MCSA- Microsoft Certified Solutions Associate

Creating and managing a Microsoft environment- Server management

Name: Shker Ameen

College: INT

Course: Cyber Security Analyst

Lecturer: Berkovich Eliran

Date: 01.09.2022

Table of Contents:

Introduction 1

Lab Preparation 3

DC server 10

Domain Controller and Active Directory 10

Creating a domain controller server: 11

Checking a successful AD installation: 17

DHCP (Domain Host Configuration Protocol) 21

DHCP Starvation attack: 25

Prevention: 26

Creating a DHCP server 32

Configuring the DHCP server 33

Connecting WIN10 and SRV1 to ameen.local 39

Routing and PAT setup 41

Creating and Configuring a Router 41

DNS (Domain Name System) 47

Configuring the DNS 53

Sharing and Mapping Features 62

Creating a “Home Folder” for all Users 63

Disable Inheriting Permissions 66

Creating the Shared Folder DATA on DC 73

Mapping a Network Drive 77

Remote Desktop Protocol (RDP) 83

Enabling Remote Access to DC and SRV1 84

Accessing DC and SRV1 from WIN10 using SysAdmin group user3-4 86

Connection **denied** to DC and SRV1- using Sales group user1-2 88

Group Policy Objects (GPO) 90

Creating GPOs on the DC server 92

Introduction

From our perspective, Cyber-security management mitigates the risk exposure of organizations using a range of managerial, legal, technological, process and social controls.

In this project we will discuss the Microsoft environment- Server management, and the local area network, in order to reduce the risk exposure for any organization as stated above.

The LAN presented in this work includes 3 main elements:

1. DC- a Windows server with domain controller- Active Directory, DHCP and DNS services installed on it.
2. SRV1- a Windows server functioning as a router with routing and NAT services.
3. WIN10- a Windows station operating as the client.

We will be starting our work by preparing our Lab and install our DC server, WIN10 and SRV1 on the VMware workstation; get the system updated and turn off all the Firewall's to make the work less complex; However, we will define the names of each devices as we can see in the diagram attached below.

Moreover, we will Check and make sure there is a successful connection between all the devices by using the PING command and ipconfig /all.

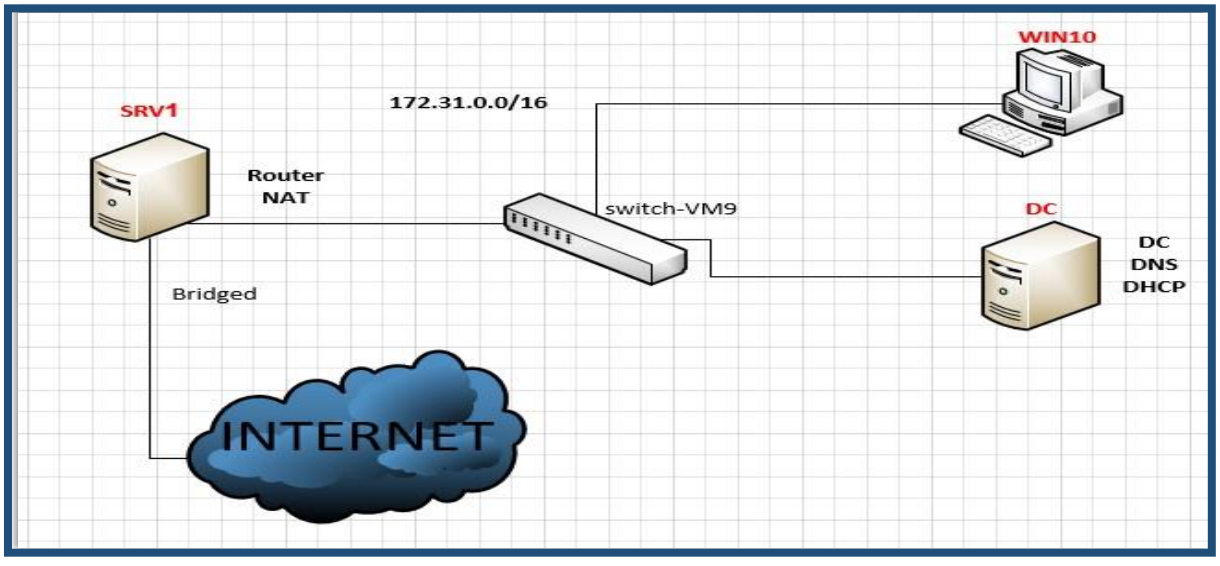
WIN10 will get an automatic assignation of an IP address, later on, which will be set to obtain its IP address automatically as a result of communication with the DHCP servers of DC.

Also we will Check the ability to access the internet in DC and WIN10 due to SRV1's routing services and more.

The following diagram presents the tropology of the network analyzed in this project:

The Switch will not be discussed though it's represented in the diagram to show a reliable depiction of the physical topology of the LAN.

Instead of that; All the devices will be connected to VMnet9 in the VMware Network Connection.



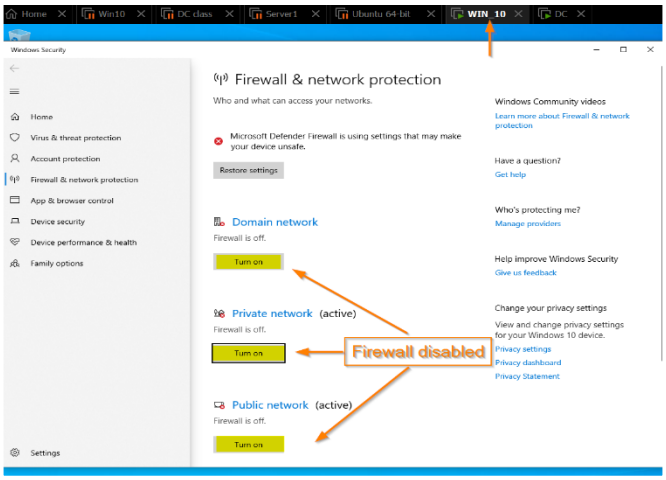
Lab Preparation

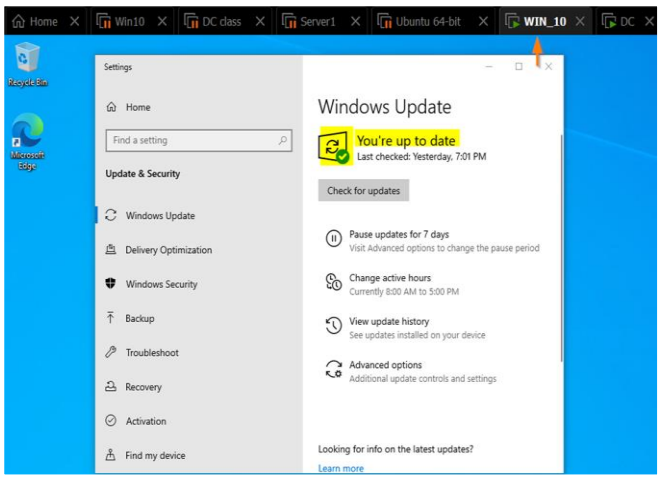
As shown in the diagram above; our IP Address in the LAN network will be based on:

IP Address:	**172.31.0.0**
CIDR Notation:	**/16**
Subnet Mask:	**255.255.0.0**
Binary Subnet Mask:	11111111.11111111.00000000.00000000
IP Class / Type:	**B / Private**
Network Address:	**172.31.0.0**
Broadcast Address:	**172.31.255.255**
Usable Host IP Range:	172.31.0.1 - 172.31.255.254
Total Number of Hosts:	65,536
Number of Usable Hosts:	65,534

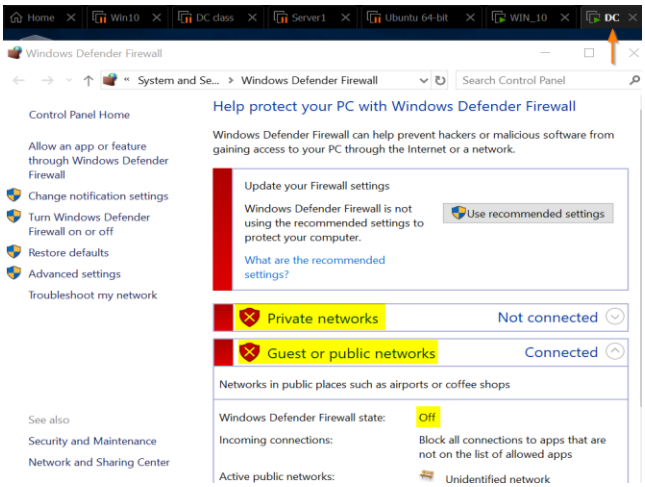
1. Firstly, I will make sure that the Microsoft system are updated and Firewall has been disabled.

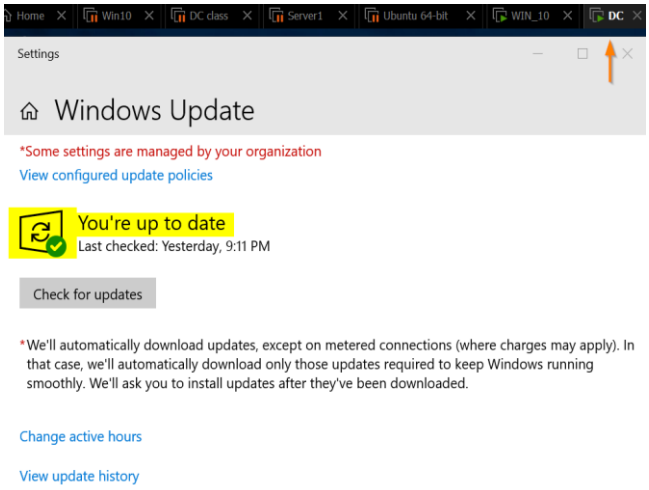
WIN10:





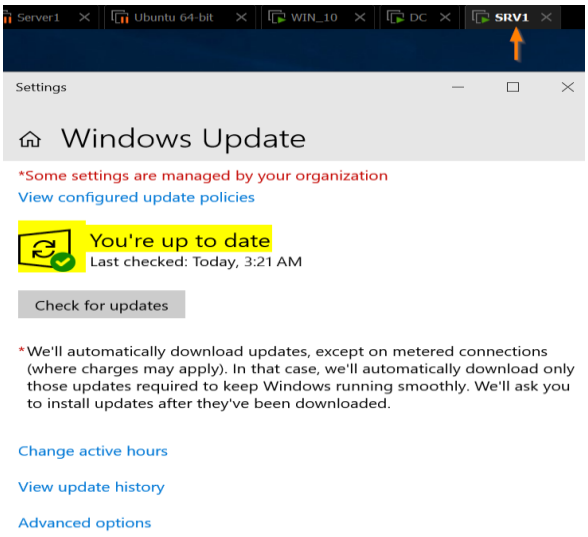
Dc:


Home
Win10
DC class
Server1
Ubuntu 64-bit
WIN_10
DC
Windows Defender Firewall
System and Se... > Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Defender Firewall
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Update your Firewall settings
Windows Defender Firewall is not using the recommended settings to protect your computer.
Use recommended settings
What are the recommended settings?
Private networks
Not connected
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Defender Firewall state:
Off
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active public networks:
Unidentified network
See also
Security and Maintenance
Network and Sharing Center


Home
Win10
DC class
Server1
Ubuntu 64-bit
WIN_10
DC
Settings
Windows Update
*Some settings are managed by your organization
View configured update policies
You're up to date
Last checked: Yesterday, 9:11 PM
Check for updates
*We'll automatically download updates, except on metered connections (where charges may apply). In that case, we'll automatically download only those updates required to keep Windows running smoothly. We'll ask you to install updates after they've been downloaded.
Change active hours
View update history

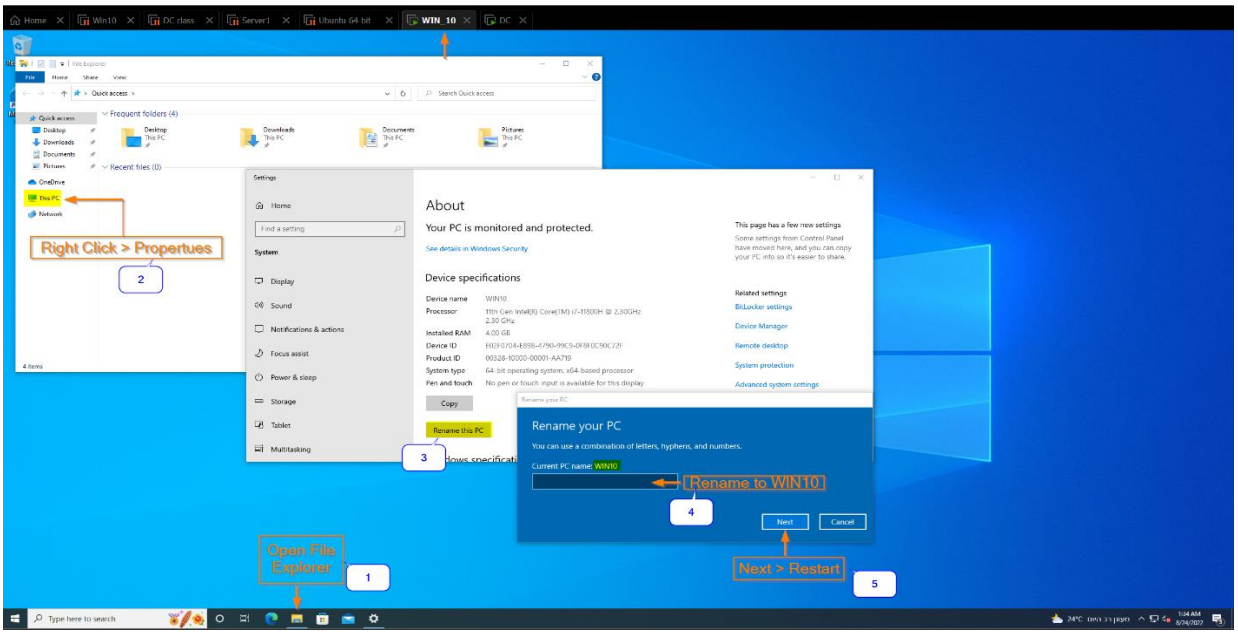
SRV1:


DC class
Server1
Ubuntu 64-bit
WIN_10
DC
SRV1
Windows Defender Firewall
Syste... > Windows Defen...
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Defender Firewall
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Update your Firewall settings
Windows Defender Firewall is not using the recommended settings to protect your computer.
Use recommended set
What are the recommended settings?
Private networks
Not connected
Guest or public net...
Connected
Networks in public places such as airports or coffee shops
Windows Defender Firewall state:
Off
See also
Security and Maintenance
Network and Sharing Center

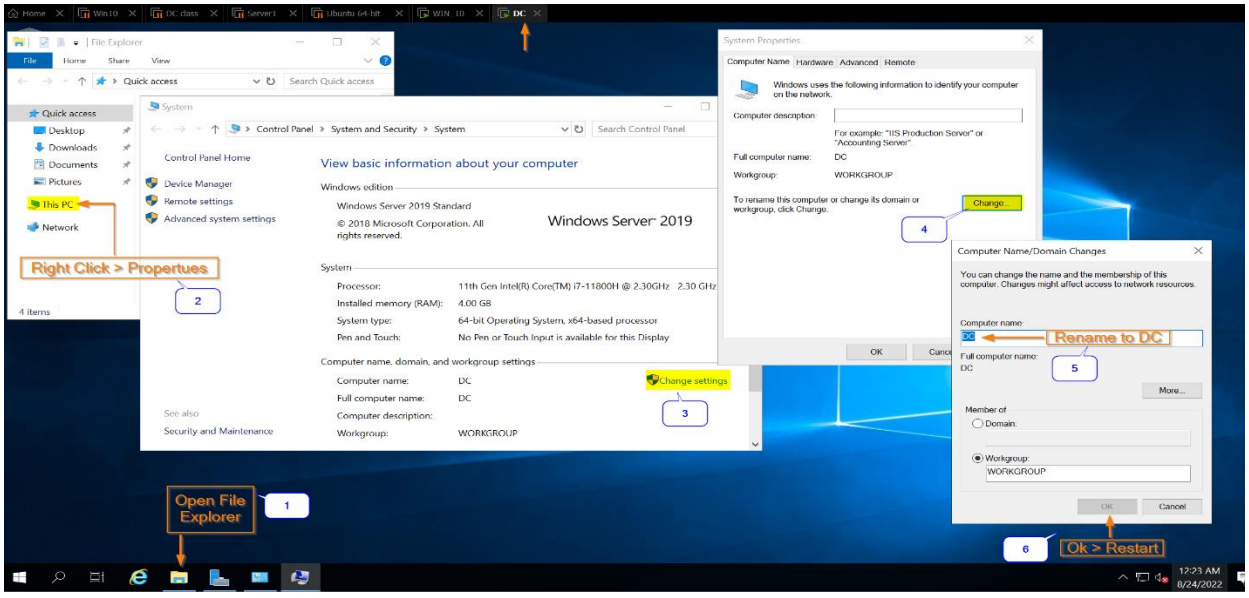

Server1
Ubuntu 64-bit
WIN_10
DC
SRV1
Settings
Windows Update
*Some settings are managed by your organization
View configured update policies
You're up to date
Last checked: Today, 3:21 AM
Check for updates
*We'll automatically download updates, except on metered connections (where charges may apply). In that case, we'll automatically download only those updates required to keep Windows running smoothly. We'll ask you to install updates after they've been downloaded.
Change active hours
View update history
Advanced options

2. Rename all the device's as required:

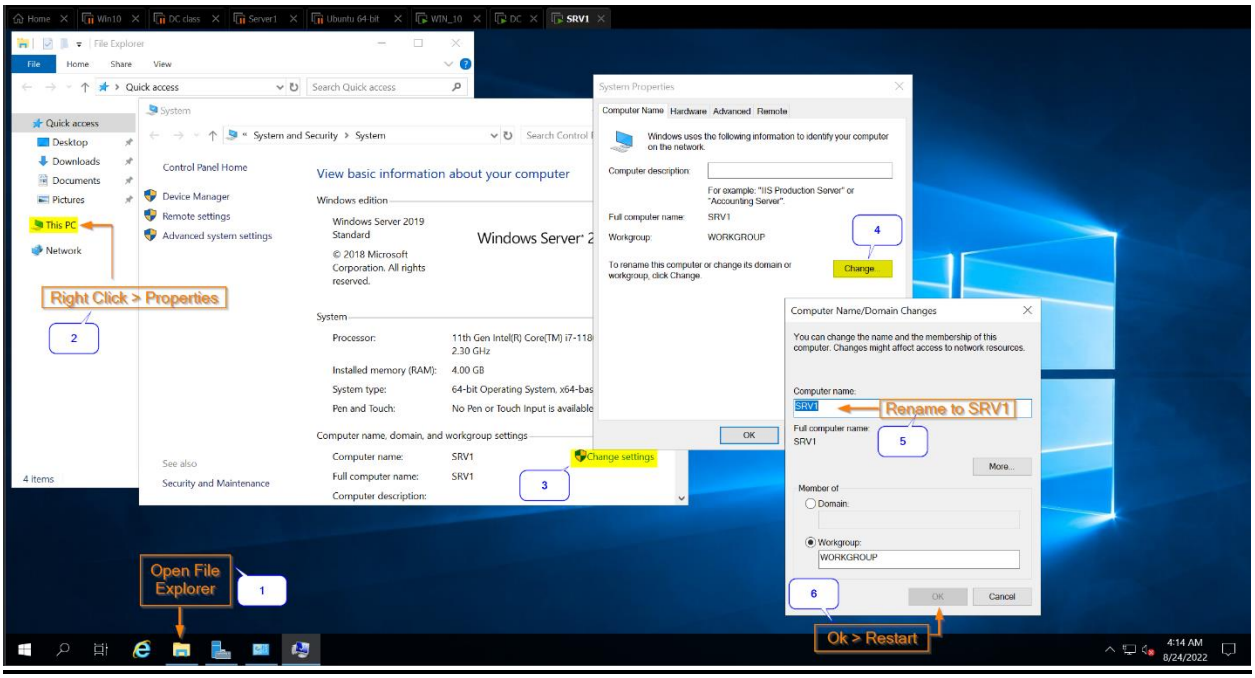
WIN10:



DC:

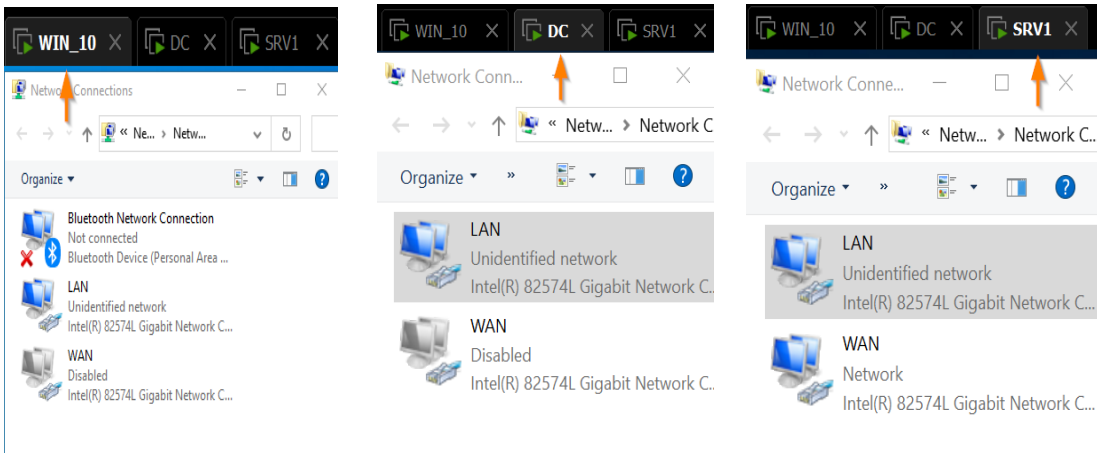


SRV1:



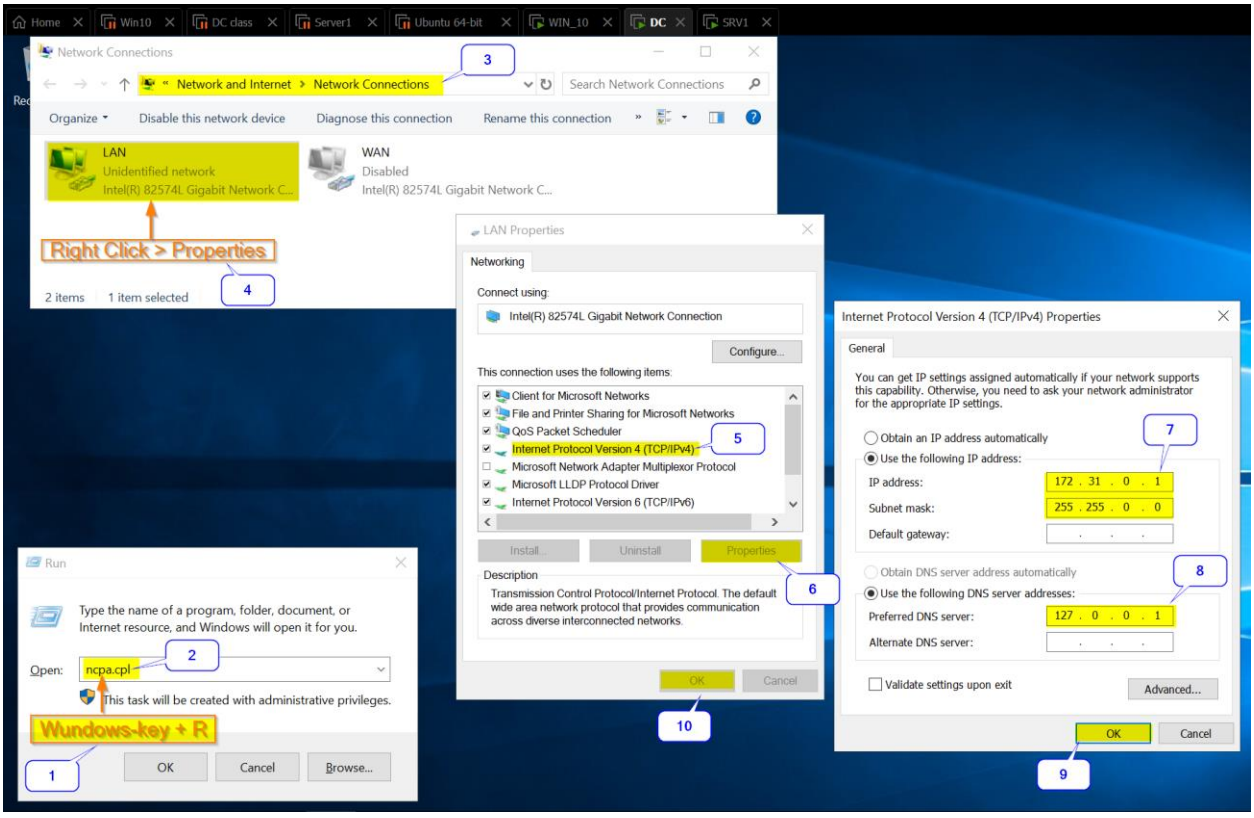
3. I will Also Rename the Ethernet0 and the Ehernet1, in the network connection- on all the devices, accordingly to WAN and LAN.

It must be pointed out that for WIN10 and DC; WAN will be disabled after we finish updating the system.



4. Before we continue the DC server installation, we must make sure to set up DC's LAN to have a fixed IP address before we create the DHCP server on DC afterwards;

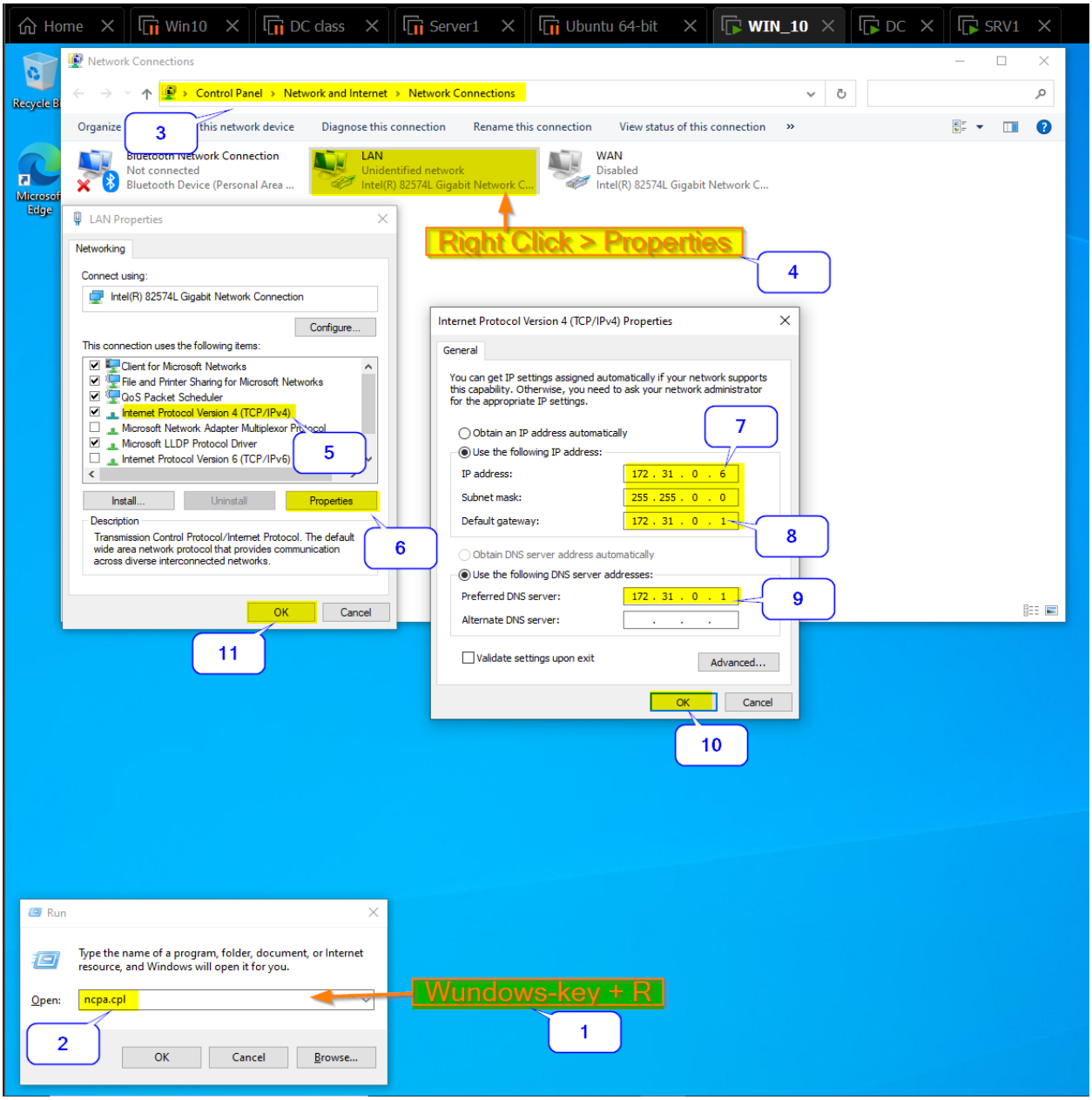
According to the IP address in our Lab; I set DC's IP to 172.31.0.1, the subnet mask to 255.255.0.0 and the preferred DNS server to the loopback address 127.0.0.1 which is DC itself.



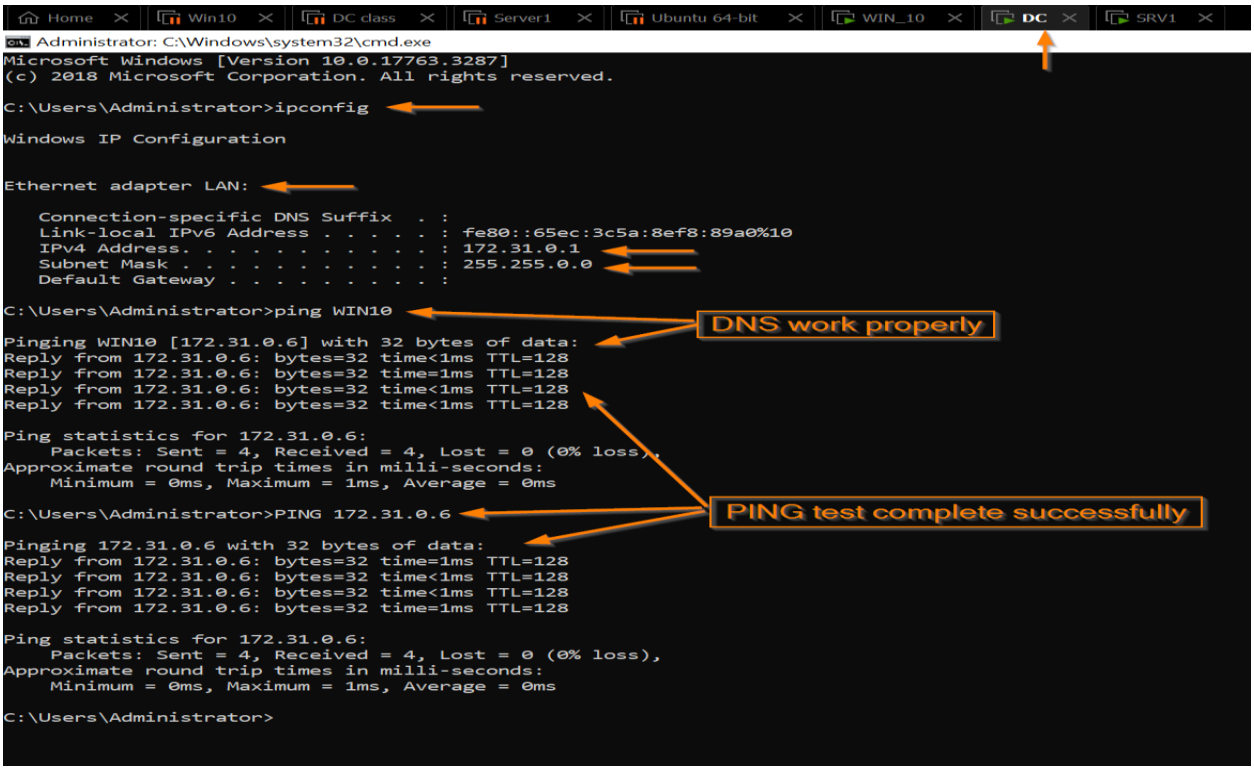
Make notice of: There is no need to set the Default Gateway to the DC, at this point, as already mentioned, there is a Switch-VM9 connection in our physical tropology between the DC and the WIN10 (NIC to NIC communication, Layer 2 protocols).

Furthermore;

I set WIN10's IP to 172.31.0.6, subnet mask to 255.255.0.0, Default gateway and the preferred DNS server to DC's IP to 172.31.0.1.



In addition, Using PING command to test connections and ensure the connectivity between the different end points.



DC server
Domain Controller and Active Directory

A domain controller **(DC)** is a server computer that responds to security authentication requests within a computer network domain. It is a network server that is responsible for allowing host access to domain resources. It authenticates users, stores user account information and enforces security policy for a domain[1].

Active Directory **(AD)** is Microsoft's proprietary directory service. It runs on Windows Server and enables administrators to manage permissions and access to network resources. Active Directory stores data as objects. An object is a single element, such as a user, group, application or device such as a printer[2].

The main service in Active Directory is Domain Services **(AD DS)**, which stores directory information and handles the interaction of the user with the domain. **AD DS** verifies access when a user signs into a device or attempts to connect to a server over a network. **AD DS** controls which users have access to each resource, as well as group policies[3].

[1] https://www.techtarget.com/searchwindowsserver/definition/domain-controller
[2] https://www.techtarget.com/searchwindowsserver/definition/Active-Directory
[3] https://www.techtarget.com/searchwindowsserver/definition/Active-Directory

Creating a domain controller server:

Before starting the installation procedure, make sure that we have completed the necessary steps below[4]:

- Renamed the server as a DC.
- Having a complex password for the Administrator account.

  If the Administrator user account does not have a complex password, then it's not possible to install the Domain Controller service.

  Complex password – at least length `8` and contains three different elements for example: w0rd$$Pa.

  In order to Set a password, pass through:

  Right click on windows icon/start button > Computer management > local Users and Groups > Users > Right click on Administrator > set password > proceed > ok.

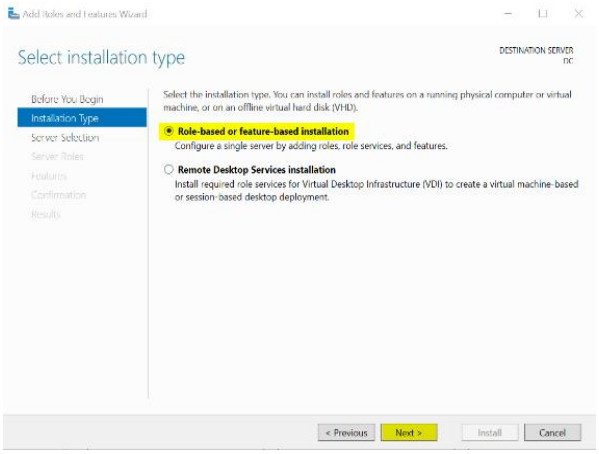
- The server must have a fixed IP address[5].

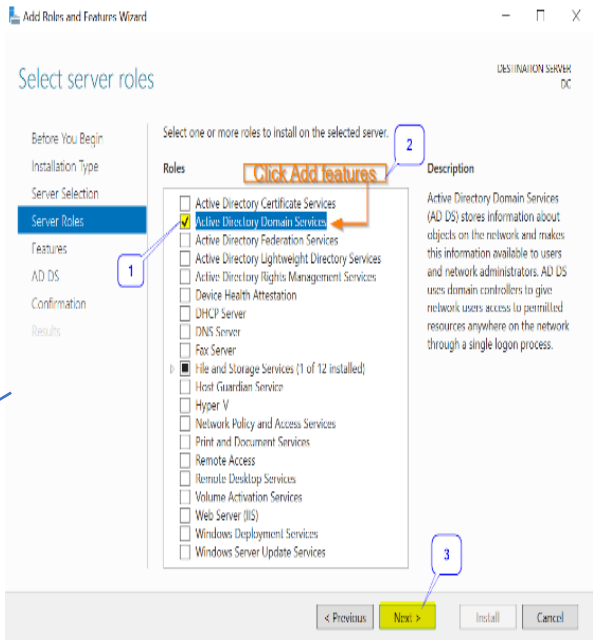
After checking all of the steps above;

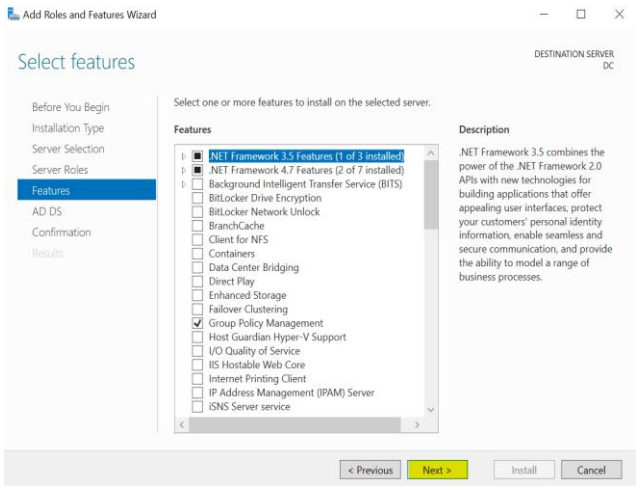
[4] ©Yaki Ben-Nissan
[5] See page 7. the above.

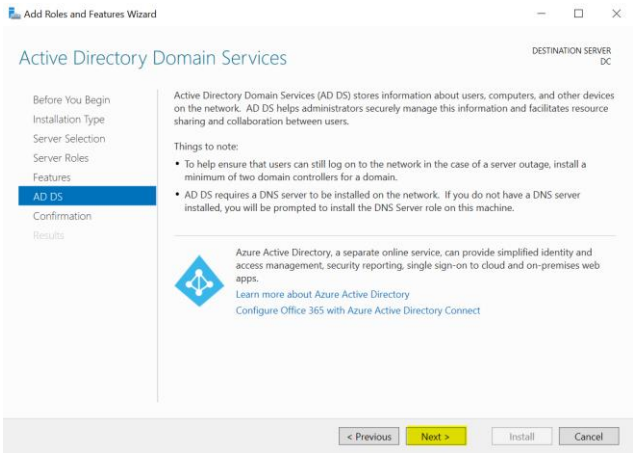
I installed the AD domain services and promoted my server into a DC, through:

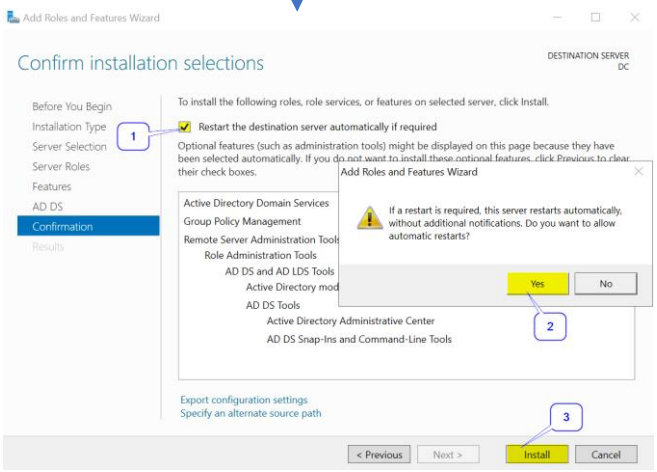
Server Manager > Dashboard > Add Roles and Features > Server Roles > Active Directory Domain Services.

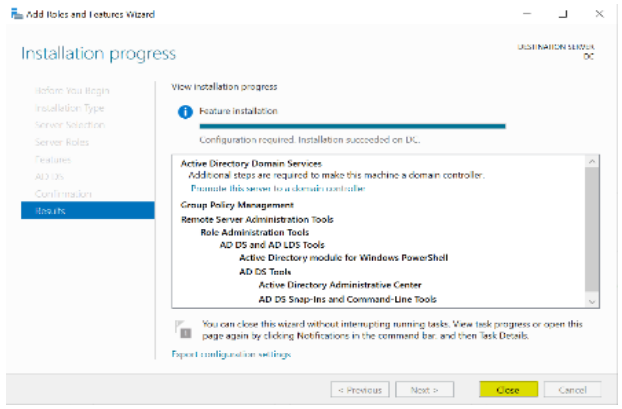


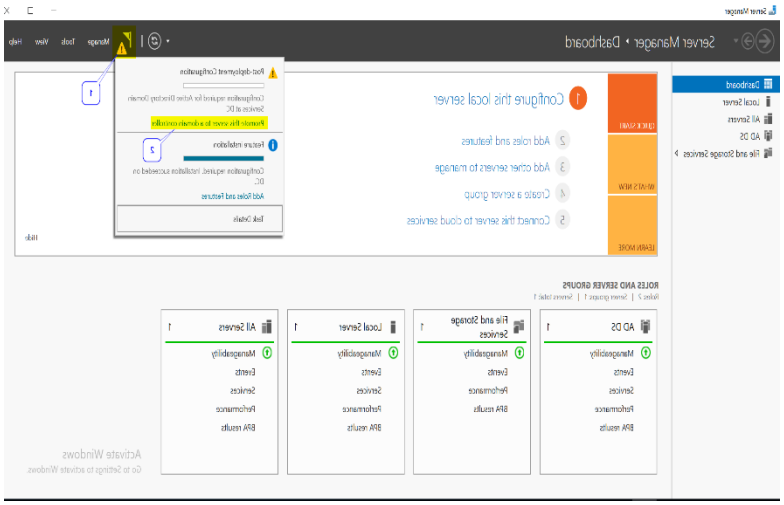


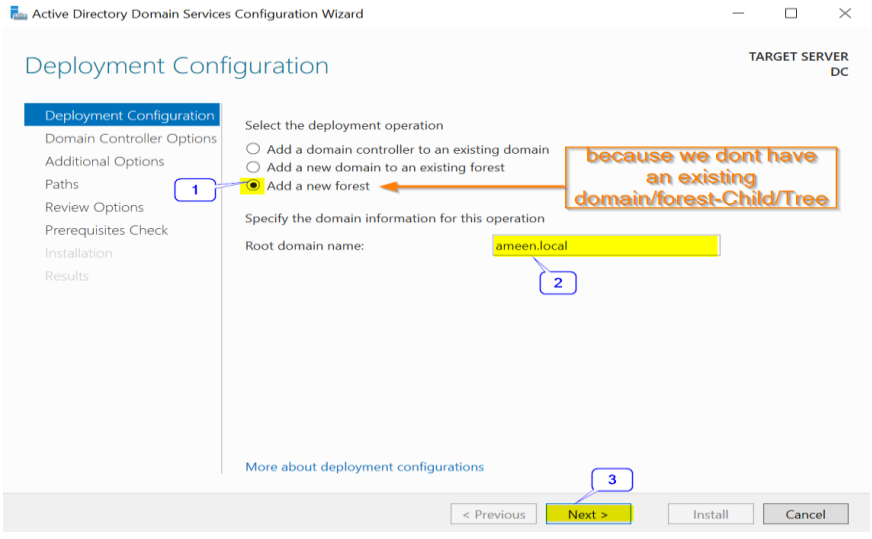


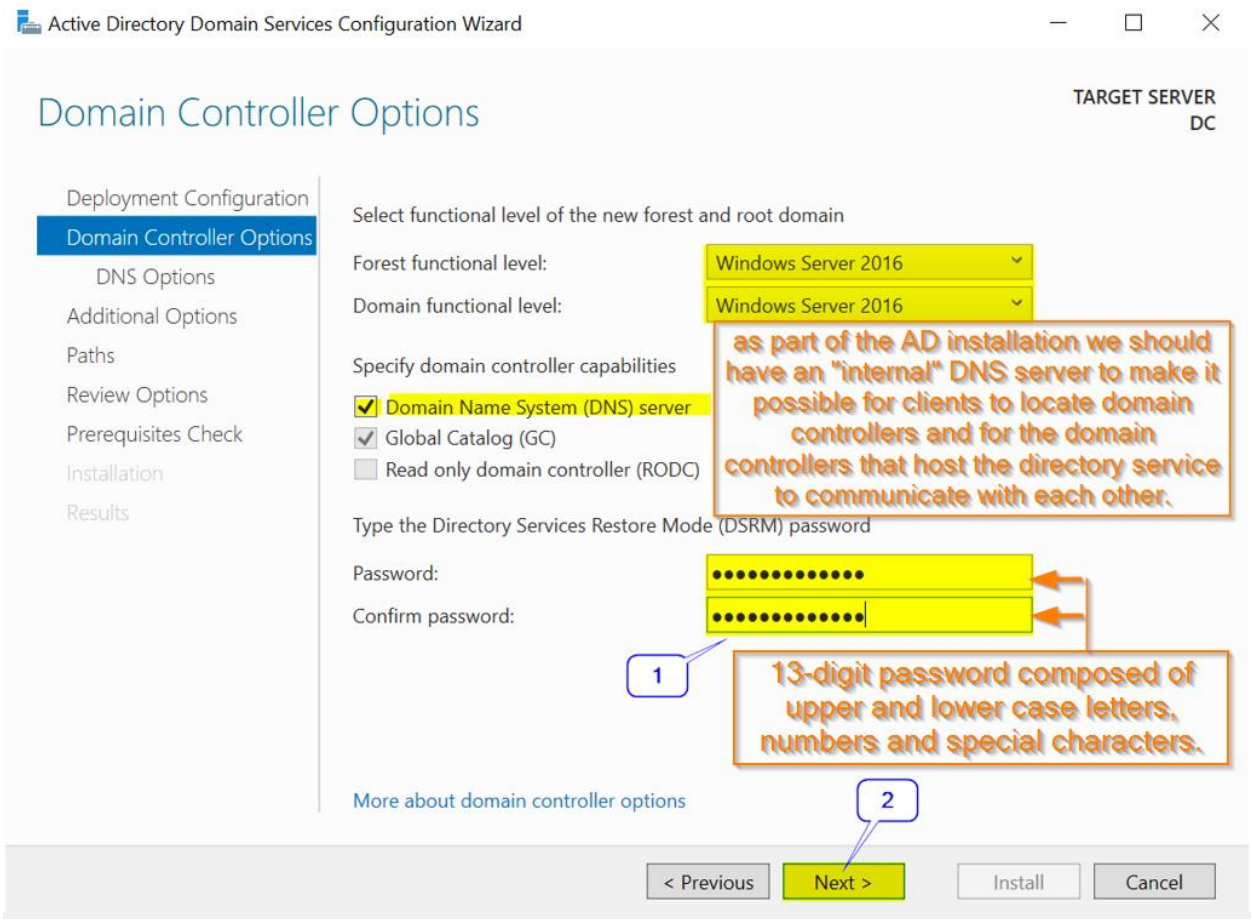


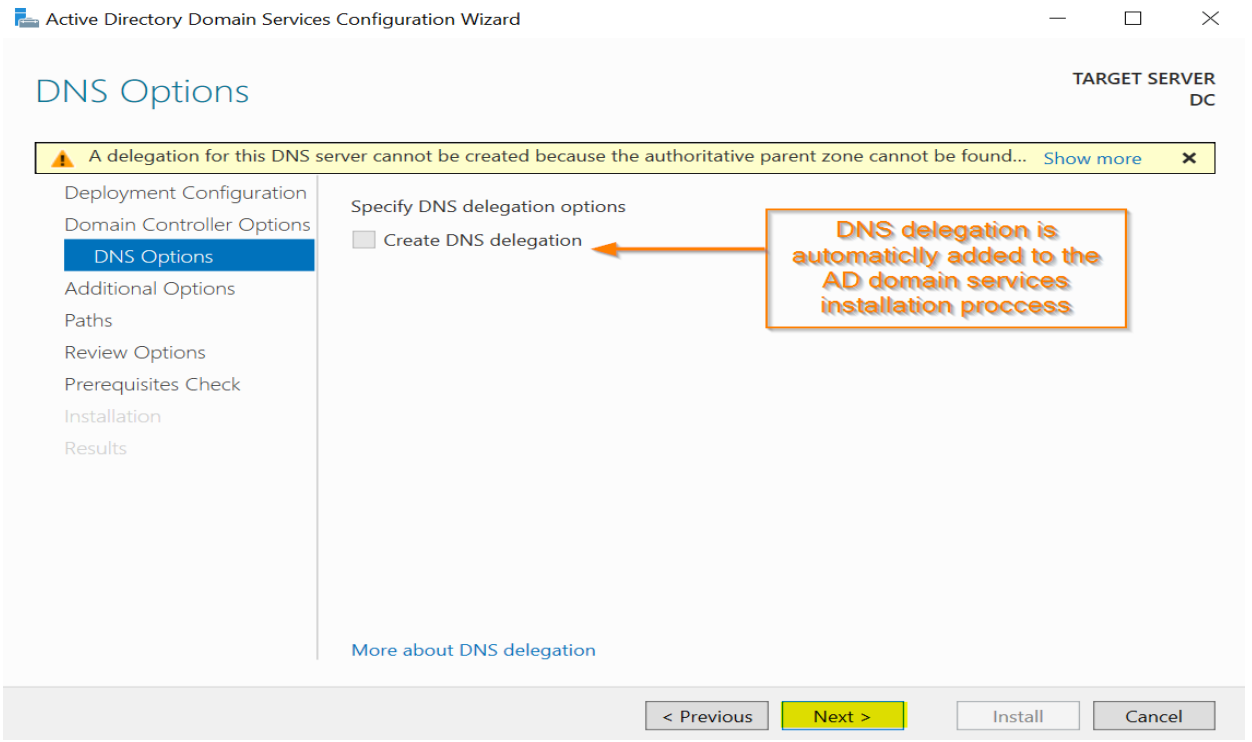

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
DC
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel
1
2
3
Add Roles and Features Wizard
If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?
Yes
No

