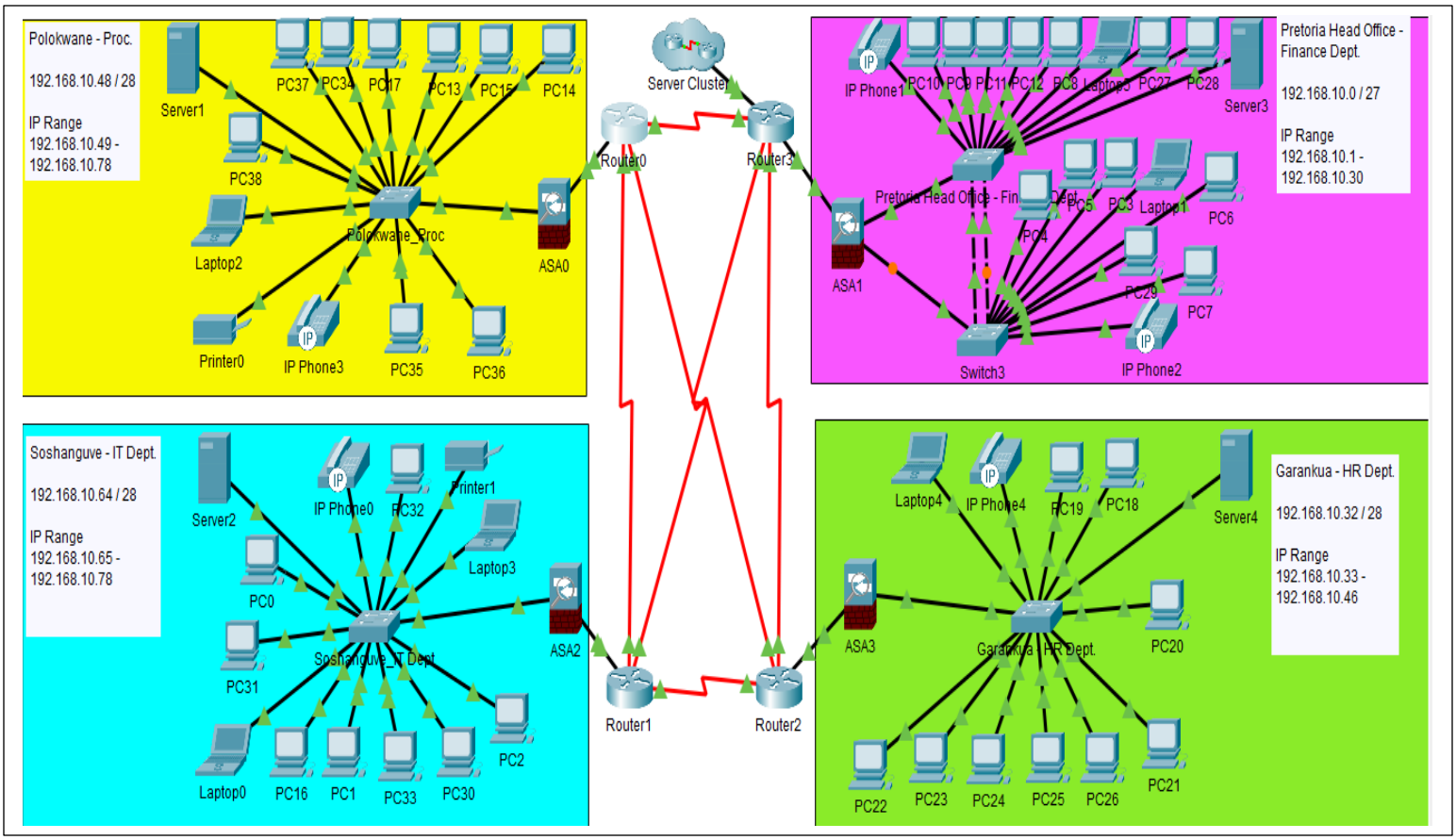
SYSTEM ADMINISTARTION AND MAINTAINANCE PROJECT

YEAR: 2025

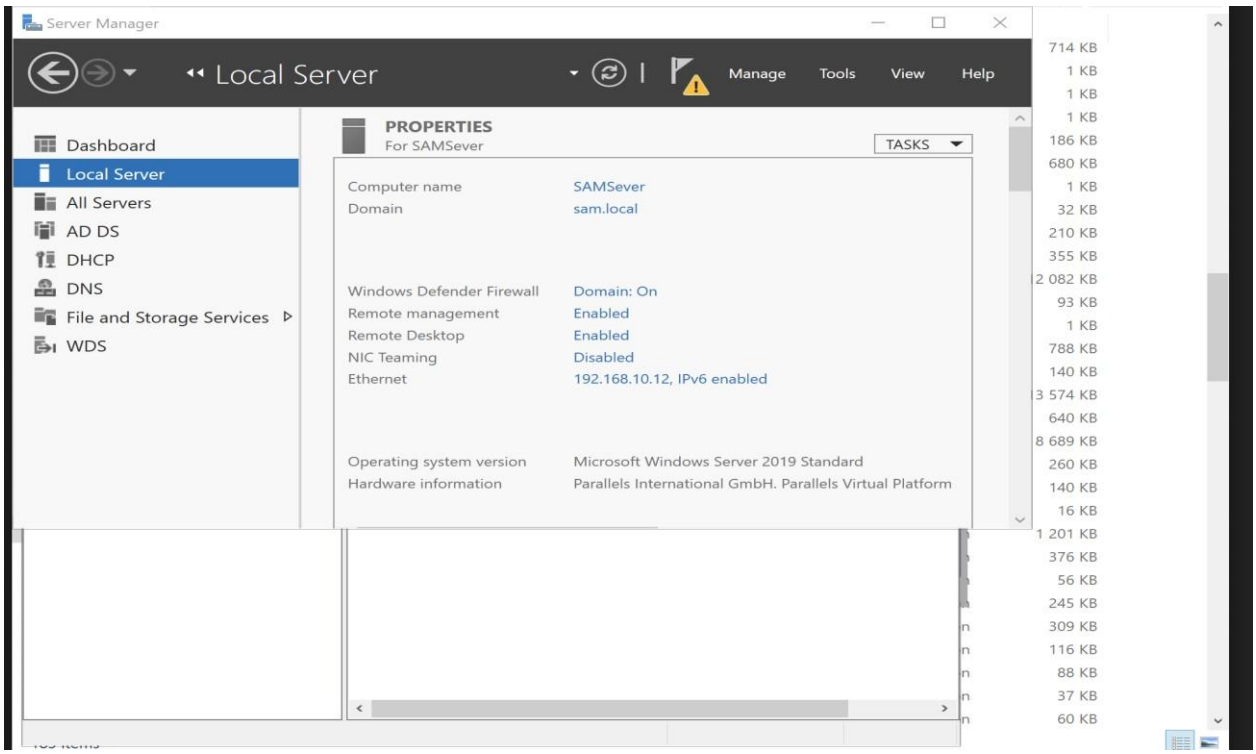
Table of Contents

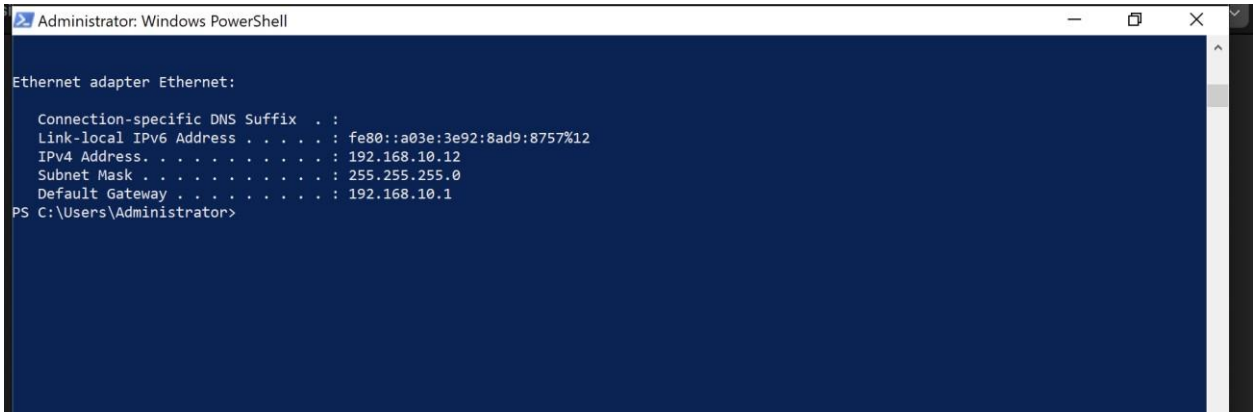
Company Network structure

The SAM Company operates its headquarters in Pretoria, along with three additional branches located in Soshanguve, Ga-rankuwa, and Polokwane. The organization is contracted to manage all the computers, servers, and internet connections within these offices. The primary server control hub is located in Pretoria. The network securely links all four branches. Every branch operates with its own systems, yet they all link to the main center in Pretoria. Our role is to ensure everything operates smoothly, remains linked, and is safeguarded against issues.

