

# 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:**

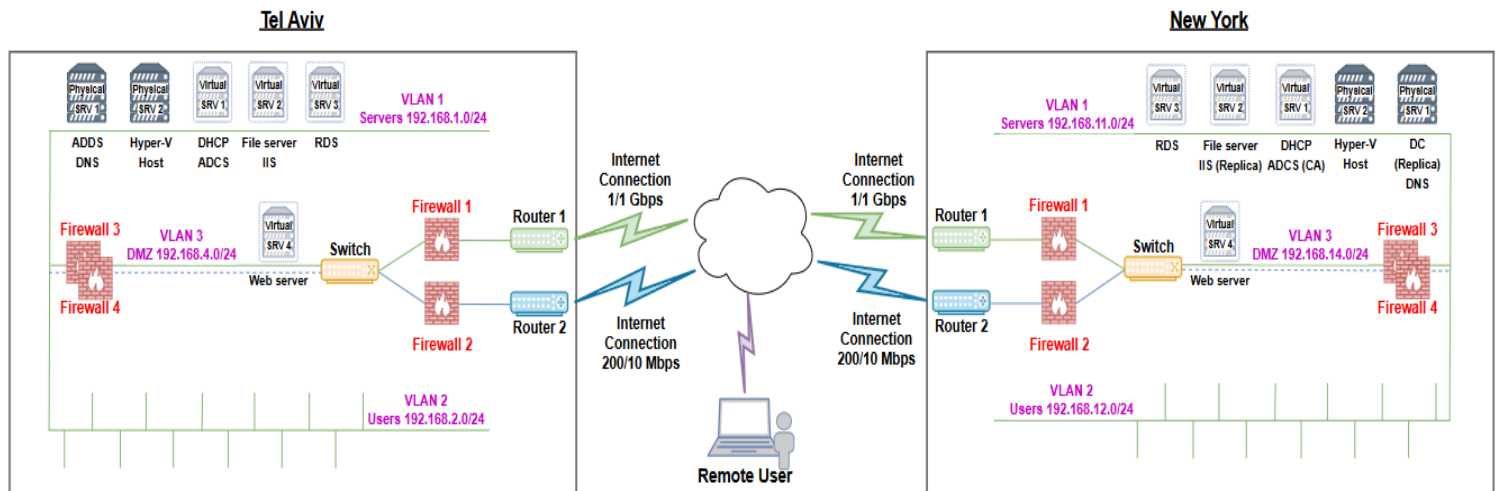
The company that began its journey in Haifa is currently moving to Tel Aviv to the new high-tech complex and establishing its new headquarters there.

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:

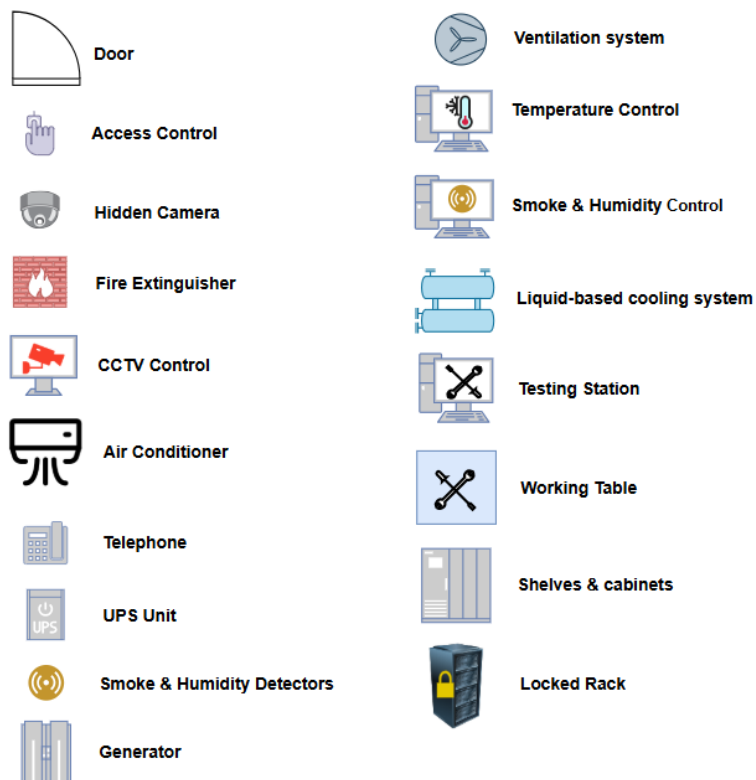
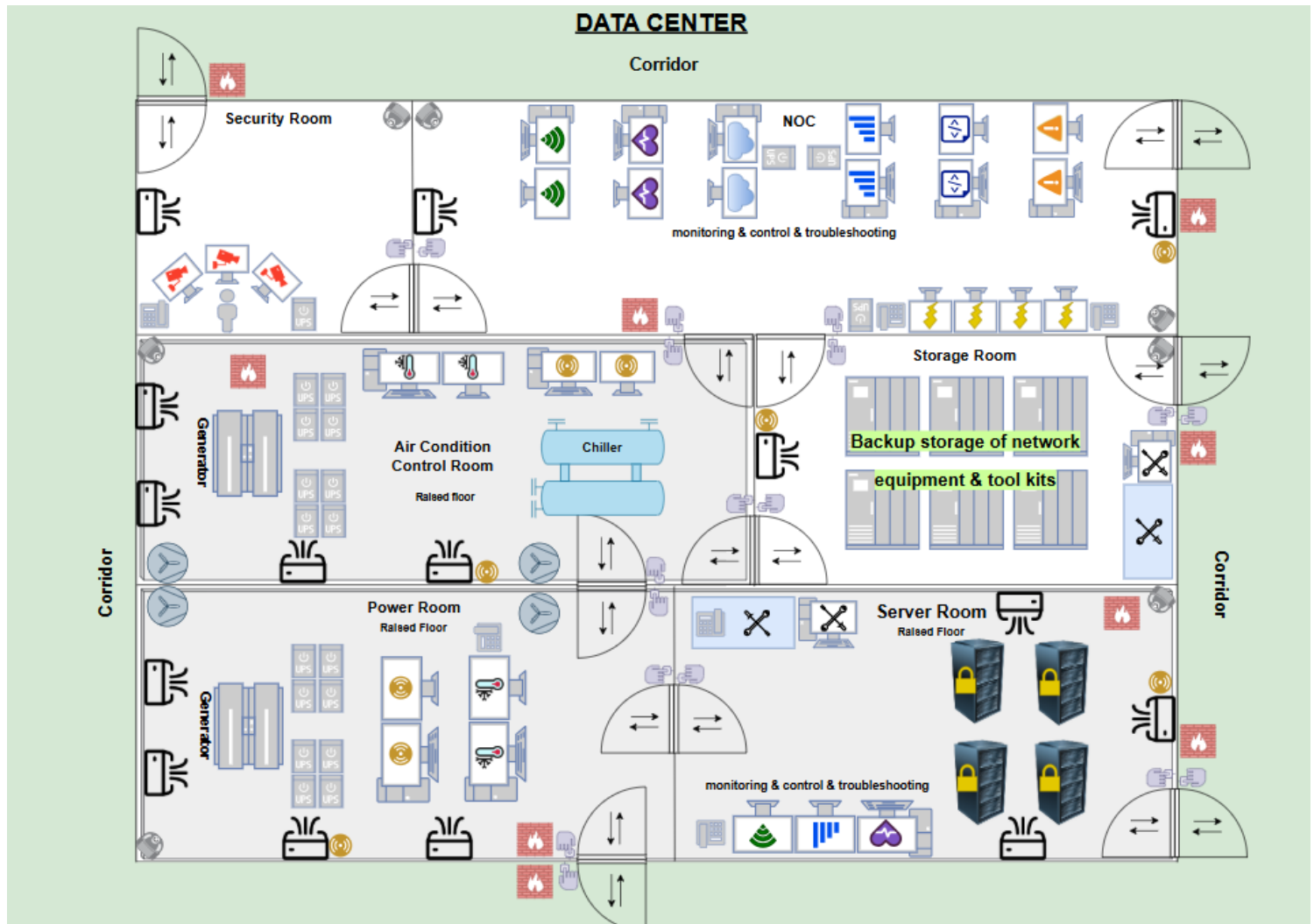


#### Tel Aviv:

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.

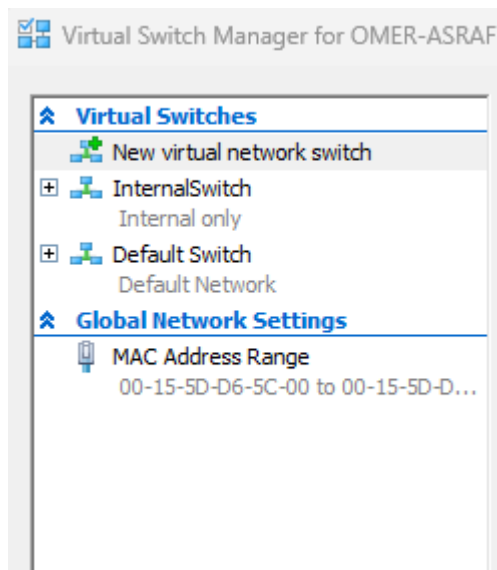
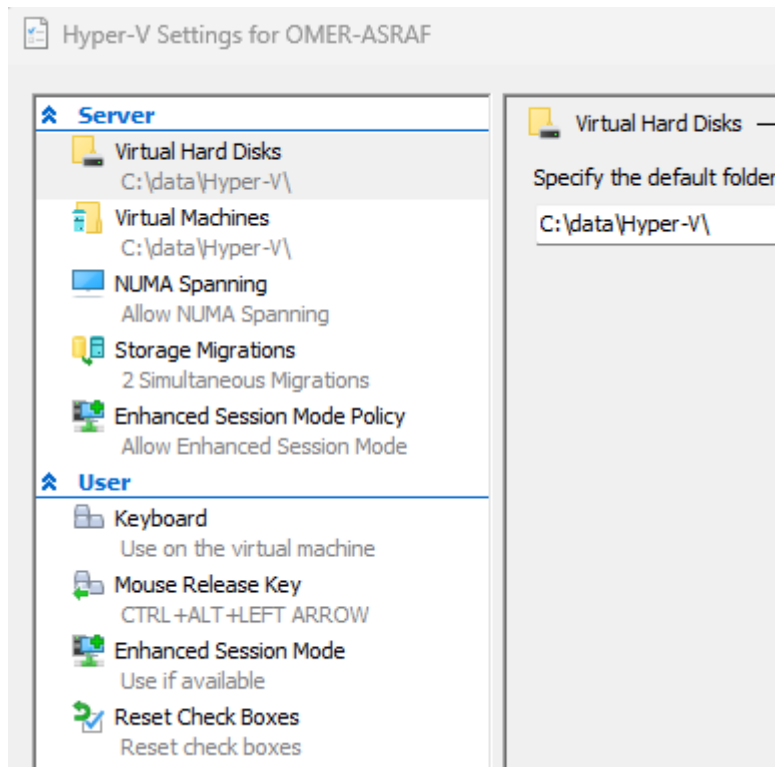
## Data Center:



### **Data Center Layout:**

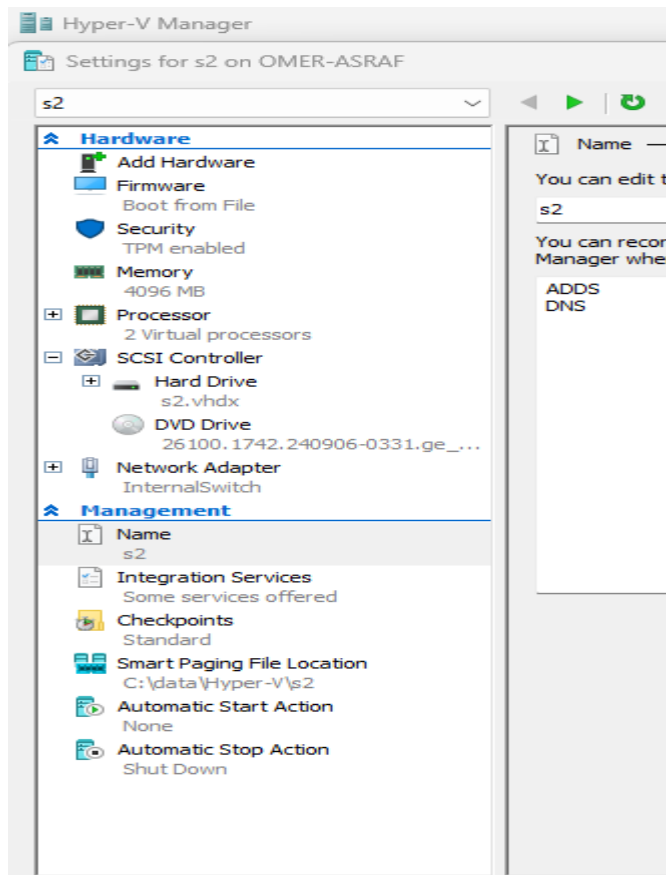
- Security Room – critical for controlling access and monitoring the overall environment. Includes access control, CCTV, emergency communication etc.
- NOC Room – monitoring and managing the data center's network, servers, and infrastructure. Includes stations for tracking systems health, traffic, alerts 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:



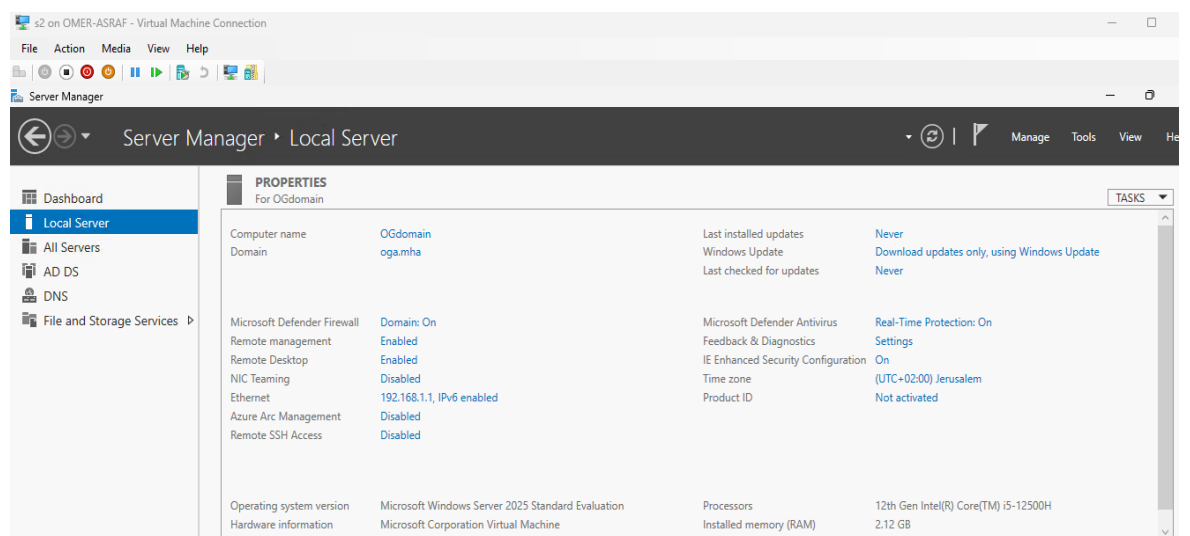
### 3. ADDS:

- 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

Active Directory Domain Services Configuration Wizard

## Deployment Configuration

TARGET SERVER  
OGdomain

**Deployment Configuration**

- Domain Controller Options
- DNS Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select the deployment operation

- ☐ Add a domain controller to an existing domain
- ☐ Add a new domain to an existing forest
- ☒ Add a new forest

Specify the domain information for this operation

Root domain name:

[More about deployment configurations](#)

< Previous   **Next >**   Install   Cancel

Active Directory Domain Services Configuration Wizard

## Review Options

**Review Options**

- Deployment Configuration
- Domain Controller Options
- DNS Options
- Additional Options
- Paths
- Review Options**
- Prerequisites Check
- Installation
- Results

tmpA7BA.tmp - Notepad

File Edit Format View Help

```
#
# Windows PowerShell script for AD DS Deployment
#

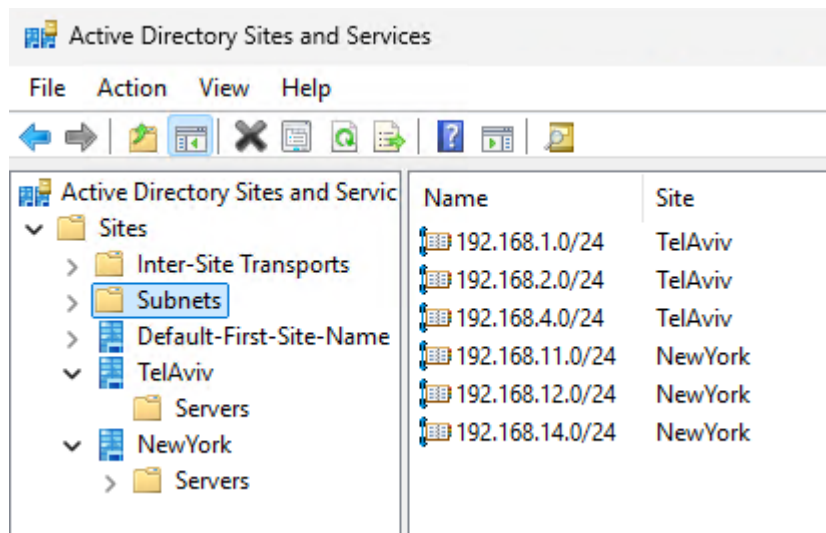
Import-Module ADDSDeployment
Install-ADDSForest `
-CreateDnsDelegation:$false `
-DatabasePath "C:\WINDOWS\NTDS" `
-DomainMode "Win2025" `
-DomainName "oga.mha" `
-DomainNetbiosName "OGA" `
-ForestMode "Win2025" `
-InstallDns:$true `
-LogPath "C:\WINDOWS\NTDS" `
-NoRebootOnCompletion:$false `
-SysvolPath "C:\WINDOWS\SYSVOL" `
-Force:$true
```



e. Initial AD configuration:

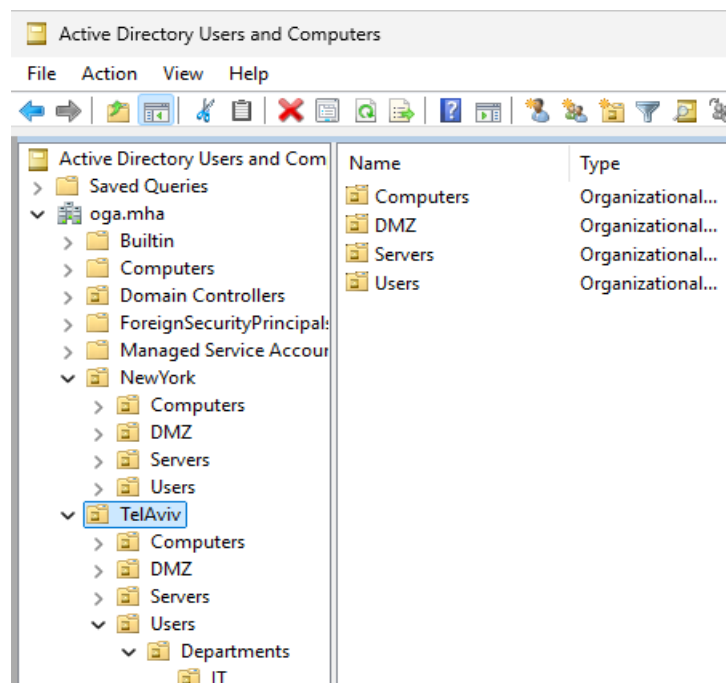
- Sites And Services:

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



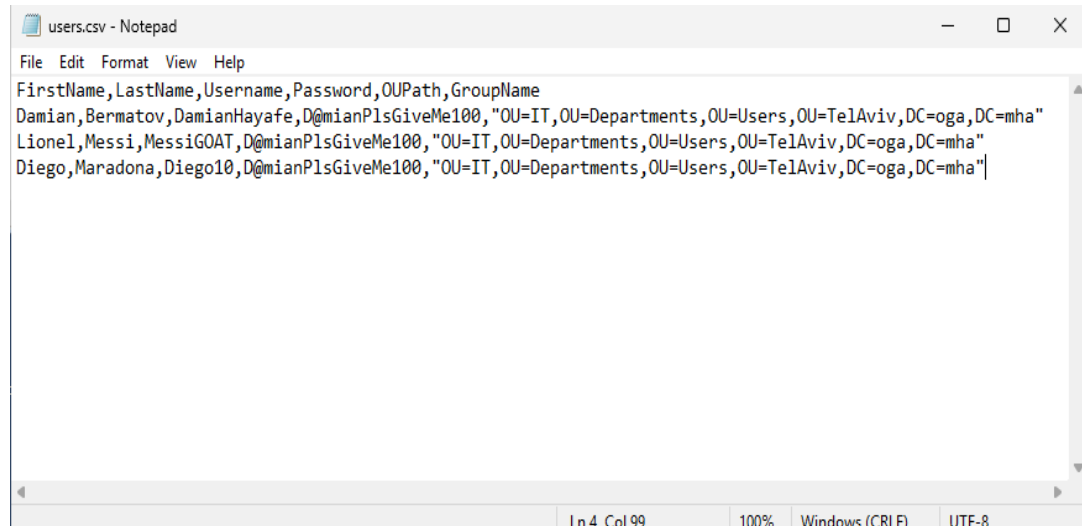
- OU Topology:

First, I'll show my topology sketch:



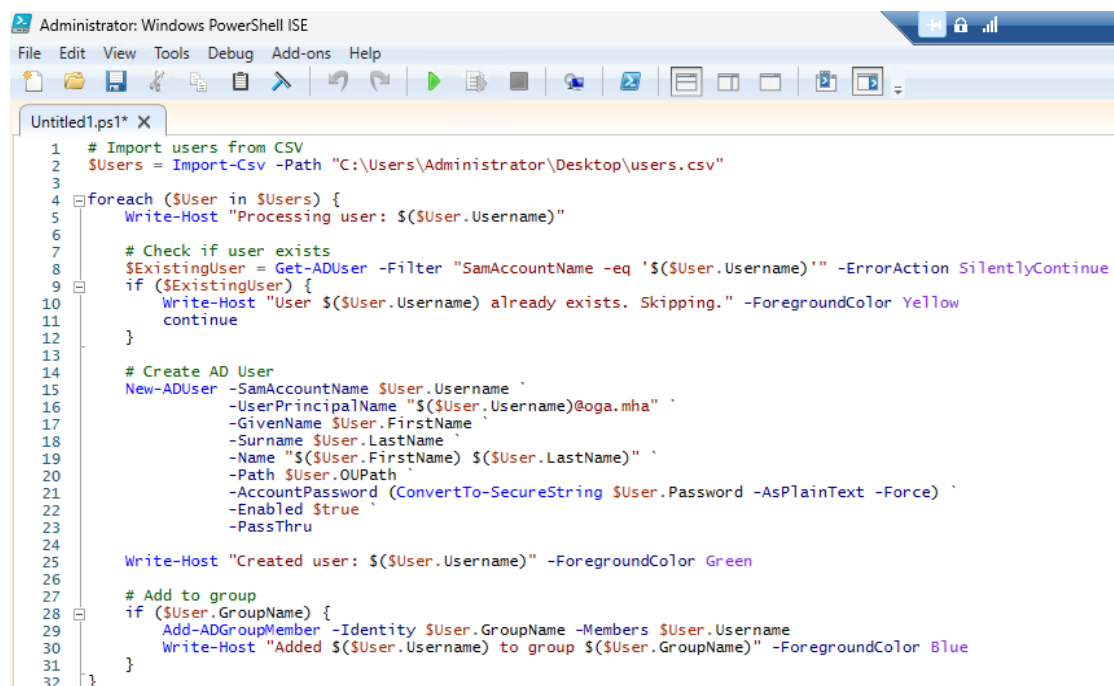
I added "Departments" inside Users and only included "IT" for the example.

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



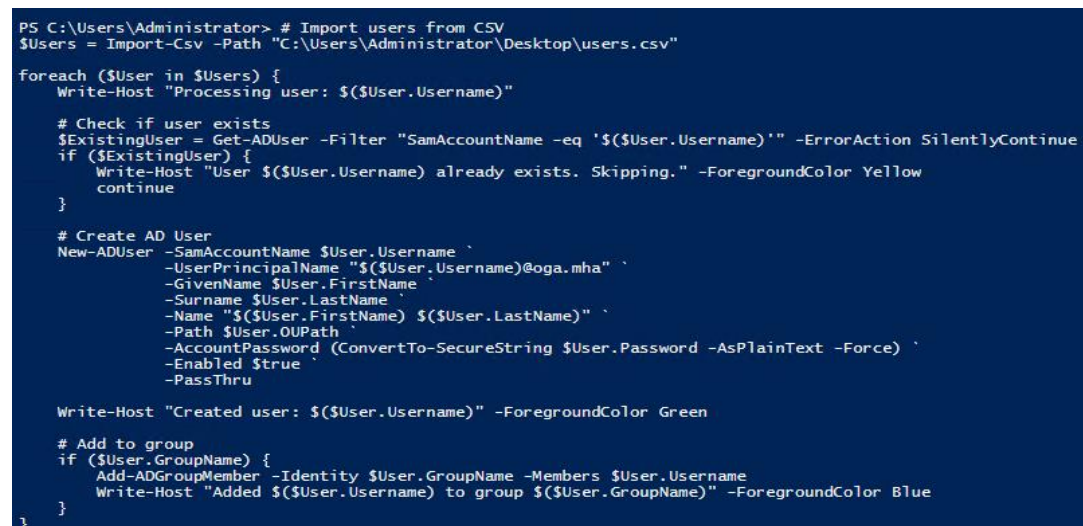
```
users.csv - Notepad
File Edit Format View Help
FirstName,LastName,Username>Password,OUPath,GroupName
Damian,Bermatov,DamianHayafe,D@mianPlsGiveMe100,"OU=IT,OU=Departments,OU=Users,OU=TelAviv,DC=oga,DC=mha"
Lionel,Messi,MessiGOAT,D@mianPlsGiveMe100,"OU=IT,OU=Departments,OU=Users,OU=TelAviv,DC=oga,DC=mha"
Diego,Maradona,Diego10,D@mianPlsGiveMe100,"OU=IT,OU=Departments,OU=Users,OU=TelAviv,DC=oga,DC=mha"
Ln 4. Col 99 100% Windows (CRLF) UTF-8
```

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



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1* X
1 # Import users from CSV
2 $Users = Import-Csv -Path "C:\Users\Administrator\Desktop\users.csv"
3
4 foreach ($User in $Users) {
5     Write-Host "Processing user: $($User.Username)"
6
7     # Check if user exists
8     $ExistingUser = Get-ADUser -Filter "SamAccountName -eq '$($User.Username)'" -ErrorAction SilentlyContinue
9     if ($ExistingUser) {
10         Write-Host "User $($User.Username) already exists. Skipping." -ForegroundColor Yellow
11         continue
12     }
13
14     # Create AD User
15     New-ADUser -SamAccountName $User.Username `
16         -UserPrincipalName "$($User.Username)@oga.mha" `
17         -GivenName $User.FirstName `
18         -Surname $User.LastName `
19         -Name "$($User.FirstName) $($User.LastName)" `
20         -Path $User.OUPath `
21         -AccountPassword (ConvertTo-SecureString $User.Password -AsPlainText -Force) `
22         -Enabled $true `
23         -PassThru
24
25     Write-Host "Created user: $($User.Username)" -ForegroundColor Green
26
27     # Add to group
28     if ($User.GroupName) {
29         Add-ADGroupMember -Identity $User.GroupName -Members $User.Username
30         Write-Host "Added $($User.Username) to group $($User.GroupName)" -ForegroundColor Blue
31     }
32 }
```

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



```
PS C:\Users\Administrator> # Import users from CSV
PSUsers = Import-Csv -Path "C:\Users\Administrator\Desktop\users.csv"

foreach ($User in $Users) {
    Write-Host "Processing user: $($User.Username)"

    # Check if user exists
    $ExistingUser = Get-ADUser -Filter "SamAccountName -eq '$($User.Username)'" -ErrorAction SilentlyContinue
    if ($ExistingUser) {
        Write-Host "User $($User.Username) already exists. Skipping." -ForegroundColor Yellow
        continue
    }

    # Create AD User
    New-ADUser -SamAccountName $User.Username `
        -UserPrincipalName "$($User.Username)@oga.mha" `
        -GivenName $User.FirstName `
        -Surname $User.LastName `
        -Name "$($User.FirstName) $($User.LastName)" `
        -Path $User.OUPath `
        -AccountPassword (ConvertTo-SecureString $User.Password -AsPlainText -Force) `
        -Enabled $true `
        -PassThru

    Write-Host "Created user: $($User.Username)" -ForegroundColor Green

    # Add to group
    if ($User.GroupName) {
        Add-ADGroupMember -Identity $User.GroupName -Members $User.Username
        Write-Host "Added $($User.Username) to group $($User.GroupName)" -ForegroundColor Blue
    }
}
```

(2/2):

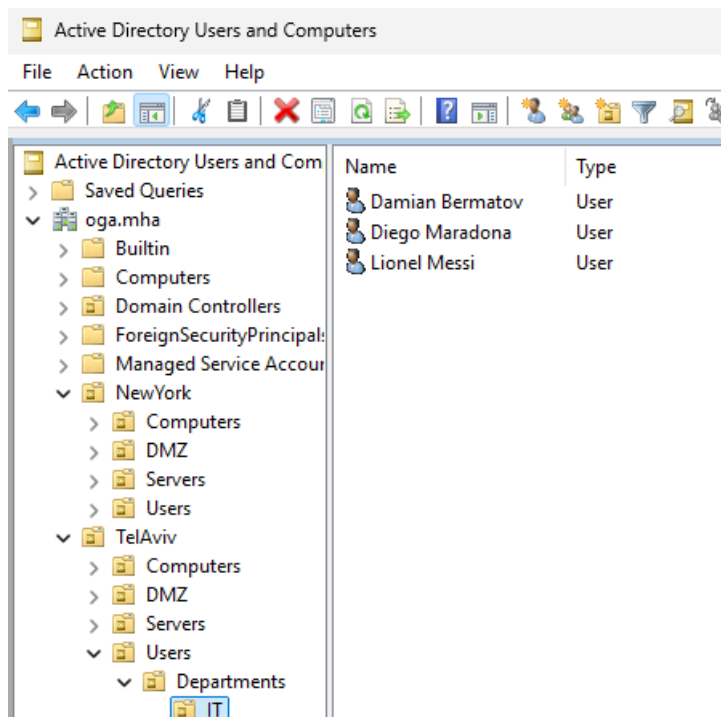
```
DistinguishedName : CN=Damian
                  : Bermatov,OU=IT,OU=Departments,OU=Users,OU=TelAviv,DC=oga,DC=mha
Enabled           : True
GivenName        : Damian
Name             : Damian Bermatov
ObjectClass      : user
ObjectGUID       : 205e8d26-a749-4d8b-9c69-83f14895a484
SamAccountName   : 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

