PRESENTER: Eitan Danon

LECTURER: Oriel Kosayev

COLLEGE: See Security

DATE OF SUBMISSION: 06.12.2020

**DOMAIN CONTROLLER(DC) & DOMAIN NAME SYSTEM (DNS) SERVER - -**

Before we setup a domain controller and DNS server, we need to understand what those things mean so we can use them property.

DOMAIN CONTROLLER(DC) – first of all domain controller is a server computer that responds to security authentication and verifies users on computer networks, or it's just the butler that holds the keys to the Castel.

With domain controller we can follow every user on the computer network and easily set type some security arraignments to every one of them, it helps us to organize the network to groups / categories that every user can be part of and mean while to decide witch user or group have the privilege to enter or create documents, files, folders.

Some of the benefits of domain controller are:

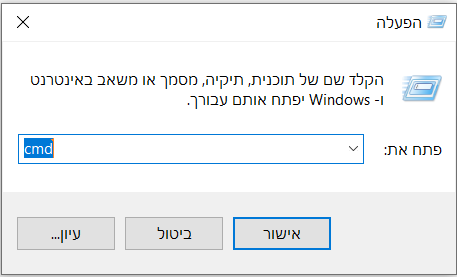
\*To manage user accounts from a central location, with full trust between locations

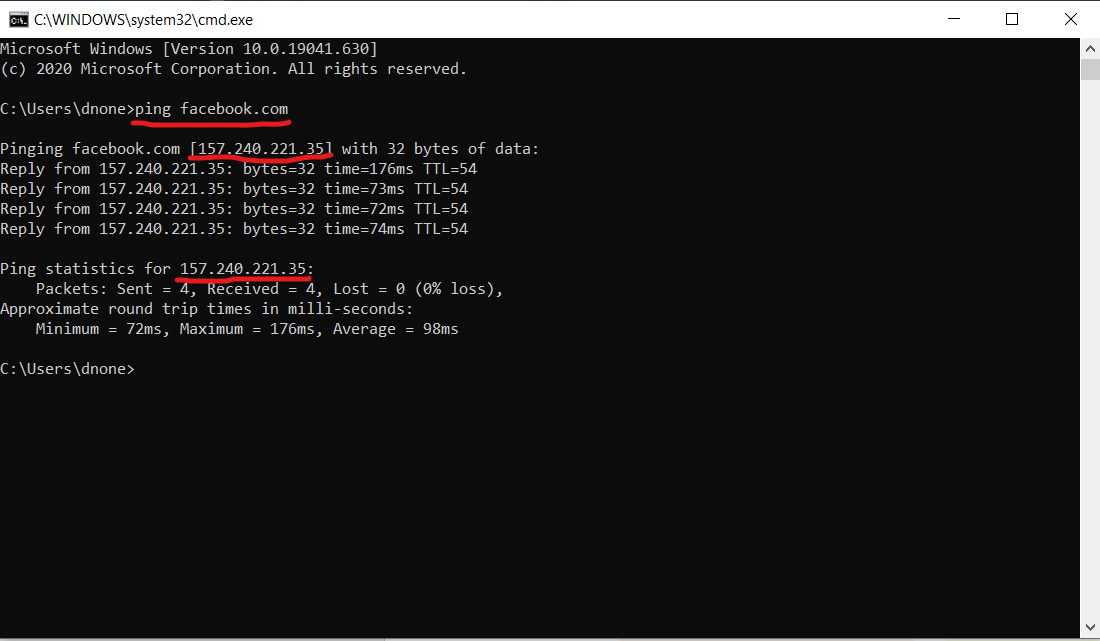
\*managing the stations centrally

\* improves security – because we decide who have privilege and who don’t

DOMAIN NAME SYSTEM (DNS)- the DNS service is like dictionary that translate us number to word that we can understand for example we will open CMD:

1)Press (win key + r) to open the run menu and type CMD and press enter /or just search for CMD on the win menu



2) on the CMD type ping facebook.com and we will see that it translate it to an number that is called IP address (157.240.221.35) that is specific to facebook.com  The IP address is required to be able to connect to a server that only knows the computer name.

So the DNS is a central part of the internet, providing a way to match names( like facbook.com) , to numbers (like 157.240.221.35) .Anything connected to the internet - laptops, tablets, mobile phones, websites - has an Internet Protocol (IP) address made up of numbers .

The DNS don’t have central database. The information is distributed to many thousands of name servers (DNS server).

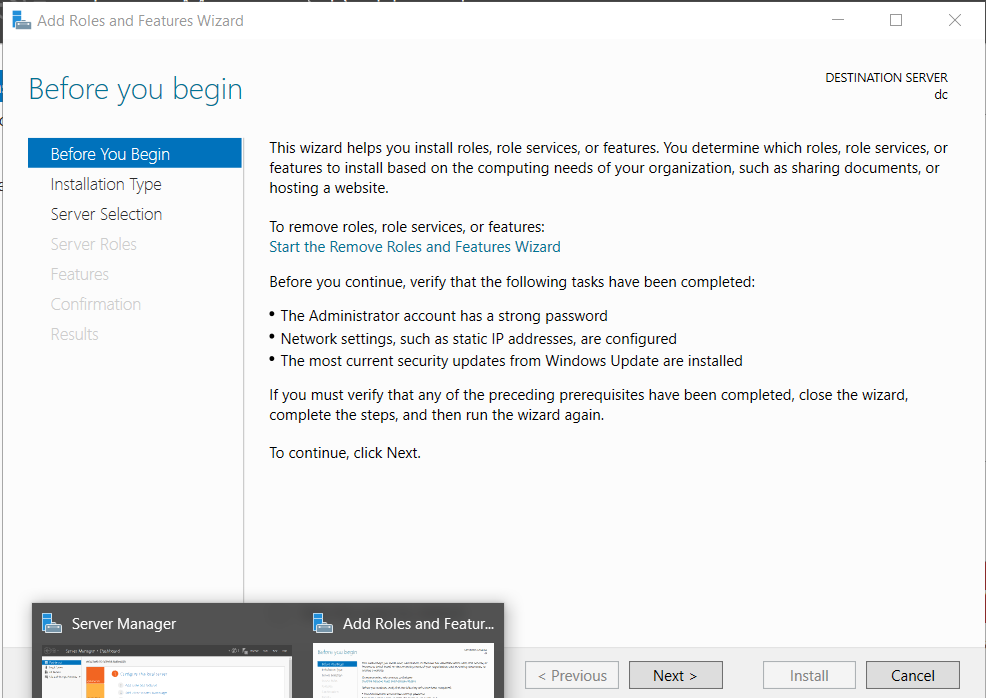
So if we don’t have an DNS server we can't go online on the internet because DNS is the one that responsible to find what we are looking for because the network don’t understand what is facebook.com , the network know what is 157.240.221.351 and the DNS translate us to an language we can understand

So, let's start setup the domain server

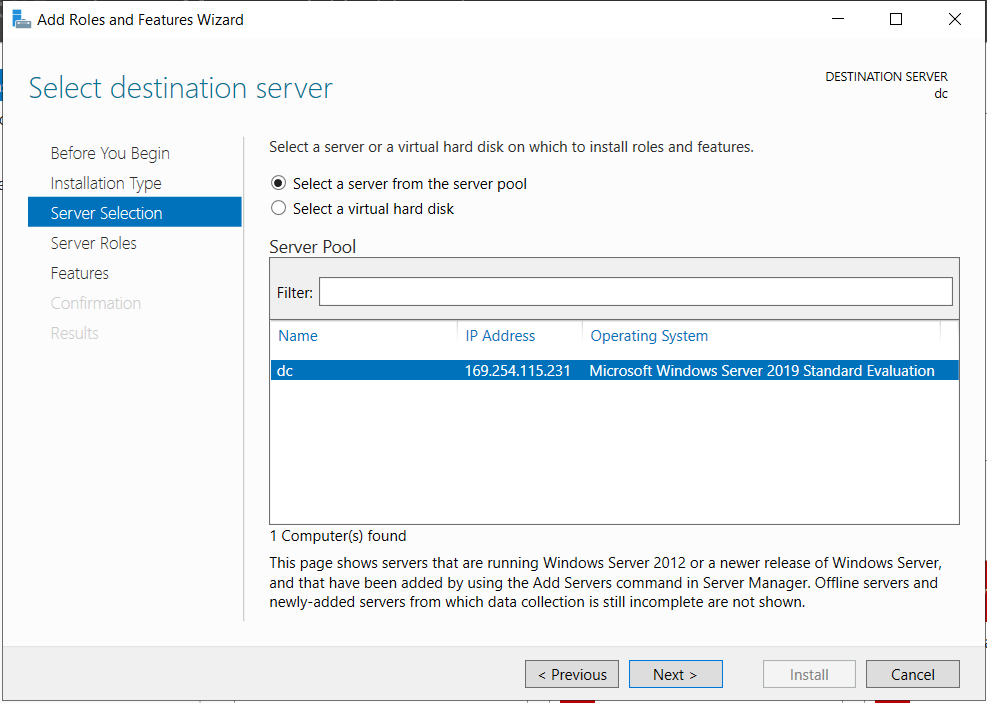
First of all, we need to install windows server 2019 on our VMware machine and name it dc

Second, we need to promote our server as domain controller at the active directory (ad) by adding DNS server and configure, how it's done?