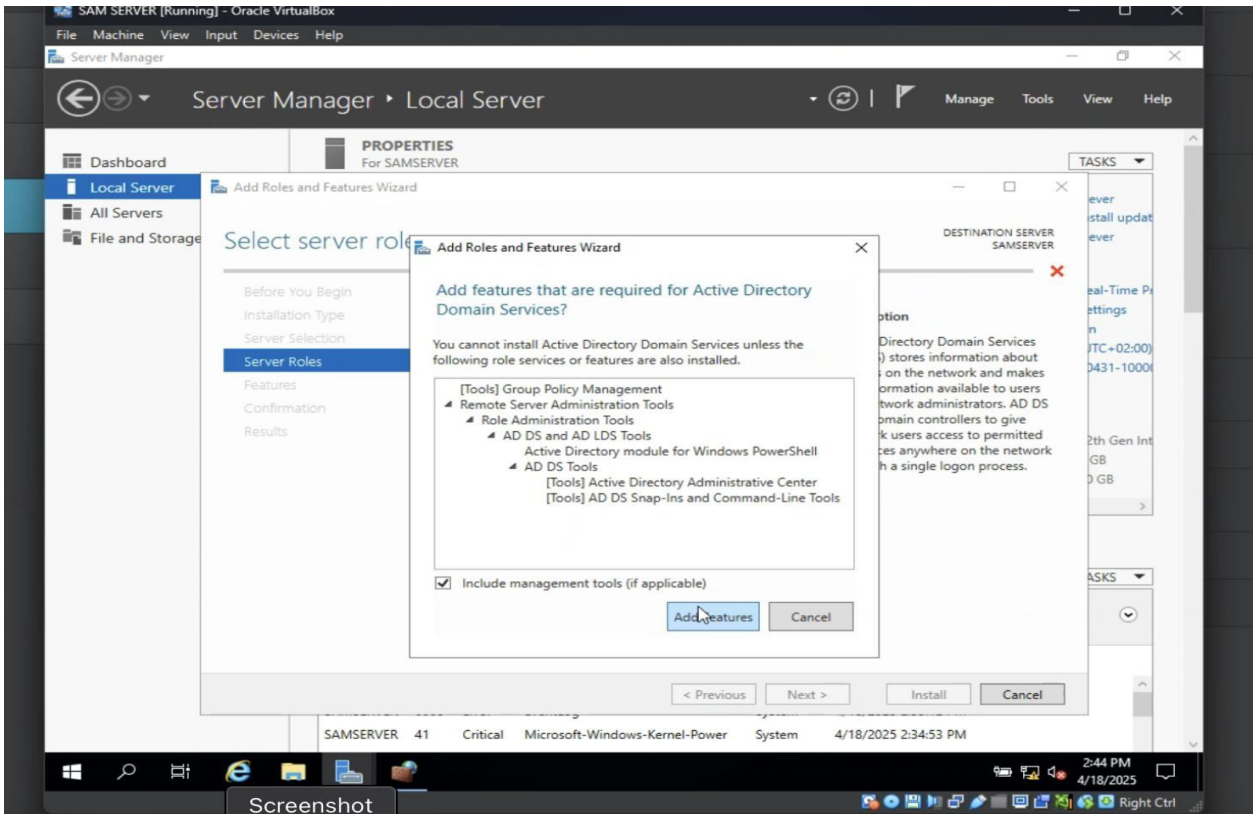


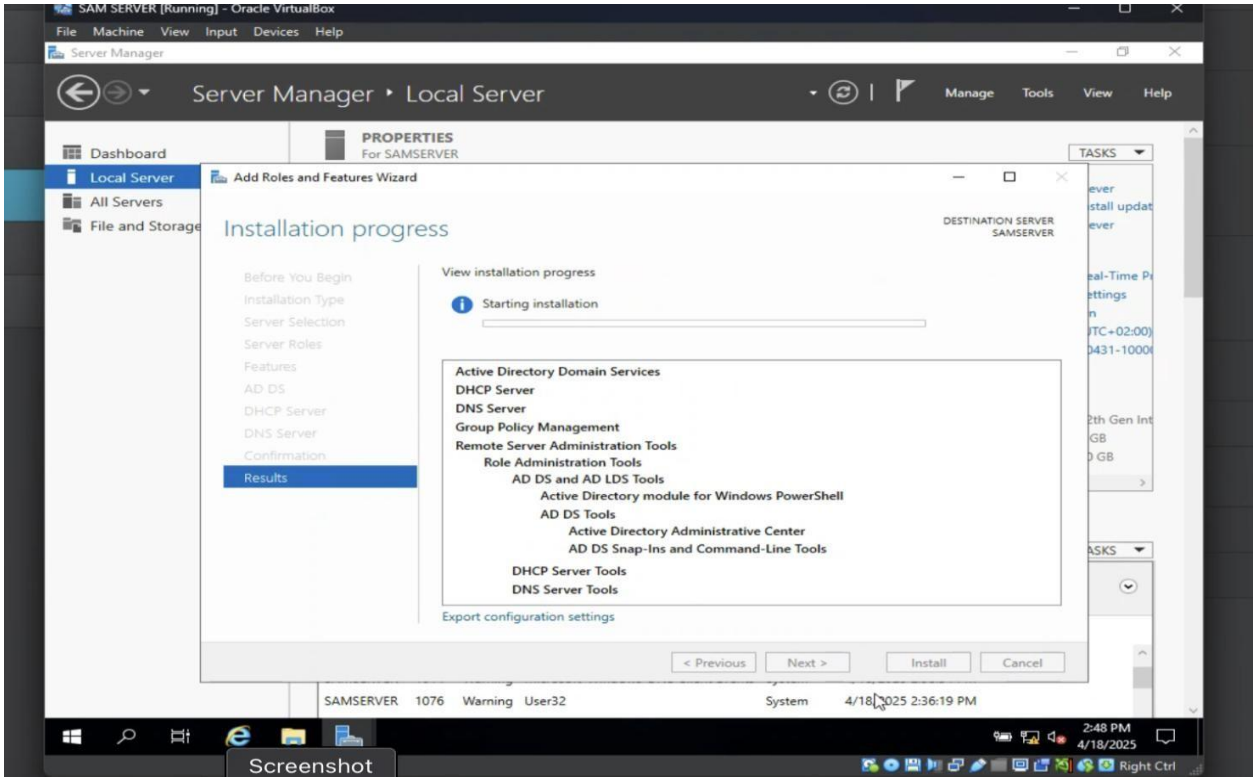
Setting IP for the Server



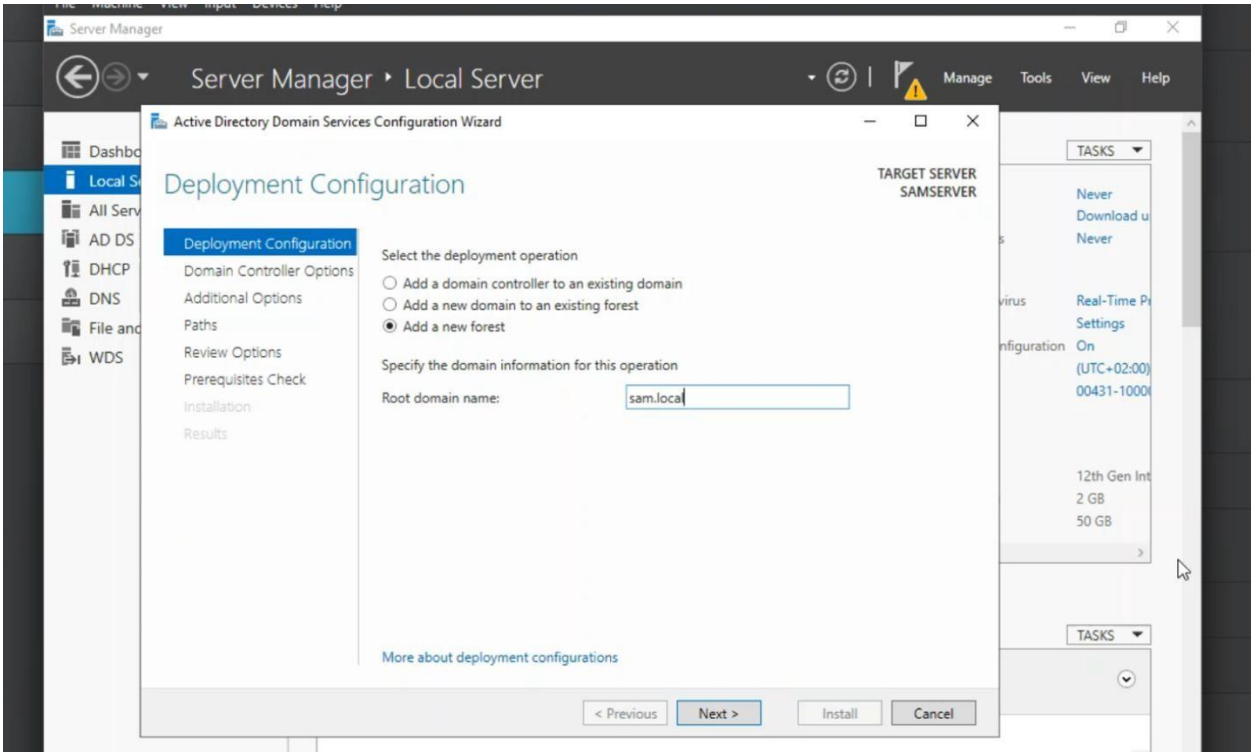


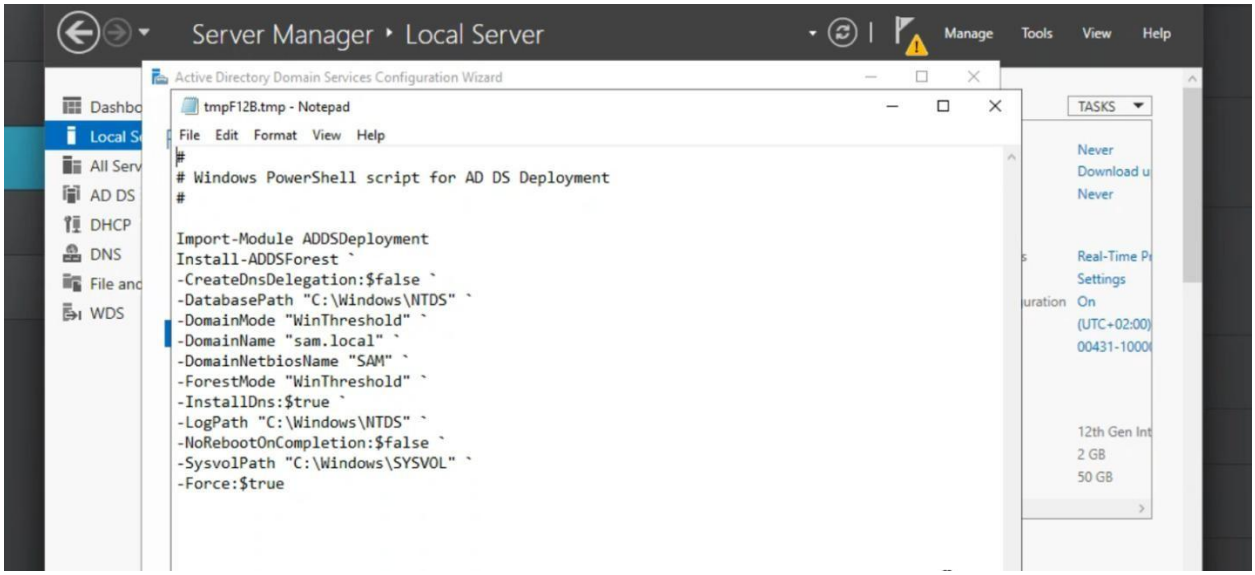
Adding Roles and Features



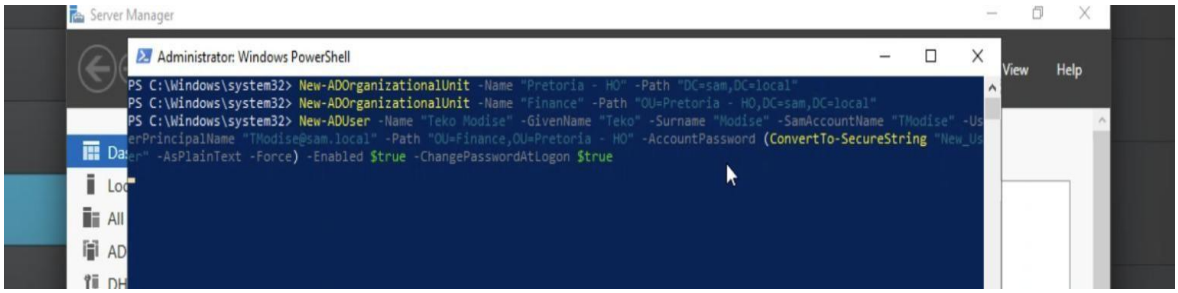


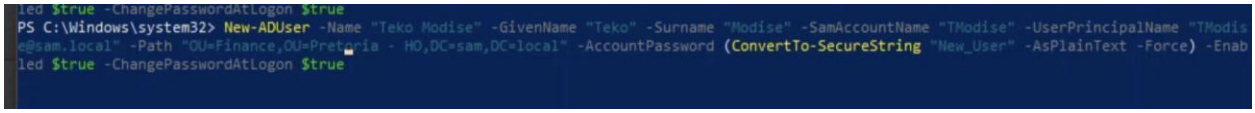
Setting Domain Name



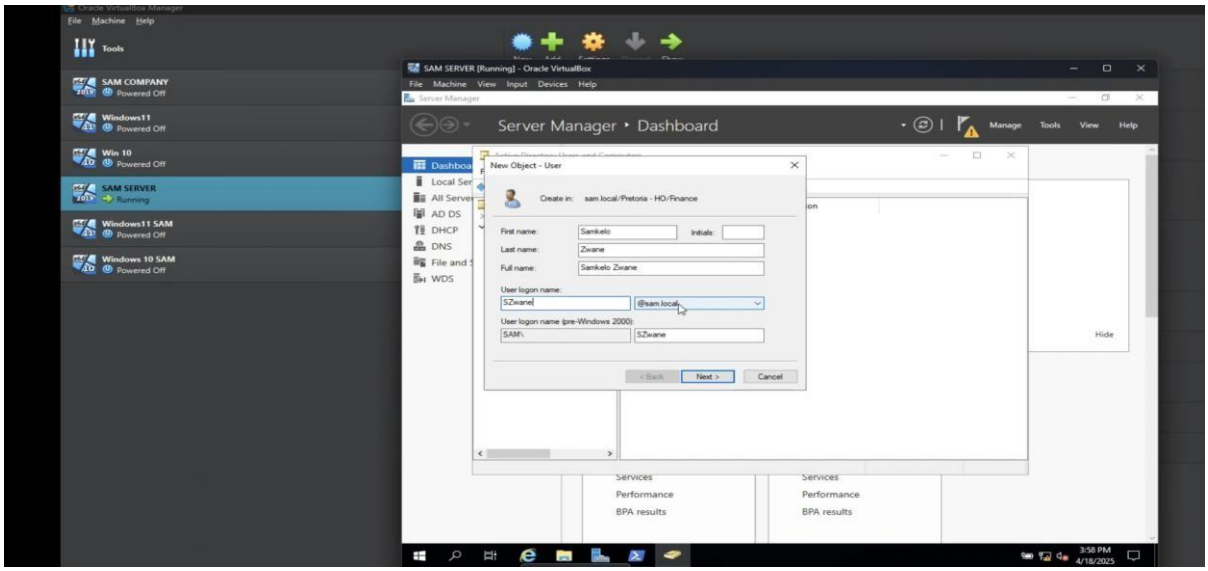


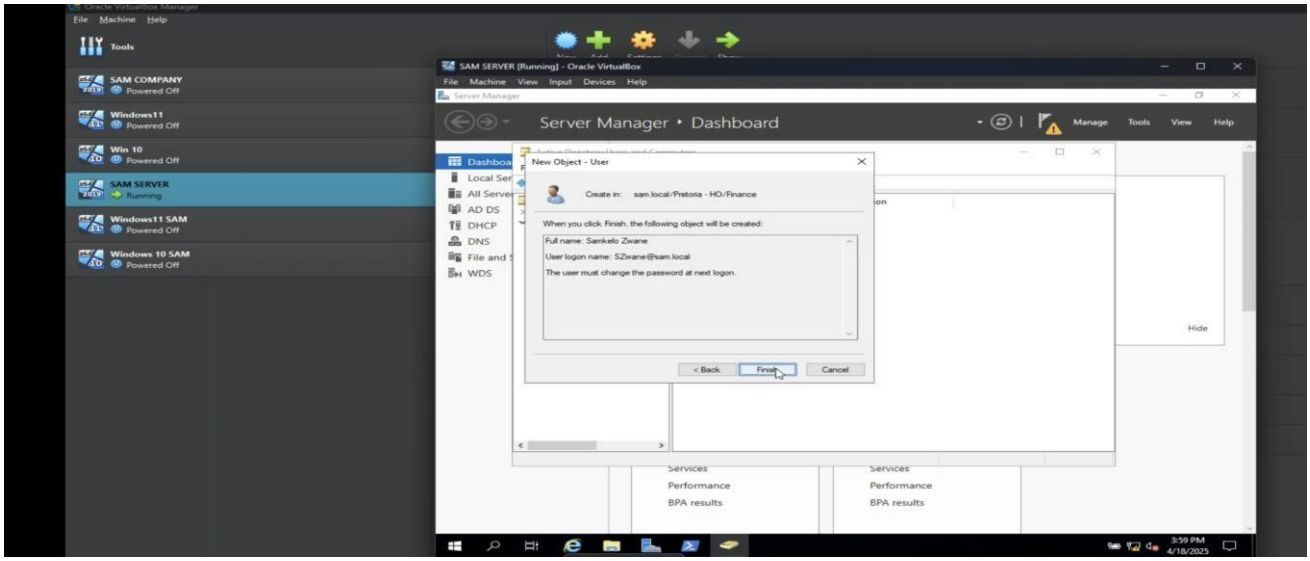
Creating Organizational Unit Using GUI

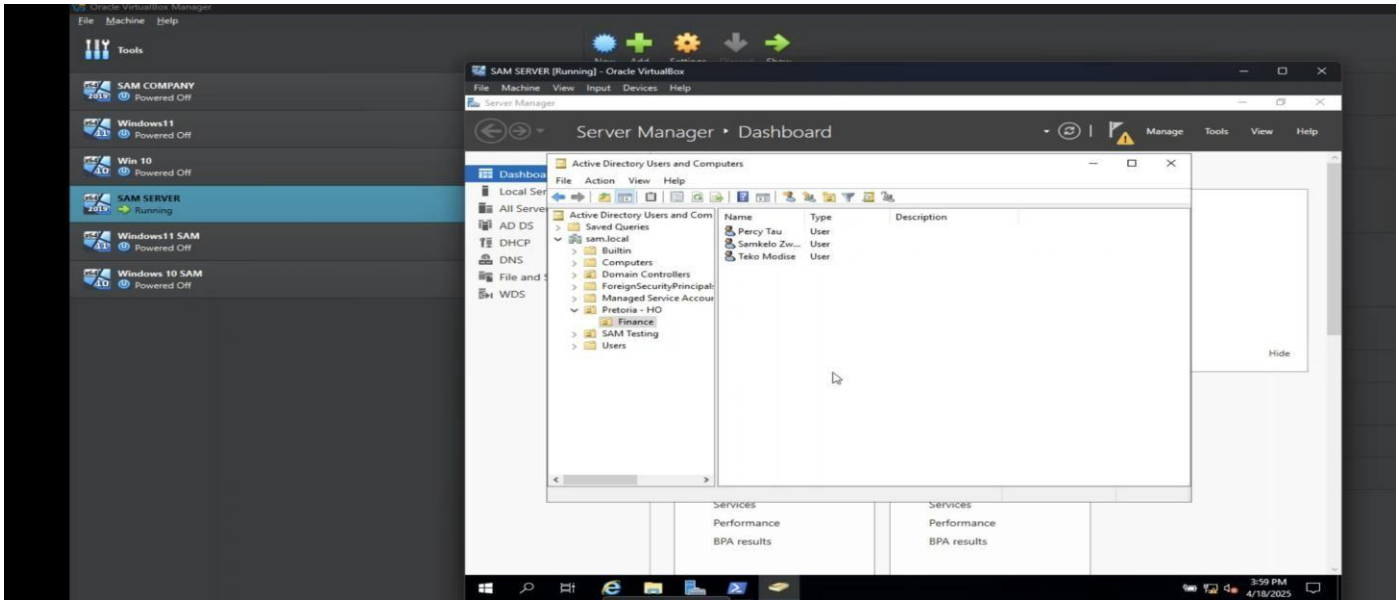




Creating new users

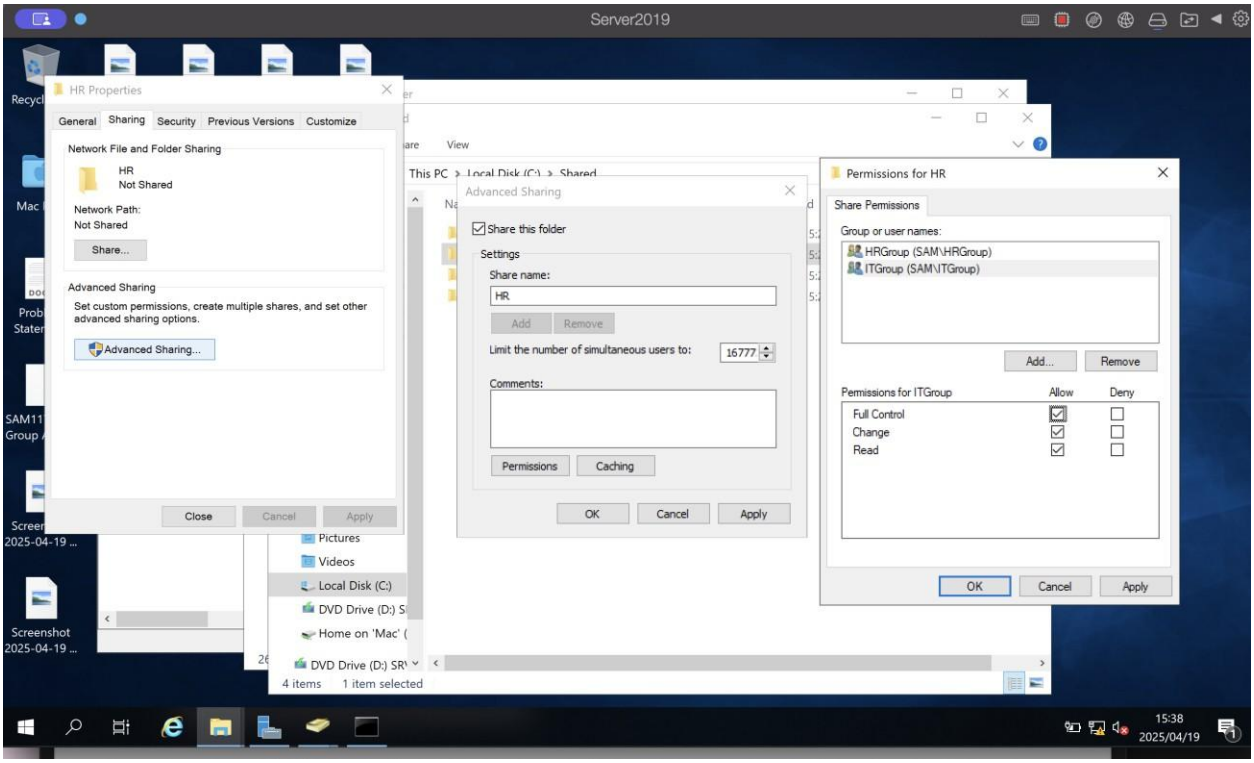




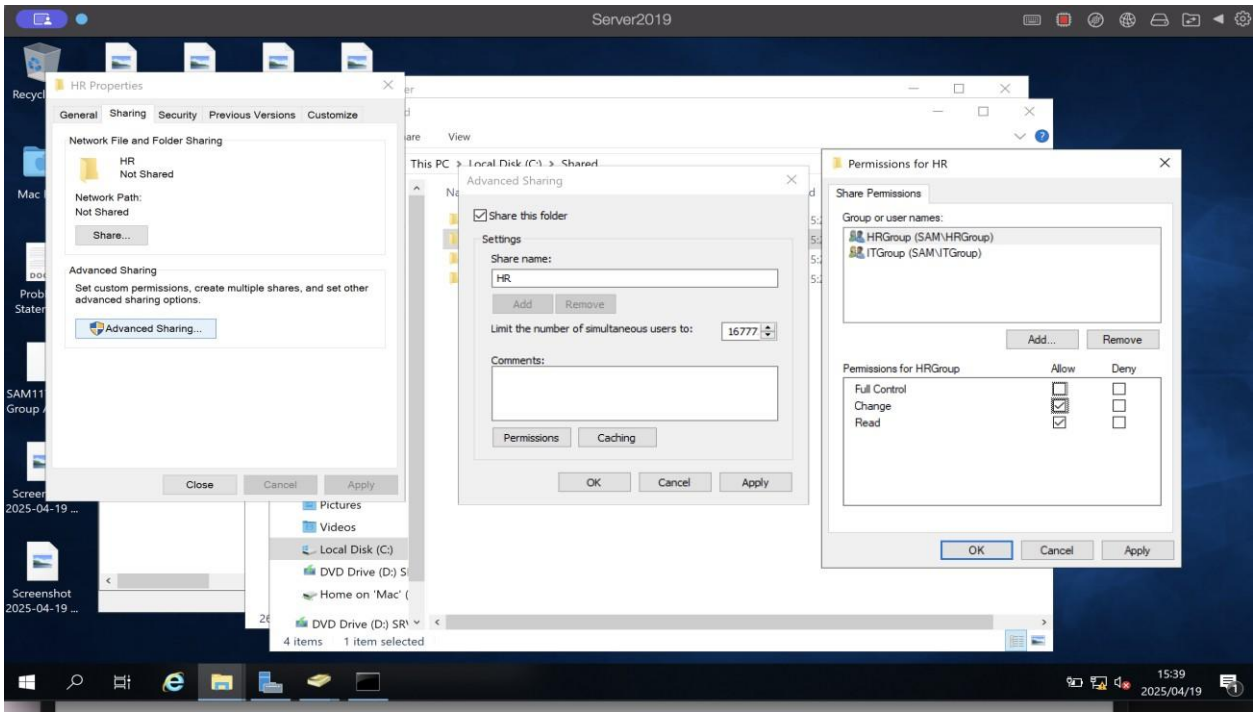


Shared Folder Access

IT Group permissions

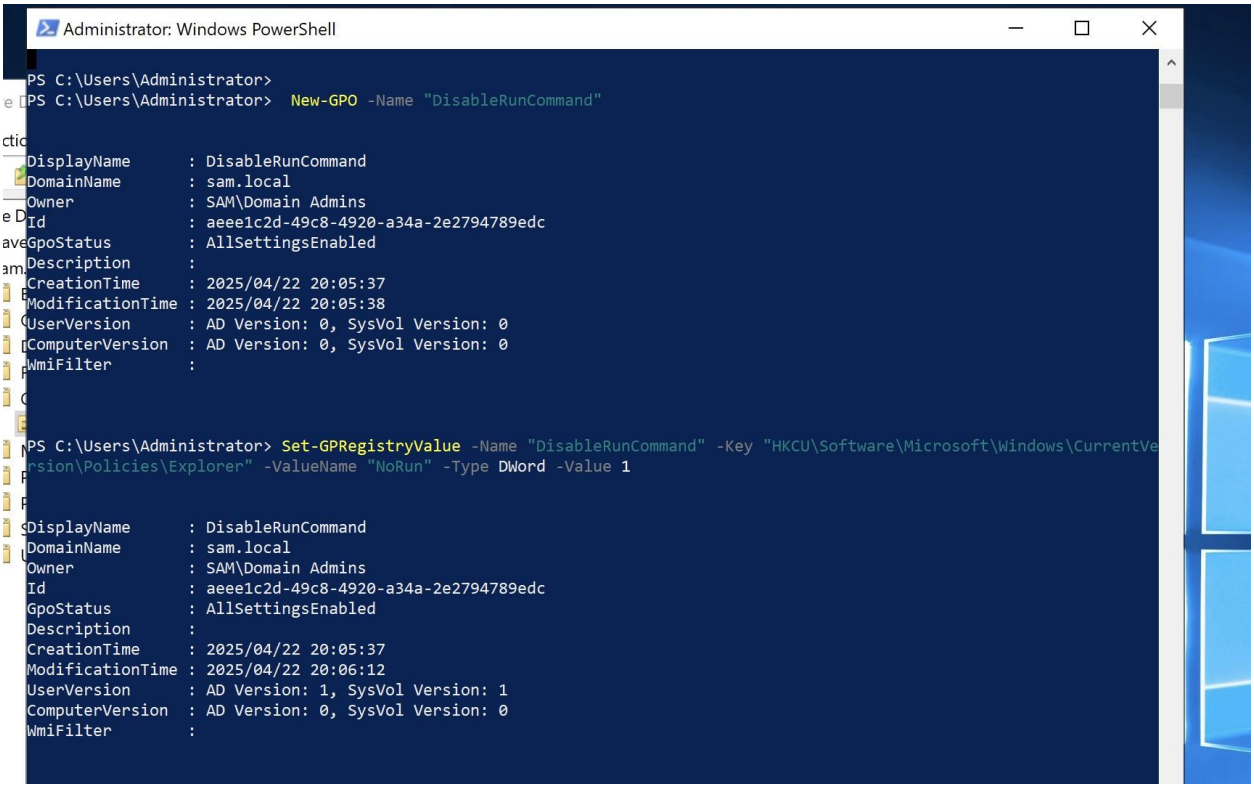


HR Permissions:

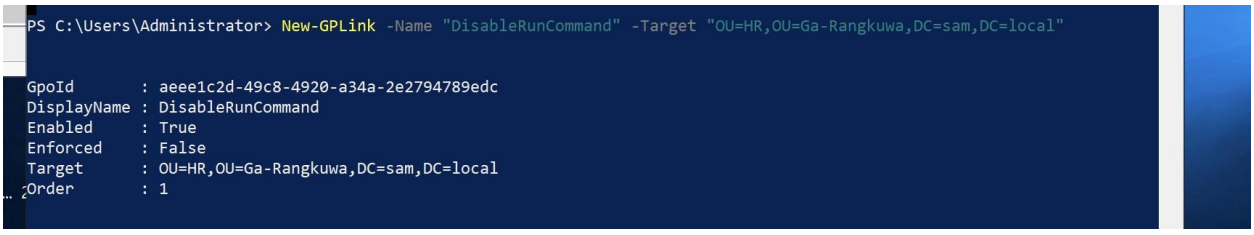


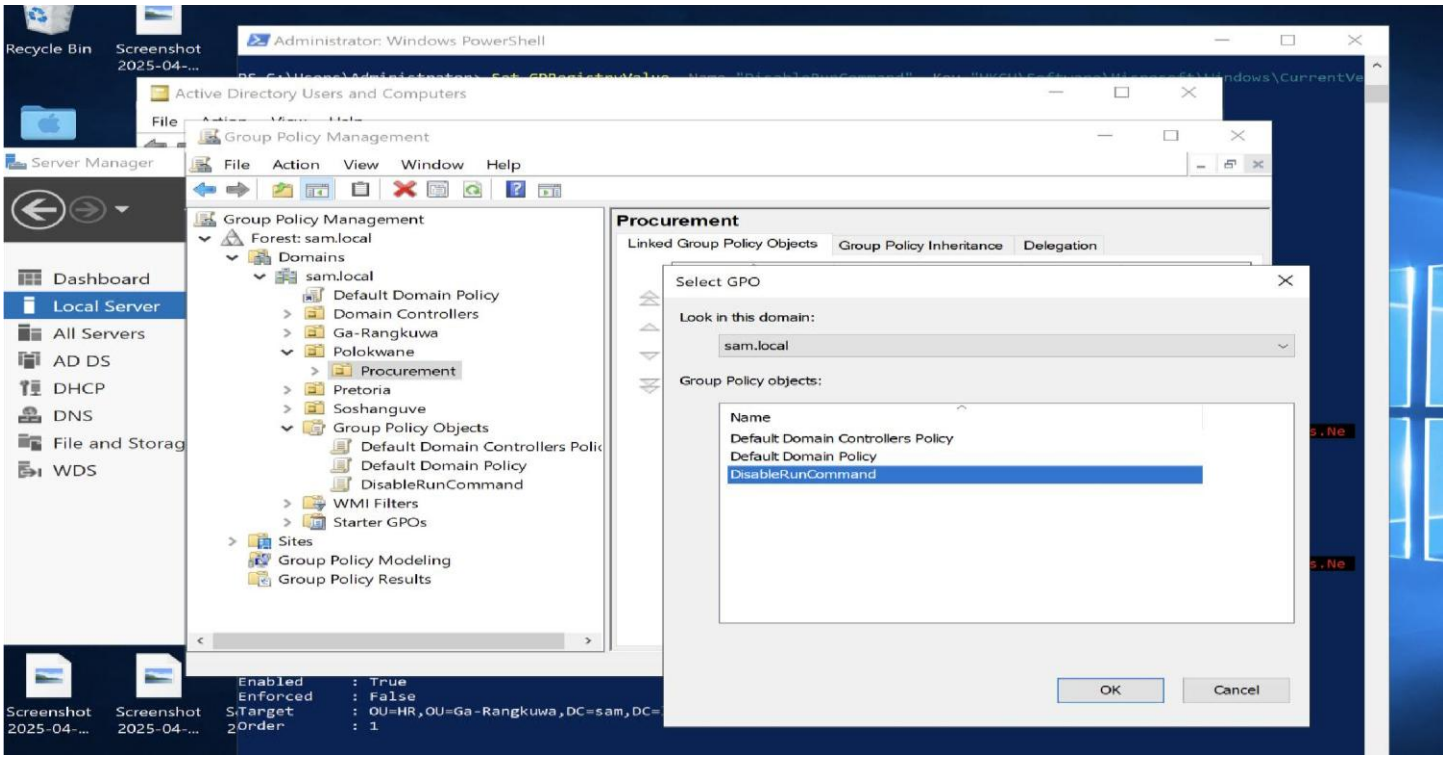
Disabling Run Function on HR, Finance and Procurement:

Creating GPO:

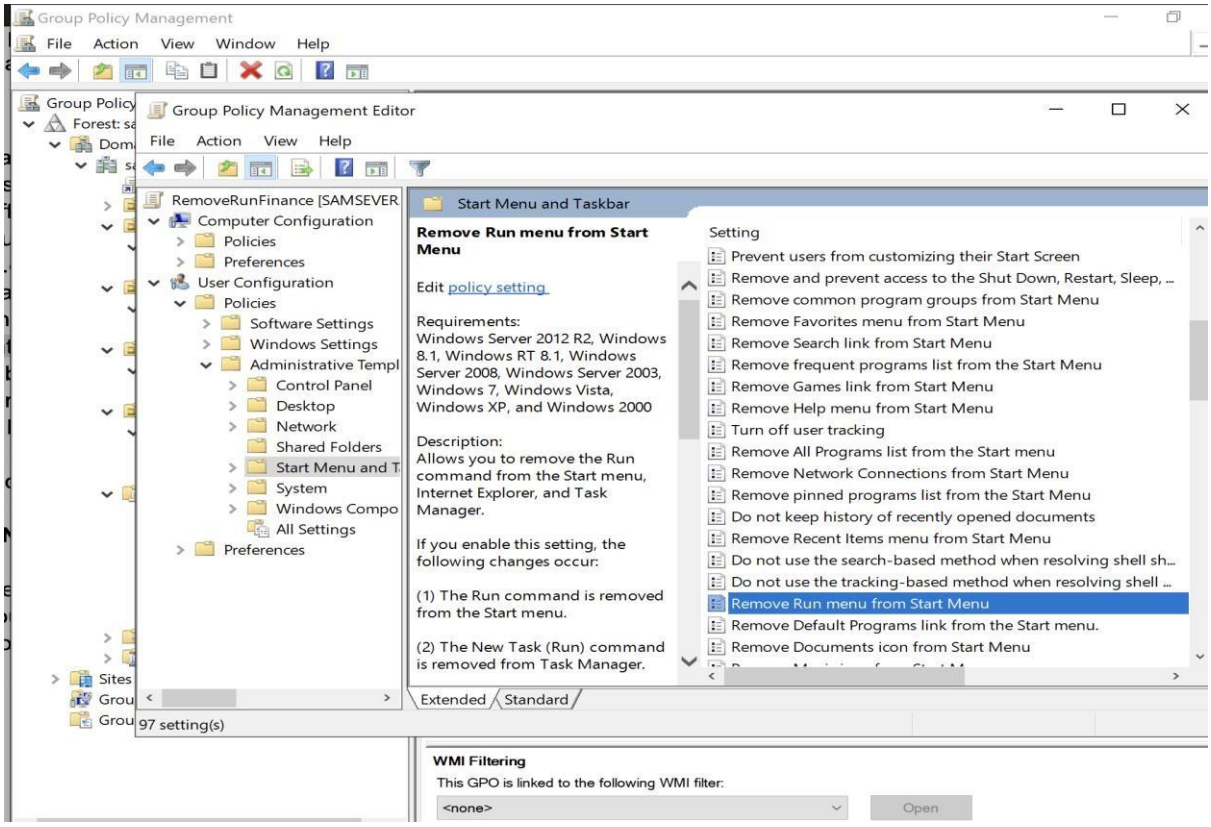


