Windows Server Administration

1- DHCP Server

2- Router and Routing Protocol

3- DHCP Relay Agent

4- Domain Environment and AD Installation

5- Domain Name Server (DNS)

6- AD Object and the Domain Adminstration

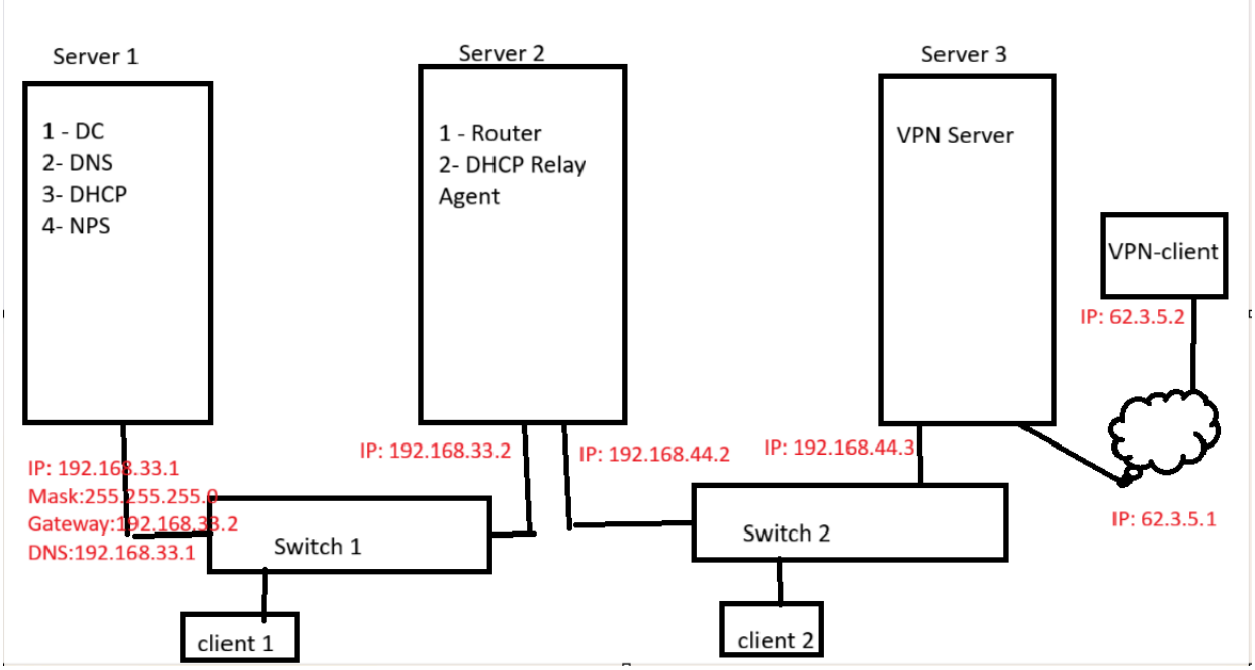
7- Group Policy Management (GPM)

8- Virtual Private Network (VPN)

9- Network Policy Service (NPS) → (RADIUS Server)

🗺️ Lab Topology

📸 Lab Network Diagram



🔧 Lab Components

- **Server 1**
  - Domain Controller (DC)
  - DNS Server
  - DHCP Server
  - NPS (RADIUS) Server
  - IP: `192.168.33.1`
  - Gateway: `192.168.33.2`
  - DNS: `192.168.33.1`
- **Server 2**
  - Router (RRAS)
  - DHCP Relay Agent
  - IP1: `192.168.33.2`
  - IP2: `192.168.44.2`
- **Server 3**

- VPN Server
- IP: `192.168.44.3`

- **Clients**
  - Client 1 (LAN1 via Switch 1)
  - Client 2 (LAN2 via Switch 2)
  - VPN Client (Public IP `62.3.5.2` → connects to VPN Server `62.3.5.1`)

▶️ 1: DHCP Server

🎯 Objective

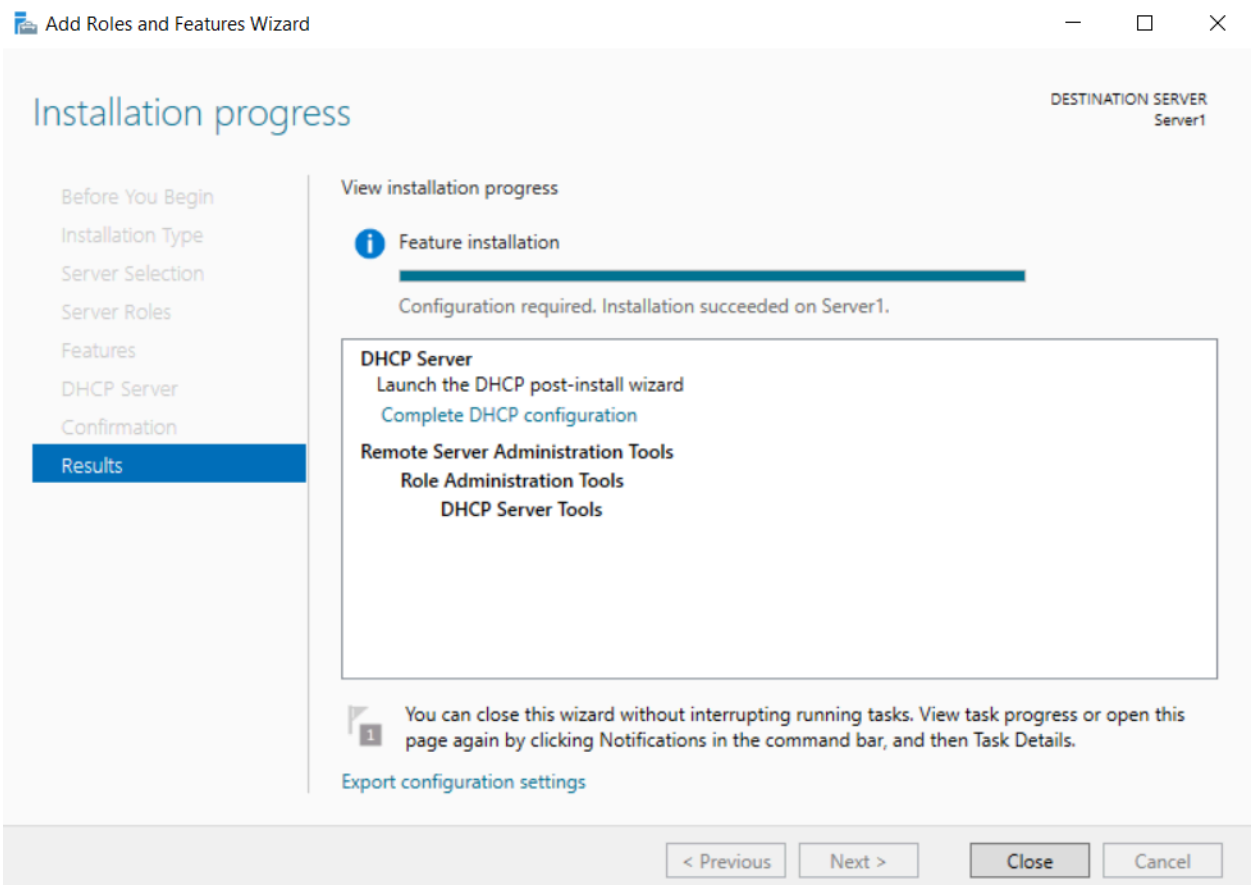
Set up a **DHCP Server** to automatically assign IP addresses to clients.