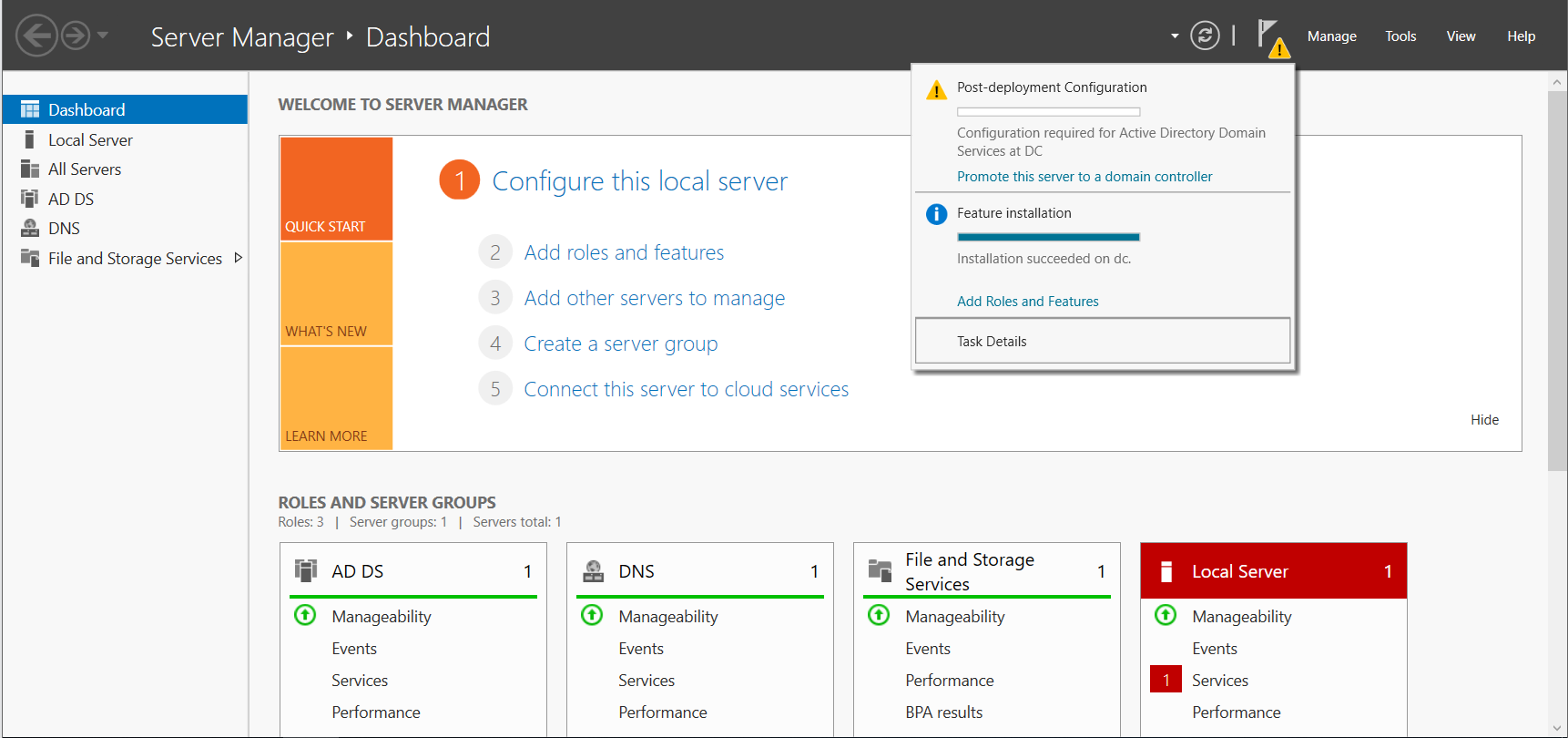
Server manager-manage- add roles and futures-server roles (1



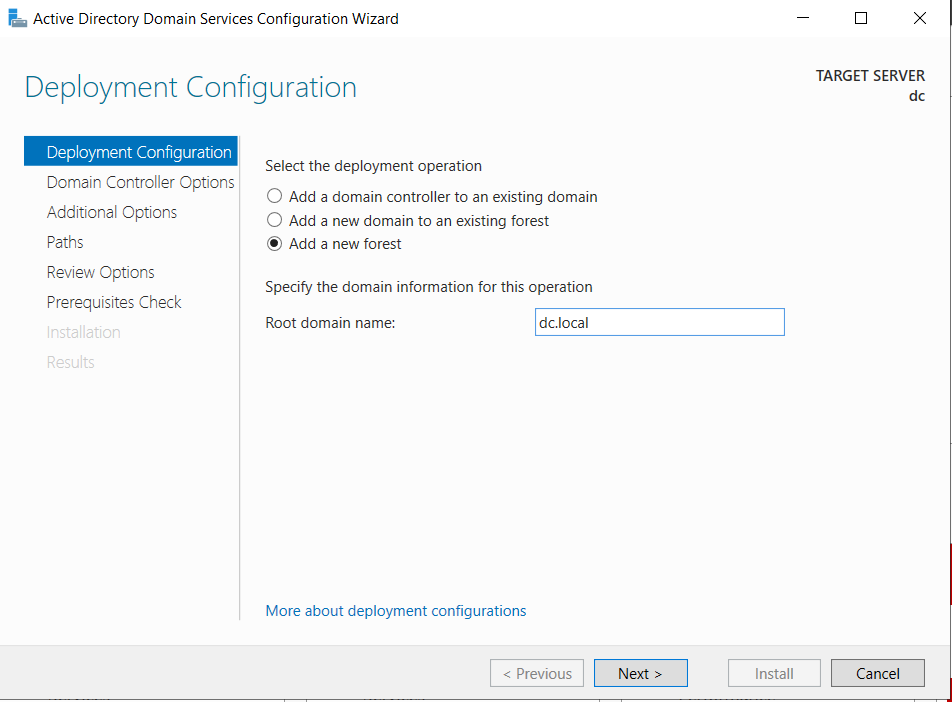
2) press next -> select role based –> next -> select the server (dc) -> next



3)Select active directory domain services & DNS service -> next -> next -> install



After we installed ad & DNS will be a yellow triangle at the flag that asks if we want to promote the server as domain controller and we will configure it as domain controller and create new forest and named it DC. Local

\*Press promote this server as dc ->add a new forest -> root domain name (DC. Local)->next->set up a password exp: Pa$$w0rd and install. That is all our server is a domain controller

So, we just setup some settings but we didn’t talk about them, what is an active directory

ACTIVE DIRECTORY (AD):

Ad is a Microsoft program for computer servers that helps to manage the network, Directory enables the structure of an organization to be replicated between different servers to provide faster services and the use of network resources or objects to be managed centrally.

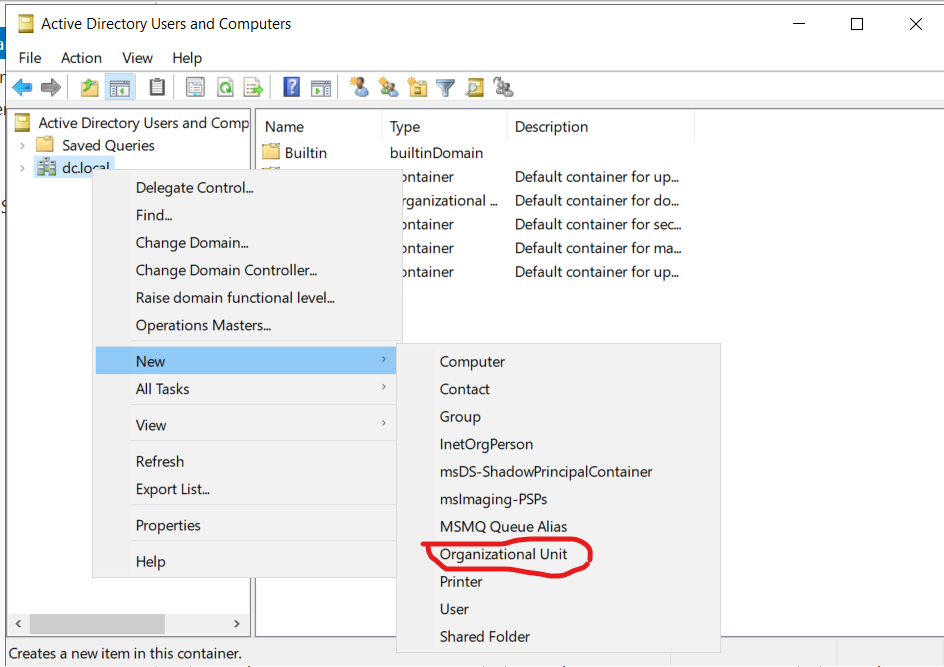
To manage an organization, we will need to create some organizational units (ou) to separate between the privilege of the workers at the organization.

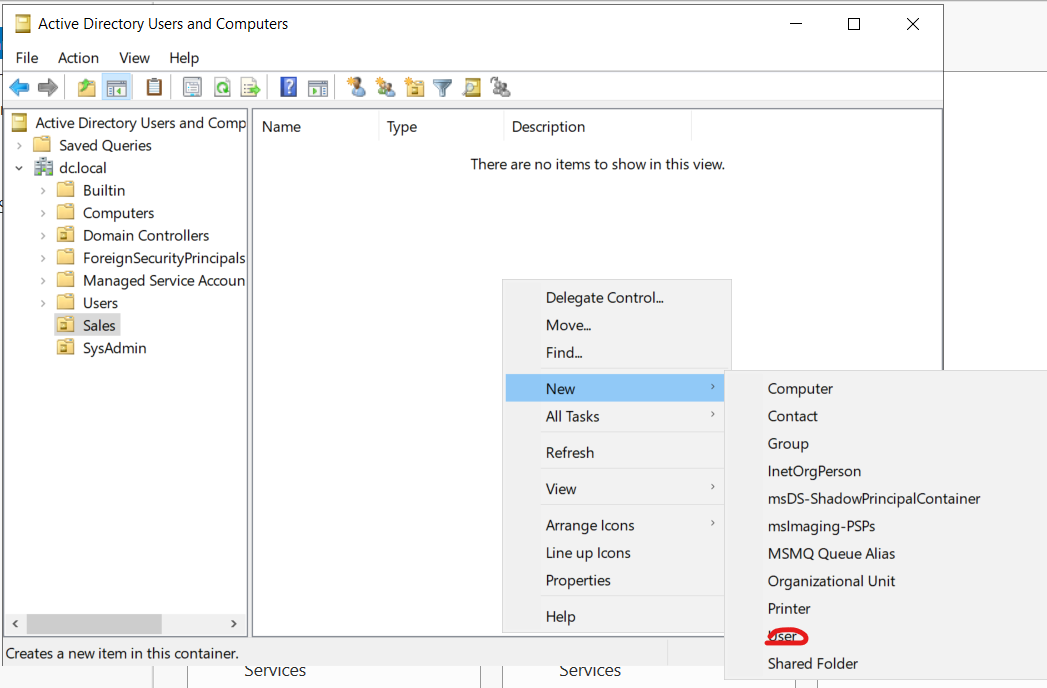
BUT WHAT IS ORGANIZATIONAL UNIT (OU) :

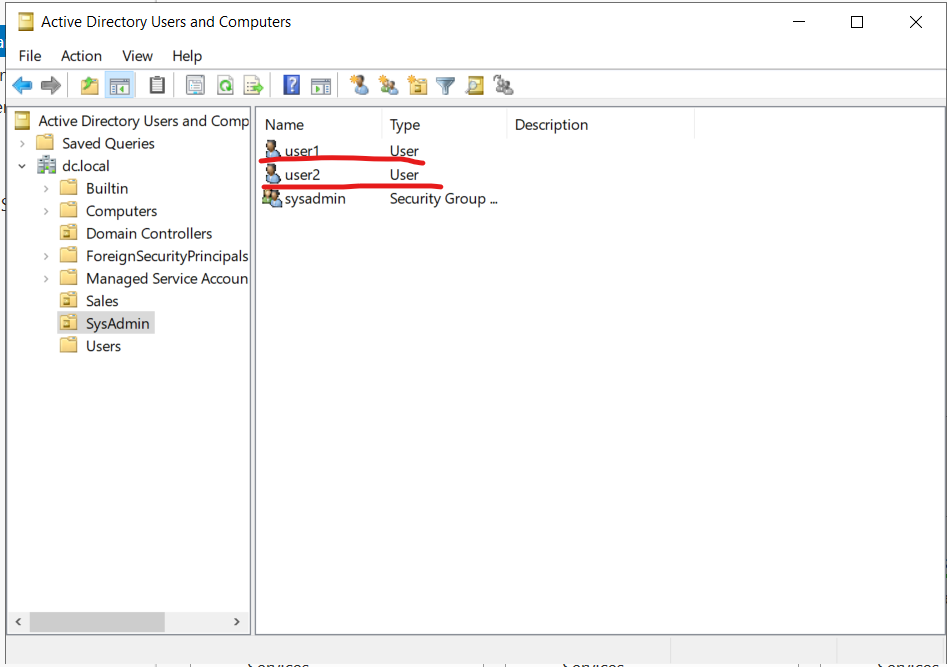
An organizational unit (OU) is a subdivision within an Active Directory into which you can place users, groups, computers, and other organizational units. You can create organizational units to mirror your organization's functional or business structure. Each domain can implement its own organizational unit hierarchy.

