

ACCA5023 – Component 2

Configure and Manage the Virtualised Enterprise Network

Student Name: Louis Shortland

Student ID: 2433889

Network Operating Systems and
Services

Contents

1. Introduction	3
2. Network Topology	3
3. Routing	7
4. Active Directory Domain Services (AD DS)	10
5. DNS Configuration	14
6. User Accounts	19
7. Domain Membership	22
8. DHCP	25
9. Connectivity Testing	28
10. Shared Folder	35
11. Internet Information Services (IIS)	37
12. Remote Desktop Services (RDS)	38
13. Troubleshooting	39
14. Conclusion	41
15. References	42

1. Introduction

The aim of this project was to configure and manage a virtualised enterprise network representing two separated office locations, Birmingham and London. Windows Server 2022 and Debian Linux were used to deploy key enterprise services including Active Directory Domain Services (AD DS), DNS, DHCP, Routing and Remote Access Services (RRAS), domain membership and user management (Microsoft, 2025b, Microsoft, 2025c, Microsoft, 2025e). The completed environment was tested to confirm successful communication, authentication and connectivity between Windows and Linux clients. This project provided practical experience of configuring, managing and troubleshooting enterprise network infrastructure within a virtual environment.

2. Network Topology

[I wasn't sure weather I was meant to create a network topology diagram or not from the assessment brief so I just put together this one on canva which labels all servers and clients and the London and Birmingham offices]

NOSS LONDON 2026 INC

Enterprise Network Topology

Active Directory Domain: louis.acca

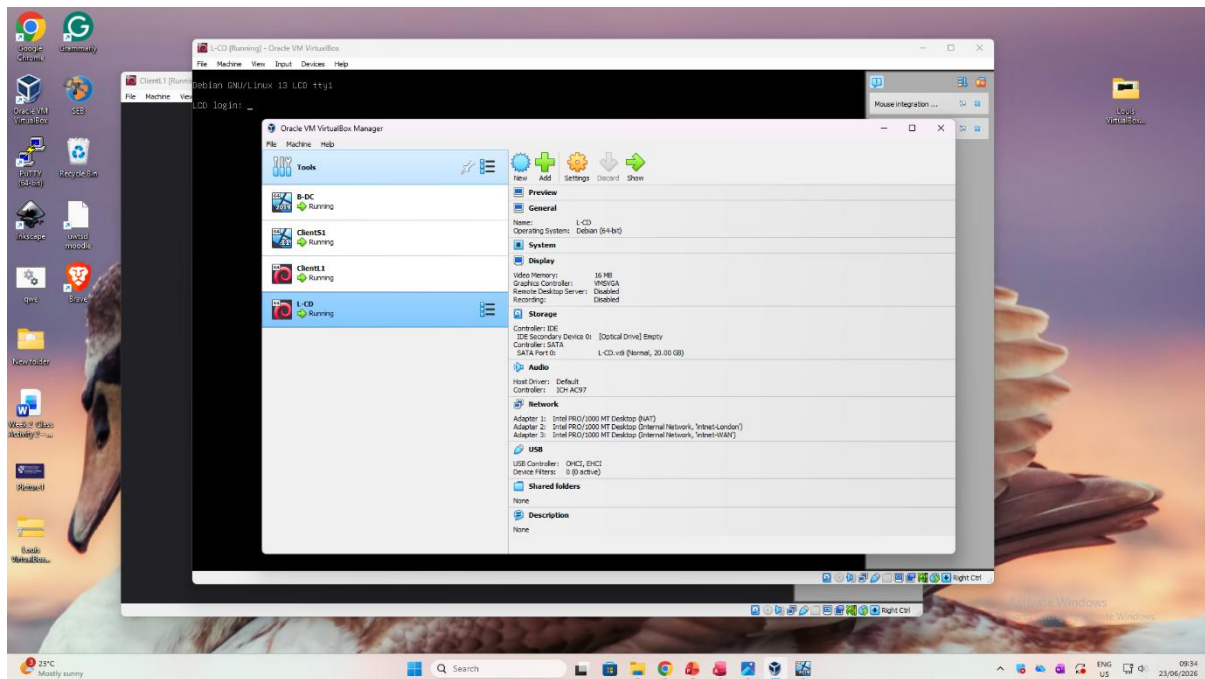
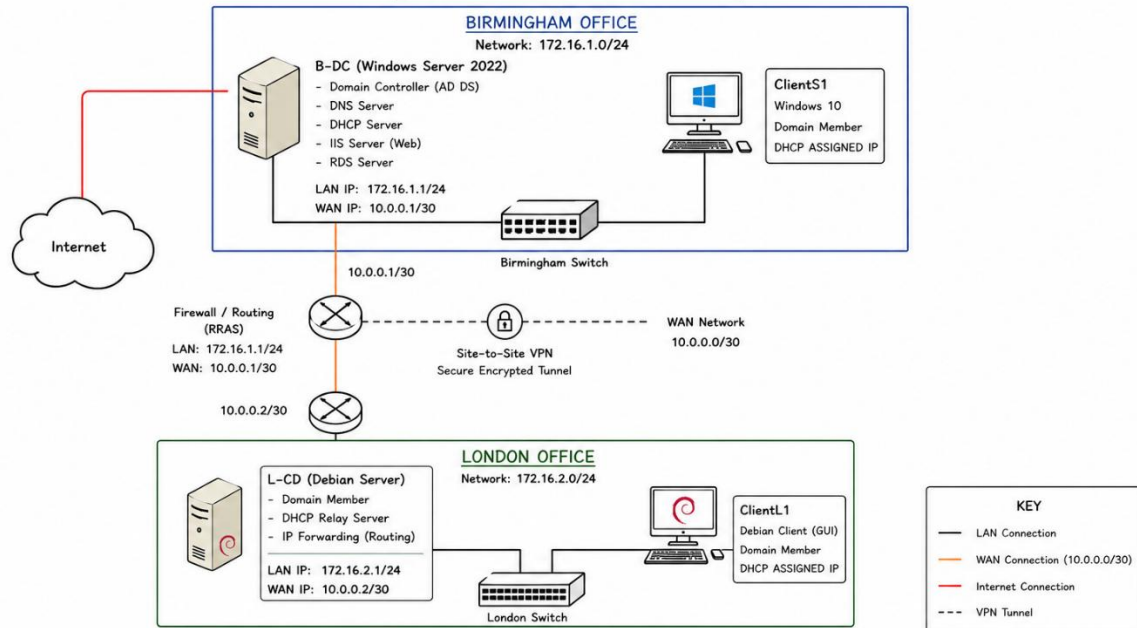


Figure 1 – Oracle VM VirtualBox Manager displaying all virtual machines configured for the enterprise network.

Objective

The objective of this task was to design and configure a virtual enterprise network representing the Birmingham and London office locations. The topology provided the foundation for implementing services including Active Directory, DNS, DHCP, routing and file sharing.

Configuration Completed

The virtual network was configured using Windows Server 2022 and Debian Linux virtual machines representing servers and clients across both office locations. Windows Server provided core infrastructure services including Active Directory Domain Services (AD DS), DNS and DHCP, while Debian supported Linux networking and routing. Each virtual machine was assigned the required network configuration to enable communication between both sites and support domain authentication, routing and file sharing.

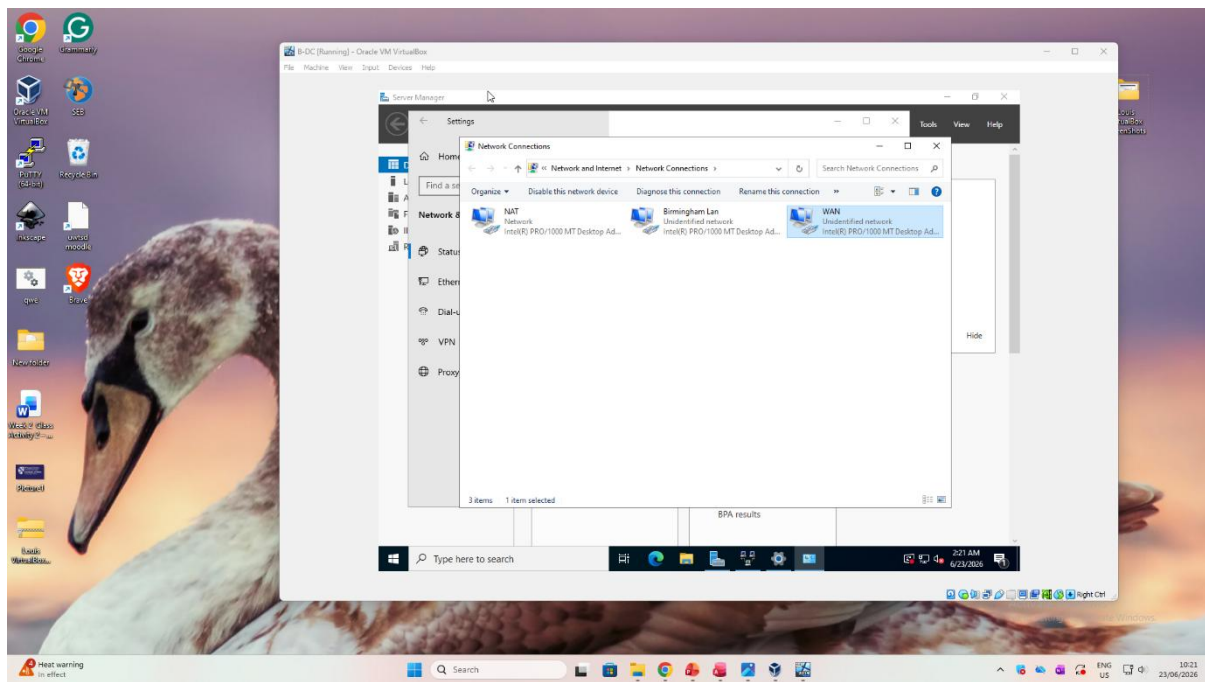


Figure 2 – Network Connections showing the configured virtual network adapters used by the enterprise environment.

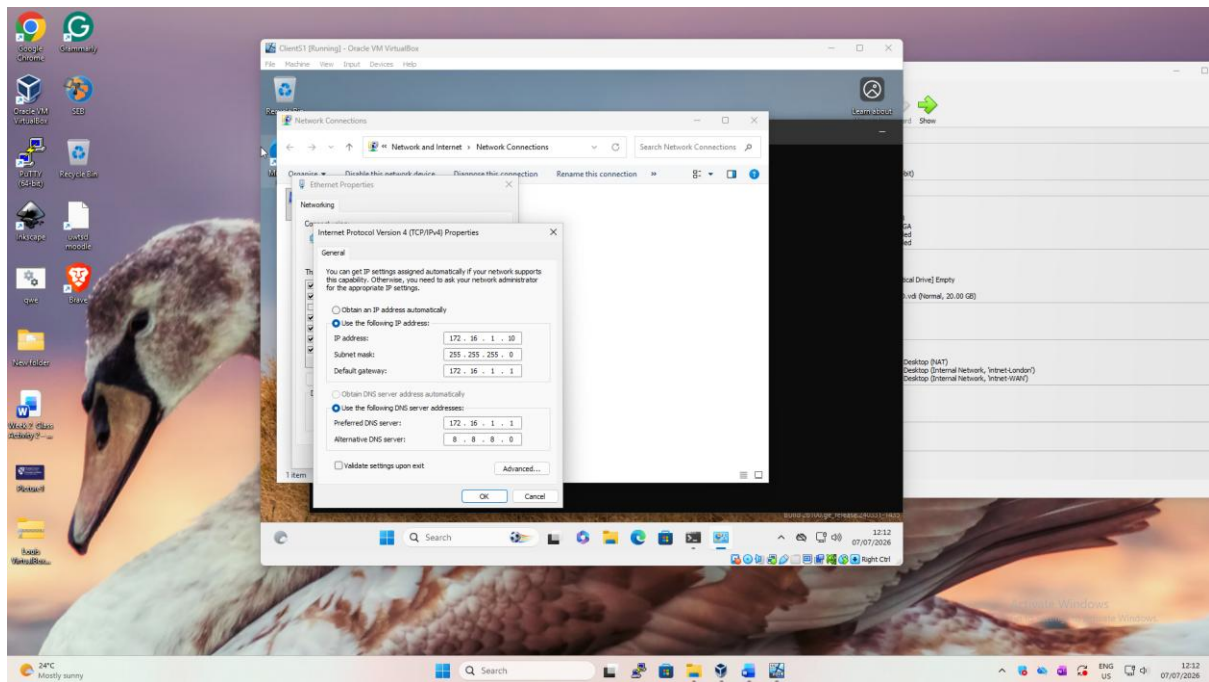


Figure 3 – IPv4 configuration for the enterprise network.

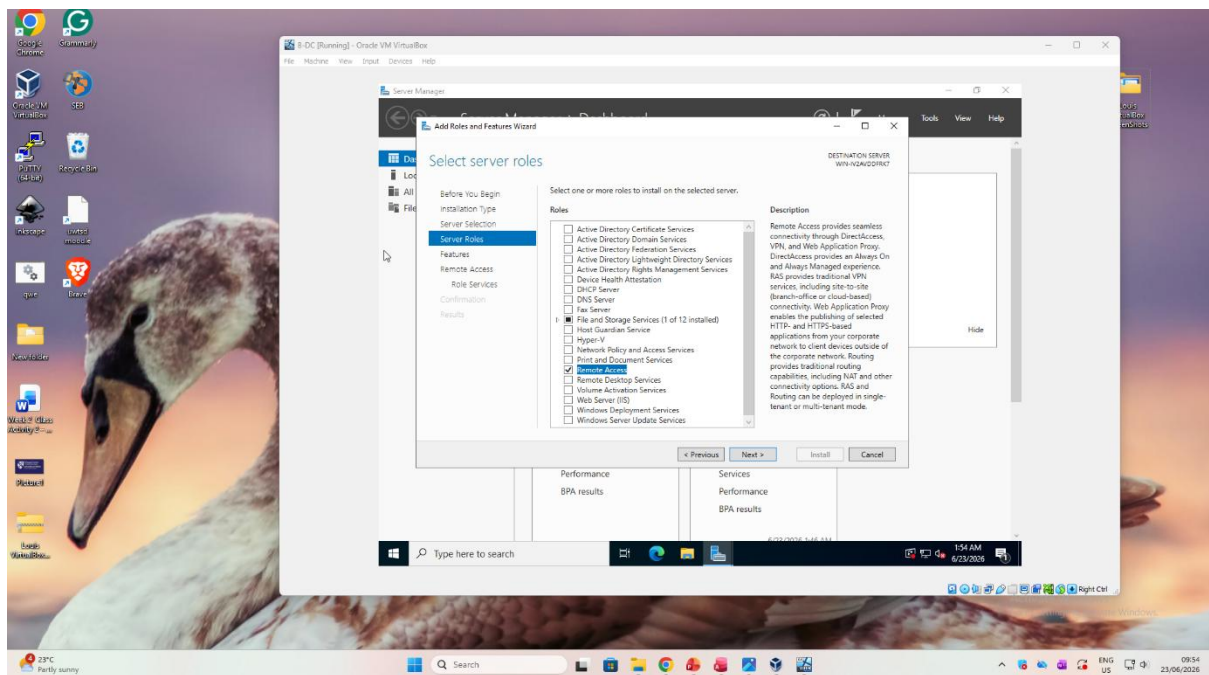


Figure 4 – Selecting the Routing role during Windows Server feature installation.

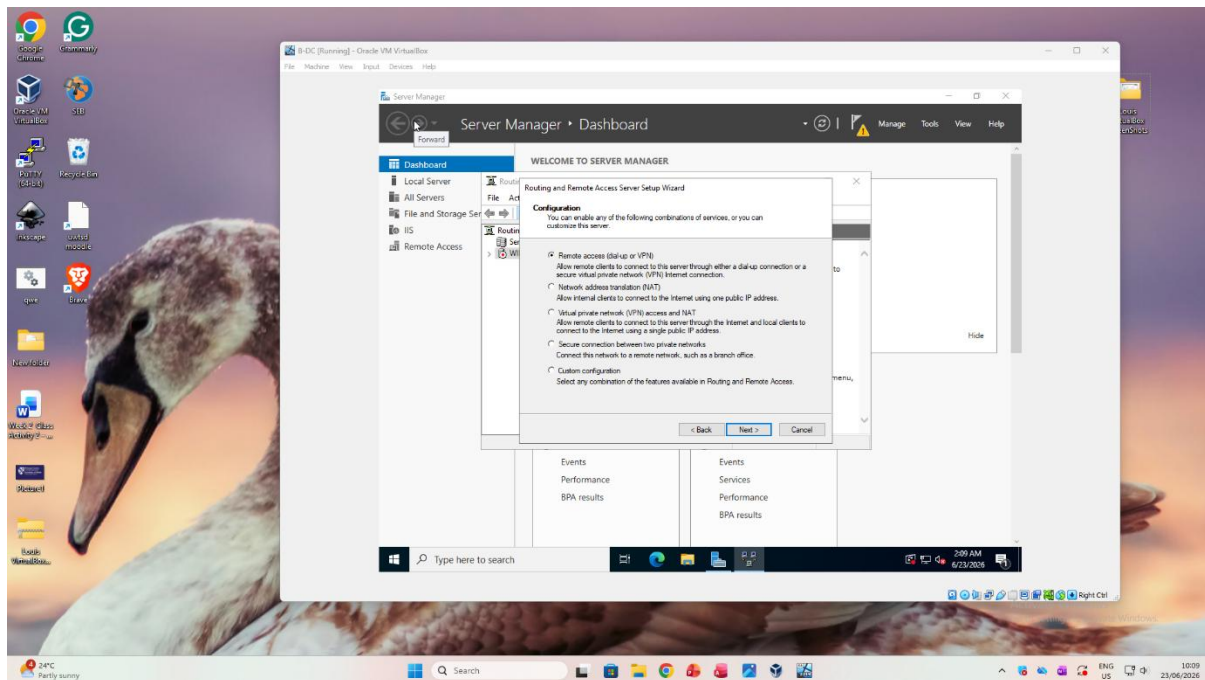


Figure 5 - Installing the Routing and Remote Access Service (RRAS).