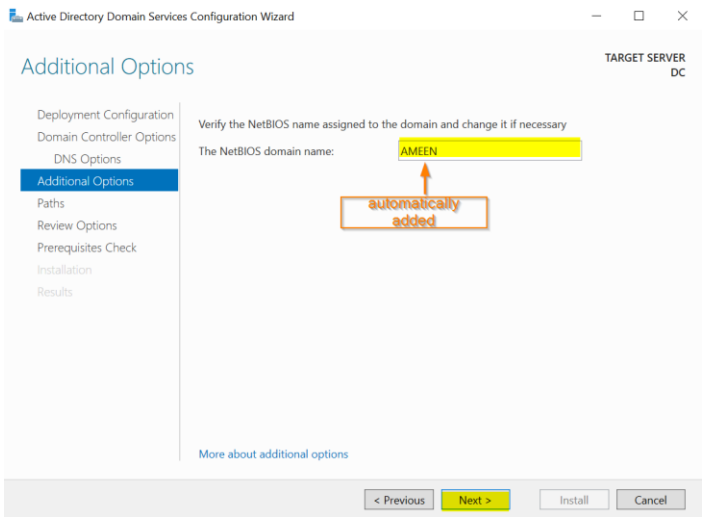

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
DC
View installation progress
Feature installation
Configuration required. Installation succeeded on DC.
Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

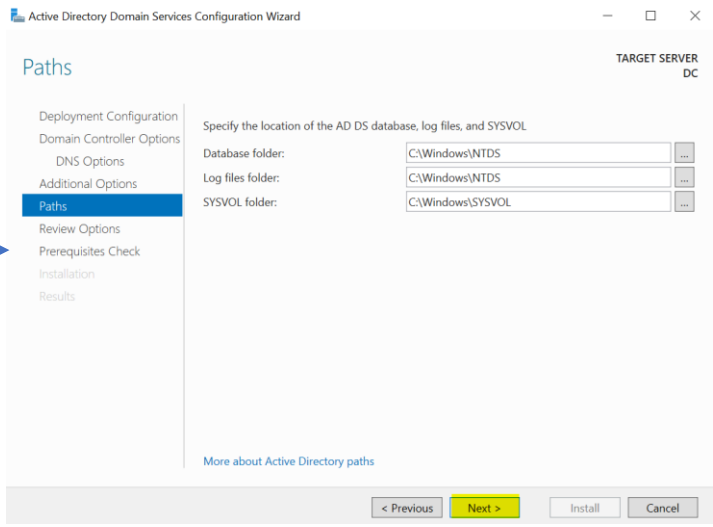

Server Manager
Dashboard
Configure this local server
Add roles and features
Add other servers to manage
Create a server group
Connect this server to cloud services
Dashboard
Local Server
All Servers
AD DS
File and Storage Services
ROLES AND SERVER GROUPS
AD DS
Local Server
All Servers
File and Storage Services
Manageability
Events
Services
Performance
BPA results

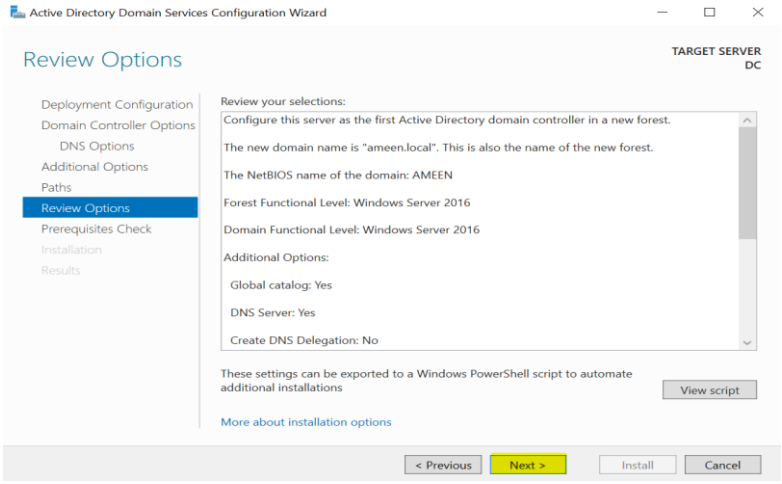

Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
DC
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
because we dont have an existing domain/forest-Child/Tree
Specify the domain information for this operation
Root domain name:
ameen.local
More about deployment configurations
< Previous
Next >
Install
Cancel
1
2
3

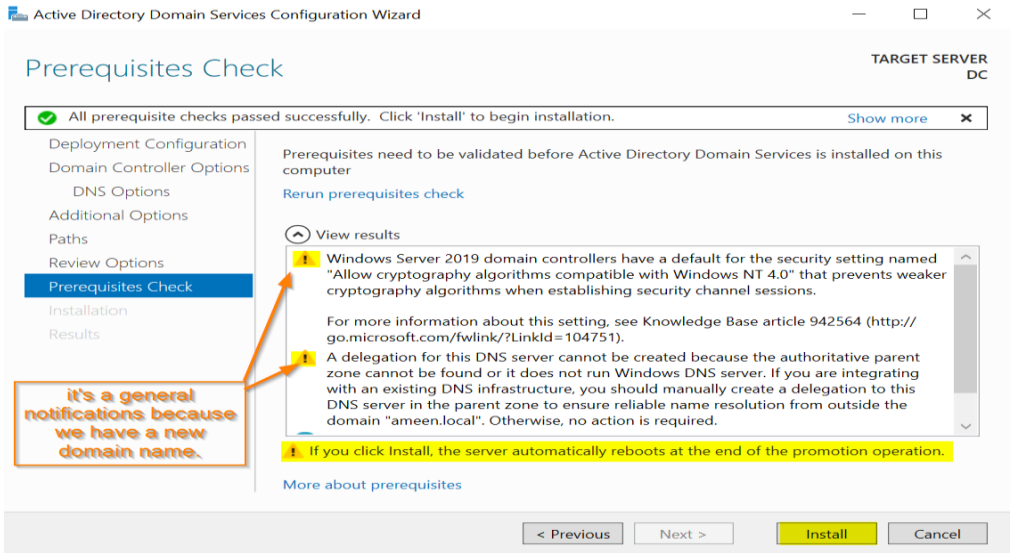

Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
DC
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server 2016
Domain functional level:
Windows Server 2016
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
as part of the AD installation we should have an "internal" DNS server to make it possible for clients to locate domain controllers and for the domain controllers that host the directory service to communicate with each other.
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
1
13-digit password composed of upper and lower case letters, numbers and special characters.
More about domain controller options
2
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
DNS Options
TARGET SERVER
DC
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify DNS delegation options
Create DNS delegation
DNS delegation is automaticlly added to the AD domain services installation proccess
More about DNS delegation
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
DC
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
AMEEN
automatically added
More about additional options
< Previous
Next >
Install
Cancel

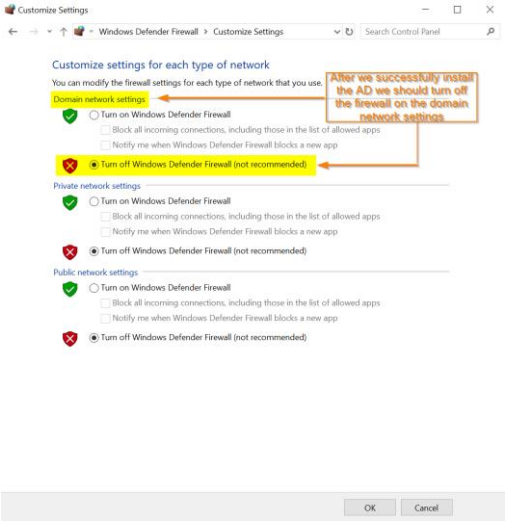

Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
DC
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
More about Active Directory paths
< Previous
Next >
Install
Cancel

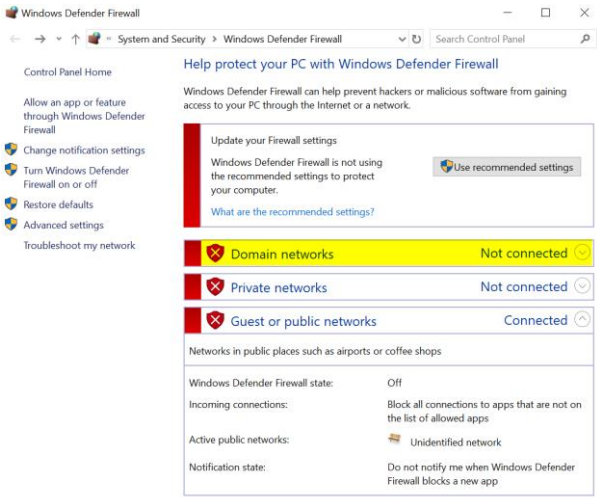

Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
DC
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Configure this server as the first Active Directory domain controller in a new forest.
The new domain name is "ameen.local". This is also the name of the new forest.
The NetBIOS name of the domain: AMEEN
Forest Functional Level: Windows Server 2016
Domain Functional Level: Windows Server 2016
Additional Options:
Global catalog: Yes
DNS Server: Yes
Create DNS Delegation: No
These settings can be exported to a Windows PowerShell script to automate additional installations
View script
More about installation options
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Prerequisites Check
TARGET SERVER
DC
All prerequisite checks passed successfully. Click 'Install' to begin installation.
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
Rerun prerequisites check
View results
Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "ameen.local". Otherwise, no action is required.
it's a general notifications because we have a new domain name.
If you click Install, the server automatically reboots at the end of the promotion operation.
More about prerequisites
< Previous
Next >
Install
Cancel

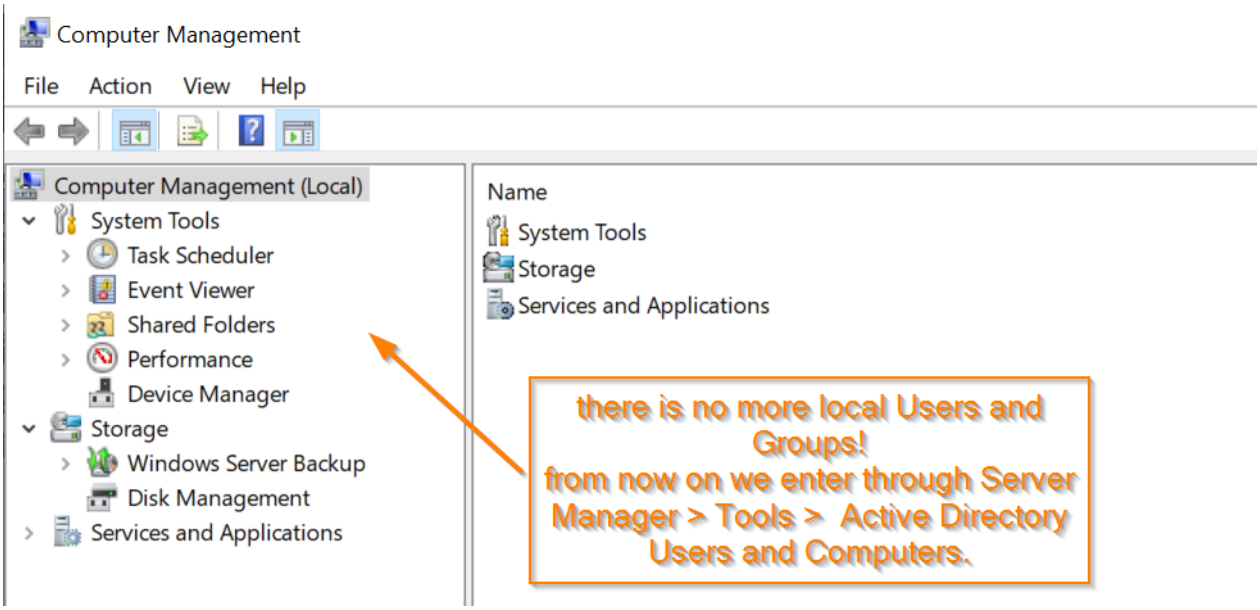
Once the installation is complete, there is two noticeable changes:

1. Turn off the Domain network settings.



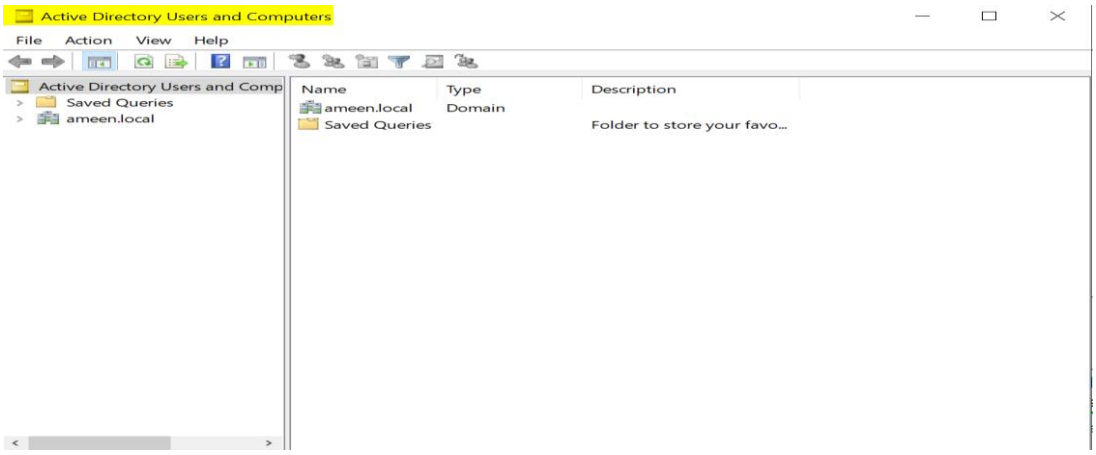


2. There is No more local Users and Groups.

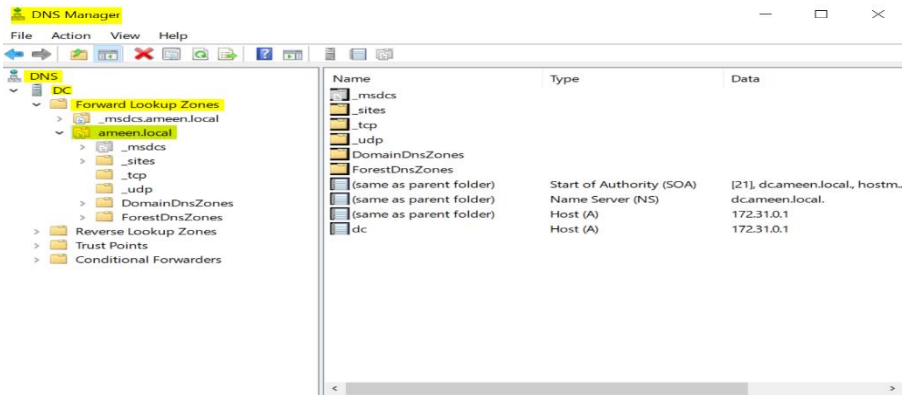


Checking a successful AD installation:

1. Successfully logging through:
   Server Manager > Dashboard > Tools > Active Directory Users and Computers.

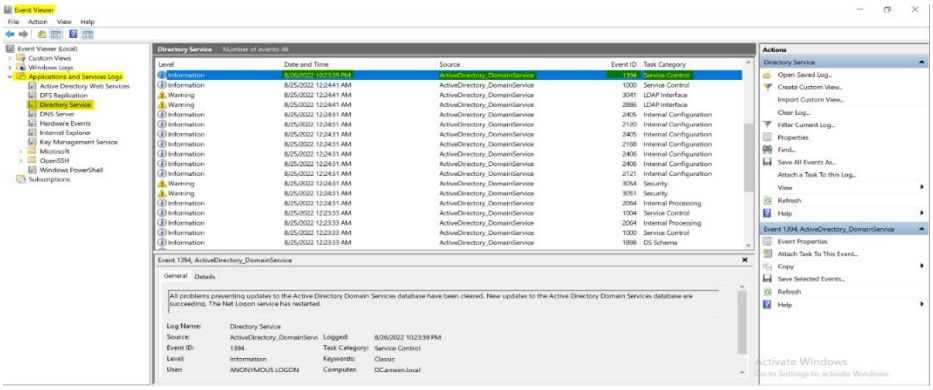


2. Successfully DNS installation, through:
   Server Manager > Dashboard > Tools > DNS > DNS Manager



3. Checking a successful Event Viewer, through:

Server Manager > Dashboard > Tools > Event Viewer.



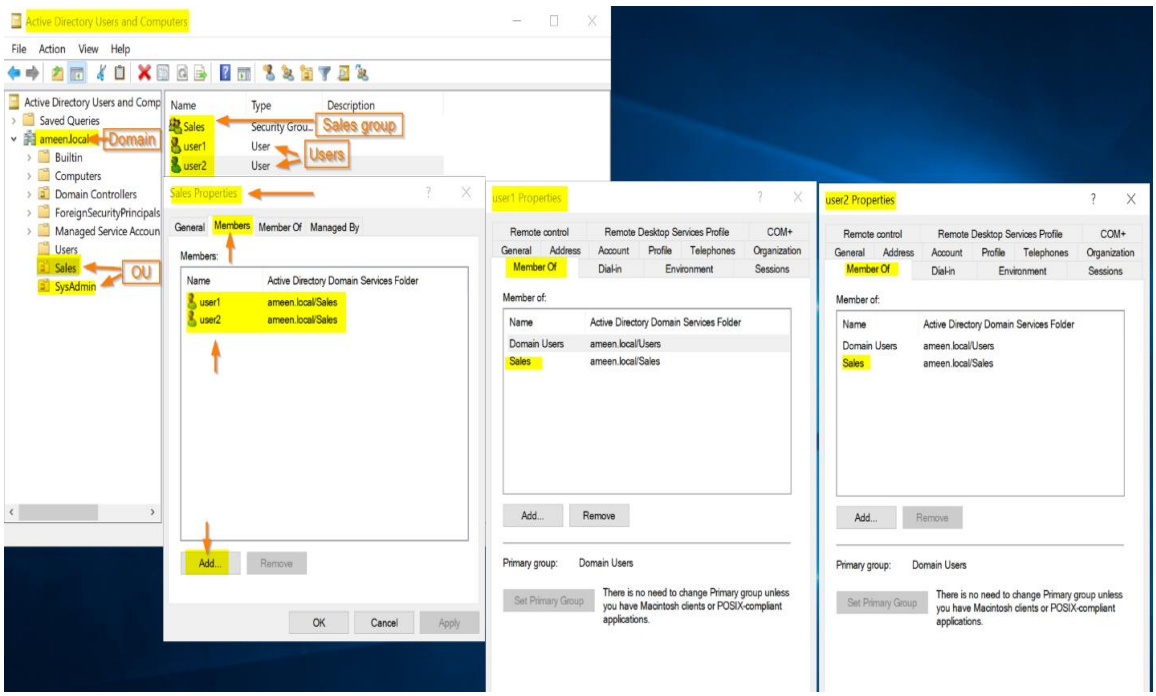
Following further steps; I entered the Active Directory Users and Computers panel, through:

Server Manager > Dashboard > Tools > Active Directory Users and Computers.

- In the AD, I created two new organizational units (OU) and named them Sales and SysAdmin.

- Then I created the user1 and user2 (that representing sales department employees in the organization) in the Sales OU.

- Built a new group called “Sales” and added user1 and user2 on it by using the “members” tab of the group’s properties.

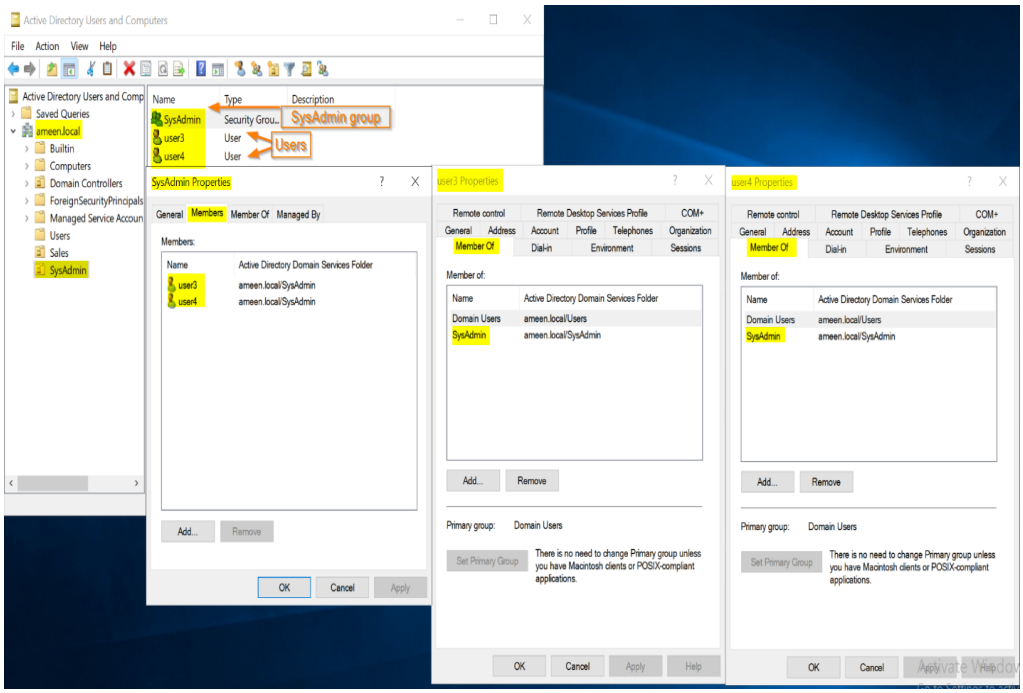


As well as;

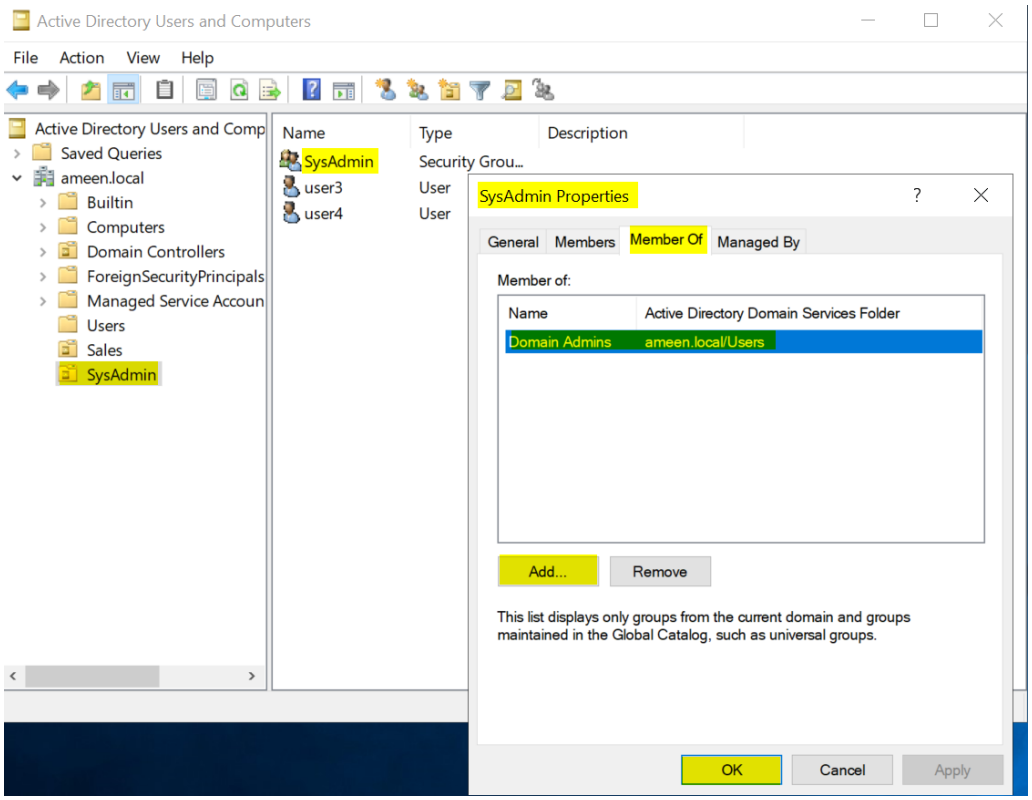
- I created the user3 and user4 (that representing SysAdmin department employees in the organization) in the SysAdmin OU.

- Built a new group called “SysAdmin” and added user3 and user4 on it by using the same method.

- Added the “SysAdmin” group into the “Domain Admins” group using the “member of” tab of the group’s properties.



Lastly, I added the "SysAdmins" group into the "Domain Admins" group using the "Member of" Tab of the group's properties.



DHCP (Domain Host Configuration Protocol)

A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients[6].

A DHCP server automatically sends the required network parameters for clients to properly communicate on the network. Without it, the network administrator has to manually set up every client that joins the network, which can be cumbersome, especially in large networks. DHCP servers usually assign each client with a unique dynamic IP address, which changes when the client's lease for that IP address has expired[7].

The process of obtaining an IP address is composed of 4 steps and is called the DORA process:

1. Discover – the host sends a discover packet in order to discover a DHCP server using broadcast transmission.

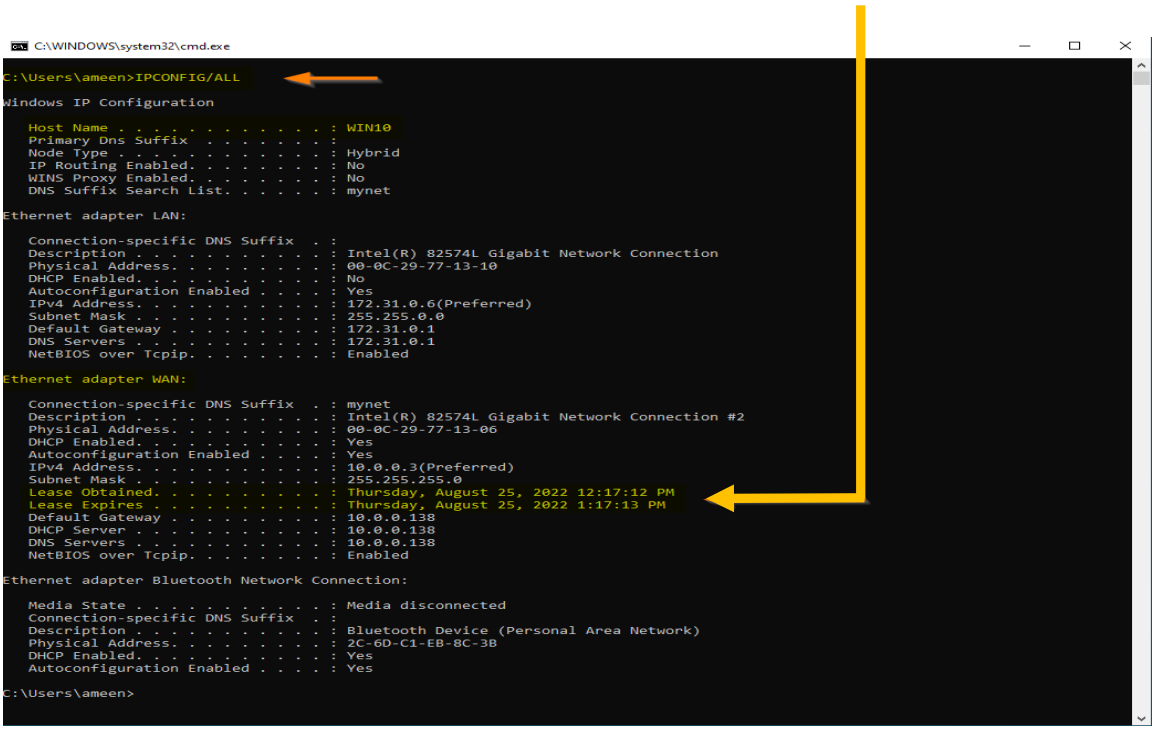
[6] https://www.infoblox.com/glossary/dhcp-server/
[7] See note NO. 6, the above.

2. Offer – all of the DHCP servers that received the discover packet, send the host an offer packet that contains the IP address offered for the host.

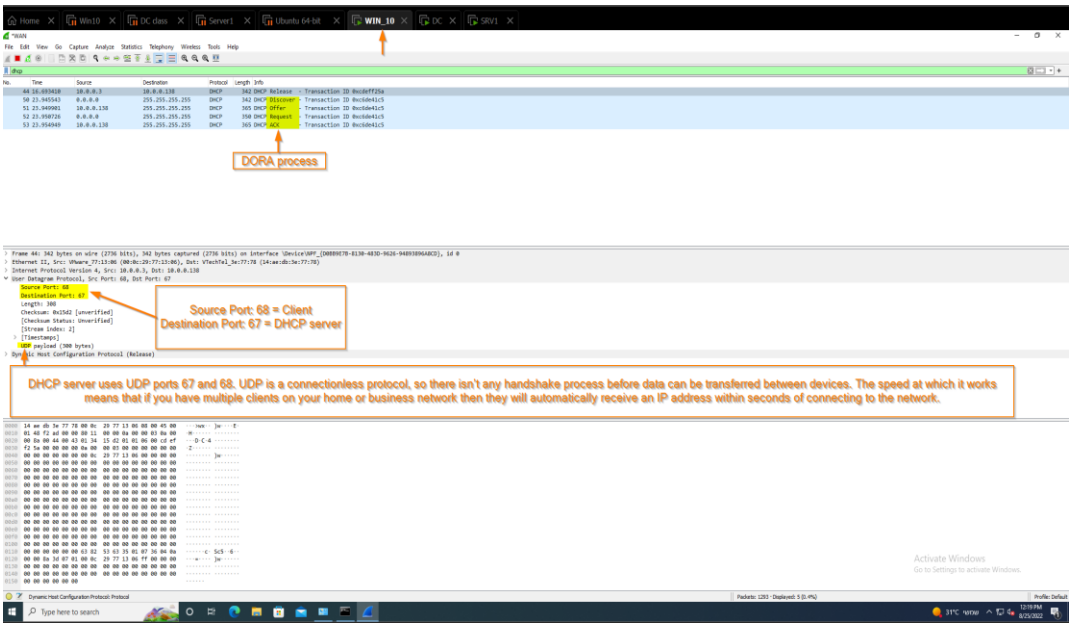
3. Request – the host will receive the IP address offered by the first DHCP server that replied to the discover packet and sends a broadcast message containing the MAC address of the server to approve the offer. This way the other DHCP servers are also notified that the communication with the host will not be continued.

4. Acknowledgement – the DHCP server that assigned the IP address that the host takes upon itself sends an acknowledgement package using unicast transmission to the host, approves the assignment of the IP address and specifies that lease time for it.

However, Every IP address assigned to a host has a specific lease time defined for the address. As we see in the screenshots below, for an example, I have a lease time for only **one hour- 60 min**.



During the **DORA** process Screenshot in Wireshark:



After 50% of the lease time which it is **30 min**. the network device will try to renew the lease from the same DHCP server for an extra hour...

and after 87.5% of the lease = 52.5 min, if no reply was received; the network device- host, will send a "discover" packet and start looking for a new server.

After 100% = 60 min / 1 hour, if no reply was received by the host, or the DHCP server wasn't available it will generate an APIPA- Automatic Private IP Address (169.254.x.x/16).

DHCP Starvation attack:

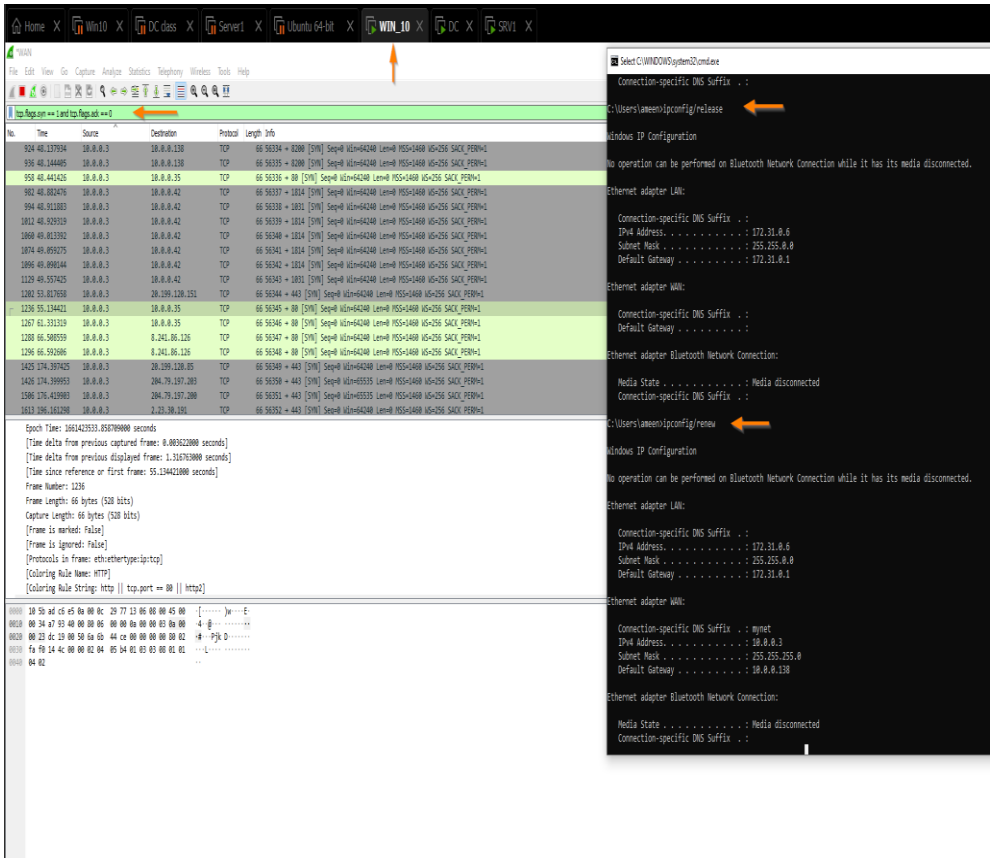
As mentioned before, a DHCP server has a limited range of IP addresses it can allocate. A DHCP starvation attack is when a threat actor sends a massive amount of fake DISCOVER packets with spoofed MAC addresses as the source, overwhelming the DHCP server. The DHCP server responds to each of these fake DISCOVER packets until it runs out of IP addresses to allocate. This denies any valid clients from obtaining an IP address, which in turn denies them service. This is commonly known as a denial of service (DoS) attack. This may cause clients on the network to look for an alternative DHCP server. While this would be an attack on its own, this is commonly followed up by the threat actor providing their own malicious DHCP server to issue IP addresses. In addition to IP addresses, the threat actor would be able to issue default DNS and gateway information. Now, clients who use those IP addresses as well as the gateway can be routed through the threat actor's machine, allowing them to read all of the traffic that the client sends and receives. This is what is known as a man-in-the-middle (MITM) attack. These attacks can cause a great amount of damage. Because of that, it is important to be able to detect when they are occurring[8].

In this case, Wireshark is a great tool to use for detecting DHCP starvation attacks, more specifically DoS attacks and MITM attacks.

Wireshark can be filtered for SYN packets without an acknowledgement using the filter: **"tcp.flags.syn == 1 and tcp.flags.ack == 0"**.

[8] https://ritcsec.wordpress.com/2022/05/06/understanding-and-preventing-dhcp-starvation-attacks/

The result should look similar to this.



Prevention:

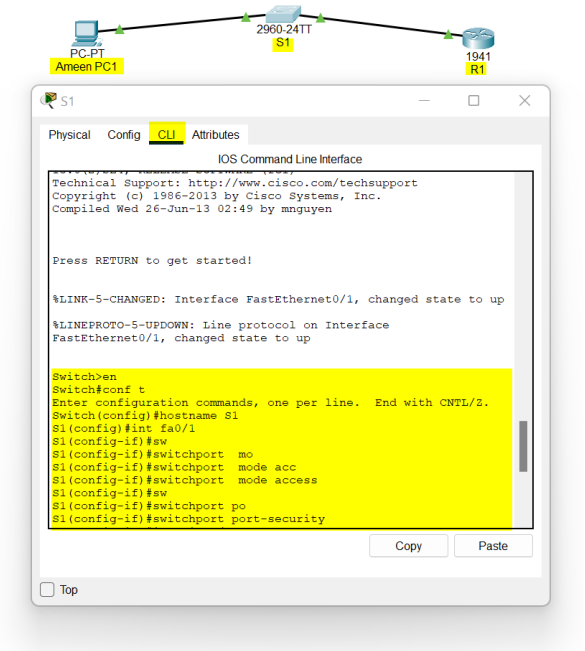
1. One way to prevent a DHCP starvation attack on a network is through port security. Port security is a layer 2 traffic control feature on switches. Switches learn MAC addresses when a frame is forwarded through a switch. By using port security, a limit of the number of source MAC addresses that a port can allow can be set. Penalties can be set for ports as well if an unauthorized user is using the port. The commands restrict, shut down, and port-security can be used to enforce these penalties.

Port security can be configured on a switch through the following steps:

- Use the "config t" command to enter global configuration mode
- Access the interface that you want port security to be enables on using the command "int {interface}"
- Use "switchport mode access" to convert the port to an access port

  For port security to work, the port must be an access port because port security only works on access ports.

- Finally, use the command "switchport port-security" to enable port security[9].



2. A Second way to prevent a DHCP starvation attack on the network, is through Enable and Configure DHCP MAC Address Filtering.

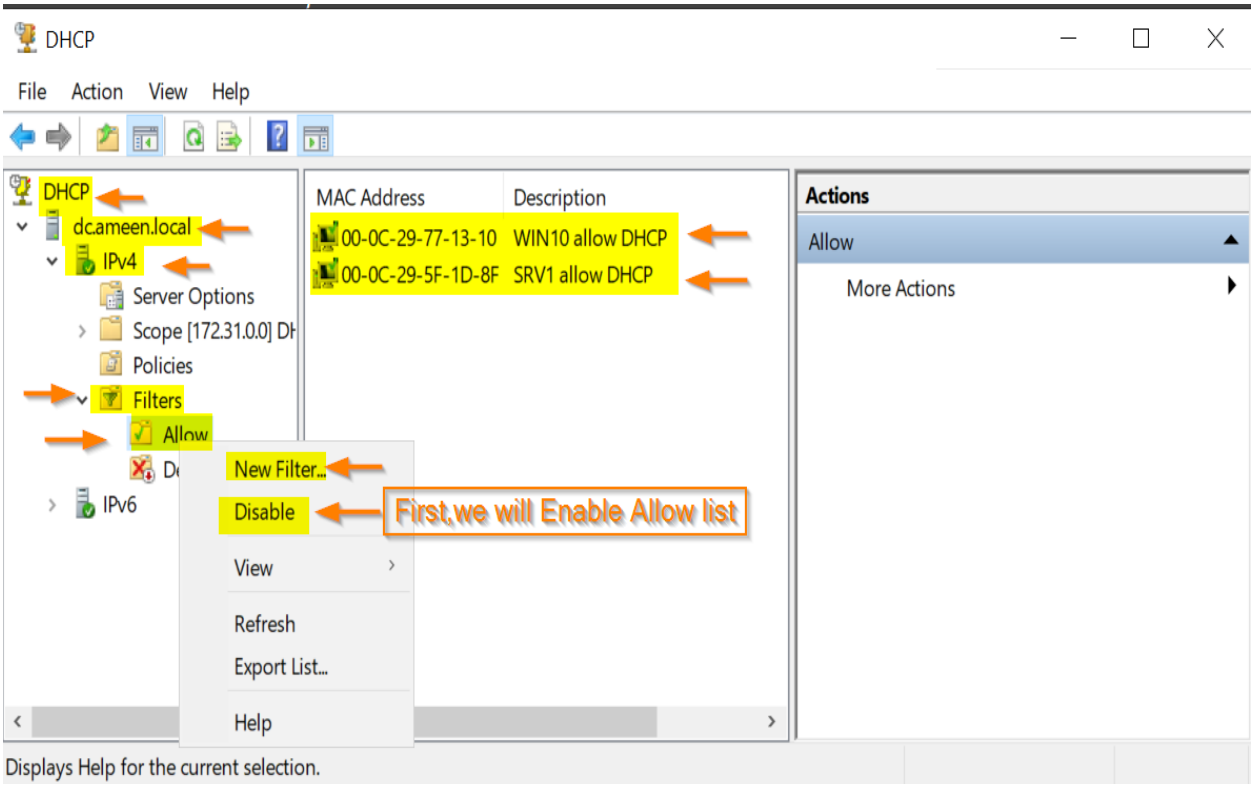
[9] See note number 6 above.

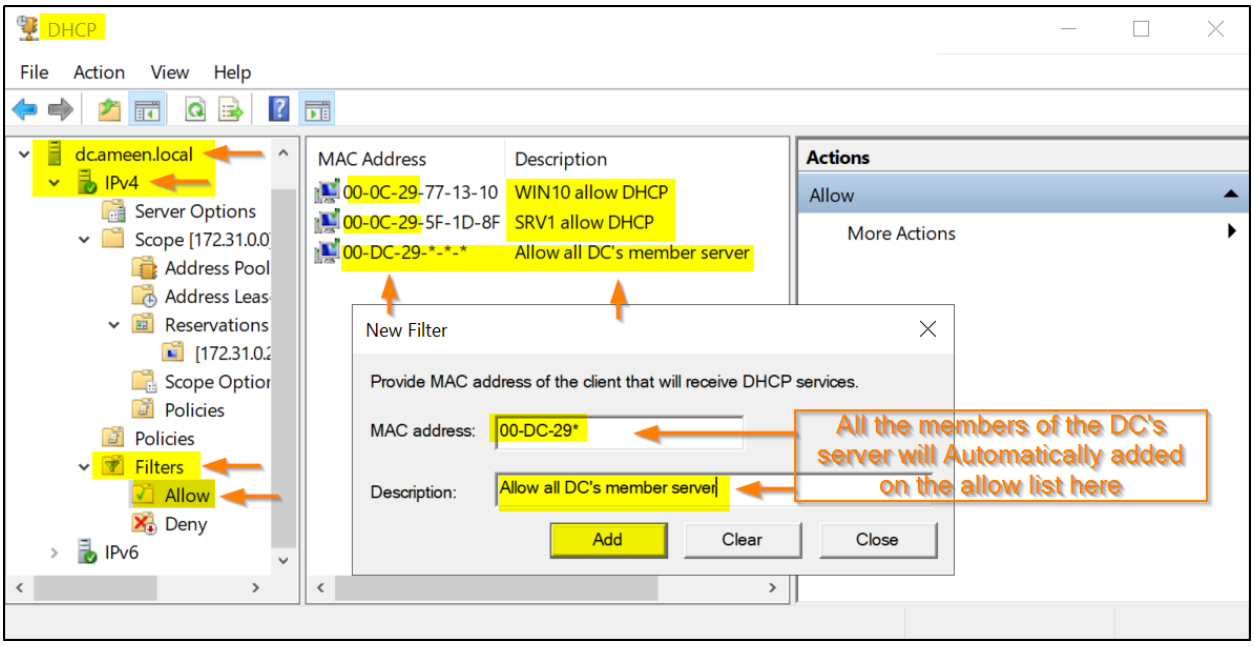
DHCP MAC address filtering can be configured with one of the following options:

Option	Explicit allow list	Explicit deny list	How it works
1	✓	X	The DHCP server will provide IP leases only to devices configured in the explicit allow list
2	X	✓	The DHCP server will provide IP leases to all devices except those configured in the explicit deny list
3	✓	✓	The DHCP server will provide IP leases only to devices configured in the explicit allow list which do not belong to the explicit deny list

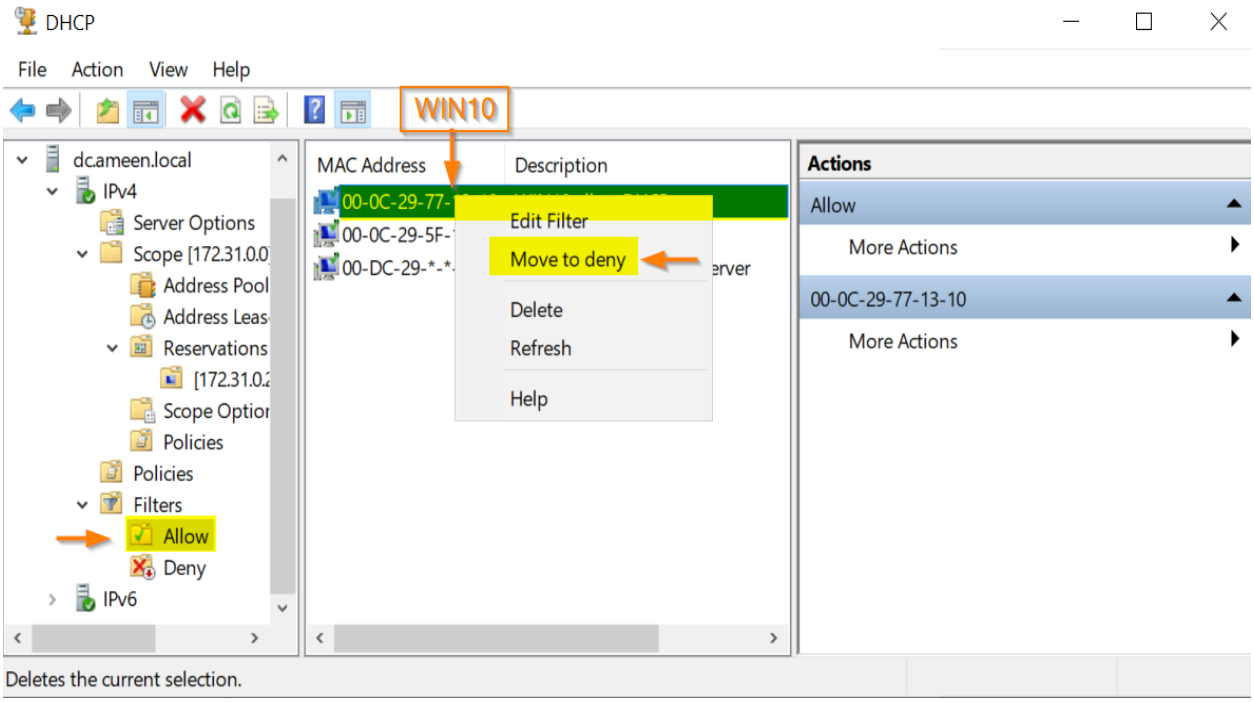
DHCP MAC address filtering is a security feature that is very easy to configure in Microsoft environments. This feature can be used to provide a highly secure DHCP service that provides DHCP leases to only trusted devices. It can also be used to deny offering leases to untrusted ones.