Creating OU –

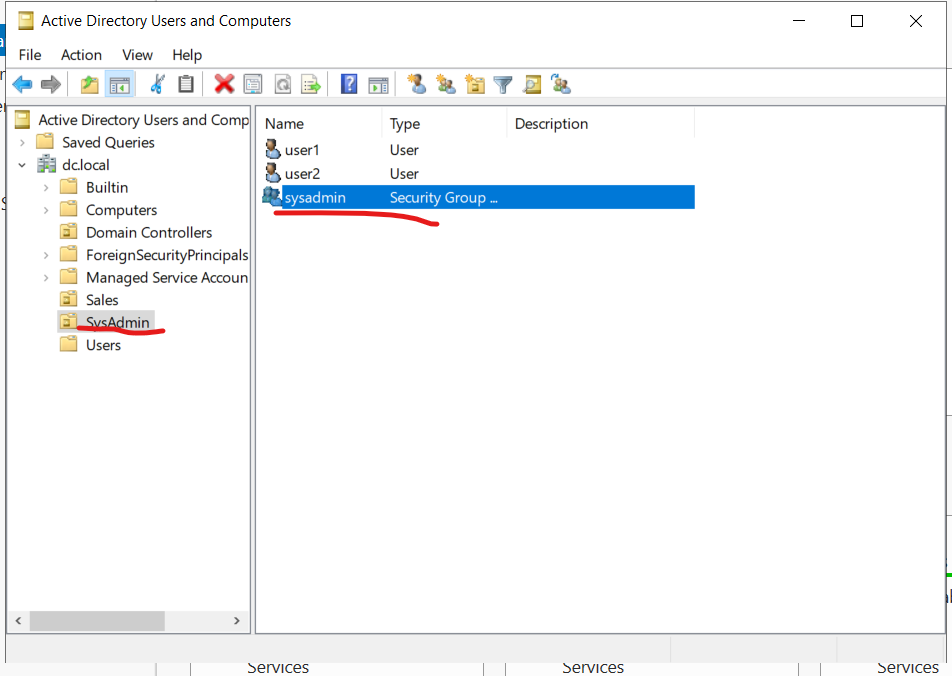
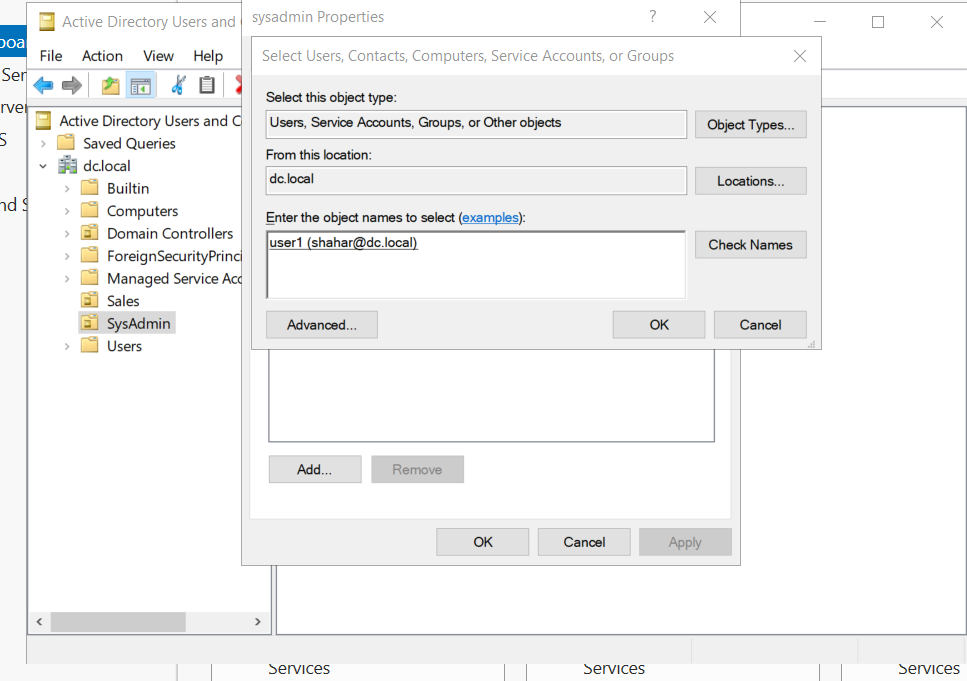
Let's create two OU's one for the “Sales” department and the other one for the “Sysadmin department, how we do that?

Tools-> active directory users and computers -> DNS server -> right click on DNS -> new -> OU

Create new two users to each of the OU's and name them (user 1/user2/user3/user4) 

After crating two users to every one of the units create group of each OU's and add the users to that group and name the group like the OU you create

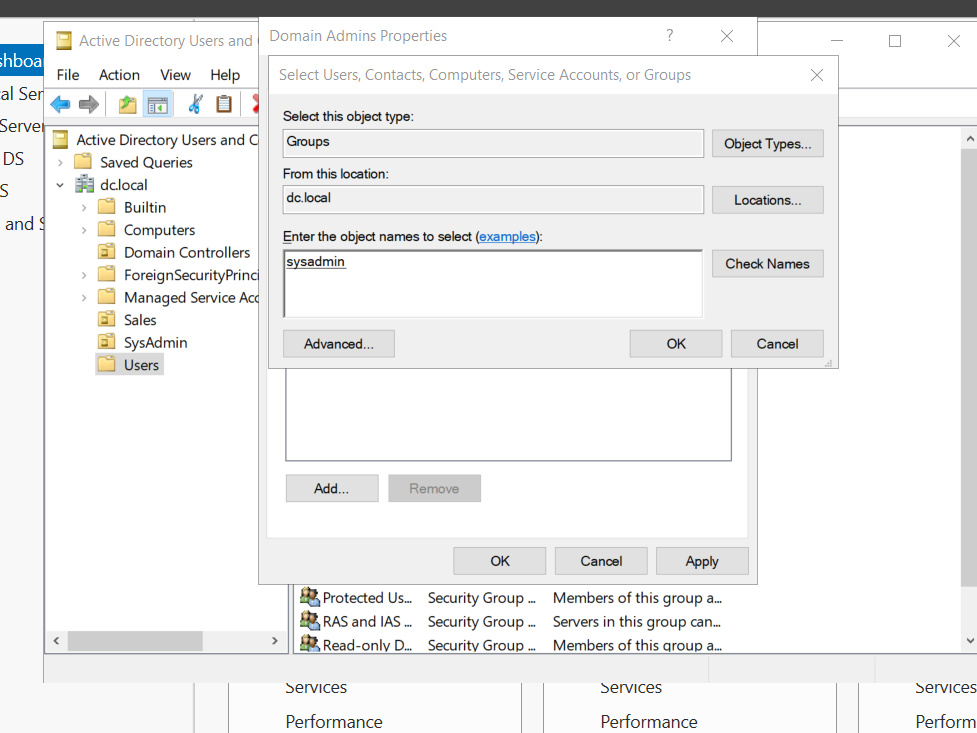
Exp:

Adding the users to the groups its going like this: double click on the group-> members ->add -> name of the users at the OU -> check name-> and add

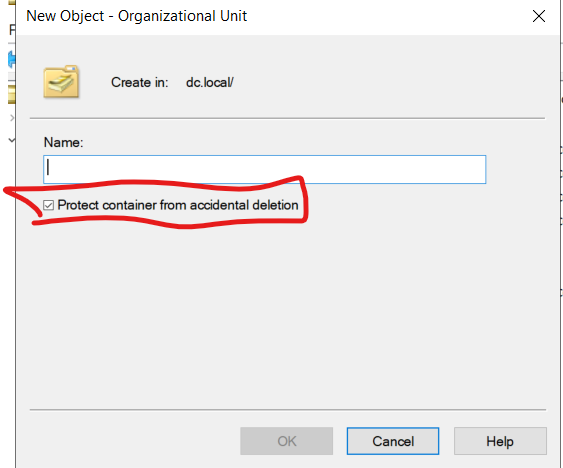
After we created users in the OU and adding them to a group we will set the privilege

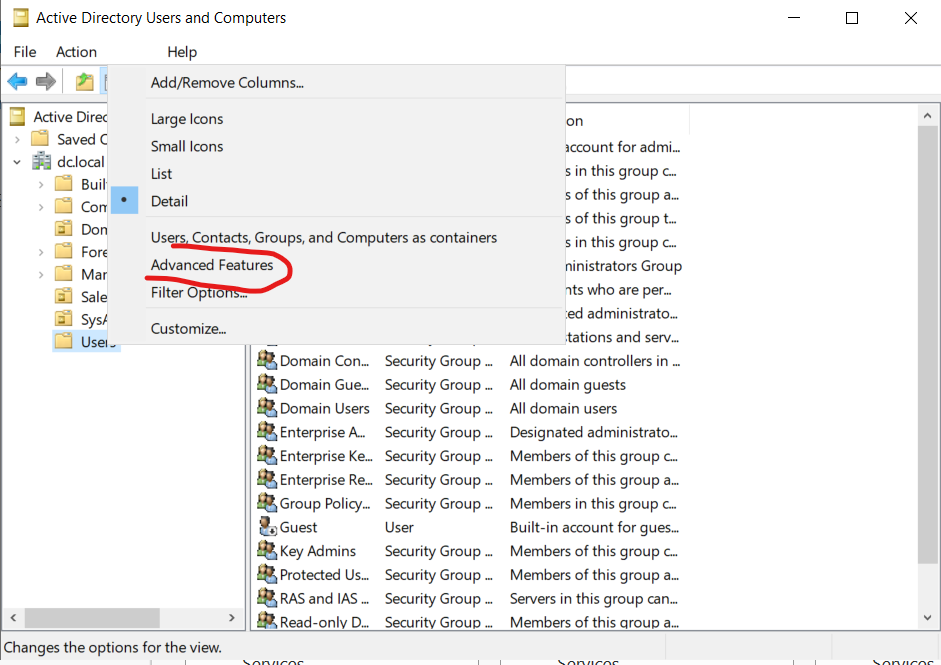
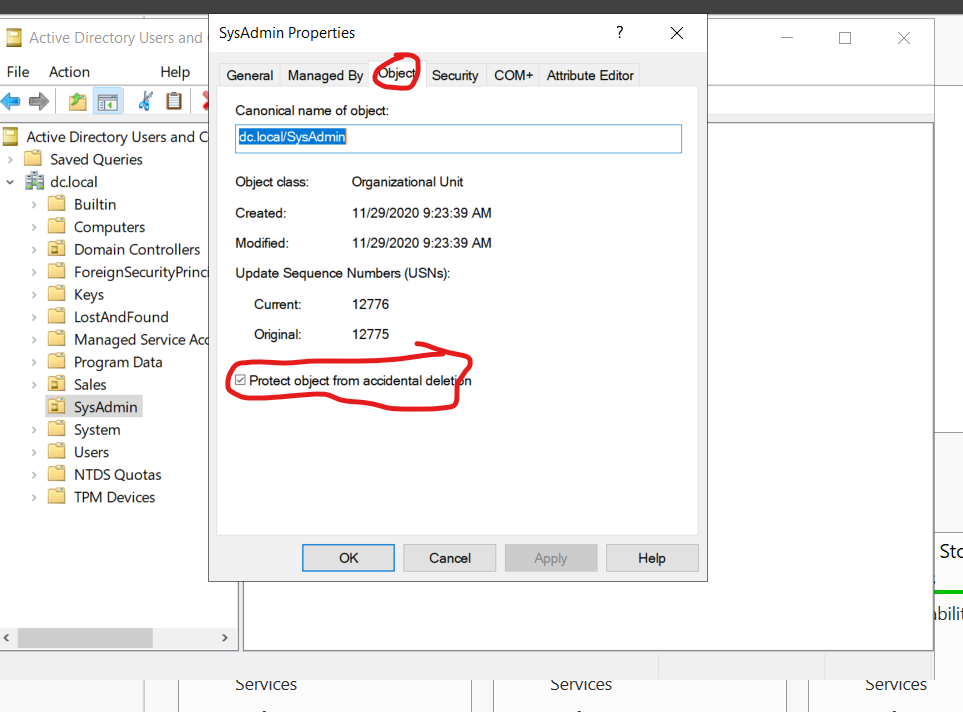
Of the units. we will add sysadmin to the domain admins, how its done?

