

# Part 1

**in**  
Eido Epstein

# MCSA Tutorial

For beginners, a simplified and short introduction to network architecture.

**By:** Eido Epstein

Dec  
**2020**

# Glossary

<b>Requirements .....</b>	<b>4</b>
<b>Active Directory .....</b>	<b>5</b>
Enabling Active Directory.....	5
Enabling Domain Controller Features.....	6
Adding Devices to a domain .....	8
<b>Setting Permissions.....</b>	<b>10</b>
Creating an OU.....	10
Creating a User.....	11
Adding an OU to a Container .....	13
<b>DHCP.....</b>	<b>16</b>
Enabling DHCP.....	16
Initial Setup .....	17
DHCP IP Allocation Check.....	22
<b>DNS .....</b>	<b>23</b>
Creating a New Forward Lookup Zone .....	25
Creating a Host(A) Record .....	27
Enabling Reverse Lookup Zone .....	28
Creating a PTR Record.....	29
Setting a Conditional Forwarding .....	31
Setting Forwarders.....	32
<b>Network Connection .....</b>	<b>33</b>
Setting a Connection.....	33
Checking Connectivity.....	37
<b>Managerial &amp; Sharing Features.....</b>	<b>40</b>
Creating a Shared Folder.....	40
Permissions for a Shared Folder .....	43
Validating Sharing Configurations .....	47

Mapping a Shared Folder .....	48
Creating a Home Folder for Clients.....	52
<b>RDP &amp; SSH Connections</b> .....	55
Enabling Remote Desktop Connection .....	55
Enabling Remote Connection with SSH .....	59
<b>Basic Hardening Rules</b> .....	64
Disabling CMD .....	64
Disabling Control Panel .....	66
Disabling USB Devices Access .....	67
<b>Conclusion</b> .....	68

## Requirements

In order to manually follow-up with this article, there are some prerequisites that needs be made;

- Two Windows Server 2019 OS installed.
- One Windows 10 OS installed.
- ❖ OS- Operating System, a system software that manages computer hardware, software resources, and provides common services for computer programs.



Make sure that the following configurations are set for each of the installed OSs on your Local Area Network, for IPv4;

	IP Address	Subnet Mask	Default Gateway	Preferred DNS
WIN10	172.31.0.3	255.255.255.192	172.31.0.61	172.31.0.1
DC	172.31.0.1	255.255.255.192	172.31.0.61	172.31.0.1
SRV1	172.31.0.61	255.255.255.192	172.31.0.61	172.31.0.1

- In order to configure the above table;
  - i. Go to- **Control Panel\Network and Internet\Network Connections**
  - ii. Right click on the network icon and choose "**Properties**"
  - iii. Double click on- "**Internet Protocol Version 4 (TCP/IPv4)**"
- On how to change your devices names please follow this- [Link](#)
- Verify that all of your devices are on the same network.

## Active Directory


Active Directory (AD), manages a list of users, devices and also handles LDAP and Kerberos protocols. The name for a group of devices that's being affected by AD is called Domain.

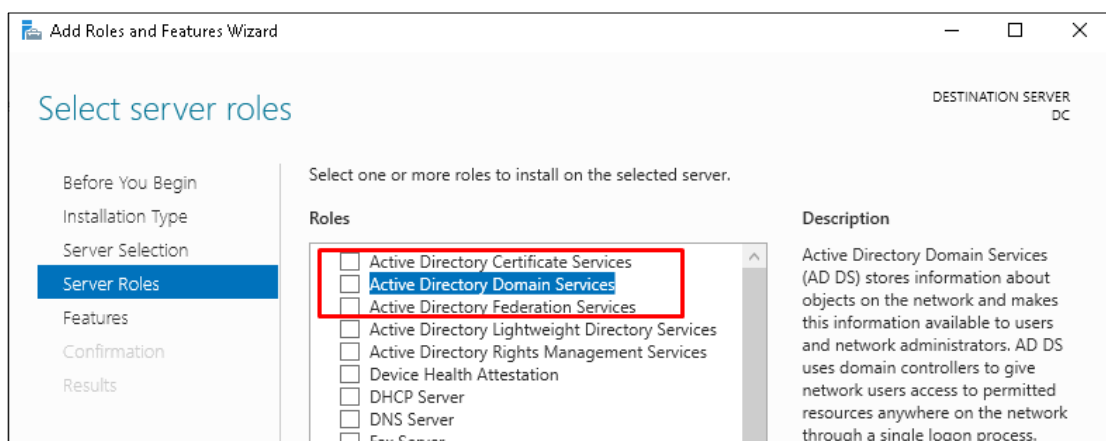
- ❖ Lightweight Directory Access Protocol (LDAP)- An Application Programming Interface (API) protocol that connects other system to our domain.
- ❖ Kerberos- The authentication protocol that's being used when a device is trying to connect to our domain.

Enabling AD services on our main server is the first step for building our network. In order to install AD on a server, the following requirements must be checked;

- i. Name the relevant server.
- ii. Assign a static IP address to the relevant server.
- iii. Enable admin user login to the relevant server only with credentials (user name and password).
  - The password must contain 7 characters and above with 3 elements- For example; Welc0me5%

### Enabling Active Directory:

- 1) On **DC** server, open the Server Manager application 
- 2) In the right top corner, click on "**Manage**" and choose "**Add Roles and Features**".
- 3) Click on the "**Next**" button until you reach the "**Server Roles**" Section.
- 4) Check the box for "**Active Directory Domain Services**" and press "**Add Feature**".



- 5) Click "**Next**" until you reach the "**Install**" button and press it.

## Enabling Domain Controller Features

Now that we have enabled AD services for our server, the next step will be to apply Domain Controller (DC) features.

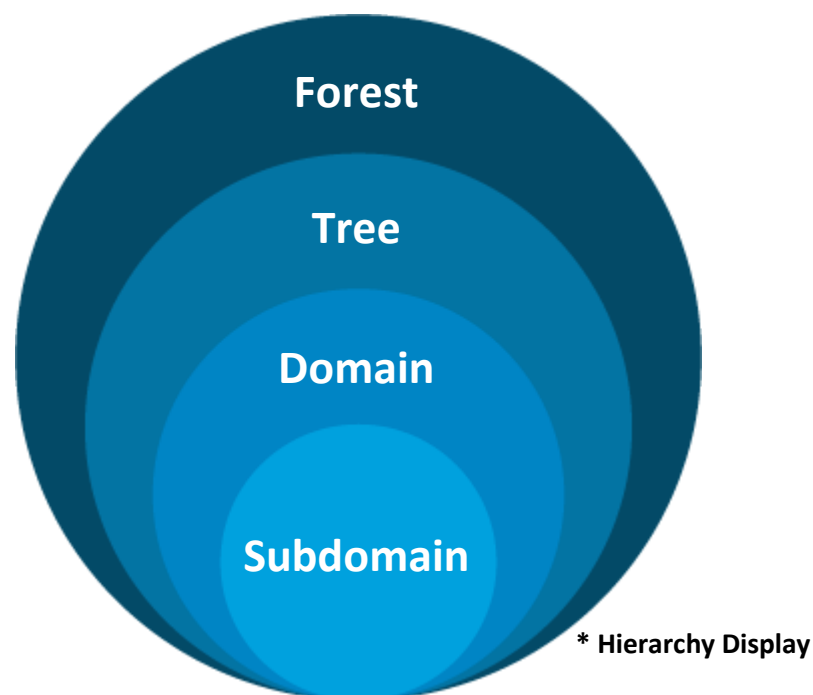
In order to unify a group of devices under the same domain, only enabling the AD services is not enough. The next step will be to promote the relevant server we use to a DC.


This promotion process is the action of actually setting the Domain for our devices.

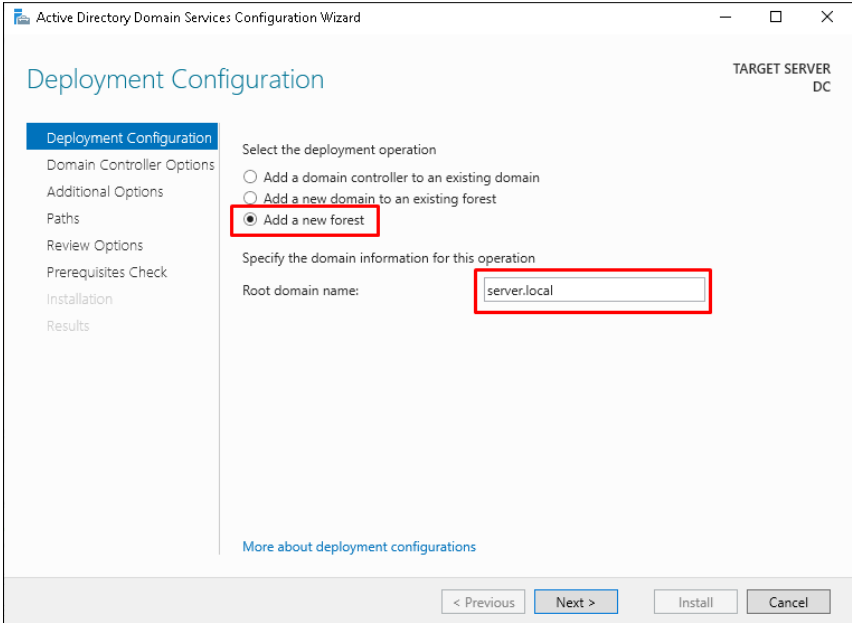
By enabling DC features we are giving ourselves the capability to control the devices and the users who will have access to our domain as a group.

The relationship for domains management is usually described by a tree model, from the Biggest to smallest;

- Forest- A group of Trees that are connected together.
- Tree- A group that contains the Domain and his Sub Domains.
- Domain- The domain name for a group of devices. For example; google.com
- Subdomain- Usually a service or a sub function in the domain.  
For example; mail.google.com



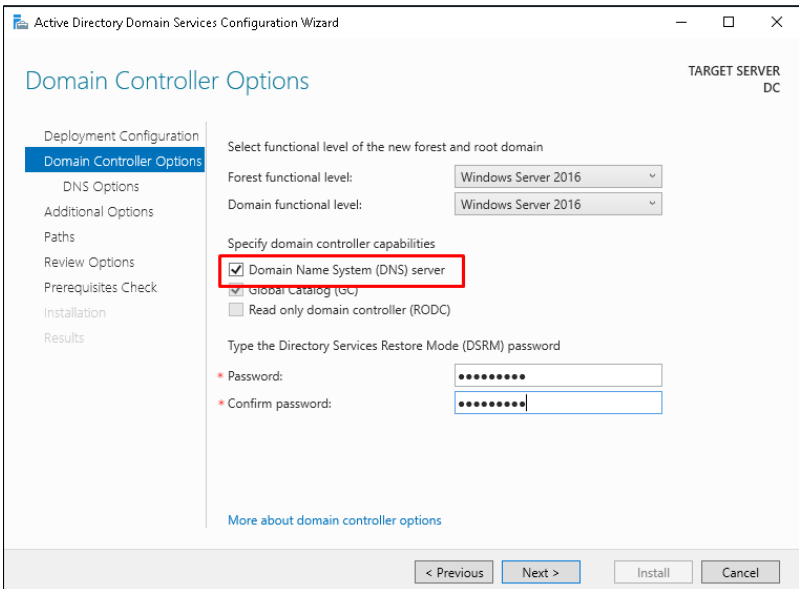
- 1) Click on the flag icon 
- 2) Press on "**Promote this server to a domain controller**".
- 3) Because this is our first Domain in a Forest, choose the "**Add a new forest**" option and name your Domain;



The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window, specifically the 'Deployment Configuration' step. The left sidebar lists various steps, with 'Deployment Configuration' selected. The main area has a section 'Select the deployment operation' with three radio buttons: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest', and 'Add a new forest'. The 'Add a new forest' option is selected and highlighted with a red box. Below this, the 'Specify the domain information for this operation' section has a 'Root domain name:' label and a text box containing 'server.local', which is also highlighted with a red box. At the bottom, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'.

- For this tutorial, we named our domain *server.local*
- Press "**Next**" when done.

- 4) Make sure that the checkbox for "**Domain Name System (DNS) server**" is marked.



The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window, specifically the 'Domain Controller Options' step. The left sidebar lists various steps, with 'Domain Controller Options' selected. The main area has a section 'Select functional level of the new forest and root domain' with two dropdown menus: 'Forest functional level' and 'Domain functional level', both set to 'Windows Server 2016'. Below this, the 'Specify domain controller capabilities' section has three checkboxes: 'Domain Name System (DNS) server' (checked and highlighted with a red box), 'Global Catalog (GC)', and 'Read only domain controller (RODC)'. At the bottom, there are fields for 'Type the Directory Services Restore Mode (DSRM) password' with 'Password:' and 'Confirm password:' labels, each followed by a masked password input field. At the bottom right, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'.

- Press "**Next**" after setting a password.

- 5) Click "**Next**" until you reach the "**Install**" button and press it.
  - Once the installation process is done, the server will perform a reset.



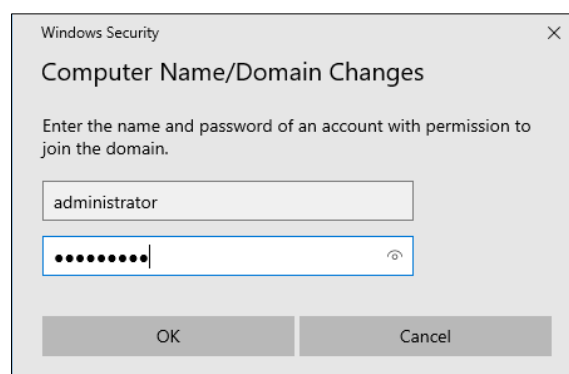
- When you login to the server the convention we semi-auto enabled for our domain in this process will be shown. In our case- **SERVER\**
- In our installation, we also installed DNS features. Later on, we will elaborate about them.

### Adding Devices to a Domain

- 1) On the relevant Windows device, go to **Control Panel\System and Security\System**
- 2) Under the "**Computer name, domain and work group settings**" section- Click on "**Change Settings**".

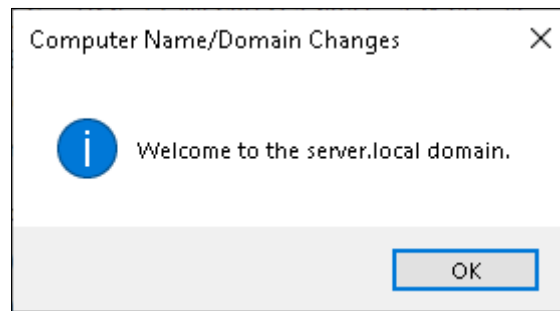


- 3) Under the "**Computer Name**" tab, click on the "**Change**" button.
- 4) Instead of the "**Workgroup**" option, choose "**Domain**" and input your domain name. In our case- **server.local**
- 5) Input your admin credentials for DC server into the login window that will appear.





6) If the credentials you input are correct the following message should appear.



- After your device will restart itself, the new full computer name should be the name of the relevant device with the addition of the domain.

Computer name, domain, and workgroup settings

Computer name: WIN10  
Full computer name: WIN10.server.local  
Computer description:  
Domain: server.local

Computer name, domain, and workgroup settings

Computer name: SRV1  
Full computer name: SRV1.server.local  
Computer description:  
Workgroup: server.local

- For this tutorial, we added **WIN10** and **SRV1** to *server.local*


## Setting Permissions

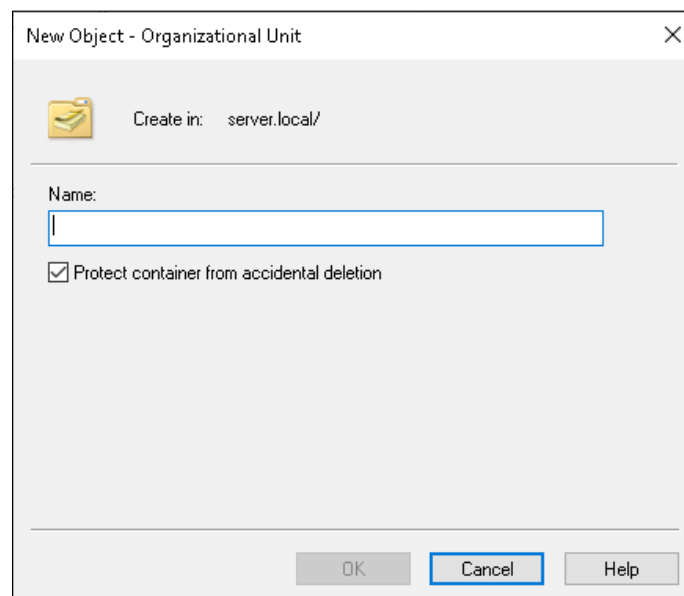
Next, we'll start with creating user credentials for our domain and unifying them according to their Organizational Unit (OU). This unification will give us better control over the permissions we would like to allocate to different groups in our organization.

In general, we have two types of permission groups for our server:




- Container Permissions- Containers are services and resources that are being used by the OS. Due to their functionality, you cannot apply or edit any group permissions for them.
- OU Permissions- According to your organization needs you can create as much of OUs as you need. OUs enable you to customize group permissions and you can add them to a Container.

### Creating an OU

- 1) On **DC** server, open the Server Manager application.
- 2) At the top right corner, click on the "**Tools**" tab and choose- "**Active Directory Users and Computers**".
- 3) Right click on the server icon  server.local - Click on "**New**" and choose "**Organizational Unit**".
- 4) Name your OU.

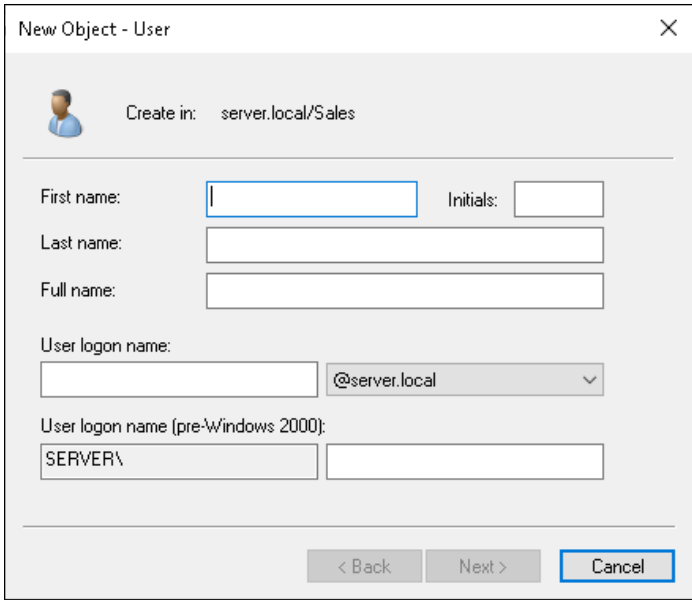


- If you keep the checkbox "**Protect container from accidental deletion**" checked you will not be able to delete it unless you uncheck this feature for your OU. In order to remove this feature, please follow these [instructions](#).

