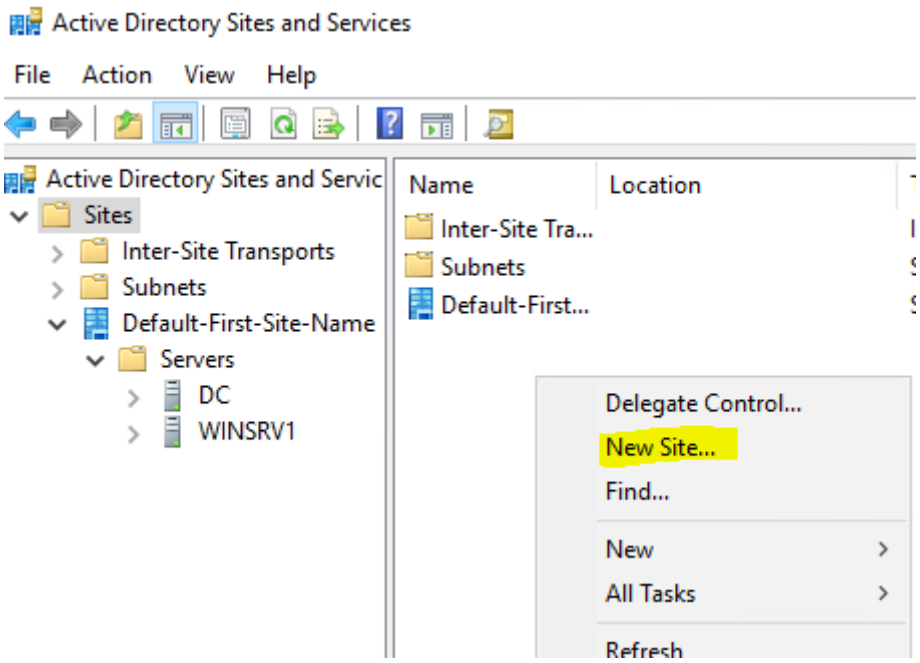
Сайты основного и дополнительного контроллеров домена AS21.local должны быть разными.

После установки RODC, если не создали в пункте про временные зоны, создаем сайт – Datacenter

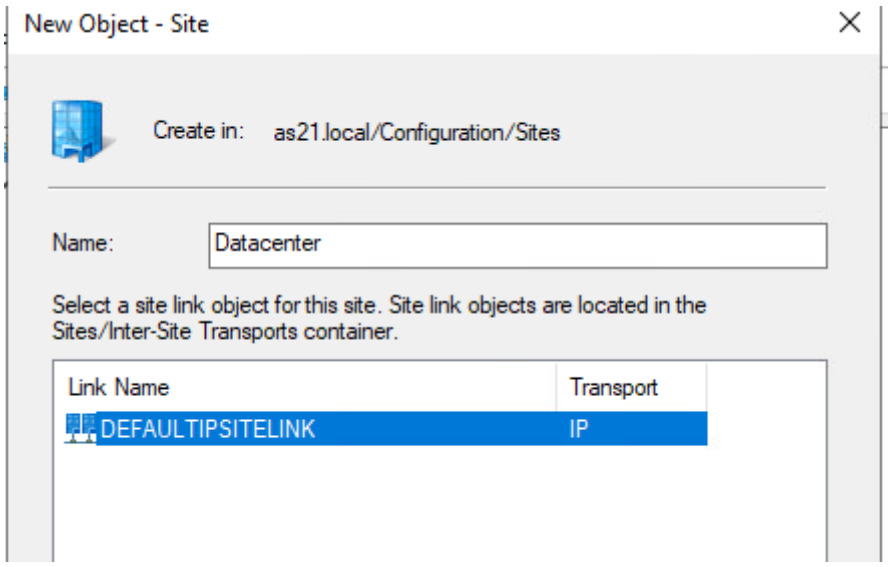
Открываем на DC оснастку Active Directory Sites and Services



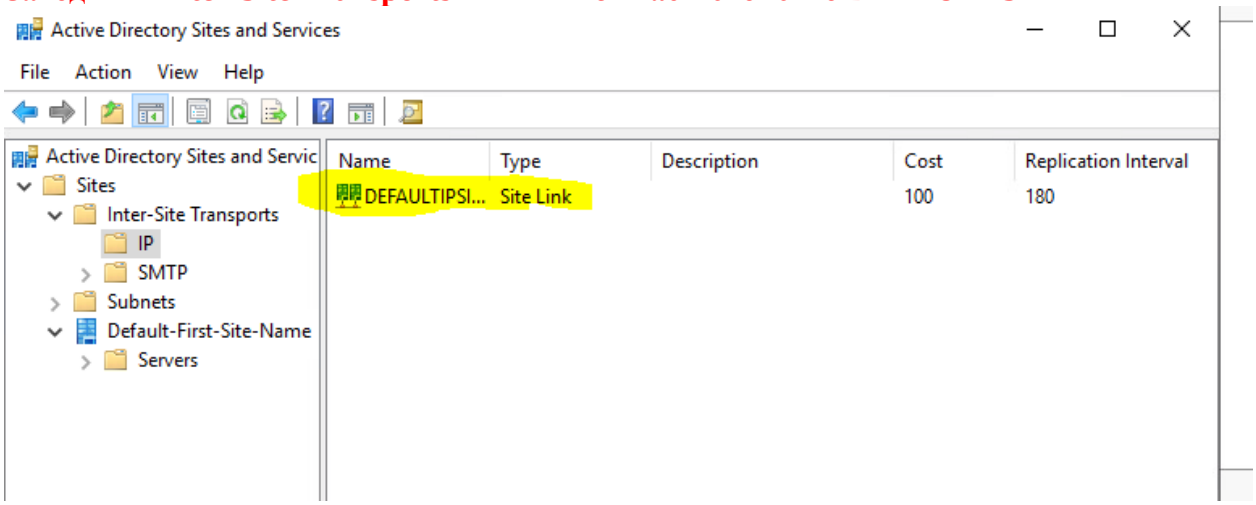
В разделе Sites создаем новый сайт – New Site



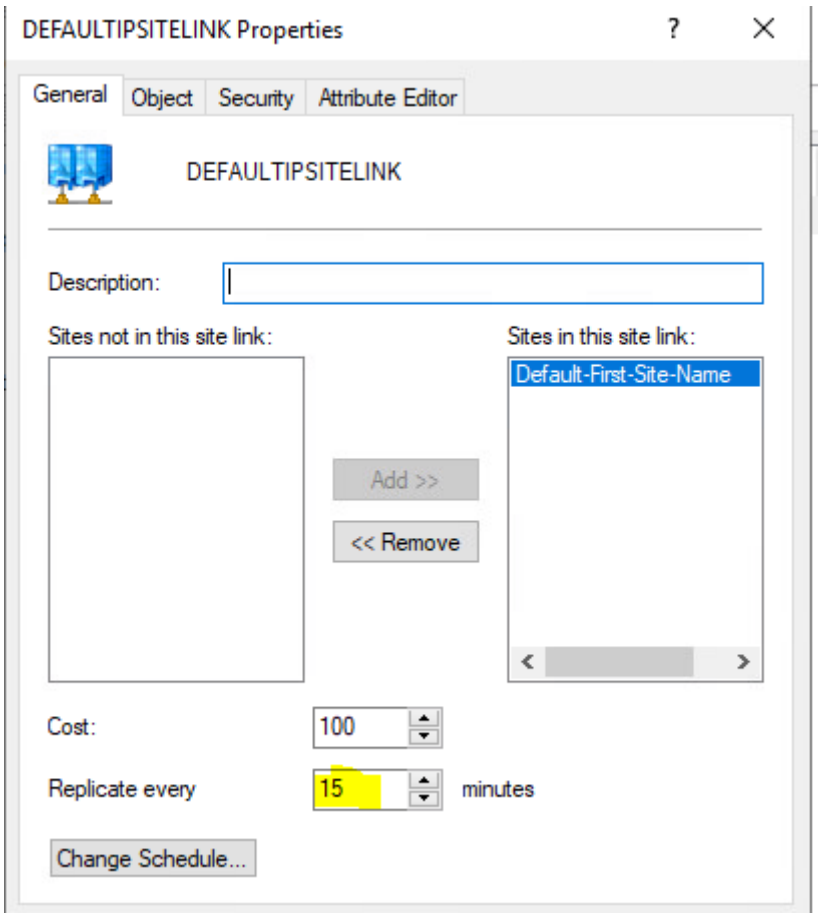
Выбираем для него соединение между сайтами по умолчанию



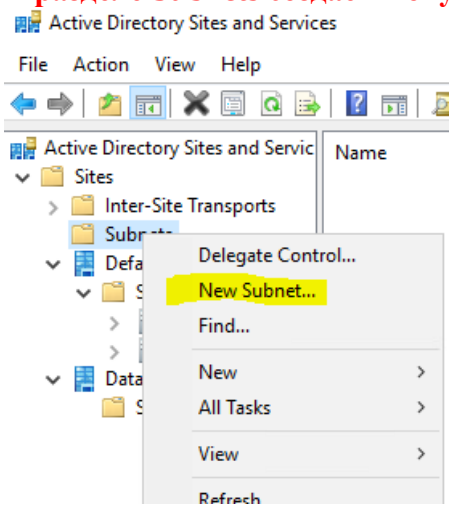
Настроим наименьшую периодичность репликации – 15 минут
Заходим в Inter-Site Transports > IP и вызываем свойство DEFAULTSITELINK



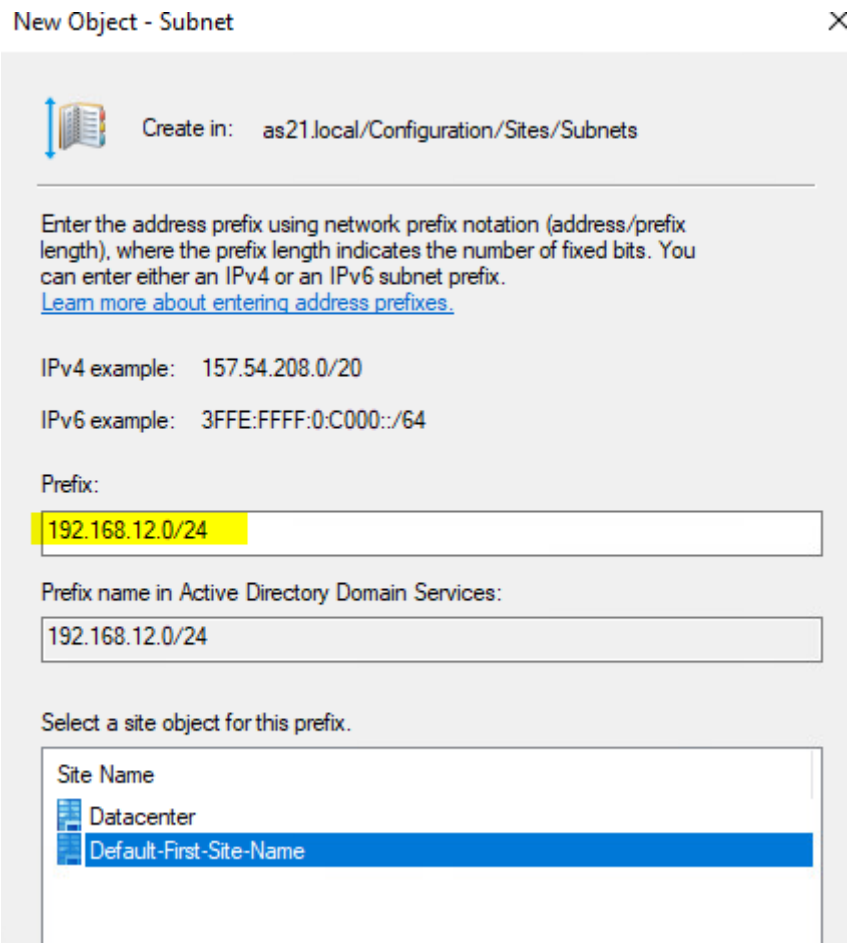
Выставляем значение Replicate every равное 15 минутам



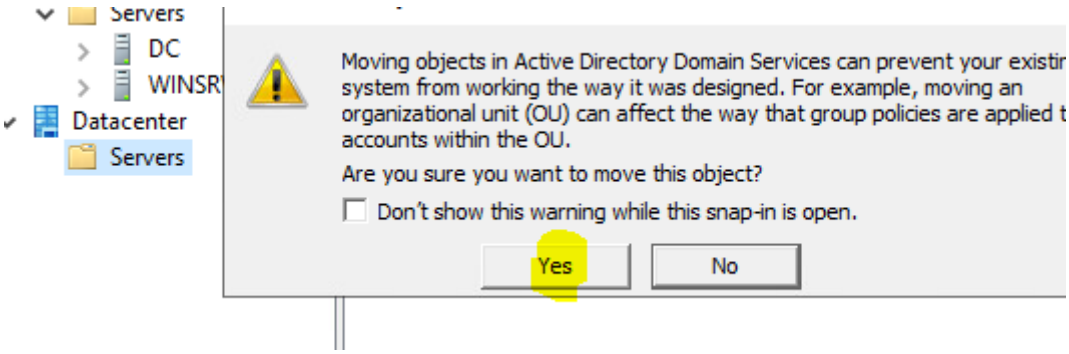
Создаем и закрепляем подсети за сайтами (все)
В разделе Subnets создаем новую подсеть - New Subnet



Пишем наименование сети формата сеть/маска. Назначаем её соответствующий сайт



Переносим соответствующий ДК в сайт. Просто перетаскивая его из папки Servers одного сайта в другой

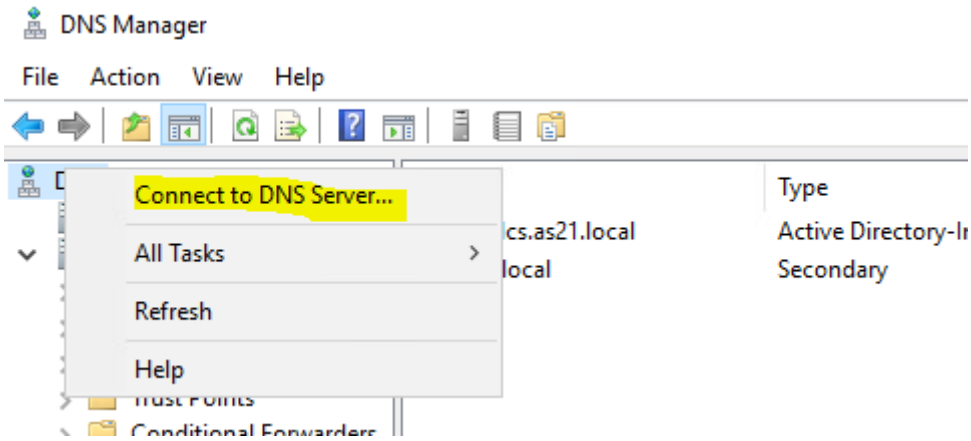


В случае появления доменных Windows-клиентов в ЦОД, они должны в первую очередь обращаться к дополнительному контроллеру, и только если он не доступен - к основному.

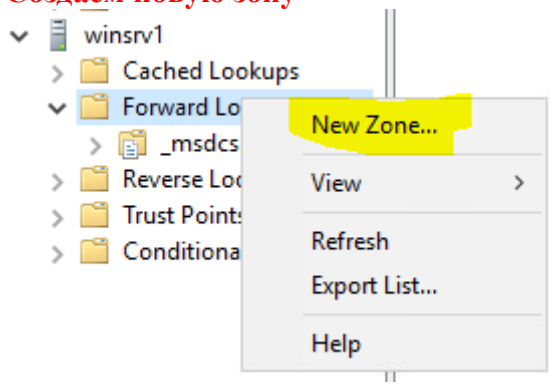
Настройка DNS на WINSRV1

Передайте на WINSRV1 все зоны прямого просмотра с сервера DC. На WINSRV1 не должно быть ни одной основной зоны.

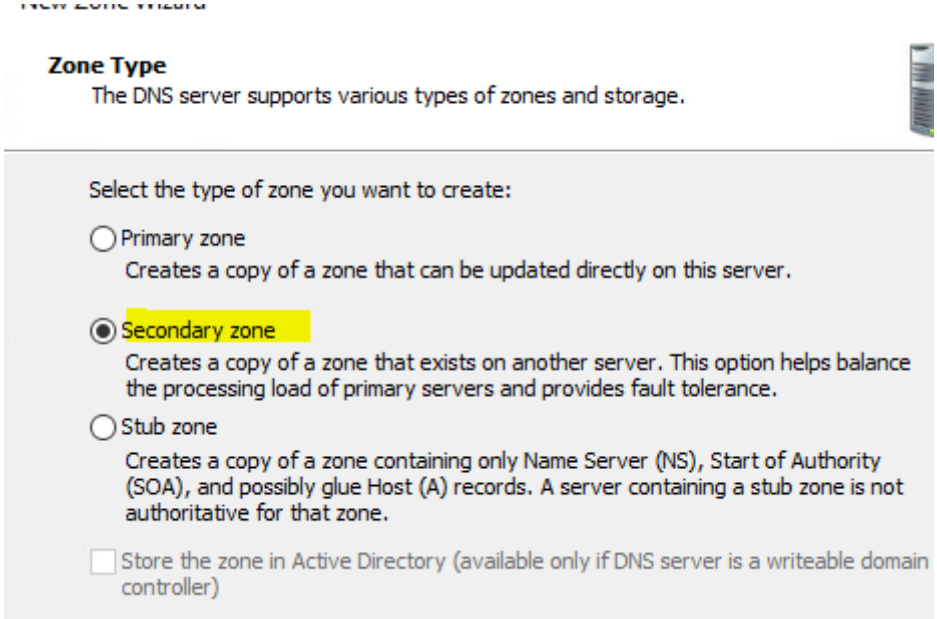
Открываем на DC оснастку DNS. Подключаемся к серверу WINSRV1



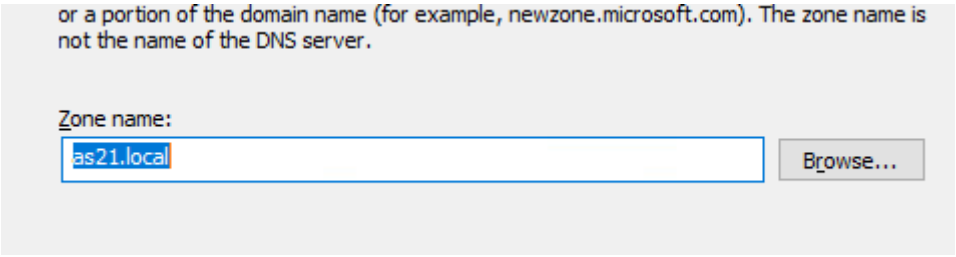
Создаем новую зону



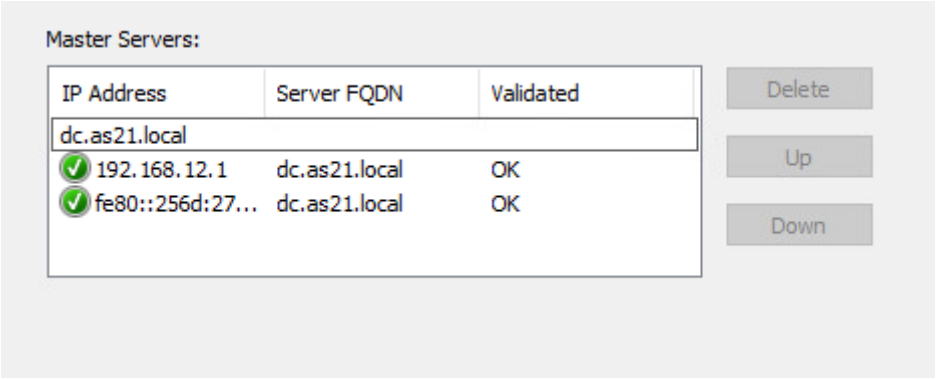
Выбираем тип зоны Scondary zone



Вписываем имя зоны, которую нужно перенести (по заданию это as21.local)

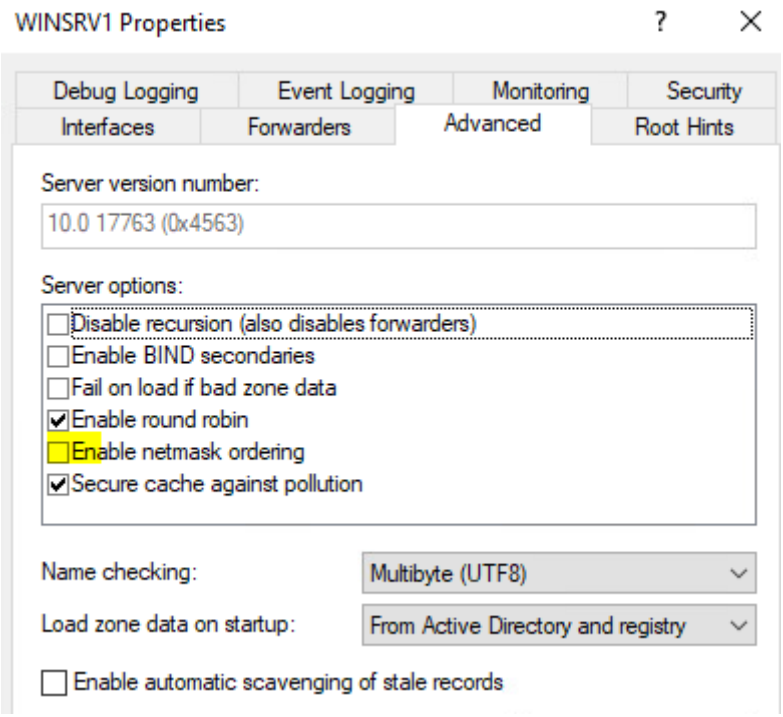


Указываем с какого сервера забирать зону – dc.as21.local



Обязательно настроить Round Robin на WINSRV1

В свойствах DNS сервера в Advanced убрать галку на Enable netmask ordering



НАСТРОЙКА SUBCA НА WINSRV2

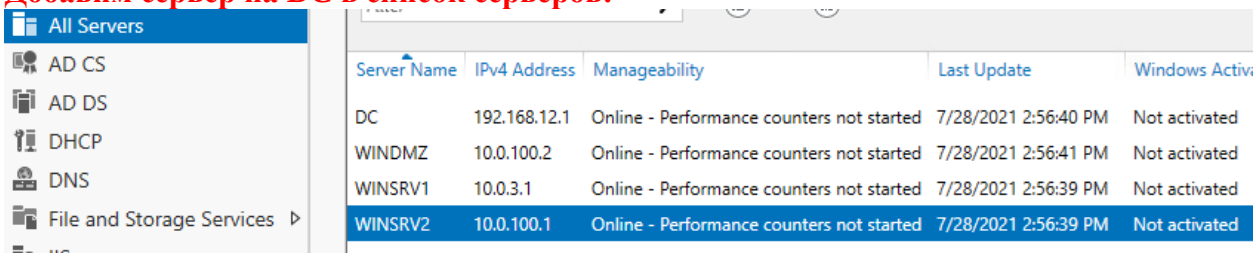
Базовая настройка

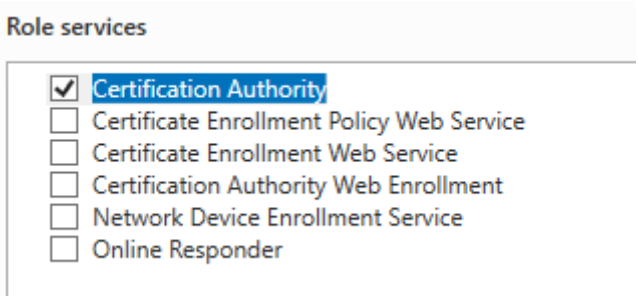
Сделайте сервер членом домена AS21.local.
Настройте на сервере подчиненный доменный центр сертификации с именем SubCA с сертификатом, действующим 3 года.

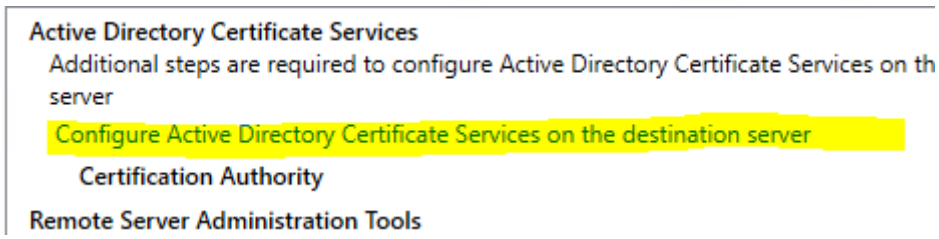
Вводим в домен.

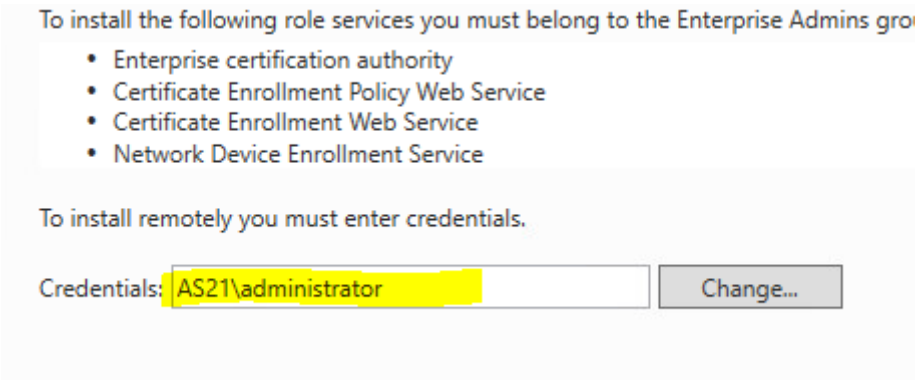
Настройте на сервере подчиненный доменный центр сертификации с именем SubCA.

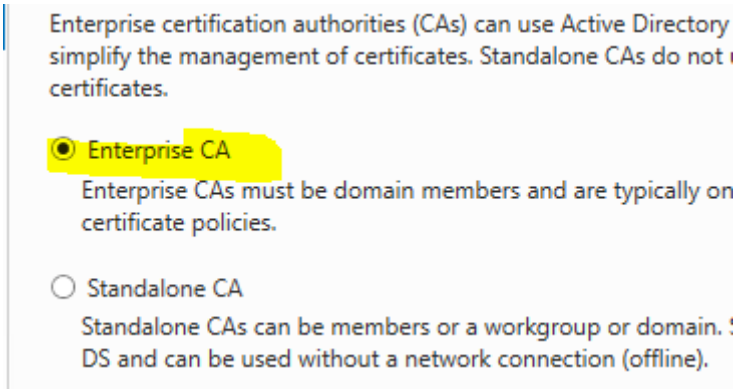
Добавим сервер на DC в список серверов:

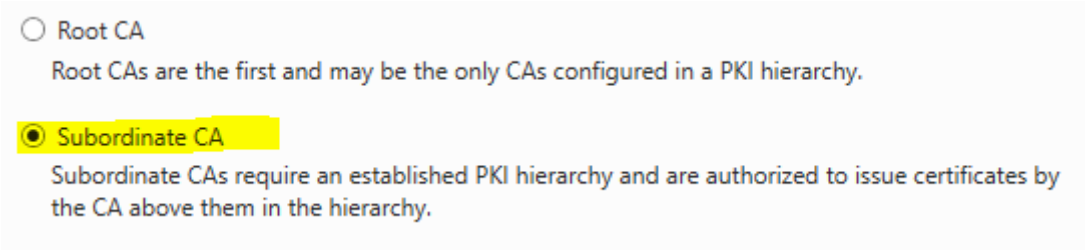


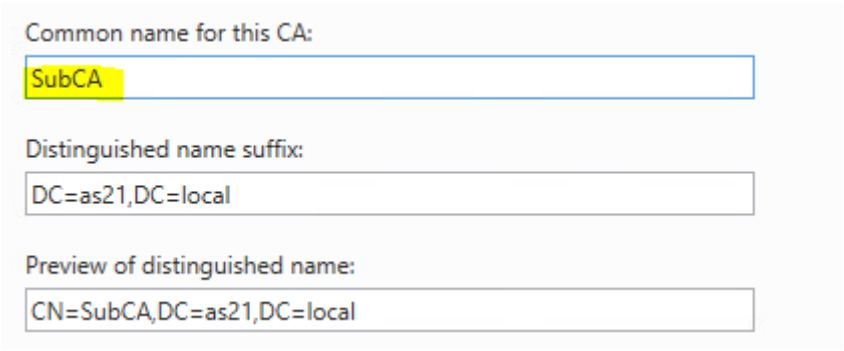


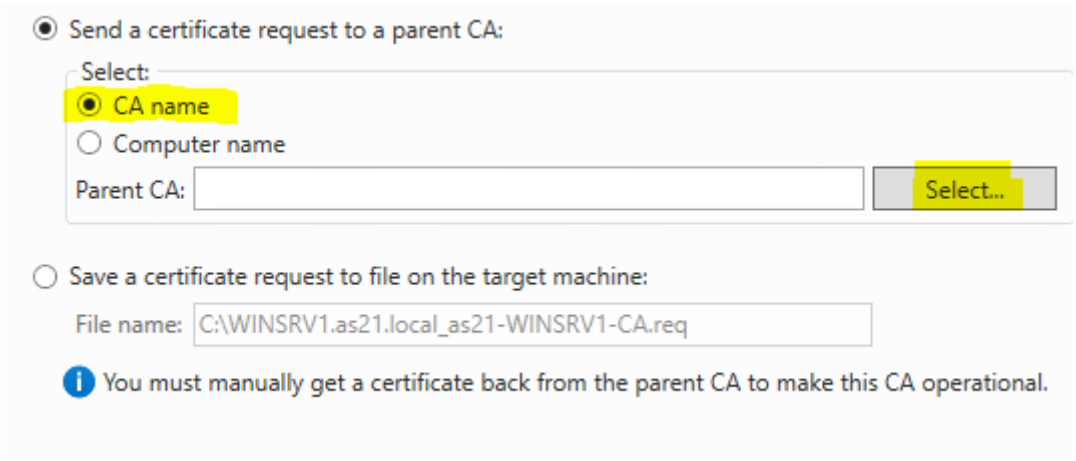


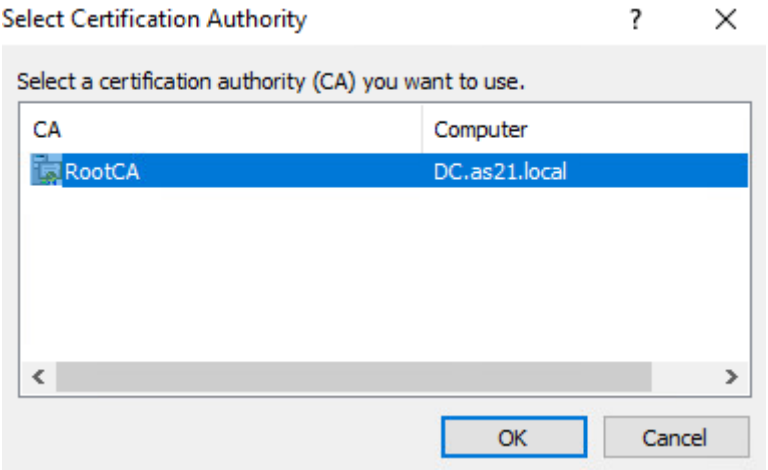










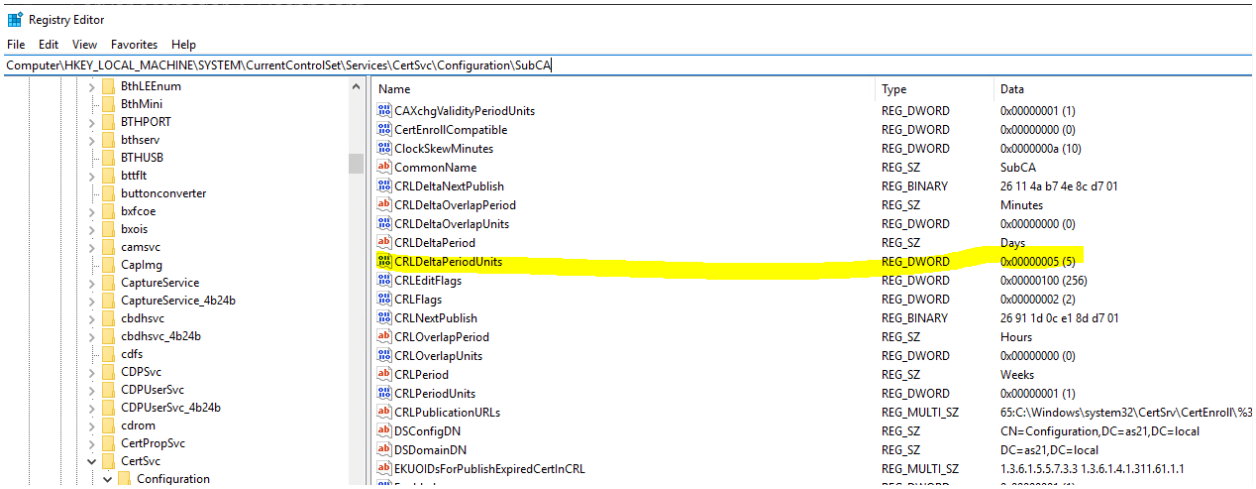


Настройка CRL на SubCA

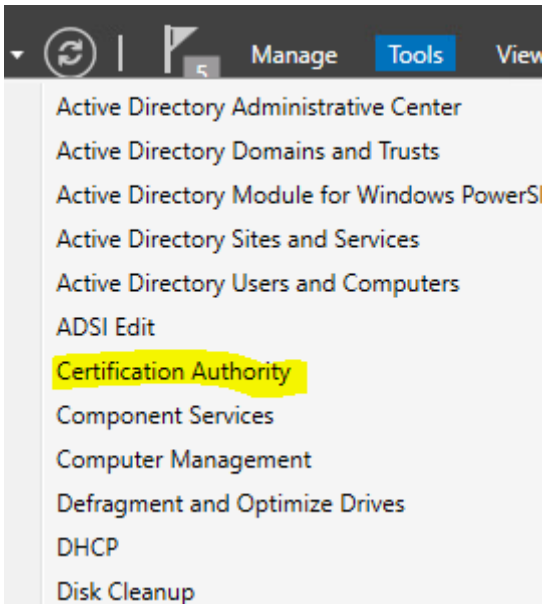
Открываем реестр на SubCA (regedit)

Переходим в раздел HKLM > SYSTEM > CurrentControlSet > Services > CertSvc > Configuration > SubCA

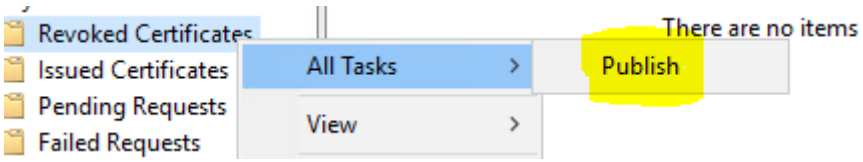
Меняем значение CRLDeltaPeriodUnits на 5

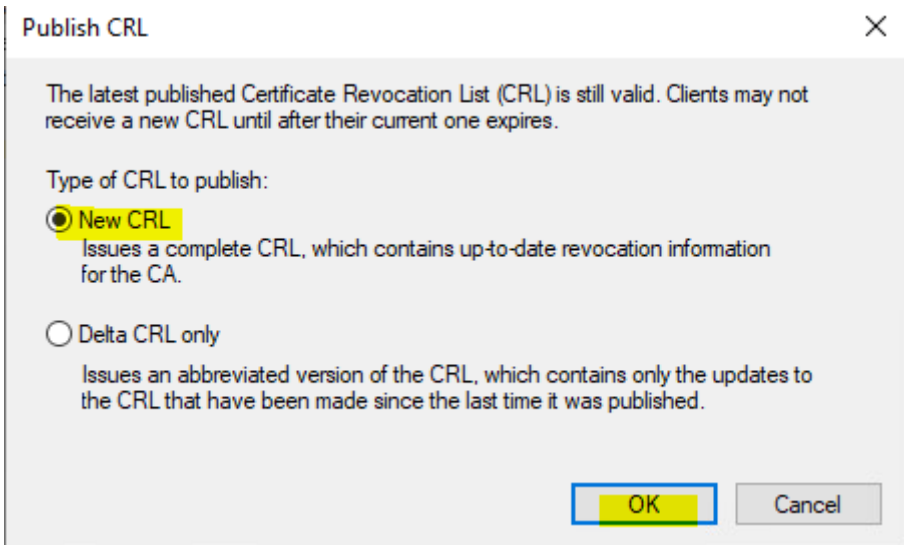


Идем в оснастку Certification Authority



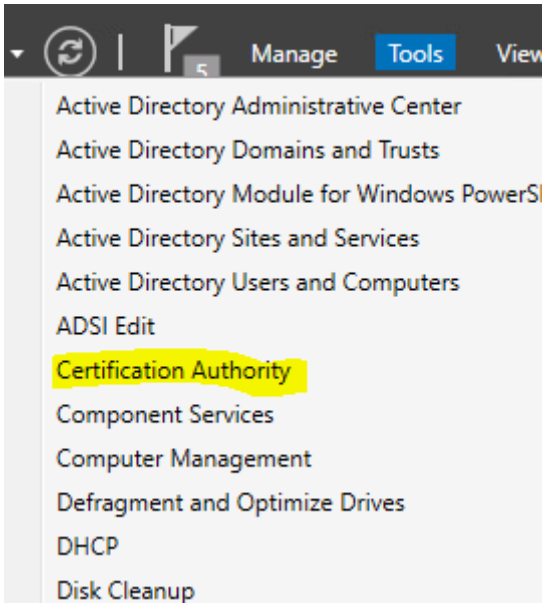
Правую кнопку по Revoked Certificates > All Tasks > Publish

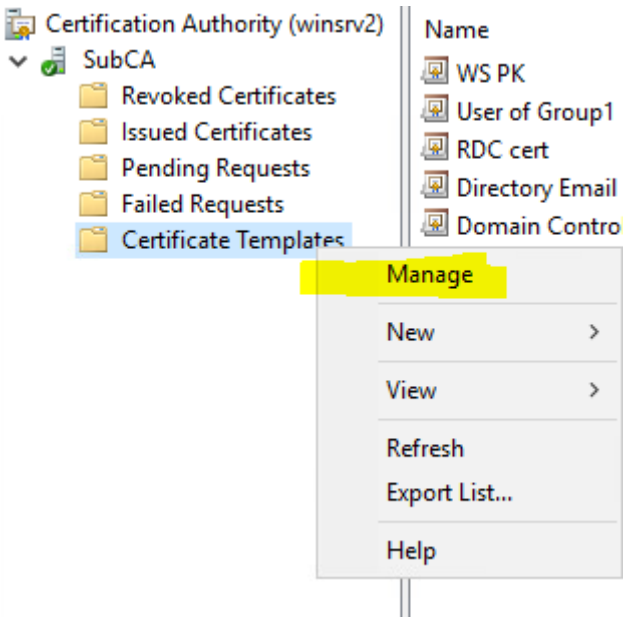




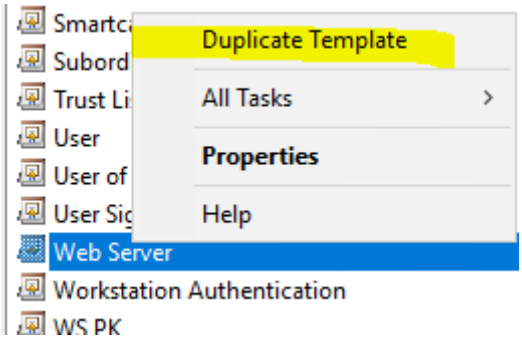
ПОДГОТОВКА ШАБЛОНА ДЛЯ WEB ДОСТУПА

Идем в оснастку Certification Authority. Правую кнопку по Certificate Templates > Manage

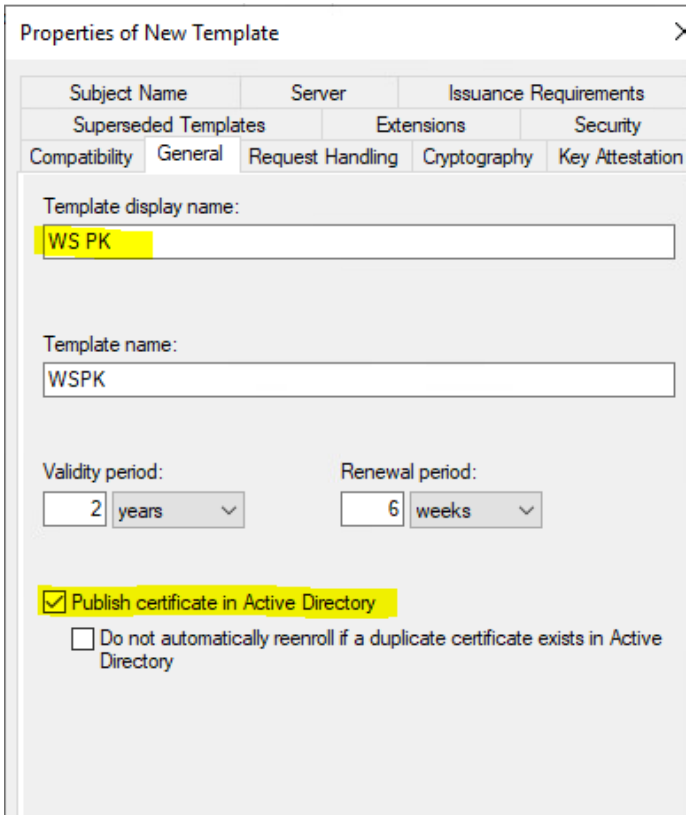


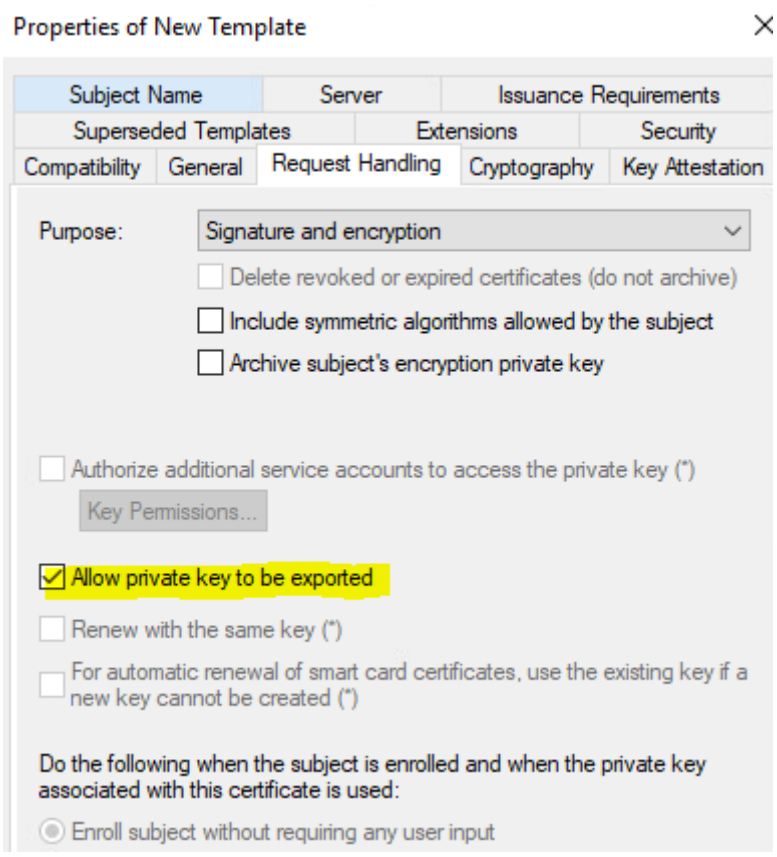


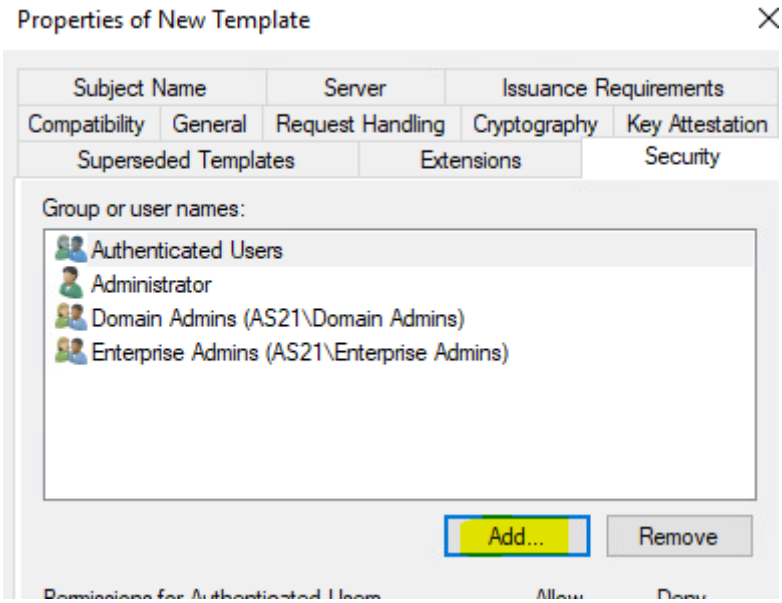
Сделаем клон шаблона Web Server

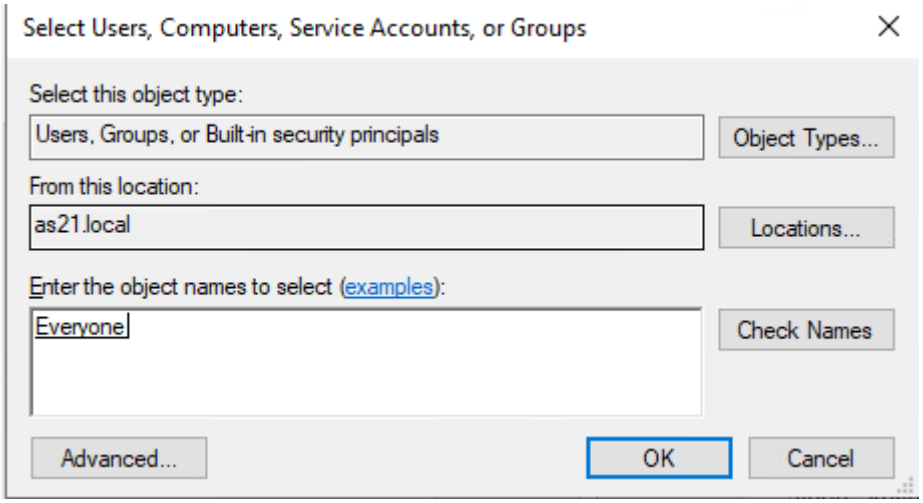


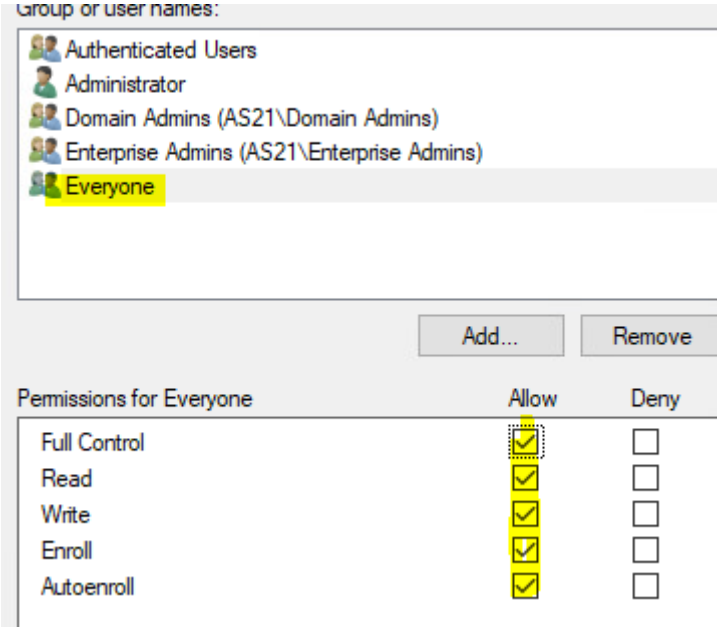
Выполним настройки нового шаблона

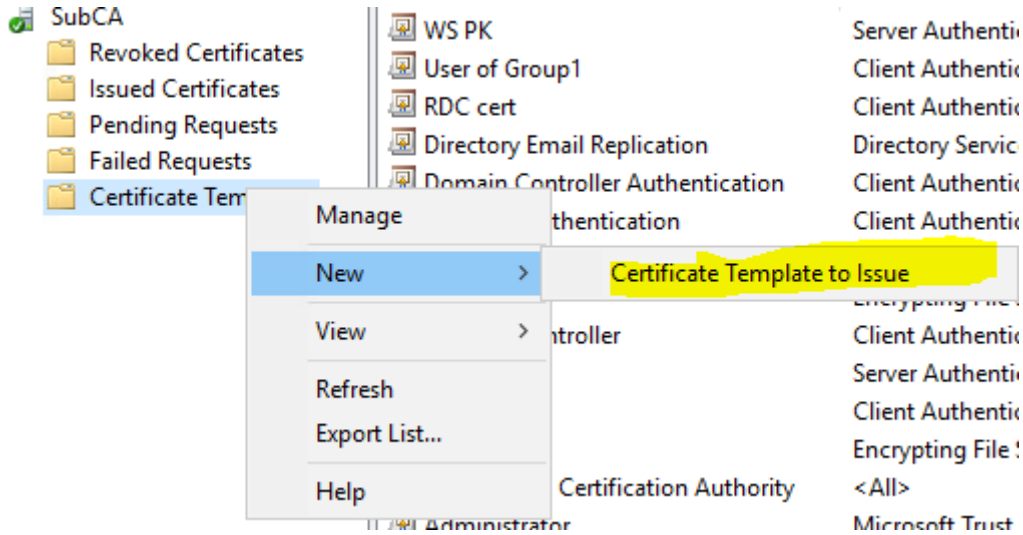


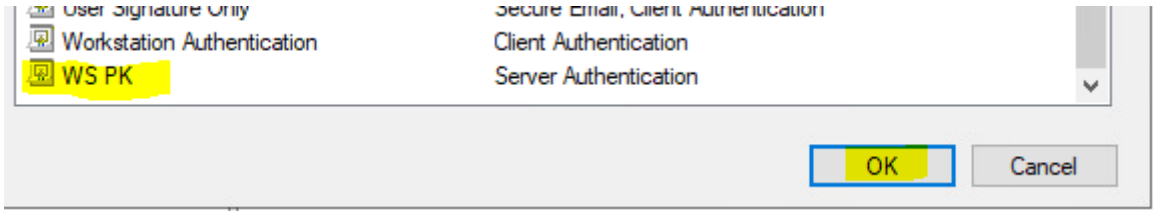

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Purpose:
Signature and encryption
Delete revoked or expired certificates (do not archive)
Include symmetric algorithms allowed by the subject
Archive subject's encryption private key
Authorize additional service accounts to access the private key (*)
Key Permissions...
Allow private key to be exported
Renew with the same key (*)
For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)
Do the following when the subject is enrolled and when the private key associated with this certificate is used:
Enroll subject without requiring any user input


Properties of New Template
Subject Name
Server
Issuance Requirements
Compatibility
General
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Group or user names:
Authenticated Users
Administrator
Domain Admins (AS21\Domain Admins)
Enterprise Admins (AS21\Enterprise Admins)
Add...
Remove


Select Users, Computers, Service Accounts, or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
as21.local
Locations...
Enter the object names to select (examples):
Everyone
Check Names
Advanced...
OK
Cancel


Group or user names:
Authenticated Users
Administrator
Domain Admins (AS21\Domain Admins)
Enterprise Admins (AS21\Enterprise Admins)
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Read
Write
Enroll
Autoenroll


SubCA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Tem
WS PK
User of Group1
RDC cert
Directory Email Replication
Manage
New
View
Refresh
Export List...
Help
Certificate Template to Issue
Certification Authority
Server Authenti
Client Authenti
Directory Servic
Encrypting File
<All>

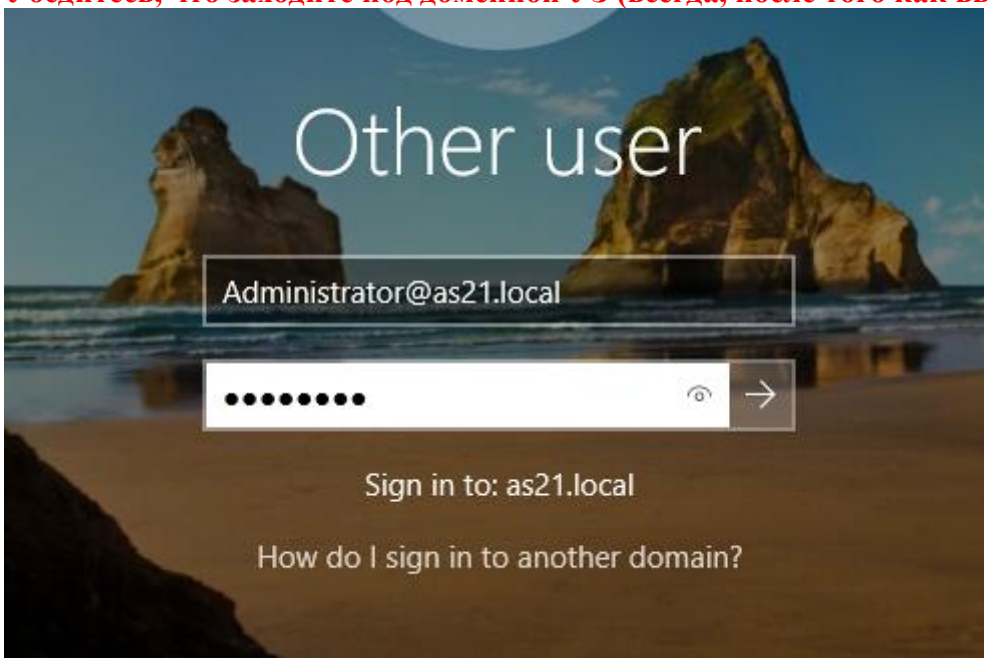


СОЗДАНИЕ RDS

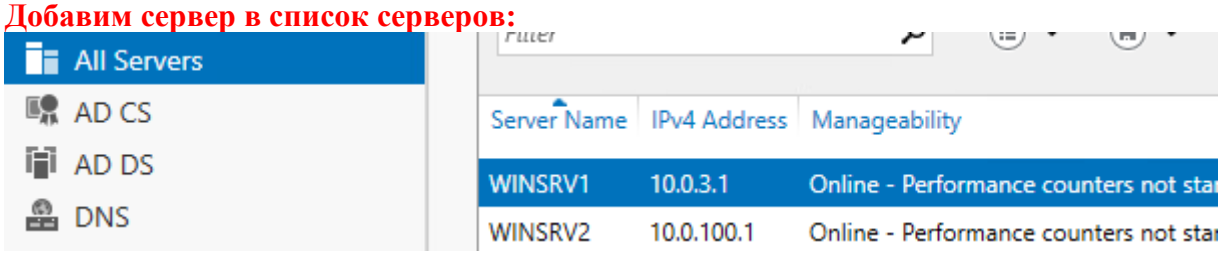
Установка ролей

Настройка сервера терминалов на WINSRV1
Разверните терминальный сервер, не устанавливайте и не настраивайте компоненты лицензирования.