📝 Steps

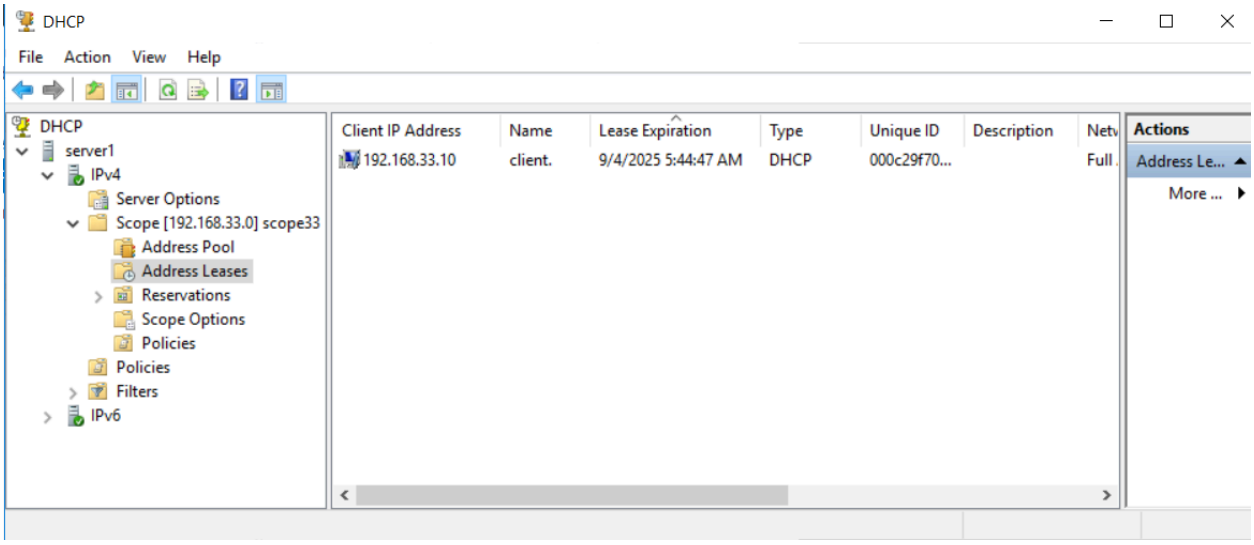
1. Open **Server Manager → Add Roles and Features**.
2. Select **DHCP Server** role and install it.
3. Open **DHCP Management Console**.
4. Create a **New Scope** → Define IP range, subnet mask, and lease duration.
5. Configure **Scope Options** (default gateway, DNS server).
6. Authorize the DHCP server in Active Directory.
7. On the client, set IP configuration to **Obtain automatically**.
8. Test lease by running `ipconfig /renew` on client.

📸 Screenshots

- Installation of DHCP Role



- Client IP Lease Verification



✅ Outcome

- DHCP successfully assigned IPs to clients.

- Network devices automatically received valid IP configuration.

▶️ 2: Router & Routing Protocol

🎯 Objective

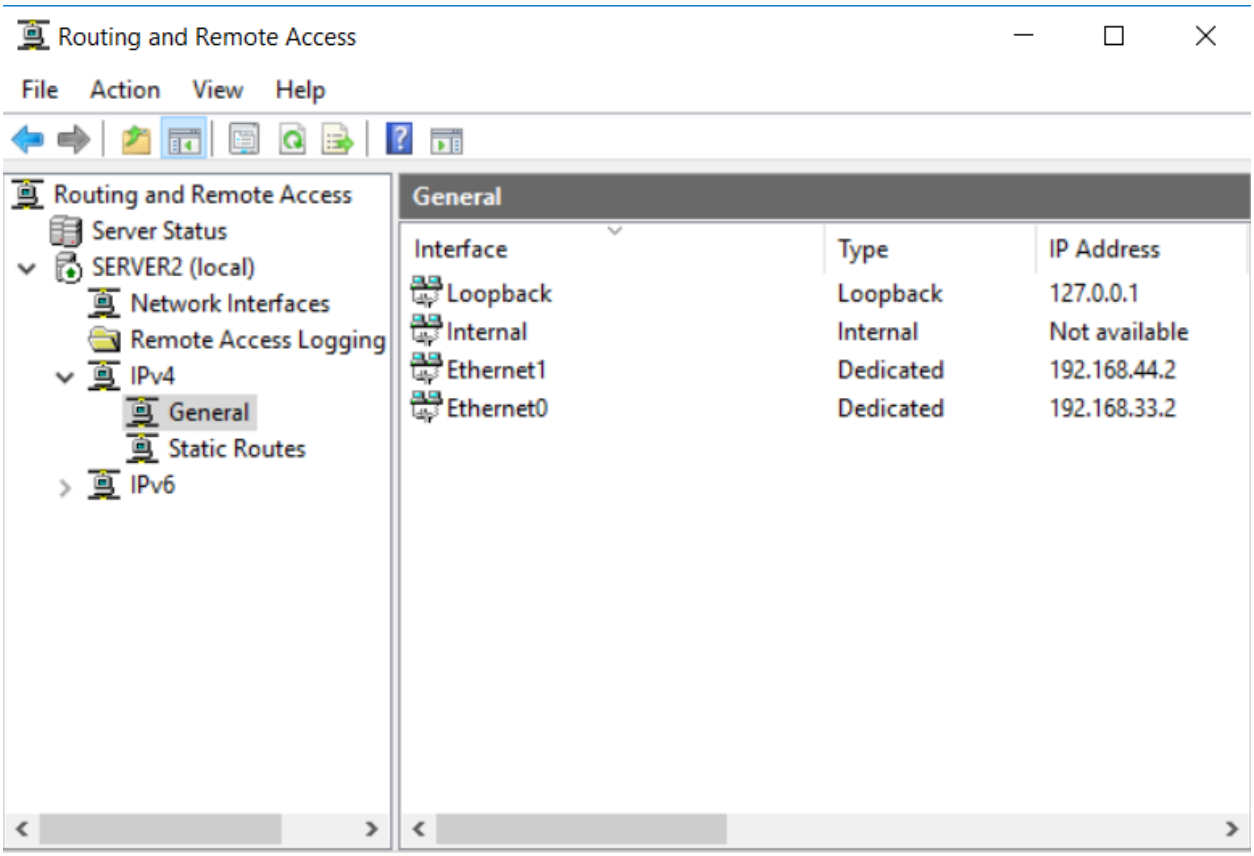
Enable **routing between different subnets** using Routing and Remote Access (RRAS).

📝 Steps

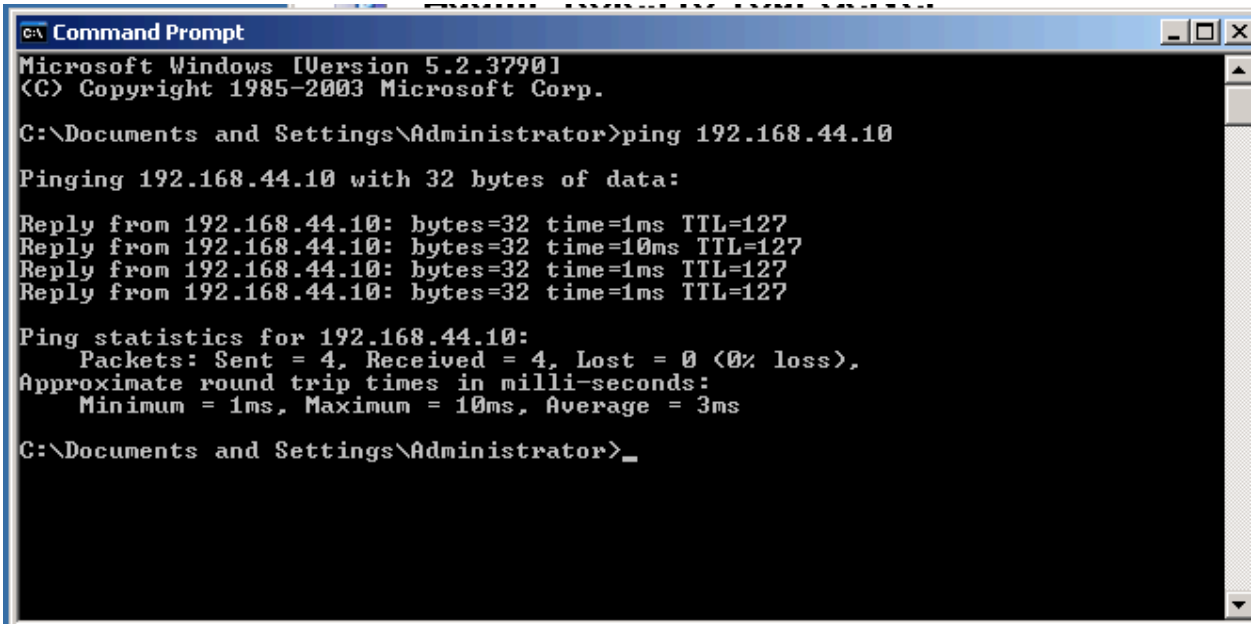
1. Install **Remote Access** role from Server Manager.
2. Open **RRAS Console → Configure and Enable Routing and Remote Access**.
3. Select **LAN Routing**.
4. Add **two NICs** (each connected to different networks).
5. Test connectivity using `ping` between clients on different subnets.