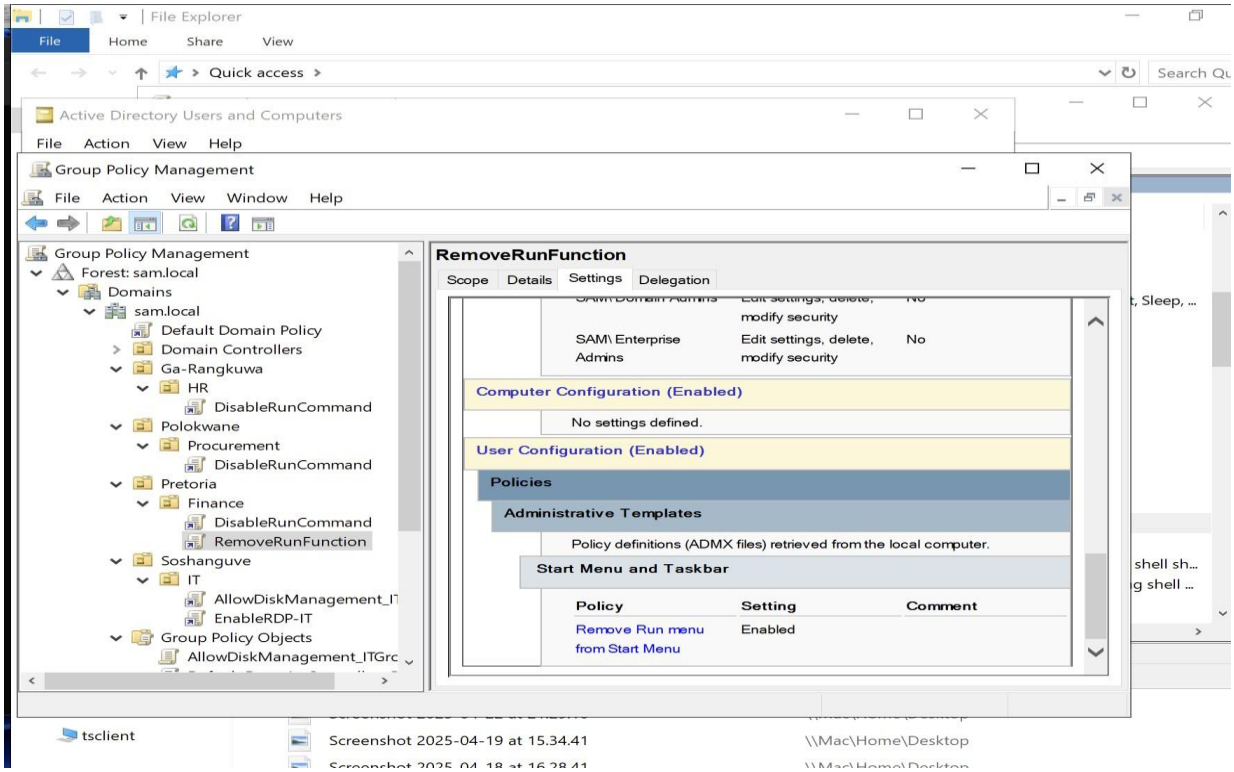
Linking GPO to the OU:



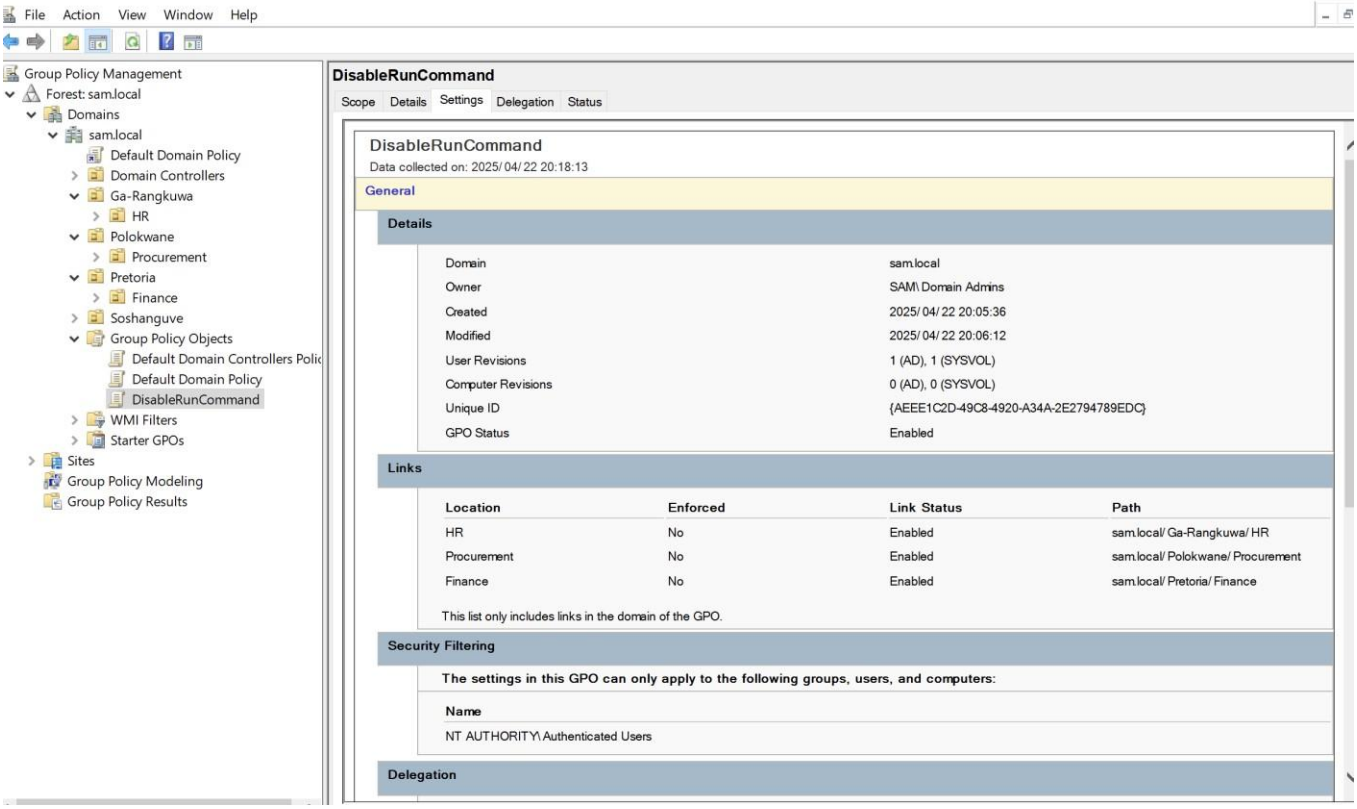

Recycle Bin
Screenshot 2025-04-...
Administrator: Windows PowerShell
Active Directory Users and Computers
Group Policy Management
File Action View Window Help
Server Manager
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storag
WDS
Group Policy Management
Forest: sam.local
Domains
sam.local
Default Domain Policy
Domain Controllers
Ga-Rangkuwa
Polokwane
Procurement
Pretoria
Soshanguve
Group Policy Objects
Default Domain Controllers Polic
Default Domain Policy
DisableRunCommand
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Procurement
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Select GPO
Look in this domain:
sam.local
Group Policy objects:
Name
Default Domain Controllers Policy
Default Domain Policy
DisableRunCommand
OK
Cancel
Enabled : True
Enforced : False
Target : OU=HR,OU=Ga-Rangkuwa,DC=sam,DC=
Order : 1

