IT INFRASTRUCTURE

Cloud Computing and CyberSecurity

WINDOWS SERVER ADMINISTRATION

Prepared By : Rajeev Khoodeeram

Submitted To : Mr Mohammed Ghori

28 April 2025

Microsoft Active Directory

Contents

Work environment

1.1 Configuration of VMs

Two different "hosts" are used in this configuration : one on a **MAC Laptop** (hosting Server 1 and one Windows 11 Client; and the second host on a **Linux Laptop** hosting the Server2 (and Server 3 and 4 for bonus as Failover Cluster).With the exception of Server 2 which has been installed via pxeboot over network from Server1, the remaining virtual computers have been configured through normal installation and domain joined to rajeevkhoodeeram.com.

The on-premise Active Directory has been synchronized with **Microsoft Entra ID** and **Intune** (Hybrid cloud solution) via Microsoft Entra Connect Sync (previously known as Azure AD Connect). At the same time, remote management of the on-premise devices on AD can be done using **Microsoft Azure** (portal.azure.com; see right DOUBLE green arrow) using Azure ARC installed on Windows Server 1.

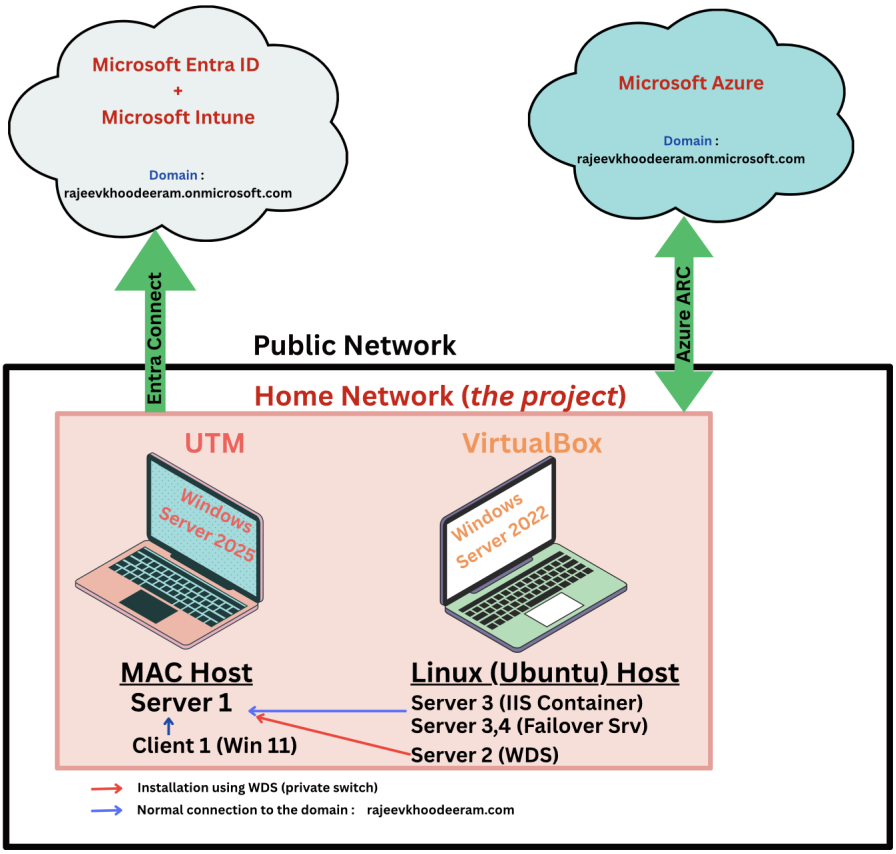


Figure 1.1: A global view of the working environment of the project and beyond

STEP 1

2.1 Installation of Server1, Active directory and domain

- Install a new VM called server1 that is connected to the External virtual switch.

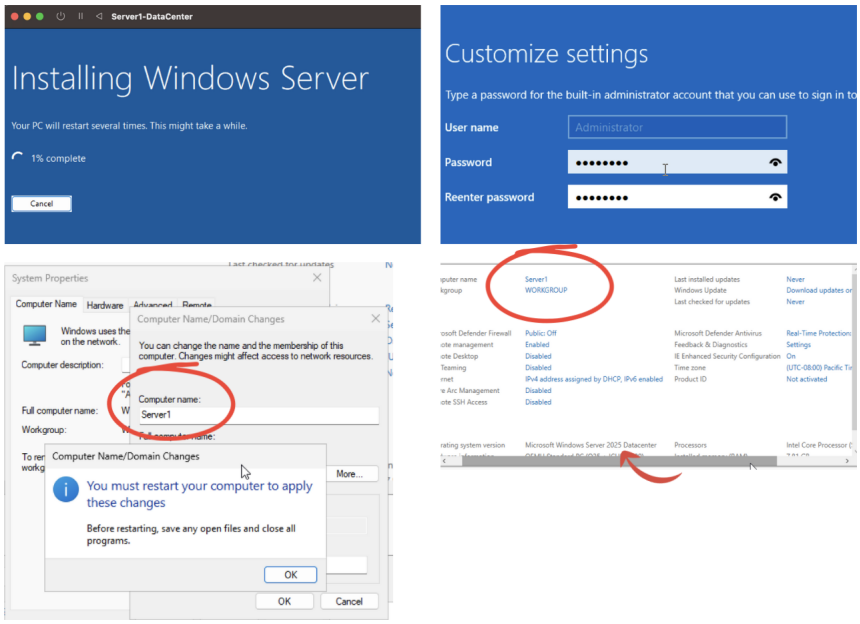


Figure 2.1: Installation of Server 1

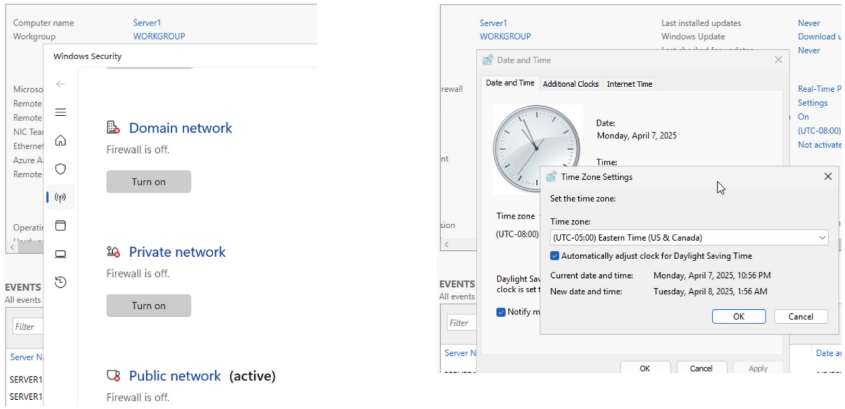


Figure 2.2: Changing default firewall settings and timezone

- Add a second NIC to server1 that is connected to the Private virtual switch and assign it a static IP of 192.168.255.1. Configure an Active Directory domain on server1 that hosts a new domain in a new forest called yourname.com.

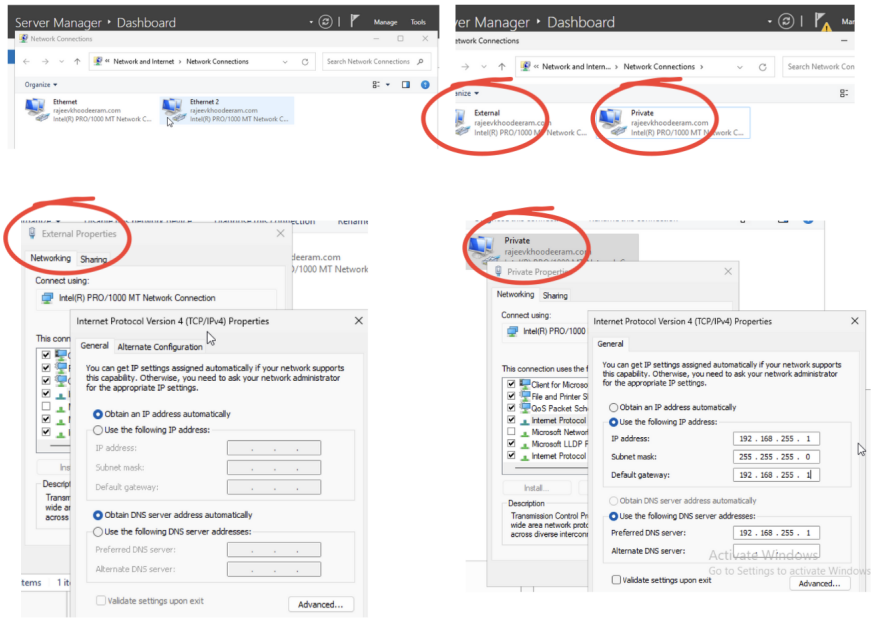


Figure 2.3: Configuring External and private switches

- Ensure that server1 is a global catalog and that your domain and forest use the highest functional levels.

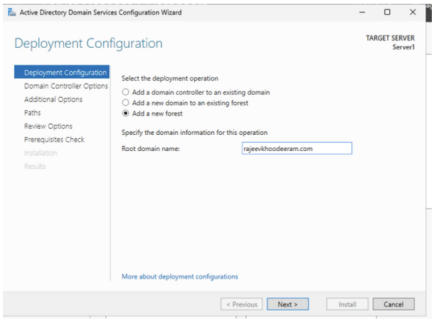


Figure 2.4: Configuring server1 as a global catalog

STEP 2

3.1 Configuration of Server1 as DHCP, DNS and WDS Server

- Configure server1 as a DHCP server that provides addresses to clients on the 192.168.255.0 network (192.168.255.100-200) and the DNS server 192.168.255.1.

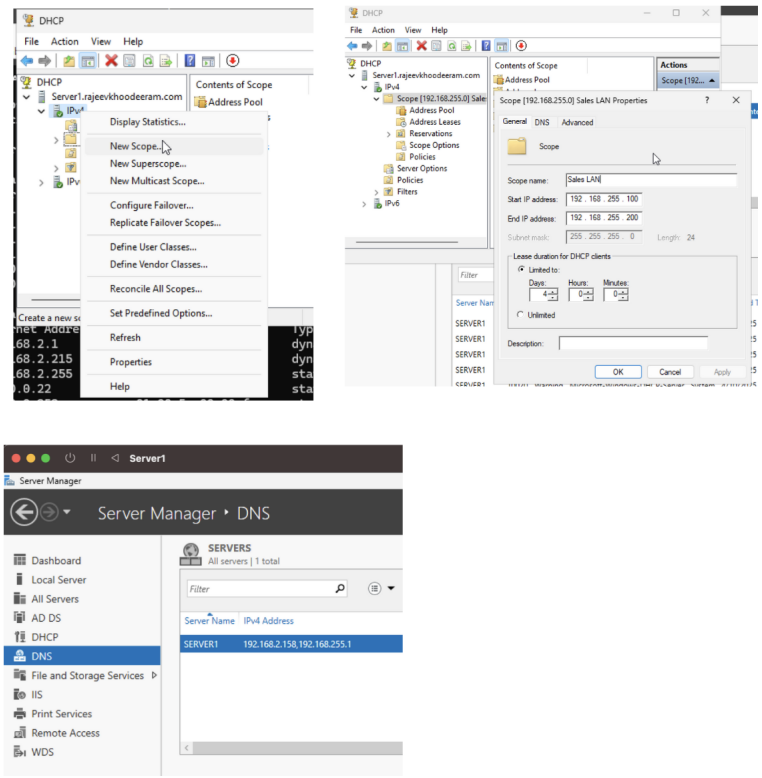


Figure 3.1: Configuration of DHCP and DNS

- Next, configure server1 as a WDS server that hosts the install.wim from the Windows Server 2022 DVD.

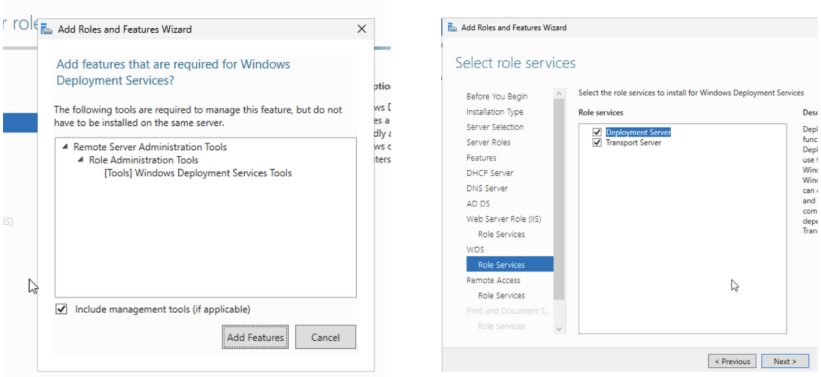


Figure 3.2: Installation of WDS server

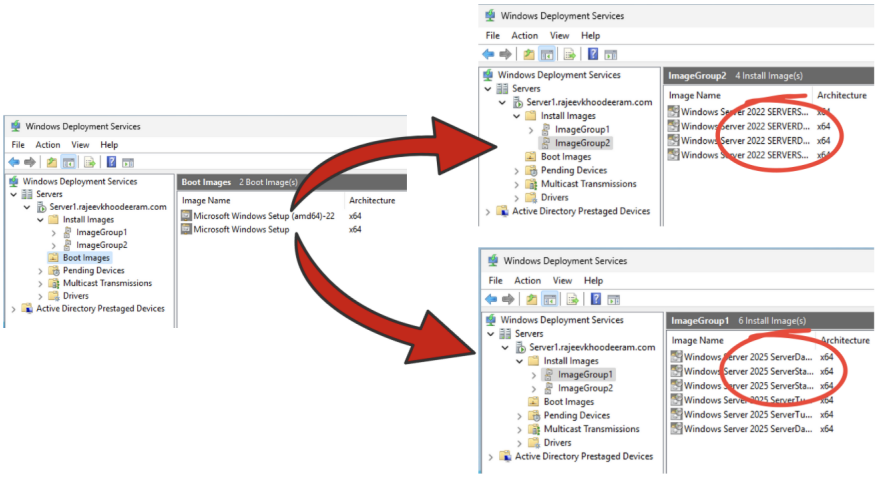


Figure 3.3: Configuration of boot and install images (Note there are two sets : one for Windows 2022 and one for Windows 2025)

- The WDS server should not join computers to the domain after installation.

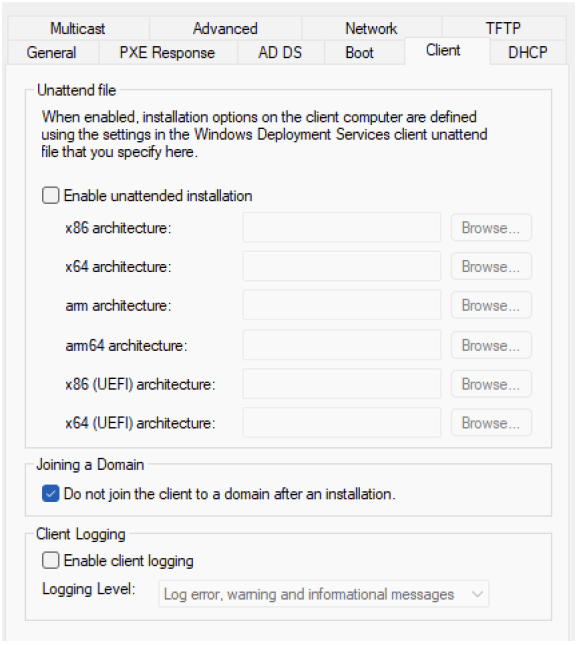


Figure 3.4: Client will not join domain

STEP 3

4.1 Using Windows Deployment Service (installation of Server2)

- Install server2 from your WDS server and set its static IP address and name afterwards.

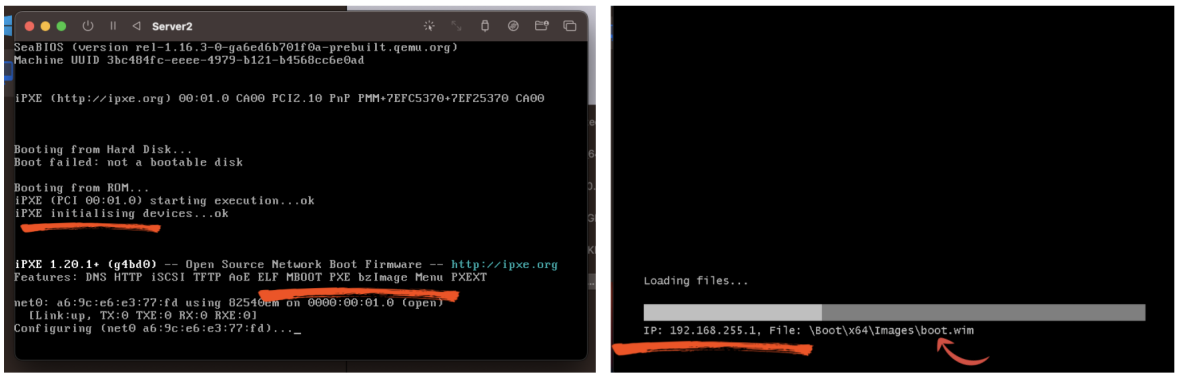


Figure 4.1: Installation of server2 using pxeboot

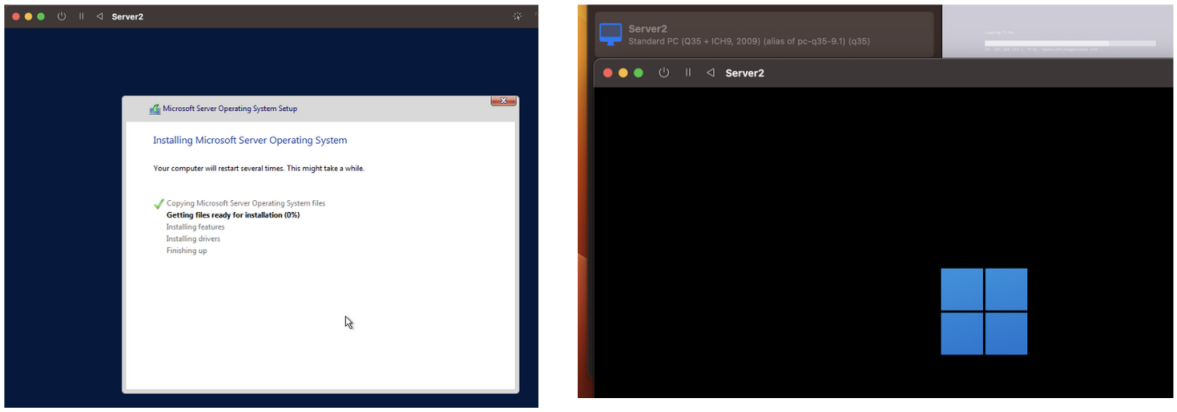


Figure 4.2: Configuration of Server2 IP Address

- Next, join it to your domain.

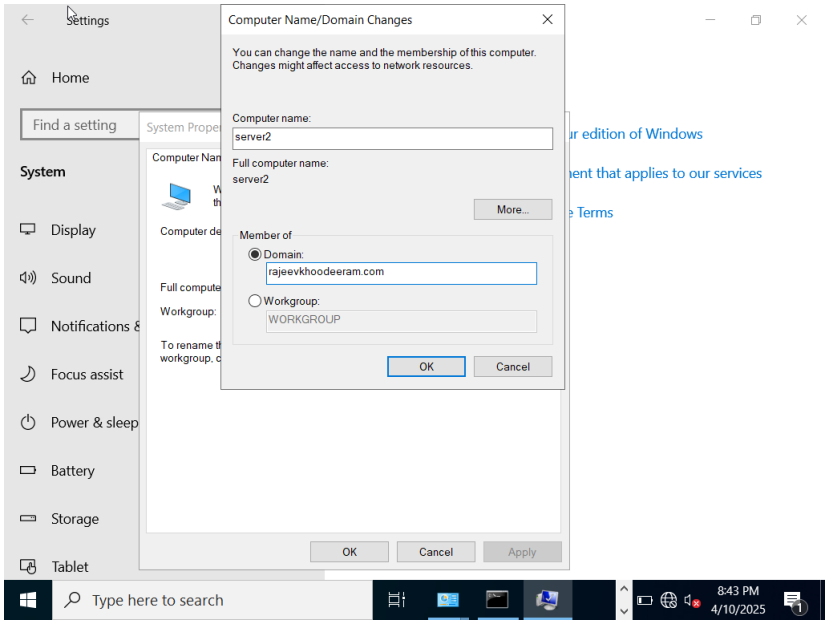


Figure 4.3: Joining server2 to the domain rajeevkhoodeeram.com

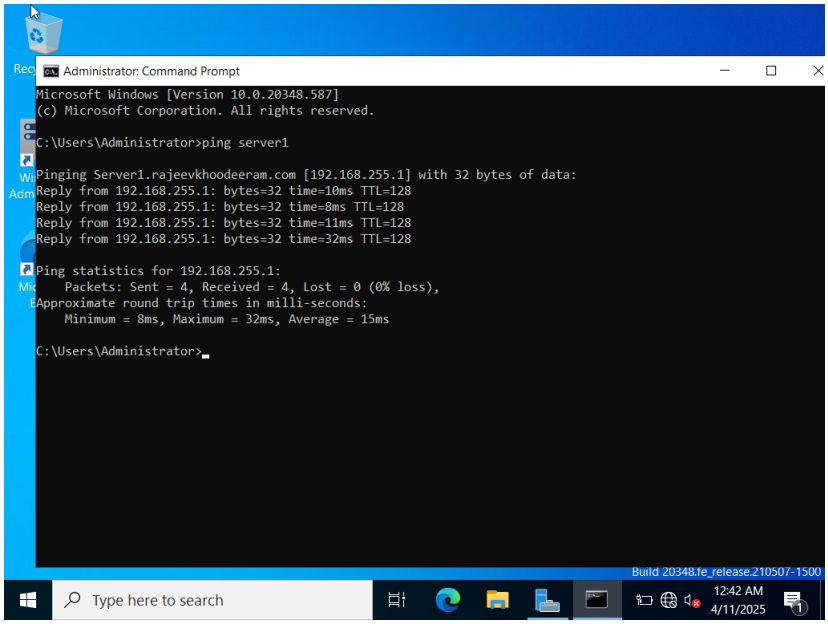


Figure 4.4: Testing connection to server1 using IP address / ping command

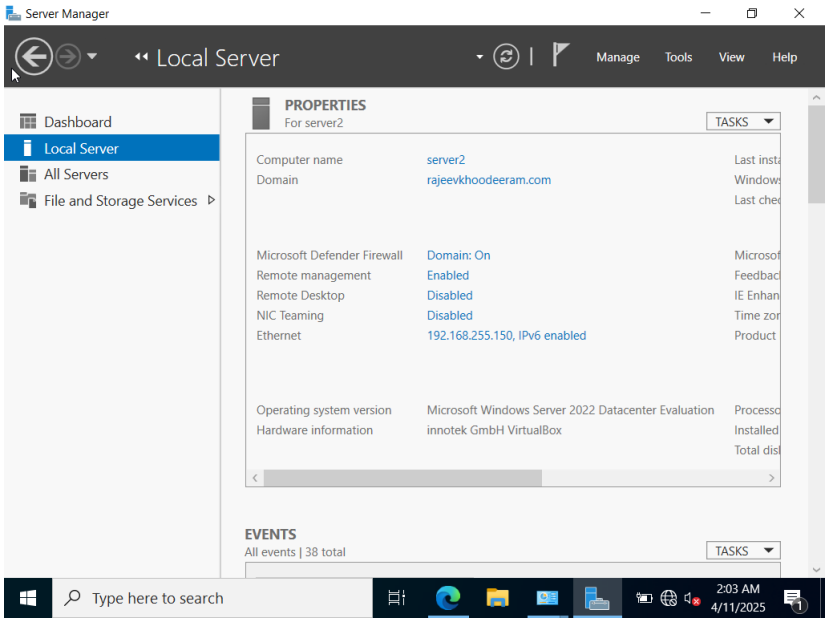


Figure 4.5: Server2 added to the domain

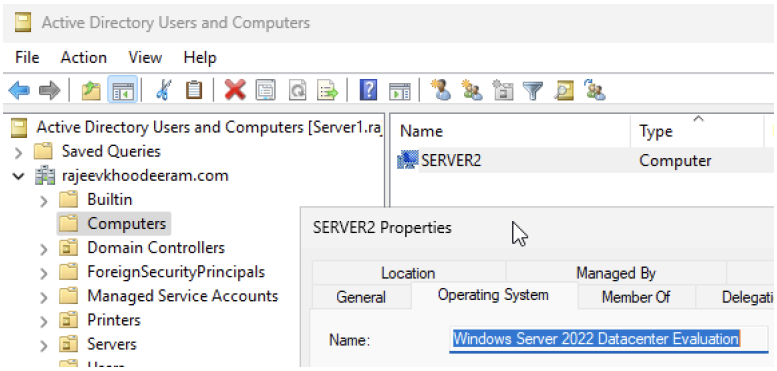


Figure 4.6: Showing the addition of server2 to the domain on server1

STEP 4

5.1 Configure the DHCP service on server1

- Modify the 192.168.255.0 scope you created earlier so that it is called “Sales LAN” and uses a lease period of 4 days. Ensure that the scope sets the default gateway and DNS server on the client to 192.168.255.1.