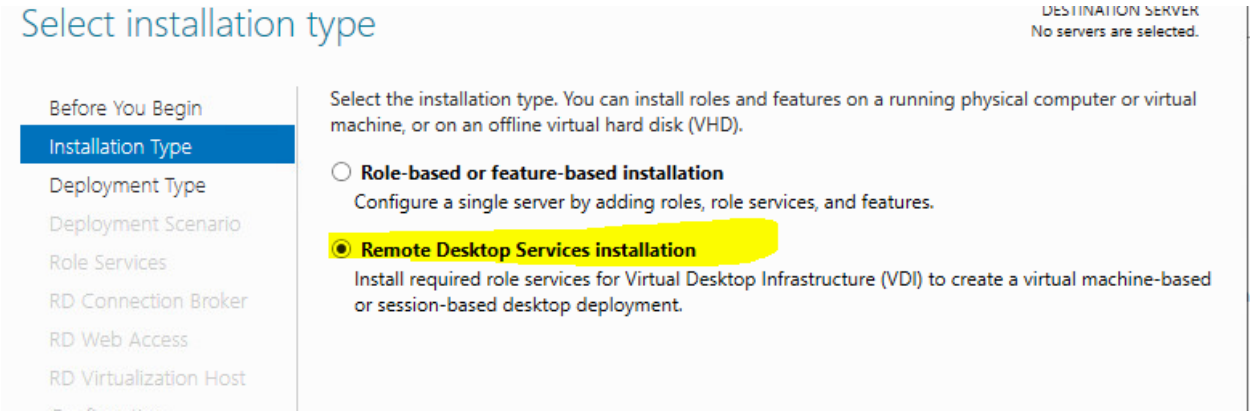
Убедитесь, что заходите под доменной УЗ (всегда, после того как введете в домен)

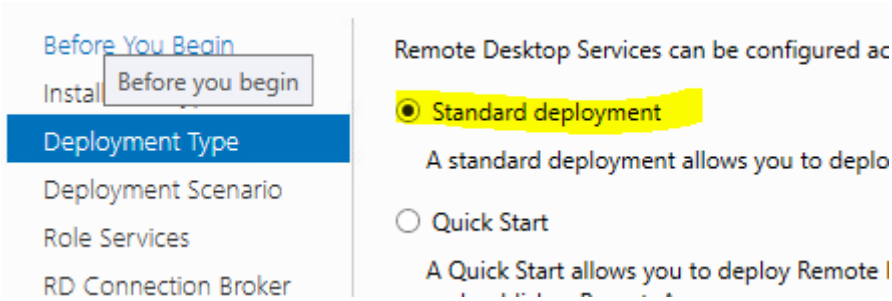


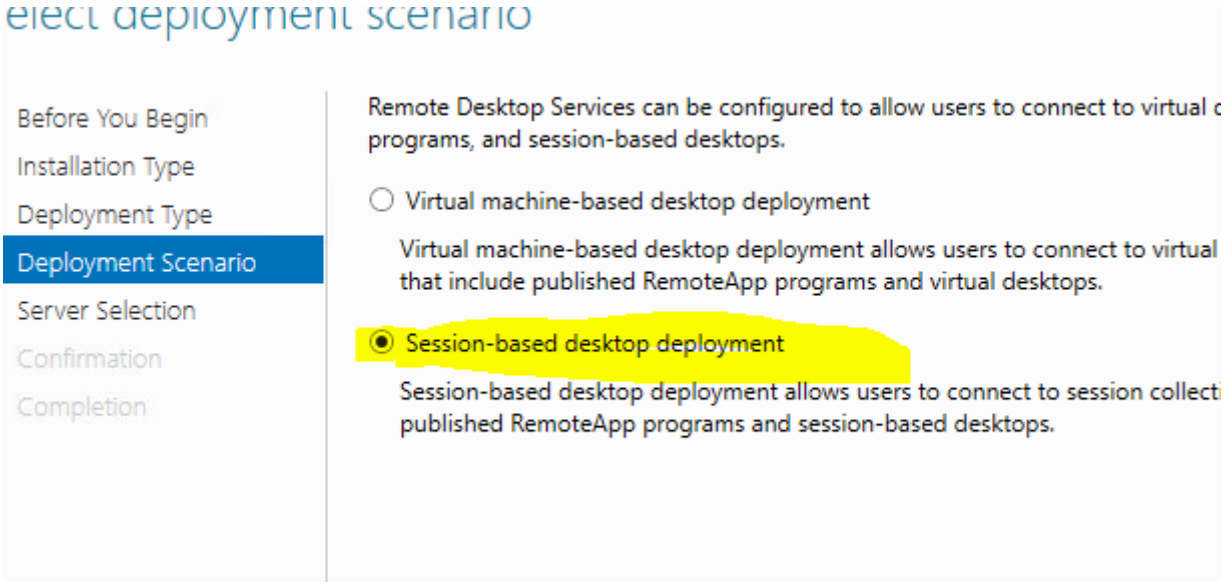
Добавим сервер в список серверов:



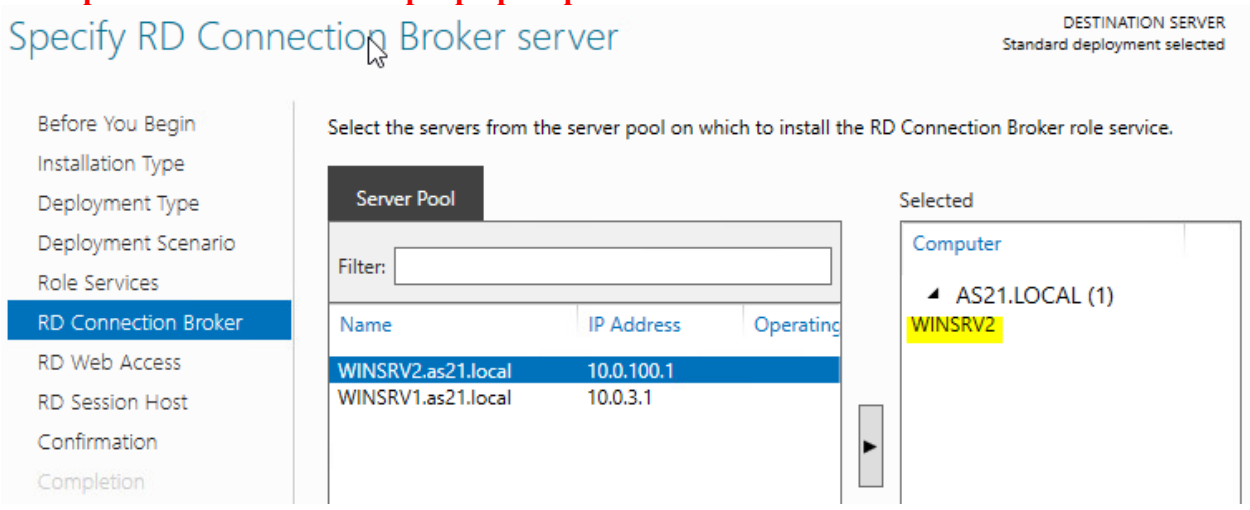
Конфигурируем в режиме Remote Desktop Services installation:



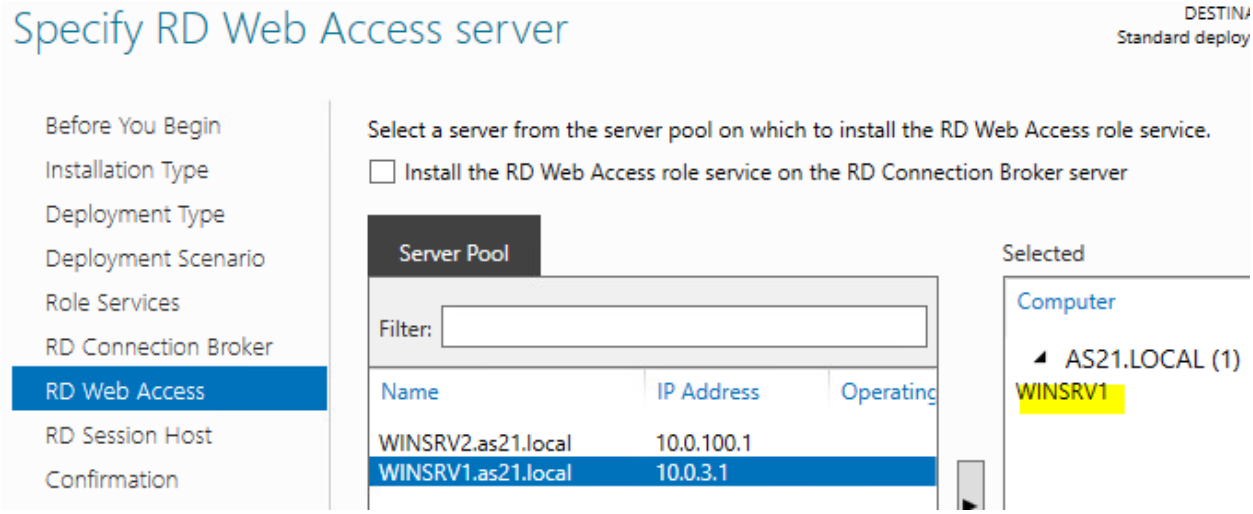




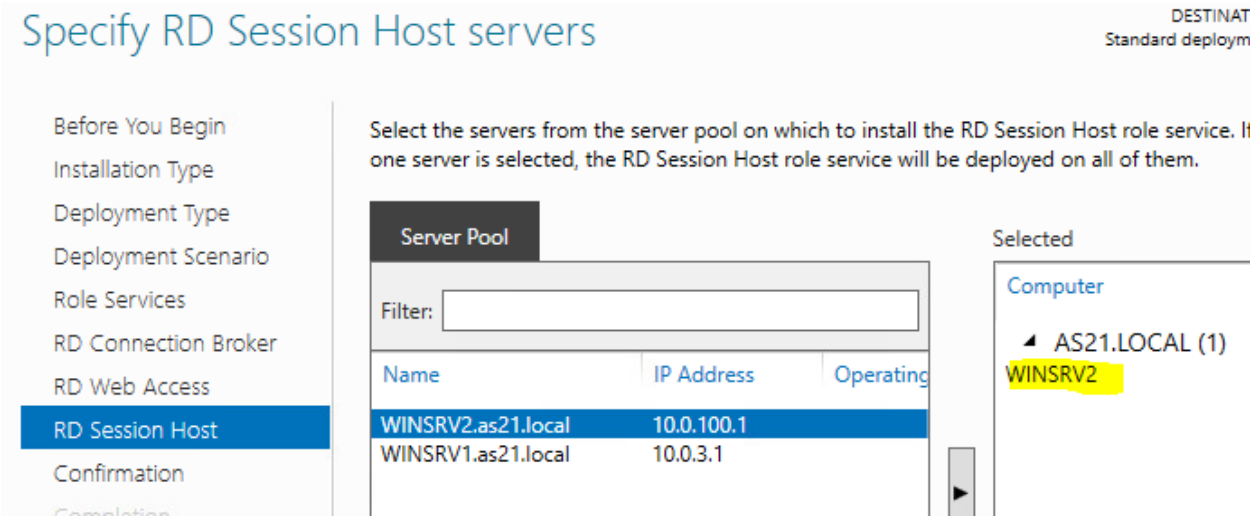
Выбираем WINSRV2 как сервер брокера



Выбираем WINSRV1 как сервер веб доступа



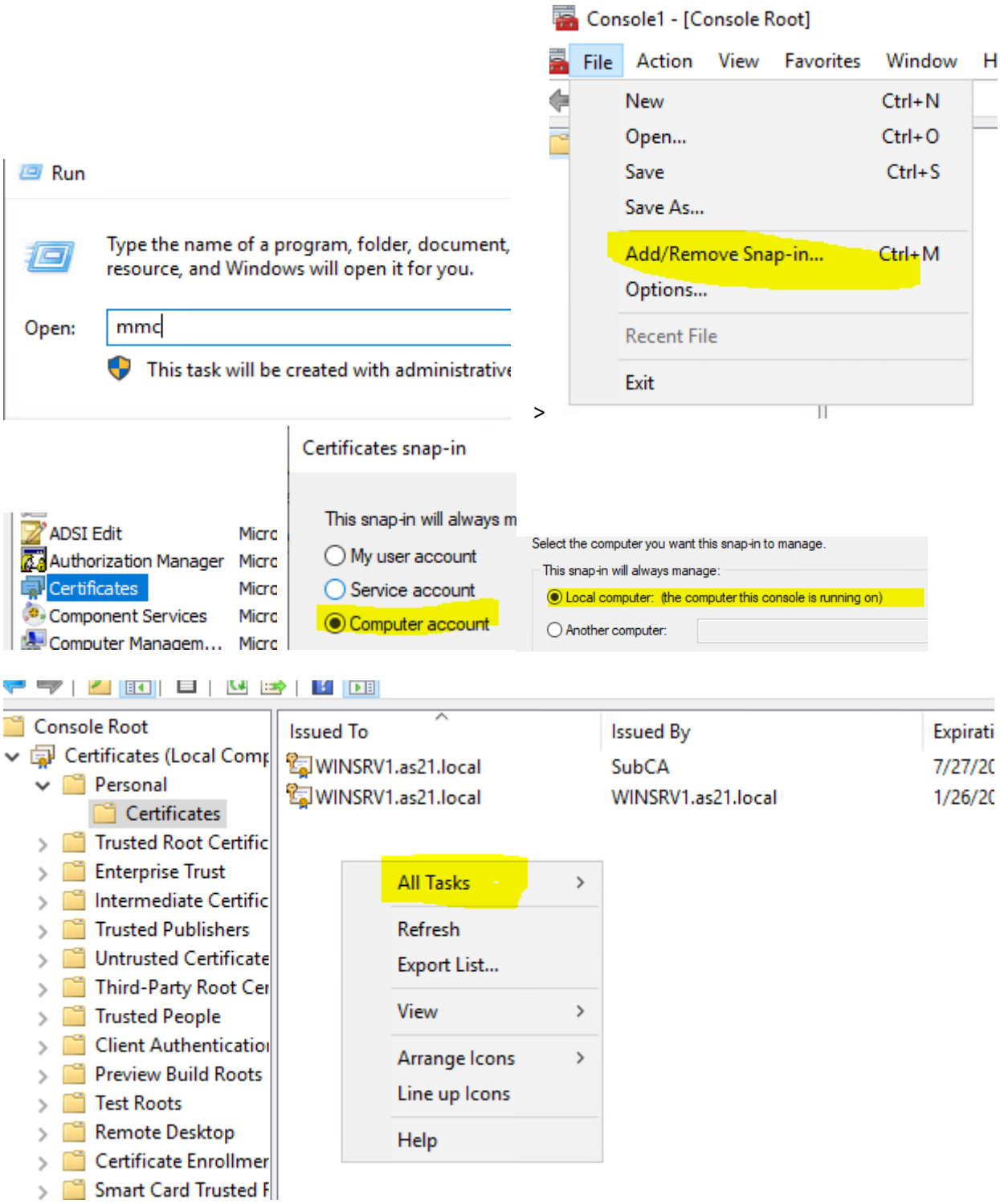
Выбираем WINSRV2 как сервер терминалов



Настройка web доступа по сертификатам

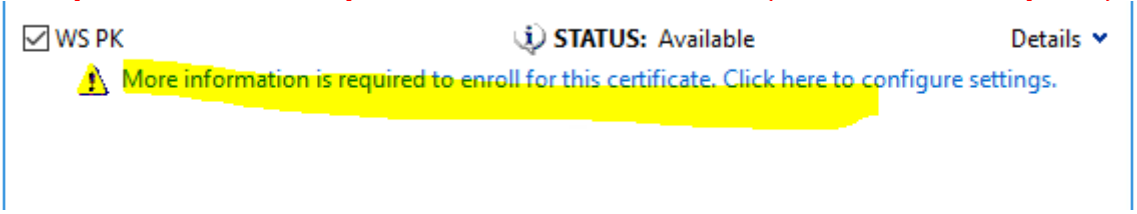
Сконфигурируйте web-доступ к службам терминалов сервера.

Запускаем mmc. Добавляем оснастку Certificates > Computer account > Local computer



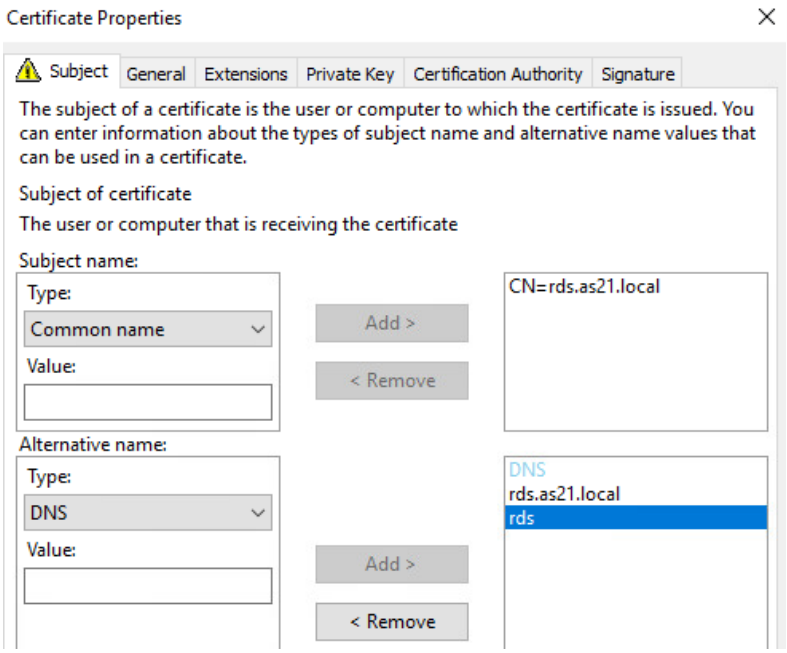
All Task > Request New Certificate

Выбираем шаблон, который был копией Web Server (подготовленный ранее)

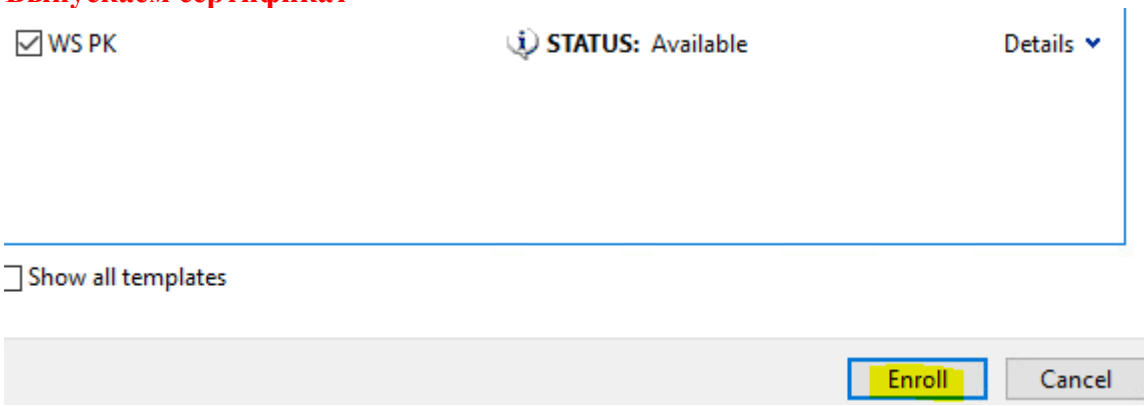


Сверху заводим Common Name – rds.as21.local

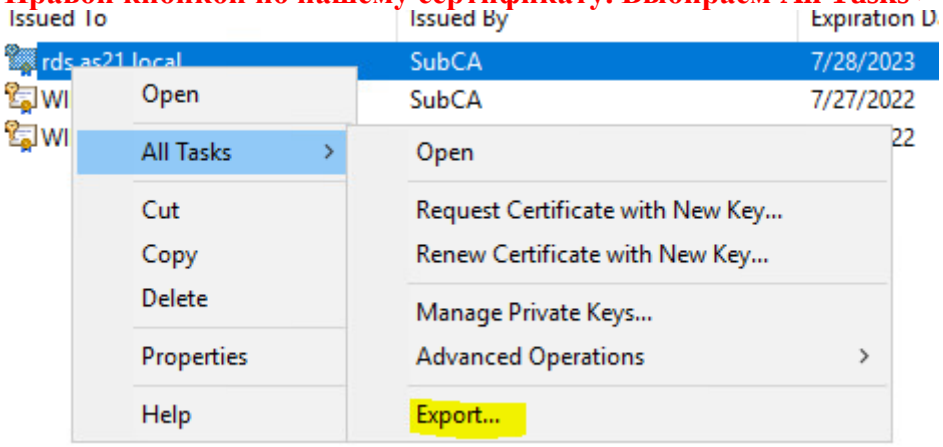
Внизу заводим DNS rds.as21.local и rds



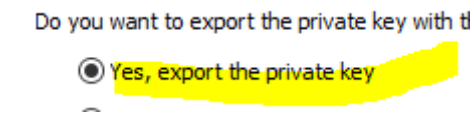
Выпускаем сертификат



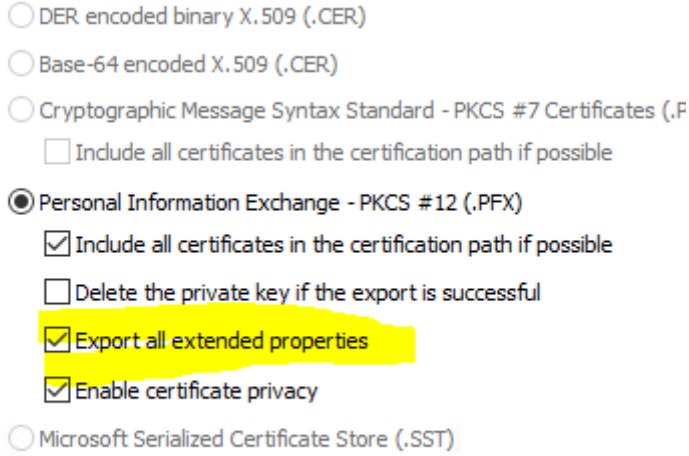
Правой кнопкой по нашему сертификату. Выбираем All Tasks > Export



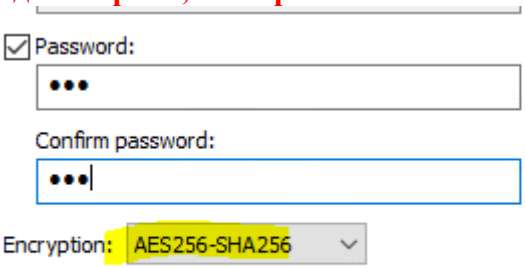
При экспорте выбираем разрешение экспорта закрытого ключа



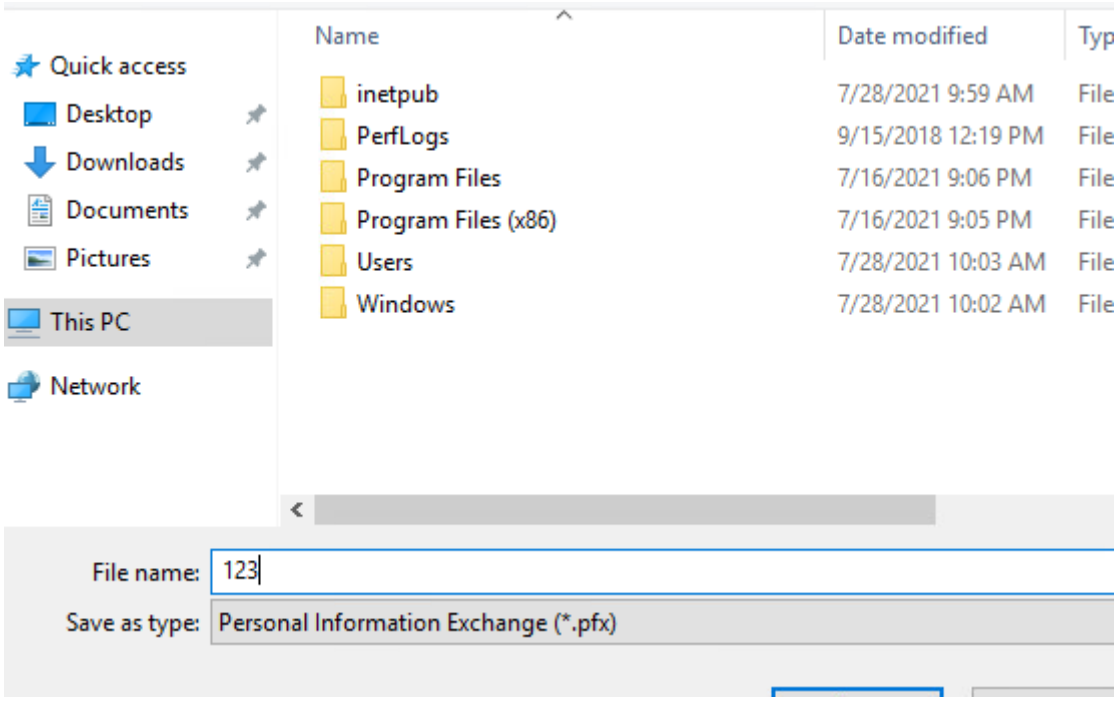
Выгружаем все параметры – Export all extended properties



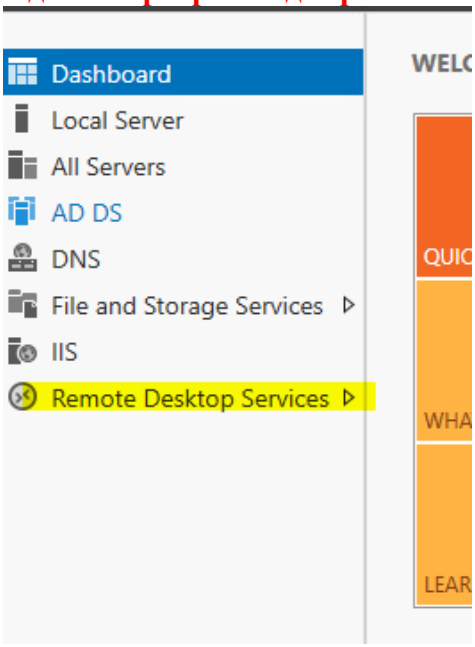
Вводим пароль, выбираем SHA256



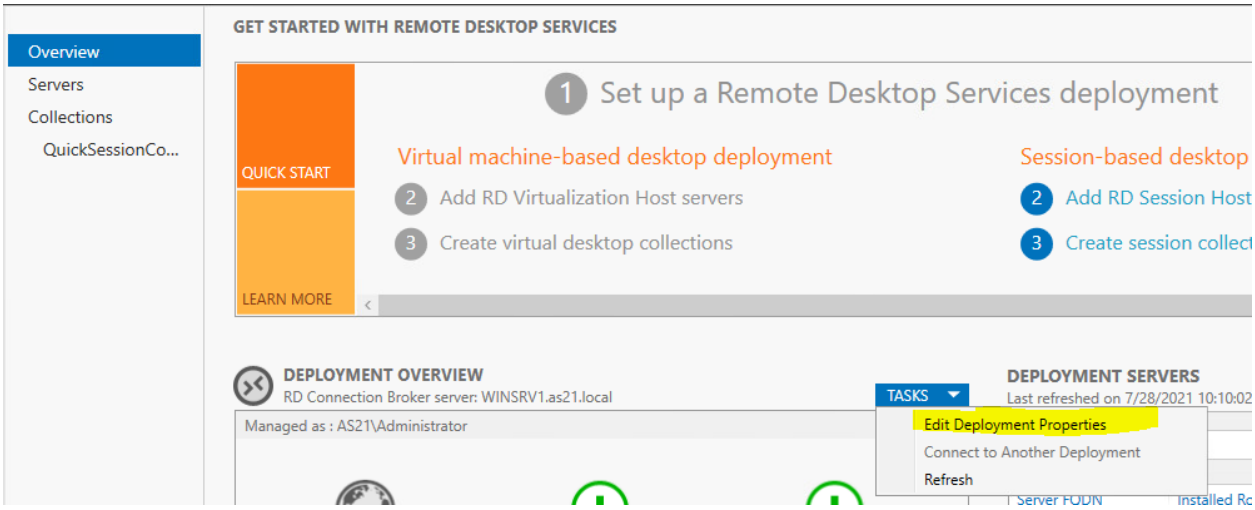
Сохраняем файл (не забываем куда)



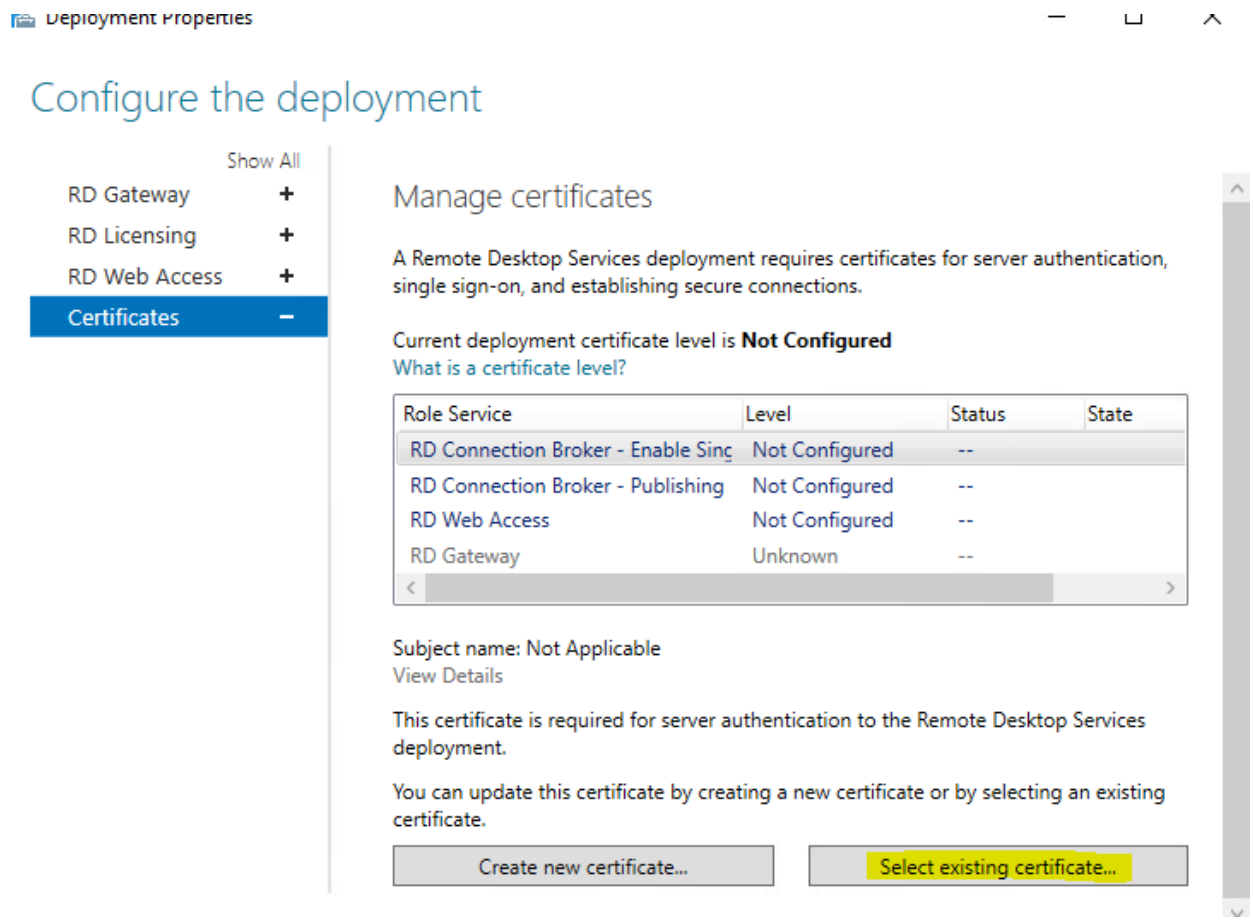
Идем в сервер менеджере в консоль RDS



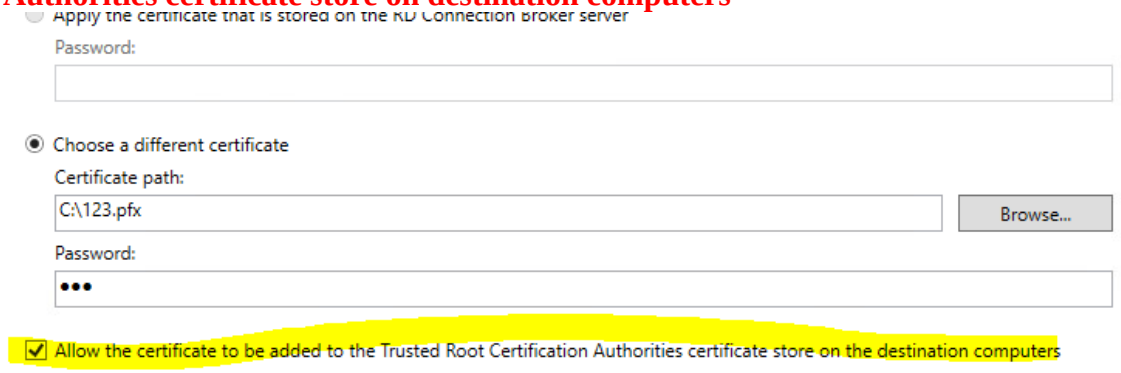
В разделе Overview > Deployment Overview выбираем Tasks > Edit Deployment Properties



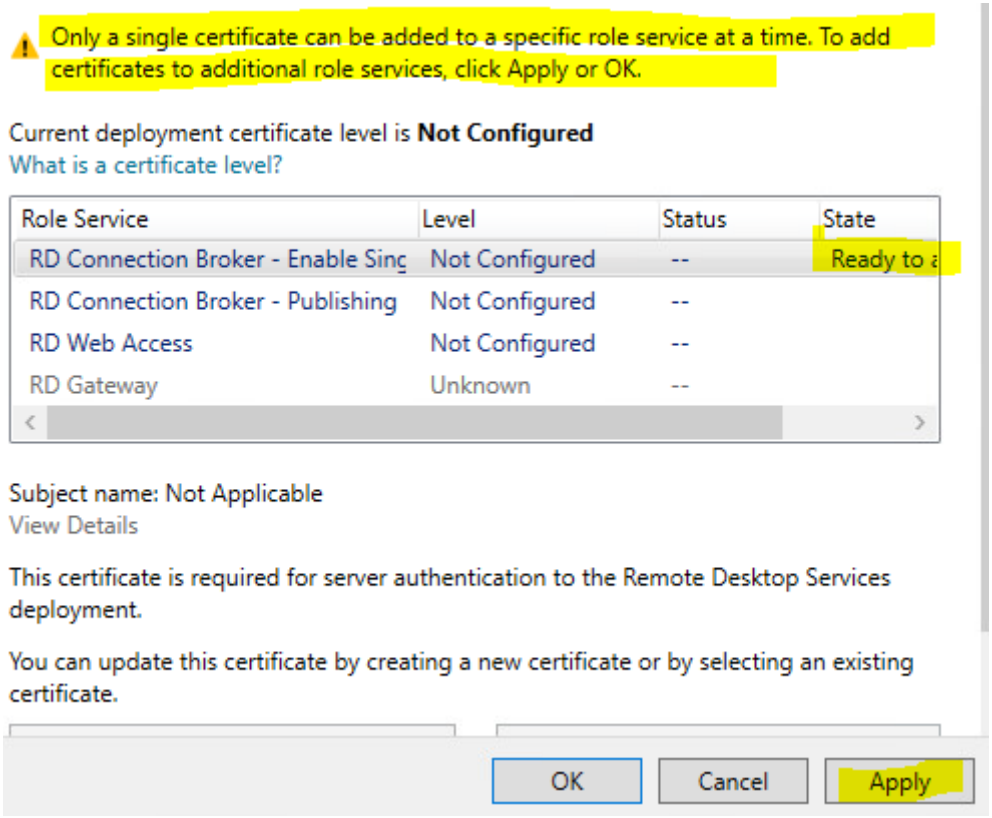
Переходим на вкладку Certificates и выбираем Select existing certificate



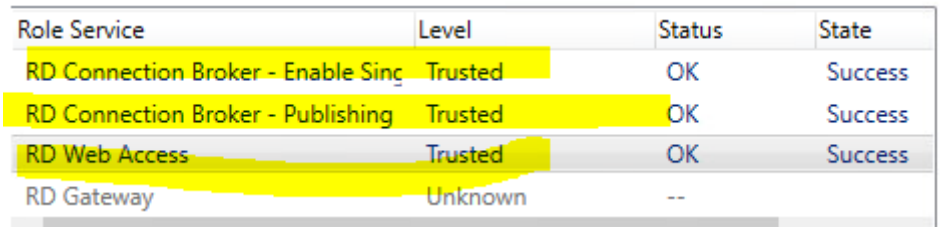
Указываем путь до предварительно сохраненного сертификата и пароль к нему. Устанавливаем Allow the certificate to be added to the Trusted Root Certification Authorities certificate store on destination computers



Должно получиться следующее. Нажимаем Apply



Повторяем для всех трех верхних ролей. Должно получиться следующее:

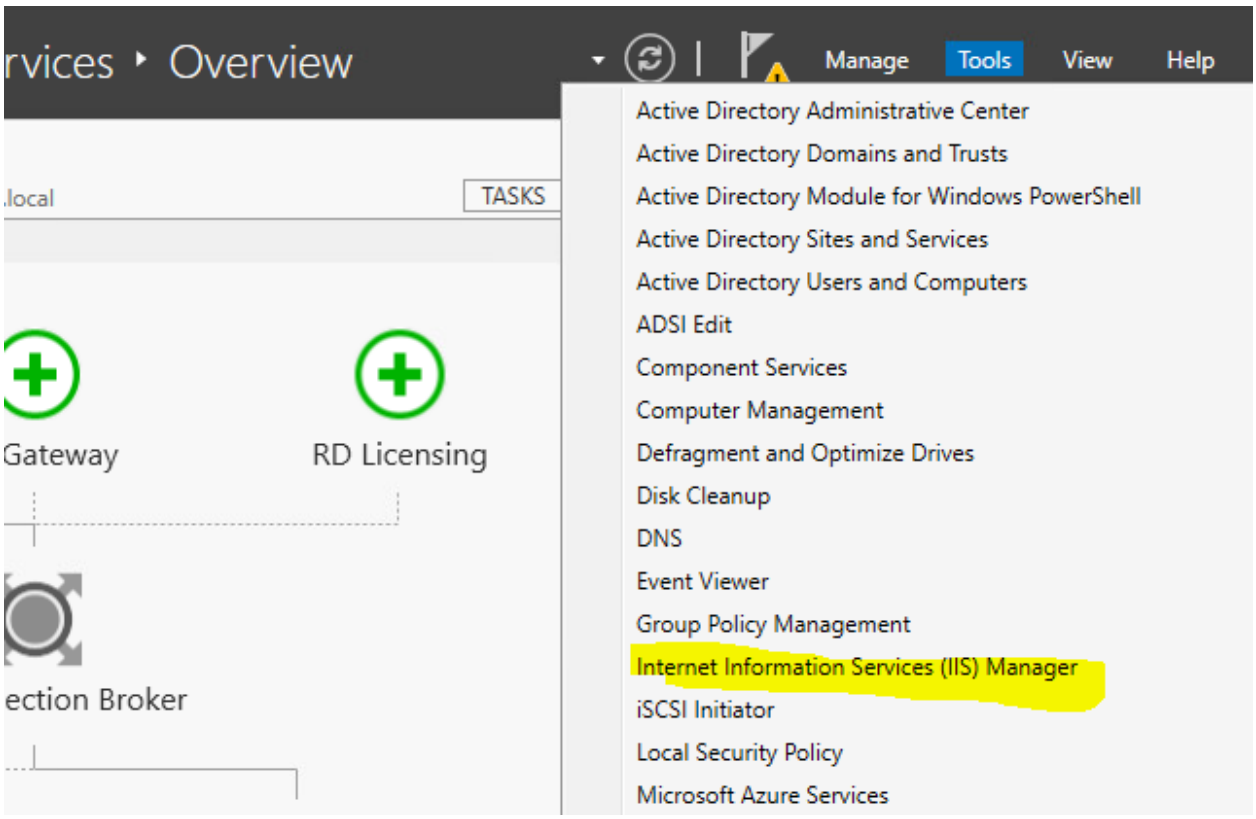


3. Web-интерфейс сервера должен быть доступен только по протоколу https по имени rds.AS21.local/RDweb.

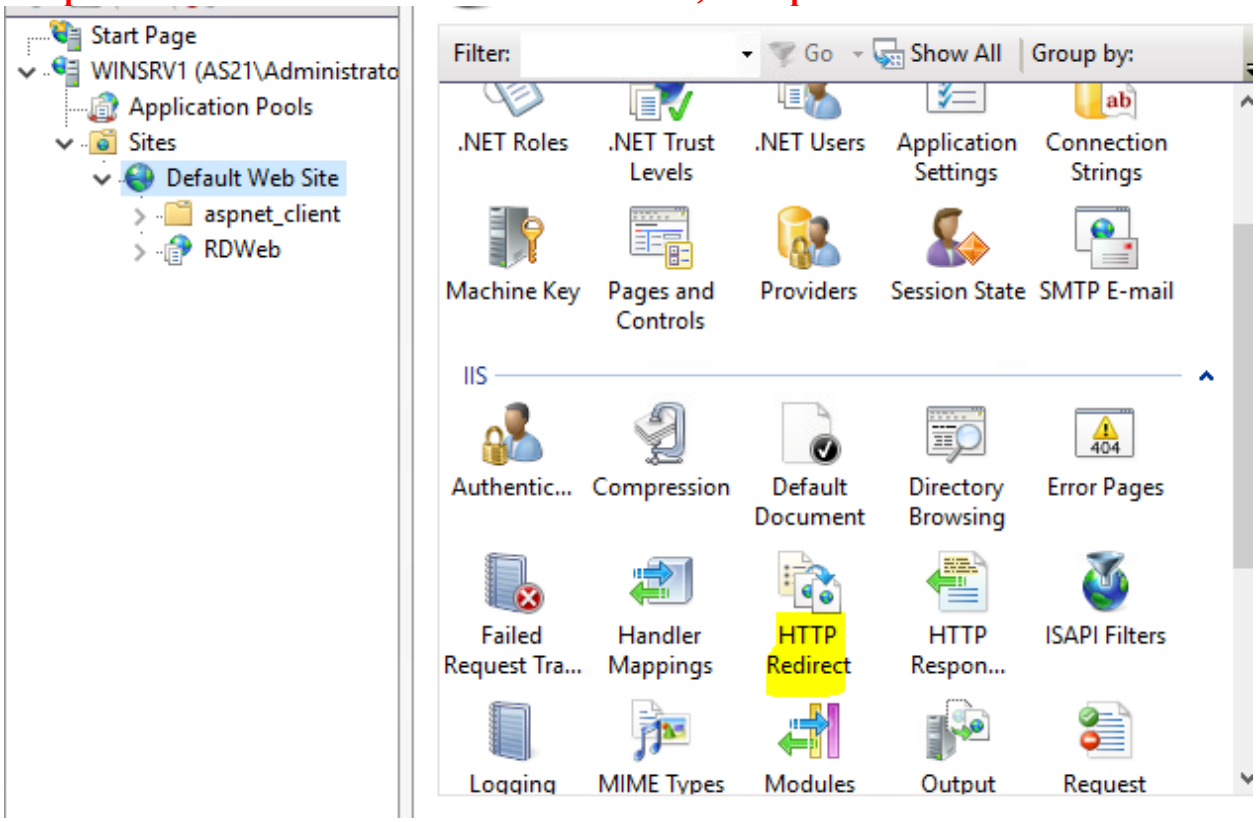
ВАЖНО!!! В данном случае у нас работать будет и так, но мы запланируем смену задания на «Web-интерфейс сервера должен быть доступен только по протоколу https по имени rds.AS21.local» поэтому нужно сделать переадресацию.

ВАЖНО!!! Убеждаемся, что в DNS есть A запись rds, которая ведет на WINSRV1. Идем в сервер менеджере в Tools > Internet Information Services (IIS) Manager

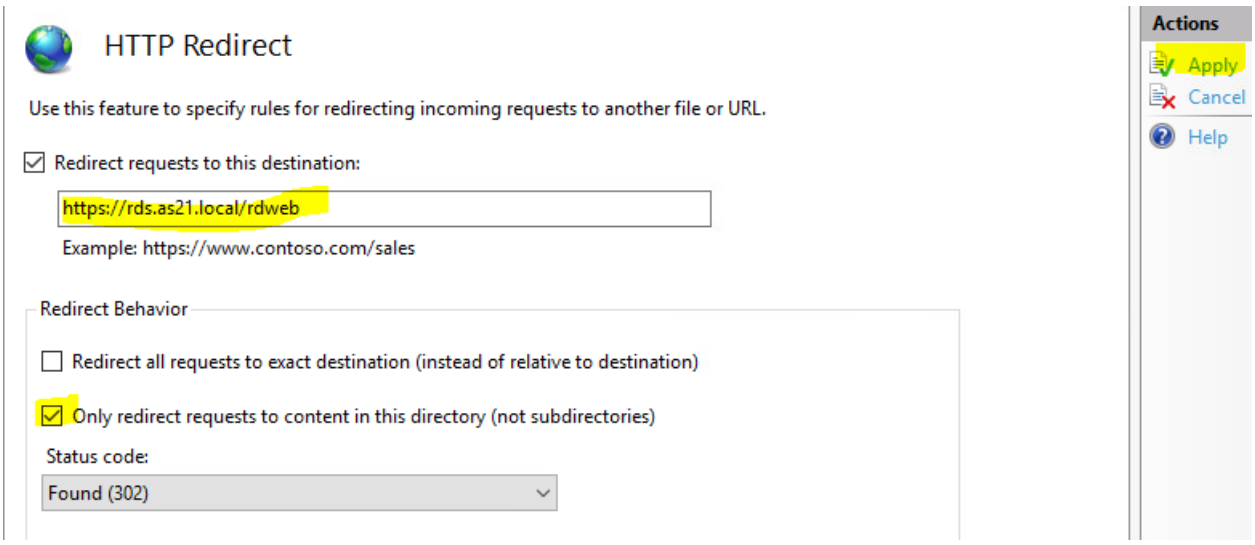
Настройка IIS RDS



Открываем WINSRV1 > Sites > Default Web Site, выбираем HTTP Redirect



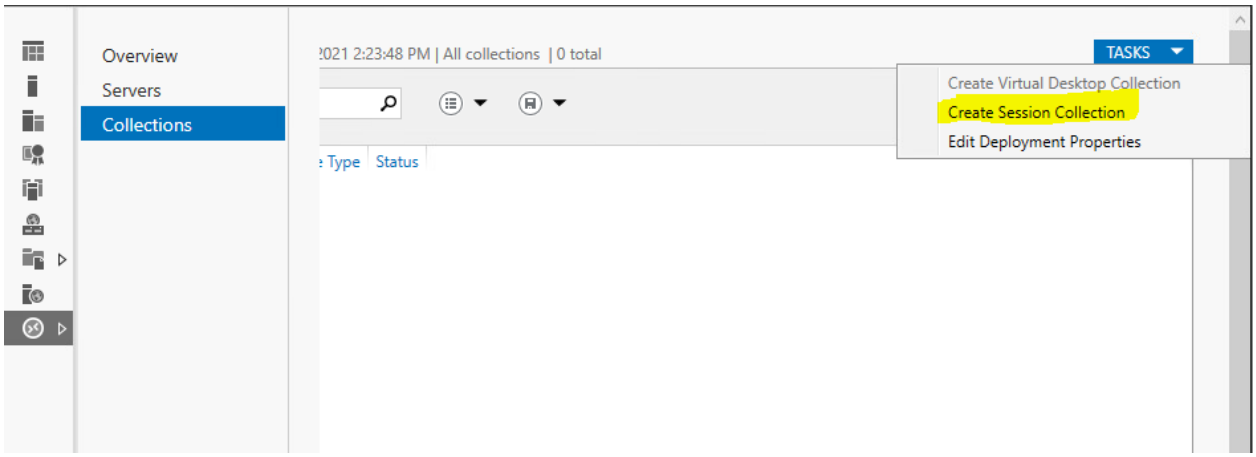
Прописываем пункт назначения переадресации https:\\rds.as21.local\RDWeb
Включаем Only redirect requests to content in this directory (not subdirectories).
Нажимаем Apply



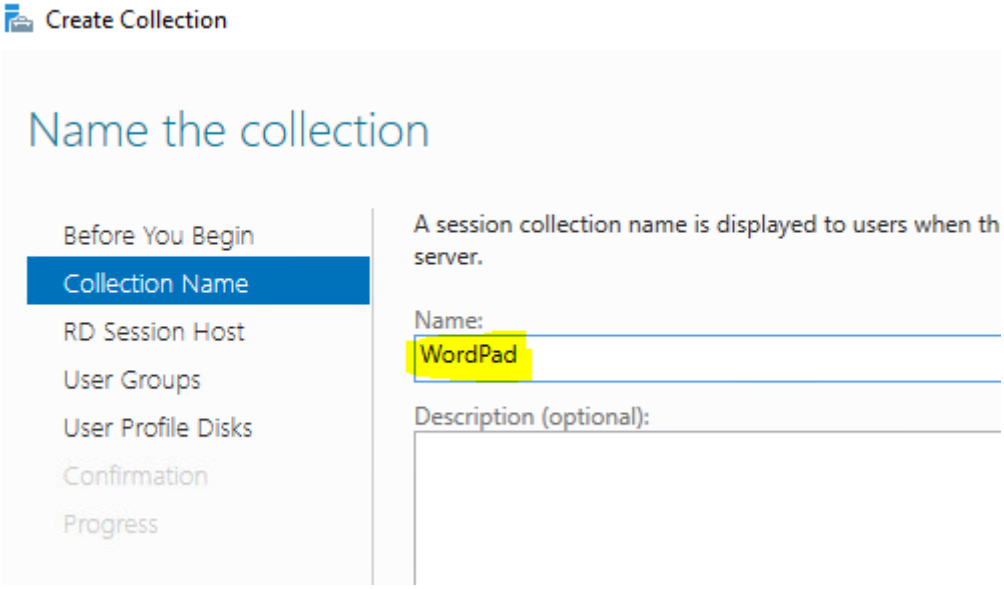
Публикация коллекции RDS

Опубликуйте программу WordPad на web-портале RemoteApp для всех членов группы Group2, при запуске этой программы у пользователей не должны появляться никакие ошибки и предупреждения системы безопасности.

