

Contents

Enterprise network requirements and future growth.	. 3
Server operating systems.	. 3
Administration and automation... ..	. 3
Licensing and overallcost..... ..	. 4
Updates and support..... ..	. 4
Hardware compatibilityandsecurity ..	. 5
Network services and roles.	. 5
DHCP and DNS..... Directory	. 5
anddomainservices... File	. 6
sharing..... Web	. 7
servicesandIIS..... Remote	. 7
accessandRDS..... Routing and	. 7
VPN..... Certificates, ...	. 8
loggingandmonitoring	. 8
Basic information security considerations	. 8
Conclusion and recommendation.	. 9
References	.10

Enterprise network requirements and future growth

NOSS2027 needs a network connecting its Swansea and London offices. The proposed setup has Windows Server 2025 in Swansea, Debian Linux managed through the command line in London, and Windows clients. Staff should be able to use services at either office, with accounts and permissions controlling access to company files.

Each office has its own local network. Routing allows traffic to move between them [1]. For example, someone in London may need a file stored on the Swansea server. Having a connection is part of this, but the user also needs to find the server, log in and open a file they have permission to use. I think testing that whole process is more useful than only checking whether one PC can ping another.

Active Directory Domain Services (AD DS) stores information about users and computers and supports sign-in and access control [2]. This gives the company one place to manage its accounts. Dynamic Host Configuration Protocol (DHCP) gives clients IP addresses and other network settings automatically [3]. When adding a new PC, these services can save time because every setting does not have to be typed into the machine separately.

As the company grows, it will need more addresses, accounts and storage. Leaving some addresses free gives room for new devices without changing the whole addressing plan. Groups also make access easier to manage. If several staff need the same folder, they can belong to a group that has permission to use it. A record of server names, IP addresses and installed services would help the team understand the setup and find faults later.

Reliability matters because both offices may depend on the same server. A failure could stop access to several services at once. Backups would help recover lost data, while an extra server could reduce dependence on one machine if the services were set up to use it. These solve different problems. Remote access may also be needed as staff start working away from the office, with suitable sign-in and permission controls.

The initial setup can stay fairly simple: working accounts, IP addresses and access to shared resources. More services can be added in stages. This also helps with troubleshooting, since fewer things are changing at the same time.

Server operating systems

Administration and automation

Windows Server has graphical tools and PowerShell for administration. DHCP can be managed through either method [3]. The graphical console makes settings easier to find when learning how a service works. PowerShell can be useful for applying the same task to several accounts or machines, instead of repeating it manually.

Debian's APT tools install and update packages and handle their dependencies [4]. In this setup, Debian is managed through the terminal. Learning the commands may take time, but they can be saved in the setup notes and used again. For example, the same tested commands could help install packages on another Debian server.

Creating accounts from a list is one task worth automating. If several staff join NOSS2027 together, a script could save time. An error in the list could also affect all those accounts, so trying it with one test account first would help catch mistakes. The test should include checking its group membership and signing in. A script finishing without an error would not show that the account has the right access.

More than one person needs to understand both servers. Otherwise, a fault could take longer to fix when the person who knows the system is away.

Licensing and overall cost

Windows Server Standard and Datacenter use core-based licensing, with relevant client access licence requirements [5]. The evaluation version used in the lab would need appropriate licensing for ongoing business use. Debian follows a free-software approach that allows software to be used, modified and distributed under its licences [6]. It does not have the equivalent Windows Server core-licensing charge.

Debian can therefore reduce licence costs, but learning, administration and support still take time and money. For NOSS2027, Windows may be worth paying for because it brings the Windows accounts and their management tools together. Debian can support services suited to Linux. Hardware, staff training and maintenance also need to be included when comparing the cost of the two systems.

Updates and support

Windows Server 2025 has mainstream support until November 2029 and extended support until November 2034 [7]. Debian 13 has full support until August 2028 and Long Term Support until June 2030, with fewer supported architectures during LTS [8]. Windows has the longer published support period here. Debian would need an earlier upgrade plan, although the two support arrangements are different.

