

Component 2

Module Name: Network Operating Systems
and Services

Module Code: ACCA5023_BIRM

Student Name: Alexandru Emilian Ciorascu

Student ID: 2436639

Lecturer Name: Md Abrar Jahin Almazi Bapon

Contents

Introduction	4
1.1 Project Background	4
1.2 Project Objectives	4
1. Routing Configuration	5
1.1 Routing in Birmingham Network	5
1.2 Routing in London Network	5
1.3 ICMP Firewall Configuration	5
1.4 Routing Validation	6
2. Domain Controller and DNS Services	6
2.1 Forest Creation	6
2.2 DNS Records	6
2.3 Reverse Lookup Zone	7
2.4 Password Policy	7
3. VPN Deployment	7
3.1 VPN Configuration	7
3.2 VPN Validation	8
4. User Account Management	8
4.1 User Creation	8
5. Domain	8
5.1 Windows Domain	8
5.2 Linux Domain	9
6. DHCP Deployment	9
6.1 DHCP Scope Configuration	9
6.2 DHCP Relay Configuration	10
6.3 Validation	10
7. Network Testing and Troubleshooting	10
7.1 Connectivity Testing	10

7.2 DNS Validation.....	11
7.3 Troubleshooting Activities.....	11
8. Shared Storage Configuration.....	11
8.1 Disk Deployment.....	12
9. IIS Web Server Deployment	12
9.1 Website Configuration	12
10. Remote Desktop Services	12
11. Security Measures	13
11.1 Password Security	13
11.2 VPN Encryption	13
12. Testing Summary	14
13. Conclusion	14
References	15
Appendix.....	16

Introduction

1.1 Project Background

The NOSSLONDON2026 project was developed to simulate a realistic enterprise network environment consisting of two interconnected sites located in Birmingham and London. Coursework 2 builds upon the infrastructure designed and implemented in Coursework 1 by introducing essential network and server services required in a modern business environment. The practical implementation focuses on deploying centralised management, secure communications and resource sharing services within a virtualised infrastructure to support organisational operations efficiently [1], [2].

1.2 Project Objectives

The main objective of this project was to configure and validate a range of enterprise network services across both locations. These services included Routing and Remote Access Services (RRAS), Active Directory Domain Services (AD DS), DNS, DHCP, VPN connectivity, file sharing, IIS web services and Remote Desktop Services. Additional objectives involved integrating client devices into the Active Directory domain, implementing security controls such as password policies and authenticated access, and performing comprehensive connectivity testing. The completed infrastructure was designed to provide secure communication, centralised administration and reliable access to network resources for users located in both Birmingham and London [2], [3].

1. Routing Configuration

1.1 Routing in Birmingham Network

Routing and Remote Access Services (RRAS) were installed and configured on the Birmingham Domain Controller (B-DC) to enable communication between the Birmingham and London subnets. The RRAS role allows Windows Server to perform routing functions by forwarding packets between different network segments. After installation, the service was configured for LAN routing, enabling devices on separate networks to exchange traffic successfully. Implementing RRAS on B-DC provided the foundation for inter-site communication and supported the deployment of additional services such as DHCP, VPN connectivity, and domain-based resource access [2].

1.2 Routing in London Network

The Debian server deployed within the London site was configured to support routing by enabling persistent IP forwarding. System parameters were modified to ensure that packet forwarding remained active following reboots. Static routes were then configured to direct traffic towards the Birmingham network through the correct gateway. This implementation allowed systems located in London to communicate with servers and services hosted in Birmingham while maintaining stable inter-site connectivity [3].

1.3 ICMP Firewall Configuration

Windows Defender Firewall settings were modified to permit ICMP traffic across the network. Enabling ICMP Echo Requests allowed connectivity testing using tools such as Ping. This configuration simplified troubleshooting procedures and provided a reliable method for verifying communication between devices located on separate network segments. Allowing ICMP traffic also helped confirm that routing services were functioning correctly following implementation [3].

1.4 Routing Validation

Following configuration, network connectivity tests were performed to verify successful routing between both locations. Communication between devices in Birmingham and London confirmed that routing services, firewall configurations and forwarding settings were operating correctly. The successful completion of these tests demonstrated that the infrastructure was ready to support the additional enterprise services required by the coursework objectives [2], [3].

2. Domain Controller and DNS Services

The Birmingham Domain Controller (B-DC) was configured as the central authentication and management server for the enterprise infrastructure. Active Directory Domain Services (AD DS) and DNS were deployed to provide centralised authentication, user management and name resolution across both the Birmingham and London networks [5].

2.1 Forest Creation

A new Active Directory forest named alexandru.acca was created on B-DC. The domain provides a central management structure for users, computers and network services. Establishing the forest enabled domain-based authentication and provided the foundation for implementing, DNS integration and resource management across the infrastructure [5].

2.2 DNS Records

A Forward Lookup Zone was configured for the alexandru.acca domain. Appropriate records were created for infrastructure devices and services located in Birmingham and

London. These records allow systems to locate resources using hostnames rather than IP addresses, improving usability and simplifying administration [6].

2.3 Reverse Lookup Zone

A Reverse Lookup Zone was configured to support IP to hostname resolution. PTR records were created for the required hosts, enabling reverse DNS lookups and improving network troubleshooting capabilities. This configuration assists administrators when diagnosing connectivity and name resolution issues [5].

2.4 Password Policy

A secure password policy was implemented using Group Policy Management. Password complexity requirements, password history and minimum password length settings were configured to improve the security of domain user accounts.

3. VPN Deployment

3.1 VPN Configuration

A Virtual Private Network (VPN) was configured to establish a secure connection between the Birmingham and London networks. The VPN enables data to be transmitted securely between both locations by encrypting traffic travelling across the network. This implementation allows users and systems located at either site to access centralised services while maintaining confidentiality and integrity of communications. The VPN infrastructure was integrated with the existing routing configuration to provide connectivity between both subnets and ensure reliable communication across the enterprise environment [7].

3.2 VPN Validation

Following deployment, connectivity tests were performed to verify that the VPN tunnel was functioning correctly. Communication between devices located in Birmingham and London confirmed that traffic was successfully traversing the secure tunnel. The validation process demonstrated that the VPN configuration provided stable intersite connectivity and supported access to domain services, DNS, DHCP and shared resources. The successful implementation of the VPN enhanced the overall security of the infrastructure while ensuring continuous communication between both locations [4], [7].

4. User Account Management

4.1 User Creation

User accounts were created within the alexandru.acca domain to provide authentication and access to network resources. To comply with the coursework requirements, a standard naming convention was implemented using the first letter of the user first name.

5. Domain

5.1 Windows Domain

The Windows client system, ClientS1 was successfully joined to the alexandru.acca domain. Joining the domain enabled the workstation to authenticate users through Active Directory rather than relying on local accounts. This configuration allowed centralised management of user access, security policies and network resources [5].

5.2 Linux Domain

The Linux systems, including ClientL1 and L-CD, were integrated with the alexandru.acca domain to ensure consistent authentication across the enterprise environment. Domain integration enabled Linux users to authenticate using Active Directory credentials while continuing access to network resources hosted across both locations. The successful domain join demonstrated interoperability between Windows and Linux systems and ensured that all devices could participate within the centrally managed infrastructure [4], [7].

6. DHCP Deployment

The Dynamic Host Configuration Protocol (DHCP) service was deployed on the Birmingham Domain Controller (B-DC) to provide centralised and automated IP address allocation throughout the infrastructure. Using DHCP eliminated the need to configure network settings on each client device manually and ensured consistent network configuration across both the Birmingham and London sites. The implementation provided clients with IP addresses, subnet masks, default gateways and DNS settings automatically, improving administrative efficiency and reducing the risk of configuration errors [4].

6.1 DHCP Scope Configuration

Separate DHCP scopes were created to support the Birmingham and London networks. Each scope was configured with an address range that complied with the coursework requirements, allowing devices to obtain IP addresses dynamically within their respective subnets. Additional scope options were configured to automatically distribute gateway and DNS server information. Centralised scope management simplified administration and ensured that all clients received the correct network settings when connecting to the infrastructure [4], [6].

6.2 DHCP Relay Configuration

Because the DHCP server was in Birmingham, the Debian server (L-CD) was configured as a DHCP Relay for the London network. The relay service forwards DHCP requests from London clients to the DHCP server on B-DC and returns the assigned configuration information to requesting devices. This approach enabled a single DHCP server to support both locations without requiring additional DHCP infrastructure.

6.3 Validation

Following deployment, client devices were configured to obtain addresses automatically. Successful lease allocation confirmed that both the DHCP scopes and relay services were functioning correctly. The assigned addresses, DNS settings and gateway information verified that devices could communicate with network resources across the enterprise environment and access services hosted within both locations [4].

7. Network Testing and Troubleshooting

Testing and troubleshooting were performed after completing all major configurations to verify that the infrastructure was operating correctly. Validation activities focused on network connectivity, DNS functionality, and routing behavior across the Birmingham and London sites. These tests were essential for confirming that the implemented services were functioning as expected and that users could successfully access network resources throughout the environment [8], [5].

7.1 Connectivity Testing

Connectivity testing was conducted using tools such as Ping. These utilities were used to verify communication between devices located in different subnets and to confirm that routing services were forwarding traffic correctly. Successful responses from hosts in both

Birmingham and London demonstrated that static routes and IP forwarding had been configured correctly. The results confirmed stable communication between all systems within the infrastructure [8].

7.2 DNS Validation

These tests confirmed that hostnames could be successfully resolved to IP addresses and that DNS records created within the alexandru.acca domain were functioning correctly. Successful name resolution demonstrated that the DNS server was operating as expected and supporting communication between users, devices and network services across both locations [4].

7.3 Troubleshooting Activities

Where necessary, troubleshooting procedures were performed by reviewing routing tables, DNS configurations and network settings. Route verification and connectivity testing helped identify potential configuration issues and confirm that corrective actions had been successful. These activities ensured that the infrastructure remained fully operational and capable of supporting all deployed services throughout the project lifecycle [4], [8].

8. Shared Storage Configuration

To provide centralised file storage within the enterprise environment, a secondary disk was attached to the Birmingham Domain Controller and configured as a shared storage location. [5].

8.1 Disk Deployment

A second virtual disk was added to the B-DC server and initialised using Windows Disk Management. The disk was formatted, assigned a drive letter and configured to host the Birmingham directory. This location was selected as the dedicated shared storage area for domain users and was integrated into the existing network infrastructure.

9. IIS Web Server Deployment

Internet Information Services (IIS) was deployed on the Birmingham Domain Controller (B-DC) to provide an internal web service accessible to authenticated domain users. The web server was configured in accordance with the coursework requirements and integrated with the existing Active Directory and DNS infrastructure [5], [9].

9.1 Website Configuration

A new website named webs.alexandru was created and configured within IIS Manager. Appropriate DNS records were added to ensure successful name resolution, and HTTPS bindings were configured to support secure access.

10. Remote Desktop Services

Remote Desktop Services (RDS) were configured to provide secure remote administration of the Birmingham Domain Controller. This service allows administrators to access and manage the server remotely without requiring physical access to the system. Implementing RDS improved infrastructure manageability and supported efficient administration of services deployed throughout the enterprise environment. The solution was integrated with

Active Directory to ensure that access could be controlled through domain authentication and existing security policies [7], [10].

11. Security Measures

Security was an important consideration throughout the implementation of the enterprise infrastructure. Several security controls were applied to protect user accounts, network communications and shared resources. These measures helped ensure that services remained accessible to authorized users while reducing the risk of unauthorized access [5], [7].

11.1 Password Security

A domain password policy was configured through Group Policy Management to enforce password complexity requirements, minimum password length and password history settings [7].

11.2 VPN Encryption

The VPN connection was implemented to provide secure communication between the Birmingham and London networks. Encryption protects data transmitted between both sites and helps maintain the confidentiality and integrity of the network [7].

12. Testing Summary

Following the completion of all configurations, testing was performed to verify that each service was functioning correctly. Connectivity tests confirmed successful routing between the Birmingham and London networks, while VPN validation demonstrated secure communication between both sites. DNS and DHCP testing verified correct name resolution and automatic IP address allocation. Active Directory authentication, shared storage access, IIS website functionality and Remote Desktop Services were also tested successfully.

13. Conclusion

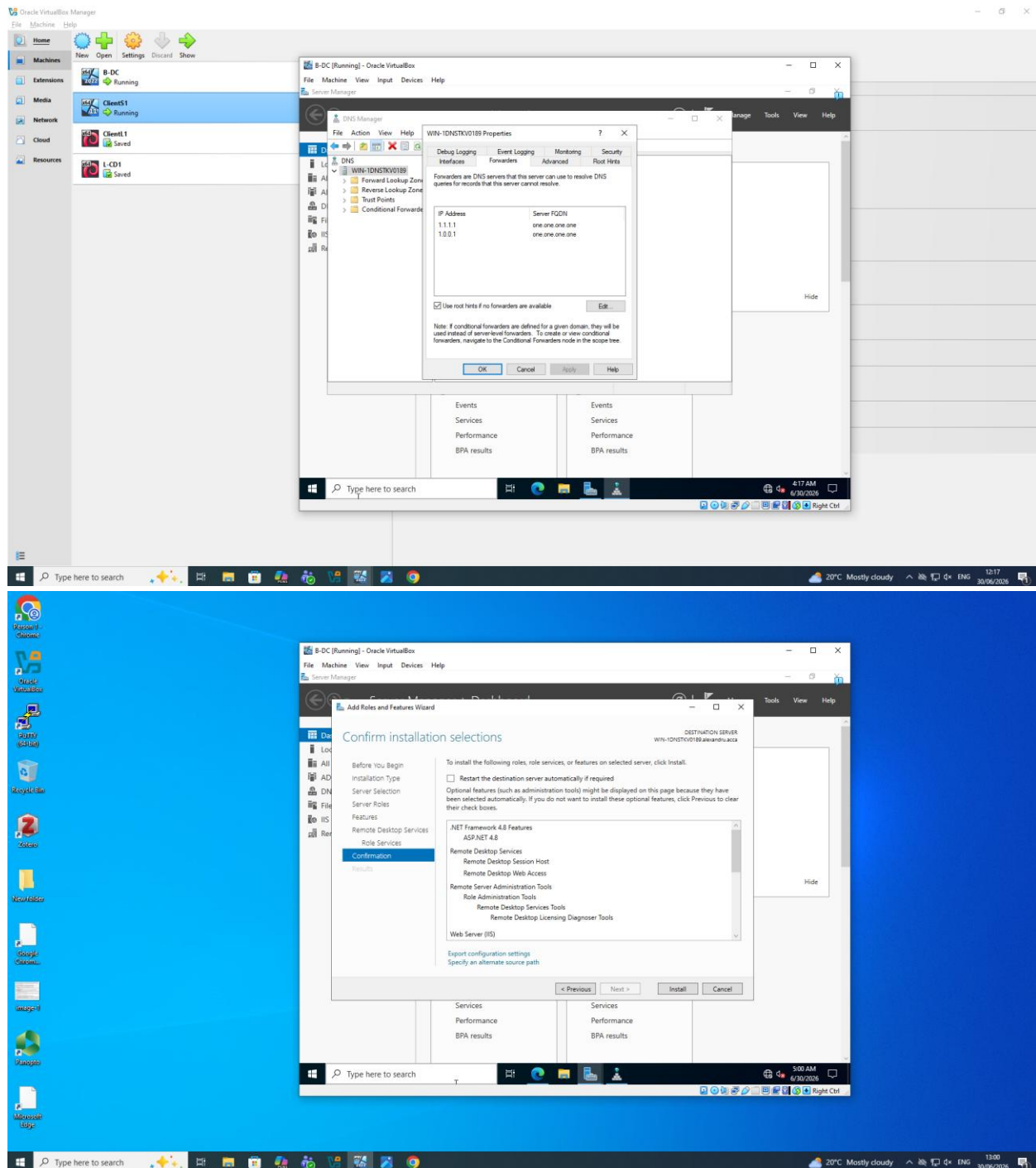
This project successfully transformed the virtual infrastructure developed during Coursework 1 into a fully operational enterprise network environment. Routing services were implemented to enable communication between Birmingham and London.

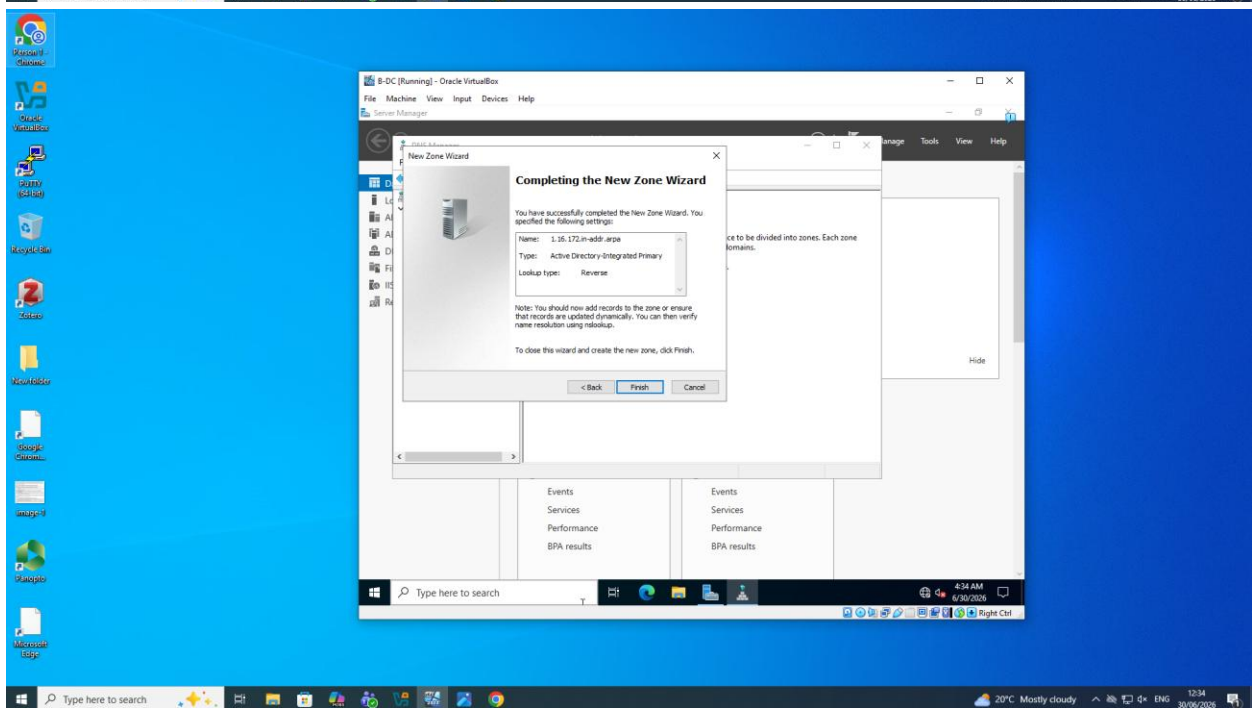
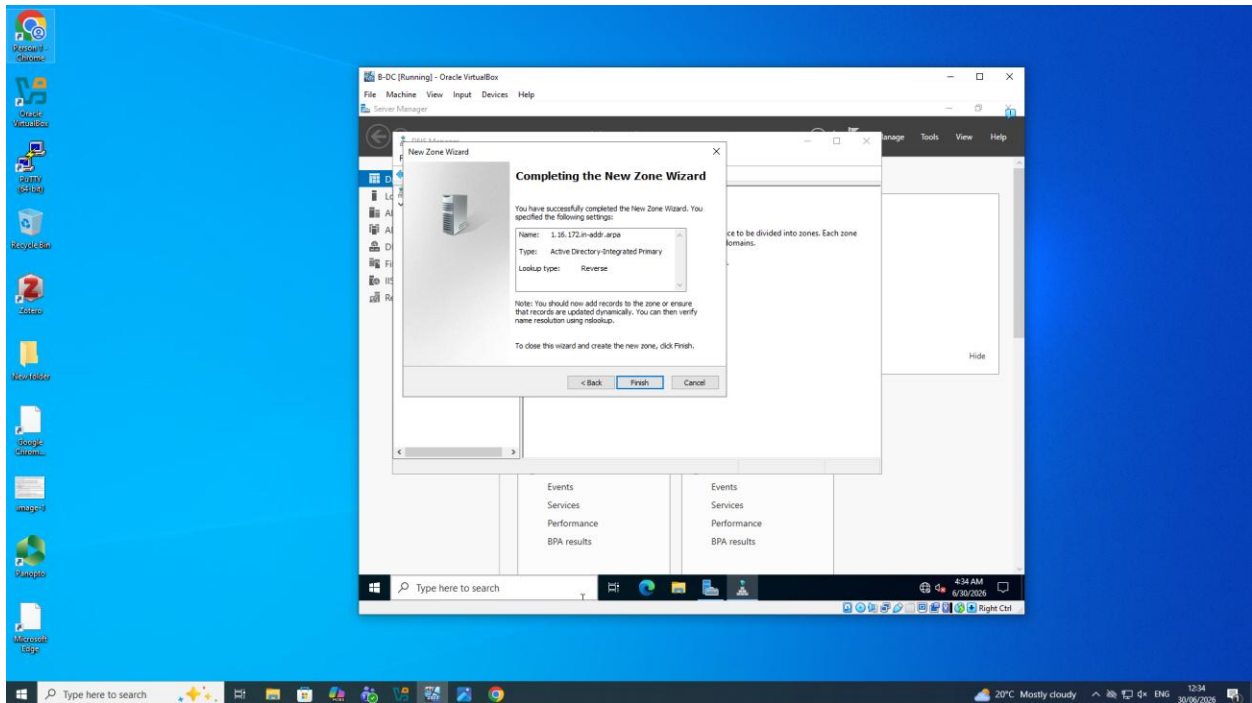
The completion of this project provided practical experience in deploying and managing enterprise network services within a virtualised environment. Valuable skills were developed in Windows Server administration, Linux server management, network routing, Active Directory implementation and troubleshooting complex network configurations. The project also strengthened understanding of security principles through the application of password policies, access permissions and encrypted communications.