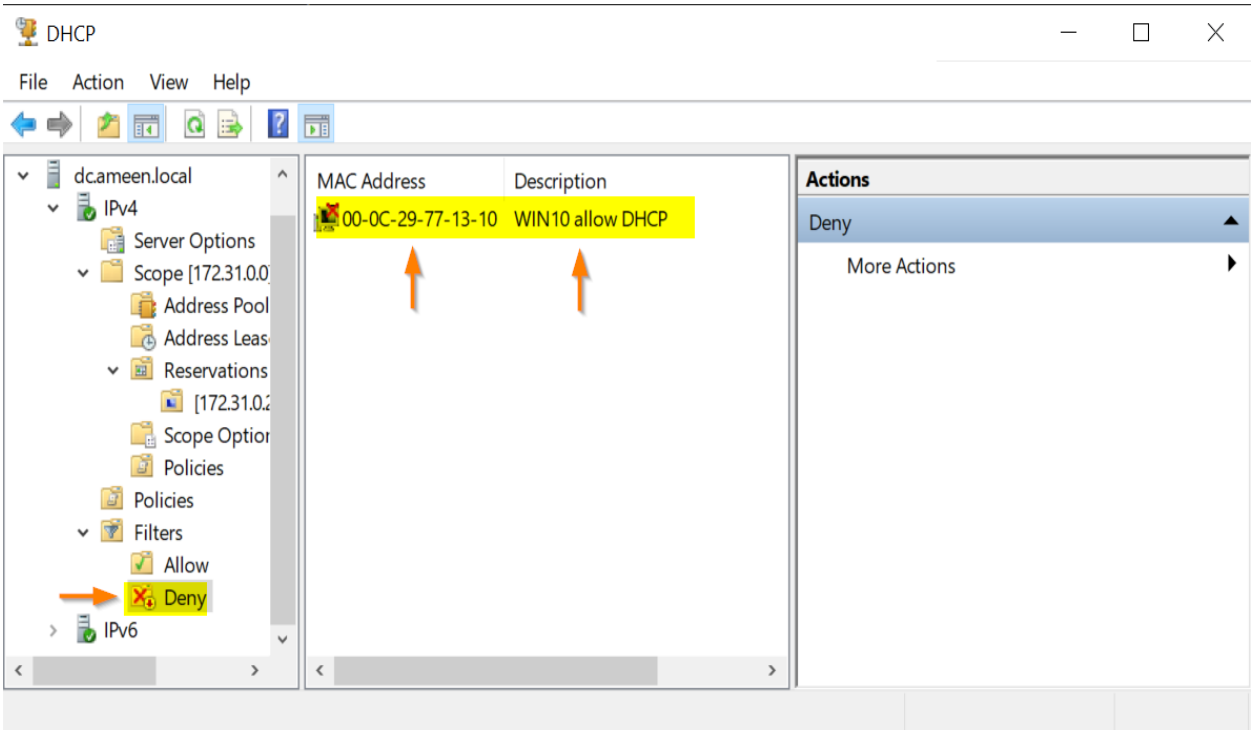
as we see through the following screenshots:



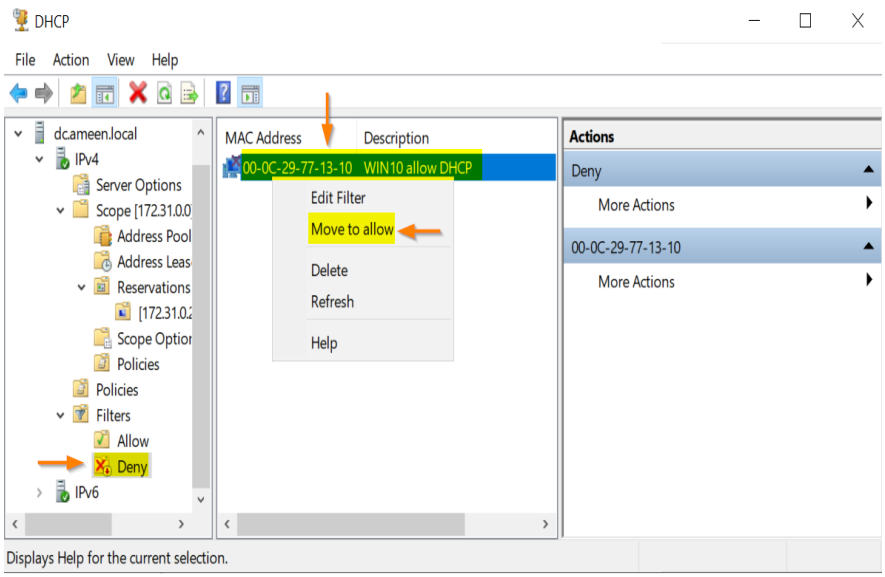


Moreover; I will add WIN10 to the deny list in order to check if it's working successfully. Once it has worked; this will make it an effective strategy against the attack as we spoke of so far.




DHCP
File Action View Help
dc.ameen.local
IPv4
Server Options
Scope [172.31.0.0]
Address Pool
Address Leas
Reservations
[172.31.0.2]
Scope Optior
Policies
Policies
Filters
Allow
Deny
IPv6
MAC Address
Description
00-0C-29-77-13-10
WIN10 allow DHCP
Actions
Deny
More Actions


Home
Win10
DC class
Server1
Ubuntu 64-bit
WIN_10
C:\WINDOWS\system32\cmd.exe
C:\Users\ameen>ipconfig /release
Windows IP Configuration
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.
Ethernet adapter LAN:
Connection-specific DNS Suffix . :
Default Gateway . . . . . :
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\ameen>ipconfig /renew
Windows IP Configuration
An error occurred while renewing interface LAN : unable to contact your DHCP server. Request has timed out.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.
C:\Users\ameen>
WIN10 - unable to connect to DHCP server; because it's in the deny list!


DHCP
File Action View Help
dc.ameen.local
IPv4
Server Options
Scope [172.31.0.0
Address Pool
Address Leas
Reservations
[172.31.0.2
Scope Optior
Policies
Policies
Filters
Allow
Deny
IPv6
MAC Address
Description
00-0C-29-77-13-10 WIN10 allow DHCP
Edit Filter
Move to allow
Delete
Refresh
Help
Actions
Deny
More Actions
00-0C-29-77-13-10
More Actions
Displays Help for the current selection.

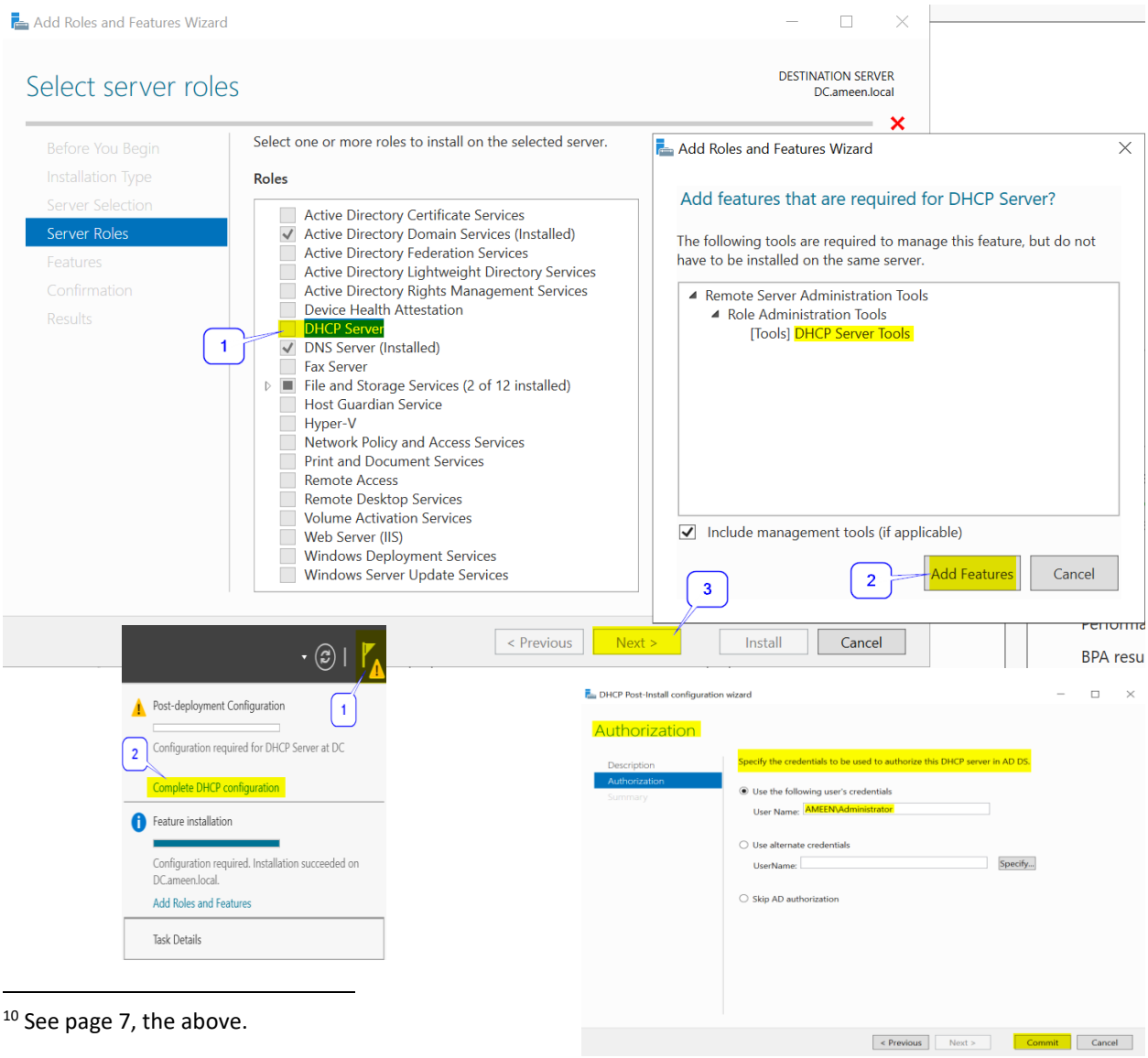

Home
Win10
DC class
Server1
Ubuntu 64-bit
WIN_10
Select C:\WINDOWS\system32\cmd.exe
Connection-specific DNS Suffix . :
C:\Users\ameen>ipconfig /renew
Windows IP Configuration
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.
Ethernet adapter LAN:
Connection-specific DNS Suffix . : ameen.local
IPv4 Address. . . . . : 172.31.0.8
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 172.31.0.2
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\ameen>ipconfig /all
Windows IP Configuration
Host Name . . . . . : WIN10
Primary Dns Suffix . . . . . : ameen.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ameen.local
Ethernet adapter LAN:
Connection-specific DNS Suffix . : ameen.local
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-77-13-10
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 172.31.0.8(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Lease Obtained. . . . . : Wednesday, August 31, 2022 1:18:43 PM
Lease Expires . . . . . : Wednesday, August 31, 2022 9:18:43 PM
Default Gateway . . . . . : 172.31.0.2
DHCP Server . . . . . : 172.31.0.1
DNS Servers . . . . . : 172.31.0.1
NetBIOS over Tcpip. . . . . : Enabled
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 2C-6D-C1-EB-8C-3B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
C:\Users\ameen>
lease for 8 houers
WIN10 - allow list! succeeded to connect to DHCP server.

Creating a DHCP server

I have Already defined the LAN network adapter of the DC server to obtain a static IP address to `172.31.0.1`, the subnet mask to `255.255.0.0` and the preferred DNS server to the loop-back address `127.0.0.1` which is DC itself[10].

In order to install DHCP services on the DC server:

Server Manager > Dashboard > Add roles and features > Select server roles > DHCP server.



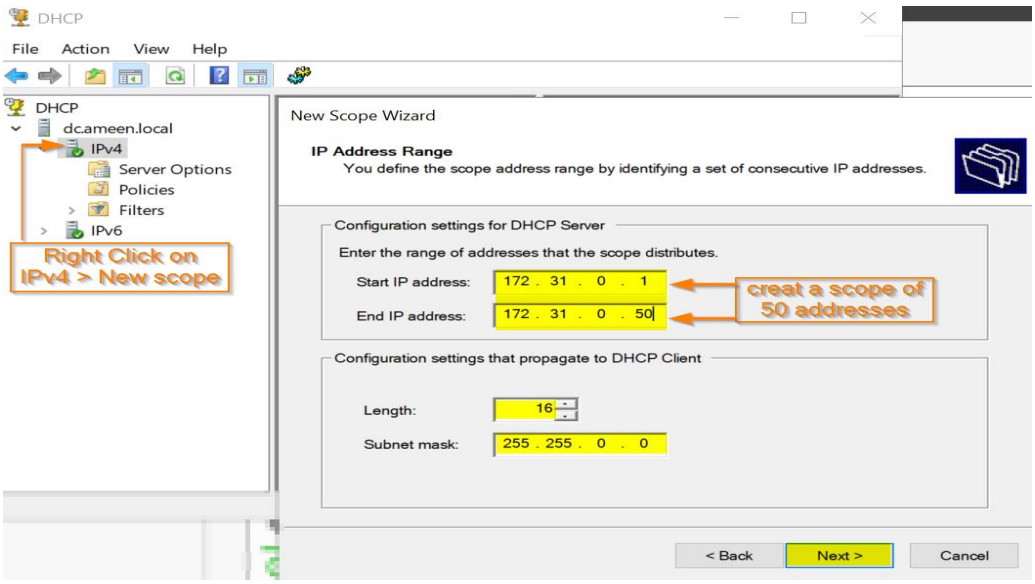
[10] See page 7, the above.

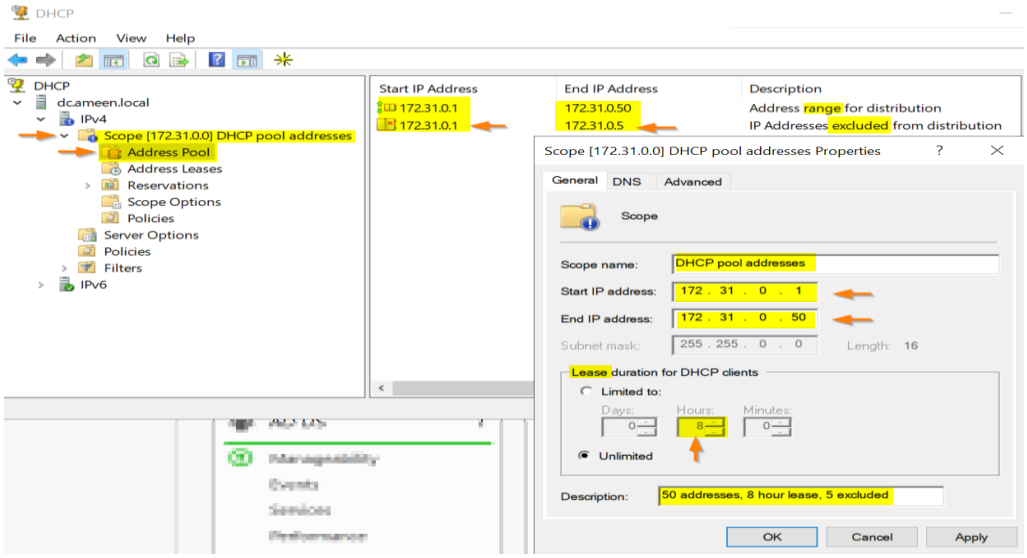
Configuring the DHCP server

As require; a DHCP server must have a pool of 50 available and defined addresses that it can assign to devices requesting an IP.

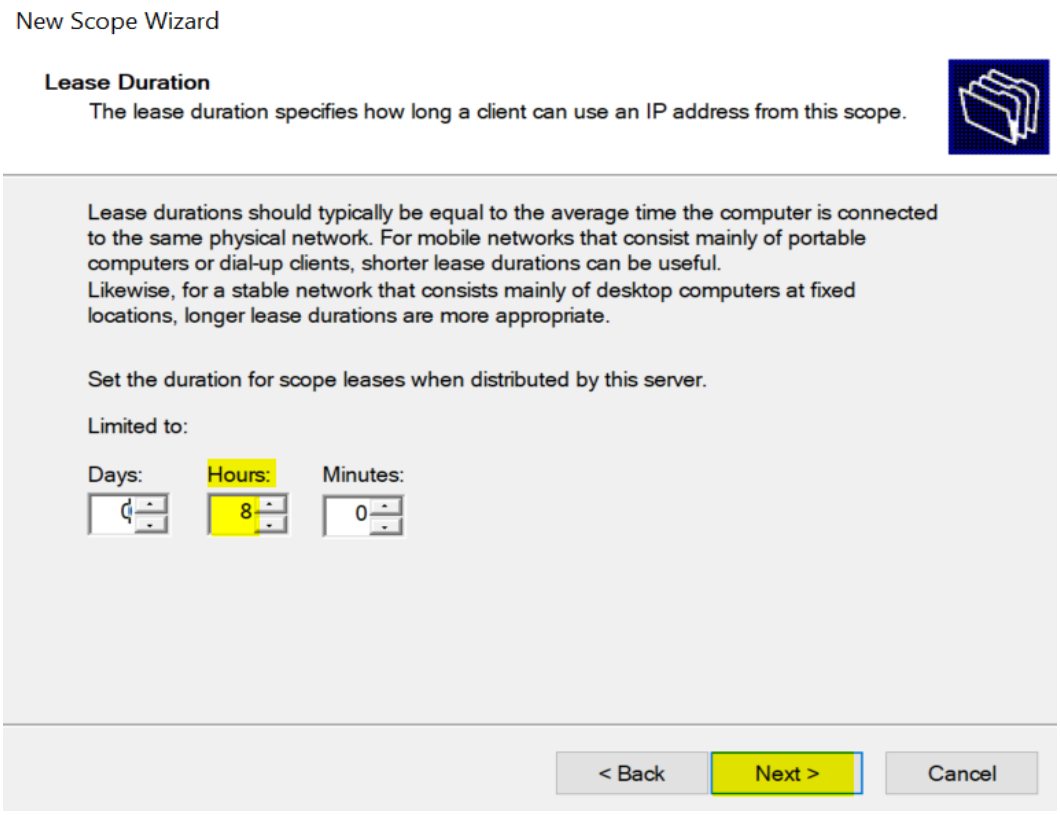
Therefore, I created a scope of 50 addresses, 172.31.0.1-172.31.0.50 through this path:

Server Manager > Dashboard > Tools > DHCP.

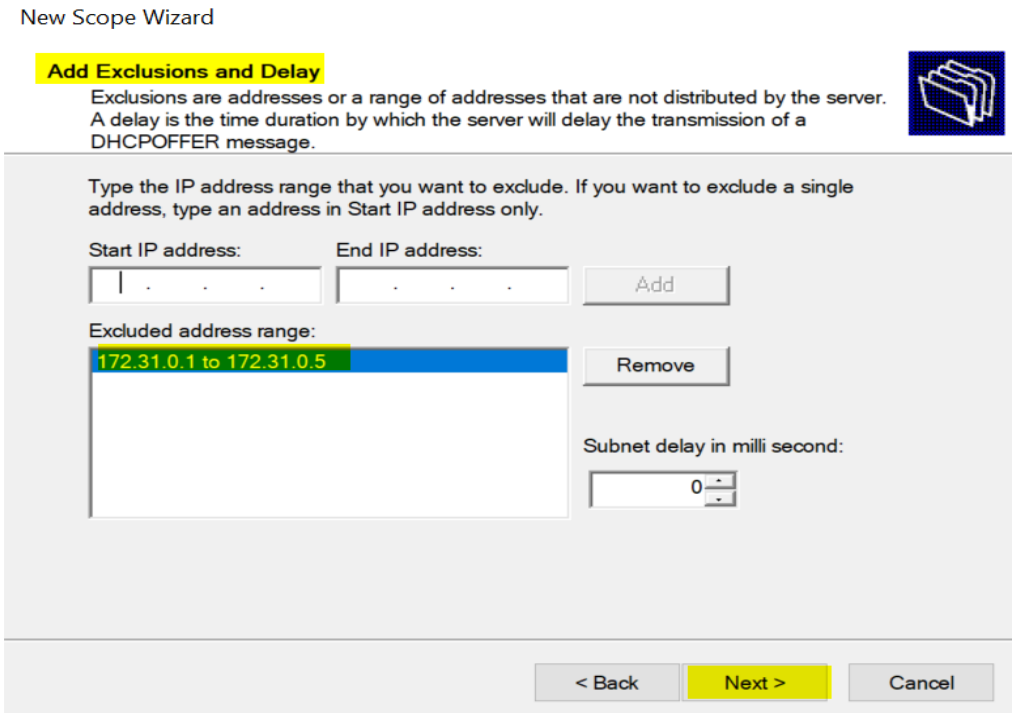




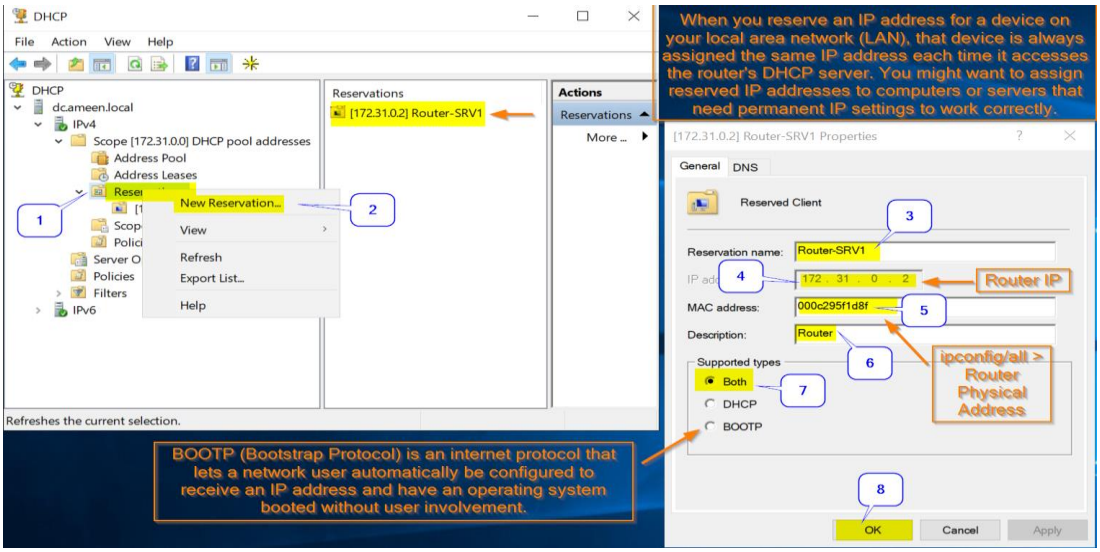
Set the scope leases limited up to 8 hours.



Set the Exclusions Addresses of the first 5 addresses from the scope.

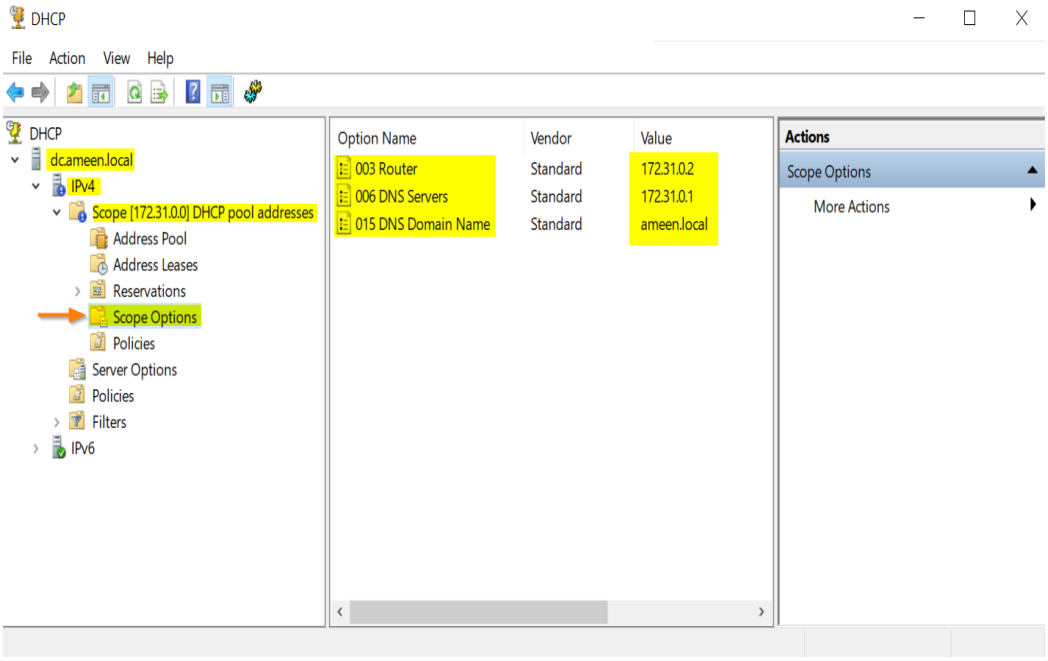


Reservation on a Router:



Set the DHCP Scope Options:

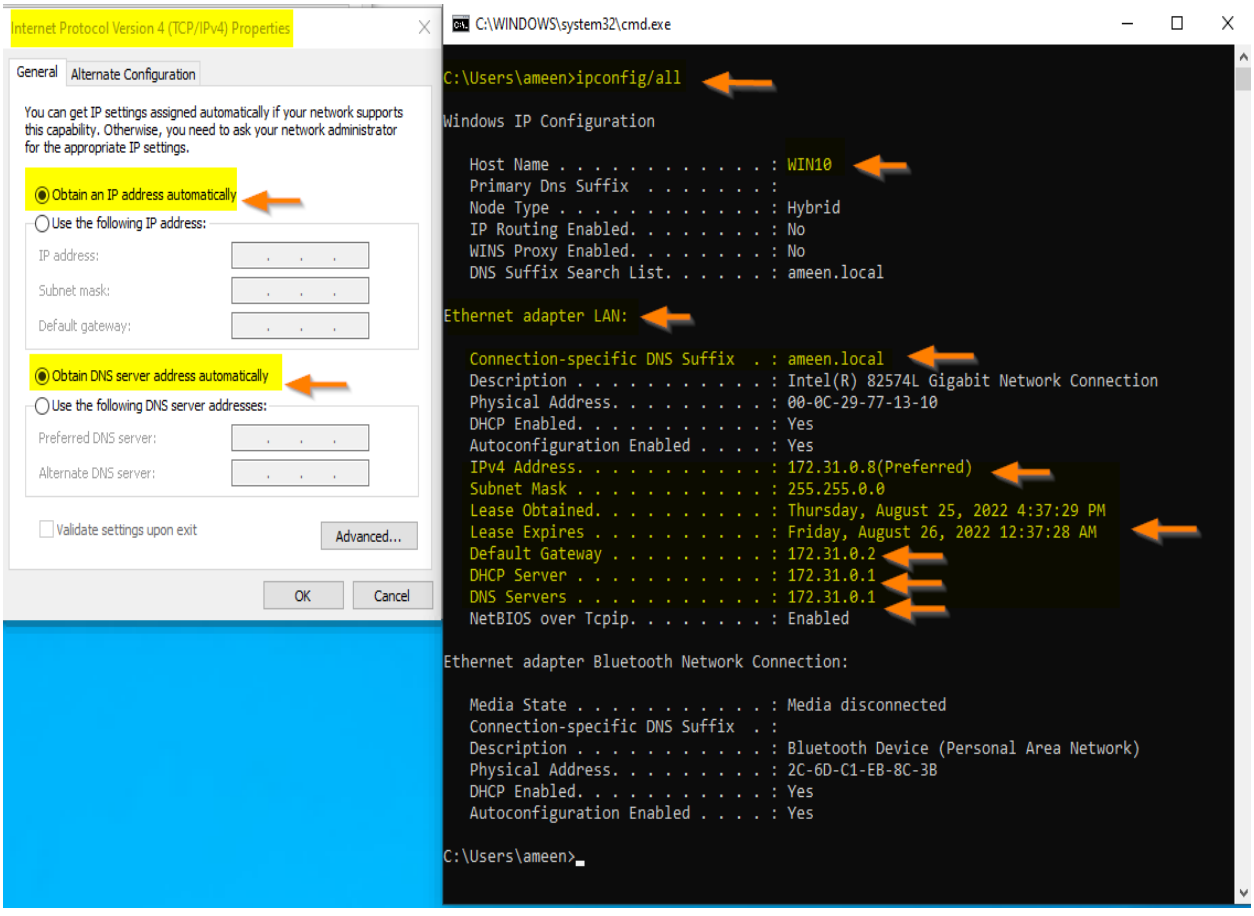
I set up the router in the scope options to my SRV1 server: 172.31.0.2
Also I set up the DNS server to be the DC server itself: 172.31.0.1
and for the suffix I set up the scope to my domain ameen.local.

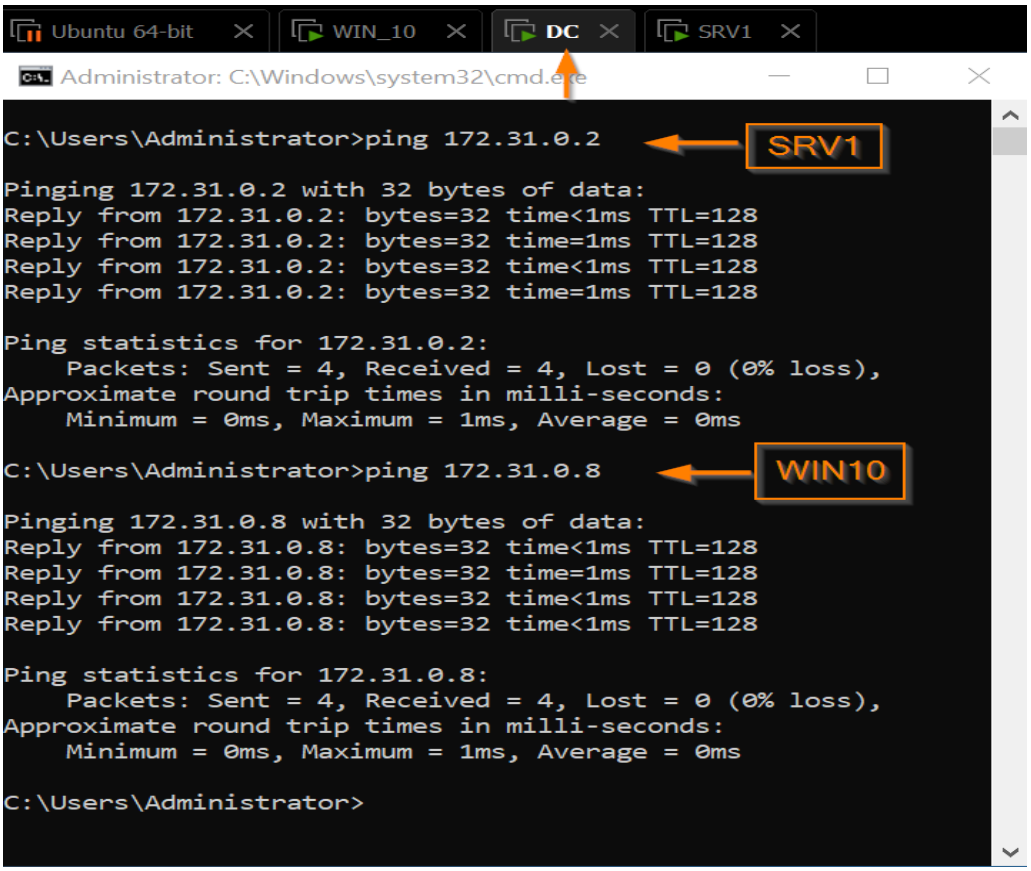


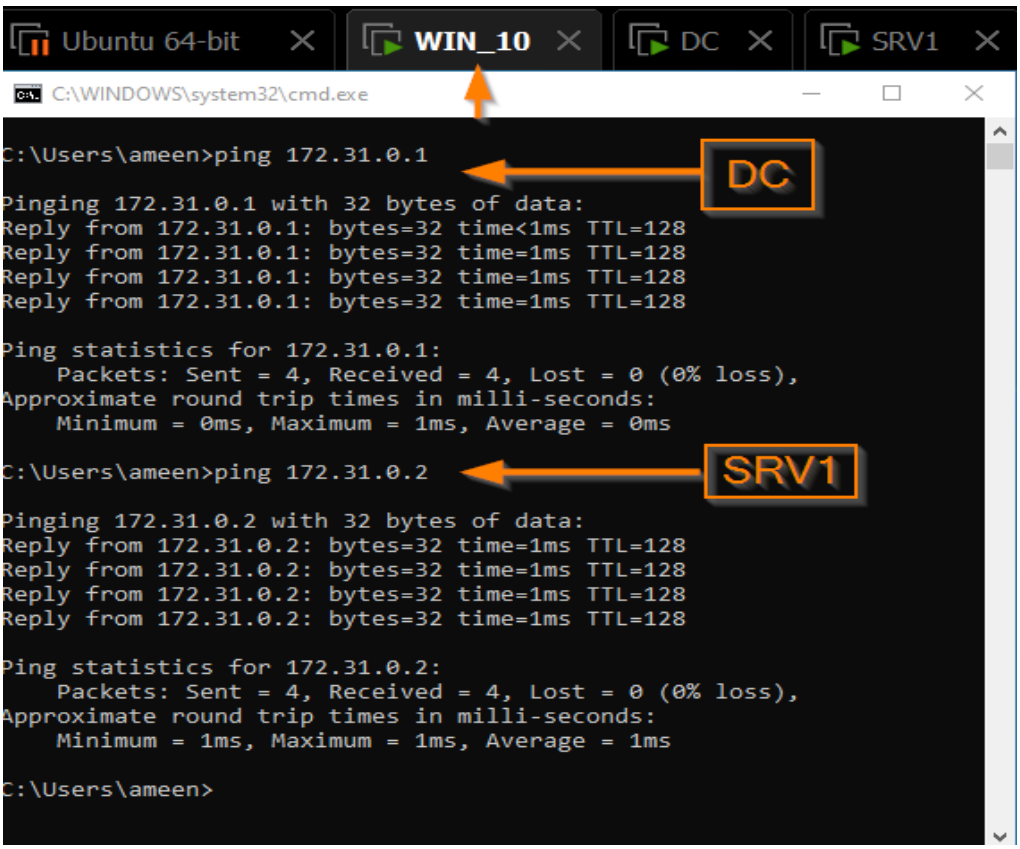
After the installation and configuration of the server as well as the creation of a relevant scope I set up my network adapter in WIN10 to obtain an IP address automatically as well as the DNS server.

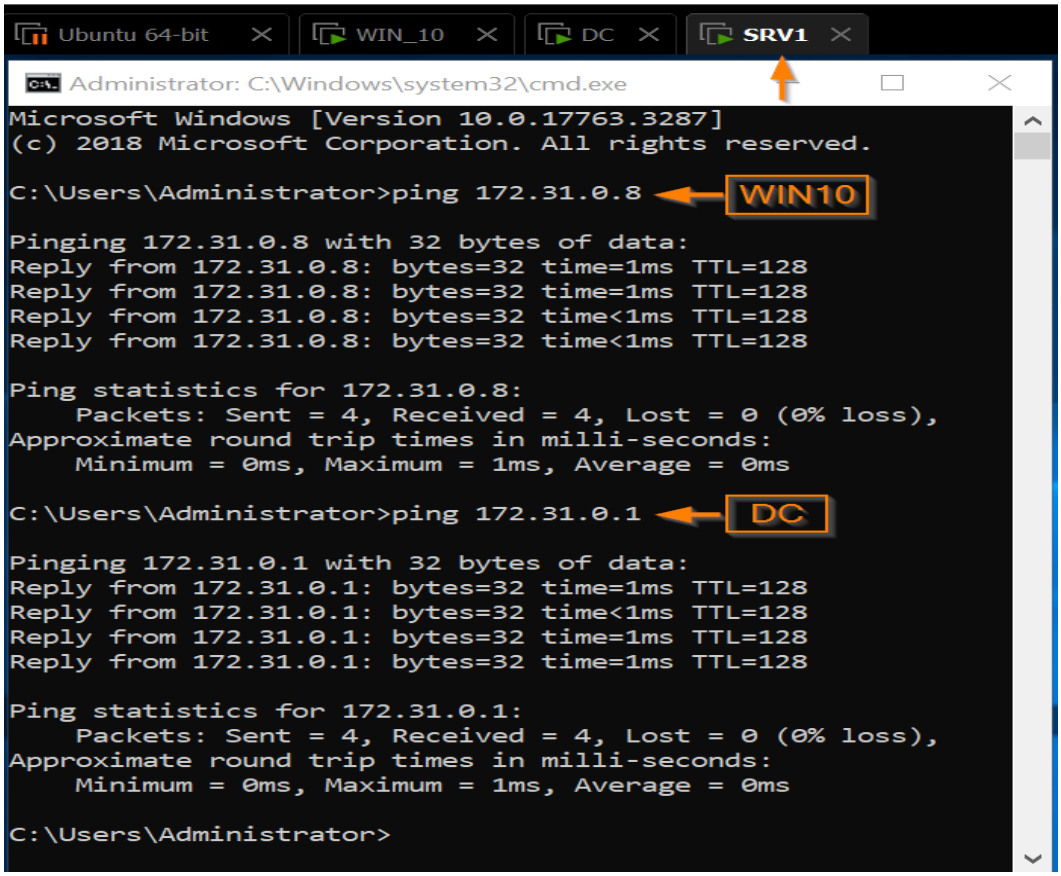
Also I performed a few ping command tests between DC, SRV1 and WIN10 to ensure the connectivity between the different end points.

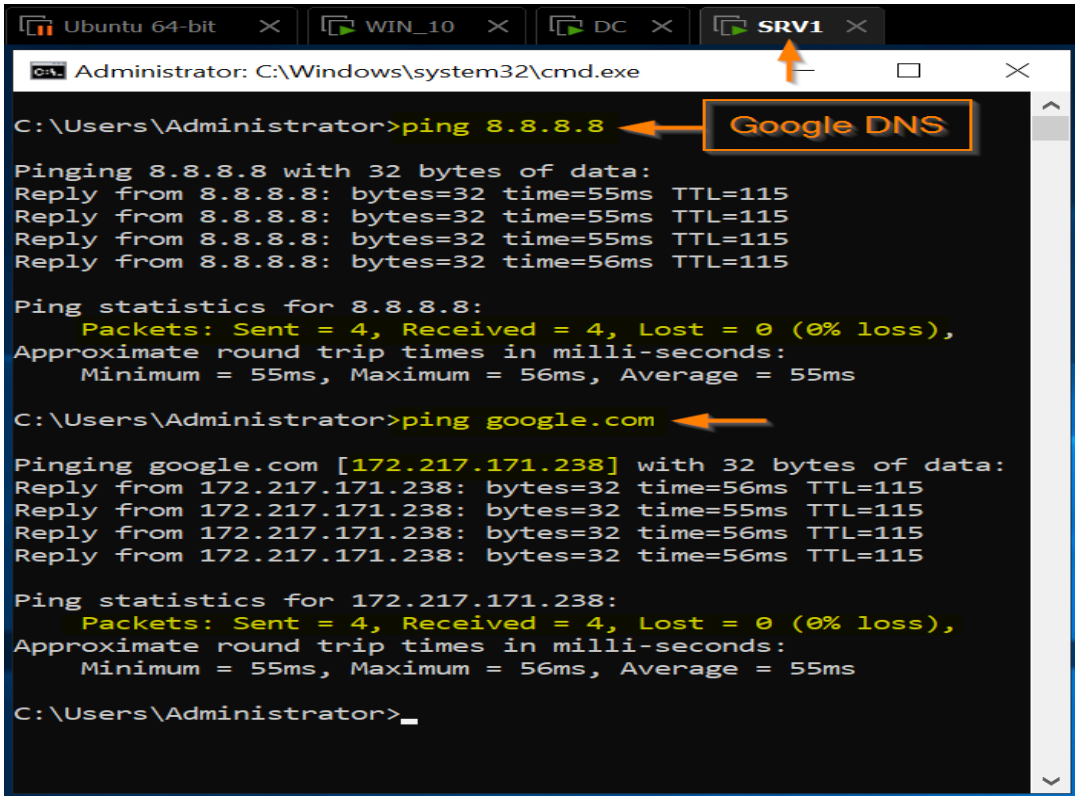
In the end, I made sure that SRV1 has an internet connection by pinging Google DNS at 8.8.8.8.




Ubuntu 64-bit
WIN_10
DC
SRV1
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 172.31.0.2
SRV1
Pinging 172.31.0.2 with 32 bytes of data:
Reply from 172.31.0.2: bytes=32 time<1ms TTL=128
Reply from 172.31.0.2: bytes=32 time=1ms TTL=128
Reply from 172.31.0.2: bytes=32 time<1ms TTL=128
Reply from 172.31.0.2: bytes=32 time=1ms TTL=128
Ping statistics for 172.31.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\Administrator>ping 172.31.0.8
WIN10
Pinging 172.31.0.8 with 32 bytes of data:
Reply from 172.31.0.8: bytes=32 time<1ms TTL=128
Reply from 172.31.0.8: bytes=32 time=1ms TTL=128
Reply from 172.31.0.8: bytes=32 time<1ms TTL=128
Reply from 172.31.0.8: bytes=32 time<1ms TTL=128
Ping statistics for 172.31.0.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\Administrator>


Ubuntu 64-bit
WIN_10
DC
SRV1
C:\WINDOWS\system32\cmd.exe
C:\Users\ameen>ping 172.31.0.1
DC
Pinging 172.31.0.1 with 32 bytes of data:
Reply from 172.31.0.1: bytes=32 time<1ms TTL=128
Reply from 172.31.0.1: bytes=32 time=1ms TTL=128
Reply from 172.31.0.1: bytes=32 time=1ms TTL=128
Reply from 172.31.0.1: bytes=32 time=1ms TTL=128
Ping statistics for 172.31.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\ameen>ping 172.31.0.2
SRV1
Pinging 172.31.0.2 with 32 bytes of data:
Reply from 172.31.0.2: bytes=32 time=1ms TTL=128
Reply from 172.31.0.2: bytes=32 time=1ms TTL=128
Reply from 172.31.0.2: bytes=32 time=1ms TTL=128
Reply from 172.31.0.2: bytes=32 time=1ms TTL=128
Ping statistics for 172.31.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\Users\ameen>

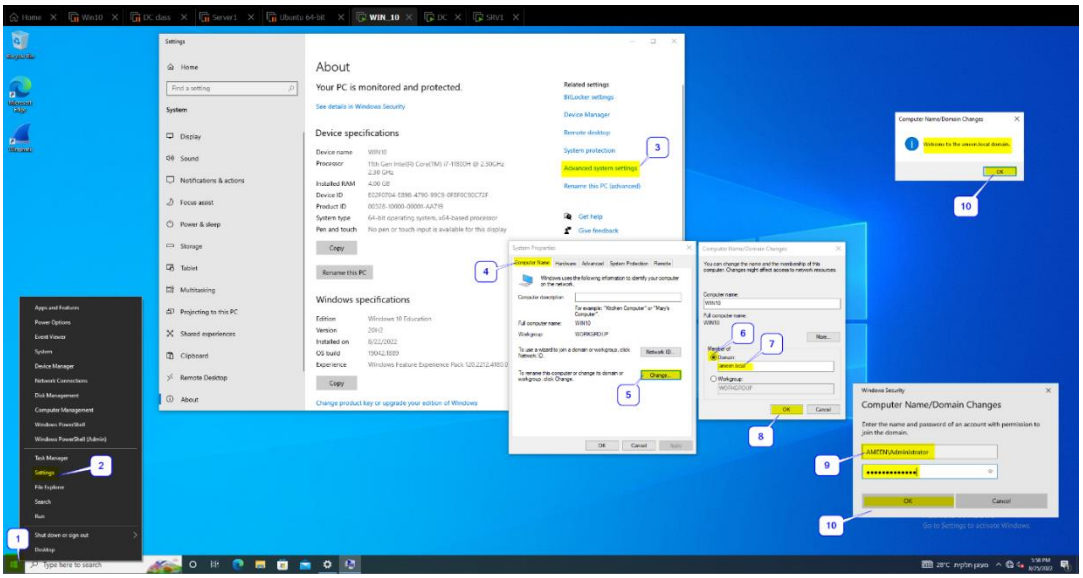

Ubuntu 64-bit
WIN_10
DC
SRV1
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.3287]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ping 172.31.0.8
WIN10
Pinging 172.31.0.8 with 32 bytes of data:
Reply from 172.31.0.8: bytes=32 time=1ms TTL=128
Reply from 172.31.0.8: bytes=32 time=1ms TTL=128
Reply from 172.31.0.8: bytes=32 time<1ms TTL=128
Reply from 172.31.0.8: bytes=32 time<1ms TTL=128
Ping statistics for 172.31.0.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\Administrator>ping 172.31.0.1
DC
Pinging 172.31.0.1 with 32 bytes of data:
Reply from 172.31.0.1: bytes=32 time=1ms TTL=128
Reply from 172.31.0.1: bytes=32 time<1ms TTL=128
Reply from 172.31.0.1: bytes=32 time=1ms TTL=128
Reply from 172.31.0.1: bytes=32 time=1ms TTL=128
Ping statistics for 172.31.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\Administrator>


Ubuntu 64-bit
WIN_10
DC
SRV1
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 8.8.8.8
Google DNS
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=55ms TTL=115
Reply from 8.8.8.8: bytes=32 time=55ms TTL=115
Reply from 8.8.8.8: bytes=32 time=55ms TTL=115
Reply from 8.8.8.8: bytes=32 time=56ms TTL=115
Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 55ms, Maximum = 56ms, Average = 55ms
C:\Users\Administrator>ping google.com
Pinging google.com [172.217.171.238] with 32 bytes of data:
Reply from 172.217.171.238: bytes=32 time=56ms TTL=115
Reply from 172.217.171.238: bytes=32 time=55ms TTL=115
Reply from 172.217.171.238: bytes=32 time=56ms TTL=115
Reply from 172.217.171.238: bytes=32 time=56ms TTL=115
Ping statistics for 172.217.171.238:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 55ms, Maximum = 56ms, Average = 55ms
C:\Users\Administrator>

Connecting WIN10 and SRV1 to ameen.local

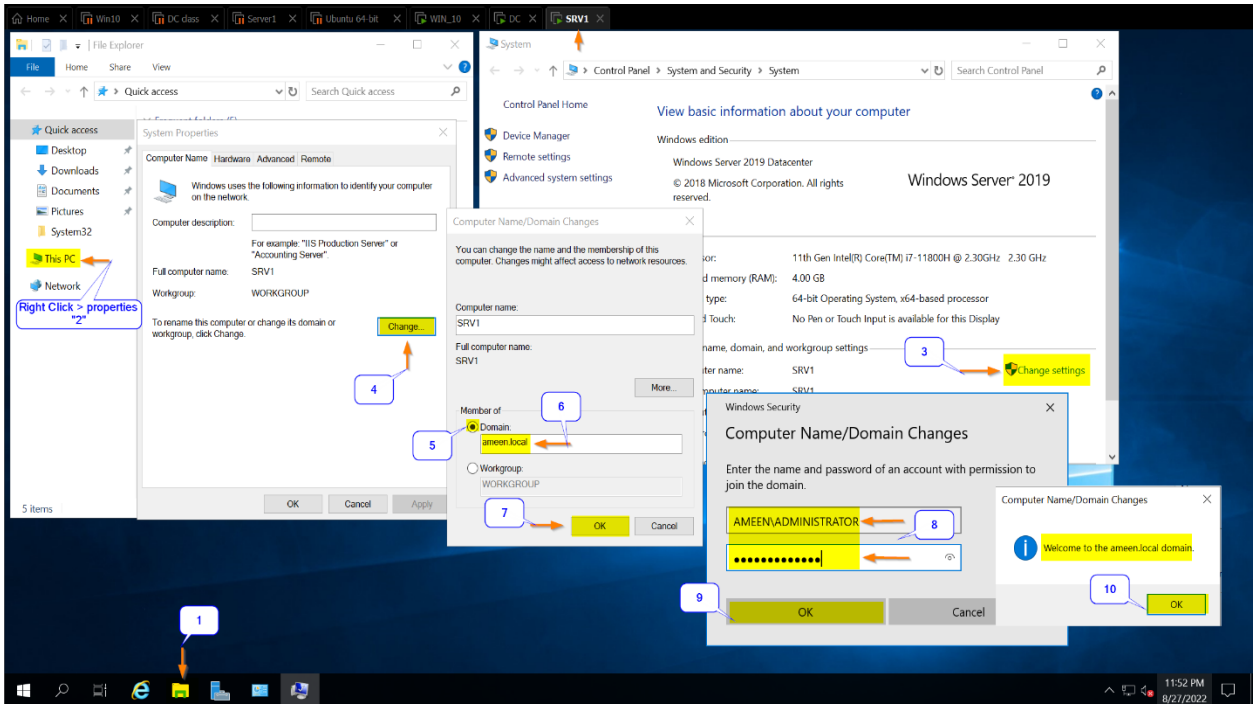
The connection of WIN10 and SRV1 to the domain will allow us to have a control over these end points through the DC and to manage all devices in the network from a centralized Place.