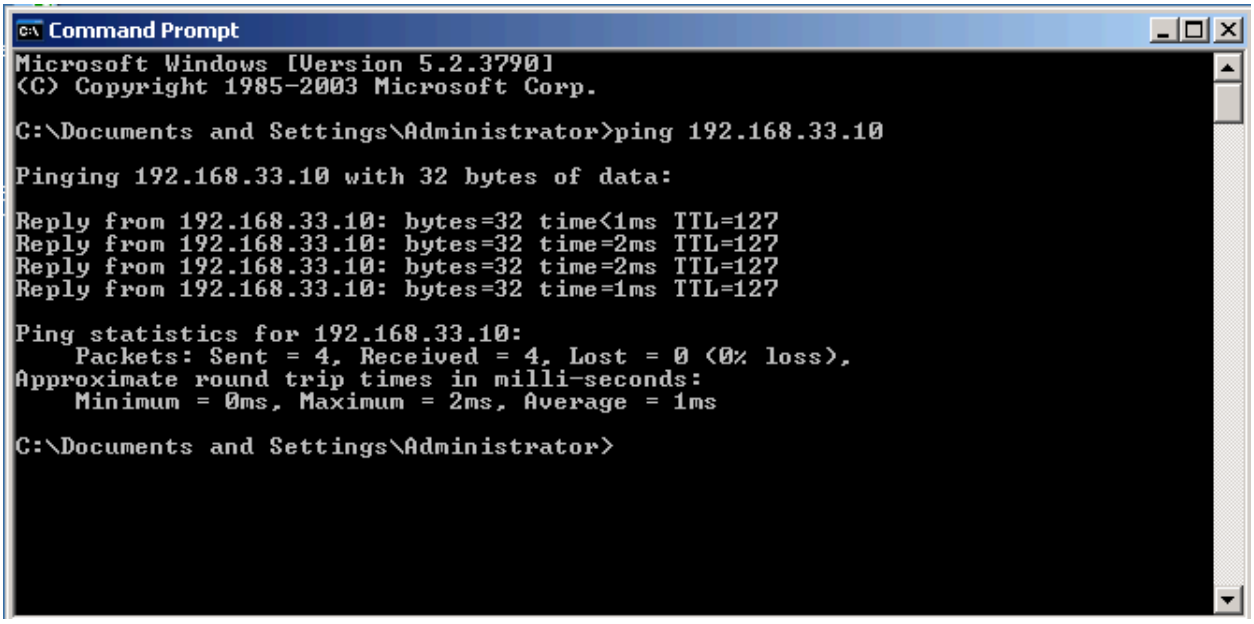
📸 Screenshots

- RRAS Setup



- Ping Test Between Subnets





✅ Outcome

- Successfully enabled communication between two networks.

▶️ 3: DHCP Relay Agent

🎯 Objective

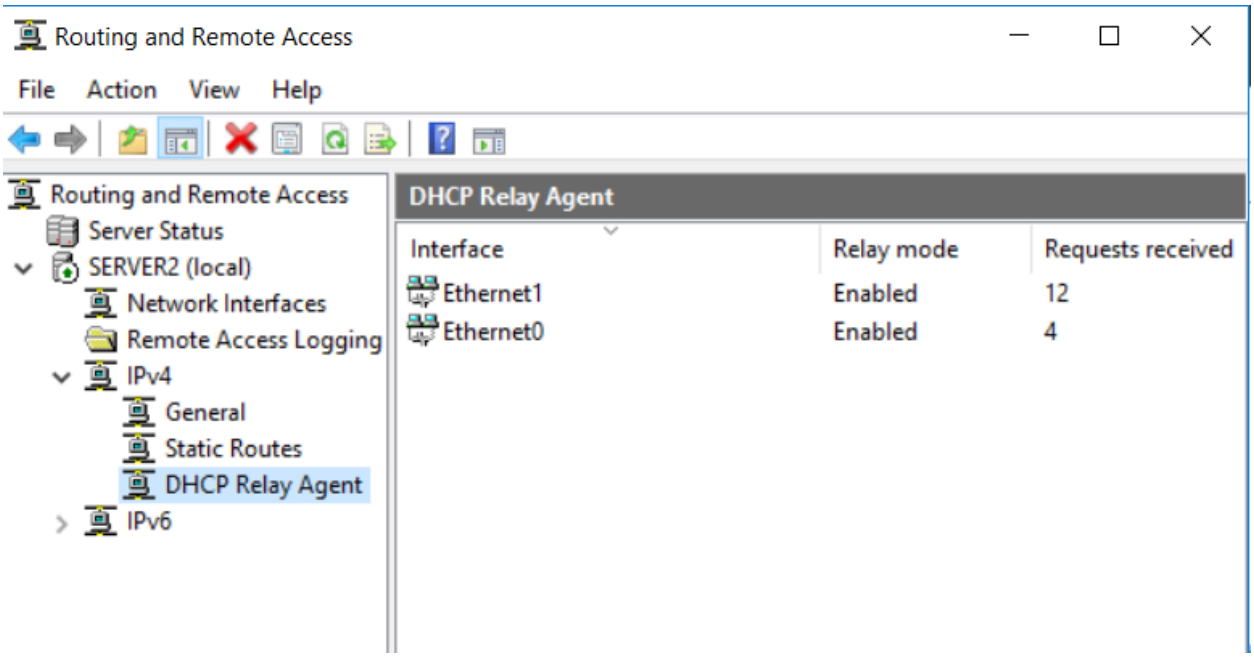
Forward DHCP requests across **different networks** using a Relay Agent.

📝 Steps

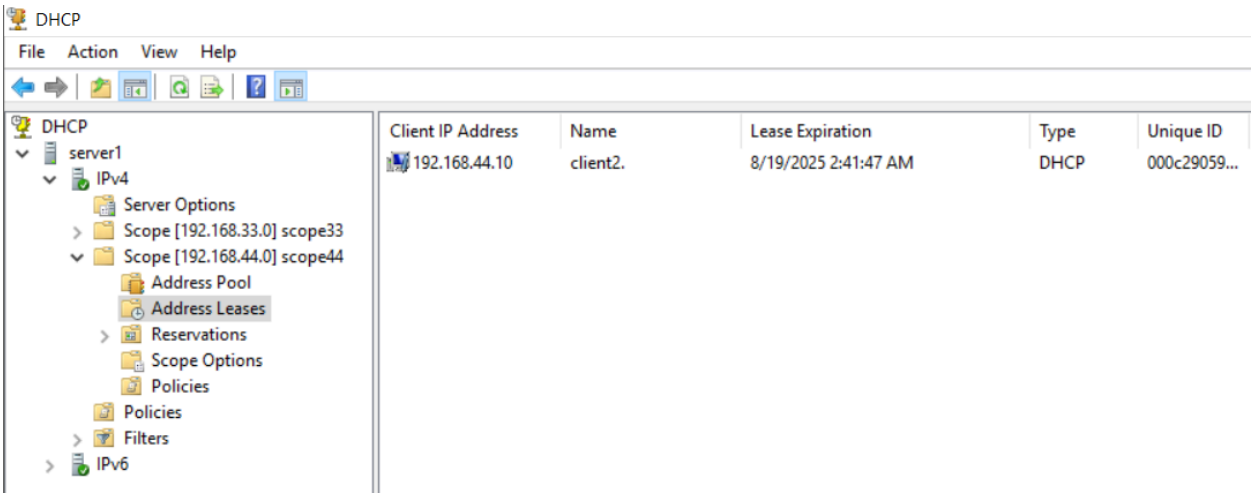
1. Install **Remote Access** role (if not already).
2. Open **RRAS Console → IPv4 → General → New Routing Protocol**.
3. Select **DHCP Relay Agent**.
4. Add the **DHCP Server IP**.
5. Configure interfaces to forward DHCP broadcasts.
6. Test by requesting an IP from a client on a different subnet.

📸 Screenshots

- Adding DHCP Relay Agent



- Client Lease From Remote DHCP



✅ Outcome

- Clients on different networks successfully received IPs from central DHCP.