Reflection

Designing the network topology before configuring services simplified the deployment process and reduced configuration errors. It also provided a clear structure for implementing and testing the remaining enterprise services throughout the project.

3. Routing

Birmingham Routing

Objective

This task involved configuring RRAS on the Birmingham Windows Server to enable communication between the Birmingham and London networks.

Configuration Completed

RRAS was installed through Server Manager and configured for LAN routing. Windows Defender Firewall was updated to allow ICMP Echo Requests, enabling ping connectivity tests.

Figure 6 – Configuring Routing and Remote Access Services (RRAS). (Screenshot lost)

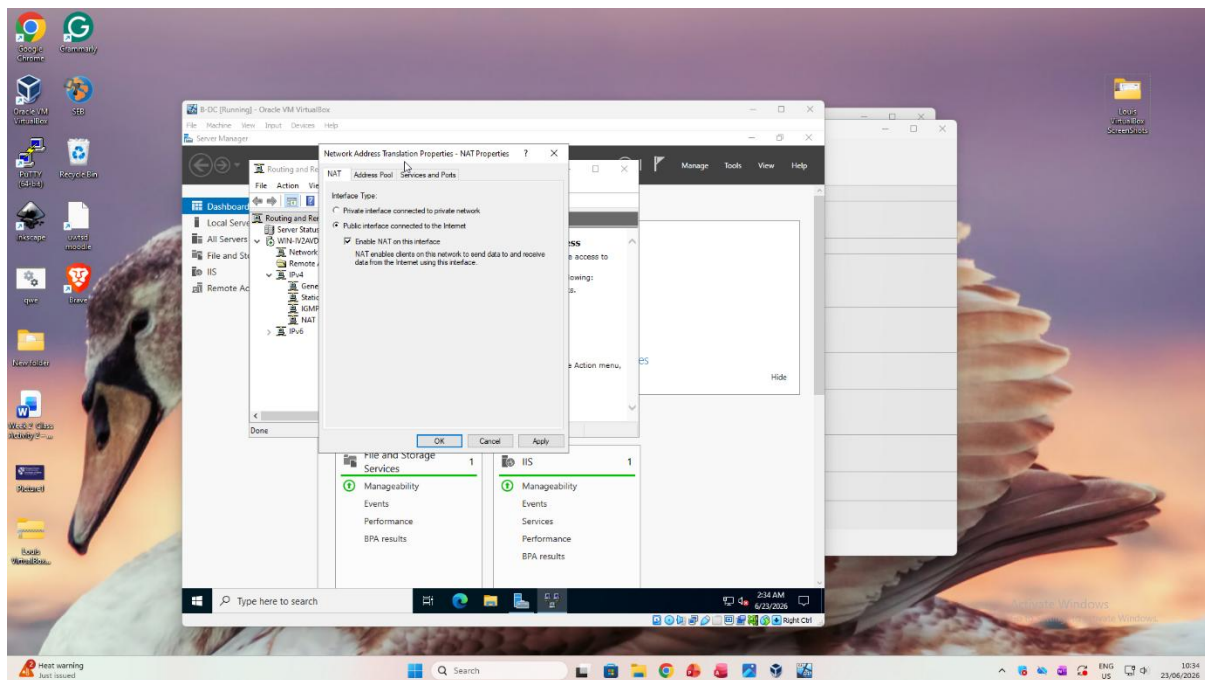


Figure 7 – Configuring Network Address Translation (NAT) within RRAS.

Figure 8 - Routing and Remote Access Services installed and configured on the Birmingham Windows Server. (Screenshot lost)

Reflection

Configuring RRAS enabled communication between network segments and provided a reliable method of verifying connectivity through ICMP testing.

London Routing

Objective

The objective of this task was to configure the Debian server to forward network traffic between the London and Birmingham networks.

Configuration Completed

IP forwarding was enabled on the Debian server and persistent routing was configured to remain active after reboot. The routing table was verified and

connectivity testing confirmed successful communication between the London and Birmingham networks.

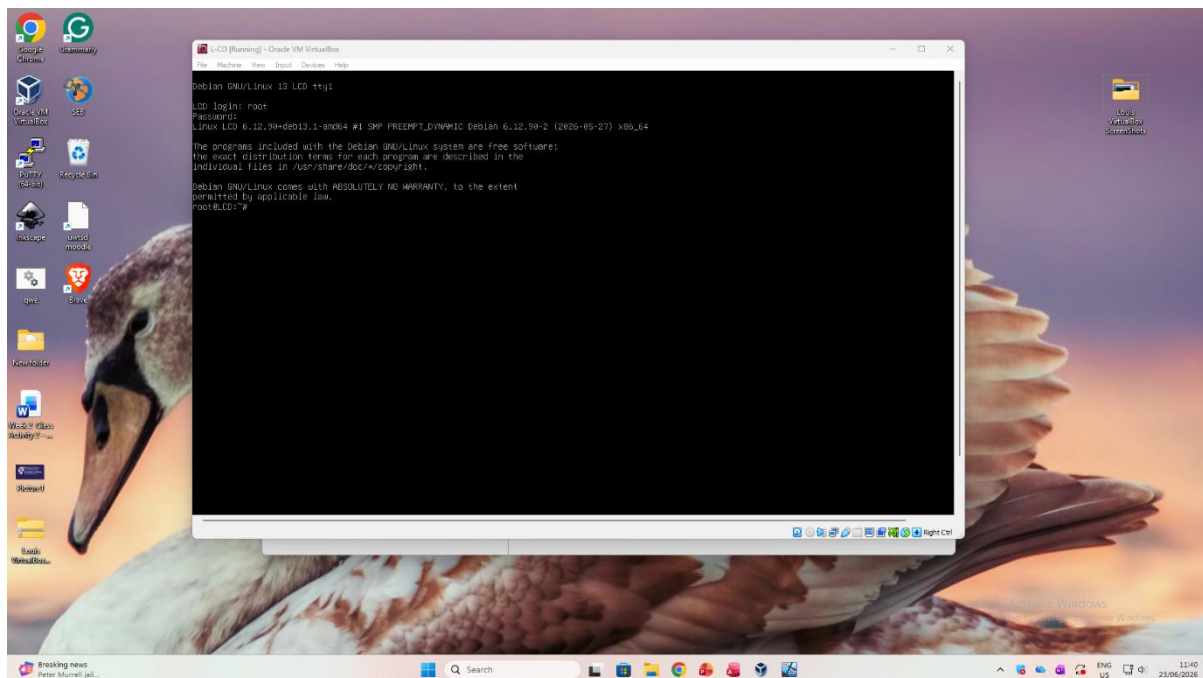


Figure 9 – Debian terminal.

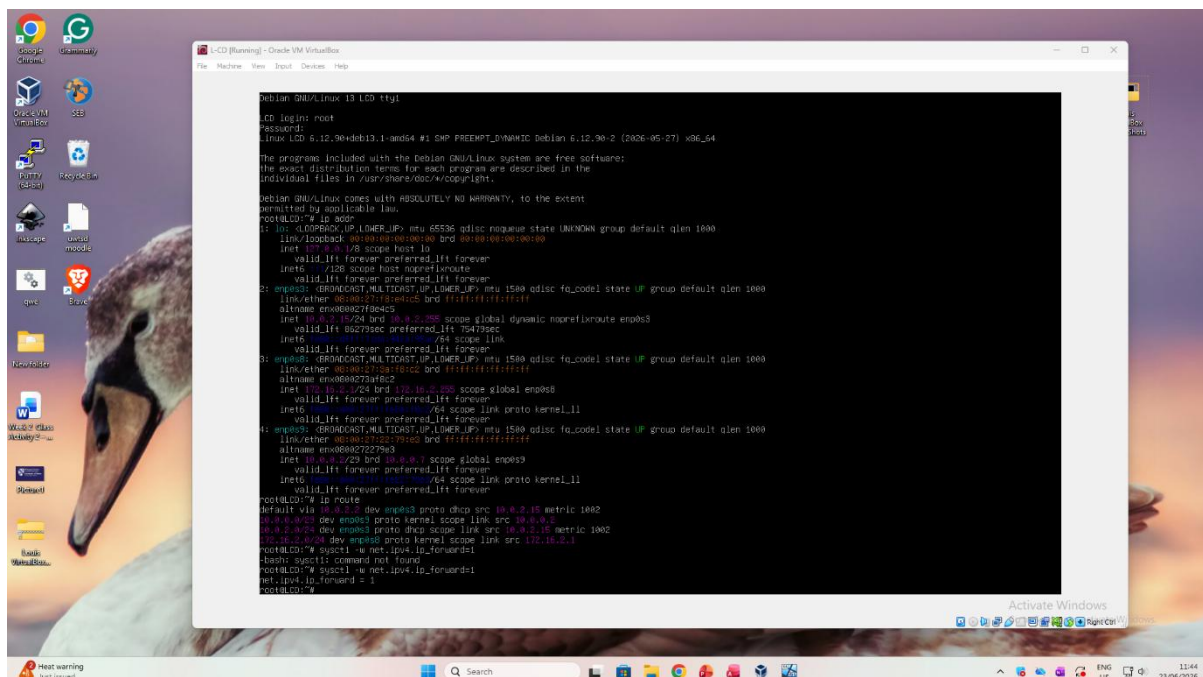


Figure 10 – IP forwarding enabled.

Figure 11 – Routing table. (Screenshot lost)

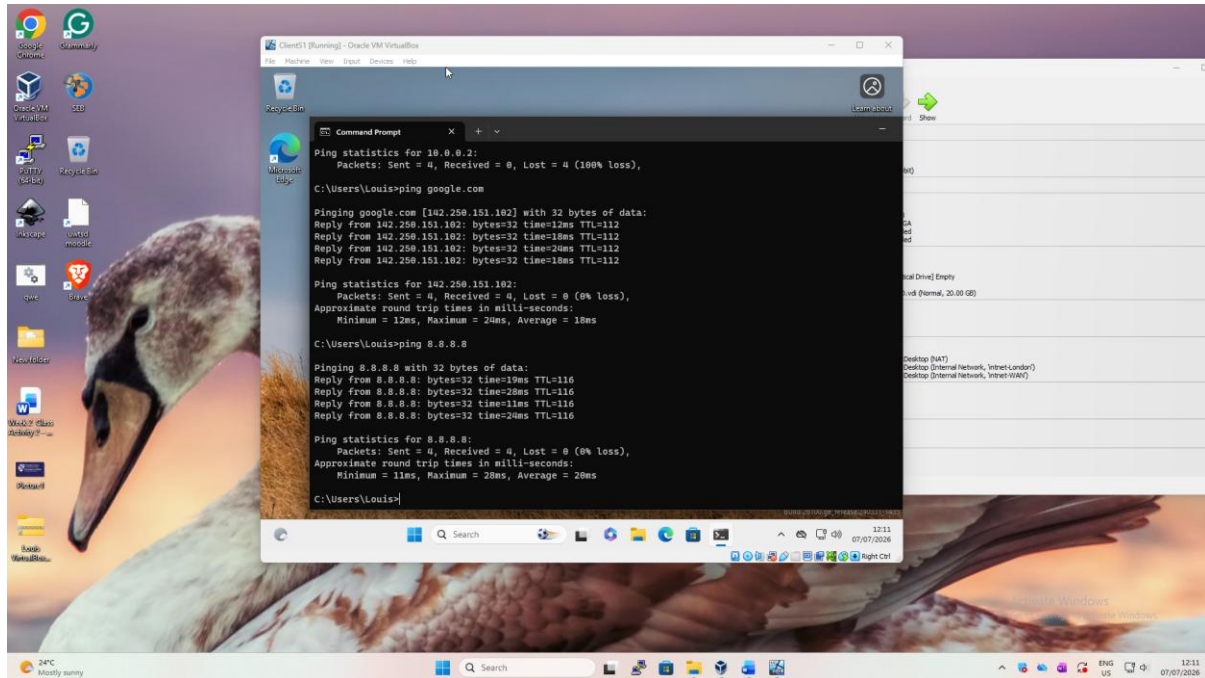


Figure 12 – Successful connectivity test.

Reflection

The Linux routing configuration allowed communication between both office networks while ensuring routing settings remained available after system restarts.

4. Active Directory Domain Services (AD DS)

Objective

This task involved installing and configuring AD DS on Windows Server 2022 to provide centralised authentication and management across the enterprise network.

Configuration Completed

The Active Directory Domain Services role was installed using Server Manager with the required management tools (Microsoft, 2025b). The server was then promoted to a Domain Controller by creating a new Active Directory forest and configuring the root domain. The DNS Server role was installed automatically, and a Directory Services Restore Mode (DSRM) password was configured. After restarting the server, Active Directory and DNS Manager were verified to confirm that the domain and required DNS zones had been created successfully, providing the foundation for domain authentication and user management.

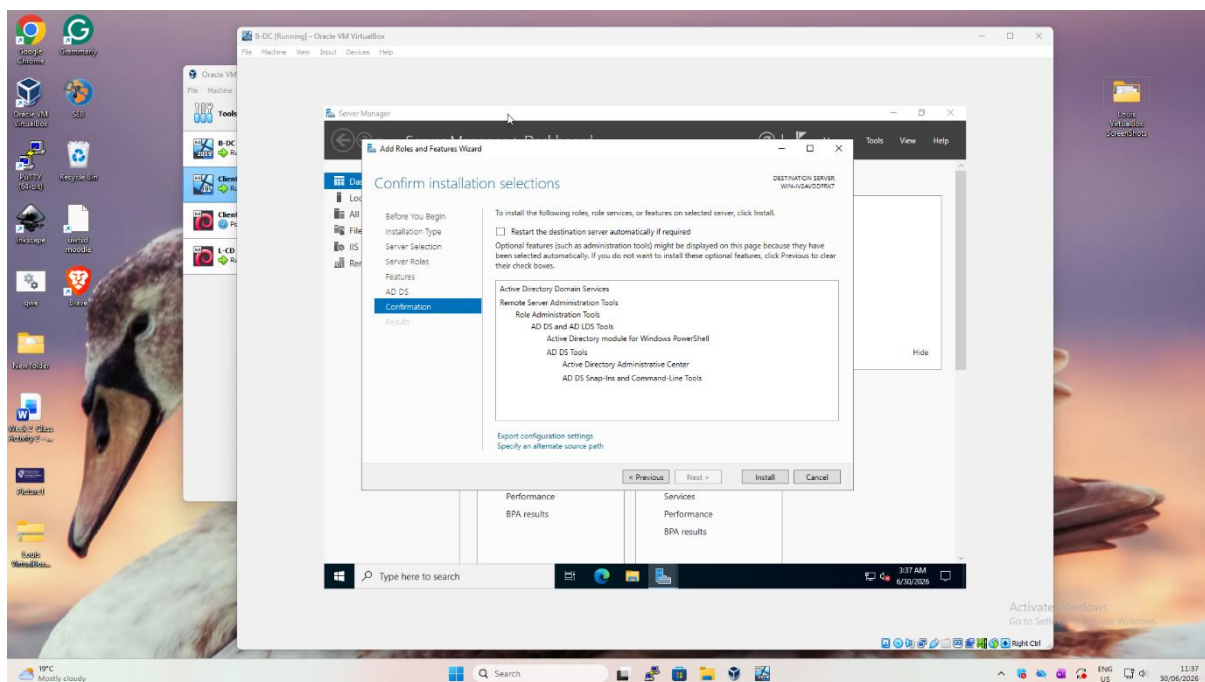


Figure 13 – Selecting the Active Directory Domain Services (AD DS) role.

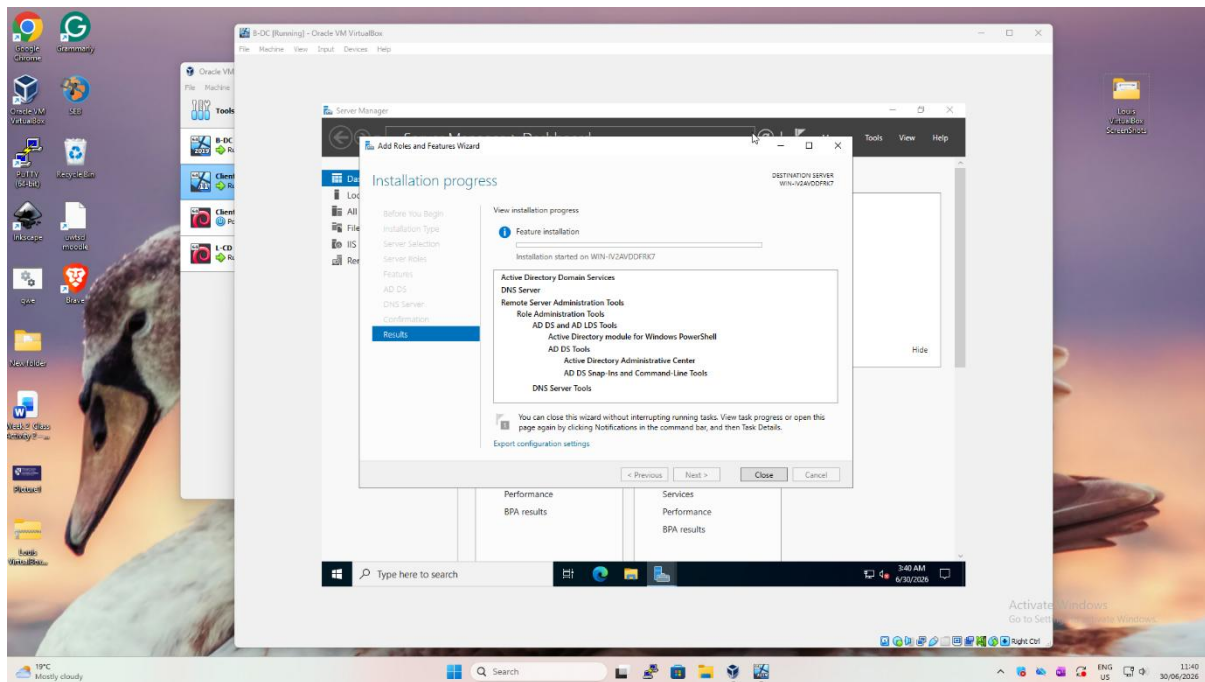


Figure 14 – Installing AD DS and required features.