Go to users -> domain admins-> right click -> properties-> members-> add-> sysadmin



Troubleshooting – Deleting an OU

If we try to delete OU we will get an error because when we create OU the windows ask us if we want to protect container from accidental delectation, so how we bypass it?

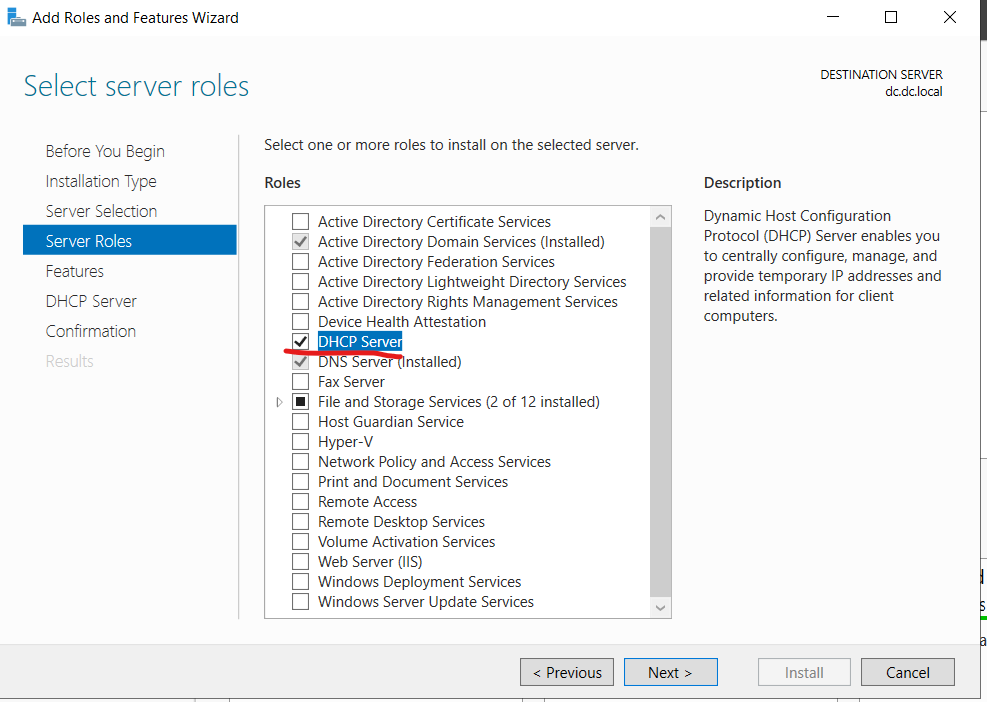
enable advanced features in View->Advanced Features now go to the OU you want to delete -> right click -> properties-> object -> un-checked “protect object from accidental deletion”. 

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) :

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring devices on IP networks, thus allowing them to use network services such as DNS, NTP, and any communication protocol based on UDP or TCP. A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks

Installing DHCP and setting static IP

To install DHCP server we will go to active directory-> tools-> add roles and features->server Roles -> add DHCP and install



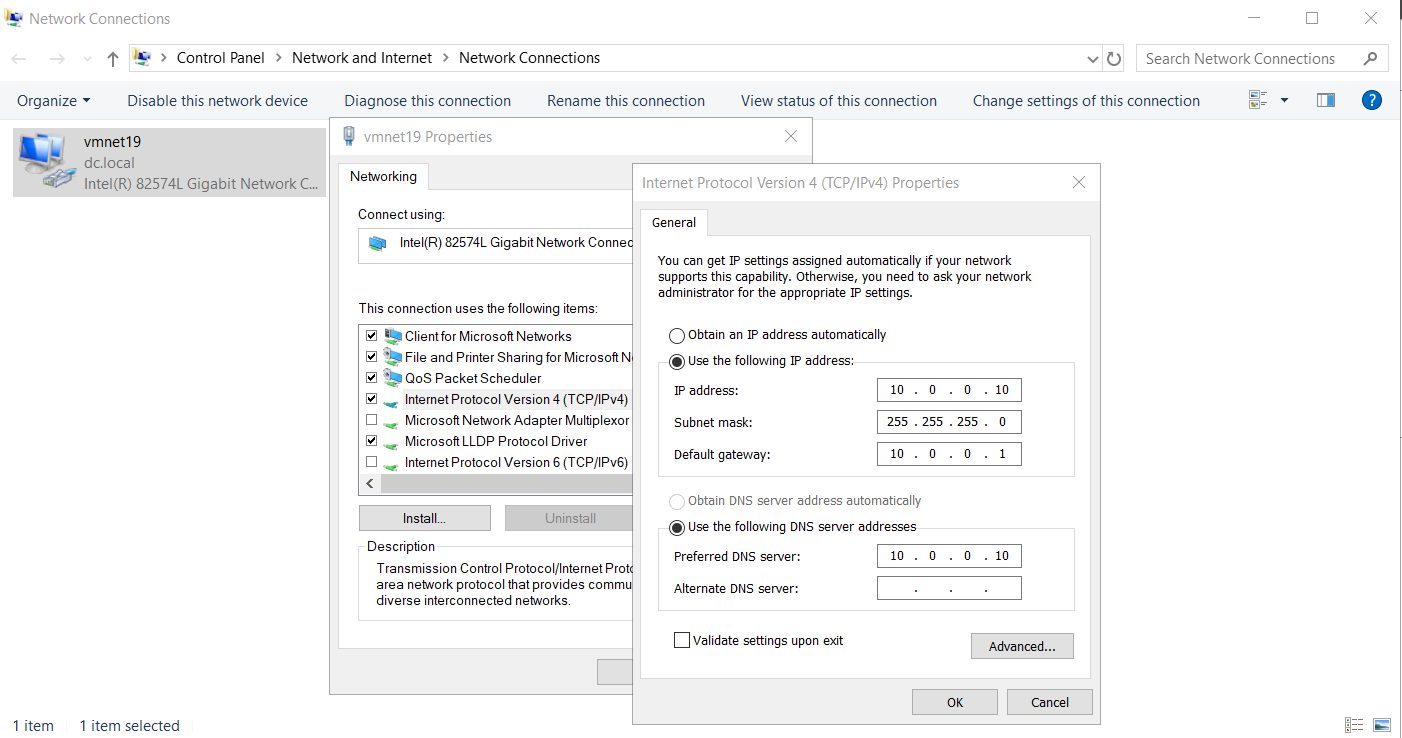
We need to configured the network driver IPv4 address by manually, by:

Win KEY+R (to open run menu) type NCPA.CPL and enter -> driver properties

And remove ipv6 and double tap on ipv4, setup those settings

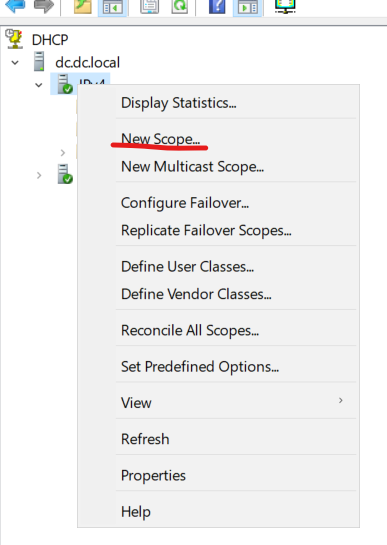
Ip 10.0.0.10

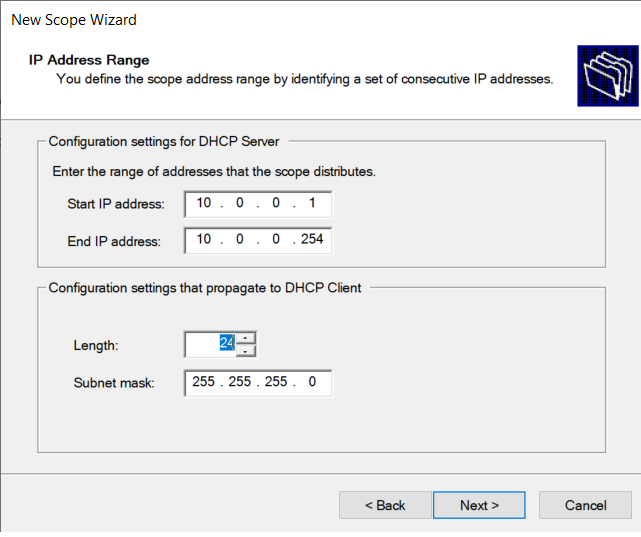
Subnet mask 255.255.255.0

And because the server is the DNS, the DNS is 10.0.0.10

After we setup the DHCP manually we will configure the DHCP (yellow flag configuration) and add to it scope that is going to dividing at least 50 IP addresses to our network,

Tools-> DHCP ->ipv4->





Set the start IP and the end IP of the network also set the subnet mask, add the server ipv4 10.0.0.10 as exclusions and set the lease time to 8 hours