▶️ 4: Domain Environment & AD Installation

🎯 Objective

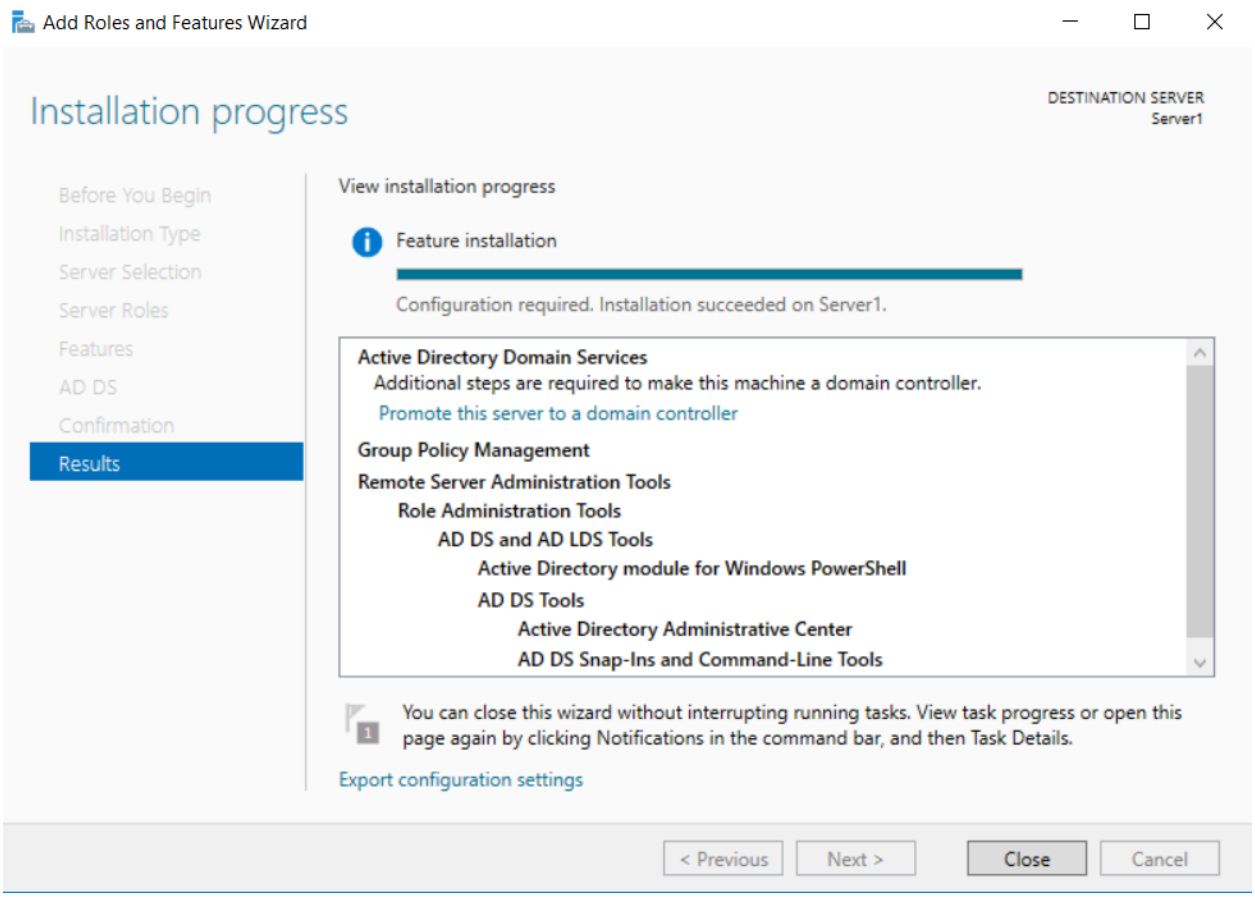
Install and configure **Active Directory Domain Services (AD DS)** to create a domain environment.

📝 Steps

1. Install **AD DS** role from Server Manager.
2. Run **AD DS Configuration Wizard**.
3. Promote server to **Domain Controller**.
4. Create a new forest (`COMPANY.ORG`).
5. Restart the server.
6. Join Windows client machines to the new domain.

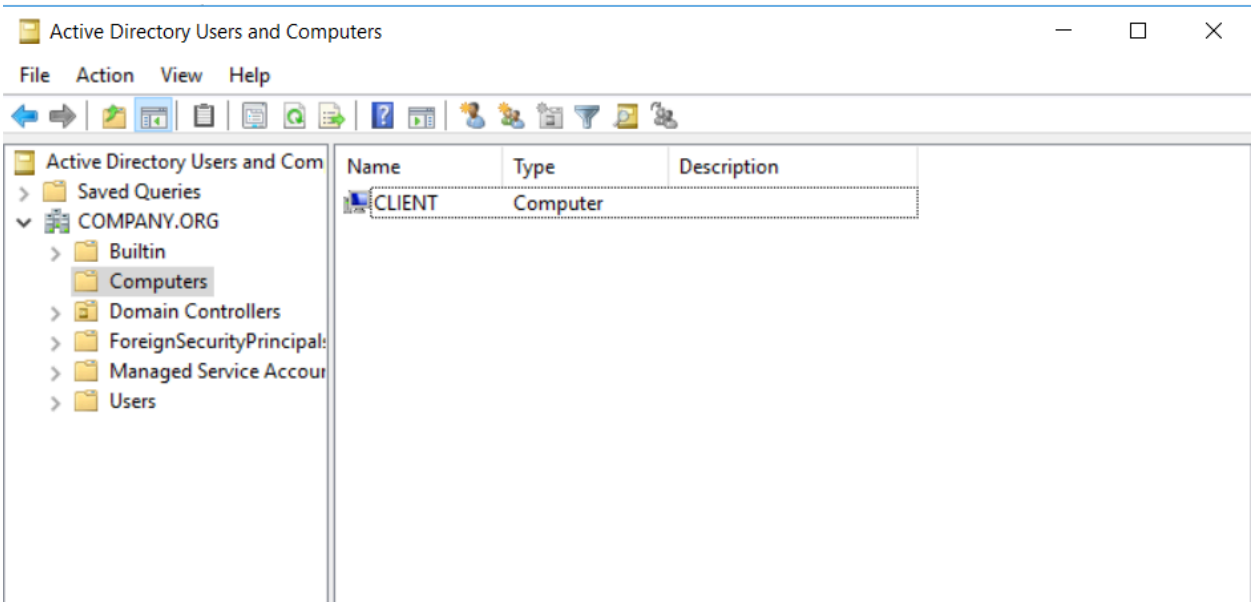
📸 Screenshots

- AD DS Installation



- Domain Controller Promotion

- Client Domain Join



✅ Outcome

- Domain successfully created.
- Clients joined and authenticated via the domain.

▶️ 5: DNS Server

🎯 Objective

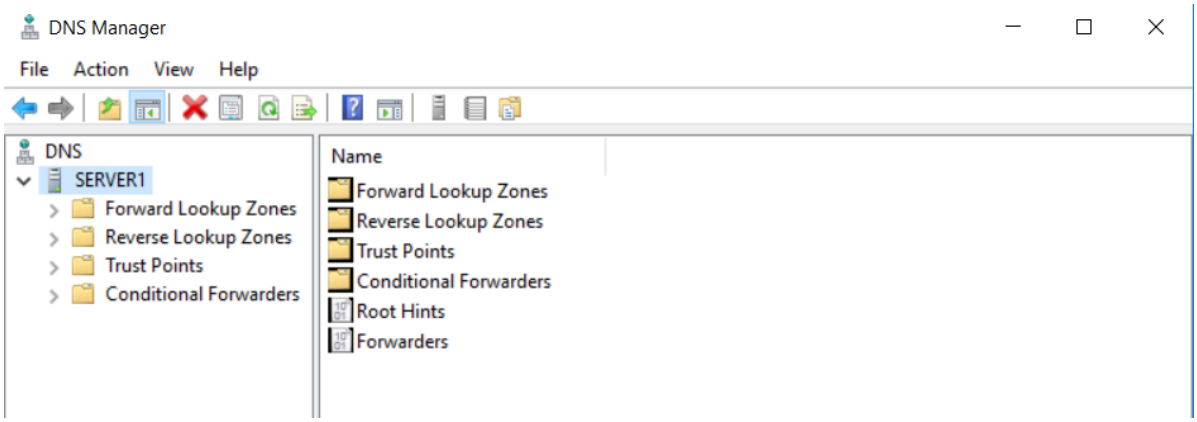
Provide **name resolution** for domain and network clients.

📝 Steps

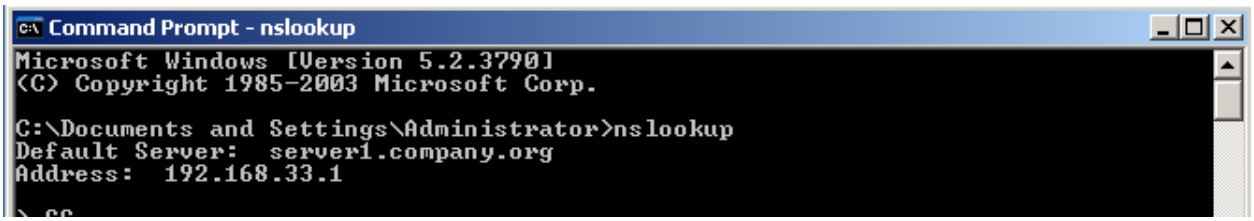
1. Install **DNS Server** role.
2. Open **DNS Manager**.
3. Configure a **Forward Lookup Zone** for COMPANY.ORG.
4. Add **Host (A) Records** for important servers.
5. Configure **Reverse Lookup Zone**.
6. Test with `nslookup` from client.

📸 Screenshots

- Zone Creation



- nslookup Test



✅ Outcome

- DNS resolved names to IPs correctly.

