

4/26/2026

Network Operating Systems and Services

Configure and manage the Virtualised Enterprise network
Assessment 2

Network Operating Systems and Services

ACCA 5023

Student Name: Evgeni Veselinov Iliev

Student ID: 2424555

Group: 1

Lecturer's Name: Dr. Sadeque Imam Shaikh

Table of Contents

Introduction	2
1. Routing	3
1.1 Routing in Swansea Network	3
2. Domain Server (Swansea.com)	4
2.1. Create a forest	4
2.2. Create all appropriate A records for all servers on SWAN Network.....	5
2.3. Create a reverse lookup zone creating PTR records for all servers.	5
3. Encrypted Connection between Swan and UWTSD.....	6
3.1. Configure Site-to-Site VPN to SWAN (Windows) Network.	6
4. Users	7
4.1. Create user accounts	7
5. Domain Membership	8
5.1. Join client to the domain.	8
6. DHCP Server	9
6.1. Configure Swansea-DC as DHCP Server.	9
6.2. All the Clients should receive IP Address automatically via DHCP Server	10
7. Test and Troubleshoot	10
7.1. Test the network for Connectivity	11
8. Disk Drive	12
8.1. Mount second disk drive.....	12
9. IIS Server	13
9.1. Create website and enable windows internal authentication.....	13
10.Remote Desktop Services	14
10.1. Configure remote access for Swansea-DC from any other machines in the network.....	14
Conclusion.....	15
References	16

Introduction

This report explains the practical network implementation completed for the **SWANSEA.COM** domain. The main Windows Server was configured as **Swansea-DC** with the manual IP address **192.168.100.10**. The client machine was first configured manually with **192.168.100.20** and later changed to automatic DHCP. After DHCP was working, the client received the IP address **192.168.100.13**.

The main tasks included routing, Active Directory, DNS, VPN, user accounts, domain membership, DHCP, testing, shared storage, IIS, and Remote Desktop access. These services are important because a business network needs more than just connected machines. It also needs proper authentication, name resolution, secure access, and central management. In this work, each service was configured and then tested to make sure it supported the rest of the network.

1. Routing

Routing was configured in the Swansea network so that devices could communicate properly. Routing is important because even if devices are connected, they may not be able to send traffic correctly without the right routing settings. Windows Server Routing and Remote Access Service can be used to support routing and remote access functions [1].

1.1 Routing in Swansea Network

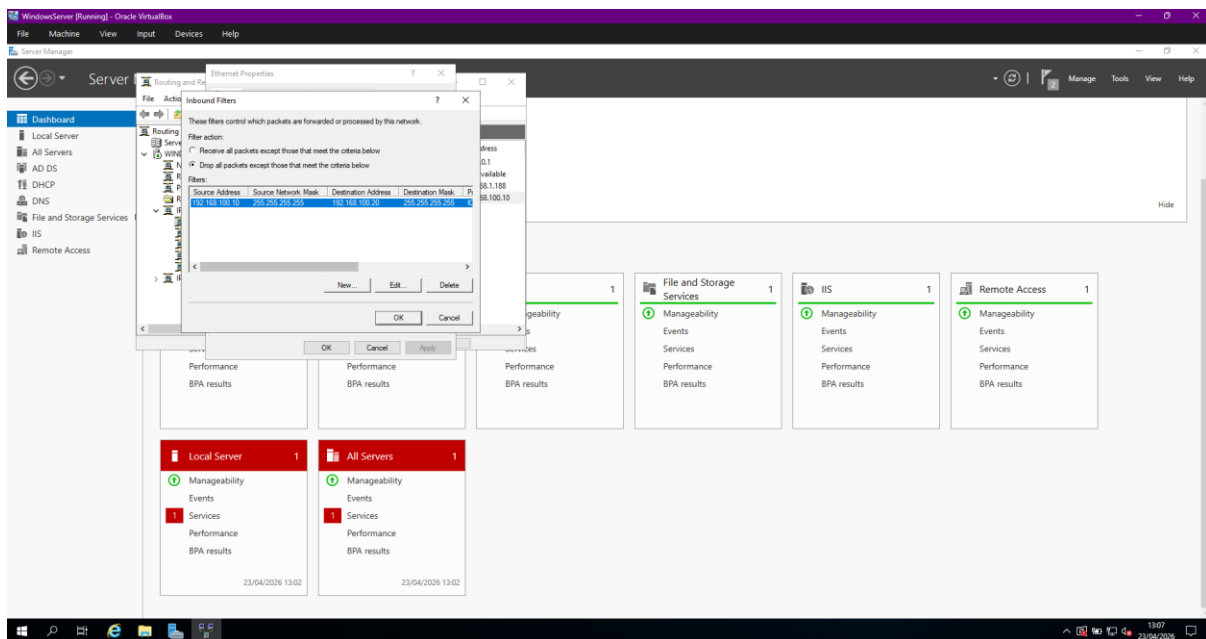


Figure 1 shows the routing configuration on Swansea-DC.

Firewall rules were also checked because routing can fail if the firewall blocks the traffic. ICMP was allowed for testing because ping is a simple way to check if two machines can communicate. This helped confirm connectivity between the client and server. However, from a security point of view, ICMP should not always be fully open in a real business network. It is useful for troubleshooting, but it can also show information about active devices. This shows that network administrators need to balance testing and security.

2. Domain Server (Swansea.com)

Swansea-DC was promoted to a domain controller, and a new forest was created using the domain name **SWANSEA.COM**. Active Directory Domain Services was used because it gives a central place to manage users, computers, and authentication [2].