APT can update software installed through Debian's package system [4]. Programs installed separately need their own update checks. A software list would help avoid missing them. After updates, checks could include signing into the domain and opening a shared file from the other office. Both offices need to know about planned server restarts because work in London could depend on the Swansea server. Updating one server and checking it before changing the other would make it easier to work out where a new fault started. A short record of changes would help too.

Hardware compatibility and security

Microsoft explains that hardware requirements depend on the applications and roles running on a server [9]. A machine used for a few accounts may not be suitable for several people running remote desktops. Memory, processing power and storage need to match that workload. Debian without a desktop avoids running the graphical environment, but its applications still need enough resources. Testing the intended services is more useful than assuming one operating system will always be faster.

The software NOSS2027 needs also affects the choice. A program designed for Windows may make Windows Server the easier option, while a Linux application may suit Debian. Drivers need to support the chosen hardware as well.

Windows is suitable for AD DS [2]. Debian can share files with Windows computers through Samba and can join a domain as a member [10]. Being a member does not make it a domain controller. Keeping AD DS on Windows gives the setup a clear place to manage accounts, with Debian handling the Linux services. Staff should be able to use their authorised shared files without being given administrator rights to the server.

Network services and roles

DHCP and DNS

DHCP gives clients IP addresses and other network settings [3]. Figure 1 shows the scope options on the Swansea server. The router and DNS server are both set to 192.168.1.1, with dan-calin.acca as the domain suffix. The configured pool runs from 192.168.1.10 to 192.168.1.20, giving eleven addresses before exclusions. The client's ipconfig output showed a lease for 192.168.1.10 from 192.168.1.1. If more devices are added, the available range needs reviewing. A reservation can keep a particular address assigned to a specific client [3].

