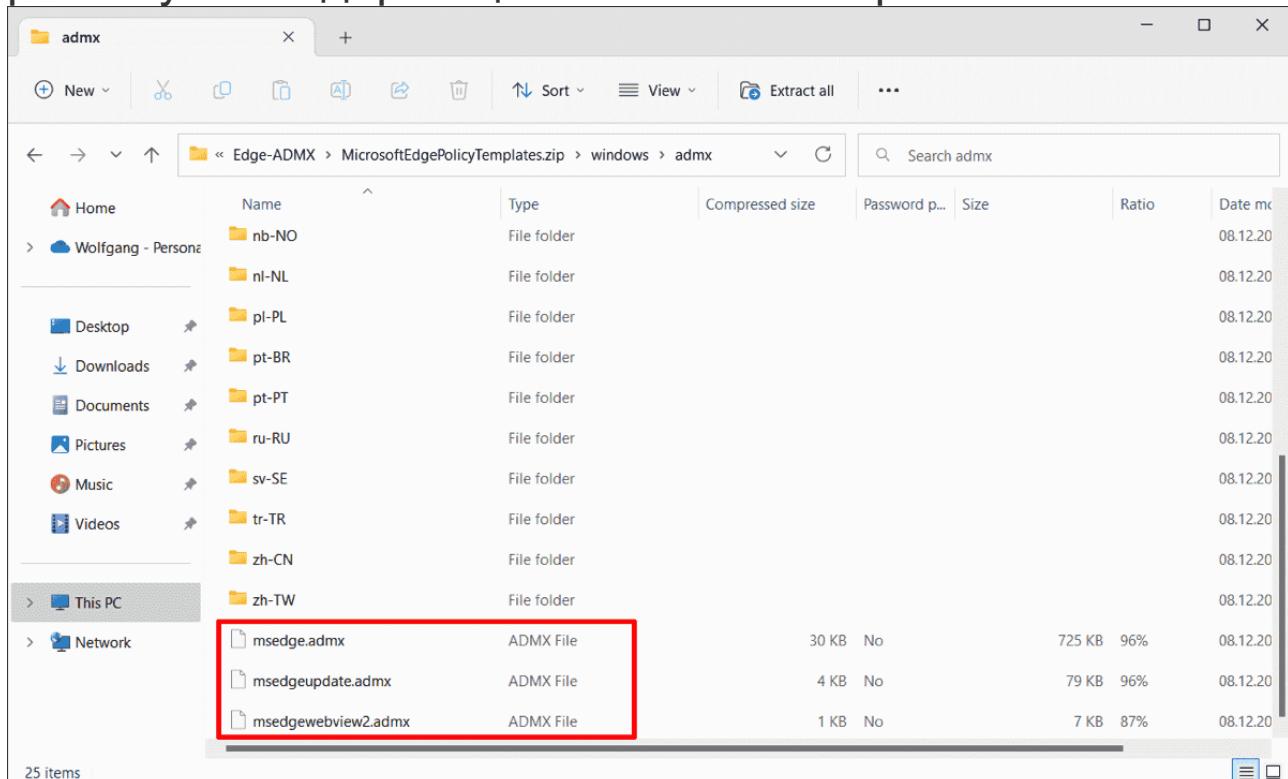


1. Установка admx, чтобы в групповых политиках отображались настройки для браузера Microsoft edge <https://www.microsoft.com/en-us/edge/business/download?form=MA13FJ>

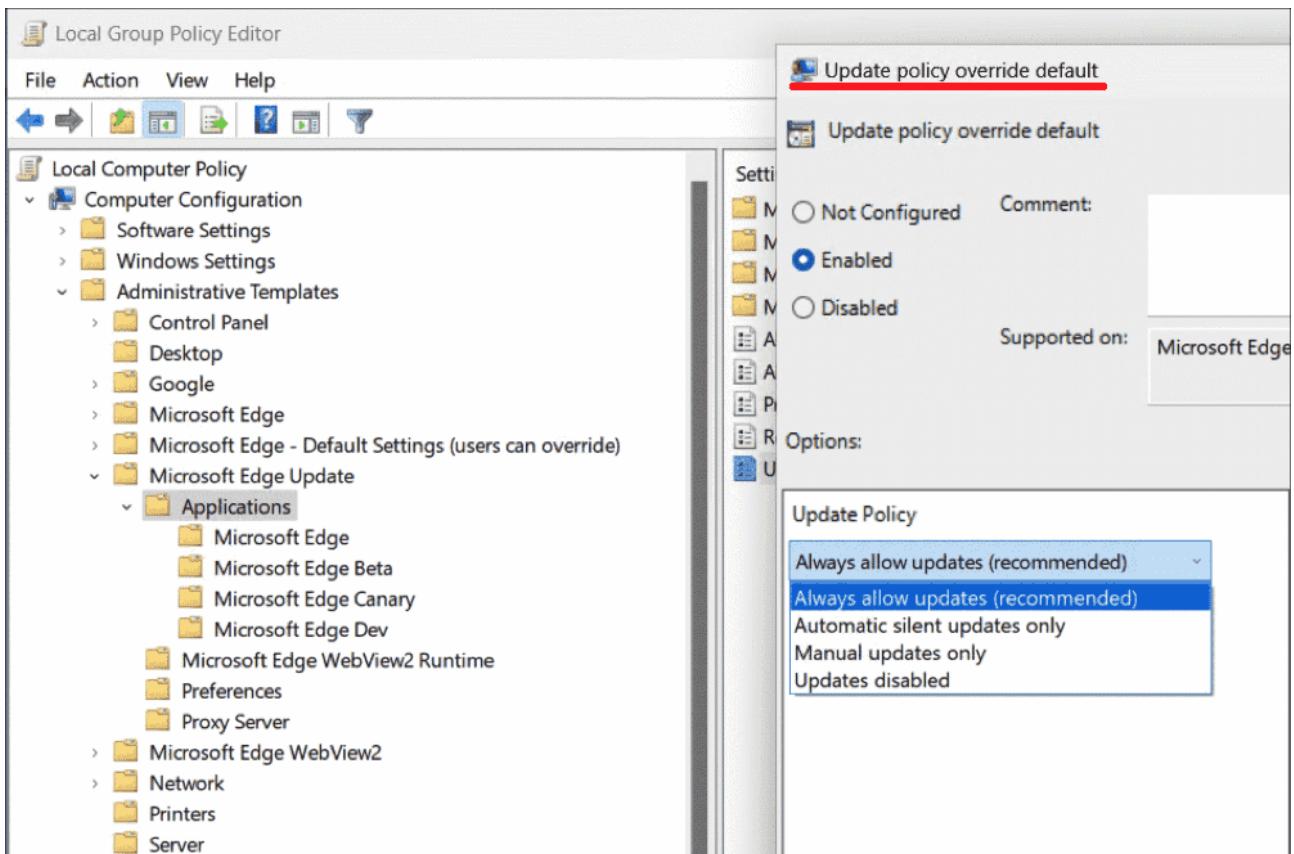
Под каждой кнопкой загрузки браузера находится ссылка с надписью « Загрузить политику Windows для 32- или 64-битных систем» . - скачиваем нужные шаблоны

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.

СА

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

DESTINATION SERVER
DC.as21.local

Installation progress

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

View installation progress

i 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 organized into certificate policies.

Standalone CA

Standalone CAs can be members or a workgroup or domain. They do not use Active Directory 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.

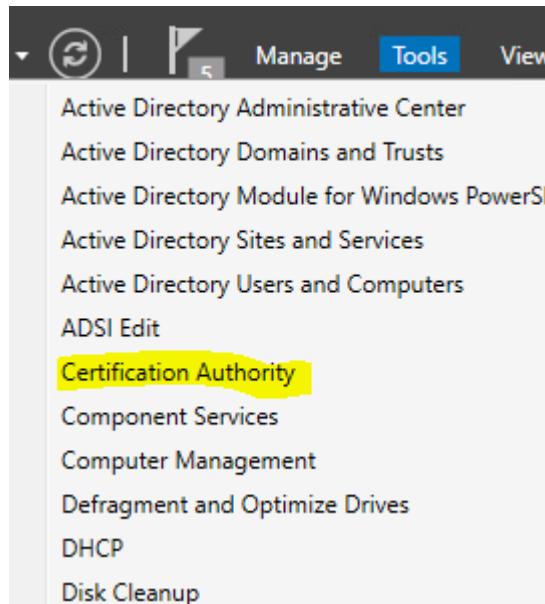
- i. Имя настраиваемого центра сертификации - RootCA.

ВНИМАНИЕ - ИМЯ ПО ЗАДАНИЮ - REA2026-СА

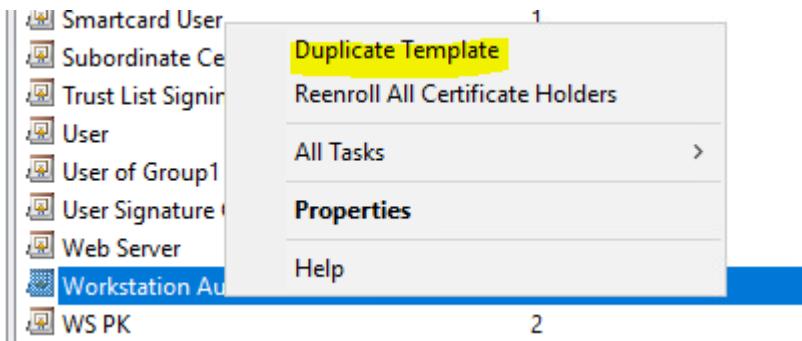
- ii. Срок действия сертификата - ЕСЛИ В ЗАДАНИИ НИЧЕГО ПРО ЭТО НЕ СКАЗАНО, ОСТАВЛЯЕМ ПО УМОЛЧАНИЮ 5 ЛЕТ ВРОДЕ.

