

Worksheet 2

Author: Tomos Leggett · **Student Code:** 1901852 · **Module Code:** ACCA5023

Worksheet 2

Task 1: Pre-requisite tasks

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

Task 3: Creating user account objects using Active Directory Users and

Computers snap-in console

Task 4: Object attributes of interest

Task 5: Adjoining the domain and testing user logins

Task 6: Observational Tasks

What is DNS?

What is it?

How does it work?

Other critical roles in an Enterprise Network

Group Policy

Firewalls & Security

What is a firewall?

Why would a business need one?

Why it's important to have different levels of access/roles within the 'Built in' Network User Account groups

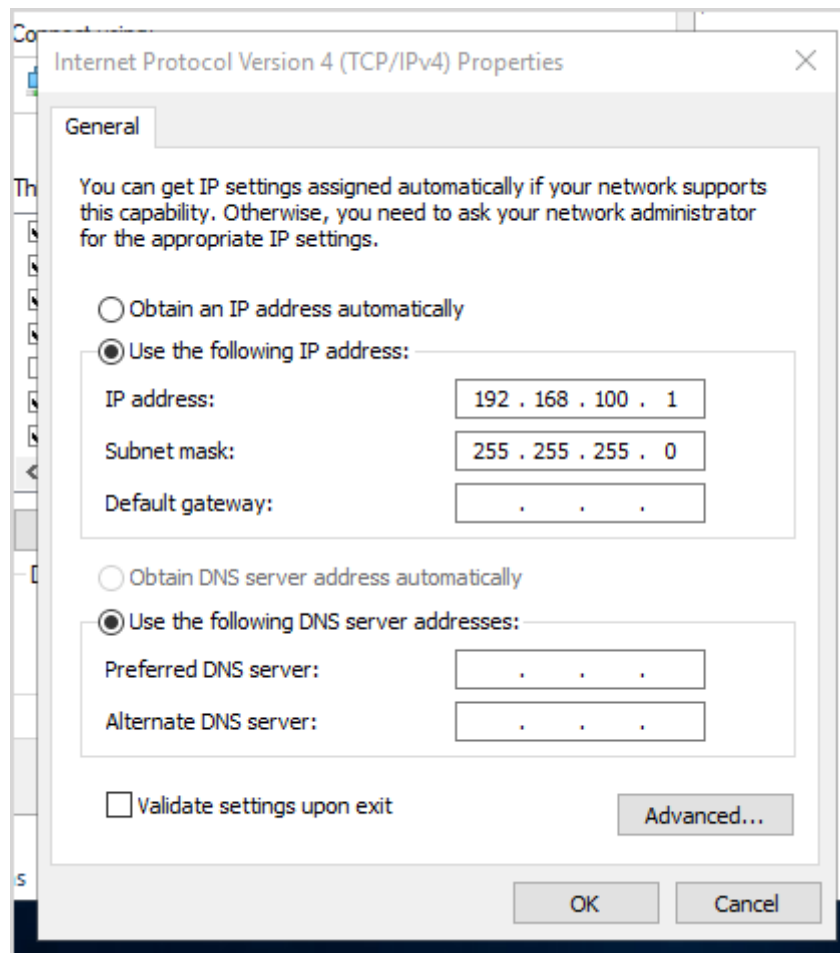
Author's opinions on Microsoft's recommendations on AGDLP and ADUDLP

What is it?

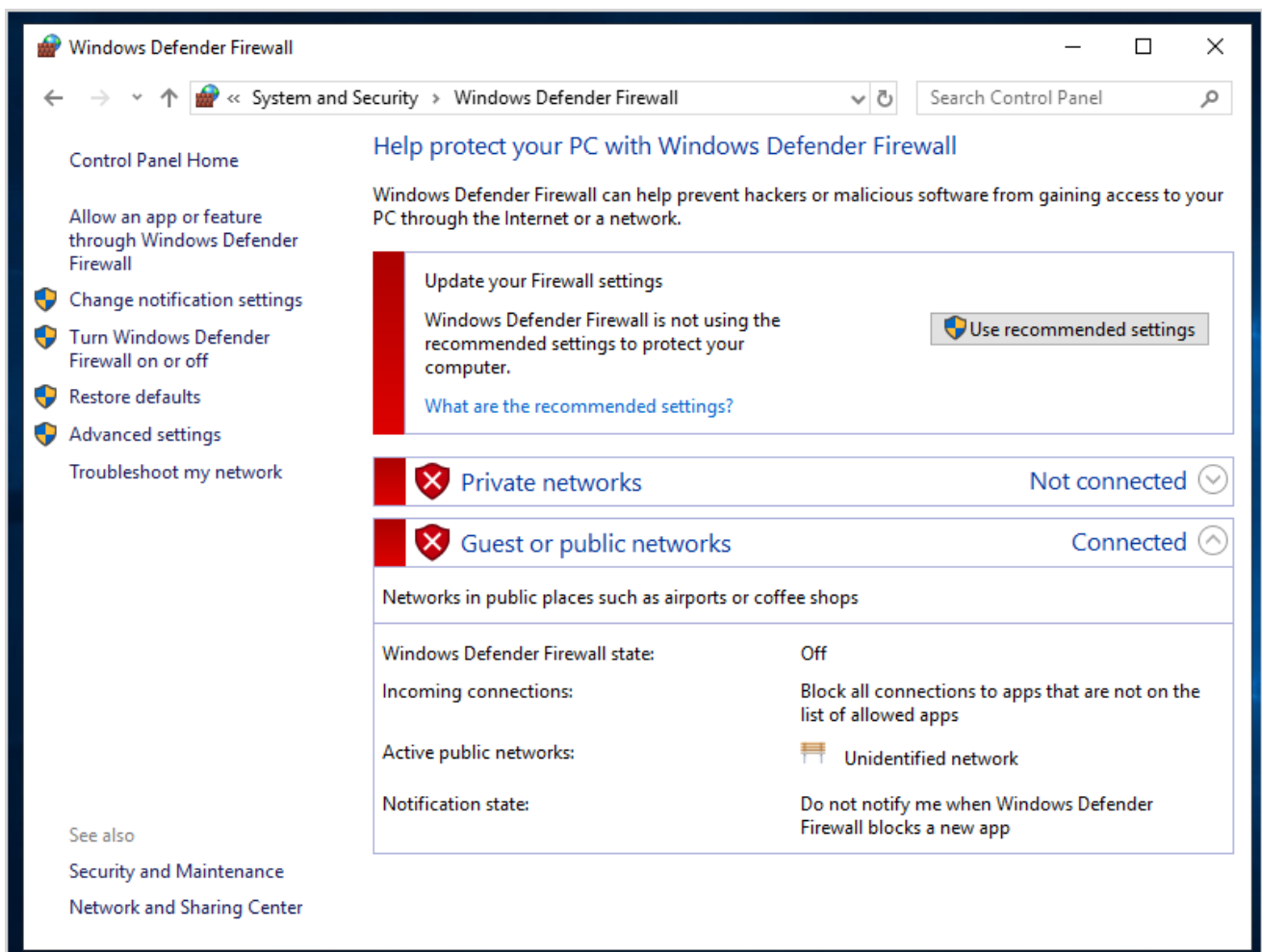
What is the author's opinion on it?

References

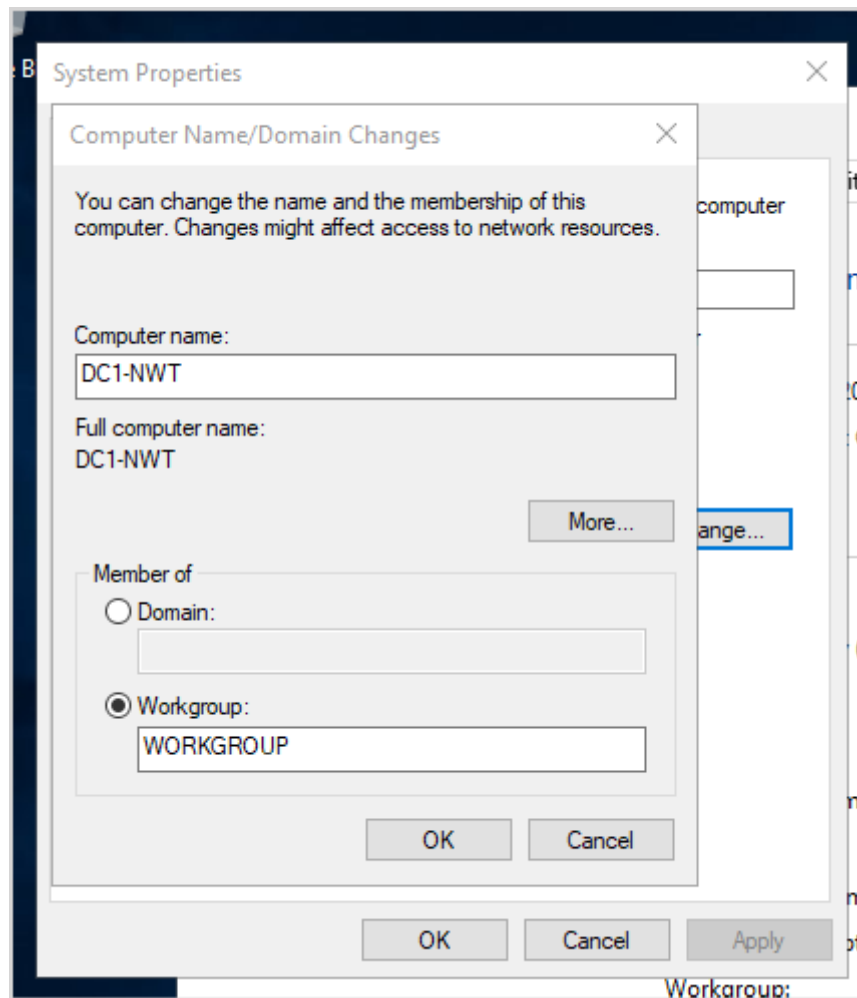
Task 1: Pre-requisite tasks



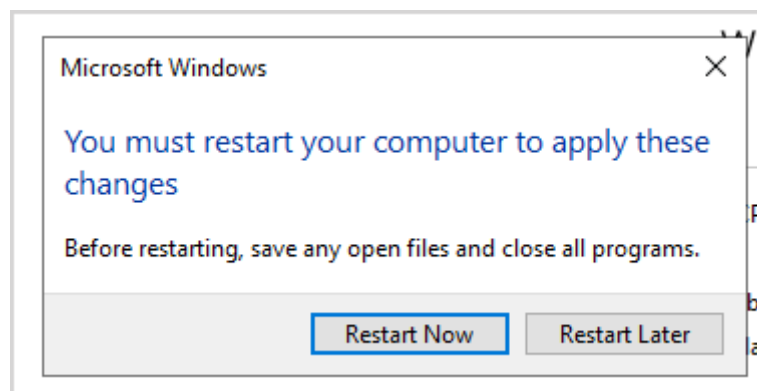
This screenshot showcases that the IP address is set as a static IP address, and that there is no DNS server setup.



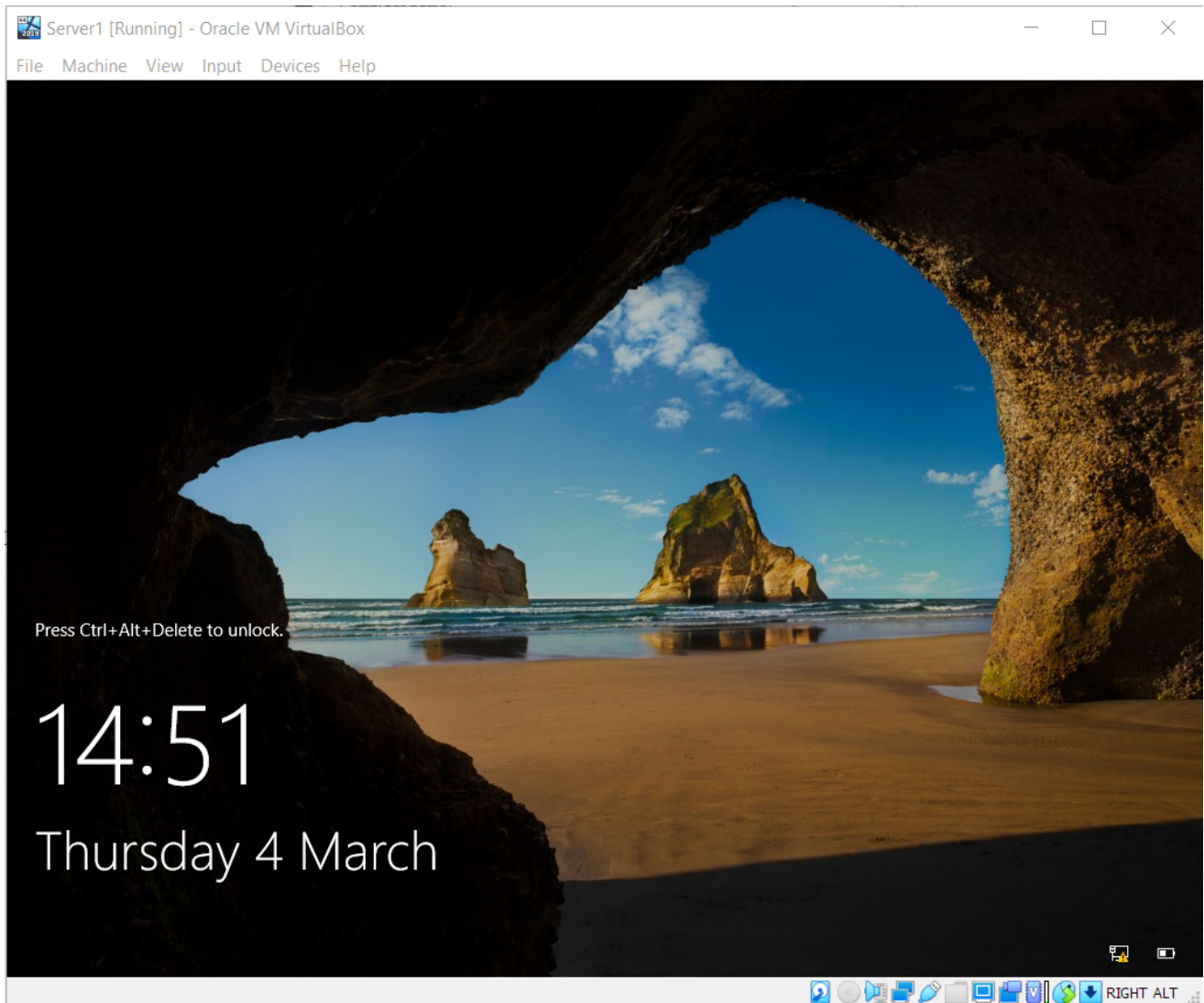
This screenshot showcases the Windows Defender Firewall current status and proves it is disabled on Server1.



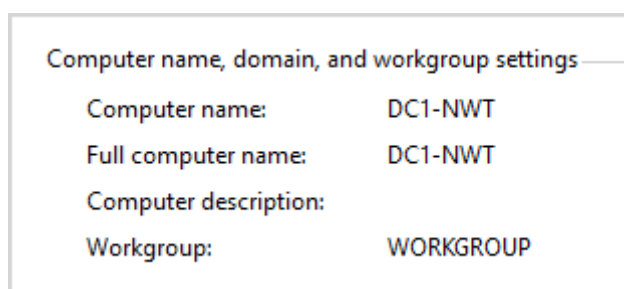
The computer was renamed to **DC1-NWT**



A prompt appeared requesting to restart the PC, **Restart Now** was selected.