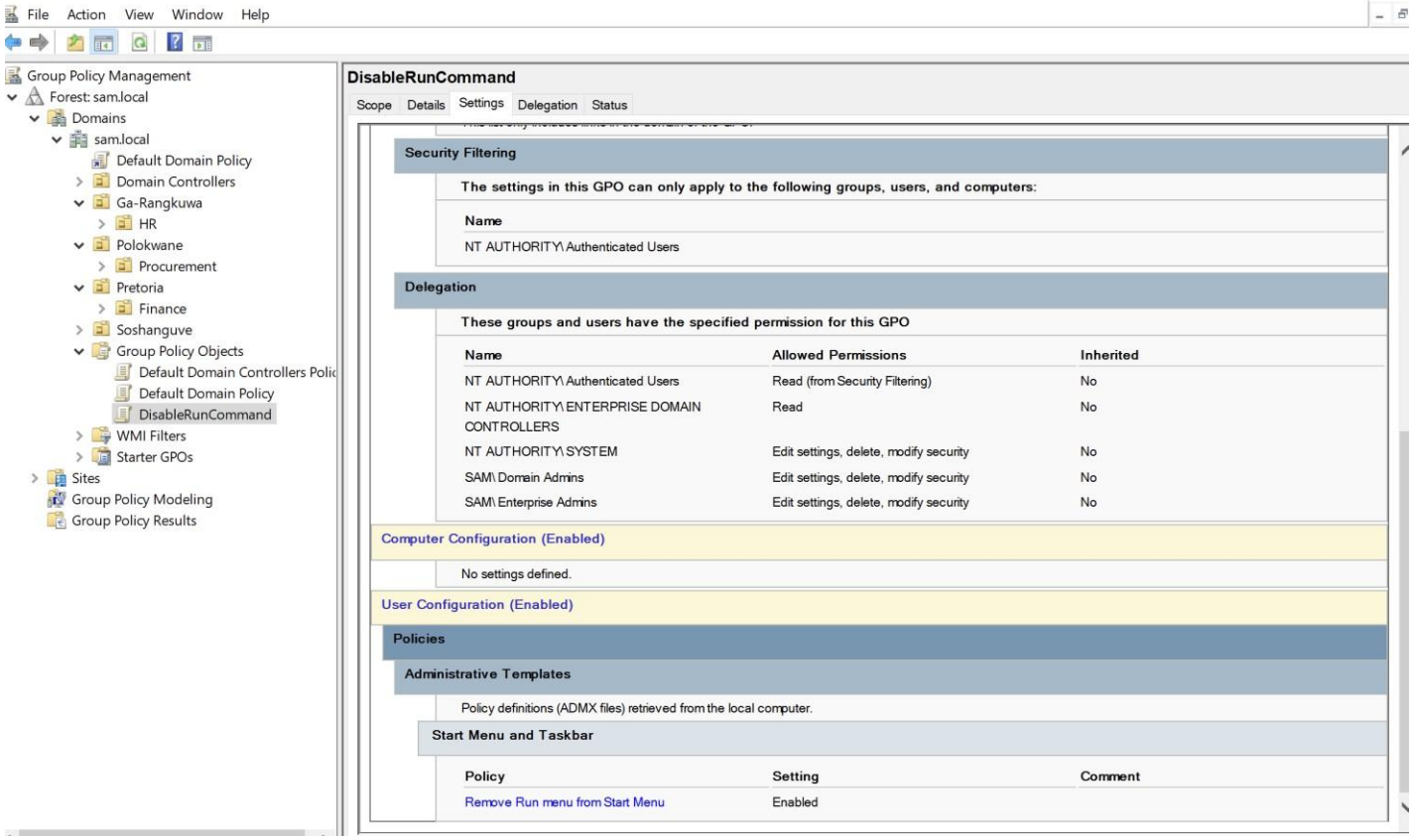
Remove Run from Finance:



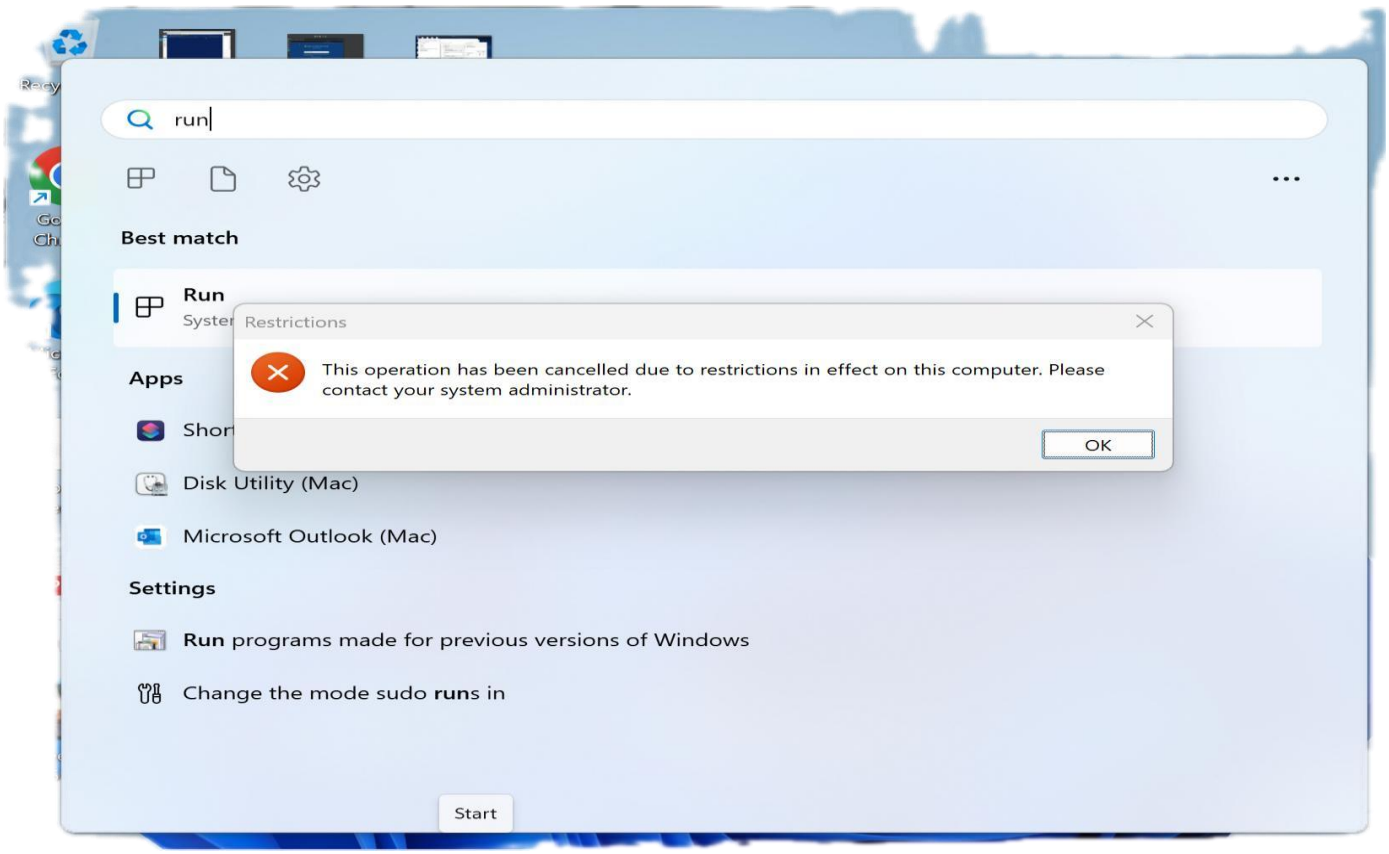


Disabling Run Function on HR and Procurement

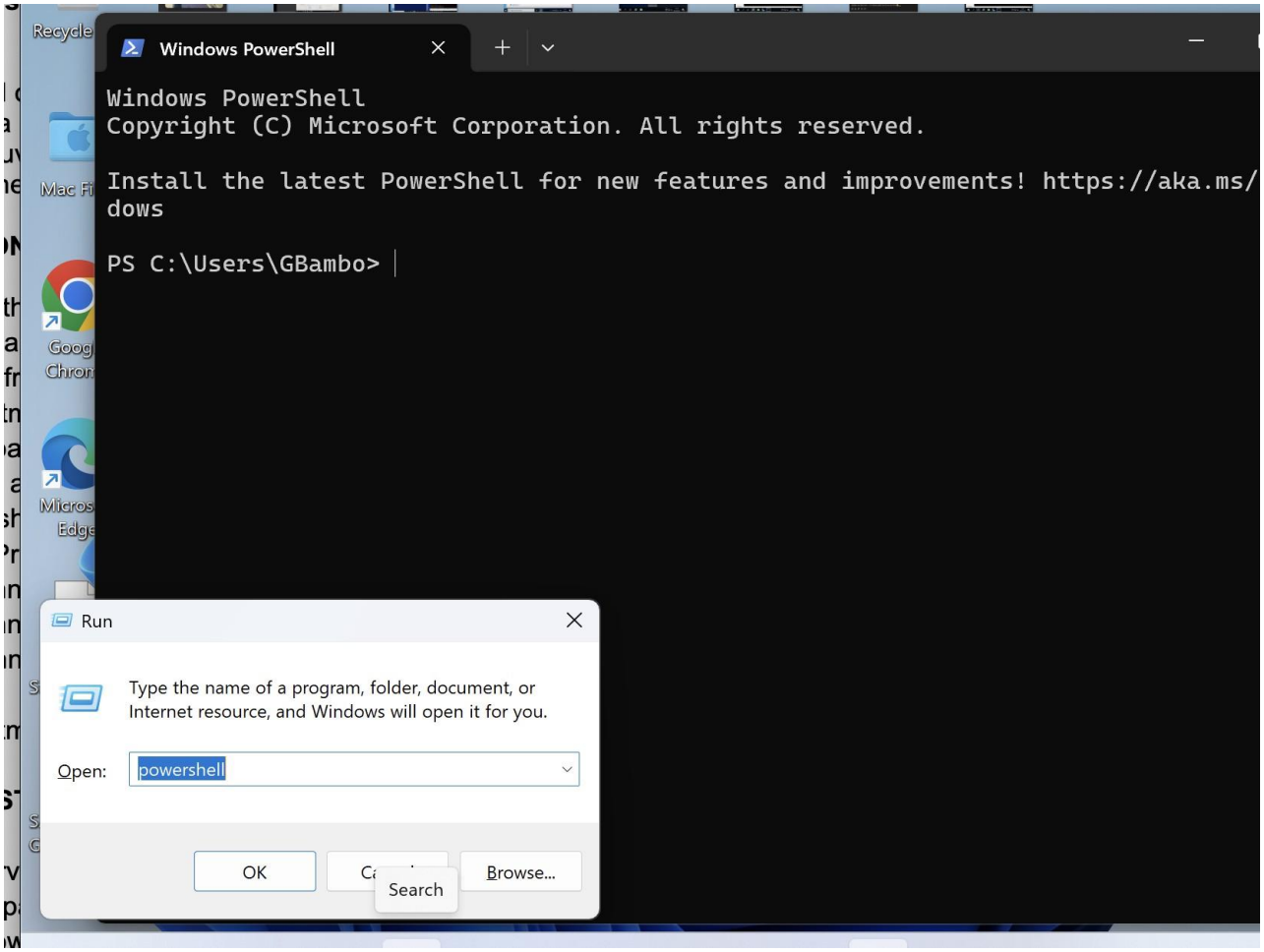



File Action View Window Help
Group Policy Management
Forest: sam.local
Domains
sam.local
Default Domain Policy
Domain Controllers
Ga-Rangkuwa
HR
Polokwane
Procurement
Pretoria
Finance
Soshanguve
Group Policy Objects
Default Domain Controllers Polic
Default Domain Policy
DisableRunCommand
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
DisableRunCommand
Scope Details Settings Delegation Status
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
NT AUTHORITY\ Authenticated Users
Delegation
These groups and users have the specified permission for this GPO
Name Allowed Permissions Inherited
NT AUTHORITY\ Authenticated Users Read (from Security Filtering) No
NT AUTHORITY\ ENTERPRISE DOMAIN CONTROLLERS Read No
NT AUTHORITY\ SYSTEM Edit settings, delete, modify security No
SAM\ Domain Admins Edit settings, delete, modify security No
SAM\ Enterprise Admins Edit settings, delete, modify security No
Computer Configuration (Enabled)
No settings defined.
User Configuration (Enabled)
Policies
Administrative Templates
Policy definitions (ADMX files) retrieved from the local computer.
Start Menu and Taskbar
Policy Setting Comment
Remove Run menu from Start Menu Enabled