▶️ 6: AD Objects & Domain Administration

🎯 Objective

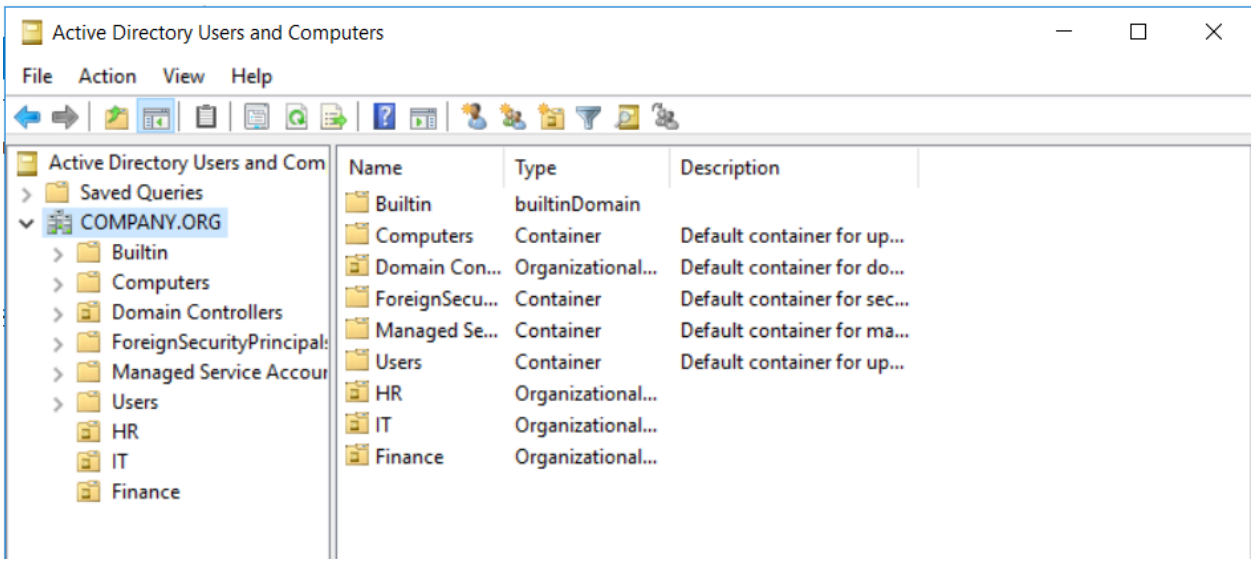
Create and manage **Users, Groups, and OUs** for centralized administration.

📝 Steps

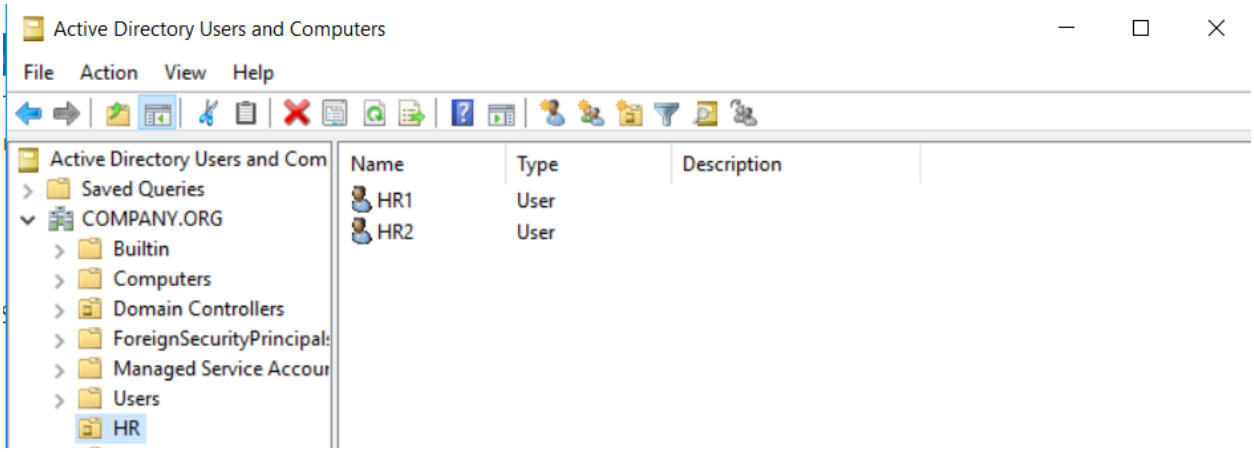
1. Open **Active Directory Users and Computers (ADUC)**.
2. Create **OU Structure** (HR, IT, Finance).
3. Add **Users** under OUs.

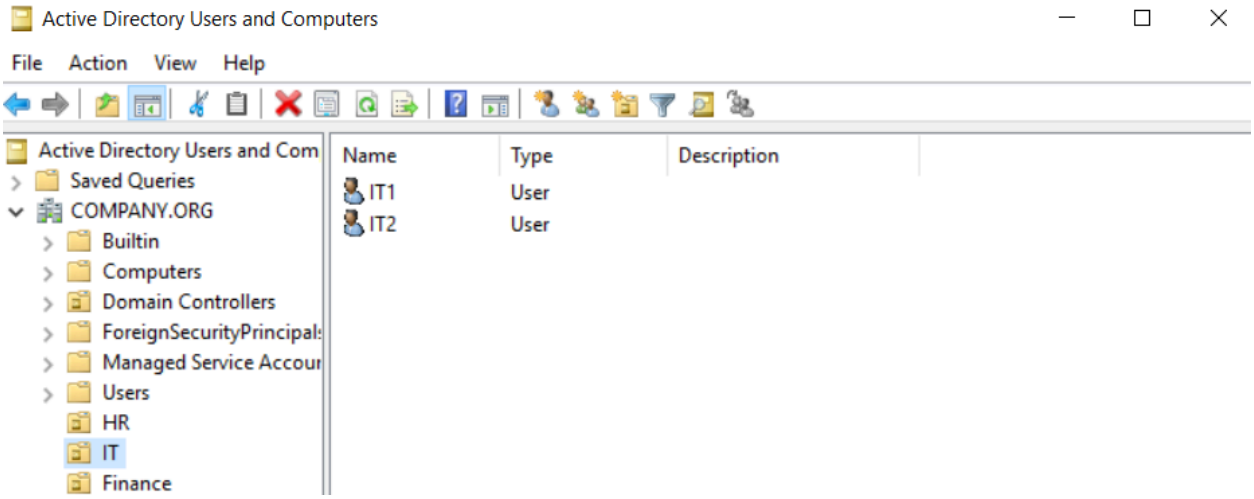
📸 Screenshots

- OU Creation



- User Creation





✅ Outcome

- Domain objects created and managed effectively.

▶️ 7: Group Policy Management (GPM)

🎯 Objective

Apply **Group Policies** for centralized control of users and computers.