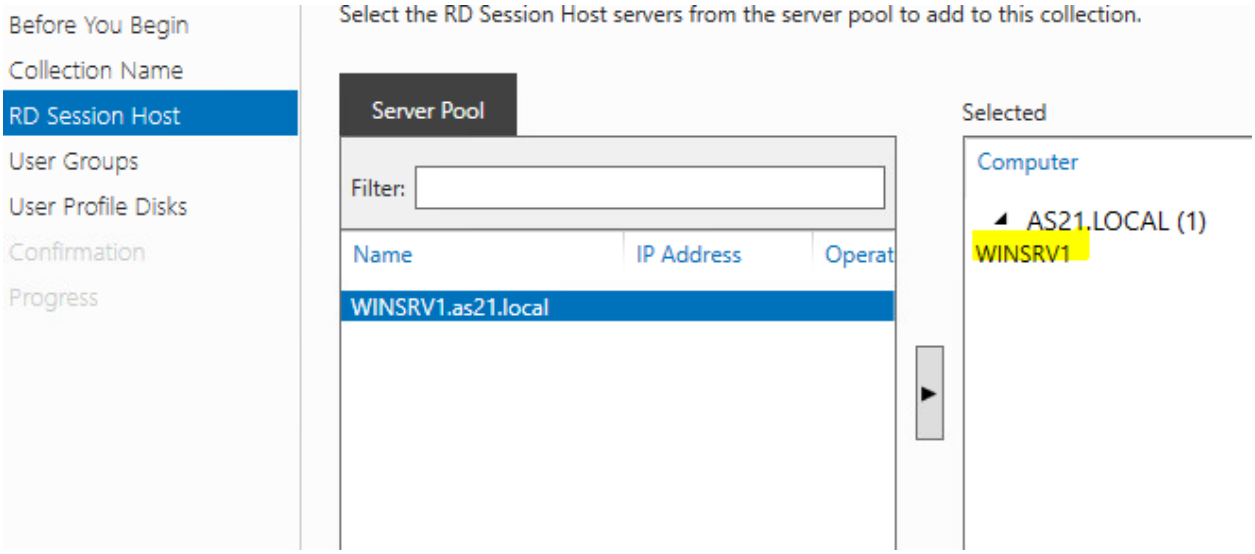
Создаем новую коллекцию



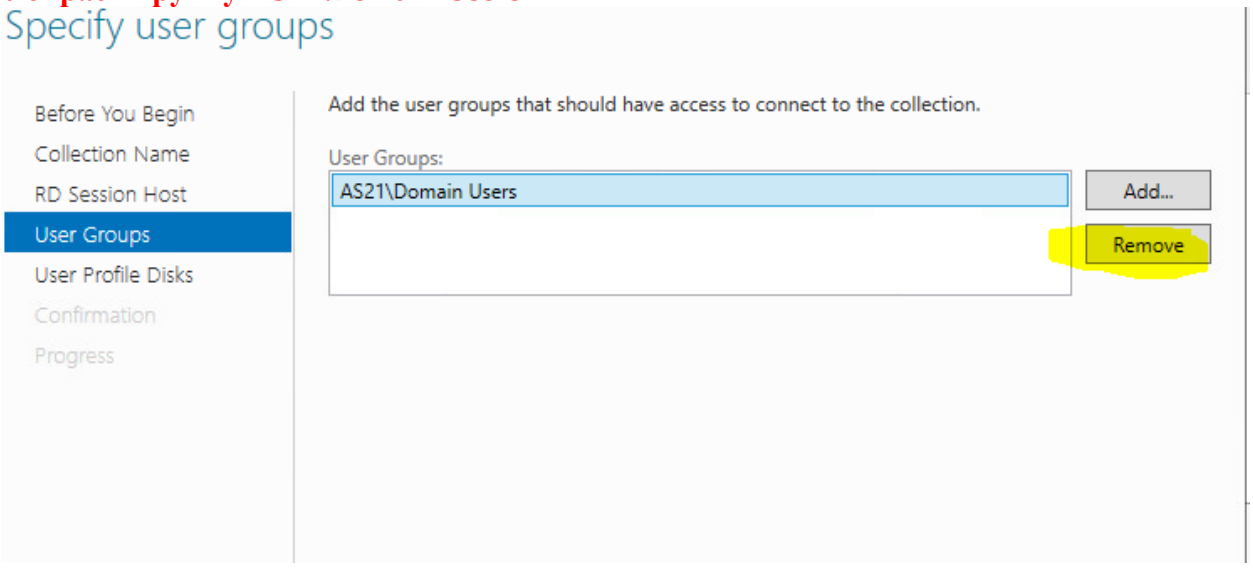
Вводим имя коллекции



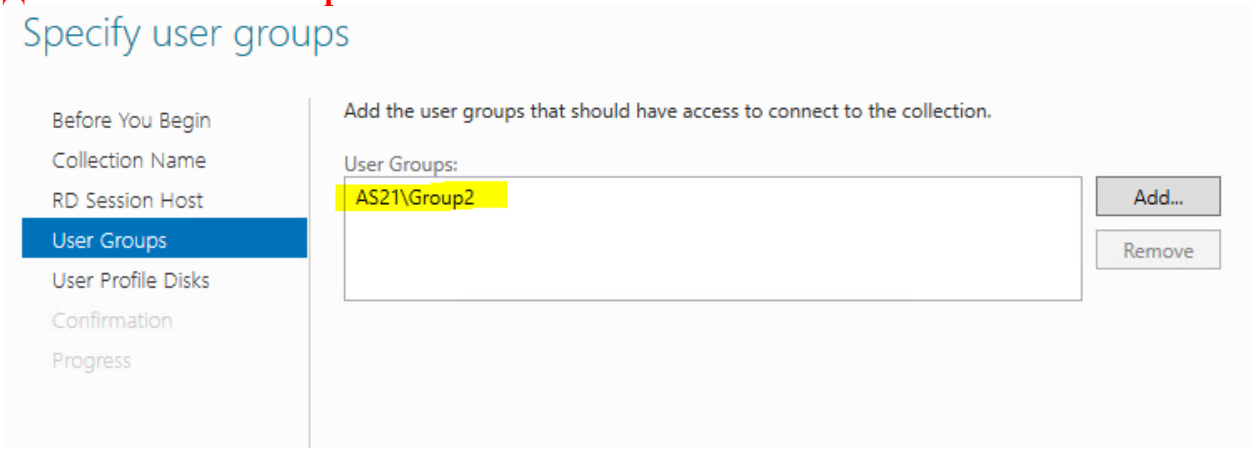
Добавляем сервер WINSRV1 как хоста коллекции



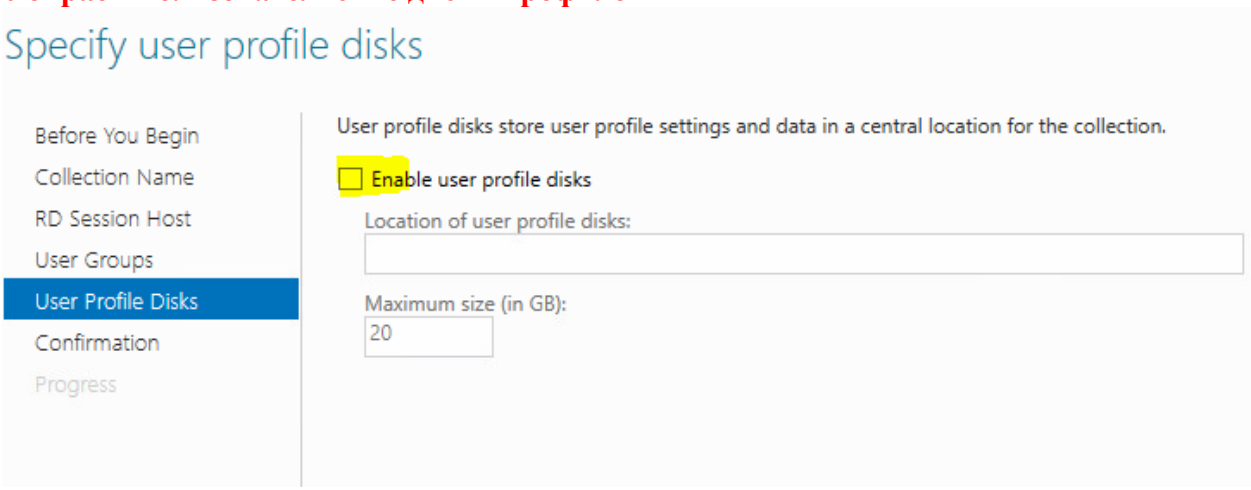
Убираем группу AS21\Domain Users



Добавляем AS21\Group2

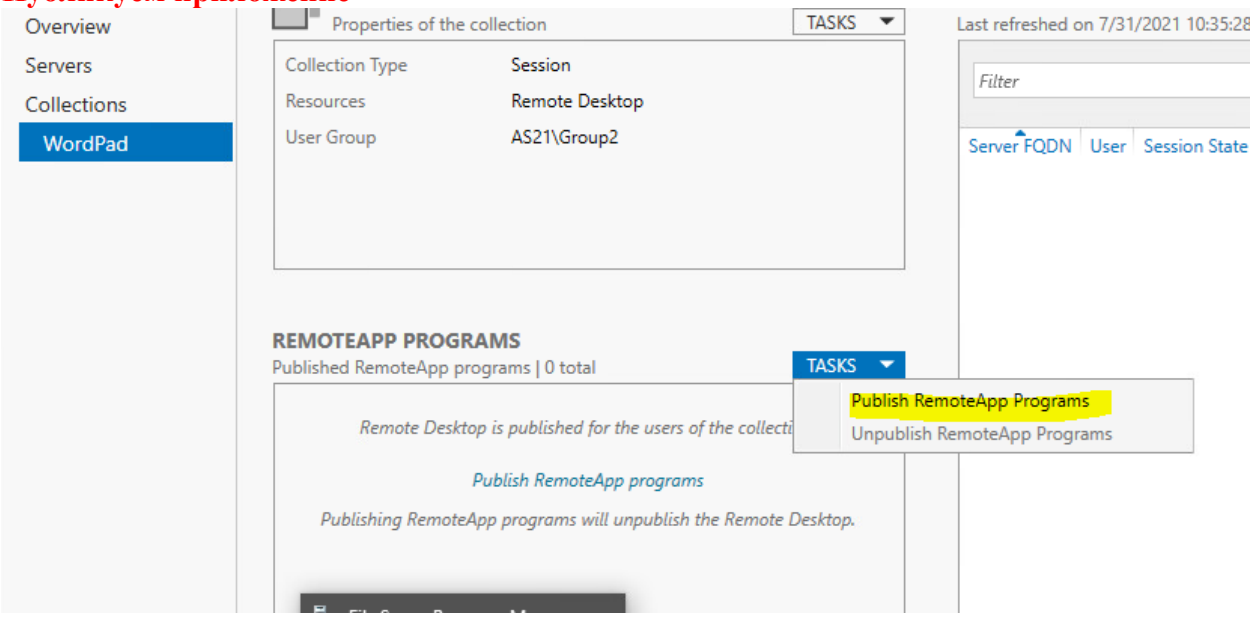


Убираем пользовательские диски профилей

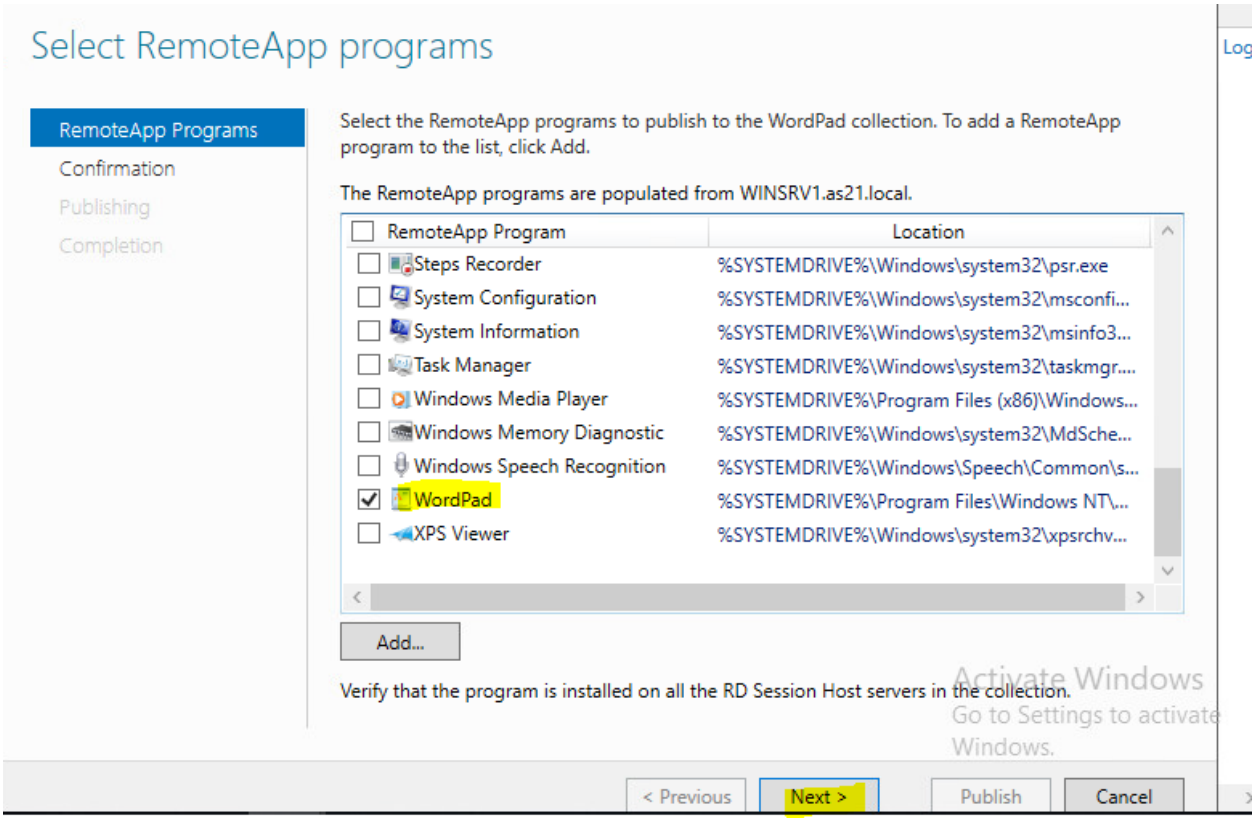


Публикация приложения RDS

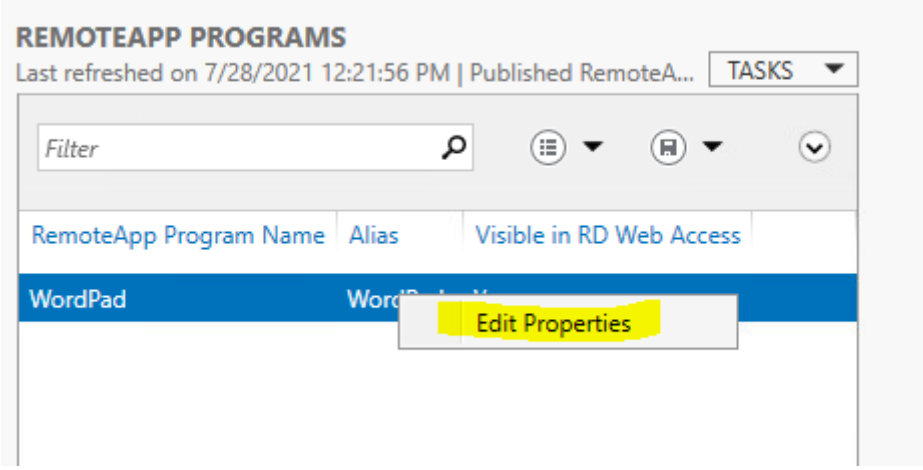
Публикуем приложение



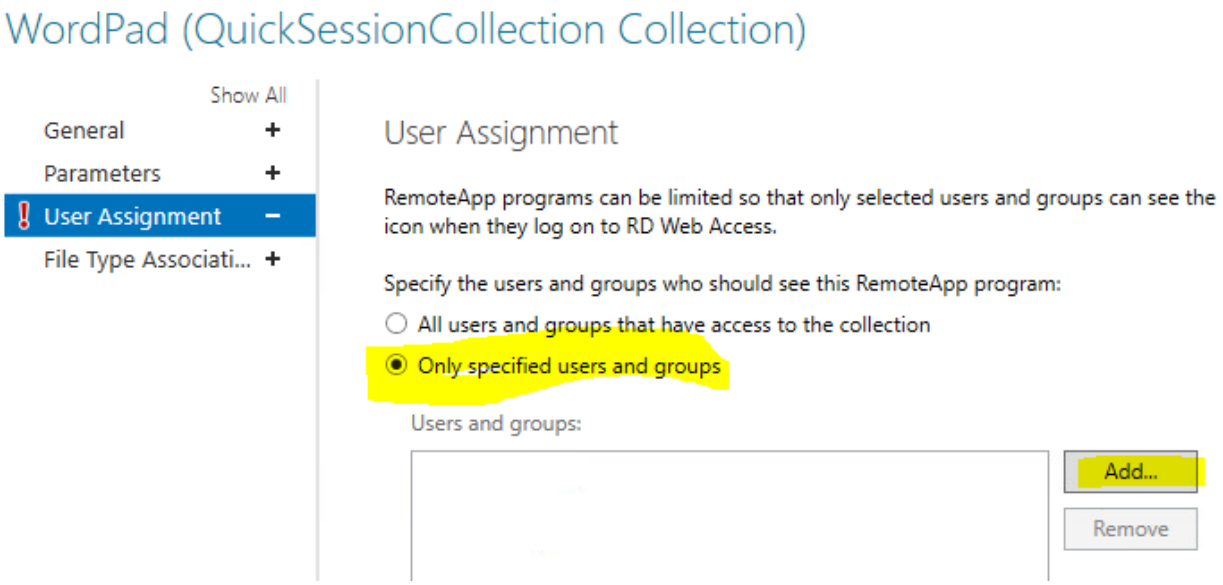
Выбираем их списка WordPad и публикуем его на RDS



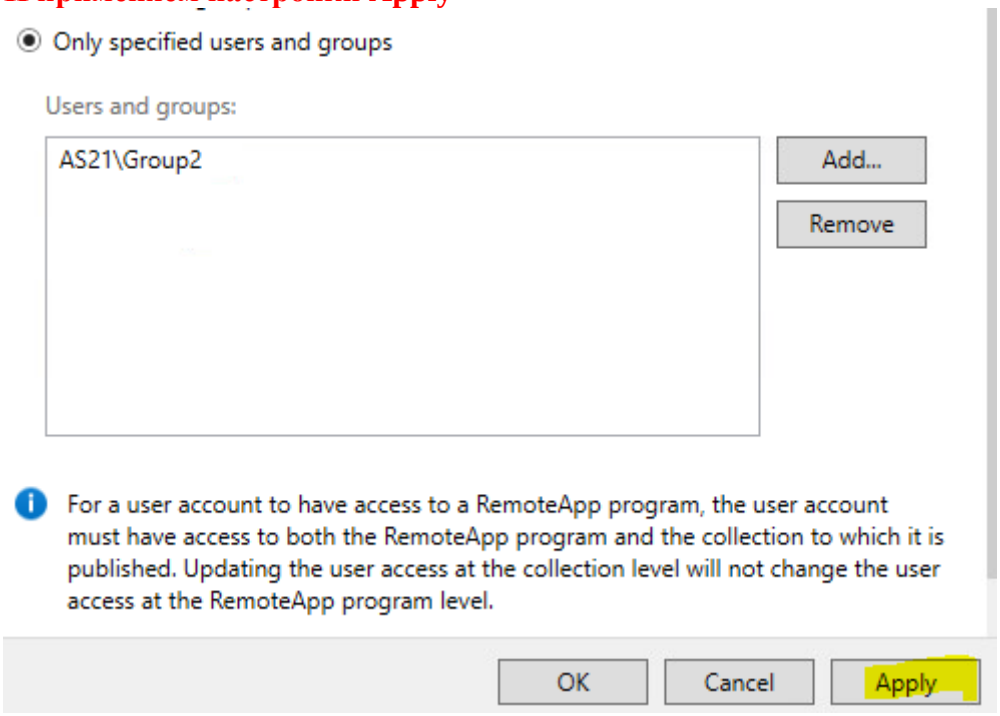
Заходим в свойство WordPad > Edit Properties



В разделе User Assignment выбираем Only specified users and groups и, после нажатия кнопки Add, добавляем Group2



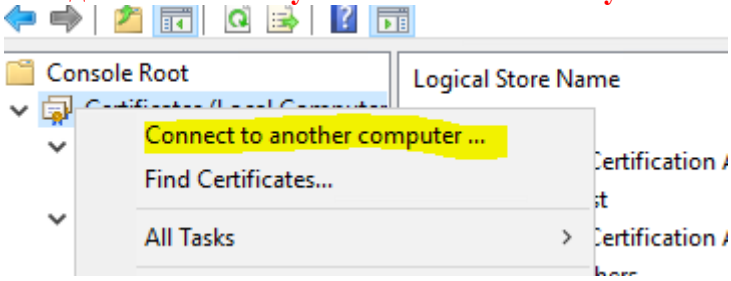
И применяем настройки Apply

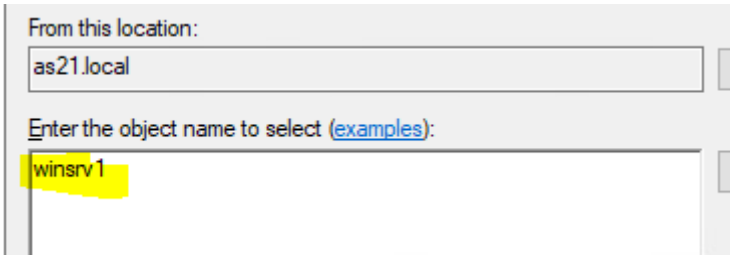


Добавление сертификата в доверенные

Убираем предупреждение при подключении

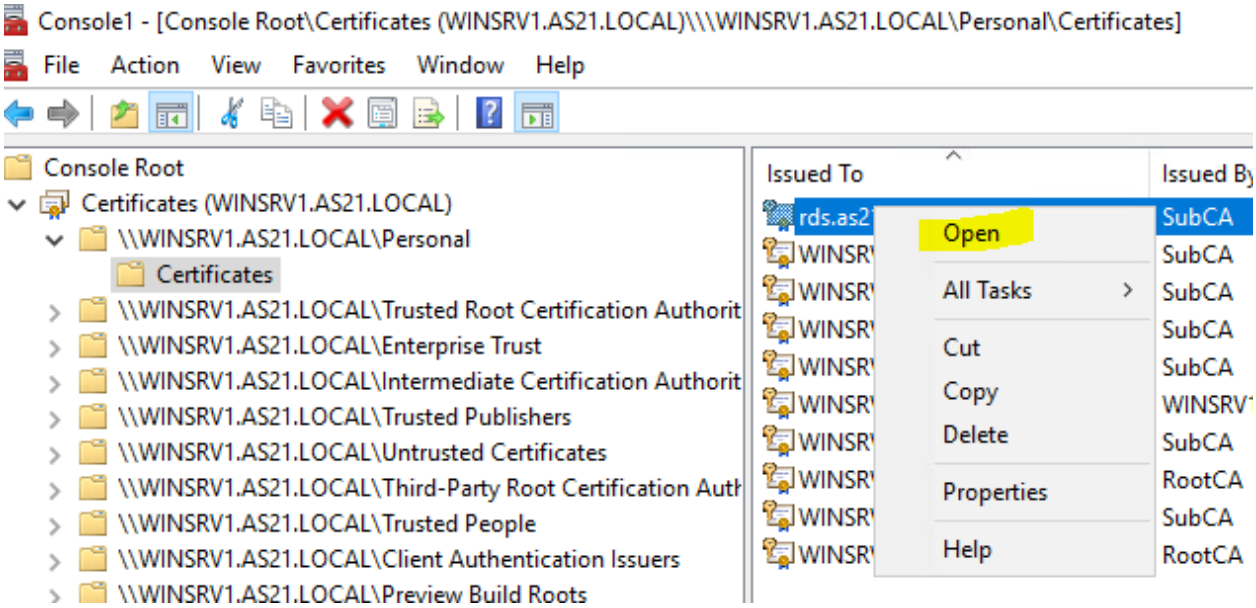
Заходим на DC. Запускаем MMC оснастку Certificates. Подключаем её к WINSRV1



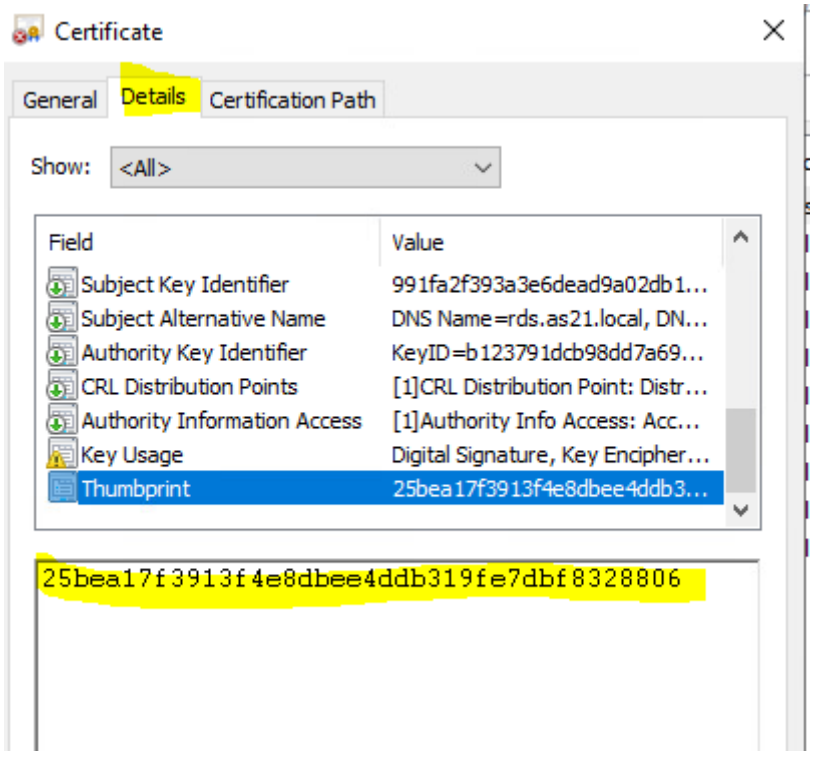


Находим выпущенный для RDS сертификат rds.as21.local

Открываем его

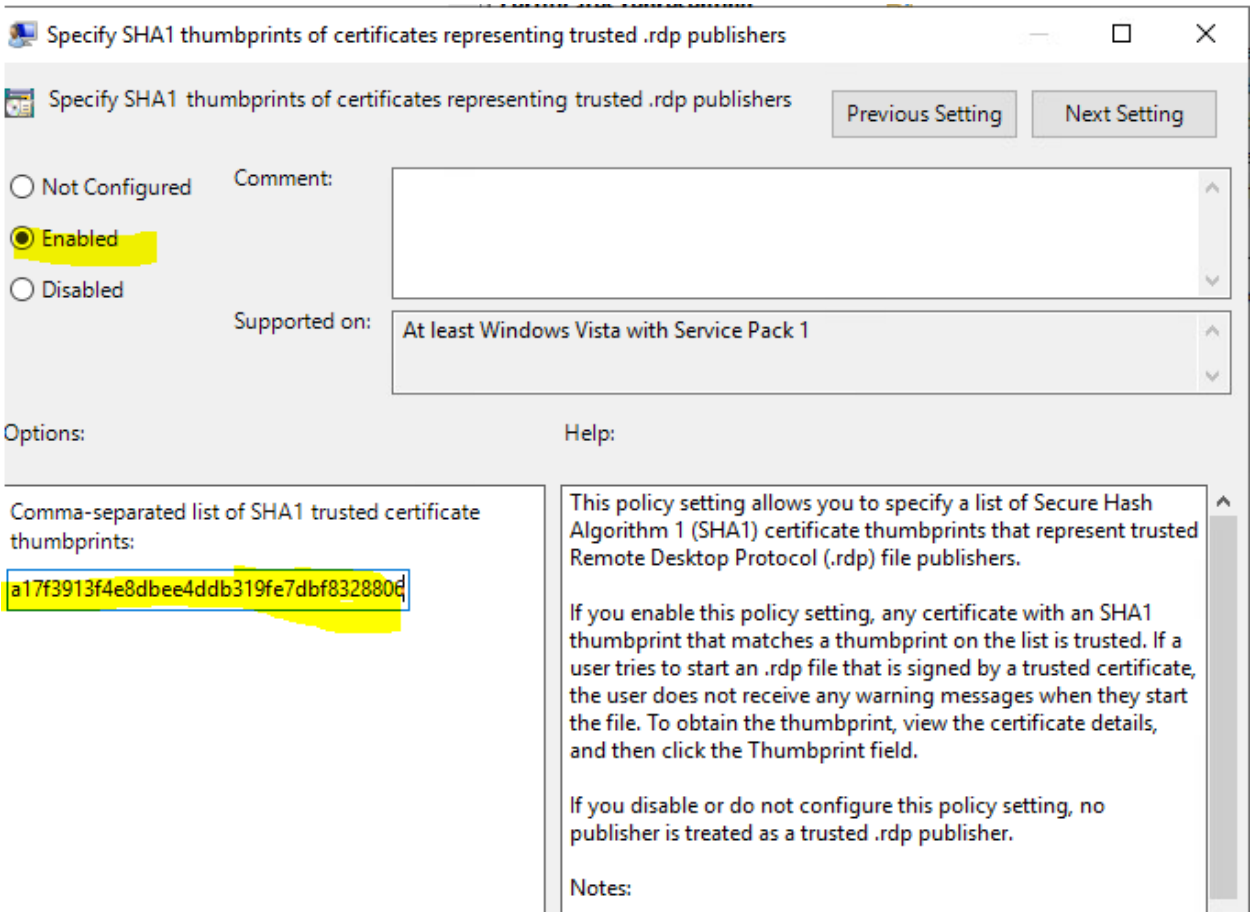


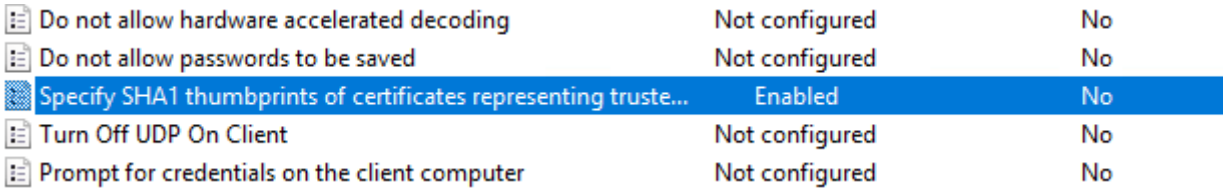
Переходим в раздел Details. Выбираем Thumbprint, где мы видим отпечаток нашего сертификата. Копируем его в буфер



Создаем GPO на домен: Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Connection Client > Specify SHA1 thumbprints of certificates trusted .rdp publishers -> Enabled

В качестве настройки вставляется отпечаток





Убираем предупреждение при открытии файла

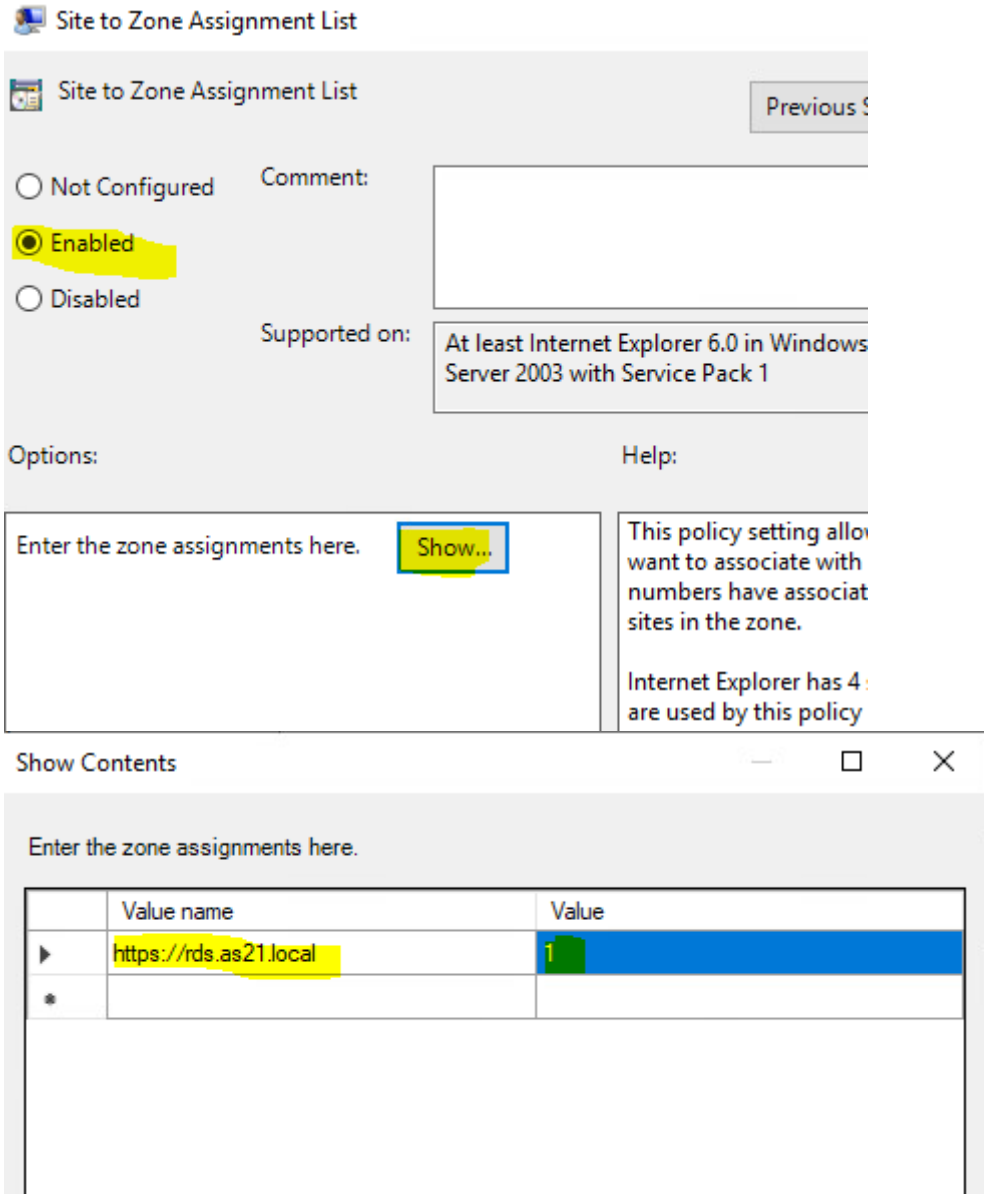
Идем в GPO, созданную на домен

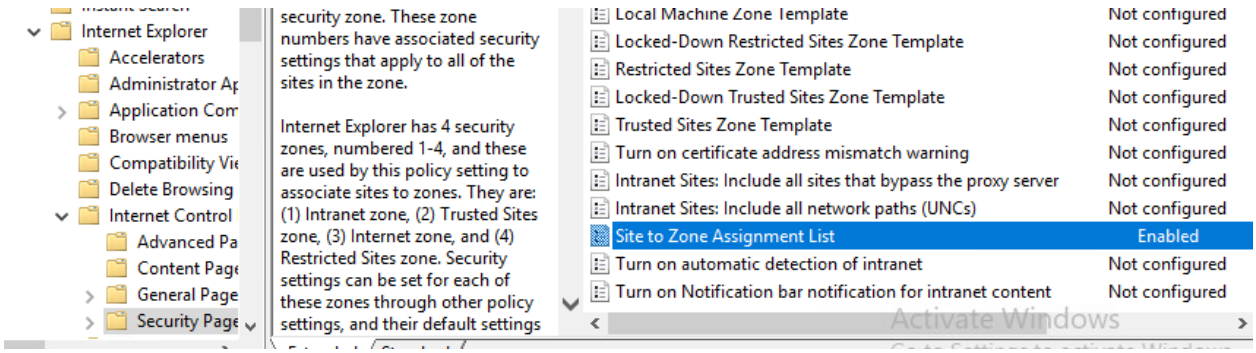
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Site to Zone Assignment List -> Enabled

Нажимаем Show

В Value Name вводим адрес нашего RDS – https://rds.as21.local

В Value пишем 1

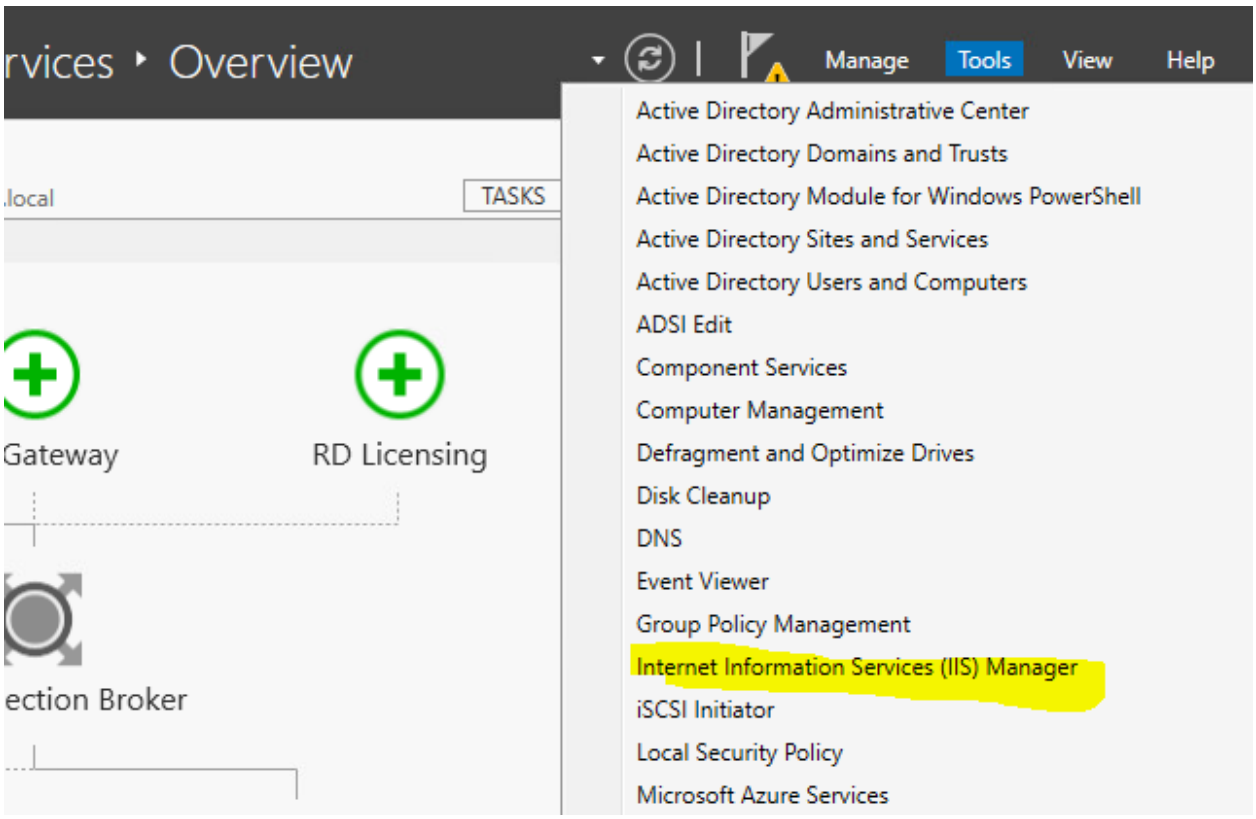




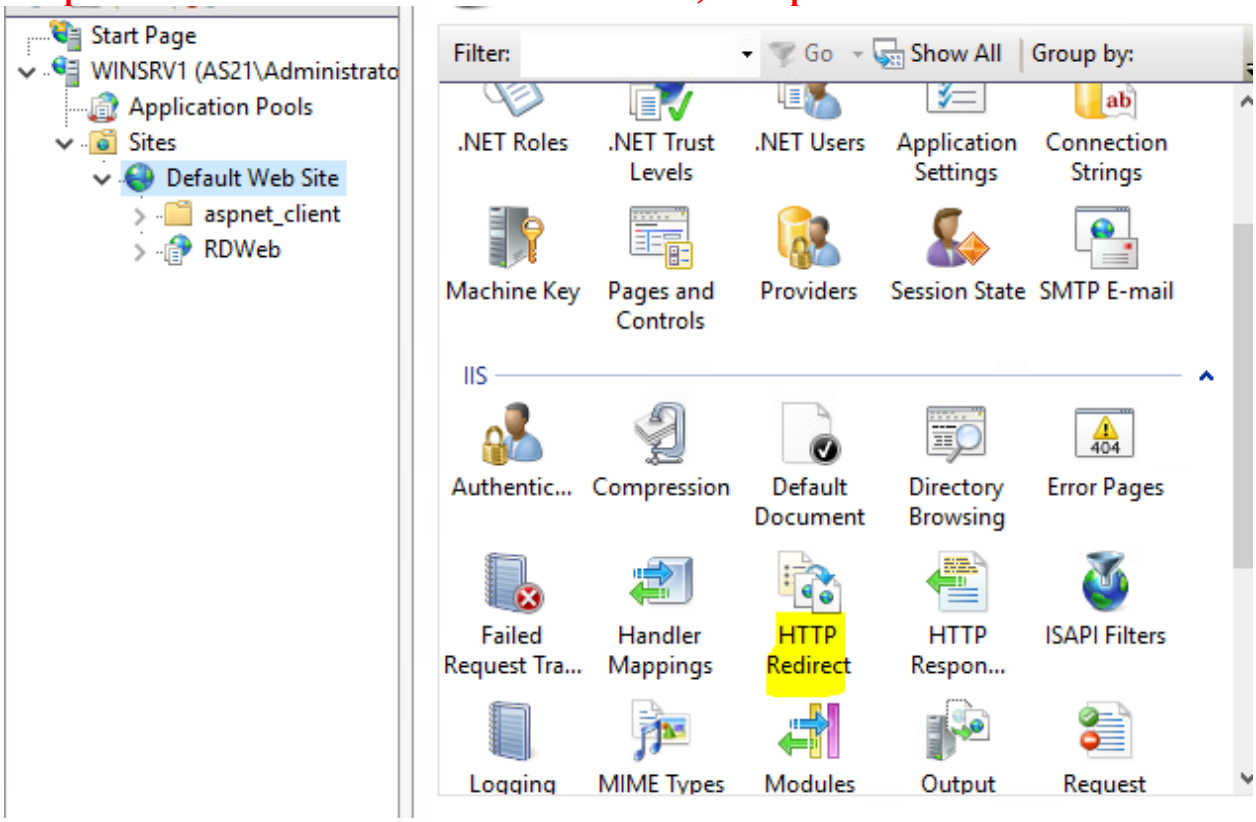
ПУБЛИКАЦИЯ CRL НА ДОМАШНЕЙ СТРАНИЦЕ

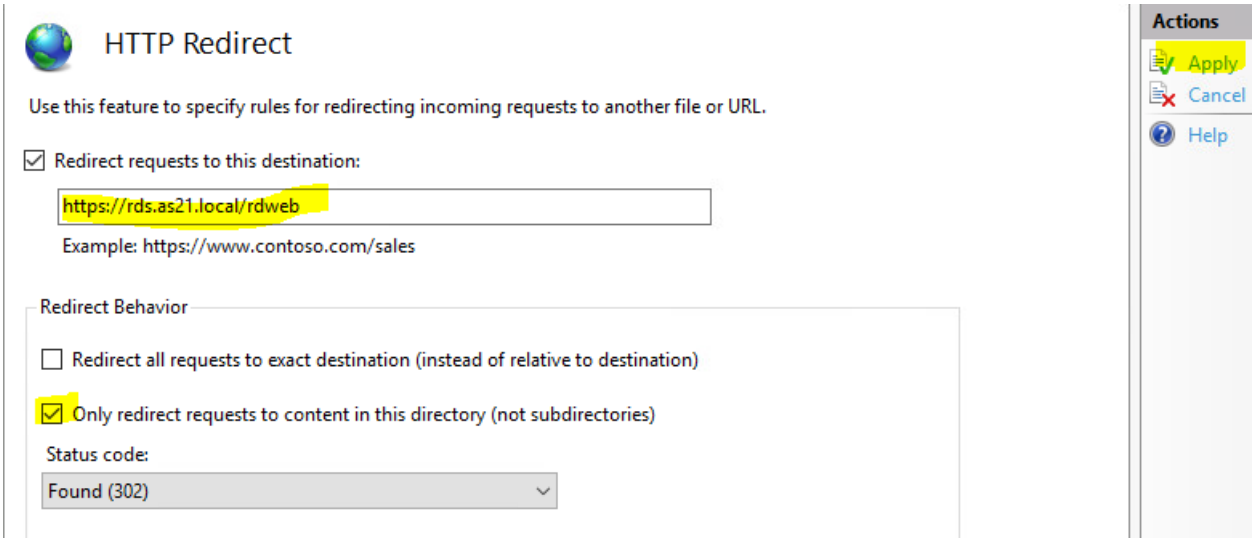
В браузере IE Explorer должна быть настроена стартовая страница с актуальным списком выданных и отозванных сертификатов SubCA, доступным для скачивания;

Проверяем, что настройки IIS в разделе HTTP Redirect верны

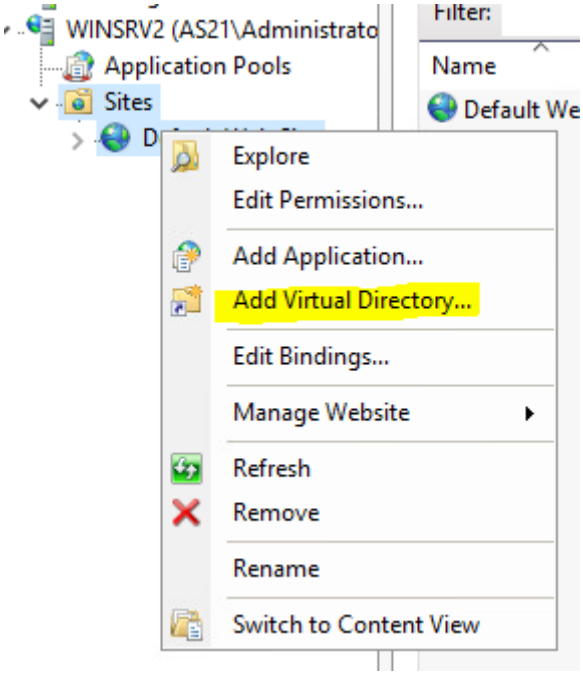


Открываем WINSRV1 > Sites > Default Web Site, выбираем HTTP Redirect

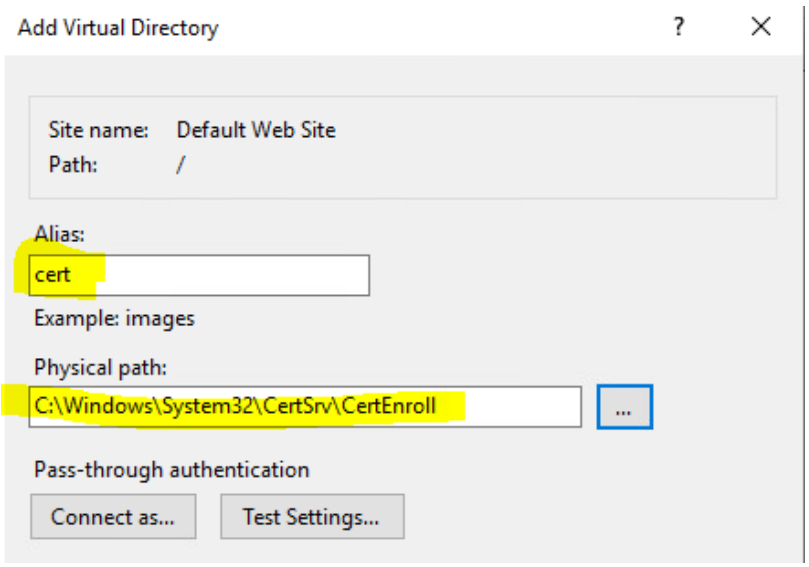




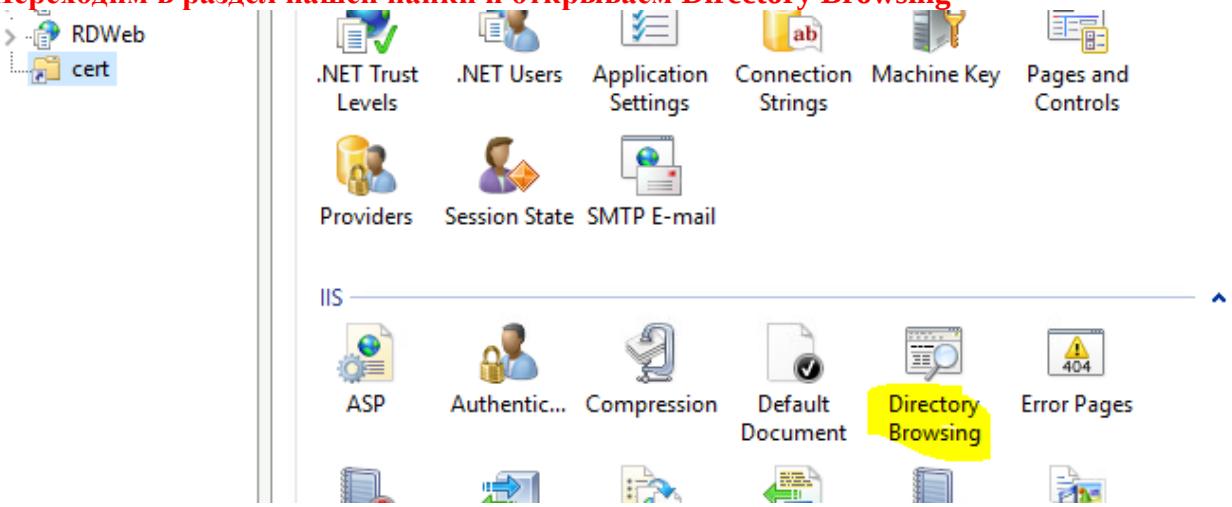
Создаем виртуальную директорию cert



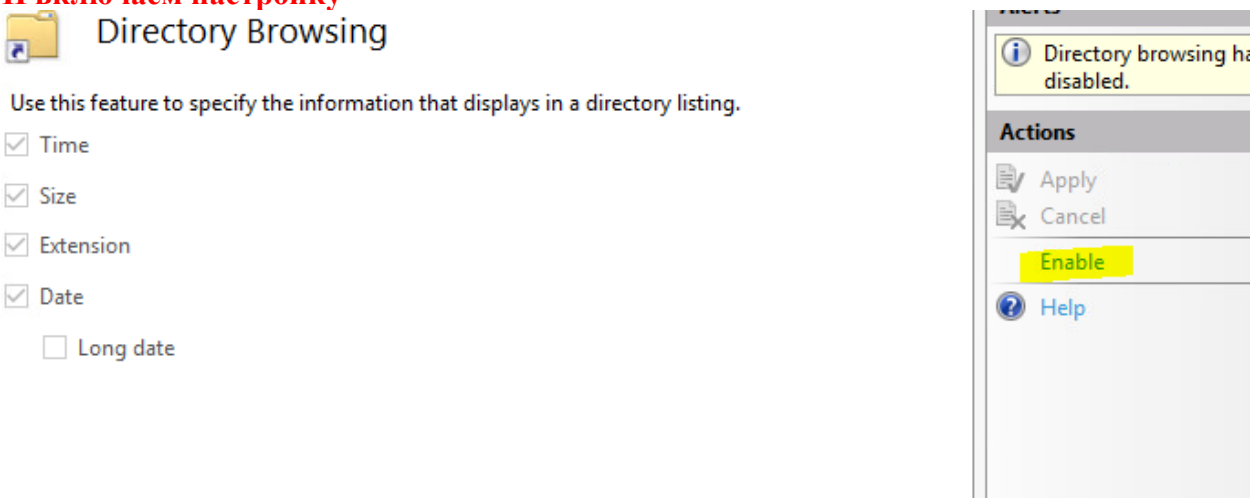
Указываем имя – cert
И путь – C:\Windows\System32\CertSrv\CertEnroll



