WINDOWS SERVER ENTERPRISE INFRASTRUCTURE

Cloud Architecture 2025 / 2026 Track

Simulation of a Multi-Site Enterprise Network with Advanced Services.

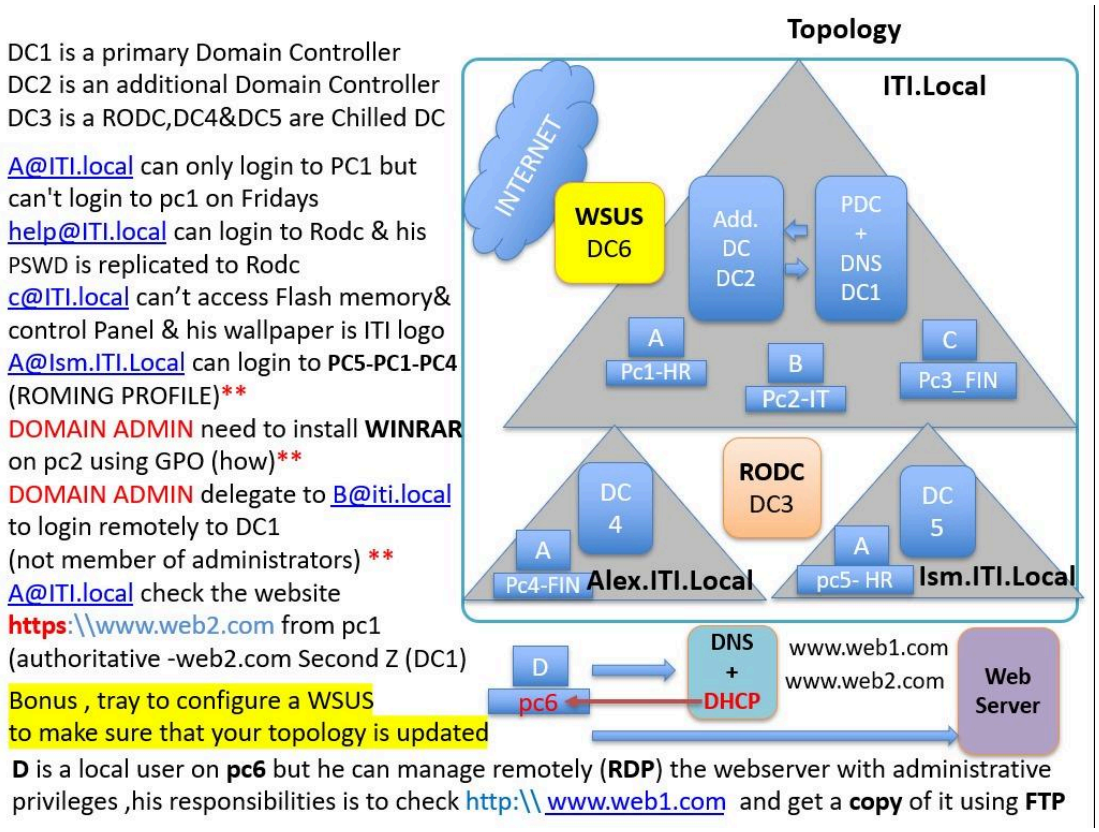
Team3:-

1. Khaled Walid Elhannat
2. Motasem Abotaleb
3. Adham Ayad
4. Mohamed Elsayed
5. Noran Mohamed

Supervised By:

Eng. Mohamed AbouSehly

Table Of Contents



1. Project Overview

1.1. Executive Summary

This project involves the design, deployment, and administration of a scalable Enterprise Network Infrastructure for a multi-site organization ("ITI Corporation"). The project simulates a real-world environment, focusing on High Availability (HA), Security, and Centralized Management using Microsoft Windows Server technologies.

1.2. Objectives

The primary goals of this project are:

- To build a Multi-Domain Active Directory Forest (Root & Child Domains).
- To implement a "**Separation of Services**" architecture to enhance performance and security.
- To deploy a secure Web Hosting environment using IIS and SSL/TLS.
- To manage IP addressing and Name Resolution dynamically for network clients.
- To enforce security policies using Group Policy Objects (GPO).

---

2. Infrastructure Architecture

The network topology is designed to mimic a production environment, divided into logical segments:

A. Identity & Access Management (The Directory Tier)

- **Root Domain Controller (PDC):** Manages the forest root (iti.local).
- **Additional Domain Controller (ADC):** Provides fault tolerance.
- **Child Domain Controllers:** Dedicated controllers for regional branches (Alexandria & Ismailia sites).

B. Network Services Infrastructure (The Network Tier)

- **Dedicated DNS & DHCP Server:** A standalone server configured to handle all client IP addressing and name resolution requests, offloading traffic from the Domain Controllers.
- **Configuration:** Custom scopes defined to avoid conflicts with the physical network environment (Bridged Mode).

C. Web Application Infrastructure (The Web Tier)

- **Dedicated Web Server (IIS):** A standalone server hosting the corporate website (www.mycompany.com).
- **Security:** Secured via **HTTPS** using Self-Signed Certificates to ensure encrypted communication.
- **Content:** Deployed using a professional HTML5/Bootstrap template to simulate a production-grade website.

---

3. Technical Environment

- **Virtualization:** VMware Workstation (Bridged Networking Mode).
- **Server OS:** Windows Server 2019 / 2022.
- **Client OS:** Windows 10 Enterprise.
- **Protocols:** TCP/IP, DNS, DHCP, HTTP/HTTPS, FTP, ICMP.

---

4. Implementation & Configuration

4.1. Phase 1: Active Directory Forest Setup

In this foundational phase, we designed and deployed a multi-tier Active Directory Forest. This involved configuring the Root Domain Controller (iti.local), establishing Child Domains for regional branches, and implementing high-availability solutions using Additional Domain Controllers (ADC) and Read-Only Domain Controllers (RODC).

