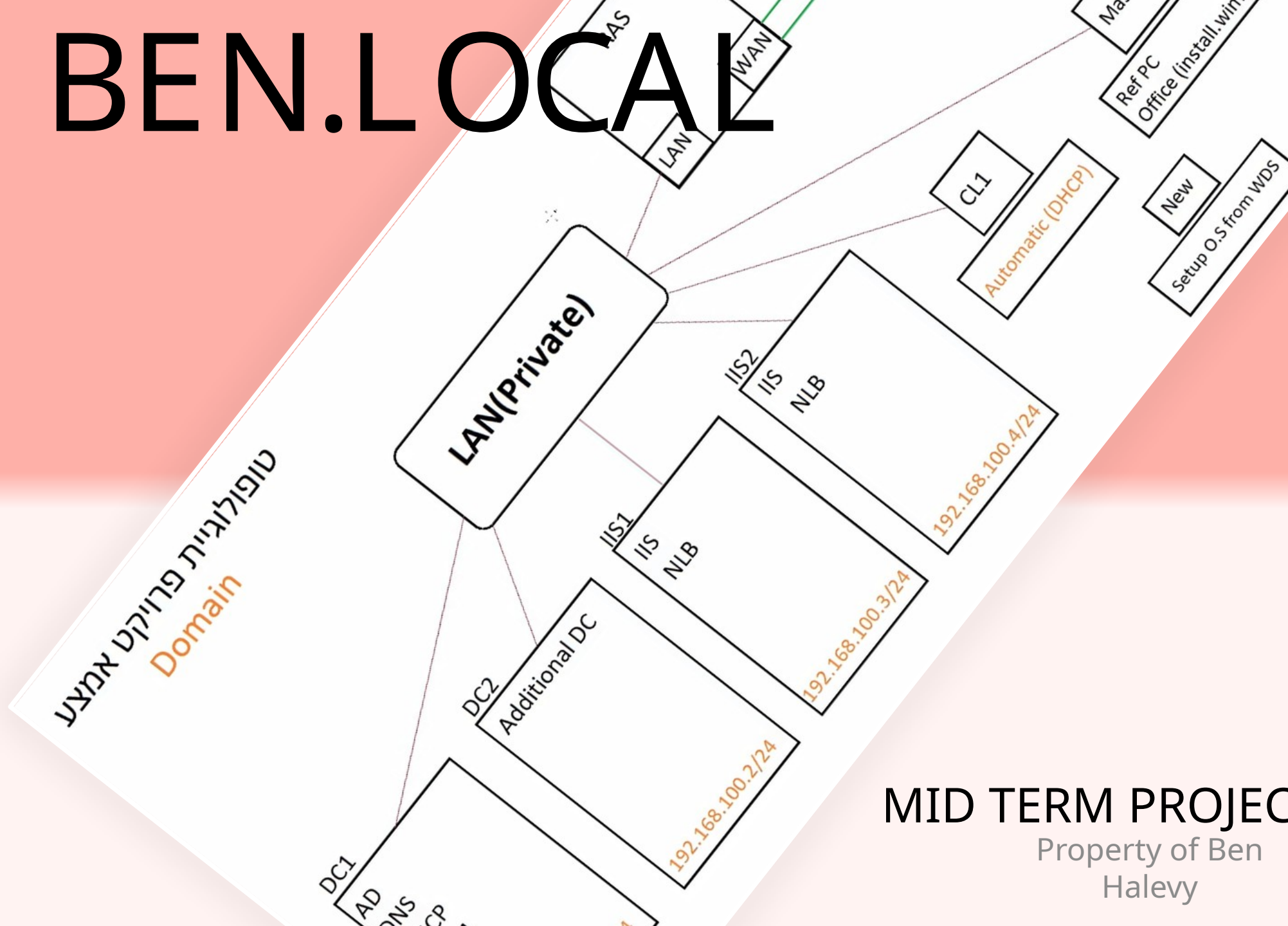
BEN.LOCAL



MID TERM PROJECT

Property of Ben Halevy

BEN.LOCAL

MID TERM PROJECT

- Our Home office is located in Lev Hagalil and requires a New Active Directory
- This Organizational Build Requires:
- 6 Different Organizational Units with different Integrated Perameters,
- User permissions, and subcompartmentalized authorizations.

- Lets Begin Our Interesting Journey.....

Property of Ben Halevy

Mission Parameters
BUILD ROADMAP

ORGANIZATIONAL INFRASTRUCTURE	SLIDES
Initial infrastructure: LAN switch, DC1, AD DS forest, DHCP, CL1	4-7
Organizational Units & user accounts (PowerShell)	8-10
Delegation of control (password reset)	11-12
Domain password & lockout policy, Fine-grained PSO	13-16
Home folders mapped to Z:	17-18
HelpDesk security group (Restricted Groups)	19-22
Folder redirection to \\DC1\Home	23-26
Removable storage block (Sales)	27-29
Application block - Calc.exe (Office)	30-33
Reports share Y: & NTFS permissions	34-37
FSRM quotas & file screens	38-42
Shadow copies (previous versions)	43-45
GPO file deployment & the FSRM / GPO bug	46-49
Control Panel restriction (Finance)	50-51
Software deployment through GPO (7-Zip)	52-53
Item-level targeted drive map S:	54-55

NETWORK INFRASTRUCTURE	SLIDES
RAS server & VPN (PPTP) with PC1	56-64
DC2, replication & RID master transfer	65-67
Network printers via GPO (Print1 / Print2)	68-83
DNS forwarders & root hints	84-85
IIS web servers & NLB cluster	86-90
iSCSI target / initiator (RAID 0 spanned volume)	91-93
Windows Deployment Services (WDS / PXE)	94-96
Golden image: Sysprep + DISM + WDS deployment	97-104

SUMMARY	SLIDE
Build map: every server, client, IP address and role	105

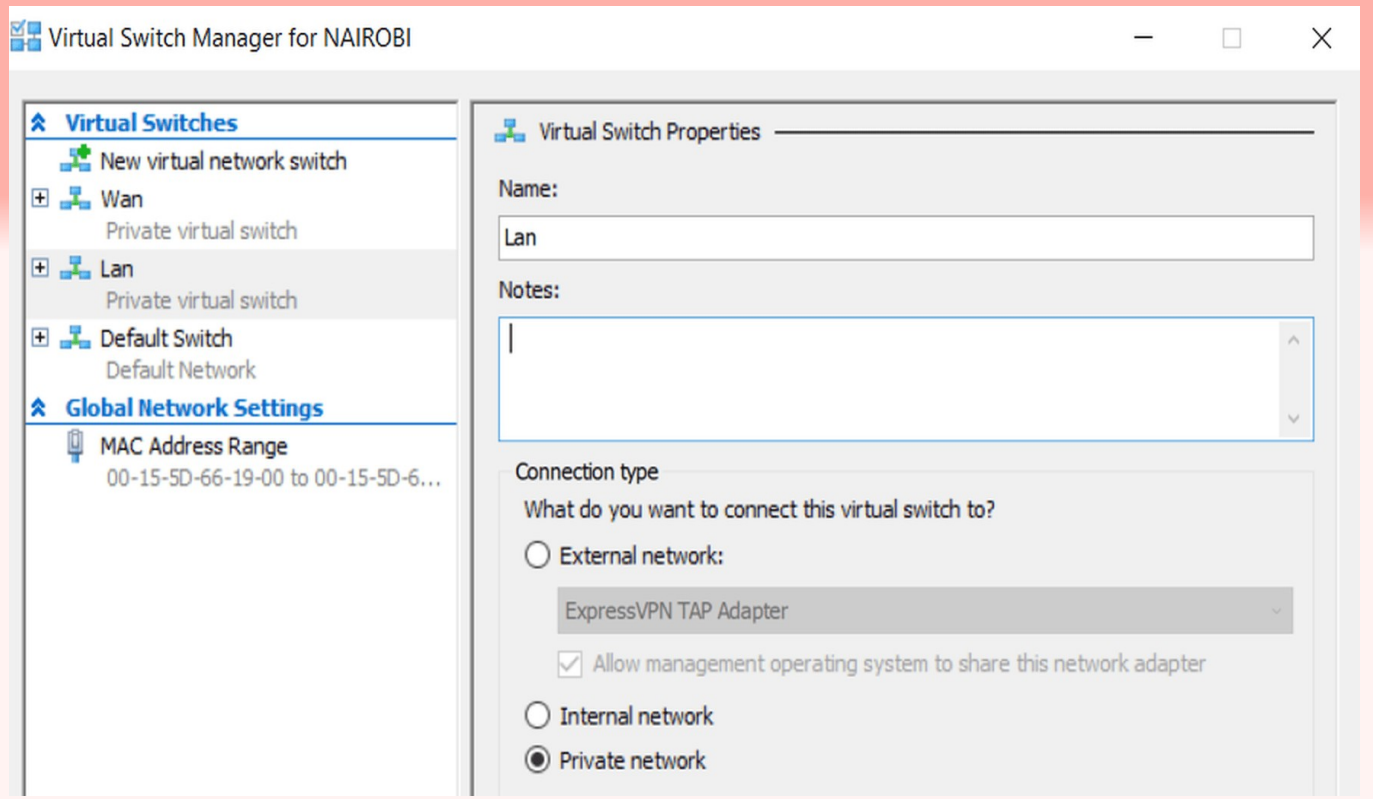
Property of Ben Halevy

Mission Parameters

INITIAL **ORGANIZATIONAL INFRASTRUCTURE**

TASK

Create a private virtual switch named LAN



Property of Ben Halevy

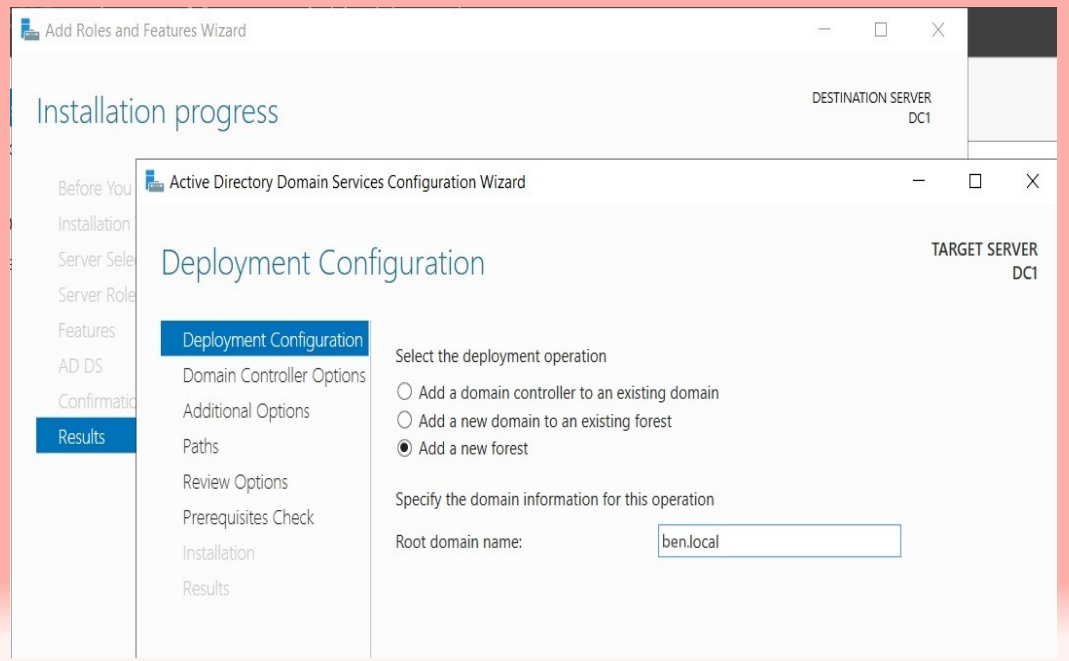
MissionParameters

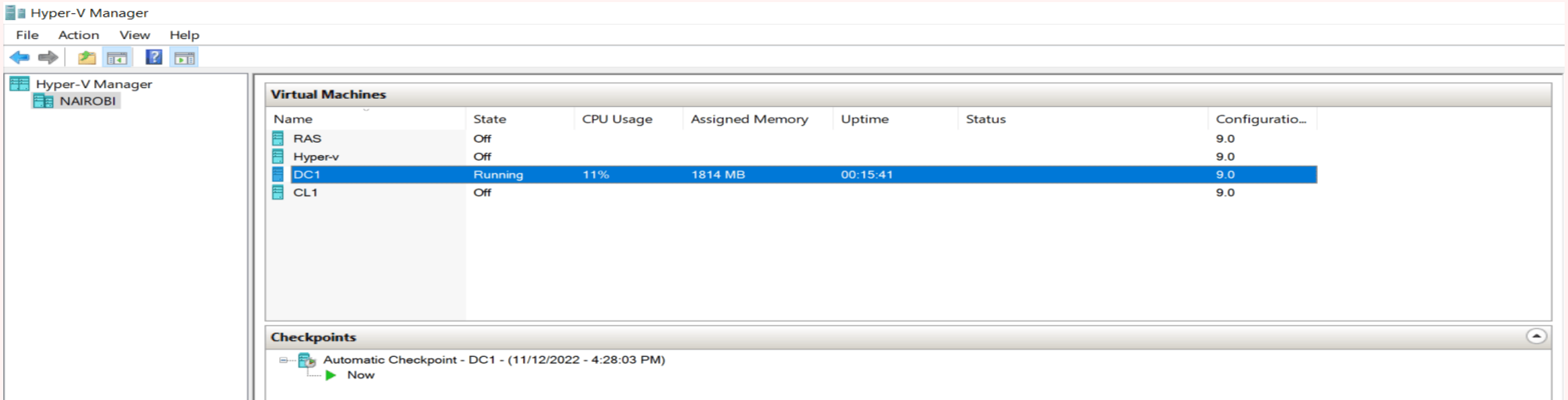
ORGANIZATIONALINFRASTRUCTURE

TASK- 1. INITIAL INFRASTRUCTURE
Create a Virtual Machine named DC1 > install Windows Server (2019) w/4GB Ram and 40 GB HD
Rename it DC1 upon first start up> Initial LAN IP Info for the DC 1 Server : Ip Address :192.168.100.1
Subnet Mask: 255.255.255.0 Class C Default Gateway: 192.168.100.254 Dns Server: 192.168.100.1
Add a Role AD Domain Services >Create a New Forest> Name it BEN.LOCAL > Install a Role (DHCP SERVER)
>AD Tools > DHCP Server > Click on BEN.LOCAL> Right click IPV4 > New Scope with the following IP
Pool : IP Range: 192.168.100.100-192.168.100.150Subnet Mask: 255.255.255.0 Class C No Exclusions 8 Day
Lease Term > Use the Default Gateway previously mentioned> Use the

Mission Parameters

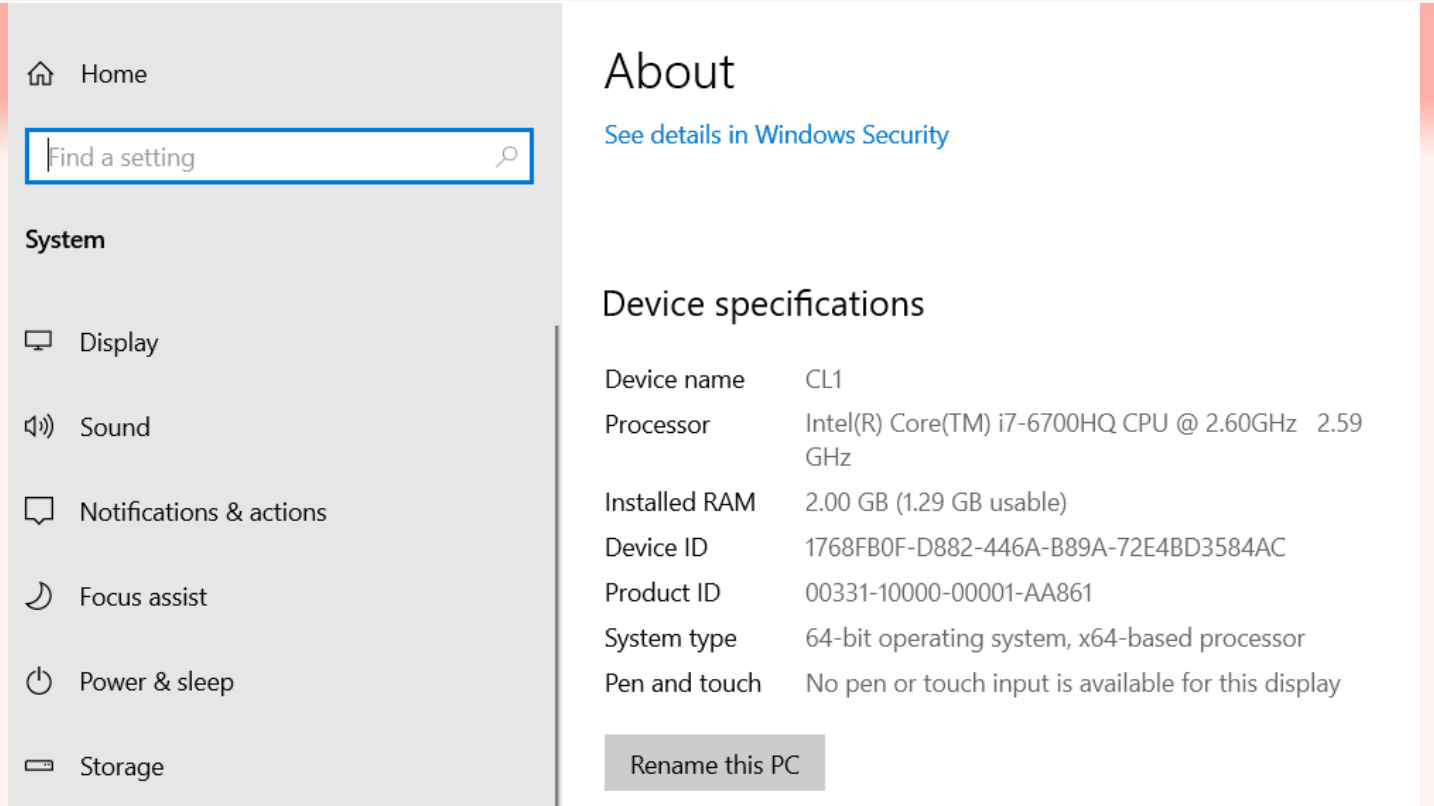
ORGANIZATIONAL INFRASTRUCTURE





Mission Parameters
ORGANIZATIONAL INFRASTRUCTURE

TASK
Created virtual machine (CL1) w/ Windows 10 Pro w/ (2GB Ram) (40 GB HD) w/ LAN connection
Rename it CL1> connect to the new network (BEN.LOCAL)> Leave the IP configuration in Automatic Mode



Property of Ben Halevy

Mission Parameters
ORGANIZATIONAL INFRASTRUCTURE

TASK
The OU’s Were Created Using Powershell Scripts, One Script to create the OU’s
Another Script to Install the users’ inherent Account Parameters
Management- 1 CEO, 2 Vice Ceo’s, 4 Managers Office - 7 users (O1-O7) Finance - 4 users (F1-F4) Sales - 5 users (S1- S5) Architects – 20 users (A1-A20) IT - 3 Employees : Alex – Network Manager ; Adam- Technician ; Amir- Technician

Property of Ben Halevy

organizationalunitsworks - Notepad

File Edit Format View Help

```
New-ADOrganizationalUnit -Name "Finance" -Path "DC=ben,DC=local"
New-ADOrganizationalUnit -Name "Sales" -Path "DC=ben,DC=local"
New-ADOrganizationalUnit -Name "It System Team" -Path "DC=ben,DC=local"
New-ADOrganizationalUnit -Name "Office" -Path "DC=ben,DC=local"
New-ADOrganizationalUnit -Name "Architects" -Path "DC=ben,DC=local"
New-ADOrganizationalUnit -Name "Managers" -Path "DC=ben,DC=local"
```

Administrator: Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

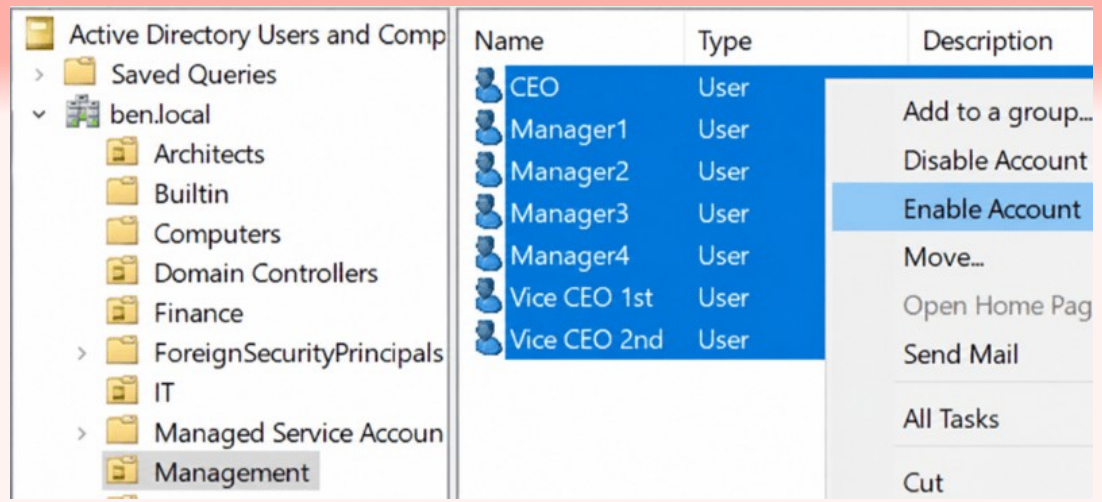
Untitled3.ps1*

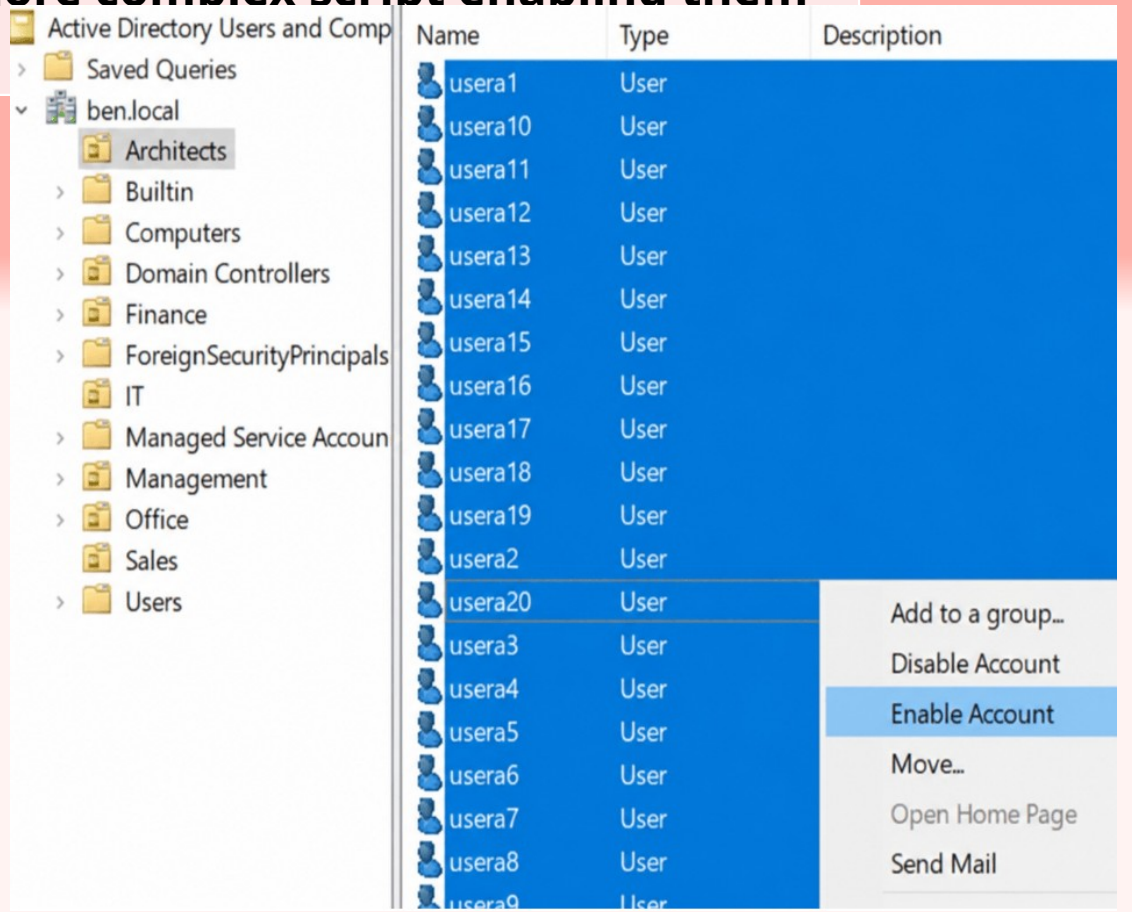
```
1  Import-Module ActiveDirectory
2  $adusers = Import-Csv -literalpath "C:\Scripts\NewUsers.csv"
3  ForEach ($user in $adusers)
4  {
5    $username = $user.username
6    $parentOU = $user.ParentOU
7    $Domain = '@Ben.local'
8    $UPN = $username + $Domain
9    New-ADUser -name "$username" -GivenName $username -Displayname $username -SamAccountName
10 }
```

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

TASK
The Scripts created the OU's and User Profiles, But required manually enabling the groups of users
In the future I would invest on a more complex script enabling them automatically





Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

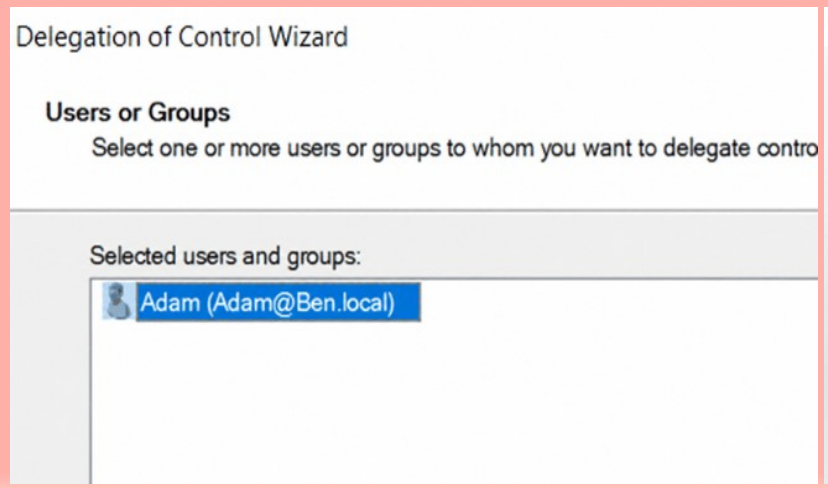
TASK
Implement an OU Wide permission Protocol (Delegation)
Adam The IT Technician is to be given permission to reset all Passwords within the Sales Dept. from his endpoint Terminal.

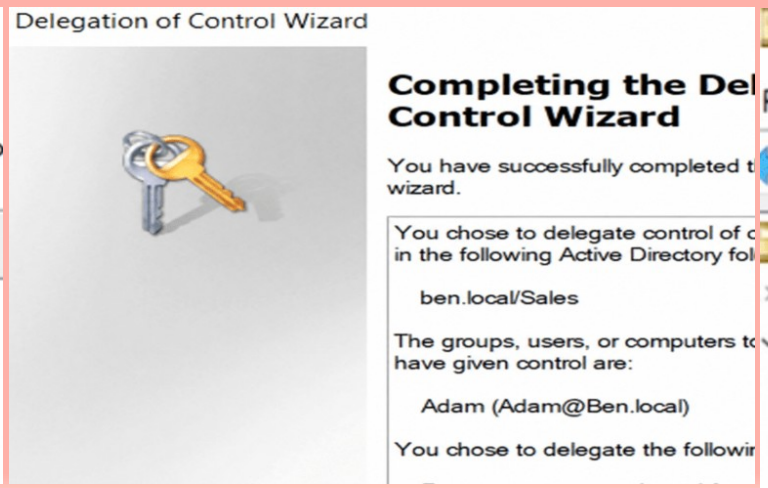
HOW TO INSTRUCTIONS
AD Users and Comps > Sales OU > Right Click > Delegate Control Label “Reset User PW”> Next > Add Adam To Selected Users

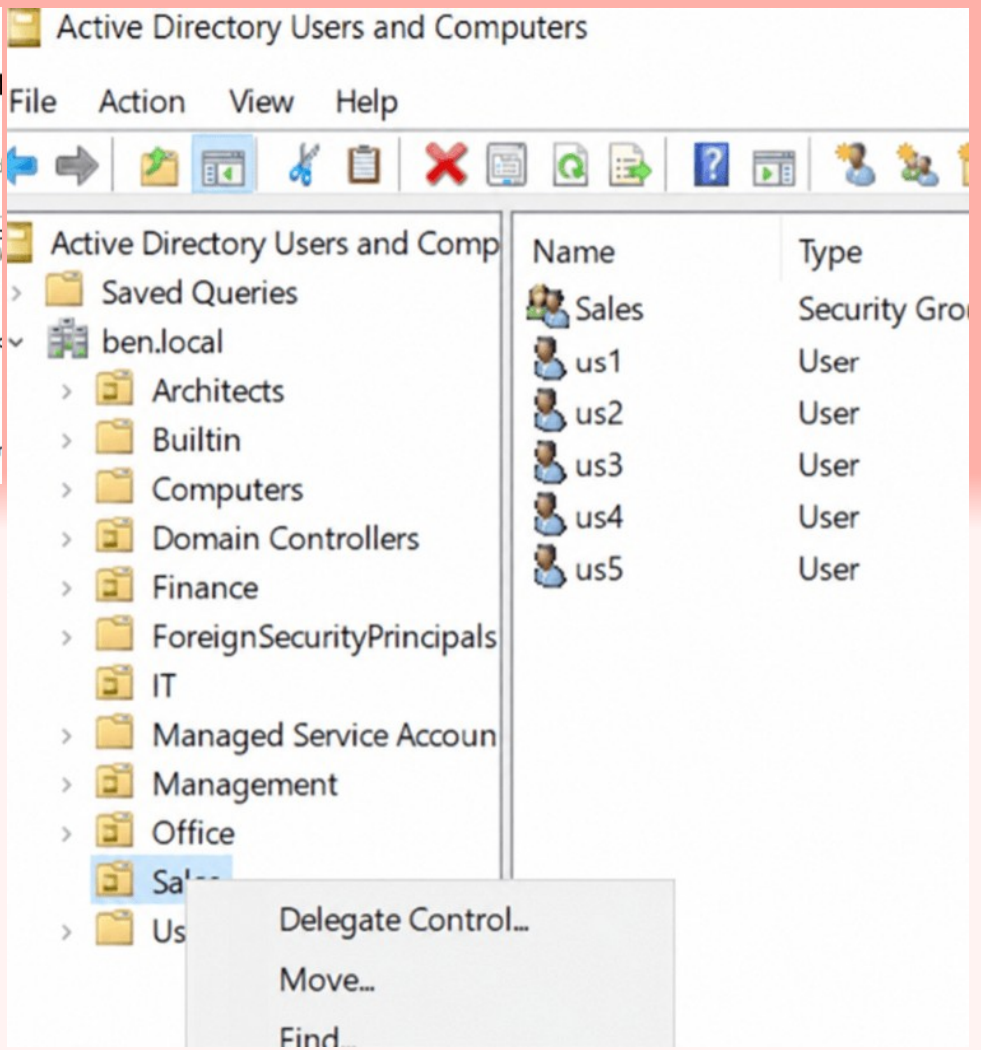
Property of Ben Halevy

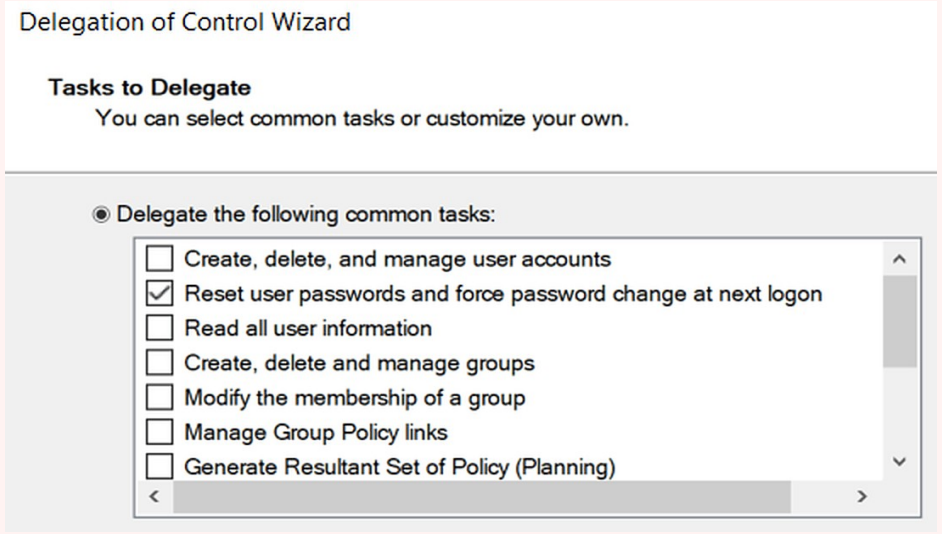
Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE









Property of Ben Halevy

Mission Parameters

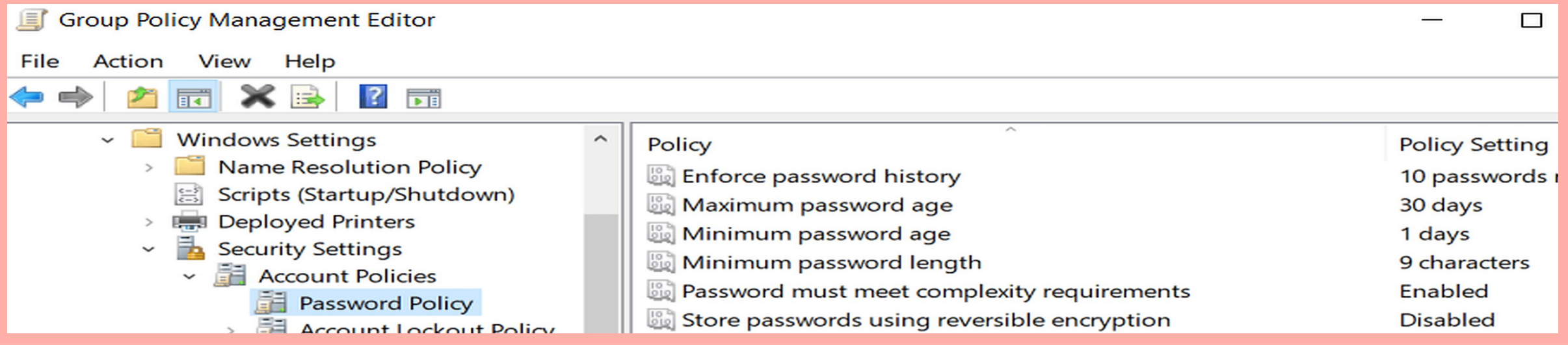
ORGANIZATIONAL INFRASTRUCTURE

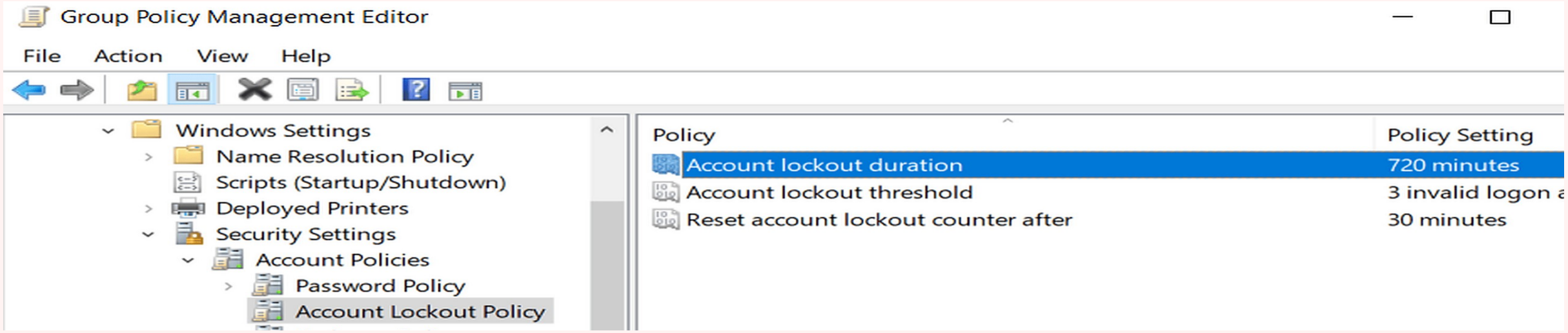
TASK
implement an Organizational Wide Dynamic PW policy
a complex PW with min 9 integers w/a required PW refresh policy every 30 days
a 30 min hibernation period after every incorrect attempt
In the occurrence of 3 incorrect PW attempts, the system would lock the user out for 12 hrs.
PW Relief in the office dept for its senior employees UserO1 and

HOW TO INSTRUCTIONS
AD Server Manager>Tools category > Group Policy Management>right click Default Domain Policy > Edit Policy
Comp Config>Policies>Windows Settings>Security Settings>Acct Policies >PW Policy
Comp Config>Policies>Windows Settings>Security Settings>Acct Policies>Acct Lockout Policy
Configure the policy to the requirements of the organizational Protocol >gpupdate /force to update the Group Policy
Created a PW relief Policy in the Sales Dept. in the AD Admin center = BEN LOCAL >system>pw

Mission Parameters

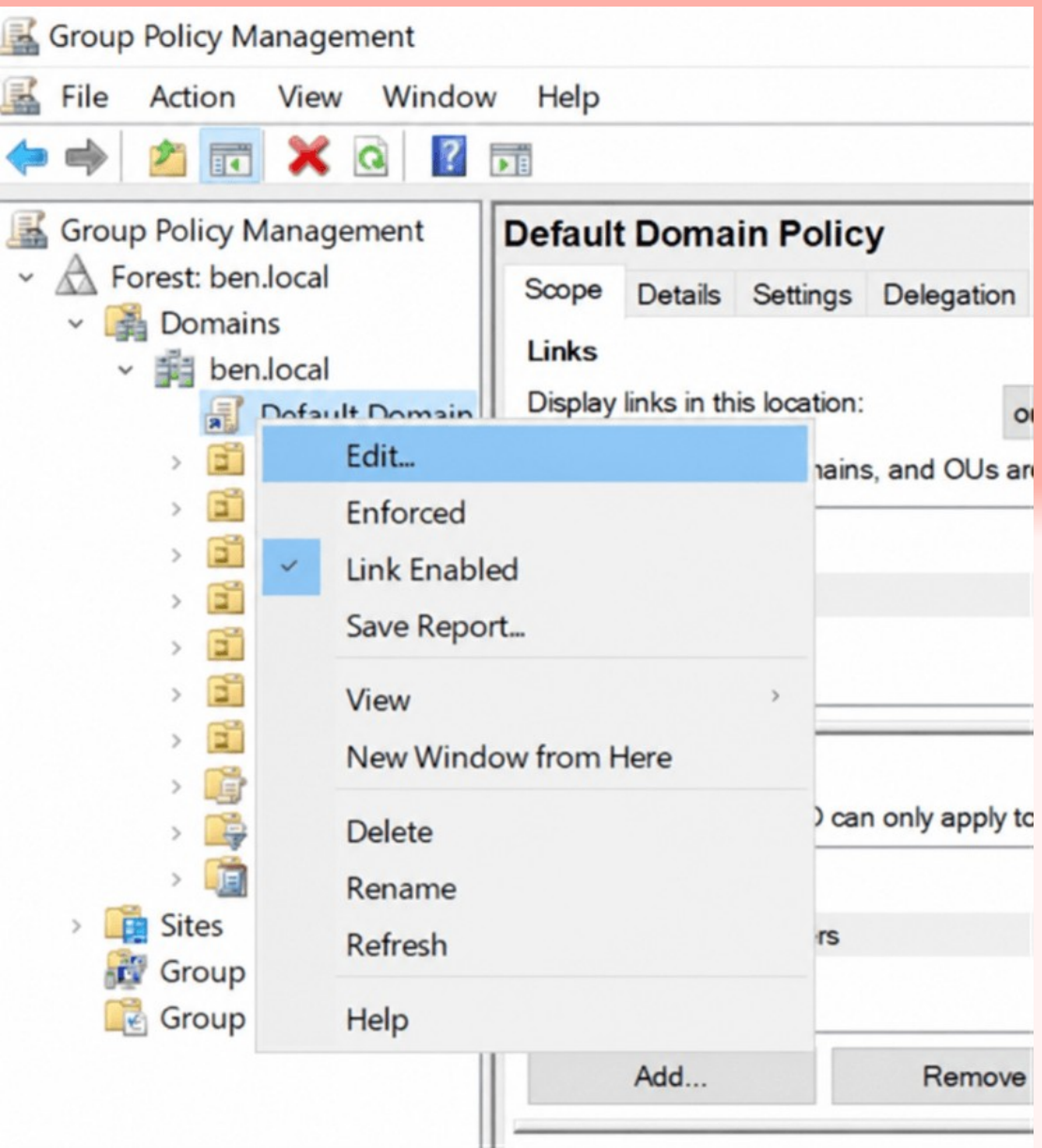
ORGANIZATIONAL INFRASTRUCTURE

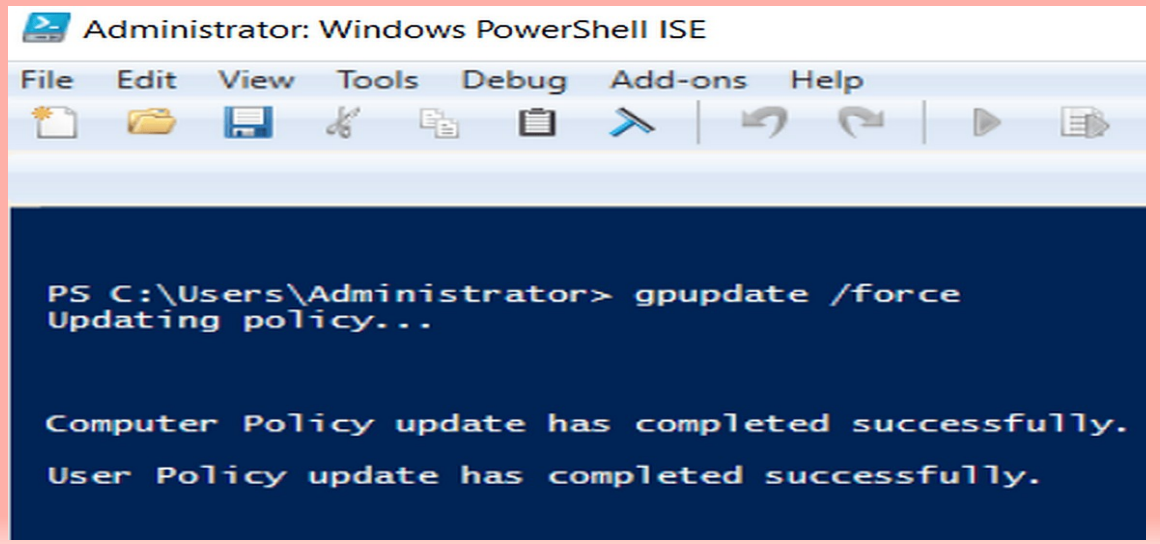


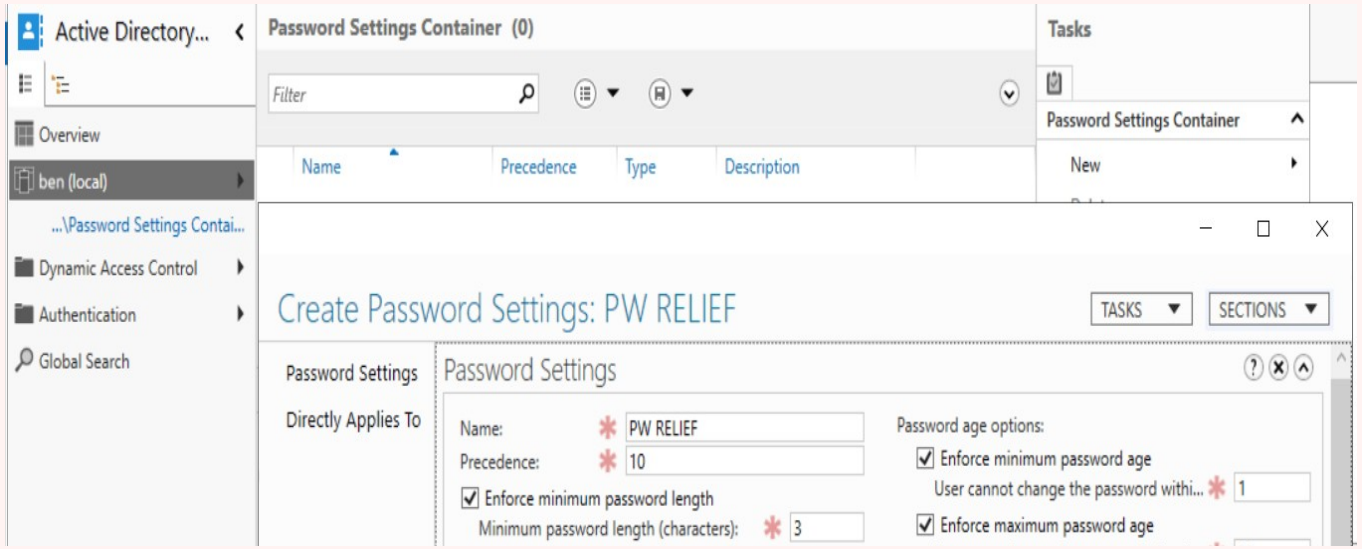


Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE



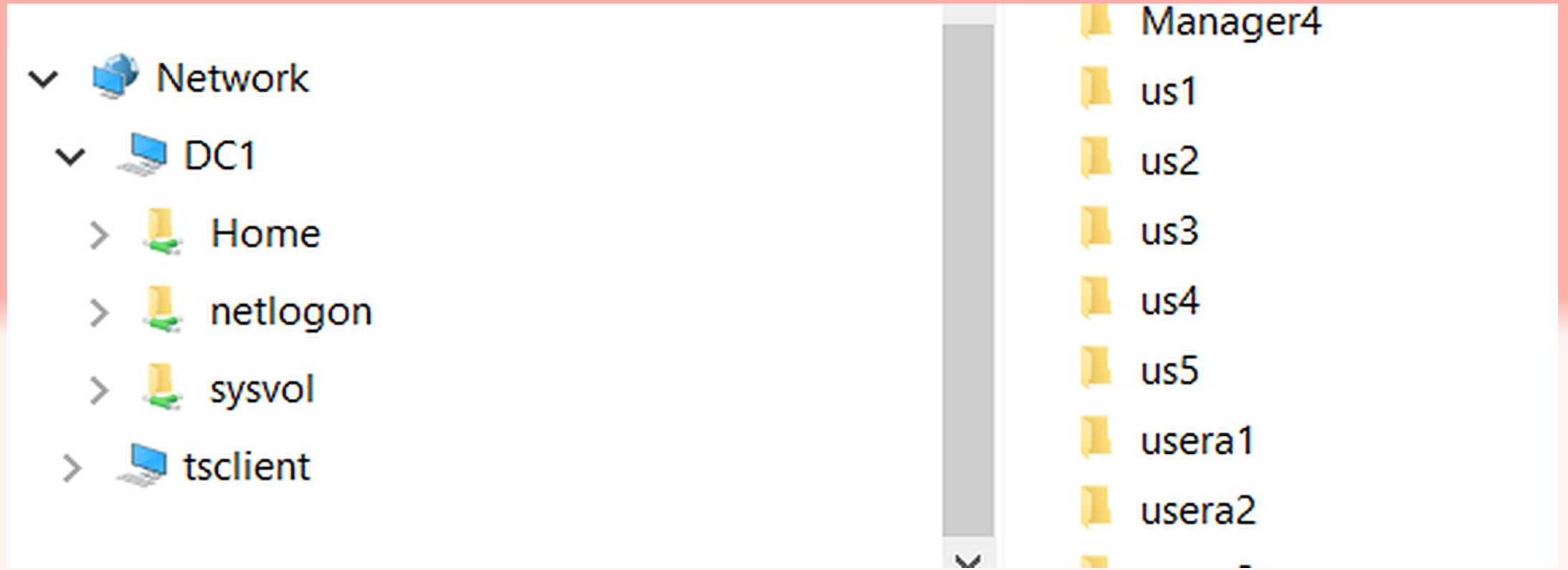




Property of Ben Halevy

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE



Property of Ben Halevy

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

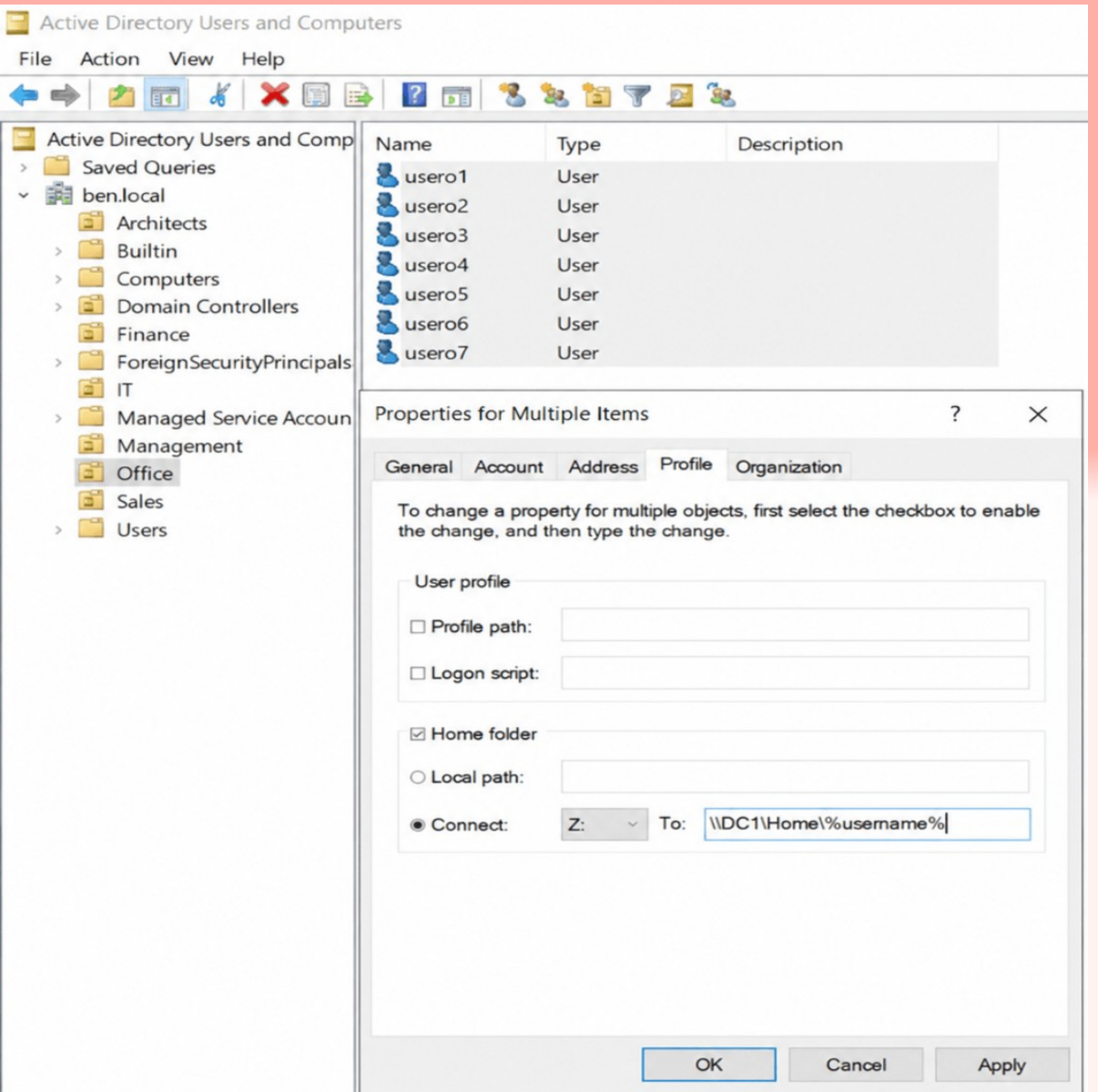
TASK
Create a Home Folder in the DC1 Server
Share the Home folder to all Organizational Employees
Map the Home Folder to Drive Z:
Configure Employee Home Folders To Route to their Network folder

