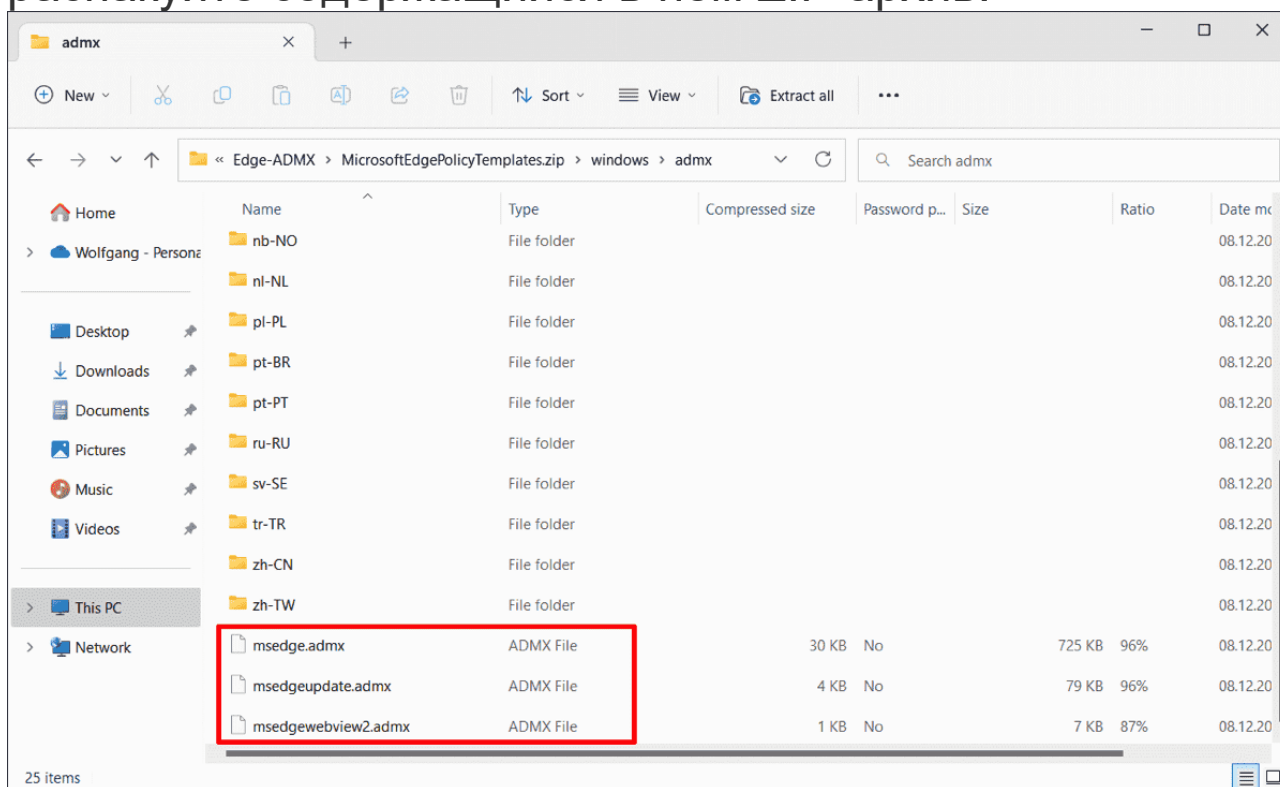


1. Установка admx, чтобы в групповых политиках отображались настройки для браузера Microsoft edge <https://www.microsoft.com/en-us/edge/business/download?form=MA13FJ>

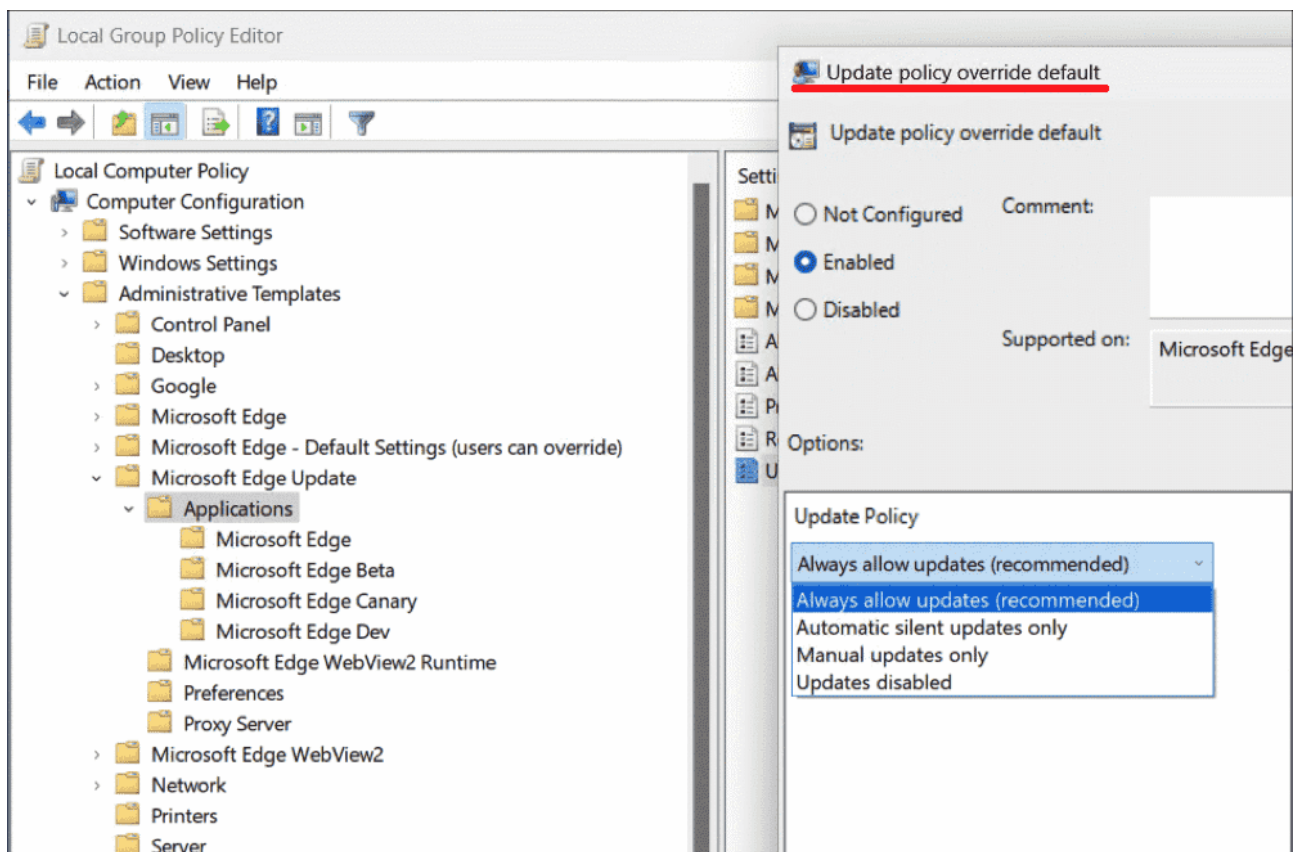
Под каждой кнопкой загрузки браузера находится ссылка с надписью «*Загрузить политику Windows для 32- или 64-битных систем*» . - скачиваем нужные шаблоны

2. Вы получите САВ-файл, который можно открыть в проводнике файлов двойным щелчком. Затем распакуйте содержащийся в нем ZIP-архив.



Содержимое файла групповой политики для Microsoft Edge

В папке windows\admx находятся три ADMX-файла: *msedge.admx* , *msedgeupdate.admx* и *msedgewebview.admx* . Только первый из них используется для фактического управления Microsoft Edge. Второй управляет автоматическим обновлением, которое следует полностью отключить через групповую политику (GPO), если вы хотите получать обновления через WSUS.



Групповые политики позволяют отключить автоматические обновления для Edge.

Если вы хотите установить административные шаблоны на локальную рабочую станцию, скопируйте файлы ADMX из ZIP-архива в папку `%systemroot%\Policydefinitions`. Кроме того, скопируйте языковые файлы из соответствующих каталогов, например, *de-DE* или *en-US*, в соответствующие папки внутри *Policydefinitions*.

2. Центр сертификации - выполняем установку роли на контроллере домена.

CA

Настройте корневой центр сертификации на контроллере домена DC

Базовая настройка RootCA

Role services

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

Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
DC.as21.local

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD CS
- Role Services
- Confirmation
- Results**

View installation progress

Feature installation

Configuration required. Installation succeeded on DC.as21.local.

Active Directory Certificate Services

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

Configure Active Directory Certificate Services on the destination server

Certification Authority

Remote Server Administration Tools

Role Administration Tools

Active Directory Certificate Services Tools

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 on a network to manage certificate policies.

☐ Standalone CA

Standalone CAs can be members of a workgroup or domain, or can be standalone. They 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.

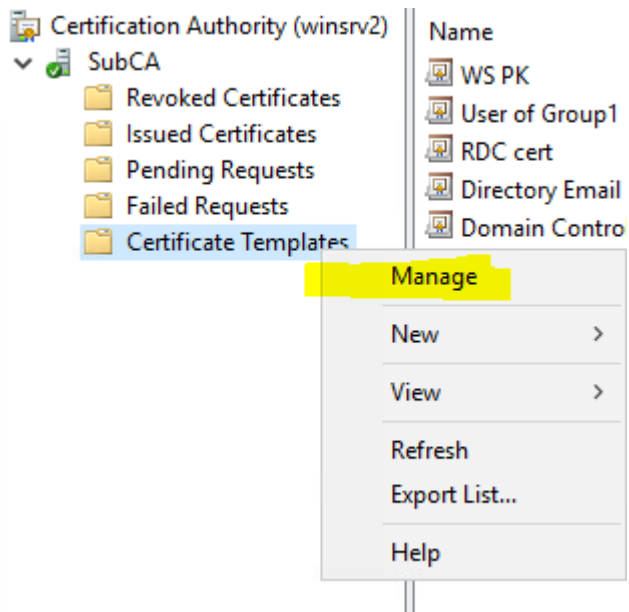
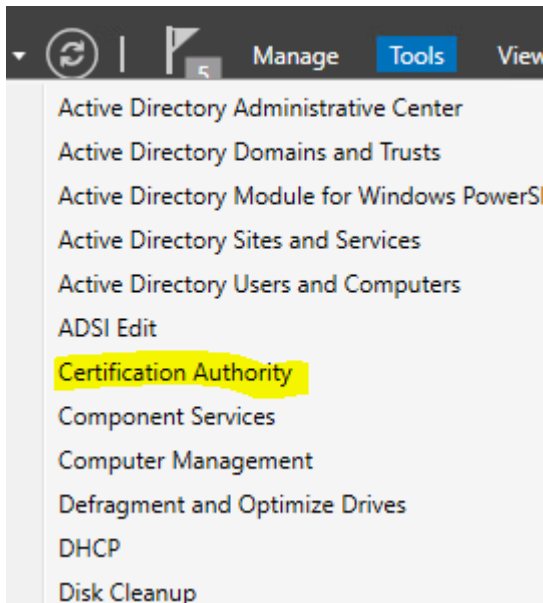
i. Имя настраиваемого центра сертификации - RootCA.

