O&G Computing Services

Advanced computing infrastructure solutions

The new standard of your network & computing environments

Introduction

Objectives:

The following document will describe and detail the planning and implementation of a new computing environment for a company whose headquarters is located in Tel Aviv and whose branch is in New York.

The document will meet the needs of all departments, including remote users, and will ensure efficient and secure activity.

In addition, this document will be able to guide the staff at the New York branch for implementation, operation and recovery in a crisis situation.

Scope:

The document will focus on the physical and virtual computing infrastructure of the company and not beyond that.

Background:

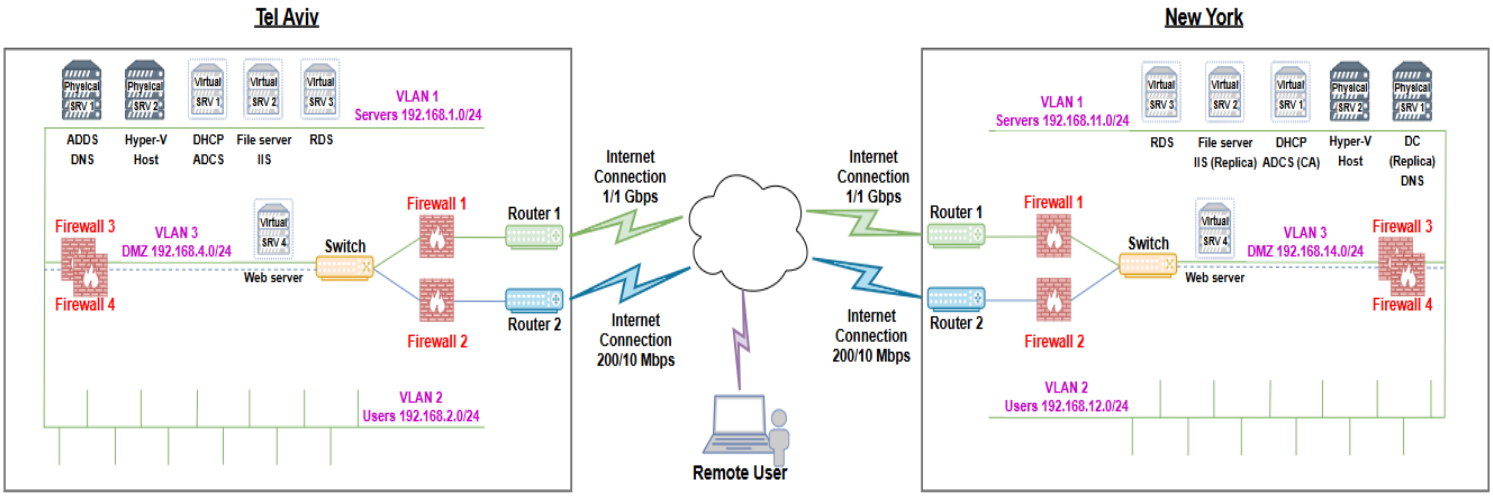
The company that began its journey in Haifa is currently moving to Tel Aviv to the new high-tech complex and establishing its new headquarters there.

Following the move, the company directors decided to invest in a modern, upgraded, robust and more secure infrastructure and computing environment that would provide good conditions for the needs of the expanding departments and offices, the remote users who would be able to work from anywhere and better communication with the branch in New York.

The solution for the task will include topics like: data centers, network topology, ADDS, DNS, DHCP, VPN, file services, ISS (Intranet Portal), RDS (Administration Server) and ADCS.

Implementation

1. Network Topology:

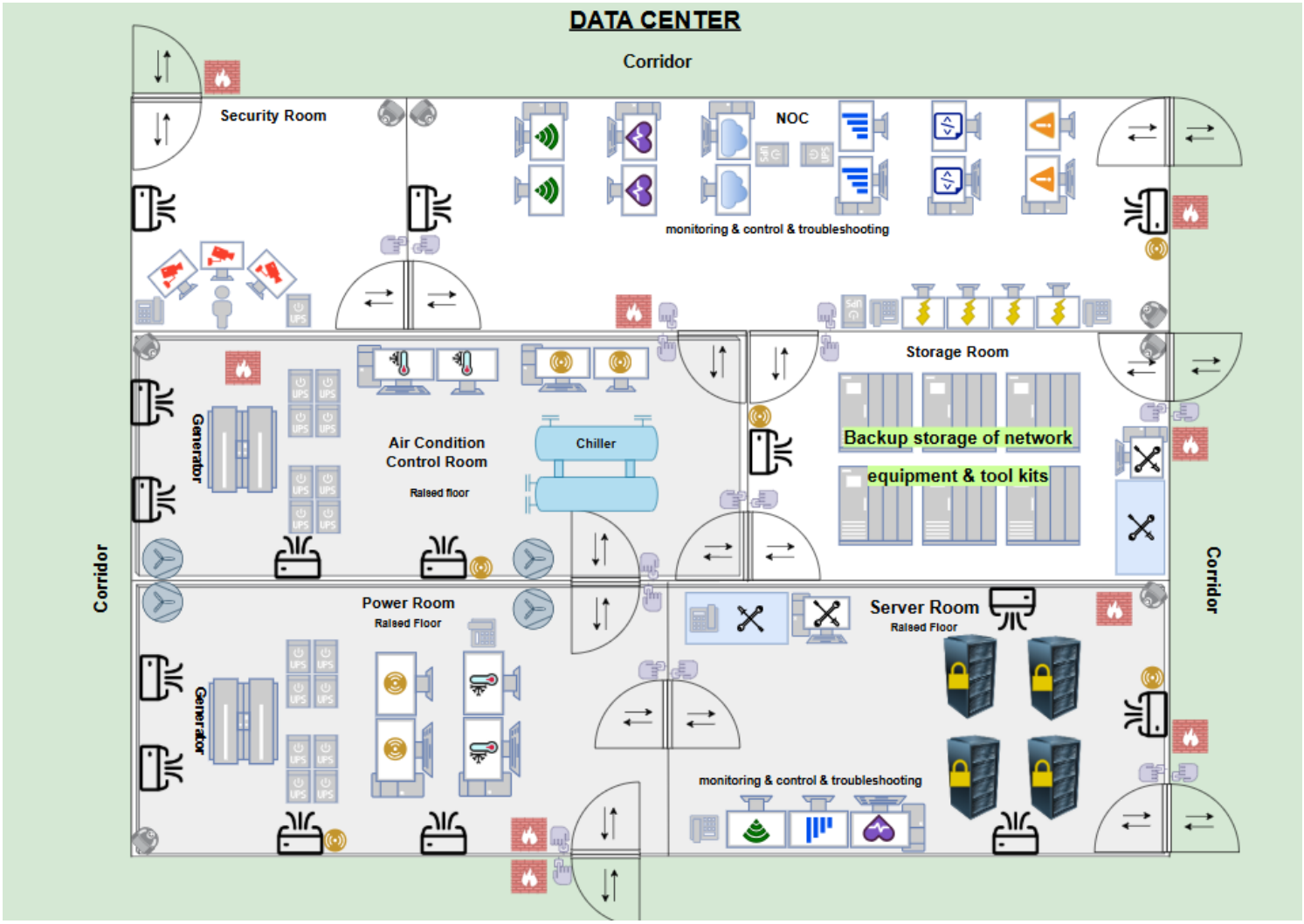


Tel Aviv:

Physical Server 1	ADDS + DNS	ensuring high availability and reliability for core services.
Physical Server 2	Hyper-V host	Virtualizes non-core roles to optimize resource usage while maintaining flexibility for future scaling or migration.
Virtual Server 1	DHCP + ADCS	grouped because they share similar backend requirements.
Virtual Server 2	File Server + IIS	grouped because they primarily serve internal needs.
Virtual Server 3	RDS	isolated to maintain performance and handle remote user access.
Virtual Server 4	Web Server	for enhanced security, isolating public-facing services from internal systems.

New York: Replicated structure to ensure redundancy, high availability, disaster recovery for critical services and a similar user experience like Tel Aviv site.

Data Center:



Door

Access Control

Hidden Camera

Fire Extinguisher

CCTV Control

Air Conditioner

Telephone

UPS Unit

Smoke & Humidity Detectors

Generator

Ventilation system

Temperature Control

Smoke & Humidity Control

Liquid-based cooling system

Testing Station

Working Table

Shelves & cabinets

Locked Rack

Data Center Layout:

- Security Room – critical for controlling access and monitoring the overall environment. Includes access control, CCTV, emergency communication etc.

- NOC Room – monitoring and managing the data center's network, servers, and infrastructure. Includes stations for tracking systems health, traffic, alerts etc.

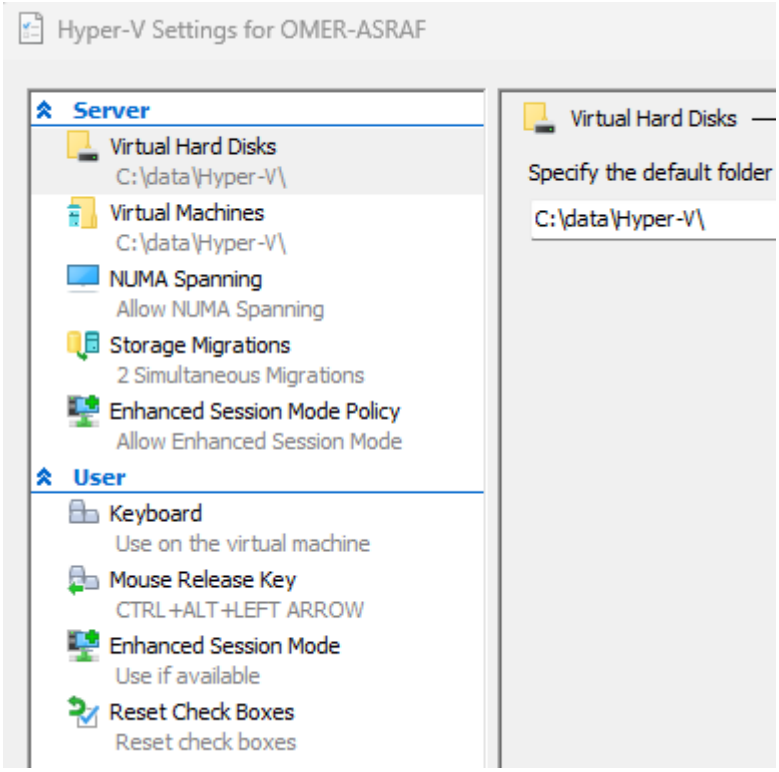
- Storage Room – dedicated to storing equipment, spare parts, and other essential items required for maintenance and repairs.

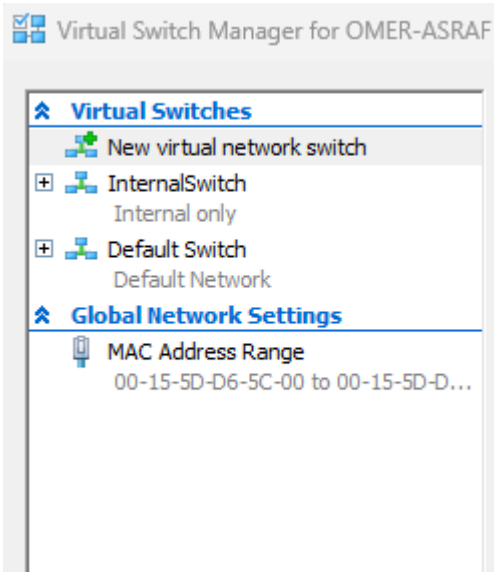
- AC Control Room – crucial for housing equipment and systems that manage the temperature, airflow, and humidity of the facility. Includes cooling units, humidity control, airflow management, power supply backup etc.

- Server Room – heart of the data center, housing servers, networking devices, and other critical IT infrastructure. Includes server racks, network devices, environmental sensors, raised floor etc.

- Power Room – (Connects to Israel Electricity Company) responsible for providing reliable and uninterrupted power to all equipment, ensuring continuous operation even during power outages or fluctuations. Includes primary power connection, power supply backup, switchgear, environmental sensors etc.

2. Hyper-V configuration:

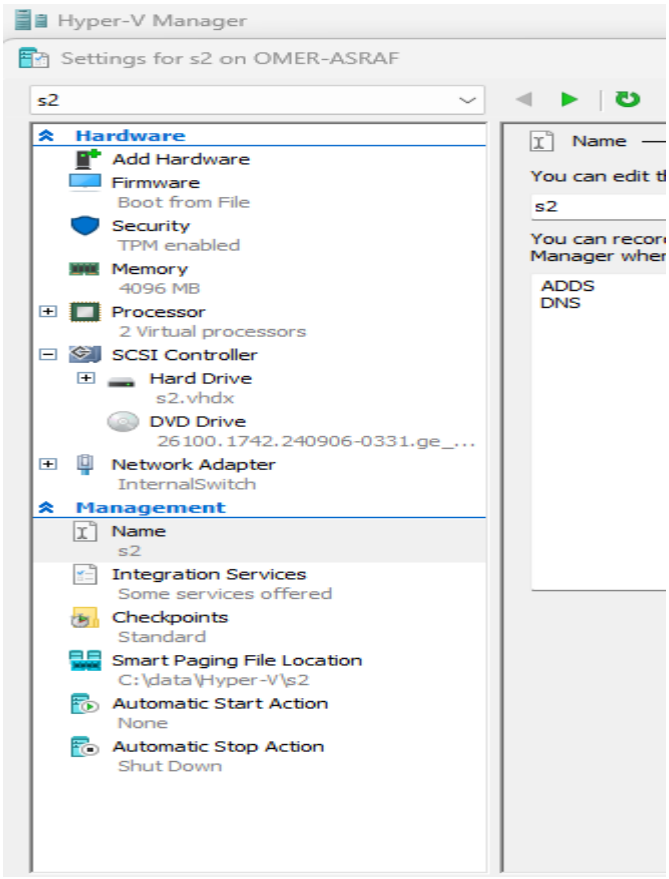




3. **ADDS:**

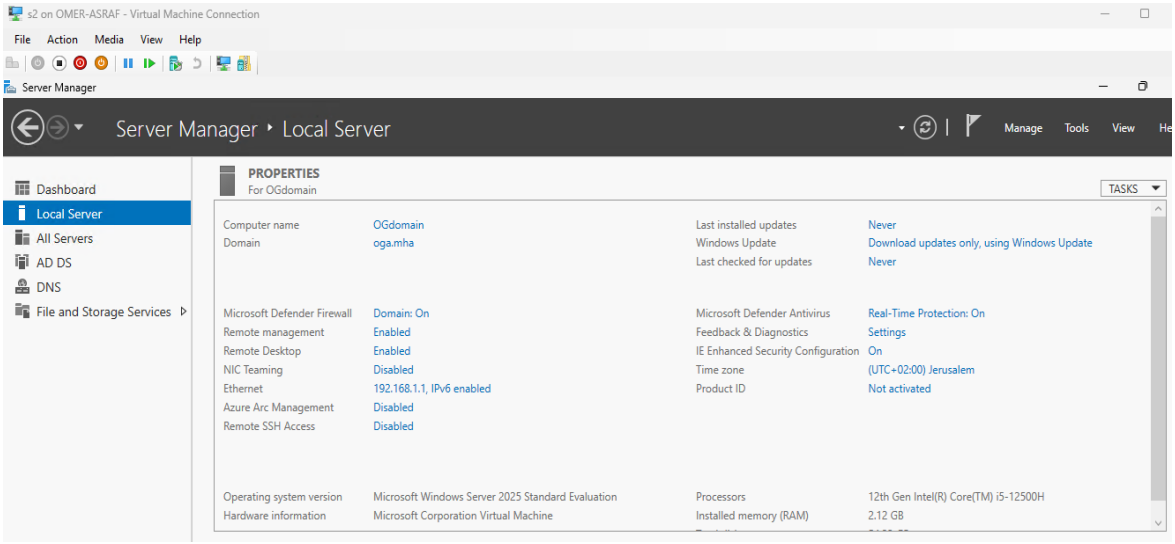
- Domain Name: oga.mha
- DC setup:

a. Create new VM:

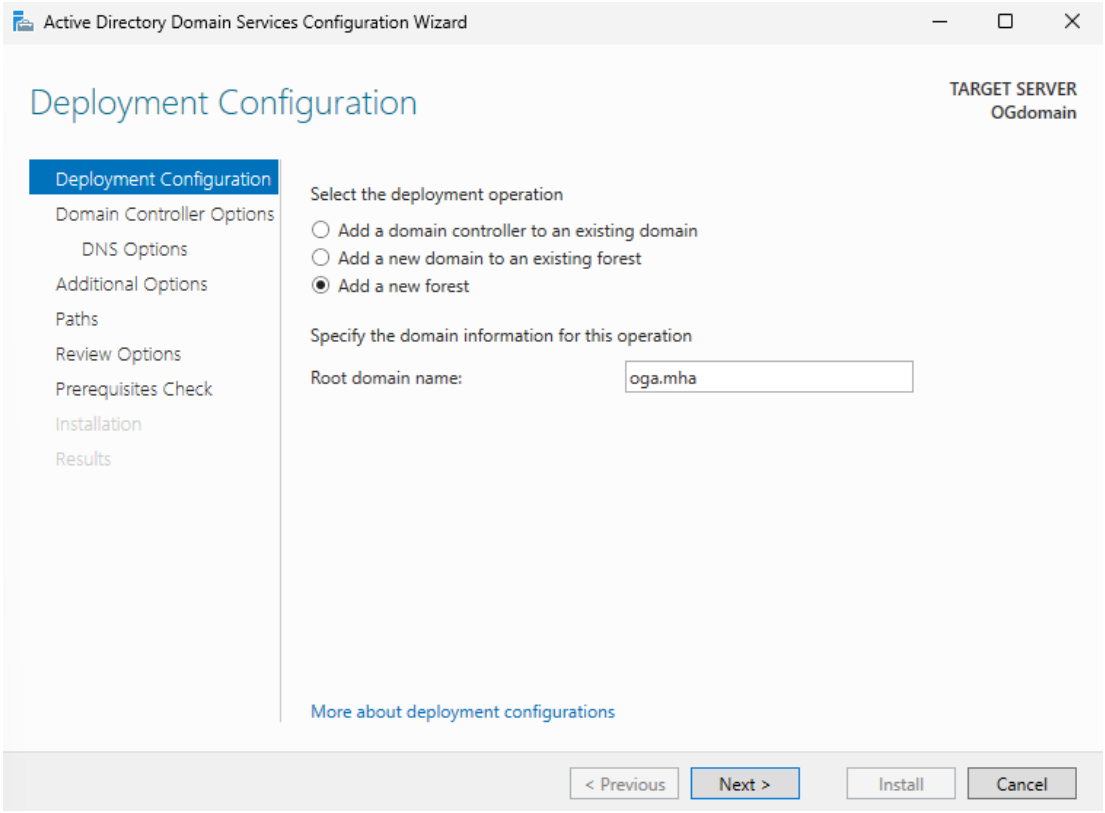


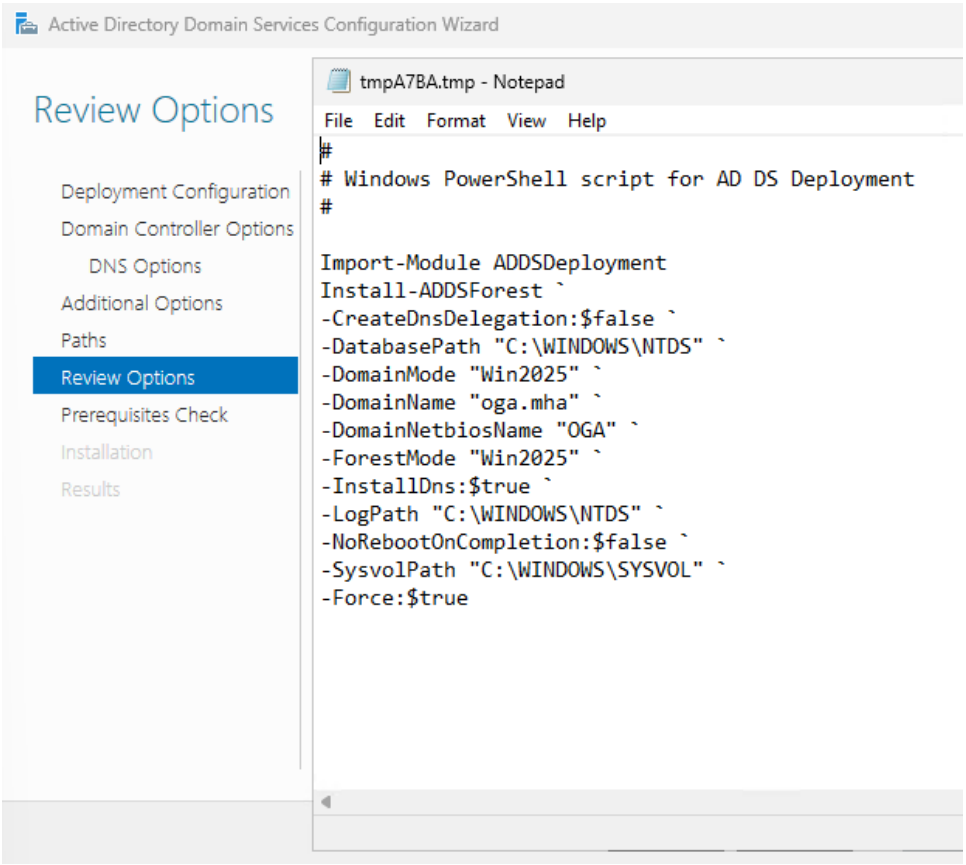
b. Windows Server 2025 installed.

c. initial configuration (the screenshot captured after ADDS)



d. promote server to DC

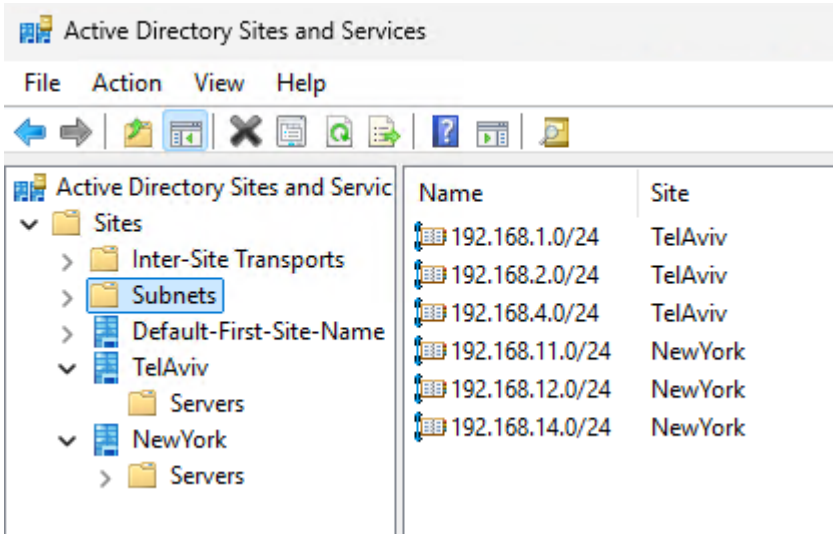




e. Initial AD configuration:

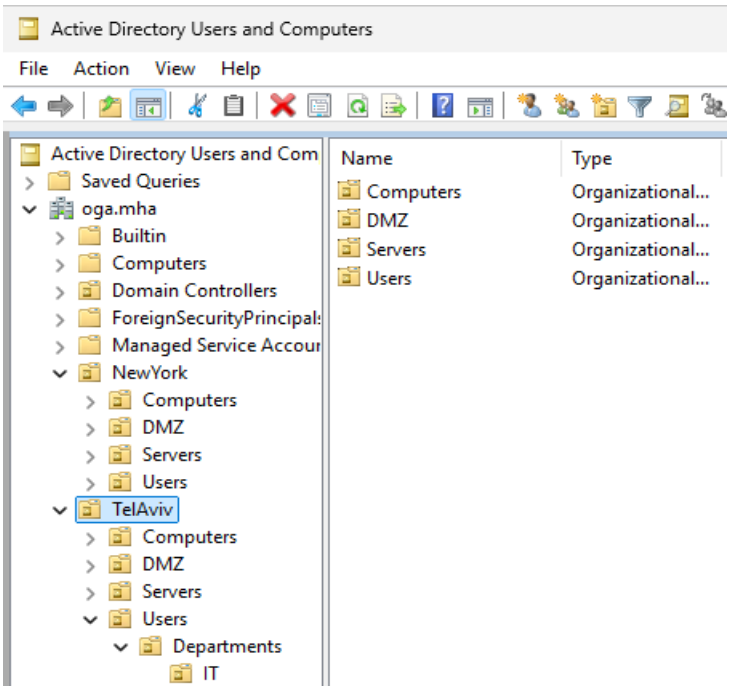
- Sites And Services:

  dssite.msc > new site > 'TelAviv' + 'NewYork'. subnets > new subnet > prefix: 192.168.1.0/24 etc. > select: TelAviv / NewYork > Ok.



- OU Topology:

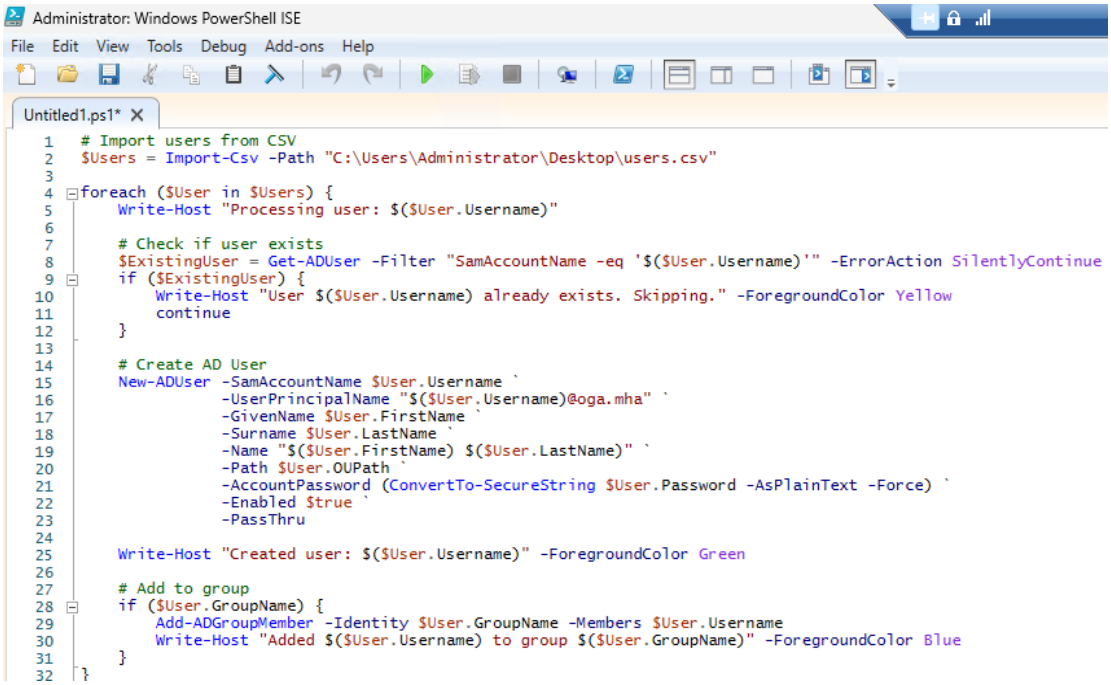
  First, I'll show my topology sketch:



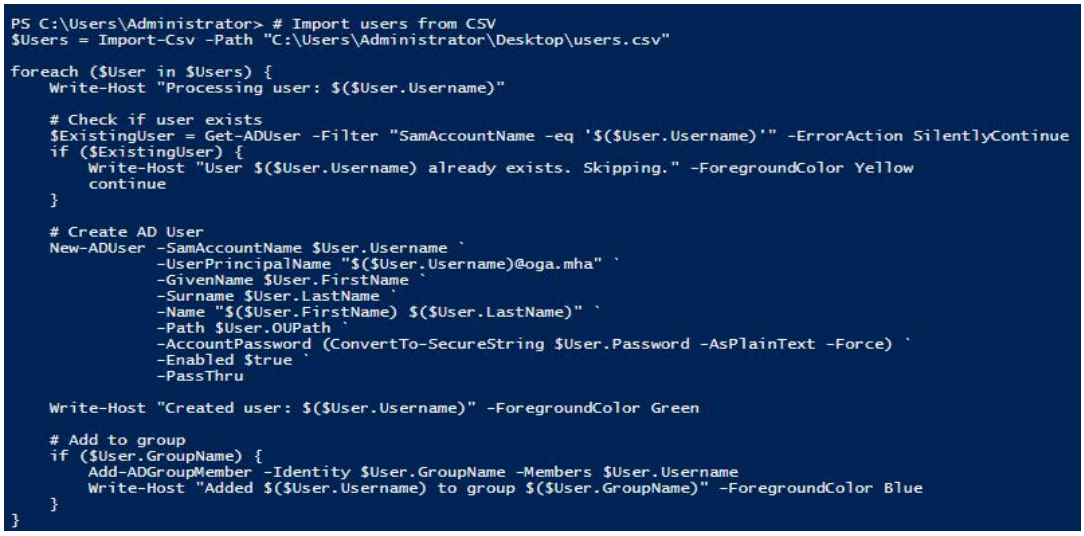
  I added "Departments" inside Users and only included "IT" for the example.

To create users I created CSV file in Notepad with the following details:

After, I used the following script to create the users and add them to path I want:



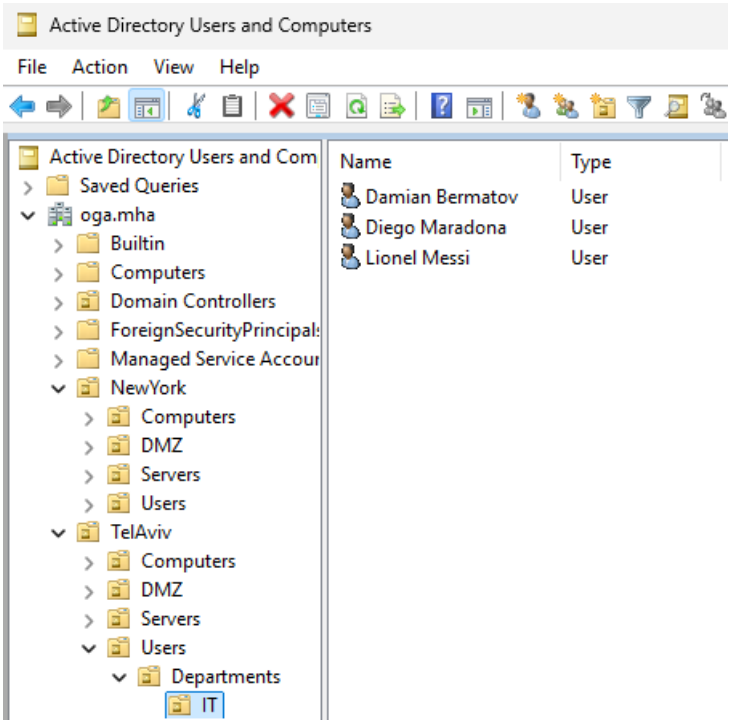
I ran the script on PowerShell as you can see and it worked (1/2):



(2/2):

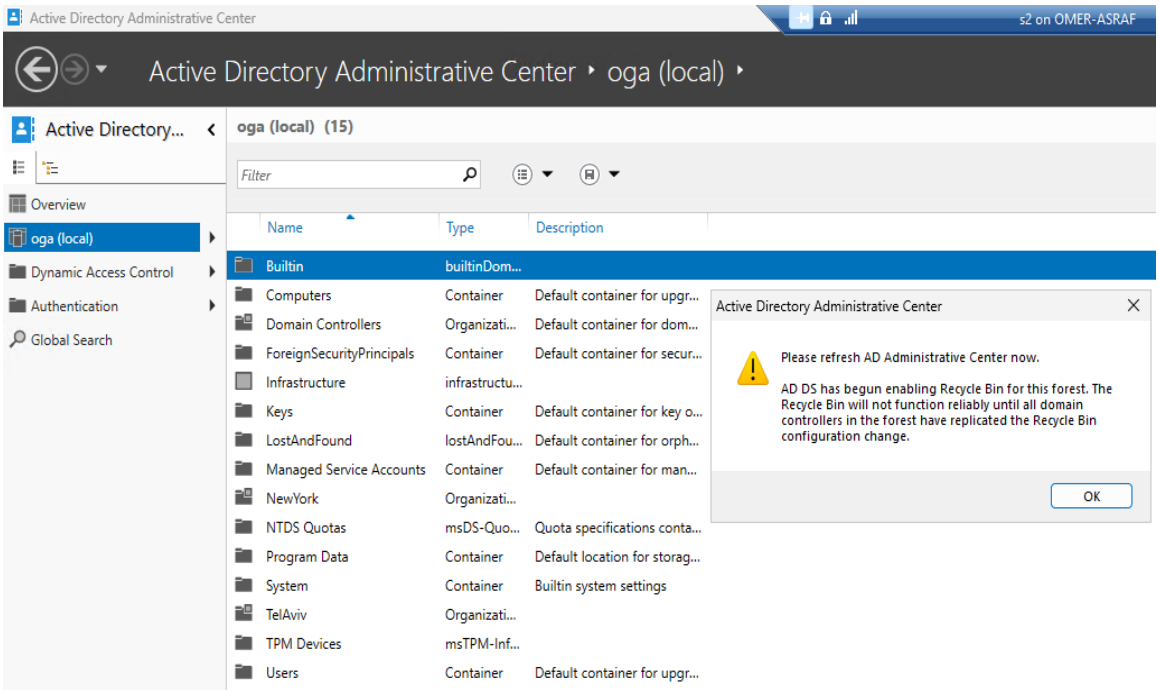
```
DistinguishedName : CN=Damian
                    Bermatov,OU=IT,OU=Departments,OU=Users,OU=TelAviv,DC=oga,DC=mha
Enabled           : True
GivenName         : Damian
Name              : Damian Bermatov
ObjectClass       : user
ObjectGUID        : 205e8d26-a749-4d8b-9c69-83f14895a484
SamAccountName    : DamianHayafe
SID               : S-1-5-21-1656588951-3106098696-1682092897-1109
Surname           : Bermatov
UserPrincipalName : DamianHayafe@oga.mha

Created user: DamianHayafe
Processing user: MessiGOAT
DistinguishedName : CN=Lionel
                    Messi,OU=IT,OU=Departments,OU=Users,OU=TelAviv,DC=oga,DC=mha
Enabled           : True
GivenName         : Lionel
Name              : Lionel Messi
ObjectClass       : user
ObjectGUID        : b85b18bd-06a0-4c88-bfb7-a4b5f45fc288
SamAccountName    : MessiGOAT
SID               : S-1-5-21-1656588951-3106098696-1682092897-1110
Surname           : Messi
UserPrincipalName : MessiGOAT@oga.mha

Created user: MessiGOAT
Processing user: Diego10
DistinguishedName : CN=Diego
                    Maradona,OU=IT,OU=Departments,OU=Users,OU=TelAviv,DC=oga,DC=mha
Enabled           : True
GivenName         : Diego
Name              : Diego Maradona
ObjectClass       : user
ObjectGUID        : 2e0ddf86-e217-421b-b55e-26011d3df7c4
SamAccountName    : Diego10
SID               : S-1-5-21-1656588951-3106098696-1682092897-1111
Surname           : Maradona
UserPrincipalName : Diego10@oga.mha

Created user: Diego10
```

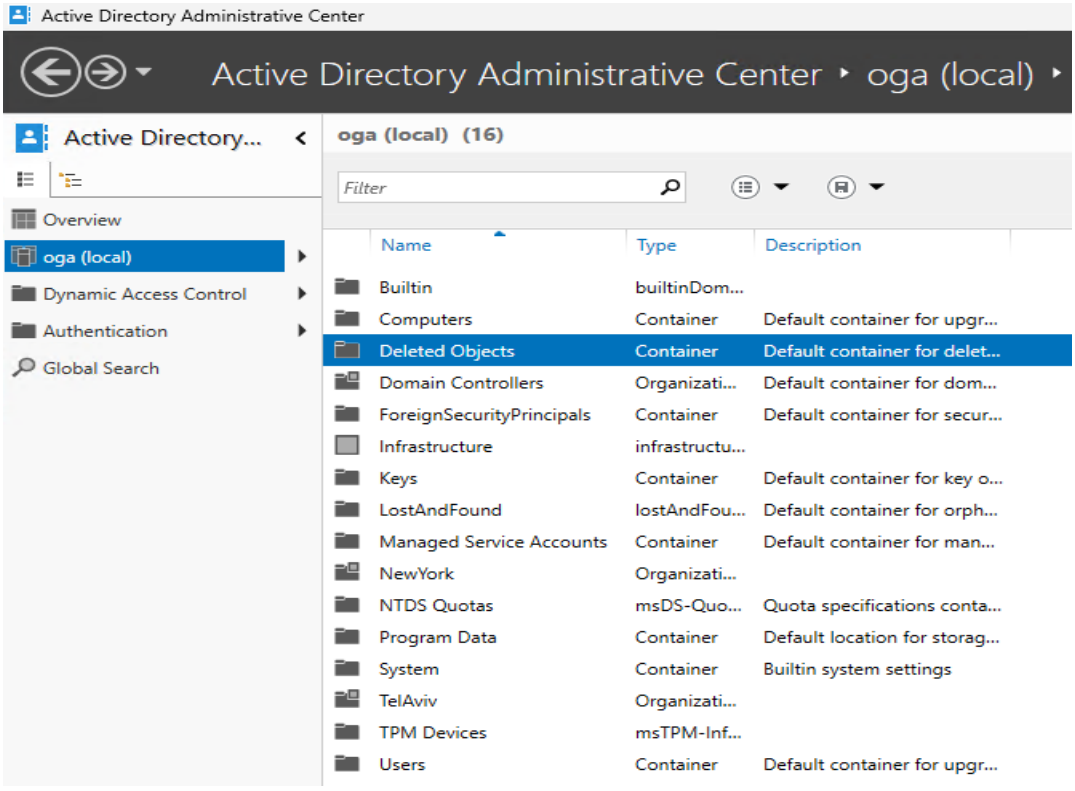
And now you can see the new IT users of Tel Aviv site exist:



Enable AD Recycle Bin:

go to dsac.exe > Right click on my domain > "Enable Recycle Bin" > Click "Ok" > refresh the AD Administrative Center.