2.1. Create a forest

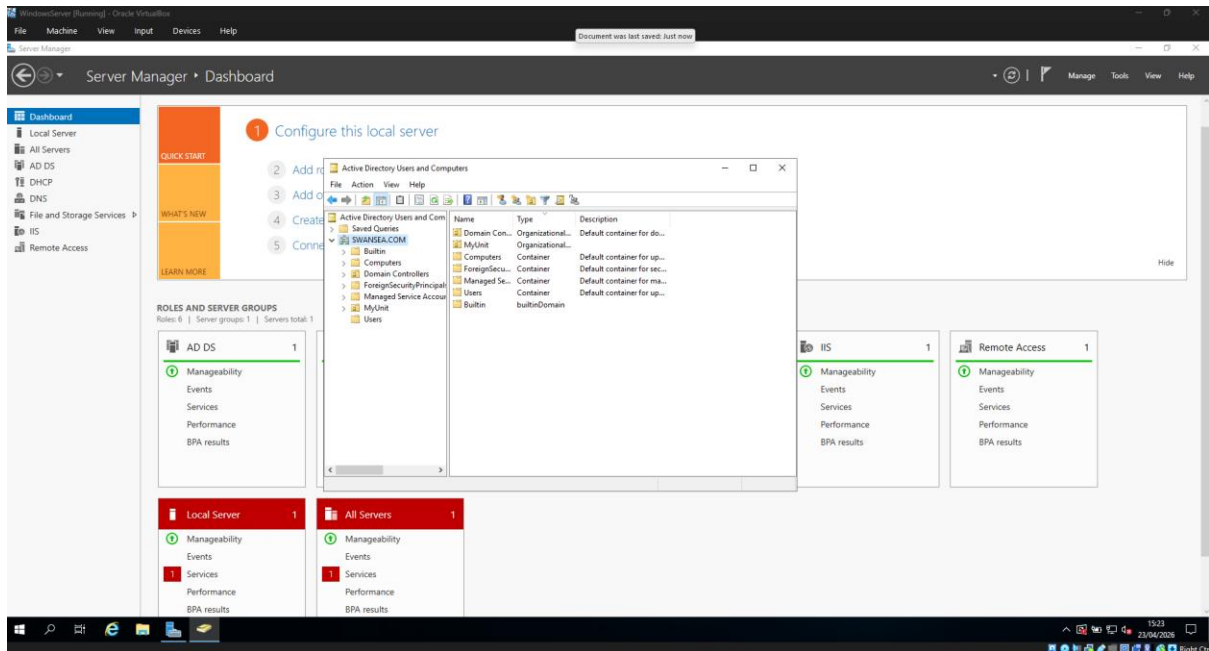


Figure 2 shows the SWANSEA.COM forest creation.

After the domain was created, DNS records were configured. A records were created for the servers in the SWAN network. These records allow server names to resolve to IP addresses. A reverse lookup zone was also created with PTR records, which allow IP addresses to resolve back to hostnames. DNS is an important part of TCP/IP networks because it changes readable names into IP addresses [3].

2.2. Create all appropriate A records for all servers on SWAN Network

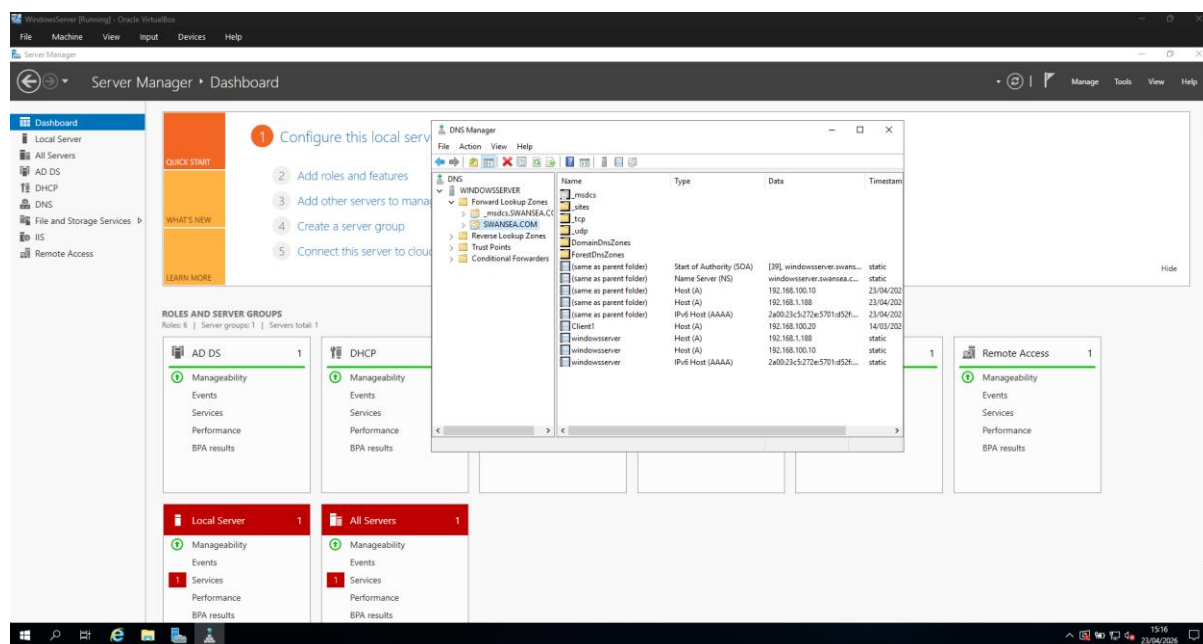


Figure 3 shows the A records created for the servers.

