

SYSTEM ADMINISTRATION AND MAINTAINANCE PROJECT

YEAR: 2025

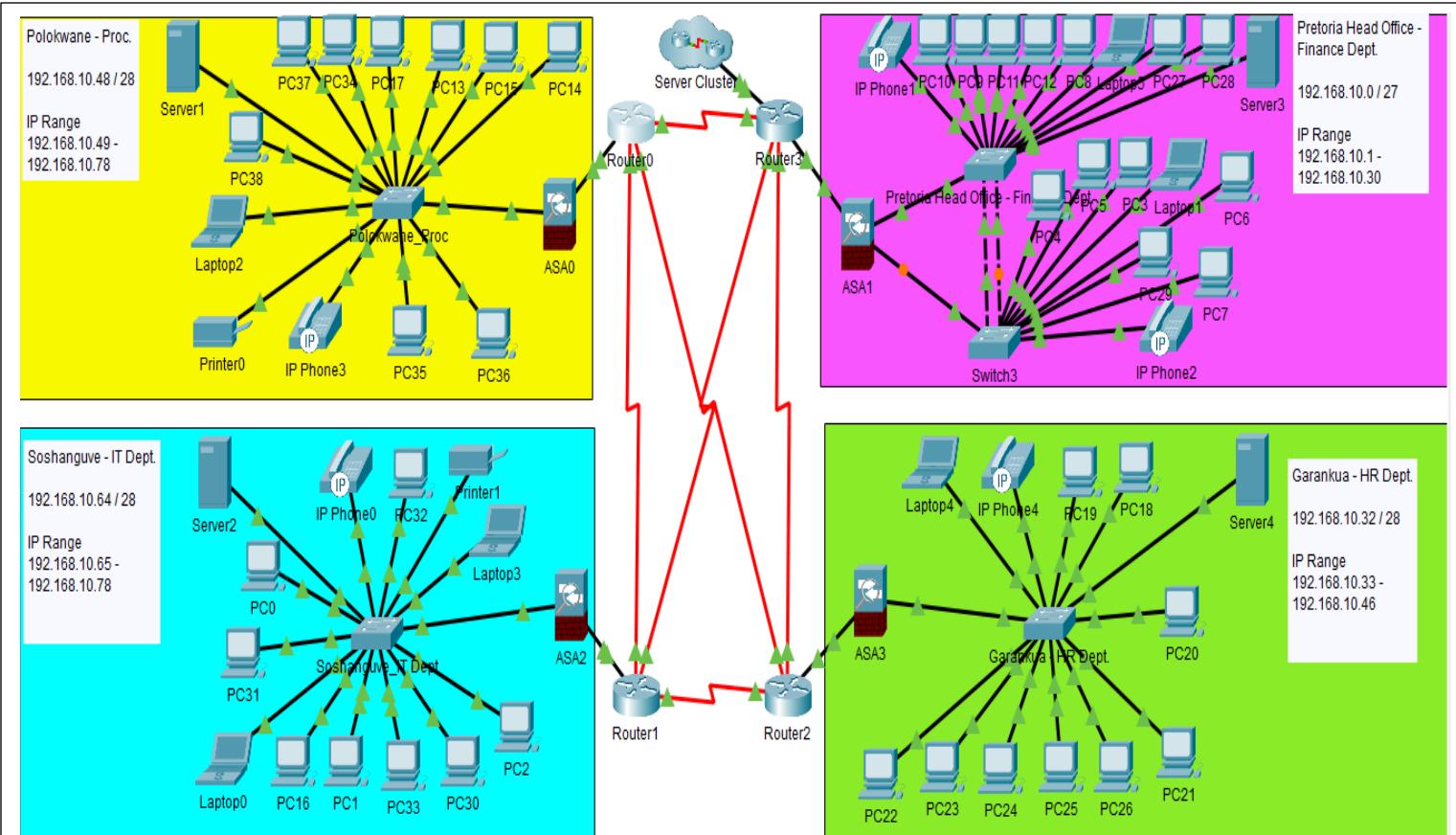
Table of Contents

Company Network structure	2
Setting IP for the Server	3
Adding Roles and Features	4
Setting Domain Name	5
Creating Organizational Unit Using GUI	6
Creating new users	7
Shared Folder Access	8
IT Group permissions	8
HR Permissions:.....	9
Disabling Run Function on HR, Finance and Procurement:	10
Creating GPO:	10
Linking GPO to the OU:	10
Remove Run from Finance:.....	12
Disabling Run Function on HR and Procurement.....	13
Testing Run Command	15
IT Personnel running Run Command, User was able to open PowerShell using the Run Function	16
Enabling RDP on ITGroup	17
GPO for enabling RDP	18
PowerShell command to enable Enable Remote Desktop Add domain group to local Administrators Open RDP port in firewall.....	19
Testing with user not linked to the Enabling RDP	20
Authorized user was able to Remote.....	21
Remote to the Server	21
Departments' basic disk to a dynamic disk and configure the disk quotas	22
IT Personnel being able to convert Disk to a dynamic disk	23

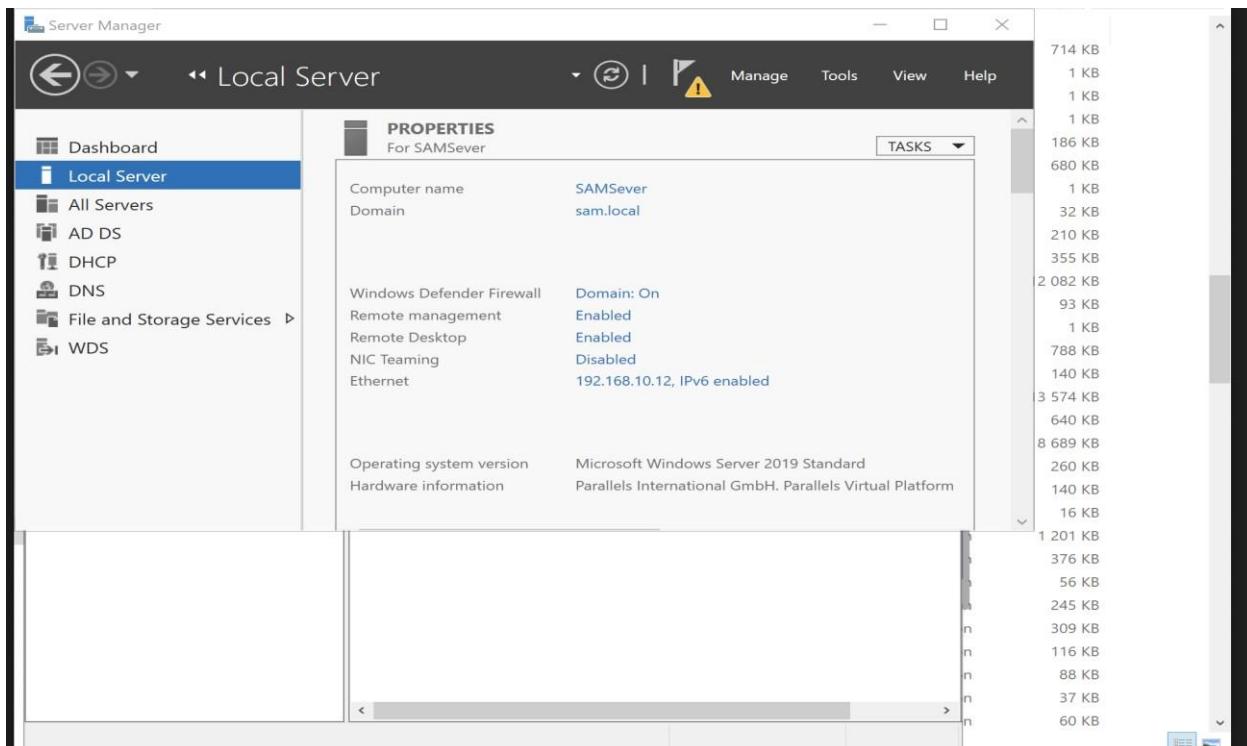
Configure the disk quotas	25
IT Department must be able to deploy servers, images and apps automatically to other machine	26
Installing Images.....	26
Boot Images.....	29
DHCP IP Address Scope	30
DNS Forward Lookup Zones.....	31
DNS Reverses Lookup Zones	32

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.



