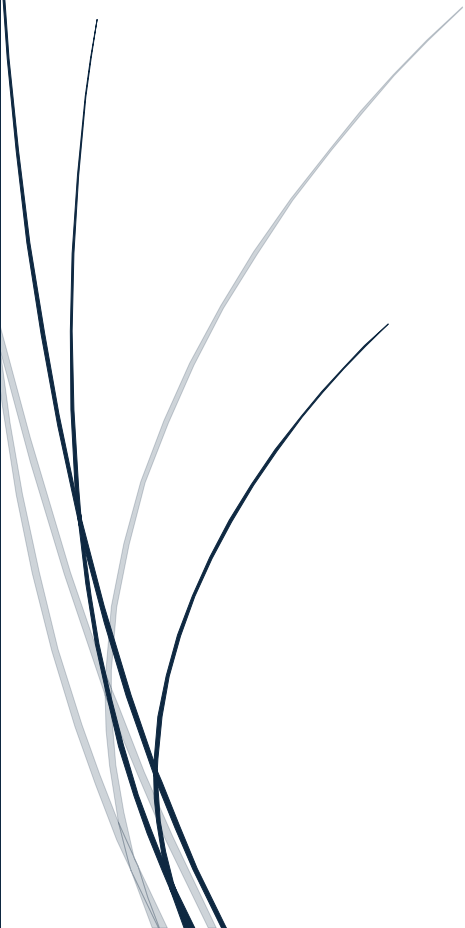




Date: TBD

Network Operating Systems and Services

Assessment 2 Part 1



Lecturer: Md. Sadeque Imam Shaikh
STUDENT: ANDREI-STEFANITA STOICA (2413927)

Table of Contents

1. Introduction	2
2. Screenshots.....	2
3. Conclusion	9

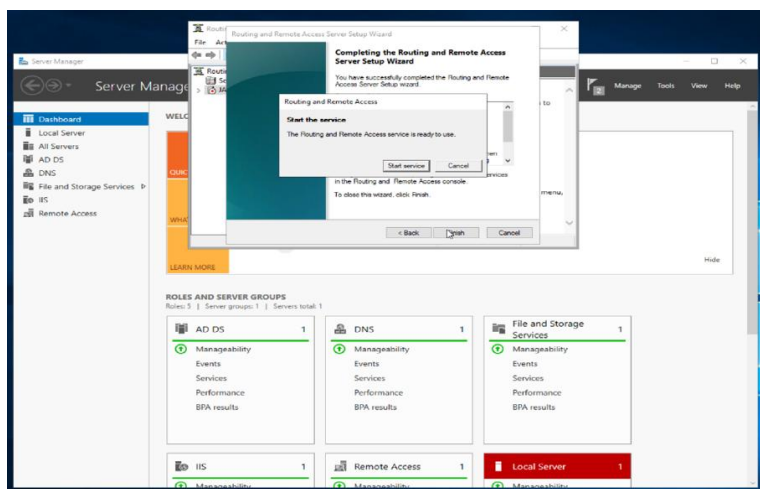
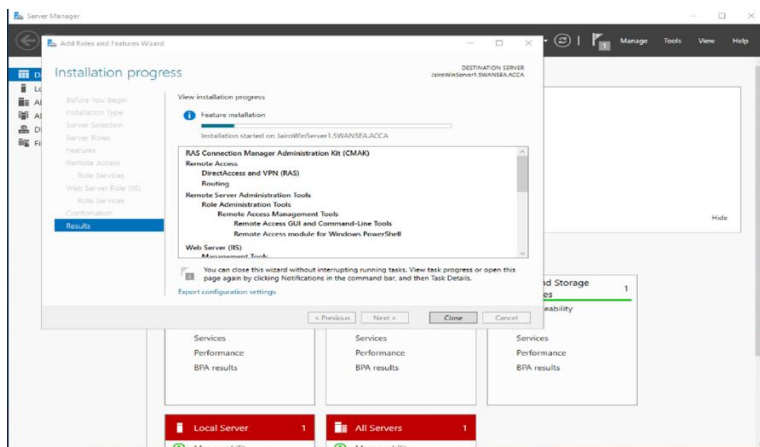
1. Introduction

The first part of this assessment revolves around further developing our skills in managing and maintaining resources applying appropriate network policies, routing and packet filtering within core TCP/IP services, file sharing, issuing certificates, drafting security practices, critical failover/redundancy practices and so on. It is imperative to complete all the tasks ahead according to the topology and instructions given.

2. Screenshots

2.1 Routing

I installed the Routing and Remote Access Service (RRAS) on the Swansea server and modified the Windows Defender Firewall rules to allow ICMP traffic. This ensured that network connectivity could be tested and verified between devices.



I configured persistent IP forwarding and routing on the London network to allow traffic to pass between different subnets.

2.2 Domain Server

I created an Active Directory forest on the Swansea Domain Controller.

I created all appropriate DNS A records for all servers located on both the Swansea and London networks to ensure proper name resolution.