3. RDP

Настройка шаблона выдачи сертификатов



A screenshot of the Certification Authority (winsrv2) interface. The left pane shows a tree structure with 'Certification Authority (winsrv2)' expanded, revealing 'SubCA' and several subfolders: 'Revoked Certificates', 'Issued Certificates', 'Pending Requests', 'Failed Requests', and 'Certificate Templates'. The 'Certificate Templates' folder is also highlighted with a yellow box. To the right, a list of certificate templates is shown under the heading 'Name': WS PK, User of Group1, RDC cert, Directory Email, and Domain Contro. A context menu is open over the 'Certificate Templates' folder, with the 'Manage' option highlighted with a yellow box. The menu options include: New >, View >, Refresh, Export List..., and Help.



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:
RDC cert

Template name:
RDCcert

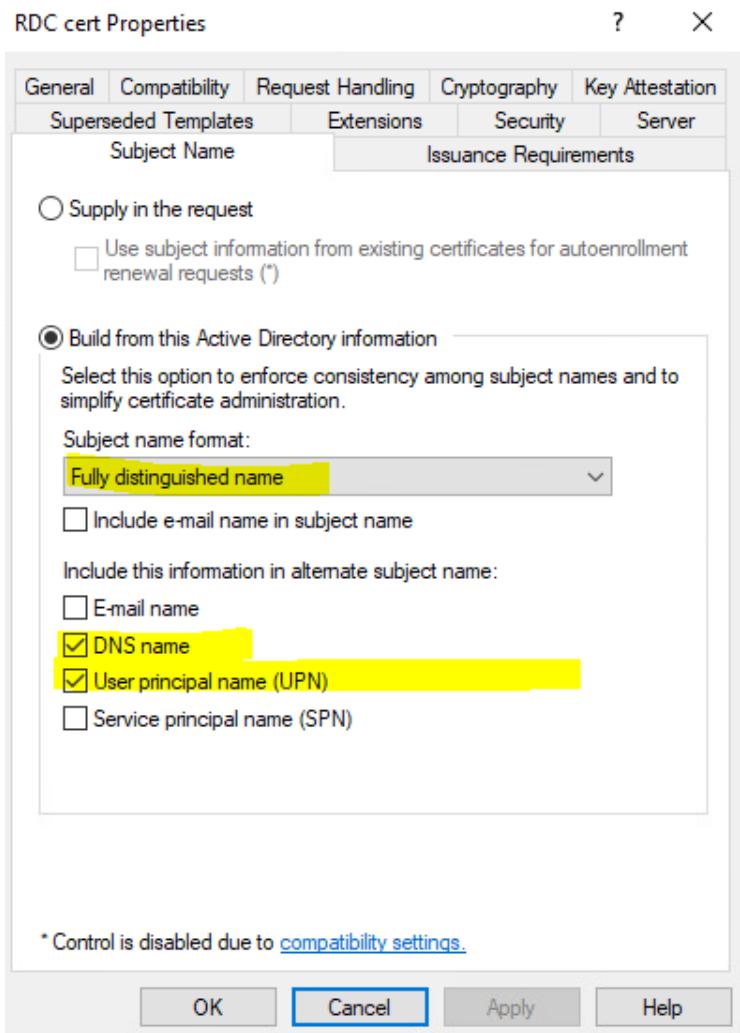
Validity period:
1 years

Renewal period:
6 weeks

Publish certificate in Active Directory

Do not automatically reenroll if a duplicate certificate exists in Active Directory

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

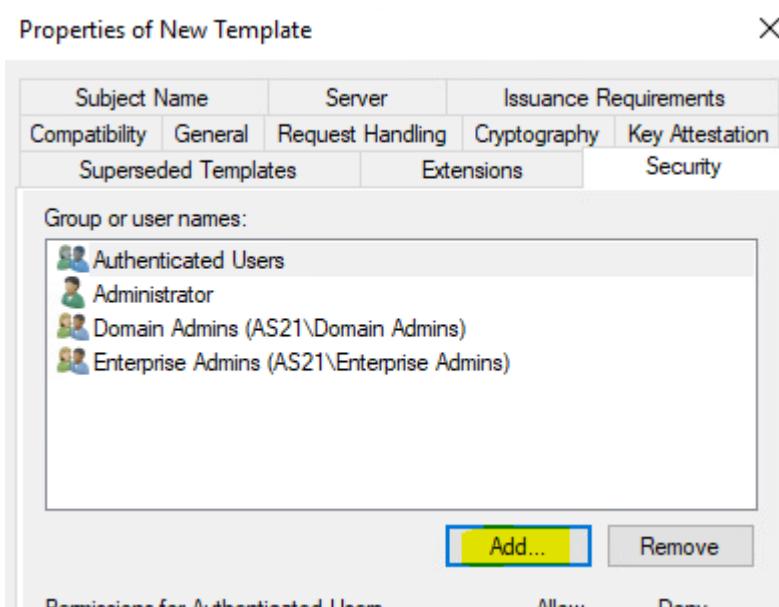


Добавляем в Extensions -> Application Policies 2 позиции:

Client Authentication

Server Authentication

Нужно добавить возможность выпуска сертификата любой машиной



Даем всем права на выпуск сертификата группе Everyone

Select Users, Computers, Service Accounts, or Groups X

Select this object type:
Users, Groups, or Built-in security principals Object Types...

From this location:
as21.local Locations...

Enter the object names to select ([examples](#)):
 Check Names

Advanced... OK Cancel

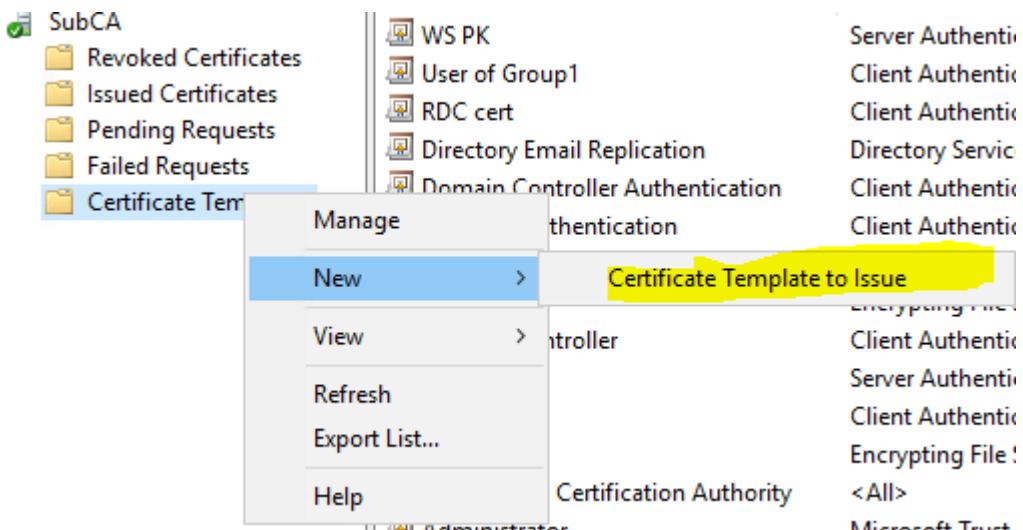
Group or user names:

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

Add... Remove

Permissions for Everyone	Allow	Deny
Full Control	<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



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

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

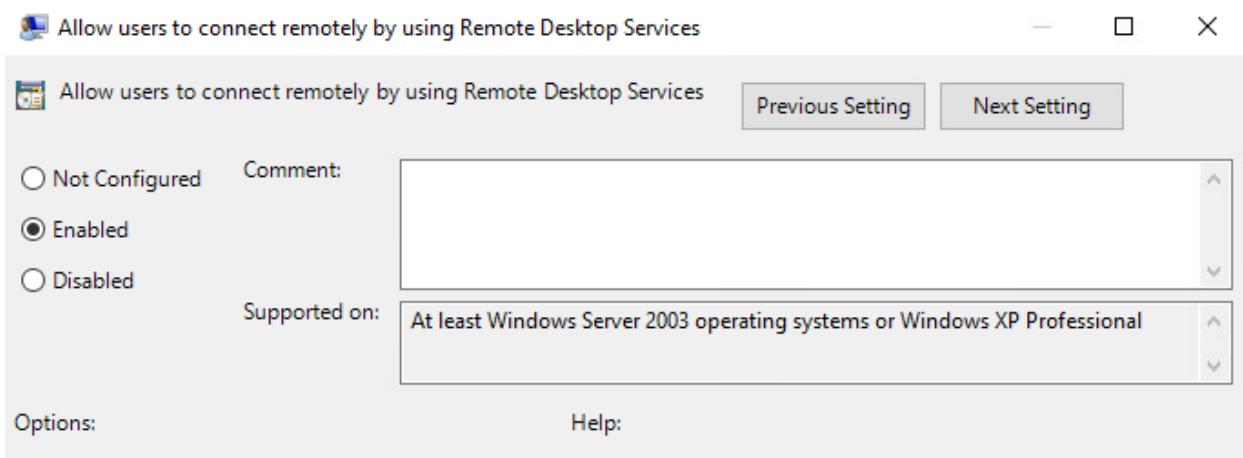
После установки центра сертификации - мы создаем шаблон для сервера рдс