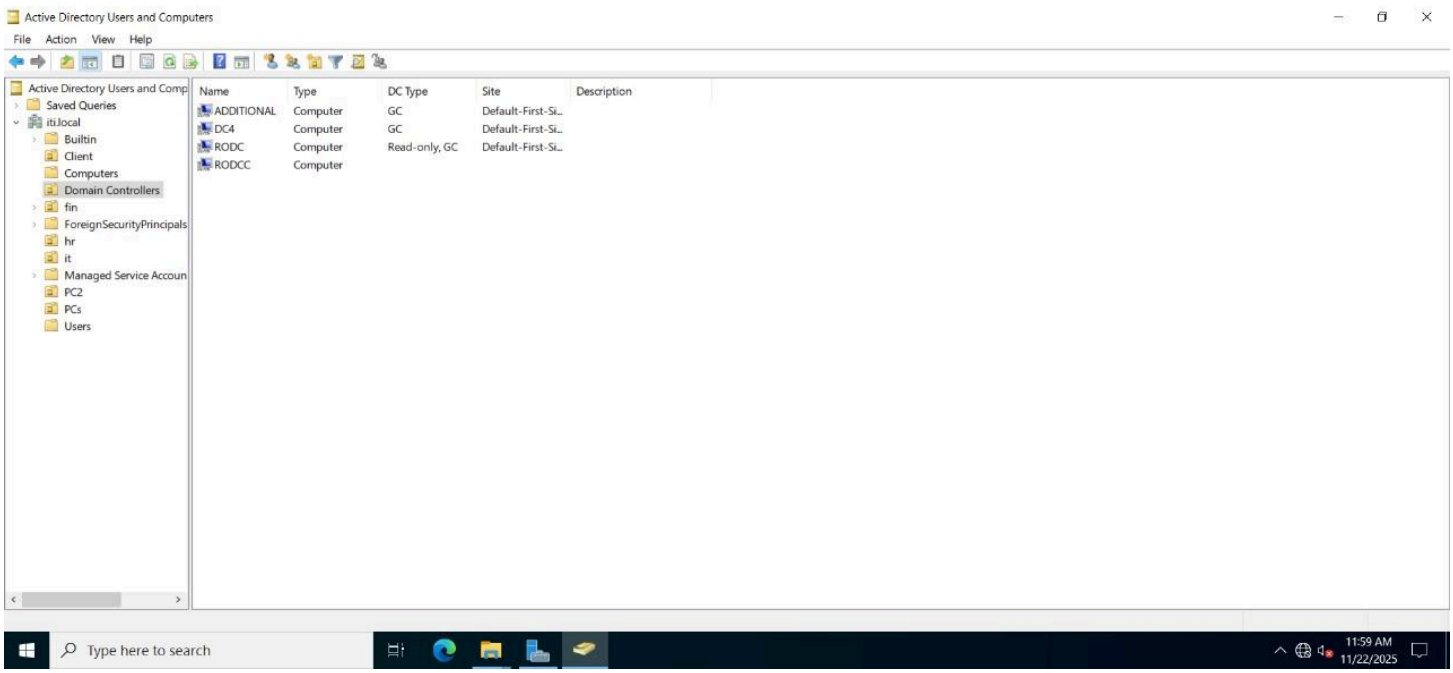


Figure 1: Domain Controller Roles: The Active Directory console displaying the deployed infrastructure, including an Additional Domain Controller (ADC) for fault tolerance and a Read-Only Domain Controller (RODC) for secure deployment in branch offices.

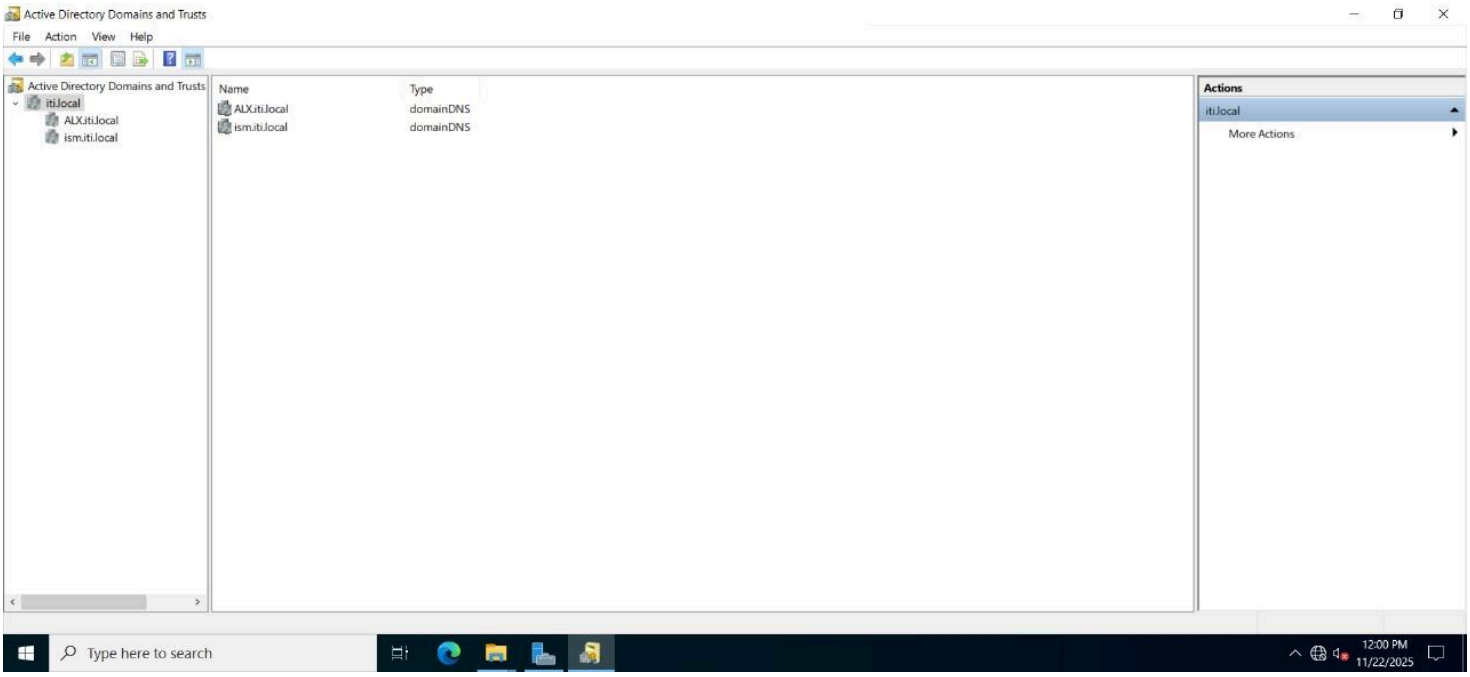


Figure 2: Forest & Trust Topology: The "Active Directory Domains and Trusts" console verifying the parent-child trust relationships established between the Root Domain (iti.local) and the regional Child Domains (ALX & ism).

4.2. Phase 2: Identity Management & Advanced Policies

In this phase, we structured the Active Directory environment to mirror the organization's hierarchy. We implemented strict security controls, user mobility features, and automated software management using Group Policy Objects (GPO).