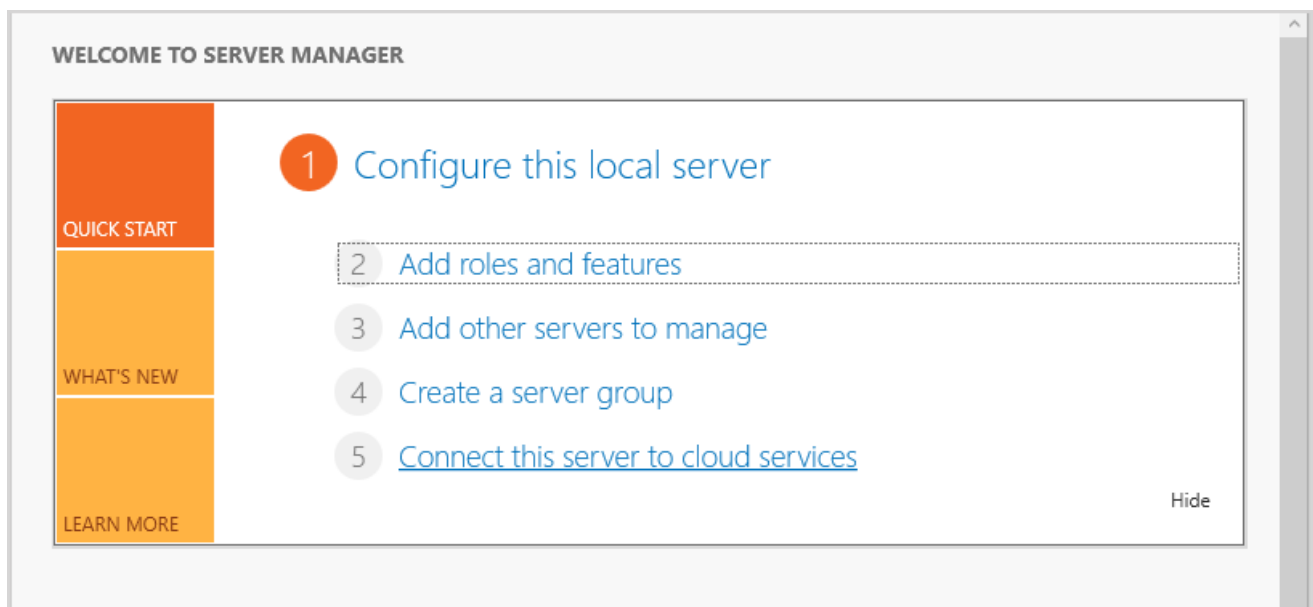


The Virtual Machine restarted successfully.

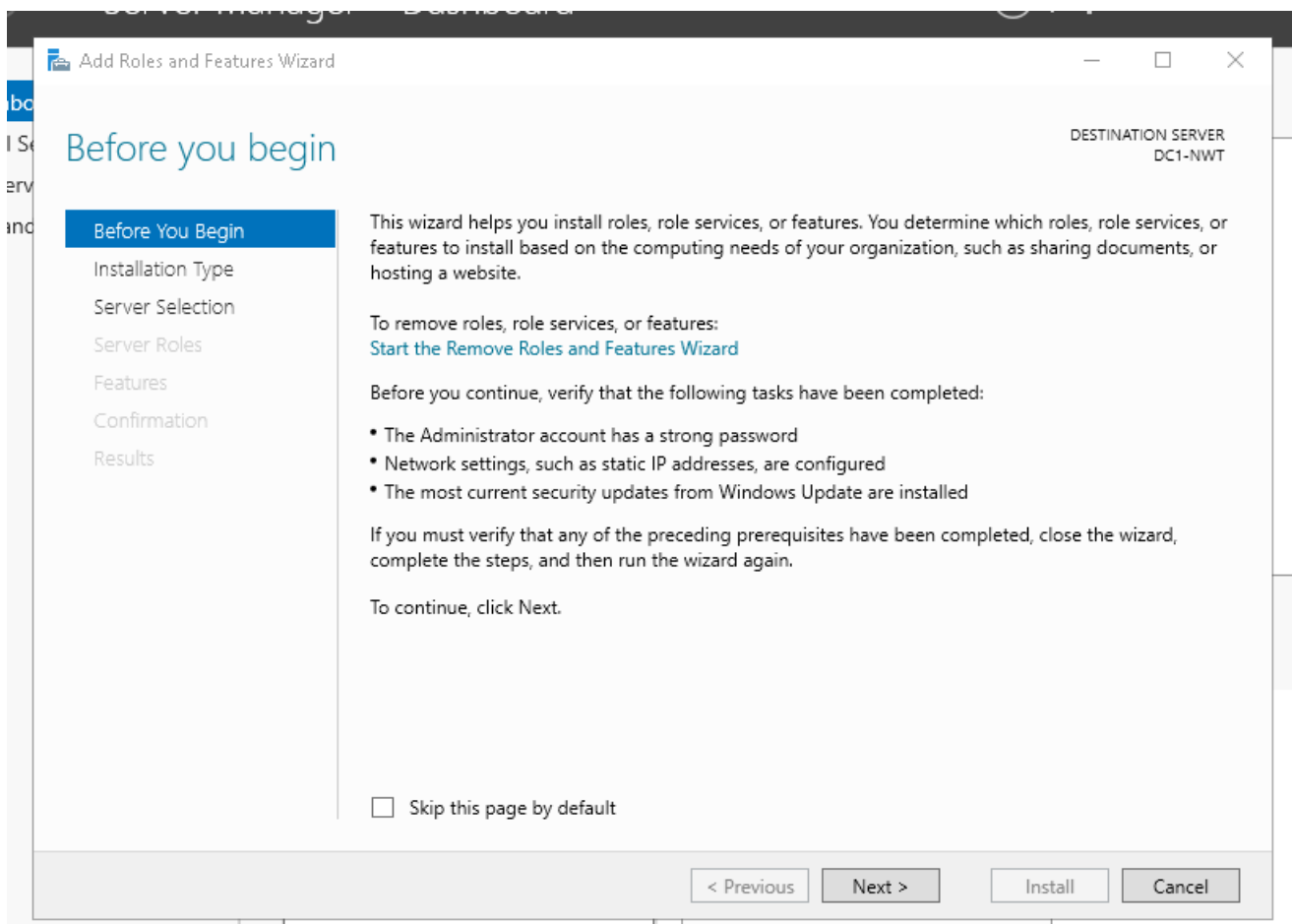


Evidence of the successful rename from the This PC properties window.

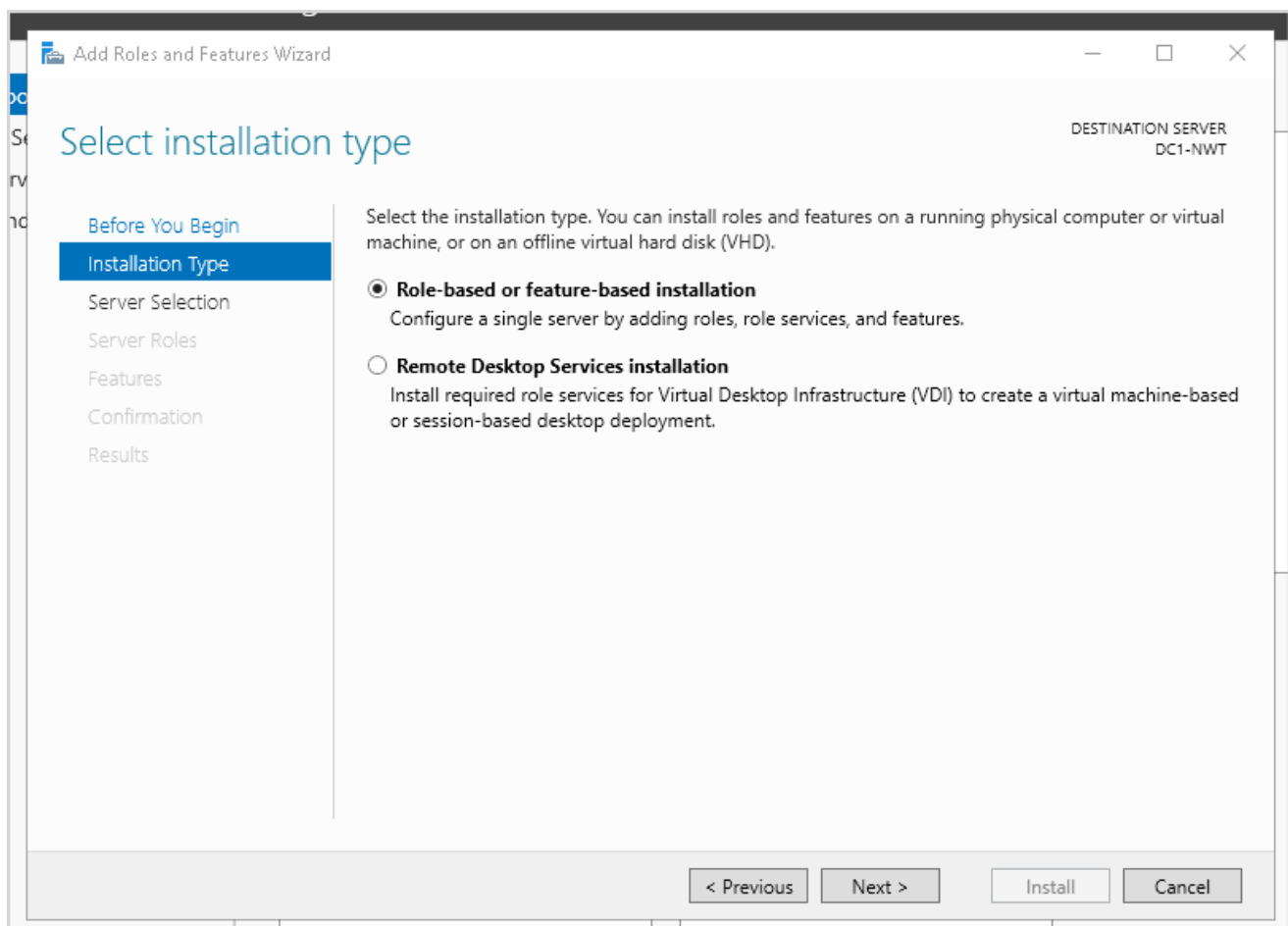
Task 2: Deploying Active Directory as a role or feature based installation



The author opened Windows Server Manager, and proceeded to select the **Add roles and features** option on the dashboard.



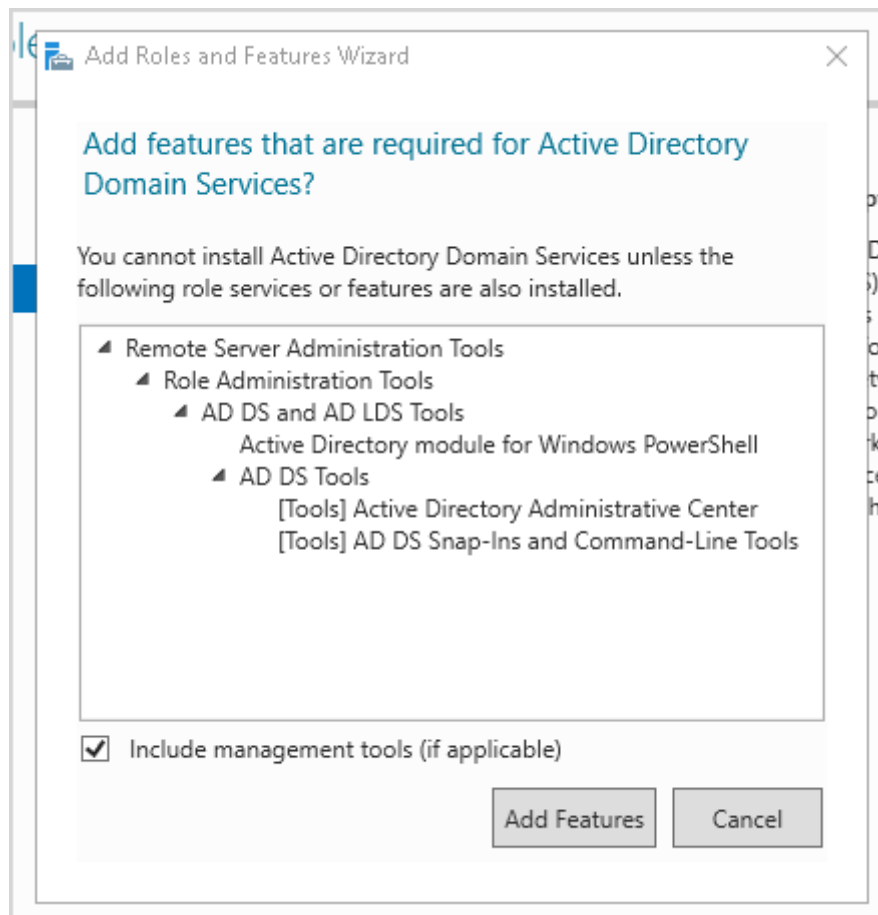
All the pre-requisites on the “Before you begin” screen have been ensured.



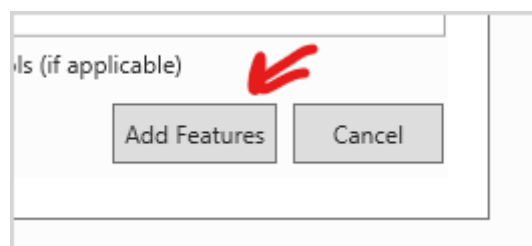
Role-based or feature-based installation was selected.

Name	IP Address	Operating System
DC1-NWT	192.168.1.100,...	Microsoft Windows Server 2019 Essentials

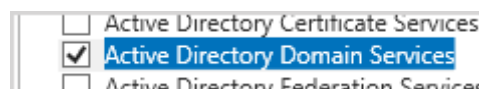
The DC1-NWT server was selected as the server.



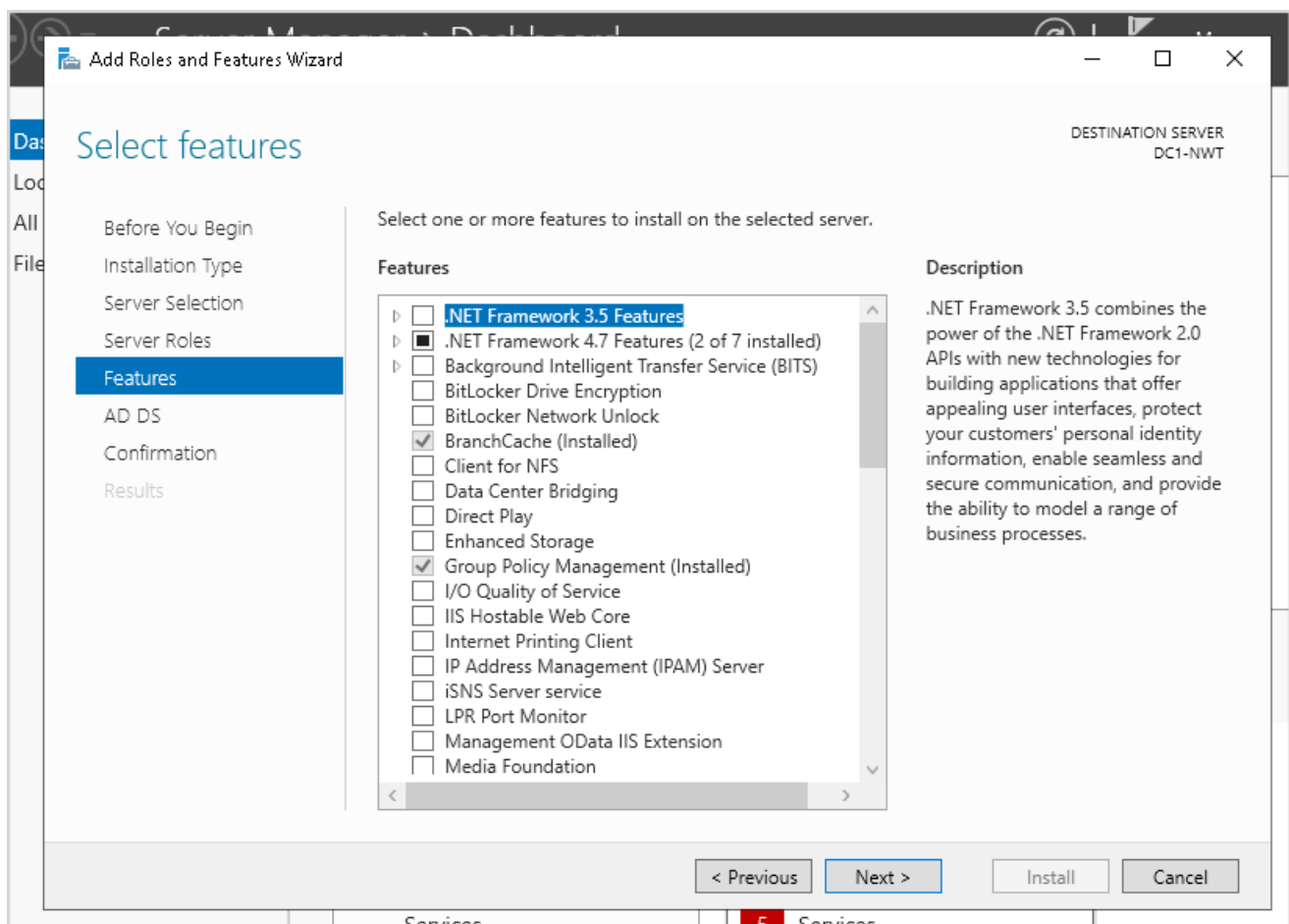
The author checked **Active Directory Domain Services** and this window appeared.



