

Network Operating Systems and Services (NOSS) (ACCA5023)

Worksheet 2 – Deploying a Network Directory Service and Creating and understanding active directory network objects.

(Practical Tasks)

STUDENT NUMBER – 1810613

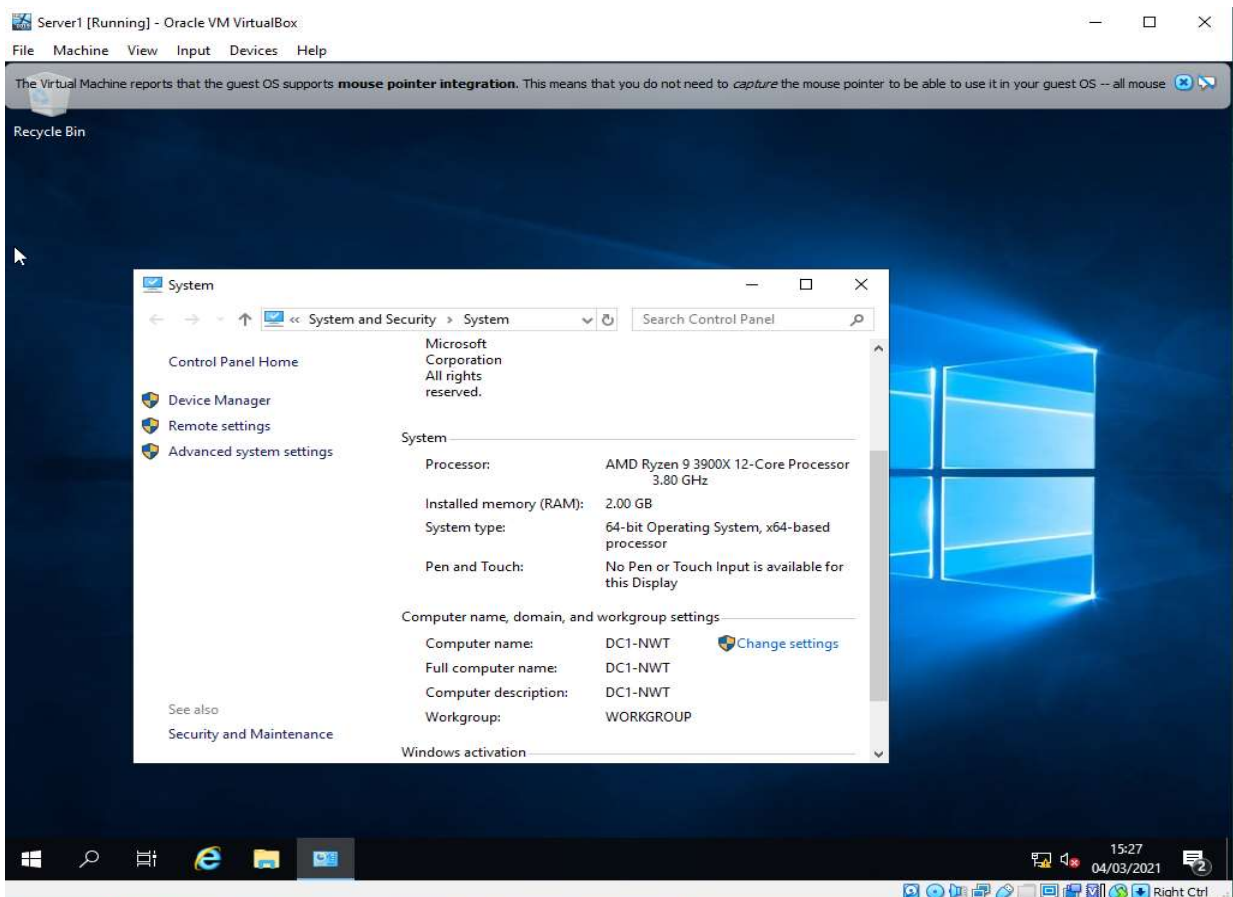
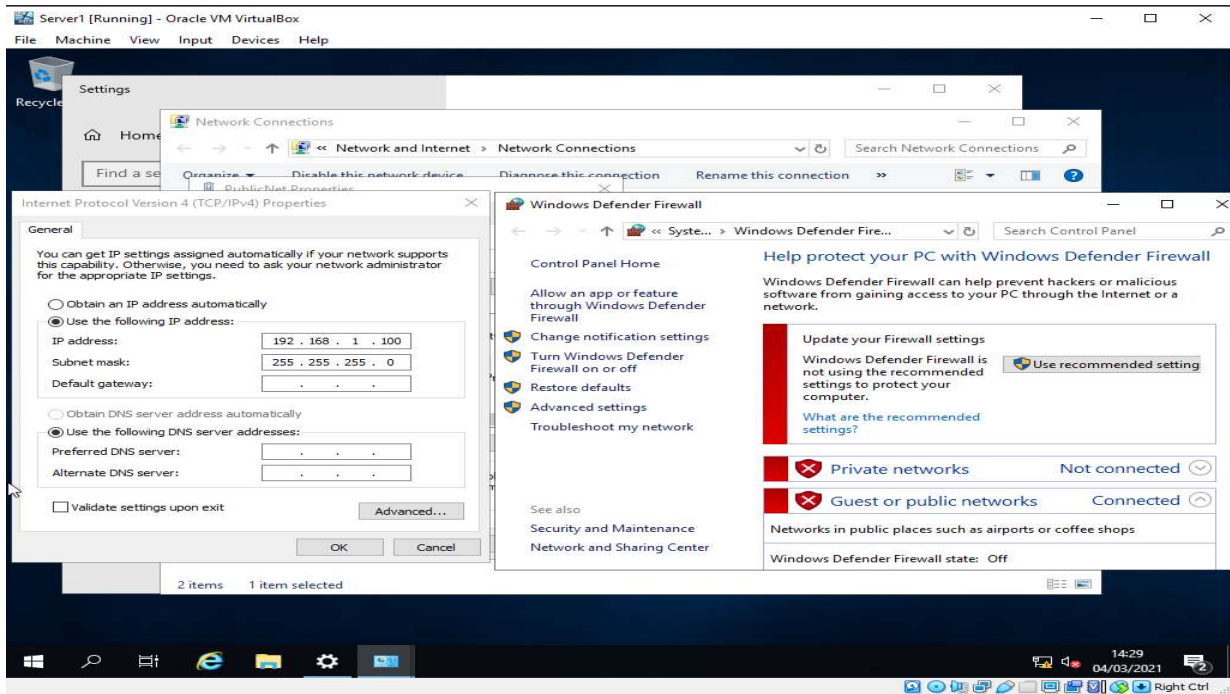
STUDENT NUMBER: 1810613

ACCA5023: WORKSHEET 2, PRACTICAL TASKS

Task 1: Pre-requisite tasks

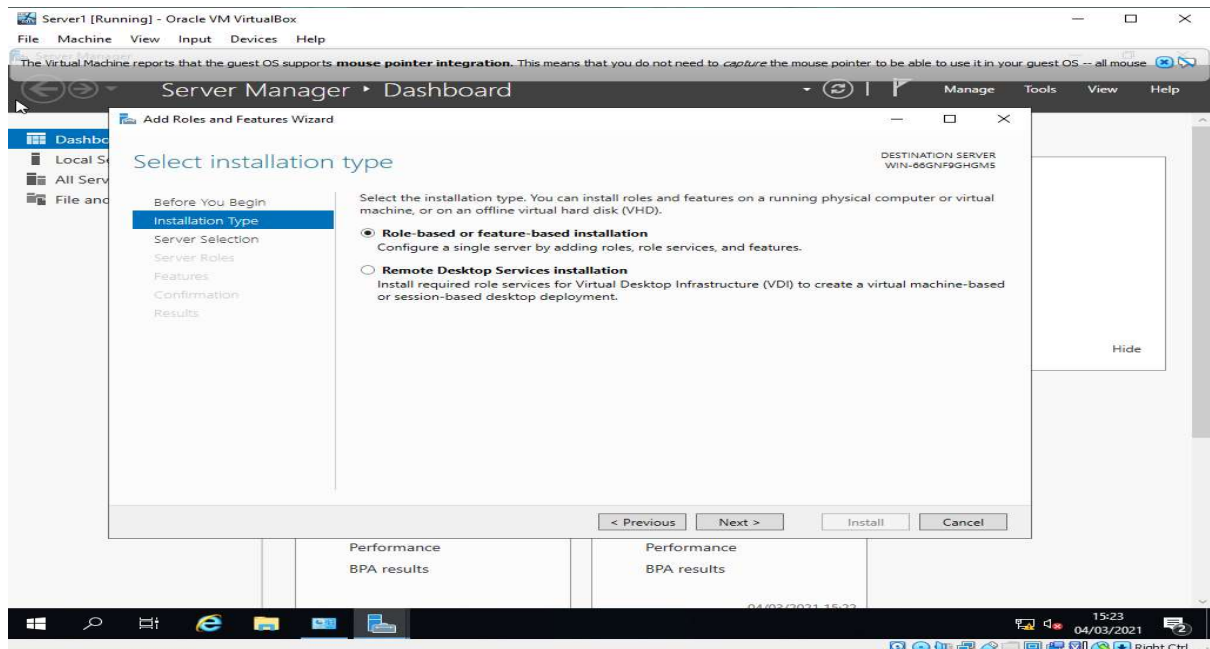
Confirmed that the IP is statically assigned for server 1, no DNS is setup, and the firewall is disabled.