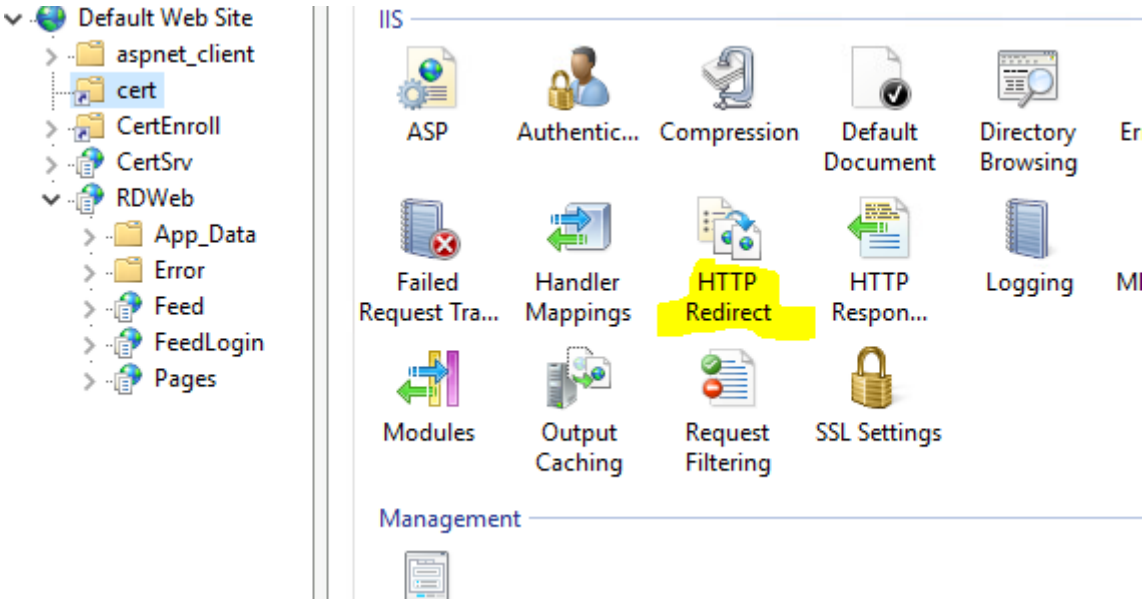
Переходим в раздел нашей папки и открываем Directory Browsing



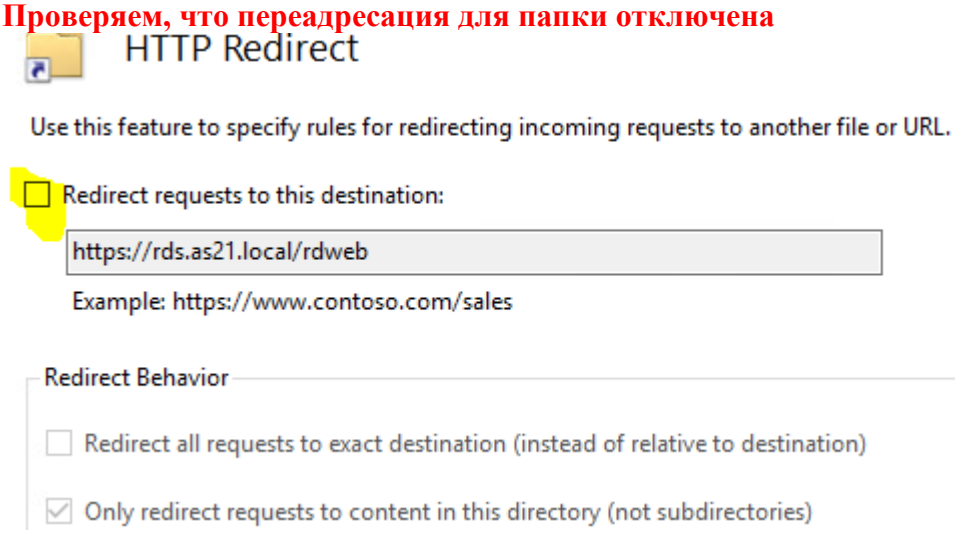
И включаем настройку



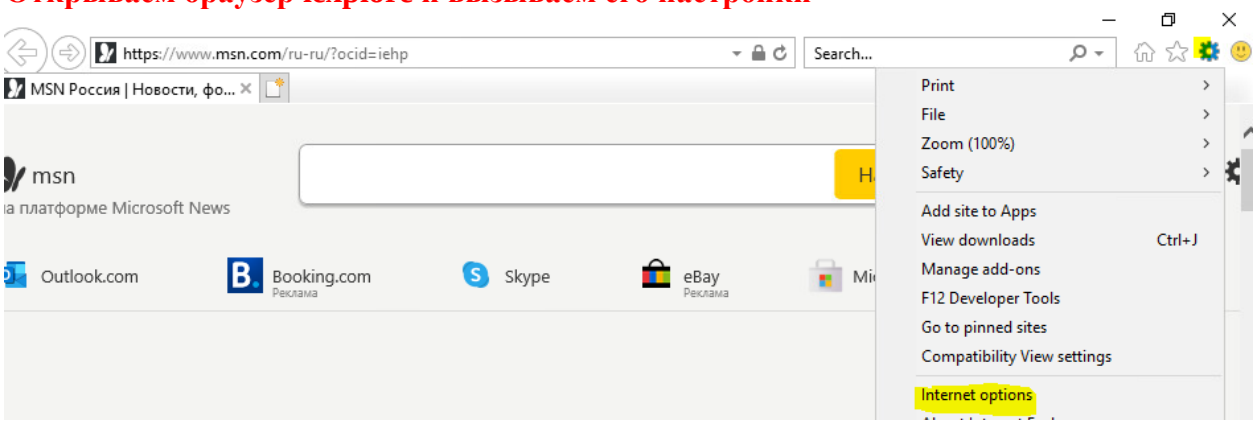
Открываем HTTP redirect для нашей папки



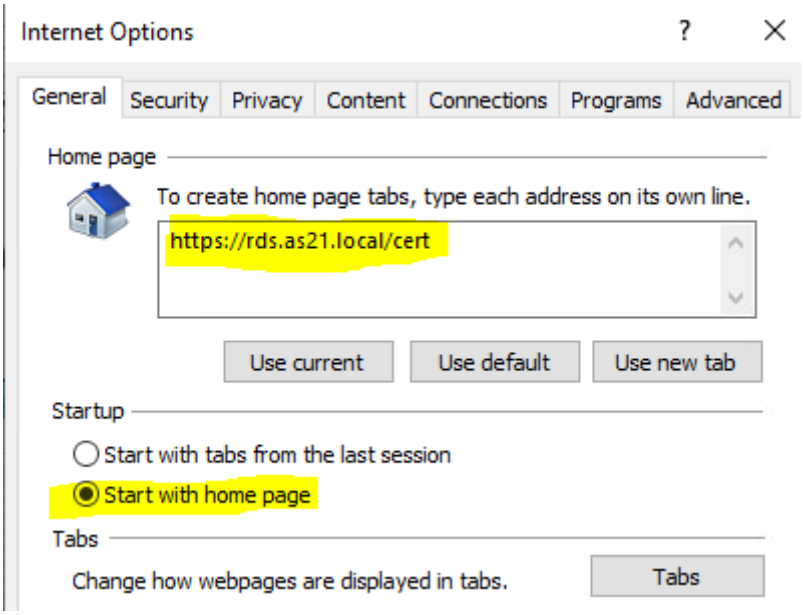
Проверяем, что переадресация для папки отключена



Открываем браузер iexplore и вызываем его настройки



Прописываем стартовую страницу и проверяем, что он должен открывать её при запуске



Сертификаты для членов группы Group3, для защиты подключений RDS, для сайтов и всех прочих целей должны быть выпущены этим центром сертификации.
Сделано ранее

WEB СЕРВЕР НА WINDMZ

Удаленное подключение к WINDMZ

Настройка web-сервера на WINDMZ
Сделайте сервер членом рабочей группы WEB.
Настраиваем на WINDMZ ip адреса и вводим в рабочую группу WEB
Создаем в DNS A запись для www, которая ссылается на ip адрес WINDMZ
Сначала нужно настроить доступ с сервера, где есть IIS, предлагаю с DC
На сервере WINDMZ настроить ip адреса. Выключить firewall
Netsh firewall set opmode mode=disable или netsh advfirewall set allprofiles state off

```
C:\Users\Administrator>netsh firewall set opmode mode=disable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .

Ok.
```

Затем набираем winrm quickconfig

```
C:\Users\Administrator>winrm quickconfig
```

На сервере DC запустить команду

```
C:\Users\Administrator>winrm help config
```

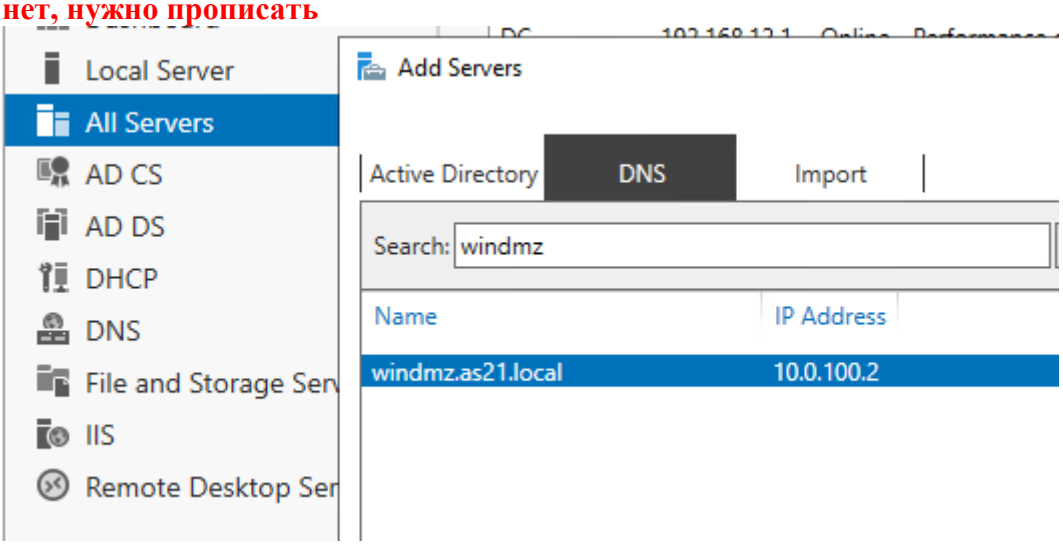
Внизу отображаемой помощи найти

```
winrm set winrm/config/client @{TrustedHosts="<local>"}
```

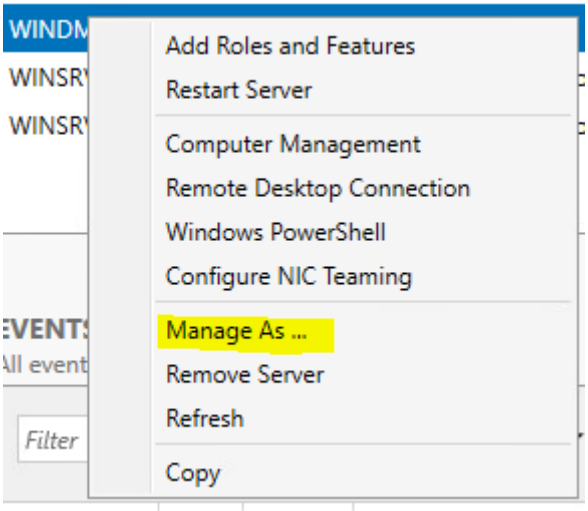
Скопировать и заменить <local> на * и запустить. Должны получить:

```
C:\Users\Administrator>winrm set winrm/config/client @{TrustedHosts="*"}
Client
    NetworkDelayms = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
    Auth
        Basic = true
        Digest = true
        Kerberos = true
        Negotiate = true
        Certificate = true
        CredSSP = false
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    TrustedHosts = *
```

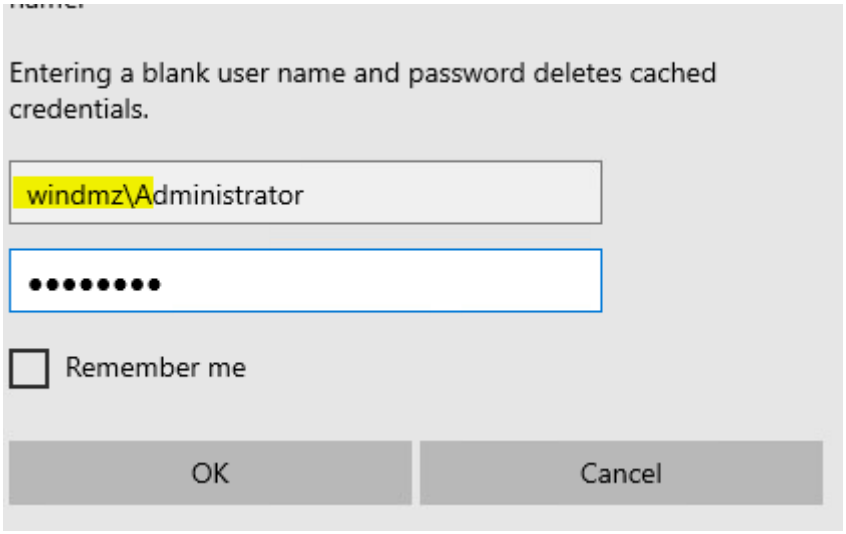
В оснастке All Servers добавляем его по DNS имени (у меня он прописан в DNS), если нет, нужно прописать



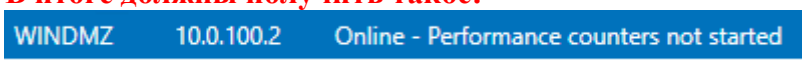
Нажать правую кнопку на WINDMZ и выбрать Manage As …



Ввести учетную запись формата WINDMZ\Administrator



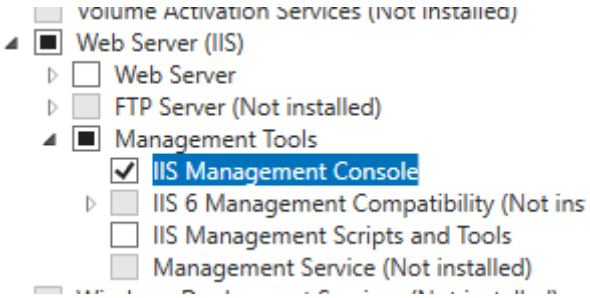
В итоге должны получить такое:



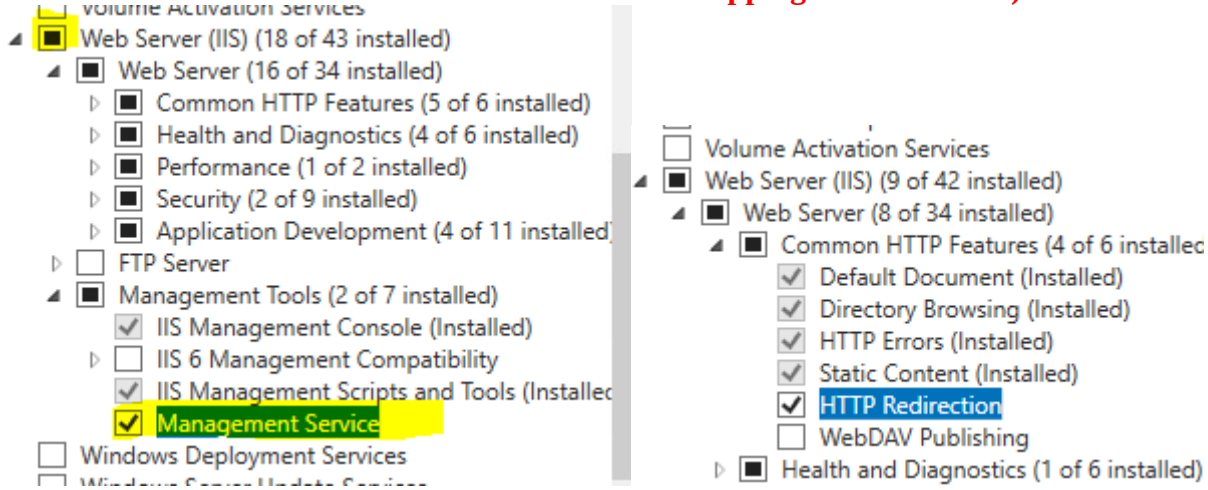
Настройка подключения консоли IIS к WINDMZ

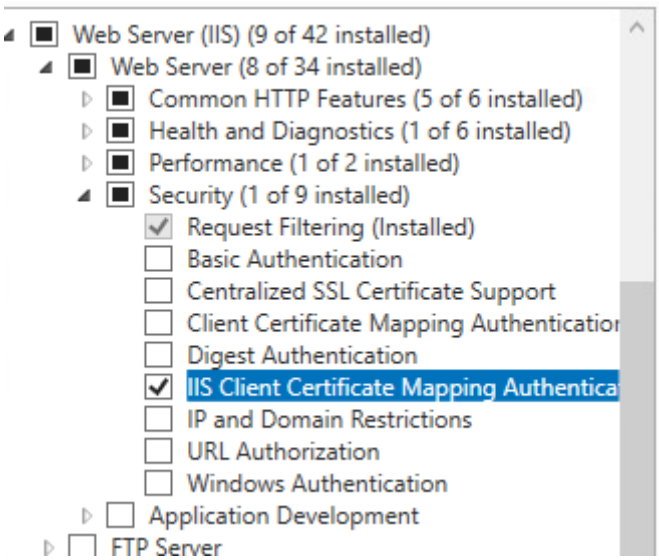
Установите на сервер компоненты IIS.

На DC устанавливаем набор инструментов IIS Management Console (если не делали эмуляцию Интернет)



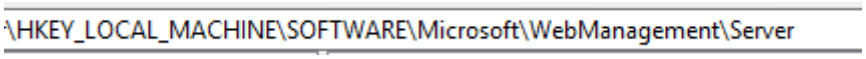
На WINDMZ устанавливаем роль IIS сервера (стандартный выбор + Management Service + HTTP Redirection + iisClientCertificateMappingAuthentication)



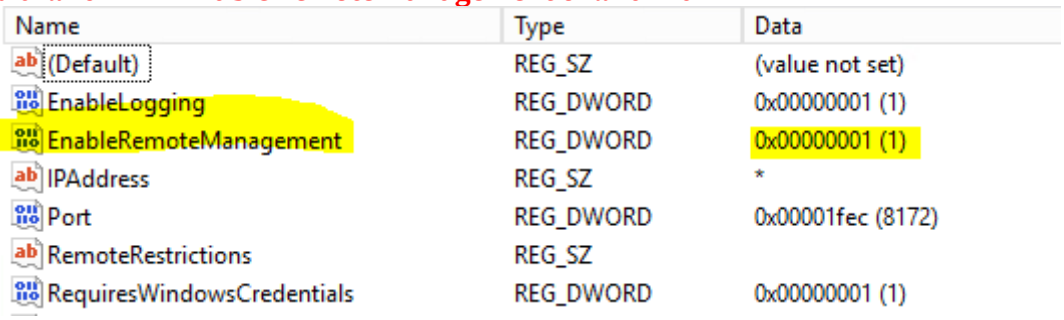


Включить firewall
Netsh firewall set opmode mode=enable или netsh advfirewall set allprofiles state on

Разрешить подключение удаленной IIS консоли
Запустить на WINDMZ regedit, найти в поиске EnableRemoteManagement или по ссылке



Установить EnableRemoteManagement значение 1



Name	Type	Data
(Default)	REG_SZ	(value not set)
EnableLogging	REG_DWORD	0x00000001 (1)
EnableRemoteManagement	REG_DWORD	0x00000001 (1)
IPAddress	REG_SZ	*
Port	REG_DWORD	0x00001fec (8172)
RemoteRestrictions	REG_SZ	
RequiresWindowsCredentials	REG_DWORD	0x00000001 (1)

Запускаем службу WMSVC: Net start wmsvc

2. Настройте сайт со следующей страницей по умолчанию:

```
<html>
        <body>
                <center>
                        <h1>
                                Test site
                        </h1>
                </center>
        </body>
</html>
```

Заходим на WINDMZ через \\WINDMZ\C$ по пути C:\inetpub\wwwroot и создаем файл index.htm (аккуратнее с двойным расширением)

```
 Directory of C:\inetpub\wwwroot

07/27/2021  10:19 PM    <DIR>          .
07/27/2021  10:19 PM    <DIR>          ..
07/27/2021  10:06 PM               703 iisstart.htm
07/27/2021  10:06 PM            99,710 iisstart.png
07/27/2021  10:19 PM                 4 index.htm
               3 File(s)        100,417 bytes
               2 Dir(s)  13,863,919,616 bytes free
```

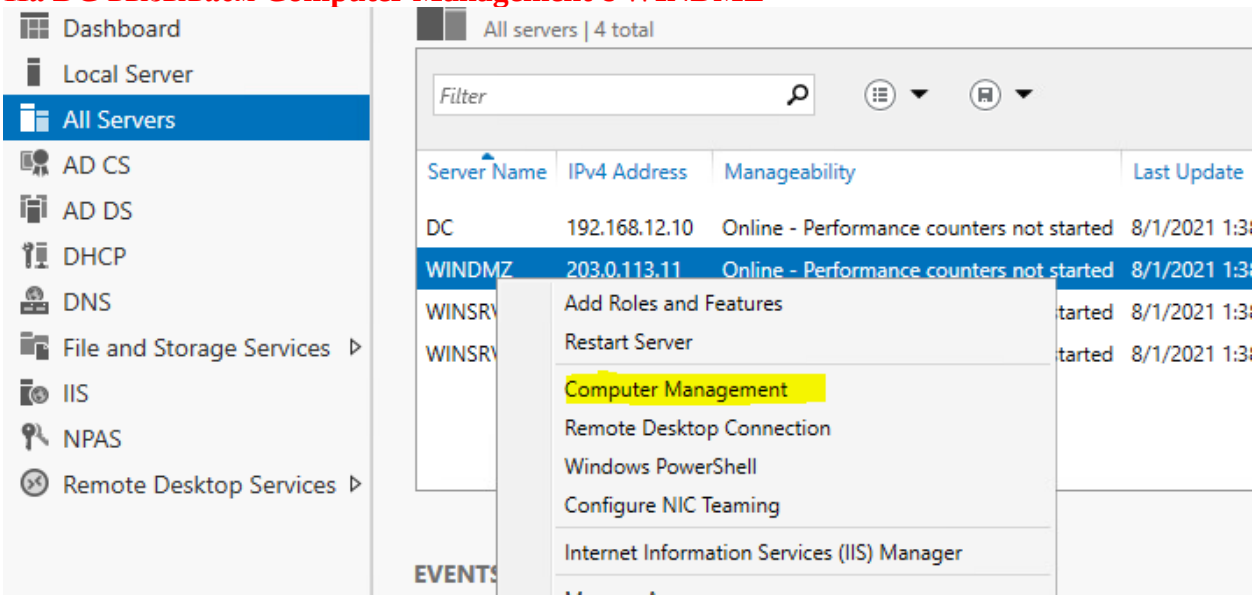
Настройка аутентификации по сертификатам

Сайт должен быть доступен по имени www.AS21.local только по протоколу https для членов группы Group1 при предъявлении пользовательского сертификата.

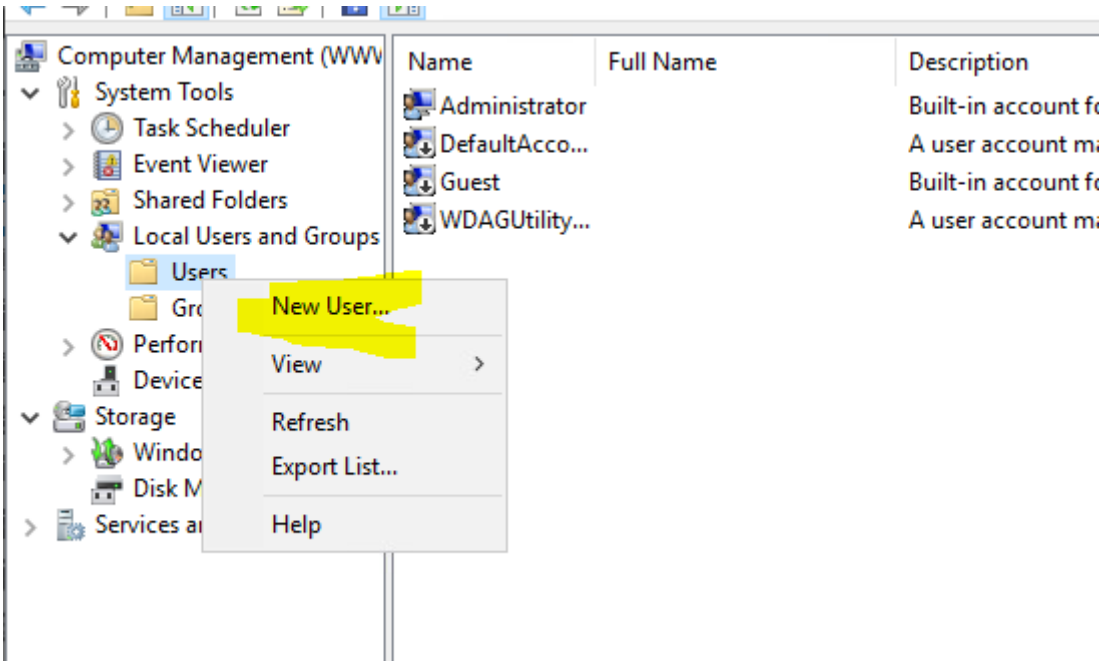
Добавление локального пользователя на WINDMZ

Создадим локального пользователя на WINDMZ, дадим ему права

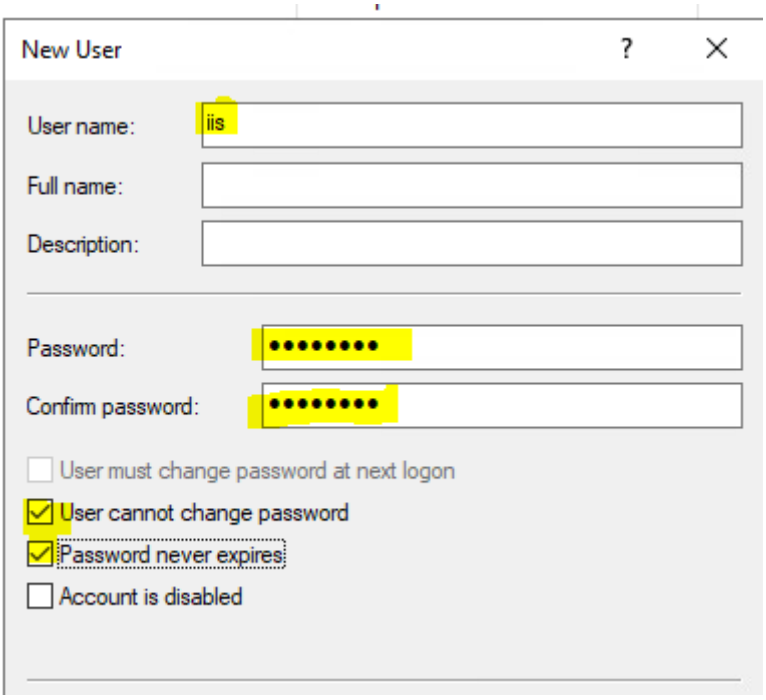
На DC вызываем Computer Management с WINDMZ

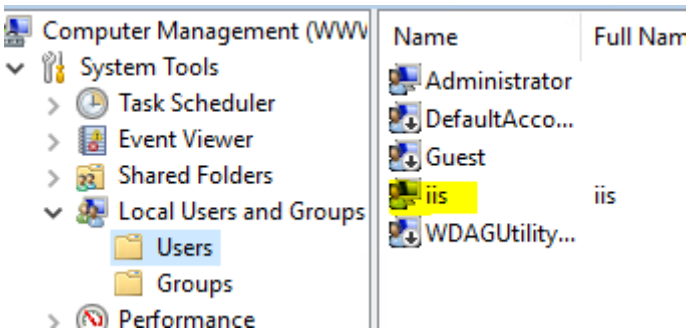


Открываем System Tools > Local Users and Groups > Users
Правой кнопкой и в меню выбираем New User



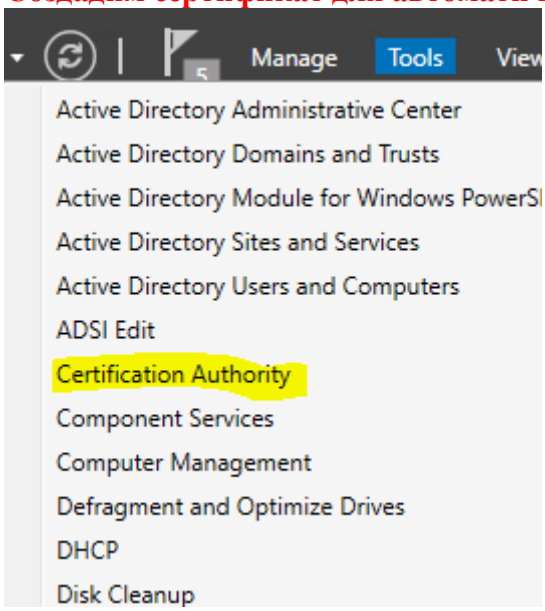
Вводим имя пользователя и пароль, устанавливаем запрет на смену пароля пользователем (User cannot change password) и бесконечность действия пароля (Password never expires)

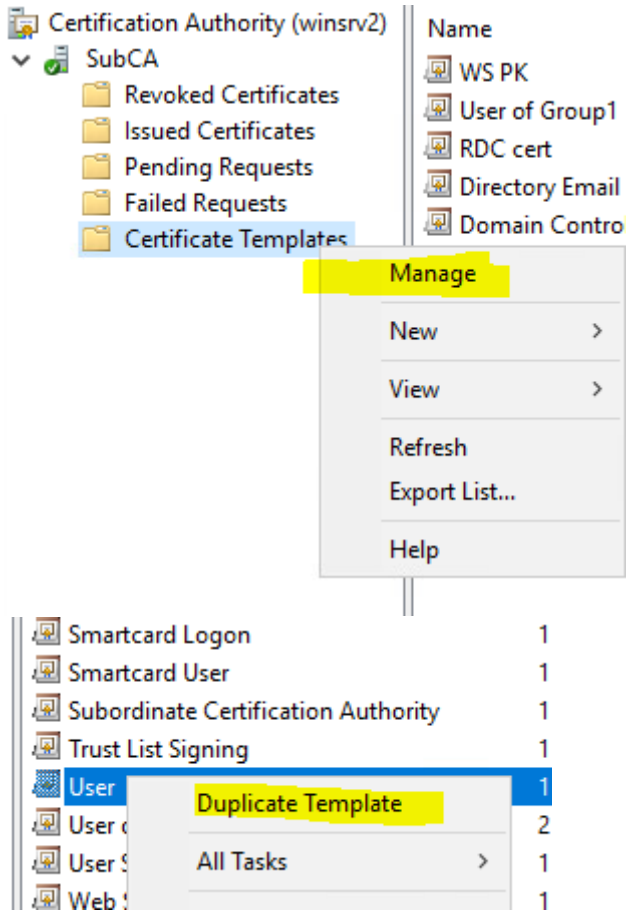


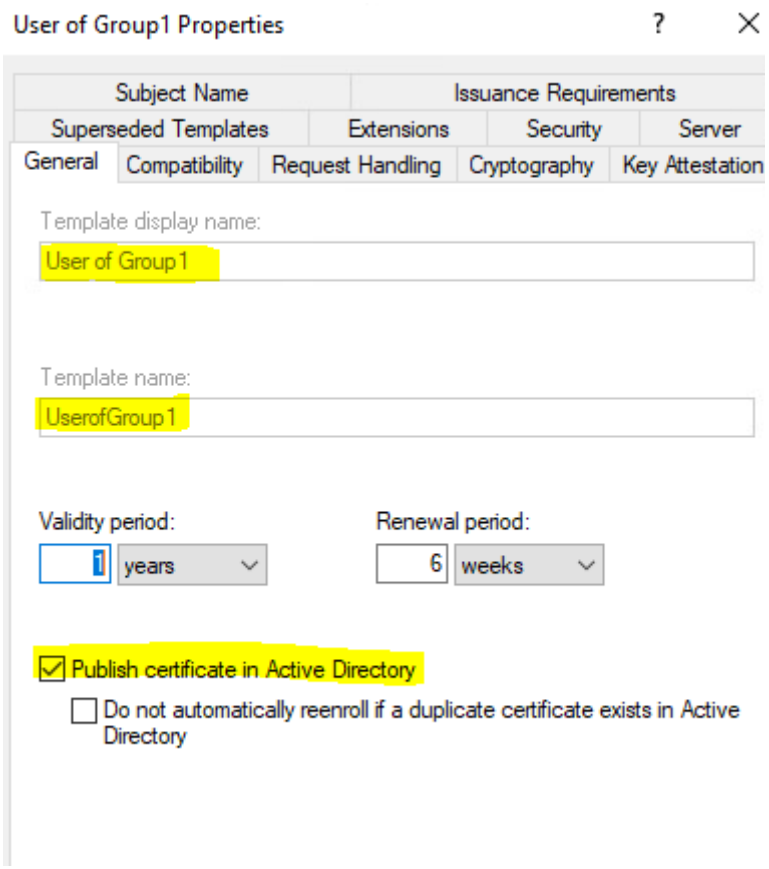


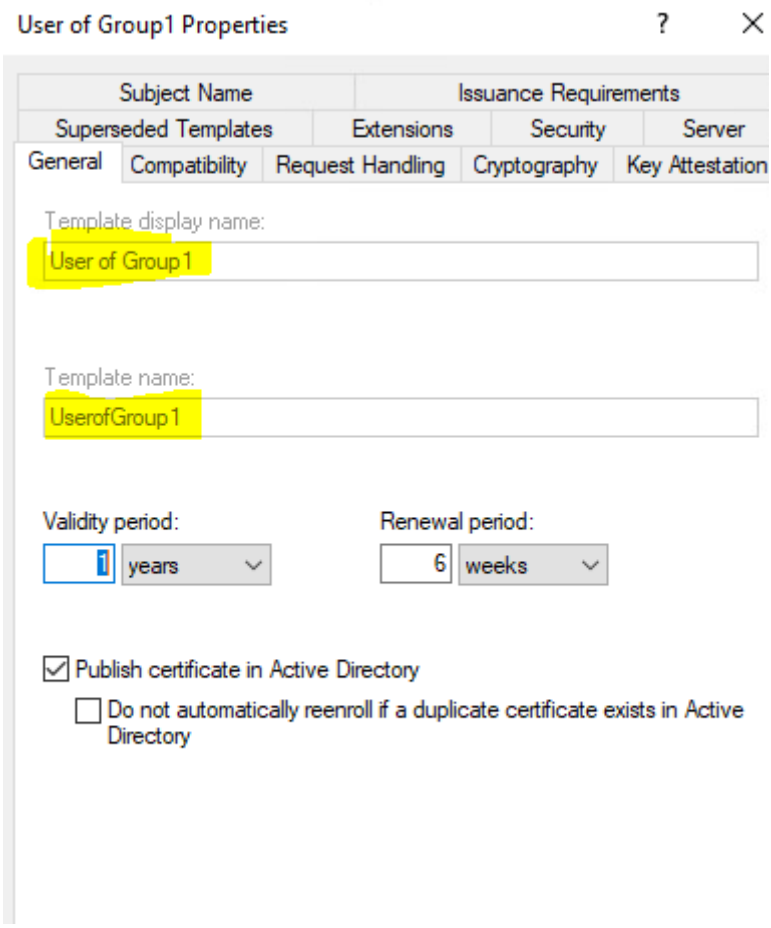
Создание шаблона для автовыдачи пользователя Group1

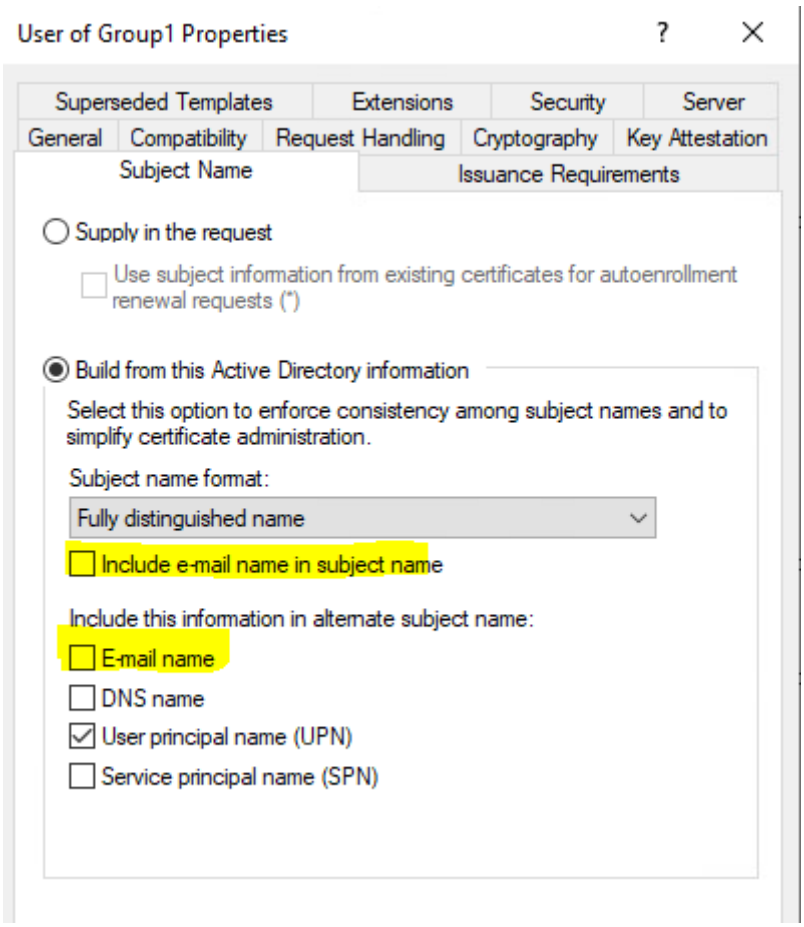
Создадим сертификат для автоматического выпуска для Group1

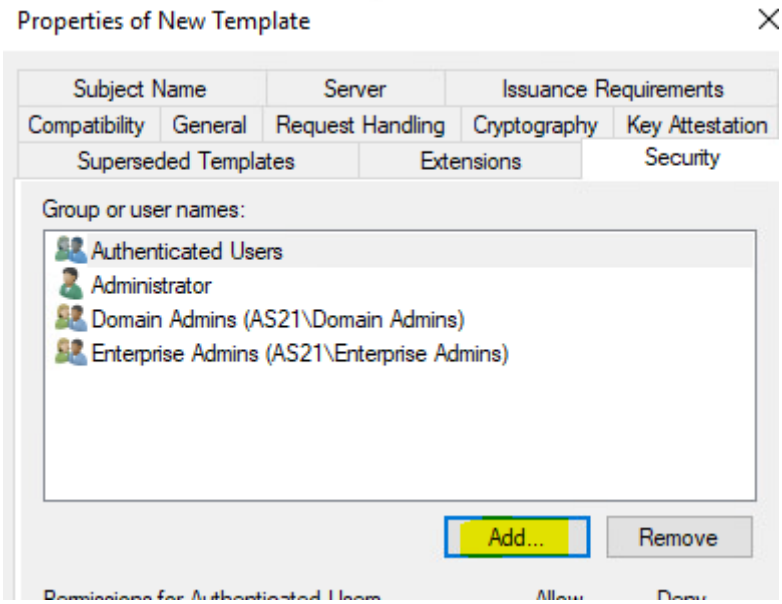


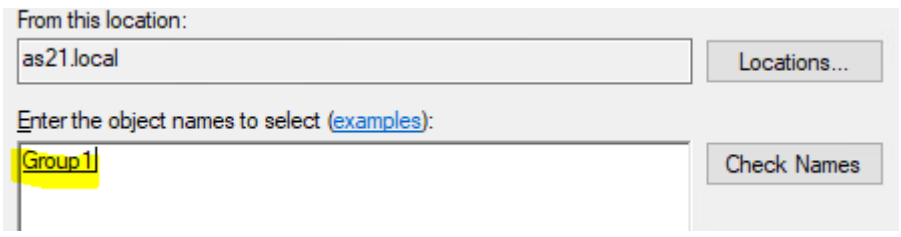


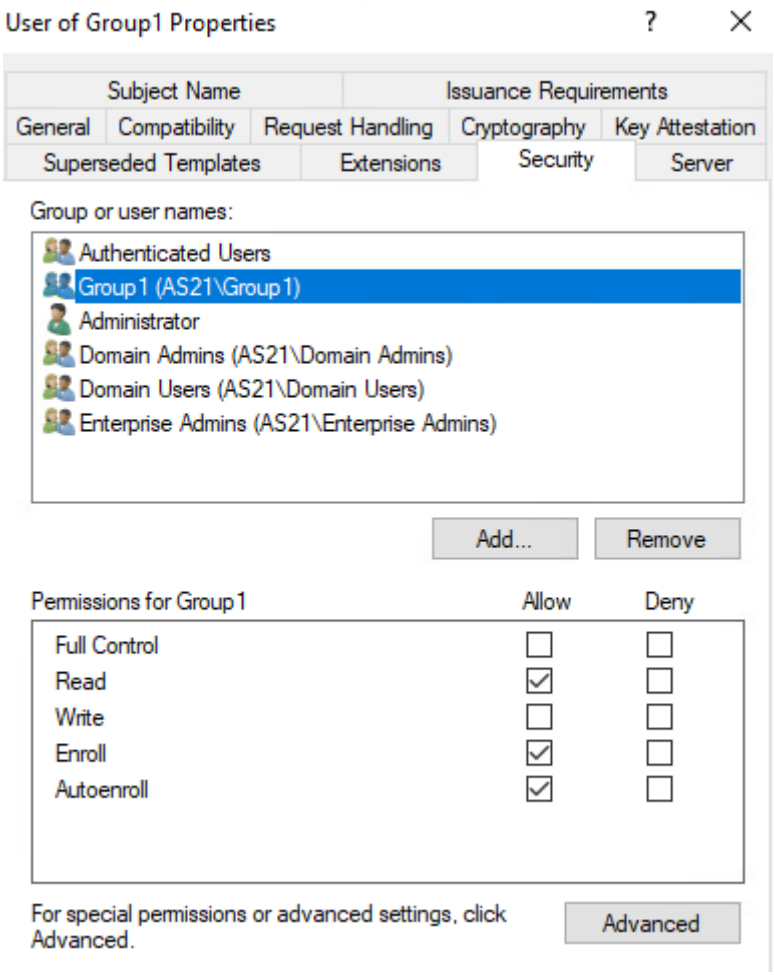

User of Group1 Properties
Subject Name
Issuance Requirements
Superseded Templates
Extensions
Security
Server
General
Compatibility
Request Handling
Cryptography
Key Attestation
Template display name:
User of Group1
Template name:
UserofGroup1
Validity period:
1
years
Renewal period:
6
weeks
Publish certificate in Active Directory
Do not automatically reenroll if a duplicate certificate exists in Active Directory

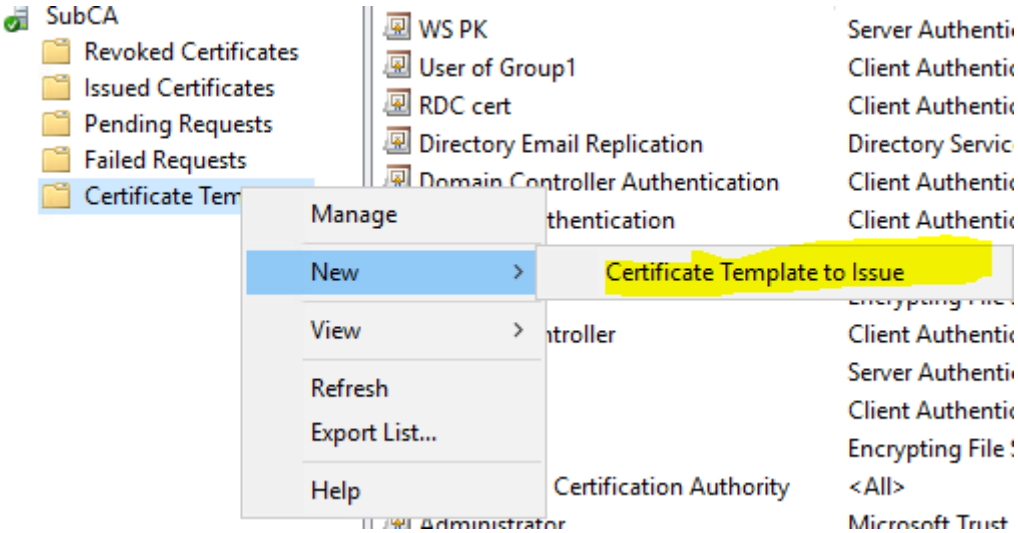

User of Group1 Properties
Subject Name
Issuance Requirements
Superseded Templates
Extensions
Security
Server
General
Compatibility
Request Handling
Cryptography
Key Attestation
Template display name:
User of Group1
Template name:
UserofGroup1
Validity period:
1
years
Renewal period:
6
weeks
Publish certificate in Active Directory
Do not automatically reenroll if a duplicate certificate exists in Active Directory

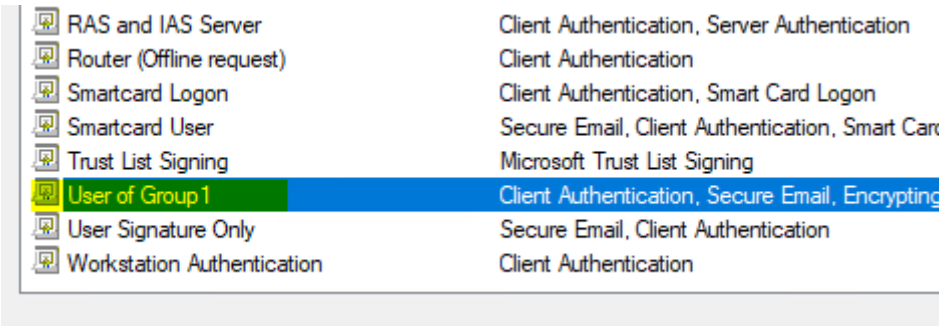

User of Group1 Properties
Superseded Templates
Extensions
Security
Server
General
Compatibility
Request Handling
Cryptography
Key Attestation
Subject Name
Issuance Requirements
Supply in the request
Use subject information from existing certificates for autoenrollment renewal requests (*)
Build from this Active Directory information
Select this option to enforce consistency among subject names and to simplify certificate administration.
Subject name format:
Fully distinguished name
Include e-mail name in subject name
Include this information in alternate subject name:
E-mail name
DNS name
User principal name (UPN)
Service principal name (SPN)


Properties of New Template
Subject Name
Server
Issuance Requirements
Compatibility
General
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Group or user names:
Authenticated Users
Administrator
Domain Admins (AS21\Domain Admins)
Enterprise Admins (AS21\Enterprise Admins)
Add...
Remove


From this location:
as21.local
Locations...
Enter the object names to select (examples):
Group1
Check Names

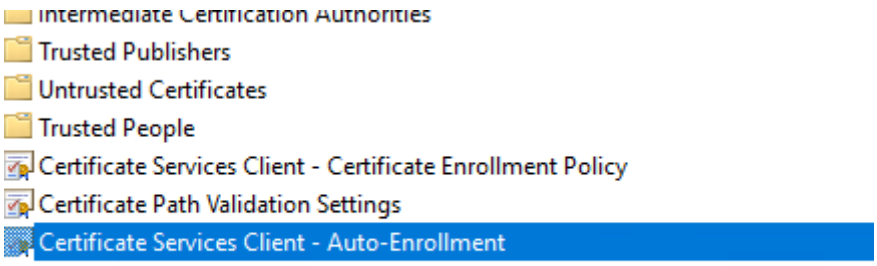

User of Group1 Properties
Subject Name
Issuance Requirements
General
Compatibility
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Server
Group or user names:
Authenticated Users
Group1 (AS21\Group1)
Administrator
Domain Admins (AS21\Domain Admins)
Domain Users (AS21\Domain Users)
Enterprise Admins (AS21\Enterprise Admins)
Add...
Remove
Permissions for Group1
Allow
Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced


SubCA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Tem
WS PK
User of Group1
RDC cert
Directory Email Replication
Manage
New
Certificate Template to Issue
View
Refresh
Export List...
Help
Certification Authority
Server Authenti
Client Authentic
Directory Servic
Encrypting File
<All>

