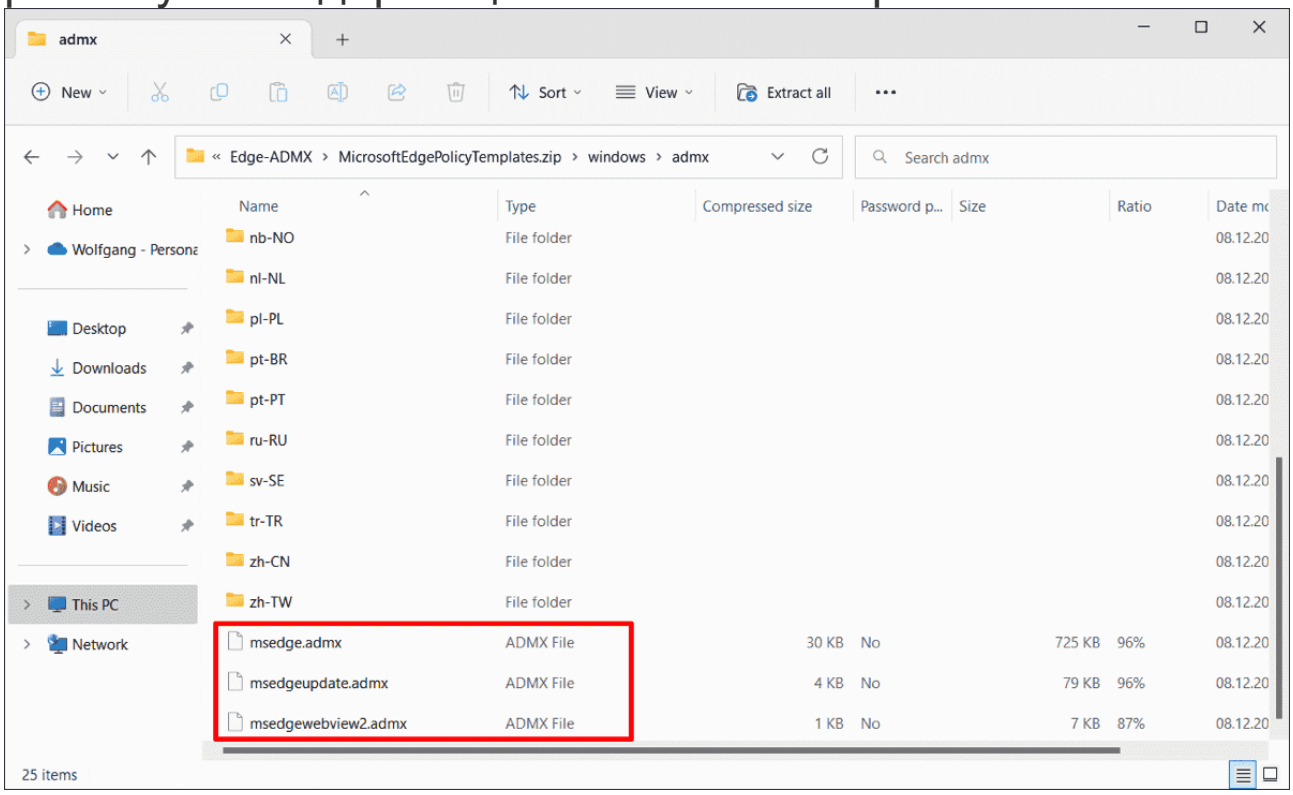
1. Установка admx, чтобы в групповых политиках отображались настройки для браузера Microsoft edge https://www.microsoft.com/en-us/edge/business/download?form=MA13FJ

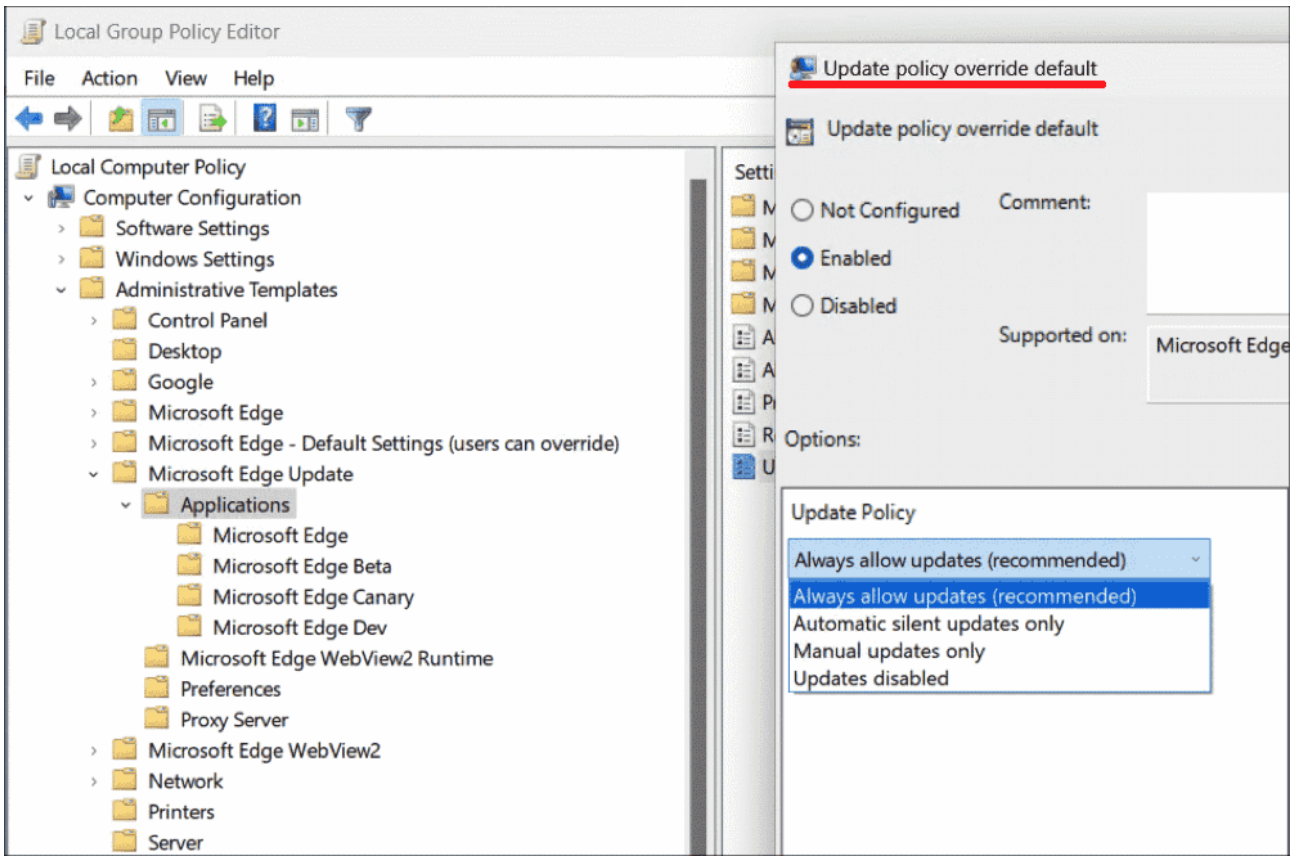
Под каждой кнопкой загрузки браузера находится ссылка с надписью « *Загрузить политику Windows для 32- или 64-битных систем»* . - скачиваем нужные шаблоны

2. Вы получите CAB-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 *msedgeweb view.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.

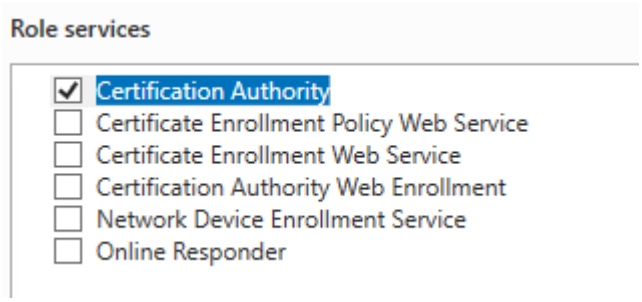
Если вы хотите установить административные шаблоны на локальную рабочую станцию, скопируйте файлы ADMX из ZIP-архива в папку *%systemroot%\Policydefinitions* . Кроме того, скопируйте языковые файлы из соответствующих каталогов, например, *de-DE* или *en-US* , в соответствующие папки внутри *Policydefinitions*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

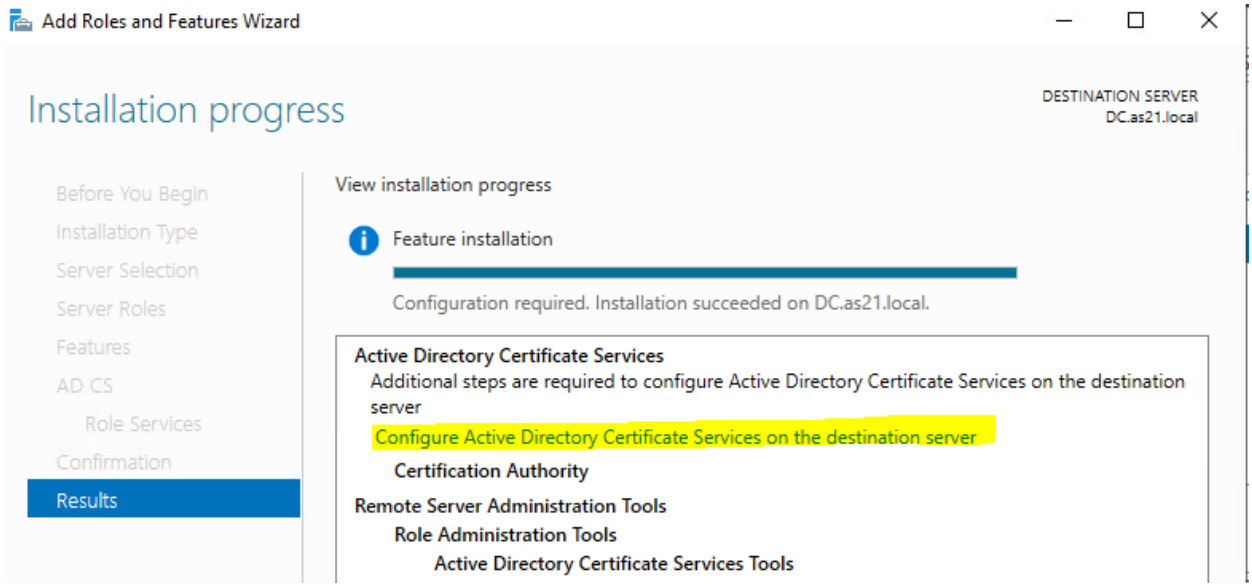
2. Центр сертификации - выполняем установку роли на контроллере домена.

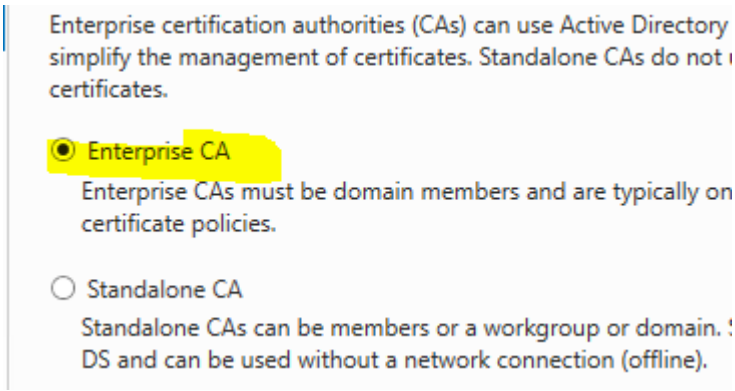
CA

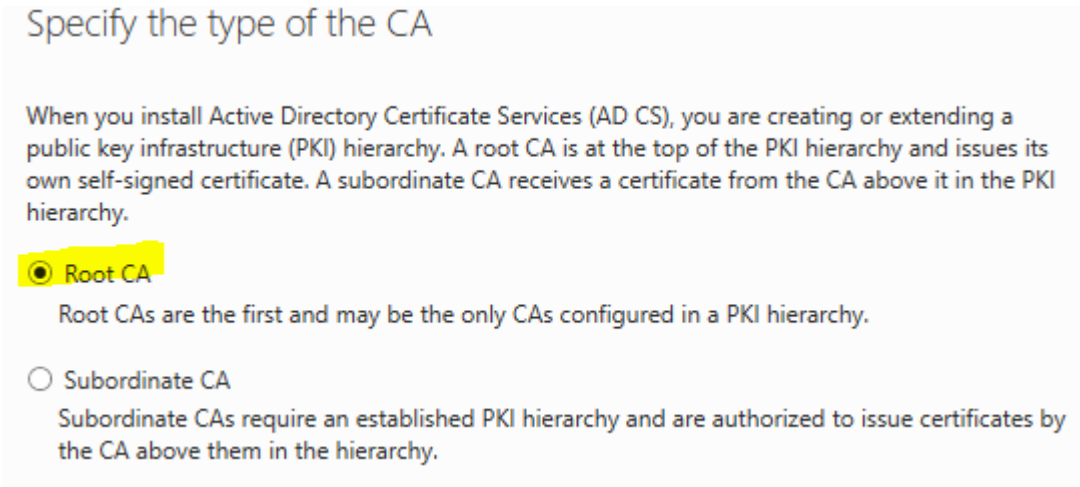
Настройте корневой центр сертификации на контроллере домена DC

Базовая настройка RootCA









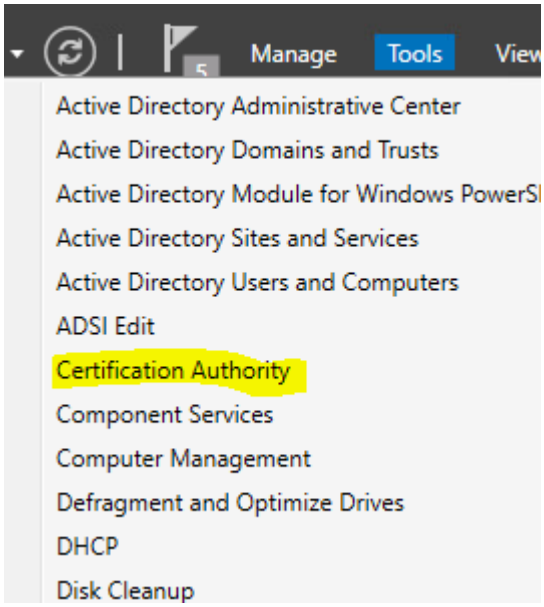
i. Имя настраиваемого центра сертификации - RootCA.