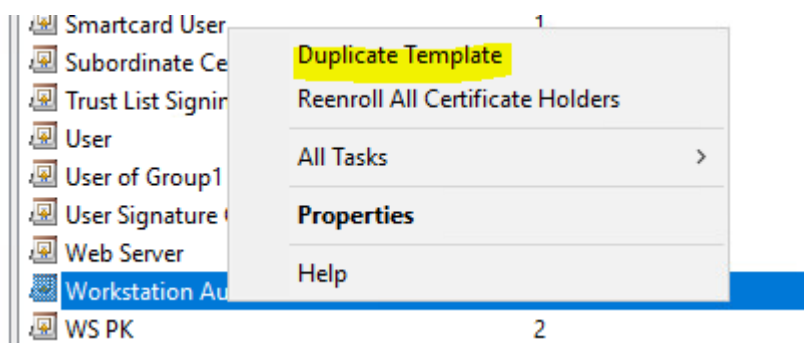
ВНИМАНИЕ - ИМЯ ПО ЗАДАНИЮ - REA2026-CA

- ii. Срок действия сертификата - ЕСЛИ В ЗАДАНИИ НИЧЕГО ПРО ЭТО НЕ СКАЗАНО, ОСТАВЛЯЕМ ПО УМОЛЧАНИЮ 5 ЛЕТ ВРОДЕ.

3. RDP

Настройка шаблона выдачи сертификатов





Вводим имя нового шаблона. Включаем публикацию в Active Directory

RDC cert Properties ? X

Subject Name		Issuance Requirements		
Superseded Templates	Extensions	Security	Server	
General	Compatibility	Request Handling	Cryptography	Key Attestation

Template display name:

Template name:

Validity period: years

Renewal period: weeks

☒ Publish certificate in Active Directory

☐ 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

RDC cert Properties

General Compatibility Request Handling Cryptography Key Attestation
Superseded Templates Extensions Security Server

Subject Name Issuance Requirements

☐ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests (*)

☒ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

Fully distinguished name

☐ Include e-mail name in subject name

Include this information in alternate subject name:

☐ E-mail name

☒ DNS name

☒ User principal name (UPN)

☐ Service principal name (SPN)

* Control is disabled due to [compatibility settings](#).

OK Cancel Apply Help

Добавляем в Extensions -> Application Policies 2 позиции:

Client Authentication

Server Authentication

Нужно добавить возможность выпуска сертификата любой машиной

Properties of New Template

Subject Name Server Issuance Requirements
Compatibility General Request Handling Cryptography Key Attestation
Superseded Templates Extensions Security

Group or user names:

Authenticated Users

Administrator

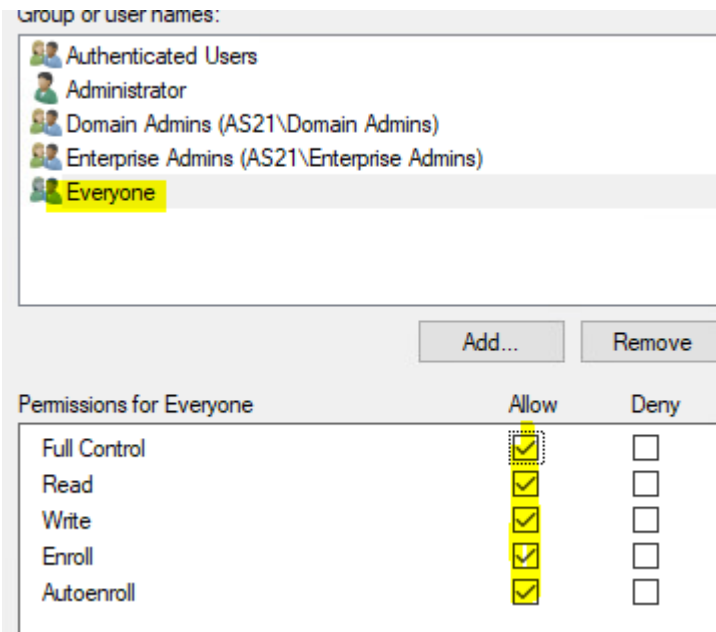
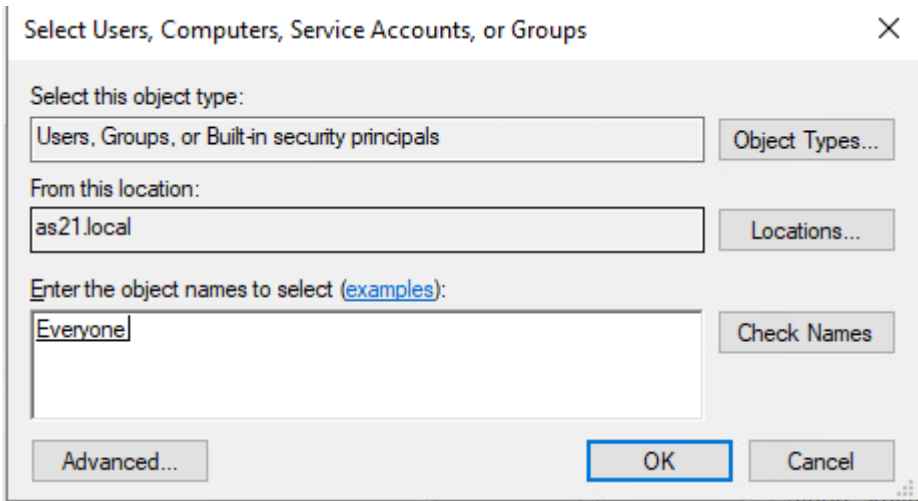
Domain Admins (AS21\Domain Admins)

Enterprise Admins (AS21\Enterprise Admins)

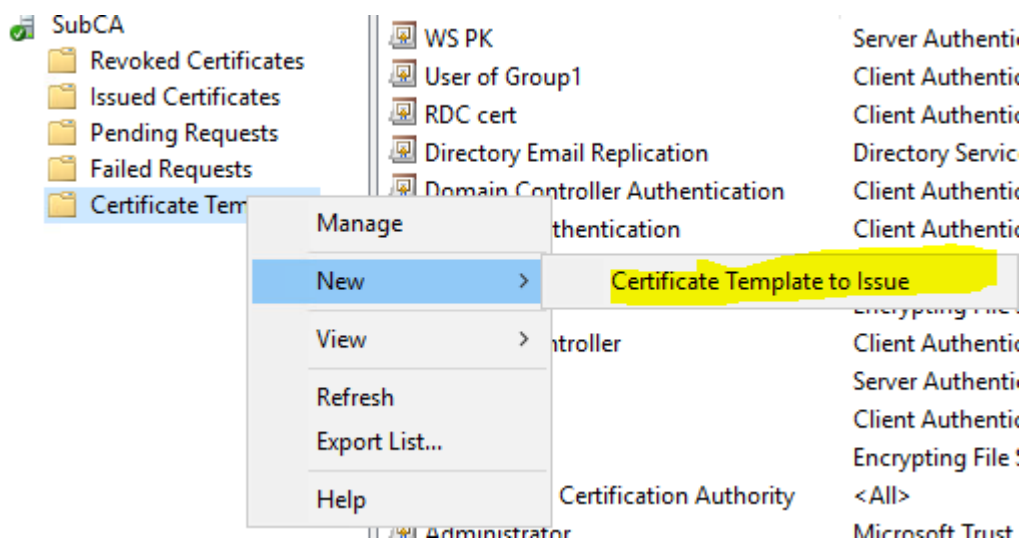
Add... Remove

Permissions for Authenticated Users Allow Deny

Даем всем права на выпуск сертификата группе Everyone



Публикуем сертификат в Active Directory



ИТАК - ЧТО МЫ СДЕЛАЛИ - МЫ УСТАНОВИЛИ АДМХ ШАБЛОНЫ, чтобы по ним настроить групповые политики из 1 пункта (напишу как позже)

Мы установили на контроллере домена центр сертификации - не тупи списываем а отсюда, а проверяем имена-все четко по заданию

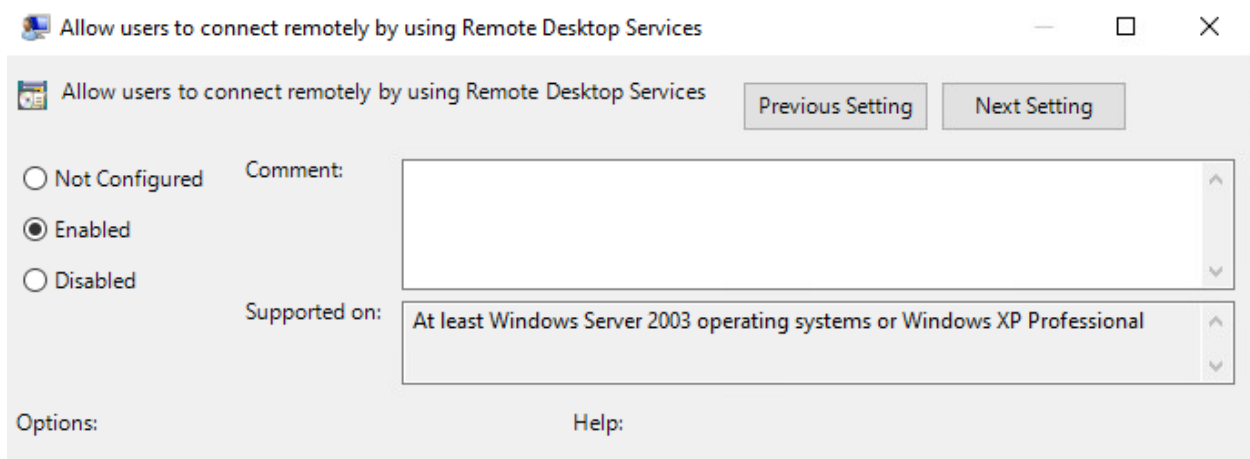
После установки центра сертификации - мы создаем шаблон для сервера рдс

После этого настраиваем групповые политики на контроллере домена, где только что настроили центр сертификации и сделали шаблон сертификата.

Настройки GPO для RDP

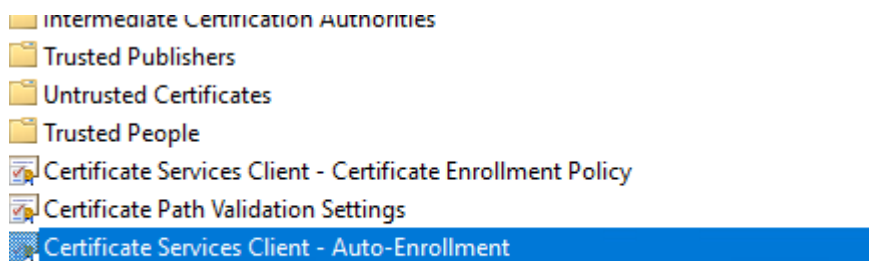
Разрешаем через GPO использование Remote Desktop Connection