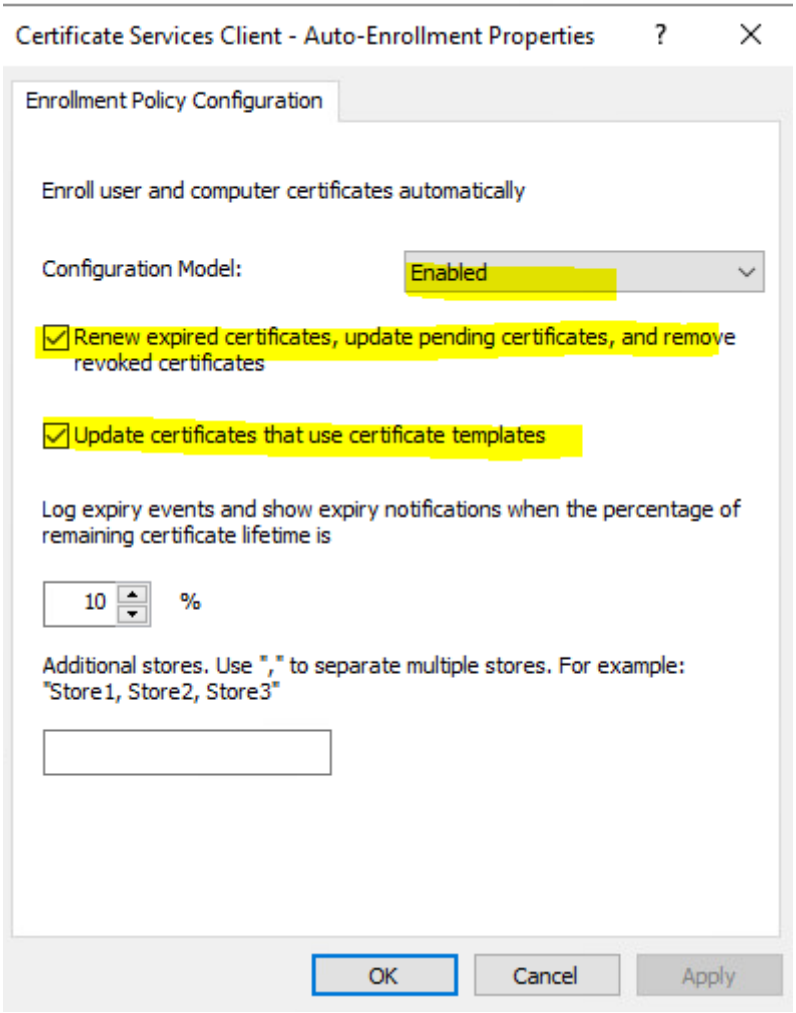

RAS and IAS Server
Client Authentication, Server Authentication
Router (Offline request)
Client Authentication
Smartcard Logon
Client Authentication, Smart Card Logon
Smartcard User
Secure Email, Client Authentication, Smart Card
Trust List Signing
Microsoft Trust List Signing
User of Group1
Client Authentication, Secure Email, Encrypting
User Signature Only
Secure Email, Client Authentication
Workstation Authentication
Client Authentication

Включаем авто выдачу сертификатов всем устройствам домена

GPO на домен: Computer Configuration > Policies > Windows Settings> Security Settings > Public Key Policies > Certificate Service Client – Auto-Enrollment -> Enabled

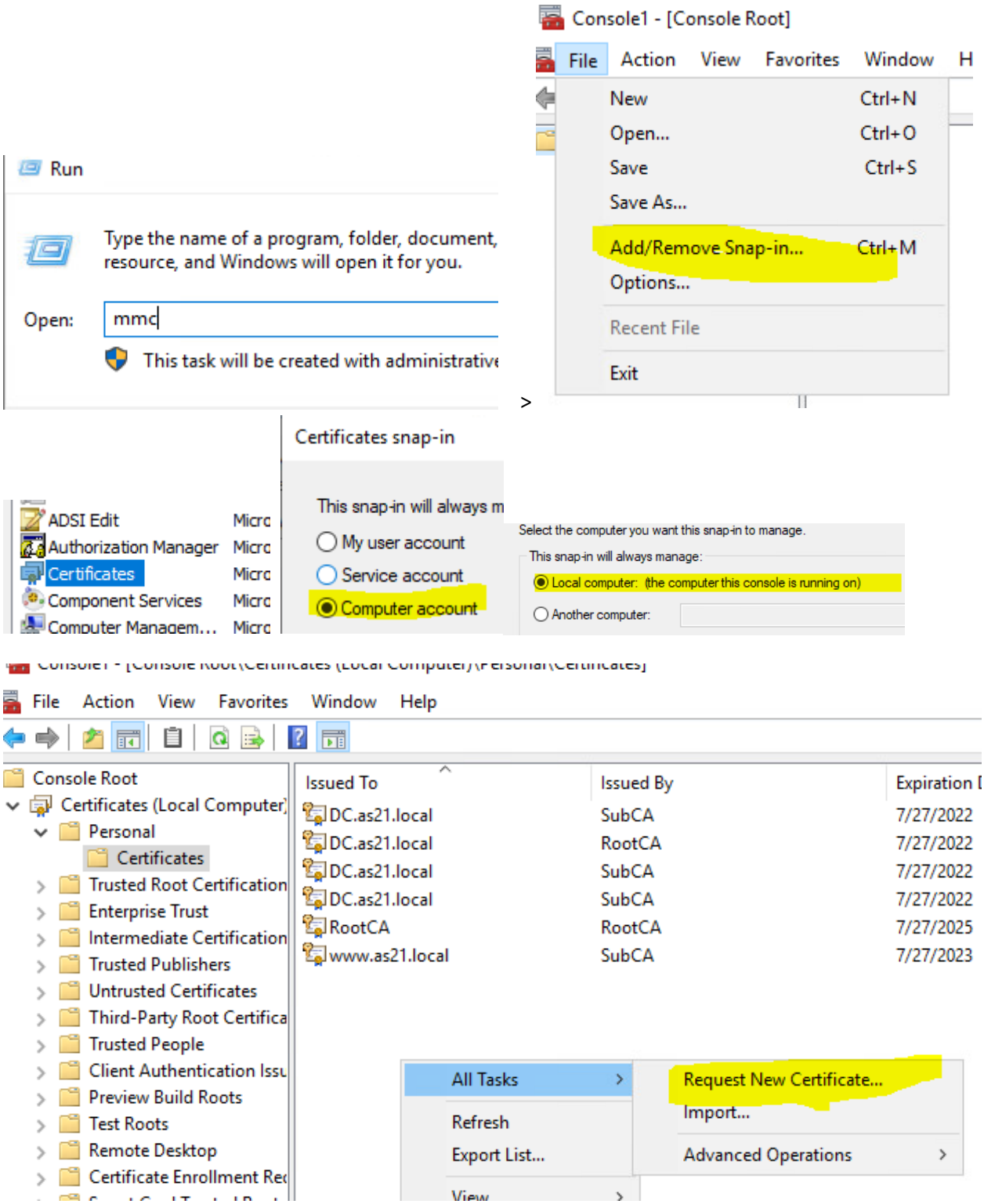


Включаем общую настройку выдачи и выбираем 2 конфигурации

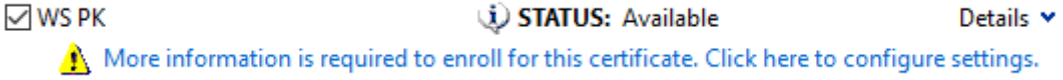


Выпуск и установка сертификата на WINDMZ

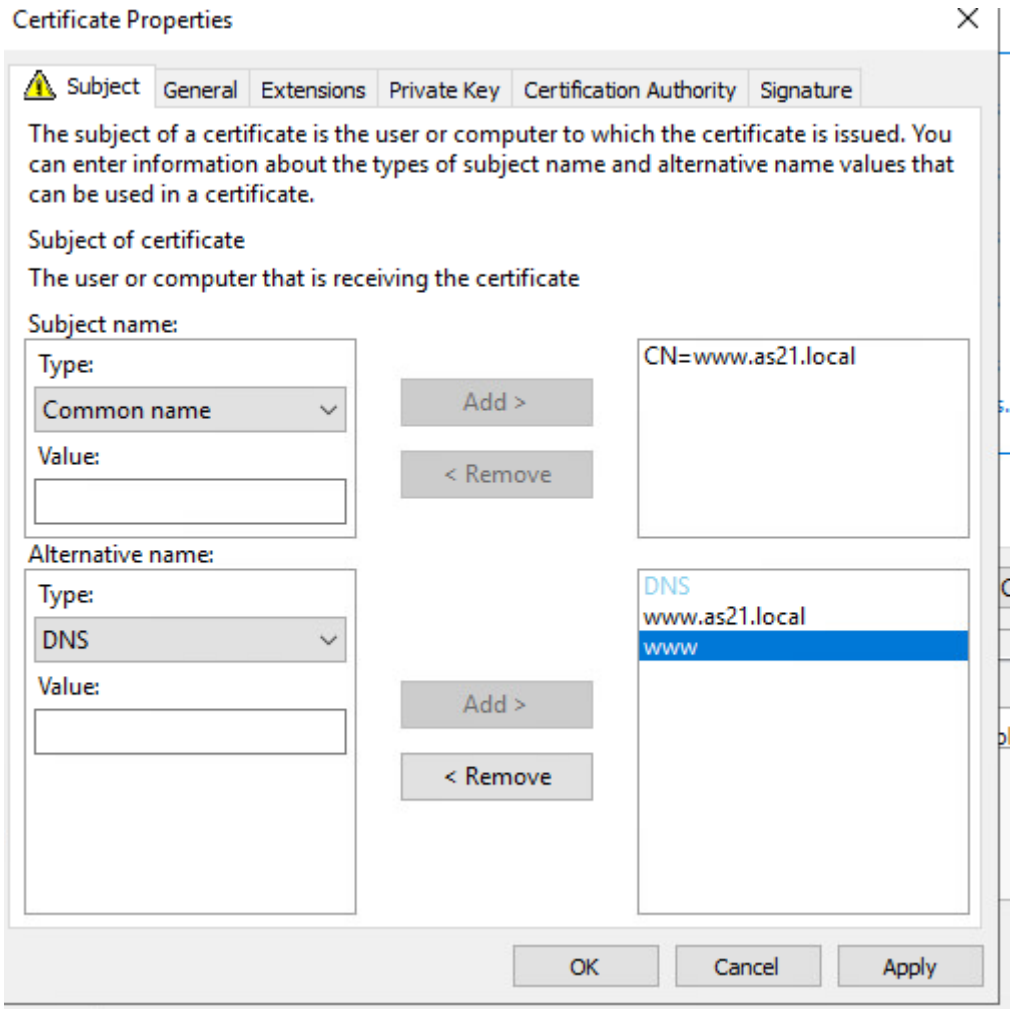
Создаем сертификат для сервера WINDMZ. Для этого на сервере DC запускаем mmc консоль Certificates



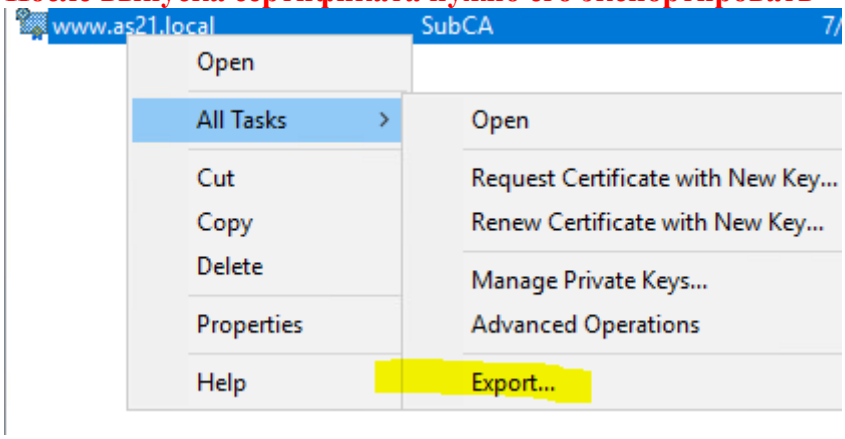
Выбираем наш шаблон, выпущенный для серверов

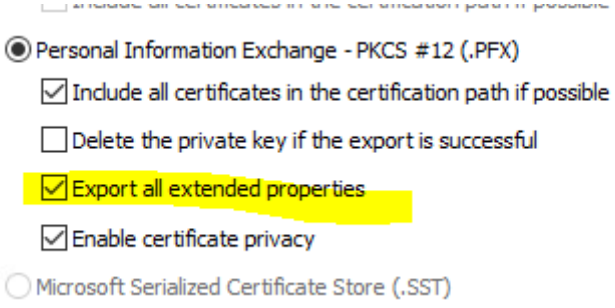


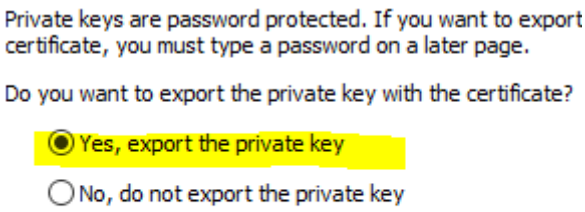
Добавляем параметры нашего сервера



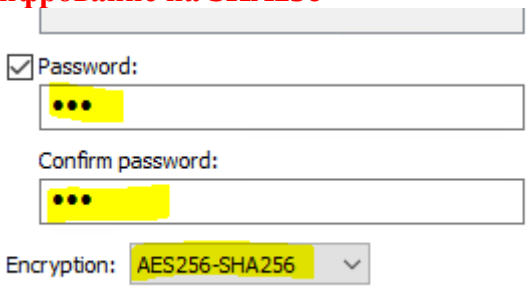
После выпуска сертификата нужно его экспортировать





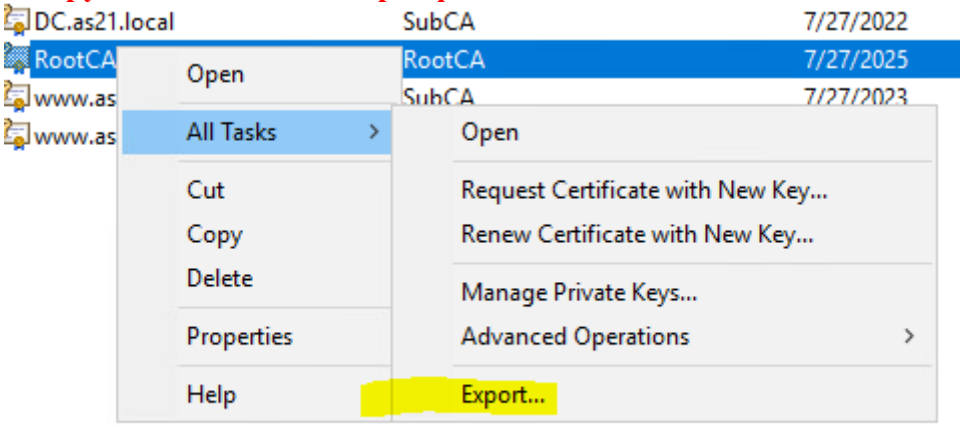


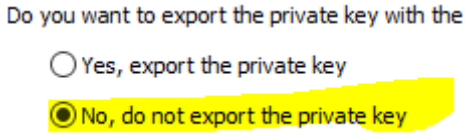
Введите пароль, который будет использован в дальнейшем при импорте и поменяйте шифрование на SHA256

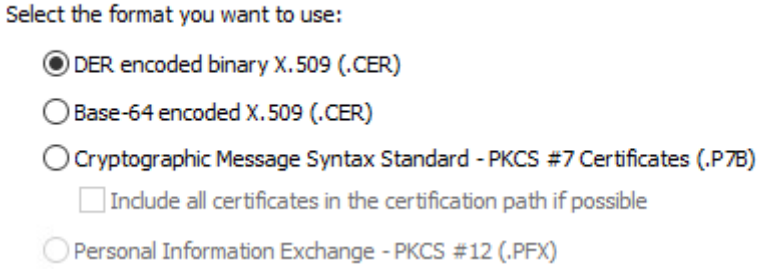


Экспортируем его на WINDMZ через \\WINDMZ\C$ по пути C:\cert.pfx

Выгружаем из консоли сертификат RootCA

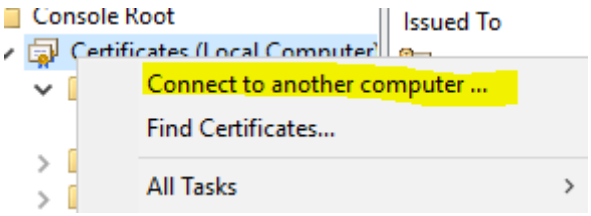


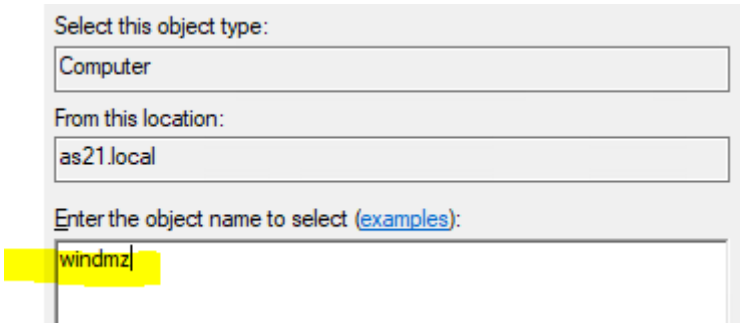




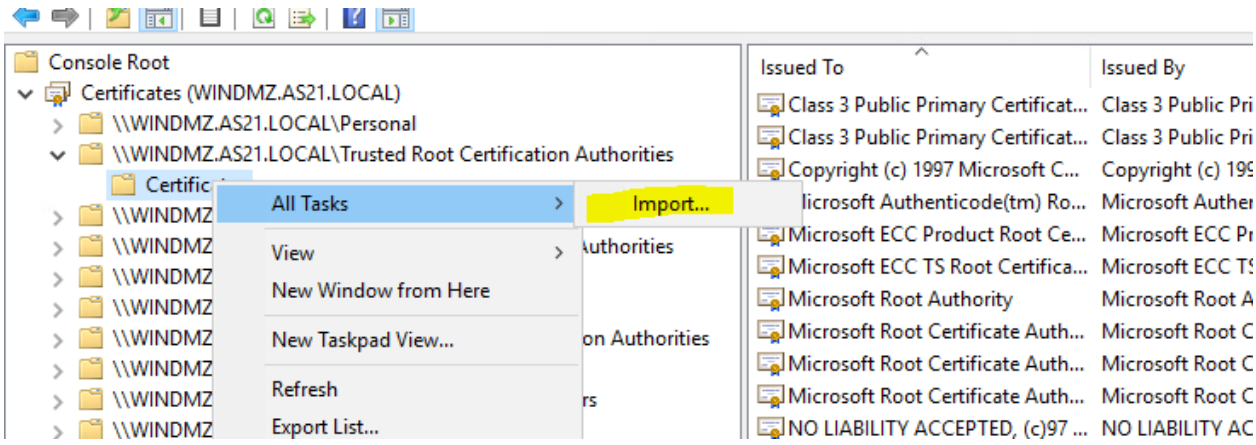
Экспортируем его по пути C:\root.cer

Из этой же консоли подключаемся к WINDMZ





Открываем Trusted Root Certification Authorities > Certificates и по правой кнопке делаем All Tasks > Import



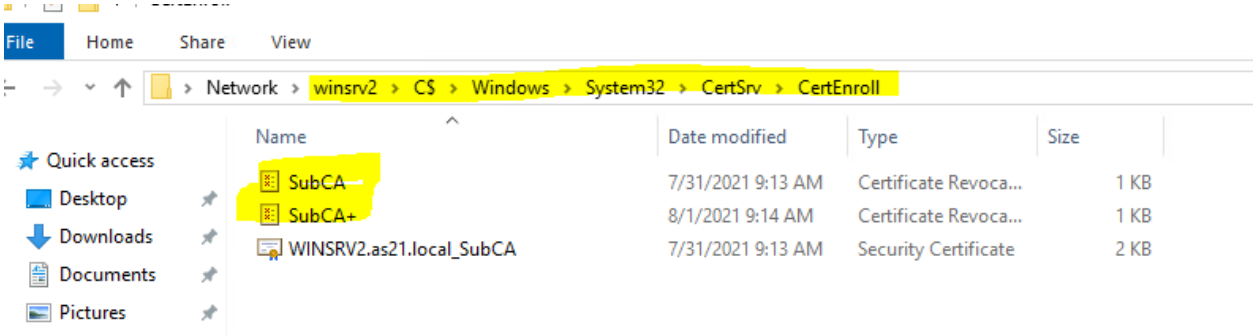
Выбираем сертификат C:\root.cer и импортируем его. ЖДЕМ пока не появится надпись, что успешно

Переходим на WINDMZ и запускаем команду
certutil –p <пароль> -importpfx C:\cert.pfx

Где пароль это тот, который устанавливали при экспорте сертификата.

Установка списка отозванных сертификатов на WINDMZ

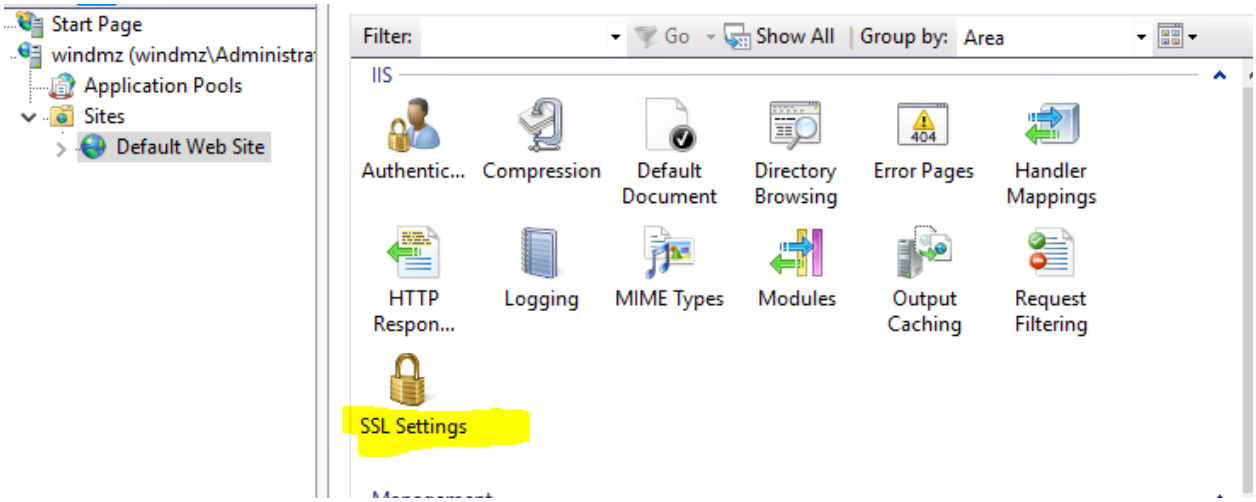
Добавляем список отозванных сертификатов на WINDMZ
Заходим на WINSRV2 по пути \\winsrv2\C$\Windows\System32\CertSrv\CertEnroll
Копируем файлы SubCA и SubCA+



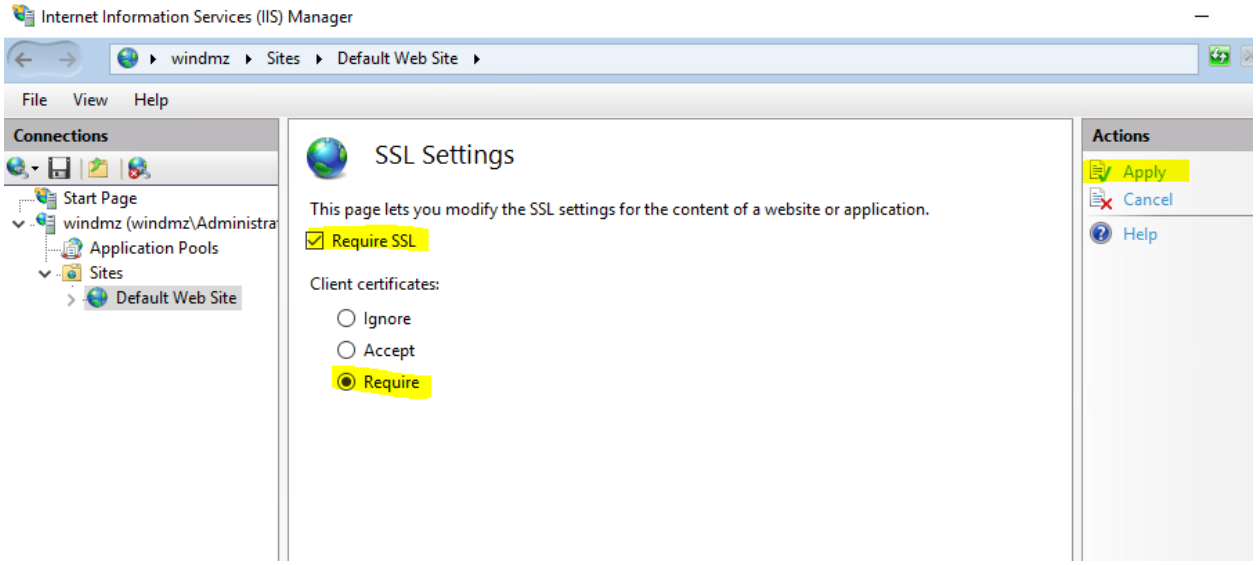
Идем на WINDMZ
Запускам команды:
certutil -addstore -f Root SubCa.crl
certutil -addstore –f Root SubCa+.crl

Настройка SSL на WINDMZ

Включим разрешение заходить только по сертификатам. Заходим в SSL Settings

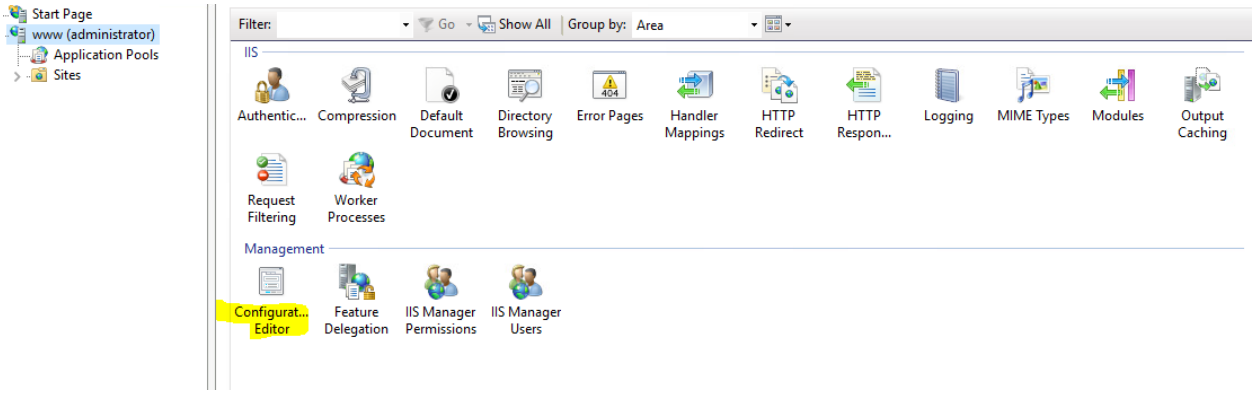


Включаем Require SSL, выбираем режим Require и нажимаем Apply

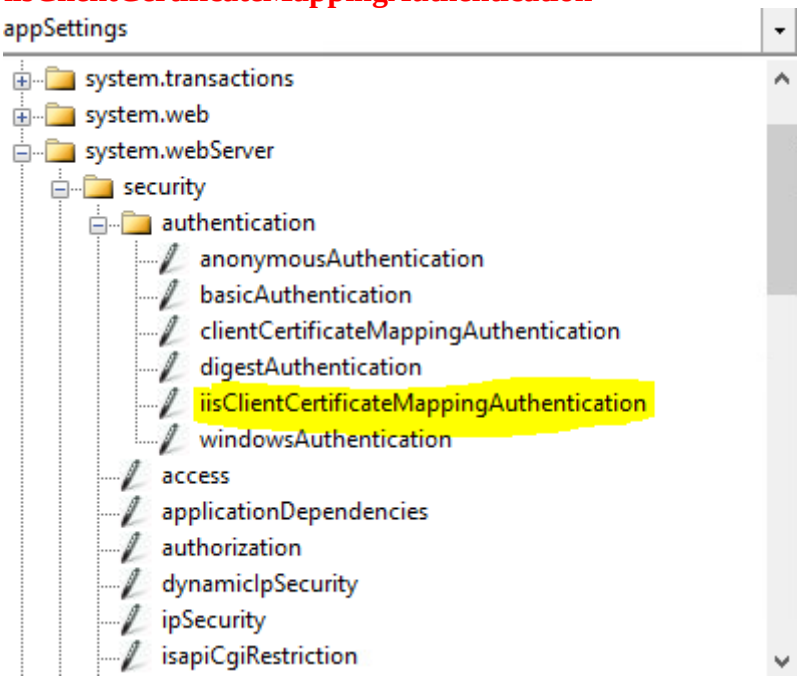


Настройка авторизации на WINDMZ

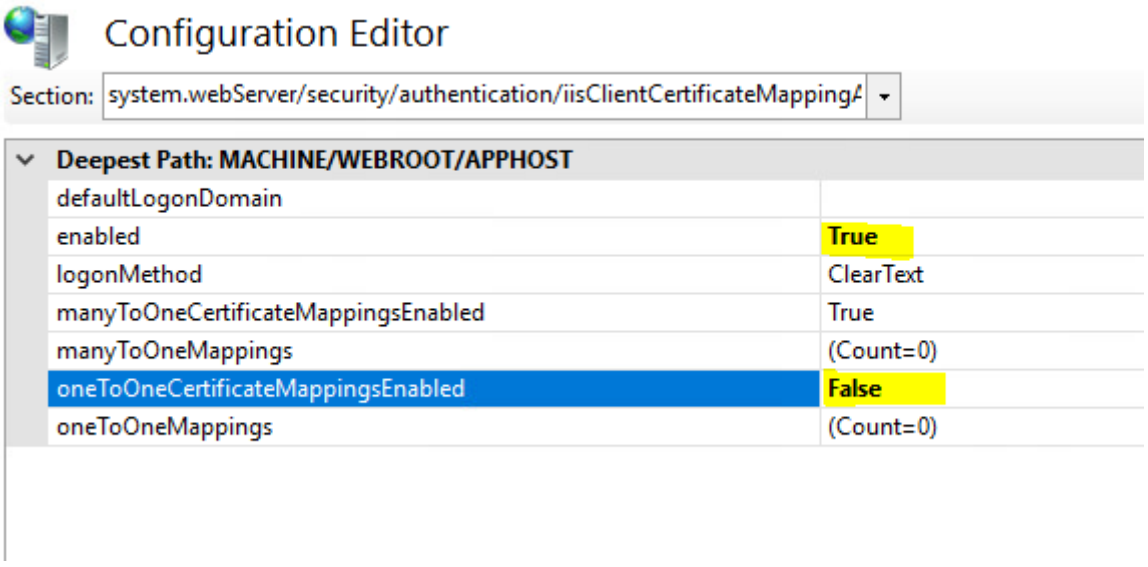
Теперь нам нужно настроить авторизацию. Идем в настройку сервера (не сайта) и запускаем Configuration Editor



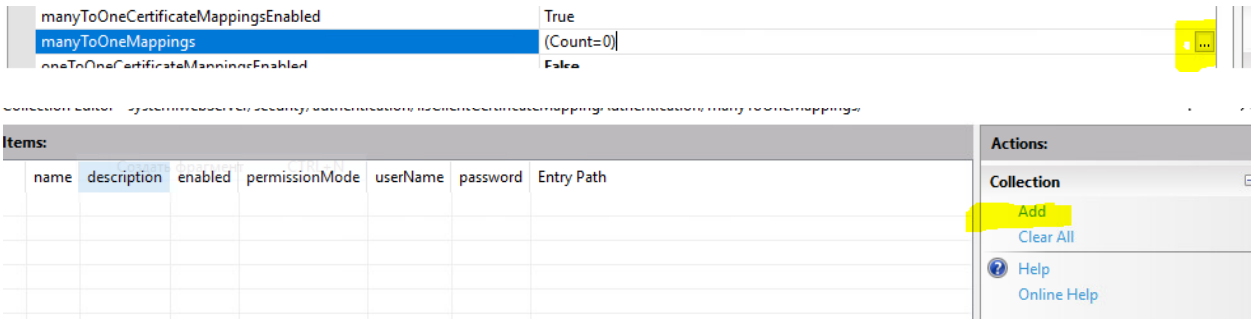
Выбираем раздел system.webServer > Security > Authentication -> iisClientCertificateMappingAuthentication



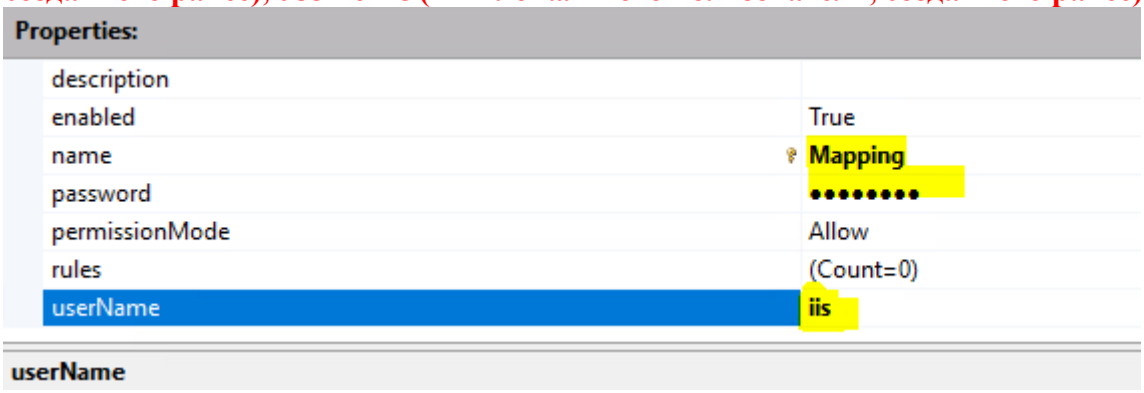
Включаем настройку (enabled = true), отключаем oneToOneCertificateMappingEnabled=false



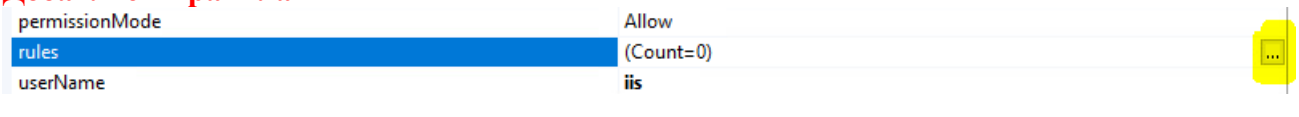
Добавляем настройки manyToOneMapping

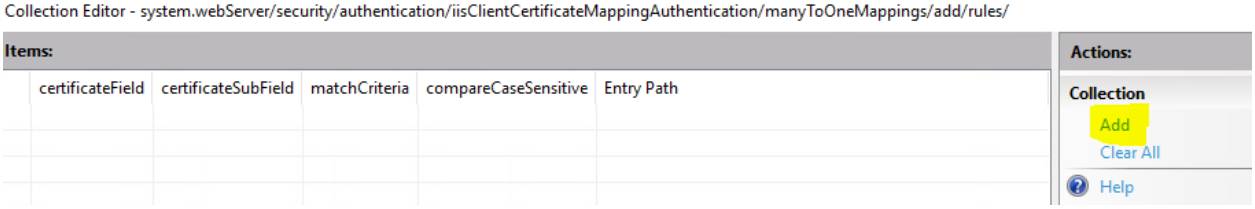


Вписываем name (любое имя), password (пароль локального пользователя, созданного ранее), username (имя локального пользователя, созданного ранее)

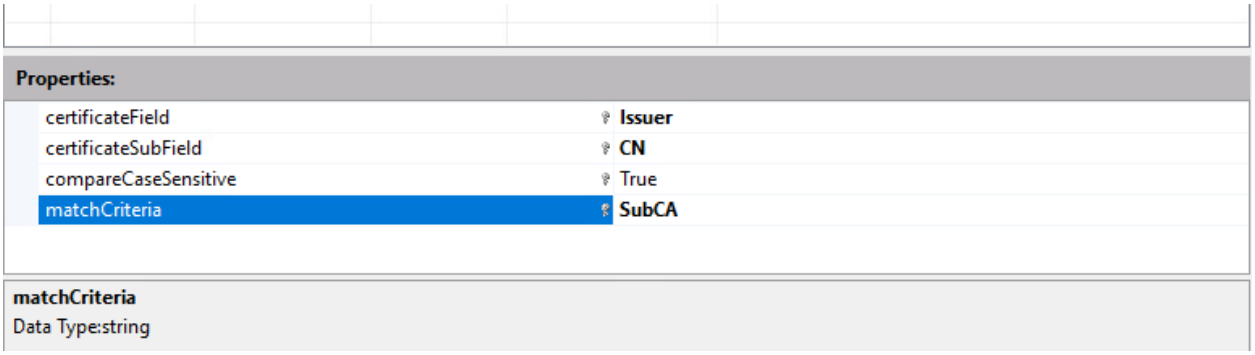


Добавляем правила



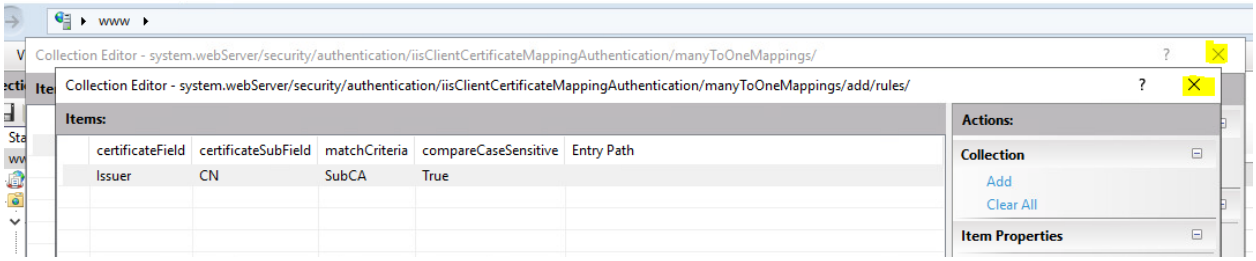


Заполняем поля

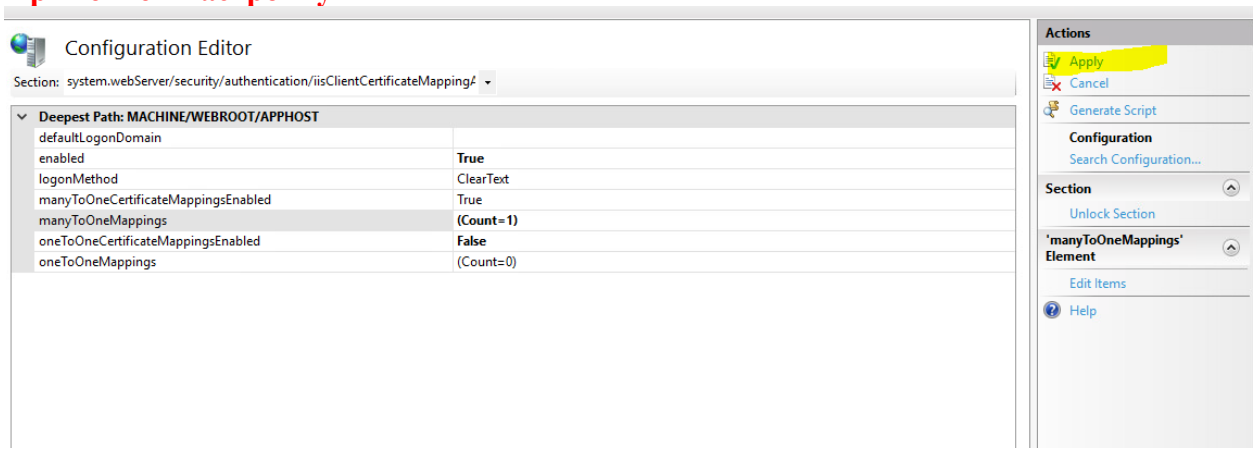


certificateField (поле сертификата, которое мы проверяем) – Issuer (издатель)
certificateSubField (тип значения в поле издателя) – CN
matchCriteria (что ищем в поле) – SubCA (наш центр сертификации)
ВАЖНО!!! Поле чувствительно к регистру

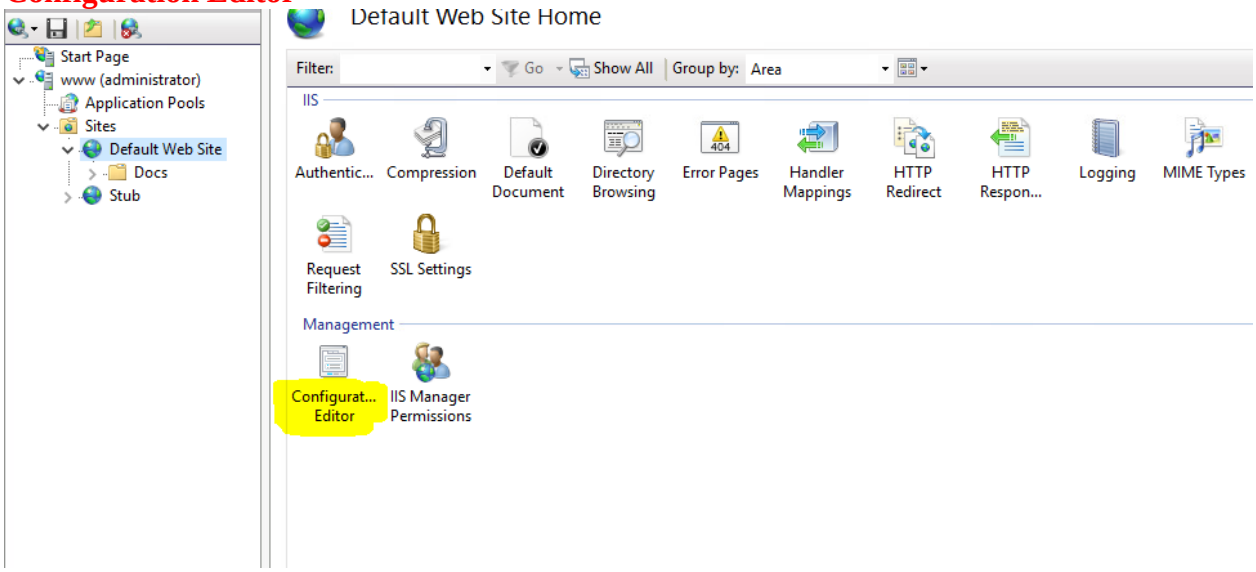
Закрываем оба окна



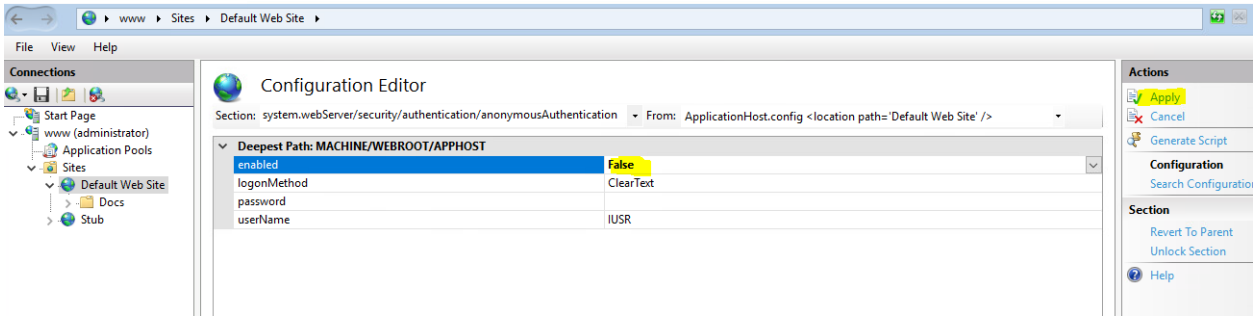
Применяем настройку



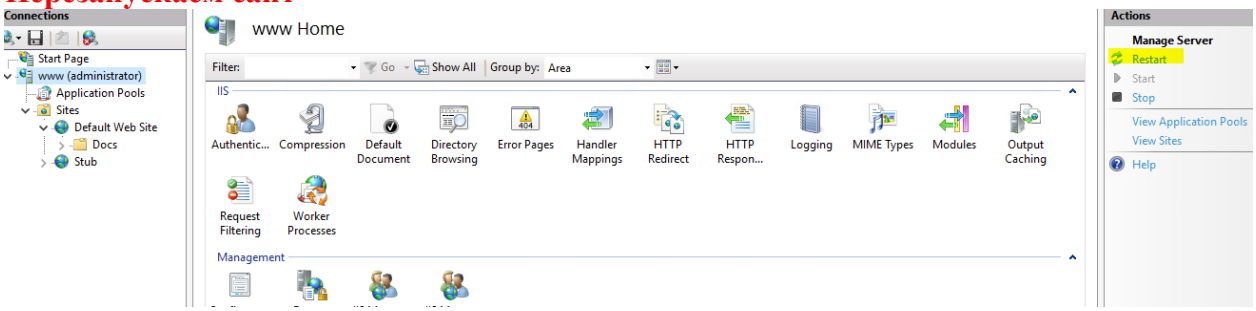
Теперь нам нужно настроить авторизацию. Идем в настройку сайта и запускаем Configuration Editor



Выбираем раздел system.webServer > Security > Authentication -> annonymousAuthentication
Отключаем настройку (enabled = false) и сохраняем изменения

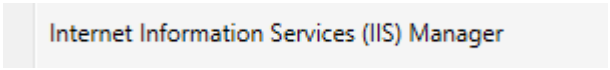


Перезапускаем сайт



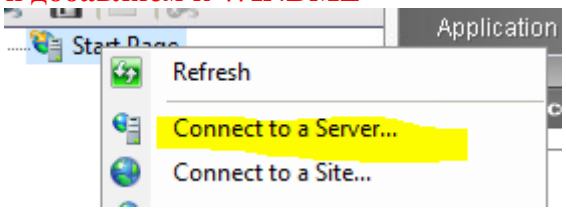
Настройка IIS на WINDMZ

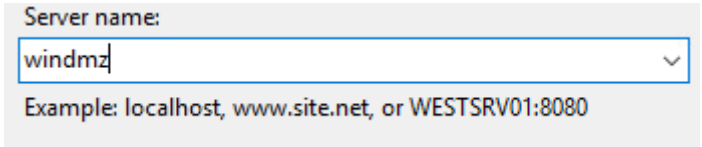
Теперь на DC запускаем консоль



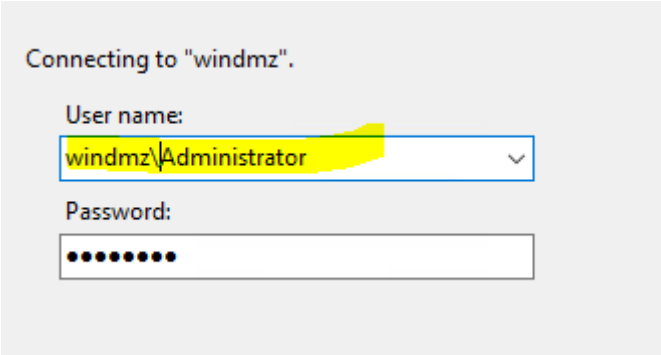
Убираем подключение к DC

и добавляем к WINDMZ

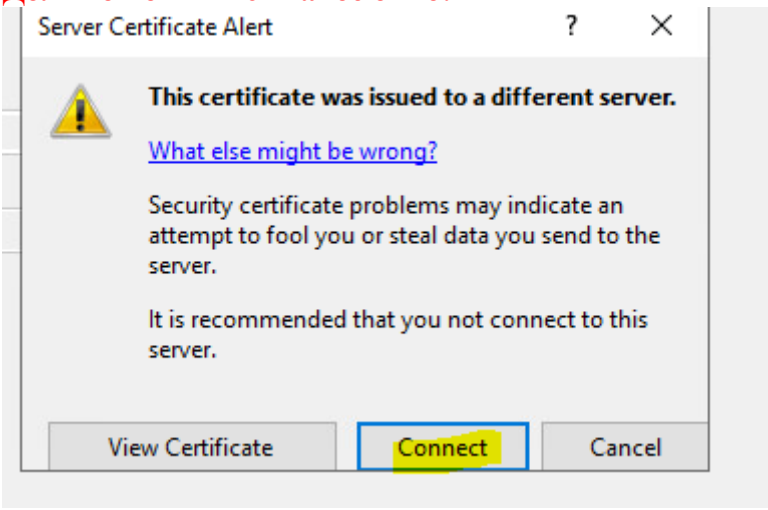




Добавляем учетную запись формата WINDMZ\Administrator



Должно появиться такое окно:

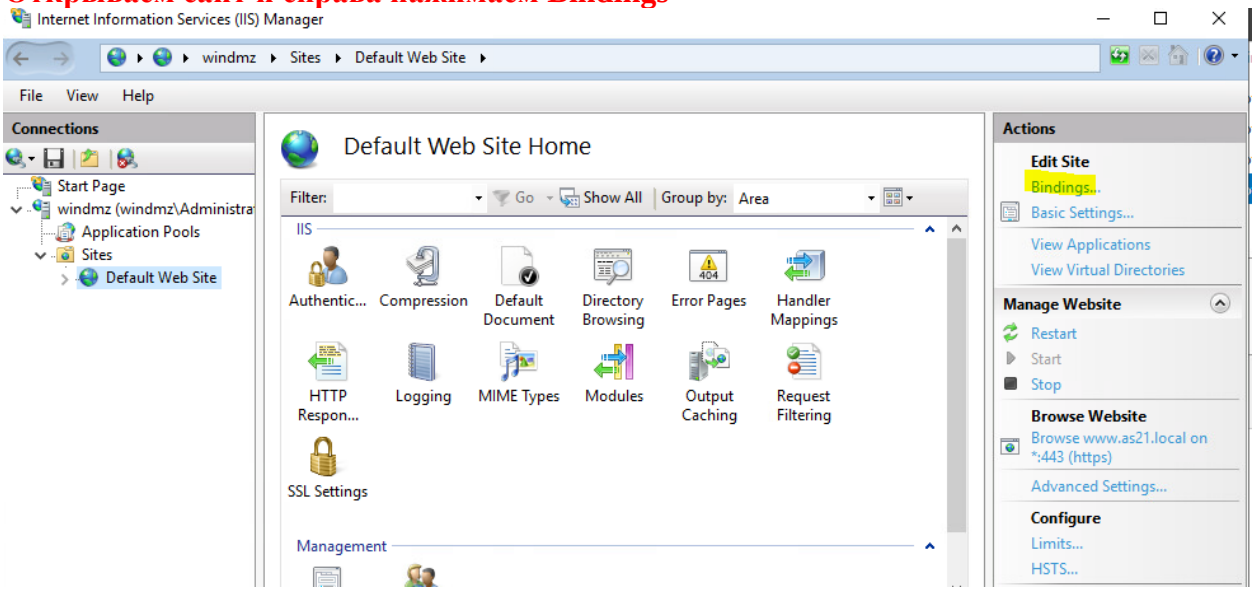


Нажимаем Connect

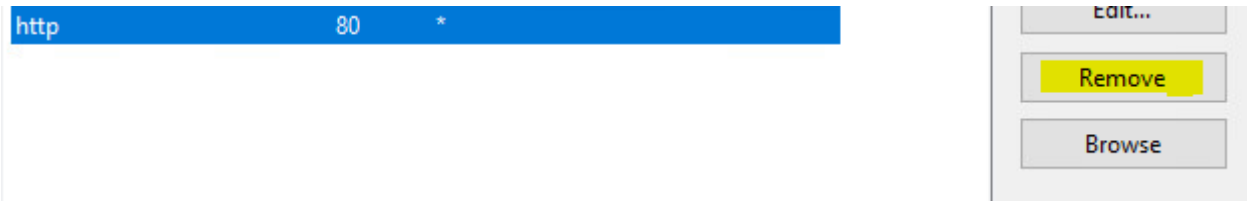
Важно!!! Если не сможет подключиться, нужно попробовать перезапустить службу на WINDMZ. Для этого идем на WINDMZ и выполняем команду: Net start wmsvc