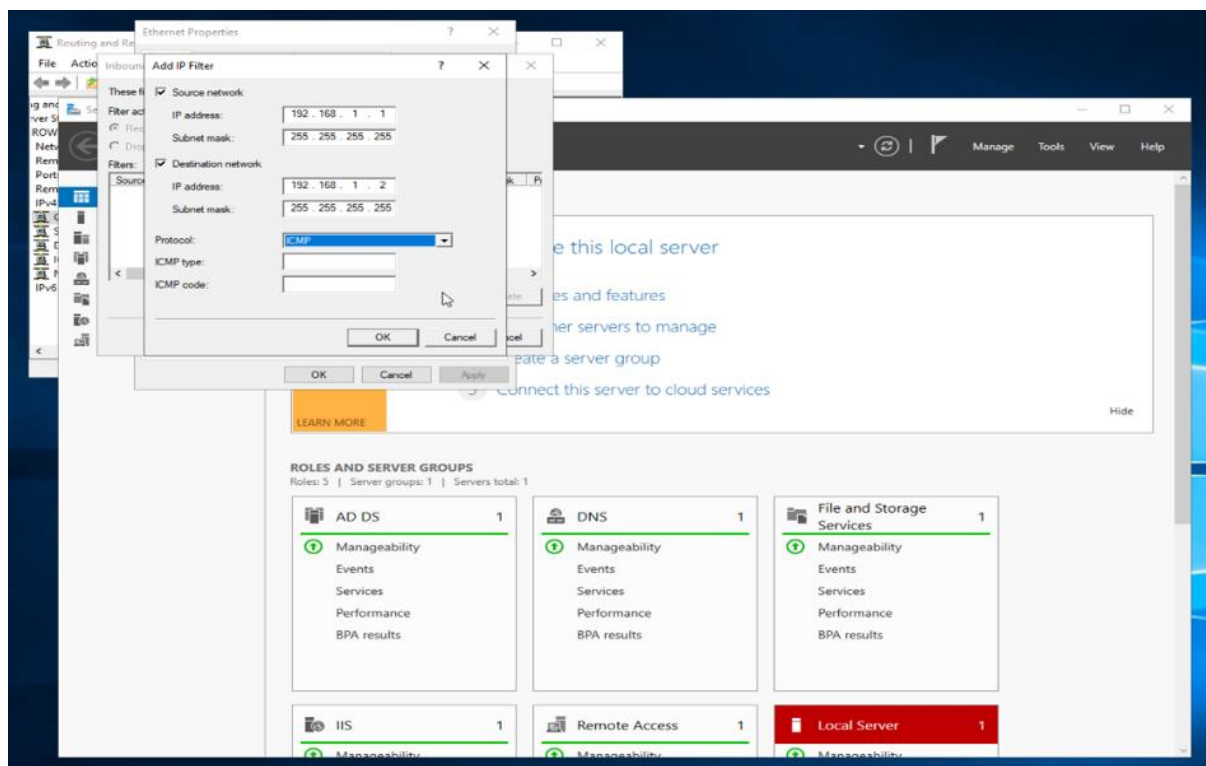
I created a reverse lookup zone and configured PTR records for all servers to support reverse DNS resolution.

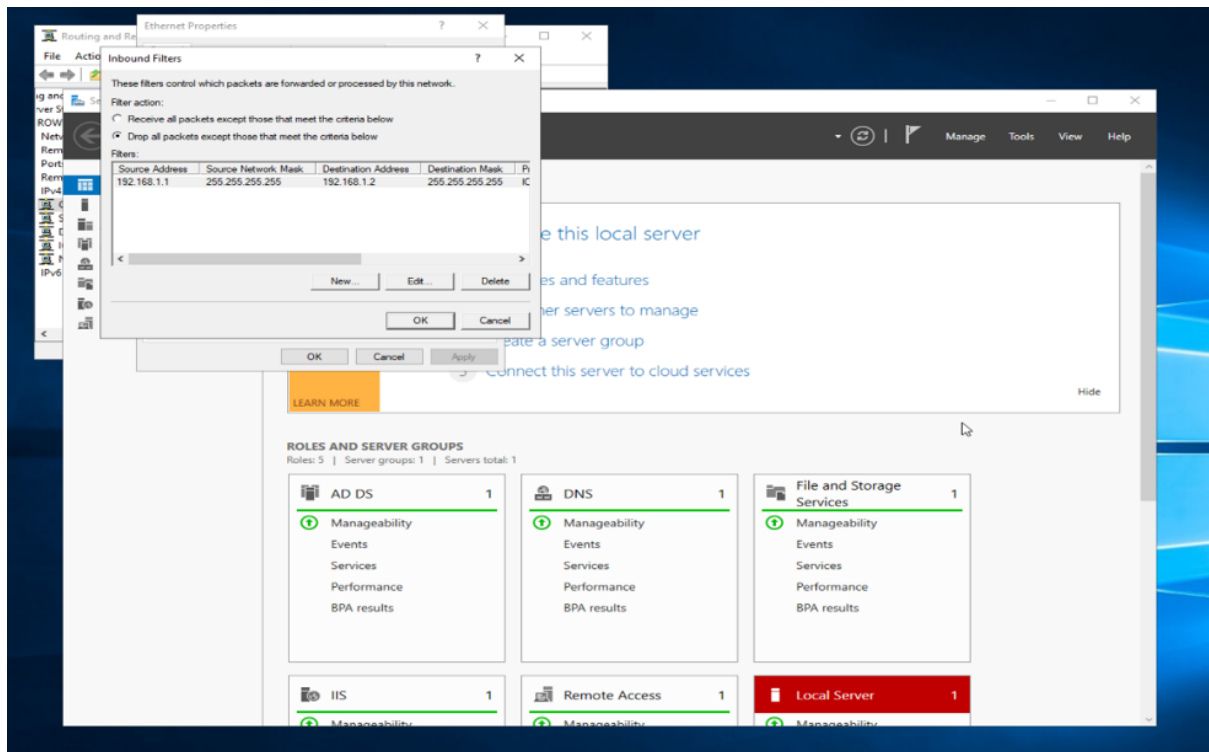
Additionally, I configured the Domain Controller with a secure password policy to enhance security. I also included A records for critical infrastructure servers, even when they were not explicitly listed, to reflect a realistic enterprise network.