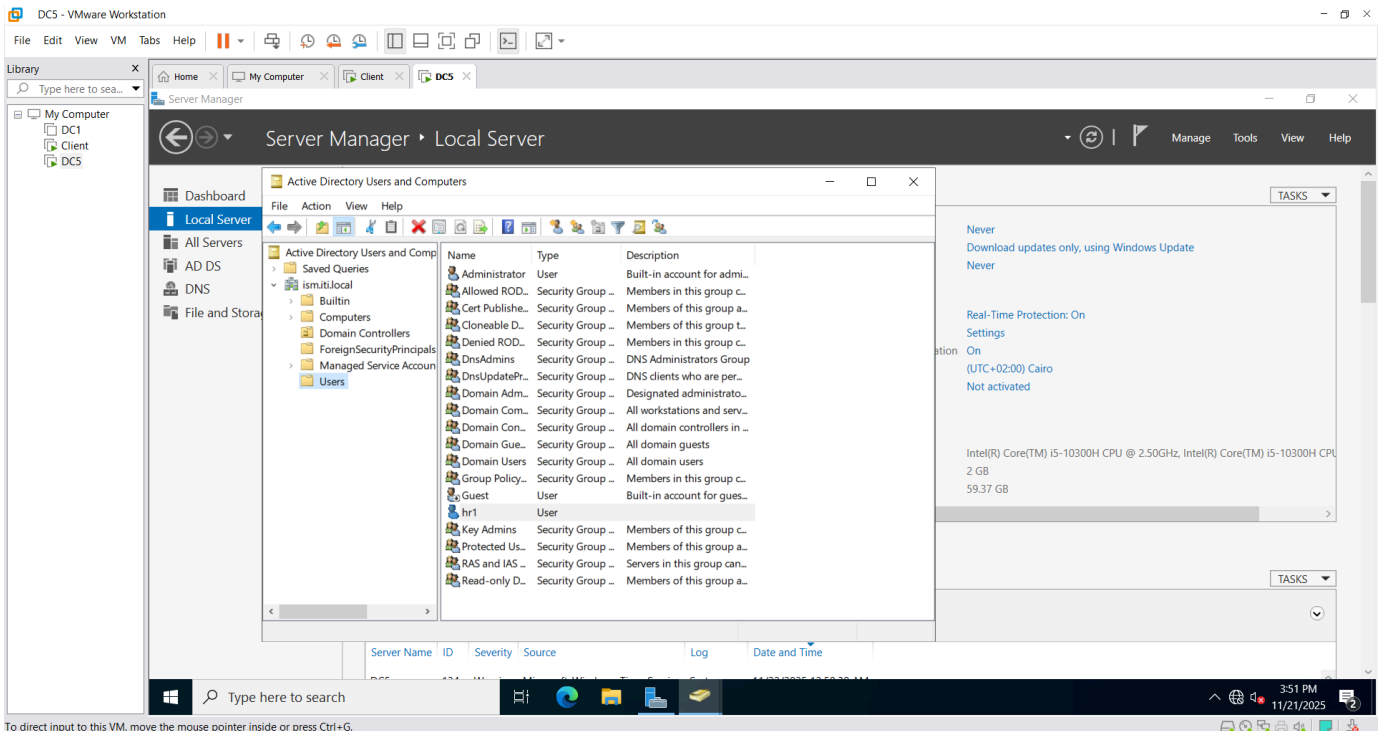


Figure 3: Organizational Units (OUs) Structure: Organizing network objects into logical units (HR, IT, Finance) to facilitate granular delegation of control and policy application.

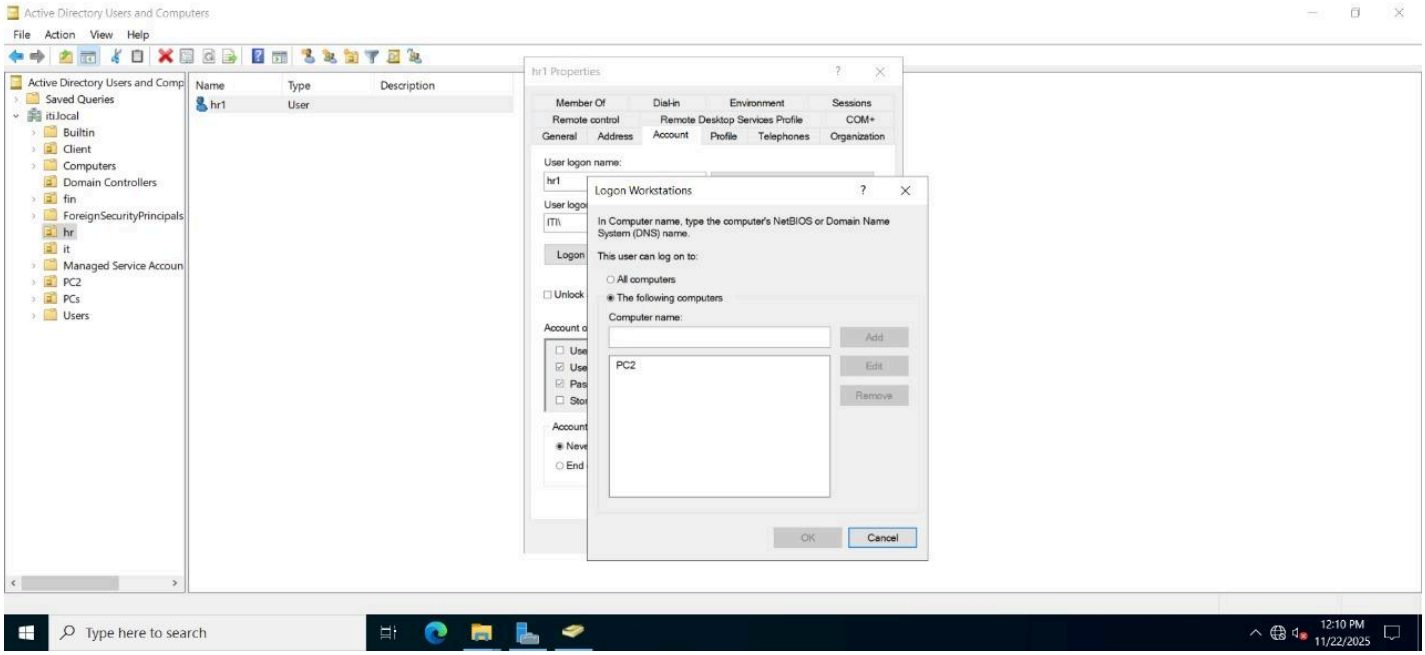


Figure 4: Access Control & Hardening: Implementing "Logon Workstation" restrictions to ensure that sensitive accounts (e.g., HR Staff) can only access the network from authorized physical machines (PC2).