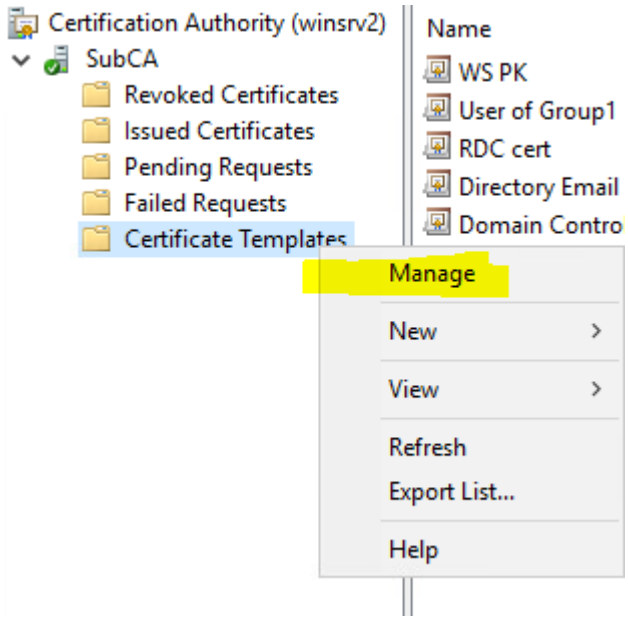
ВНИМАНИЕ - ИМЯ ПО ЗАДАНИЮ - REA2026-CA

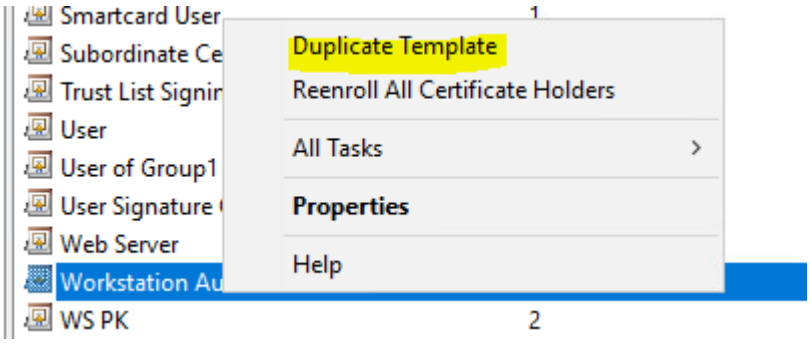
ii. Срок действия сертификата - ЕСЛИ В ЗАДАНИИ НИЧЕГО ПРО ЭТО НЕ СКАЗАНО, ОСТАВЛЯЕМ ПО УМОЛЧАНИЮ 5 ЛЕТ ВРОДЕ.

3. RDP

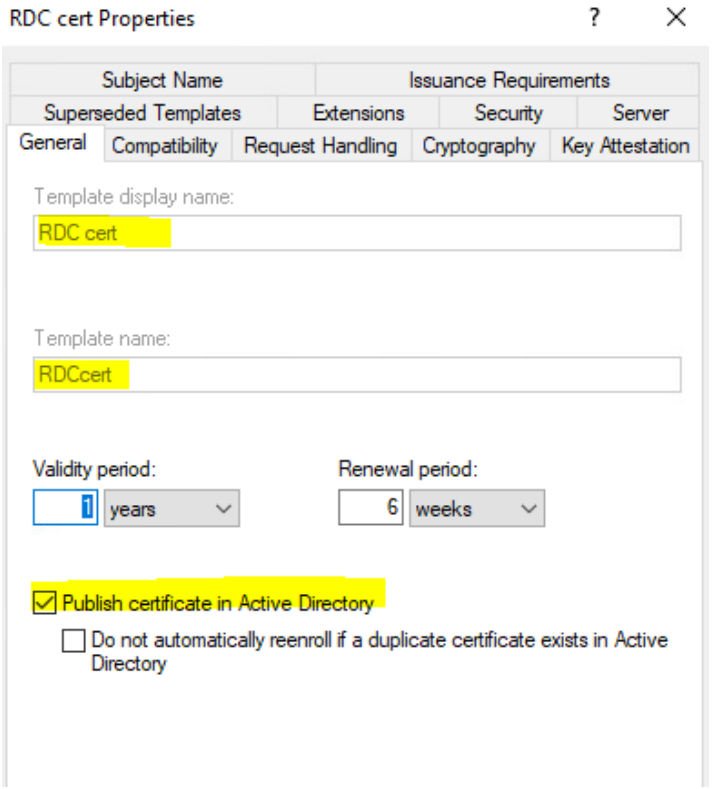
Настройка шаблона выдачи сертификатов



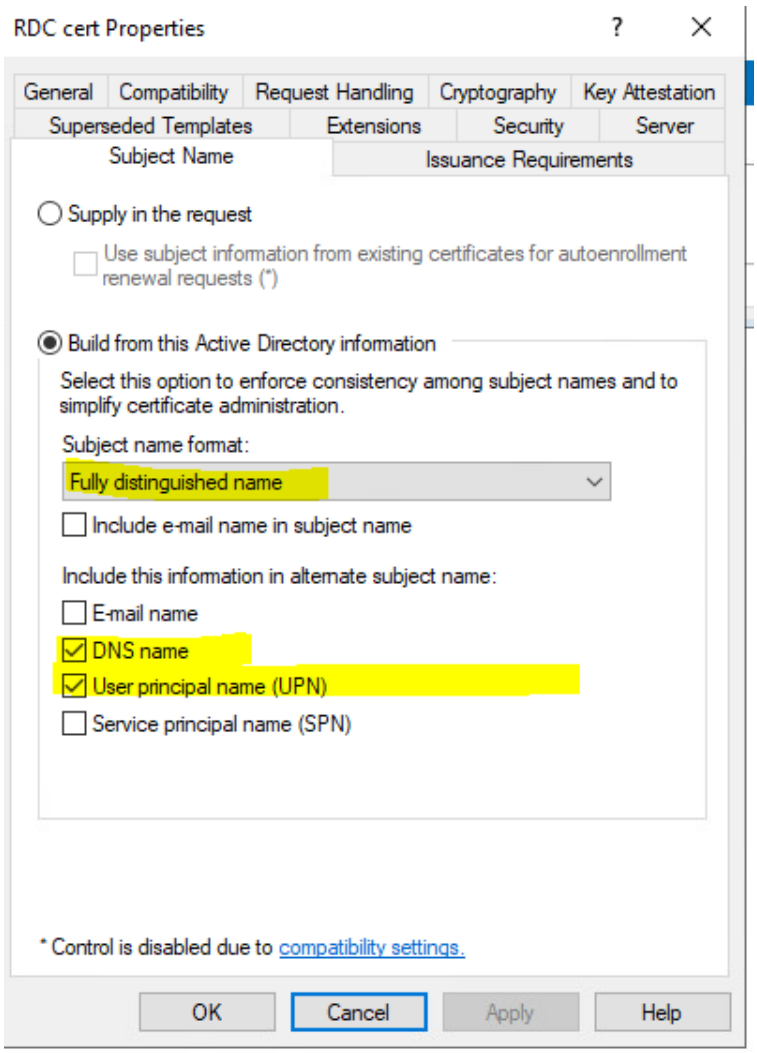




Вводим имя нового шаблона. Включаем публикацию в Active Directory



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

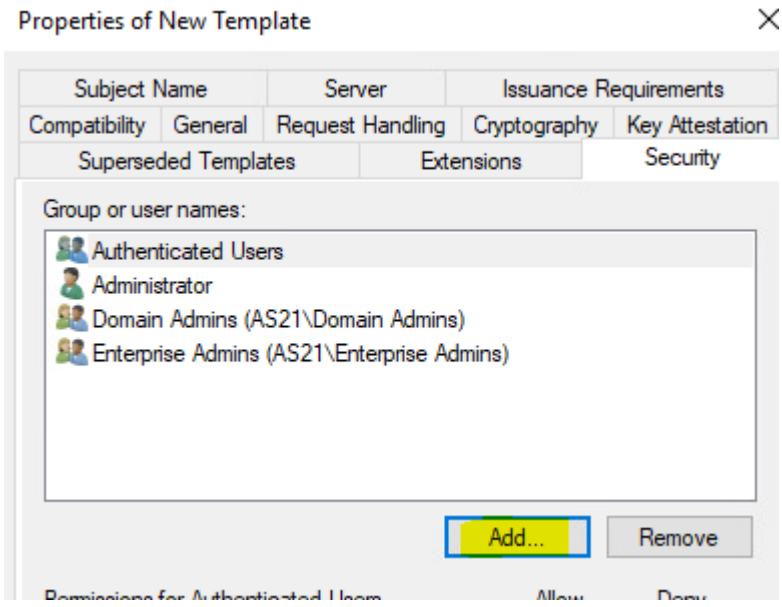


Добавляем в Extensions -> Application Policies 2 позиции:

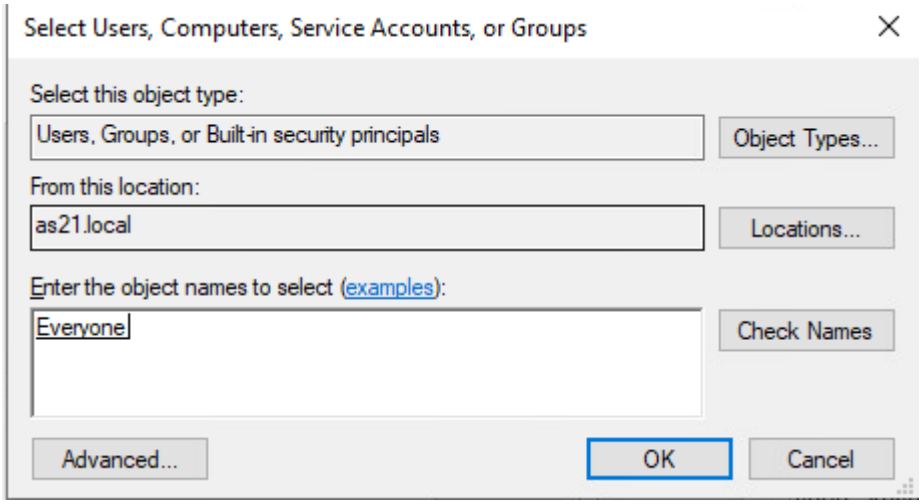
Client Authentication

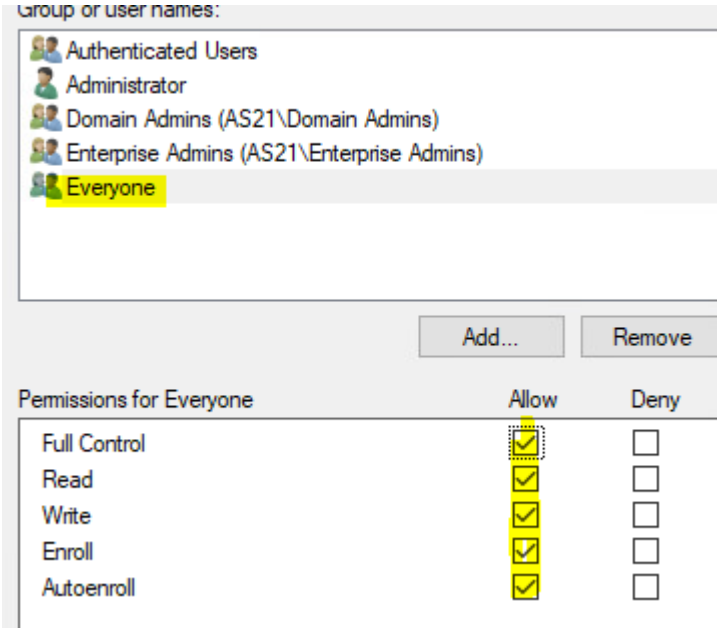
Server Authentication

Нужно добавить возможность выпуска сертификата любой машиной

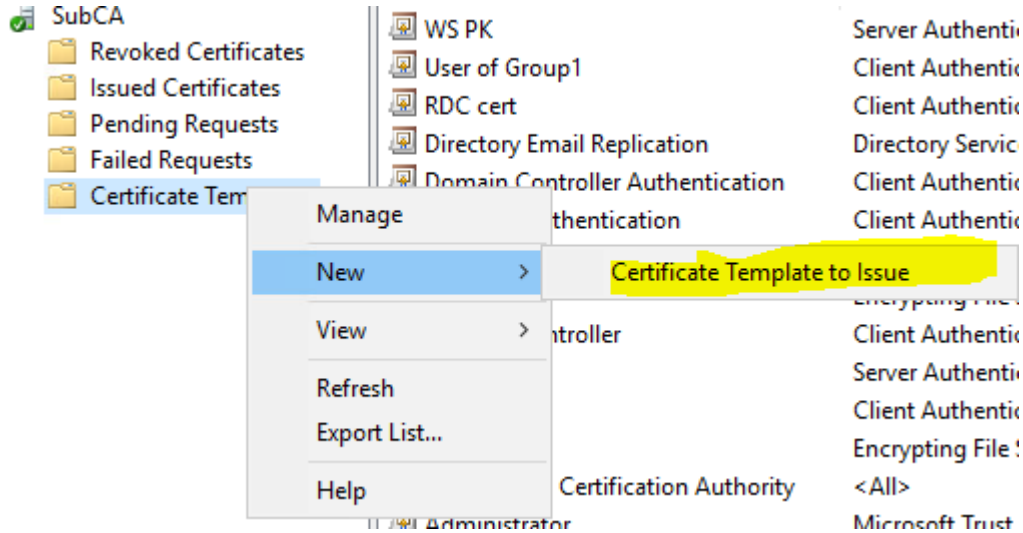


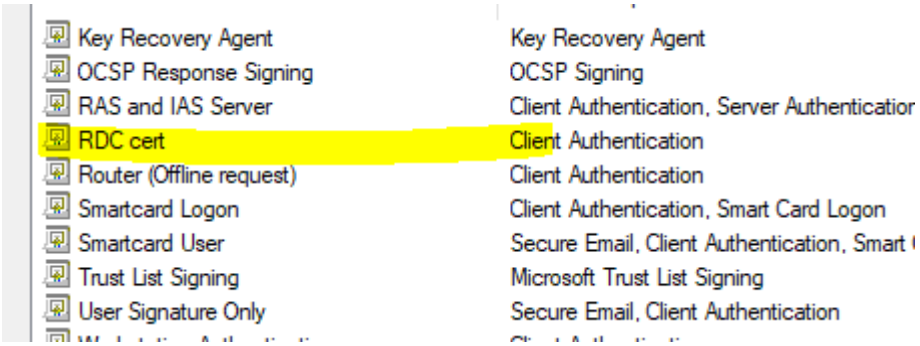
Даем всем права на выпуск сертификата группе Everyone





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

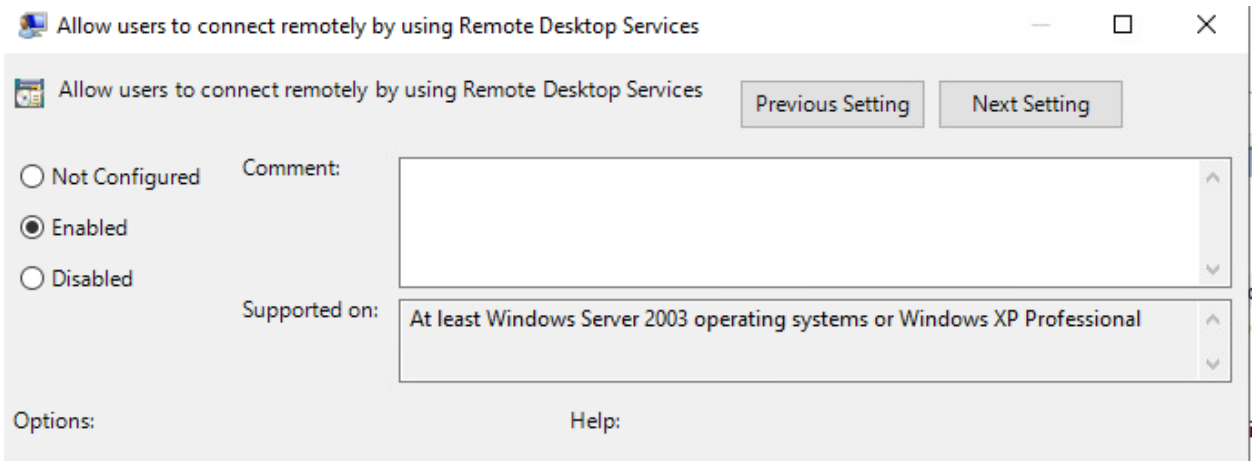
После установки центра сертификации - мы создаем шаблон для сервера рдс