Computer name has been changed to DC1-MWT

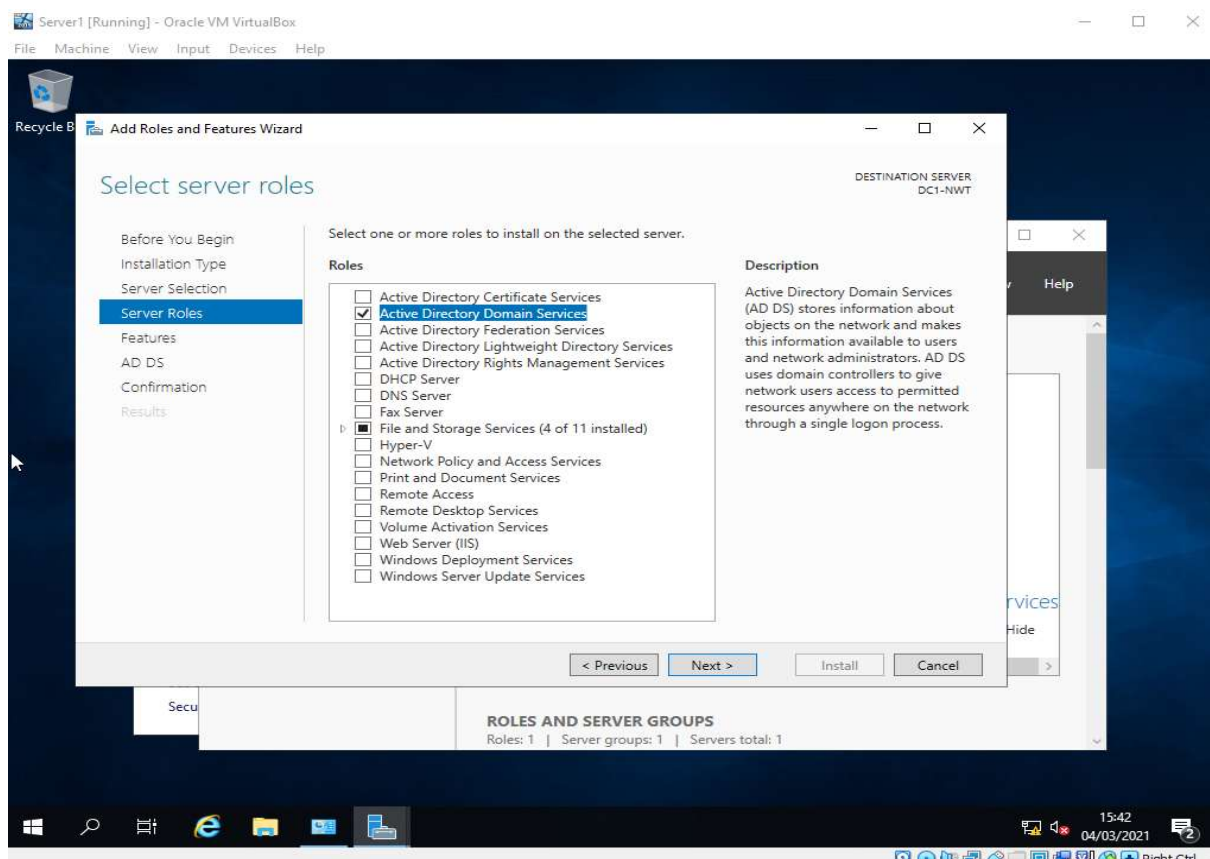


Task 2: Deploying Active Directory as a role or feature based installation

Role or feature based installation selected.



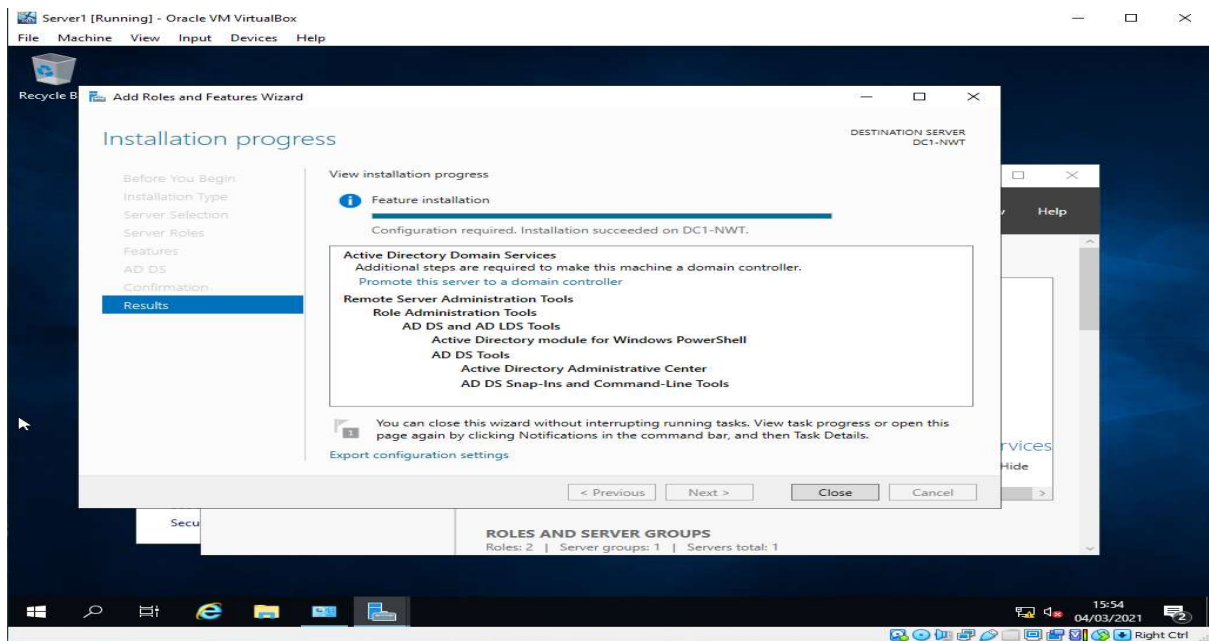
Active directory domain service enabled.