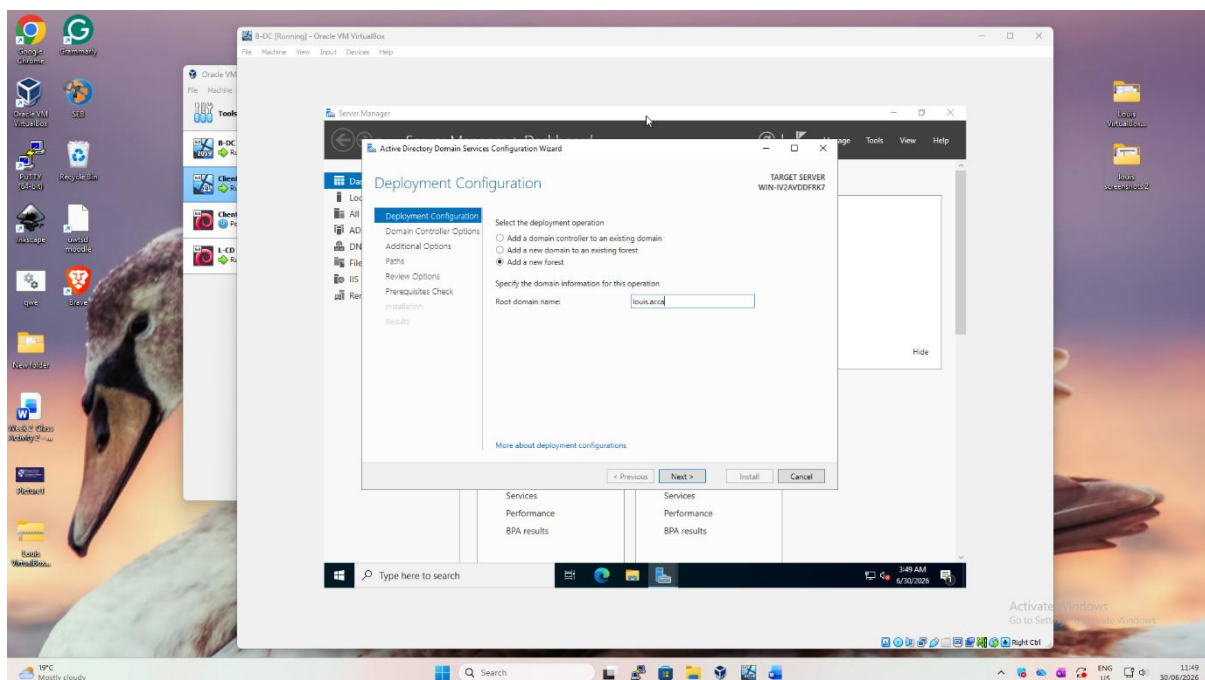


Figure 15 – Creating a new Active Directory forest.

Figure 16 - Configuring Domain Controller options, including DNS Server and the Directory Services Restore Mode (DSRM) password. (Screenshot lost)

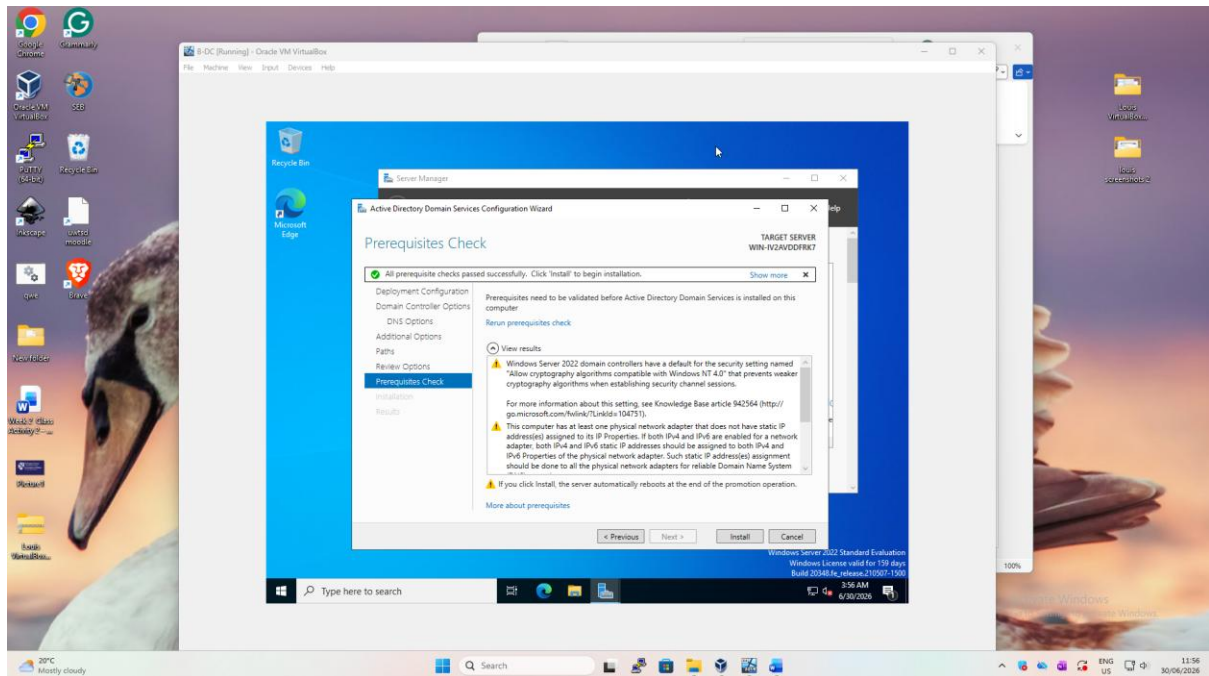


Figure 17 - Active Directory Domain Services prerequisite checks completed successfully before Domain Controller installation.

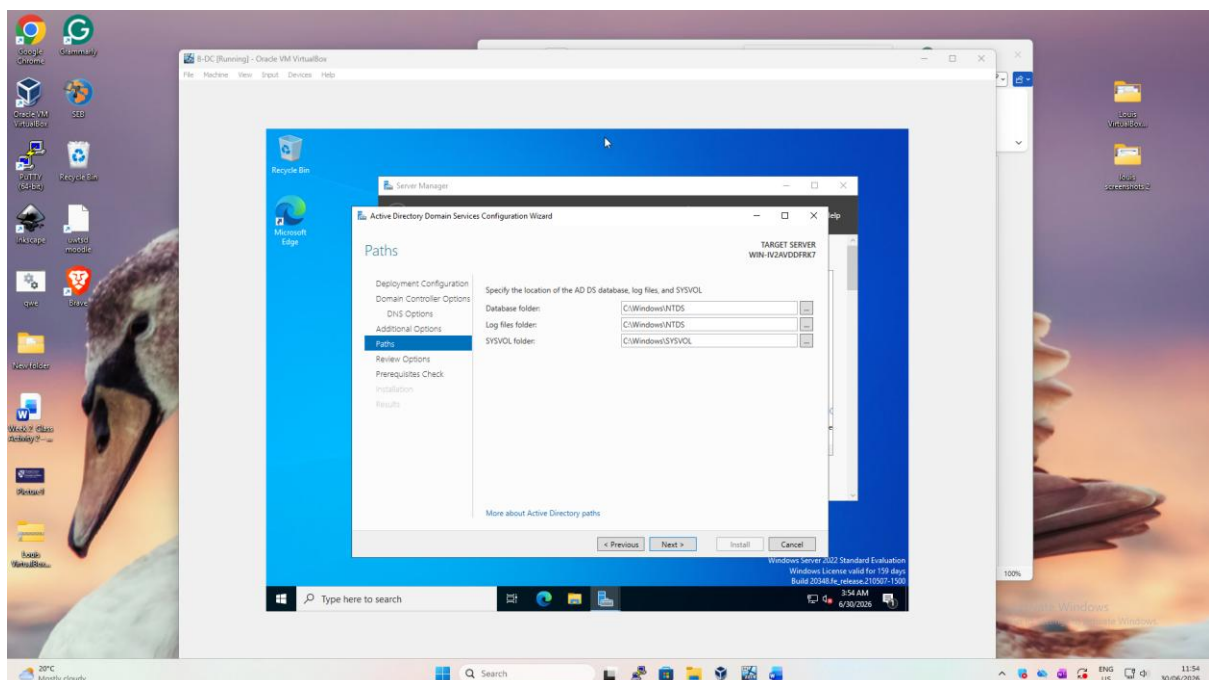


Figure 18 - Specifying the Active Directory database, log files and SYSVOL folder locations during Domain Controller configuration.

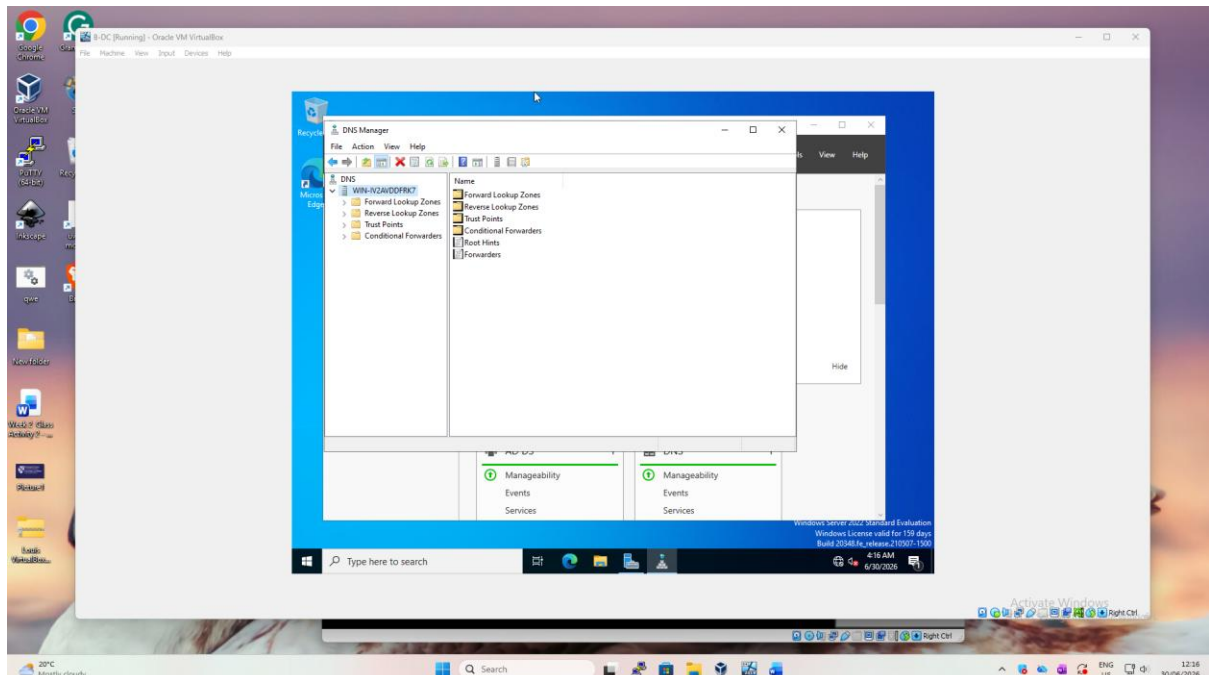


Figure 19 - DNS Manager showing the newly created Active Directory domain.

Reflection

Installing AD DS provided centralised authentication and formed the foundation for DNS, user accounts and domain membership.

5. DNS Configuration

Forward Lookup Zone

Objective

The objective of this task was to configure DNS to provide hostname resolution across the enterprise network and support services such as Active Directory and file sharing.

Configuration Completed

Following the installation of Active Directory, DNS Manager was used to verify the Forward Lookup Zone created during domain promotion (Microsoft, 2025c). A (Host) records were then added for the required enterprise servers, mapping hostnames to

IPv4 addresses. The records were verified to ensure that clients could locate network resources using DNS.

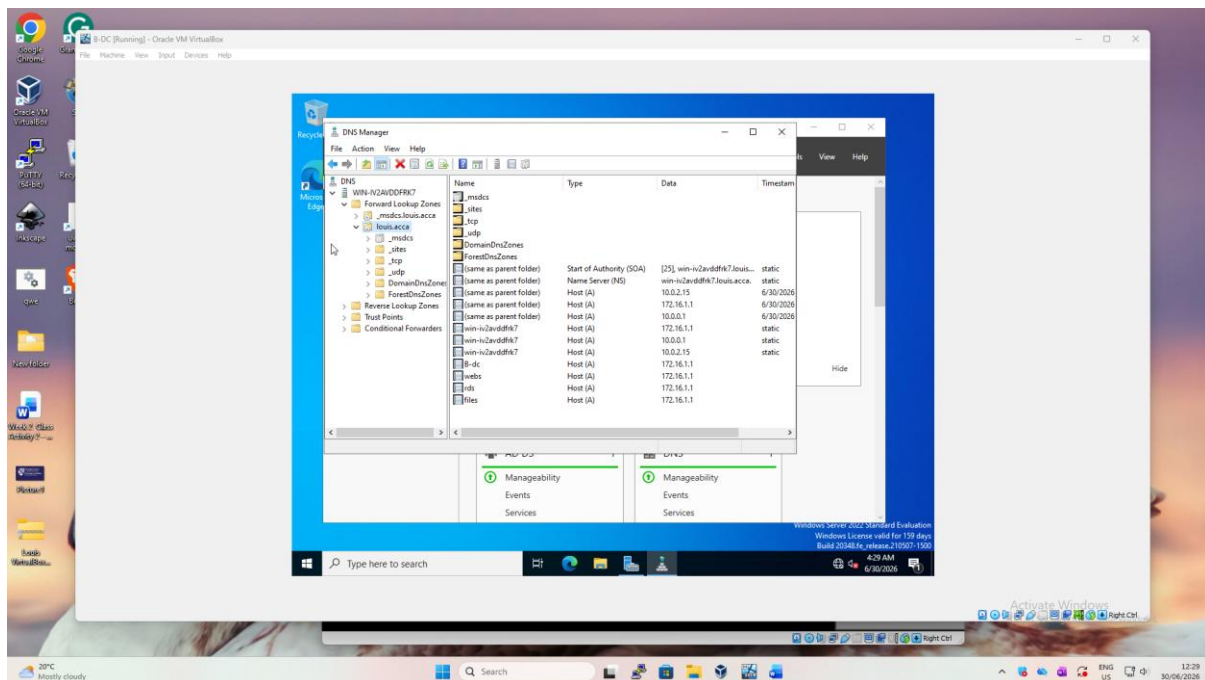


Figure 20 - DNS Manager displaying the Forward Lookup Zone for the enterprise domain.

Figure 21 - Forward Lookup Zone displaying the enterprise domain and DNS records (Screenshot lost)

Configuration Completed

A Reverse Lookup Zone was created using the appropriate IPv4 network ID, and PTR records were configured to map IP addresses to hostnames. The completed configuration enabled both forward and reverse name resolution across the enterprise network.

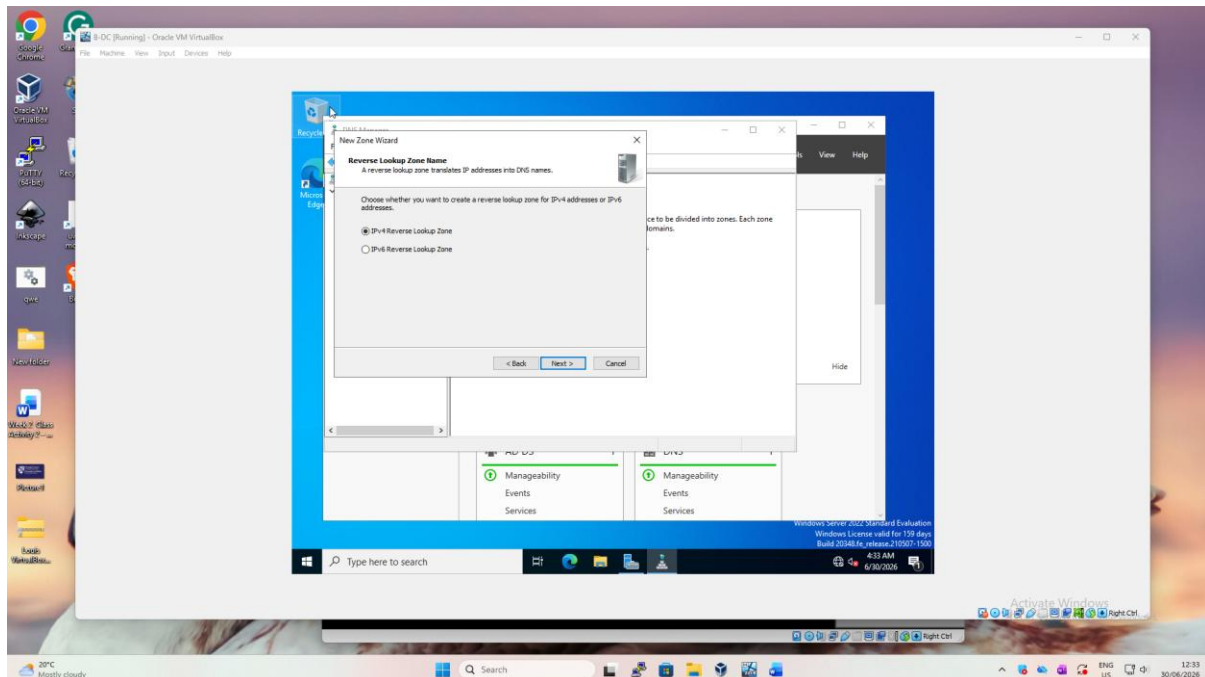


Figure 24 - Creating a new Reverse Lookup Zone using the New Zone Wizard.