- 5) Once approved you will see your new OU with this icon- 
- For this tutorial, we created two OUs;  Sales  SysAdmin

### Creating a User

- 1) On **DC** server, open the Server Manager application.
- 2) At the top right corner, click on the "**Tools**" tab and choose- "**Active Directory Users and Computers**".
- 3) Choose the OU you want to add a user to.
- 4) Right click on the relevant OU, click on "**New**" and choose "**User**".
- 5) Input the user's credentials;



New Object - User

Create in: server.local/Sales

First name:  Initials:

Last name:

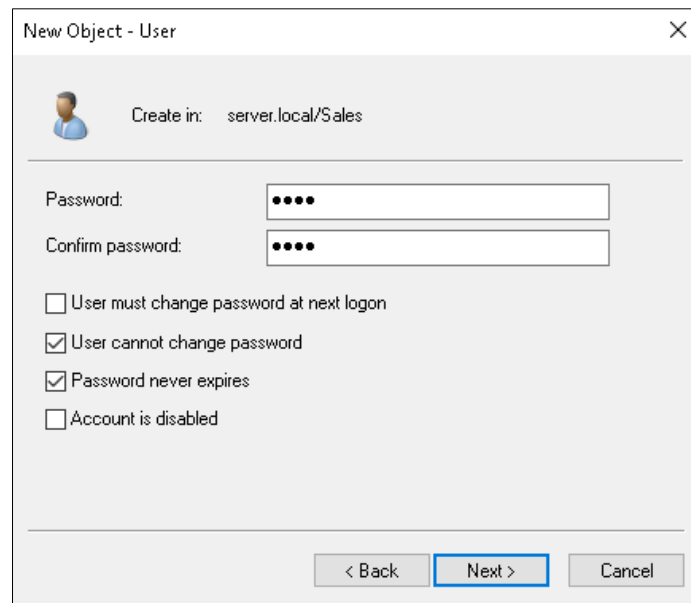
Full name:

User login name:  @server.local

User login name (pre-Windows 2000):  SERVER\

< Back Next > Cancel

6) Configure the rules for the user's password;



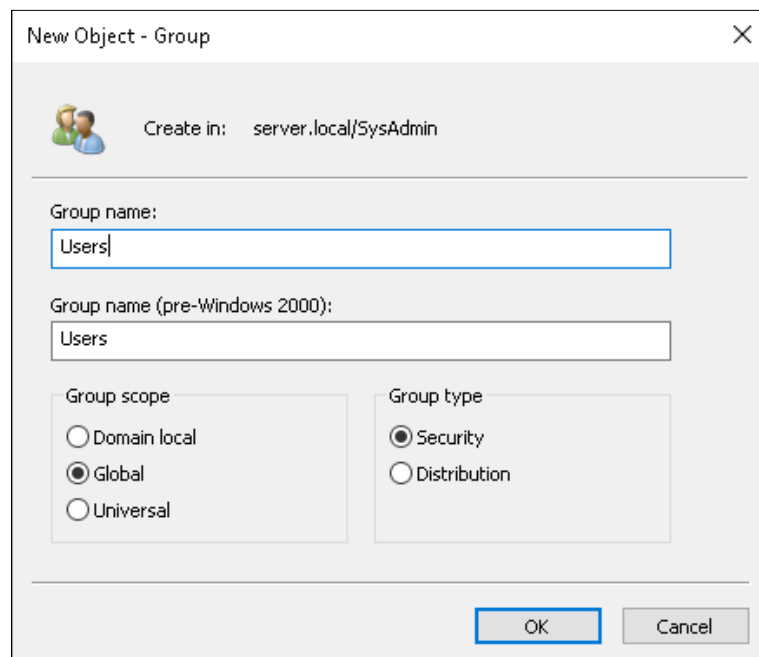
- For this tutorial, we are using two password rules;
  - **"User cannot change password"**
  - **"Password never expires"**

7) Press **"Next"** and then **"Finish"**.

- For this tutorial, we created four users:
  - ***user1*** and ***user2*** for the ***Sales*** OU.
  - ***user3*** and ***user4*** for the ***SysAdmin*** OU.

### Adding an OU to a Container

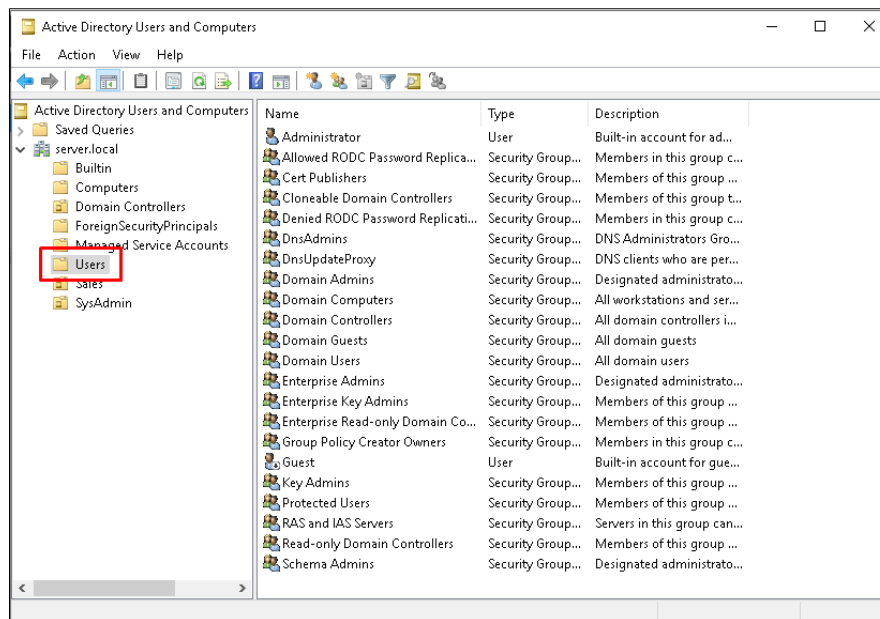
- 1) On **DC** server, open the Server Manager application.
- 2) At the top right corner, click on the "**Tools**" tab and choose- "**Active Directory Users and Computers**".
- 3) Choose the OU you want to add a group to.
- 4) click on the relevant OU, click on "**New**" and choose "**Group**".



The screenshot shows the 'New Object - Group' dialog box. At the top, it says 'Create in: server.local/SysAdmin'. Below this, there are two text boxes for 'Group name:' and 'Group name (pre-Windows 2000):', both containing the text 'Users'. Under 'Group scope', there are three radio buttons: 'Domain local', 'Global' (which is selected), and 'Universal'. Under 'Group type', there are two radio buttons: 'Security' (which is selected) and 'Distribution'. At the bottom right, there are 'OK' and 'Cancel' buttons.

- 5) Right click on a group of users inside the OU, choose "**Add to a group**" and add the users to the group you just created.

6) Click on the "**Users**" container directory



- For this tutorial, we specifically chose the "**Users**" container and a policy inside it. You can choose other Container directories and their respective policies as well.

7) Right click on "**Domain Users**" and choose "**Properties**".

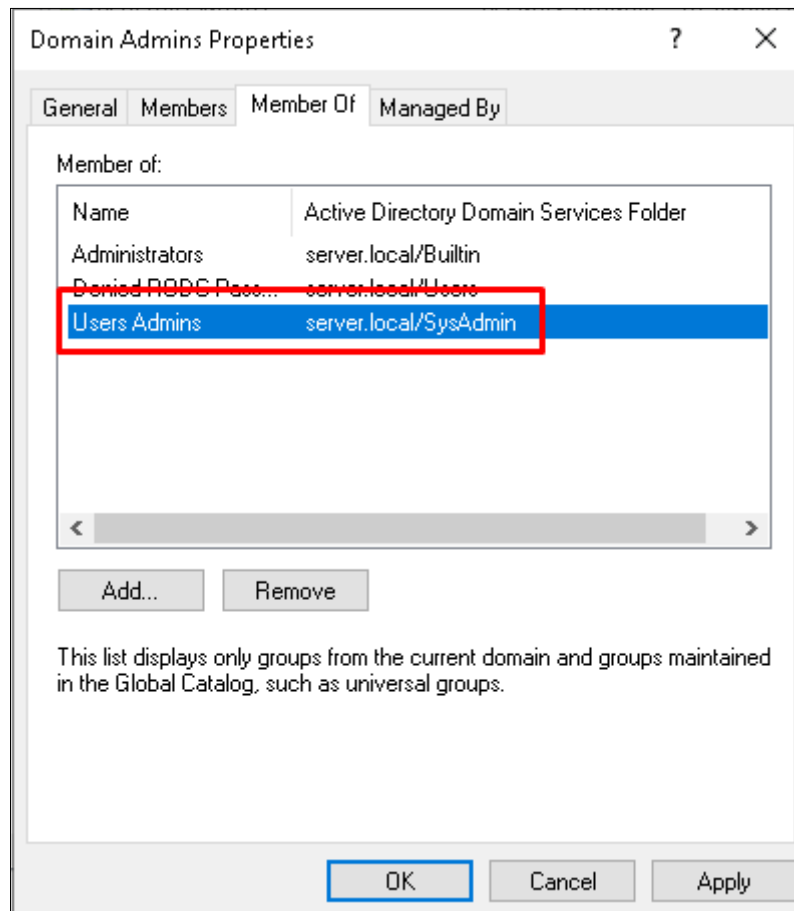
8) Under the "**Member Of**" tab, click on the "**Add**" button.

9) Click on "**Locations**" and find your OU- pick it and press "**OK**".

10) Input the group name for your users.

- In our case- **Users Admins** and **Users Sales**.

- 11) Press "**OK**", if you input the correct name of the relevant group it will be added to the "**Domain Users**" container.



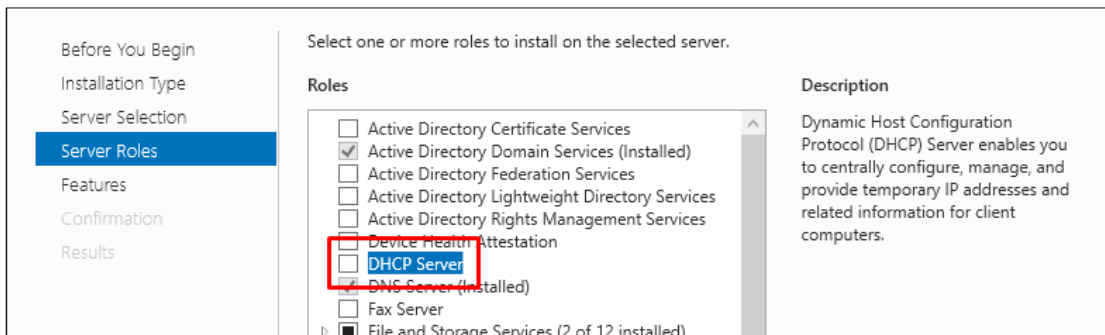
- 12) Press "**Apply**" and then "**OK**".

## DHCP

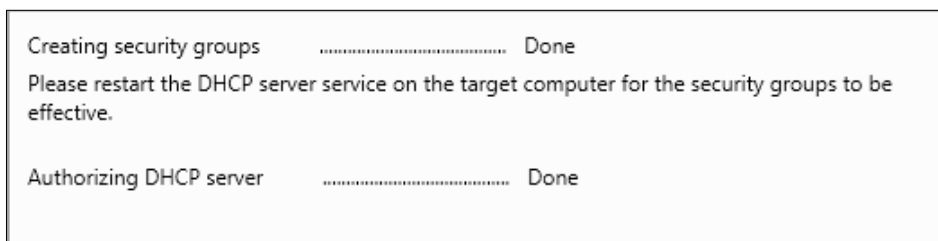
Dynamic Host Configuration Protocol (DHCP), is a protocol that helps us in managing IP addresses on a network. By enabling this feature we'll be able to assign an IP address range for a certain group, auto allocating IP addresses to devices under our network, reserve IP addresses for specific services and more.

### Enabling DHCP

- 1) On **DC** server, open the Server Manager application.
- 2) At the right top corner, click on "**manage**" and choose "**Add Roles and Features**".
- 3) Click the "**Next**" button until you reach the "**Server Roles**" Section.
- 4) Check the box for "**DHCP Server**" and press "**Add Feature**".



- 5) Click "**Next**" until you reach the "**Install**" button and press it.
- 6) At the right top corner, click on the flag icon and choose- "**Complete DHCP configuration**".
- 7) Press "**Next**" and following to that, on the "**Commit**" button.
- 8) If the configuration was successful, the following will be shown;





## Initial Setup

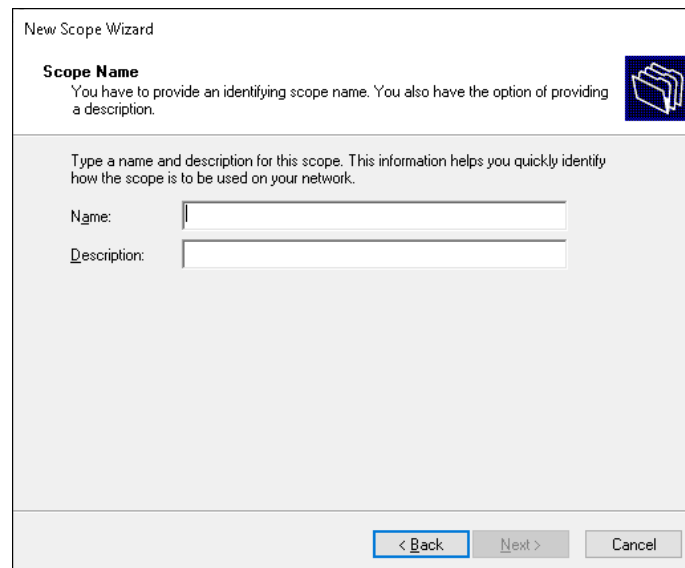
In order to begin with managing our network we need to prepare a predetermined Scope of IP addresses we need to receive from our organization in order to further configure our DHCP service before we begin with actually managing our network.

- 1) On **DC** server, open the Server Manager application.
- 2) At the top right corner, click on the "**Tools**" tab and choose "**DHCP**".
- 3) At the left bar, expand the options for your domain- Right click "**IPv4**" and choose "**New Scope**".



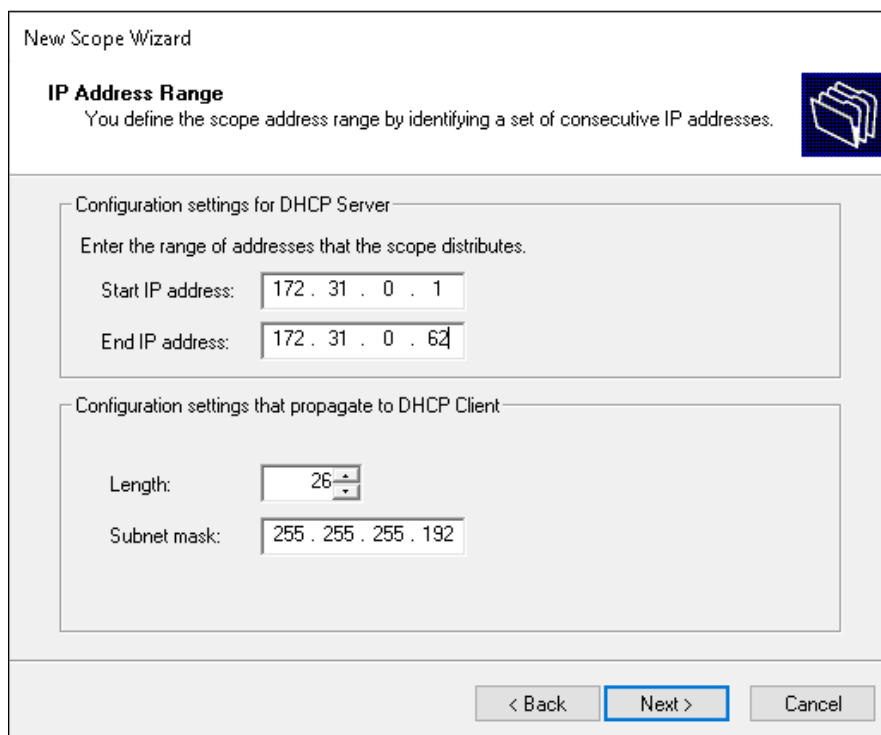
- Click on the "**Next**" Button.

- 4) Choose the name you want for your new Scope and click "**Next**".



The screenshot shows the 'New Scope Wizard' window at the 'Scope Name' step. The title bar says 'New Scope Wizard'. Below the title, there's a section header 'Scope Name' followed by the instruction: 'You have to provide an identifying scope name. You also have the option of providing a description.' To the right of this text is a blue icon of a folder. Below the instruction, there's a paragraph: 'Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.' Under this paragraph, there are two text input fields: 'Name:' and 'Description:'. At the bottom of the window, there are three buttons: '< Back' (highlighted with a blue border), 'Next >' (disabled), and 'Cancel' (disabled).

- 5) Next, we need to define the IP addresses range we are going to work with.



The screenshot shows the 'New Scope Wizard' window at the 'IP Address Range' step. The title bar says 'New Scope Wizard'. Below the title, there's a section header 'IP Address Range' followed by the instruction: 'You define the scope address range by identifying a set of consecutive IP addresses.' To the right of this text is a blue icon of a folder. Below the instruction, there are two sections. The first section is titled 'Configuration settings for DHCP Server' and contains the text 'Enter the range of addresses that the scope distributes.' followed by two text input fields: 'Start IP address:' with the value '172 . 31 . 0 . 1' and 'End IP address:' with the value '172 . 31 . 0 . 62'. The second section is titled 'Configuration settings that propagate to DHCP Client' and contains two text input fields: 'Length:' with the value '26' (which is a spinner box) and 'Subnet mask:' with the value '255 . 255 . 255 . 192'. At the bottom of the window, there are three buttons: '< Back' (disabled), 'Next >' (highlighted with a blue border), and 'Cancel' (disabled).

- The range we use contains 60 available IP addresses; A subnet mask of 255.255.255.192 like we originally defined for our devices.
- Press "**Next**" and continue on.

- 6) In the "Add Exclusion and Delay" window, we can define IPs that we don't want to be distributed to client devices from our range. This is usually being done for devices that receive a static IP address- In our case, the **DC** and **SRV1** servers.

New Scope Wizard

**Add Exclusions and Delay**

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: End IP address: Add

Excluded address range:

- Address 172.31.0.1
- Address 172.31.0.2
- Address 172.31.0.3
- Address 172.31.0.4
- Address 172.31.0.5
- Address 172.31.0.61

Remove

Subnet delay in milliseconds: 0

< Back Next > Cancel

- For this tutorial, we excluded the first 5 IP addresses in our network. In addition, you can also see that the static IPs for DC (172.31.0.1) and SRV1 (172.31.0.61) are also excluded.
- Press "**Next**" and continue on.

- 7) In the "**Lease Duration**" window we determine the time that each IP is being associated with a device on our new work. Leases can be refreshed for a device and they follow these rules:
- At 50% of the lease duration, the device that received the IP address associated to him will send a request to refresh the expiration date from the DHCP server that provided him with the relevant address.
  - At 87.5% of the lease duration, the device will send a request without a specific receiver (Broadcast) in order to detect a DHCP service that will grant him with an IP address.
  - At 100% of the lease duration, the leased duration ended and no DHCP server was detected. In this case, the relevant device will be granted with an APIPA address.
- ❖ Automatic Private Internet Protocol Address (APIPA)- A range of internal IP addresses, between 169.254.0.1 – 169.254.254.255 that are being assigned to a device if a connection to a DHCP server is not available.

New Scope Wizard

**Lease Duration**  
The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

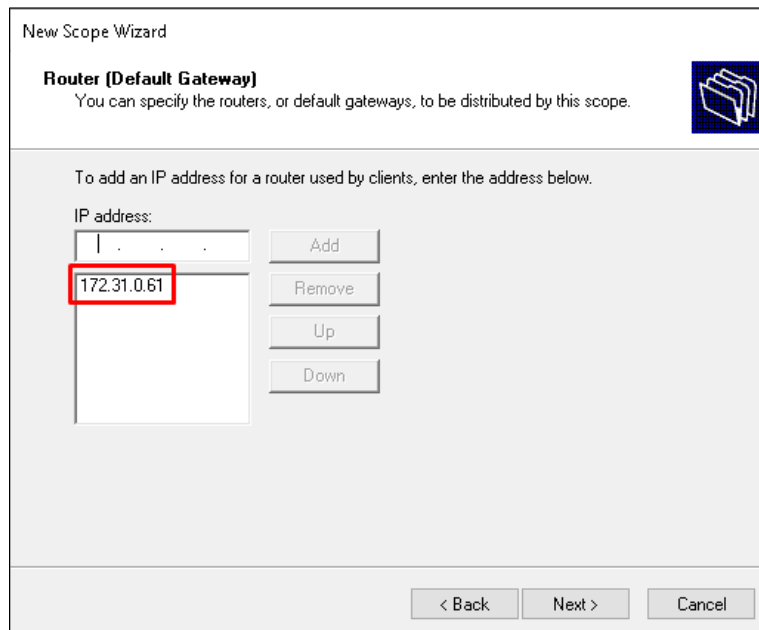
Limited to:

Days: 0 Hours: 8 Minutes: 0

< Back Next > Cancel

- For this tutorial, we defined the lease duration to eight hours.
  - Press "**Next**" and continue on.
- 8) Make sure the option "**Yes, I want to configure these options now**" is marked and press on "**Next**".

- 9) In the "**Router (Default Gateway)**" window, we define the IP addresses that are acting as our communication channel with networks that are not a part of our local environment.



New Scope Wizard

**Router (Default Gateway)**  
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

172.31.0.61

Add  
Remove  
Up  
Down

< Back   Next >   Cancel

our case **SRV1** will act as our Router (Default Gateway).  
Therefore, **SRV1**'s IP address- 172.31.0.61 was added in this section.

- Press "**Next**" and continue on.

- 10) In the "**Domain Name and DNS Servers**" window, we define the name of the main DNS server we want our clients to use and the scope.

- In our case, there is no need to do any additional adjustments.
- Press "**Next**" and continue on.