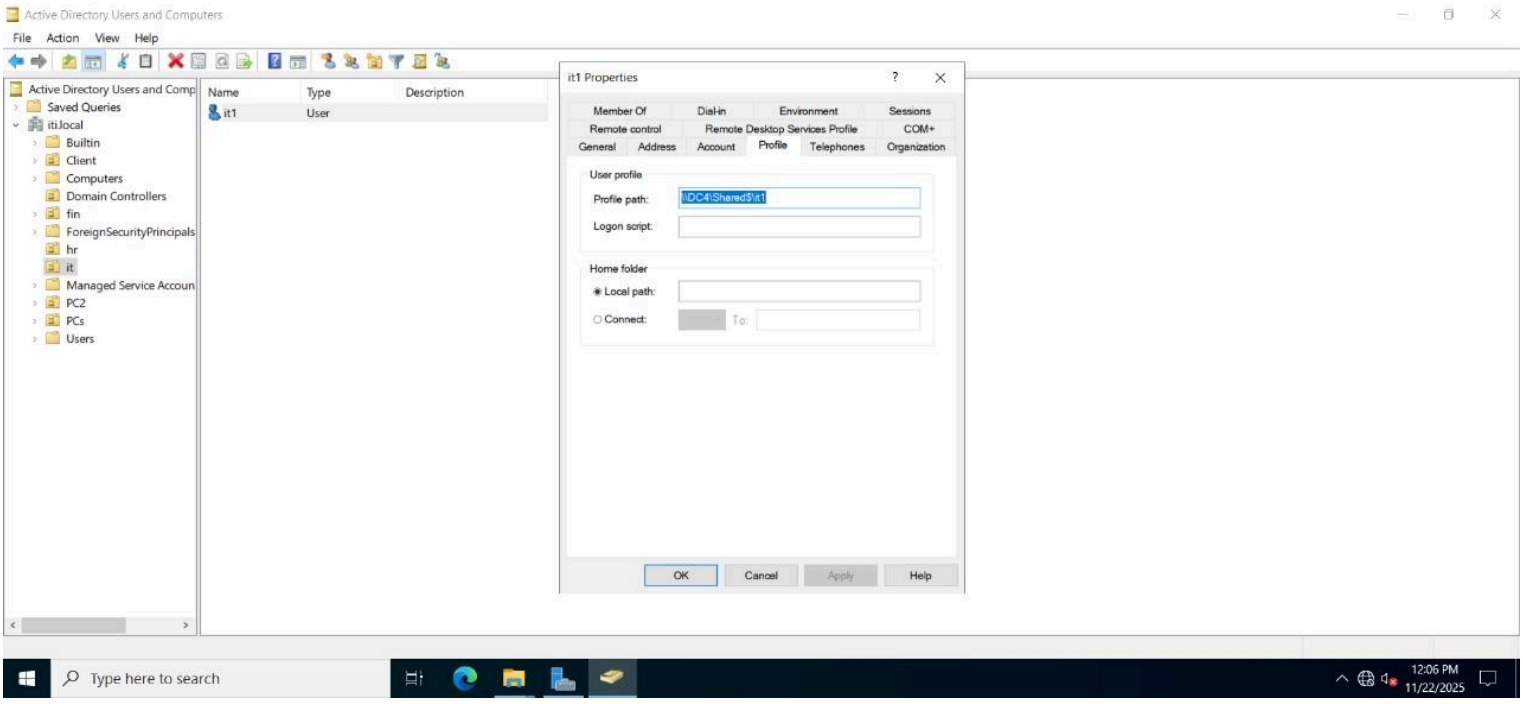


Figure 5: Roaming Profiles Implementation: Configuring centralized profiles for IT administrators (\\DC4\Shared$), allowing their personal settings and data to follow them across any workstation in the domain.

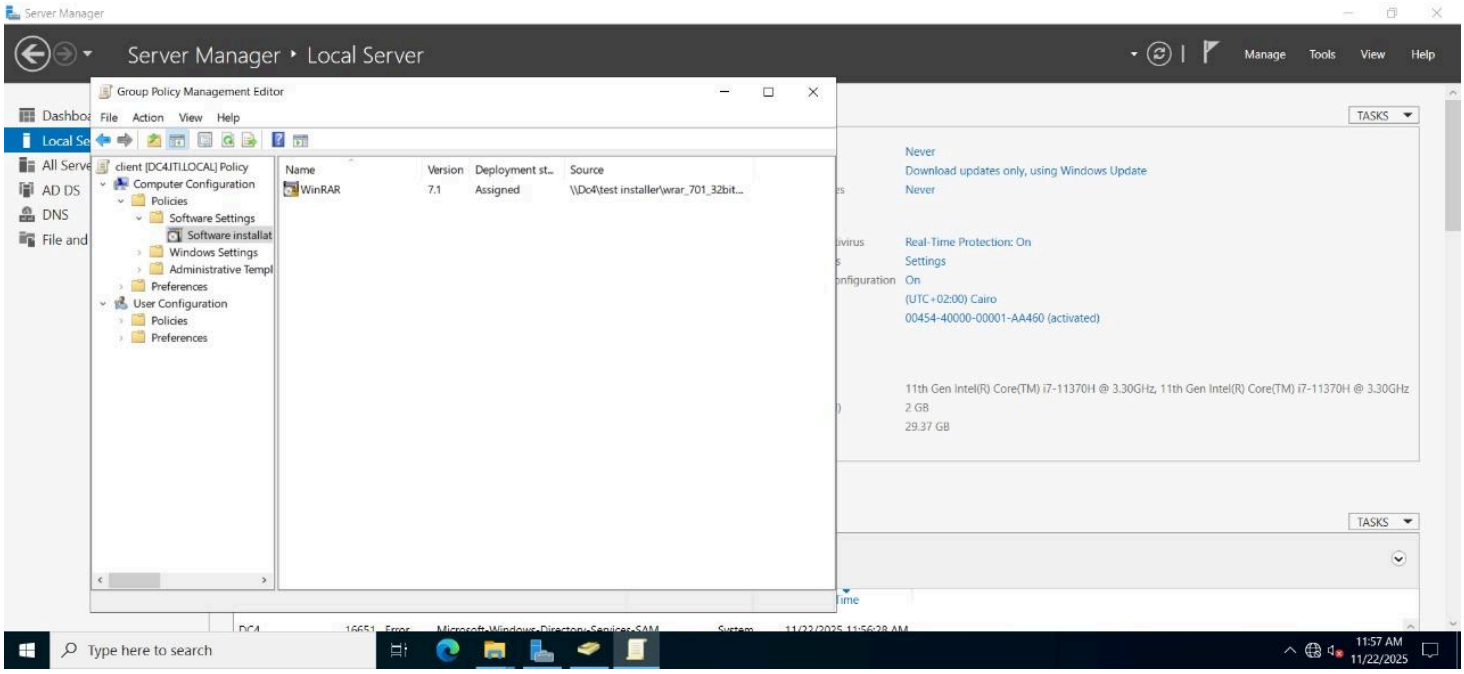


Figure 6: Automated Software Deployment: Utilizing Group Policy to automatically deploy essential software packages (e.g., WinRAR) to client computers at startup, reducing manual administration overhead.