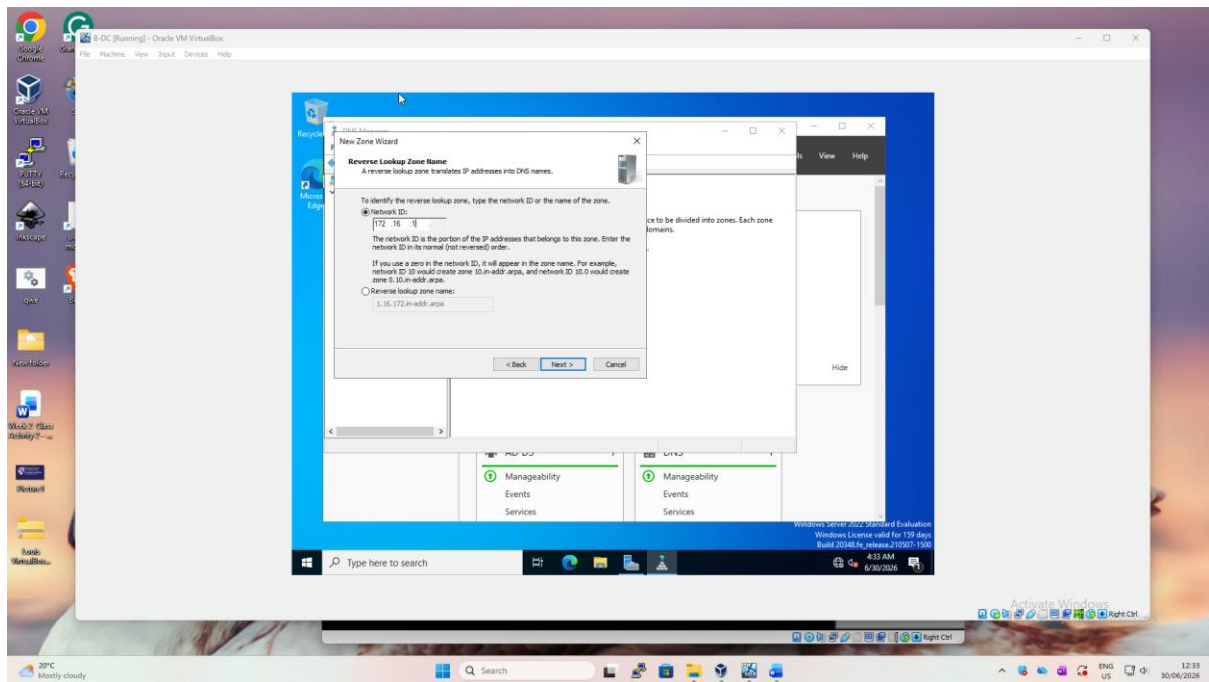


Figure 25 - Configuring the IPv4 Network ID for the Reverse Lookup Zone.

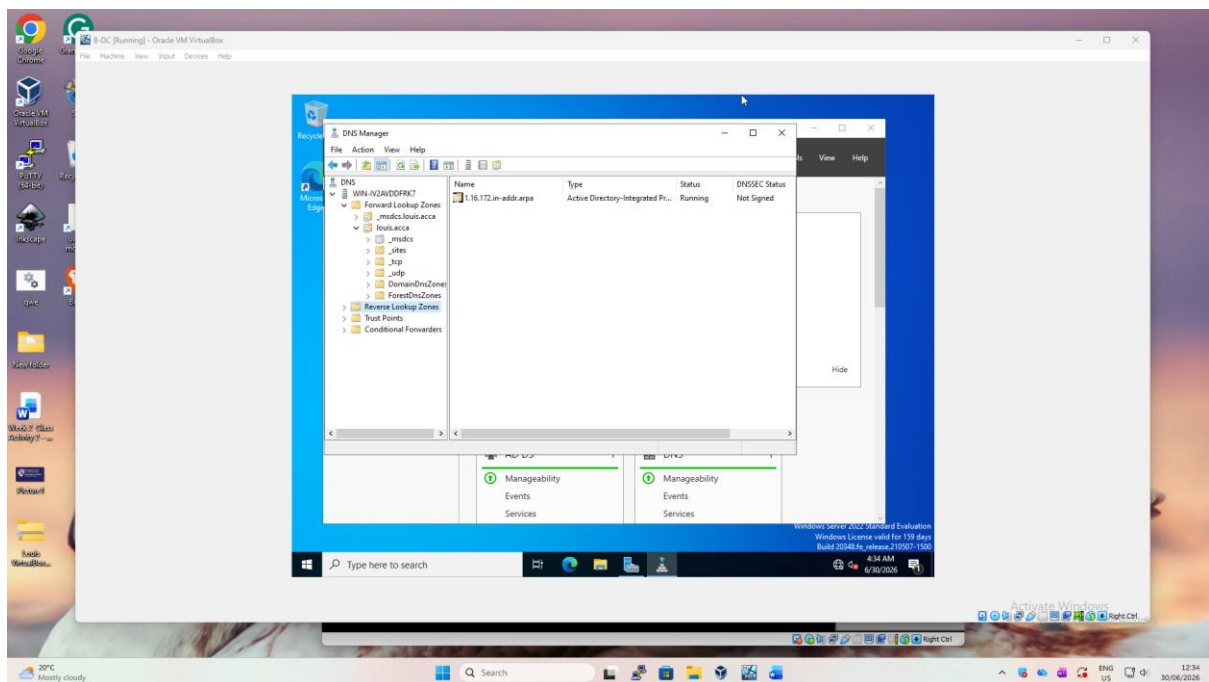


Figure 26 - Completed Reverse Lookup Zone showing successful reverse DNS configuration.

Reflection

Configuring both Forward and Reverse Lookup Zones ensured reliable name resolution throughout the enterprise network. This supported Active Directory, network communication and troubleshooting activities.

6. User Accounts

Objective

The objective of this task was to create and manage Active Directory user accounts efficiently by using PowerShell to automate the import of multiple users into an Organisational Unit (OU).

Configuration Completed

An Organisational Unit (OU) was created within Active Directory Users and Computers to store domain user accounts. PowerShell was then used to execute an import script that automatically created multiple user accounts from the supplied data (Microsoft, 2025d). After the script completed, the accounts were verified within Active Directory to confirm they had been imported successfully into the correct OU. This automated process reduced manual administration and improved consistency.

Figure 27 – Active Directory Users and Computers displaying the enterprise domain.
(Lost screenshot apologies)

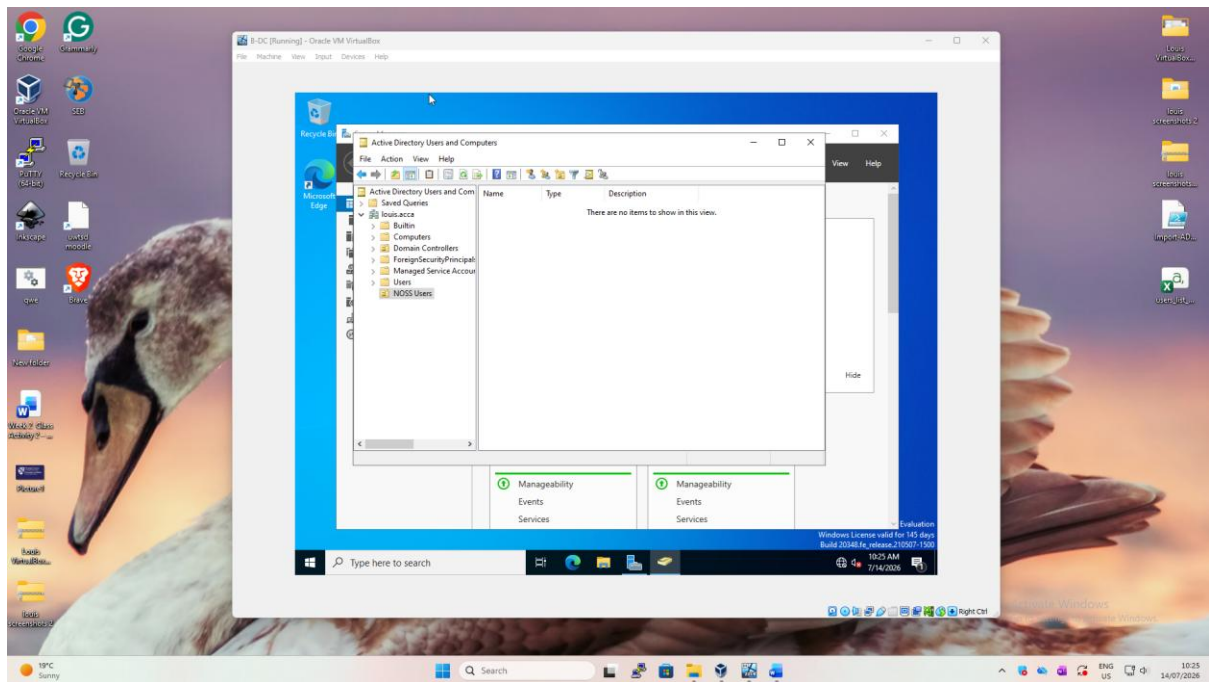


Figure 28 – Creating the Clients organisational unit within Active Directory.

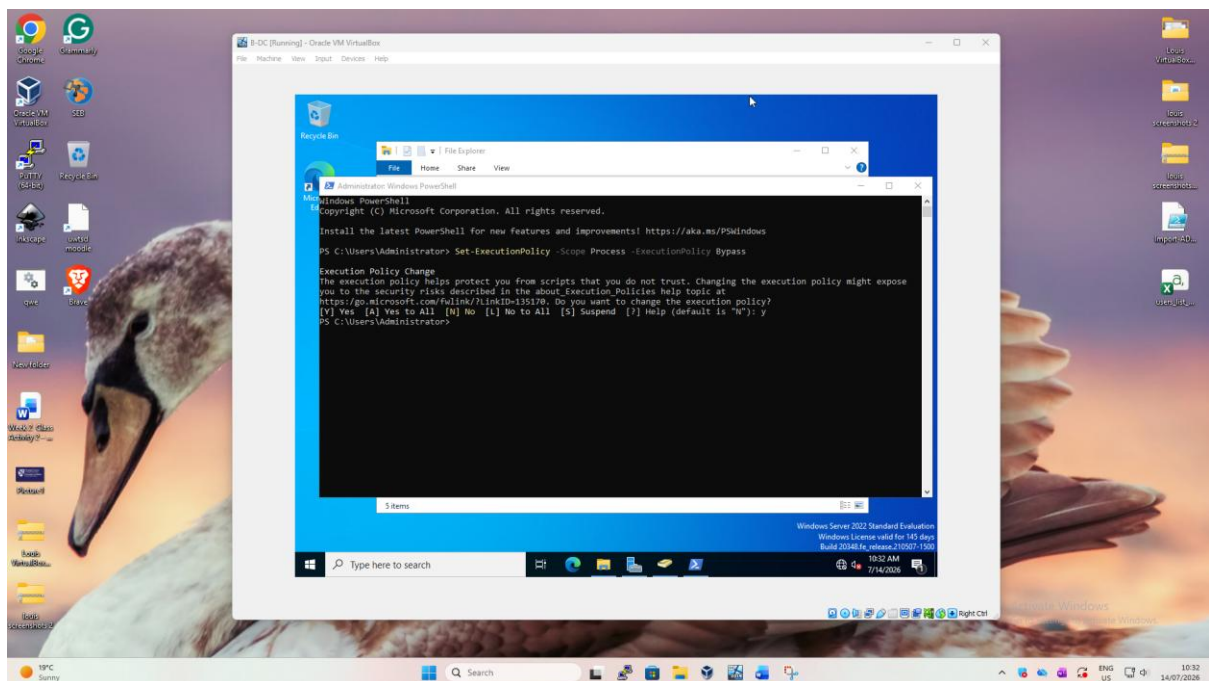


Figure 29 – Windows PowerShell opened with administrative privileges.

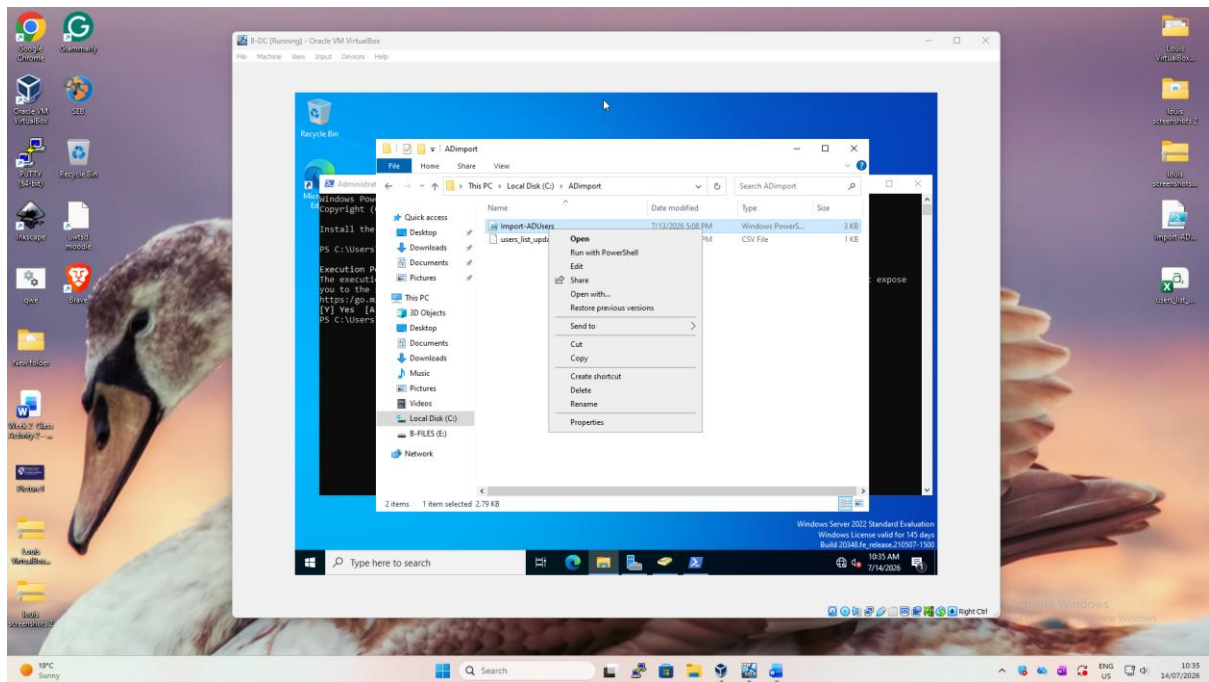


Figure 30 – Navigating to the folder containing the PowerShell import script.

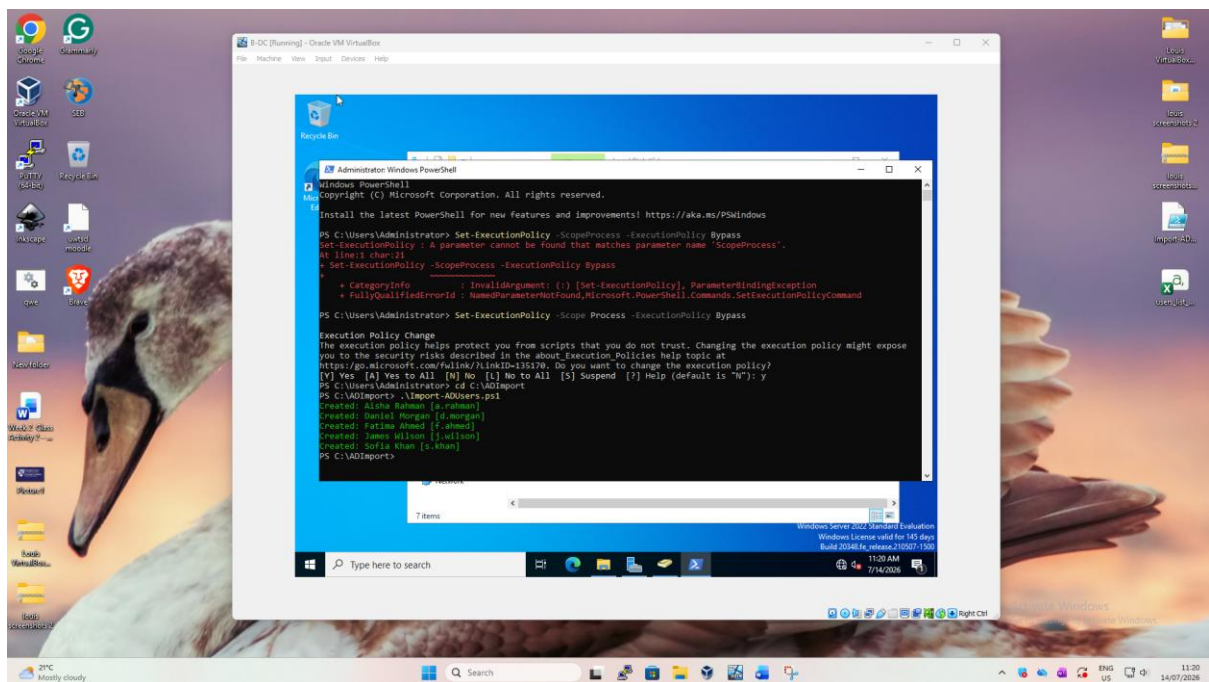


Figure 31 – Executing the PowerShell script to import Active Directory users.