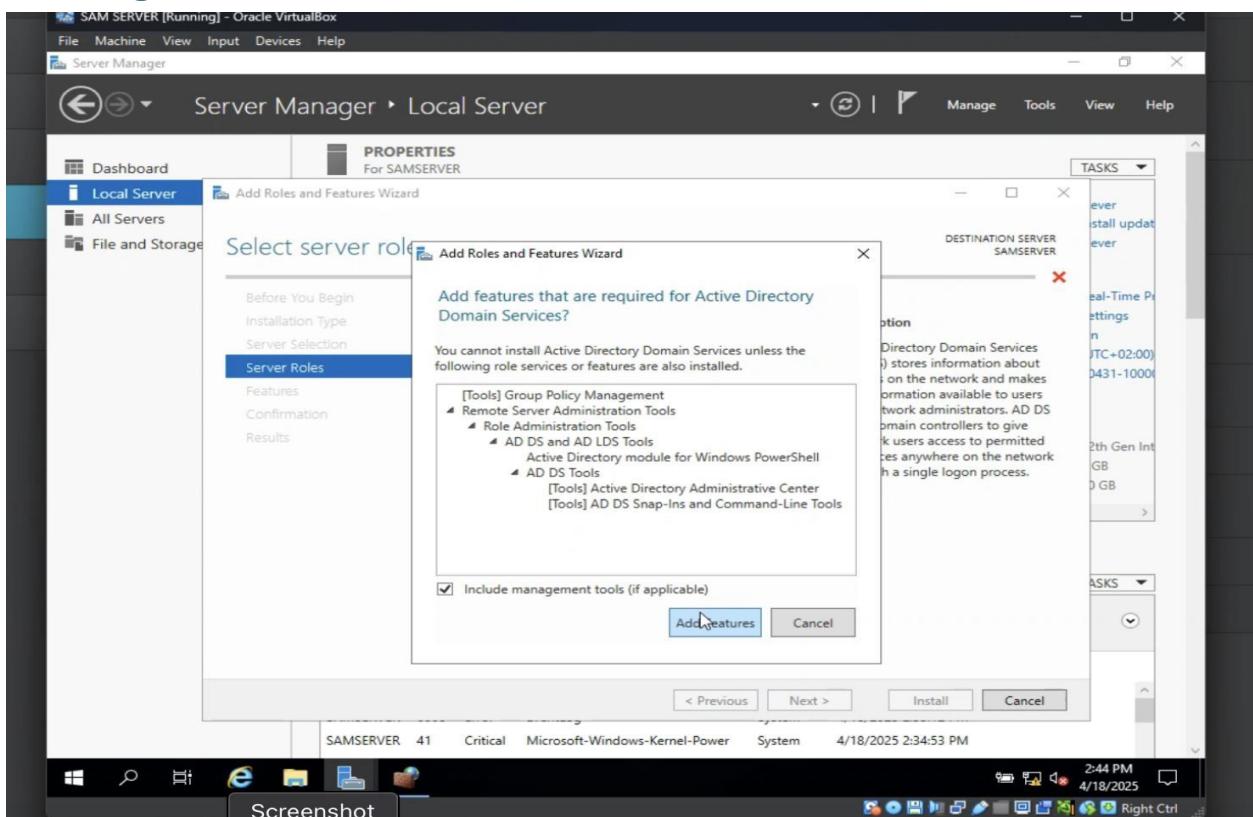
Setting IP for the Server

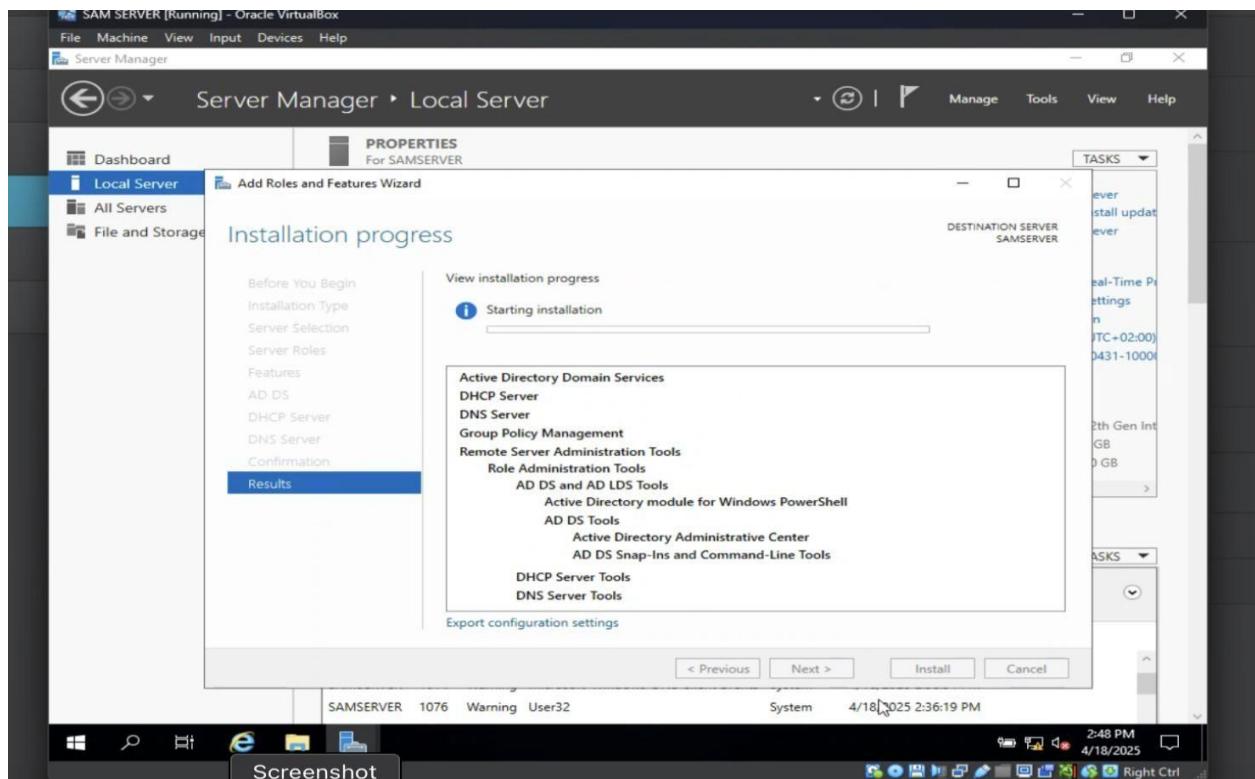


```
[Administrator: Windows PowerShell]
Ethernet adapter Ethernet:

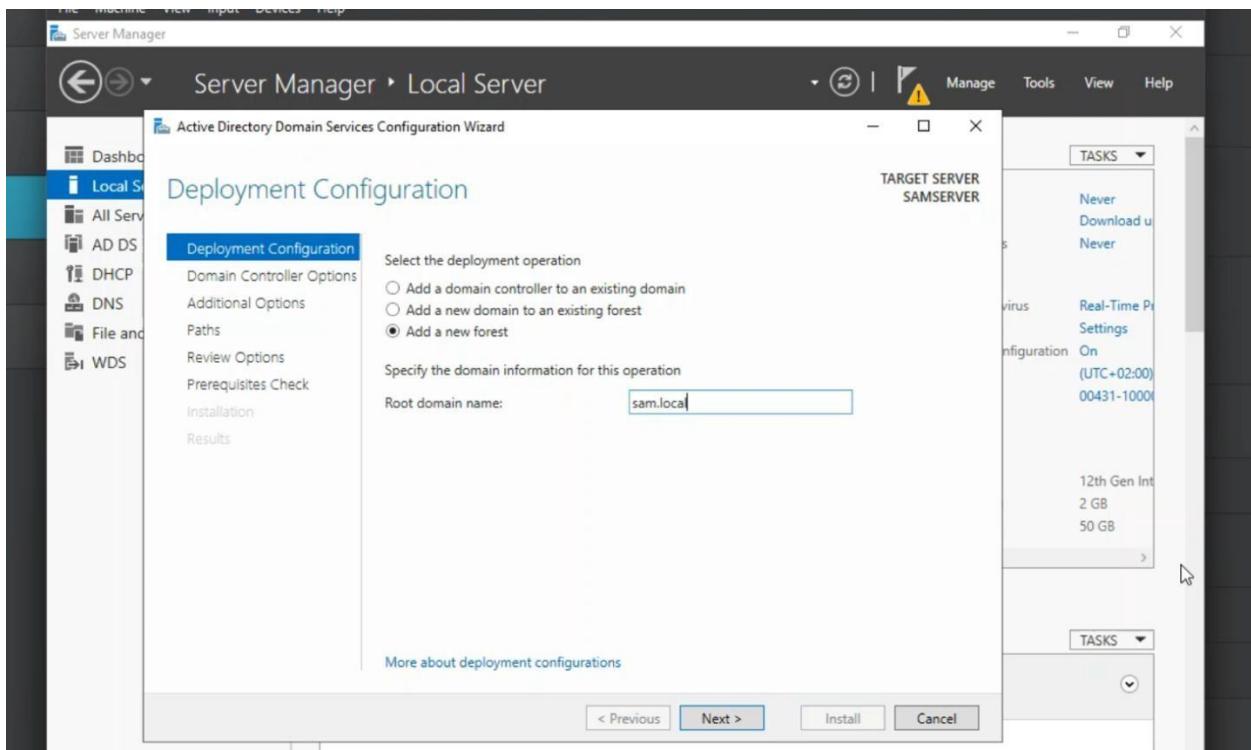
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . : fe80::a03e:3e92:8ad9:8757%12
IPv4 Address . . . . . : 192.168.10.12
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1
PS C:\Users\Administrator>
```

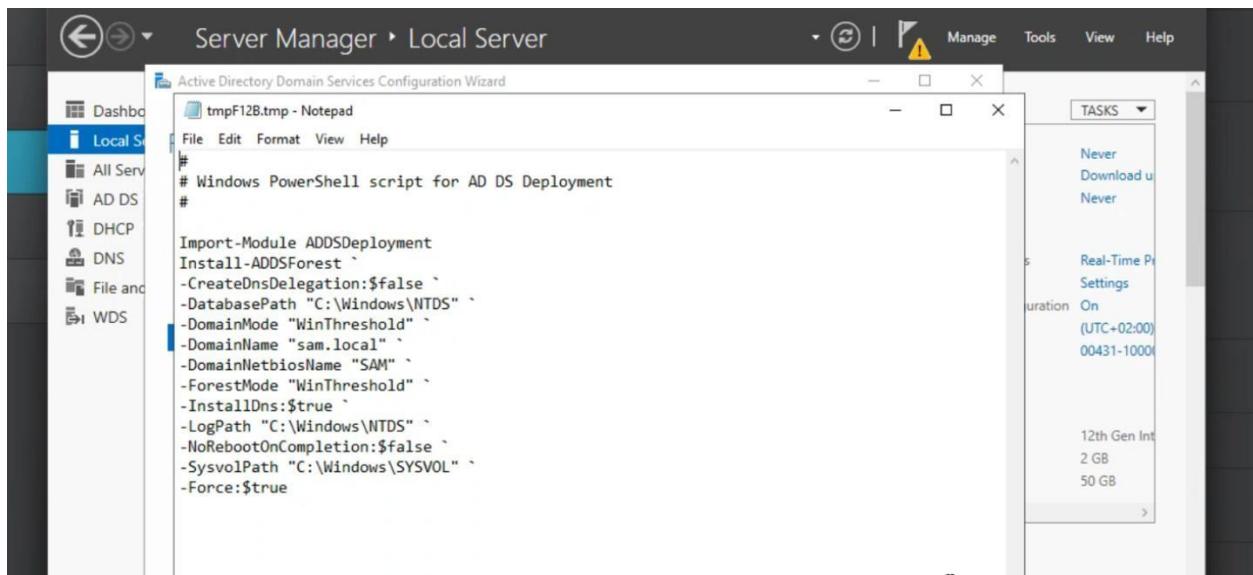
Adding Roles and Features



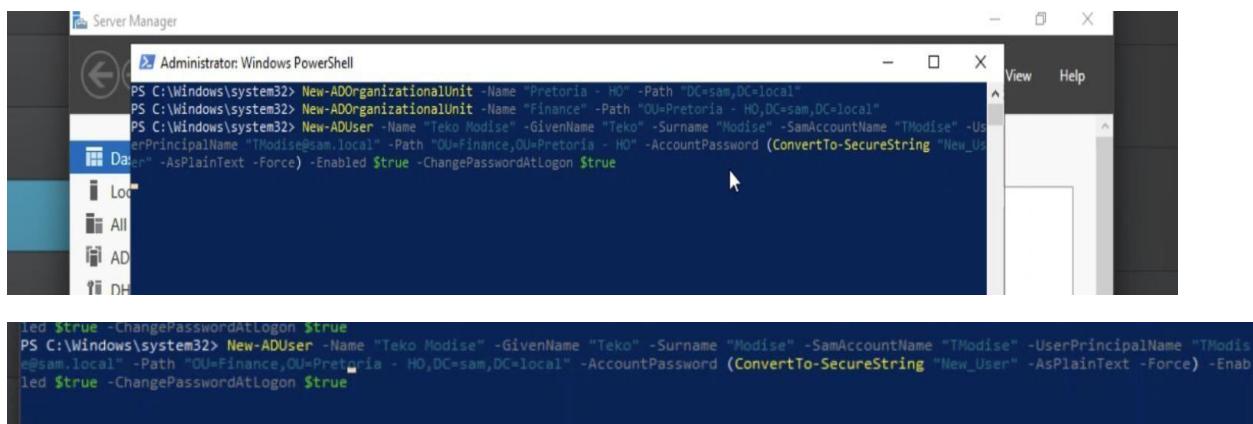


Setting Domain Name

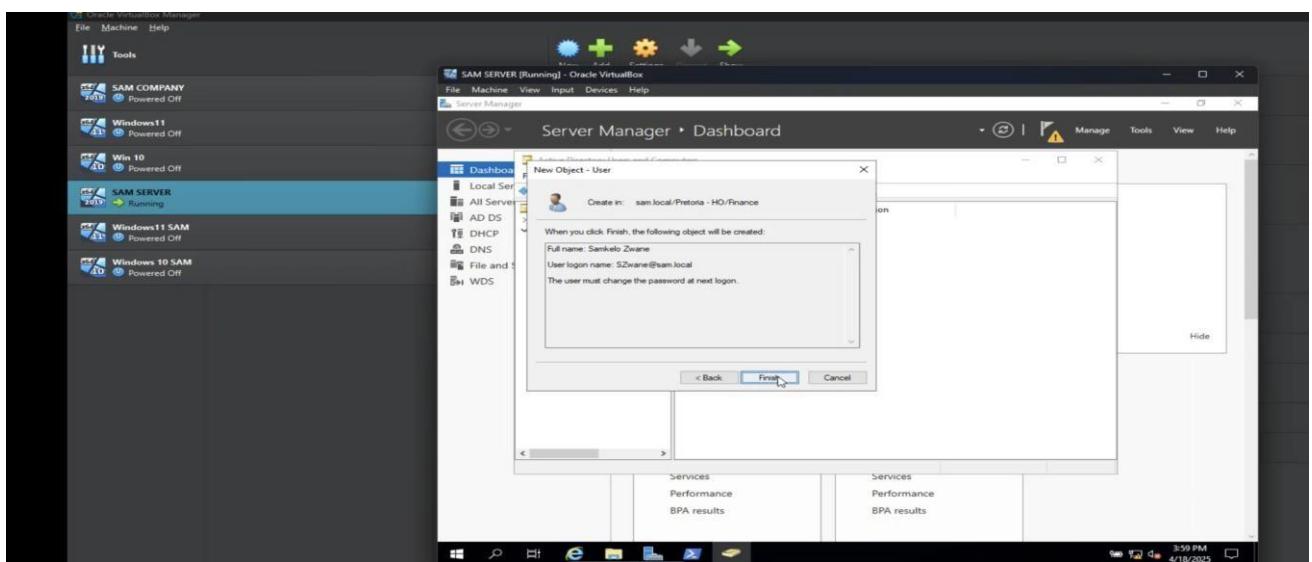
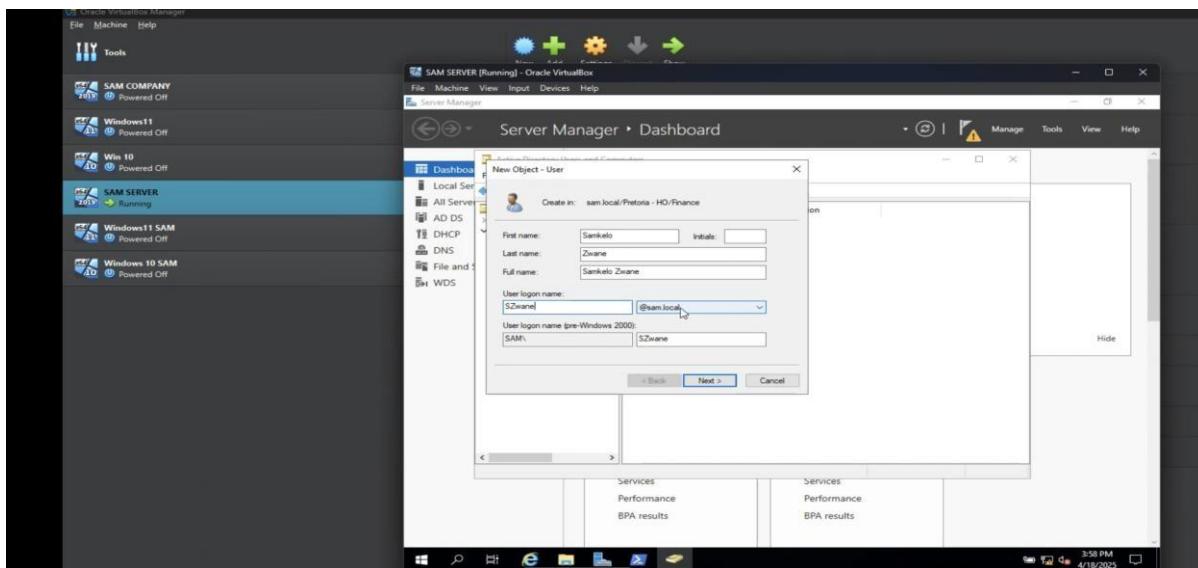