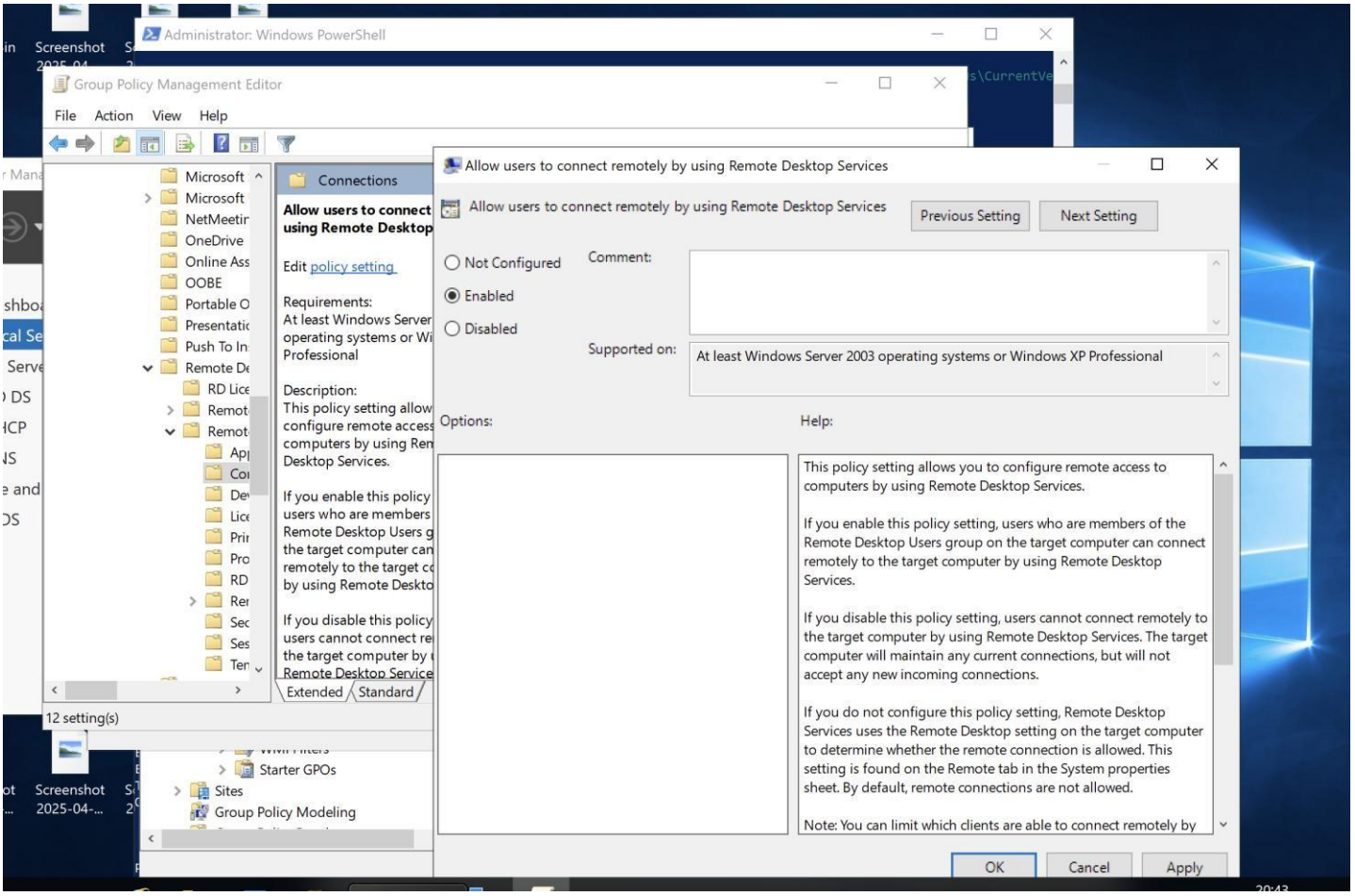
Testing Run Command



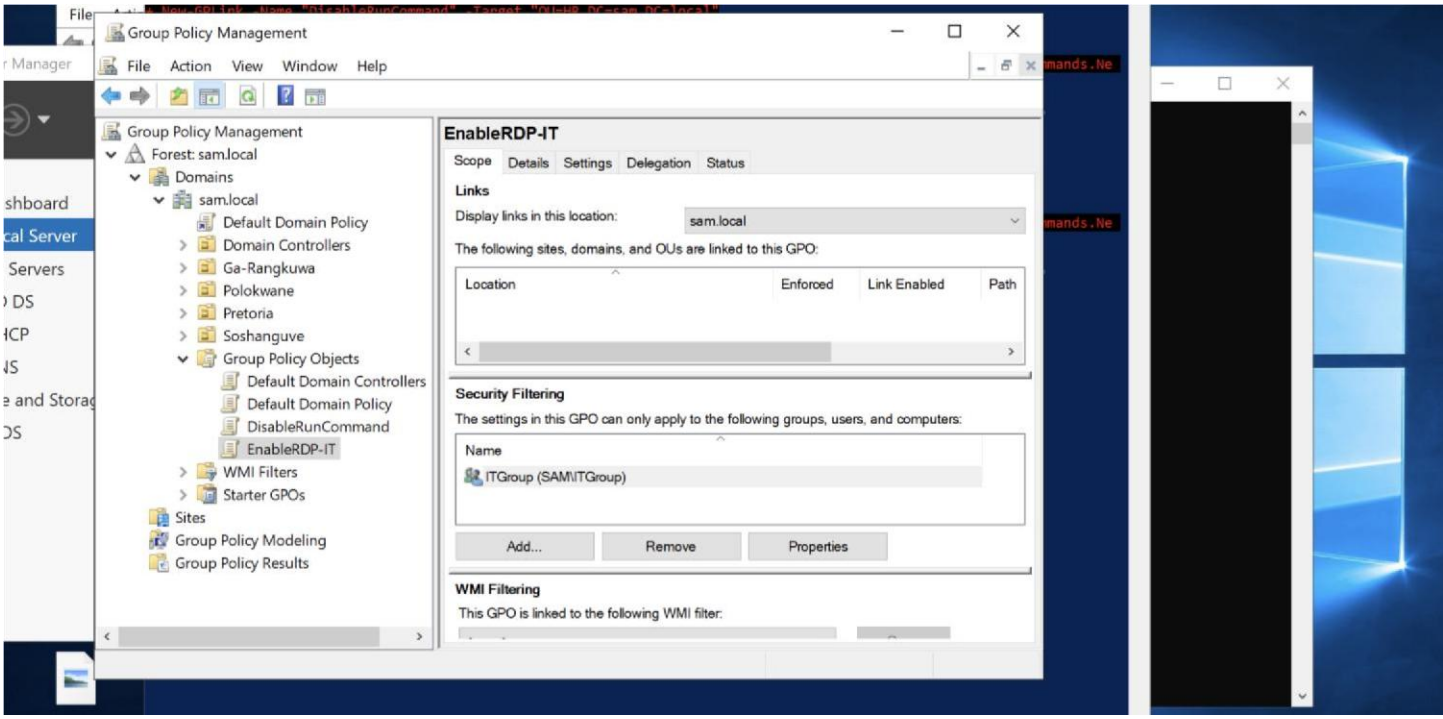
IT Personnel running Run Command, User was able to open PowerShell using the Run Function

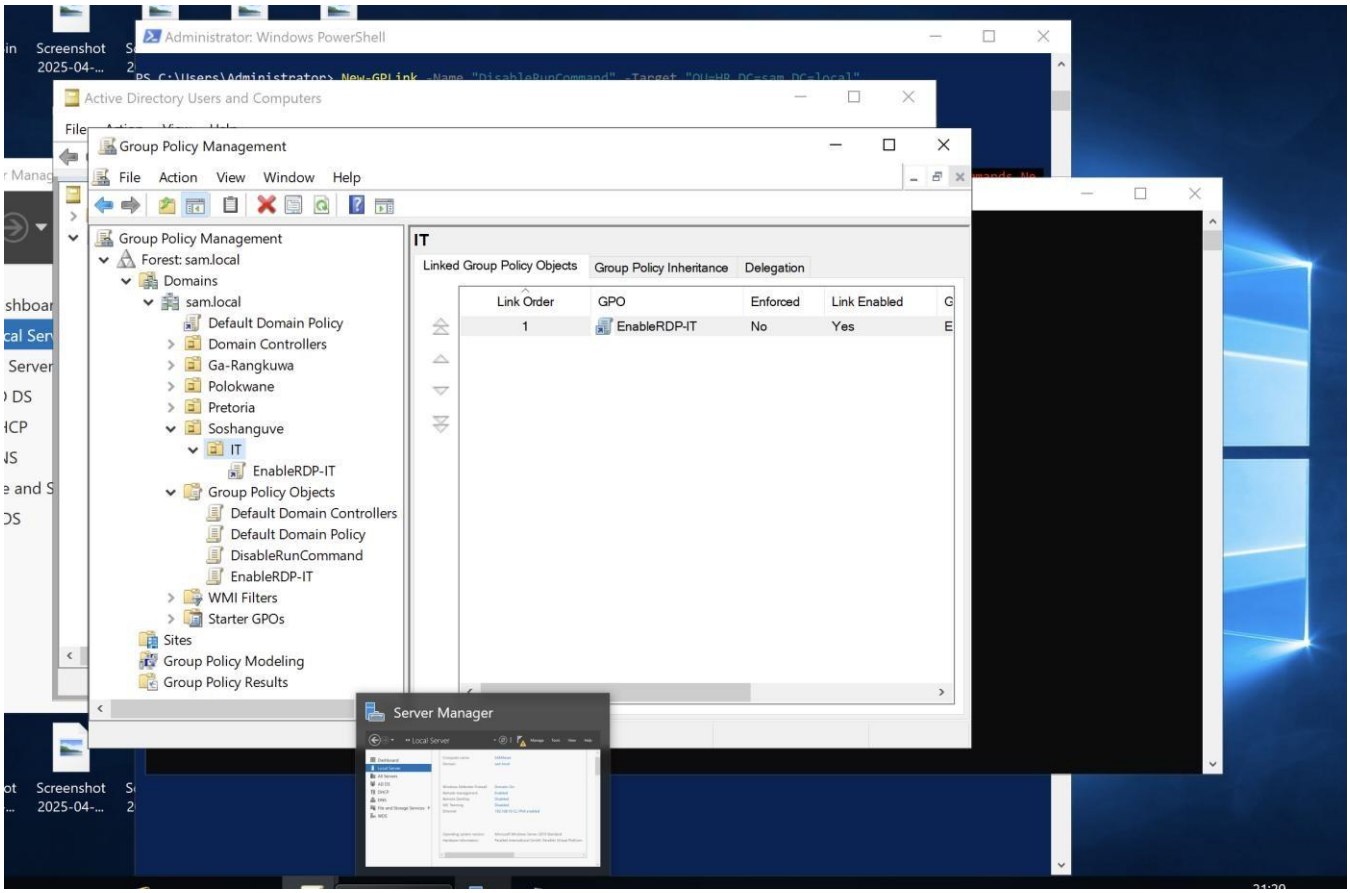


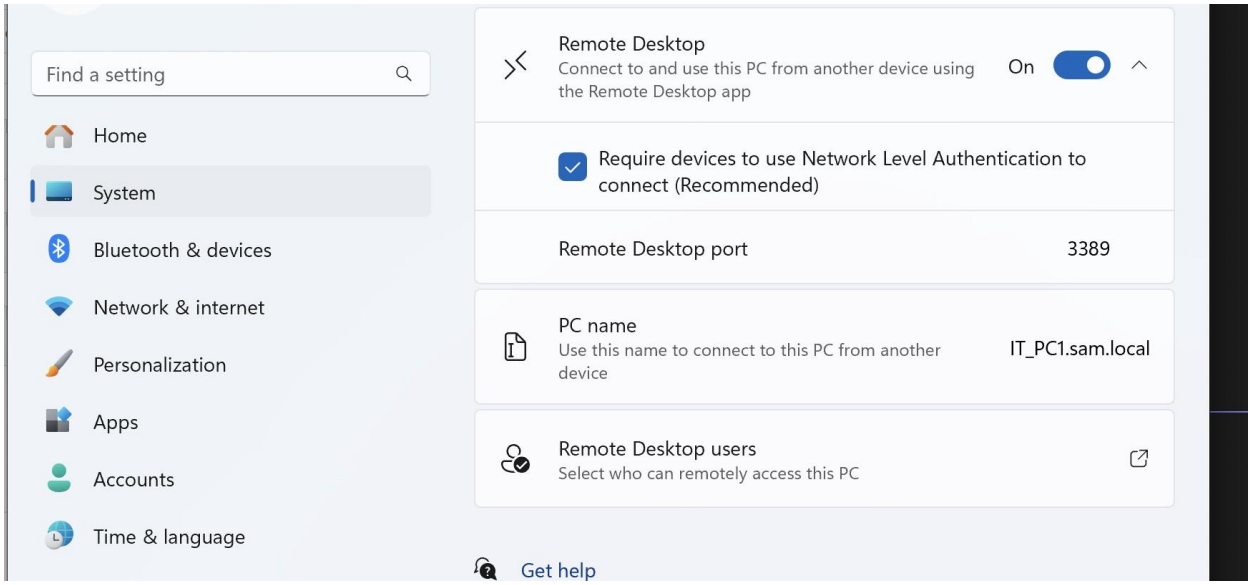
Enabling RDP on ITGroup



GPO for enabling RDP



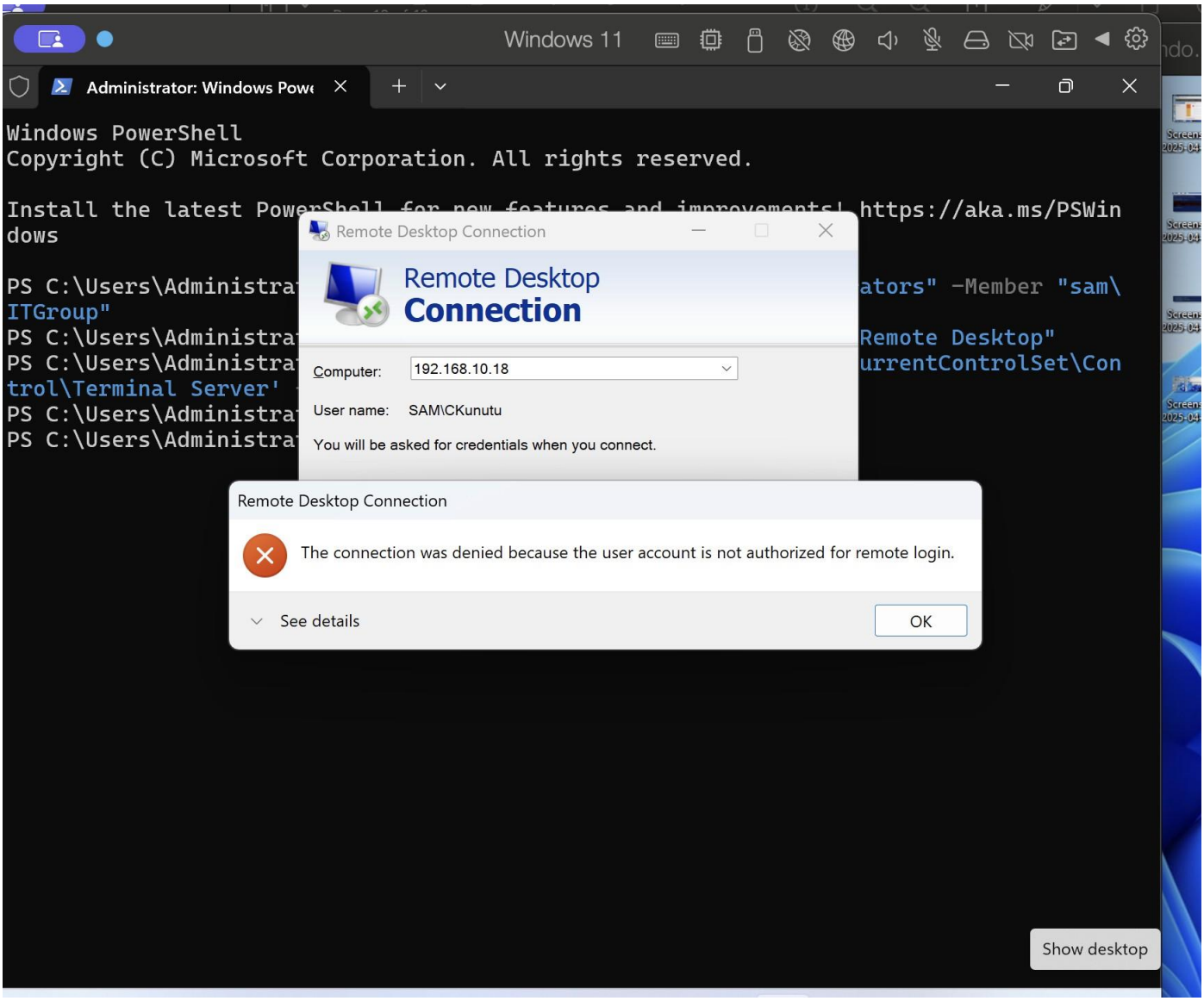




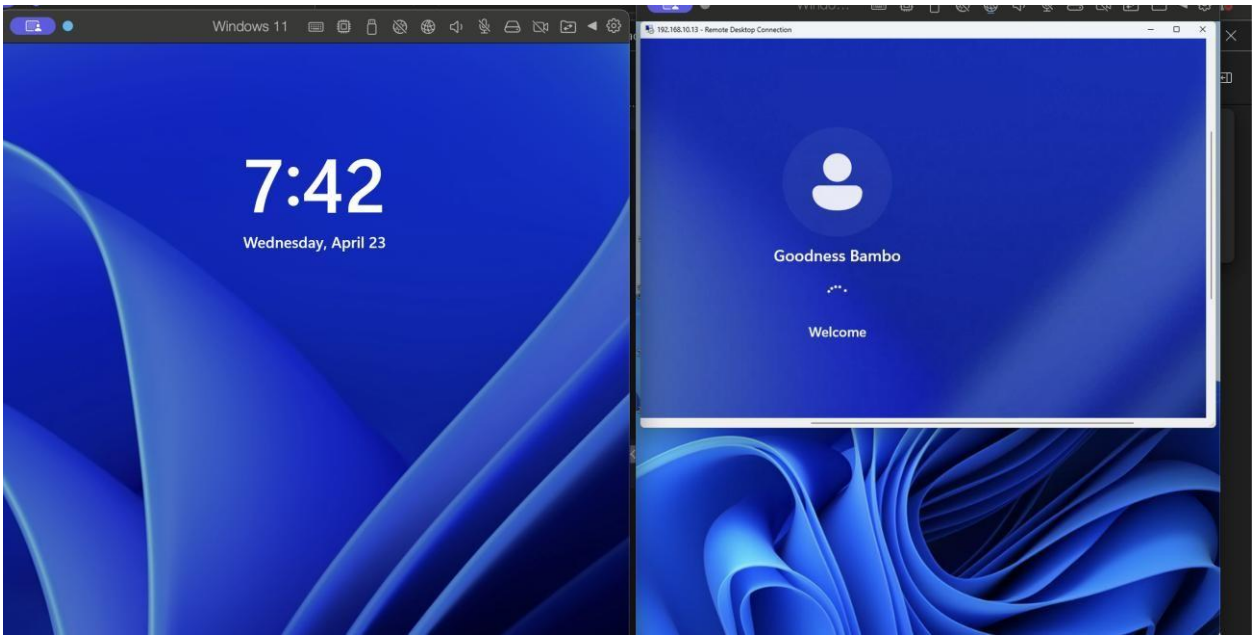
PowerShell command to enable Enable Remote Desktop | Add domain group to local Administrators | Open RDP port in firewall

```
PS C:\Windows\system32> Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -
Name fDenyTSConnections -Value 0
PS C:\Windows\system32> Add-LocalGroupMember -Group "Administrators" -Member "sam\ITGroup"
PS C:\Windows\system32> Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
PS C:\Windows\system32>
```