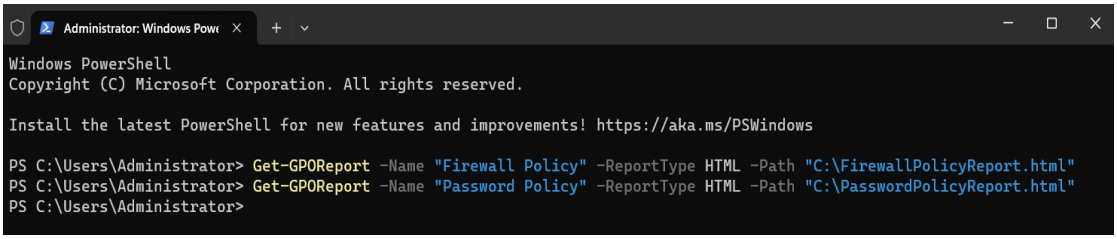


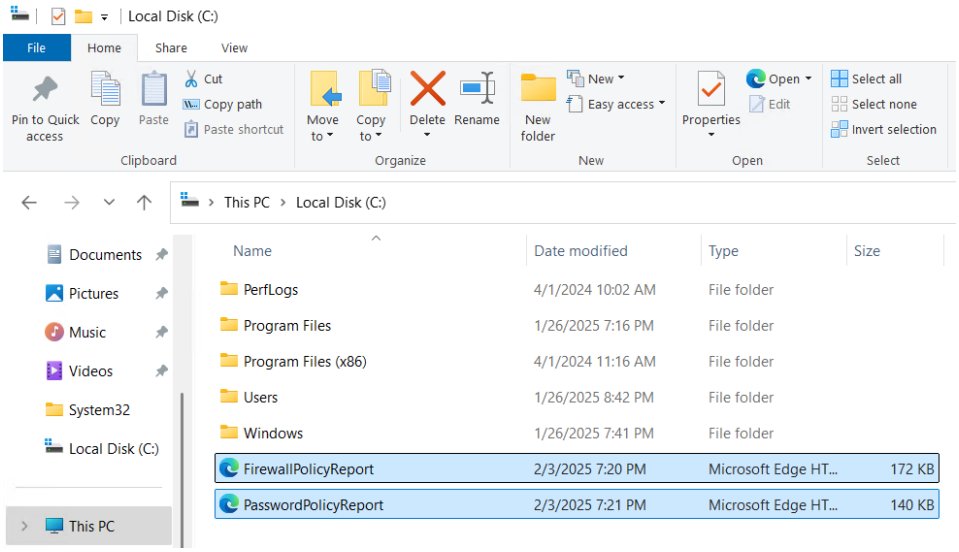


Now I can restore deleted AD objects (users, groups, OUs, etc.)

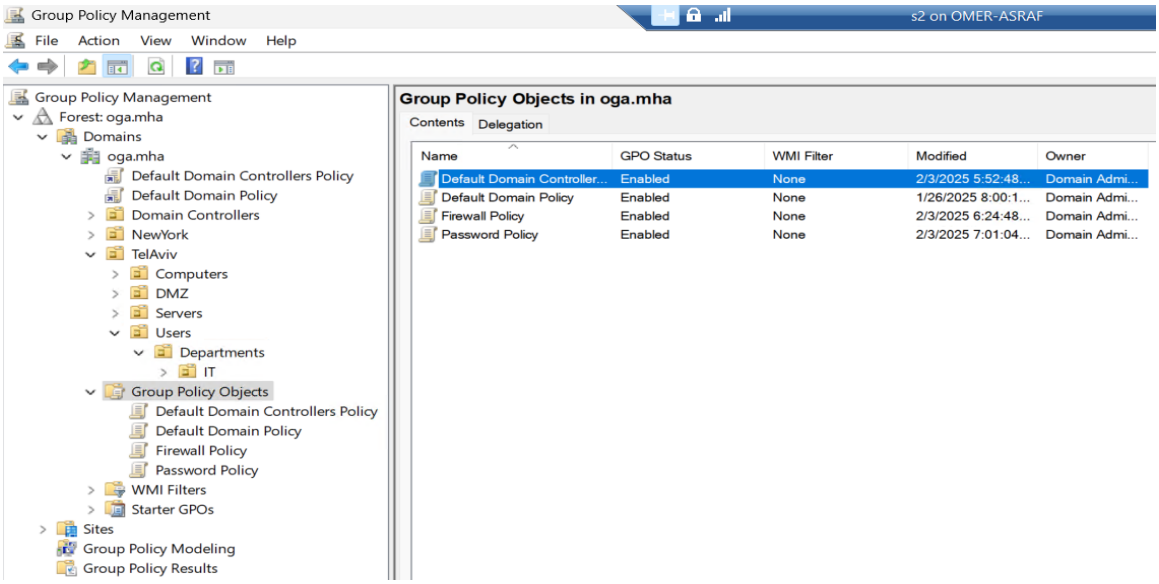
- Group Policy & Password Policy:

  First, I created an HTML reports for policies I intend to configure.

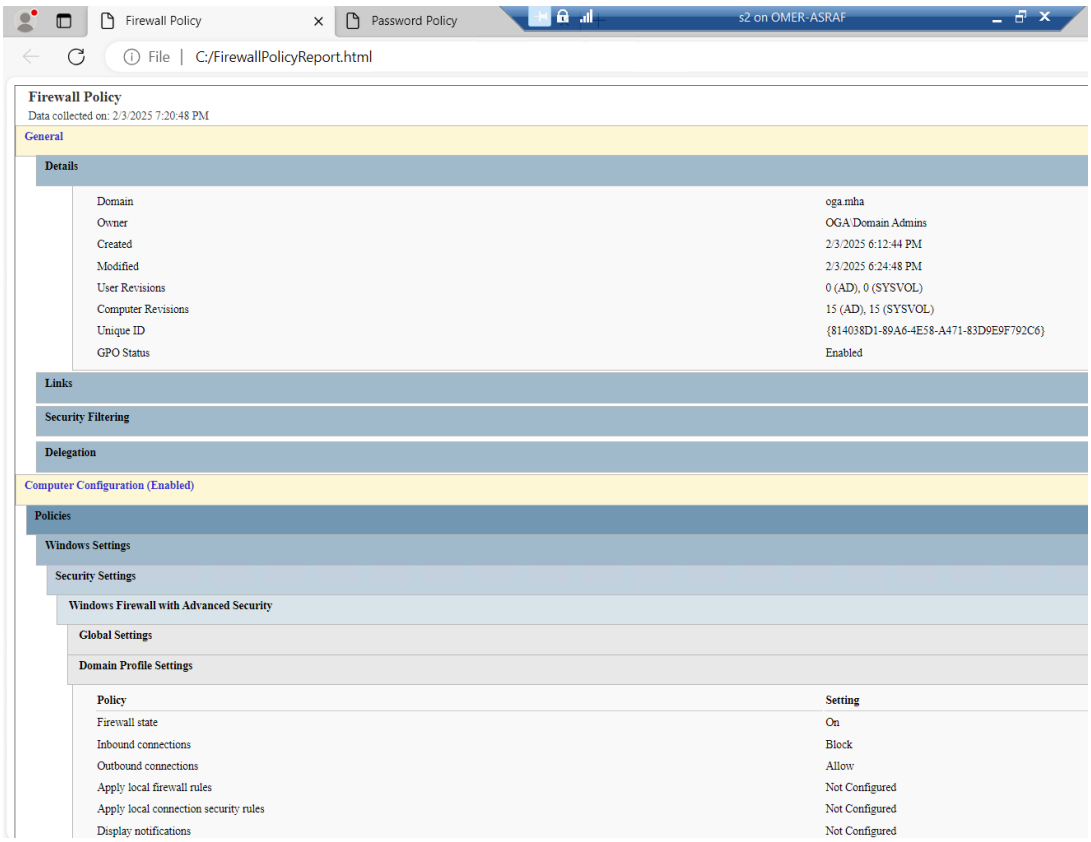


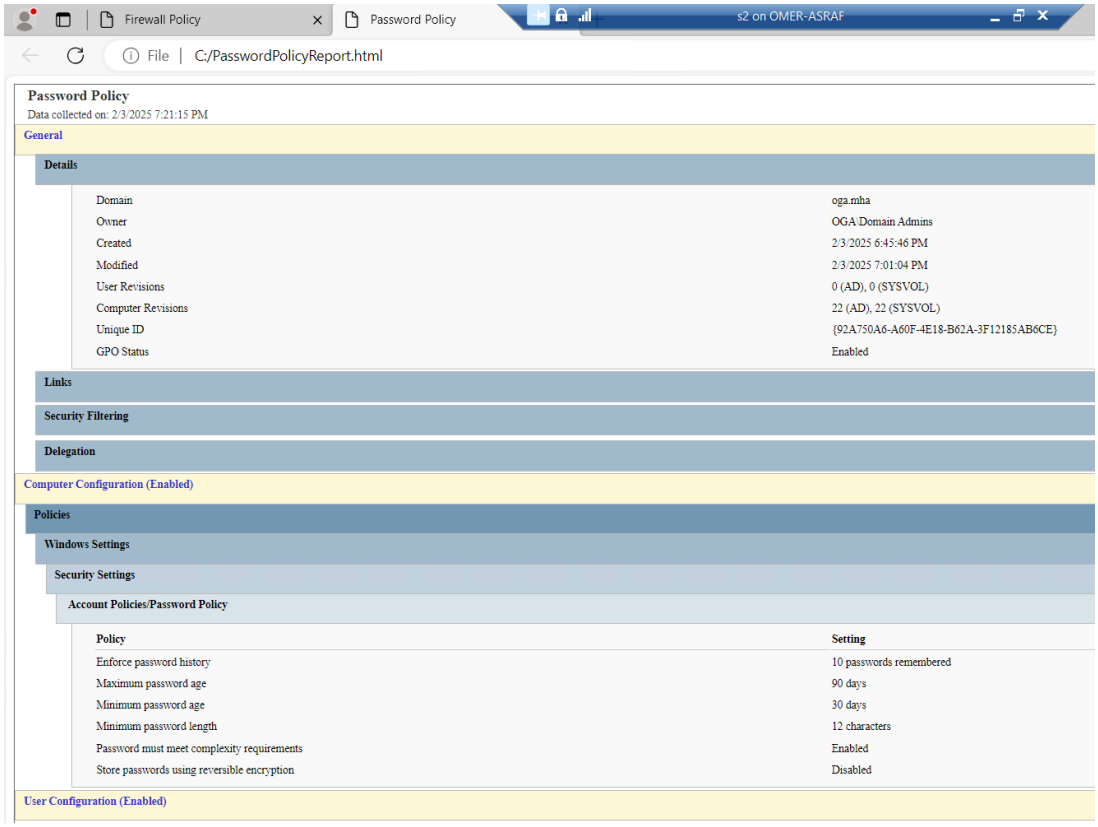


Second, I created new 2 policies in Group Policy Objects.



After I configured the policies, I forced the update on clients using CMD > 'gpupdate /force' and verified in the HTML reports.

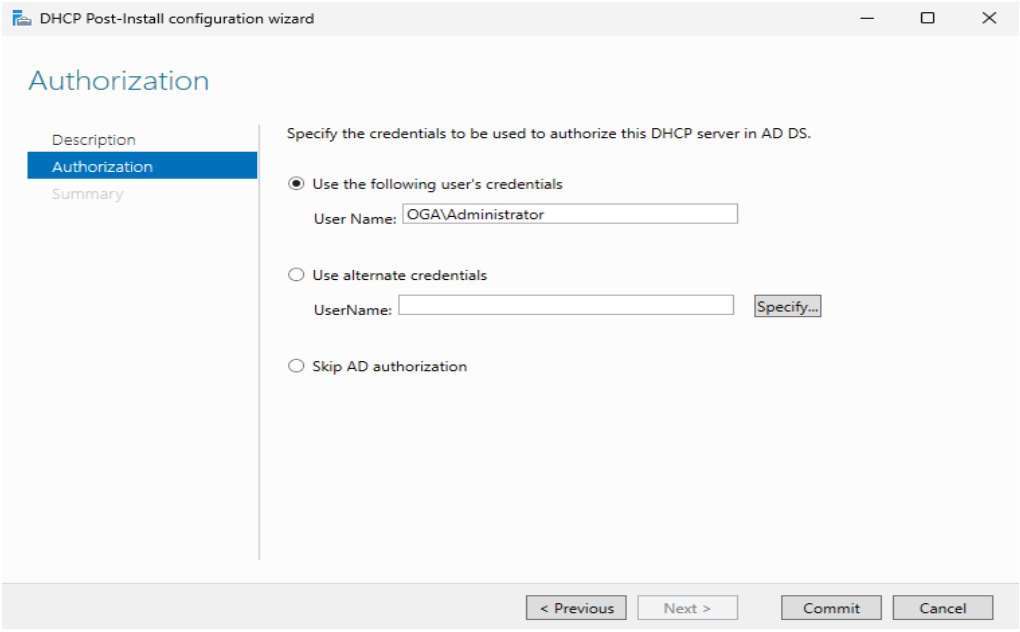




Now I can link the policies I made to users & groups I want.

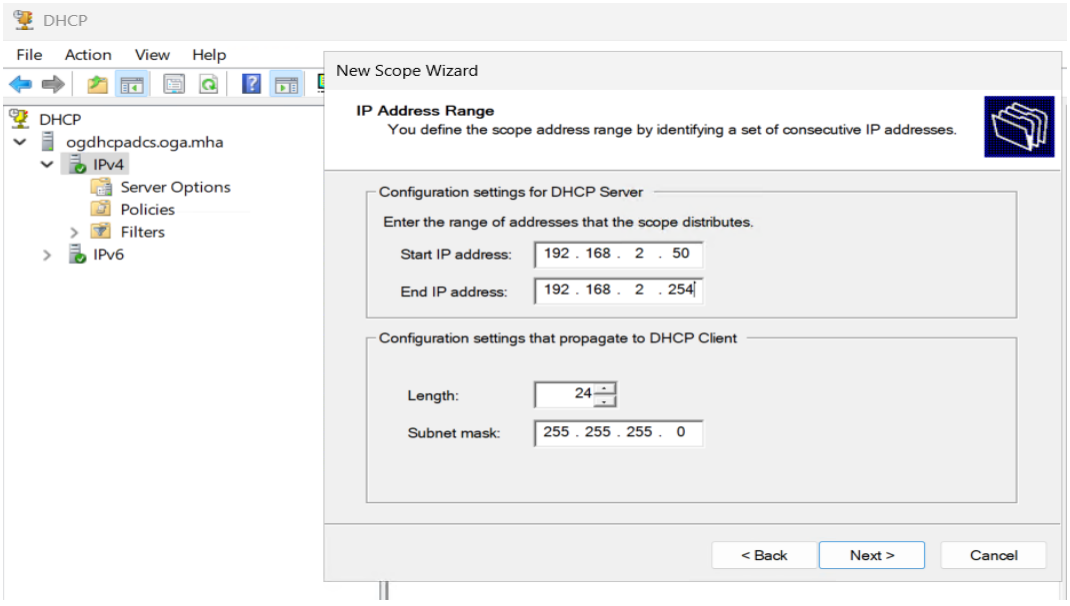
4. DHCP:

I created another VM, added it to 'oga.mha' and installed DHCP role.



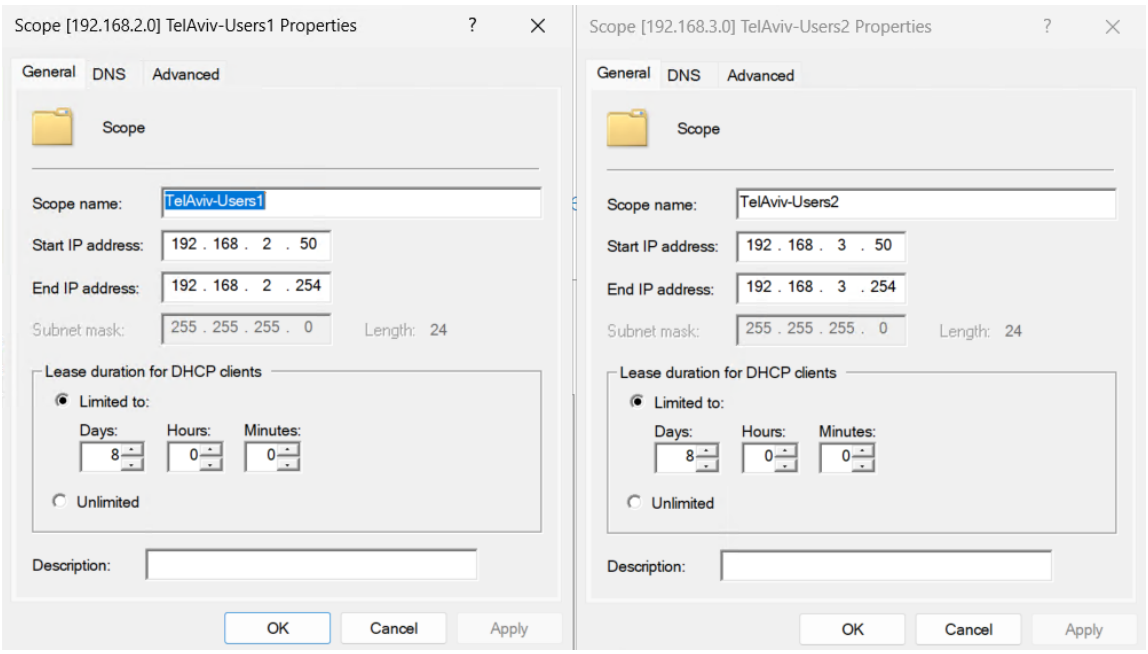
Now I can configure DHCP scopes for Users VLANs.

dhcpmgmt.msc > IPv4 > New Scope > etc.