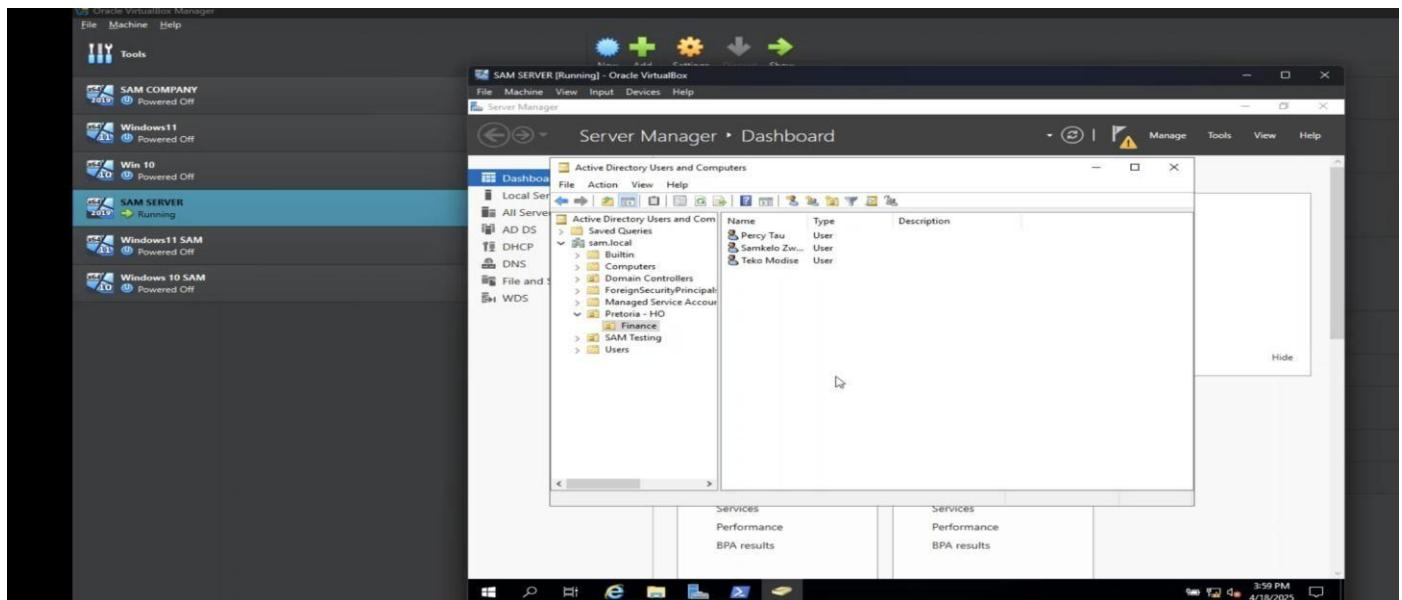


Creating Organizational Unit Using GUI

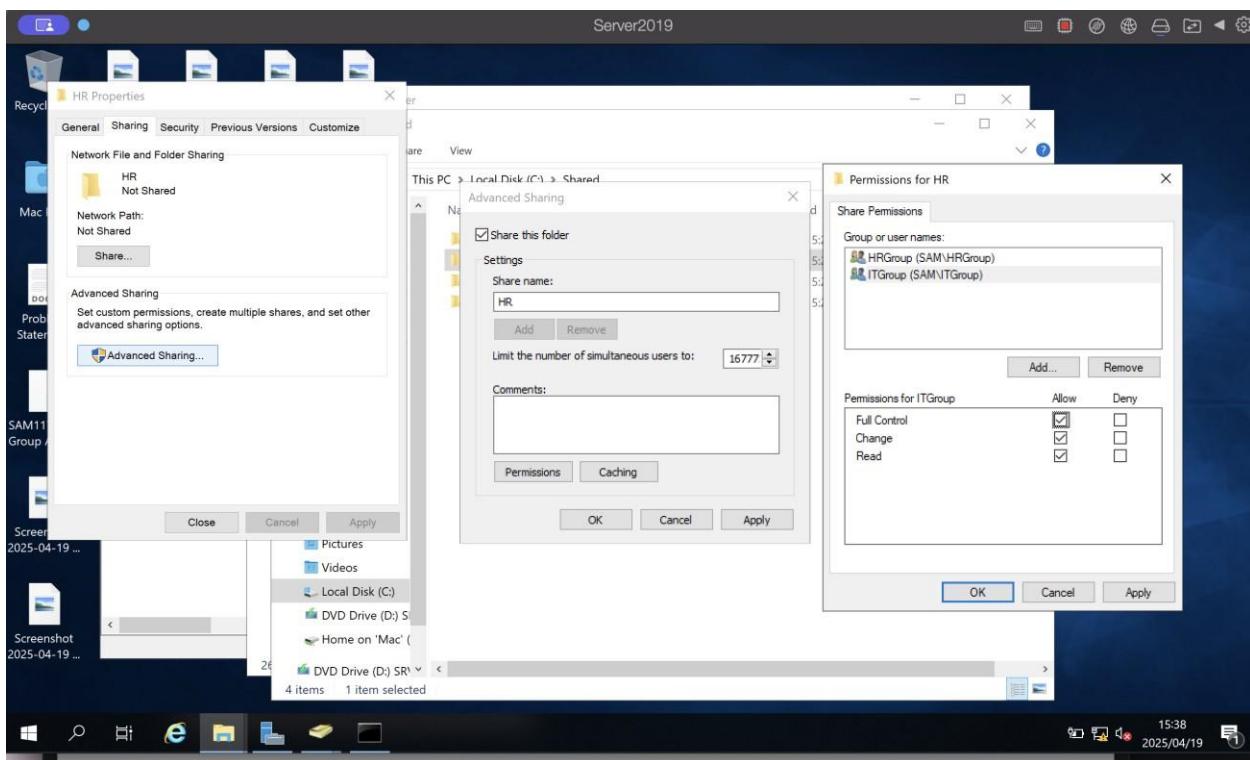


Creating new users

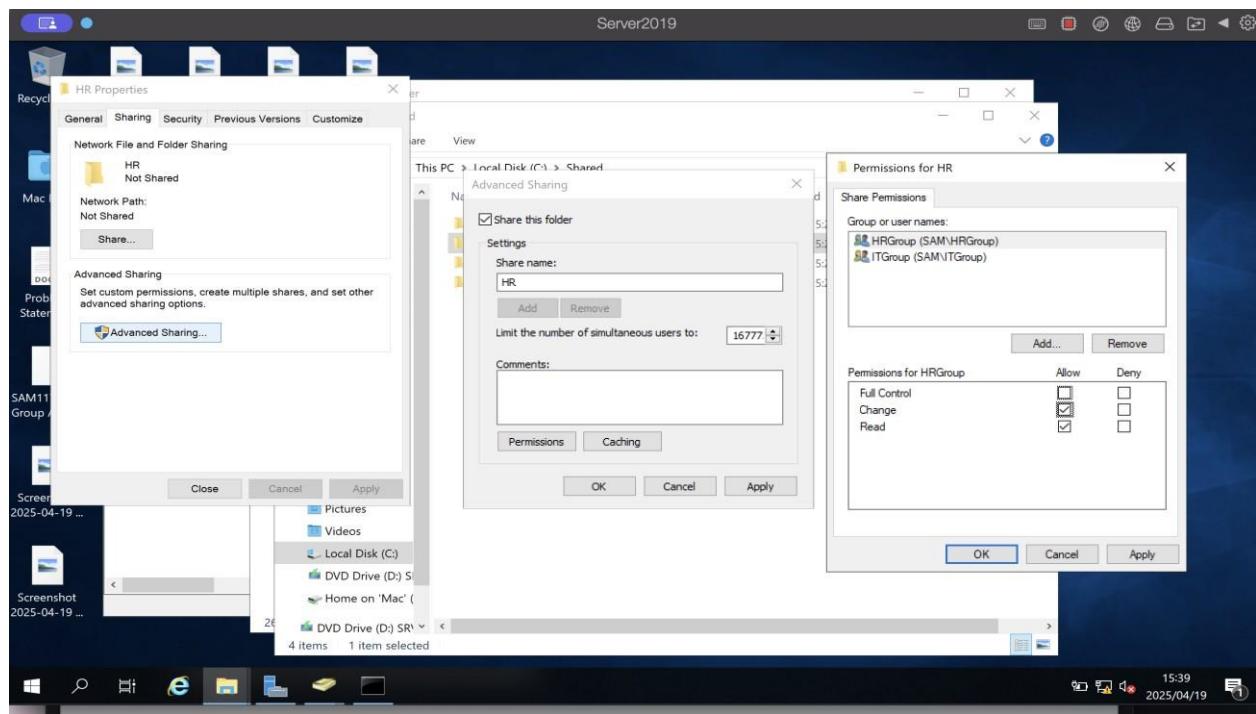




Shared Folder Access IT Group permissions

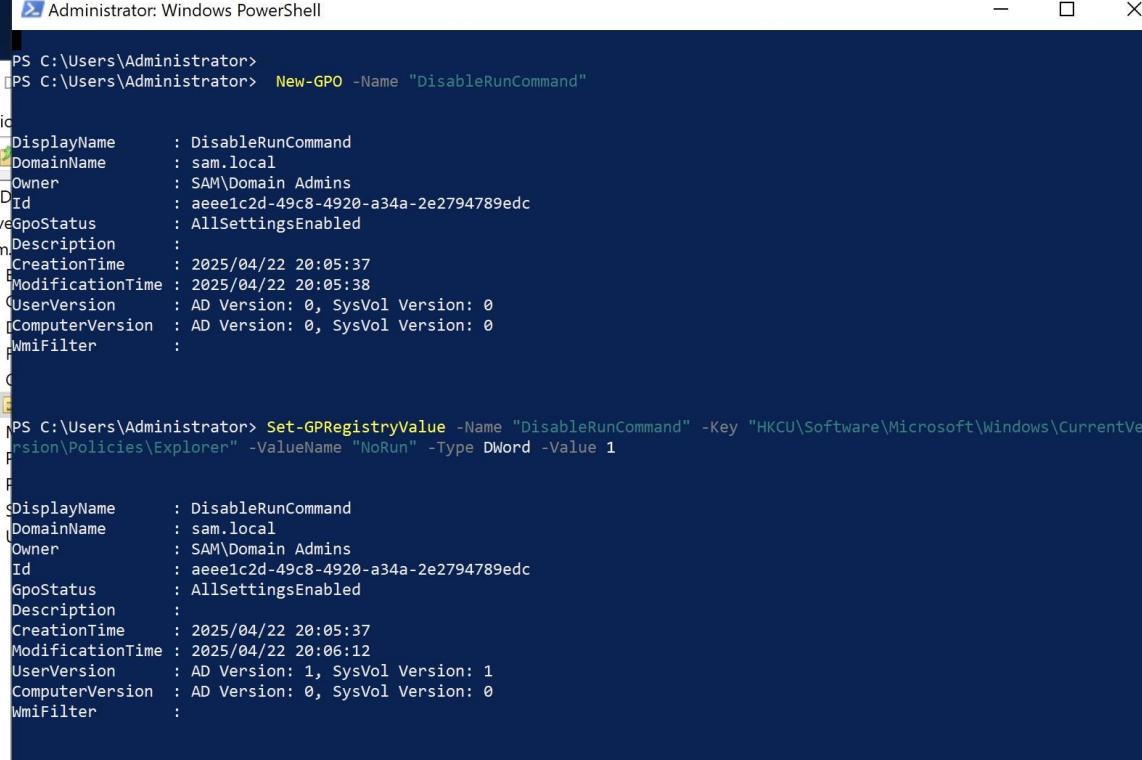


HR Permissions:



Disabling Run Function on HR, Finance and Procurement:

Creating GPO:



```
Administrator: Windows PowerShell

PS C:\Users\Administrator> New-GPO -Name "DisableRunCommand"

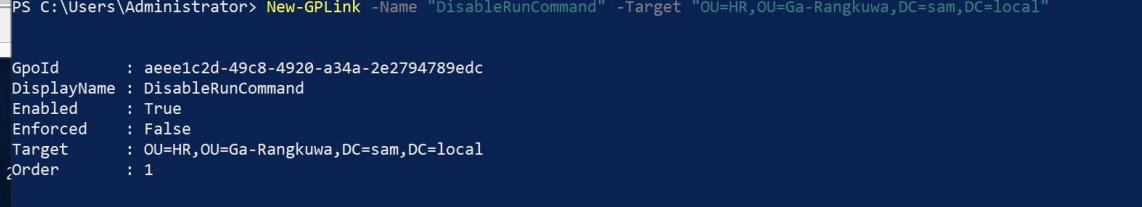
GPO
└─ DisplayName      : DisableRunCommand
   DomainName     : sam.local
   Owner          : SAM\Domain Admins
   Id             : aeee1c2d-49c8-4920-a34a-2e2794789edc
   GpoStatus      : AllSettingsEnabled
   Description    :
   CreationTime   : 2025/04/22 20:05:37
   ModificationTime: 2025/04/22 20:05:38
   UserVersion    : AD Version: 0, SysVol Version: 0
   ComputerVersion: AD Version: 0, SysVol Version: 0
   WmiFilter      :

PS C:\Users\Administrator> Set-GPRegistryValue -Name "DisableRunCommand" -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" -ValueName "NoRun" -Type DWord -Value 1

PS C:\Users\Administrator>

GPO
└─ DisplayName      : DisableRunCommand
   DomainName     : sam.local
   Owner          : SAM\Domain Admins
   Id             : aeee1c2d-49c8-4920-a34a-2e2794789edc
   GpoStatus      : AllSettingsEnabled
   Description    :
   CreationTime   : 2025/04/22 20:05:37
   ModificationTime: 2025/04/22 20:06:12
   UserVersion    : AD Version: 1, SysVol Version: 1
   ComputerVersion: AD Version: 0, SysVol Version: 0
   WmiFilter      :
```