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**

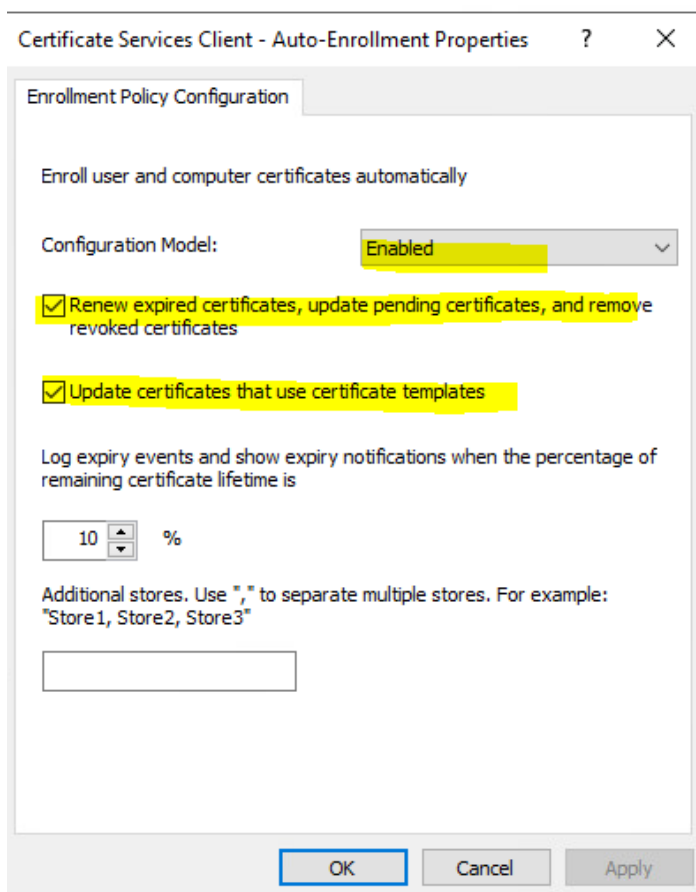


Включаем авто выдачу сертификатов всем устройствам домена

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

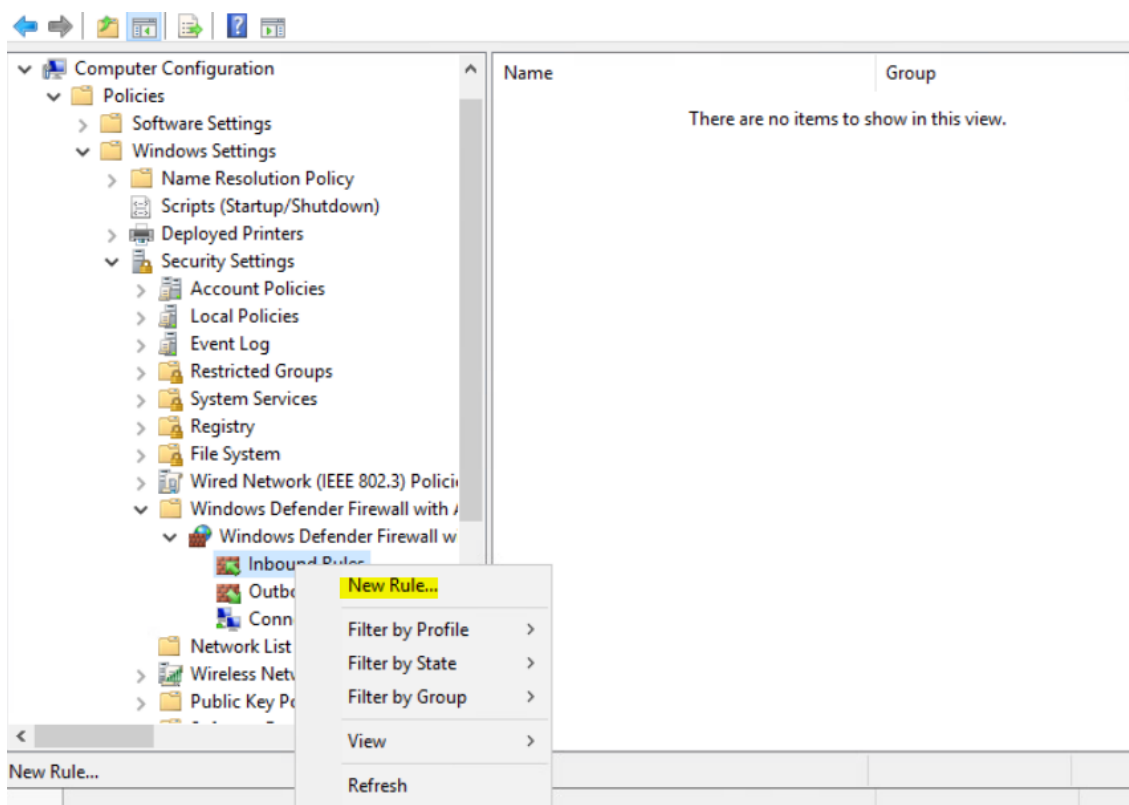


Включаем общую настройку выдачи и выбираем 2 конфигурации

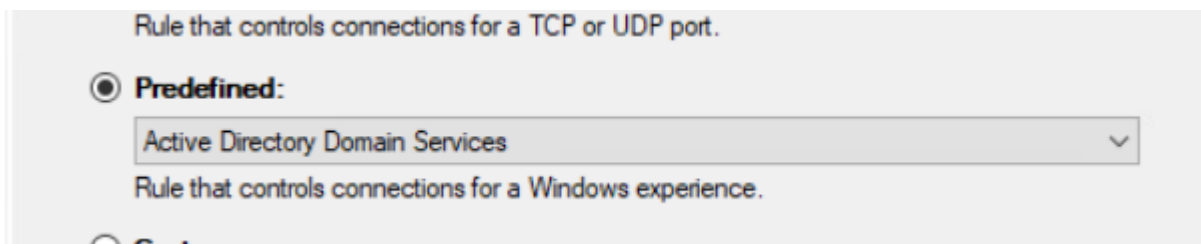


Разрешаем подключение по RDP компьютерам домена

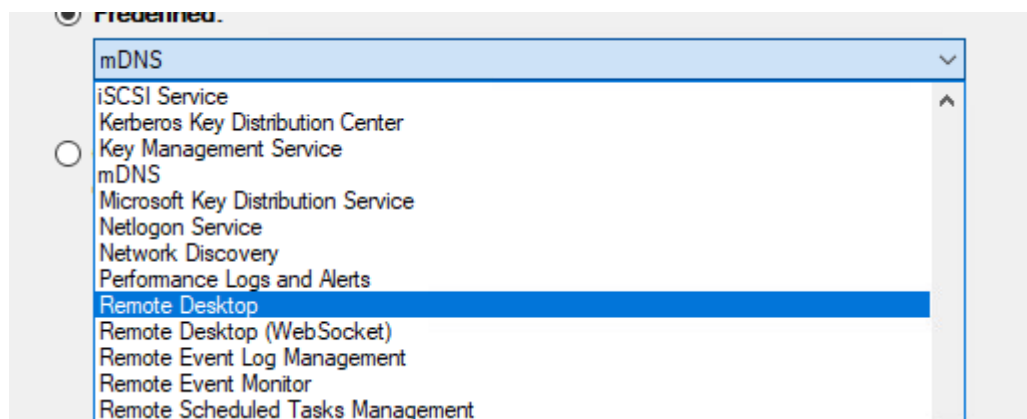
Computer Configuration > Policies > Windows Settings > Security Settings > Windows Defender Firewall and Advanced Security > Inbound Rules -> **New Rule**



Выбираем predefined (Predefined)



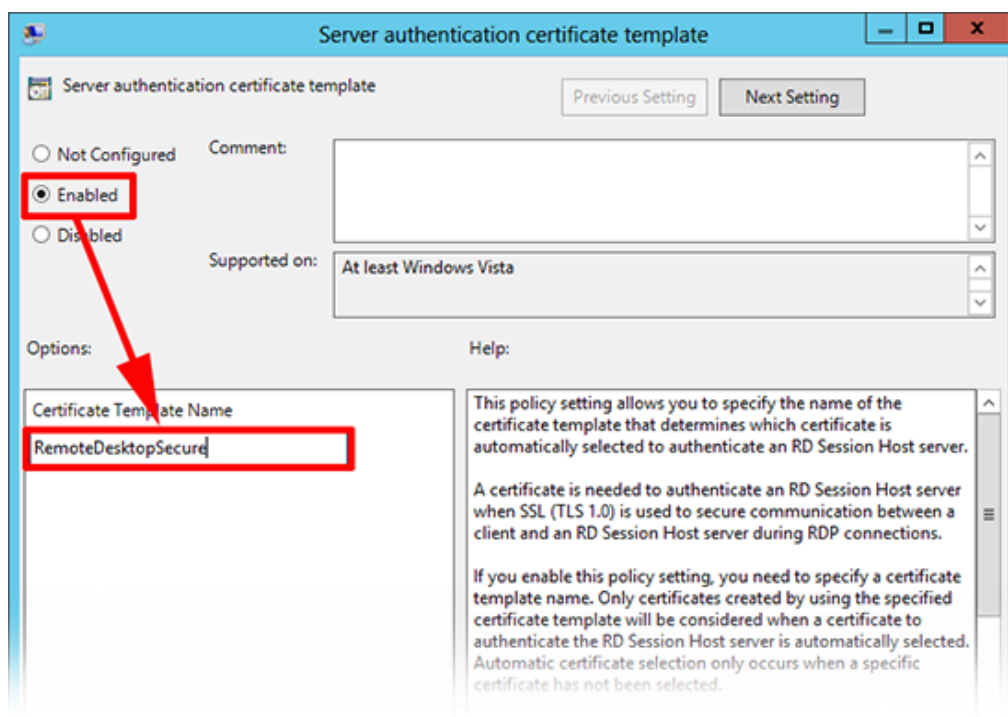
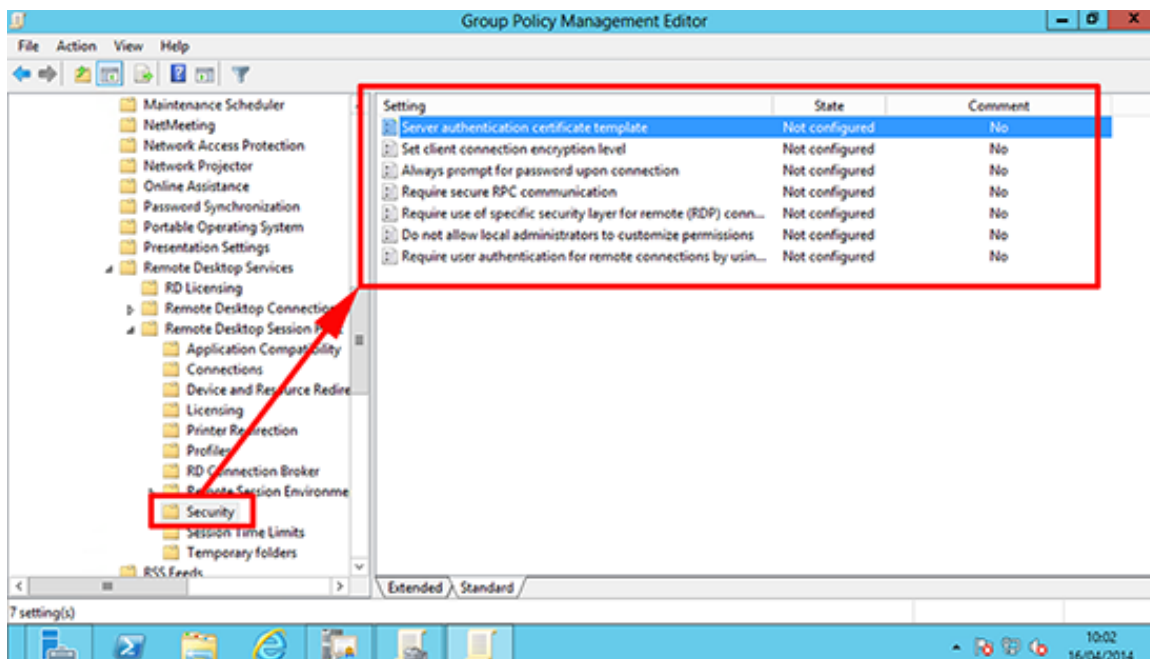
Выбираем Remote Desktop