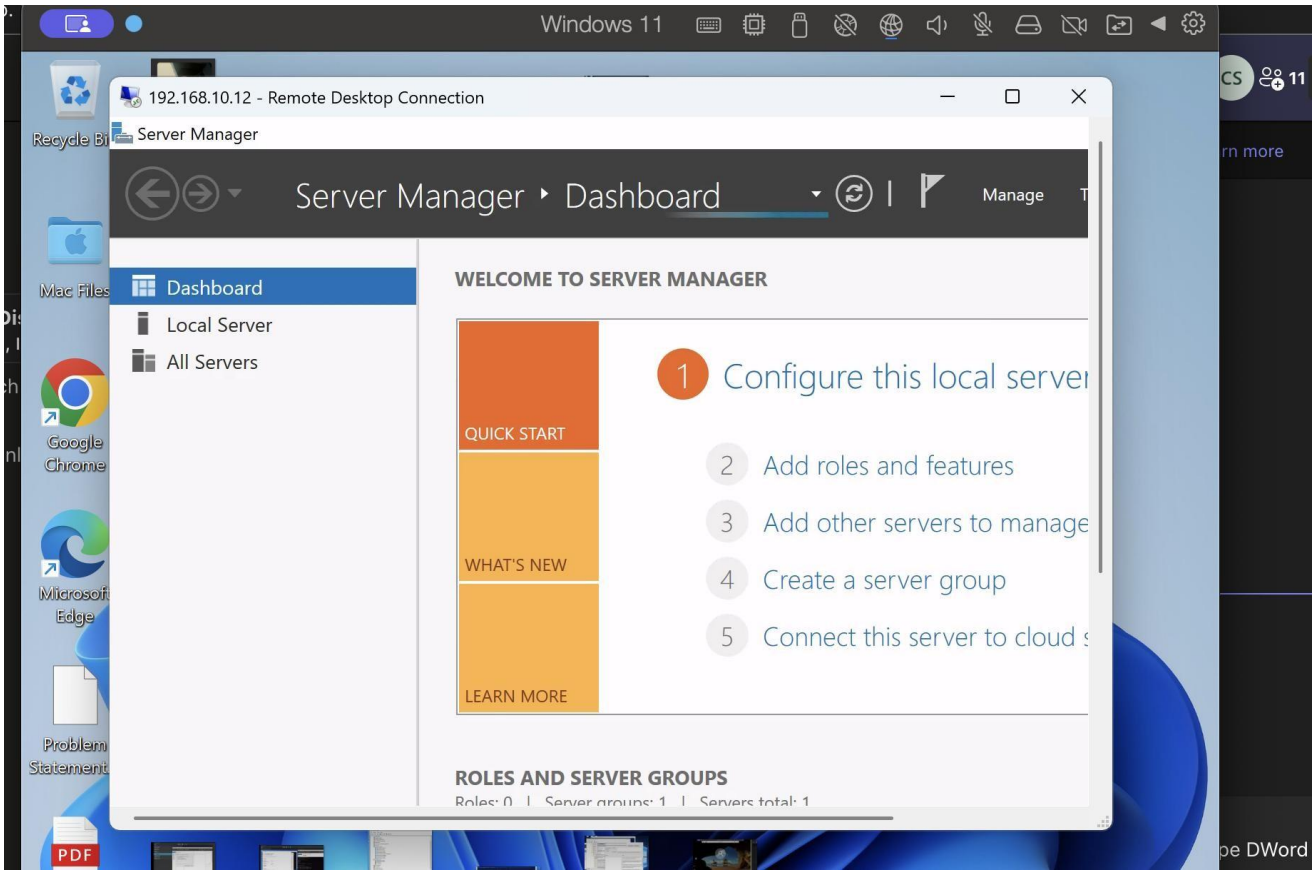
Testing with user not linked to the Enabling RDP