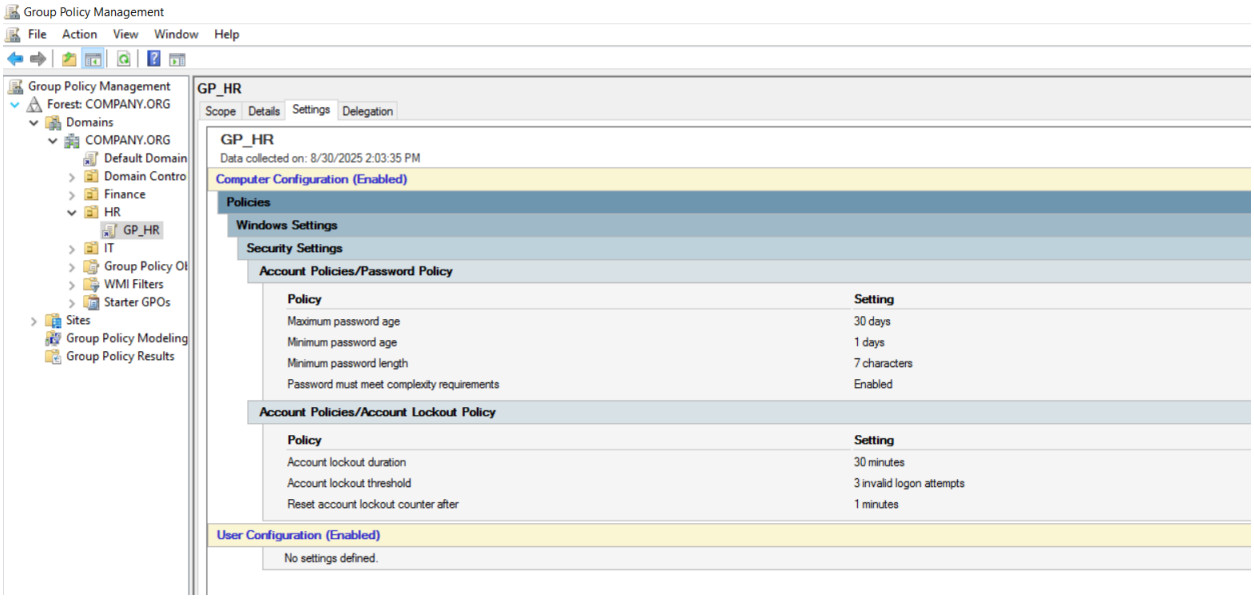
📝 Steps

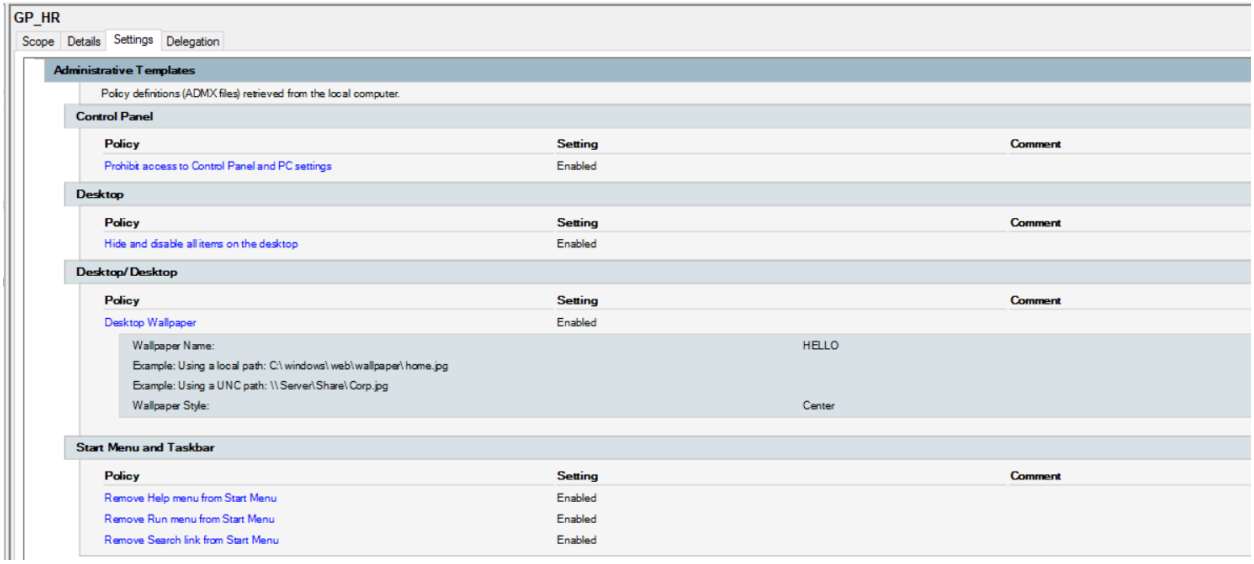
1. Open **Group Policy Management Console (GPMC)**.

2. Create new GPO → name it **GP_HR**
3. Link GPO to **HR OU**.
4. Configure policies:
    - Password Policy
    - Hide *Run from start menu*
    - Remove desktop items
    - Remove *Search from start menu*
    - Disable *Help from start menu*
5. Run `gpupdate /force`.
6. Verify with `gpresult /r`.

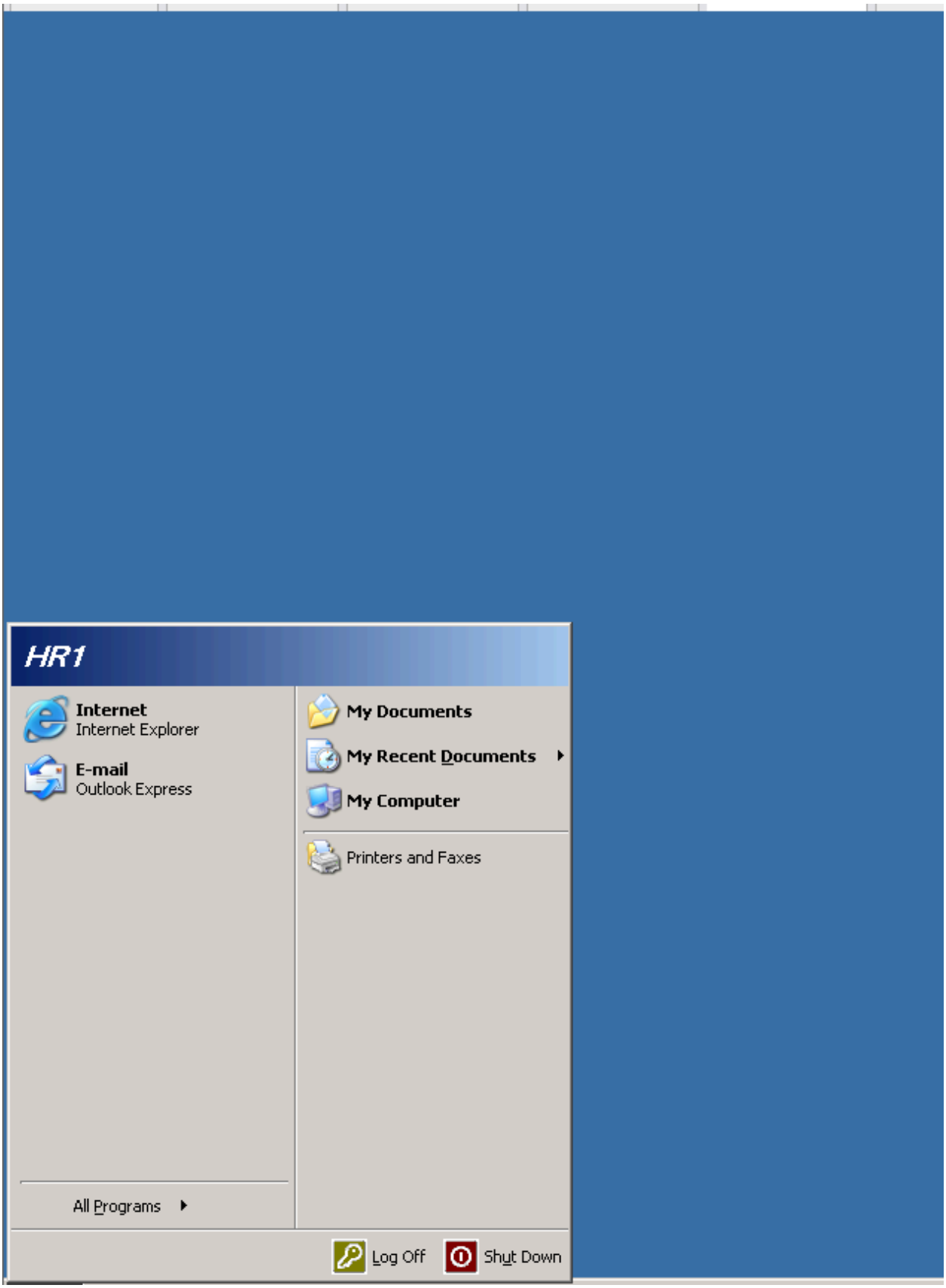
📸 Screenshots

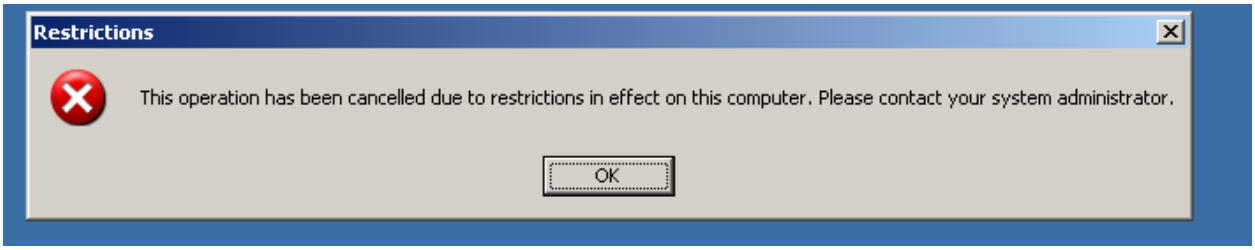
- Linked to OU and its Report





- Client Policy Applied


HR1
Internet
Internet Explorer
E-mail
Outlook Express
My Documents
My Recent Documents
My Computer
Printers and Faxes
All Programs
Log Off
Shut Down



✅ Outcome

- Policies successfully applied to target users and computers.