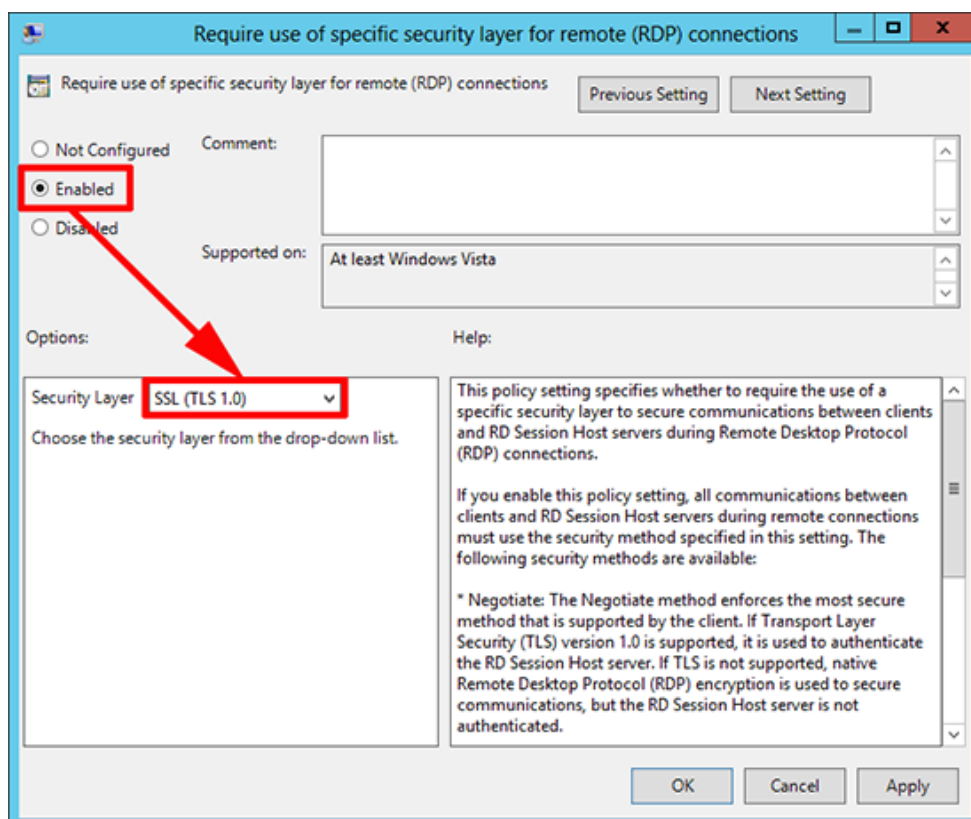
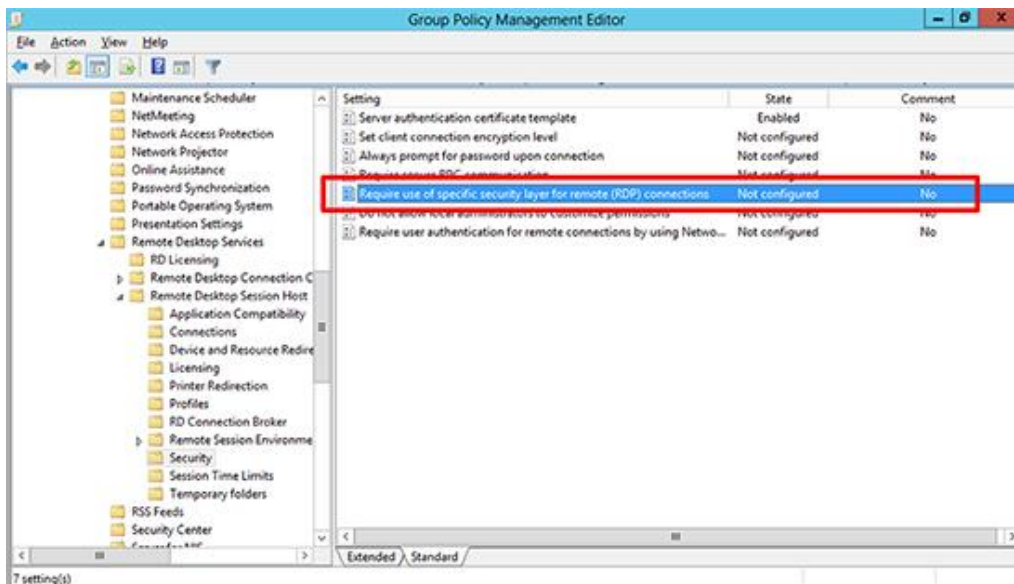
Name	Group	Profile
✓ Remote Desktop - Shadow (TCP-In)	Remote Desktop	All
✓ Remote Desktop - User Mode (UDP-In)	Remote Desktop	All
✓ Remote Desktop - User Mode (TCP-In)	Remote Desktop	All

Включаем требование к использованию сертификатов

GPO на домен: Computer Configuration > Policies > Administrative Templates > Windows > Components > Remote Desktop Services > Remote Desktop Session Host > Security > Server authentication certificate template -> **Enabled** <Пишем имя шаблона для подключения - Template Name. В нашем случае это **RDCcert**>



GPO на домен: Computer Configuration > Policies > Administrative Templates > Windows > Components > Remote Desktop Services > Remote Desktop Session Host > Security > Require use of specific security layer for remote (RDP) connections' policy -> Enabled выбираем SSL (TLS 1.0)



Вот ЗДЕСЬ НАЧИНАЕТСЯ САМОЕ ИНТЕРЕСНОЕ— идем на машинку с названием RDS

3. RDS

СОЗДАНИЕ RDS

Установка ролей

Роль называется remote desktop services

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](#)
Installation
Deployment Type
[Deployment Scenario](#)
[Role Services](#)
[RD Connection Broker](#)

Remote Desktop Services can be configured as follows:

☒ **Standard deployment**
A standard deployment allows you to deploy Remote Desktop Services on a single server or on a virtual machine.

☐ Quick Start
A Quick Start allows you to deploy Remote Desktop Services on a single server or on a virtual machine.

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 desktops, published RemoteApp programs, and session-based desktops.

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

☒ **Session-based desktop deployment**
Session-based desktop deployment allows users to connect to session collections that include published RemoteApp programs and session-based desktops.

Выбираем rds для разворачивания роли - на скрине неправильно

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

Selected

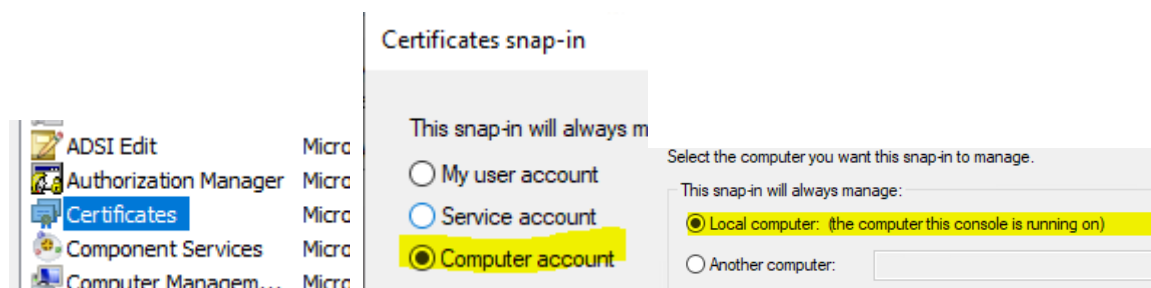
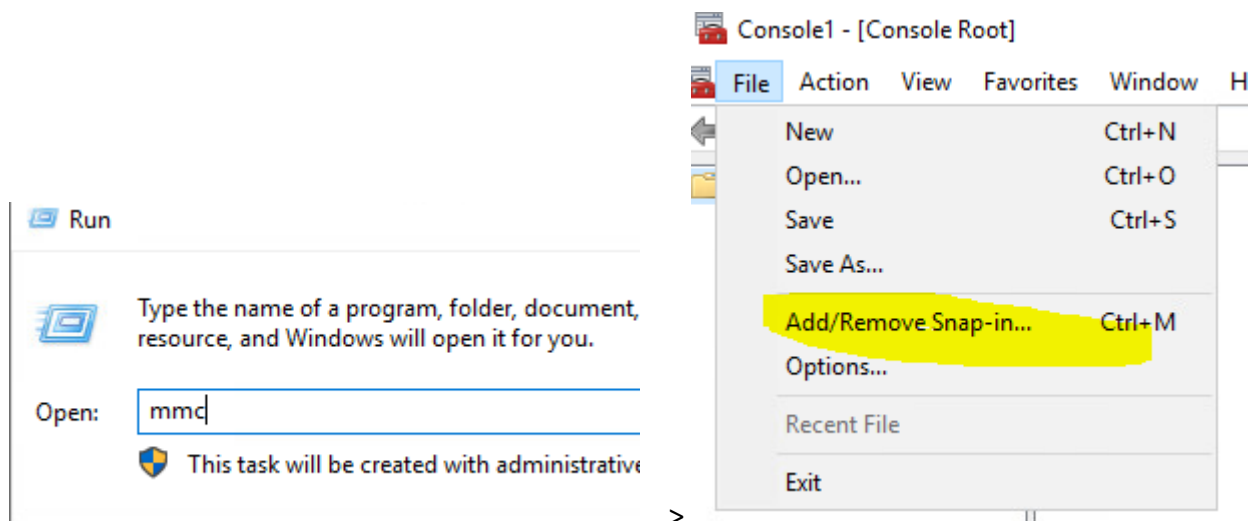
Computer

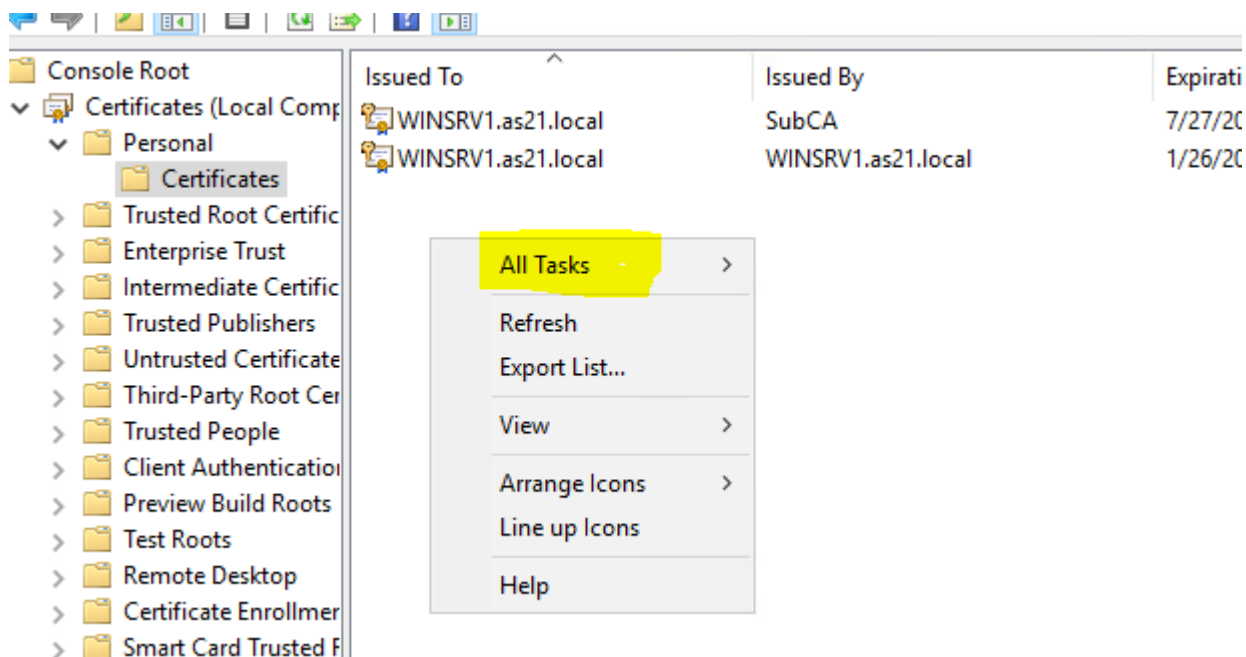
- AS21.LOCAL (1)
 - WINSRV2

Настройка web доступа по сертификатам

Сконфигурируйте web-доступ к службам терминалов сервера.