Additionally, the DNS zones were configured to accommodate future IP address allocations within the subnets

2.3 Encrypted Connection Between London and Swansea

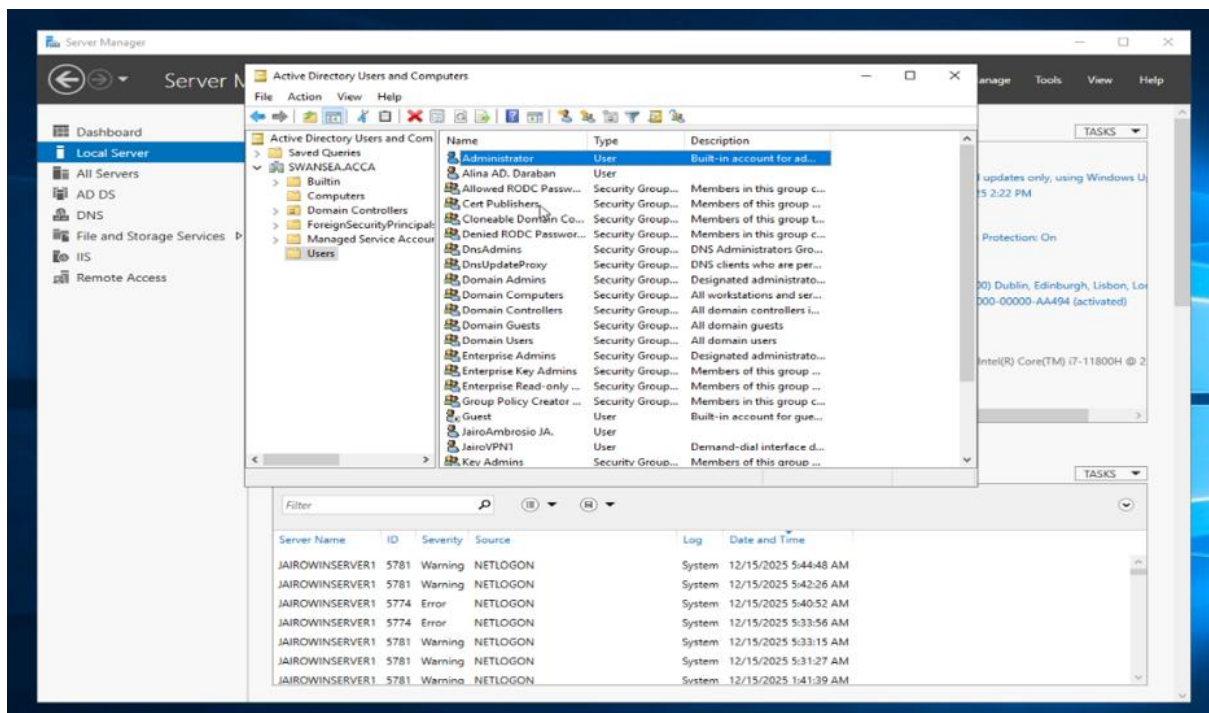
I configured a site-to-site VPN connection between the Swansea and London networks.