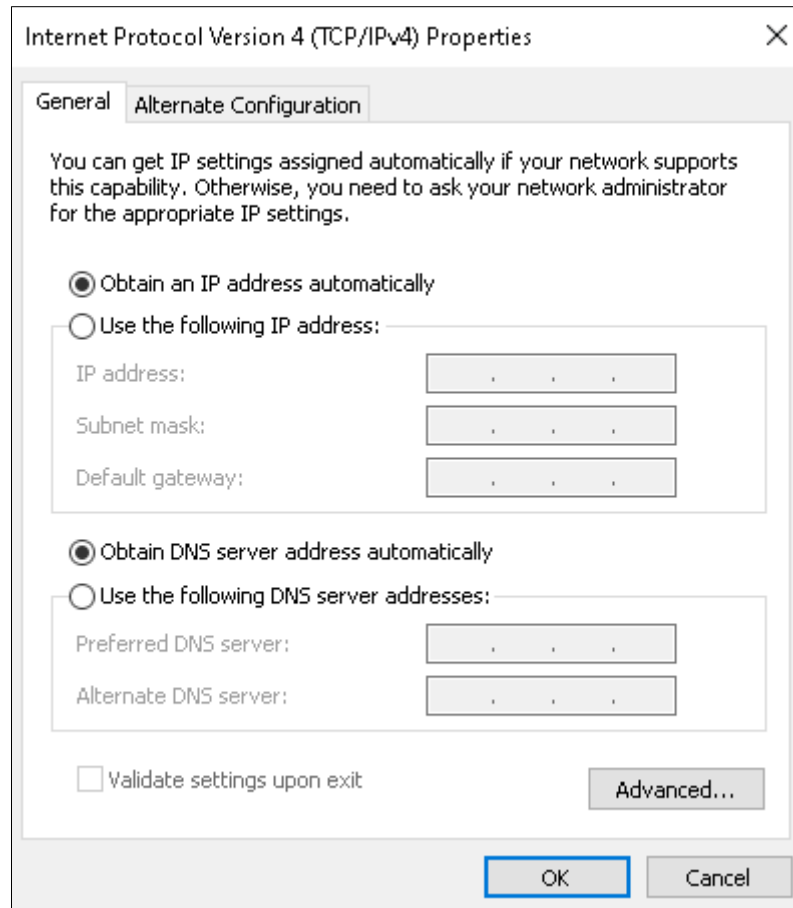
- 11) In the "**WINS Servers**" window, you can configure a specific service named Windows Internet Name Service (WINS). This service is no longer being commonly used.

- Press "**Next**" and continue on.

- 12) Press "**Next**" and finally- "**Finish**".

## DHCP IP Allocation Check

- 1) In order to check if our process was right, we'll switch the network configurations for **WIN10** back to its default configurations- Automatically receiving the IPv4 and DNS data.



- 2) Next, we will check if our client device was able to receive an IP address and a DNS server address from our DHCP.
  - i. Open Command Prompt (CMD) on the client device.
  - ii. Input the command **ipconfig** and press on Enter.
  - iii. If you correctly preformed the setup for DHCP and its Scope you should see data similar to the following:

```
Connection-specific DNS Suffix . : server.local
Link-local IPv6 Address . . . . . : fe80::40df:1d1b:1cad:8833%8
IPv4 Address. . . . . : 172.31.0.6
Subnet Mask . . . . . : 255.255.255.192
Default Gateway . . . . . : 172.31.0.61
```

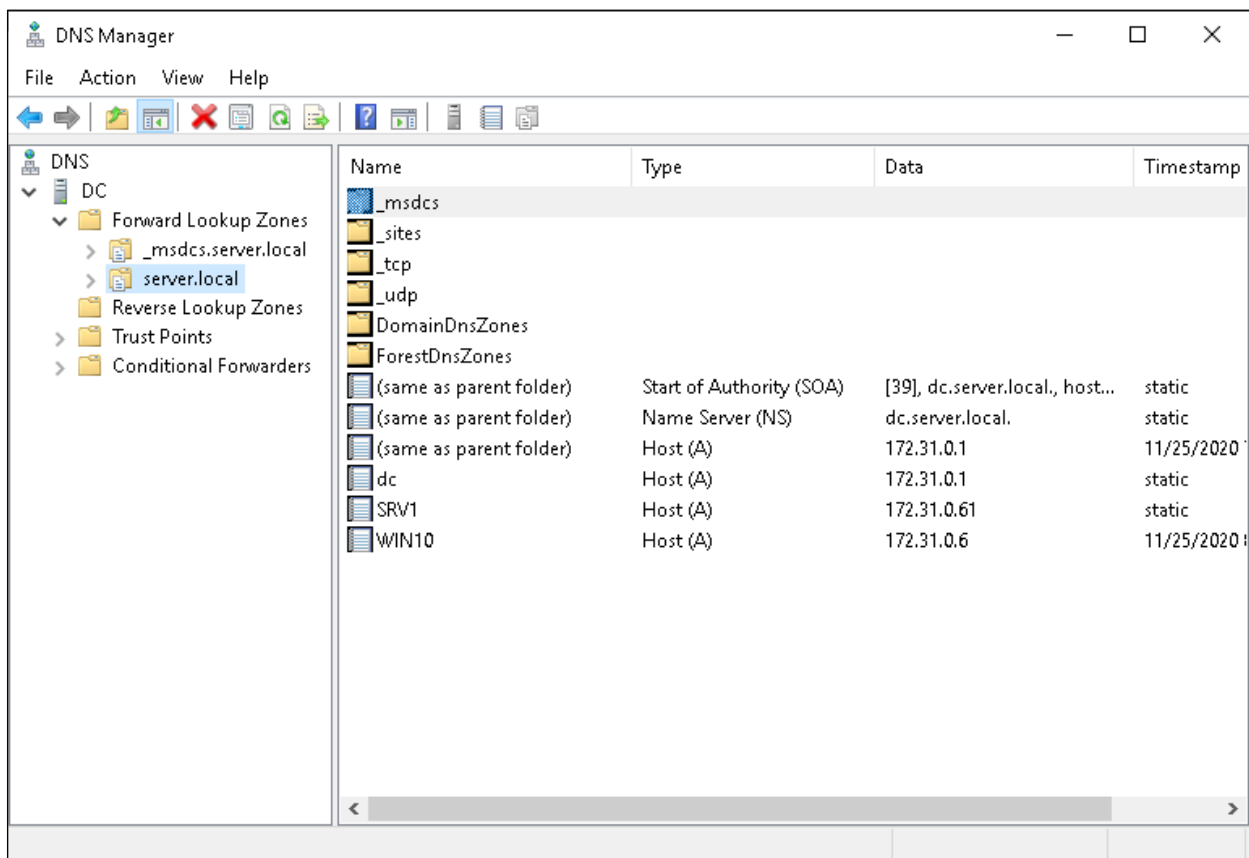
## DNS

When we installed the DC features, we also made sure to install DNS services for our server. Domain Name Server/System (DNS) mainly enables us to associate our servers IP addresses with names that humans can better remember.

In addition, DNS services give us the ability to control and manage the manner in which we handle those IP addresses with their respective names and enabling us to send requests to devices that are outside of our local network.

In order to better understand the basic DNS features, there are several definitions that we must talk about first;

- 1) On **DC** server, open the Server Manager application.
- 2) At the top right corner, click on the "**Tools**" tab and choose "**DNS**".



- **Forward Lookup Zone**- Responsible for translating Domain Names to IP addresses.
- **\_msdcs...**- Configurations that are internally integrated in our DNS and are a part of the Active Directory (AD).
- **server.local**- Our domain, all of the definitions that are relevant to the devices under our domain will be located here.
- **Host(A)**- A (IPv4) or AAAA (IPv6) Records; Each one contains an IP address and the domains associated to him.

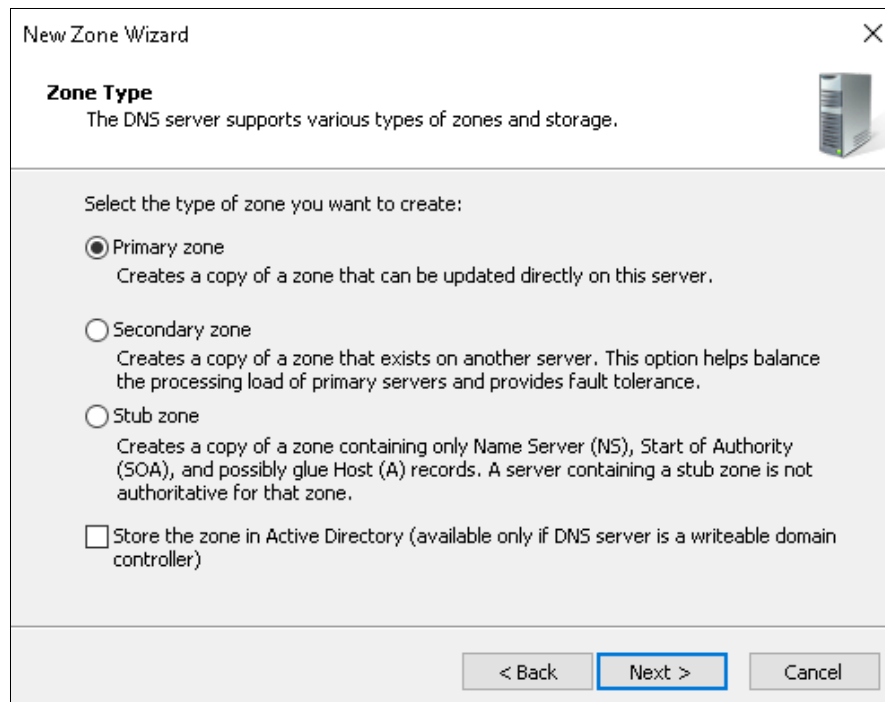
- **CNAME**- Canonical Name, also called Alias; The function of adding another domain name that will be connected to an existing record. Multiple names can be connected to the same IP address.
- **MX**- Mail Exchanger, creating this record will create a domain name that will be associated with a mail server.
- **PTR checkbox in a record**- Pointer Records enables us to search for a network from IP to domain. Also needs to be created in the Reverse Lookup Zone.
- **Reverse Lookup Zone**- Responsible for translating IP addresses to domains names.
- **PTR Records**- Each contain an IP address and the domains associated with him.
- **SOA**- Start Of Authority, the DNS server sync; Determining the primary server between multiple DNS servers and the TTL configs for the relevant DNS.
- **NS**- Name Server, another server (secondary) that provides DNS services or is being used as a fail safe for a primary DNS record.
- **Conditional Forwarders**- Used for setting an IP address or a non-existing address with an existing domain.
- **Zone Transfers**- Dedicated for zones that are not on AD. Allows the secondary zone (DNS server) to receive updates from the Master zone. A Master zone can be any type of zone (Primary/Secondary/AD).
- **Forwarders**- Addresses of remotes DNS servers that aren't located in our network and we would like our DNS servers to contact them for cases when they are not able to detect the domain and IP address a device on out network was looking for.

Next, we'll set some basic configuration for our DNS server on the DC device.



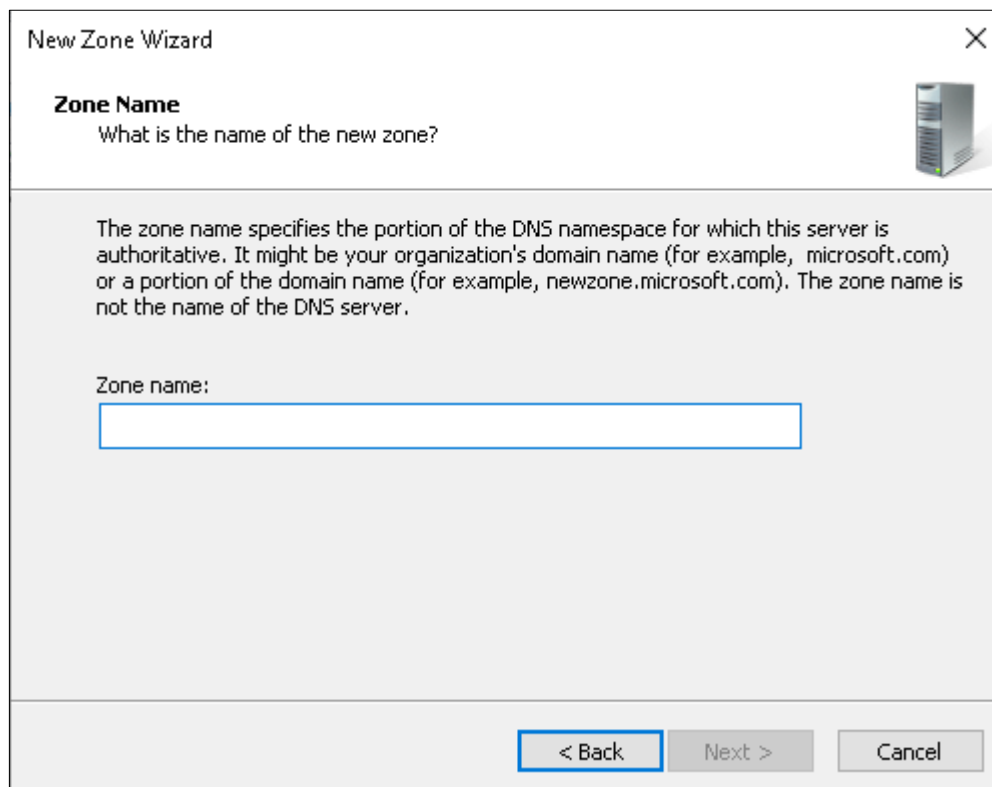
## Creating a New Forward Lookup Zone

- 1) On **DC** server, open the Server Manager application.
- 2) At the top right corner, click on the "**Tools**" tab and choose- "**DNS**".
- 3) Right click on the "**Forward Lookup Zones**" directory and choose "**New Zone**".
- 4) Click "**Next**" and choose your zone functionality according to your needs.



- For this tutorial, we will need a new primary zone that we don't want it to be associated with our AD. Therefore, we chose the option of "**Primary zone**" and removed the check box that ask whether to store the zone in AD.
- Press "**Next**" and continue on.

5) Name your zone.



The image shows a Windows-style dialog box titled "New Zone Wizard". It has a close button (X) in the top right corner. Below the title bar, there is a section titled "Zone Name" with a server icon to its right. The text asks "What is the name of the new zone?". Below this, a paragraph explains that the zone name specifies the portion of the DNS namespace for which the server is authoritative, giving examples like "microsoft.com" or "newzone.microsoft.com", and noting that it is not the name of the DNS server. A text input field is labeled "Zone name:". At the bottom, there are three buttons: "< Back" (highlighted with a blue border), "Next >" (disabled), and "Cancel" (disabled).

New Zone Wizard

**Zone Name**  
What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:

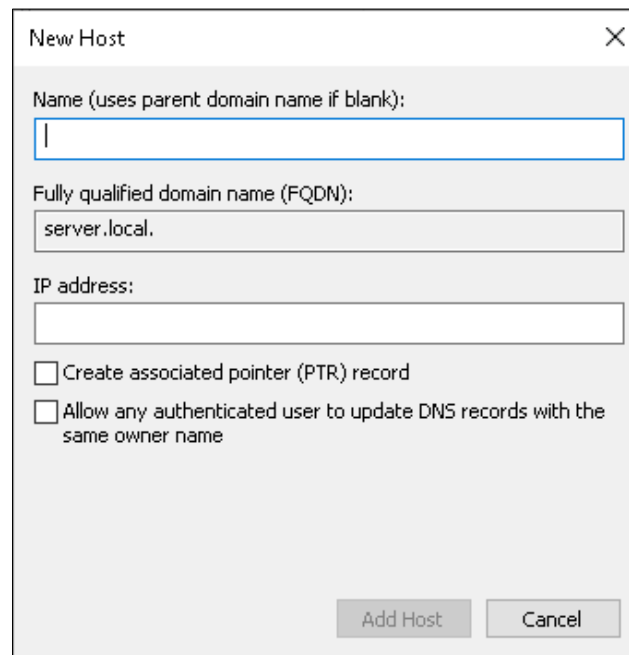
< Back   Next >   Cancel

- Press "**Next**" and continue on.

6) Press "**Next**" until you reach the final window, press on "**Finish**".

## Creating a Host(A) Record

- 1) On **DC** server, open the Server Manager application.
- 2) At the top right corner, click on the "**Tools**" tab and choose "**DNS**".
- 3) Choose the relevant zone you want to add a Host(A) for it.
  - In our case we will add a record to **server.local**
- 4) Right click on the relevant zone and choose "**New Host (A or AAAA)**".
- 5) Input the Domain Name and IP address you would like to be associated together.



The screenshot shows the 'New Host' dialog box with the following fields and options:

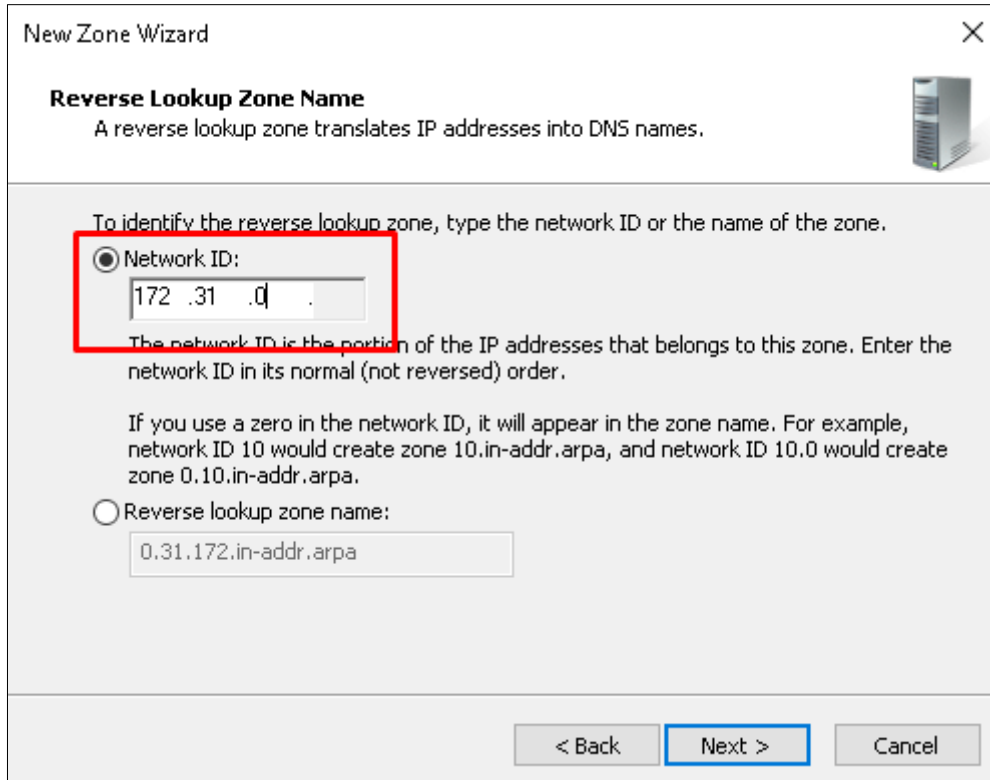
- Name (uses parent domain name if blank):** A text box containing a single vertical bar '|'.
- Fully qualified domain name (FQDN):** A text box containing 'server.local'.
- IP address:** An empty text box.
- ☐ Create associated pointer (PTR) record
- ☐ Allow any authenticated user to update DNS records with the same owner name
- Buttons:** 'Add Host' and 'Cancel' at the bottom right.

- 6) Once you are done, click on "**Add Host**".

## Enabling Reverse Lookup Zone

This feature is not automatically enabled once you enable DNS features for your server. In order to enable Reverse Lookup Zone;

- 1) On **DC** server, open the Server Manager application.
- 2) In the top right corner, click on the "**Tools**" tab and choose- "**DNS**".
- 3) Right click on "**Reverse Lookup Zone**" and choose "**New Zone**".
- 4) Click on "**Next**" until you reach a window that lets you configure your Network ID.



New Zone Wizard

**Reverse Lookup Zone Name**  
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

☒ Network ID:  
172 .31 .0 .