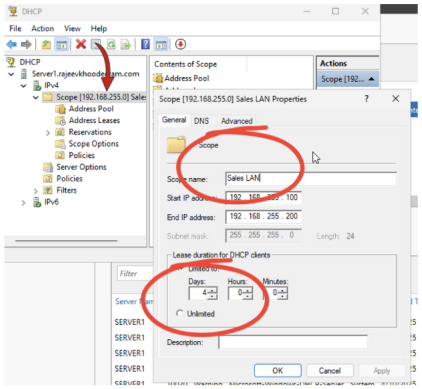


Figure 5.1: Modify the 192.168.255.0 scope to “Sales LAN”

- Add an exclusion to the scope for 192.168.255.188 (used by a UNIX server that has a static IP address) as well as the static IPs used by server1 and server2.

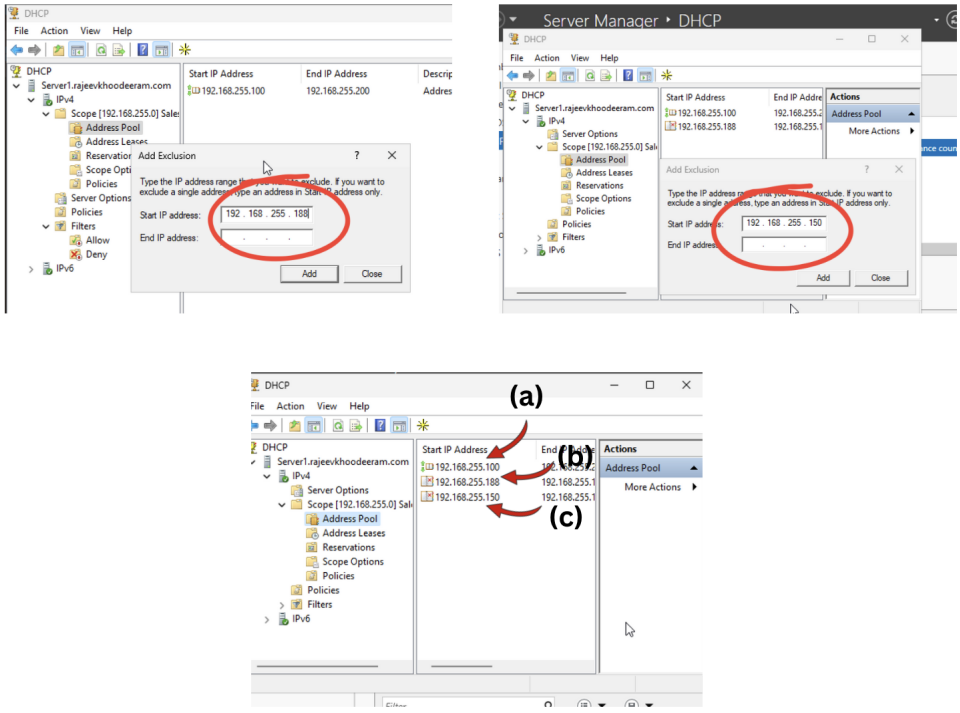


Figure 5.2: Adding exclusion to the scope 192.168.255.188

- Add a reservation called “Ricoh8320Printer” that assigns 192.168.255.191 to the MAC address 00-01-03-E1-0F-B7.

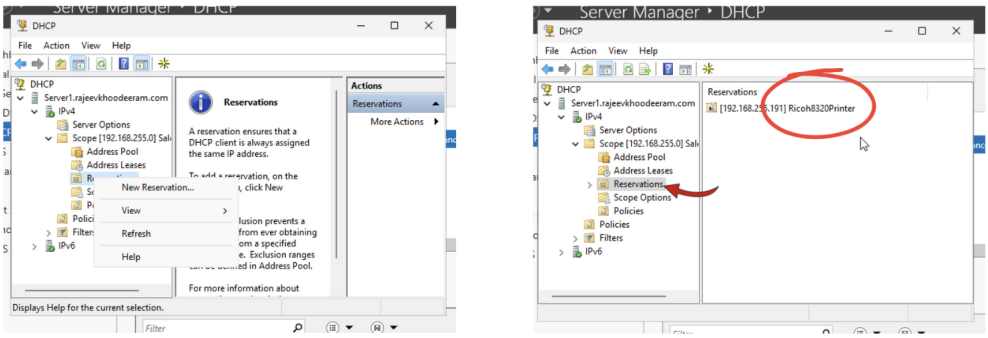


Figure 5.3: Adding the reservation Ricoh8320Printer

- Convert your exclusion for server2 to a reservation.

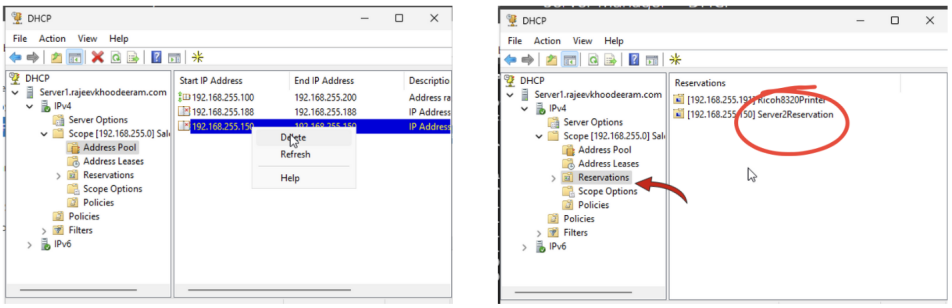


Figure 5.4: Converting exclusion to reservation

- Create a scope called “Mfg LAN” that assigned addresses from the range 172.16.5.1-172.16.5.254 for a lease period of unlimited. Ensure that the scope sets the default gateway and DNS server on the client to 172.16.0.200. Since your DHCP server does not have a network interface on the 172.16.0.0 network, we will assume that a DHCP relay agent will be configured on a router to forward requests for this network to your DHCP server.

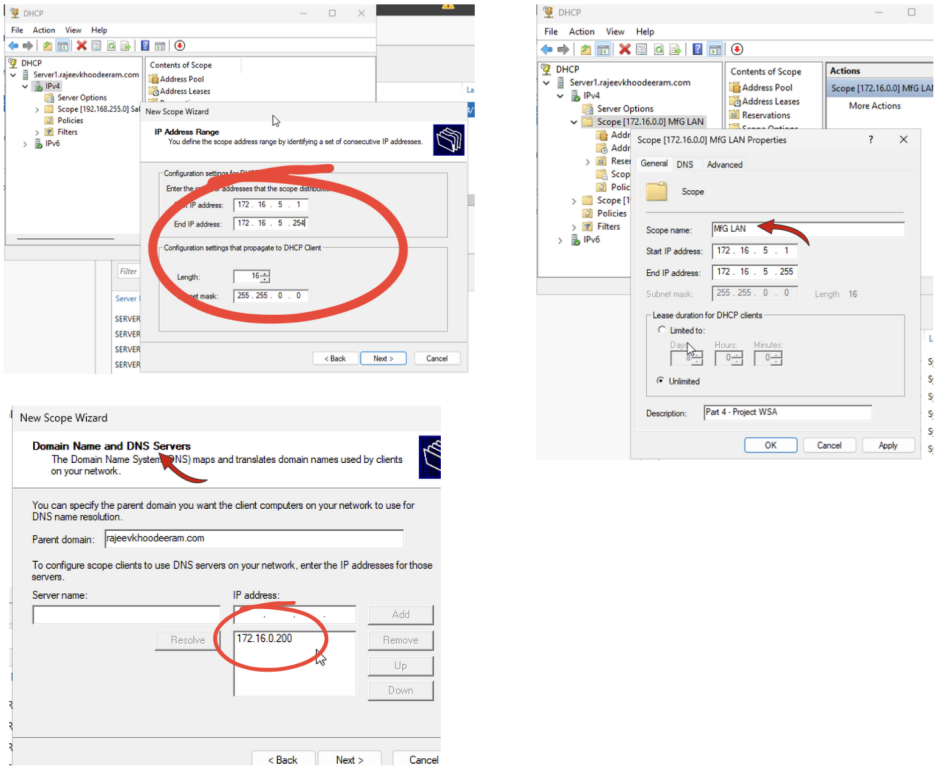


Figure 5.5: Adding scope Mfg LAN with default gateway

- Add a server option that sets the WINS server for all clients in the company to 192.168.255.1.

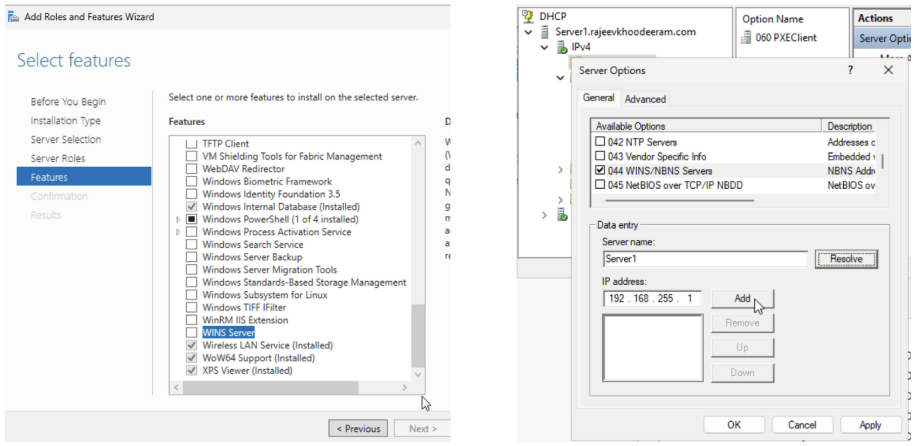


Figure 5.6: Configuring server option on WINS Server

- Ensure that Windows 98 clients that receive an IP address from the "Sales LAN" scope instead receive a gateway of 192.168.255.253, a DNS server of 10.0.1.2, and a WINS server of 10.0.2.2). Using DHCP Policies based on the client's OS or MAC address to apply special options only to Windows 98 machines.

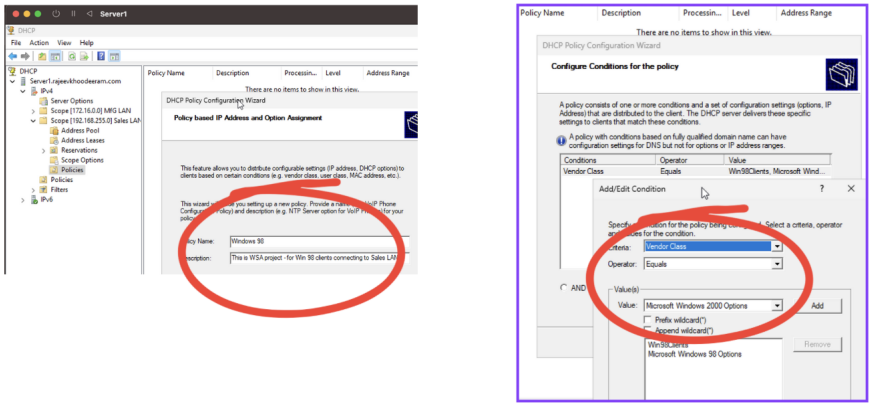


Figure 5.7: Configuring DHCP policy for Windows 98 clients under Sales LAN

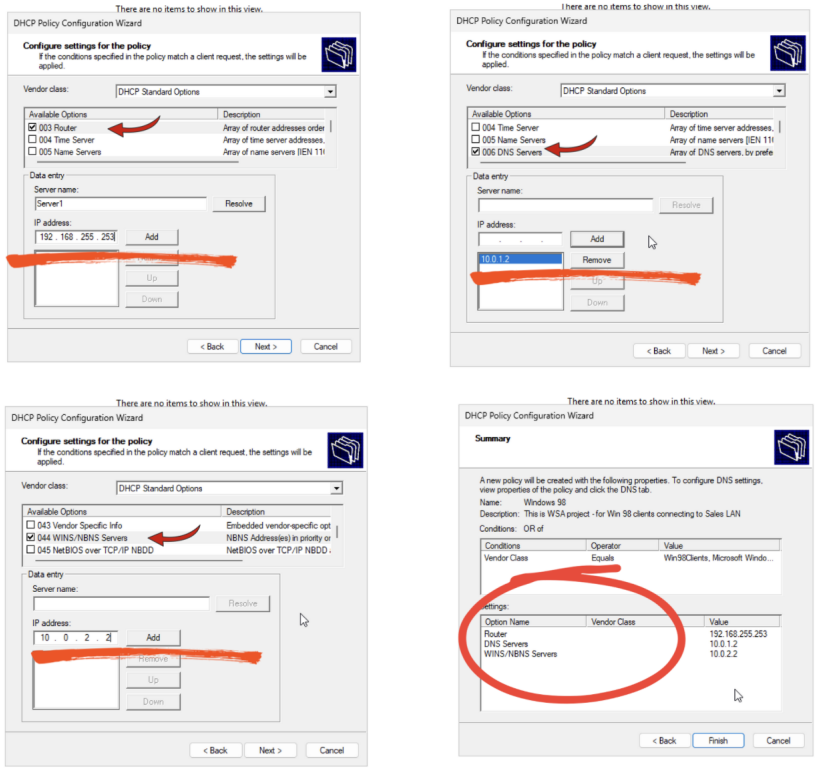


Figure 5.8: Adding the required IP addresses for Router, DNS and WINS

- Ensure that your classroom VoIP phone model will receive a default gateway of 192.168.255.222 on that Sales LAN.

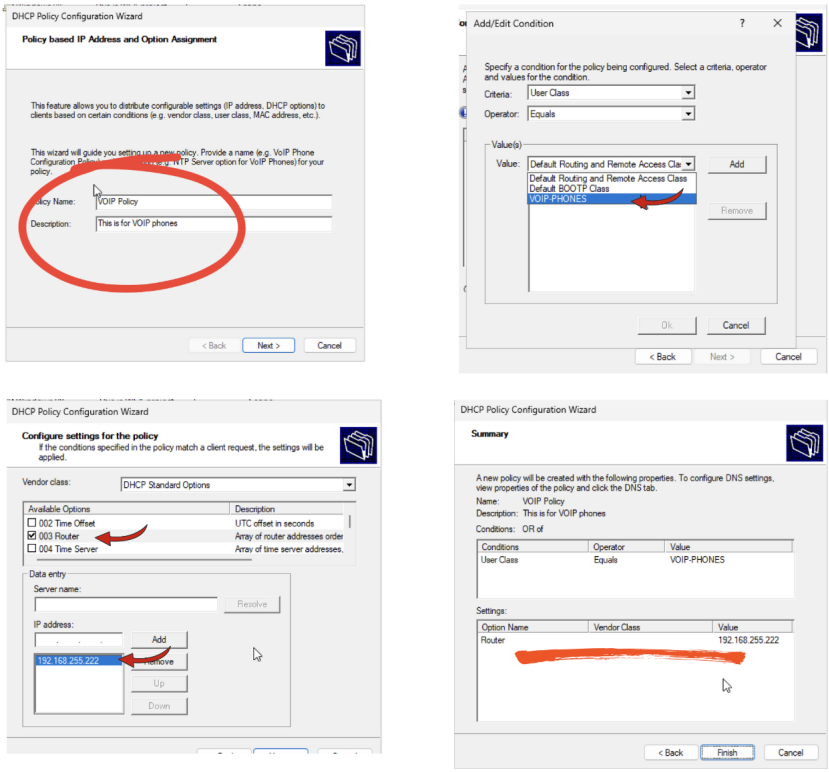


Figure 5.9: Configuration of VoIP phones with default gateway

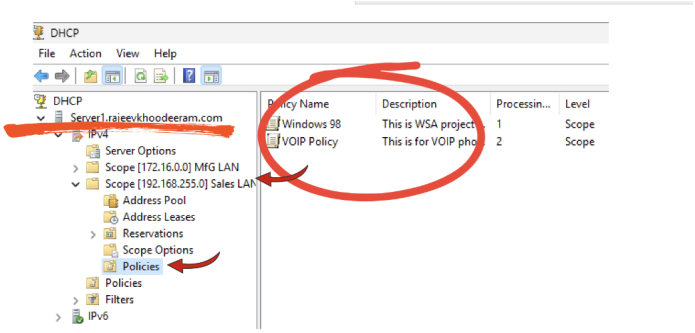


Figure 5.10: Overall policies applied to Sales LAN : Win98 clients and VOIP phones

- Ensure that your DHCP server always updates A and PTR records for all clients.

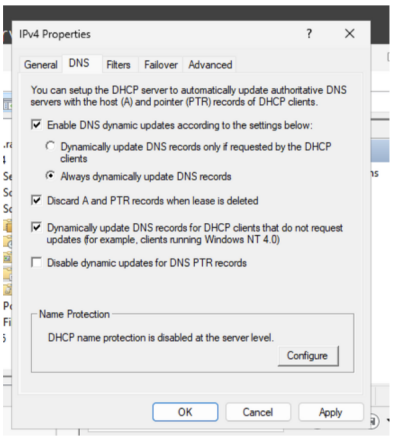


Figure 5.11: Configuration of DHCP Server with A and PTR records

- Configure server2 as a DHCP server in a failover relationship with server1.

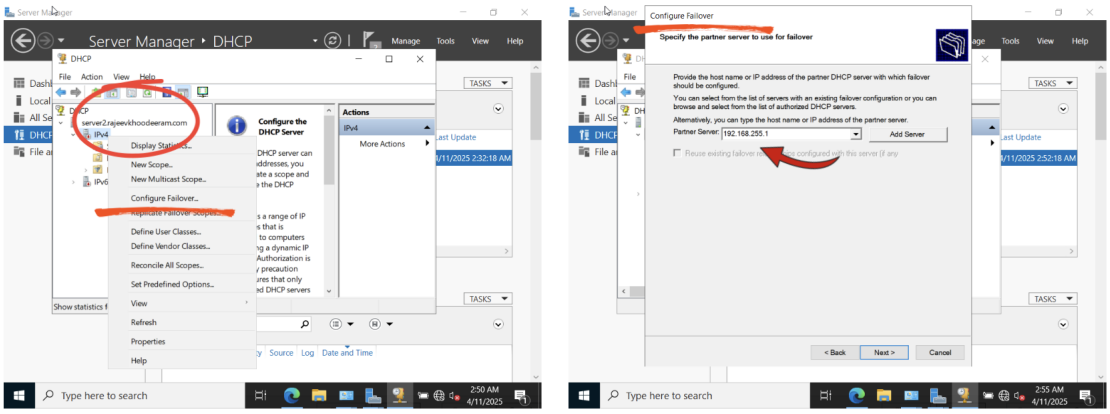


Figure 5.12: Configuration of Server2 as failover server

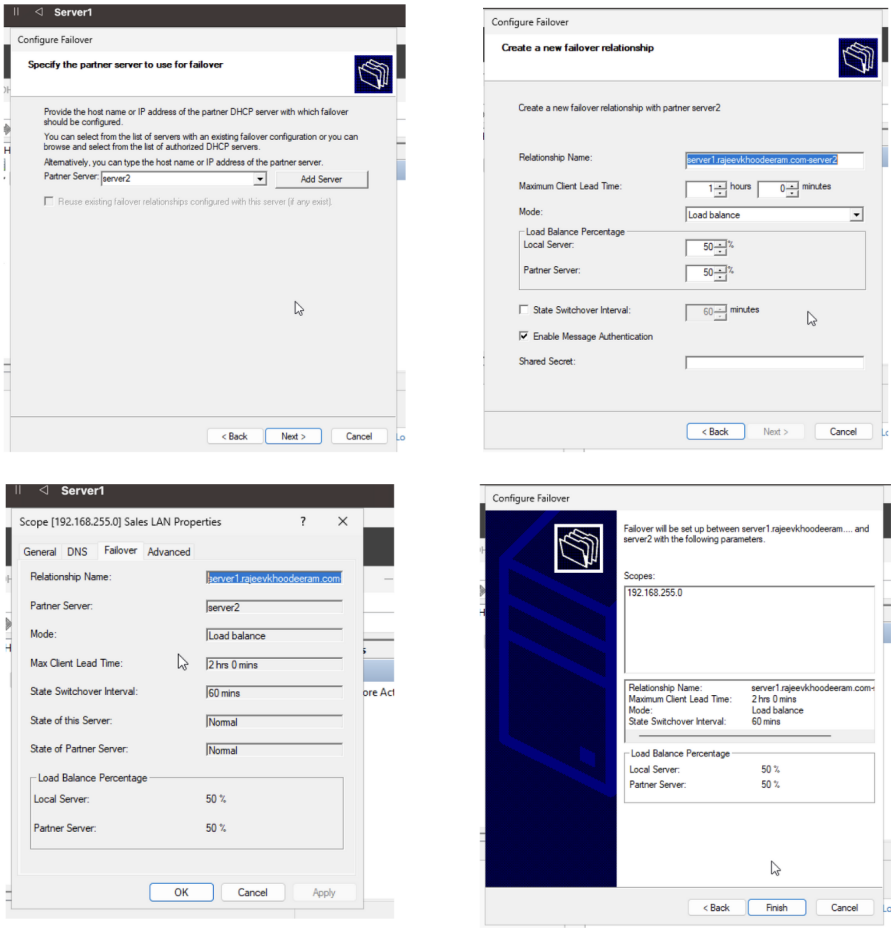


Figure 5.13: Configuration of Server1 for failover with Server2

STEP 5

6.1 Configure server1 and server2 as WINS servers

WINS stands for Windows Internet Name Service. A WINS Server is used to resolve NetBIOS names to IP addresses in a network (specifically for older Windows networking, where systems used NetBIOS names instead of DNS).

- Configure server1 and server2 as WINS servers in a push/pull relationship and ensure that NetBIOS name records for both your computers are automatically created in the WINS database (remember the bug in Server 2022).

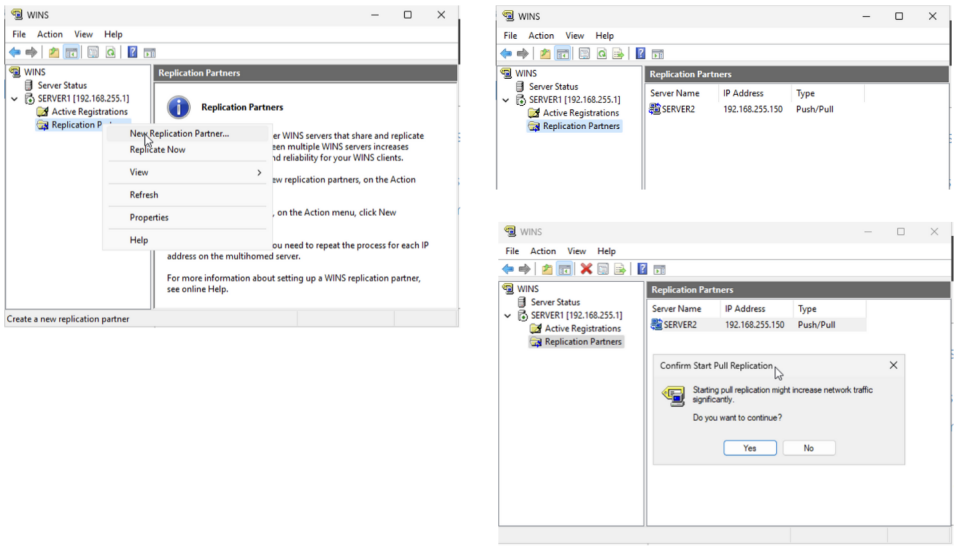


Figure 6.1: Configuring Server1 as WINS Servers (1)

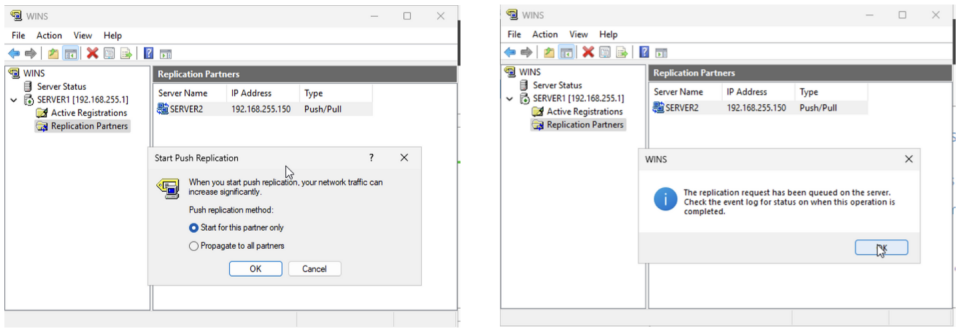


Figure 6.2: Configuring Server1 as WINS Servers (2)

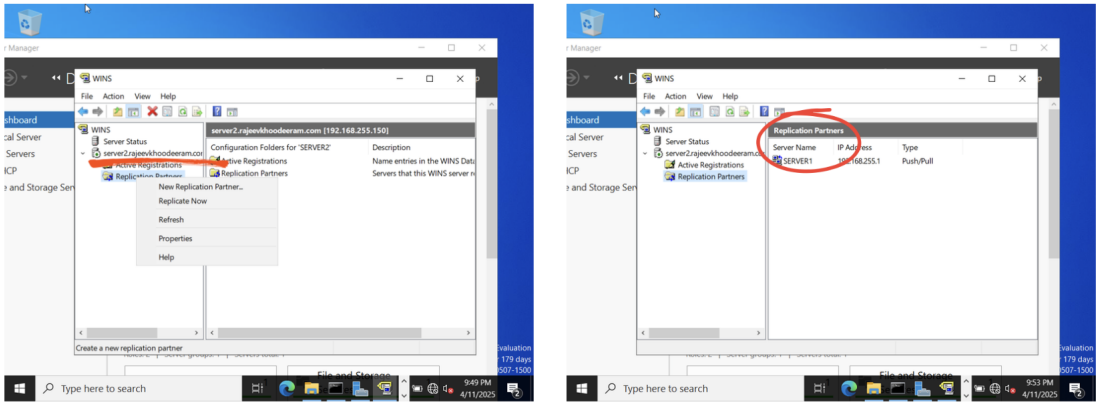


Figure 6.3: Configuring Server2 as WINS Servers

- Next, add a static mapping to the WINS database for 192.168.255.188 (which is used by a UNIX server named SCIBORG that has a static IP address).