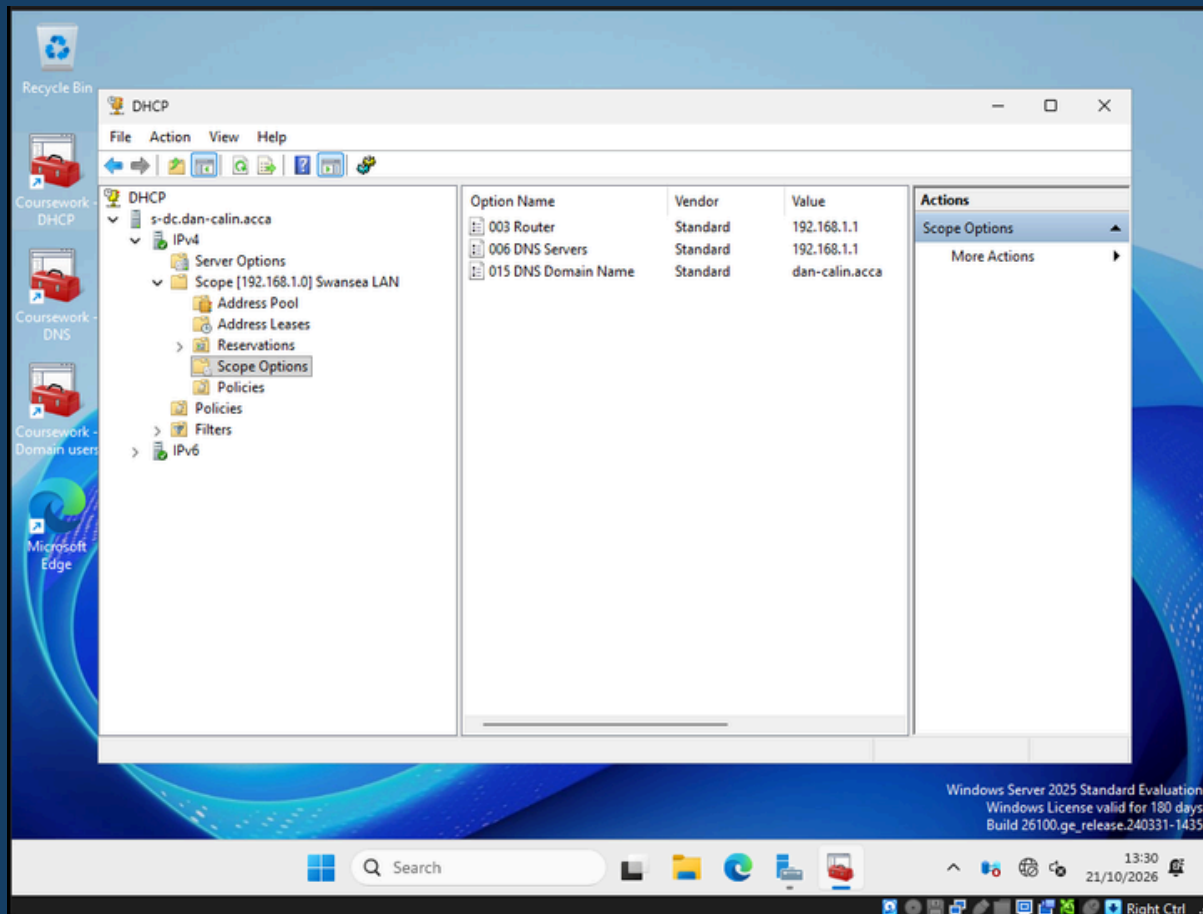


Figure 1. DHCP scope options showing the router, DNS server and domain suffix.

The Domain Name System (DNS) resolves names to IP addresses and helps clients find Active Directory domain controllers [11]. The separate client output showed s-dc.dan-calin.acca resolving to 192.168.1.1. A DNS problem could affect domain sign-in even when the client has an IP address and a working network connection.

DHCP failover could improve availability. Microsoft's implementation uses two Microsoft DHCP servers to share IPv4 leases. Changes to scope settings need to be replicated to the partner [12]. The Debian server cannot act as the partner in this Windows DHCP failover arrangement. London would need a local DHCP service or a DHCP relay to forward requests to a server on another subnet [3].

Directory and domain services

AD DS gives the company a central place to manage users and computers [2]. When an employee changes roles, their group memberships can be updated instead of creating a separate account on each machine. Access that is no longer needed should be removed too.

The Windows client has successfully joined the lab domain. The next checks should use an ordinary domain account to see what resources it can access. An administrator may have much wider access, so testing only that account could hide a permission problem.

A second domain controller could help if the first became unavailable. AD DS supports replication between domain controllers [2]. The second server would also need updates and backups, so it adds maintenance as well as improving availability.

File sharing

Windows file sharing fits the planned domain accounts at NOSS2027. Server Message Block (SMB) allows files to be read and written across a network [13]. Samba could provide file sharing on Debian too [10], but both services are not needed just to offer the same folders.

A shared folder containing staff instructions is one example. Most users would need read access, while only those maintaining the instructions would need write access. A separate working folder could let a team save and edit documents. A read-only user should be able to open an instruction file but be refused when trying to change it. Windows share permissions and NTFS permissions both need checking. With Samba, the share settings and Linux file permissions also matter. These are proposed tests for the shared folders. Restoring a deleted file from backup would be another useful check before staff rely on the service.

The same file tests should be run from London as well as Swansea. A folder opening on a nearby PC would not show whether staff at the other office can use it successfully.

Web services and IIS

Internet Information Services (IIS) could host a staff website for notices or documents. Windows Authentication would let staff use their domain accounts. Anderson and Larkin describe this as suitable for intranet applications [14]. Signing in would not automatically give everyone permission to edit the website; that would depend on their role.

Apache on Debian is another option, with Transport Layer Security (TLS) available through mod_ssl [15]. It could suit a Linux web application. IIS is the starting choice here because the proposed staff website would use Windows Authentication.