References

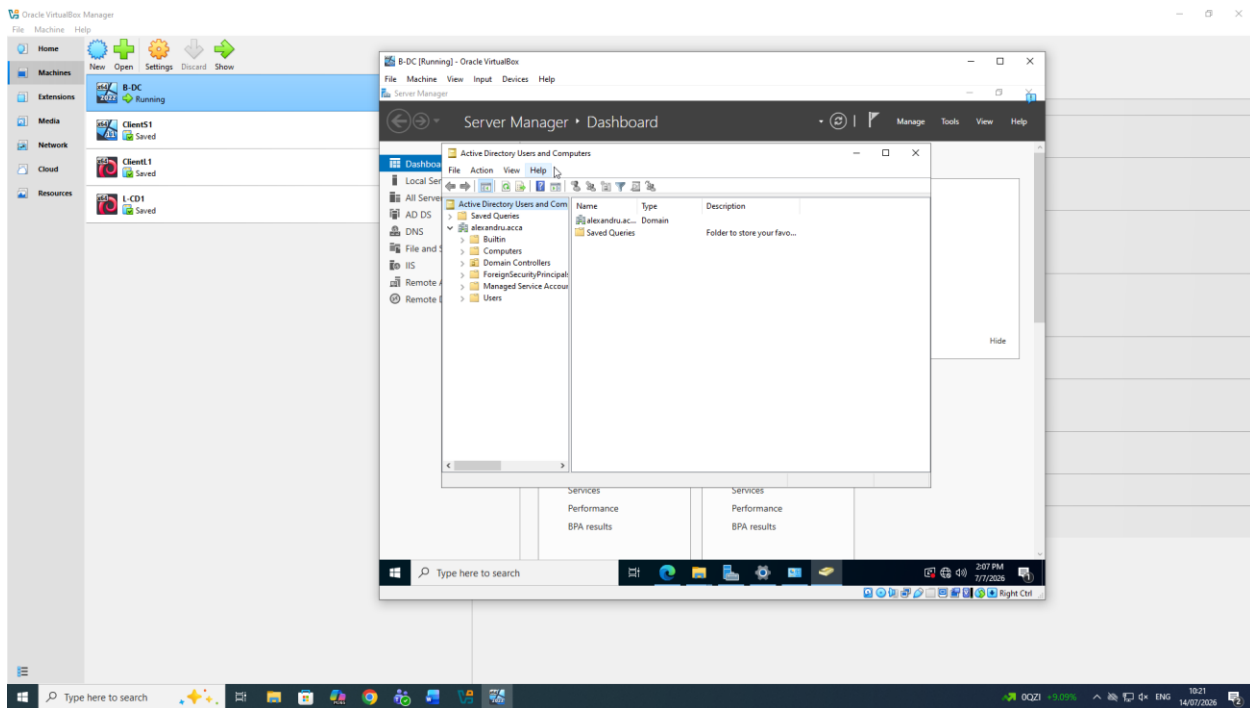
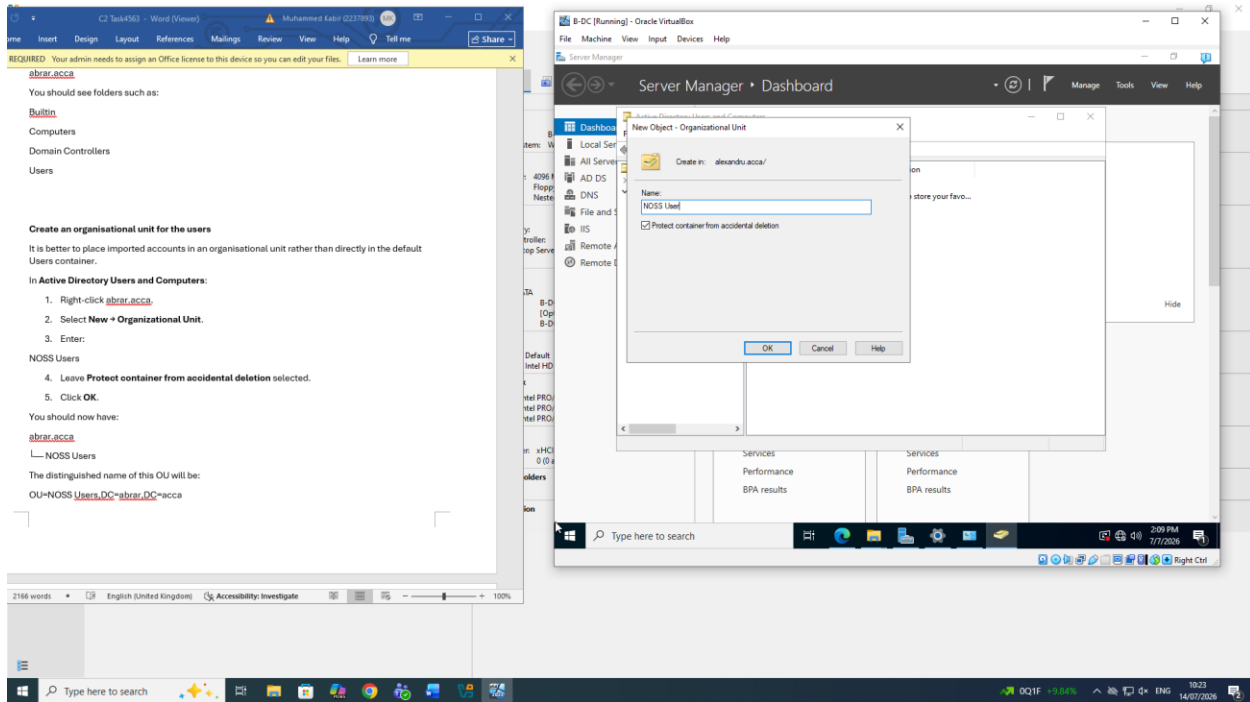
- [1] Oracle Corporation, *Oracle VM VirtualBox User Manual, 2024*. Accessed: Jul. 24, 2026. [Online]. Available: <https://www.virtualbox.org/manual/UserManual.html>
- [2] Microsoft, *Windows Server Documentation*. Accessed: Jul. 24, 2026. [Online]. Available: <https://learn.microsoft.com/windows-server/>
- [3] A. S. Tanenbaum, N. Feamster, and D. Wetherall, *Computer networks*, Sixth edition. Harlow: Pearson, 2021.
- [4] Microsoft, *DHCP Overview*. Accessed: Jul. 24, 2026. [Online]. Available: <https://learn.microsoft.com/windows-server/networking/technologies/dhcp/dhcp-top>
- [5] Microsoft, *Active Directory Domain Services Overview*. Accessed: Jul. 24, 2026. [Online]. Available: <https://learn.microsoft.com/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
- [6] Y. Wang, A. Zhou, S. Liao, R. Zheng, R. Hu, and L. Zhang, "A comprehensive survey on DNS tunnel detection," *Computer networks (Amsterdam, Netherlands : 1999)*, vol. 197, Art. no. 108322, Oct. 2021, doi: 10.1016/j.comnet.2021.108322.
- [7] W. Stallings, *Network security essentials : applications and standards*, Sixth edition. Harlow, England: Pearson, 2017.
- [8] A. S. Tanenbaum, N. Feamster, and D. Wetherall, *Computer networks*, Sixth edition. Harlow: Pearson, 2021.
- [9] S. Rofes, Carpenteria, CA. *Windows Server 2016: Web Segura, Internet Information Services*, (2018).
- [10] E. Magaña, I. Sesma, D. Morató, and M. Izal, "Remote access protocols for Desktop-as-a-Service solutions," *PloS one*, vol. 14, no. 1, p. e0207512, Jan. 2019, doi: 10.1371/journal.pone.0207512.

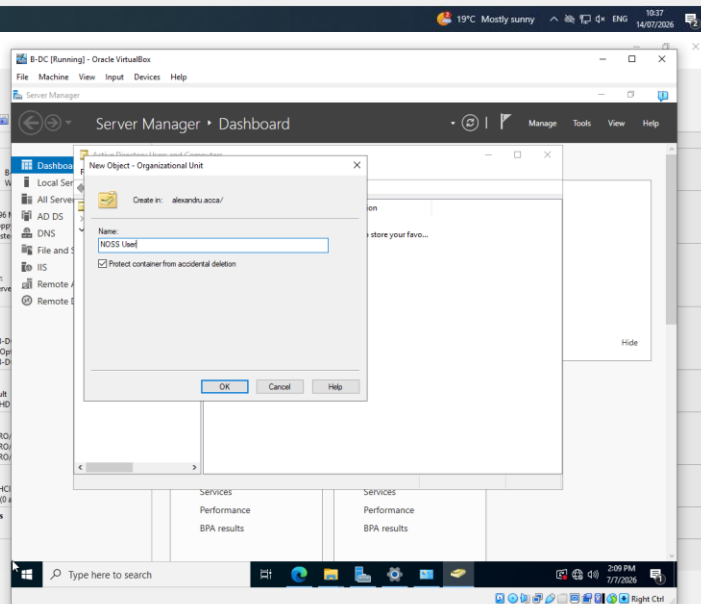
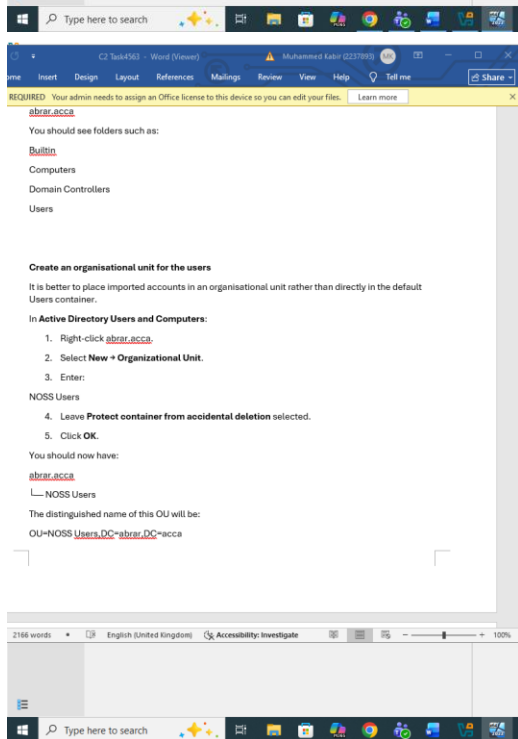
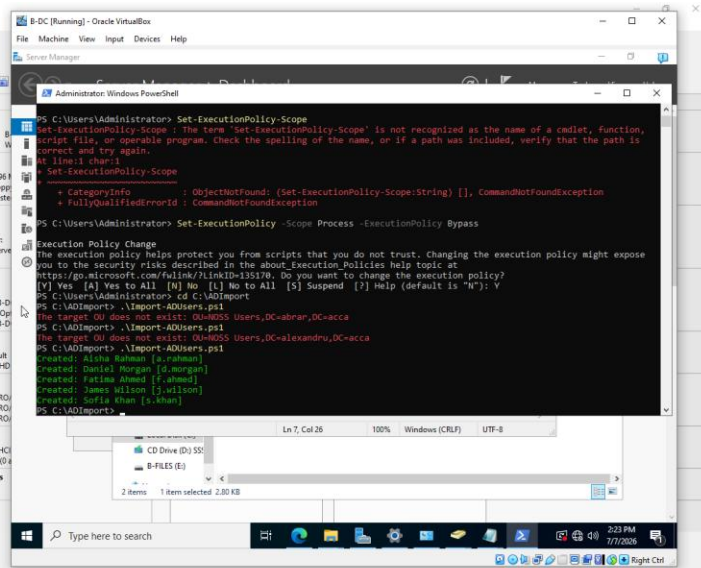
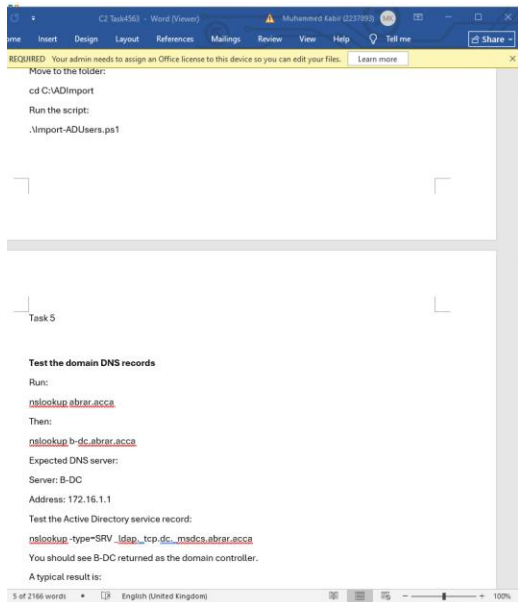
Appendix

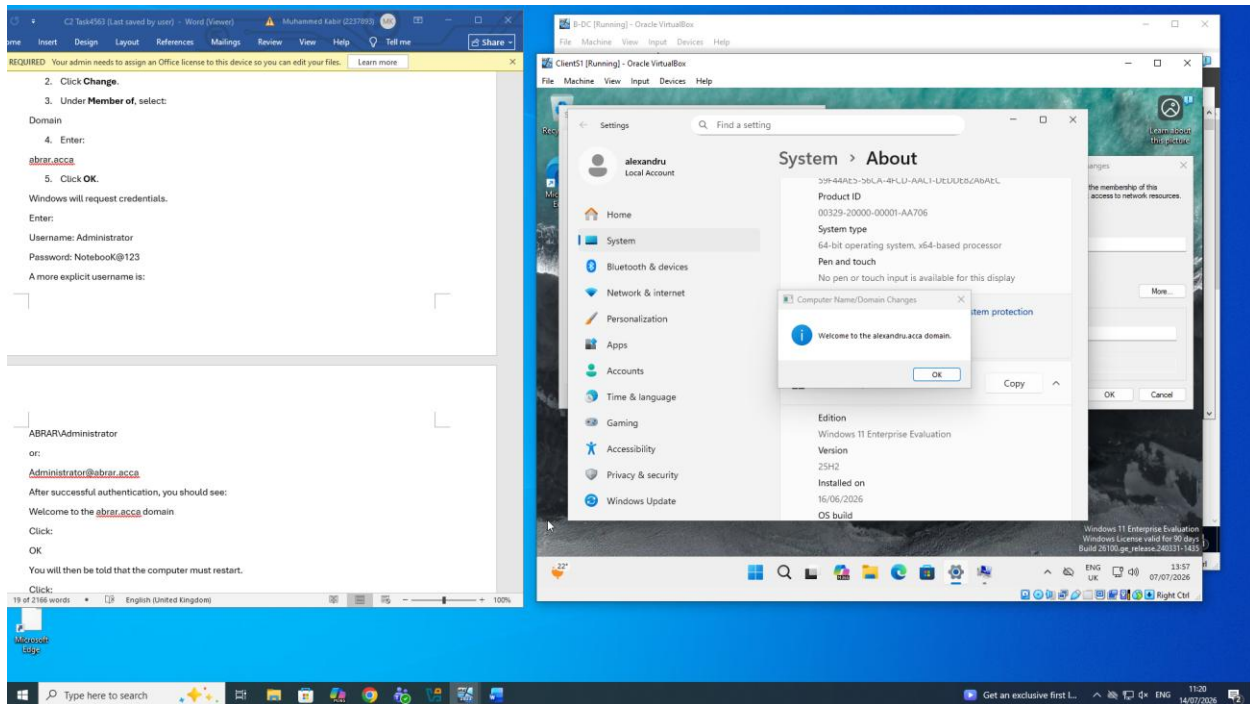
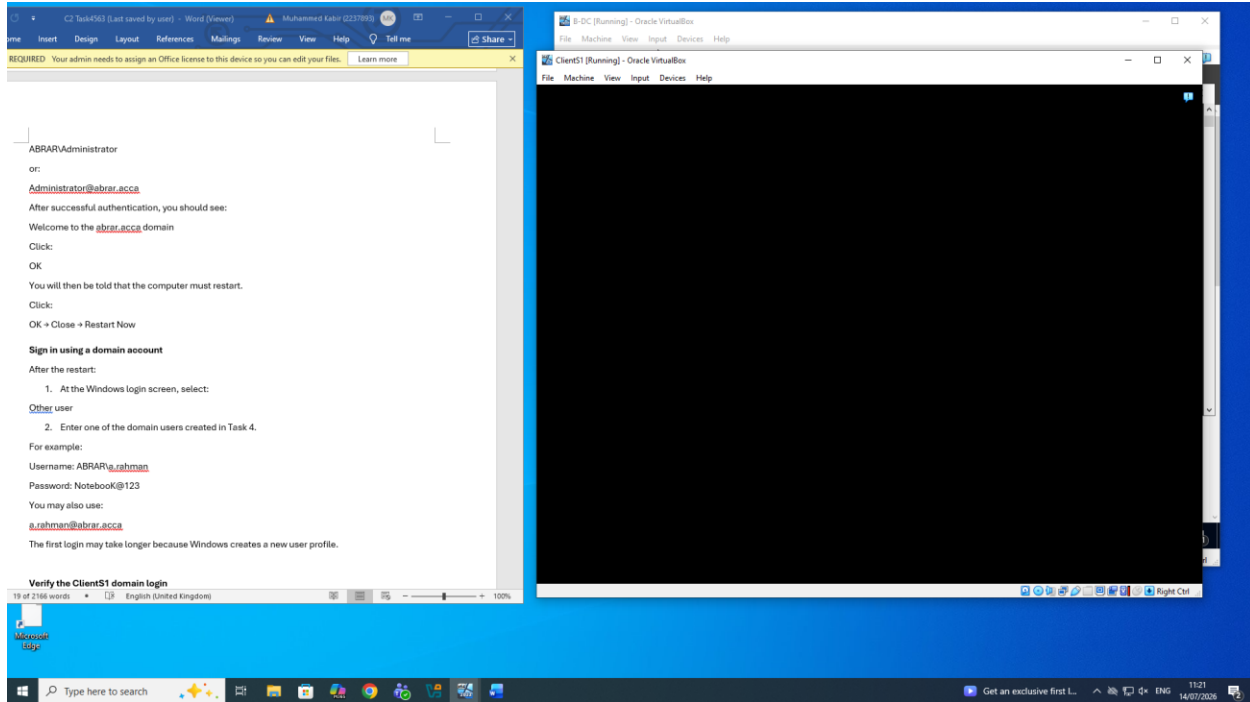


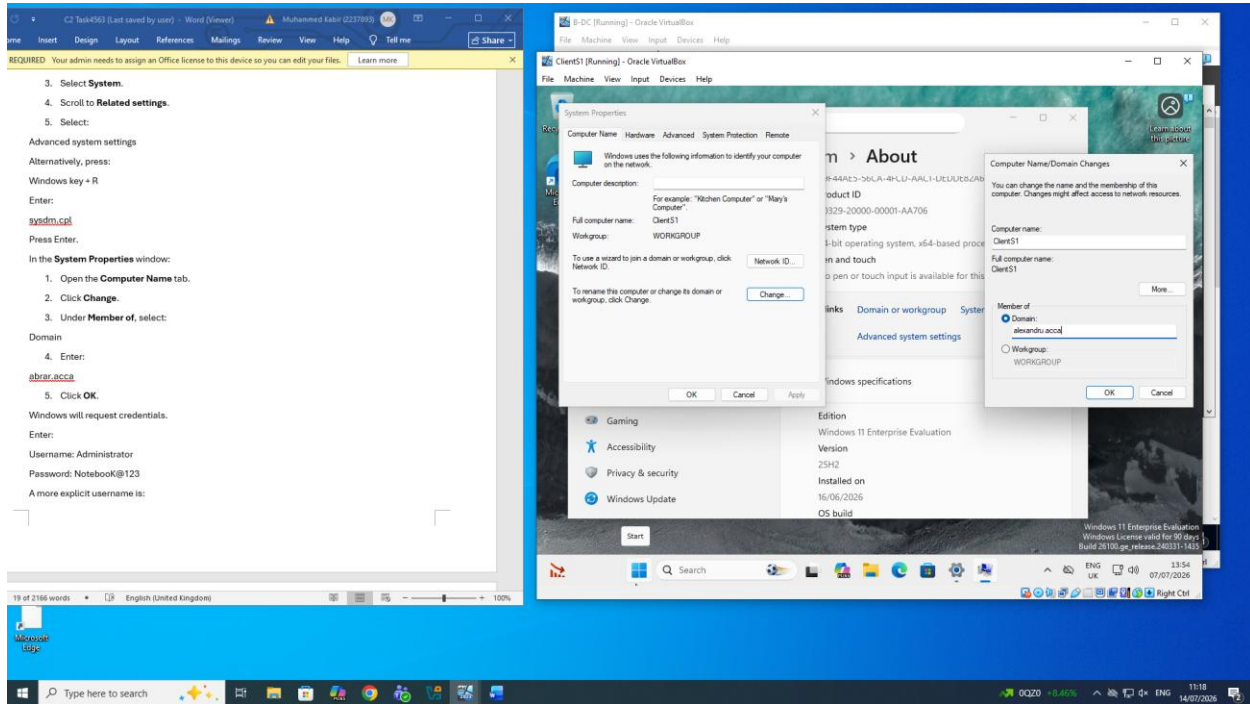
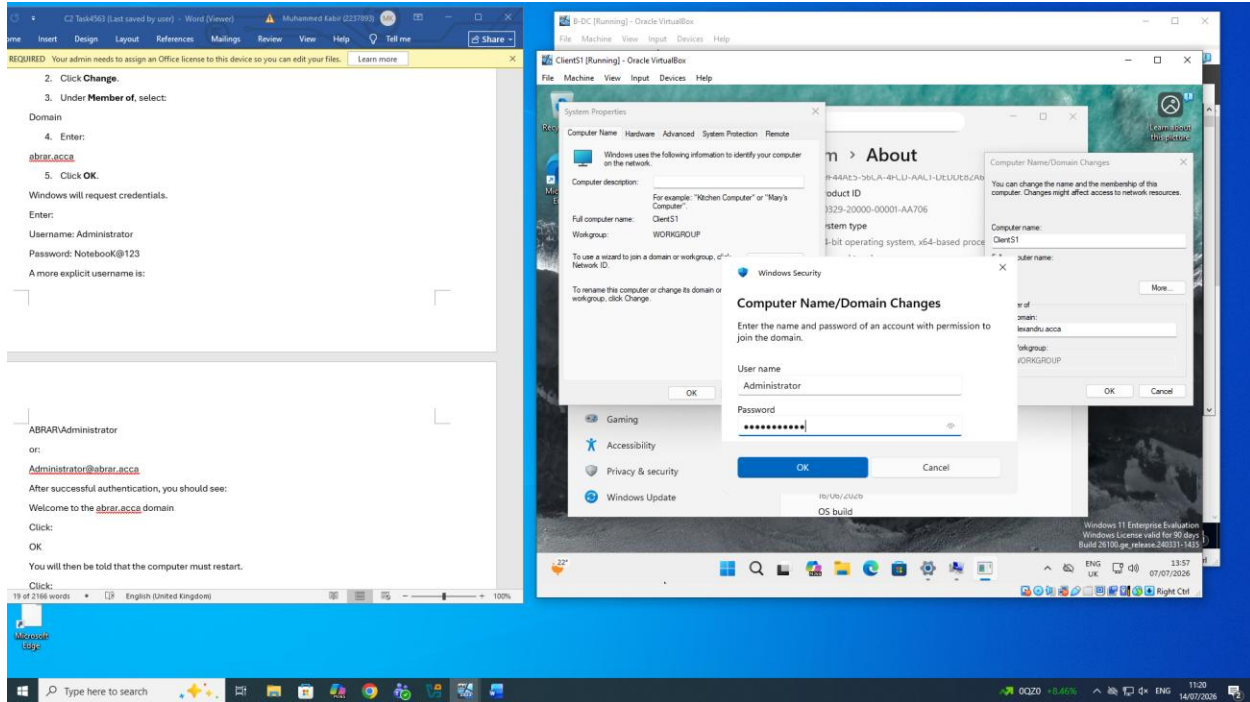


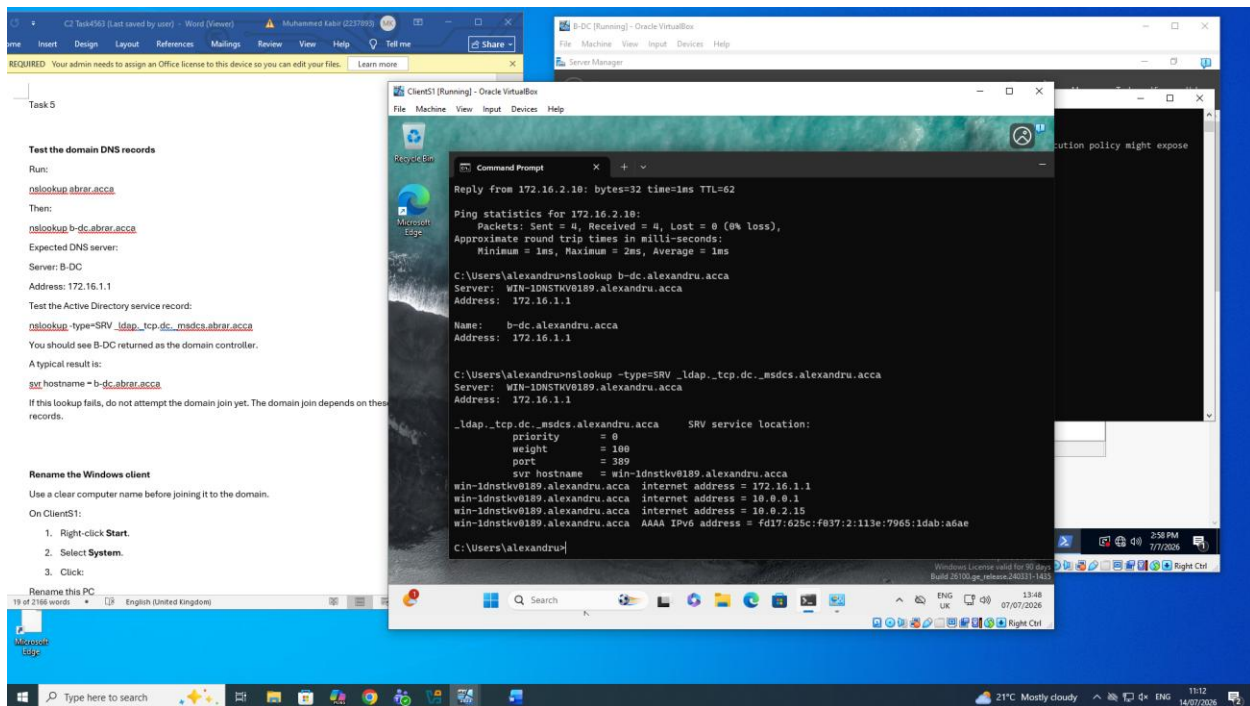
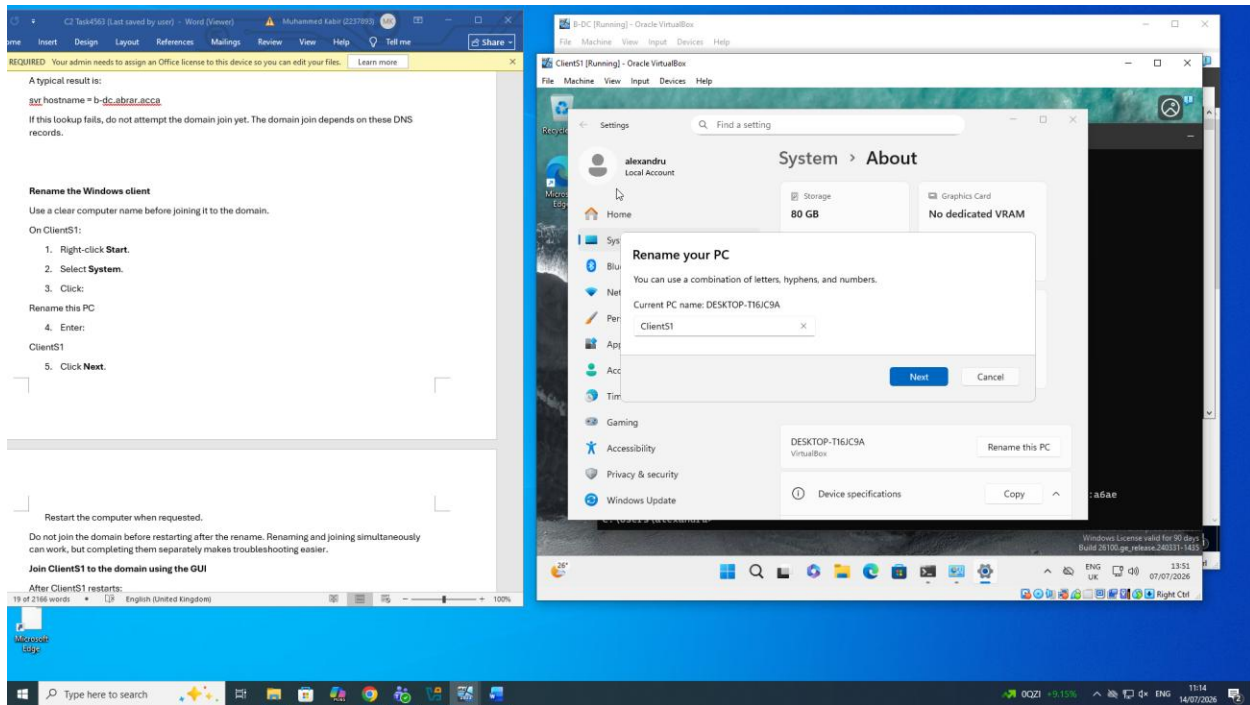












Task 5

Test the domain DNS records

Run:

```
nslookup abrar.acca
```

Then:

```
nslookup b-dc.abrar.acca
```

Expected DNS server:

Server: B-DC

Address: 172.16.1.1

Test the Active Directory service record:

```
nslookup -type=SRV _ldap._tcp.dc._msdcs.abrar.acca
```

You should see B-DC returned as the domain controller.