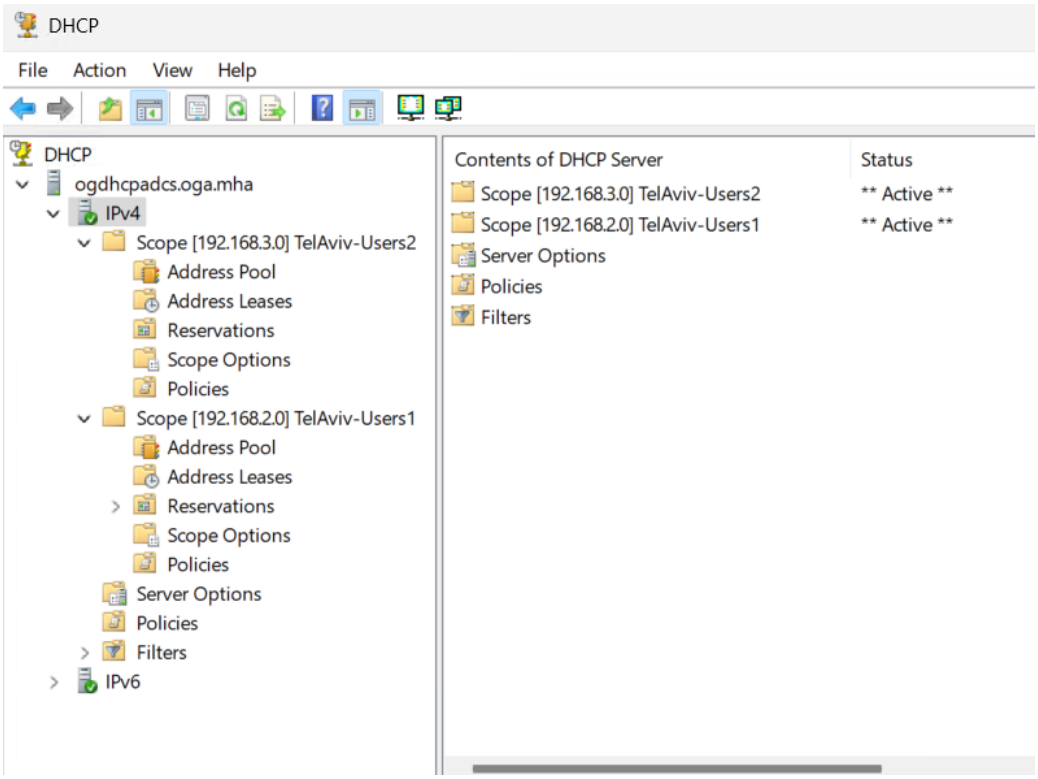
Lease Duration limited to 8 days for Tel Aviv Users.

Router (Default Gateway) IP Address – 192.168.2.1



I chose this IP ranges because I reserved IPs for Network Infrastructure at 192.168.2.2-49 IP range (firewalls ,switches ,printers etc.).

In addition, I reserved VLAN3 for the rest of the users and additional to join in the future if needed.



configuring DHCP failover is highly recommended to ensure high availability and load balancing in case the primary DHCP server fails.

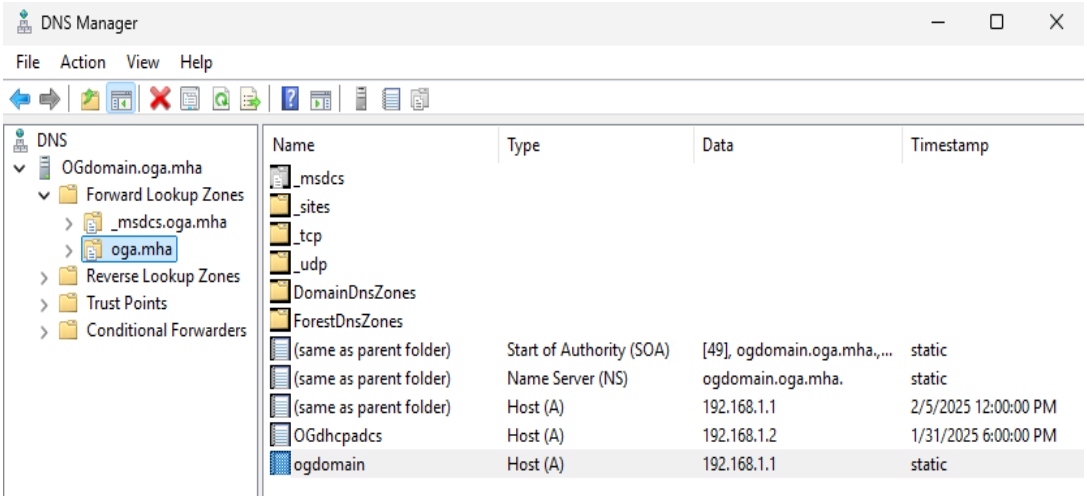
So my failover setup can be:

DHCP server TLV – 192.168.1.2 & DHCP server NY – 192.168.11.2

Tel Aviv - Hot Standby – 192.168.1.2 primary & 192.168.11.2 secondary.

NY – Hot Standby - 192.168.11.2 primary & 192.168.1.2 secondary.

5. DNS / Name Resolution:



This DNS Configuration ensures each site prefers its own DC for DNS resolution while having a backup if the local DNS server is unavailable:

192.168.1.1 – Tel Aviv DC – 'oga.mha'

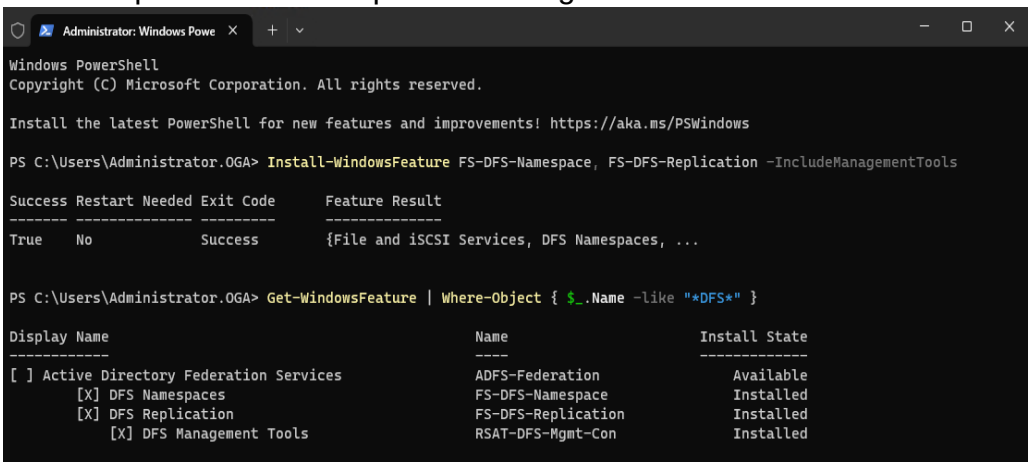
192.168.11.1 – New York DC (in theory)

Tel Aviv servers & clients: preferred 192.168.1.1, alternate 192.168.11.1 .

New York servers & clients: preferred 192.168.11.1, alternate 192.168.1.1 .

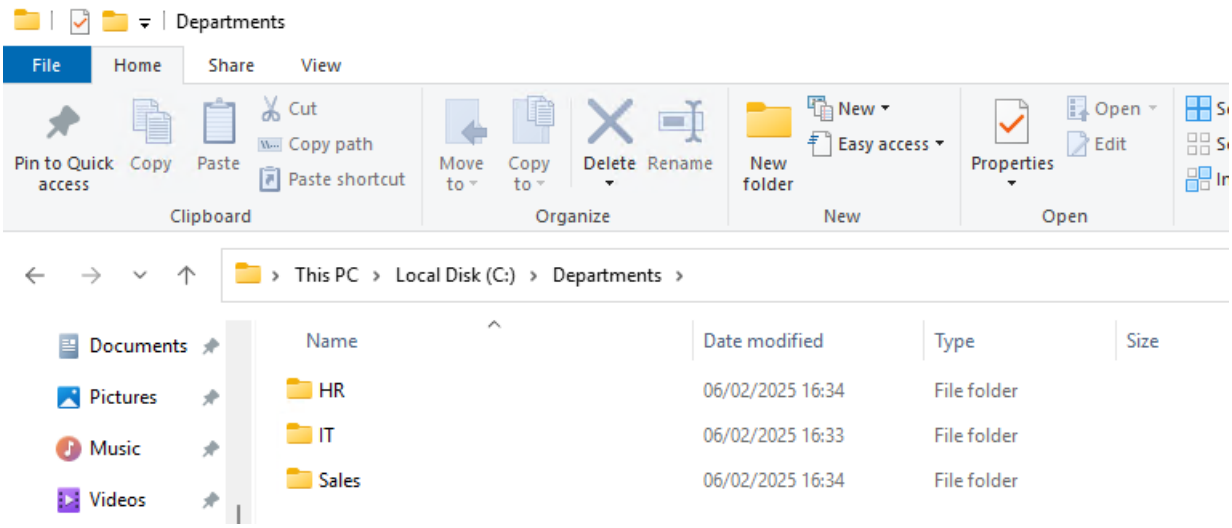
6. File Service solution (DFS):

I created another VM as a File server, I added it to 'oga.mha' and installed DFS Namespaces & DFS Replication using PowerShell.



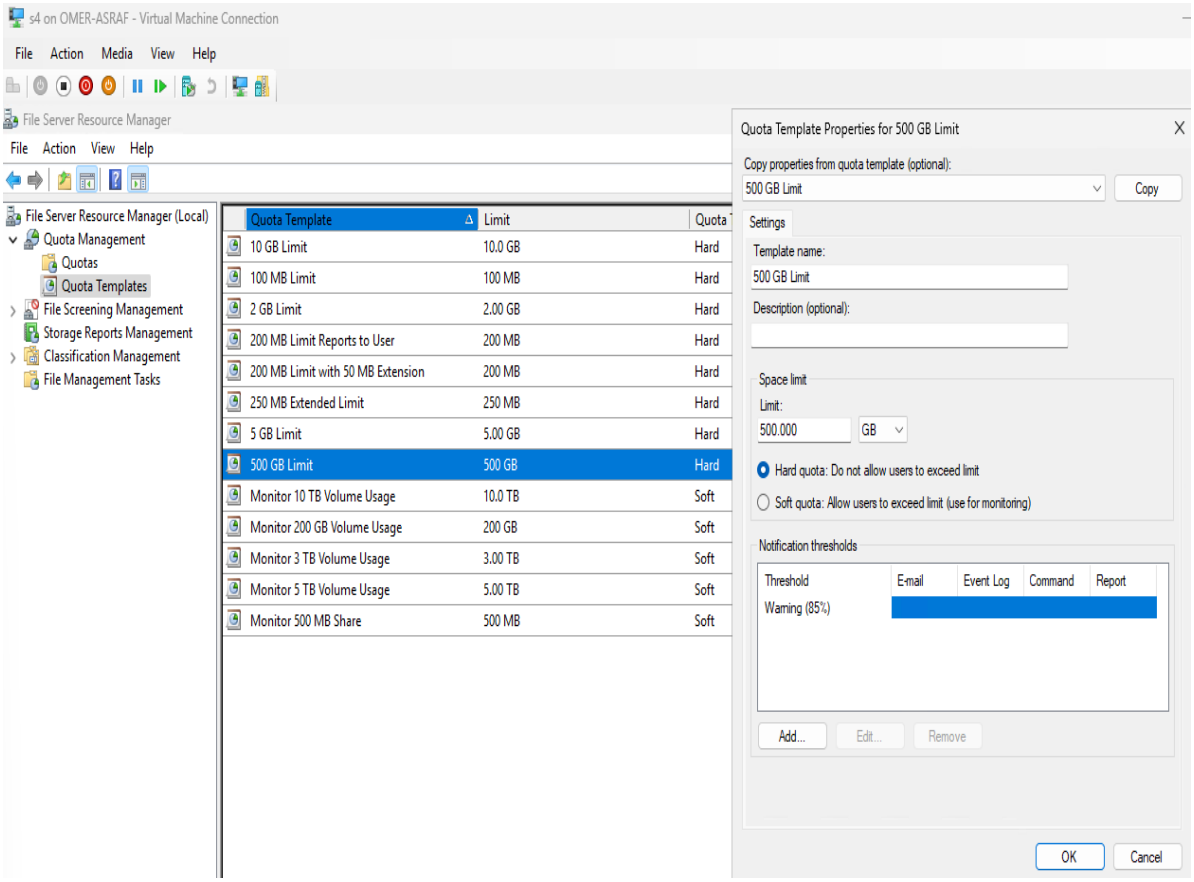
I

created folders for IT and HR departments for example.

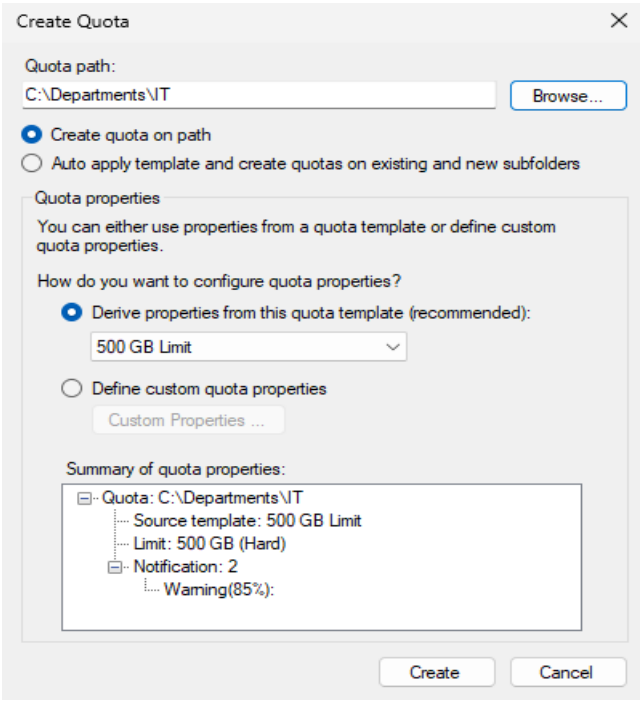


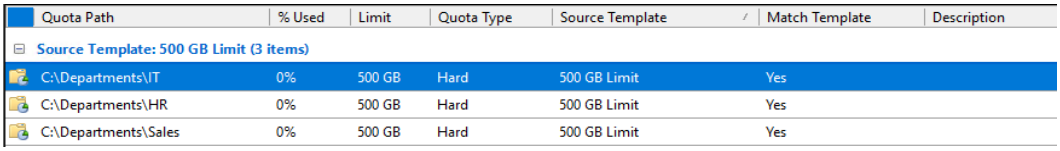
I had to install File Server Resource Manager to create a Quota Template for 500GB.

fsrm.msc > Quota Management > Create Quota Template > Configure the Template > Thresholds (adding Emails in theory).



Apply the Template to Department Folders ("IT" folder example)

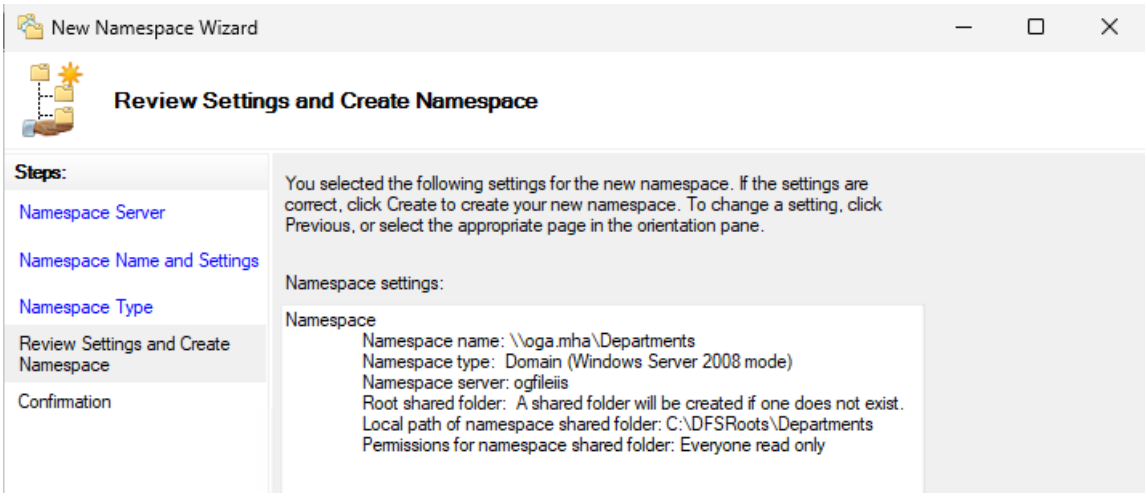




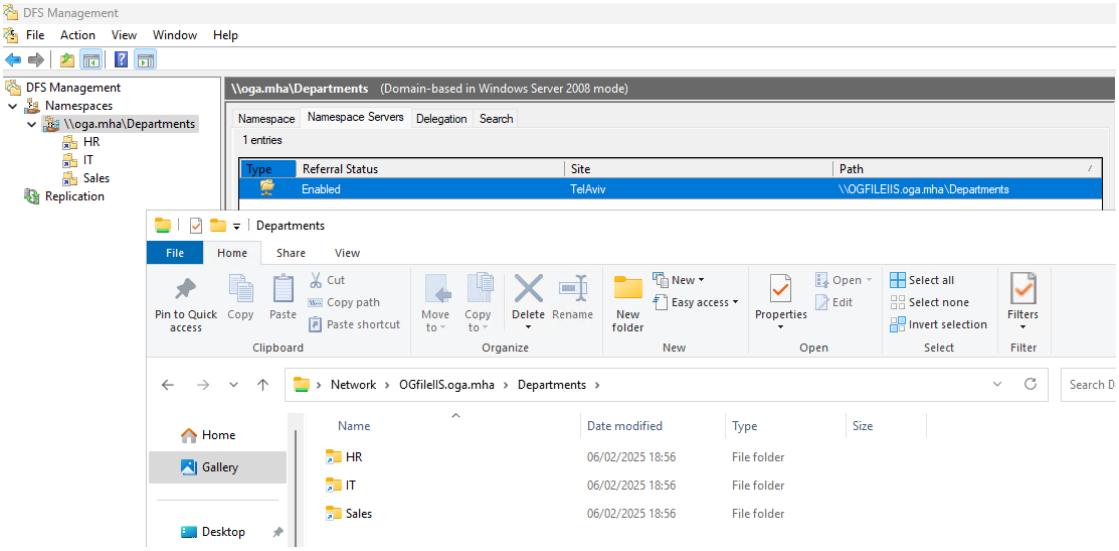
Quota Path	% Used	Limit	Quota Type	Source Template	Match Template	Description
Source Template: 500 GB Limit (3 items)						
C:\Departments\IT	0%	500 GB	Hard	500 GB Limit	Yes	
C:\Departments\HR	0%	500 GB	Hard	500 GB Limit	Yes	
C:\Departments\Sales	0%	500 GB	Hard	500 GB Limit	Yes	

(In theory) gives full access to users according to their department's shared folder.