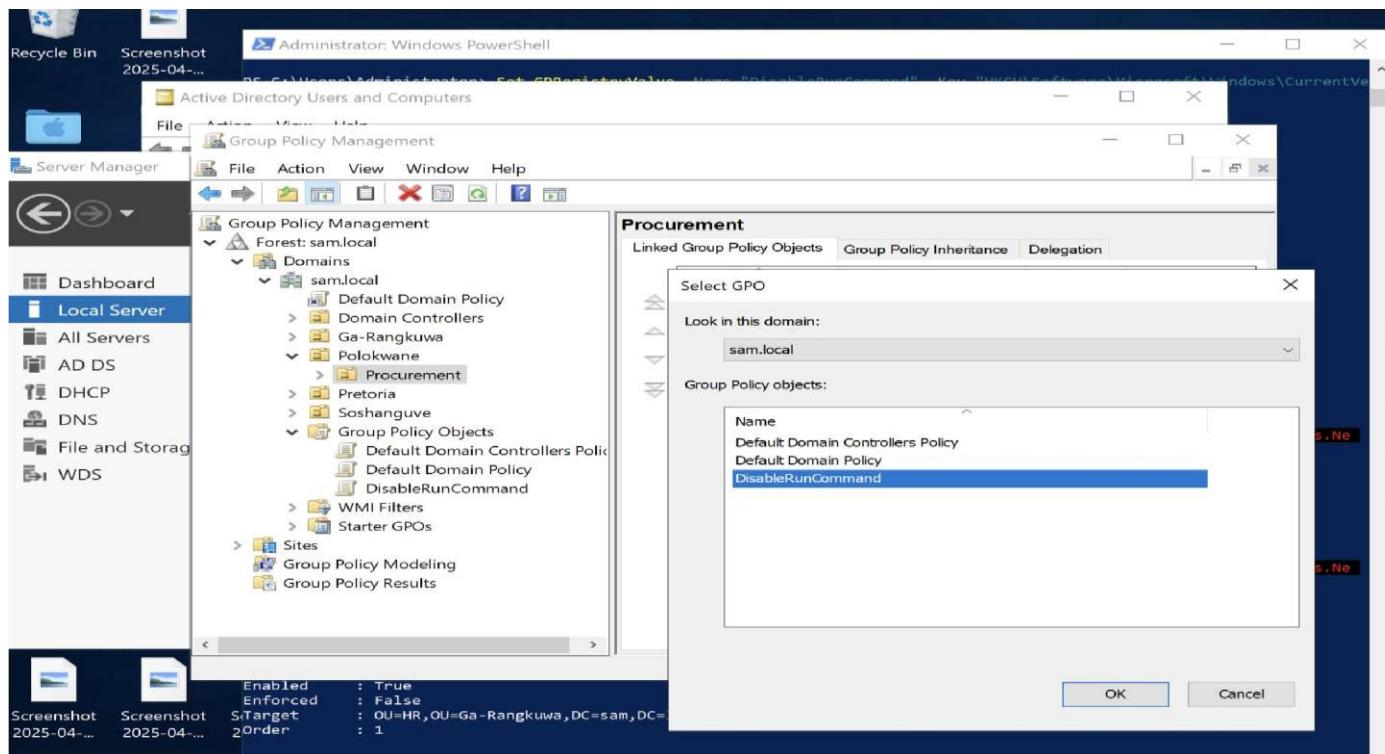
Linking GPO to the OU:



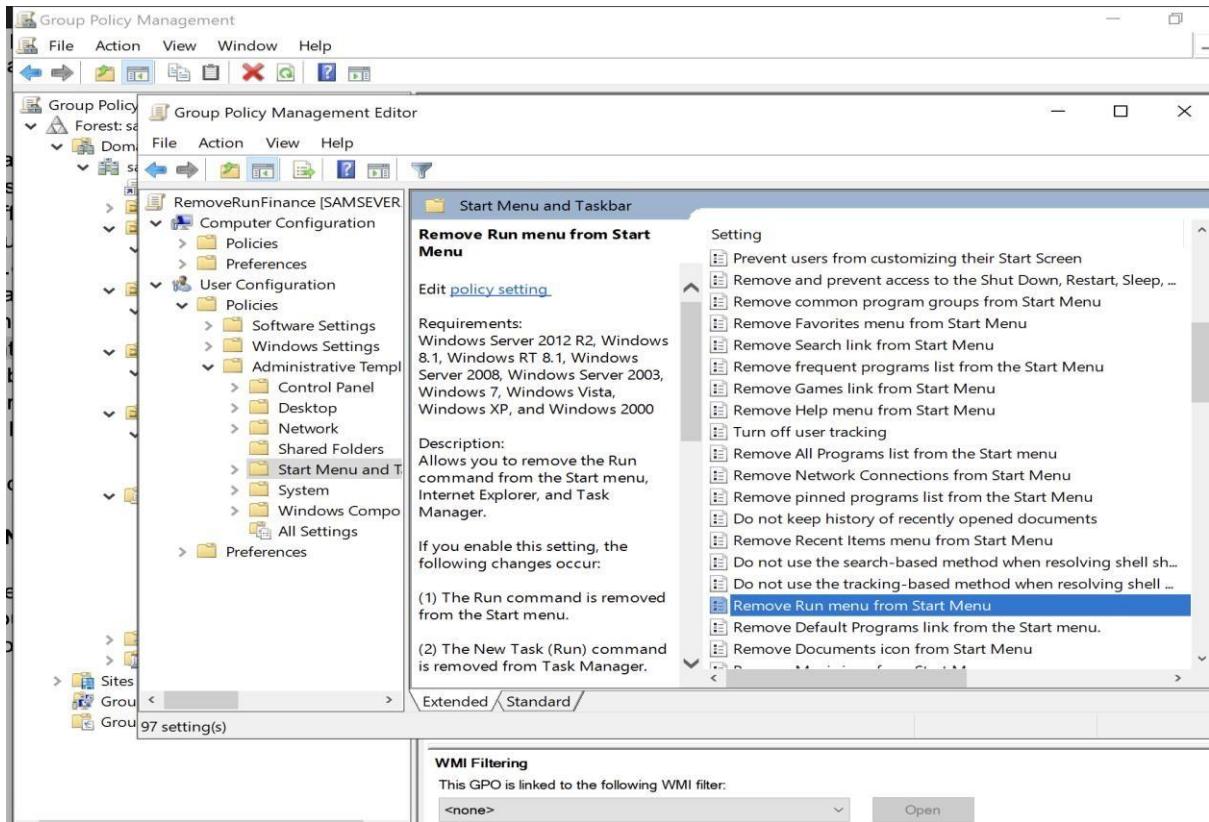
```
Administrator: Windows PowerShell

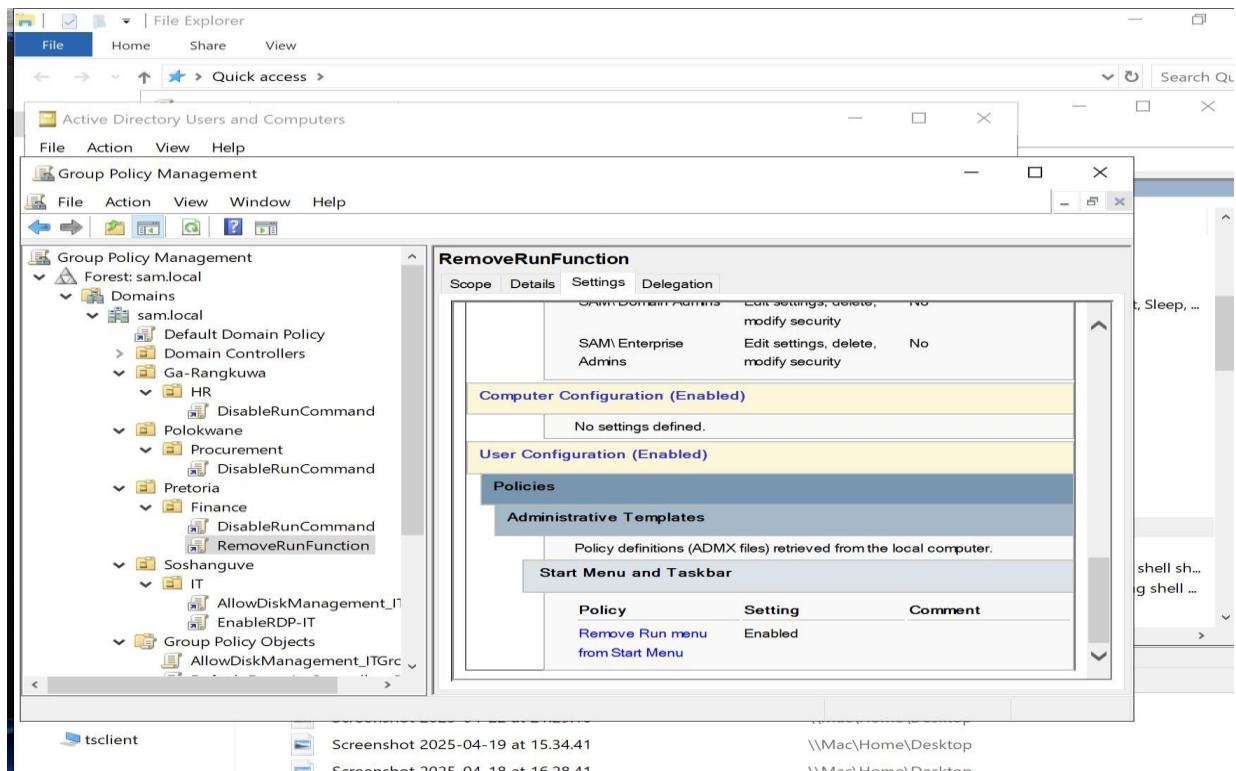
PS C:\Users\Administrator> New-GPLink -Name "DisableRunCommand" -Target "OU=HR,OU=Ga-Rangkuwa,DC=sam,DC=local"

GPOLink
└─ GpoId      : aeee1c2d-49c8-4920-a34a-2e2794789edc
   DisplayName : DisableRunCommand
   Enabled    : True
   Enforced   : False
   Target     : OU=HR,OU=Ga-Rangkuwa,DC=sam,DC=local
   Order      : 1
```



Remove Run from Finance:





Disabling Run Function on HR and Procurement

Location	Enforced	Link Status	Path
HR	No	Enabled	sam.local/Ga-Rangkuwa/ HR
Procurement	No	Enabled	sam.local/Polokwane/ Procurement
Finance	No	Enabled	sam.local/Pretoria/ Finance

This list only includes links in the domain of the GPO.

Name
NT AUTHORITY\Authenticated Users

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 Policy
 - 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

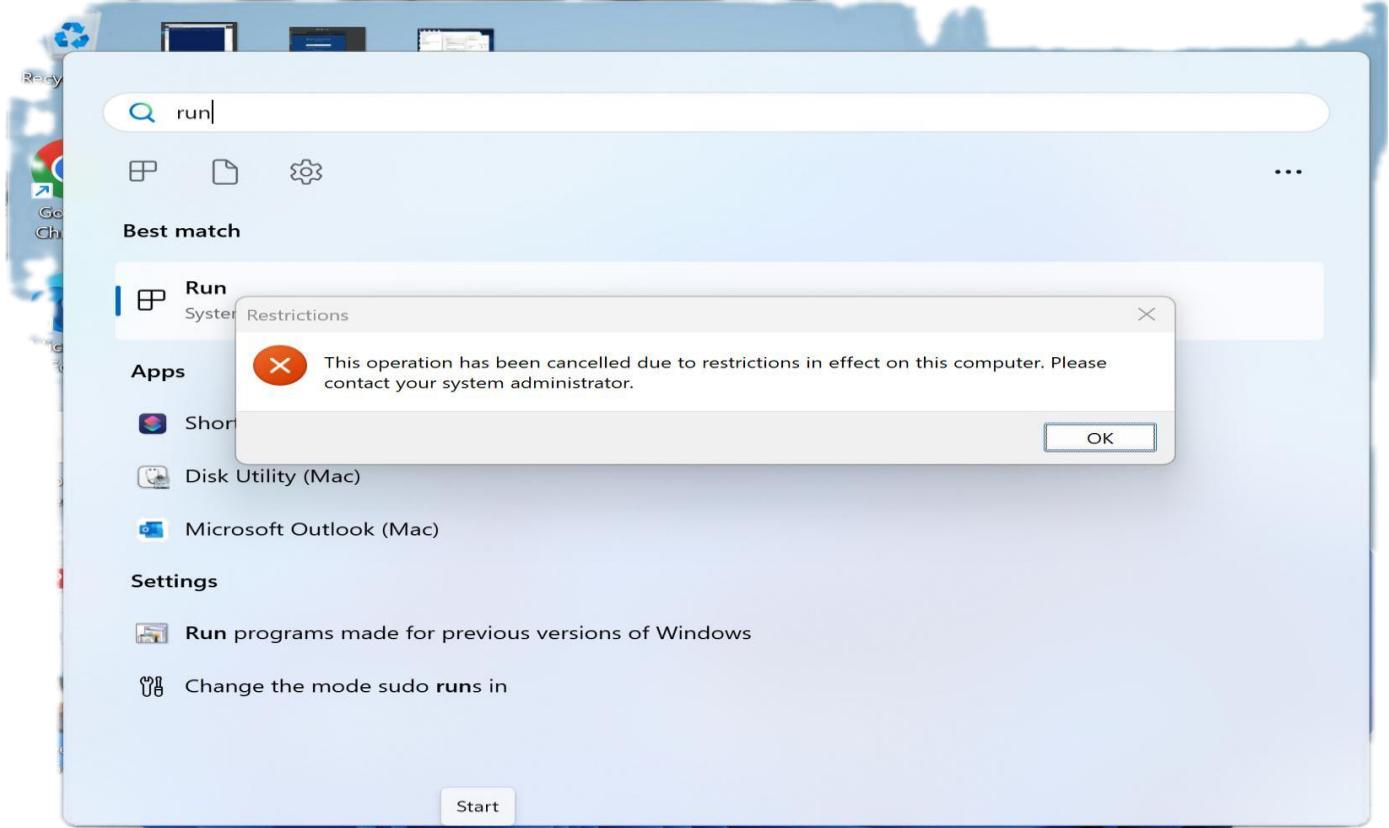
Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