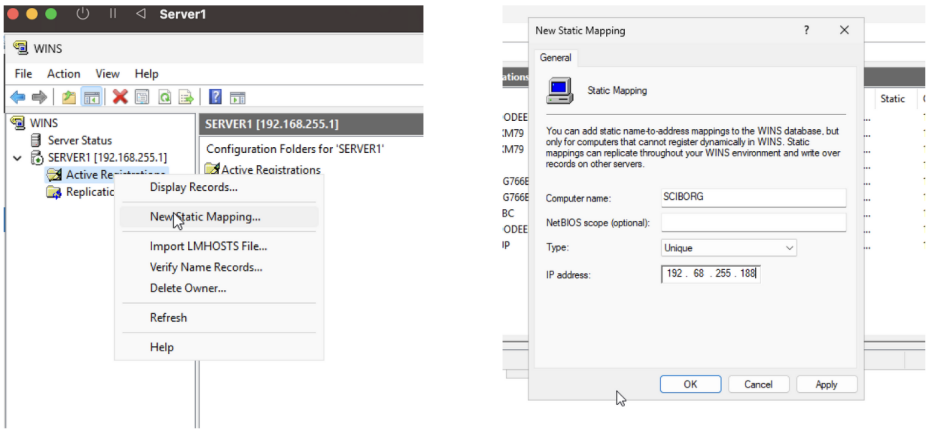


Figure 6.4: Adding Unix Server SCIBORG to WINS database

STEP 6

7.1 Configure the DNS service on Server1

- Create a standard forward lookup zone called yourname.net that accepts secure and unsecure dynamic updates.

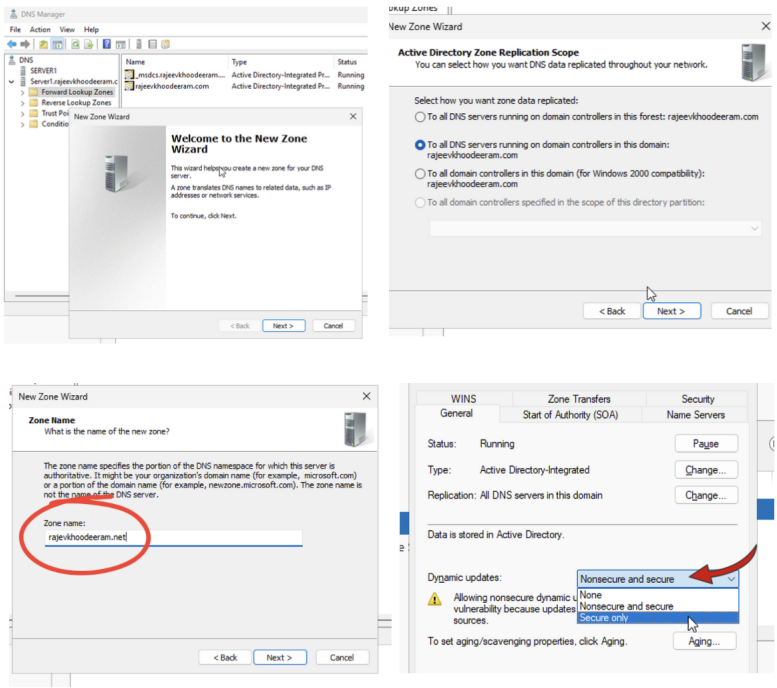


Figure 7.1: Create a standard forward lookup zone called rajevkhoodeeram.net

- Add the following A records to your zone (format *webserver.yourname.net*):
  - webserver.rajevkhoodeeram.net = 192.168.255.222
  - webserver.rajevkhoodeeram.net = 192.168.255.223
  - webserver.rajevkhoodeeram.net = 192.168.255.224
  - fileserver.rajevkhoodeeram.net = 192.168.255.225
  - mailserver.rajevkhoodeeram.net = 192.168.255.226

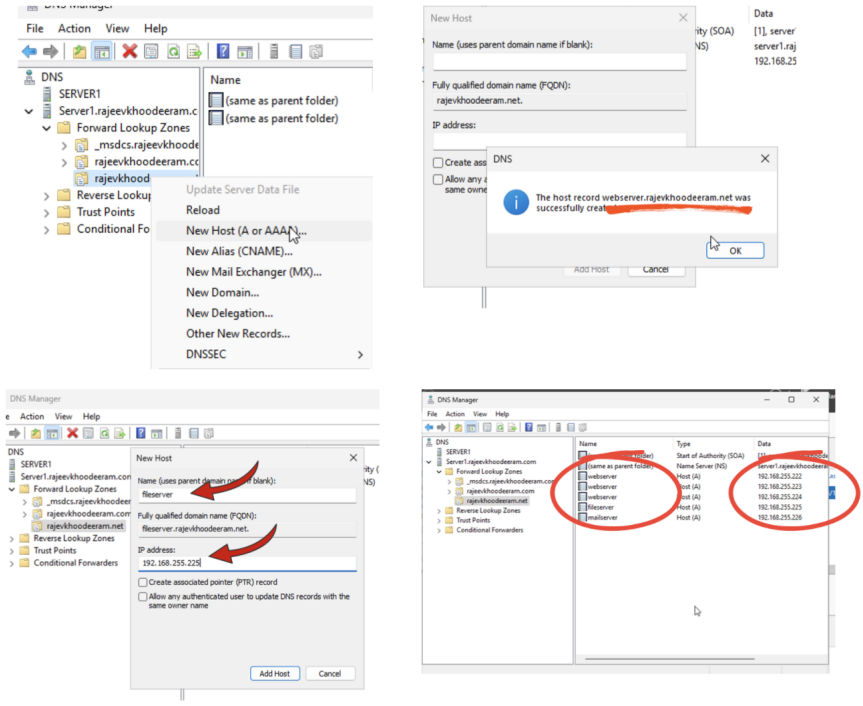


Figure 7.2: Adding A records to the domain

- Add a CNAME record that maps www.rajevkhoodeeram.net to webserver.rajevkhoodeeram.net.

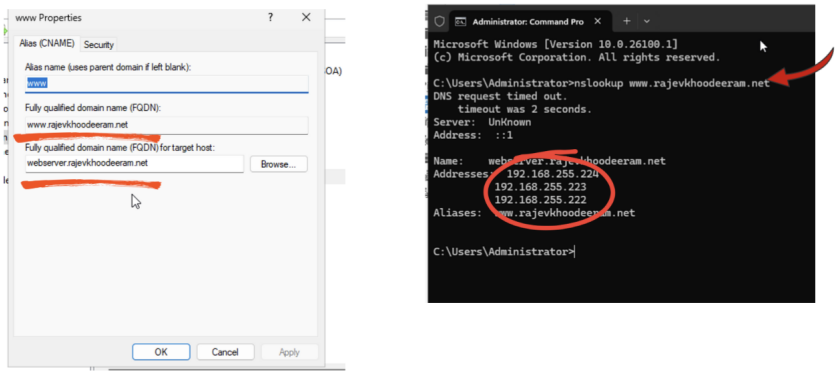


Figure 7.3: Adding CNAME record with mapping

- Add an MX record (priority = 20) for mailserver.yourname.net for the yourname.net zone.

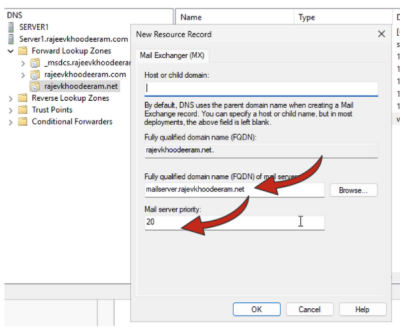


Figure 7.4: Adding an MX record for mailserver.rajevkhoodeeram.net

- Ensure that your DNS server can also use the WINS servers you created earlier for name resolution if FQDN name resolution fails.

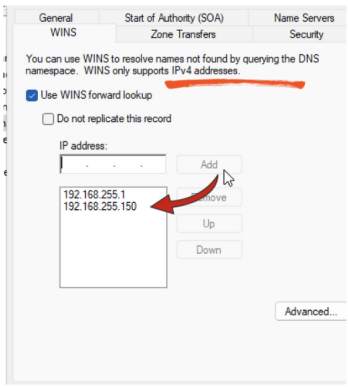


Figure 7.5: Configuring DNS server to use WINS server

- Ensure that any FQDN name resolution requests for the acme.com domain are forwarded to 192.168.255.226.

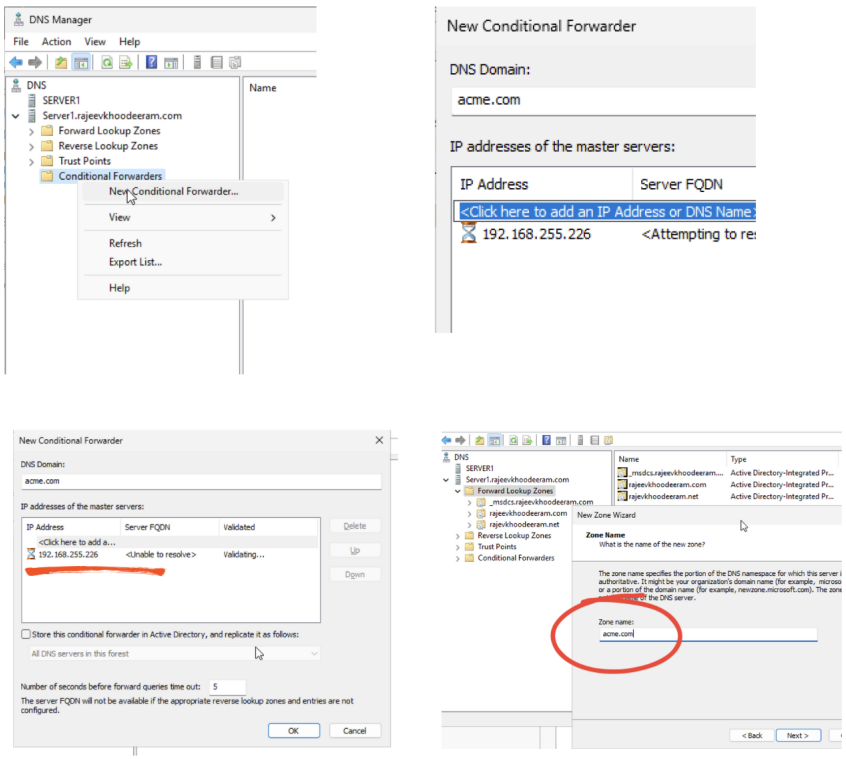


Figure 7.6: FQDN resolution for acme.com

- Add a standard primary reverse lookup zone for the 192.168.255.0 network that does not allow dynamic updates and create the appropriate PTR records for webserver.yourname.net.

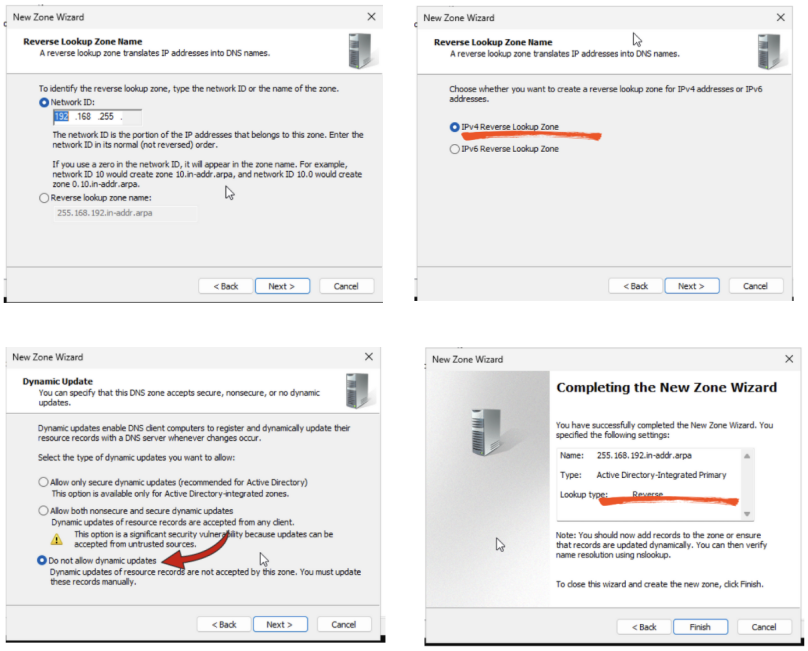


Figure 7.7: Primary reverse lookup zone

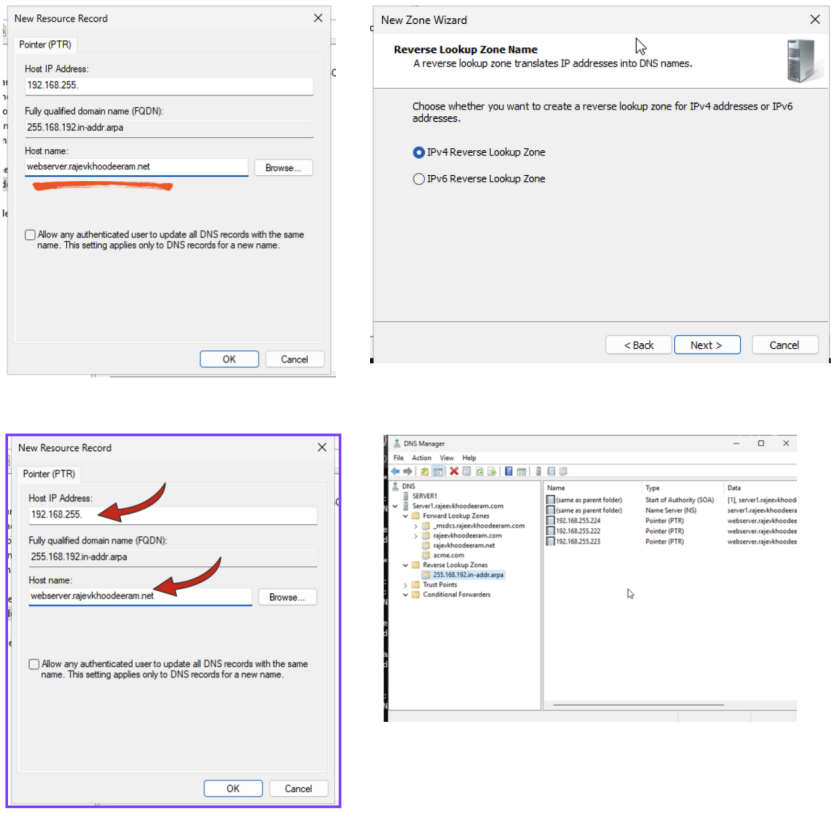


Figure 7.8: Adding PTR records for webserver.rajevkhoodeeram.net

STEP 7

8.1 Configure the DNS service on server2 to host a secondary copy of the yourname.net

- Configure the DNS service on server2 to host a secondary copy of the yourname.net (here rajevkhoodeeram.net) forward lookup zone and 192.168.255.0 reverse lookup zone from the previous steps.

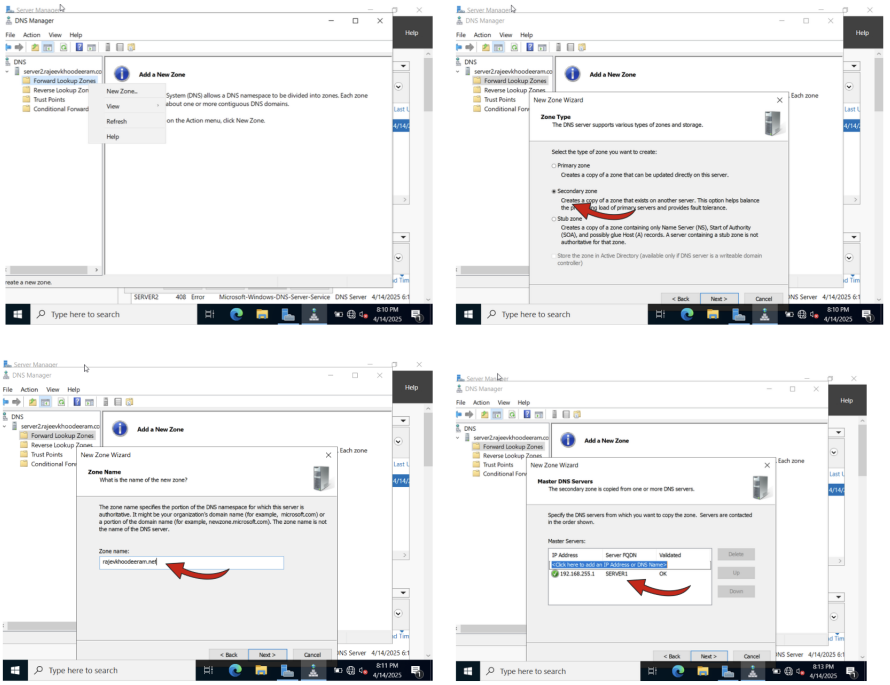


Figure 8.1: Create Secondary Zones on Server2 (1)

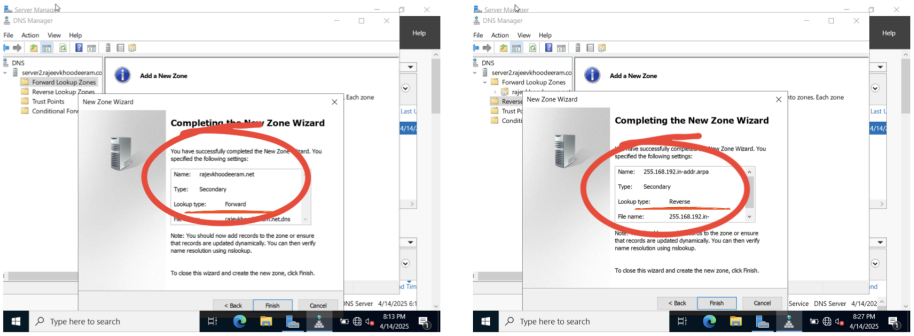


Figure 8.2: Create Secondary Zones on Server2 (2)

- Ensure that the secondary zones query the primary zones every 5 minutes for new records.

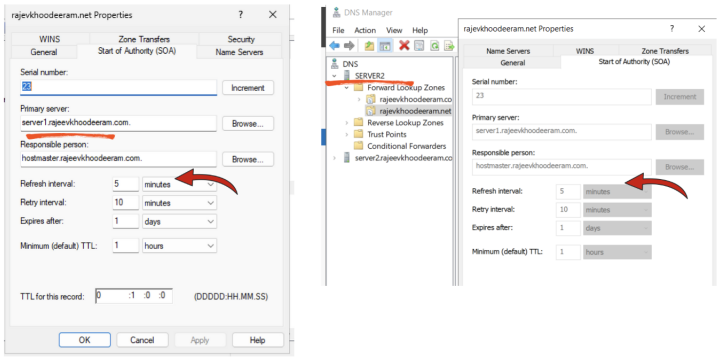


Figure 8.3: Set Zone Transfer Interval to 5 Minutes

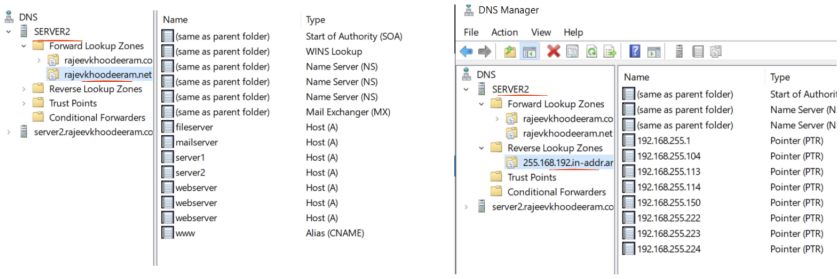


Figure 8.4: Results after testing - Zone transfer occurs from Server 1 to Server 2

- Test that both servers can be queried for the records and that round robin functionality is working.

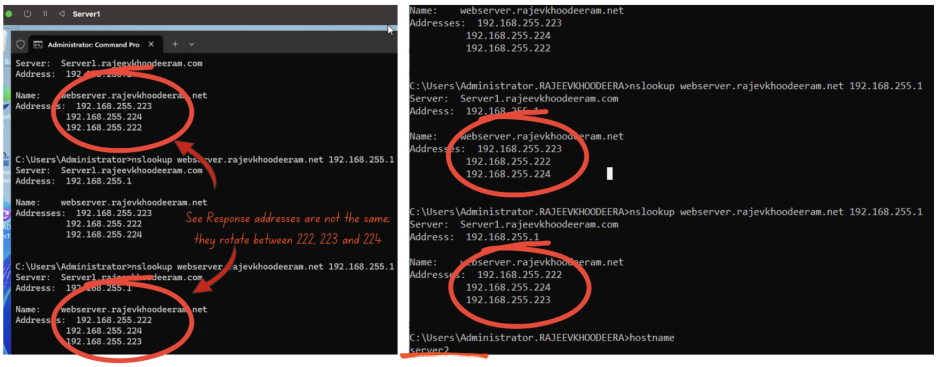


Figure 8.5: Testing of records being updated on Server 1(left) and Server 2 (right) - Round Robin is working as IP addresses rotate in the response with nslookup

STEP 8

9.1 Convert the rajevkhoodeeram.net to AD integrated

- Convert the yourname.net (here it is rajevkhoodeeram.net) and 192.168.255.0 zones on server1 to be Active Directory integrated and accept secure dynamic updates only.

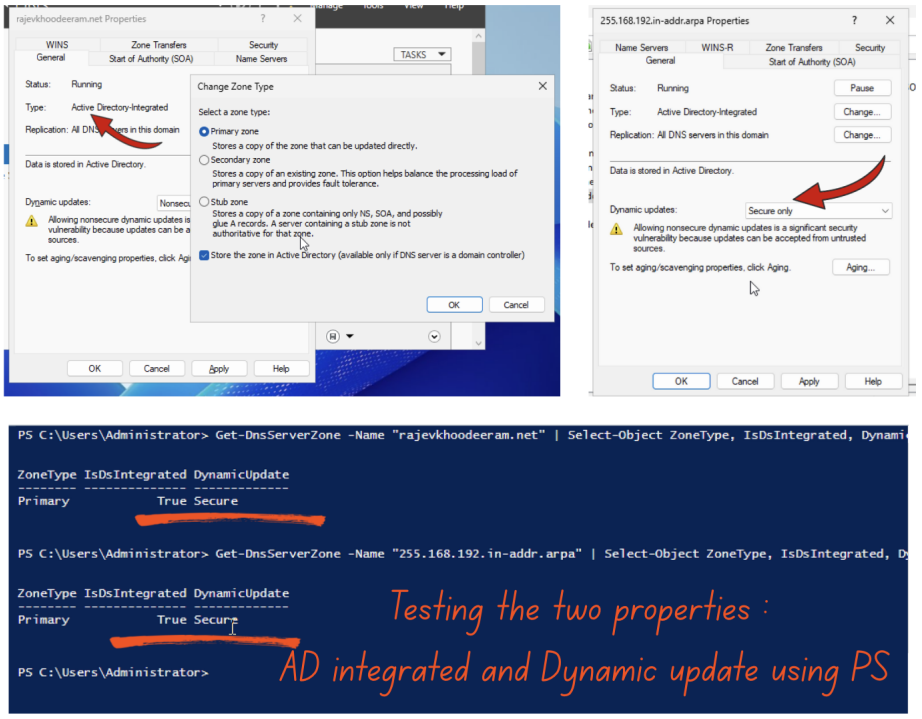


Figure 9.1: Convert domain to AD integrated

STEP 9

10.1 Configure server1 as a VPN server

A VPN (Virtual Private Network) is used to create a secure, encrypted connection ("tunnel") between a user (or device) and a private network — over the internet. Here Server1 is turned into a VPN server, so authorized users (like employees) can connect remotely to the organization's network using a safe tunnel and get an internal IP (e.g., 172.16.0.x) — behaving like they're inside the office LAN.