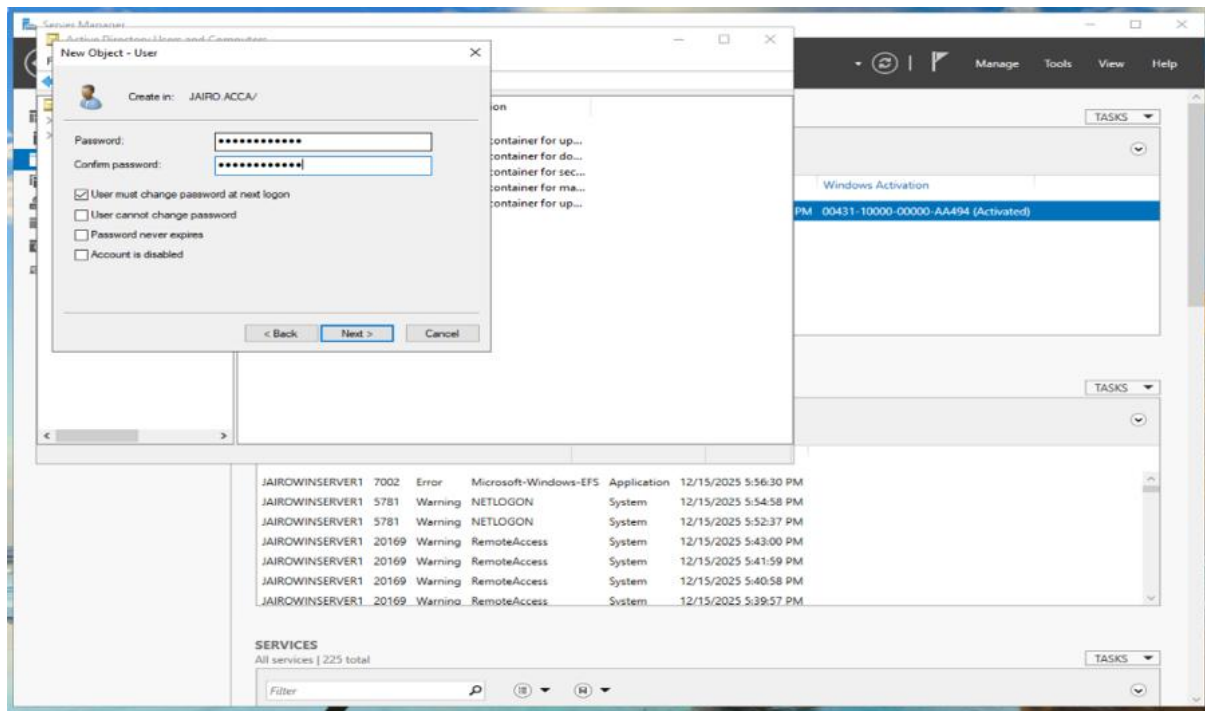




2.4 Users Creation

I created user accounts for the **yourname.acca** domain using the parameters defined by the lecturer. I followed the required naming convention by using the first letter of the first name, followed by a dot and the last name as the SAM Account Name.