The website also needs HTTPS. Signing in with a domain account does not by itself encrypt the web traffic. Its certificate needs to be valid for the website and trusted by staff computers.

Remote access and RDS

Remote Desktop Services (RDS) provides access to desktops and applications running on central servers [16]. Staff could use the same software from either office or while working remotely. Performance would depend on the connection and the server resources available. Testing several sessions together would help show whether the server can handle the expected users. If staff only need one shared application, providing that application may be enough. Full remote desktops would make more sense where they need a whole working environment.

RDS session access has client access licence requirements [17], in addition to the relevant Windows Server licensing [5]. The number and type of licences need checking separately; successful logins do not prove that licensing is correct. Access should be limited to authorised staff, with administrative connections protected from unnecessary internet exposure.

Routing and VPN

Routing allows traffic to move between Swansea and London [1]. A virtual private network (VPN) would protect it when crossing an untrusted network. The National Institute of Standards and Technology (NIST) describes using Internet Protocol Security (IPsec) to protect IP communications, normally configured through Internet Key Exchange [18]. A site-to-site VPN would suit the connection between these offices.

The lab routes are already in place, but the VPN has not been configured. Both ends would need to authenticate each other and use compatible security settings. Tests should check that the required traffic passes through the tunnel and that it works after a restart. Temporarily disconnecting the link would also show which services each office can still use on its own.

Certificates, logging and monitoring

Active Directory Certificate Services (AD CS) can issue and manage certificates [19]. These could be used for the website and other services. Clients need to trust the certificate authority, and each service needs its certificate configured. Recording renewal dates would help avoid unexpected expiry. The private keys also need protection.

Logs can help investigate faults and suspicious activity. Joint guidance led by the Australian Cyber Security Centre recommends a logging policy, centralised and protected logs, and plans for detecting threats [20]. Failed sign-ins, changes to administrator access and service failures would be useful events to monitor. Someone needs to review alerts and act on them. Consistent time settings would help compare events from the two offices [20]. For example, repeated failed sign-ins could be checked against the account and source computer involved. They might be a typing mistake or an attack, so the event needs investigating rather than assuming either explanation.

Basic information security considerations

Authentication checks who a user is, while authorisation controls what they can access. NOSS2027 should give staff individual accounts and manage access through groups. A person who only edits documents does not need administrator access to the server. This follows least privilege: giving people the access needed for their work. Tests should include ordinary users as well as administrators.

NIST requires at least fifteen characters when a password is the only authentication factor. Passwords should be checked against commonly used or compromised values. The guidance says not to force periodic password changes, but to require a change when there is evidence of compromise [21]. Multi-factor authentication would add protection for remote users and administrators.

Firewall rules need to allow the services that should communicate. If a client cannot reach a server, the relevant rule can be checked without leaving the firewall disabled. Temporary troubleshooting rules should be removed afterwards. Accounts and permissions also need reviewing so old access does not remain available when someone's role changes or they leave.

Updates need to cover applications and operating systems. Before a major change, there should be a way to return to a working setup if something fails. Backups need protection and restore tests, rather than only checking that the backup job completed. A snapshot on the same virtual machine host should not be the only backup. The lab also needs separation from unrelated networks so its DHCP server does not give settings to the wrong devices. These checks can continue as more services are added in Component 2.

Conclusion and recommendation

I would use Windows Server for AD DS, DNS and DHCP, with Debian handling the London routing and Linux services. Windows file sharing and IIS fit the planned domain accounts. Debian gives the company another option for applications suited to Linux and avoids the equivalent Windows Server licence cost.

Using two operating systems means learning and maintaining both, so clear setup notes and an update plan matter. The Windows client has joined the domain; Debian domain integration and the VPN still need completing. Shared folders then need testing with ordinary accounts, including attempts to change files that should be read-only. Getting these everyday tasks working between the offices is the next priority.

