

AtomSkills 2021

ПОСЛЕ СОЗДАНИЯ ДОМЕНА AS21.LOCAL.....	3
LOGON BANNER	5
НАСТРОЙКА WINCLI1 и WINCLI2	5
ПРИВЕТСТВЕННАЯ АНИМАЦИЯ.....	5
TEXT.TXT ПРИ ПЕРВОМ ВХОДЕ ПОЛЬЗОВАТЕЛЕЙ.....	6
RDP ПОДКЛЮЧЕНИЕ ПО СЕРТИФИКАТАМ	6
Настройка серверов для работы по ip.....	6
Настройка шаблона выдачи сертификатов	7
Настройки GPO для RDP	11
РАБОТОСПОСОБНОСТЬ DNS.....	13
Настройка Forwarders.....	13
Настройка Round Robin	14
НАСТРОЙКА DHCP	15
ФАЙЛОВЫЕ СЛУЖБЫ НА DC (File Restrictions).....	15
СЛУЖБА ВРЕМЕНИ (NTP)	18
Настройка DC на получение времени с Moogle.....	18
Настройка клиентов на получение времени с DC	18
Настройка временной зоны	19
СОЗДАНИЕ ПОЛЬЗОВАТЕЛЕЙ ДОМЕНА.....	24
РАЗРЕШИТЬ GROUPLIST ЗАХОДИТЬ НА DC	25
ROAMING PROFILES	26
План А	27
План Б	30
ROOT CA.....	32
Базовая настройка RootCA.....	32
Подготовка RootCA для выпуска сертификата SubCA.....	34
НАСТРОЙКА RODC.....	36
Установка контроллера домена.....	36
Настройка сайтов.....	37
Настройка DNS на WINSRV1	40
НАСТРОЙКА SUBCA НА WINSRV2	42
Базовая настройка	42
Настройка CRL на SubCA.....	44

ПОДГОТОВКА ШАБЛОНА ДЛЯ WEB ДОСТУПА.....	46
СОЗДАНИЕ RDS.....	50
Установка ролей	50
Настройка web доступа по сертификатам.....	52
Настройка IIS RDS.....	58
Публикация коллекции RDS.....	60
Публикация приложения RDS.....	62
Добавление сертификата в доверенные.....	64
Убираем предупреждение при открытии файла.....	66
ПУБЛИКАЦИЯ CRL НА ДОМАШНЕЙ СТРАНИЦЕ	67
WEB Сервер на WINDMZ	72
Удаленное подключение к WINDMZ	72
Настройка подключения консоли IIS к WINDMZ.....	74
Настройка аутентификации по сертификатам	76
Добавление локального пользователя на WINDMZ.....	76
Создание шаблона для автоворыдачи пользователя Group1	78
Выпуск и установка сертификата на WINDMZ.....	82
Установка списка отзываемых сертификатов на WINDMZ.....	86
Настройка SSL на WINDMZ	87
Настройка авторизации на WINDMZ.....	87
Настройка IIS на WINDMZ.....	91
Настройка привязки (Bindings)	92
Перенаправление с http на https	93
Виртуальный каталог Docs.....	95
Настройка файловых служб на ЦОД (WINSRV1 и WINSRV2)	98
Настройка DFS.....	98
Настройка квот.....	105
Настройка запрета на хранение файлов	107
Настройка NPS.....	108
Настройка политики	108
Разрешить подключение пользователя	117
Настройка firewall для работы NPS	118
Эмуляция Интернет	121

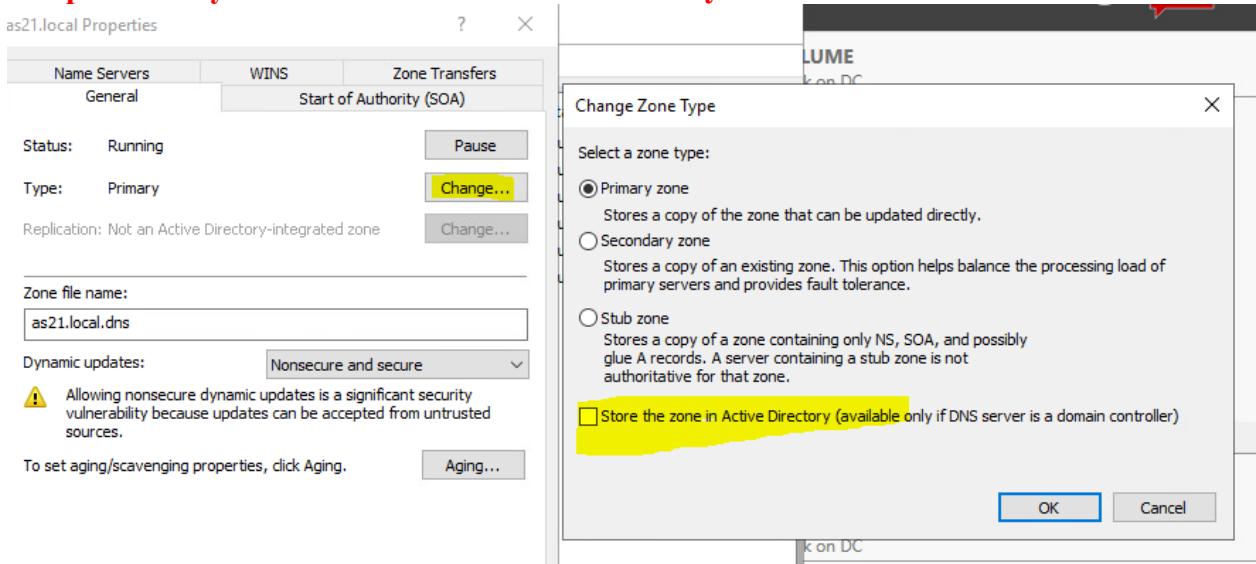
ПОСЛЕ СОЗДАНИЯ ДОМЕНА AS21.LOCAL

Сделайте сервер DC контроллером домена AS21.local.

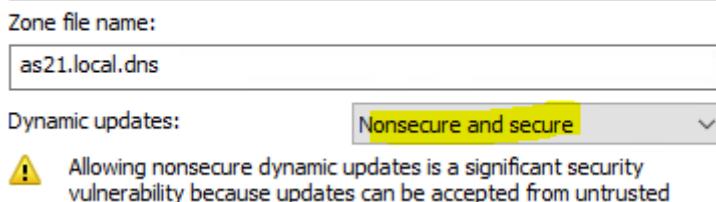
Настройка сервиса DNS для переноса на WINSRV1

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:

12.168.192.in-addr.arpa Properties

General		Start of Authority (SOA)					
Name Servers		WINS-R	Zone Transfers				
To add name servers to the list, click Add.							
Name servers: <table border="1"> <thead> <tr> <th>Server Fully Qualified Domain Name (FQDN)</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td>dc.as21.local.</td> <td>Unknown</td> </tr> </tbody> </table>				Server Fully Qualified Domain Name (FQDN)	IP Address	dc.as21.local.	Unknown
Server Fully Qualified Domain Name (FQDN)	IP Address						
dc.as21.local.	Unknown						
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Remove"/>							
<small>* represents an IP address retrieved as the result of a DNS query and may not represent actual records stored on this server.</small>							

Name Servers	WINS-R		
To add name servers to the list, click Add.			
Name servers: <table border="1"> <thead> <tr> <th>Server Fully Qualified Domain Name (FQDN)</th> </tr> </thead> <tbody> <tr> <td>dc.as21.local.</td> </tr> </tbody> </table>		Server Fully Qualified Domain Name (FQDN)	dc.as21.local.
Server Fully Qualified Domain Name (FQDN)			
dc.as21.local.			

Разрешить передачу зоны на сервера, указанные ранее

12.168.192.in-addr.arpa Properties

General		Start of Authority (SOA)					
Name Servers		WINS-R	Zone Transfers				
A zone transfer sends a copy of the zone to the servers that request a copy.							
<input checked="" type="checkbox"/> Allow zone transfers: <input type="radio"/> To any server <input checked="" type="radio"/> Only to servers listed on the Name Servers tab <input type="radio"/> Only to the following servers							
<table border="1"> <thead> <tr> <th>IP Address</th> <th>Server FQDN</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>				IP Address	Server FQDN		
IP Address	Server FQDN						
<input type="button" value="Edit"/>							

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

Active Directory Users and Computers	Name	Type	DC
Saved Queries			
as21.local	DC	Computer	GC
AtomSkills			
Builtin			
Computers			
Domain Controllers			
PDC			
ForeignSecurityPrincipal			

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!**

Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	Warning! Property of RosAtom!
Interactive logon: Message title for users attempting to log on	Warning! Property of RosAtom!
Interactive logon: Number of previous logons to cache (in c...	Not Defined

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**

<input checked="" type="checkbox"/> Do not display network selection UI	Not configured	True
<input checked="" type="checkbox"/> Do not enumerate connected users on domain-joined computers	Not configured	No
<input checked="" type="checkbox"/> Show first sign-in animation	Disabled	No
<input checked="" type="checkbox"/> 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

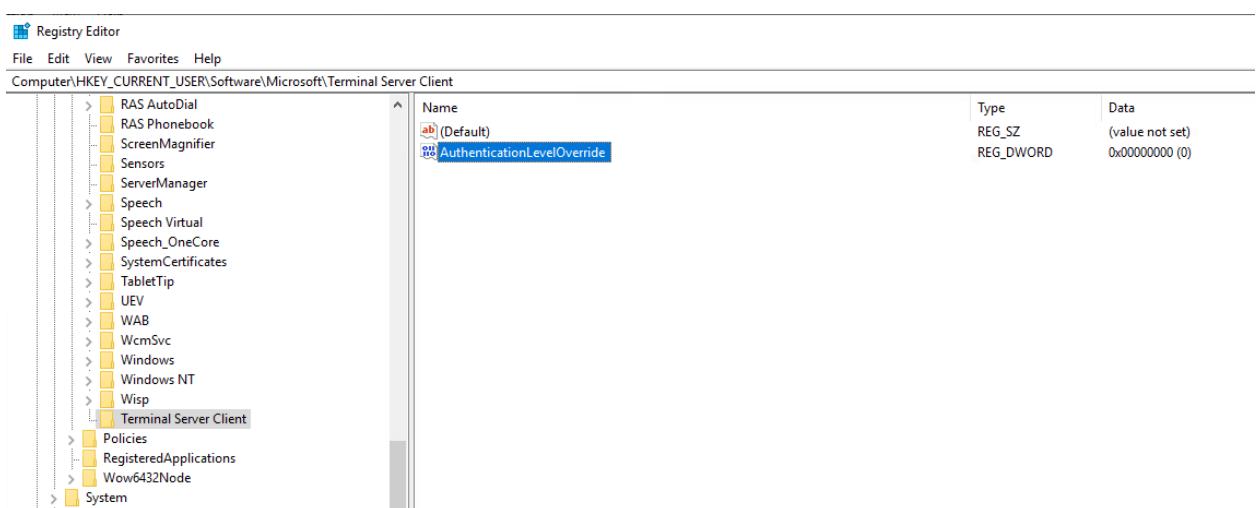
RDP ПОДКЛЮЧЕНИЕ ПО СЕРТИФИКАТАМ

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)

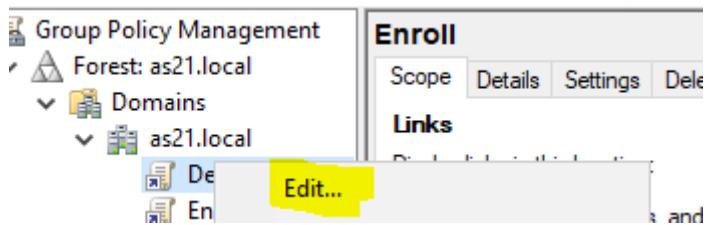
Настройка серверов для работы по ip

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



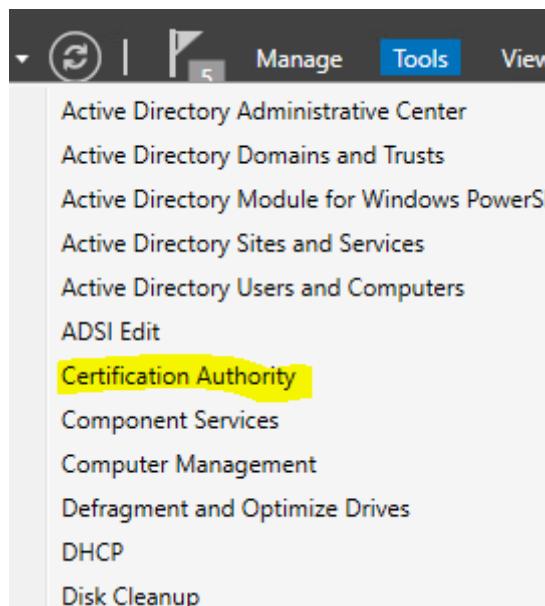
User Configuration > Preferences > Windows Settings > Registry -> New -> Registry Wizard

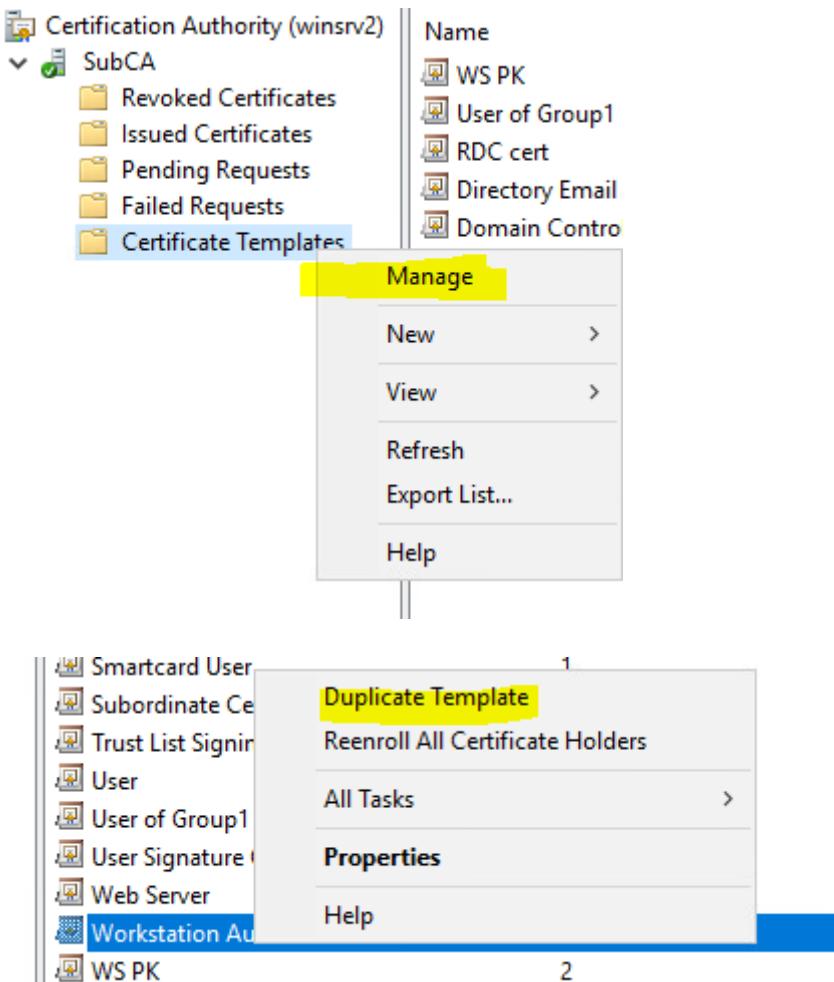
Создать «визардом» новую запись Local Computer выбираем ветку
HKEY_CURRENT_USER > Software > Microsoft > Terminal Server Client

Выбираем все параметры оттуда

Настройка шаблона выдачи сертификатов

Настроим выдачу нужного сертификата на WINSRV2



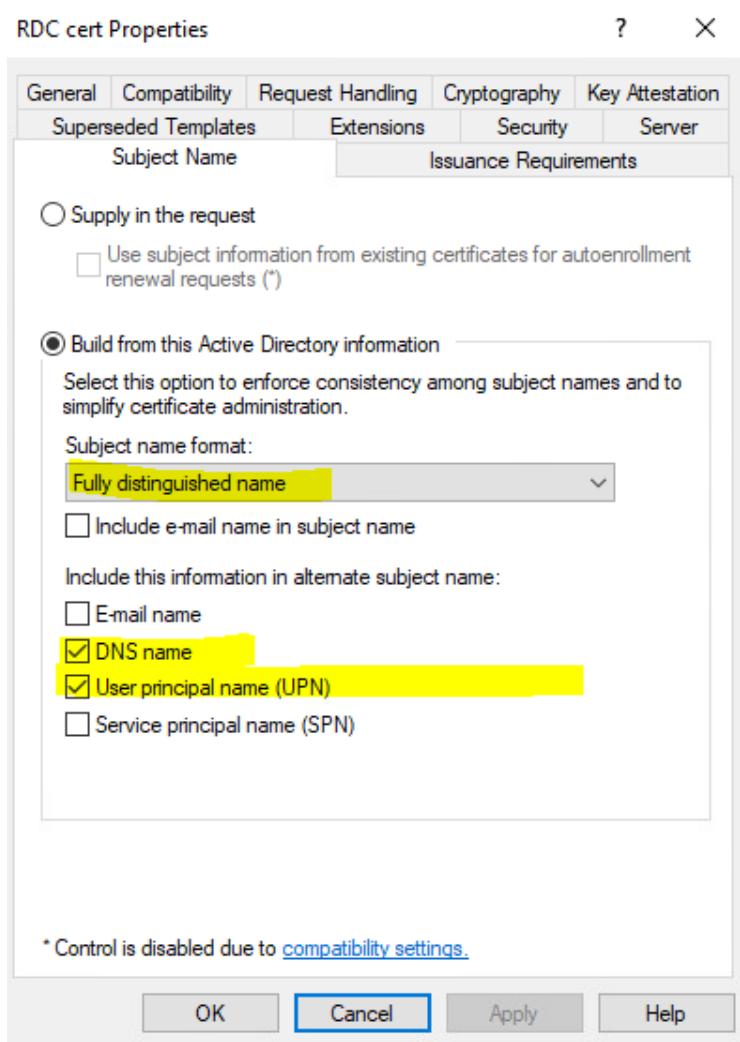


Вводим имя нового шаблона. Включаем публикацию в Active Directory

RDC cert Properties

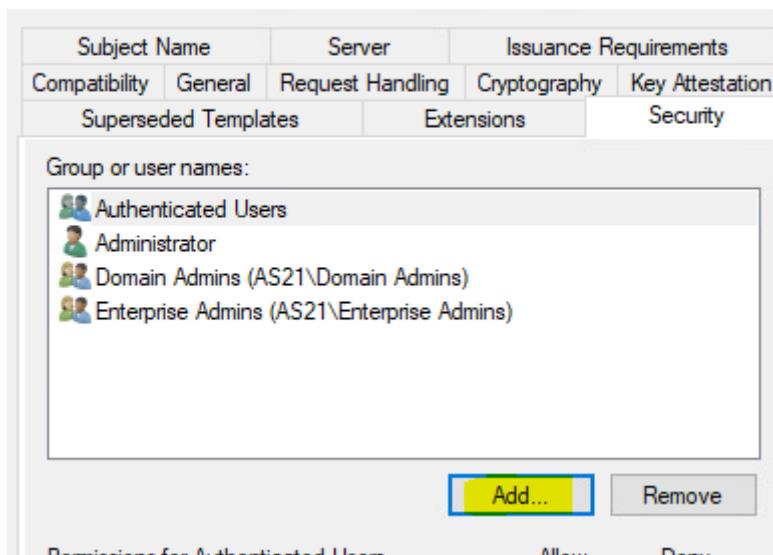
Subject Name		Issuance Requirements			
Superseded Templates		Extensions	Security	Server	
General	Compatibility	Request Handling	Cryptography	Key Attestation	
Template display name:					
<input type="text" value="RDC cert"/>					
Template name:					
<input type="text" value="RDCcert"/>					
Validity period:		Renewal period:			
<input type="text" value="1"/>	years	<input type="text" value="6"/>	weeks		
<input checked="" type="checkbox"/> Publish certificate in Active Directory <input type="checkbox"/> Do not automatically reenroll if a duplicate certificate exists in Active Directory					

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

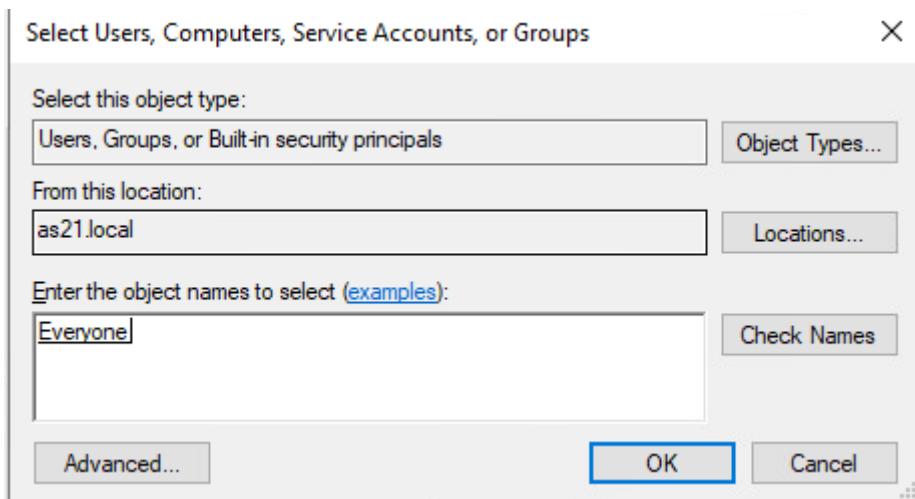


Нужно добавить возможность выпуска сертификата любой машиной

Properties of New Template



Даем всем права на выпуск сертификата группе Everyone



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	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Публикуем сертификат в Active Directory

SubCA

- Revoked Certificates
- Issued Certificates
- Pending Requests
- Failed Requests
- Certificate Templates

WS PK User of Group1 RDC cert Directory Email Replication Domain Controller Authentication

Manage Authentication

New > Certificate Template to Issue

View > Controller

Refresh

Export List...

Help Certification Authority

Administrator

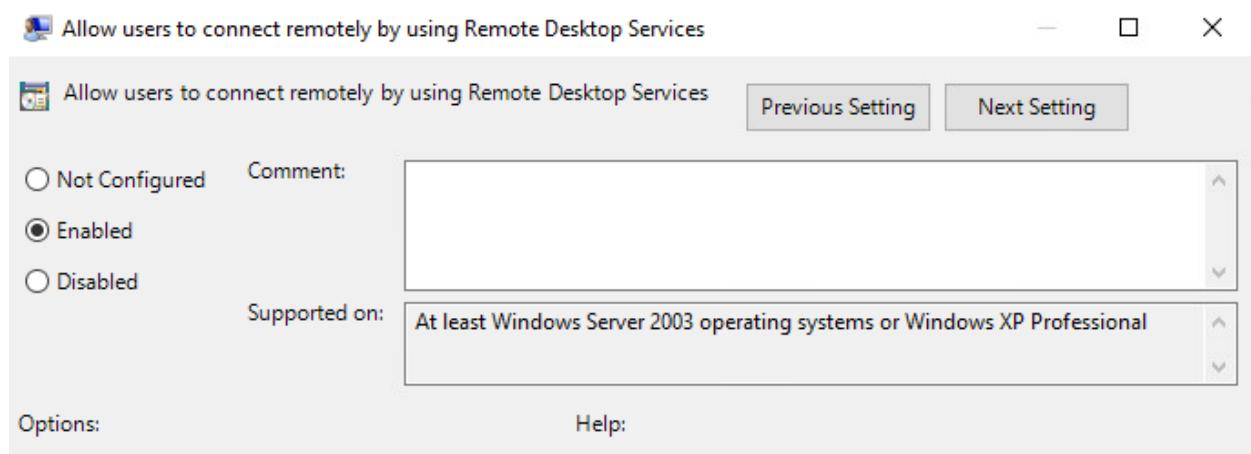
Server Authentication Client Authentication Client Authentication Directory Services Client Authentication Client Authentication

Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
RDC cert	Client Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon
Trust List Signing	Microsoft Trust List Signing
User Signature Only	Secure Email, Client Authentication

Настройки GPO для RDP

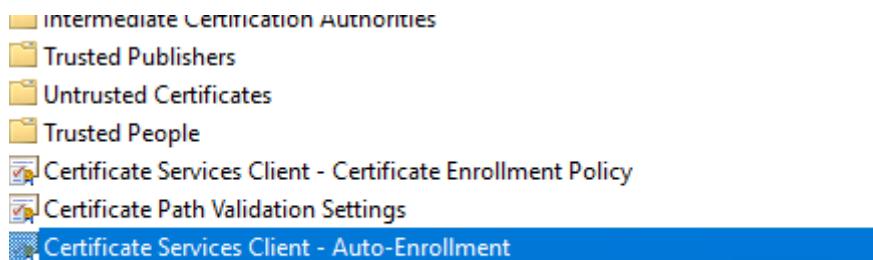
Разрешаем через GPO использование Remote Desktop Connection

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**

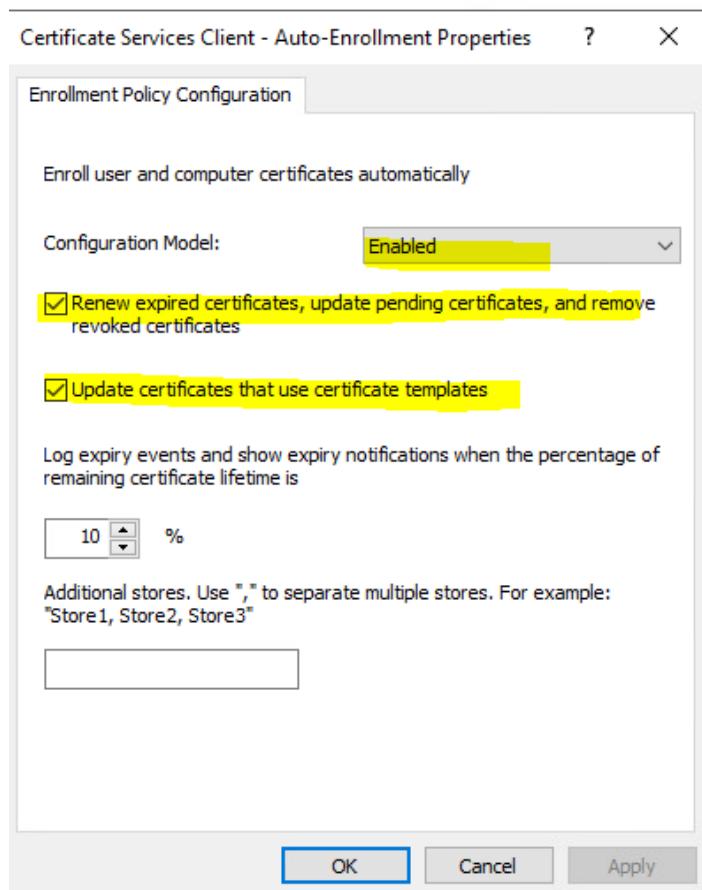


Включаем авто выдачу сертификатов всем устройствам домена

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

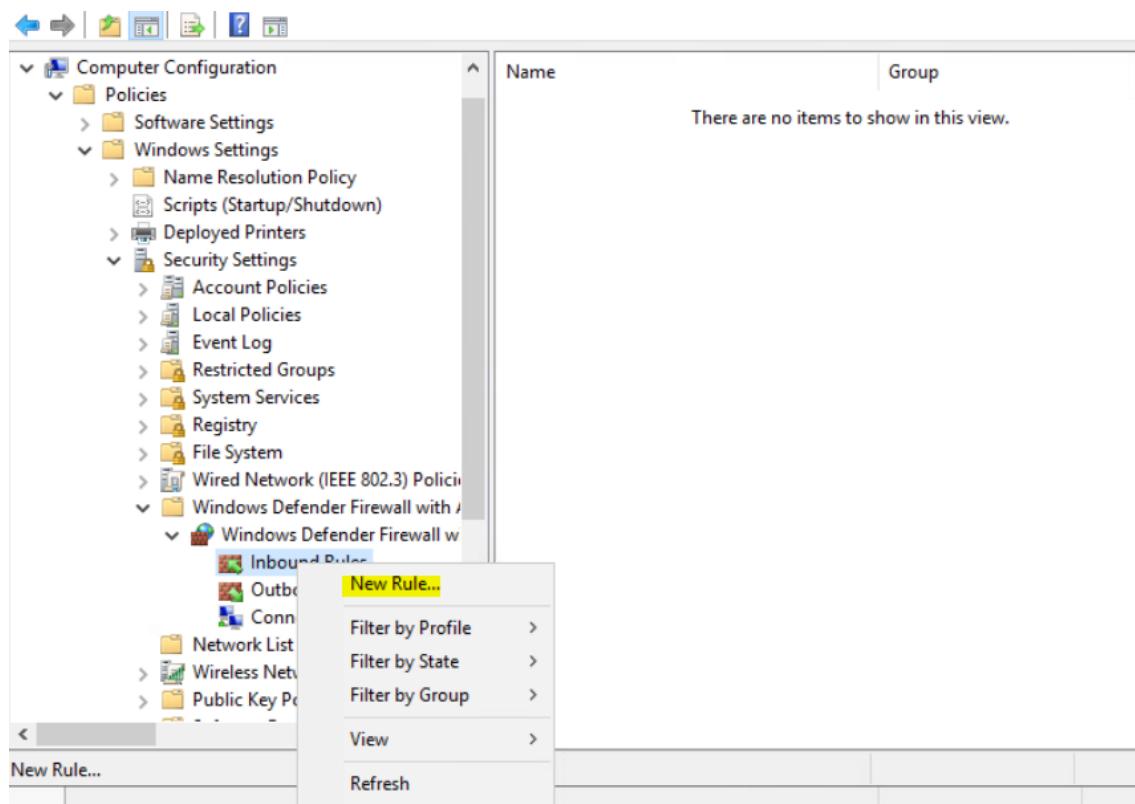


Включаем общую настройку выдачи и выбираем 2 конфигурации



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)

Rule that controls connections for a TCP or UDP port.

Predefined:

Active Directory Domain Services

Rule that controls connections for a Windows experience.

Custom:

Выбираем Remote Desktop

Predefined:

mDNS

iSCSI Service

Kerberos Key Distribution Center

Key Management Service

mDNS

Microsoft Key Distribution Service

Netlogon Service

Network Discovery

Performance Logs and Alerts

Remote Desktop

Remote Desktop (WebSocket)

Remote Event Log Management

Remote Event Monitor

Remote Scheduled Tasks Management

Name	Group	Profile
✓ Remote Desktop - Shadow (TCP-In)	Remote Desktop	All
✓ Remote Desktop - User Mode (UDP-In)	Remote Desktop	All
✓ Remote Desktop - User Mode (TCP-In)	Remote Desktop	All

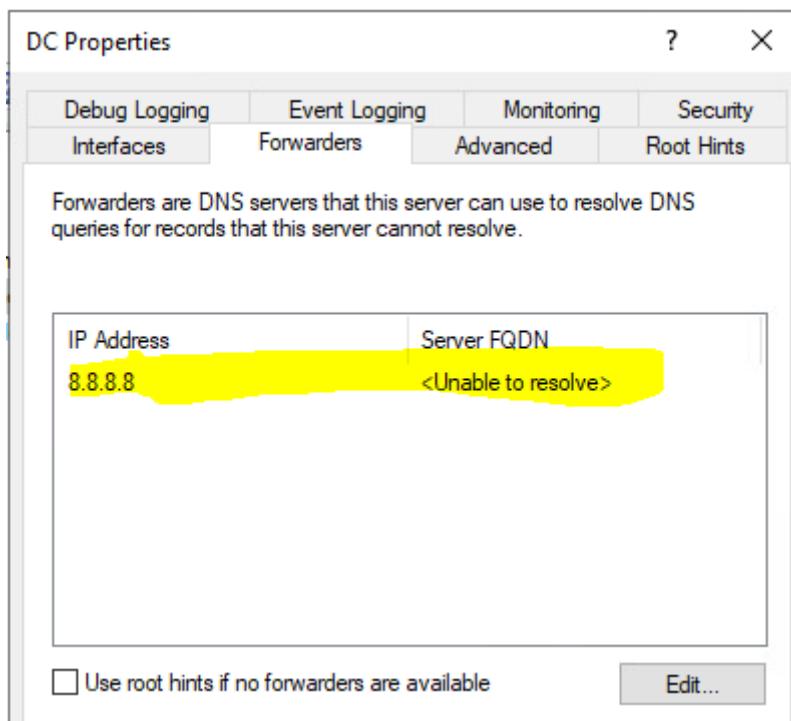
РАБОТОСПОСОБНОСТЬ DNS

Настройка Forwarders

Обеспечьте работоспособность службы DNS на DC.

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

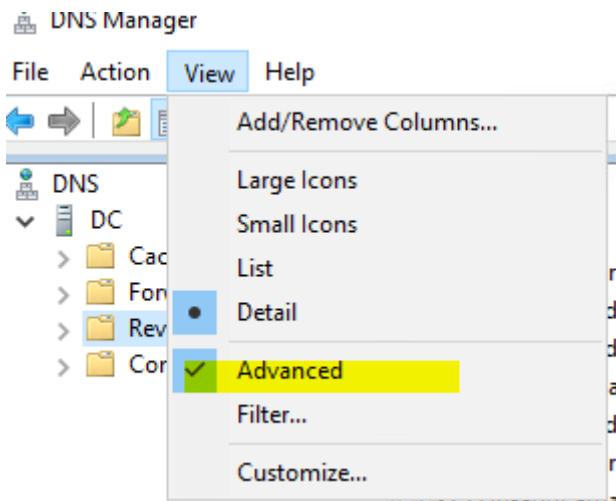
В свойствах DNS сервера прописать Forwarders на 8.8.8.8. Остальные можно удалить



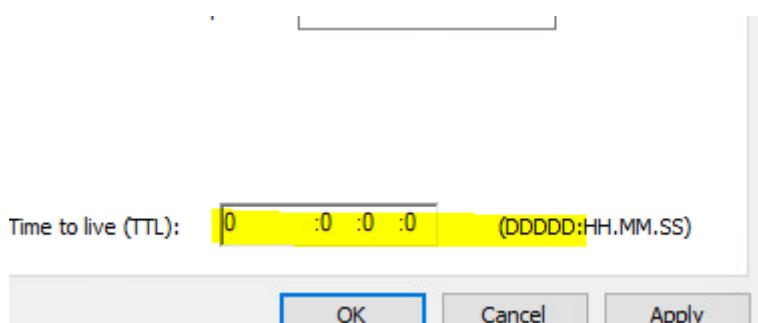
Настройка Round Robin

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 частого обновления зон.

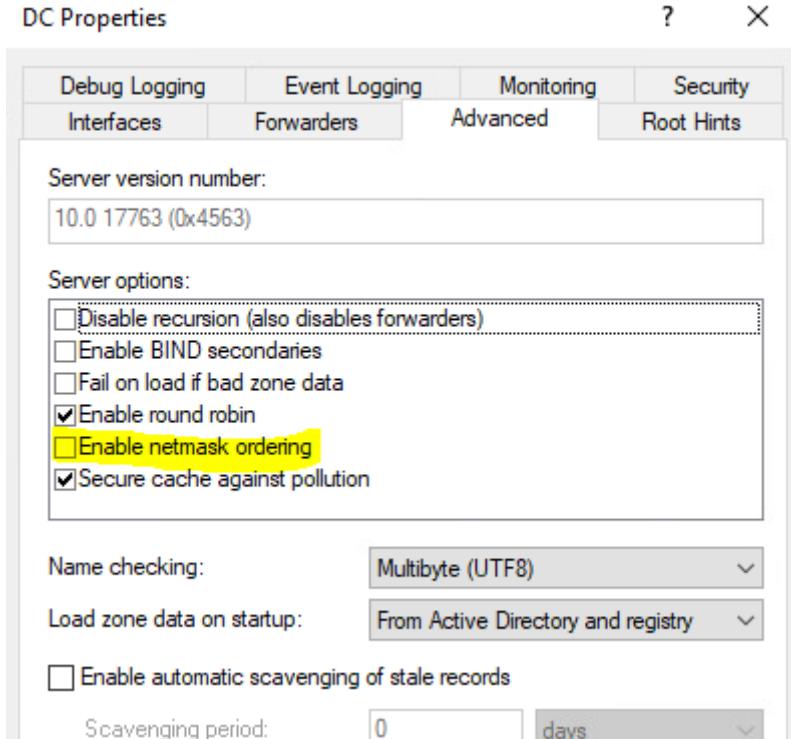
Включить DNS Manager > View > Advanced



Установить TTL для одинаковых А 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

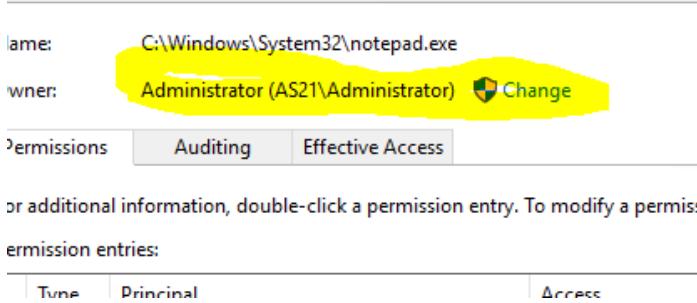
пользователю Engineer1/P@ssw0rd и Projects1/P@ssw0rd соответственно.

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

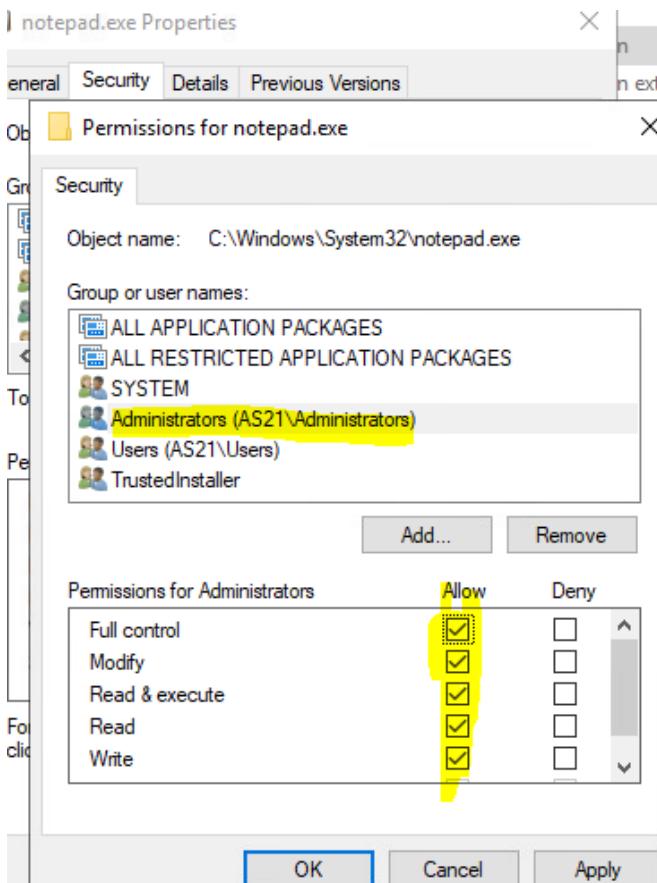
Переместите в общую папку Work исполняемый файл notepad.exe; обеспечьте возможность запуска notepad.exe из общей папки Work, но учтите, что никакие другие исполняемые файлы не должны запускаться из этой папки.