- Configure server1 as a VPN server. The VPN network should use IP addresses on the 172.16.0.0 network.

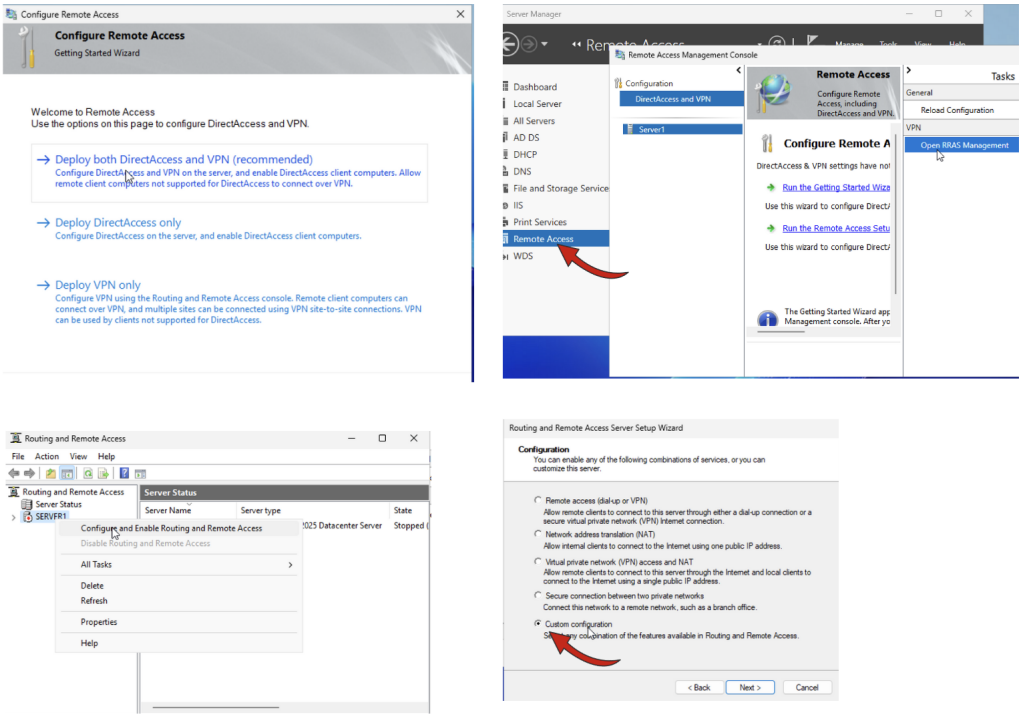


Figure 10.1: Configure Server1 as VPN server on 172.16.0.0 network (1)

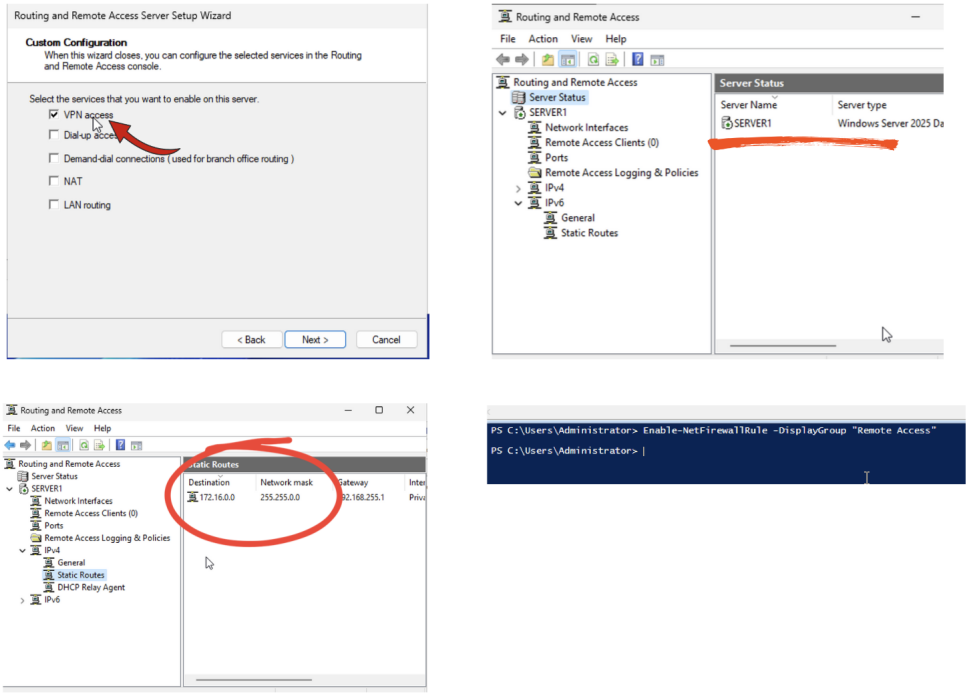


Figure 10.2: Configure Server1 as VPN server on 172.16.0.0 network (2)

- Moreover, the VPN server should use a RADIUS server configured on server1 for authentication and logging, as well as use an NPS policy that disconnects idle sessions after 2 minutes.

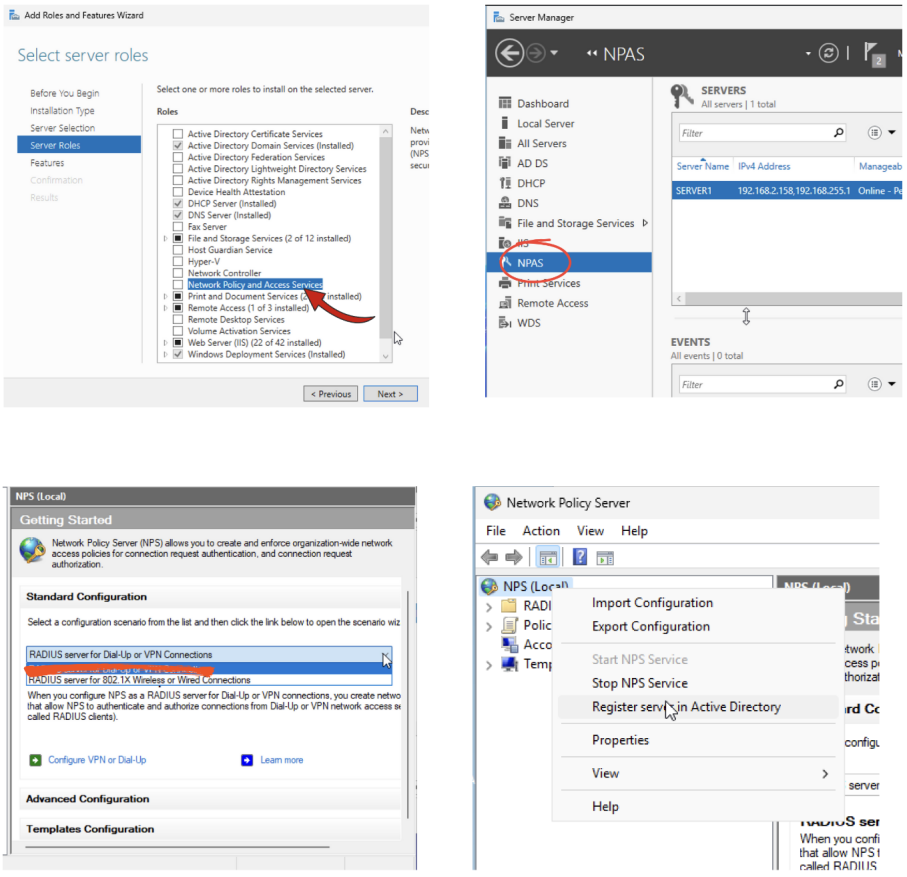


Figure 10.3: Installing NPS

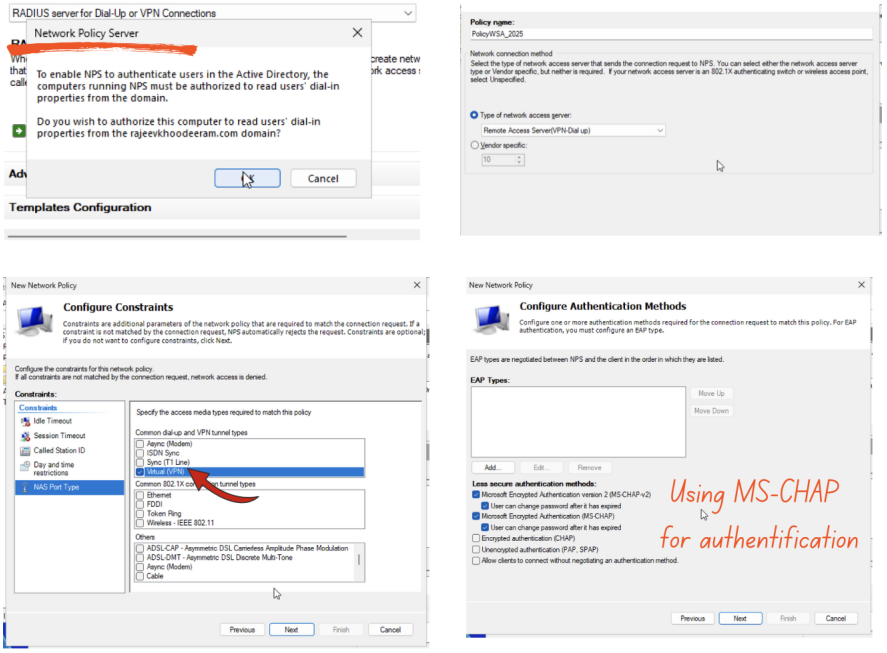


Figure 10.4: Register NPS in Active Directory

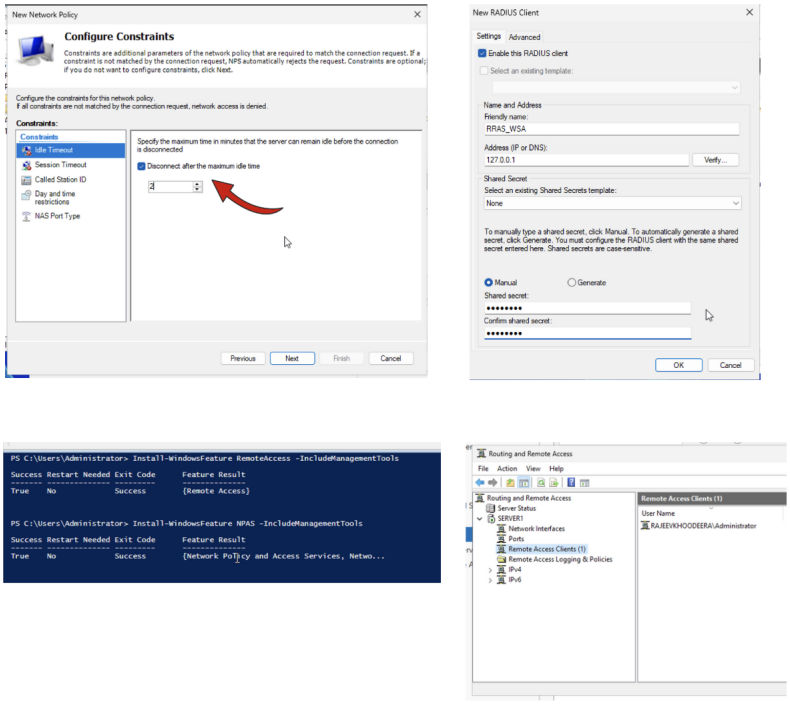


Figure 10.5: Configure RRAS to Use RADIUS (NPS) for Authentication

- Test your configuration from server2 using split tunneling.

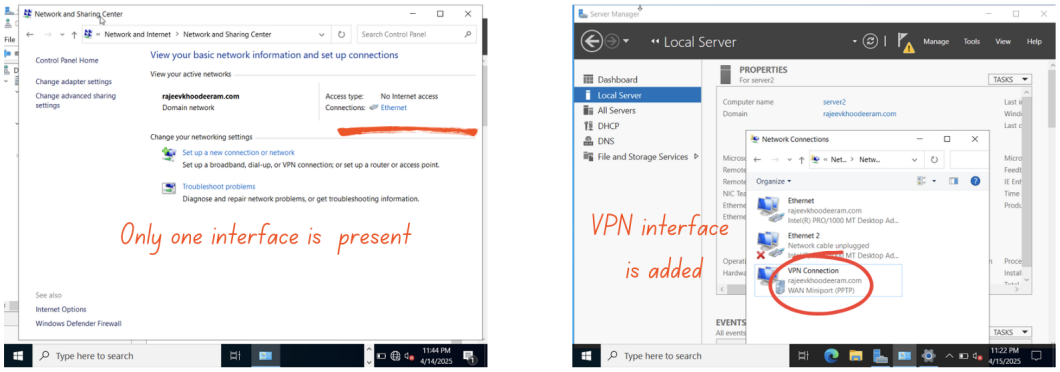
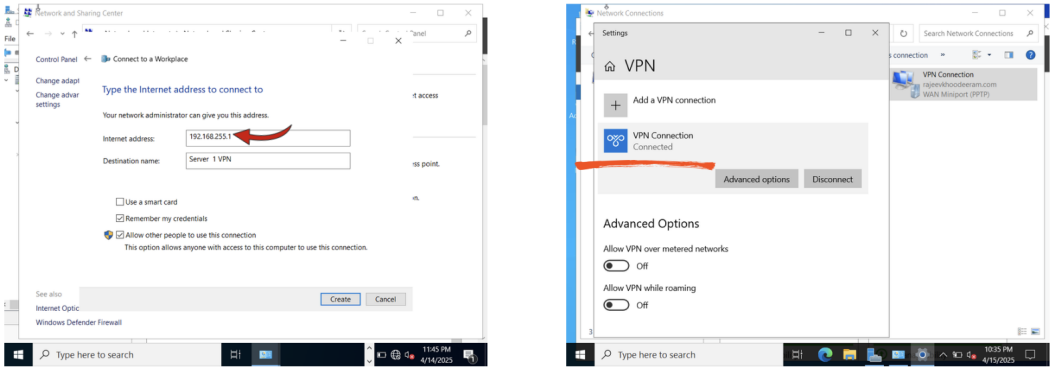


Figure 10.6: Adding the VPN interface



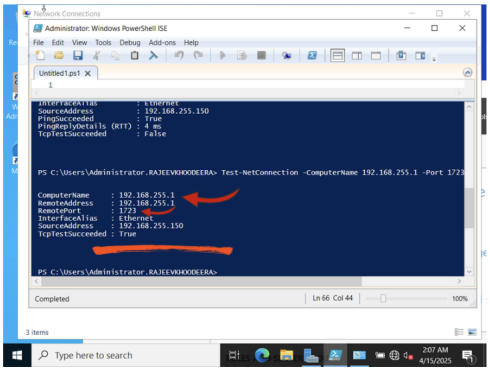


Figure 10.7: Testing VPN connection to Server 1

STEP 10

11.1 Creating a domain-based DFS namespace for your domain

DFS stands for Distributed File System. It's a Windows Server role that organizes shared folders across multiple servers into one unified directory structure (called a namespace). Users see just one logical tree of folders — even though the data may be stored on different servers or locations behind the scenes.

- Configure a domain-based DFS namespace for your domain called warehouse
  - Install DFS (run below cmdlet on both server1 and server2)
    Install-WindowsFeature FS-DFS-Namespace -IncludeManagementTools
  - Must also do this otherwise DFS Replication service not installed message
    Install-WindowsFeature FS-DFS-Replication -IncludeManagementTools

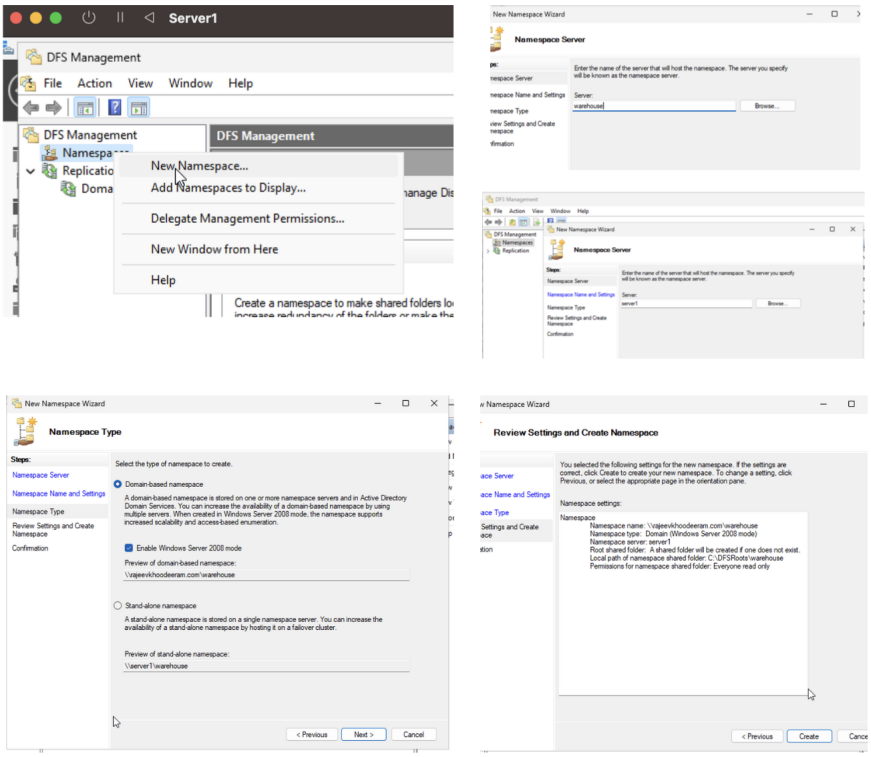


Figure 11.1: Configuring the DFS and namespace on the domain

- Add three shared folders (called share1 through share3) to this namespace that meet the following criteria. Share1 and share2 reside on server1. Share3 resides on both server1 and server2, with the contents synchronized using DFS replication.

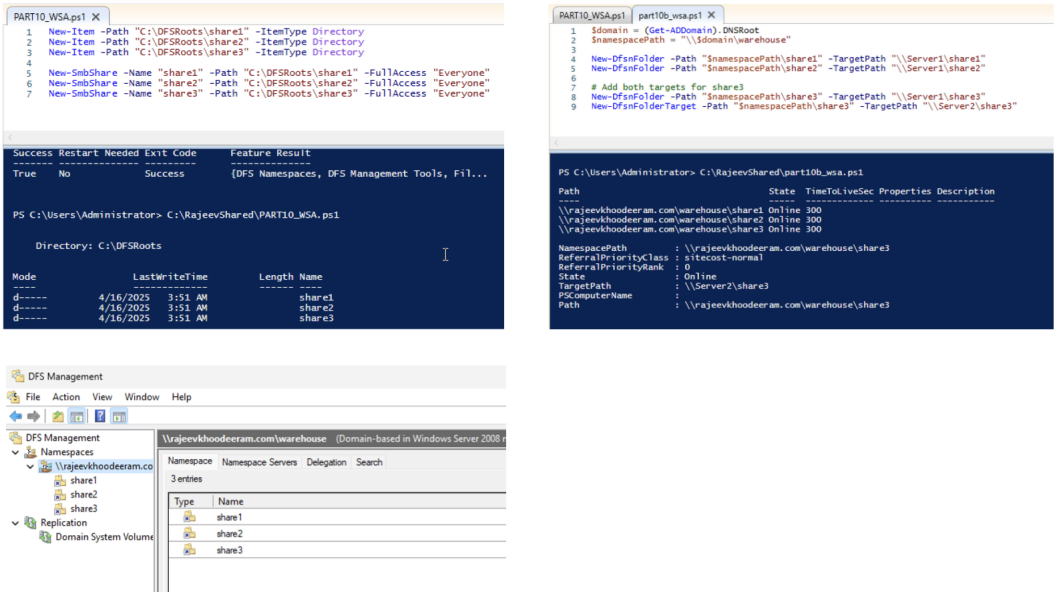


Figure 11.2: Configuring the shared folders

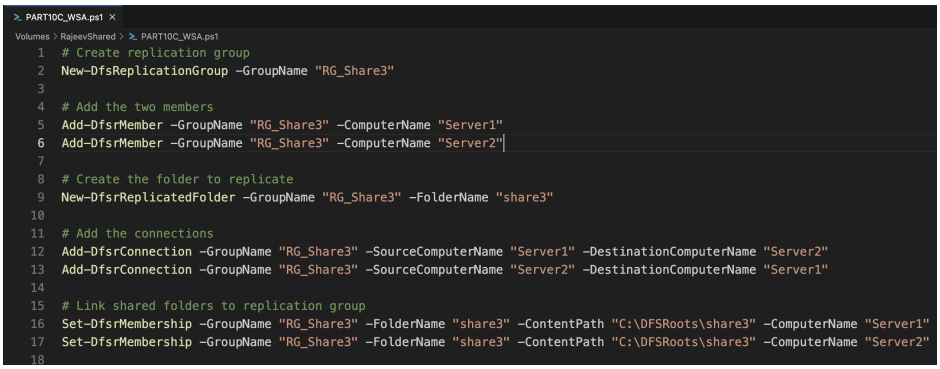


Figure 11.3: Link shared folders to replication group

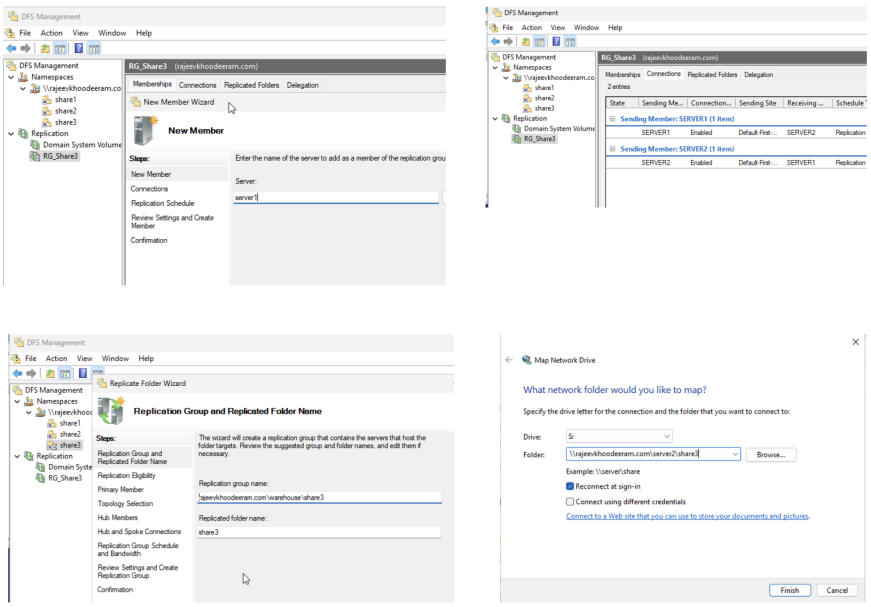


Figure 11.4: Configuration of DFS and Replication service (1)

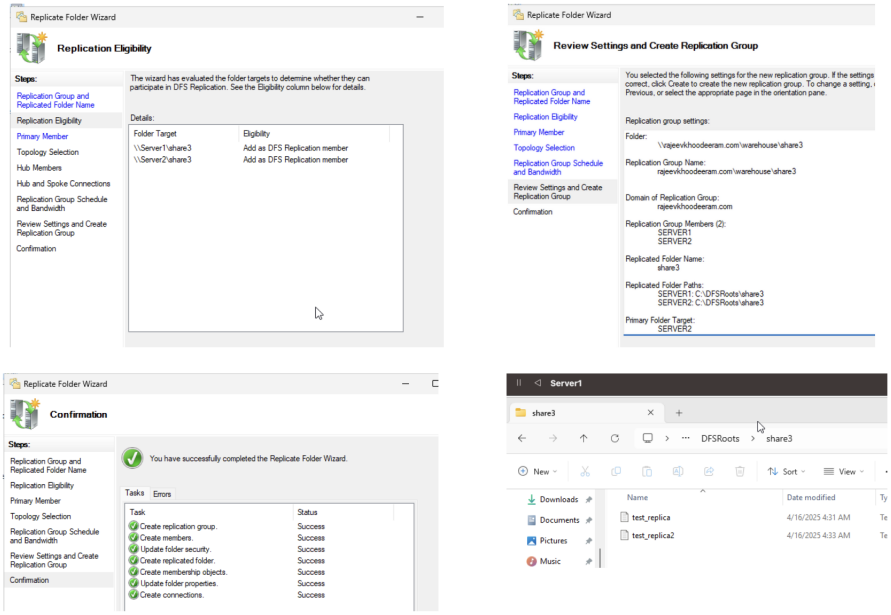


Figure 11.5: Configuration of DFS and Replication service (2)

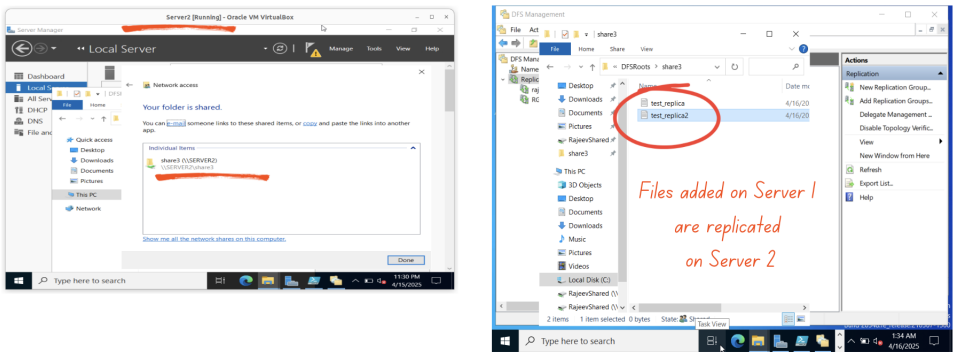


Figure 11.6: Share3 on Server2 and how files are replicated from Server1

The following three Powershell commands can be used to install the RRAS services :

- Install-WindowsFeature RemoteAccess -IncludeManagementTools
- Install-WindowsFeature DirectAccess-VPN -IncludeManagementTools
- Install-WindowsFeature Routing -IncludeManagementTools

STEP 11

12.1 Create the following OU structure underneath your domain

There are two ways to create the requested OU structure : Powershell or GUI; three Powershell scripts have been used.