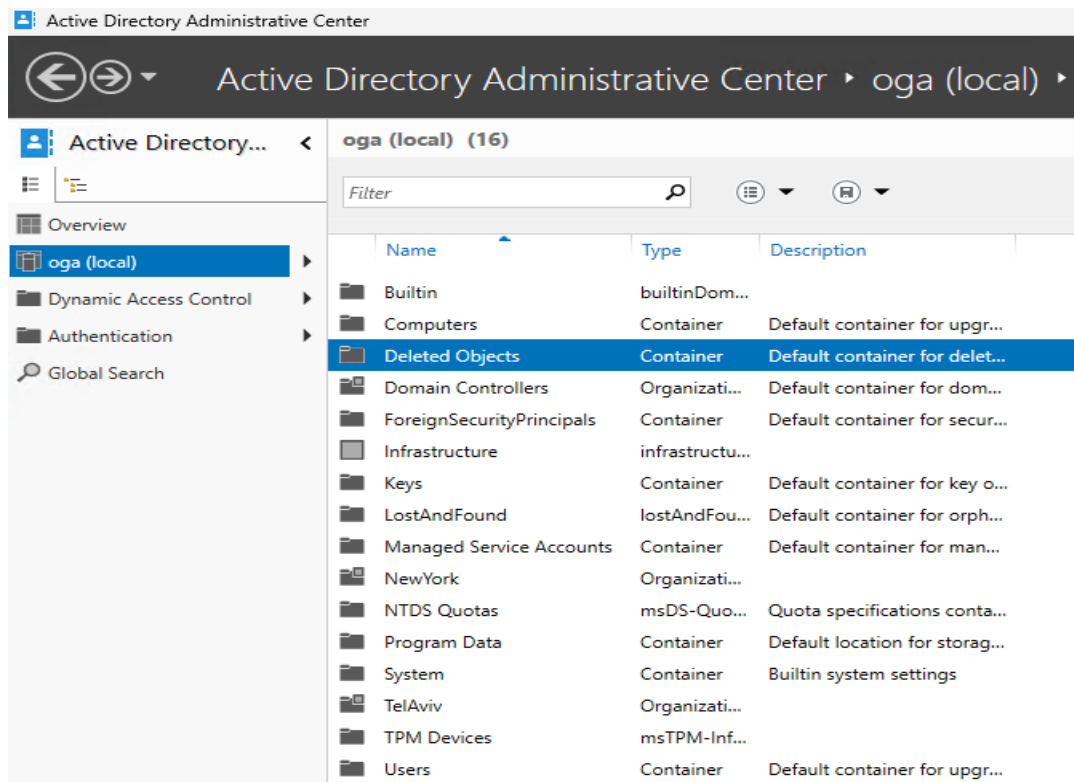
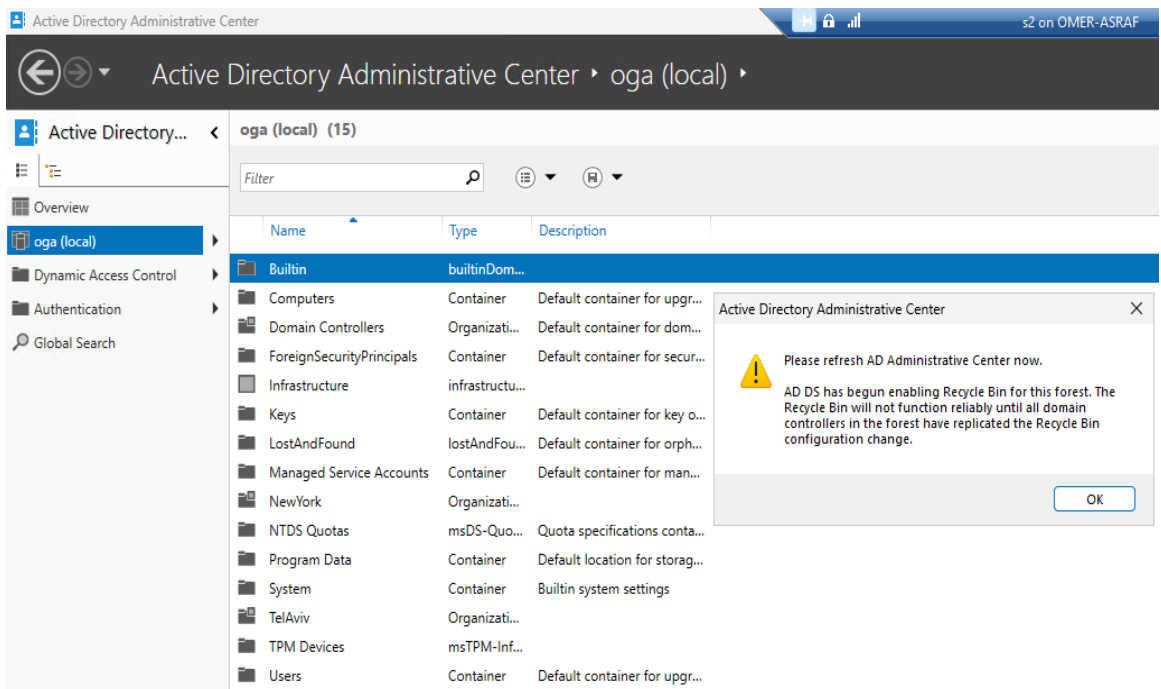
Created user: Diego10
```

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



Enable AD Recycle Bin:

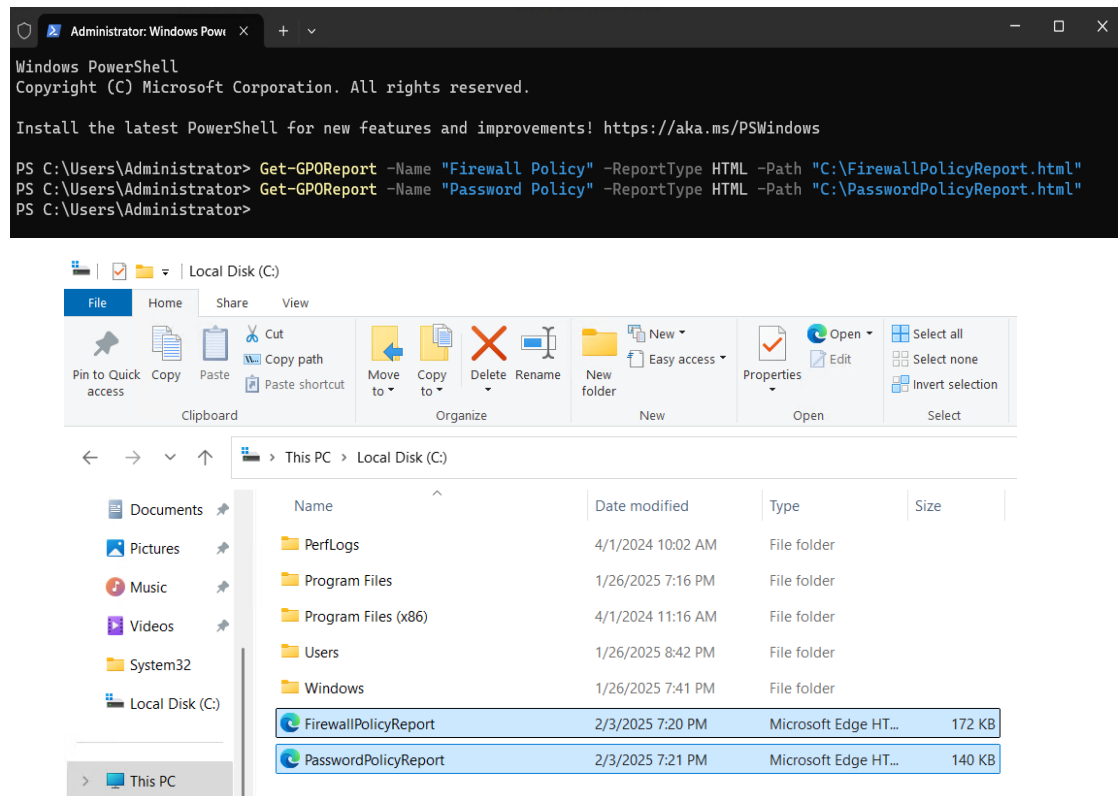
go to dsac.exe > Right click on my domain > "Enable Recycle Bin" > Click "Ok" > refresh the AD Administrative Center.



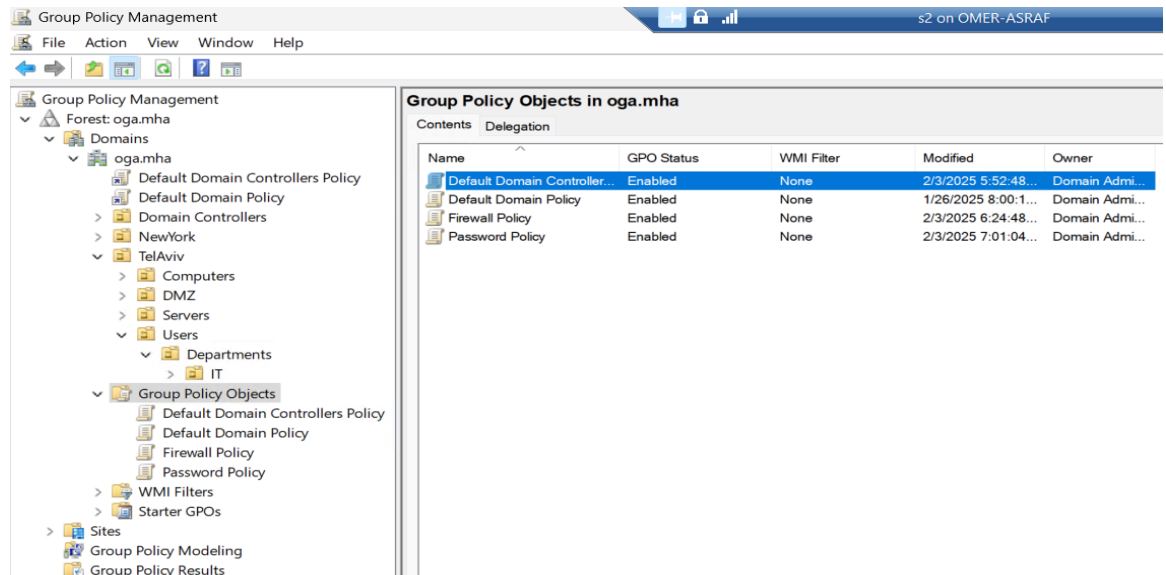
Now I can restore deleted AD objects (users, groups, OUs, etc.)

- 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.

Firewall Policy

Data collected on: 2/3/2025 7:20:48 PM

General

Details

Domain	oga.mha
Owner	OGA\Domain Admins
Created	2/3/2025 6:12:44 PM
Modified	2/3/2025 6:24:48 PM
User Revisions	0 (AD), 0 (SYSVOL)
Computer Revisions	15 (AD), 15 (SYSVOL)
Unique ID	{814038D1-89A6-4E58-A471-83D9E9F792C6}
GPO Status	Enabled

Links

Security Filtering

Delegation

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Windows Firewall with Advanced Security

Global Settings

Domain Profile Settings

Policy	Setting
Firewall state	On
Inbound connections	Block
Outbound connections	Allow
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	Not Configured

Password Policy

Data collected on: 2/3/2025 7:21:15 PM

General

Details

Domain	oga.mha
Owner	OGA\Domain Admins
Created	2/3/2025 6:45:46 PM
Modified	2/3/2025 7:01:04 PM
User Revisions	0 (AD), 0 (SYSVOL)
Computer Revisions	22 (AD), 22 (SYSVOL)
Unique ID	{92A750A6-A60F-4E18-B62A-3F12185AB6CE}
GPO Status	Enabled

Links

Security Filtering

Delegation

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	10 passwords remembered
Maximum password age	90 days
Minimum password age	30 days
Minimum password length	12 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

User Configuration (Enabled)

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.

The screenshot shows the 'DHCP Post-Install configuration wizard' window. The 'Authorization' tab is selected in the left sidebar. The main area contains the instruction: 'Specify the credentials to be used to authorize this DHCP server in AD DS.' There are three radio button options: 'Use the following user's credentials' (selected), 'Use alternate credentials', and 'Skip AD authorization'. Under the selected option, the 'User Name' field is populated with 'OGA\Administrator'. At the bottom of the window are buttons for '< Previous', 'Next >', 'Commit', and 'Cancel'.

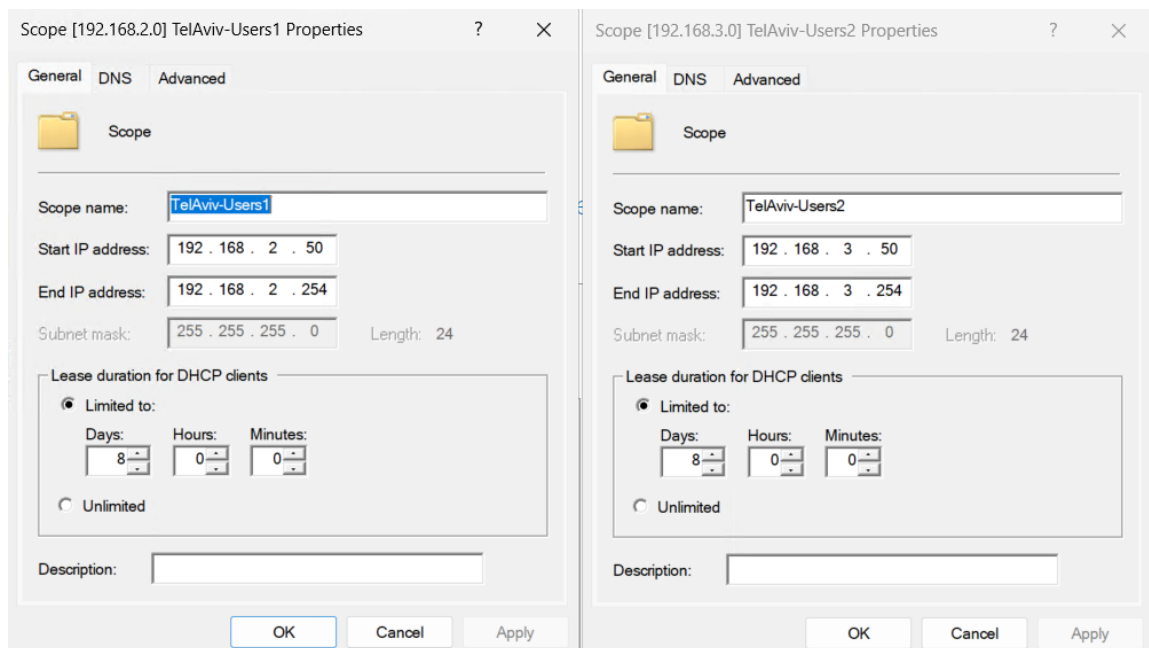