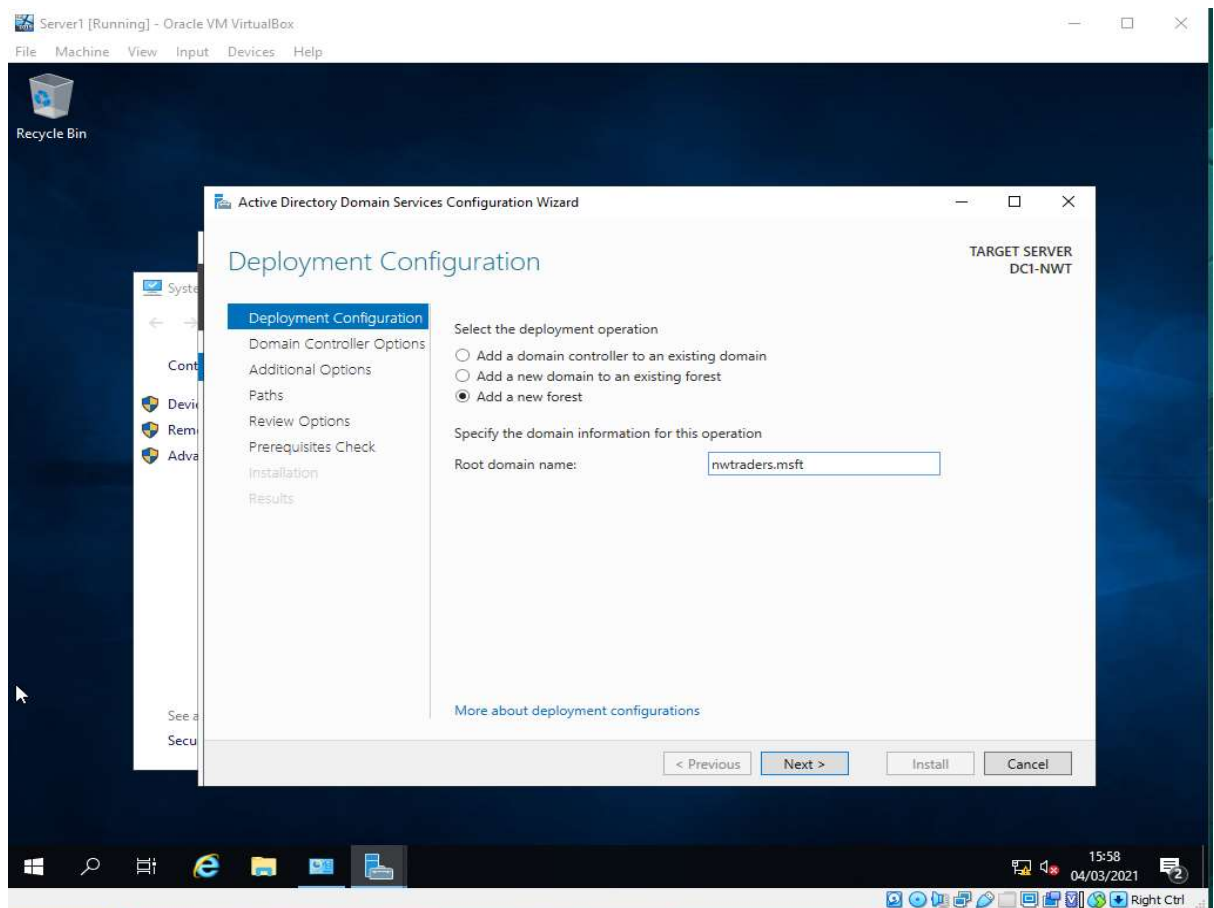
STUDENT NUMBER: 1810613

ACCA5023: WORKSHEET 2, PRACTICAL TASKS

ADDS (Active Directory Domain Service) Installation Complete



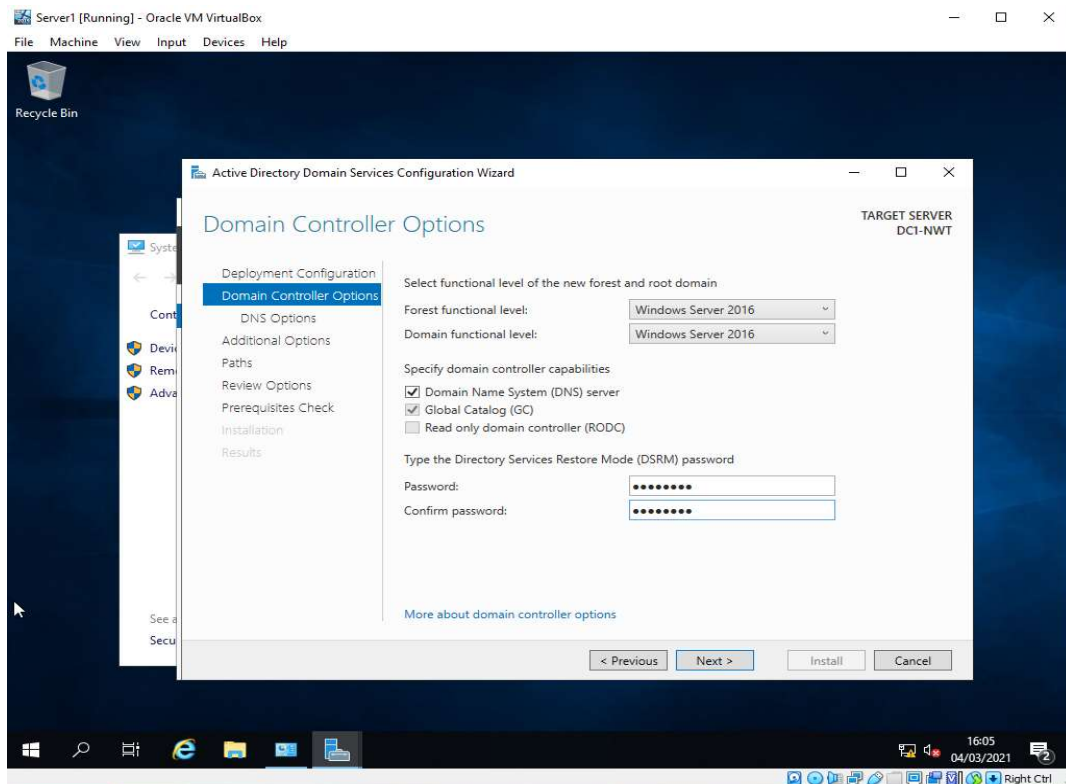
Server promoted to a domain controller. Root Domain specified as 'nwtraders.msft'.



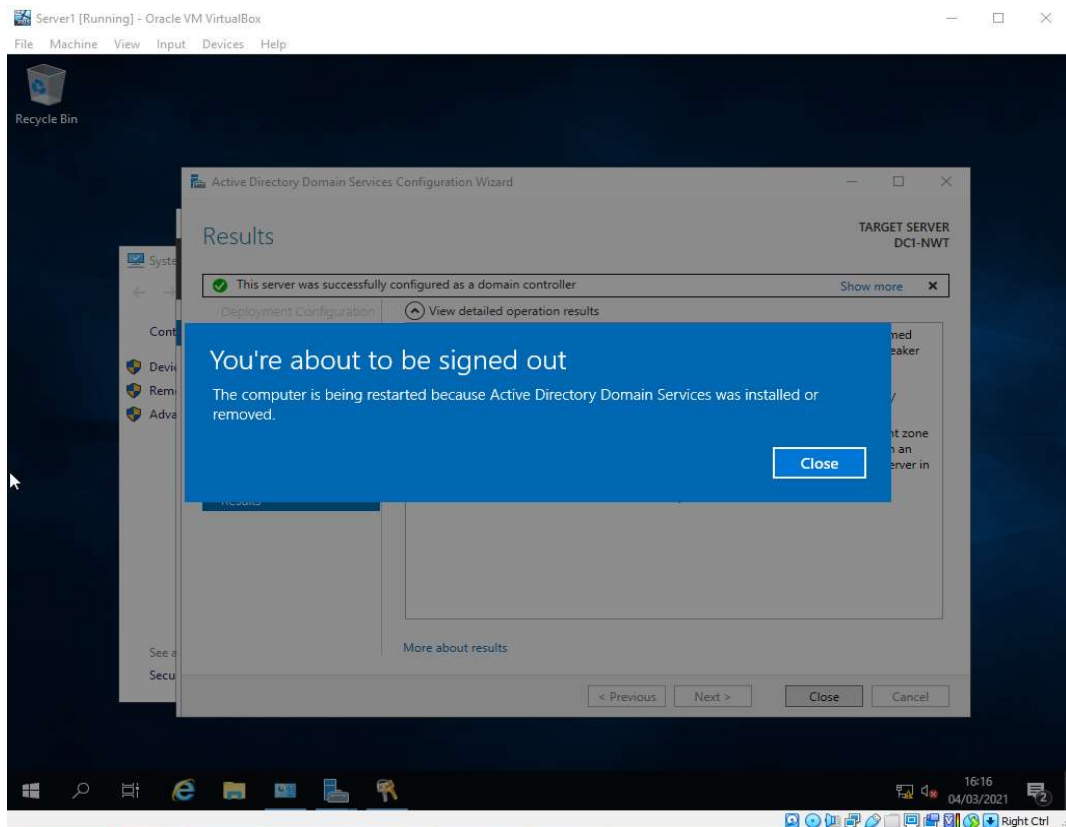
STUDENT NUMBER: 1810613

ACCA5023: WORKSHEET 2, PRACTICAL TASKS

Deployment has been configured: forest and functional level set to windows server 2016. DNS and global catalogue have been enabled and a secure password has been set.



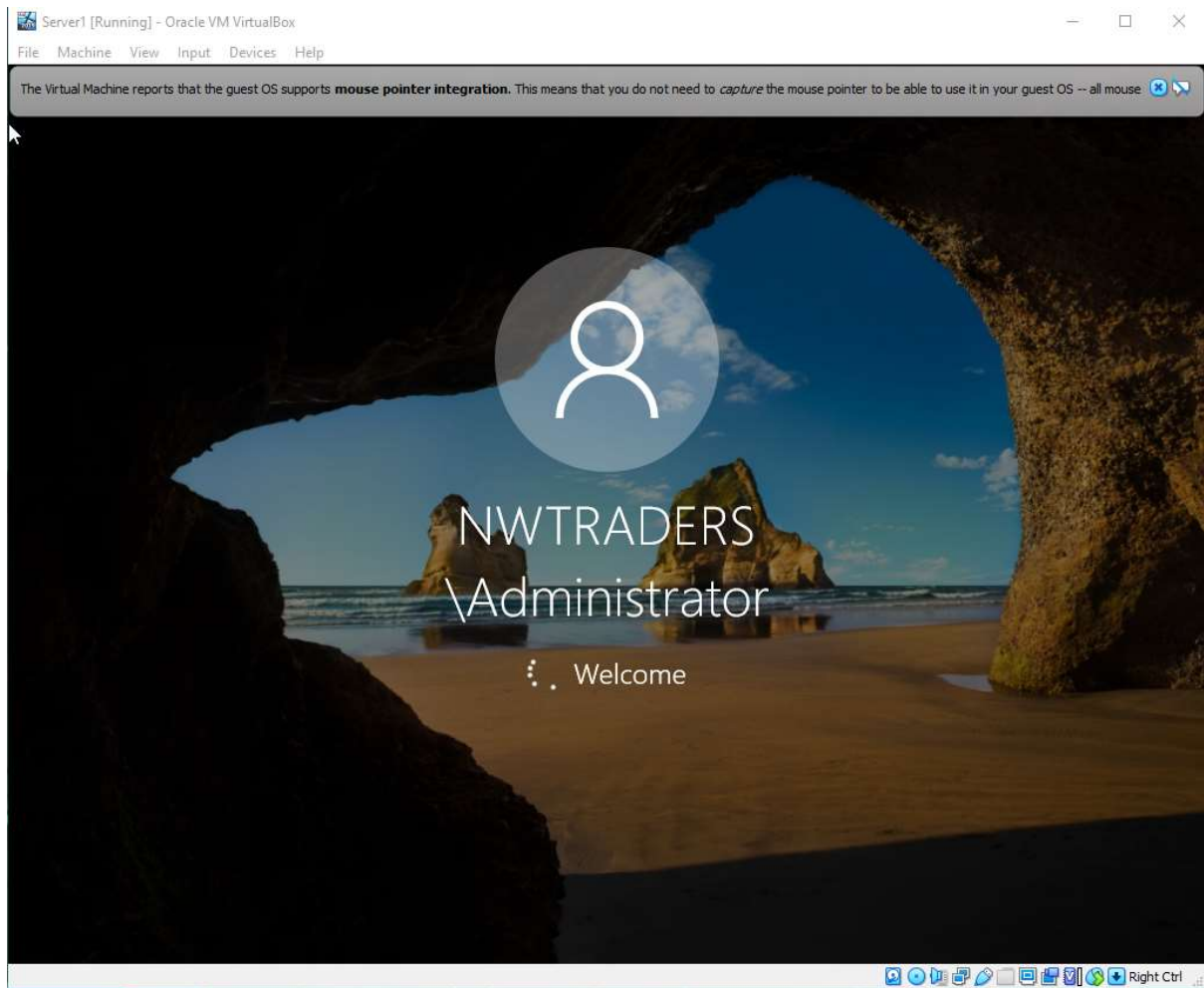
The machine has successfully been set up as an active directory domain controller.