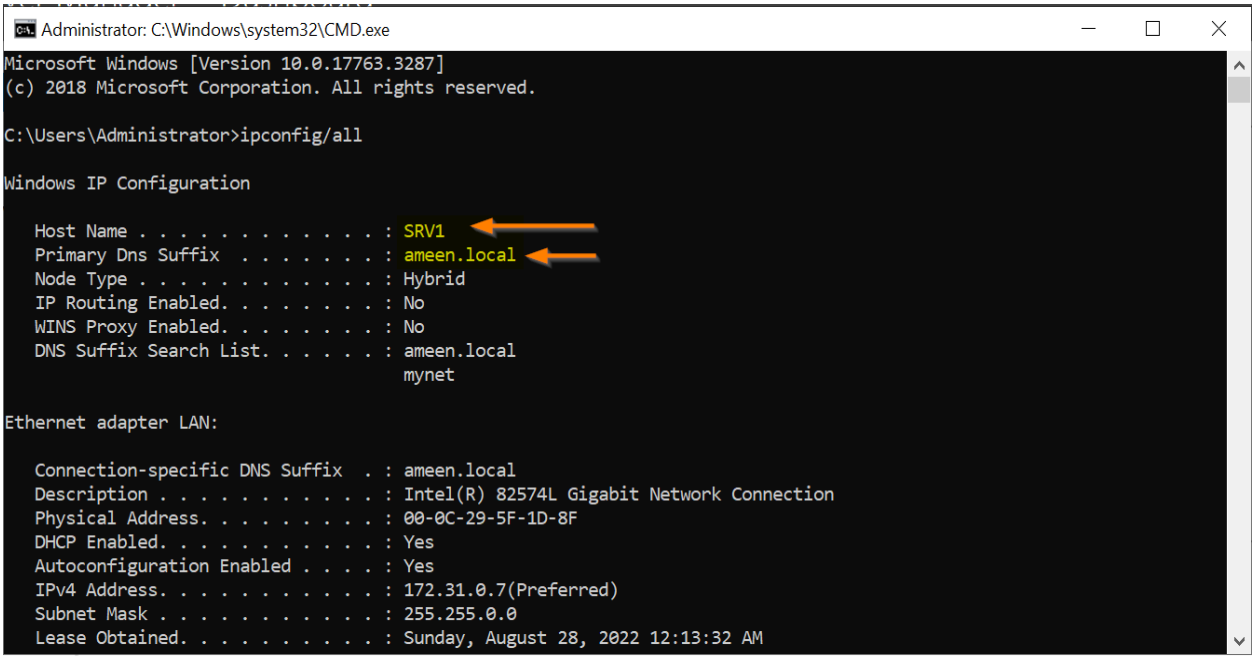
WIN10




```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19042.1889]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ameen>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN10
   Primary Dns Suffix  . . . . . . . : ameen.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : ameen.local

Ethernet adapter LAN:

   Connection-specific DNS Suffix  . : ameen.local
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-77-13-10
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.31.0.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Lease Obtained. . . . . . . . . . : Sunday, August 28, 2022 12:13:57 AM
   Lease Expires . . . . . . . . . . : Sunday, August 28, 2022 8:13:56 AM
   Default Gateway . . . . . . . . . : 172.31.0.2
   DHCP Server . . . . . . . . . . . : 172.31.0.1
   DNS Servers . . . . . . . . . . . : 172.31.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

SRV1


Right Click > properties "2"
Change...
Change settings
Computer Name/Domain Changes
Windows Security
Computer Name/Domain Changes
Enter the name and password of an account with permission to join the domain.
AMEEN\ADMINISTRATOR
Welcome to the ameen.local domain.
OK
Cancel

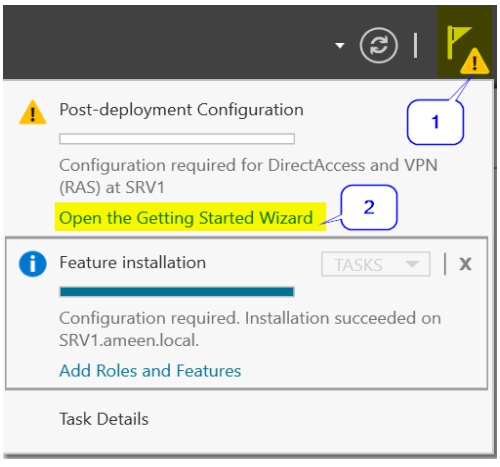

Administrator: C:\Windows\system32\CMD.exe
Microsoft Windows [Version 10.0.17763.3287]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ipconfig/all
Windows IP Configuration
Host Name . . . . . : SRV1
Primary Dns Suffix . . . . . : ameen.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ameen.local
mynet
Ethernet adapter LAN:
Connection-specific DNS Suffix . : ameen.local
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-5F-1D-8F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 172.31.0.7(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Lease Obtained. . . . . : Sunday, August 28, 2022 12:13:32 AM

Routing and PAT setup

Routing and Remote Access Service (RRAS) is a Microsoft API and server software that makes it possible to create applications to administer the routing and remote access service capabilities of the operating system, to function as a network router[11].
On the other hand; Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses. Most home networks use PAT[12].

Creating and Configuring a Router

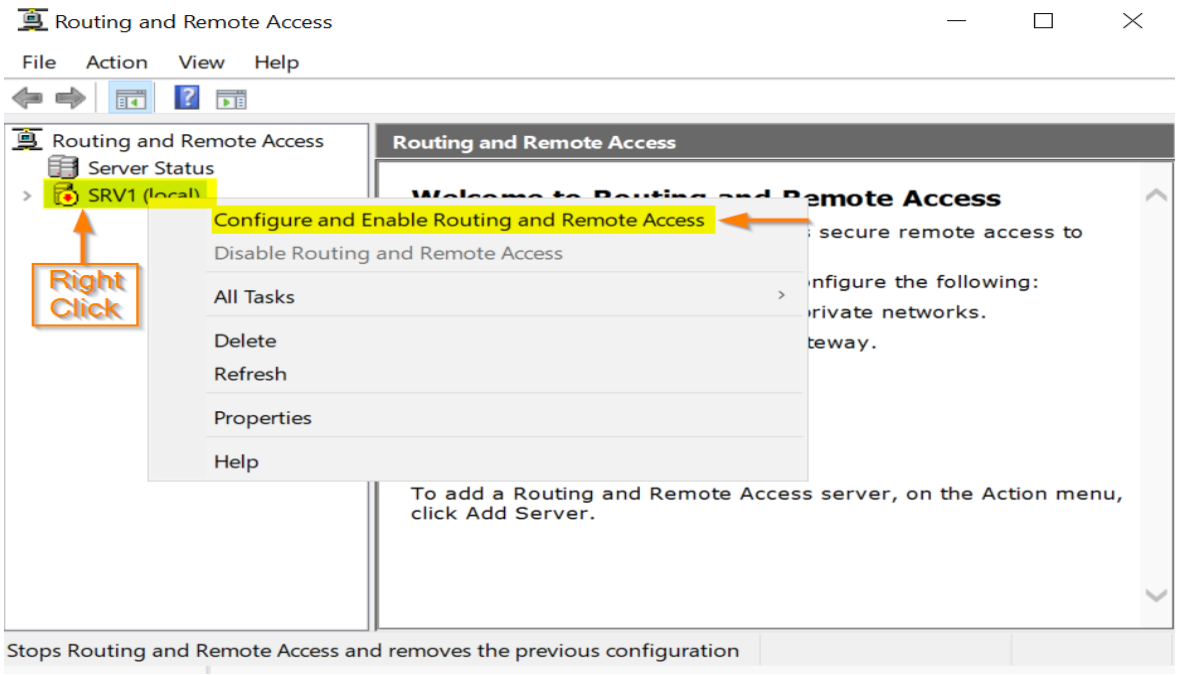
In order to add the Routing and Remote Access Service (RRAS), I accessed the path:
Server Manager > Dashboard > Add Roles and Features > Remote Access.

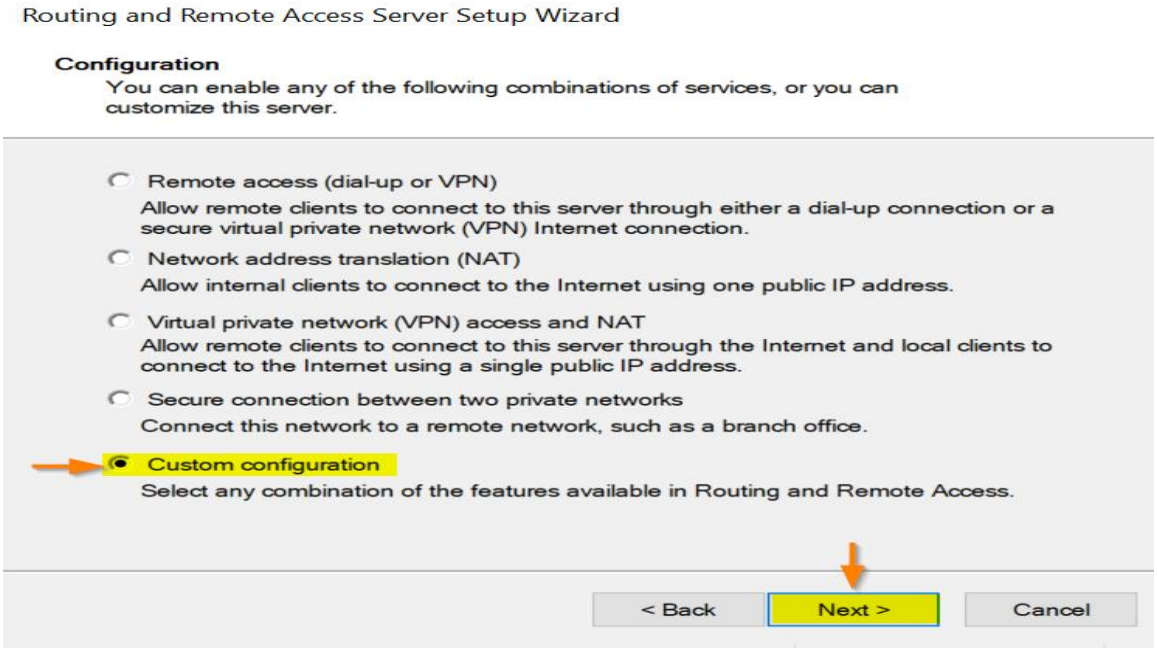


[11] https://www.techopedia.com/definition/3424/routing-and-remote-access-service-rras
[12] https://www.techtarget.com/searchnetworking/definition/Port-Address-Translation-PAT

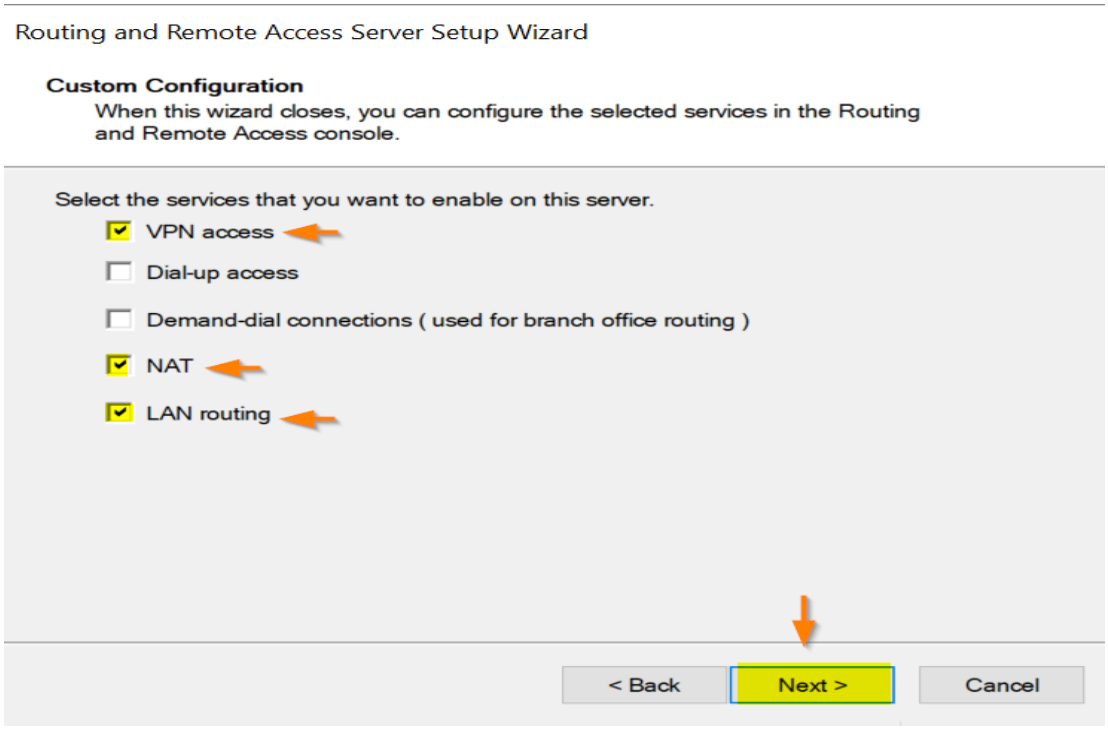
I then configured the RRAS through:

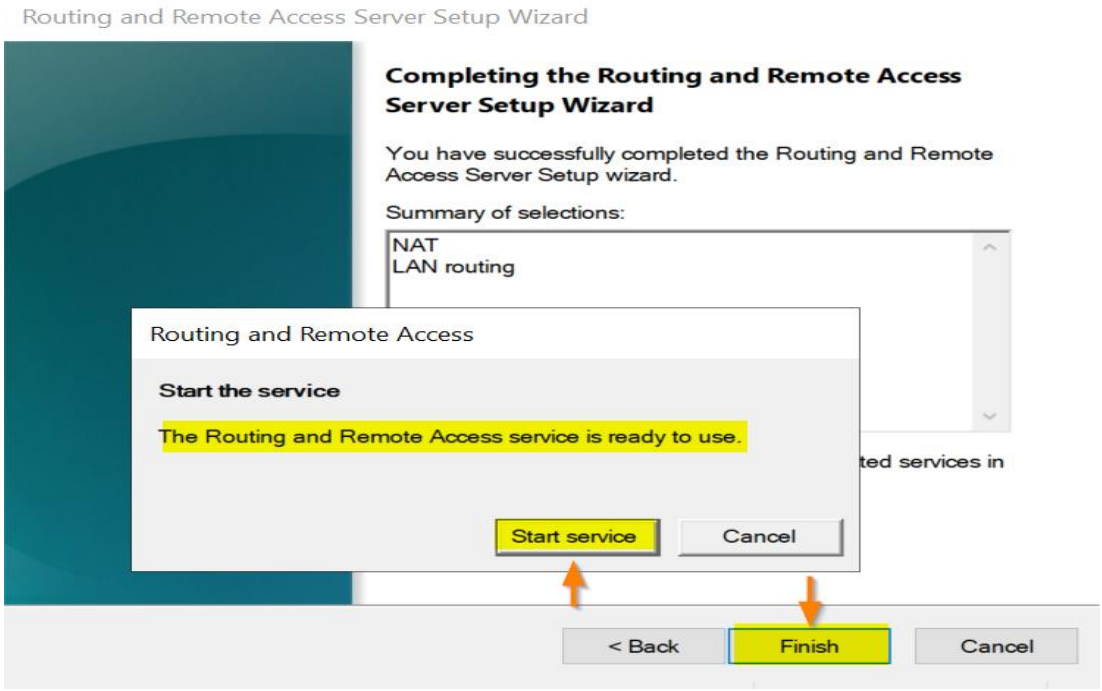
Server Manager > Dashboard > Tools > Routing and Remote Access.





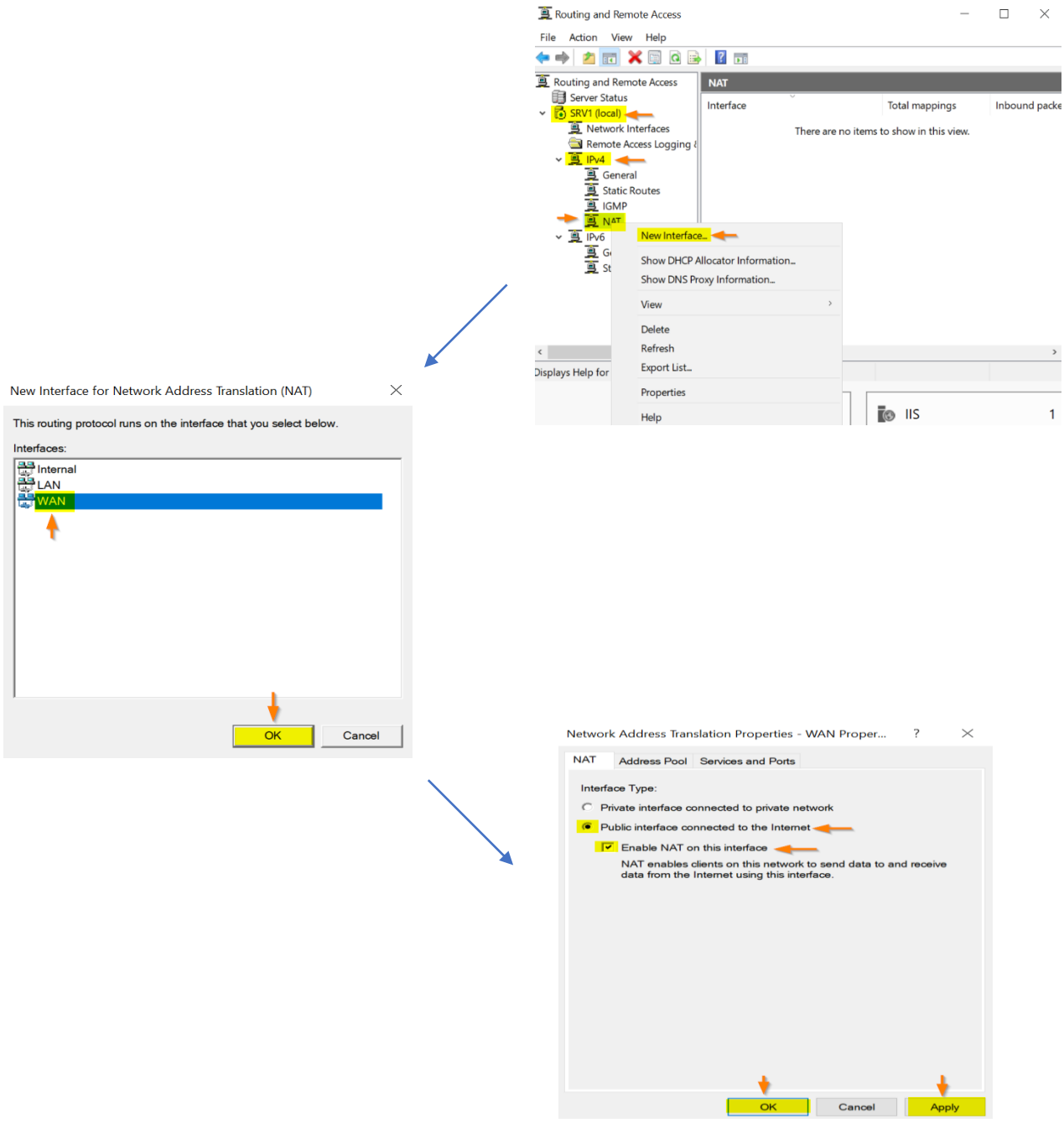
Enabled VPN access, Nat and LAN Routing.





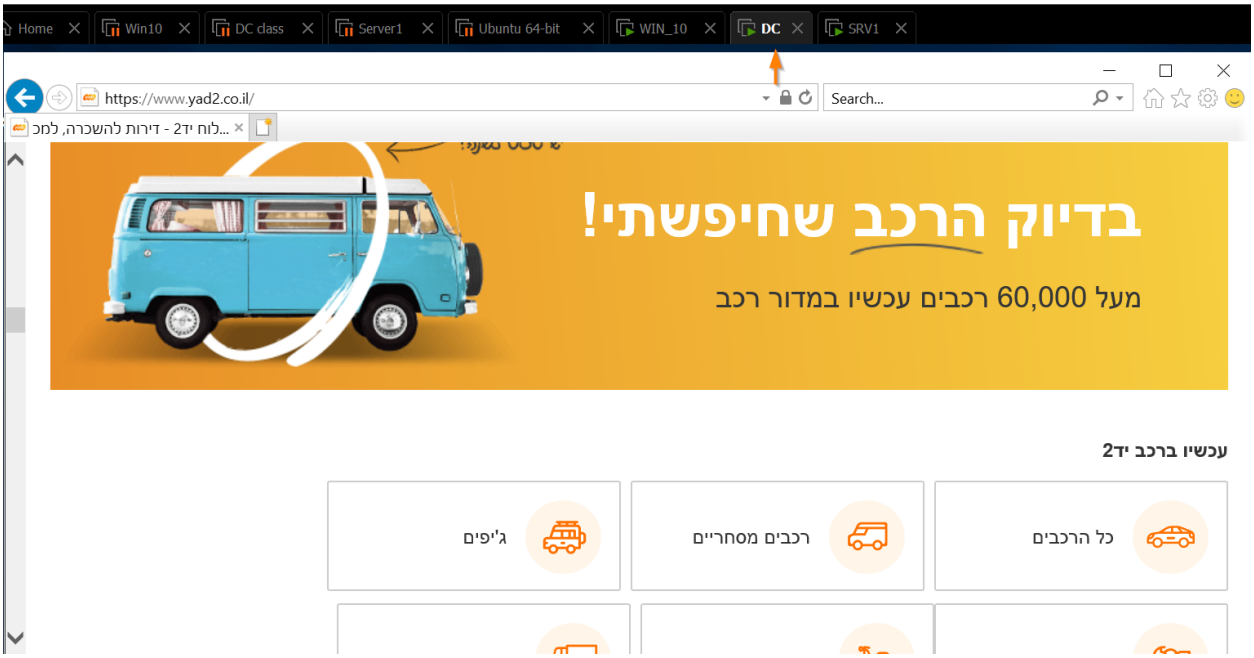
As part of the Router setup process, I had to configure the NAT service and set the WAN network adapter as the one that the NAT will operate on using the path:

Server Manager > Dashboard > Tools > Routing and Remote Access.

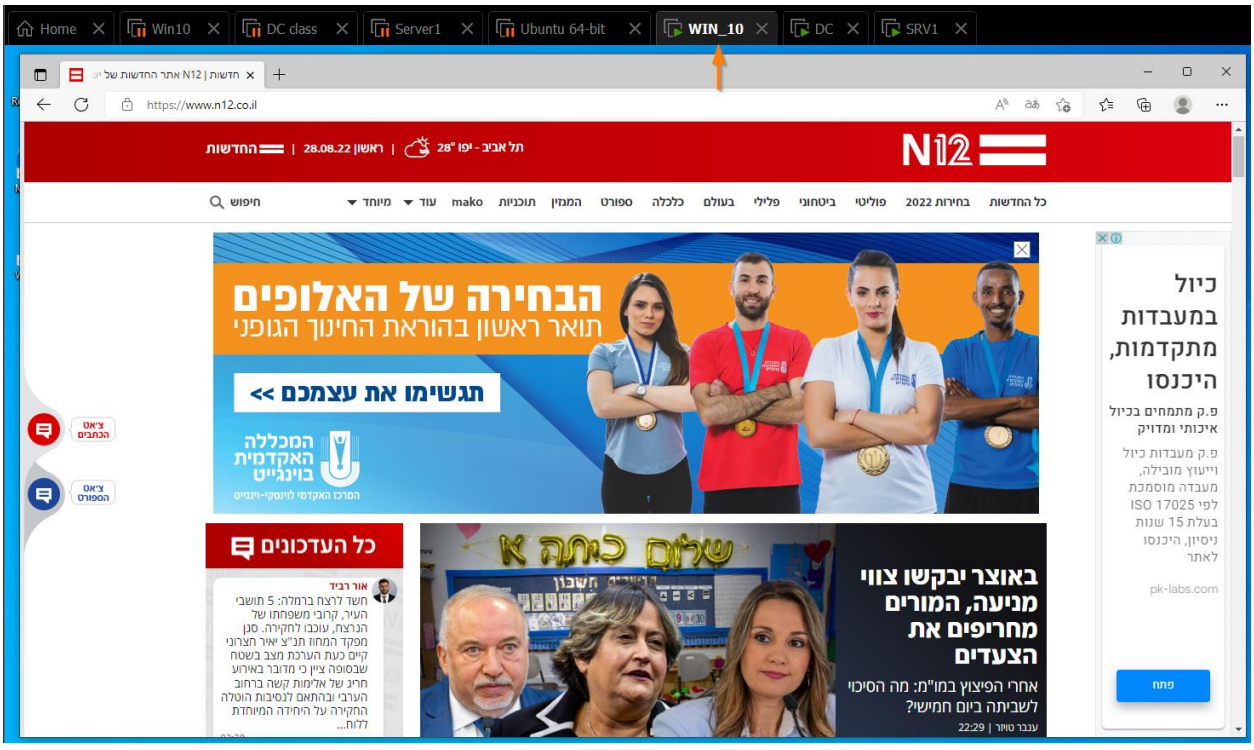


After completing the RRAS process successfully, I've made sure all of the network components were able to access the internet.

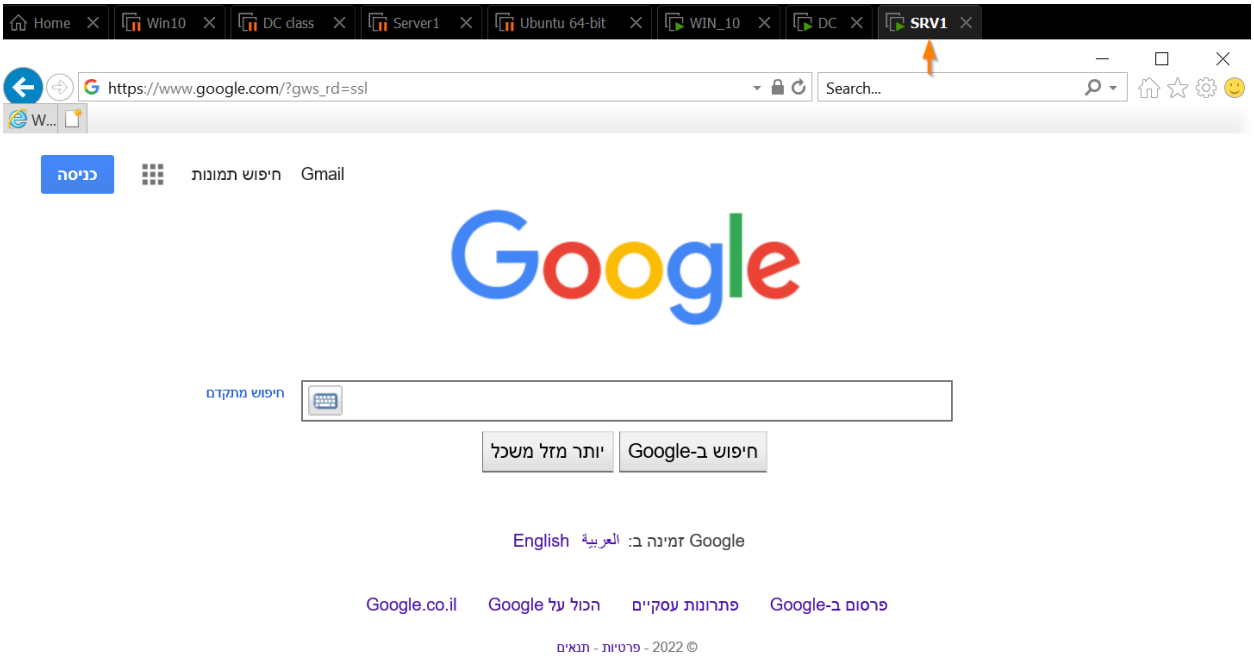
DC:



Win10:



SRV1:


Home
Win10
DC class
Server1
Ubuntu 64-bit
WIN_10
DC
SRV1
https://www.google.com/?gws_rd=ssl
Search...
כניסה
חיפוש תמונות
Gmail
Google
חיפוש מתקדם
חיפוש ב-Google
יותר מזל משכל
Google זמינה ב: English العربية
Google.co.il
הכול על Google
פתרונות עסקיים
פרסום ב-Google
© 2022 - פרטיות - תנאים

DNS (Domain Name System)

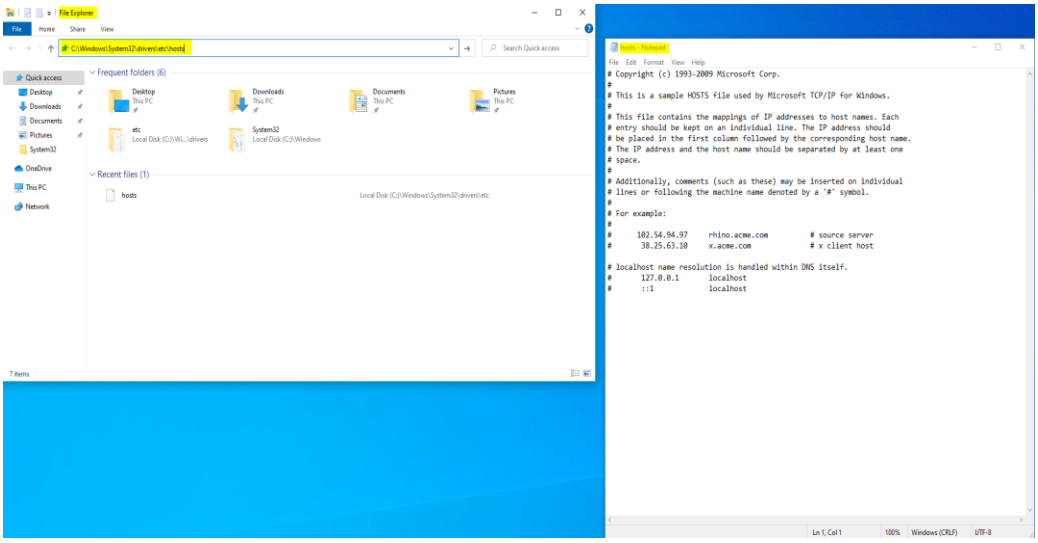
The Domain Name System (DNS) turns domain names into IP addresses, which browsers use to load internet pages. Every device connected to the internet has its own IP address, which is used by other devices to locate the device.

DNS servers make it possible for people to input normal words into their browsers, such as Fortinet.com, without having to keep track of the IP address for every website[13].

The DNS works with UDP port 53 and can translates the Fully Qualified Domain Name (FQDN) witch is a combination of the host name and the DNS suffix; in our case for example DC.ameen.local.

There are 2 records of name translations to IP addresses present on the DNS server:

1. Hosts file – a file found through the path: **%systemroot%\System32\drivers\etc\hosts.**



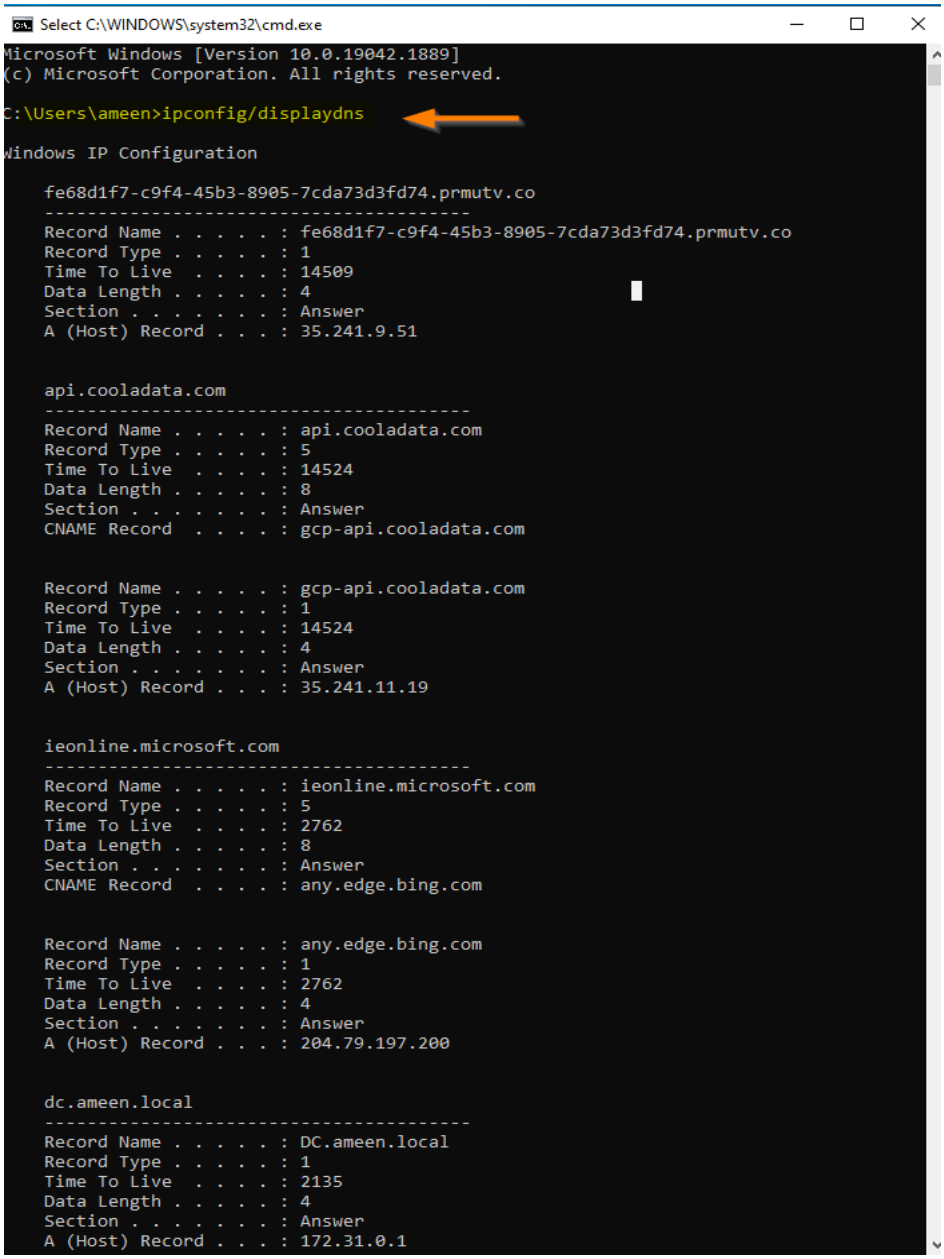
[13] https://www.fortinet.com/resources/cyberglossary/what-is-dns

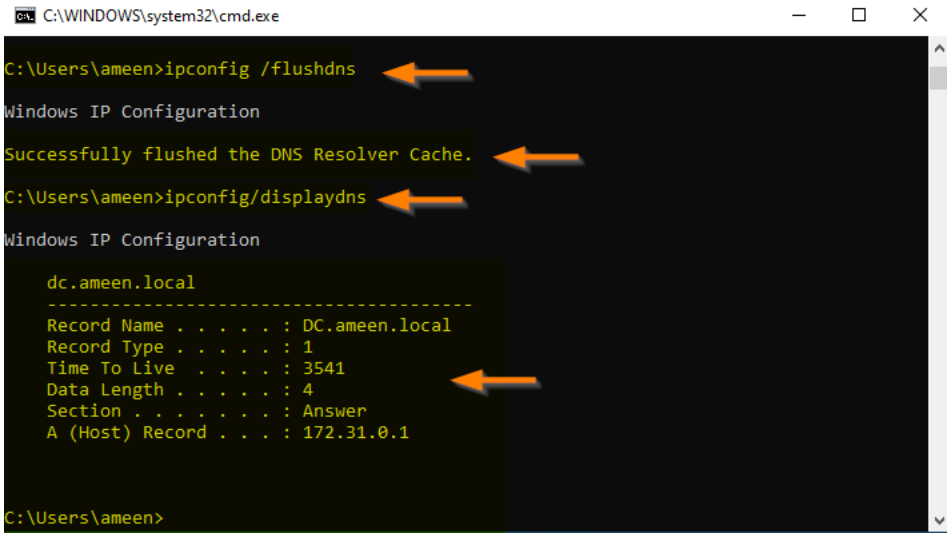
2. DNS Cache – names that have been translated by the DNS server are saved in the DNS cache for a specified period of time (TTL).

   To see the current DNS settings, type ipconfig /displaydns and press Enter.

   To delete the entries, type ipconfig /flushdns and press Enter.

   To see your DNS settings again, type ipconfig /displaydns and press Enter.

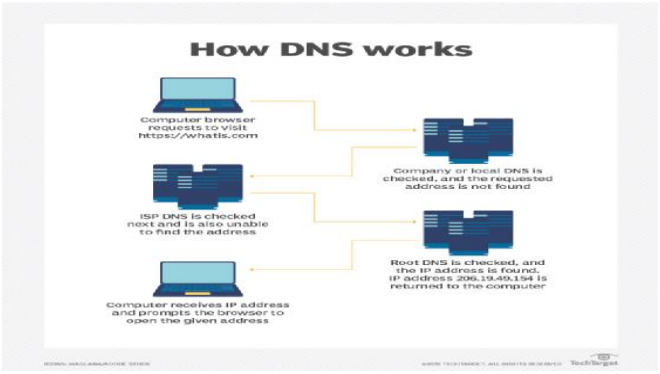




These records both increase the efficiency of the translation process and prevent unnecessary network traffic.

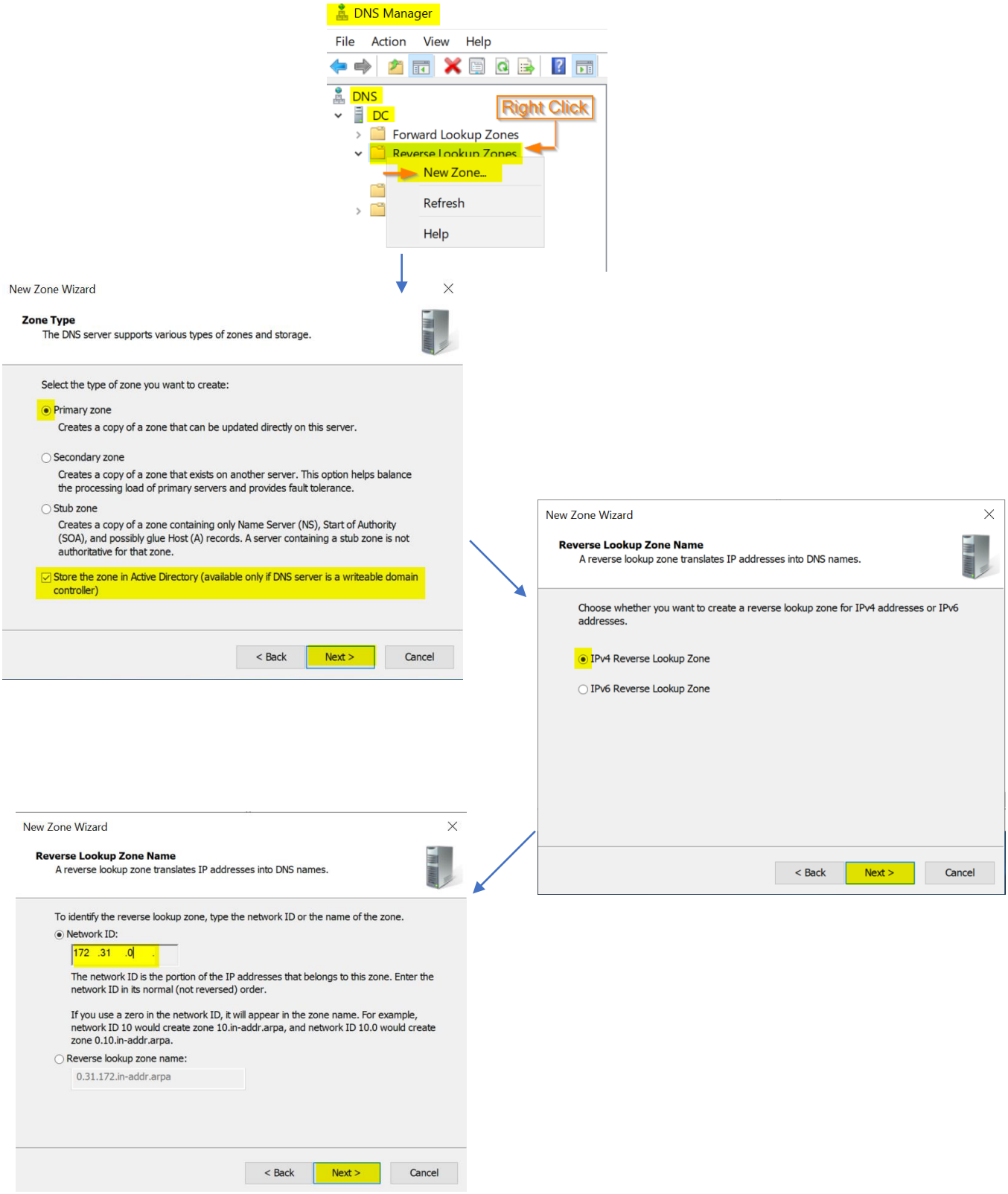
The DNS server is already installed with the active directory domain services On the DC server[14].

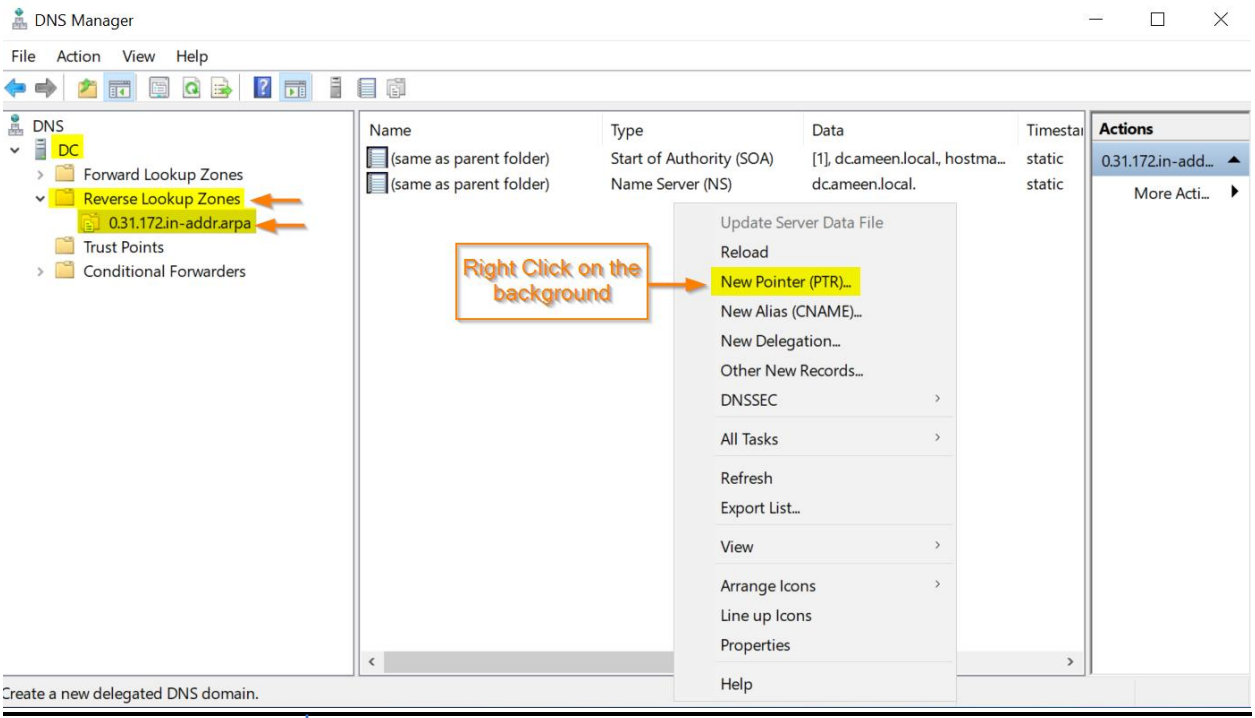
DNS services can be installed both as part of a different service's installation or manually by itself. In our case the DNS was installed in accompaniment with the Active Directory domain services installed initially on the DC server.

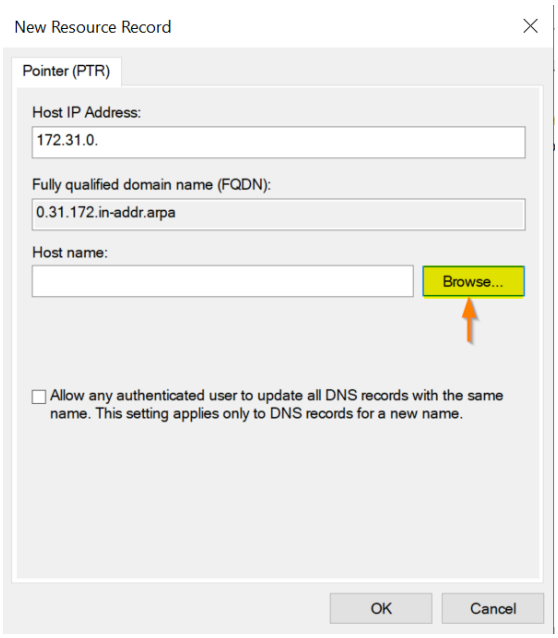


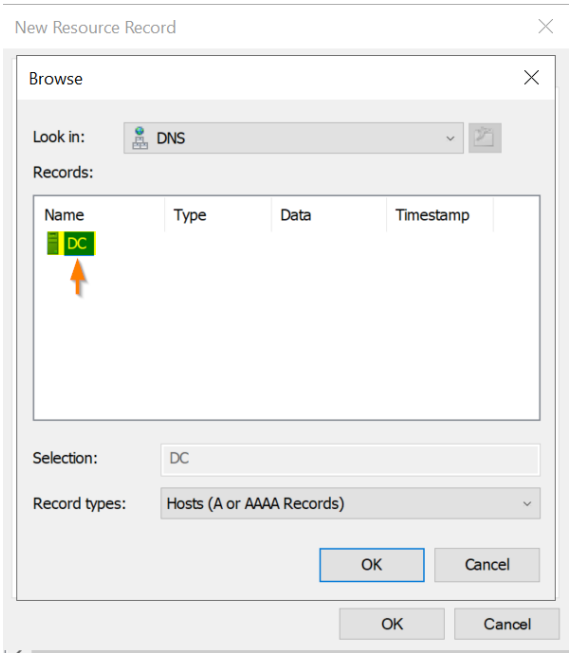
[14] See page 14, the above.

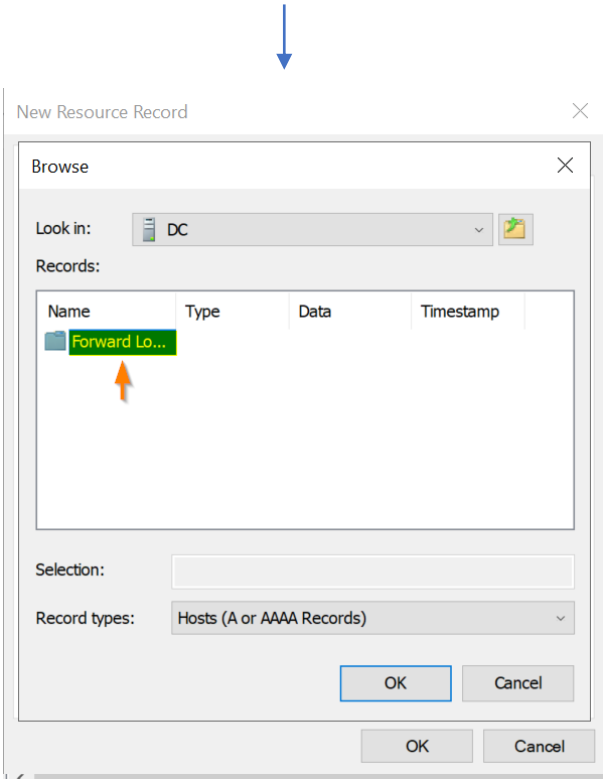
Let's Now create a **IPv4 Reverse Lookup Zones** on our DNS server.

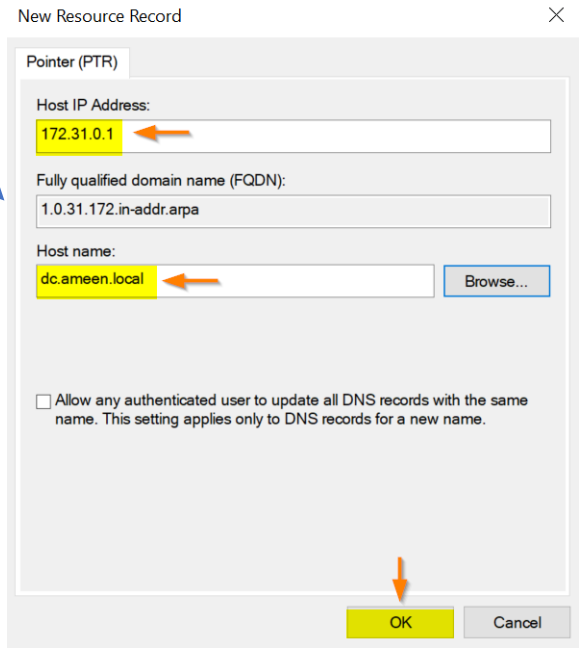



DNS Manager
File Action View Help
DNS
DC
Forward Lookup Zones
Reverse Lookup Zones
0.31.172.in-addr.arpa
Trust Points
Conditional Forwarders
Name
Type
Data
(same as parent folder)
Start of Authority (SOA)
[1], dc.ameen.local., hostma...
(same as parent folder)
Name Server (NS)
dc.ameen.local.
static
Actions
0.31.172.in-add...
More Acti...
Right Click on the background
Update Server Data File
Reload
New Pointer (PTR)...
New Alias (CNAME)...
New Delegation...
Other New Records...
DNSSEC
All Tasks
Refresh
Export List...
View
Arrange Icons
Line up Icons
Properties
Help
Create a new delegated DNS domain.


New Resource Record
Pointer (PTR)
Host IP Address:
172.31.0.
Fully qualified domain name (FQDN):
0.31.172.in-addr.arpa
Host name:
Browse...
Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.
OK
Cancel

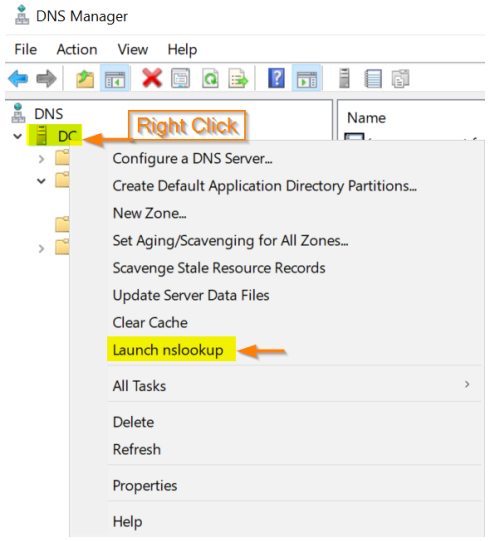

New Resource Record
Browse
Look in:
DNS
Records:
Name
Type
Data
Timestamp
DC
Selection:
DC
Record types:
Hosts (A or AAAA Records)
OK
Cancel
OK
Cancel

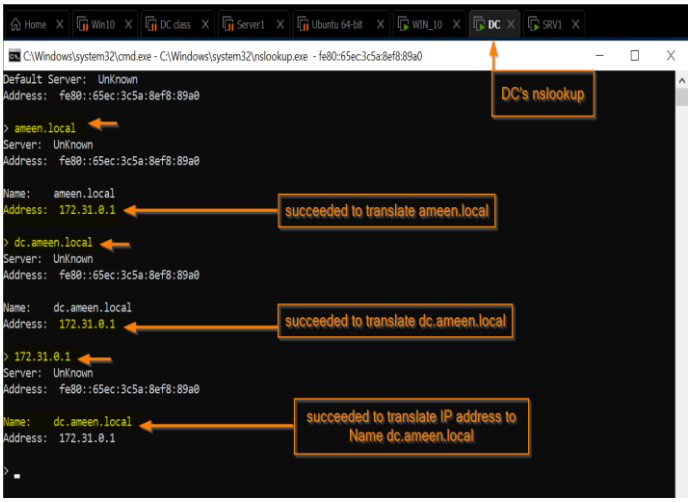




Nslookup check:

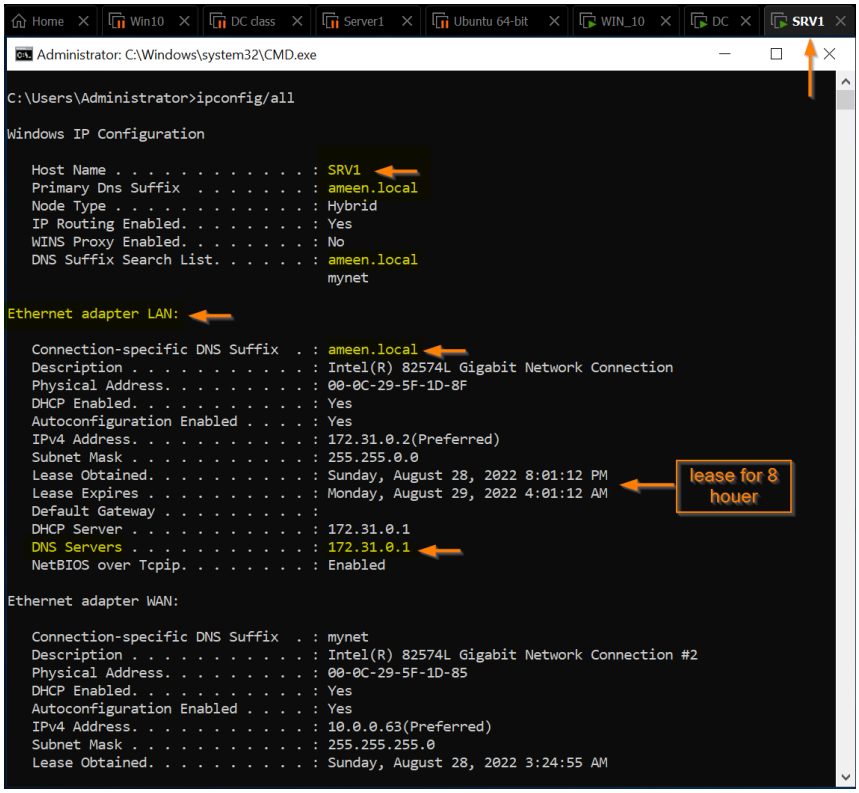
Double check and confirm.

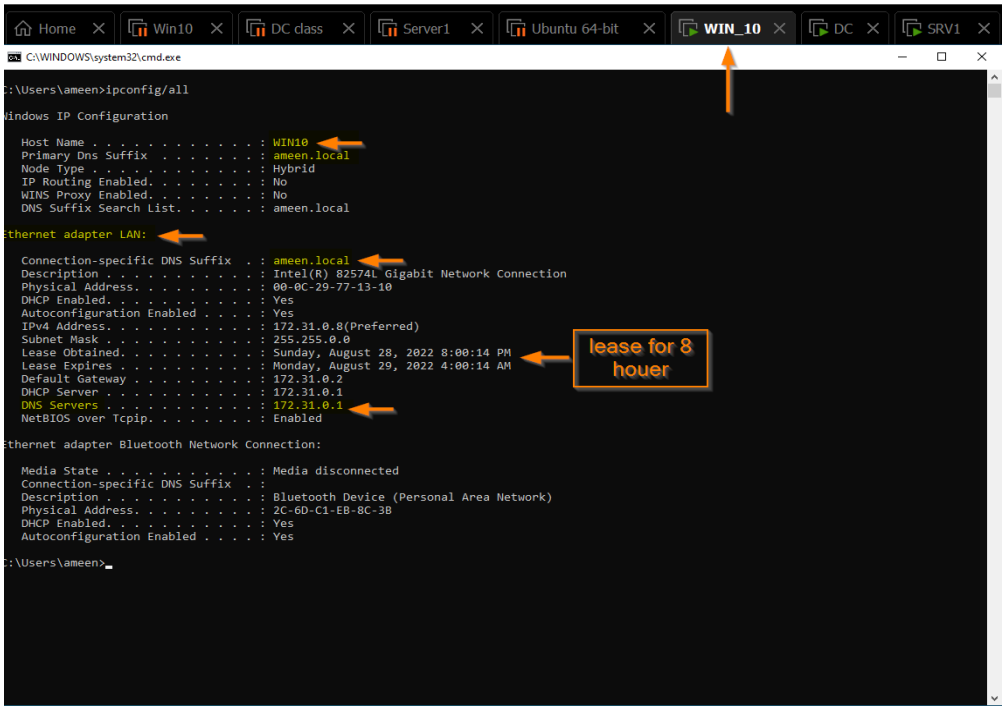




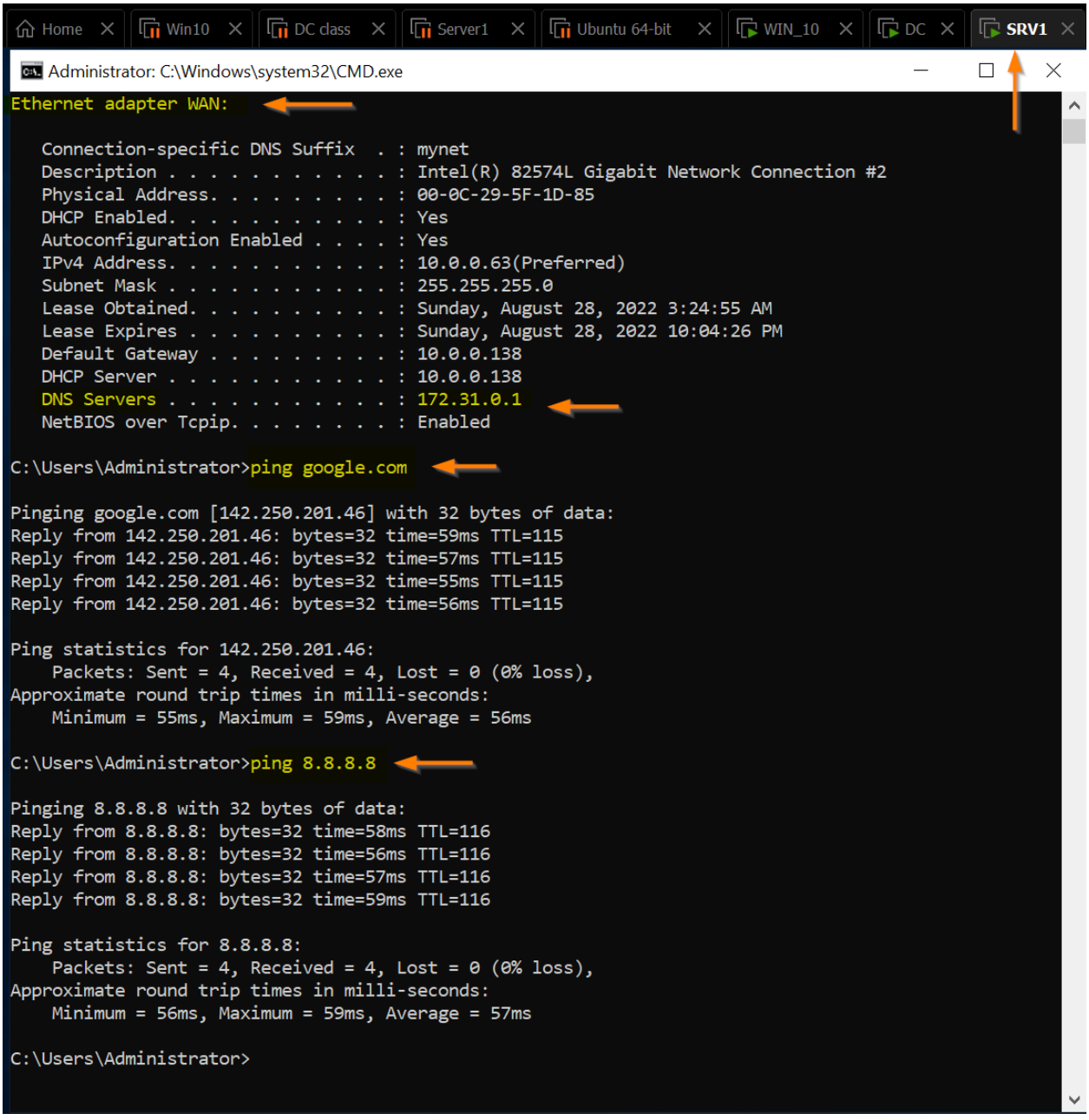
Configuring the DNS

First, I will make sure all the devices are configured to use the DC's DNS.





Manual DNS setting on SRV1's bridged card to use DC's DNS:



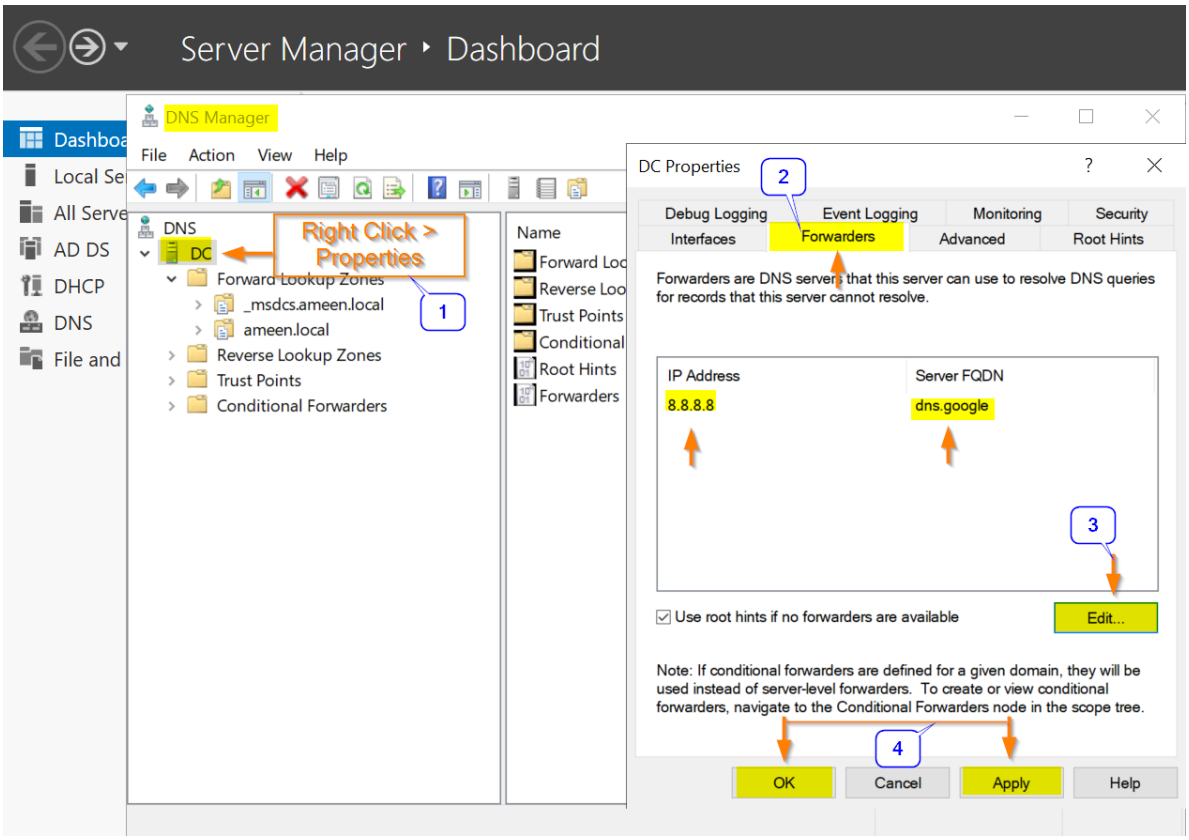