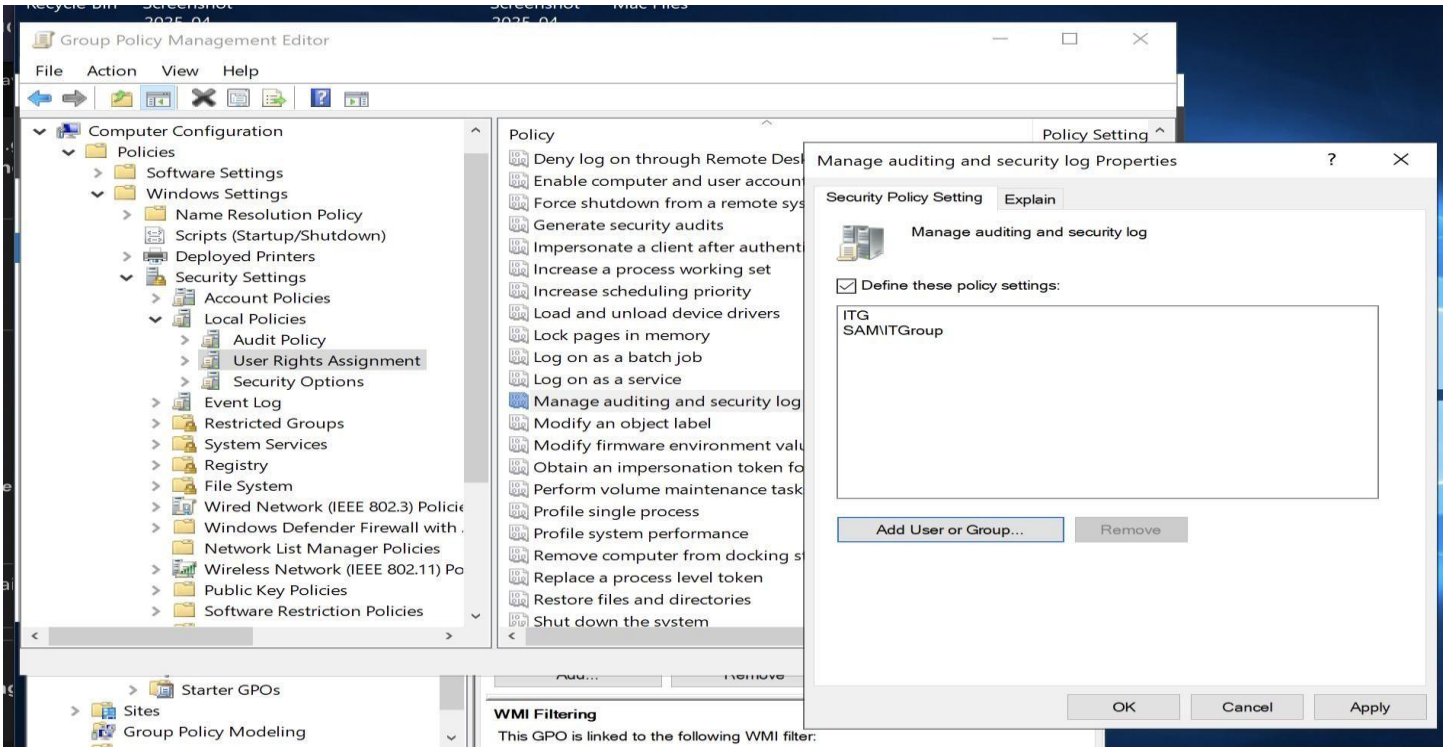
Authorized user was able to Remote



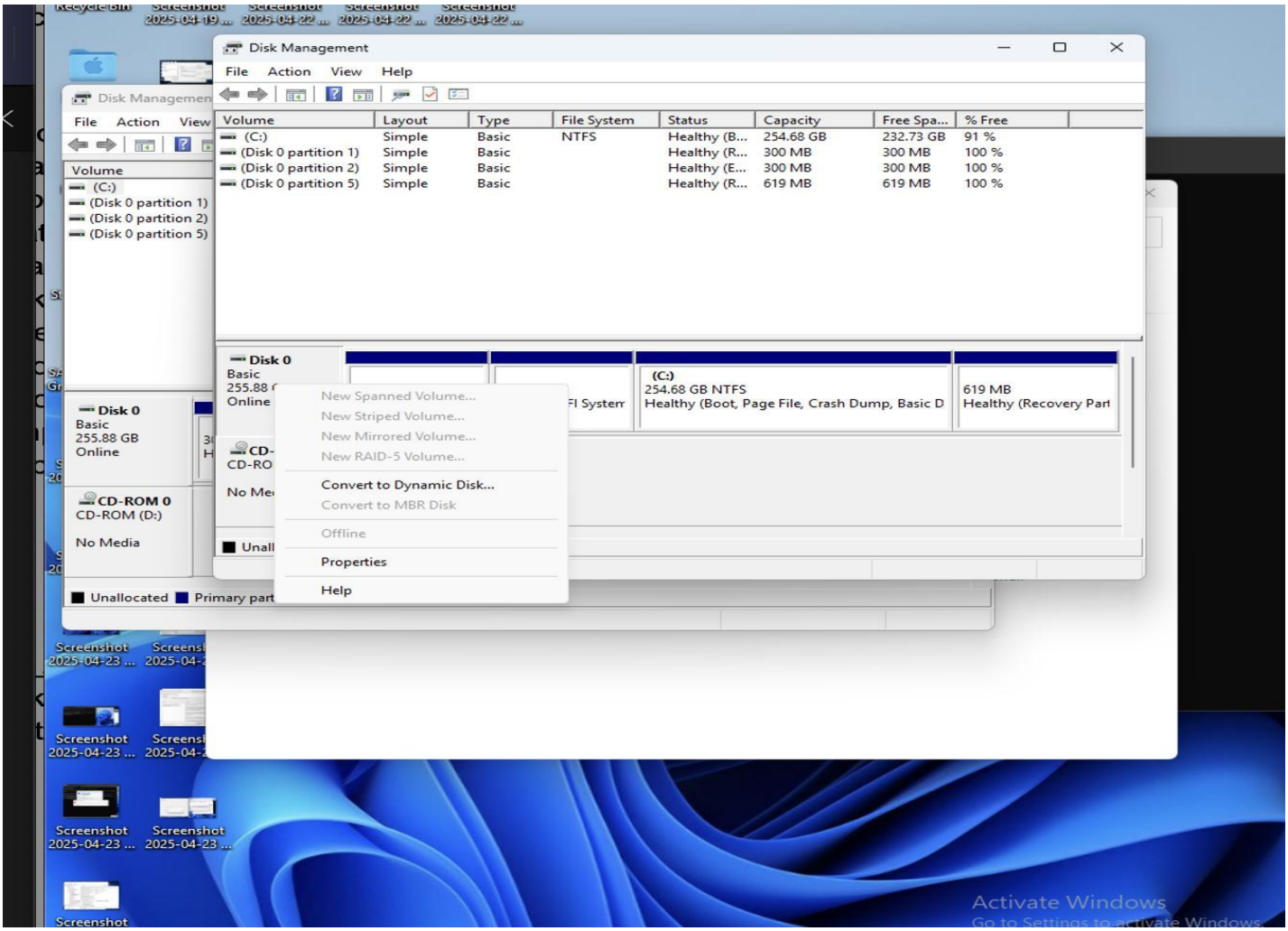
Remote to the Server

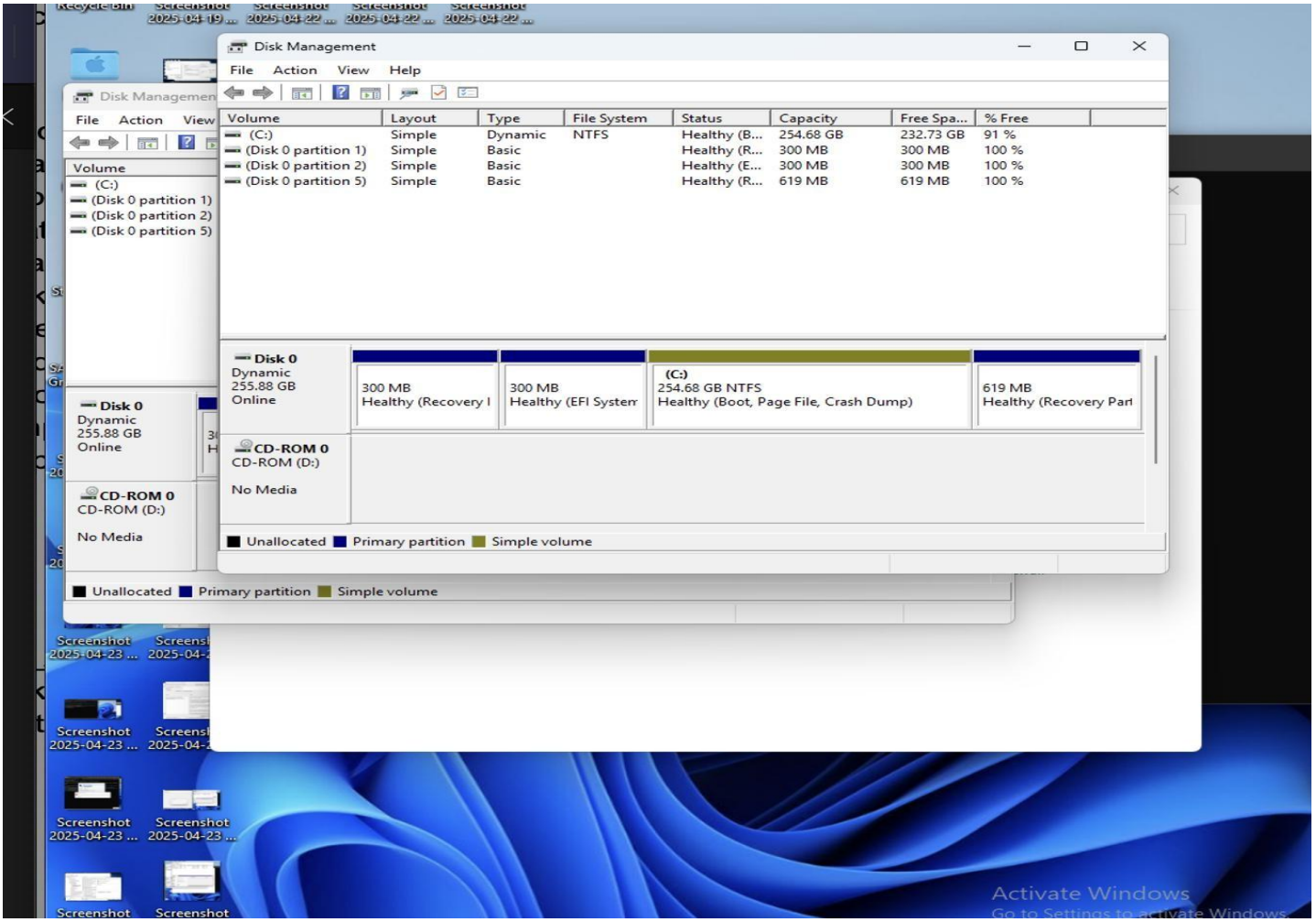


Departments’ basic disk to a dynamic disk and configure the disk quotas

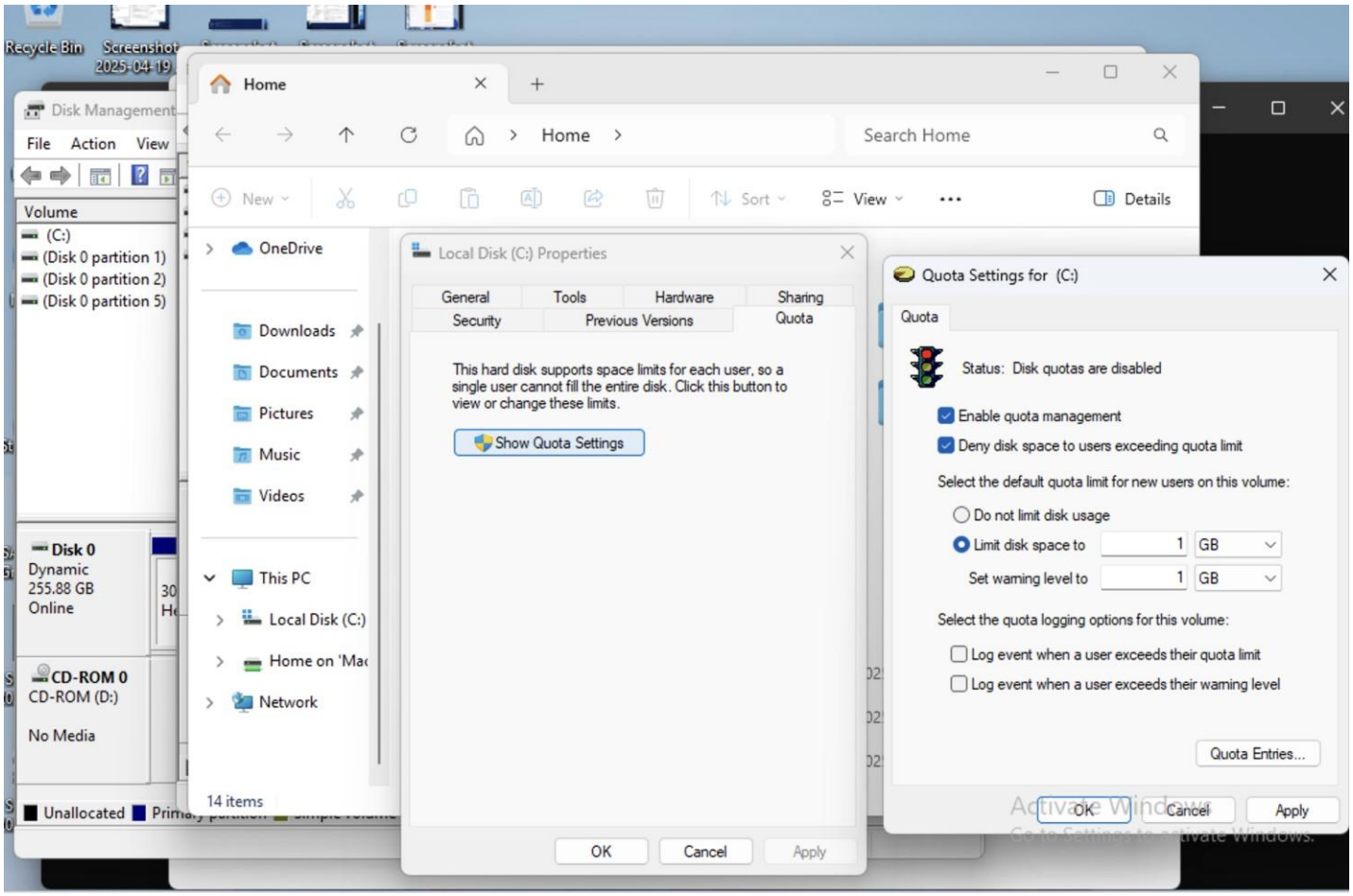


IT Personnel being able to convert Disk to a dynamic disk



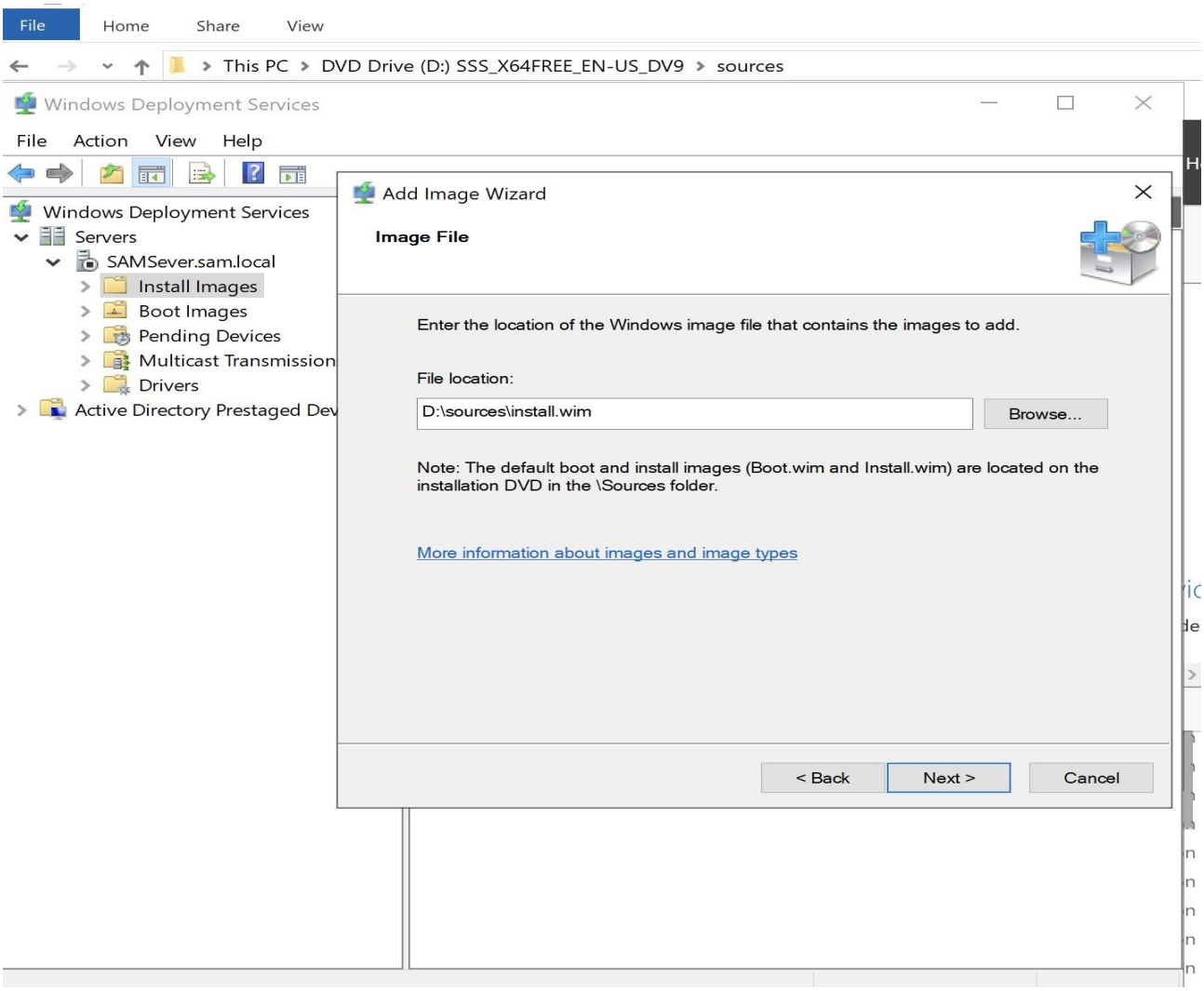

Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Spa... % Free
(C:) Simple Dynamic NTFS Healthy (B... 254.68 GB 232.73 GB 91 %
(Disk 0 partition 1) Simple Basic Healthy (R... 300 MB 300 MB 100 %
(Disk 0 partition 2) Simple Basic Healthy (E... 300 MB 300 MB 100 %
(Disk 0 partition 5) Simple Basic Healthy (R... 619 MB 619 MB 100 %
Disk 0
Dynamic
255.88 GB
Online
300 MB
Healthy (Recovery I
300 MB
Healthy (EFI System
(C:)
254.68 GB NTFS
Healthy (Boot, Page File, Crash Dump)
619 MB
Healthy (Recovery Part
CD-ROM 0
CD-ROM (D:)
No Media
Unallocated Primary partition Simple volume
Activate Windows

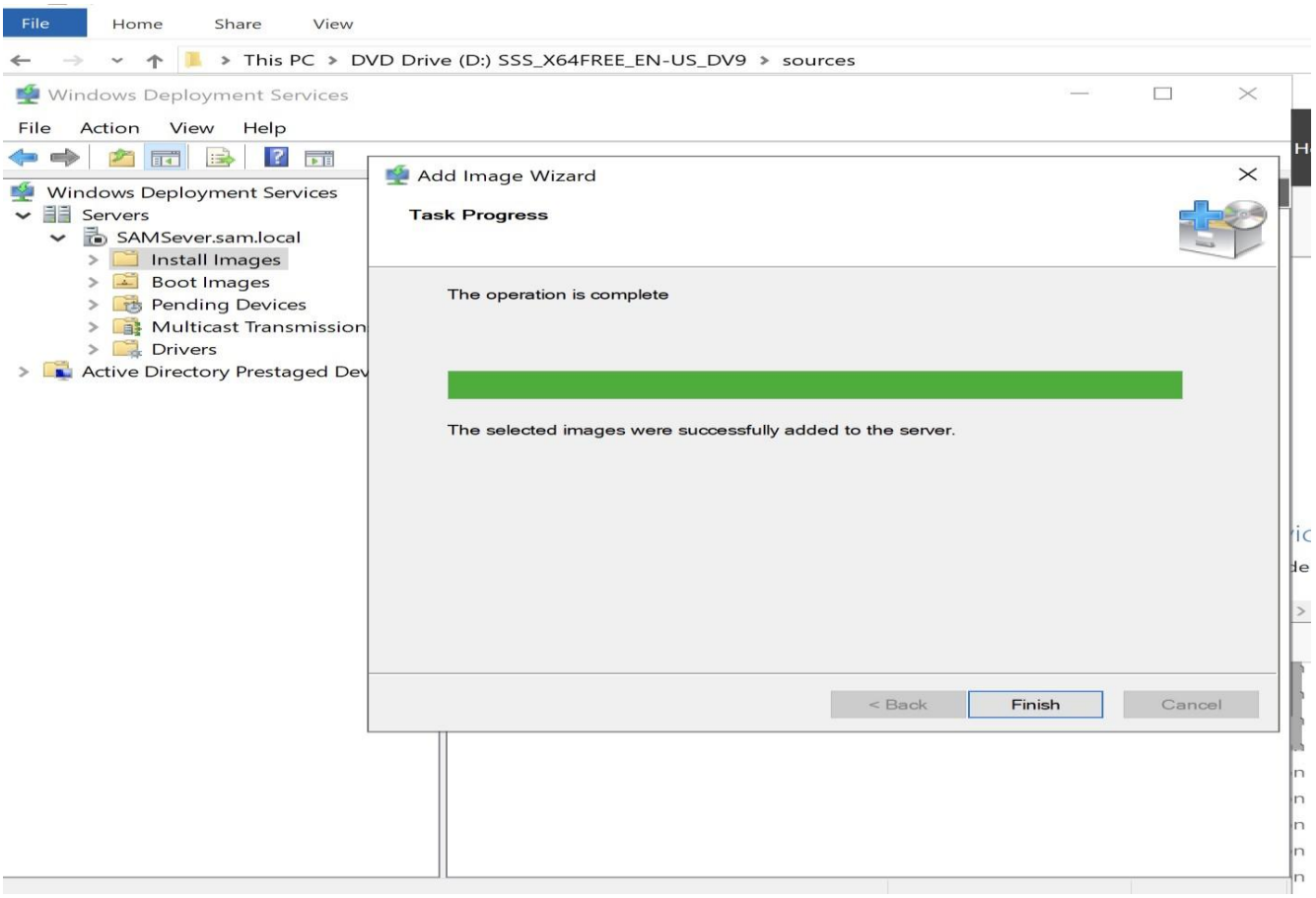
Configure the disk quotas

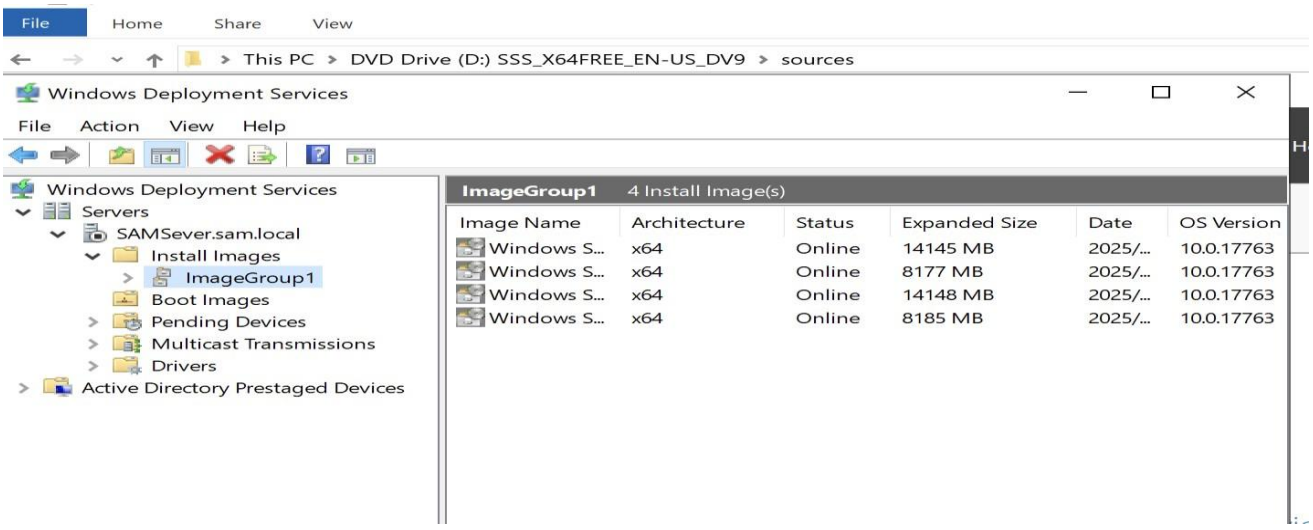


IT Department must be able to deploy servers, images and apps automatically to other machine

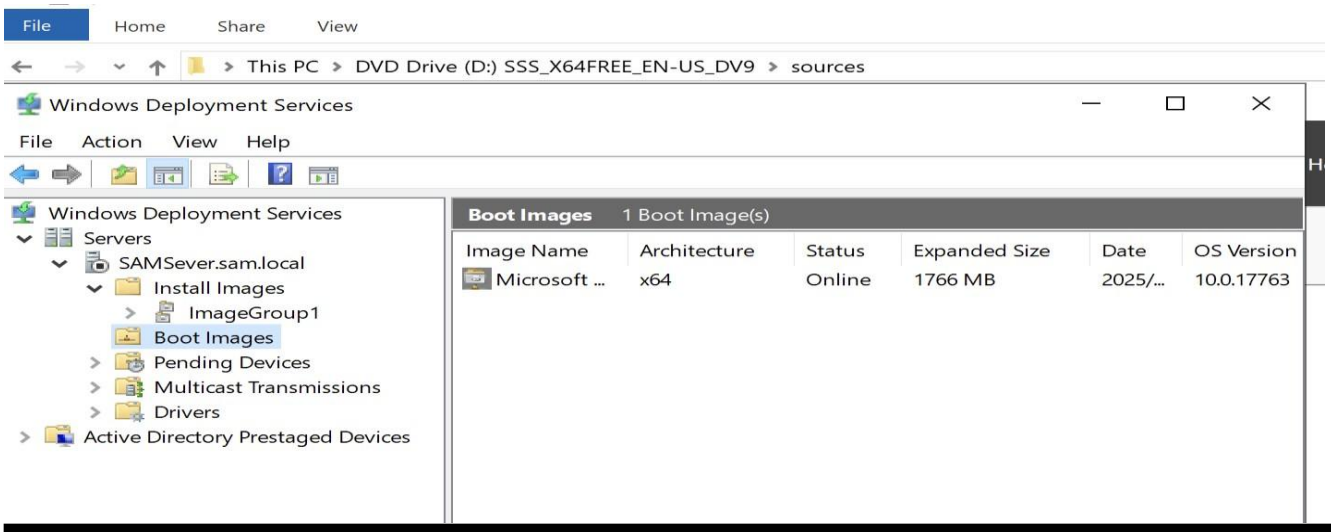
Installing Images

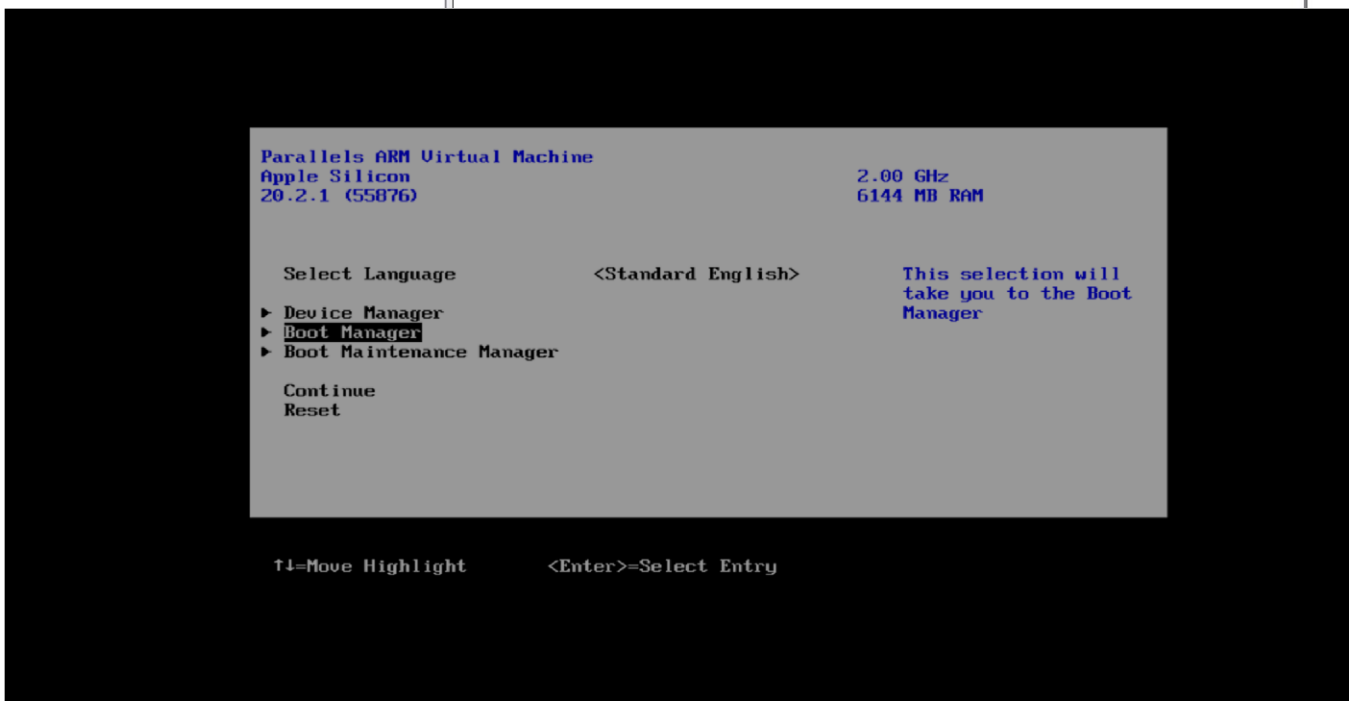



File
Home
Share
View
This PC > DVD Drive (D:) SSS_X64FREE_EN-US_DV9 > sources
Windows Deployment Services
File
Action
View
Help
Windows Deployment Services
Servers
SAMSever.sam.local
Install Images
Boot Images
Pending Devices
Multicast Transmission
Drivers
Active Directory Prestaged Dev
Add Image Wizard
Task Progress
The operation is complete
The selected images were successfully added to the server.
< Back
Finish
Cancel