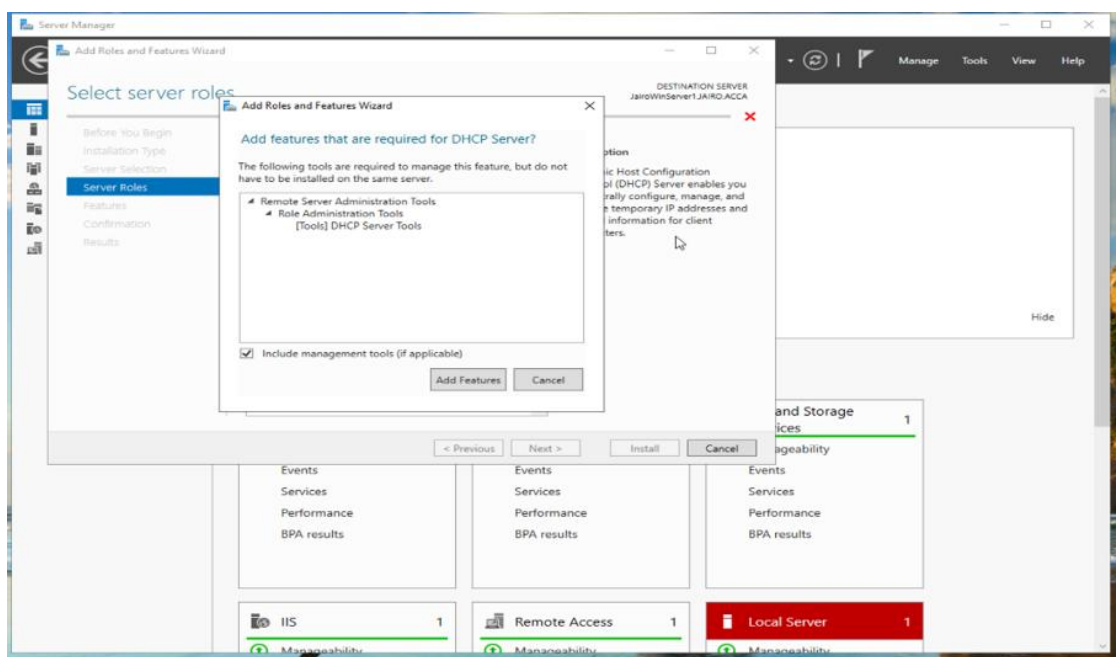


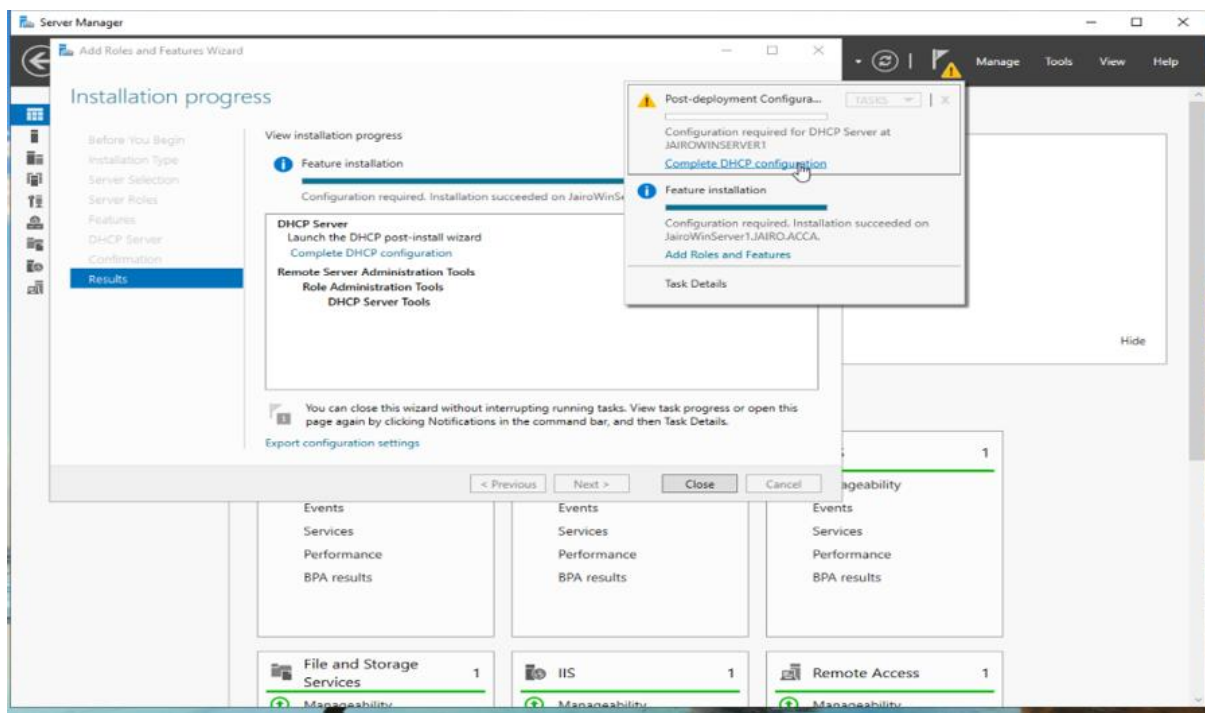
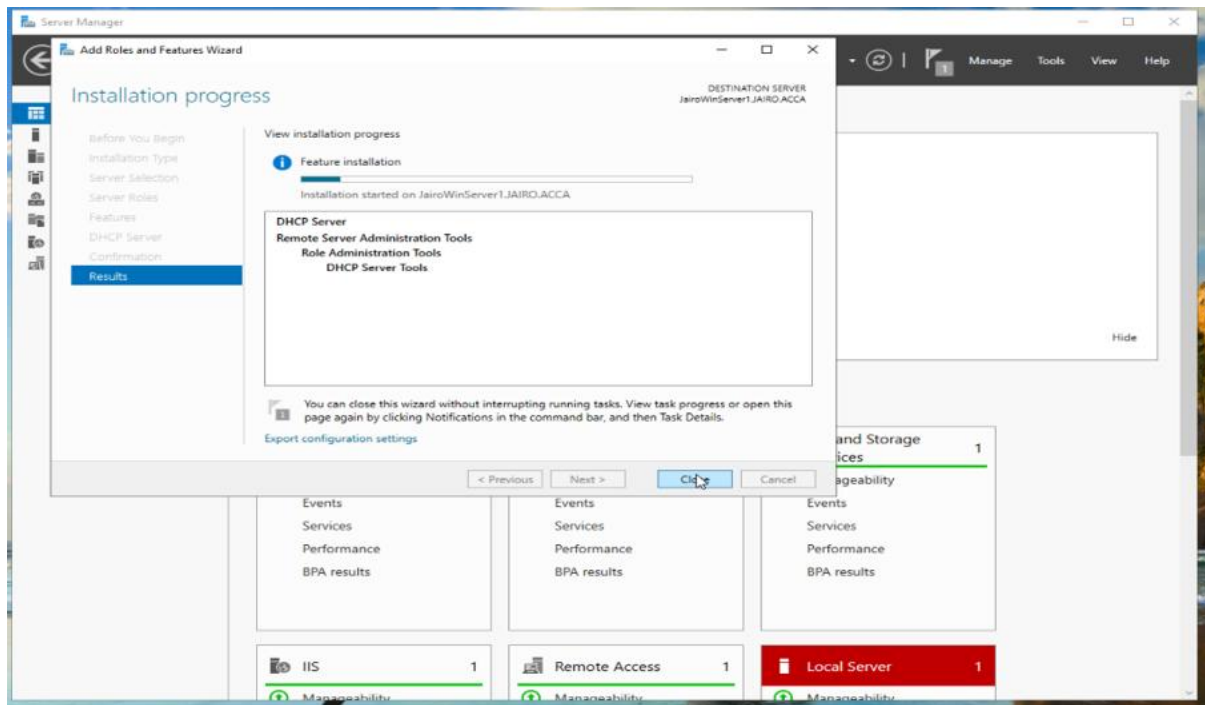
2.5 DHCP Server

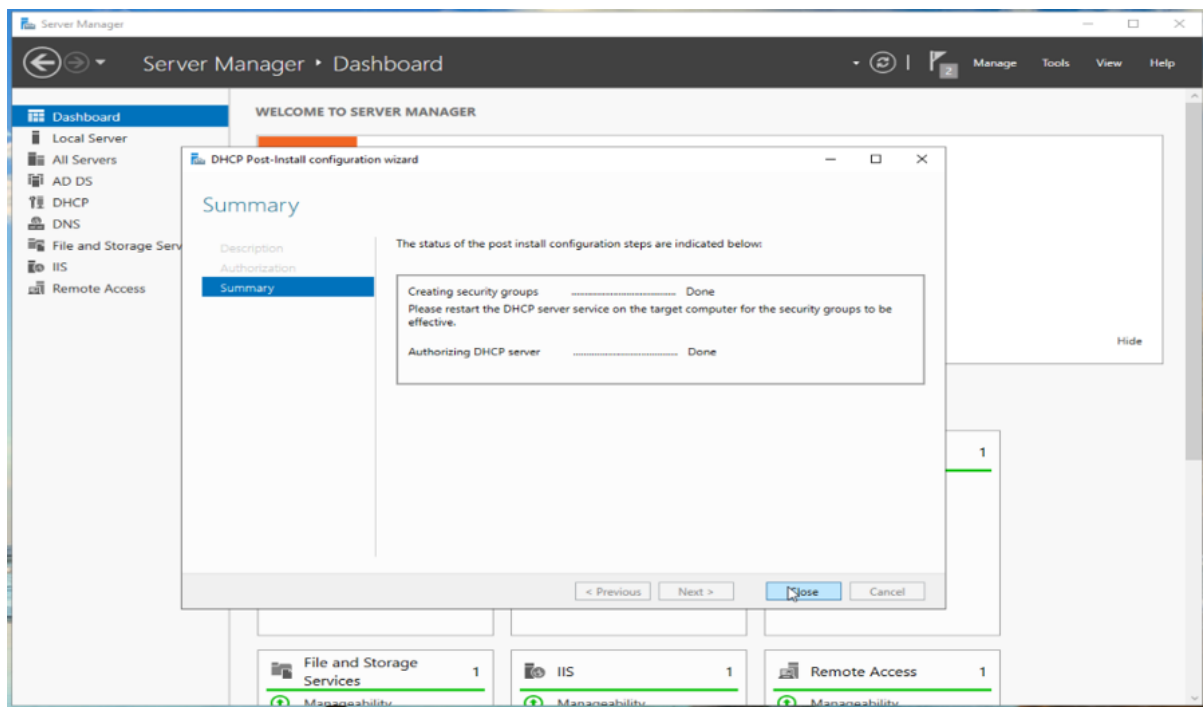
I configured **S-DC** as the DHCP server and defined the IP address range **X.X.X.10 – X.X.X.20** for each network. I also configured appropriate DHCP options based on the infrastructure requirements.