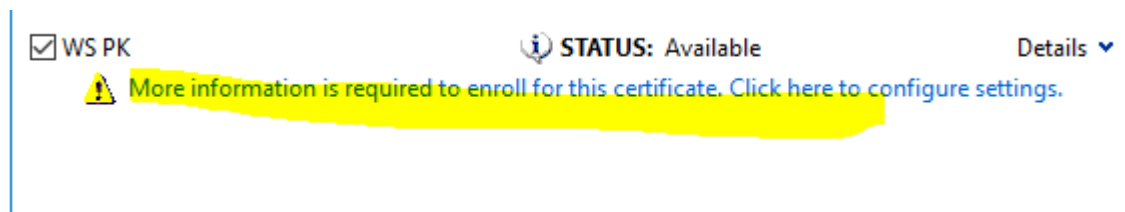
Запускаем mmc. Добавляем оснастку Certificates > Computer account > Local computer





All Task > Request New Certificate

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



Сверху заводим Common Name – rds.reaskills2026.local

И

rds.rea2026.ru и *.reaskills2026.local

Внизу заводим DNS rds.reaskills2026.local

И

rds.rea2026.ru

И

***.reaskills2026.local**

Certificate Properties

Subject General Extensions Private Key Certification Authority Signature

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate
The user or computer that is receiving the certificate

Subject name:

Type:
Common name

Add >

Value:

< Remove

CN=rds.as21.local

Alternative name:

Type:
DNS

Add >


Value:

< Remove

DNS
rds.as21.local
rds

Выпускаем сертификат

☒ WS PK

 STATUS: Available

Details ▾

☐ Show all templates

Enroll Cancel

Правой кнопкой по нашему сертификату. Выбираем All Tasks > Export

Issued To	Issued By	Expiration D
rds.as21.local	SubCA	7/28/2023
WI	SubCA	7/27/2022
WI		22

Open

All Tasks >

Cut

Copy

Delete

Properties

Help

Open

Request Certificate with New Key...

Renew Certificate with New Key...

Manage Private Keys...

Advanced Operations >

Export...

При экспорте выбираем разрешение экспорта закрытого ключа

Do you want to export the private key with tl

☒ 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:

...

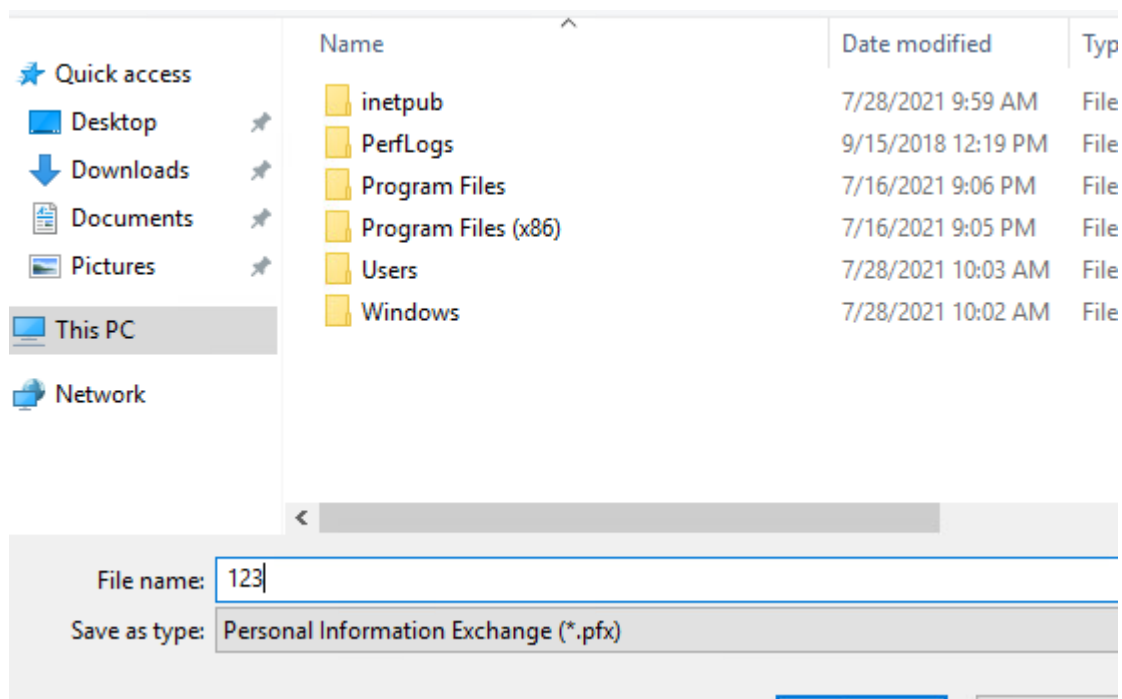
Confirm password:

...

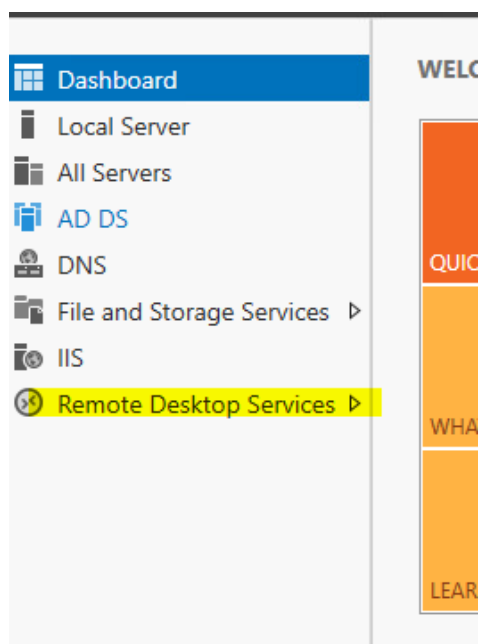
Encryption: AES256-SHA256



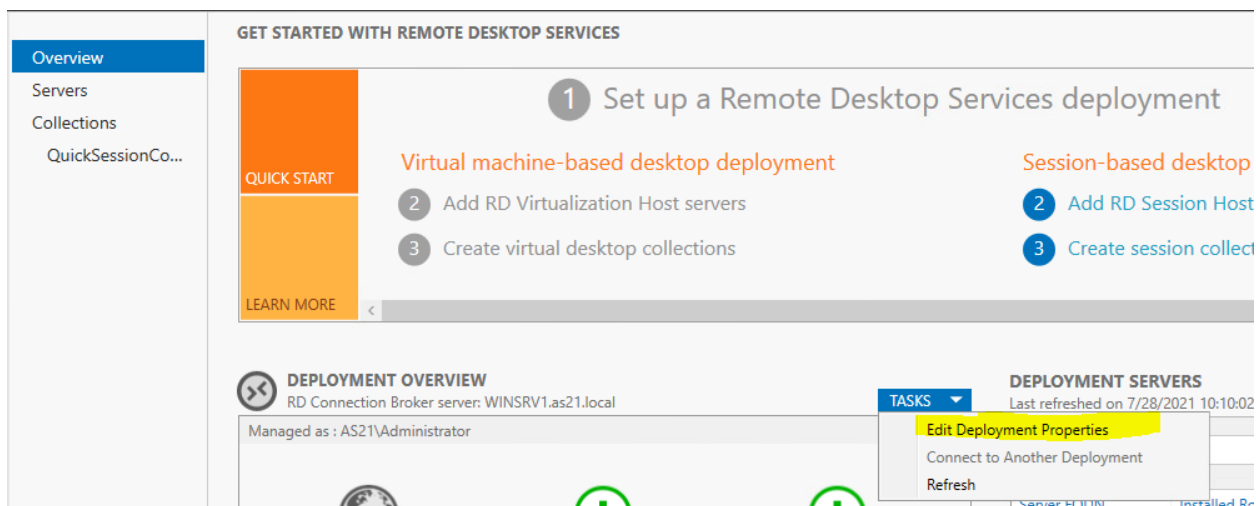
Сохраняем файл (не забываем куда)



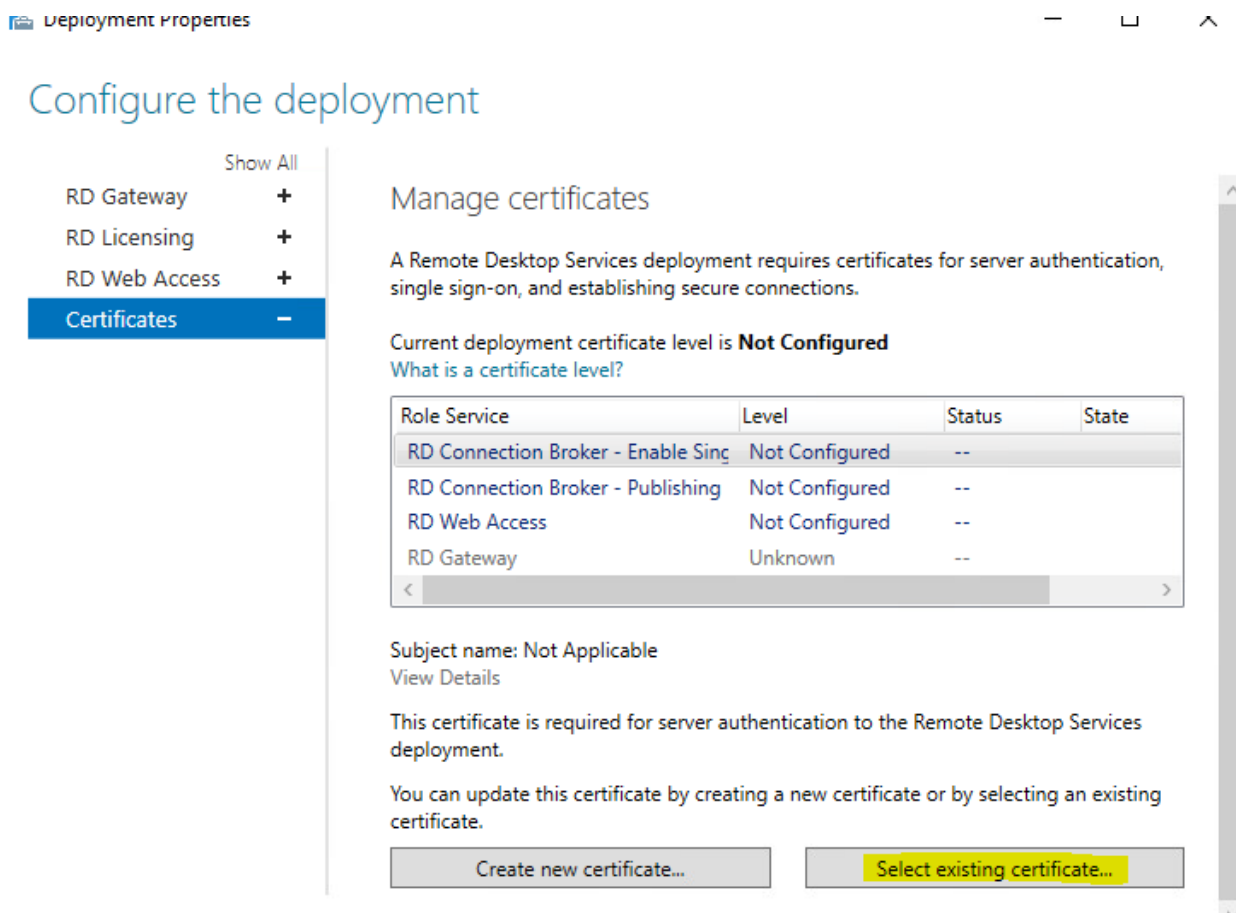
Идем в сервер менеджере в консоль RDS



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



Переходим на вкладку **Certificates** и выбираем **Select existing certificate**



Указываем путь до предварительно сохраненного сертификата и пароль к нему.