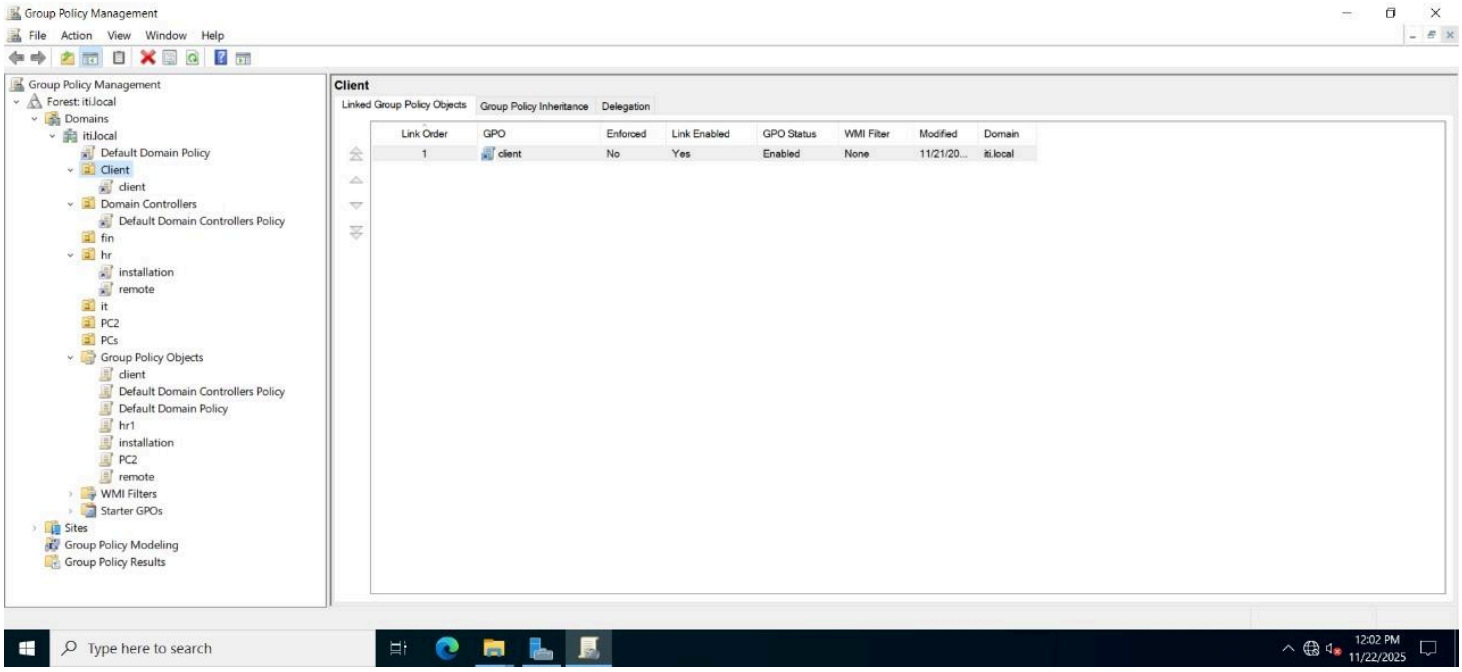


Figure 7: Group Policy Management: Linking the created policies (e.g., Client Setup) to the appropriate domains and OUs to ensure they are enforced on the target users.

4.3 Phase 3: Network Infrastructure (DNS & DHCP)

To ensure network isolation and stability, we configured a dedicated server for IP addressing and name resolution.

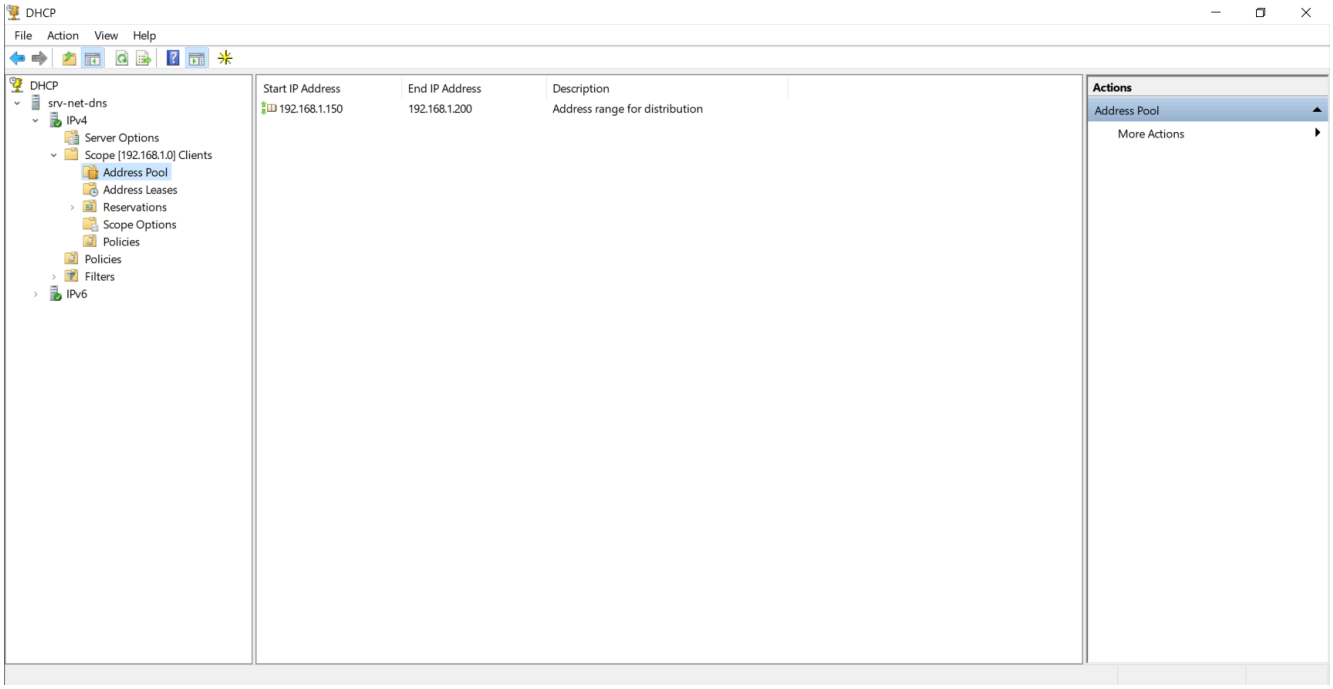


Figure 8: DHCP Configuration: Creating a custom Scope (192.168.1.150-200) to isolate client traffic from the physical network.