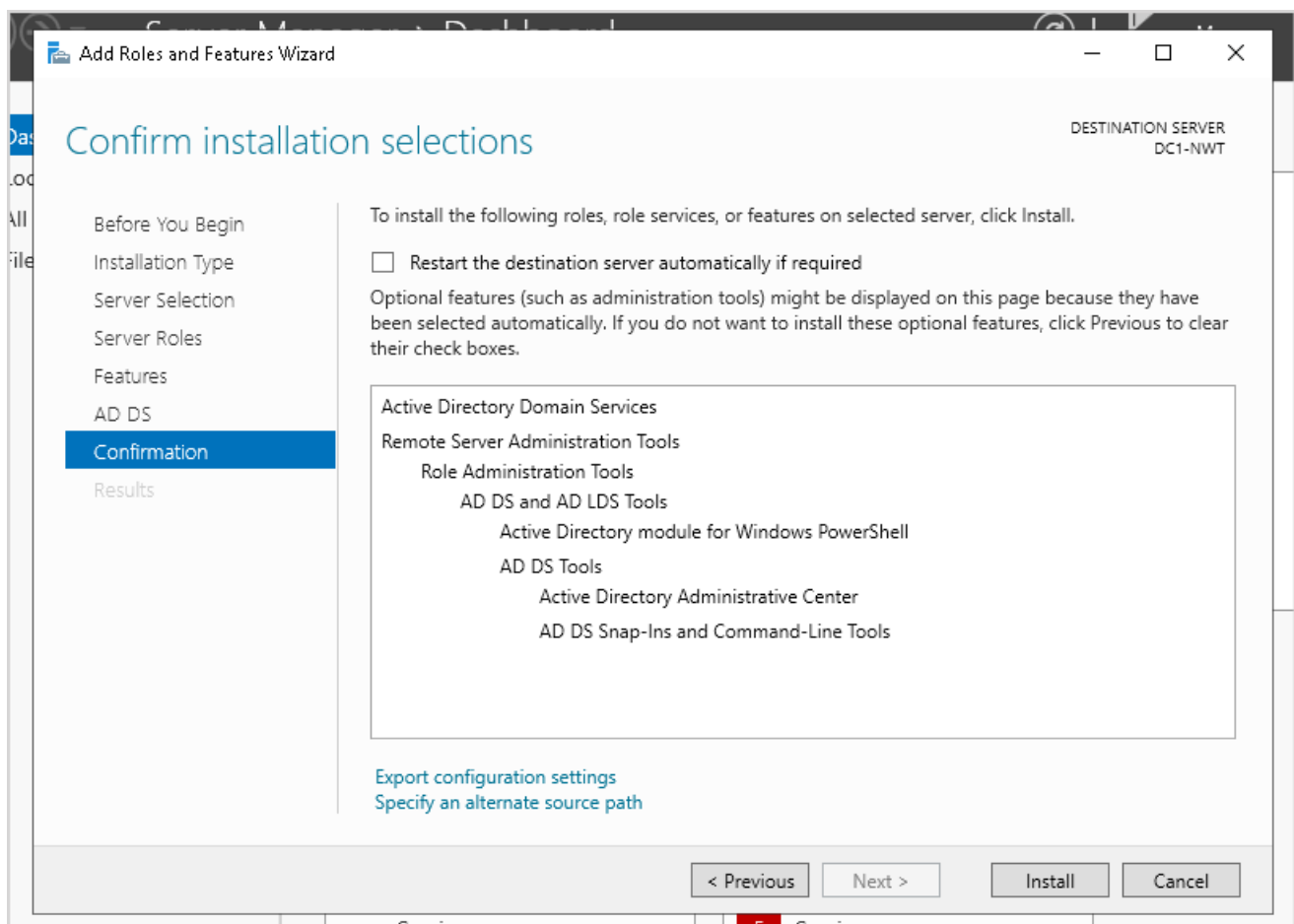
The **Add Features** option was selected.



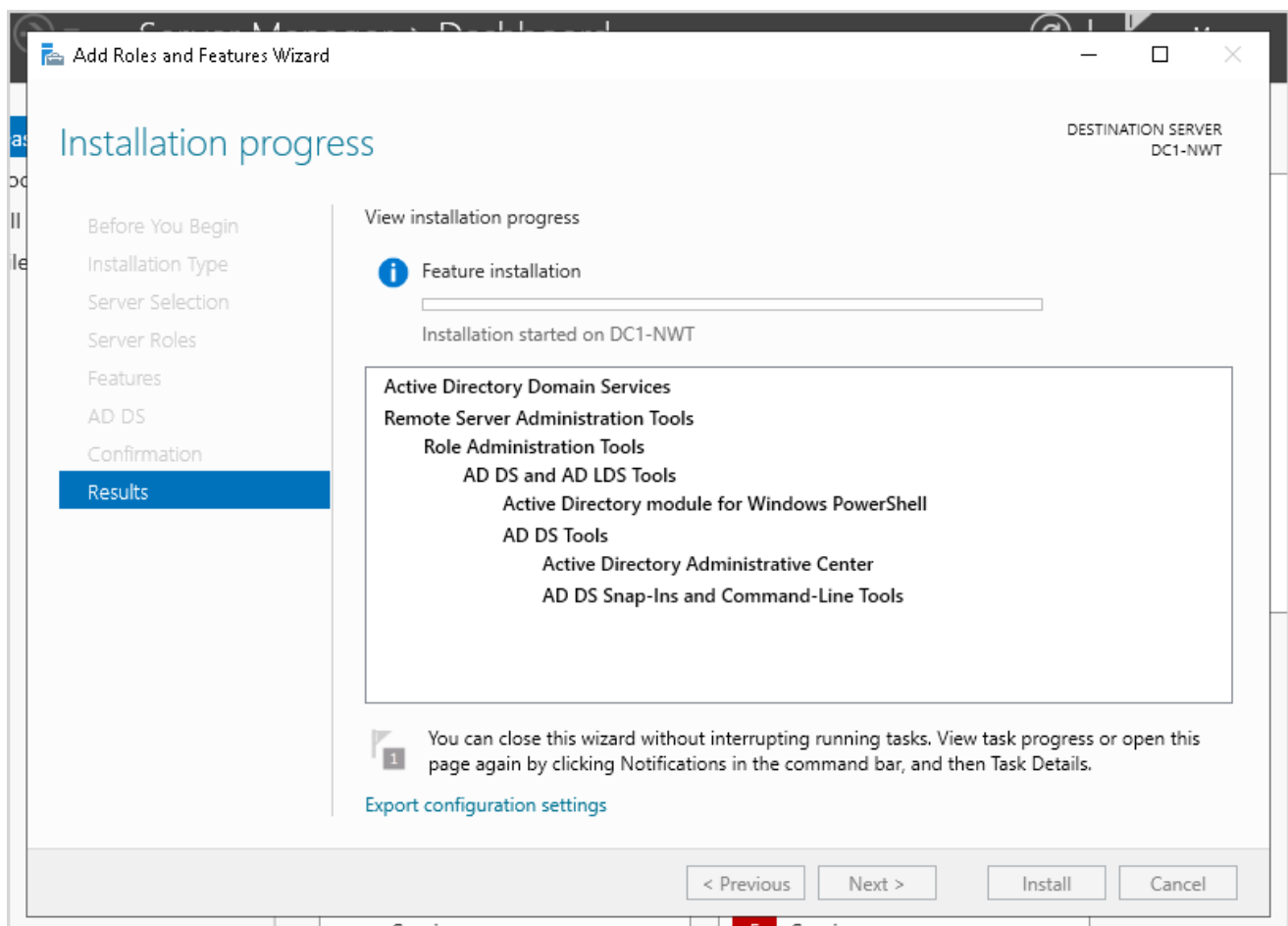
And thus, the **Active Directory Domain Services** item was checked on the features list.



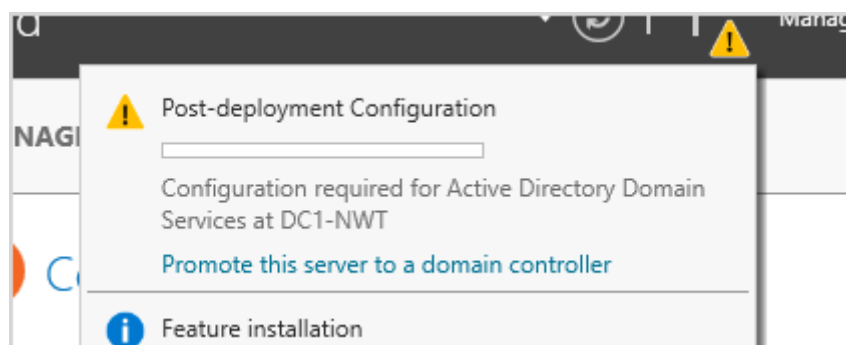
The default features were left selected.



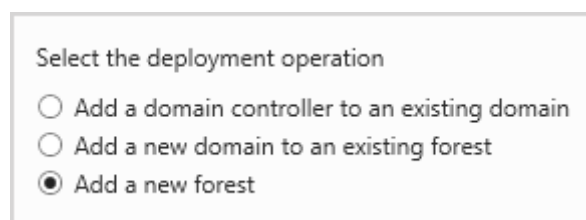
A confirmation screen appeared, and the **Install** option was selected.



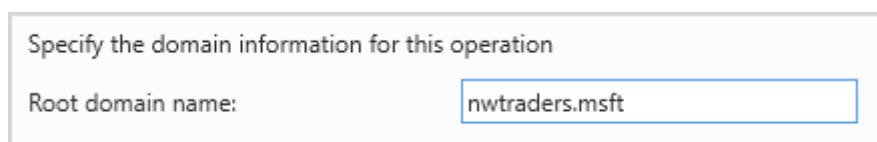
The install process began.



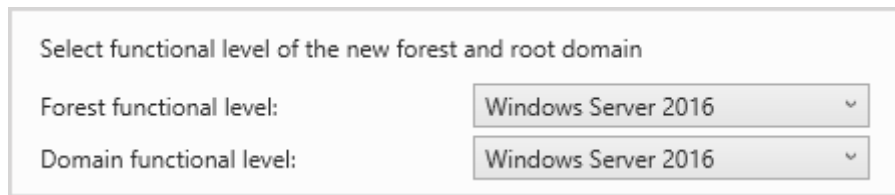
The notification prompt was opened, and the **Promote this server to a domain controller** option was selected.



As we are adding a new forest, **add a new forest** was checked under “Select the deployment operation”.



The root domain name was specified as the root domain name instructed by the brief.

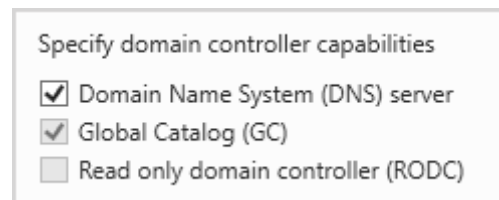


Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Windows Server 2016 was selected as the Forest functional level and Domain functional level.



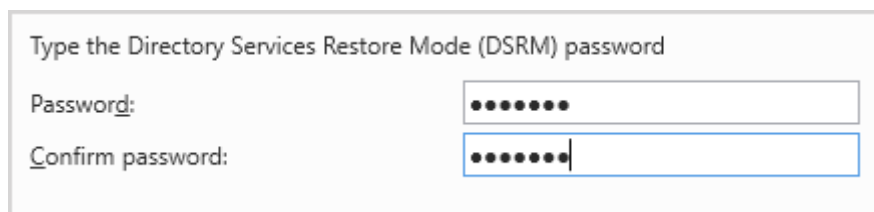
Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

The options specified by the brief were checked by default.

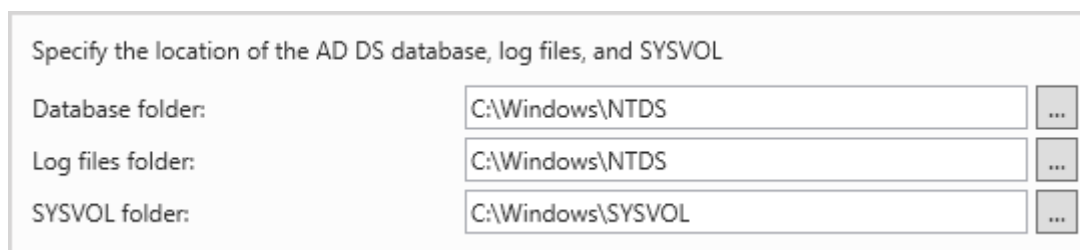


Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

The password **n3twork** was set as the Directory Services Restore Mode password as instructed by the brief.