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

Настройки GPO для RDP

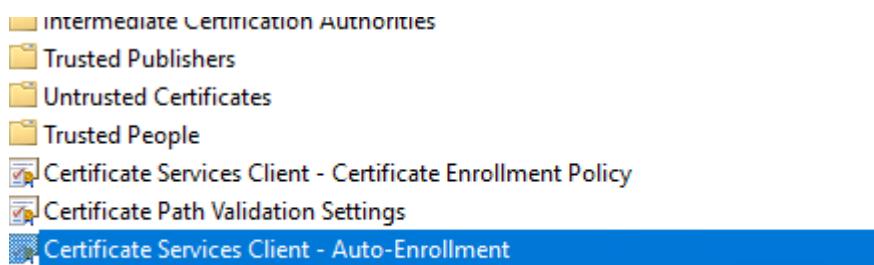
Разрешаем через GPO использование Remote Desktop Connection

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**

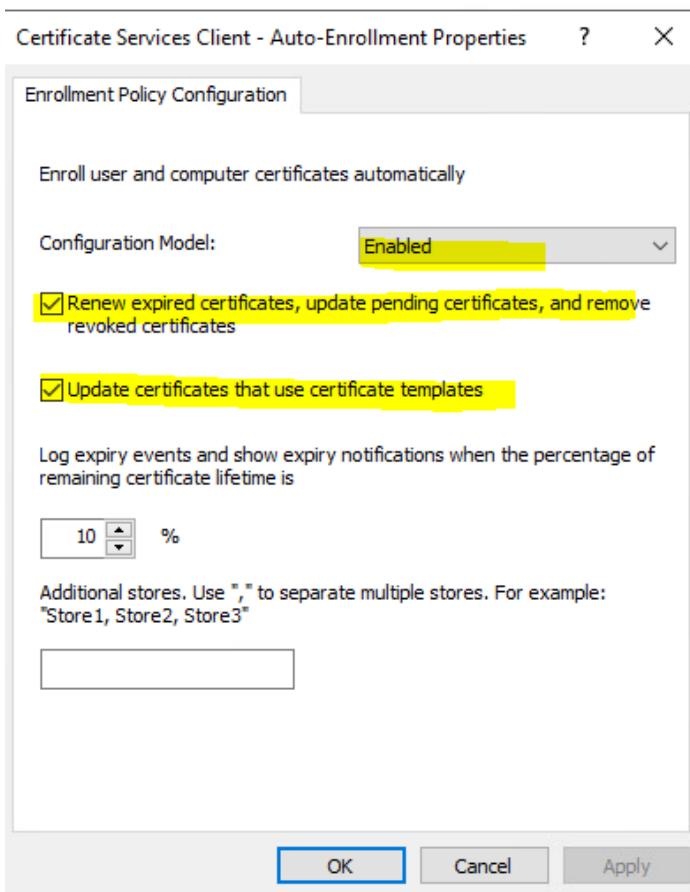


Включаем авто выдачу сертификатов всем устройствам домена

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

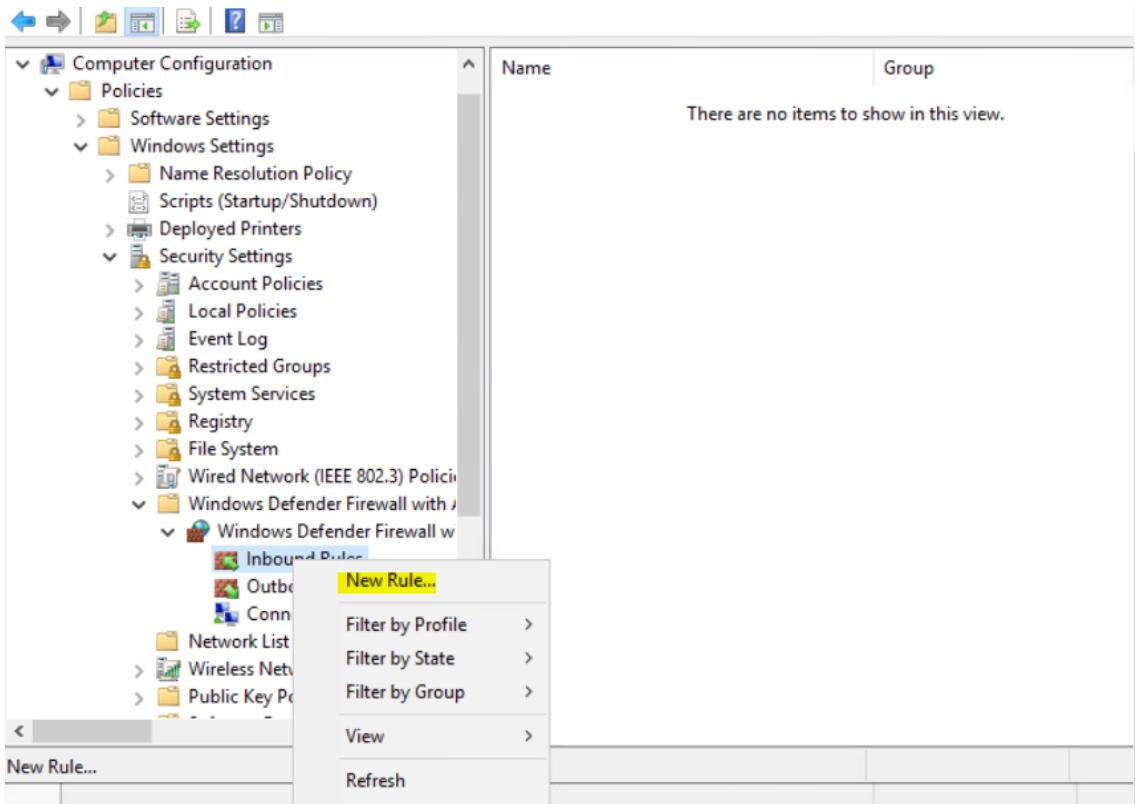


Включаем общую настройку выдачи и выбираем 2 конфигурации



Разрешаем подключение по RDP компьютерам домена

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



Выбираем предопределенные (Predefined)

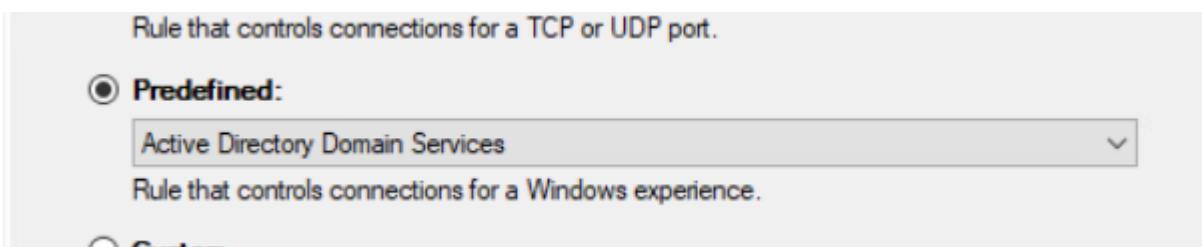
Rule that controls connections for a TCP or UDP port.

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

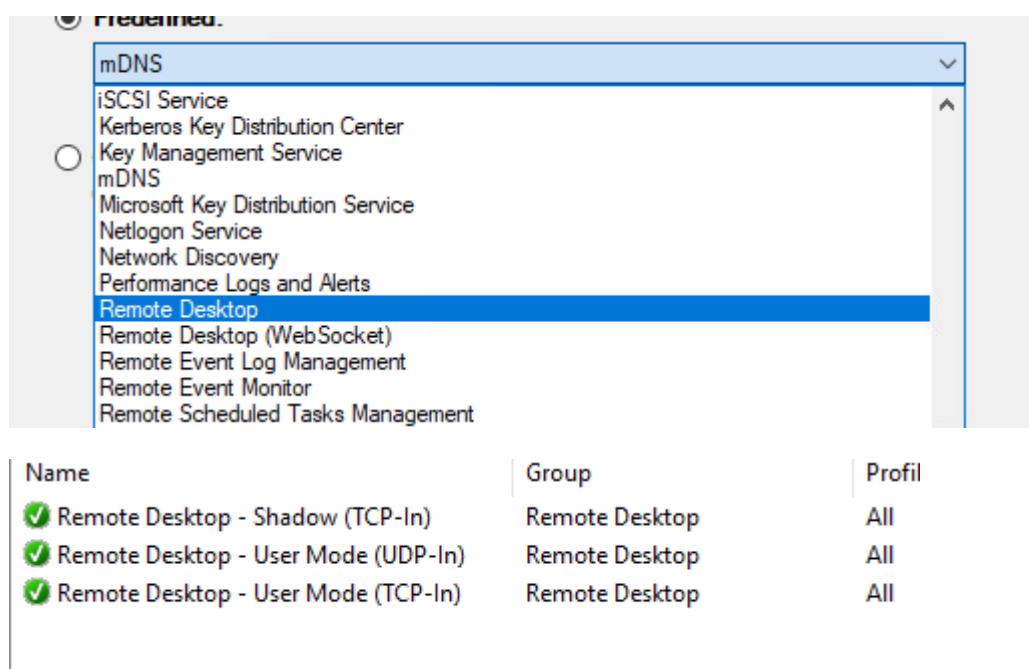
Remote Desktop (WebSocket)