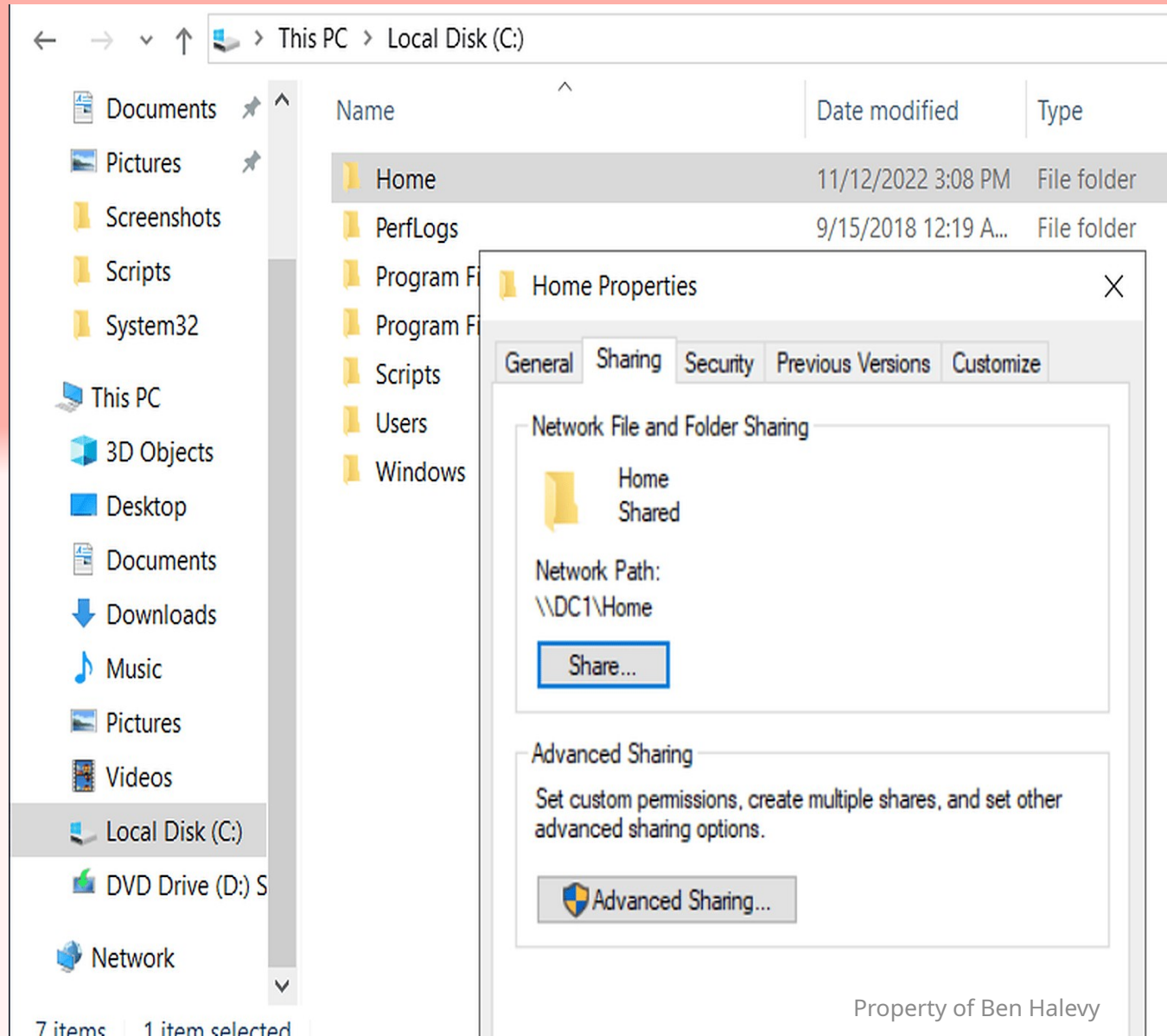
HOW TO INSTRUCTIONS
Create the home folder in the DC1 Server
Users & Computers > mark all users in a OU> right click > properties
Profile> Mark Home Folder> Connect Z:\ \DC1\Home\%username%
Don’t Forget to TURN ON NETWORK DISCOVERY

Property of Ben Halevy

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE





Property of Ben Halevy

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

TASK
Create New Security Group Named HelpDesk in the IT Dept
Add the Group Members as Admins throughout the Organization
This new security Group will be Created in AD Users and Computers

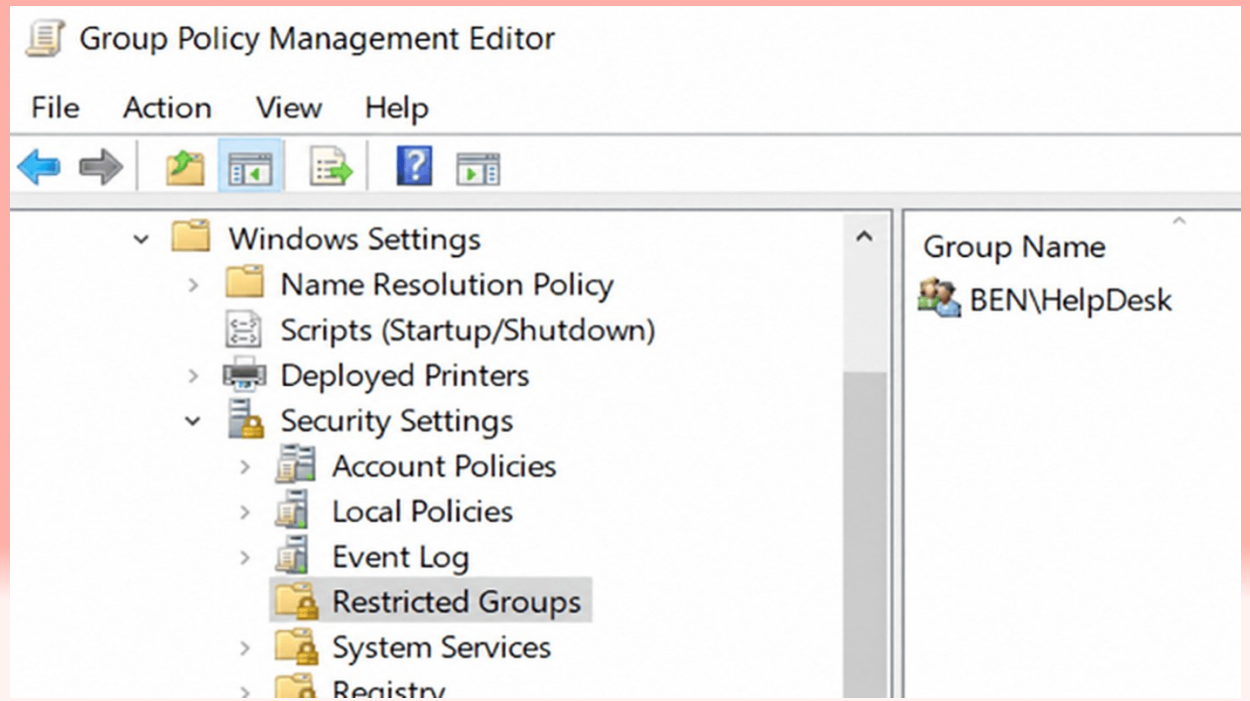
How to Instructions
Create a GPO >Edit>Comp Policy>Windows>Security>Restricted Group
Create ‘HelpDesk’>Add Members > add Group as member of ADMINS
Right click on every OU and click ‘Link existing

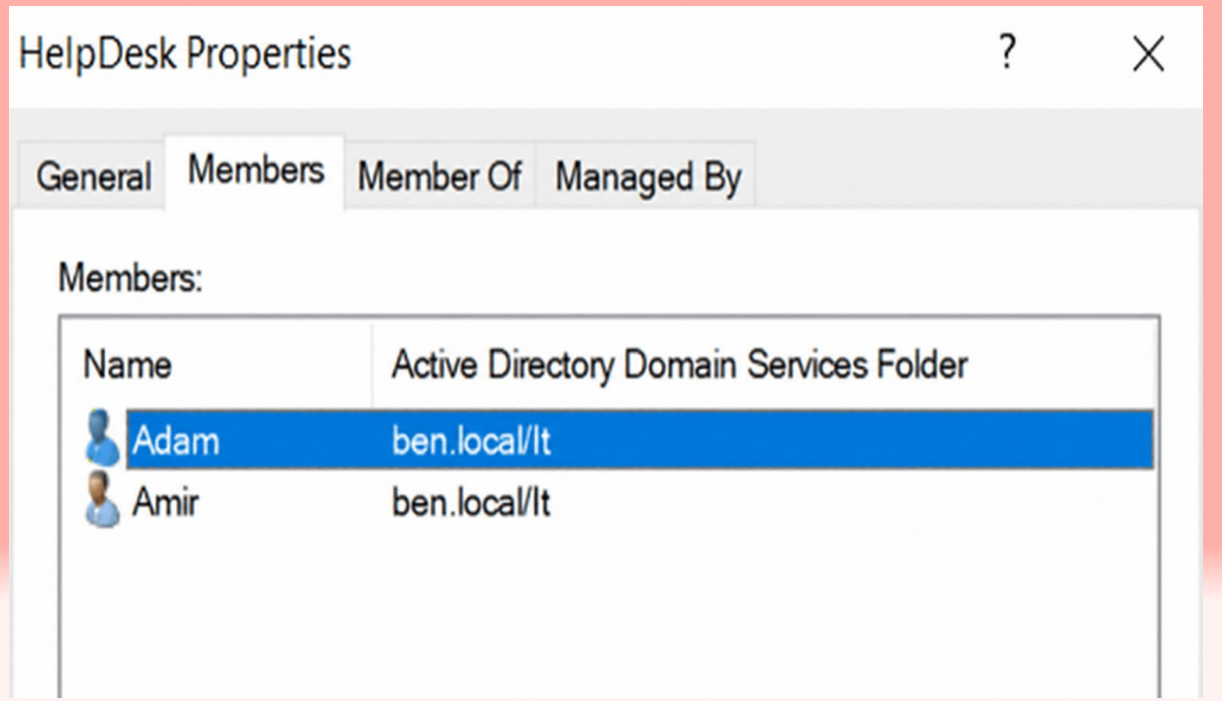
ADDITIONAL TASK
we must also account for the computer we added upon initial installation (CL1), as this comp is currently a built in container
Not actually within an OU, So in Essence, the current policy we just created does not

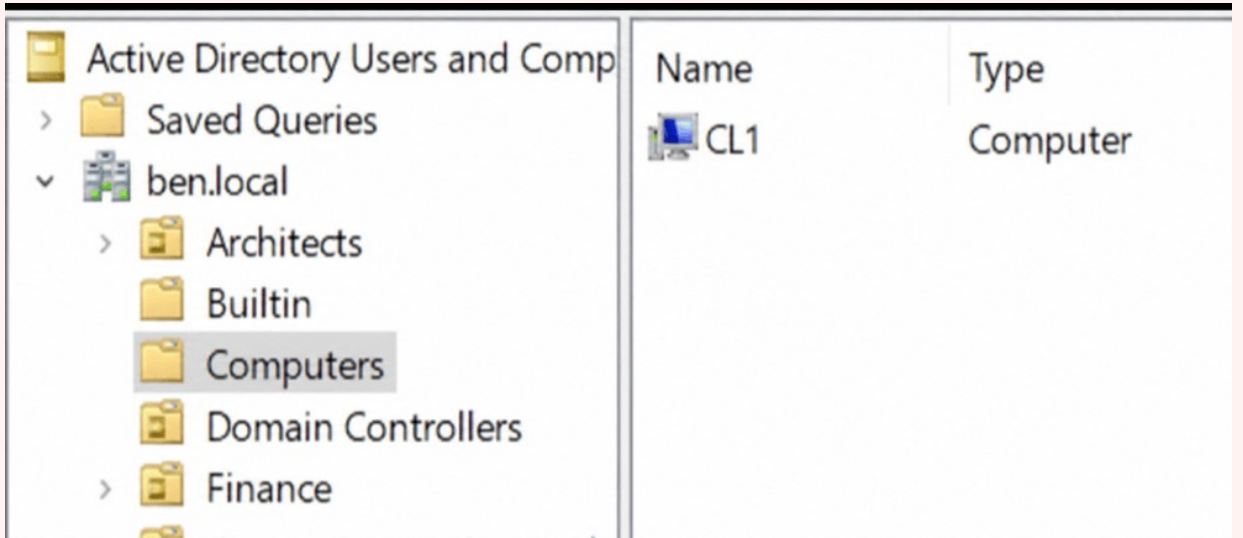
Property of Ben Halevy

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE



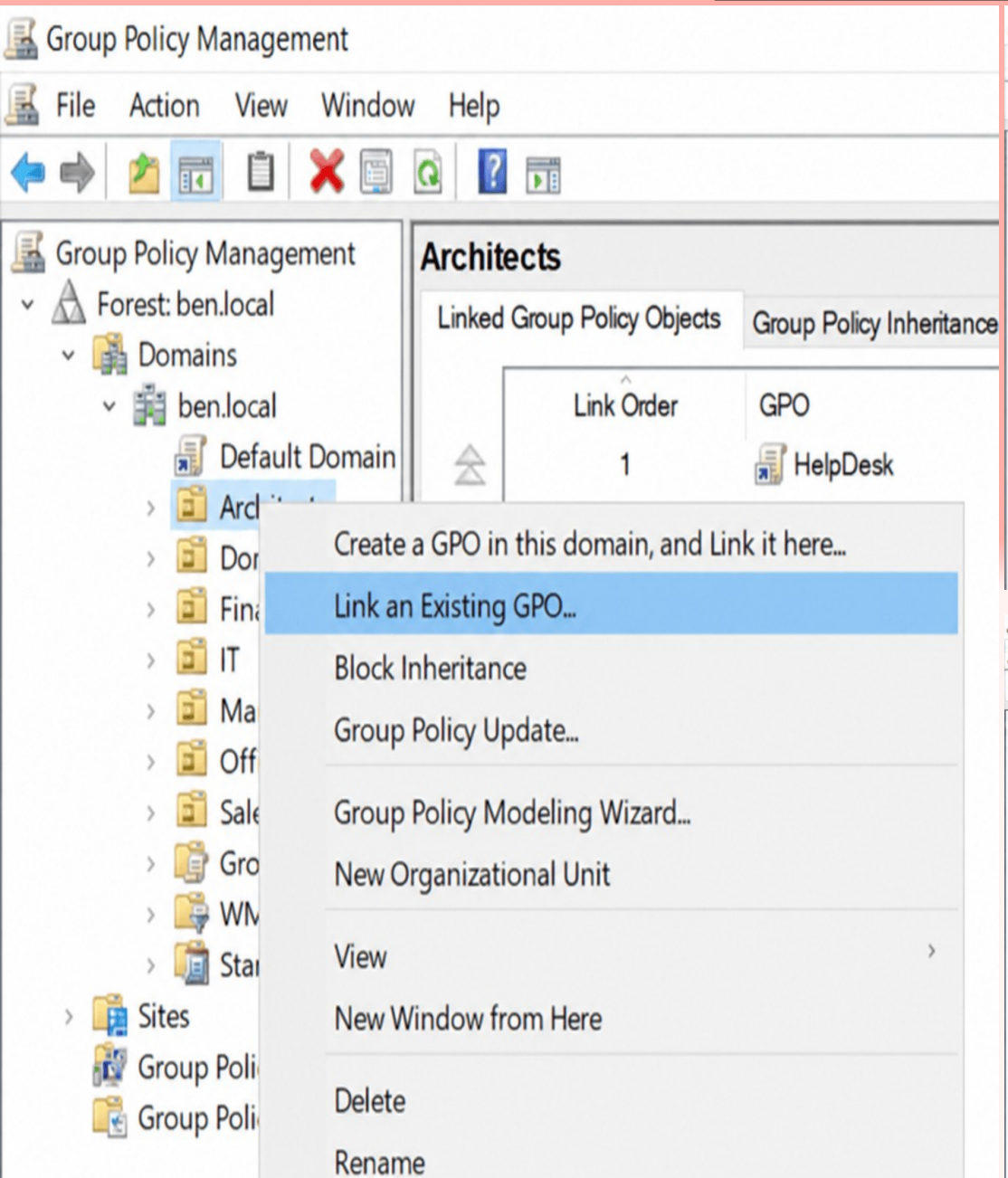


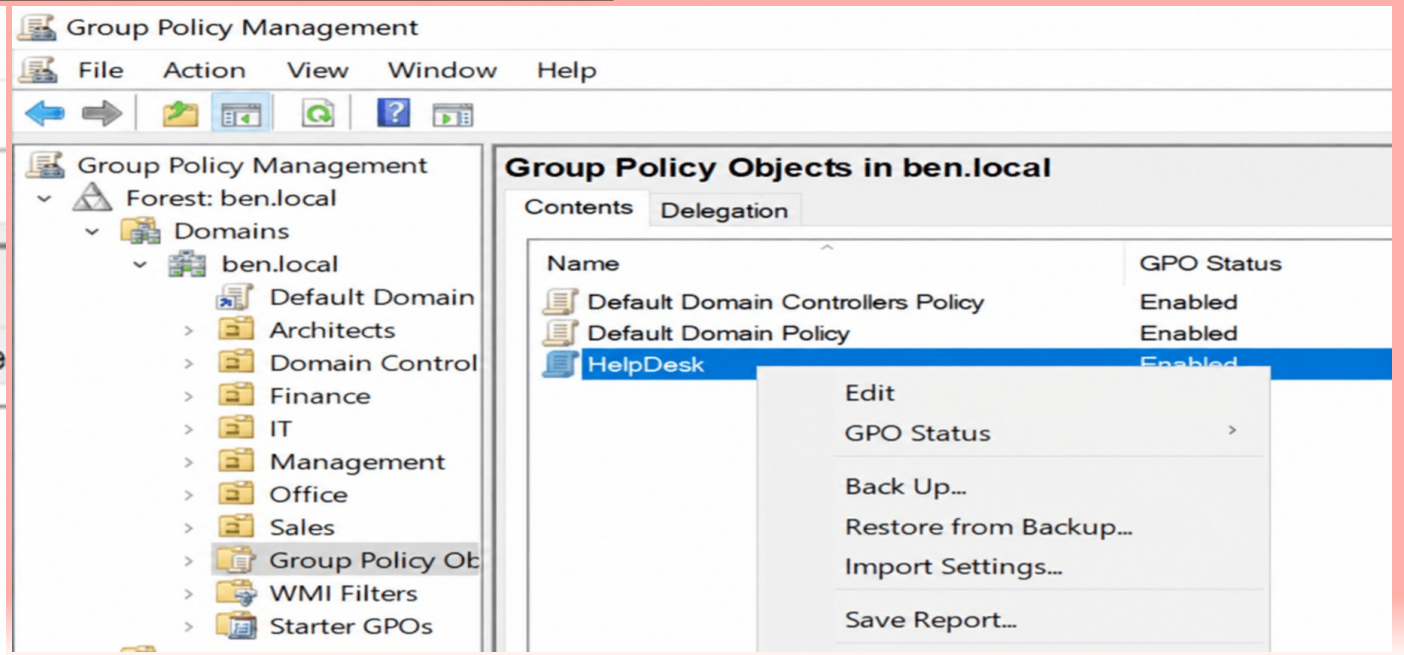


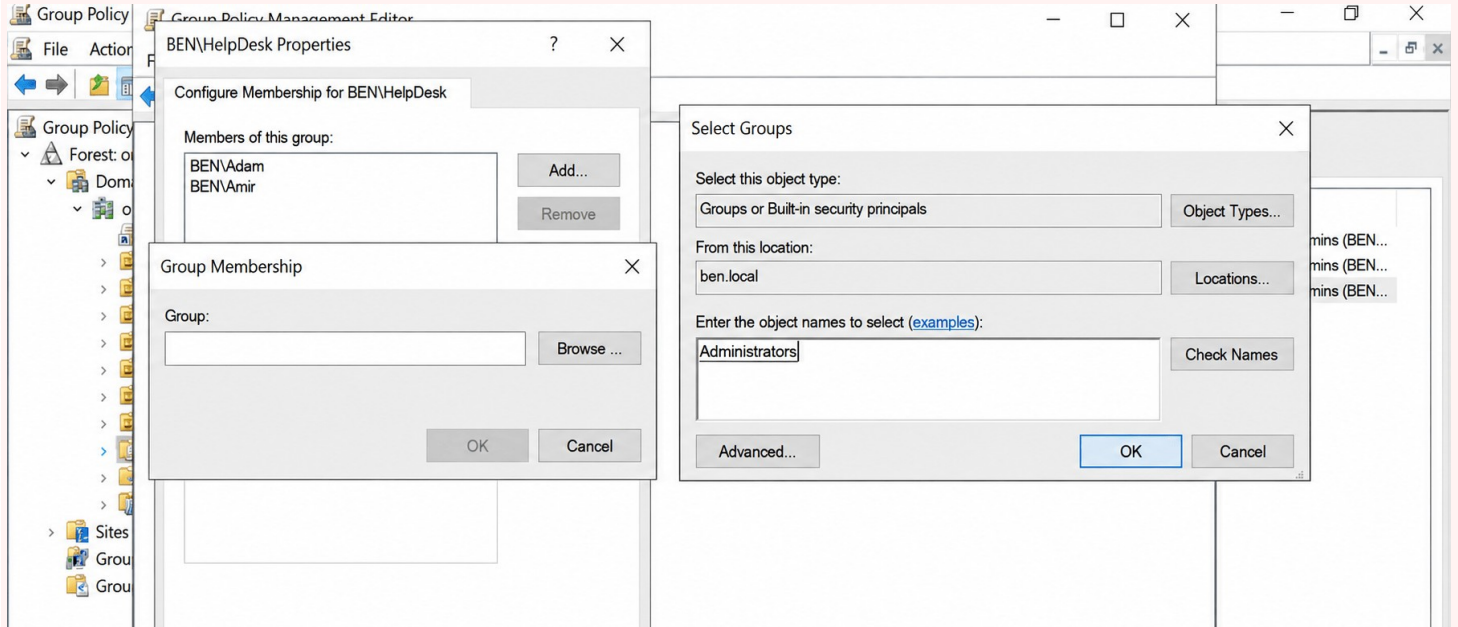
Property of Ben Halevy

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE





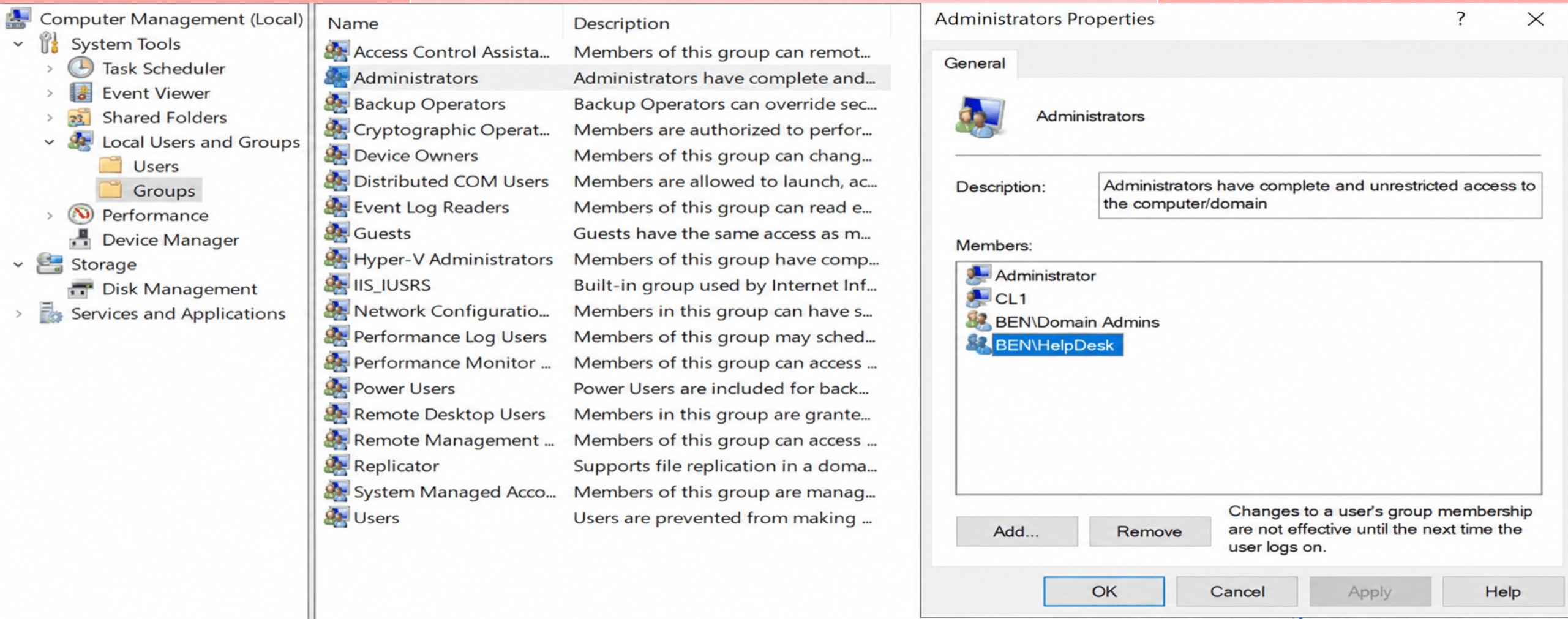


Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

TASK

Here the IT user (Adam) is Logged In to CL1 w/admin group properties



Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

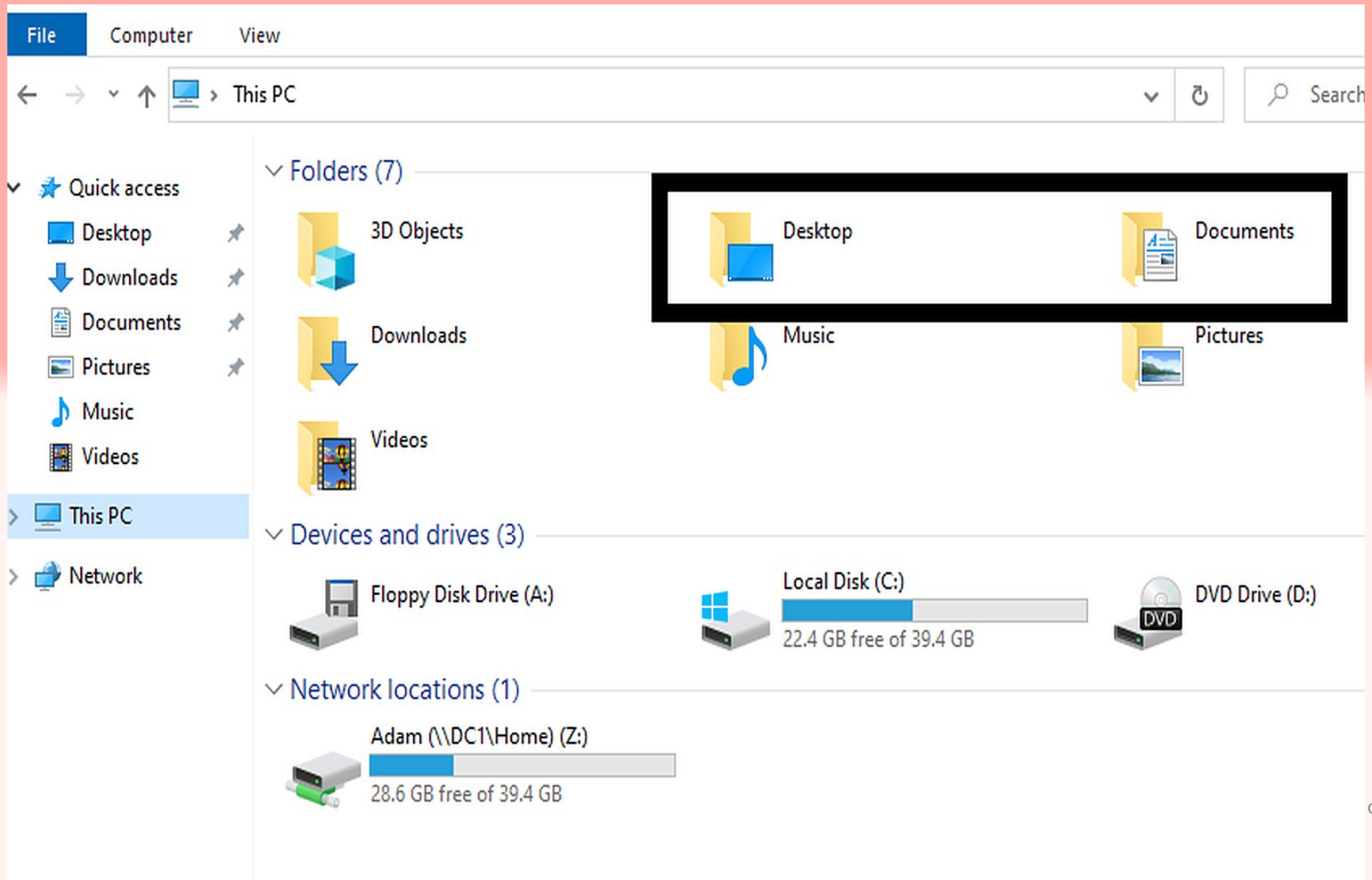
TASK
Next I will Create a Group Policy to implement a Folder Redirection for the entire organization
That way Can Designate all Desktop and Document Folders be redirected to Each Users Private Home folder.

How to Instructions
New GPO>Edit>User Policy>Windows>Folder Redirection>
right click on ea Folder>Target>Setting>Basic> In the Target
Folder Location> create a folder for each user>

Property of Ben Halevy

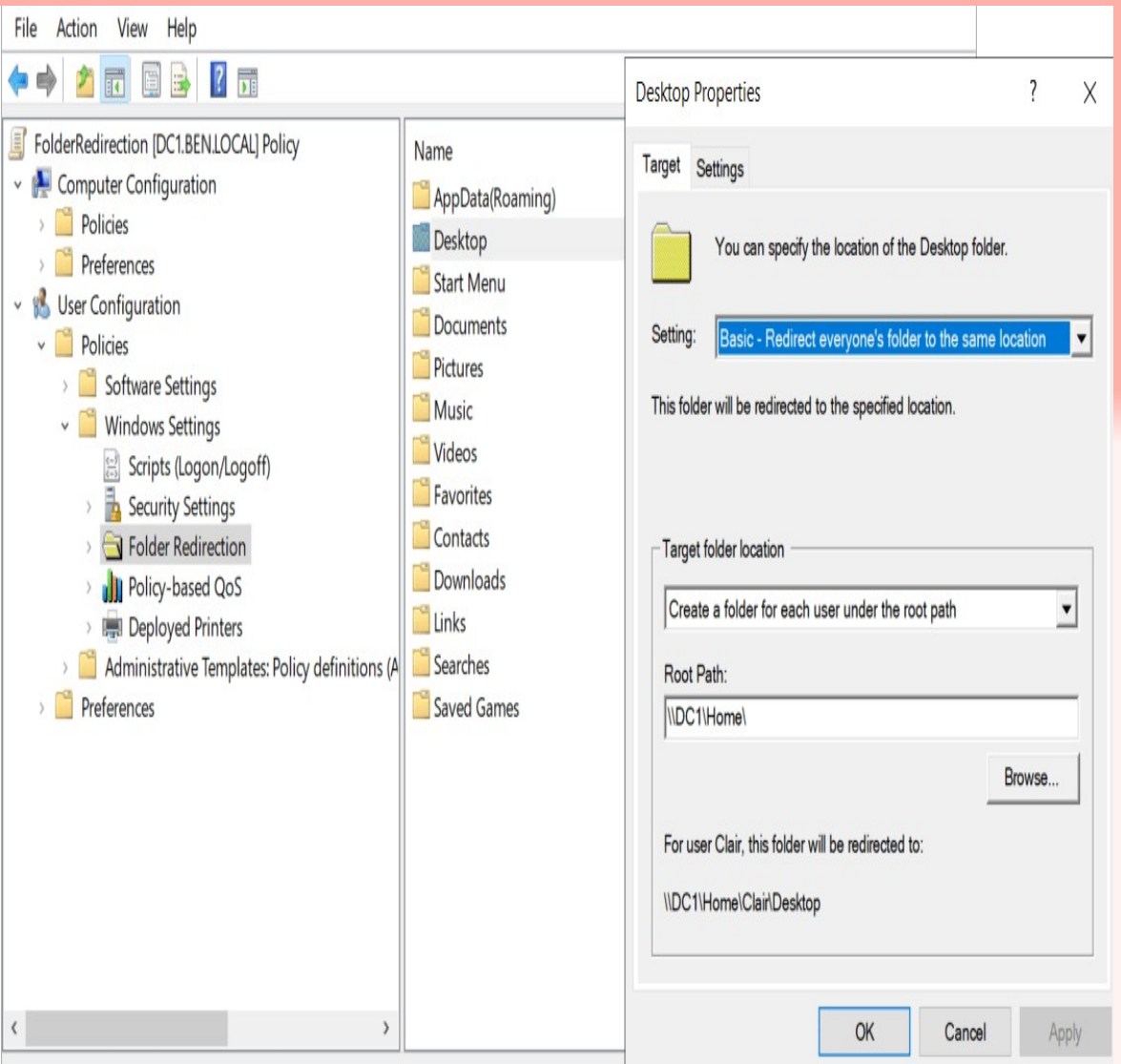
Mission Parameters

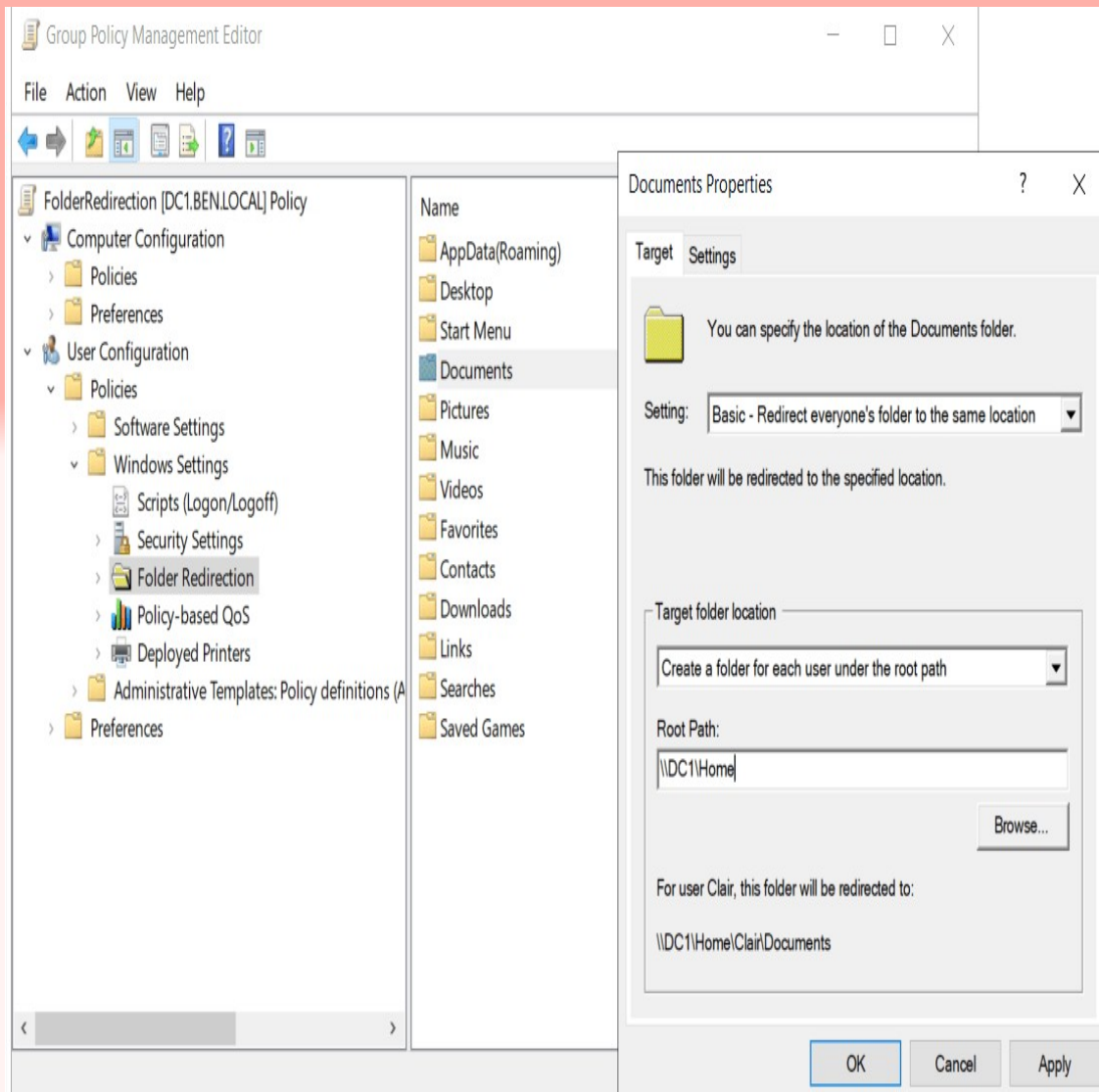
ORGANIZATIONAL INFRASTRUCTURE



Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

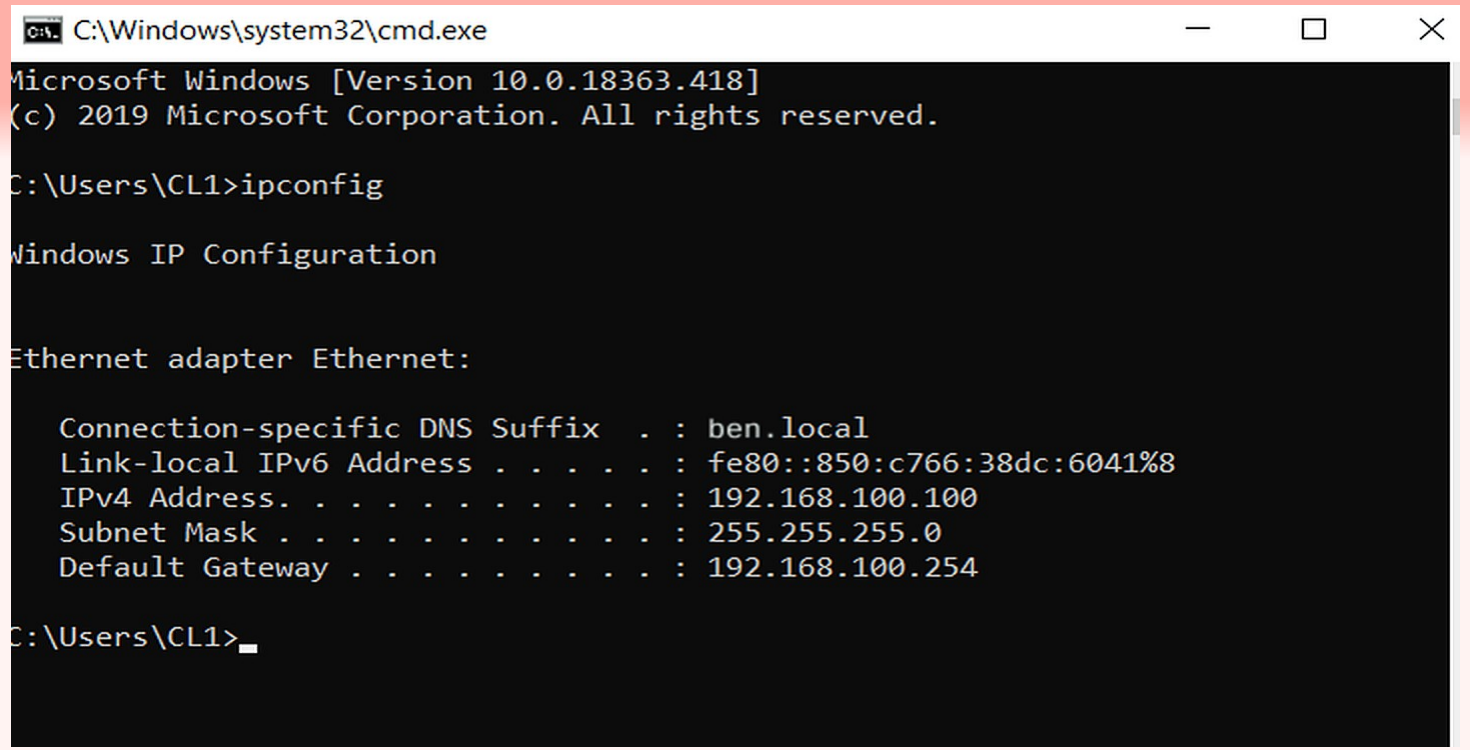




Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

TASK
So far I have completed 10 mission Parameters, I want to make sure
The DHCP Service is still active so I logged into CL1 for an Ipconfig check



Property of Ben Halevy

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

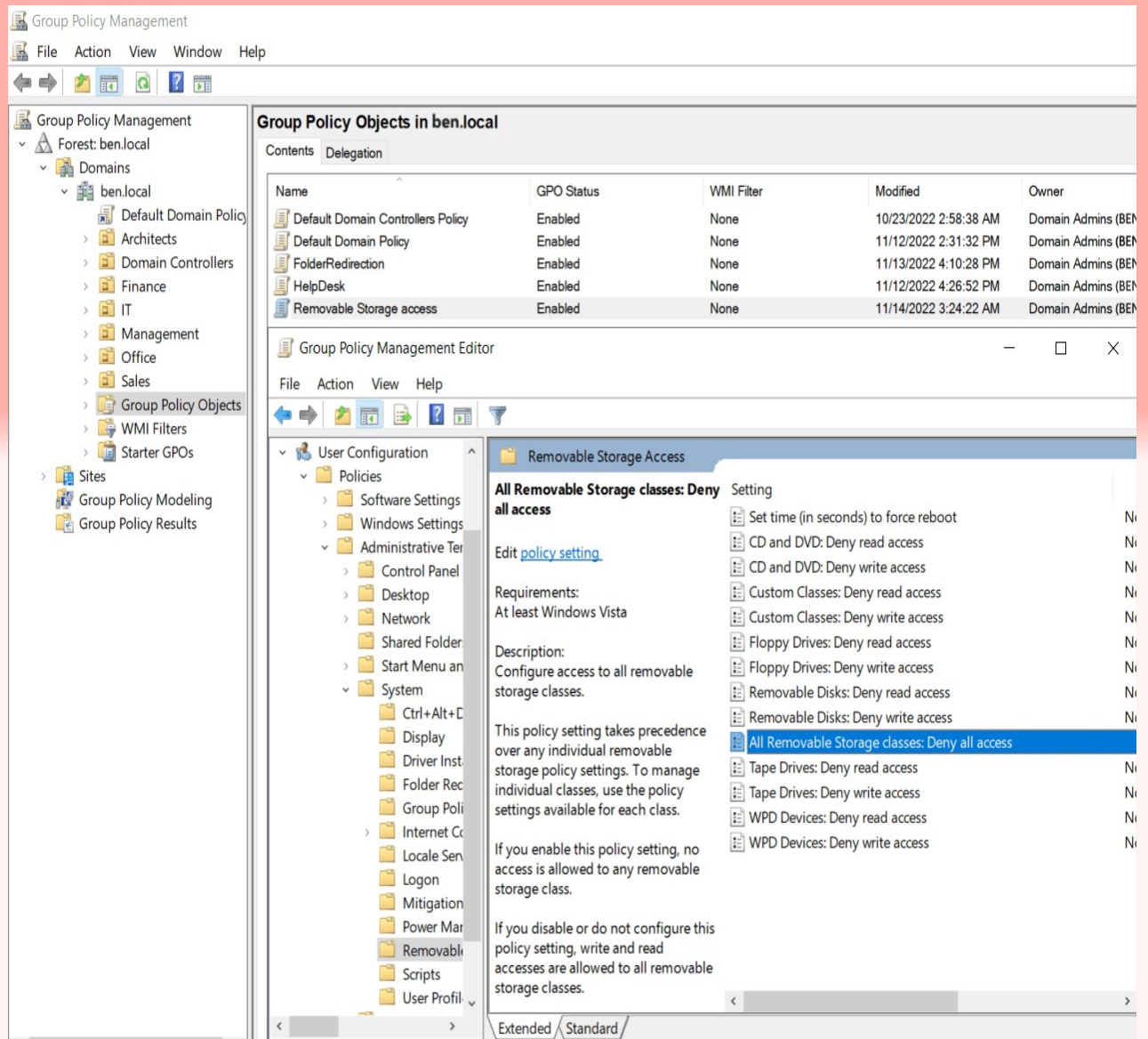
Task
One of the most vulnerable threats in an organization's security Is Human Error
As such I will be blocking the sales dept from having access to the usb ports at their end points.
To Perform this I will be using a GPO to block all access to removable storage

How to Instructions
GP Management> New GPO> edit> renamed Removable storage access> User policies>
admin temp> system> remove storage access> Right click Deny all access> enable>
then link existing GPO to the Sales OU> Gpupdate /force