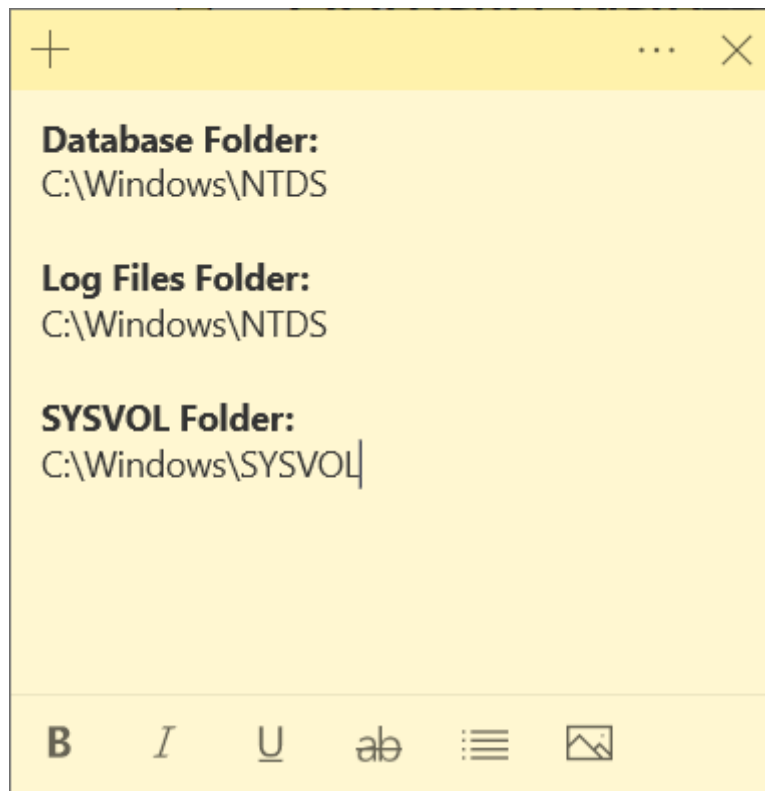


Specify the location of the AD DS database, log files, and SYSVOL

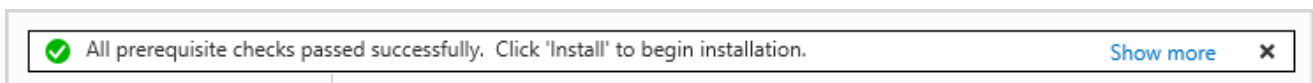
Database folder: C:\Windows\NTDS

Log files folder: C:\Windows\NTDS

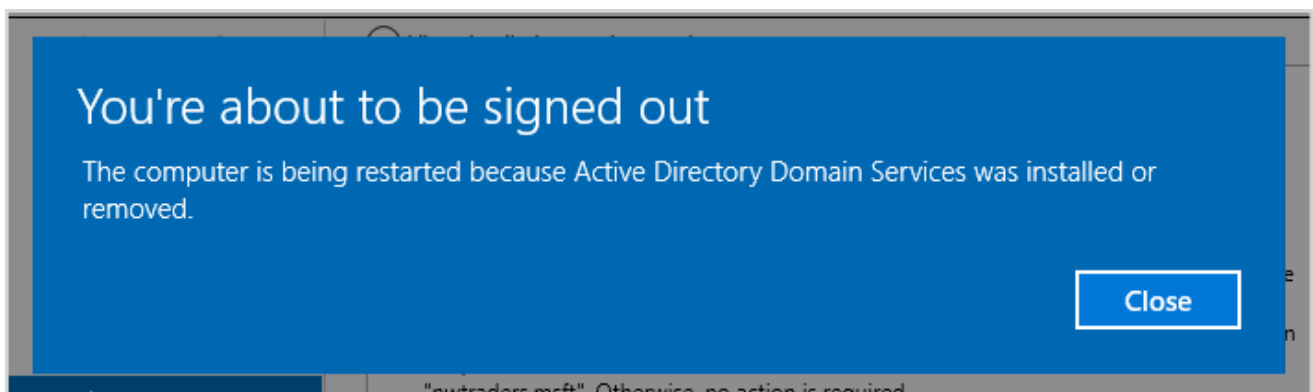
SYSVOL folder: C:\Windows\SYSVOL



As required by the brief, the author made a note of the folder directories on a sticky note on the host system.



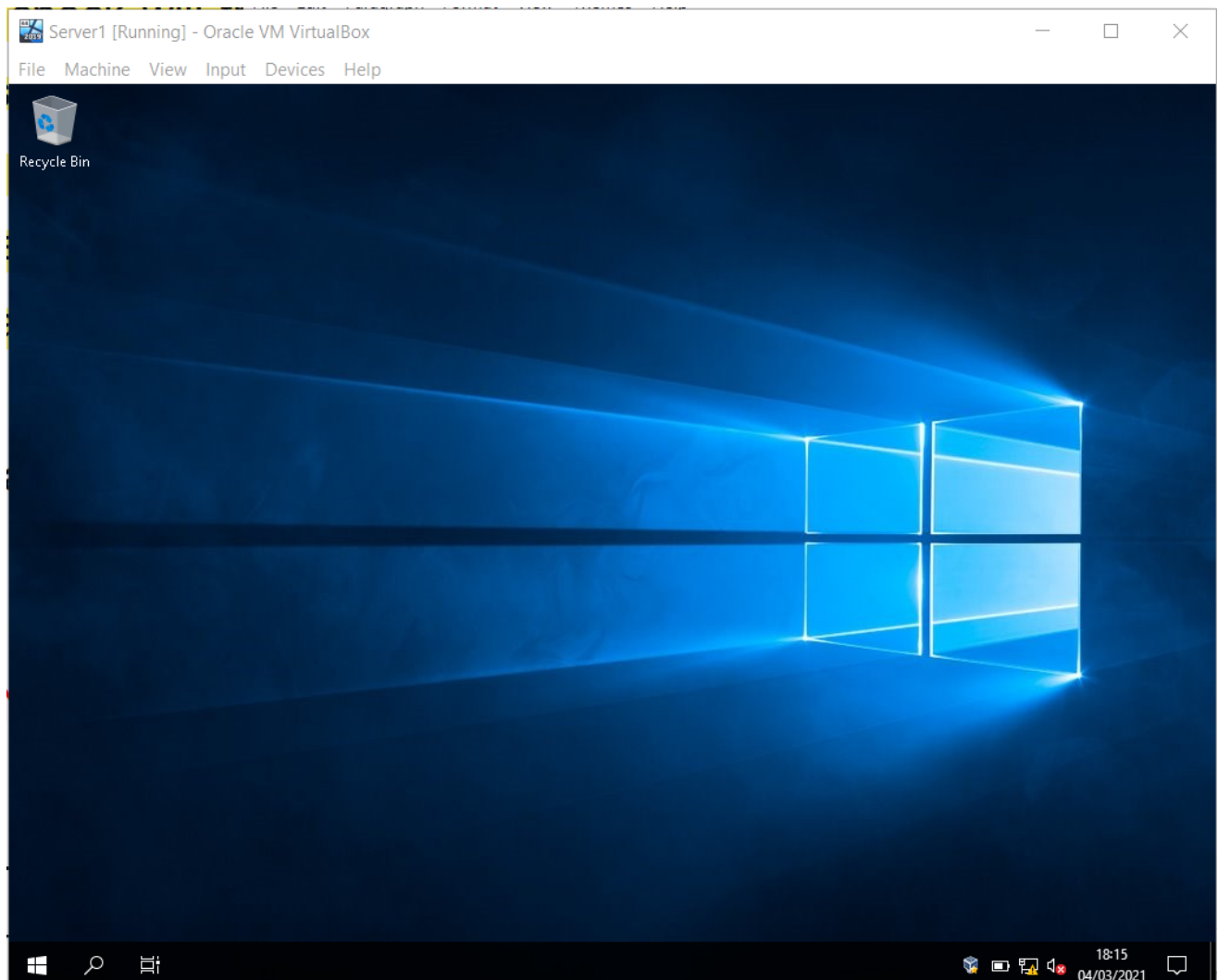
The prerequisite check passed successfully.



Active Directory was install successfully – The system restarted automatically.

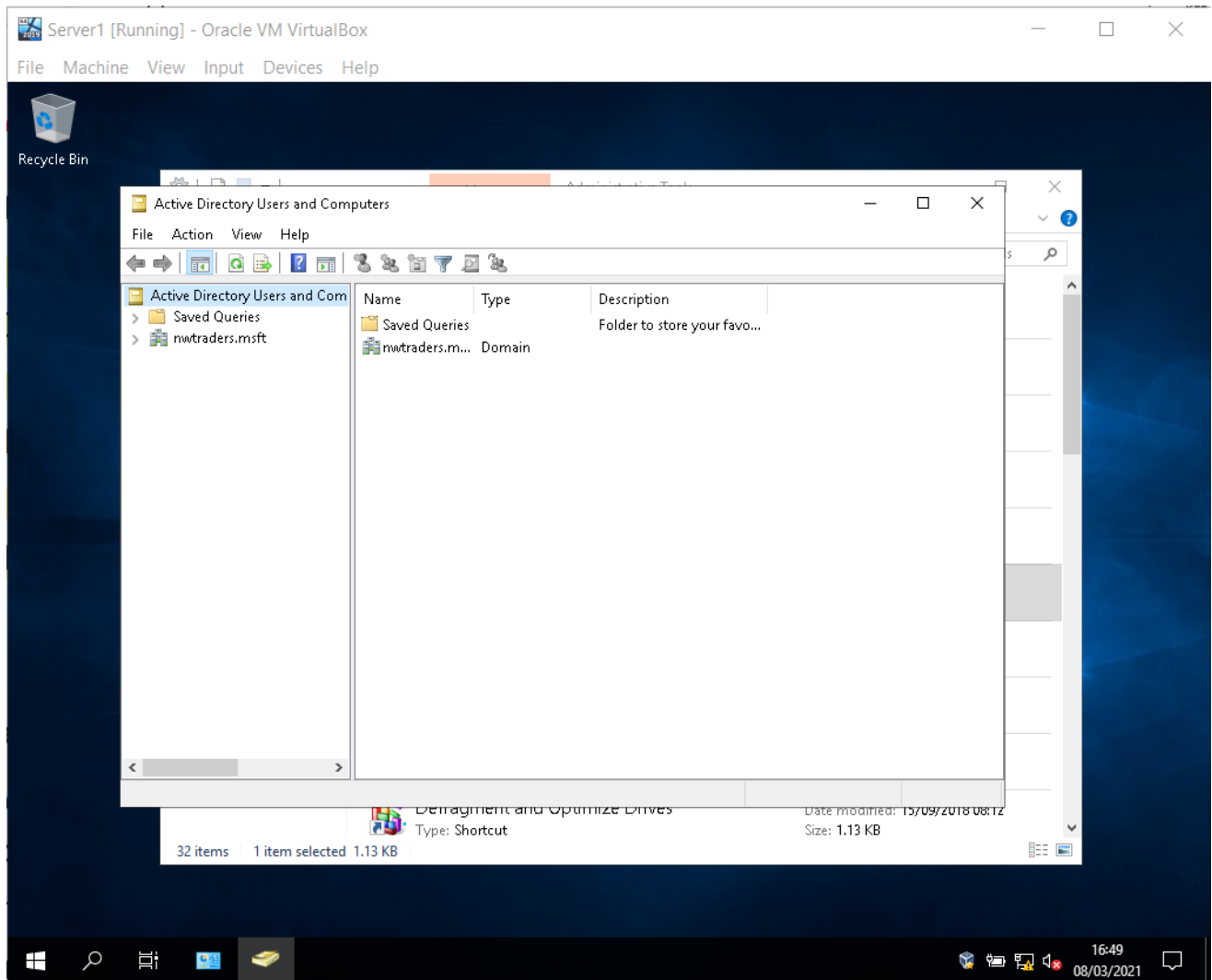


The default password (**P@ssw0rd**) was entered.

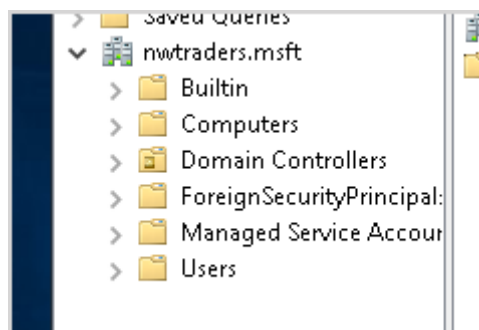


The desktop appeared successfully.

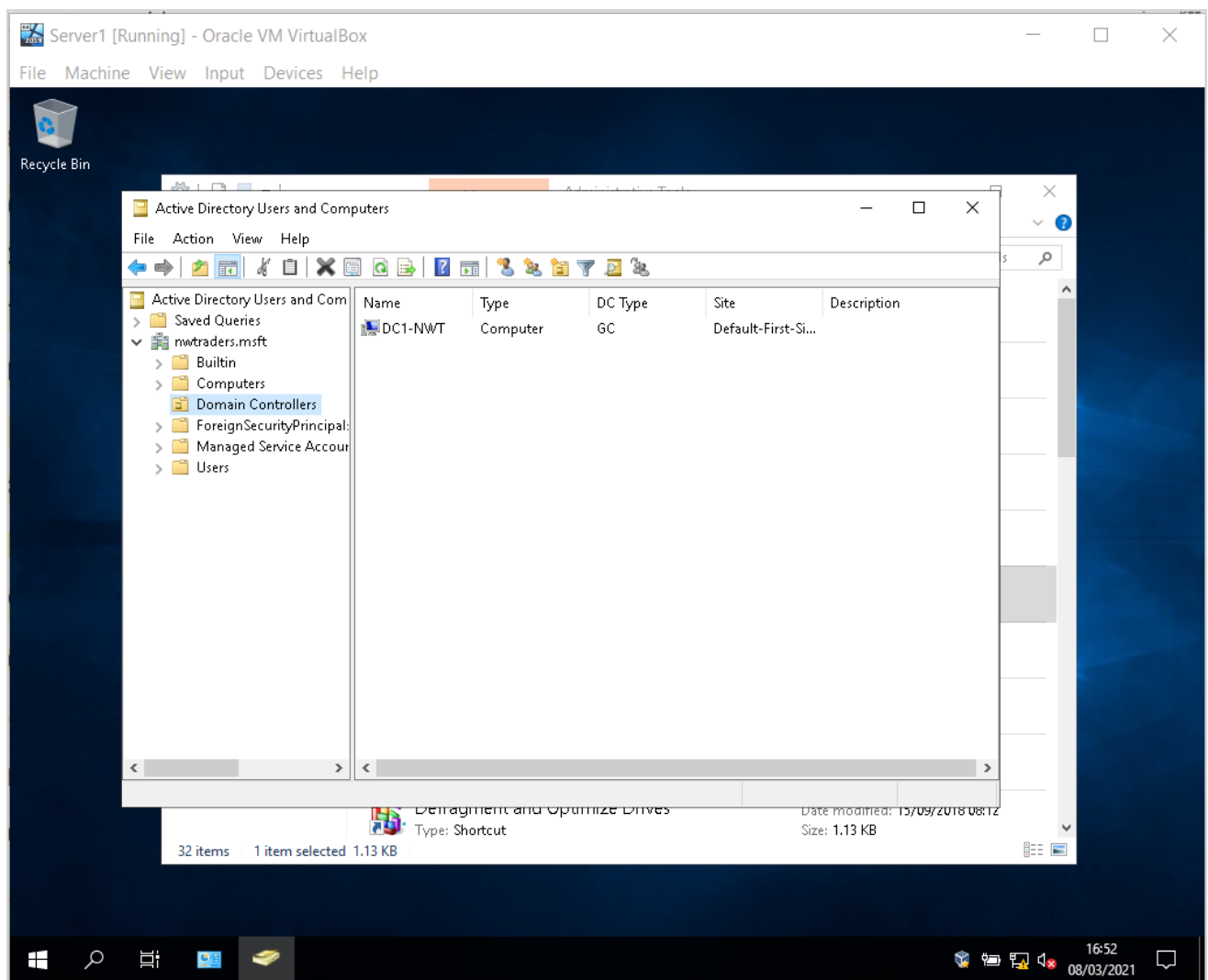
Task 3: Creating user account objects using Active Directory Users and Computers snap-in console