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

Настройки GPO для RDP

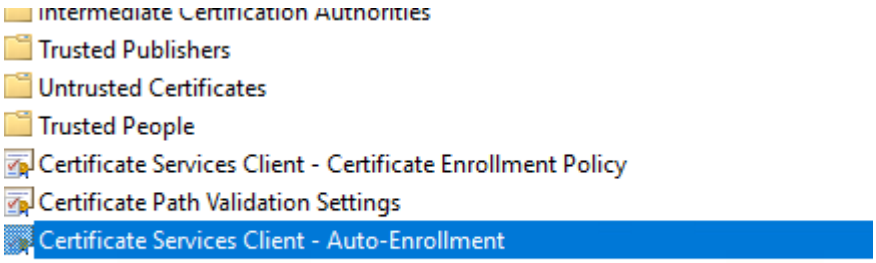
Разрешаем через GPO использование Remote Desktop Connection

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

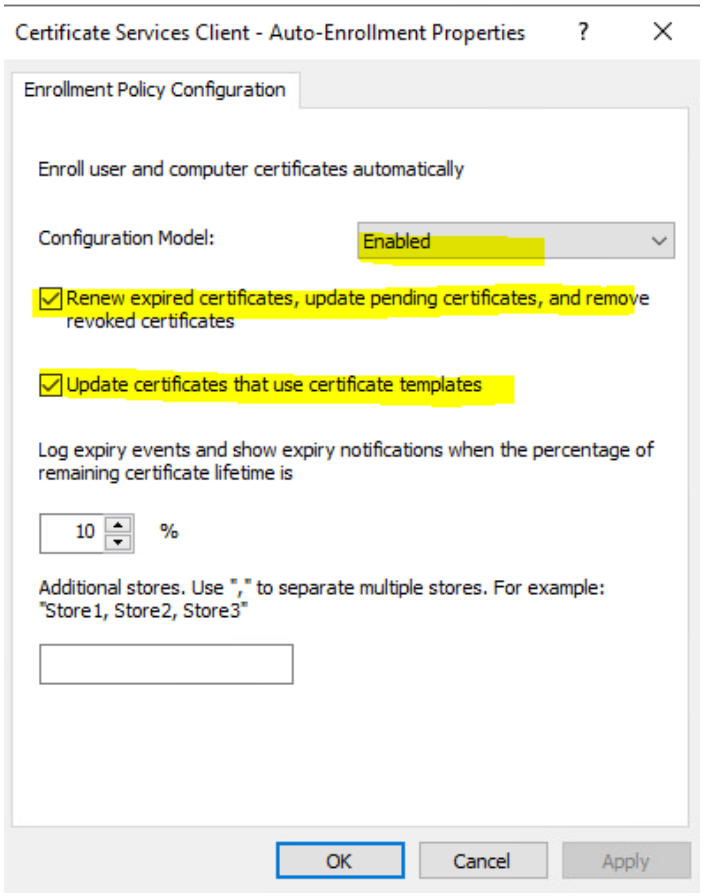


Включаем авто выдачу сертификатов всем устройствам домена

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

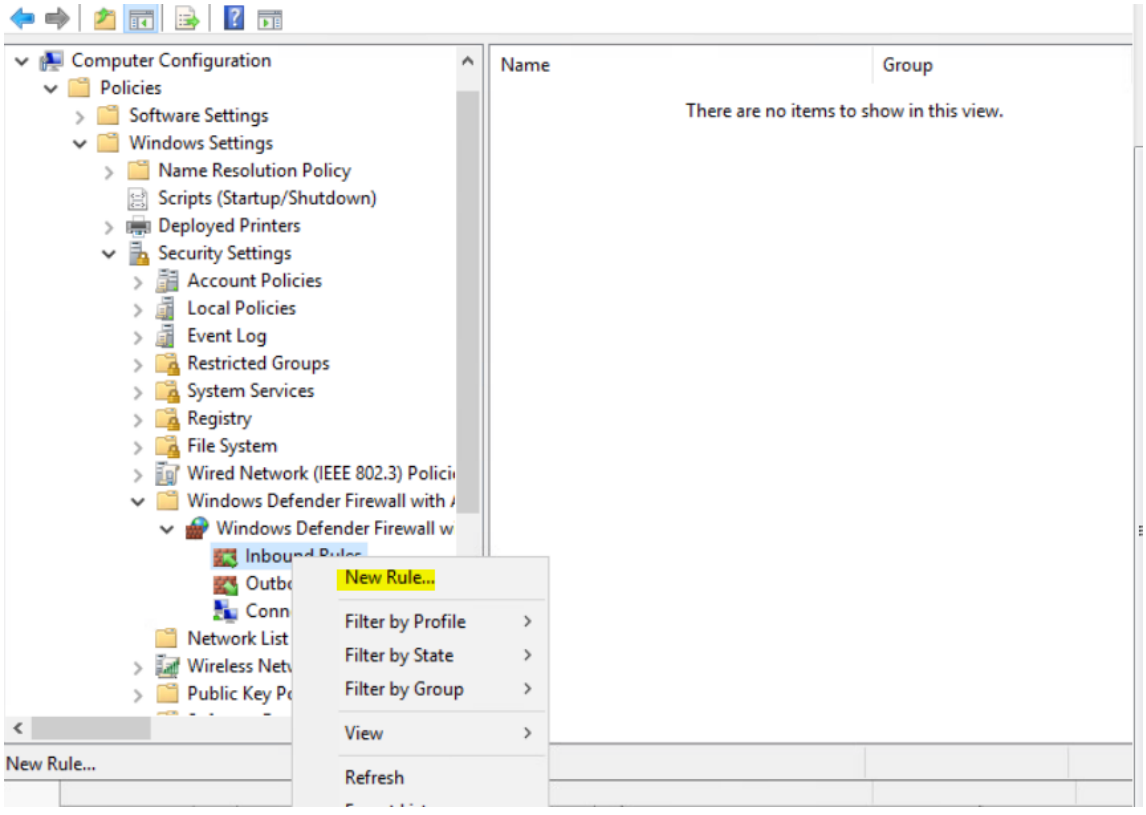


Включаем общую настройку выдачи и выбираем 2 конфигурации

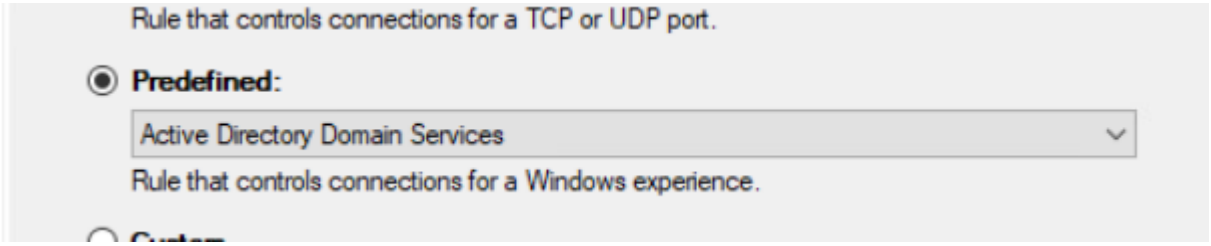


Разрешаем подключение по RDP компьютерам домена

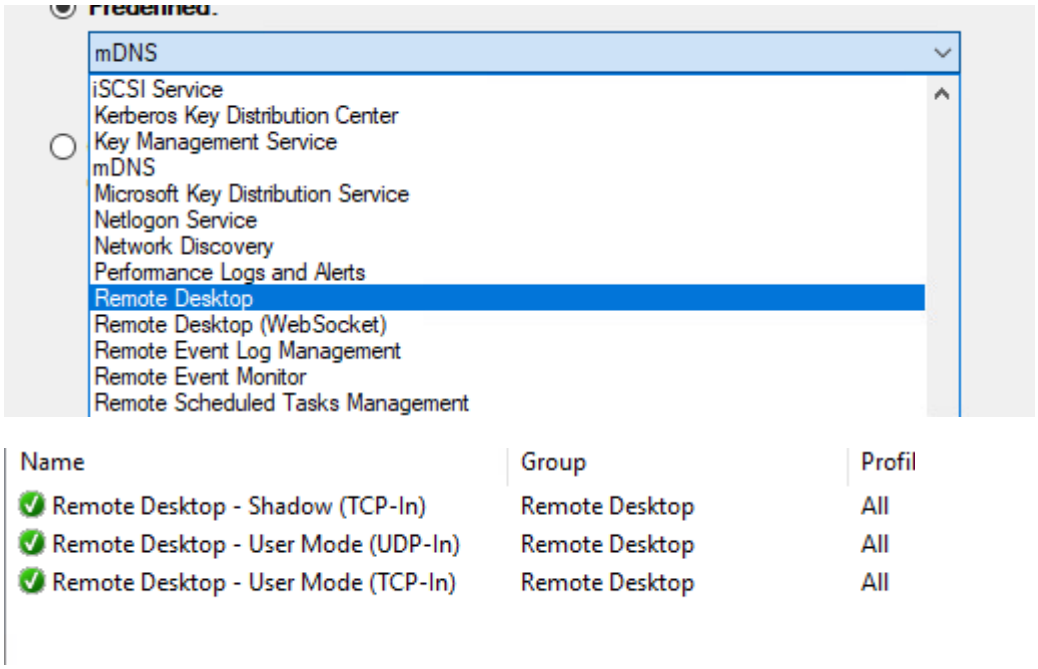
Computer Configuration > Policies > Windows Settings > Security Settings >Windows Defender Firewall and Advanced Security > Inbound Rules -> New Rule



Выбираем предопределенные (Predefined)

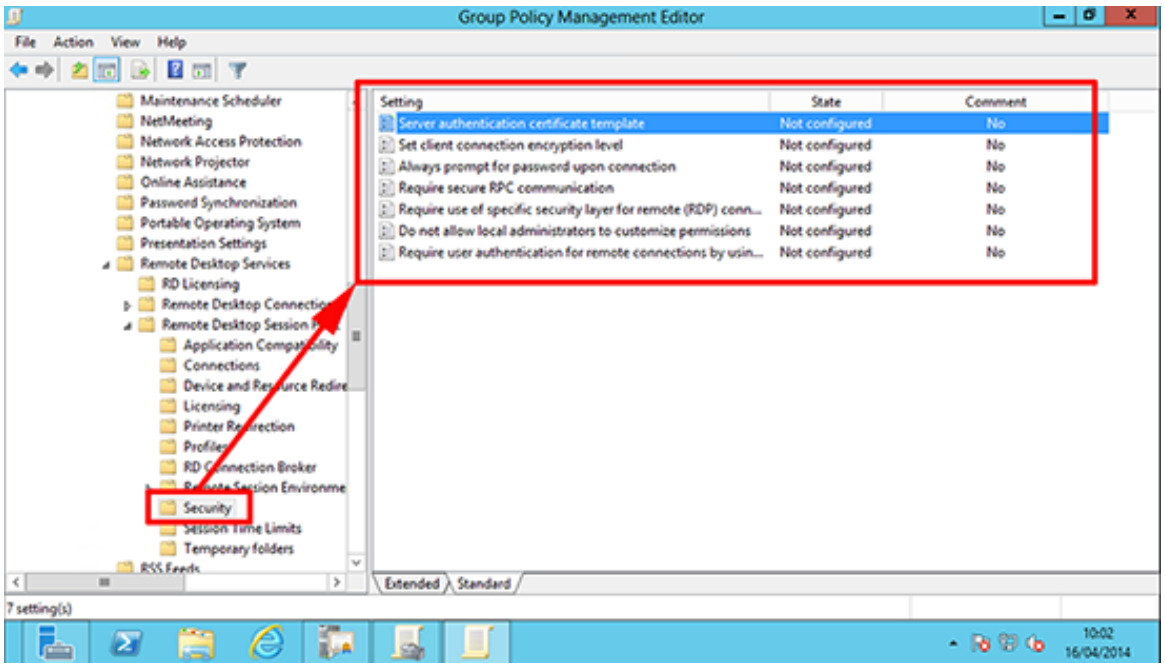


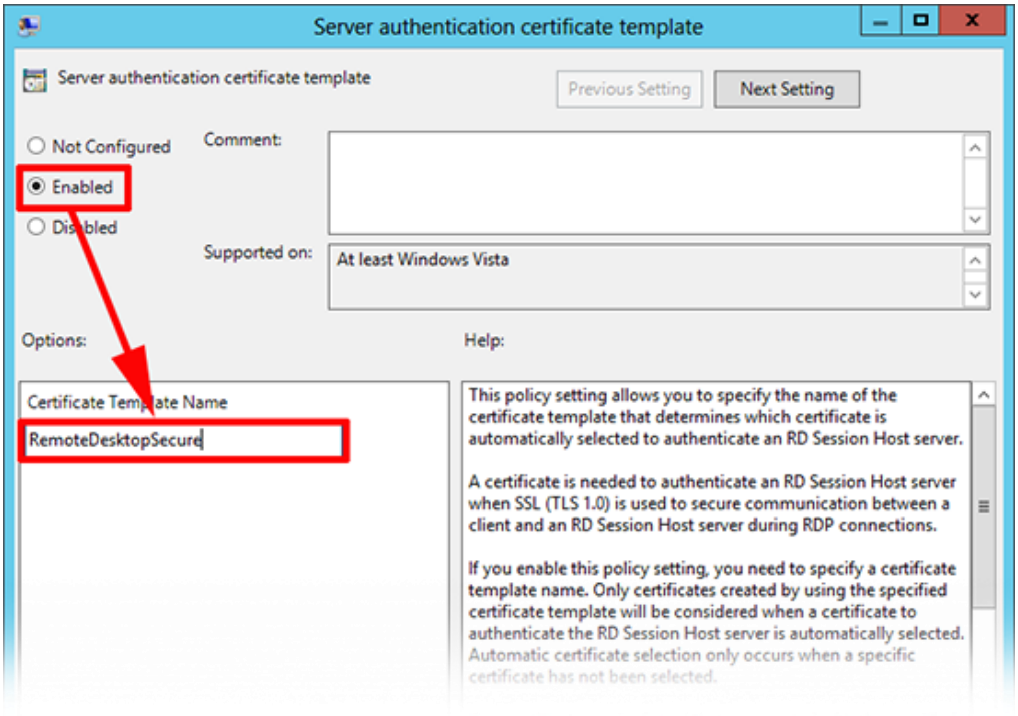
Выбираем Remote Desktop



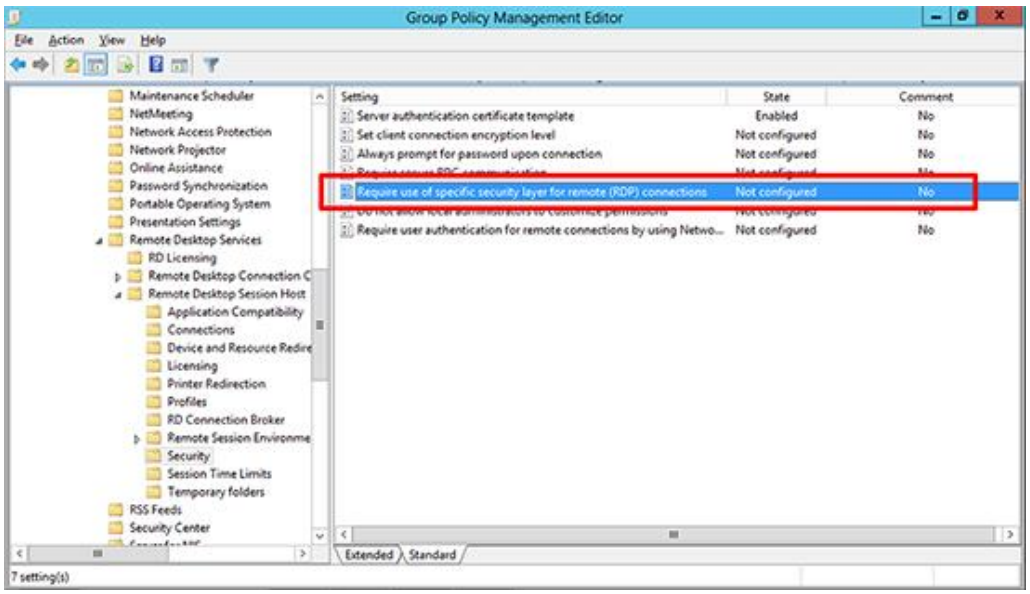
Включаем требование к использованию сертификатов