2.3. Create a reverse lookup zone creating PTR records for all servers.

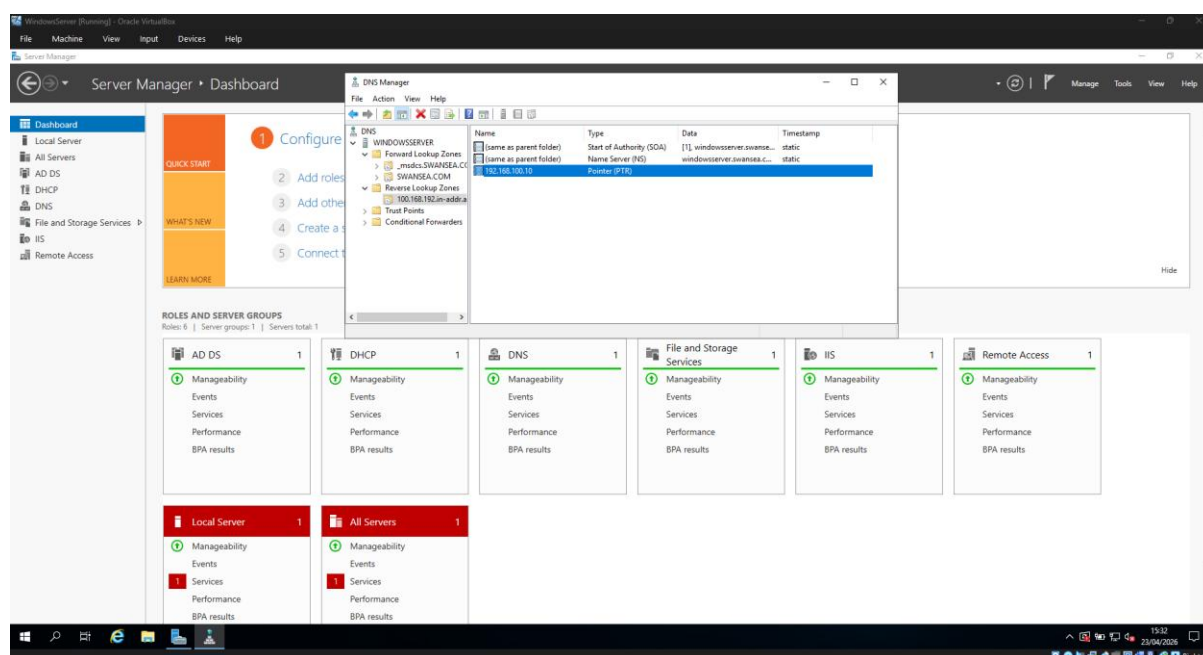


Figure 4 shows the A records created for the servers.

This task was important because Active Directory depends heavily on DNS. If DNS is not configured correctly, the client may fail to join the domain, or users may have problems logging in. From this task, I understood that DNS is not only a small background service. It is one of the main parts of a working domain network.

3. Encrypted Connection between Swan and UWTSD

A site-to-site VPN was configured between the **Swan** and **UWTSD** networks. The VPN user account used was **VPN1**. The purpose of the VPN was to create a secure connection between the two networks, instead of allowing traffic to pass without protection. IPsec VPNs are commonly used to protect data moving between networks by using authentication and encryption [5].

3.1. Configure Site-to-Site VPN to SWAN (Windows) Network.

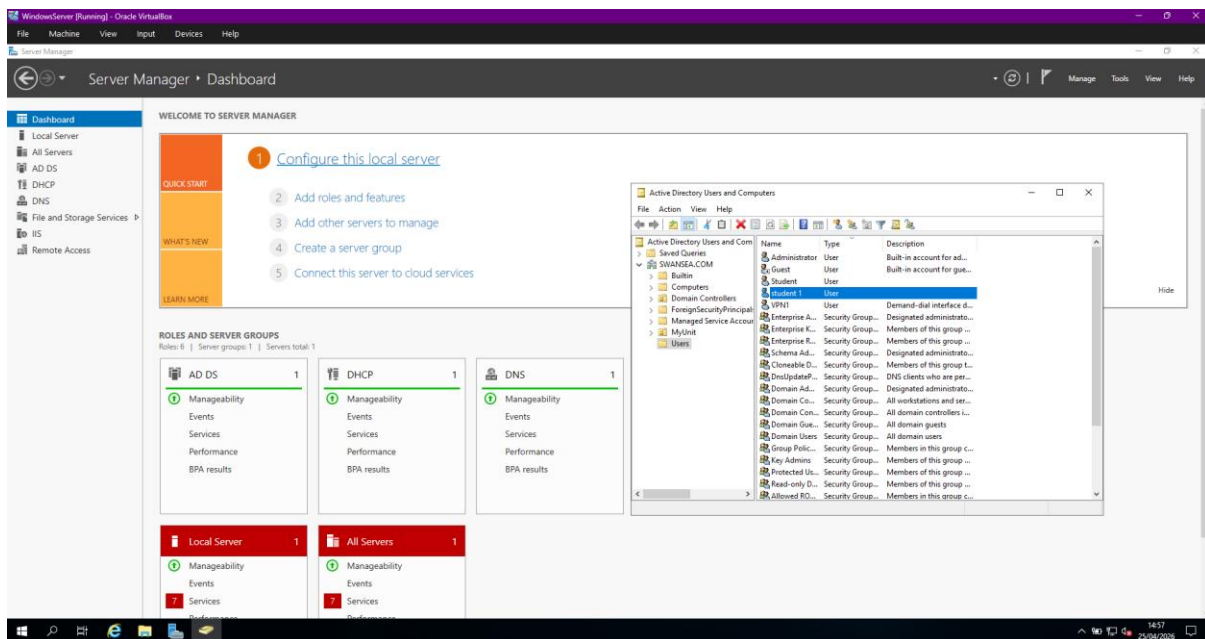


Figure 5 shows the VPN configuration using the VPN1 account.