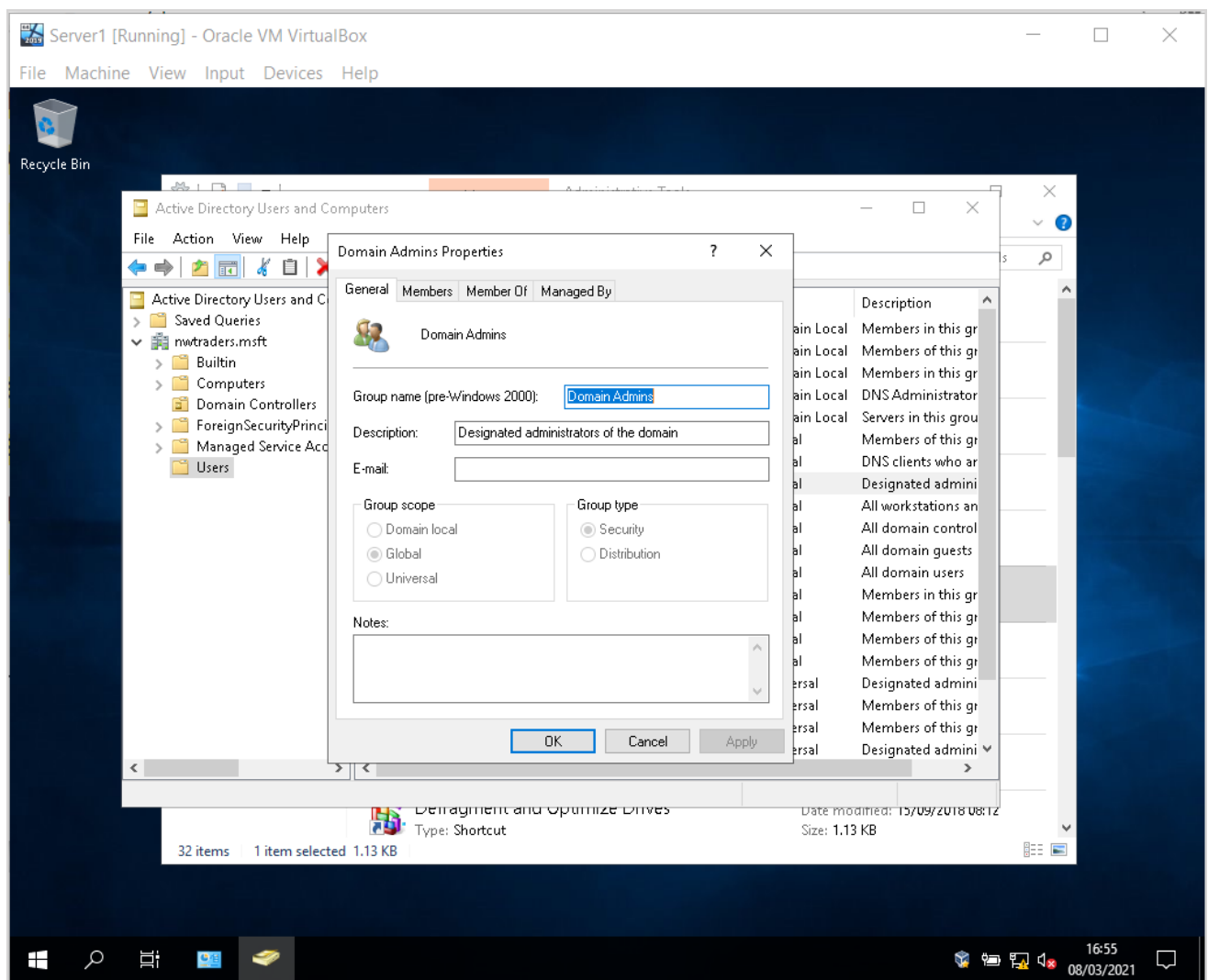
Active Directory Users and Computers from the Administrator Tools was opened by the author as required by the brief.



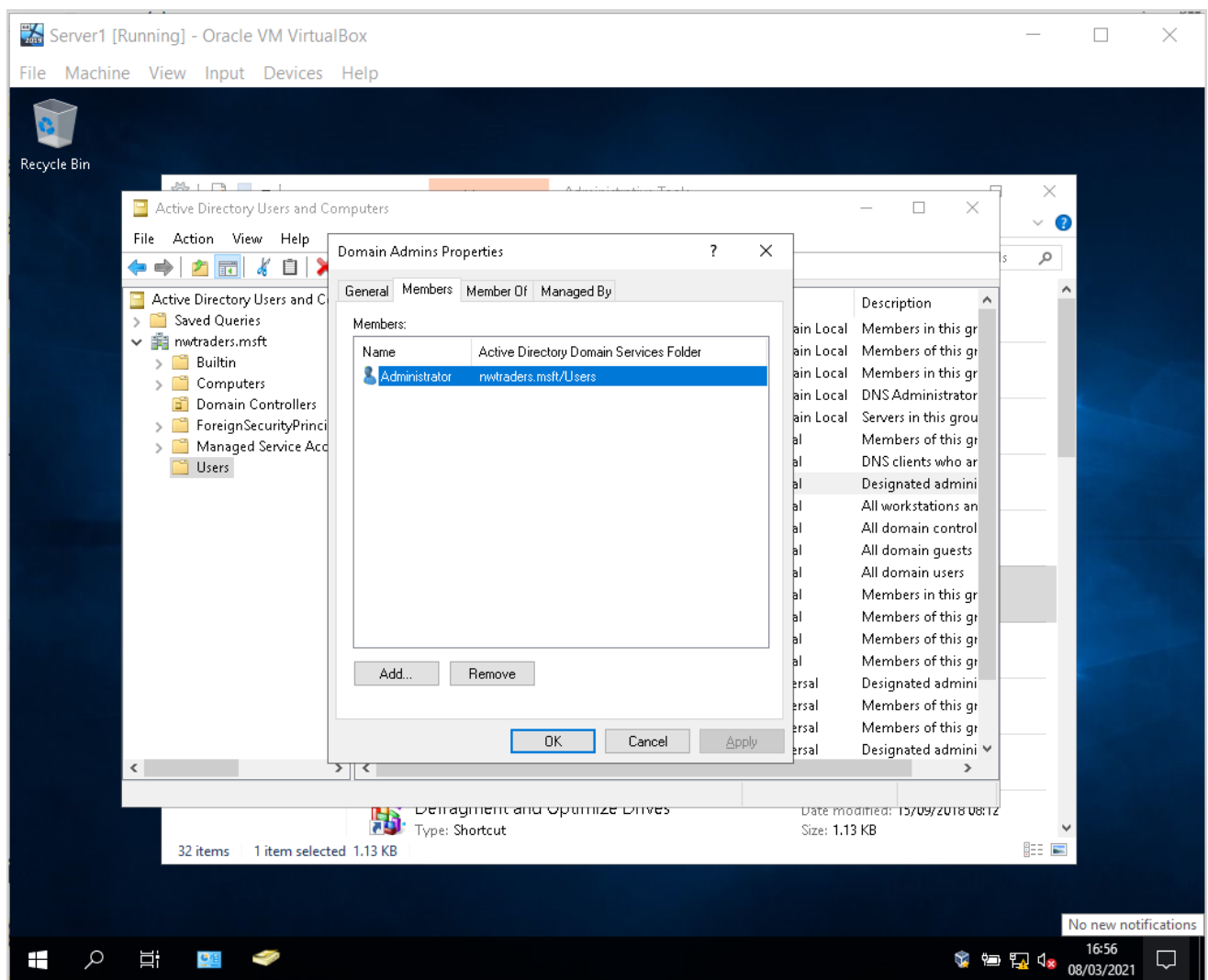
the **nwtraders.msft** domain was expanded



Here you can see **DC1-NWT** is listed as a domain controller.



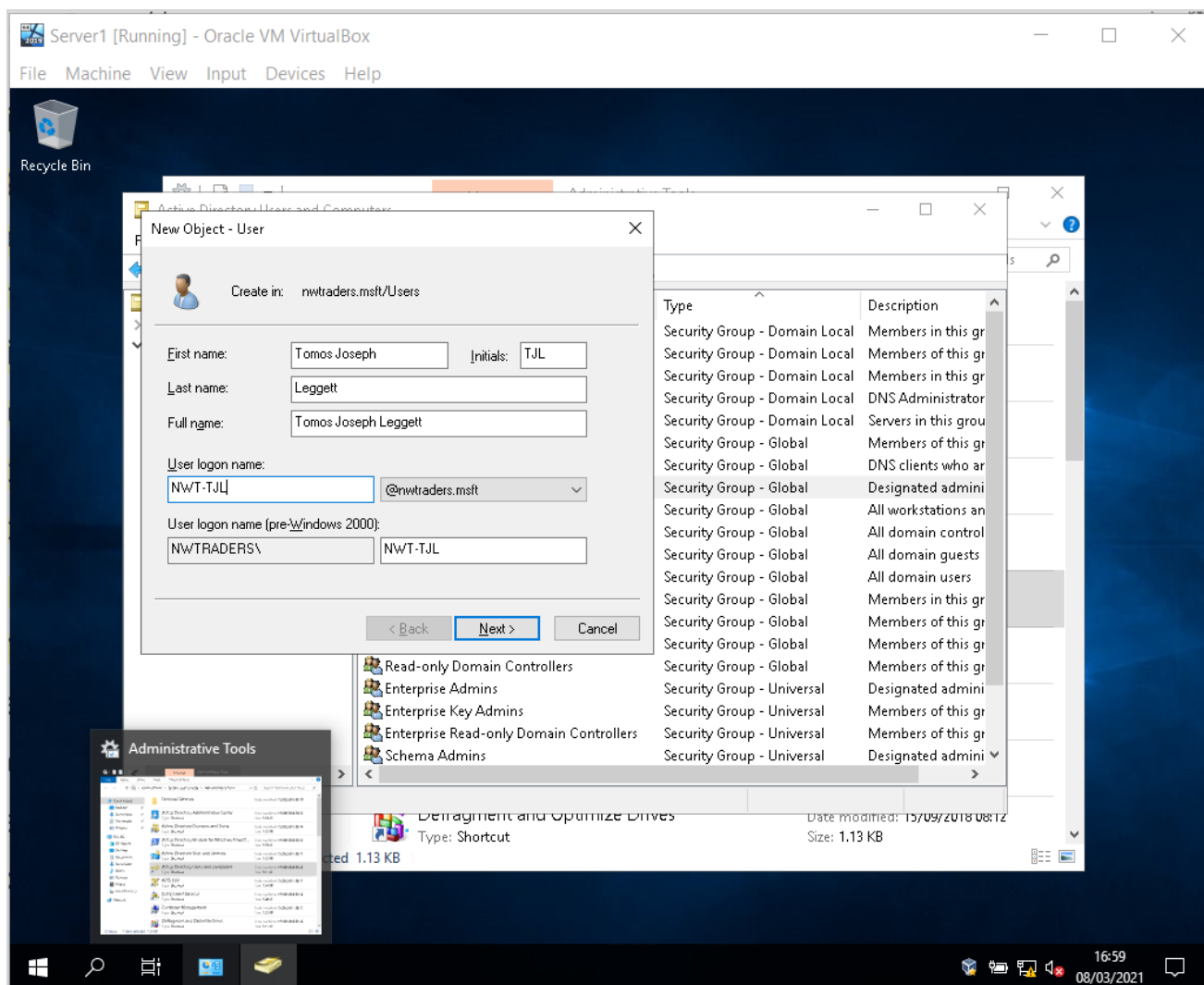
The domain admins property window was launched.



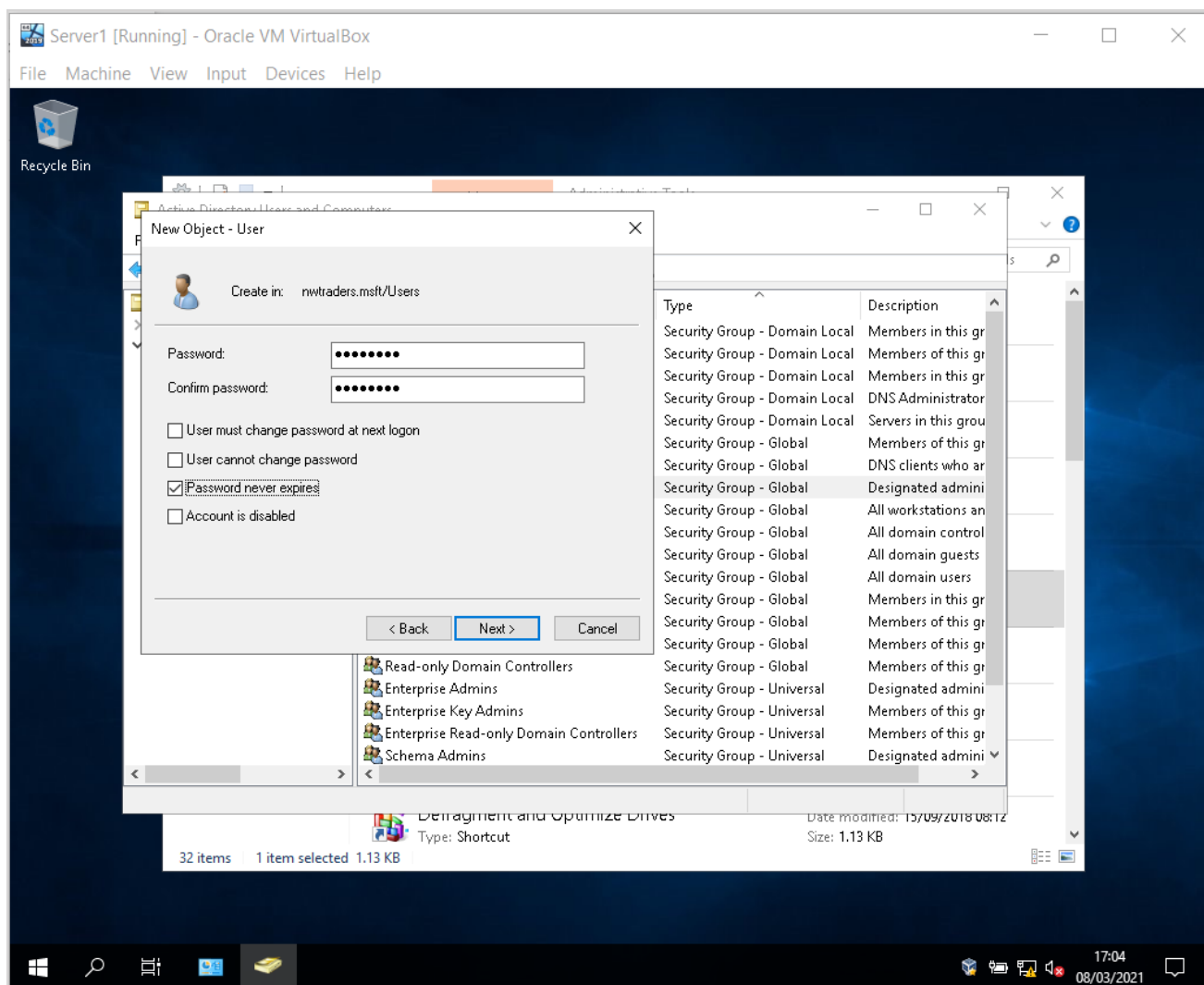
The author switched to the **Members** tab. The author was instructed to create an additional account as a fail safe if the default Administrator Account was hacked or access complications arise.



The author will create a new user.