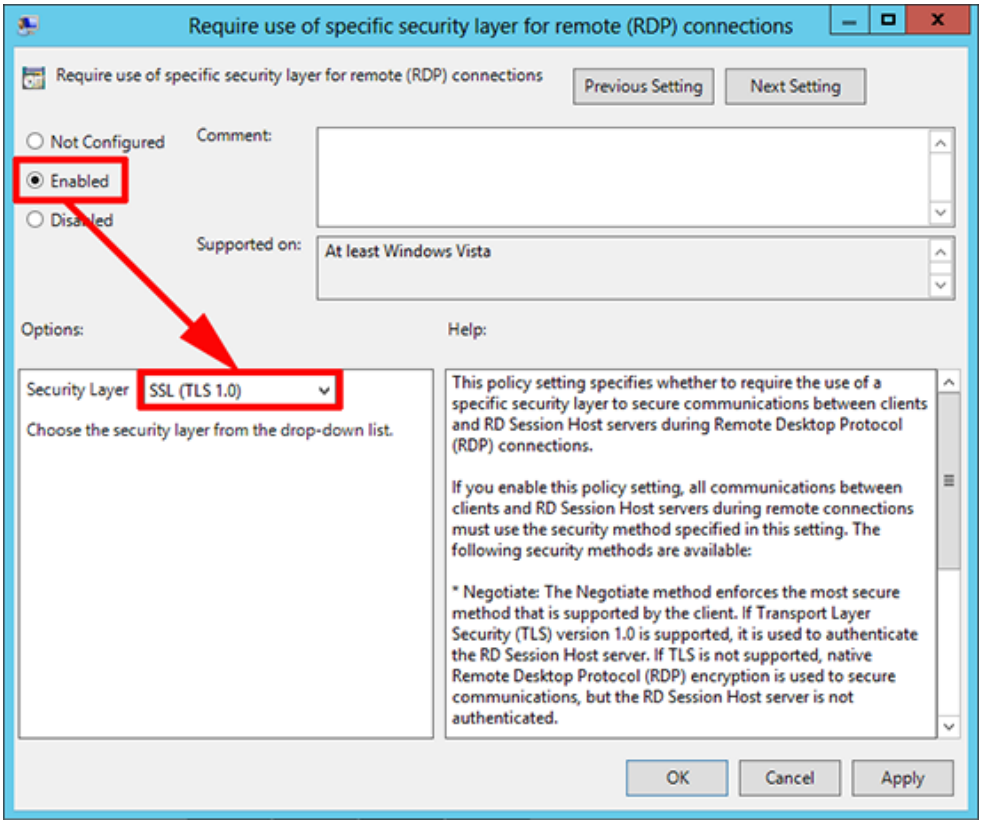
GPO на домен: Computer Configuration> Policies >Administrative Templates > Windows > Components > Remote Desktop Services >Remote Desktop Session Host > Security > Server authentication certificate template -> Enabled <Пишем имя шаблона для подключения - Template Name. В нашем случае это RDCcert>





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

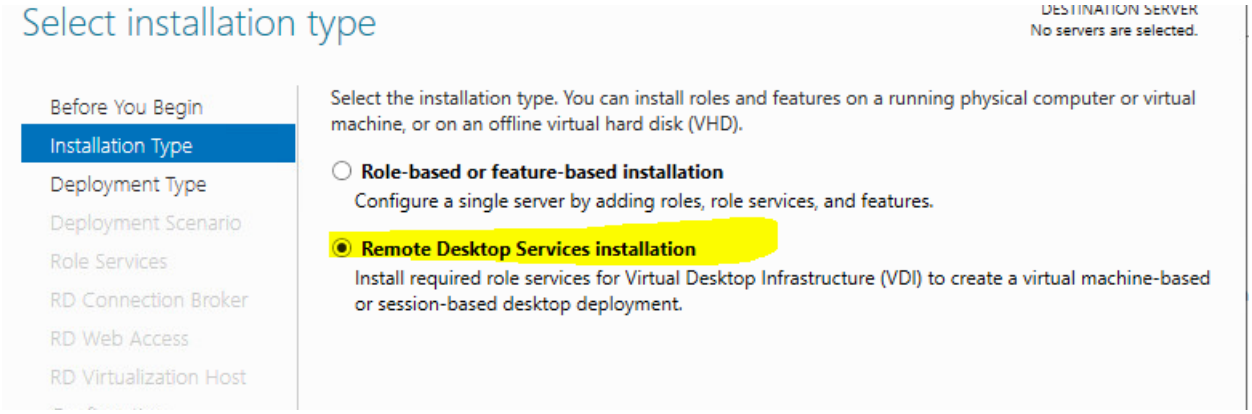
3. RDS

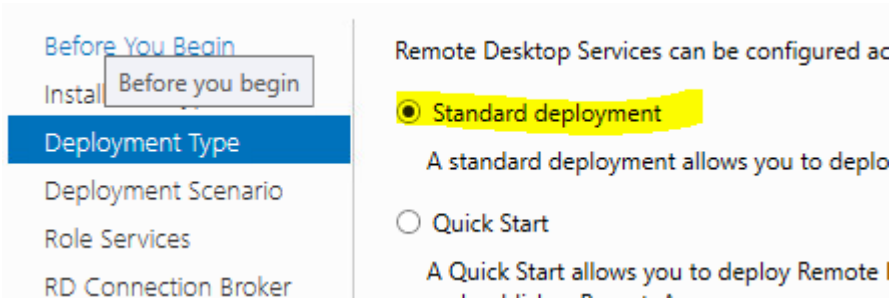
СОЗДАНИЕ RDS

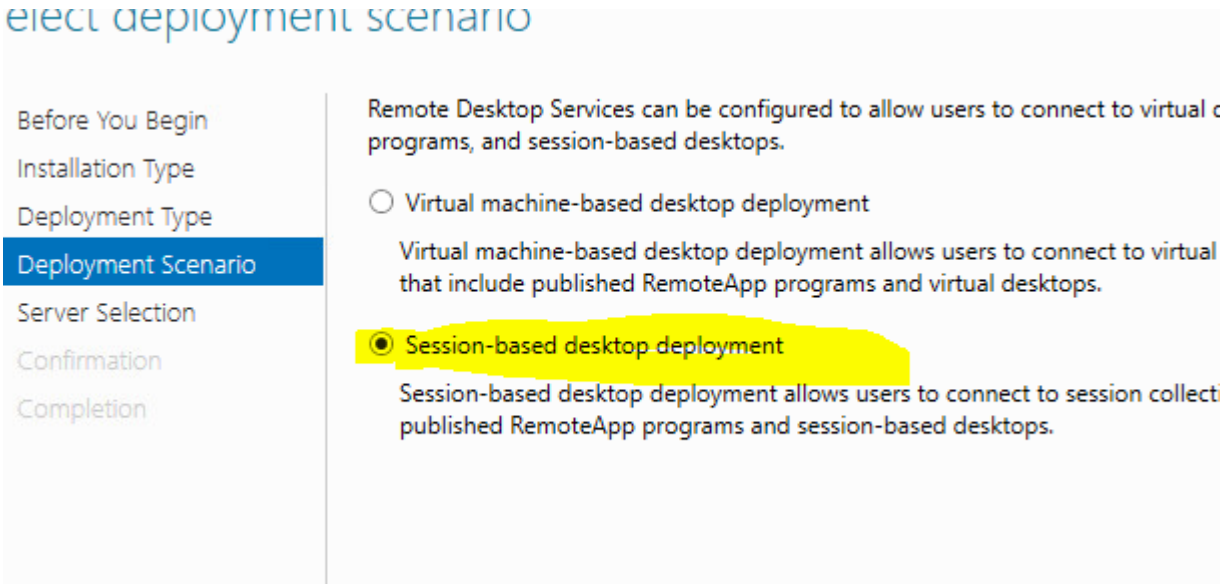
Установка ролей

Роль называется remote desktop services

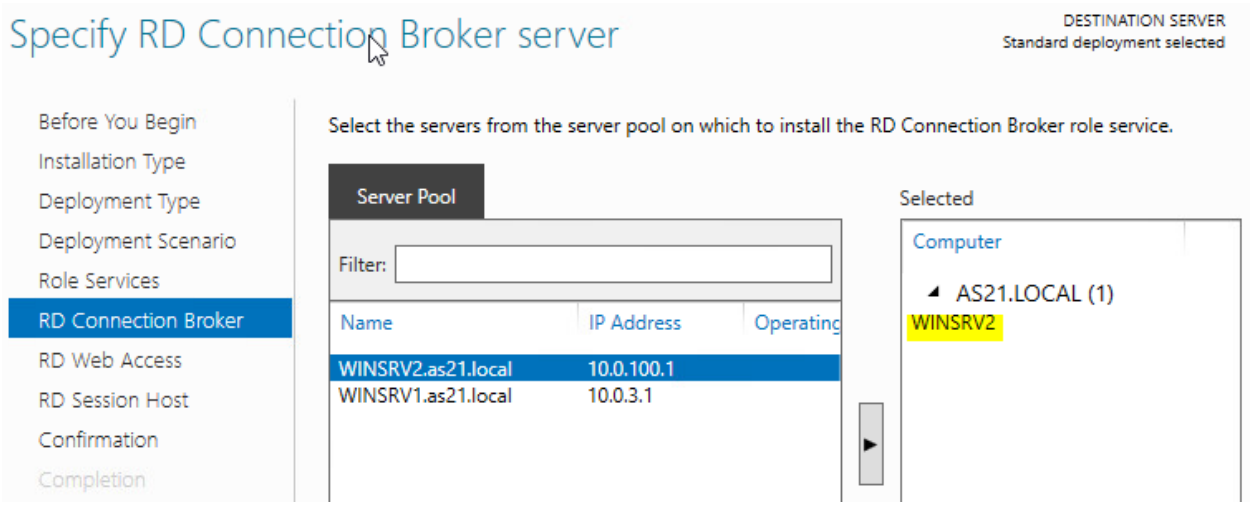
Конфигурируем в режиме Remote Desktop Services installation:







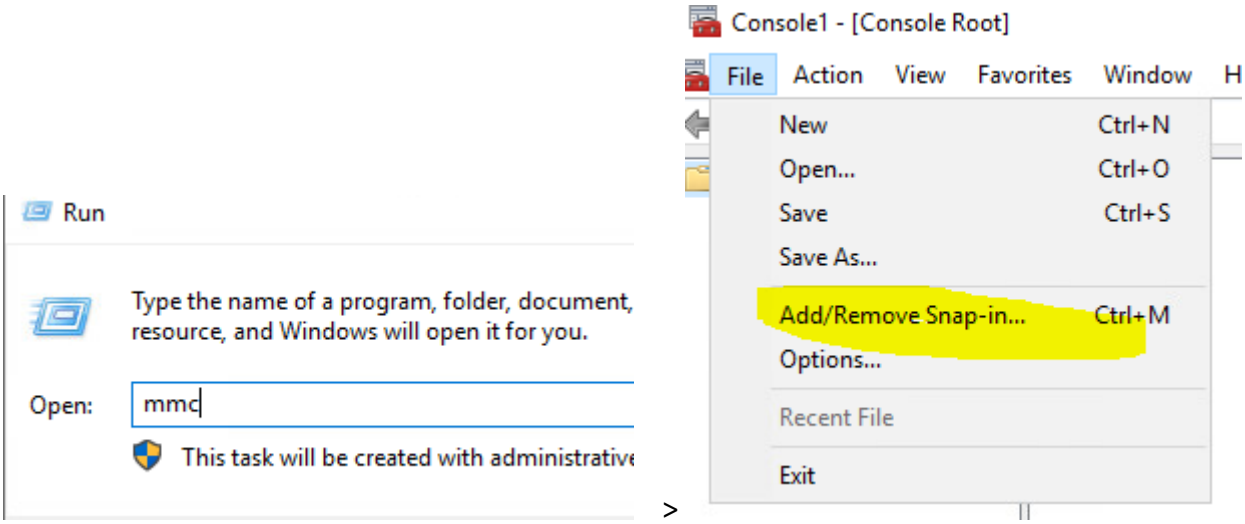
Выбираем rds для разворачивания роли - на скрине неправильно

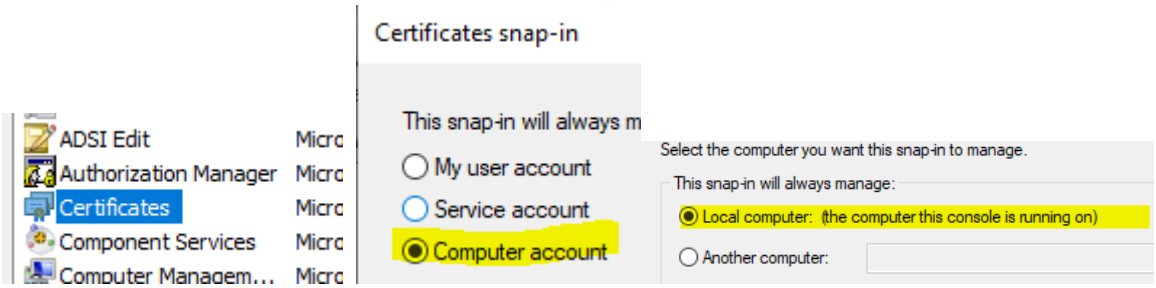


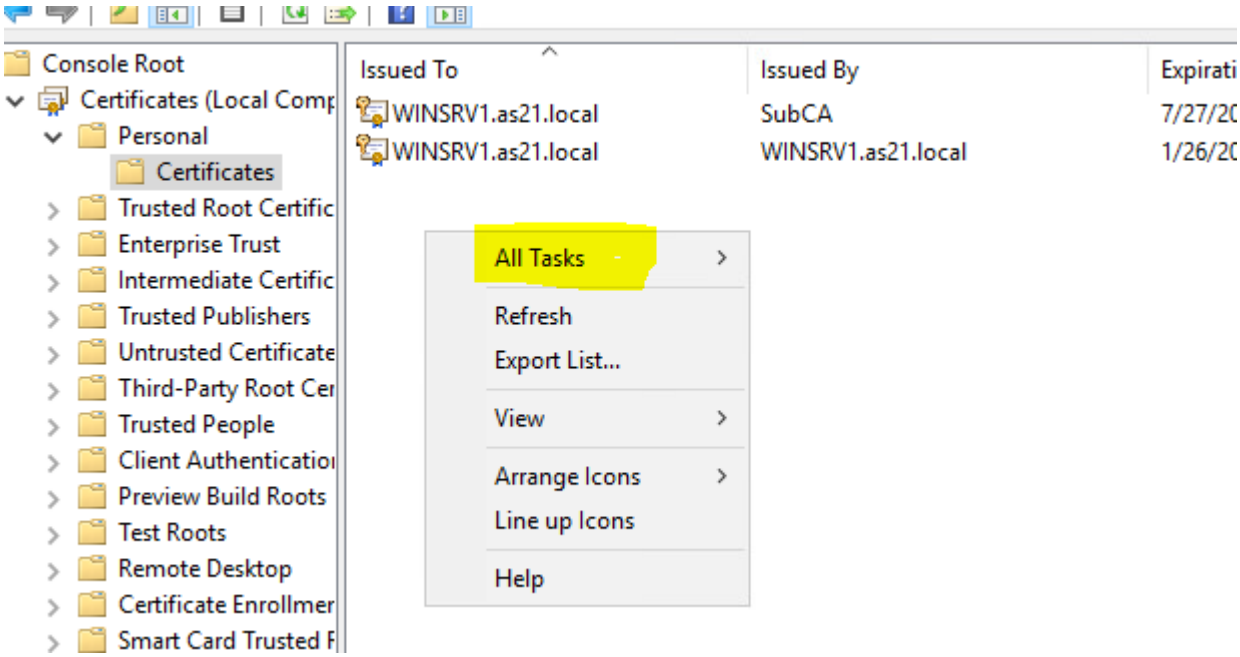
Настройка web доступа по сертификатам

Сконфигурируйте web-доступ к службам терминалов сервера.