Now I can configure DHCP scopes for Users VLANs.

dhcpcgmt.msc > IPv4 > New Scope > etc.

The screenshot shows the 'DHCP' console window with the 'New Scope Wizard' open. The left pane shows the tree structure: DHCP > ogdhcpadcs.oga.mha > IPv4. The wizard has two main sections: 'IP Address Range' and 'Configuration settings for DHCP Server'. In the 'IP Address Range' section, the 'Start IP address' is '192.168.2.50' and the 'End IP address' is '192.168.2.254'. In the 'Configuration settings for DHCP Server' section, the 'Length' is '24' and the 'Subnet mask' is '255.255.255.0'. At the bottom of the wizard are buttons for '< Back', 'Next >', and 'Cancel'.

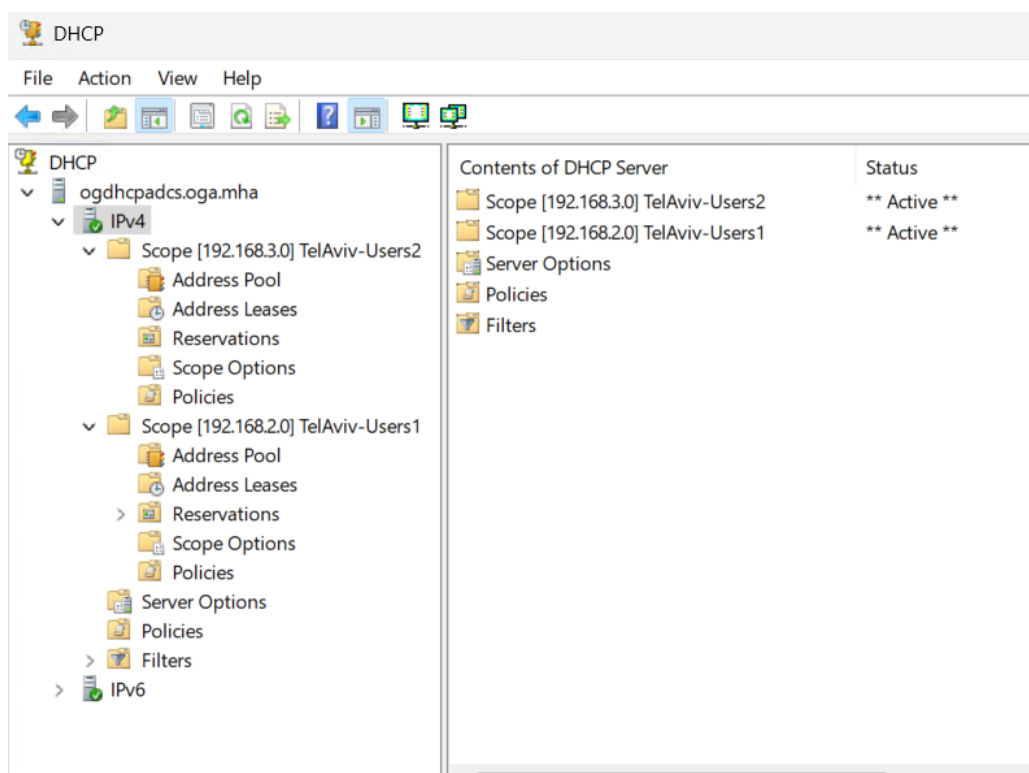
Lease Duration limited to 8 days for Tel Aviv Users.

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.

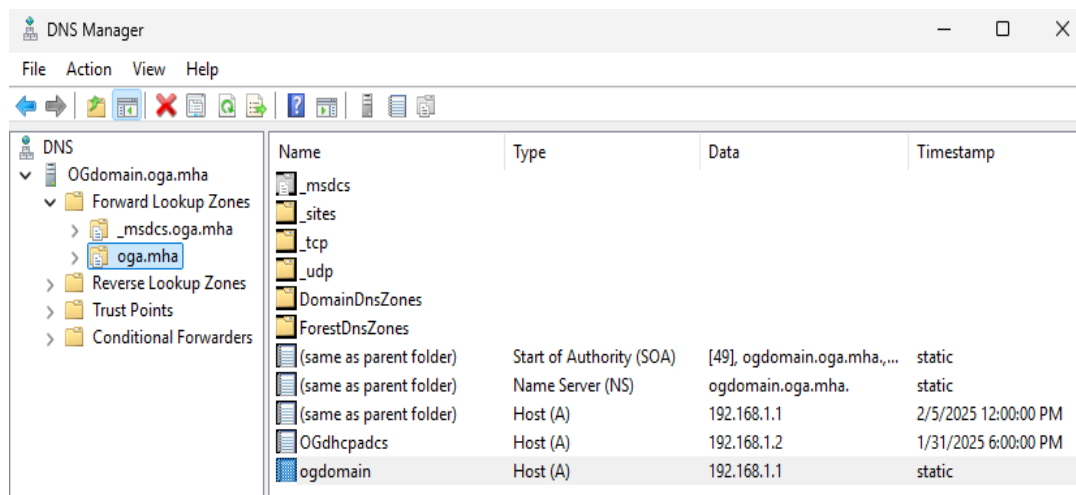
So my failover setup can be:

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'

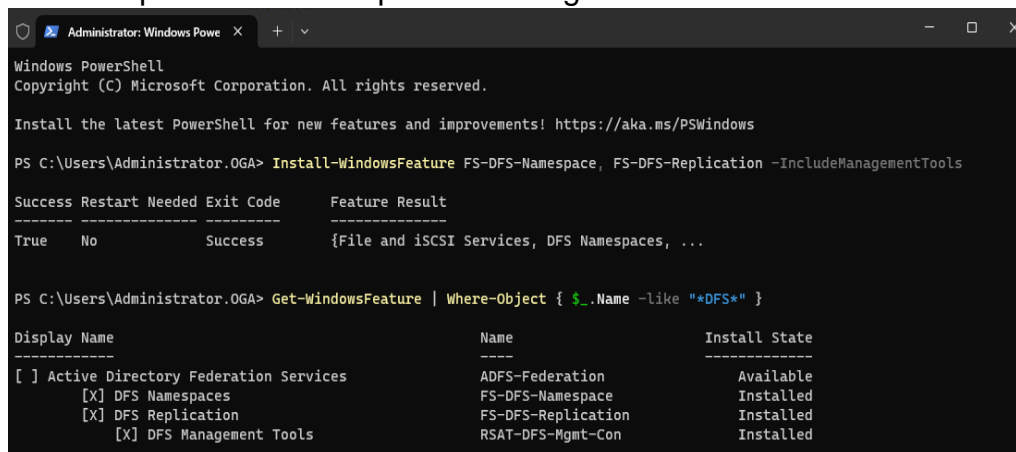
192.168.11.1 – New York DC (in theory)

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

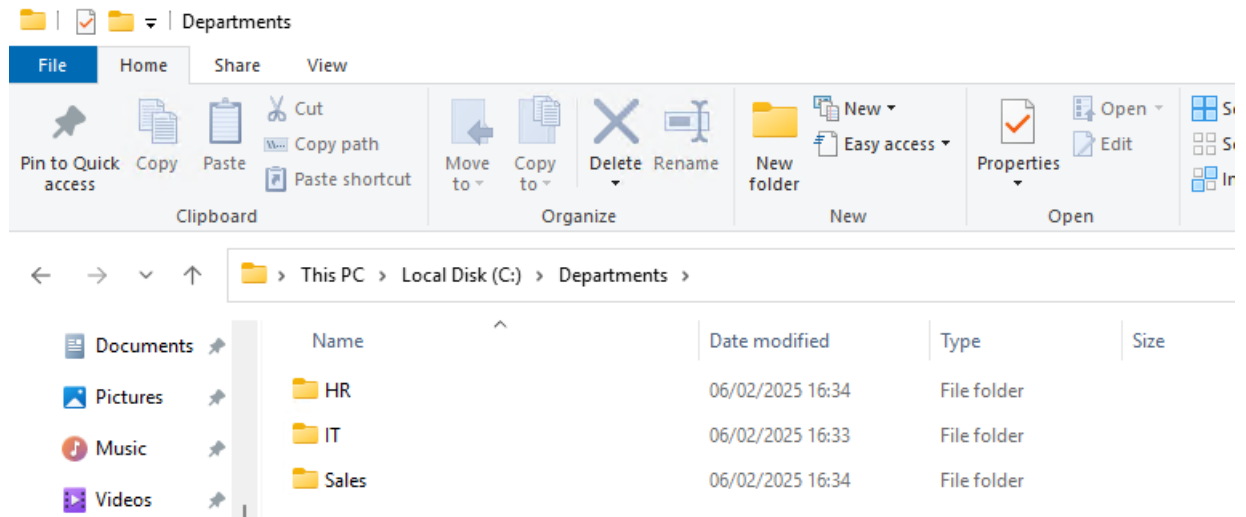
New York servers & clients: preferred 192.168.11.1, alternate 192.168.1.1 .

## 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.

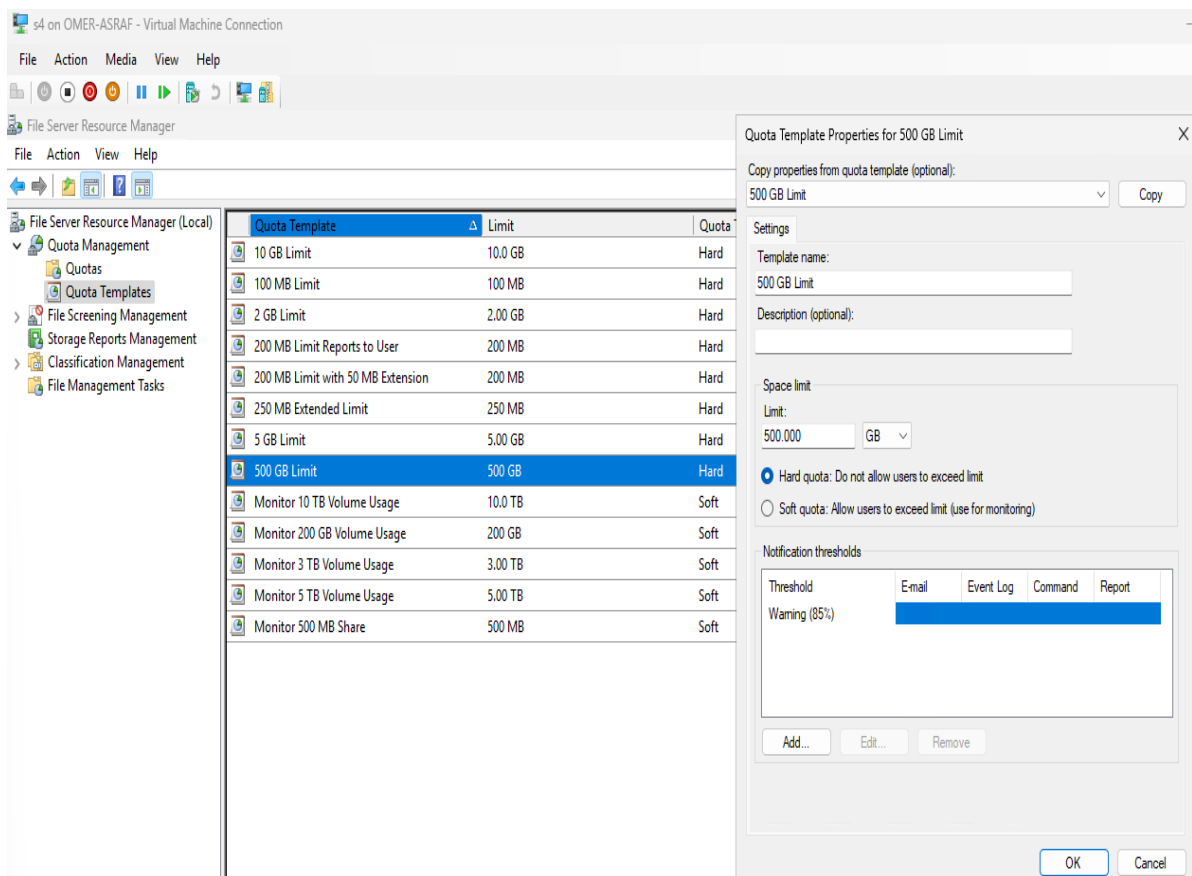


created folders for IT and HR departments for example.

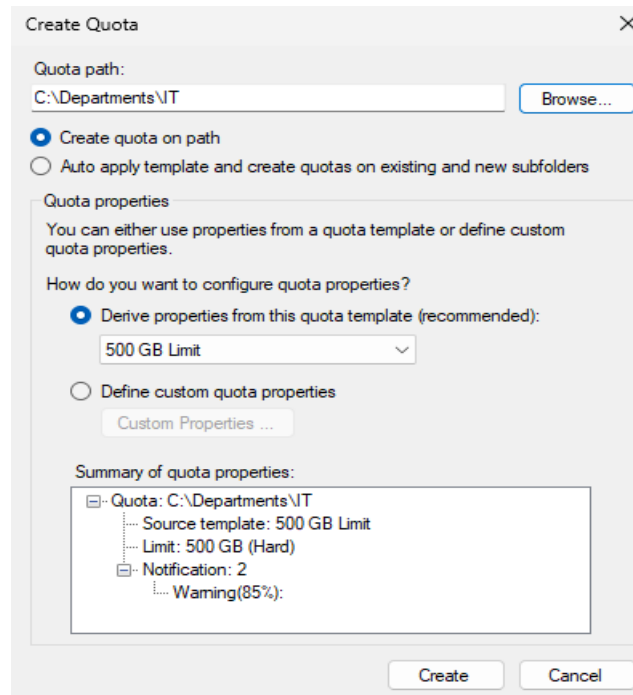


I had to install File Server Resource Manager to create a Quota Template for 500GB.

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



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

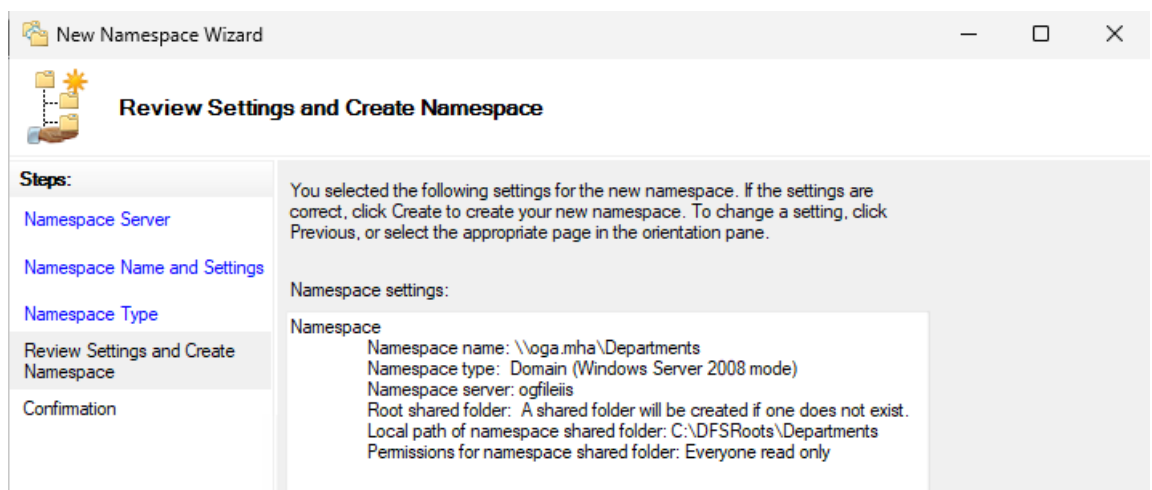


The 'Create Quota' dialog box is shown. The 'Quota path' is set to 'C:\Departments\IT'. The 'Create quota on path' radio button is selected. Under 'Quota properties', the option 'Derive properties from this quota template (recommended):' is selected, with a dropdown menu showing '500 GB Limit'. The 'Summary of quota properties' section shows a tree view with 'Quota: C:\Departments\IT' expanded, showing 'Source template: 500 GB Limit', 'Limit: 500 GB (Hard)', 'Notification: 2', and 'Warning(85%)'. 'Create' and 'Cancel' buttons are at the bottom.

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.



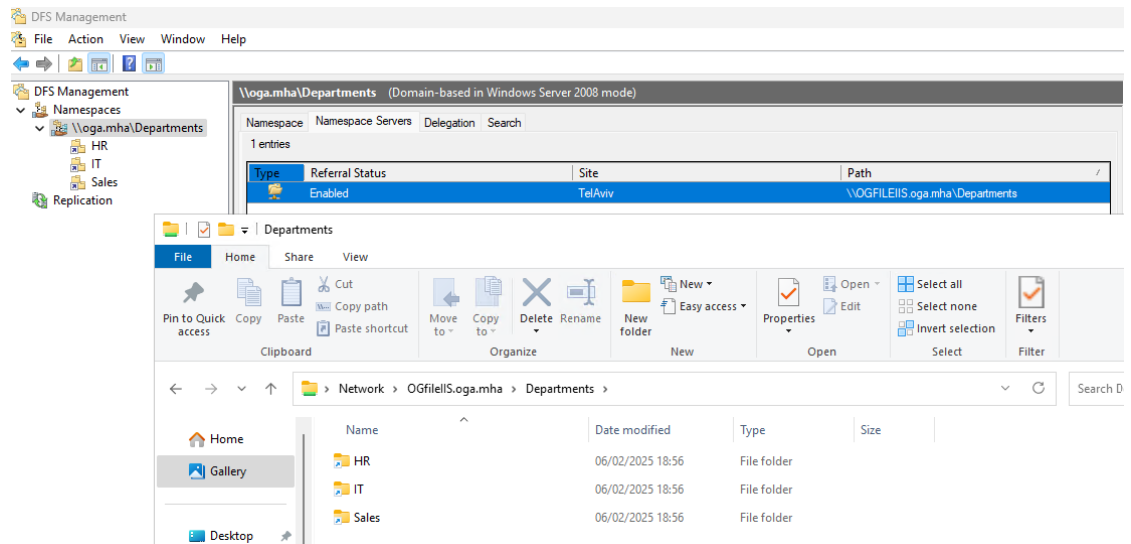
The 'New Namespace Wizard' is shown at the 'Review Settings and Create Namespace' step. The 'Steps' pane on the left lists: Namespace Server, Namespace Name and Settings, Namespace Type, Review Settings and Create Namespace (selected), and Confirmation. The main area shows the following settings:

Namespace settings:

Namespace

- Namespace name: \\oga.mha\Departments
- Namespace type: Domain (Windows Server 2008 mode)
- Namespace server: ogfileiis
- Root shared folder: A shared folder will be created if one does not exist.
- Local path of namespace shared folder: C:\DFSRoots\Departments
- Permissions for namespace shared folder: Everyone read only

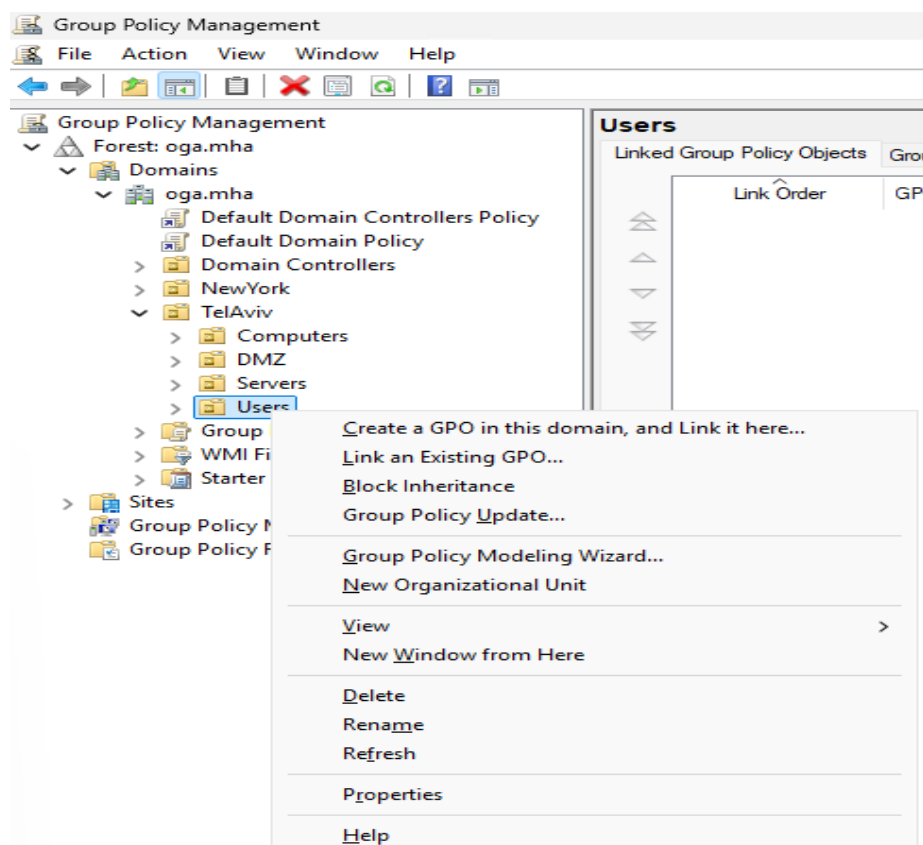
Add folder targets > [path](#) > adding 'IT' & 'HR' & 'Sales'



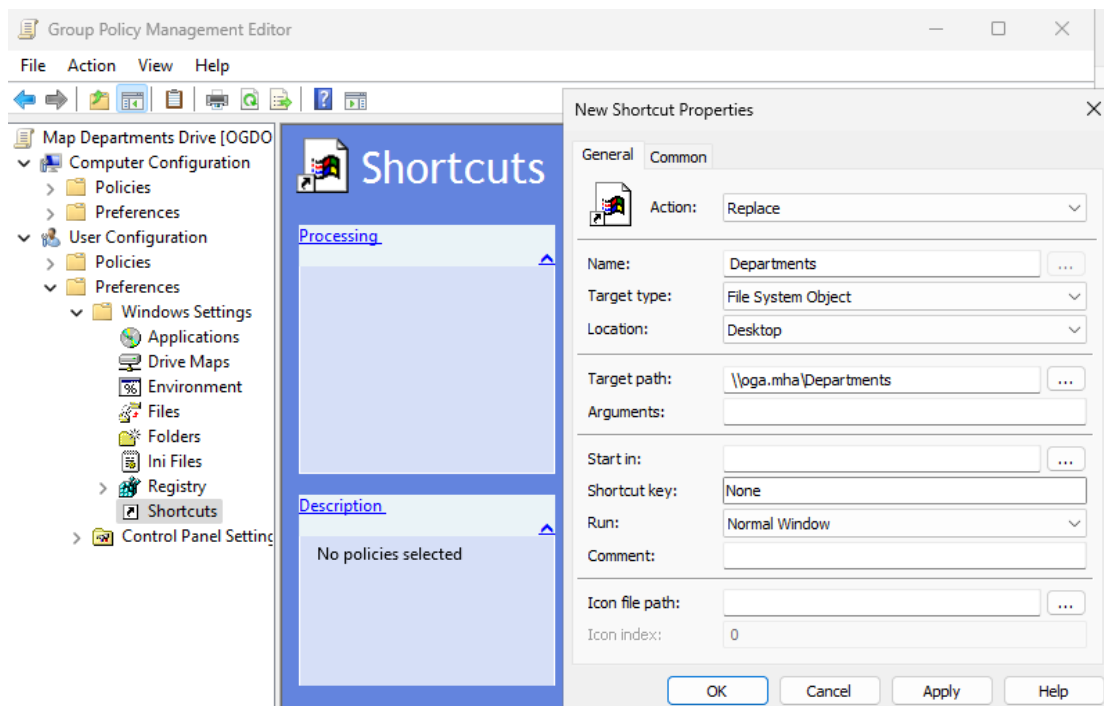
Replication > New replication group > Multipurpose Replication Group >  
Name: 'DepartmentsReplication' > domain: oga.mha > members: other servers >  
full mesh > etc.

State	Local Path	Membership Status	Member	Replicated Folder
Replicated Folder: Departments (1 item)				
	C:\Departments	Enabled	OGFILEIS	Departments

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

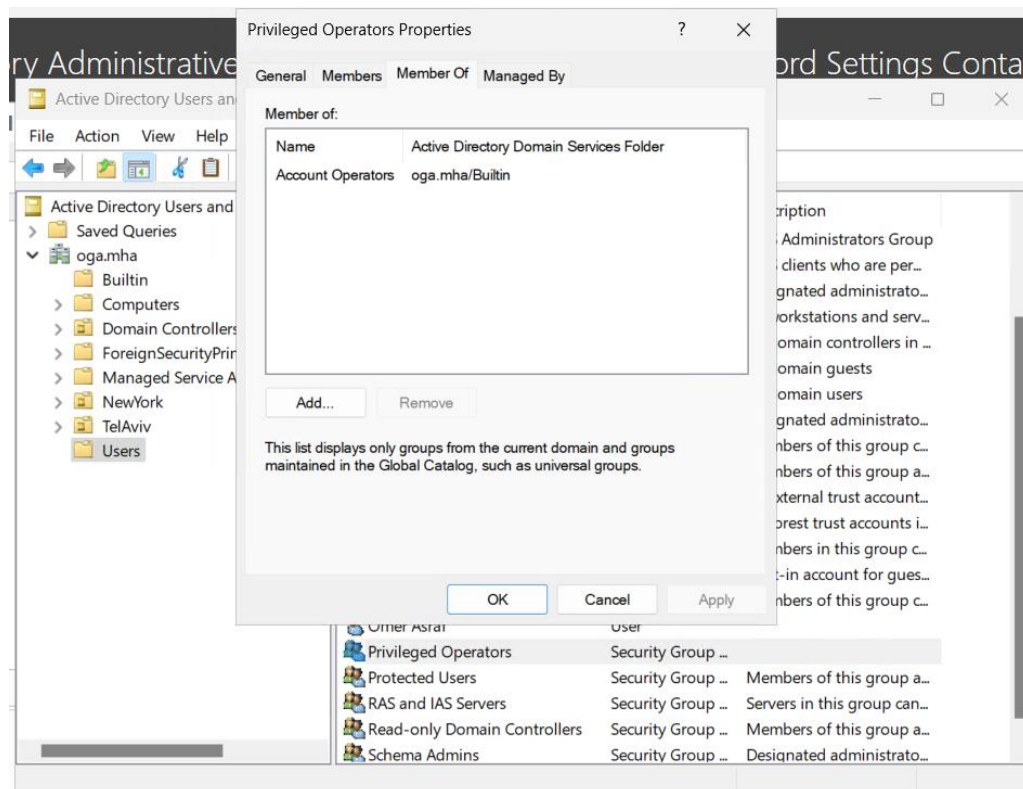


'Map Departments Drive' GPO > Edit > User configuration > Preferences > Windows Settings > Shortcuts > New Shortcut > etc.



## 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:

**Create Password Settings: PrivilegedAccounts**

Tasks: [v] Sections: [v]

Password Settings  
Directly Applies To

Name: \* PrivilegedAccounts  
Precedence: \* 1

☒ Enforce minimum password length  
Minimum password length (characters): \* 12

☒ Enforce password history  
Number of passwords remembered: \* 5

☒ Password must meet complexity requirements

☐ Store password using reversible encryption

☒ Protect from accidental deletion

Description:  
Fine Grained Password Policy for privileged accounts

Password age options:

☒ Enforce minimum password age  
User cannot change the password withi... \* 1

☒ Enforce maximum password age  
User must change the password after (... \* 60

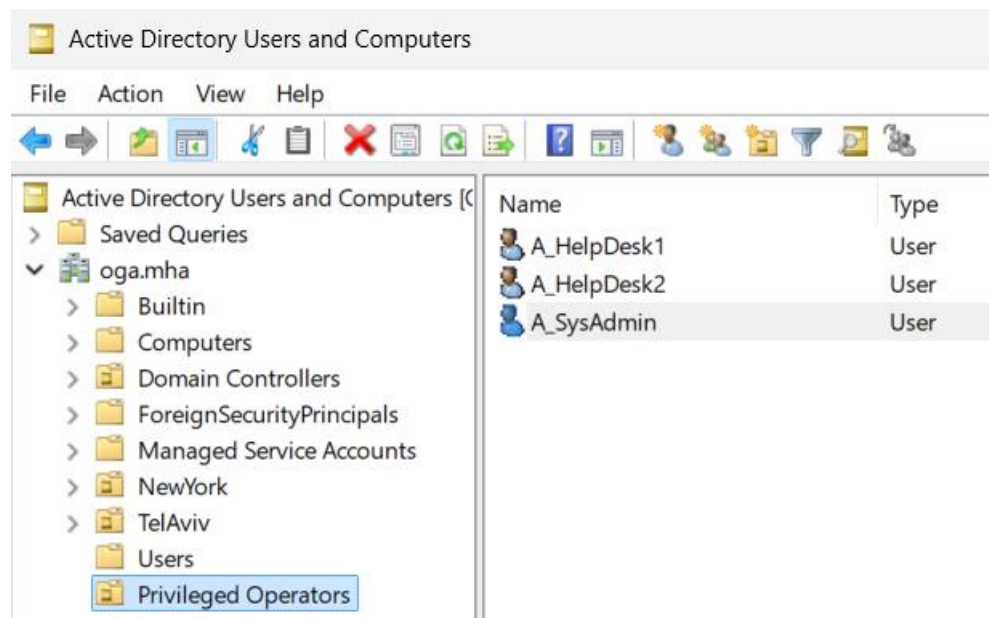
☒ Enforce account lockout policy:  
Number of failed logon attempts allowed: \* 3  
Reset failed logon attempts count after (m... \* 30  
Account will be locked out  
☒ For a duration of (mins): \* 30  
☐ Until an administrator manually unlocks the account

Directly Applies To

Name	Mail
Domain Admins	
Privileged Operators	

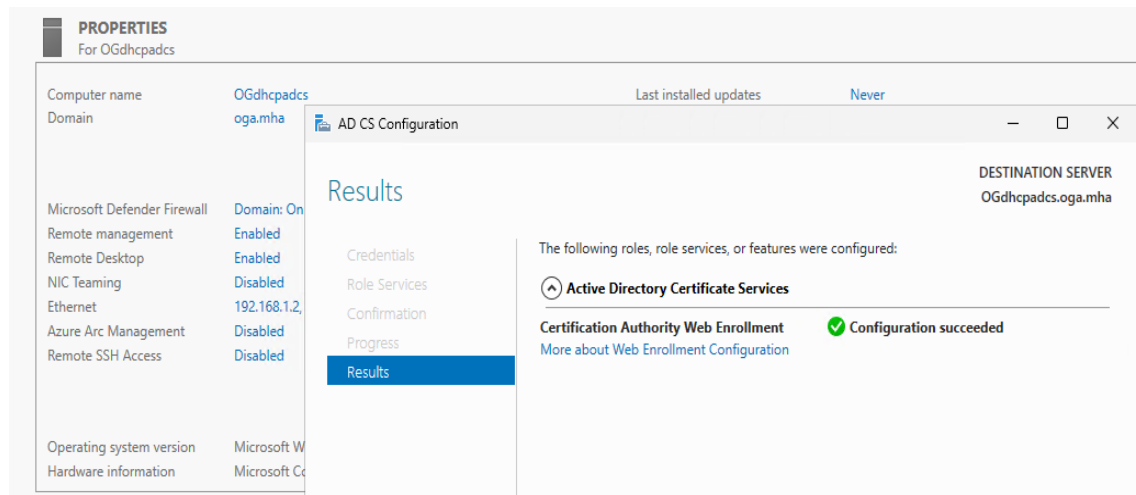
More Information [v] OK Cancel

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