PART11_WSA.ps1

Volumes > RajeevShared > PART11_WSA.ps1

```
1
2  # Top-level OUs
3  #New-ADOrganizationalUnit -Name "Usrs"
4  #New-ADOrganizationalUnit -Name "Wrkstns"
5  #New-ADOrganizationalUnit -Name "Printers"
6  #New-ADOrganizationalUnit -Name "Servers"
7
8  # Usrs Sub-OUs
9  New-ADOrganizationalUnit -Name "Sales" -Path "OU=Usrs,DC=rajeevkhoodeeram,DC=com"
10 New-ADOrganizationalUnit -Name "Mfg" -Path "OU=Usrs,DC=rajeevkhoodeeram,DC=com"
11 New-ADOrganizationalUnit -Name "Engrg" -Path "OU=Usrs,DC=rajeevkhoodeeram,DC=com"
12 New-ADOrganizationalUnit -Name "IT" -Path "OU=Usrs,DC=rajeevkhoodeeram,DC=com"
13
14 # Mfg Sub-OUs
15 New-ADOrganizationalUnit -Name "No. Amer" -Path "OU=Mfg,OU=Usrs,DC=rajeevkhoodeeram,DC=com"
16 New-ADOrganizationalUnit -Name "So. Amer" -Path "OU=Mfg,OU=Usrs,DC=rajeevkhoodeeram,DC=com"
17 New-ADOrganizationalUnit -Name "Canada" -Path "OU=Mfg,OU=Usrs,DC=rajeevkhoodeeram,DC=com"
18
19 # Servers Sub-OUs
20 New-ADOrganizationalUnit -Name "DHCP/WINS" -Path "OU=Servers,DC=rajeevkhoodeeram,DC=com"
21 New-ADOrganizationalUnit -Name "File/Print" -Path "OU=Servers,DC=rajeevkhoodeeram,DC=com"
22 New-ADOrganizationalUnit -Name "SMS" -Path "OU=Servers,DC=rajeevkhoodeeram,DC=com"
```

Figure 12.1: Powershell scripts to generate the OUs

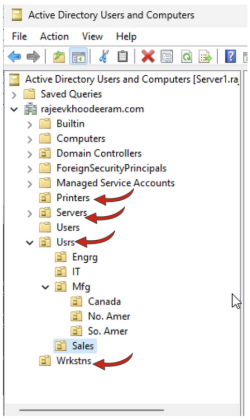


Figure 12.2: Visual representation of the OUs in the Active Directory

STEP 12

13.1 Nesting group structure

In this step, three Powershell scripts have been used to generate the nesting group structure. Create a nested group structure that allows permissions to be easily assigned to:

- Members of the Sales, Mfg, Engrg, and IT groups (in your domain; **Domain-level**)

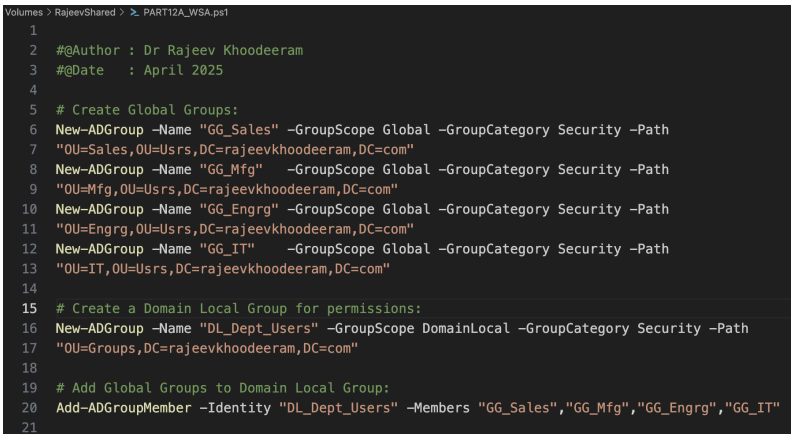


Figure 13.1: Domain level group

- Mfg members in No.Amer, So.Amer, and Canada (in your domain; **Department-level**)

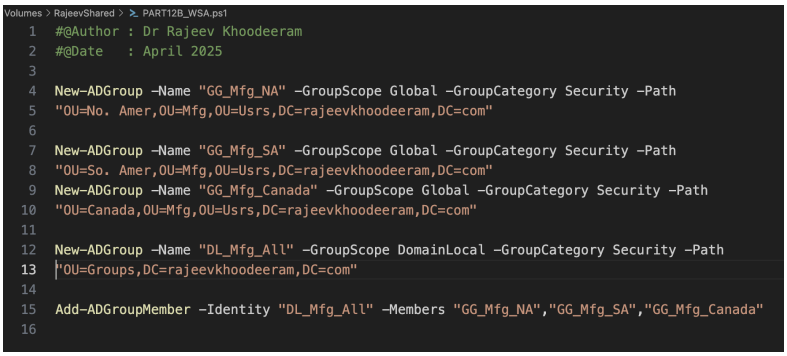


Figure 13.2: Department level group

- Members of the Sales, Mfg, Engrg, and IT groups (in your entire forest; **Forest-wide**)

Figure 13.3: Forest wide group

Figure 13.4: Overall hierarchy created for the OUs

STEP 13

14.1 Creating local group : Project-Printer

- Create a local group called Project-Printer within the File/Print OU.

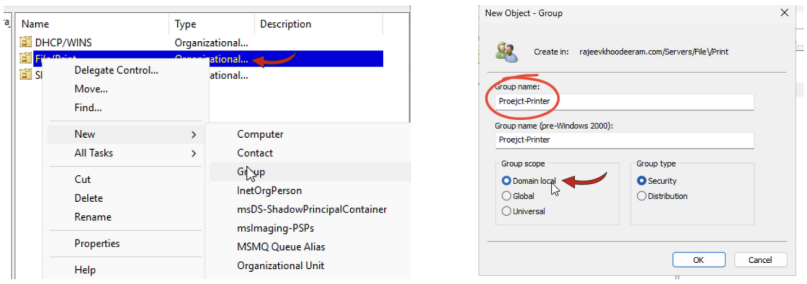


Figure 14.1: Create the Local Security Group in File/Print OU

- Next, create a fictitious printer on your host OS that grants Print permission only to members of the Mfg (forest-wide) while using this local group.

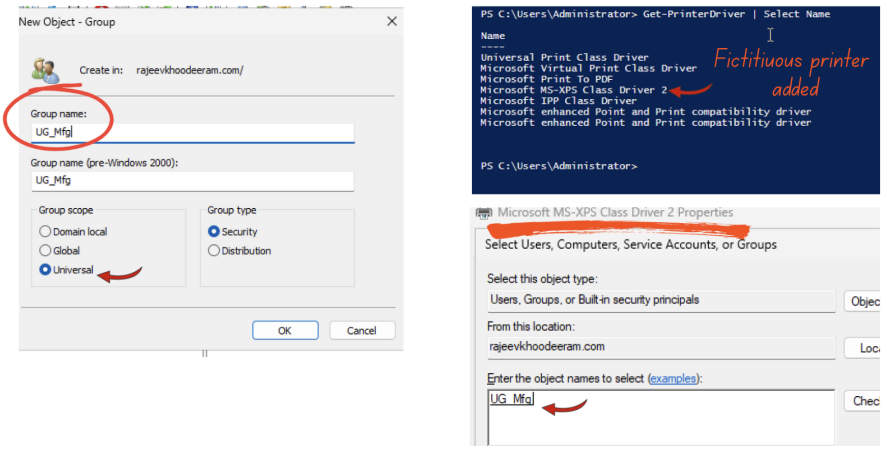


Figure 14.2: Add the forest-wide Mfg group (assumed Universal Group)

The list of drivers installed on the server can be retrieved using :

Get-PrinterDriver | Select Name

STEP 14

15.1 Creating user accounts in organizational units

- Create 3 user accounts (of your choice) within the 6 OUs that "should" contain user accounts. Each user account should be a member of the appropriate groups from the previous step.

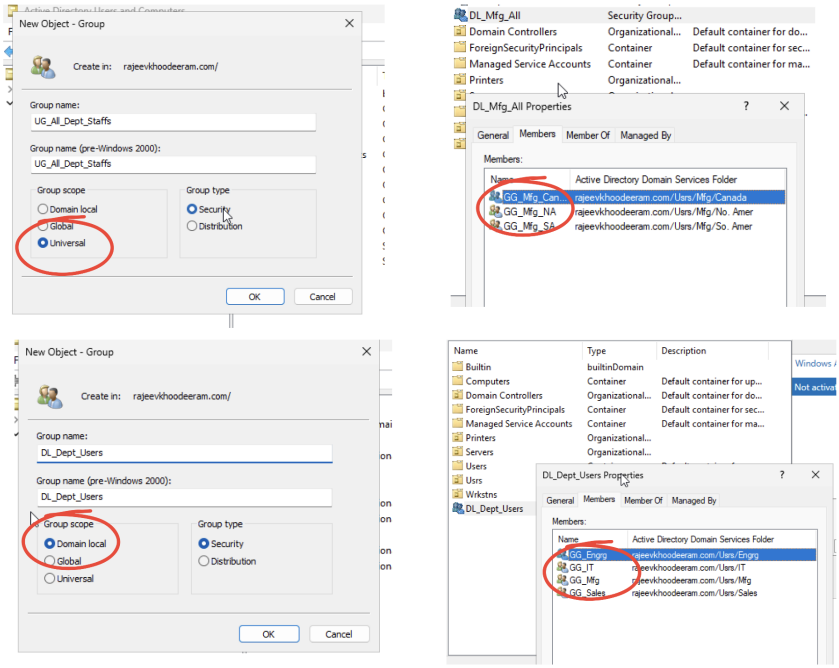


Figure 15.1: Creating the different groups in the OUs

```powershell
# ****************************
#@Author : Dr Rajeev Khoodeeram
#@Date   : April 2025
# ****************************

# Sample user data
$users = @(
    @{Name="AliceSales"; OU="OU=Sales, DC=rajeevkhoodeeram,DC=com"; Group="GG_Sales"},
    @{Name="BobMfg"; OU="OU=Mfg,DC=rajeevkhoodeeram,DC=com"; Group="GG_Mfg"},
    @{Name="CarolEng"; OU="OU=Engrg,DC=rajeevkhoodeeram,DC=com"; Group="GG_Engrg"},
    @{Name="DavidIT"; OU="OU=IT,DC=rajeevkhoodeeram,DC=com"; Group="GG_IT"},
    @{Name="EveNAMfg"; OU="OU=No.Amer,DC=rajeevkhoodeeram,DC=com"; Group="GG_Mfg"},
    @{Name="FrankSAMfg"; OU="OU=So.Amer,DC=DC=rajeevkhoodeeram,DC=com"; Group="GG_Mfg"}
)
# Create each user with a default password in the domain, and add tgem to the appropriate group
foreach ($u in $users) {
    $username = $u.Name
    $password = ConvertTo-SecureString "P@ssw0rd123!" -AsPlainText -Force
    # Create the user
    New-ADUser -Name $username `
               -SamAccountName $username `
               -UserPrincipalName "$username@rajeevkhoodeeram.com" `
               -AccountPassword $password `
               -Path $u.OU `
               -Enabled $true
    # Add to group
    Add-ADGroupMember -Identity $u.Group -Members $username
}
```

Figure 15.2: Powershell script to create random user accounts in each OUs

STEP 15

16.1 Develop a workstation naming convention and pre-stage computers and users

Develop a workstation naming convention, and pre-stage computer accounts for 2 workstations within the Workstations OU (for general-purpose workstations) as well as pre-stage computer accounts for 2 workstations within the same 6 OUs that contain user accounts from the previous step.

- Develop a workstation naming convention, and pre-stage computer accounts for 2 workstations within the Workstations OU (for general-purpose workstations)

  Format: [Location]-[Department/OU]-[DeviceType]-[UniqueID]

  Example

  - Toronto-IT-WS-01
  - Toronto-IT-WS-02

- Create pre-stage computer accounts for 2 workstations within the same 6 OUs that contain user accounts from the previous step.

  If workstations are created for the 6 OUs, then we can use this format :

  Format: [Department/OU]-[Location]-[DeviceType]-[UniqueID]

  Example

  - Mfg-NA-WS-01
  - Mfg-SA-WS-02

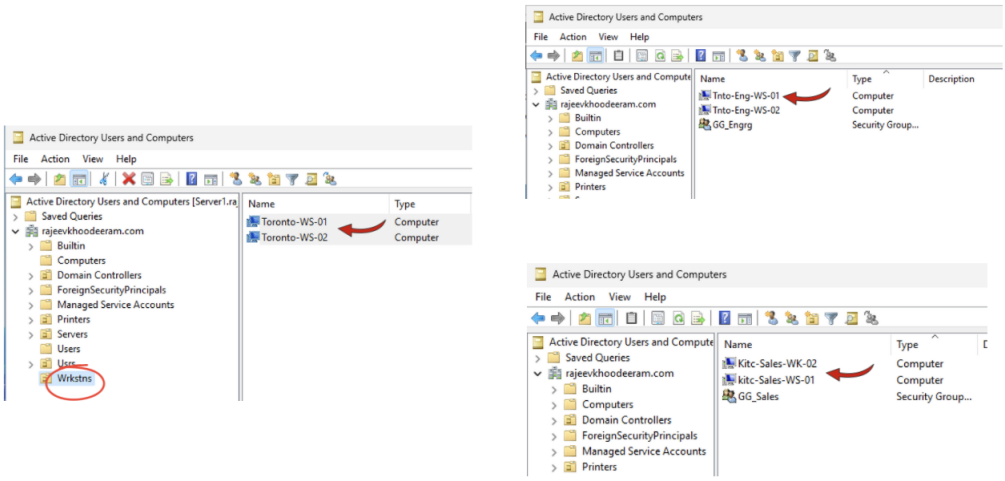


Figure 16.1: Pre-staging workstation with naming convention

STEP 16

17.1 Create and link a new GPO called GPO-Mfg to the Mfg OU

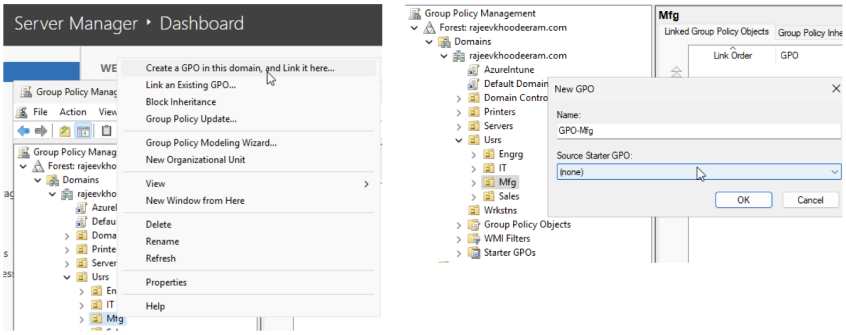


Figure 17.1: Create and Link the GPO : GPO-Mfg

- Locks out users for 2 hours if they log in 3 times unsuccessfully within 1 minute.
  Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Account Lockout Policy

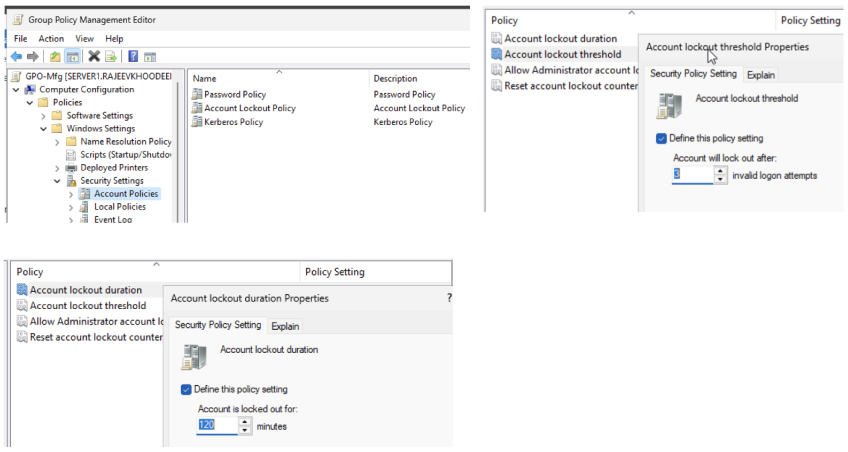


Figure 17.2: Account Lockout (2 hours after 3 failed attempts within 1 minute)

- Removes Control Panel access.
  User Configuration → Policies → Administrative Templates → Control Panel

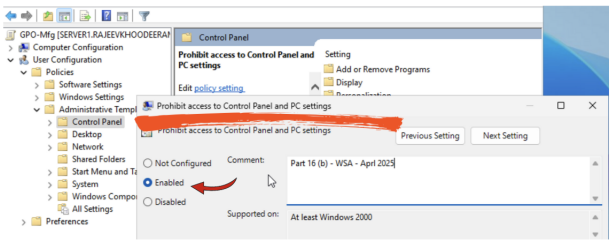


Figure 17.3: Removes Control Panel access

- Ensures that the Print Spooler service is always started.
  Computer Configuration → Policies → Windows Settings → Security Settings → System Services

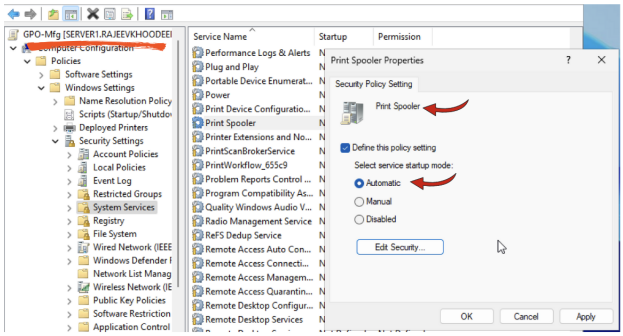


Figure 17.4: Set Startup Mode to Automatic for Print Spooler

- Specifies that the system event log should be 40MB in size maximum and that old events will be cleared automatically as necessary.
  Computer Configuration → Policies → Administrative Templates → Windows Components → Event Log Service → System

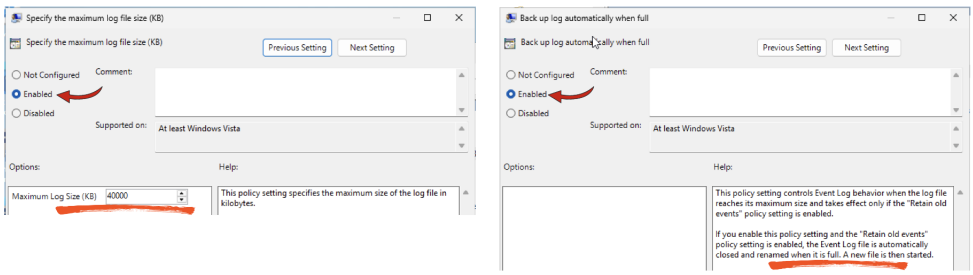


Figure 17.5: Maximum log size (KB) = 40960 (for 40MB) and Retention method

- Sets the background wallpaper (your choice).
  User Configuration → Policies → Administrative Templates → Desktop → Desktop

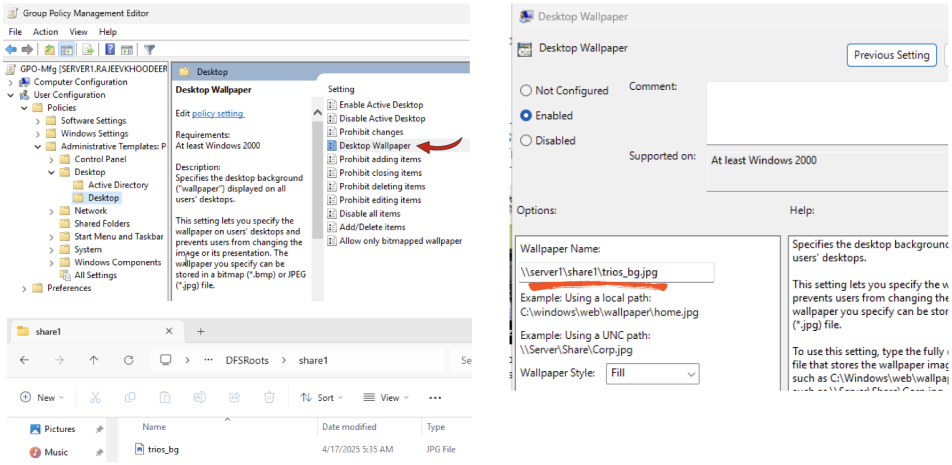


Figure 17.6: Setting Desktop Wallpaper

- Gives Bob the right to log on locally and shut down the computer.
  Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment

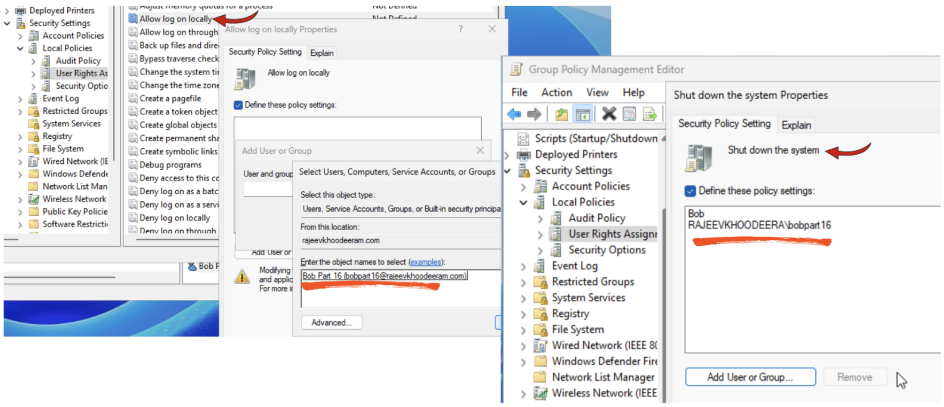


Figure 17.7: Allow log on locally and Shut down the system for user

- Assigns a software package (of your choice) to all computers.
  Computer Configuration → Policies → Software Settings → Software Installation

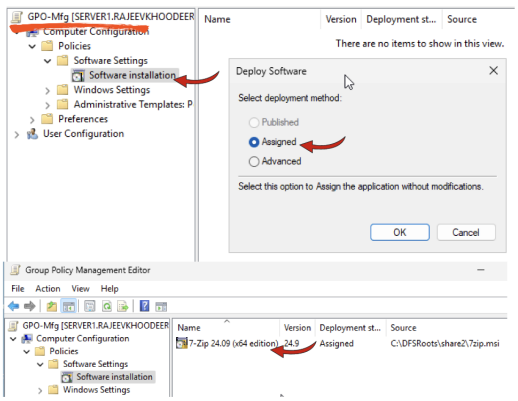


Figure 17.8: Assigns a software package (of your choice) to all computers.