Property of Ben Halevy

Mission Parameters

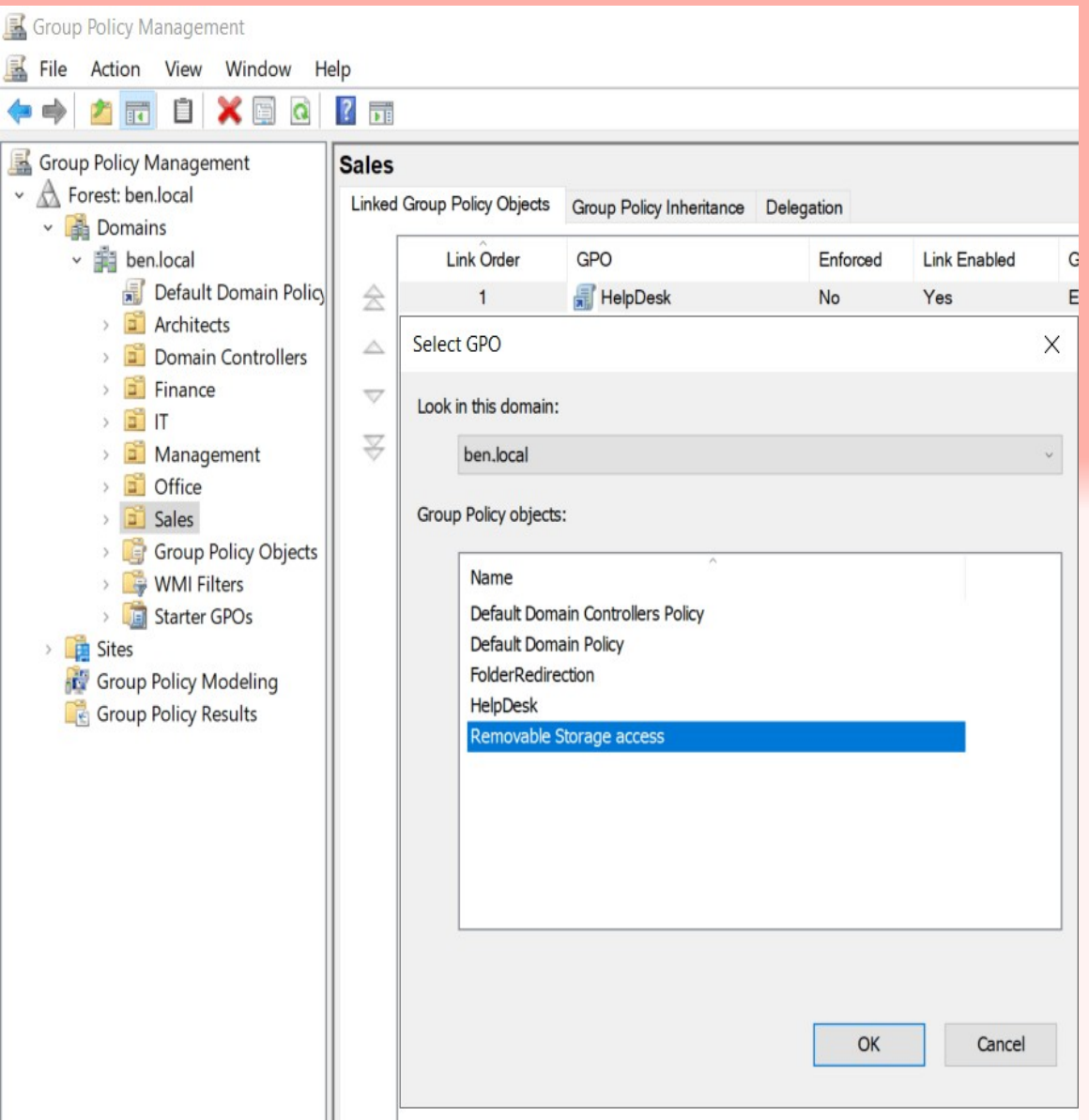
ORGANIZATIONAL INFRASTRUCTURE

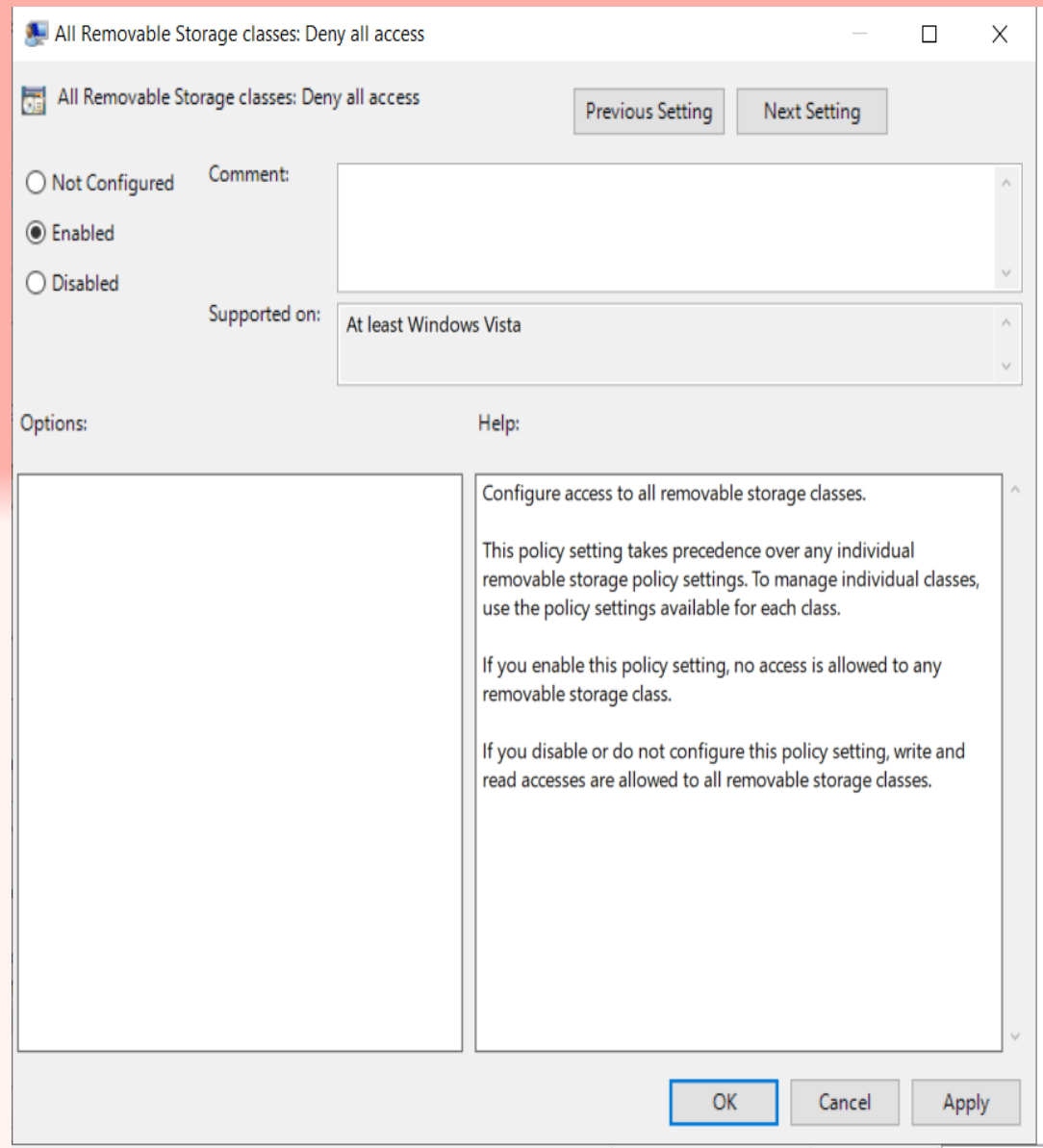


Property of Ben Halevy

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE





Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

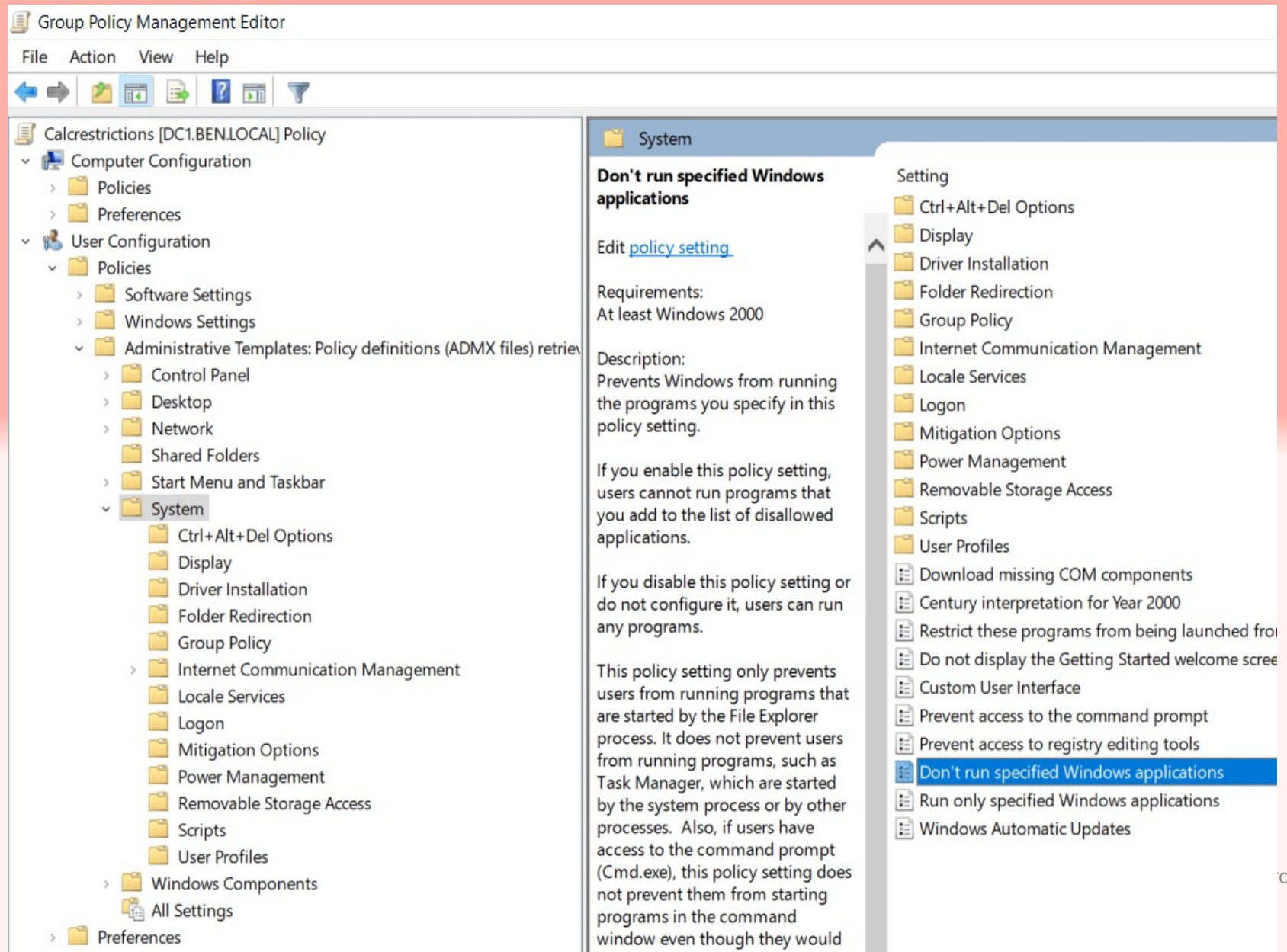
Task
The Calculator program in the office dept is a known security Threat to combat
such a threat I will remove access to the program from The entire OU.

How to Instructions
New GPO> edit> User Policies>Admin Temp> System> Double Click
Don’t Run Specific Win Apps> Enable> Show Disallowed apps> under
Value enter the Executable command for the Program you want to

Property of Ben Halevy

Mission Parameters

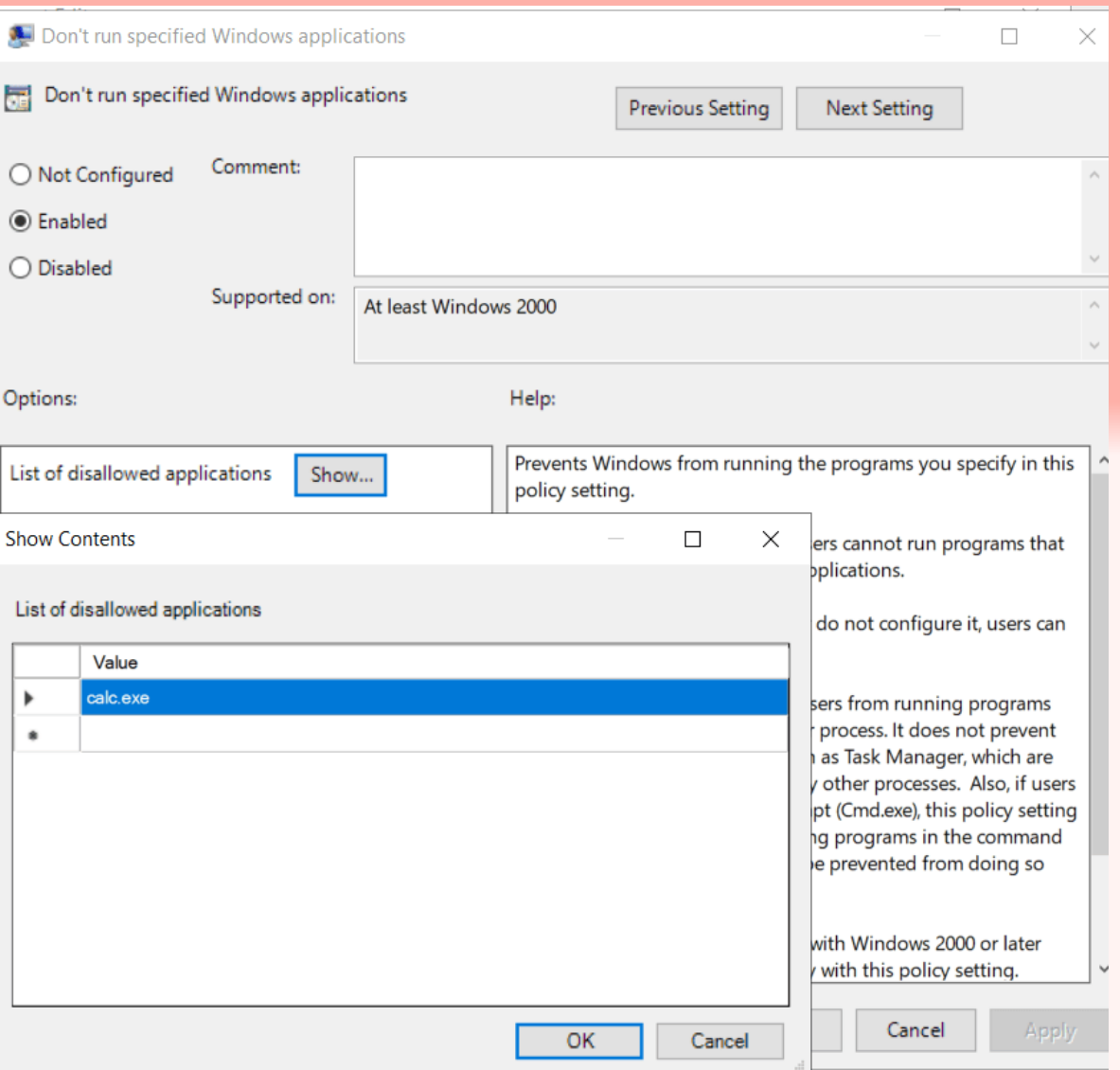
ORGANIZATIONAL INFRASTRUCTURE

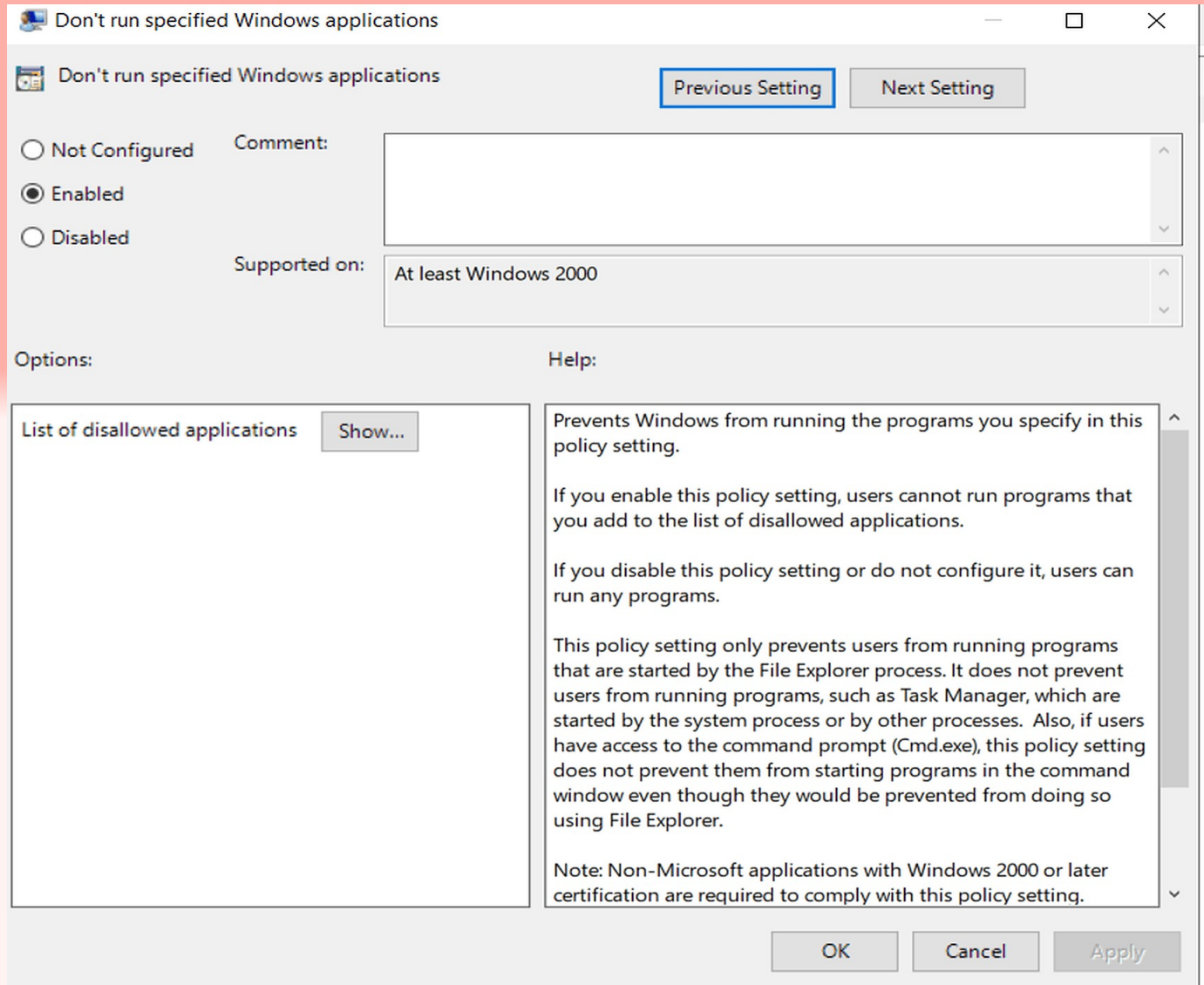


roperty of Ben Halevy

Mission Parameters

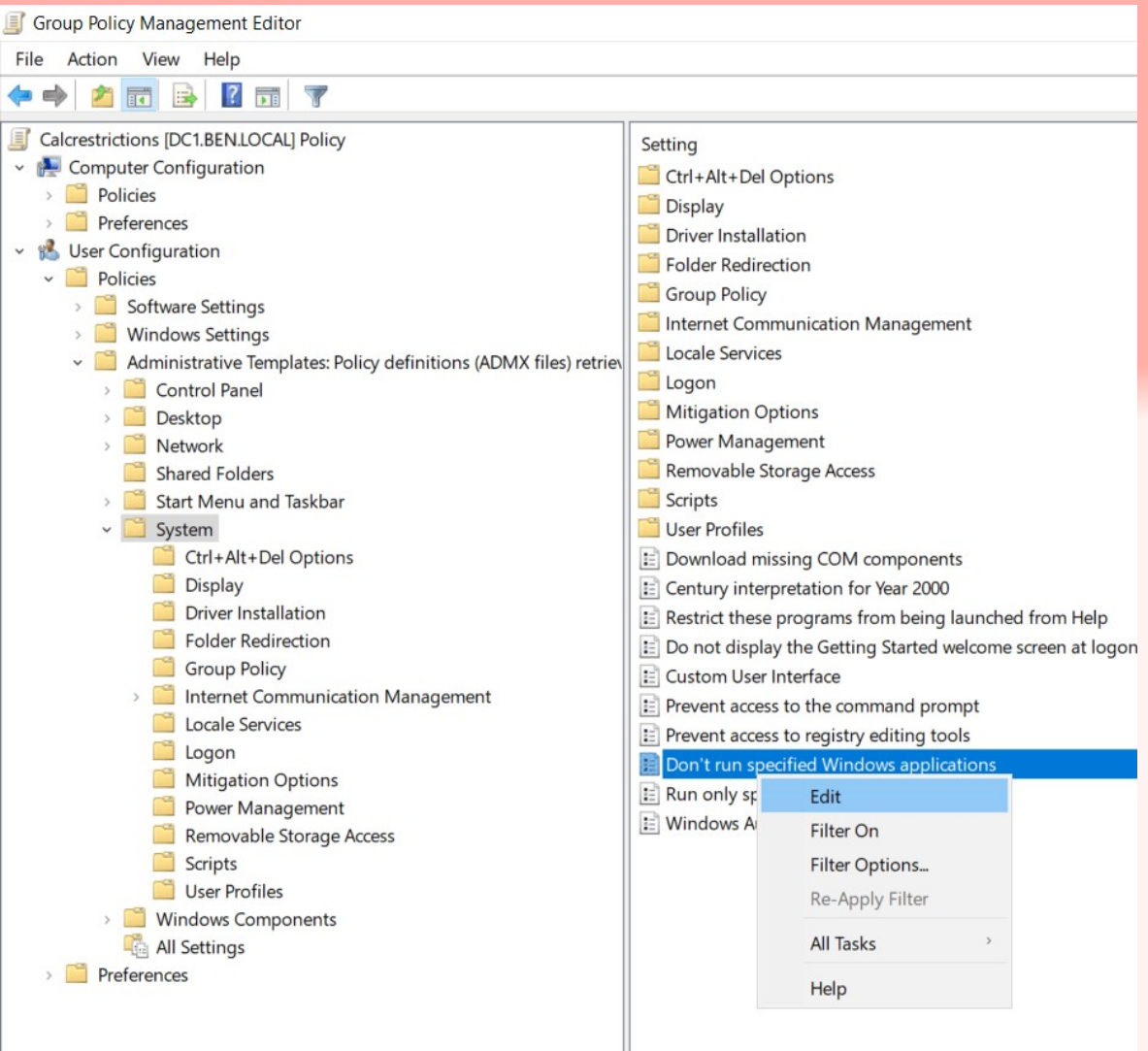
ORGANIZATIONAL INFRASTRUCTURE

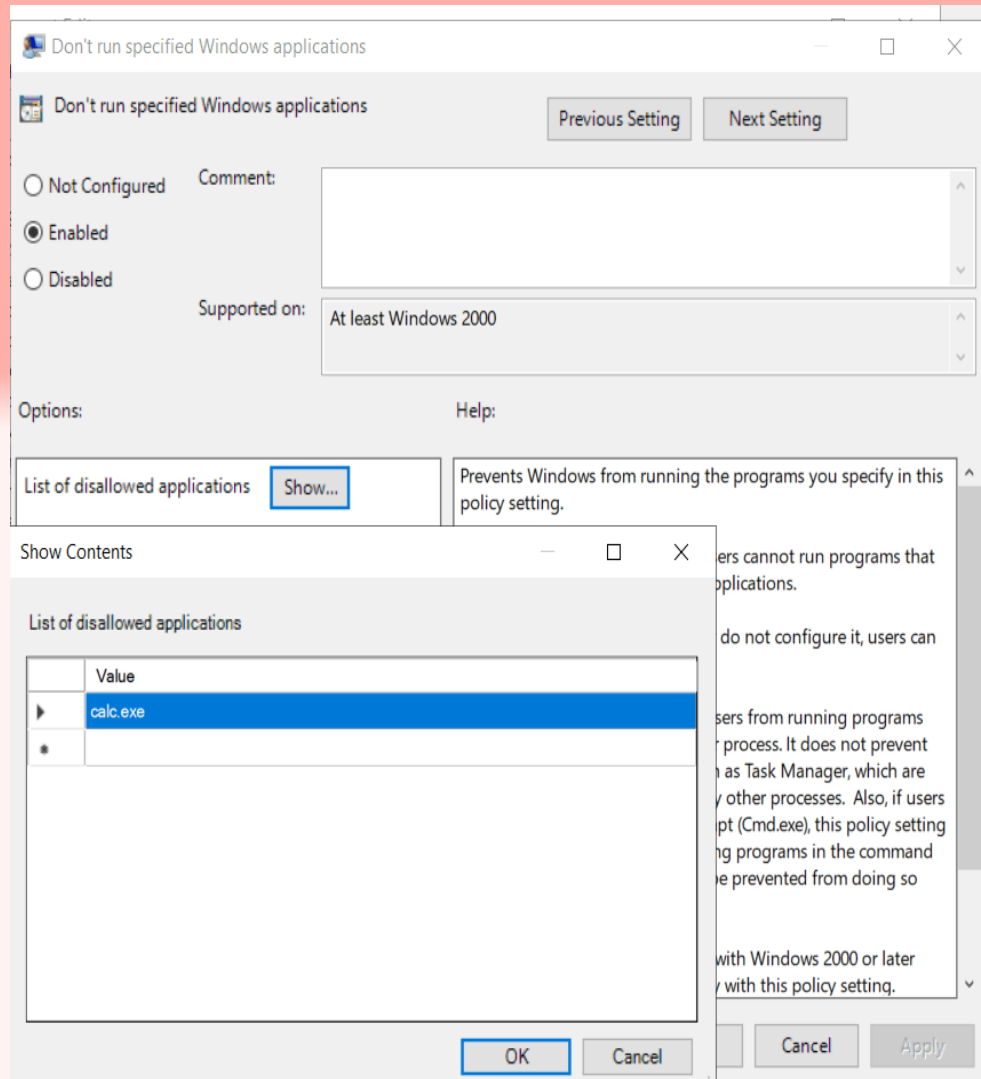




Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE





Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

Task
I created a Folder (C:\Reports) on the DC1 Server to be shared within the network
I will map the Folder to all the Organizational endpoints as drive Y:
This Folder will have specific Permission protocols :
Sales, Finance, Office and Architect Employees will have Read only Permissions
The Management Dept. will have Read and Write Permissions
The IT Employees (Adam and Amir) will have no access to the Folder at all
The IT Employee(Alex) will have FULL CONTROL over the Folder

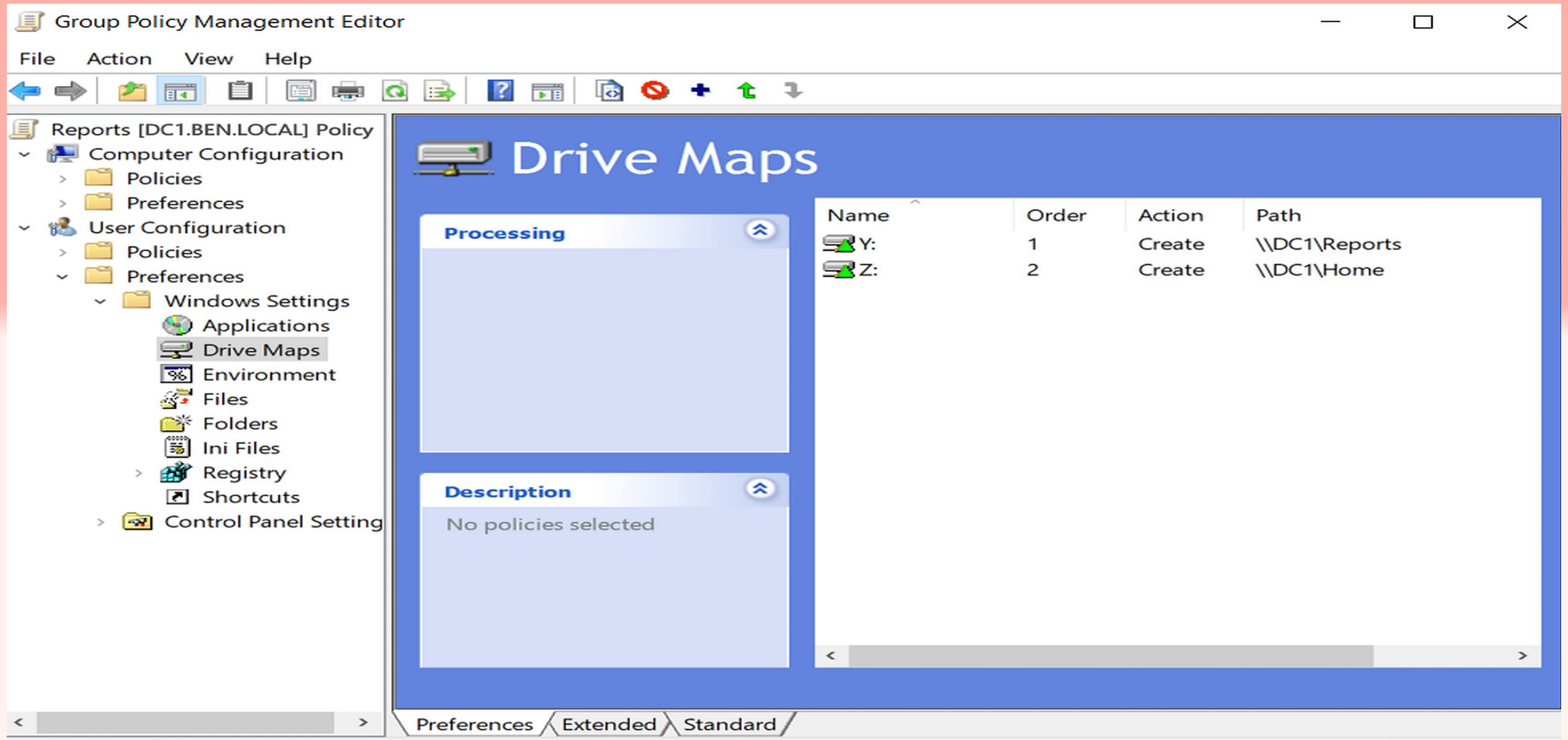
FYI Organization

's are Containers

First we employe
Create Folder in C:Reports >Share Folder>create a GPO>Edit>UserPref>Windows>Drive Maps>New> Action:Create
>Location:\\DC1\Reports>Letter Y:> afterwards add GPO to each OU and

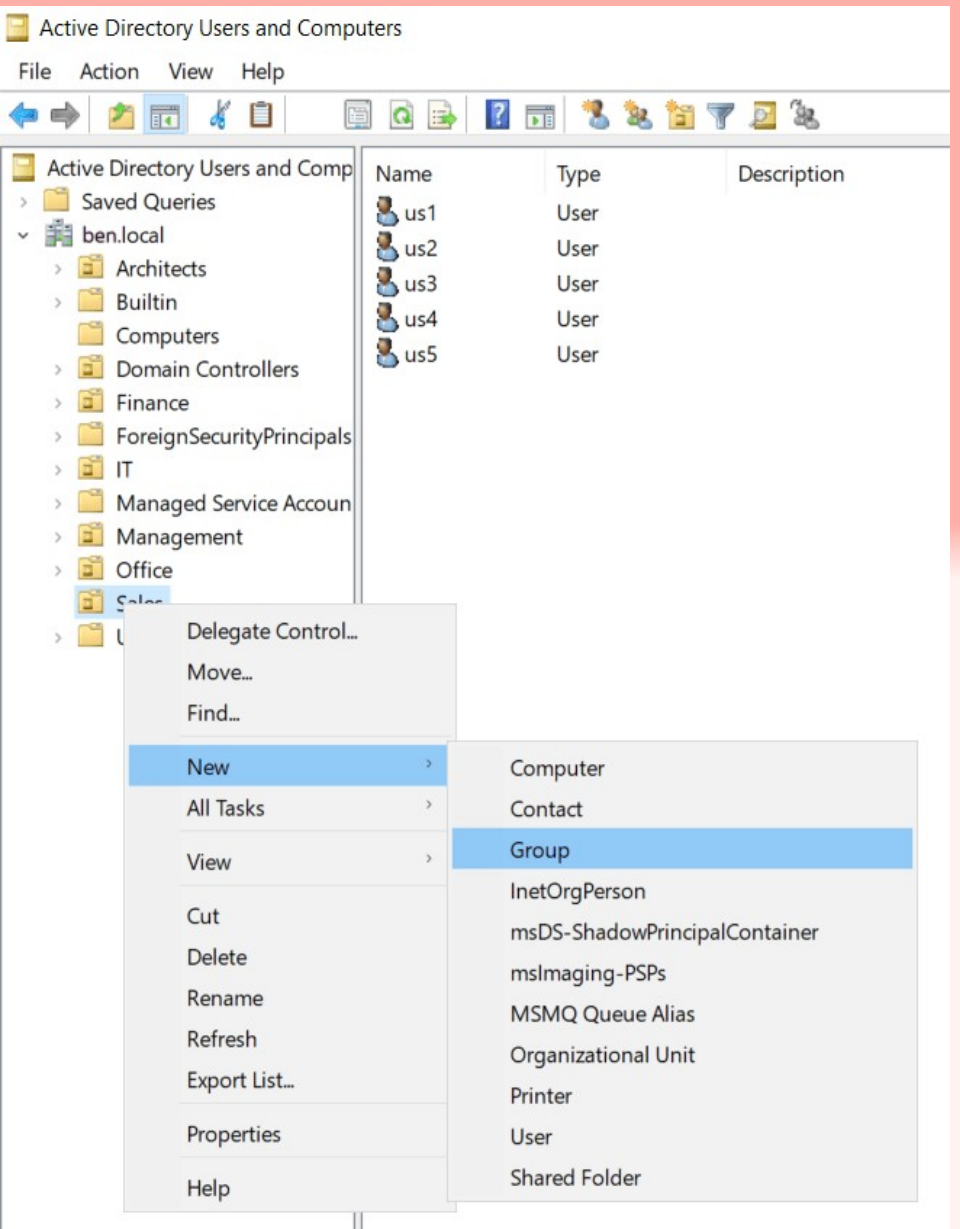
Mission Parameters

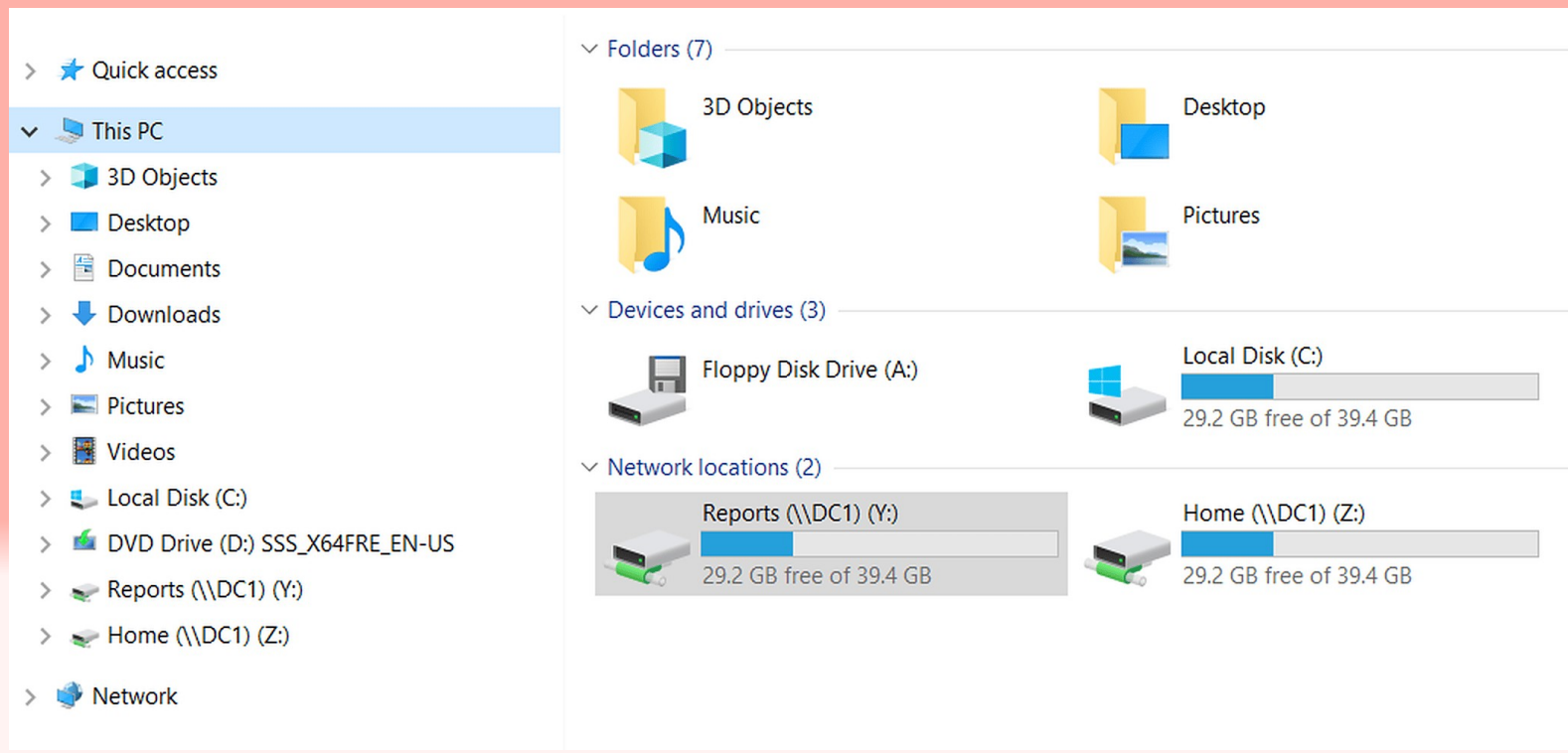
ORGANIZATIONAL INFRASTRUCTURE

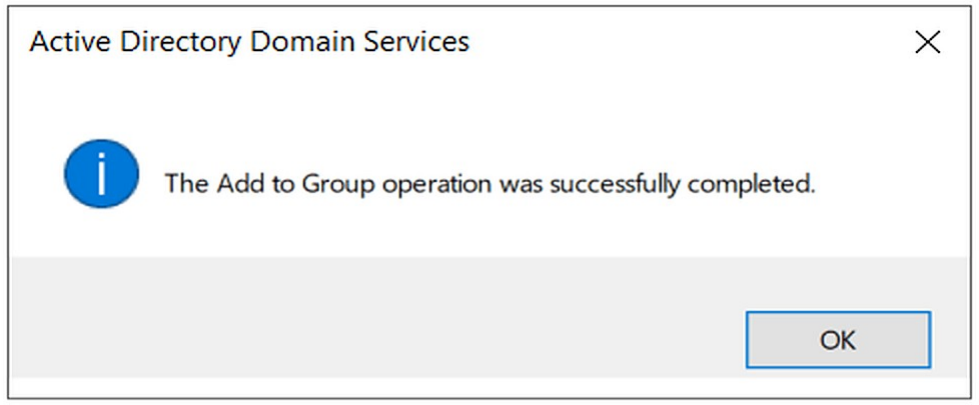


Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

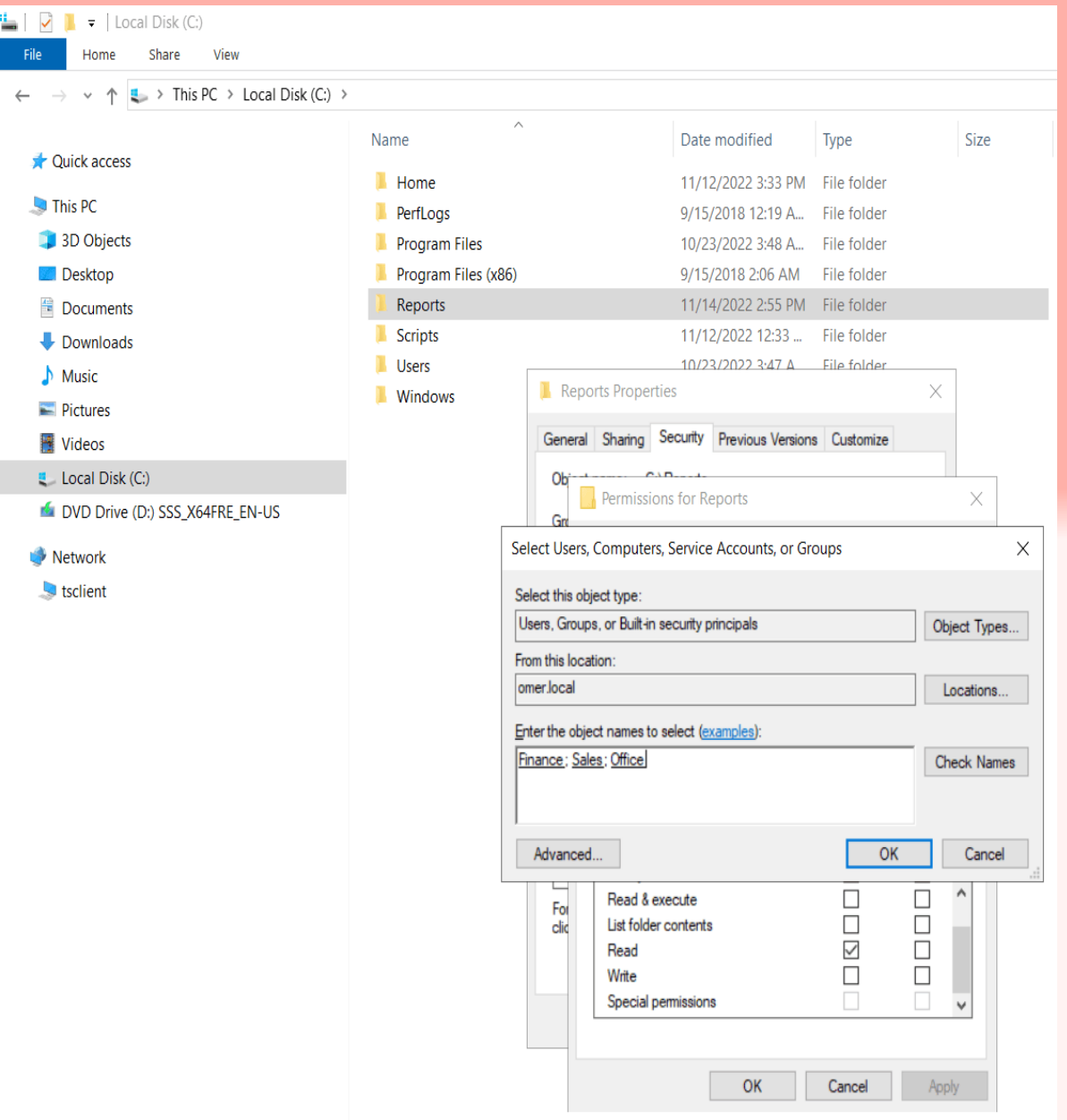


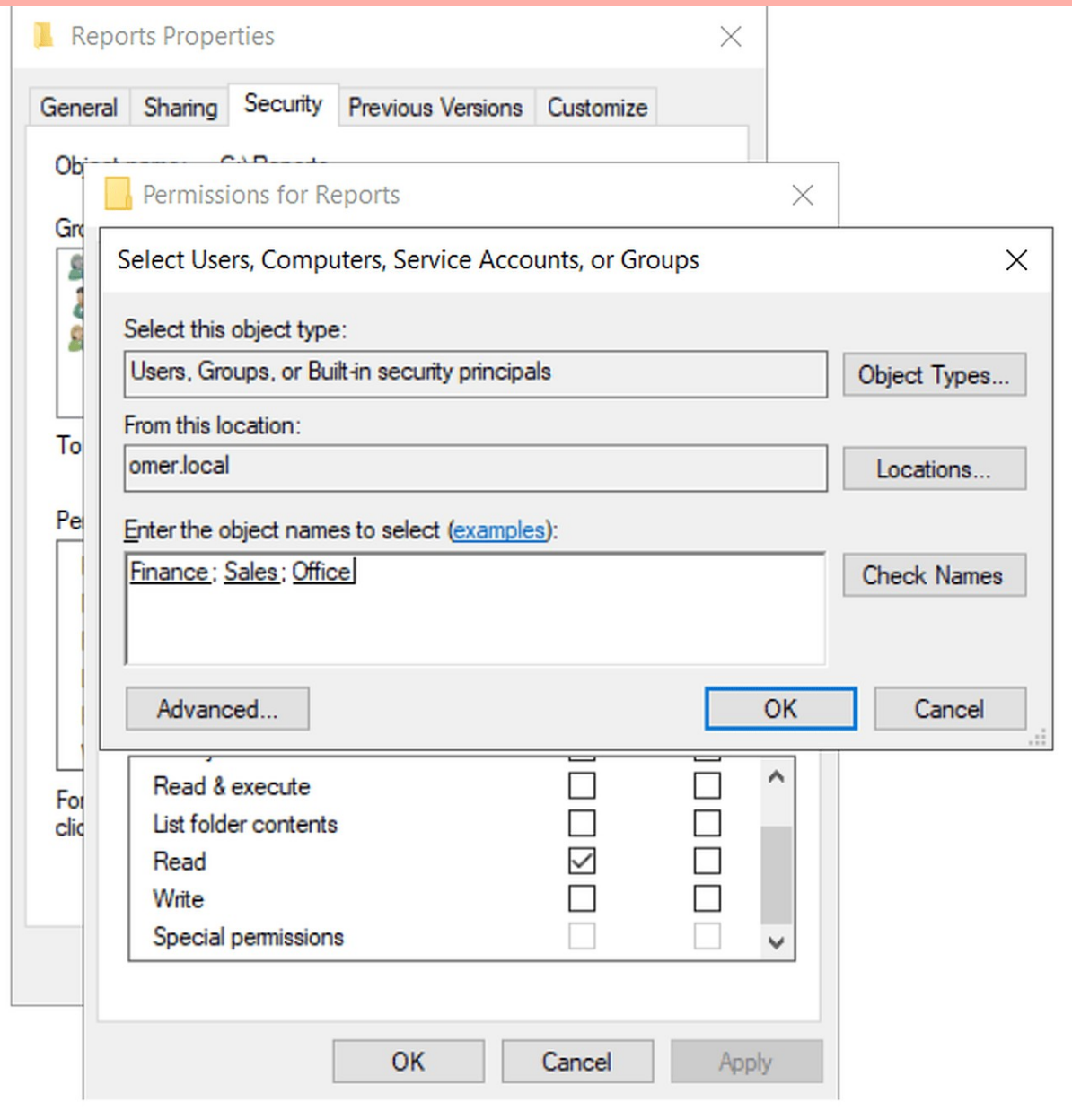




Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE





Mission Parameters

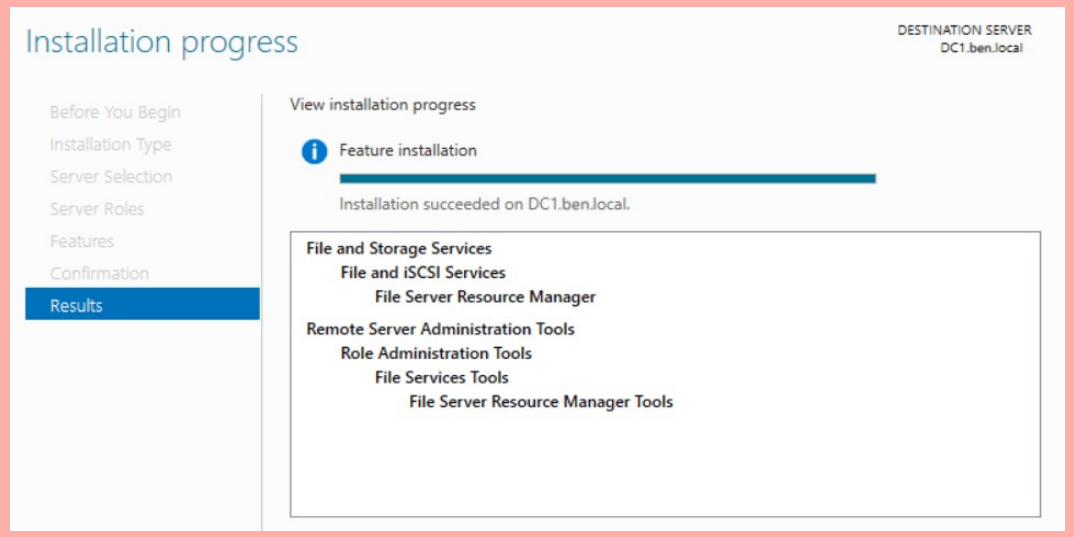
ORGANIZATIONAL INFRASTRUCTURE

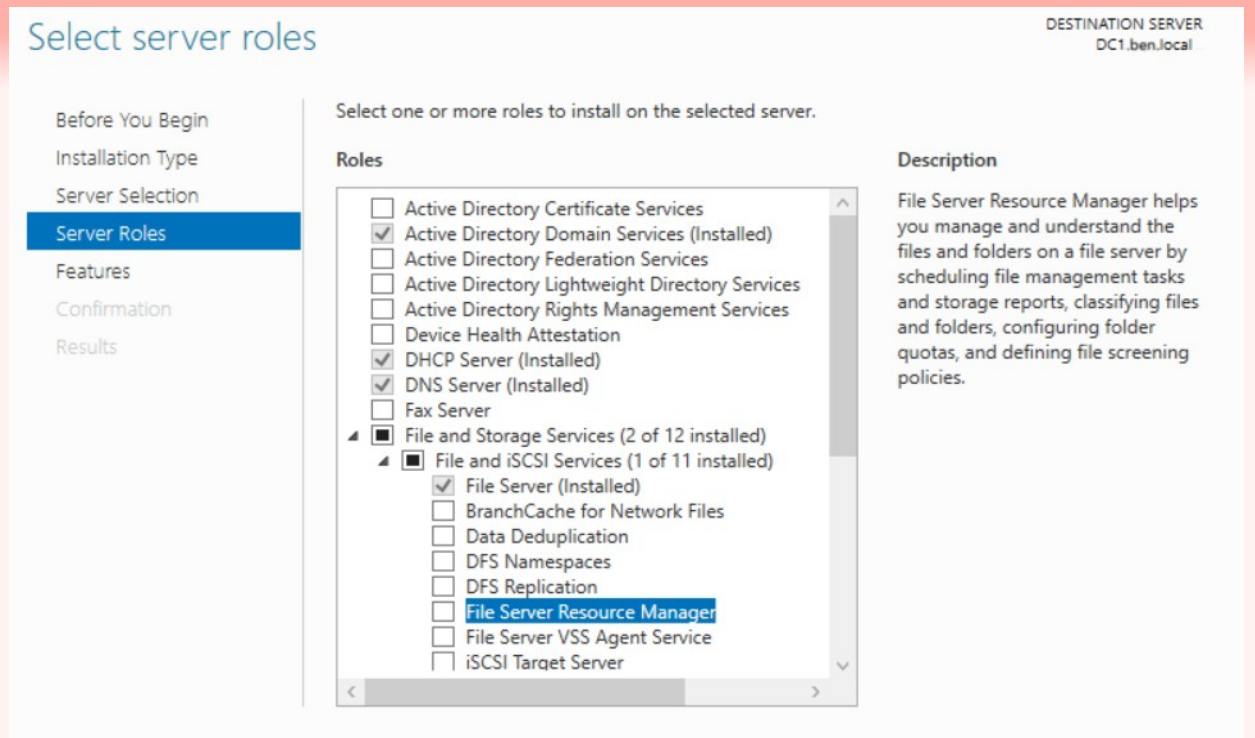
Task
Designate Restrictions on the Home and Report Folders:
a. Restrict the Home folder of all users to a size limit of 2GB
b. Restrict the Report folder of all users to a size limit of 3GB
c. Block the ability to save audio files, video files or photos in the Report folder

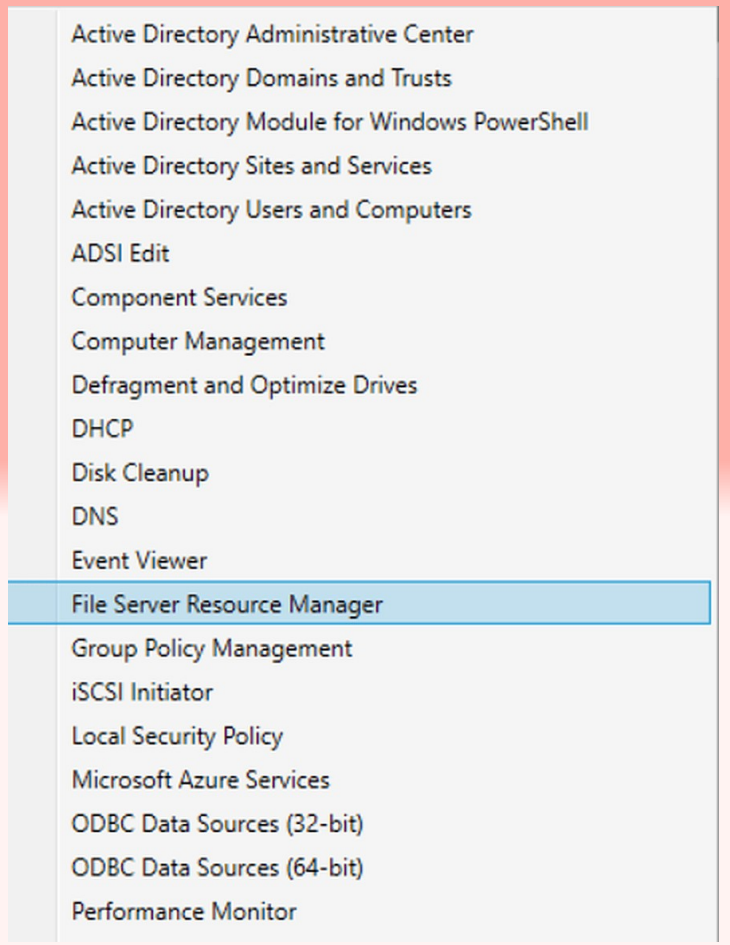
How To Instructions
1. To Place Restrictions , we first need to add a Server Role Called “FSRM” File Server Resource Manager . Active Directories need to remain
Dynamic, as such it is better to create templates that can be used again later AD Tools> File Resource Manager > Quota Management > Quota Template
> Create Quota Template > Set Name (Report) > Set Size Limit > Ok > do the same for (Home) > then go to Quotas > create >C:Home or C:Reports