I configured **L-CD** as a DHCP relay server to forward DHCP requests to the central DHCP server.

I ensured that all client machines received their IP addresses automatically from the DHCP server





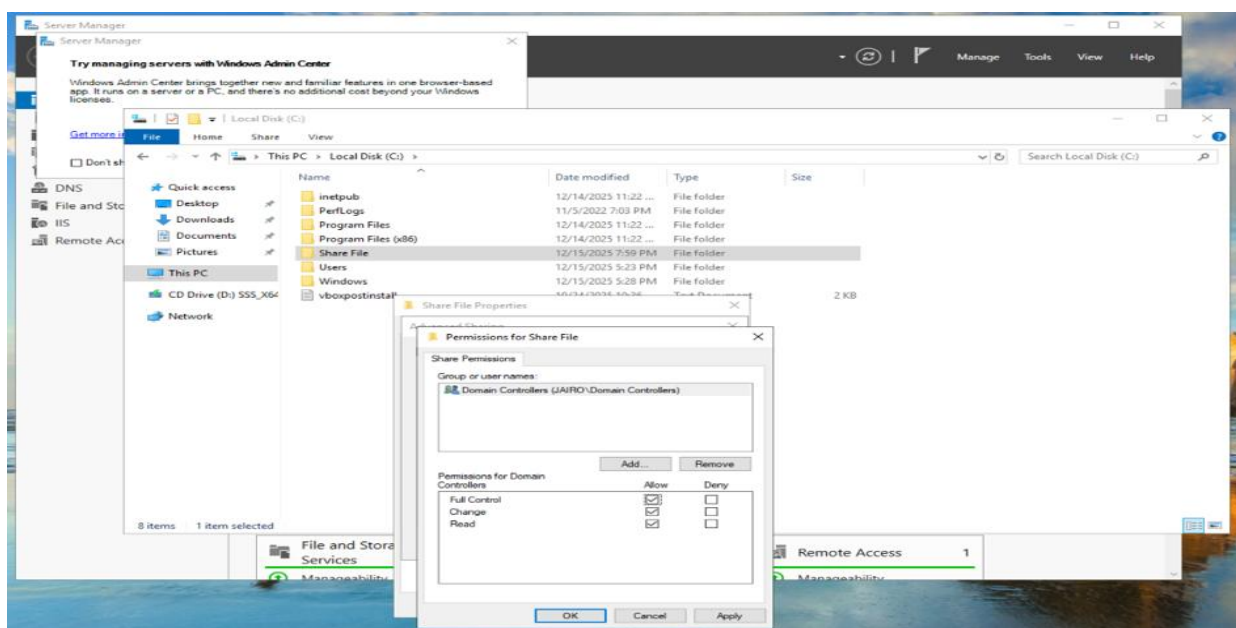


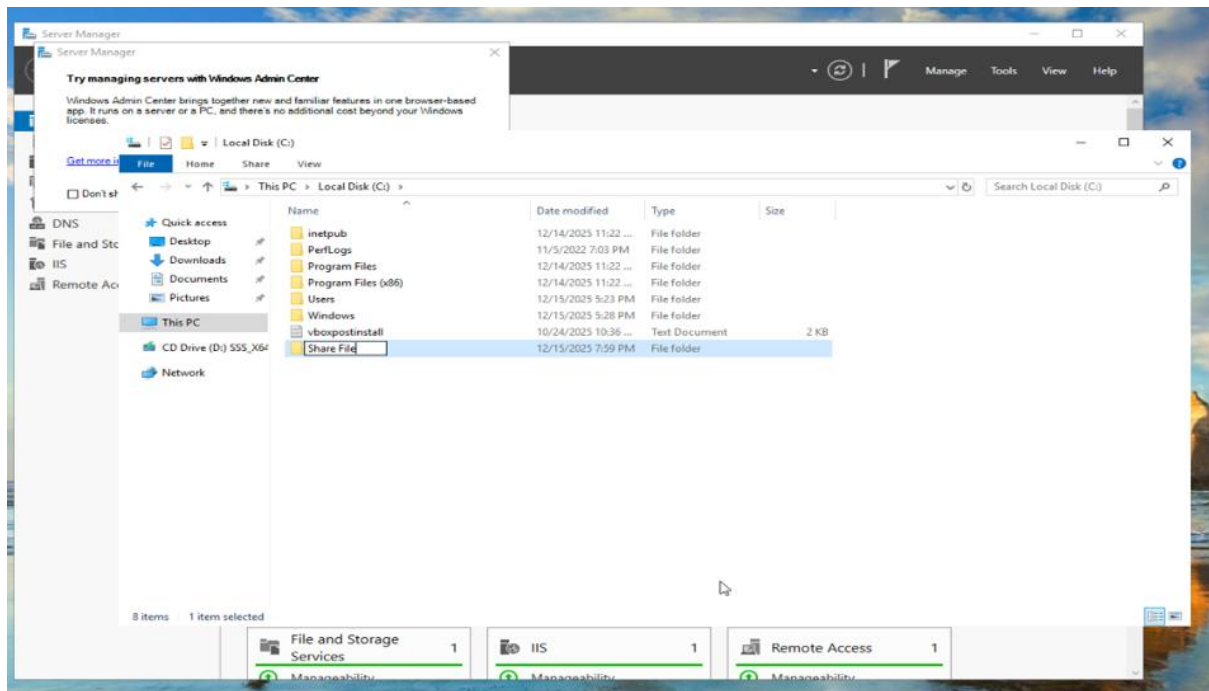
IP addresses were successfully allocated from S-DC with properly configured scopes, lease durations, and security measures. Where appropriate, Group Policy was used to enforce DHCP-related settings on client machines.