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

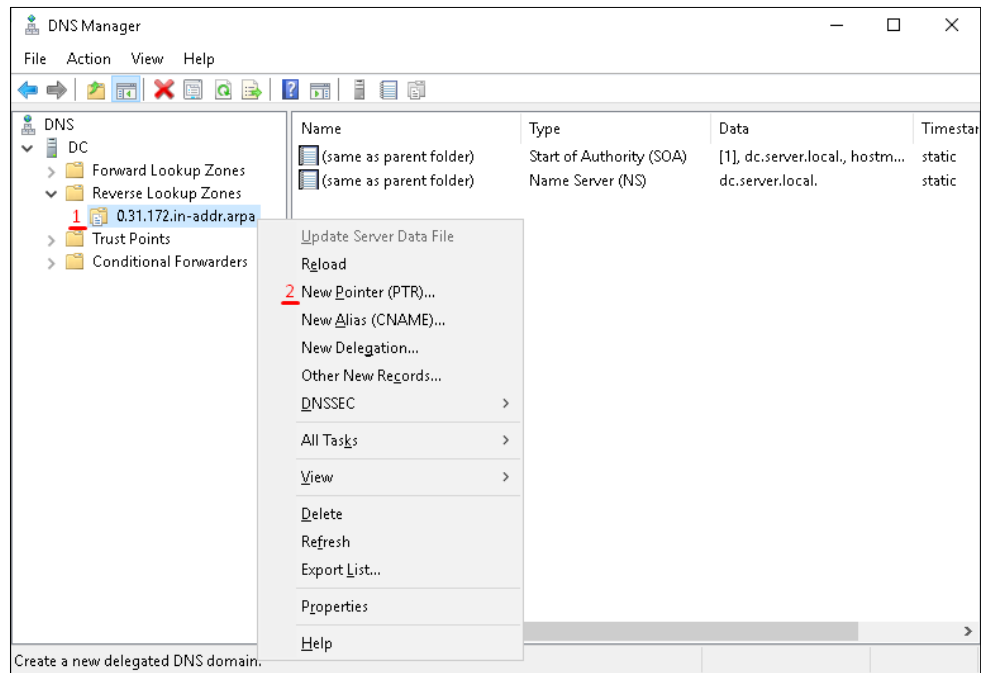
☐ Reverse lookup zone name:  
0.31.172.in-addr.arpa

< Back Next > Cancel

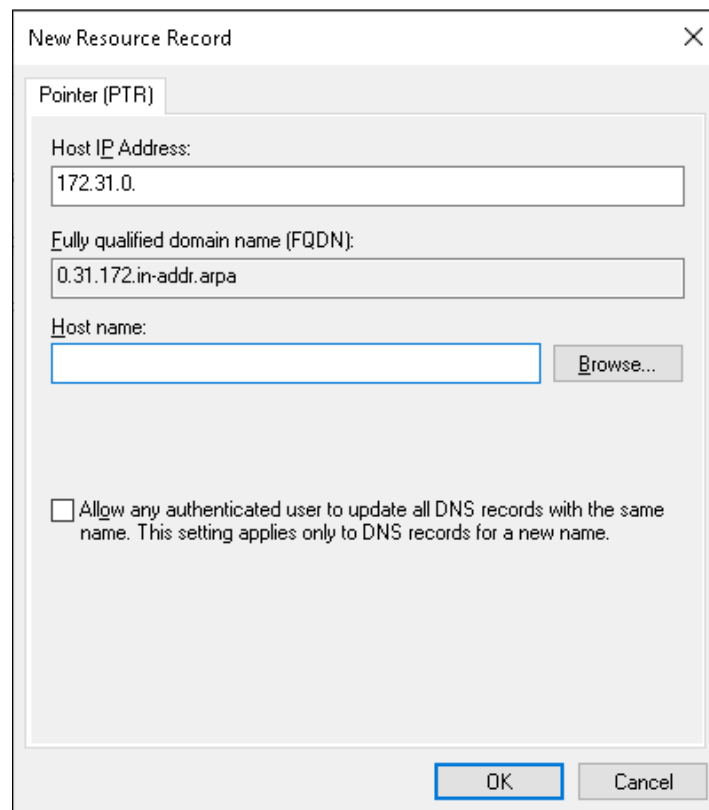
- Configure your Network ID according to your scope.
  - For this tutorial, the IP address zone we'll use is **172.31.0**
  - Press "**Next**" and continue on.
- 5) Press "**Next**" and finally "**Finish**".

## Creating a PTR Record

- 1) On **DC** server, open the Server Manager application.
- 2) In the top right corner, click on the "**Tools**" tab and choose- "**DNS**".
- 3) Click on "**Reverse Lookup Zone**" and choose a zone.
  - In our case, the zone we just created- **0.31.172-addr.arpa**
- 4) Right click on the relevant zone and choose "**New Pointer (PTR)**".



5) Input the IP address and Domain Name you want to be associated together.

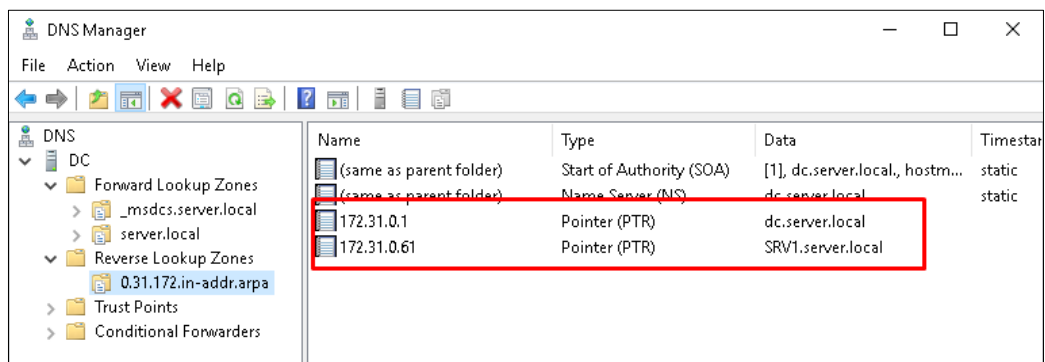


The 'New Resource Record' dialog box is shown with the 'Pointer (PTR)' tab selected. It contains the following fields and options:

- Host IP Address:** 172.31.0.
- Fully qualified domain name (FQDN):** 0.31.172.in-addr.arpa
- Host name:** (empty text box) with a 'Browse...' button.
- ☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.
- Buttons:** OK and Cancel.

- For this tutorial, we'll input two PTR records to our Reverse Lookup Zone. One for **DC.server.local** and the other for **SRV1.server.local**
- When you are done for configuring, press "OK".

6) When you complete the process, a new PTR record should appear.



The DNS Manager console shows the hierarchy: DNS > DC > Reverse Lookup Zones > 0.31.172.in-addr.arpa. The main pane displays a table of DNS records.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[1], dc.server.local., hostm...	static
(same as parent folder)	Name Server (NS)	dc.server.local	static
172.31.0.1	Pointer (PTR)	dc.server.local	
172.31.0.61	Pointer (PTR)	SRV1.server.local	

## Setting a Conditional Forwarding

Setting an existing domain with an IP address that's not being used.

By doing so, we are blocking our clients from accessing the relevant domain.

- 1) On **DC** server, open the Server Manager application.
- 2) At the top right corner, click on the "**Tools**" tab and choose "**DNS**".
- 3) Right click on "**Conditional Forwarders**" and press on "**New Conditional Forwarder**".
- 4) Input a Domain name and an IP address that's not currently being used.

The screenshot shows the 'New Conditional Forwarder' dialog box. The 'DNS Domain' field contains 'facebook.com'. Below it, the 'IP addresses of the master servers' section contains a table with one entry: IP Address '172.31.0.60', Server FQDN '<Unable to resolve>', and Validated 'A timeout occurred during v.'. To the right of the table are buttons for 'Delete', 'Up', and 'Down'. Below the table is a checkbox 'Store this conditional forwarder in Active Directory, and replicate it as follows:' which is checked. Below this checkbox is a dropdown menu showing 'All DNS servers in this forest'. A warning icon and text state: 'This will not replicate to DNS servers that are pre-Windows Server 2003 domain controllers'. Below this is a field 'Number of seconds before forward queries time out:' with the value '5'. At the bottom right are 'OK' and 'Cancel' buttons.

IP Address	Server FQDN	Validated
<Click here to add a...>		
172.31.0.60	<Unable to resolve>	A timeout occurred during v.

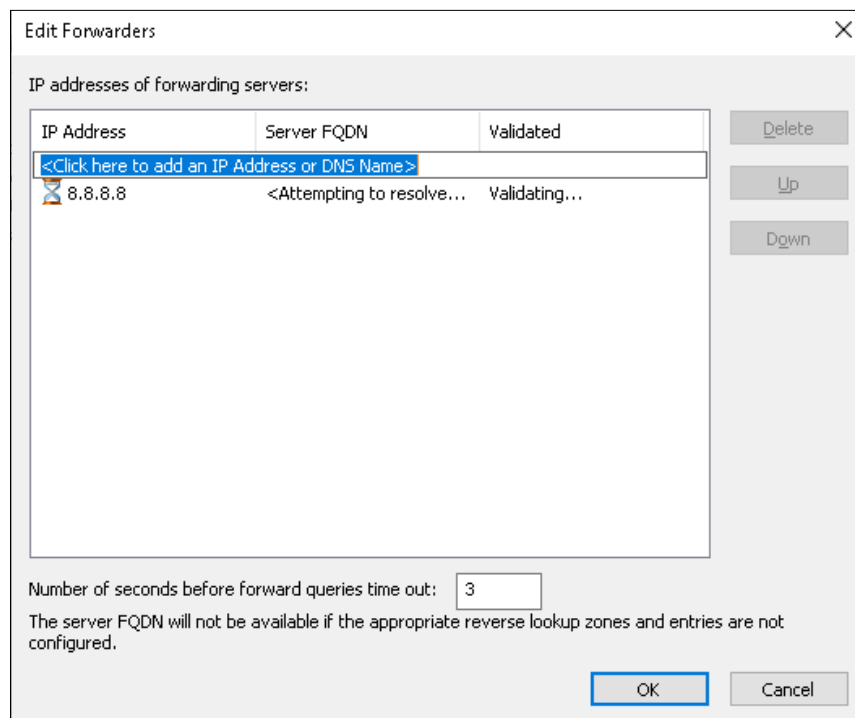
- For this tutorial, we set **facebook.com** with IP address **172.31.0.60**.
- Since this condition is being applied in our AD server, you need to mark the "**Store this conditional forwarder in Active Directory...**" checkbox in order to approve the process.

- 5) Press "**OK**" once you are done.

## Setting Forwarders

Enables us to make sure our DNS server will have the option to ask another DNS server about domains that he will not be able to locate- IPs and their associated domains.

- 1) On **DC** server, open the Server Manager application.
- 2) In the top right corner, click on the "**Tools**" tab and choose- "**DNS**".
- 3) Right click on your DNS server name, in our case "**DC**" and choose "**Properties**".
- 4) Under the "**Forwarders**" tab, click on "**Edit**".
- 5) Input the IP address of the remote server you wish to send queries to in case our DNS will fail to find the domain and IP address.



- For this tutorial, we added a Google DNS IP address- **8.8.8.8**
  - Press "**OK**" once you are done.
- 6) Press "**Apply**" and finally "**OK**".



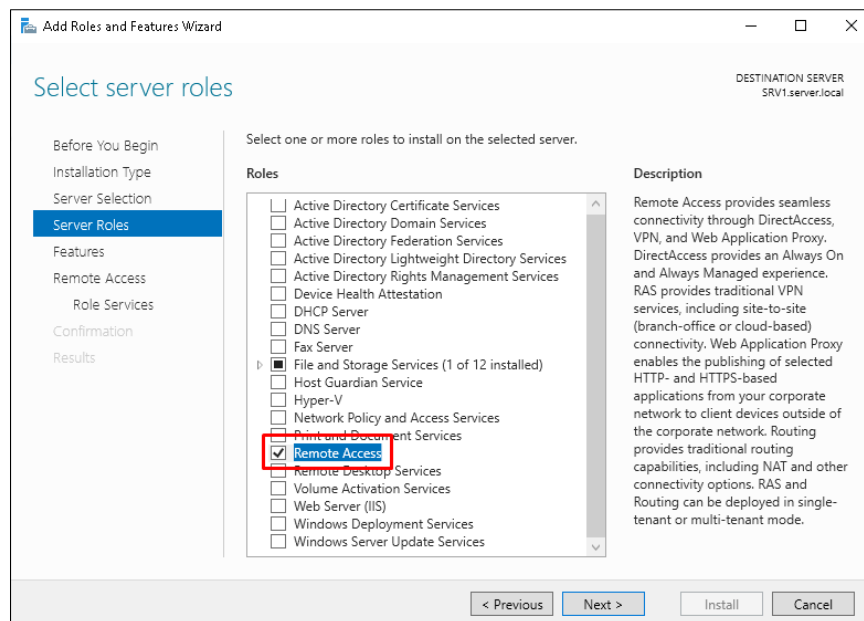
## Network Connection

### Setting a Connection

Now we will establish a network connection for our environment. We will do this by setting **SRV1** as a Router that will connect us to other networks.

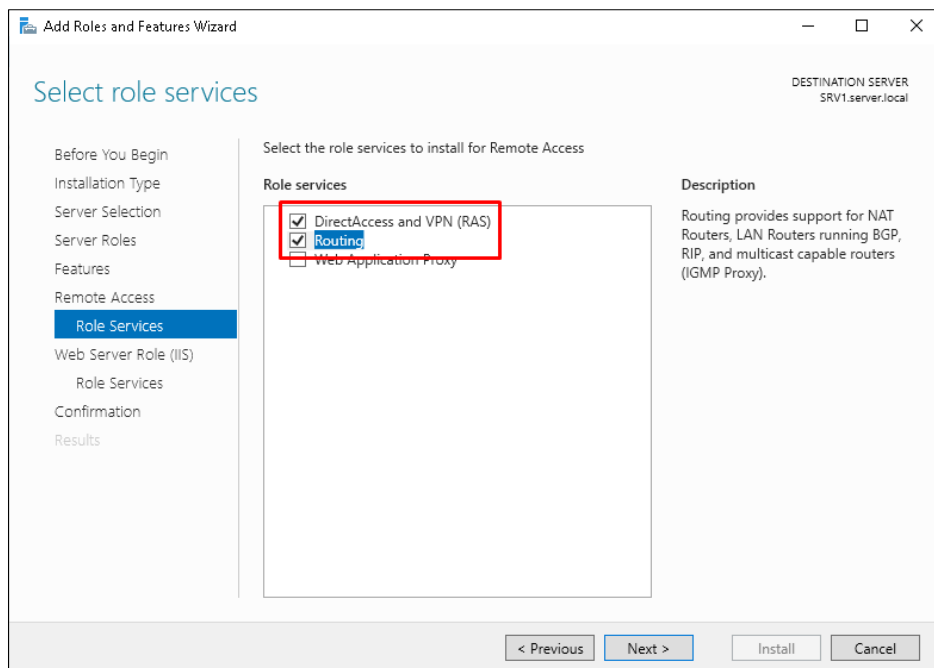
In order to establish this connection, you must have a physical connection already set.

- 1) On **SRV1** server, open the Server Manager application.
- 2) In the top right corner, click on the "**Manage**" tab and choose- "**Add Roles and Features**".
- 3) Click "**Next**" until you reach the "**Server Roles**" section.



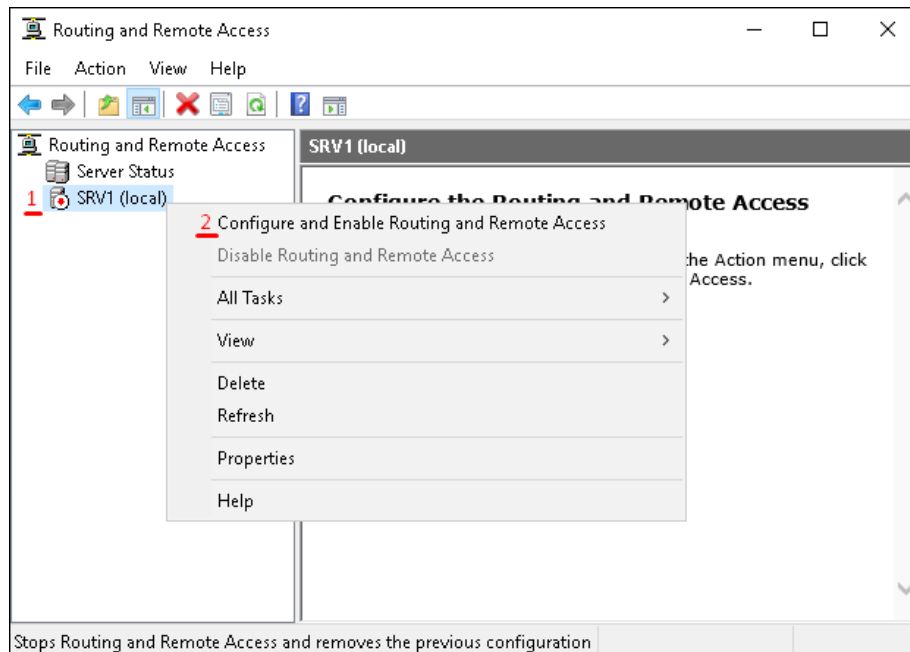
- Mark the "**Remote Access**" checkbox and press on "**Next**".

4) Press "**Next**" until you reach the "**Role Services**" section.

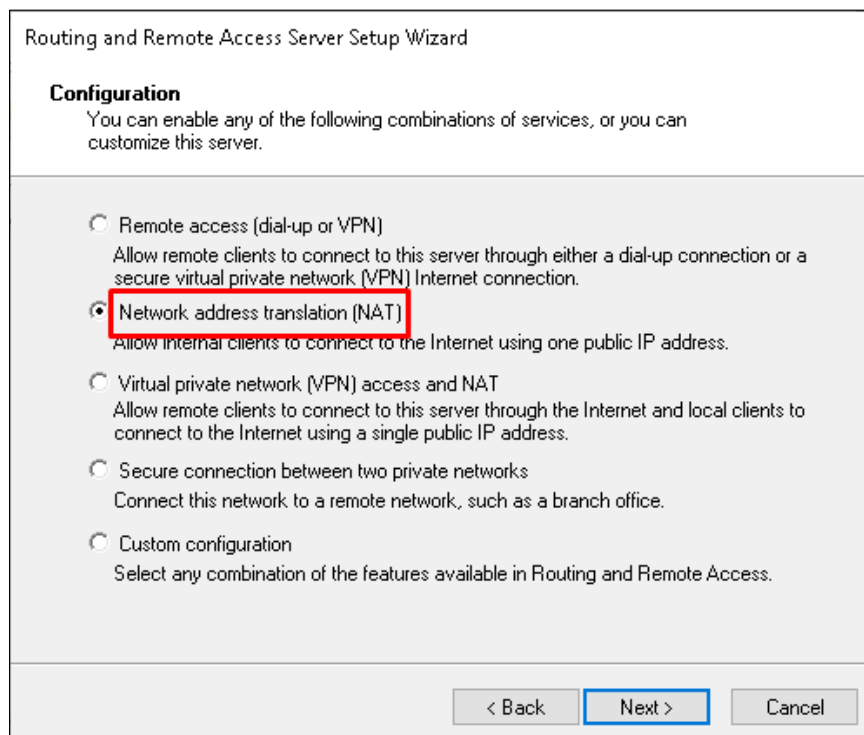


- Check the box for "**Routing**" and press on "**Add Features**" in the window that will appear.
  - Pay attention, this action will also add the "**DirectAccess and VPN (RAS)**" service.
  - Press "**Next**" and continue on.
- 5) Press "**Next**" until you reach the "**Confirmation**" section, finally press on "**Install**".
- 6) Once the installation is complete, go to "**Tools**" at the Server Manager application and choose "**Routing and Remote Access**".
- You can ignore the flag raised in the Server Manager's main page.

- 7) Right click on the connection that has your server name and press on-  
**"Configure and Enable Routing and Remote Access"**.



- 8) Click **"Next"** and choose in the **"Configuration"** window the-  
**"Network address translation (NAT)"** option.



- Press **"Next"** and continue on.

- 9) In the "**NAT Internet Connection**" window, we are selecting the interface we are using in order to establish connection with other networks (Internet).

Routing and Remote Access Server Setup Wizard

**NAT Internet Connection**  
You can select an existing interface or create a new demand-dial interface for client computers to connect to the Internet.

☒ Use this public interface to connect to the Internet:

Network Interfaces:

Name	Description	IP Address
Ethernet0	Intel(R) 82574L Gigabit	172.31.0.61
Ethernet1	Intel(R) 82574L Gigabit...	192.168.139.130 (DHCP)

☐ Create a new demand-dial interface to the Internet  
A demand-dial interface is activated when a client uses the Internet. Select this option if this server connects with a modem or by using the Point-to-Point Protocol over Ethernet. The Demand-Dial Interface Wizard will start at the end of this wizard.

< Back Next > Cancel

- For this tutorial, we created our environment using a Virtual Machine (VM). The connection we are establishing in this case is through the computer we are using; therefore, we received a local IP address (192.168.139.130) from that device. In order to create a connection through, it to the Internet.
- In cases you don't see the list of available IPs, simply cancel the process and fully repeat it again.
- Press "**Next**" and continue on.