Настройка привязки (Bindings)

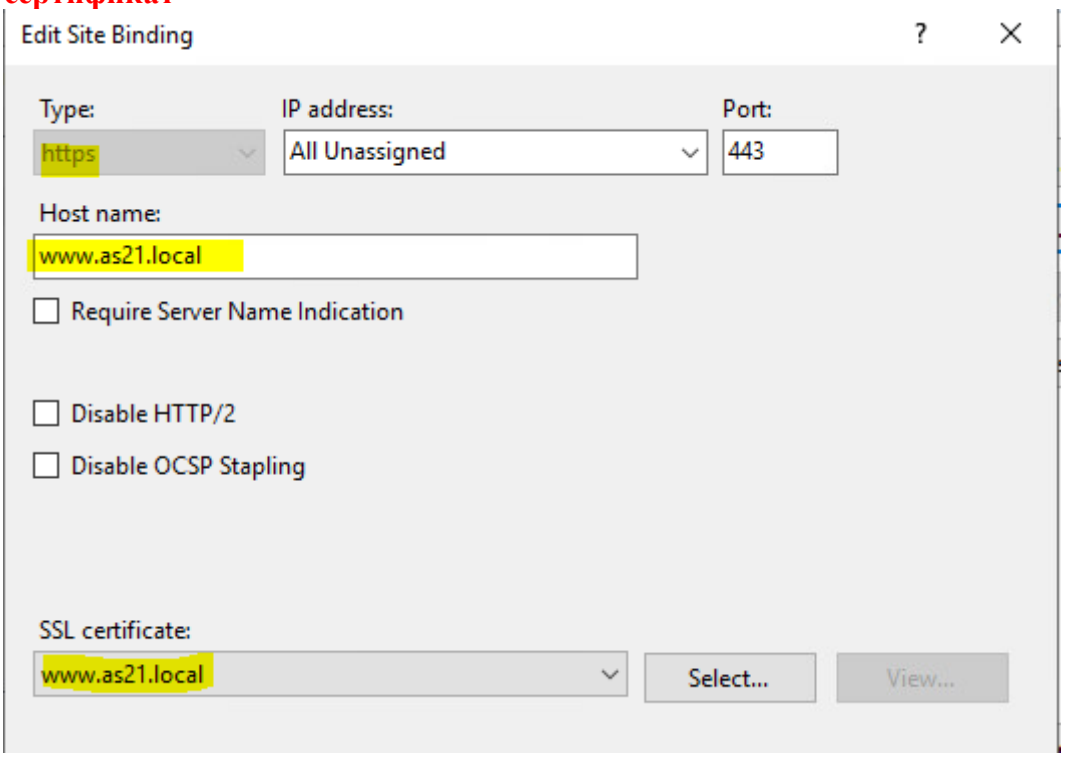
Открываем сайт и справа нажимаем Bindings

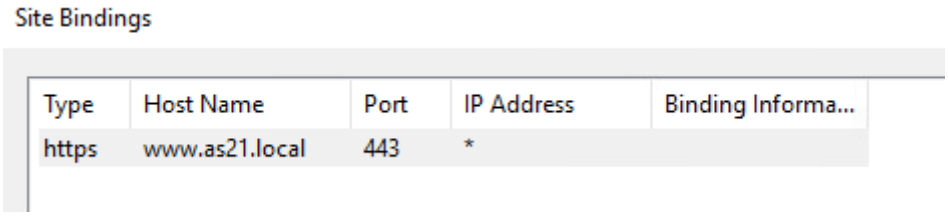


Удаляем имеющуюся там привязку по http



Добавляем привязку по https, вписываем имя сайта www.as21.local и выбираем наш сертификат

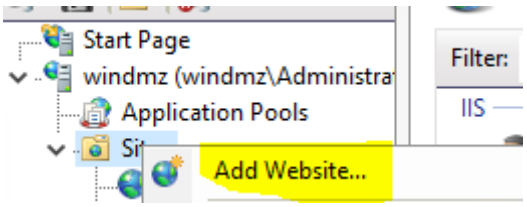




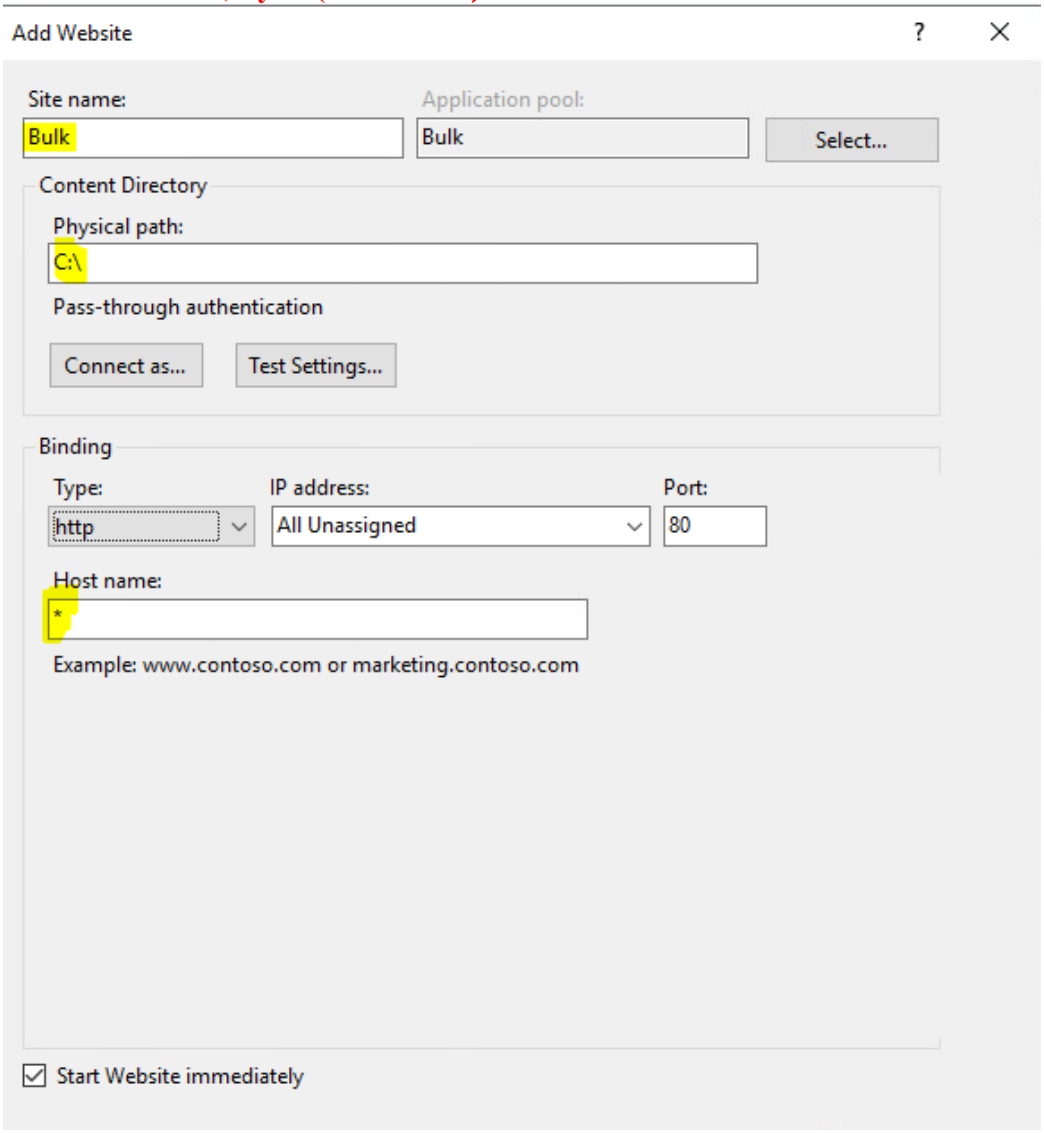
Перенаправление с http на https

Создадим перенаправление с http на https. Для этого заходим в HTTP Redirect

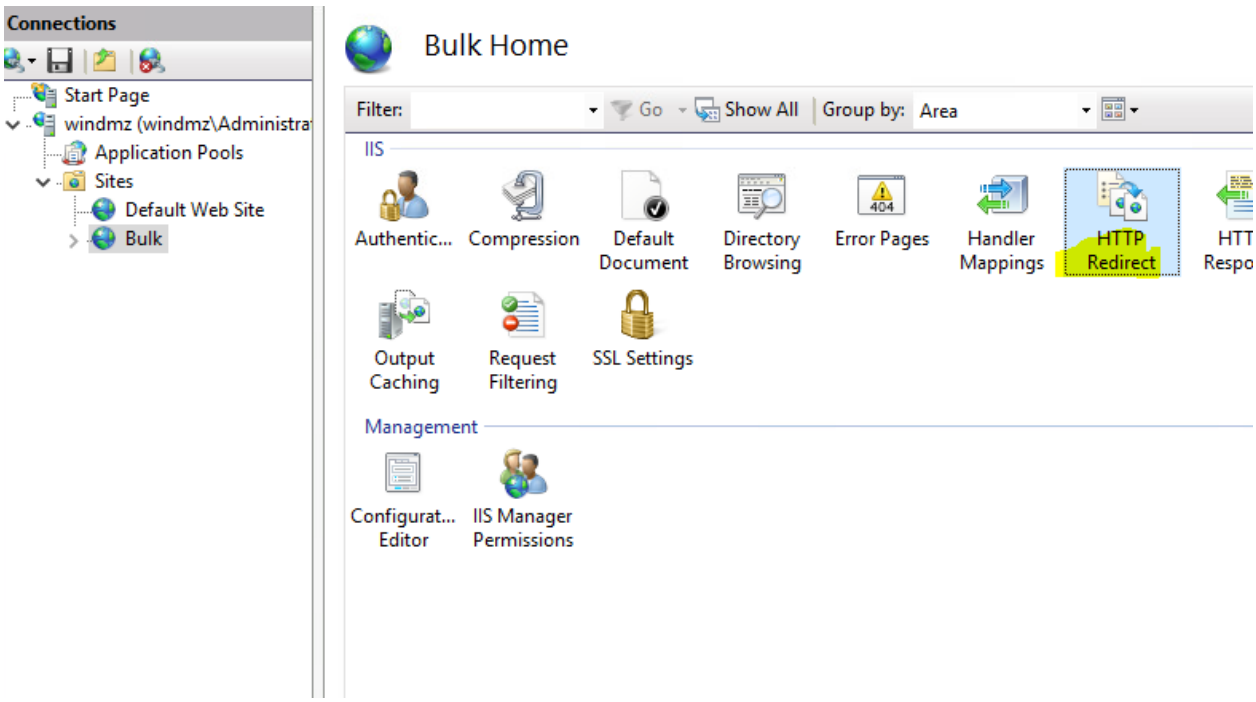
Создадим сайт-заглушку



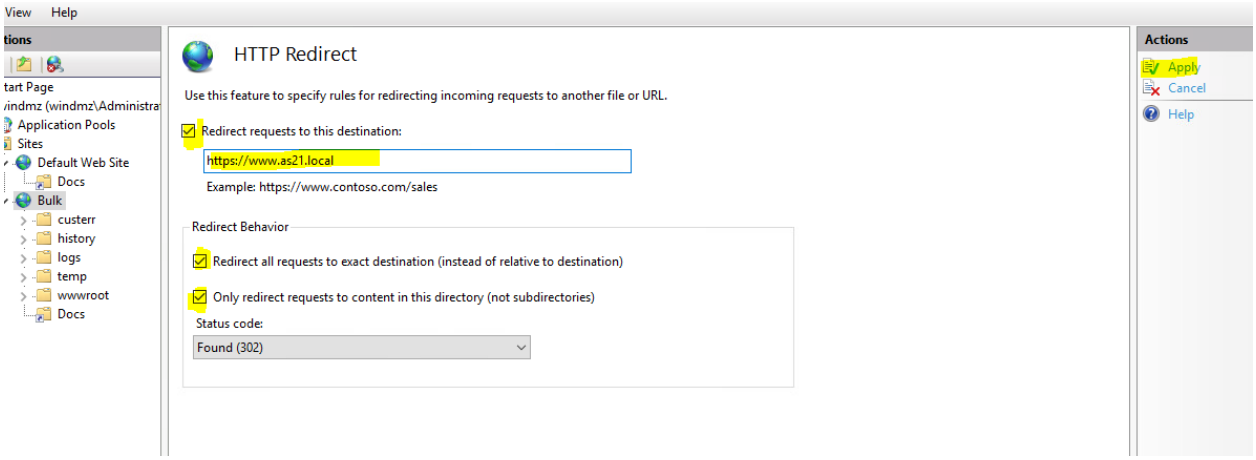
Задаем его имя, путь (можно C:\) и Host name пишем *



В настройках НОВОГО сайта заглушки идем в HTTP Redirect



Прописываем пункт назначения переадресации https:\\www.as21.local
Включаем Only redirect requests to contene in the directory и Redirect all requests to exact destination. Нажимаем Apply

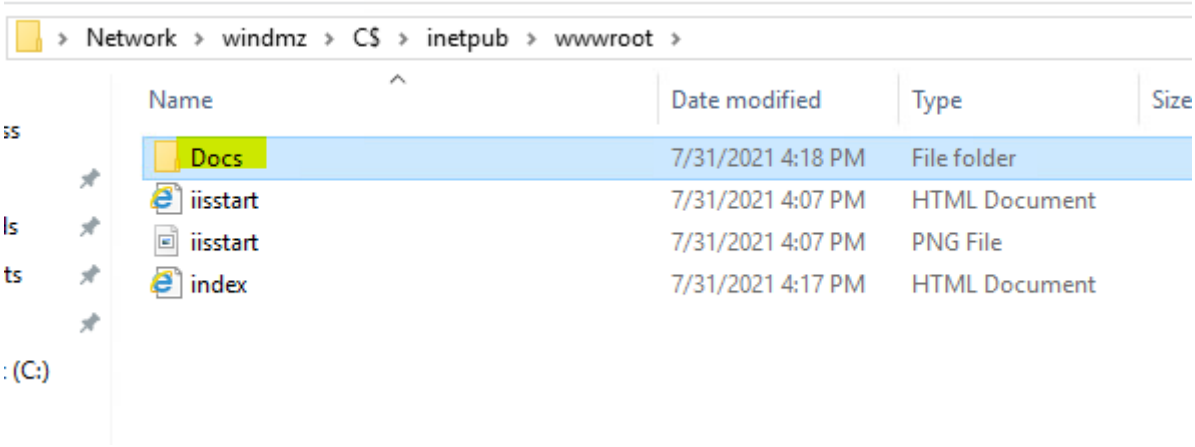


ВАЖНО!!! Больше сайт заглушка нам не нужен! Все остальные операции делаются на основном сайте

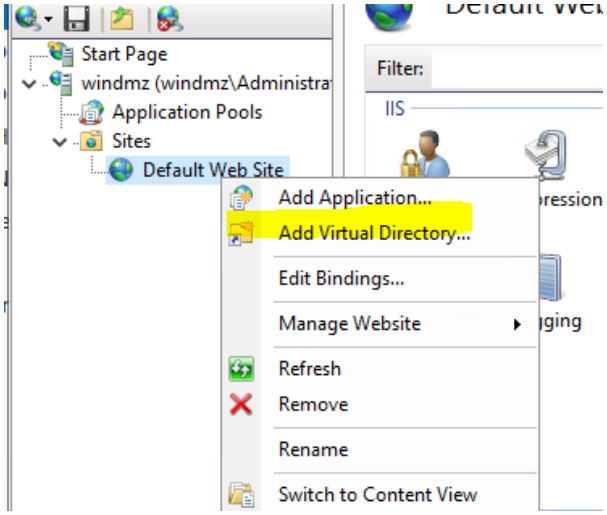
Виртуальный каталог Docs

Внутри сайта создайте виртуальный каталог Docs. Поместите в него текстовый файл Test.txt. Включите возможность обзора содержимого каталога при подключении к нему пользователей через браузер.

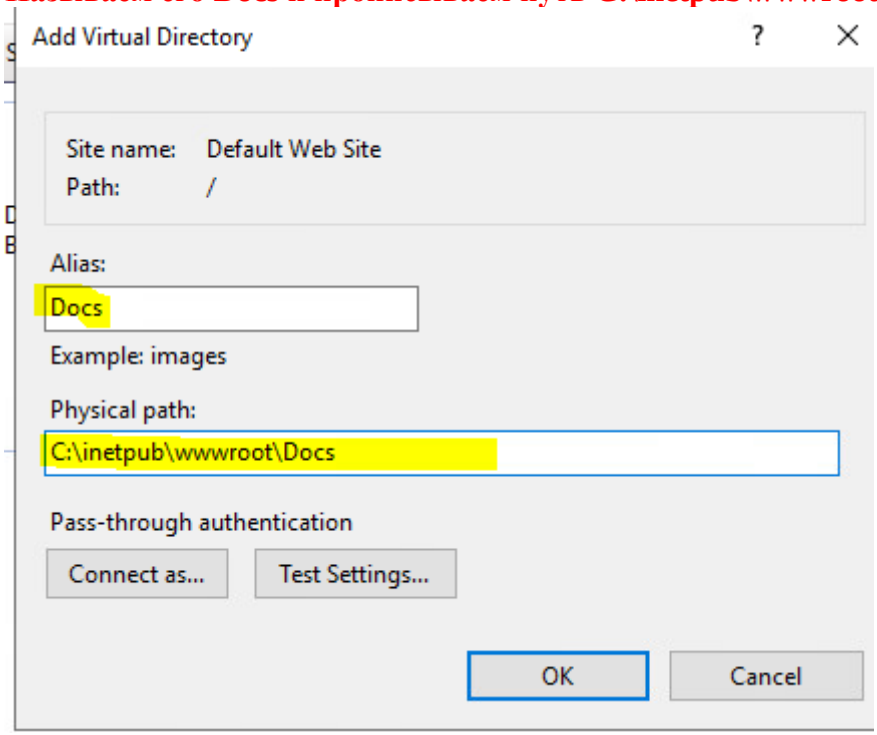
Создаем на WINDMZ папку C:\inetpub\wwwroot\Docs\ (её можно создать через подключение по \\WINDMZ\C$) и создаем в ней файл Test.txt

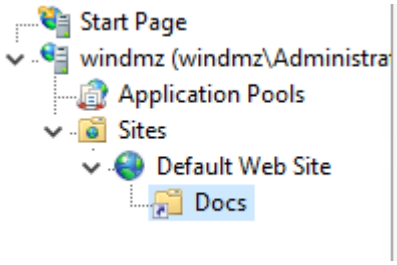


Нажимаем правую кнопку на сайте и выбираем Add Virtual Directory

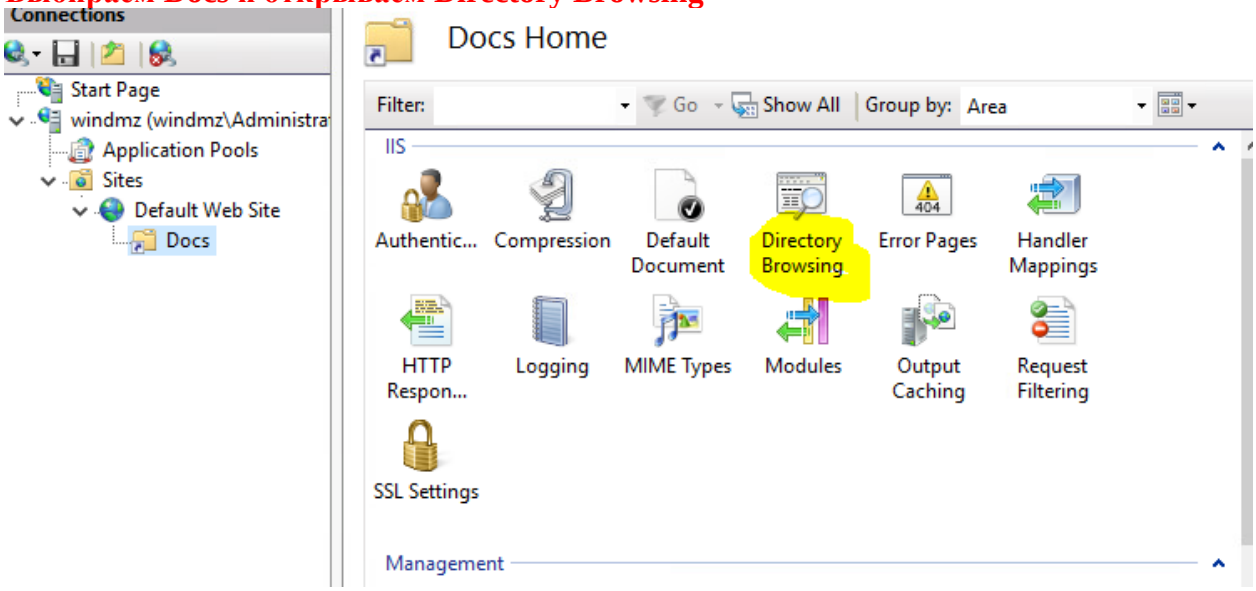


Называем его Docs и прописываем путь C:\inetpub\wwwroot\Docs

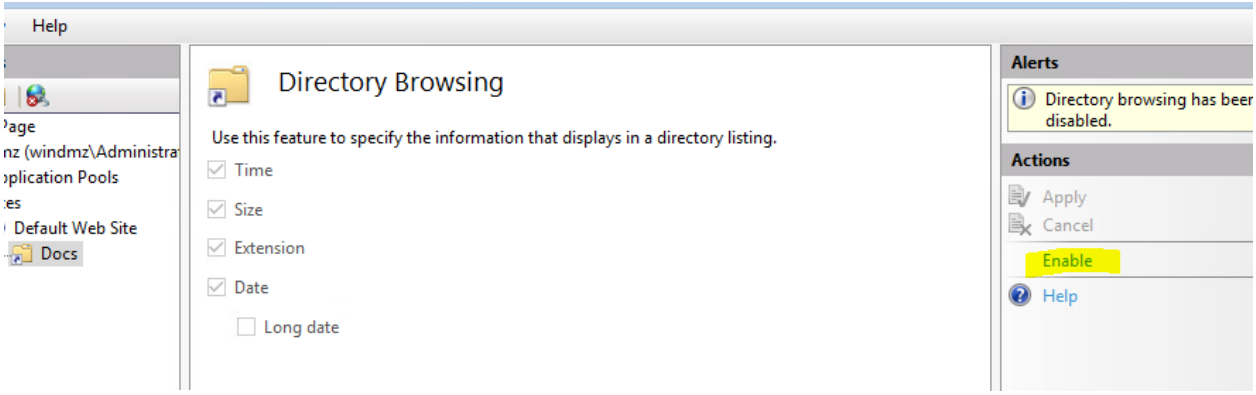


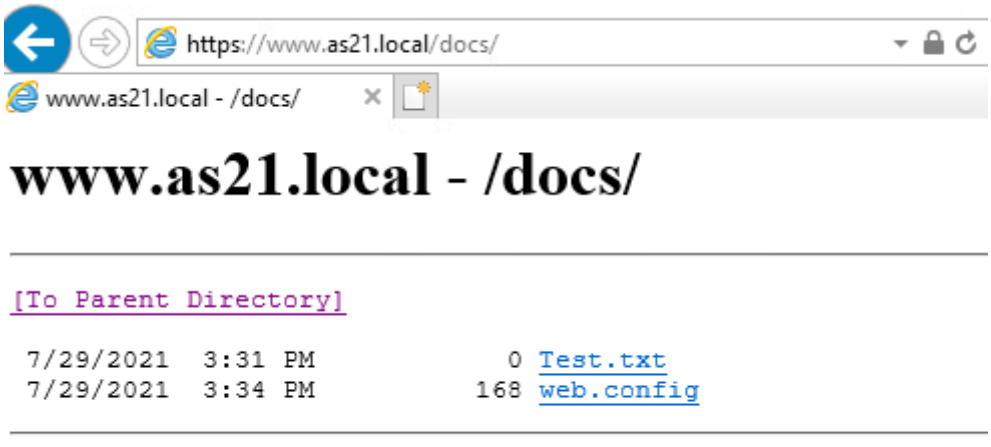


Выбираем Docs и открываем Directory Browsing



Нажимаем Enable



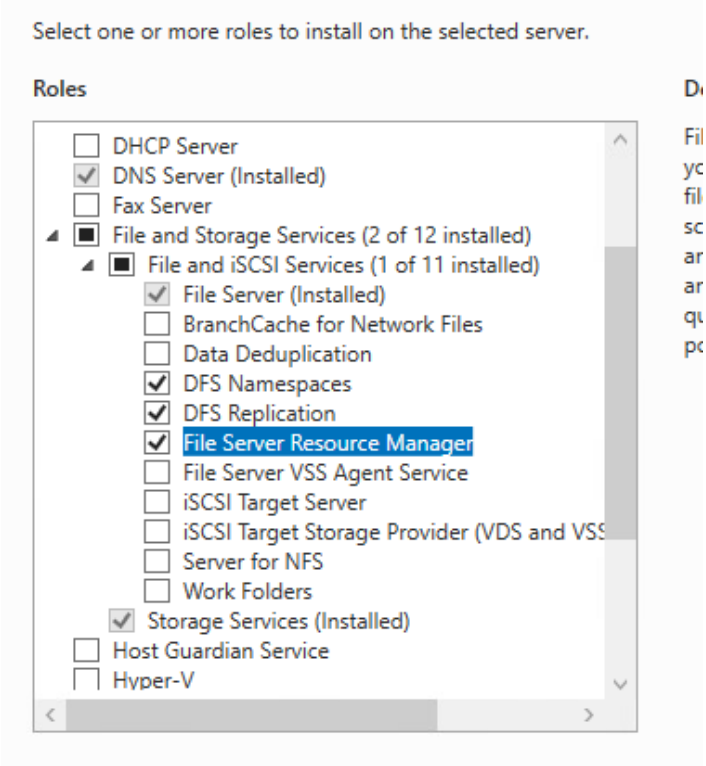


Настройка файловых служб на ЦОД (WINSRV1 и WINSRV2)

Настройка DFS

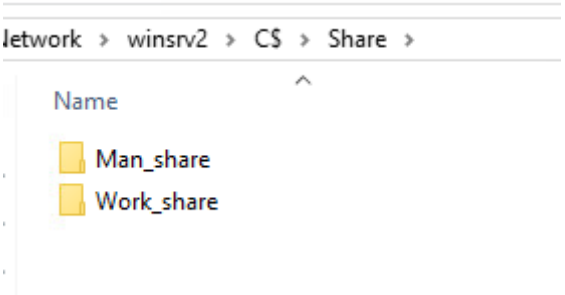
На серверах WINSRV1 и WINSRV2 установите соответствующие роли для организации распределенной файловой системы.

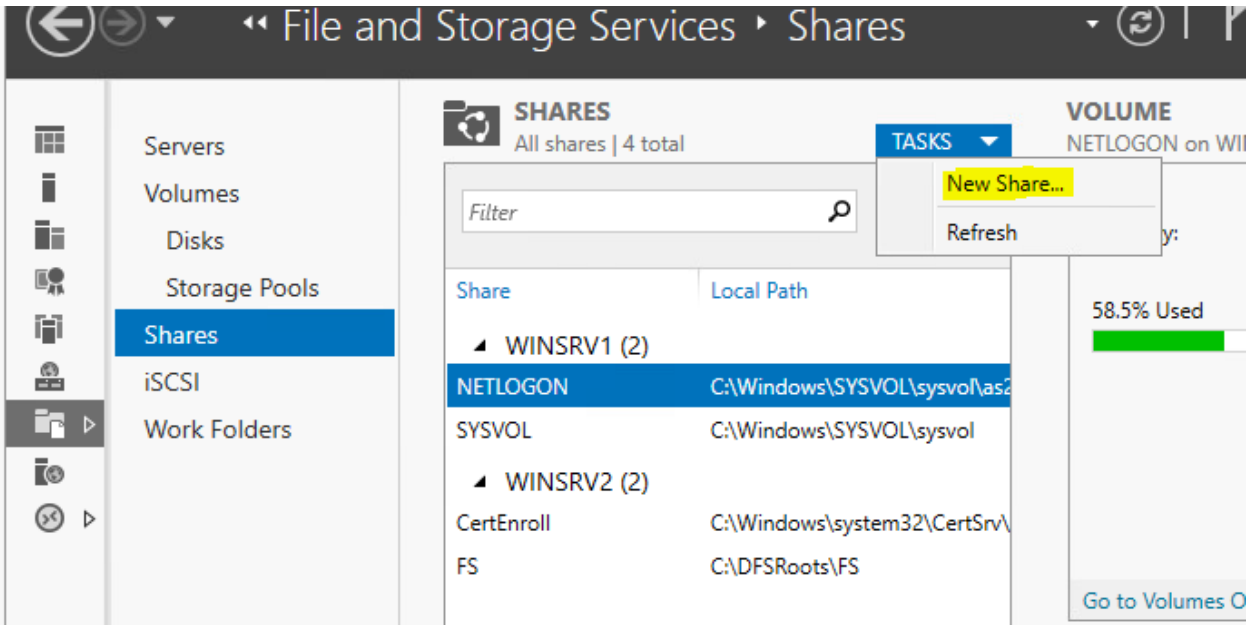
Заходим на WINSRV2 и через сервер менеджер ставим 3 службы на WINSRV1 и WINSRV2

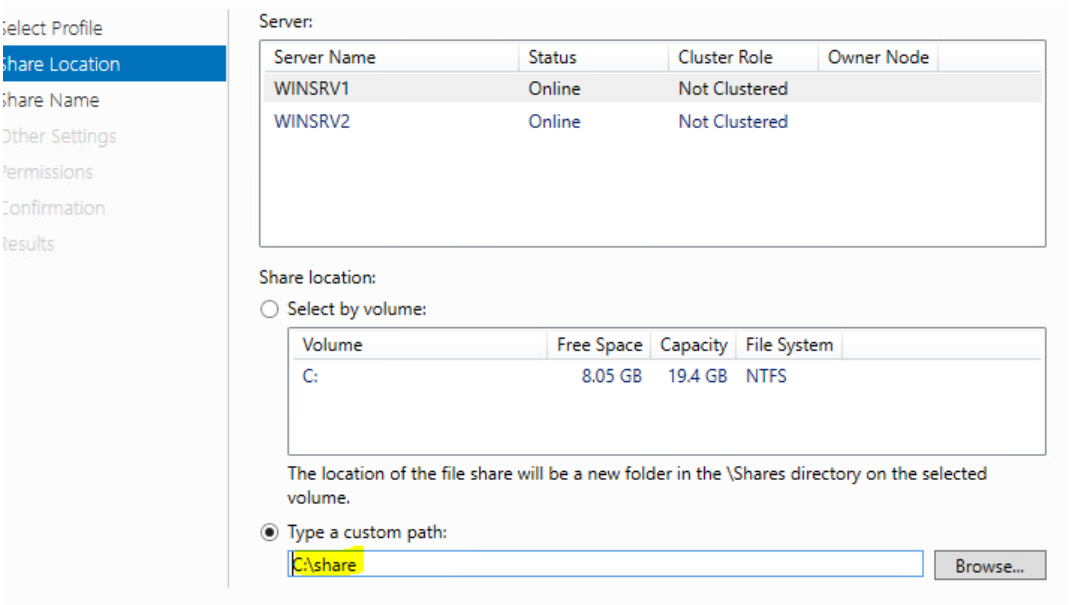


Создайте папку C:\Share на сервере WINSRV1 и папку C:\Share на сервере WINSRV2. Внутри созданных папок создайте папки Man_share и Work_share. Создайте корень DFS с именем FS. Данный корень должен поддерживаться обоими серверами. Создайте под этим корнем папку с именем Share, ссылающуюся на сетевые директории с тем же именем (Share) созданные вами ранее на каждом сервере. Обеспечьте членам группы Group1 доступ к этой папке на запись. Настройте репликацию между папками средствами DFS.

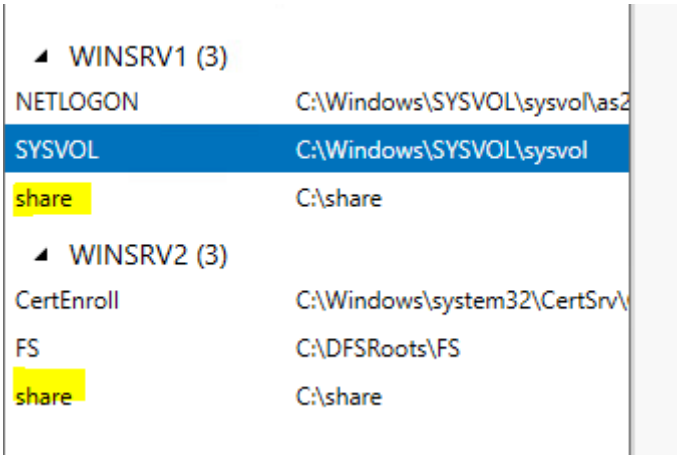
На WINSRV2 создаем нужные папки.



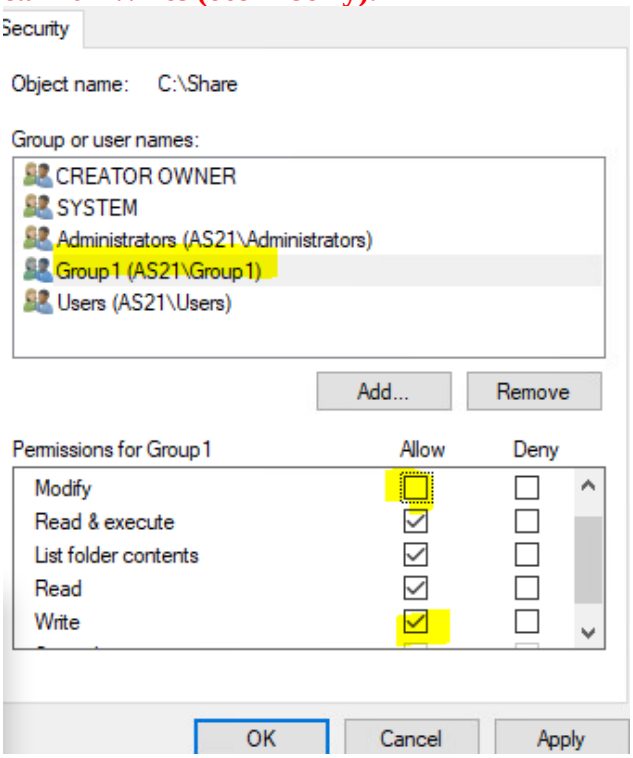




На обоих серверах сделайте общую папку Share (напоминание Shared Permissions – Everyone Full Control). Если делать как описано ниже, права Shared Permissions будут правильные

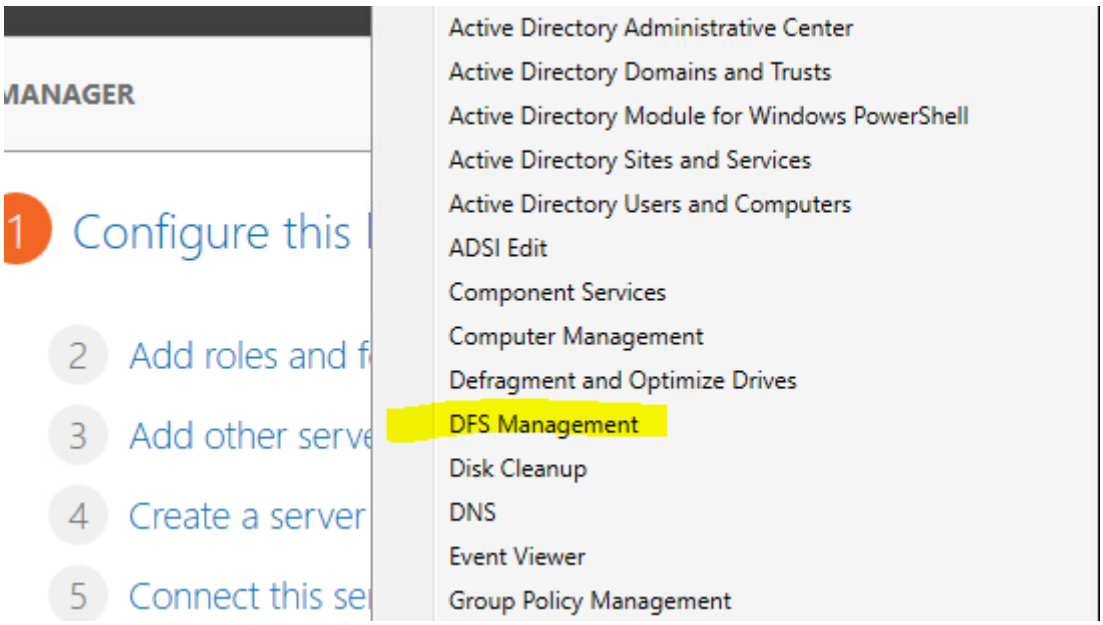


Теперь нужно добавить NTFS разрешения записи на папку Share. Именно на запись Write (без Modify).

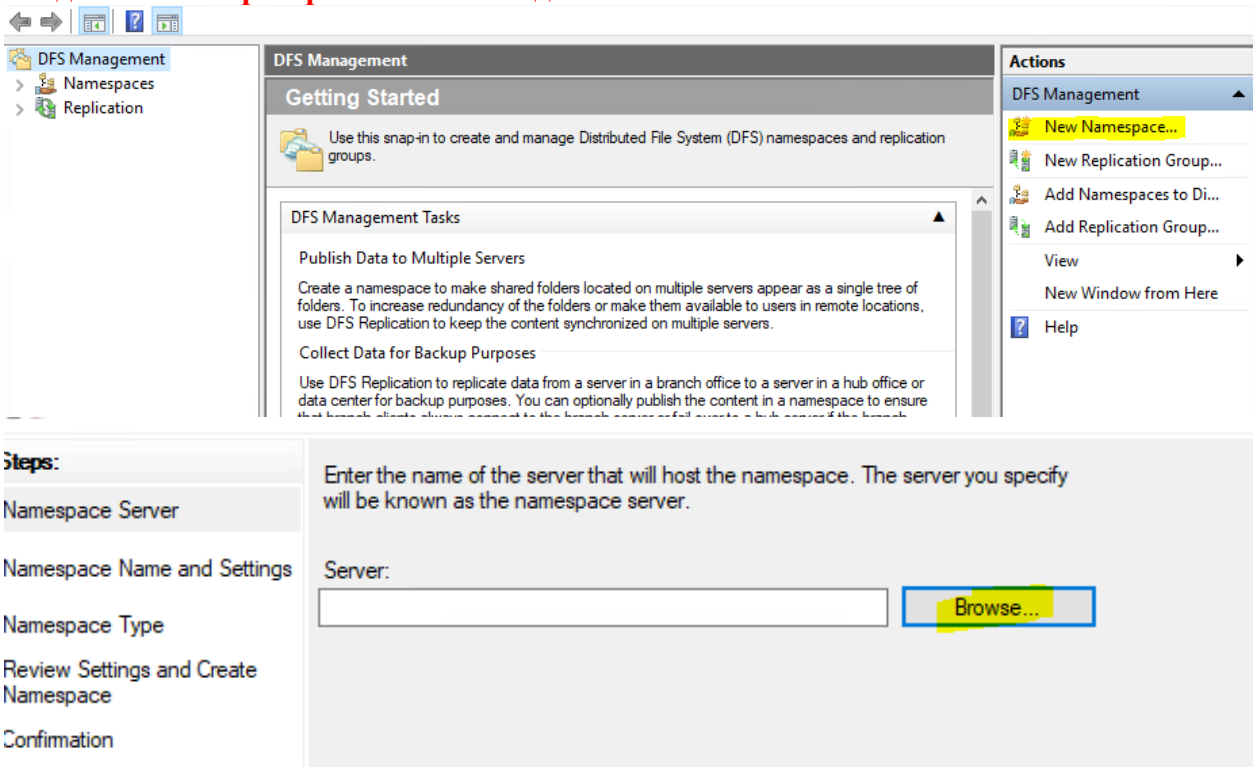


ВАЖНО!!! Проделать эти действия на WINSRV1 и WINSRV2

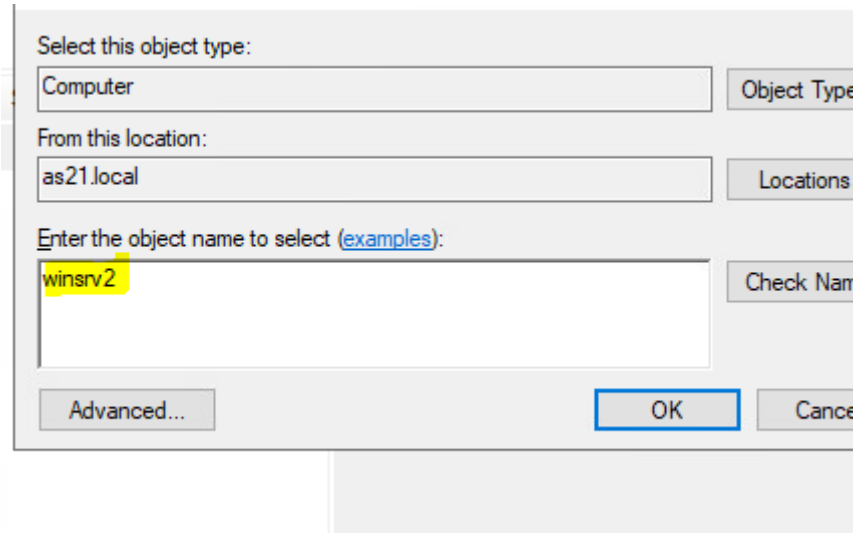
Настраиваем DFS. Заходим на WINSRV2. Открываем консоль DFS Management



Создаем новое пространство имен в домене

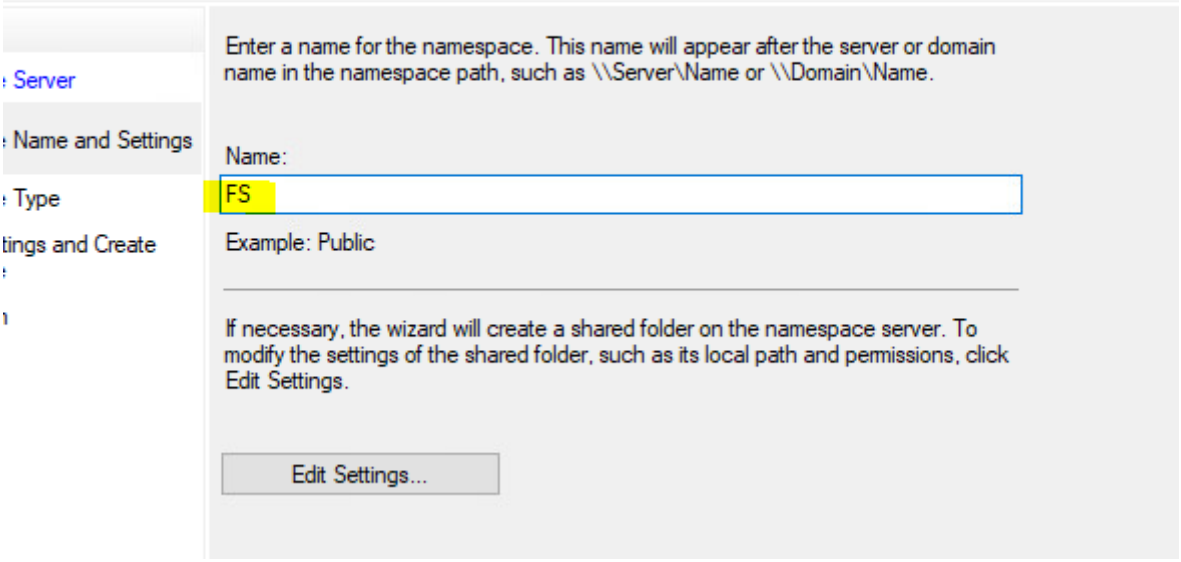


Выбираем первый сервер (можно выбрать WINSRV2)

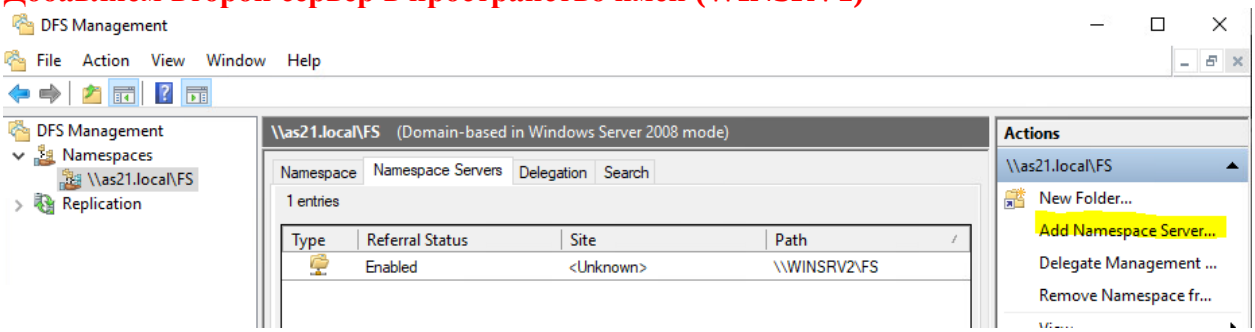


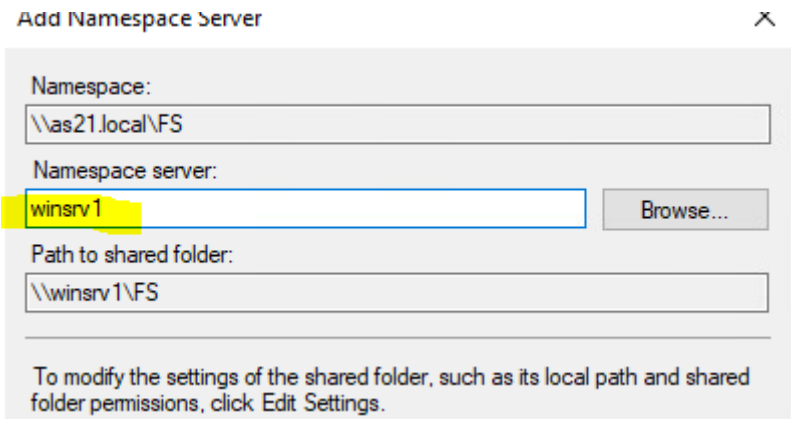
Выбираем имя FS на для нашего DFS

Namespace Name and Settings

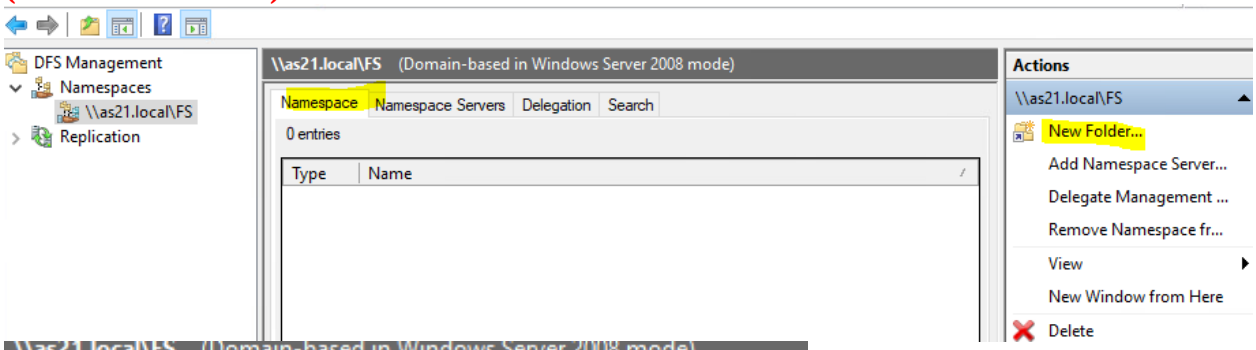


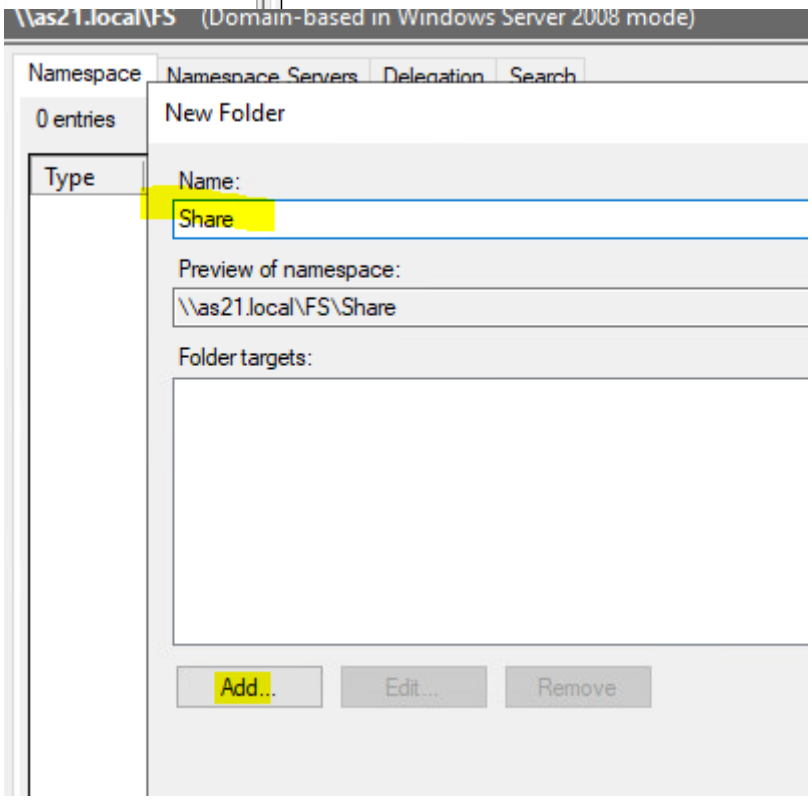
Добавляем второй сервер в пространство имен (WINSRV1)

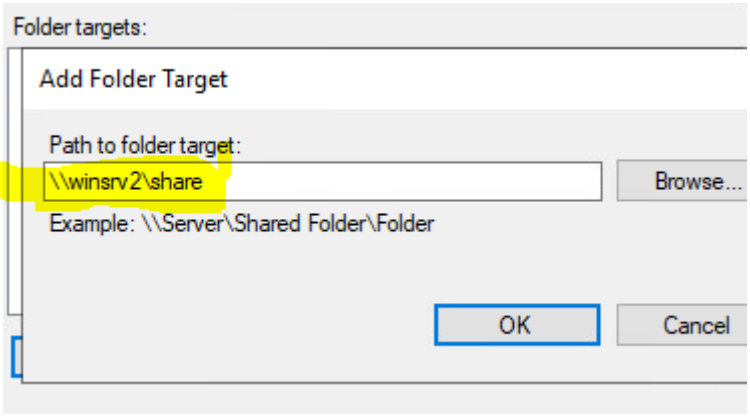




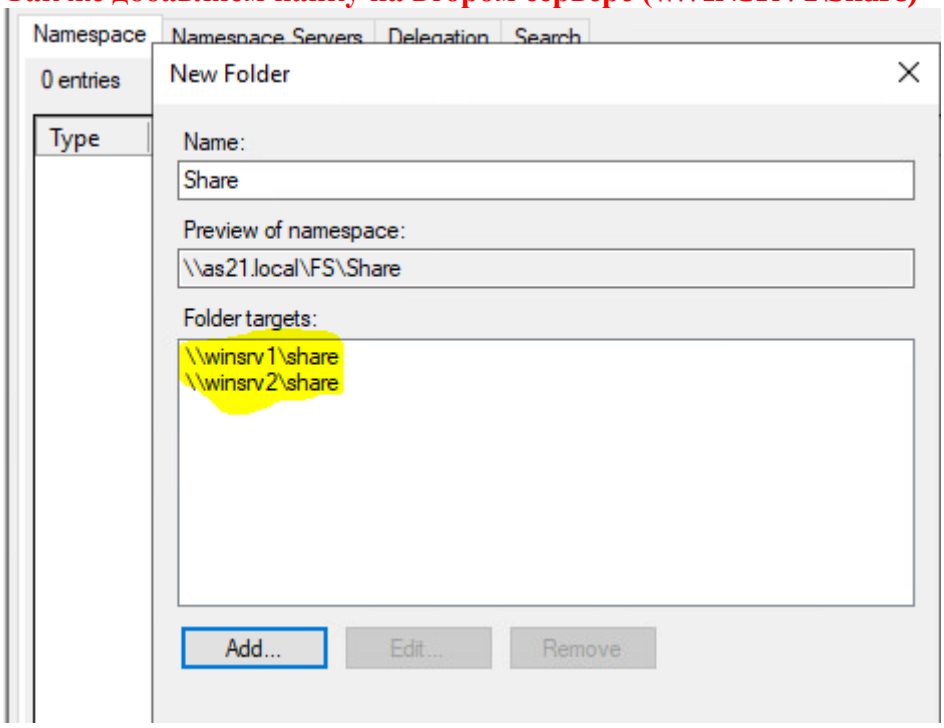
Добавляем папку для репликации. Указываем путь формата \\сервер\папка (\\WINSRV2\Share)



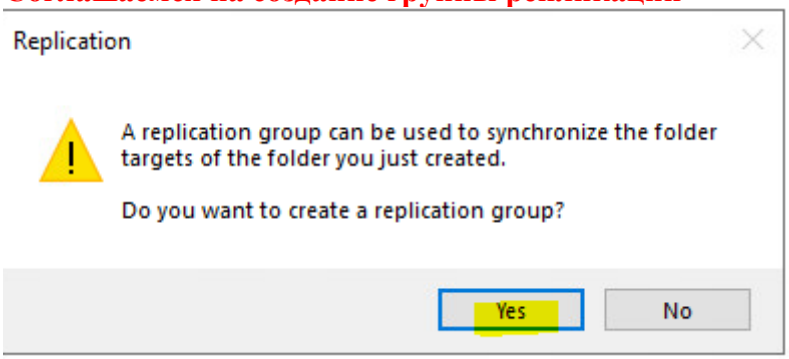




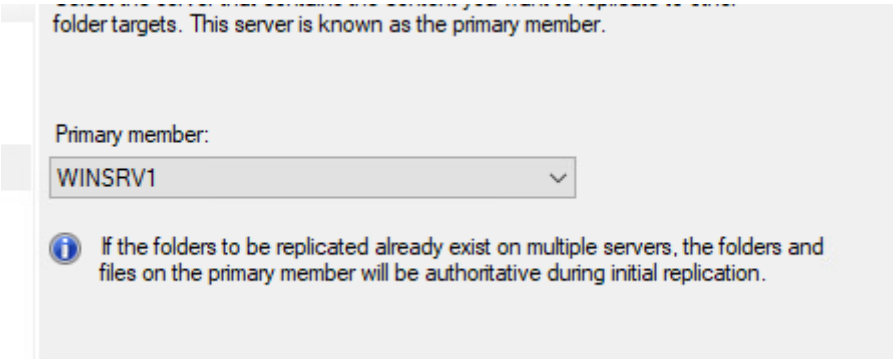
Так же добавляем папку на втором сервере (\\WINSRV1\Share)



Соглашаемся на создание группы репликации



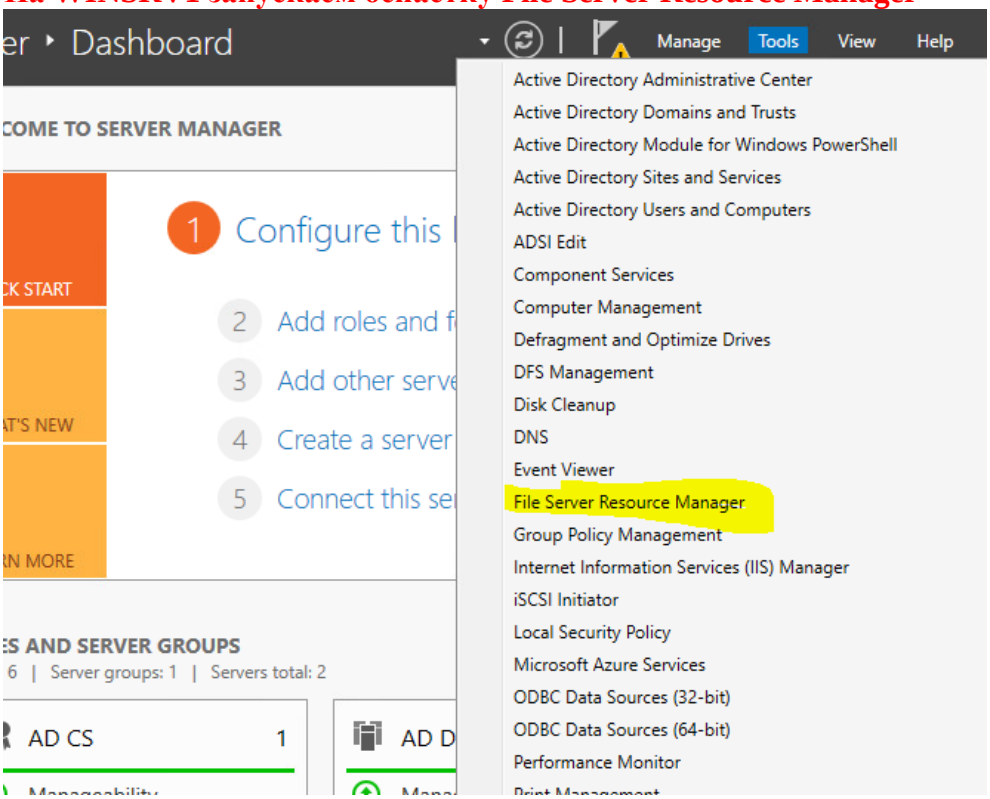
Там везде «Next» (нас все устраивает). В последнем вопросе выбираем главный сервер для репликации – WINSRV1



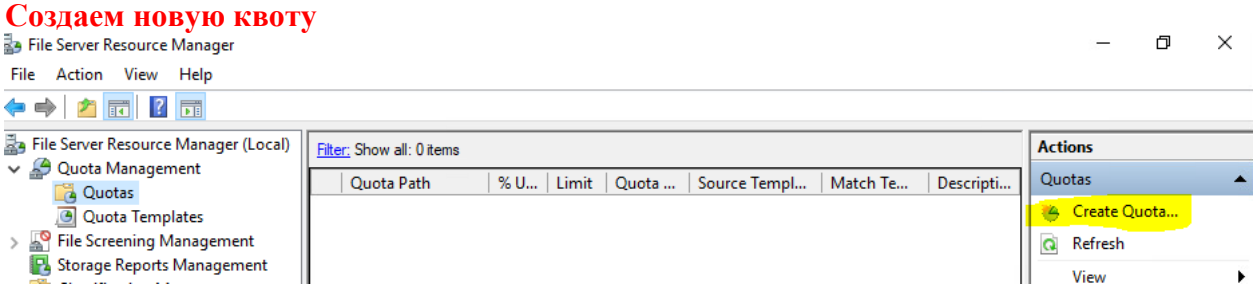
Настройка квот

Установите жесткое ограничение 1Гб на размер папки FS\Share.