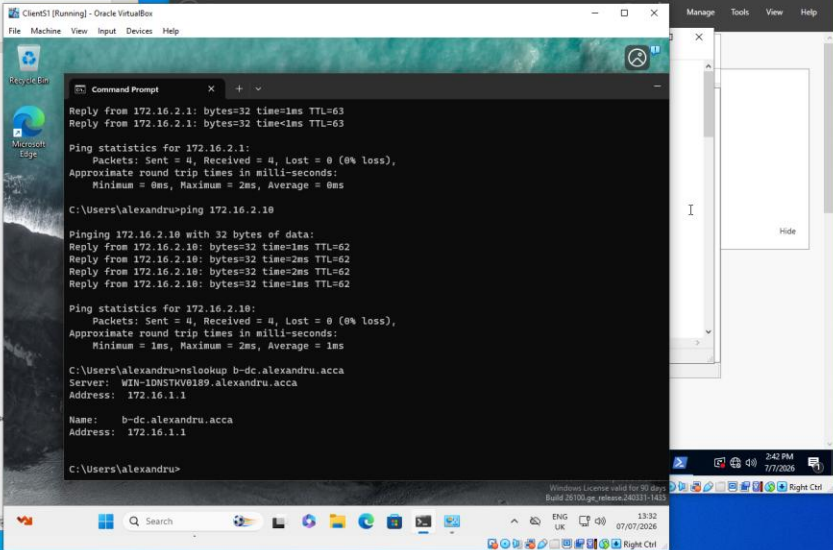
A typical result is:

```
avl hostname = b-dc.abrar.acca
```

If this lookup fails, do not attempt the domain join yet. The domain join depends on these records.

Rename the Windows client

Use a clear computer name before joining it to the domain.



Description: DHCP addresses for Birmingham network

Click **Next**.

Enter the Birmingham address range

Configure:

Start IP address: 172.16.1.10

End IP address: 172.16.1.20

Length: 24

Subnet mask: 255.255.255.0

Click **Next**.

Click **Next**.

Set the lease duration

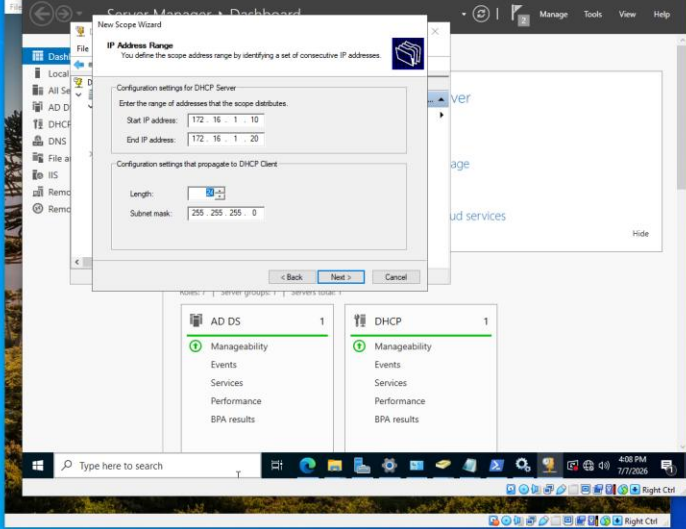
For the lab, use:

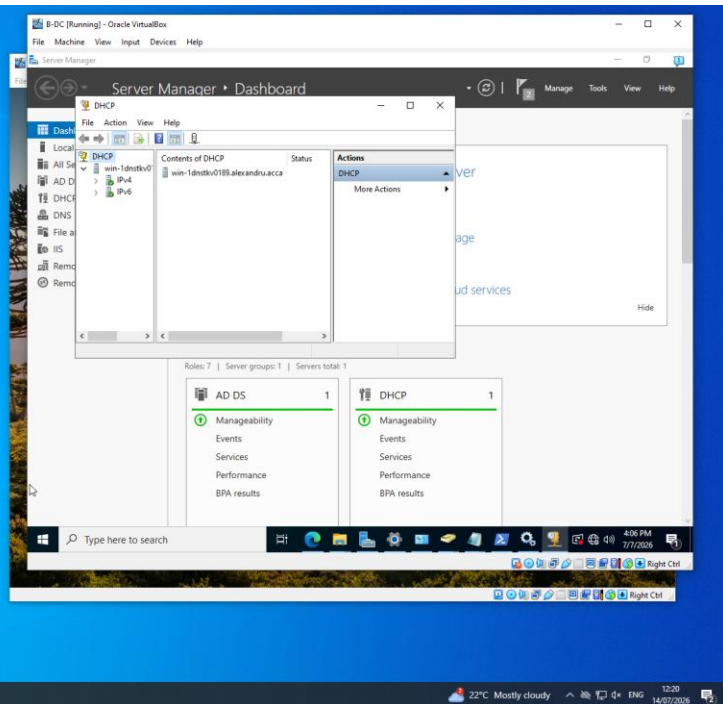
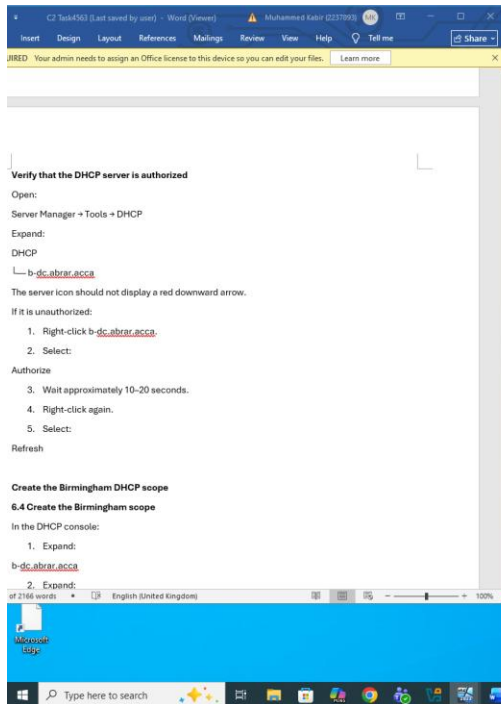
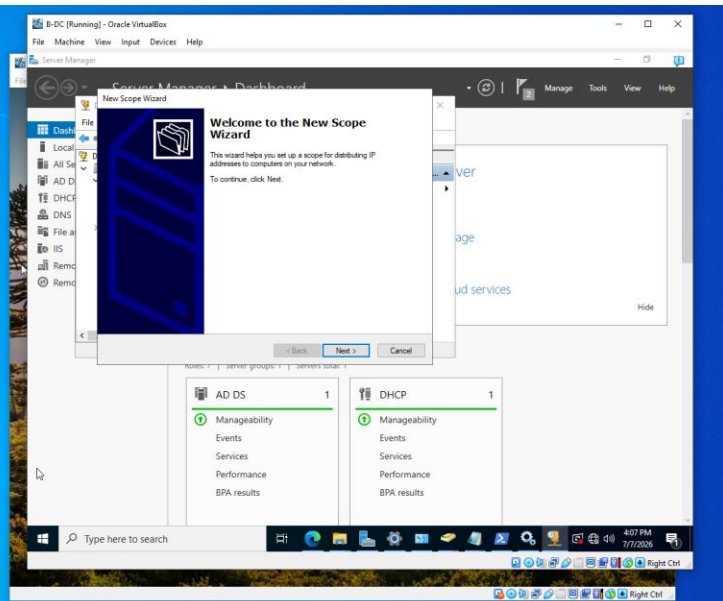
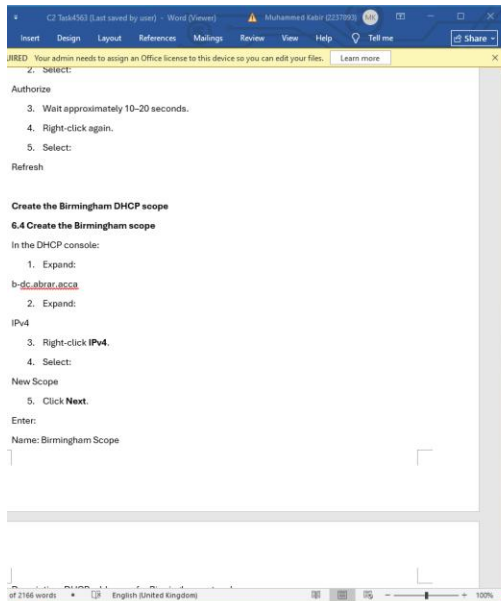
Days: 8

Hours: 0

Minutes: 0

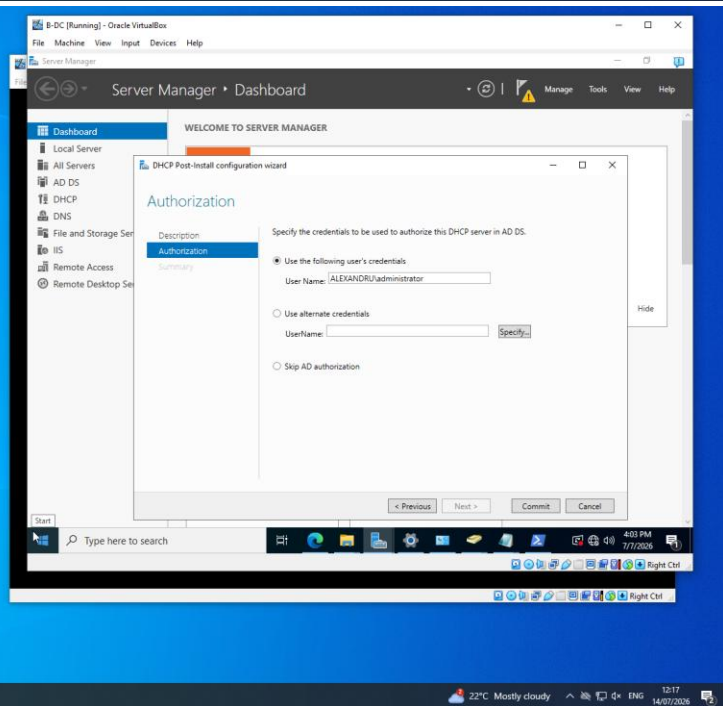
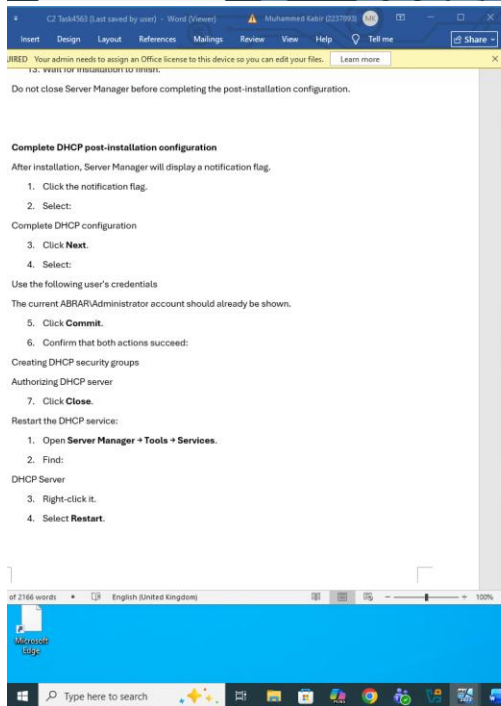
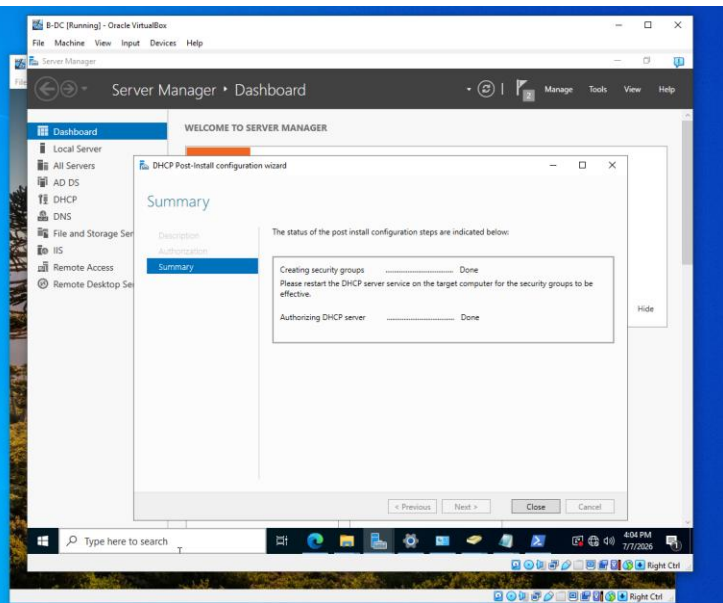
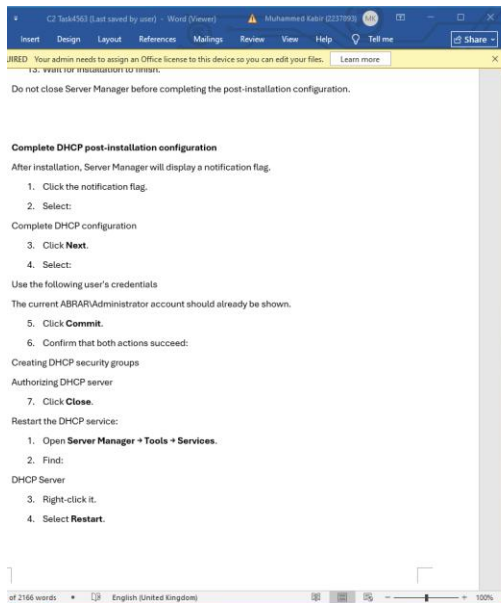
Click **Next**.