Remote Event Log Management

Remote Event Monitor

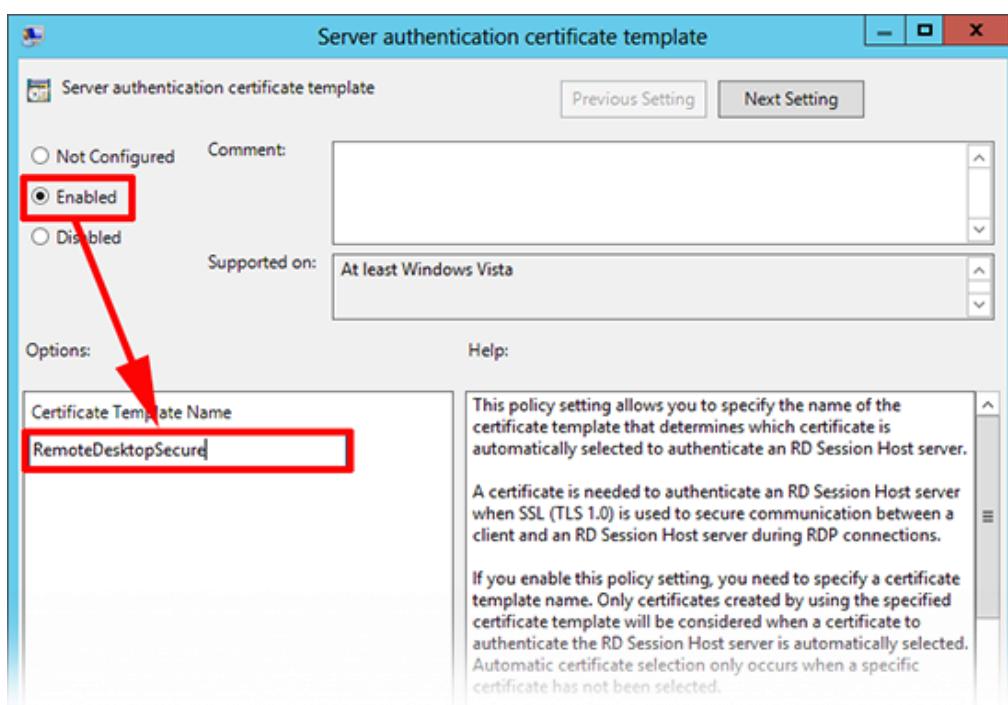
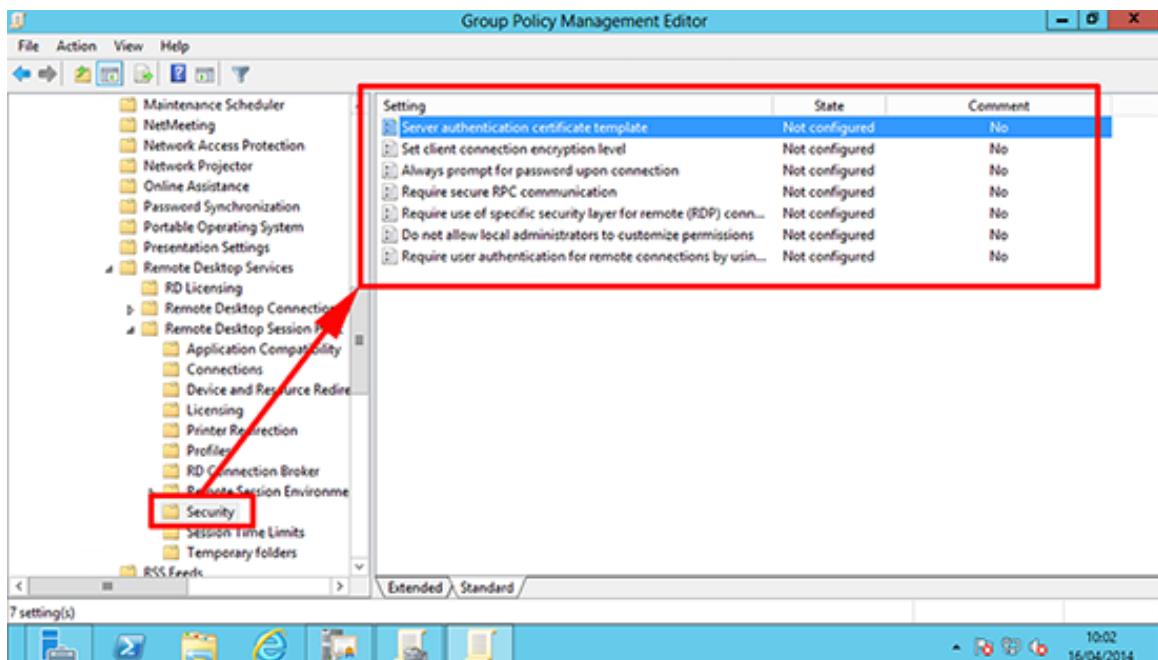
Remote Scheduled Tasks Management

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

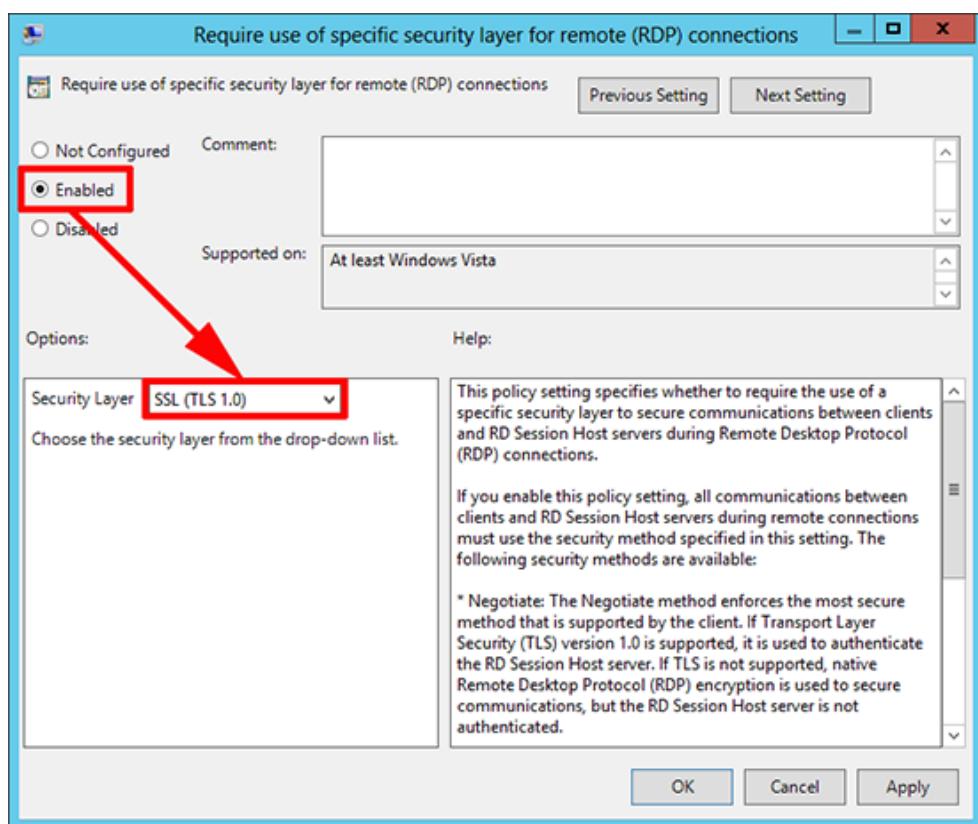
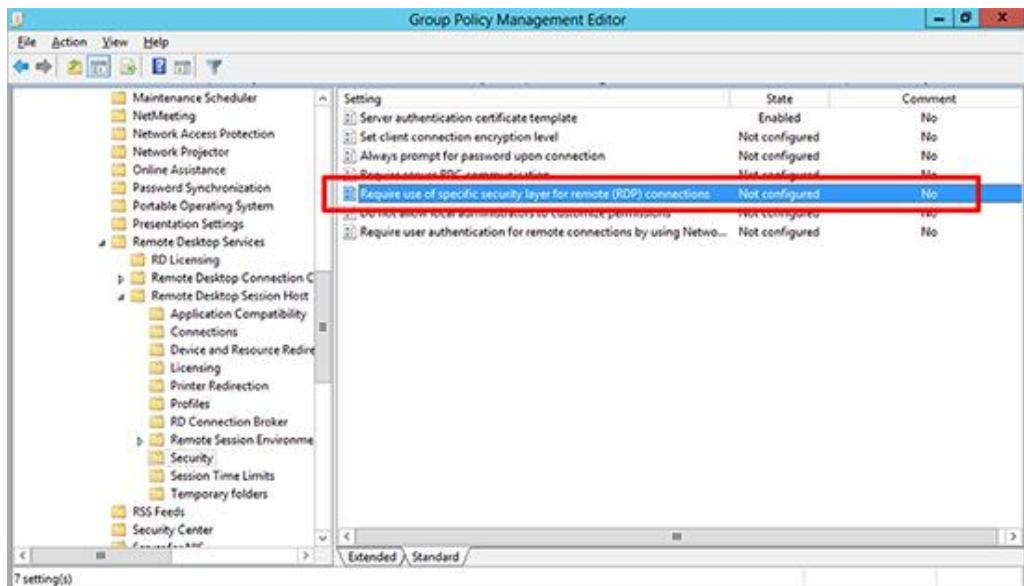


Включаем требование к использованию сертификатов

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
Install Before you begin

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

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

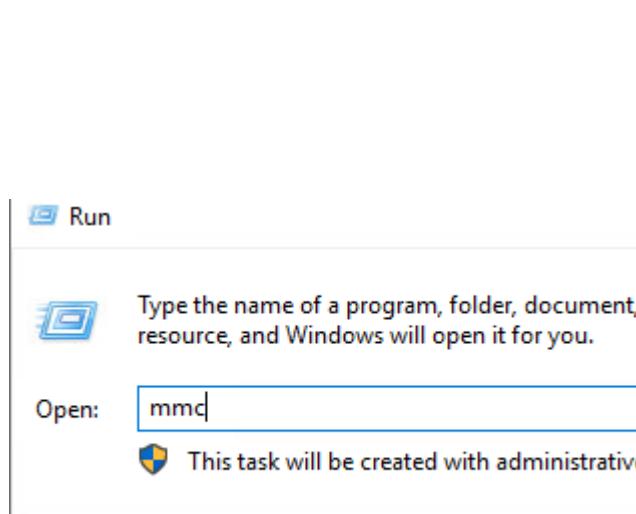
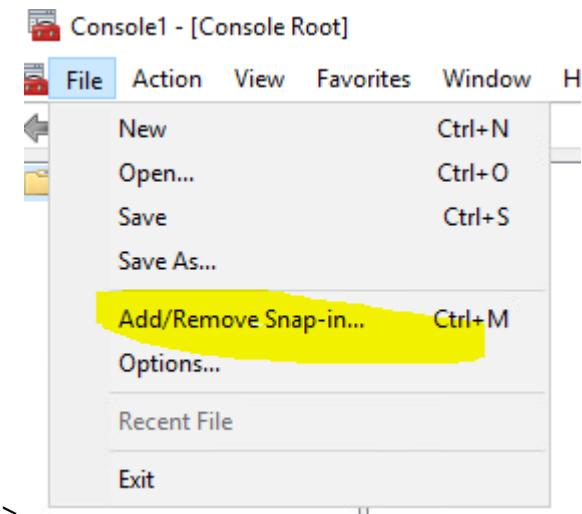
Selected