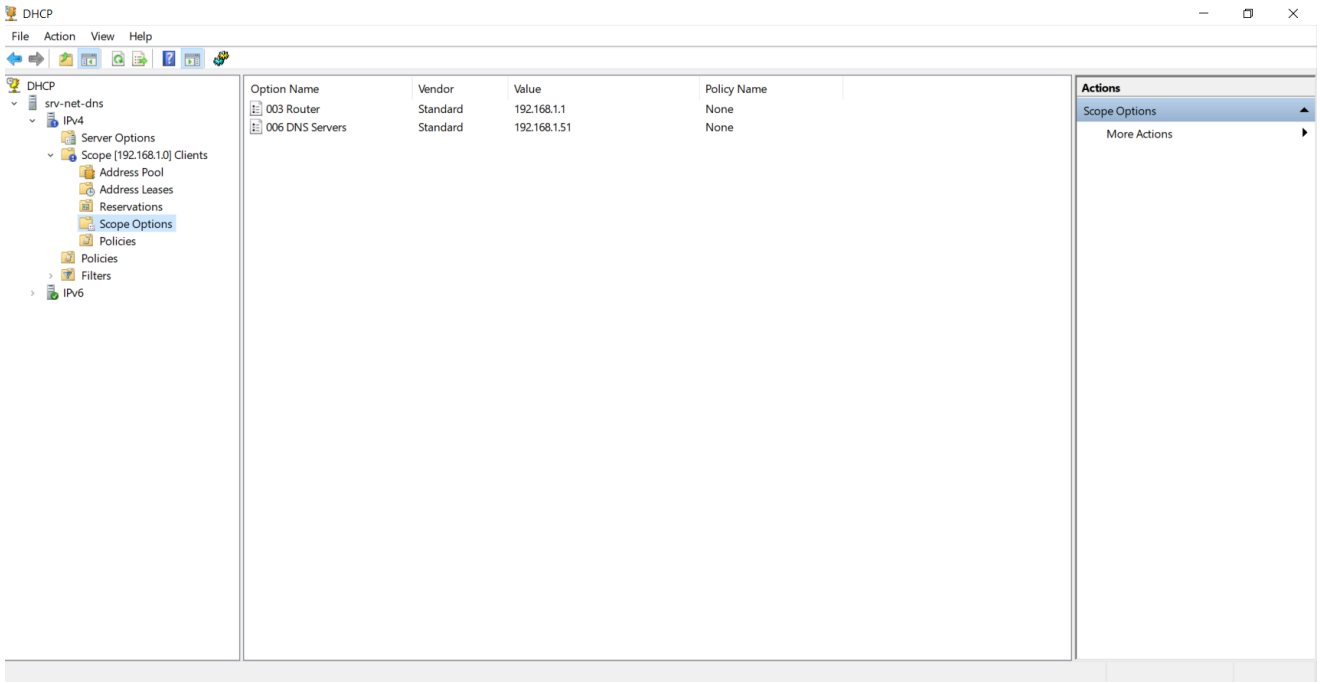


Figure 9: DHCP Options: Configuring Option 006 to point clients to our dedicated DNS Server, ensuring proper name resolution.

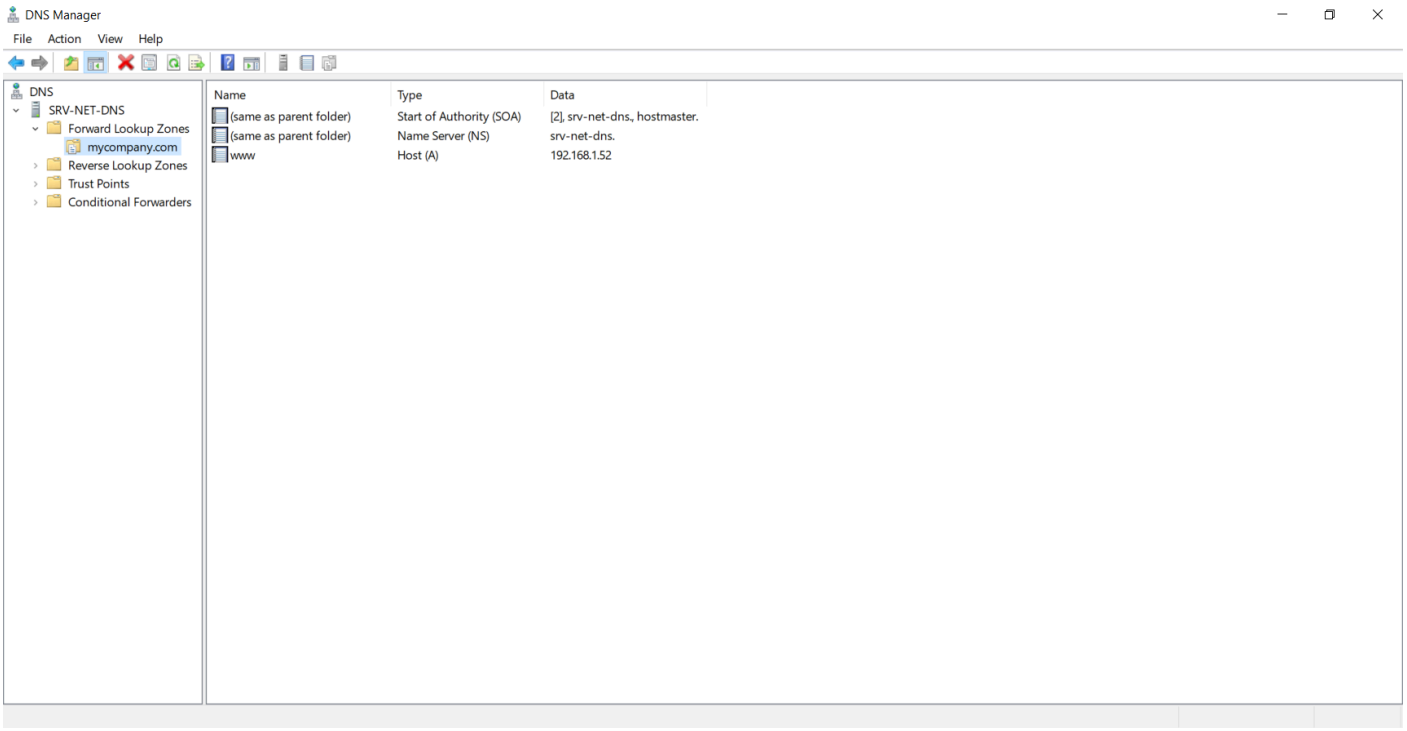


Figure 10: DNS Manager: Creating Forward Lookup Zones for the web application (mycompany.com) pointing to the Web Server IP.

4.4 Phase 4: Web Server & Security (IIS)

We deployed a dedicated IIS Web Server to host the corporate portal, securing it with SSL certificates.