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

The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane is expanded to show Computer Configuration > Policies > Windows Settings > Security Settings. The main pane displays a table of rules:

Name	Type	Security Level	Description
%HKEY_LOCAL_MACHINE\Software\...	Path	Unrestricted	
%HKEY_LOCAL_MACHINE\Software\...	Path	Unrestricted	
\dc.as21.local\Work*.*	Path	Disallowed	
\dc\Work*.*	Path	Disallowed	
NOTEPAD.EXE (10.0.17763.475) Notepad ...	Hash	Unrestricted	

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

The screenshot shows the Group Policy Management Editor interface. The navigation pane is identical to the previous one. The main pane displays a table of rules, which appears to be the same as the one in the previous screenshot, indicating that the policy has been applied successfully.

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 Mongle

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

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

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

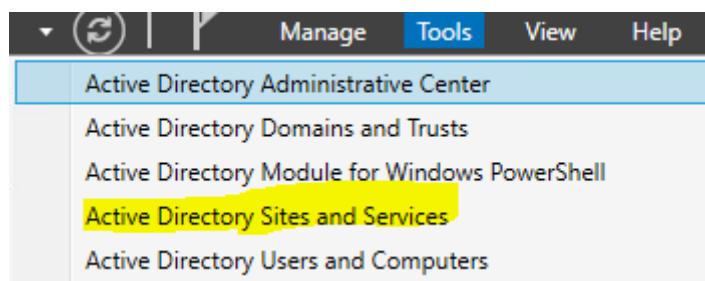
w32tm /config /syncfromflags:manual /manualpeerlist:dc.as21.local /reliable:yes

w32tm /resync /rediscover

Настройка временной зоны

Создаем сайт – Datacenter

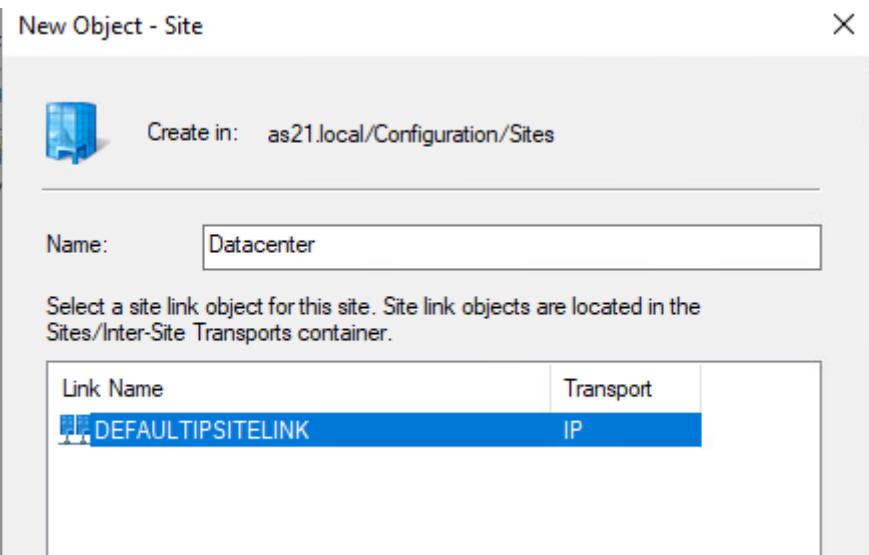
Открываем на DC оснастку Active Directory Sites and Services



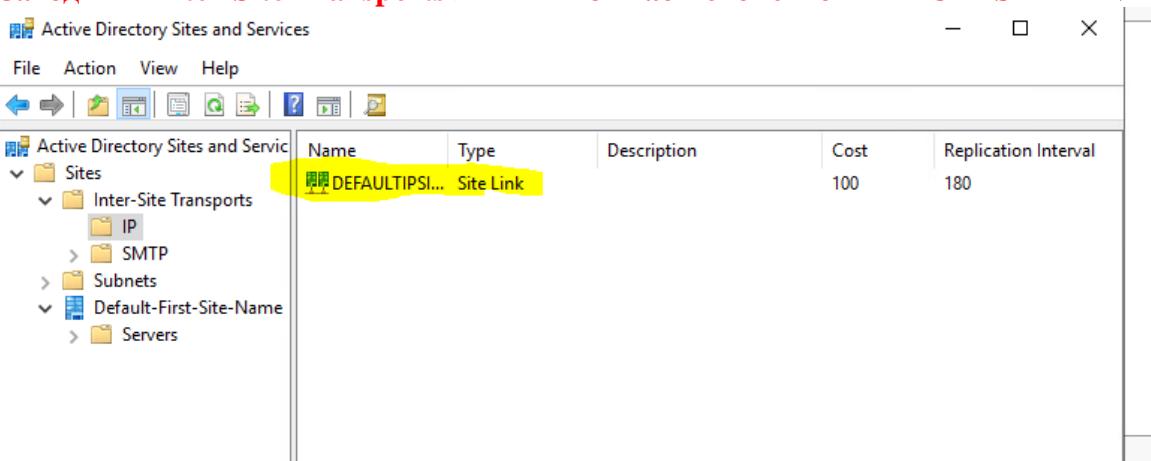
В разделе Sites создаем новый сайт – New Site

The screenshot shows the 'Active Directory Sites and Services' console. On the left, the tree view shows 'Sites' expanded, with 'Inter-Site Transports', 'Subnets', and 'Default-First-Site-Name' nodes. Under 'Default-First-Site-Name', there are 'Servers' with 'DC' and 'WINSRV1'. On the right, a list of sites is shown with columns 'Name' and 'Location'. A context menu is open over the 'Default-First-Site-Name' node, listing options: 'Delegate Control...', 'New Site...', 'Find...', 'New', 'All Tasks', and 'Refresh'. The 'New Site...' option is highlighted with a yellow box.

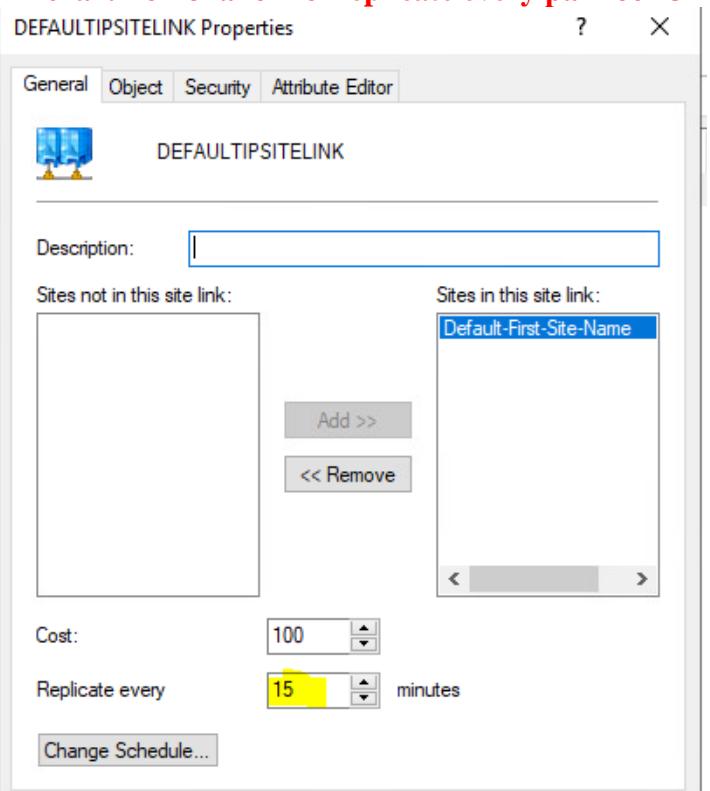
Выбираем для него соединение между сайтами по умолчанию



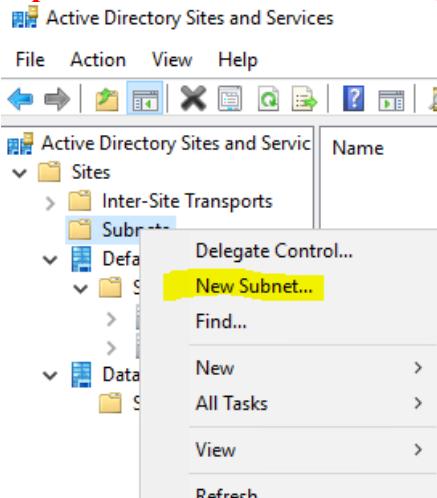
**Настроим наименьшую периодичность репликации – 15 минут
Заходим в Inter-Site Transports > IP и вызываем свойство DEFAULTSITELINK**



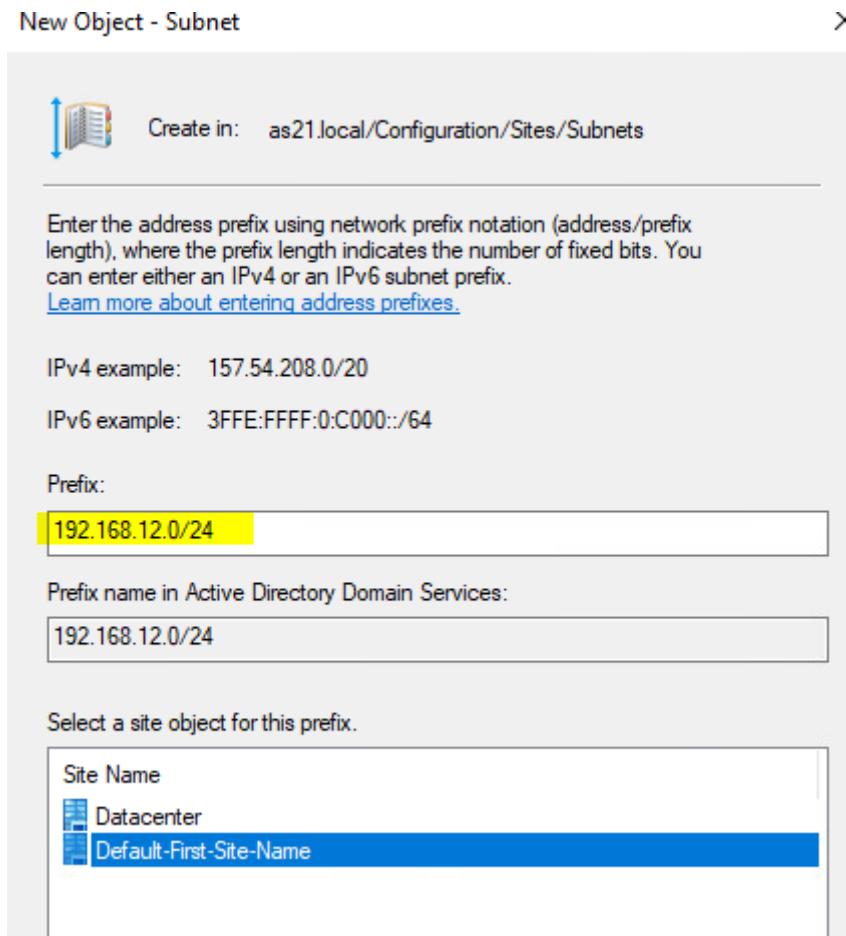
Выставляем значение Replicate every равное 15 минутам



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



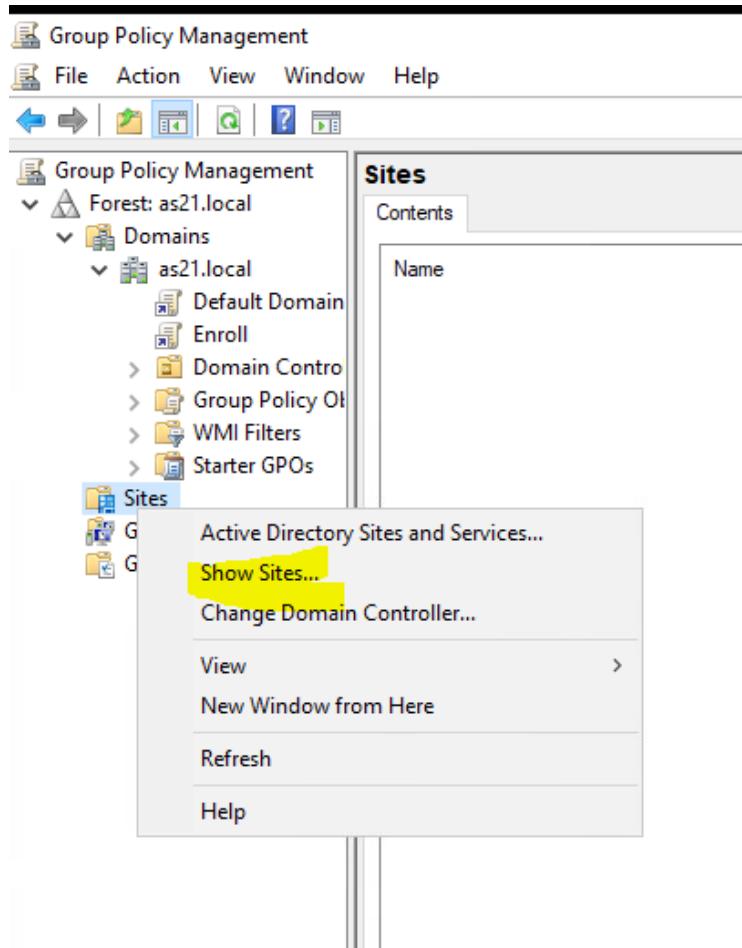
Пишем наименование сети формата сеть/маска. Назначаем её соответствующий сайт



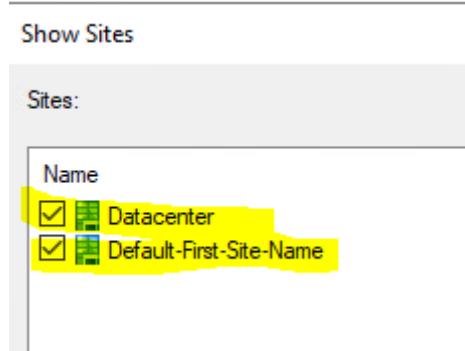
На всех компьютерах домена в ЦОД должна быть установлена зона "Moscow Standard Time"; эта настройка должна действовать всегда, в том числе, после перезагрузки.

Устанавливаем на DC зону Moscow Standard Time +3.

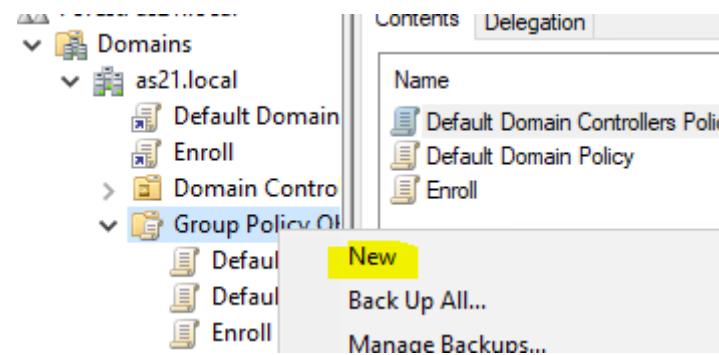
В оснастке Group Policy Management правой кнопкой по Sites и выбираем Show Sites



Выбираем оба сайта



Правой кнопкой по разделу Group Policy Objects

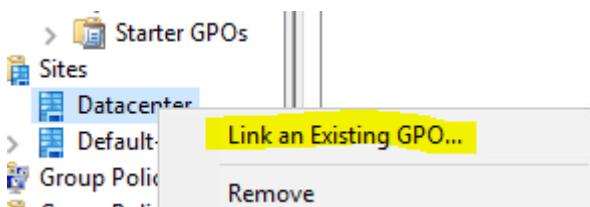


Создаем GPO для ЦОД (Datacenter): Computer Configuration > Preferences > Windows Settings > Registry -> New -> Registry Wizard

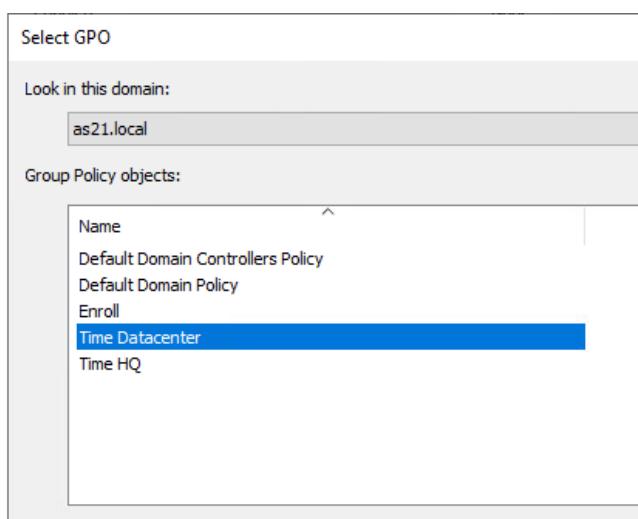
Создать «визардом» новую запись Local Computer выбираем ветку
HKLM\System\CurrentControlSet\Control\TimeZoneInformation\

Выбираем все параметры оттуда

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



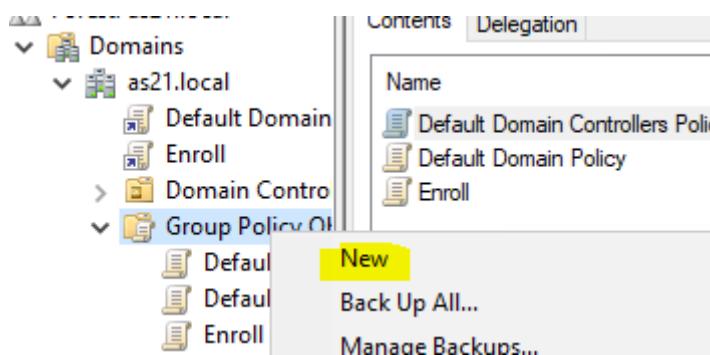
Выбираем наше GPO для ЦОД, созданное ранее



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

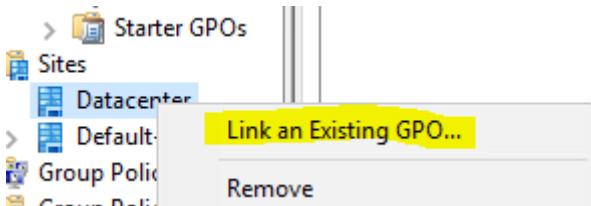


Создаем GPO для центрального офиса (Default-First-Site-Name): Computer Configuration > Preferences > Windows Settings > Registry -> New -> Registry Wizard

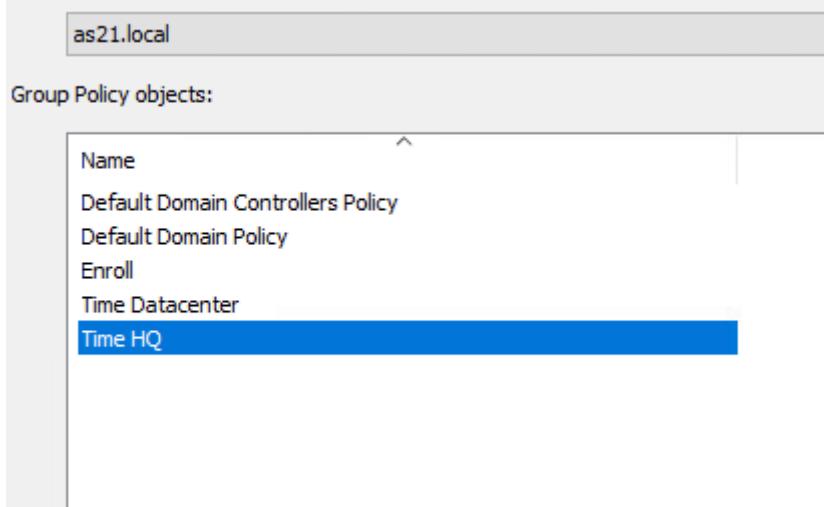
Создать «визардом» новую запись Local Computer выбираем ветку HKLM\System\CurrentControlSet\Control\TimeZoneInformation

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

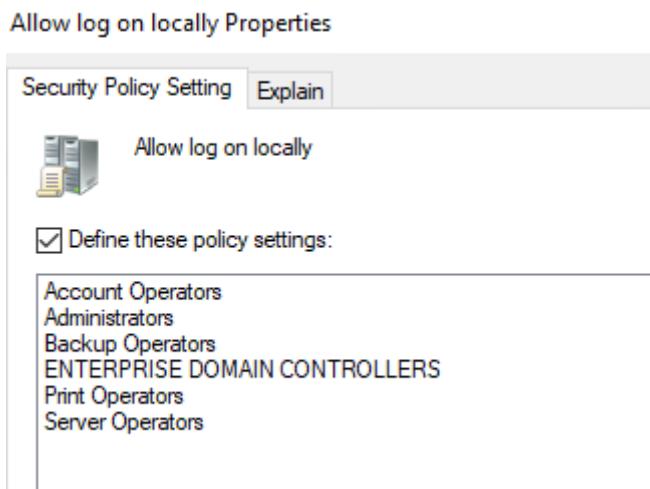
РАЗРЕШИТЬ GROUP3 ЗАХОДИТЬ НА DC

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

Allow log on locally Properties

Allow log on locally

Define these policy settings:

- Account Operators
- Administrators
- AS21\Group3
- Backup Operators
- ENTERPRISE DOMAIN CONTROLLERS
- Print Operators
- Server Operators

Add User or Group... Remove

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.

Profiles Properties

Profiles

Show All

General +

Permissions +

Settings -

Settings

Enable access-based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

Allow caching of share

Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

Enable BranchCache on the file share

BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

Encrypt data access

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

Leave Windows Installer and Group Policy Software Installation	Not configured	No
Only allow local user profiles	Not configured	No
Set roaming profile path for all users logging onto this computer	Enabled	No
Download roaming profiles on primary computers only	Not configured	No

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

The screenshot shows the 'Set roaming profile path for all users logging onto this computer' policy settings dialog box. The 'Enabled' radio button is selected. The 'Comment' field is empty. The 'Supported on:' field shows 'At least Windows Vista'. The 'User documentation' section contains the path '\\dc.as21.local\Profiles\%USERNAME%' in a yellow box, with a note below it: 'It is recommended to add %USERNAME% in the path to give each user different profile directory.' The 'Help' section describes the policy setting and its usage.

Set roaming profile path for all users logging onto this computer

Set roaming profile path for all users logging onto this computer

Comment:

Enabled Disabled

Supported on: At least Windows Vista

Options: Help:

Users logging onto this computer should use this roaming profile path:
\\dc.as21.local\Profiles\%USERNAME%

It is recommended to add %USERNAME% in the path to give each user different profile directory.

This policy setting specifies whether Windows should use the specified network path as the roaming user profile path for all users logging onto this computer. To use this policy setting, type the path to the network share in the form \\Computername\Sharename\\. It is recommended to use a path such as \\Computername\Sharename\%USERNAME% to give each user an individual profile folder. If not specified, all users logging onto this computer will use the same roaming profile folder as specified by this policy. You need to ensure that you have set the appropriate security on the folder to allow all

Идем сюда:

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

Ставим параметр Merge

Configure user Group Policy loopback processing mode

Configure user Group Policy loopback processing mode

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on:

At least Windows 2000

Options: Help:

Mode: Merge

This policy setting directs the system to apply the set of Group Policy objects for the computer to any user who logs on to a computer affected by this setting. It is intended for special-use computers, such as those in public places, laboratories, and classrooms, where you must modify the user setting based on the computer that is being used.

By default, the user's Group Policy Objects determine which user

Configure software installation policy processing	Not configured	No
Configure Start Menu preference extension policy processing	Not configured	No
Configure user Group Policy loopback processing mode	Enabled	No
Configure web-to-app linking with app URI handlers	Not configured	No

Теперь нужно ограничить распространение данной политики группой Group3

Выделяем политику и в окне Scope удаляем Authenticated Users

Group Policy Management

- Forest: as21.local
 - Domains
 - as21.local
 - Autonroll
 - Default Domain
 - Domain Time
 - No 1st aminatio
 - RDC
 - Roaming Profile**
 - AtomSkills
 - Domain Contro
 - Default Dom
 - PDC
 - Banner
 - File Bloc
 - Group3
 - PDC Tim
 - Office
 - Group Policy Obj
 - WMI Filters
 - Starter GPOs
 - Sites
 - Group Policy Modeling
 - Group Policy Results

Roaming Profiles

Scope Details Settings Delegation

Links

Display links in this location: as21.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
as21.local	No	Yes	as21.local

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name

Authenticated Users

Add... Remove Properties

WMI Filtering

И добавляем Group3

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name

Select this object type:
User, Group, or Built-in security principal

From this location:
as21.local

Enter the object name to select (examples):
group3

Advanced... OK

Add... Remove Properties

WMI Filtering

Security Filtering

The settings in this GPO can only apply to the following group:

A screenshot of the Group Policy Management console. A tree view on the left shows 'Forest: as21.local' with 'Domains' expanded, showing 'as21.local' which has 'Roaming Profile' selected. On the right, a 'Name' search bar at the top contains 'Group3 (AS21\Group3)'. Below it is a table titled 'Groups and users:' with a single row containing 'Group3 (AS21\Group3)'.

Переходим во вкладку Delegation

A screenshot of the Group Policy Management console. The 'Delegation' tab is highlighted in yellow. On the left, the same tree view is shown with 'Roaming Profile' selected. On the right, the 'Roaming Profiles' dialog shows the 'Delegation' tab selected. It displays a table titled 'Groups and users:' with several entries: 'Domain Admins (AS21\Domain Admins)', 'Enterprise Admins (AS21\Enterprise Admins)', 'ENTERPRISE DOMAIN CONTROLLERS', 'Group3 (AS21\Group3)', and 'SYSTEM'.

Добавляем Domain Computers с правами Read

A screenshot of the 'Add Group or User' dialog. In the 'Matching names:' section, 'Domain Computers' is selected. In the 'Permissions:' dropdown, 'Read' is selected. At the bottom, there are 'OK' and 'Cancel' buttons. The status bar at the bottom shows 'Enterprise Admins (AS21\Enterprise Admins)' and 'ENTERPRISE DOMAIN CONTROLLERS'.

План Б

Если план А не завелся

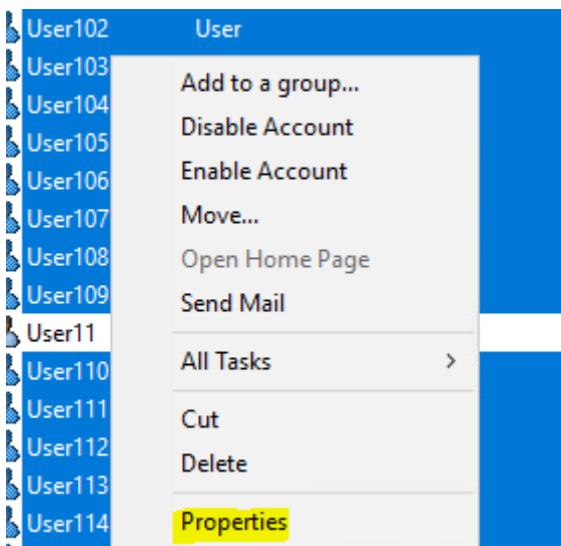
Удаляем GPO с плана А

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

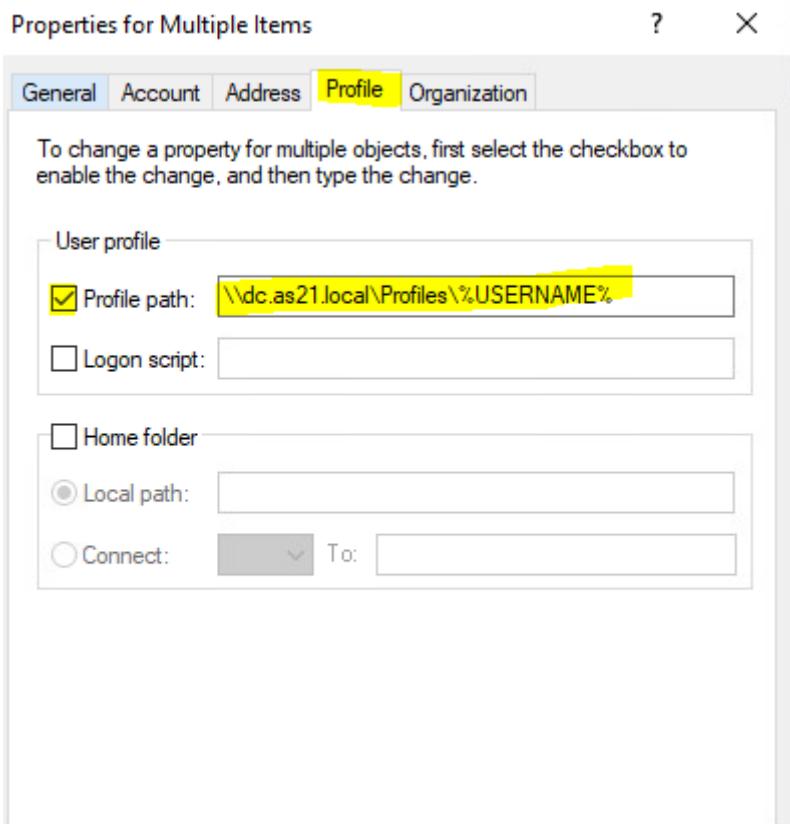
The screenshot shows the Windows Active Directory Users and Computers management console. On the left is a navigation tree for the domain 'as21.local'. In the main pane, a table lists 16 user accounts under the heading 'Group3'. The columns are 'Name', 'Type', and 'Description'. All users listed are of type 'User'. The users are: User1, User10, User100, User101, User102, User103, User104, User105, User106, User107, User108, User109, User11, User110, User111, User112, User113, and User114. The entire list of users is highlighted with a blue selection box.

Name	Type	Description
User1	User	
User10	User	
User100	User	
User101	User	
User102	User	
User103	User	
User104	User	
User105	User	
User106	User	
User107	User	
User108	User	
User109	User	
User11	User	
User110	User	
User111	User	
User112	User	
User113	User	
User114	User	

Вызываем их свойство



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



ROOT CA

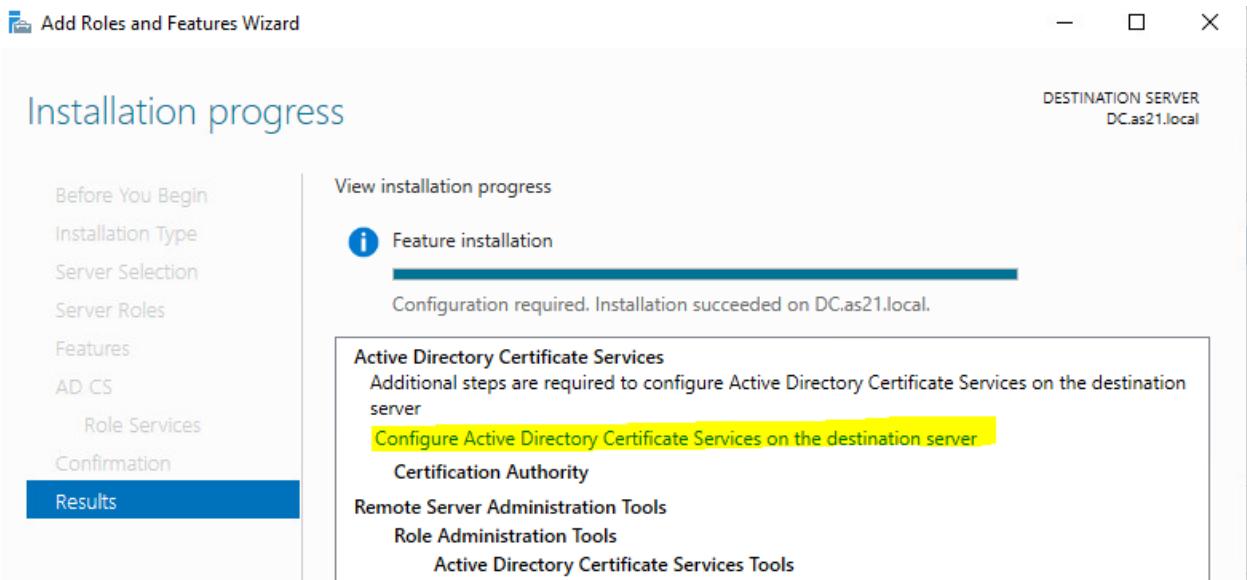
Настройте корневой центр сертификации на контроллере домена DC

Базовая настройка RootCA

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

Role services

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



Enterprise certification authorities (CAs) can use Active Directory simplify the management of certificates. Standalone CAs do not ! certificates.

Enterprise CA

Enterprise CAs must be domain members and are typically on certificate policies.

Standalone CA

Standalone CAs can be members or a workgroup or domain. ! DS and can be used without a network connection (offline).

Specify the type of the CA

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

Root CA

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

Subordinate CA

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

- i. Имя настраиваемого центра сертификации - RootCA.

Specify the name of the CA

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

Common name for this CA:

RootCA

Distinguished name suffix:

DC=as21,DC=local

Preview of distinguished name:

CN=RootCA,DC=as21,DC=local

- ii. Срок действия сертификата - 4 года.

Specify the validity period

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

4

Years



CA expiration Date: 7/28/2025 2:56:00 AM

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

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

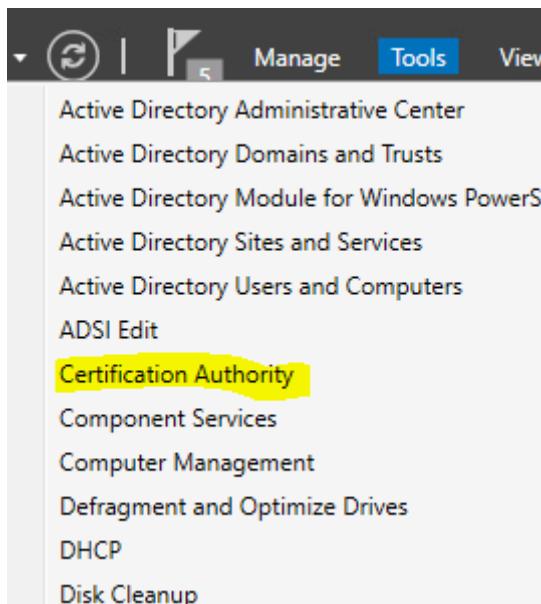
Registry Editor

File Edit View Favorites Help

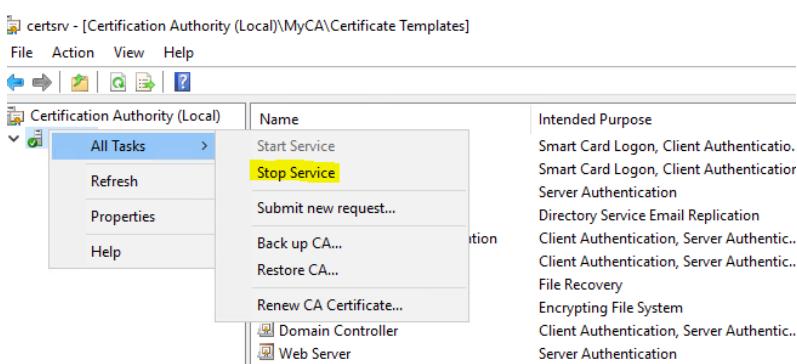
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\RootCA

	Name	Type	Data
	CRLPeriodUnits	REG_DWORD	0x00000001 (1)
	CRLPublicationURLs	REG_MULTI_SZ	65:C:\Windows\system32\CertSrv\
	DSConfigDN	REG_SZ	CN=Configuration,DC=as21,DC=local
	DDomainDN	REG_SZ	DC=as21,DC=local
	EKUOIDsForPublishExpiredCertInCRL	REG_MULTI_SZ	1.3.6.1.5.5.7.3.3 1.3.6.1.4.1.311.61.1.1
	Enabled	REG_DWORD	0x00000001 (1)
	EnforceX500NameLengths	REG_DWORD	0x00000001 (1)
	ForceTeletex	REG_DWORD	0x00000012 (18)
	HighSerial	REG_DWORD	0x00000029 (41)
	InterfaceFlags	REG_DWORD	0x00000641 (1601)
	KRACertCount	REG_DWORD	0x00000000 (0)
	KRACertHash	REG_MULTI_SZ	
	KRAFlags	REG_DWORD	0x00000000 (0)
	LogLevel	REG_DWORD	0x00000003 (3)
	MaxIncomingAllocSize	REG_DWORD	0x00010000 (65536)
	MaxIncomingMessageSize	REG_DWORD	0x00010000 (65536)
	PolicyFlags	REG_DWORD	0x00000000 (0)
	Security	REG_BINARY	01 00 14 84 20 01 00 00 30 01 00 00 1
	SetupStatus	REG_DWORD	0x00000001 (1)
	SignedAttributes	REG_MULTI_SZ	
	SubjectTemplate	REG_MULTI_SZ	
	UseDS	REG_DWORD	0x00000001 (1)
	ValidityPeriod	REG_SZ	Years
	ValidityPeriodUnits	REG_DWORD	0x00000003 (3)
	ViewAgeMinutes	REG_DWORD	0x00000010 (16)

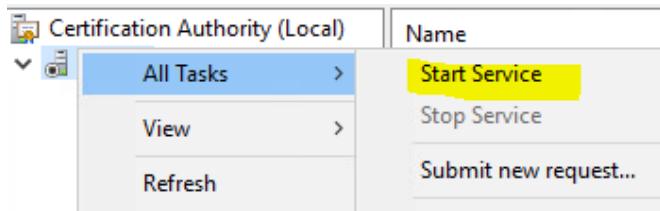
Идем в оснастку Certification Authority



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.