I tested the network for full connectivity and verified that both the Swansea and London networks were connected and fully operational.

2.6 Disk Drive

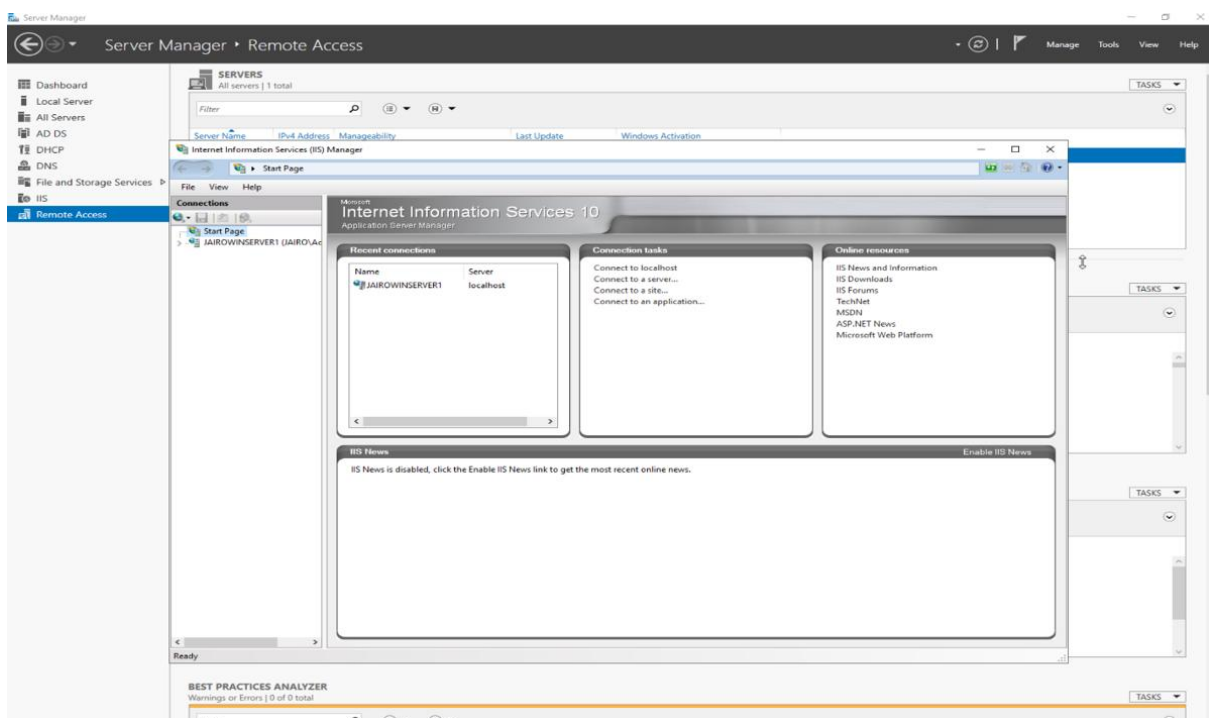
I mounted the second disk drive as **E:\SwanseaFiles**, shared it on the network, and assigned the required permissions. Domain Users were granted full control, while other network users were given read-only access.