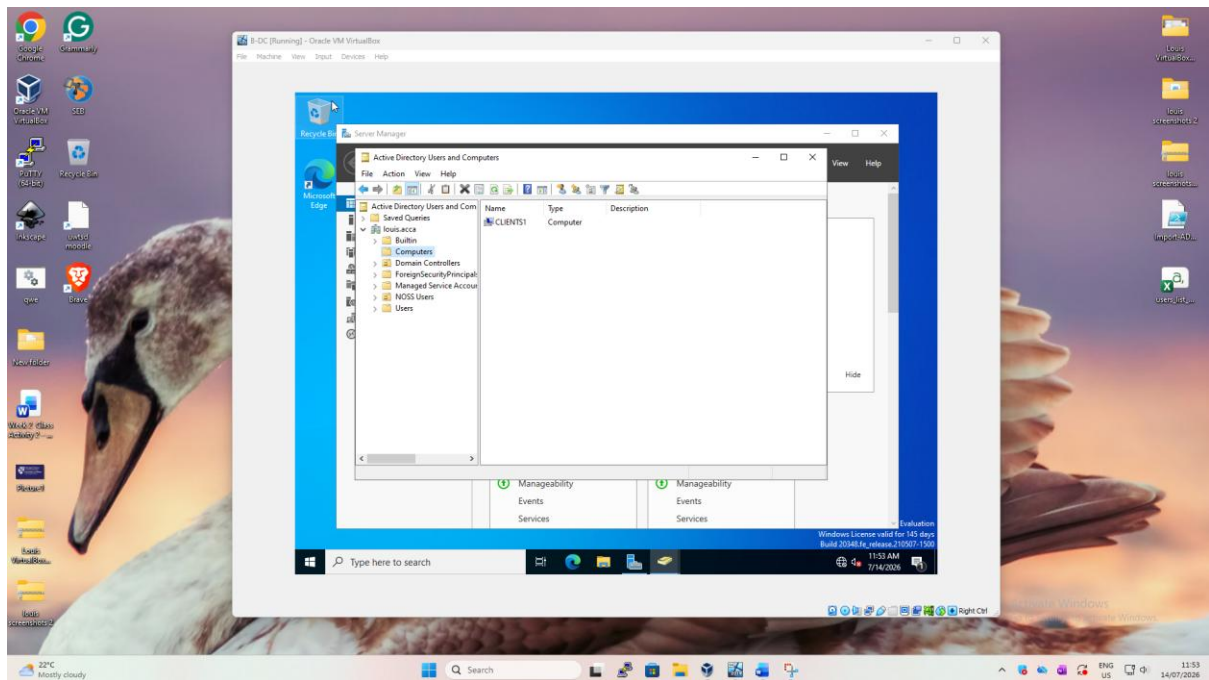


Figure 32 – Imported user accounts successfully displayed within the Clients organisational unit.

Reflection

Using PowerShell to automate user creation reduced manual effort and minimised the risk of configuration errors. Organising the accounts within an OU also simplified future administration.

7. Domain Membership

Objective

The objective of this task was to join client computers to the Active Directory domain to enable centralised authentication, management and access to enterprise network resources.

Configuration Completed

After Active Directory was configured, the client computers were joined to the domain using valid domain credentials (Microsoft, 2025b, Debian Project, 2025). The systems were restarted to complete the process, after which they successfully authenticated with the Domain Controller and appeared in Active Directory Users

and Computers. This confirmed that domain membership had been configured correctly and that the clients were ready for centralised management.

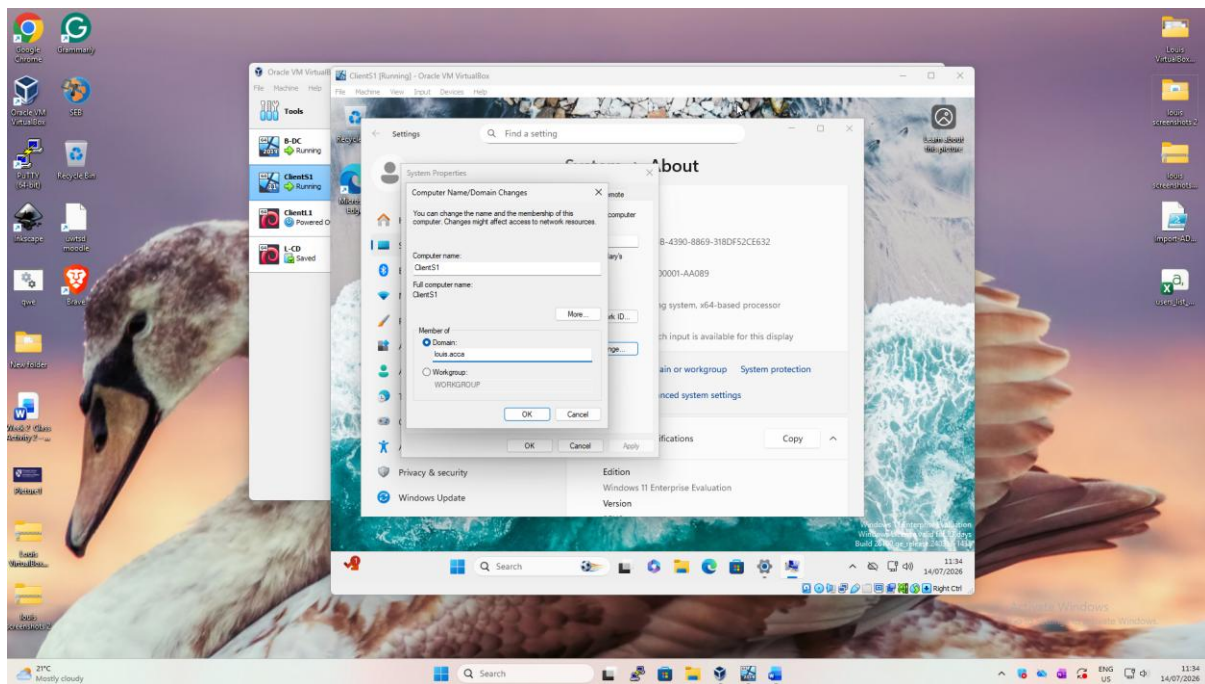


Figure 33 – Joining ClientS1 to the Active Directory domain.

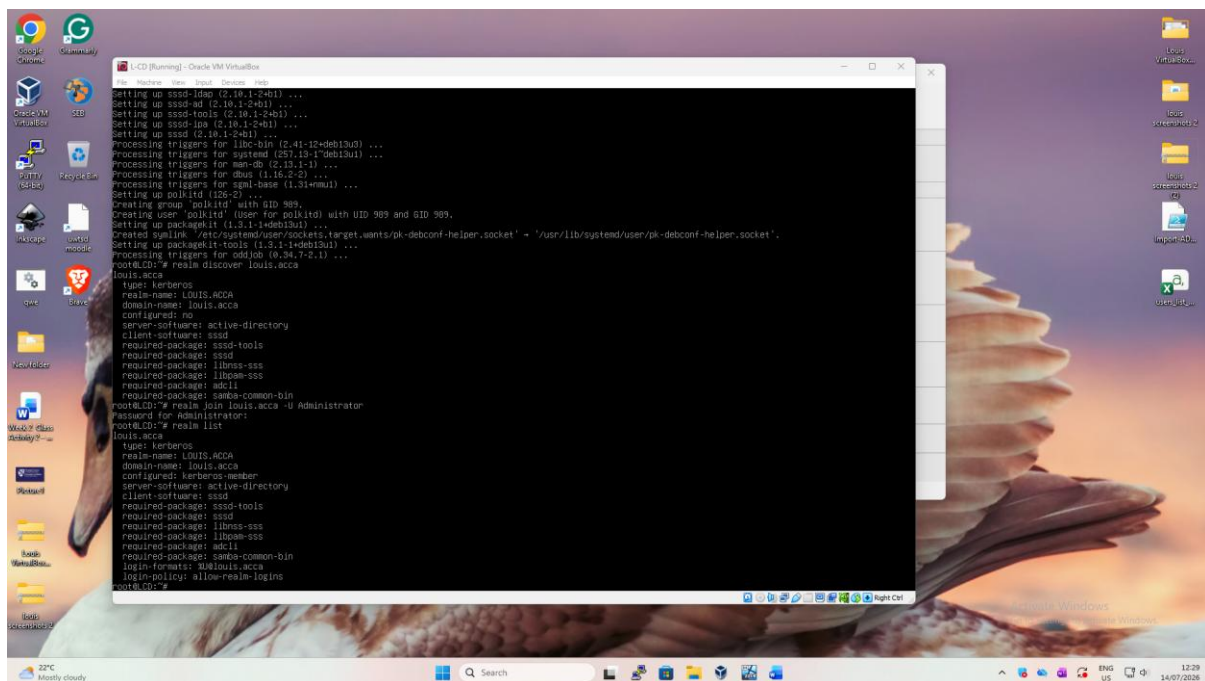


Figure 34 – Joining ClientL1 to the Active Directory domain.

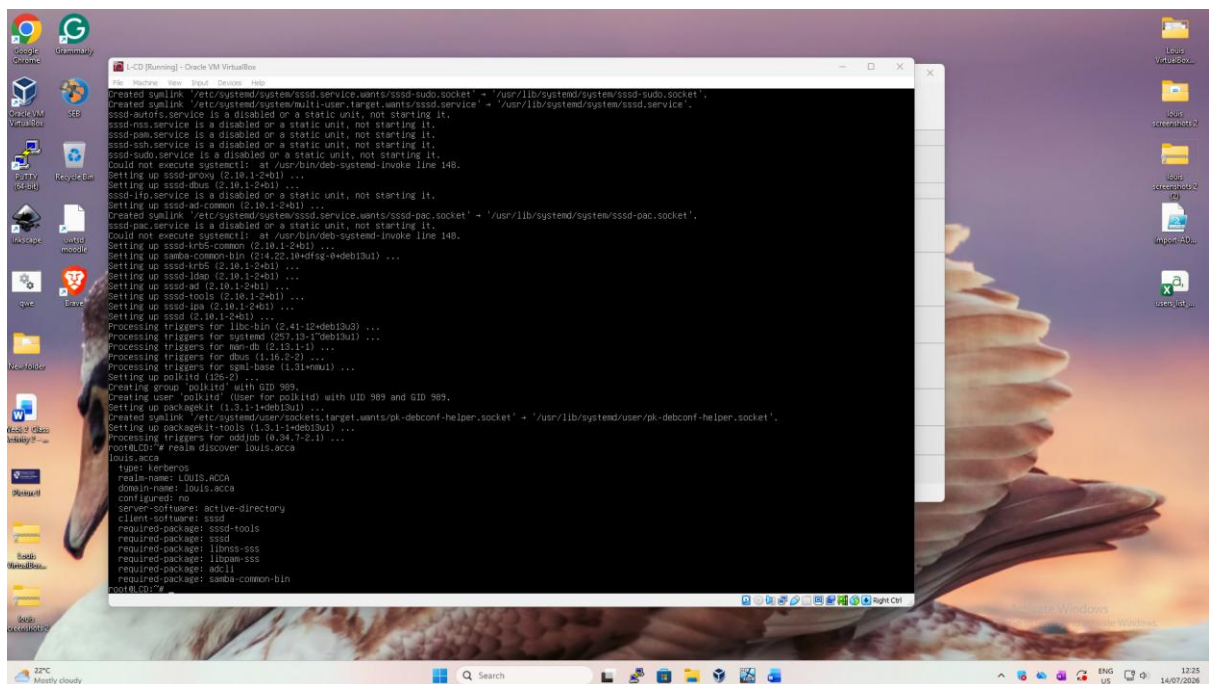


Figure 35 – Linux client successfully joined to the enterprise domain.

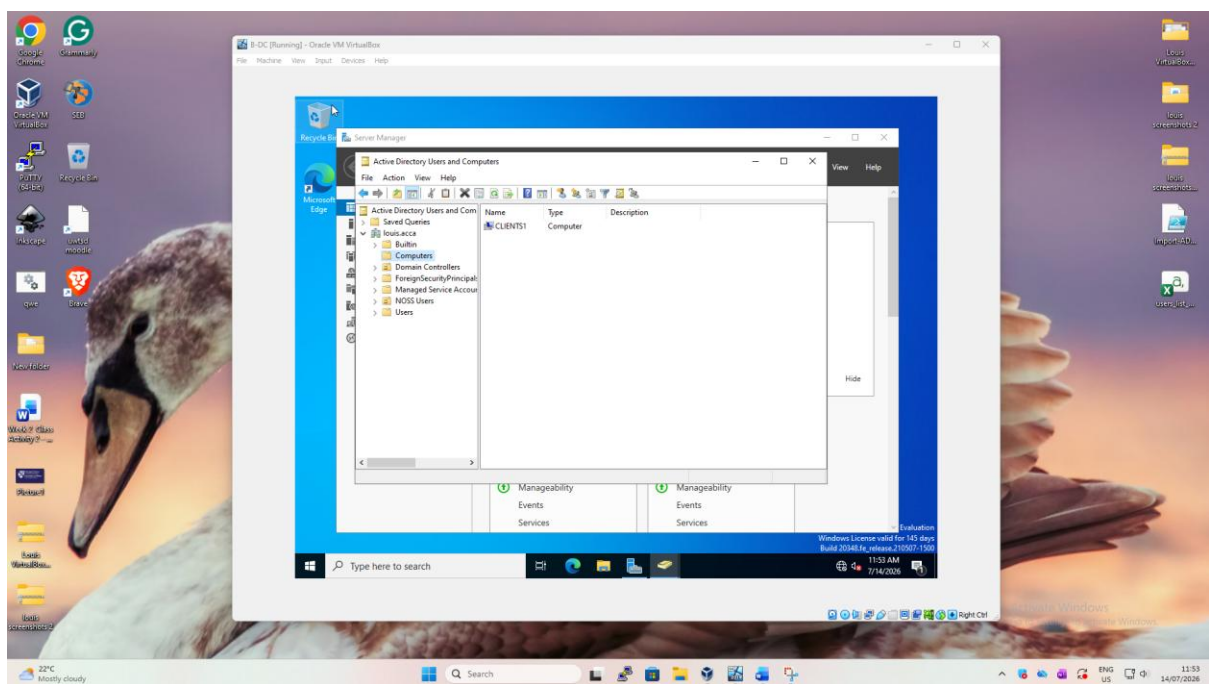


Figure 36 – Active Directory Users and Computers displaying the joined client devices. (Lost screenshot apologies)

Reflection

Joining the client computers to the domain enabled centralised authentication and administration. Successful domain membership also confirmed that Active Directory and DNS were functioning correctly.

8. DHCP

Objective

The objective of this task was to configure DHCP to automatically assign IP addresses and network settings to client devices, reducing manual configuration and improving network management.

Configuration Performed

The DHCP Server role was installed and authorised within Active Directory (Microsoft, 2025e). An IPv4 scope was then created by defining the network range, subnet mask, lease duration and excluded addresses. Scope options including the default gateway and DNS server were configured to provide clients with the required network settings automatically. Successful IP address allocation confirmed that the DHCP service was operating correctly.

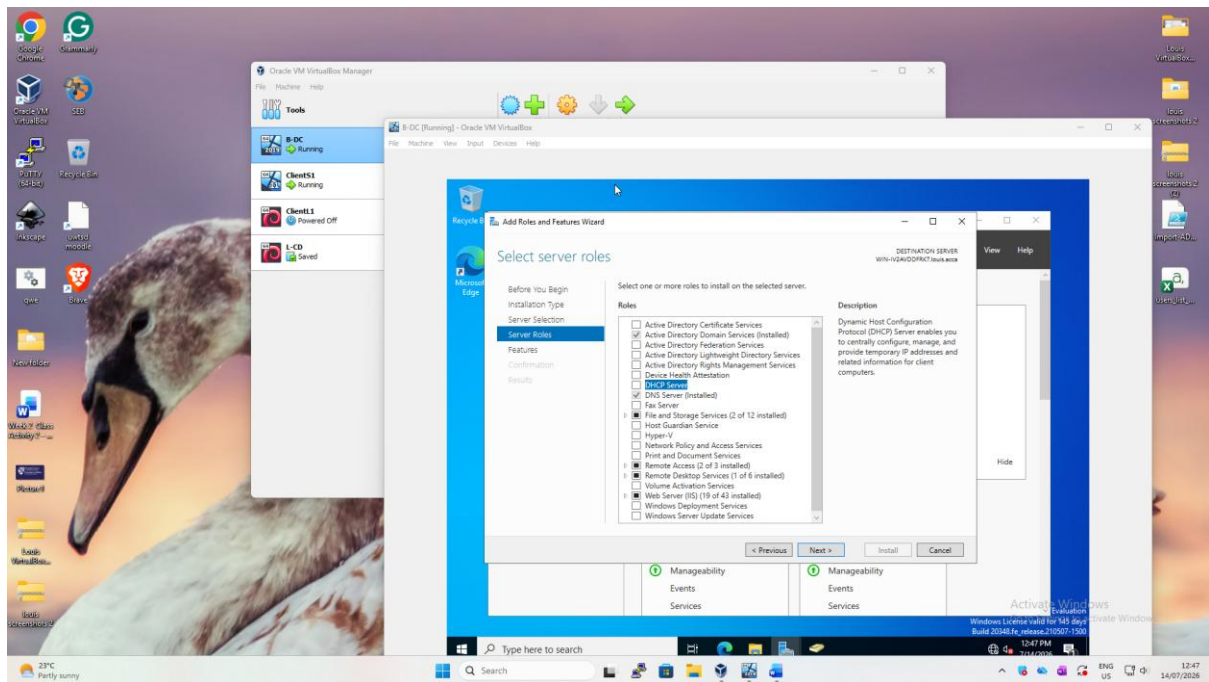


Figure 37 – Installing DHCP through Server Manager.