- Redirects the Desktop and Documents folders for users to a shared folder on server1.
  User Configuration → Policies → Windows Settings → Folder Redirection

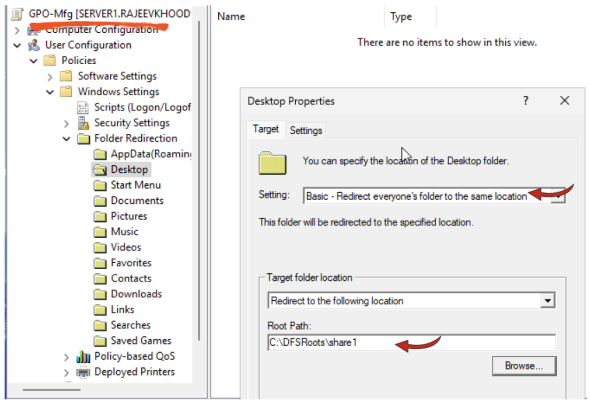


Figure 17.9: Redirects the Desktop and Documents folders for users to a shared folder on server1.

- Prevents the Windows Calculator program from executing.
  User Configuration → Policies → Administrative Templates → System

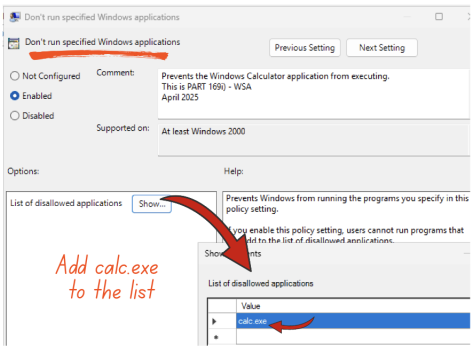


Figure 17.10: Don't run specified Windows applications (here calc.exe)

Step 17

18.1 Testing GPO

- Test your GPO by temporarily moving your server2 computer account into the Mfg OU, and by logging on to it using a user account within the Mfg OU. Next, ensure that GPO-Mfg does not apply to users or computers within the So.Amer OU.

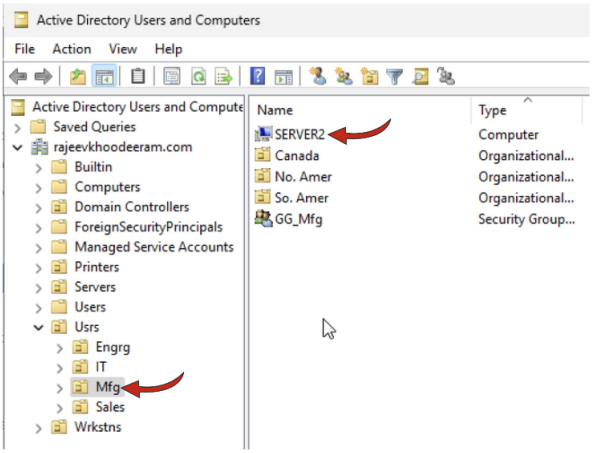


Figure 18.1: Moving Server2 in the Mfg OU

STEP 18

19.1 Creating a conditional forwarder and a trust relationship

A Conditional Forwarder is used to forward DNS queries to specific DNS servers based on the domain name in the query., and Trust relationships are used to establish communication and resource sharing between different Active Directory domains or forests.

- Create a conditional forwarder in DNS to world.com (IP = 192.168.255.188).

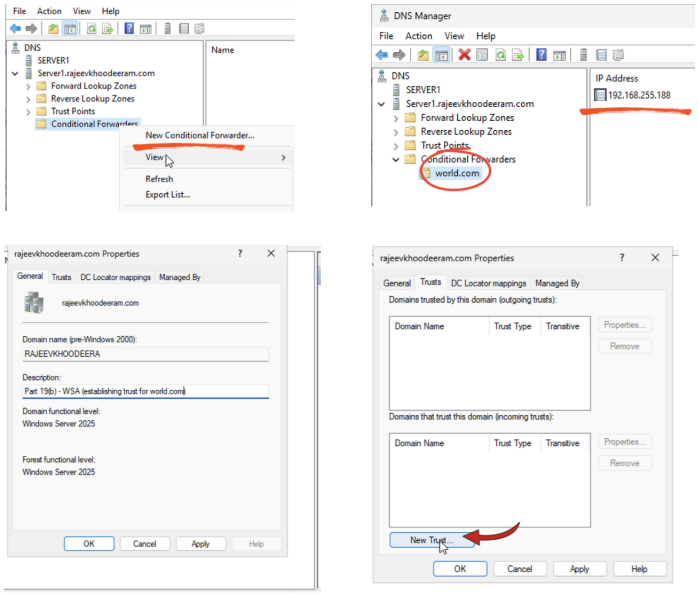


Figure 19.1: Creating a conditional forwarder in DNS of Server1

- Next, create a 2-way transitive Realm trust relationship between your forest and world.com. This is Active Directory Domains and Trusts side. Realm Trust is used when connecting to non-Windows Kerberos v5 realms or even another Windows environment.

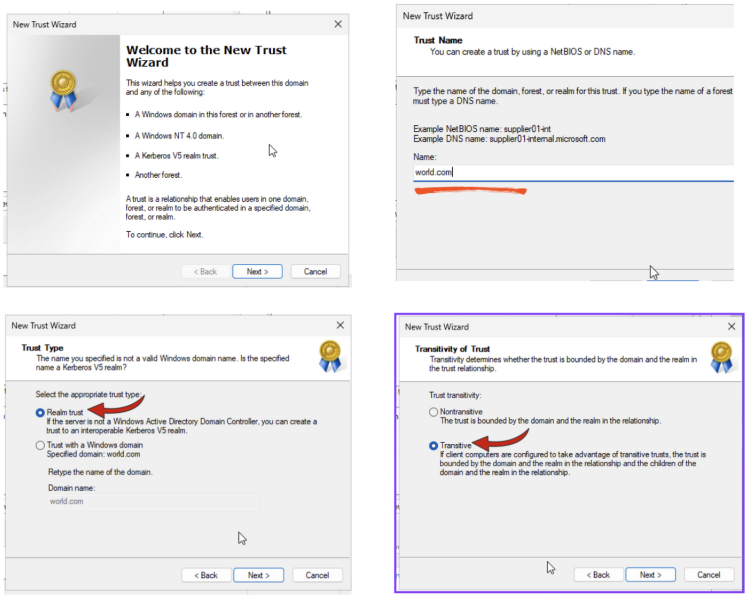


Figure 19.2: Creating a 2-way transitive Realm trust relationship (1)

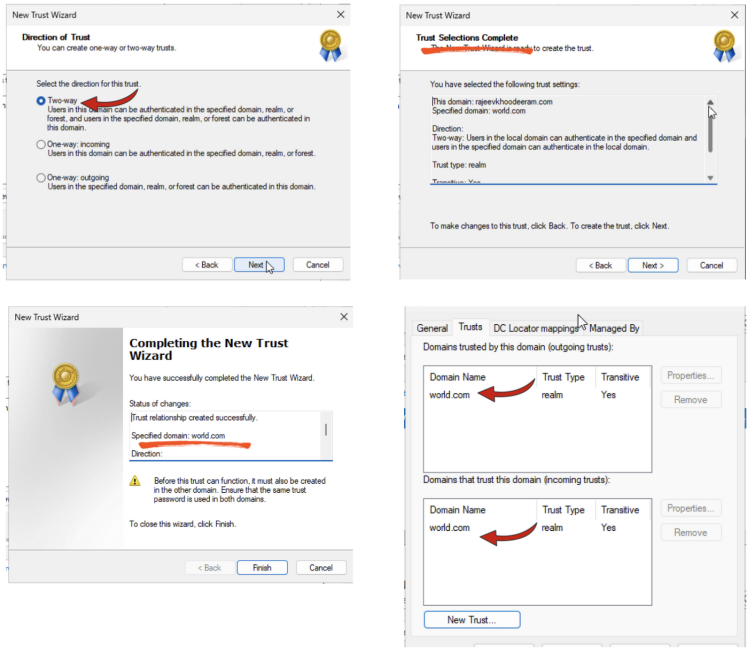


Figure 19.3: Creating a 2-way transitive Realm trust relationship (2)

STEP 19

20.1 Managing sites

- Configure your domain with 3 sites (Kitchener, London, Toronto).

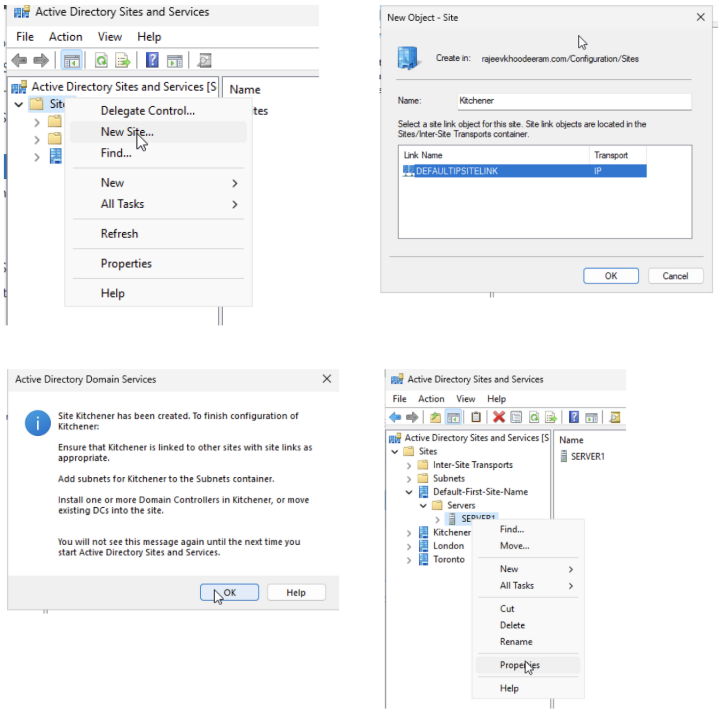


Figure 20.1: Creating 3 sites

- Ensure that your DC account resides within the closest site to your physical classroom location.

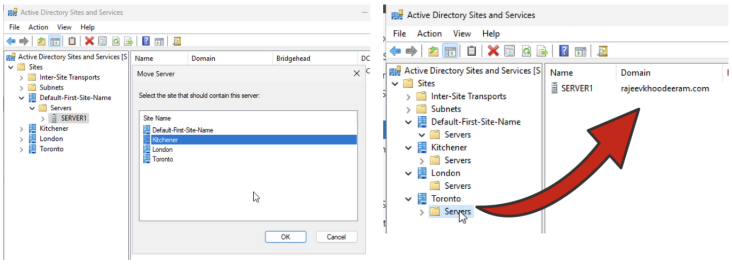


Figure 20.2: Assigning current domain to Toronto site

- Ensure that intersite replication occurs every 90 minutes between all locations.

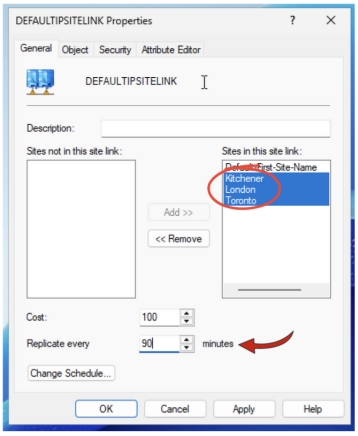


Figure 20.3: Configuring replication between 3 sites

STEP 20

21.1 Configuring Server as a Certificate Authority

Configure server1 as a CA that auto-enrolls all users and computers within the domain for generic user and computer certificates and test your results by restarting server2 and logging in as Administrator in the domain. In the Certification Authority console on server1, right-click Issued Certificates, click Export List and save the list as C:\project\certificates.txt.

- Configure server1 as a CA that auto-enrolls all users and computers within the domain for generic user and computer certificates

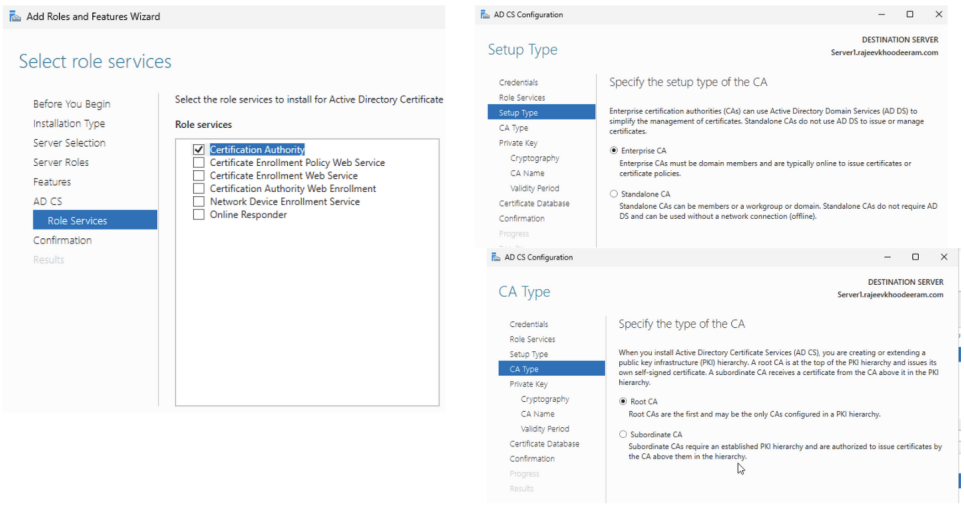


Figure 21.1: Install AD Certificate Services (CA) on Server1 (1)

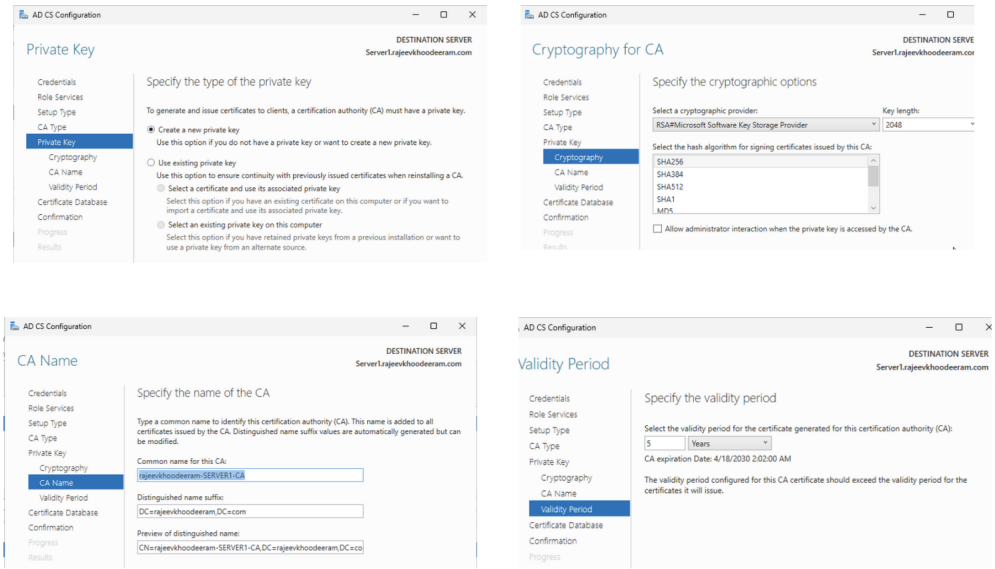


Figure 21.2: Install AD Certificate Services (CA) on Server1 (2)

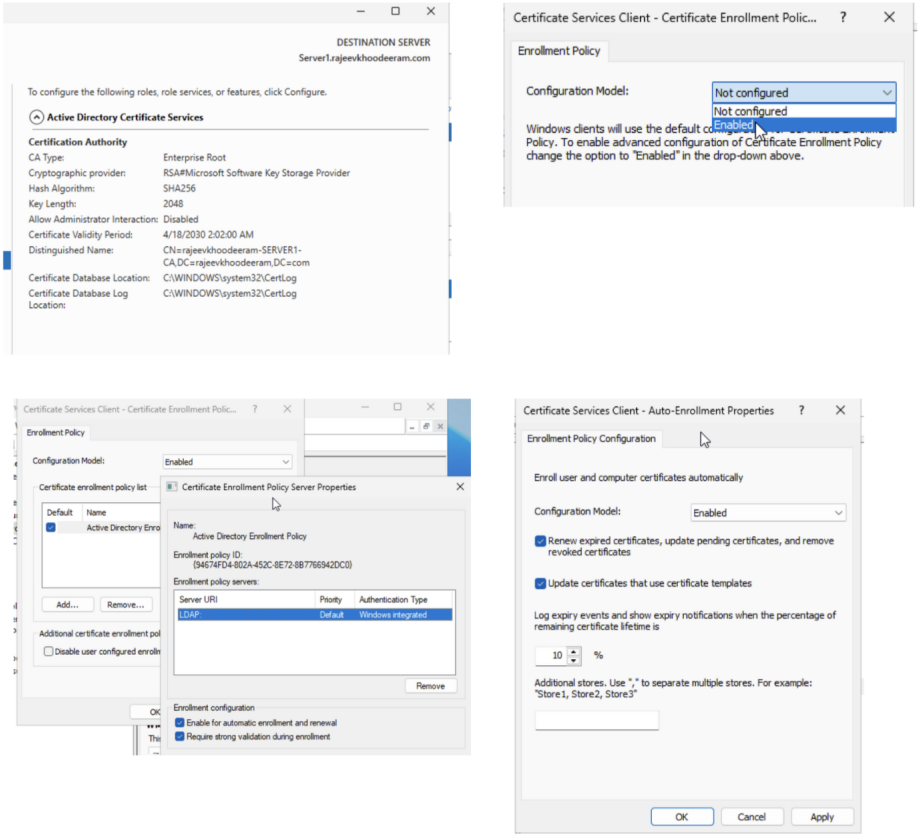


Figure 21.3: Configuring Auto-Enrollment for clients

- Test your results by restarting server2 and logging in as Administrator in the domain.

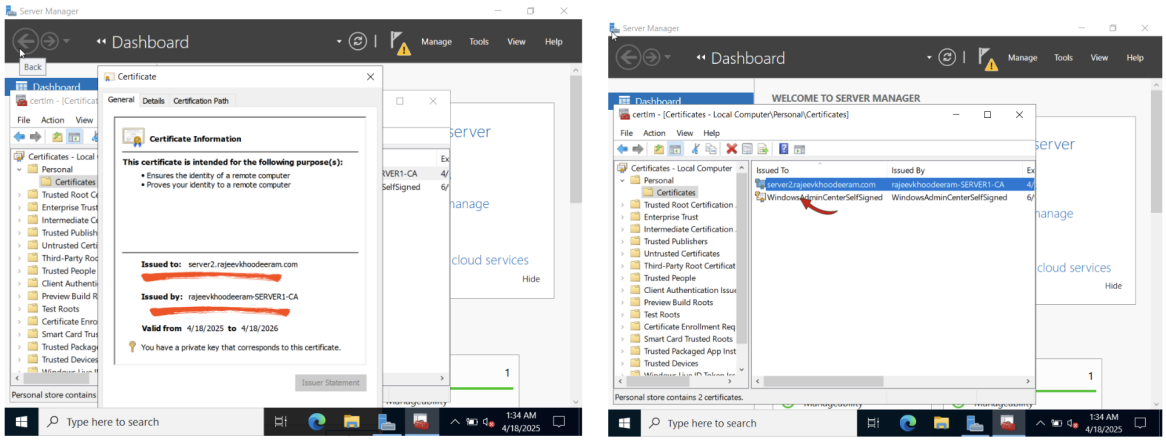


Figure 21.4: Testing the issue of certificates on Server 2

- In the Certification Authority console on server1, right-click Issued Certificates, click Export List and save the list as C:\ project \ certificates.txt.

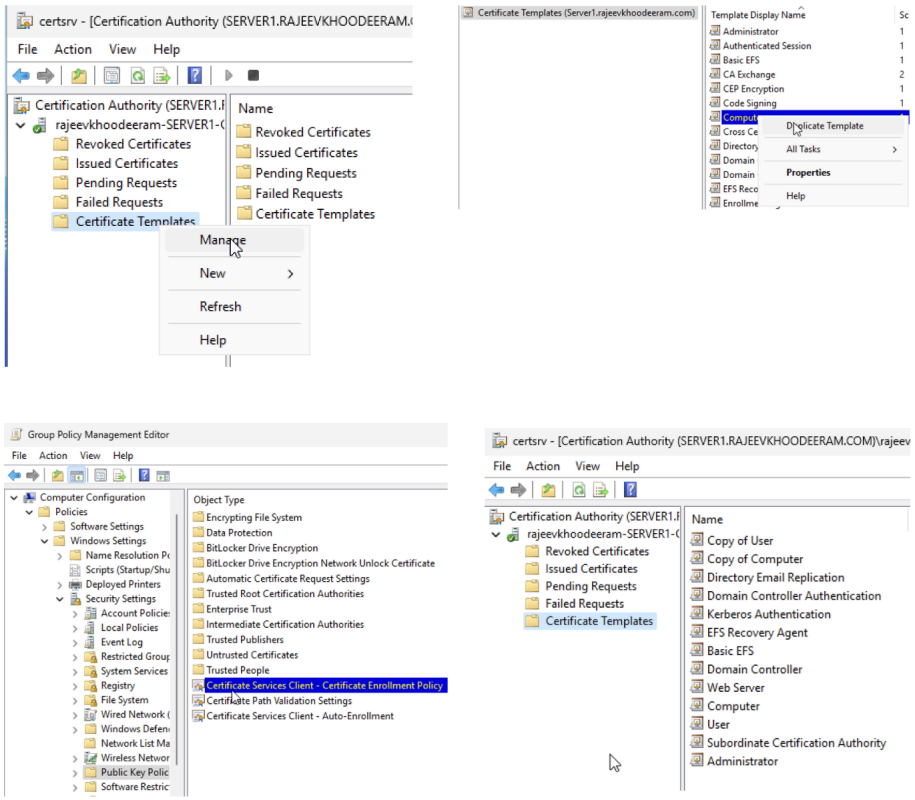


Figure 21.5: Setup Certificate Templates

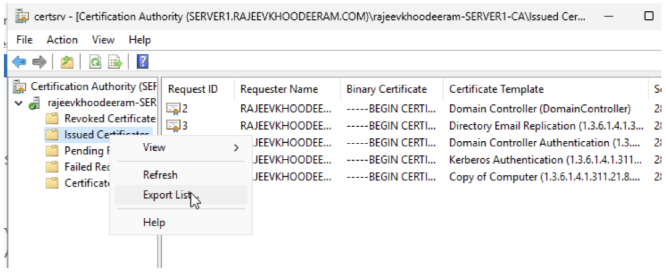


Figure 21.6: Export the List of Issued Certificates

STEP 21

22.1 Server1 as iSCSI SAN

iSCSI SAN (Internet Small Computer Systems Interface; Storage Area Network) is a technology that allows servers (initiators) to connect to remote storage devices (targets) over a TCP/IP network as if the storage was locally attached.

The following key steps are involved in the the configuration of Server 1 as iSCSI SAN (as target server) and Server 2 as iSCSI Initiator :

1. Install the iSCSI Target Server Role on Server 1
2. Create an iSCSI Virtual Disk and configure target and initiator
3. Enable authentication (optional but recommended for security): You can configure CHAP for example
4. On Server2, open iSCSI Initiator
5. Configure the iSCSI Disk and Initialize Disk

- Configure Server1 as an iSCSI SAN that shares a 50GB iSCSI virtual disk to Server2.