STUDENT NUMBER: 1810613

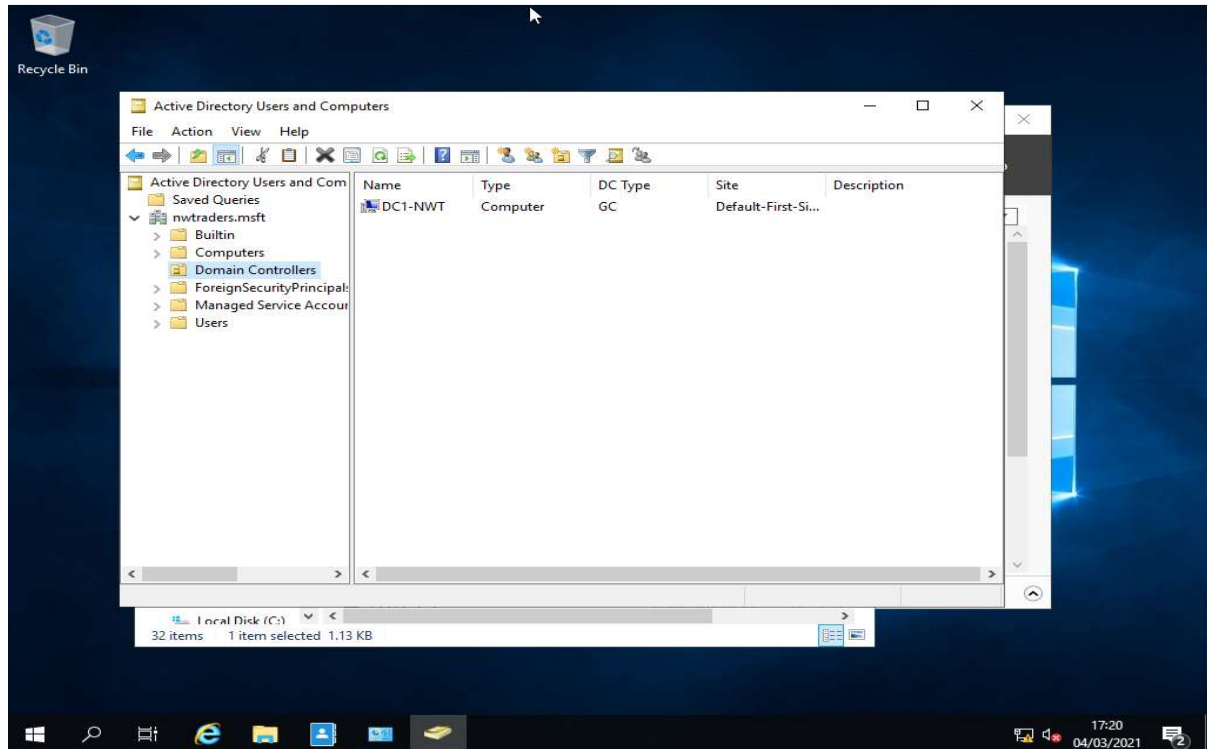
ACCA5023: WORKSHEET 2, PRACTICAL TASKS

Confirmation of login for the networks domain 'NWTRADERS'

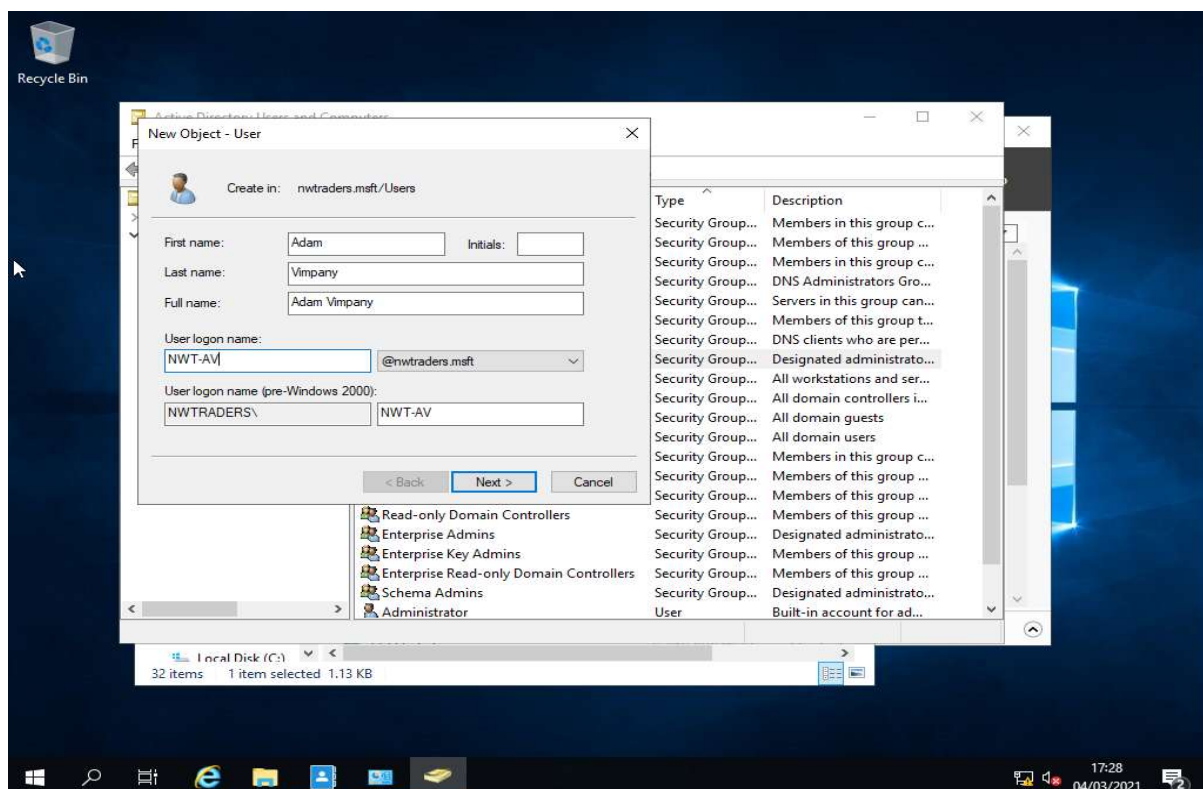


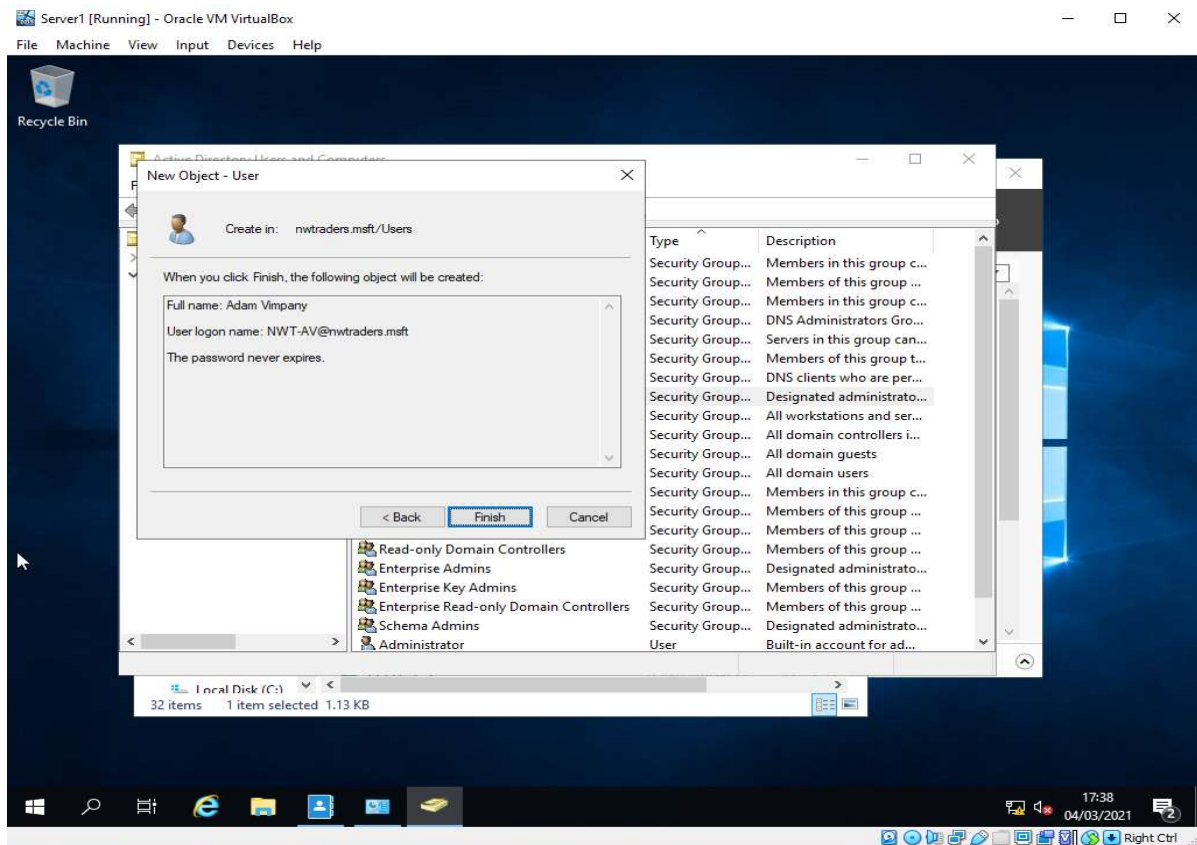
Task 3: Creating user account objects using Active Directory Users and Computers snap-in console