- 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

Certificates snap-in

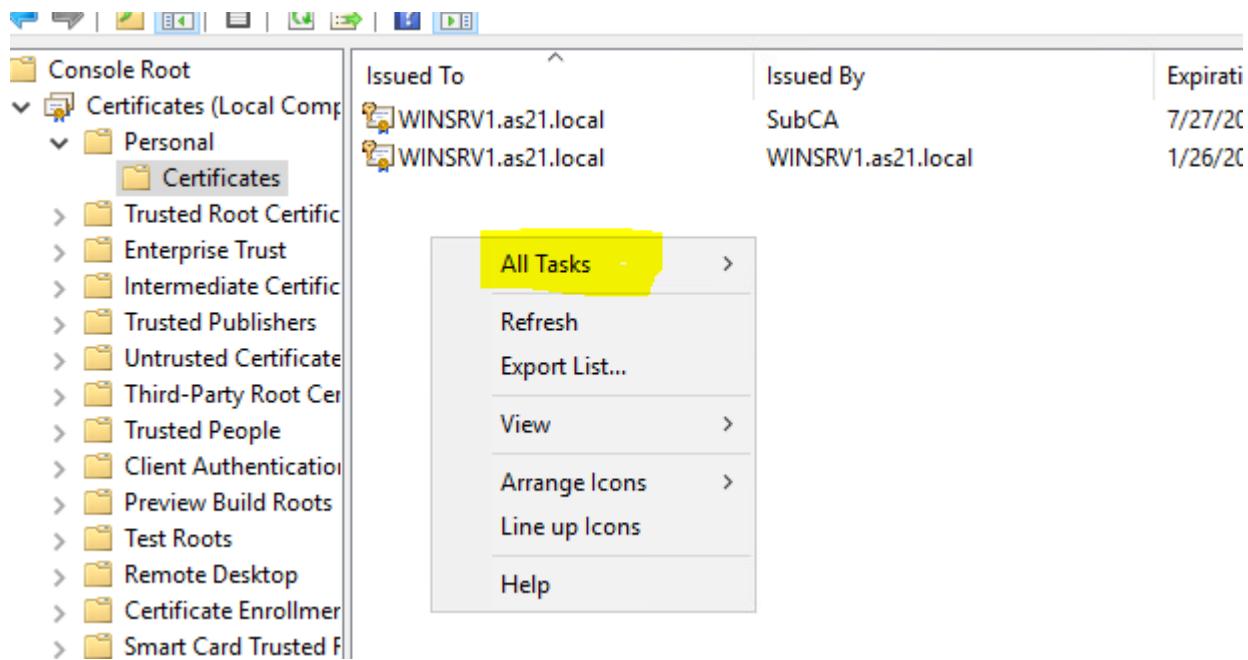
This snap-in will always manage:

My user account
 Service account
 Computer account

Select the computer you want this snap-in to manage.

This snap-in will always manage:

Local computer: (the computer this console is running on)
 Another computer: [text input field]

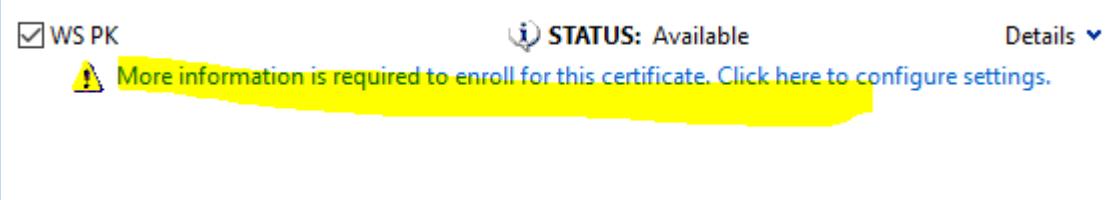


A screenshot of the Windows Certificate Manager. On the left, there's a tree view with 'Console Root' expanded, showing 'Certificates (Local Computer)' under 'Personal'. A context menu is open over one of the certificates, with 'All Tasks' highlighted in yellow.

Issued To	Issued By	Expirati
WINSRV1.as21.local	SubCA	7/27/20
WINSRV1.as21.local	WINSRV1.as21.local	1/26/20

All Task > Request New Certificate

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



The screenshot shows a 'Request New Certificate' dialog. On the left, there's a checkbox labeled 'WS PK' which is checked. In the center, there's a status indicator showing 'STATUS: Available' with an information icon. Below it, a warning message reads: 'More information is required to enroll for this certificate. Click here to configure settings.' On the right, there's a 'Details' button with a dropdown arrow.

Сверху заводим Common Name – rds.reaskills2026.local

И

rds.rea2026.ru и *.reaskills2026.local

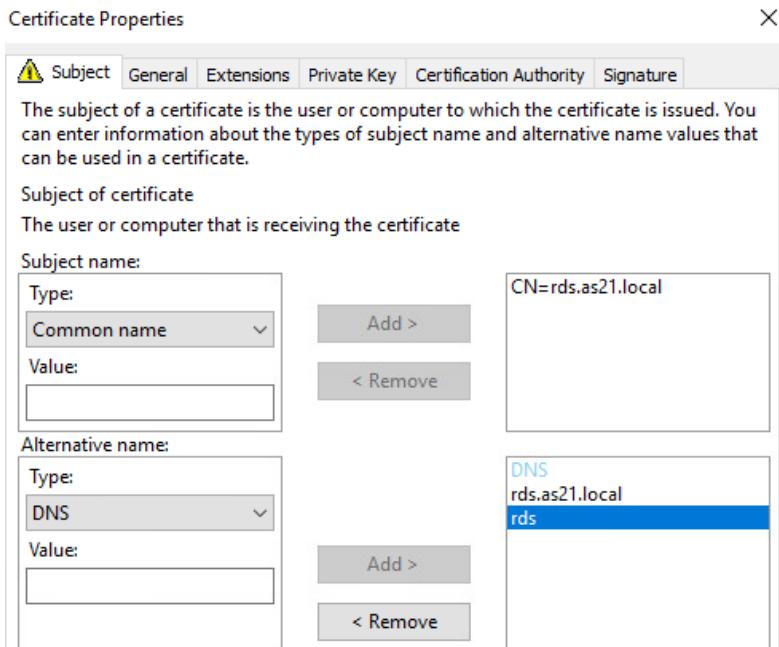
Внизу заводим DNS rds.reaskills2026.local

И

rds.rea2026.ru

И

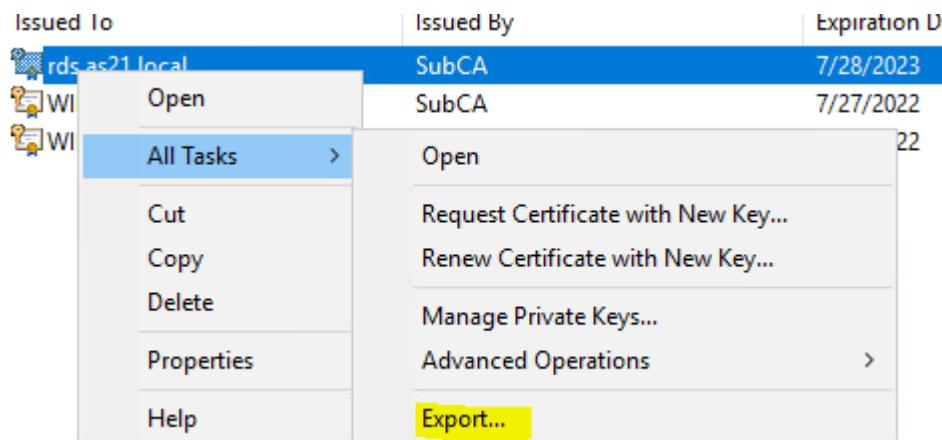
*.reaskills2026.local



Выпускаем сертификат

The screenshot shows the certificate issuance interface. The 'WS PK' checkbox is checked. The status is 'Available'. The 'Enroll' button is highlighted in yellow.