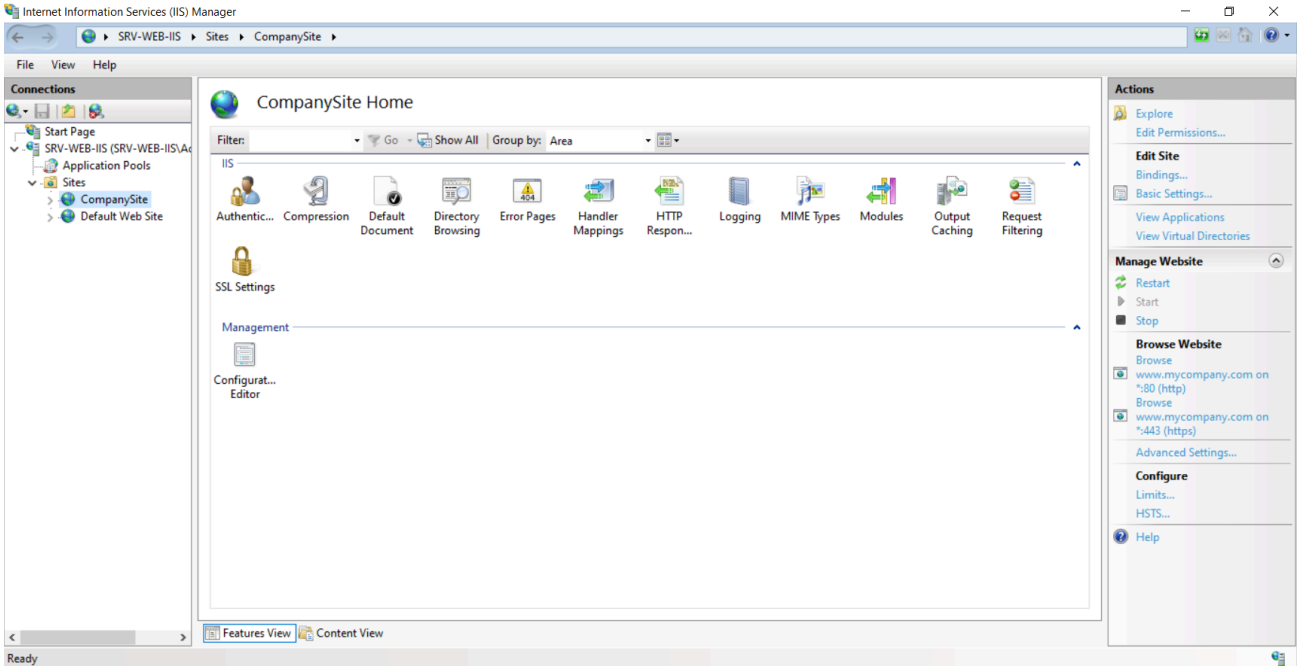


Figure 11: IIS Manager: Hosting the corporate website (www.mycompany.com) and mapping it to the local physical path.

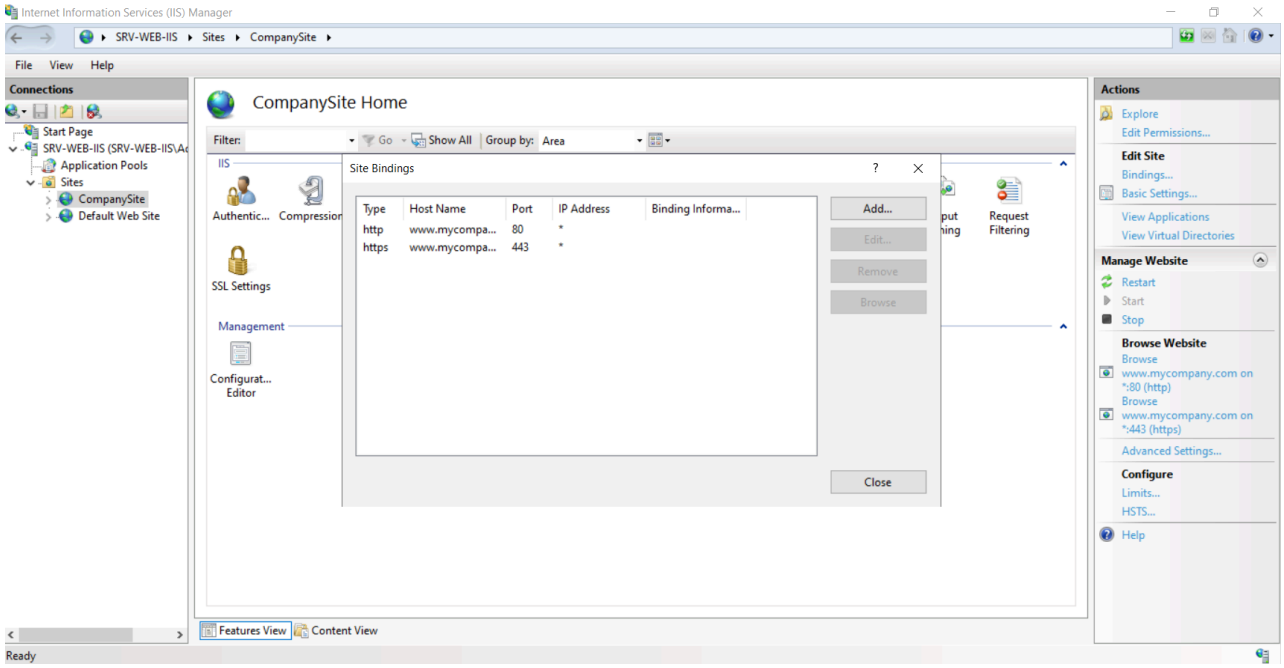
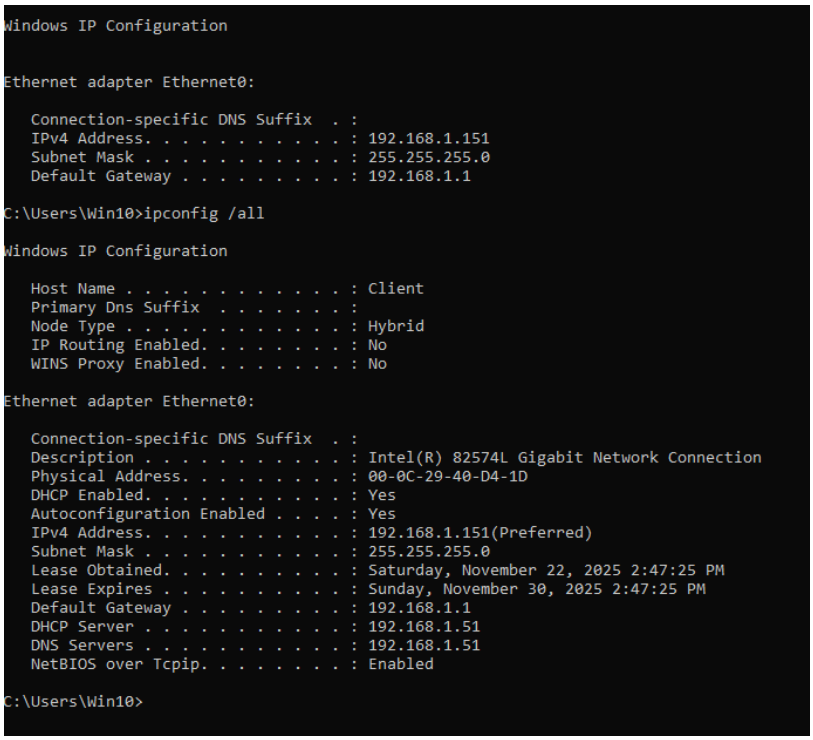


Figure 12: Security Bindings: Configuring HTTPS (Port 443) using a Self-Signed Certificate to encrypt web traffic.