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE



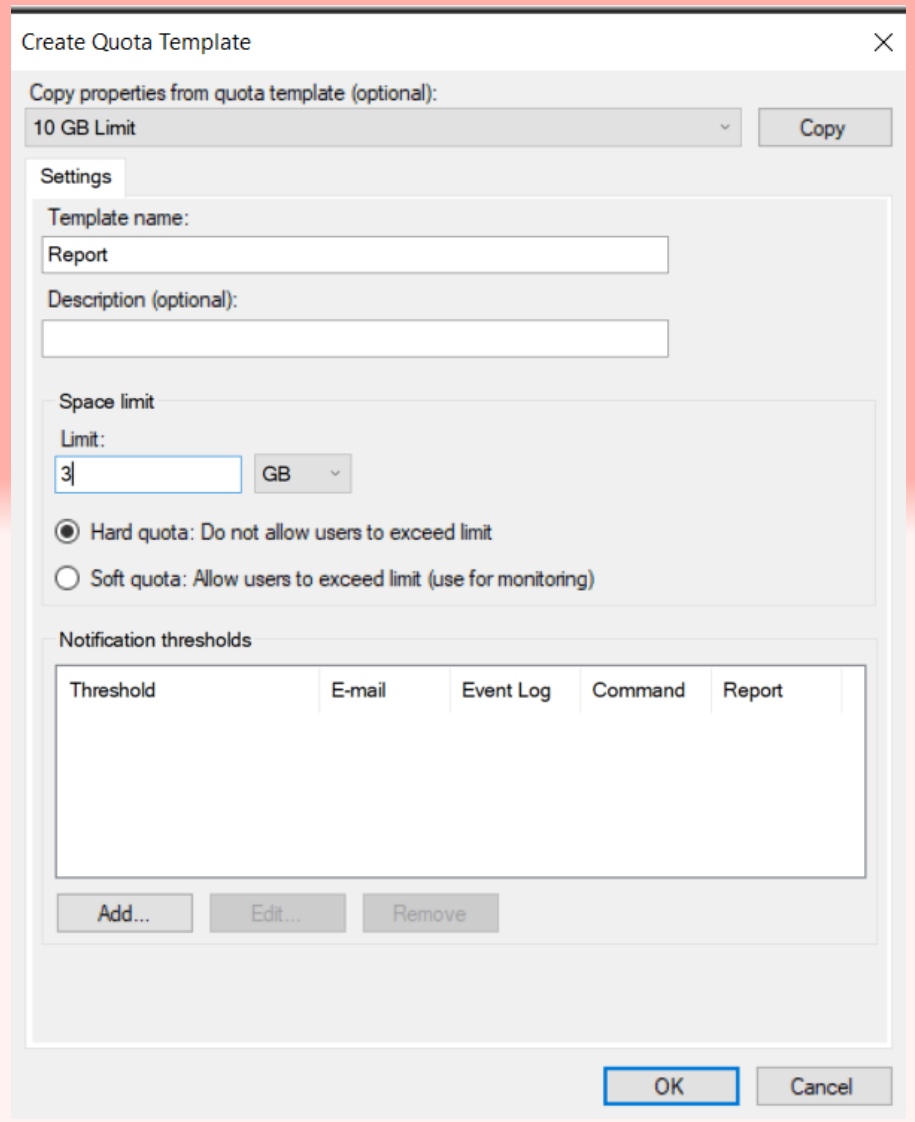


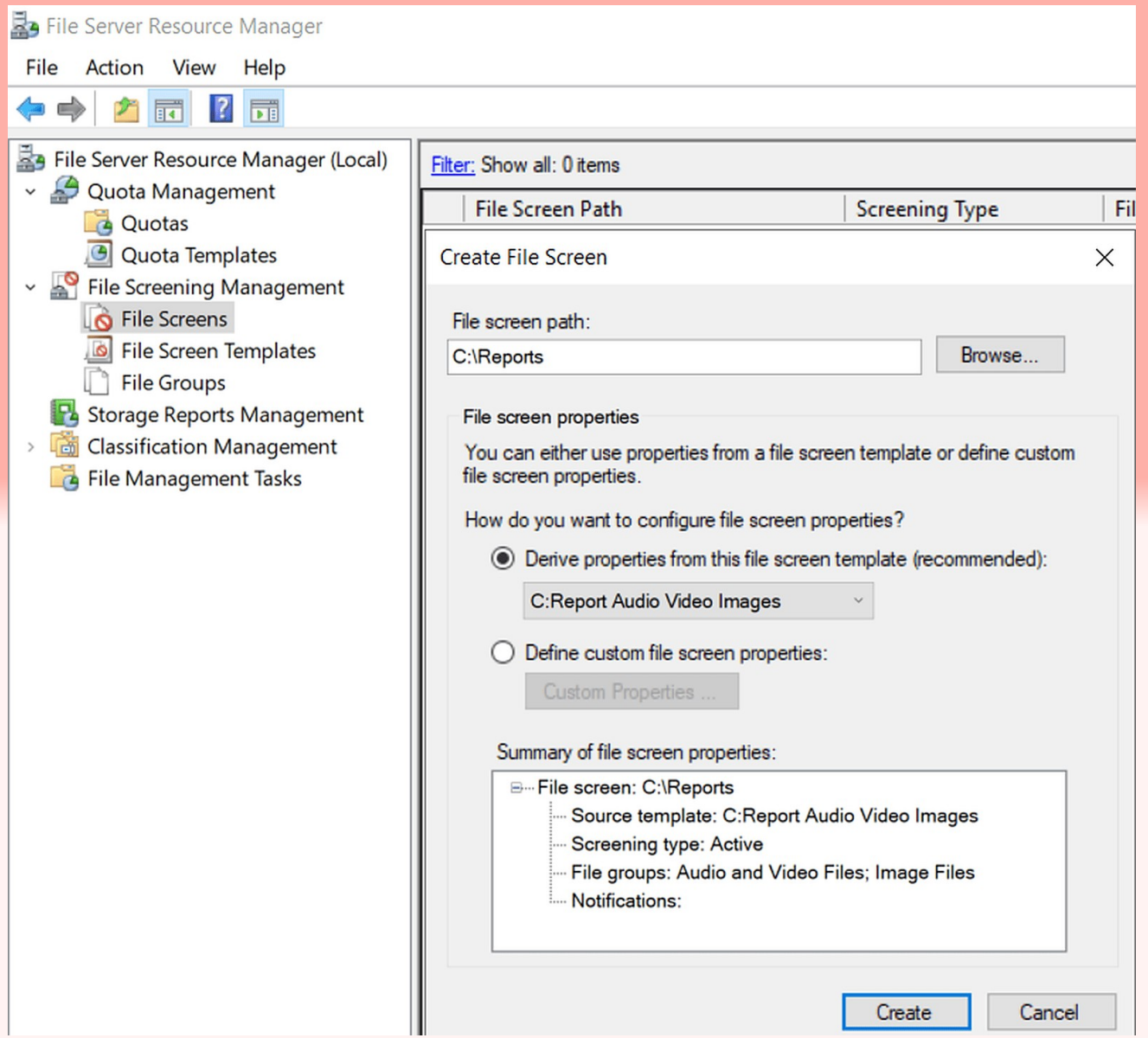


Property of Ben Halevy

Mission Parameters

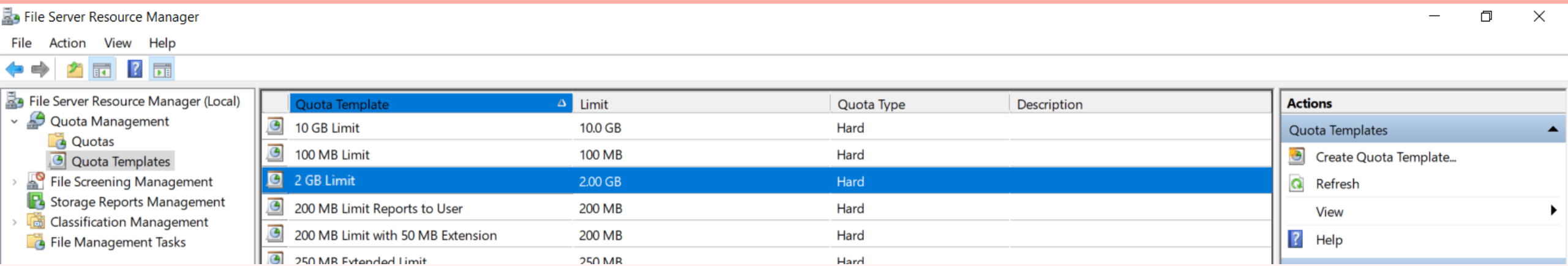
ORGANIZATIONAL INFRASTRUCTURE

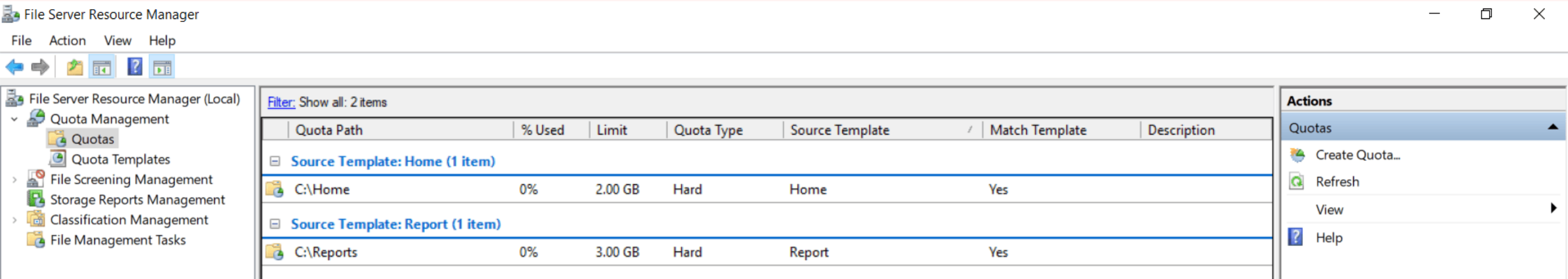




Mission Parameters

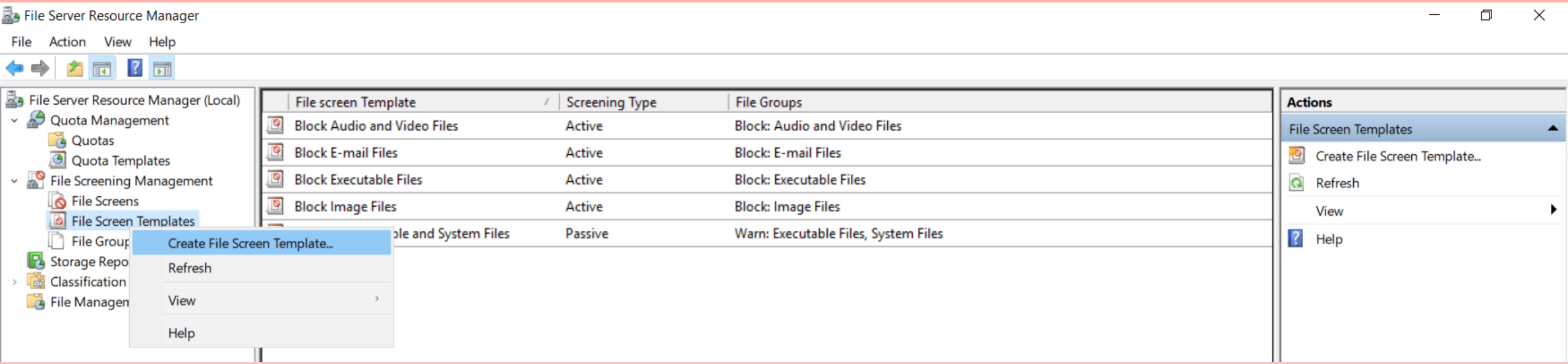
ORGANIZATIONAL INFRASTRUCTURE

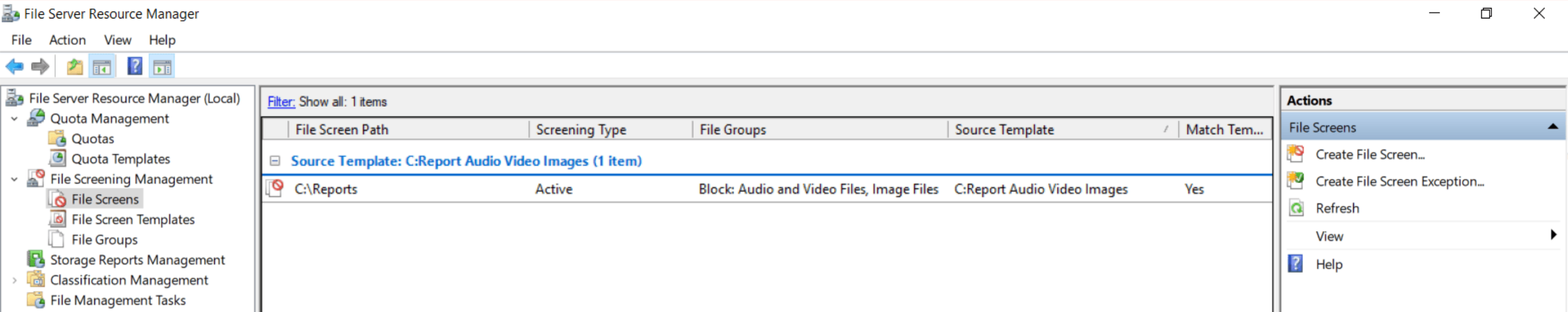




Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE





Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

Task
Designate a recovery option from previous versions of user accounts

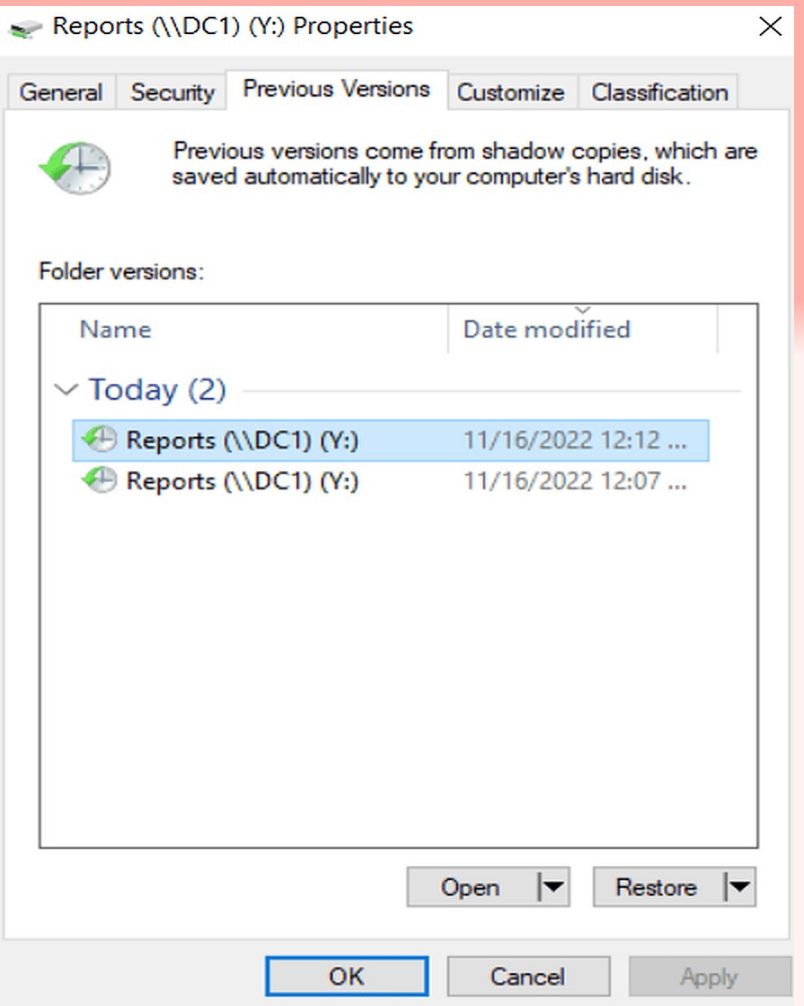
How To Instructions
This pc > right Click on C:> Configure Shadow Copies > Enable>Create Now

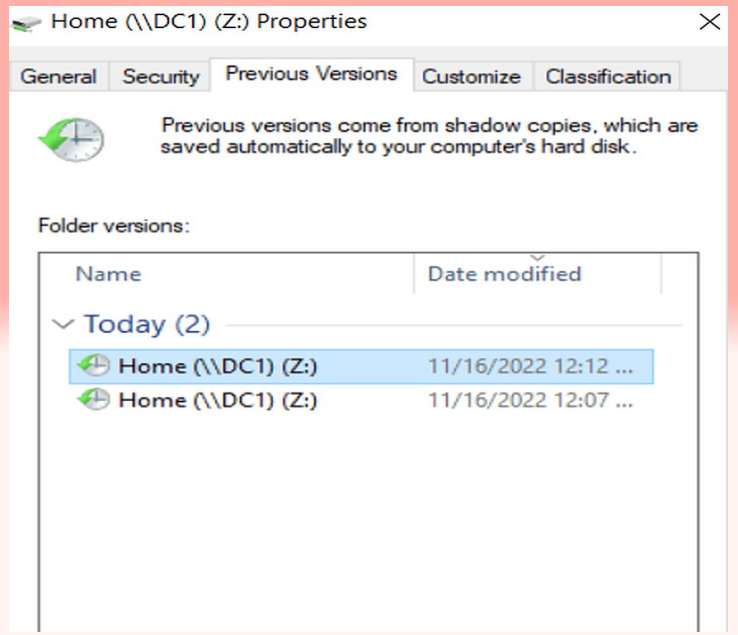
*** Important Note – This has at times disconnected network drives during the creation of a Shadow Copy , simply Right click network drive and remap the C:Home(Z:) and the C:Reports (Y:) Folders**

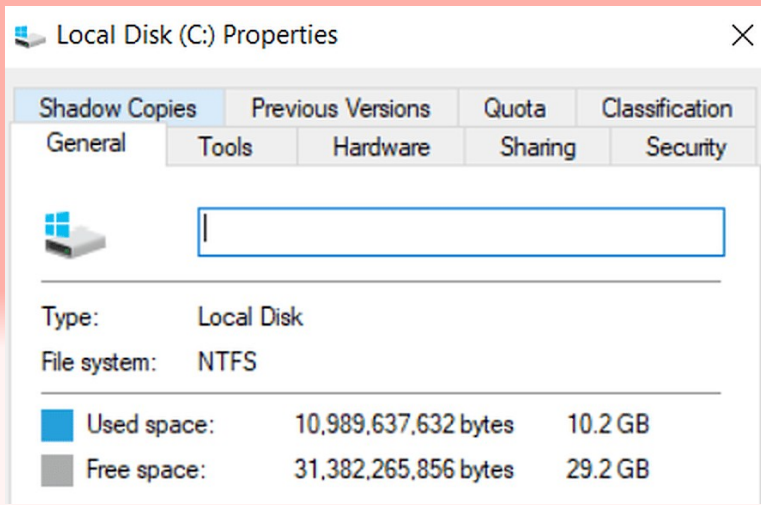
Property of Ben Halevy

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE



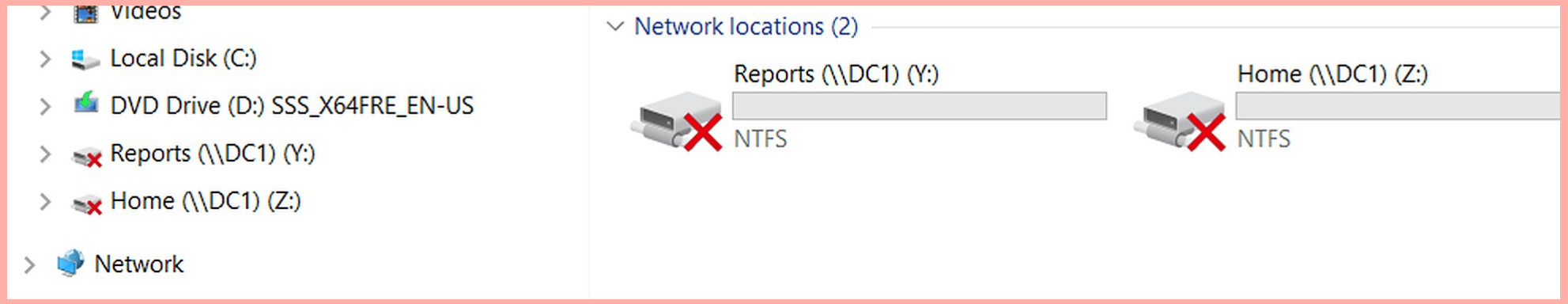


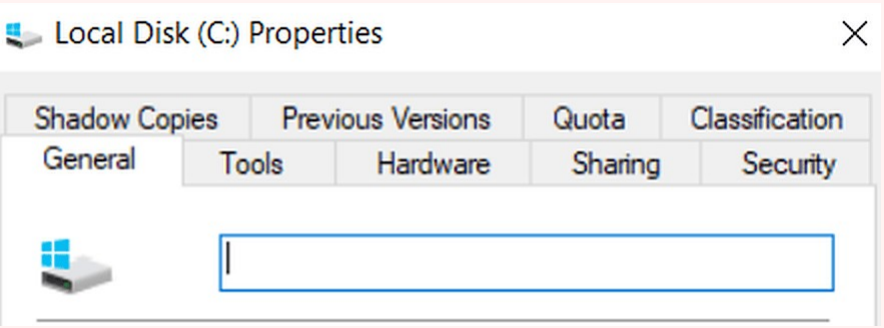


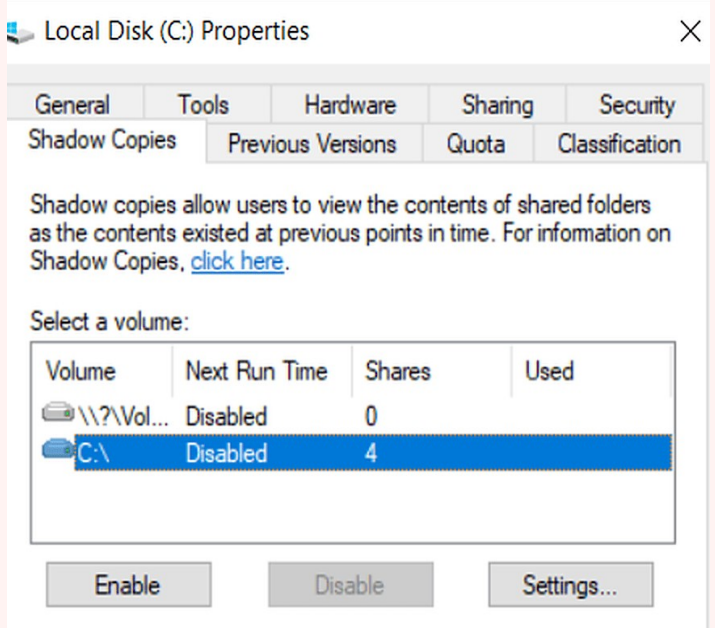
Property of Ben Halevy

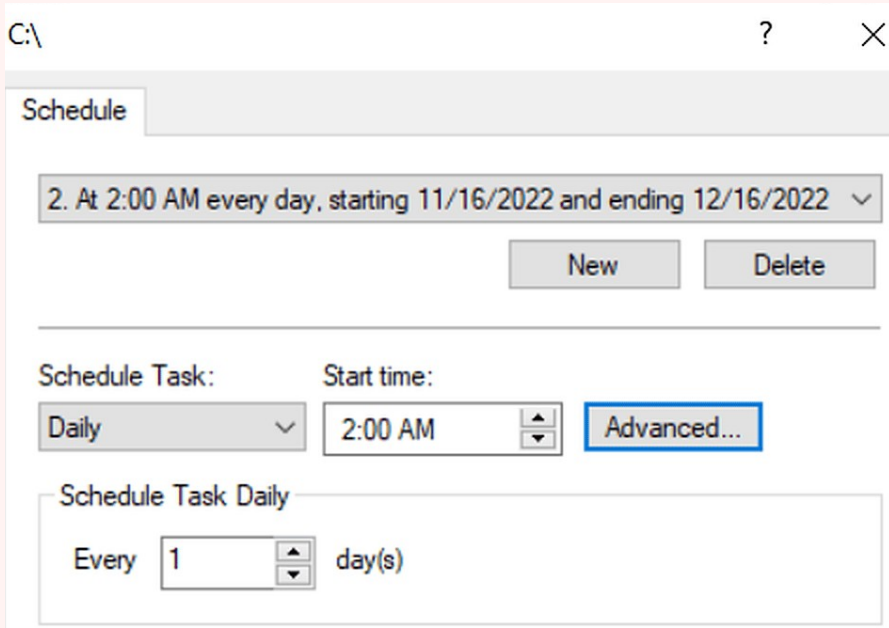
Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE









Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

Task
Create a Document and Place it On the Desktop Of Every End User of the Office Dept.
The File Should Read “Please Turn Off Your Computer

I have Recently Installed the Role FSRM and Created

This Has Caused A System Failure to Create or Edit GPO’S in any way and Removes the Domain Entirely From the Group Policy Management System

To Combat this Known FSRM Bug disable the filter driver by running: fltmc unload datascrn >Edit the GPO >

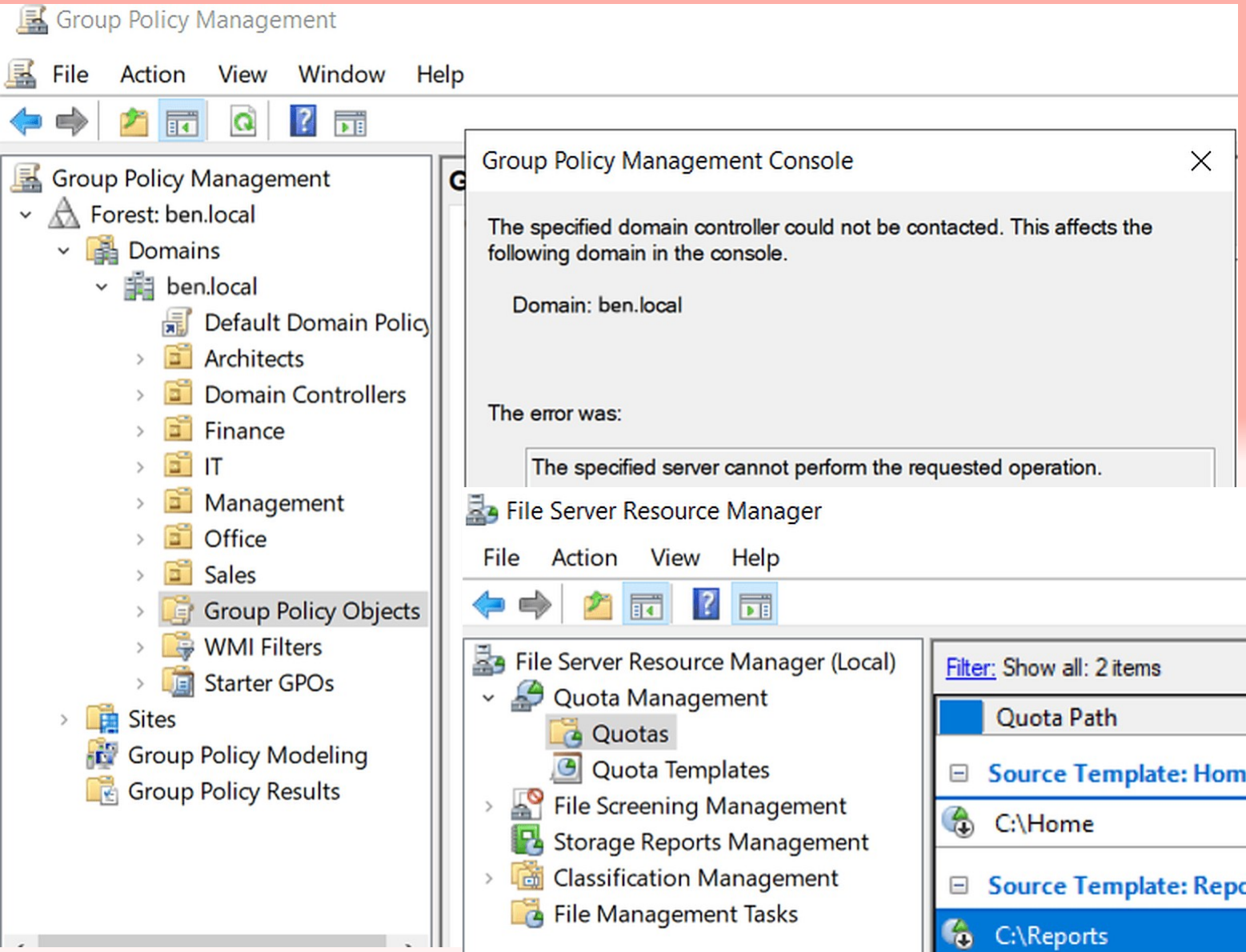
When you're finished editing the GPO re-enable the filter driver by running: fltmc load datascrn

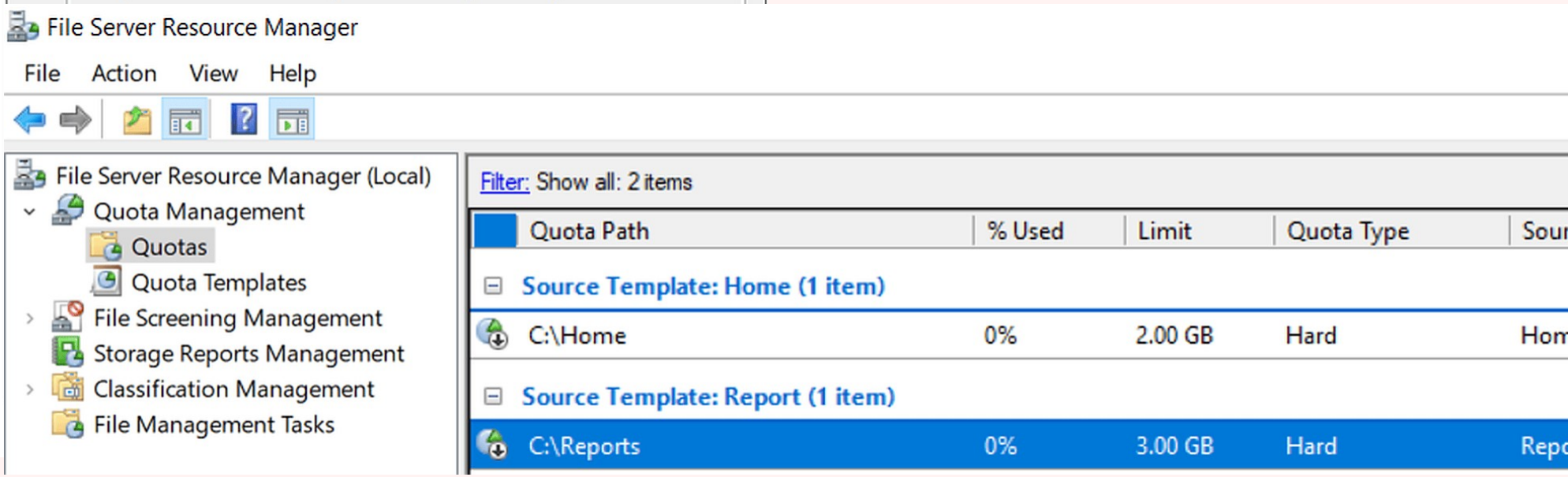
FSRM BREAKS GPO EDITING ON WINDOWS 2019

How To Instructions
Create A Shared Folder in C: Named “Instructions” > Share it > New GPO> User Pref > Windows Settings > Folders > New > Action: Create >
Source: Network Path for The intented File > Destination should have the %DesktopDir% \Instructions.txt file > read only +Archive >

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

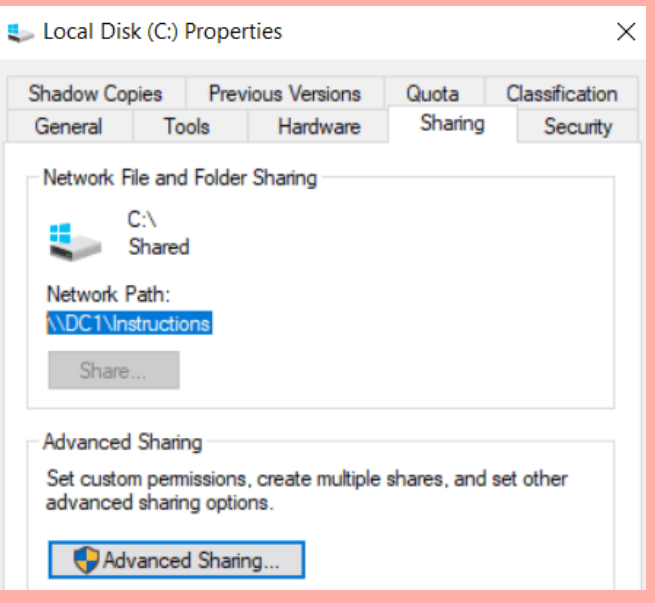


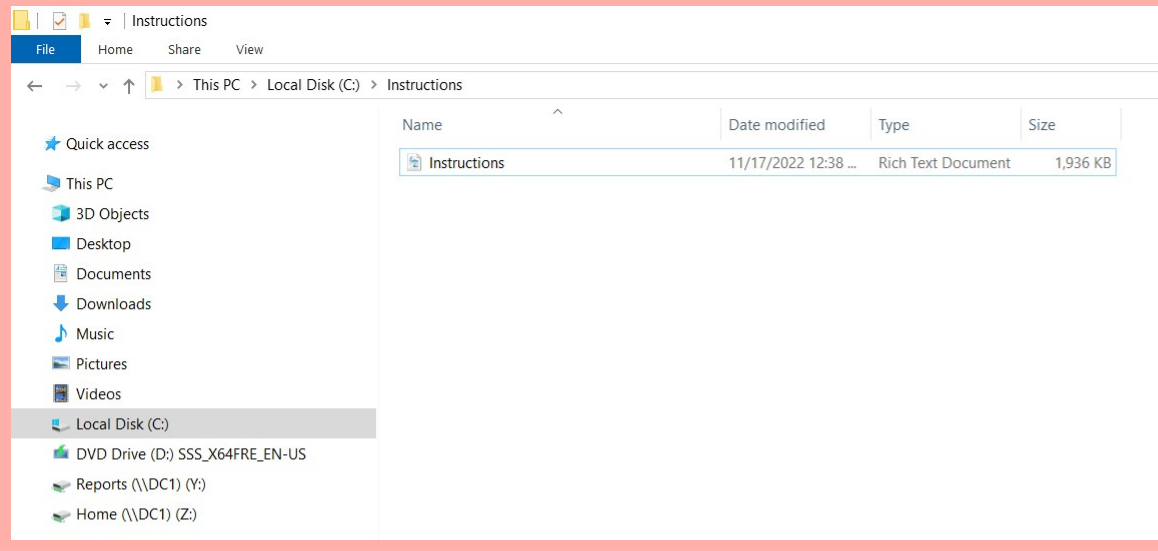


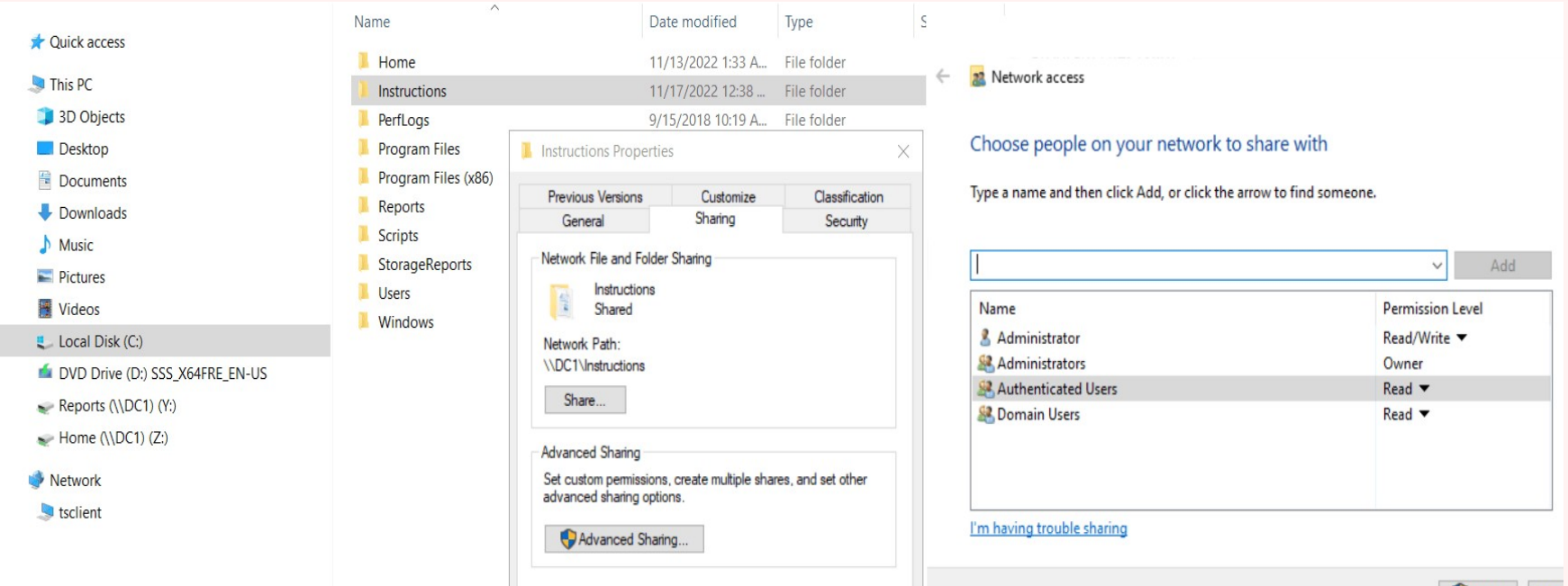
FSRM BREAKS GPO EDITING ON WINDOWS 2019

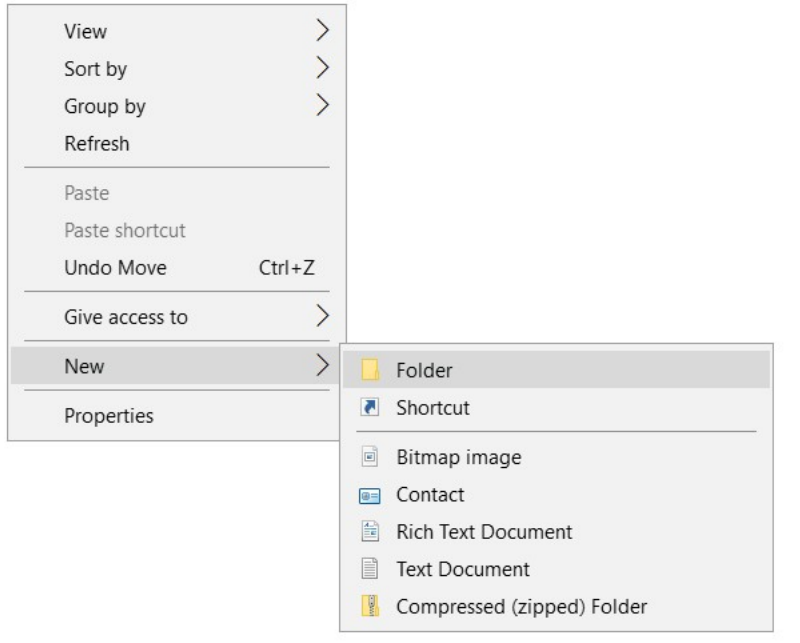
Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE



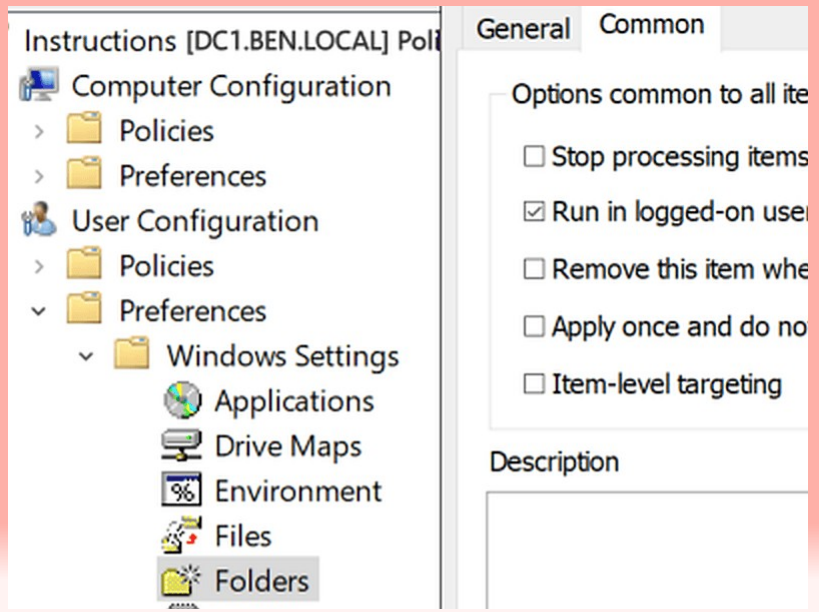






Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE




```
PS C:\Users\Administrator> fltmc unload datascrn

PS C:\Users\Administrator> gpupdate /force
Updating policy...

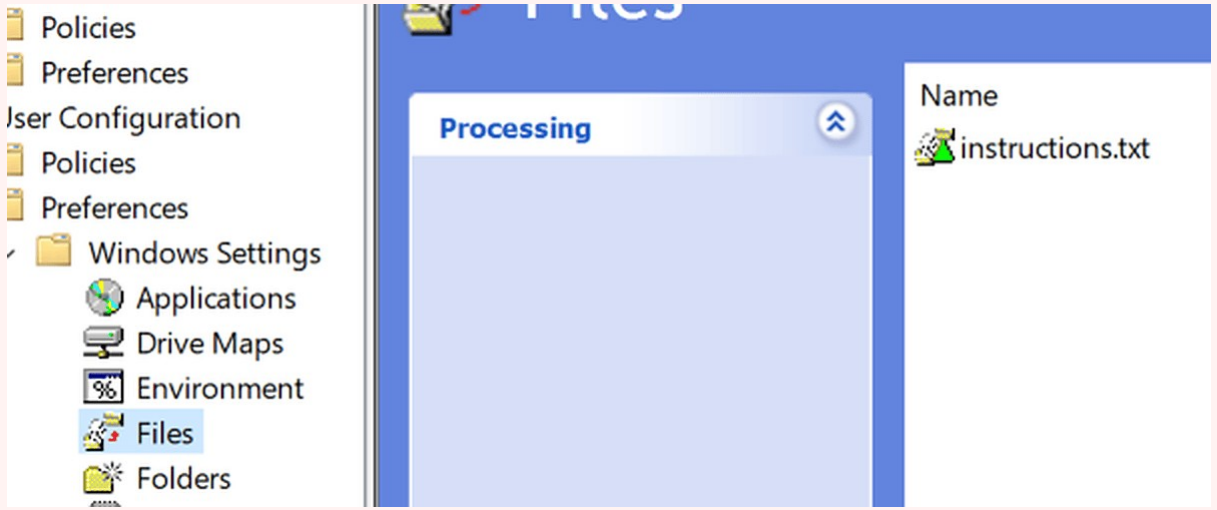

Computer Policy update has completed successfully.

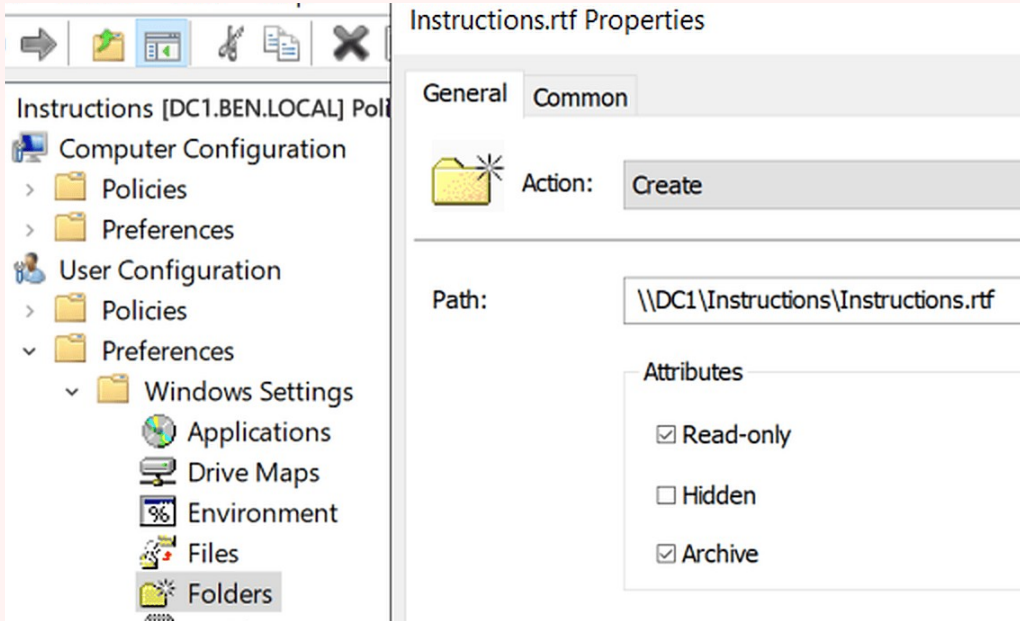
User Policy update has completed successfully.



PS C:\Users\Administrator> fltmc load datascrn

PS C:\Users\Administrator> |
```





Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

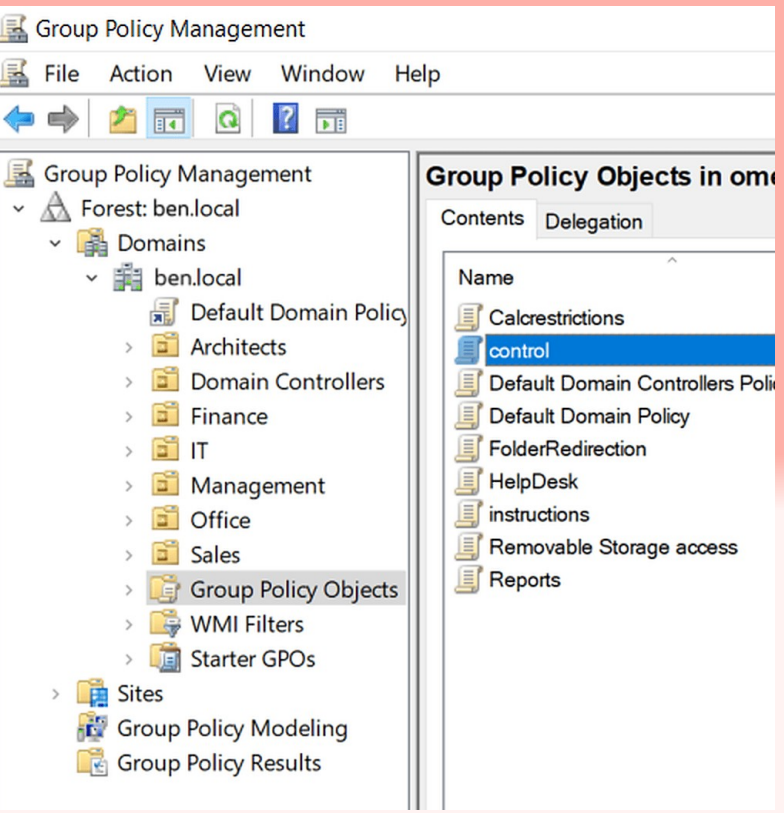
Task
Prohibit the Finance Dept Access to the EndPoint Control Panel & CMD

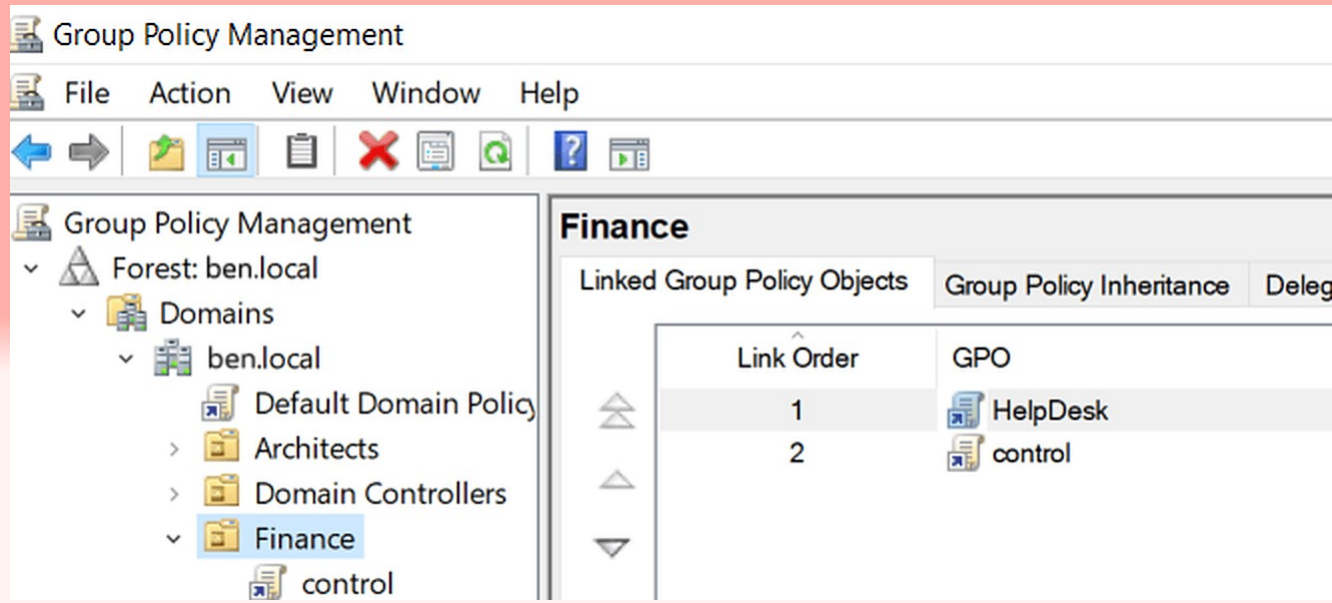
How To Instructions
fltmc unload datascrn > New GPO “Control”> User Policies > Admin Temp > Control Panel > Prohibit Access to Control Panel
and Pc Settings > Enable > Ok > Exit > Finance Dept GPO > Link Existing “Control”> Gpupdate /force > fltmc load datascrn