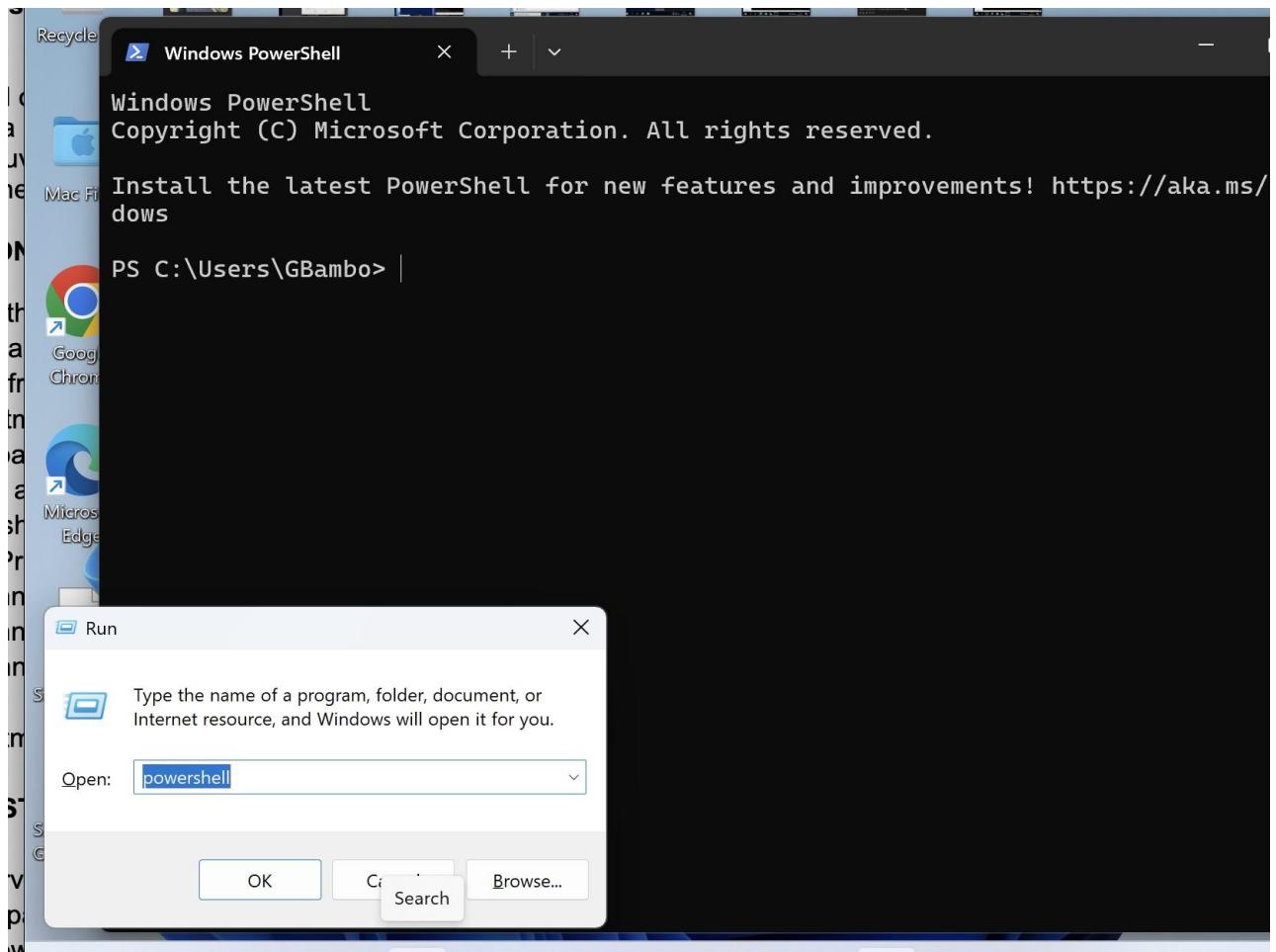
Start Menu and Taskbar

Policy	Setting	Comment
Remove Run menu from Start Menu	Enabled	

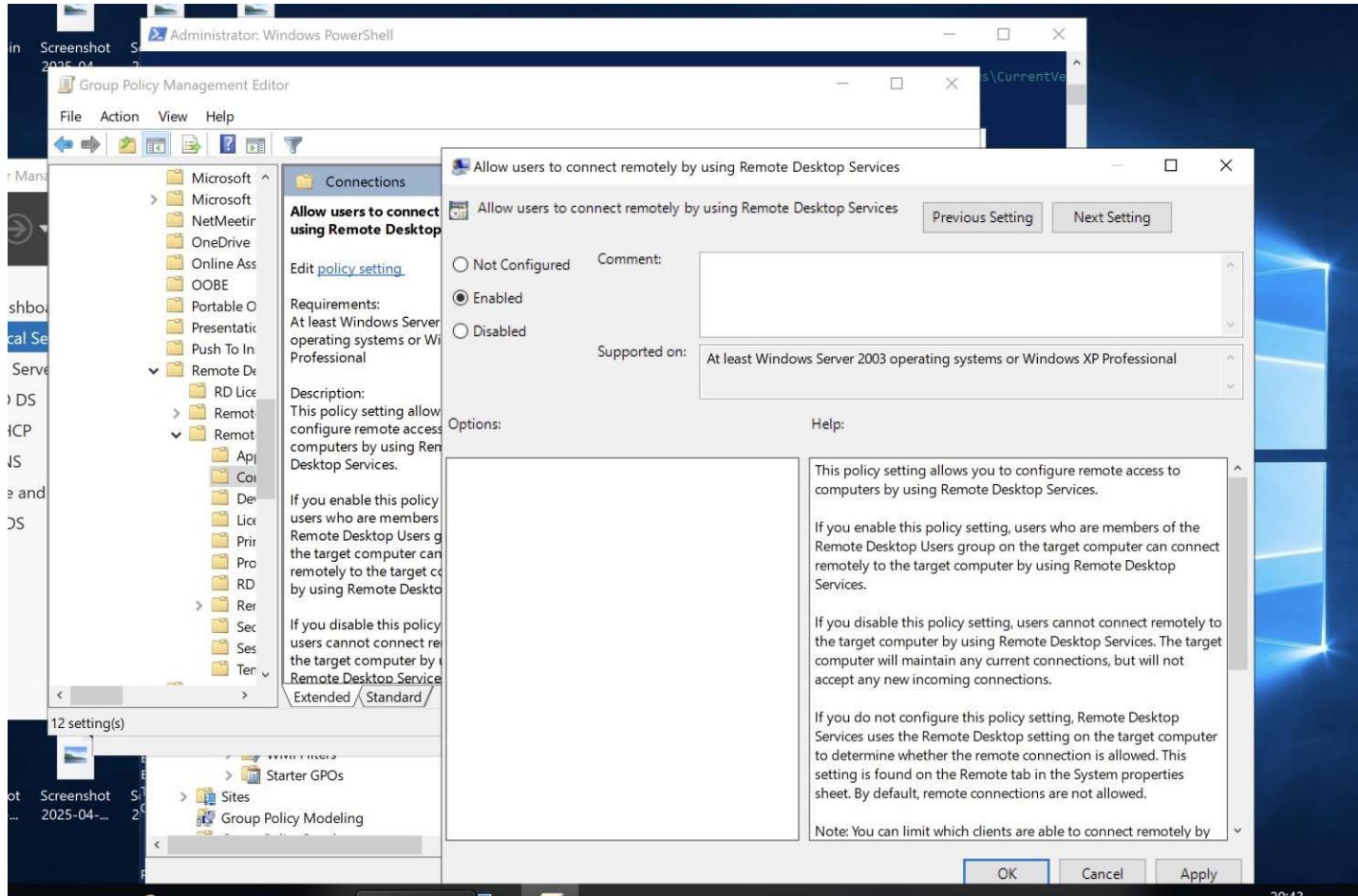
Testing Run Command



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



Enabling RDP on ITGroup



GPO for enabling RDP

The screenshot shows the Windows Server 2012 Group Policy Management console. The left navigation pane shows the Active Directory structure under 'Forest: sam.local'. In the main pane, a GPO named 'EnableRDP-IT' is selected. The 'Details' tab is active, displaying the following information:

- Links:** The GPO is linked to the domain 'sam.local'.
- Security Filtering:** The GPO applies to the security group 'ITGroup (SAM\ITGroup)'.
- WMI Filtering:** The GPO is linked to the WMI filter 'DisableRunCommand'.

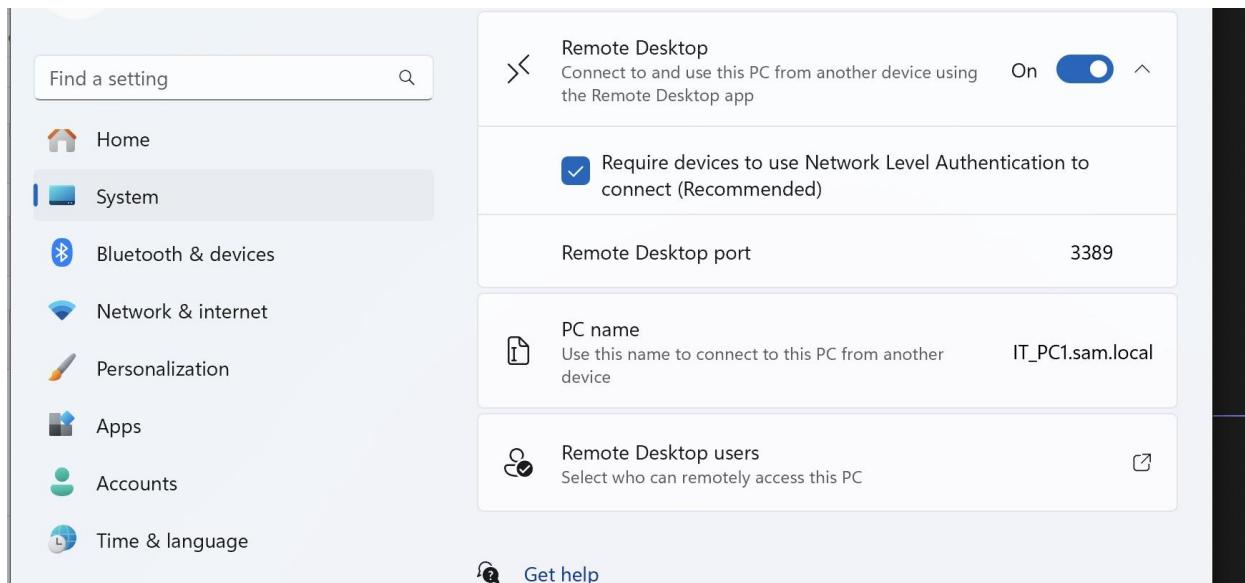
Below the main pane, a PowerShell window is open, showing the command used to link the GPO to the domain:

```
PS C:\Users\Administrator> New-GPLink -Name "DisableRunCommand" -Target "OU=HR, DC=sam, DC=local"
```

This screenshot shows the 'Delegation' tab of the Group Policy Management console. It lists the GPOs linked to the 'IT' organizational unit (OU) in the 'sam.local' domain. The table shows:

Link Order	GPO	Enforced	Link Enabled	Group
1	EnableRDP-IT	No	Yes	IT

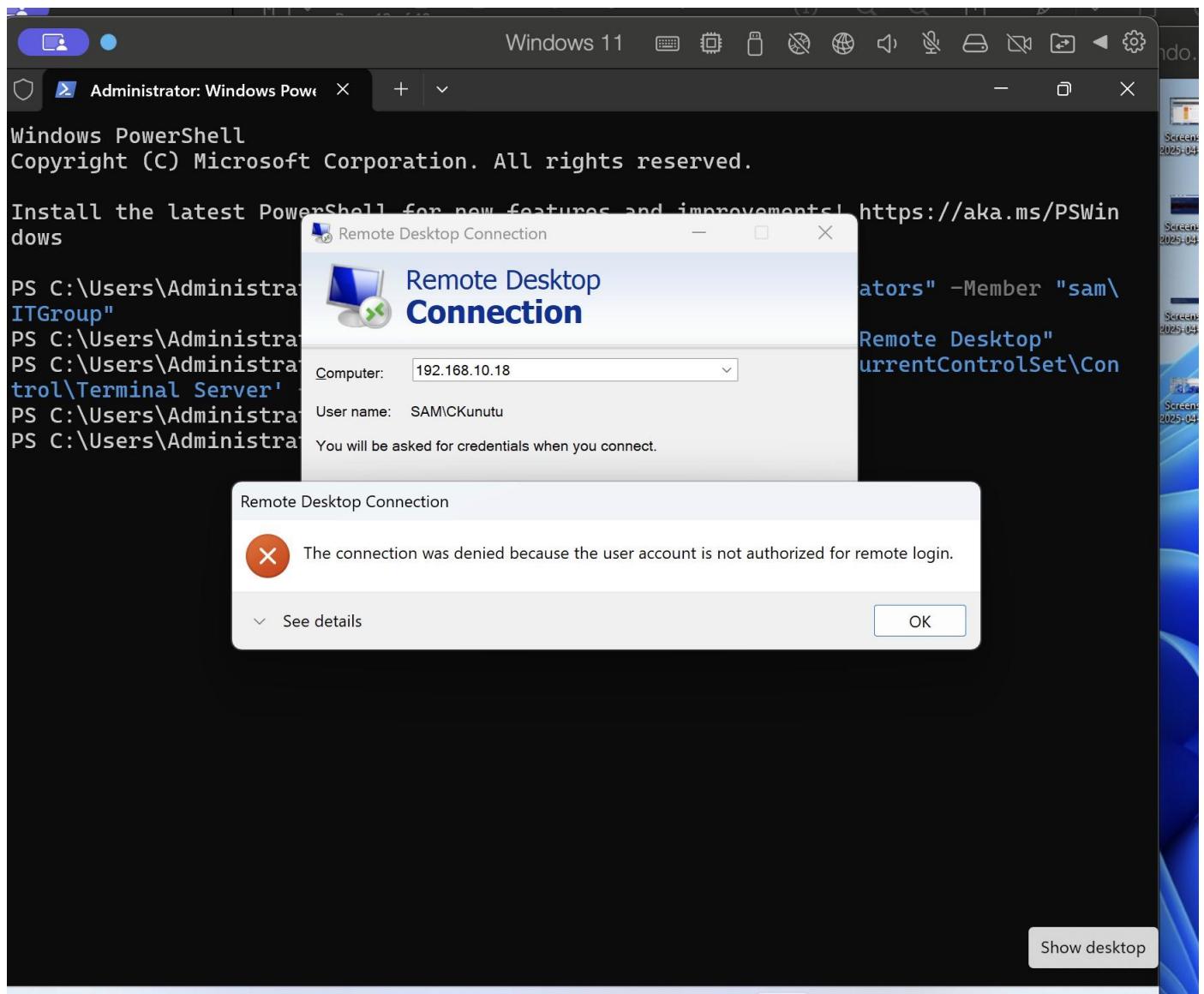
At the bottom of the screen, a portion of the Server Manager interface is visible, showing the status of various services and components on the local server.