The next step I entered the DNS configuration and the setup was adding DNS Forwarders and Conditional Forwarders.

The forwarders setting allows adding a DNS server that queries will be forwarded, in our case, DNS cannot reply to a query using its own zone and cache.

The Conditional Forwarders queries are available under the condition of a specific domain related.

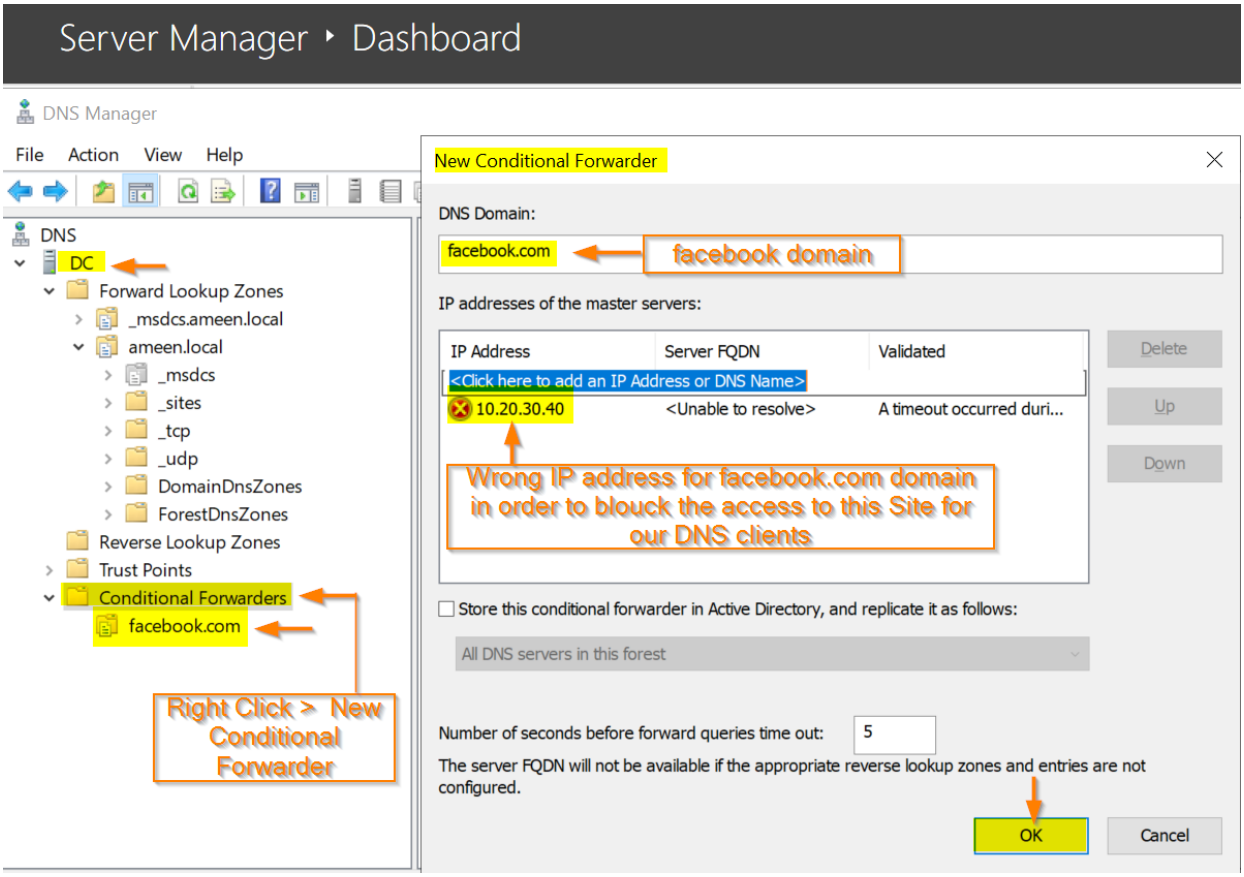
NOW I will add google DNS (8.8.8.8) to the Forwarders of the DC server DNS services through the bath:

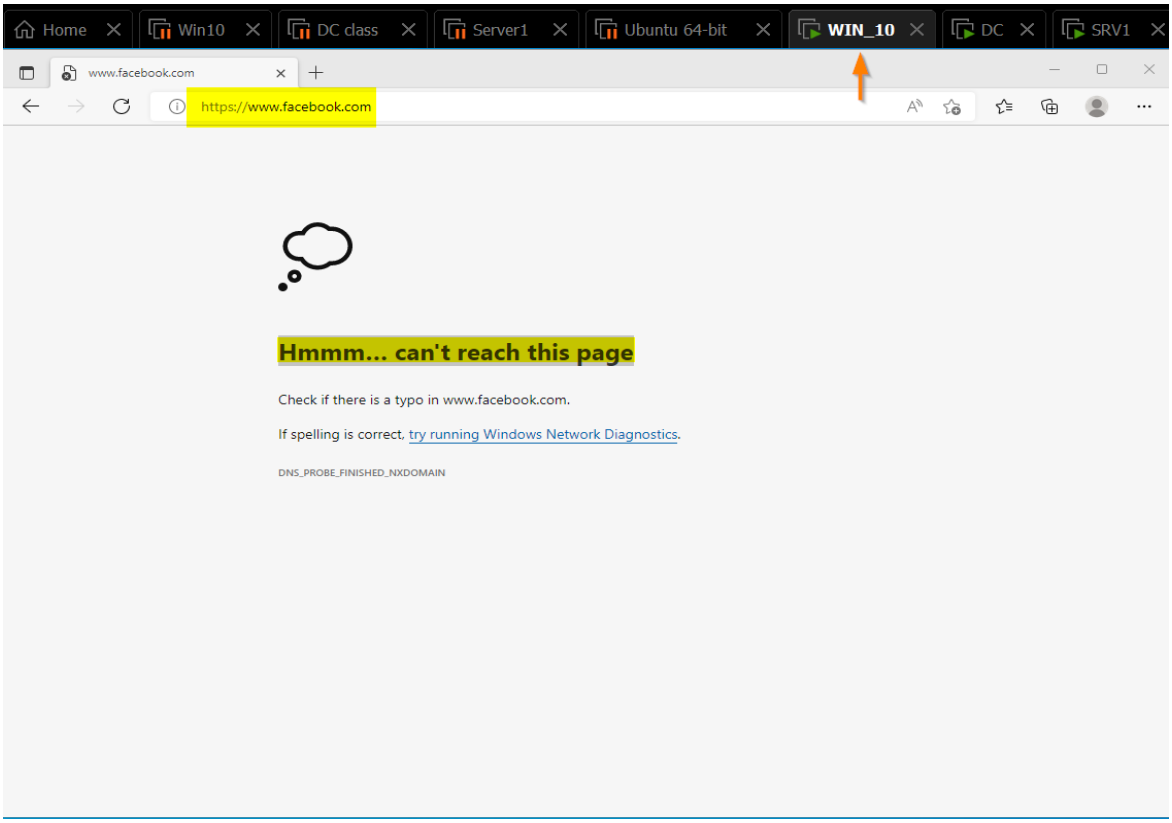
Server Manager >Dashboard > Tools > DNS > DC> Properties > Forwarders.

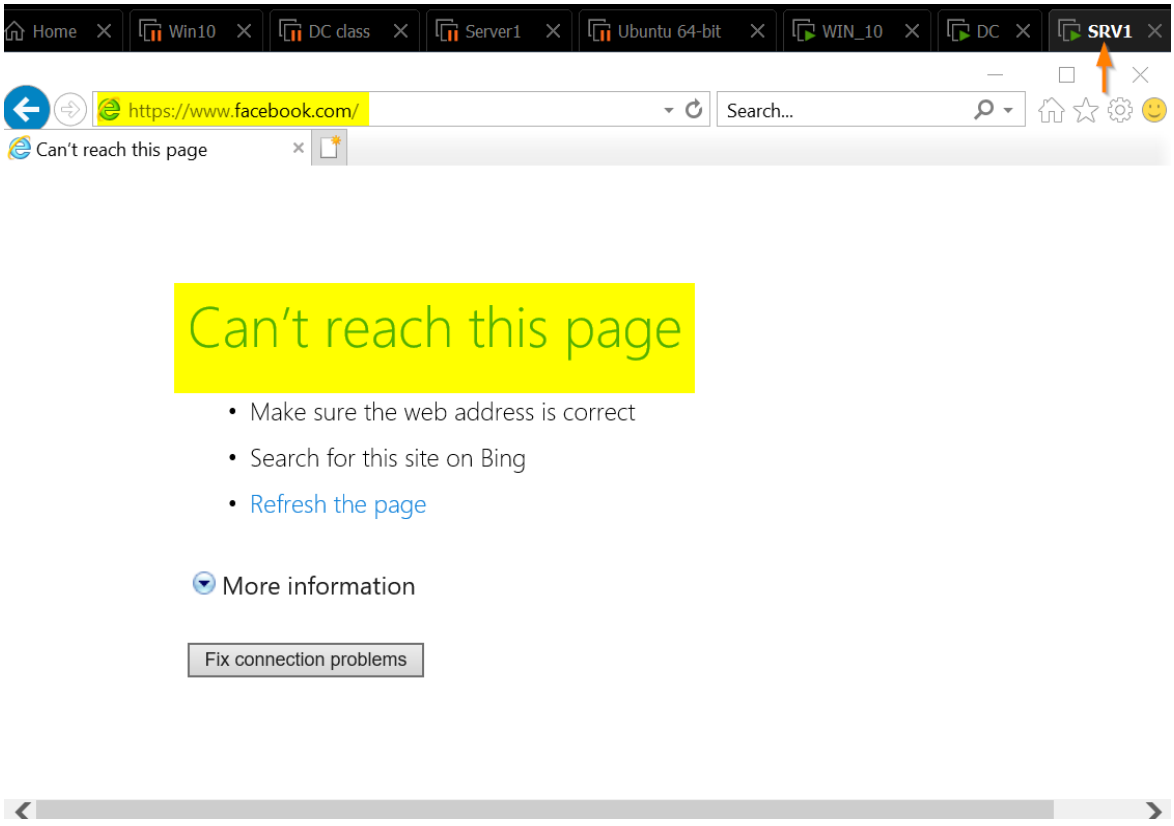


I also added facebook.com as a Conditional Forwarders and set a wrong IP address (10.20.30.40) for the website to block access to Facebook of stations connected to the server. I did so using the bath:

Server Manager >Dashboard > Tools > DNS > Dc > Properties > Conditional Forwarders > New Conditional Forwarder.




Home
Win10
DC class
Server1
Ubuntu 64-bit
WIN_10
DC
SRV1
www.facebook.com
https://www.facebook.com
Hmmm... can't reach this page
Check if there is a typo in www.facebook.com.
If spelling is correct, try running Windows Network Diagnostics.
DNS_PROBE_FINISHED_NXDOMAIN


Home
Win10
DC class
Server1
Ubuntu 64-bit
WIN_10
DC
SRV1
https://www.facebook.com/
Search...
Can't reach this page
Can't reach this page
Make sure the web address is correct
Search for this site on Bing
Refresh the page
More information
Fix connection problems

The DNS configuration options includes creating a new zone, the options of zones include:

1. Primary zone:

   A Primary (Master) DNS zone is the original Read-Write Authoritative DNS zone of portion of a DNS Namespace.

   The ZONE is stored in AD DS or on a hard disk inside the file:

   %systemroot%\system32\dns\zone_name.dns

2. Secondary zone:

   A read only(Slave); copy of another Primary/Secondary zone. The secondary zone cannot process updates and can only retrieve updates from the primary zone.

   Its purpose is to serve as an additional zone i
   n an attempt to improve response times (distribution of loads).

   The synchronization process between the servers is called Zone Transfer.

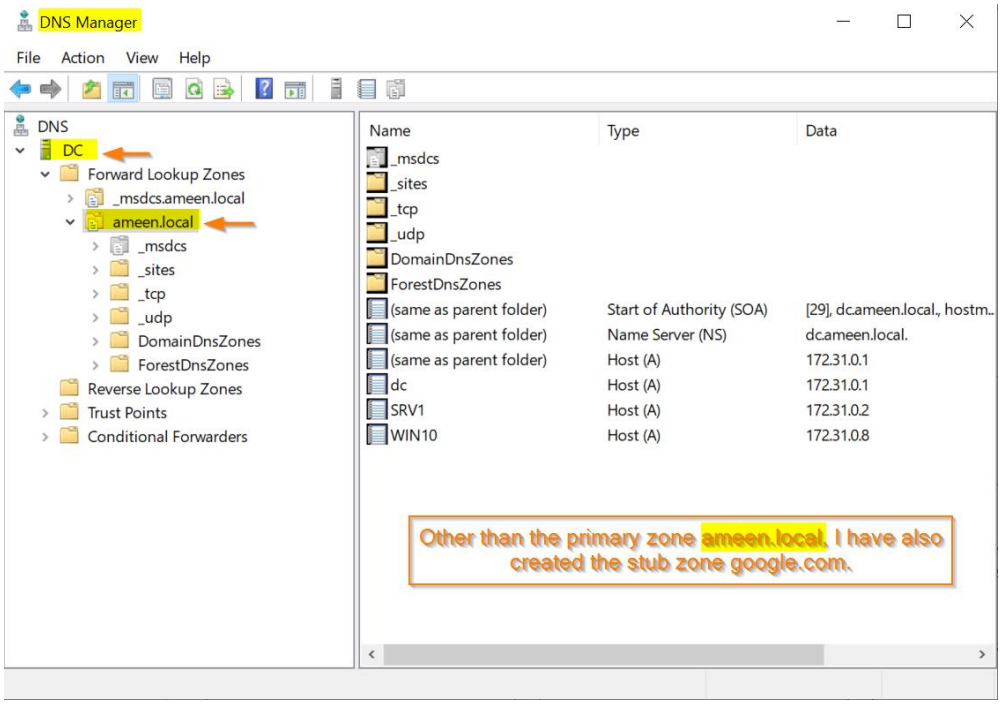
3. Stub zone:

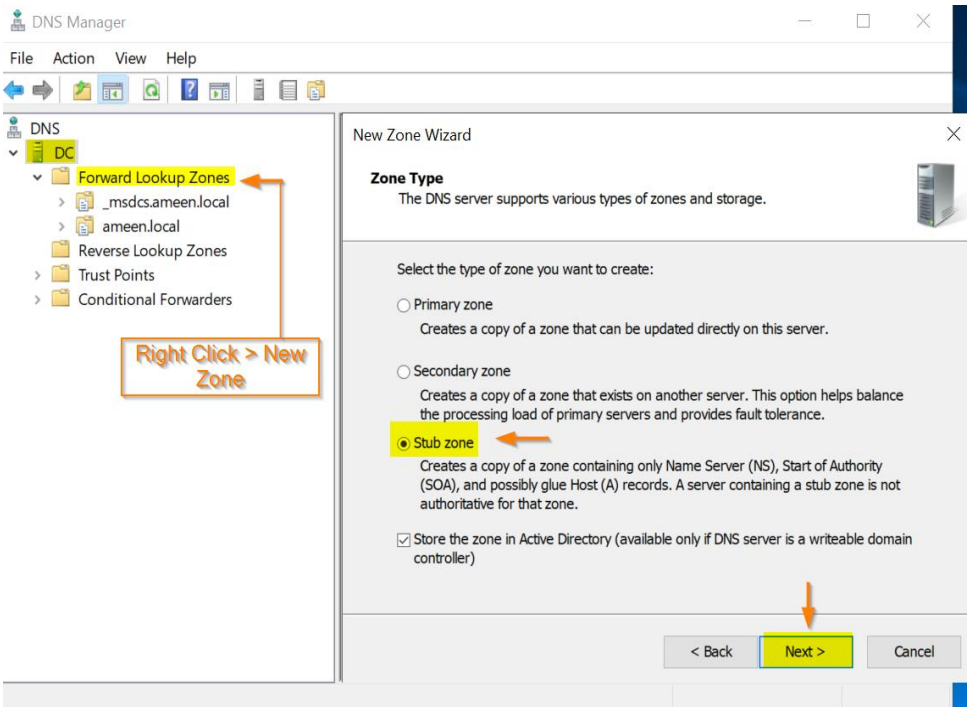
   DNS stub zones are used to enable your DNS servers to resolve records in another domain. The information in the stub zone allows your DNS to contact the authoritative DNS server directly. This does sound a bit like conditional forwarding, and actually, it is!

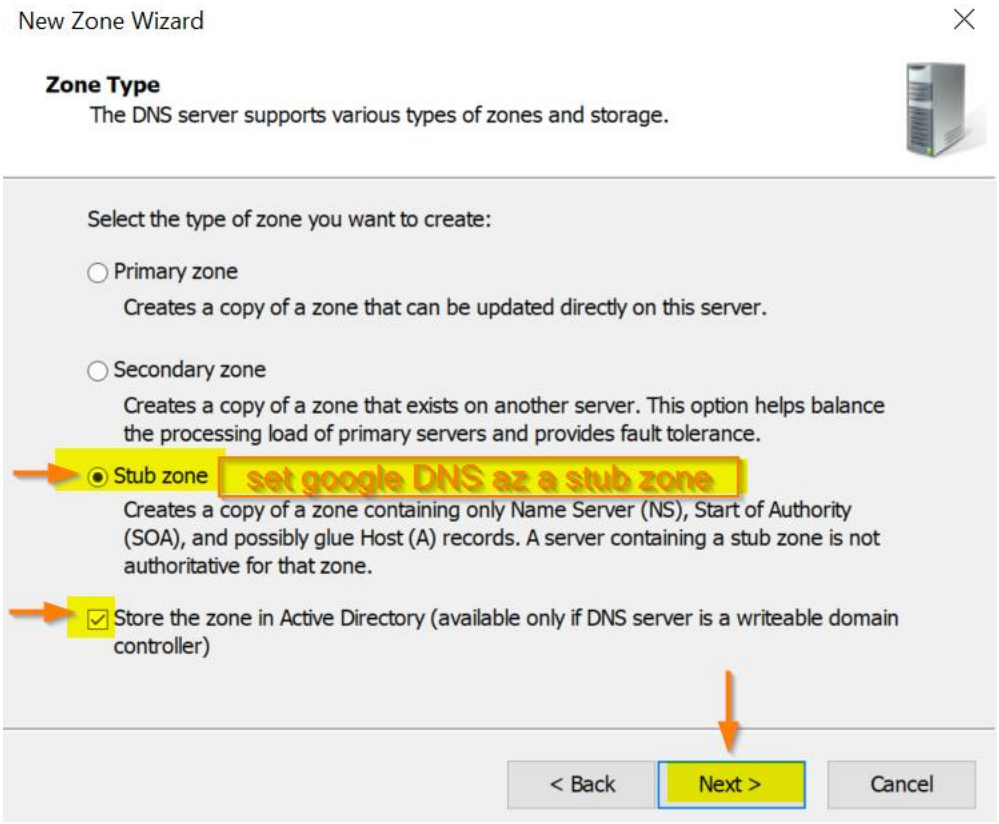
   It only keeps the NS and SOA records of the primary zone and cannot reply to DNS queries.

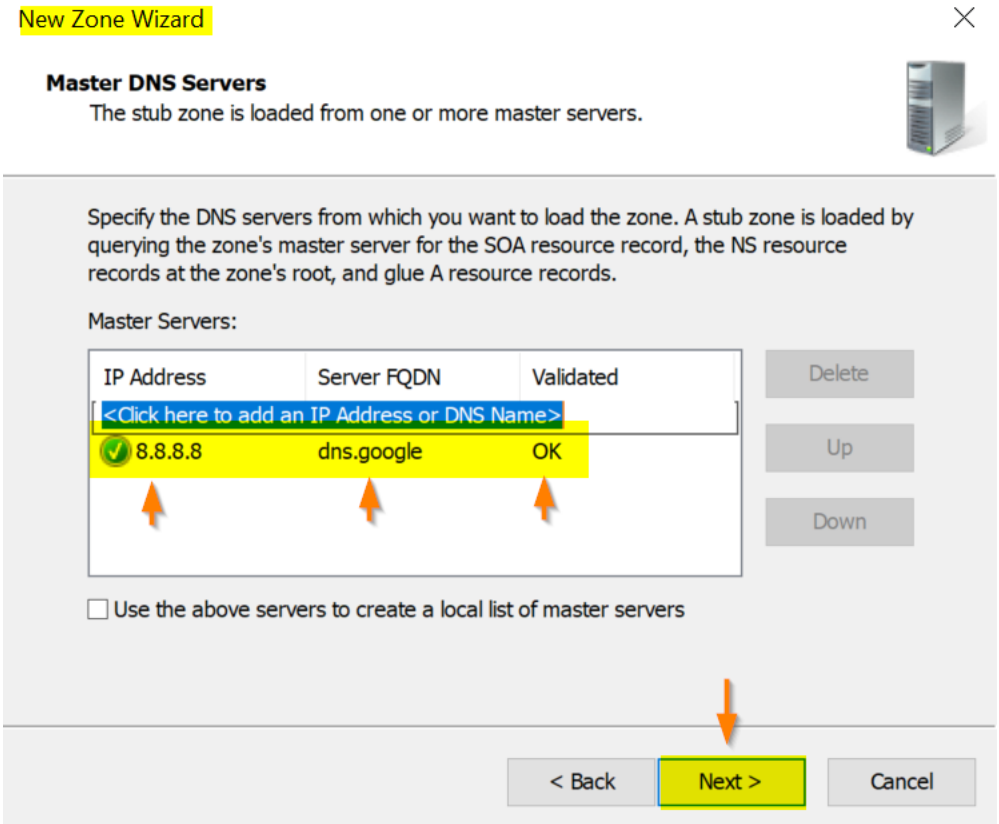
To create a new Stub zone, I accessed the path:

Server Manager >Dashboard > Tools > DNS > DC> New Zone.

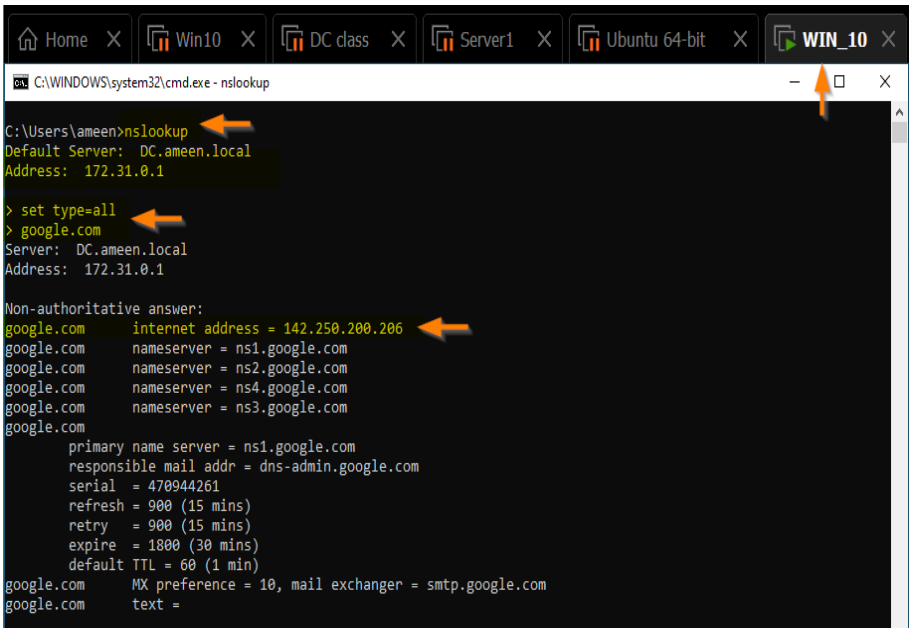


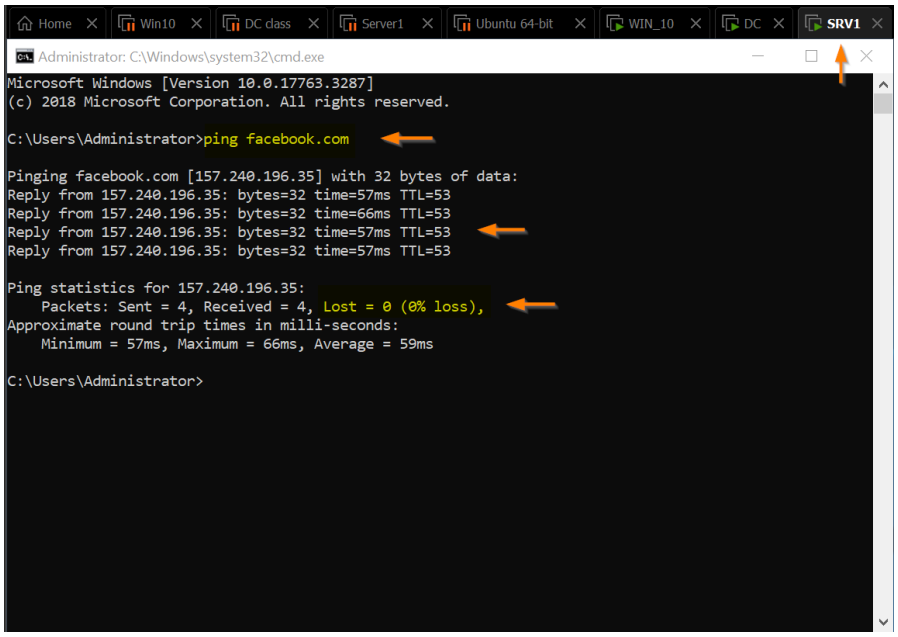



New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
set google DNS az a stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next >
Cancel


New Zone Wizard
Master DNS Servers
The stub zone is loaded from one or more master servers.
Specify the DNS servers from which you want to load the zone. A stub zone is loaded by querying the zone's master server for the SOA resource record, the NS resource records at the zone's root, and glue A resource records.
Master Servers:
IP Address
Server FQDN
Validated
<Click here to add an IP Address or DNS Name>
8.8.8.8
dns.google
OK
Delete
Up
Down
Use the above servers to create a local list of master servers
< Back
Next >
Cancel

Now I made sure that WIN10 nslookup command succeeded to translate www.google.com', and have performed a ping to www.facebook.com from SRV1.





Sharing and Mapping Features

ONE of the features in the AD DC services are the sharing of folders and files and the mapping of those as drives on stations connected to the domain.

The ability to share folders allows to increase the efficiency and structuring of the organization's data storage and usage methods.

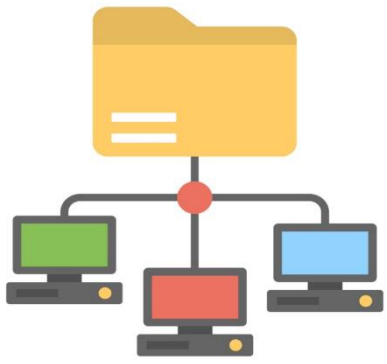
It's also one of the features that allow the network administrator to improve the accessibility and convenience of the most various types of users while maintaining the needed security and management levels.

there are only 3 sharing permissions available and 6 different security permission types:

Read, Change and Full control for the sharing permission.

And;

Full control, Modify, Read & execute, List folder contents, Read, Write and Special permissions.



Creating a "Home Folder" for all Users

Also called home directory, a user's private folder for storing personal files. Home folders for users are usually centrally located on a network server for the following reasons[15]:

- To ensure that their contents are backed up regularly.
- To make home folders available from any computer on the network.
- To make home folders available from any client operating system.

To specify a network path for the home folder, we must first create the network share and set permissions that permit the user access. we can do this with Shared Folders in Computer Management on the server computer, DC in our case.

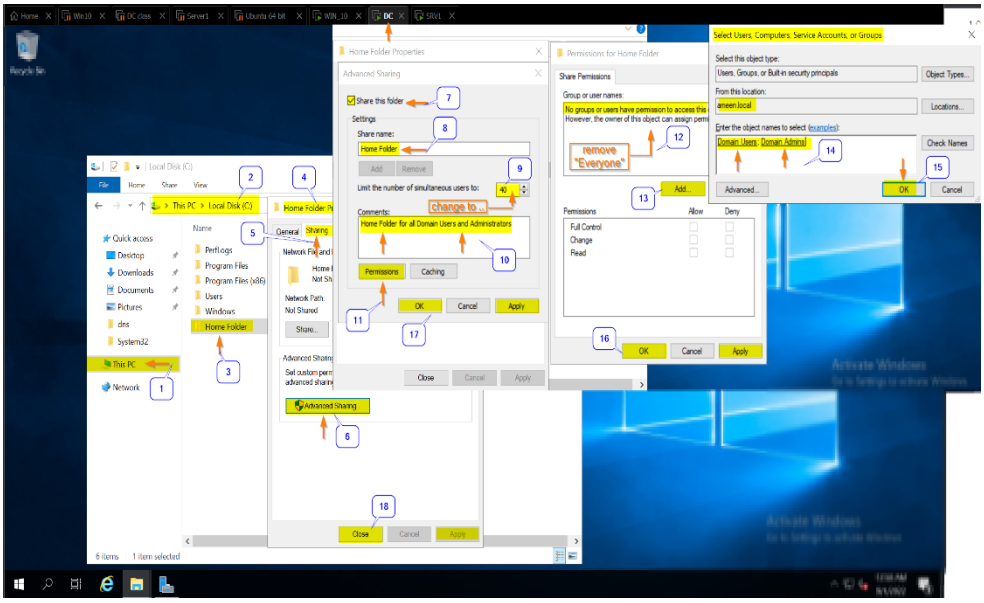
In order to create a home folder for all users-user1-4, I will create the folder "Home Folder" on the DC server which I shared to all domain users:

File Explorer > This PC > Local Disk (c) > New > Folder > named "Home Folder".

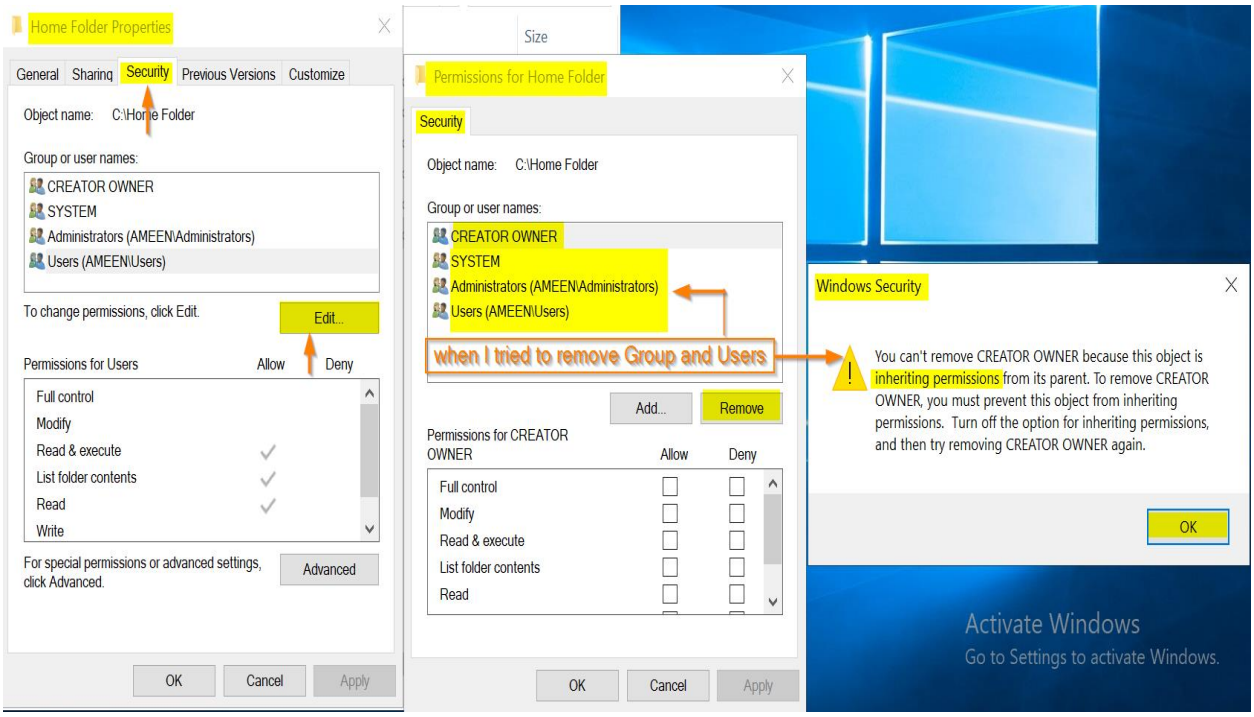
I then shared it through:

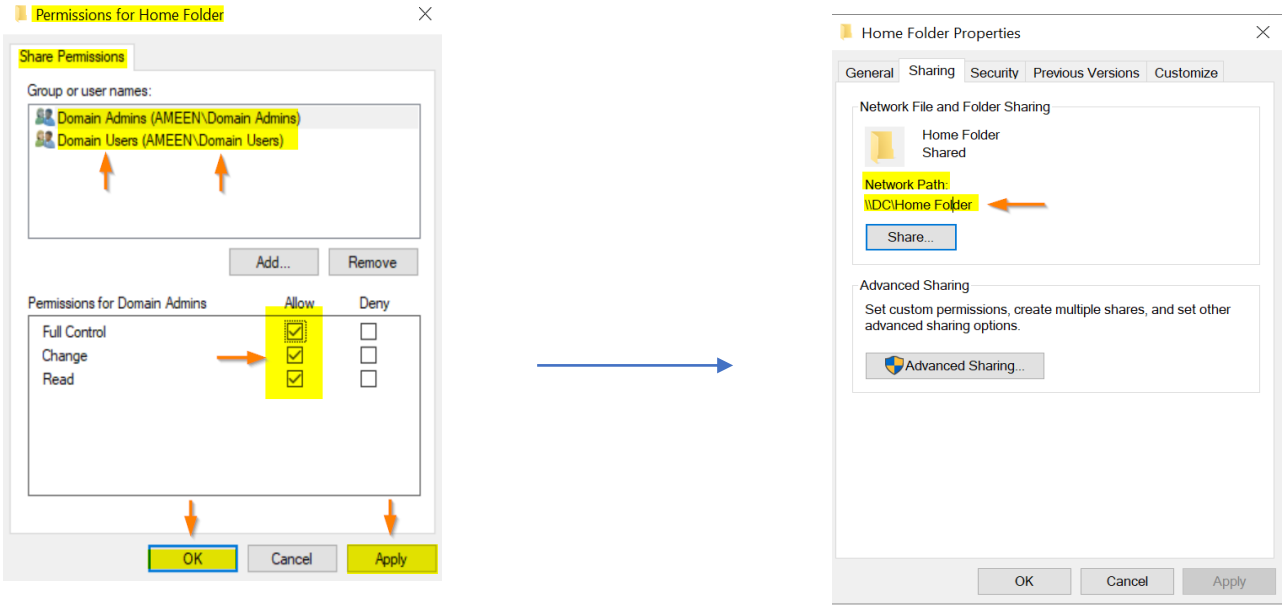
Home Folder > Properties > Sharing > Advanced Sharing.

[15] https://networkencyclopedia.com/home-folder/

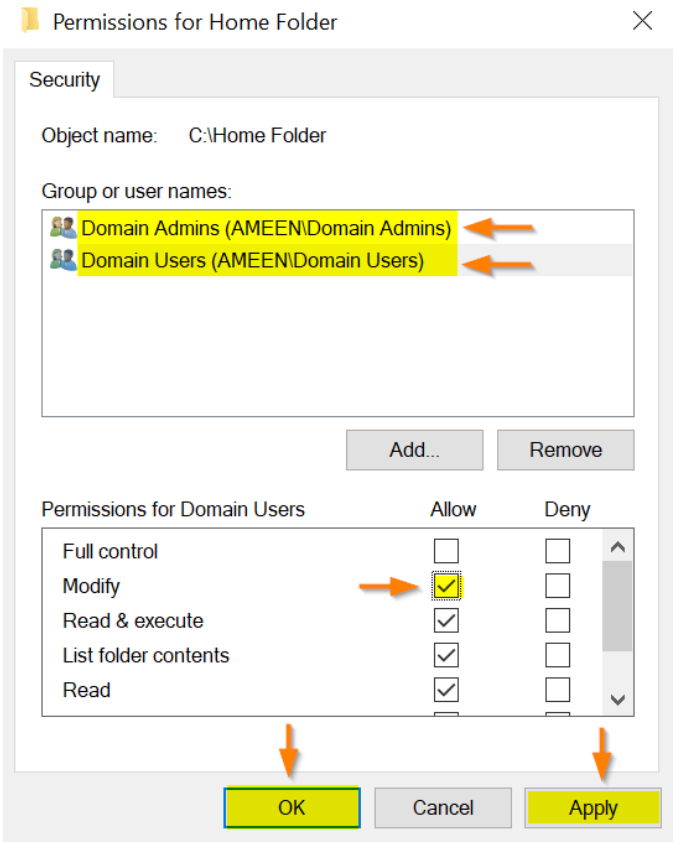


I checked the box “Share this folder” and edited the sharing permissions to allow access to the domain users and administrators.

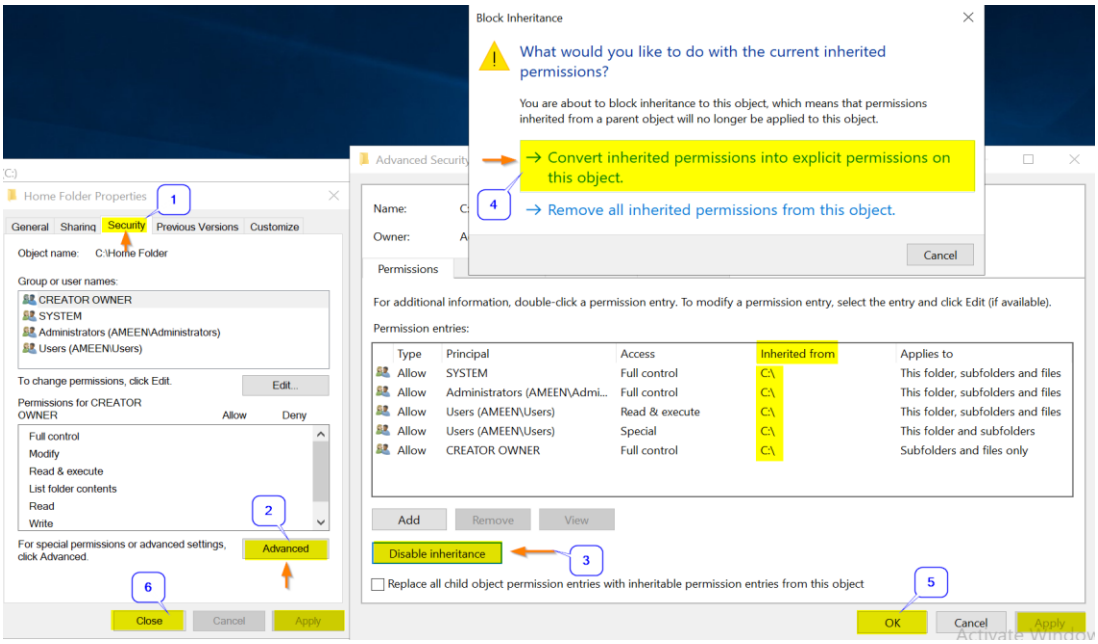


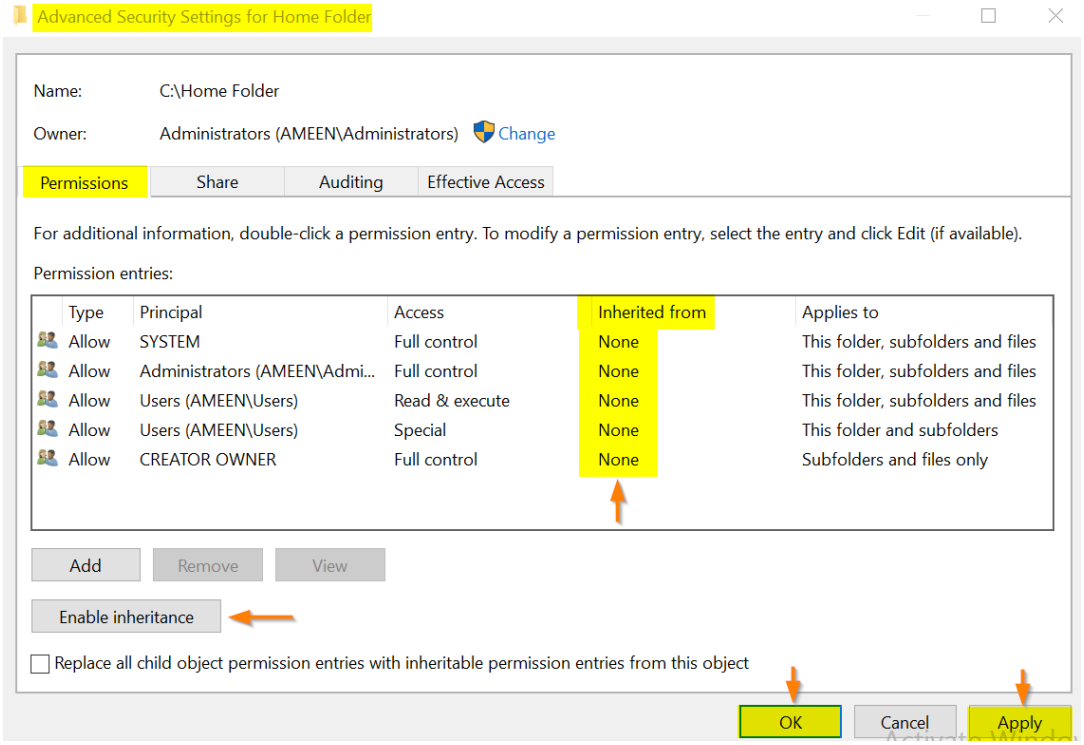


I also set the security permissions to match the "Home Folder" permissions:



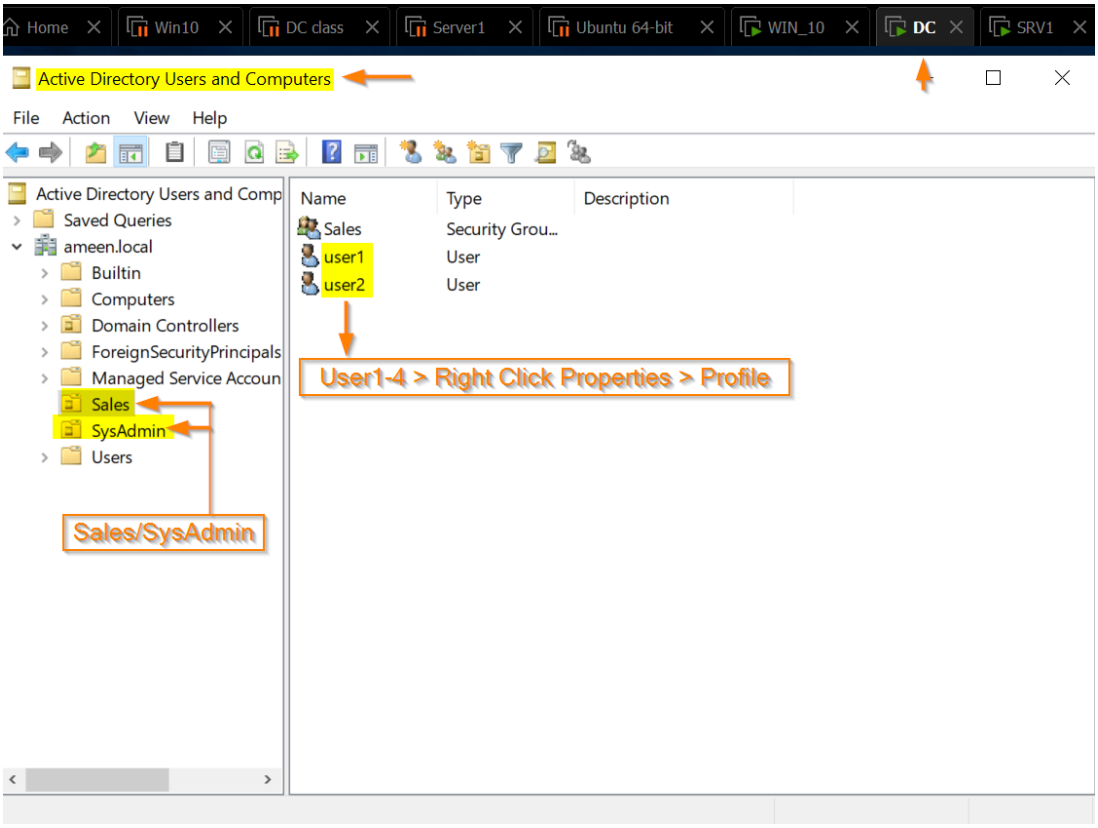
Disable Inheriting Permissions

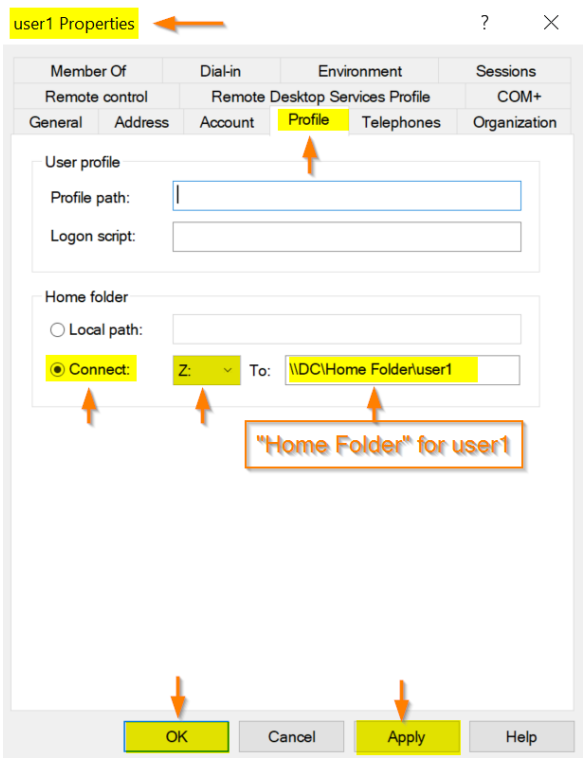


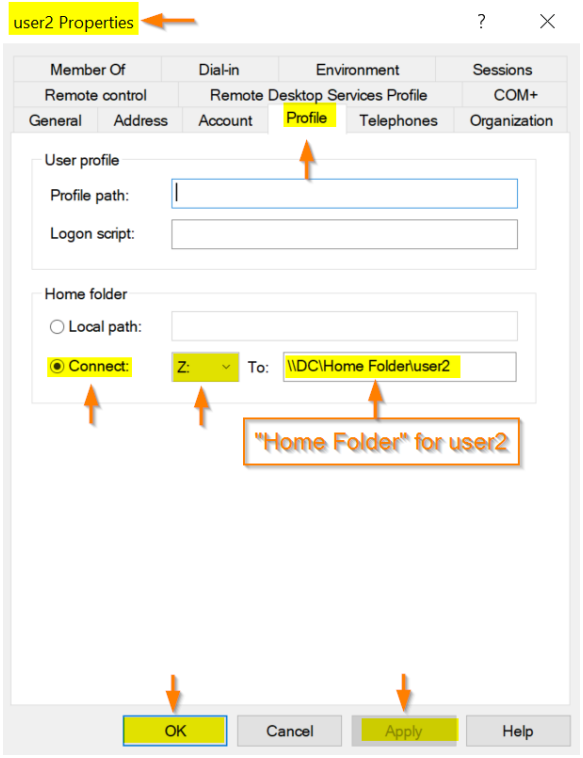


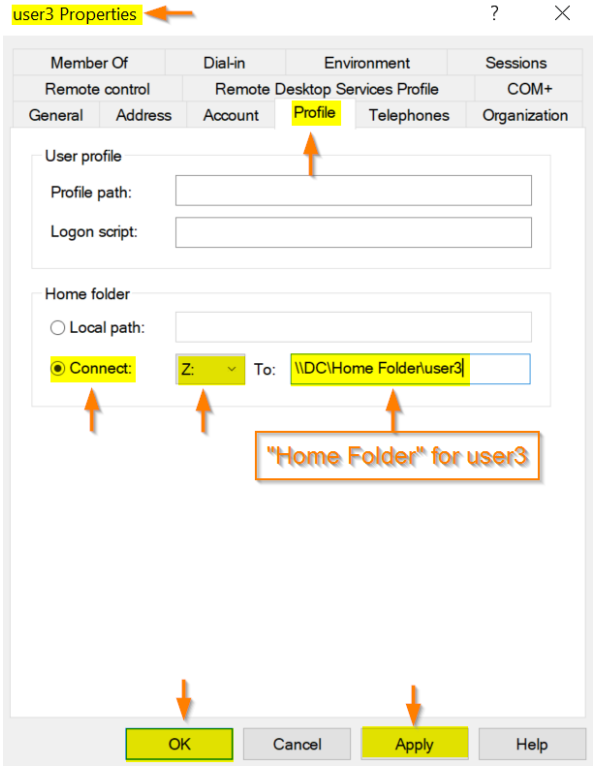
And then I accessed the AD Users and Computers Manager, and used each users profile settings to create a home folder for the user:

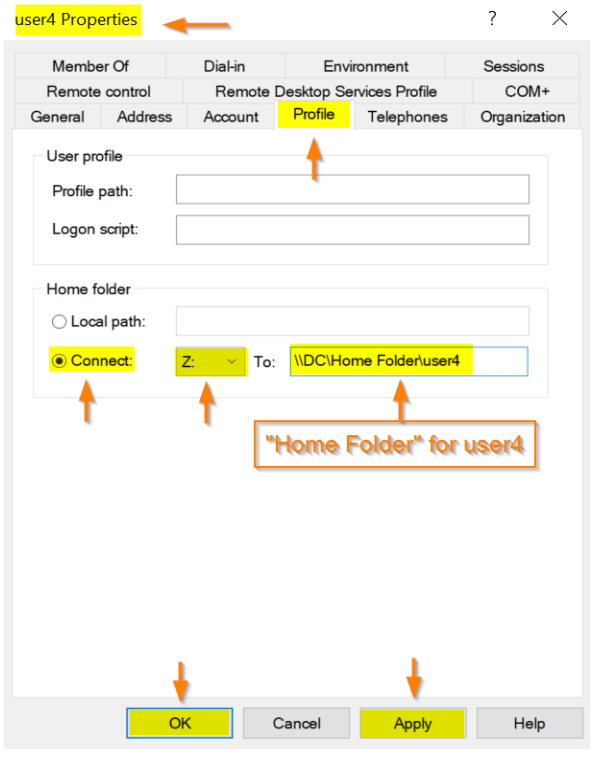
Server Manager >Dashboard > Tools > Active Directory Users and Computers > Sales/SysAdmin > user (1-4) > Properties > Profile > Home folder > Connect to: \\DC\Home Folder\user (1-4).




user1 Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
User profile
Profile path:
Logon script:
Home folder
Local path:
Connect:
Z:
To:
\\DC\Home Folder\user1
"Home Folder" for user1
OK
Cancel
Apply
Help

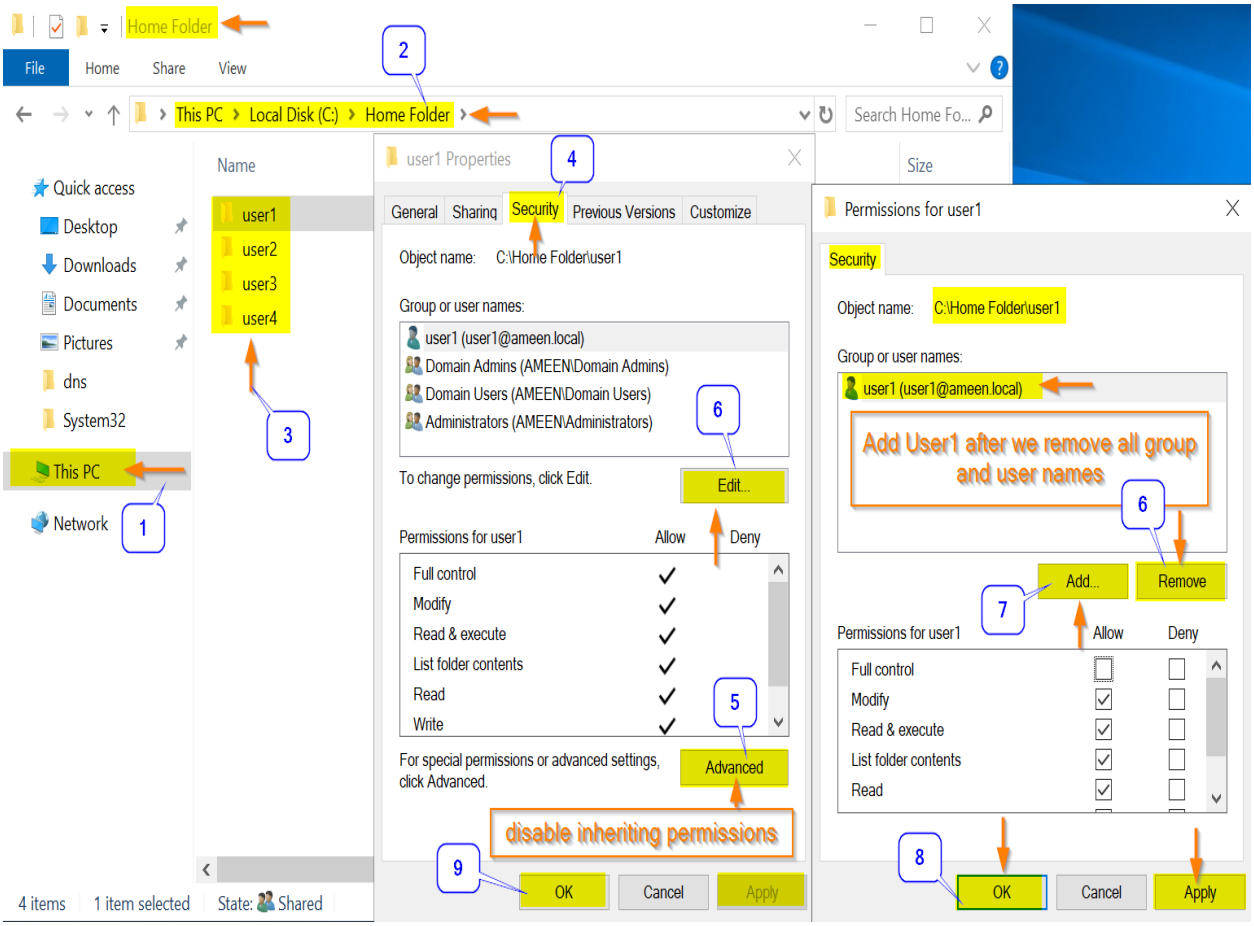

user2 Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
User profile
Profile path:
Logon script:
Home folder
Local path:
Connect:
Z:
To:
\\DC\Home Folder\user2
"Home Folder" for user2
OK
Cancel
Apply
Help


user3 Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
User profile
Profile path:
Logon script:
Home folder
Local path:
Connect:
Z:
To:
\\DC\Home Folder\user3
"Home Folder" for user3
OK
Cancel
Apply
Help


user4 Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
User profile
Profile path:
Logon script:
Home folder
Local path:
Connect:
Z:
To:
\\DC\Home Folder\user4
"Home Folder" for user4
OK
Cancel
Apply
Help

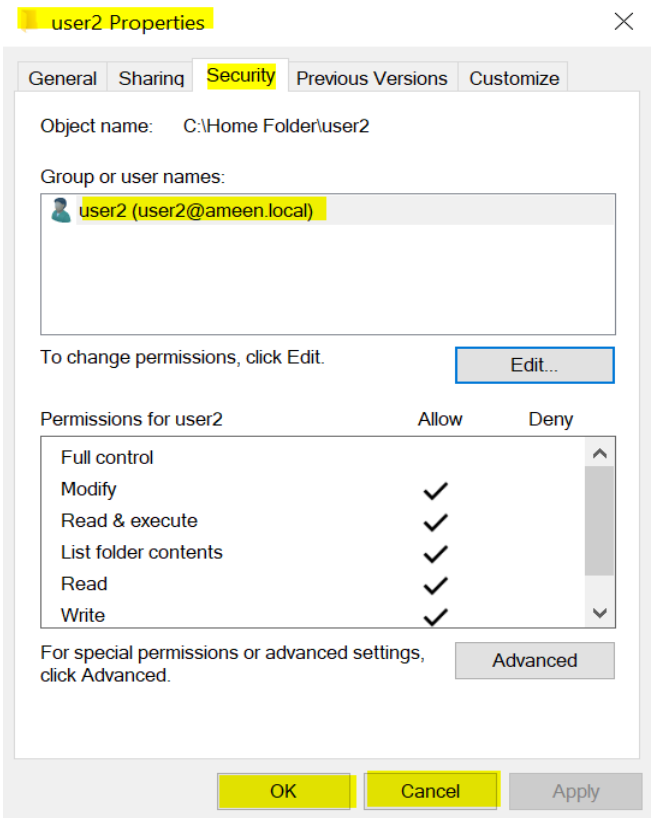
Further, I managed the security permissions to assure every user could only access his own folder:

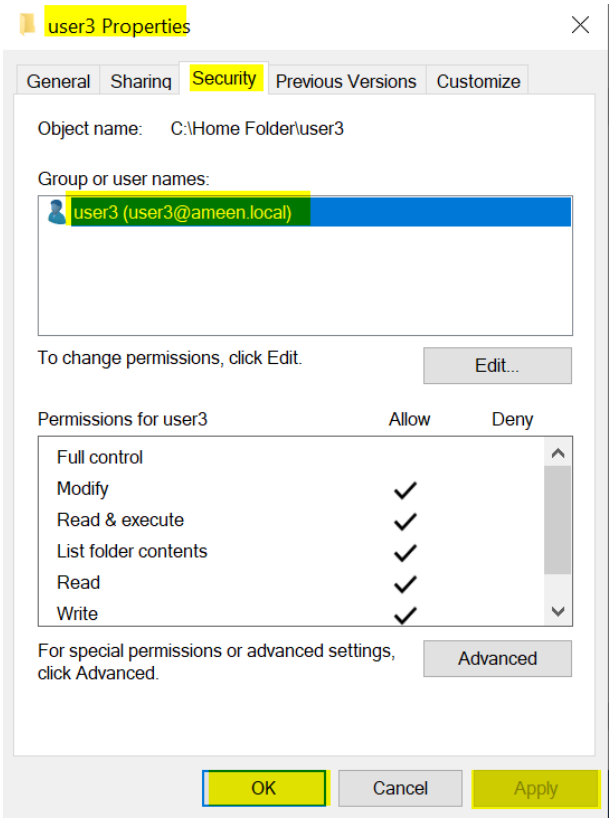
DC > File Explorer > This PC > Local Disk (c) > Home Folder > User1 > Properties > Security.

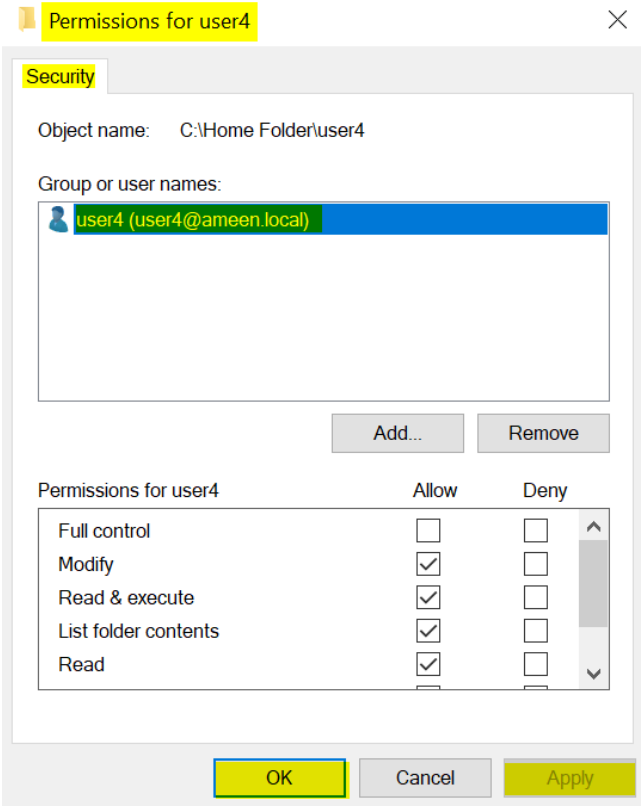


I repeated the same process for all users[16];

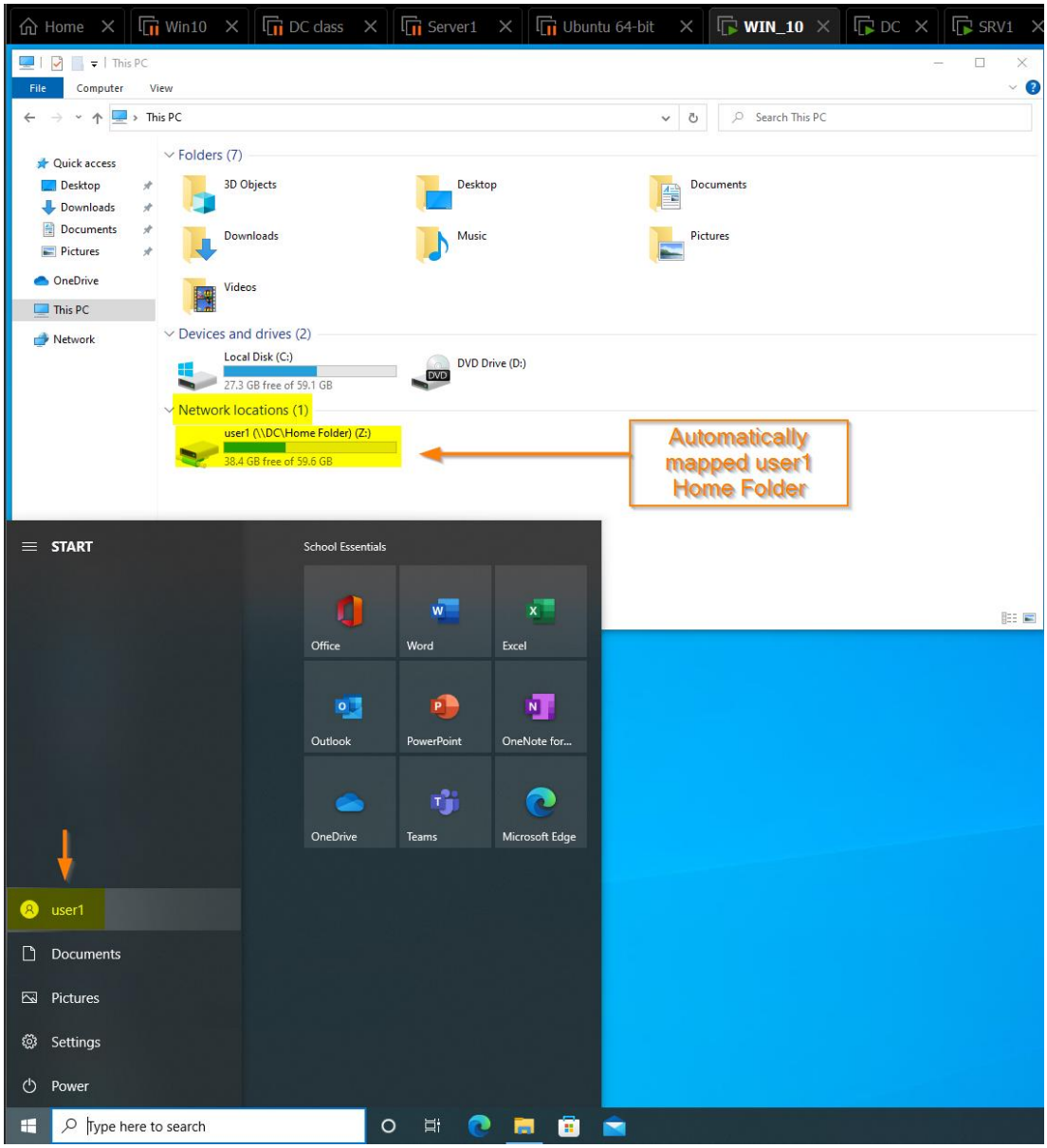
[16] See the Next page here.

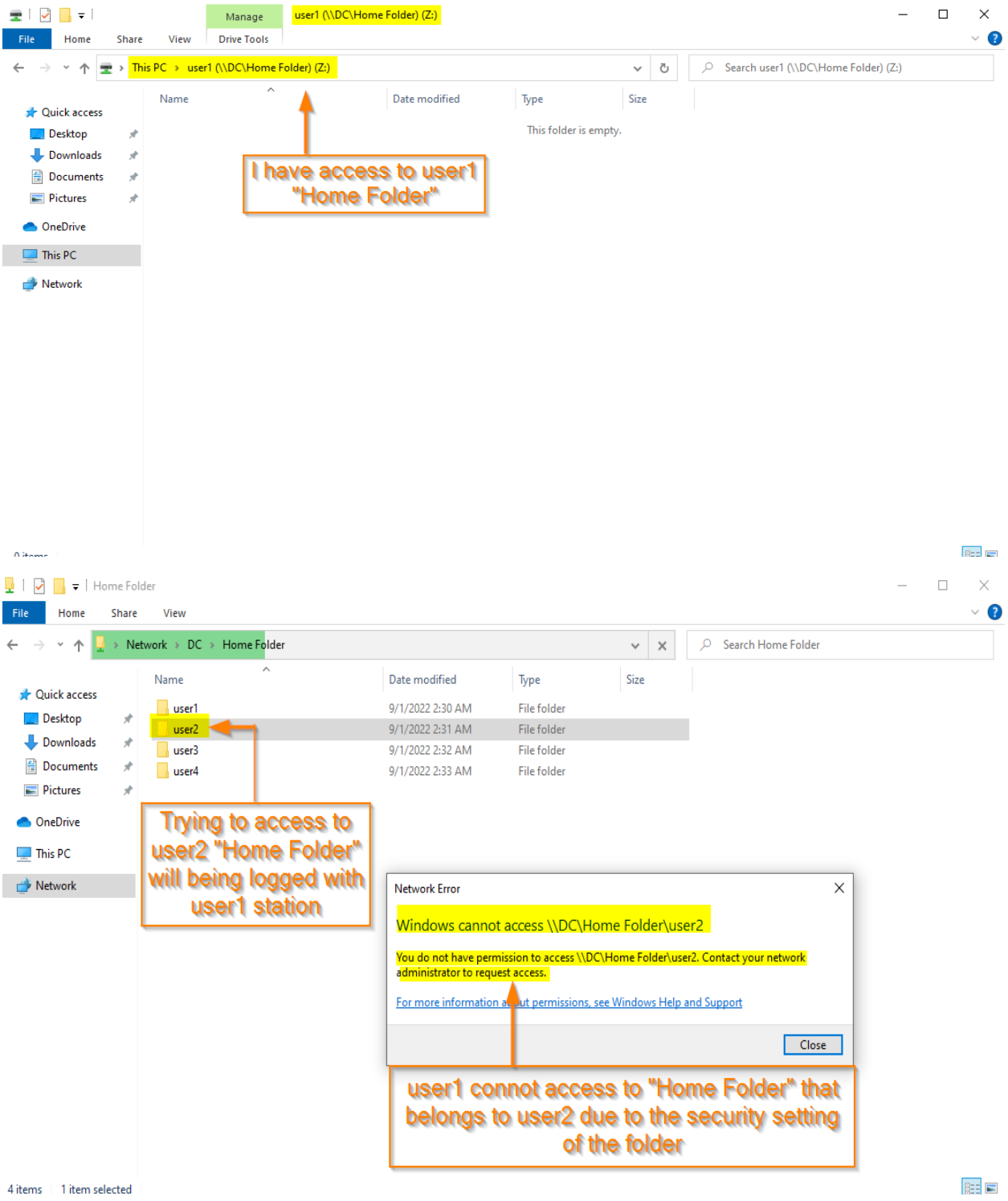

user2 Properties
General
Sharing
Security
Previous Versions
Customize
Object name: C:\Home Folder\user2
Group or user names:
user2 (user2@ameen.local)
To change permissions, click Edit.
Edit...
Permissions for user2
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply


user3 Properties
General
Sharing
Security
Previous Versions
Customize
Object name: C:\Home Folder\user3
Group or user names:
user3 (user3@ameen.local)
To change permissions, click Edit.
Edit...
Permissions for user3
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply


Permissions for user4
Security
Object name: C:\Home Folder\user4
Group or user names:
user4 (user4@ameen.local)
Add...
Remove
Permissions for user4
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
OK
Cancel
Apply

In order to make sure each user could only access his own “Home Folder”. I’ve checked that each of the user’s “Home Folder” is mapped as a drive when logging into the user and that the users can’t access each other’s “Home Folder”. As we can see in the attached screenshots below;




Manage
user1 (\\DC\Home Folder) (Z:)
File
Home
Share
View
Drive Tools
This PC › user1 (\\DC\Home Folder) (Z:)
Search user1 (\\DC\Home Folder) (Z:)
Quick access
Desktop
Downloads
Documents
Pictures
OneDrive
This PC
Network
Name
Date modified
Type
Size
This folder is empty.
I have access to user1 "Home Folder"
Home Folder
File
Home
Share
View
Network › DC › Home Folder
Search Home Folder
Quick access
Desktop
Downloads
Documents
Pictures
OneDrive
This PC
Network
Name
Date modified
Type
Size
user1
9/1/2022 2:30 AM
File folder
user2
9/1/2022 2:31 AM
File folder
user3
9/1/2022 2:32 AM
File folder
user4
9/1/2022 2:33 AM
File folder
Trying to access to user2 "Home Folder" will being logged with user1 station
Network Error
Windows cannot access \\DC\Home Folder\user2
You do not have permission to access \\DC\Home Folder\user2. Contact your network administrator to request access.
For more information about permissions, see Windows Help and Support
Close
user1 connot access to "Home Folder" that belongs to user2 due to the security setting of the folder
4 items
1 item selected

Creating the Shared Folder DATA on DC

Using the same process as it shown in the previous title, I constructed a new shared folder called “DATA” on the DC server.

I created the shared folder through:

File Explorer > This PC > Local Disk (C) > New > Folder > named “DATA”.

and then shared it through:

DATA > Properties > Sharing > Advanced Sharing;

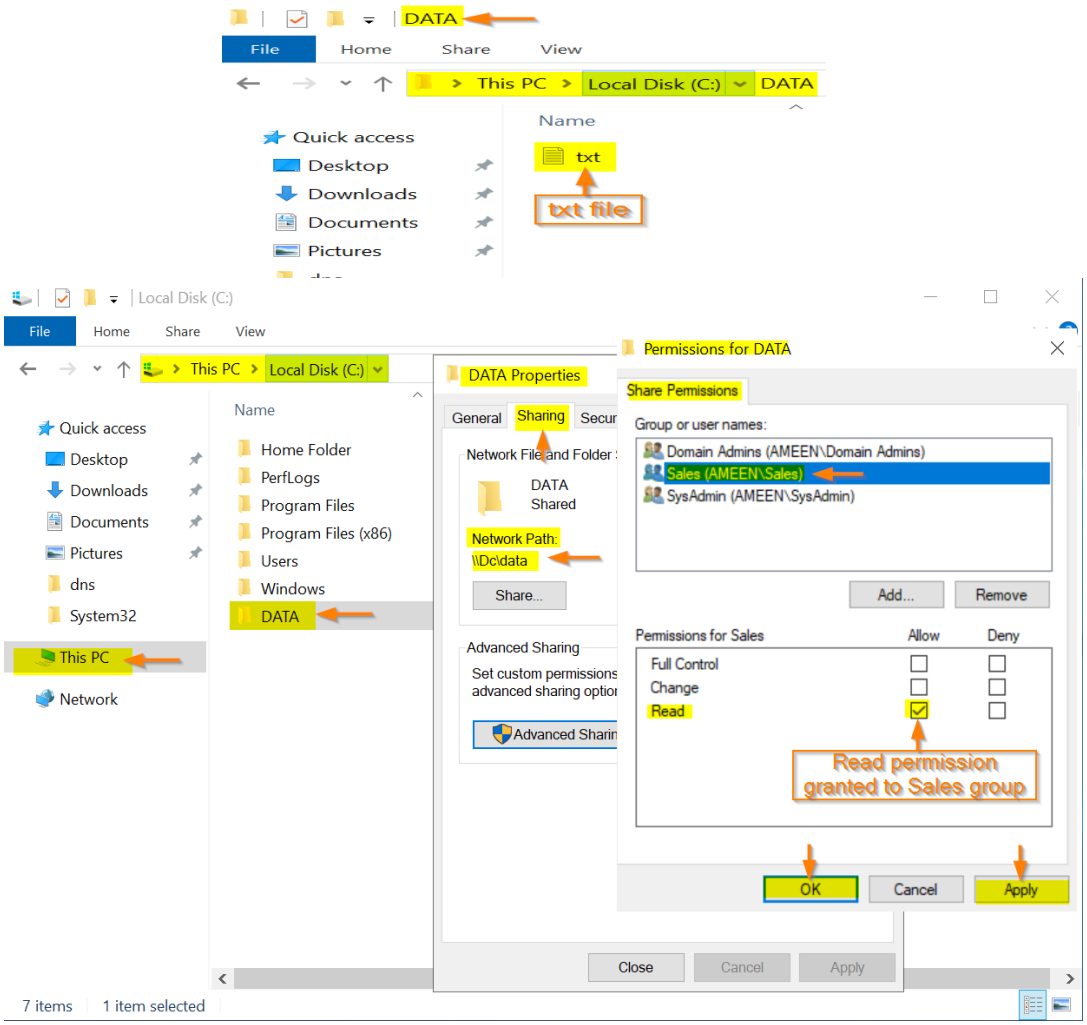
with checking the box **“Share this folder”** and edited the sharing and security permissions of the folder.

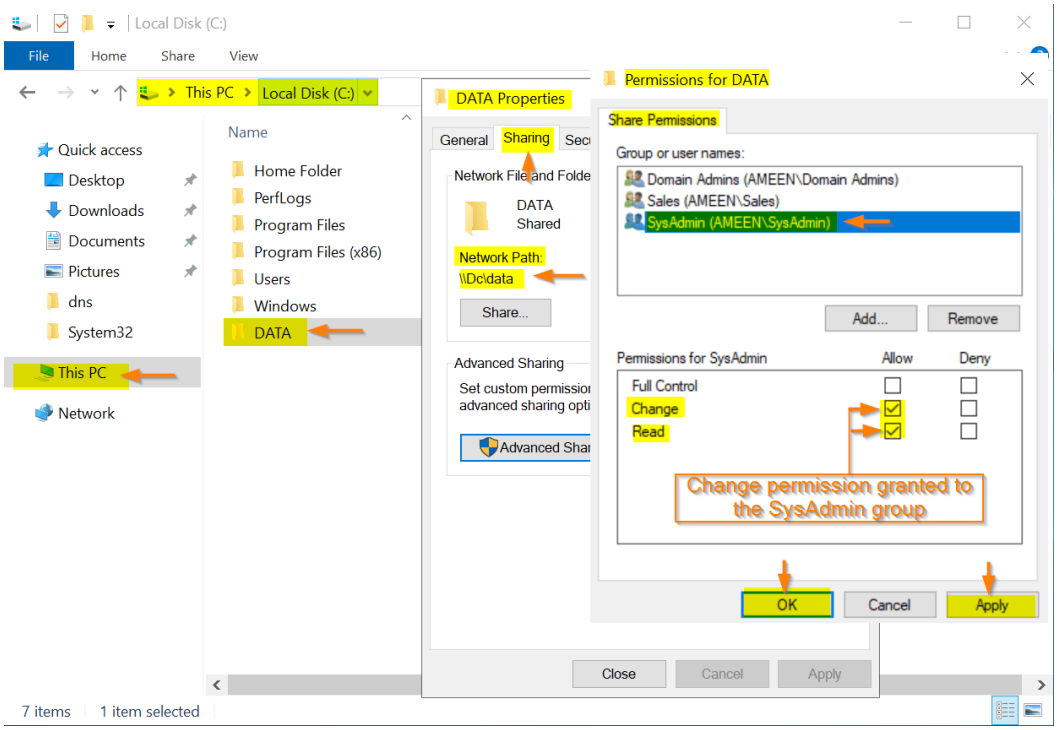
I gave the “SysAdmins” group with the “Modify” security permission and the Change sharing permission.

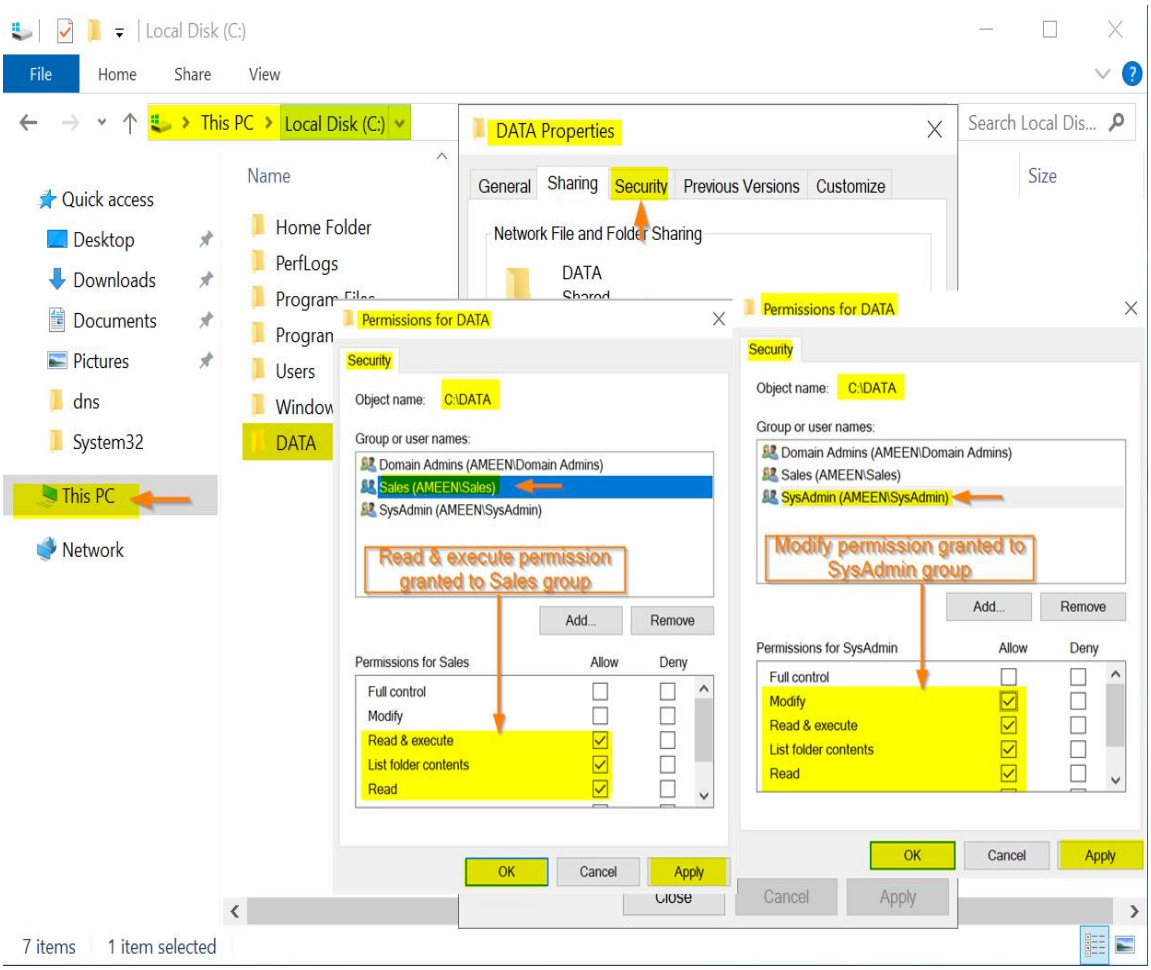
And;

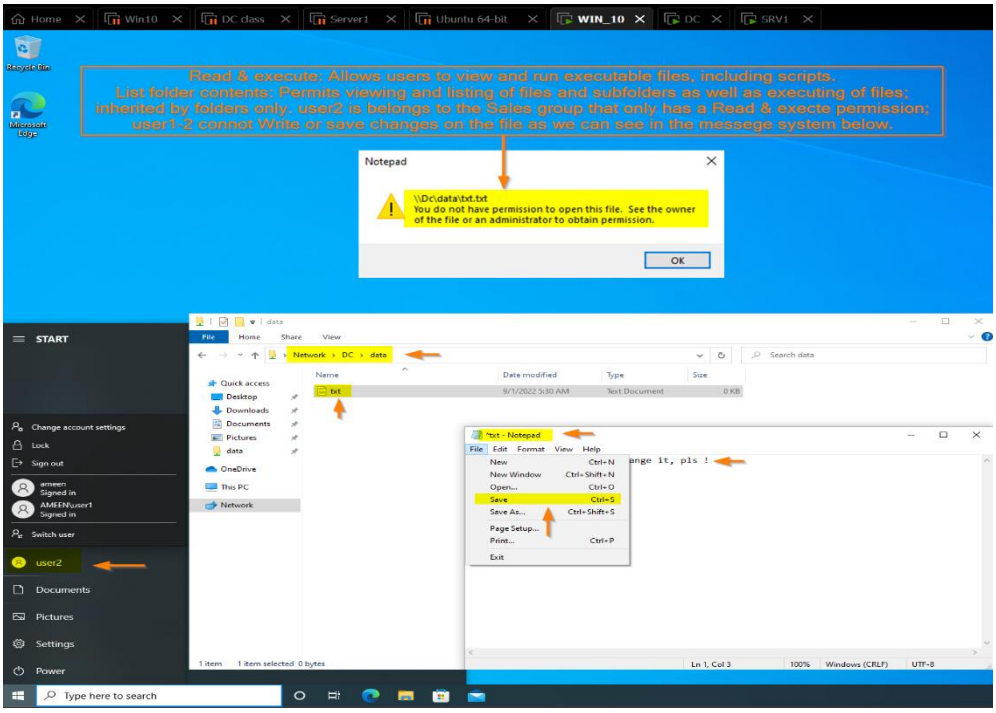
The “Sales” group with the “Read & Execute” security permission and the Read sharing permission.

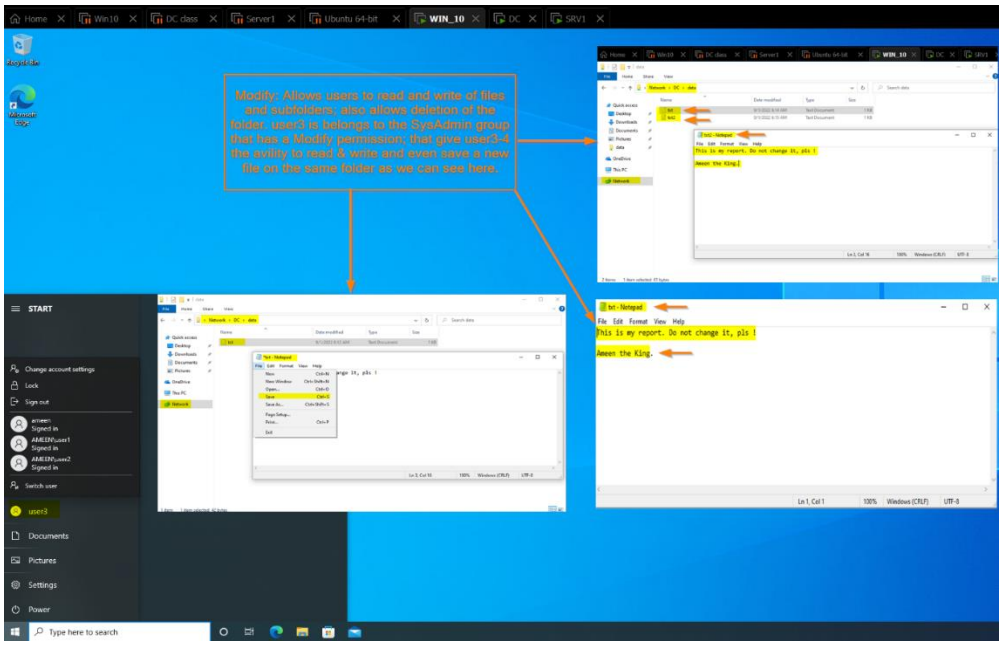
I also added a “txt” file to the “DATA” folder.


DATA
File
Home
Share
View
This PC
Local Disk (C:)
DATA
Quick access
Desktop
Downloads
Documents
Pictures
Name
txt
txt file
Local Disk (C:)
Home Folder
PerfLogs
Program Files
Program Files (x86)
Users
Windows
dns
System32
Network
DATA Properties
General
Sharing
Network File and Folder
DATA
Shared
Network Path:
\\Dc\data
Share...
Advanced Sharing
Set custom permissions
advanced sharing optio
Permissions for DATA
Share Permissions
Group or user names:
Domain Admins (AMEEN\Domain Admins)
Sales (AMEEN\Sales)
SysAdmin (AMEEN\SysAdmin)
Add...
Remove
Permissions for Sales
Allow
Deny
Full Control
Change
Read
Read permission granted to Sales group
OK
Cancel
Apply
Close
7 items
1 item selected


Local Disk (C:)
File
Home
Share
View
This PC
Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
dns
System32
This PC
Network
Name
Home Folder
PerfLogs
Program Files
Program Files (x86)
Users
Windows
DATA
DATA Properties
General
Sharing
Network File and Folde
DATA
Shared
Network Path:
\\Dc\data
Share...
Advanced Sharing
Set custom permissio
advanced sharing opti
Permissions for DATA
Share Permissions
Group or user names:
Domain Admins (AMEEN\Domain Admins)
Sales (AMEEN\Sales)
SysAdmin (AMEEN\SysAdmin)
Add...
Remove
Permissions for SysAdmin
Allow
Deny
Full Control
Change
Read
Change permission granted to the SysAdmin group
OK
Cancel
Apply
Close
7 items
1 item selected


Local Disk (C:)
File
Home
Share
View
This PC
Local Disk (C:)
Search Local Dis...
Quick access
Desktop
Downloads
Documents
Pictures
dns
System32
This PC
Network
Name
Home Folder
PerfLogs
Users
DATA
Size
DATA Properties
General
Sharing
Security
Previous Versions
Customize
Network File and Folder Sharing
DATA
Permissions for DATA
Security
Object name: C:\DATA
Group or user names:
Domain Admins (AMEEN\Domain Admins)
Sales (AMEEN\Sales)
SysAdmin (AMEEN\SysAdmin)
Read & execute permission granted to Sales group
Add...
Remove
Permissions for Sales
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
OK
Cancel
Apply
Permissions for DATA
Security
Object name: C:\DATA
Group or user names:
Domain Admins (AMEEN\Domain Admins)
Sales (AMEEN\Sales)
SysAdmin (AMEEN\SysAdmin)
Modify permission granted to SysAdmin group
Add...
Remove
Permissions for SysAdmin
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
OK
Cancel
Apply
Close
Cancel
Apply
7 items
1 item selected


Read & execute: Allows users to view and run executable files, including scripts.
List folder contents: Permits viewing and listing of files and subfolders as well as executing of files; inherited by folders only. user2 is belongs to the Sales group that only has a Read & exects permission; user1-2 connot Write or save changes on the file as we can see in the messege system below.
Notepad
\\Dc\data\txt.txt
You do not have permission to open this file. See the owner of the file or an administrator to obtain permission.
OK
START
user2
Documents
Pictures
Settings
Power
Type here to search


Modify: Allows users to read and write of files and subfolders; also allows deletion of the folder. user3 is belongs to the SysAdmin group that has a Modify permission; that give user3-4 the avility to read & write and even save a new file on the same folder as we can see here.
This is my report. Do not change it, pls !
Ameen the King.
START
user3
Documents
Pictures
Settings
Power
Type here to search

Mapping a Network Drive

Mapping a drive means that we are going to make a specific drive available to other users connected to a common network. When a certain drive is mapped, it will also appear on the File Explorer section of other computers as if it is part of their hard drive and all of its contents are available to them[17].

It is also possible to map a network drive using a batch file that includes the net use:

```
net use Z: \\DEVICE-NAME-OR-IP\SHARED-FOLDER
```

In the command, replace "Z" with the drive letter not already in use you want to use. Then replace DEVICE-NAME-OR-IP and SHARED-FOLDER for the computer name or IP address of the device hosting the shared folder and the name of the shared[18].

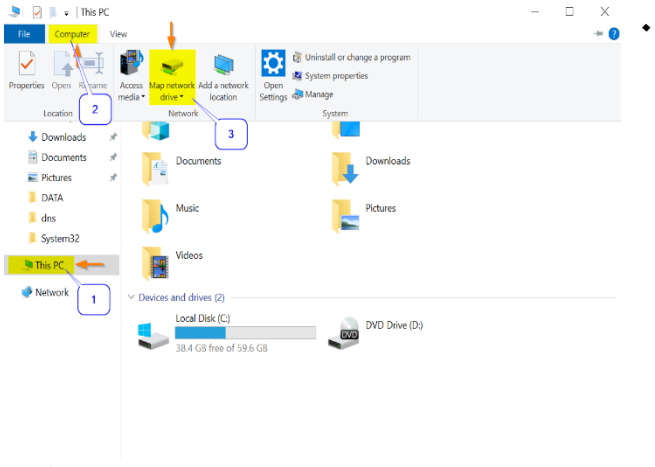
In our case; the command will be:

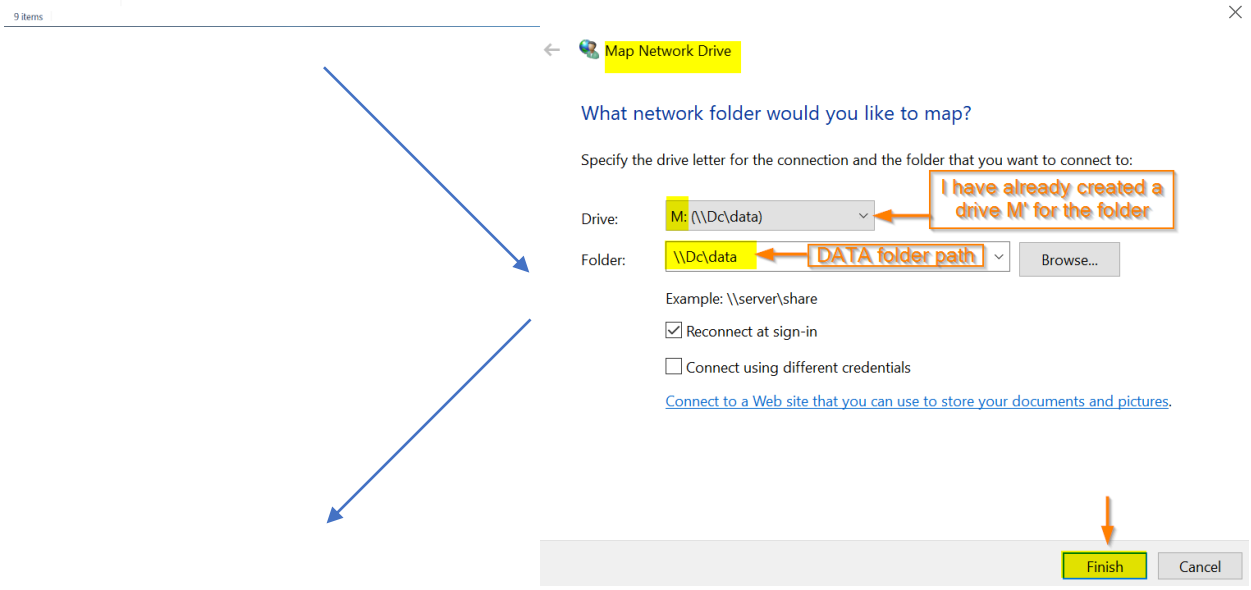
```
net use M: \\dc\data
```

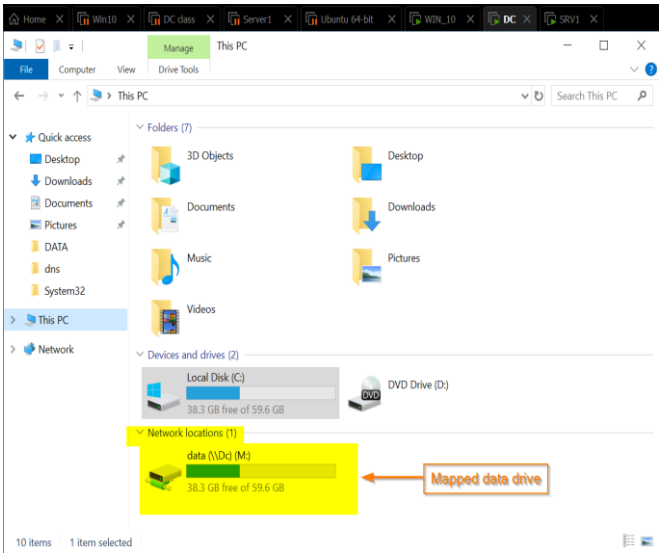
To map the "DATA" folder as a drive using the File Explorer:

File Explorer > This PC > Computer tab > Map Network Drive > Folder: \\DC\\data

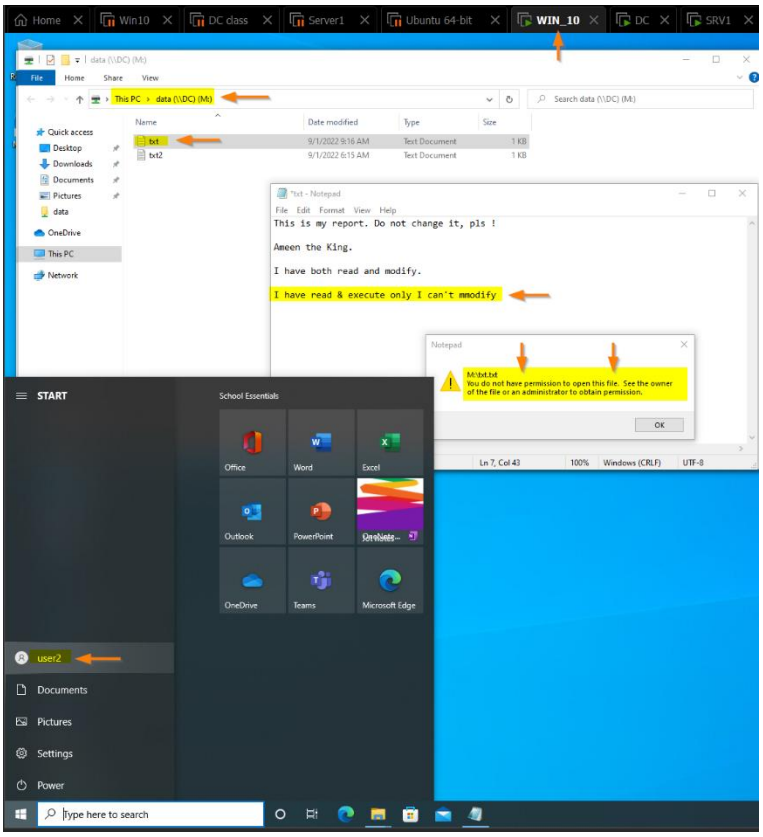
[17] https://windowstechies.com/what-does-mapping-a-drive-do-and-how-can-you-take-advantage-of-it/
[18] https://pureinfotech.com/map-network-drive-command-prompt-windows-10/


This PC
File
Computer
View
Map network drive
Add a network location
Open Settings
Uninstall or change a program
System properties
Manage
Location
Network
System
2
3
Downloads
Documents
Pictures
DATA
dns
System32
This PC
Network
1
Documents
Downloads
Music
Pictures
Videos
Devices and drives (2)
Local Disk (C:)
38.4 GB free of 59.6 GB
DVD Drive (D:)
9 items

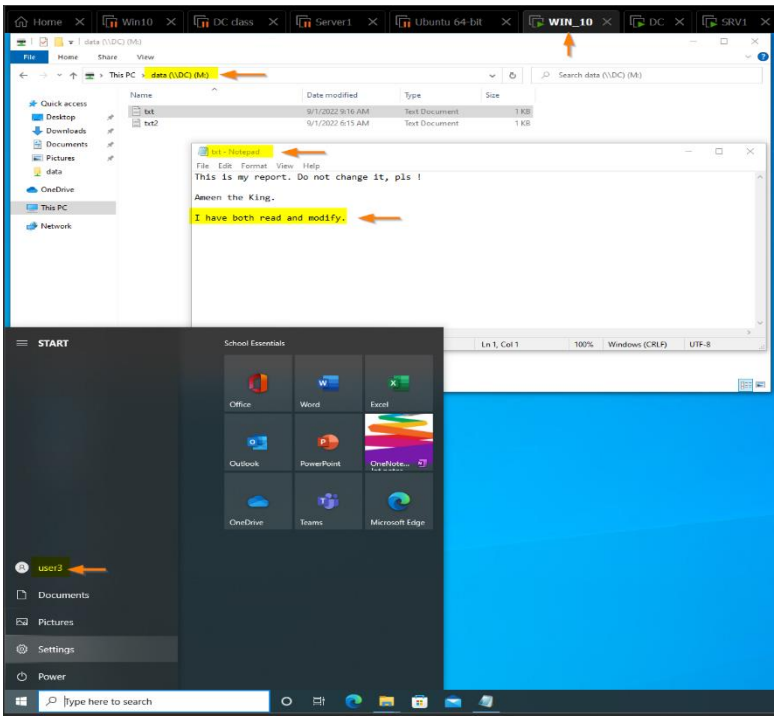

Map Network Drive
What network folder would you like to map?
Specify the drive letter for the connection and the folder that you want to connect to:
Drive:
M: (\\Dc\data)
I have already created a drive M' for the folder
Folder:
\\Dc\data
DATA folder path
Browse...
Example: \\server\share
Reconnect at sign-in
Connect using different credentials
Connect to a Web site that you can use to store your documents and pictures.
Finish
Cancel


Home
Win10
DC class
Server1
Ubuntu 64-bit
WIN_10
DC
SRV1
Manage
This PC
File
Computer
View
Drive Tools
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
DATA
dns
System32
This PC
Network
Folders (7)
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Devices and drives (2)
Local Disk (C:)
38.3 GB free of 59.6 GB
DVD Drive (D:)
Network locations (1)
data (\\Dc) (M:)
38.3 GB free of 59.6 GB
Mapped data drive
10 items
1 item selected

User2 can access and read the documents but can't modify:

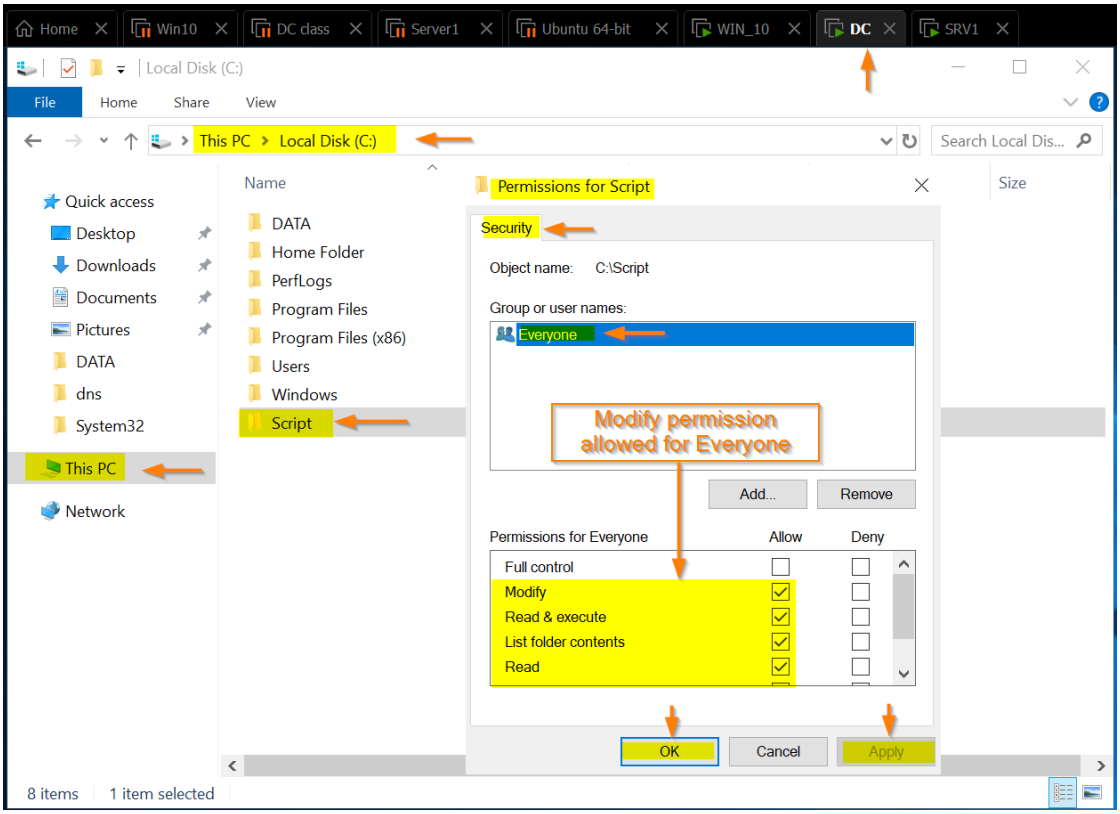


User3 can access, read and modify the txt document:



Now I will create a batch file with the purpose of mapping the folder as a drive once activated.

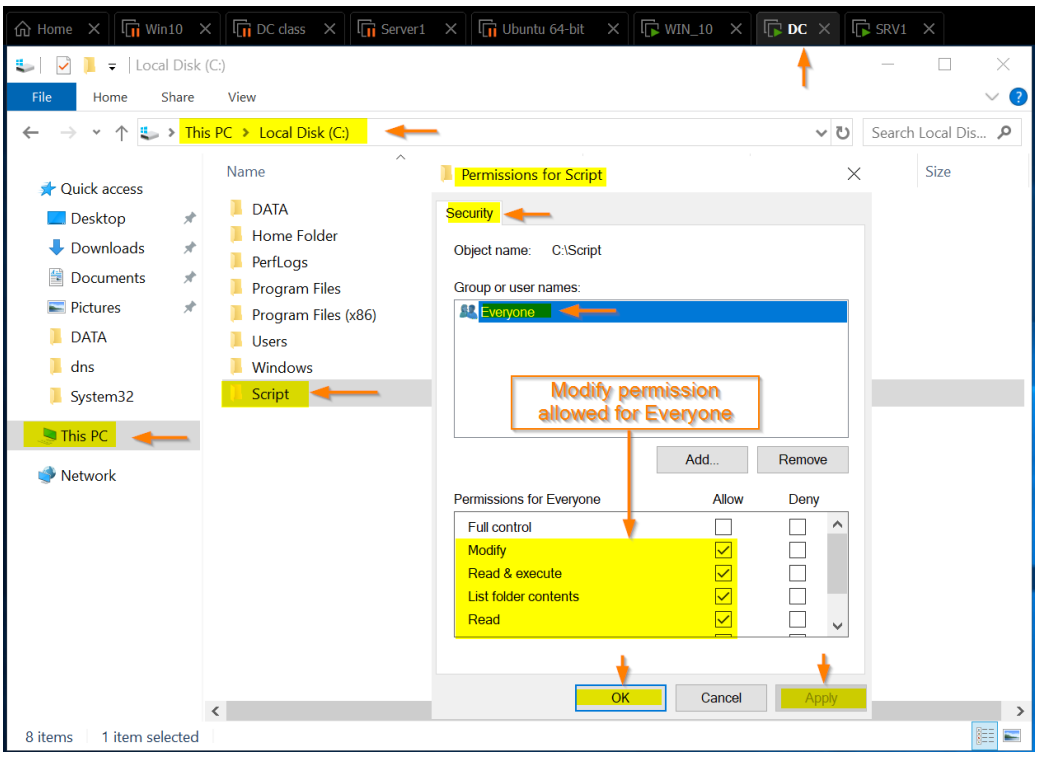
I did it by creating a shared folder called “Script”. I set the security permissions as ‘Modify’ for everyone.

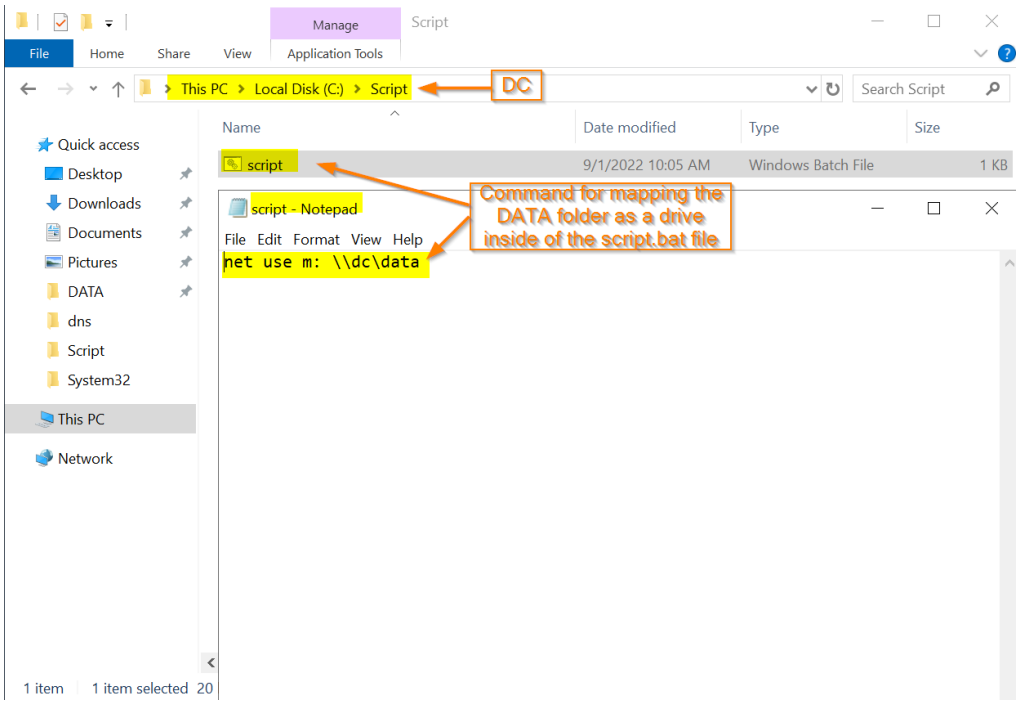


Then I created a text file by using the command:

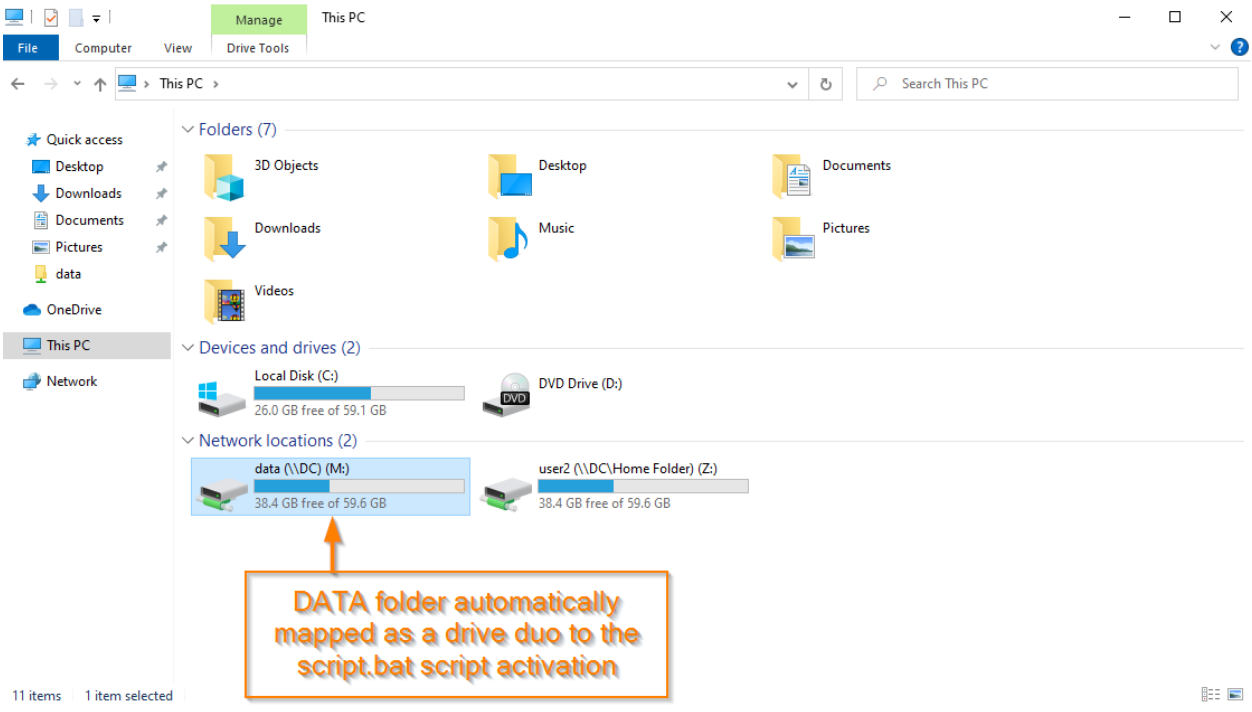
net use M: \\dc\data

and then I saved the file under the name **script.bat**, which turned it into a batch script.


Home
Win10
DC class
Server1
Ubuntu 64-bit
WIN_10
DC
SRV1
Local Disk (C:)
File
Home
Share
View
This PC > Local Disk (C:)
Search Local Dis...
Quick access
Desktop
Downloads
Documents
Pictures
DATA
dns
System32
This PC
Network
Name
DATA
Home Folder
PerfLogs
Program Files
Program Files (x86)
Users
Windows
Script
Permissions for Script
Security
Object name: C:\Script
Group or user names:
Everyone
Modify permission allowed for Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
OK
Cancel
Apply
Size
8 items
1 item selected


Manage
Script
File
Home
Share
View
Application Tools
This PC > Local Disk (C:) > Script
DC
Search Script
Quick access
Desktop
Downloads
Documents
Pictures
DATA
dns
Script
System32
This PC
Network
Name
Date modified
Type
Size
script
9/1/2022 10:05 AM
Windows Batch File
1 KB
script - Notepad
File Edit Format View Help
net use m: \\dc\data
Command for mapping the DATA folder as a drive inside of the script.bat file
1 item
1 item selected 20


Path to access the script.bat from WIN10
script
File
Home
Share
View
Network › DC › script
Search script
Name
Date modified
Type
Size
script
9/1/2022 10:05 AM
Windows Batch File
1 KB
Quick access
Desktop
Downloads
Documents
Pictures
data
OneDrive
This PC
Network
1 item


Manage
This PC
File
Computer
View
Drive Tools
This PC ›
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
data
OneDrive
This PC
Network
Folders (7)
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Devices and drives (2)
Local Disk (C:)
26.0 GB free of 59.1 GB
DVD Drive (D:)
DVD
Network locations (2)
data (\\DC) (M:)
38.4 GB free of 59.6 GB
user2 (\\DC\Home Folder) (Z:)
38.4 GB free of 59.6 GB
DATA folder automatically mapped as a drive duo to the script.bat script activation
11 items
1 item selected

Remote Desktop Protocol (RDP)

Remote Desktop Protocol (RDP) is a secure network communications protocol developed by Microsoft. It enables network administrators to remotely diagnose problems that individual users encounter and gives users remote access to their physical work desktop computers[19].
From a cyber-security point of view there are some vulnerability and weakness points; These are the most important vulnerabilities in RDP[20]:

1. Weak user sign-in credentials. Most desktop computers are protected by a password, and users can typically make this password whatever they want. The problem is that the same password is often used for RDP remote logins as well. Companies do not typically manage these passwords to ensure their strength, and they often leave these remote connections open to brute force or credential stuffing attacks.

2. Unrestricted port access. RDP connections almost always take place at port 3389*. Attackers can assume that this is the port in use and target it to carry out on-path attacks, among others.

Therefore, the maintenance and general usage of the RDP services should be conditioned by the adherence to the following criteria: strong passwords, multi factor authentication, the principle of least privilege, checks ensuring the proper configuration of RDP ports etc.

[19] https://www.techtarget.com/searchenterprisedesktop/definition/Remote-Desktop-Protocol-RDP
[20] https://www.cloudflare.com/learning/access-management/rdp-security-risks/

Enabling Remote Access to DC and SRV1

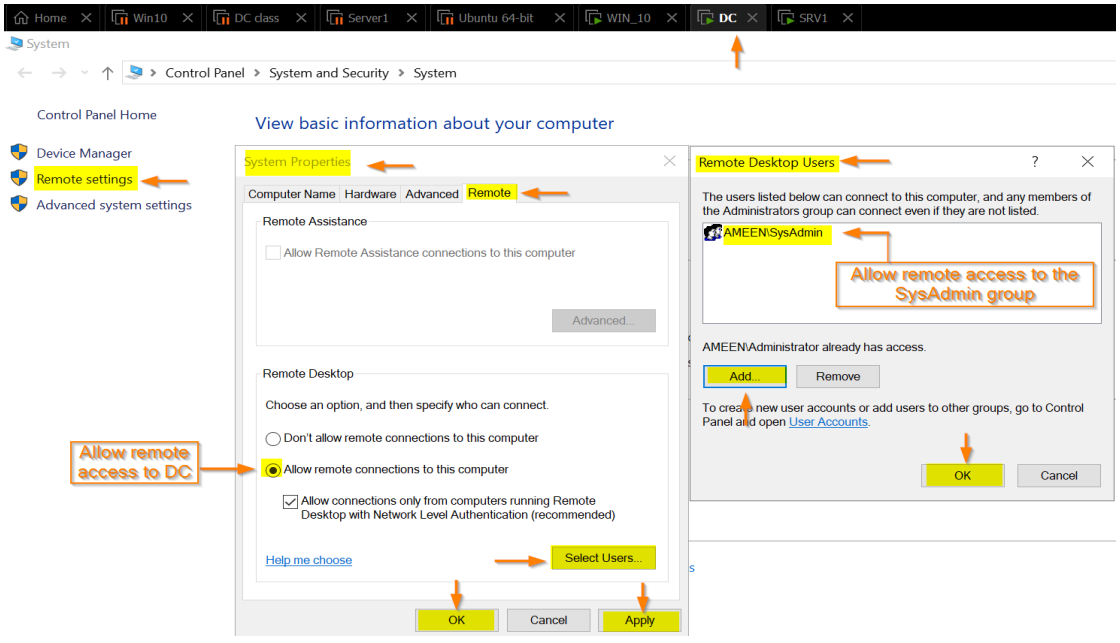
To enable the Remote access of chosen users to my DC and SRV1 servers. I entered each of the servers' remote properties and manually edited the permissions of the remote access services through:

File Explorer > This PC > Properties >Remote settings > Allow remote connections to this computer > Select users.

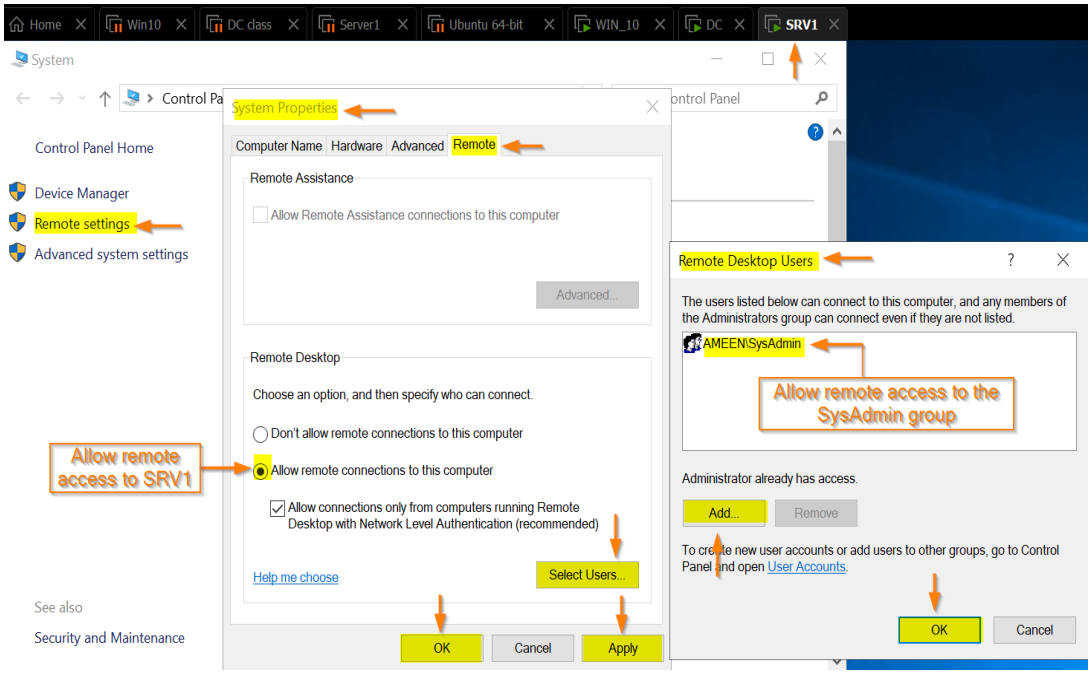
For WIN10 I enabled the Remote Desktop Feature on the client through:

File Explorer > This PC > Properties > Remote Desktop > Enable Remote Desktop on this computer

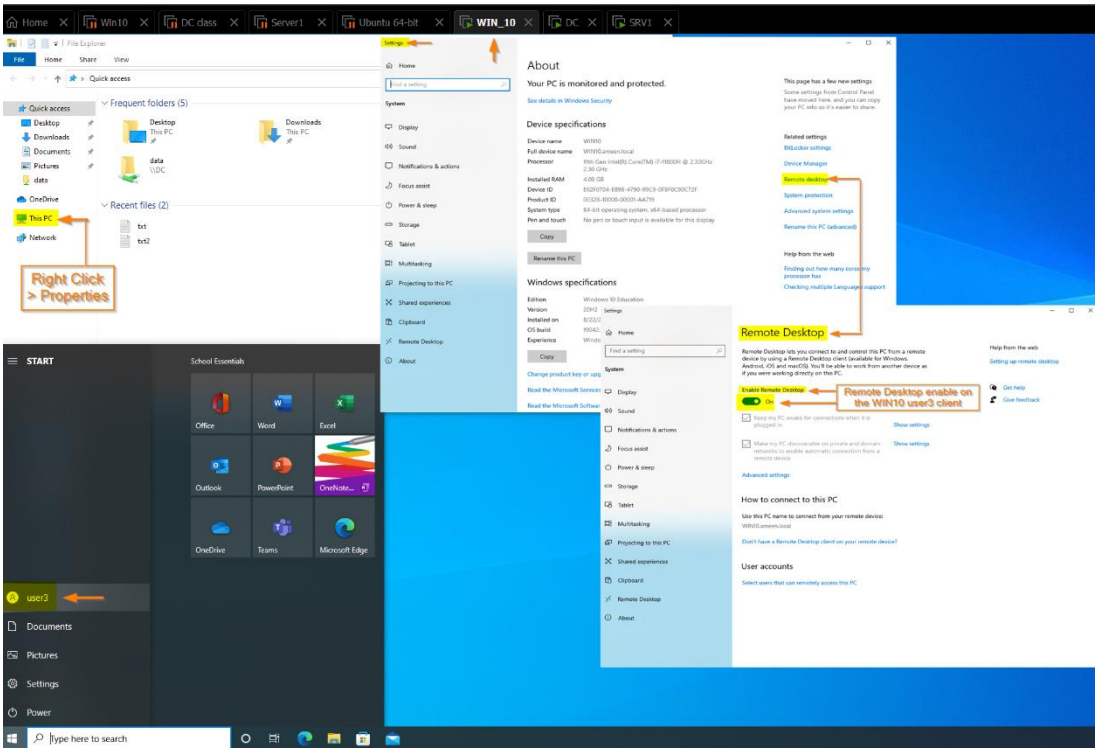
DC server:



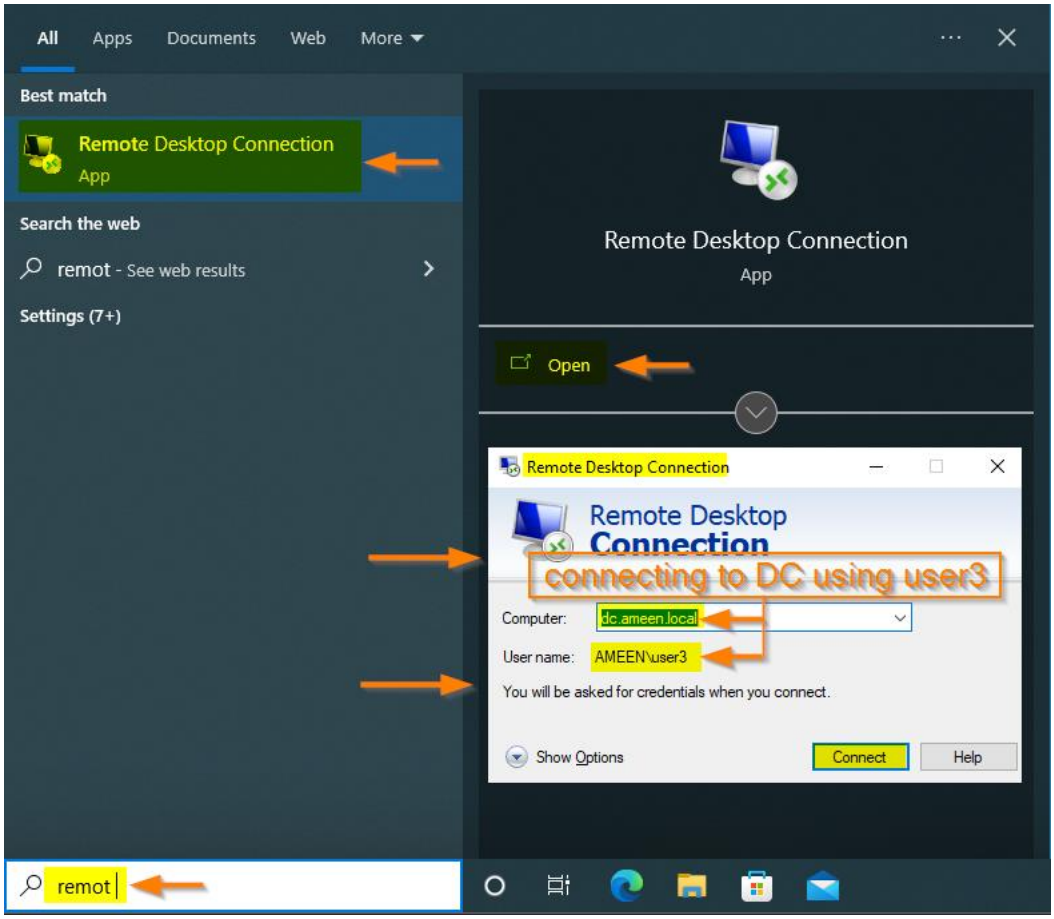
SRV1 server:

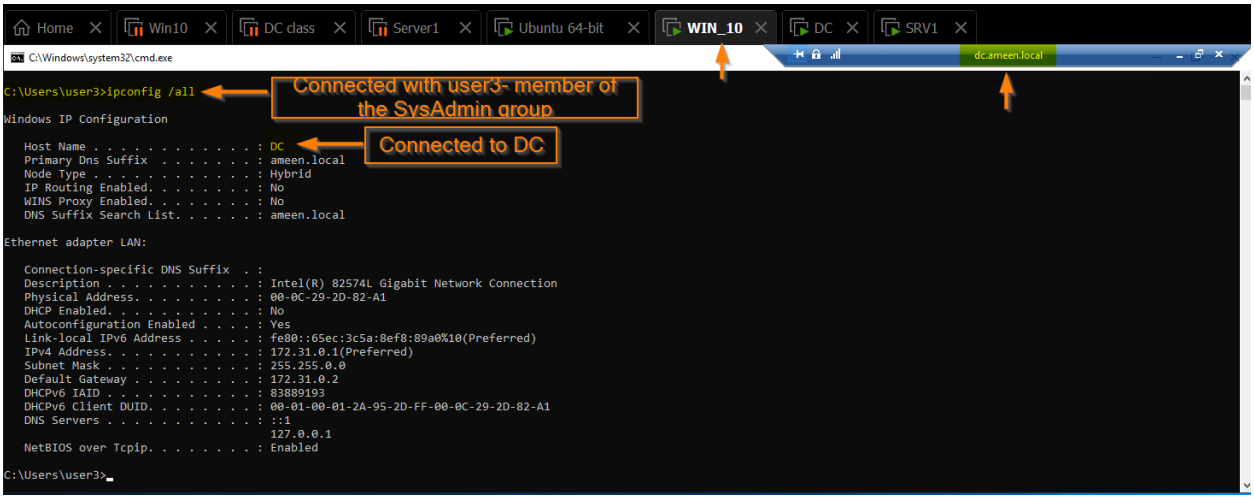


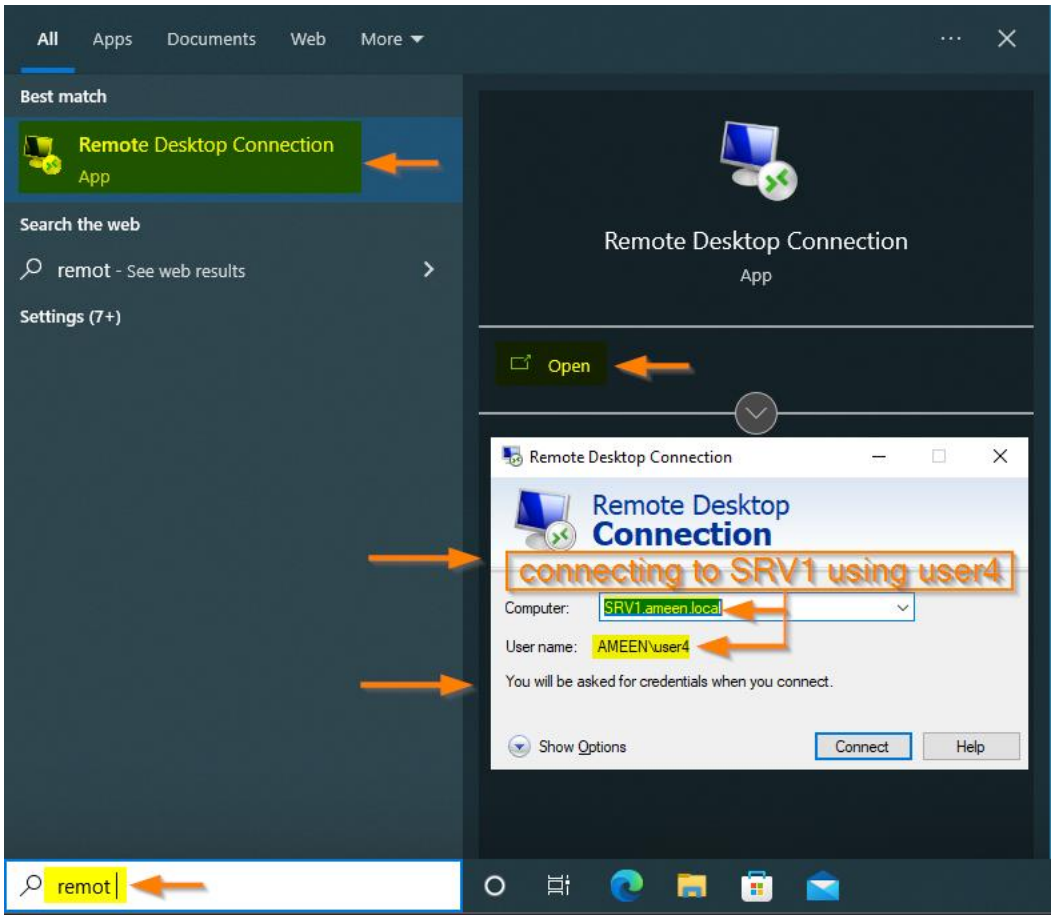
WIN10 client:



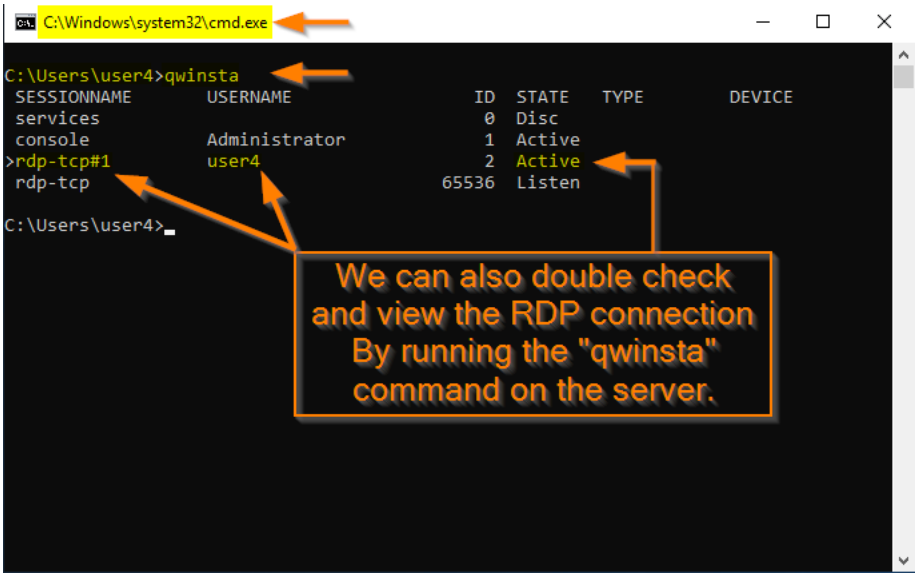
Accessing DC and SRV1 from WIN10 using SysAdmin group user3-4



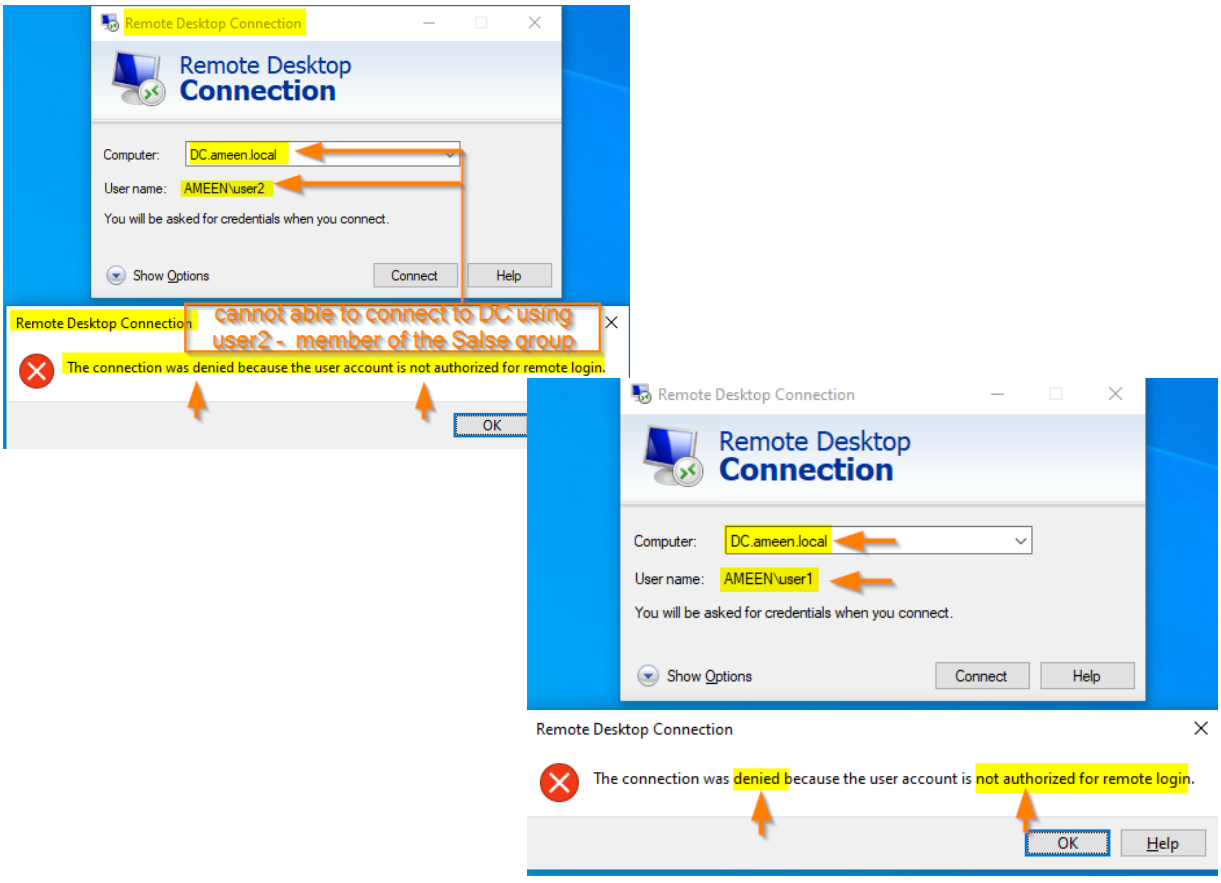


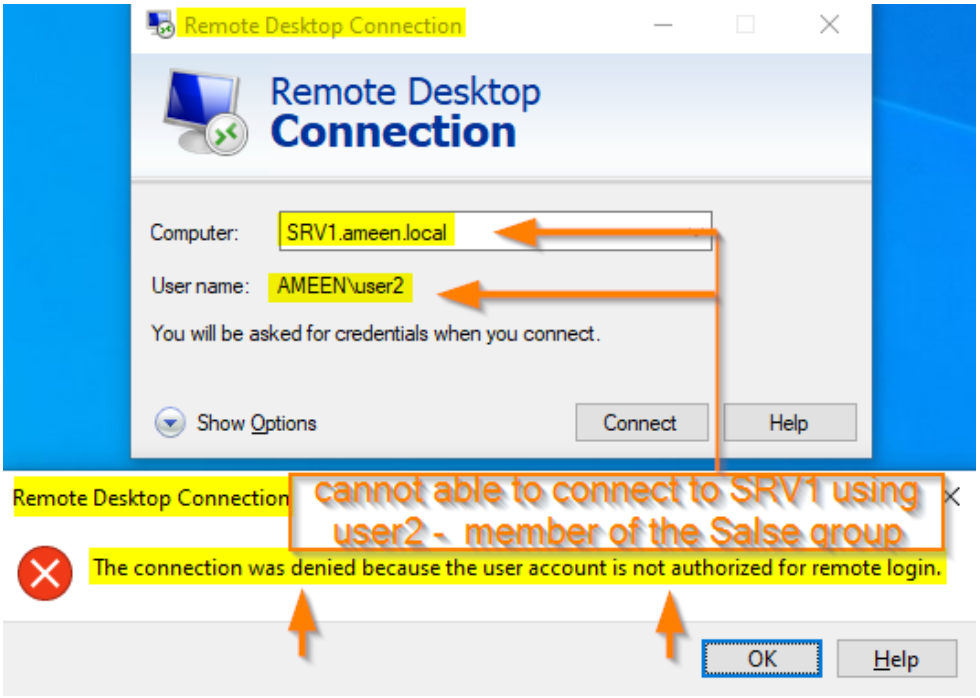

All
Apps
Documents
Web
More
Best match
Remote Desktop Connection
App
Search the web
remot - See web results
Settings (7+)
Remote Desktop Connection
App
Open
Remote Desktop Connection
Remote Desktop
Connection
connecting to SRV1 using user4
Computer:
SRV1.ameen.local
User name:
AMEEN\user4
You will be asked for credentials when you connect.
Show Options
Connect
Help
remot

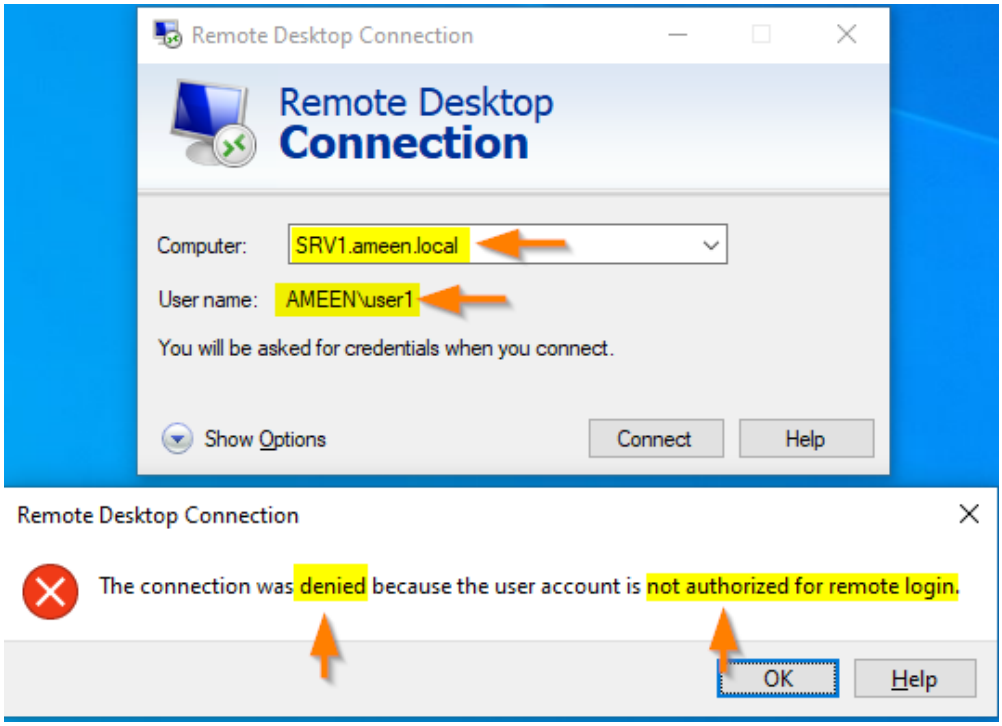

Home
Win10
DC class
Server1
Ubuntu 64-bit
WIN_10
DC
SRV1
C:\Windows\system32\cmd.exe
SRV1.ameen.local
Microsoft Windows [Version 10.0.17763.3287]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\user4>ipconfig /all
Connected with user4- member of the SysAdmin group
Windows IP Configuration
Host Name . . . . . : SRV1
Connected to SRV1