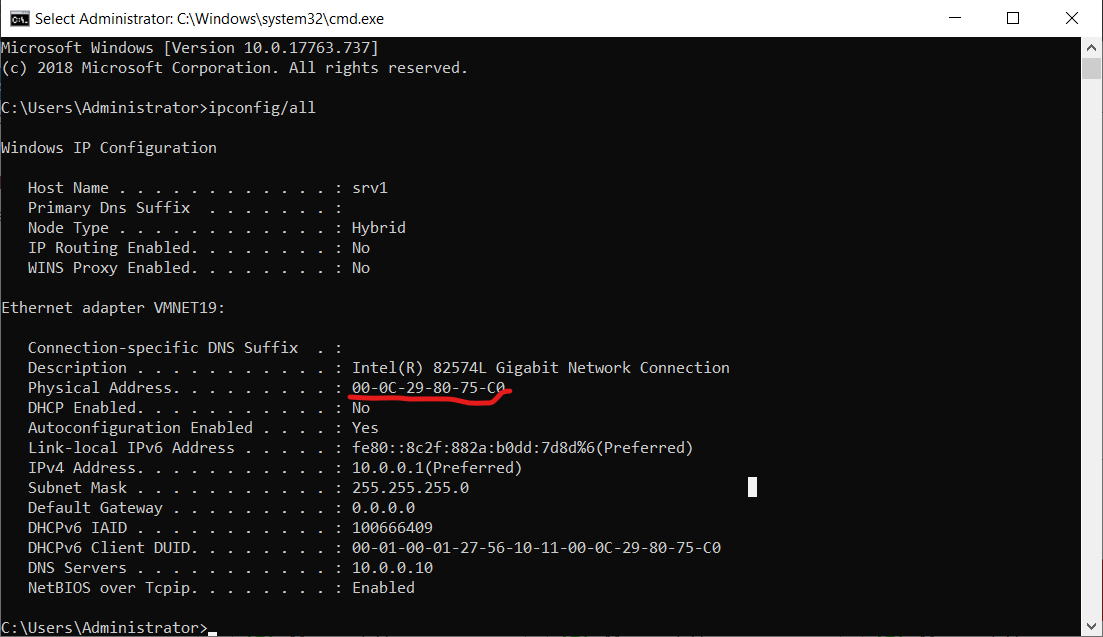
Now let's crater new reservation for our new server after we install it , we are going to name it SRV and its going to serve us as a router under the IP 10.0.0.1 that we excluded earlier as a default getaway, lets setup

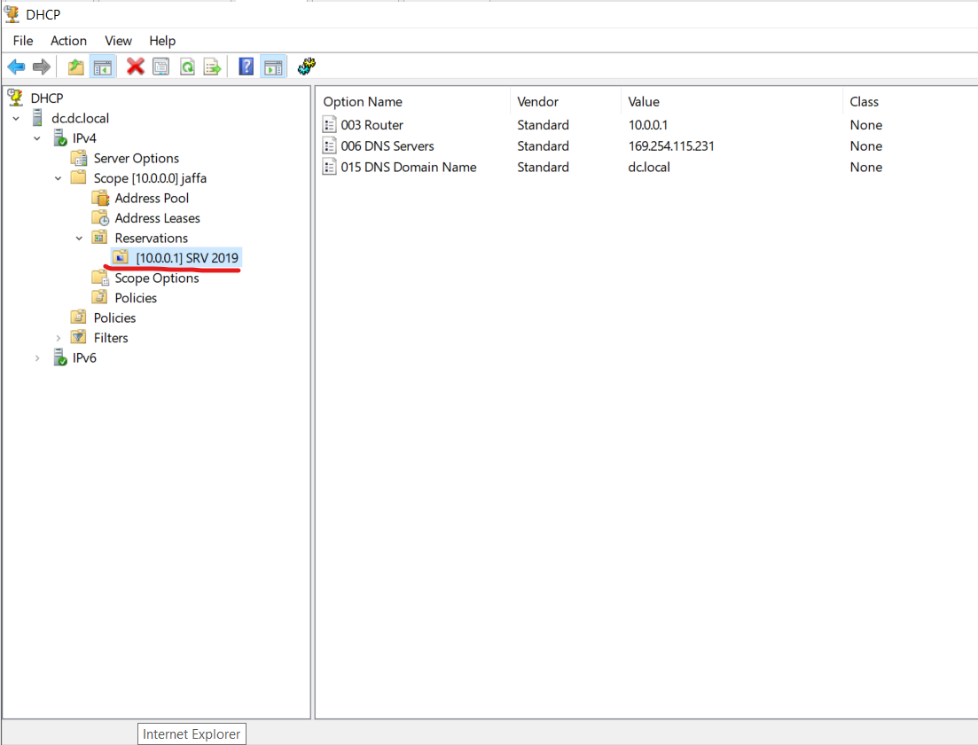
Go to server manager-> tools -> DHCP->scope->scope reservation-> new reservation->put the IP address as 10.0.0.1

now we need to put mac address, how?

go to the new server (SRV) -> WIN+R-> type CMD and press enter ->type ipconfig/all-its going to show us all the IP configuration of the server, and we will see the mac address

copy it and type it on the reservation in the DC server



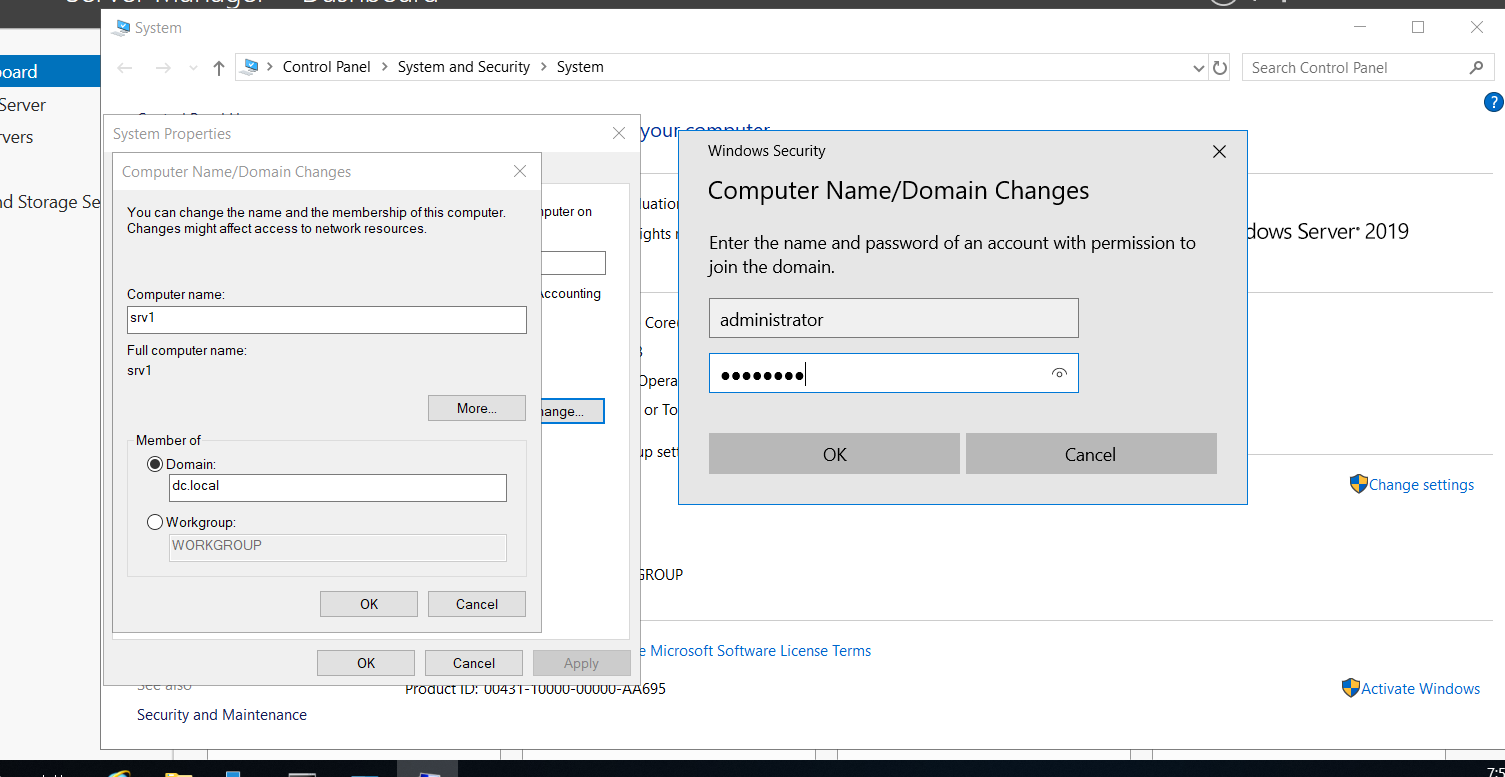
And press ok and that’s all now we can see we have the SRV reservation on the domain controller ,

Now lets check if the IP address is correct like we did at the reservation –

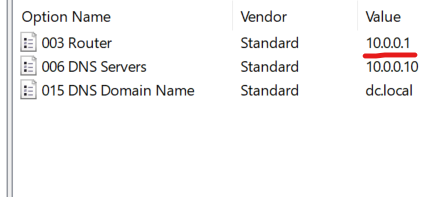
WIN key+ k -> CMD-> ipconfig/all



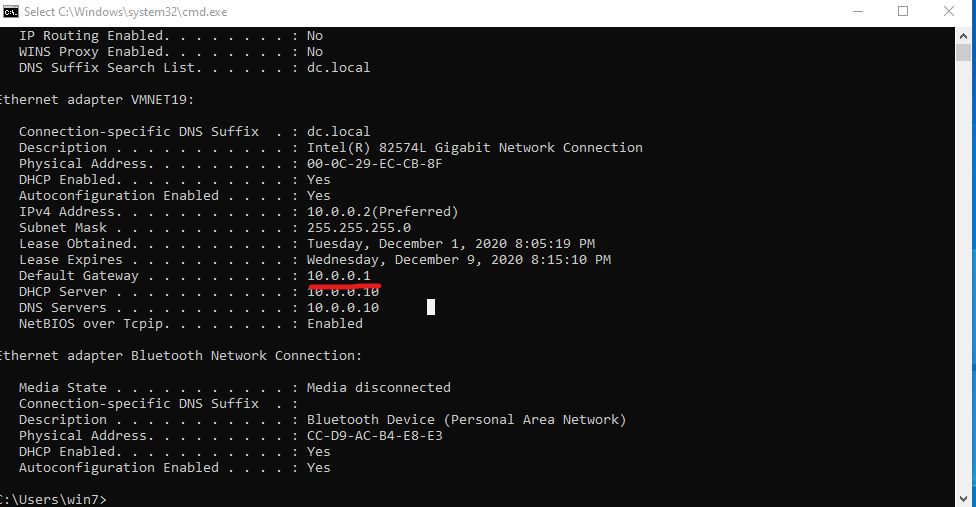
Every thing is working fine . we can see that we have DHCP AND DNS from (DC)