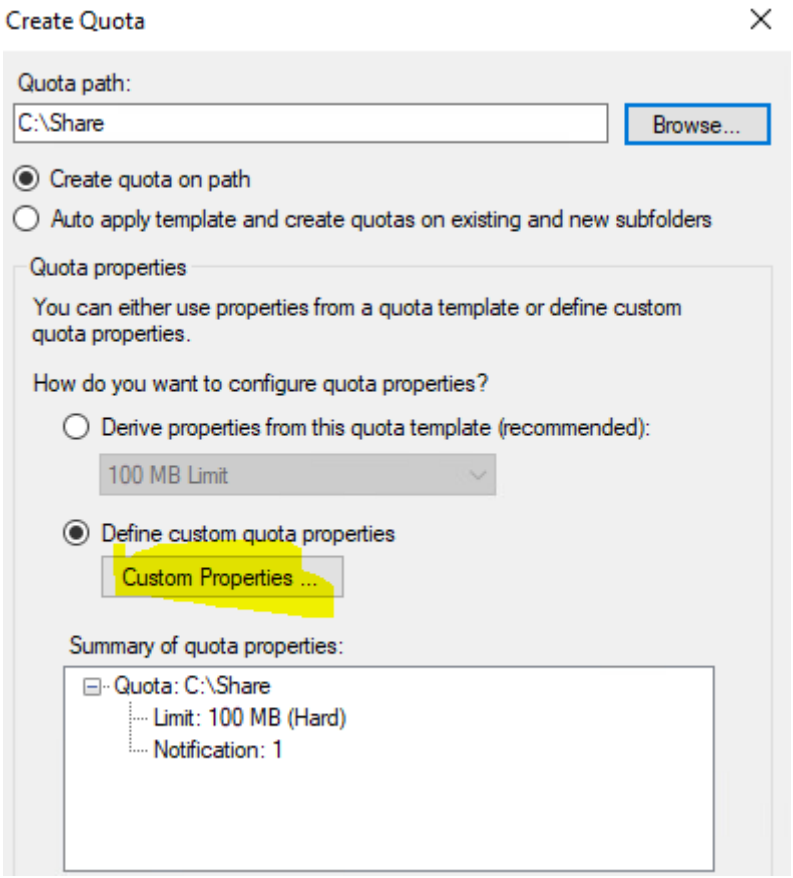
На WINSRV1 запускаем оснастку File Server Resource Manager



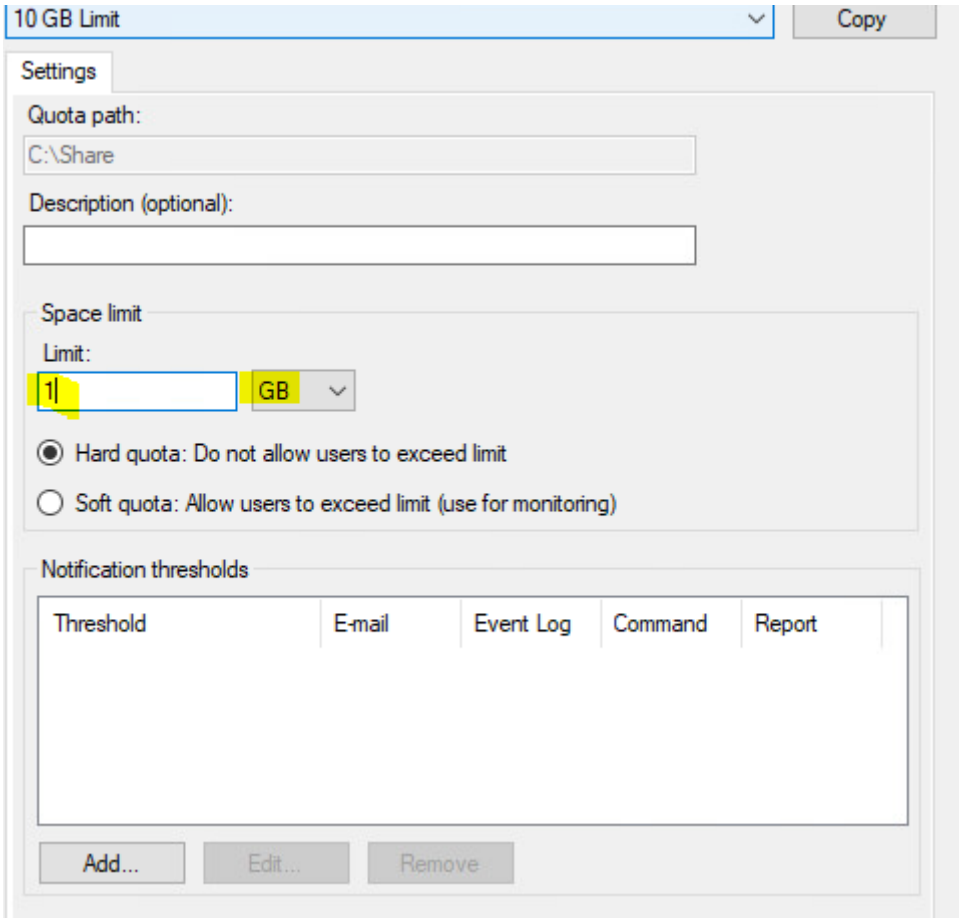
Создаем новую квоту



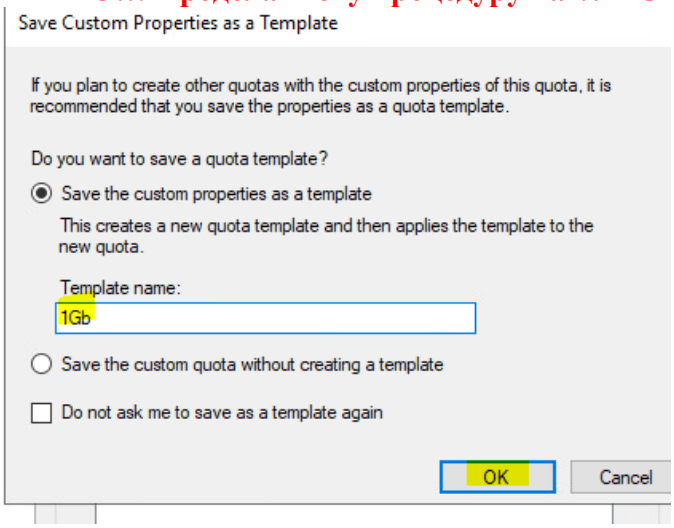
Прописываем путь квоты. Наша папка C:\Share. Так как квота в 1Gb не является стандартной, то нажимаем Custom Properties



Выбираем лимит в 1Gb для квоты



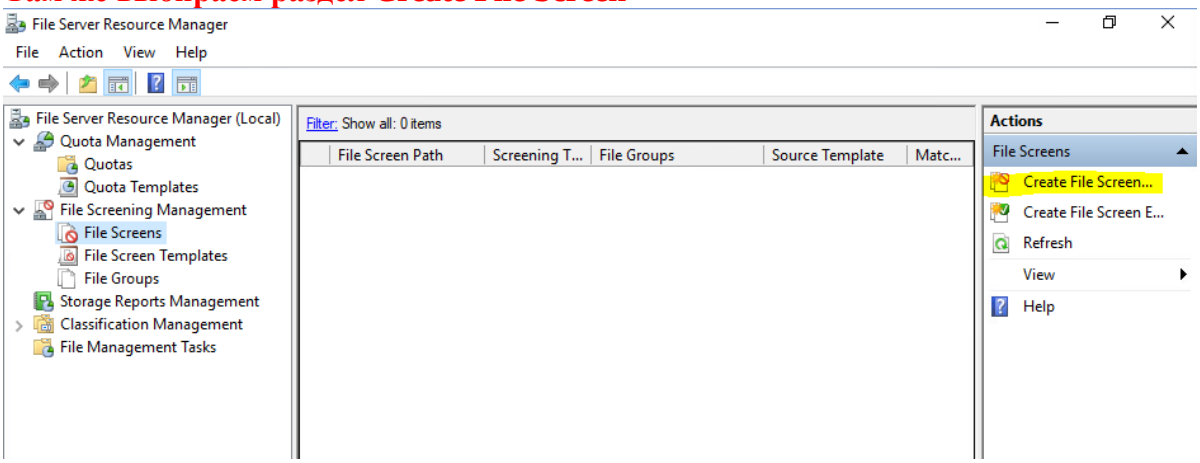
Сохраняем шаблон для нашей квоты и саму квоту.
ВАЖНО!!! Проделать эту процедуру на WINSRV1 и WINSRV2



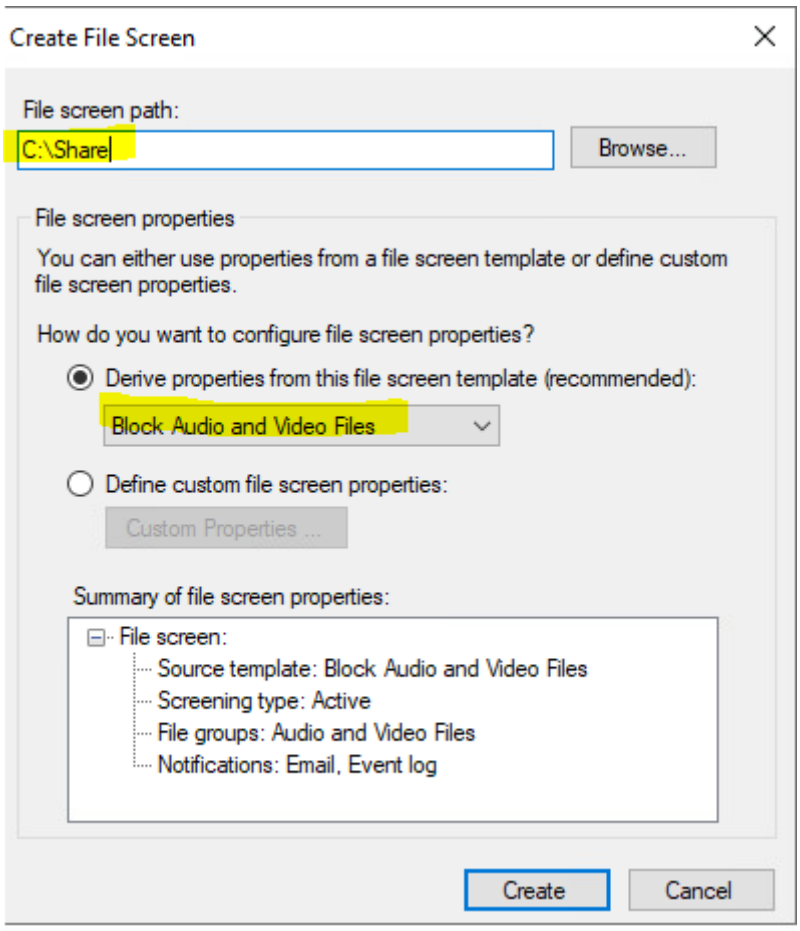
Настройка запрета на хранение файлов

Запретите хранение аудио- и видео-файлов в папках C:\Share на серверах WINSRV1 и WINSRV2.

Там же выбираем раздел Create File Screen



Там же выбираем раздел Create File Screen. Прописываем путь к папке (C:\Share\). Свойства квоты должны быть – Block Audio and Video Files. Создаем квоту

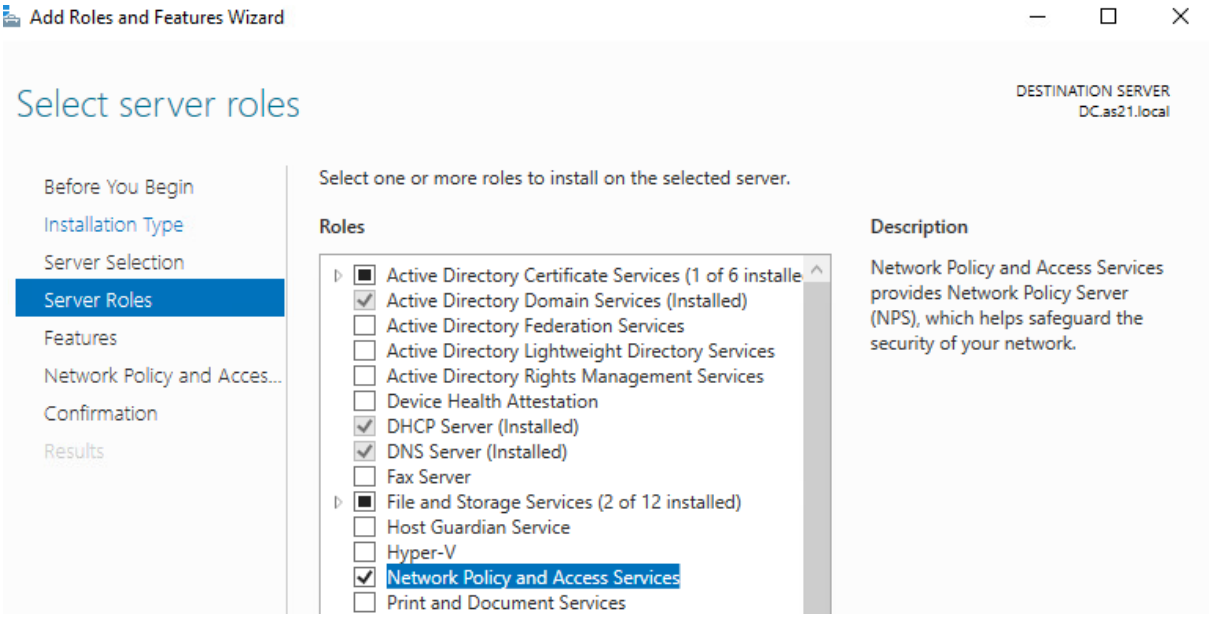


ВАЖНО!!! Проделать эту процедуру на WINSRV1 и WINSRV2

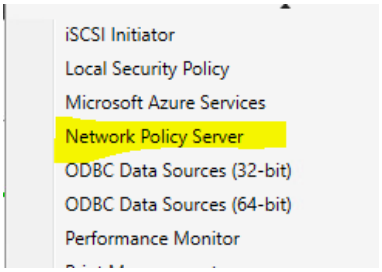
10. На всех компьютерах под управлением ОС Microsoft Windows обеспечьте функционирование Defender Firewall. При этом работоспособность настроенных ранее сервисов не должна нарушиться.

Настройка NPS

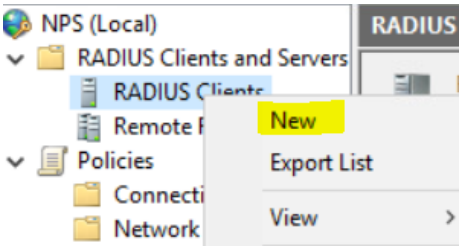
Настройка политики



Запускаем остнастку Network Policy Server



В остнастке NPS идем в RADIUS Clients and Servers > RADIUS Clients -> New

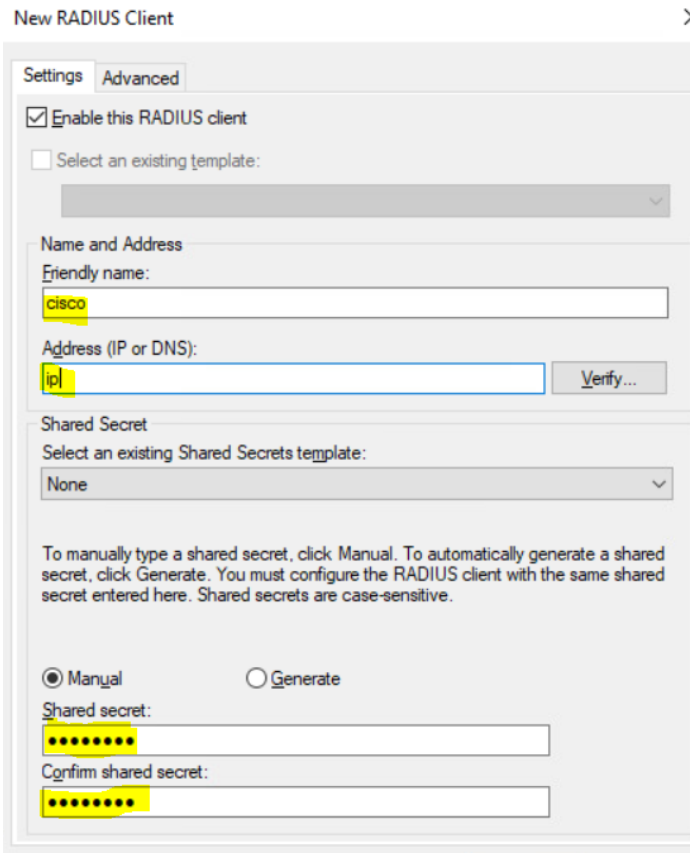


Вводим:

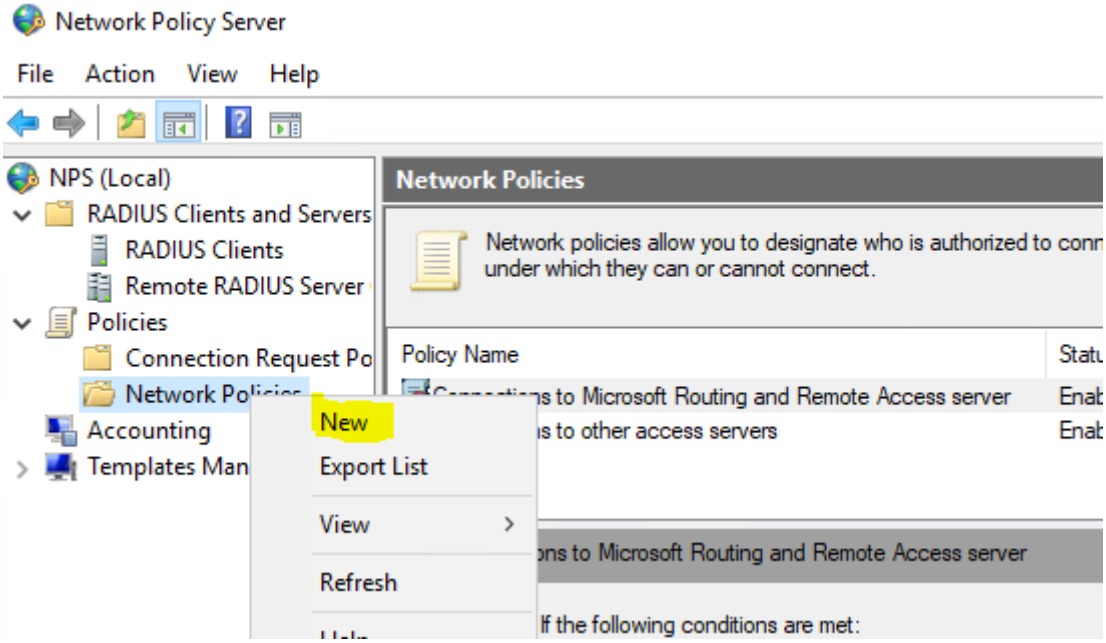
Friendly name – Cisco

Address (IP or DNS) – ip адрес устройства

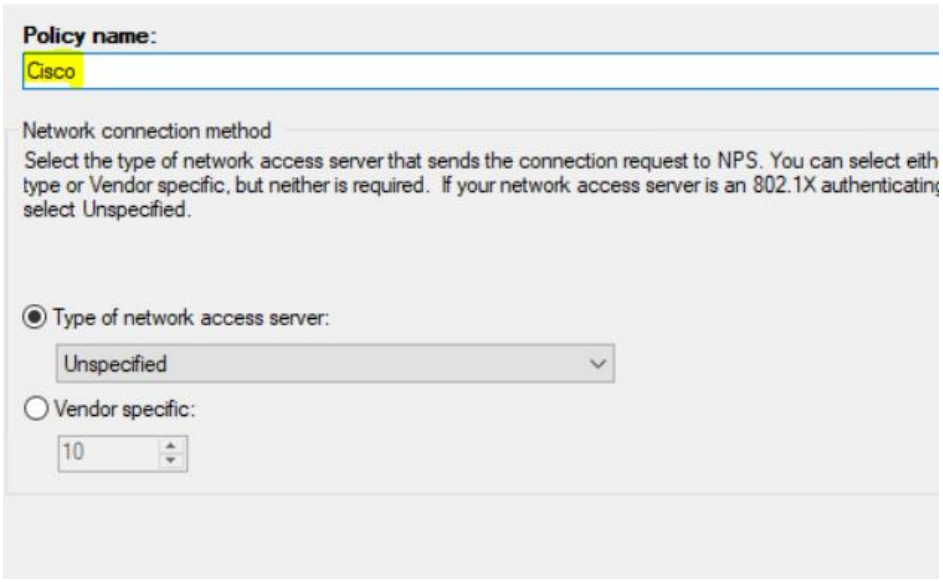
Shared Secret – произвольный паролль, который нужно прописать в устройстве



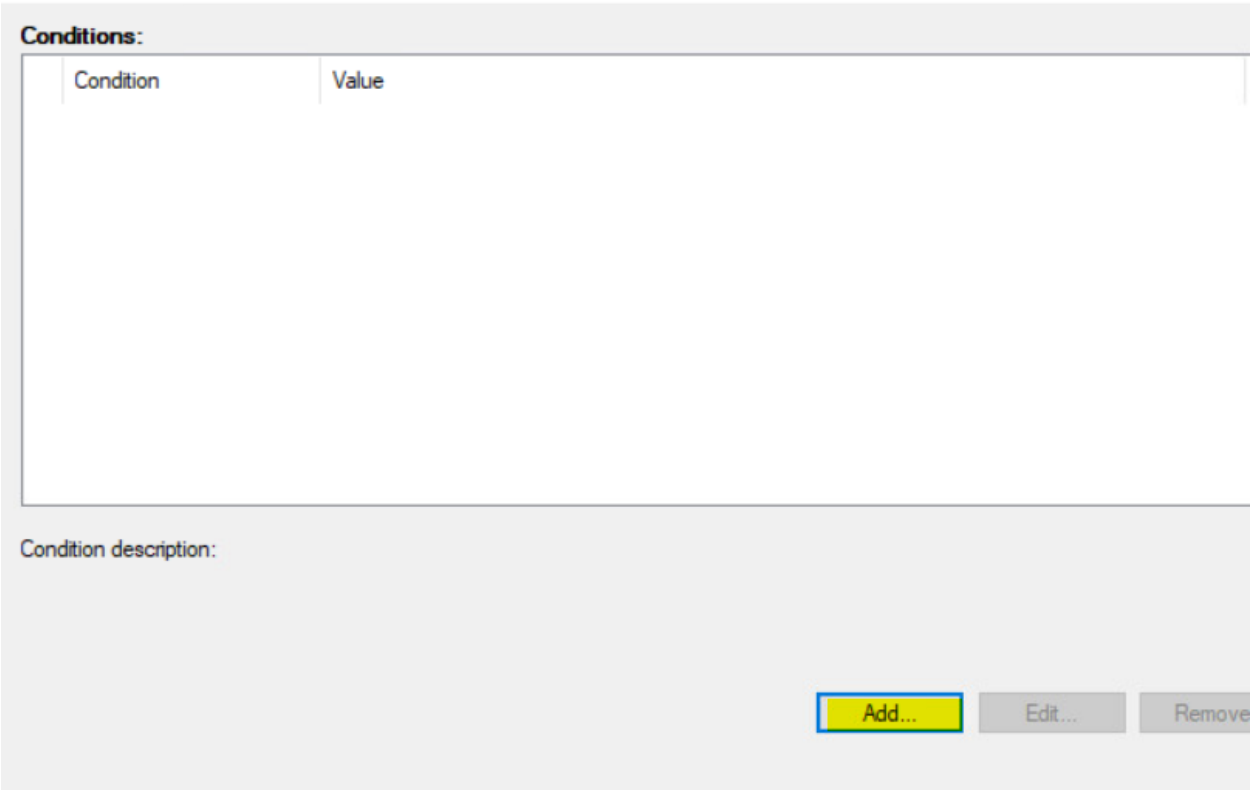
Идем в Policies > Network Policies -> New



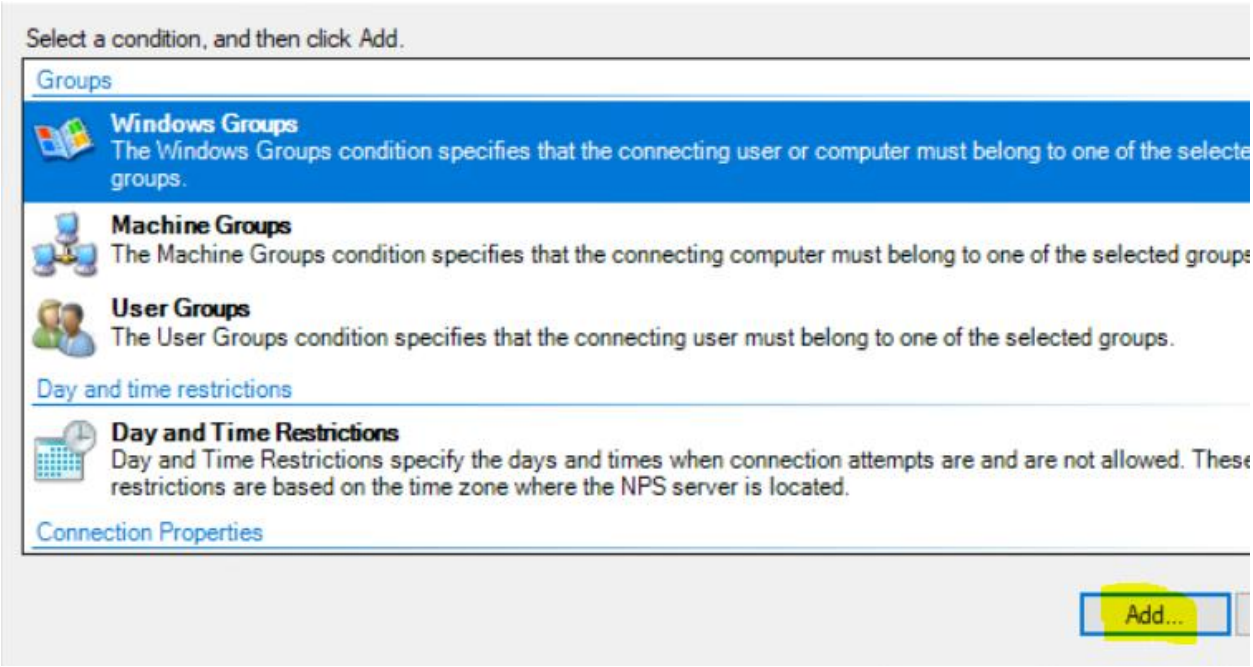
Создаем новую политику. Вводим имя политики



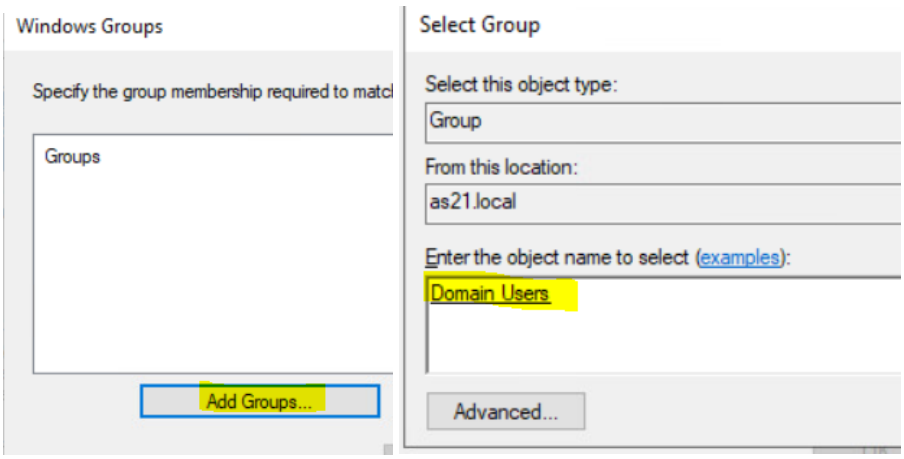
Добавляем условия срабатывания



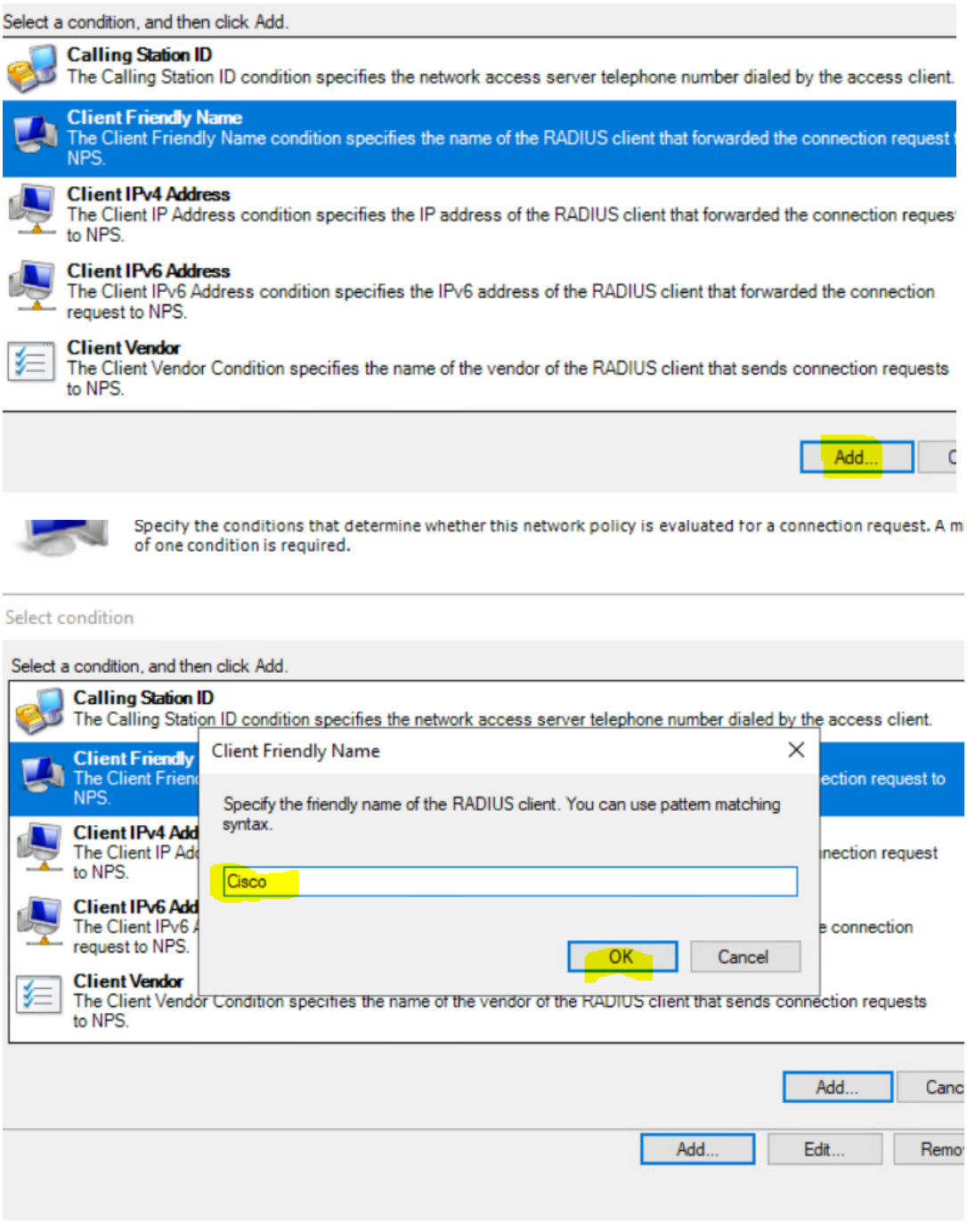
Windows Group (группа безопасности из Active Directory)



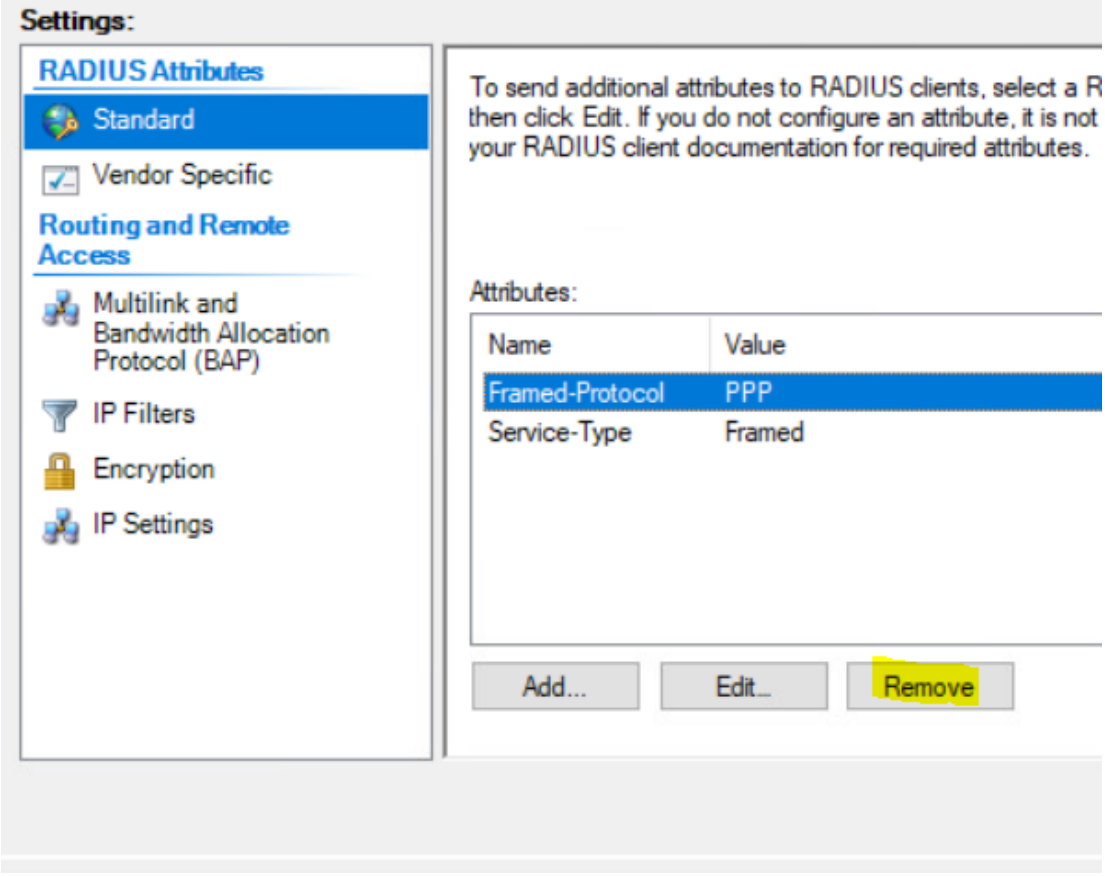
Добавляем группу безопасности (Domain Users)



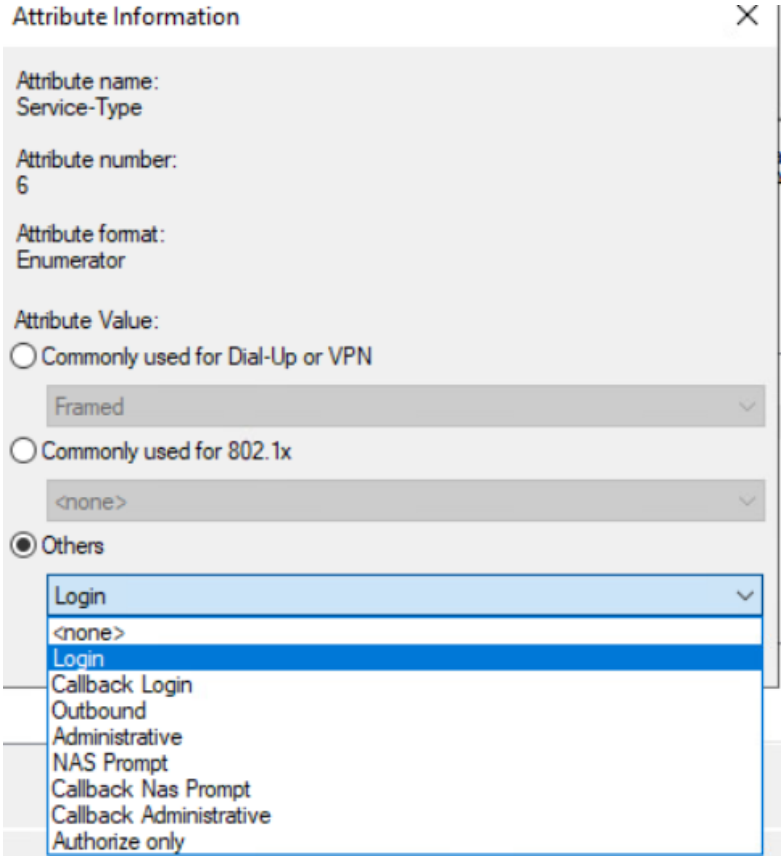
Указываем имя Radius клиента, настроенного ранее (в нашем случае будет Cisco)

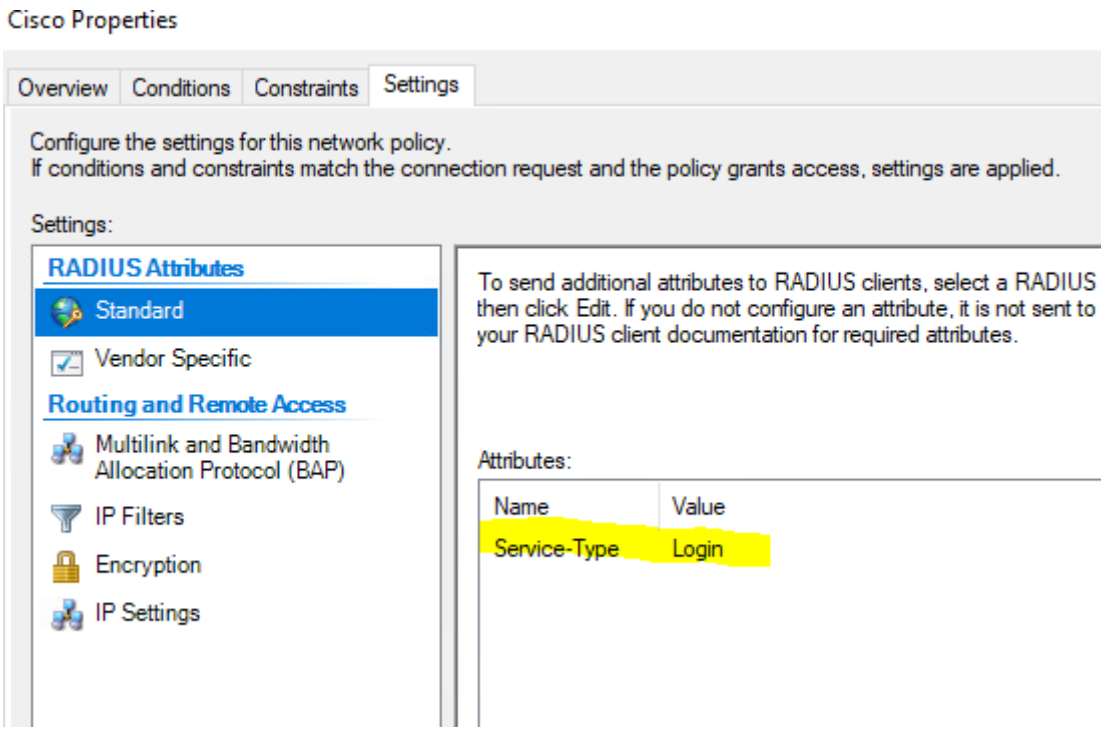


Убираем стандартную настройку Framed-Protocol = PPP

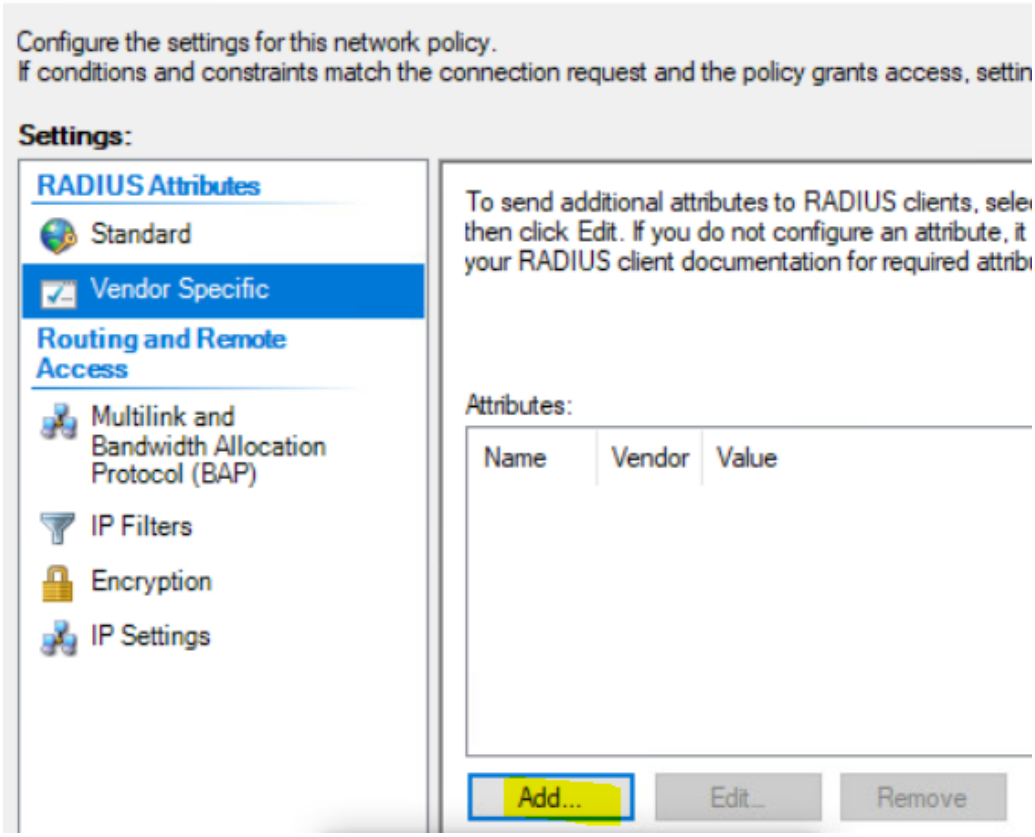


И меняем Service-Type = Framed на Login



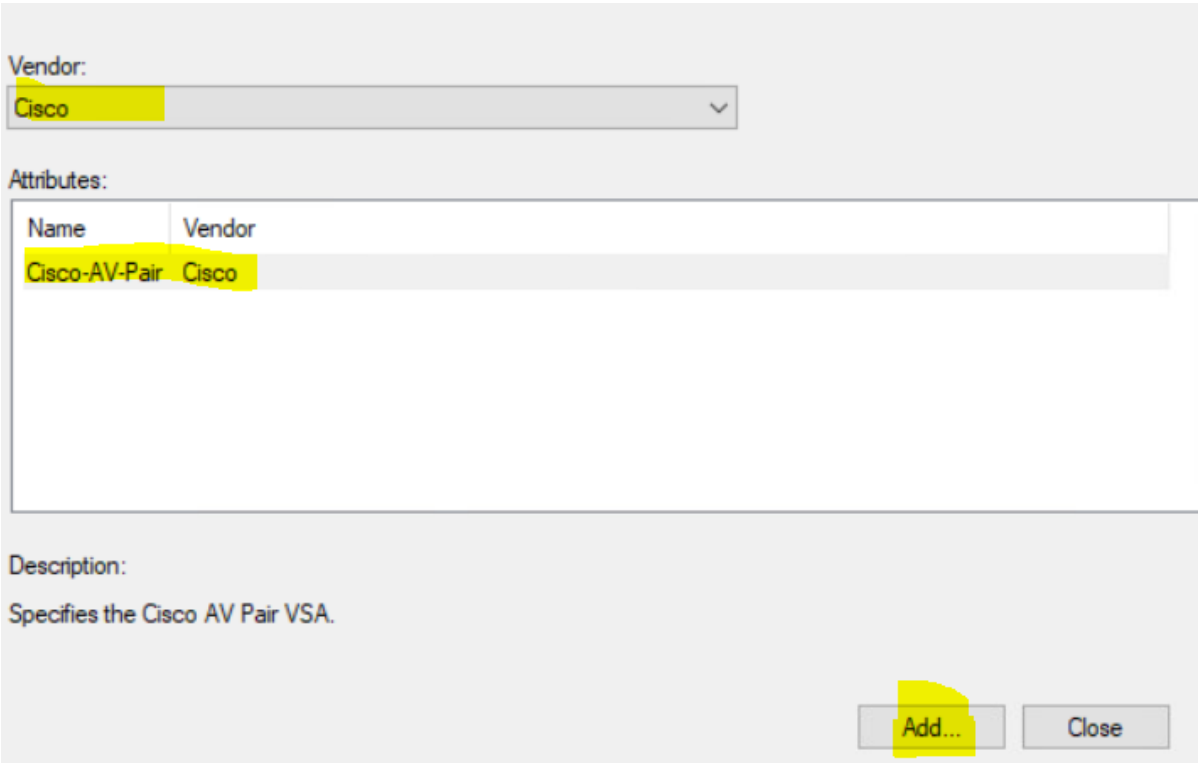


В разделе Vendor Specific добавляем атрибут

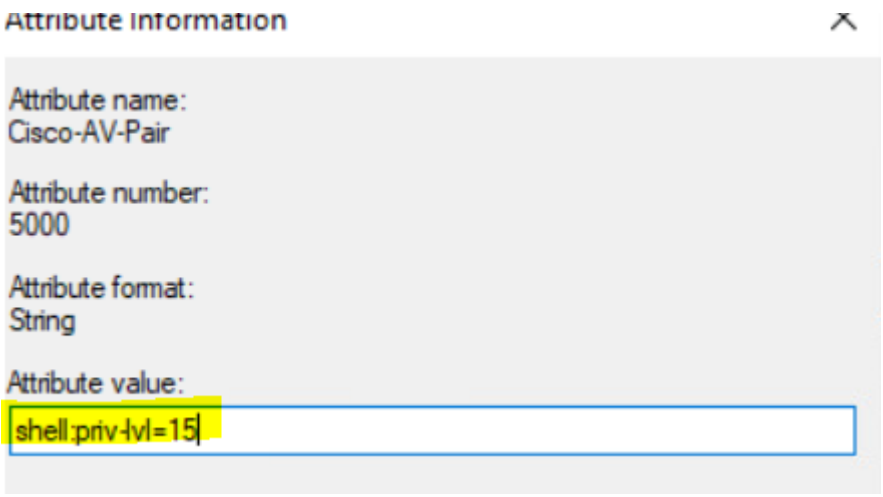


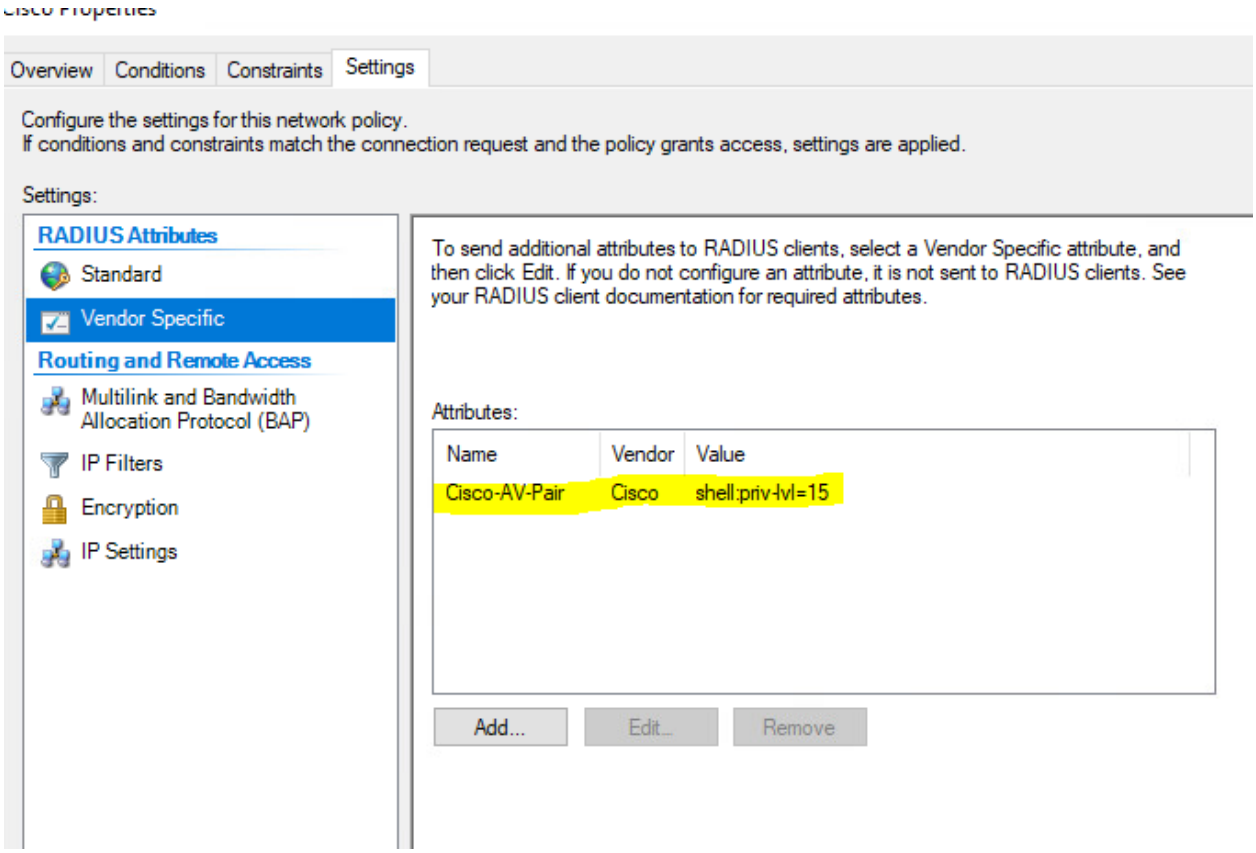
Выбираем Vendor – Cisco

Атрибут – Cisco-AV-Pair

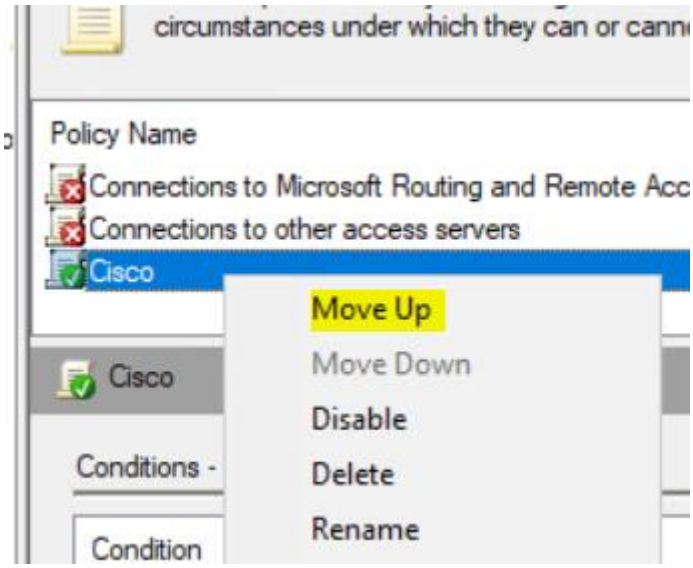


В значении атрибута прописываем shell:priv-lvl=15





Поднимаем нашу политику наверх



Policy Name	Status	Processing Order	Access Type	Source
Cisco	Enabled	1	Grant Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified
Connections to other access servers	Enabled	999999	Deny Access	Unspecified