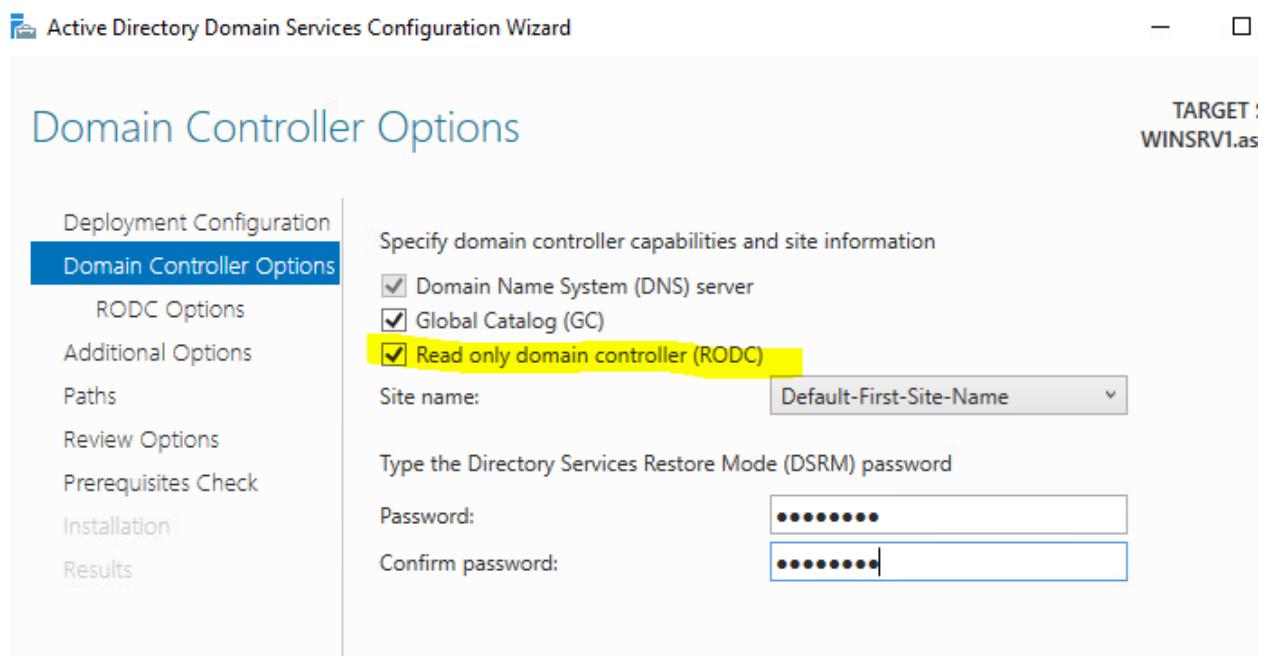
НАСТРОЙКА RODC

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.

The screenshot shows the 'Add a Domain Controller' wizard. Step 1 of 3. The user has selected the radio button for 'Add a domain controller to an existing domain'. Below this, there is a section titled 'Specify the domain information for this operation' with a 'Domain:' field containing 'as21.local' and a 'Select...' button. Further down, there is a section titled 'Supply the credentials to perform this operation' with a field containing 'AS21\Administrator (Current user)' and a 'Change...' button.

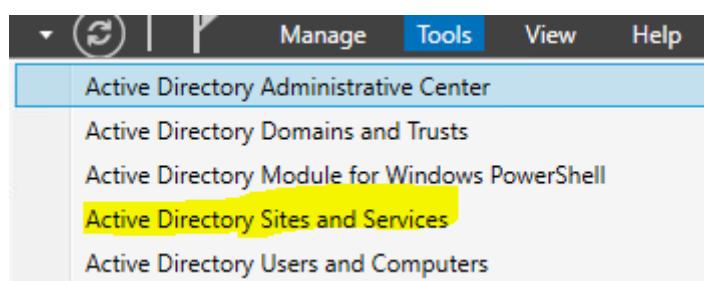


Настройка сайтов

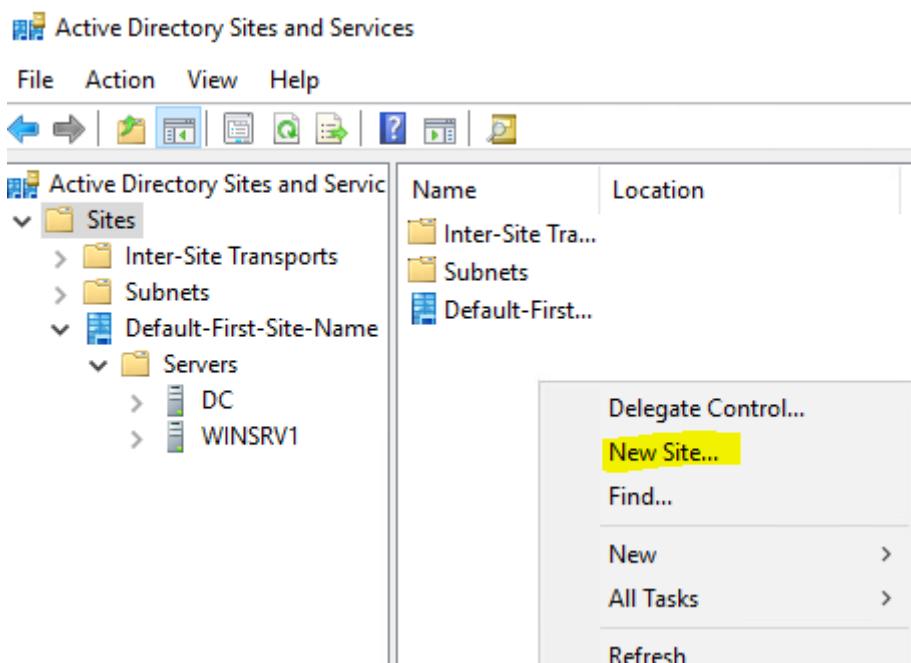
Сайты основного и дополнительного контроллеров домена AS21.local должны быть разными.

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

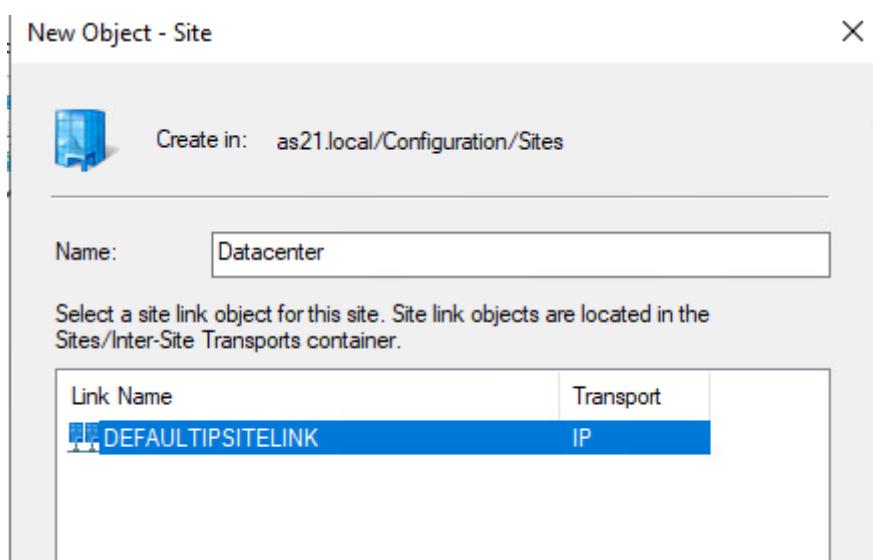
Открываем на DC оснастку Active Directory Sites and Services



В разделе Sites создаем новый сайт – New Site

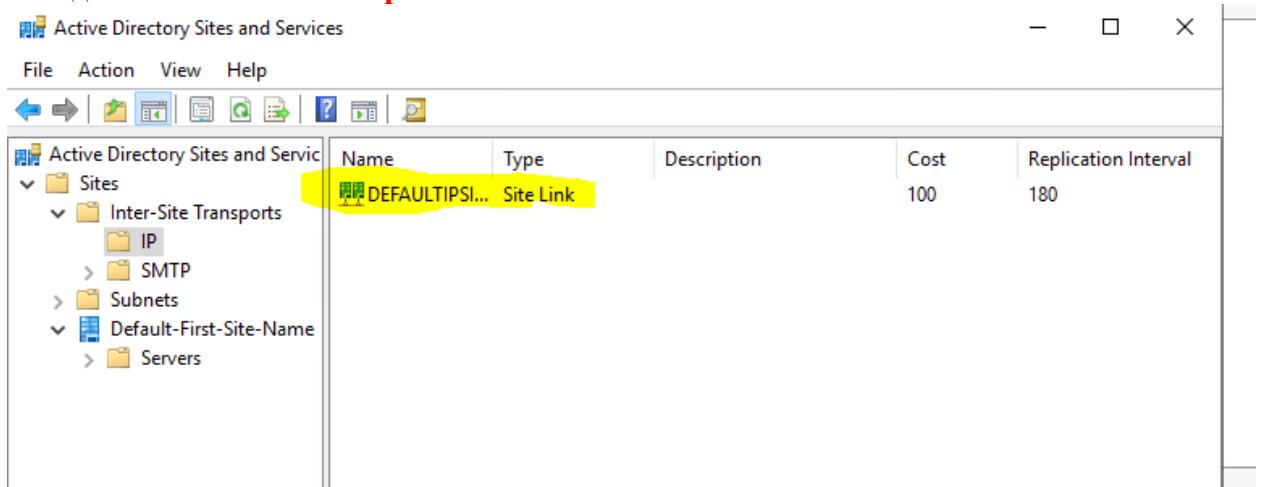


Выбираем для него соединение между сайтами по умолчанию

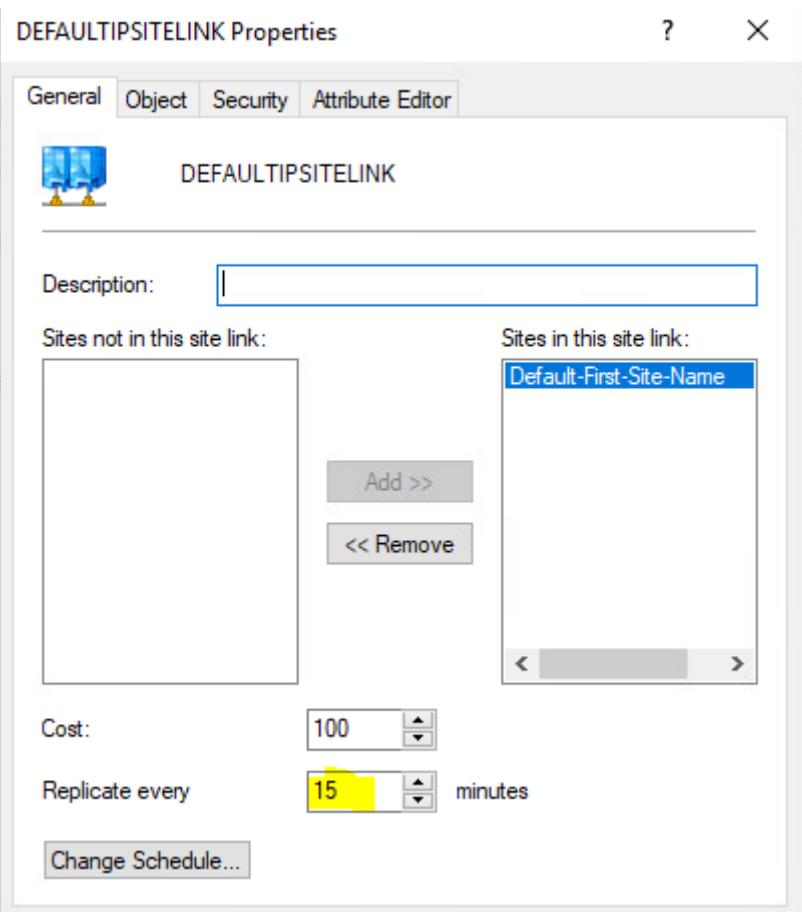


Настроим наименьшую периодичность репликации – 15 минут

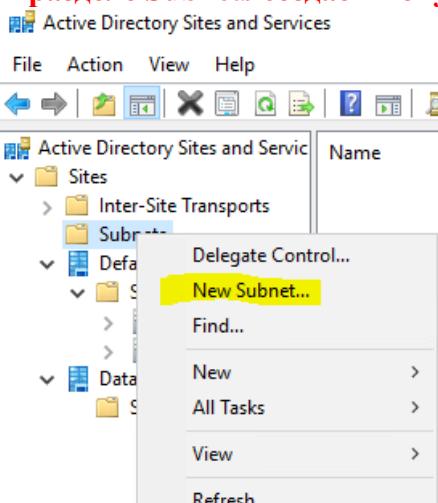
Заходим в Inter-Site Transports > IP и вызываем свойство DEFAULTSITELINK



Выставляем значение Replicate every равное 15 минутам



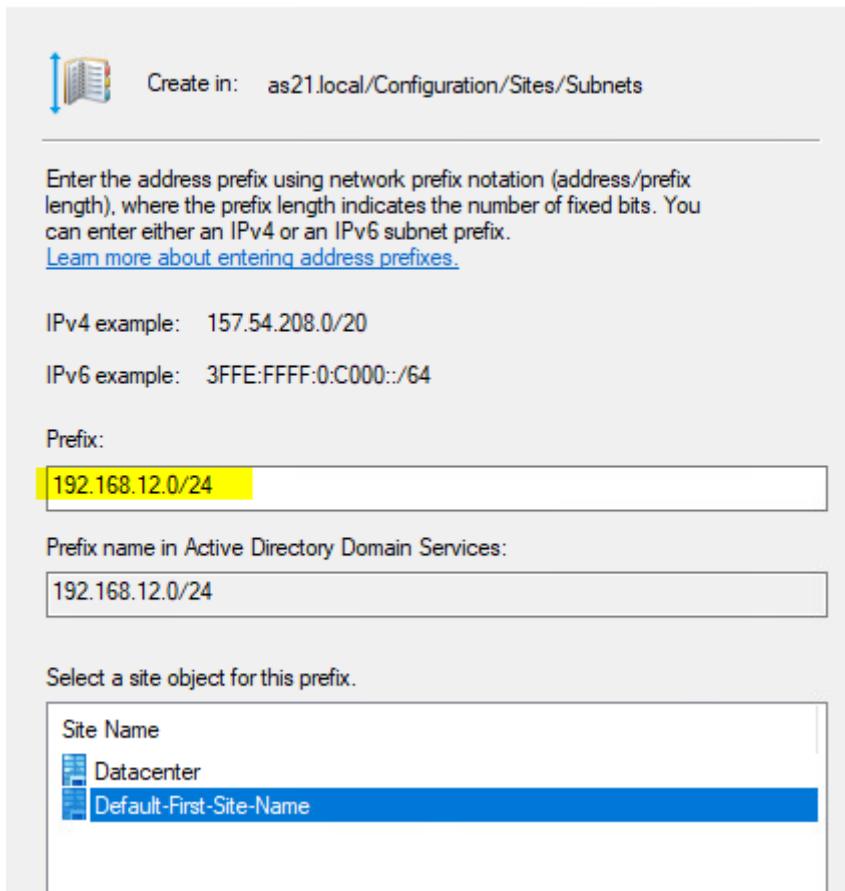
**Создаем и закрепляем подсети за сайтами (все)
В разделе Subnets создаем новую подсеть - New Subnet**



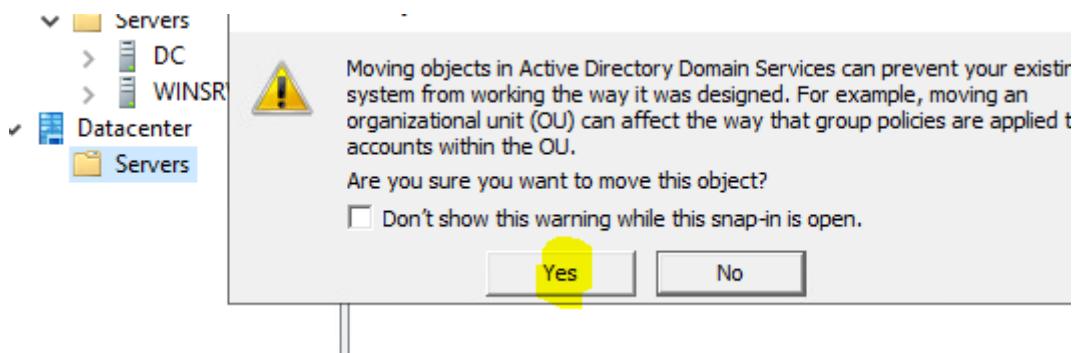
Пишем наименование сети формата сеть/маска. Назначаем её соответствующий сайт

New Object - Subnet

X



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

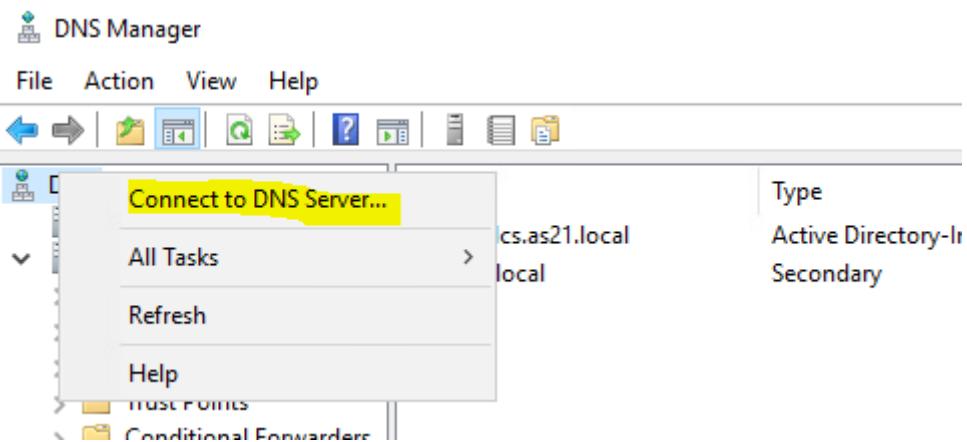


В случае появления доменных Windows-клиентов в ЦОД, они должны в первую очередь обращаться к дополнительному контроллеру, и только если он не доступен - к основному.

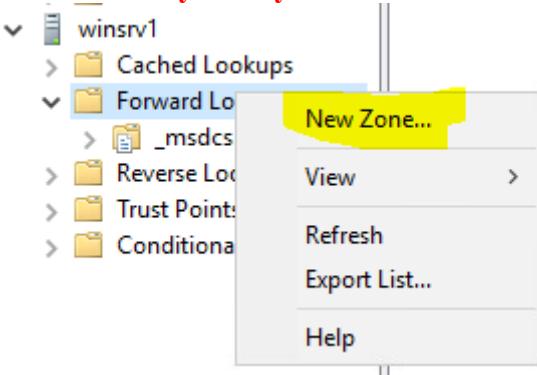
Настройка DNS на WINSRV1

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

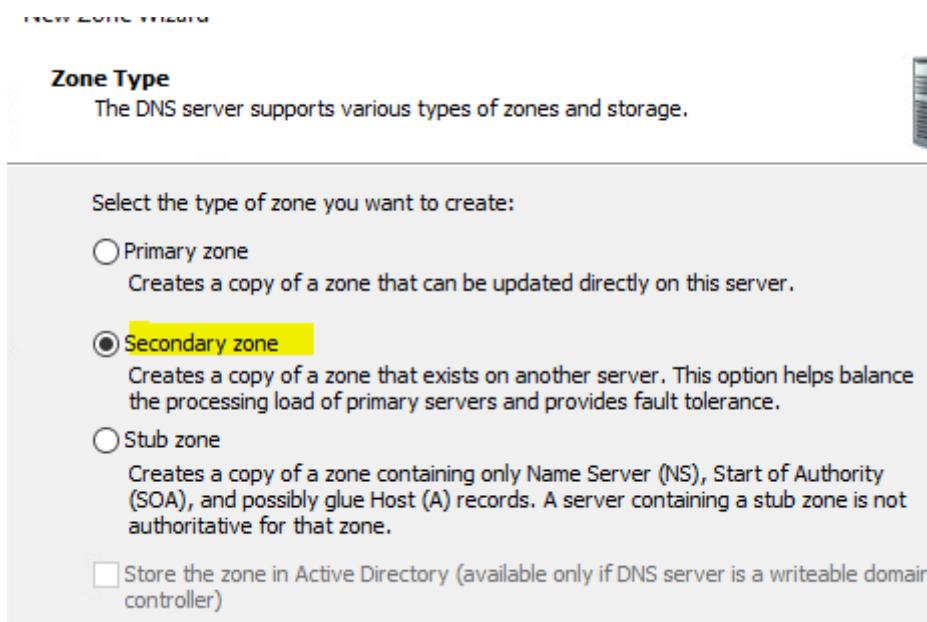
Открываем на DC оснастку DNS. Подключаемся к серверу WINSRV1



Создаем новую зону



Выбираем тип зоны Secondary zone



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

or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:

as21.local

[Browse...](#)

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

Master Servers:

IP Address	Server FQDN	Validated
dc.as21.local		
<input checked="" type="checkbox"/> 192.168.12.1	dc.as21.local	OK
<input checked="" type="checkbox"/> fe80::256d:27ff%1	dc.as21.local	OK

[Delete](#) [Up](#) [Down](#)

Обязательно настроить Round Robin на WINSRV1

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

WINSRV1 Properties

Debug Logging Event Logging Monitoring Security
Interfaces Forwarders Advanced Root Hints

Server version number:
10.0 17763 (0x4563)

Server options:
 Disable recursion (also disables forwarders)
 Enable BIND secondaries
 Fail on load if bad zone data
 Enable round robin
 Enable netmask ordering
 Secure cache against pollution

Name checking: Multibyte (UTF8)
Load zone data on startup: From Active Directory and registry
 Enable automatic scavenging of stale records

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:

Server Name	IPv4 Address	Manageability	Last Update	Windows Activi
DC	192.168.12.1	Online - Performance counters not started	7/28/2021 2:56:40 PM	Not activated
WINDMZ	10.0.100.2	Online - Performance counters not started	7/28/2021 2:56:41 PM	Not activated
WINSRV1	10.0.3.1	Online - Performance counters not started	7/28/2021 2:56:39 PM	Not activated
WINSRV2	10.0.100.1	Online - Performance counters not started	7/28/2021 2:56:39 PM	Not activated

Role services

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

Active Directory Certificate Services

Additional steps are required to configure Active Directory Certificate Services on this server

[Configure Active Directory Certificate Services on the destination server](#)

Certification Authority

Remote Server Administration Tools

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

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

To install remotely you must enter credentials.

Credentials: [Change...](#)

Enterprise certification authorities (CAs) can use Active Directory to simplify the management of certificates. Standalone CAs do not use Active Directory to manage certificates.

Enterprise CA

Enterprise CAs must be domain members and are typically organized by certificate policies.

Standalone CA

Standalone CAs can be members of a workgroup or domain. They do not use Active Directory and can be used without a network connection (offline).

Root CA

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

Subordinate CA

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

Common name for this CA:

SubCA

Distinguished name suffix:

DC=as21,DC=local

Preview of distinguished name:

CN=SubCA,DC=as21,DC=local

Send a certificate request to a parent CA:

Select:

CA name

Computer name

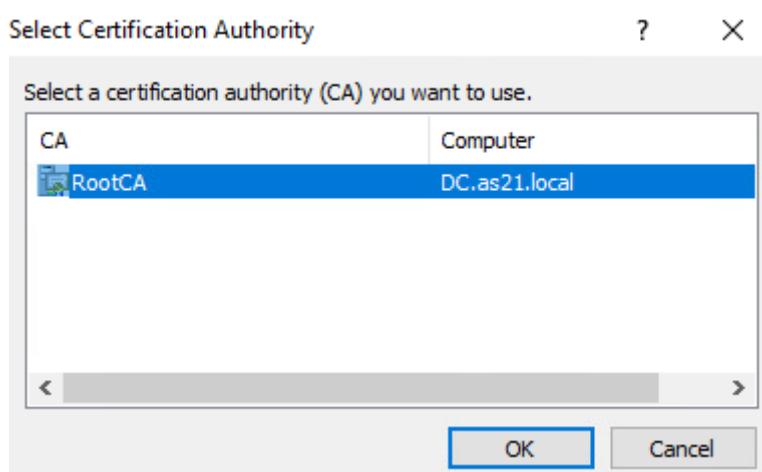
Parent CA:

Select...

Save a certificate request to file on the target machine:

File name: C:\WINSRV1.as21.local_as21-WINSRV1-CA.req

i You must manually get a certificate back from the parent CA to make this CA operational.



Настройка CRL на SubCA

Открываем реестр на SubCA (regedit)

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

Меняем значение CRLDeltaPeriodUnits на 5

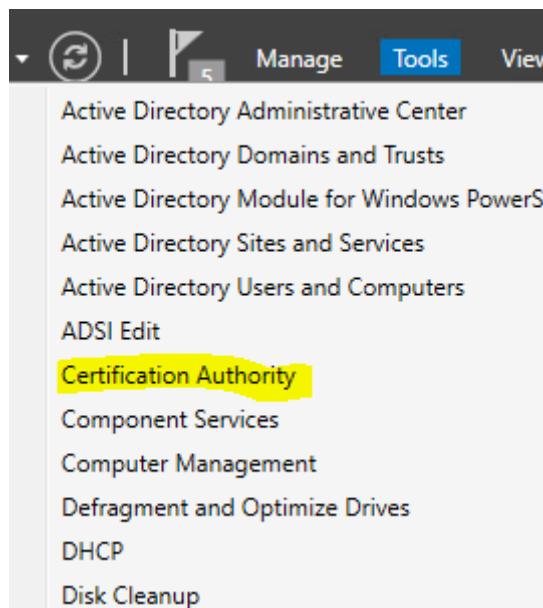
Registry Editor

File Edit View Favorites Help

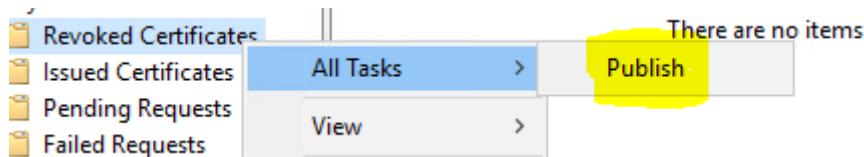
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\SubCA

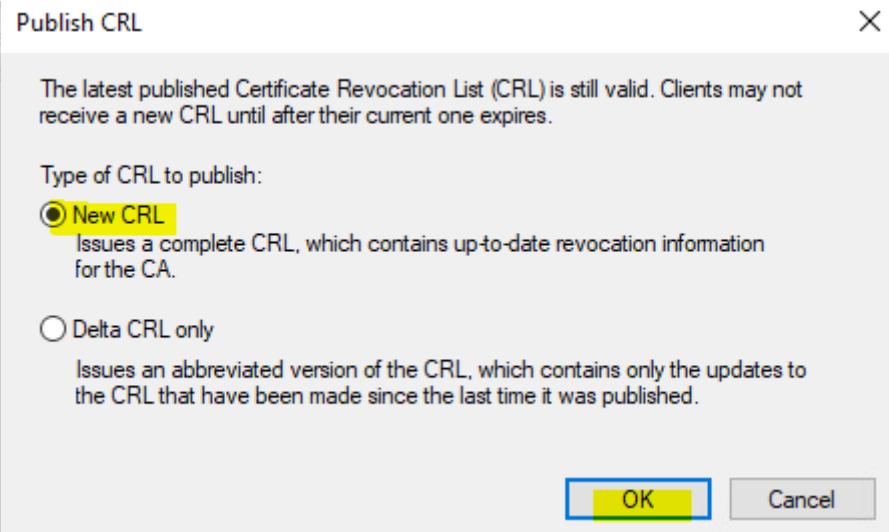
Name	Type	Data
CAXchgValidityPeriodUnits	REG_DWORD	0x00000001 (1)
CertEnrollCompatible	REG_DWORD	0x00000000 (0)
ClockSkewMinutes	REG_DWORD	0x0000000a (10)
CommonName	REG_SZ	SubCA
CRLDeltaNextPublish	REG_BINARY	26 11 4a b7 4e 8c d7 01
CRLDeltaOverlapPeriod	REG_SZ	Minutes
CRLDeltaOverlapUnits	REG_DWORD	0x00000000 (0)
CRLDeltaPeriod	REG_SZ	Days
CRLDeltaPeriodUnits	REG_DWORD	0x00000005 (5)
CRLEditFlags	REG_DWORD	0x00000100 (256)
CRLFlags	REG_DWORD	0x00000002 (2)
CRLNextPublish	REG_BINARY	26 91 1d 0c e1 8d d7 01
CRLOverlapPeriod	REG_SZ	Hours
CRLOverlapUnits	REG_DWORD	0x00000000 (0)
CRLPeriod	REG_SZ	Weeks
CRLPeriodUnits	REG_DWORD	0x00000001 (1)
CRLPublicationURLs	REG_MULTI_SZ	65:C:\Windows\system32\CertSnv\CertEnroll\%3
DSConfigDN	REG_SZ	CN=Configuration,DC=as21,DC=local
DSDomainDN	REG_SZ	DC=as21,DC=local
EKUOIDsForPublishExpiredCertInCRL	REG_MULTI_SZ	1.3.6.1.5.7.3.3 1.3.6.1.4.1.311.61.1.1

Идем в оснастку Certification Authority



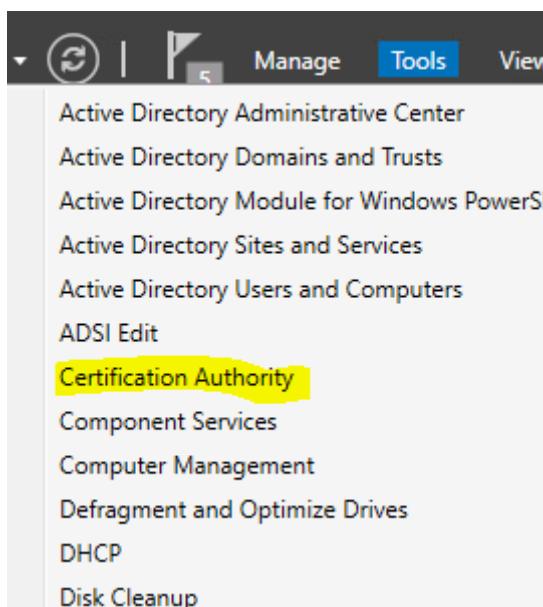
Правую кнопку по Revoked Certificates > All Tasks > Publish

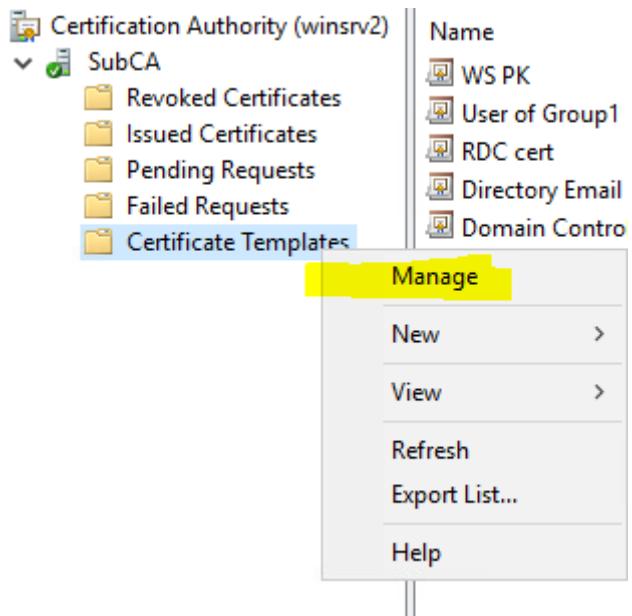




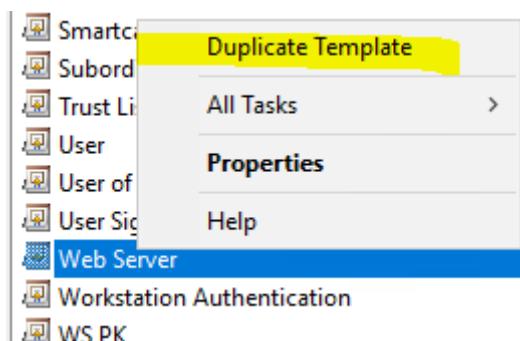
ПОДГОТОВКА ШАБЛОНА ДЛЯ WEB ДОСТУПА

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

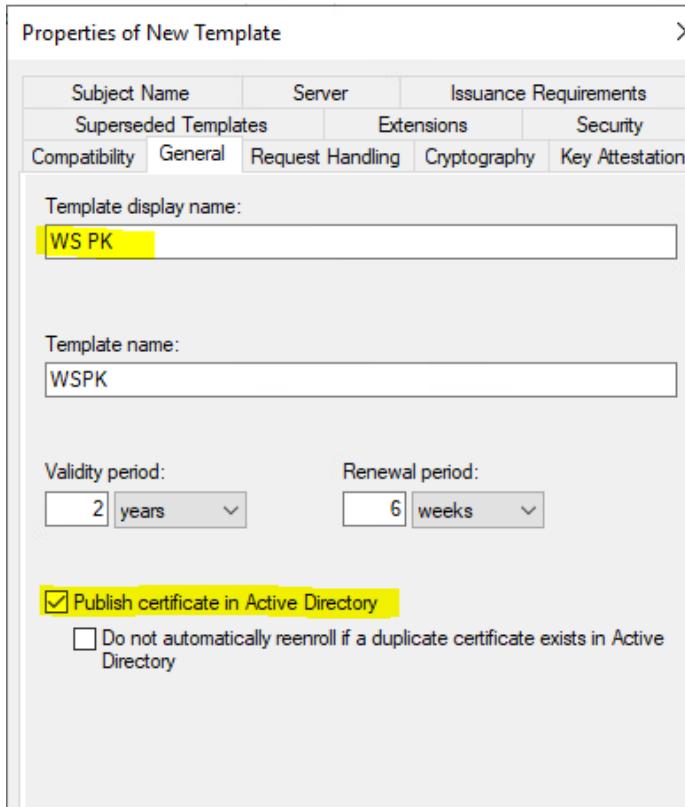




Сделаем клон шаблона Web Server



Выполним настройки нового шаблона

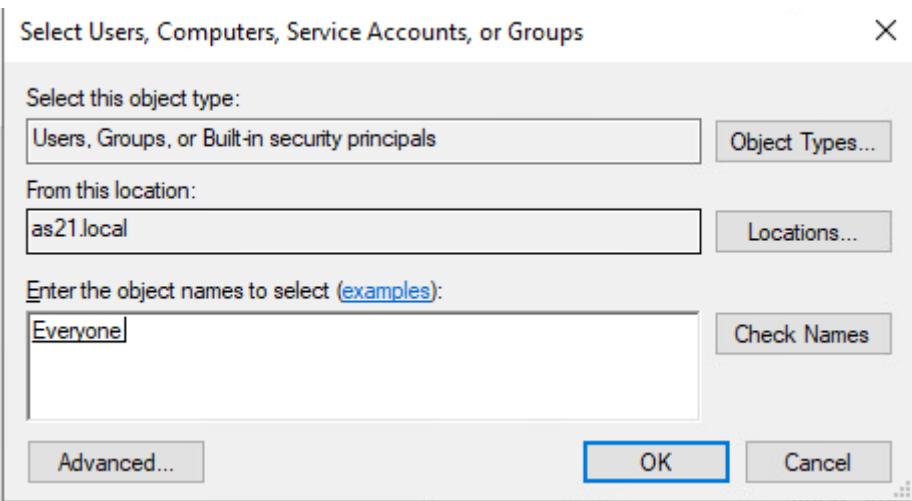


Properties of New Template

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

Properties of New Template

Subject Name	Server	Issuance Requirements
Compatibility	General	Request Handling Cryptography Key Attestation
Superseded Templates	Extensions	Security
<p>Group or user names:</p> <ul style="list-style-type: none"> Authenticated Users Administrator Domain Admins (AS21\Domain Admins) Enterprise Admins (AS21\Enterprise Admins) <p>Add... Remove</p> <p>Permissions for Authenticated Users</p> <p>Allow Deny</p>		



Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (AS21\Domain Admins)
- Enterprise Admins (AS21\Enterprise Admins)
- Everyone

Permissions for Everyone	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>

SubCA

- Revoked Certificates
- Issued Certificates
- Pending Requests
- Failed Requests
- Certificate Template

Manage > Certification Authority

- Certificate Template to Issue
- Controller
-
-
- Certification Authority

<input type="checkbox"/> WS PK	Server Authentication
<input type="checkbox"/> User of Group1	Client Authentication
<input type="checkbox"/> RDC cert	Client Authentication
<input type="checkbox"/> Directory Email Replication	Directory Services
<input type="checkbox"/> Domain Controller Authentication	Client Authentication
<input type="checkbox"/> Client Authentication	Client Authentication
<input type="checkbox"/> Encrypting File System	Client Authentication
<input type="checkbox"/> <All>	Client Authentication
<input type="checkbox"/> Microsoft Trust	Microsoft Trust



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:

Server Name	IPv4 Address	Manageability
WINSRV1	10.0.3.1	Online - Performance counters not sta...
WINSRV2	10.0.100.1	Online - Performance counters not sta...

Конфигурируем в режиме Remote Desktop Services installation:

Select installation type

DESTINATION SERVER
No servers are selected.

Before You Begin

Installation Type

Deployment Type

Deployment Scenario

Role Services

RD Connection Broker

RD Web Access

RD Virtualization Host

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

Role-based or feature-based installation

Configure a single server by adding roles, role services, and features.

Remote Desktop Services installation

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Before You Begin

Install

Deployment Type

Deployment Scenario

Role Services

RD Connection Broker

Remote Desktop Services can be configured ac

Standard deployment

A standard deployment allows you to deplo

Quick Start

A Quick Start allows you to deploy Remote I

Select deployment scenario

Before You Begin

Installation Type

Deployment Type

Deployment Scenario

Server Selection

Confirmation

Completion

Remote Desktop Services can be configured to allow users to connect to virtual c
programs, and session-based desktops.

Virtual machine-based desktop deployment

Virtual machine-based desktop deployment allows users to connect to virtual
that include published RemoteApp programs and virtual desktops.

Session-based desktop deployment

Session-based desktop deployment allows users to connect to session collect
published RemoteApp programs and session-based desktops.

Выбираем WINSRV2 как сервер брокера

Specify RD Connection Broker server

DESTINATION SERVER
Standard deployment selected

Before You Begin

Installation Type

Deployment Type

Deployment Scenario

Role Services

RD Connection Broker

RD Web Access

RD Session Host

Confirmation

Completion

Select the servers from the server pool on which to install the RD Connection Broker role service.

Server Pool		
Name	IP Address	Operating System
WINSRV2.as21.local	10.0.100.1	Windows Server 2012 R2 Standard
WINSRV1.as21.local	10.0.3.1	Windows Server 2012 R2 Standard

Selected

Computer
AS21.LOCAL (1)
WINSRV2

Выбираем WINSRV1 как сервер веб доступа

Specify RD Web Access server

DESTIN/ Standard deploy

The screenshot shows the 'Specify RD Web Access server' step of the wizard. On the left, a navigation pane lists steps: Before You Begin, Installation Type, Deployment Type, Deployment Scenario, Role Services, RD Connection Broker, RD Web Access (which is selected), RD Session Host, and Confirmation. The main area contains a 'Server Pool' table with two rows:

Name	IP Address	Operating
WINSRV2.as21.local	10.0.100.1	
WINSRV1.as21.local	10.0.3.1	

A checkbox labeled 'Install the RD Web Access role service on the RD Connection Broker server' is present. To the right, a 'Selected' pane shows 'Computer' with 'AS21.LOCAL (1)' expanded, and 'WINSRV1' highlighted in yellow.