Server DC1-NWT is listed as the nwtraders.msft domain controller

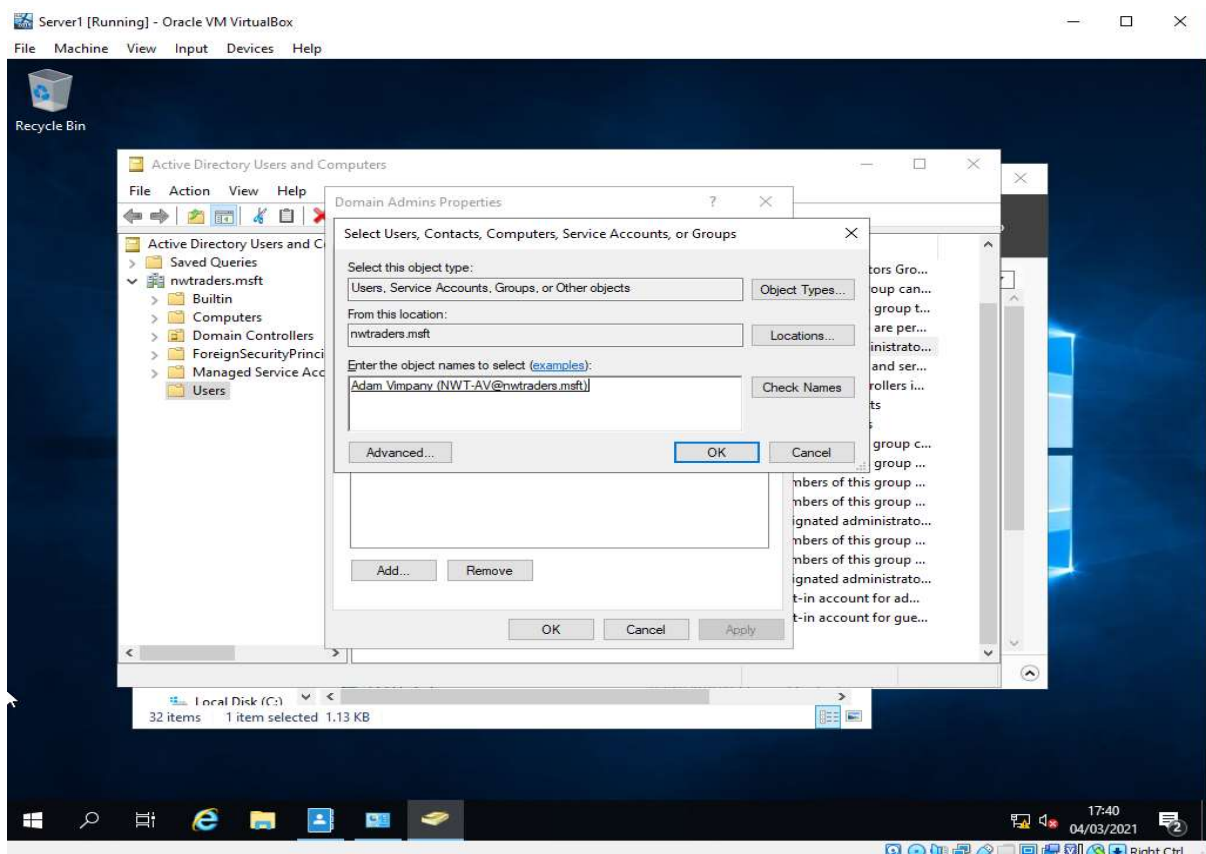


Evidence of new user creation



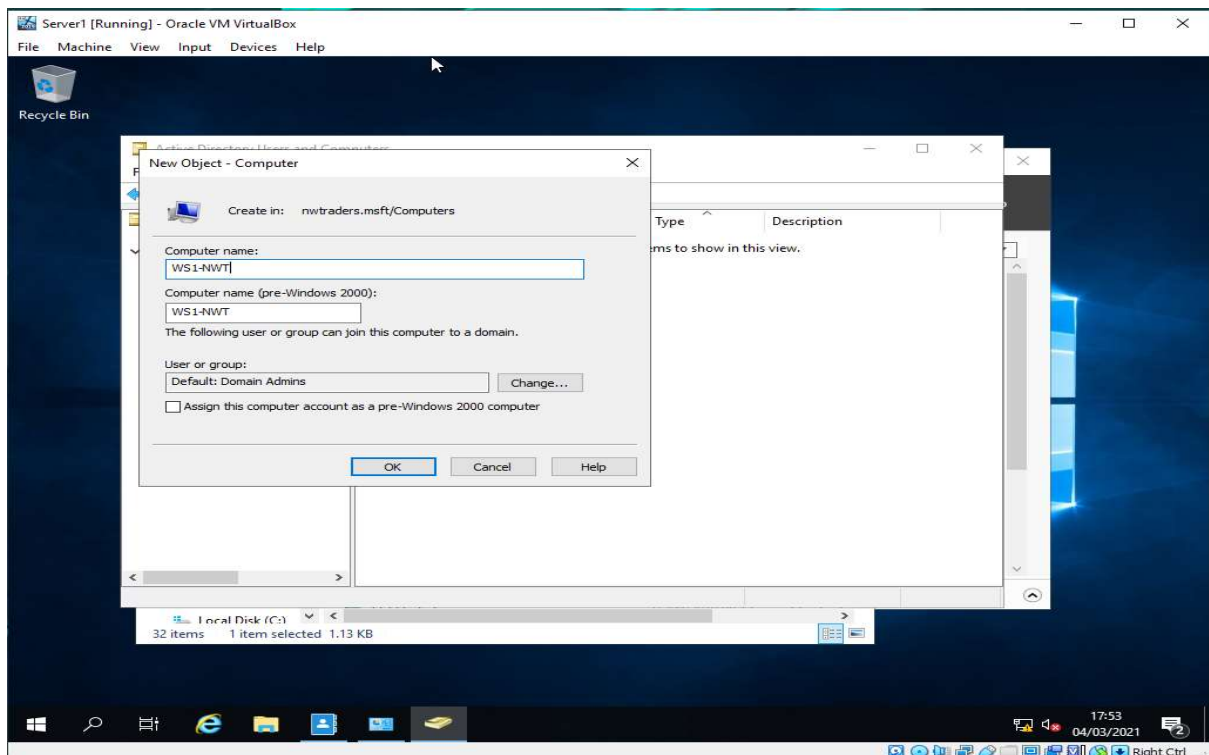


Added the failsafe account to the domain admins group 'nwtraders.msft'

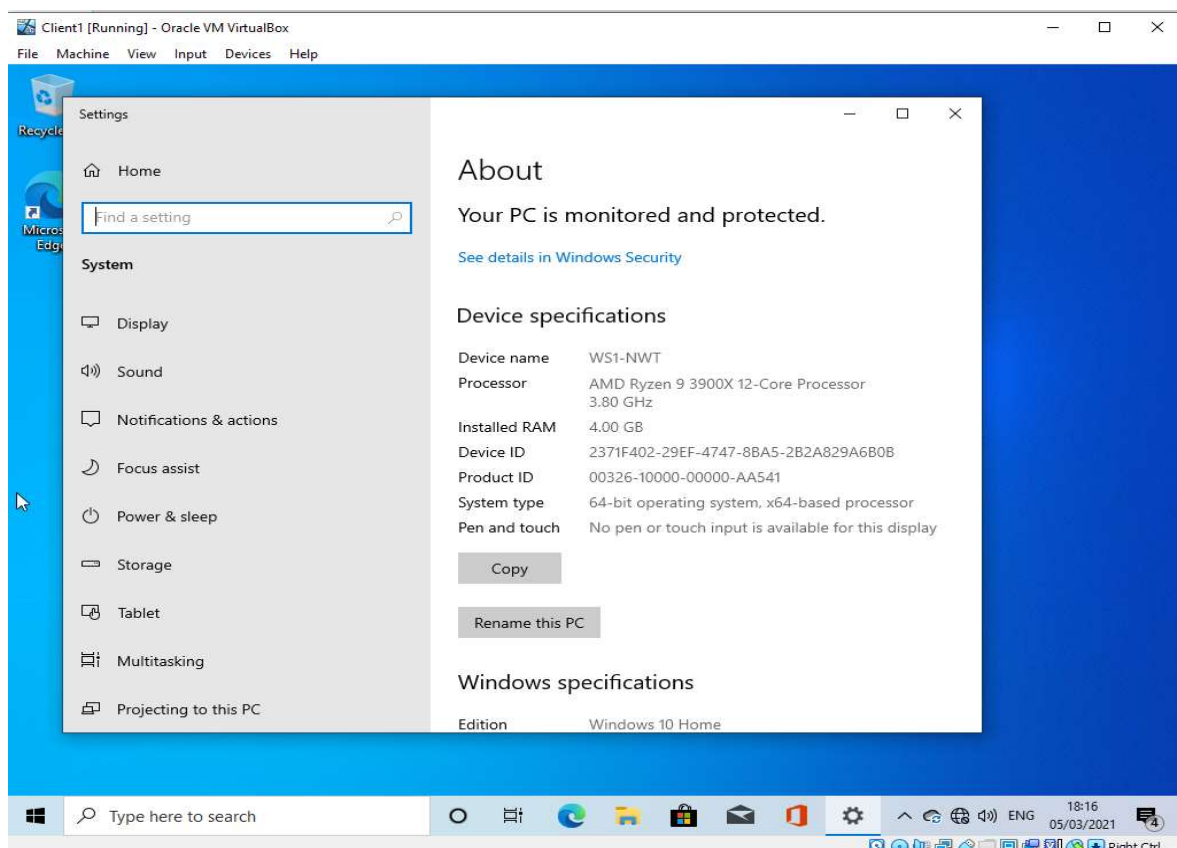


Task 5: Adjoining the domain and testing user logins

Computer object account created in active directory.