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

☐ 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 Sing	Not Configured	--	Ready to a
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:

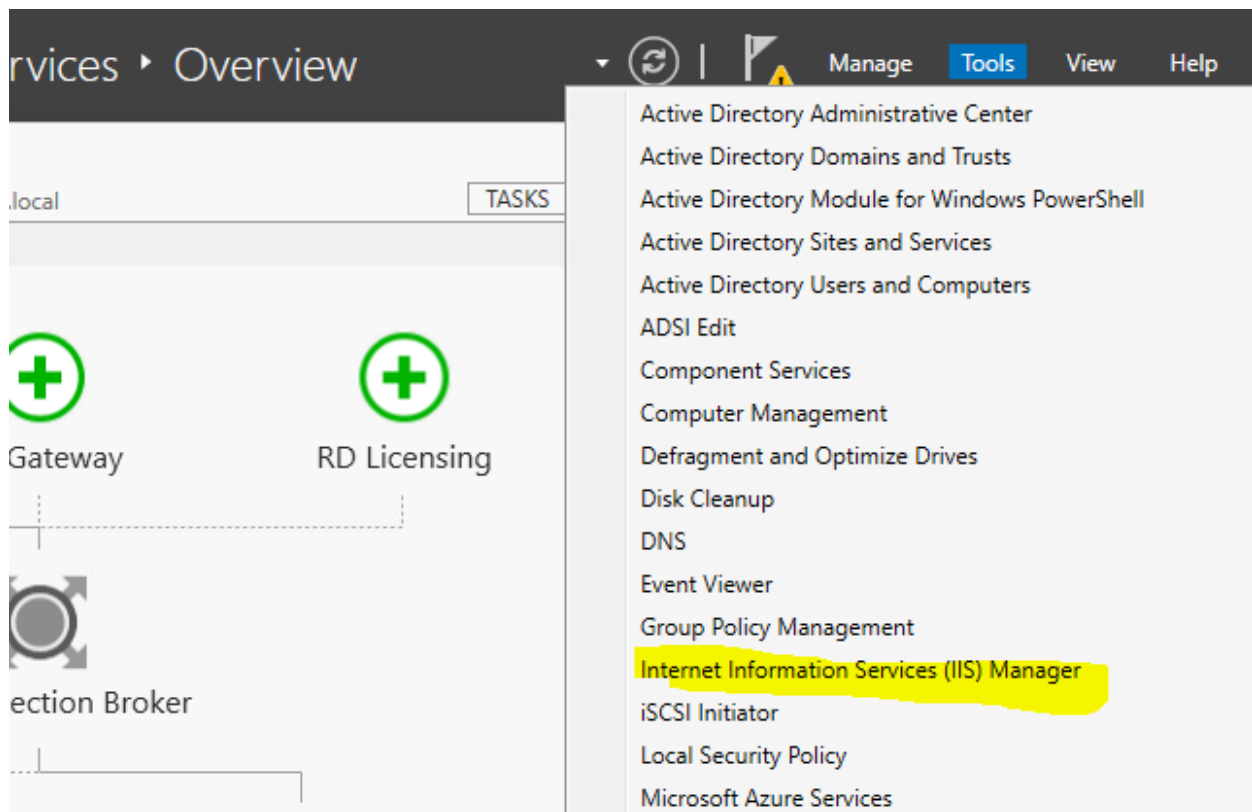
Role Service	Level	Status	State
RD Connection Broker - Enable Sing	Trusted	OK	Success
RD Connection Broker - Publishing	Trusted	OK	Success
RD Web Access	Trusted	OK	Success
RD Gateway	Unknown	--	

3. Web-интерфейс сервера должен быть доступен только по протоколу https по имени rds.reaskills2026.local/RDweb.

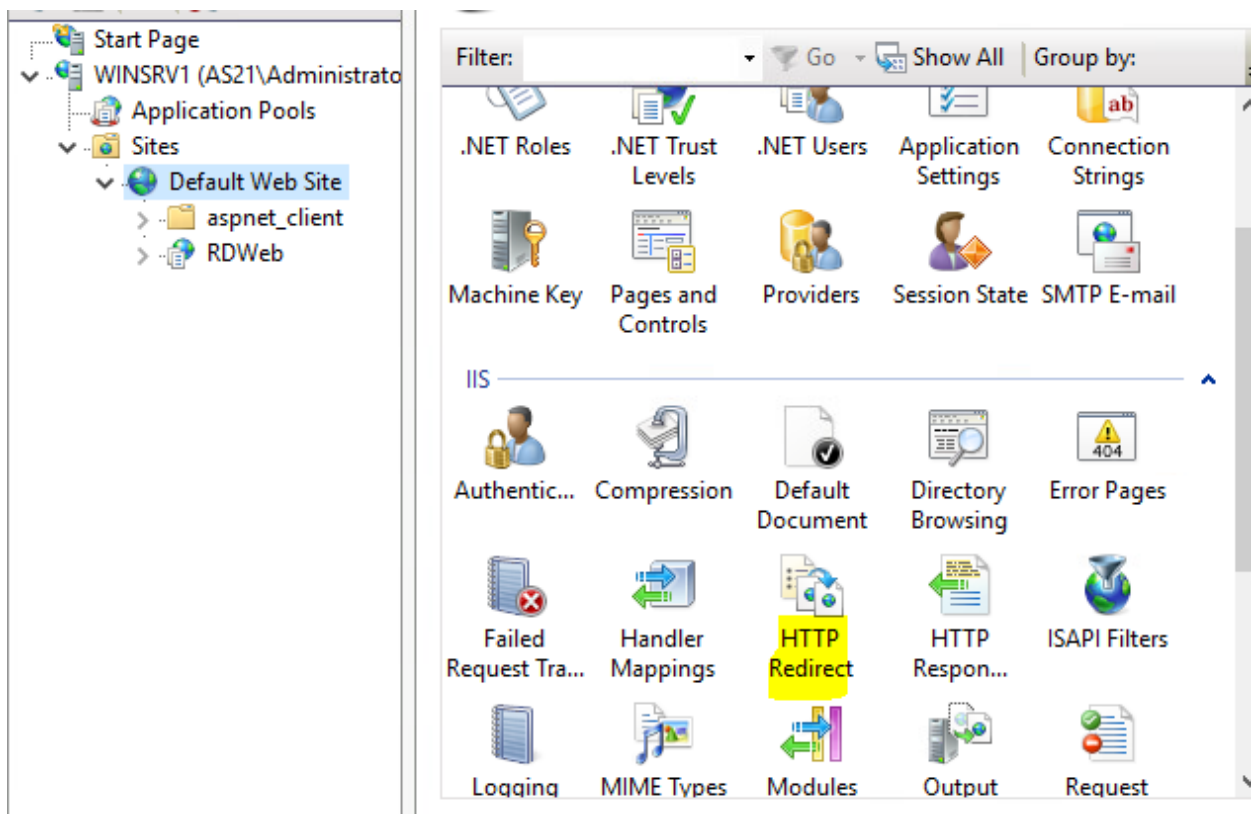
ВАЖНО!!! Убеждаемся, что в DNS есть A запись rds, которая ведет на rds.

Идем в сервер менеджере в Tools > Internet Information Services (IIS) Manager

Настройка IIS RDS



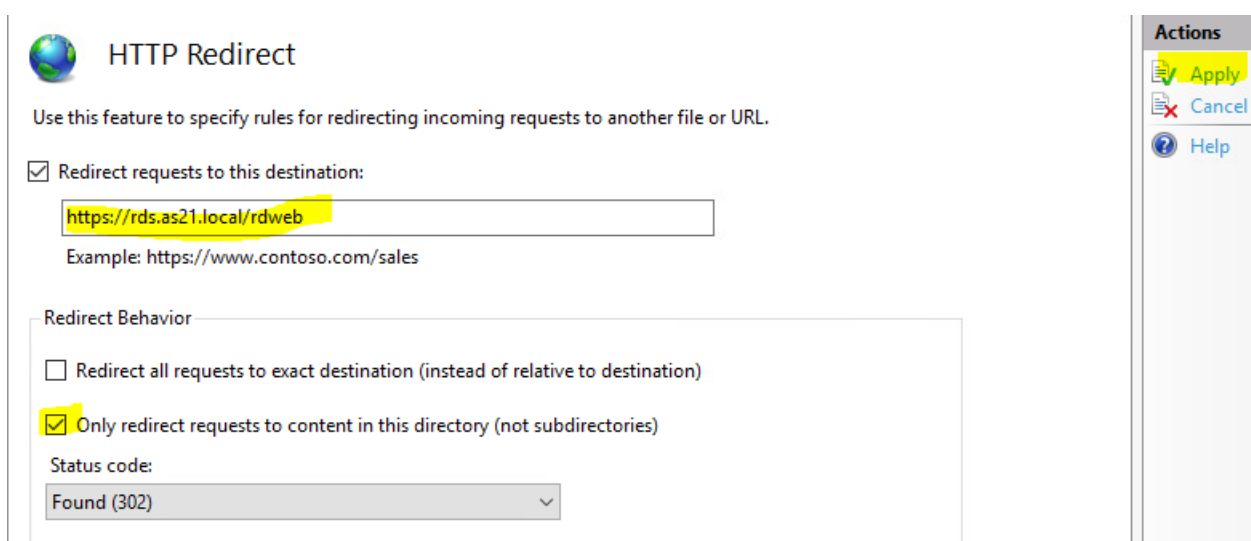
Открываем WINSRV1 > Sites > Default Web Site, выбираем HTTP Redirect



Прописываем пункт назначения переадресации <https://rds.as21.local/RDWeb/>

Включаем Only redirect requests to content in this directory (not subdirectories). Нажимаем Apply

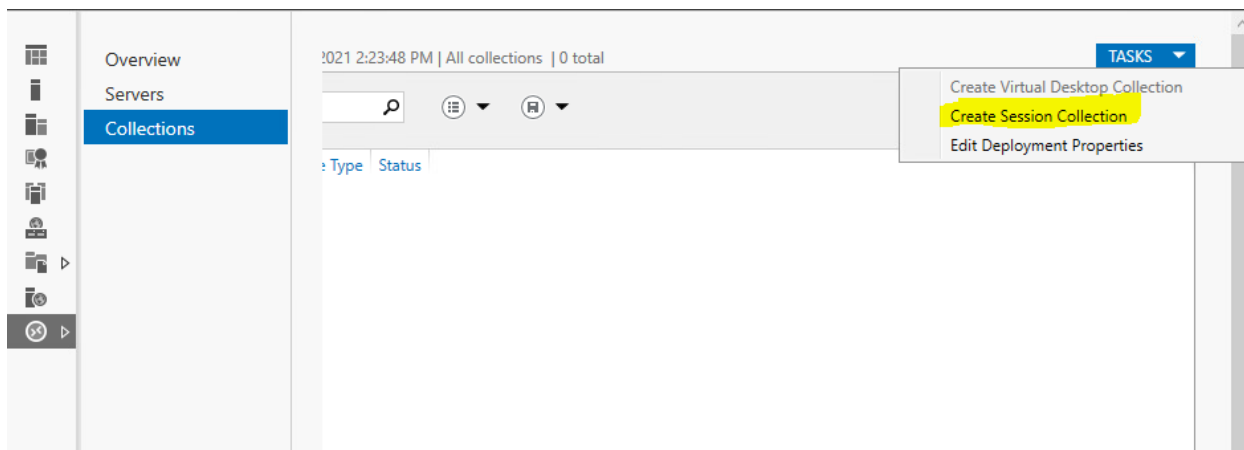
Здесь прописываем <https://rds.reaskills2026.local/rdweb>