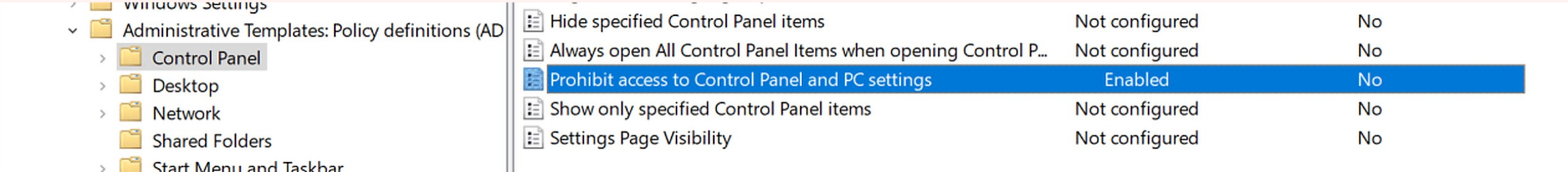
Property of Ben Halevy

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE







Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

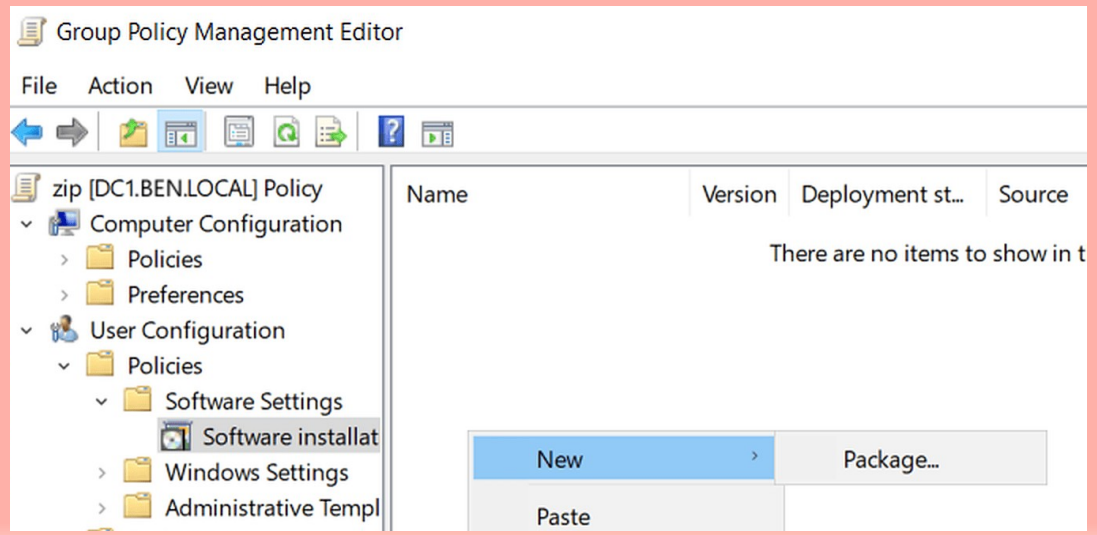
Task
Create A Shared Folder and Distribute Software through the GPO

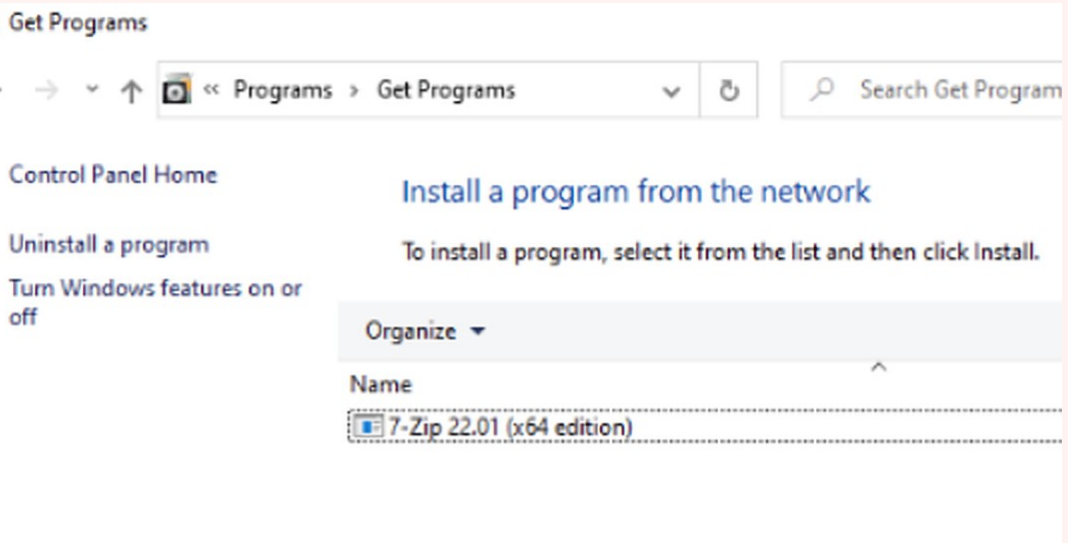
How To Instructions
Create a shared folder named “ZIP” > download the 7zip.msi file into shared folder>
create a GPO named “ZIP” > Edit > User Config > Policy >Software Settings >New Package
> Input the network address for the file > Publish > Link existing GPO

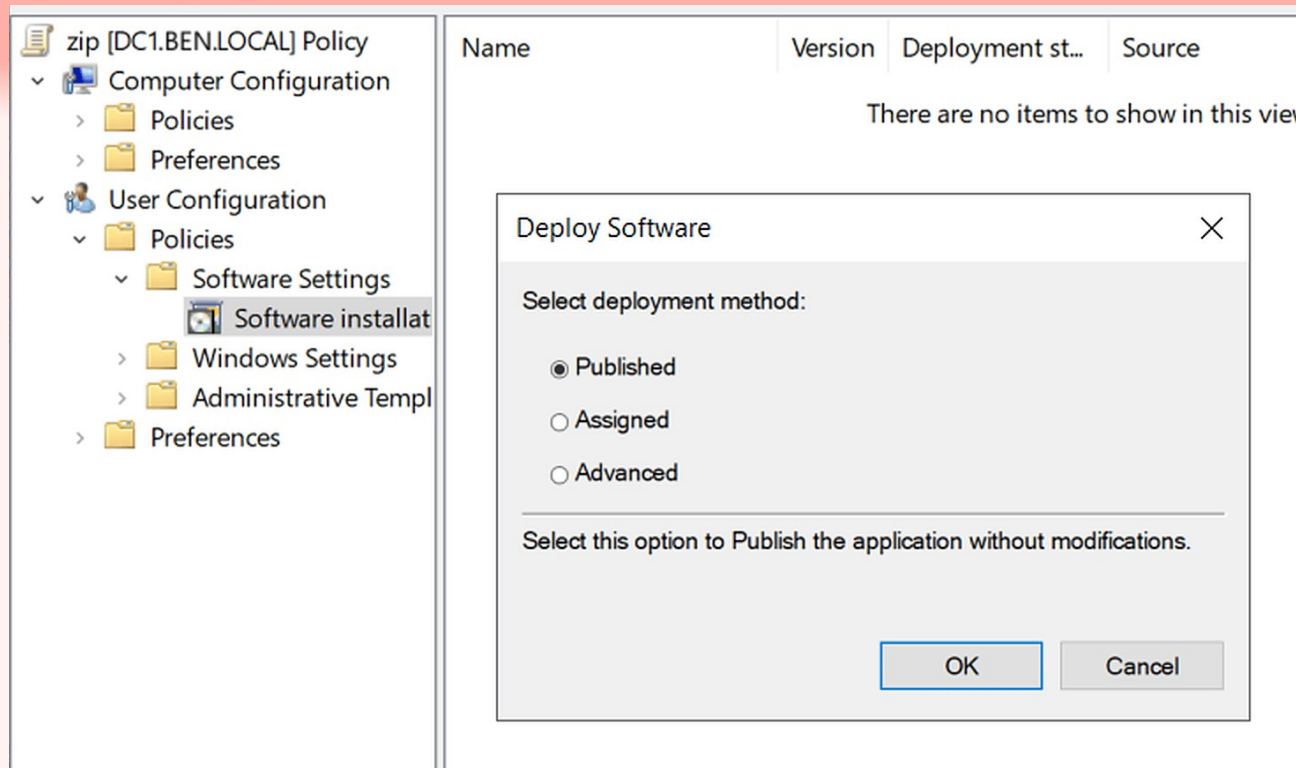
perty of Ben Halevy

Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE



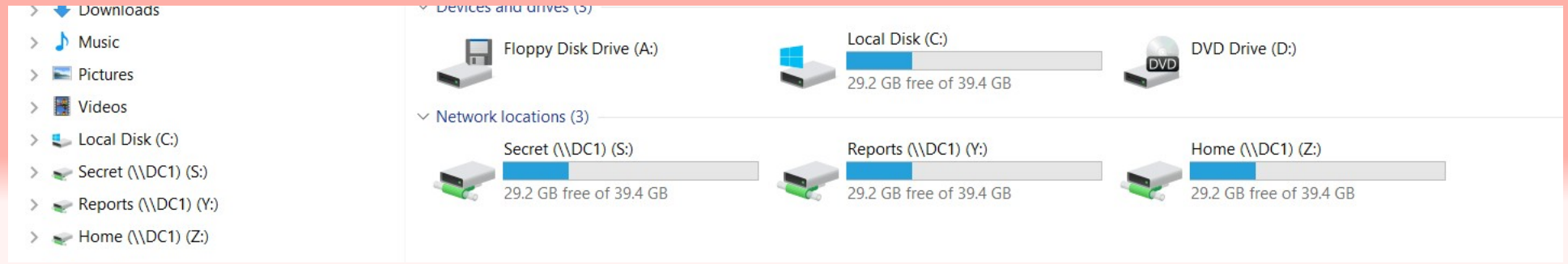




Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE

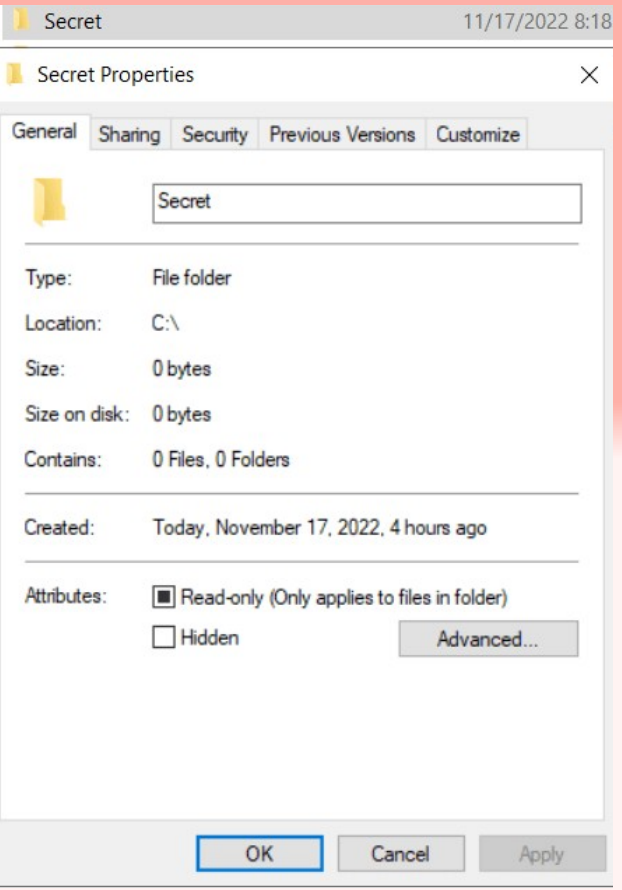
Task
Create a Shared Drive that is parameter specific and map it to the Network

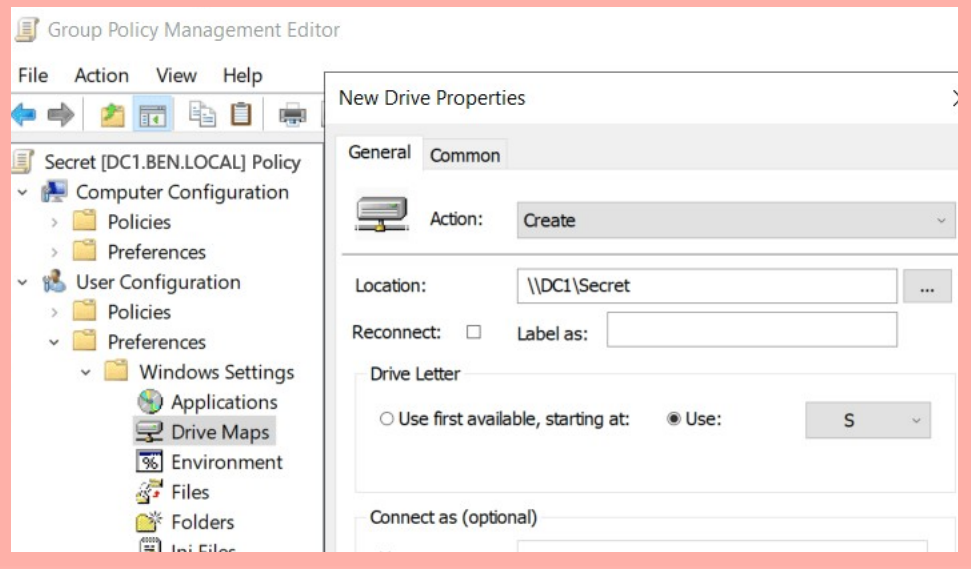


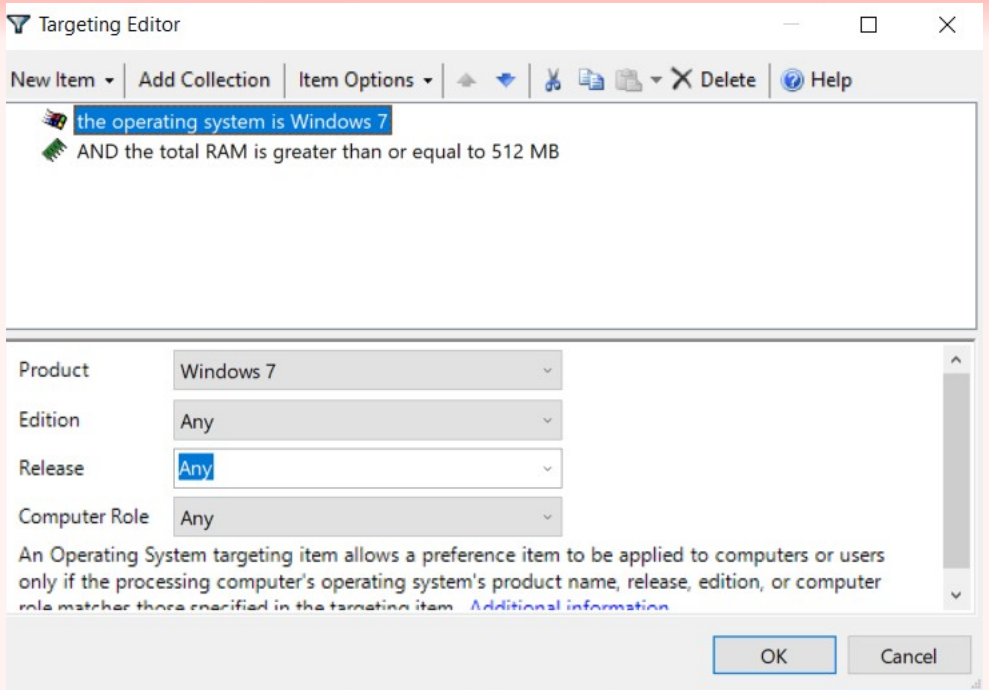
How To Instructions
Create a new Folder and Share it to the Network >Create new GPO>Edit> User preference >windows>New Drive Map O.S is
>create>DC folder address\\DC1\Secret > Drive letter S:> Common Tab > Item Level Targetting > New Item > Specify Which
required > New Item > Specify How Much Ram is required > after which you will

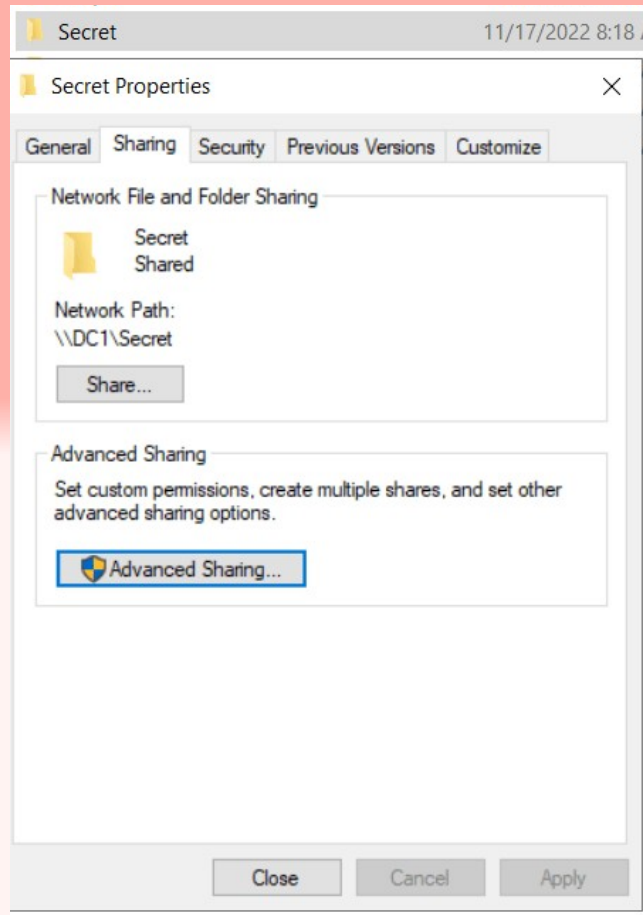
Mission Parameters

ORGANIZATIONAL INFRASTRUCTURE









Property of Ben Halevy

Mission Parameters
NETWORK INFRASTRUCTURE

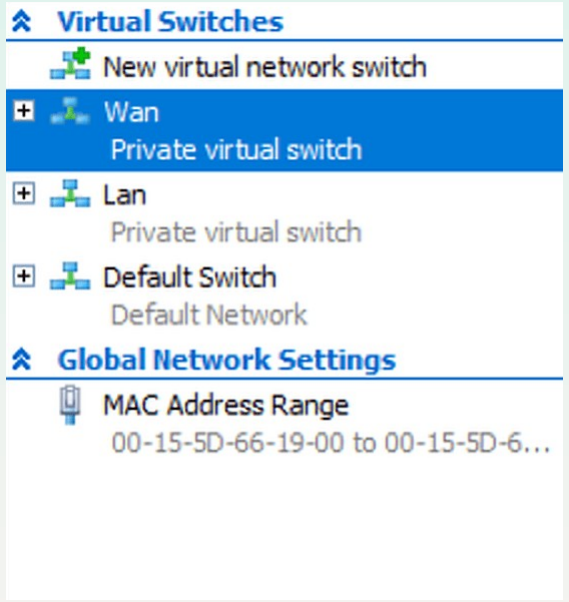
Task
Infrastructure settings for the Organization's VPN connection

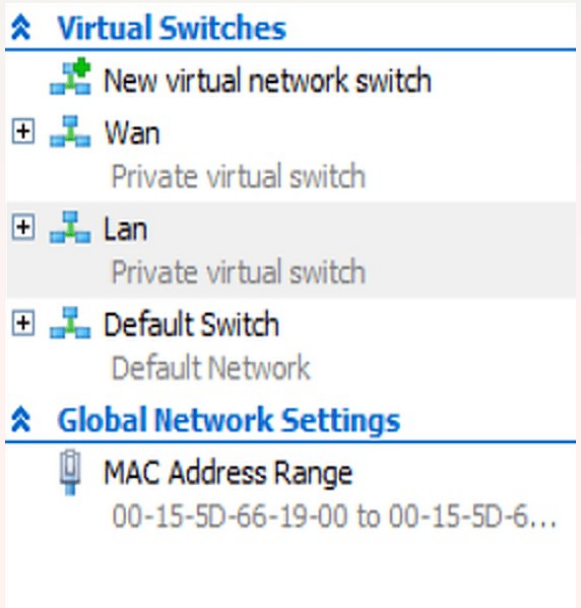
LAN	IP Config	WAN
IP address:192.168.100.254		IP address: 192.168.200.1
Subnet Mask: 255.255.255.0		Subnet Mask: 255.255.255.0
Default Gateway: Leave Empty		
Primary DNS : 192.168.100.1		

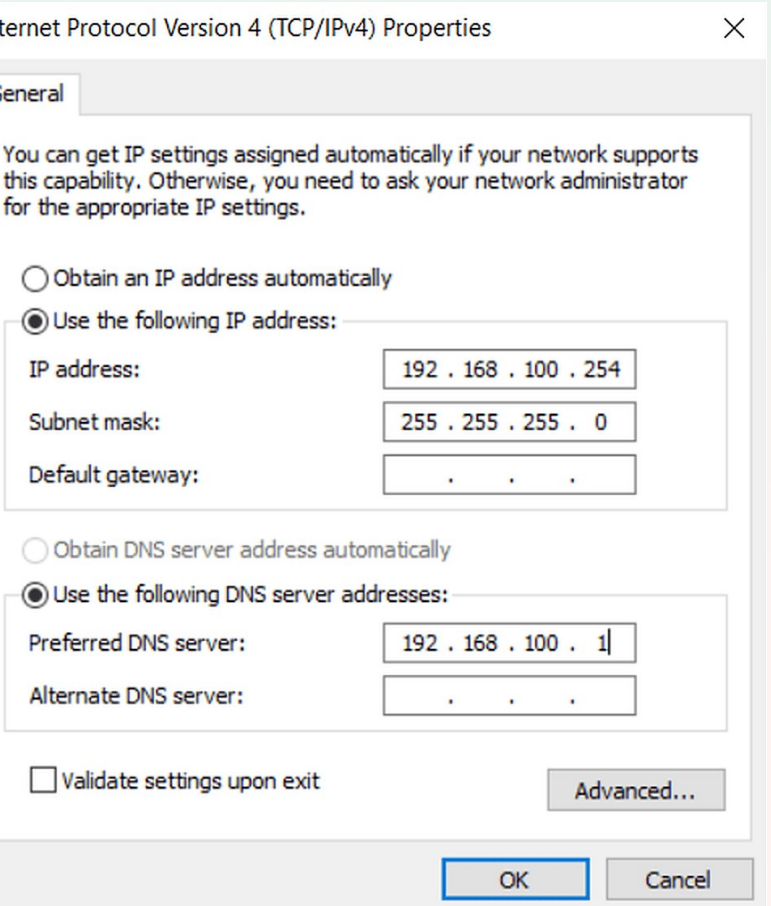
Create A Virtual Private Network In Hyper-V named "WAN"
Create a Virtual Machine Named RAS w/a Dual Core Processor, (2gb ram), (40gb) HDD
Give the Machine 2 NIC's , the 1st being the LAN, the 2nd being the WAN

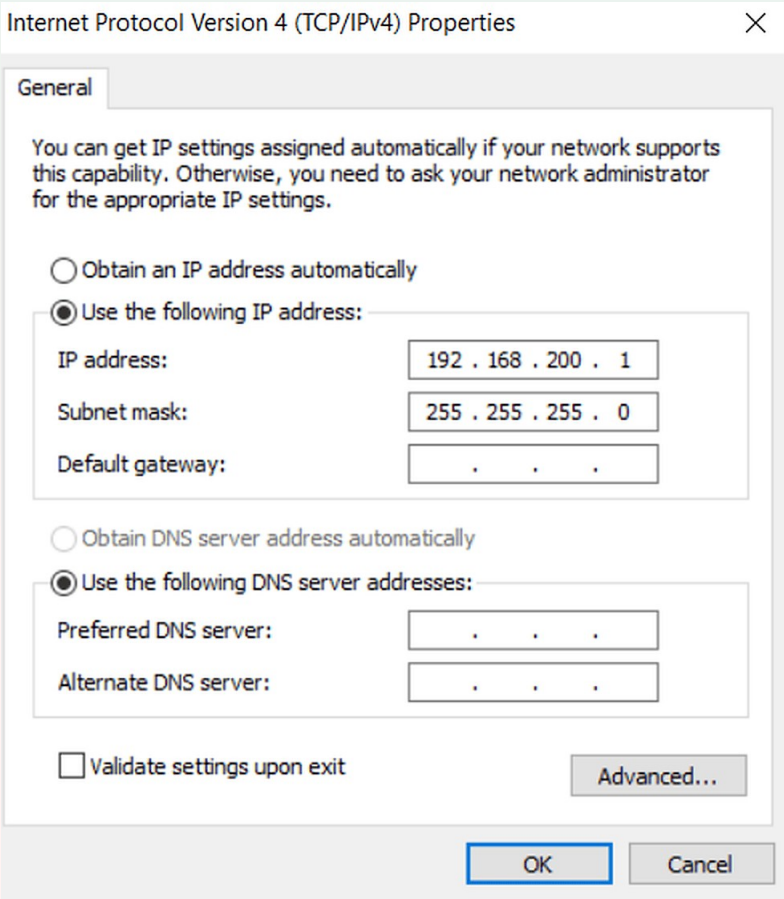
Property of Ben Halevy

Mission Parameters
NETWORK INFRASTRUCTURE



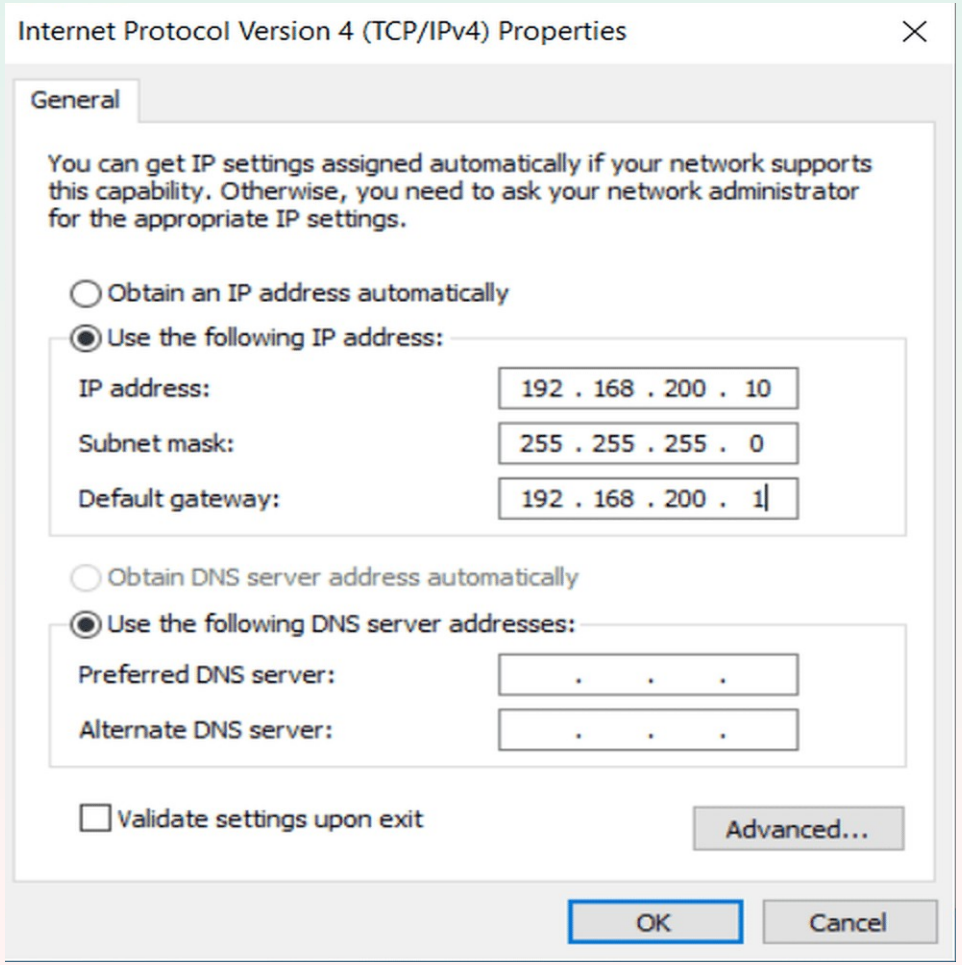






Mission Parameters
NETWORK INFRASTRUCTURE

Task
Create A Virtual Machine PC1



TCP/IP Configuration
IP: 192.168.200.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.200.1
DNS: Empty

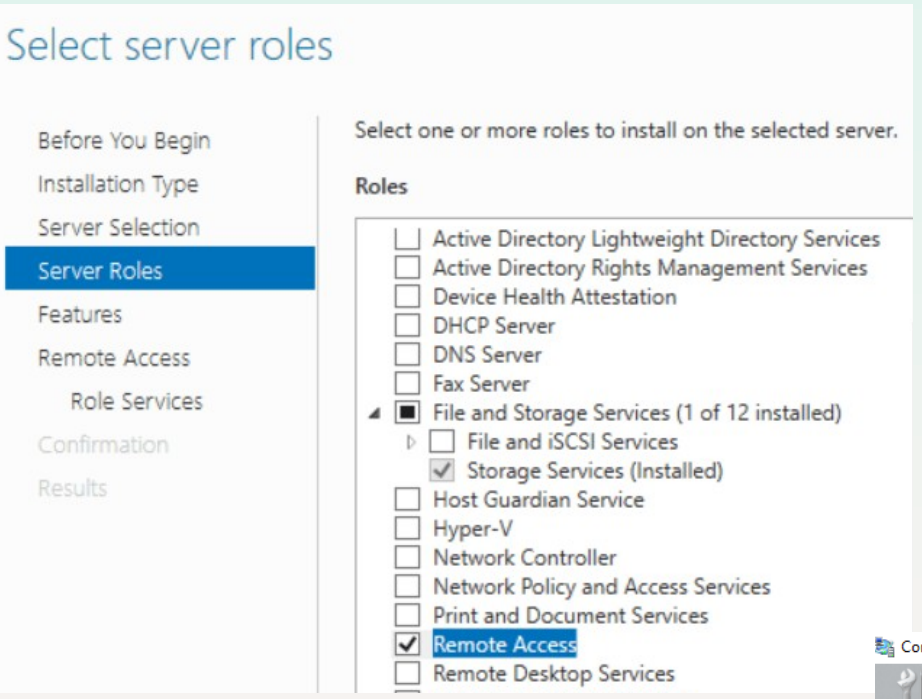
How To Instructions
Virtual machine named PC1, (1GB Ram) (30GB HDD) WAN

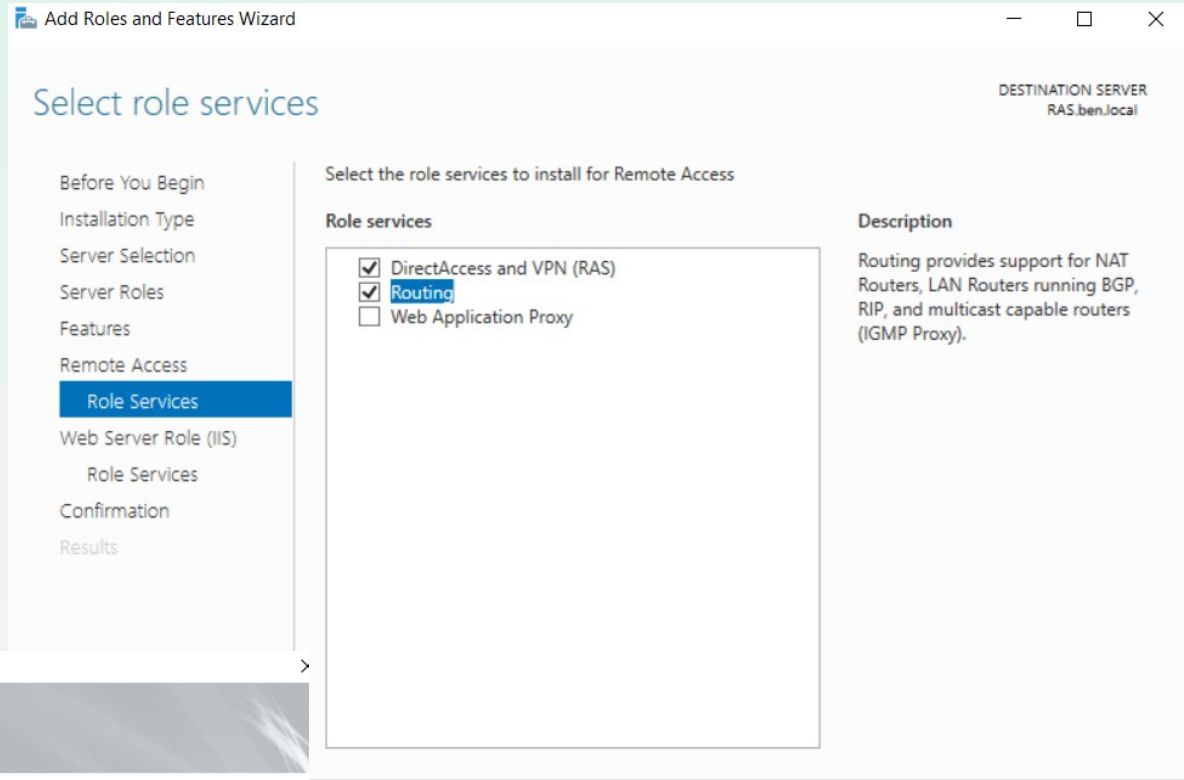
Property of Ben Halevy

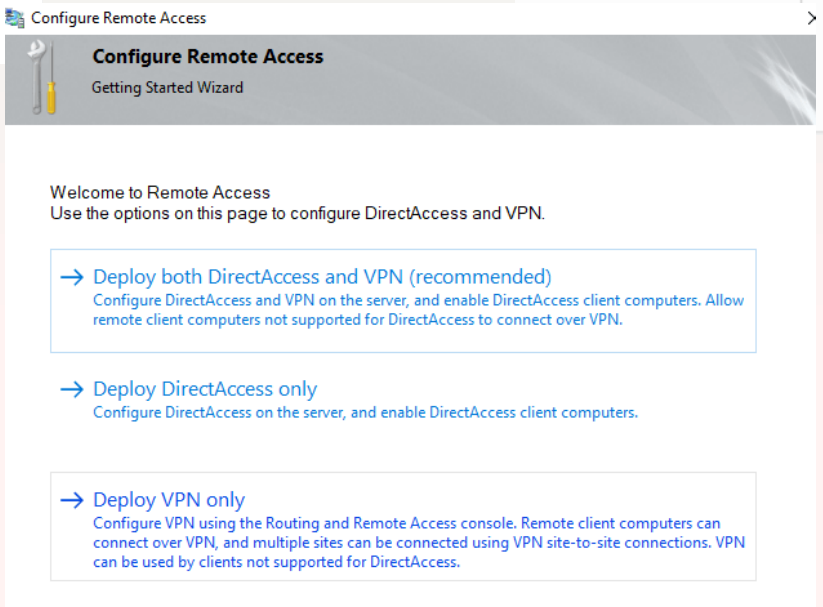
Tasks
Configure a VPN Server

How To Instructions
Add New Role(Routing and Remote Access) On the RAS Virtual Machine > Choose Direct Access +VPN Routing > Only Configure the VPN
>once the role has been created > Right click on RAS> Choose Routing and remote access > custom config > pick VPN and Dial up
> Policy name – Management VPN > Remote access Server > Specify Condition (User Group) > grant access + click on Dial in Properties
> Configure Device Remote Access +Dial Routing (Max 7 Ports) >under devices – Close all Ports other than the 7 PPTP ports designated
> Designate the NPC Condition to give the Management group the ability to Connect < Set up the VPN

Mission Parameters
NETWORK INFRASTRUCTURE

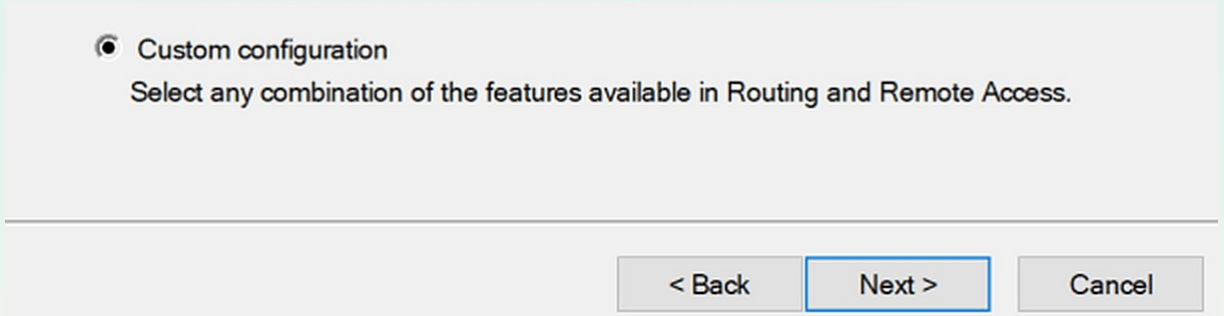


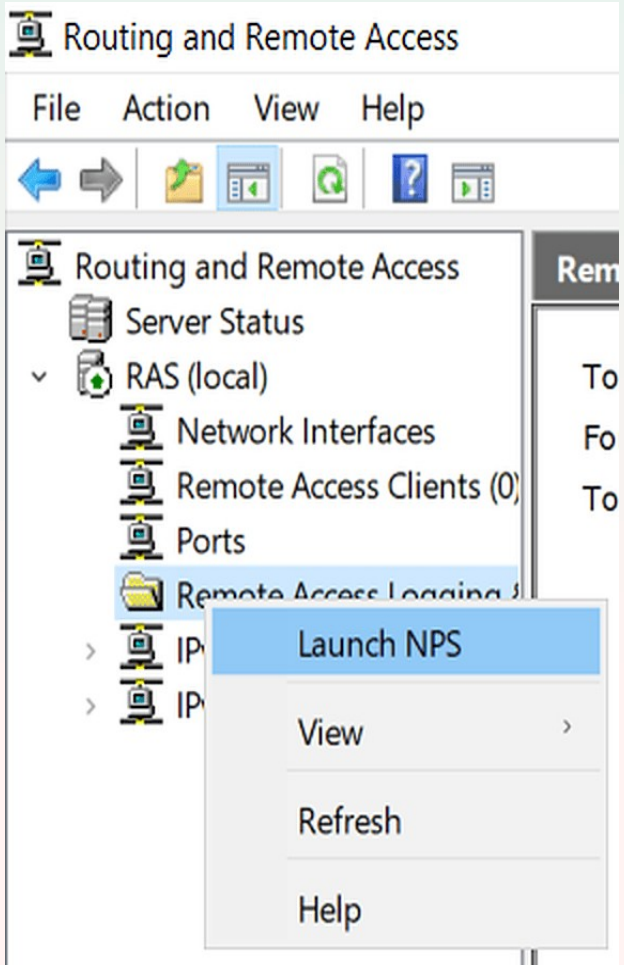


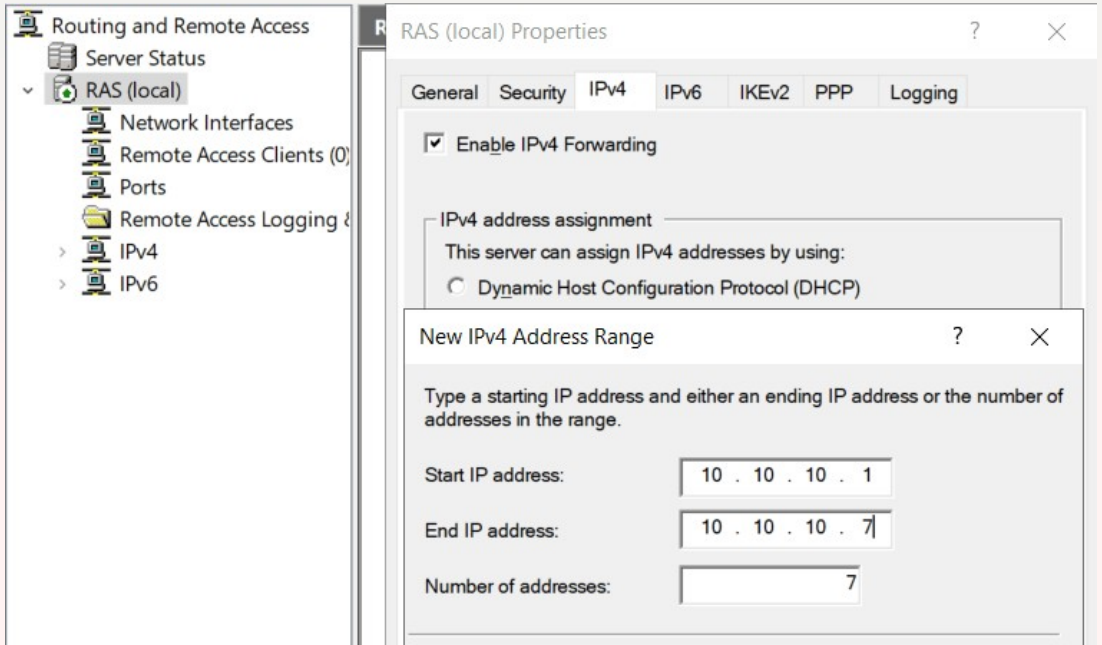


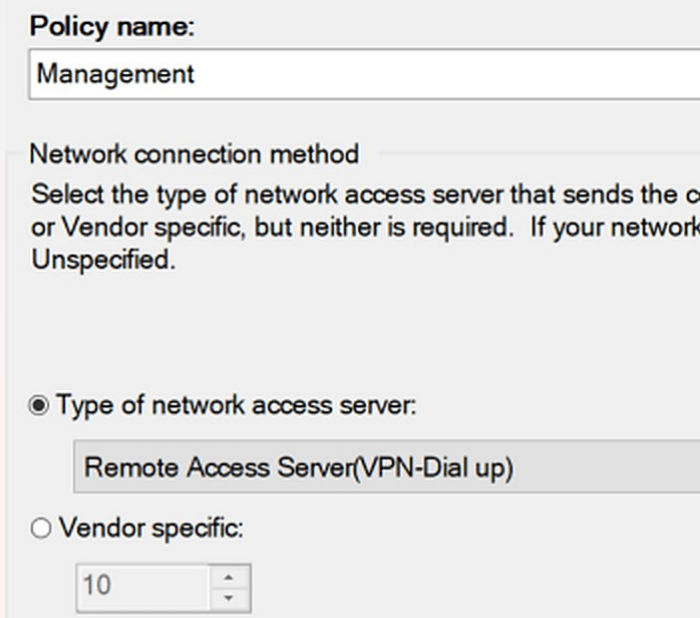
Property of Ben Halevy

Mission Parameters
NETWORK INFRASTRUCTURE

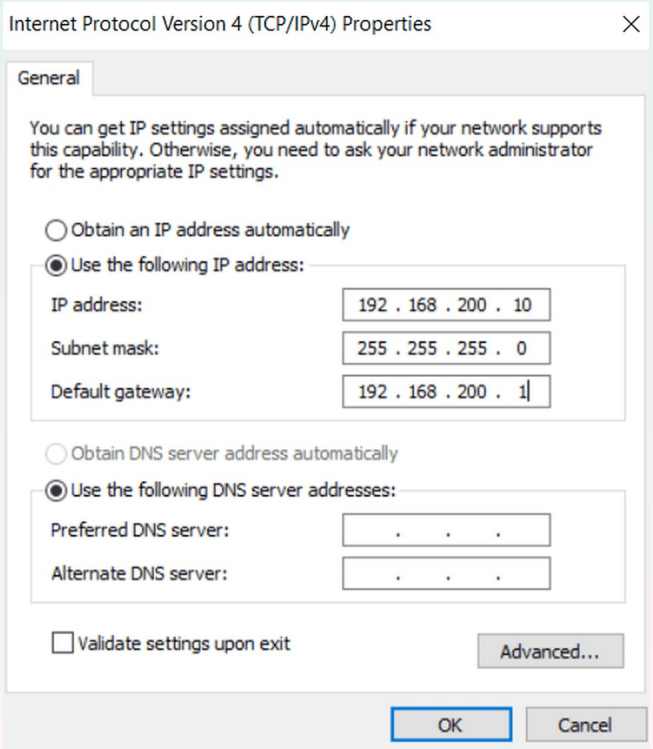


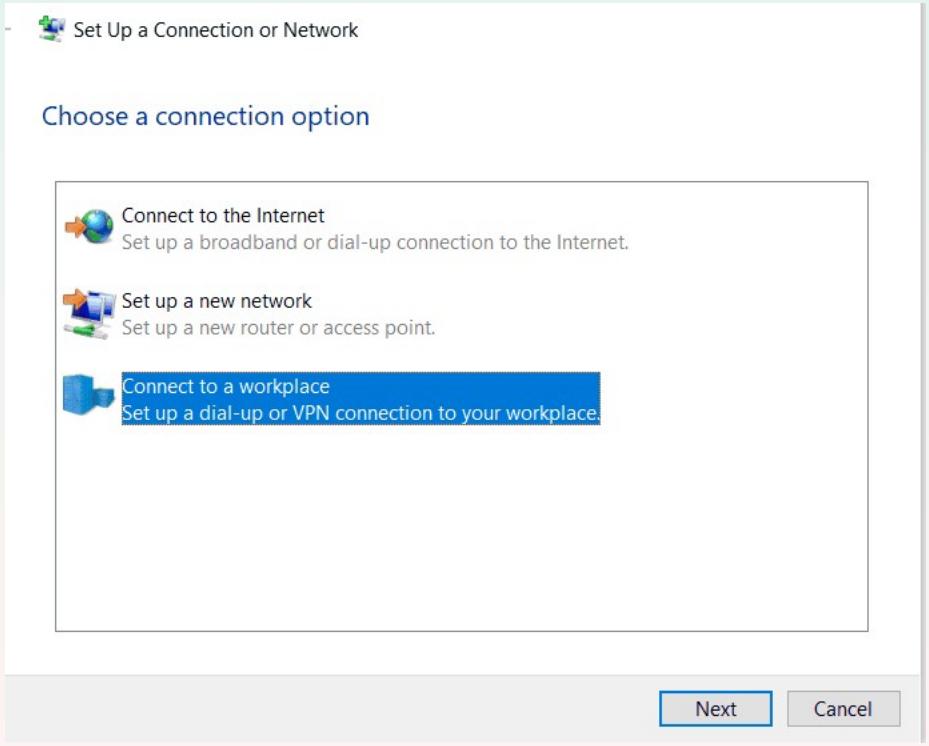


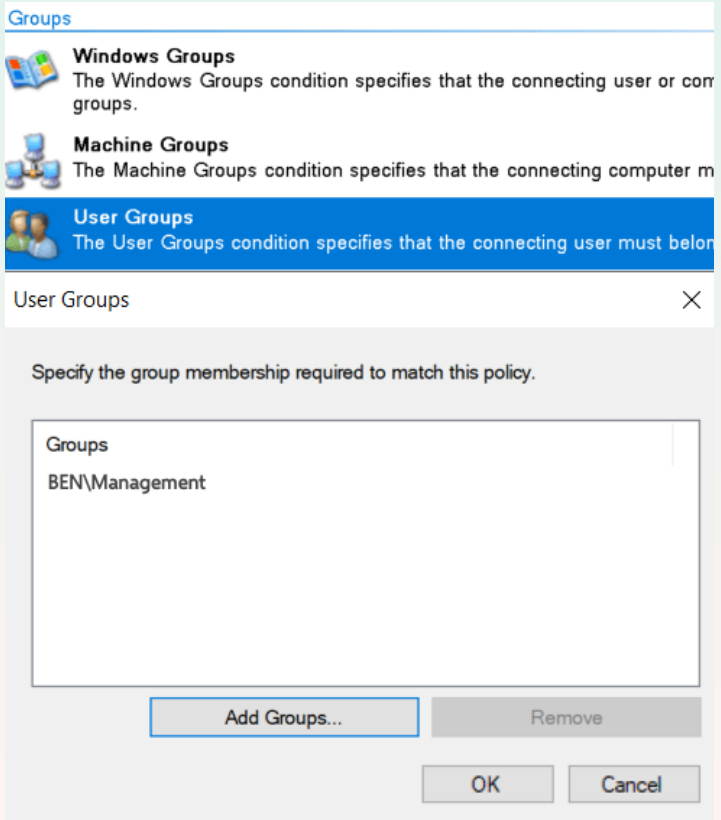




Mission Parameters
NETWORK INFRASTRUCTURE

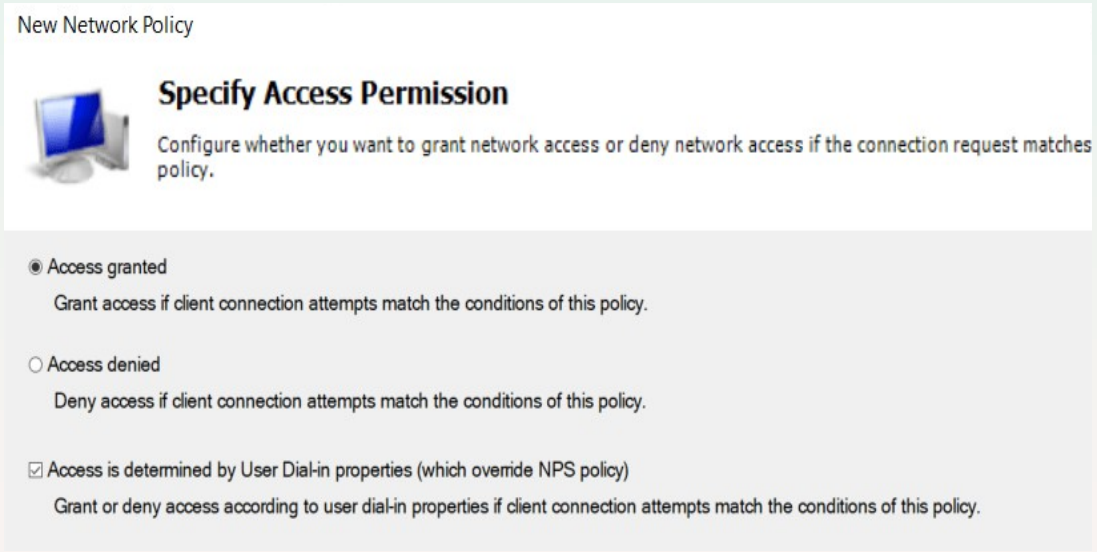


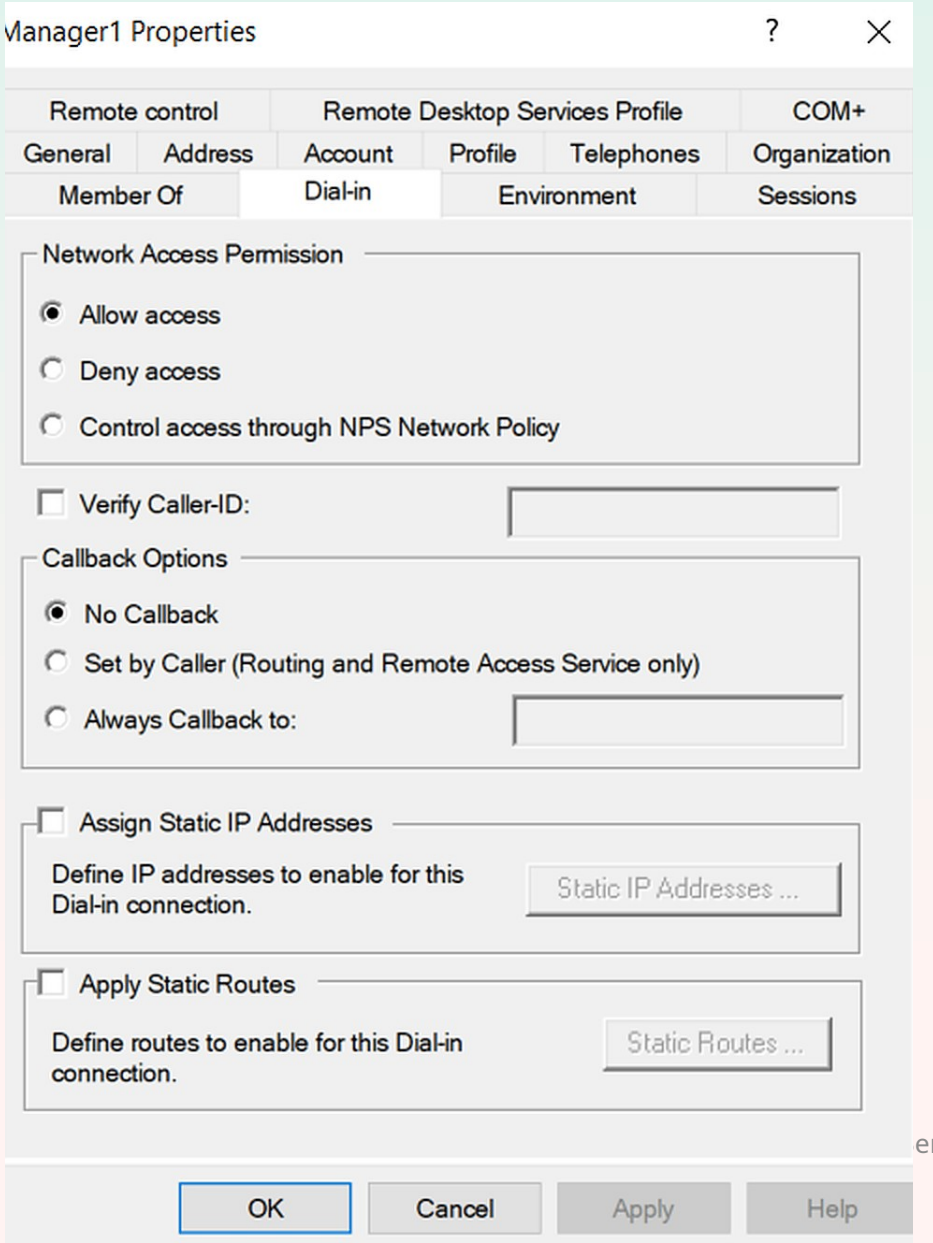




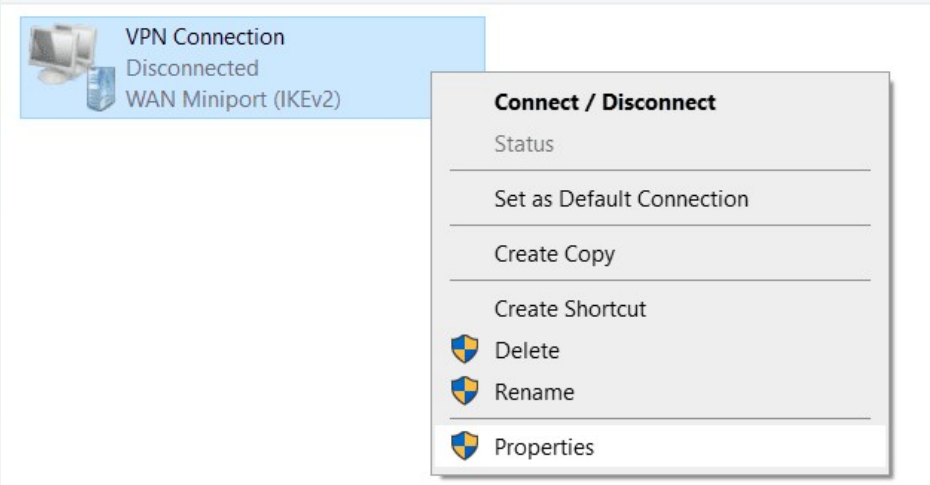
Property of Ben Halevy

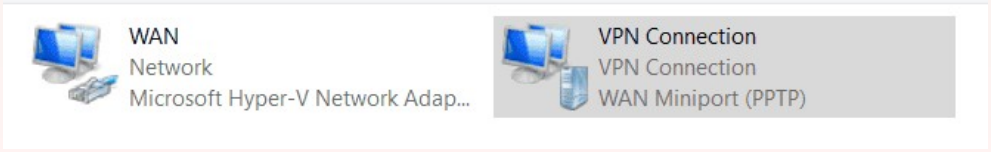
Mission Parameters
NETWORK INFRASTRUCTURE