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

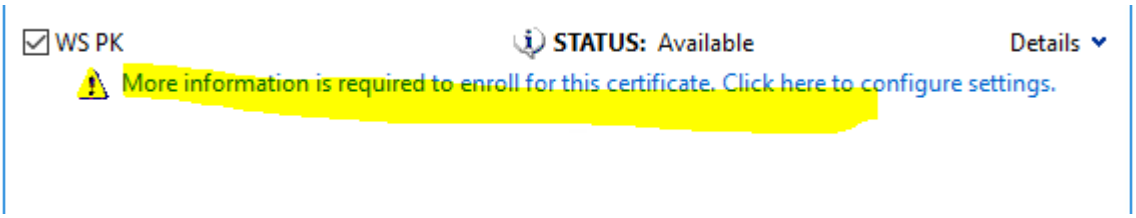






All Task > Request New Certificate

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



Сверху заводим Common Name – rds.reaskills2026.local

И

rds.rea2026.ru **и *.reaskills2026.local**

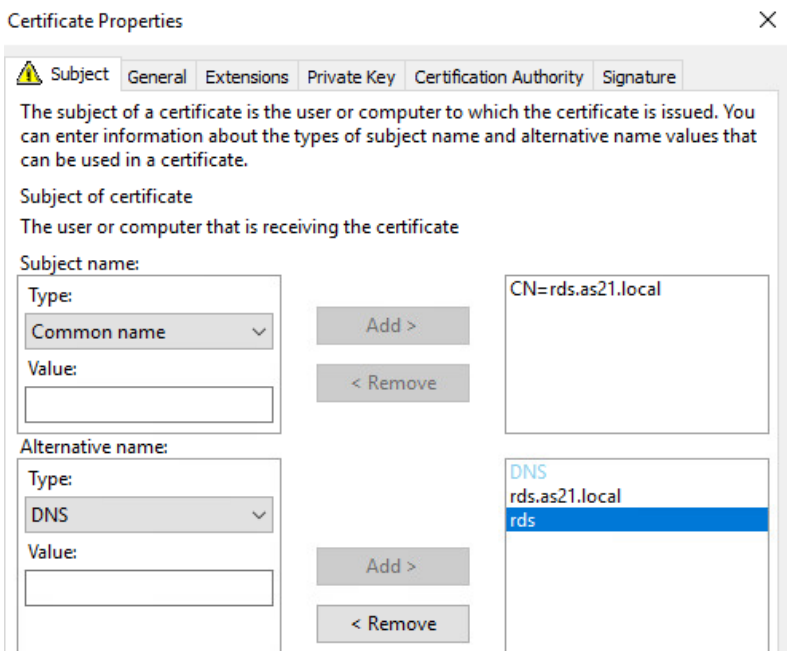
Внизу заводим DNS rds.reaskills2026.local

И

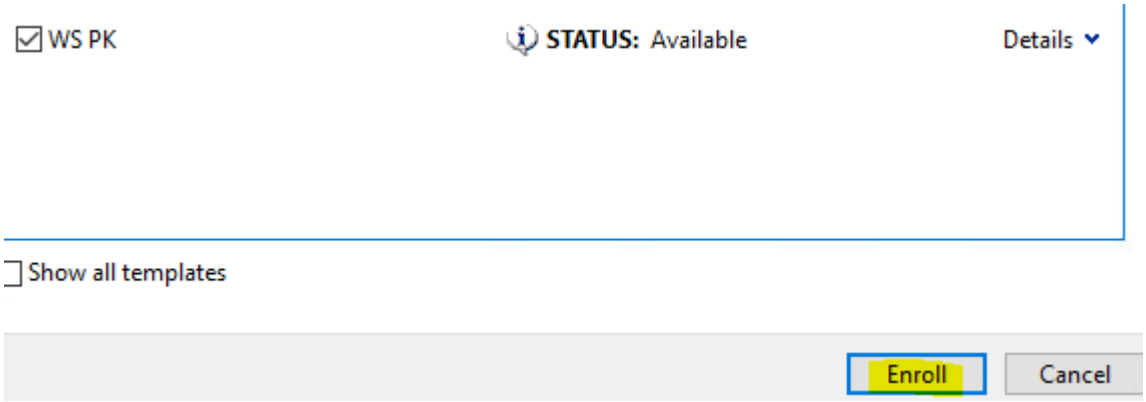
rds.rea2026.ru

И

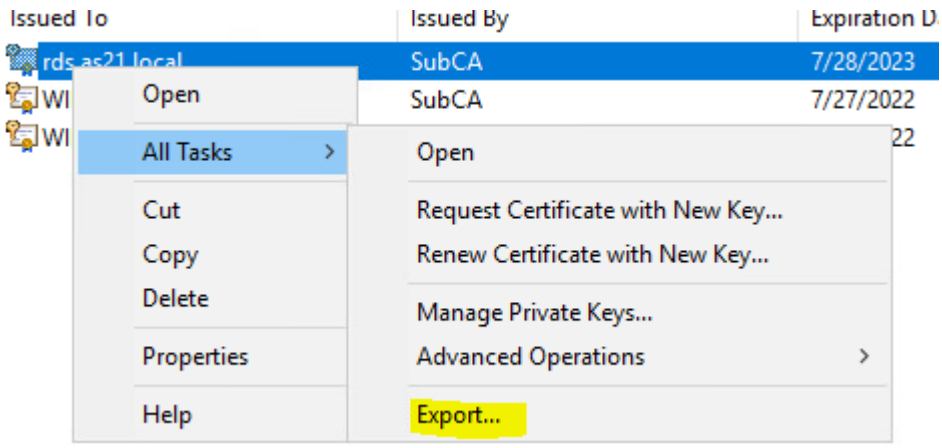
***.reaskills2026.local**



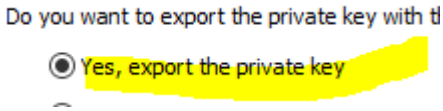
Выпускаем сертификат



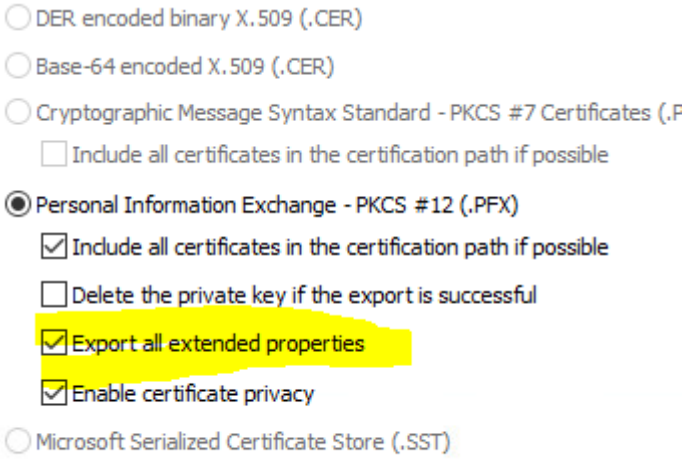
Правой кнопкой по нашему сертификату. Выбираем All Tasks > Export



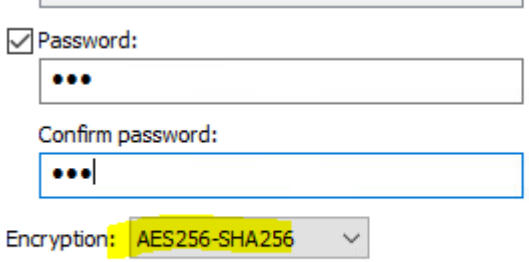
При экспорте выбираем разрешение экспорта закрытого ключа



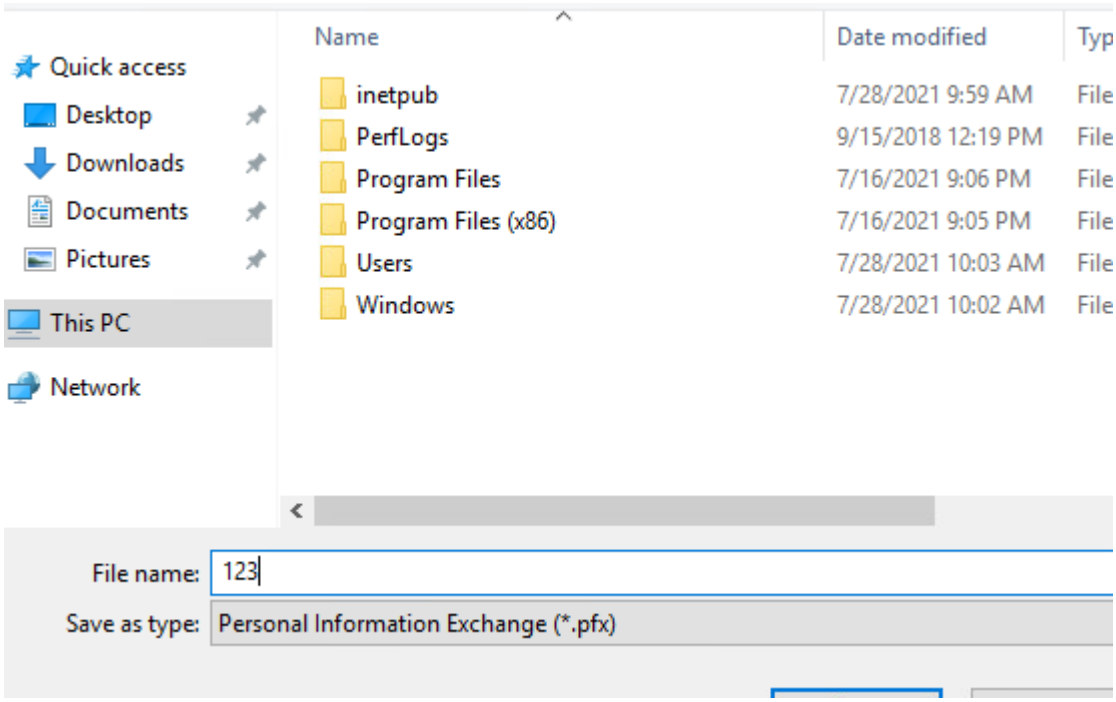
Выгружаем все параметры – Export all extended properties



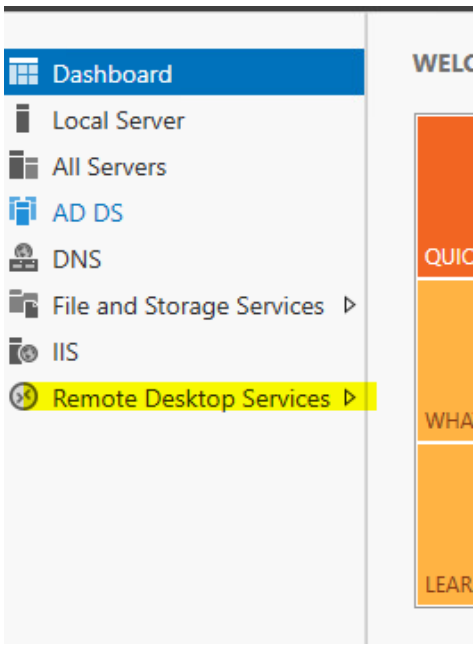
Вводим пароль, выбираем SHA256



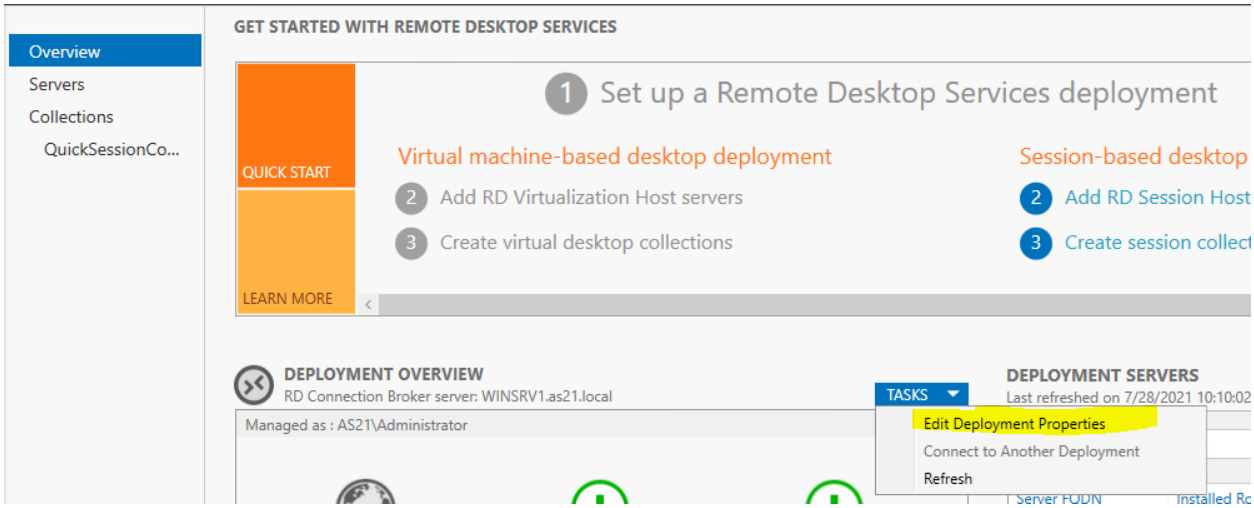
Сохраняем файл (не забываем куда)