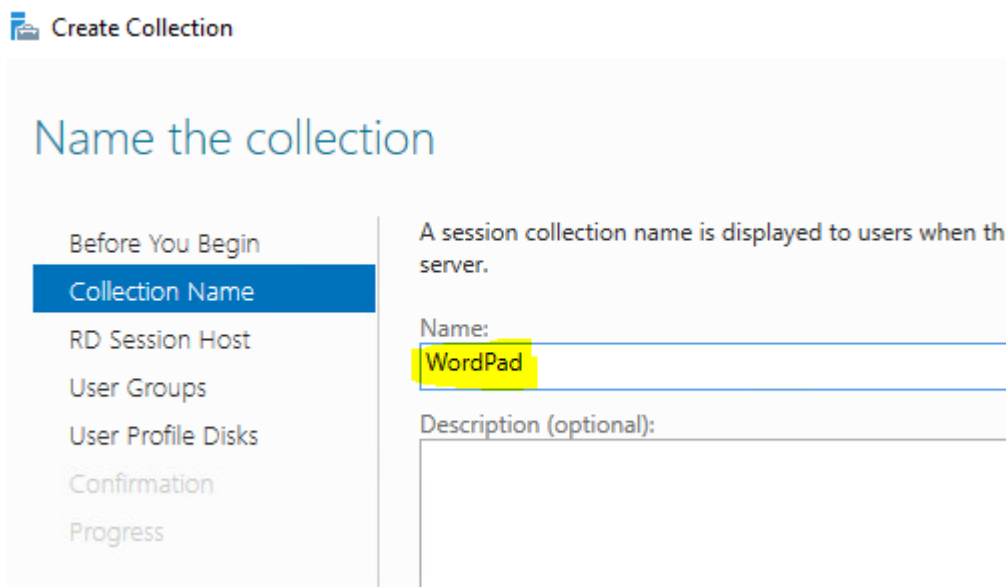
Публикация коллекции RDS

Опубликуйте программу max (вы скачаете ярлык с интернета) на web-портале RemoteApp при запуске этой программы у пользователей не должны появляться никакие ошибки и предупреждения системы безопасности.

Создаем новую коллекцию



Вводим имя коллекции - пусть будет MAX



Добавляем сервер RDS как хоста коллекции - на скрине неправильно

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:

Name	IP Address	Operat
WINSRV1.as21.local		

Selected

Computer

AS21.LOCAL (1)

WINSRV1

Оставляем группу 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

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

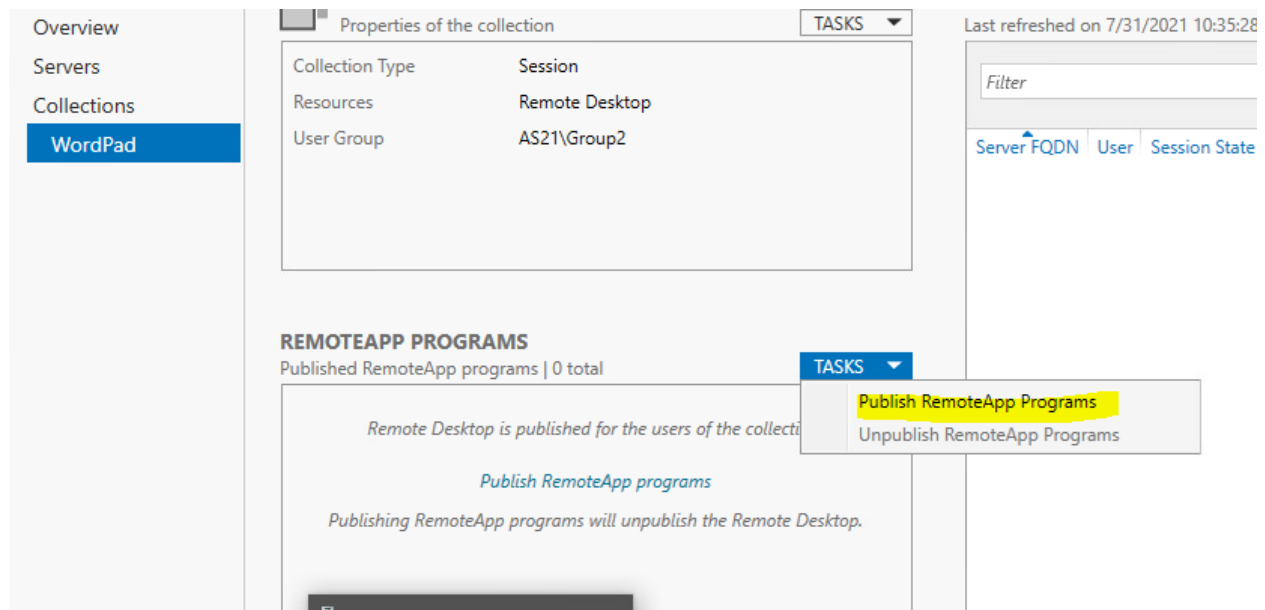
Location of user profile disks:

Maximum size (in GB):

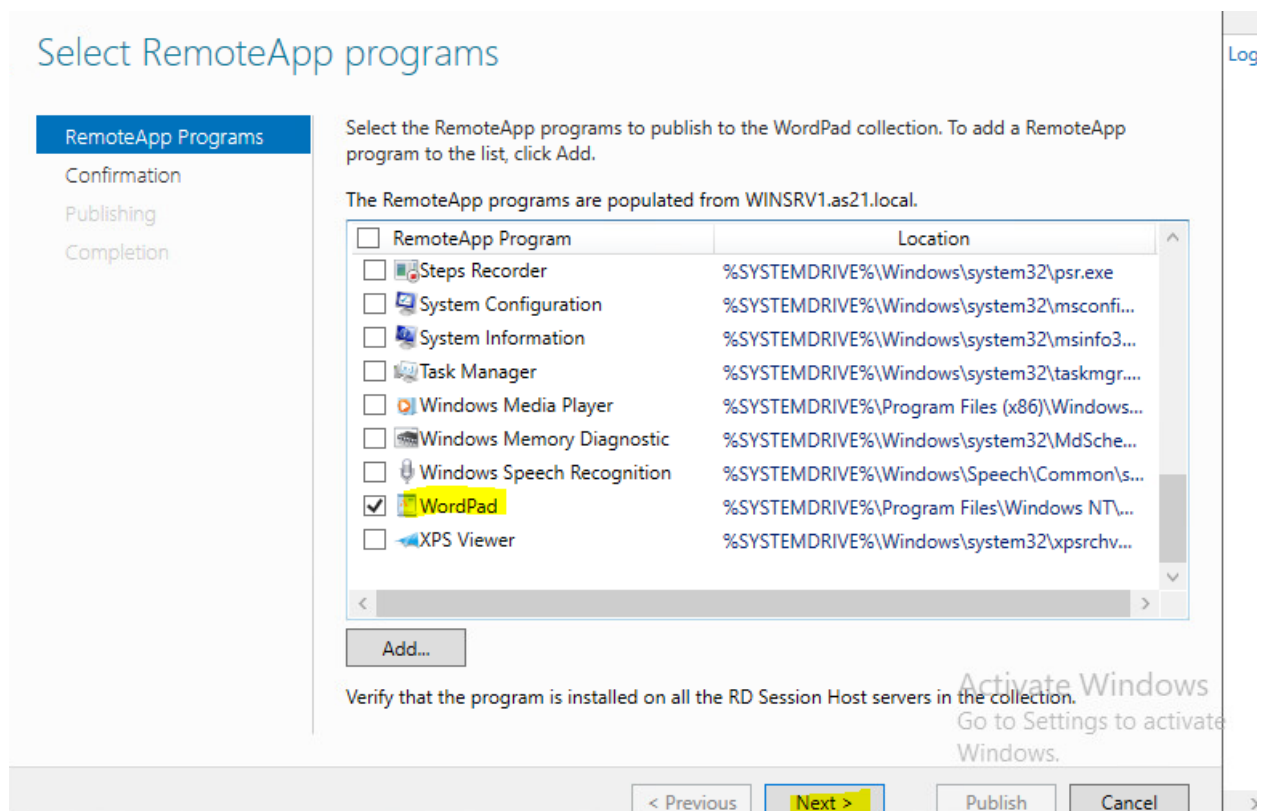
20

Публикация приложения RDS

Публикуем приложение



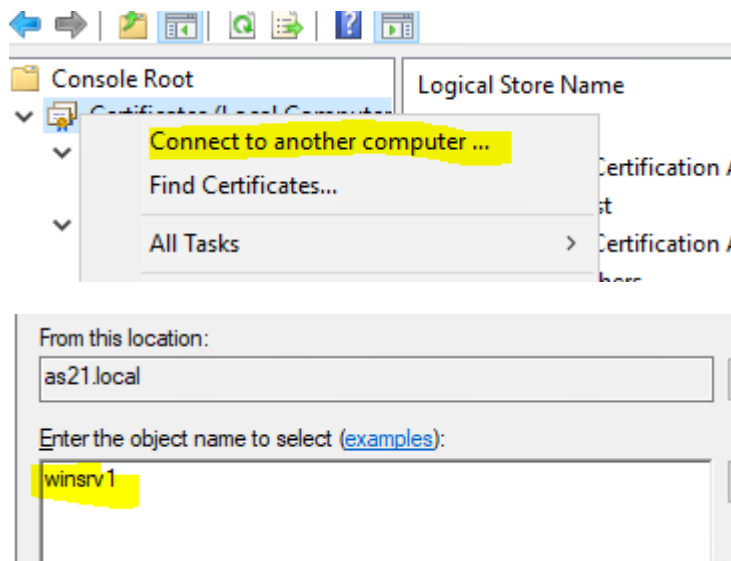
Выбираем из списка тех публикуем его на RDS