4.5 Client-Side Verification (Final Testing)

Final validation was performed from a Windows 10 Client machine to ensure all services are reachable and policies are applied.



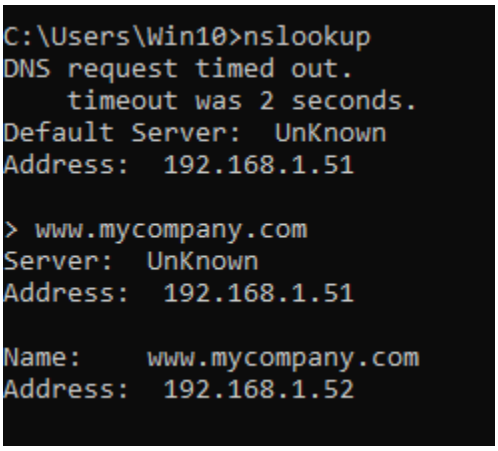


Figure 13 & 14: Network & DNS Verification: The Command Line Interface confirms that the client received a dynamic IP from our dedicated DHCP server, and the nslookup command successfully resolves the hostname www.mycompany.com to the Web Server's IP.

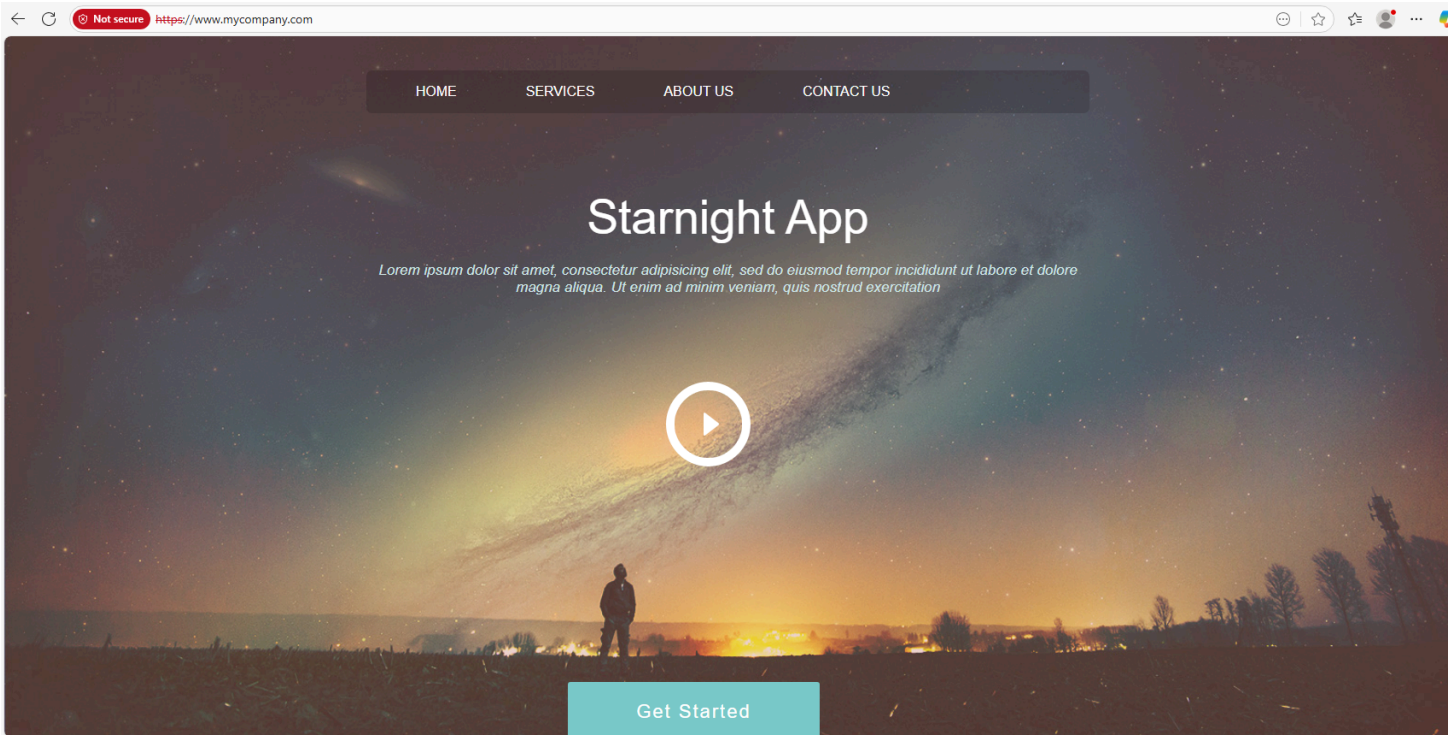


Figure 15: End-User Experience: The client browser successfully accessing the hosted web application via the internal domain name over a secure HTTPS connection.

---

5. Challenges & Conclusion

During the implementation of this project, we encountered several technical challenges that were successfully resolved:

1. **IP Conflict Management:**
    - *Challenge*: Integrating the virtual lab with the physical network caused IP conflicts with the local gateway.
    - *Solution*: We designed a custom DHCP Scope (.150-.200) and manually configured the DNS pointers to ensure total isolation while maintaining connectivity.
2. **Service Blocking (Firewalls):**
    - *Challenge*: Initial connectivity tests (Ping/DNS) failed between servers.
    - *Solution*: We diagnosed that Windows Defender Firewall was blocking ICMP and Port 53 packets. We configured the necessary Inbound/Outbound rules to allow traffic between the separated zones.
3. **Web Server Permissions:**
    - *Challenge*: The Web Server initially returned "403 Forbidden" errors.
    - *Solution*: We reconfigured the IIS "Default Document" settings and adjusted the physical path permissions to correctly serve the HTML template.

---

6. Conclusion

This project successfully demonstrated the deployment of a **scalable and secure Enterprise Network**. By implementing the **"Separation of Services"** architecture and **Advanced Active Directory features**, we achieved:

- **Better Performance:** Offloading DNS/DHCP roles from the Domain Controllers.
- **Enhanced Security:** Isolating the Web Server, implementing SSL, and applying strict Logon Policies.
- **User Mobility & Automation:** Successfully deploying Roaming Profiles and automating software installation via GPO.

The final testing confirmed that all clients could automatically join the network, resolve hostnames, receive policies, and access hosted applications seamlessly.

Special Thanks

A group photo with our mentor, ***Eng. Mohamed Abousehly****.*
Thank you for your guidance, support, and for pushing us to achieve our best in this project.