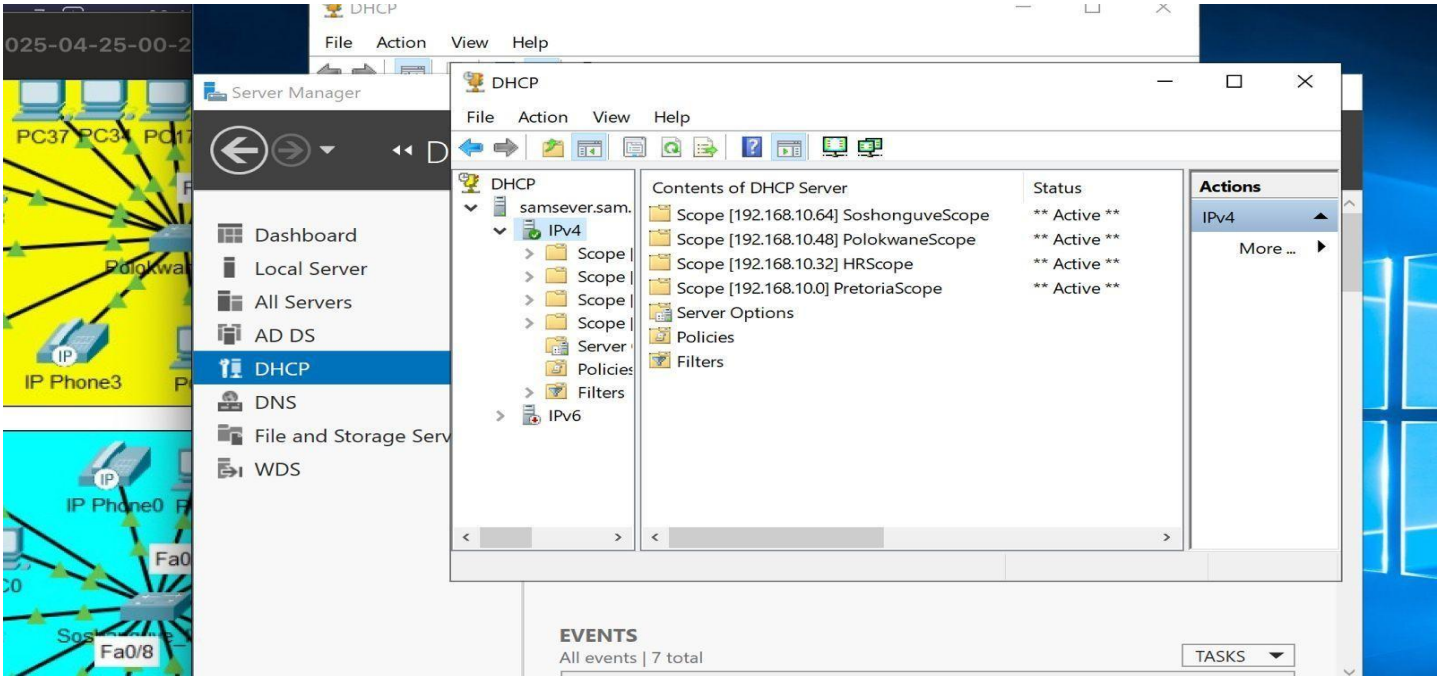

File
Home
Share
View
This PC > DVD Drive (D:) SSS_X64FREE_EN-US_DV9 > sources
Windows Deployment Services
File
Action
View
Help
Windows Deployment Services
Servers
SAMSever.sam.local
Install Images
ImageGroup1
Boot Images
Pending Devices
Multicast Transmissions
Drivers
Active Directory Prestaged Devices
ImageGroup1
4 Install Image(s)
Image Name
Architecture
Status
Expanded Size
Date
OS Version
Windows S...
x64
Online
14145 MB
2025/...
10.0.17763
Windows S...
x64
Online
8177 MB
2025/...
10.0.17763
Windows S...
x64
Online
14148 MB
2025/...
10.0.17763
Windows S...
x64
Online
8185 MB
2025/...
10.0.17763

Boot Images:

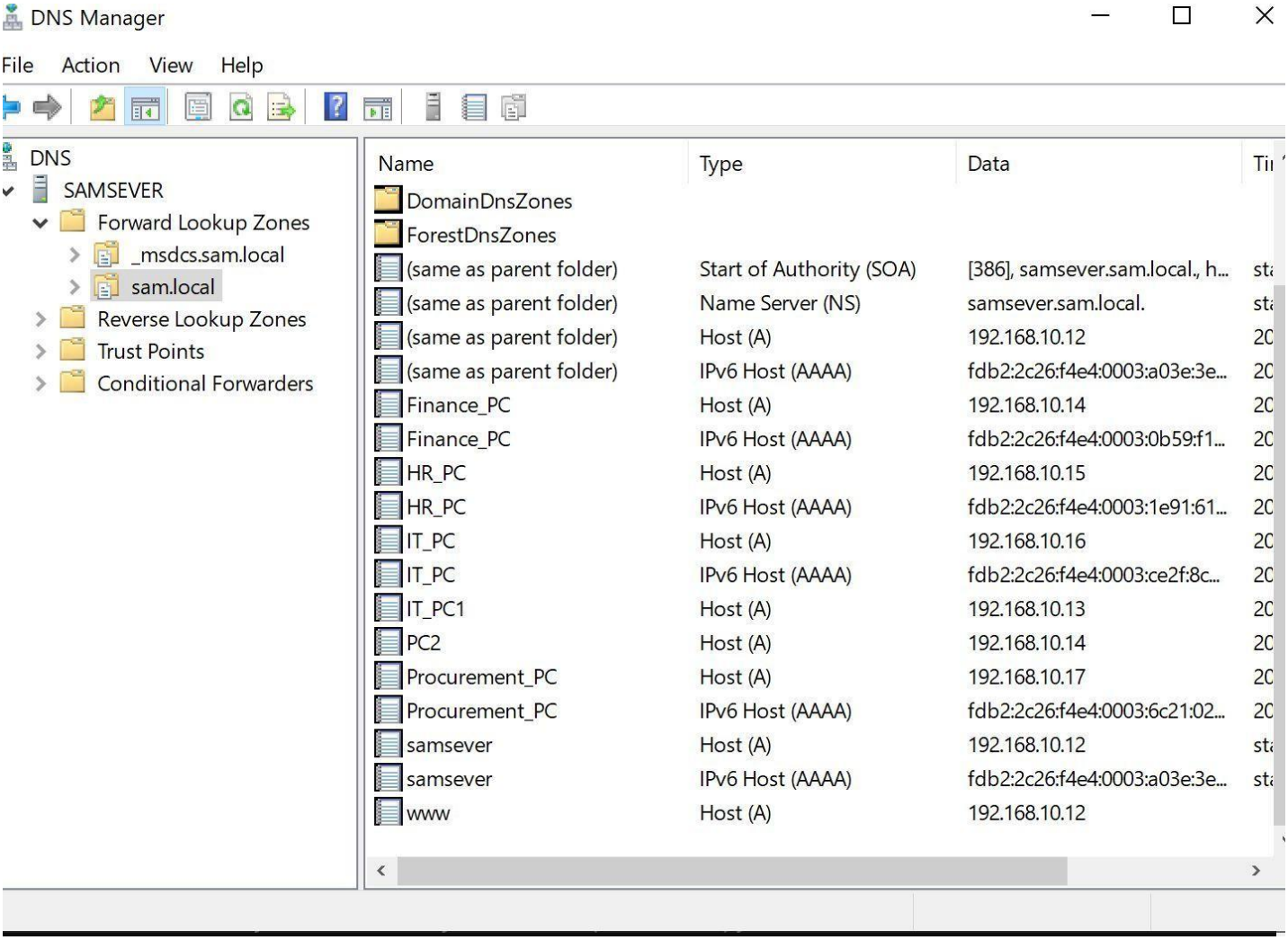

File
Home
Share
View
This PC > DVD Drive (D:) SSS_X64FREE_EN-US_DV9 > sources
Windows Deployment Services
File
Action
View
Help
Windows Deployment Services
Servers
SAMSever.sam.local
Install Images
ImageGroup1
Boot Images
Pending Devices
Multicast Transmissions
Drivers
Active Directory Prestaged Devices
Boot Images
1 Boot Image(s)
Image Name
Architecture
Status
Expanded Size
Date
OS Version
Microsoft ...
x64
Online
1766 MB
2025/...
10.0.17763


Parallels ARM Virtual Machine
Apple Silicon
20.2.1 (55876)
2.00 GHz
6144 MB RAM
Select Language
<Standard English>
This selection will take you to the Boot Manager
Device Manager
Boot Manager
Boot Maintenance Manager
Continue
Reset
↑↓=Move Highlight
<Enter>=Select Entry

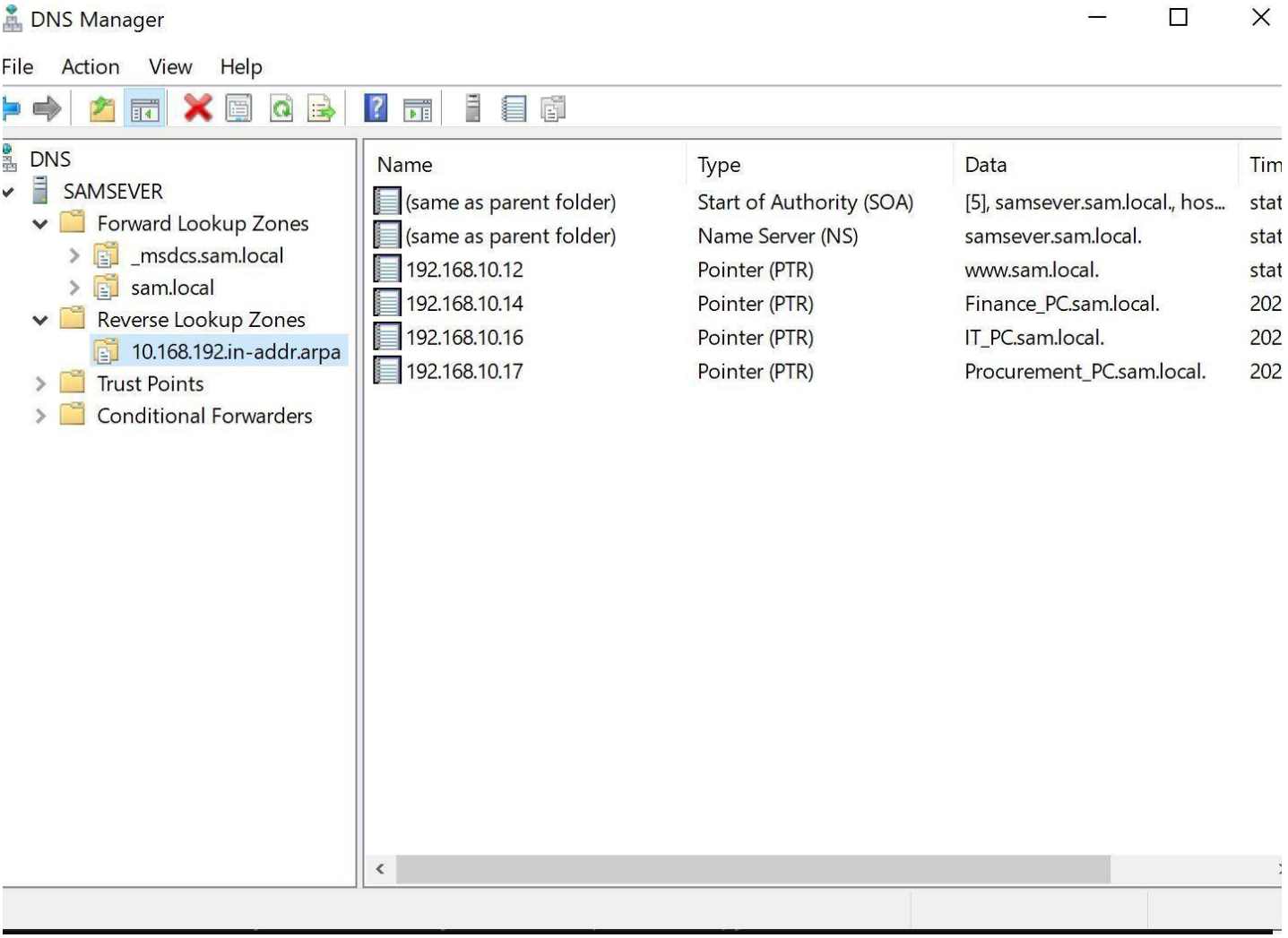
DHCP IP Address Scope

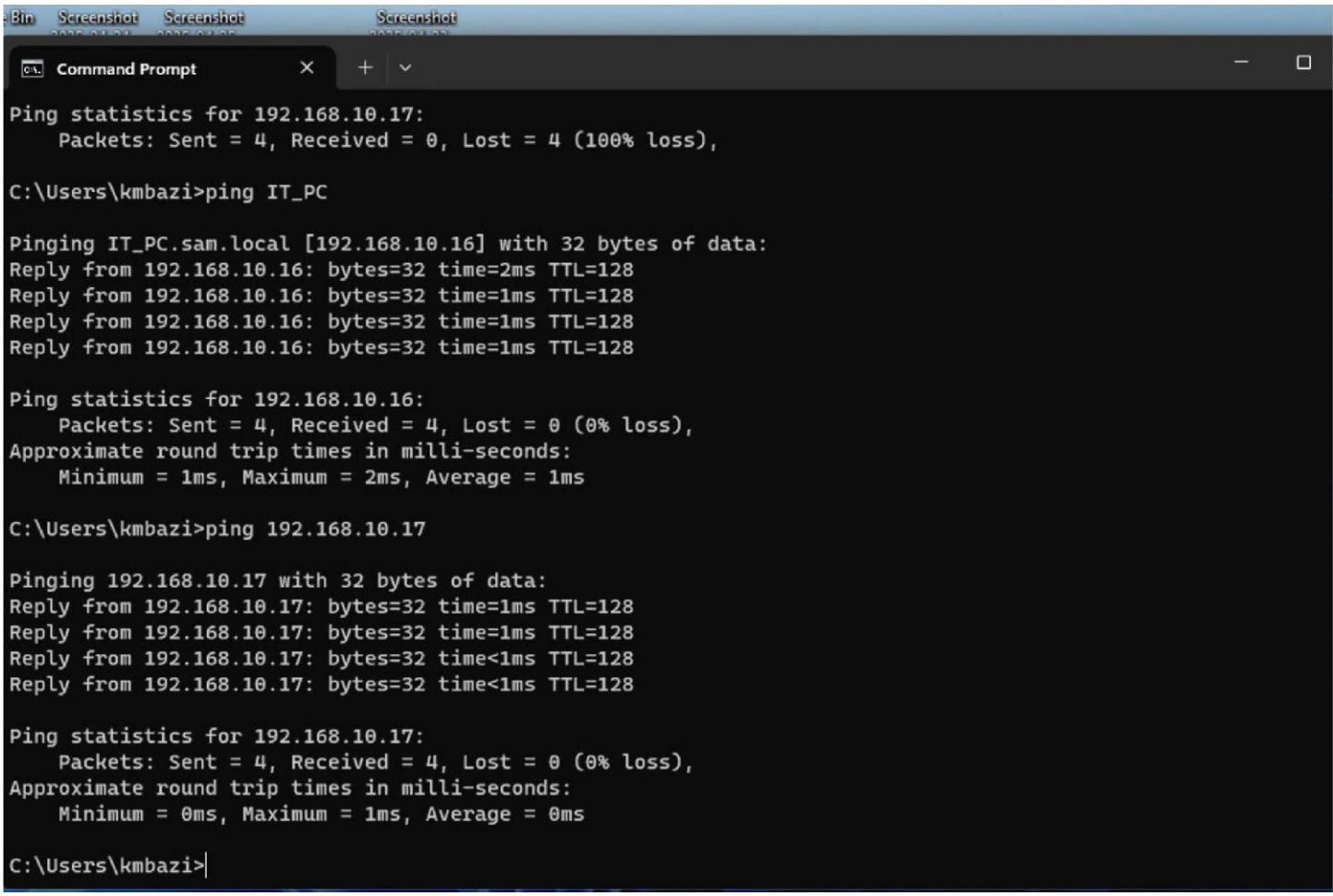


DNS Forward Lookup Zones



DNS Reverses Lookup Zones




Bin
Screenshot
Screenshot
Screenshot
Command Prompt
Ping statistics for 192.168.10.17:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\kmbazi>ping IT_PC
Pinging IT_PC.sam.local [192.168.10.16] with 32 bytes of data:
Reply from 192.168.10.16: bytes=32 time=2ms TTL=128
Reply from 192.168.10.16: bytes=32 time=1ms TTL=128
Reply from 192.168.10.16: bytes=32 time=1ms TTL=128
Reply from 192.168.10.16: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.10.16:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\kmbazi>ping 192.168.10.17
Pinging 192.168.10.17 with 32 bytes of data:
Reply from 192.168.10.17: bytes=32 time=1ms TTL=128
Reply from 192.168.10.17: bytes=32 time=1ms TTL=128
Reply from 192.168.10.17: bytes=32 time<1ms TTL=128
Reply from 192.168.10.17: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.10.17:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\kmbazi>