After check everything is fine we need to put the SRV at the domain (dc.local) Go to my pc-> settings> change setting->change ->member of domain-> type the domain name and password and that’s all 

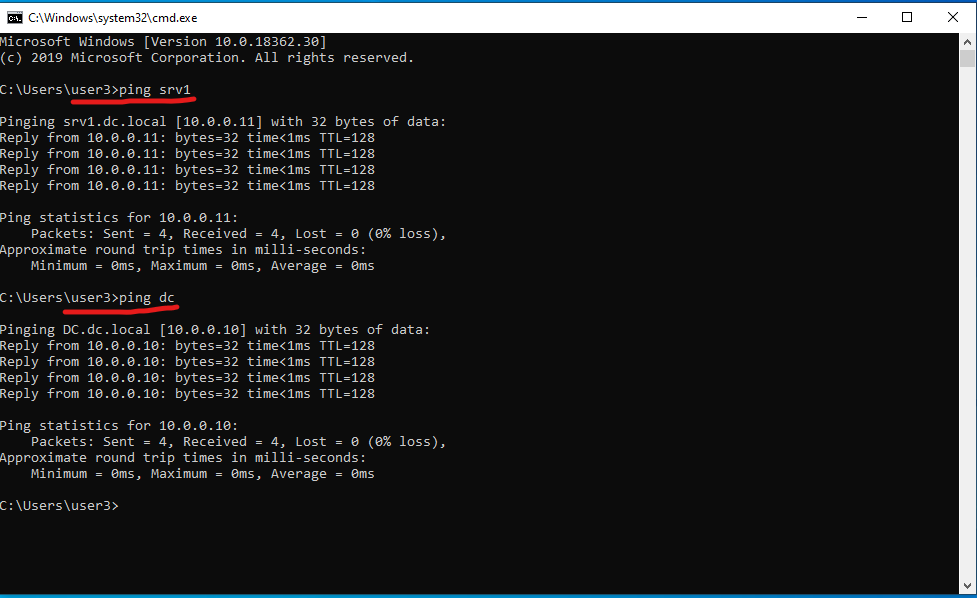
And that’s all.

Now let's set the default getaway as 10.0.0.1(the SRV Ip address) on the DHCP scope settings – server manager->tools->DHCP-> scope->scope option -> router-> 10.0.0.1

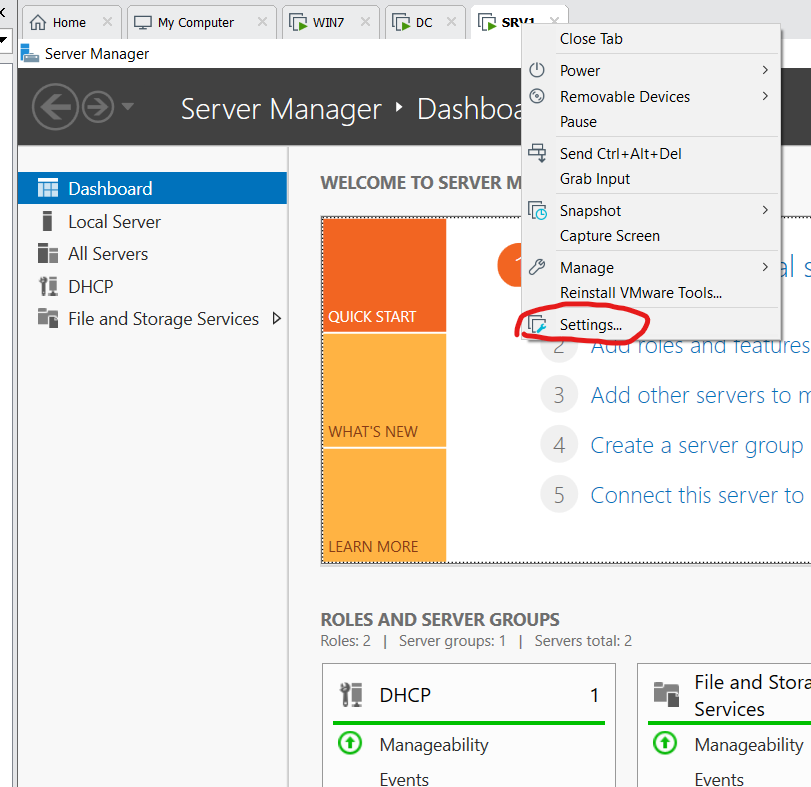
Lets modify at the win10(client) that the DG is correct – CMD->ipconfig/all

 We can see the Win10 client received the IP address 10.0.0.2 from the DHCP of DC and the default gateway of SRV which is 10.0.0.1.

And now lets see if there is an connection between DC to the SRV and the Client with CMD (ping command )

 Here we see we have connection between the client and the servers.

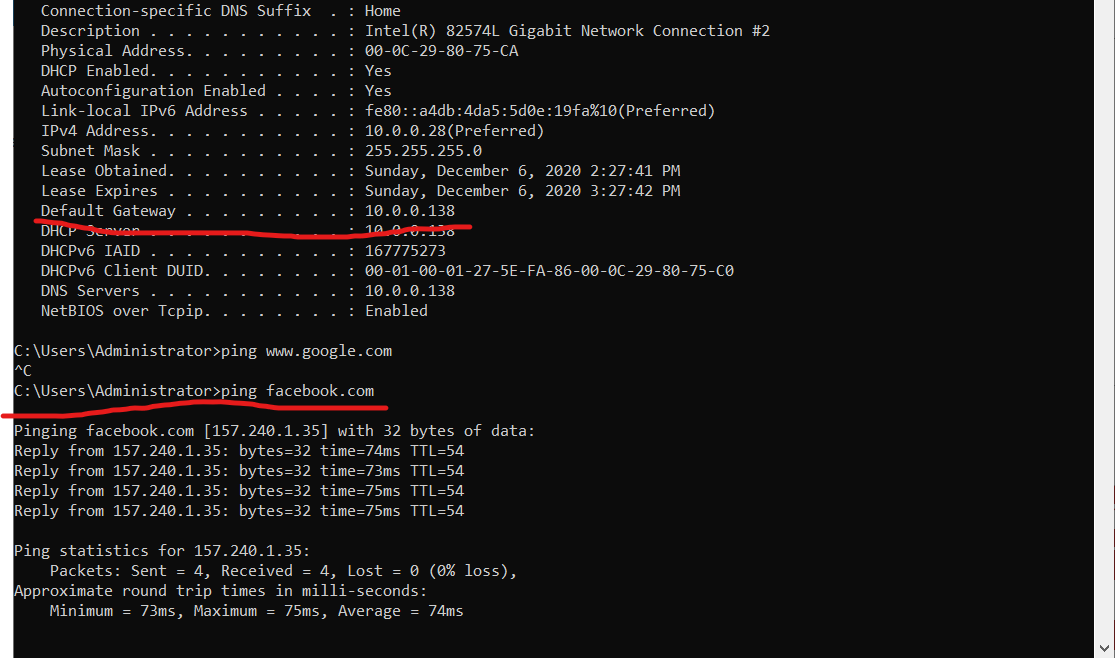
SRV Internet connection (WAN) –

To begin browser at the internet we need to connect our SRV1 to public connection , so we are going to the srv1 and add network adapter but this time we will don’t set it as VMNET but as NAT

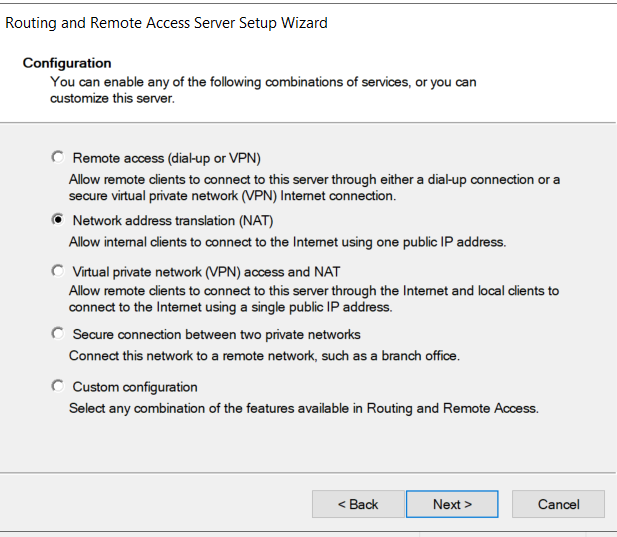
Settings->add->network adapter-> NAT

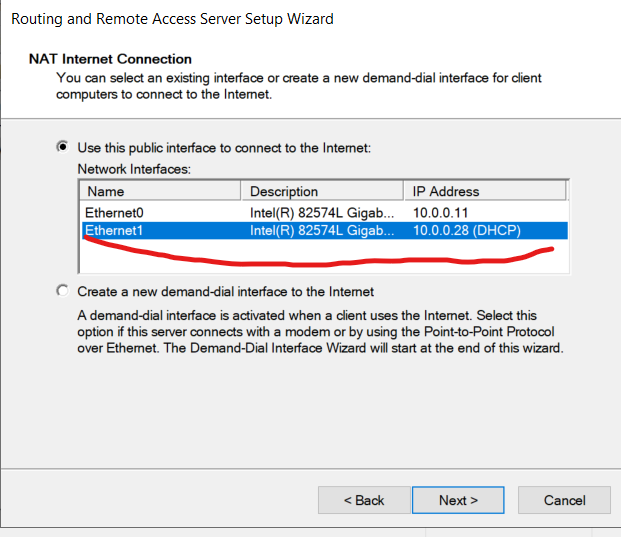
Now we can see we have internet connection

Now after we apply the internet connection, we will verify that is working ,so I ping facebook.com to see if we have connection and it worked

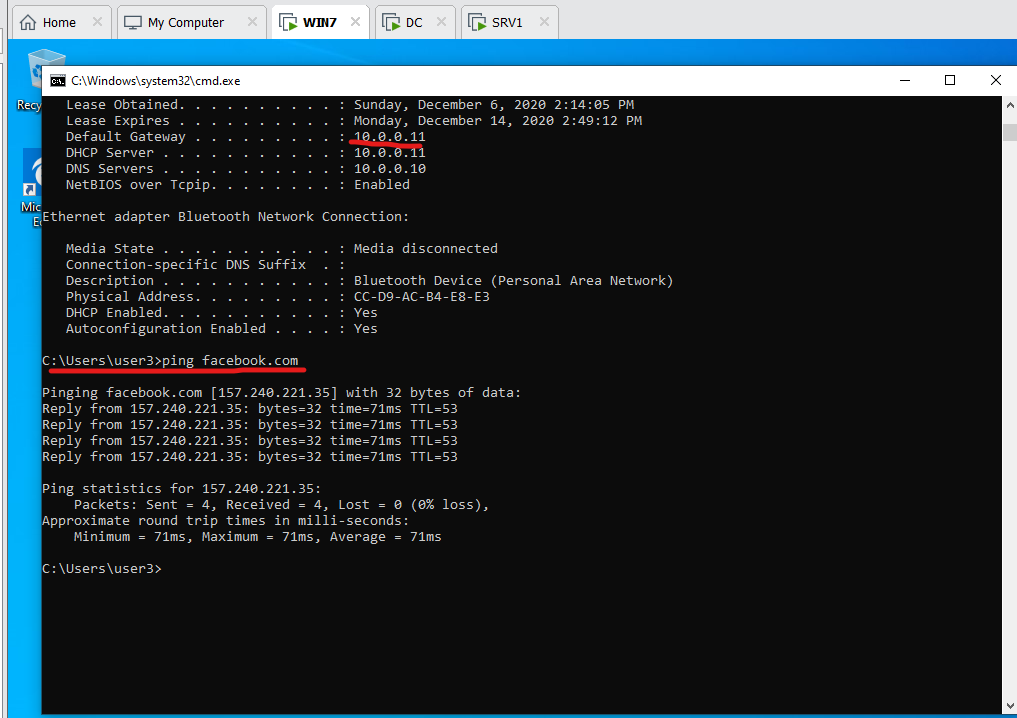


If we look closer, we will see we have default getaway and DNS server from our WI-FI 10.0.0.138

Routing & PAT I installed a new role which called NPAS (Network Policy and Access Services) and RA (Remote Access) in Server manager->Add Roles and Features->NPAS & RA (for RA I added Direct access and VPN & Routing options in the role services part).