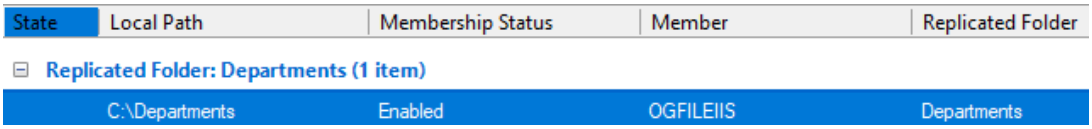
After this, I created DFS Namespace: dfsmgmt.msc > new namespace etc. > Create namespace Success.



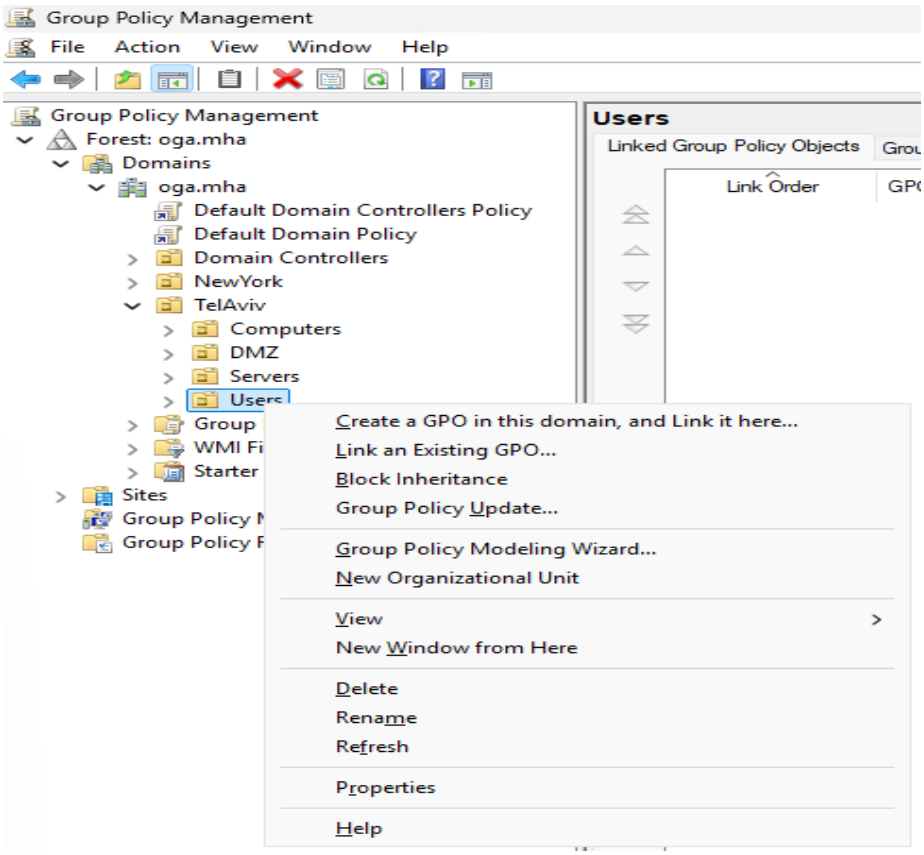
Add folder targets > path > adding 'IT' & 'HR & 'Sales'



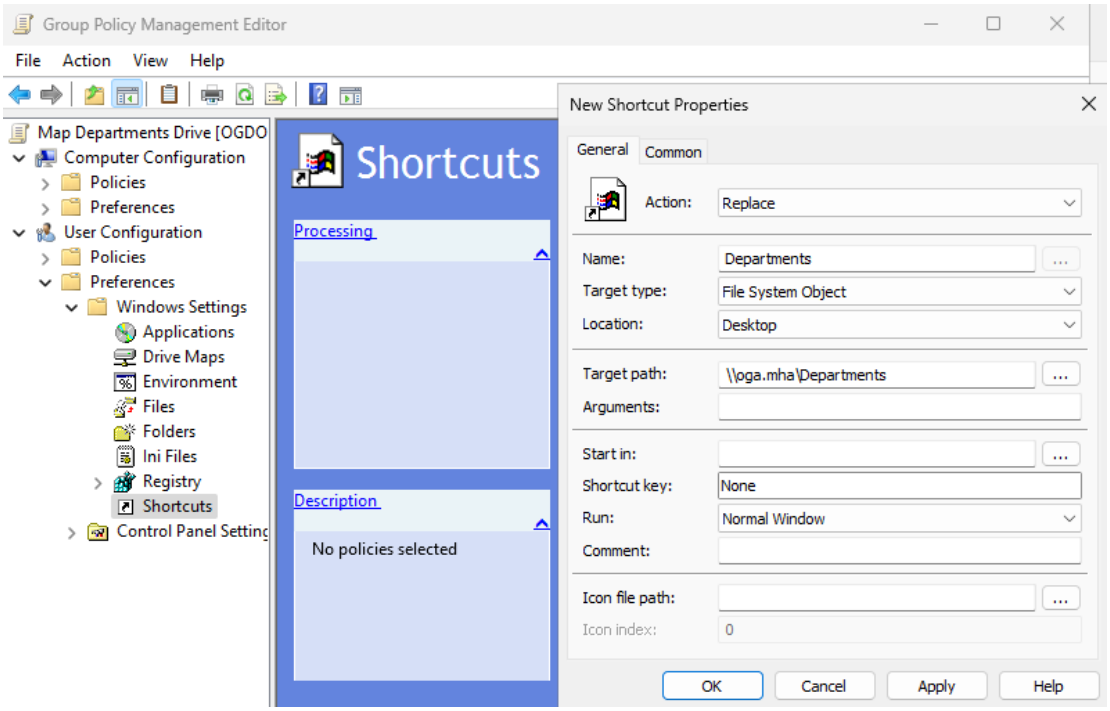
Replication > New replication group > Multipurpose Replication Group > Name: 'DepartmentsReplication' > domain: oga.mha > members: other servers > full mesh > etc.



To deploy shortcut to employees desktops I'll create a GPO and link it in the relevant OU called 'Map Departments Drive'. For example:

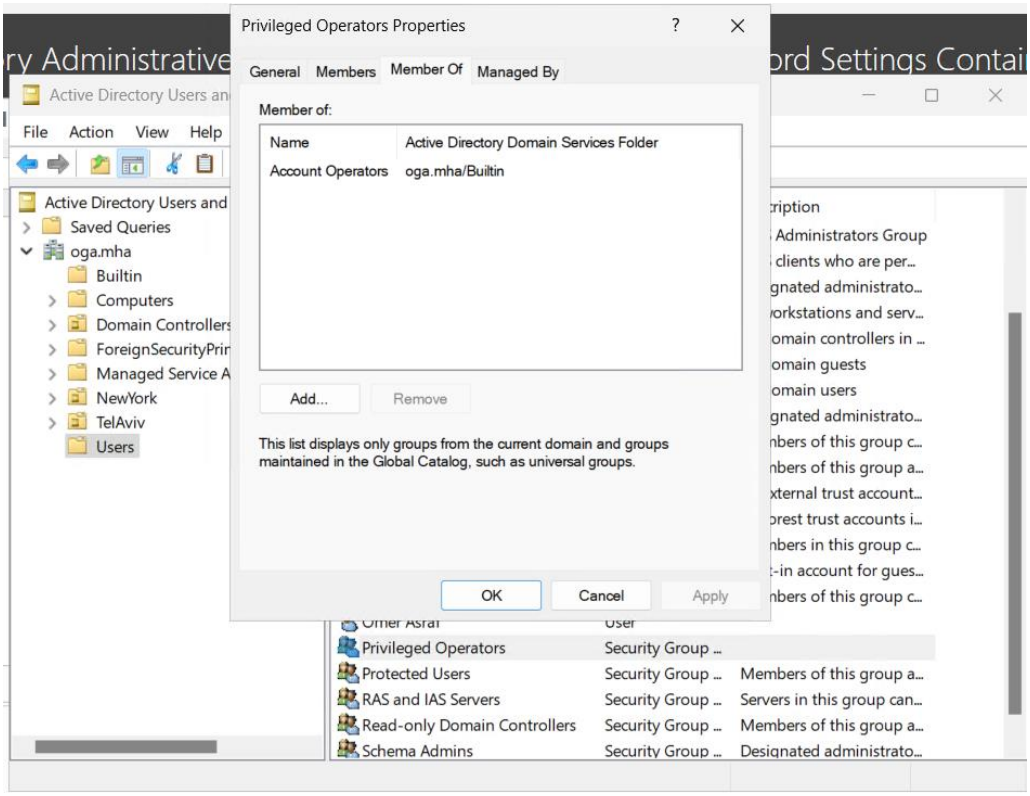


'Map Departments Drive' GPO > Edit > User configuration > Preferences > Windows Settings > Shortcuts > New Shortcut > etc.

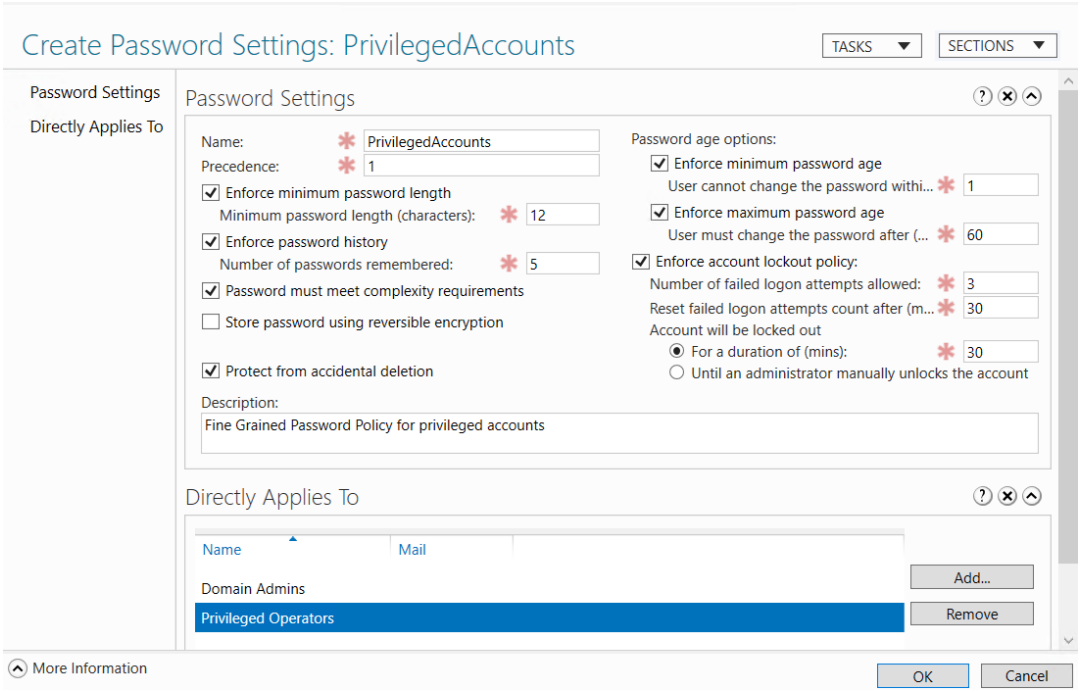


7. **Privileged account:**

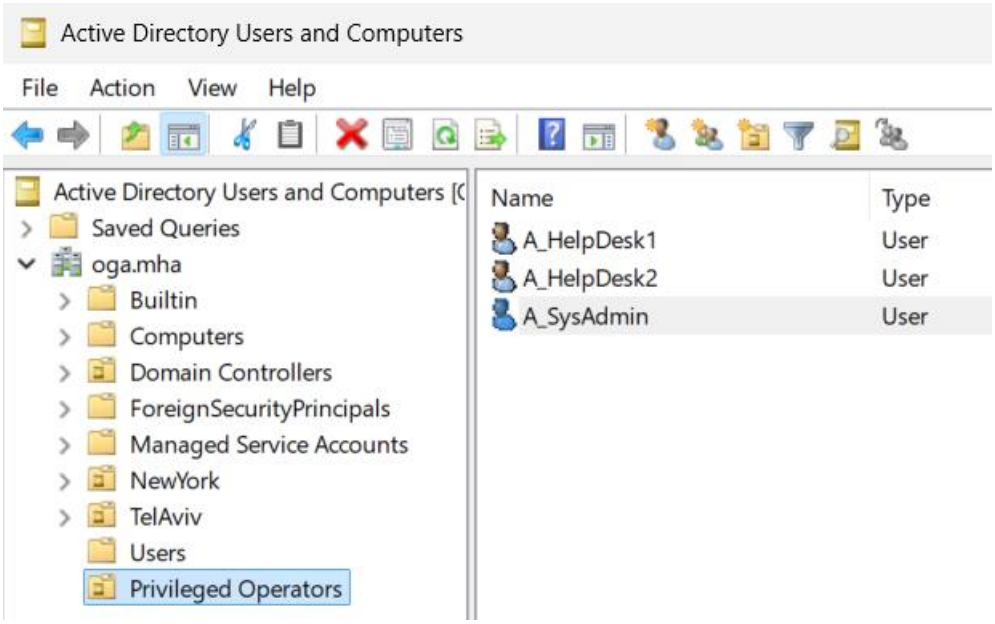
First, I created new Security Group in AD Users & Computers called 'Privileged Operators' and added to members of 'Account Operators' from Built-In.



To Create a Fine Grained Password Policy I went to ADAC (dsac.exe) > 'oga' (local) > system > password settings container > new > password settings > filled details > added relevant groups to policy:

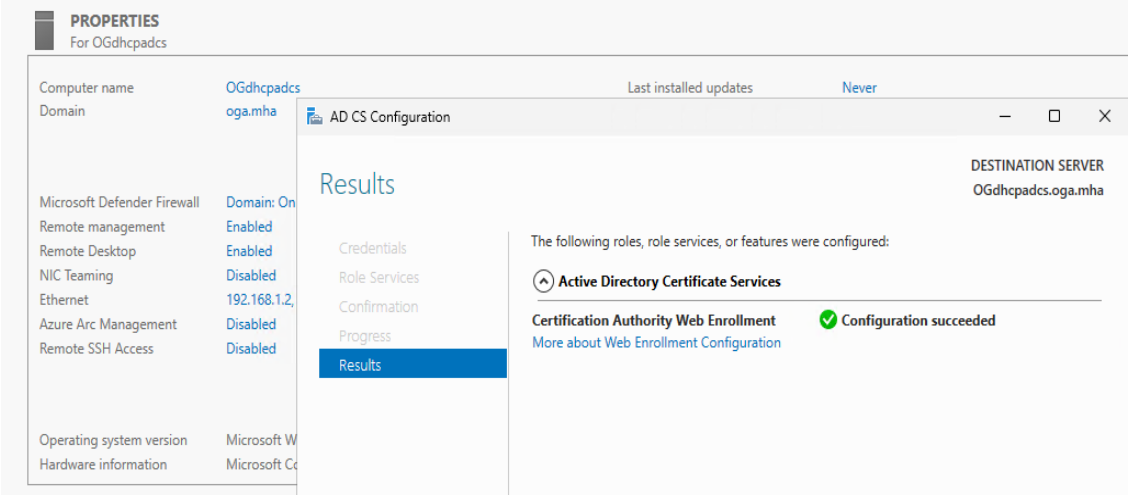


After, I created new OU called 'Privileged Operators' and created under this OU 2 helpdesk users & 1 system admin.

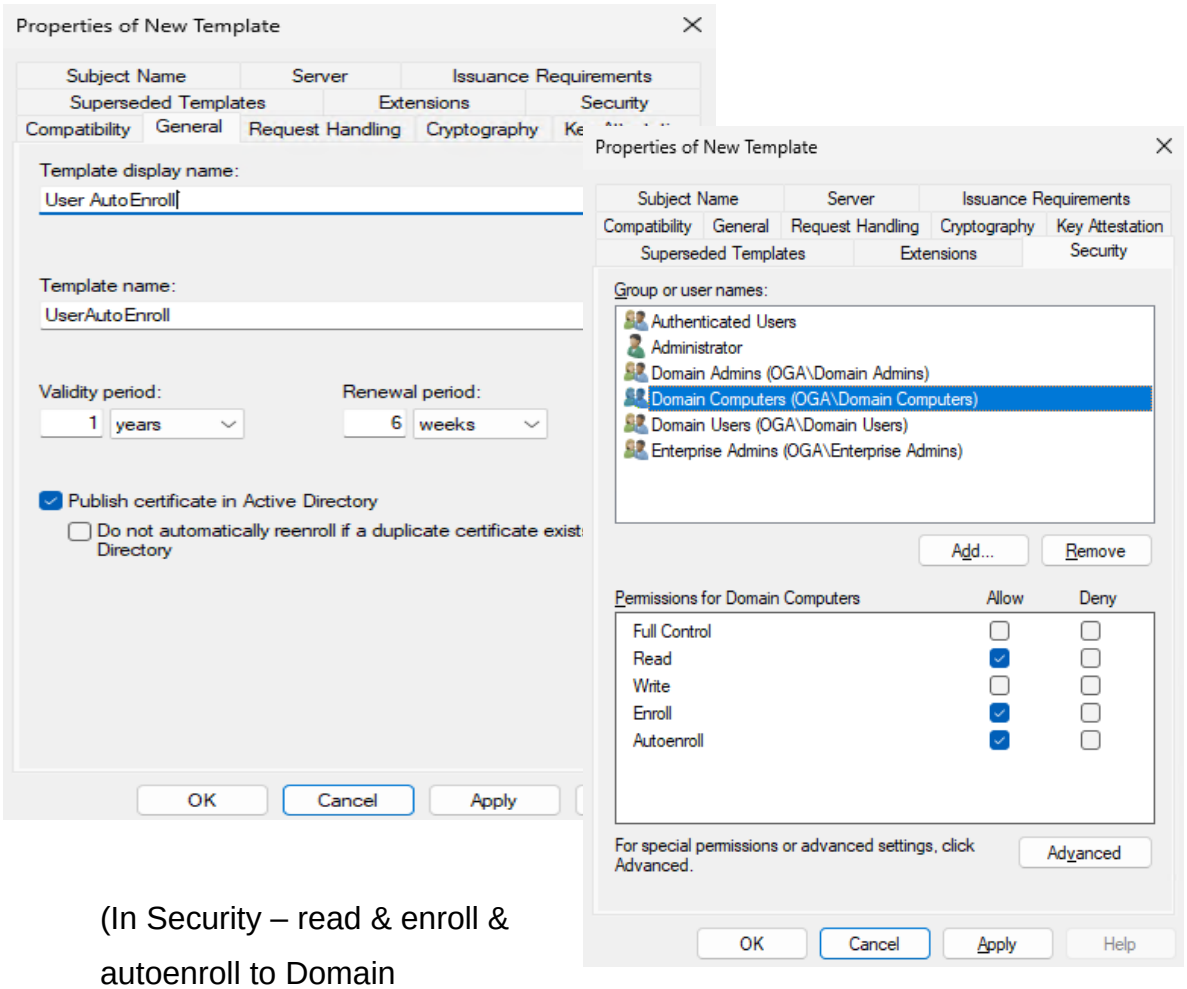


8. **ADCS:**

   On my DHCP + ADCS server ('OGdhcpadcs') I installed the role 'Certificate Authority Web Enrollment'.