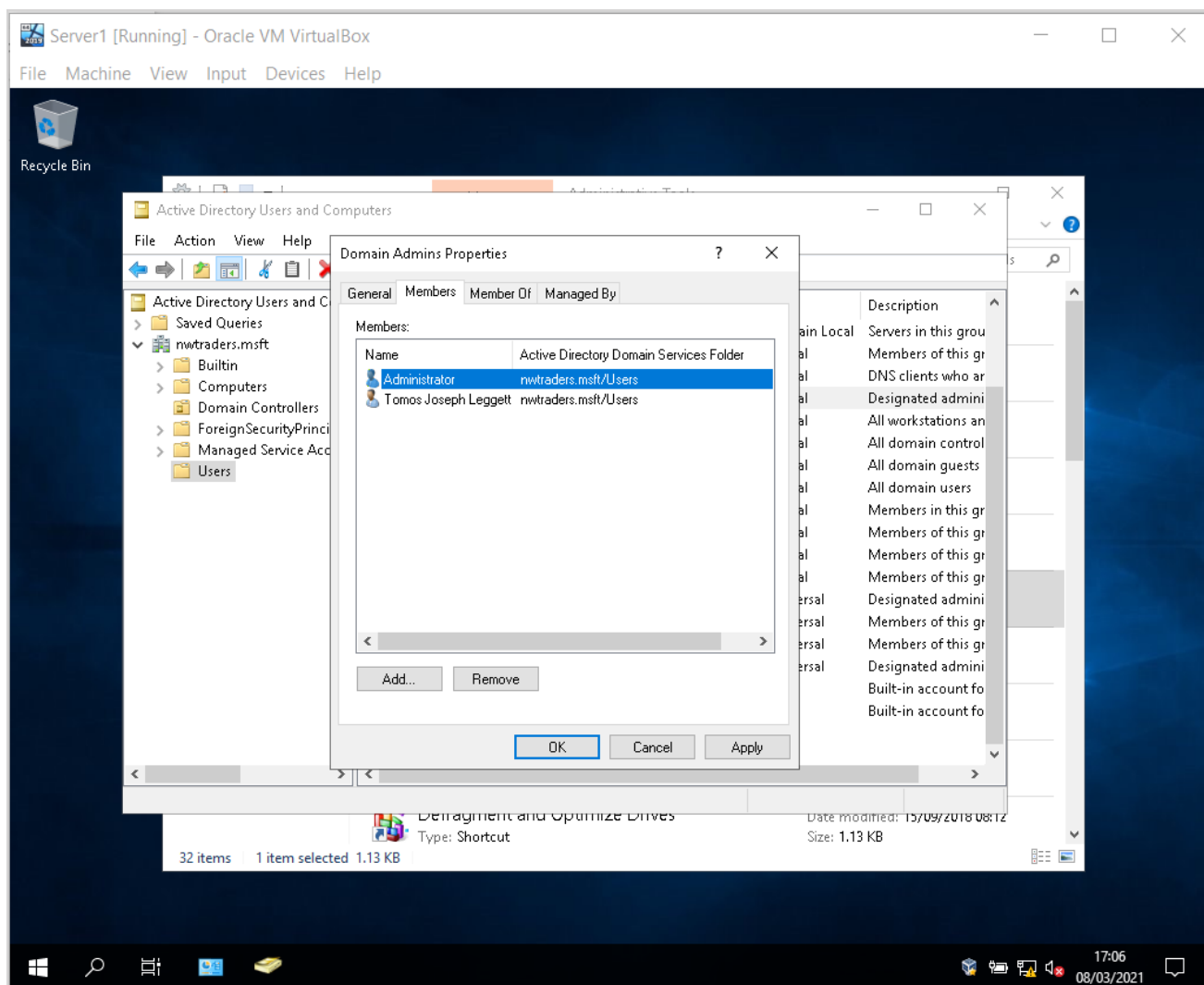


The author has set the username as **NWT-TJL@nwtraders.msft**



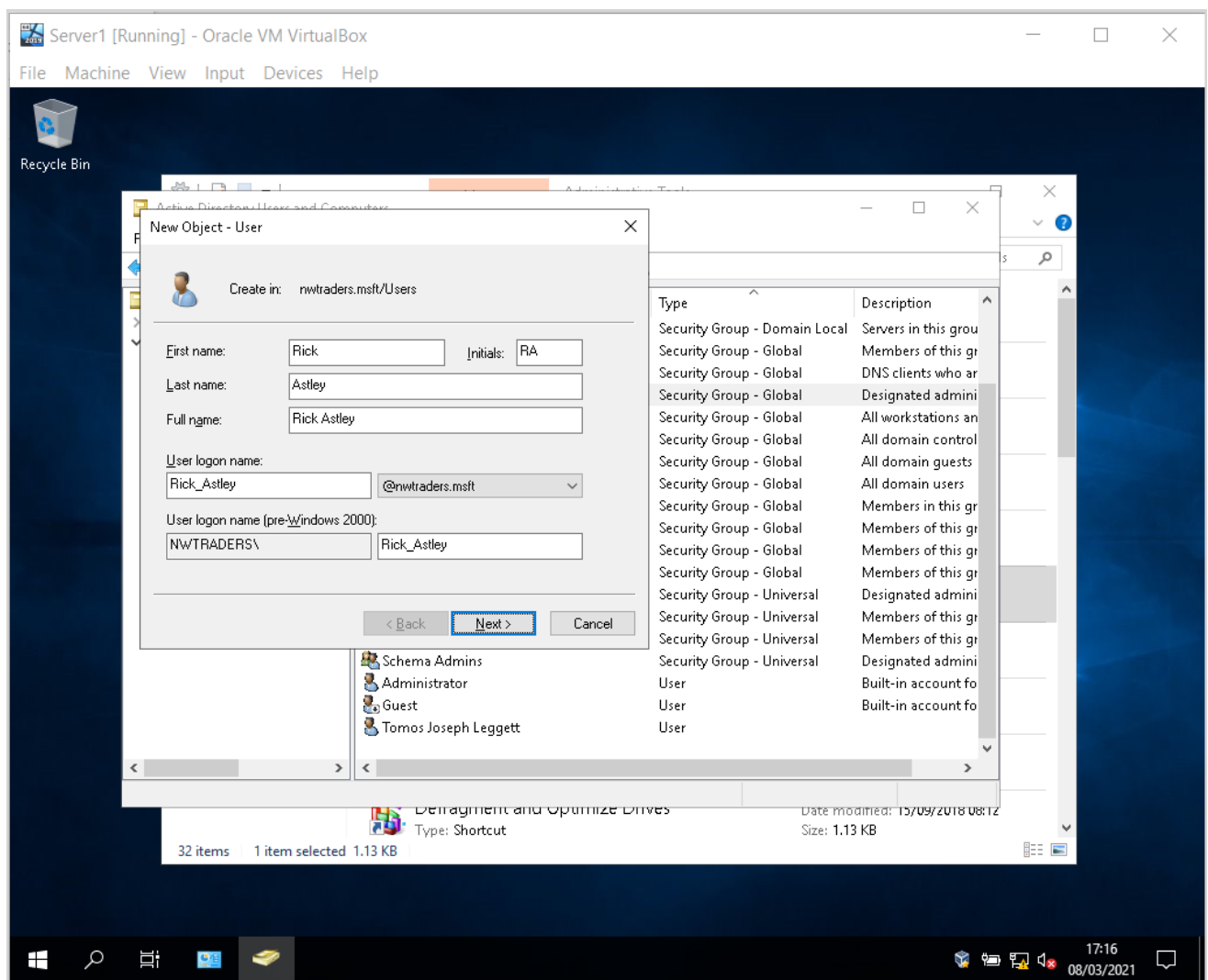
The password was set to **T@L6M69@**.

The password was set to never expire and “User must change password at next logon” was unchecked.



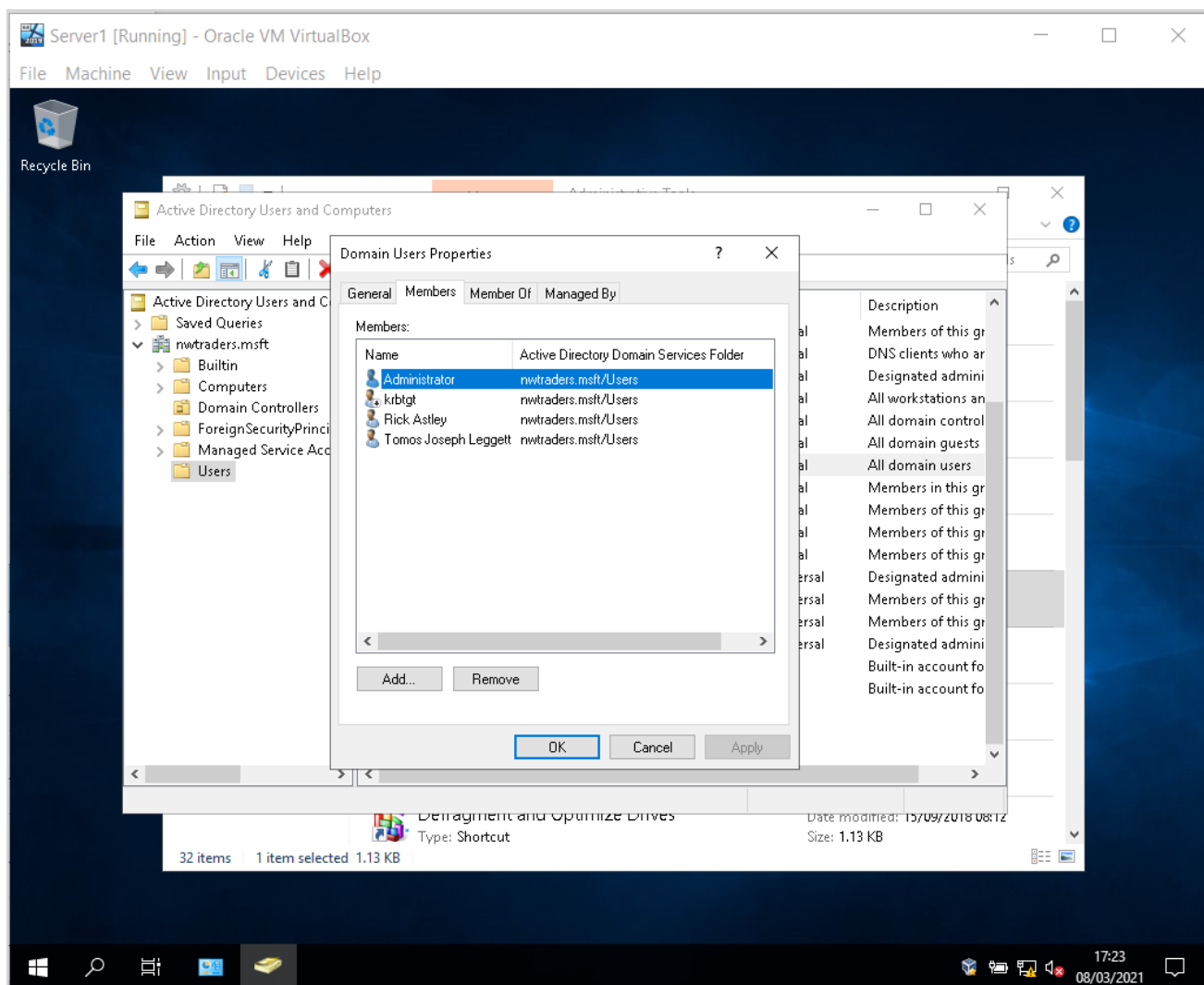
Under the Domain Admin Group, My user account (Tomos Joseph Leggett) was added to the group.

Task 4: Object attributes of interest

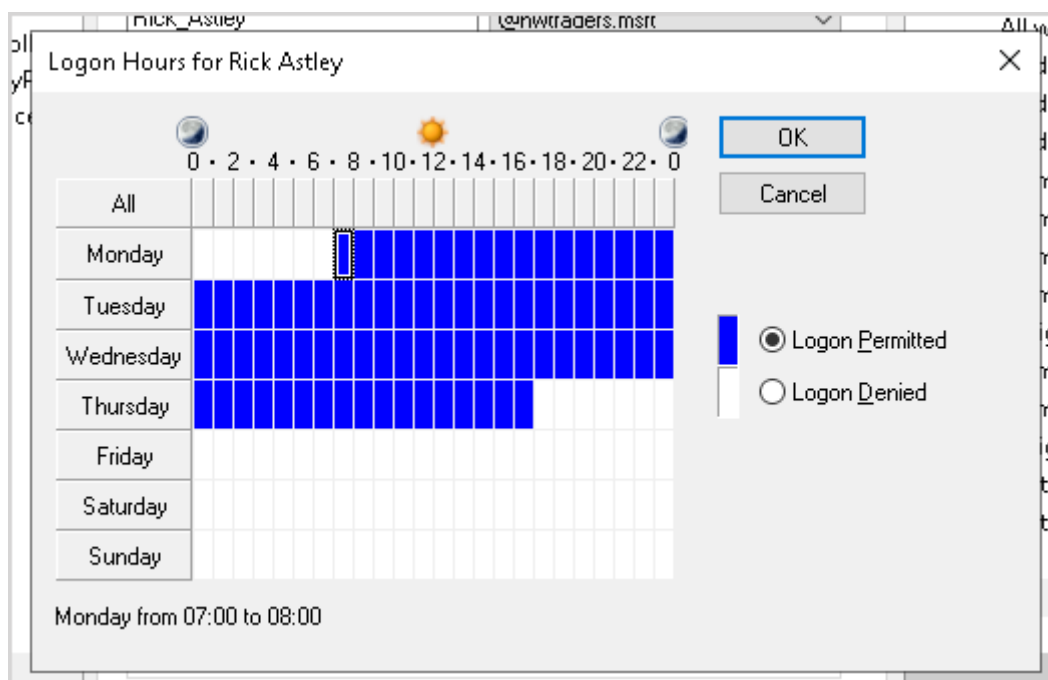


A new user named **Rick Astley** was created.

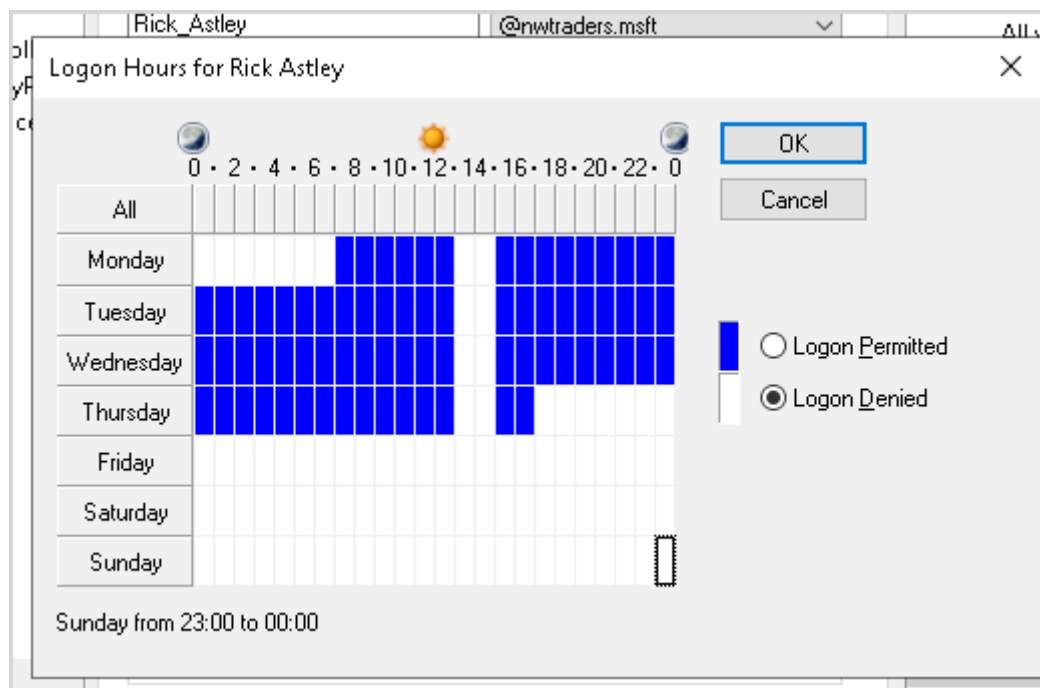
The password was set as @NgGyU!



Rick Astley appeared in the Domain Users Members.



Rick Astley's Logon times were set between **Monday 8am** and **Thursday 5pm**, as instructed by the brief.