- 10) Click on "**Finish**".

- There is a possibility that the connection will not work even though you followed this guide correctly. In this case, turn **DC** and **SRV1** off and on again and the error should be resolved.

## Checking Connectivity

In order to check whether our installations and configurations succeeded, we will open our client device (**WIN10**) and check whether everything is working as expected;

A few basic commands we will be using for our tests:

**ping** – A command that enables us to check connectivity with other devices.

**ipconfig** – Will display to you some basic information on your network.

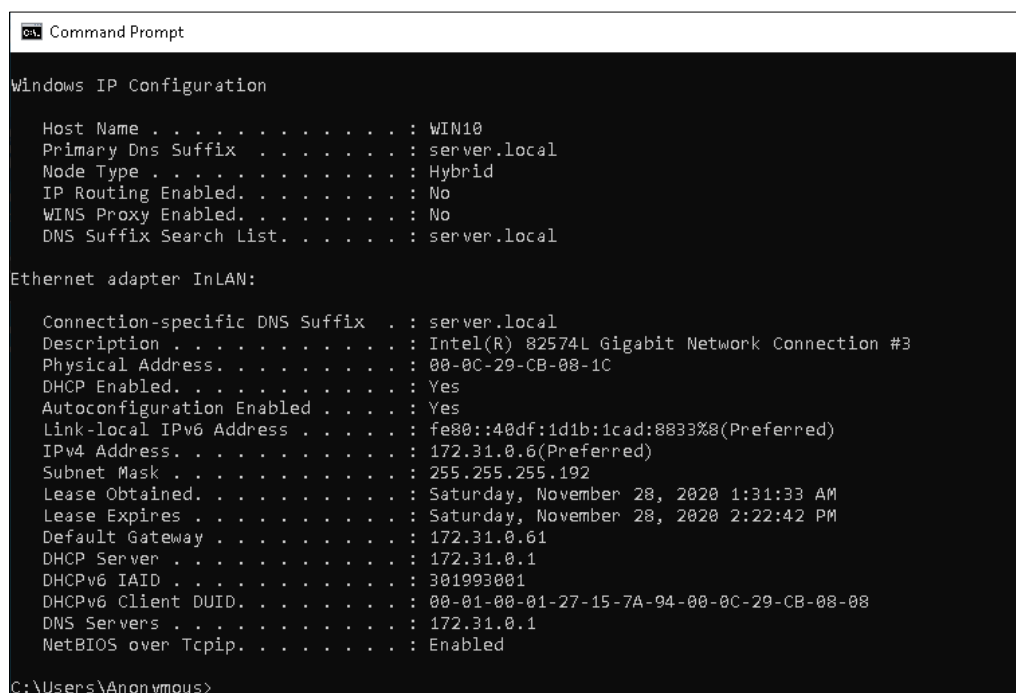
**ipconfig /all** – Will display to you a more detailed information on your network.

**ipconfig /release** – Will drop the IP address received from the DHCP server we used for IP addresses distribution.

**ipconfig /renew** – Will send a request to all available DHCP server (Broadcast) for being assigned with an IP address. Our device will connect with the first DHCP server that replied back.

**nslookup** – Enables us to resolve to a domain name by its respective IP address.

- 1) By running the command **ipconfig /all**, we are able to see that all of our configurations were properly set.



```
Command Prompt
Windows IP Configuration

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

Ethernet adapter InLAN:

    Connection-specific DNS Suffix . : server.local
    Description . . . . . : Intel(R) 82574L Gigabit Network Connection #3
    Physical Address. . . . . : 00-0C-29-CB-08-1C
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . : fe80::40df:1d1b:1cad:8833%8(Preferred)
    IPv4 Address. . . . . : 172.31.0.6(Preferred)
    Subnet Mask . . . . . : 255.255.255.192
    Lease Obtained. . . . . : Saturday, November 28, 2020 1:31:33 AM
    Lease Expires . . . . . : Saturday, November 28, 2020 2:22:42 PM
    Default Gateway . . . . . : 172.31.0.61
    DHCP Server . . . . . : 172.31.0.1
    DHCPv6 IAID . . . . . : 301993001
    DHCPv6 Client DUID. . . . . : 00-01-00-01-27-15-7A-94-00-0C-29-CB-08-08
    DNS Servers . . . . . : 172.31.0.1
    NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Anonymous>
```

- Our DHCP and DNS servers (services) are both resolving from **DC** (172.31.0.1).
- Our IP address (172.31.0.6) and Subnet (255.255.255.192) were both been assigned according to how we defined our DHCP server.
- Our Lease duration for the IPv4 address we received for **WIN10** is set to 8 hours- Like we configured in our DHCP server.
- Our Default Gateway (Router) IP address (172.31.0.61) is our **SRV1** server.

- 2) We'll send a **ping** request to Google's DNS IP address and see if we were able to establish a connection with network outside of our environment;

```
C:\Users\Anonymous>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=51ms TTL=127
Reply from 8.8.8.8: bytes=32 time=49ms TTL=127
Reply from 8.8.8.8: bytes=32 time=51ms TTL=127
Reply from 8.8.8.8: bytes=32 time=50ms TTL=127

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 49ms, Maximum = 51ms, Average = 50ms
```

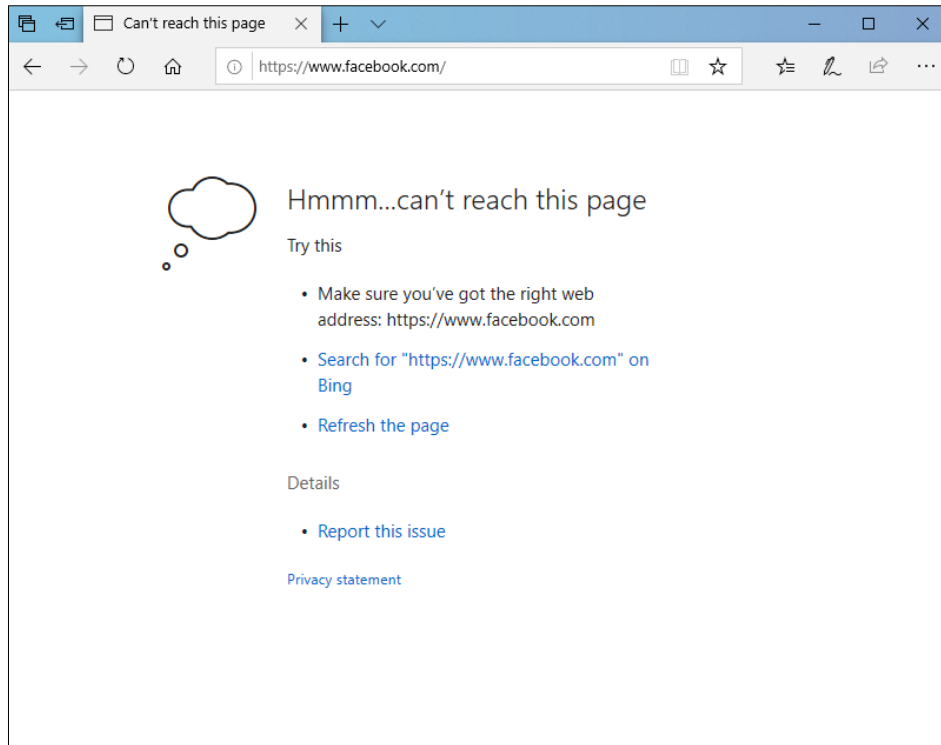
- 3) We will also use **nslookup** to check whether our server can translate a Domain Name to its associated IP address;

```
C:\Users\Anonymous>nslookup google.com
Server:  DC.server.local
Address:  172.31.0.1

Non-authoritative answer:
Name:     google.com
Addresses: 2a00:1450:4006:80a::200e
          172.217.171.206
```

- 4) Check that you are able to use the internet via a browser.

- 5) Finally, we will verify that the Conditional Forwarder we set for **facebook.com** is working properly.



- By browsing to **facebook.com** with our **WIN10** device, we shouldn't have access to this domain.

## Managerial & Sharing Features

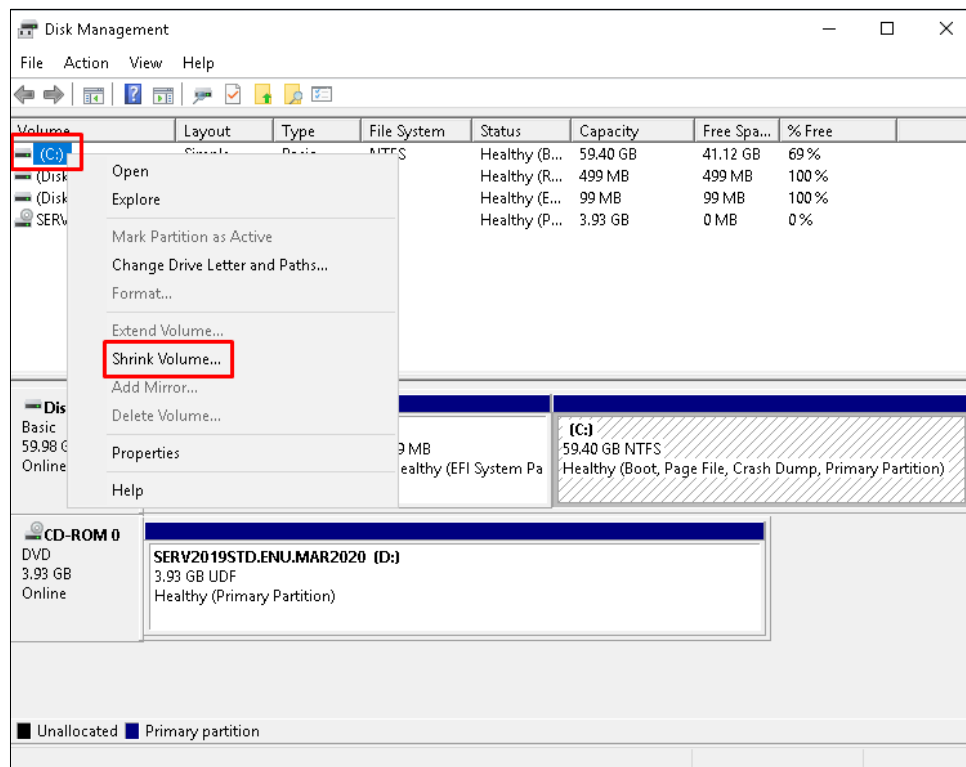
Now that all of our configurations were established and are working properly. We will start on assigning our users with permissions and features that would help us to better managing our environment.

### Creating a Shared Folder

In all organizations, users need to communicate with each other via their respective environment- Sharing files, presentations, videos and more.

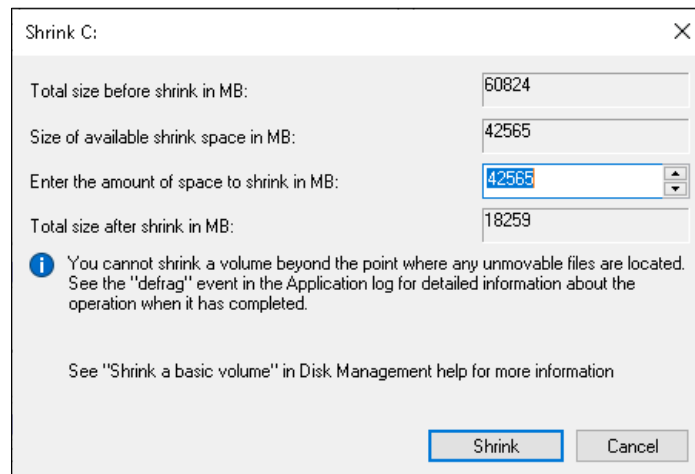
Creating a shared folder for our users helps them to better communicate and work with each other.

- 1) On **DC** server, open the search bar and type- **run**
- 2) Open the application and type- **diskmgmt.msc**
- 3) In the "**Disk Management**" window, right click on your main drive and choose- "**Shrink Volume**".



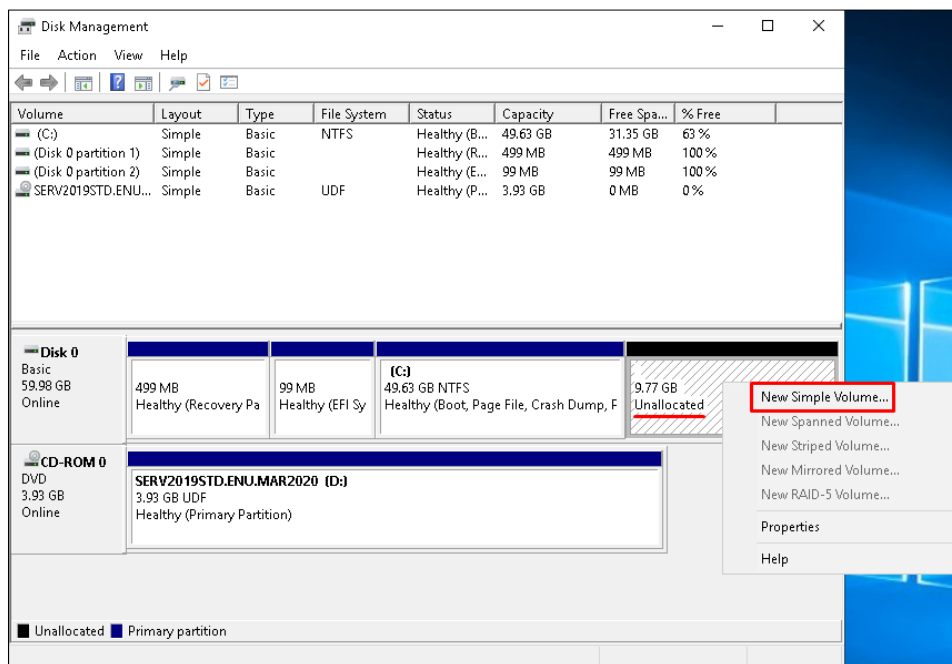


4) Press on **"Shrink"**.

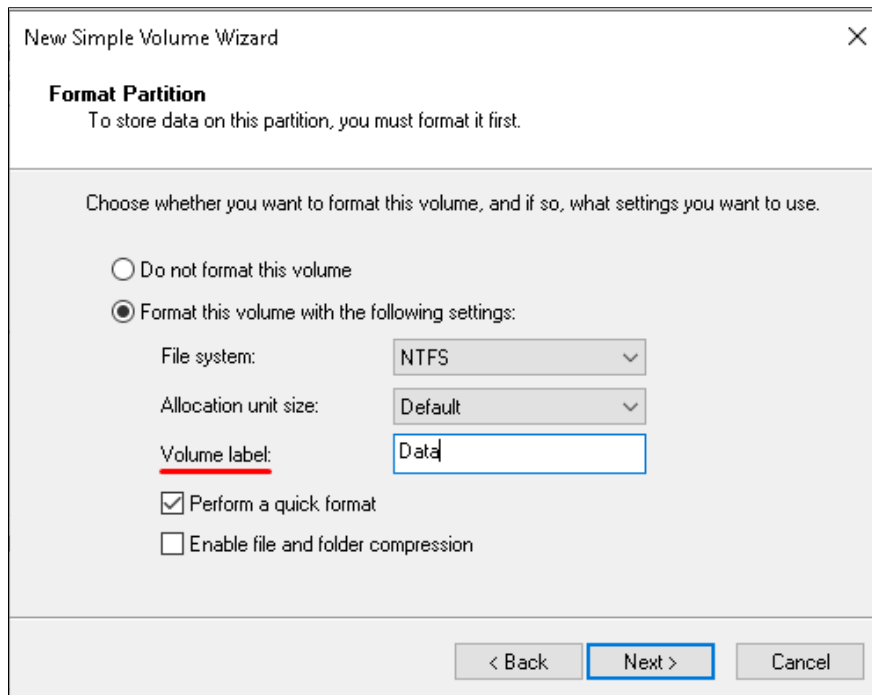


- Pay attention, you can also set the size before pressing on the button.
- For this tutorial, we took 10G of space from our existing driver.

5) In the **"Disk Management"** window, right click on the unallocated space you created and choose **"New Simple Volume"**.



- 6) Press on "**Next**" until you reach the "**Format Partition**" window.



- Name your drive- In our case we named our driver- **Data**
- Press "**Next**" and continue on.

- 7) Finally, press on "**Finish**".

- If the process was done correctly you should see a new drive in DC server.

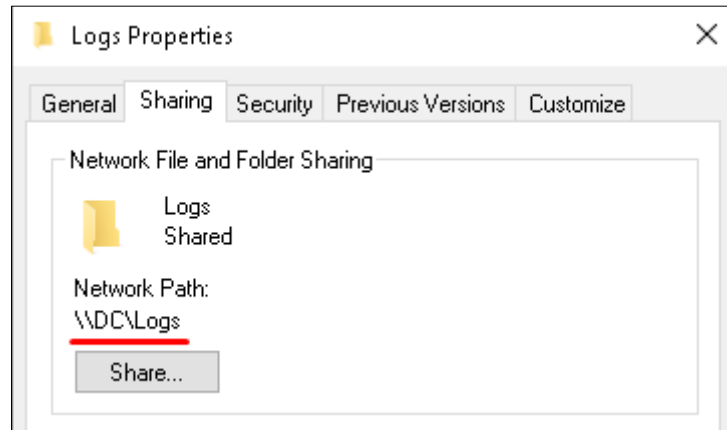


- 8) Next, we'll create a folder in our **Data** drive and name it **Logs**.

- Inside the folder we will also create a .txt file with the name **TrafficLog** in order to later on check the permissions we applied.

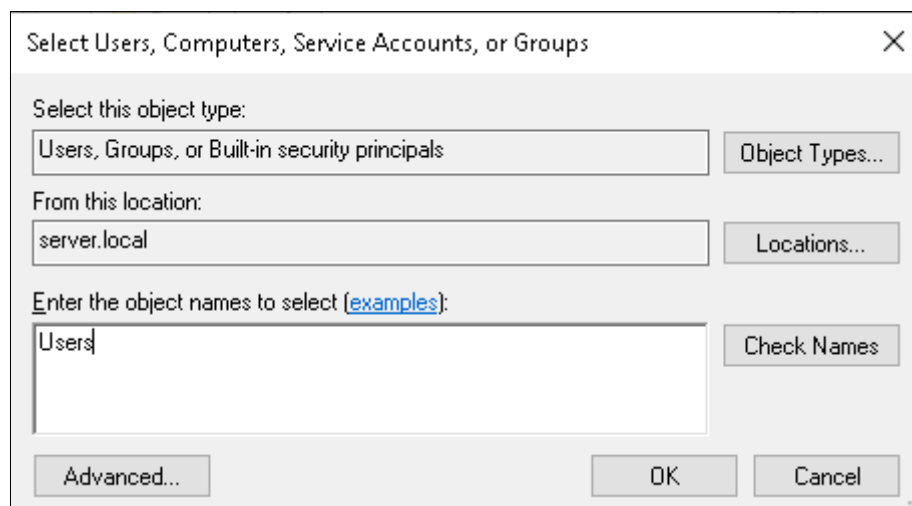
- 9) Right click on the **Logs** folder, press on "**Properties**" and go to the "**Sharing**" tab.

- 10) Press on "**Advanced Sharing**" and mark the checkbox that states "**Share this folder**".
- 11) Press on "**Apply**" and then "**OK**".
  - If you correctly followed this process, you'll see that your relevant folder received a new Network Path by default.