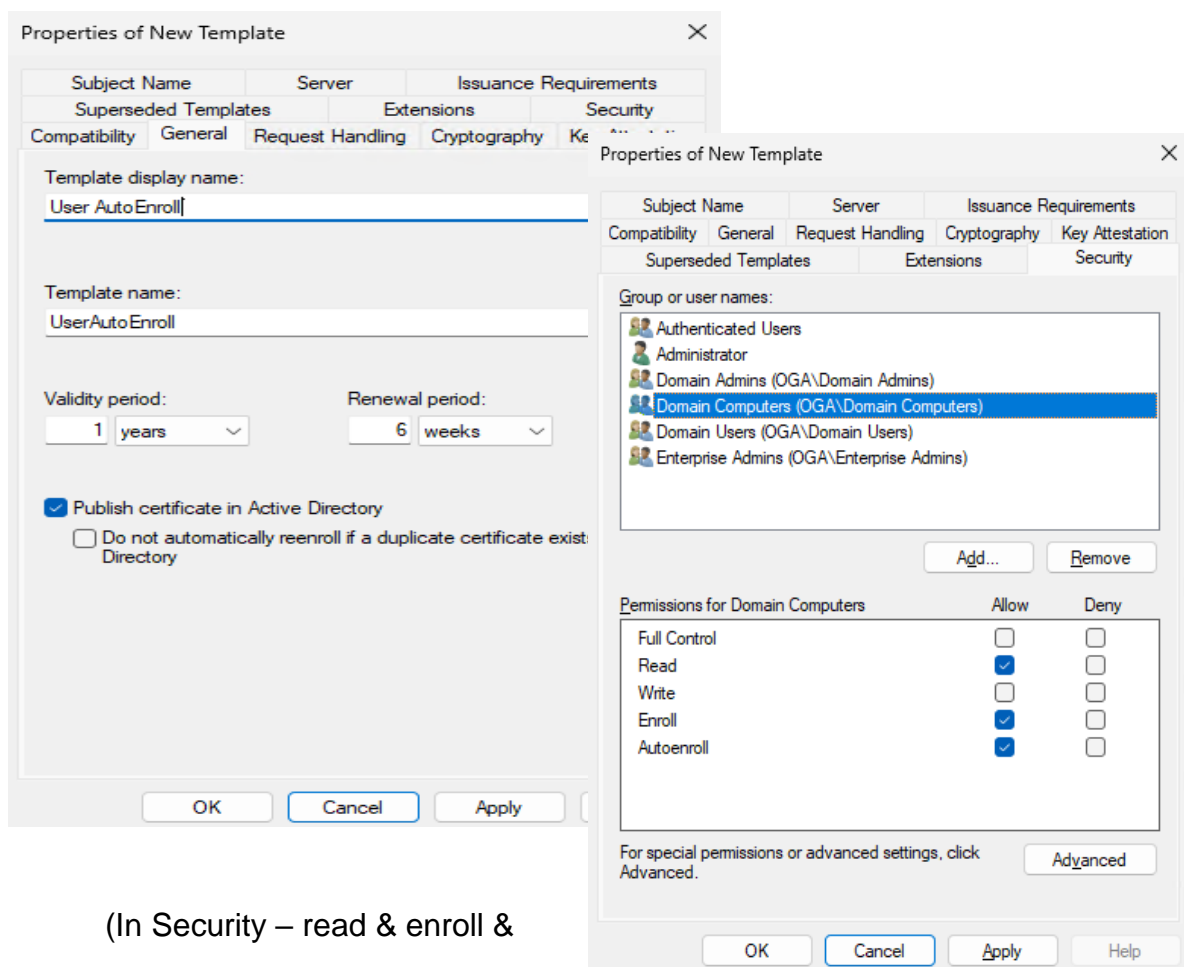


## 8. ADCS:

On my DHCP + ADCS server ('OGdhcpcads') 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.

Properties of New Template

Subject Name      Server      Issuance Requirements

Superseded Templates      Extensions      Security

Compatibility      General      Request Handling      Cryptography      Key Attestation

Template display name:  
Computer AutoEnroll

Template name:  
ComputerAutoEnroll

Validity period:      Renewal period:  
1 years      6 weeks

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

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 (OGA\Domain Admins)
- Domain Computers (OGA\Domain Computers)**
- Enterprise Admins (OGA\Enterprise Admins)

Add...      Remove

Permissions for Domain Computers

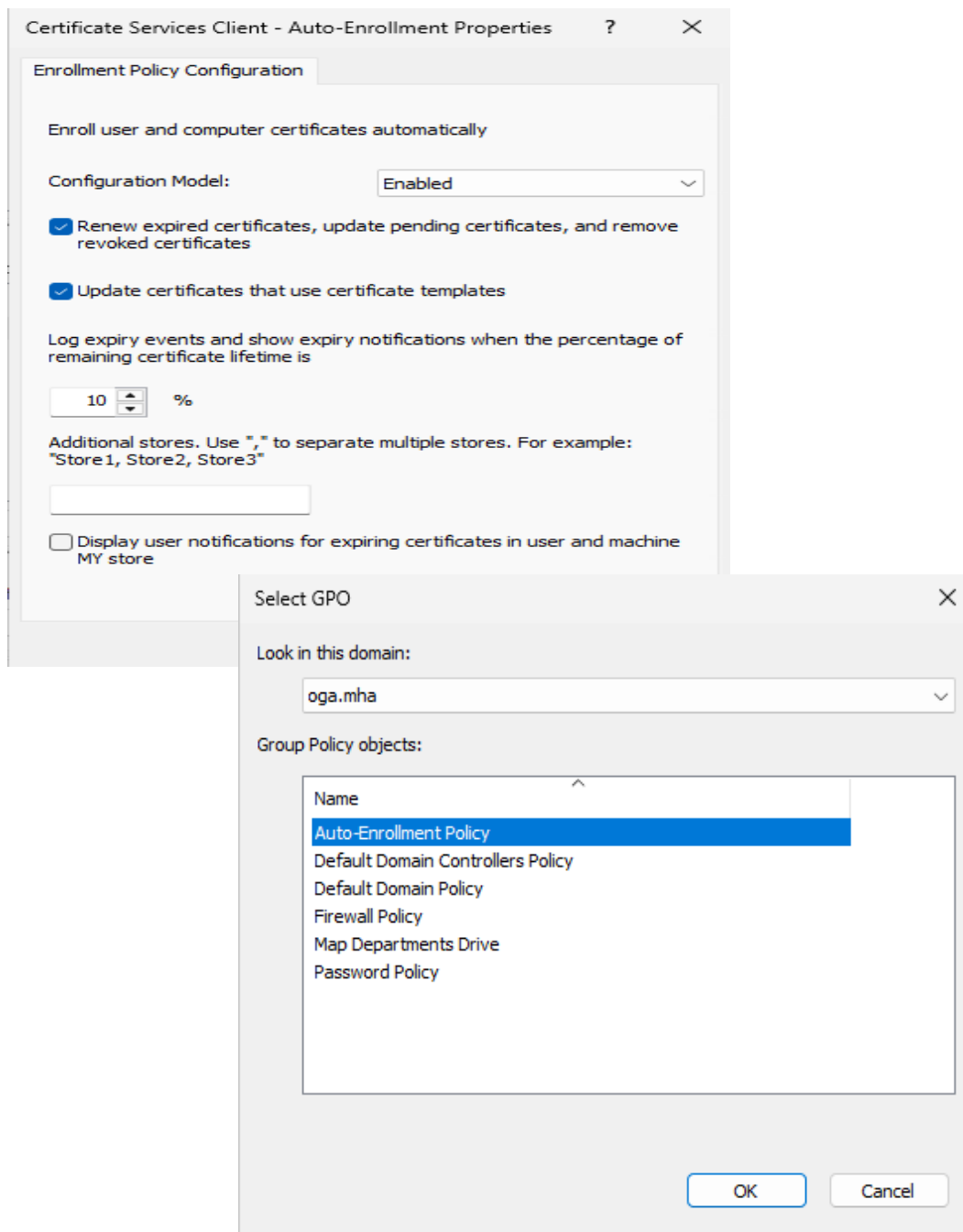
	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>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

	User AutoEnroll	2	100.3	Client Authentication, Secure Email, Encrypting File System
	Computer AutoEnroll	2	100.3	Client Authentication, Server Authentication

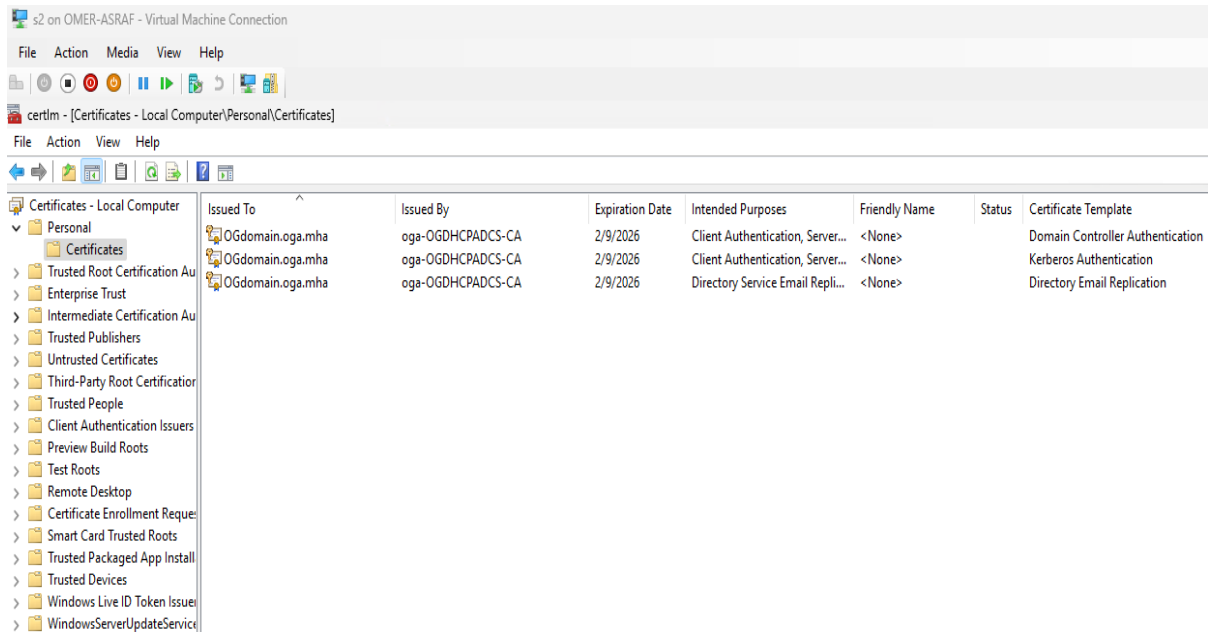


After, I went back to certsrv.msc > created new certificate template to Issue > selected User AutoEnroll" & "Computer AutoEnroll > Ok.

- Configure Auto-Enrollment in Group Policy > went to DC > gpmmc.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'.



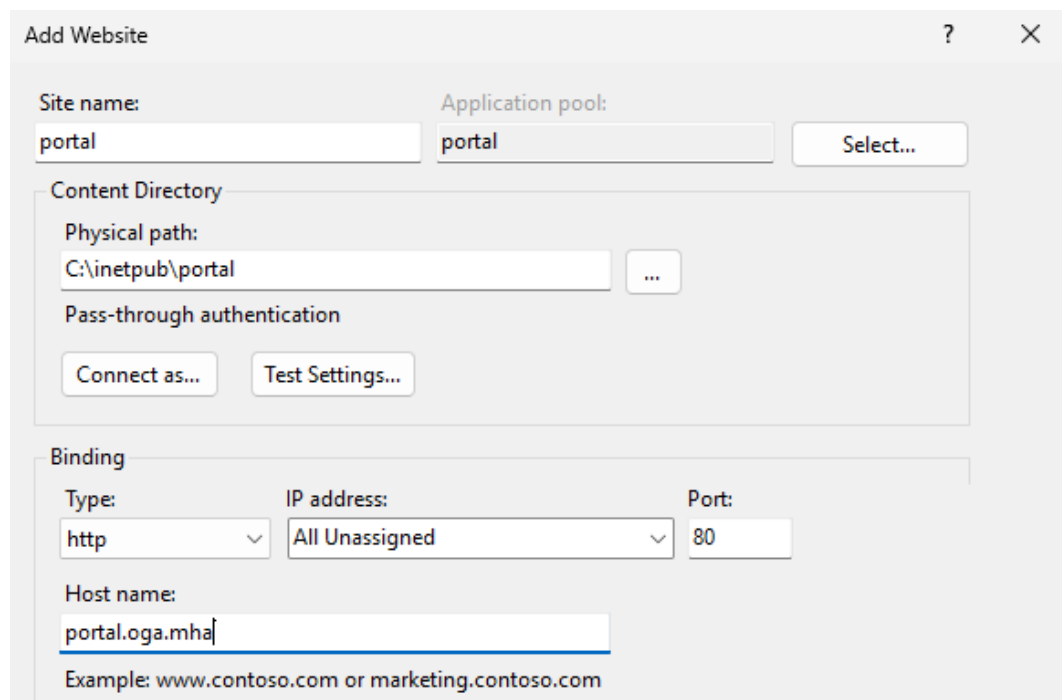
certlm.msc > Personal > Certificates.



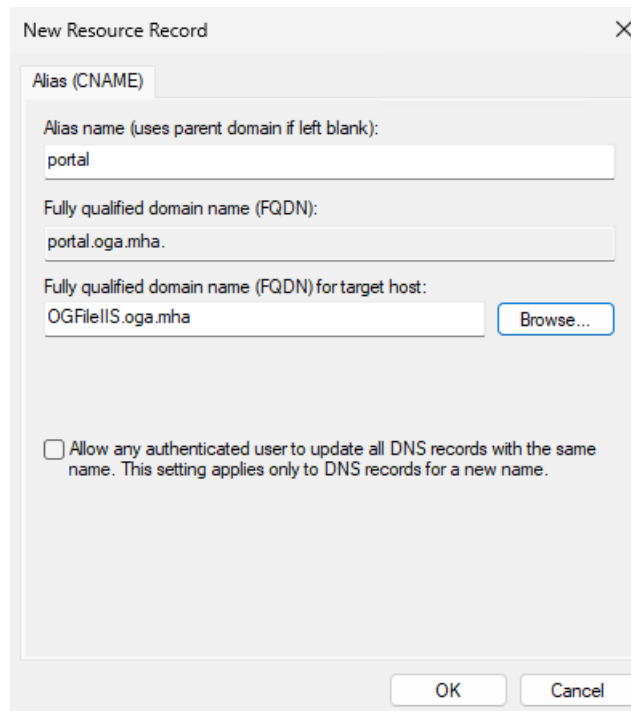
## 9. Intranet Portal:

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

Create web folder 'C:\inetpub\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)



New Resource Record

Alias (CNAME)

Alias name (uses parent domain if left blank):  
portal

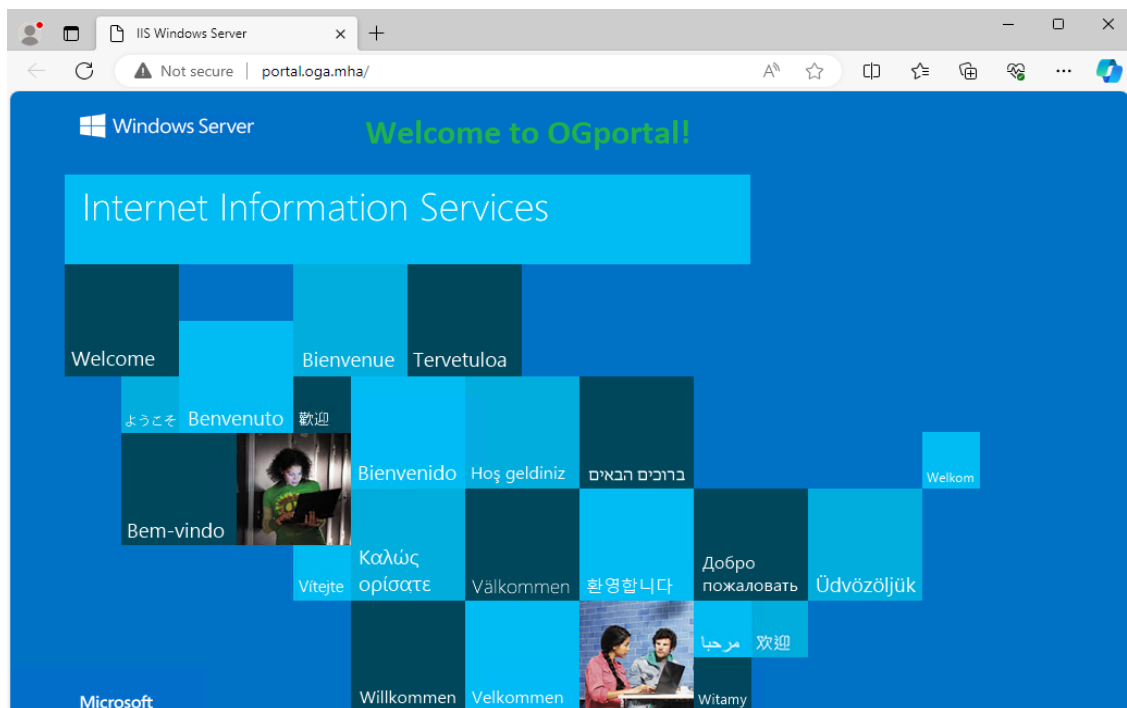
Fully qualified domain name (FQDN):  
portal.oga.mha.

Fully qualified domain name (FQDN) for target host:  
OGFileIIS.oga.mha Browse...

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel

browsed <http://portal.oga.mha>



## Create Self-Signed Certificate using PowerShell.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator.0GA> New-SelfSignedCertificate -DnsName "portal.oga.mha" -CertStoreLocation "Cert:\LocalMachine\My"

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                               Subject
-----
C7F1D114365FAF6F044EEFD99D507C9A2B1AC8F6  CN=portal.oga.mha
```