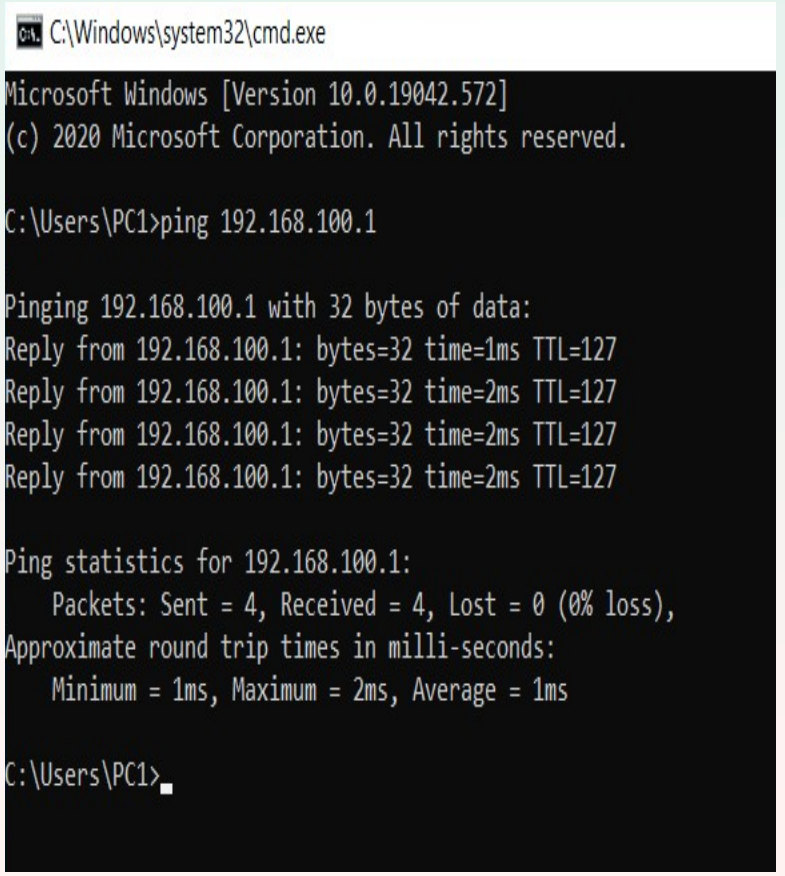




Mission Parameters
NETWORK INFRASTRUCTURE







Property of Ben Halevy

Mission Parameters
NETWORK INFRASTRUCTURE

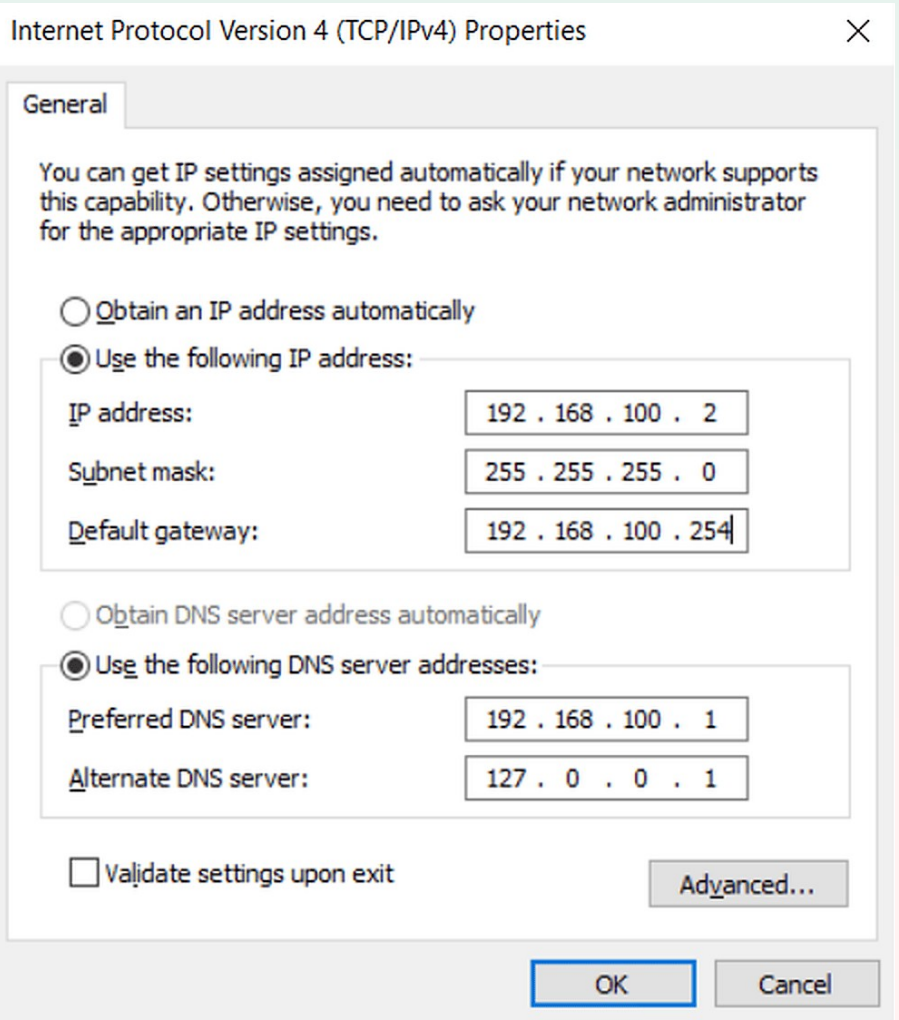
Tasks
Create New Virtual Machine – DC2 Server
Add Role AD DC
Associate it to BEN.LOCAL
Transfer the Role RID Pool

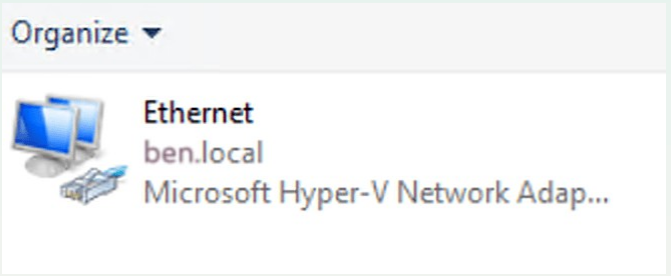
IP Address
Ip: 192.168.100.2
Netmask: 255.255.255.0
Default : 192.168.100.254
DNS : 192.168.100.1

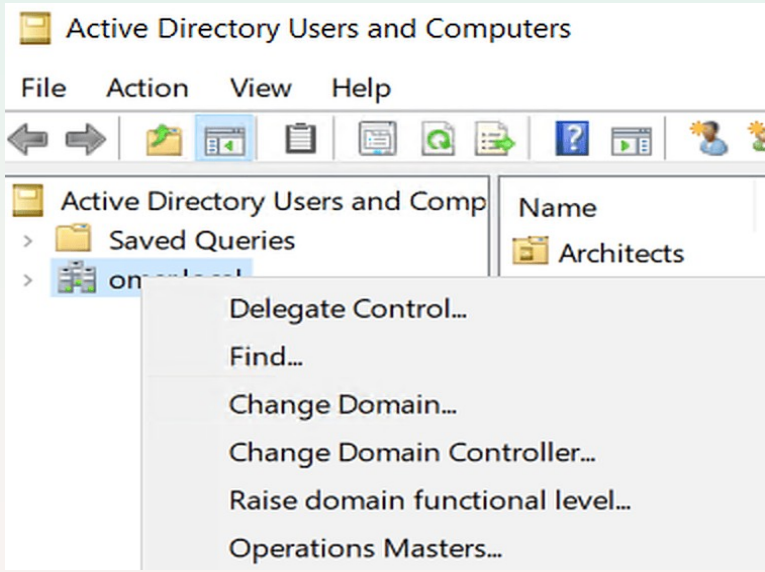
New Virtual Machine (2GI Change Name to DC2> Change IP > add Role Active Dir >
Promote Server to DC >Add DC to Existing Domain >upon completion

perty of Ben Halevy

Mission Parameters
NETWORK INFRASTRUCTURE

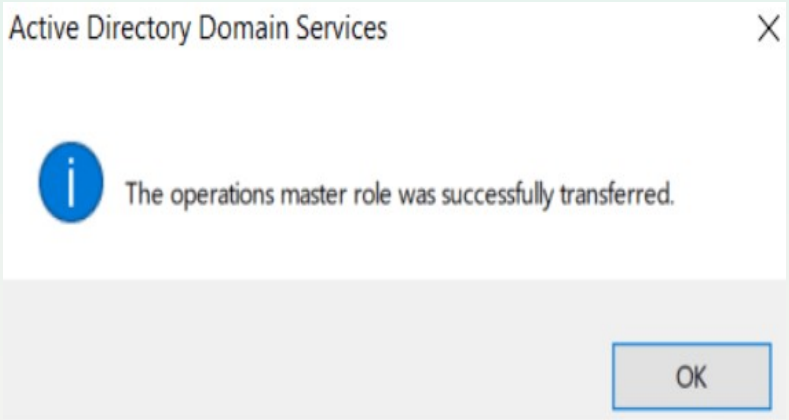






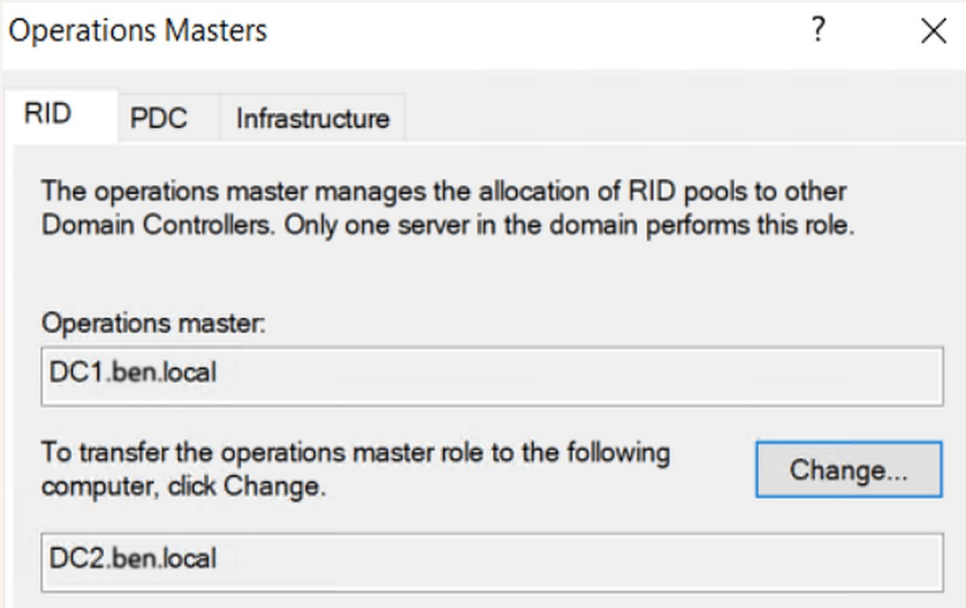
Property of Ben Halevy

Mission Parameters
NETWORK INFRASTRUCTURE




```
PS C:\Users\Administrator.BEN> netdom query fsmo
Schema master               DC1.ben.local
Domain naming master        DC1.ben.local
PDC                         DC1.ben.local
RID pool manager            DC1.ben.local
Infrastructure master       DC1.ben.local
The command completed successfully.


PS C:\Users\Administrator.BEN> netdom query fsmo
Schema master               DC1.ben.local
Domain naming master        DC1.ben.local
PDC                         DC1.ben.local
RID pool manager            DC2.ben.local
Infrastructure master       DC1.ben.local
The command completed successfully.
```

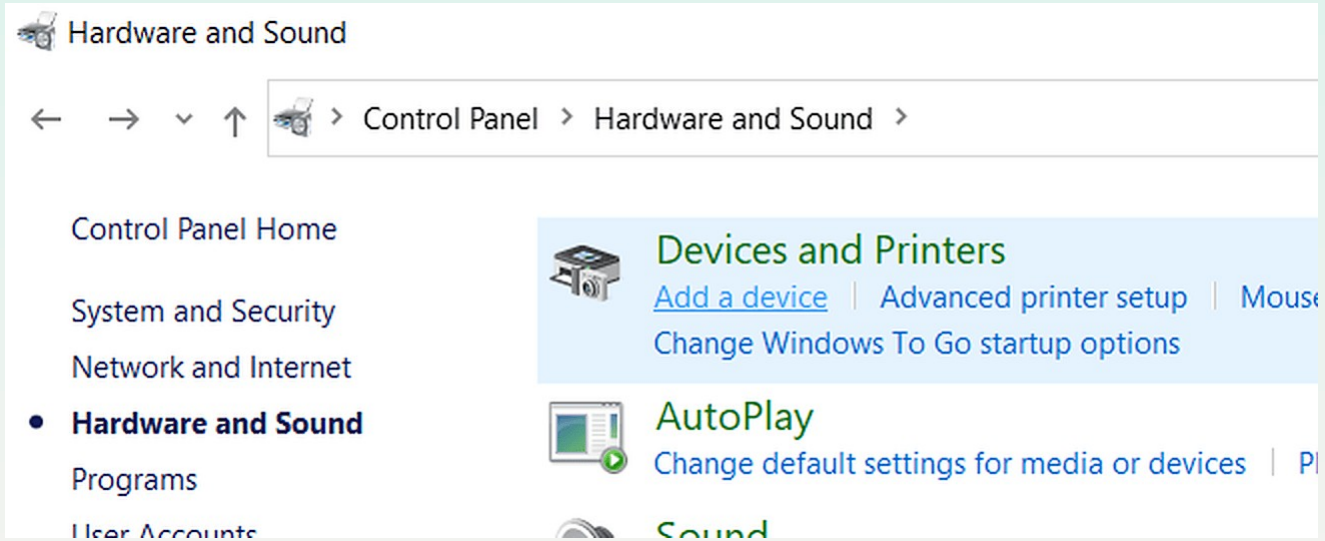


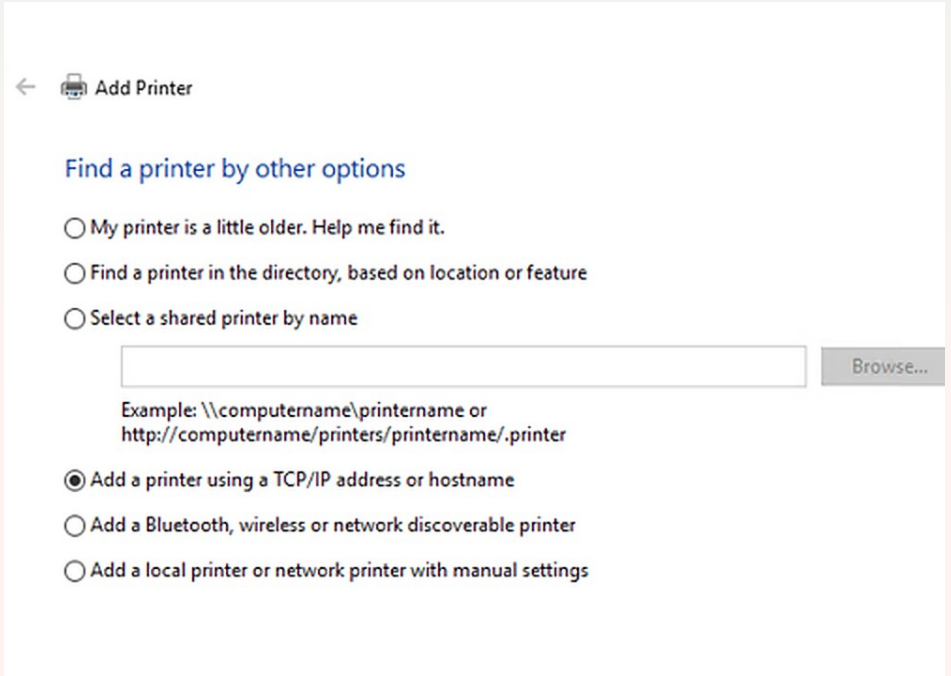
Mission Parameters
NETWORK INFRASTRUCTURE

Tasks
Install A Printer to DC1
IP: 192.168.100.50
Share the Printer w/ the Finance & Office Dept.
Grant the IT Dept Managing Permissions of the Printer
Make the Printer available in the Active Directory
Map the Printer Via GPO (Print1) to Finance & Office Dept.

Control Panel > Hardware > Devices and Printers > add >Find a Printer By Other Options >Use Tcp/Ip > add the Printer's Ip address > Pick the Printer
Driver to install >right click on the printer you selected > Sharing tab > Share this Printer > List in the Directory > go to Security tab > Grant the IT Dept.
Group Permissions to Printer > New GPO > Edit > User Preference > Cntrl Panel > Printers > New > Tcp/Ip Printer > General Tab > Create > Input Ip

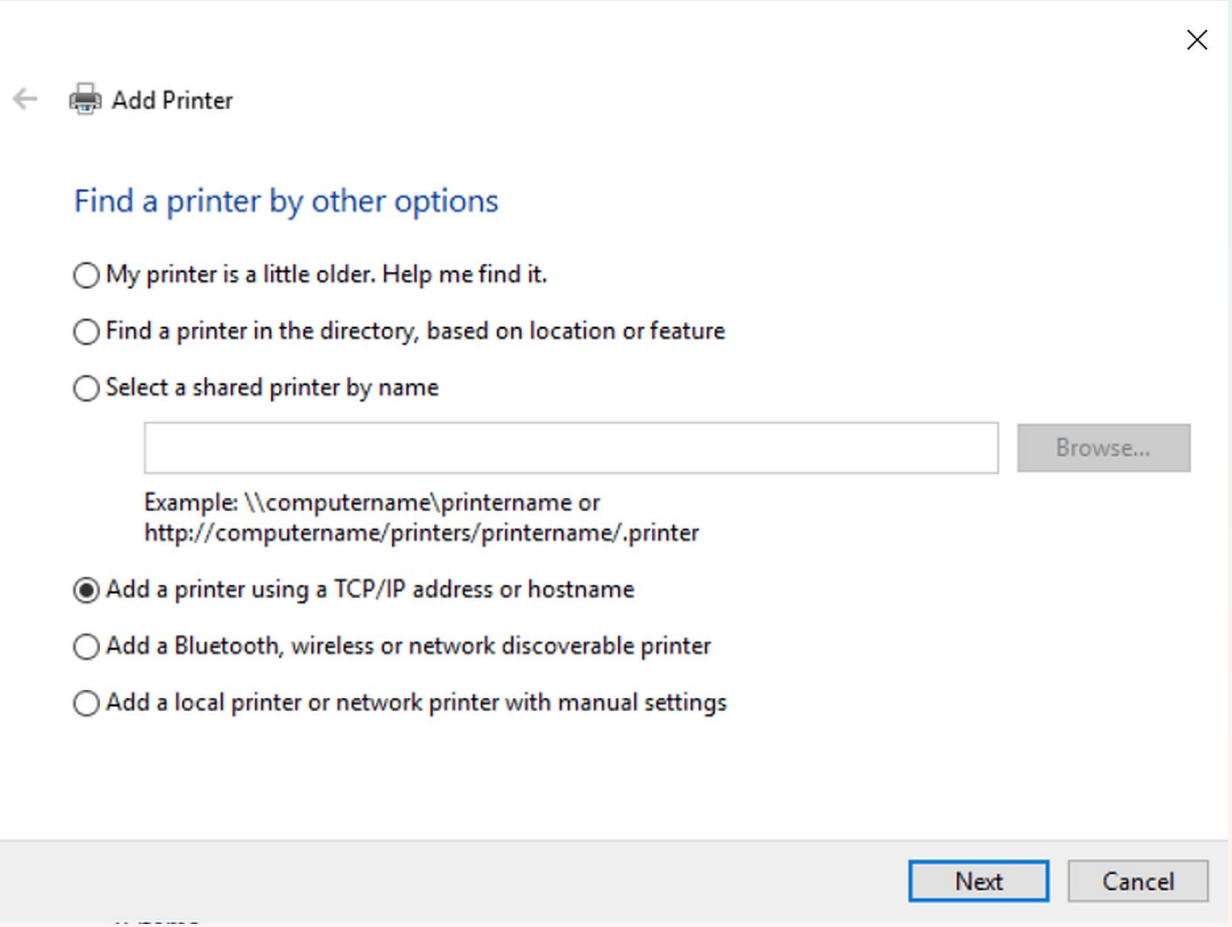
Mission Parameters
NETWORK INFRASTRUCTURE

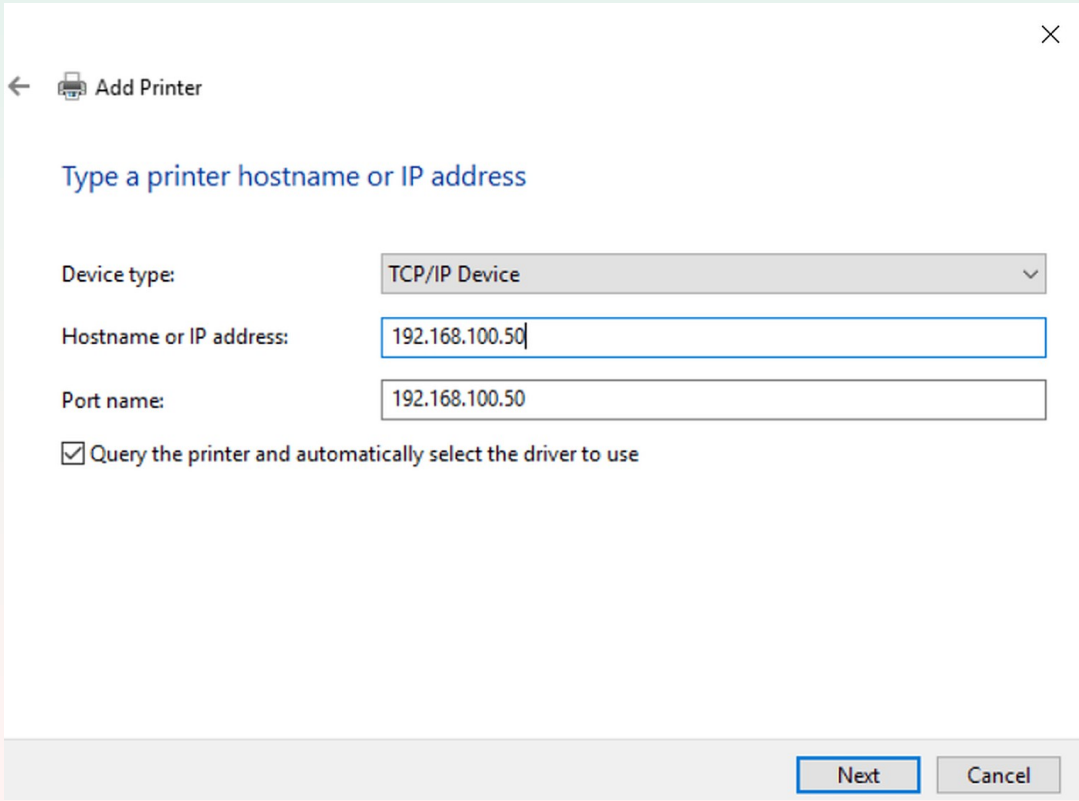




Property of Ben Halevy

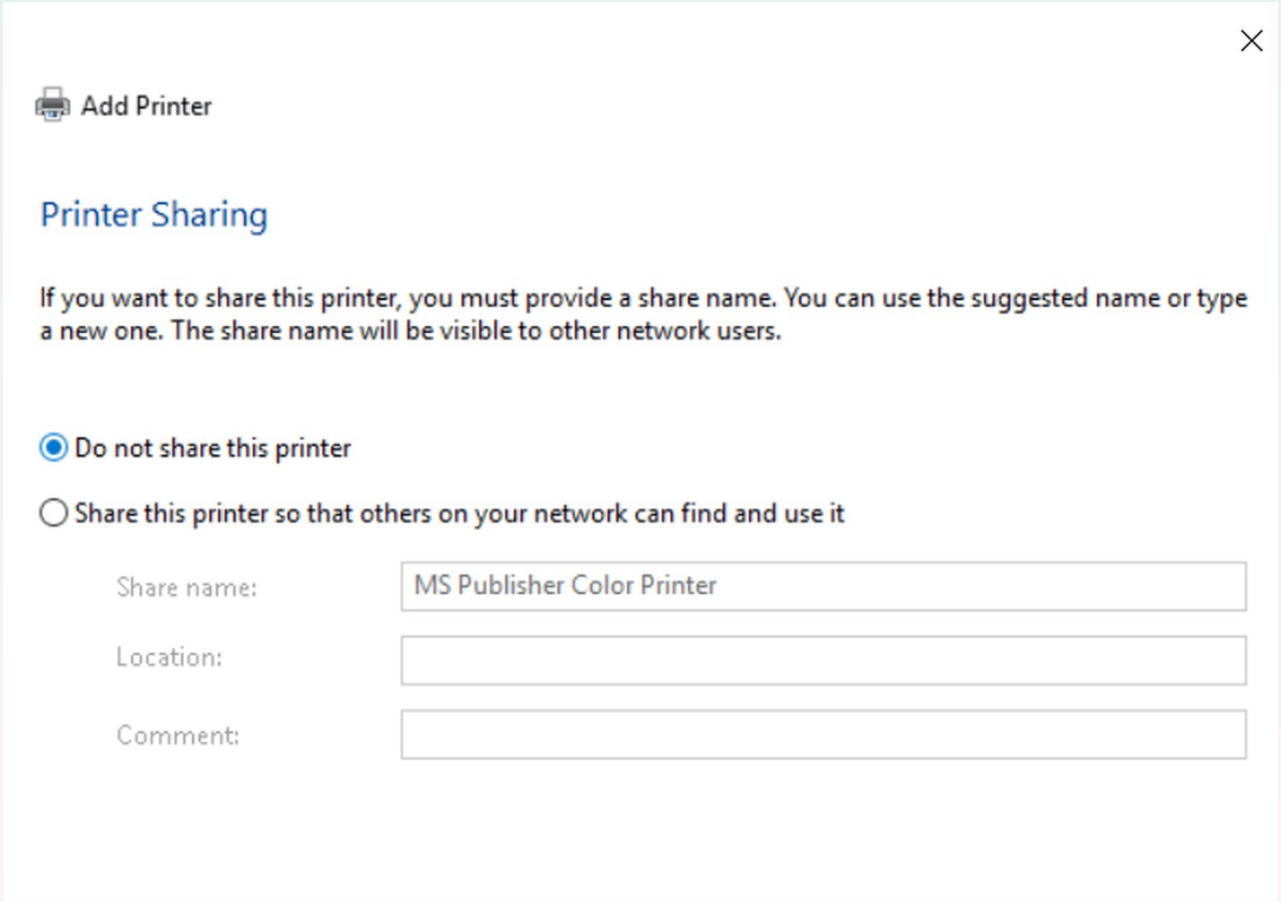
Mission Parameters
NETWORK INFRASTRUCTURE





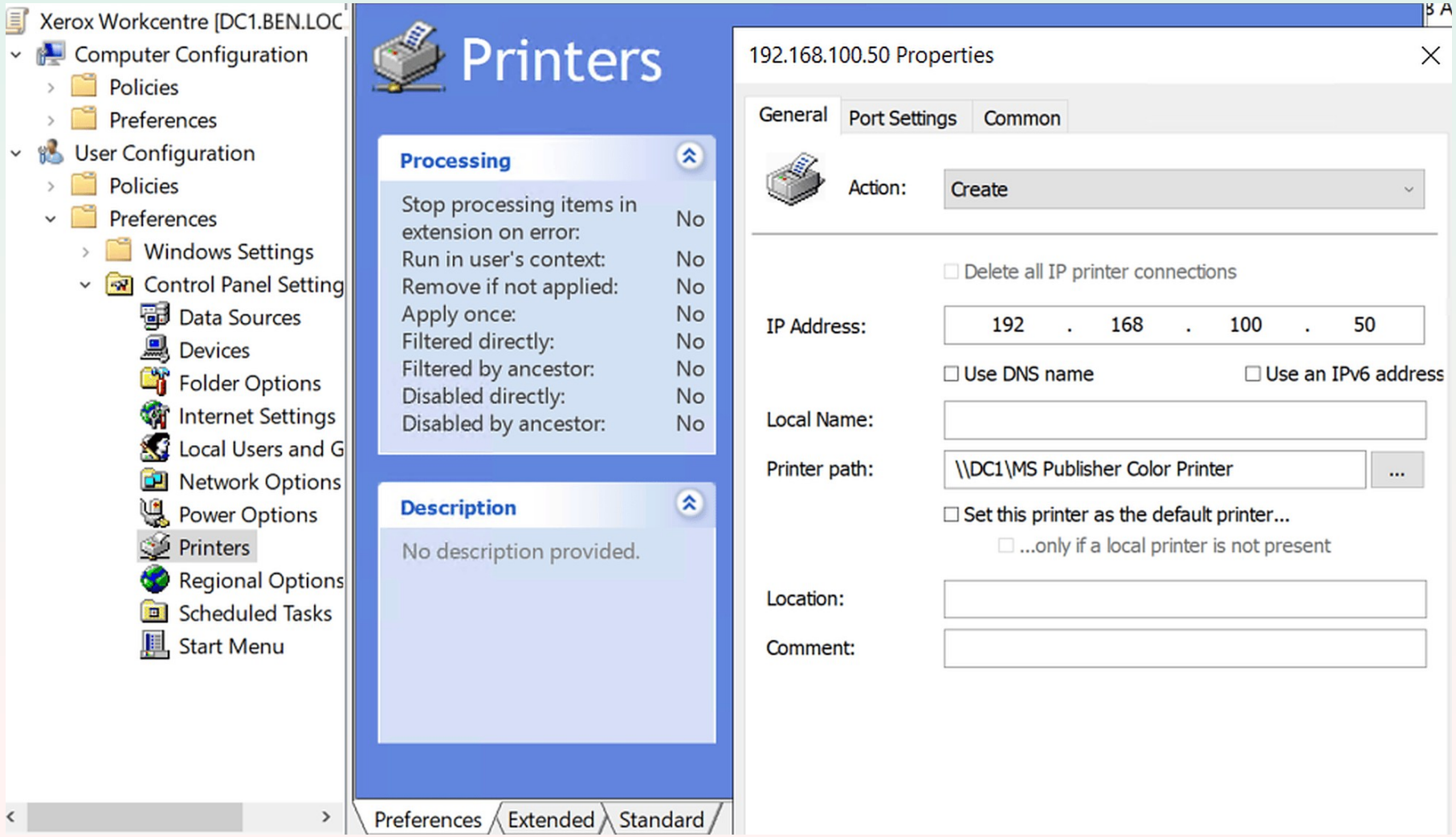
Property of Ben Halevy

Mission Parameters
NETWORK INFRASTRUCTURE



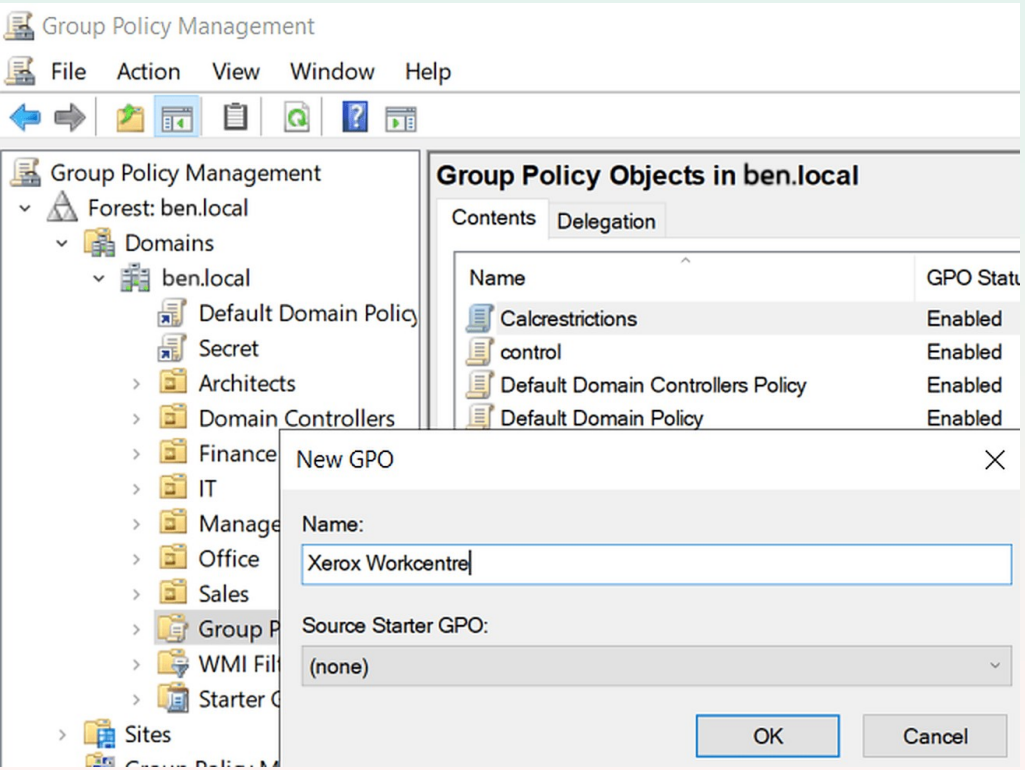
Property of Ben Halevy

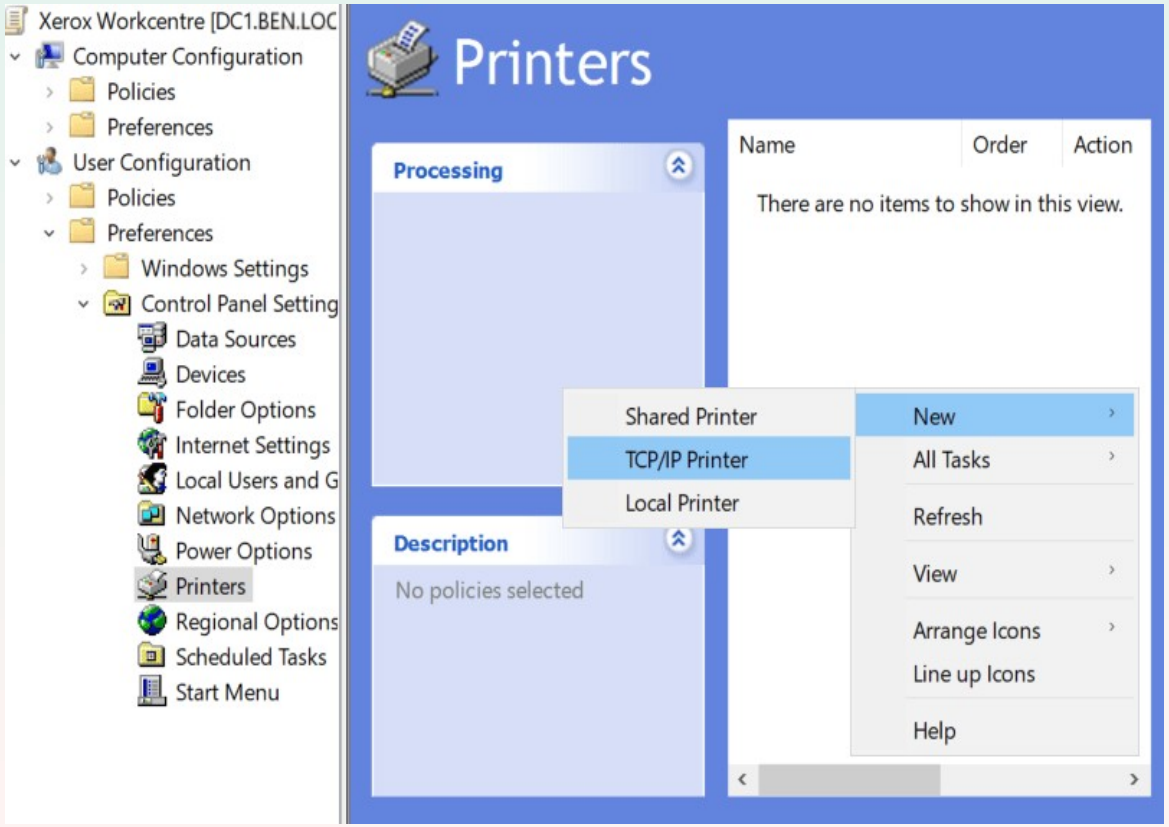
Mission Parameters
NETWORK INFRASTRUCTURE



Property of Ben Halevy

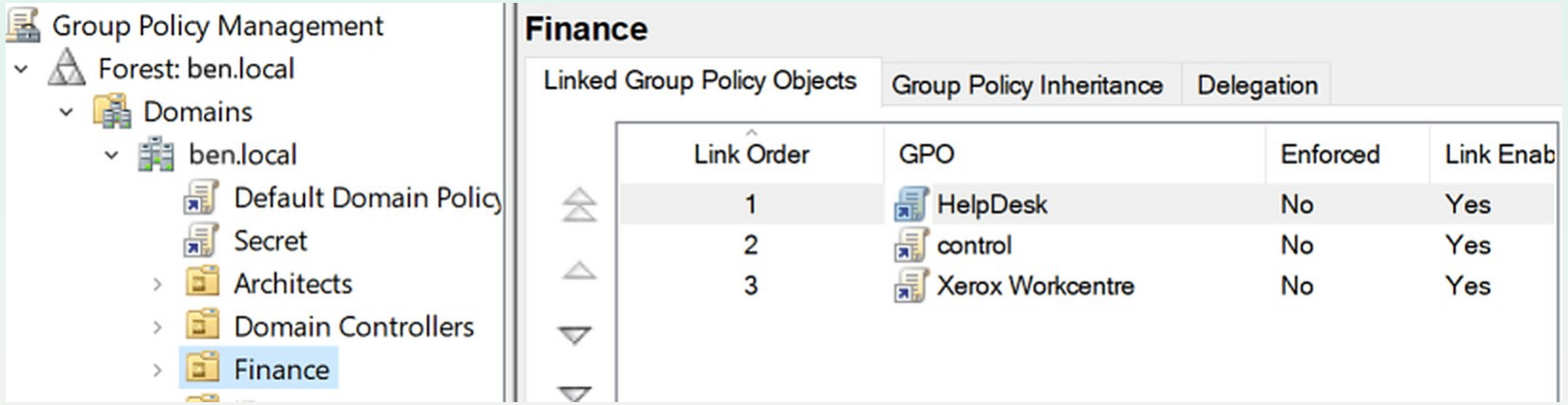
Mission Parameters
NETWORK INFRASTRUCTURE

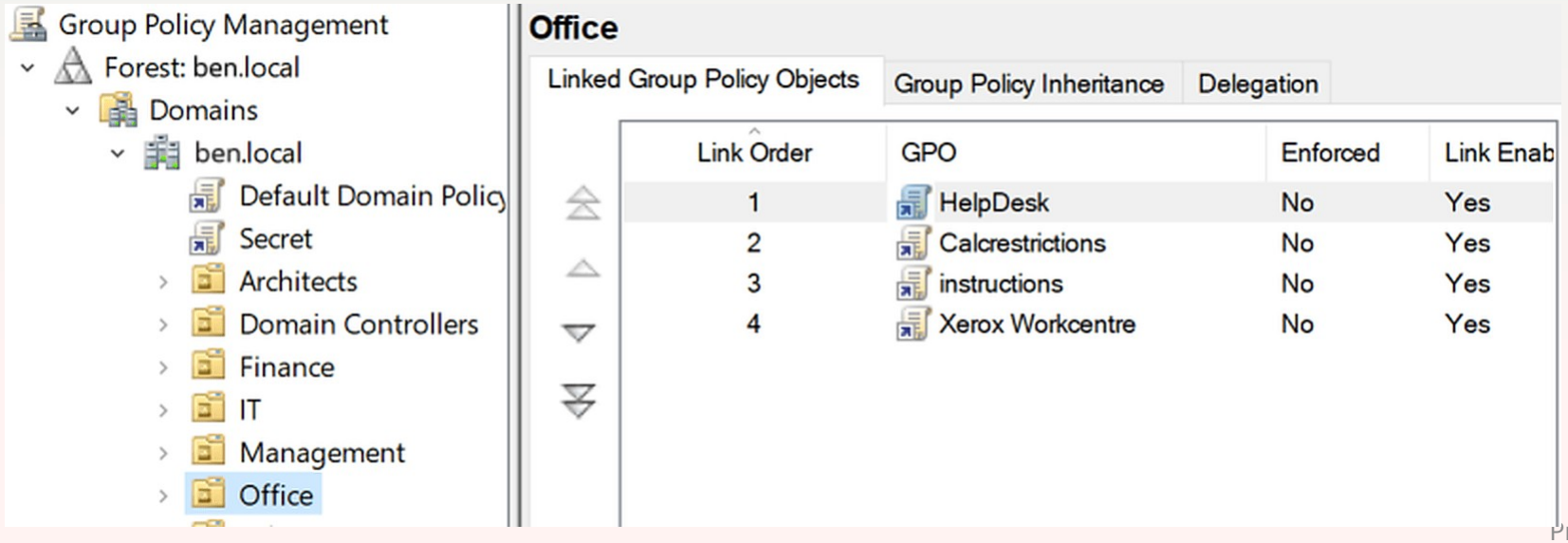




Property of Ben Halevy

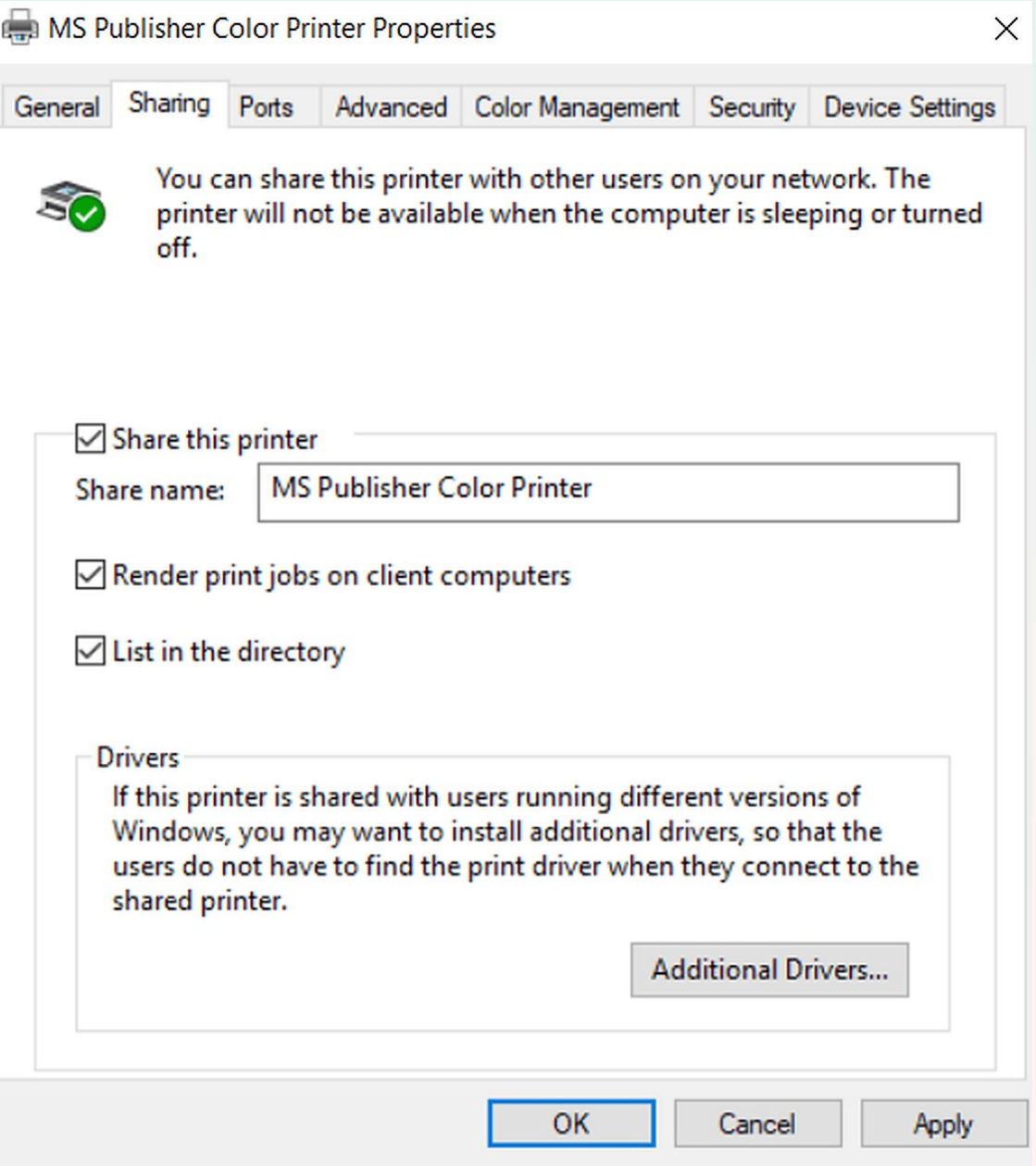
Mission Parameters
NETWORK INFRASTRUCTURE