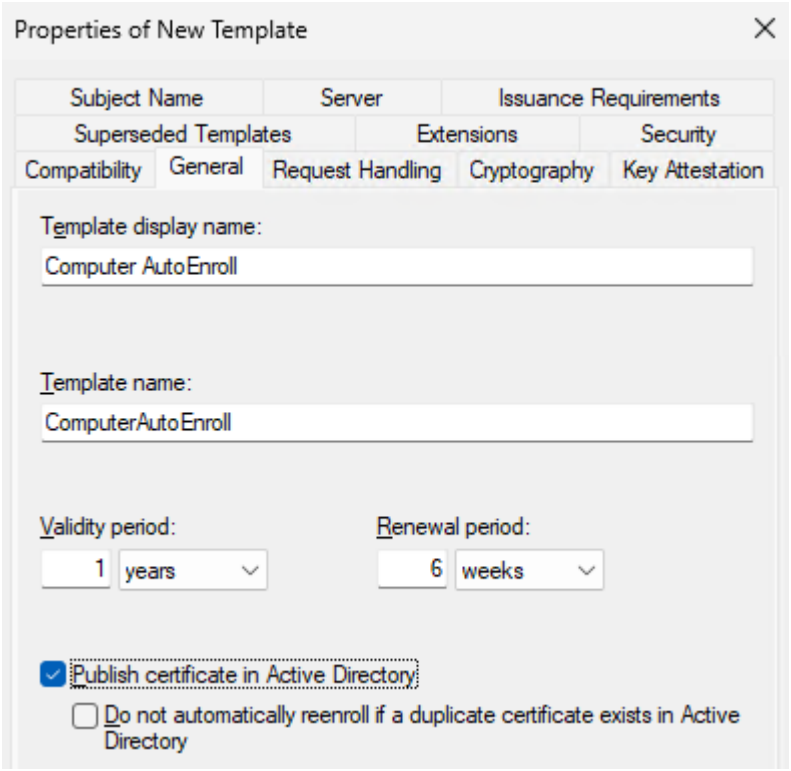


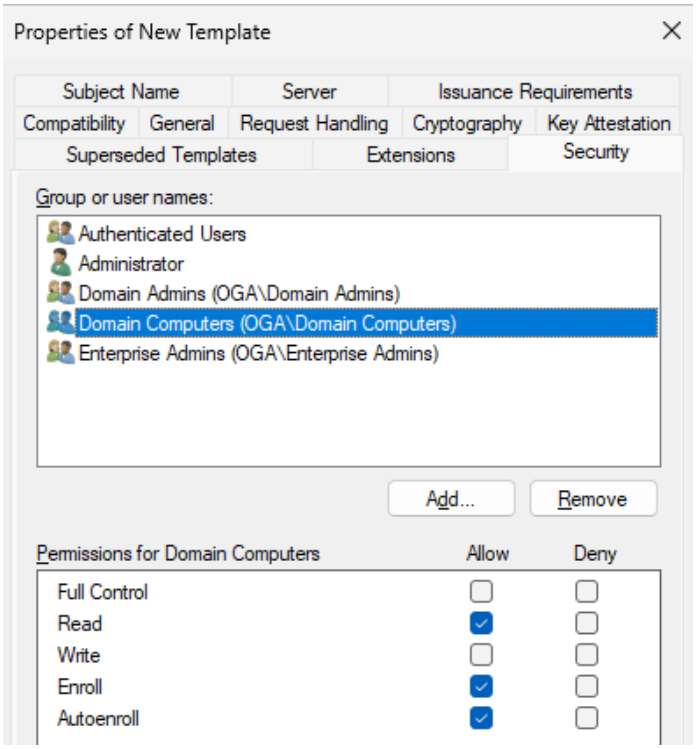
- Configure certificate templates for auto-enrollment > certsrv.msc > 'oga-OGDHCPADCS-CA' > Certificate Templates > Manage > 'User' & 'Computer' templates > Duplicate Template > and configure in General & Security:

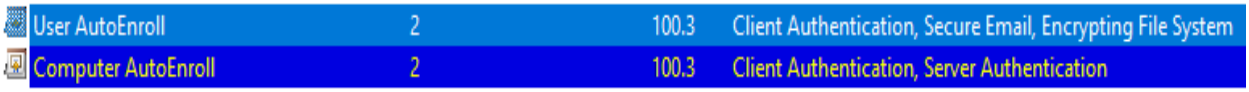


   (In Security – read & enroll & autoenroll to Domain Computers & Domain Users.

Also same for 'Computer' template > Duplicate template > etc.

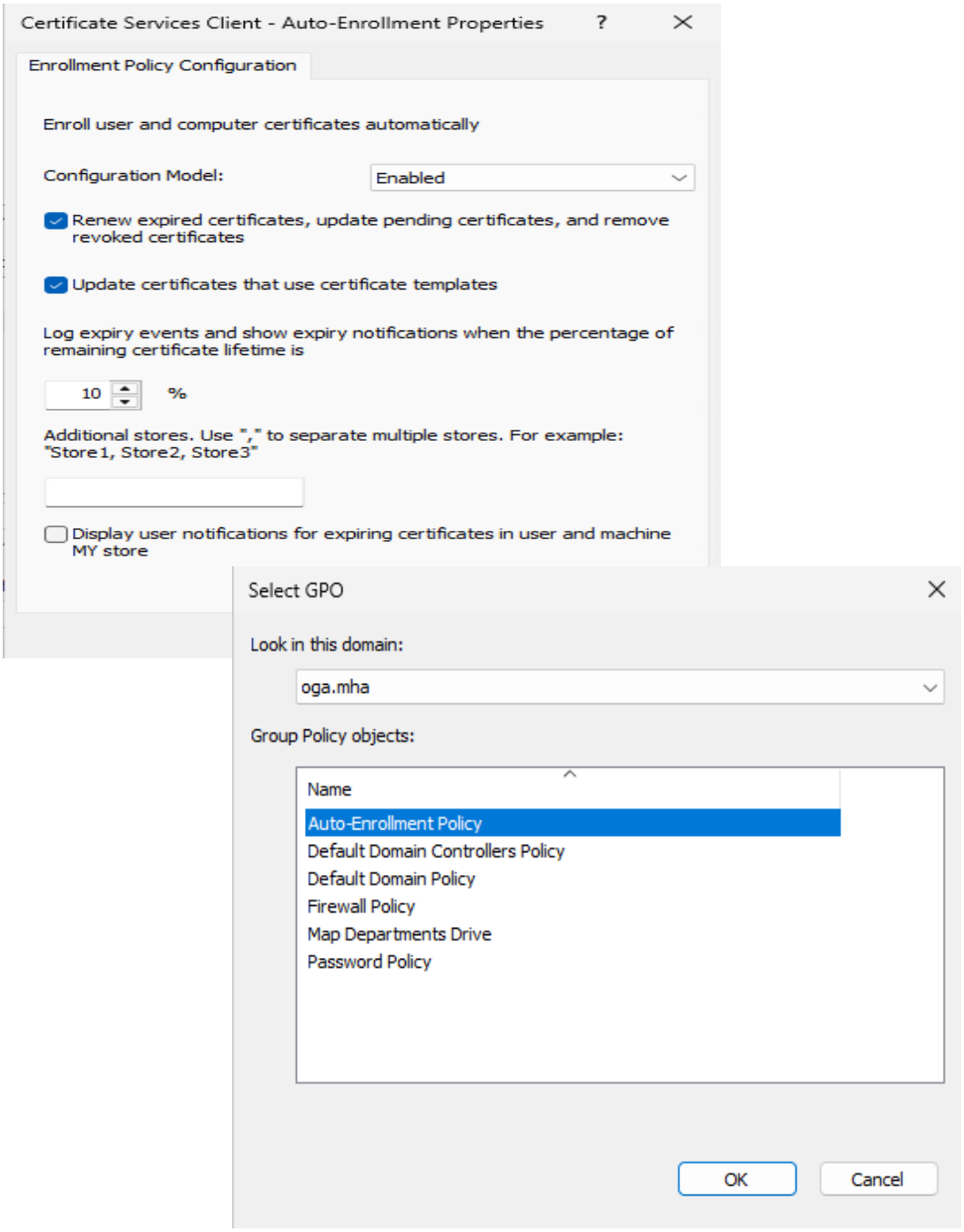




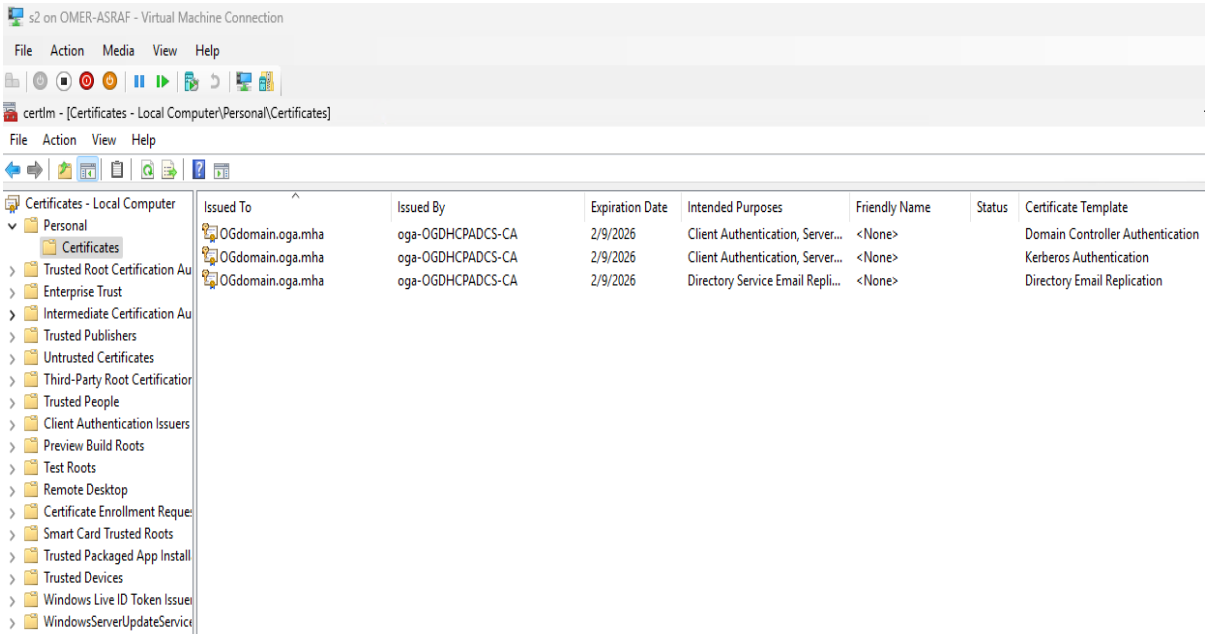


After, I went back to certsrv.msc > created new certificate template to Issue > selected User AutoEnroll" & "Computer AutoEnroll > Ok.

- Configure Auto-Enrollment in Group Policy > went to DC > gpmc.msc > created new GPO named 'Auto-Enrollment Policy' > edit > in both Computer & User Configuration went to Policies > etc. > 'Public Key Policies' > Enabled > mark V on Renew… & Update… > Link GPO to 'oga.mha'.



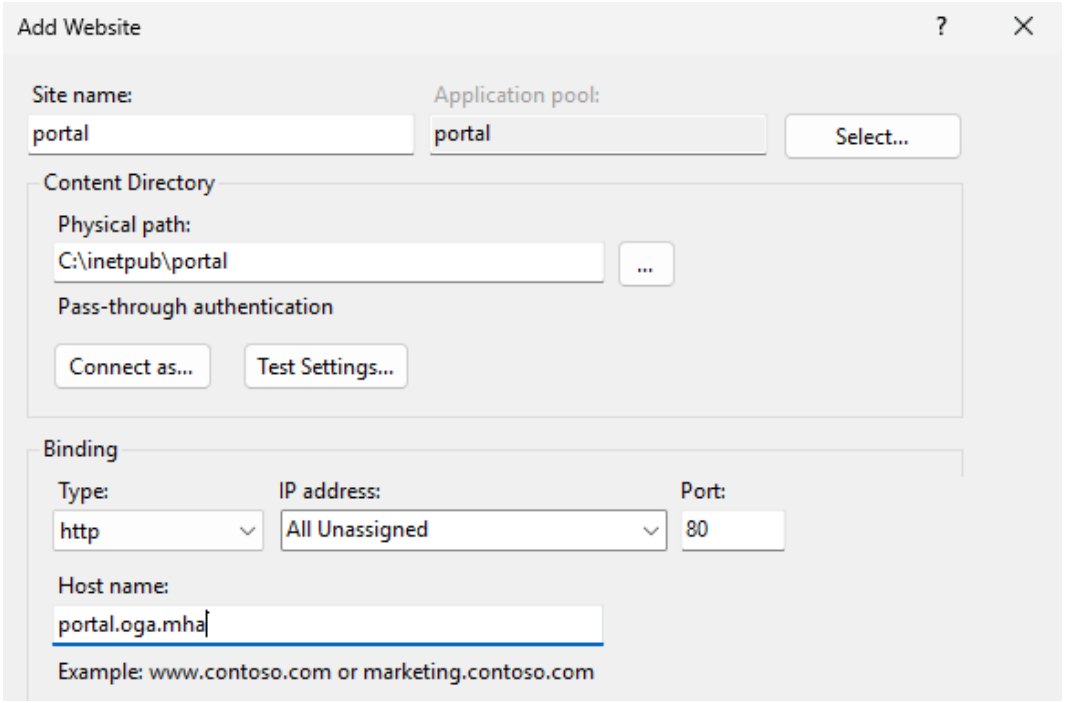
certlm.msc > Personal > Certificates.



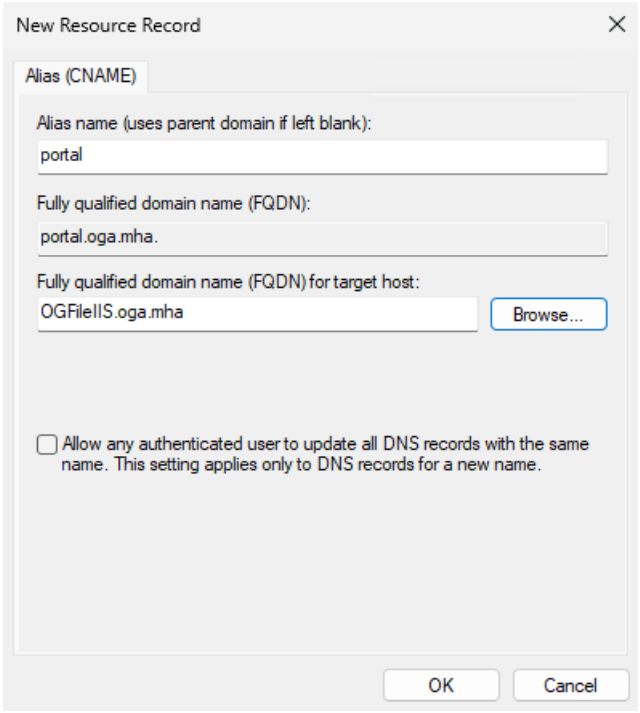
9. **Intranet Portal:**

   On my File & IIS server ('OGfileIIS') I installed Web Server (IIS) role.