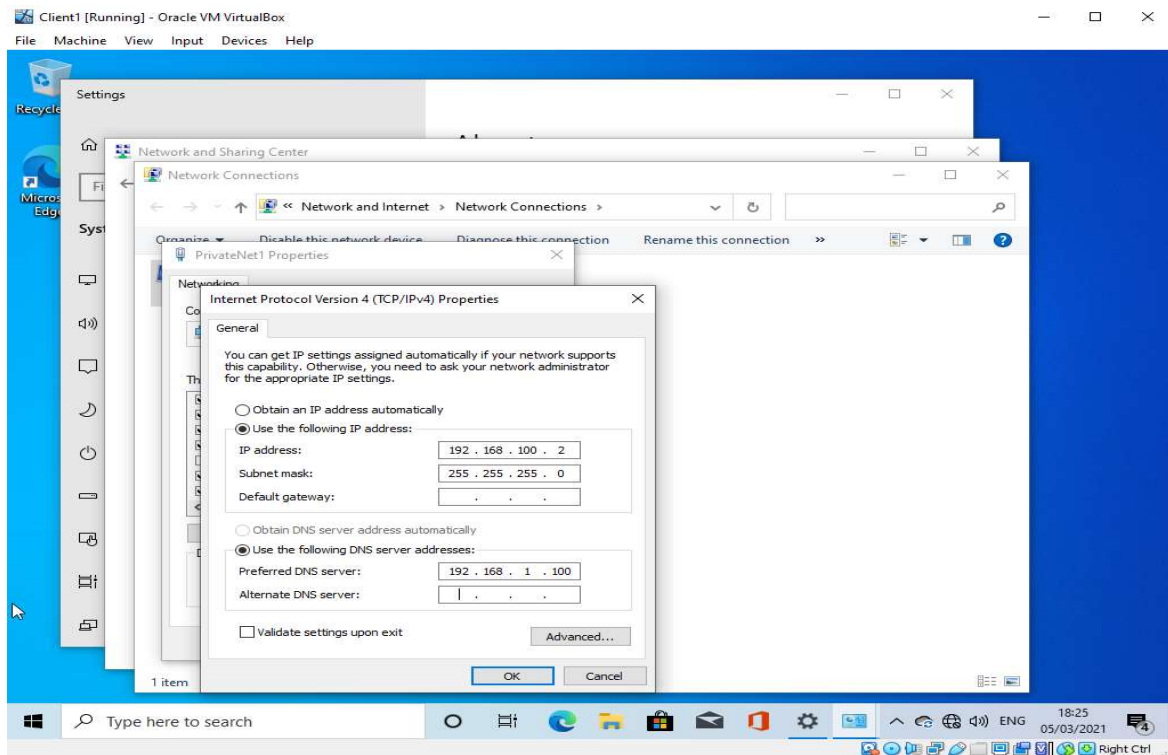
Client1 has been renamed to WS1-NWT



STUDENT NUMBER: 1810613

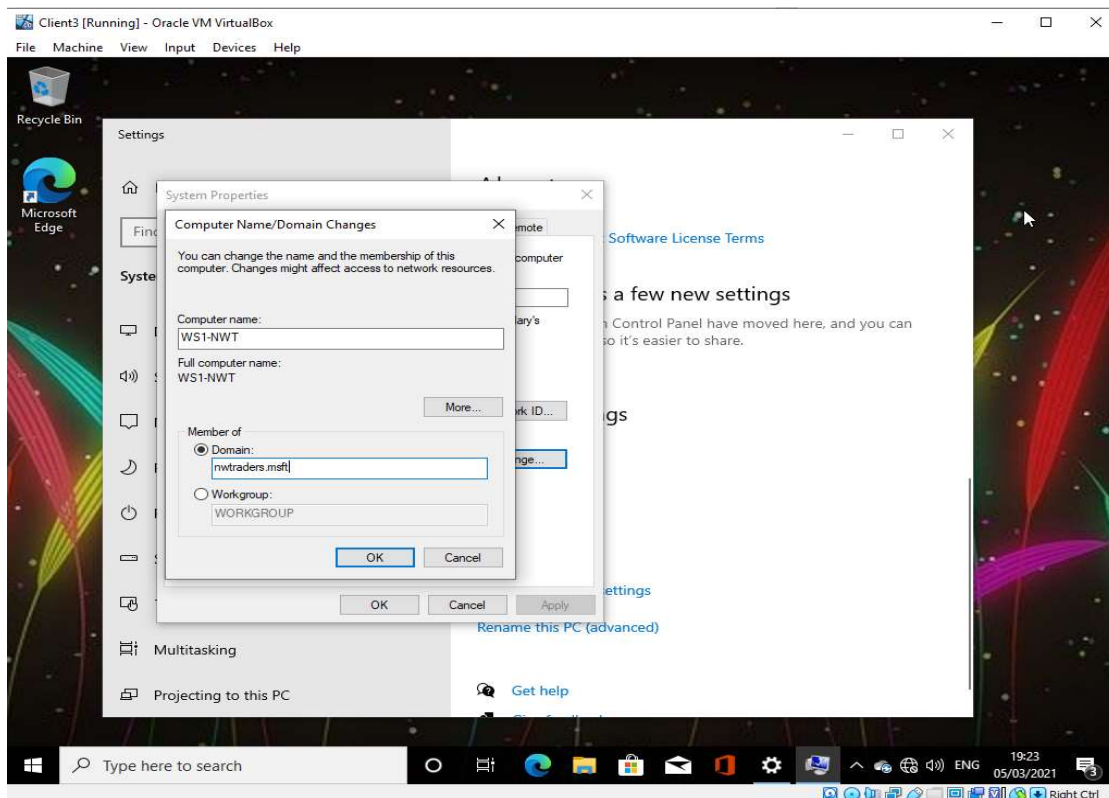
ACCA5023: WORKSHEET 2, PRACTICAL TASKS

Preferred DNS server set up on client 1



(Note: had to rebuild client1 machine as Windows 10 pro edition as Windows 10 home edition is unable to join domains.

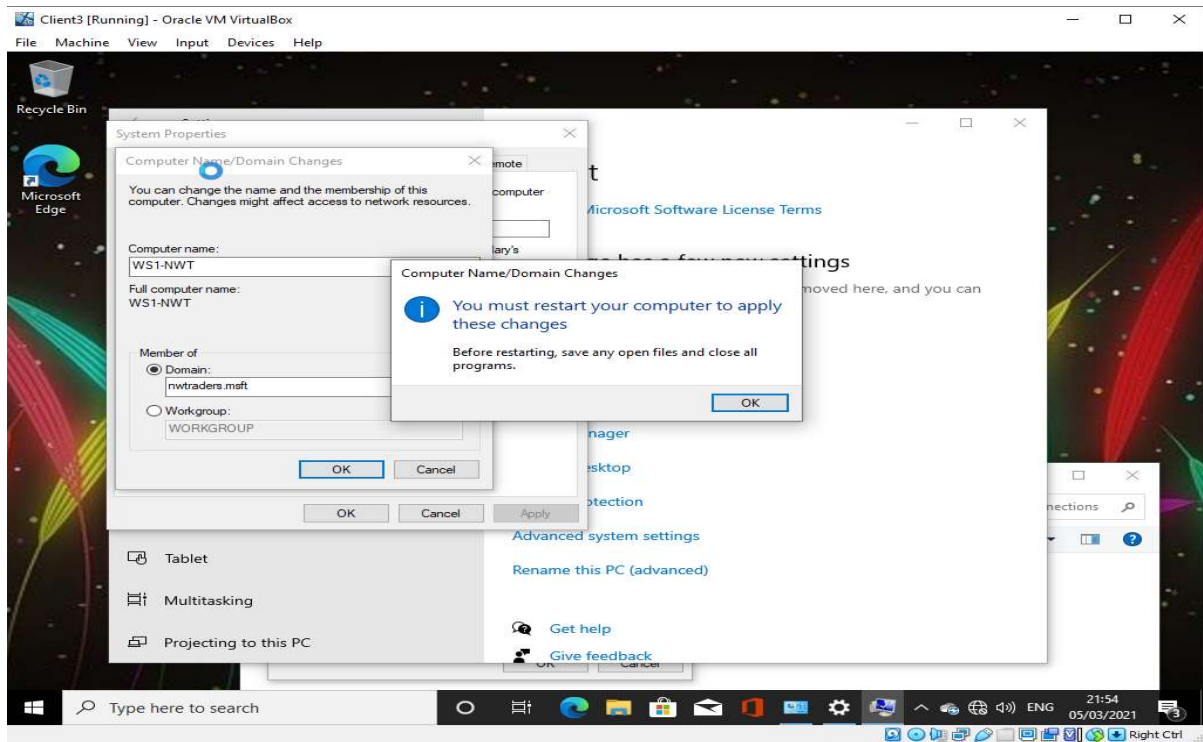
Made a member of Nwtraders.msft domain.