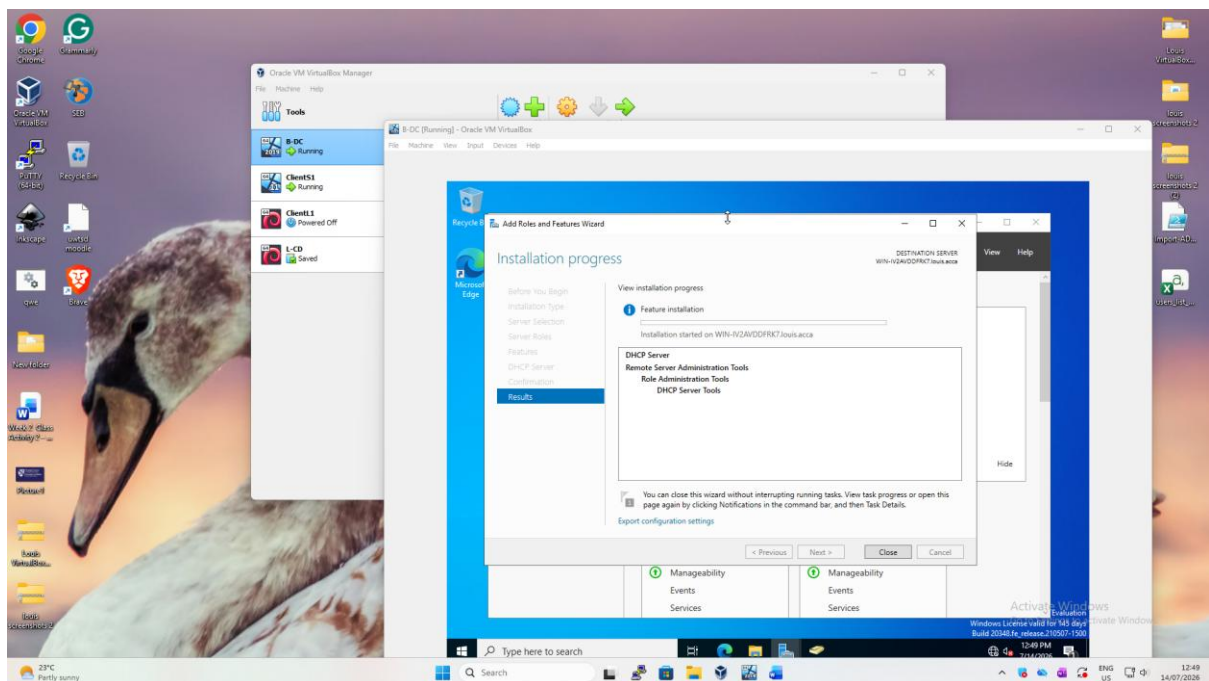


Figure 38 – Completing DHCP post-installation configuration.

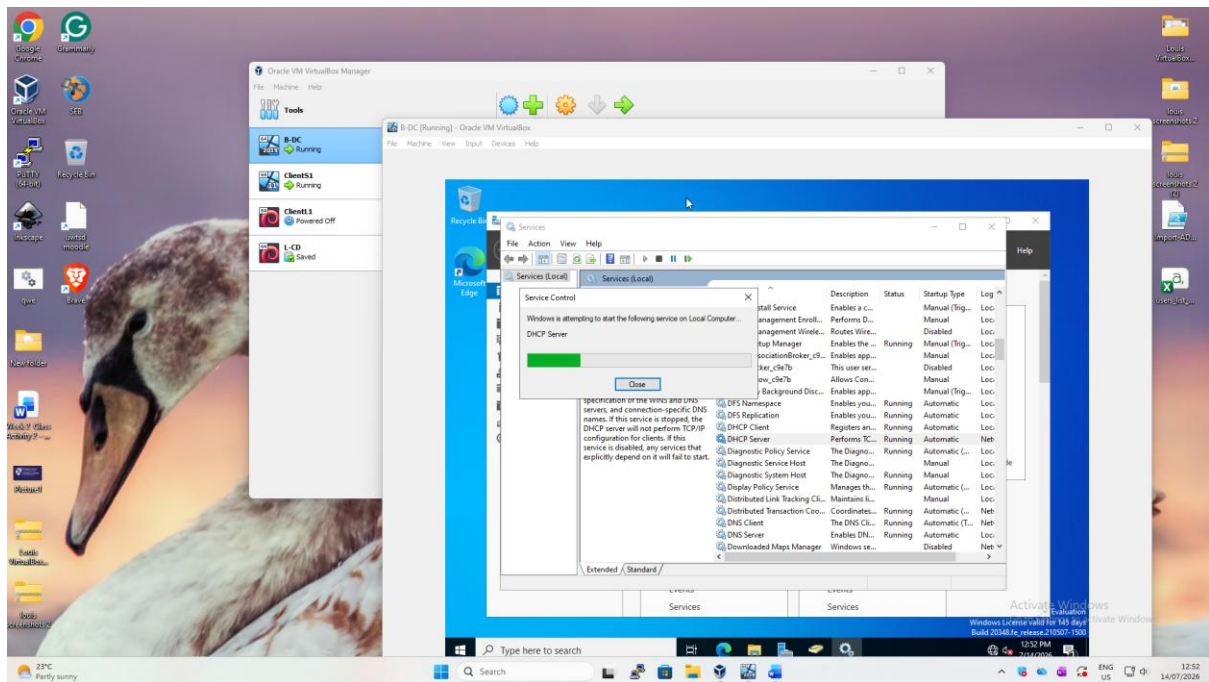


Figure 39 – Verifying DHCP server is authorised.

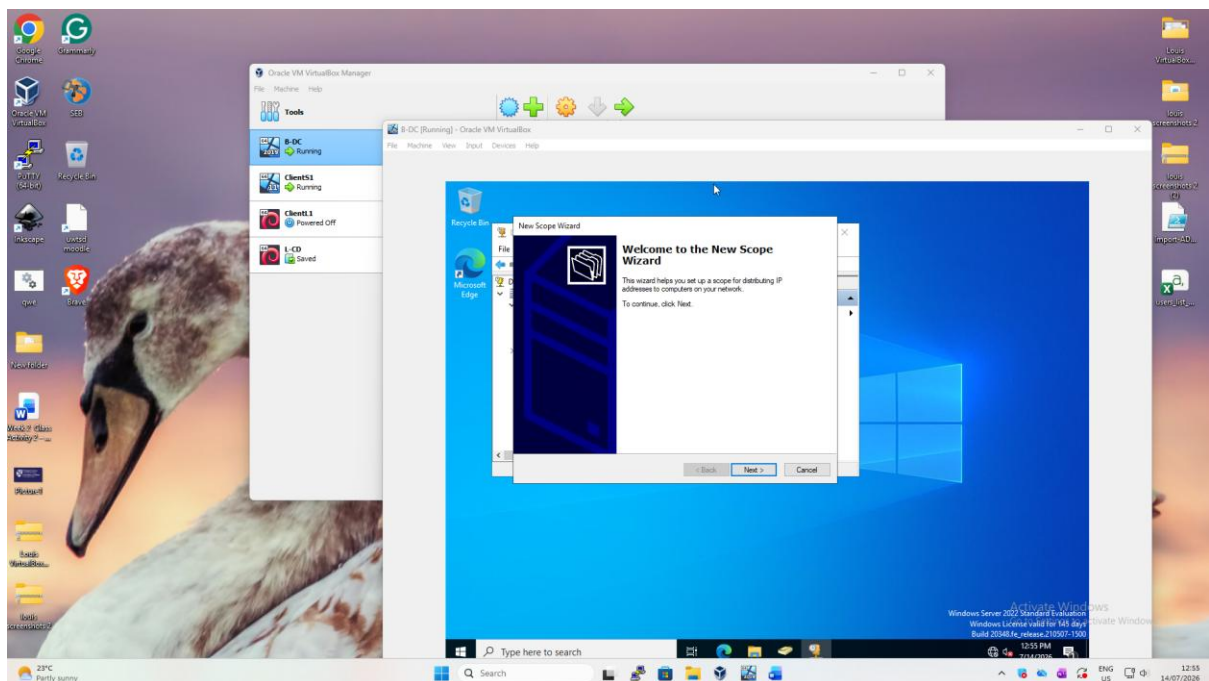


Figure 40 – Creating the Birmingham DHCP scope.

Reflection

Configuring DHCP automated IP address allocation, reduced the risk of manual configuration errors and ensured consistent network settings across client devices.

9. Connectivity Testing

Objective

The objective of this task was to verify network communication, domain authentication and name resolution following the completion of the server and client configurations.

Tests Performed

Network connectivity was verified using standard Windows and Linux commands. The **ping** command confirmed successful communication between devices, while **nslookup** verified that DNS was resolving hostnames correctly. The **whoami** command confirmed successful authentication against the Active Directory domain. On the Linux client, domain discovery and authentication were also verified following the Kerberos and domain join configuration. The successful test results confirmed that communication and authentication were functioning correctly throughout the enterprise environment.

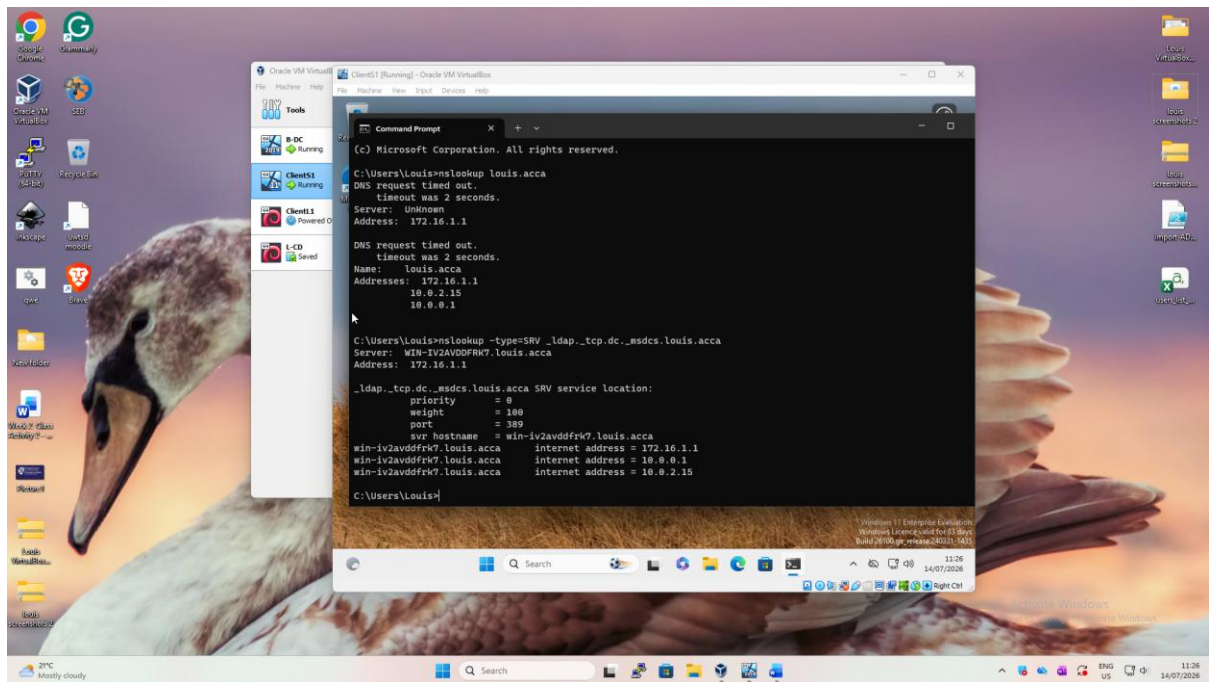


Figure 41 – Testing the domain and DNS records.

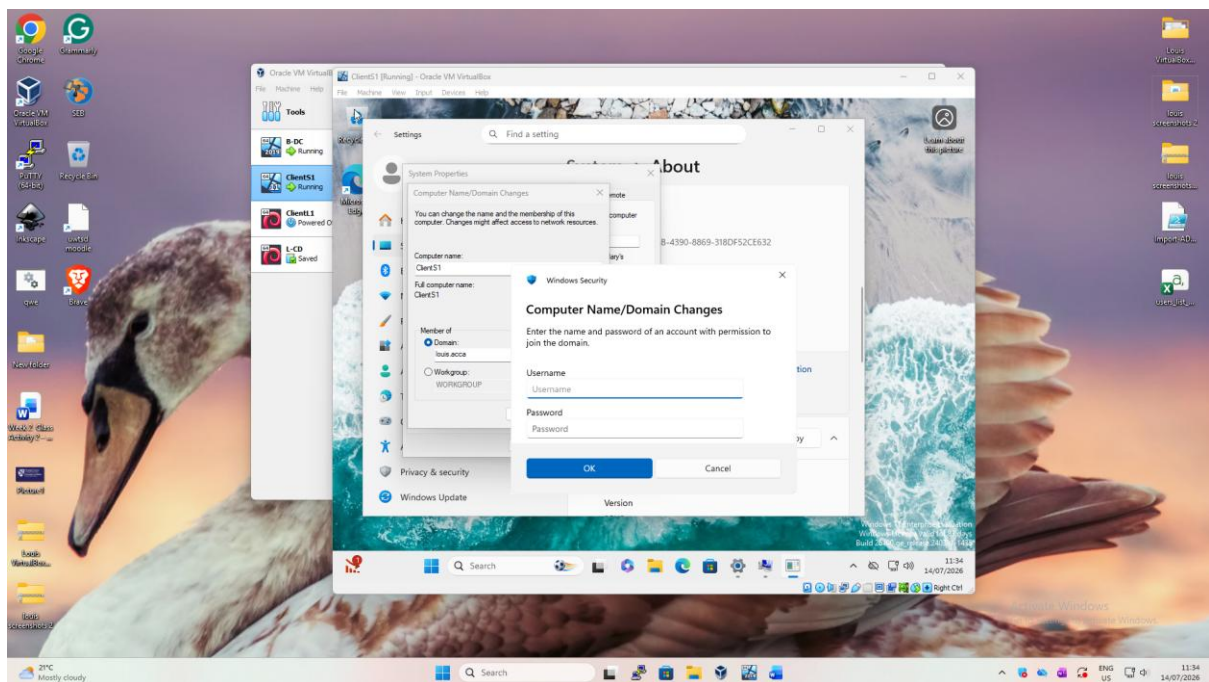


Figure 42 – Renaming the Windows client.

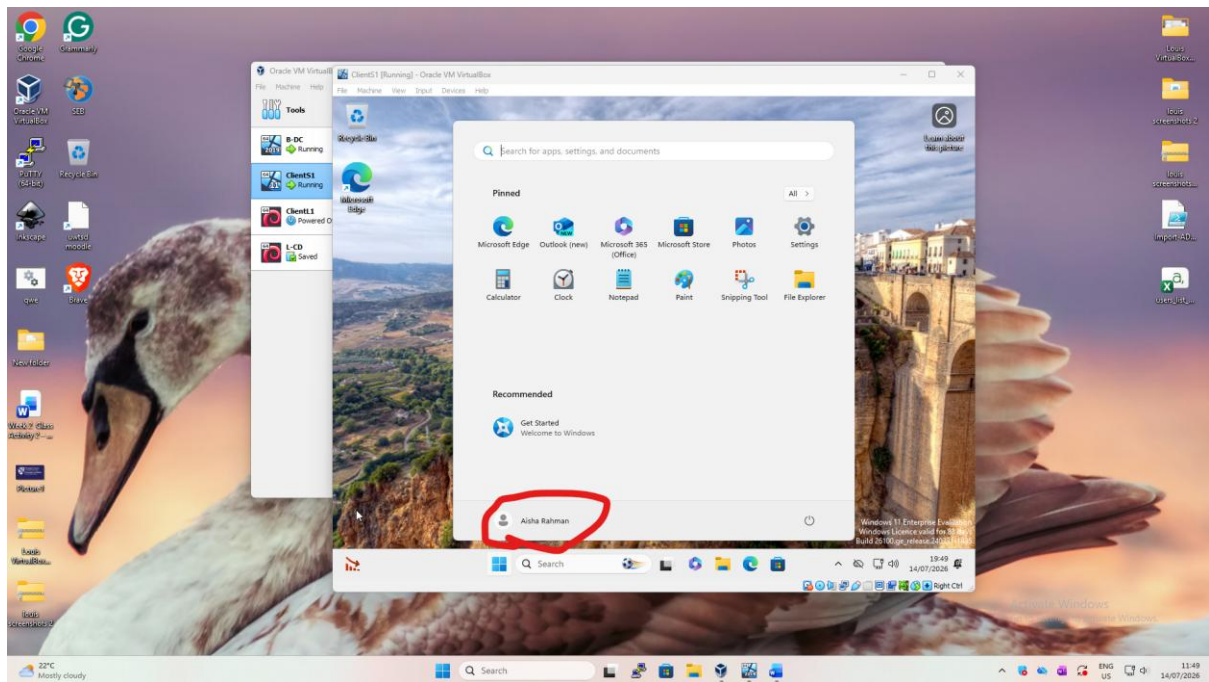


Figure 43 – Signed in using a domain account.

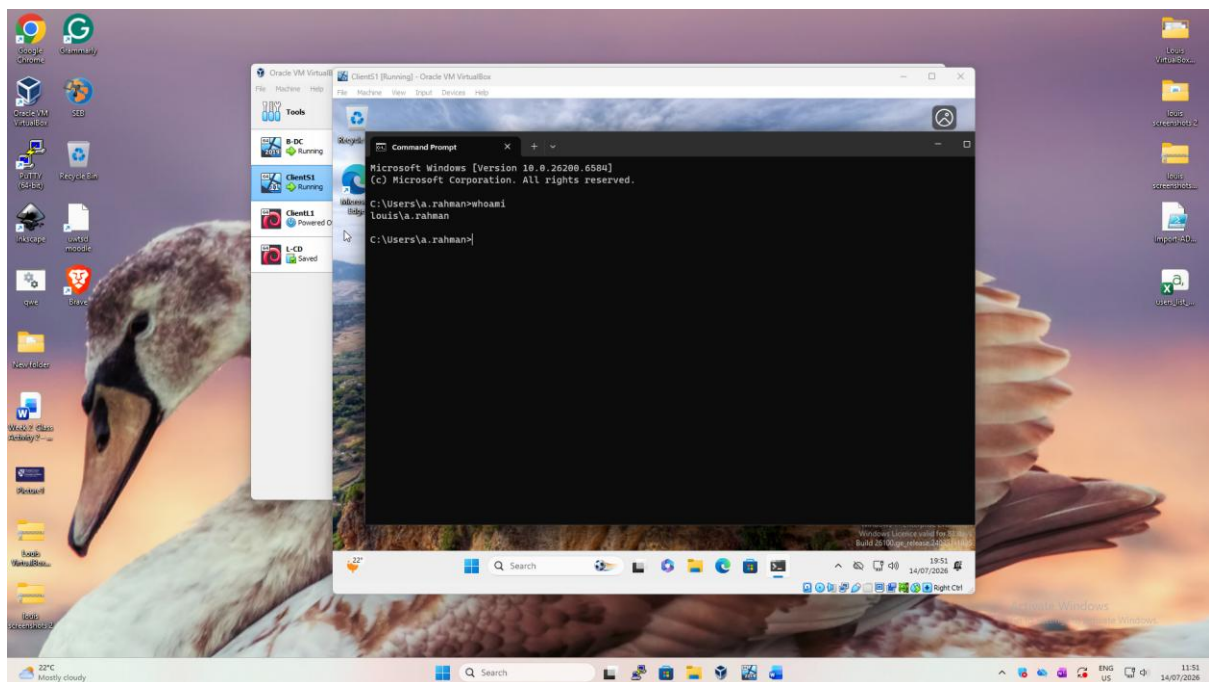


Figure 44 – whoami command output.