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:

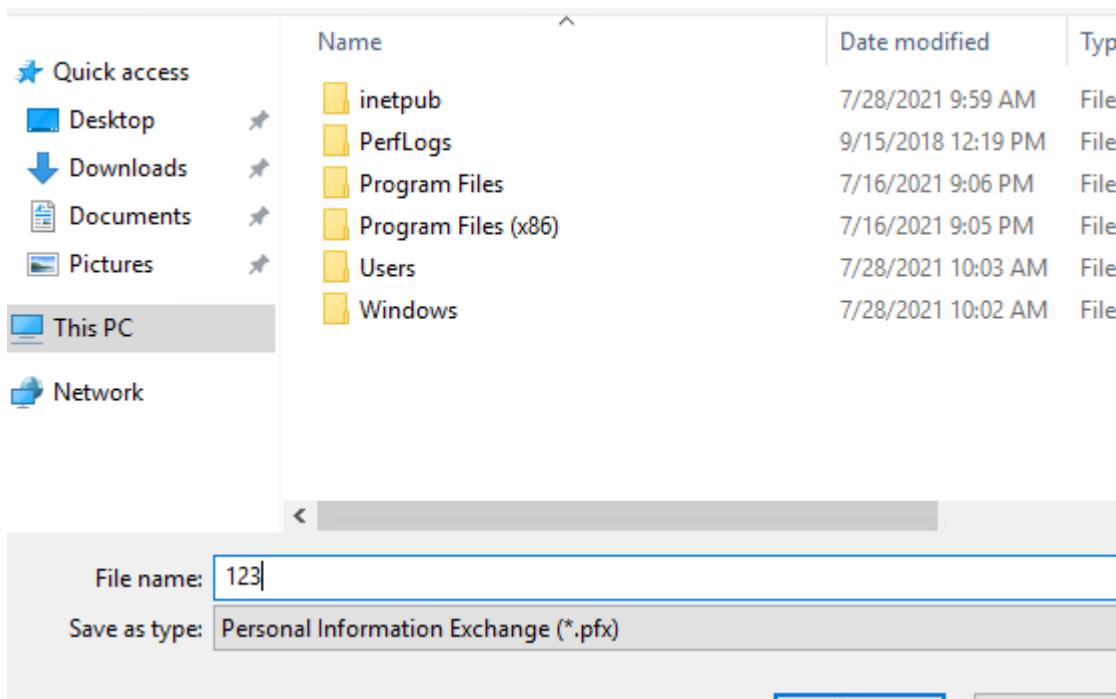
•••

Confirm password:

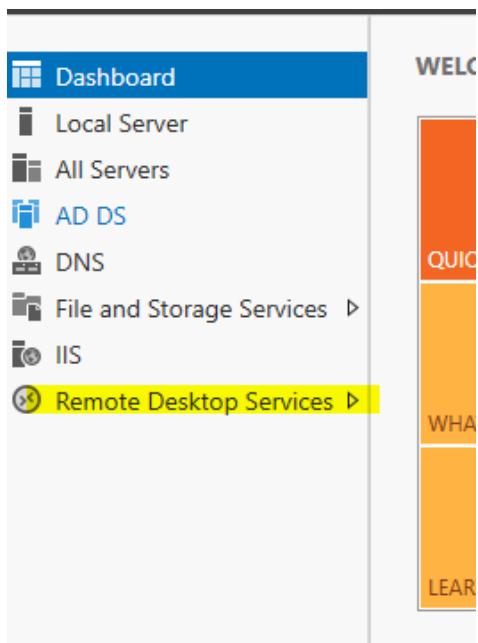
•••

Encryption: AES256-SHA256

Сохраняем файл (не забываем куда)



Идем в сервер менеджере в консоль RDS



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

GET STARTED WITH REMOTE DESKTOP SERVICES

1 Set up a Remote Desktop Services deployment

Virtual machine-based desktop deployment

2 Add RD Virtualization Host servers

3 Create virtual desktop collections

Session-based desktop

2 Add RD Session Host

3 Create session collect

LEARN MORE < | >

DEPLOYMENT OVERVIEW

RD Connection Broker server: WINSRV1.as21.local

Managed as : AS21\Administrator

TASKS

DEPLOYMENT SERVERS

Last refreshed on 7/28/2021 10:10:02

Edit Deployment Properties

Connect to Another Deployment

Refresh

Server FQDN Installed Rc

Переходим на вкладку Certificates и выбираем Select existing certificate

Deployment Properties

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 Sing	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:

 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 Sinc	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.

Повторяем для всех трех верхних ролей. Должно получиться следующее:

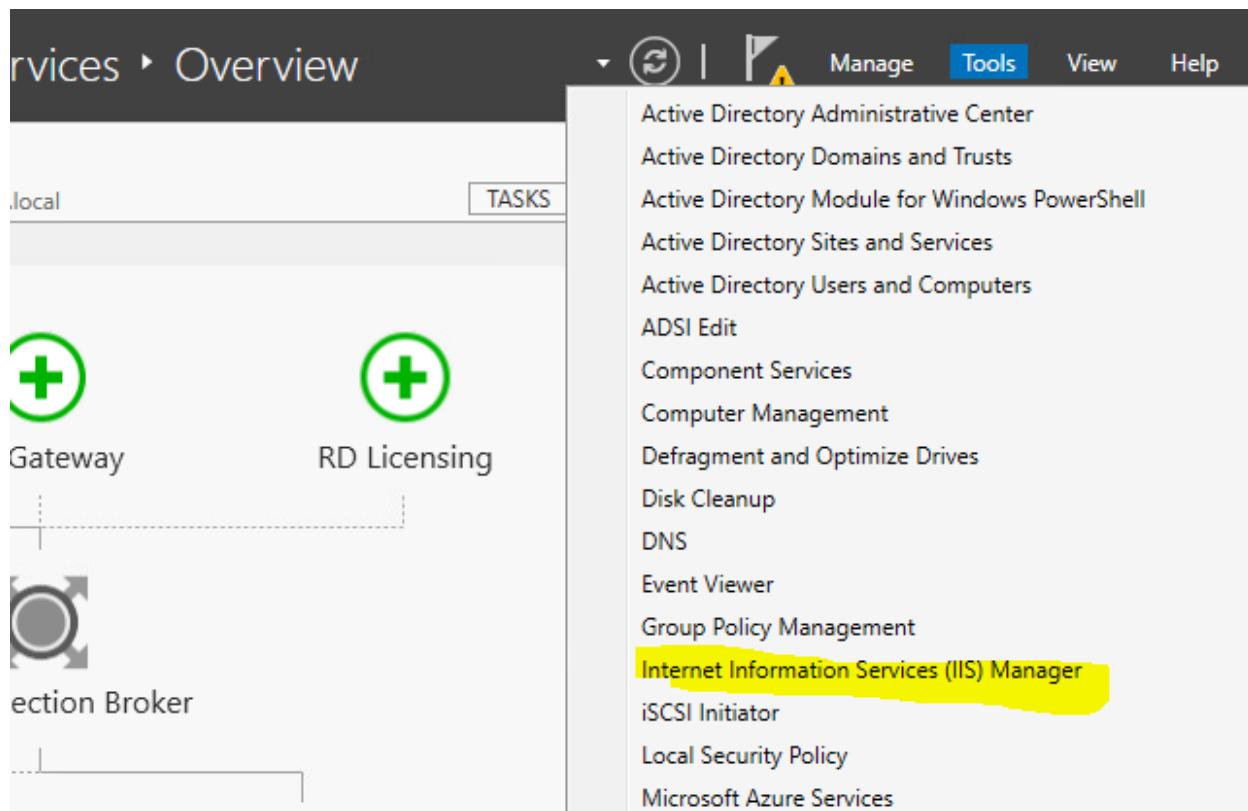
Role Service	Level	Status	State
RD Connection Broker - Enable Sinc	Trusted	OK	Success
RD Connection Broker - Publishing	Trusted	OK	Success
RD Web Access	Trusted	OK	Success
RD Gateway	Unknown	--	

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

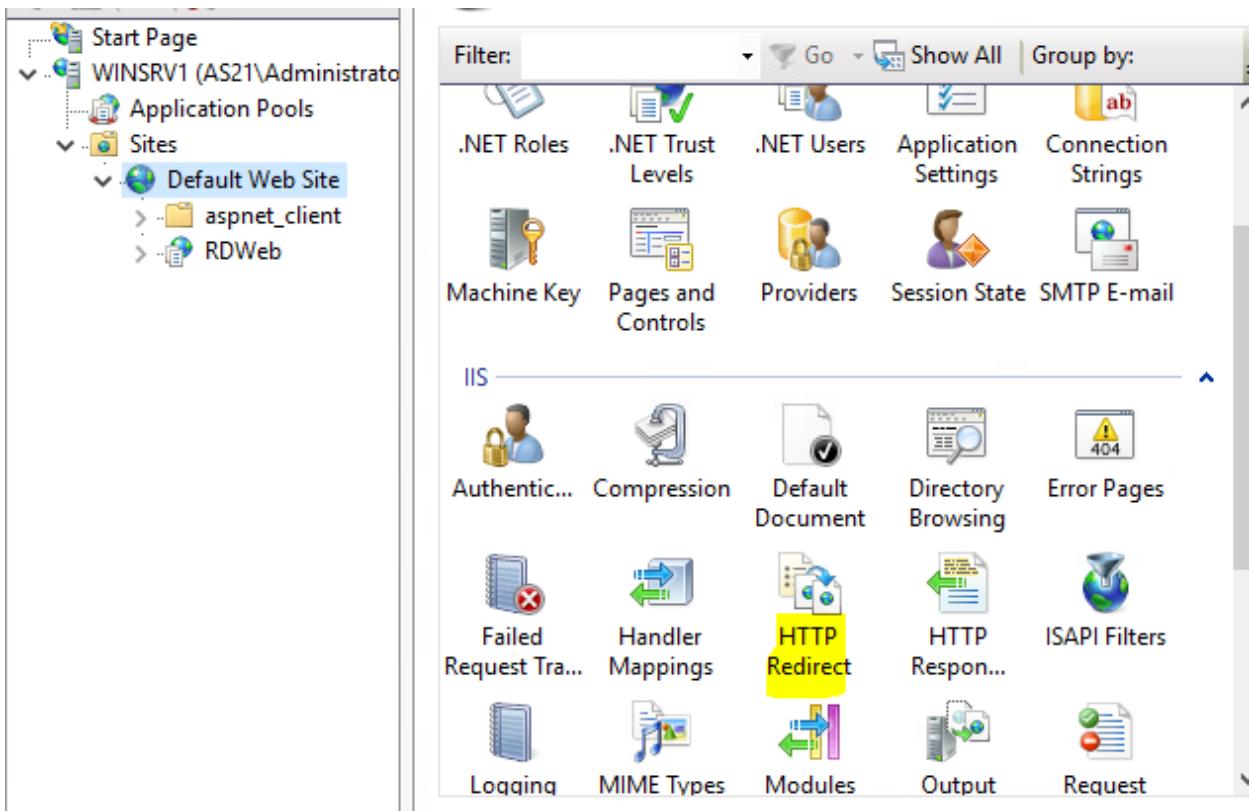
ВАЖНО!!! Убеждаемся, что в DNS есть A запись rds, которая ведет на rds.