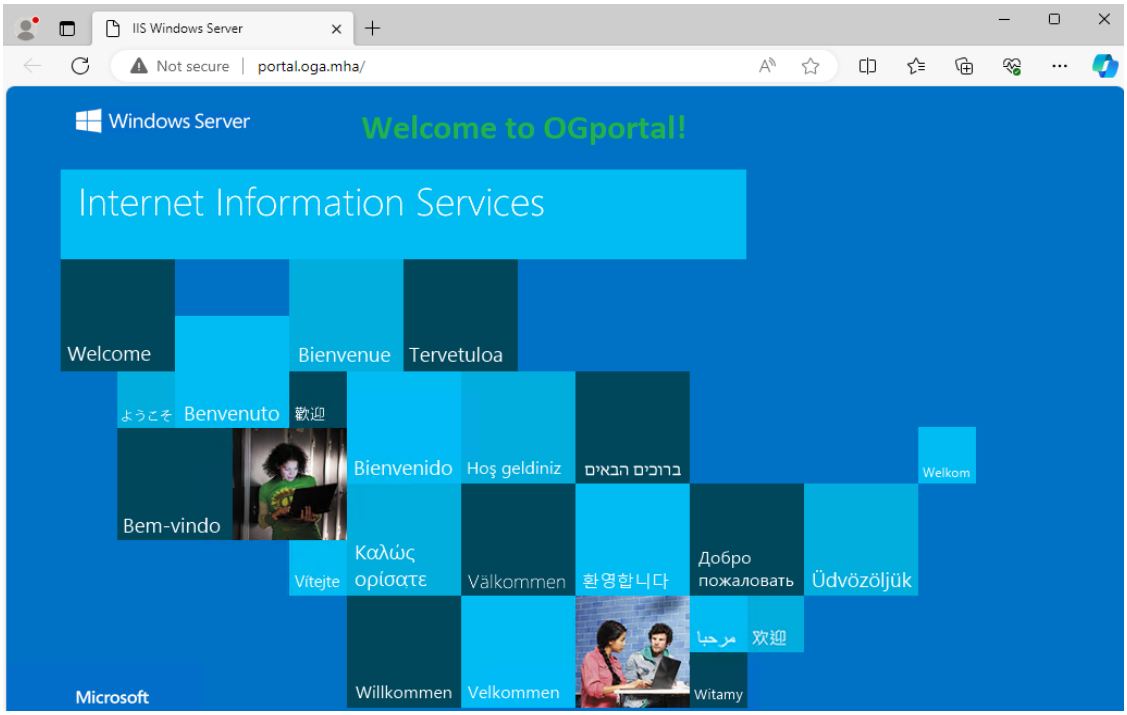
   Create web folder 'C:\interpub\portal' > went to inetmgr > create a New Site



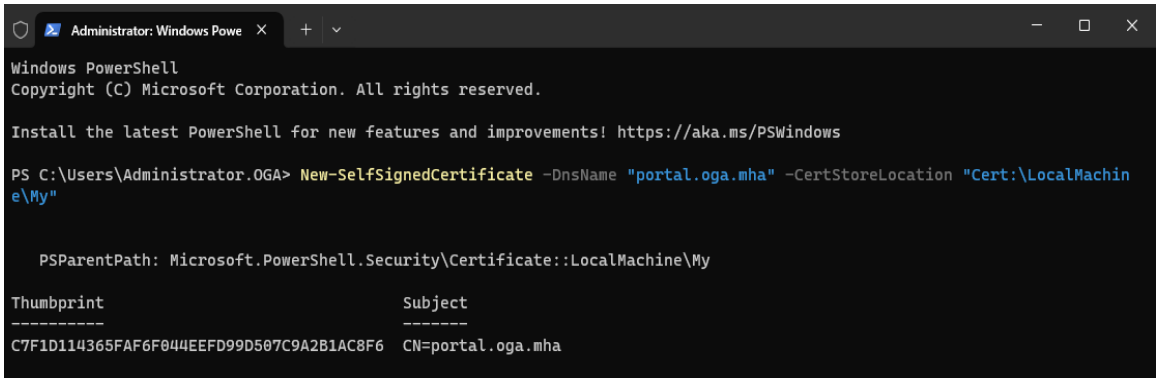
Configure DNS for portal > went to DC > dnsmgmt.msc > forward lookup zones > IP Address of 'OGfileIIS' (192.168.1.3)



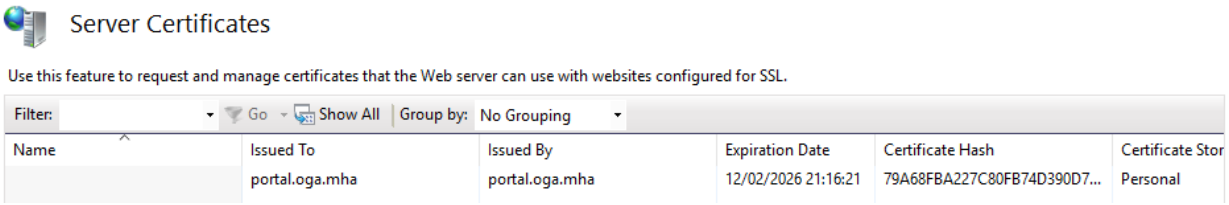
browsed http://portal.oga.mha



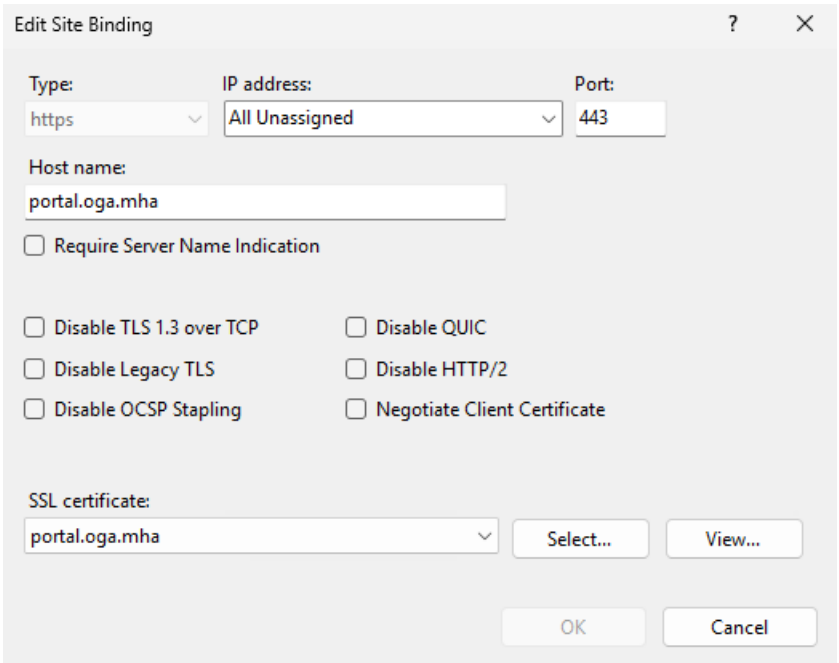
Create Self-Signed Certificate using PowerShell.



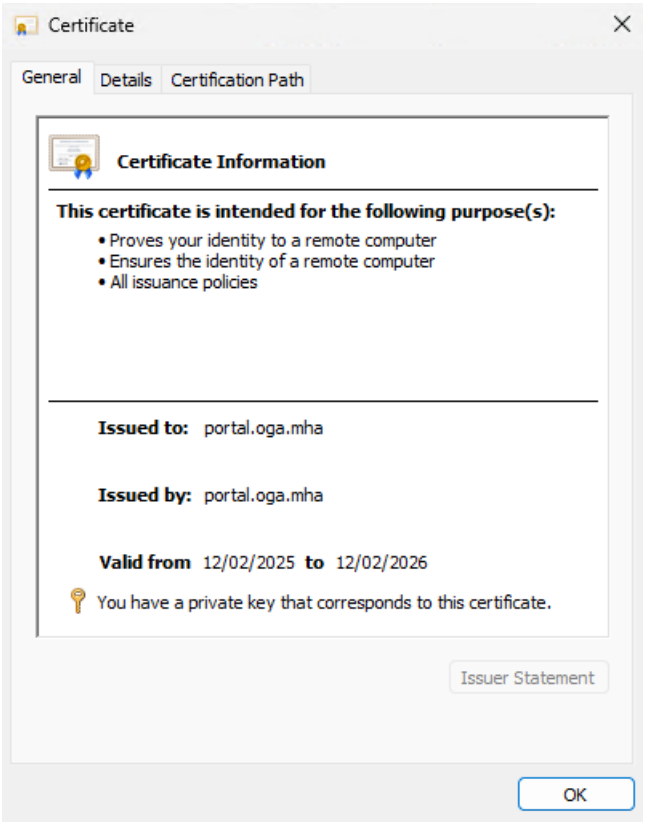
Import it to inetmgr > OGFILEIIS > 'Server Certificates'.



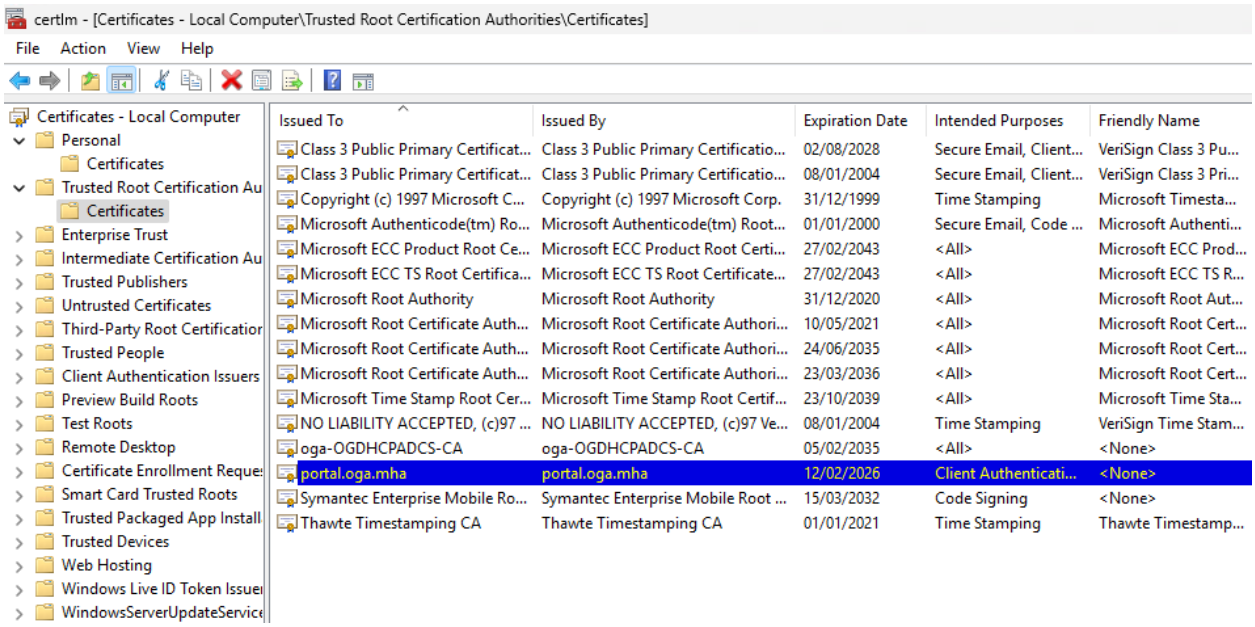
Added site binding > https://portal.oga.mha



'Copy to file' to the Self-Signed Certificate from 'Server Certificates' > export it to certlm.msc > certificates – local > Personal.



Trust the Certificate > imported to 'Trusted Root Certification Authorities'

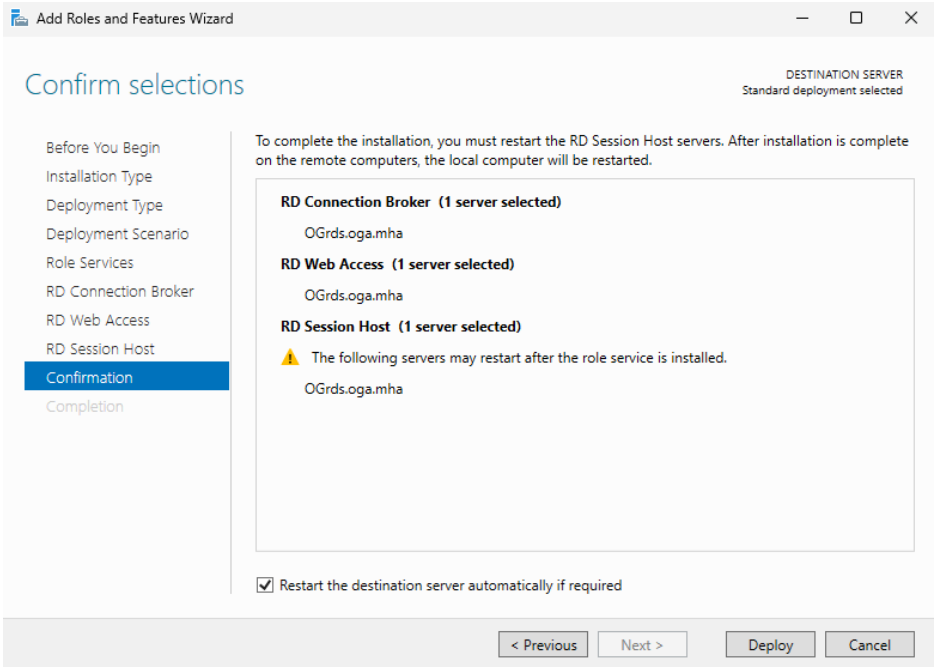


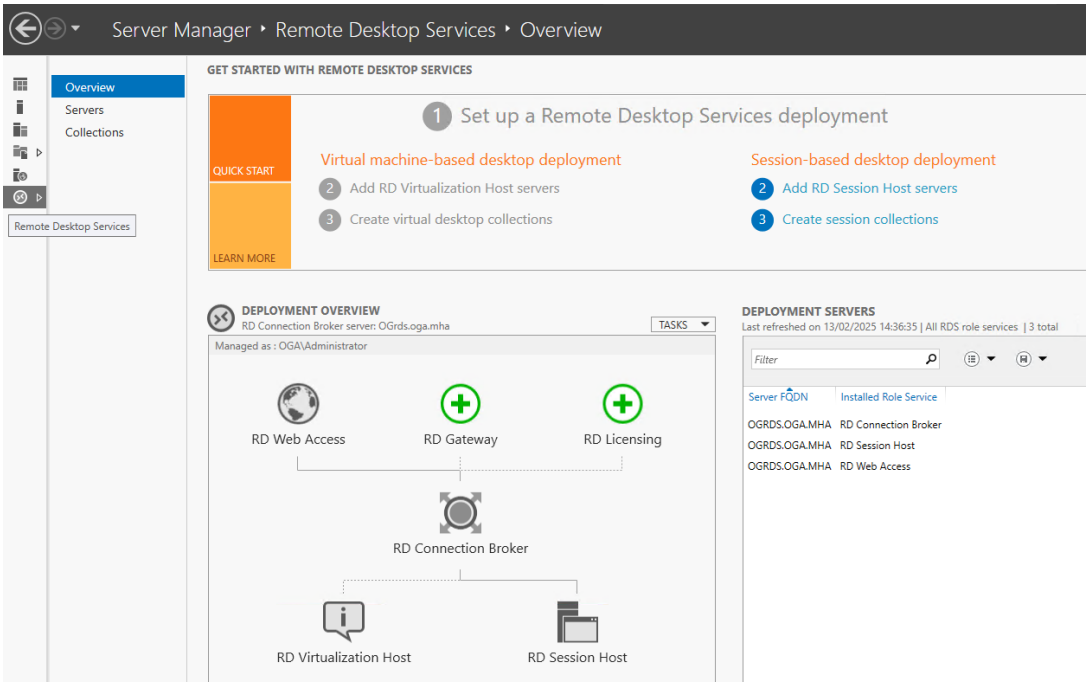
After, went to CMD > 'iisreset' > browsed https://portal.oga.mha

10. Management Station:

On my RDS server ('OGrds') I installed Remote Desktop Services.

Remote Desktop Services Installation > Standard Deployment > Session-based desktop deployment > RDS roles installation > Deploy.



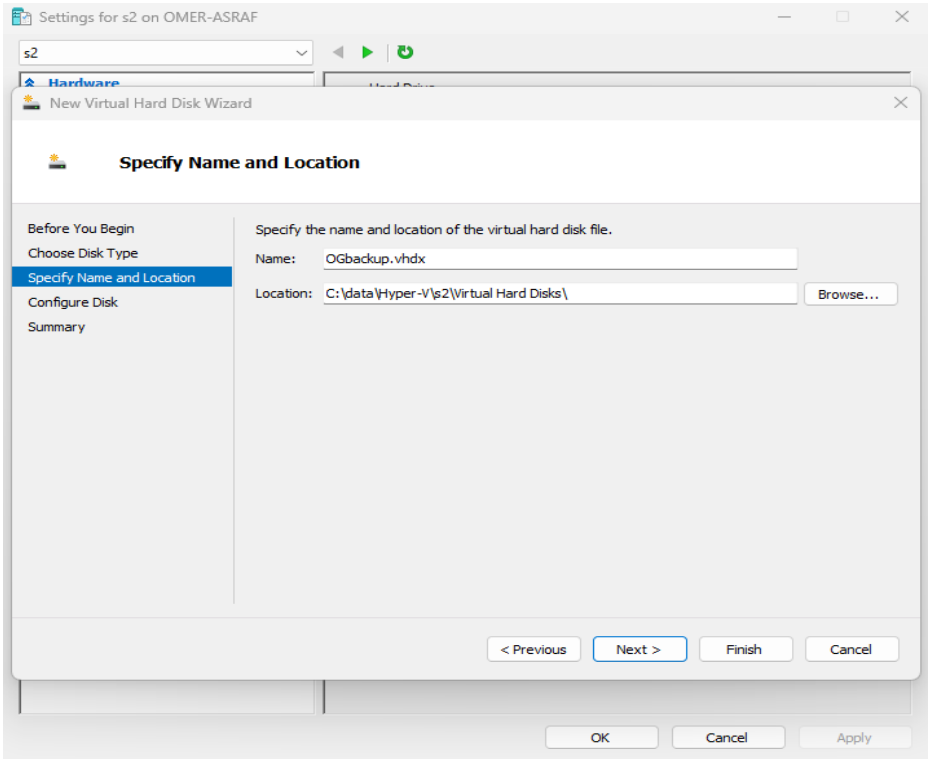


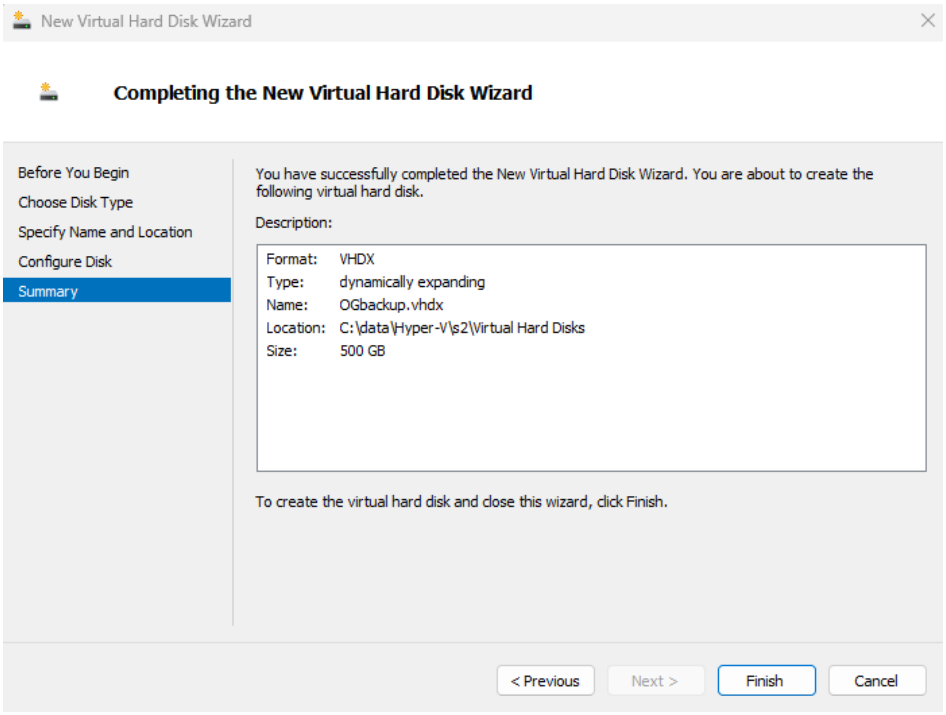
Edit Deployment Properties > RD Licensing > per user.

(The continuation of the section in the last page of the project).