▶️ 8: Virtual Private Network (VPN)

🎯 Objective

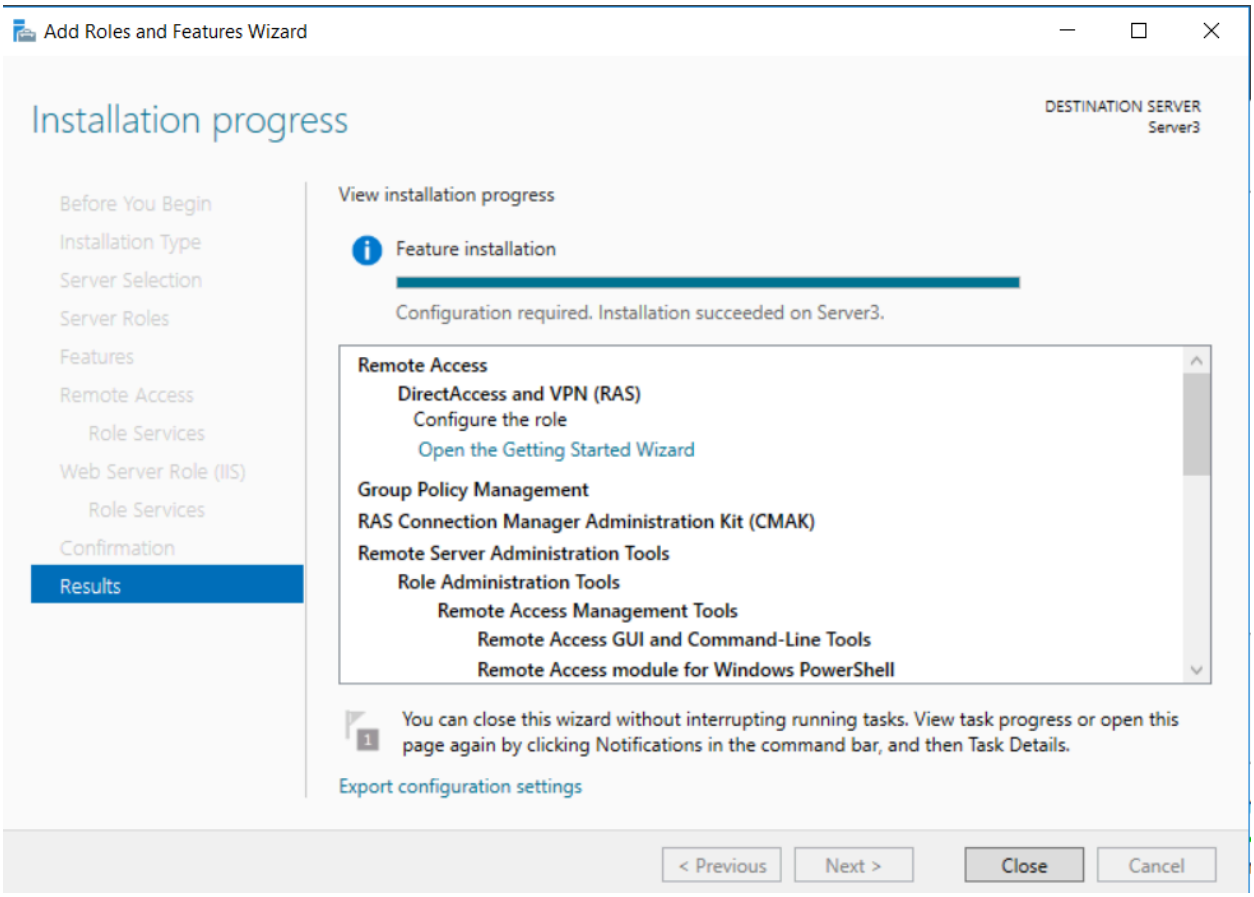
Set up a **VPN** for secure remote access.

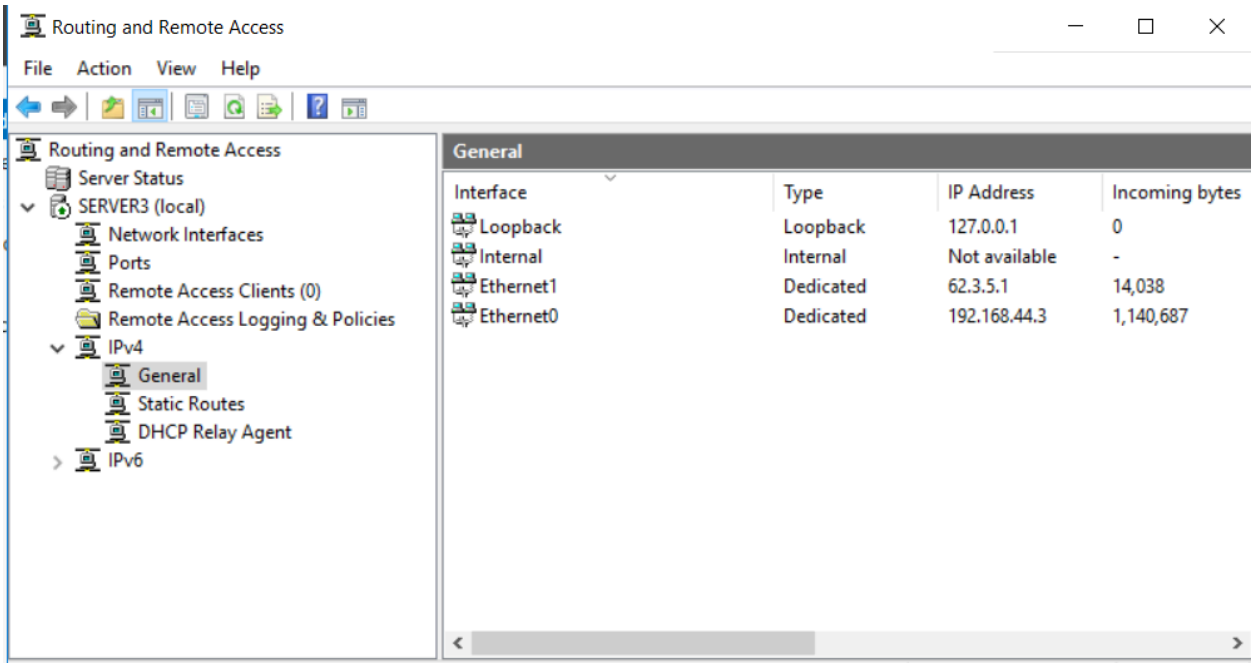
📝 Steps

1. Install **Remote Access → VPN** role.
2. Configure **RRAS for VPN Access**.
3. Set authentication method (username/password).
4. Create a VPN connection on the client.
5. Connect and test access to internal resources.

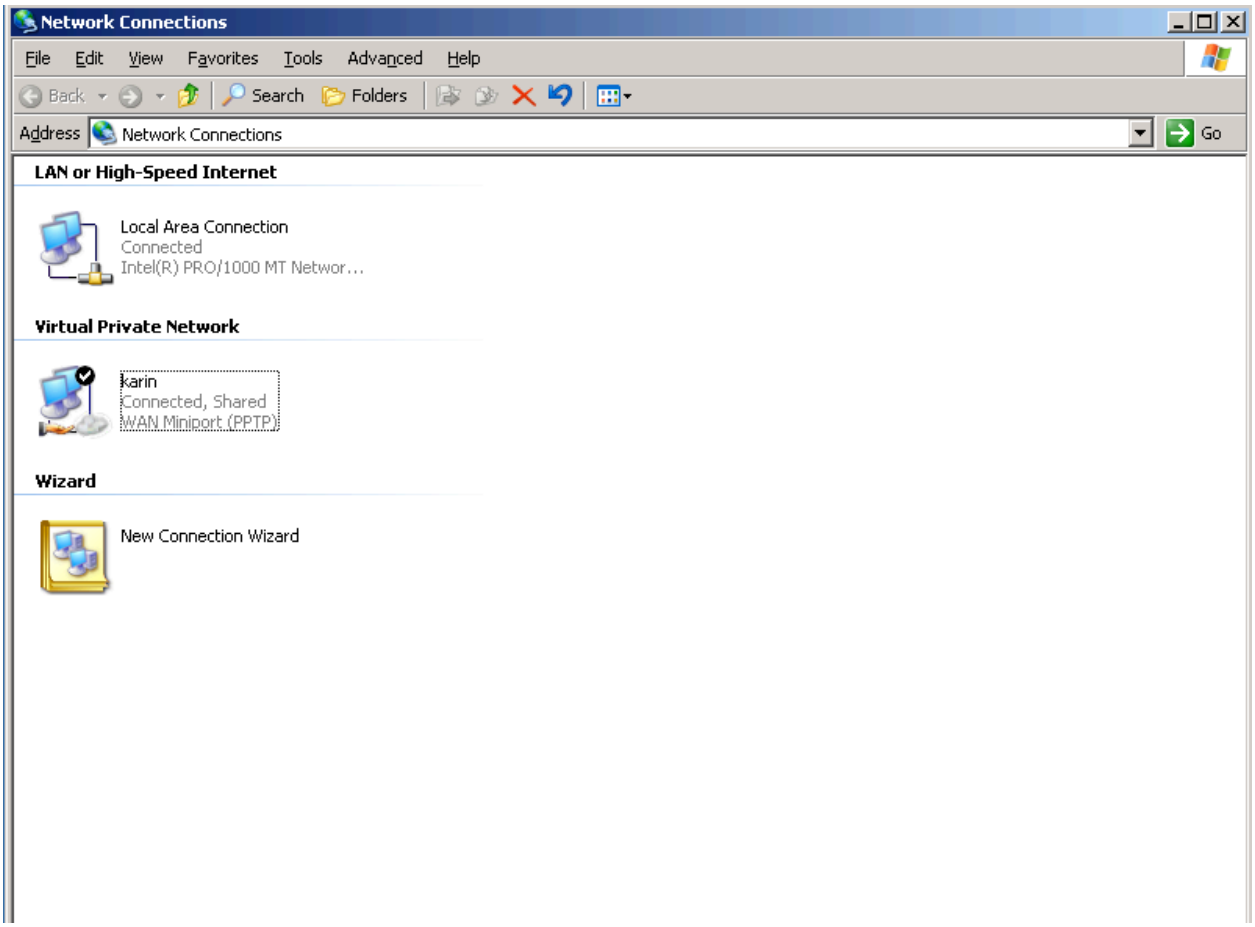
📸 Screenshots

- RRAS VPN Setup





- Client VPN Connection



✅ Outcome

- VPN successfully established and client accessed domain resources.