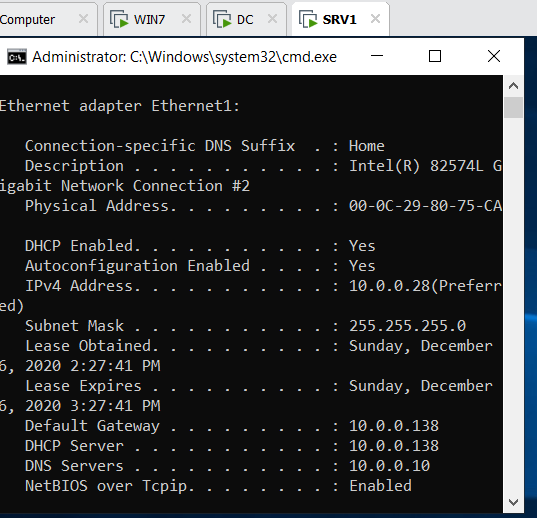


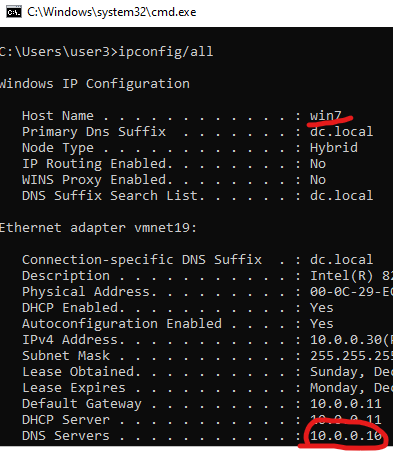
We need to choose the new adapter we just add (the internet port ) and not the vmnet19

In the photo below, I checked if Win7-client can access the internet

And we can see Win7-client is able to get reply from FACEBOOK (there is internet connection)..

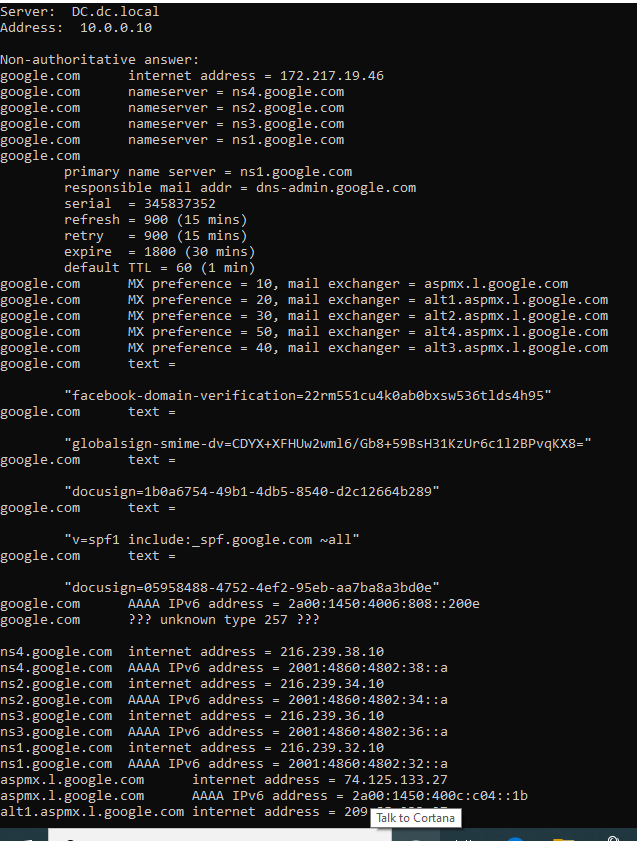
DNS Server Configuration

Before we start the configuration, we need to check if all the servers and clients use the same DNS server (DC-10.0.0.10)



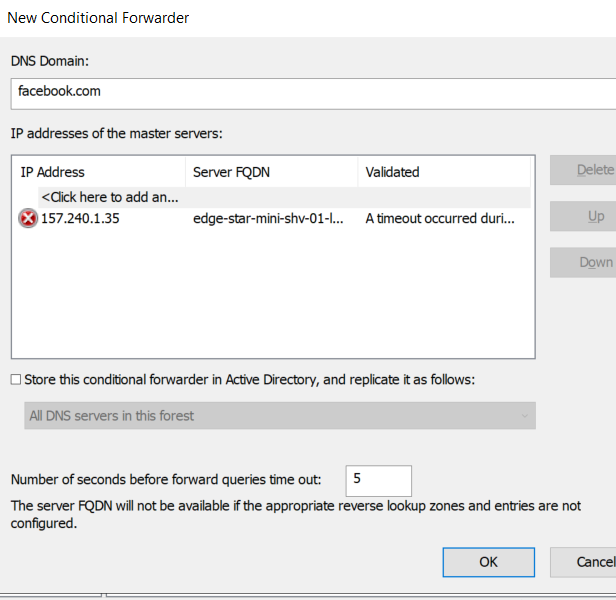
On the DNS manager within the DC server I added google forwarder (8.8.8.8) in the DNS server.



Now to see if there is a forward on google.com DNS server – we will go to CMD at win7 -client and see if there is a translation from google.com to IP address by using (NSLOOKUP)

Like we can see every thing is working like it spouse to be.

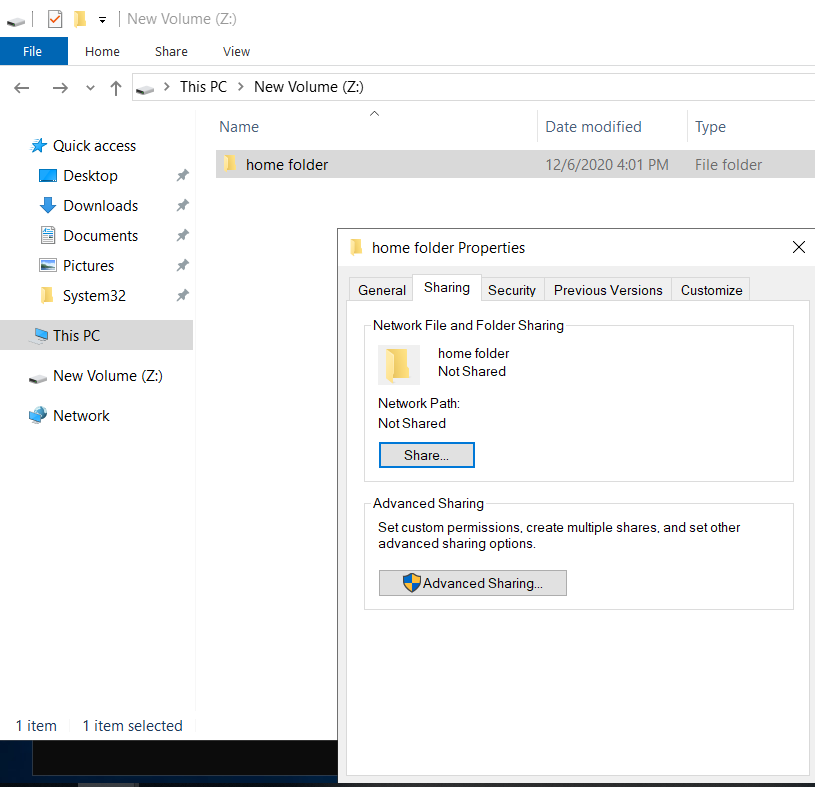
Now in my organization I want people to work and not to play games and talk to people so I will block FACEBOOK with Conditional Forwarding.

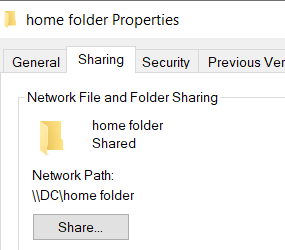


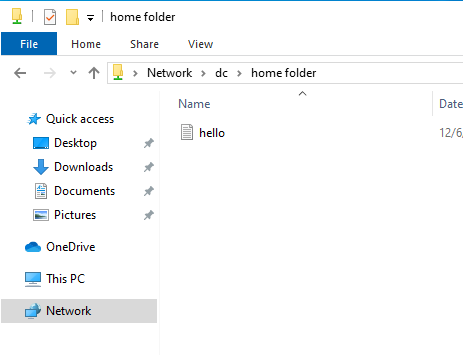
Now lets check if it works: by going to the browser and type facebook.com

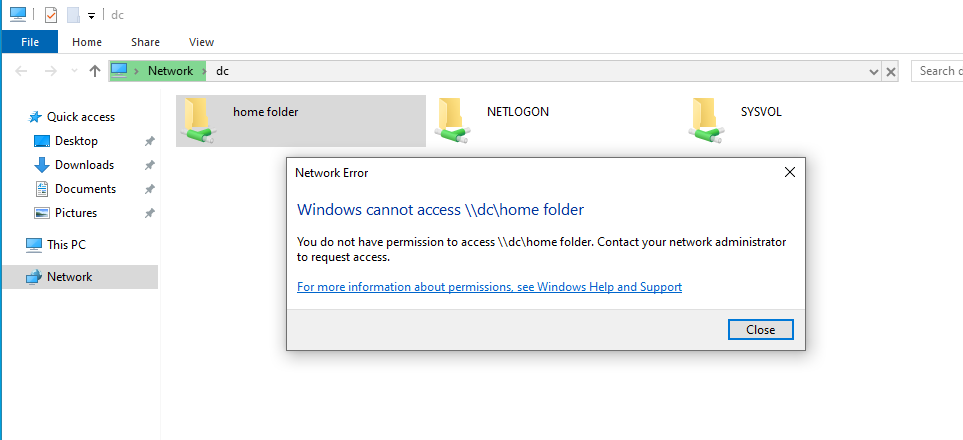


Shares and mapping-

I created new disk partition with 30 GB space and set the path Z:\ and in the folder properties i started setup the permissions of everyone. Exp: only user1 can access folder of user 1 , and user 2 can access folder of user 2 .