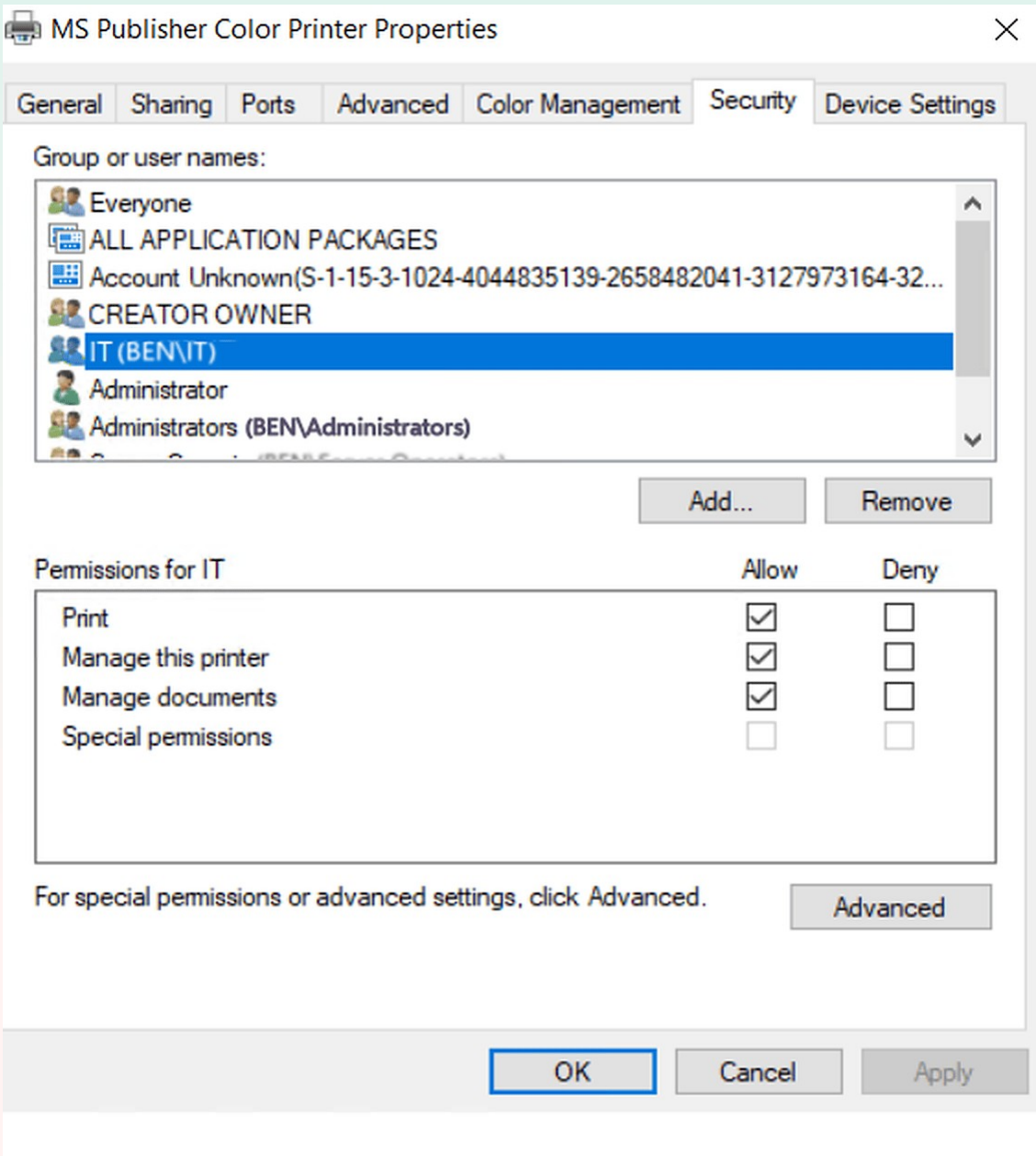




Property of Ben Halevy

Mission Parameters
NETWORK INFRASTRUCTURE





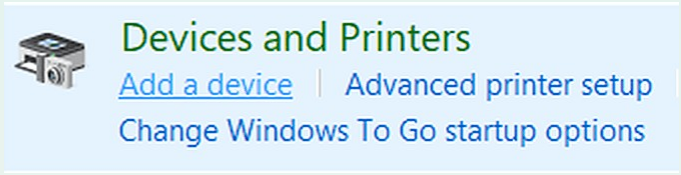
Mission Parameters
NETWORK INFRASTRUCTURE

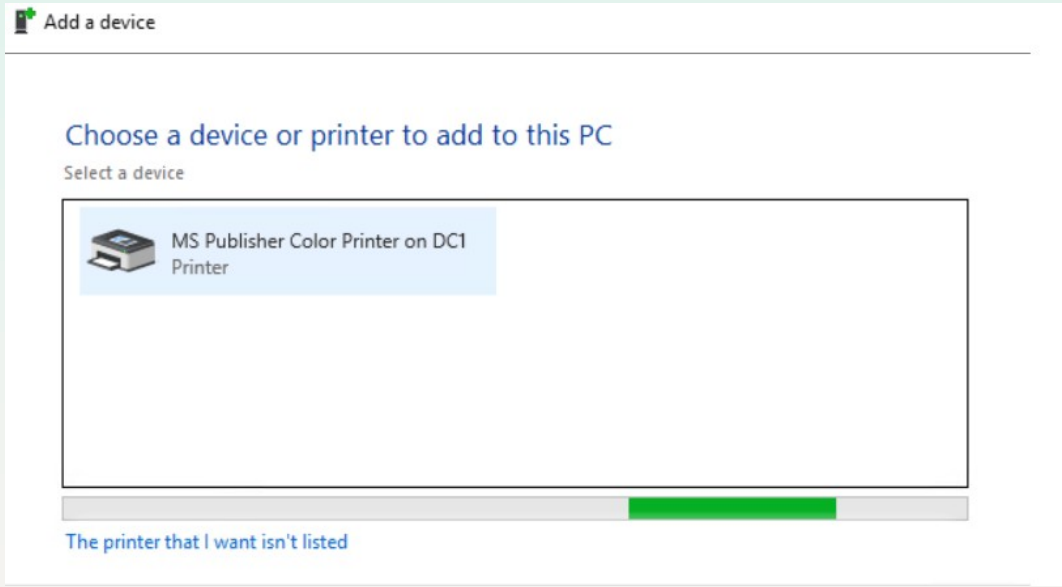
Task
Install a Network Printer On DC1, Share w/ Sales & Architects
Give the IT Dept. the ability to Manage the Printer

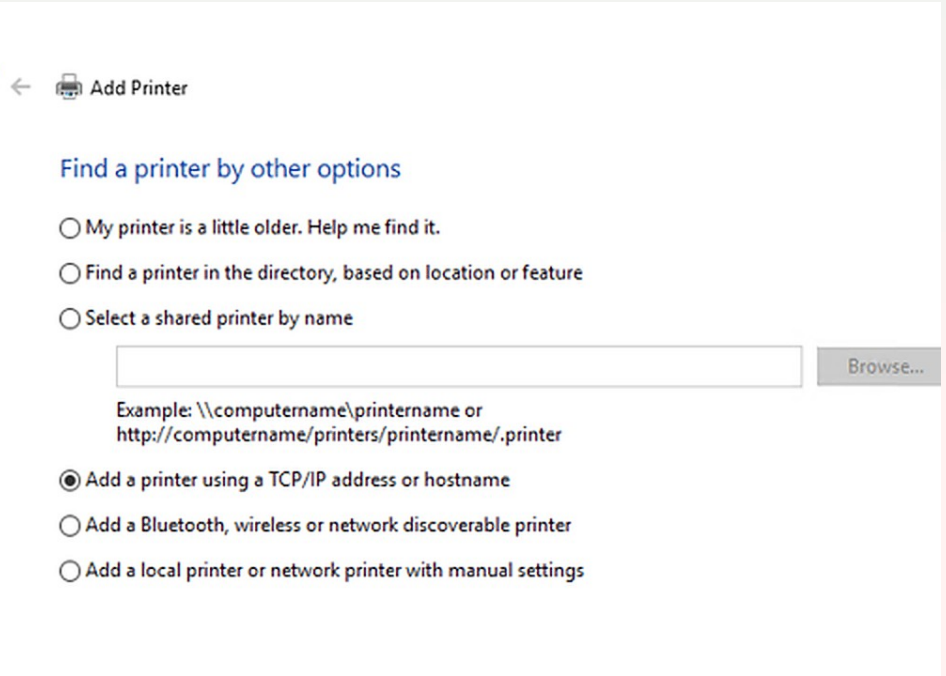
How To Instructions
Control Panel > Hardware > Devices and Printers > Add >Find a Printer By Other Options >Use Tcp/Ip
> add the Printer's Ip address > Pick The Epson Printer > install Driver > right click on the printer you
selected > Sharing tab > Share this Printer > List in the Directory > go to Security tab > Grant the IT >
Group Managing Permissions > Grant the Architect & Sales Groups

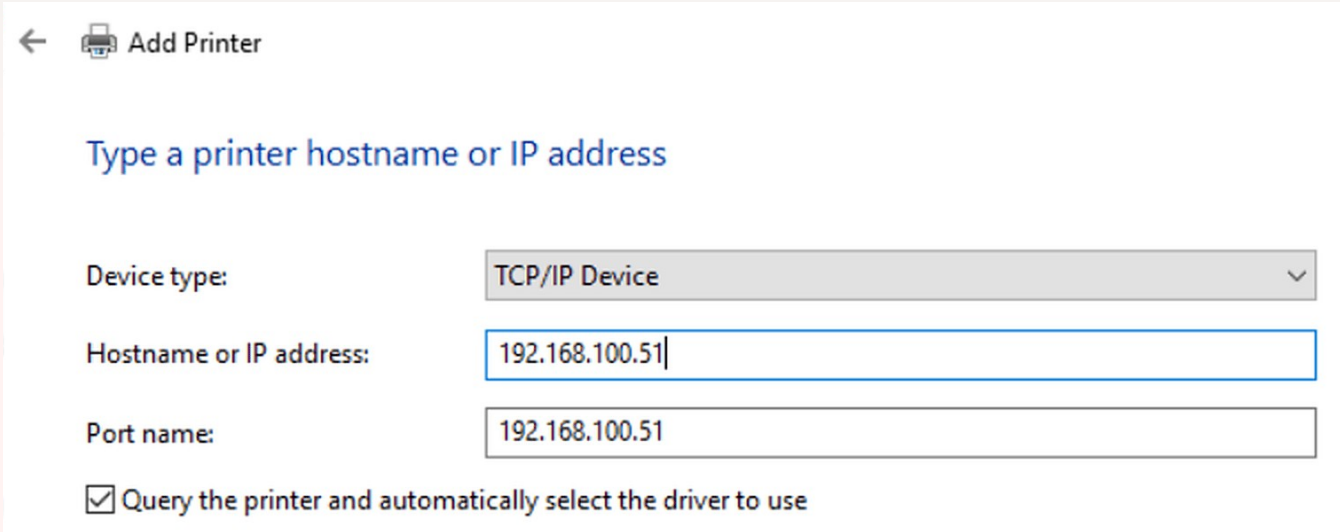
perty of Ben Halevy

Mission Parameters
NETWORK INFRASTRUCTURE

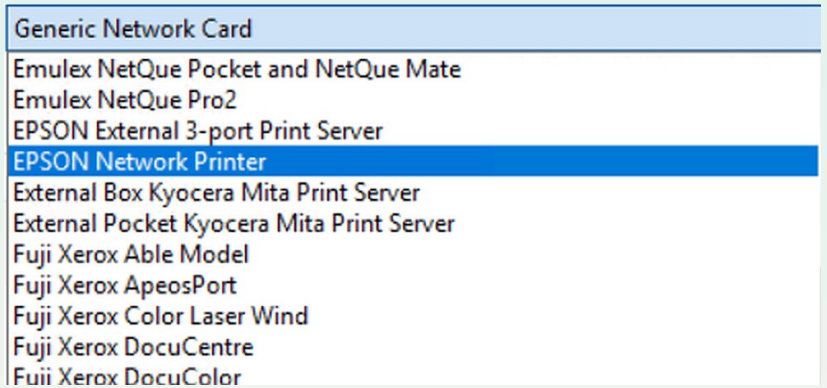


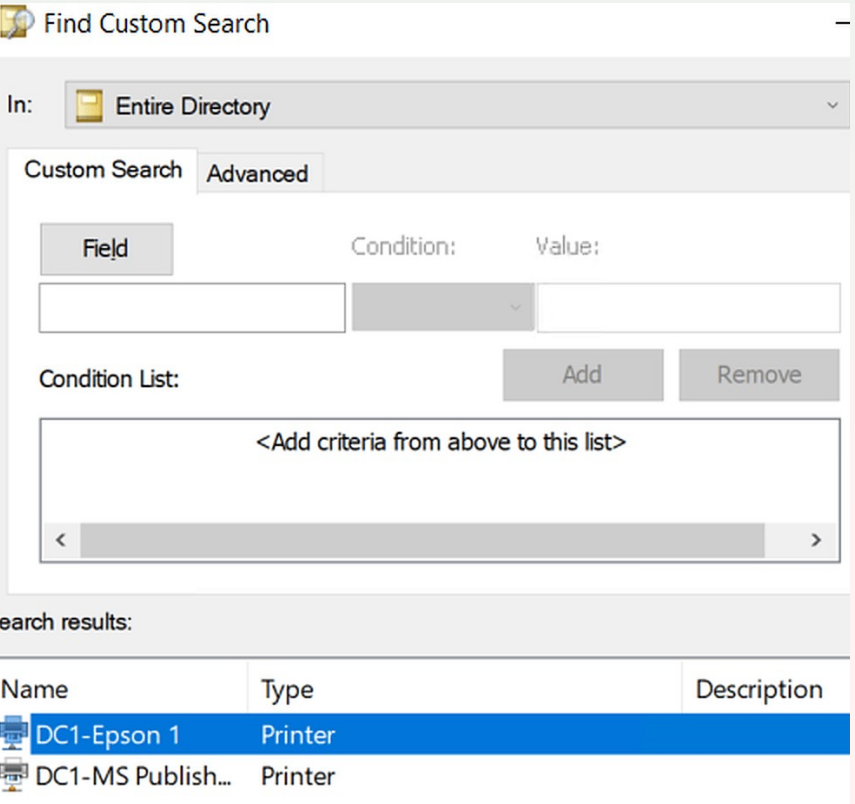


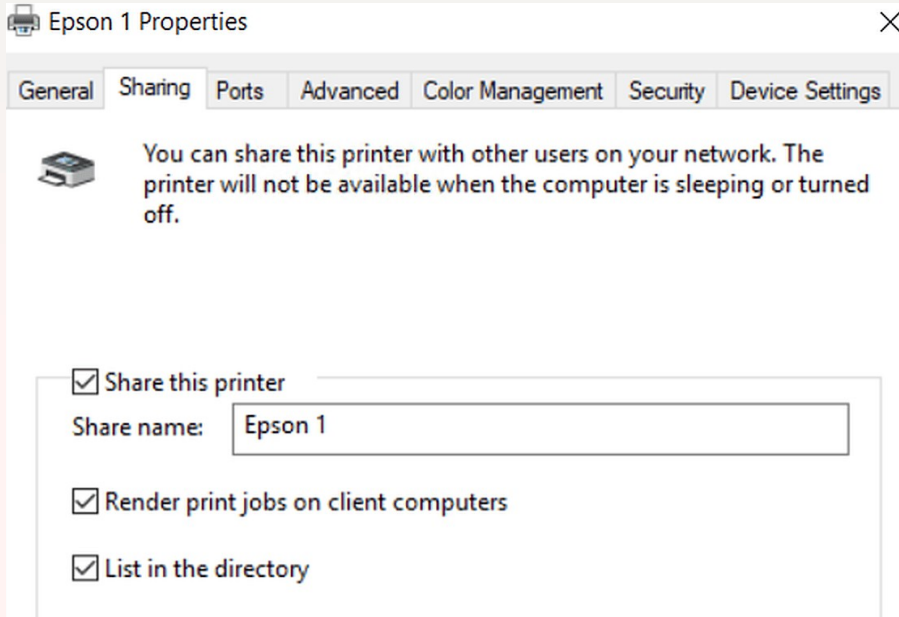




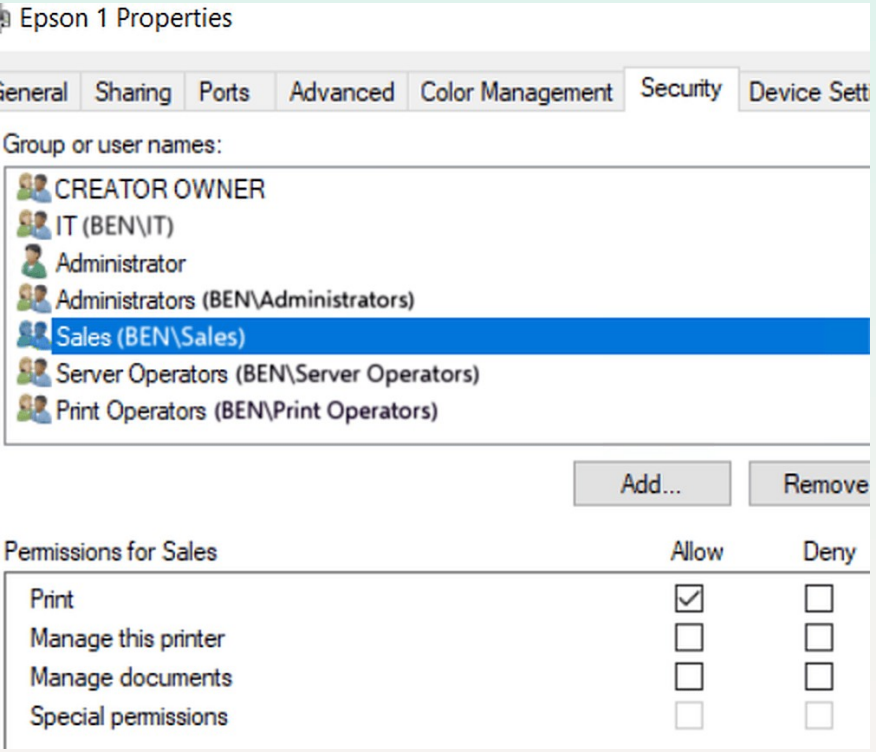
Mission Parameters
NETWORK INFRASTRUCTURE

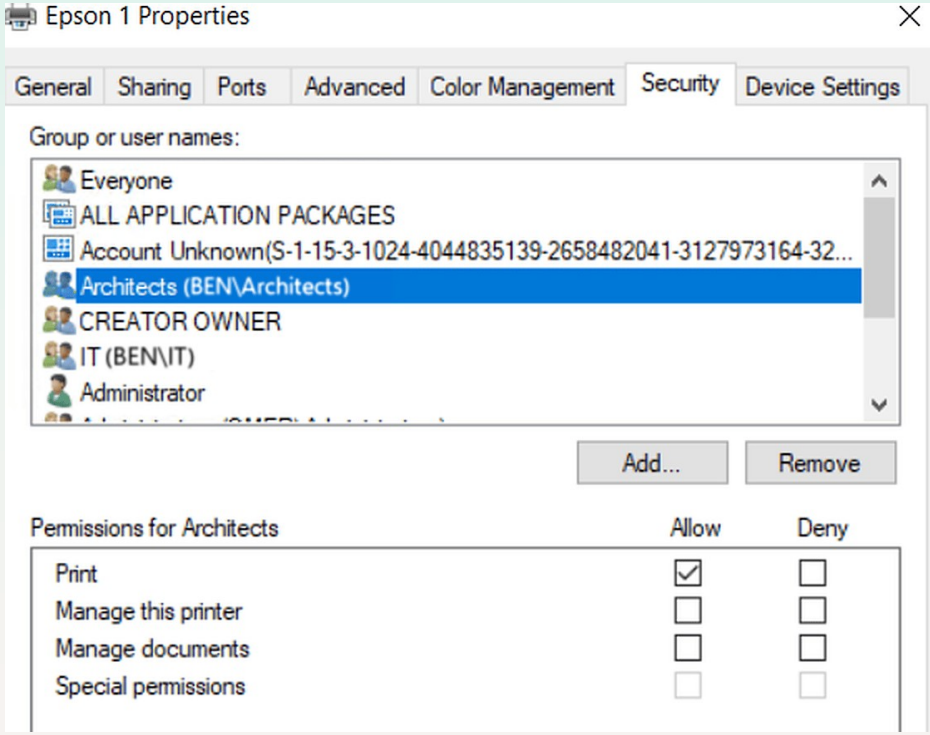


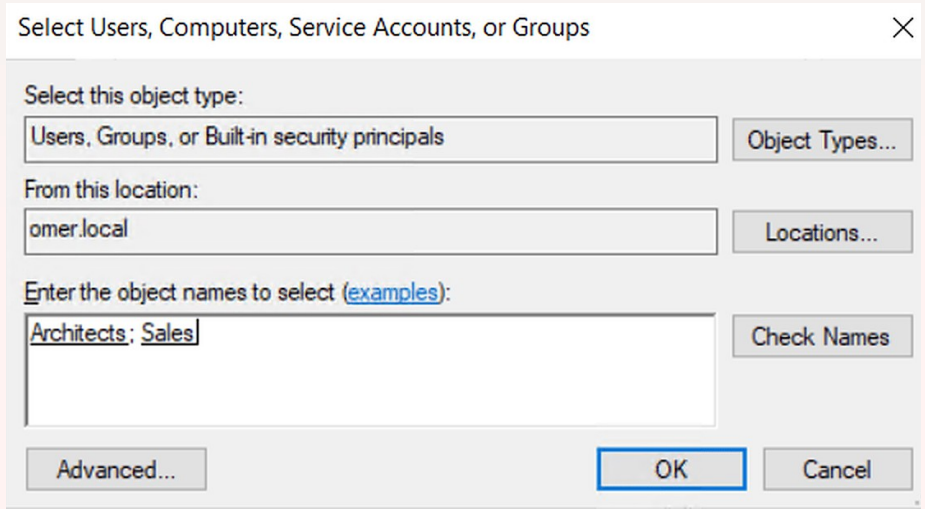


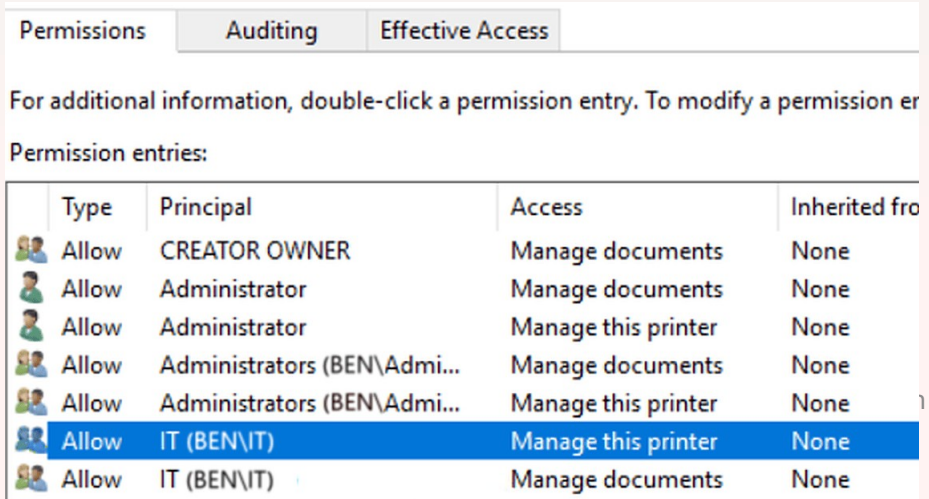


Mission Parameters
NETWORK INFRASTRUCTURE

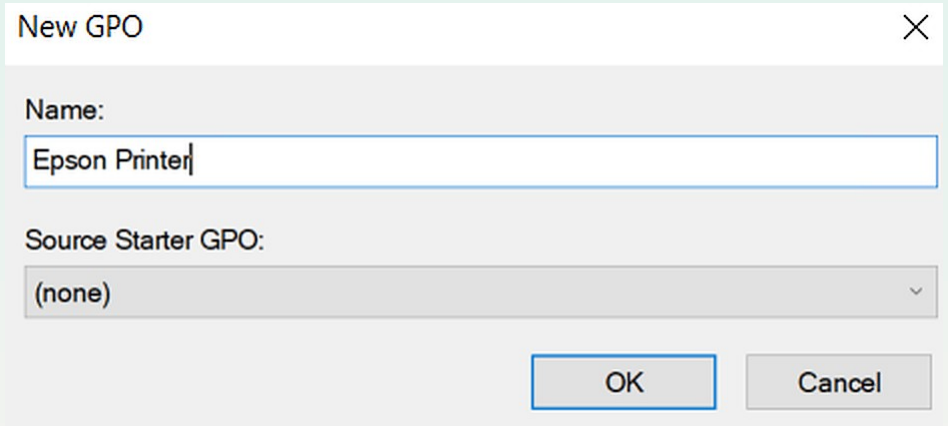


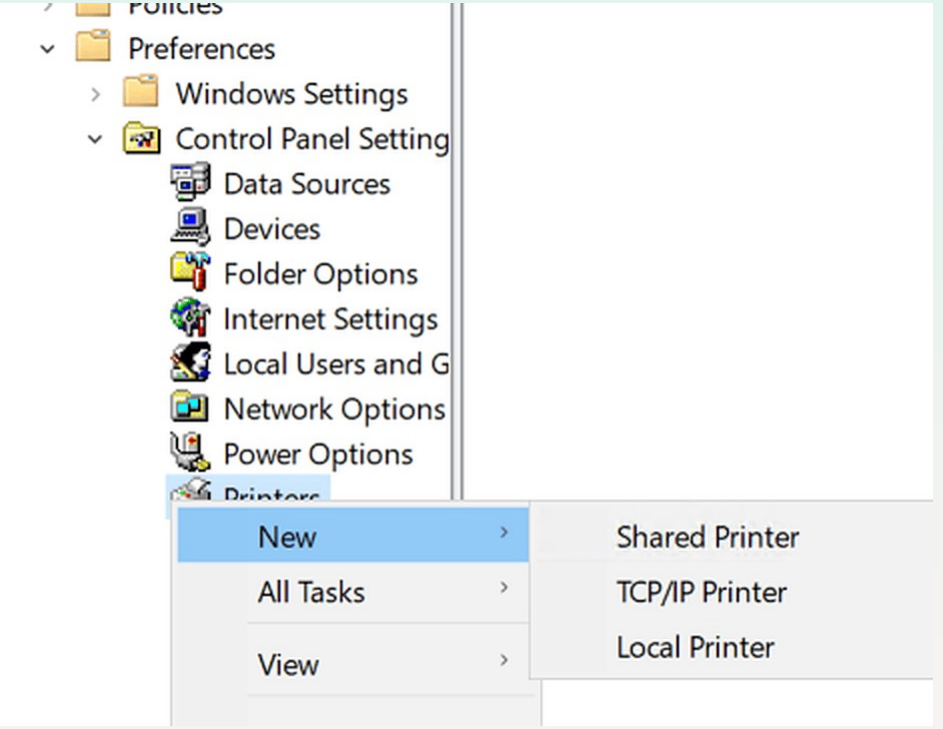


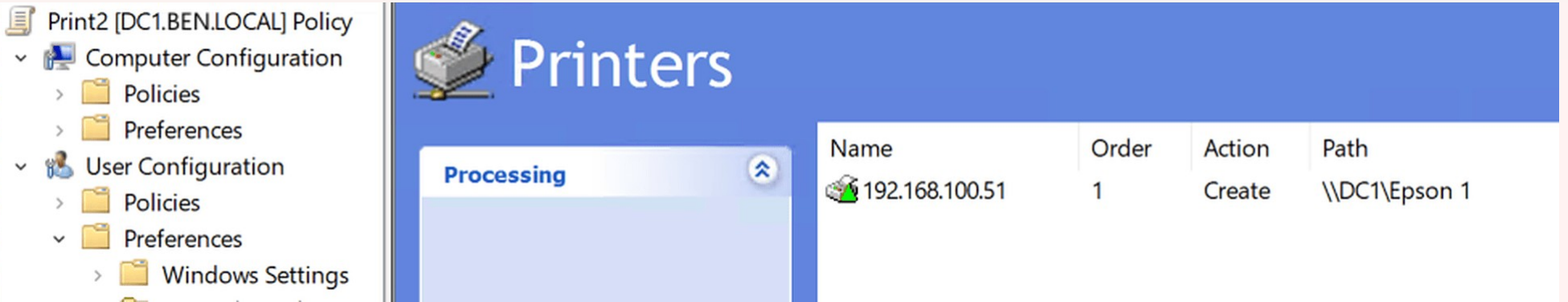




Mission Parameters
NETWORK INFRASTRUCTURE

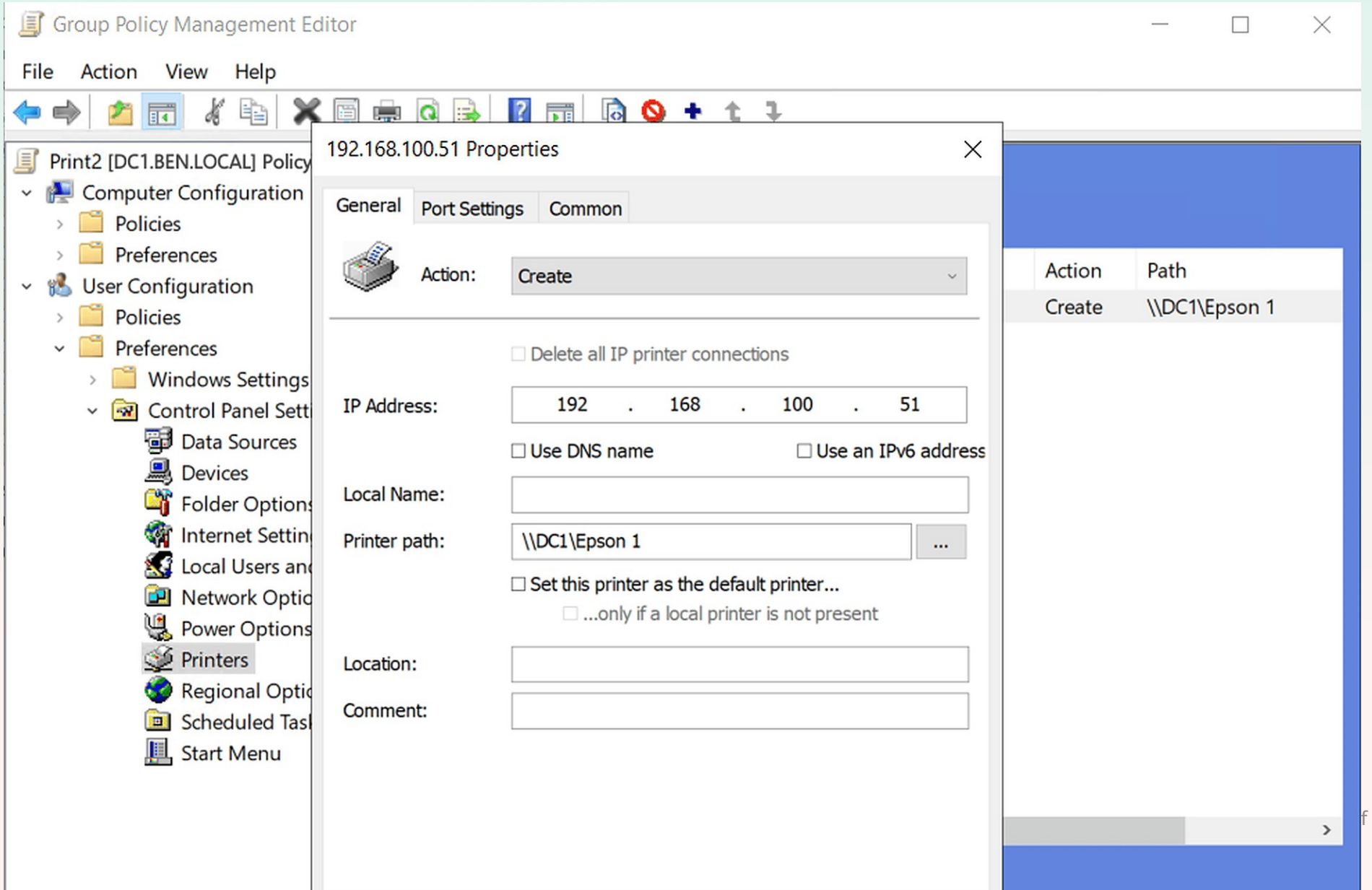






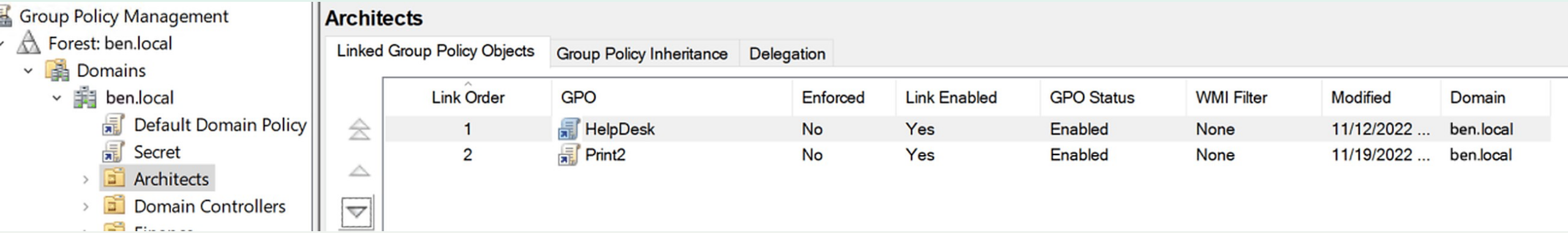
Property of Ben Halevy

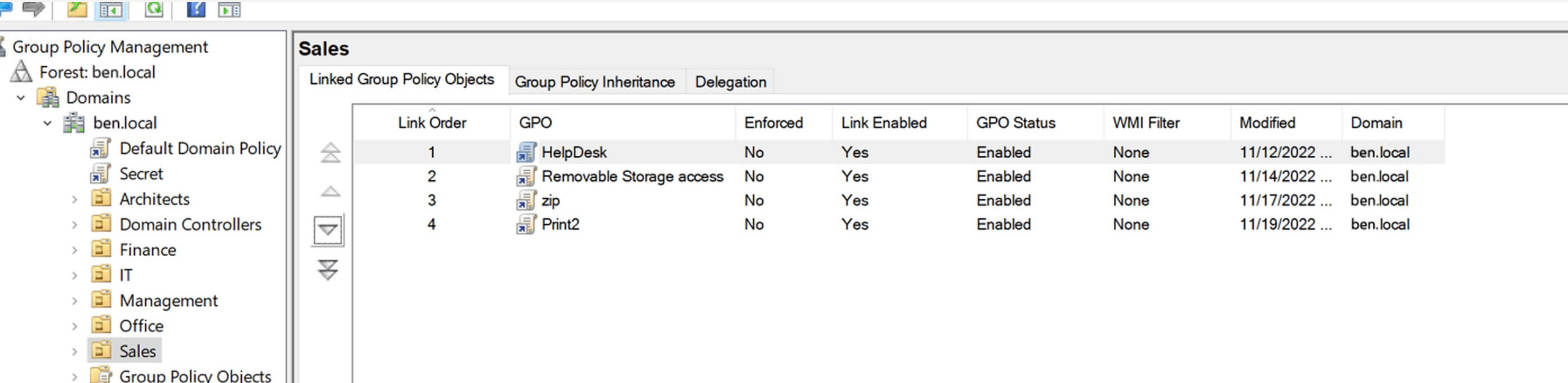
Mission Parameters
NETWORK INFRASTRUCTURE



f Ben Halevy

Mission Parameters
NETWORK INFRASTRUCTURE





Mission Parameters
NETWORK INFRASTRUCTURE


```
PS C:\Users\Administrator> gpupdate /force
Updating policy...


Computer Policy update has completed successfully.

User Policy update has completed successfully.



PS C:\Users\Administrator> gpupdate /force
Updating policy...


Computer Policy update has completed successfully.

User Policy update has completed successfully.



PS C:\Users\Administrator>
```

Property of Ben Halevy

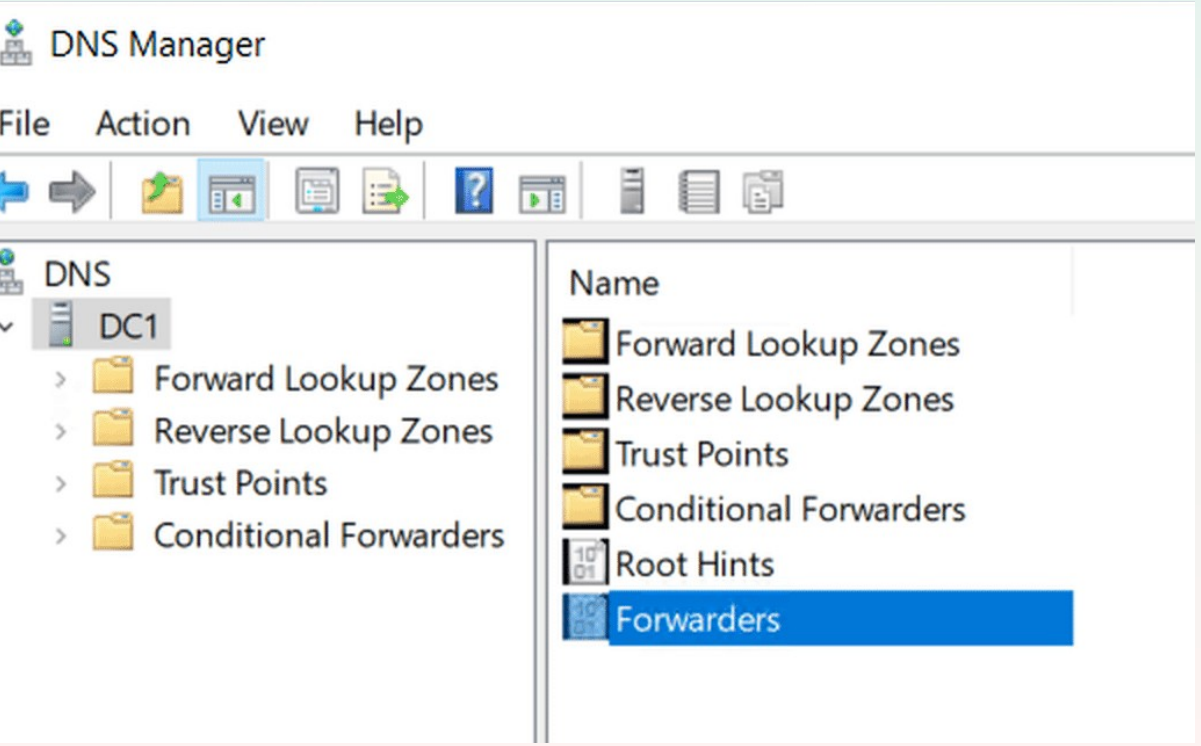
Task
Adjust DC Server DNS Settings (Forwarder, Root Hints)

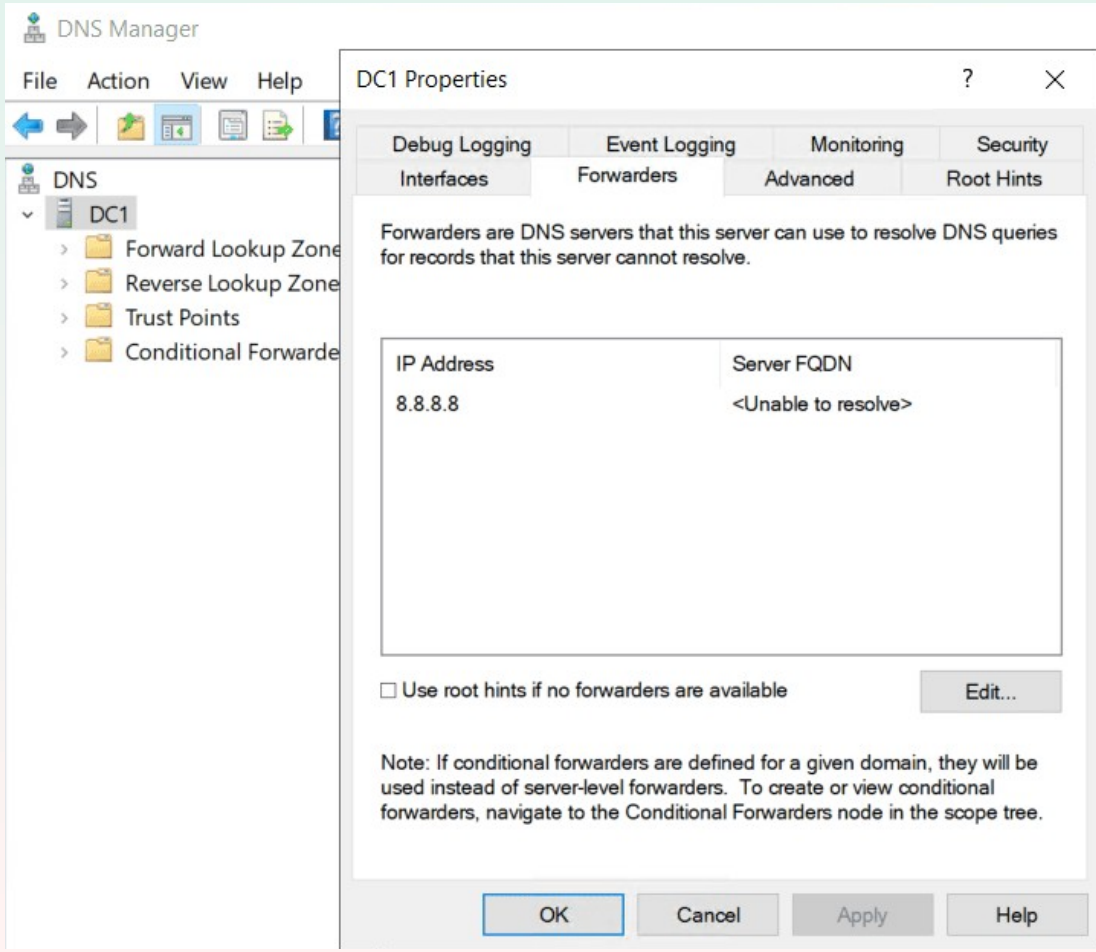
How To Instructions
AD Tools > DNS > Right Click on On DC1 > Properties > Forwarders > Edit > Enter Ip Address or Dns Name
(For our purpose I entered 8.8.8.8) > OK > Uncheck “User Root Hints if no Forwarders are available”

Property of Ben Halevy

Mission Parameters

NETWORK INFRASTRUCTURE



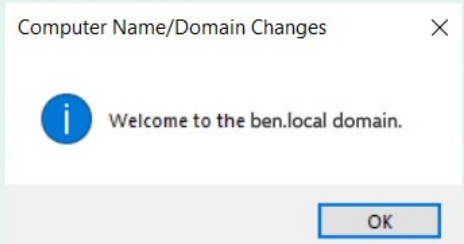


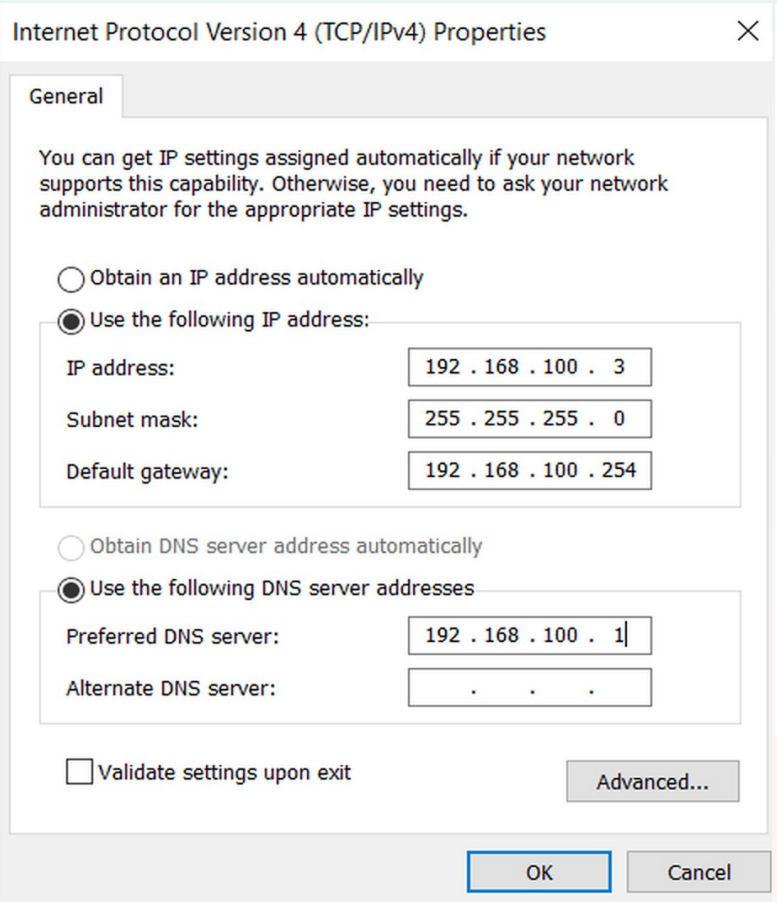
Property of Ben Halevy

Mission Parameters
NETWORK INFRASTRUCTURE

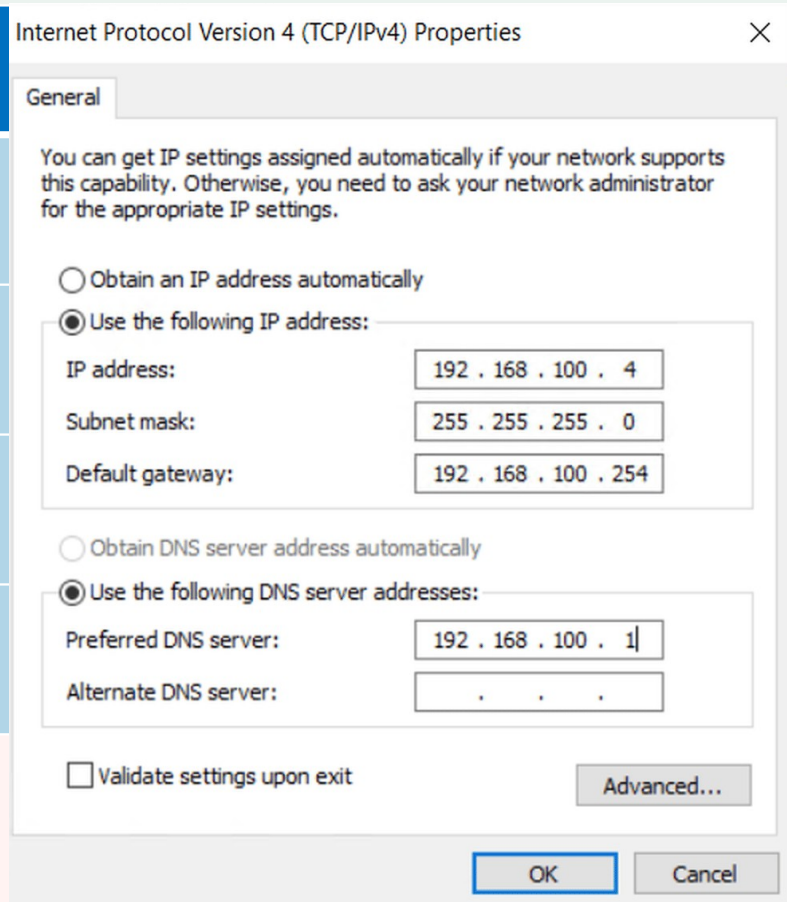
Task
Create 2 Virtual Machines (2Gb Ram) (30Gb HD) Ea. (IS1 & IS2), Install on both Machines IIS(webservers) Roles , Add the Feature of Network
Load Balance Manager on Both Machines , Create one Website, Place the site On Both Machines , Create an NLB Cluster with both of the IS servers
Change Names > Manage> Add Features > Network Load Balancing > after installation on both machines restart > Manage > Add Role > Web Server (IIS) >
input the following IP information for each respective Machine > add the two servers to the domain BEN.LOCAL > Create A Folder in each Machine
C:Myfolder > in each Machine Folder Create A File Named Site.html > Tools > Internet Information Services Manager (IIS) > Click On IS2 > Right Click on
Go To IS1 > Tools > Network Load Balancing > Right Click on NLBC > Create New Cluster > Enter Host IP 192.168.100.3 > Cluster Operations – Multicast >
Cluster Port Range : 80-80 > TCP Protocol > once finished add another cluster with IS2 Credentials > Once Complete go to DC1 to Associate the Website
To the DNS Server > Tools > DNS > Click on DC1 > New Forward Lookup Zone > Zone Name : site.com > you will see many more classifications in the wizard >