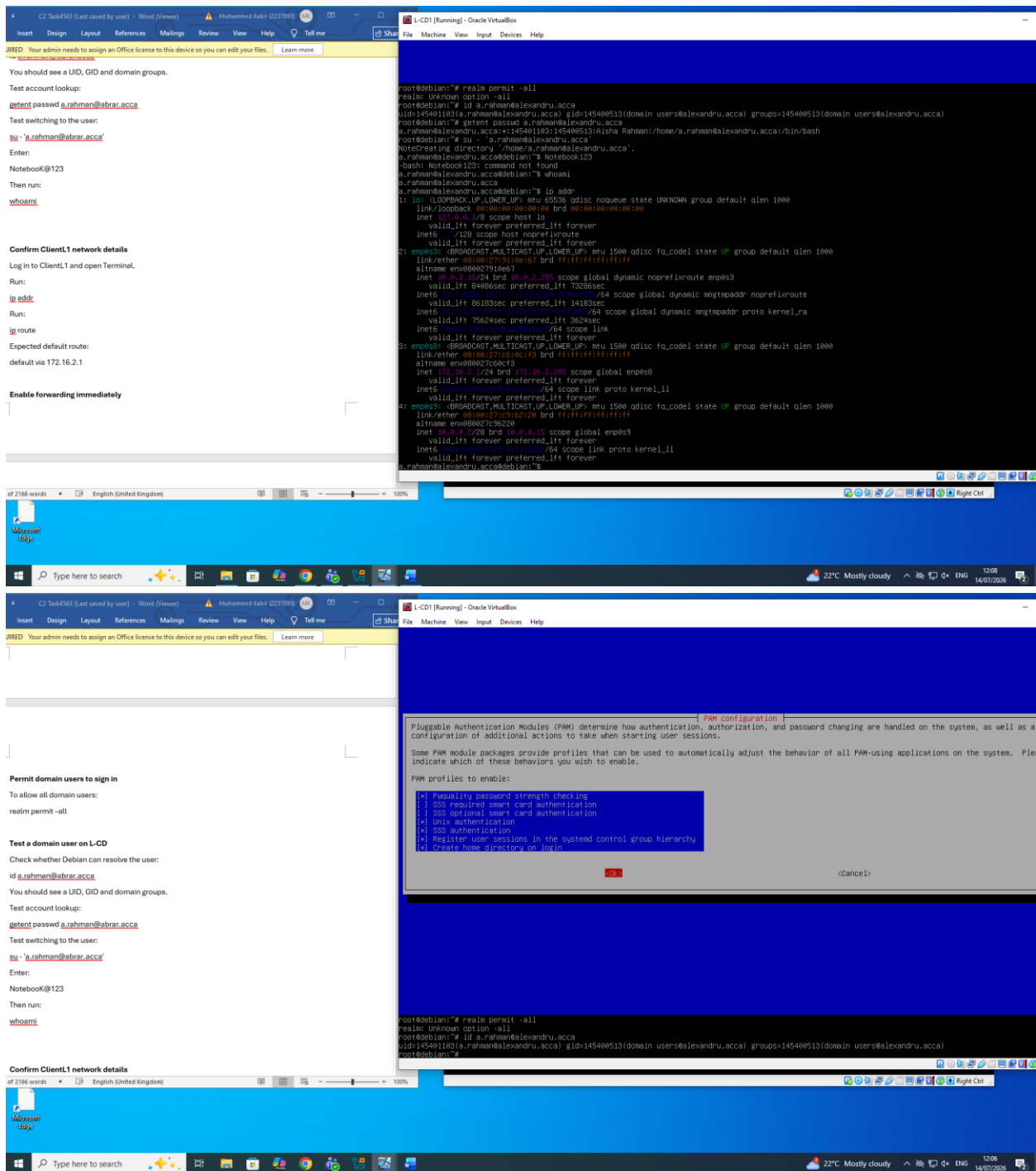


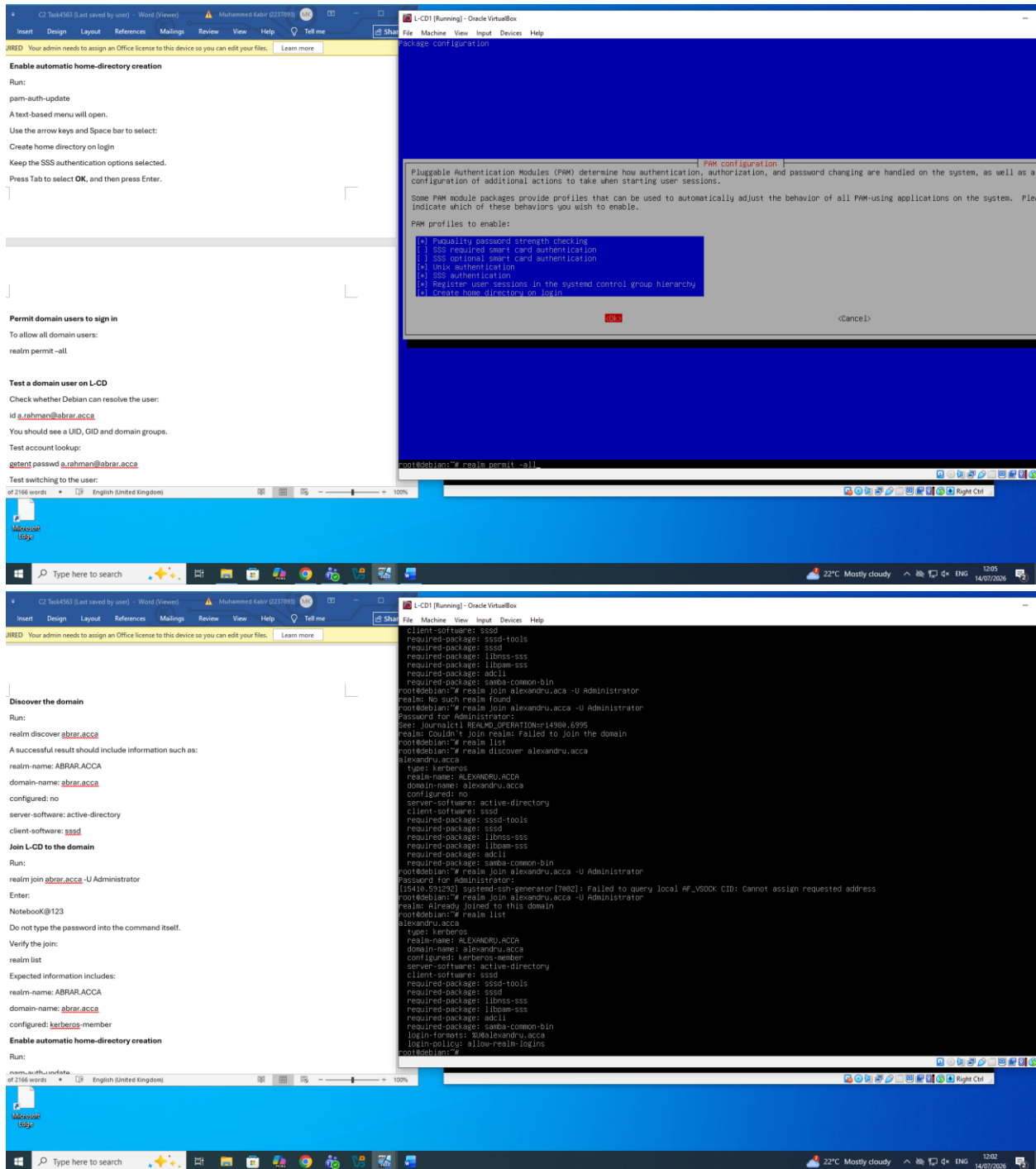


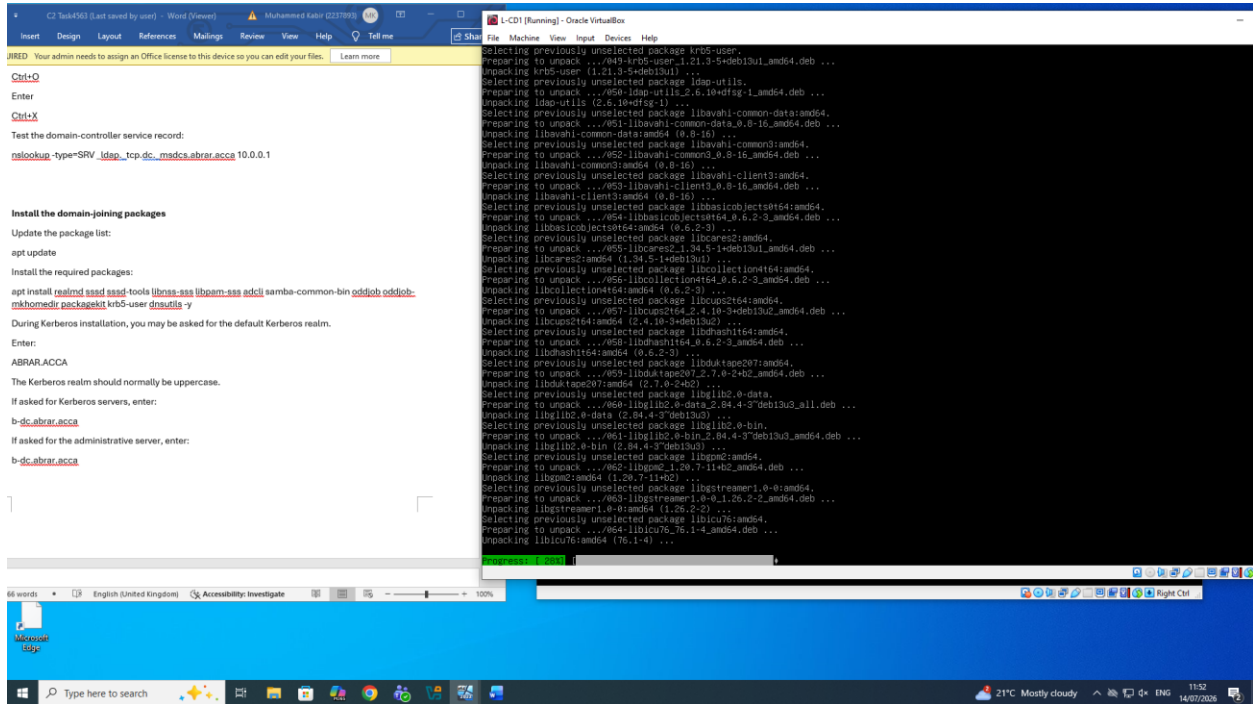
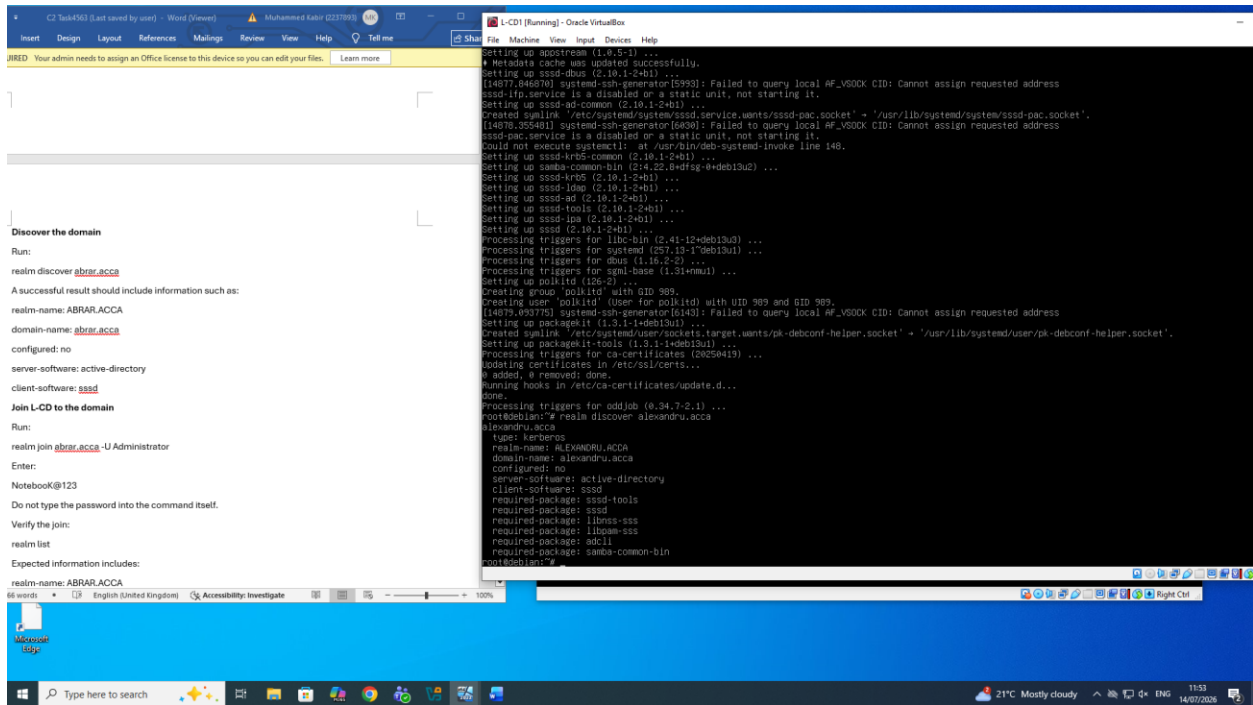
[illegible]

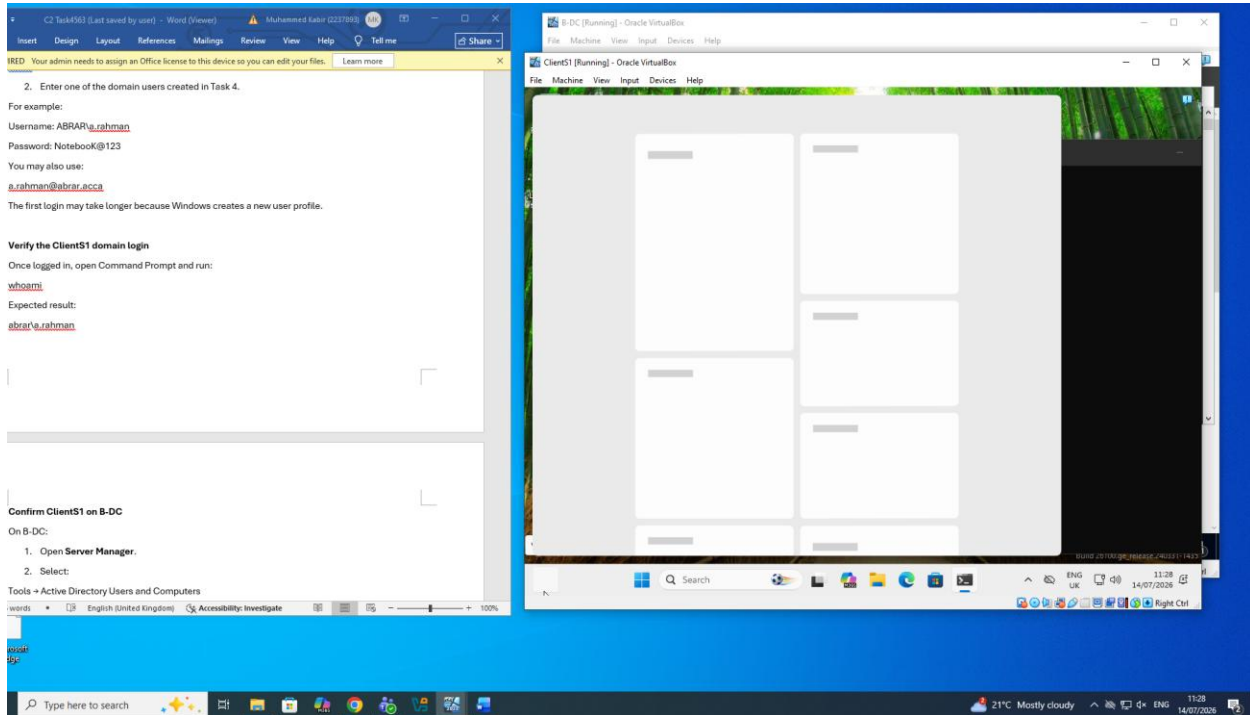
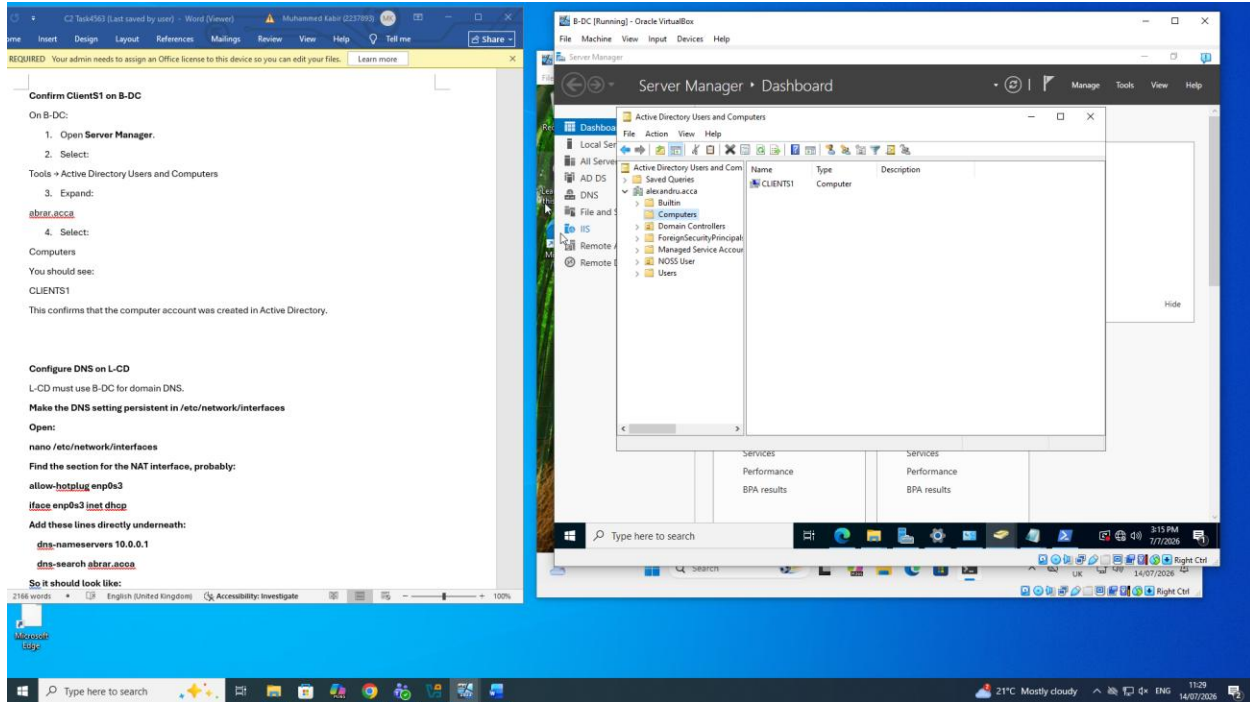
The screenshot shows the Windows Server Manager interface. The 'Services' window is open, displaying a list of services. The 'DHCP Server' service is selected, and its context menu is open. The service is currently running. The context menu options include Start, Stop, Pause, Resume, Restart, Refresh, Properties, and Help. The DHCP service is configured to start automatically and is running on the local computer.

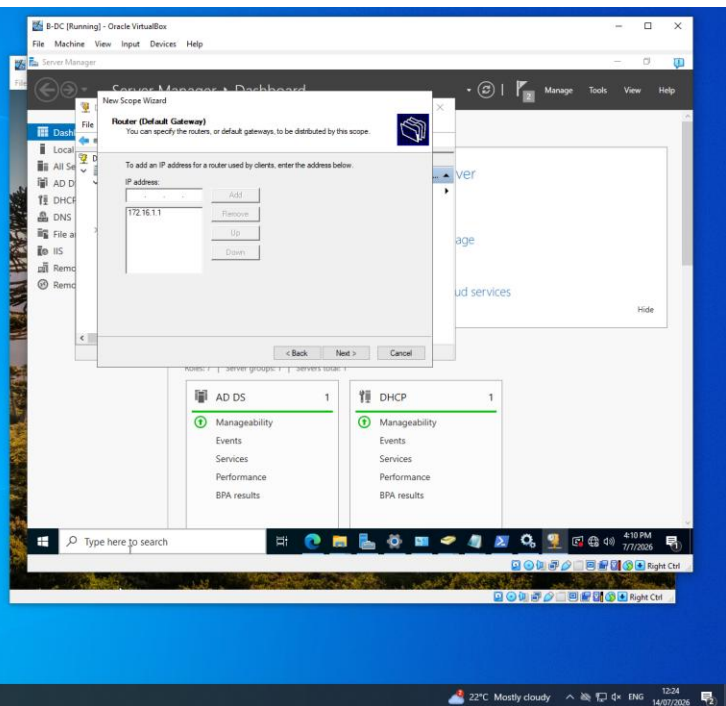
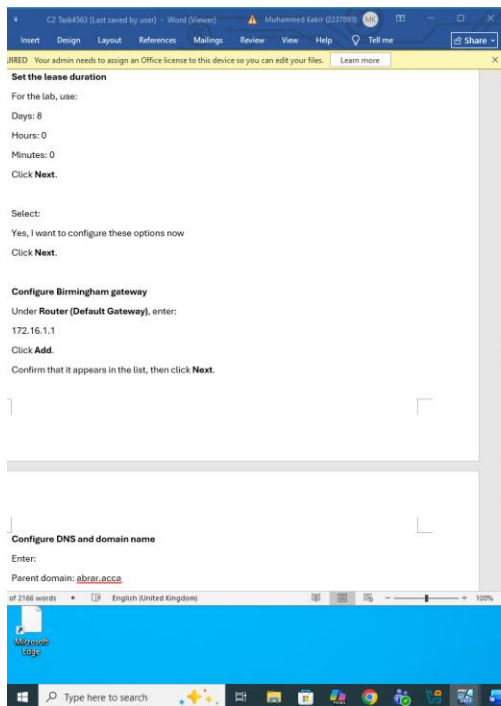
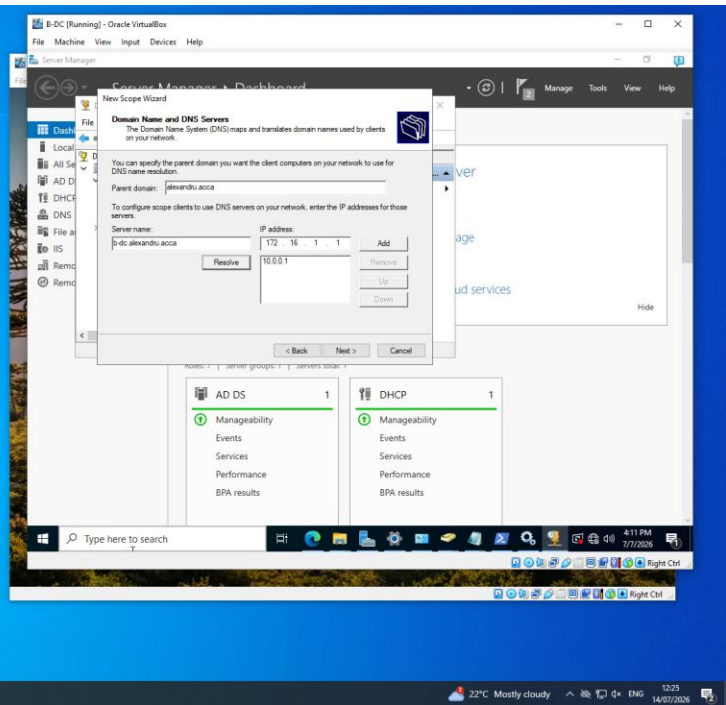
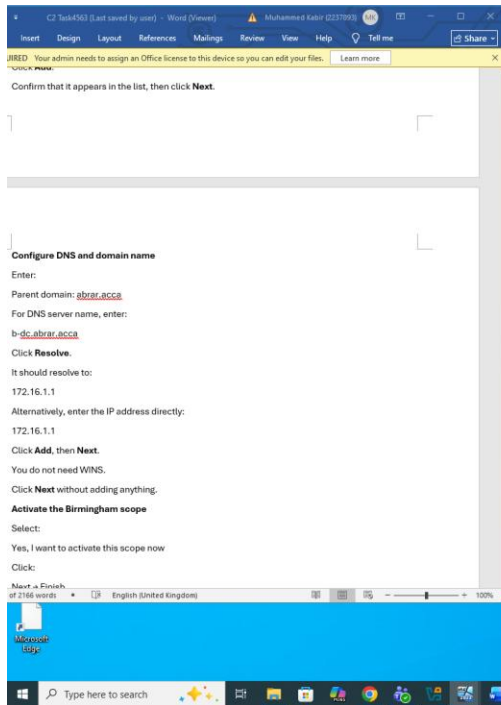


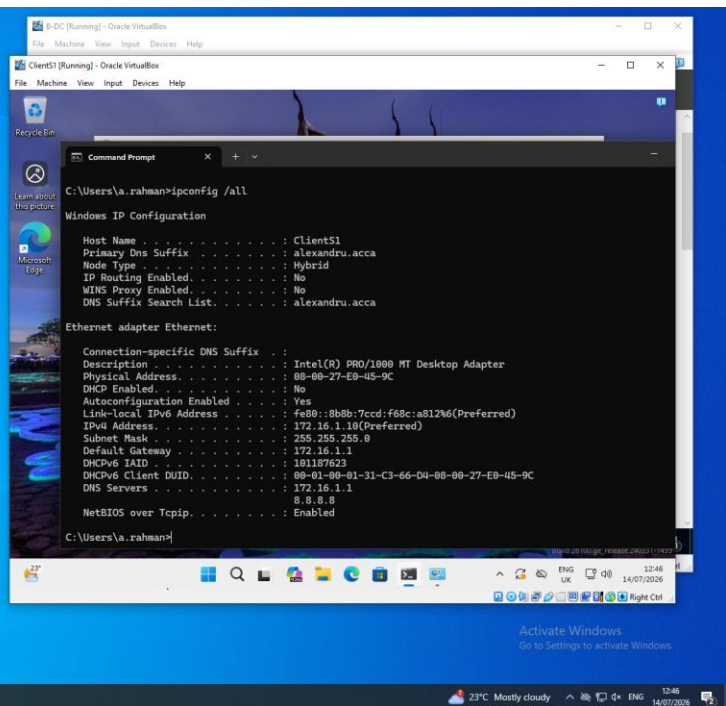
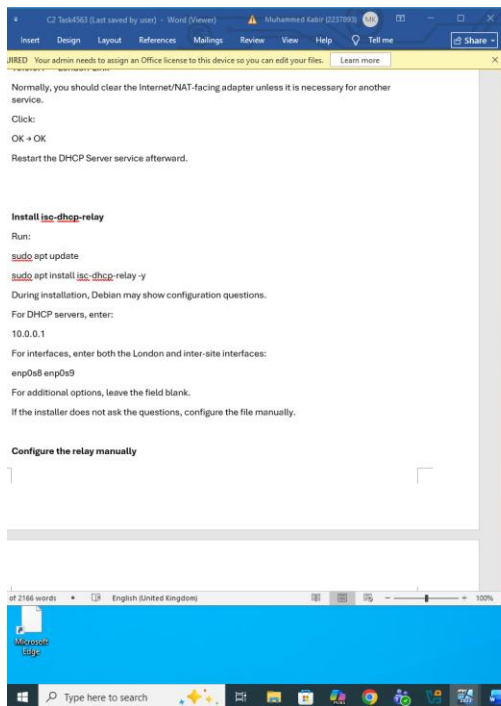
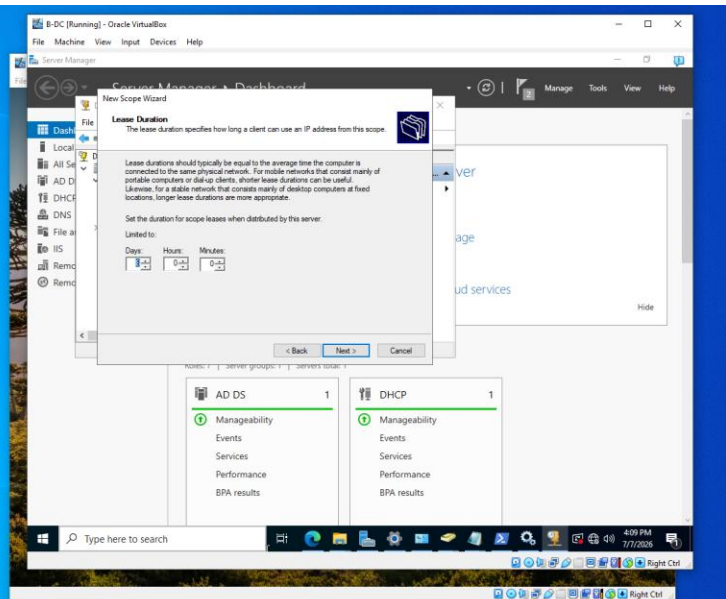
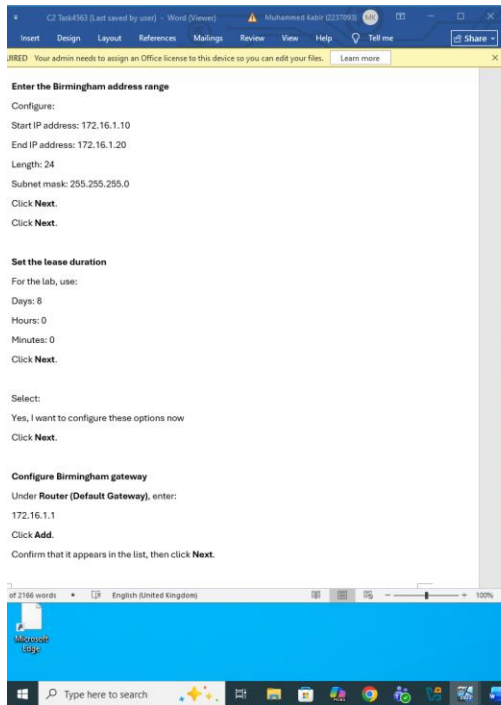