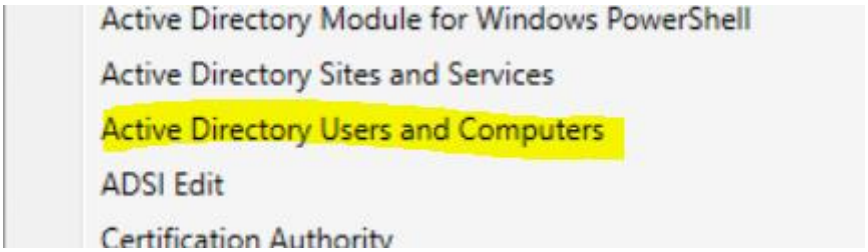
Cisco

Conditions - If the following conditions are met:

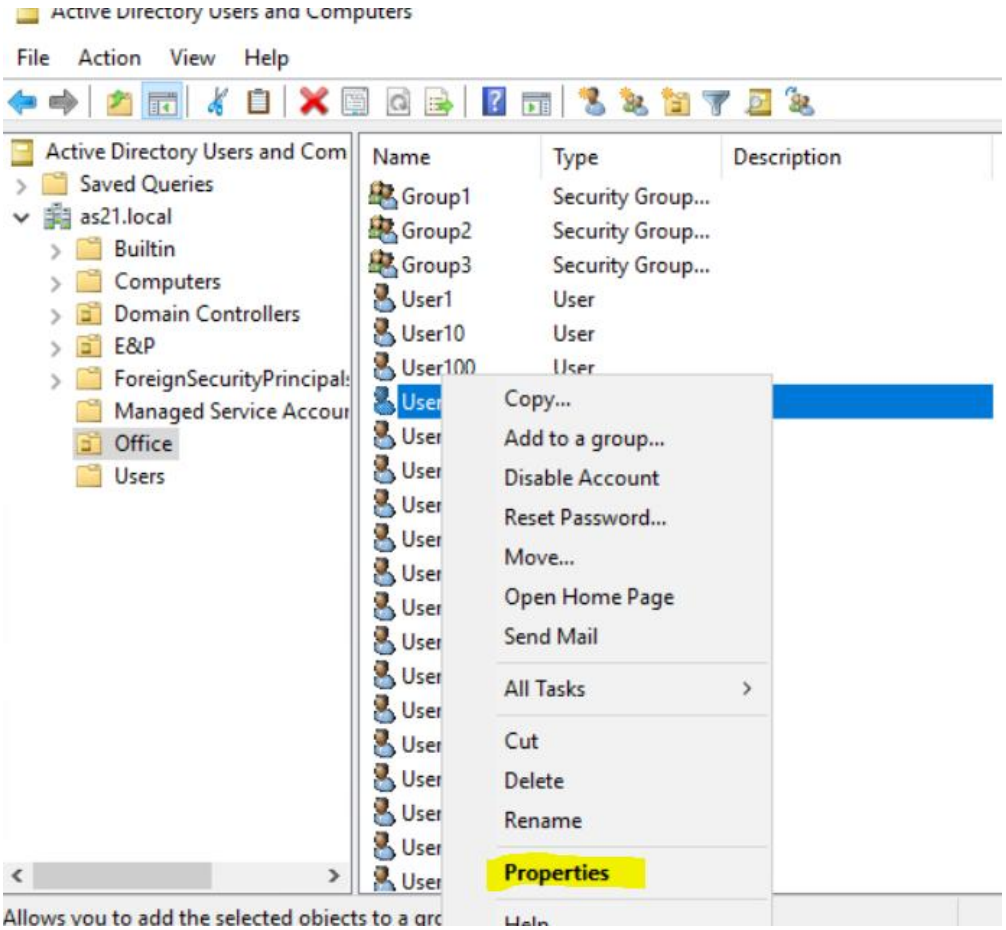
Condition	Value
User Groups	AS21\Domain Admins
Client Friendly Name	Cisco

Разрешить подключение пользователя

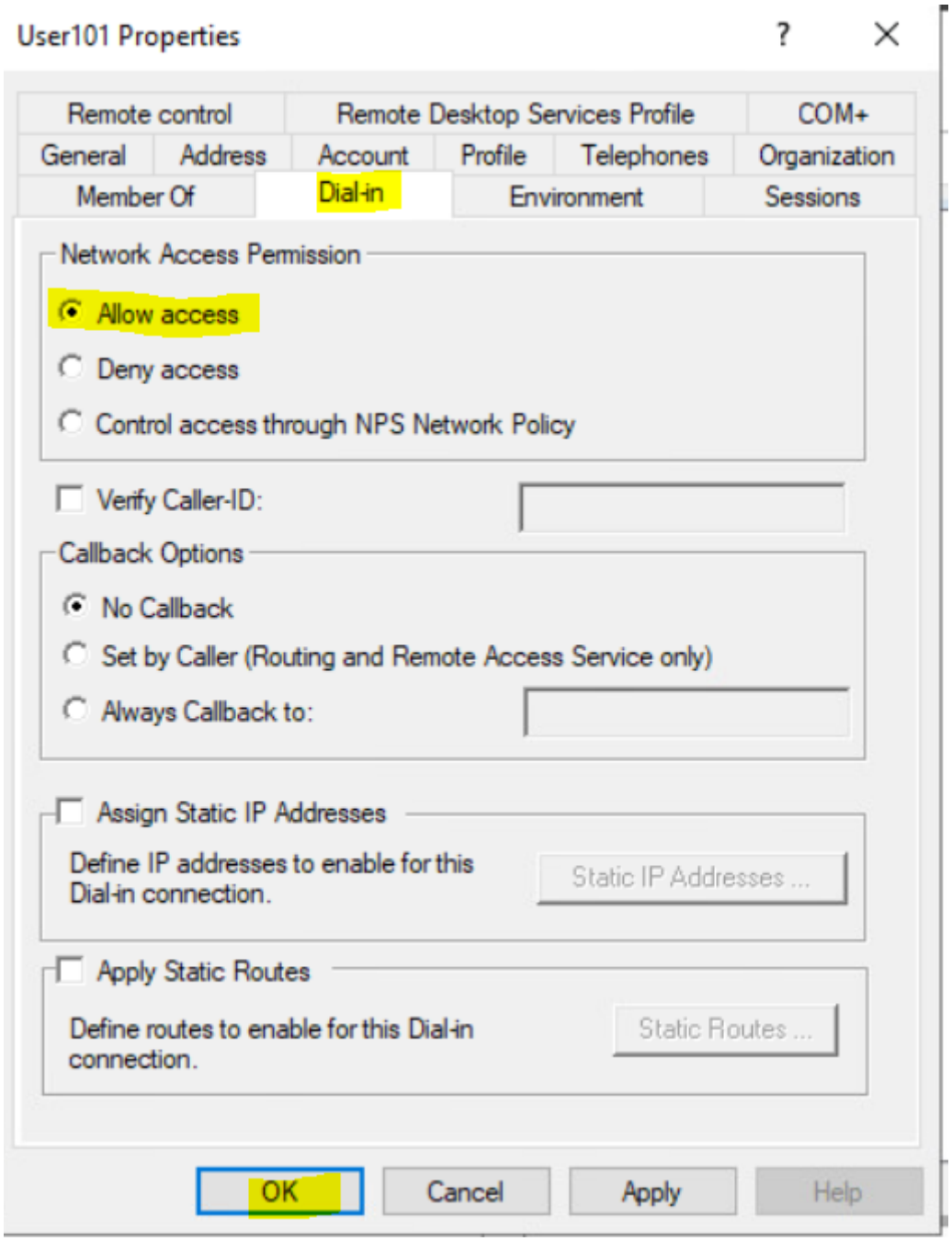
Идем в Active Directory Users and Computers



Выбираем пользователя, который должен подключаться. Вызываем его свойство

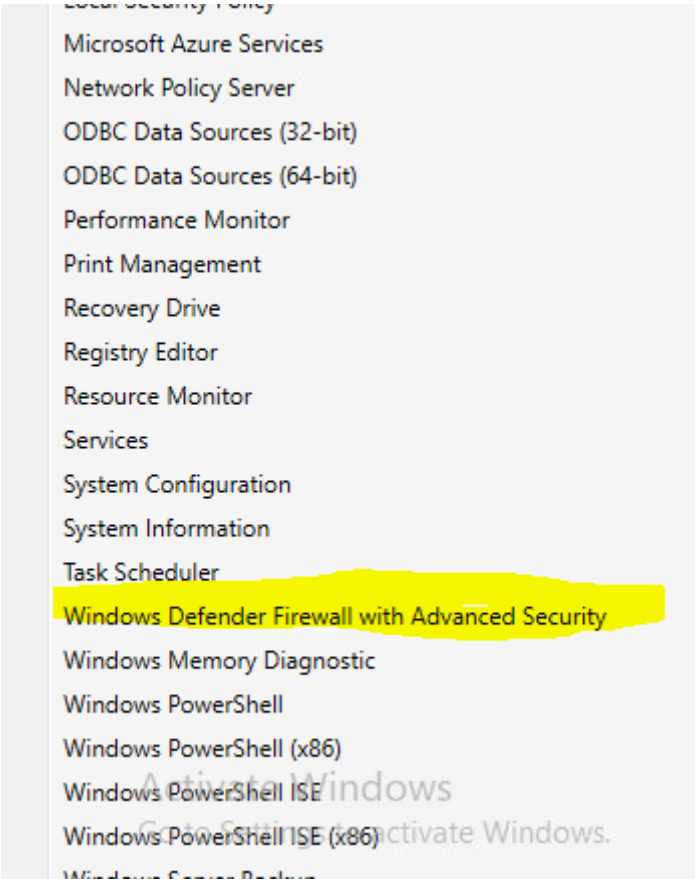


В разделе Dial-in в Network Access Permission выставляем значение Allow Access

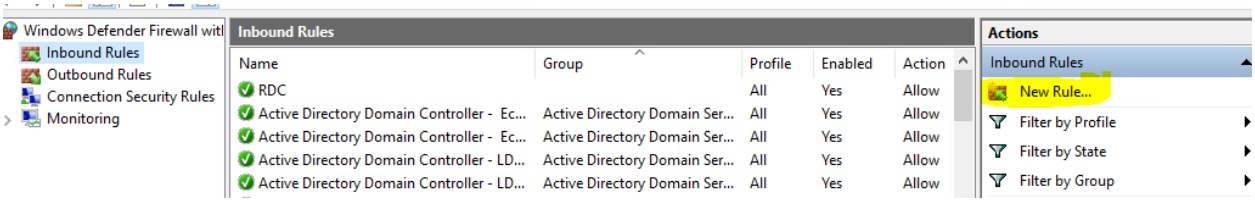


Настройка firewall для работы NPS

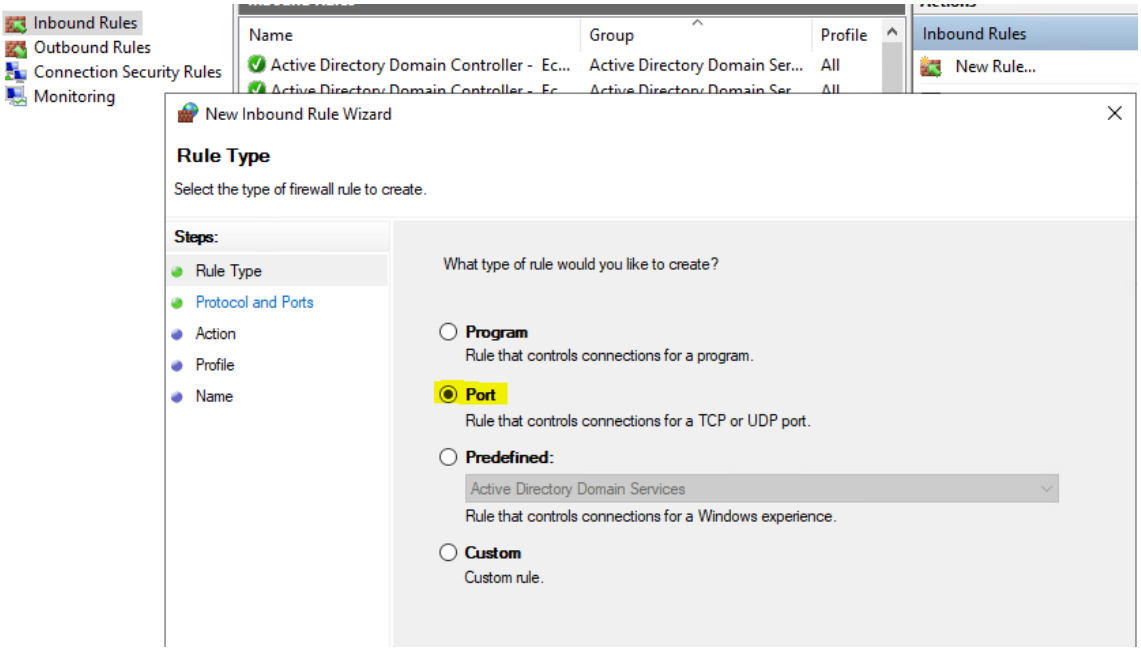
Открываем оснастку Windows Defender Firewall with Advanced Security



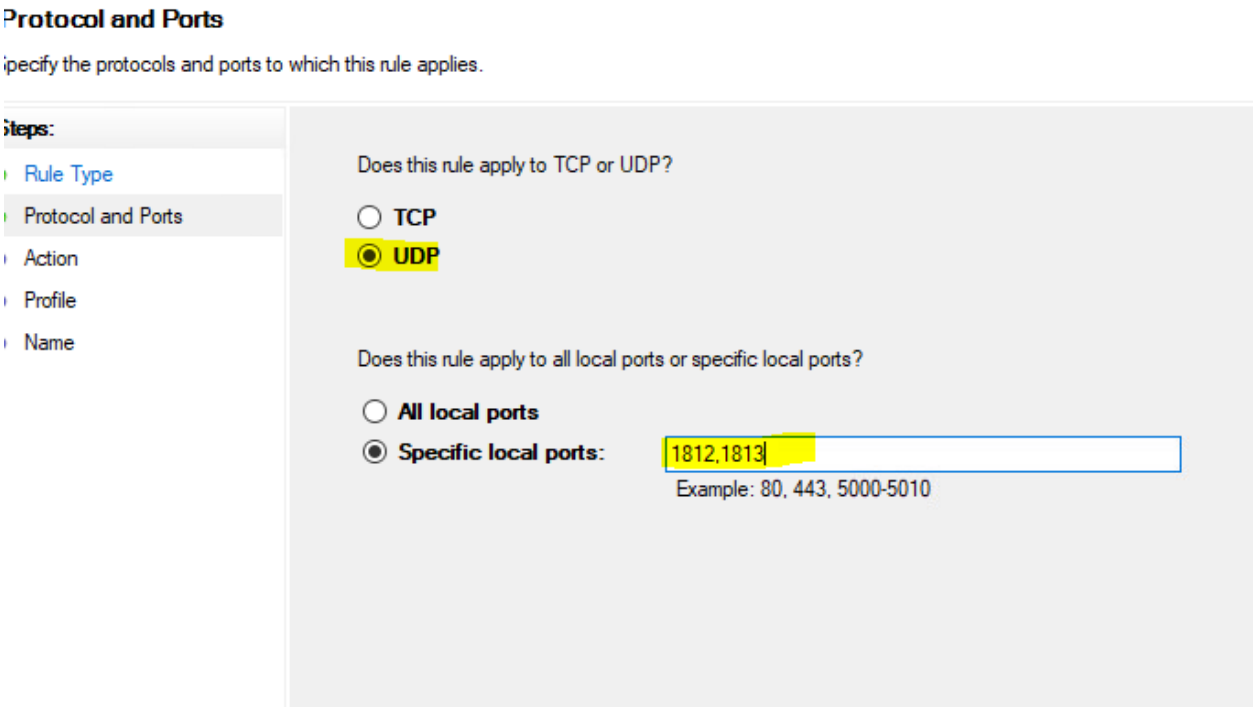
В разделе Inbound Rules создаем новое правило New Rule



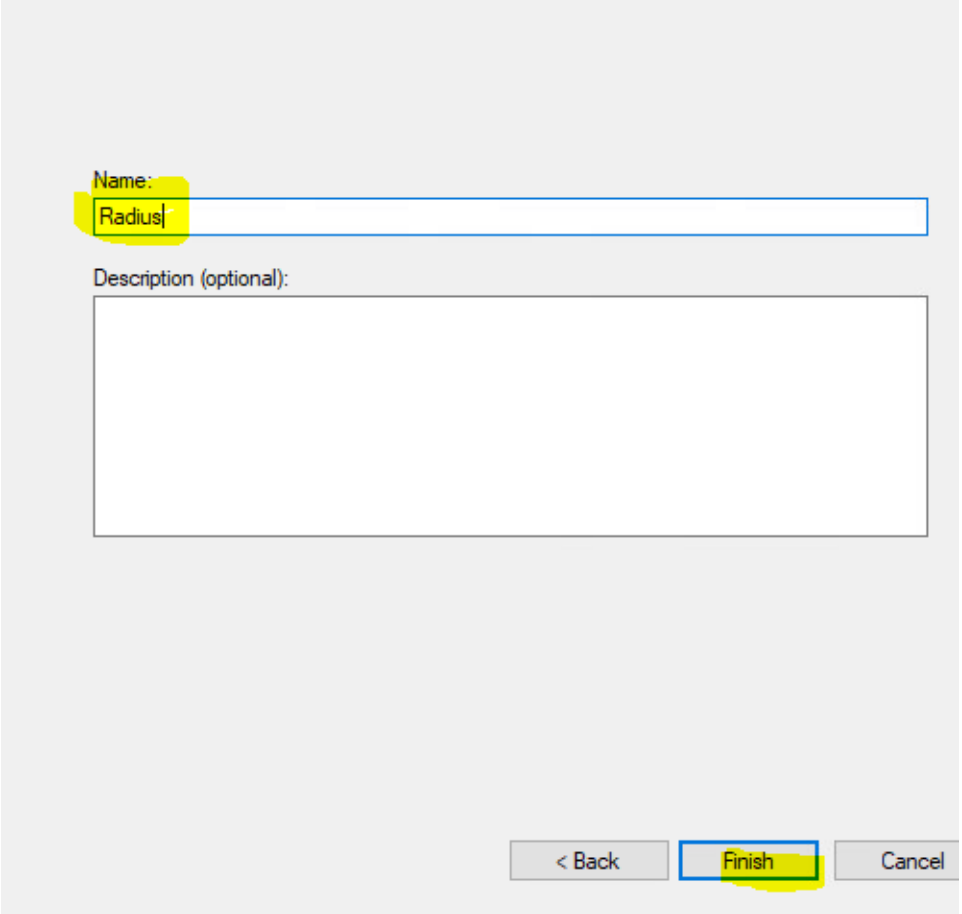
В типе правила выбираем Port



Указываем порты UDP 1812,1813 (1812, чтобы запомнить, год Бородинского сражения и следующий)



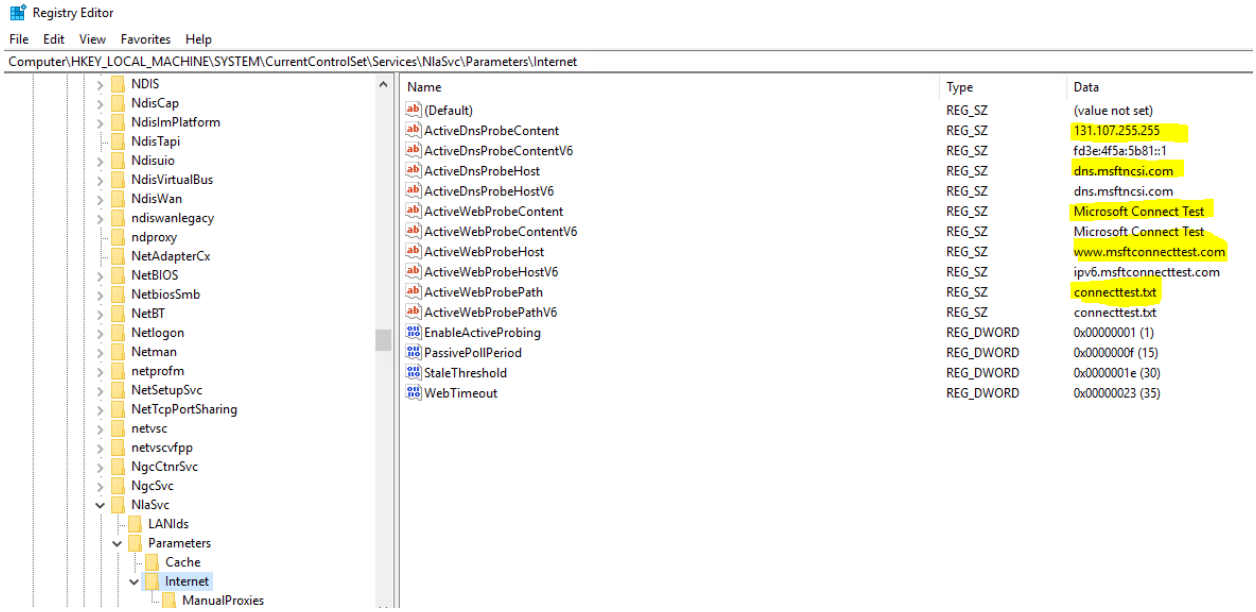
Вводим имя правила - Radius



Эмуляция Интернет

Если с памятью хорошо, то пункт пролистываем, иначе, чтобы вспомнить настройки идем в реестр на DC (regedit)

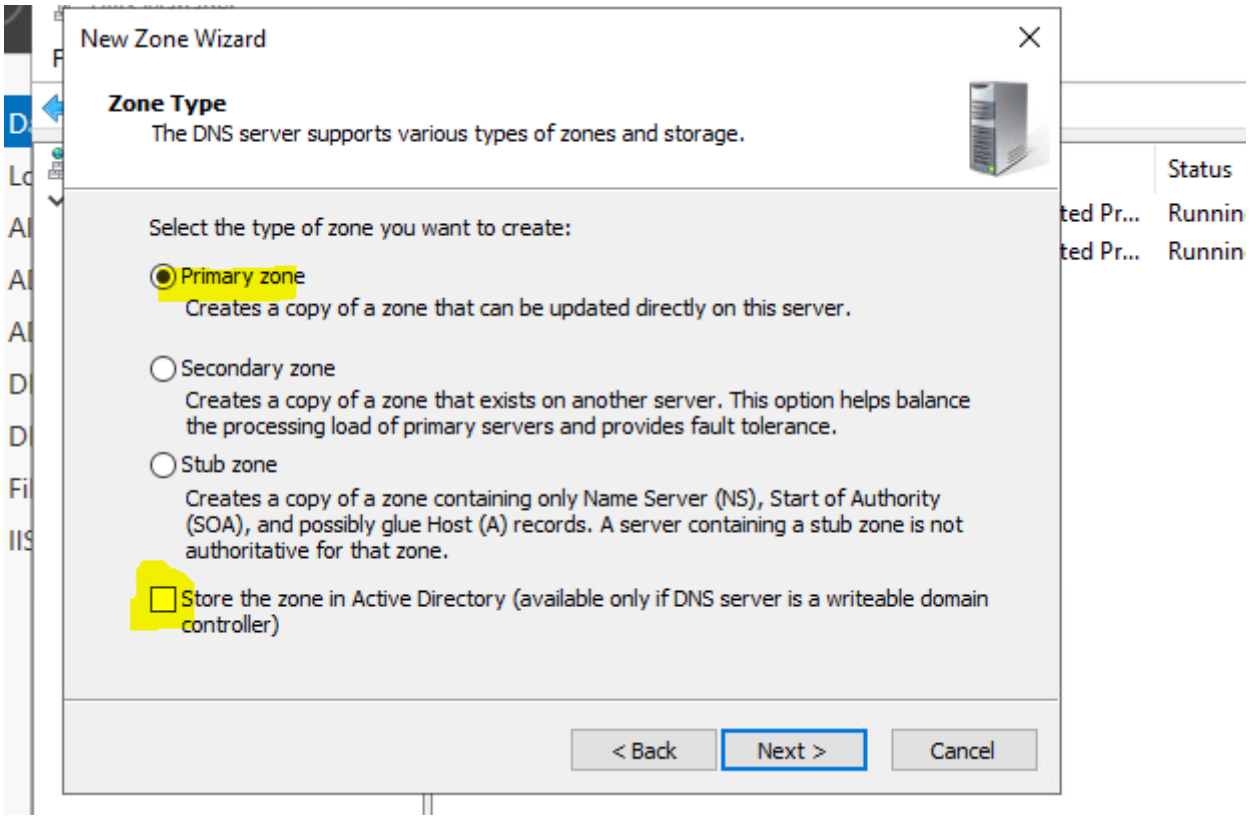
HKLM > SYSTEM > CurrentControlSet > Services > NlaSvc >Parameters > Internet



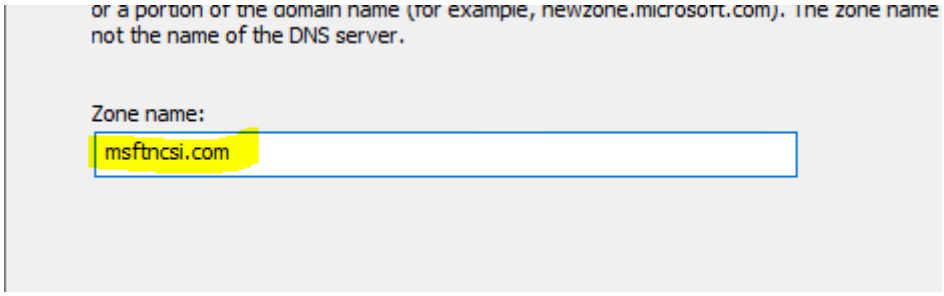
Запоминаем значения или не закрываем окно

Идем в DNS Manager

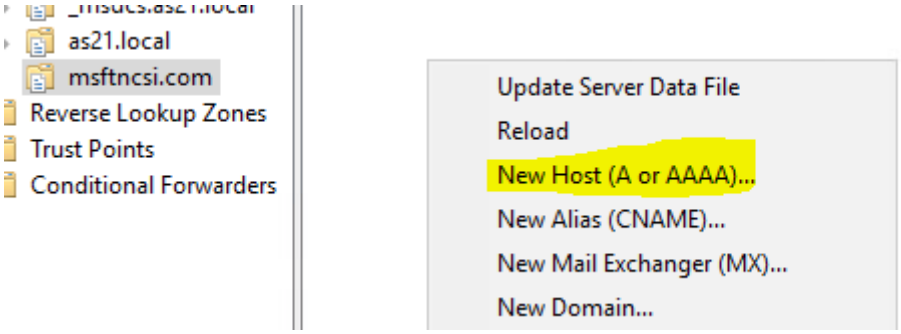
Создаем новую Primary zone. Не забываем убрать галку о хранении в Active Directory



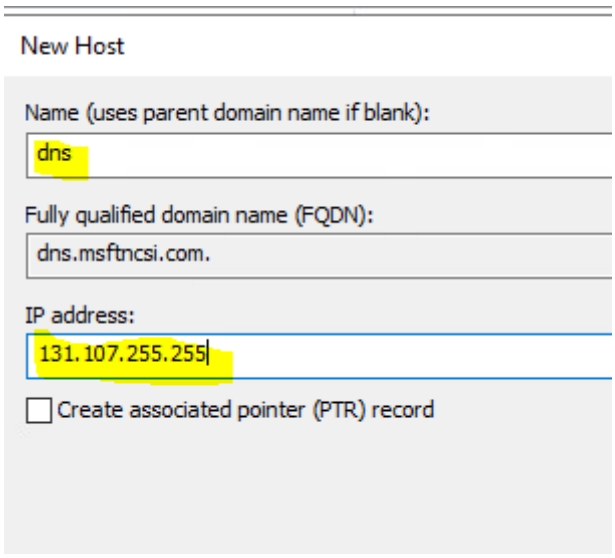
Пишем имя зоны из значения ActiveDNSProbeHost – msftncsi.com (без хоста dns)



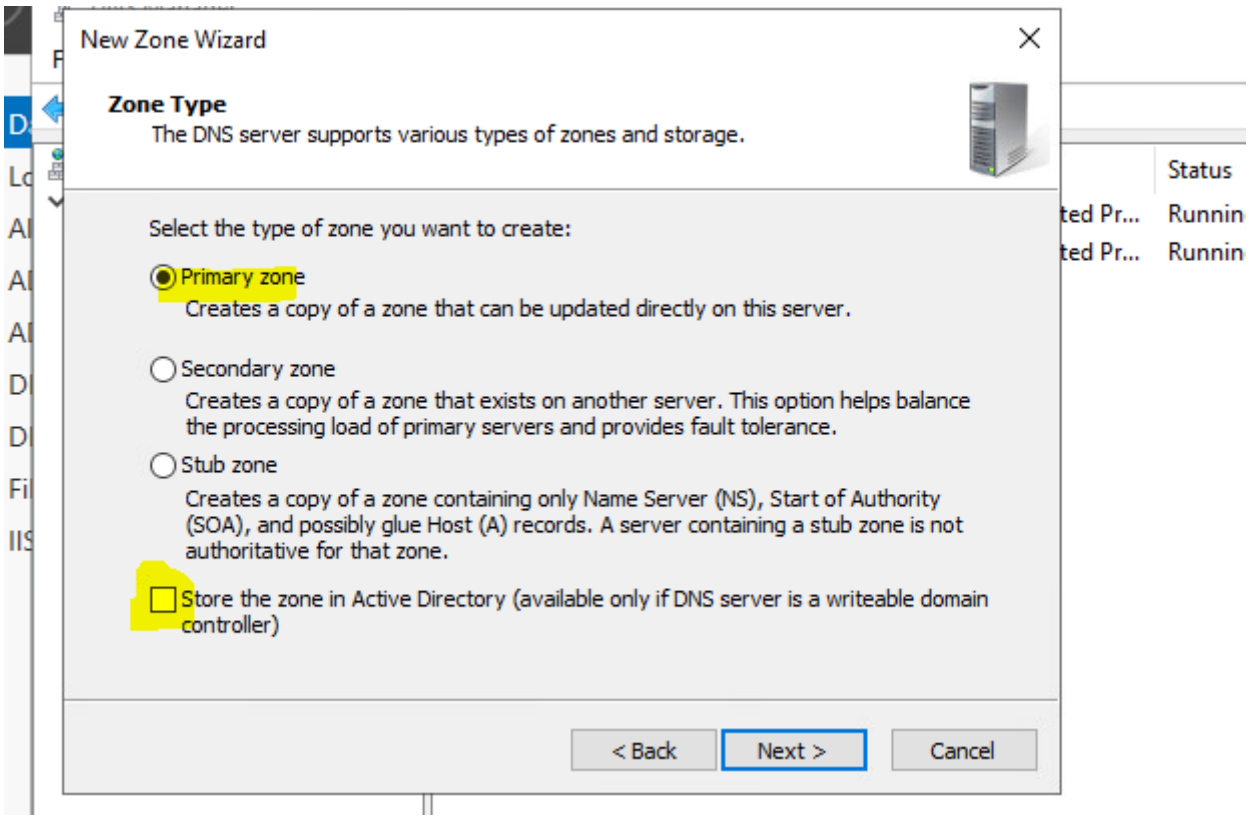
Внутри зона создаем A запись



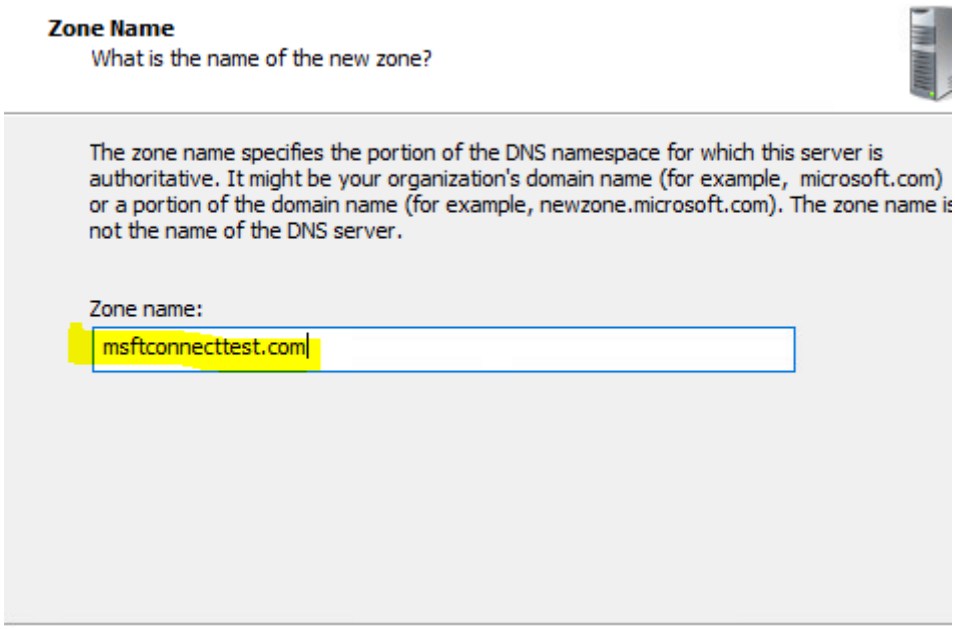
С именем dns и записью из поля ActiveDNSProbeContent – 131.107.255.255



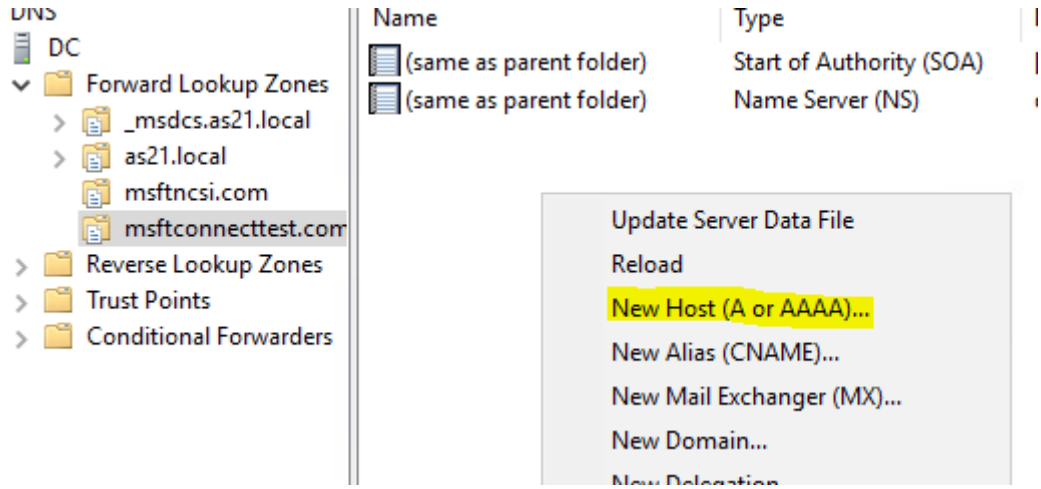
Создаем новую Primary zone. Не забываем убрать галку о хранении в Active Directory



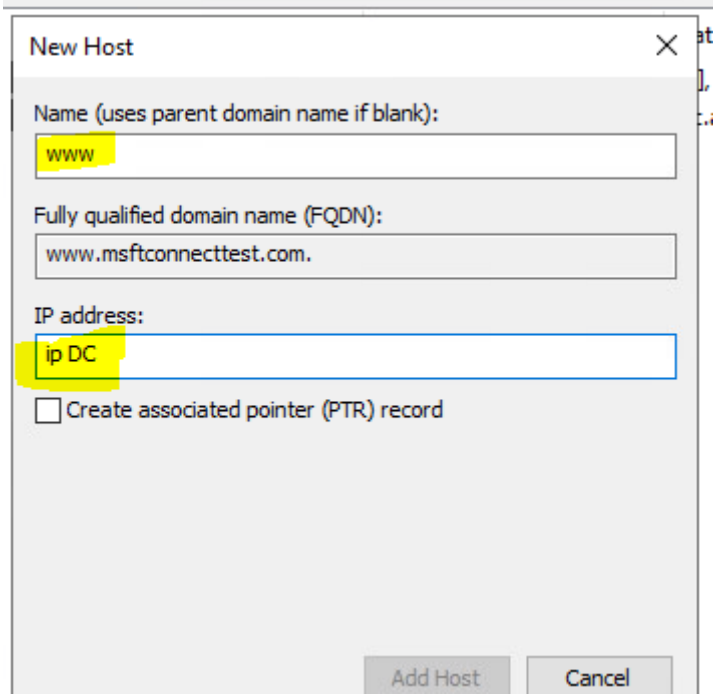
Пишем имя зоны из значения ActiveWebProbeHost – msftconnecttest.com (без хоста www)



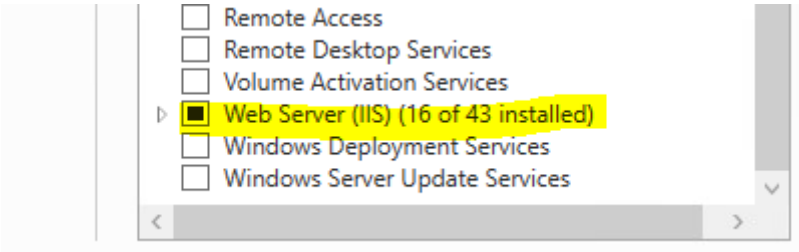
Внутри зона создаем А запись



С именем www и записью ip адрес DC

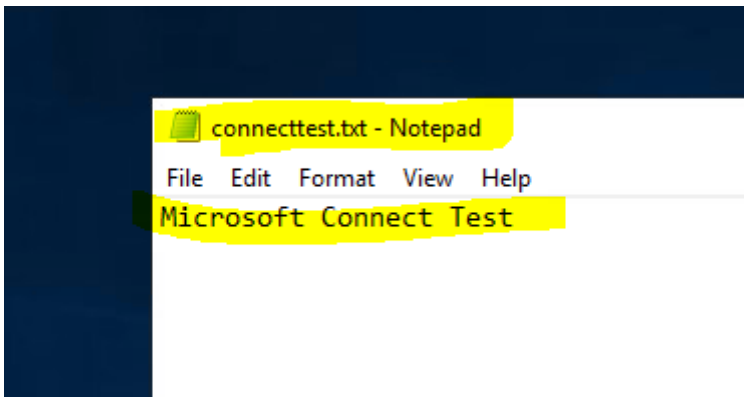


Устанавливаем IIS сервер на DC в стандартной комплектации

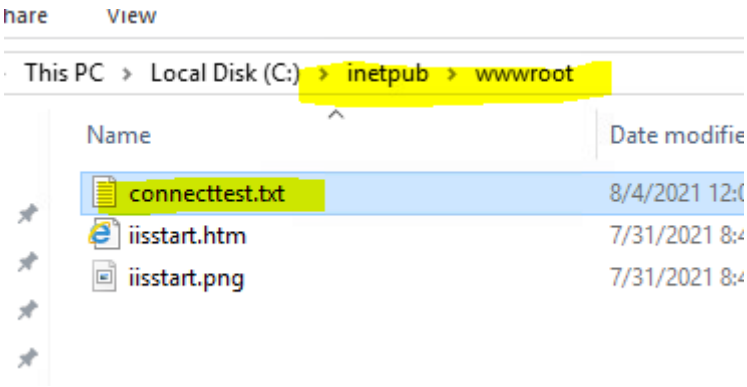


После установки создаем файл из ActiveWebProbePath – connecttest.txt (аккуратнее с расширениями файлов)

Внутри файла пишем из ActiveWebProbeContent – Microsoft Connect Test



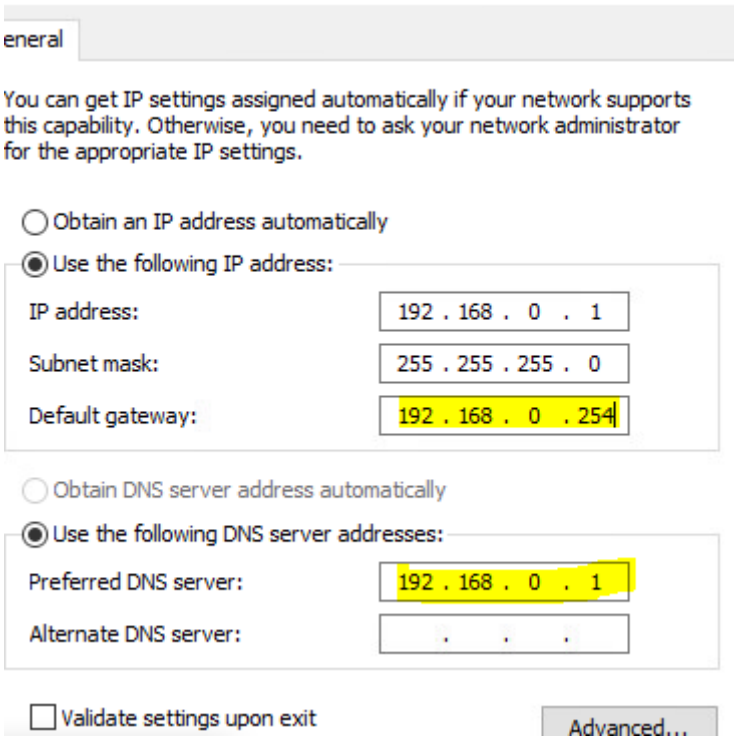
Кладем файл по пути – C:\inetpub\wwwroot



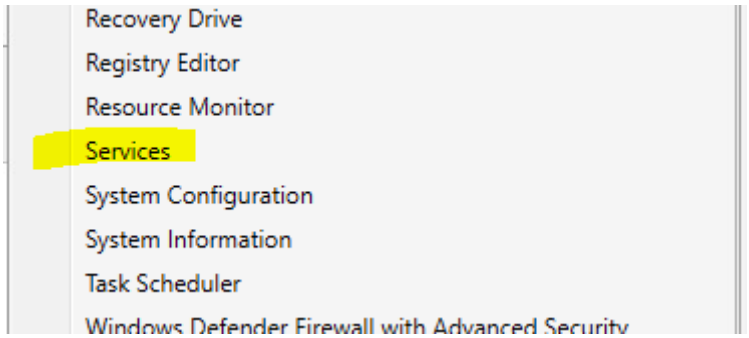
Открываем настройки адаптера на DC

Меняем 127.0.0.1 на адрес вашего DC сервера (127.0.0.1 в DNS быть не должно вообще)

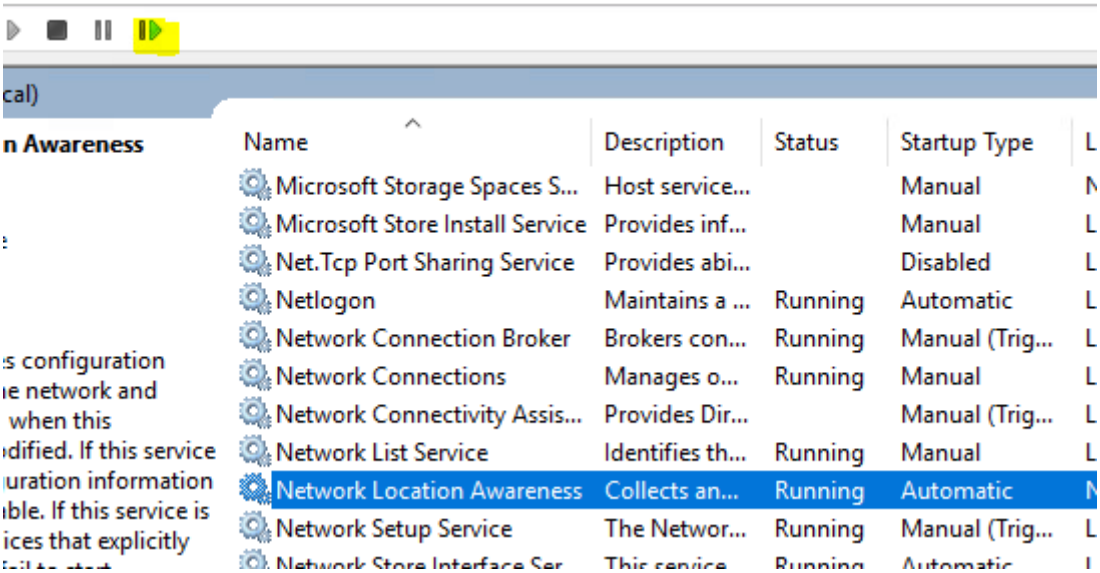
Проверяем, что заполнено поле Default gateway



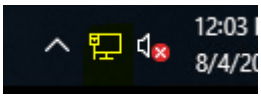
Чтобы проверить, идем в Services



Перезапускаем службу Network Location Awareness



 **- это не правильная пиктограмма**

 **- это правильная пиктограмма**