This configuration helped the two networks communicate more securely. However, a VPN is only strong if it is configured correctly. For example, the VPN account should have a strong password and should only be used for the correct purpose. If the VPN account is weak or shared with too many users, it can become a security risk. Therefore, the VPN setup was not only about making the connection work, but also about making sure access was controlled.

4. Users

User accounts were created in the **SWANSEA.COM** domain. One example user account created was **Student.1**. Creating users in Active Directory is better than creating separate local accounts on each machine because the administrator can manage users from one central place.

4.1. Create user accounts

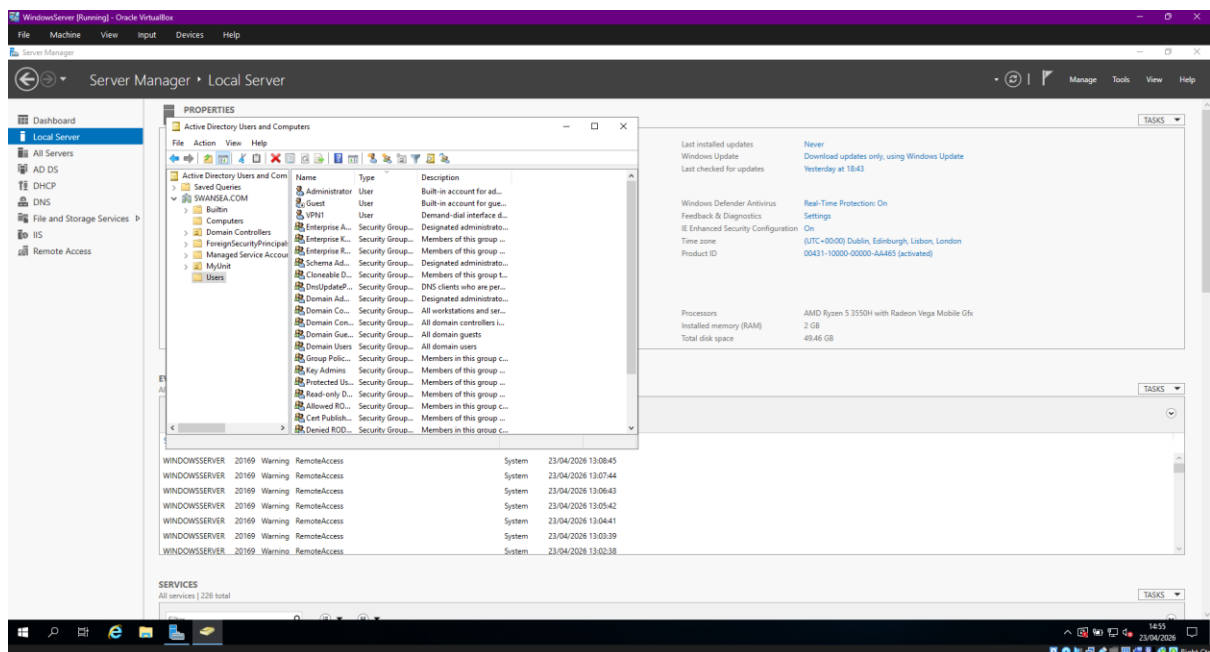


Figure 6 shows the created user accounts, including Student.1.

This makes the network easier to manage. For example, if a user no longer needs access, their account can be disabled from Active Directory. It also helps with shared folders, login control, and future Group Policy settings. However, account management still needs to be planned carefully. Usernames should follow a clear format, and passwords should be strong. NIST guidance supports the use of proper access control to reduce security risks [6].

5. Domain Membership

The client machine was joined to the **SWANSEA.COM** domain. Before DHCP was tested, the client used the manual IP address **192.168.100.20**. After joining the domain, the client could authenticate using the domain controller instead of only using a local account.