Выбираем WINSRV2 как сервер терминалов

Specify RD Session Host servers

DESTIN/ Standard deploy

The screenshot shows the 'Specify RD Session Host servers' step of the wizard. On the left, a navigation pane lists steps: Before You Begin, Installation Type, Deployment Type, Deployment Scenario, Role Services, RD Connection Broker, RD Web Access, RD Session Host (which is selected), and Confirmation. The main area contains a 'Server Pool' table with two rows:

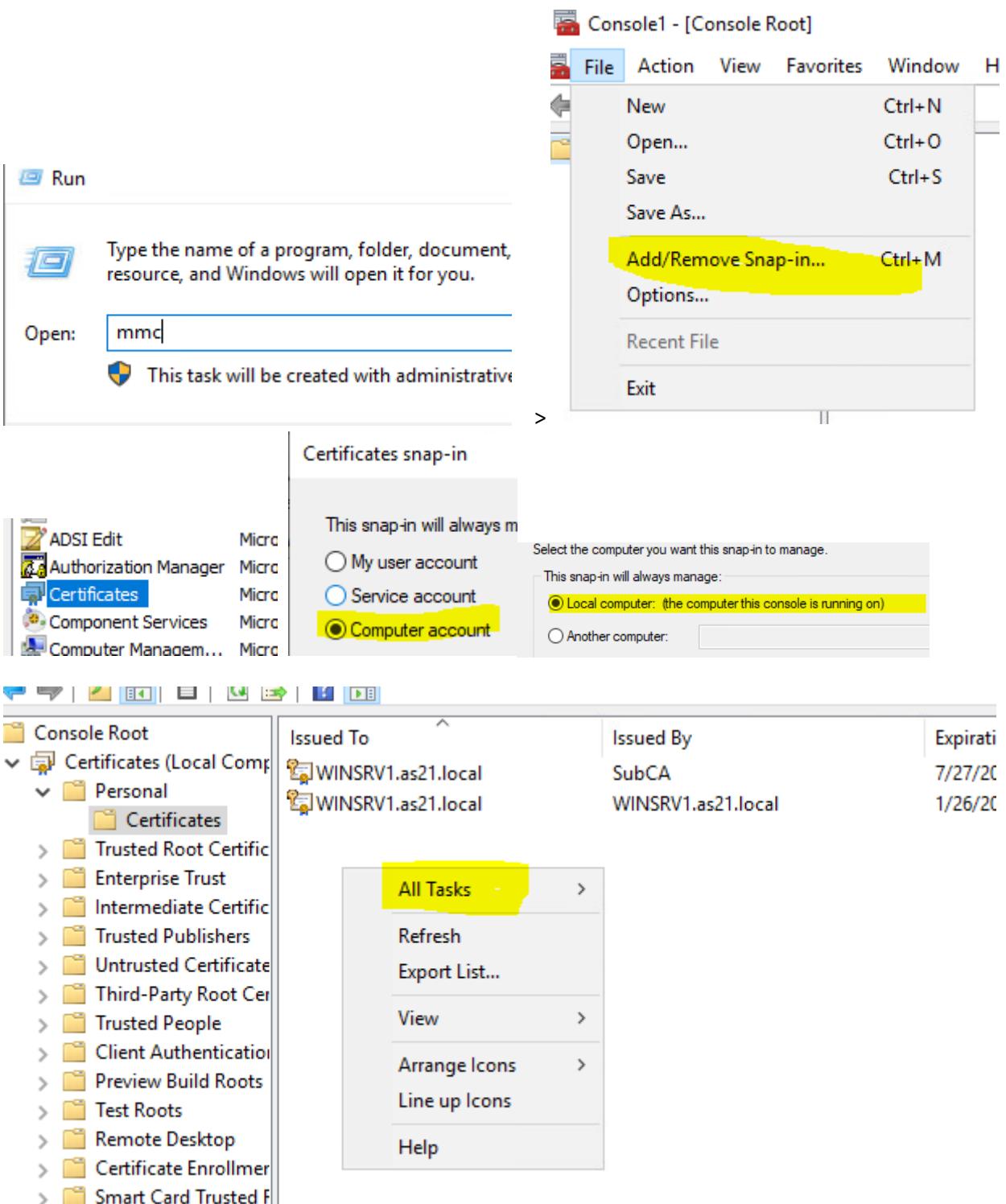
Name	IP Address	Operating
WINSRV2.as21.local	10.0.100.1	
WINSRV1.as21.local	10.0.3.1	

A 'Selected' pane on the right shows 'Computer' with 'AS21.LOCAL (1)' expanded, and 'WINSRV2' highlighted in yellow.

Настройка web доступа по сертификатам

Сконфигурируйте web-доступ к службам терминалов сервера.

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



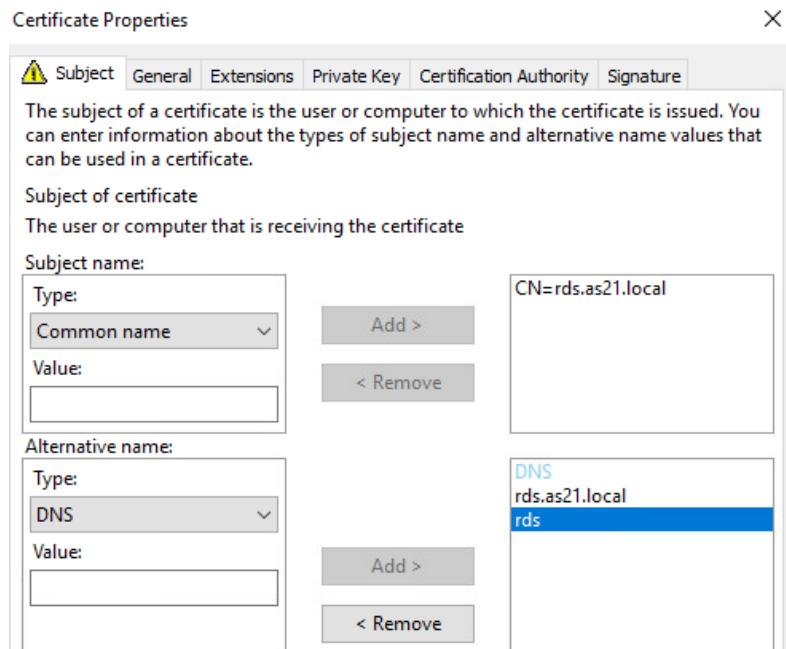
All Task > Request New Certificate

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

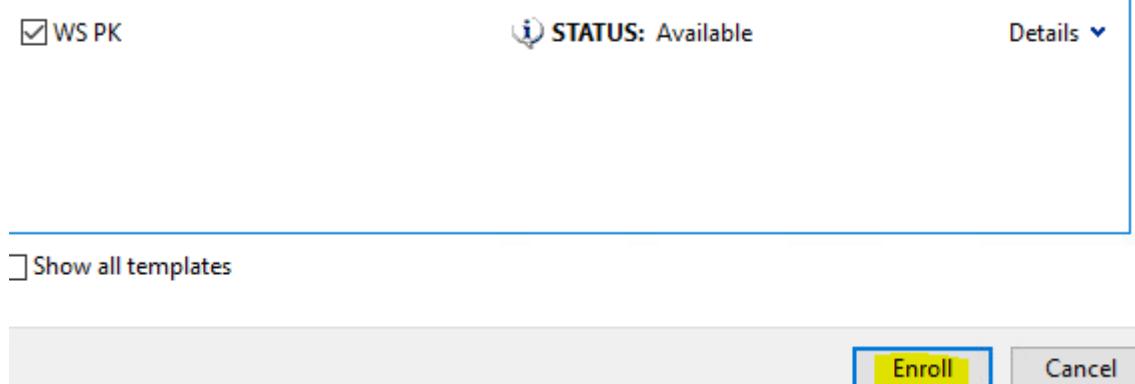
<input checked="" type="checkbox"/> WS PK	STATUS: Available	Details ▾
⚠ More information is required to enroll for this certificate. Click here to configure settings.		

Сверху заводим Common Name – rds.as21.local

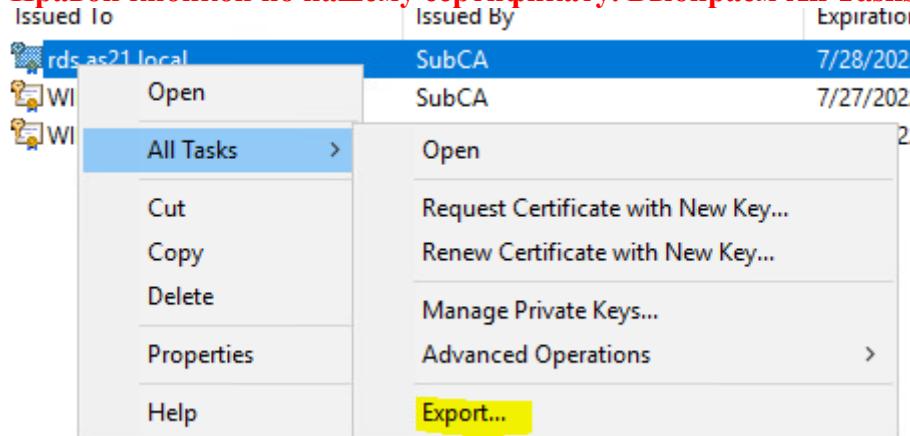
Внизу заводим DNS rds.as21.local и rds



Выпускаем сертификат



Правой кнопкой по нашему сертификату. Выбираем All Tasks > Export



При экспорте выбираем разрешение экспорта закрытого ключа

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

Yes, export the private key

Выгружаем все параметры – Export all extended properties

- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
- Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)
- Include all certificates in the certification path if possible
- Delete the private key if the export is successful
- Export all extended properties
- Enable certificate privacy
- Microsoft Serialized Certificate Store (.SST)

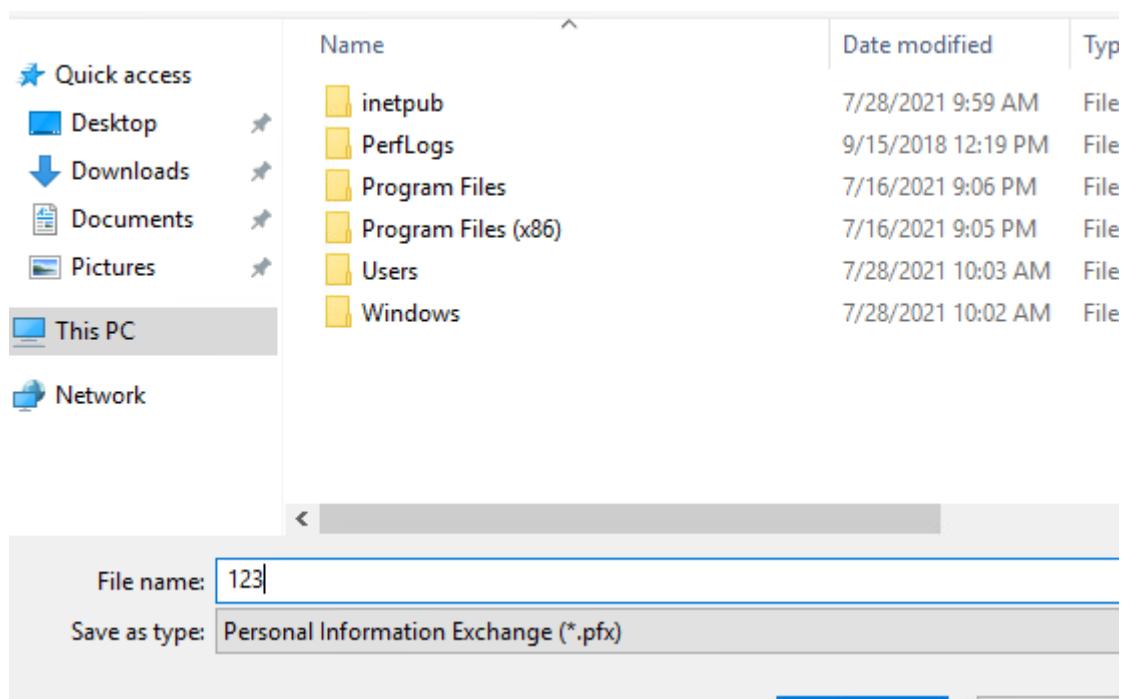
Вводим пароль, выбираем SHA256

Password:
•••

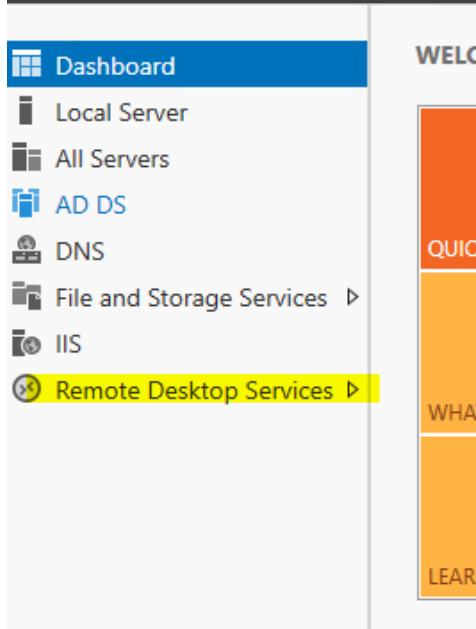
Confirm password:
•••

Encryption:

Сохраняем файл (не забываем куда)



Идем в сервер менеджер в консоль RDS



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

Переходим на вкладку Certificates и выбираем Select existing certificate

Configure the deployment

Show All

- RD Gateway +
- RD Licensing +
- RD Web Access +
- Certificates** -

Manage certificates

A Remote Desktop Services deployment requires certificates for server authentication, single sign-on, and establishing secure connections.

Current deployment certificate level is **Not Configured**

What is a certificate level?

Role Service	Level	Status	State
RD Connection Broker - Enable Sinc	Not Configured	--	
RD Connection Broker - Publishing	Not Configured	--	
RD Web Access	Not Configured	--	
RD Gateway	Unknown	--	

Subject name: Not Applicable
[View Details](#)

This certificate is required for server authentication to the Remote Desktop Services deployment.

You can update this certificate by creating a new certificate or by selecting an existing certificate.

[Create new certificate...](#) [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**

Apply the certificate that is stored on the RD Connection Broker server

Password:

Choose a different certificate

Certificate path: [Browse...](#)

Password:

Allow the certificate to be added to the Trusted Root Certification Authorities certificate store on the destination computers

Должно получиться следующее. Нажимаем Apply

⚠ Only a single certificate can be added to a specific role service at a time. To add certificates to additional role services, click Apply or OK.

Current deployment certificate level is **Not Configured**
What is a certificate level?

Role Service	Level	Status	State
RD Connection Broker - Enable Single Sign-On	Not Configured	--	Ready to Assign
RD Connection Broker - Publishing	Not Configured	--	
RD Web Access	Not Configured	--	
RD Gateway	Unknown	--	

Subject name: Not Applicable

[View Details](#)

This certificate is required for server authentication to the Remote Desktop Services deployment.

You can update this certificate by creating a new certificate or by selecting an existing certificate.

OK

Cancel

Apply

Повторяем для всех трех верхних ролей. Должно получиться следующее:

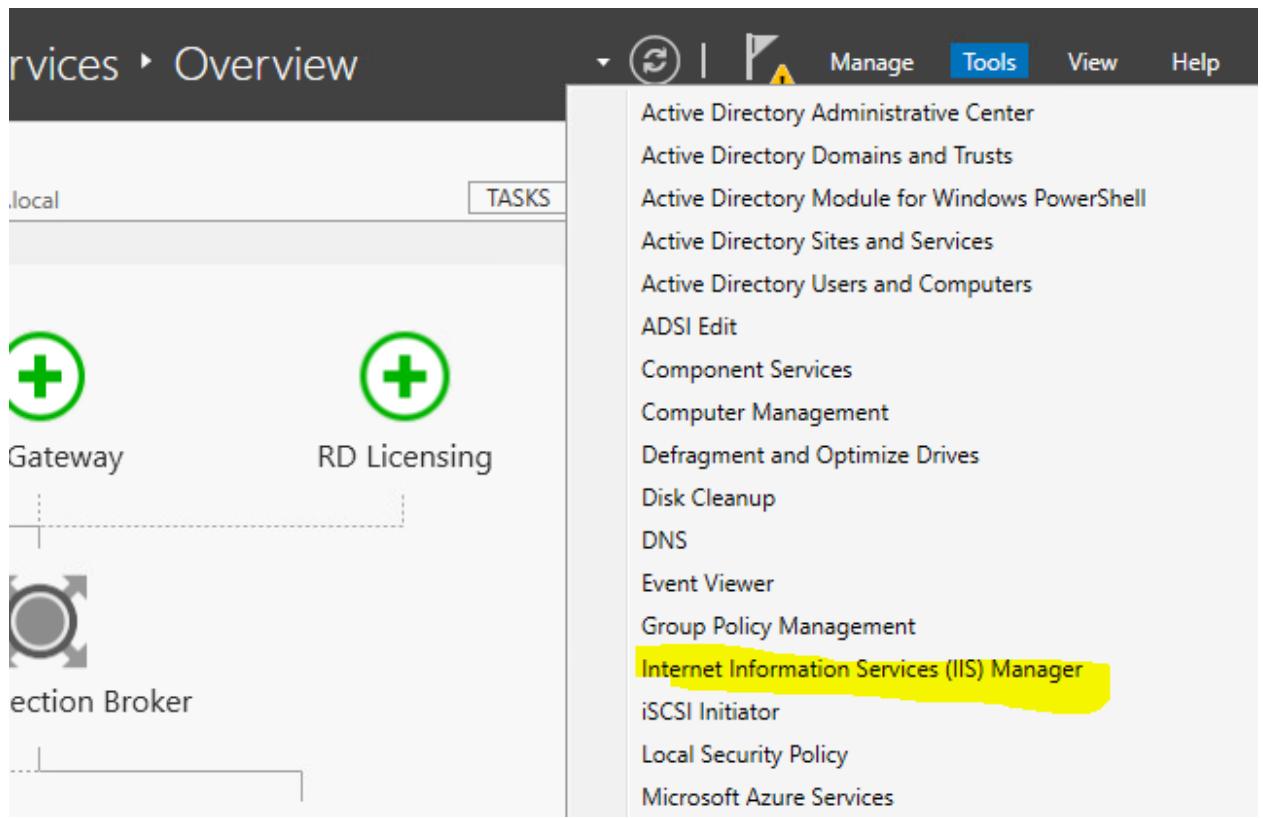
Role Service	Level	Status	State
RD Connection Broker - Enable Single Sign-On	Trusted	OK	Success
RD Connection Broker - Publishing	Trusted	OK	Success
RD Web Access	Trusted	OK	Success
RD Gateway	Unknown	--	

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 менеджер в Tools > Internet Information Services (IIS) Manager

Настройка IIS RDS



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

The screenshot shows the IIS Manager interface. On the left, the tree view shows 'Start Page', 'WINSRV1 (AS21\Administrator)', 'Application Pools', and 'Sites'. Under 'Sites', 'Default Web Site' is selected, showing its sub-items: 'aspnet_client' and 'RDWeb'. On the right, there's a toolbar with 'Filter:', 'Go', 'Show All', and 'Group by:' buttons. Below the toolbar are several configuration icons: '.NET Roles', '.NET Trust Levels', '.NET Users', 'Application Settings', 'Connection Strings', 'Machine Key', 'Pages and Controls', 'Providers', 'Session State', 'SMTP E-mail', 'Authentic...', 'Compression', 'Default Document', 'Directory Browsing', 'Error Pages', 'Failed Request Tra...', 'Handler Mappings', 'HTTP Redirect' (which is highlighted in yellow), 'HTTP Respon...', 'ISAPI Filters', 'Logging', 'MIME Types', 'Modules', 'Output', and 'Request'.

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

 **HTTP Redirect**

Use this feature to specify rules for redirecting incoming requests to another file or URL.

Redirect requests to this destination:

Example: <https://www.contoso.com/sales>

Redirect Behavior

Redirect all requests to exact destination (instead of relative to destination)

Only redirect requests to content in this directory (not subdirectories)

Status code:

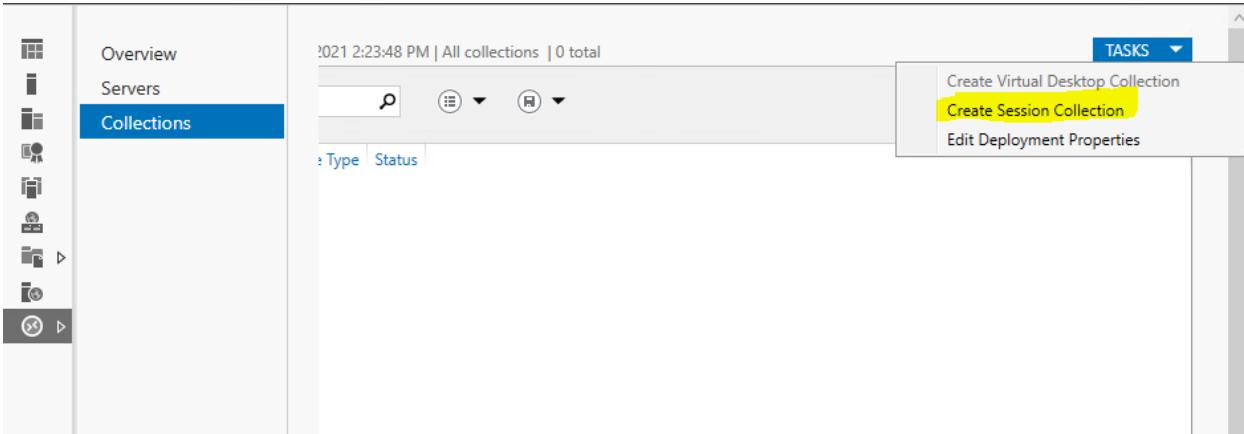
Actions

 [Apply](#)
 [Cancel](#)
 [Help](#)

Публикация коллекции RDS

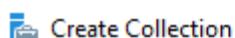
Опубликуйте программу WordPad на web-портале RemoteApp для всех членов группы Group2, при запуске этой программы у пользователей не должны появляться никакие ошибки и предупреждения системы безопасности.

Создаем новую коллекцию



The screenshot shows the 'Collections' tab selected in the navigation bar. The main area displays a summary: '2021 2:23:48 PM | All collections | 0 total'. Below this are search and filter controls. On the far right, a 'TASKS' dropdown menu is open, showing options: 'Create Virtual Desktop Collection', 'Create Session Collection' (which is highlighted with a yellow box), and 'Edit Deployment Properties'.

Вводим имя коллекции



Name the collection

Before You Begin
Collection Name
RD Session Host
User Groups
User Profile Disks
Confirmation
Progress

A session collection name is displayed to users when the server.

Name:

WordPad

Description (optional):

Добавляем сервер WINSRV1 как хоста коллекции

Before You Begin
Collection Name
RD Session Host
User Groups
User Profile Disks
Confirmation
Progress

Select the RD Session Host servers from the server pool to add to this collection.

Server Pool		
Filter: <input type="text"/>		
Name	IP Address	Operat
WINSRV1.as21.local		

Selected

Computer
AS21.LOCAL (1) WINSRV1

Убираем группу AS21\Domain Users

Specify user groups

Before You Begin
Collection Name
RD Session Host
User Groups
User Profile Disks
Confirmation
Progress

Add the user groups that should have access to connect to the collection.

User Groups:

AS21\Domain Users	<input type="button" value="Add..."/>
	<input type="button" value="Remove"/>

Добавляем AS21\Group2

Specify user groups

Before You Begin
Collection Name
RD Session Host
User Groups
User Profile Disks
Confirmation
Progress

Add the user groups that should have access to connect to the collection.

User Groups:

AS21\Group2

Add...
Remove

Убираем пользовательские диски профилей

Specify user profile disks

Before You Begin
Collection Name
RD Session Host
User Groups
User Profile Disks
Confirmation
Progress

User profile disks store user profile settings and data in a central location for the collection.

Enable user profile disks

Location of user profile disks:

Maximum size (in GB):
20

Публикация приложения RDS

Публикуем приложение

Overview
Servers
Collections
WordPad

Properties of the collection

Collection Type: Session
Resources: Remote Desktop
User Group: AS21\Group2

Last refreshed on 7/31/2021 10:35:28

Filter

Server FQDN User Session State

REMOTEAPP PROGRAMS

Published RemoteApp programs | 0 total

Remote Desktop is published for the users of the collection

PUBLISH

Publish RemoteApp programs
Unpublish RemoteApp Programs

Выбираем их списка WordPad и публикуем его на RDS

Select RemoteApp programs

Log

RemoteApp Programs

Confirmation
Publishing
Completion

Select the RemoteApp programs to publish to the WordPad collection. To add a RemoteApp program to the list, click Add.

The RemoteApp programs are populated from WINSRV1.as21.local.

RemoteApp Program	Location
<input type="checkbox"/> Steps Recorder	%SYSTEMDRIVE%\Windows\system32\psr.exe
<input type="checkbox"/> System Configuration	%SYSTEMDRIVE%\Windows\system32\msconfig...
<input type="checkbox"/> System Information	%SYSTEMDRIVE%\Windows\system32\msinfo3...
<input type="checkbox"/> Task Manager	%SYSTEMDRIVE%\Windows\system32\taskmgr....
<input type="checkbox"/> Windows Media Player	%SYSTEMDRIVE%\Program Files (x86)\Windows...
<input type="checkbox"/> Windows Memory Diagnostic	%SYSTEMDRIVE%\Windows\system32\MdSche...
<input type="checkbox"/> Windows Speech Recognition	%SYSTEMDRIVE%\Windows\Speech\Common\s...
<input checked="" type="checkbox"/> WordPad	%SYSTEMDRIVE%\Program Files\Windows NT\...
<input type="checkbox"/> XPS Viewer	%SYSTEMDRIVE%\Windows\system32\xpsrchv...

Add...

Verify that the program is installed on all the RD Session Host servers in the collection.
Go to Settings to activate Windows.

< Previous Next > Publish Cancel

Заходим в свойство WordPad > Edit Properties

REMOTEAPP PROGRAMS

Last refreshed on 7/28/2021 12:21:56 PM | Published RemoteA... TASKS

RemoteApp Program Name	Alias	Visible in RD Web Access
WordPad	WordPad	Edit Properties

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

WordPad (QuickSessionCollection Collection)

The screenshot shows the 'User Assignment' section of the 'WordPad (QuickSessionCollection Collection)' properties. The 'Only specified users and groups' radio button is selected. A yellow box highlights this selection. Below it, a list box contains 'AS21\Group2'. To the right are 'Add...' and 'Remove' buttons.

Show All

General +

Parameters +

User Assignment -

File Type Associati... +

User Assignment

RemoteApp programs can be limited so that only selected users and groups can see the icon when they log on to RD Web Access.

Specify the users and groups who should see this RemoteApp program:

All users and groups that have access to the collection

Only specified users and groups

Users and groups:

AS21\Group2

Add...

Remove

И применяем настройки Apply

Only specified users and groups

Users and groups:

AS21\Group2

Add...

Remove

- For a user account to have access to a RemoteApp program, the user account must have access to both the RemoteApp program and the collection to which it is published. Updating the user access at the collection level will not change the user access at the RemoteApp program level.

OK

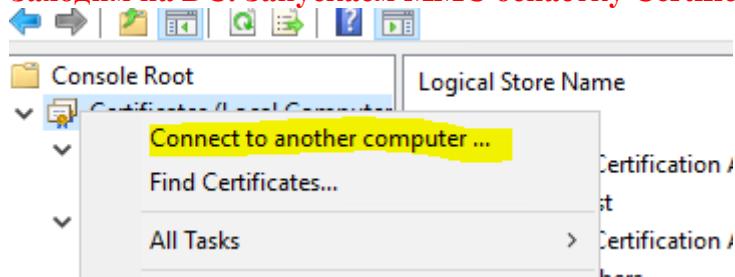
Cancel

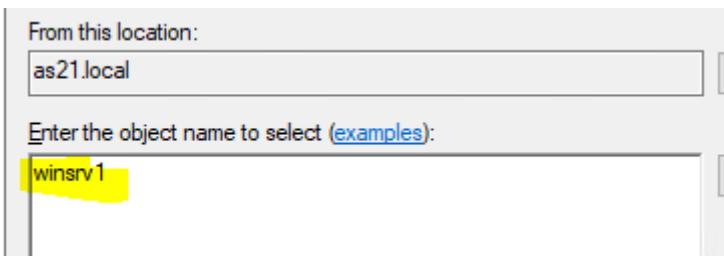
Apply

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

Console1 - [Console Root\Certificates (WINSRV1.AS21.LOCAL)\\\WINSRV1.AS21.LOCAL\Personal\Certificates]

File Action View Favorites Window Help

Console Root

Certificates (WINSRV1.AS21.LOCAL)

\\WINSRV1.AS21.LOCAL\Personal

Certificates

\\WINSRV1.AS21.LOCAL\Trusted Root Certification Authority

\\WINSRV1.AS21.LOCAL\Enterprise Trust

\\WINSRV1.AS21.LOCAL\Intermediate Certification Authority

\\WINSRV1.AS21.LOCAL\Trusted Publishers

\\WINSRV1.AS21.LOCAL\Untrusted Certificates

\\WINSRV1.AS21.LOCAL\Third-Party Root Certification Authority

\\WINSRV1.AS21.LOCAL\Trusted People

\\WINSRV1.AS21.LOCAL\Client Authentication Issuers

\\WINSRV1.AS21.LOCAL\Preview Build Roots

Issued To	Issued By
rds.as21.local	SubCA
WINSRV1.AS21.LOCAL	RootCA
WINSRV1.AS21.LOCAL	SubCA
WINSRV1.AS21.LOCAL	RootCA

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

Certificate

General Details Certification Path

Show: <All>

Field	Value
Subject Key Identifier	991fa2f393a3e6dead9a02db1...
Subject Alternative Name	DNS Name=rds.as21.local, DN...
Authority Key Identifier	KeyID=b123791dc98dd7a69...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Key Usage	Digital Signature, Key Encipher...
Thumbprint	25bea17f3913f4e8dbbee4ddb3...

25bea17f3913f4e8dbbee4ddb319fe7dbf8328806

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

The screenshot shows the 'Specify SHA1 thumbprints of certificates representing trusted .rdp publishers' GPO settings dialog box. The 'Enabled' radio button is selected. The 'Comment' field is empty. The 'Supported on:' field shows 'At least Windows Vista with Service Pack 1'. The 'Options' section contains a text input field with the value 'a17f3913f4e8dbbee4ddb319fe7dbf8328806'. The 'Help' section provides a detailed description of the policy setting, stating it allows specifying a list of SHA1 certificate thumbprints for trusted RDP file publishers. It explains that enabling the setting trusts any certificate with a matching thumbprint, while disabling it treats no publisher as trusted. The 'Notes' section lists other policy settings: 'Do not allow hardware accelerated decoding' (Not configured, No), 'Do not allow passwords to be saved' (Not configured, No), 'Specify SHA1 thumbprints of certificates representing trust...' (Enabled, No), 'Turn Off UDP On Client' (Not configured, No), and 'Prompt for credentials on the client computer' (Not configured, No).

Do not allow hardware accelerated decoding	Not configured	No
Do not allow passwords to be saved	Not configured	No
Specify SHA1 thumbprints of certificates representing trust...	Enabled	No
Turn Off UDP On Client	Not configured	No
Prompt for credentials on the client computer	Not configured	No

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

Site to Zone Assignment List

Site to Zone Assignment List

Comment:

Not Configured

Enabled

Disabled

Supported on: At least Internet Explorer 6.0 in Windows Server 2003 with Service Pack 1

Options: Help:

Enter the zone assignments here. Show...

This policy setting allows you to associate sites with security zones. These zone numbers have associated security settings that apply to all of the sites in the zone.

Internet Explorer has 4 security zones, numbered 1-4, and these are used by this policy setting to associate sites to zones. They are: (1) Intranet zone, (2) Trusted Sites zone, (3) Internet zone, and (4) Restricted Sites zone. Security settings can be set for each of these zones through other policy settings, and their default settings

Show Contents

Enter the zone assignments here.

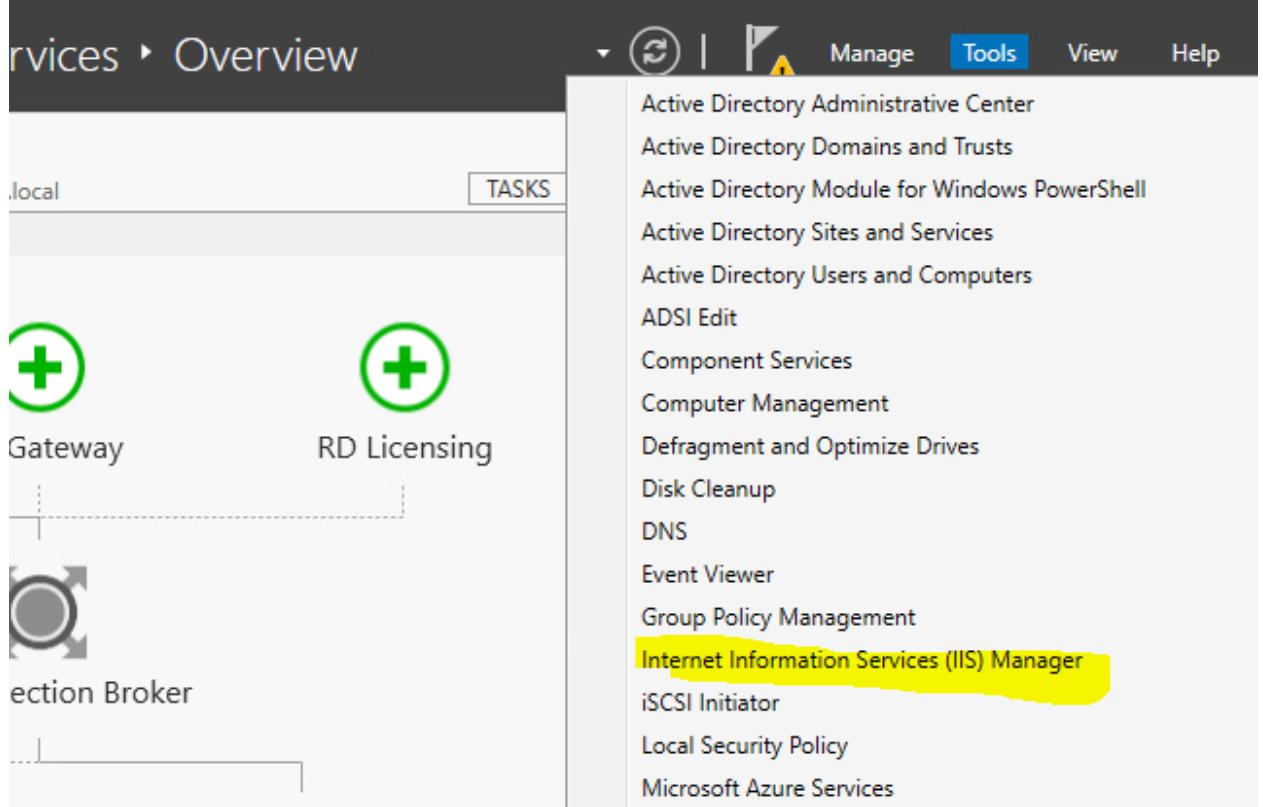
	Value name	Value
▶	https://rds.as21.local	1
*		

Local Machine Zone Template
Locked-Down Restricted Sites Zone Template
Restricted Sites Zone Template
Locked-Down Trusted Sites Zone Template
Trusted Sites Zone Template
Turn on certificate address mismatch warning
Intranet Sites: Include all sites that bypass the proxy server
Intranet Sites: Include all network paths (UNCs)
Site to Zone Assignment List Enabled
Turn on automatic detection of intranet
Turn on Notification bar notification for intranet content

ПУБЛИКАЦИЯ CRL НА ДОМАШНЕЙ СТРАНИЦЕ

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

Проверяем, что настройки ПС в разделе HTTP Redirect верны



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

The screenshot shows the Internet Information Services (IIS) Manager interface. The left pane shows the site structure under 'WINSRV1 (AS21\Administrator)'. The 'Default Web Site' is selected. The right pane displays various IIS configuration icons, with 'HTTP Redirect' highlighted with a yellow box.

Filter: Show All | Group by:

- .NET Roles
- .NET Trust Levels
- .NET Users
- Application Settings
- Connection Strings
- Machine Key
- Pages and Controls
- Providers
- Session State
- SMTP E-mail

IIS

- Authentic... Compression Default Document Directory Browsing Error Pages
- Failed Request Tra... Handler Mappings HTTP Redirect HTTP Respon... ISAPI Filters
- Logging MIME Types Modules Output Request

Actions

Redirect requests to this destination:
https://rds.as21.local/rdweb

Example: <https://www.contoso.com/sales>

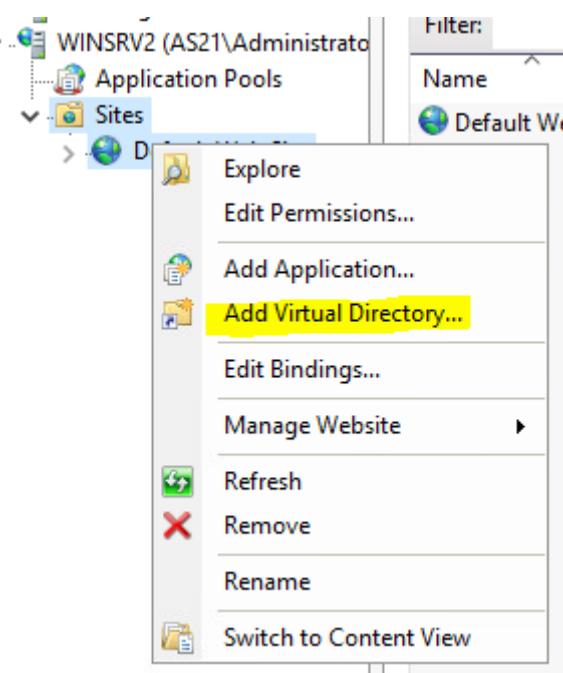
Redirect Behavior

Redirect all requests to exact destination (instead of relative to destination)

Only redirect requests to content in this directory (not subdirectories)

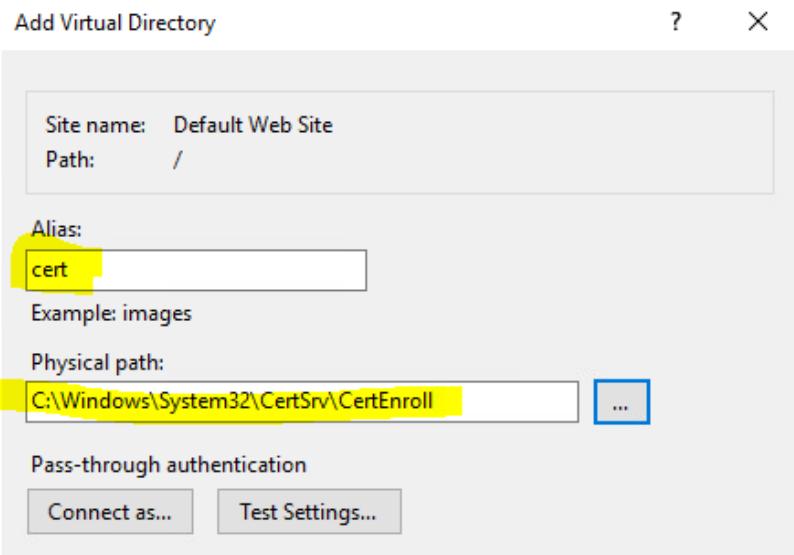
Status code:
Found (302)

Создаем виртуальную директорию cert



The screenshot shows the Windows Server Manager interface. On the left, there's a tree view with 'WINSRV2 (AS21)\Administrators' expanded, showing 'Application Pools' and 'Sites'. Under 'Sites', there's a folder named 'cert'. A context menu is open over this folder, listing options: 'Explore', 'Edit Permissions...', 'Add Application...', 'Add Virtual Directory...', 'Edit Bindings...', 'Manage Website', 'Refresh', 'Remove', 'Rename', and 'Switch to Content View'. The 'Add Virtual Directory...' option is highlighted with a yellow box.