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



### Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter:	Go	Show All	Group by:	No Grouping	
Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Stor
	portal.oga.mha	portal.oga.mha	12/02/2026 21:16:21	79A68FBA227C80FB74D390D7...	Personal

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

?

×

Type:

IP address:

Port:

https

All Unassigned

443

Host name:

portal.oga.mha

☐ Require Server Name Indication

☐ Disable TLS 1.3 over TCP

☐ Disable QUIC

☐ Disable Legacy TLS

☐ Disable HTTP/2

☐ Disable OCSP Stapling

☐ Negotiate Client Certificate

SSL certificate:

portal.oga.mha

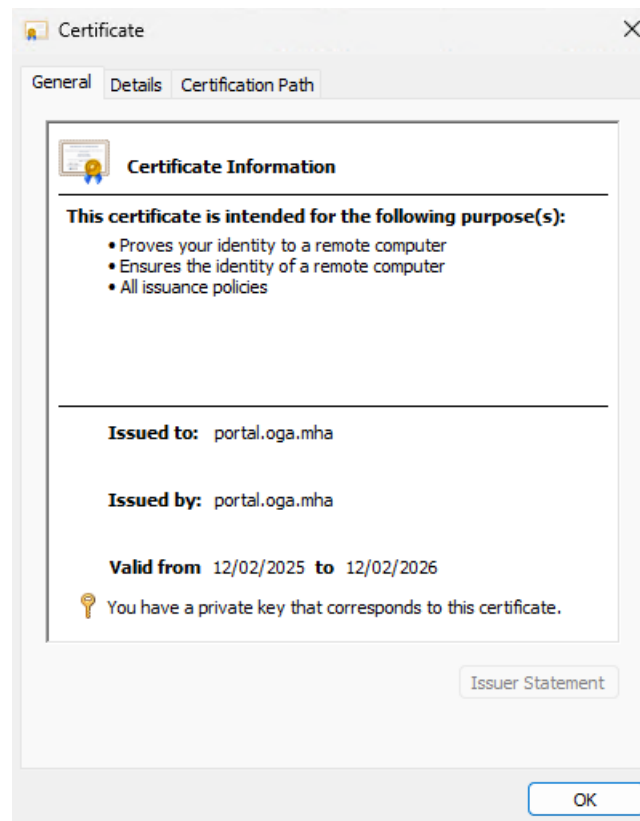
Select...

View...

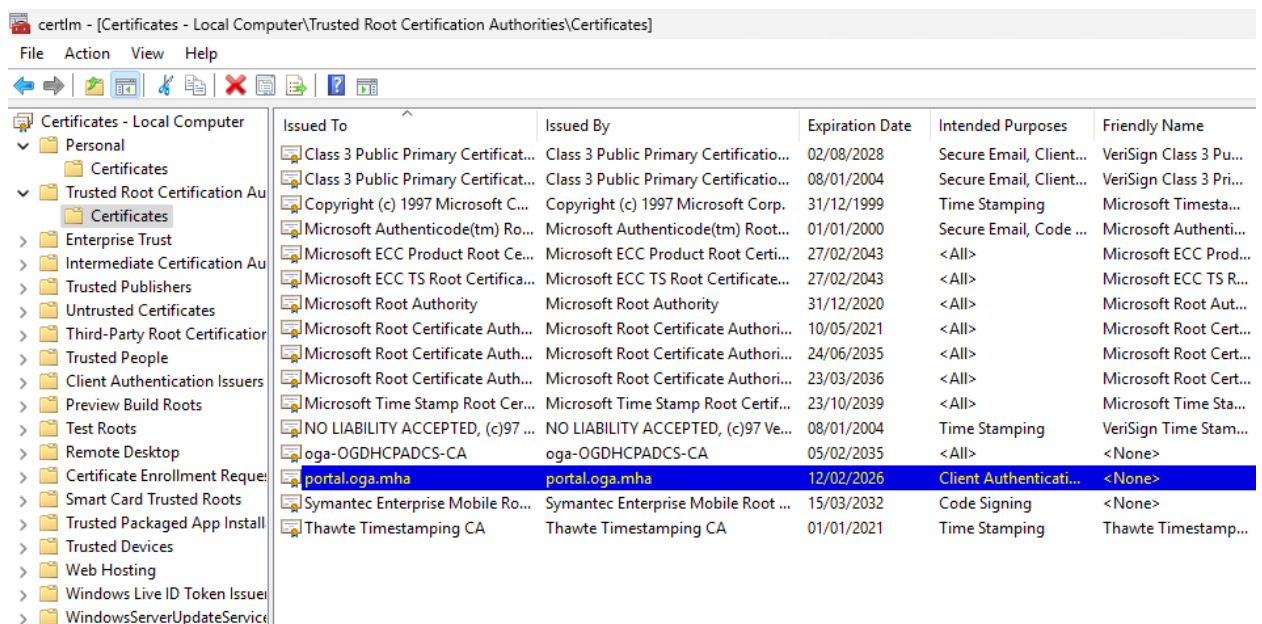
OK

Cancel

'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'

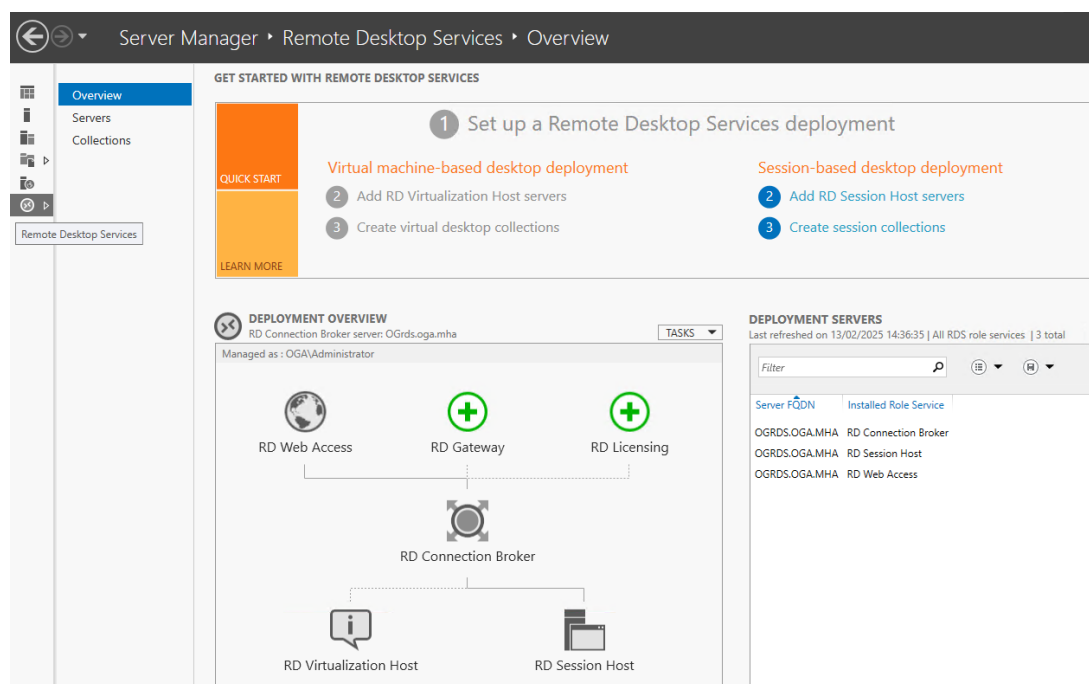
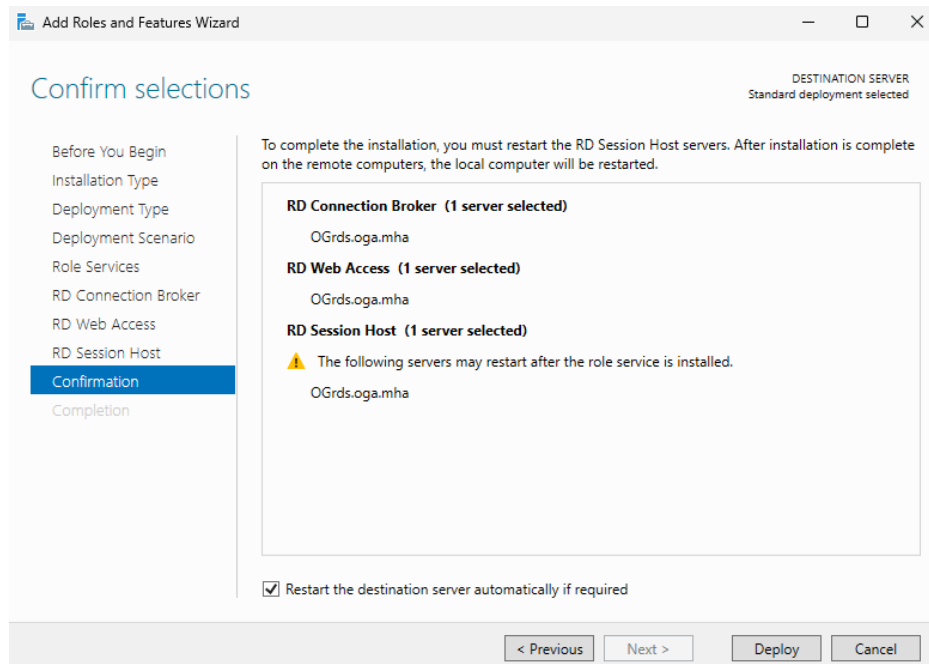


After, went to CMD > 'iisreset' > browsed <https://portal.oga.mha>

## 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.

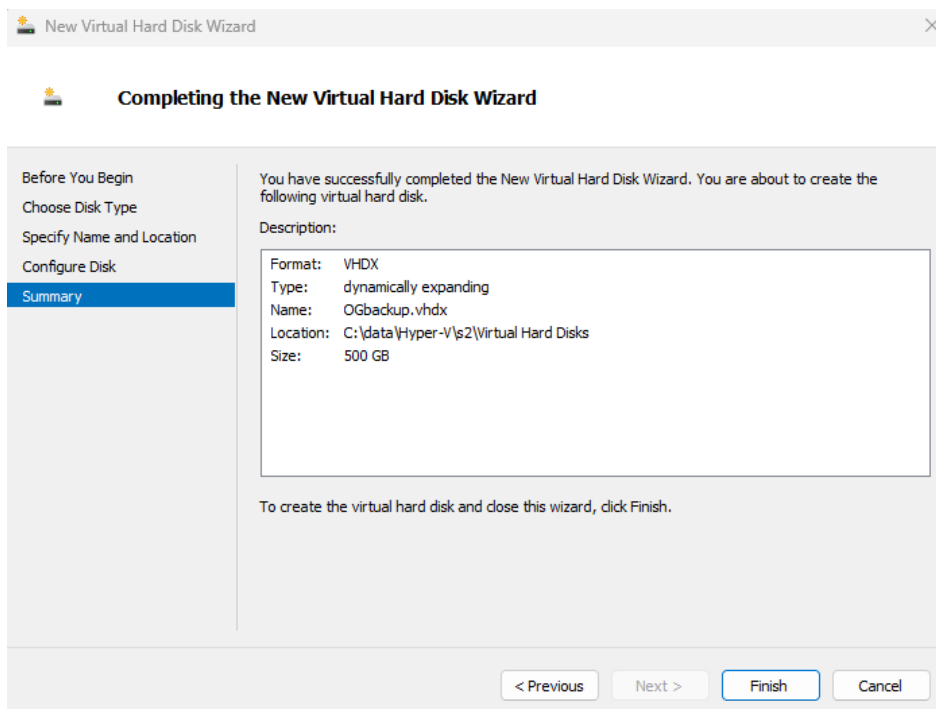
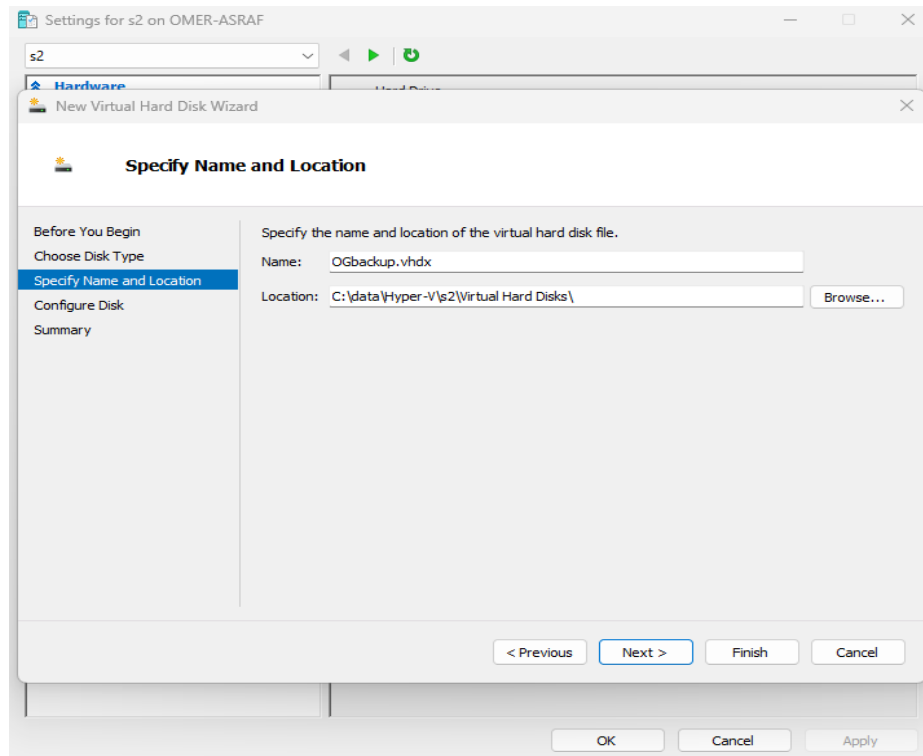


Edit Deployment Properties > RD Licensing > per user.