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>

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:

Found (302)

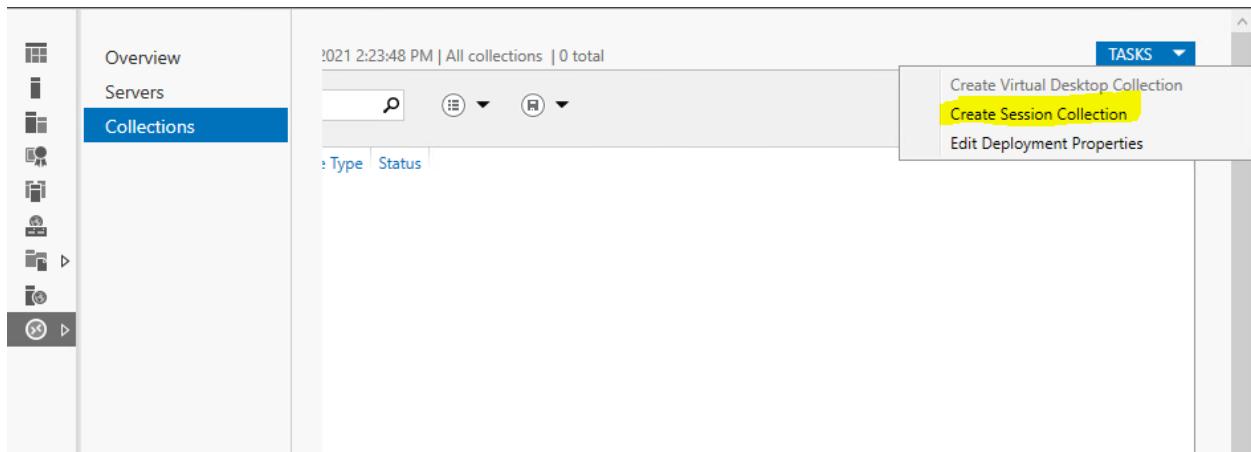
Actions

- Apply
- Cancel
- Help

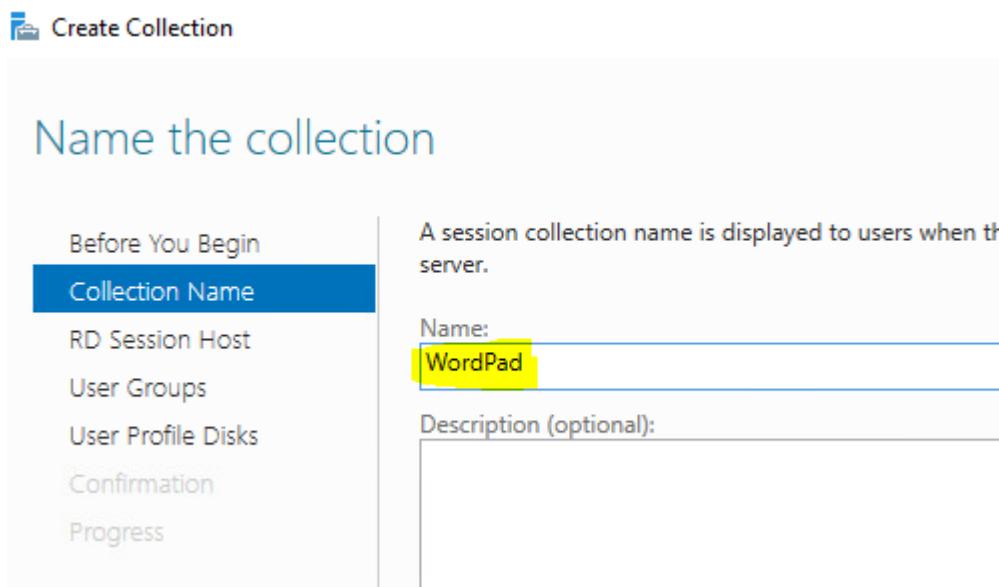
Публикация коллекции RDS

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	<input type="button" value="Add..."/>
	<input type="button" value="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):

Публикация приложения RDS

Публикуем приложение

The screenshot shows the 'Properties of the collection' dialog for a 'WordPad' collection. The 'Collection Type' is set to 'Session' and 'Resources' to 'Remote Desktop'. The 'User Group' is 'AS21\Group2'. On the right, there's a list of users with a 'Filter' input field and buttons for 'Server FQDN', 'User', and 'Session State'. Below this, the 'REMOTEAPP PROGRAMS' section shows 'Published RemoteApp programs | 0 total'. It includes a note that 'Remote Desktop is published for the users of the collection' and two buttons: 'Publish RemoteApp Programs' (highlighted with a yellow box) and 'Unpublish RemoteApp Programs'. A warning message below states: 'Publishing RemoteApp programs will unpublish the Remote Desktop.' A progress bar at the bottom indicates the task is in progress.

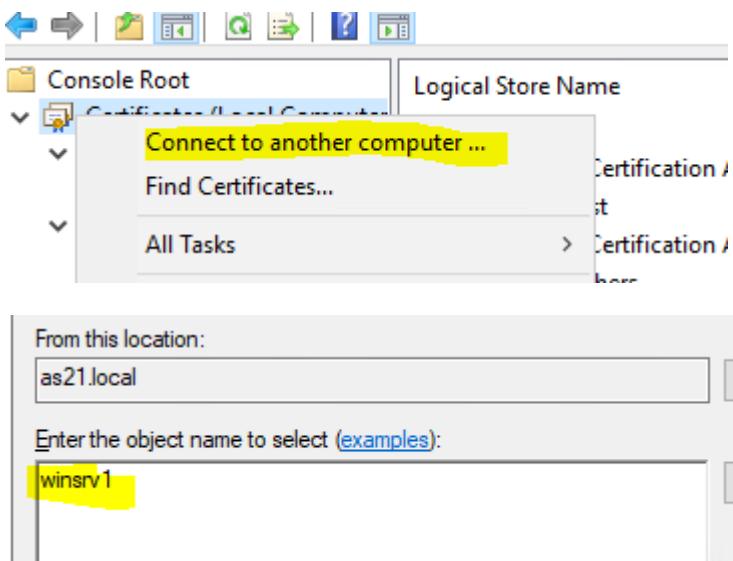
Выбираем их списка max публикуем его на RDS

The screenshot shows the 'Select RemoteApp programs' step in a wizard. The left sidebar has tabs for 'RemoteApp Programs' (selected), 'Confirmation', 'Publishing', and 'Completion'. The main area displays a list of available RemoteApp programs from the host server ('WINSRV1.as21.local'). The 'WordPad' program is selected (indicated by a checked checkbox). Other programs listed include Steps Recorder, System Configuration, System Information, Task Manager, Windows Media Player, Windows Memory Diagnostic, Windows Speech Recognition, and XPS Viewer. Below the list is an 'Add...' button. A note at the bottom says: 'Verify that the program is installed on all the RD Session Host servers in the collection.' Buttons at the bottom include '< Previous', 'Next >' (highlighted with a yellow box), 'Publish', and 'Cancel'.