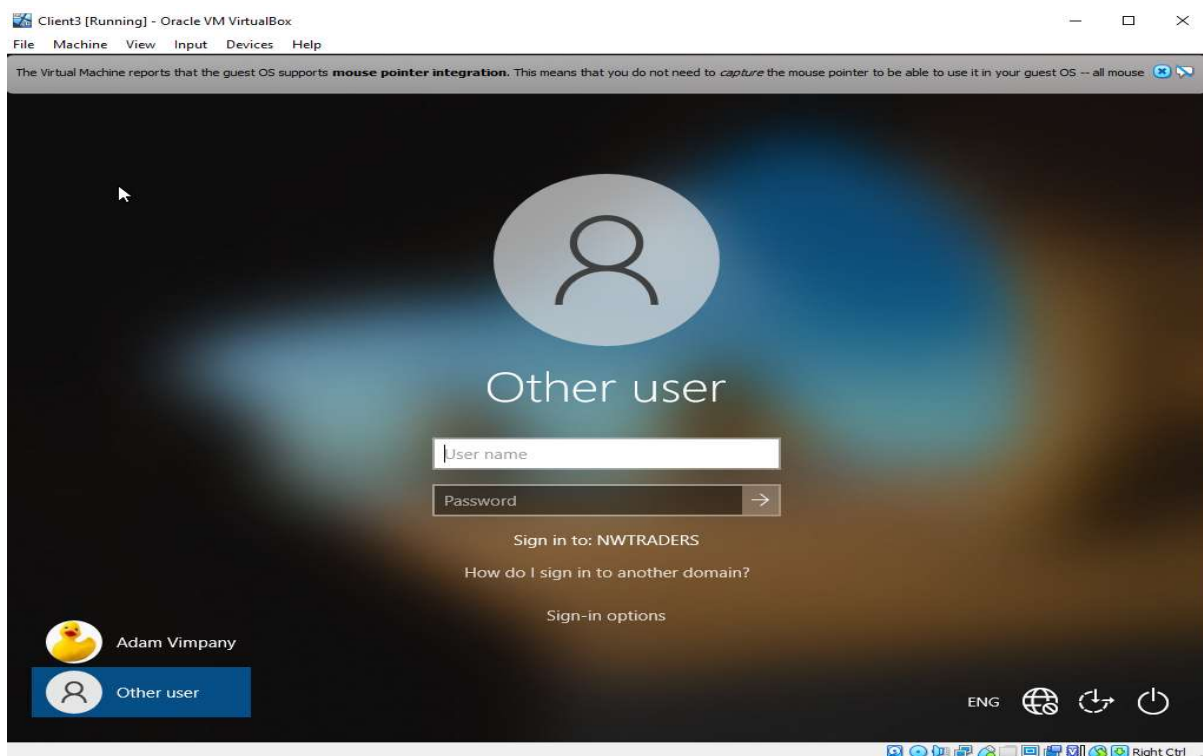
STUDENT NUMBER: 1810613

ACCA5023: WORKSHEET 2, PRACTICAL TASKS

Confirmed that client1 has been added to the nwtraders.msft domain.



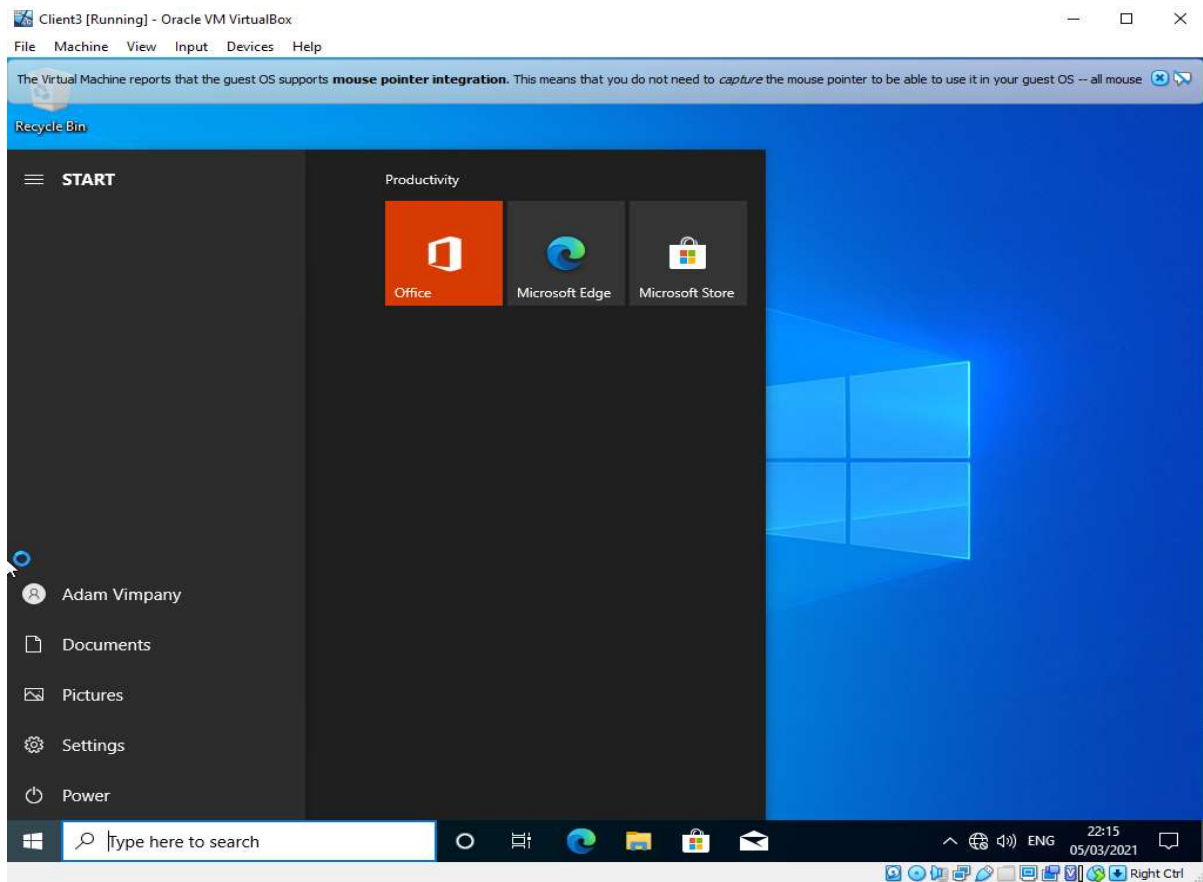
Option to log in to the NWTRADERS domain.



STUDENT NUMBER: 1810613

ACCA5023: WORKSHEET 2, PRACTICAL TASKS

Confirmation that the non admin account “NWT-AV” can successfully log in. (Note display name “Adam Vimpany” in the below screenshot.



Network Operating Systems and Services (NOSS) (ACCA5023)

Worksheet 2 – Deploying a Network Directory Service and Creating and understanding active directory network objects.

(Observational Tasks)

STUDENT NUMBER – 1810613

Task 6: Observational Tasks

6 a) DNS - explain what it is, how it works (illustrations) and its significance within Active Directory Domain Services.

The Domain Name System (DNS) matches domain names to an IP address, a process known as forward lookup. It allows a user to submit an easily memorable text-based query (i.e. a web address), with the DNS then matching this to the IP address for them.

The DNS Recursor (also referred to as the Recursive Resolver) is the first step between the client and a DNS name server. First, the client's own DNS resolver will check the client's cache for the domain information and return the IP address if it is stored there. If unsuccessful, the router nameserver will check its own cache (where this facility exists, not all routers have a cache) for IP address and returns it. Where cached data does not exist, the router nameserver refers the request on to the root nameserver (1). Commonly, the Internet Service Provider DNS services are used, but other DNS services are available. The DNS provider's root nameserver does not resolve the name request itself, but it returns a file known as the root zone file which contains all top-level domains (TLD, examples of which include ".co.uk", ".org" etc.) and the TLD server that is responsible for each (2). The root nameserver then sends a further request to whichever TLD server that is responsible for the requested TLD. The TLD server then informs the requesting server on which of the DNS servers the domain name is stored (1). The ISP root nameserver finally makes a request of the authoritative nameserver specific to the domain name and normally receives the IP address (2). The IP address is stored in the DNS A Record, in which case it is sent back again: from the ISP resolver, to the router and finally to the client resolver and browser. Alternatively, it may have a CNAME Record, in which case an alias domain is returned to the DNS resolver, and the process repeated in order to receive a DNS A Record IP address (1).

The Active Directory holds information about network resources, and Active Directory domains use DNS to allow PCs, servers etc. within a network to locate the domain controller; domain controllers to locate each other; and map user/workstation names to IP addresses (3). In the most common set up, the DNS servers are accessible to both the external namespace (i.e. the domain registered for use as an internet client) and the internal namespace (the AD domain) (4). Domain controllers run the domain server role for Active Directory. Domain controllers with DNS installed have Active Directory zone types. These zone types allow the Active Directory to maintain DNS records, such as A Records, CNAME records, NS Records (nameserver records) etc., these therefore contain information on all of the computers and other appliances that comprise the network (5). Zones can be integrated into Active Directory (Active Directory Integrated Zones) so that domain servers can update their own authoritative zones (6), which means that all domain controllers on the network will have the same information. This prevents the need for data transfer and increases redundancy. Other zones include Primary and Secondary Zones: a primary zone may or not be integrated, and a secondary zone will receive only a read-only copy of the data and so cannot be integrated (6).

6 b) AD is one critical 'Role or Feature based installation' as part of an enterprise network, identify and provide a brief overview of 2 other critical roles?

IIS

Internet Information Services (IIS) is a software package that is used for hosting web services on a web server (7). It is used to create, maintain and publish websites, as well as more advanced options, such as optimising performance or security settings. It supports webpages built with ASP.NET, PHP, HTML and other common scripting languages used in web development (8). It is not automatically installed when using the default settings of many Windows Server OSes, and so must be installed onto web servers by using either PowerShell or the Server Manager (7).

Remote Desktop Services

Another feature of Microsoft Windows Server is Remote Desktop Services (RDS), which can be installed using the "Role or Feature Based Installation" menu. It allows multiple users of the network to access a single server that is hosting desktops, applications and devices (such as printers) through the Remote Desktop Session Host (9). RD Connection Brokers is a role that controls access to databases or remote desktops, by authenticating users and load balancing of servers (10). RD Gateway allows users to access RDS features and network resources from outside of the internal network (11), RD Licensing ensures that client access licenses (CALs, used by the RD Session Host server to allow users to connect to it) are issued and tracked (12) while the RD web client allows users to access the remote desktop services through a web browser (13).

6 c) Explain why it is important to have different levels of access/roles within the 'Built in' Network User Account groups (e.g. Domain Admins, DHCP Admins, etc).

When Active Directory is installed, it creates "BuiltIn" user accounts and group accounts automatically. Each of these groups have pre-set user rights settings, which limit the types of tasks the user can perform depending on their access level. Examples of automatically created groups include the "Account Operators", members of which can add or remove user accounts and perform group management; "BackUp Operators", members of which can perform back-ups or restore files; "Guest" accounts, who have minimal permissions; and "Administrators", members of which have overarching control (14). These roles can be amended to work across the entire network, or be limited to a specific secondary domain controller only.