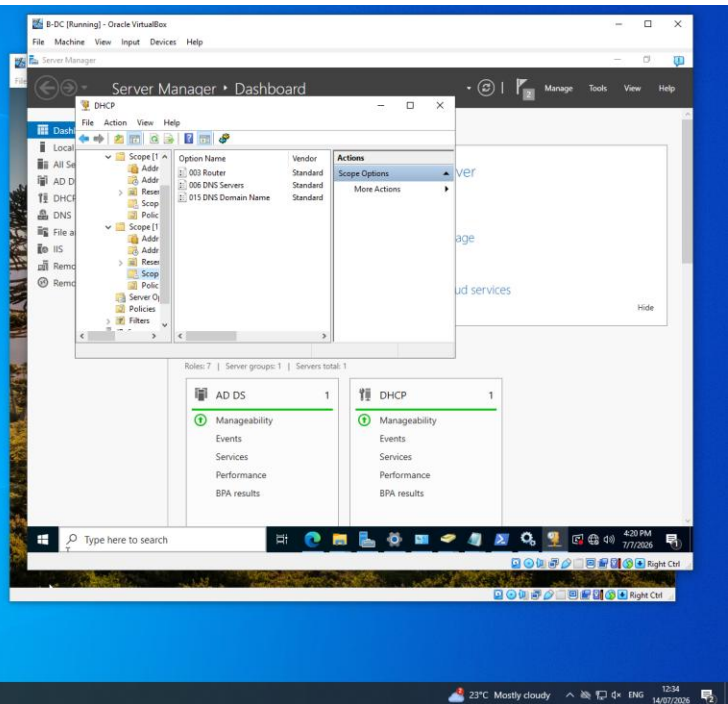
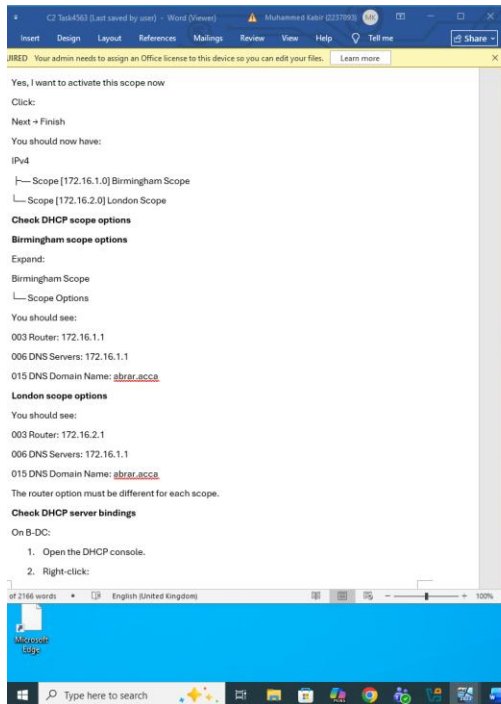
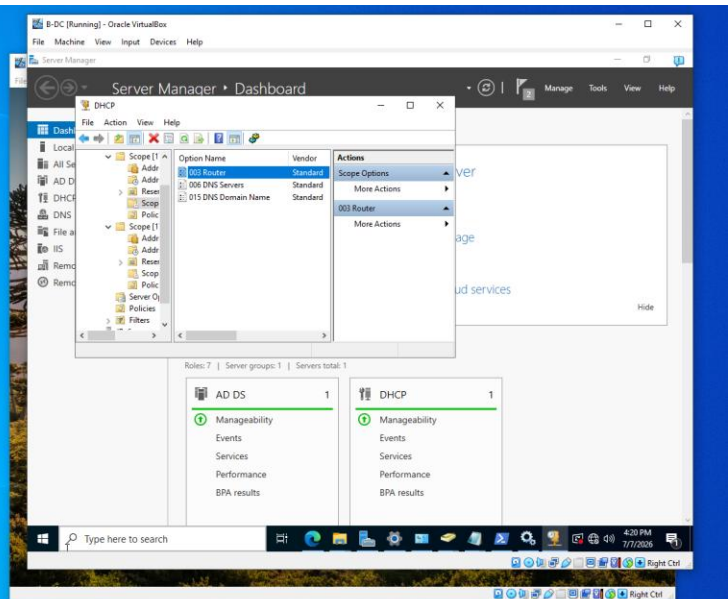
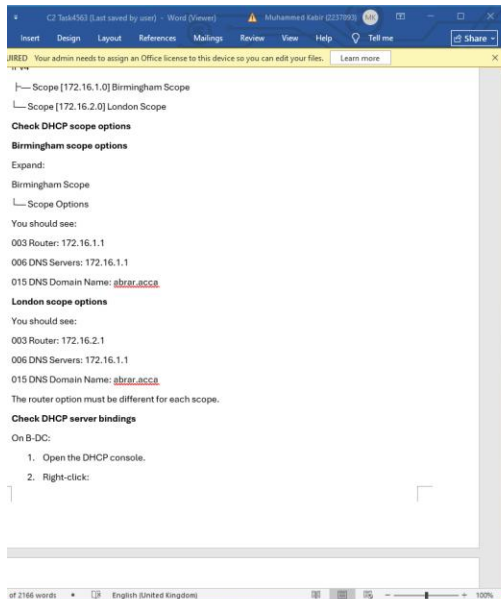


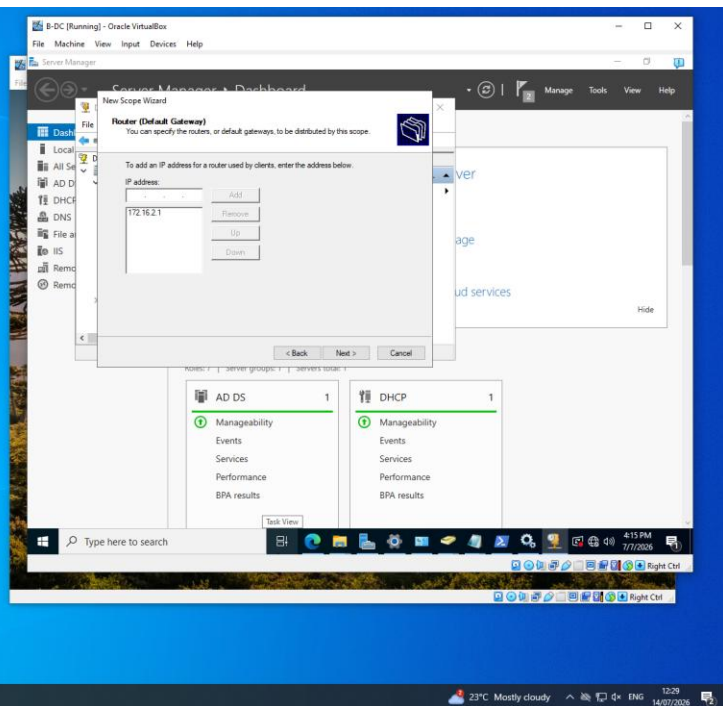
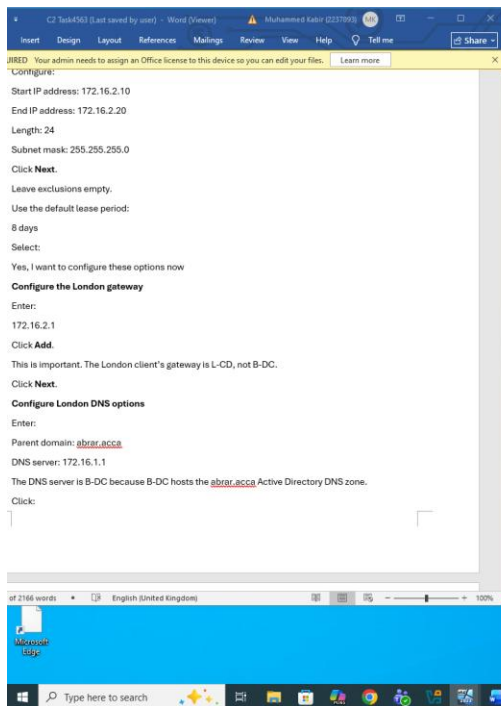
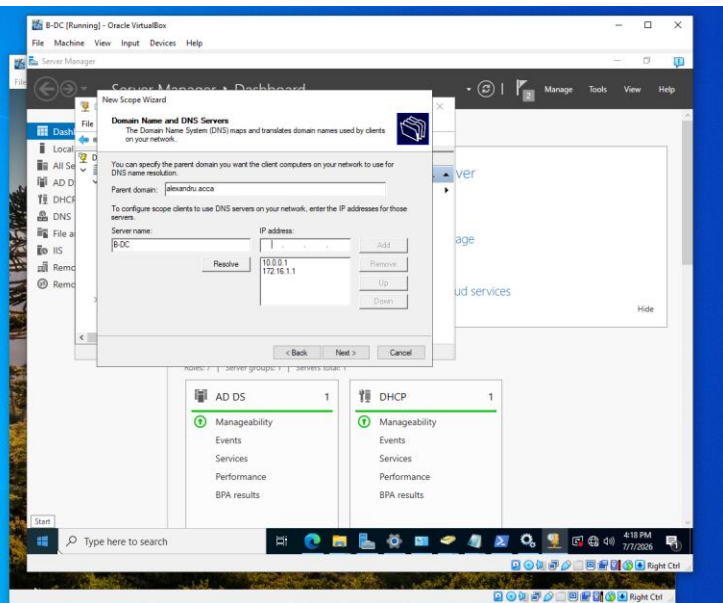
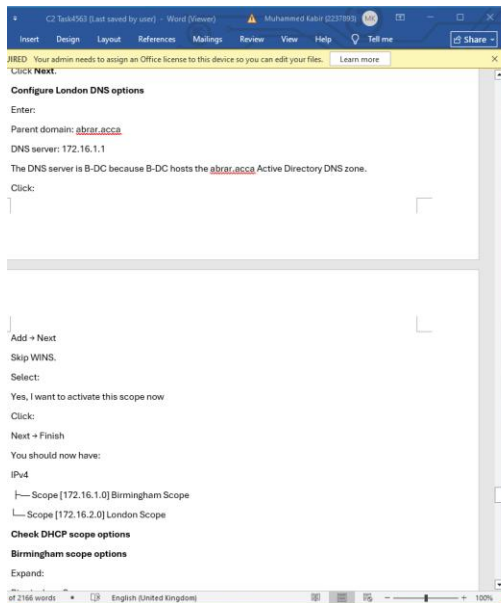




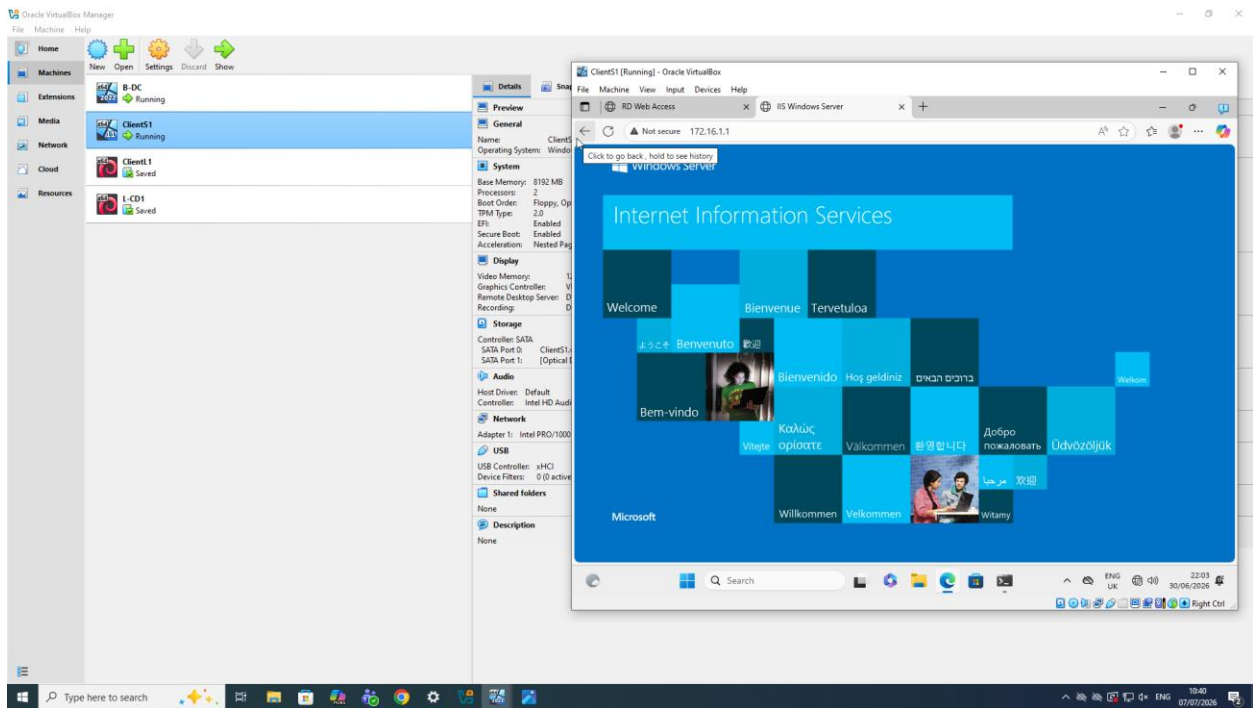
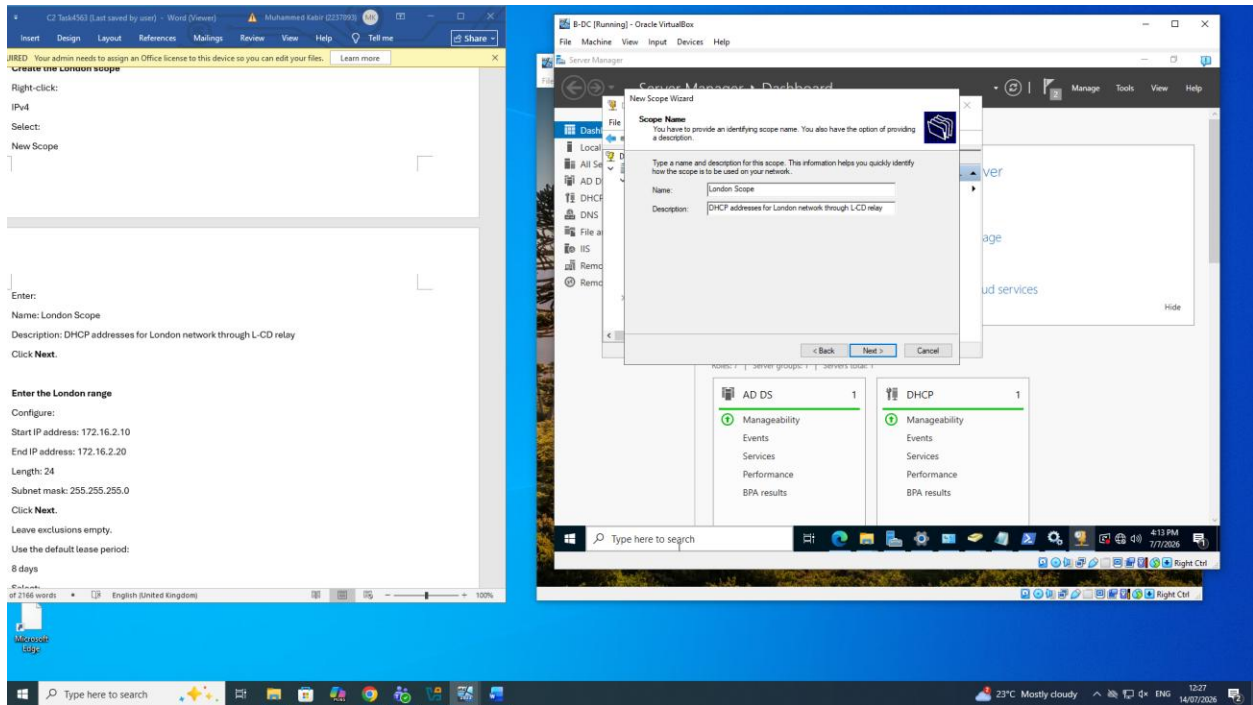


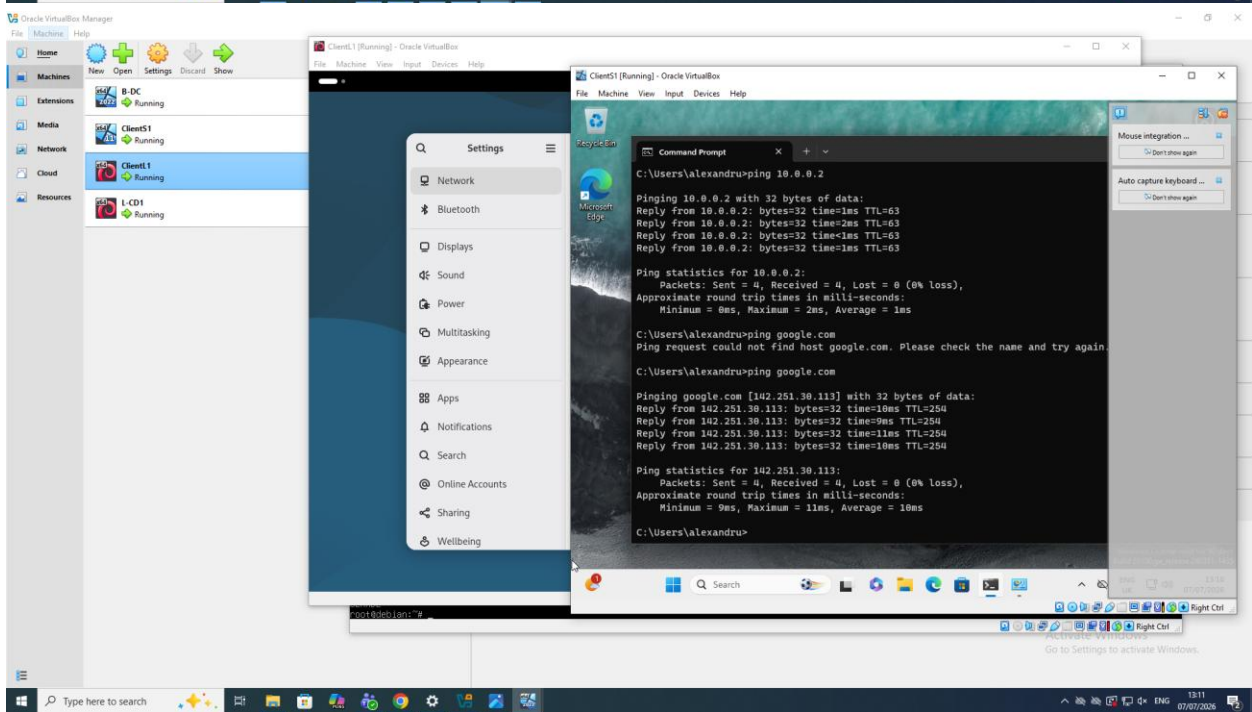
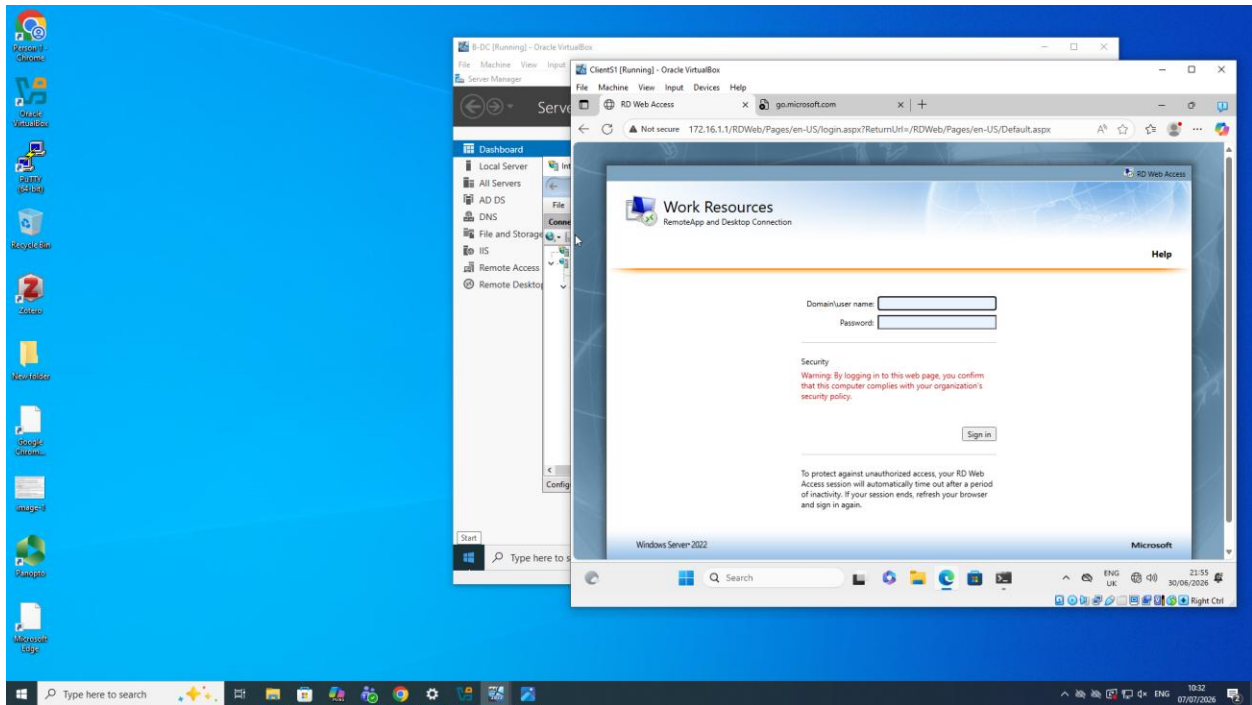


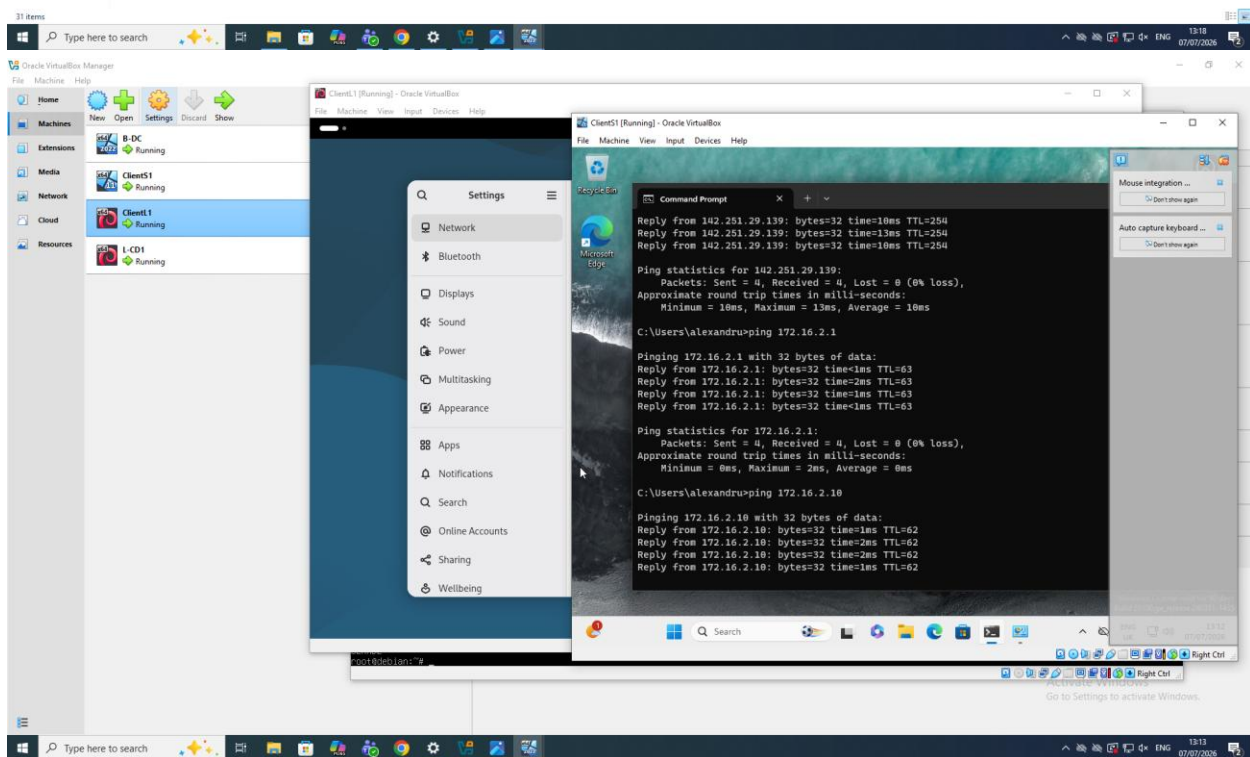
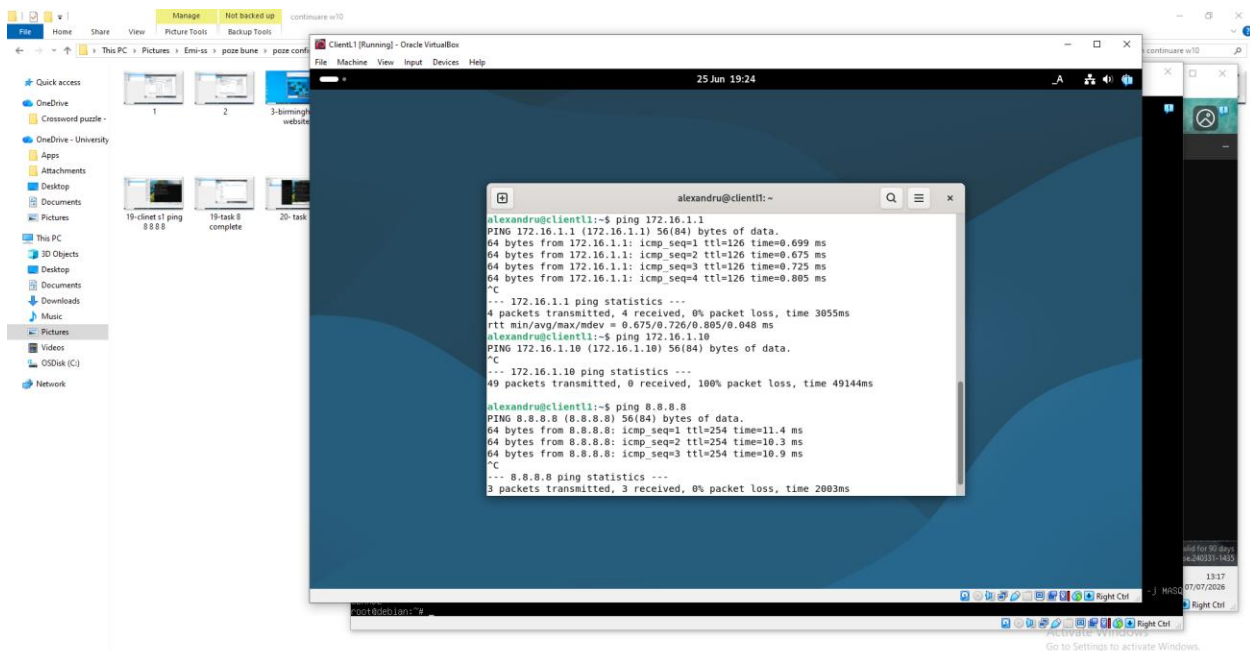