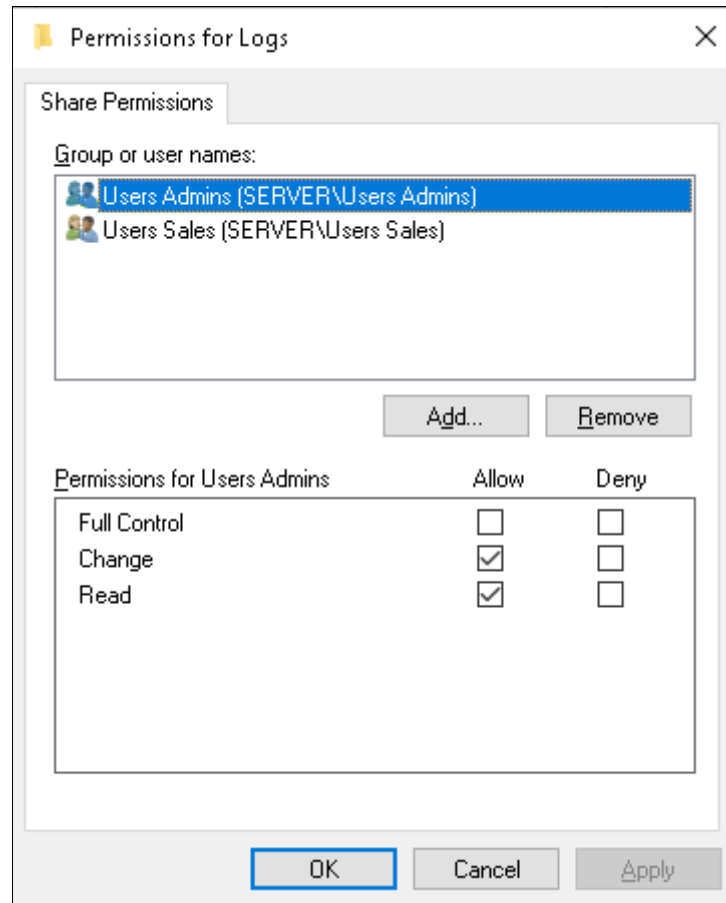


### Permissions for a Shared Folder

- 1) Right click on the **Logs** folder, press on "**Properties**" and go to the "**Sharing**" tab.
- 2) Press on "**Advanced Sharing**" and then "**Permissions**".
  - Remove the "**Everyone**" permission and instead add the **Users Admins** and **Users Sales** groups.

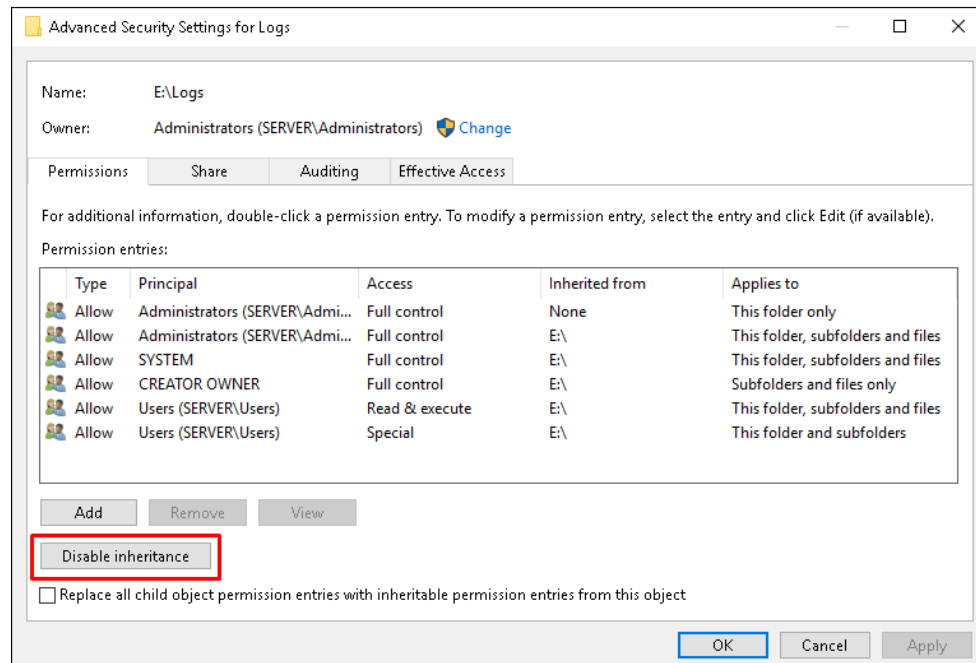


- 3) Once you are done with adding the groups, change their permissions according to your needs.



- For this tutorial, each group received the following permissions;
    - **Users Admins**- Change, Read.
    - **Users Sales**- Read.
  - Press on "**Apply**" and then "**OK**".
- 4) Go to the "**Security**" tab, press on "**Advanced**".

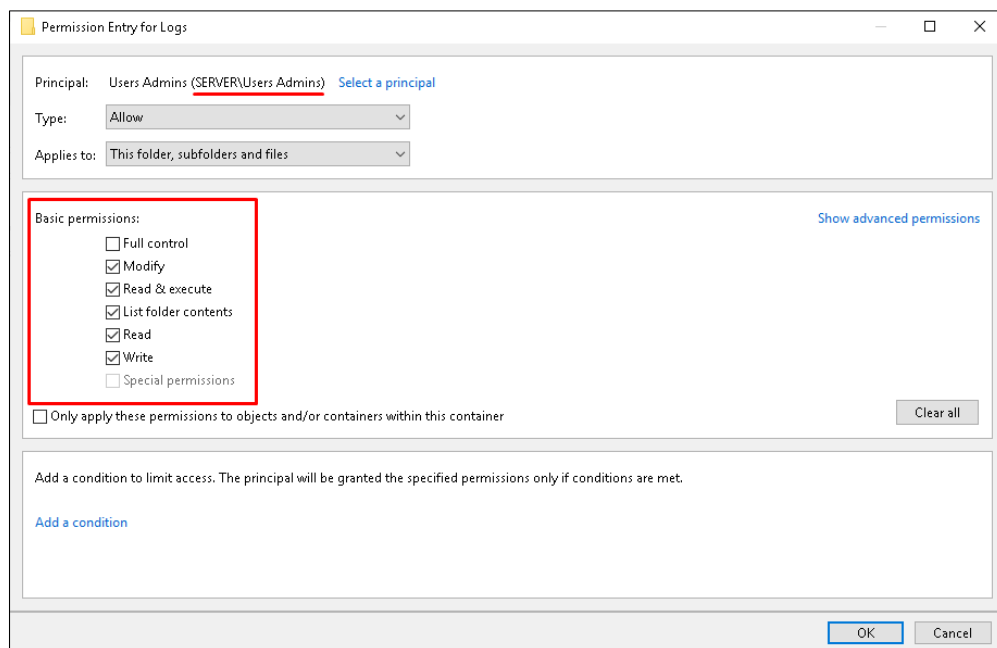
- 5) In order to make sure the specific permissions we are going to make will be applied. We'll remove any inheritance our policy groups may get from predefined default policies our system has.



- Press on **"Disable inheritance"** and the on-  
**"Remove all inherited permissions from this object"**.
- 6) Next, add our user groups- Press on **"Add"**.
- 7) Press on **"Select a principal"** and add a group.

8) Choose the permissions for the relevant group.

- **Full control**- Everything can be done.
- **Modify**- Everything can be done except of editing permissions.
- **Read & Execute**- View, Read and execute capabilities.
- **List Folder Contents**- View, only on folders.
- **Read**- As implies.
- **Write**- As implies, can't delete.
- **Special Permissions**- As implies.



- For this tutorial, we applied **Modify** permissions for the **Users Admins** group and **Read & Execute** permissions for the **Users Sales** group.

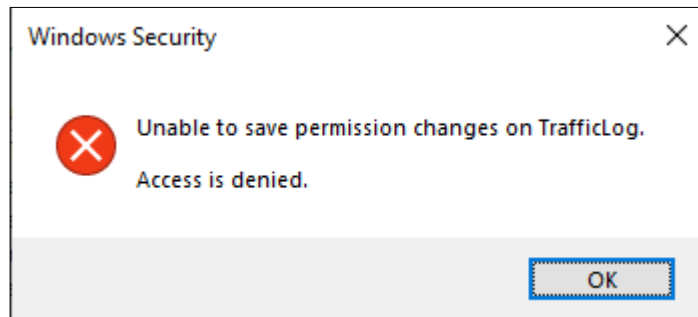
9) Press on "Apply" and then "OK".

## Validating Sharing Configurations

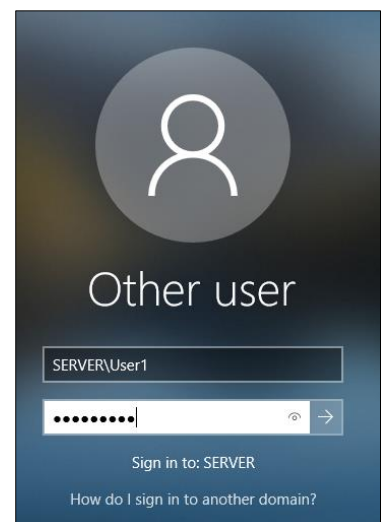
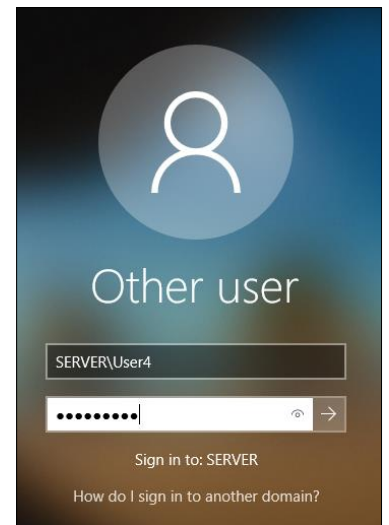
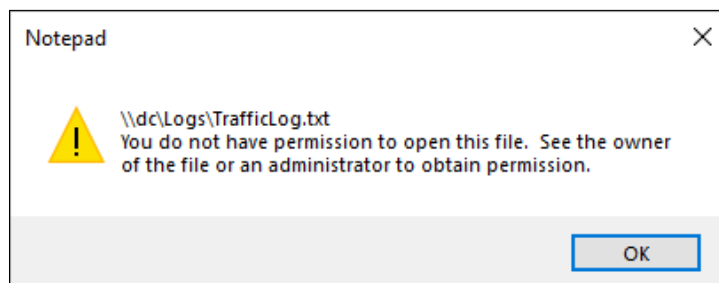
- 1) First, we will login to **User4 (Users Admins)**.
- 2) In the search bar, type **run** and enter the application.
- 3) Type the name of the server where the relevant folder is being shared from.
  - In our case- **\\dc**.
- 4) There, you will see the shared **Logs** folder- Enter.



- 5) Right click on the **TrafficLog** file and choose "**Properties**".
- 6) Under the "**Security**" tab, we can notice that we can't edit any of the existing permissions.



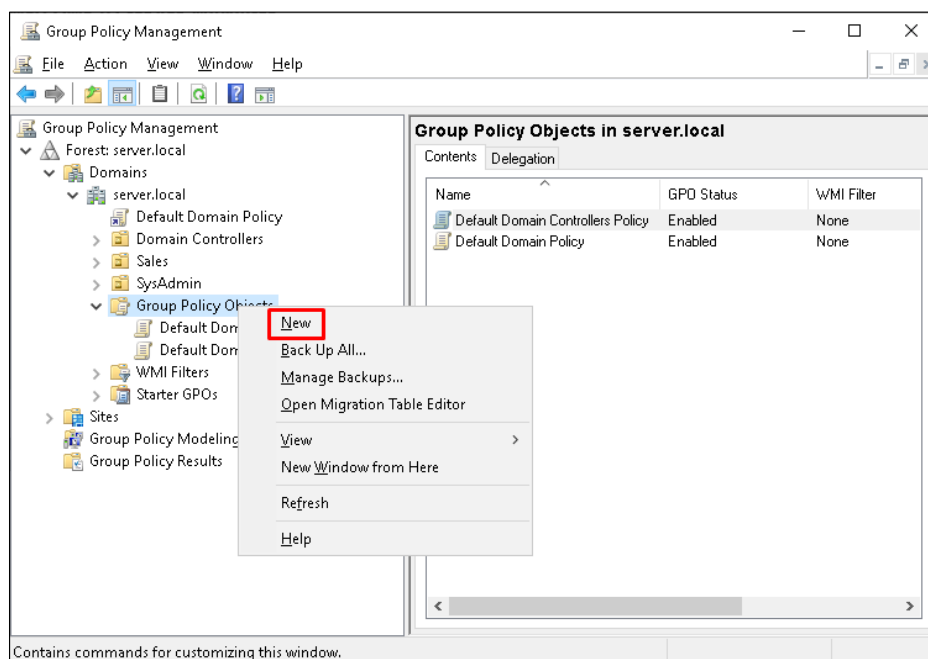
- 7) Now, we will login to **User1 (Users Sales)**.
- 8) Enter the folder sharing directory and access the **Logs** folder.
- 9) Right click on the **TrafficLog** file and choose "**Properties**".
- 10) Due to the fact that **User1** is set only for **Read & Execute**. We won't be able to make any change to our **TrafficLog** file.



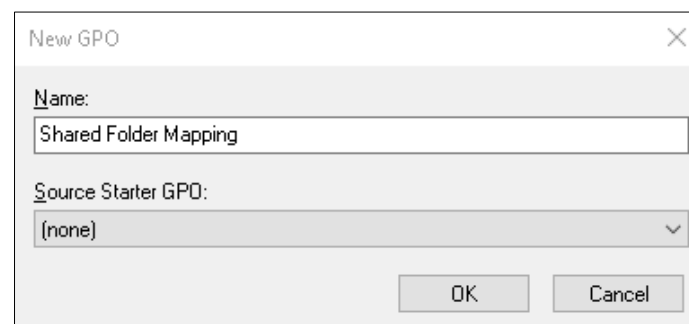
## Mapping a Shared Folder

In order to make the process of accessing the shared folder is more comfortable for users. We'll create a shortcut to our folder in each user's device main directory. We'll do this by creating a Group Policy Object that will be applied on all the clients using the shared folder.

- ❖ Group Policy Object (GPO), provides centralized management and configuration of operating systems, applications, and users' settings in an AD environment. A set of Group Policy configurations is called a GPO.
- 1) On **DC**, open the Server Manager.
  - 2) In the top right corner, click on the "**Tools**" tab and choose- "**Group Policy Management**".
  - 3) Expand your domain directory, right click on "**Group Policy Objects**" and choose- "**New**".



- 4) Name your new GPO.

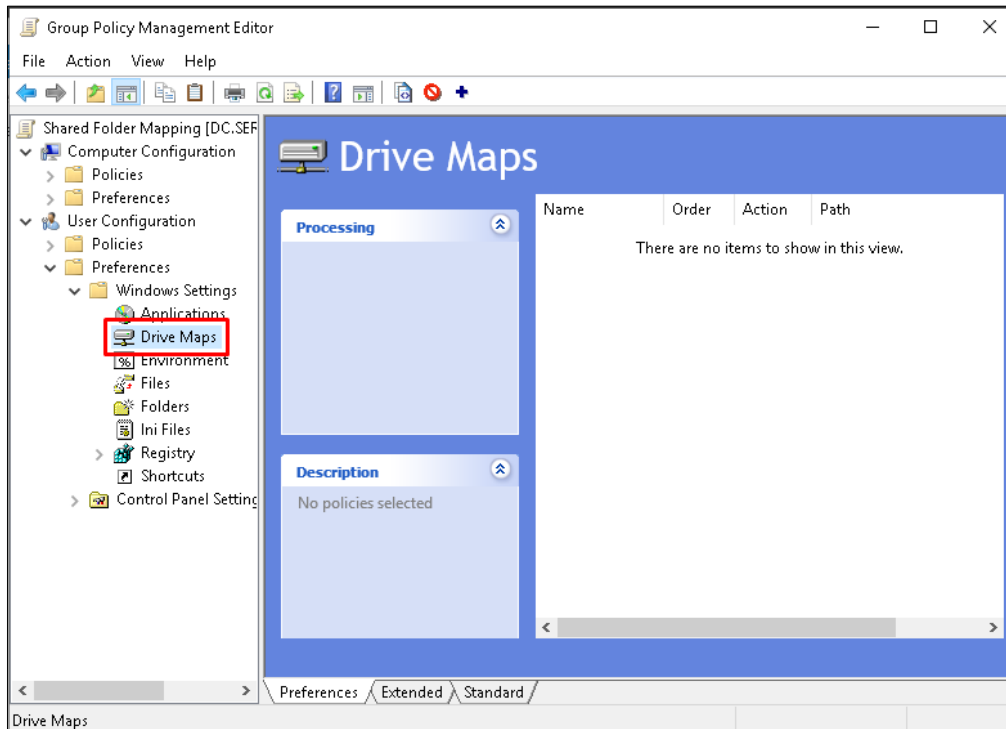


- In our case we named the GPO- **Shared Folder Mapping**.
- 5) Right click on the newly created GPO and choose "**Edit**".

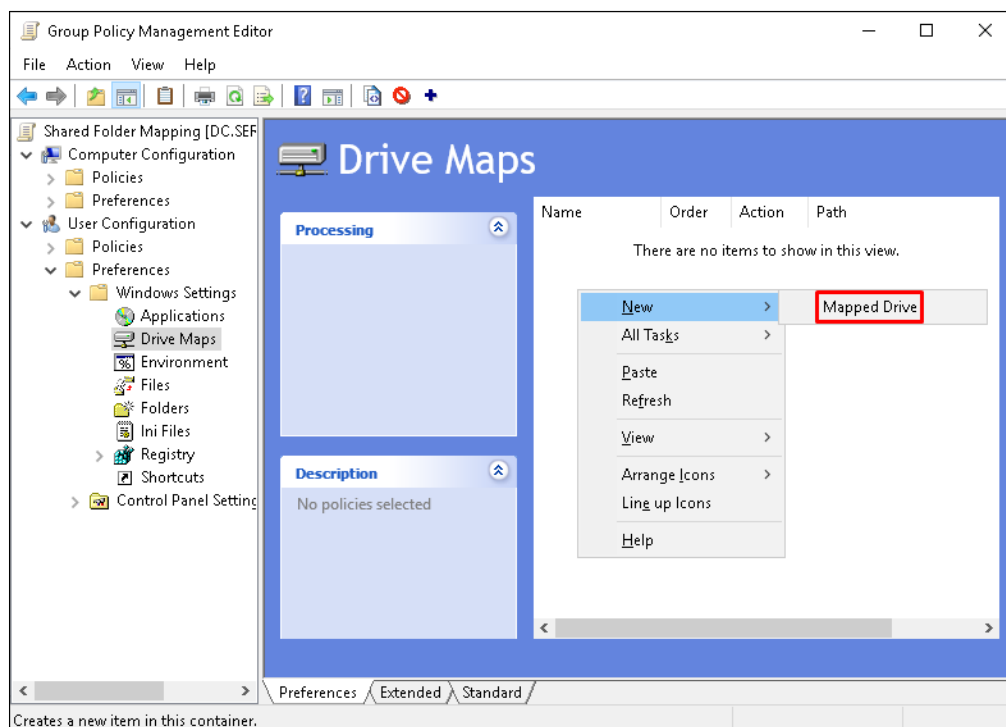


6) At the "**Group Policy Management Editor**" window, go to the left bar and follow this folder directory;

- ↓ i. User Configurations.
- ii. Preferences.
- iii. Windows Settings.
- iv. Drive Maps.



7) Right click on the empty list to the right, choose "**New**" and then- "**Mapped Drive**"



- 8) In the "New Drive Properties" window, input the location, the letter of the driver we use and adjust the visibility for the driver.

E: Properties

General Common

Action: Create

Location: \\dc\\logs

Reconnect: ☐ Label as:

Drive Letter

☒ Use first available, starting at: ☐ Use: E

Connect as (optional)

User name: Password: Confirm password:

Hide/Show this drive

☐ No change  
☐ Hide this drive  
☒ Show this drive

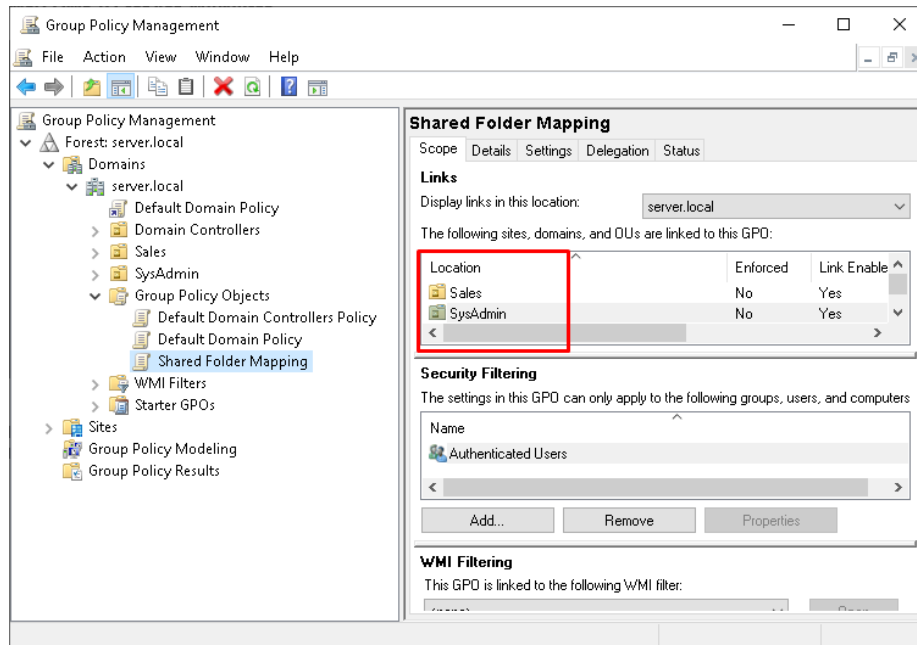
Hide/Show all drives

☐ No change  
☐ Hide all drives  
☒ Show all drives

OK Cancel Apply Help

- 9) Press "Apply" and then "OK".