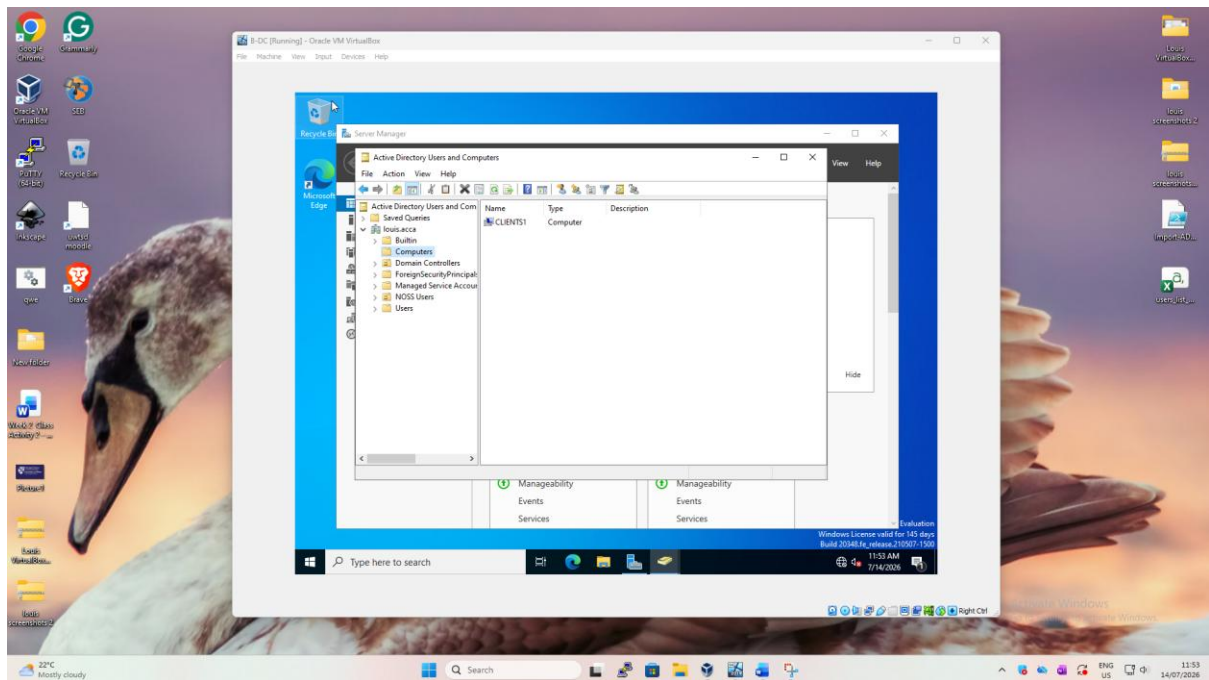


Figure 45 – Confirming Clients1 on the Domain Controller.

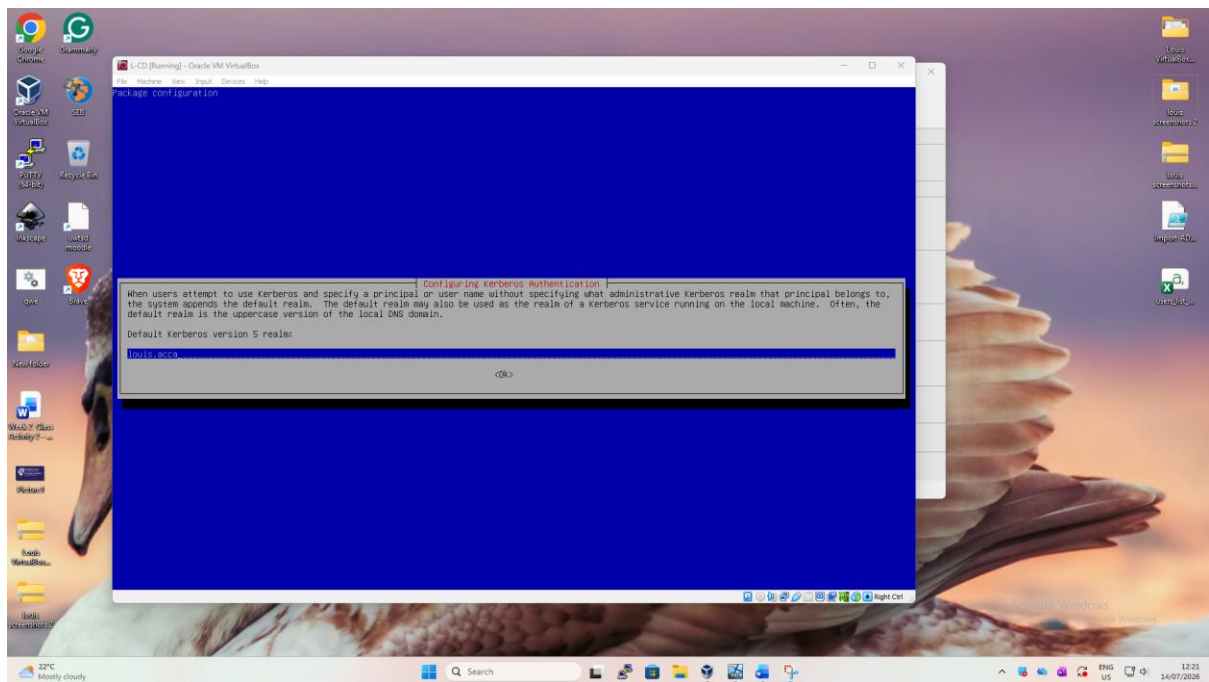


Figure 46 – Installing Kerberos.

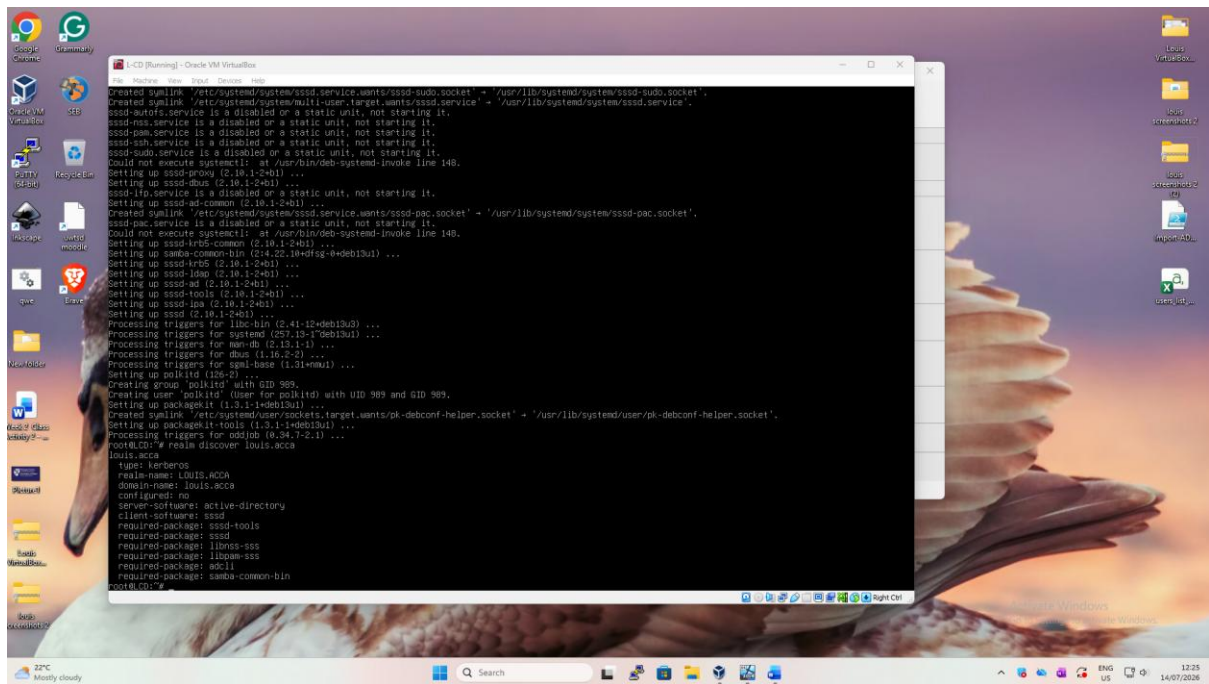


Figure 47 — Discover the domain command.

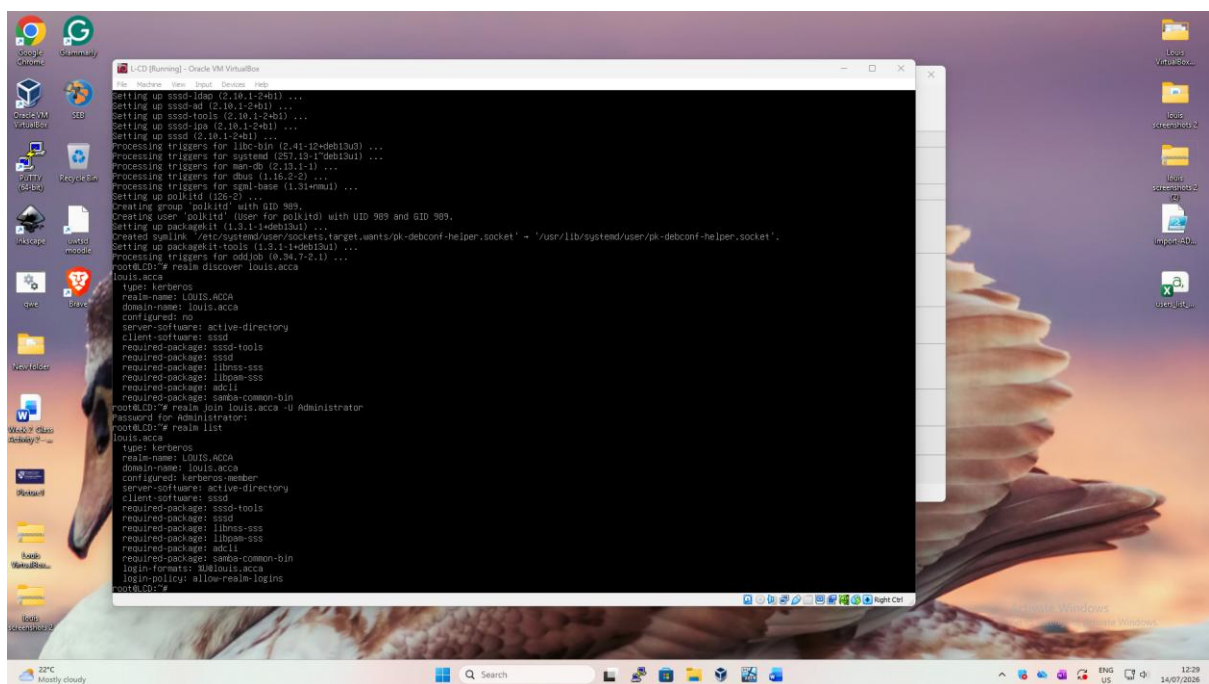


Figure 48 — Joining L-CD to the domain.

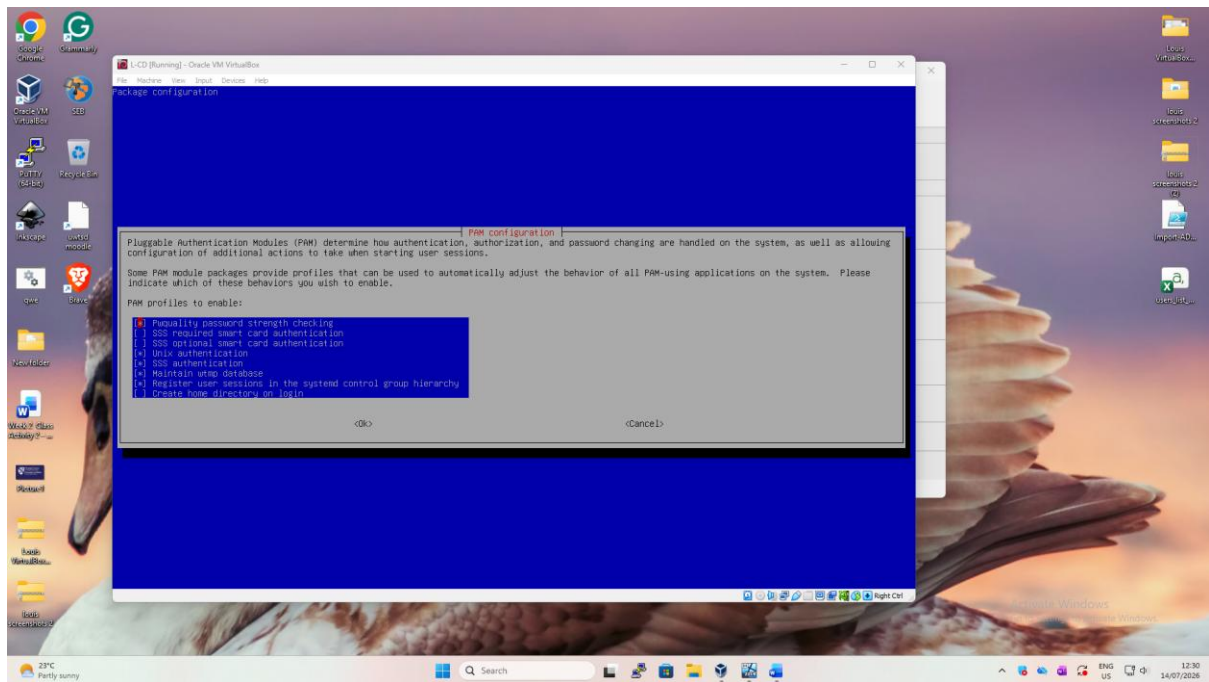


Figure 49 – Enabling automatic home directory creation.

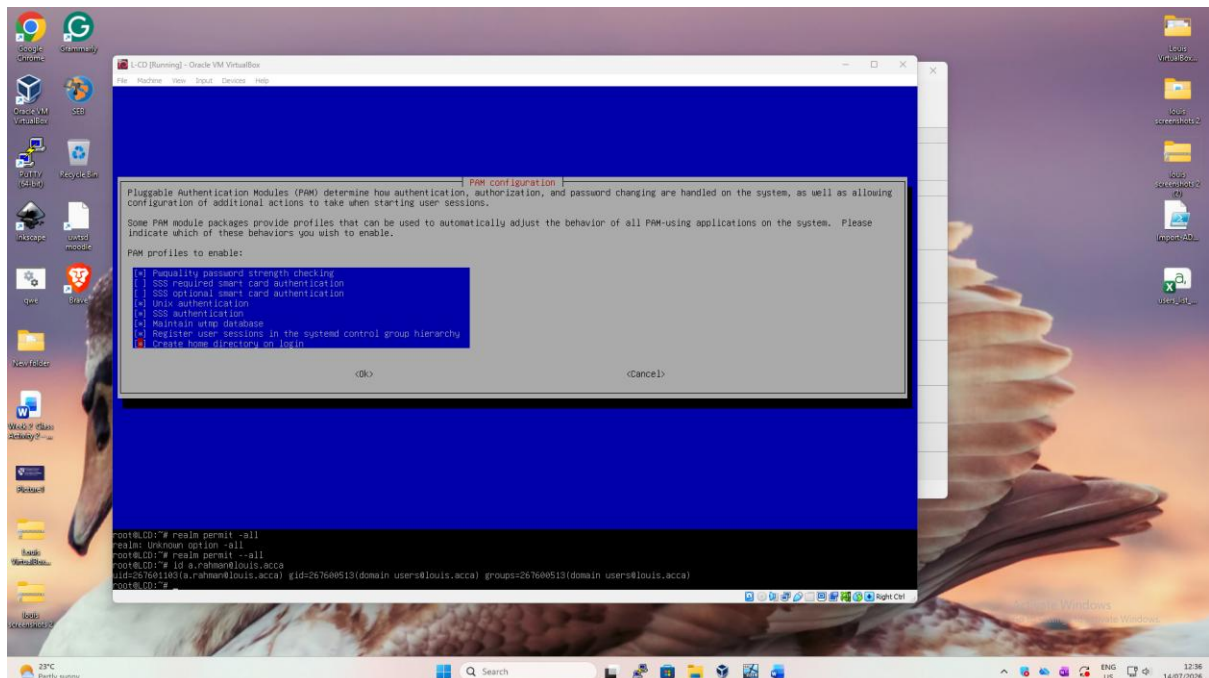


Figure 50 – Testing a domain user on L-CD.

Reflection

Connectivity testing confirmed that the enterprise network had been configured successfully. The results demonstrated that routing, DNS, Active Directory and domain authentication were operating correctly across both Windows and Linux systems.

10. Shared Folder

Objective

The objective of this task was to configure a shared folder that allowed authorised domain users to access shared files across the enterprise network.

Configuration Performed

A shared folder was created on the Windows Server using Disk Management, and the required directory was prepared for sharing. The configuration was verified to confirm that the shared folder had been created successfully and was available for use within the network environment (Microsoft, 2025e).