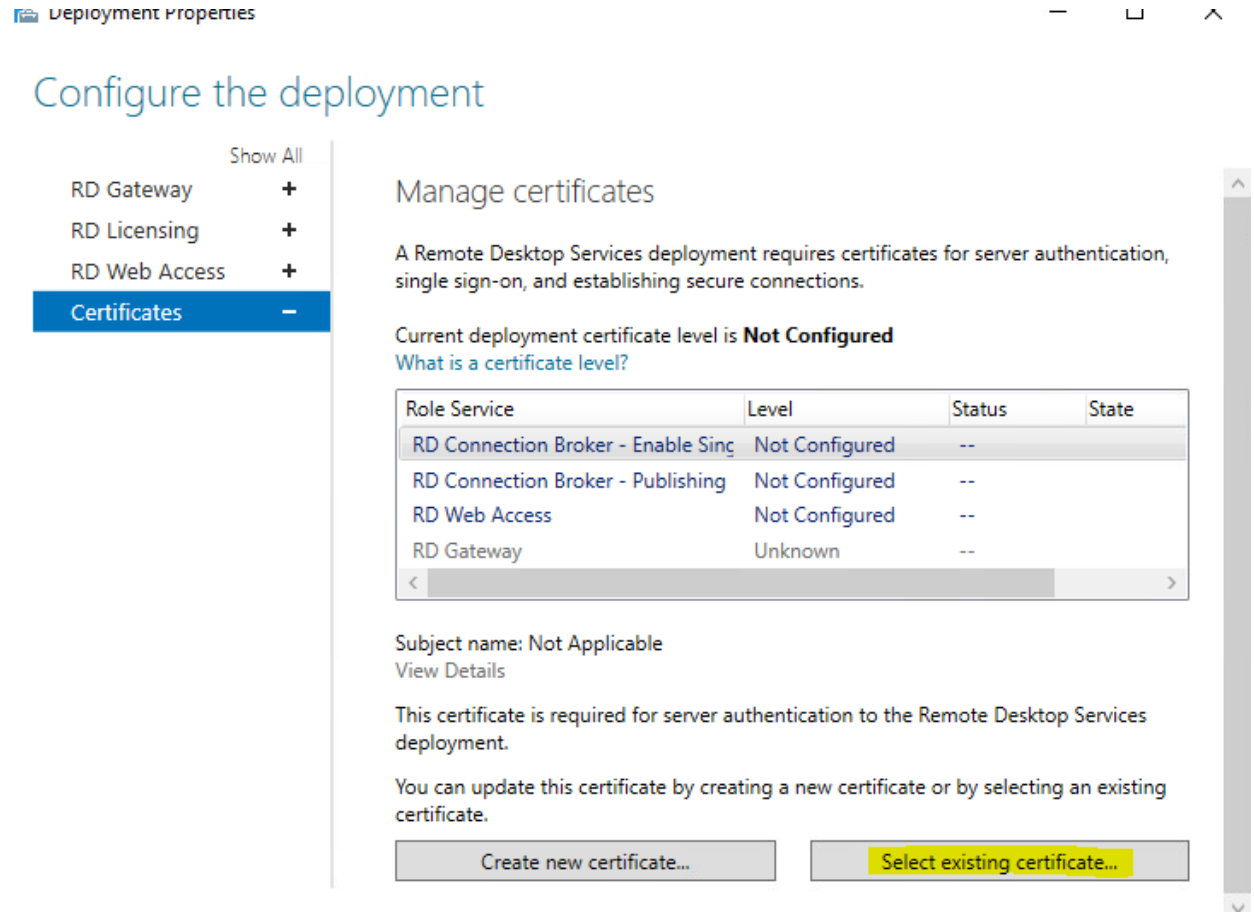
Идем в сервер менеджере в консоль RDS



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

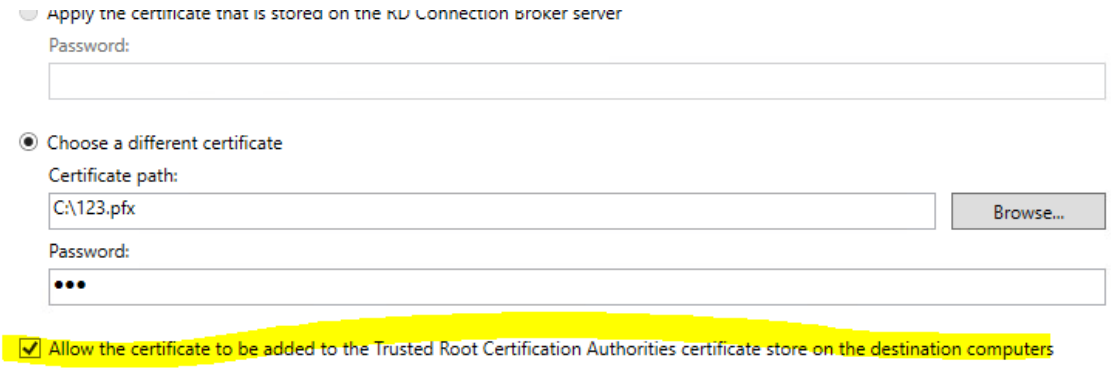


Переходим на вкладку Certificates и выбираем Select existing certificate

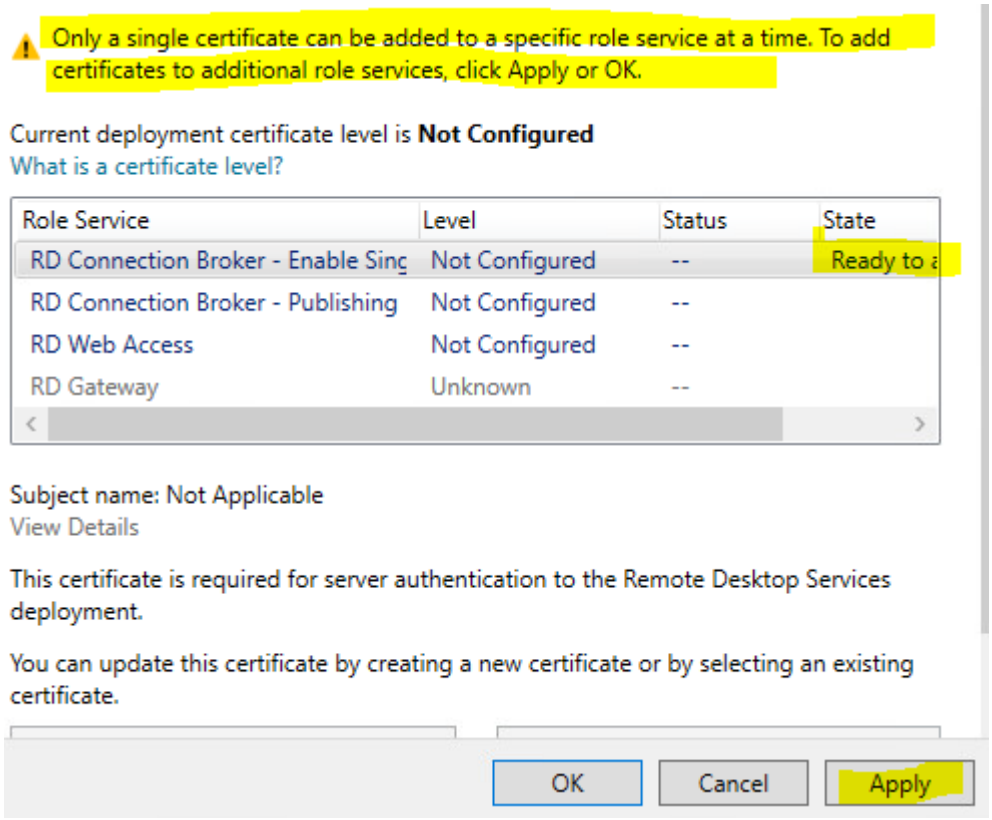


Указываем путь до предварительно сохраненного сертификата и пароль к нему.

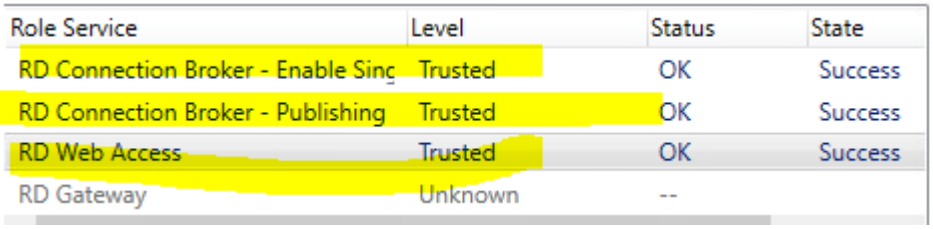
Устанавливаем Allow the certificate to be added to the Trusted Root Certification Authorities certificate store on destination computers



Должно получиться следующее. Нажимаем Apply



Повторяем для всех трех верхних ролей. Должно получиться следующее:

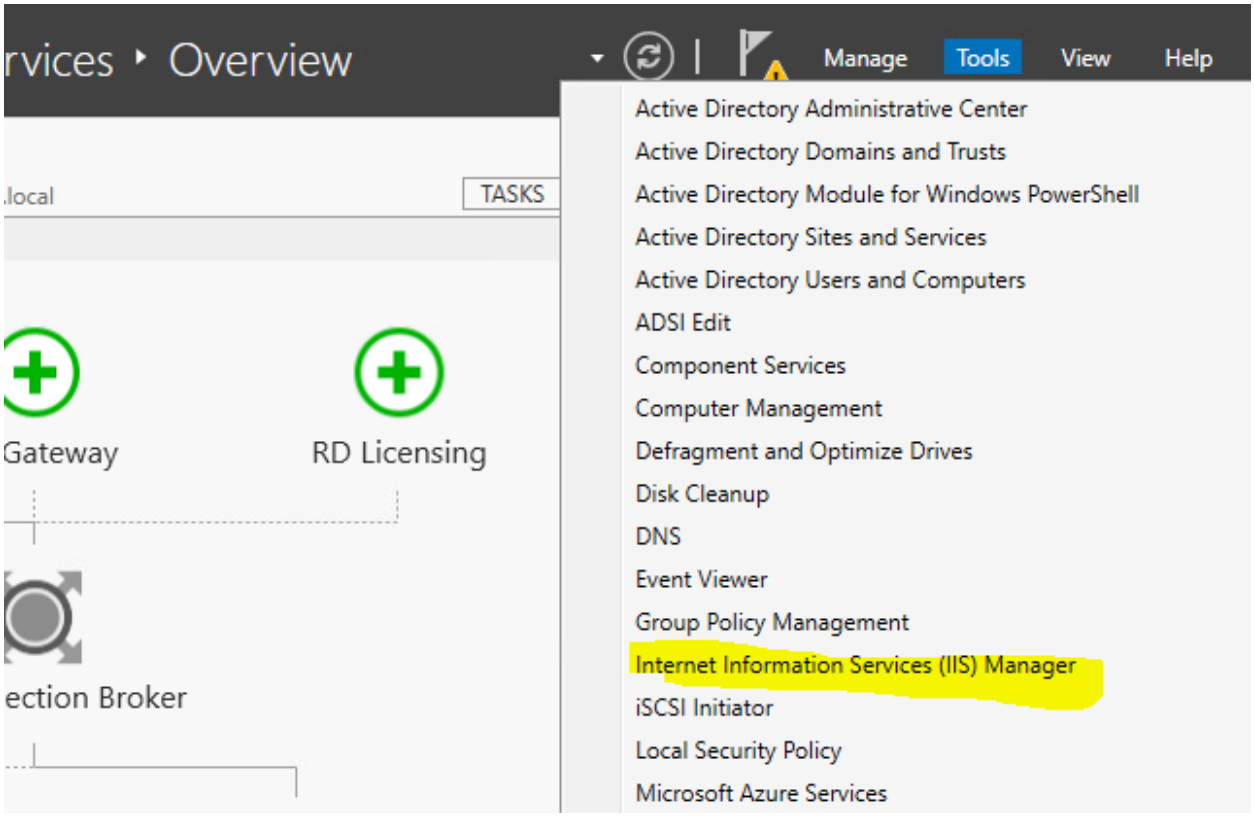


3. Web-интерфейс сервера должен быть доступен только по протоколу https по имени rds.reaskills2026.local/RDweb.

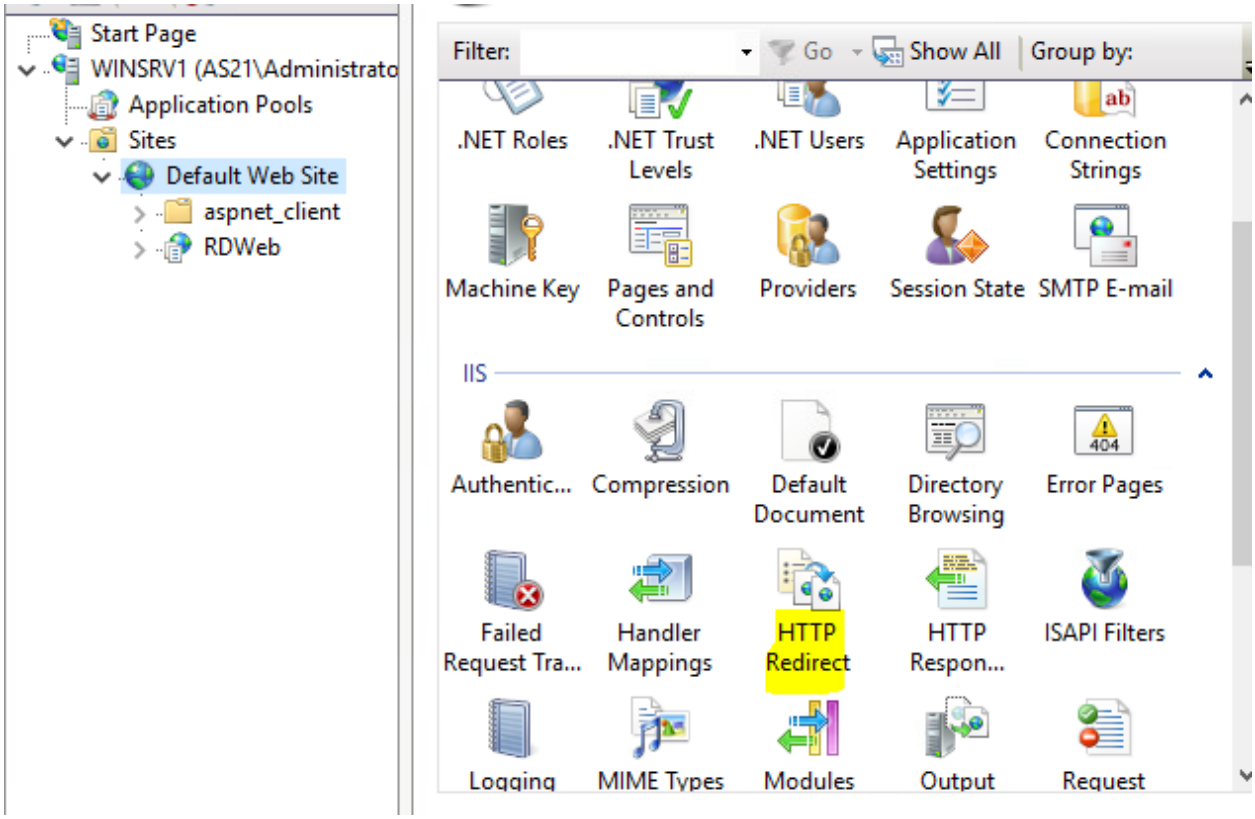
ВАЖНО!!! Убеждаемся, что в DNS есть А запись rds, которая ведет на rds.