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



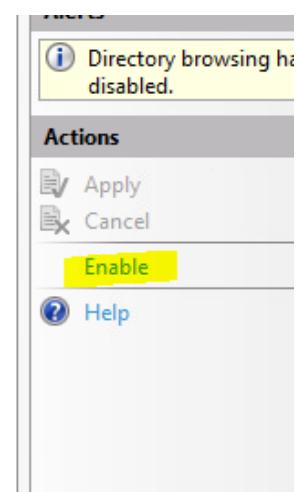
Переходим в раздел нашей папки и открываем Directory Browsing

The screenshot shows the IIS Manager interface. On the left, the 'cert' folder under 'RDWeb' is selected. In the center, various IIS features are listed: .NET Trust Levels, .NET Users, Application Settings, Connection Strings, Machine Key Strings, Providers, Session State, SMTP E-mail, ASP, Authentication, Compression, Default Document, and Error Pages. The 'Directory Browsing' icon is highlighted with a yellow box.

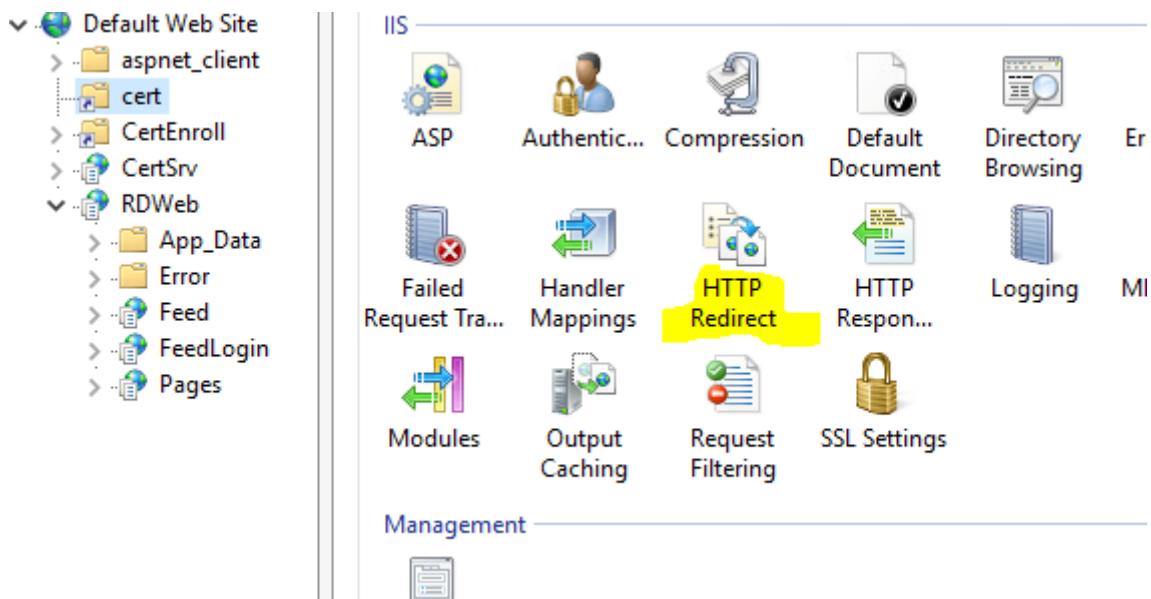
И включаем настройку
Directory Browsing

Use this feature to specify the information that displays in a directory listing.

- Time
- Size
- Extension
- Date
- Long date



Открываем HTTP redirect для нашей папки



Проверяем, что переадресация для папки отключена

HTTP Redirect

Use this feature to specify rules for redirecting incoming requests to another file or URL.

Redirect requests to this destination:

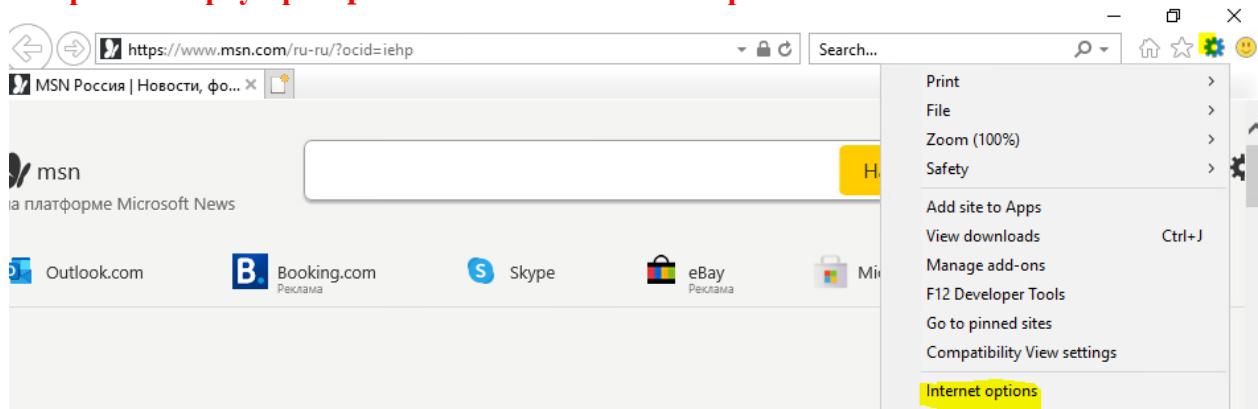
Example: <https://www.contoso.com/sales>

Redirect Behavior

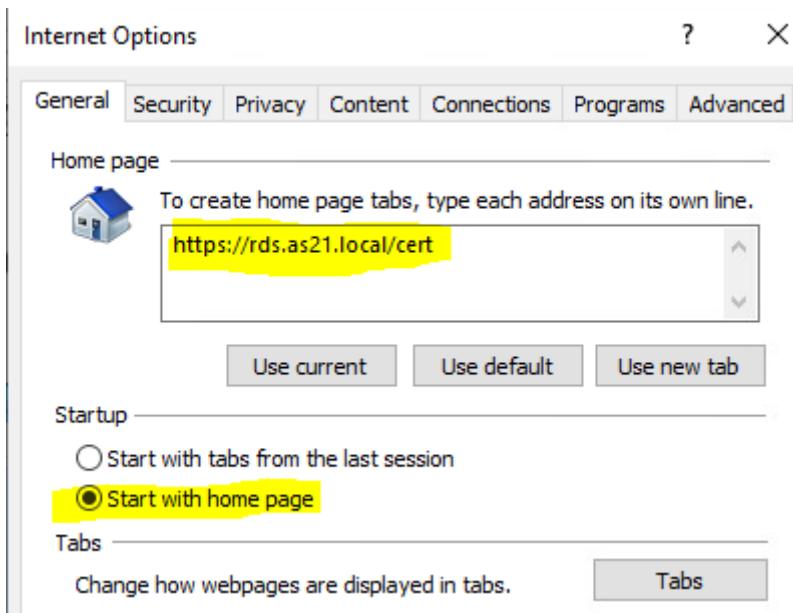
Redirect all requests to exact destination (instead of relative to destination)

Only redirect requests to content in this directory (not subdirectories)

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
```

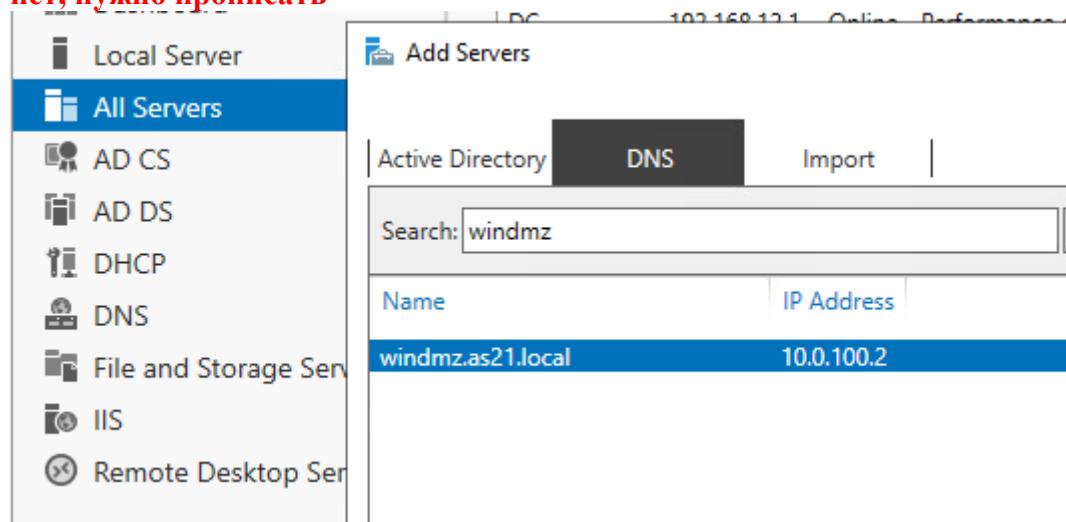
Внизу отображаемой помощи найти

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

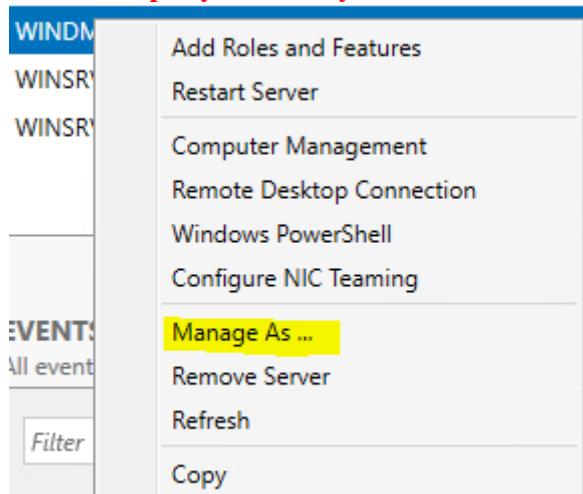
Скопировать и заменить <local> на * и запустить. Должны получить:

```
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 = *
```

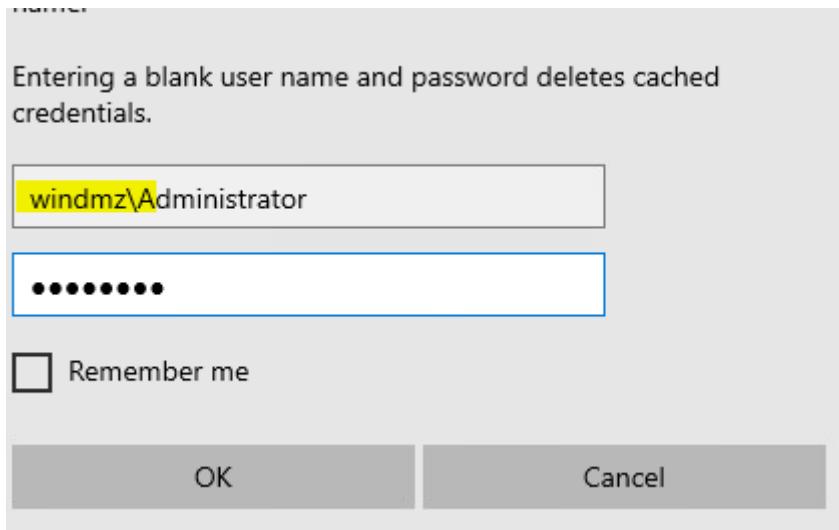
В оснастке All Servers добавляем его по DNS имени (у меня он прописан в DNS), если нет, нужно прописать



Нажать правую кнопку на WINDMZ и выбрать Manage As ...



Ввести учетную запись формата WINDMZ\Administrator



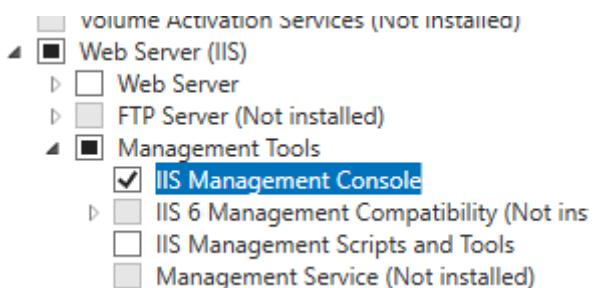
В итоге должны получить такое:

WINDMZ 10.0.100.2 Online - Performance counters not started

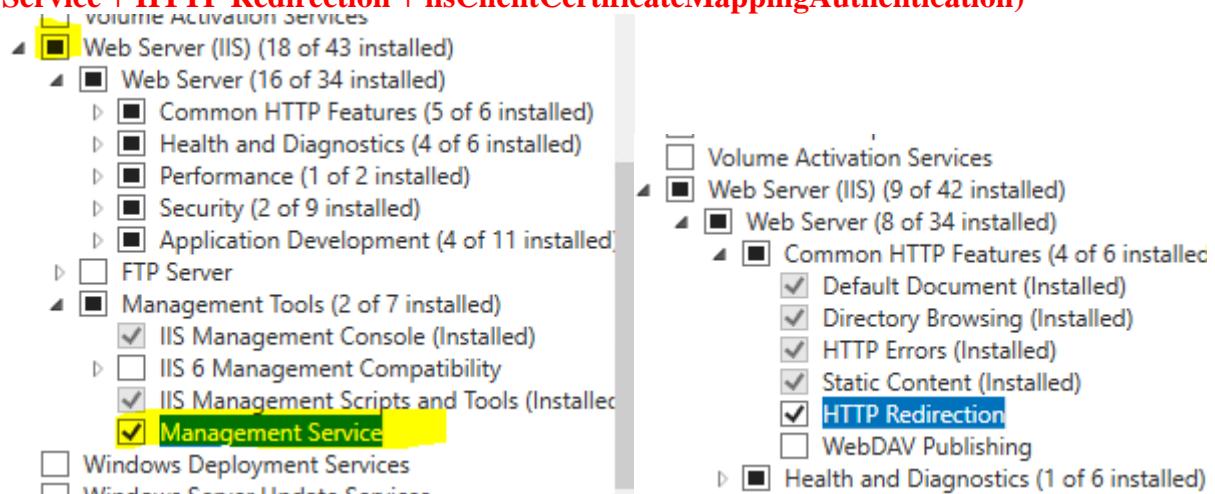
Настройка подключения консоли IIS к WINDMZ

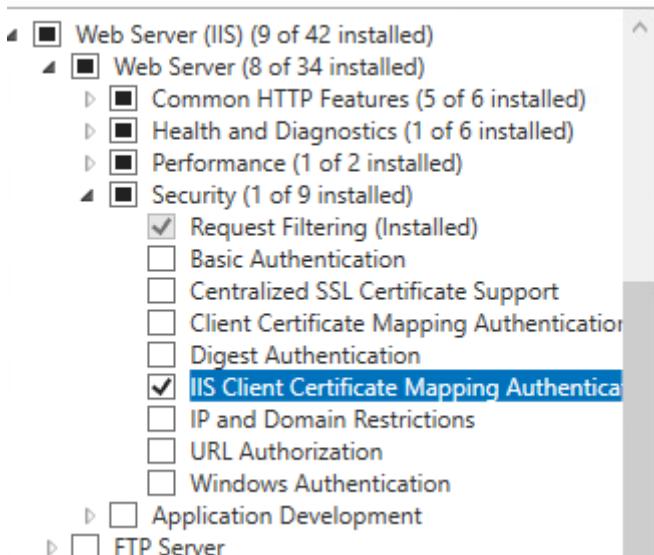
Установите на сервер компоненты IIS.

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 ПС консоли

Запустить на WINDMZ regedit, найти в поиске EnableRemoteManagement или по ссылке

\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WebManagement\Server

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

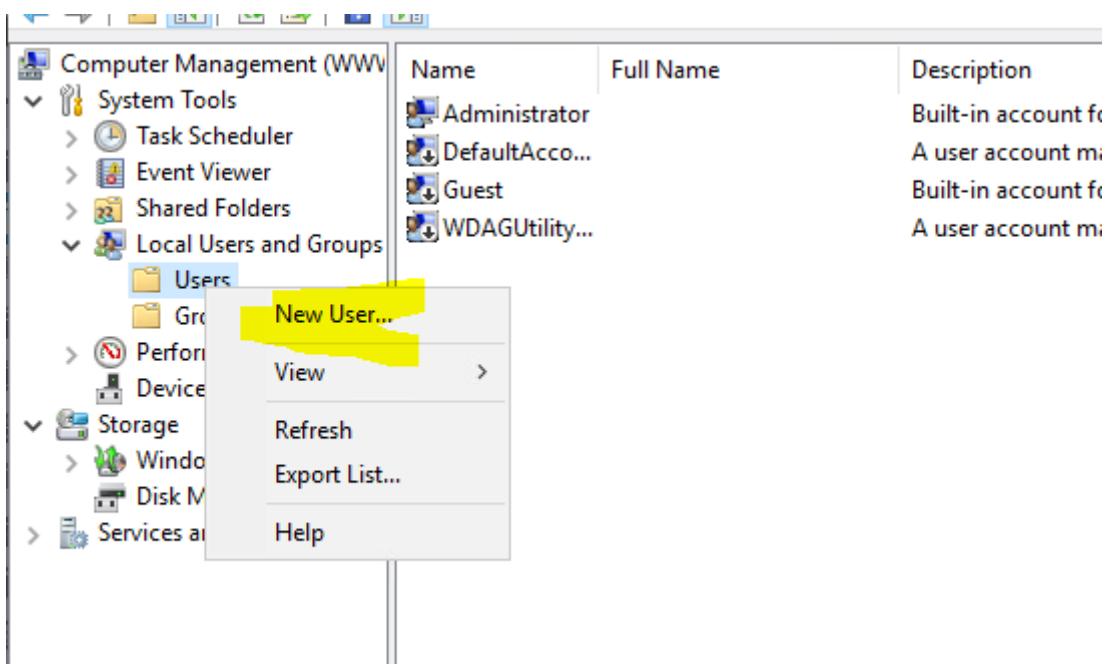
Создадим локального пользователя на WINDMZ, дадим ему права

На DC вызываем Computer Management с WINDMZ

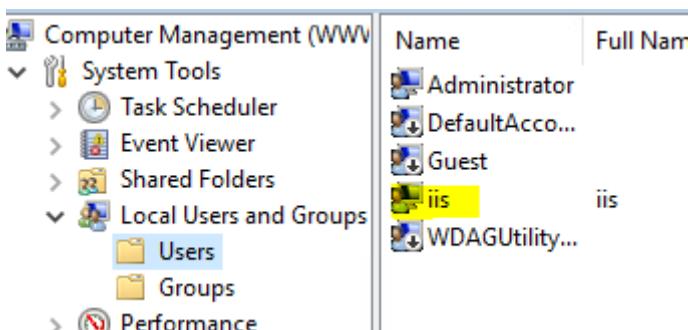
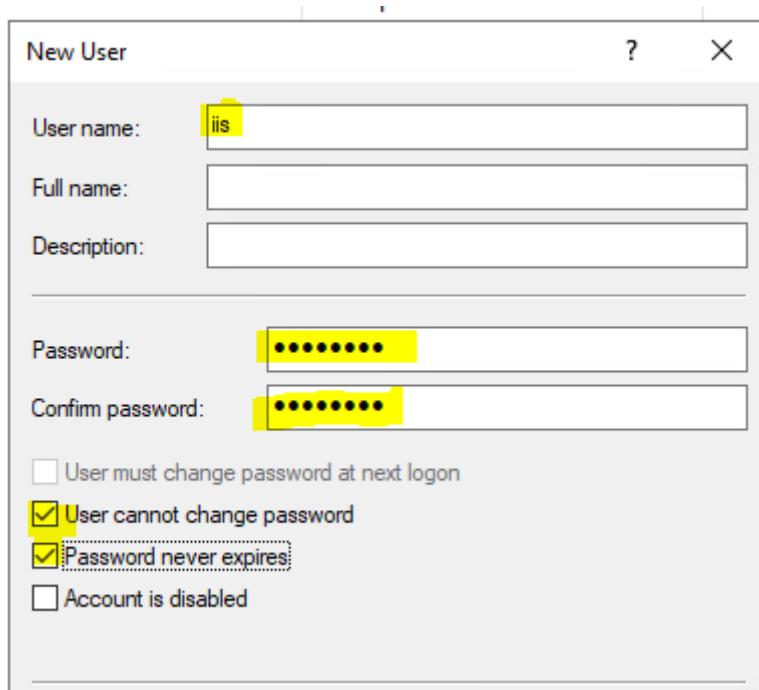
Server Name	IPv4 Address	Manageability	Last Update
DC	192.168.12.10	Online - Performance counters not started	8/1/2021 1:31:49 AM
WINDMZ	203.0.113.11	Online - Performance counters not started	8/1/2021 1:31:49 AM
WINSRV		Add Roles and Features	
WINSRV		Restart Server	
		Computer Management	
		Remote Desktop Connection	
		Windows PowerShell	
		Configure NIC Teaming	
		Internet Information Services (IIS) Manager	
		...	

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

The screenshot shows the Active Directory Administrative Center interface. The top navigation bar includes 'Manage' and 'Tools' tabs, with 'Tools' currently selected. A sidebar on the left lists various management tools, with 'Certification Authority' highlighted. The main pane displays the 'Certification Authority (winsrv2)' node, which is expanded to show 'SubCA' and 'Certificate Templates'. The 'Certificate Templates' node is also highlighted. A context menu is open over the 'User' template, with the 'Duplicate Template' option highlighted. The bottom pane shows a list of certificate templates with their names and counts:

Name	Count
Smartcard Logon	1
Smartcard User	1
Subordinate Certification Authority	1
Trust List Signing	1
User	1
User	2
User S	1
Web	1

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

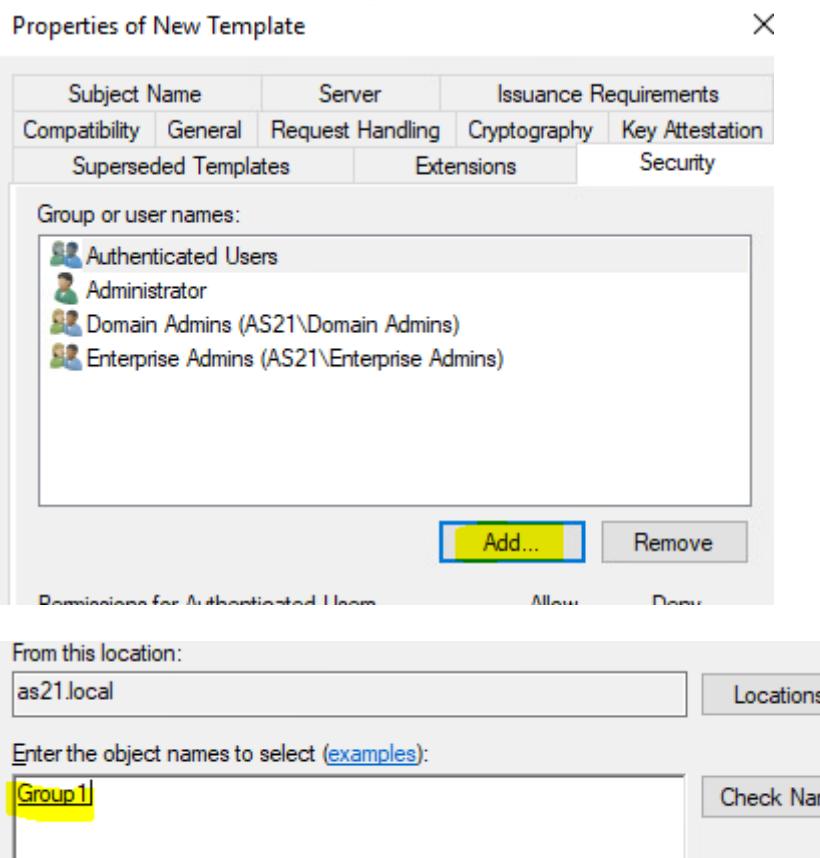
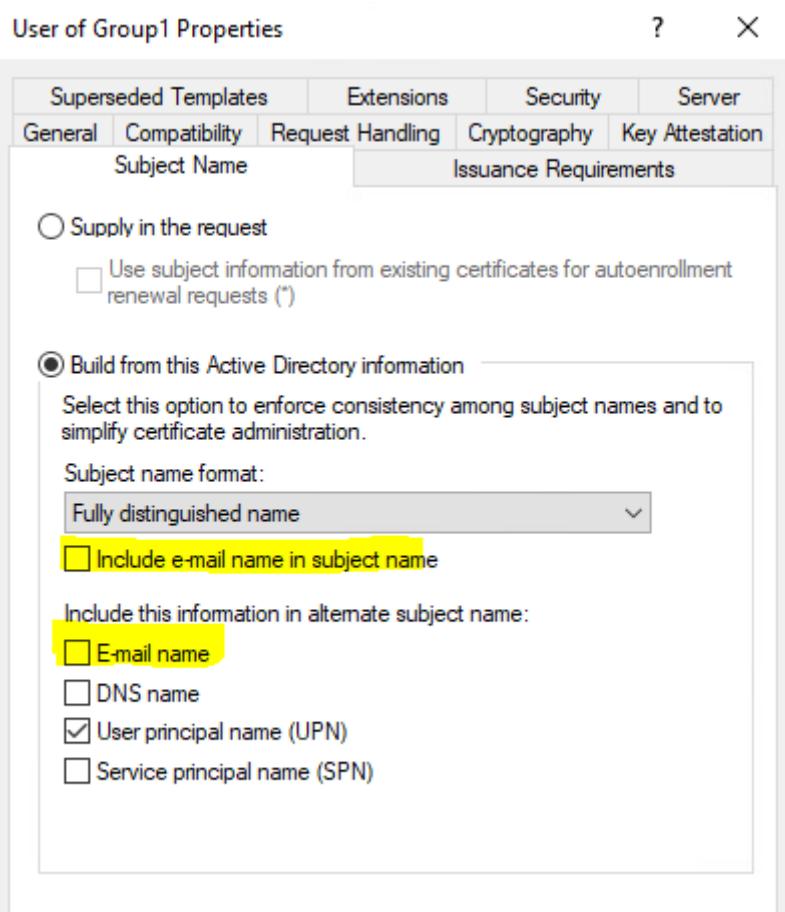
General Compatibility Request Handling Cryptography Key Attestation

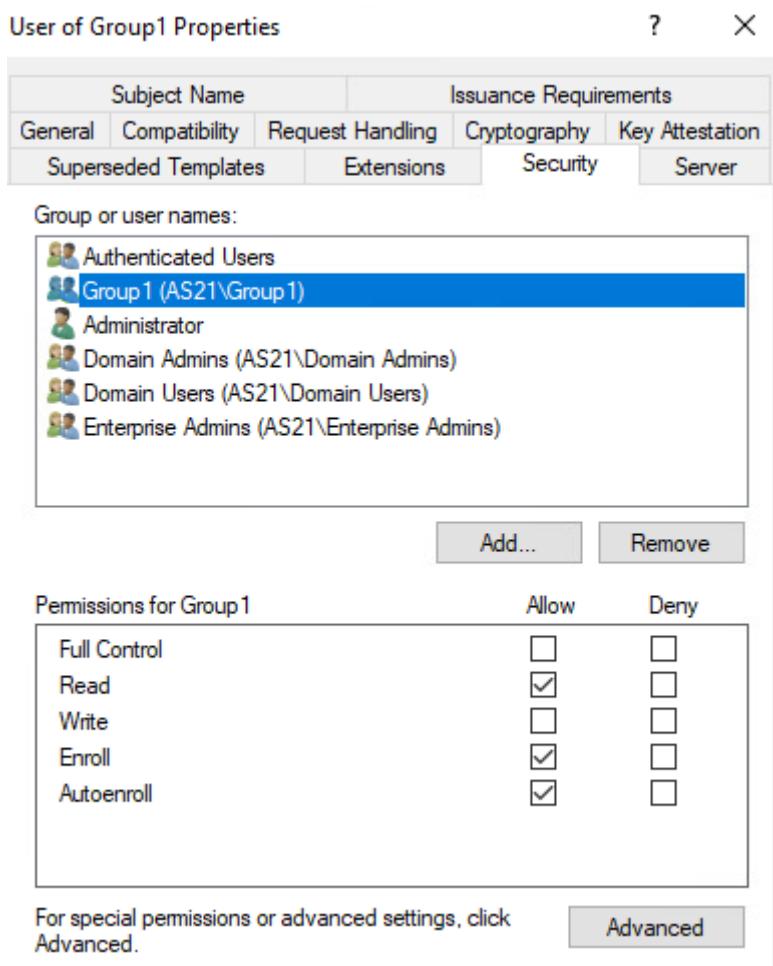
Template display name:
User of Group1

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





SubCA

- Revoked Certificates
- Issued Certificates
- Pending Requests
- Failed Requests
- Certificate Template**

WS PK User of Group1 RDC cert Directory Email Replication Domain Controller Authentication

Manage Authentication

- New > Certificate Template to Issue
- View > Controller
- Refresh
- Export List...
- Help

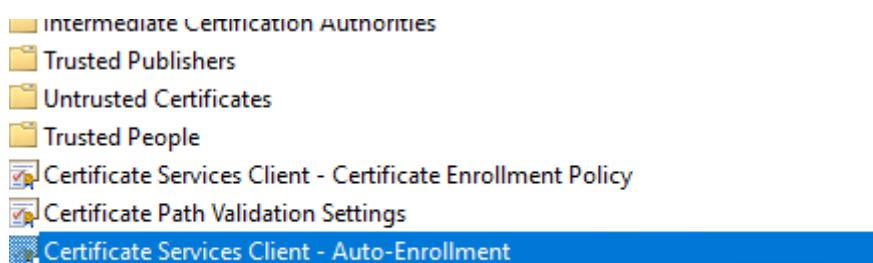
Certification Authority

Administrator

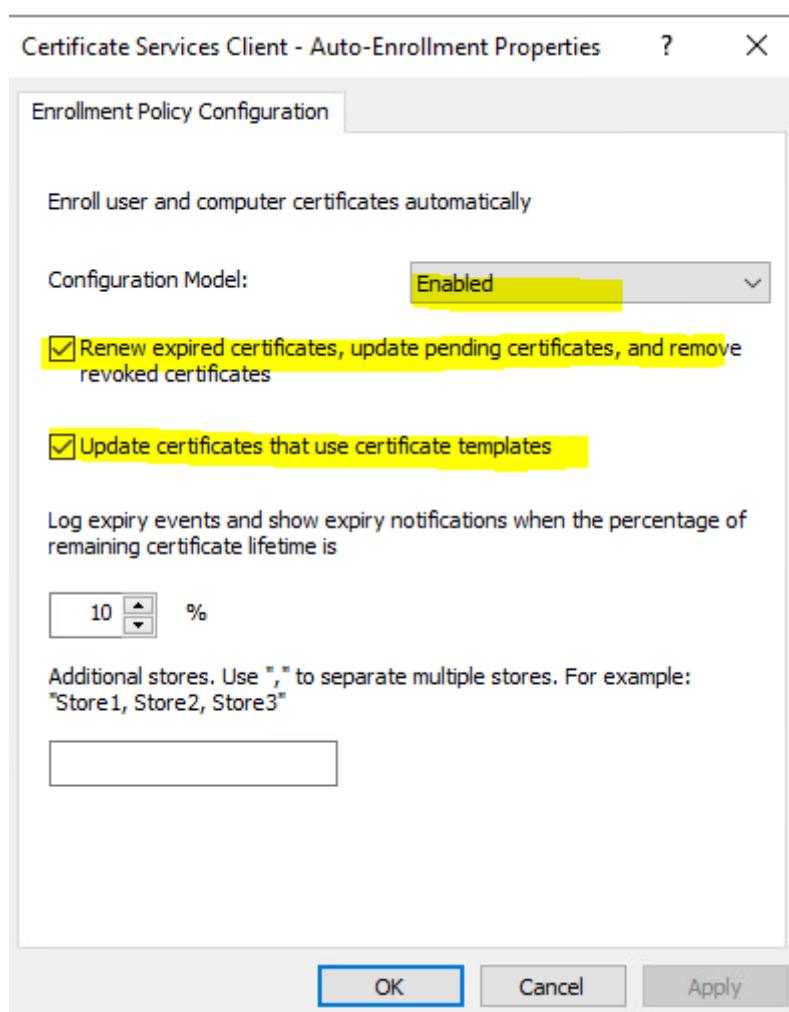
RAS and IAS Server Client Authentication, Server Authentication
 Router (Offline request) Client Authentication
 Smartcard Logon Client Authentication, Smart Card Logon
 Smartcard User Secure Email, Client Authentication, Smart Card
 Trust List Signing Microsoft Trust List Signing
User of Group1 Client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

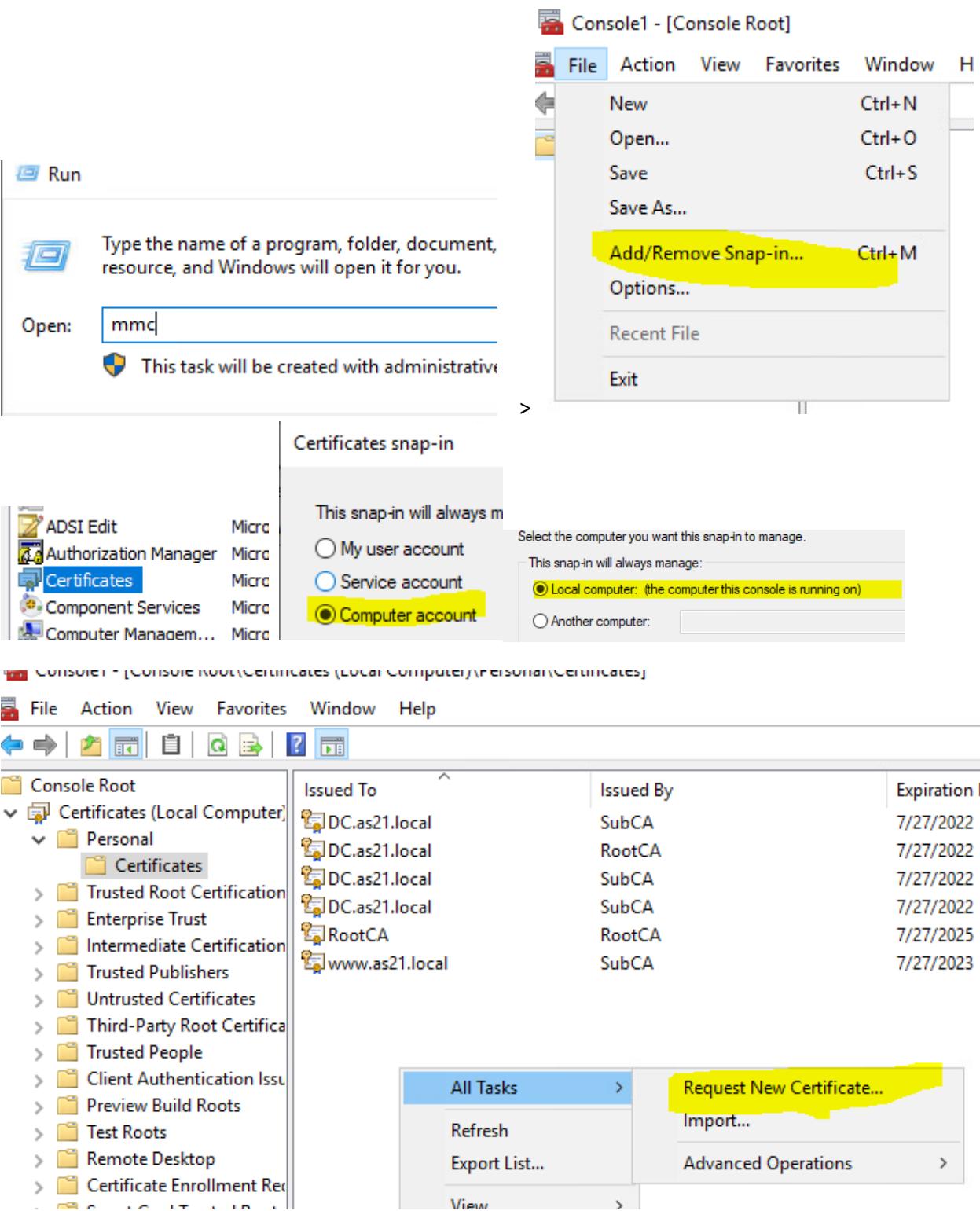


Включаем общую настройку выдачи и выбираем 2 конфигурации



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

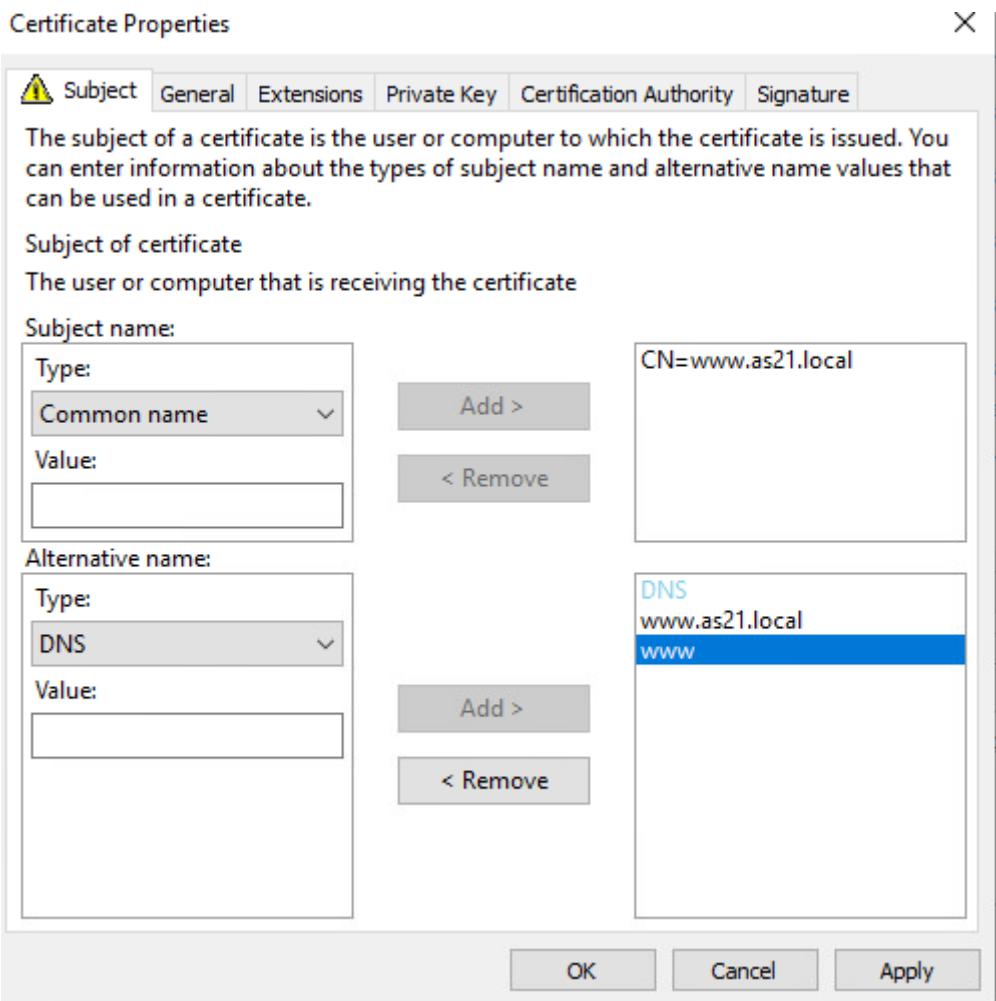
WS PK

i STATUS: Available

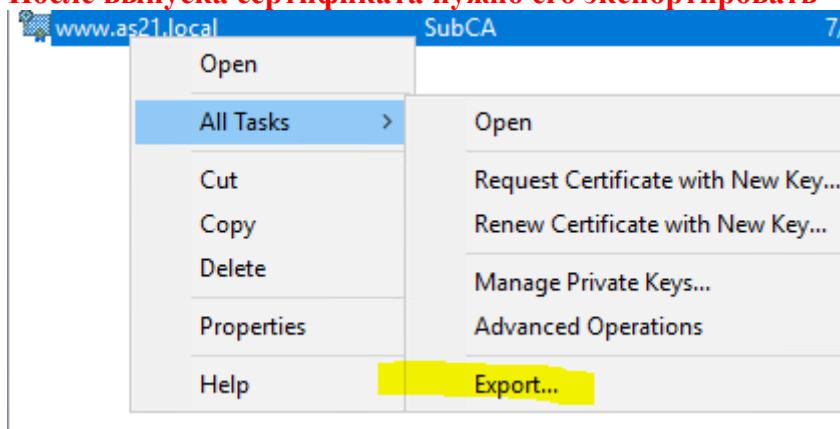
Details ▾

⚠ More information is required to enroll for this certificate. Click here to configure settings.

Добавляем параметры нашего сервера



После выпуска сертификата нужно его экспортовать



- Personal Information Exchange - PKCS #12 (.PFX)
- Include all certificates in the certification path if possible
- Delete the private key if the export is successful
- Export all extended properties
- Enable certificate privacy
- Microsoft Serialized Certificate Store (.SST)

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

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

Yes, export the private key

No, do not export the private key

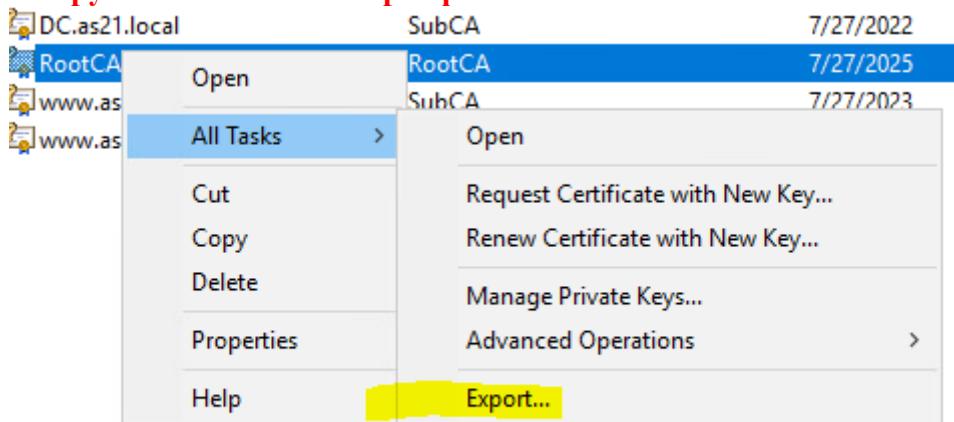
Введите пароль, который будет использован в дальнейшем при импорте и поменяйте шифрование на SHA256

Password:
[REDACTED]
Confirm password:
[REDACTED]

Encryption: AES256-SHA256

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

Выгружаем из консоли сертификат RootCA



Do you want to export the private key with the

Yes, export the private key

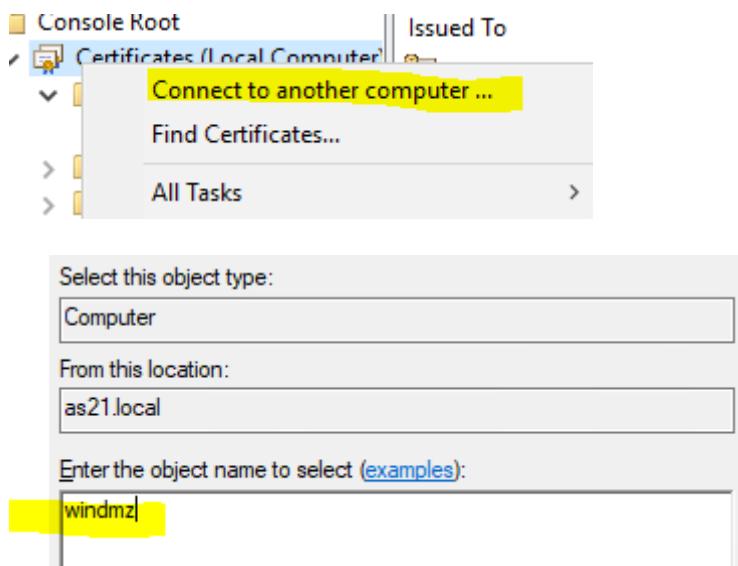
No, do not export the private key

Select the format you want to use:

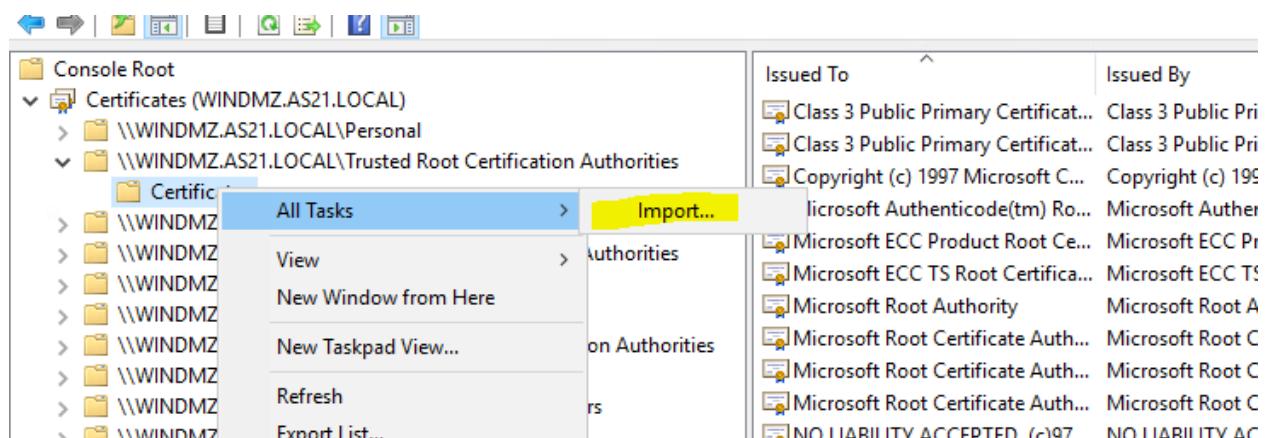
- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 - Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)

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 отзываемых сертификатов на WINDMZ

Добавляем список отзываемых сертификатов на WINDMZ

Заходим на WINSRV2 по пути \\winsrv2\C\$\Windows\System32\CertSrv\CertEnroll

Копируем файлы SubCA и SubCA+

Name	Date modified	Type	Size
SubCA	7/31/2021 9:13 AM	Certificate Revoca...	1 KB
SubCA+	8/1/2021 9:14 AM	Certificate Revoca...	1 KB
WINSRV2.as21.local_SubCA	7/31/2021 9:13 AM	Security Certificate	2 KB

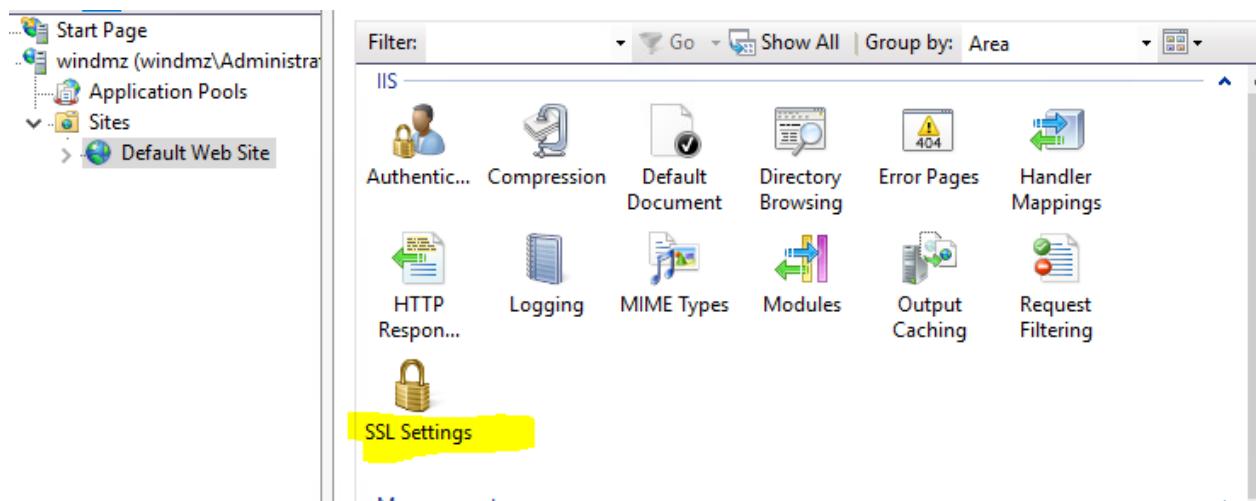
Идем на WINDMZ

Запускаем команды:

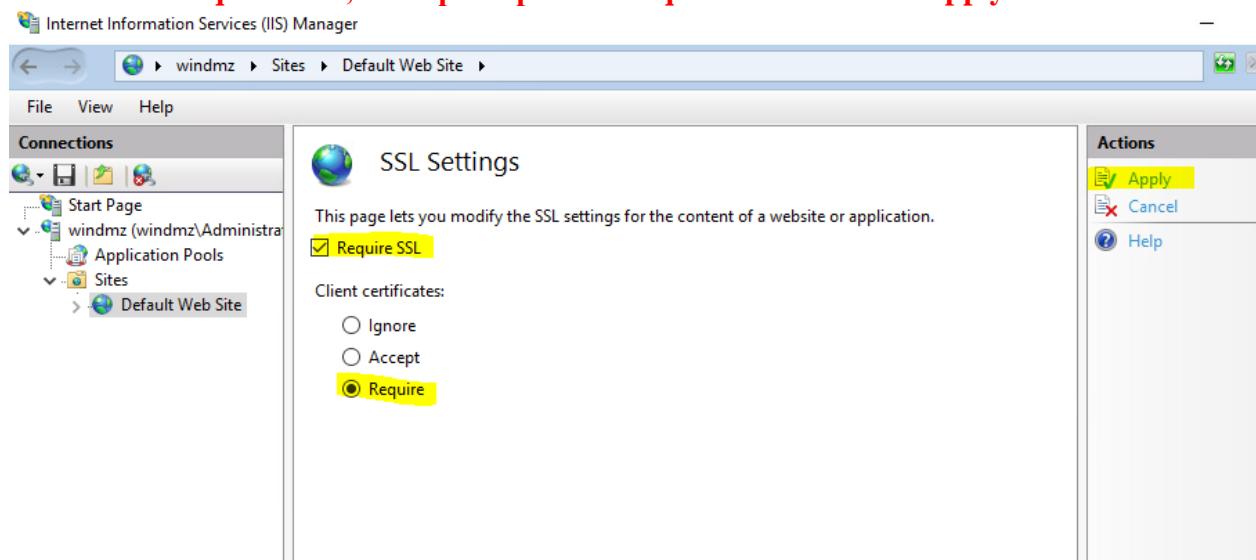
`certutil -addstore -f Root SubCa.crl`
`certutil -addstore -f Root SubCa+.crl`

Настройка SSL на WINDMZ

Включим разрешение заходить только по сертификатам. Заходим в SSL Settings

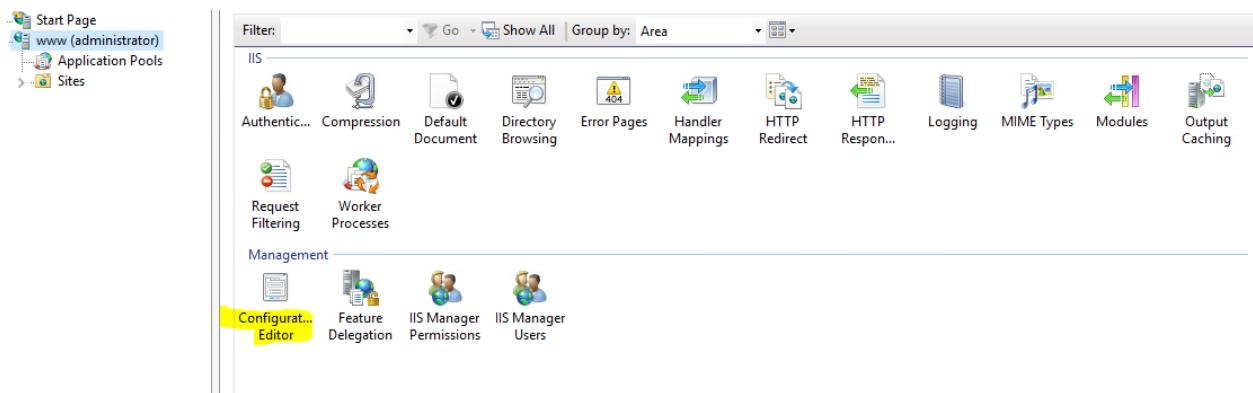


Включаем Require SSL, выбираем режим Require и нажимаем Apply



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

appSettings

- + system.transactions
- + system.web
- system.webServer
 - security
 - authentication
 - anonymousAuthentication
 - basicAuthentication
 - iisClientCertificateMappingAuthentication**
 - digestAuthentication
 - windowsAuthentication
 - access
 - applicationDependencies
 - authorization
 - dynamicIpSecurity
 - ipSecurity
 - isapiCgiRestriction

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

Configuration Editor

Section: system.webServer/security/authentication/iisClientCertificateMappingA/

Deepest Path: MACHINE/WEBROOT/APPHOST	
defaultLogonDomain	
enabled	True
logonMethod	ClearText
manyToOneCertificateMappingsEnabled	True
manyToOneMappings	(Count=0)
oneToOneCertificateMappingsEnabled	False
oneToOneMappings	(Count=0)

Добавляем настройки manyToOneMapping

manyToOneCertificateMappingsEnabled
manyToOneMappings
oneToOneCertificateMappingEnabled

True
(Count=0)
False

Items:

name	description	enabled	permissionMode	userName	password	Entry Path

Actions:

- Collection
- Add
- Clear All
- Help
- Online Help

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

Properties:

description	
enabled	True
name	
password	Mapping *****
permissionMode	Allow
rules	(Count=0)
userName	iis

userName

Добавляем правила

Collection Editor - system.webServer/security/authentication/iisClientCertificateMappingAuthentication/manyToOneMappings/add/rules/

Items:

certificateField	certificateSubField	matchCriteria	compareCaseSensitive	Entry Path

Actions:

- Collection
- Add
- Clear All
- Help

Заполняем поля

Properties:

certificateField	Issuer
certificateSubField	CN
compareCaseSensitive	True
matchCriteria	SubCA

matchCriteria
Data Type:string

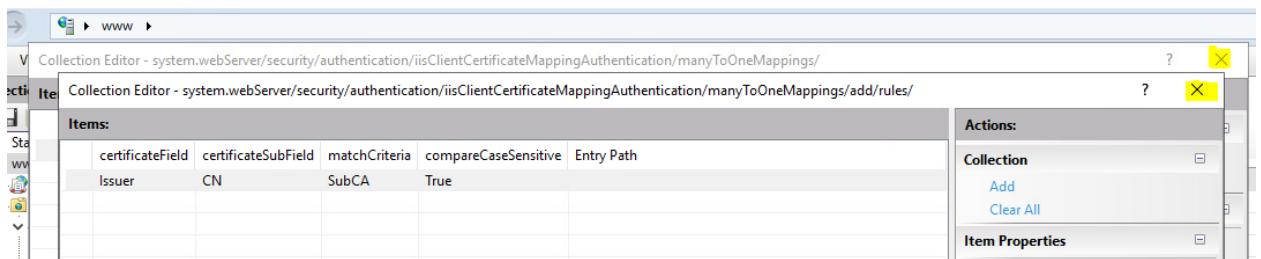
certificateField (поле сертификата, которое мы проверяем) – Issuer (издатель)

certificateSubField (тип значения в поле издателя) – CN

matchCriteria (что ищем в поле) – SubCA (наш центр сертификации)

ВАЖНО!!! Поле чувствительно к регистру

Закрываем оба окна



Применим настройку

Configuration Editor

Section: system.webServer/security/authentication/iisClientCertificateMapping/

Deepest Path: MACHINE/WEBROOT/APPHOST	
defaultLogonDomain	True
enabled	ClearText
logonMethod	True
manyToOneCertificateMappingsEnabled	(Count=1)
manyToOneMappings	(Count=1)
oneToOneCertificateMappingsEnabled	False
oneToOneMappings	(Count=0)

Actions:

- Collection
- Add
- Clear All

Item Properties

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

Default Web Site Home

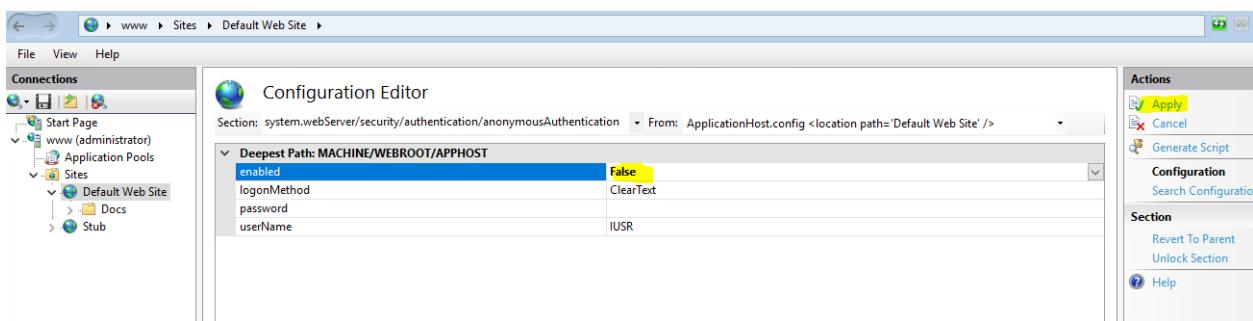
IIS

- Authentic...
- Compression
- Default Document
- Directory Browsing
- Error Pages
- Handler Mappings
- HTTP Redirect
- HTTP Respon...
- Logging
- MIME Types

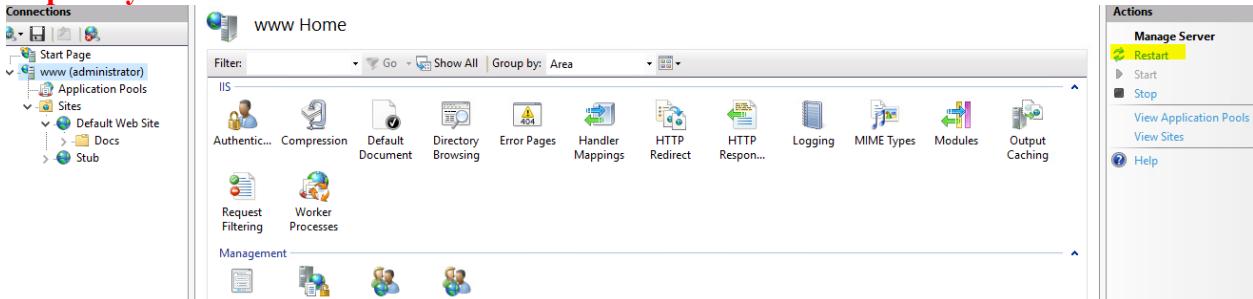
Management

- Request Filtering
- SSL Settings
- Configurat... Editor
- IIS Manager Permissions

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



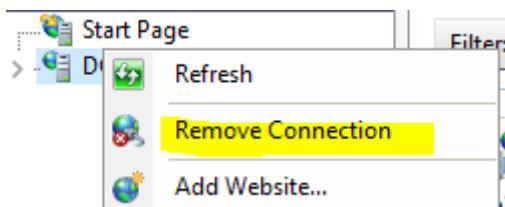
Перезапускаем сайт



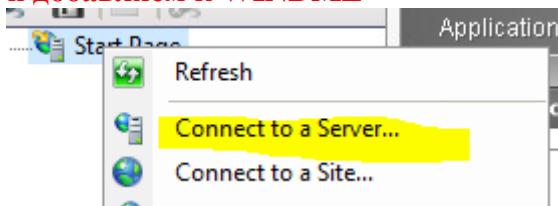
Настройка IIS на WINDMZ

Теперь на DC запускаем консоль
Убираем подключение к DC

Internet Information Services (IIS) Manager



и добавляем к WINDMZ

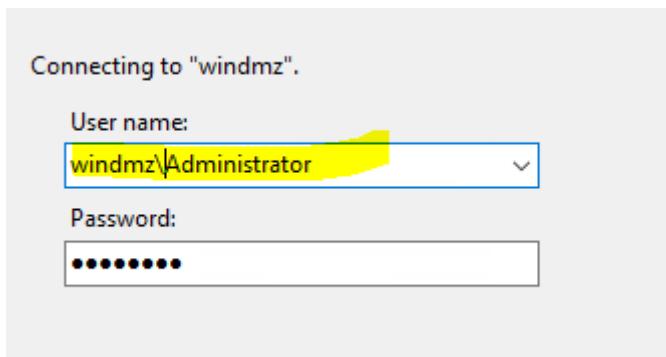


Server name:

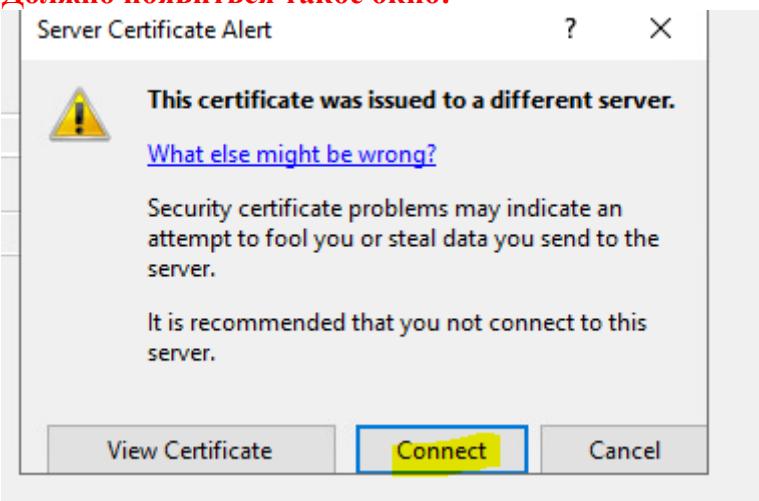
windmz

Example: localhost, www.site.net, or WESTSRV01:8080

Добавляем учетную запись формата WINDMZ\Administrator



Должно появиться такое окно:

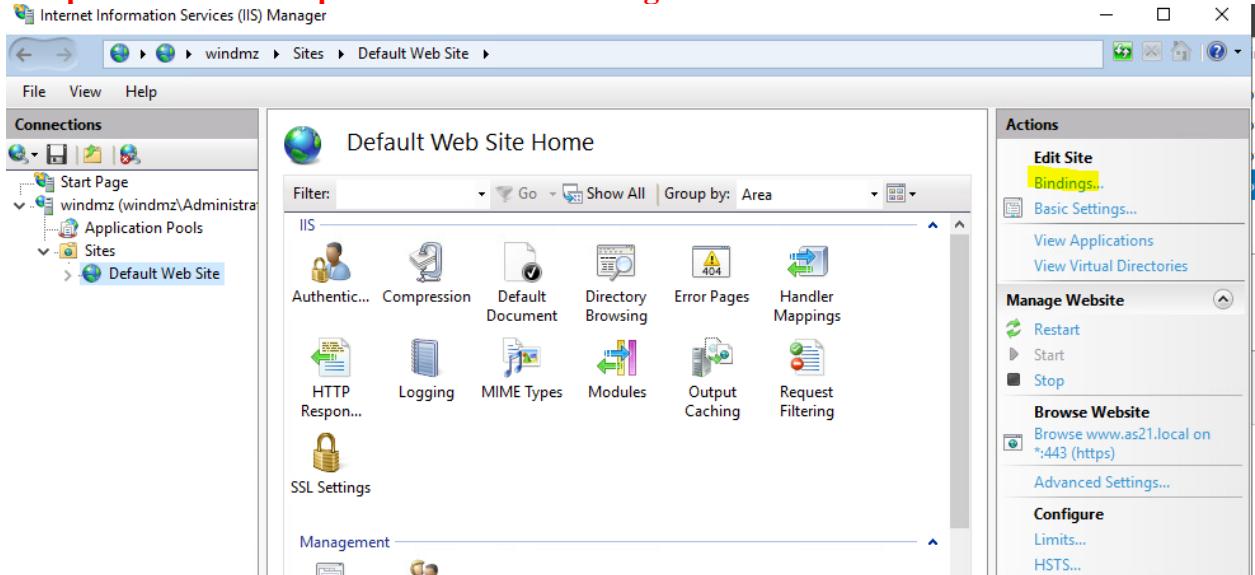


Нажимаем Connect

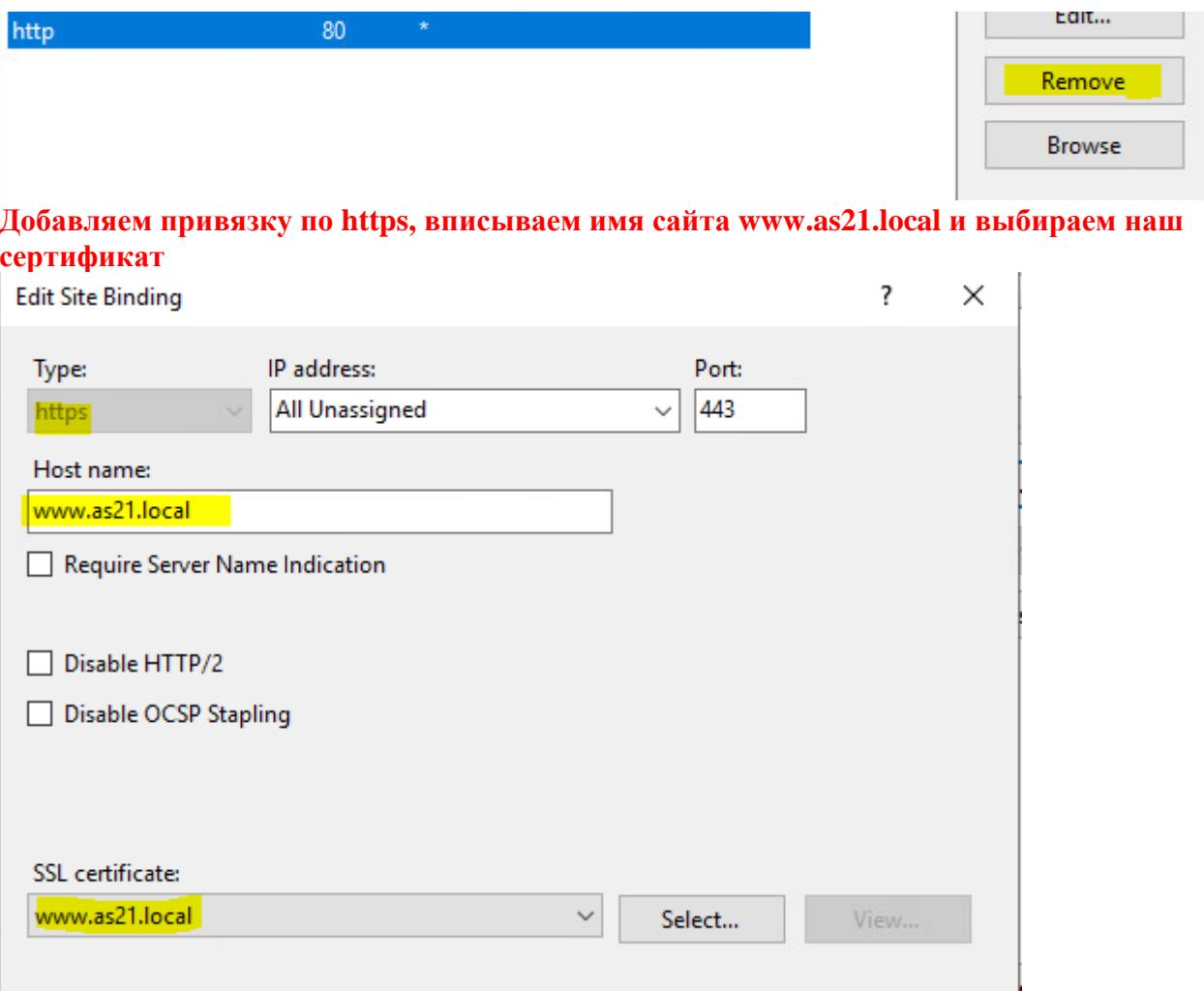
Важно!!! Если не сможет подключиться, нужно попробовать перезапустить службу на WINDMZ. Для этого идем на WINDMZ и выполняем команду: Net start wmsvc

Настройка привязки (Bindings)

Открываем сайт и справа нажимаем Bindings



Удаляем имеющуюся там привязку по http



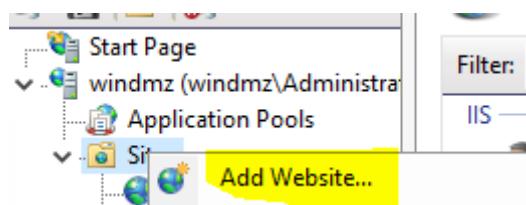
Site Bindings

Type	Host Name	Port	IP Address	Binding Information
https	www.as21.local	443	*	

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 *

Add Website

Site name: Bulk Application pool: Bulk Select...

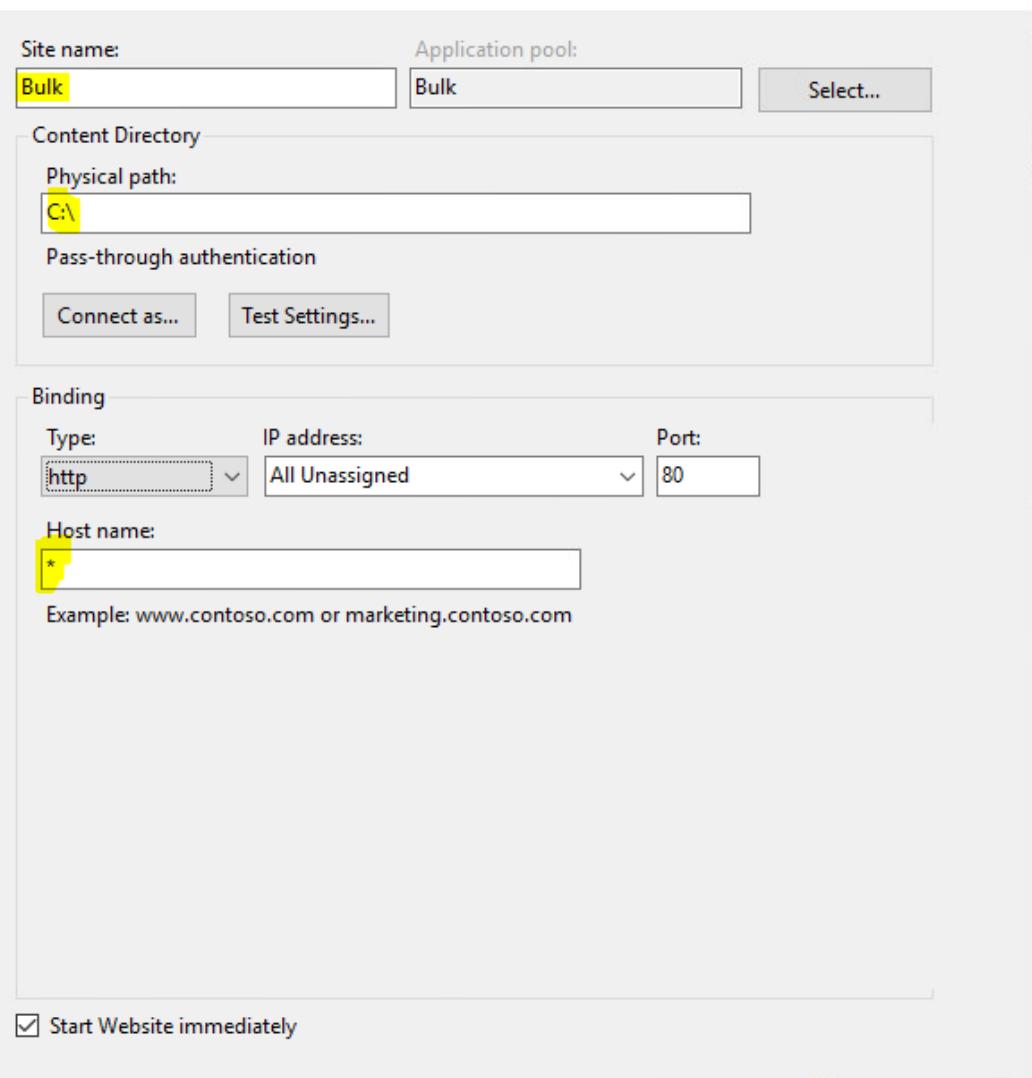
Content Directory
Physical path: C:\

Pass-through authentication
Connect as... Test Settings...

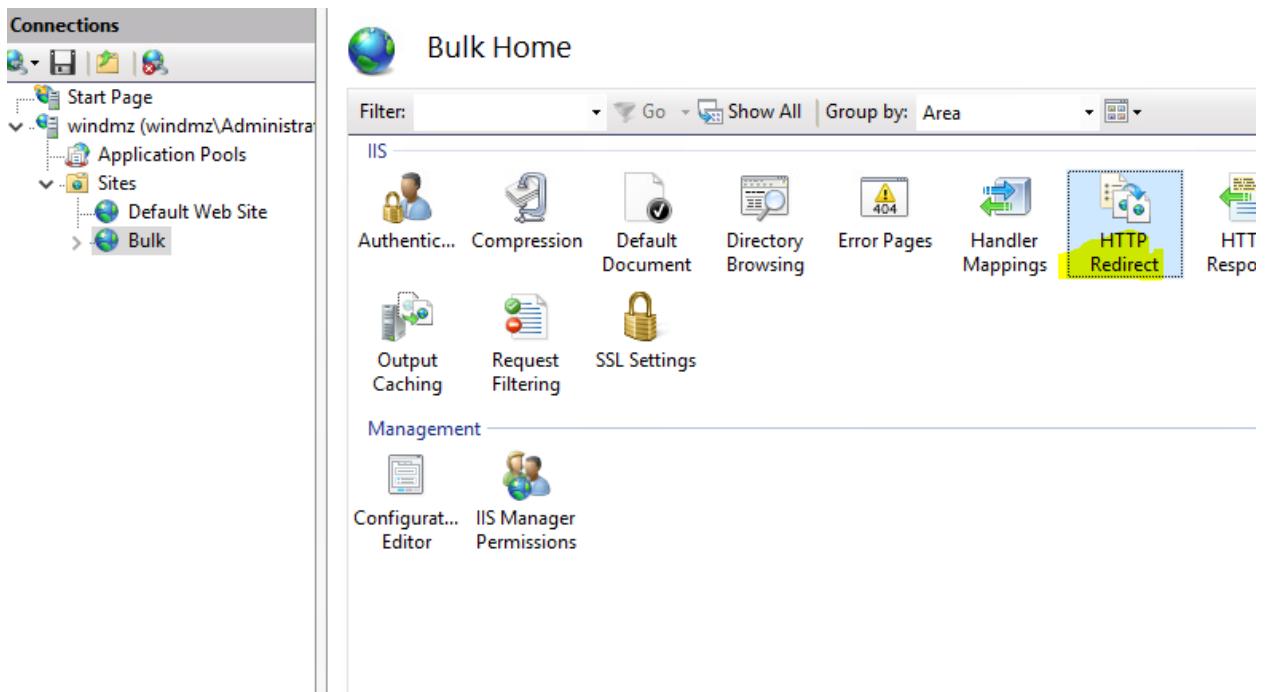
Binding
Type: http IP address: All Unassigned Port: 80
Host name: *

Example: www.contoso.com or marketing.contoso.com

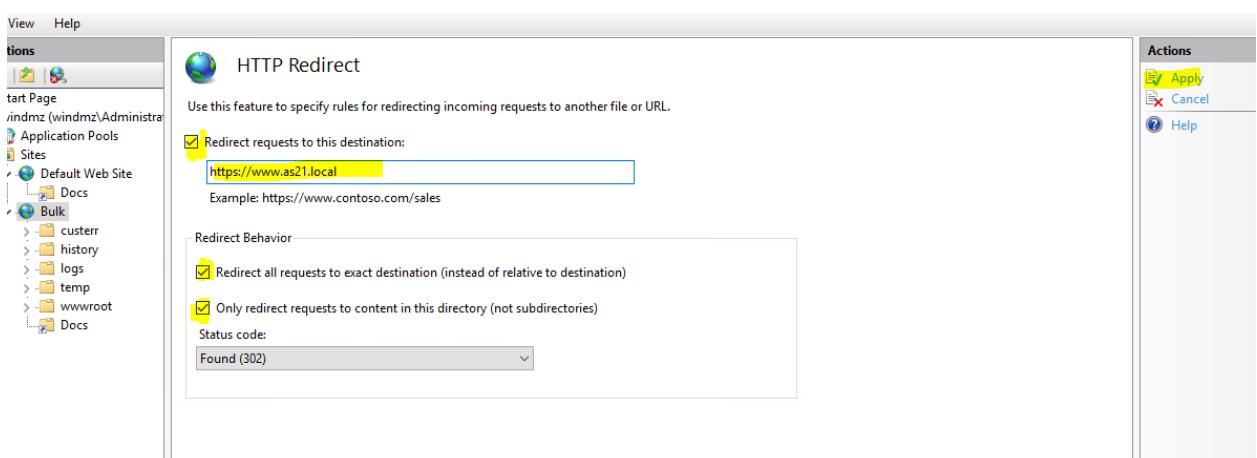
Start Website immediately



В настройках НОВОГО сайта заглушки идем в HTTP Redirect



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



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