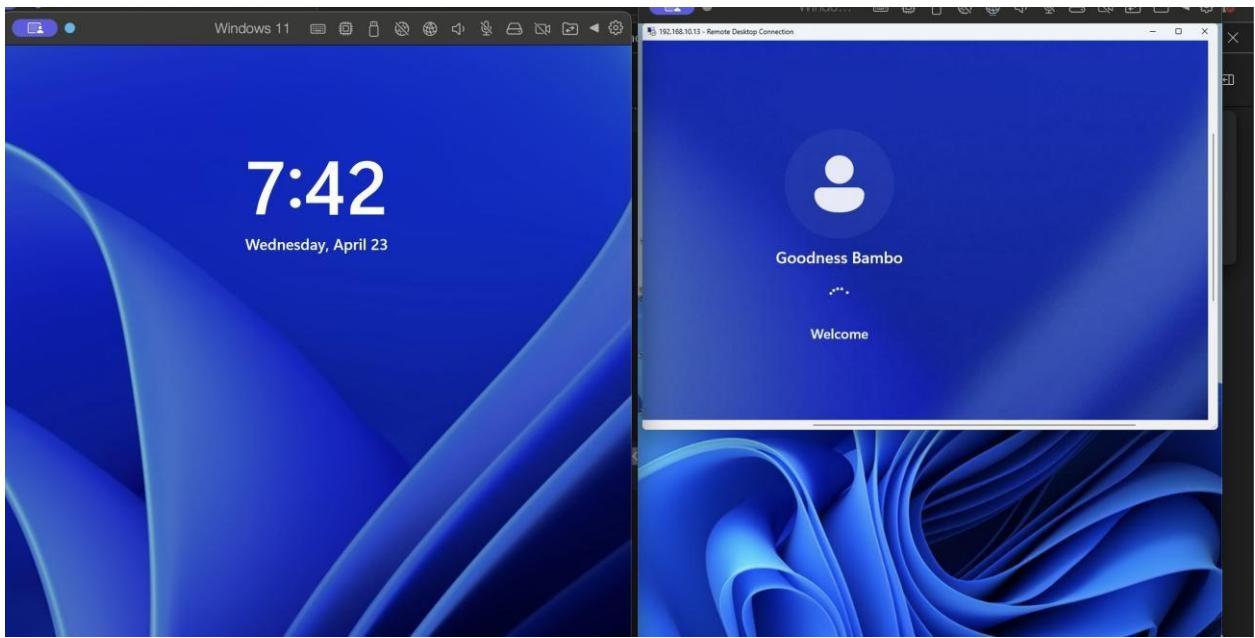
PowerShell command to enable Enable Remote Desktop | Add domain group to local Administrators | Open RDP port in firewall

```
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>
```

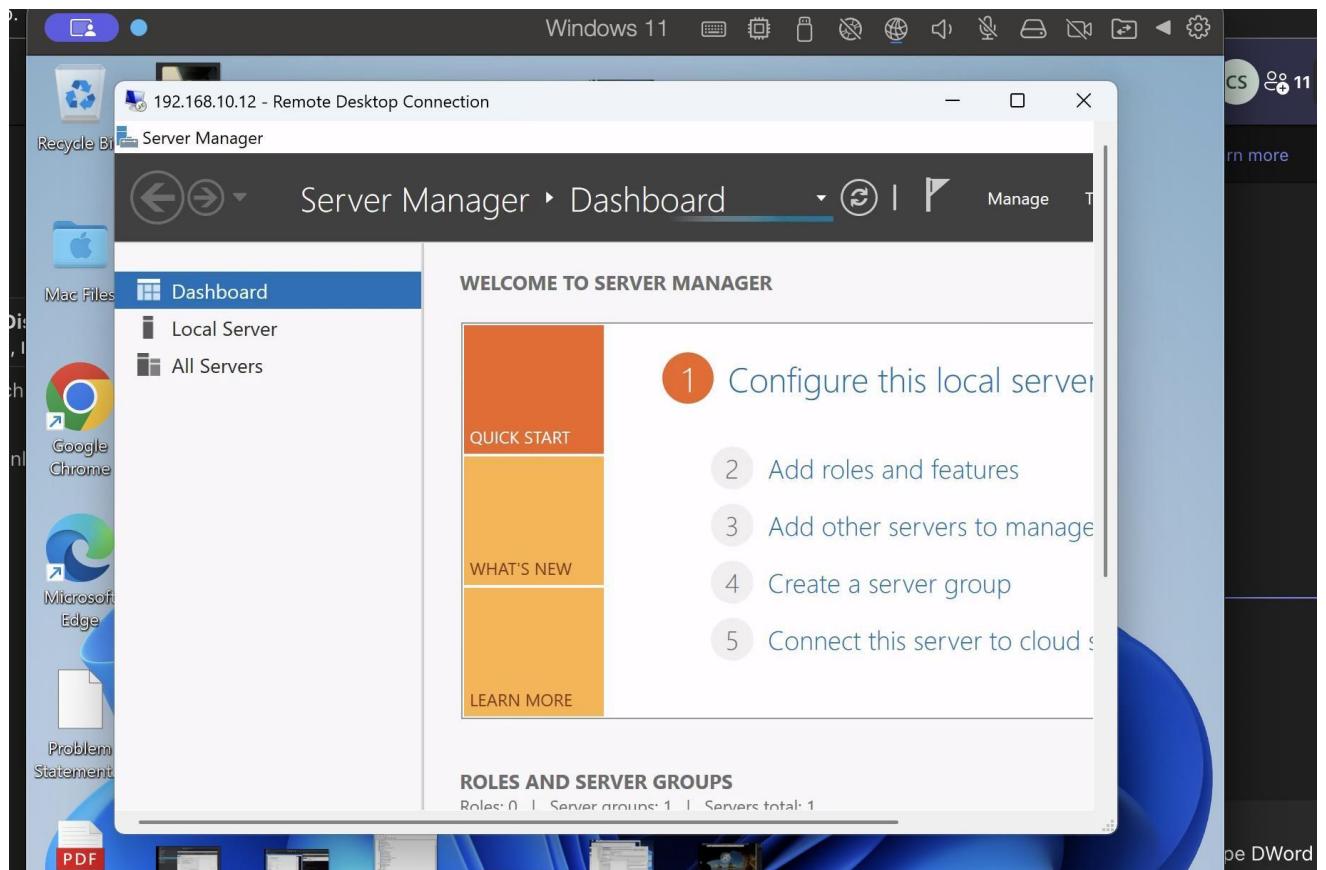
Testing with user not linked to the Enabling RDP