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

Настройка IIS RDS



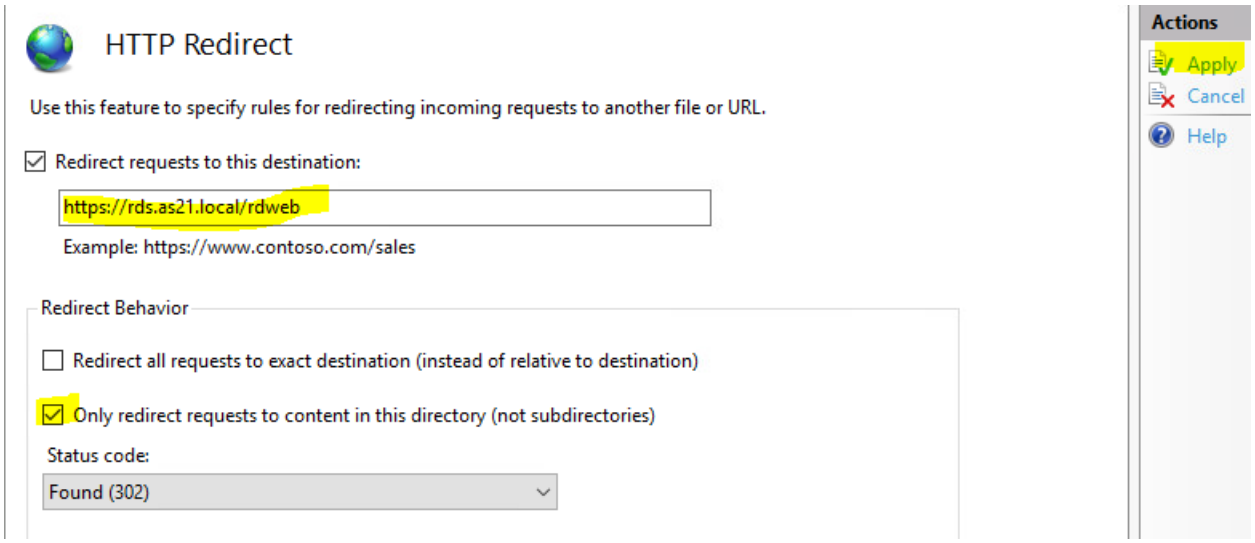
Открываем WINSRV1 > Sites > Default Web Site, выбираем HTTP Redirect



Прописываем пункт назначения переадресации https:\\rds.as21.local\RDWeb

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

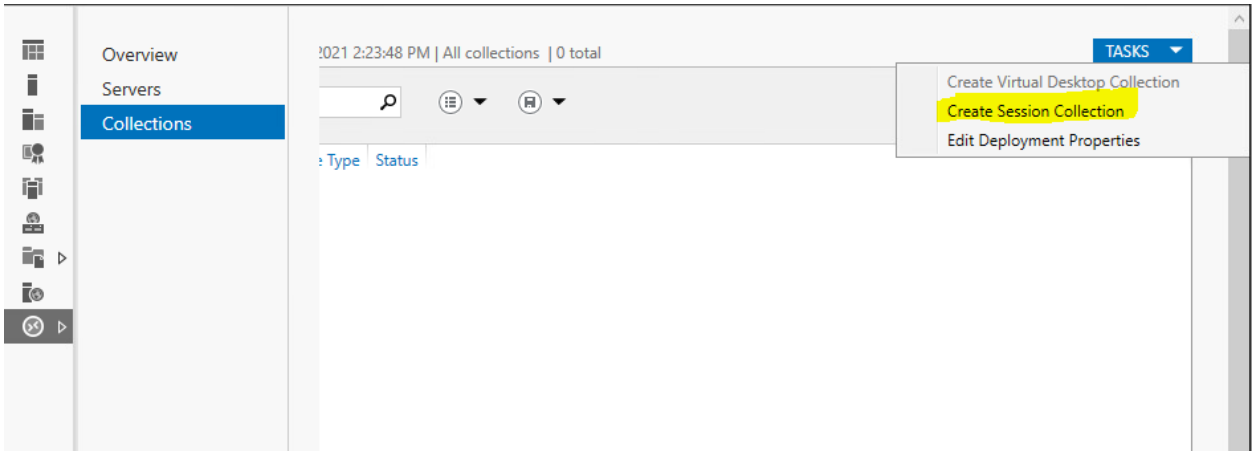
Здесь прописываем https://rds.reaskills2026.local/rdweb



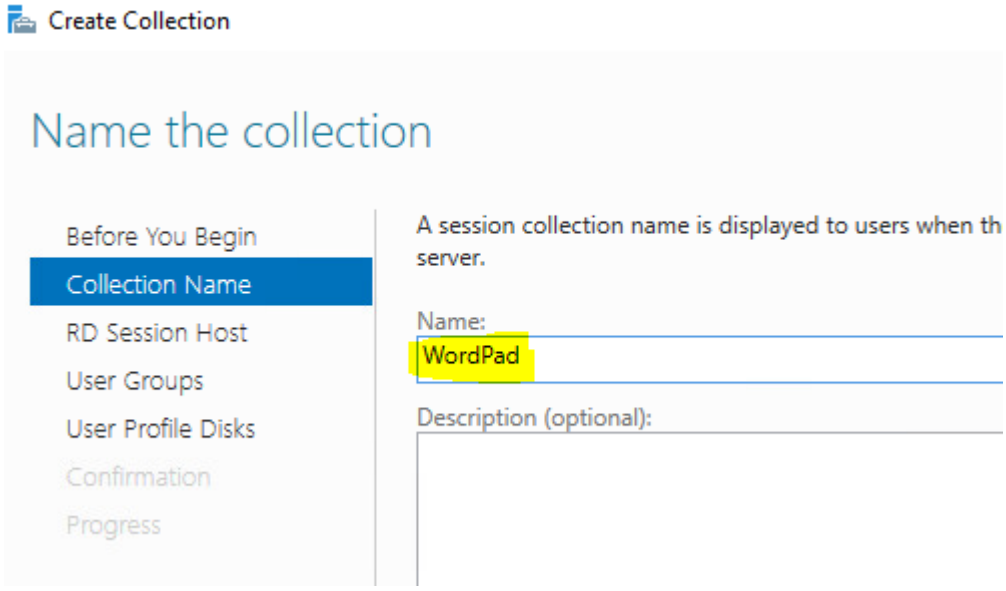
Публикация коллекции RDS

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.

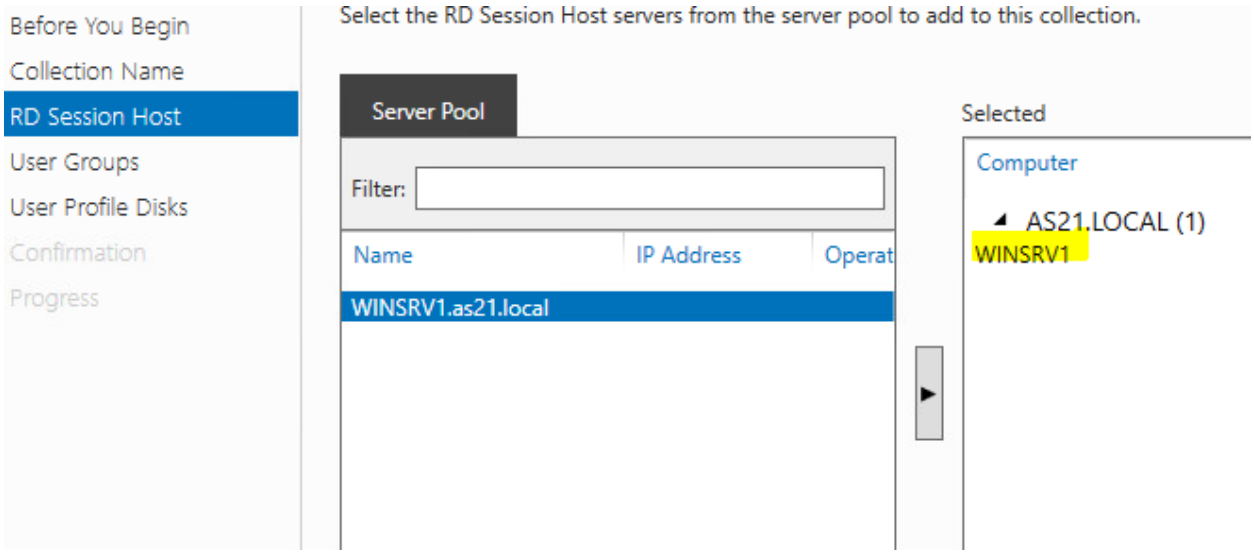
Создаем новую коллекцию



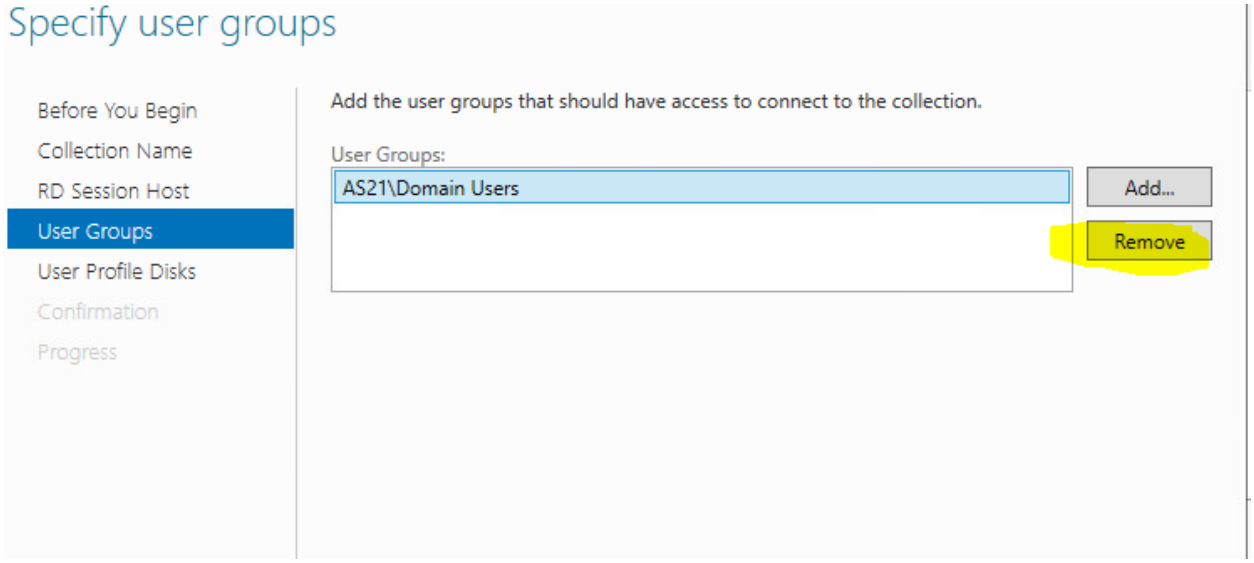
Вводим имя коллекции - пусть будет MAX



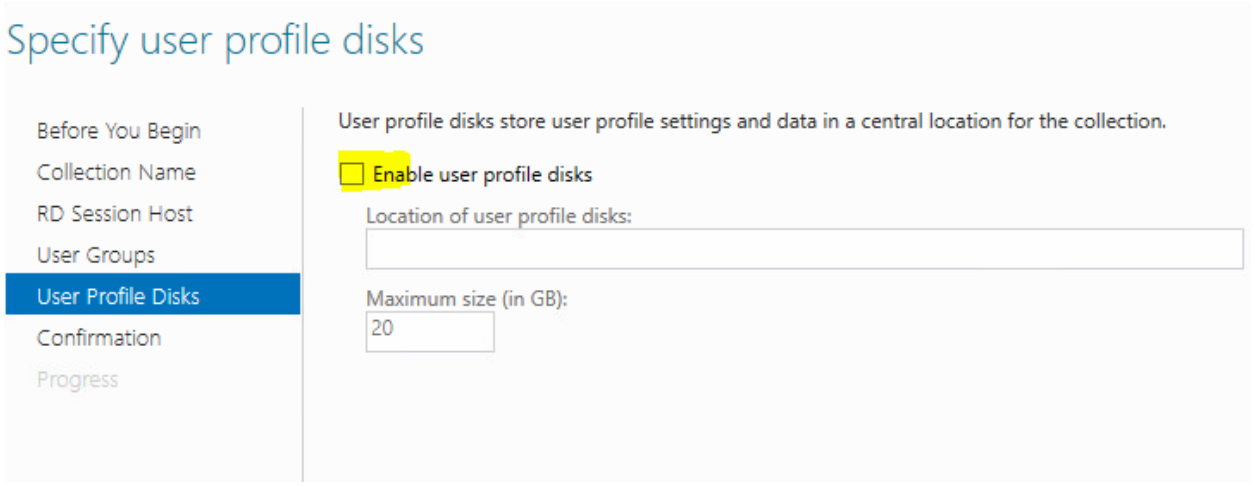
Добавляем сервер RDS как хоста коллекции - на скрине неправильно