Добавление сертификата в доверенные

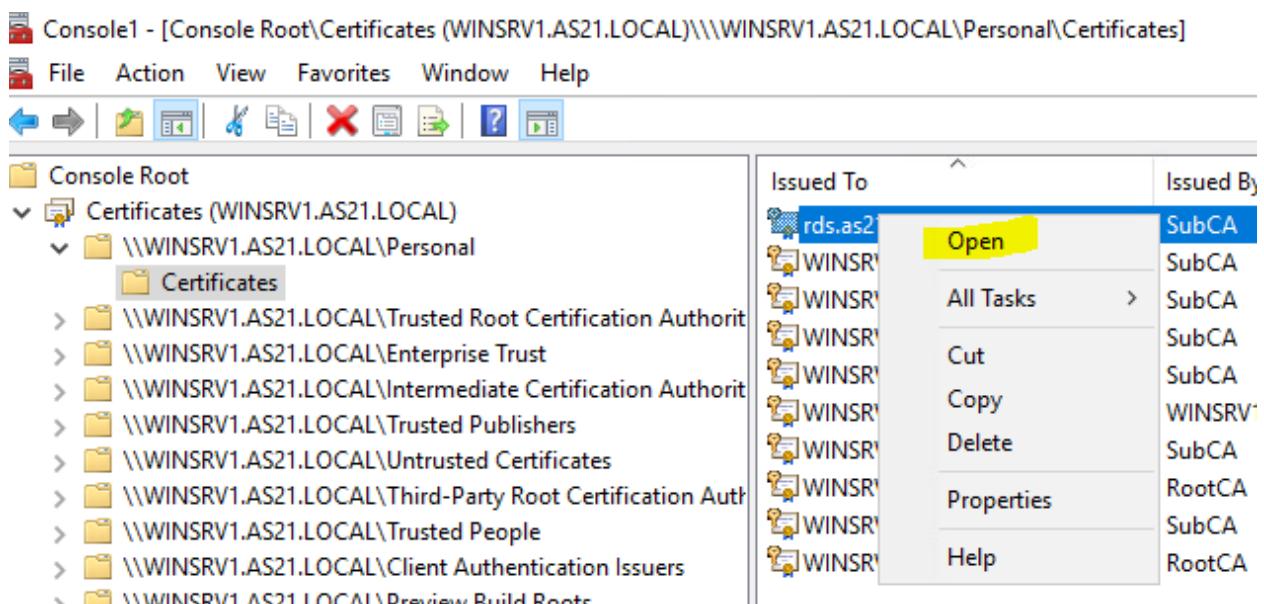
Убираем предупреждение при подключении

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

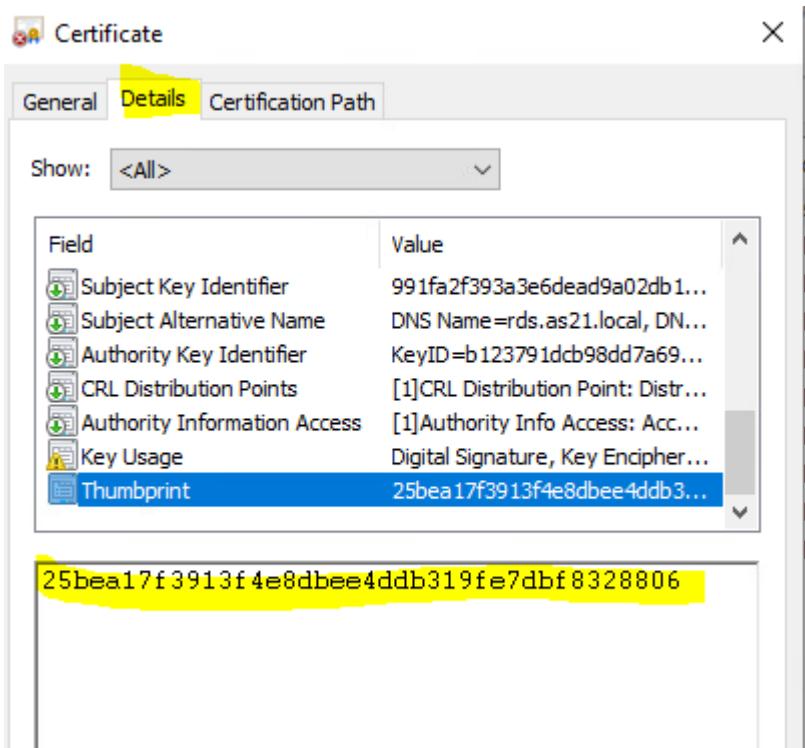


Находим выпущенный для RDS сертификат rds.reaskills2026.local

Открываем его

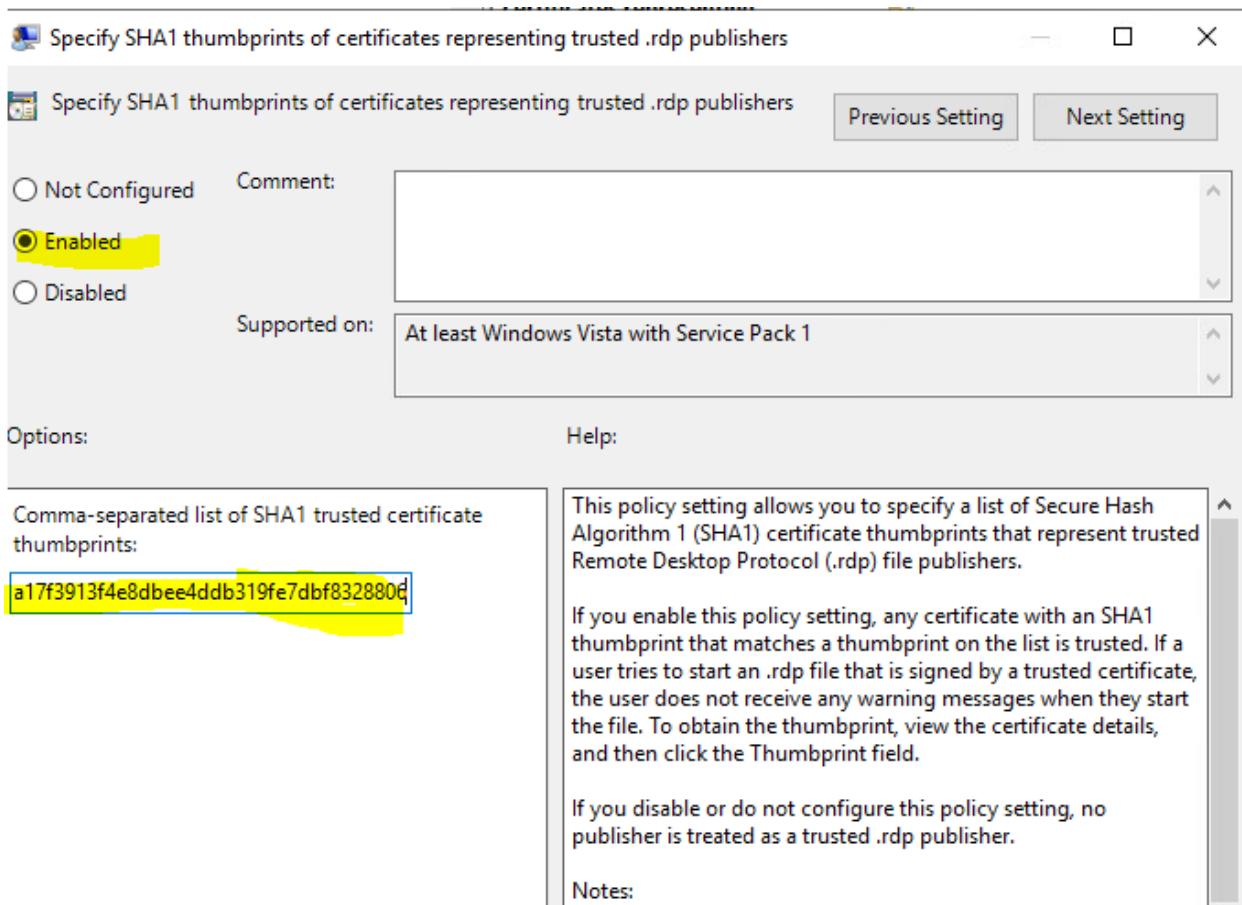


Переходим в раздел Details. Выбираем Thumbprint, где мы видим отпечаток нашего сертификата. Копируем его в буфер



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 trustee...	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

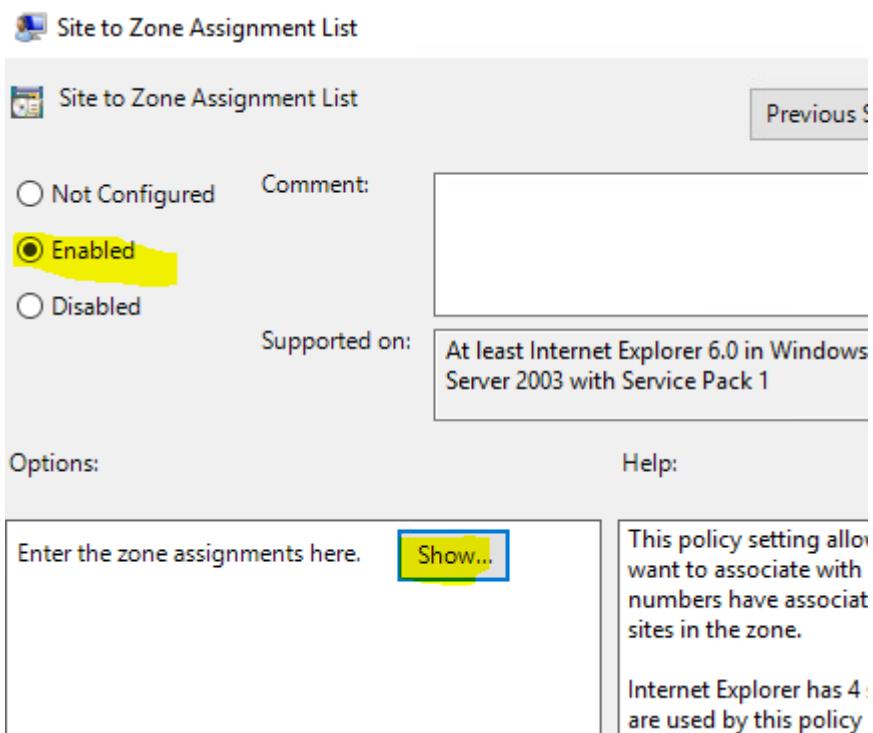
Идем в GPO, созданную на домен

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



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

Show Contents

— □ X

Enter the zone assignments here.

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

Добавляем

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

B Value пишем 1

The screenshot shows the Group Policy Management Editor interface. On the left, there is a navigation tree with several policy categories expanded, such as Internet Explorer, Application Control, and Internet Control. In the center, a detailed description of the 'Site to Zone Assignment List' policy setting is provided, stating that it associates sites to security zones (Intranet, Trusted, Internet, Restricted). On the right, a list of configuration options for this setting is shown in a table format:

Setting	Status
Local Machine Zone Template	Not configured
Locked-Down Restricted Sites Zone Template	Not configured
Restricted Sites Zone Template	Not configured
Locked-Down Trusted Sites Zone Template	Not configured
Trusted Sites Zone Template	Not configured
Turn on certificate address mismatch warning	Not configured
Intranet Sites: Include all sites that bypass the proxy server	Not configured
Intranet Sites: Include all network paths (UNCs)	Not configured
Site to Zone Assignment List	Enabled
Turn on automatic detection of intranet	Not configured
Turn on Notification bar notification for intranet content	Not configured