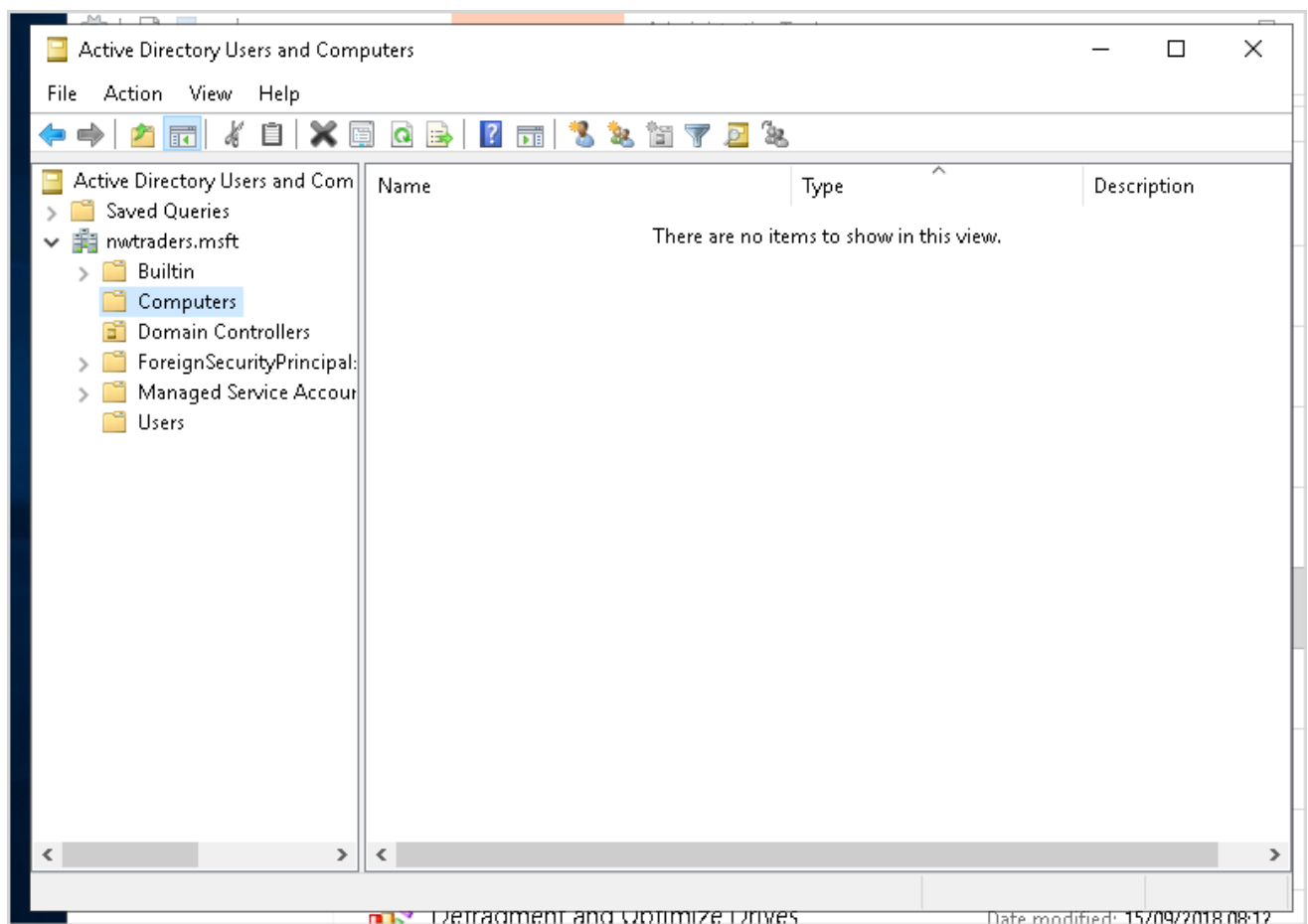


The user was also restricted from log-on access between 1pm and 2pm everyday.

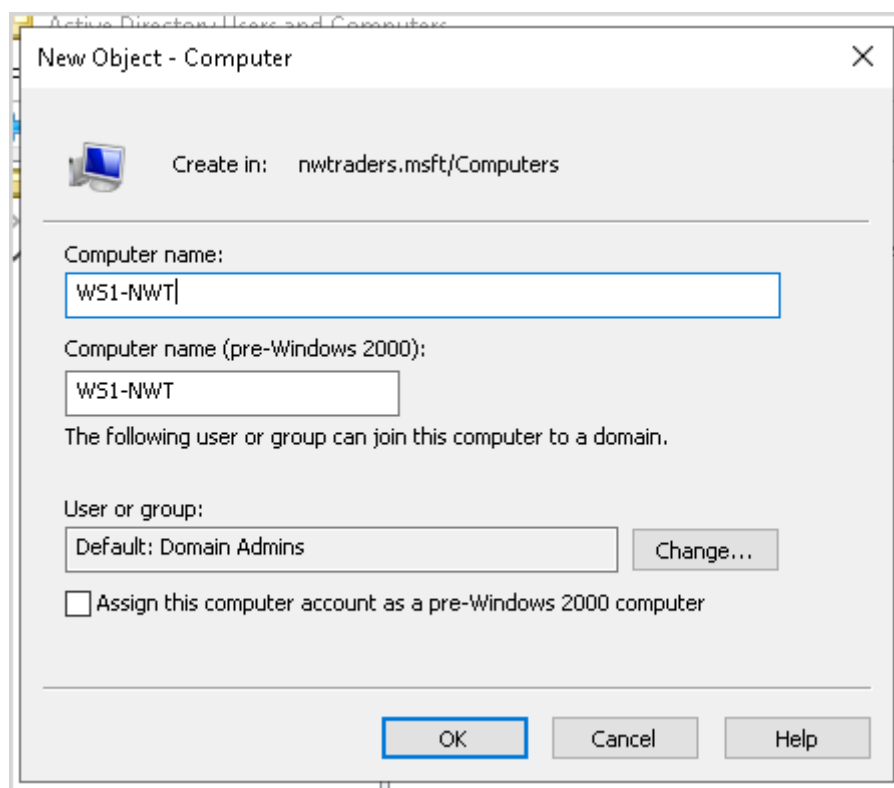


Rick was restricted from changing their password as well.

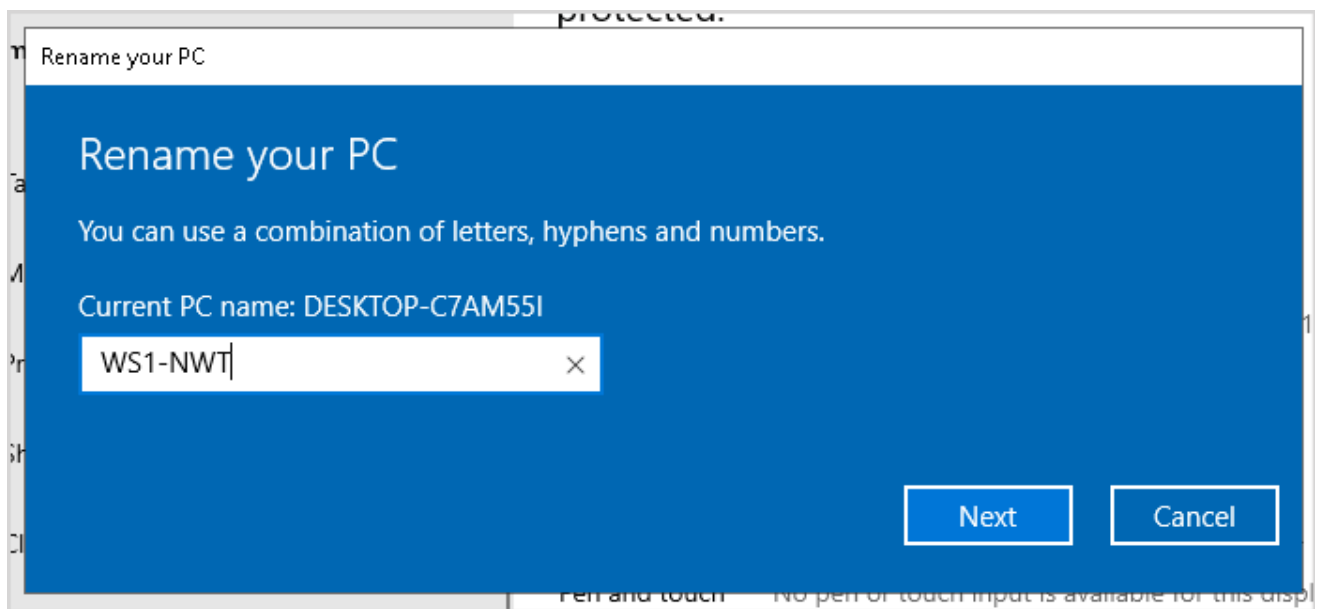
Task 5: Adjoining the domain and testing user logins



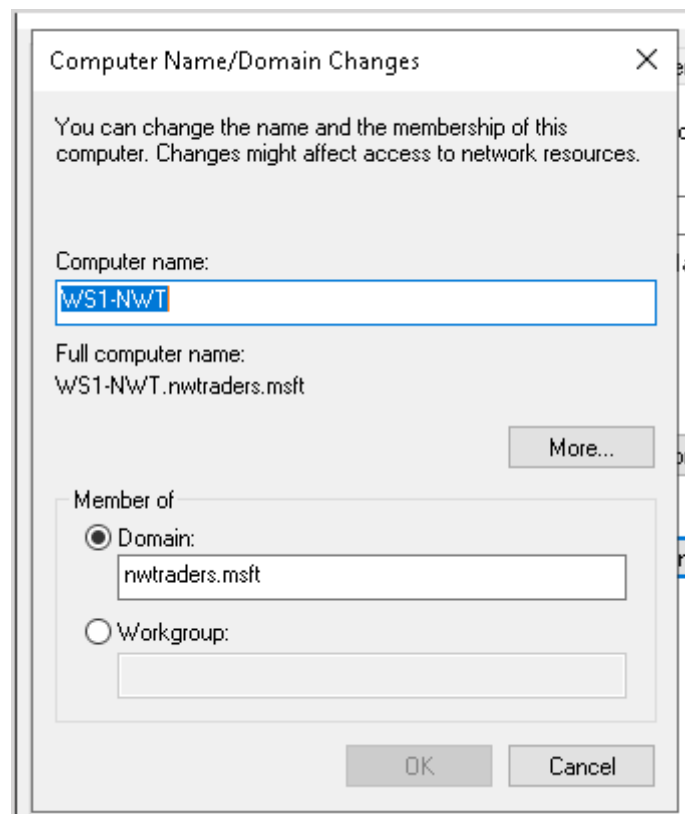
Verification that there are no client computers connected, as requested by the brief.



A new computer was created, named **WS1-NWT**.



On Client 1, the computer was renamed to **WS1-NWT**.

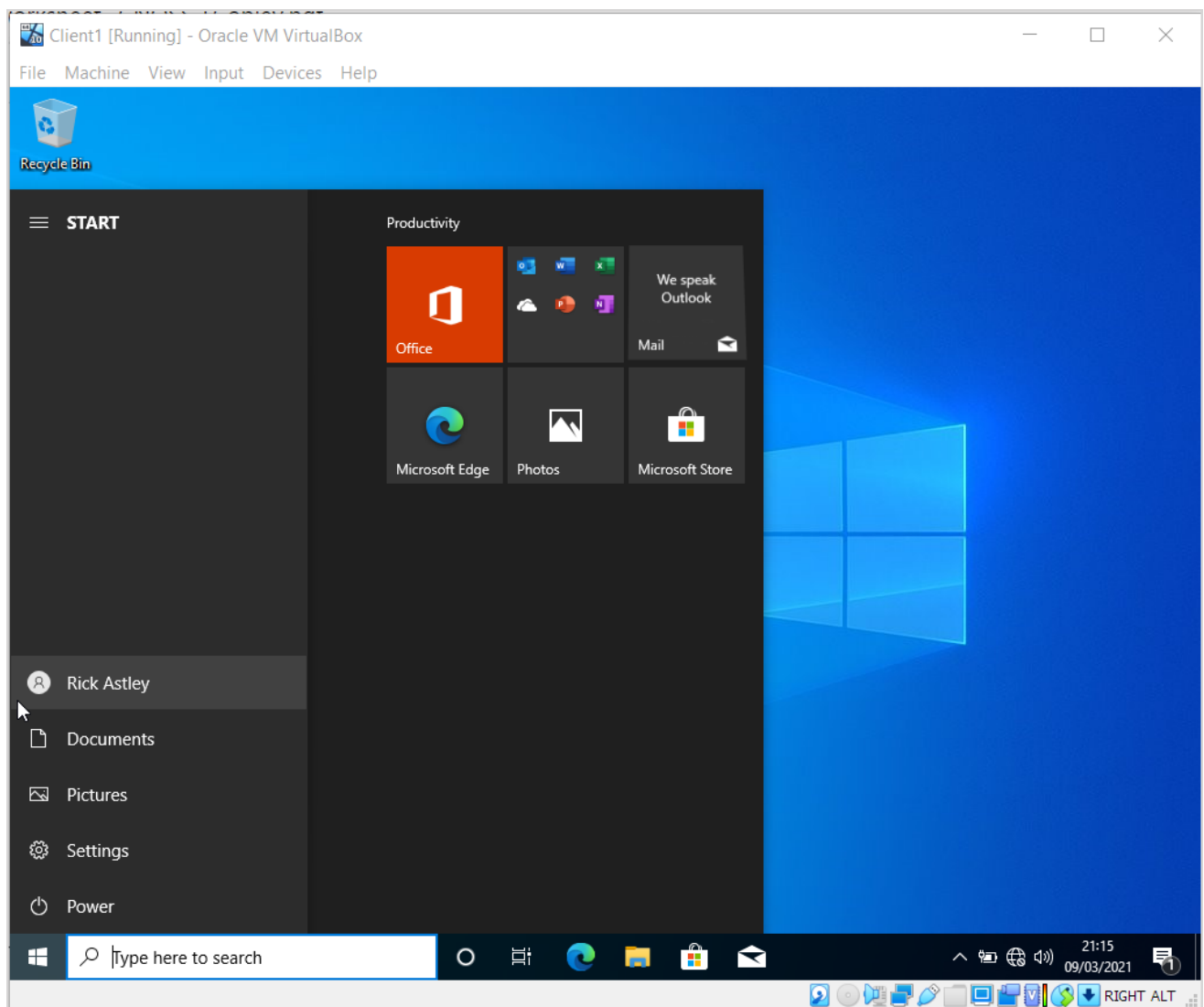


The client was set to connect to the **nwtraders.msft** domain.

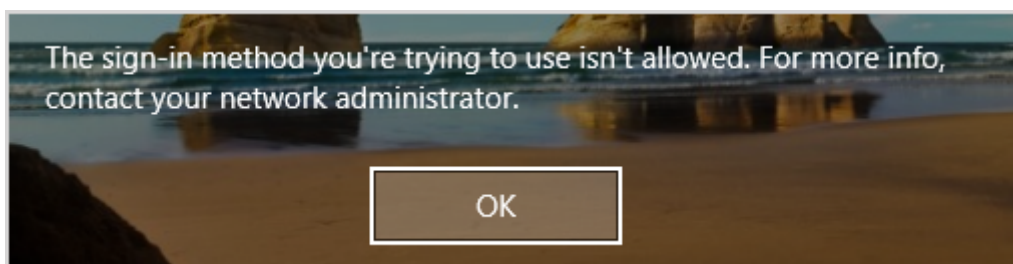
A domain confirmation appeared and the device restarted.

The brief required the author to attempt a log-in to the secondary non-admin account added to the server.

The author signed in as "Rick_Astley".



Rick Astley was connected successfully.