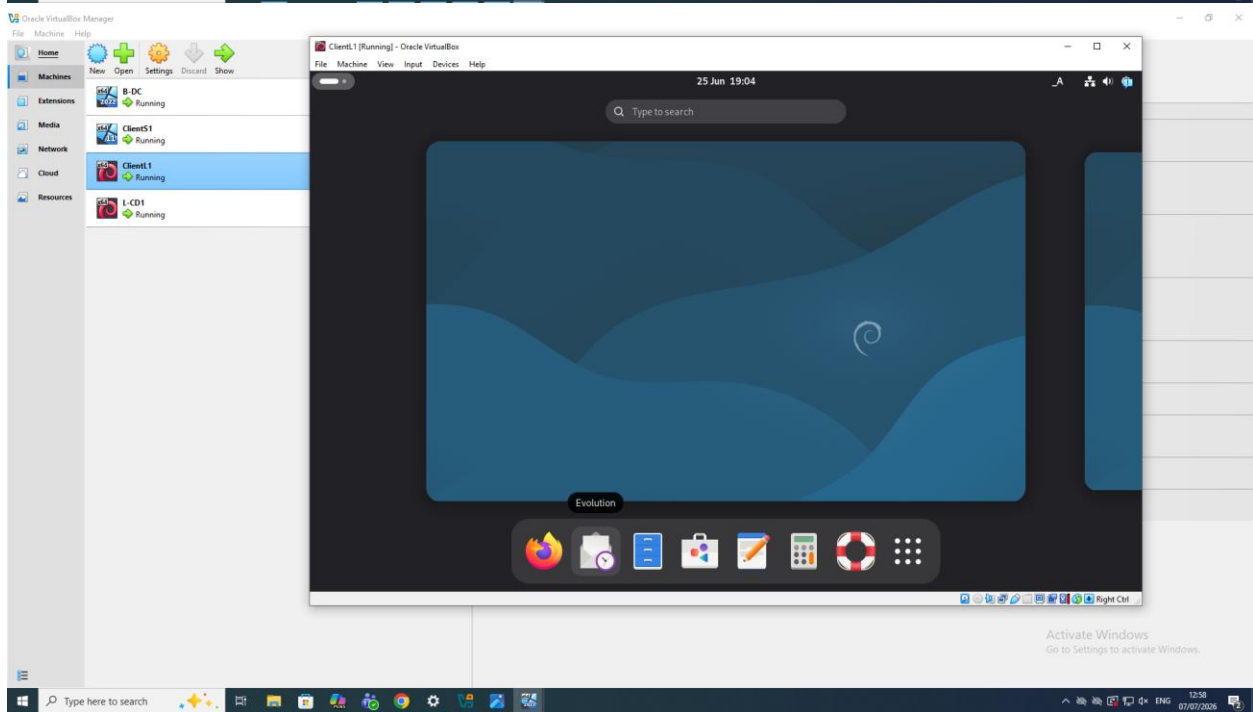
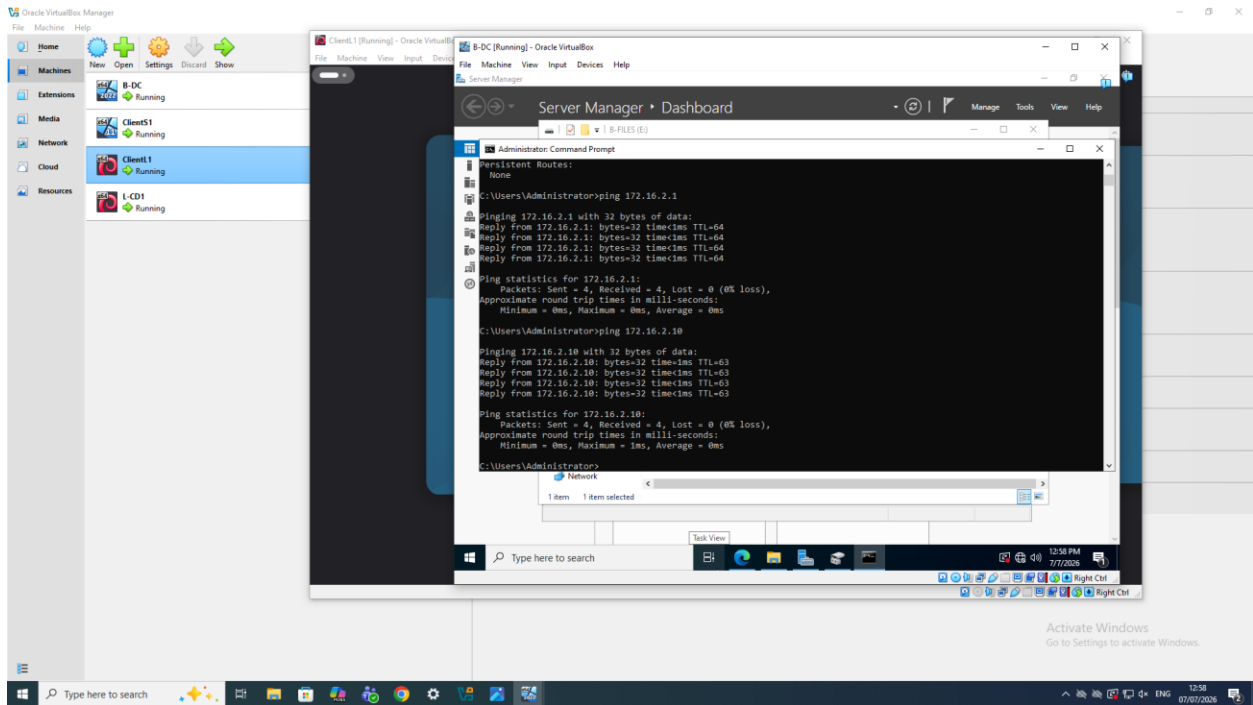


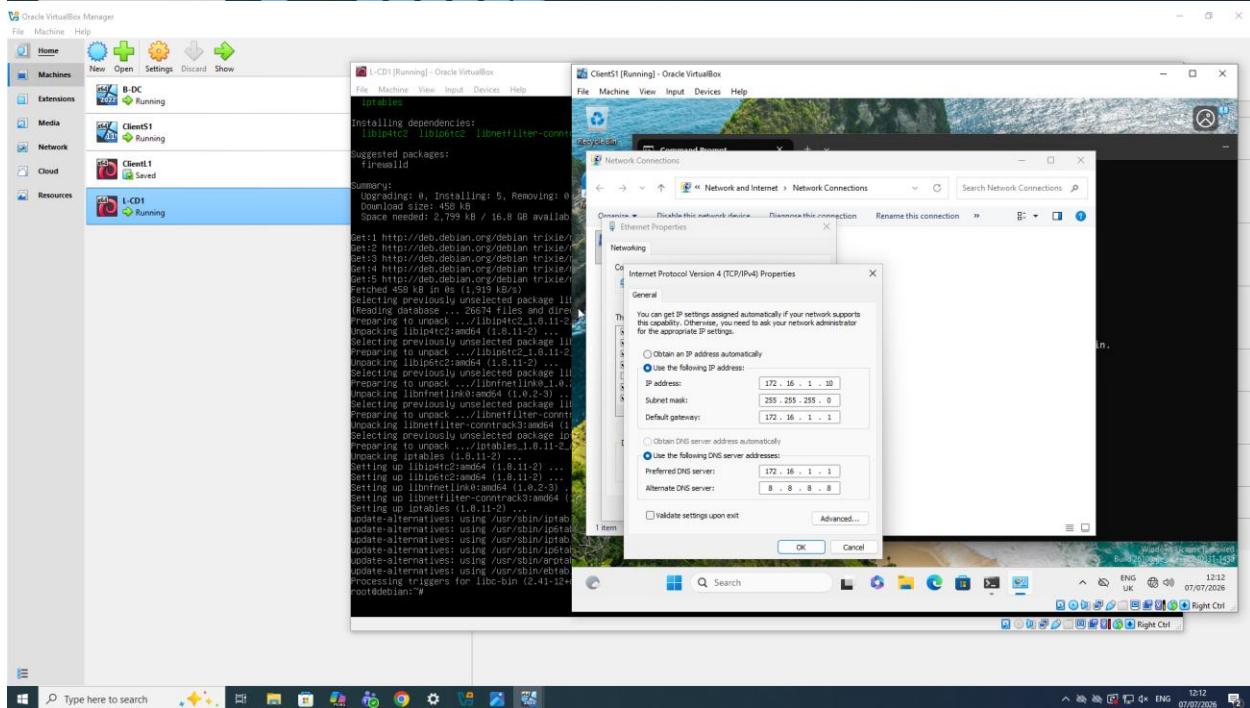
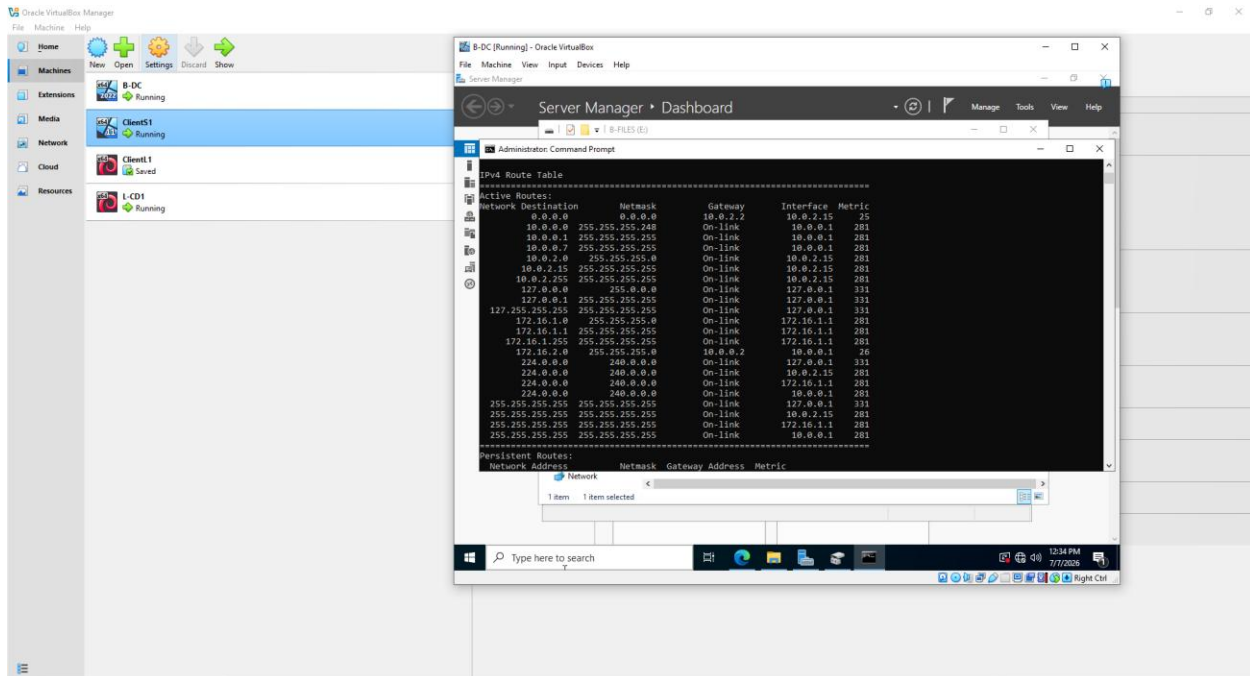
The screenshot displays a Windows 7 desktop environment. In the foreground, the 'Server Manager' console is open, showing the 'roleserver' server. Under the 'Server Groups' section, two roles are listed: 'AD DS' (Active Directory Domain Services) and 'DHCP' (Dynamic Host Configuration Protocol). Both roles have a green checkmark indicating they are installed. Below each role, a list of features is shown: 'Manageability', 'Events', 'Services', 'Performance', and 'BPA results'. In the background, the 'IP Address Range' configuration wizard is open. The wizard is titled 'New Scope Wizard' and 'IP Address Range'. It prompts the user to 'Define the scope address range by identifying a set of consecutive IP addresses.' The configuration settings for the DHCP server are shown: 'Start IP address' is 172.16.2.10, 'End IP address' is 172.16.2.20, and 'Subnet mask' is 255.255.255.0. The wizard also shows configuration settings for the DHCP client, including 'Length' and 'Subnet mask'. The desktop background is a blue wallpaper with a tree. The taskbar at the bottom shows the Start button, a search bar, and several application icons. The system tray in the bottom right corner shows the time as 4:14 PM on 7/7/2020.

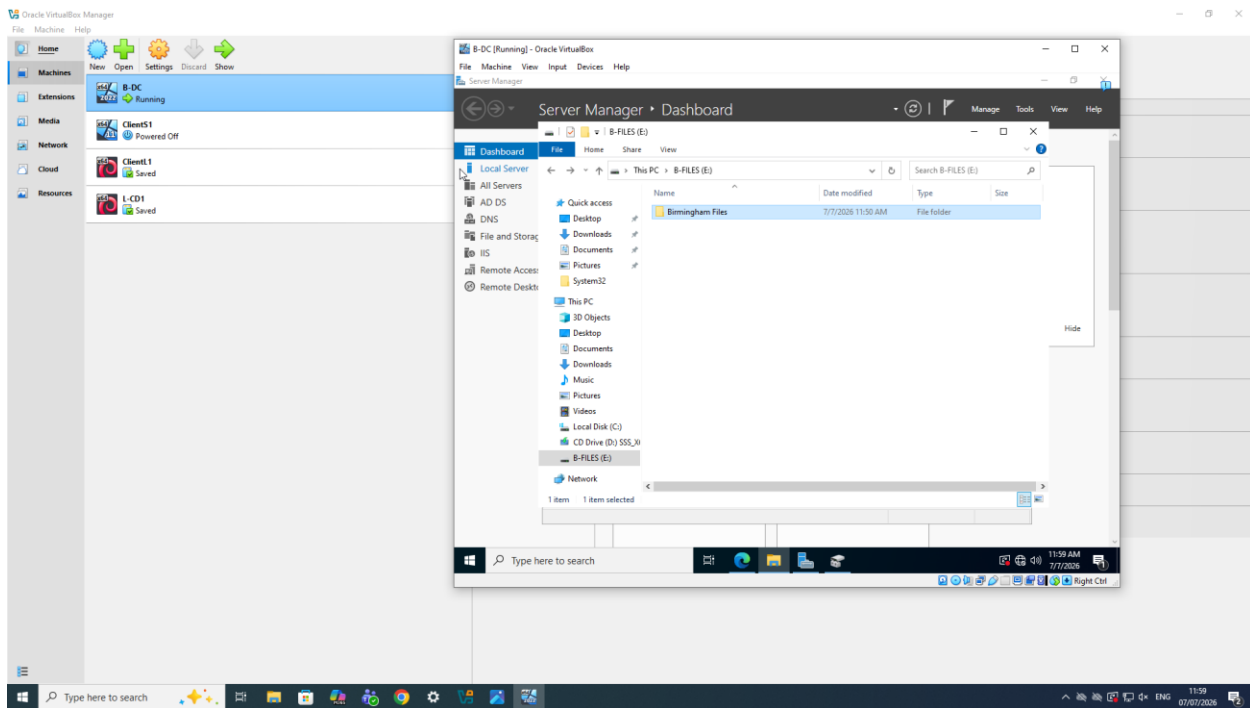
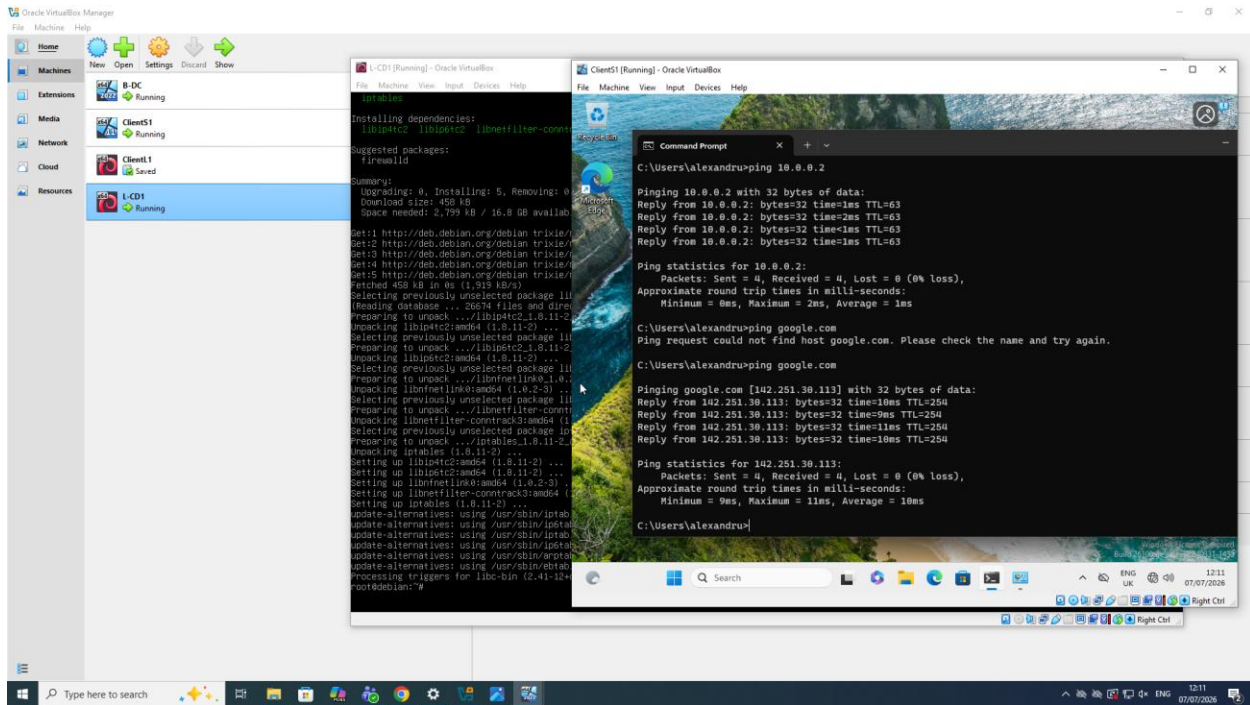


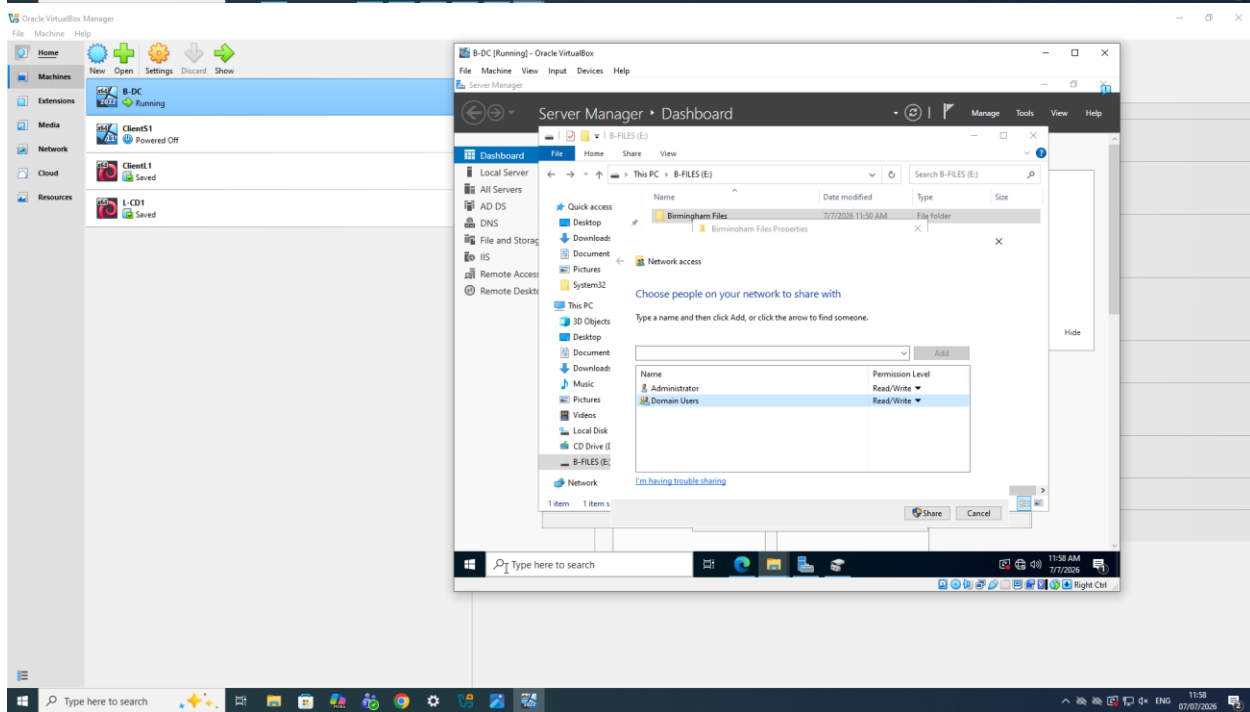
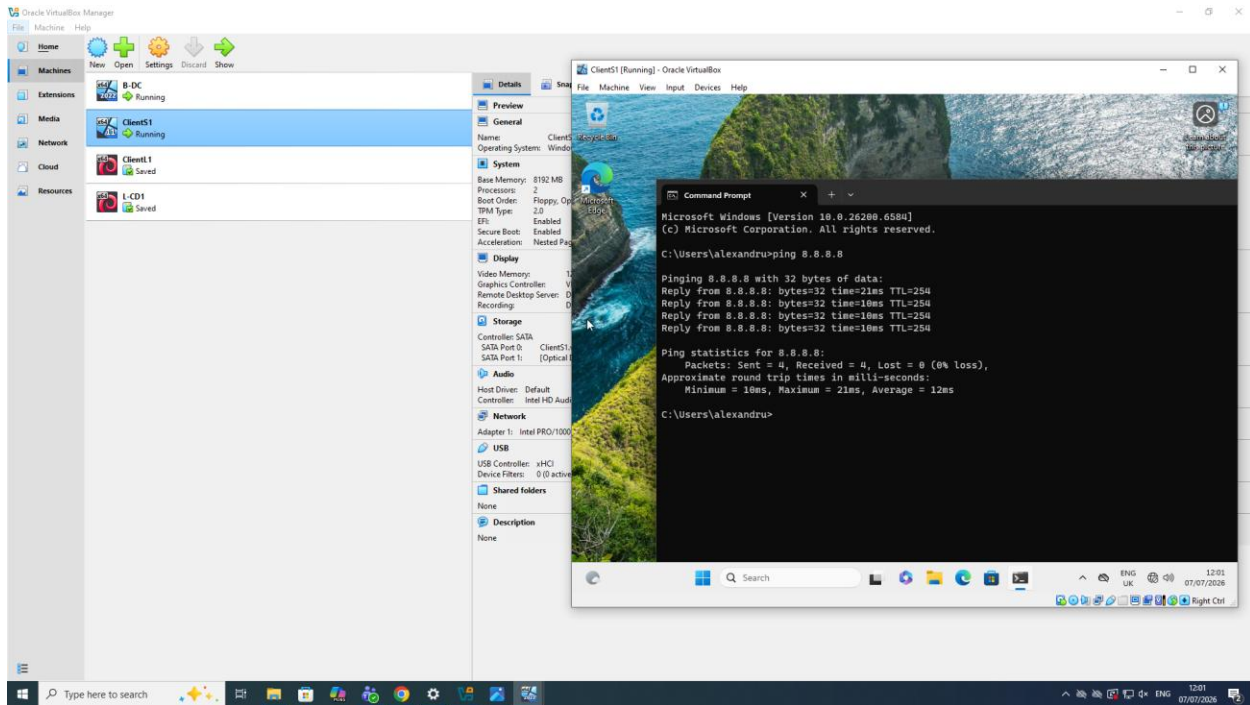