Добавление сертификата в доверенные

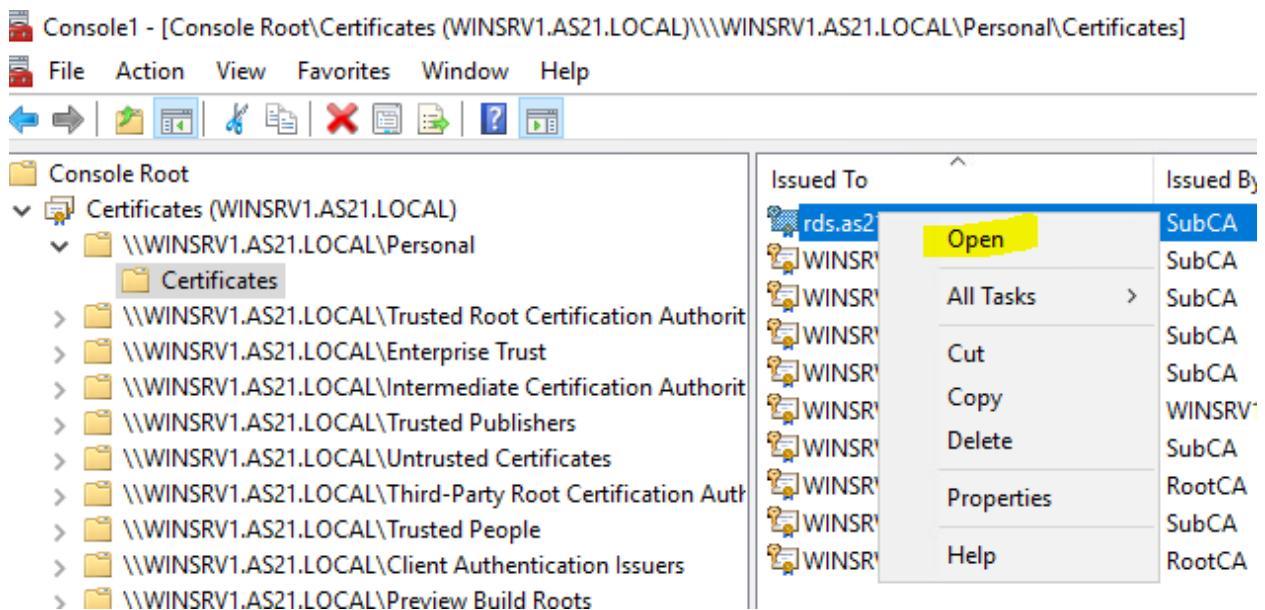
Убираем предупреждение при подключении

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

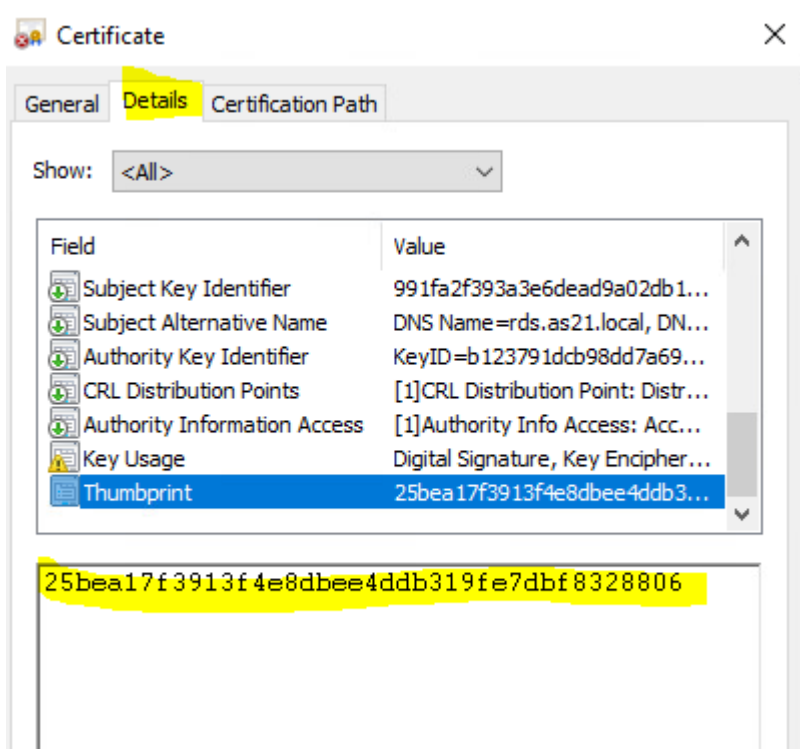


Находим выпущенный для RDS сертификат rds.reaskills2026.local

Открываем его

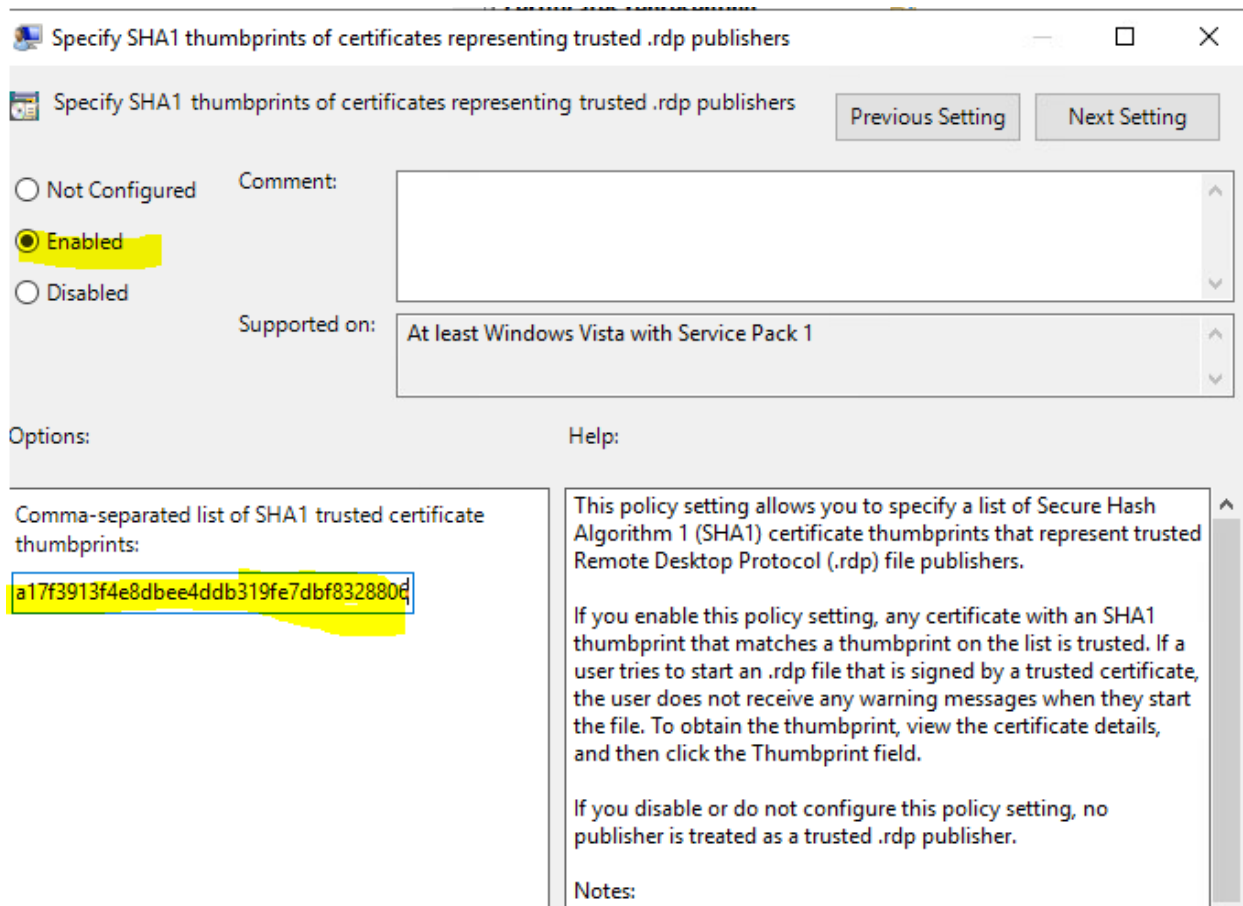







Переходим в раздел Details. Выбираем Thumbprint, где мы видим отпечаток нашего сертификата. Копируем его в буфер



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

В качестве настройки вставляется отпечаток



 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 truste...	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

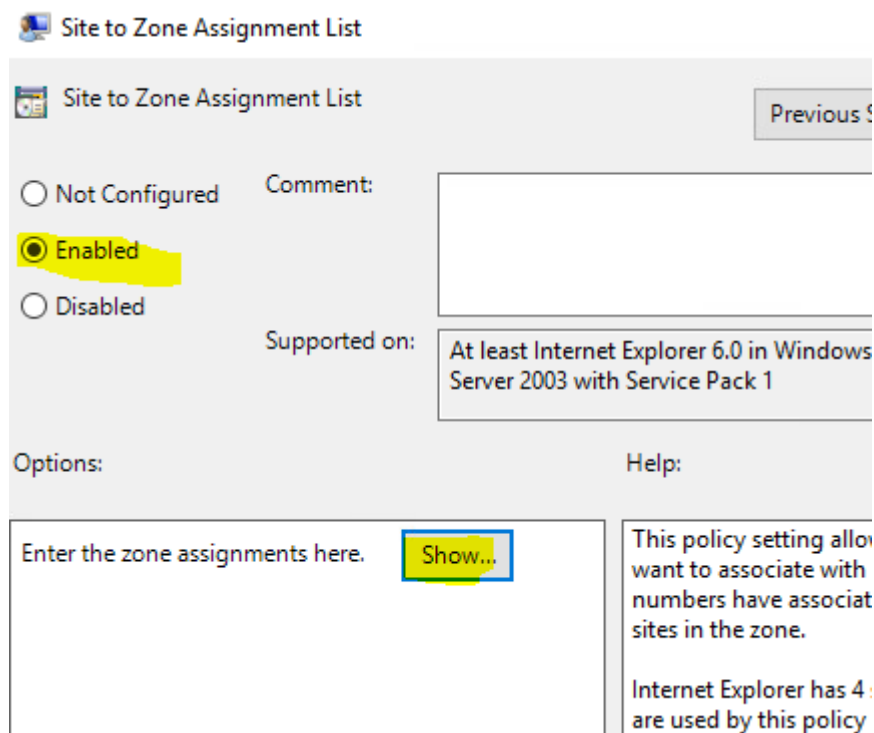
Идем в GPO, созданную на домен

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.reaskills2026.local>

В Value пишем 1



Site to Zone Assignment List

Site to Zone Assignment List

Previous S...

☐ Not Configured
 ☒ Enabled
 ☐ Disabled

Comment:

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

Options:

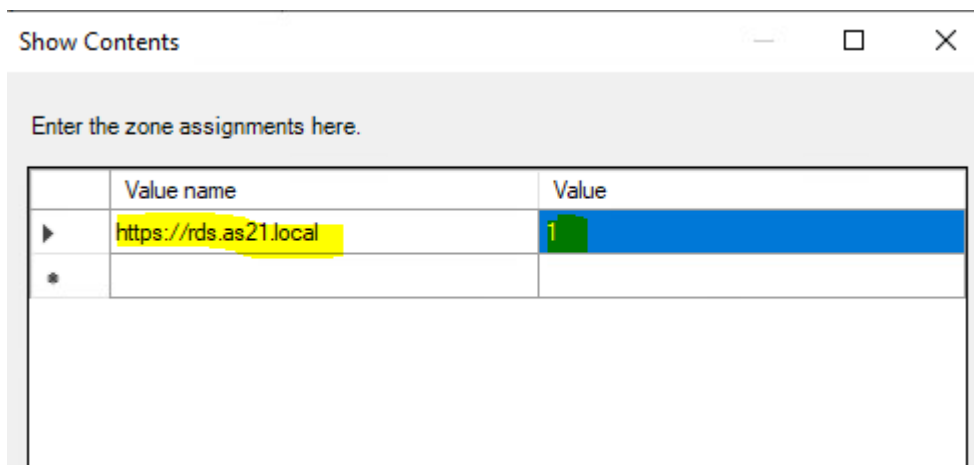
Enter the zone assignments here. [Show...](#)

Help:

This policy setting allows you to associate with numbers have associated sites in the zone.

Internet Explorer has 4 zones are used by this policy

Тут имя <https://rds.reaskills2026.local>



Добавляем

Value Name вводим адрес нашего RDS – https://rds.reaskills2026.local

В Value пишем **1**