5.1. Join client to the domain.

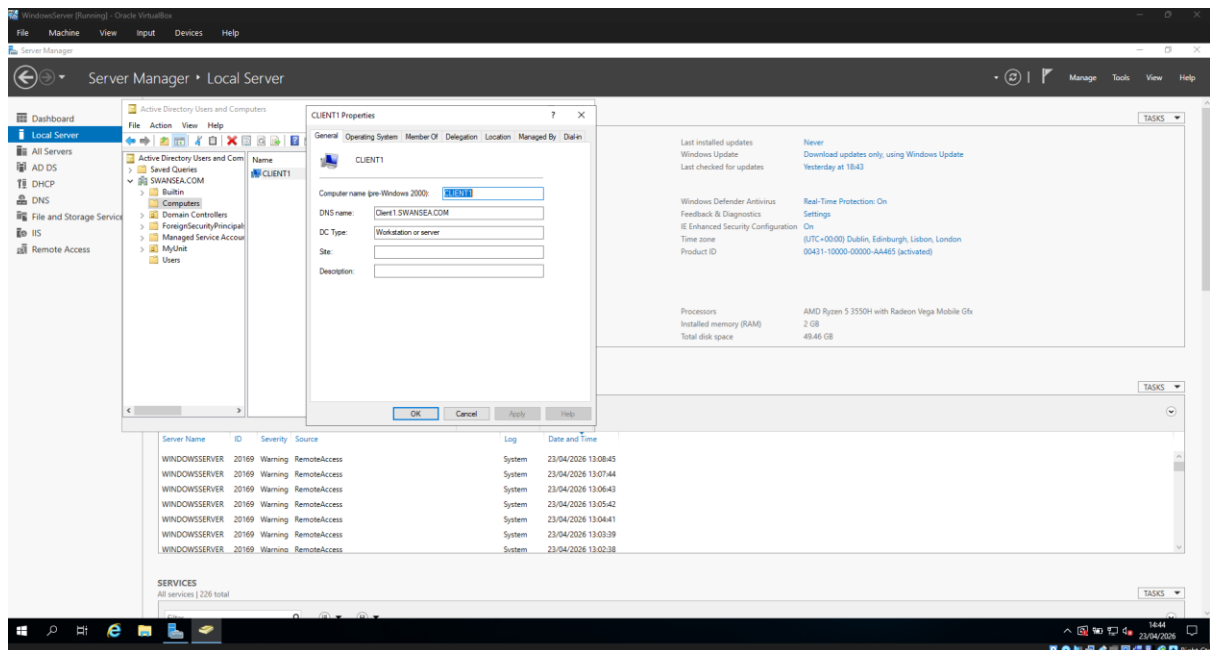


Figure 7 shows the client successfully joined to the SWANSEA.COM domain.

This task helped prove that other services were working. For example, if DNS or IP settings were wrong, the client would normally fail to join the domain. This means domain membership is a useful test point. It shows that the server, client, DNS, and Active Directory are working together. In a real organisation, joining computers to the domain also makes it easier to manage security settings across many machines.

6. DHCP Server

Swansea-DC was configured as the DHCP server. DHCP was used so that clients could receive IP addresses automatically instead of being configured manually. DHCP is designed to automatically provide IP configuration to devices on a TCP/IP network [4].

6.1. Configure Swansea-DC as DHCP Server.

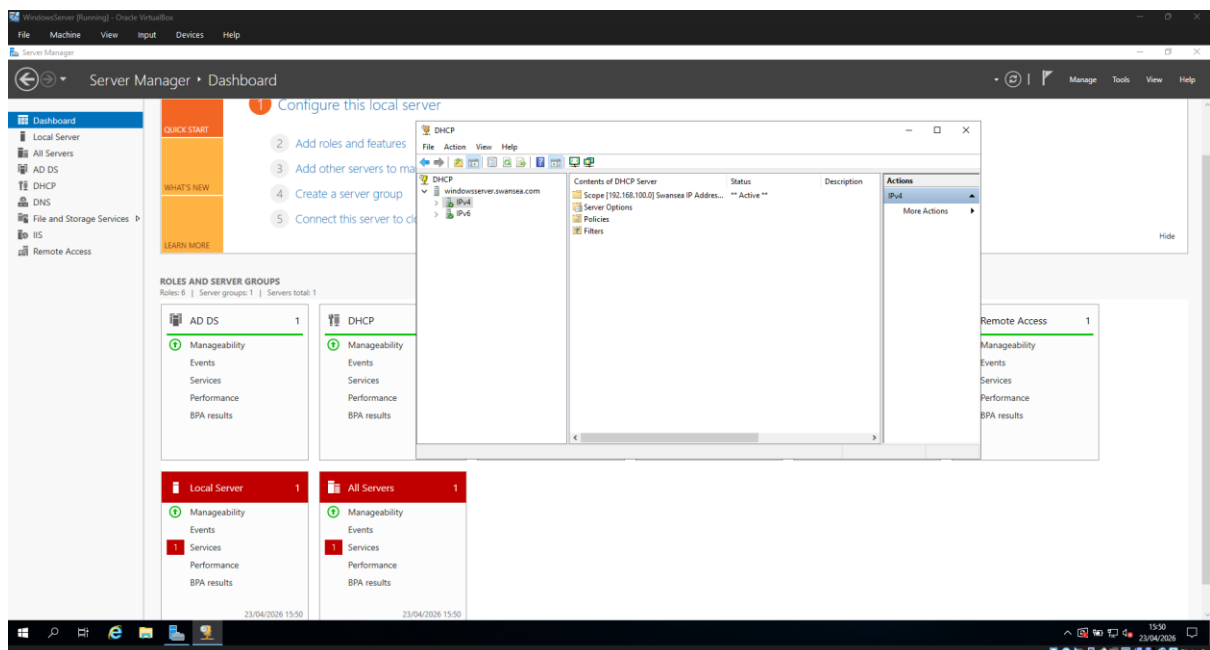


Figure 8 shows the DHCP scope configured on Swansea-DC.

6.2. All the Clients should receive IP Address automatically via DHCP Server

After DHCP was configured, the client was changed from manual IP addressing to automatic IP addressing. The client then received the IP address **192.168.100.11**.