References

- [1] L. Peterson and B. Davie, “3.3 Internet (IP),” *Computer Networks: A Systems Approach*, open-source online edition. Accessed: Oct. 21, 2026. [Online]. Available: <https://github.com/SystemsApproach/book/blob/master/internetworking/basic-ip.rst>
- [2] Microsoft, “Active Directory Domain Services overview.” Accessed: Oct. 21, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
- [3] Microsoft, “What is Dynamic Host Configuration Protocol (DHCP) Server in Windows Server?” Accessed: Oct. 21, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top>
- [4] O. Aoki, “Debian package management,” *Debian Reference*, ver. 2.152, ch. 2. Accessed: Oct. 21, 2026. [Online]. Available: <https://www.debian.org/doc/manuals/debian-reference/ch02.en.html>
- [5] Microsoft, “Windows Server 2025 licensing guidance.” Accessed: Oct. 21, 2026. [Online]. Available: <https://www.microsoft.com/licensing/guidance/Windows-Server-2025>
- [6] Debian Project, “What does free mean?” Accessed: Oct. 21, 2026. [Online]. Available: <https://www.debian.org/intro/free>
- [7] Microsoft, “Windows Server 2025,” *Microsoft Lifecycle*. Accessed: Oct. 21, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2025>
- [8] Debian Project, “Debian ‘trixie’ Release Information.” Accessed: Oct. 21, 2026. [Online]. Available: <https://www.debian.org/releases/trixie/>
- [9] Microsoft, “Hardware requirements for Windows Server.” Accessed: Oct. 21, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/get-started/hardware-requirements?pivots=windows-server-2025>
- [10] Samba Team, “smb.conf,” *Samba manual*. Accessed: Oct. 21, 2026. [Online]. Available: <https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>
- [11] Microsoft, “What is Domain Name System (DNS)?” Accessed: Oct. 21, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/networking/dns/dns-overview>

References (continued)

- [12] Microsoft, "DHCP failover overview." Accessed: Oct. 21, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-failover>
- [13] Microsoft, "What is SMB File Sharing for Windows and Windows Server?" Accessed: Oct. 21, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview>
- [14] R. Anderson and K. Larkin, "Configure Windows Authentication in ASP.NET Core." Accessed: Oct. 21, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/aspnet/core/security/authentication/windowsauth?view=aspnetcore-10.0>
- [15] Apache Software Foundation, "Apache Module mod_ssl," *Apache HTTP Server Version 2.4 documentation*. Accessed: Oct. 21, 2026. [Online]. Available: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html
- [16] Microsoft, "Remote Desktop Services overview in Windows Server." Accessed: Oct. 21, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/overview>
- [17] Microsoft, "License Remote Desktop Services with Client Access Licenses (CALs)." Accessed: Oct. 21, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-client-access-license>
- [18] E. Barker, Q. Dang, S. Frankel, K. Scarfone, and P. Wouters, *Guide to IPsec VPNs*, NIST SP 800-77 Rev. 1, Jun. 2020, doi: 10.6028/NIST.SP.800-77r1. Accessed: Oct. 21, 2026. [Online]. Available: <https://csrc.nist.gov/pubs/sp/800/77/r1/final>
- [19] Microsoft, "What is Active Directory Certificate Services?" Accessed: Oct. 21, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/active-directory-certificate-services-overview>
- [20] Australian Signals Directorate's Australian Cyber Security Centre et al., "Best practices for event logging and threat detection," Aug. 22, 2024. Accessed: Oct. 21, 2026. [Online]. Available: <https://www.cyber.gov.au/publication/best-practices-for-event-logging-and-threat-detection>
- [21] D. Temoshok et al., *Digital Identity Guidelines: Authentication and Authenticator Management*, NIST SP 800-63B-4, Jul. 2025, doi: 10.6028/NIST.SP.800-63b-4. Accessed: Oct. 21, 2026. [Online]. Available: <https://pages.nist.gov/800-63-4/sp800-63b.html>