11. Backup solution:

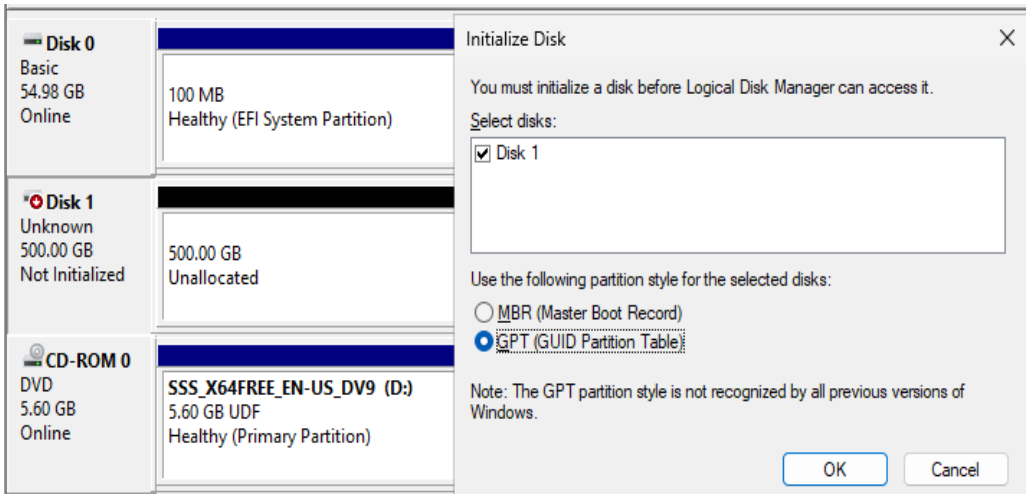
Added a New Virtual Disk (VHDX) to DC >



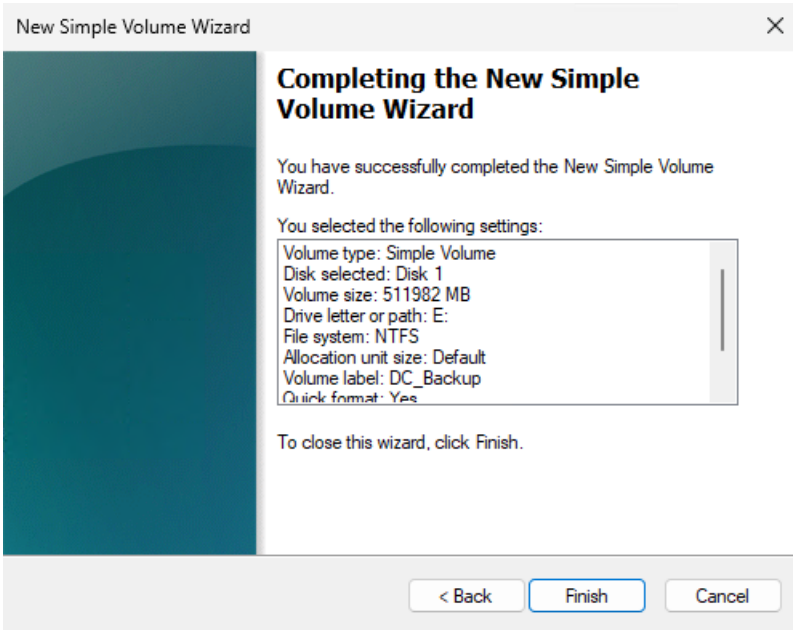


finish > apply > ok.

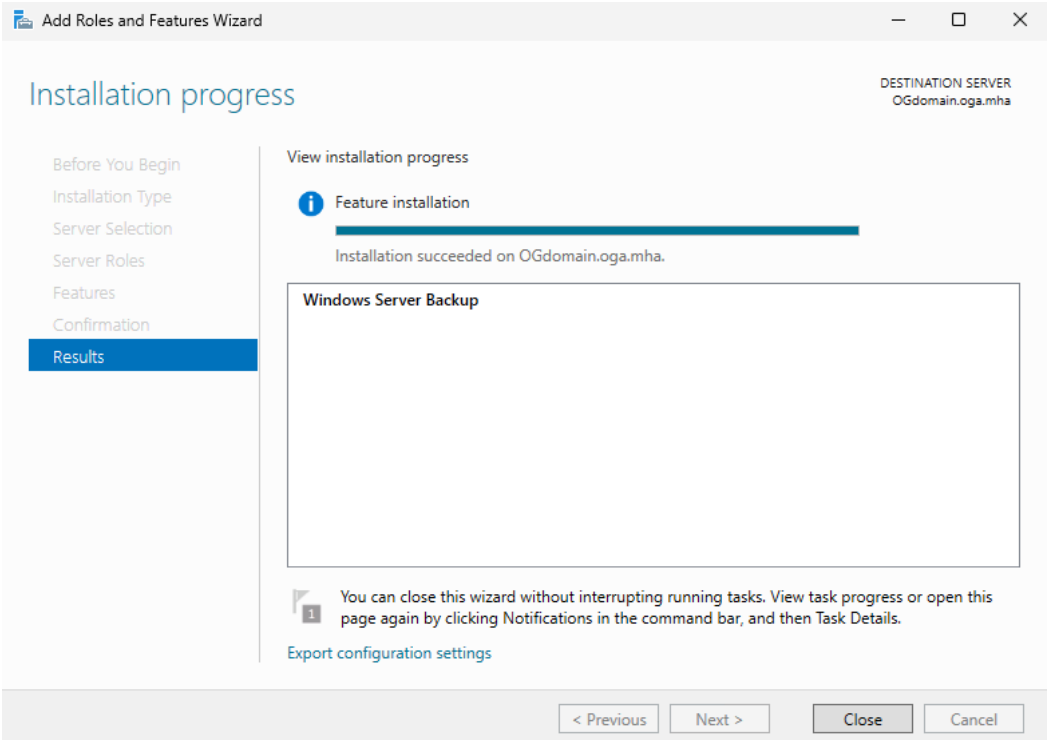
Initialize and Format the Disk in Windows > went into DC > diskmgmt.msc > Initialize Disk (the unknown) > GPT (GUID Partition Table) > ok.



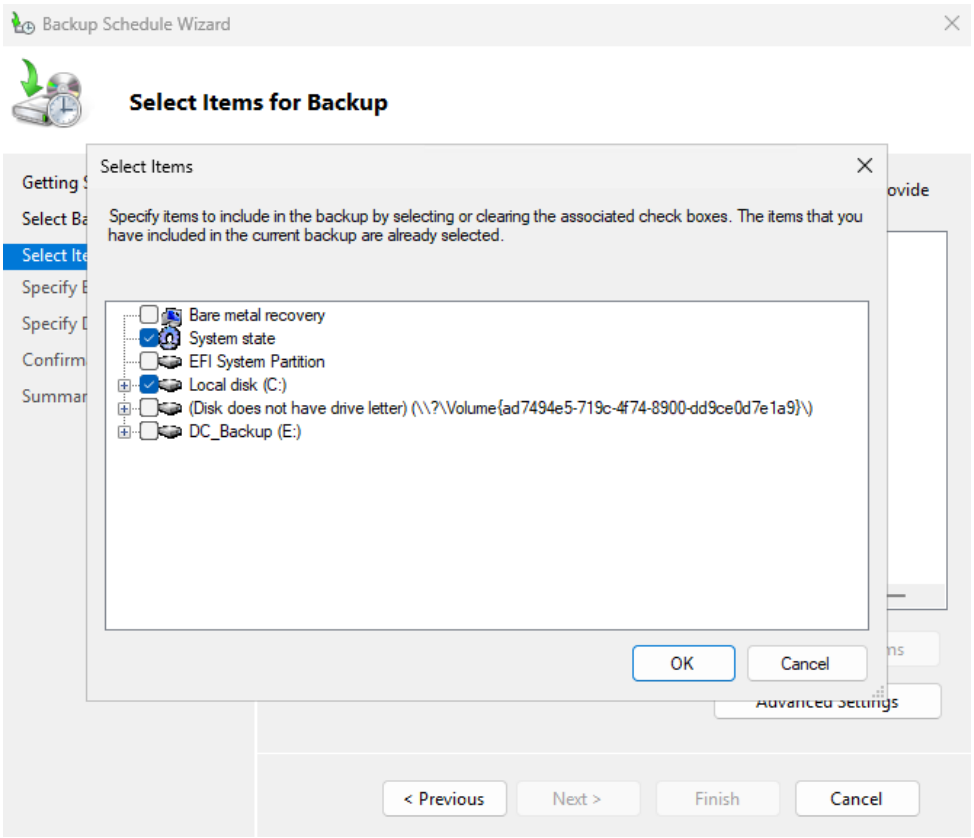
Unallocated space > New Simple Volume wizard > Finish.



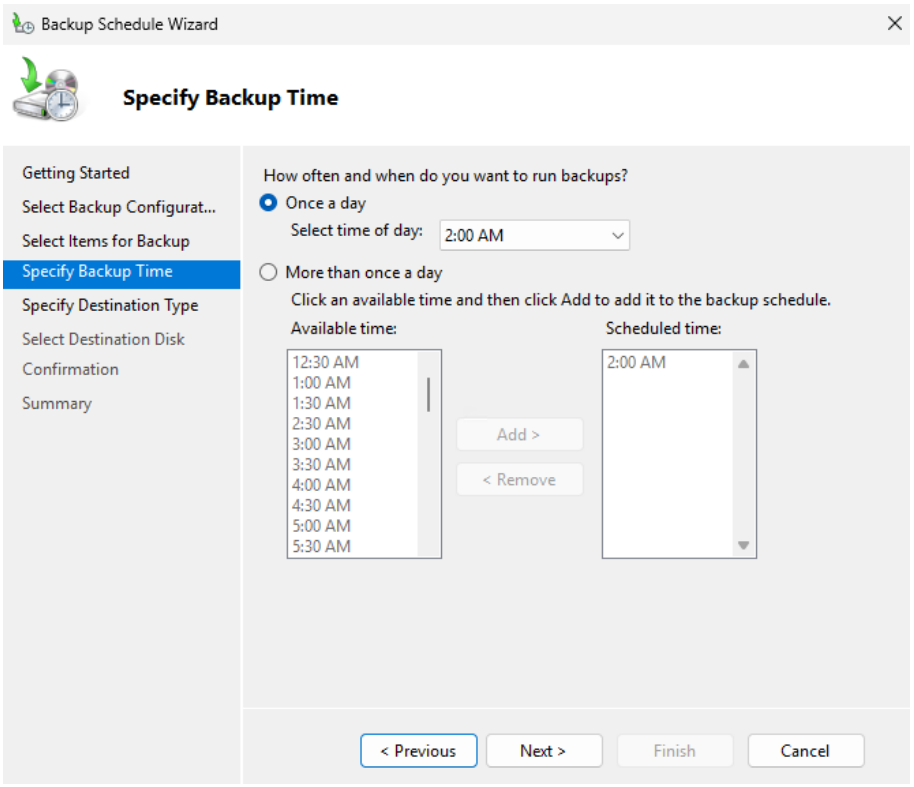
Now

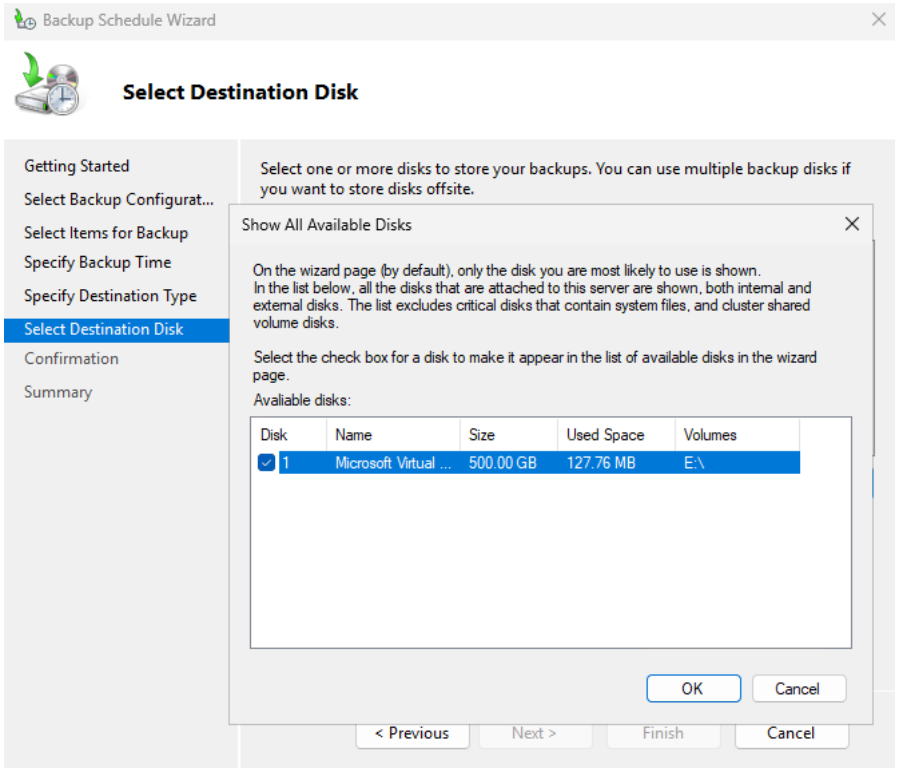


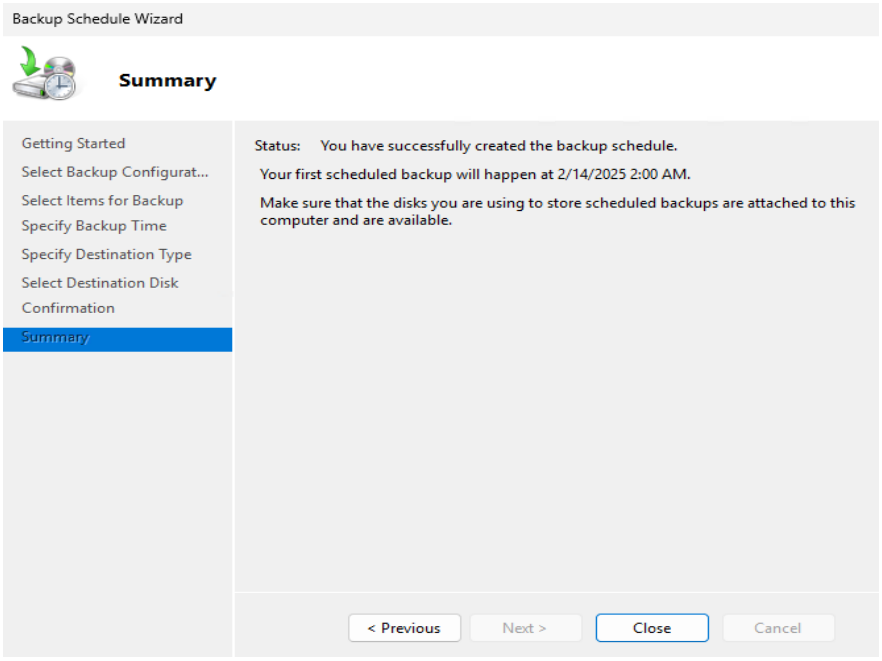
Windows Server Backup installation on DC (OGdomain)

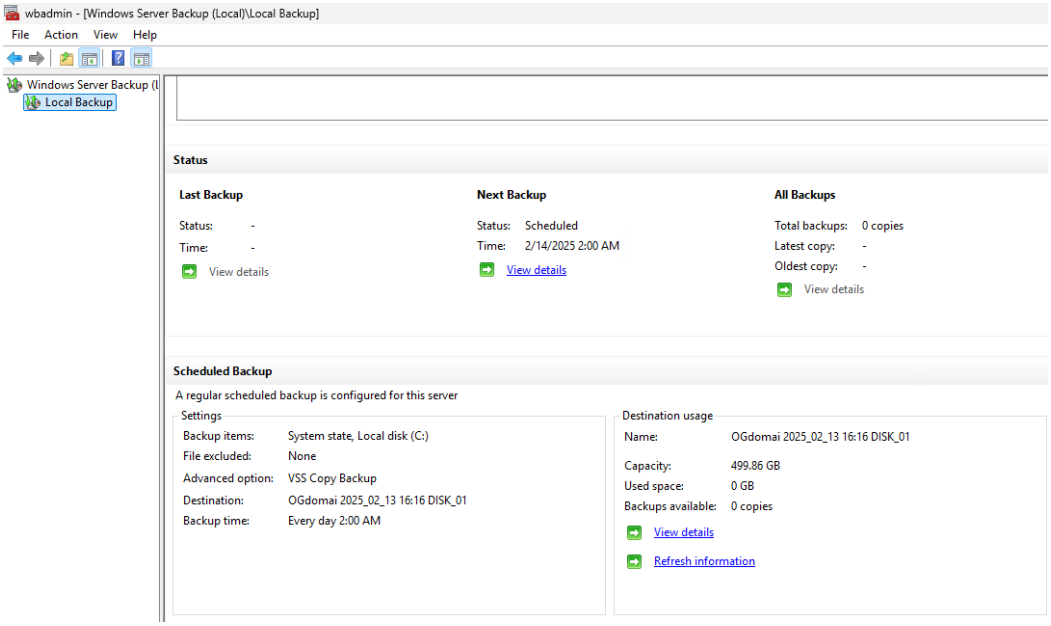


Configure Weekly Backup Schedule > wbadmin.msc > Local Backup > Backup Schedule… > Custom > etc.


Backup Schedule Wizard
Specify Backup Time
Getting Started
Select Backup Configurat...
Select Items for Backup
Specify Backup Time
Specify Destination Type
Select Destination Disk
Confirmation
Summary
How often and when do you want to run backups?
Once a day
Select time of day:
2:00 AM
More than once a day
Click an available time and then click Add to add it to the backup schedule.
Available time:
12:30 AM
1:00 AM
1:30 AM
2:30 AM
3:00 AM
3:30 AM
4:00 AM
4:30 AM
5:00 AM
5:30 AM
Add >
< Remove
Scheduled time:
2:00 AM
< Previous
Next >
Finish
Cancel


Backup Schedule Wizard
Select Destination Disk
Getting Started
Select Backup Configurat...
Select Items for Backup
Specify Backup Time
Specify Destination Type
Select Destination Disk
Confirmation
Summary
Select one or more disks to store your backups. You can use multiple backup disks if you want to store disks offsite.
Show All Available Disks
On the wizard page (by default), only the disk you are most likely to use is shown.
In the list below, all the disks that are attached to this server are shown, both internal and external disks. The list excludes critical disks that contain system files, and cluster shared volume disks.
Select the check box for a disk to make it appear in the list of available disks in the wizard page.
Avaliable disks:
Disk
Name
Size
Used Space
Volumes
1
Microsoft Virtual ...
500.00 GB
127.76 MB
E:\
OK
Cancel
< Previous
Next >
Finish
Cancel





O&G Computing Services backup solution based on:

- Windows Server Backup configured on DC.
- Weekly scheduled backups to a dedicated virtual backup disk (E:).
- Backup items include Active Directory, System State, OS, C:\ (System Drive).
- Primary Backup: Local backup on E:\ (DC_Backup).
- Secondary Backup: Replicate to a backup server in NY (in theory).

Section 10 continuing – Management Station:

Secure RDS with Group Policy > went to DC > gpmc.msc > Created a new GPO called 'Secure RDS Access Policy' > linked it to Privileged Operators OU > edit GPO > Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment > Added Privileged Operators to Allow log on through RDS > Added Domain Users to Deny log on through RDS.