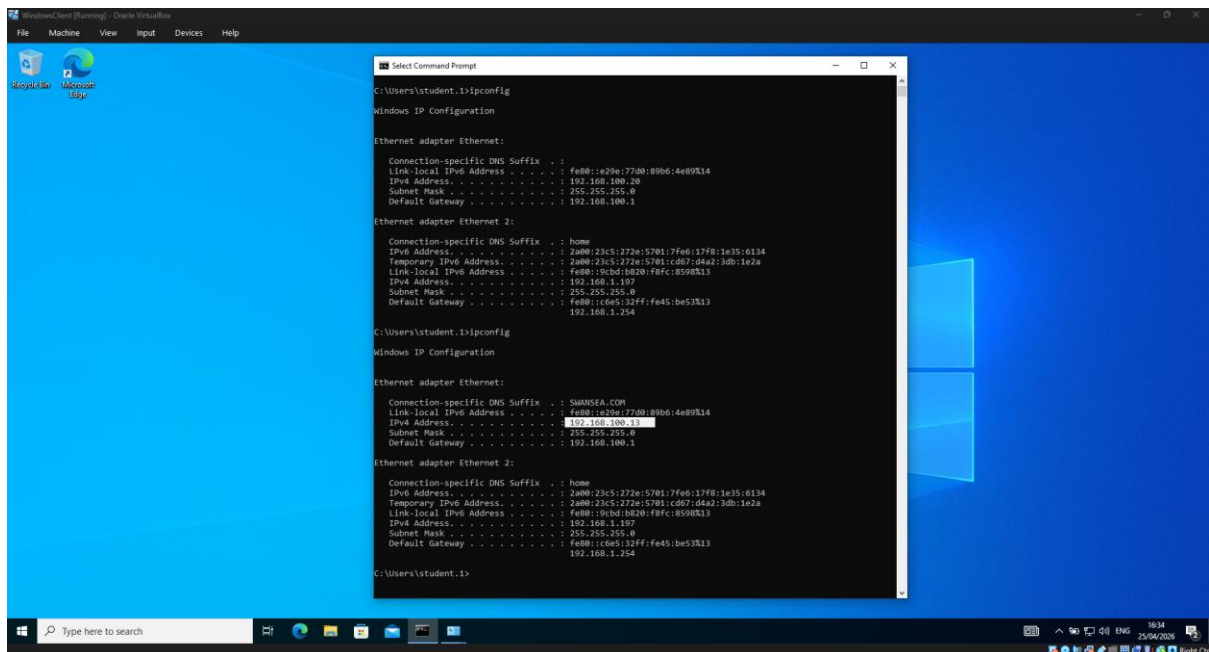


Figure 9 shows the client receiving 192.168.100.13 automatically from DHCP.

This proved that DHCP was working correctly. It also showed why DHCP is useful in a business network. Manual IP addressing may be fine for a small lab, but it can cause mistakes when there are many clients. DHCP saves time and reduces human error. However, DHCP should still be controlled because a wrong or unauthorised DHCP server could give clients incorrect network settings.

7. Test and Troubleshoot

Testing was completed to make sure the network services were working correctly. Ping tests and IP configuration checks were used to test communication between the client and Swansea-DC. The client receiving **192.168.100.11** from DHCP was also a clear sign that the client could communicate with the server.

7.1. Test the network for Connectivity

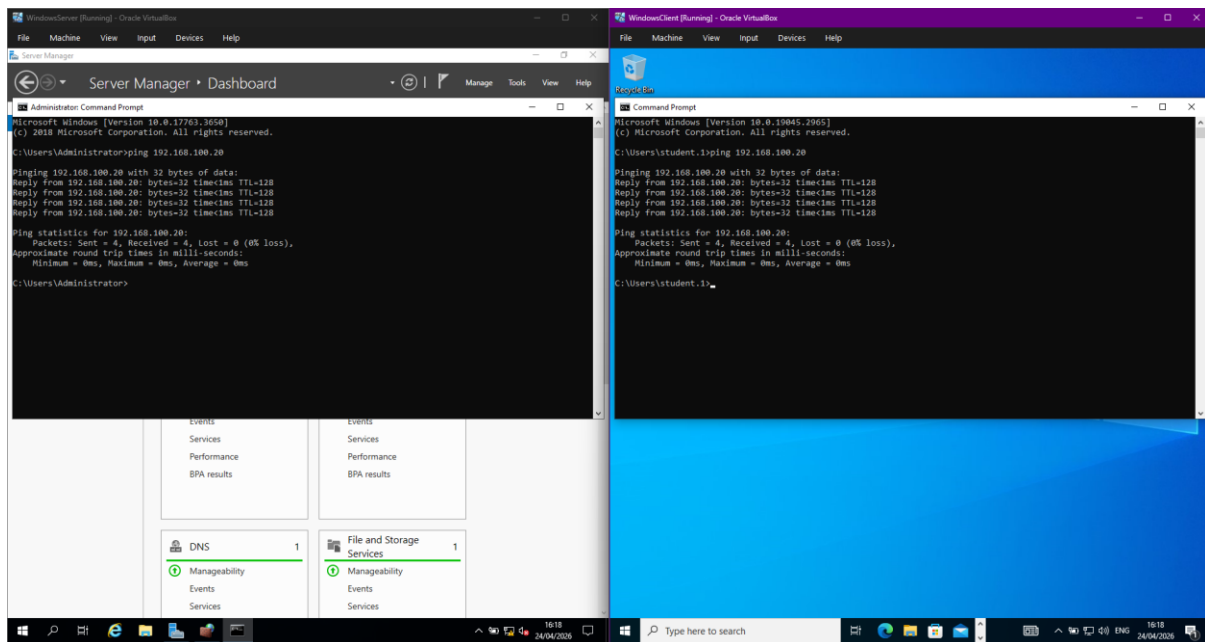


Figure 10 shows successful connectivity testing between the client and Swansea-DC.

This stage was important because network problems can come from different places. For example, a problem may look like a login issue, but the real cause could be DNS, DHCP, firewall rules, or routing. Because of this, troubleshooting should be done step by step. This helped me understand that testing is not just the final step; it is part of the whole configuration process.

8. Disk Drive

A second disk drive was mounted and used for shared storage. The shared folder was named **UWTSD**. This folder was shared so that users could access files across the network.