Primary Dns Suffix . . . . . : ameen.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : Yes
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ameen.local
mynet
Ethernet adapter LAN:
Connection-specific DNS Suffix . : ameen.local
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-5F-1D-8F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 172.31.0.2(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Lease Obtained. . . . . : Wednesday, August 31, 2022 10:16:52 AM
Lease Expires . . . . . : Thursday, September 1, 2022 11:58:28 PM
Default Gateway . . . . . :
DHCP Server . . . . . : 172.31.0.1
DNS Servers . . . . . : 172.31.0.1
NetBIOS over Tcpip. . . . . : Enabled
Ethernet adapter WAN:
Connection-specific DNS Suffix . : mynet
Description . . . . . : Intel(R) 82574L Gigabit Network Connection #2
Physical Address. . . . . : 00-0C-29-5F-1D-85
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 10.0.0.63(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, August 31, 2022 10:21:04 AM
Lease Expires . . . . . : Thursday, September 1, 2022 8:14:01 PM
Default Gateway . . . . . : 10.0.0.138
DHCP Server . . . . . : 10.0.0.138
DNS Servers . . . . . : 172.31.0.1
NetBIOS over Tcpip. . . . . : Enabled
C:\Users\user4>



Connection **denied** to DC and SRV1- using Sales group user1-2




Remote Desktop Connection
Remote Desktop
Connection
Computer:
SRV1.ameen.local
User name:
AMEEN\user2
You will be asked for credentials when you connect.
Show Options
Connect
Help
Remote Desktop Connection
cannot able to connect to SRV1 using user2 - member of the Salse group
The connection was denied because the user account is not authorized for remote login.
OK
Help


Remote Desktop Connection
Remote Desktop
Connection
Computer:
SRV1.ameen.local
User name:
AMEEN\user1
You will be asked for credentials when you connect.
Show Options
Connect
Help
Remote Desktop Connection
The connection was denied because the user account is not authorized for remote login.
OK
Help

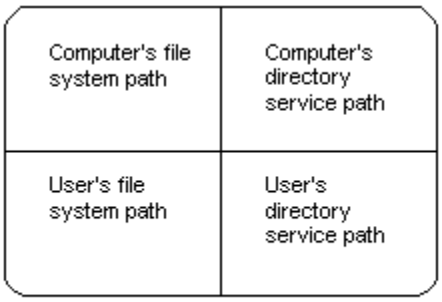
Group Policy Objects (GPO)

A Group Policy Object (GPO) is a virtual collection of policy settings. A GPO has a unique name, such as a GUID.

Group Policy settings are contained in a GPO. A GPO can represent policy settings in the file system and in the Active Directory. GPO settings are evaluated by clients using the hierarchical nature of Active Directory[21].

There are pre-made GPO settings which come in a form of Administrative Temple (*.adm)[22].

The following illustration shows the structure of a GPO:



Group Policy Object (GPO)

[21] https://docs.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-objects
[22] © Yaki Ben-Nissan

The hierarchy of the effect of a GPO on a specific object in the AD- From lowest to highest[23]:

- Local policy
- GPO attached to a site
- GPO attached to a domain
- GPO attached to an OU

GPO properties[24]:

- Enforced - makes the GPO stronger and its settings take effect even if there is a conflict with settings of other GPOs. Passes even if there is no inheritance.

- Multiple Links - If there are several GPOs on a certain OU then the last one (the lowest number) is the strongest.

Inheritance blocking:

Inheritance can be blocked by enabling the Inheritance Policy Block option on the OU.

In any case, it is not possible to block Enforced.

[23] © Yaki Ben-Nissan
[24] © Yaki Ben-Nissan

Creating GPOs on the DC server

In order to harden the network access and increase its security, I created **3** GPOs that affect the domain users:

1. Preventing all users except members of the SysAdmin group from accessing the Control Panel.

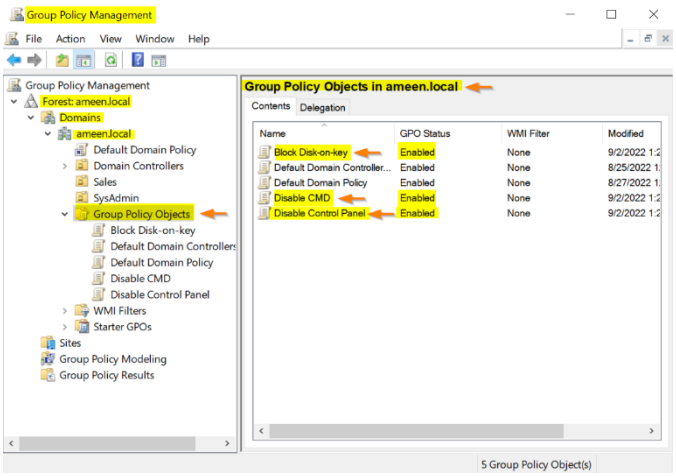
2. Preventing all users except members of the SysAdmin group from accessing the CMD.

3. Preventing all domain users from using a disk-on-key.

To create the GPOs, I entered the Group Policy Management by:

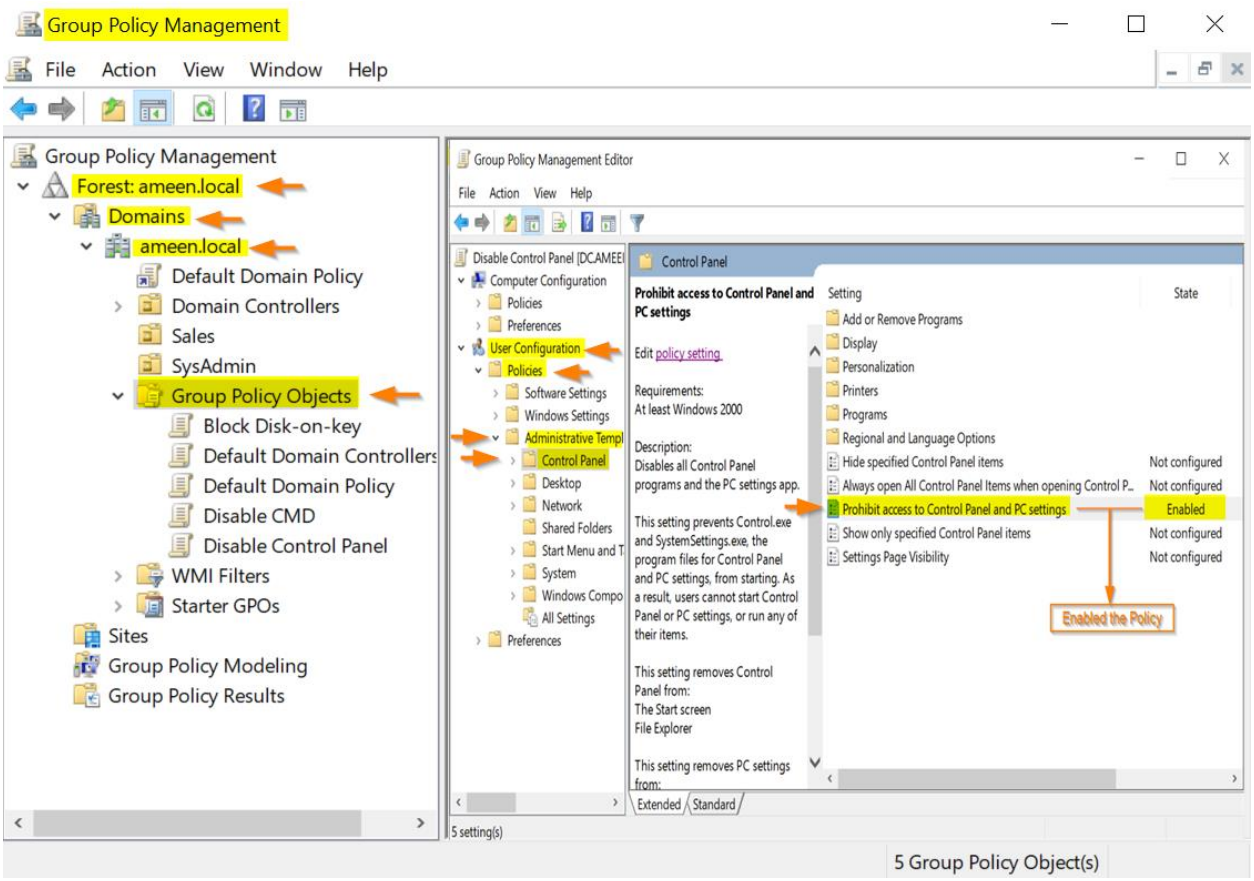
Server Manager > Dashboard >Tools > Group Policy Management > Forest: ameen.local > Domains > ameen.local > Group Policy Objects > New.

I then created **3** new objects as we said in the above.

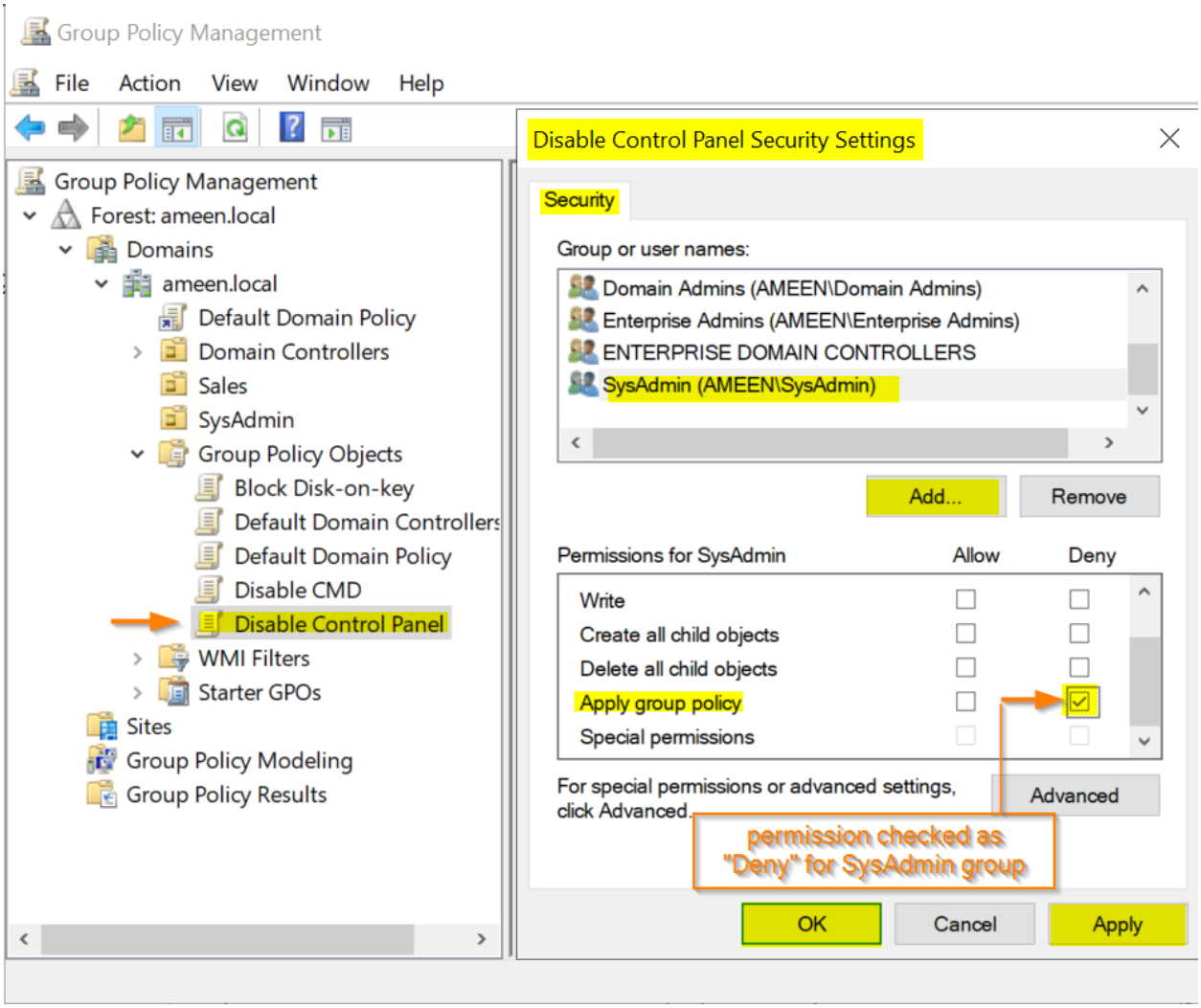


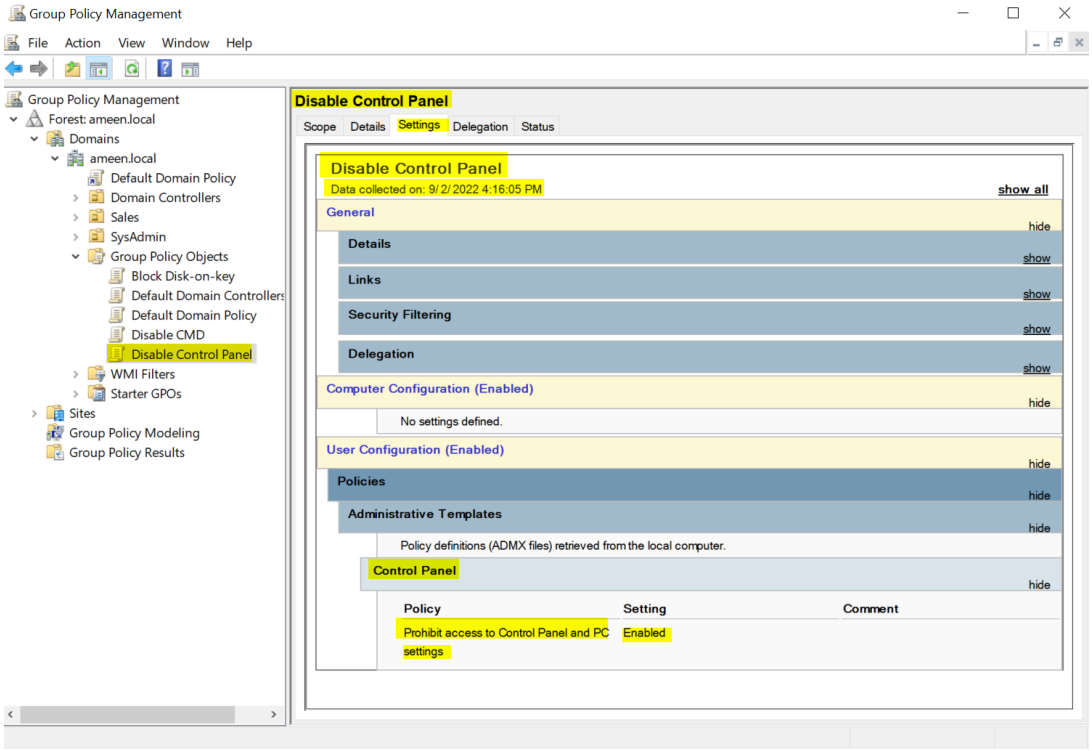
In order to prevent all users except members of the SysAdmin group from accessing the Control Panel, I accessed through:

Right Click on Disable Control Panel > Edit > User Configuration > Policies > Administrative Templates > Control Panel > Prohibit access to Control Panel and PC settings > Enable.

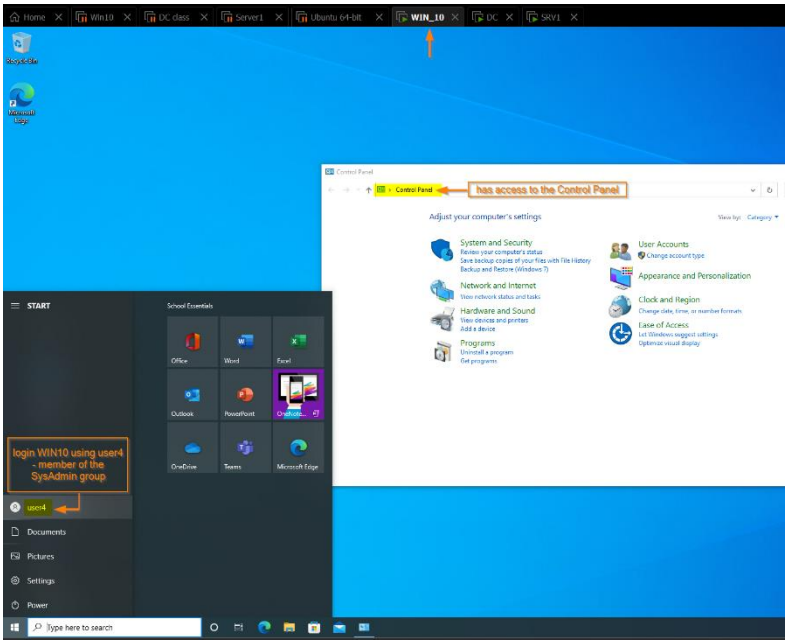


Then using the “Delegation” tab, go to “Advanced” > “Security” Setting > “Add” > add SysAdmin to the Group or user name > then I checked the “Deny” box next to the “Apply group policy” permission for the SysAdmin group in order to exclude the group from the policy and allow the access of its members to the Control Panel.



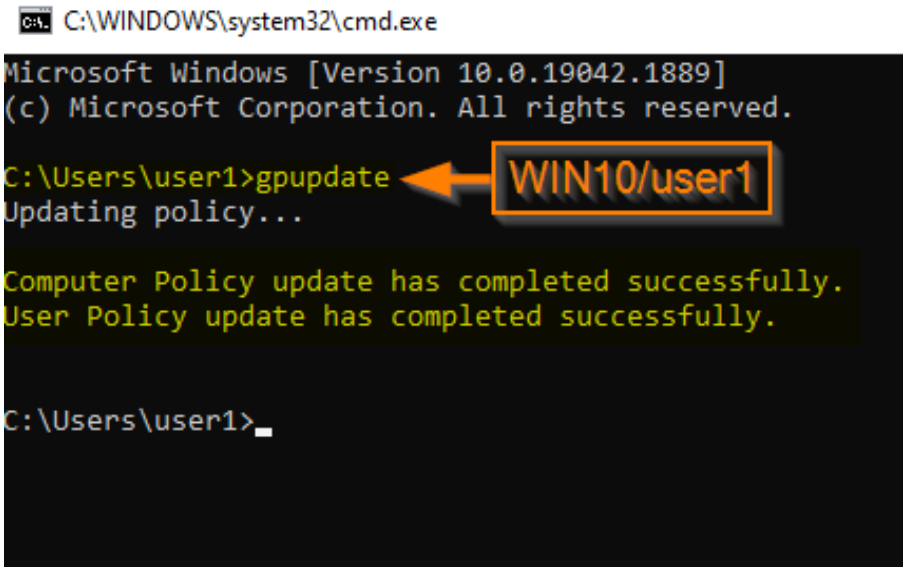


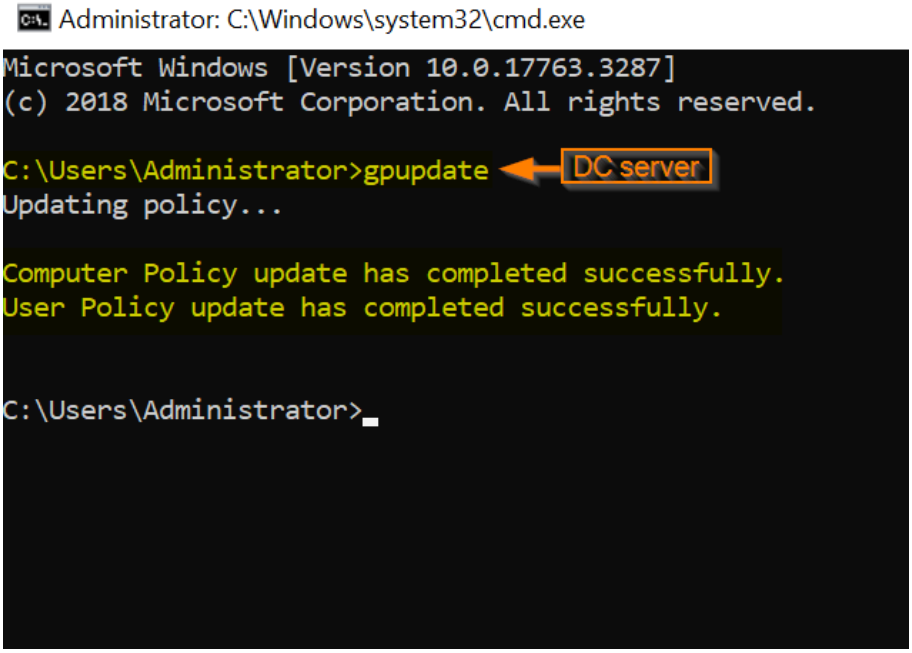
WIN10 > user4 - member of the SysAdmin group, has access to the Control Panel.



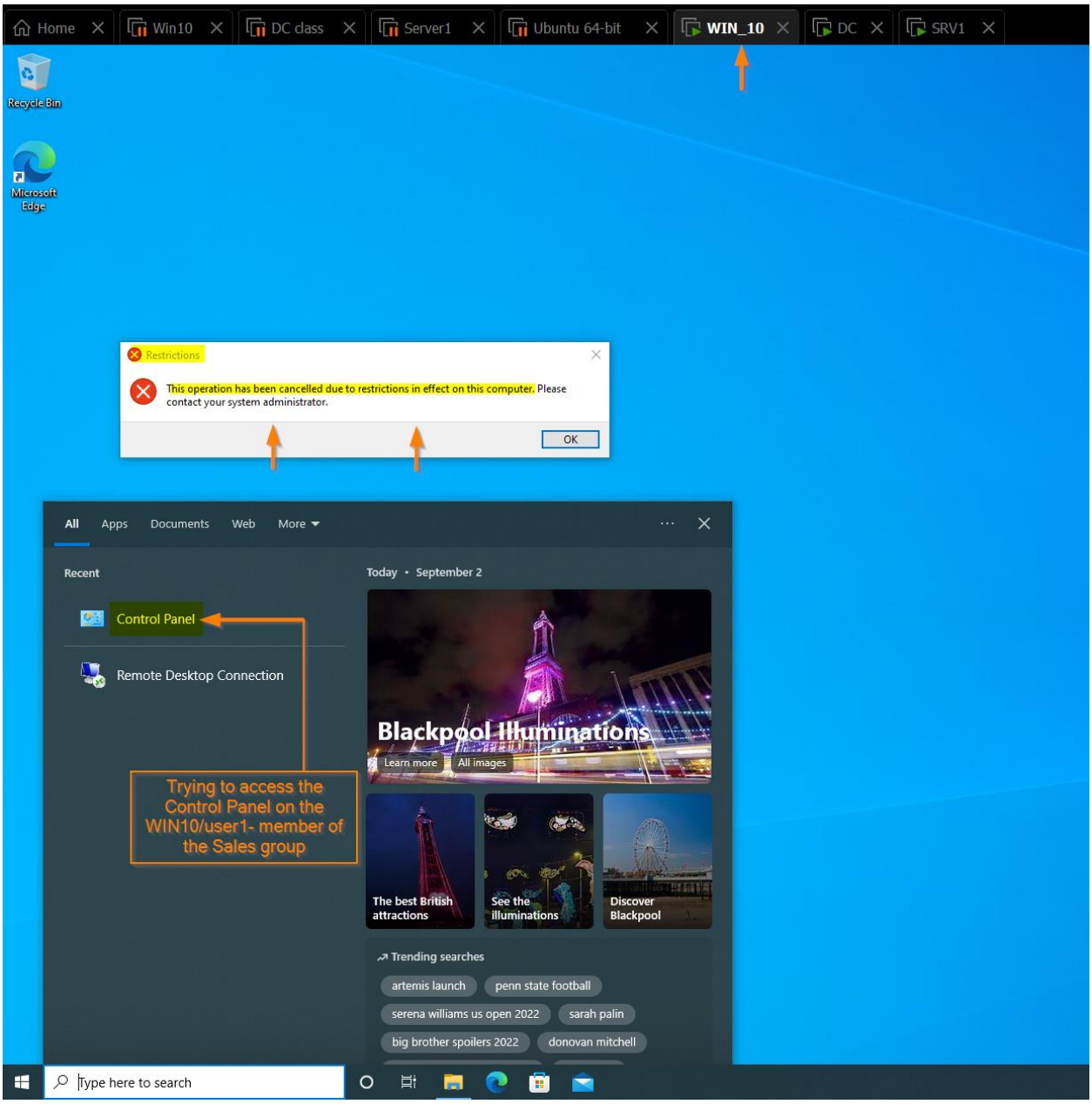
In my case I wasn't able to enforce the GPO on the Sales group users-user1-2, to deny the access to Control Panel!

So the problem was solved after I used the "gpupdate" command, both sides, from the DC server and the client-WIN10/user1.





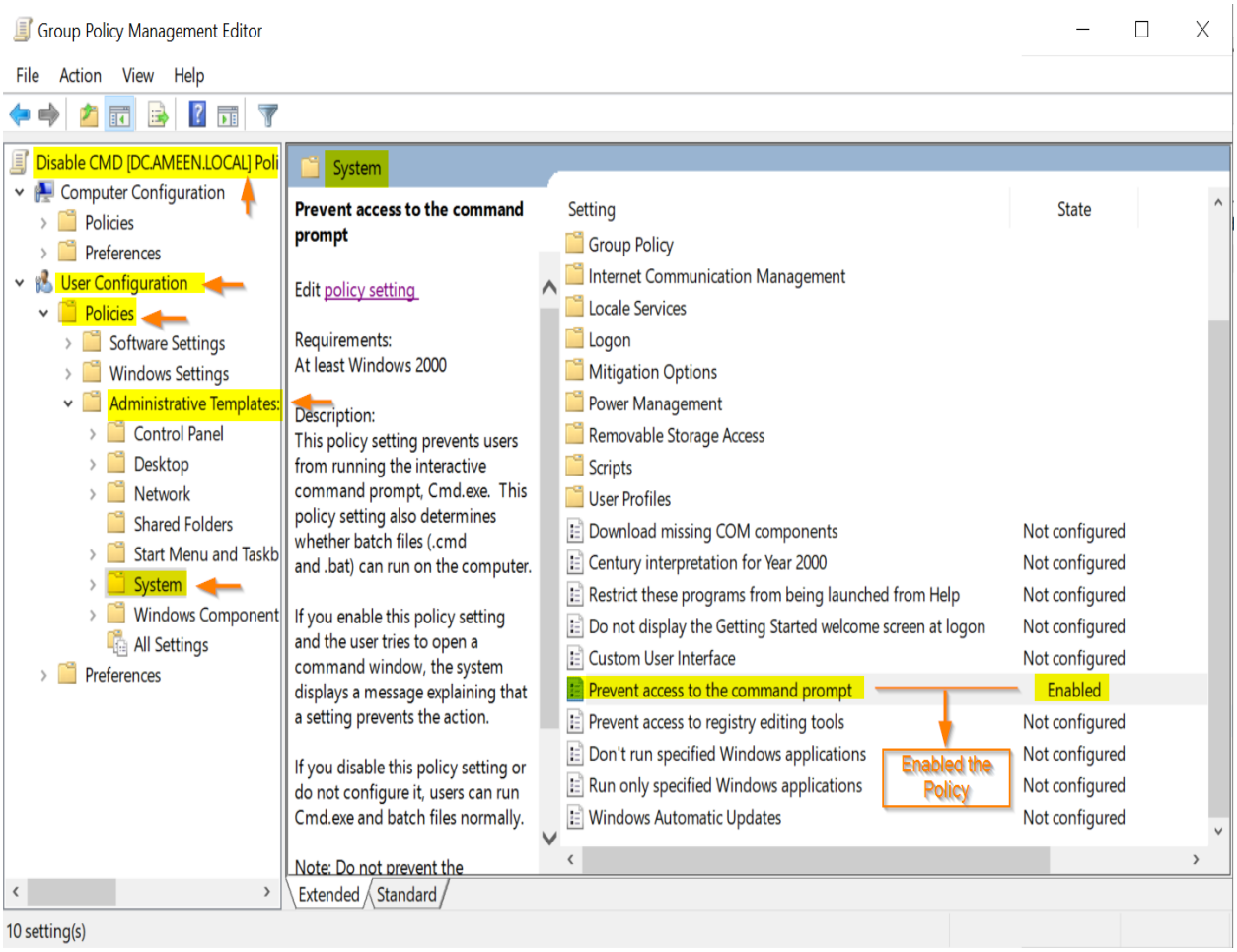
WIN10 > user1 - member of the Sales group, has **NO** access to the Control Panel.

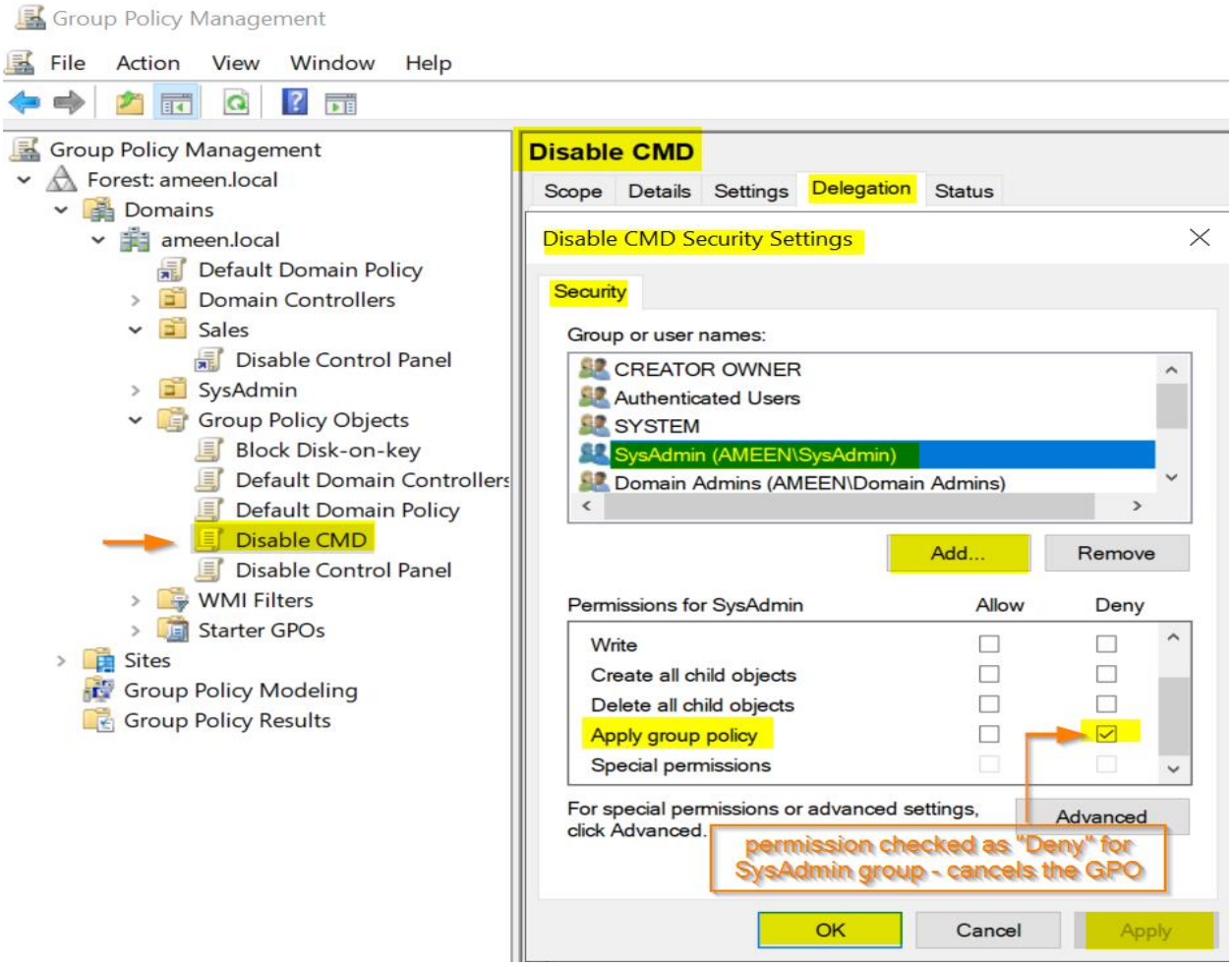


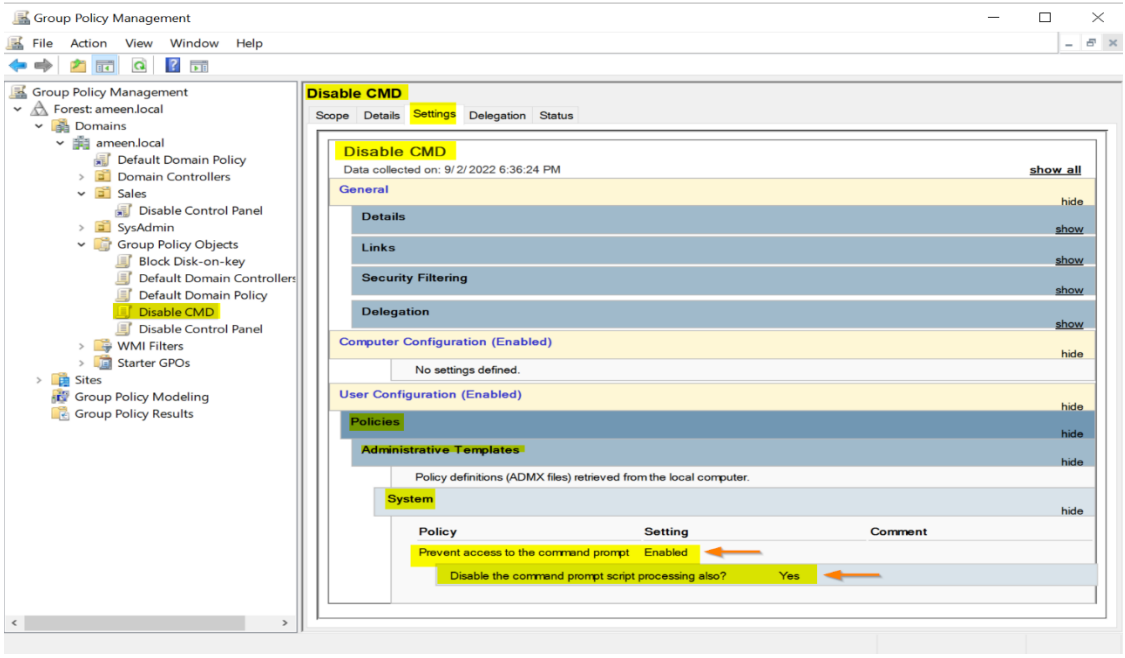
to prevent all users except members of the SysAdmin group from accessing the CMD:

Right Click Disable CMD > Edit > User Configuration > Policies > Administrative Templates > System > Prevent access to command prompt > Enable.

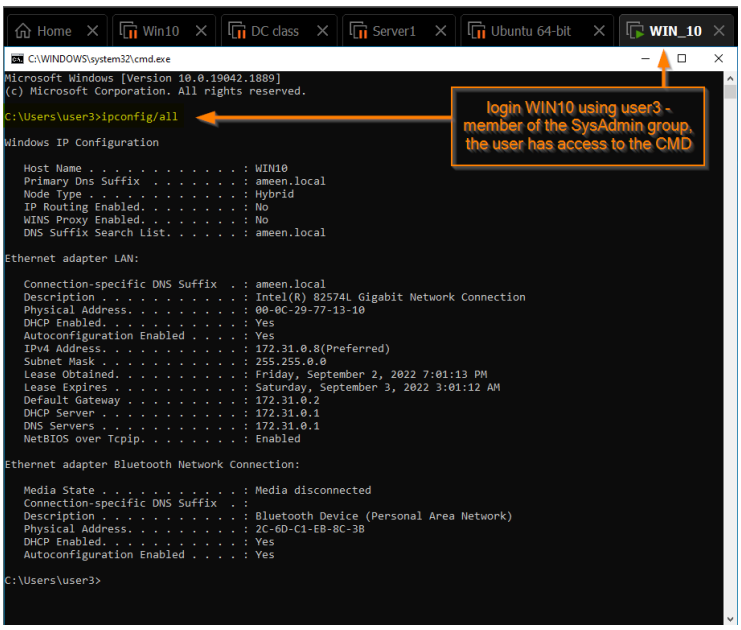
Once again, I also managed the object's permissions.



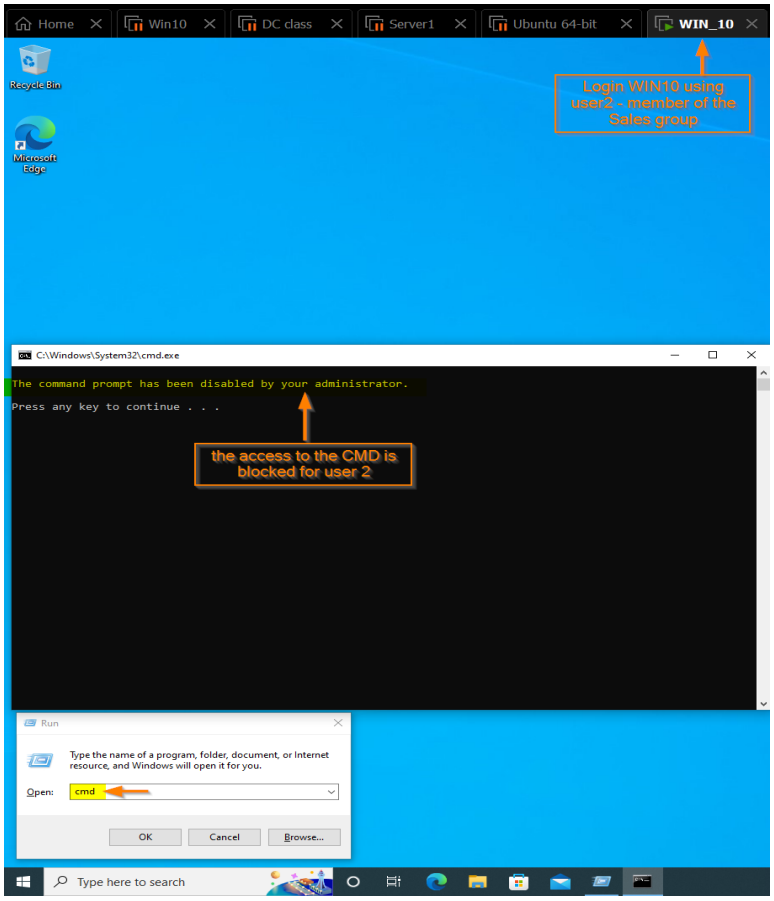

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: ameen.local
Domains
ameen.local
Default Domain Policy
Domain Controllers
Sales
Disable Control Panel
SysAdmin
Group Policy Objects
Block Disk-on-key
Default Domain Controllers
Default Domain Policy
Disable CMD
Disable Control Panel
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Disable CMD
Scope Details Settings Delegation Status
Disable CMD Security Settings
Security
Group or user names:
CREATOR OWNER
Authenticated Users
SYSTEM
SysAdmin (AMEEN\SysAdmin)
Domain Admins (AMEEN\Domain Admins)
Add... Remove
Permissions for SysAdmin Allow Deny
Write
Create all child objects
Delete all child objects
Apply group policy
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
permission checked as "Deny" for SysAdmin group - cancels the GPO
OK Cancel Apply


Group Policy Management
File Action View Window Help
Disable CMD
Scope Details Settings Delegation Status
Disable CMD
Data collected on: 9/2/2022 6:36:24 PM
show all
General
Details
Links
Security Filtering
Delegation
Computer Configuration (Enabled)
No settings defined.
User Configuration (Enabled)
Policies
Administrative Templates
Policy definitions (ADMX files) retrieved from the local computer.
System
Policy Setting Comment
Prevent access to the command prompt Enabled
Disable the command prompt script processing also? Yes

WIN10 > user3 - member of the SysAdmin group, has access to the CMD.

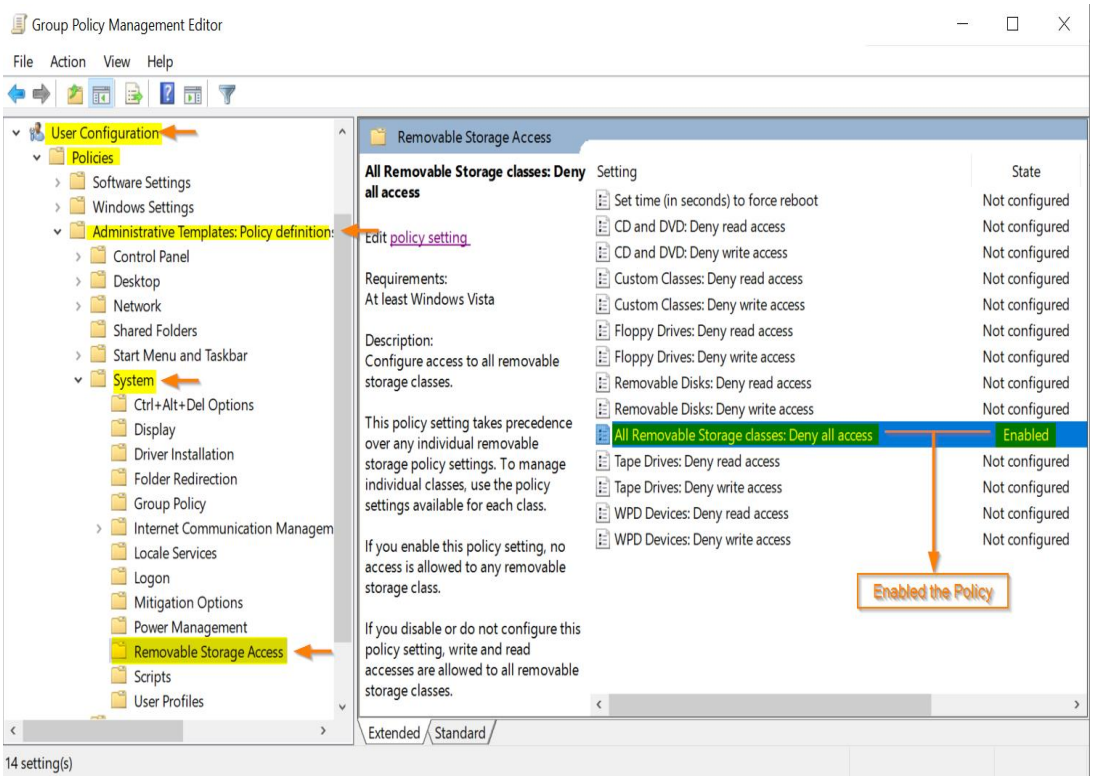


WIN10 > user2 - member of the Sales group, has **NO** access to the CMD.



Finally, to prevent all domain users from using a Disk-on-key, through:

Right Click on Block Disk-on-key > User Configuration > Policies > Administrative Templates > System > Removable Storage Access > All Removable Storage classes; Deny all access > Enable.



WIN10 > prevent all Domain users from using the removable Disk-on-key including the SysAdmin group.