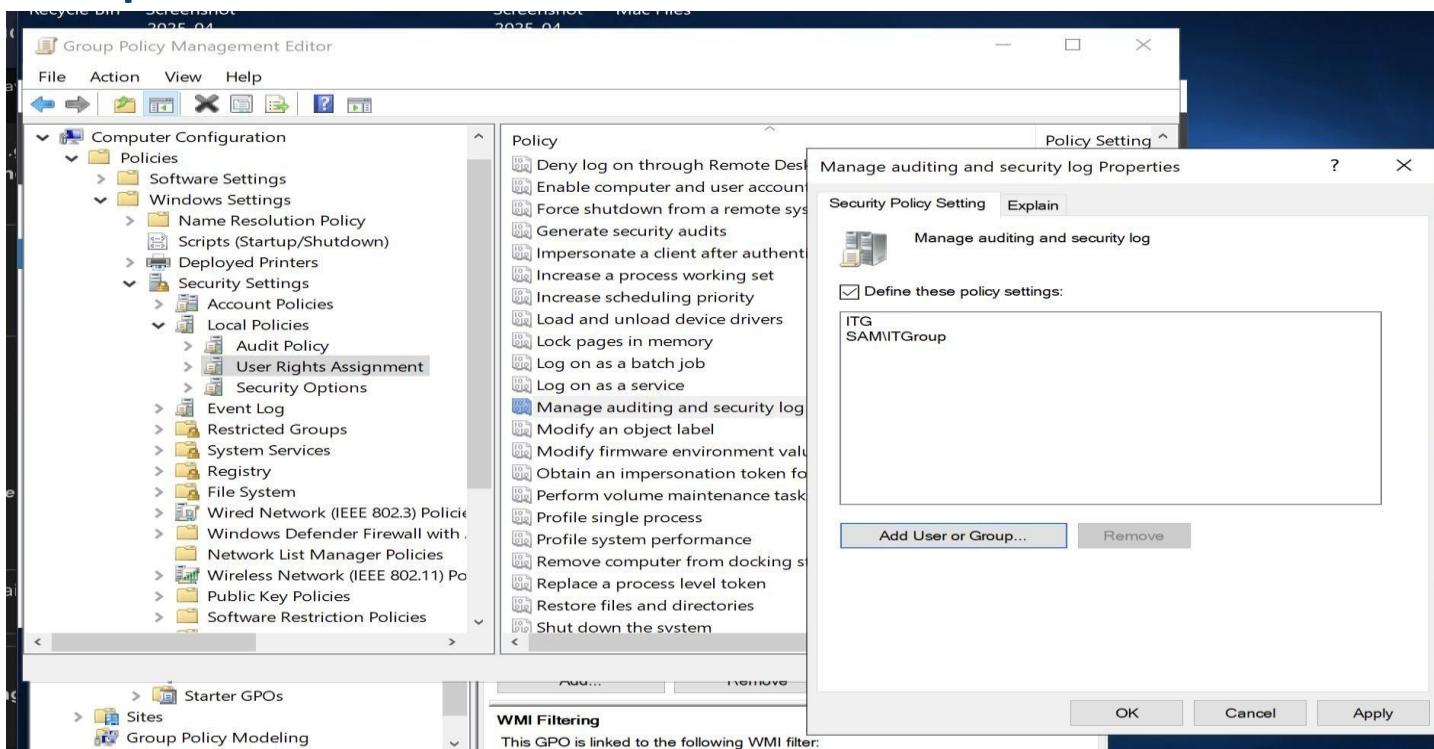
Authorized user was able to Remote



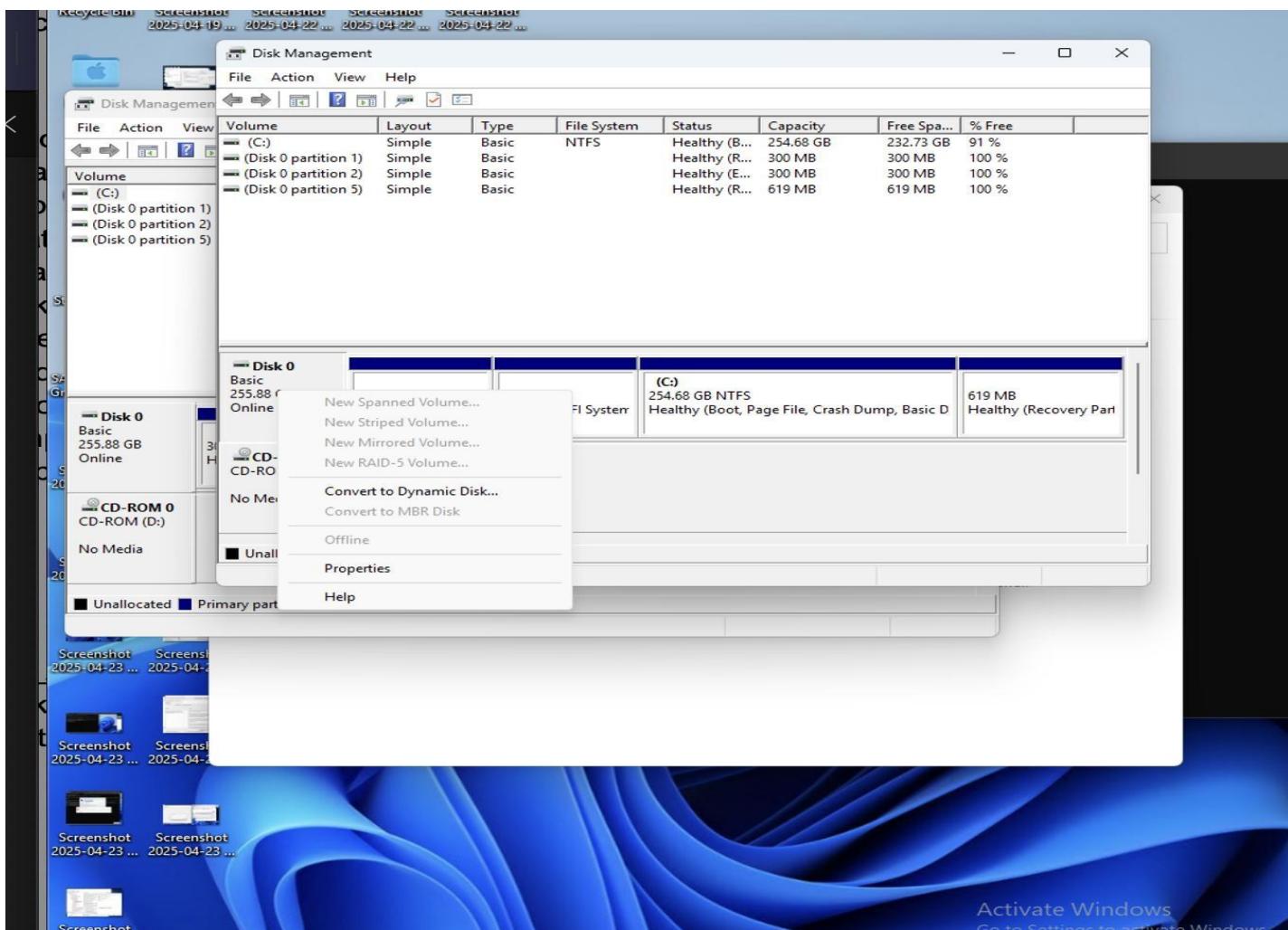
Remote to the Server

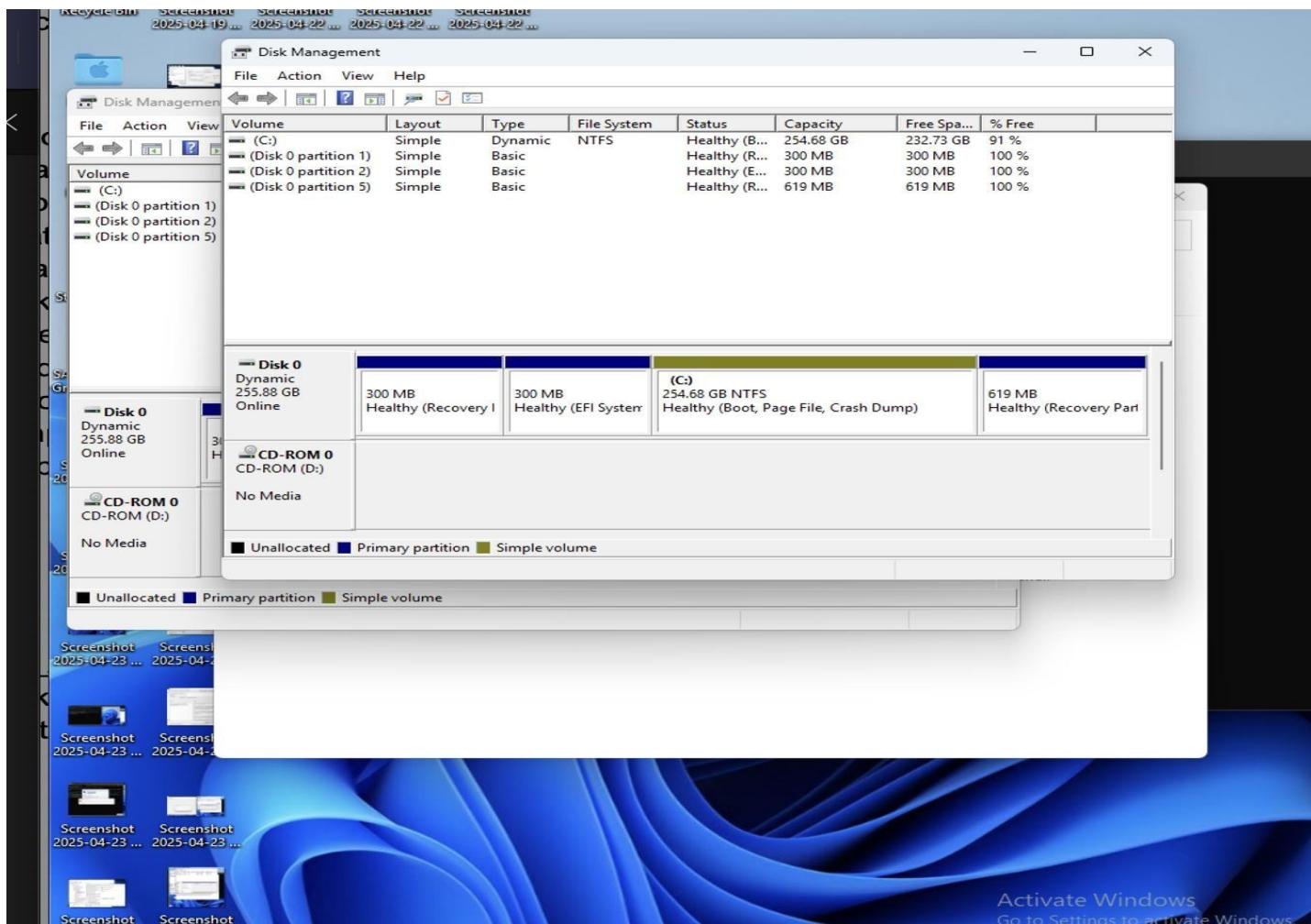


Departments' basic disk to a dynamic disk and configure the disk quotas

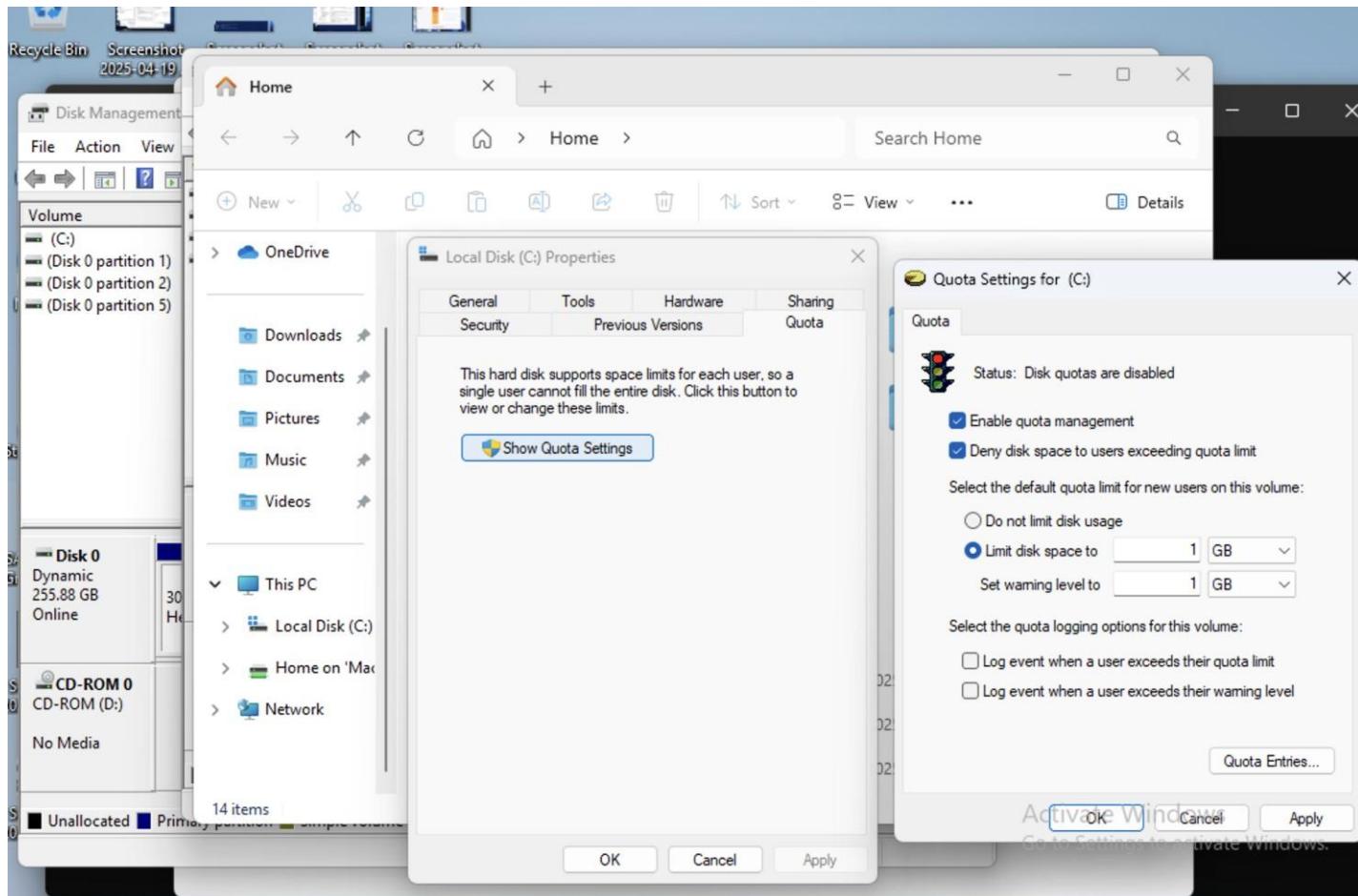


IT Personnel being able to convert Disk to a dynamic disk



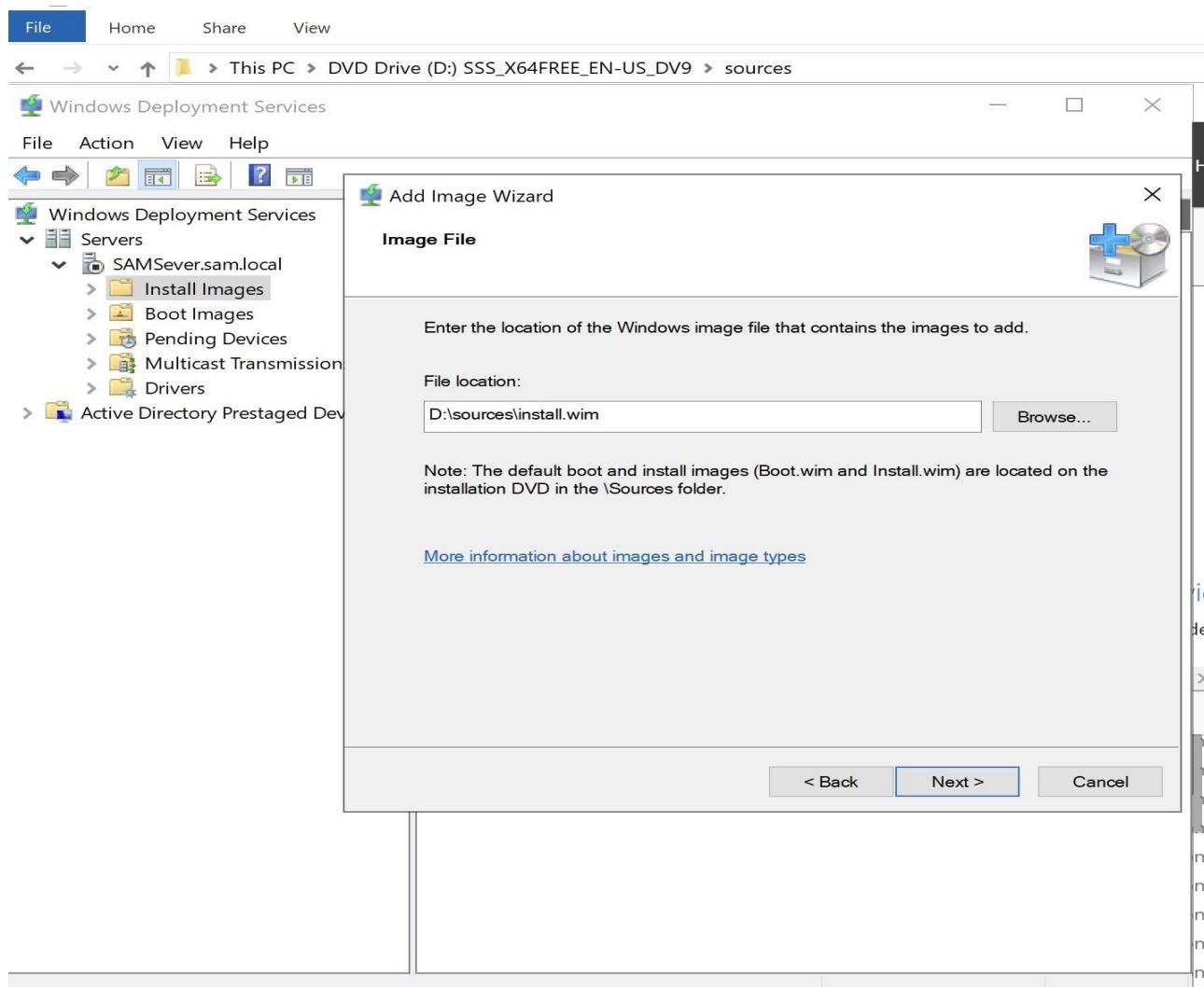


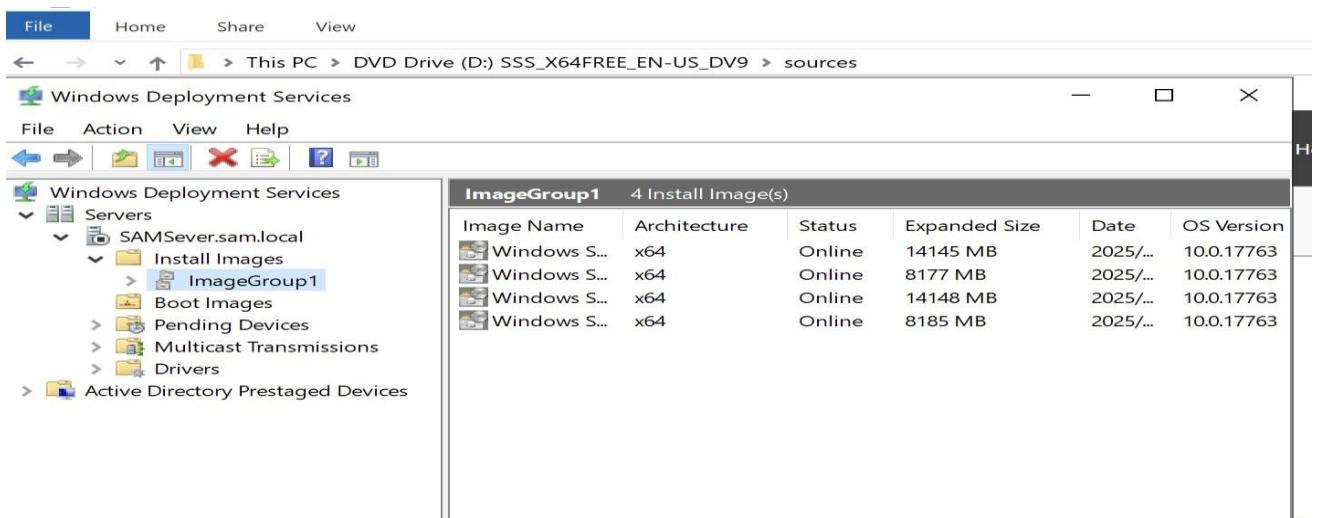
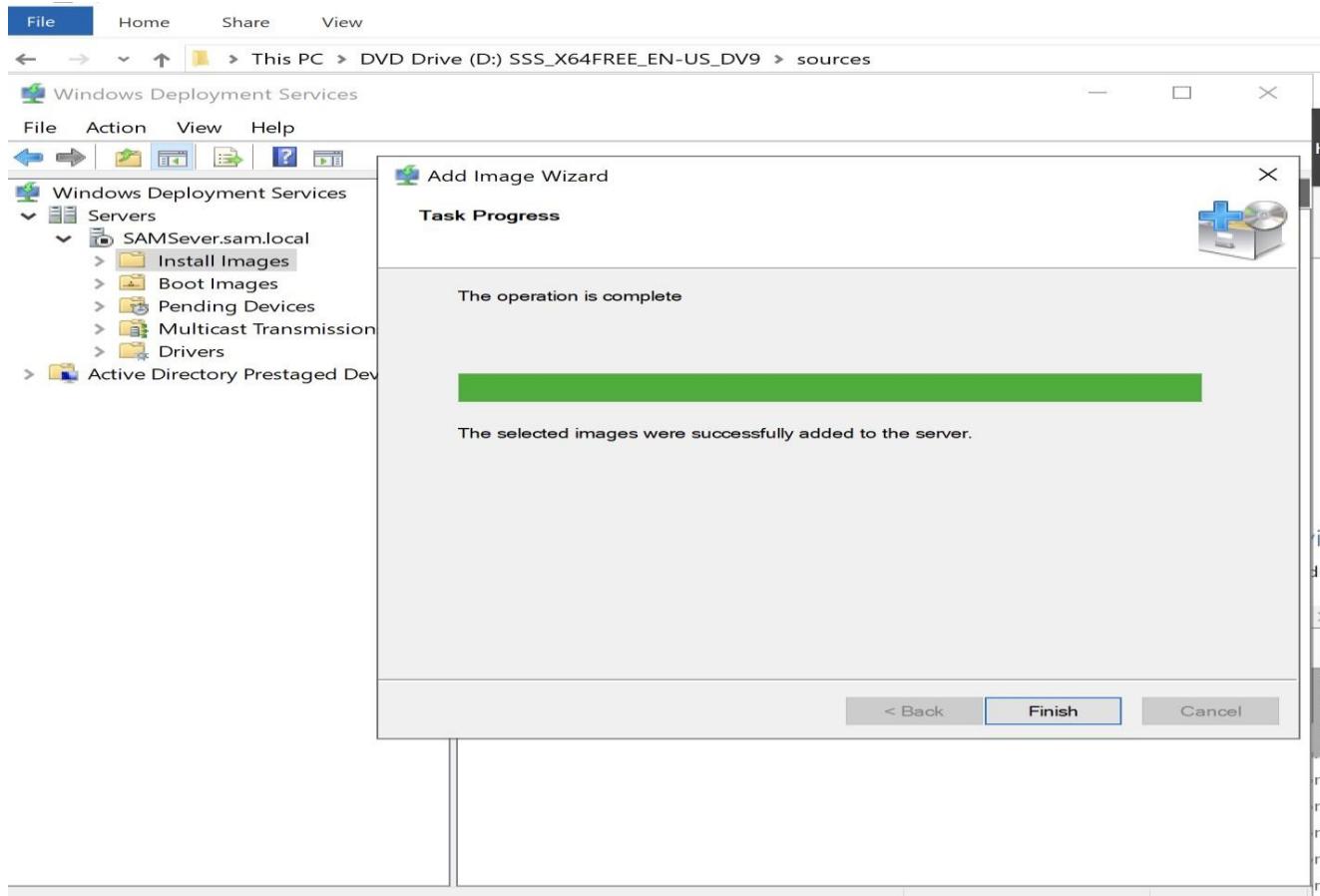
Configure the disk quotas



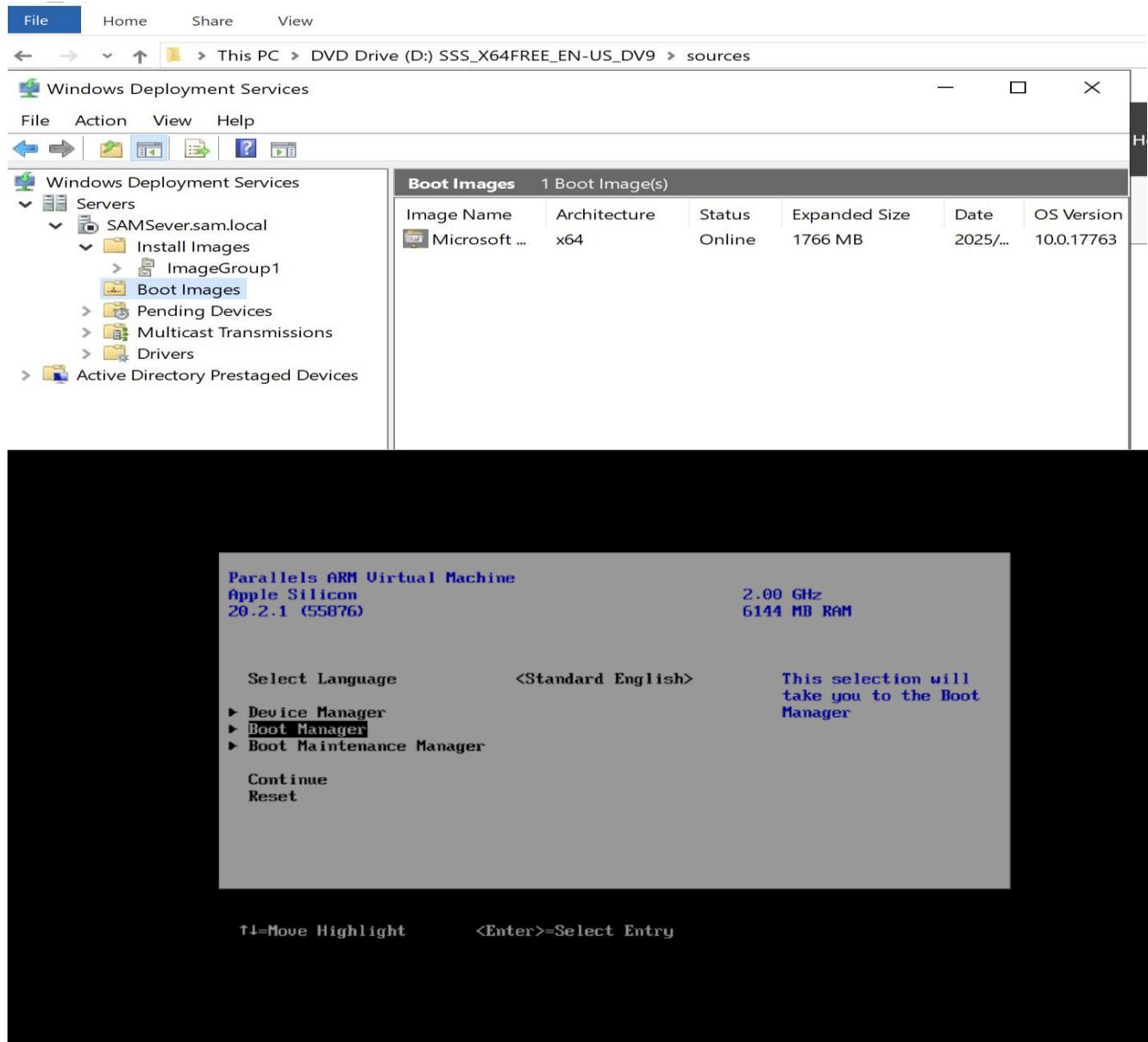
IT Department must be able to deploy servers, images and apps automatically to other machine

Installing Images

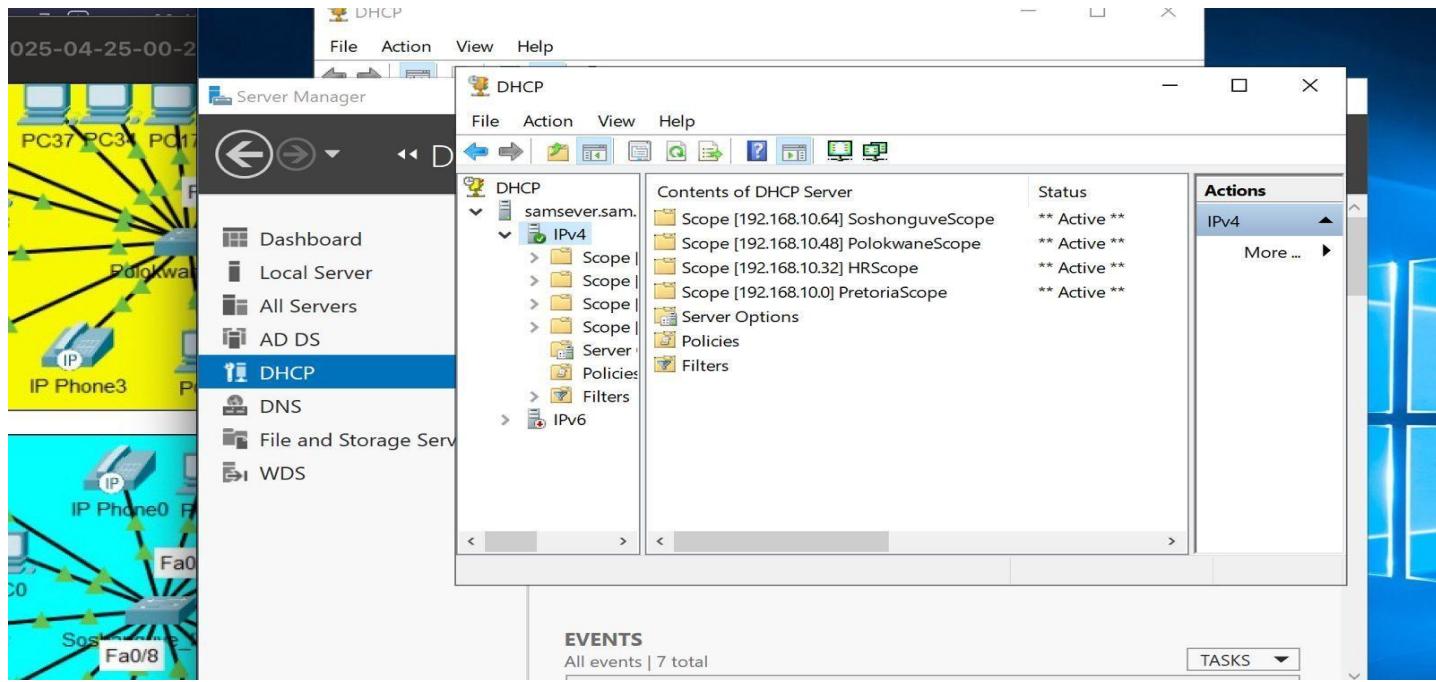




Boot Images:



DHCP IP Address Scope



DNS Forward Lookup Zones

DNS Manager

File Action View Help

File Manager

Name	Type	Data	Time
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[386], samsever.sam.local, h...	standard
(same as parent folder)	Name Server (NS)	samsever.sam.local.	standard
(same as parent folder)	Host (A)	192.168.10.12	2014-01-01 00:00:00
(same as parent folder)	IPv6 Host (AAAA)	fdb2:2c26:f4e4:0003:a03e:3e...	2014-01-01 00:00:00
Finance_PC	Host (A)	192.168.10.14	2014-01-01 00:00:00
Finance_PC	IPv6 Host (AAAA)	fdb2:2c26:f4e4:0003:0b59:f1...	2014-01-01 00:00:00