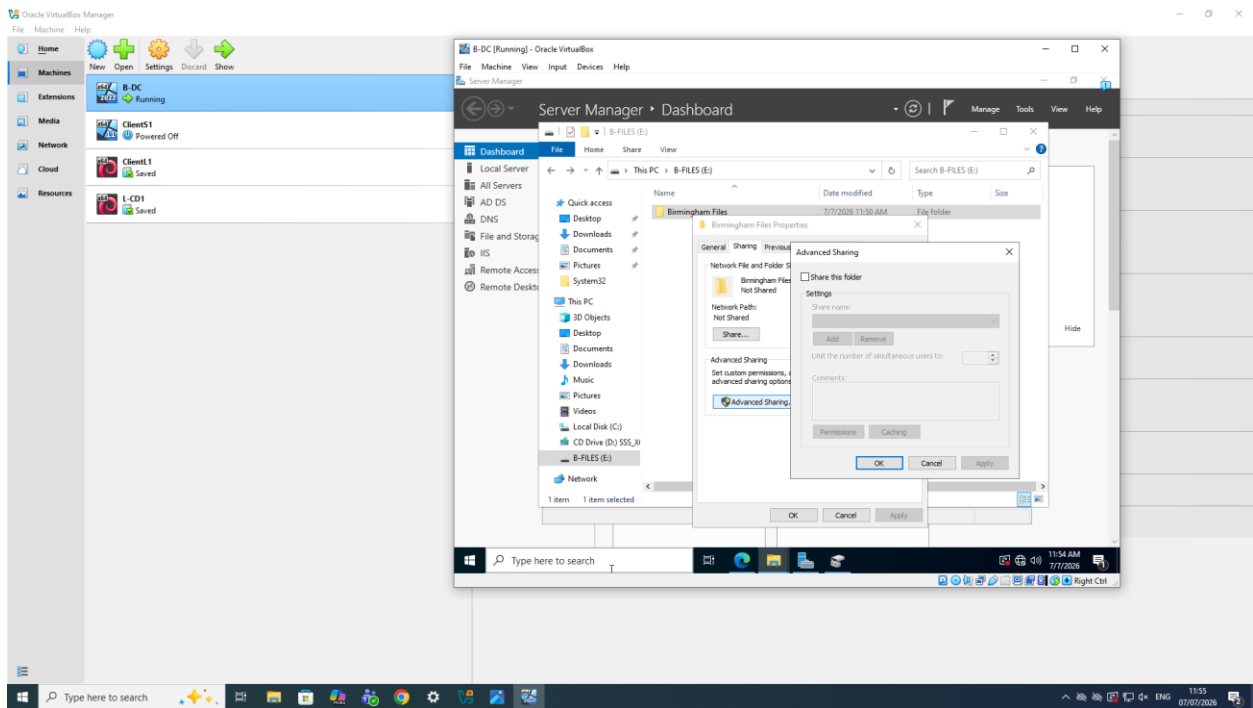
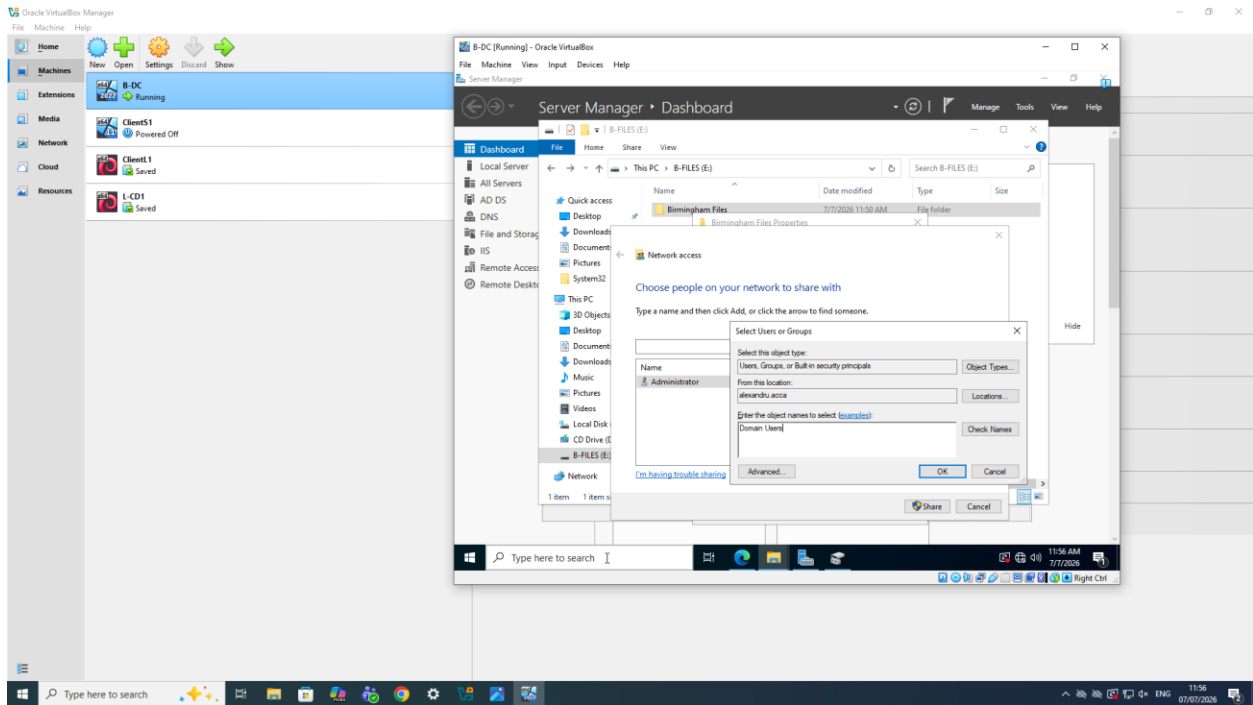


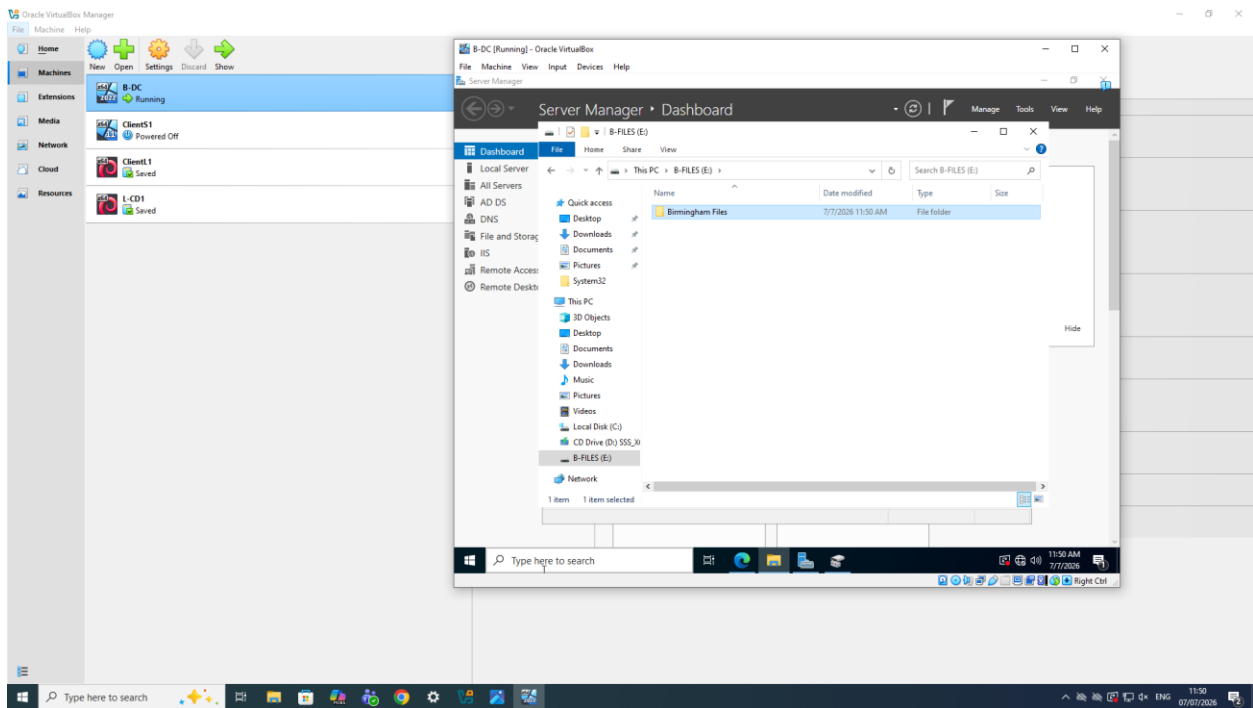
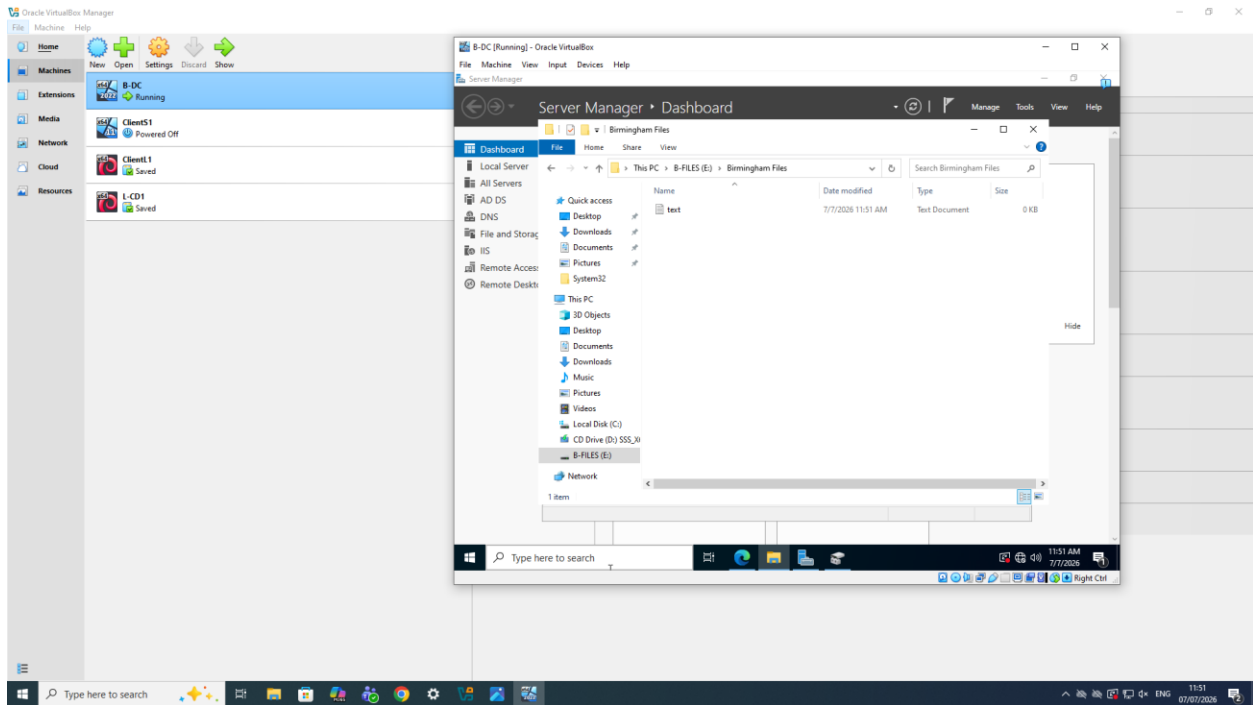


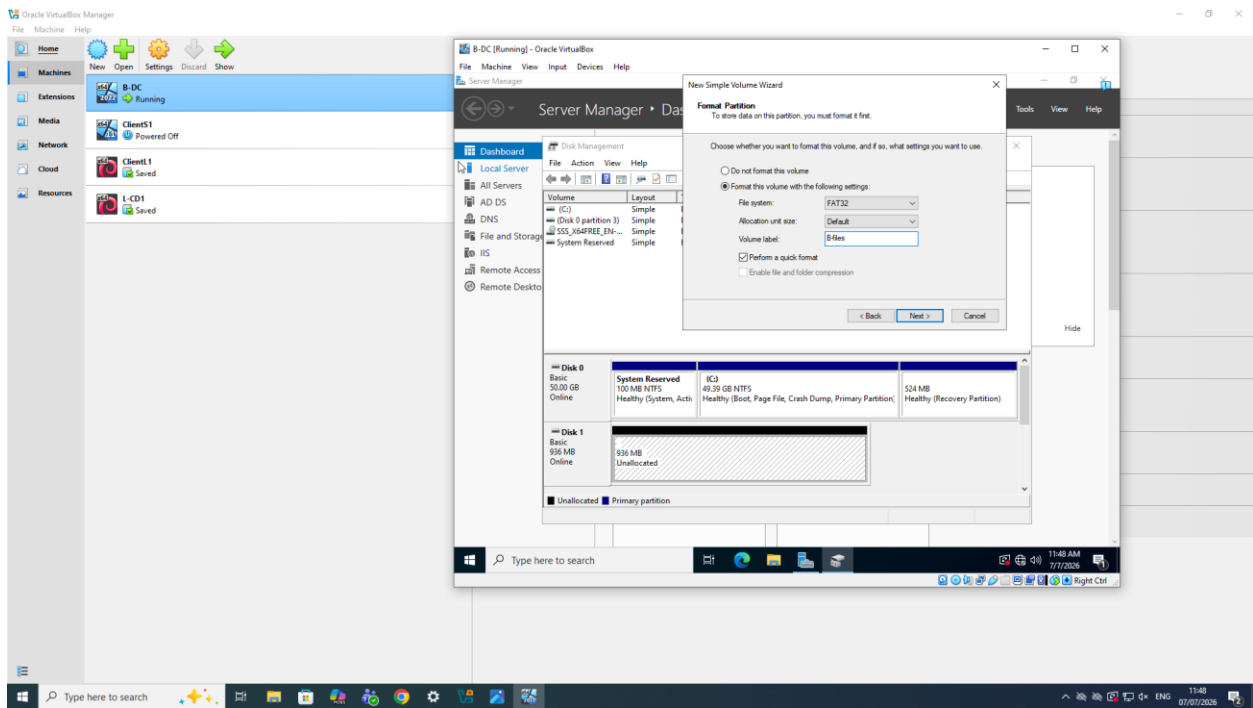
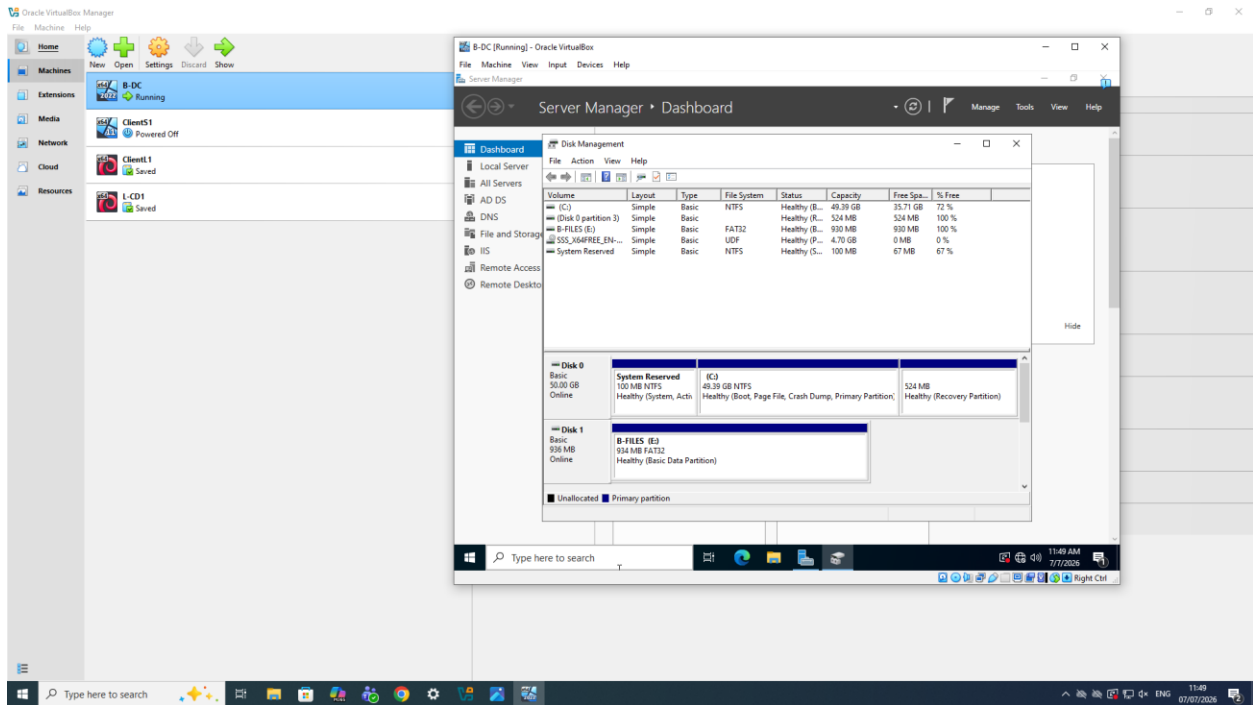


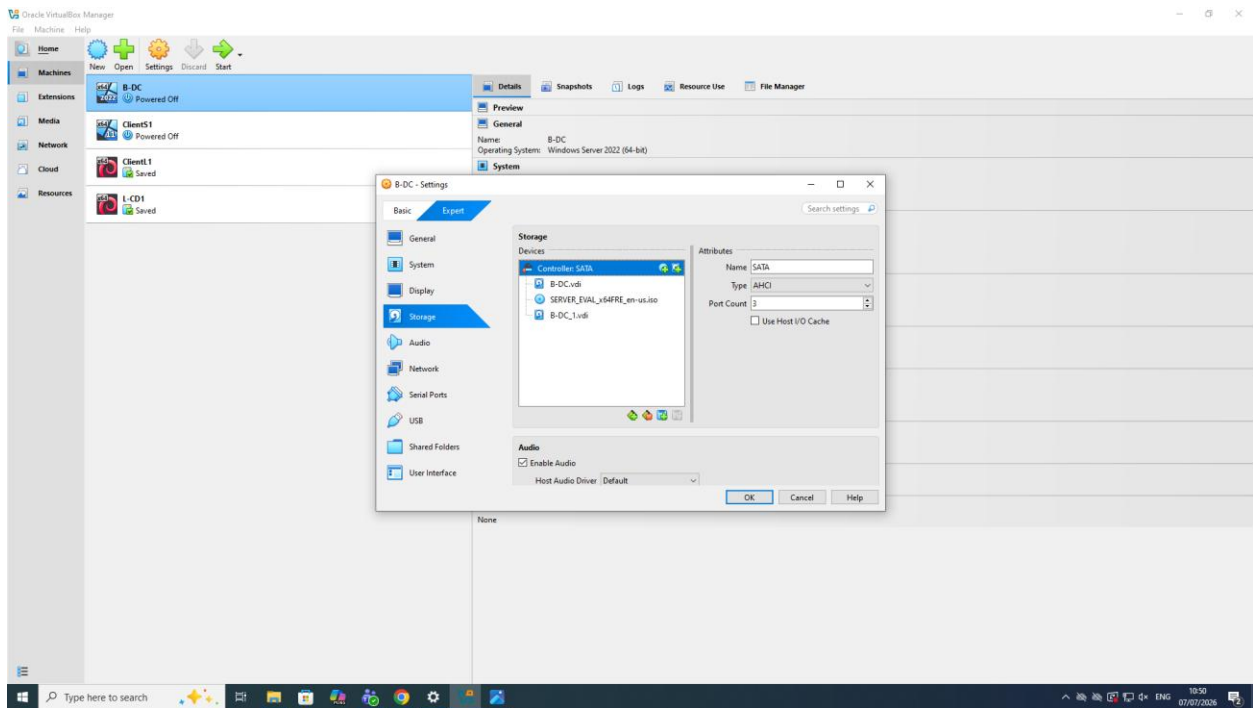
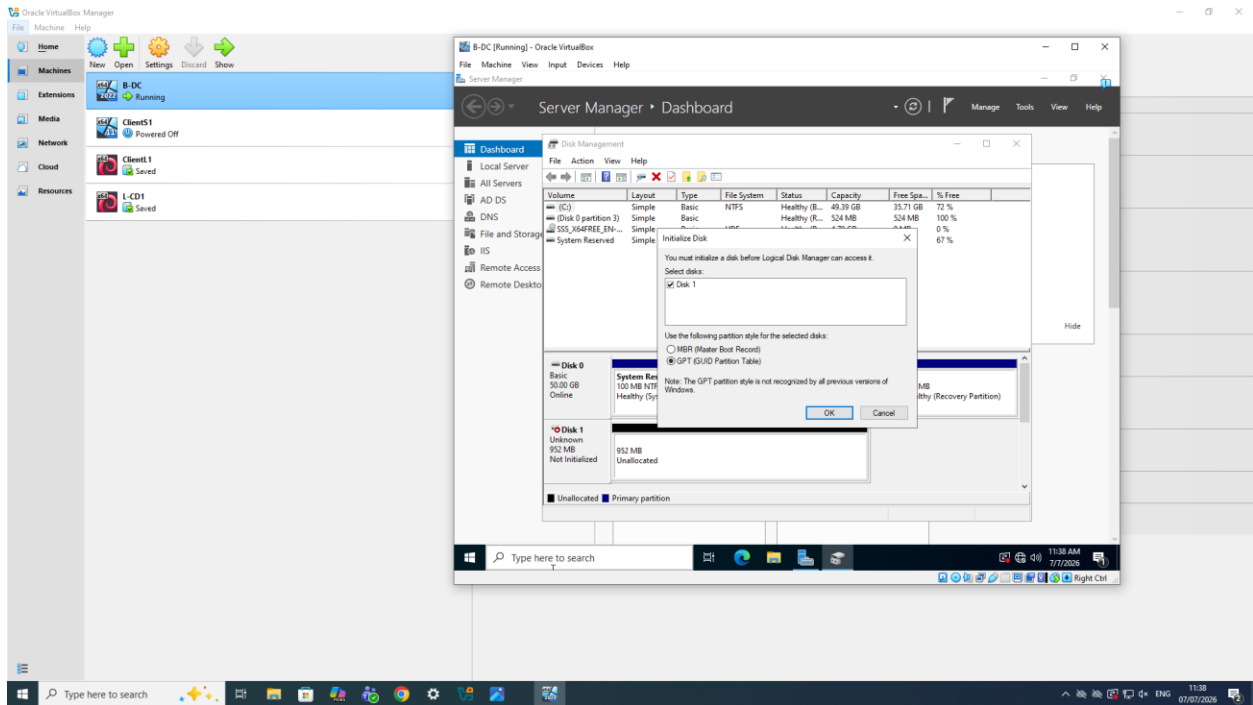