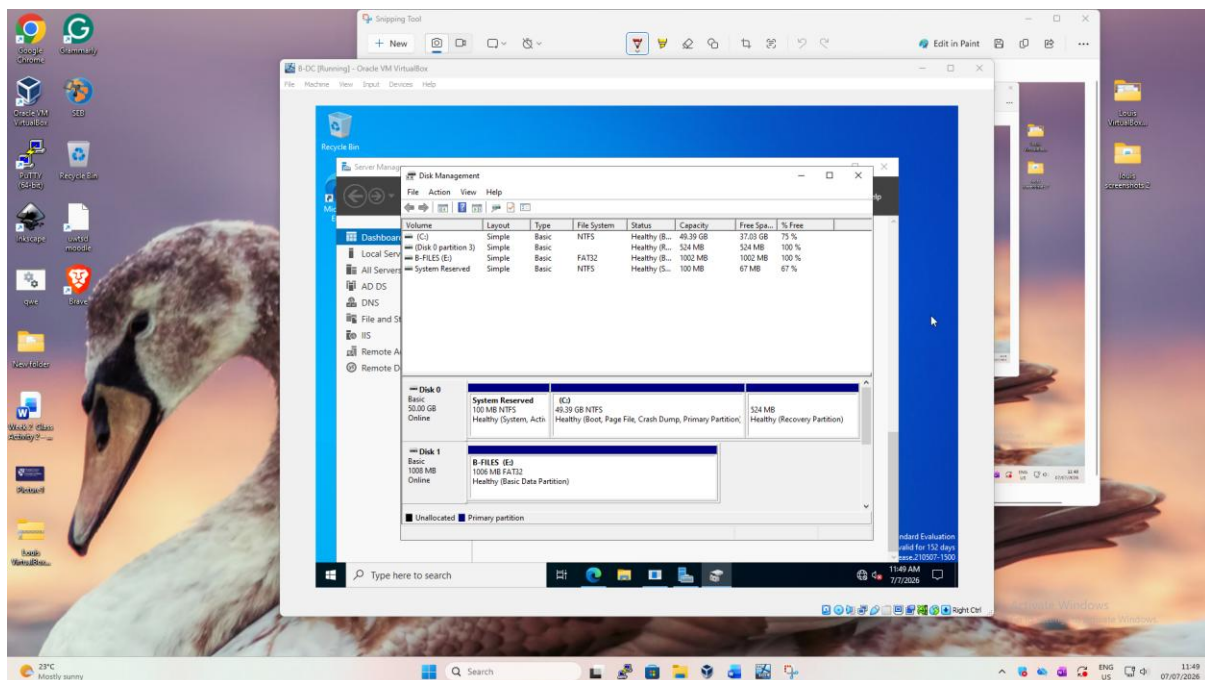


Figure 53 – Disk Management showing the additional storage volume.

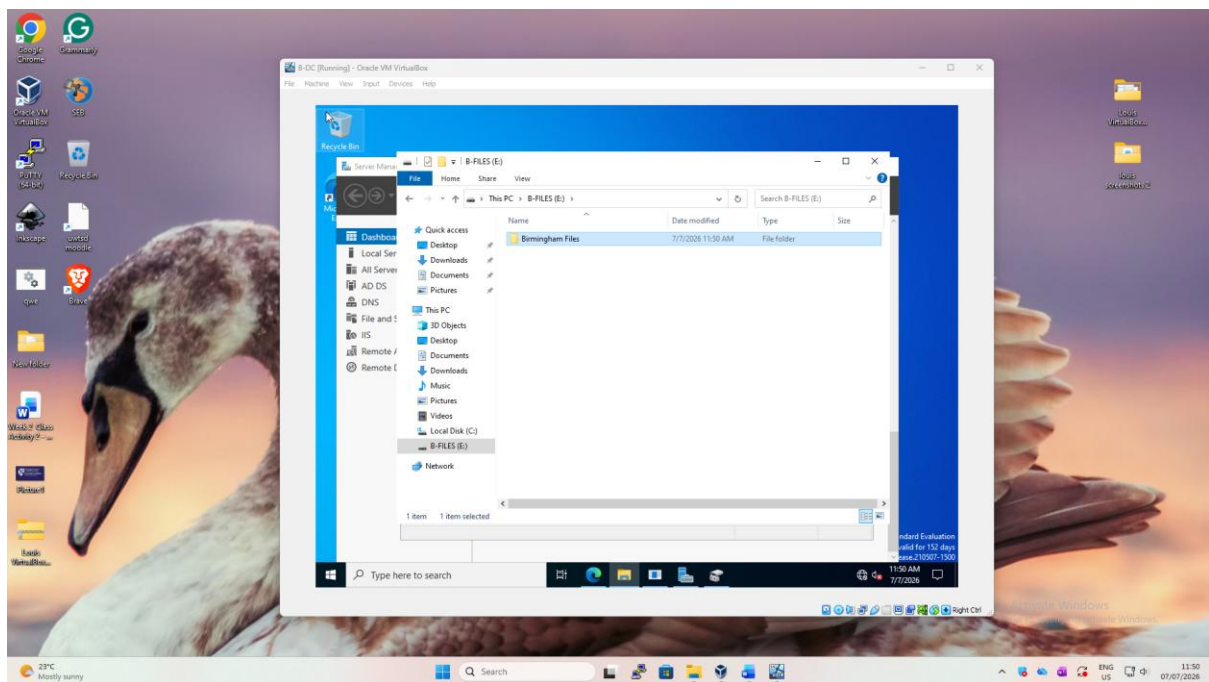


Figure 54 – Creation of the **BirminghamFiles** shared folder.

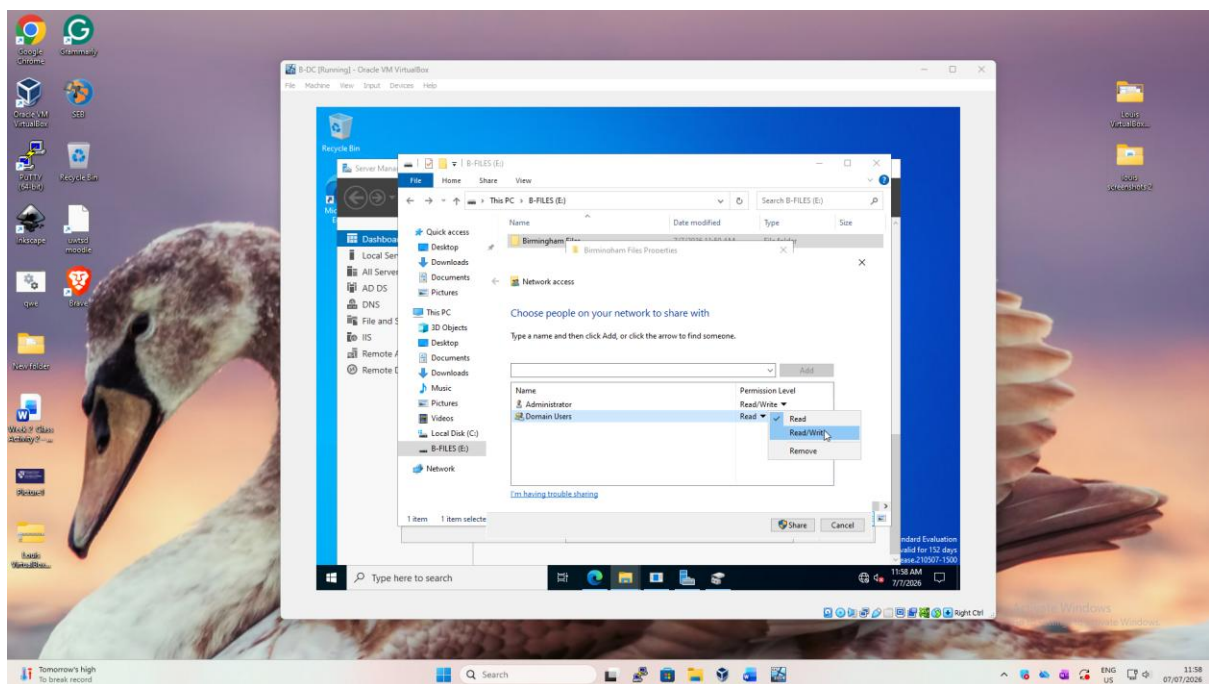


Figure 55 – Shared folder configuration

Reflection

Creating a shared folder provided a central location for storing and managing files within the network. This demonstrated the initial configuration required for shared network resources and prepared the environment for future access by authorised users.

11. Internet Information Services (IIS)

Objective

The objective of this task was to configure Internet Information Services (IIS) to host the required enterprise website.

Configuration Completed

IIS was installed on the Windows Server and configured to host the required website (Microsoft, 2025f). The site was successfully accessed through a web browser, confirming that the web service was operating correctly.

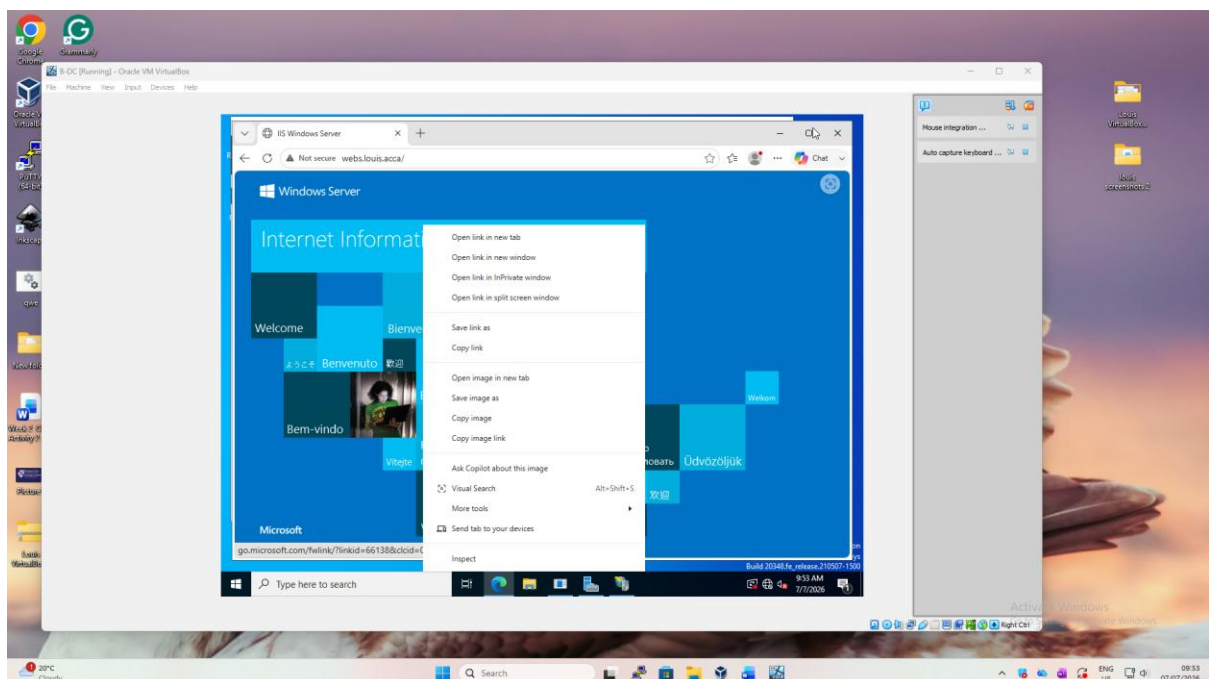


Figure 56 – Internet Information Services (IIS) website successfully displayed in a web browser.

Reflection

Configuring IIS demonstrated the deployment of web services within the enterprise environment and confirmed successful website hosting.

12. Remote Desktop Services (RDS)

Objective

The objective of this task was to configure Remote Desktop Services to allow authorised users to securely access enterprise resources through a web interface.

Configuration Completed

Remote Desktop Services was configured on the Windows Server and the RD Web Access portal was successfully accessed through a web browser. The login page confirmed that the service was installed and available for authenticated users.

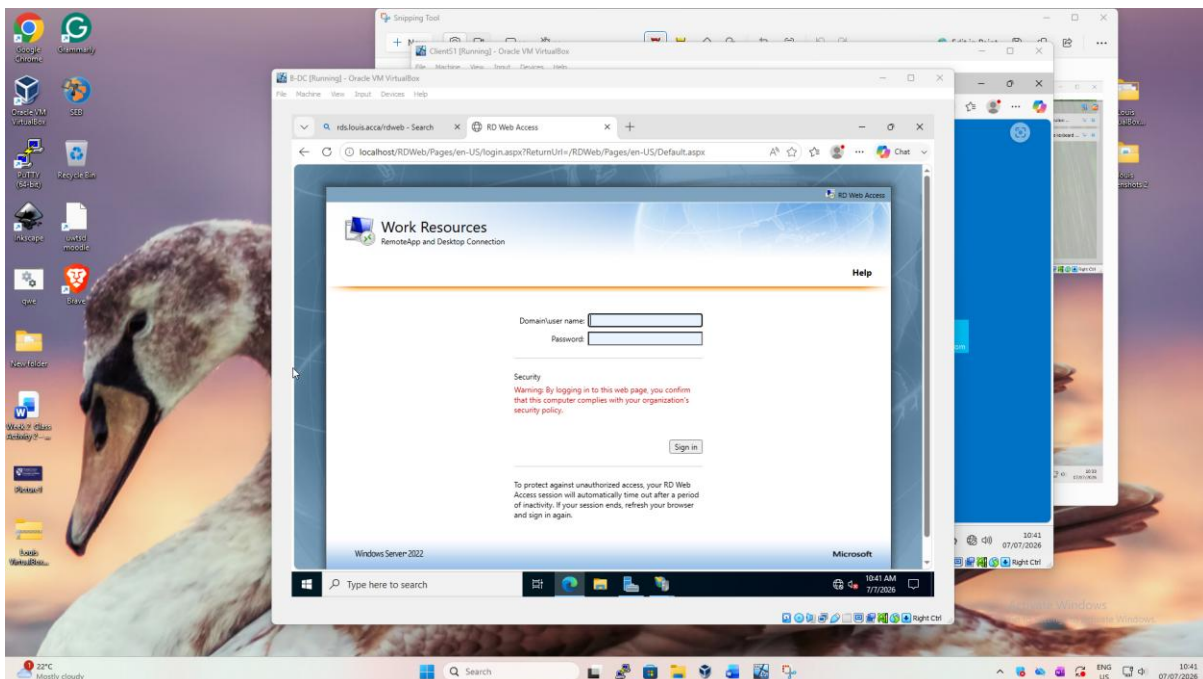


Figure 57 – Remote Desktop Services (RD Web Access) login page displayed successfully.

13. Troubleshooting

Objective

The objective of this task was to identify and resolve configuration issues encountered during the implementation of the enterprise network to ensure all services operated correctly.

Issue 1 – Client Unable to Join the Domain

Issue

A client computer was initially unable to join the Active Directory domain.

Cause

The client configuration required verification to ensure that it could locate the Domain Controller and communicate with the domain services.

Solution

The client configuration was checked, DNS functionality was verified and the computer was joined to the domain using valid domain credentials. After restarting the client, the domain membership was confirmed.

Result

The client successfully joined the domain and authenticated using a domain account.

Issue 2 – User Account Verification

Issue

It was necessary to confirm that imported users had been created correctly.

Cause

Bulk user creation required verification to ensure that the PowerShell script completed successfully.

Solution

The imported accounts were checked in Active Directory Users and Computers, and logon testing was carried out using a domain account.

Result

The users were successfully created and authenticated using the Active Directory domain.

Issue 3 – DHCP Configuration

Issue

The DHCP service required configuration before client computers could receive automatic IP addressing.

Cause

The DHCP role must be installed, authorised and configured before it can issue leases.

Solution

The DHCP Server role was installed, post-installation tasks were completed, the server was authorised and the Birmingham scope was created.

Result

The DHCP server was successfully configured and ready to allocate IP addresses automatically.

Reflection

Throughout the project, troubleshooting was an essential part of configuring a reliable enterprise network. Testing each service after configuration helped identify issues early and ensured that Active Directory, DNS, DHCP and domain authentication operated correctly before additional services were implemented. Working through these issues improved my understanding of how different network services depend on one another and reinforced the importance of systematic testing during enterprise network deployment.

14. Conclusion

In my project i successfully demonstrated the configuration and management of a virtual enterprise network using Windows Server 2022 and Debian Linux. Core services, including Active Directory Domain Services (AD DS), DNS, DHCP, routing, domain membership and automated user account creation, were implemented to support communication between servers and client devices.

The completed network provided centralised authentication, automated IP address allocation and reliable name resolution for both Windows and Linux clients. Connectivity testing confirmed that the deployed services operated together successfully within the enterprise environment.

Completing this project strengthened my practical understanding a little more on enterprise networking, particularly the relationship between Active Directory, DNS and DHCP but there is still plenty more room for improvement. It also reinforced the importance of careful planning, configuration and troubleshooting when deploying network services.

15. References

Debian Project (2025) *Debian Documentation*. Available at:

<https://www.debian.org/doc/>

Microsoft (2025a) *Windows Server documentation*. Microsoft Learn. Available at:

<https://learn.microsoft.com/windows-server/>

Microsoft (2025b) *Active Directory Domain Services overview*. Microsoft Learn.

Available at: <https://learn.microsoft.com/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

Microsoft (2025c) *DNS and Active Directory Domain Services*. Microsoft Learn.

Available at: <https://learn.microsoft.com/windows-server/identity/ad-ds/plan/dns-and-ad-ds>

Microsoft (2025d) *Introduction to Active Directory Domain Services*. Microsoft Learn.

Available at: <https://learn.microsoft.com/training/modules/introduction-to-ad-ds/>

Microsoft (2025e) *Windows Server Networking*. Microsoft Learn. Available at:

<https://learn.microsoft.com/windows-server/>

Microsoft (2025f) *Internet Information Services (IIS) documentation*. Microsoft Learn.

Available at: <https://learn.microsoft.com/iis/>

Microsoft (2025g) *Remote Desktop Services overview*. Microsoft Learn. Available at:

<https://learn.microsoft.com/windows-server/remote/remote-desktop-services/overview>