The brief also requested a log-in attempt to the same account from the Server.

An error message appeared, as appropriate.

Task 6: Observational Tasks

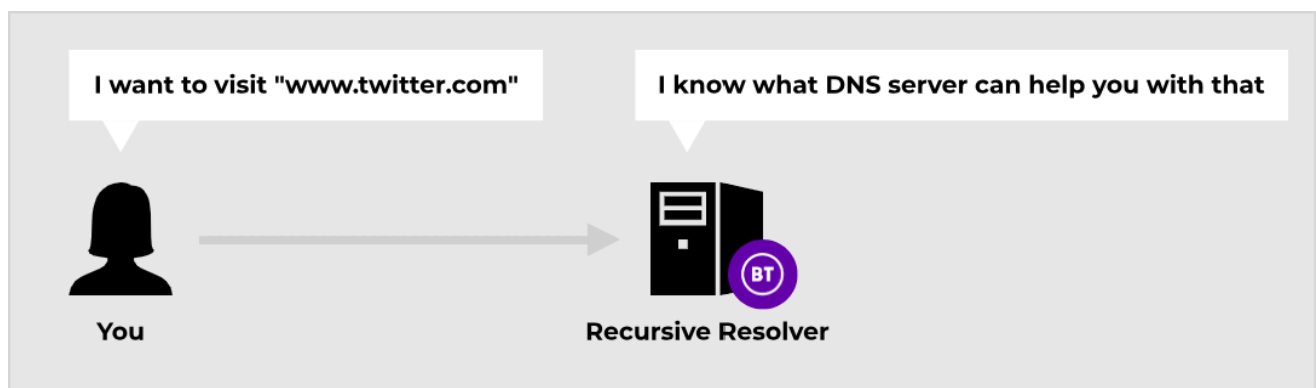
What is DNS?

What is it?

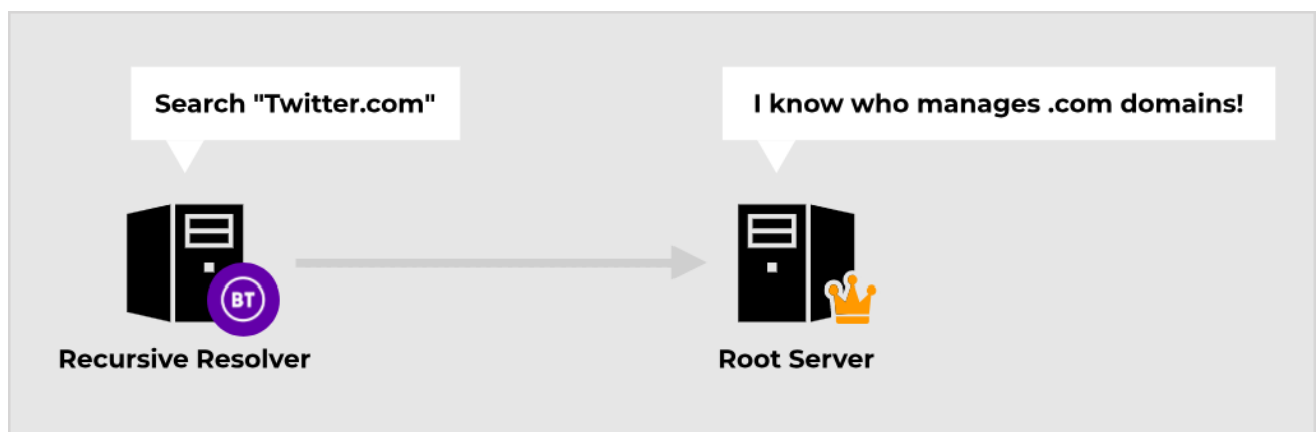
Most end users visit websites via a URL with a domain name (such as example.com). However, most browsers load web pages using the IP address of the server. DNS works much like a phone book but for computer domains, registering a domain to an IP address of a server to make it easier for the end user to access (so they don't have to type in/remember a long number). [1]

How does it work?

When you type a URL into your browser, that request is sent to a server called the **Recursive Resolver** which is usually operated by your internet service provider such as Virgin or BT. This resolver knows what other DNS servers to ask to retrieve the domain name/IP address for the URL you requested.

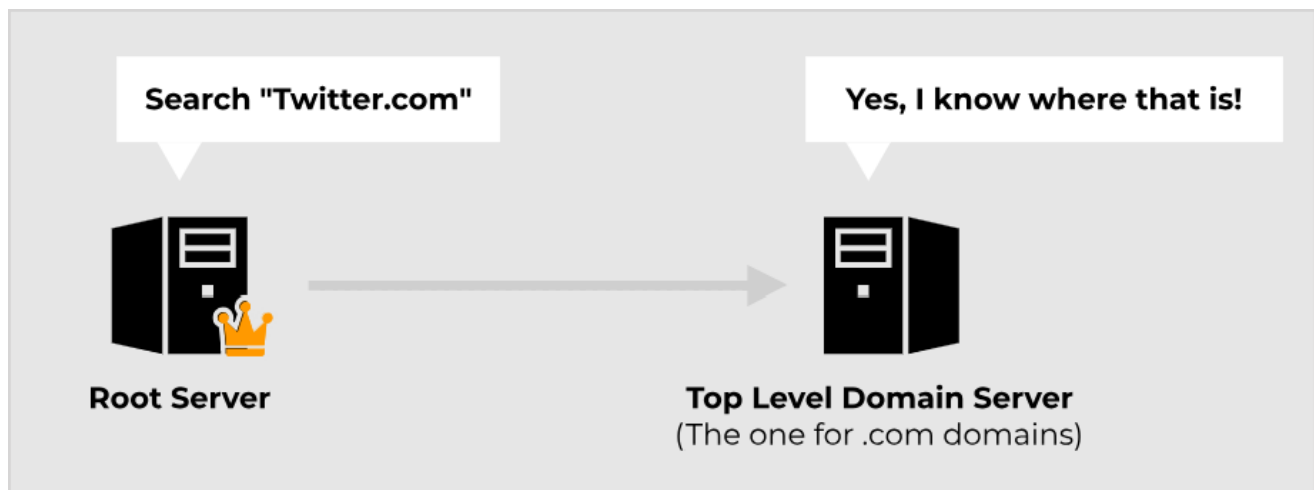


The Recursive Resolver then talks to is the **Root Server**. Root Servers run around the globe and house information about **top level domains** such as .com, .net etc. These Root Servers are usually housed where the most internet activity occurs in a certain region. There are 600 DNS root servers around the world, and these servers are controlled by the National Telecommunications and Information Administration (NTIA) of the US Department of Commerce. [2]

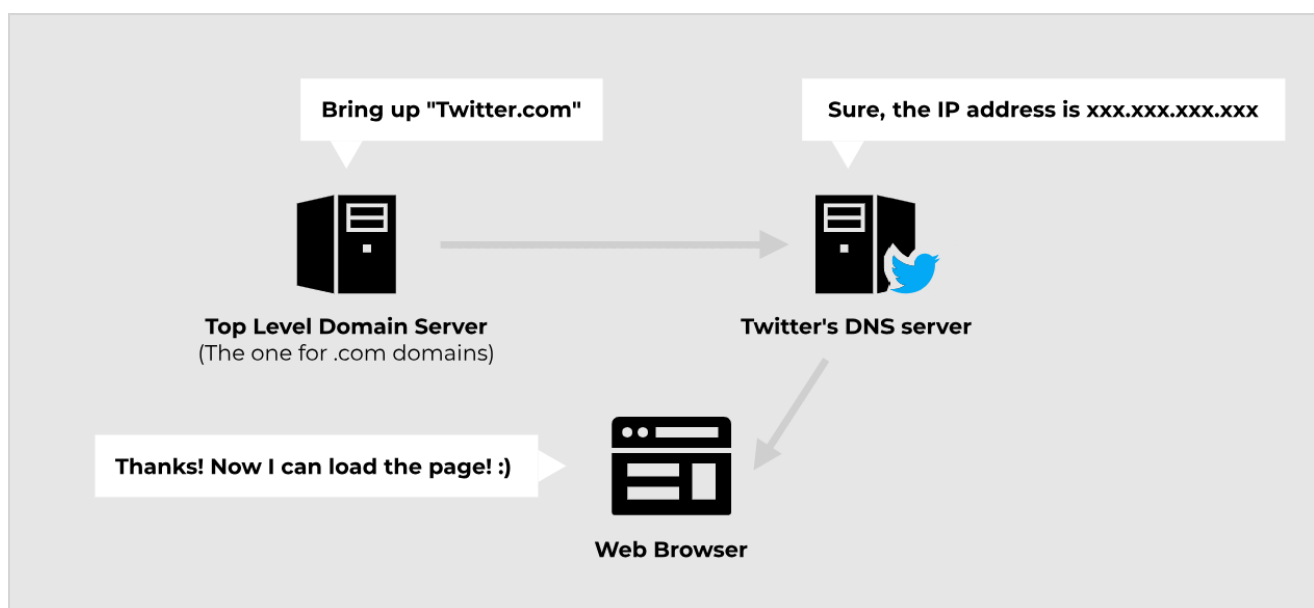


The Recursive Resolver then asks the **Top Level Domain** server to verify the address of the second level domain of the query, for this example, the Top Level Domain of Twitter is ".com". These servers house the address of another server that houses the IP address of the second-level domain (in this case, twitter.com (twitter)). The Top Level Domain server will respond with another address, which will link to the second-level domain and continue the query to load that specific website from that specific domain. Top Level Domains usually have either an **organisational**

hierarchy (such as .com, .edu, .gov, .net.) or **Geographical Hierarchy** (including .co.uk, .co.nz, etc.) [3]



Finally, the The Recursive Resolver sends the query to the domain's name server, which then translates it into an IP address for the web browser to connect to, and deliver the user experience to the user appropriately, and thus, ends the cycle that takes a mere tenth of a second (if that). [4]



And so, the journey is complete.

Other critical roles in an Enterprise Network

Group Policy

Along with active directory, **Group Policy** is vital in an enterprise network as it sets the grounds for policies regarding what various users can and cannot do. Based on a user's membership in the domain, a set of policies will be applied on boot or on sign in using WinLogon. These policies dictate what the user has permission to do, such as whether or not they can install software, access certain files and/or folders or change the desktop wallpaper etc.

Some group policies are vital for ensuring absolute protection to prevent security breaches, for example, it is recommended that prohibiting access to the **control panel** in order to prevent users from changing inappropriate settings for malicious intent or by accident.

Preventing access to other applications like the **command prompt** is also vital for security as policies and settings can be changed using the command prompt.

Setting minimum password lengths for all accounts also ensures that safe, secure passwords are set, and setting a short expiry date. [4]

Firewalls & Security

What is a firewall?

Firewalls are a security method developed to ensure that all established internet traffic follows certain security regulations to filter unsafe or malicious connections establishing a connection with your device. Firewalls usually check packet headers for information such as the address of the packet, where it's been sent from and where it's intended on going, and checks if it matches a security rule set. If it doesn't, the packet gets denied access and destroyed. [5]

Why would a business need one?

Without a firewall, your business is extremely susceptible to a cyber attack, which could lead to private information being exposed, viruses and/or malware destroying important data or breaking computers and servers, damaging the network and lowering company efficiency, productivity and even in some cases harming sales.

"Did you know, 60% of small businesses close within 6 months of a cyber-attack."
Netstar.co.uk

A properly configured firewall that is both maintained and monitored properly can protect important data along with your devices and business network. [6] As of lately, especially due to the affects of covid-19, remote workers and businesses have seen a major increase in cyber attacks in 2020 and 2021, and the average cost of these cyber attacks are expensive, with malware attacks costing businesses \$2.6 million (£1.86 million). These cyber attacks can be greatly reduced with an enterprise enforced firewall (perhaps enforced by group policy), as:

"95% of cybersecurity breaches are caused by human error."
varonis.com

Why it's important to have different levels of access/roles within the 'Built in' Network User Account groups

it's extremely important to have different levels of access or roles within a domain for security reasons. Different levels of access are vital for ensuring that malicious intent by employees isn't executed on a business network, such as changing settings or adjusting/reading/sending restricted corporate files. User access levels also moderate what settings a user can change, and what commands or programs a user can execute, in both the front end and the back end of the system. [8]

Author's opinions on Microsoft's recommendations on AGDLP and ADUDLP

What is it?

AGDLP stands for Accounts, Global groups, Domain Local groups and Permissions and is a network feature that is configured and designed to simplify the process of managing permission and group memberships. With AGDLP you have the advantages of assigning local resource access to user accounts in other domains, you can remove users from a group, and it'll immediately remove their access from a resource and finally, when you create a new user account on the domain, the only thing you'll need to do is add them to an appropriate group, and their permissions will be configured instantly. [9]

What is the author's opinion on it?

ADUDLP as a concept is extremely useful for sysadmins as it cuts out the workload and makes work as a sysadmin much easier, in both a physical sense and a metaphorical sense, as with AGDLP/ADUDLP, the sysadmin can ensure that they aren't delivering the wrong regulations to the wrong user accounts, as the system generally makes the process more mainstream and easier.

Another added advantage of ADUDLP is the security luxury of being able to remove access to resources by simply removing a user from a group, or re-configuring the group policies entirely. As time is an extremely important factor, removing access from those resources within mere hours or even minutes is far safer on your company's resources than having those access rights removed within days or weeks, so the security aspect is a major luxury for sysadmins as well.

References

[1, 4] "What Is DNS? | How DNS Works", *cloudflare*. [Online]. Available: <https://www.cloudflare.com/learning/dns/what-is-dns>. [Accessed: 09- Mar- 2021]

[2] "DNS Root Server", *cloudflare*. [Online]. Available: <https://www.cloudflare.com/learning/dns/glossary/dns-root-server/>. [Accessed: 09- Mar- 2021]

- [3] "DNSMap - Articles - What are Top-Level Domain (TLD) Name Servers?", *Dnsmap.io*. [Online]. Available: [https://dnsmap.io/articles/what-are-top-level-domain-\(tld\)-name-servers](https://dnsmap.io/articles/what-are-top-level-domain-(tld)-name-servers). [Accessed: 09- Mar- 2021]
- [4] D. Murphy, "Top 10 Most Important Group Policy Settings for Preventing Security Breaches - Lepide Blog: A Guide to IT Security, Compliance and IT Operations", *Lepide Blog: A Guide to IT Security, Compliance and IT Operations*, 2021. [Online]. Available: <https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches/>. [Accessed: 09- Mar- 2021]
- [5] "What is a Firewall?", *Forcepoint*, 2021. [Online]. Available: <https://www.forcepoint.com/cyber-edu/firewall>. [Accessed: 09- Mar- 2021]
- [6] "Why do I need a firewall? | Netstar IT Support London", *Netstar IT Support*, 2021. [Online]. Available: <https://www.netstar.co.uk/why-do-i-need-a-firewall-business/>. [Accessed: 09- Mar- 2021]
- [7] "134 Cybersecurity Statistics and Trends for 2021 | Varonis", *Inside Out Security*, 2021. [Online]. Available: <https://www.varonis.com/blog/cybersecurity-statistics/>. [Accessed: 09- Mar- 2021]
- [8] D. Godwin, "Administrator and Different Types of User Accounts: Explained", *Newcmi.com*, 2021. [Online]. Available: <https://www.newcmi.com/blog/administrator-and-different-types-of-user-accounts-explained>. [Accessed: 09- Mar- 2021]
- [9] "AGDLP reduces account management, permissions management headaches", *SearchWindowsServer*, 2021. [Online]. Available: <https://searchwindowsserver.techtarget.com/tip/AGDLP-reduces-account-management-permissions-management-headaches>. [Accessed: 09- Mar- 2021]