Виртуальный каталог Docs

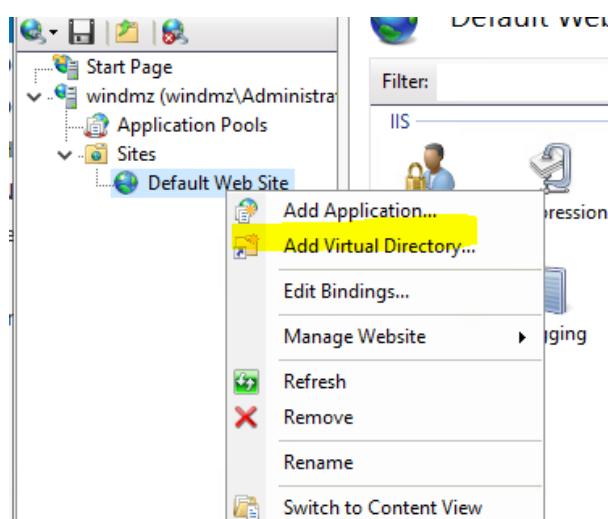
Внутри сайта создайте виртуальный каталог Docs. Поместите в него текстовый файл Test.txt. Включите возможность обзора содержимого каталога при подключении к нему пользователей через браузер.

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

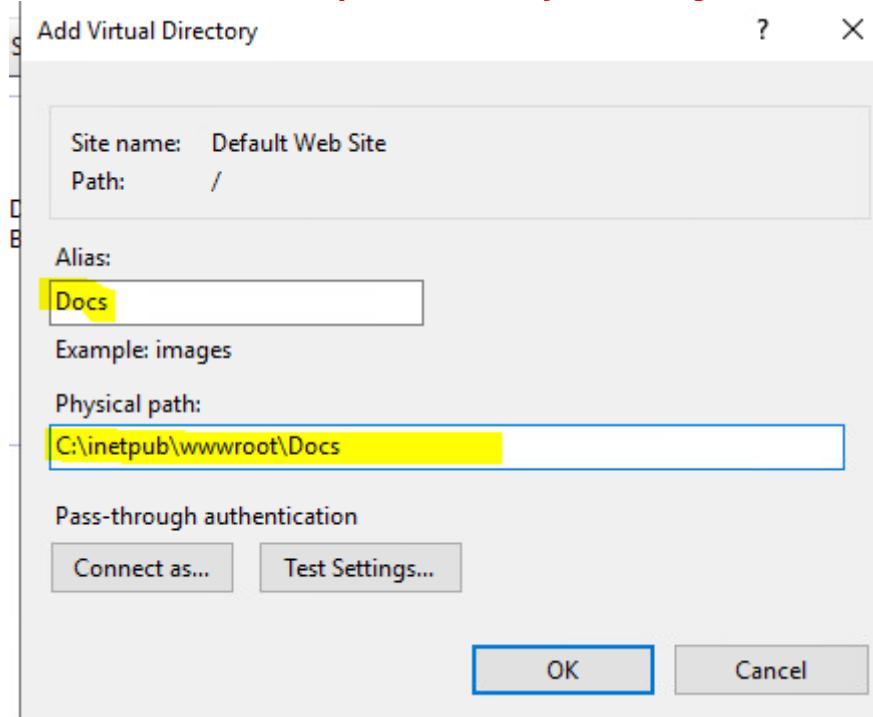
Network > windmz > CS > inetpub > wwwroot >

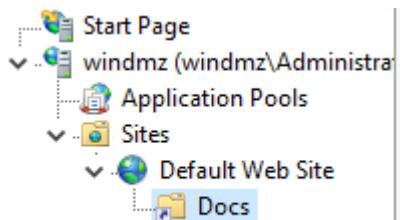
	Name	Date modified	Type	Size
ss	Docs	7/31/2021 4:18 PM	File folder	
ls	iisstart	7/31/2021 4:07 PM	HTML Document	
ts	iisstart	7/31/2021 4:07 PM	PNG File	
	index	7/31/2021 4:17 PM	HTML Document	
: (C:)				

Нажимаем правую кнопку на сайте и выбираем Add Virtual Directory



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



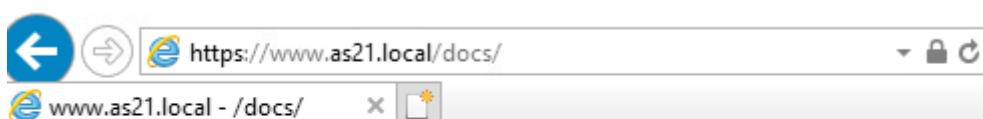


Выбираем Docs и открываем Directory Browsing

The screenshot shows the IIS Manager interface. On the left, the 'Connections' pane displays the site structure. In the center, the 'Docs Home' page is shown with various configuration icons. One of these icons, 'Directory Browsing', is highlighted with a yellow box.

Нажимаем Enable

The screenshot shows the 'Directory Browsing' configuration page. It lists several options: Time, Size, Extension, Date, and Long date. A checkbox next to 'Time' is checked. On the right side, there is an 'Actions' panel with an 'Enable' button, which is also highlighted with a yellow box.



www.as21.local - /docs/

[\[To Parent Directory\]](#)

7/29/2021 3:31 PM	0 Test.txt
7/29/2021 3:34 PM	168 web.config

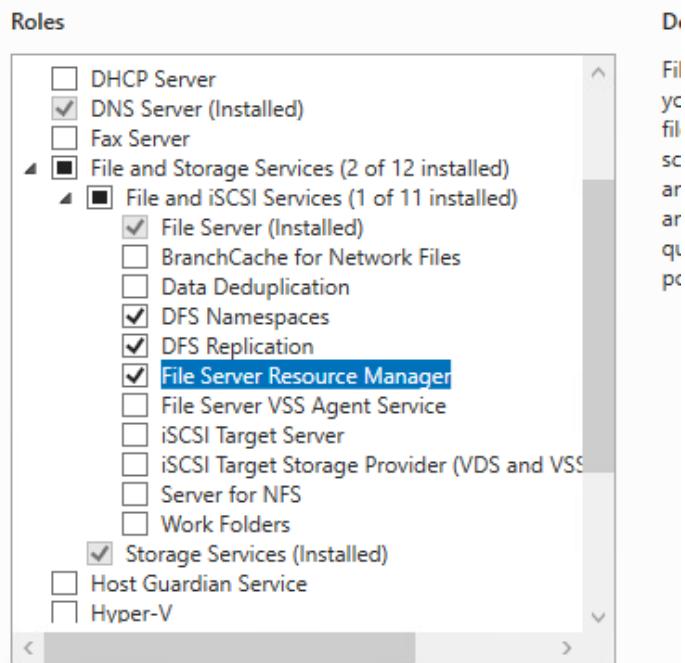
Настройка файловых служб на ЦОД (WINSRV1 и WINSRV2)

Настройка DFS

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

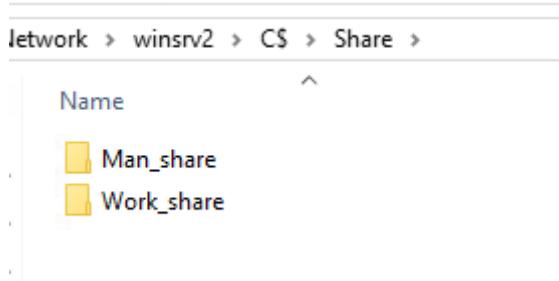
Заходим на WINSRV2 и через сервер менеджер ставим 3 службы на WINSRV1 и WINSRV2

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



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.



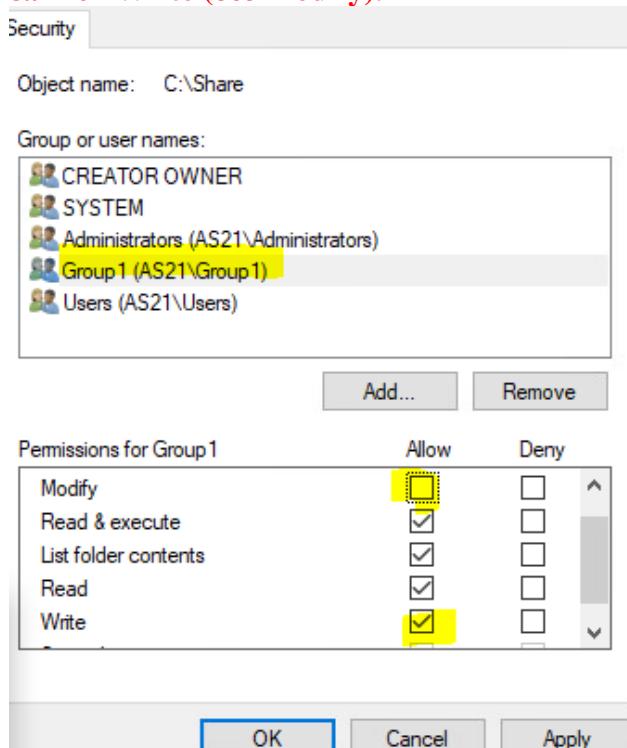
The screenshot shows the 'Shares' section of the File and Storage Services management console. On the left, a navigation pane lists 'Servers', 'Volumes', 'Disks', 'Storage Pools', 'Shares' (which is selected), 'iSCSI', and 'Work Folders'. The main area displays a table of existing shares under the heading 'SHARES' with a count of '4 total'. The table includes columns for 'Share' and 'Local Path'. The shares listed are: 'WINSRV1 (2)' (NETLOGON at C:\Windows\SYSVOL\sysvol\as2 and SYSVOL at C:\Windows\SYSVOL\sysvol), and 'WINSRV2 (2)' (CertEnroll at C:\Windows\system32\CertSrv\ and FS at C:\DFSRoots\FS). A 'TASKS' dropdown menu is open, with 'New Share...' highlighted. A 'VOLUME' summary on the right indicates 'NETLOGON on WIL' with '58.5% Used'.

This screenshot shows the 'Share Location' step of a 'New Share' wizard. On the left, a sidebar lists steps: 'Select Profile' (selected), 'Share Location' (highlighted in blue), 'Share Name', 'Other Settings', 'Permissions', 'Confirmation', and 'Results'. The main area shows 'Server:' information for two servers: 'WINSRV1' (Online, Not Clustered) and 'WINSRV2' (Online, Not Clustered). Below this is a 'Share location:' section. It contains a radio button for 'Select by volume:' which is selected, and a table showing 'Volume' (C:), 'Free Space' (8.05 GB), 'Capacity' (19.4 GB), and 'File System' (NTFS). There is also an option for 'Type a custom path:' with a text input field containing 'C:\share' and a 'Browse...' button.

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

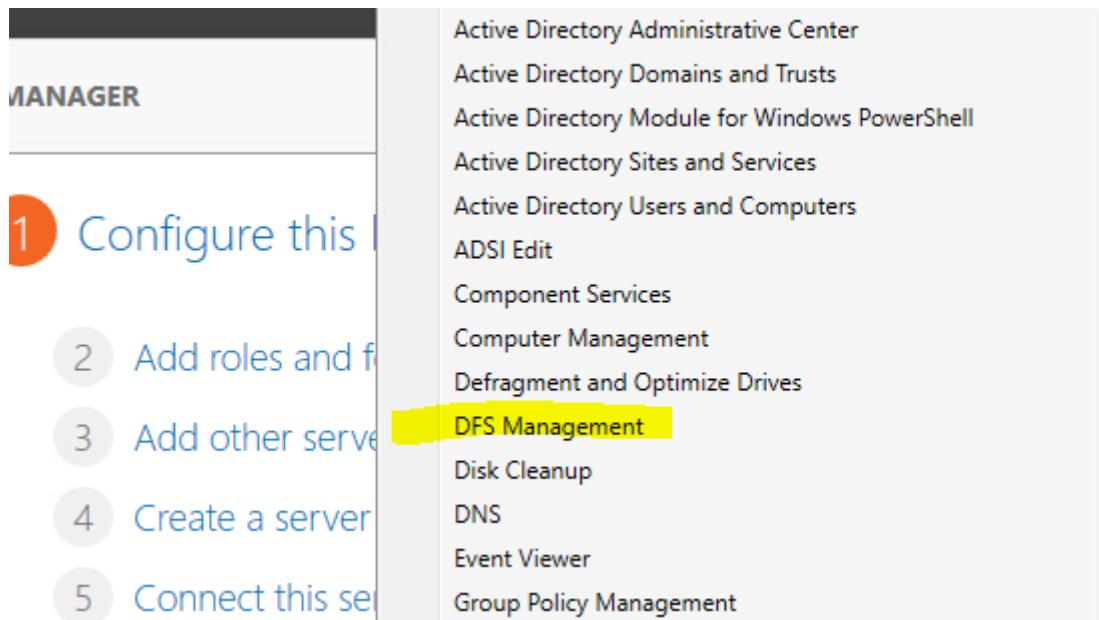
WINSRV1 (3)	
NETLOGON	C:\Windows\SYSVOL\sysvol\as2
SYSVOL	C:\Windows\SYSVOL\sysvol
share	C:\share
WINSRV2 (3)	
CertEnroll	C:\Windows\system32\CertSrv\
FS	C:\DFSRoots\FS
share	C:\share

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

DFS Management

Namespaces

Replication

Getting Started

Use this snap-in to create and manage Distributed File System (DFS) namespaces and replication groups.

DFS Management Tasks

Publish Data to Multiple Servers

Create a namespace to make shared folders located on multiple servers appear as a single tree of folders. To increase redundancy of the folders or make them available to users in remote locations, use DFS Replication to keep the content synchronized on multiple servers.

Collect Data for Backup Purposes

Use DFS Replication to replicate data from a server in a branch office to a server in a hub office or data center for backup purposes. You can optionally publish the content in a namespace to ensure that branch offices always connect to the branch office of the hub office.

Actions

DFS Management

New Namespace...

New Replication Group...

Add Namespaces to Di...

Add Replication Group...

View

New Window from Here

Help

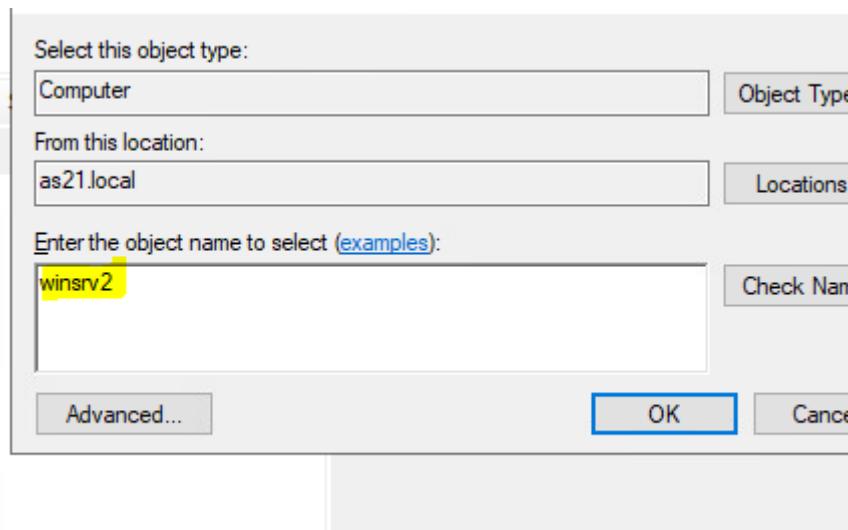
Steps:

- Namespace Server
- Namespace Name and Settings
- Namespace Type
- Review Settings and Create Namespace
- Confirmation

Enter the name of the server that will host the namespace. The server you specify will be known as the namespace server.

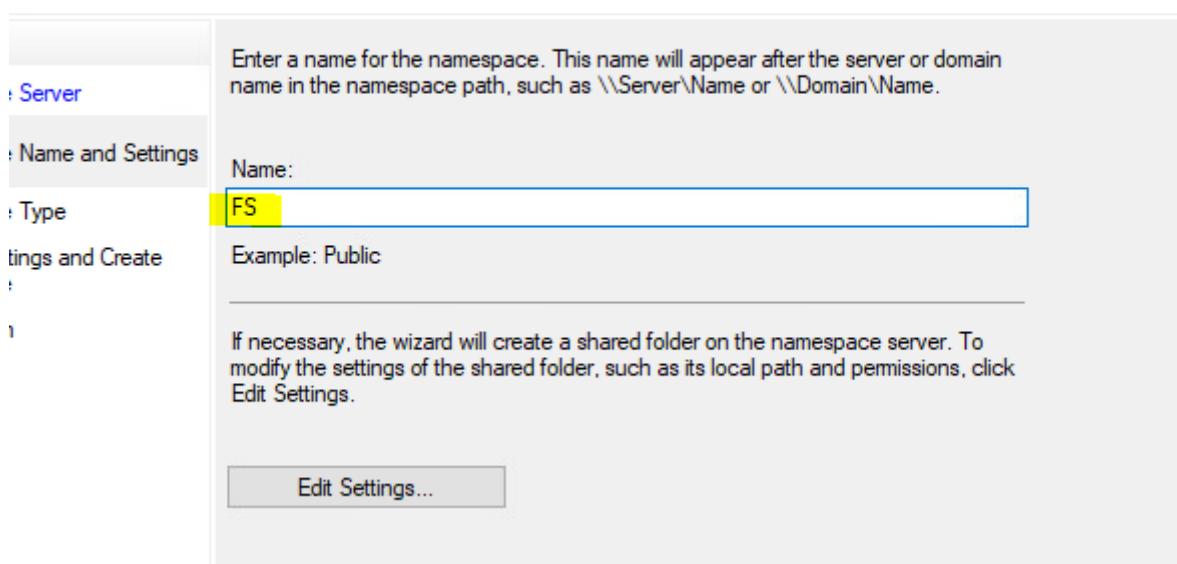
Server: **Browse...**

Выбираем первый сервер (можно выбрать WINSRV2)

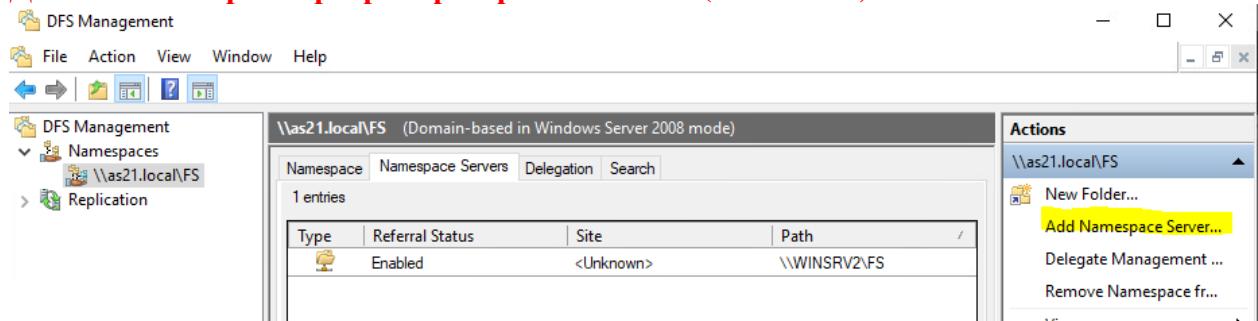


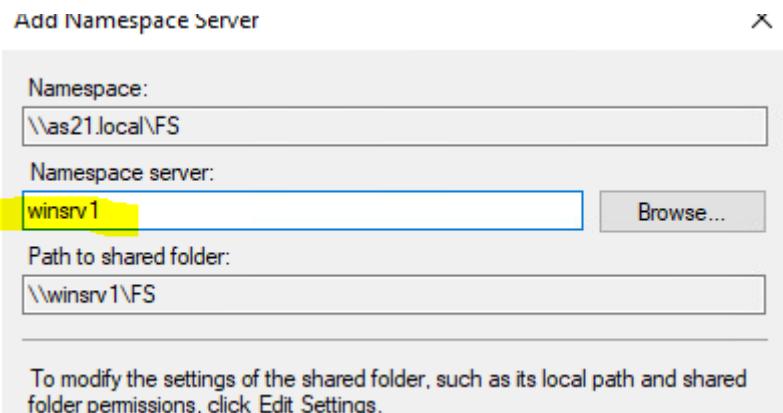
Выбираем имя FS на для нашего DFS

Namespace Name and Settings

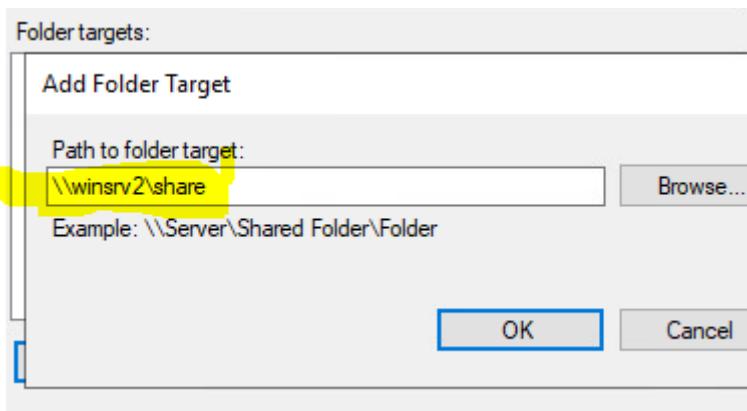


Добавляем второй сервер в пространство имен (WINSRV1)

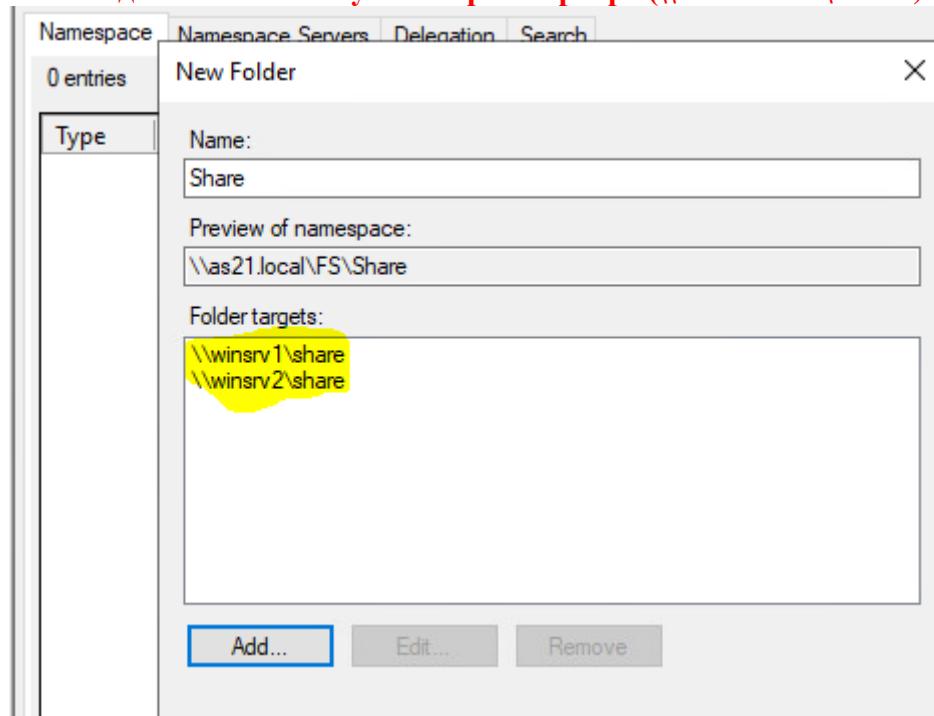




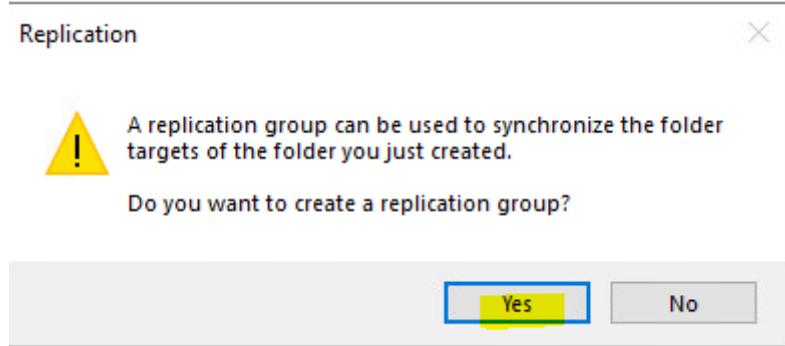
Добавляем папку для репликации. Указываем путь формата \\сервер\папка (\\WINSRV2\Share)



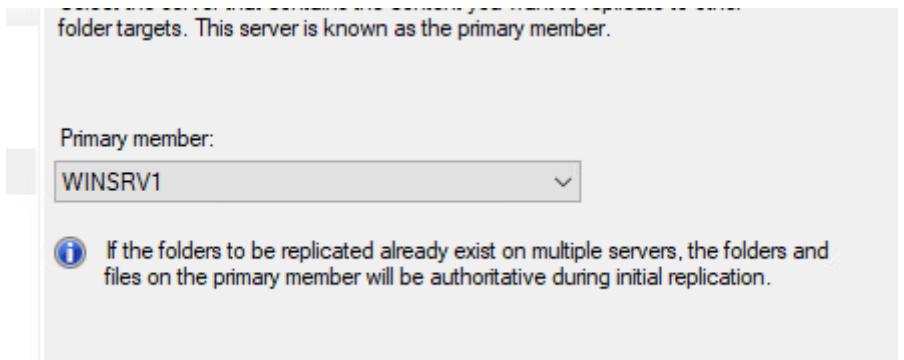
Так же добавляем папку на втором сервере (\\\\WINSRV1\\Share)



Соглашаемся на создание группы репликации



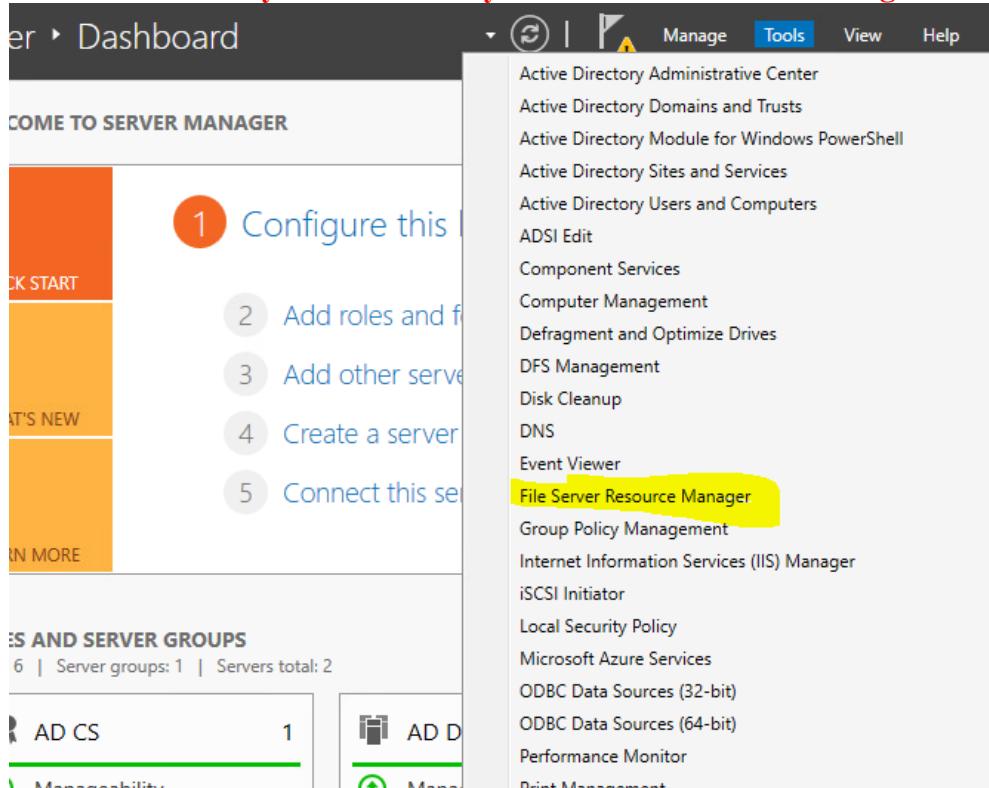
Там везде «Next» (нас все устраивает). В последнем вопросе выбираем главный сервер для репликации – WINSRV1



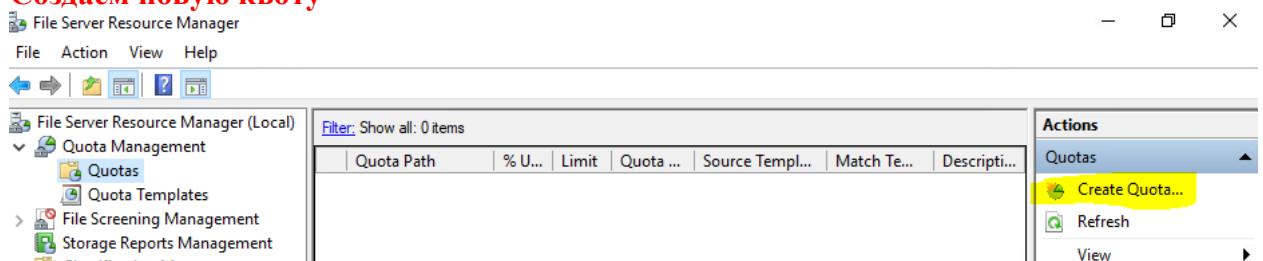
Настройка квот

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

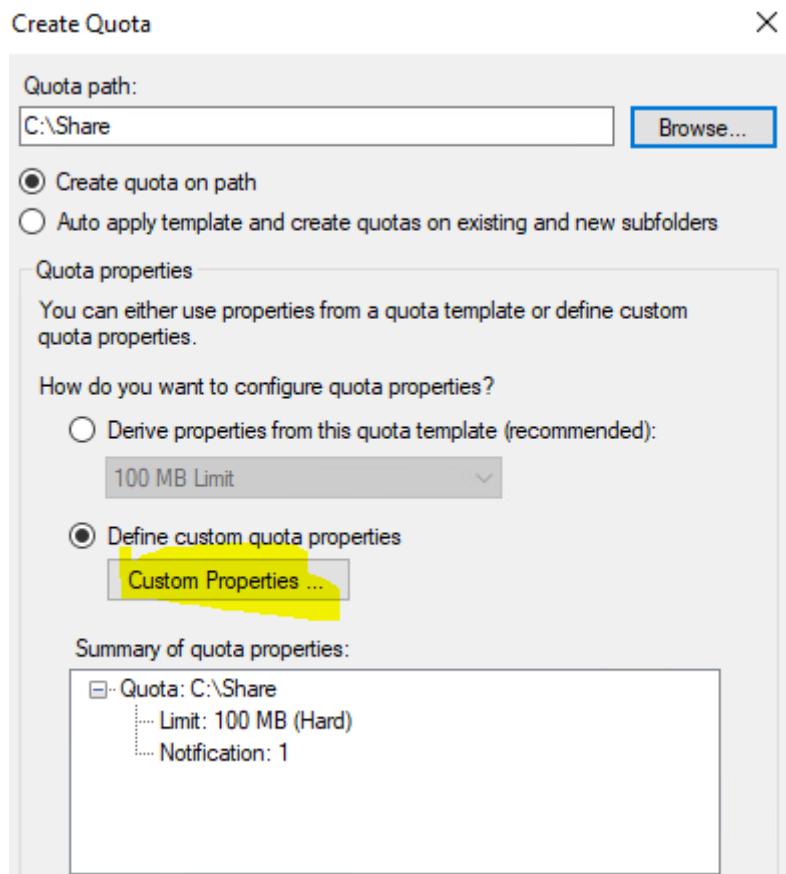
На WINSRV1 запускаем оснастку File Server Resource Manager



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

10 GB Limit

Settings

Quota path:
C:\Share

Description (optional):

Space limit

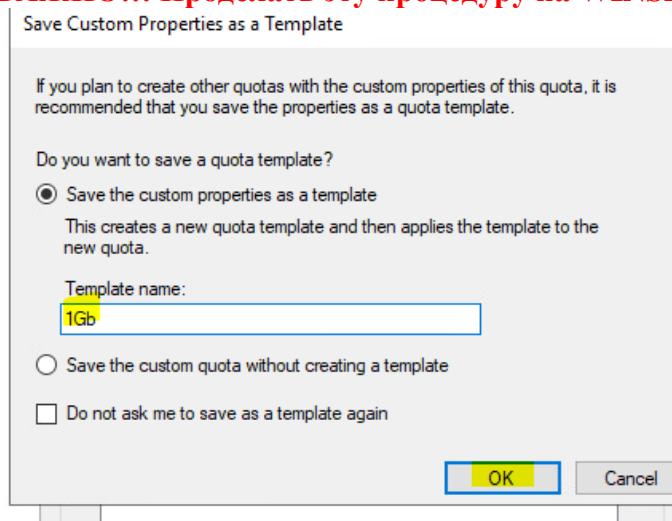
Limit:
1

Hard quota: Do not allow users to exceed limit
 Soft quota: Allow users to exceed limit (use for monitoring)

Notification thresholds

Threshold	E-mail	Event Log	Command	Report

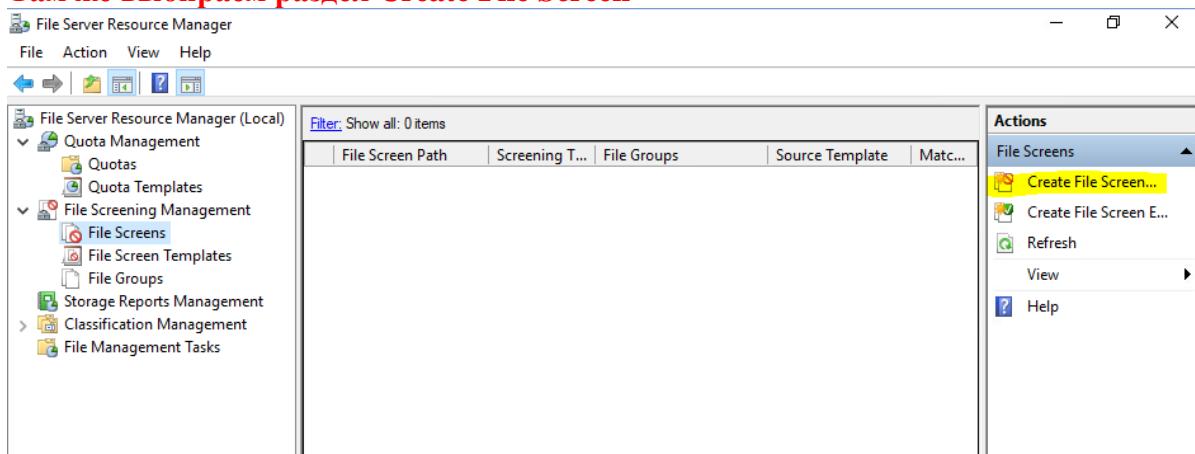
**Сохраняем шаблон для нашей квоты и саму квоту.
ВАЖНО!!! Проделать эту процедуру на WINSRV1 и WINSRV2**



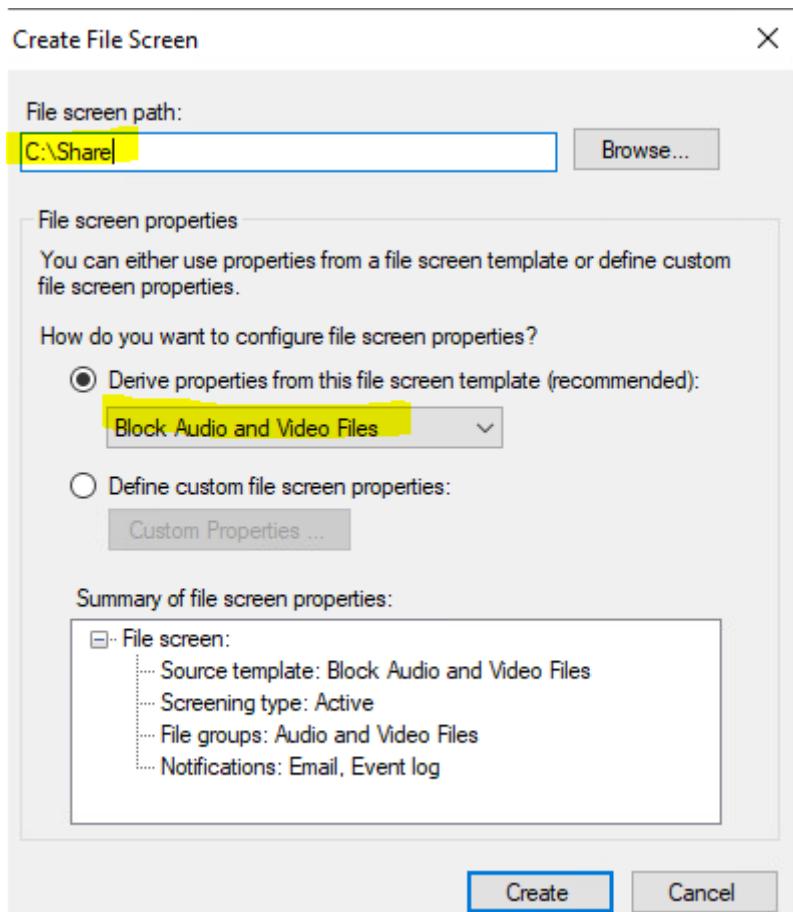
Настройка запрета на хранение файлов

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

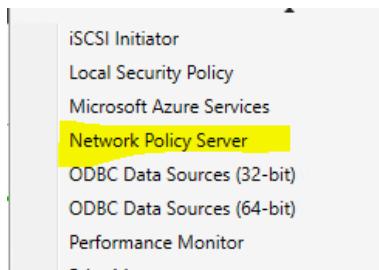
10. На всех компьютерах под управлением ОС Microsoft Windows обеспечьте функционирование Defender Firewall. При этом работоспособность настроенных ранее сервисов не должна нарушиться.

Настройка NPS

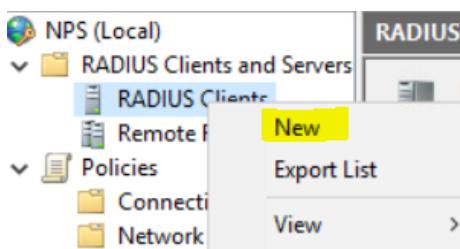
Настройка политики

Select one or more roles to install on the selected server.	
	Description
<input checked="" type="checkbox"/> Active Directory Certificate Services (1 of 6 installed)	Provides secure communication for Active Directory.
<input checked="" type="checkbox"/> Active Directory Domain Services (Installed)	Manages users, groups, and resources in a domain.
<input type="checkbox"/> Active Directory Federation Services	Allows users from different domains to access resources.
<input type="checkbox"/> Active Directory Lightweight Directory Services	Provides a simplified version of Active Directory for mobile devices.
<input type="checkbox"/> Active Directory Rights Management Services	Manages digital rights for files and documents.
<input type="checkbox"/> Device Health Attestation	Monitors the health of devices connected to the network.
<input checked="" type="checkbox"/> DHCP Server (Installed)	Assigns IP addresses dynamically.
<input checked="" type="checkbox"/> DNS Server (Installed)	Maps domain names to IP addresses.
<input type="checkbox"/> Fax Server	Manages fax services.
<input checked="" type="checkbox"/> File and Storage Services (2 of 12 installed)	Manages storage and file sharing.
<input type="checkbox"/> Host Guardian Service	Protects hosts from malicious software.
<input type="checkbox"/> Hyper-V	Manages virtual machines.
<input checked="" type="checkbox"/> Network Policy and Access Services	Provides Network Policy Server (NPS), which helps safeguard the security of your network.
<input type="checkbox"/> Print and Document Services	Manages printing and document sharing.

Запускаем оконочку Network Policy Server



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



Вводим:

Friendly name – Cisco

Address (IP or DNS) – ip адрес устройства

Shared Secret – произвольный пароль, который нужно прописать в устройстве

A screenshot of the 'New RADIUS Client' dialog box. It has two tabs: 'Settings' (selected) and 'Advanced'.

- Enable this RADIUS client
- Select an existing template:
[dropdown menu]

Name and Address

Friendly name:

Address (IP or DNS):

Shared Secret

Select an existing Shared Secrets template:
[dropdown menu] None

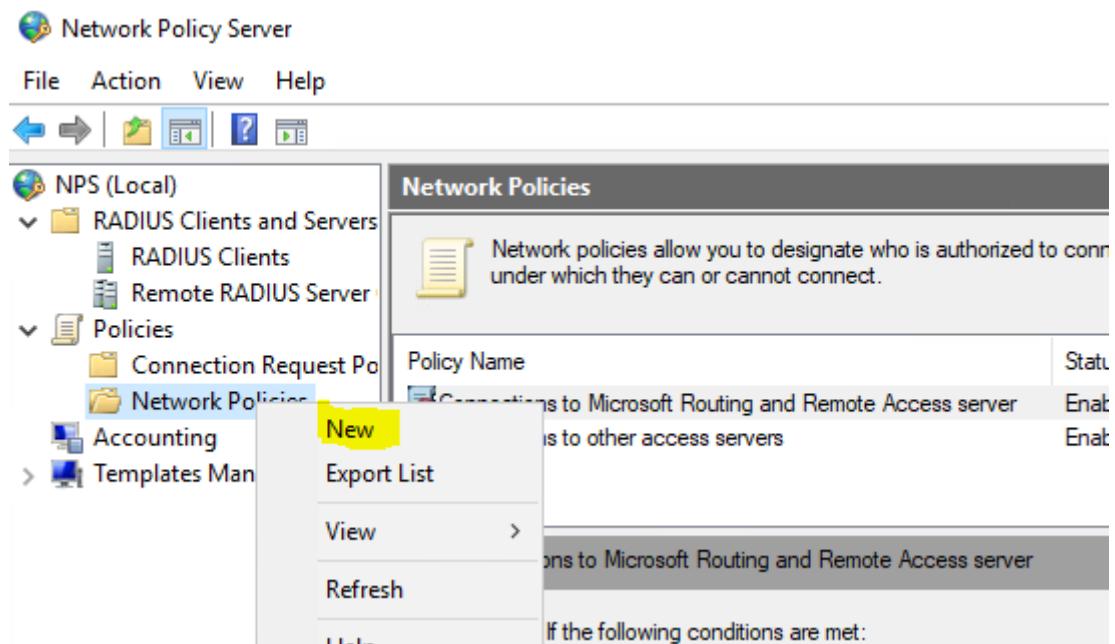
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual Generate

Shared secret:

Confirm shared secret:

Идем в Policies > Network Policies -> New



Создаем новую политику. Вводим имя политики

This screenshot shows the 'New Policy' configuration dialog. The 'Policy name:' field is filled with 'Cisco' (highlighted with a yellow box). The 'Network connection method' section is visible, containing a descriptive text about selecting the type of network access server. Two radio button options are present: 'Type of network access server:' (selected) and 'Vendor specific:'.

Policy name:
Cisco

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating, select Unspecified.

Type of network access server:
Unspecified

Vendor specific:
10

Добавляем условия срабатывания

Conditions:

Condition	Value

Condition description:

Add... **Edit...** **Remove**

Windows Group (группа безопасности из Active Directory)

Select a condition, and then click Add.

Groups

- Windows Groups**
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.
- Machine Groups**
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.
- User Groups**
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

Day and time restrictions

- Day and Time Restrictions**
Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.