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

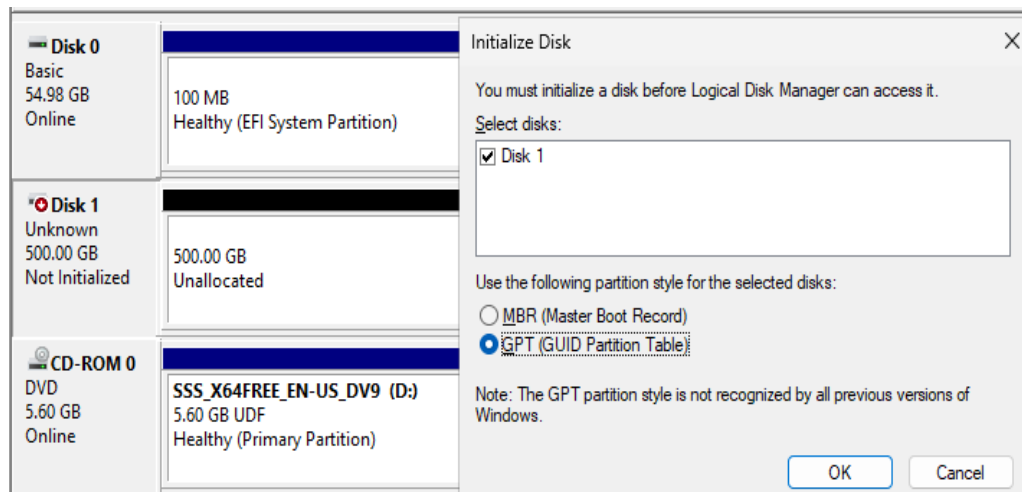
## 11. Backup solution:

Added a New Virtual Disk (VHDX) to DC >

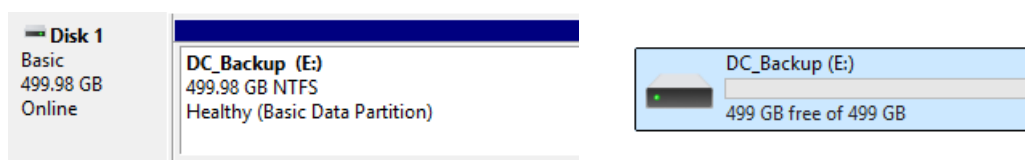
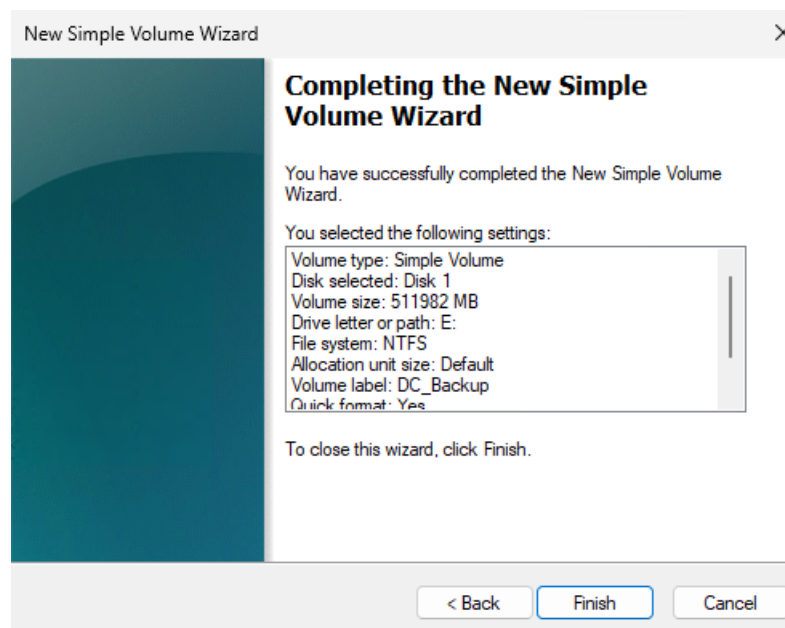


finish > apply > ok.

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

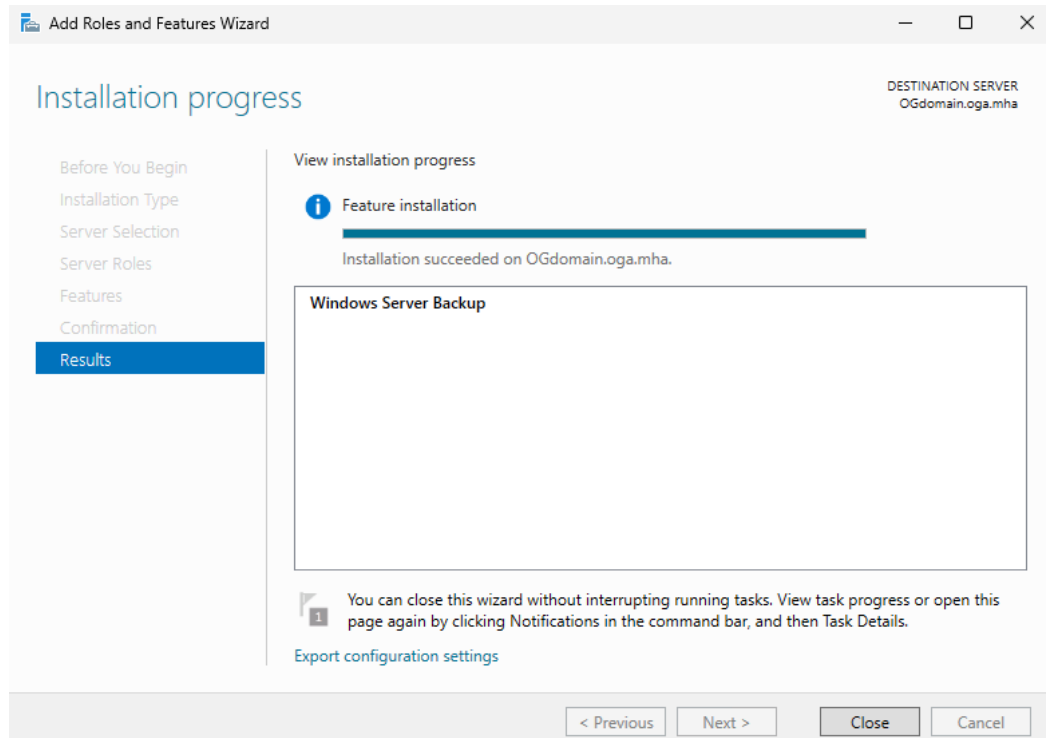


Unallocated space > New Simple Volume wizard > Finish.

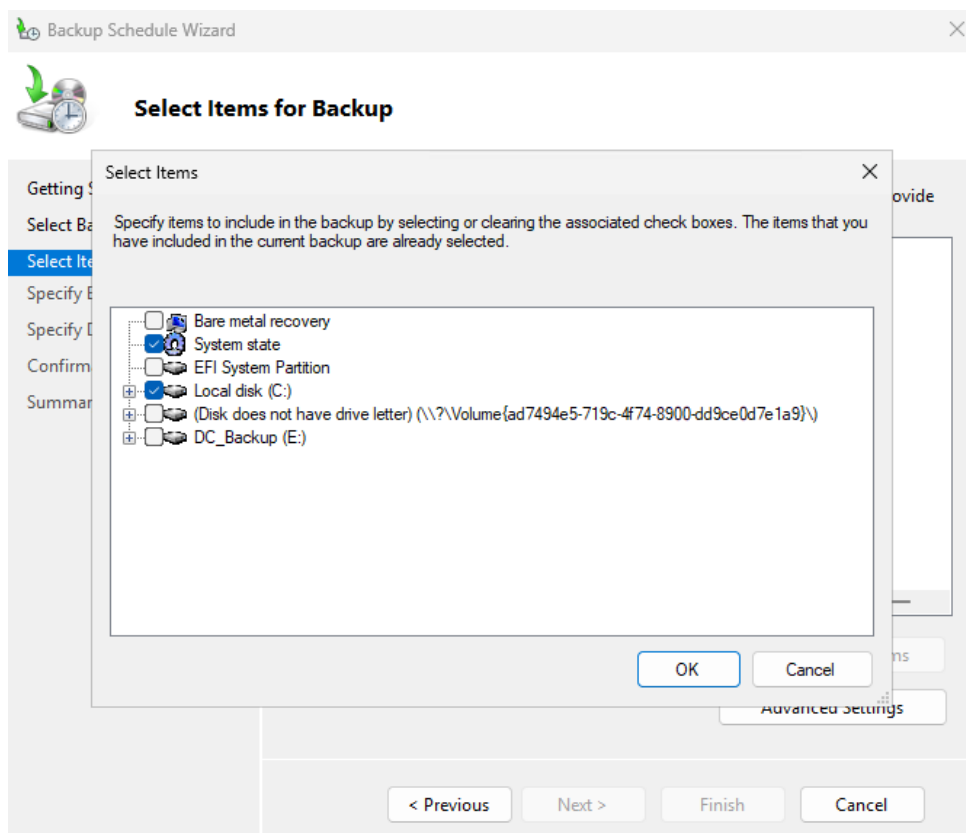




Now




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.

Available disks:

Disk	Name	Size	Used Space	Volumes
<input checked="" type="checkbox"/> 1	Microsoft Virtual ...	500.00 GB	127.76 MB	E:\

OK

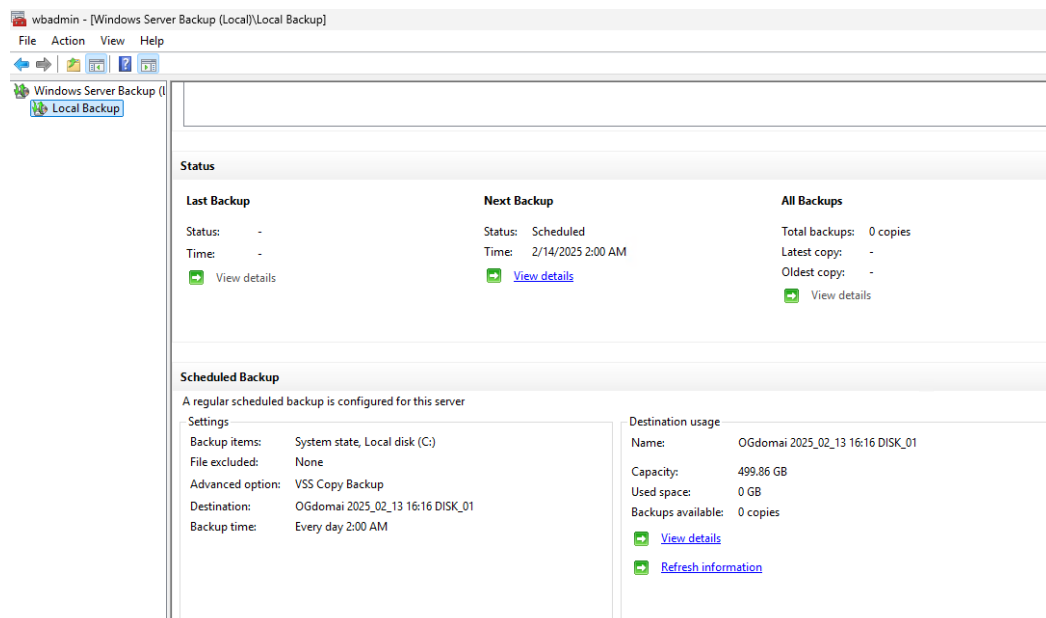
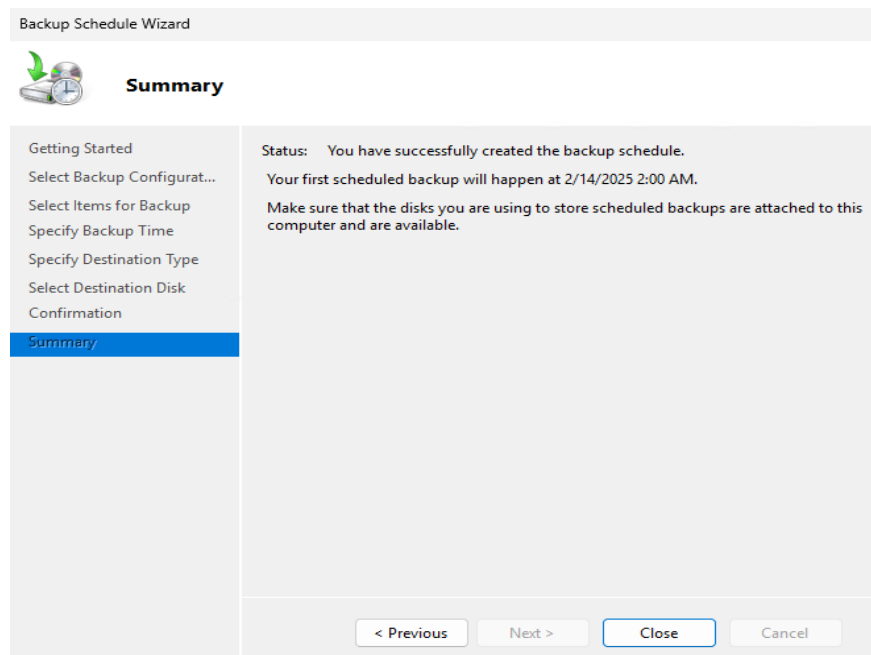
Cancel

< 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 > gpmmc.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.