Оставляем группу Domain Users

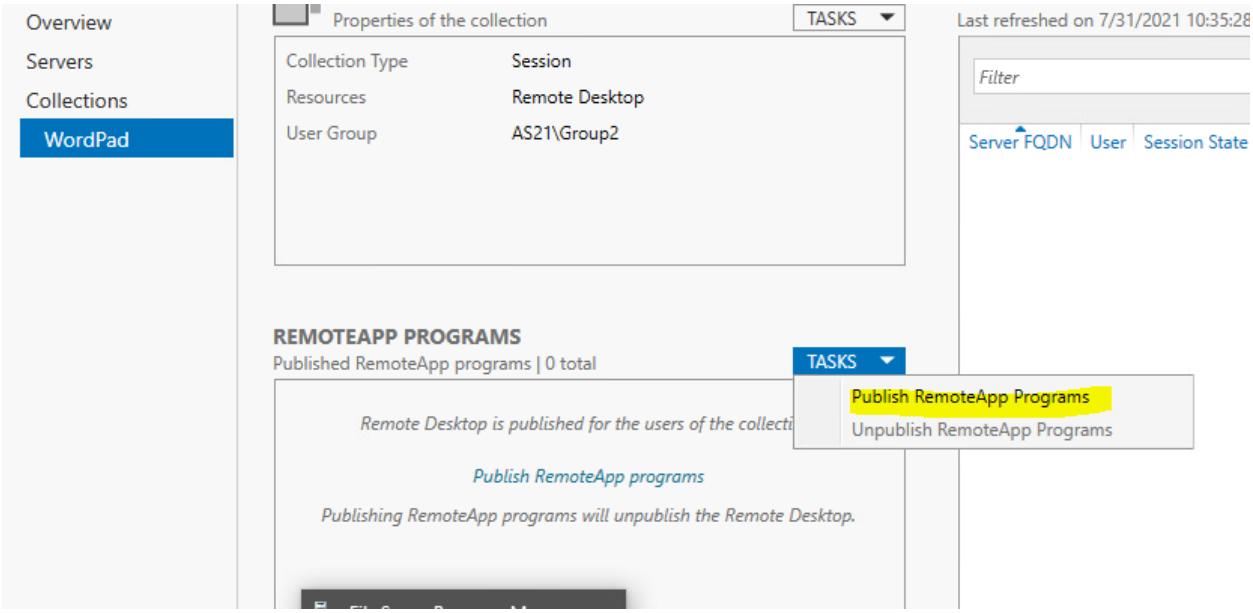


Убираем пользовательские диски профилей

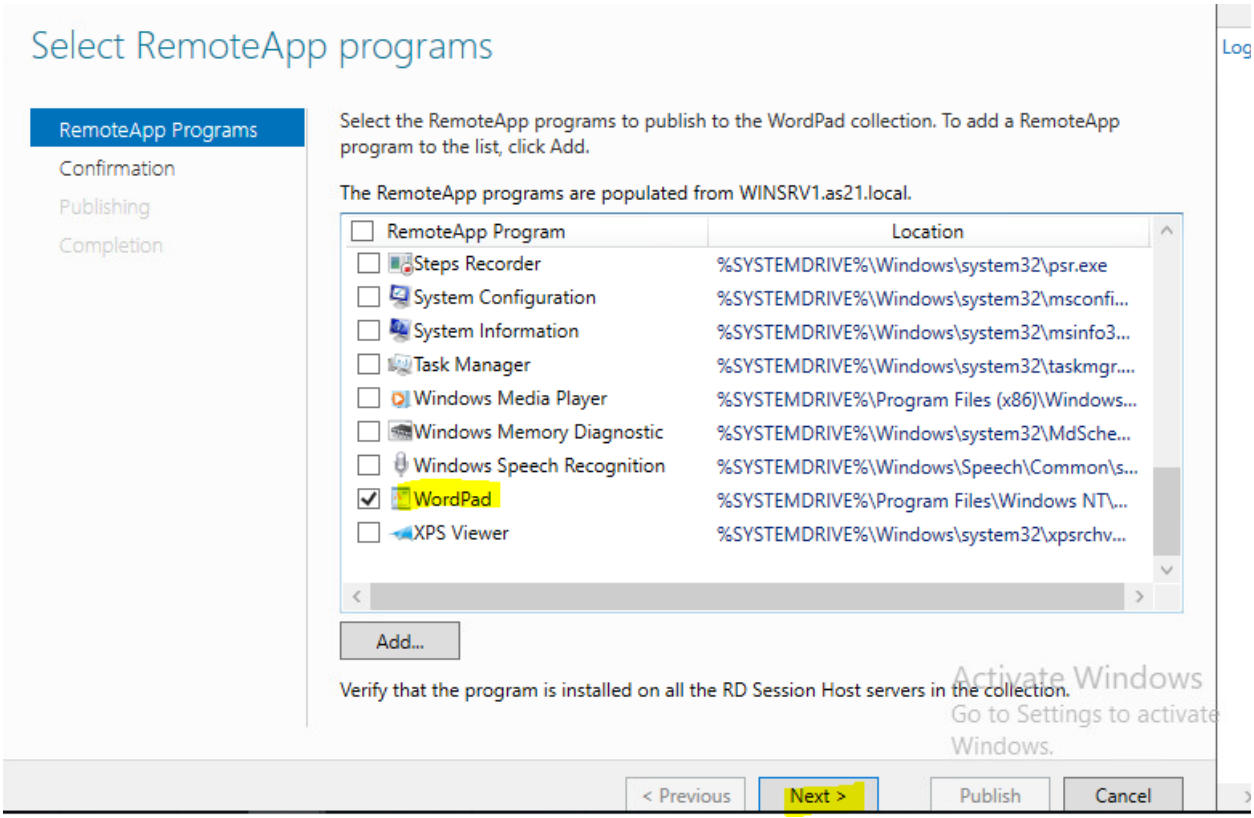


Публикация приложения RDS

Публикуем приложение



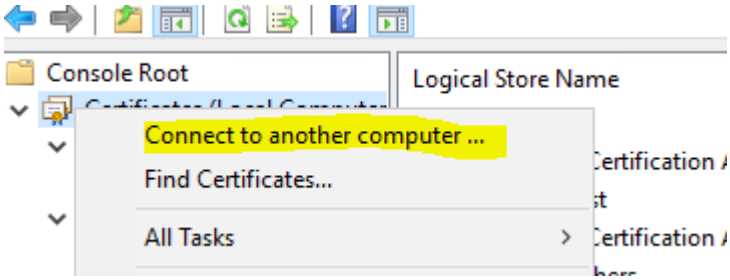
Выбираем их списка max публикуем его на RDS

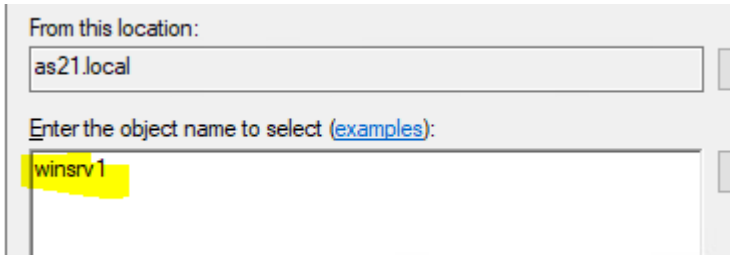


Добавление сертификата в доверенные

Убираем предупреждение при подключении

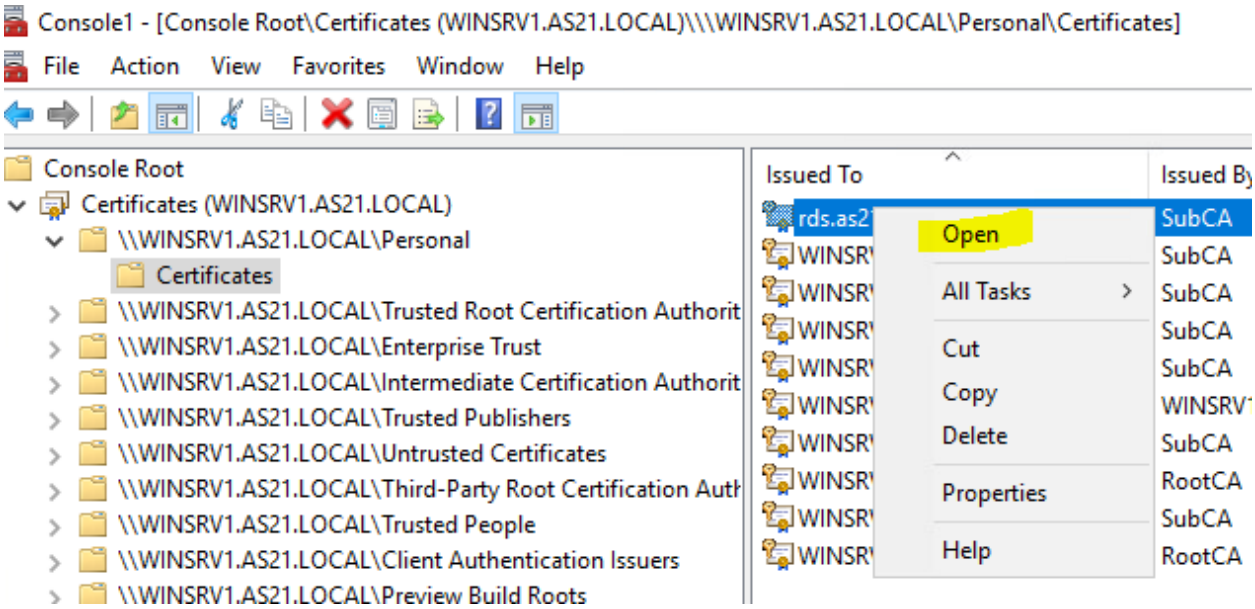
Заходим на DC. Запускаем MMC оснастку Certificates. Подключаем её к rds



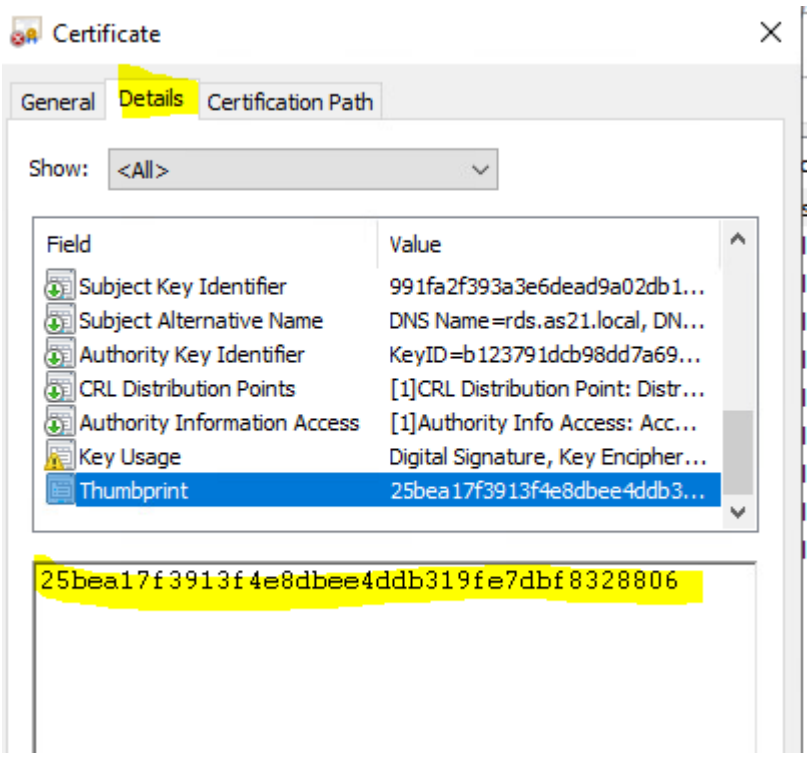


Находим выпущенный для RDS сертификат rds.reaskills2026.local

Открываем его

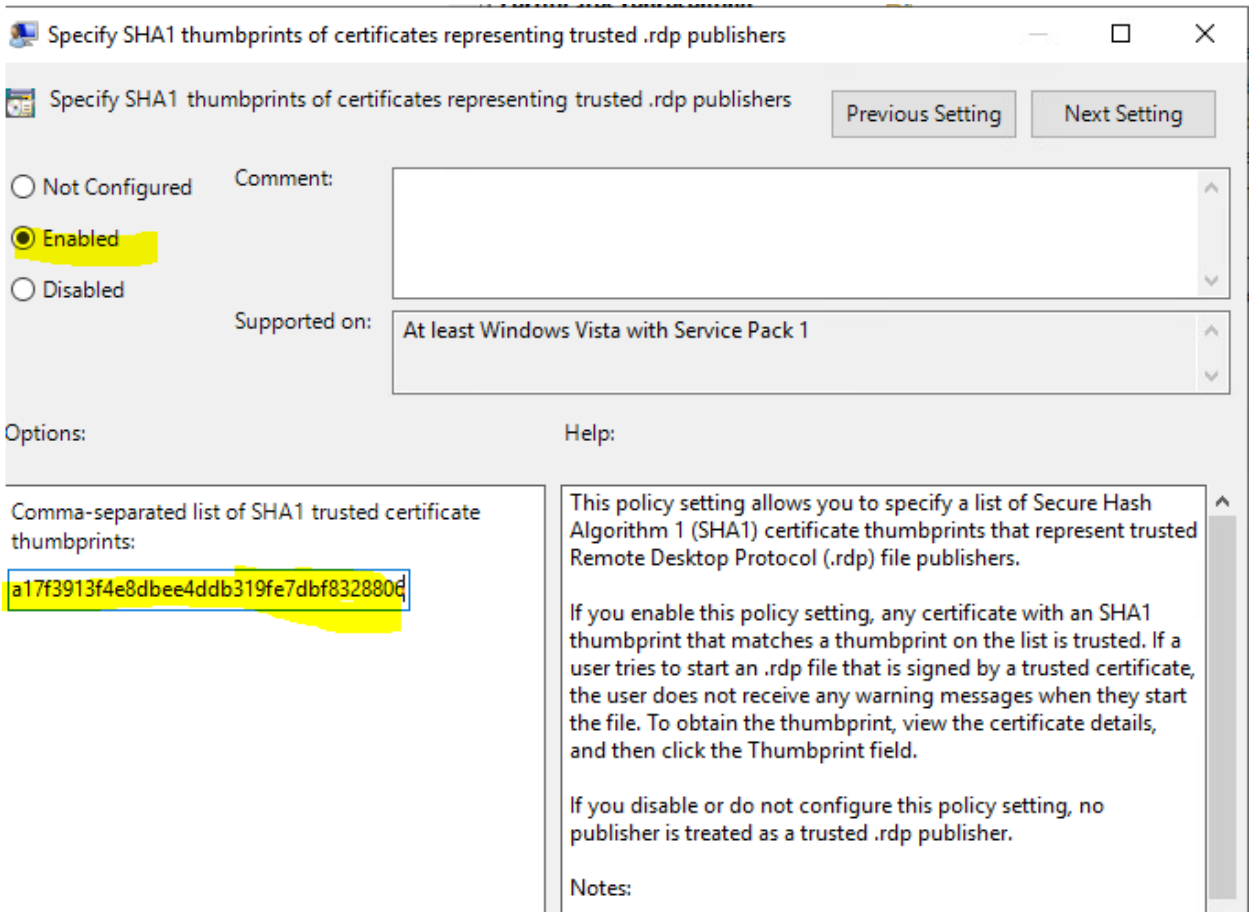


Переходим в раздел Details. Выбираем Thumbprint, где мы видим отпечаток нашего сертификата. Копируем его в буфер



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

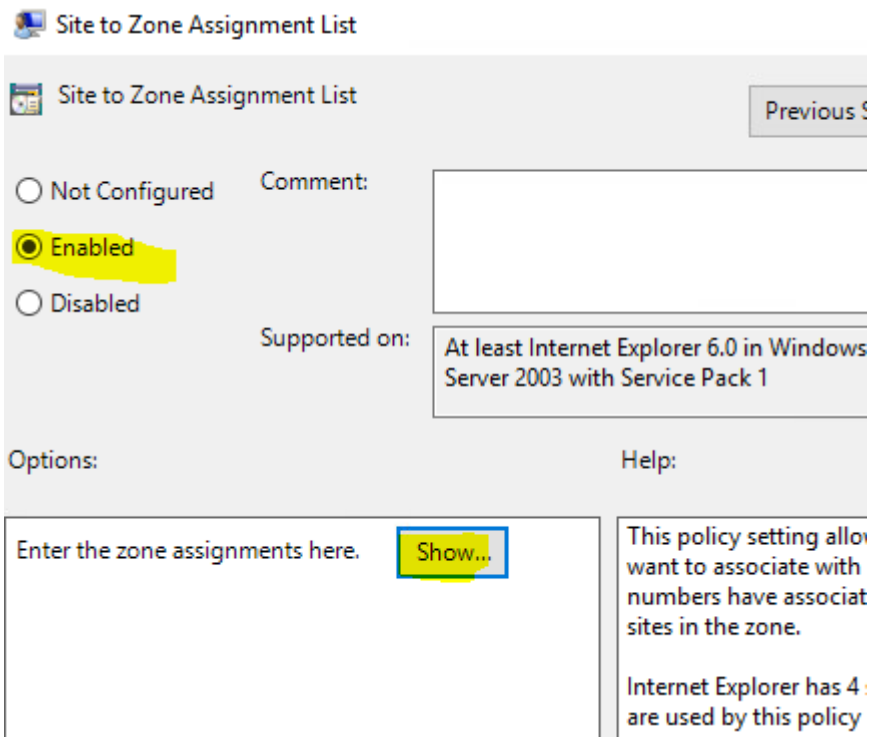
Идем в GPO, созданную на домен

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

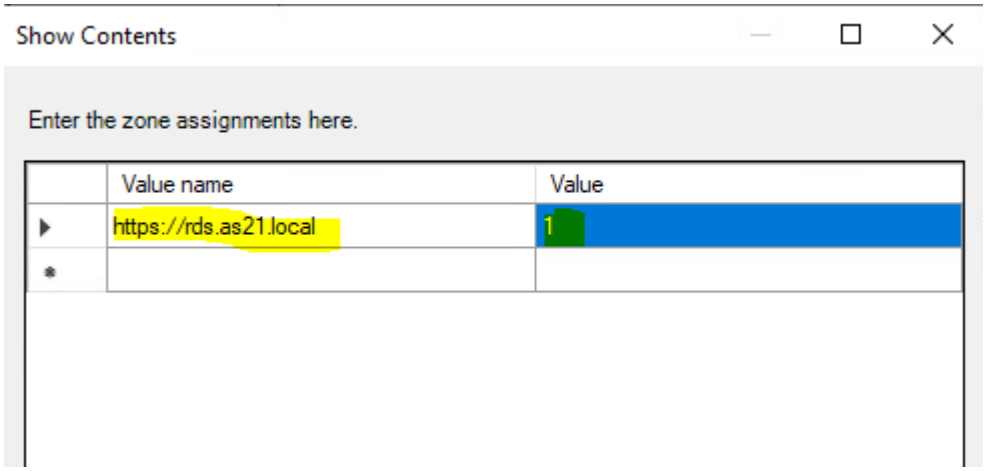
Нажимаем Show

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

В Value пишем 1



Тут имя https://rds.reaskills2026.local



Добавляем

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

В Value пишем 1