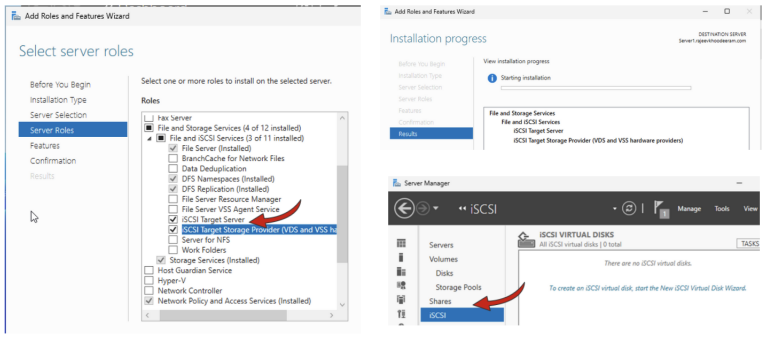


Figure 22.1: Installing the iSCSI Service

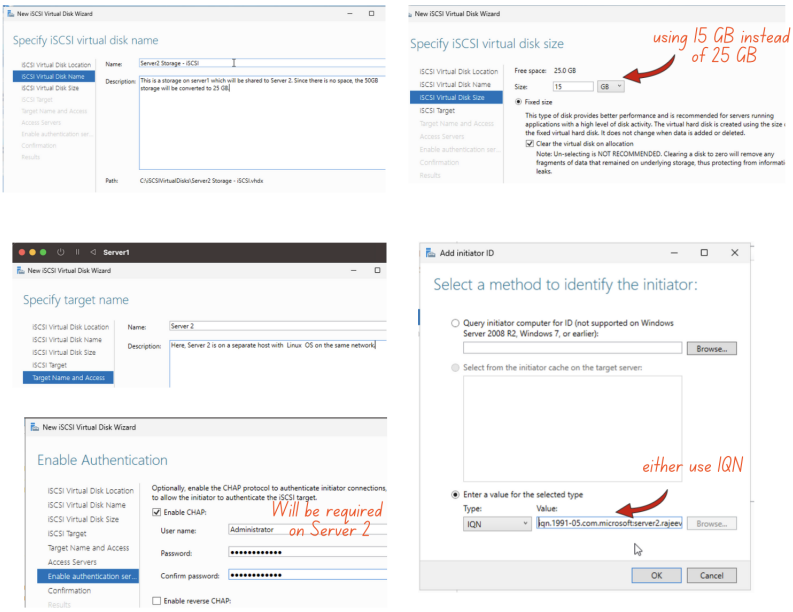


Figure 22.2: Configuring the iSCSI service

- Format this virtual disk with NTFS and ensure that server2 can access it using X:.

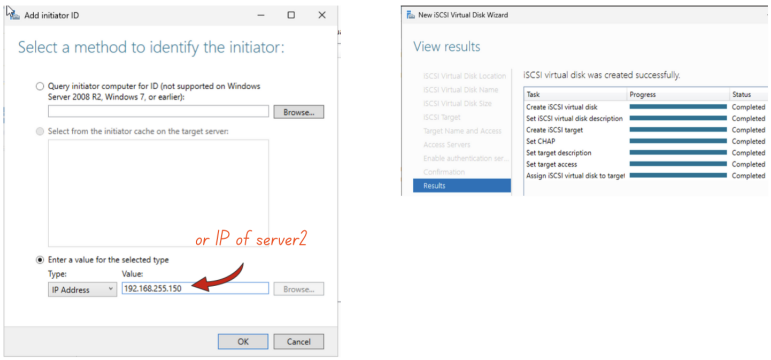


Figure 22.3: Finishing the installation

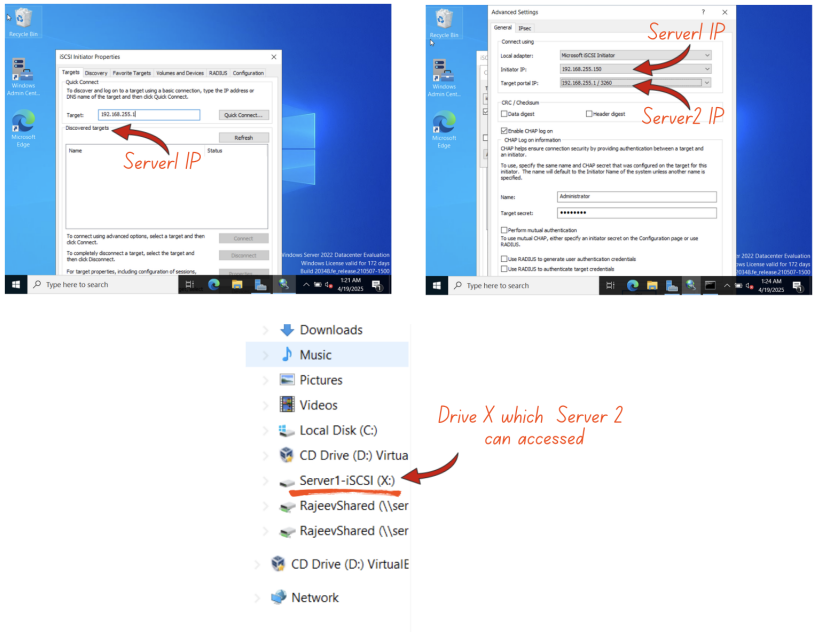


Figure 22.4: Server2 accessing the X drive

- Also ensure that data deduplication is enabled for X:.

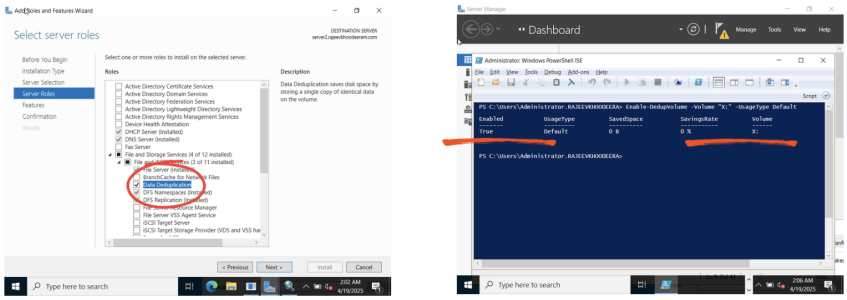


Figure 22.5: Enabling Data Deduplication using either GUI or Powershell

STEP 22

23.1 Performance baseline for server1 and server2

- Take a sample performance baseline for server1 and server2.
  A performance baseline is basically taking a snapshot of the server's performance (CPU, memory, disk, network) when everything is healthy, so you can compare later if things go wrong.

```
Volumes > RajeevShared > PART22_BASELINE.ps1
1  logman create counter "Server1Baseline" -c
2  "\Processor(_Total)\% Processor Time","\Memory\Available MBytes","\LogicalDisk(_Total)\% Free Space"
3  "\Network Interface(*)\Bytes Total/sec"
4  -si 15 -o "C:\project\Server1Baseline.html"
5
6  logman start Server1Baseline
7  timeout /t 300
8  logman stop Server1Baseline
```

Figure 23.1: Powershell script used to generate the baseline

- Save these baselines as server1baseline.html and server2baseline.html in the C:project folder on server1.

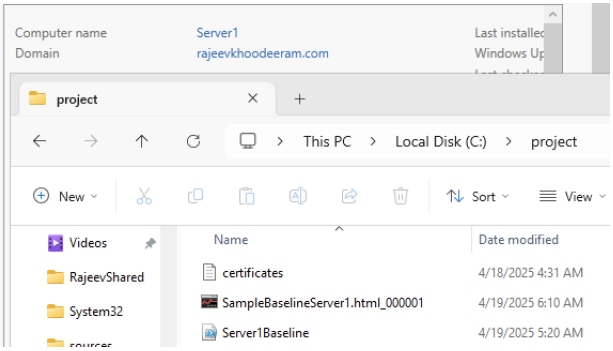


Figure 23.2: Server 1 Baseline

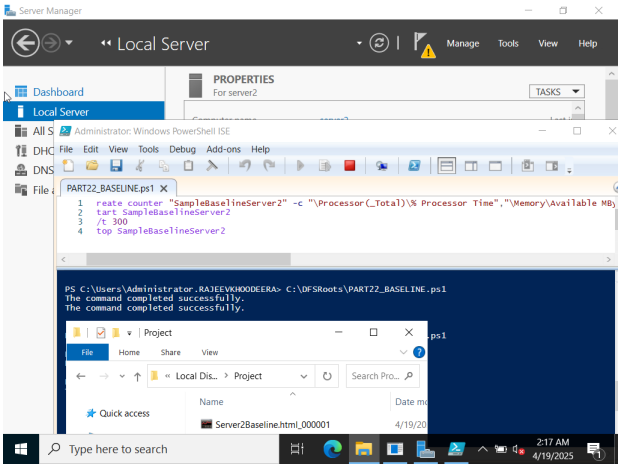


Figure 23.3: Server 2 Baseline

STEP 23

24.1 Windows Server Update Services

- Configure server1 as a WSUS server that provides updates to the computers within the domain (do not download the updates – only download the Windows Update Catalog).

  Some key steps for installing and using WSUS server are :

  – Install WSUS Role on Server1

    1. Click Manage → Add Roles and Features.
    2. Click Next → Next until you reach Server Roles.
    3. Check Windows Server Update Services.
    4. Under Role Services, select: WSUS Services : Windows Internal Database (or use SQL Server if you have one, but WID is fine for basic setup)

  – Post-Install Tasks : Select your content location → Pick a folder where WSUS will store updates (example: D:\ WSUS \).

  – Perform First Catalog Synchronization

    1. In WSUS console, right-click Server1 → Synchronize Now.
    2. WSUS will connect to Microsoft, and only pull metadata (Windows Update Catalog).

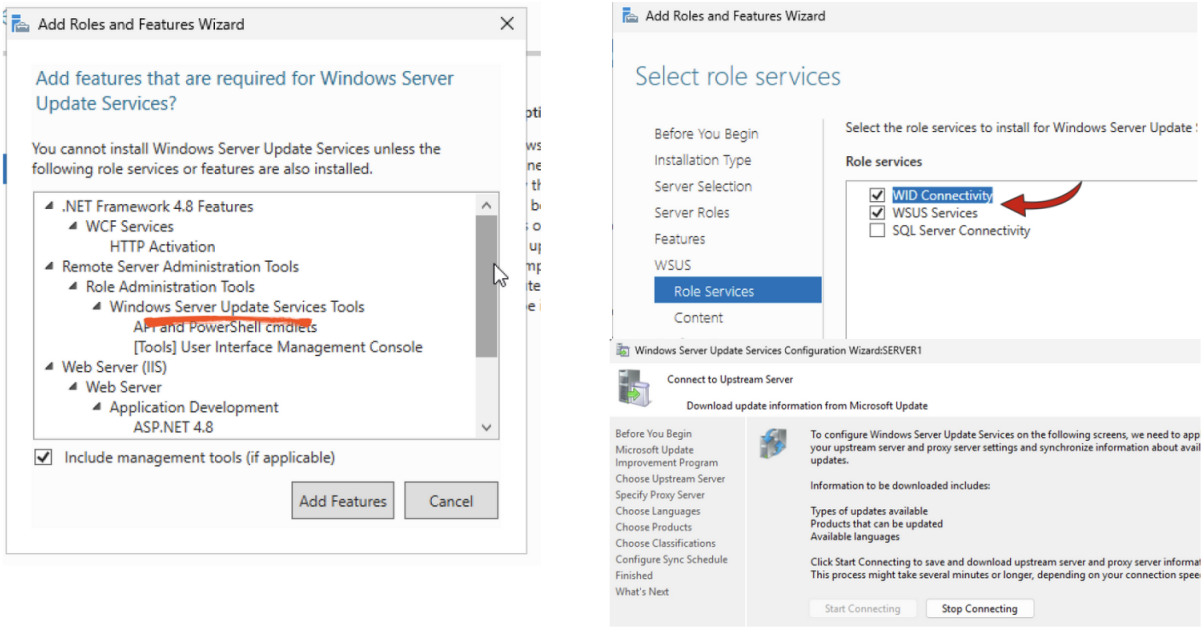


Figure 24.1: Installation of WSUS server

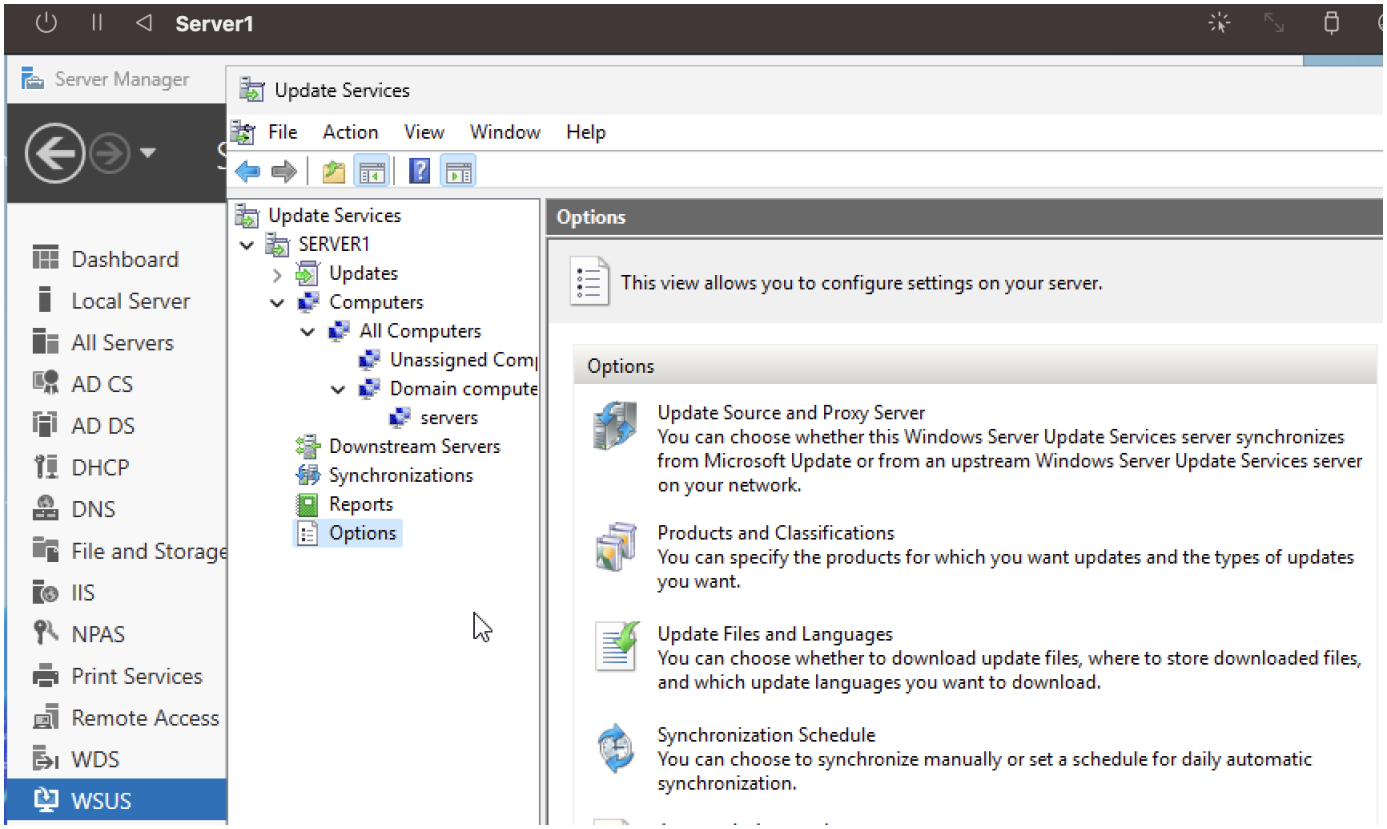


Figure 24.2: WSUS server on Server1 - PDC

STEP 24

25.1 Installation and configuration reports using PowerShell

In this section of the report, sample powershell scripts are executed to get details of all services that have been installed throughout the project (all these files are included in the project zip file).

25.1.1 DHCP (scope, lease, etc): file1.txt

25.1.2 WDS: file2.txt

25.1.3 Active Directory - OUs & GP: file3.txt

25.1.4 VPN: file4.txt

25.1.5 FailOver servers: file5.txt

25.1.6 DFS: file6.txt

25.1.7 SAN: file8.txt

25.1.8 WSUS: file9.txt

25.1.9 iSCSI: file10.txt

25.1.10 IP configuration : file11.txt

25.1.11 Firewall Profile: file15.txt

25.1.12 Timezone: file16.txt

25.1.13 DNS: file18.txt

BONUS

26.1 Bonus 1: IIS / Docker container

26.1.1 Installation of Docker

The following steps are used to install docker as an IIS Container on Server 3 (Windows Server 2022 which is hosted on the Linux Laptop):

- Install-WindowsFeature -Name Containers Install the Containers Feature
- Install-Module -Name DockerMsftProvider -Repository PSGallery -Force
- Invoke-WebRequest "$https://download.docker.com/win/static/stable/x86_64/docker-24.0.7.zip$" -$OutFile$"$C:\docker.zip$"
- Expand-Archive -Path "$C:\docker.zip$" $-DestinationPath$"$C:\docker$"
- Copy-Item "$C:\docker\docker*$" $-Destination$"$C:\ProgramFiles\Docker$" $-Recurse$
- $env:Path += "$;C:\ProgramFiles\Docker$" [Environment]::SetEnvironmentVariable("Path", $env:Path, [System.EnvironmentVariableTarget]::Machine$)
- dockerd –register-service
- Start-Service docker
- docker version or docker info

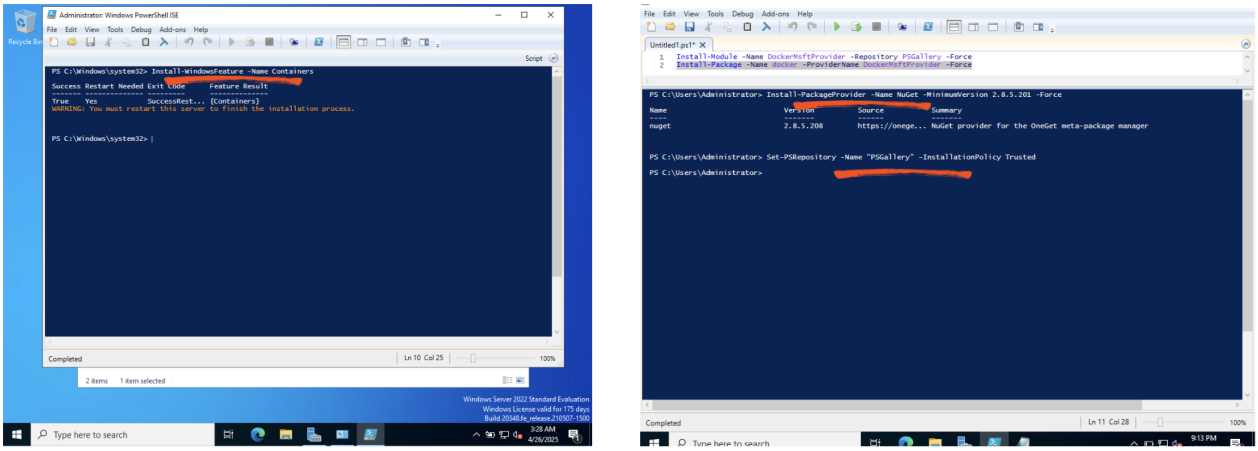


Figure 26.1: Installation of Docker container on Server 3

26.1.2 Pulling and running the container

- Pull the IIS image
  docker pull mcr.microsoft.com/windows/servercore/iis

- Run the container
  docker run -d -p 80:80 –name myiis mcr.microsoft.com/windows/servercore/iis

  It is important to note that :

  - Runs the container in the background (-d)
  - Maps port 80 on the host to port 80 in the container (-p 80:80)
  - Names it myiis

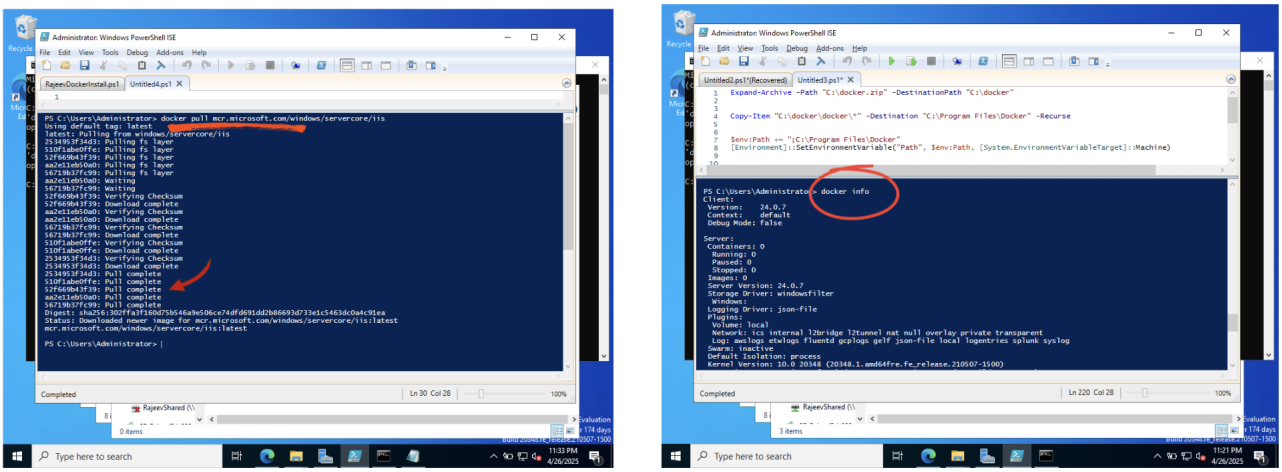


Figure 26.2: Pulling the IIS container from Windows website and naming it myIIS

26.1.3 Check running containers

The running container can be checked using *docker ps* and the output is shown as follows :

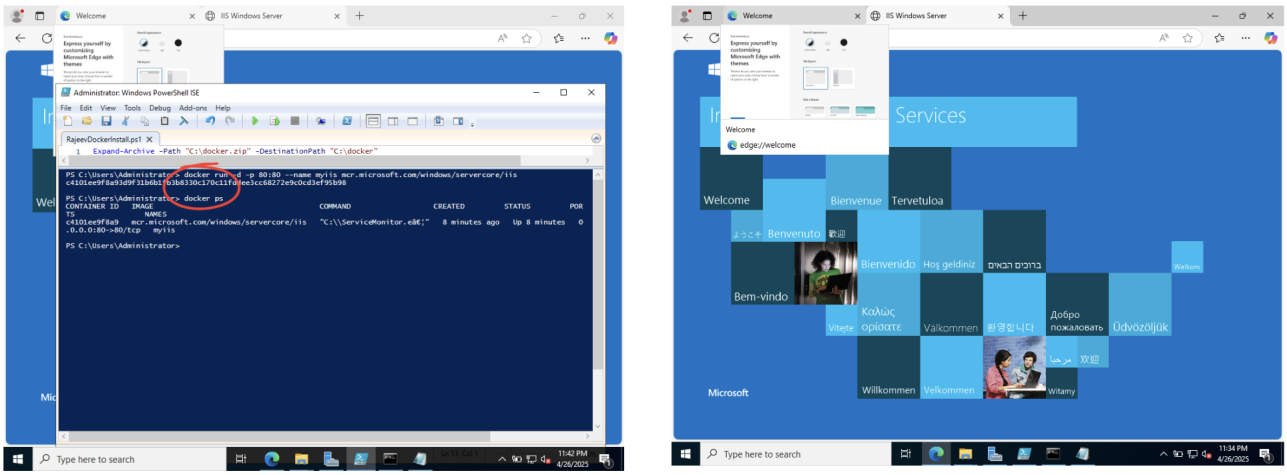


Figure 26.3: Checking if docker is installed and getting the running docker container