- 10) At the "**Group Policy Management**" window, drag your newly created GPO to the relevant groups you want the rule to be applied on and click on "**OK**" when a confirmation window is shown.
- If you followed the process correctly the groups will be shown in your GPO "**Scope**" tab.



- 11) In **WIN10**, login as a user who belongs to either **SysAdmin** or **Sales** groups.
- 12) Open CMD and type **gpupdate /force**
- 13) Wait until the following messages will be presented.

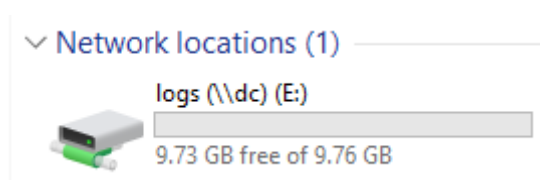
```

Microsoft Windows [Version 10.0.18362.1082]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\User4>gpupdate /force
Updating policy...

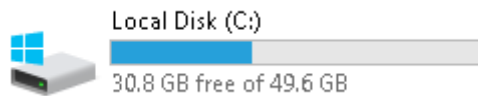
Computer Policy update has completed successfully.
User Policy update has completed successfully.
  
```

- 14) Open **This PC** directory, there you should see your new folder shortcut.

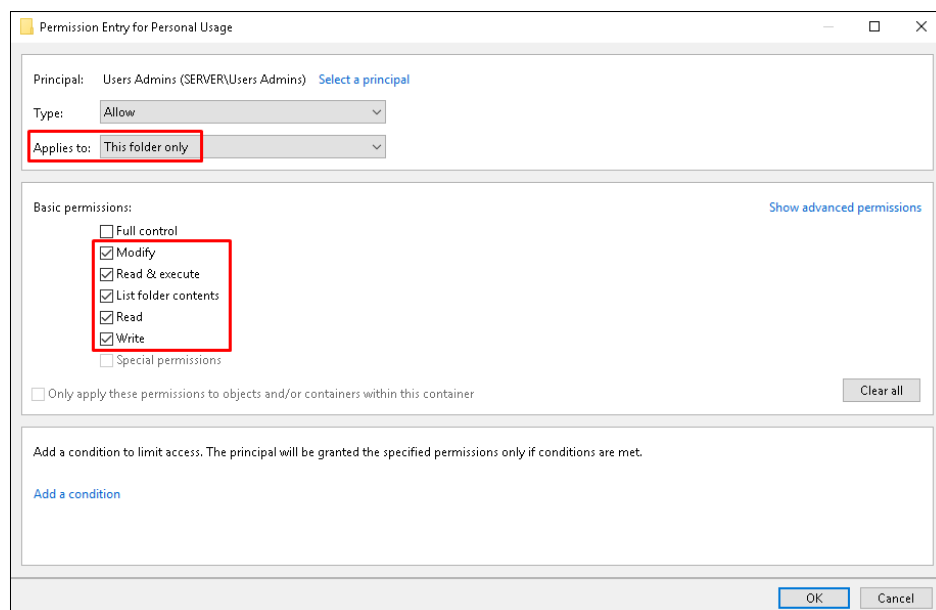


## Creating a Home Folder for Clients

- 1) On **DC**, open the **Local Disk (C:)** directory create a new folder.



- In our case, we named the folder **Personal Usage**.
- 2) Right click on the folder you created and choose "**Properties**".
  - 3) Under the "**Sharing**" tab, press on "**Advanced Sharing**".
  - 4) Check the "**Share this folder**" box, and press on "**Permissions**".
  - 5) Make sure that the "**Allow**" check boxes for "**Read**", "**Change**" and "**Full Control**" are marked.
  - 6) Press on "**Apply**" and then "**OK**".
  - 7) Under the "**Security**" tab, press on "**Advanced**".
  - 8) Press on "**Disable inheritance**" and choose- "**Convert inherited permissions to explicit permissions...**"
  - 9) Remove both **Users (SERVER\Users)** permissions with **Read & execute** and **Special Access configurations**.
  - 10) Press on "**Select a principal**" and add the relevant user groups.
    - For this tutorial, we will add the **Sales** and **SysAdmin** groups.
  - 11) Make sure the group is marked in the "**Applies to:**" section with- "**This folder only**" and give the relevant group the relevant permissions.



- For this tutorial, we applied **Modify** permissions.
- Press on "**OK**"

- 12) Press on **"Apply"** and then **"OK"**.
- 13) Open the Server Manager application.
- 14) At the right top corner, click on **"Tools"** and choose-  
**"Active Directory Users and Computers"**.
- 15) Choose a group and mark all the users in it.

Name	Type	Description
Users Sales	Security Group...	
User2	User	
User1	User	

- 16) Right click on the marked users and choose **"Properties"**.
- 17) Under the **"Profile"** tab, mark the **"Home folder"** check box.
- 18) Mark the **"Connect"** option, choose a non-existing drive and input the path for generating user folders.

Properties for Multiple Items

General Account Address Profile Organization

To change a property for multiple objects, first select the checkbox to enable the change, and then type the change.

User profile

☐ Profile path:

☐ Logon script:

☒ Home folder

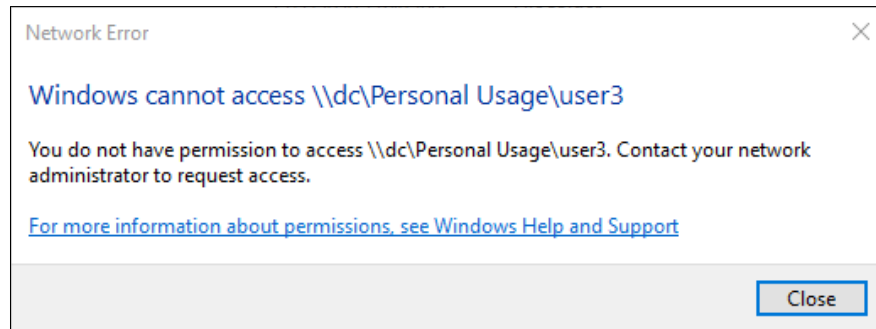
☐ Local path:

☒ Connect: Z: To: \\dc\Personal Usage\%username%

OK Cancel Apply

- In order to make sure each user will get a folder; you need to add the variable **%username%**
- For this guide, we added to the **Personal Usage** directory both the **Sales** and **SysAdmin** groups.

- 19) Press on **"Apply"** and then **"OK"**.
- 20) On **WIN10**, access a user who is associated with one of the relevant groups.
- 21) Access the folder that is stored on your network and contains the private folders
  - For this guide, the directory is **\\dc\Personal Usage**.
- 22) When trying to access a folder that is not belong to the logged user.  
The following will be shown;

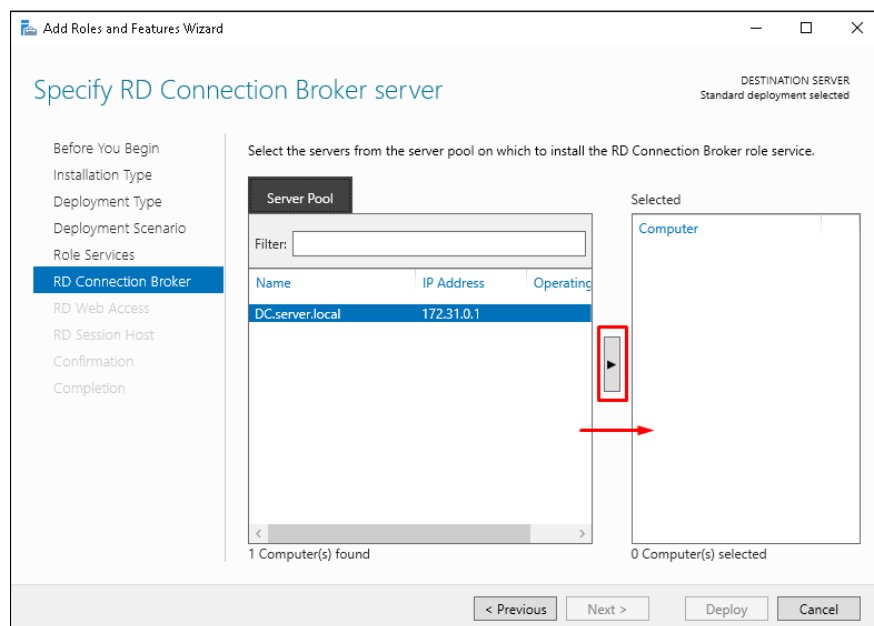


## RDP & SSH Connections

### Enabling Remote Desktop Connection

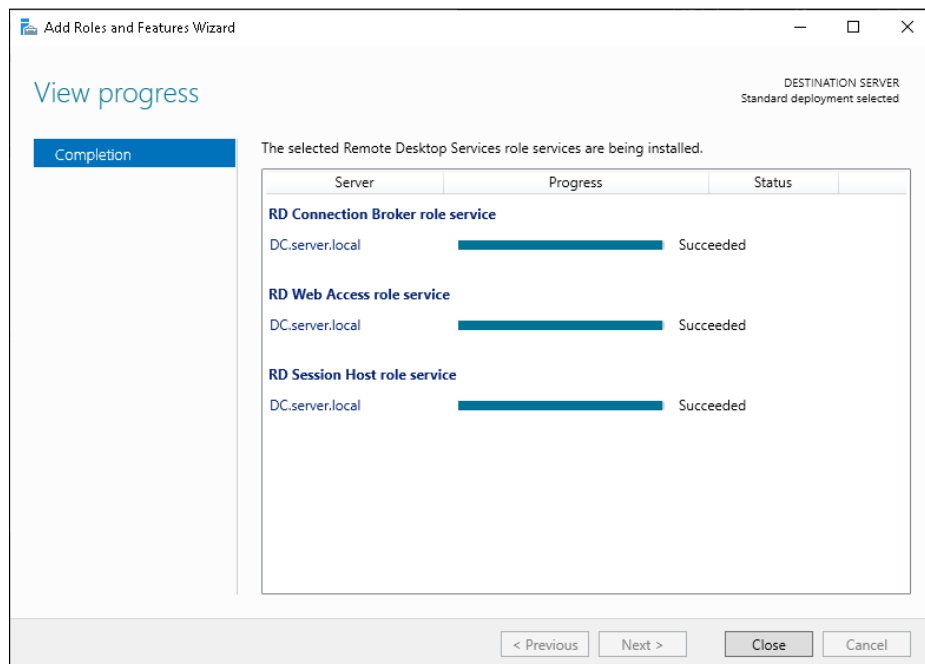
Next, we'll enable our **SysAdmin** group to access our **DC** server's environment via **WIN10**. This feature is in order for our admins to be able to manage the environment we created. This process is being done using the Remote Desktop Protocol.

- ❖ Remote Desktop Protocol (RDP), is a protocol that enables users to connect to a remote device.
- 1) On **DC** server, open the Server Manager application.
  - 2) At the top right corner, click on the "**Manage**" tab and choose- "**Add Roles and Features**", after that, press on "**Next**".
  - 3) At the "**Installation type**" section, choose- "**Remote Desktop Services installation**" and press on "**Next**".
  - 4) At the "**Deployment Scenario**" section, choose- "**Session-based desktop deployment**" and press on "**Next**".
  - 5) At the "**Role Services**" section, press on "**Next**".
  - 6) At the "**RD Connection Broker**" section, pass your server to the right-side window and press on "**Next**".



- 7) At the "**RD Web Access**" section, pass your server to the right-side window and press on "**Next**".
- 8) At the "**RD Session Host**" section, pass your server to the right-side window and press on "**Next**".

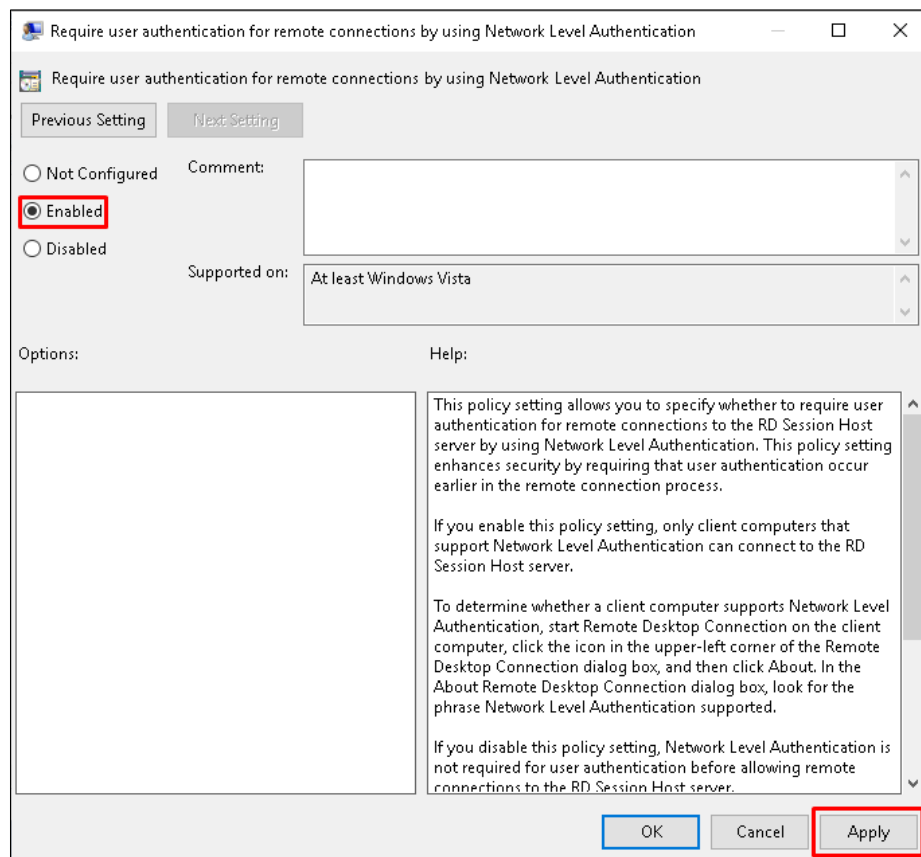
- 9) At the "**Confirmation**" section, mark the checkbox- "**Restart the destination server automatically if required**" and press on "**Deploy**".
- The server will start installing RDP services.



- 10) Close the installation window once the process is done.
- Next, we'll apply a GPO that will make sure that only users from the **SysAdmin** group can connect remotely.
- 11) In the top right corner, click on the "**Tools**" tab and choose- "**Group Policy Management**".
- 12) At the left bar, under "**Group Policy Objects**" create a new GPO.
- 13) Name the new GPO, right click on it and choose "**Edit**".
- For this tutorial, we named the GPO; **RDP – No Access**.
- 14) At the left bar, follow this folder directory;
- ↓ i. User Configuration
  - ii. Policies
  - iii. Administrative Templates
  - iv. Windows Components
  - v. Remote Desktop Services
  - vi. Remote Desktop Session Host
  - vii. Security
  - viii. Require user authentication for remote connections by using Network Level Authentication.



15) Select the "**Disabled**" option, press on "**Apply**" and then "**OK**".



16) Drag your GPO to the relevant OU that you want to make sure that it won't be able to connect via RDP to DC server.

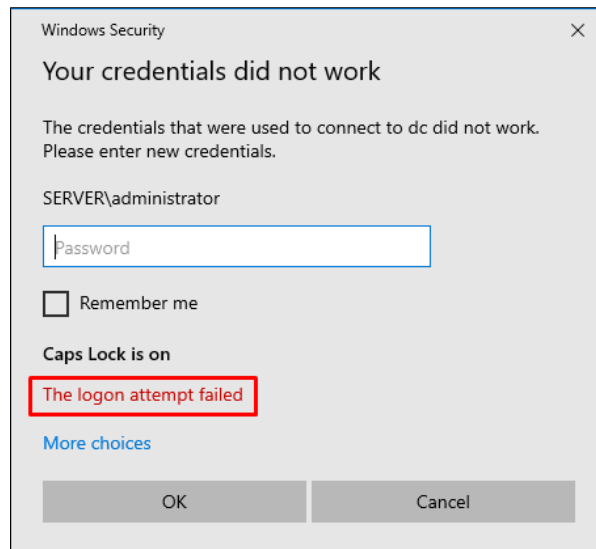
17) In order to test your newly added GPO simply login with a user who's not supposed to have access.

18) At the desktop search bar, type **mstsc** and enter the application.

19) Input the server's IP address and following to that the admin user credentials.

- In our case, the IP address is- **172.31.0.1**

20) The following message will be shown;



- If you will try to login from a permitted user, you will have access to the server.

## Enabling Remote Connection with SSH

In order to enable this feature, you first need to have OpenSSH installed on your server and an internet connection.

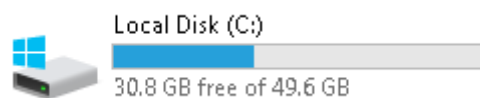
[Download link](#)

[Installing OpenSSH with PowerShell](#)

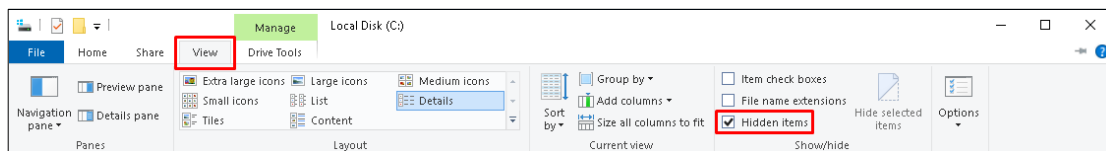
[SSH Client - Putty](#)

- ❖ Secure Shell (SSH), a cryptographic network protocol for operating network services securely over an unsecured network. Usually SSH connections are being handled through a dedicated client user interface software.

- 1) On **DC**, after doing the initial SSH installation- Open **Local Disk (C:)** drive.



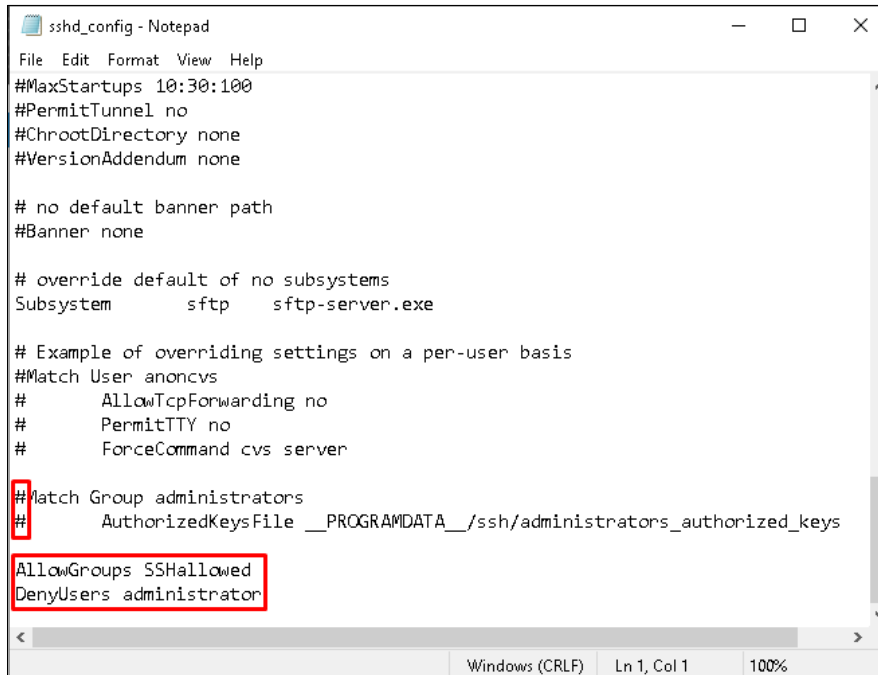
- 2) At the top bar, click on the **"View"** tab and mark the **"Hidden Items"** checkbox.



- 3) Enter the directory **C:\ProgramData\ssh**, right click on the **"sshd\_config"** file and open it with Notepad.