Mission Parameters
NETWORK INFRASTRUCTURE

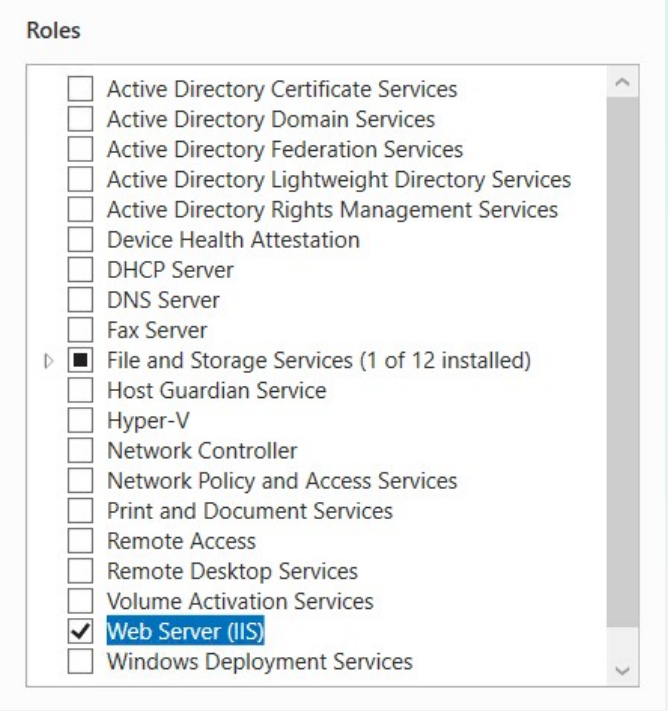


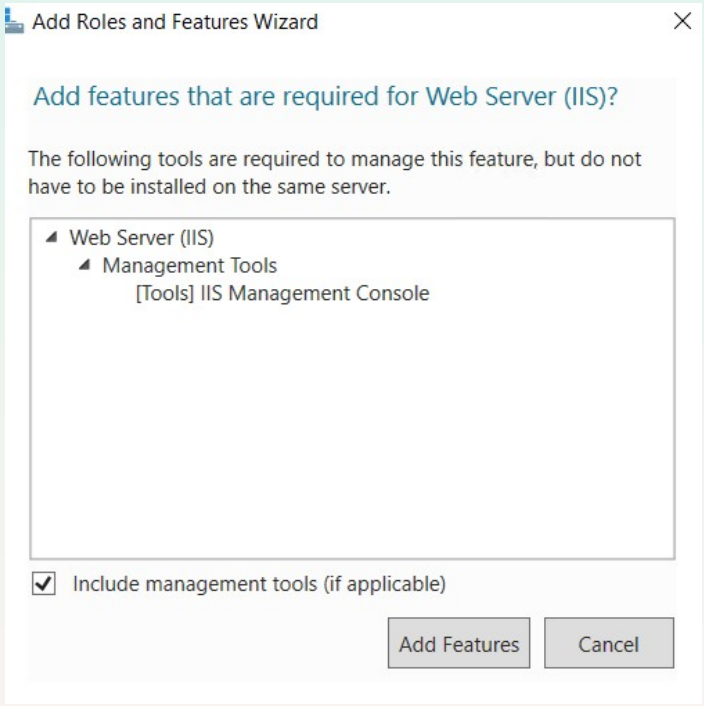


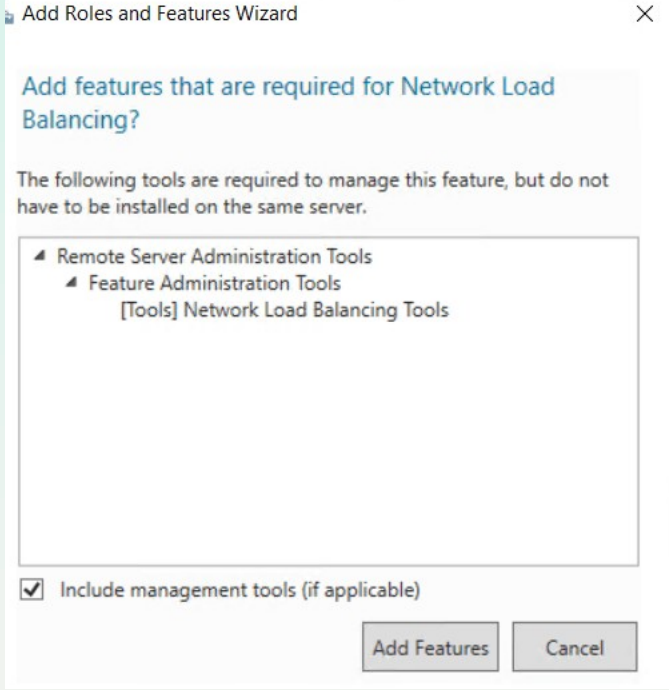
IS1	IPV4 Properties	IS2
IP:192.168.100.3		IP: 192.168.100.4
Subnet: 255 255.255.0		Subnet: 255 255.255.0
Default : 192.168.100.254		Default : 192.168.100.254
DNS: 192.168.100.1		DNS: 192.168.100.1

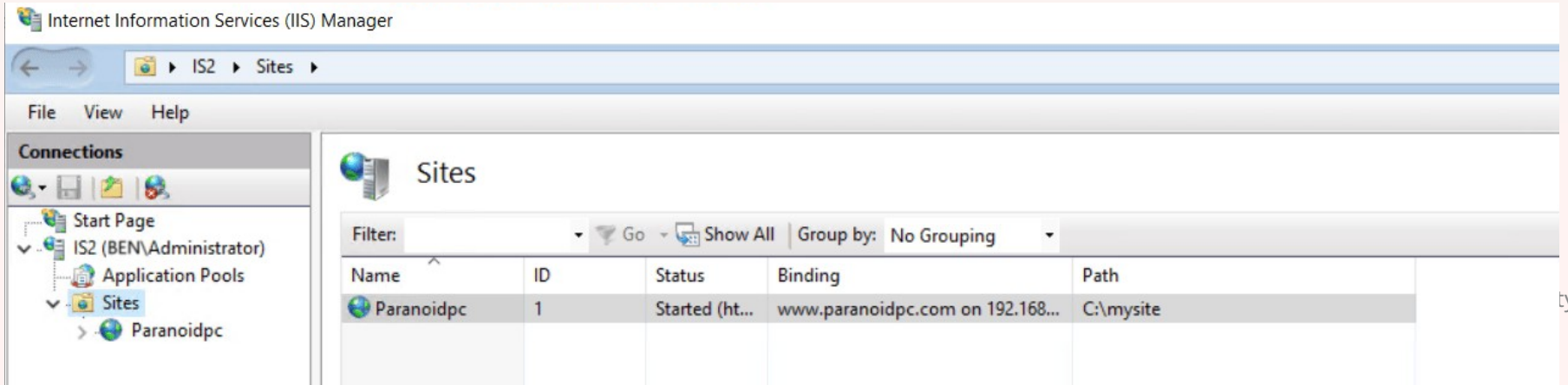


Mission Parameters
NETWORK INFRASTRUCTURE



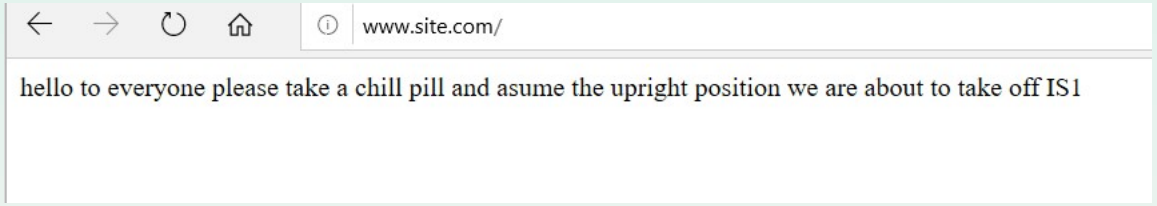


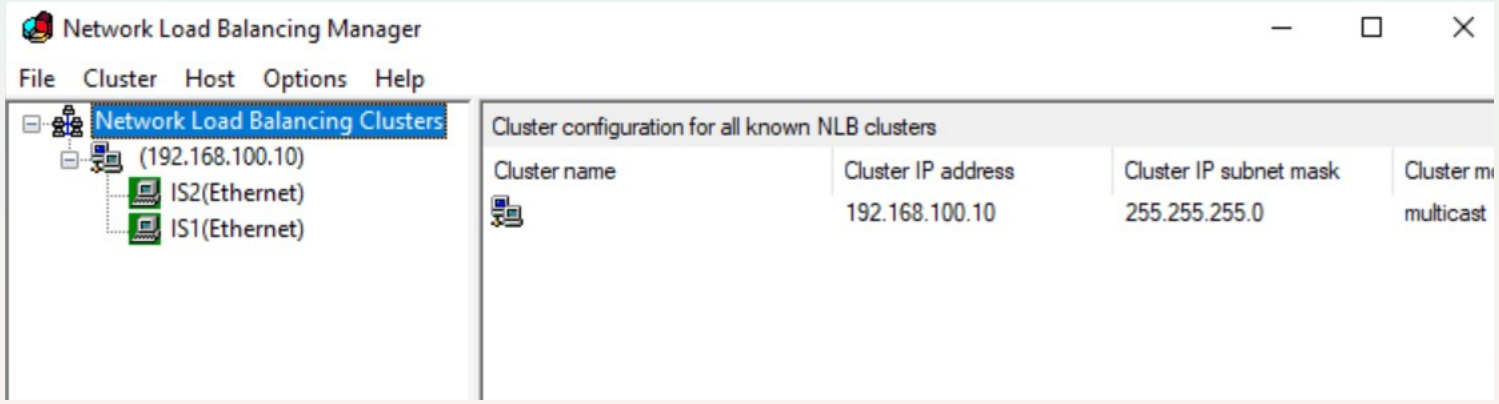


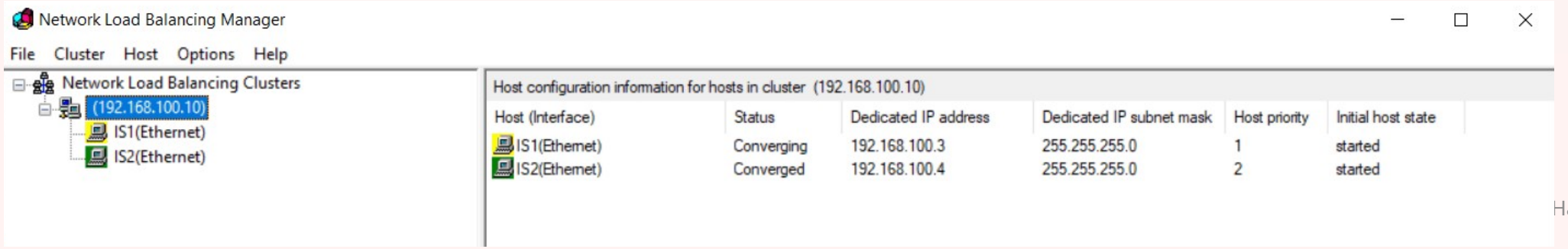


ty of Ben Halevy

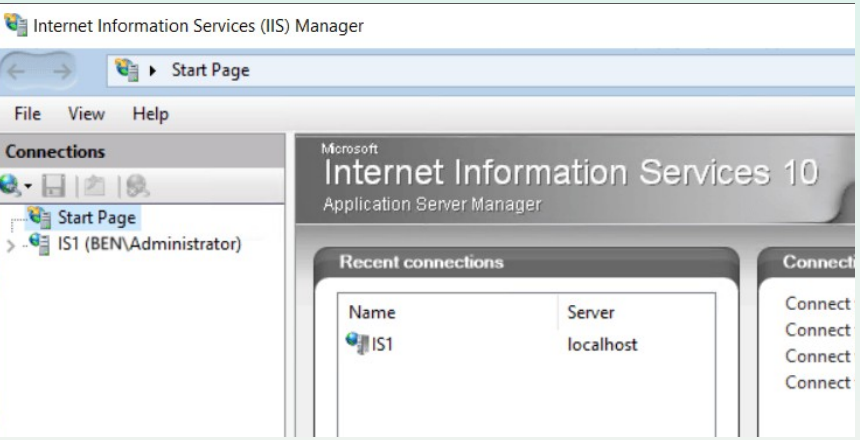
Mission Parameters
NETWORK INFRASTRUCTURE

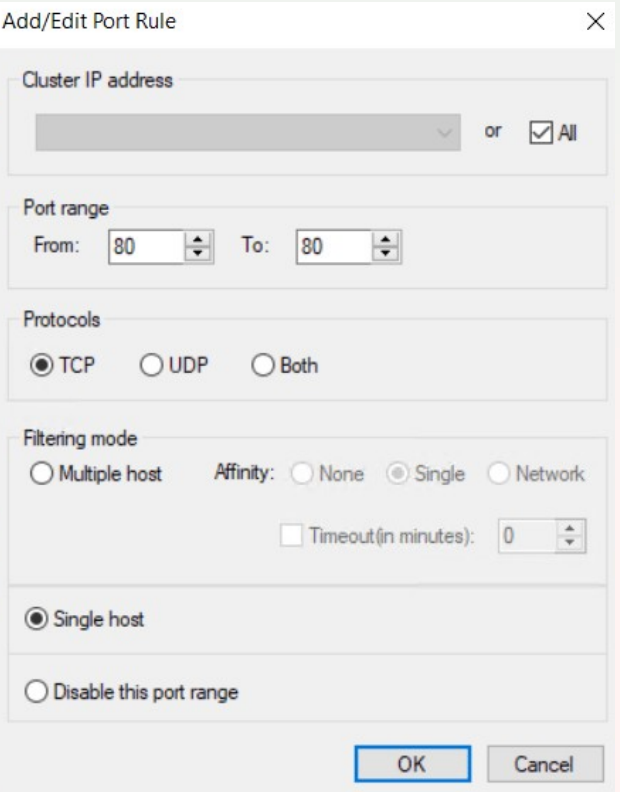


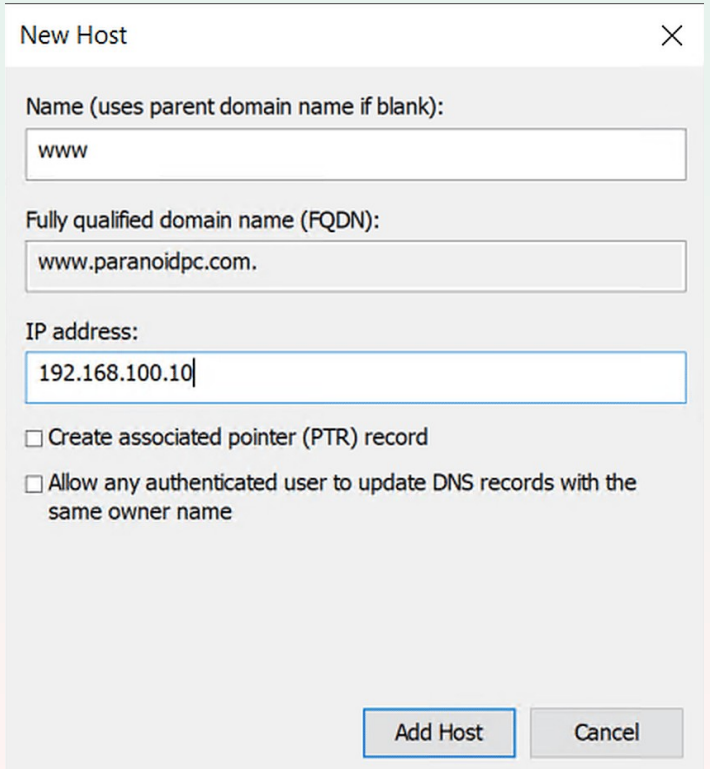


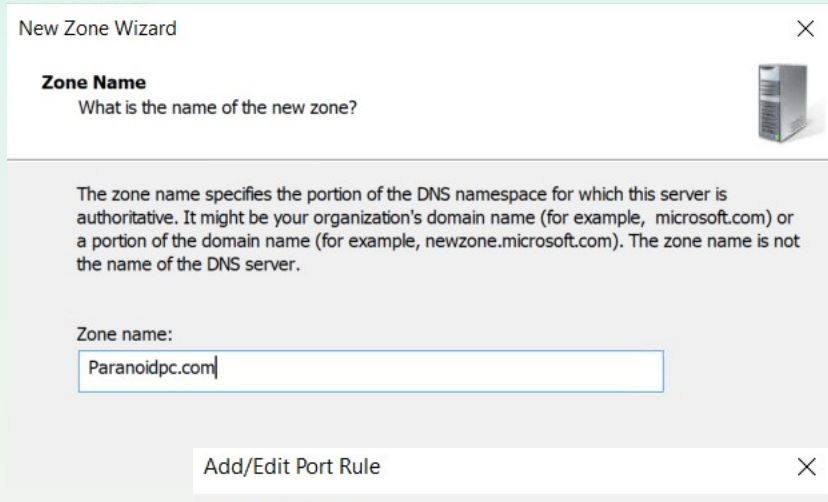


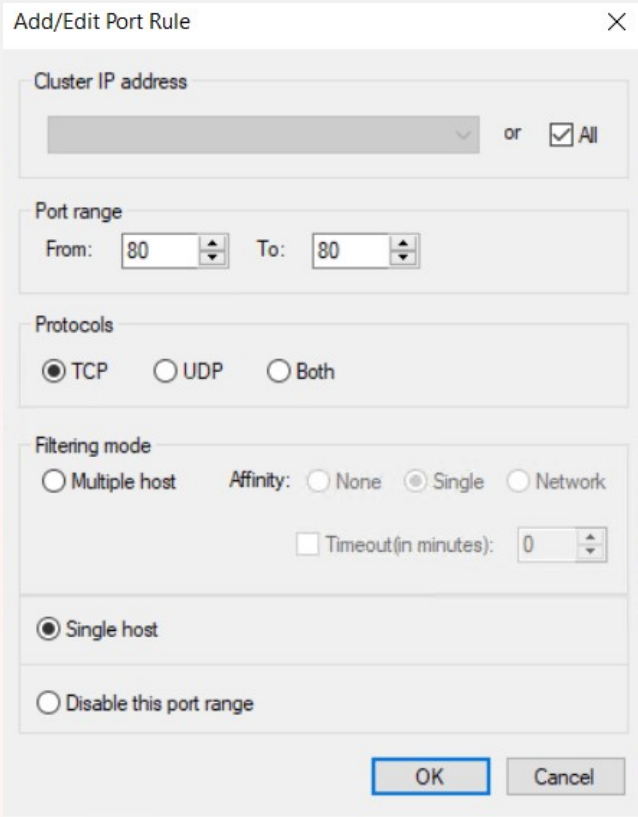
Mission Parameters
NETWORK INFRASTRUCTURE









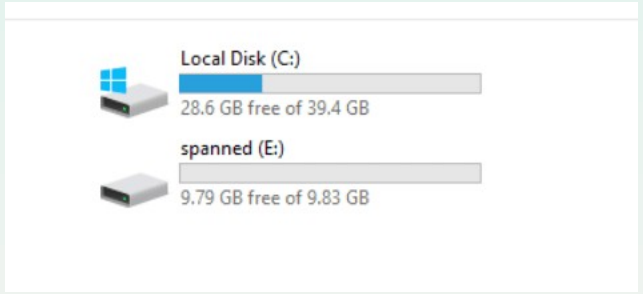


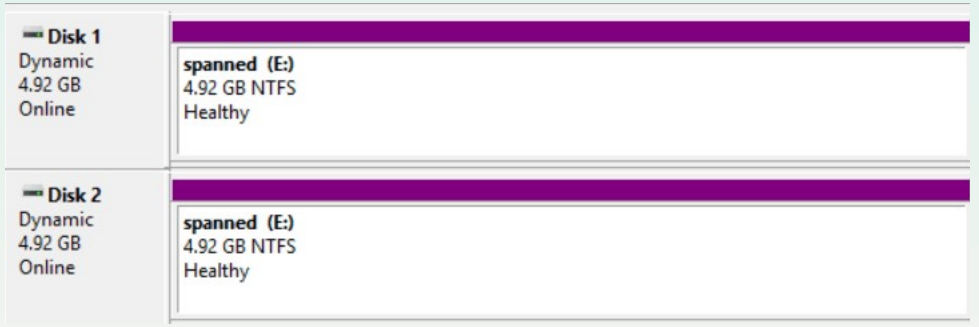
Mission Parameters
NETWORK INFRASTRUCTURE

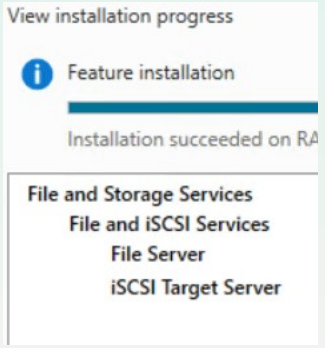
Task
Connect Two HD's to the RAS Server , Ea. Hd (5Gb) Configure the RAS Server as A ISCSI Target with those
Two HD's ; Connect the DC2 Server to the two HD's Connected to the RAS Server
Through the Initiator/Target Protocol So that you see A 10 GB On the DC2 Server was Drive E:

How To Instructions
Begin By Adding to Virtual HDD's to the RAS Server > Inialize the Drives >Place them in Online status > Format them >Create Two Simple Volumes >
Give the RAS Server a New Role (ISCSI Target) > Once the Role Is Installed, Install a New Pool with the First HD > Associate the DC2 IP to the Pool >

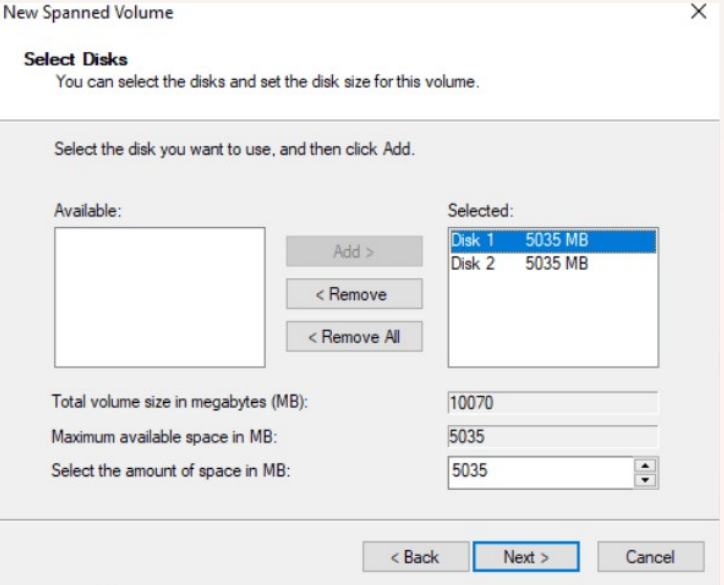
Mission Parameters
NETWORK INFRASTRUCTURE



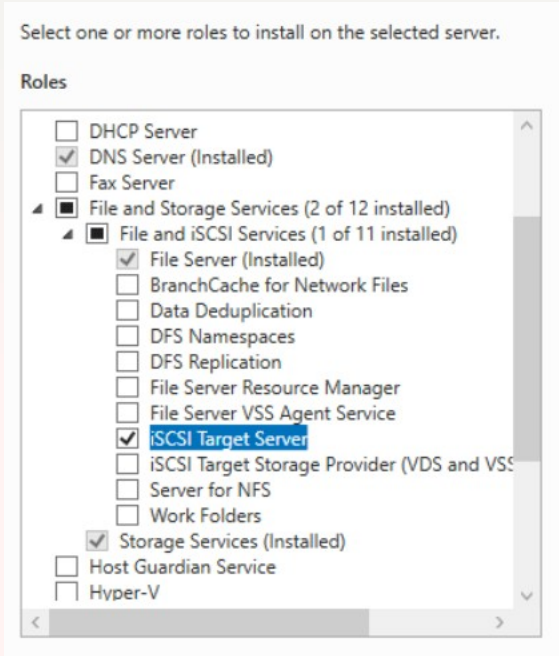












Mission Parameters
NETWORK INFRASTRUCTURE

Confirm that the following are the correct settings,

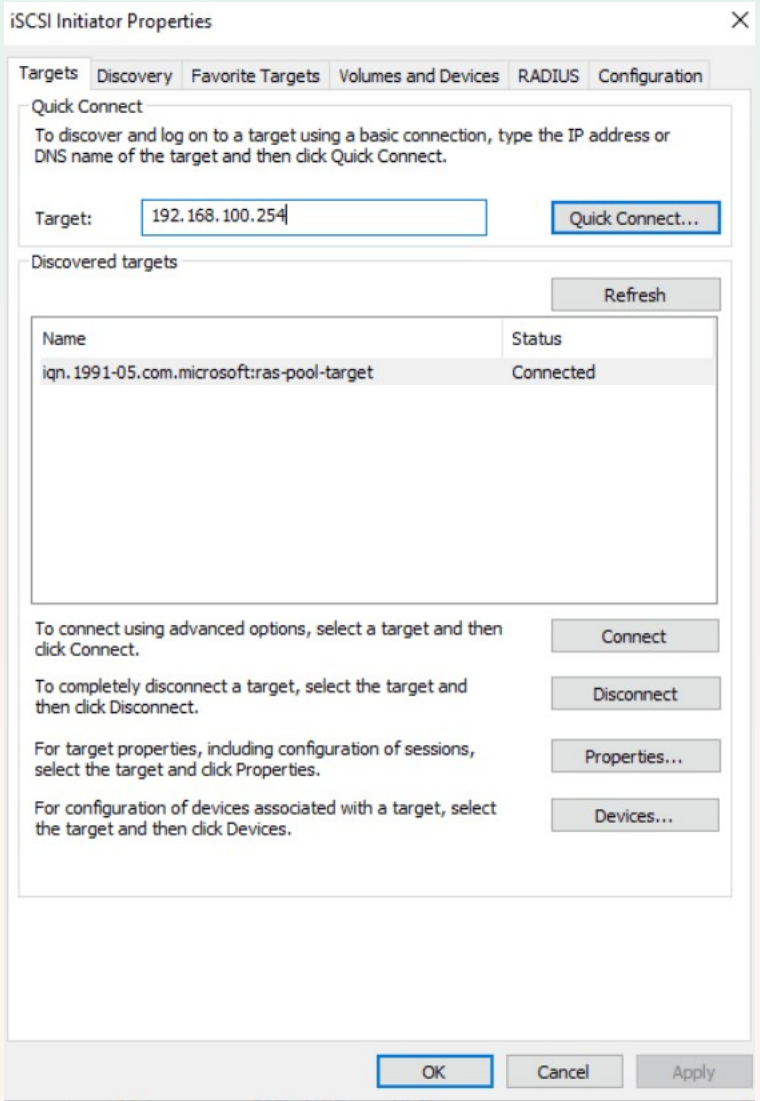
ISCSI VIRTUAL DISK LOCATION
Server: RAS
Cluster role: Not Clustered
Path: F:\iSCSIVirtualDisks\poo2.vhdx

ISCSI VIRTUAL DISK PROPERTIES
Name: poo2
Size: 4.92 GB

TARGET PROPERTIES
Name: pool

ACCESS SERVERS
IP Address: 192.168.100.2

SECURITY
CHAP: Disabled
Reverse CHAP: Disabled



Confirm that the following are the correct settings,

ISCSI VIRTUAL DISK LOCATION
Server: RAS
Cluster role: Not Clustered
Path: E:\iSCSIVirtualDisks\vol3.vhdx

ISCSI VIRTUAL DISK PROPERTIES
Name: vol3
Size: 4.92 GB

TARGET PROPERTIES
Name: pool

ACCESS SERVERS
IP Address: 192.168.100.2

SECURITY
CHAP: Disabled
Reverse CHAP: Disabled

Property of Ben Halevy

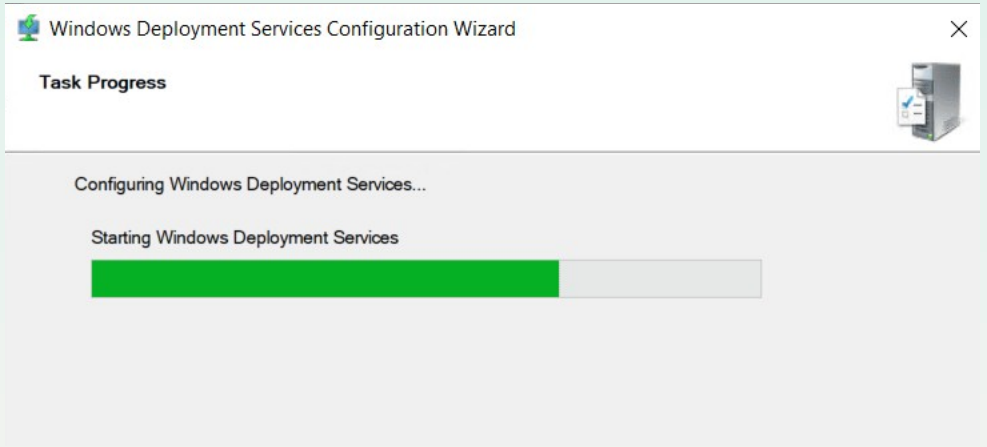
Mission Parameters
NETWORK INFRASTRUCTURE

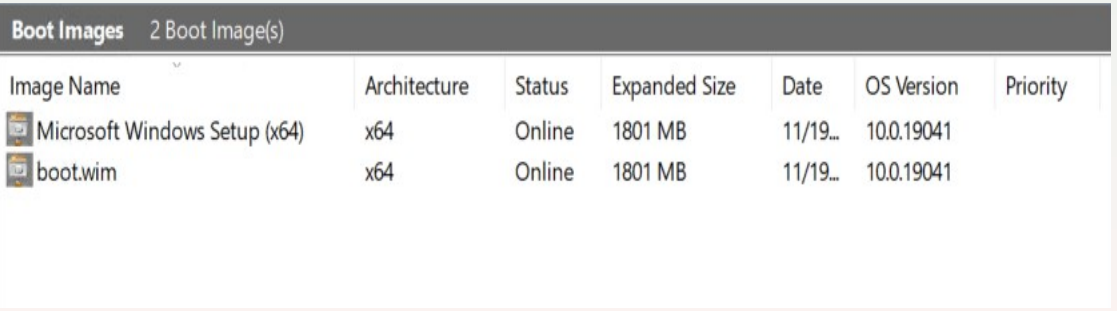
Task
Create A New Virtual Machine Named NEW (1Gb Ram) (20Gb HD)
LAN Connection , W/PXE BOOT . Install WDS Role On DC1 Server
Perform the necessary Protocols to Remotely install a Windows 10
Operating System On the Virtual Machine New.

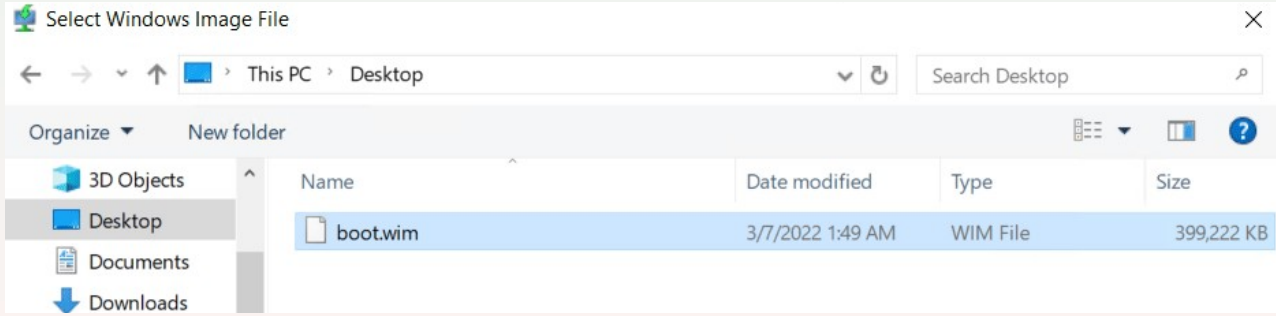
How To Instructions
In addition to creating a new VM named New > Create A new VM named Master so that you have a readily available fresh installation of Windows to obtain
the necessary file required to perform the remote install Install the Role Windows Deployment Services On DC1 > Erase the Digital Footprint of the
Operating System On the VM (Master) > (SYSPREP)> Generalize > Shutdown >Use the WDS to Distribute

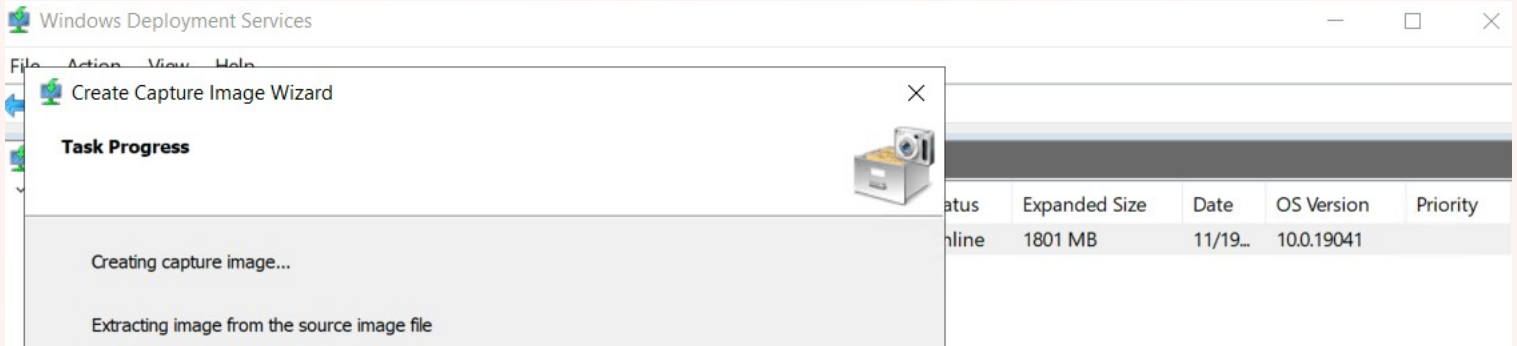
Mission Parameters
NETWORK INFRASTRUCTURE





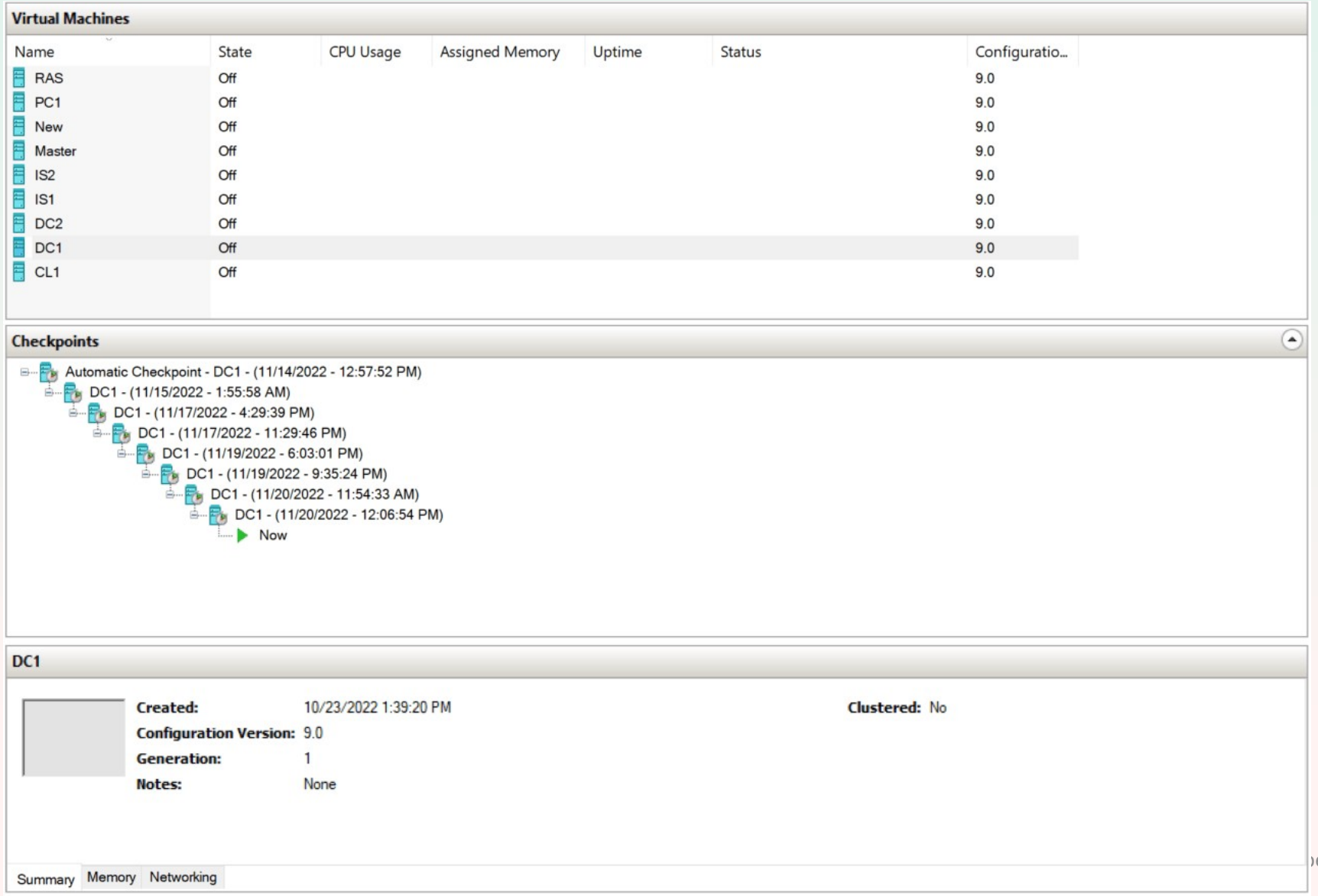






Property of Ben Halevy

Mission Parameters
NETWORK INFRASTRUCTURE



erty of Ben Halevy

Mission Parameters
IMAGE DEPLOYMENT

TASK
Build ONE fully prepared Windows 10 "golden image" on the VM Master and deploy it to any number of endpoints over the network from DC1.
Tools: Sysprep (generalize) > DISM (capture & offline servicing) > WDS (PXE network deployment) - the standard path for mass roll-outs.



COMPONENT	ROLE IN THIS PROCESS
DC1 (192.168.100.1)	**AD DS (BEN.LOCAL), DNS, DHCP scope 192.168.100.100-150, Windows Deployment Services**
Master (VM, LAN)	**Reference Windows 10 Pro installation - customised once, generalized, captured**
NEW (VM, LAN, PXE)	**Target endpoint - 1 GB RAM, 20 GB HD, Legacy Network Adapter, receives the image**
C:\Images on DC1	**Working folder for .WIM files, shared as \\DC1\Images (folder name chosen for this lab)**
install.wim / boot.wim	**Install image = the operating system; Boot image = Windows PE that PXE clients start first**

Property of Ben Halevy

Mission Parameters
IMAGE DEPLOYMENT

TASK – STEP 1: PREPARE THE REFERENCE VM "MASTER"
Create VM Master: Hyper-V Generation 1, 2 GB RAM, 40 GB HD, LAN switch
Install Windows 10 Pro and everything every endpoint must receive
Customise in Audit mode, so no personal user profile ends up in the image
Checkpoint the VM before Sysprep, so the reference can be reused

COMMANDS - MASTER (elevated CMD)

```
REM At the first OOBE screen press  Ctrl + Shift + F3
REM Windows restarts in Audit mode (built-in Administrator)

REM Install updates, drivers, 7-Zip, settings ... then
REM check the component store before capturing:
Dism /Online /Cleanup-Image /ScanHealth

REM Optional - shrink the component store (permanent):
Dism /Online /Cleanup-Image /StartComponentCleanup /ResetBase
```

How To Instructions
Hyper-V Manager > New > Virtual Machine > Name: Master > Generation 1 > 2048 MB > Connection: LAN > 40 GB VHDX > Install from ISO
Windows Setup > Windows 10 Pro > at the region / OOBE screen press Ctrl+Shift+F3 > the PC reboots into Audit mode, the Sysprep window opens - leave it open
Install Windows updates, drivers and the applications the organization uses (e.g. 7-Zip) > apply desktop / system settings
Do NOT install or update Microsoft Store apps before generalizing - Sysprep will fail
After /ResetBase, installed updates can no longer be uninstalled > Hyper-V > Master > Checkpoint before moving to Step 2

Property of Ben Halevy

Mission Parameters
IMAGE DEPLOYMENT

TASK – STEP 2: GENERALIZE MASTER WITH SYSPREP
Remove every machine-unique value so one image can serve many PCs
Sysprep resets the SID, clears restore points and deletes event logs
The VM must shut down - its next boot is into Windows PE for capture
Generalize even when the target hardware is identical

COMMANDS - MASTER (elevated CMD)

```
cd /d %WINDIR%\System32\Sysprep

sysprep.exe /generalize /oobe /shutdown

REM Syntax:
REM Sysprep.exe [/oobe | /audit] [/generalize] [/mode:vm]
REM   [/reboot | /shutdown | /quit] [/quiet]
REM   [/unattend:<answerfile>]

REM /mode:vm = only when the VHD stays on the same
REM hypervisor - not used here (image goes to WDS)
```

How To Instructions
GUI alternative: System Cleanup Action = Enter System Out-of-Box Experience (OOBE) > tick Generalize > Shutdown Options = Shutdown > OK
/generalize - prepares the installation to be imaged: removes unique system information (SID reset, restore points, event logs)
/oobe - the next start runs the Out-Of-Box Experience (region, keyboard, user) on each new endpoint
/shutdown - powers the VM off when finished. Do not start Master into Windows now - boot it into Windows PE for the capture (Step 4)
Sysprep can be run up to 1001 times on one image (Windows 8.1 / Server 2012 and later) - after that the image must be recreated

Property of Ben Halevy

Mission Parameters
IMAGE DEPLOYMENT

TASK – STEP 3: PREPARE WDS ON DC1 FOR PXE
DHCP and WDS share DC1: WDS must not take DHCP port 67
DHCP option 60 tells PXE clients that a PXE server exists
Boot image (boot.wim) already added on slide 95 - verify it
Optional: a Capture boot image for the graphical capture wizard

COMMANDS - DC1 (elevated CMD)

```
REM DHCP + WDS on the same server:
wdsutil /Set-Server /UseDhcpPorts:No /DhcpOption60:Yes

REM Answer every PXE client (no prestaging):
wdsutil /Set-Server /AnswerClients:All

REM Optional capture image from the existing boot image:
wdsutil /New-CaptureImage /Image:"Microsoft Windows Setup (x64)"
   /Architecture:x64 /DestinationImage /FilePath:C:
   \Images\Capture.wim /Name:"Capture (x64)"
wdsutil /Add-Image /ImageFile:C:\Images\Capture.wim /ImageType:Boot
```

How To Instructions
Create C:\Images on DC1 > Properties > Sharing > share as \\DC1\Images > give Domain Admins Change permission (this is where Step 4 saves the .WIM)
Server Manager > Tools > Windows Deployment Services > DC1 > Properties > PXE Response > Respond to all client computers
DHCP tab: tick "Do not listen on DHCP ports" and "Configure DHCP options for PXE" (same as the wdsutil line above)
Boot Images > right-click Microsoft Windows Setup (x64) > Create Capture Image > name + local path > Finish > right-click Boot Images > Add Boot Image > select it
The capture image starts the WDS Image Capture Wizard (graphical). Step 4 shows the same capture done manually with DISM

Property of Ben Halevy

Mission Parameters
IMAGE DEPLOYMENT

TASK – STEP 4: CAPTURE THE IMAGE WITH DISM
PXE-boot the generalized Master into Windows PE (never into Windows)
Find the Windows volume - drive letters change inside Windows PE
Capture the Windows volume into a compressed .WIM on \ \DC1\Images
Verify the captured image before it is deployed

COMMANDS - MASTER (Windows PE command prompt)

```
diskpart
  list volume      REM note the Windows volume, e.g. D:
  exit
net use Z: \\DC1\Images /user:BEN\Administrator

REM Optional - faster first boot after deployment:
Dism /Image:D:\ /Optimize-Image /Boot

Dism /Capture-Image /ImageFile:Z:\Win10-Master.wim /CaptureDir:D:\
   /Name:"Win10 Pro - BEN.LOCAL" /Compress:max /CheckIntegrity

Dism /Get-ImageInfo /ImageFile:Z:\Win10-Master.wim
```

How To Instructions
Master > Settings > Add Hardware > Legacy Network Adapter (LAN) > BIOS: move Legacy Network Adapter to the top of the startup order
Start Master > press F12 when prompted > choose Microsoft Windows Setup (x64) > on the first Setup screen press Shift+F10 to open a command prompt
Run the commands on the right: diskpart finds the volume, net use maps the share on DC1, Dism /Capture-Image writes the .WIM
/CaptureDir = volume to capture /Name = image name /Compress:max = smallest file /CheckIntegrity = detect .WIM corruption
Dism /Get-ImageInfo shows Index 1 with the name, size and Windows edition - the image is ready. wpeutil shutdown turns Master off

Property of Ben Halevy

Mission Parameters
IMAGE DEPLOYMENT

TASK – STEP 5: SERVICE THE IMAGE OFFLINE WITH DISM
Update the image once - instead of every endpoint after deployment
Mount the .WIM to a folder, add drivers / updates, check features
Commit the changes, then Export to a clean, compact install.wim
Use /Discard instead of /Commit to throw away a bad change

COMMANDS - DC1 (elevated CMD)

```
md C:\Mount
Dism /Mount-Image /ImageFile:C:\Images\Win10-Master.wim /Index:1
   /MountDir:C:\Mount

Dism /Image:C:\Mount /Add-Driver /Driver:C:\Drivers /Recurse
Dism /Image:C:\Mount /Add-Package /PackagePath:C:\Updates\update.cab
Dism /Image:C:\Mount /Get-Features

Dism /Unmount-Image /MountDir:C:\Mount /Commit

Dism /Export-Image /SourceImageFile:C:\Images\Win10-Master.wim
   /SourceIndex:1 /DestinationImageFile:C:\Images\install.wim
   /Compress:max
```

How To Instructions
Mount - the image is opened read/write in C:\Mount and can be changed like a normal folder tree
Add-Driver /Recurse adds every .inf driver in C:\Drivers and its sub-folders - handy, but it can bloat the image, so keep the folder clean
Add-Package installs a .cab update into the offline image; Get-Features lists Windows features and their state
Unmount /Commit saves the changes into the .WIM (Dism /Commit-Image saves without unmounting)
Export-Image copies index 1 into a new install.wim with maximum compression - this is the file imported into WDS in Step 6

Property of Ben Halevy

Mission Parameters
IMAGE DEPLOYMENT

TASK – STEP 6: IMPORT THE GOLDEN IMAGE INTO WDS
Install images are stored in image groups on the WDS server
Create a group for the organization and import install.wim
Give the image a clear name - it is what the technician picks
Confirm the image is listed and online

COMMANDS - DC1 (PowerShell as Administrator)

```
New-WdsInstallImageGroup -Name "BEN Win10"

Import-WdsInstallImage -Path "C:\Images\install.wim" -ImageGroup "BEN
   Win10" -NewImageName "Windows 10 Pro - BEN.LOCAL"

Get-WdsInstallImage

# If only one image group exists, -ImageGroup
# may be omitted - WDS uses that group by default
```

How To Instructions
GUI: Windows Deployment Services > DC1 > right-click Install Images > Add Image Group > Name: BEN Win10
Right-click BEN Win10 > Add Install Image > Browse > C:\Images\install.wim > Next > tick the image > Next > Finish
The image now appears under Install Images > BEN Win10 with Status: Online
Boot Images keeps Microsoft Windows Setup (x64) - this is the Windows PE that every PXE client loads first

Property of Ben Halevy

Mission Parameters
IMAGE DEPLOYMENT

TASK – STEP 7: DEPLOY TO VM "NEW" OVER PXE
NEW: 1 GB RAM, 20 GB HD, LAN, Legacy Network Adapter (PXE)
PXE boot > Windows PE > pick the golden image > install
The endpoint receives the exact same pre-built system
Join BEN.LOCAL - the GPOs from the earlier tasks then apply

VERIFY - NEW (CMD after first sign-in)

```
systeminfo | findstr /B /C:"OS Name" /C:"Domain"

REM After joining BEN.LOCAL and restarting:
gpupdate /force
gpresult /r

REM DC1 - confirm the computer account:
REM AD Users and Computers > Computers > NEW
```

How To Instructions
Hyper-V > NEW > Settings > remove the standard Network Adapter > Add Hardware > Legacy Network Adapter > LAN > BIOS: Legacy Network Adapter first
Start NEW > it receives an address from DHCP on DC1 > press F12 for network boot > Windows Boot Manager > Microsoft Windows Setup (x64)
Enter BEN\Administrator credentials > select Windows 10 Pro - BEN.LOCAL > choose the 20 GB disk > Windows installs from \\DC1 over the network
OOBE completes > join the domain: System > Rename this PC (advanced) > Change > Domain: BEN.LOCAL > restart
Repeat for any number of endpoints - every new PC receives the identical, already-patched system

Property of Ben Halevy

Mission Parameters
BEN.LOCAL BUILD MAP

MACHINE	SPECIFICATION	IP ADDRESS	ROLES & SERVICES
DC1	Windows Server 2019, 4 GB / 40 GB	192.168.100.1	AD DS forest BEN.LOCAL, DNS (forwarder 8.8.8.8), DHCP, WDS, FSRM, shares Home Z: / Reports Y: / Secret S:, print server
DC2	Windows Server, 2 GB / 40 GB	192.168.100.2	Additional domain controller, RID pool manager, iSCSI initiator - spanned volume E: (10 GB)
RAS	Windows Server 2016, 2 GB / 40 GB	LAN 192.168.100.254 WAN 192.168.200.1	Routing & Remote Access - VPN (PPTP, 7 ports) for Management, iSCSI target (2 x 5 GB)
IS1 / IS2	2 GB / 30 GB each	192.168.100.3 / .4	IIS web servers, NLB cluster 192.168.100.10 (multicast, TCP 80) - www.site.com
CL1	Windows 10 Pro, 2 GB / 40 GB	DHCP (100-150)	Domain client in the IT OU - test endpoint for every GPO
PC1	Windows 10, 1 GB / 30 GB	192.168.200.10 (WAN)	Remote user - VPN client to RAS
Print1 / Print2	TCP/IP printers	192.168.100.50 / .51	Print1 > Finance & Office, Print2 > Sales & Architects (deployed by GPO)
Master / NEW	Windows 10 Pro VMs	DHCP (PXE)	Golden-image reference and PXE deployment target (WDS on DC1)
LAN / WAN	Hyper-V private switches	192.168.100.0/24 /	Internal network / simulated external network for the VPN
Organizational Units: Management, Office, Finance, Sales, Architects, IT - all policies on the previous slides are linked to these OUs			

Property of Ben Halevy

BEN.LOCAL

Special Thanks
My Cyber Teacher for always reminding me that there is always a way
If we have the patience to find it , it didn’t hurt that he always had a smile
One his face whenever he explained a new Feature or Protocol



Property of Ben Halevy