26.1.4 Testing the IIS

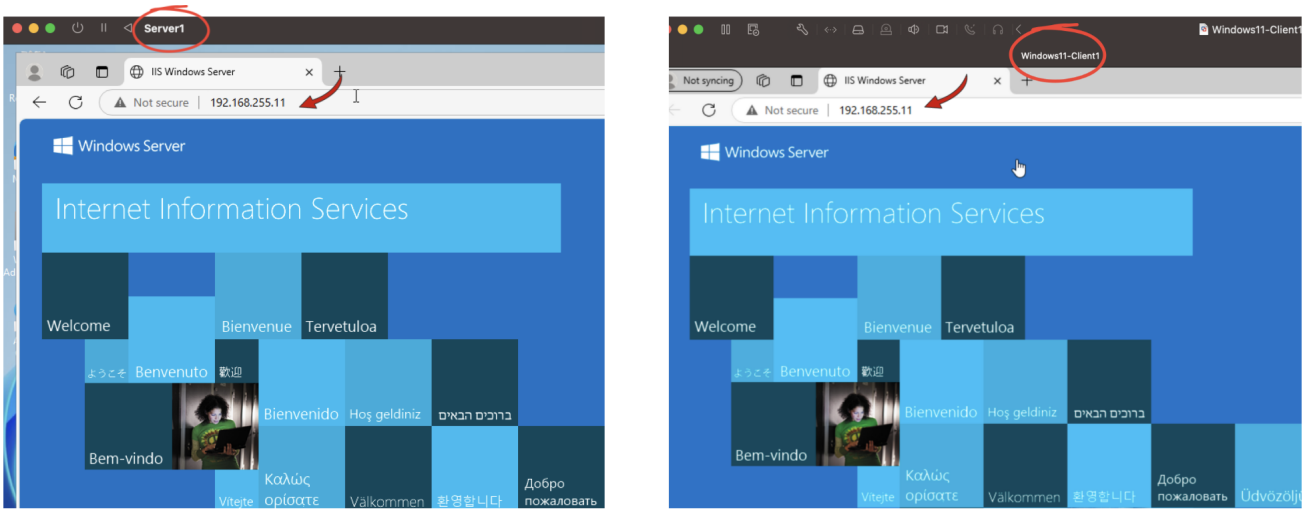
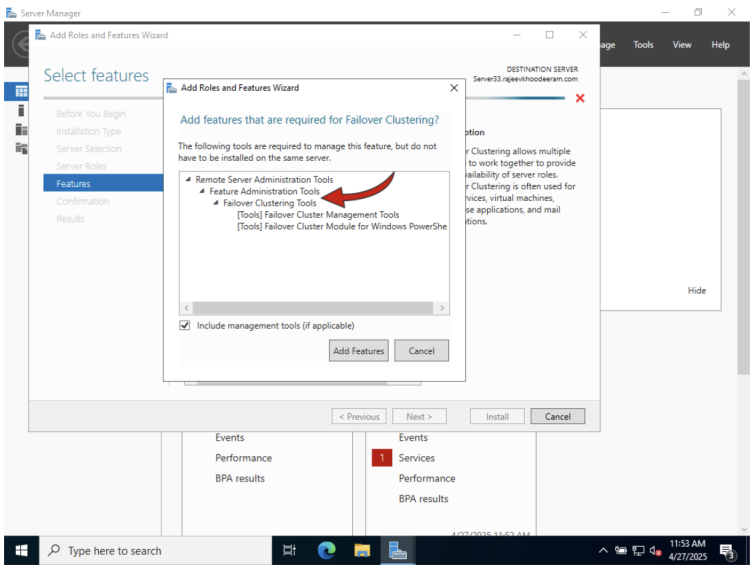


Figure 26.4: Testing the IIS container from Server 1 and from Client 1 (Windows client)

26.2 Bonus 2: Failover Clusters



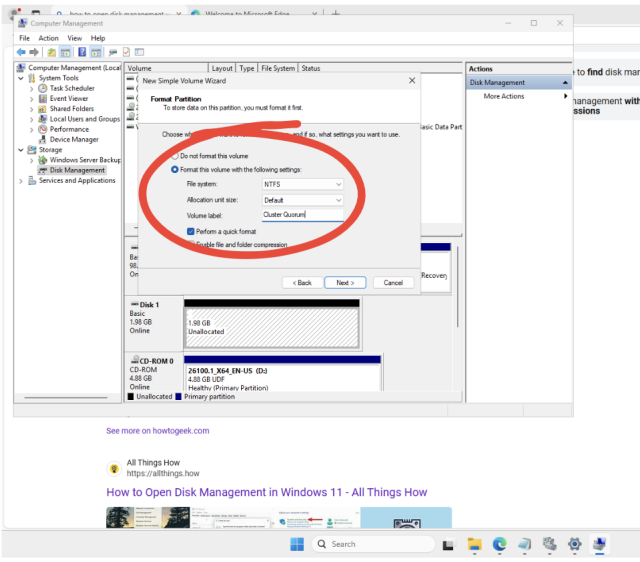
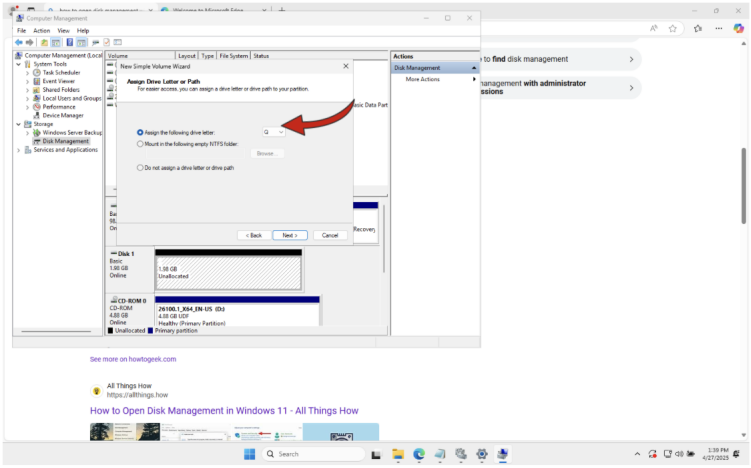
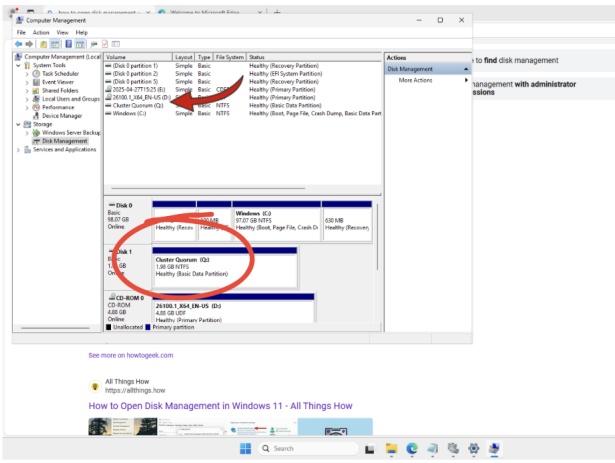


Figure 26.5:





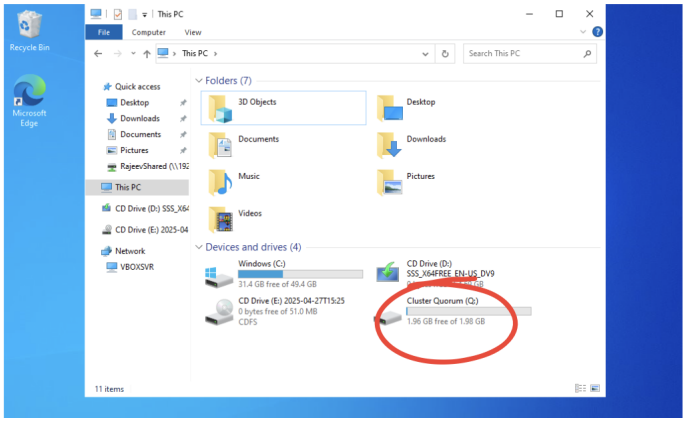
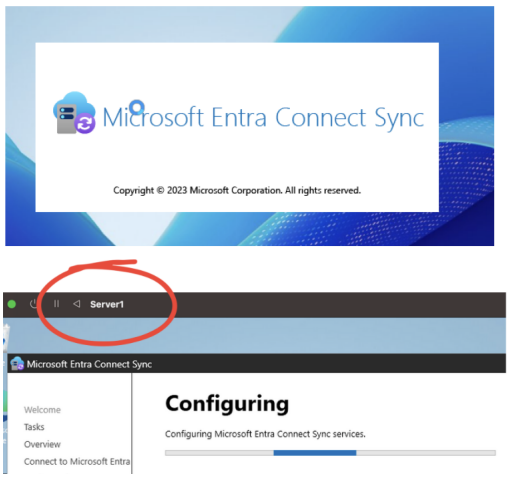


Figure 26.6:

26.3 Bonus 3: Going beyond....in the cloud

In this section, we shift our focus from on-premise to cloud management of devices using three main platforms provided by Microsoft namely :

26.3.1 Microsoft Entra ID



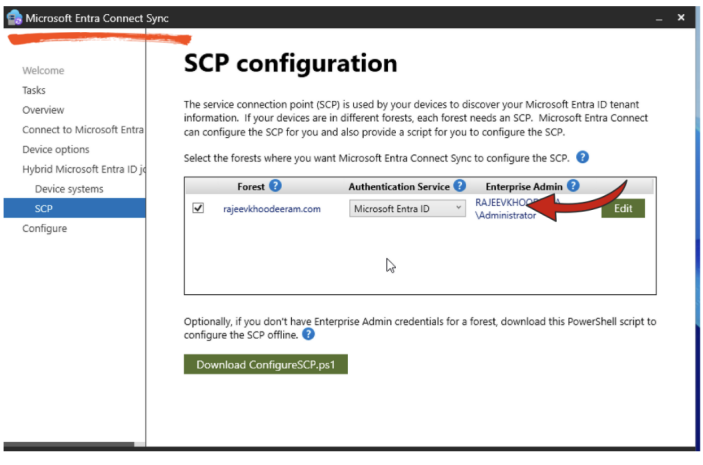


Figure 26.7: Synchronization using Entra Connect from Server 1

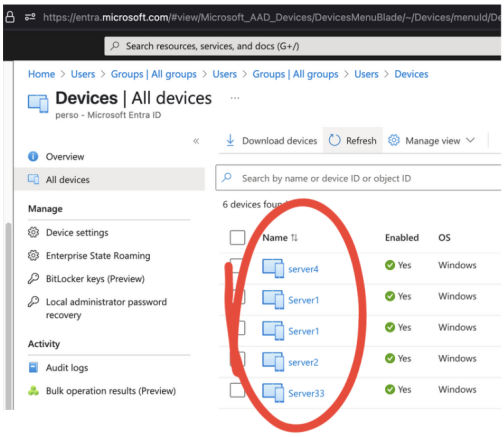


Figure 26.8: All devices from on-premises are now visible on Entra platform online

26.3.2 Microsoft Intune

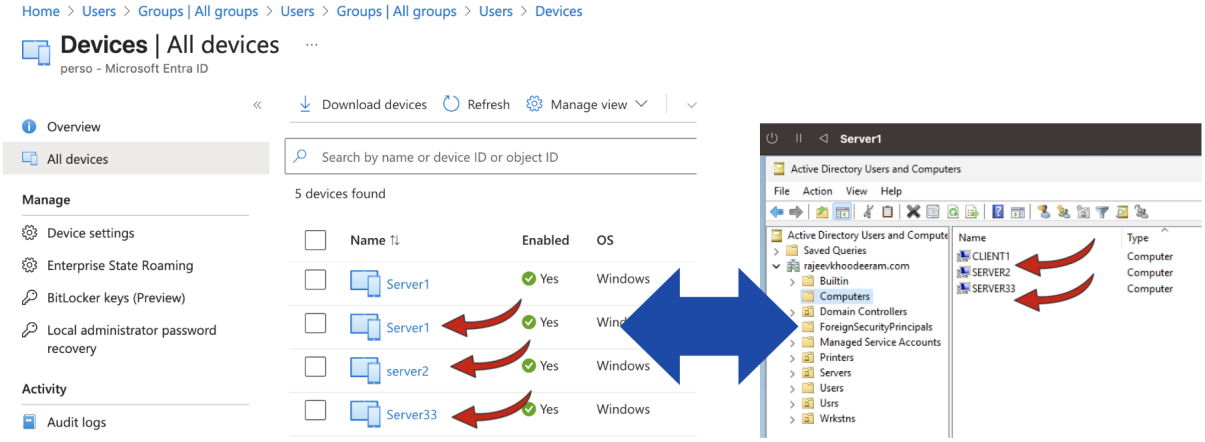


Figure 26.9: On-premise Devices as they appear on Microsoft Intune

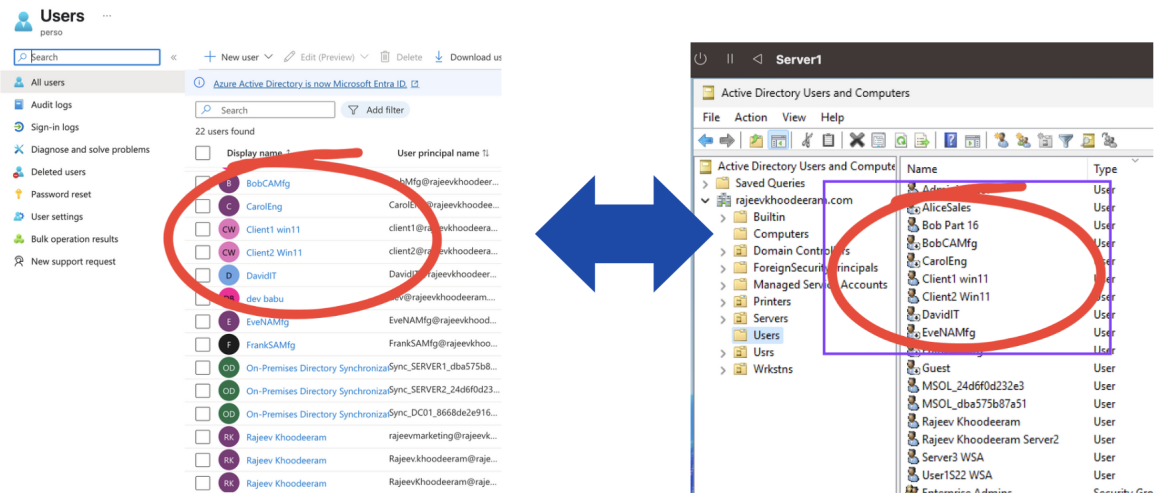


Figure 26.10: On-premise Users as they appear on Microsoft Intune

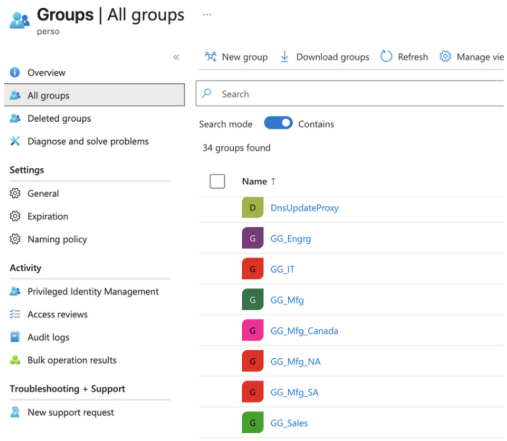


Figure 26.11: Groups of on-premise as they appear on Microsoft Intune

26.3.3 Microsoft Azure

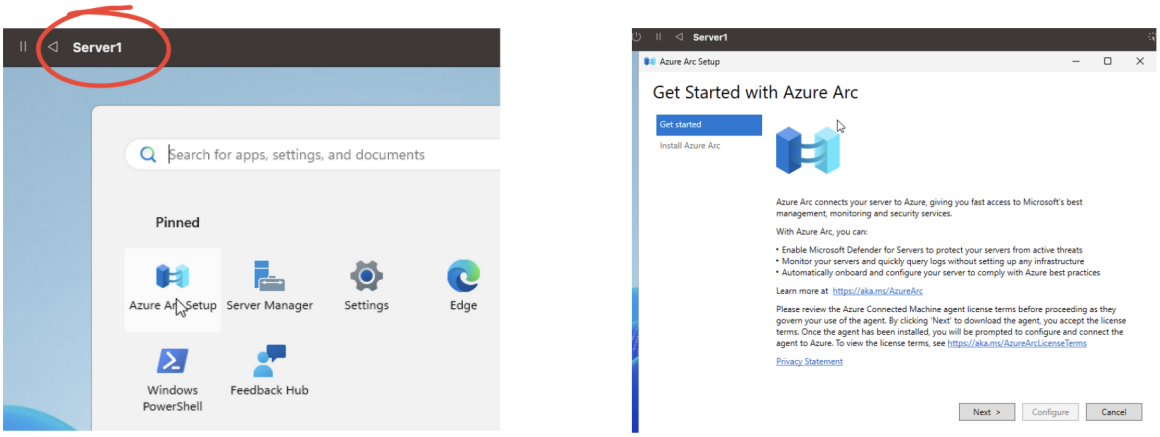


Figure 26.12: Installation and configuration of Azure Arc on Server 1 (1)

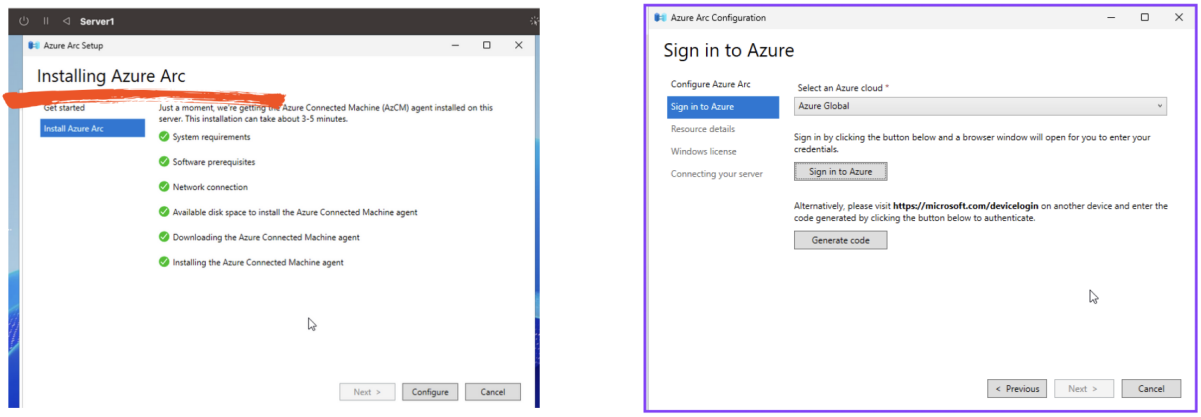


Figure 26.13: Installation and configuration of Azure Arc on Server 1 (2)

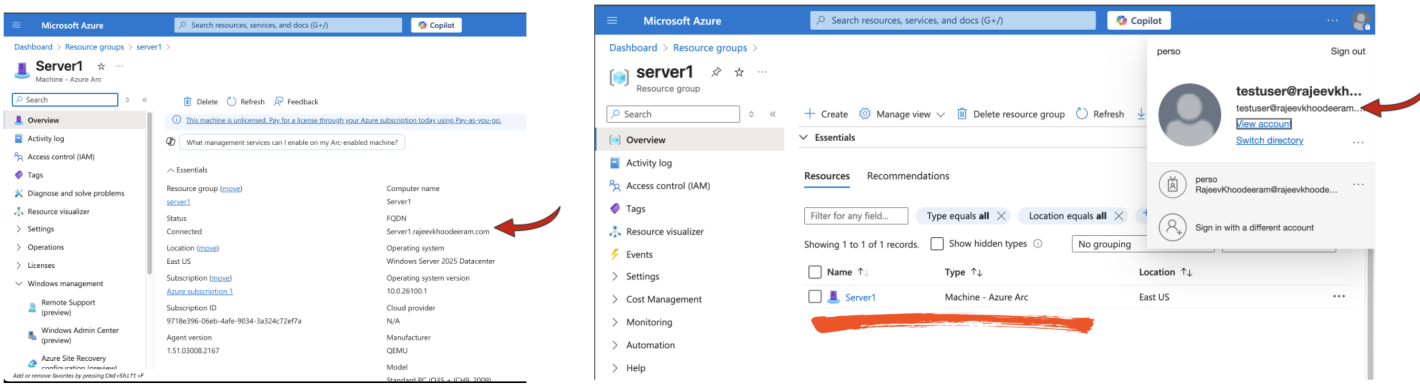


Figure 26.14: Deploying resources on Azure

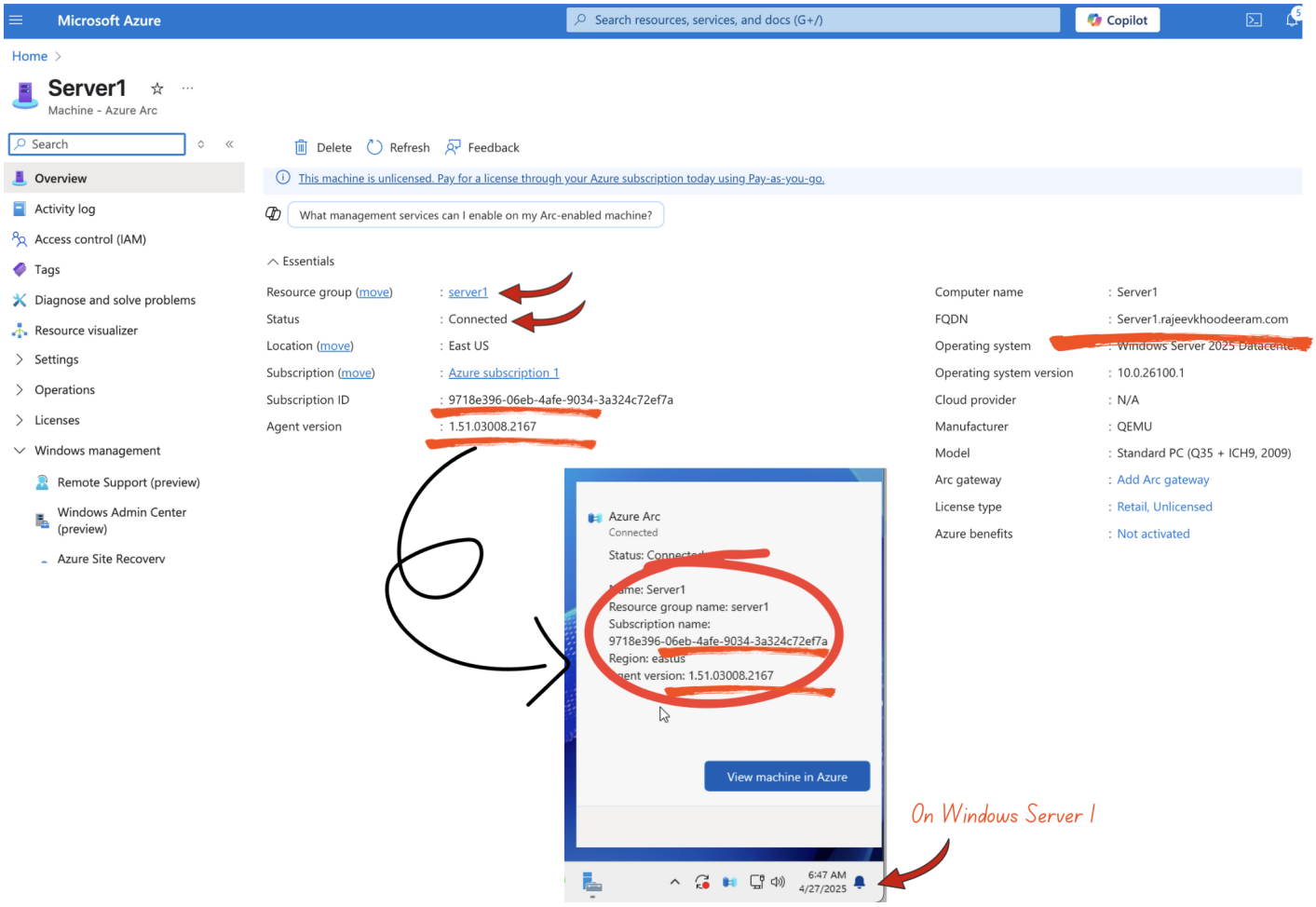


Figure 26.15: An example of one resource (Server1) as it appears on Azure

Reflection

27.1 Concluding words

Completing the Windows Server Administration course has been a transformative experience for me, both technically and professionally. After completing the Windows Client Administration, now we are armed with the skills on how to administer the Windows Server and some key services to deploy on an enterprise network. Over the past weeks, I had the opportunity to work hands-on with core services like DNS, DHCP, WDS, DFS, VPN, Certificate Authority (CA), and RRAS, each of which forms the backbone of a modern enterprise network infrastructure.

This journey allowed me to move beyond theoretical knowledge and develop real-world skills in configuring, managing, and troubleshooting critical server roles. I gained a solid understanding of how DNS and DHCP work together to manage name resolution and IP address assignments within a domain (including scope, exclusion, etc). Setting up WDS taught me the value of automation in operating system deployments, and working with DFS deepened my appreciation for efficient, resilient file sharing across the network. Configuring VPN and RRAS services provided me with hands-on experience in enabling secure remote access — an essential skill in today's remote and hybrid work environments. Setting up a Certificate Authority (CA) also gave me insight into how public key infrastructure (PKI) supports authentication, encryption, and digital security within an organization. I go beyond the requested deliverables to acquire extensive hands on using cloud facilities provided by Microsoft namely Entra ID, Intune and Azure, which allow me to mimic a real-life network settings in an entreprise.

Throughout the course, I developed stronger troubleshooting skills, improved my PowerShell scripting capabilities, and built a solid foundation for advanced topics such as high availability, disaster recovery, and security hardening. I also learned the importance of planning and documentation — ensuring that every configuration is both functional and maintainable. Above all, this course reinforced the value of patience, structured problem-solving, and continuous learning in the IT field. It was incredibly rewarding to see a fully functioning network, built from scratch, come together as the result of careful planning and execution. I convey my sincere gratitude to *Mr Mohammed Ghori* for providing ongoing support to the class with additional materials.

I feel more confident than ever stepping into roles that require Windows Server expertise, and I am excited to continue expanding my skills further in systems administration, cloud integration, and cybersecurity, and *the adventure continues...*