HR_PC	Host (A)	192.168.10.15	2014-01-01 00:00:00
HR_PC	IPv6 Host (AAAA)	fdb2:2c26:f4e4:0003:1e91:61...	2014-01-01 00:00:00
IT_PC	Host (A)	192.168.10.16	2014-01-01 00:00:00
IT_PC	IPv6 Host (AAAA)	fdb2:2c26:f4e4:0003:ce2f:8c...	2014-01-01 00:00:00
IT_PC1	Host (A)	192.168.10.13	2014-01-01 00:00:00
PC2	Host (A)	192.168.10.14	2014-01-01 00:00:00
Procurement_PC	Host (A)	192.168.10.17	2014-01-01 00:00:00
Procurement_PC	IPv6 Host (AAAA)	fdb2:2c26:f4e4:0003:6c21:02...	2014-01-01 00:00:00
samsever	Host (A)	192.168.10.12	standard
samsever	IPv6 Host (AAAA)	fdb2:2c26:f4e4:0003:a03e:3e...	standard
www	Host (A)	192.168.10.12	

DNS Reverses Lookup Zones

DNS Manager

File Action View Help

DNS

SAMSEVER

- Forward Lookup Zones
 - _msdcs.sam.local
 - sam.local
- Reverse Lookup Zones
 - 10.168.192.in-addr.arpa
- Trust Points
- Conditional Forwarders

Name	Type	Data	Time
(same as parent folder)	Start of Authority (SOA)	[5], samsever.sam.local., hos...	stat
(same as parent folder)	Name Server (NS)	samsever.sam.local.	stat
192.168.10.12	Pointer (PTR)	www.sam.local.	stat
192.168.10.14	Pointer (PTR)	Finance_PC.sam.local.	202
192.168.10.16	Pointer (PTR)	IT_PC.sam.local.	202
192.168.10.17	Pointer (PTR)	Procurement_PC.sam.local.	202

```
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>
```