▶️ 9: Network Policy Service (NPS / RADIUS)

🎯 Objective

Configure **NPS (RADIUS)** for centralized authentication of VPN and network devices.

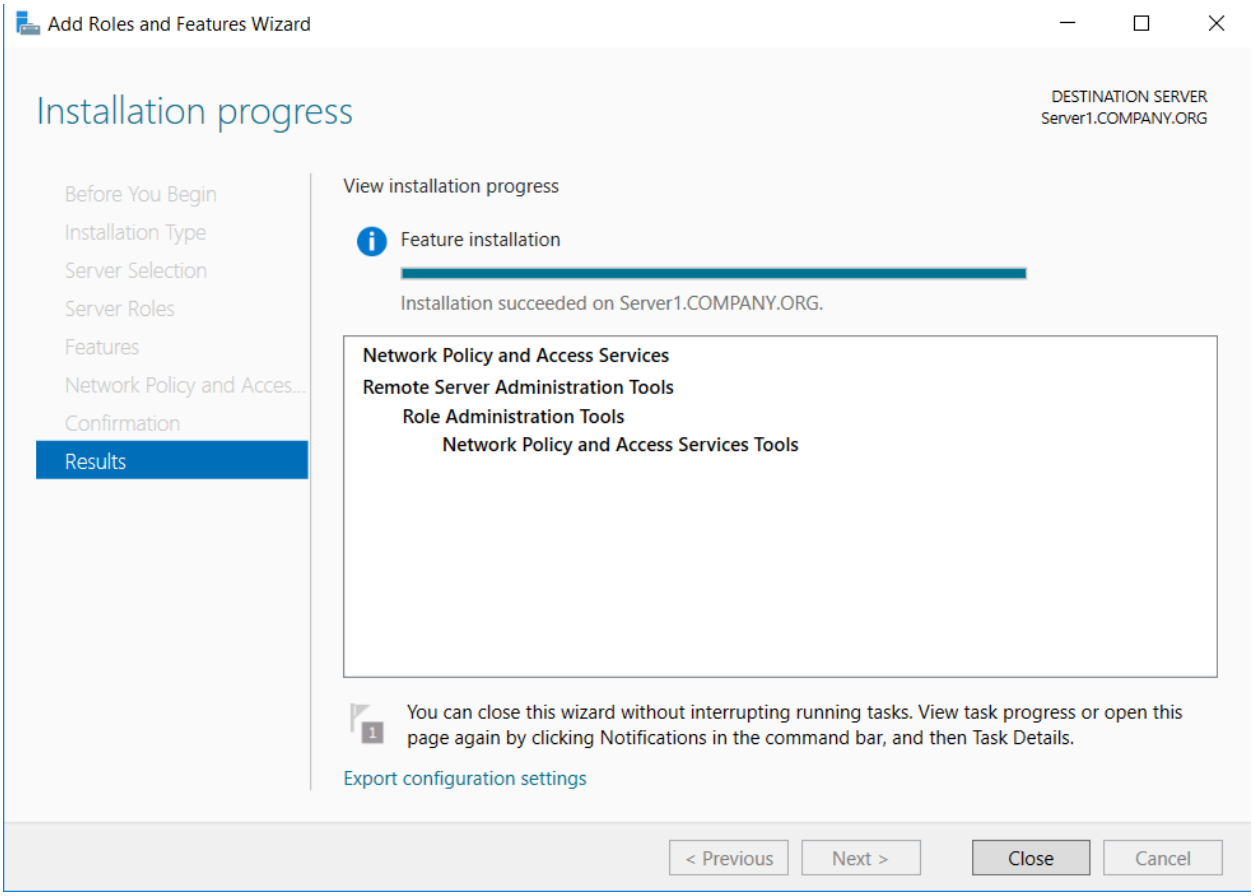
📝 Steps

1. Install **Network Policy and Access Services** role.
2. Open **NPS Console**.
3. Configure **RADIUS Clients** (e.g., VPN server).

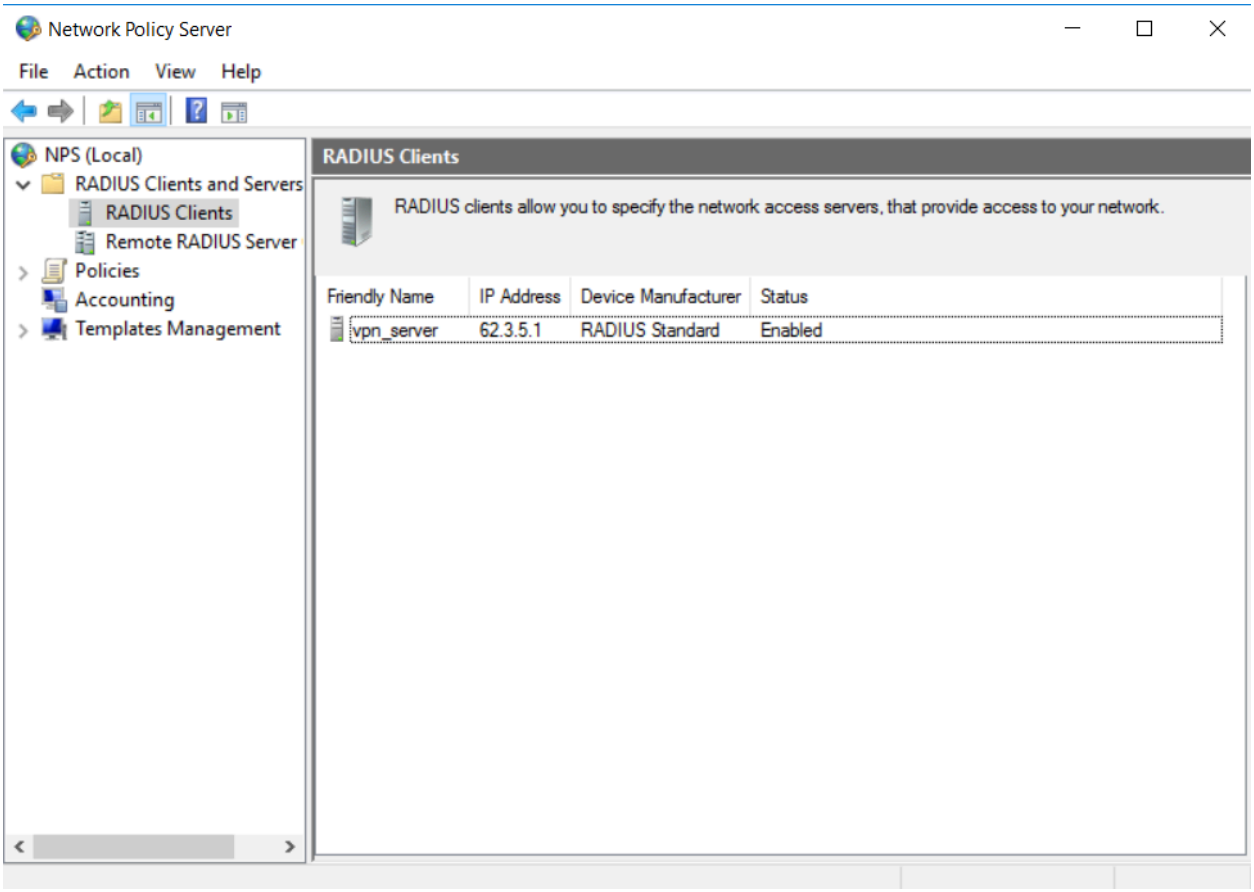
4. Create **Network Policies** for authentication.
5. Test authentication via client.

📸 Screenshots

- NPS Installation



- RADIUS Client Configuration



✅ Outcome

- NPS successfully authenticated users via RADIUS.

🔚 Conclusion

This workshop provided a **hands-on, end-to-end lab** covering the most essential Windows Server administration roles:

- Automated IP management with **DHCP**.
- Inter-network communication through **RRAS Routing** and **DHCP Relay**.
- Centralized management using **Active Directory (AD DS)**.
- Reliable name resolution with **DNS**.
- Secure, policy-driven administration via **Group Policy Objects (GPOs)**.
- Remote connectivity through **VPN**.
- Centralized authentication and authorization using **NPS (RADIUS)**.

✅ By completing these steps, we built a fully functional **enterprise-like Windows Server environment**, with proper domain services, secure authentication, and centralized administration.