8.1. Mount second disk drive

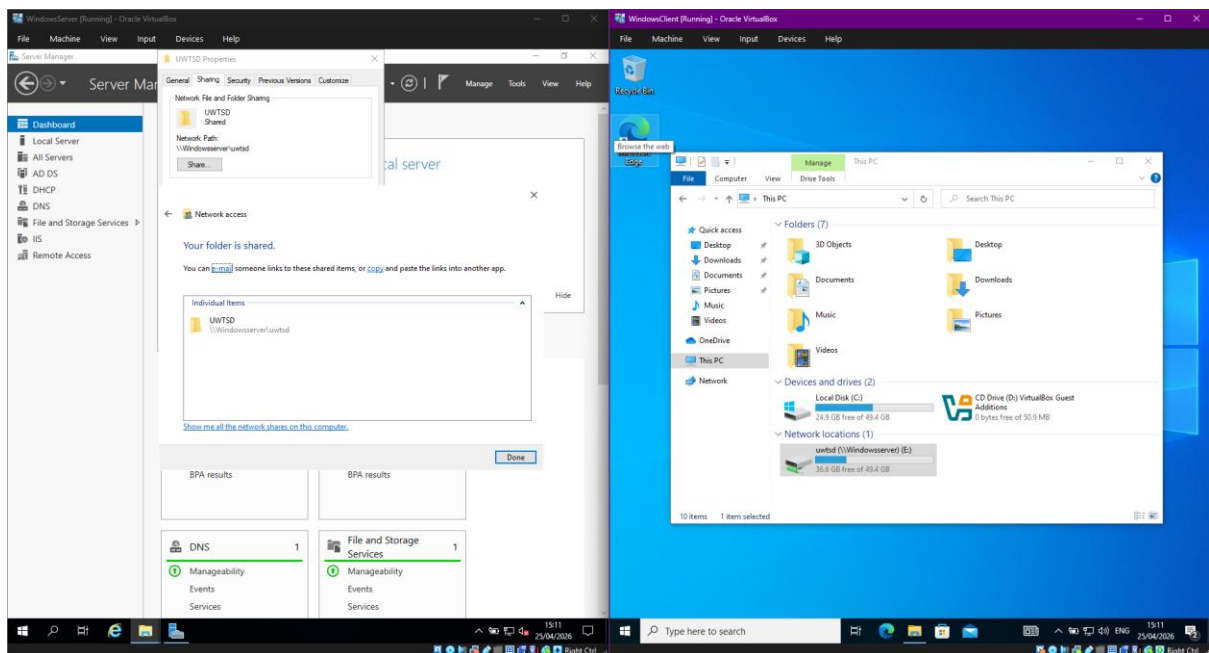


Figure 11 shows the mounted disk and the shared UWTSD folder.

This task showed the importance of permissions. Sharing a folder is easy but sharing it safely is more important. In a real business, users should not all have full access to every folder. The principle of least privilege means users should only get the access they need for their work [6]. This reduces the chance of accidental changes, deleted files, or unauthorised access.

9. IIS Server

An IIS website was created, and Windows Authentication was enabled. Windows Authentication is useful in an internal domain network because users can log in using their Windows domain credentials [7].

9.1. Create website and enable windows internal authentication.

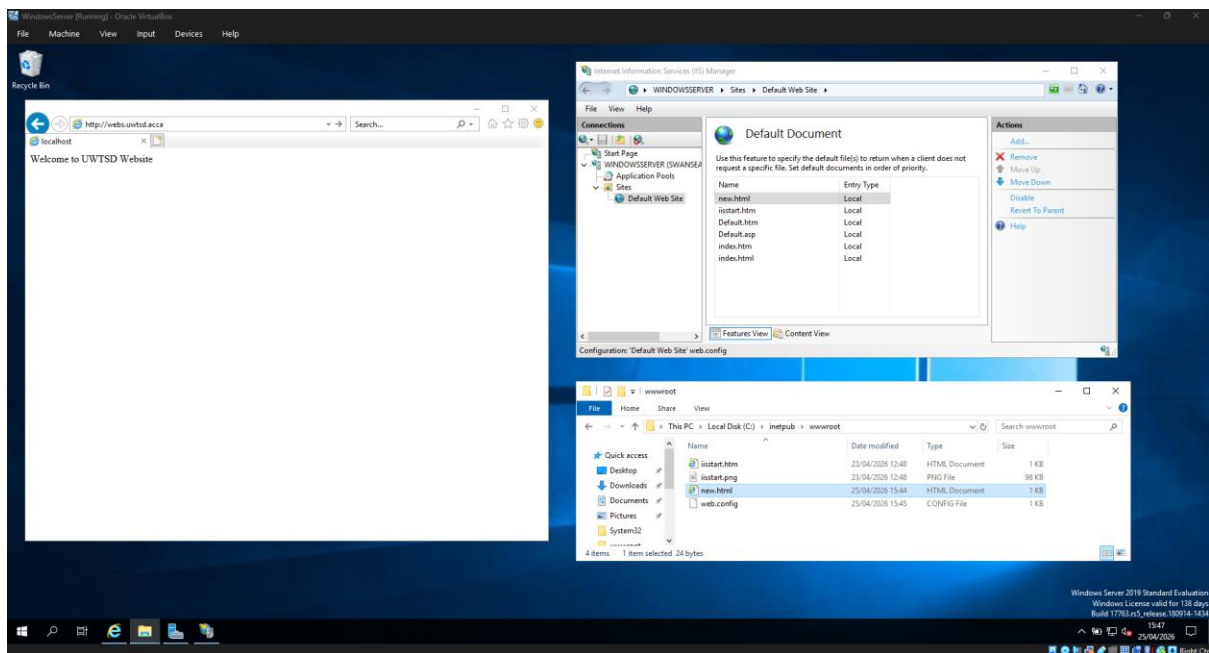


Figure 12 shows the IIS website with Windows Authentication enabled.