The highest level of access for the BuiltIn user account groups is the "Administrators" (14). These users must be carefully selected because of their access to the highest level of user rights. Some examples of high-level user rights that must be strictly controlled include the ability to add or remove user accounts, as setting up an account incorrectly may cause security vulnerabilities (14), and incorrectly deleting or modifying an account may cause operational problems. That said, the default "Account Operators" group is unable to make changes to, add or delete administrators, which prevents them from modifying their own accounts to increase their authority, or removing privileges from administrators inappropriately (15). These privileges could be used as a security exploit, for example, by

increasing their own privileges to an “Administrator” account, deleting genuine Administrator accounts, and then accessing or modifying operations or sensitive data maliciously.

Careful, correct configuration of user accounts is paramount for the secure functioning of the entire network. Users must have sufficient rights and permissions in order to perform their work duties, but must not be able to make changes to system-critical operations, for example. User rights and permissions must be set to prevent unauthorised access or cause security vulnerabilities. Having BuiltIn user account pre-sets simplifies the process of adding and removing users, as they can be given a “role” with set user rights and permissions that are appropriate for their job role, without having to configure individual settings for each and every user (16). This is beneficial for administrators of the system, as once these roles are configured, new users can be added quickly and efficiently with less chance of oversights occurring that could lead to a security vulnerability. For large enterprises, it is essential: where large numbers of employees join or leave the organisation or change job roles, setting appropriate user rights for every user would quickly become unwieldy leading to errors (16). Additionally, a single user can be assigned multiple roles (16), for example, a senior member of staff may have the same roles as the other members of their department, plus an additional role that grants them access to sensitive data, or the ability to add or remove accounts on their domain local group.

Having a hierarchy of roles ensures that user groups automatically inherit lower ranking user rights (for example, administrators will always be able to shut down the system or restore files and so on) without these rights having to specifically be granted to them (16). This streamlines the process of assigning user rights. Having all user accounts added to groups allows this information to be easily audited.

6 d) Share your ideas in-detail on Microsoft’s recommendations on AGDLP and AGUDLP for assigning permissions. How do you view them in the perspective of a System Administrator in strategizing and implementing within your network?

AGDLP (Account, Global, Domain Local, Permission) and AGUDLP (Account, Global, Universal, Domain Local, Permission) are recommendations made by Microsoft for assigning permissions. AGDLP are the recommendations for RBAC (Role-Based Access Controls), while AGUDLP are for Active Directory forests. Essentially, the acronym lists how the users and groups are nested: that is, for AGDLP, Accounts are added to Global Groups; the global groups are added to Domain Local Groups; these groups are then assigned Permissions.

AGDLP

A system administrator will create a number of Global Groups for the various roles across the organisation, for example, *Role_IT_Helpdesk* or *Role_Sales_Associate* (17). As a user can be a member of multiple global groups (e.g. their departmental role, a senior management role, and a location-based role) these should be succinct for ease of management. These global

groups are then added to Domain Local Groups, which each contain the permissions appropriate for members of that group, and grants them access to the relevant network resources (18). This is advantageous for the system administrator, as once the various groups have been created, it is simple to make changes and maintain permissions in the future. For example, if a department (who are all members of a global group) implements a new application, then it is simple to grant the entire global group access to it, without having to amend permissions for every member of the department. When a user moves to a different role within the same organisation, their account can be moved from one global group to another, without needing to manually revoke irrelevant rights and implement new ones.

When the system is first being created, using AGDLP is simpler than using AGUDLP. However, if necessary AGDLP groups can be converted to AGUDLP groups in the future, and combined with other AGDLP groups, assuming they use the same naming conventions (17). Conversion from AGDLP to AGUDLP is simple, as global groups are added to a newly created Universal Group, and the Universal Group is then added to the Domain Local Group.

AGUDLP

AGUDLP is used to allow administrators to control different areas of the “forest” (18). This may be where a large organisation is spread out geographically, with workplaces based in different locales, each with its own administrators. These administrators will control the Global Groups within their own domains. The next level is the Universal Group, or the Resource Group. This can contain Global Groups, for example, all of the “*Role_IT_Helpdesk*” Global Groups from every location in the organisation, but it can also contain other Universal Groups or individual users. These universal groups are then added to the Domain Local Group as described above. A centralised administrator(s) will control access levels across the organisation, while allowing other domain administrators to control their own domains (17), which is important in large organisations and enterprises. It is important when implementing groups that they are carefully planned so as to prevent redundant groups: if every Domain Local group on the system contains a single Universal group that in turn contains a single global group, it is likely that there is a better method of delegation. For example, a universal group might be created for financial resources, which senior management, accounting and finance global groups are each added to rather than access to the same resources being set separately for each individual global group. This means that changes to financial resources permissions can be set in the universal group once, rather than being amended redundantly across multiple domain local groups (which defeats the intentions of AGDLP/AGUDLP somewhat).

Bibliography

1. **CloudFlare**. DNS Server Types. *CloudFlare*. [Online] [Cited: 03 02, 2021.] <https://www.cloudflare.com/learning/dns/dns-server-types/>.
2. **IONOS**. What is a root server? Definition and mechanics. *Digital Guide IONOS*. [Online] 09 14, 2017. [Cited: 03 02, 2021.] <https://www.ionos.co.uk/digitalguide/server/know-how/what-is-a-root-server-definition-and-background/>.
3. **Microsoft**. Domain Name System (DNS). *Microsoft*. [Online] 07 08, 2020. [Cited: 03 02, 2021.] [https://docs.microsoft.com/en-us/windows-server/networking/dns/dns-top#:~:text=Active%20Directory%20Domain%20Services%20\(AD,its%20domain%20controller%20location%20mechanism.&text=When%20you%20configure%20a%20TCP,computer%20names%20to%20IP%20addresses..](https://docs.microsoft.com/en-us/windows-server/networking/dns/dns-top#:~:text=Active%20Directory%20Domain%20Services%20(AD,its%20domain%20controller%20location%20mechanism.&text=When%20you%20configure%20a%20TCP,computer%20names%20to%20IP%20addresses..)
4. **IT Services, Oxford University**. How to configure DNS for Active Directory. *Oxford University IT Services: IT Help*. [Online] [Cited: 03 02, 2021.] <https://help.it.ox.ac.uk/configure-dns-for-active-directory#collapse2530076>.
5. **Microsoft**. How DNS Support for Active Directory Works. *Microsoft*. [Online] 11 19, 2014. [Cited: 03 03, 2021.] [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759550\(v=ws.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759550(v=ws.10)?redirectedfrom=MSDN).
6. **Allen, R**. Windows Server DNS Zones Explained. *Active Directory Pro*. [Online] 11 18, 2018. [Cited: 03 03, 2021.] <https://activedirectorypro.com/windows-dns-zones-explained/#:~:text=Active%20Directory%20Integrated%20Zones&text=Integrated%20zones%20can%20be%20replicated,for%20which%20they%20are%20authoritative..>
7. **IONOS**. Installing IIS on a Server with Windows Server Minimal Installation. *IONOS*. [Online] [Cited: 03 05, 2021.] <https://www.ionos.co.uk/help/server-cloud-infrastructure/server-administration/installing-iis-on-a-server-with-windows-server-minimal-installation/>.
8. **TechTerms**. IIS. *TechTerms*. [Online] 12 11, 2013. [Cited: 03 05, 2021.] <https://techterms.com/definition/iis>.
9. **Madden, J**. Remote Desktop Services (RDS). *TechTarget*. [Online] [Cited: 03 05, 2021.] <https://searchvirtualdesktop.techtarget.com/definition/Remote-Desktop-Services-RDS>.
10. **Kemp Technologies**. Remote Desktop Services. *Kemp Support*. [Online] 12 04, 2020. [Cited: 03 05, 2021.] <https://support.kemptechnologies.com/hc/en-us/articles/203858115-remote-desktop-services>.
11. **Microsoft**. Remote Desktop Services - Access from anywhere. *Microsoft*. [Online] 03 11, 2016. [Cited: 03 05, 2021.] <https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-plan-access-from-anywhere>.

12. —. License your RDS deployment with client access licenses (CAL). *Microsoft*. [Online] 12 02, 2020. [Cited: 03 05, 2021.] <https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-client-access-license>.
13. —. Set up the Remote Desktop web client for your users. *Microsoft*. [Online] 09 19, 2019. [Cited: 03 05, 2021.] <https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-web-client-admin>.
14. —. Appendix B: Privileged Accounts and Groups in Active Directory. *Microsoft*. [Online] 05 31, 2017. [Cited: 03 04, 2021.] <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory>.
15. **Smith, RF**. Controlling User Rights and Built-in Groups. *ITProToday*. [Online] 02 19, 2002. [Cited: 03 03, 2021.] <https://www.itprotoday.com/windows-78/controlling-user-rights-and-built-groups>.
16. **Gallagher MP, O'Connor AC & Kropp, B**. *The Economic Impact of Role-Based Access Controls*. Durham, NC : RTI International, 2002.
17. **Bertram, A**. Active Directory nesting groups strategy and implementation. *TechTarget Network*. [Online] 04 08, 2020. [Cited: 03 05, 2021.] <https://searchwindowsserver.techtarget.com/tip/Active-Directory-nesting-groups-strategy-and-implementation>.
18. **Network Encyclopedia**. Domain Local Group. *Network Encyclopedia*. [Online] [Cited: 03 04, 2021.] <https://networkencyclopedia.com/domain-local-group/#:~:text=Domain%20local%20groups%20are%20Windows,control%20access%20to%20these%20resources..>