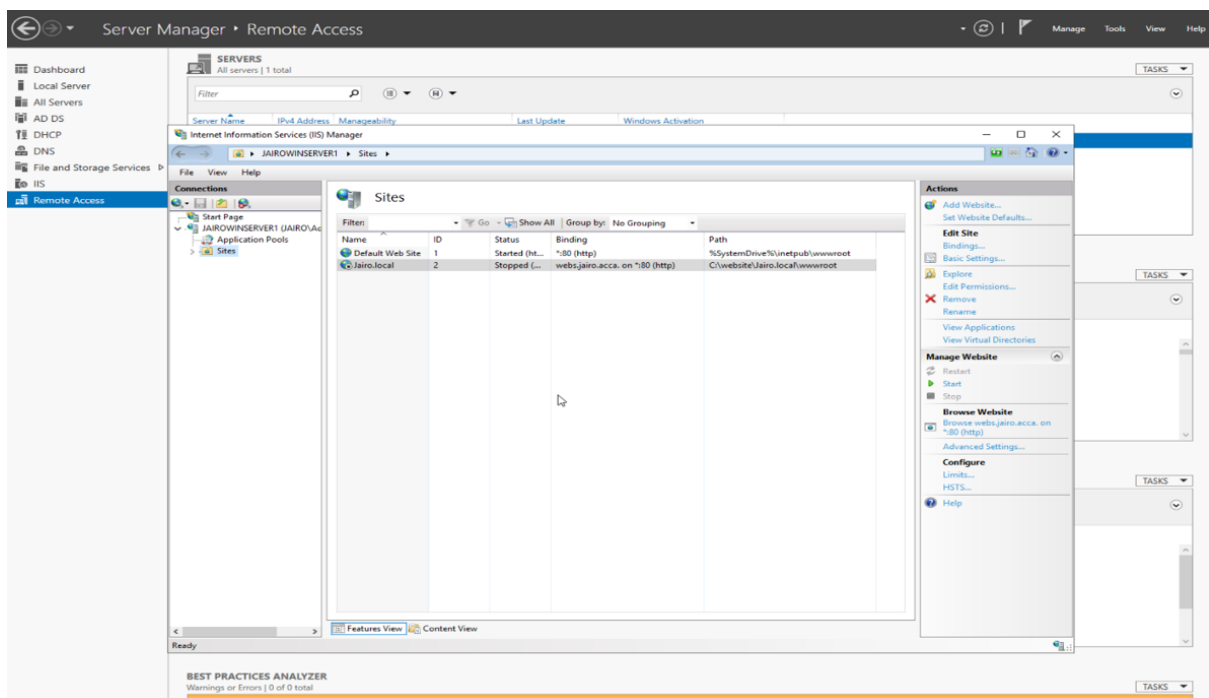
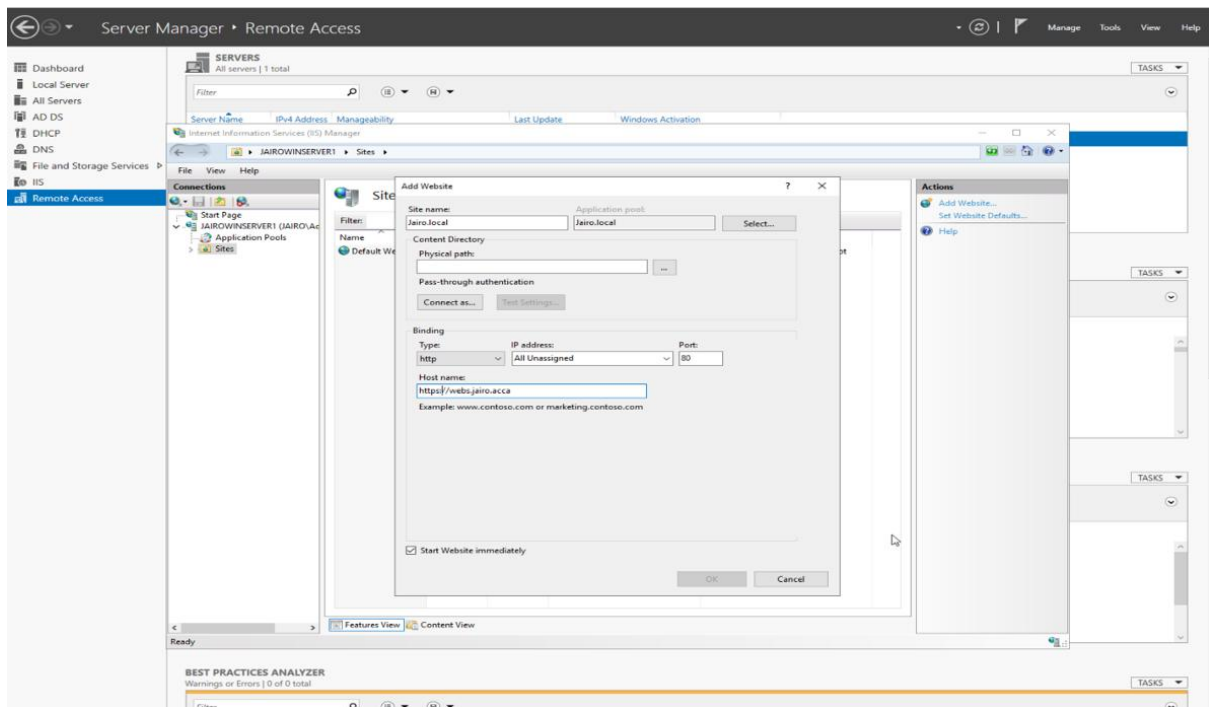




The shared drive was accessible from both the Swansea and London networks with the correct permissions applied.

2.7 IIS Server





The website was securely accessible via <https://webs.yourname.acca>, and all domain users were authenticated successfully. Upon authentication, users were presented with the message **“Welcome to Swansea Website”**.

3. Conclusion

This project showcased the successful setup and integration of essential Windows Server services in a simulated enterprise environment. Routing and Remote Access was configured with a persistent site-to-site VPN, alongside the creation of a new

Active Directory forest and domain, enabling secure connectivity and centralized identity management. Core supporting services—including DNS, DHCP, and file sharing—were also deployed to provide reliable name resolution, automated IP addressing, and shared storage.

User accounts were created using standardized naming conventions, emphasizing the value of consistency and ease of management in enterprise identity systems. The implementation of reverse lookup zones and PTR records further reflected DNS best practices, enhancing troubleshooting and overall reliability.

Throughout the project, theoretical concepts were reinforced through hands-on configuration, with screenshots confirming each step. The result is a fully functional infrastructure that closely reflects real-world enterprise environments and demonstrates how networking, security, and directory services work together to support modern IT operations.