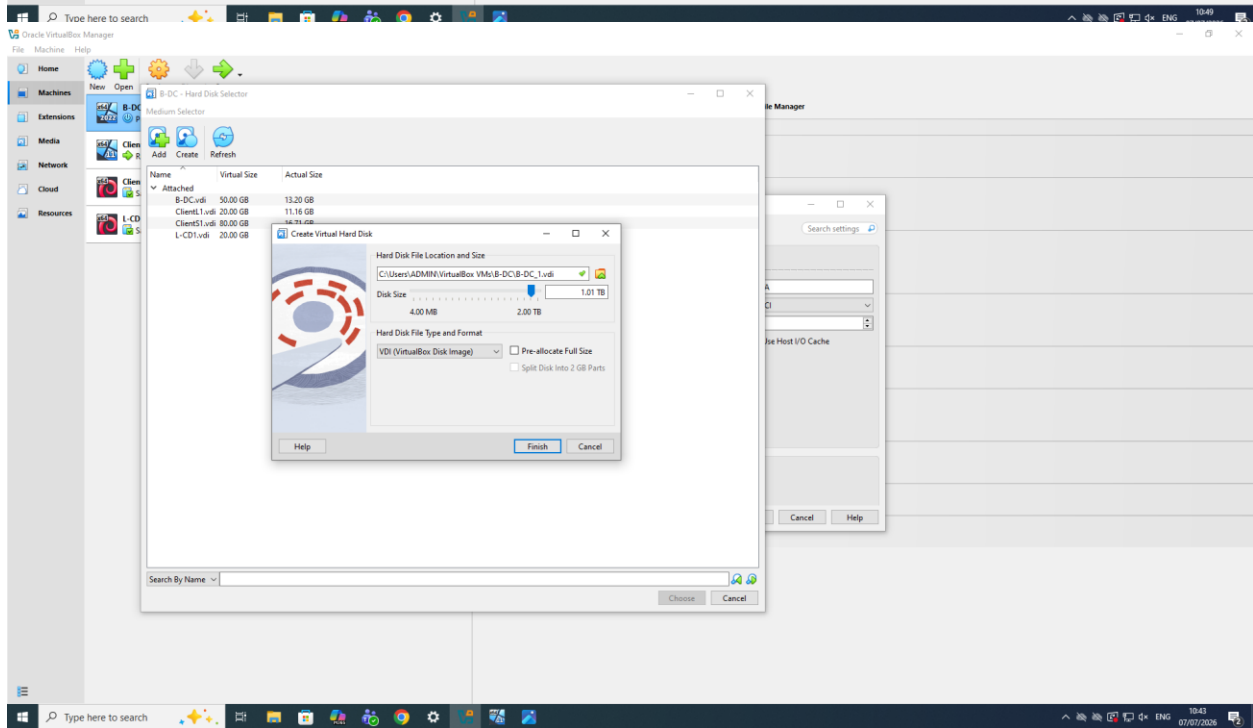
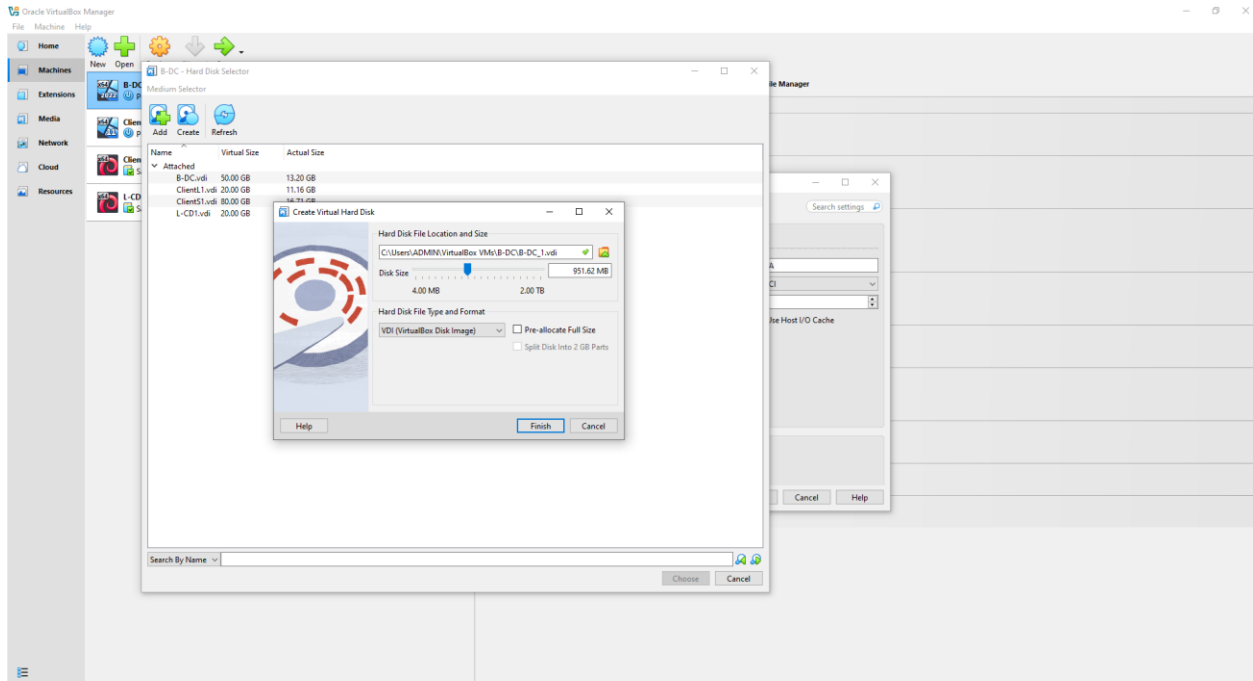


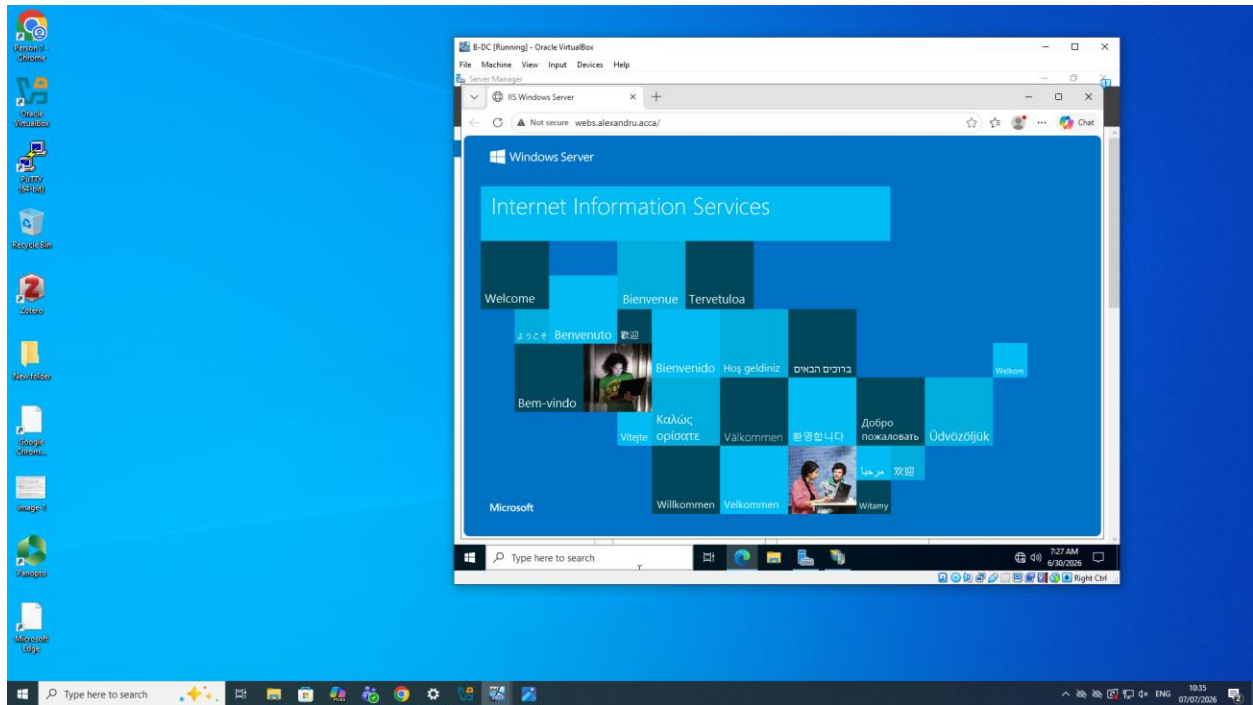


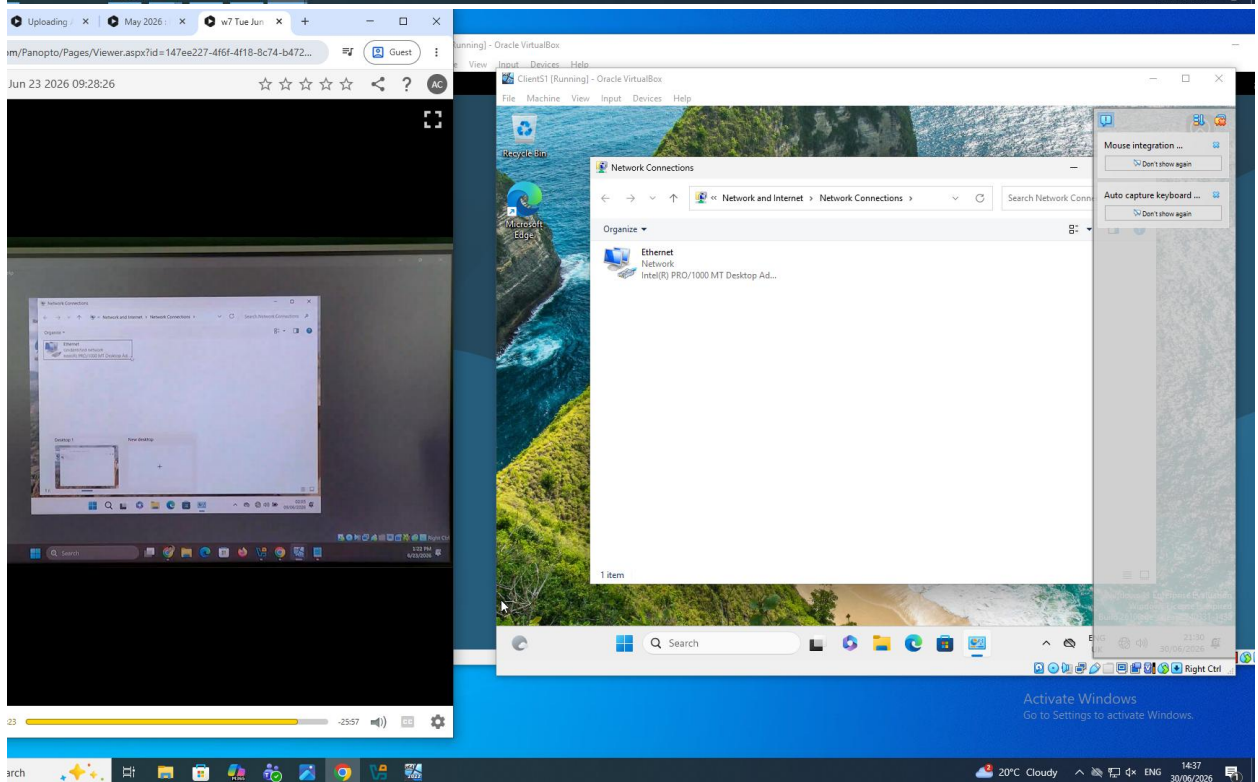
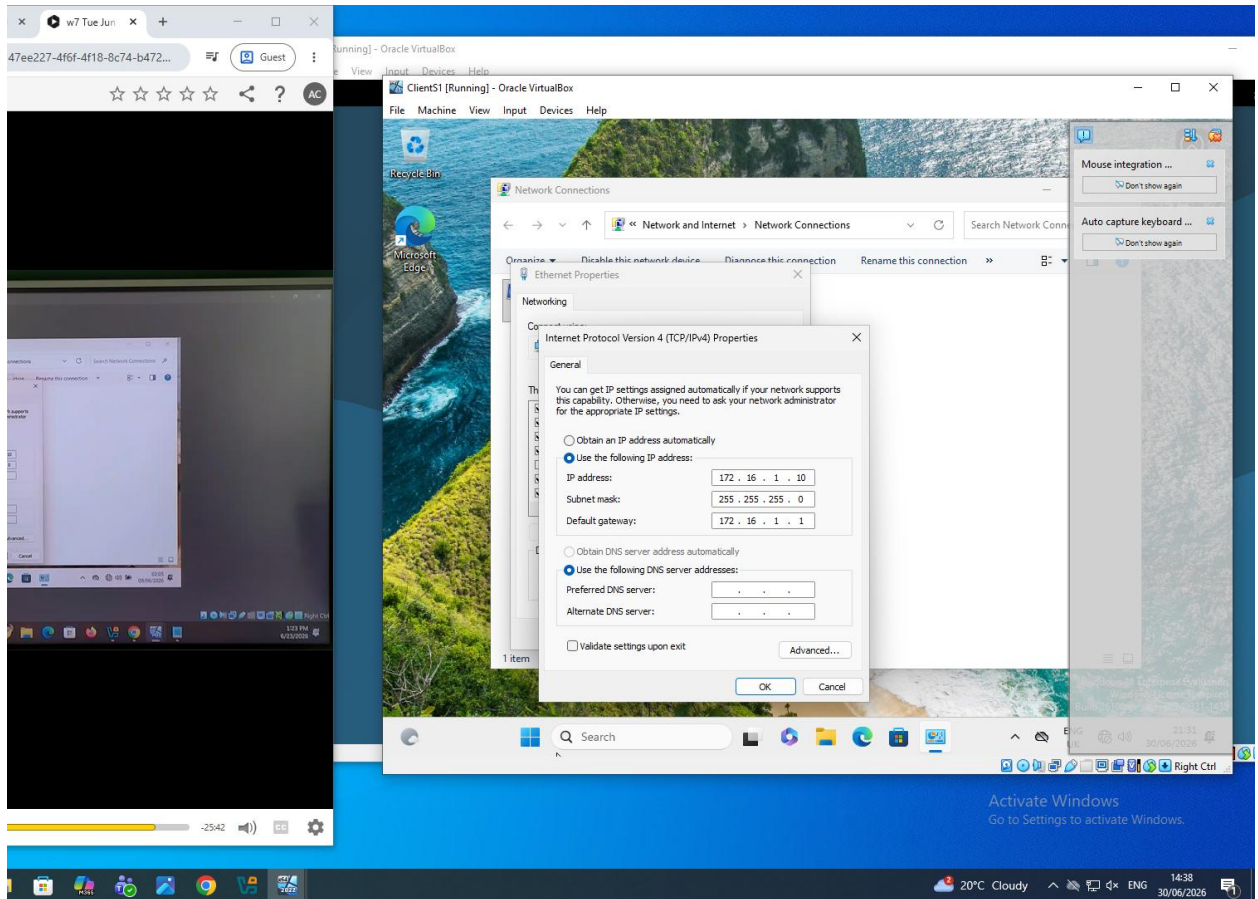


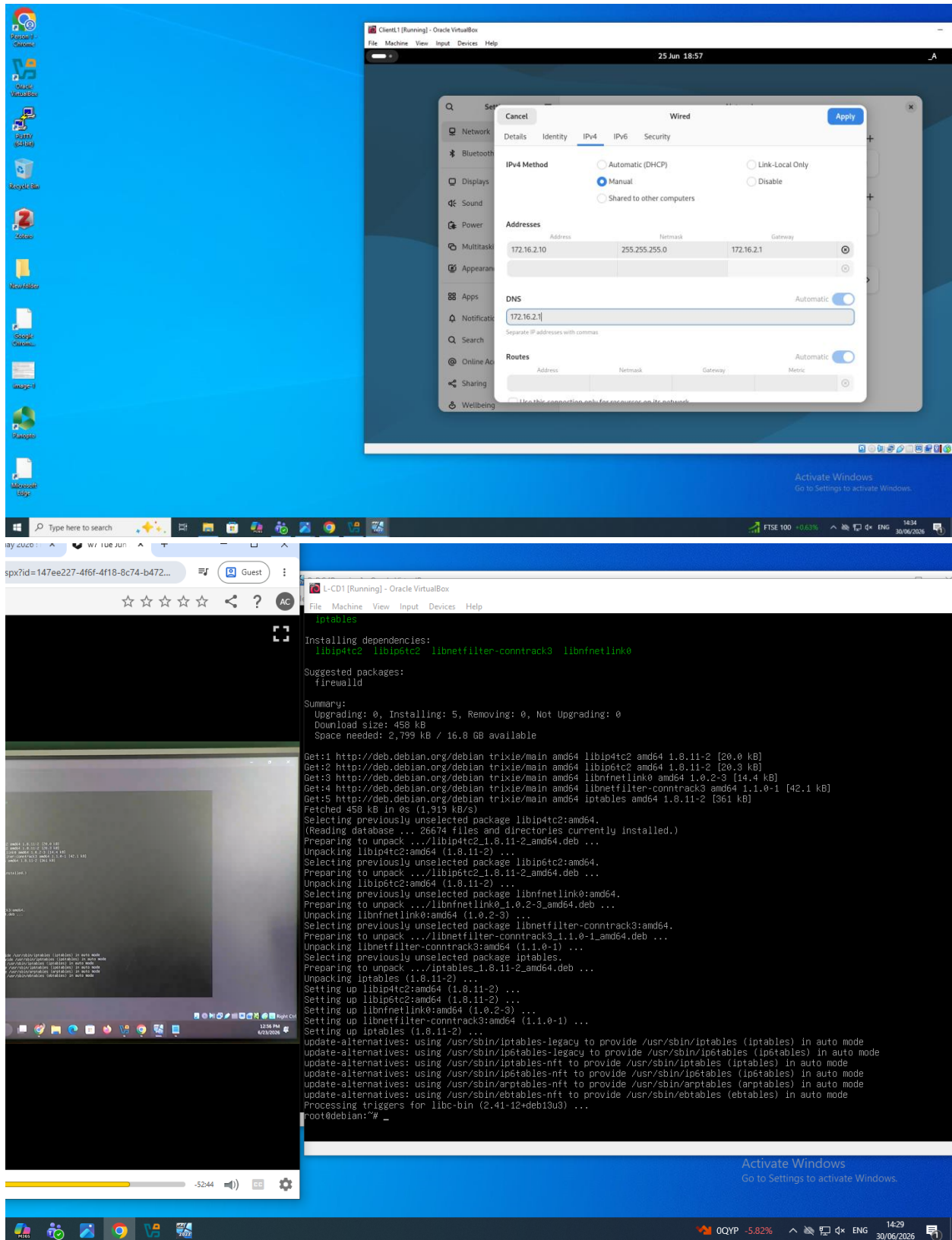


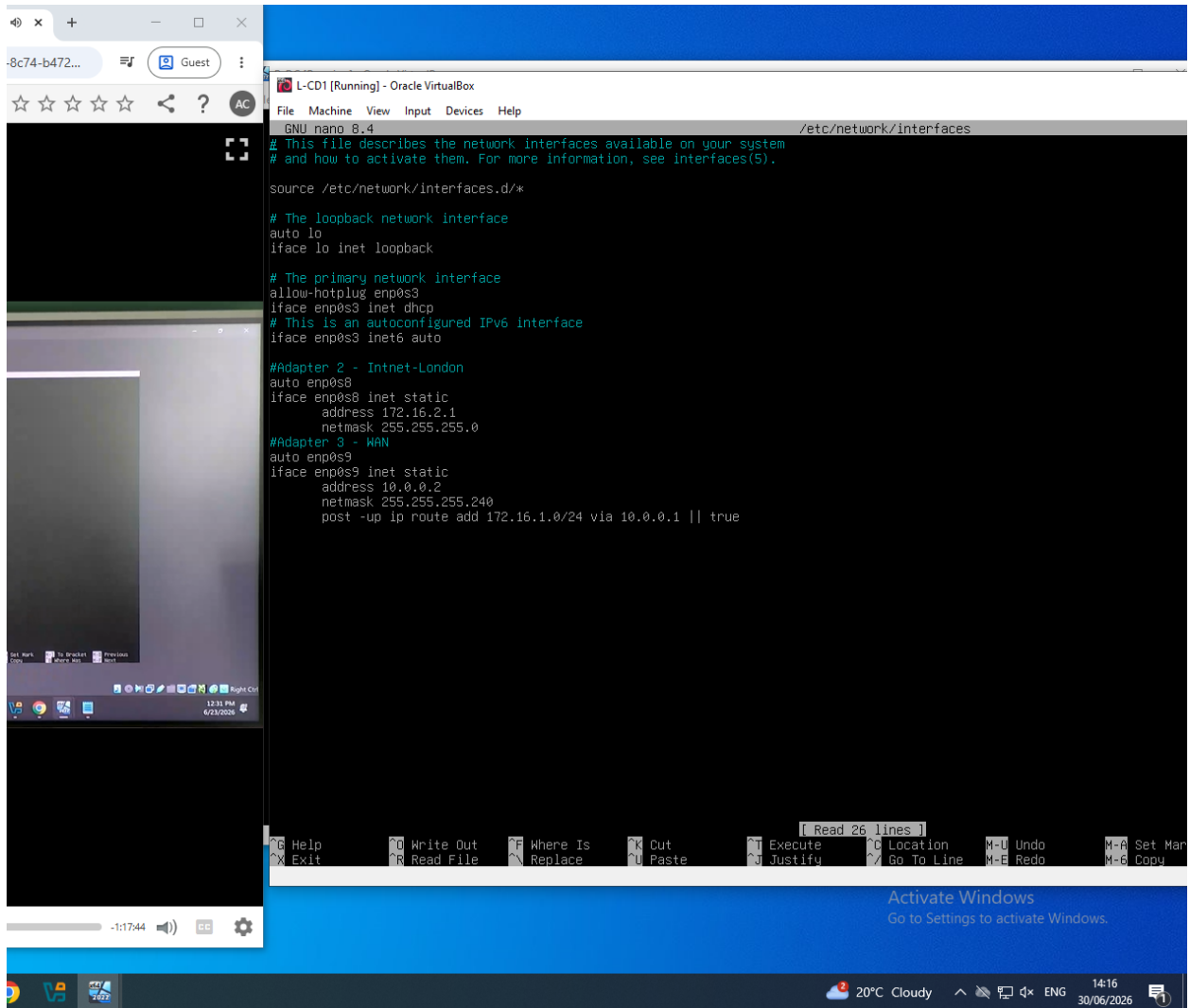












Two screenshots of a Panopto video player showing a Linux terminal session. The top screenshot shows the initial setup of network interfaces. The bottom screenshot shows the configuration of IP addresses and routes.

Top Screenshot:

```
root@debian:~# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet dhcp
# This is an autoconfigured IPv6 interface
iface enp0s3 inet6 auto

#adapter 2 - Internet-London
auto enp0s8
iface enp0s8 inet static
address 172.16.2.1
netmask 255.255.255.0

#adapter 3 - WAN
auto enp0s9
iface enp0s9 inet static
address 10.0.0.2
netmask 255.255.255.240
post-up ip route add 172.16.1.0/24 via 10.0.0.1 || true

root@debian:~#
```

Bottom Screenshot:

```
root@debian:~# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:19:0a:67 brd ff:ff:ff:ff:ff:ff
    altname enx080027190a67
    inet 10.0.2.24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86393sec preferred_lft 75553sec
    inet6 ::2/64 scope global dynamic noprefixroute
        valid_lft 86348sec preferred_lft 14348sec
    inet6 ::3/64 scope global dynamic noprefixroute
        valid_lft 85913sec preferred_lft 13913sec
    valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c6:ac:f3 brd ff:ff:ff:ff:ff:ff
    altname enx080027c6acf3
    valid_lft forever preferred_lft forever
    inet 172.16.2.1/24 brd 172.16.2.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 ::1/64 scope link proto kernel ll
        valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:19:0a:20 brd ff:ff:ff:ff:ff:ff
    altname enx080027190a20
    inet 10.0.0.2/20 brd 10.0.0.15 scope global enp0s9
        valid_lft forever preferred_lft forever
    inet6 ::2/64 scope link proto kernel ll
        valid_lft forever preferred_lft forever
root@debian:~# ip routes
Object "routes" is unknown, try "ip help".
root@debian:~# ip route
default via 10.0.0.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 1002
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.1
172.16.1.0/24 dev enp0s8 proto kernel scope link src 172.16.2.1
root@debian:~# sysctl -w net.ipv4.ip_forward=1
sysctl: command line(0): invalid syntax, continuing...
root@debian:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@debian:~#
```