Connection Properties

Add...

Добавляем группу безопасности (Domain Users)

Windows Groups

Specify the group membership required to match:

Groups

Add Groups...

Select Group

Select this object type:
Group

From this location:
as21.local

Enter the object name to select (examples):
Domain Users

Advanced...

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

Select a condition, and then click Add.

Calling Station ID
The Calling Station ID condition specifies the network access server telephone number dialed by the access client.

Client Friendly Name
The Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connection request to NPS.

Client IPv4 Address
The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.

Client IPv6 Address
The Client IPv6 Address condition specifies the IPv6 address of the RADIUS client that forwarded the connection request to NPS.

Client Vendor
The Client Vendor Condition specifies the name of the vendor of the RADIUS client that sends connection requests to NPS.

Add...

Specify the conditions that determine whether this network policy is evaluated for a connection request. A maximum of one condition is required.

Select condition

Select a condition, and then click Add.

Calling Station ID
The Calling Station ID condition specifies the network access server telephone number dialed by the access client.

Client Friendly Name
The Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connection request to NPS.

Client IPv4 Address
The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.

Client IPv6 Address
The Client IPv6 Address condition specifies the IPv6 address of the RADIUS client that forwarded the connection request to NPS.

Client Vendor
The Client Vendor Condition specifies the name of the vendor of the RADIUS client that sends connection requests to NPS.

Cisco

OK Cancel

Add... Cancel Remove

Убираем стандартную настройку Framed-Protocol = PPP

Settings:

RADIUS Attributes

Standard

Vendor Specific

Routing and Remote Access

Multilink and Bandwidth Allocation Protocol (BAP)

IP Filters

Encryption

IP Settings

To send additional attributes to RADIUS clients, select a R then click Edit. If you do not configure an attribute, it is not your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Add... Edit... Remove

И меняем Service-Type = Framed на Login

Attribute Information

Attribute name:
Service-Type

Attribute number:
6

Attribute format:
Enumerator

Attribute Value:

Commonly used for Dial-Up or VPN
 Commonly used for 802.1x
 <none>
 Others

Login
<none>
Login
Callback Login
Outbound
Administrative
NAS Prompt
Callback Nas Prompt
Callback Administrative
Authorize only

Cisco Properties

Overview Conditions Constraints Settings

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes <input checked="" type="radio"/> Standard <input checked="" type="checkbox"/> Vendor Specific	To send additional attributes to RADIUS clients, select a RADIUS then click Edit. If you do not configure an attribute, it is not sent to your RADIUS client documentation for required attributes.
--	---

Attributes:

Name	Value
Service-Type	Login

В разделе Vendor Specific добавляем атрибут

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes <input checked="" type="radio"/> Standard <input checked="" type="checkbox"/> Vendor Specific	To send additional attributes to RADIUS clients, select a RADIUS then click Edit. If you do not configure an attribute, it is not sent to your RADIUS client documentation for required attributes.
--	---

Attributes:

Name	Vendor	Value

Add... Edit... Remove

Выбираем Vendor – Cisco

Атрибут – Cisco-AV-Pair

Vendor:

Cisco

Attributes:

Name	Vendor
Cisco-AV-Pair	Cisco

Description:

Specifies the Cisco AV Pair VSA.

Add... Close

This screenshot shows a configuration dialog box. At the top, a dropdown menu is set to 'Cisco'. Below it, a table lists an attribute named 'Cisco-AV-Pair' with its vendor set to 'Cisco'. A descriptive text below the table states 'Specifies the Cisco AV Pair VSA.' At the bottom right are 'Add...' and 'Close' buttons.

В значении атрибута прописываем shell:priv-lvl=15

Attribute information

Attribute name:
Cisco-AV-Pair

Attribute number:
5000

Attribute format:
String

Attribute value:
shell:priv-lvl=15

This screenshot shows the 'Attribute information' dialog for the 'Cisco-AV-Pair' attribute. It displays the attribute name as 'Cisco-AV-Pair', attribute number as '5000', format as 'String', and the current value as 'shell:priv-lvl=15'. The 'Attribute value' field is highlighted with a blue border.

CISCO PROPERTIES

Overview Conditions Constraints Settings

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

- Standard
- Vendor Specific

Routing and Remote Access

- Multilink and Bandwidth Allocation Protocol (BAP)
- IP Filters
- Encryption
- IP Settings

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Cisco-AV-Pair	Cisco	shell:priv-lvl=15

Add... Edit... Remove

Поднимаем нашу политику наверх

circumstances under which they can or cannot connect to the network.

Policy Name

- Connections to Microsoft Routing and Remote Access
- Connections to other access servers
- Cisco

Move Up

Move Down

Disable

Delete

Rename

Cisco

Conditions -

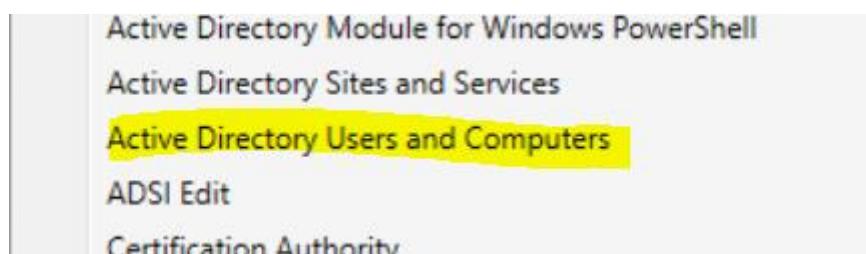
Condition

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

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

Разрешить подключение пользователя

Идем в Active Directory Users and Computers



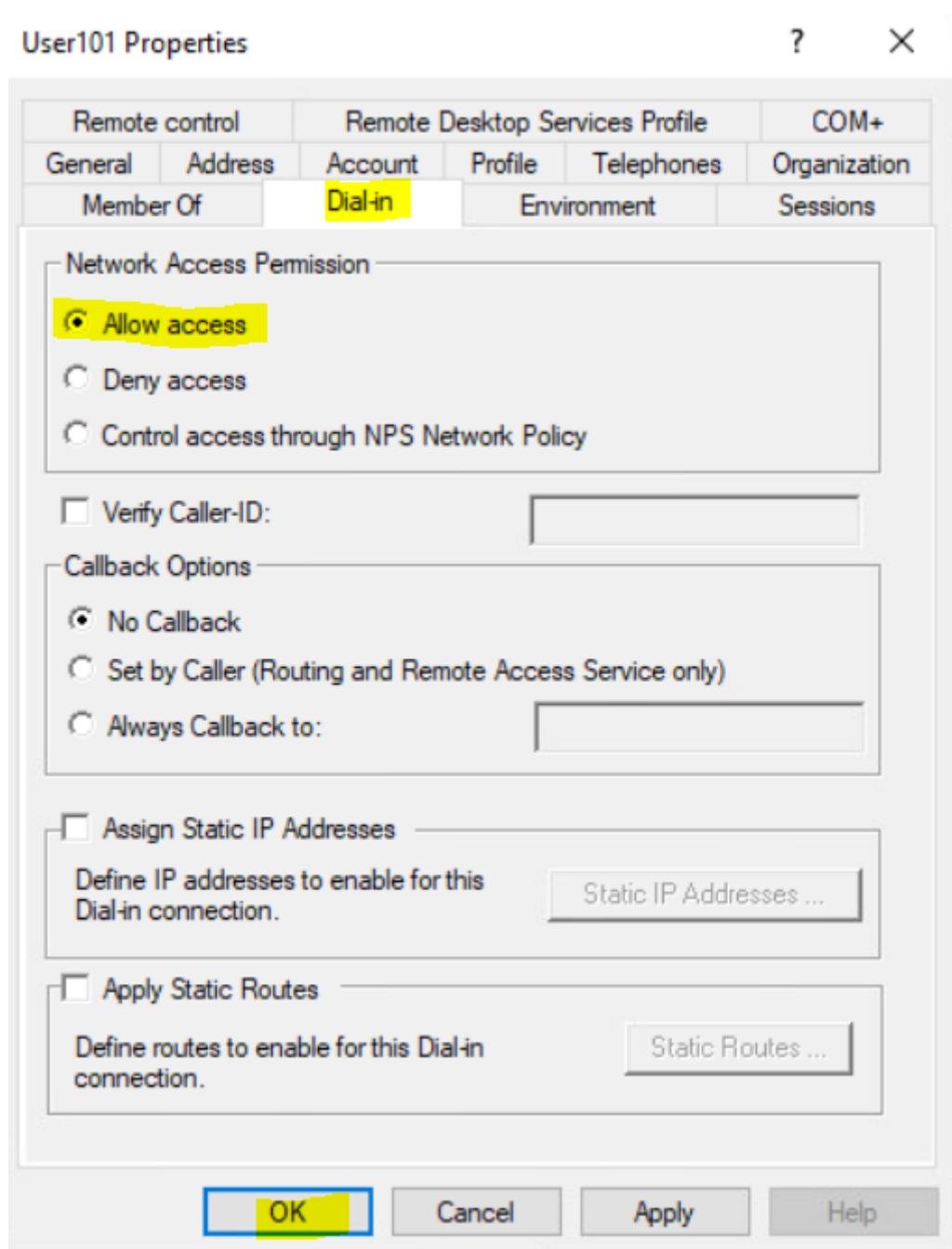
Выбираем пользователя, который должен подключаться. Вызываем его свойство

The screenshot shows the Active Directory Users and Computers console. The left pane shows a tree structure of Active Directory objects. In the center pane, a list of users is displayed. A context menu is open over a user account named "User". The menu options include:

- Copy...
- Add to a group...
- Disable Account
- Reset Password...
- Move...
- Open Home Page
- Send Mail
- All Tasks >
- Cut
- Delete
- Rename
- Properties** (highlighted in yellow)

A tooltip at the bottom left says: "Allows you to add the selected objects to a group".

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

Name	Group	Profile	Enabled	Action
RDC	All	Yes	Allow	
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes	Allow

В типе правила выбираем Port

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type (selected)
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

Program
Rule that controls connections for a program.

Port
Rule that controls connections for a TCP or UDP port.

Predefined:
Active Directory Domain Services
Rule that controls connections for a Windows experience.

Custom
Custom rule.

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

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

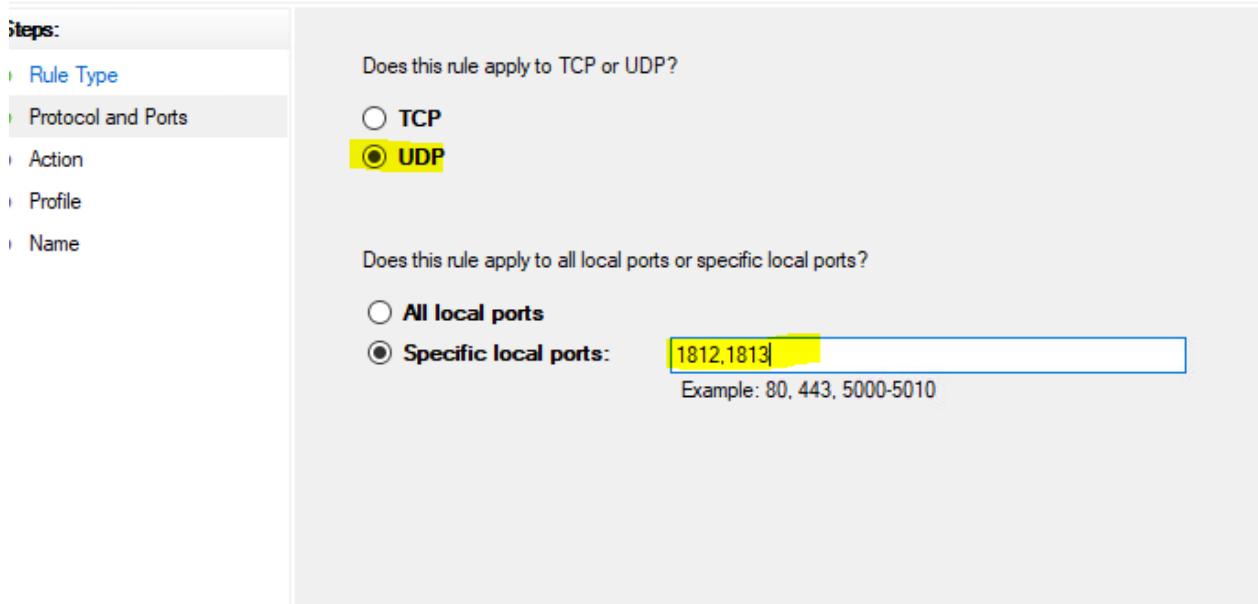
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

TCP
 UDP

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

All local ports
 Specific local ports:
Example: 80, 443, 5000-5010

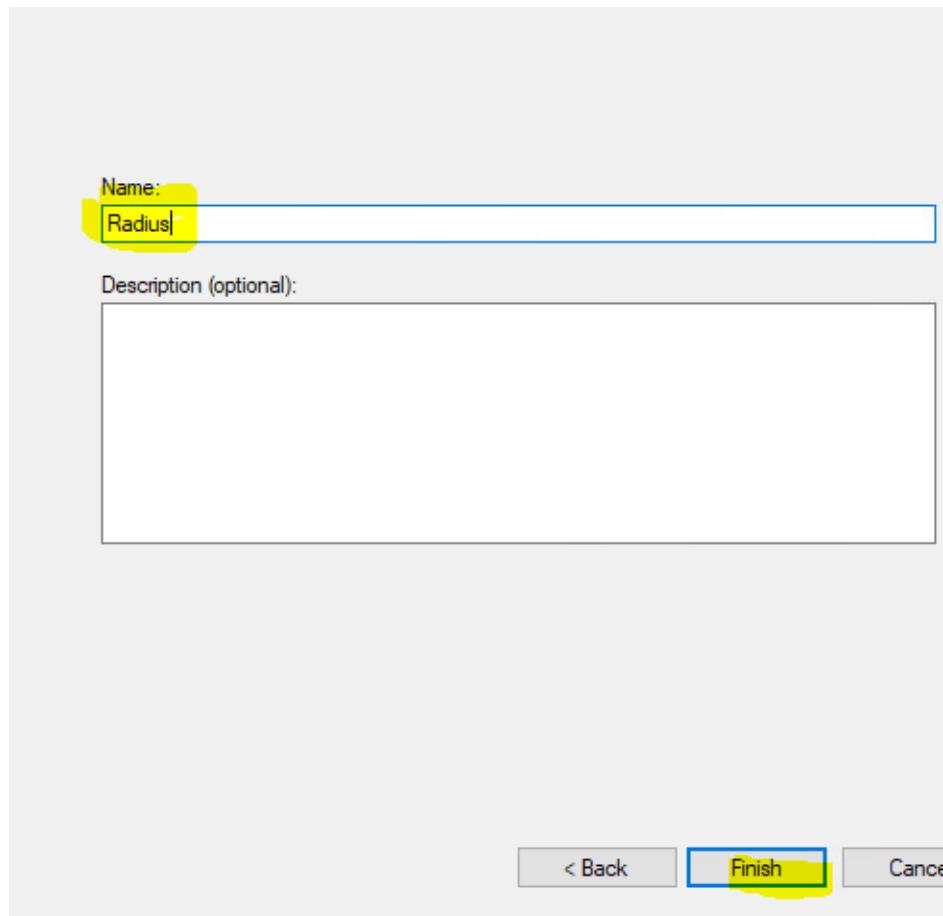


Вводим имя правила - Radius

Name:

Description (optional):

[< Back](#) [Finish](#) [Cancel](#)



Эмуляция Интернет

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

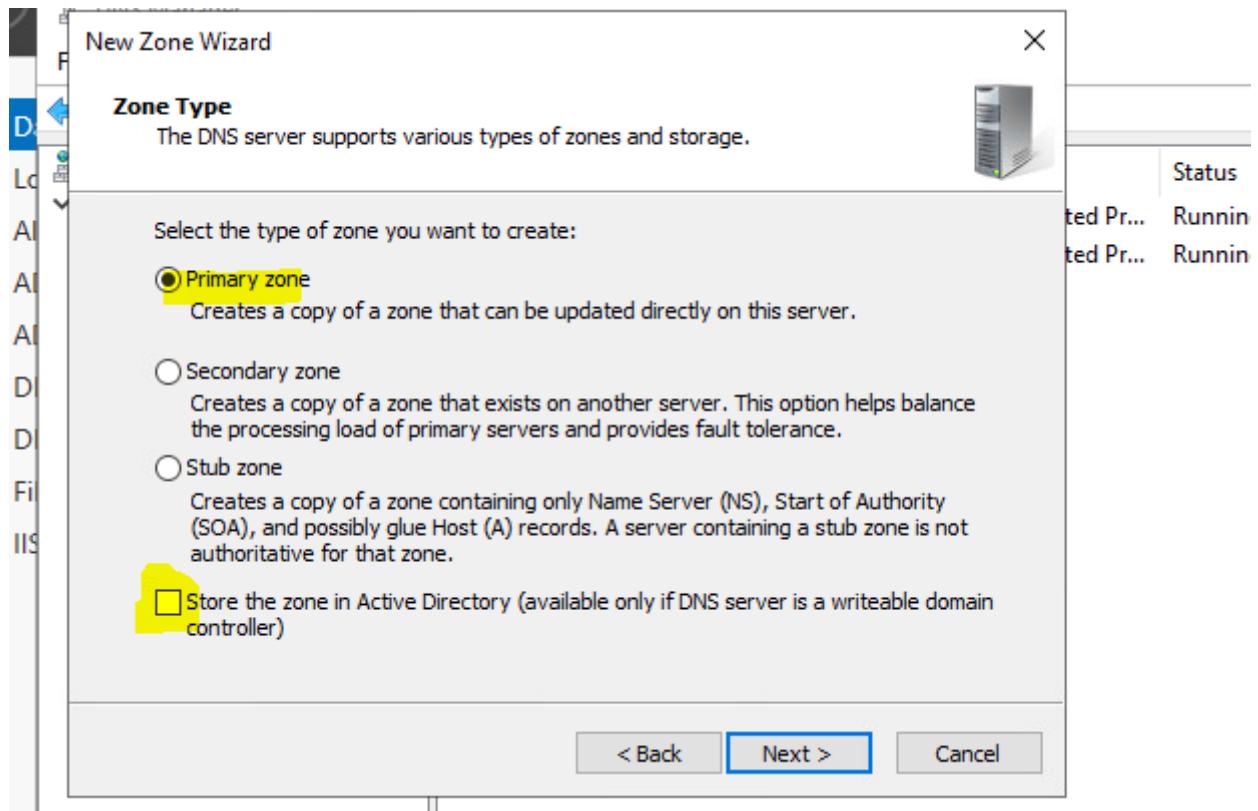
HKLM > SYSTEM > CurrentControlSet > Services > NlaSvc >Parameters > Internet

Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveDnsProbeContent	REG_SZ	131.107.255.255
ActiveDnsProbeContentV6	REG_SZ	fd3e:4f5a:5b81::1
ActiveDnsProbeHost	REG_SZ	dns.msftncsi.com
ActiveDnsProbeHostV6	REG_SZ	dns.msftncsi.com
ActiveWebProbeContent	REG_SZ	Microsoft Connect Test
ActiveWebProbeContentV6	REG_SZ	Microsoft Connect Test
ActiveWebProbeHost	REG_SZ	www.msftconnecttest.com
ActiveWebProbeHostV6	REG_SZ	www.msftconnecttest.com
ActiveWebProbePath	REG_SZ	ipv6.msftconnecttest.com
ActiveWebProbePathV6	REG_SZ	connectedtest.txt
EnableActiveProbing	REG_DWORD	0x00000001 (1)
PassivePollPeriod	REG_DWORD	0x0000000f (15)
StaleThreshold	REG_DWORD	0x0000001e (30)
WebTimeout	REG_DWORD	0x00000023 (35)

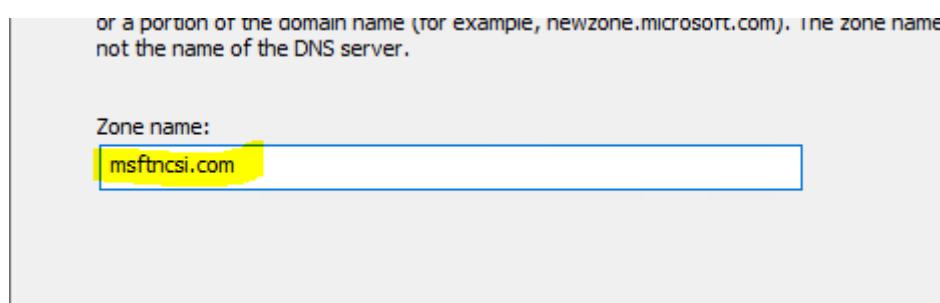
Запоминаем значения или не закрываем окно

Идем в DNS Manager

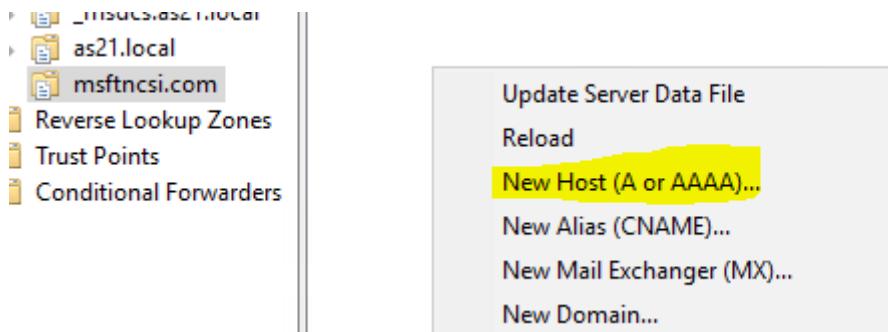
Создаем новую Primary zone. Не забываем убрать галку о хранении в Active Directory



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



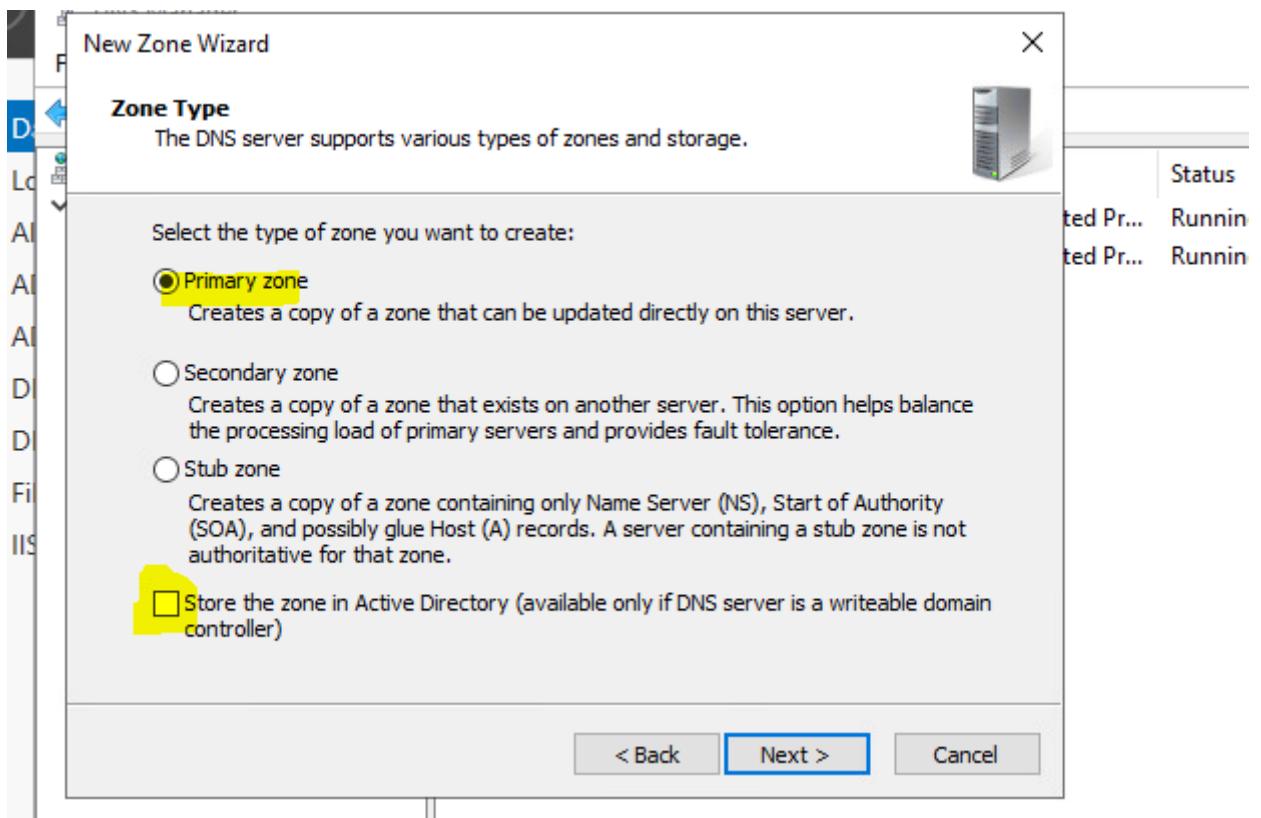
Внутри зоны создаем А запись



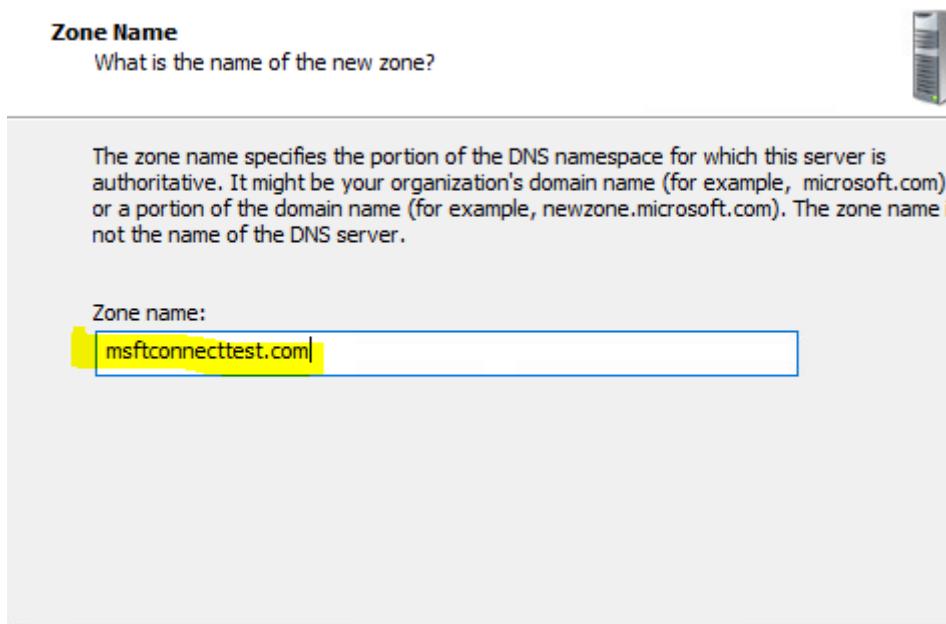
С именем dns и записью из поля ActiveDNSProbeContent – 131.107.255.255

The 'New Host' dialog is shown with the following fields:
Name (uses parent domain name if blank): dns
Fully qualified domain name (FQDN): dns.msftncsi.com.
IP address: 131.107.255.255
 Create associated pointer (PTR) record

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



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



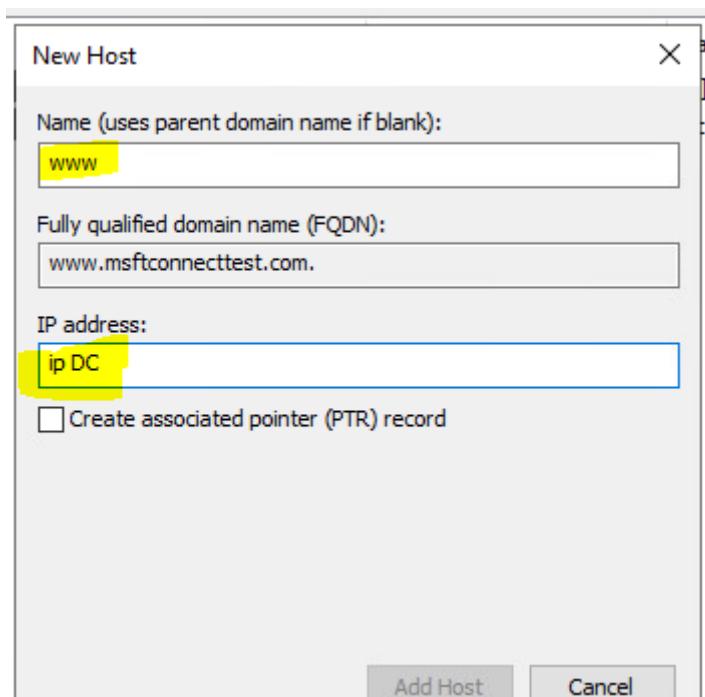
Внутри зоны создаем А запись

DNS

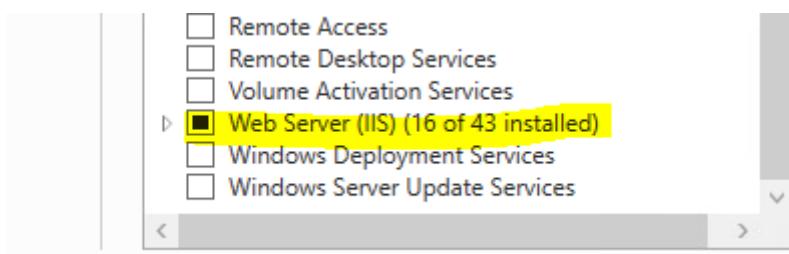
- DC
- Forward Lookup Zones
 - _msdcs.as21.local
 - as21.local
 - msftncsi.com
 - msftconnecttest.com
- Reverse Lookup Zones
- Trust Points
- Conditional Forwarders

Name	Type
(same as parent folder)	Start of Authority (SOA)
(same as parent folder)	Name Server (NS)

С именем www и записью ip адрес DC

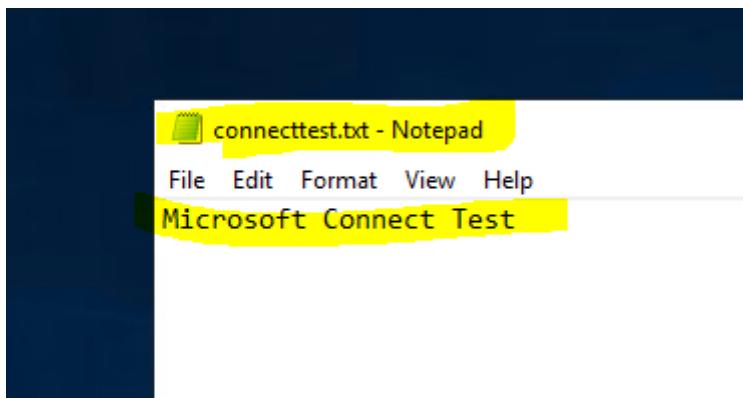


Устанавливаем IIS сервер на DC в стандартной комплектации

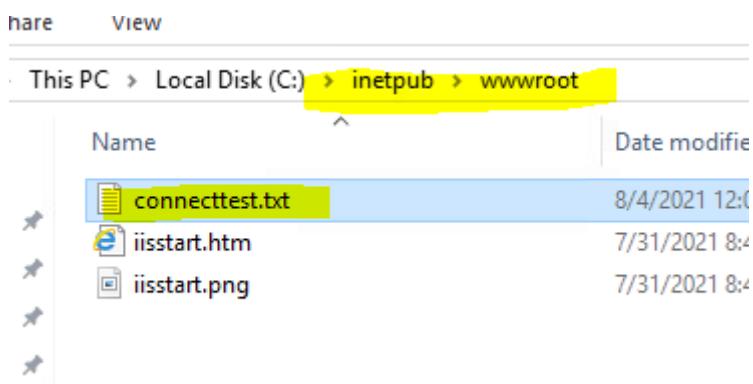


После установки создаем файл из ActiveWebProbePath – connecttest.txt (аккуратнее с расширениями файлов)

Внутри файла пишем из ActiveWebProbeContent – Microsoft Connect Test



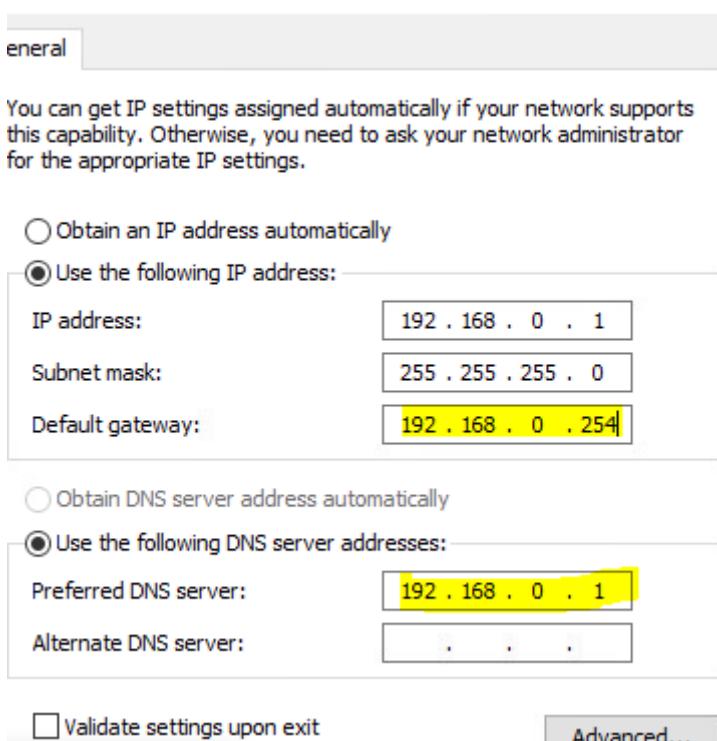
Кладем файл по пути – C:\inetpub\wwwroot



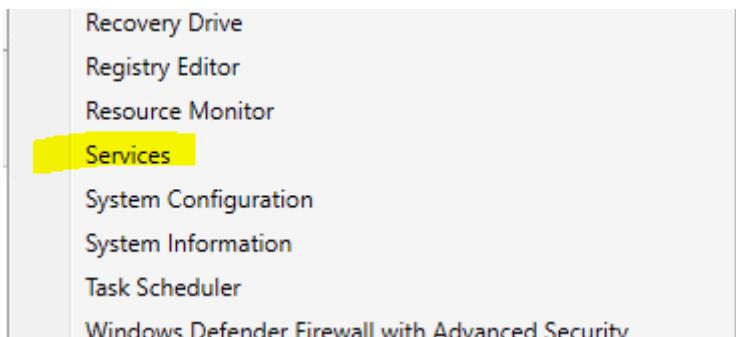
Открываем настройки адаптера на DC

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

Name	Description	Status	Startup Type	L
Microsoft Storage Spaces S...	Host service...	Manual	Manual	N
Microsoft Store Install Service	Provides inf...	Manual	Manual	L
Net.Tcp Port Sharing Service	Provides abi...	Disabled	Automatic	L
Netlogon	Maintains a ...	Running	Automatic	L
Network Connection Broker	Brokers con...	Running	Manual (Trig...	L
Network Connections	Manages o...	Running	Manual	L
Network Connectivity Assis...	Provides Dir...	Manual (Trig...	Automatic	L
Network List Service	Identifies th...	Running	Manual	L
Network Location Awareness	Collects an...	Running	Automatic	N
Network Setup Service	The Networ...	Running	Manual (Trig...	L
Network Share Interface Ser...	This service	Running	Automatic	I