This was a good way to connect the web service with Active Directory. Instead of allowing anonymous access, the website required authenticated users. This is better for an internal company website because access can be controlled. However, if the website was used in a real business, HTTPS should also be used to protect the connection. Authentication controls who enter, but encryption helps protect the data while it travels.

10.Remote Desktop Services

Remote access was configured for **Swansea-DC** from another machine on the network. This allowed the server to be managed without sitting directly in front of it.

10.1. Configure remote access for Swansea-DC from any other machines in the network

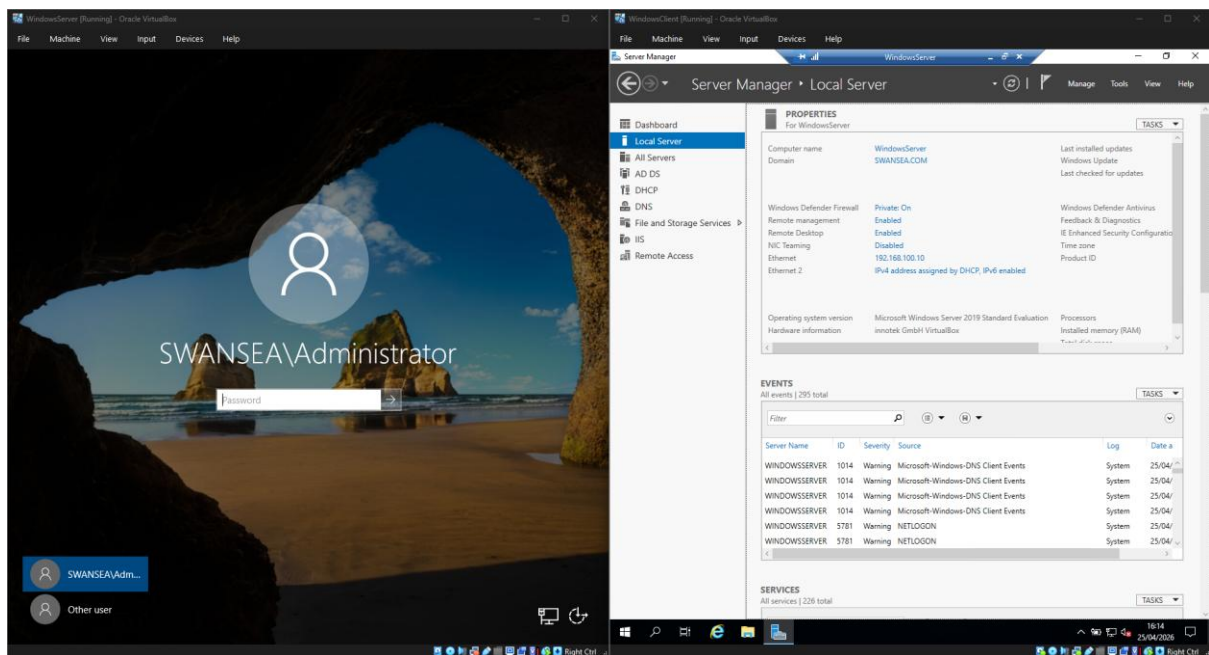


Figure 13 shows Remote Desktop access to Swansea-DC.

Remote Desktop is useful for administration, but it also needs strong security. CISA explains that weak security controls and poor credential practices are commonly exploited by attackers [8]. For this reason, Remote Desktop should only be available to trusted administrators. Strong passwords, limited access, and certificates should be used where possible. In my opinion, remote access is helpful, but it should never be left open without control because it gives direct access to important systems.

Conclusion

Overall, the implementation created a working Windows Server network using the **SWANSEA.COM** domain. Swansea-DC provided the main services, including Active Directory, DNS, DHCP, VPN, shared storage, IIS, and Remote Desktop access. The client successfully joined the domain and received the DHCP address **192.168.100.13**, which showed that the main services were working together.

The most important thing I learned is that network services depend on each other. DNS supports the domain, DHCP supports client addressing, routing supports communication, and permissions protect resources. If one part is configured badly, it can affect the whole network. Because of this, proper planning, testing, and security are needed to maintain a reliable network.

References

- [1] Microsoft, "Routing and Remote Access Service," *Microsoft Learn*, 2016. [Online]. Available: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140(v=ws.11))
- [2] Microsoft, "Active Directory Domain Services overview," *Microsoft Learn*, 2025. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
- [3] P. Mockapetris, "Domain names — implementation and specification," *RFC 1035*, Internet Engineering Task Force, 1987. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc1035>
- [4] R. Droms, "Dynamic Host Configuration Protocol," *RFC 2131*, Internet Engineering Task Force, 1997. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc2131>
- [5] S. Frankel and S. Krishnan, "Guide to IPsec VPNs," *NIST Special Publication 800-77 Revision 1*, National Institute of Standards and Technology, 2020. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final>
- [6] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," *NIST Special Publication 800-53 Revision 5*, 2020. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
- [7] Microsoft, "Windows Authentication," *Microsoft Learn*, 2022. [Online]. Available: <https://learn.microsoft.com/en-us/iis/configuration/system.webserver/security/authentication/windowsauthentication/>
- [8] Cybersecurity and Infrastructure Security Agency, "Weak Security Controls and Practices Routinely Exploited for Initial Access," *CISA*, 2022. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a>