4) Scroll down to the bottom of the file and there, add the following;

- ***AllowGroups <groupname>***
- ***DenyUsers <username>***



```
sshd_config - Notepad
File Edit Format View Help
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# override default of no subsystems
Subsystem sftp sftp-server.exe

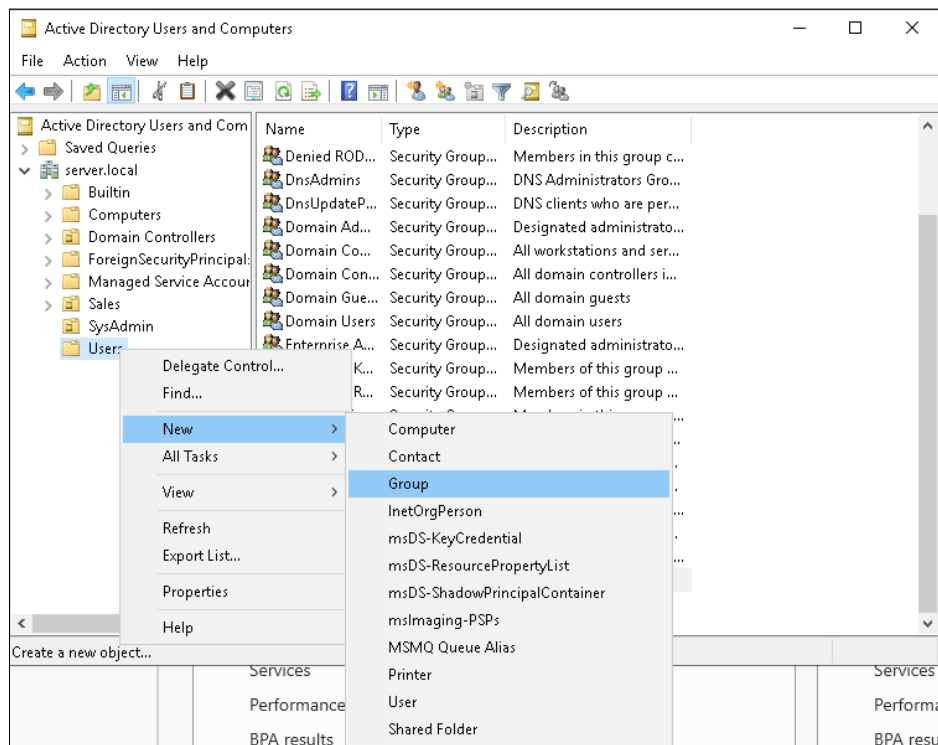
# Example of overriding settings on a per-user basis
#Match User anoncvs
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server
#Match Group administrators
#    AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys
AllowGroups SSHallowed
DenyUsers administrator

Windows (CRLF) Ln 1, Col 1 100%
```

- Pay attention to also add the '#' marks according to the above screenshot.
- For this tutorial, we are adding a ***SSHallowed*** group and ***administrator*** user.
- Save your changes and exit the file.

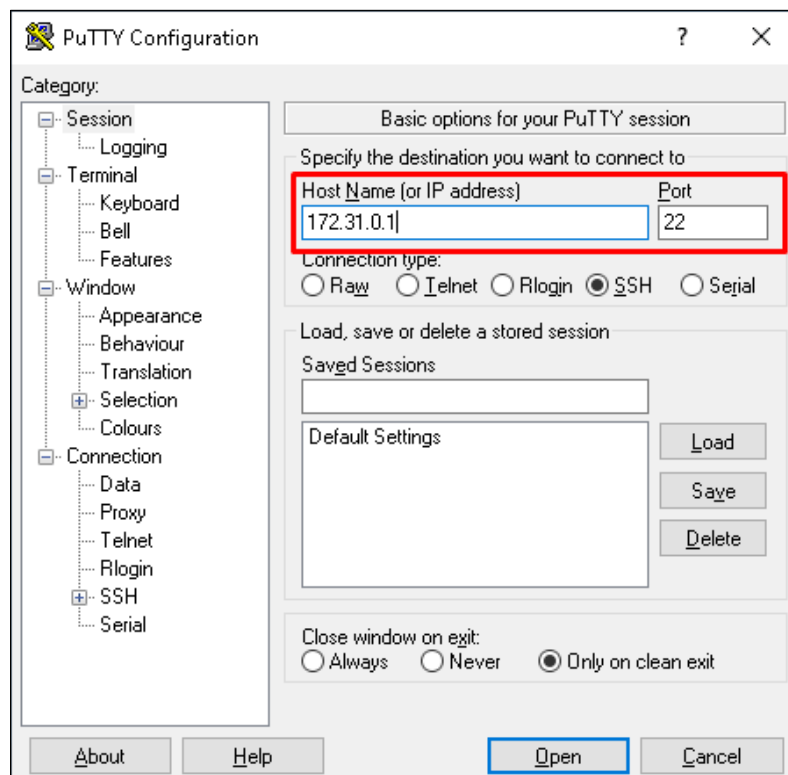
5) In the Server Manager application, at the top right corner choose "**Tools**" and click on "**Active Directory Users and Computers**".

- 6) At the left bar, right click on "**Users**", choose "**New**" and select "**Group**".



- 7) Name your group for allowed users.
- In our case we named the group **SSHallowed**
- 8) Associate the users you want to be allowed to connect via SSH with the newly created group.
- In our case we are adding **SysAdmin** users.
- 9) At the desktop search bar, type "**services**" and enter the application.
- 10) Search for "**OpenSSH SSH Server**", right click on it and choose "**Restart**".
- This will make sure that all the changes we did are being currently used.
- 11) On **WIN10**'s admin account, install PuTTY.
- ❖ PuTTY- An SSH client interface that will make the login process a bit more comfortable. Installing PuTTY on **WIN10**'s admin account will make sure all of our users will be able to use PuTTY the next time they are logging in.
- 12) In the desktop search bar, type **putty** and open the application.

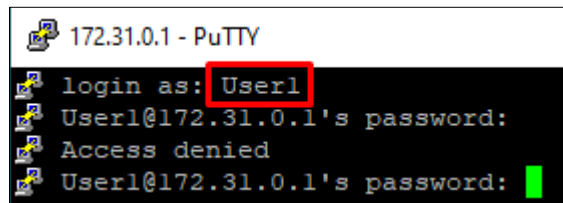
13) Input **DC** server's IP address and press on "**Open**".



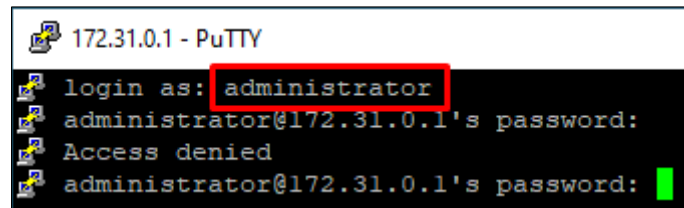
- For this tutorial, **DC** server's IP address is **172.31.0.1**.

14) In the "PuTTY Security Alert" window, press on "Yes".

- Users who are not in the allowed group or trying to access DC with the administrator credentials, the following will be shown;

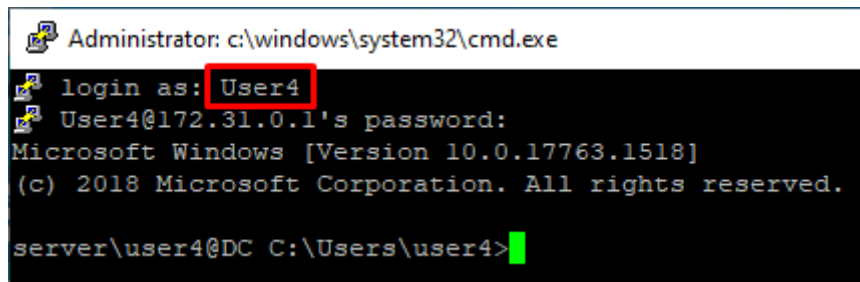


```
172.31.0.1 - PuTTY
login as: User1
User1@172.31.0.1's password:
Access denied
User1@172.31.0.1's password:
```



```
172.31.0.1 - PuTTY
login as: administrator
administrator@172.31.0.1's password:
Access denied
administrator@172.31.0.1's password:
```

- Users who belong to the allowed group will be able to login to DC server.



```
Administrator: c:\windows\system32\cmd.exe
login as: User4
User4@172.31.0.1's password:
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.


server\user4@DC C:\Users\user4>
```

## Basic Hardening Rules

In this section we'll apply some basic limitations on users that are not admins. We are applying these GPOs in order to make sure our environment is better secured and for reducing the chance of human error that may cause trouble for our network.

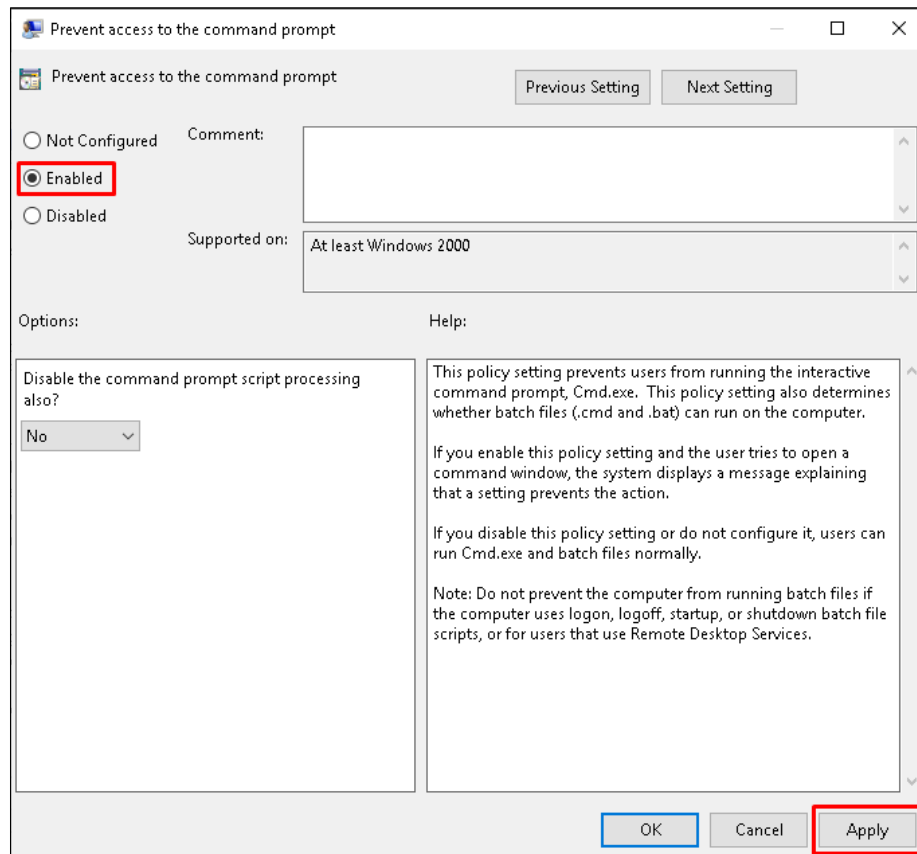
- For this tutorial, we will be applying each rule separately. However, all of them can be included in one GPO.

### Disabling CMD

- 1) On **DC** server, Open the server Manager.
- 2) At the top right corner, press on "**Tools**" and click on- "**Group Policy Management**"
- 3) Create a new GPO and name it.
  - In our case, we named it ***Block CMD***.
- 4) Right click on the relevant GPO and choose "**Edit**".
- 5) At the left bar, follow this directory;
  -  i. User configuration
  - ii. Policies
  - iii. Administrative Templates
  - iv. System
  - v. Prevent access to command prompt



6) At the rule configuration mark the rule as "Enabled".

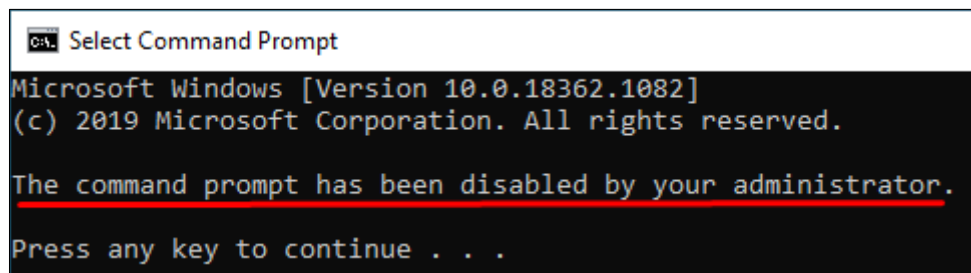


7) Press on "Apply" and then "OK".

8) Drag the GPO to the relevant group you wish to be unable to access CMD.

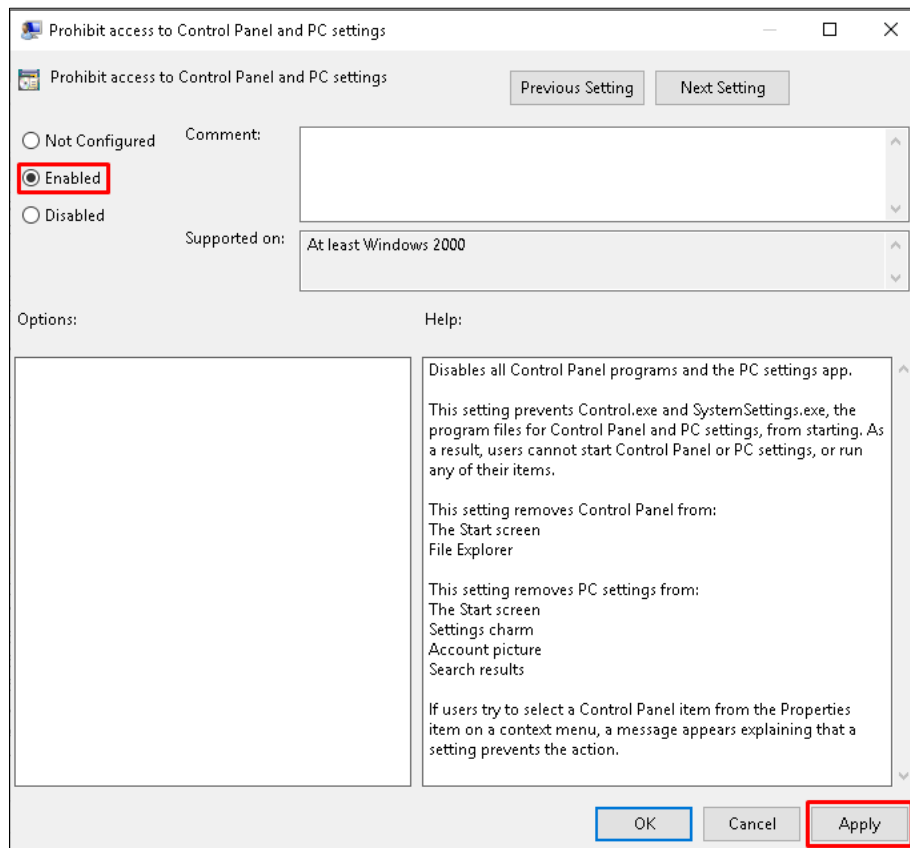
9) Restart the **WIN10** device in order to force user policies to update.

10) When trying to access CMD from a denied user, the following will be shown;



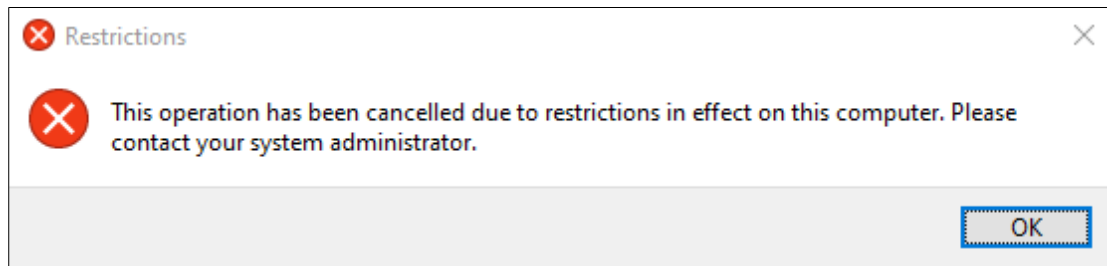
## Disabling Control Panel

- 1) On **DC** server, Open the server Manager.
- 2) At the top right corner, press on "**Tools**" and click on- "**Group Policy Management**"
- 3) Create a new GPO and name it.
  - In our case, we named it **Block CP**.
- 4) Right click on the relevant GPO and choose "**Edit**".
- 5) At the left bar, follow this directory;
  - ↓ i. User Configuration
  - ii. Policies
  - iii. Administrative Templates
  - iv. Control Panel
  - v. Prohibited Access to Control Panel and PC settings
- 6) At the rule configuration mark the rule as "**Enabled**".



- 7) Press on "**Apply**" and then "**OK**".
- 8) Drag the GPO to the relevant group you wish to be unable to access CMD.
- 9) Restart the **WIN10** device in order to force user policies to update.

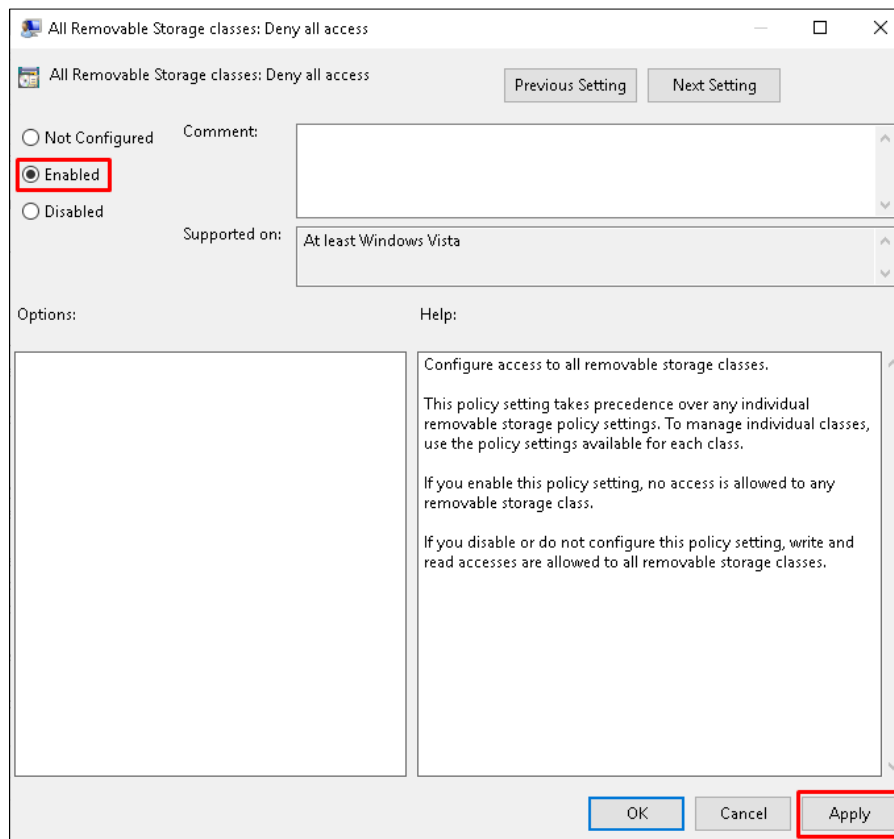
- 10) When trying to access the Control Panel from a denied user, the following will be shown;



### Disabling USB Devices Access

- 1) On **DC** server, Open the server Manager.
- 2) At the top right corner, press on "**Tools**" and click on- "**Group Policy Management**"
- 3) Create a new GPO and name it.
- 4) In our case, we named it ***Block USB Access***.
- 5) Right click on the relevant GPO and choose "**Edit**".
- 6) At the left bar, follow this directory;
  - i. Computer Configuration
  - ii. Policies
  - iii. Administrative Templates
  - iv. System
  - v. Removable Storage Access
  - vi. All Removable Storage Classes: Deny all access

7) At the rule configuration mark the rule as **"Enabled"**.



8) Press on **"Apply"** and then **"OK"**.

9) Drag the GPO to the relevant group you wish to be unable to access CMD.

10) Restart the **WIN10** device in order to force user policies to update.

11) When trying to insert a USB device from a denied user, a message indicating- **"Access Denied"** will be shown.

## Conclusion

In this tutorial we learned about some of the basic functions of computer networking and server configurations. I'll also take the opportunity to emphasize that this is only one of the first steps in exposing the reader who followed this tutorial to the procedures and methods organizations take in order to secure their assets.

In order to keep on advance and learning, I urge you to take advantage of social media platforms and keep on developing yourself on this world- Google, YouTube and etc. are excellent tools for trouble shooting, learning and investigating.

I promise to make an effort and publish the second part of this tutorial as soon as I am able.

**Mail:** [eidoepstein@gmail.com](mailto:eidoepstein@gmail.com)

**Phone:** (+972) 507-513-270

**LinkedIn:** [www.linkedin.com/in/eido-epstein](http://www.linkedin.com/in/eido-epstein)