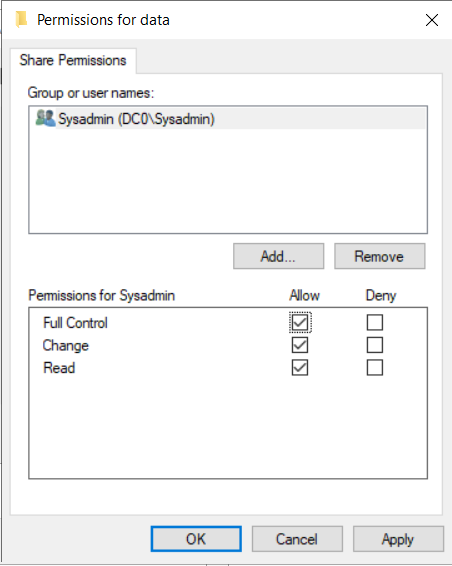
First we need to share the folder by going the folder properties-> advance sharing-> share folder->permission->remove everyone -> add Sysadmin group

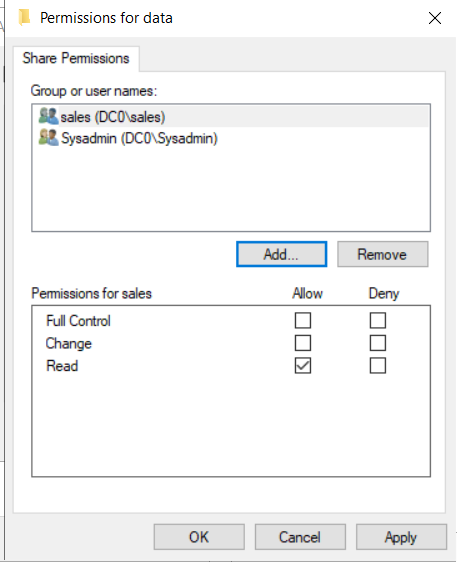
After we did that we can see we have path to home folder but only user under Sysadmin group can access it lets check that. We can see that with user 3 (Sysadmin) I can access to the folder

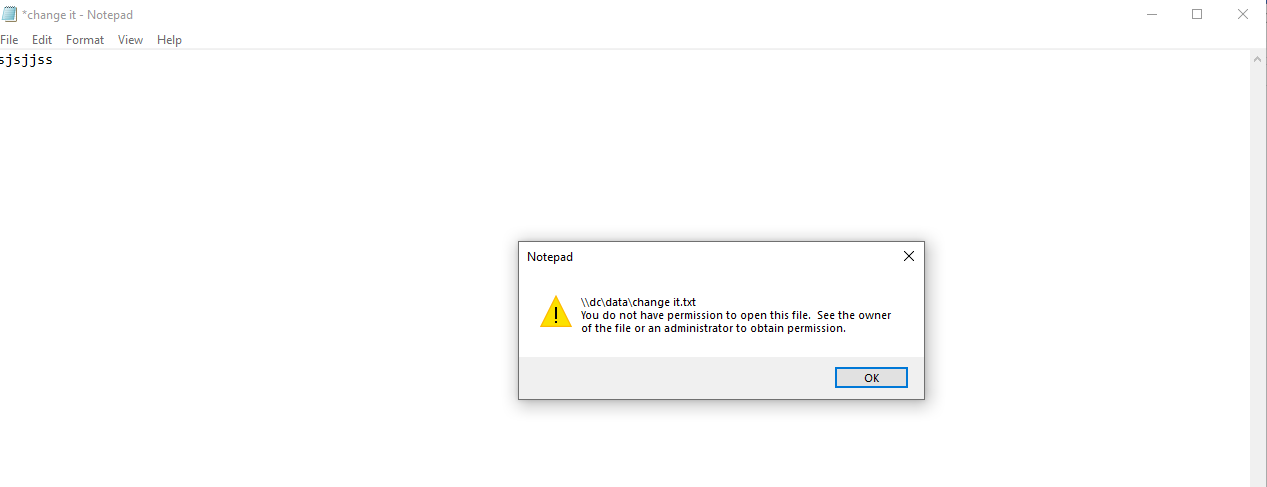


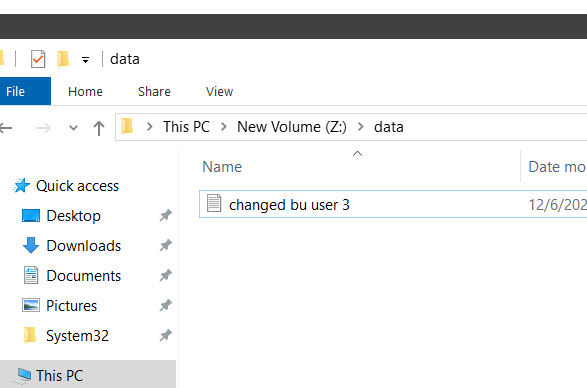
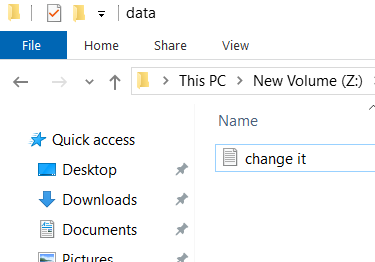
Now let's check on user that don’t have permission to the folder, if he can open it. And we see that he can't .

Data folder-

I created new folder named (Data), in this folder properties I enabled sharing and removed Everyone access. I added new sharing access to “SysAdmin” group with Modify permission and “Sales” group with only read & execute access.

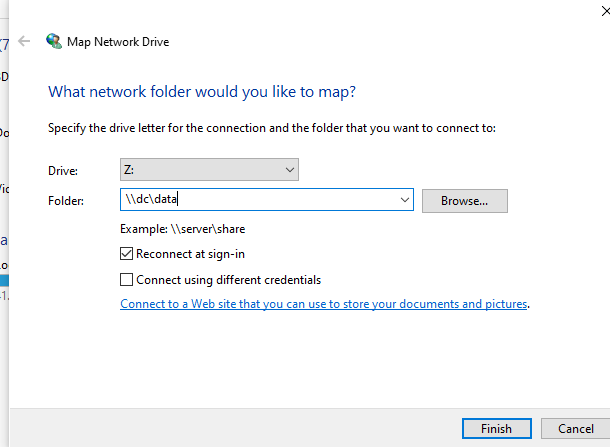
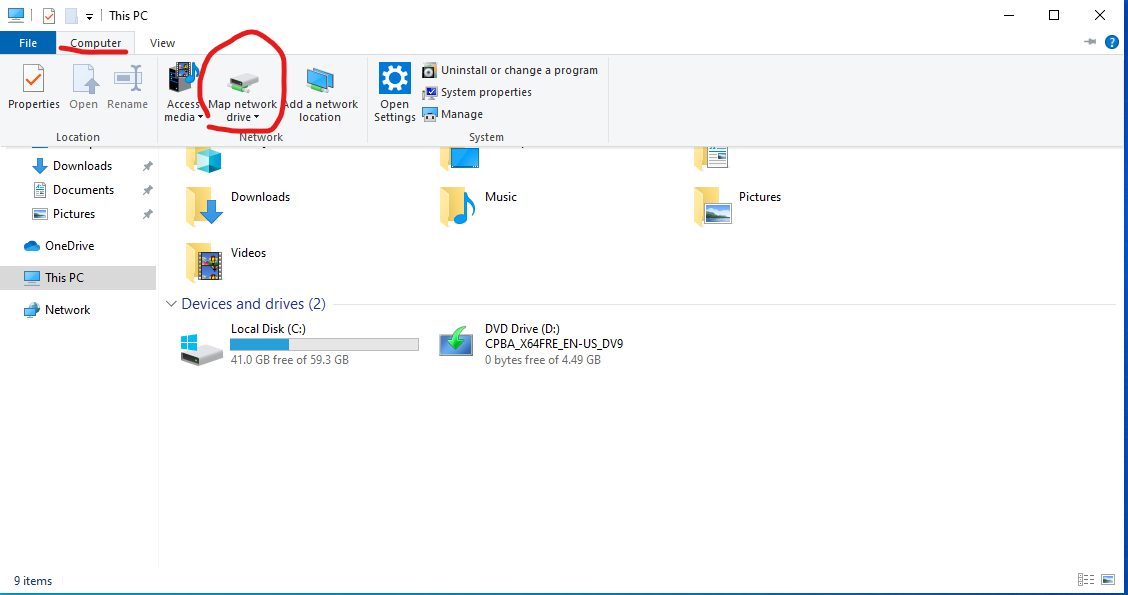


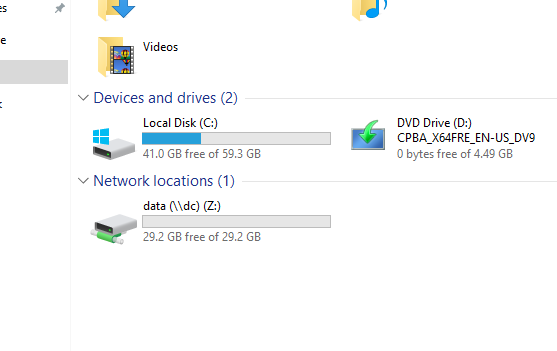
Here we can see that I set the permissions of the sales and Sysadmin groups , in the right side we have sales group with read and execute permission and in the left side we have the Sysadmin group with modify permission. Now to see if our permissions works we neet to test it.



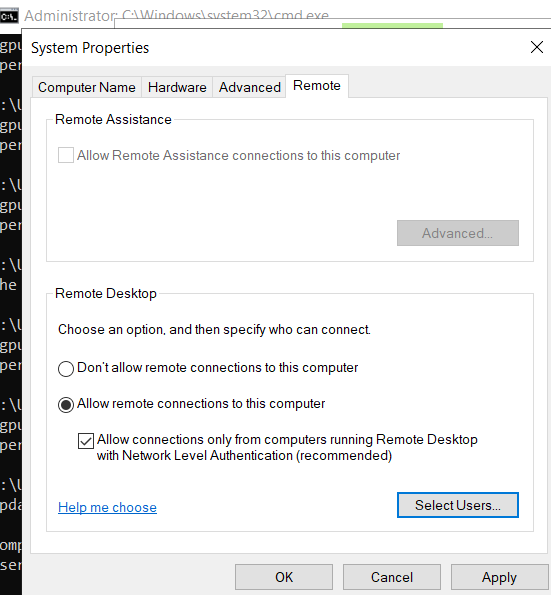
Like we see user 1(sales) cant save the file because the permission of only read ,now lets try with user from (Sysadmin) group, user 3 changed the name

Data folder mapping –

To map the folder Data to all the users inside “SysAdmin” & “Sales” groups, we need to go to folder browser -> this pc -> computer (at the task bar on the top->

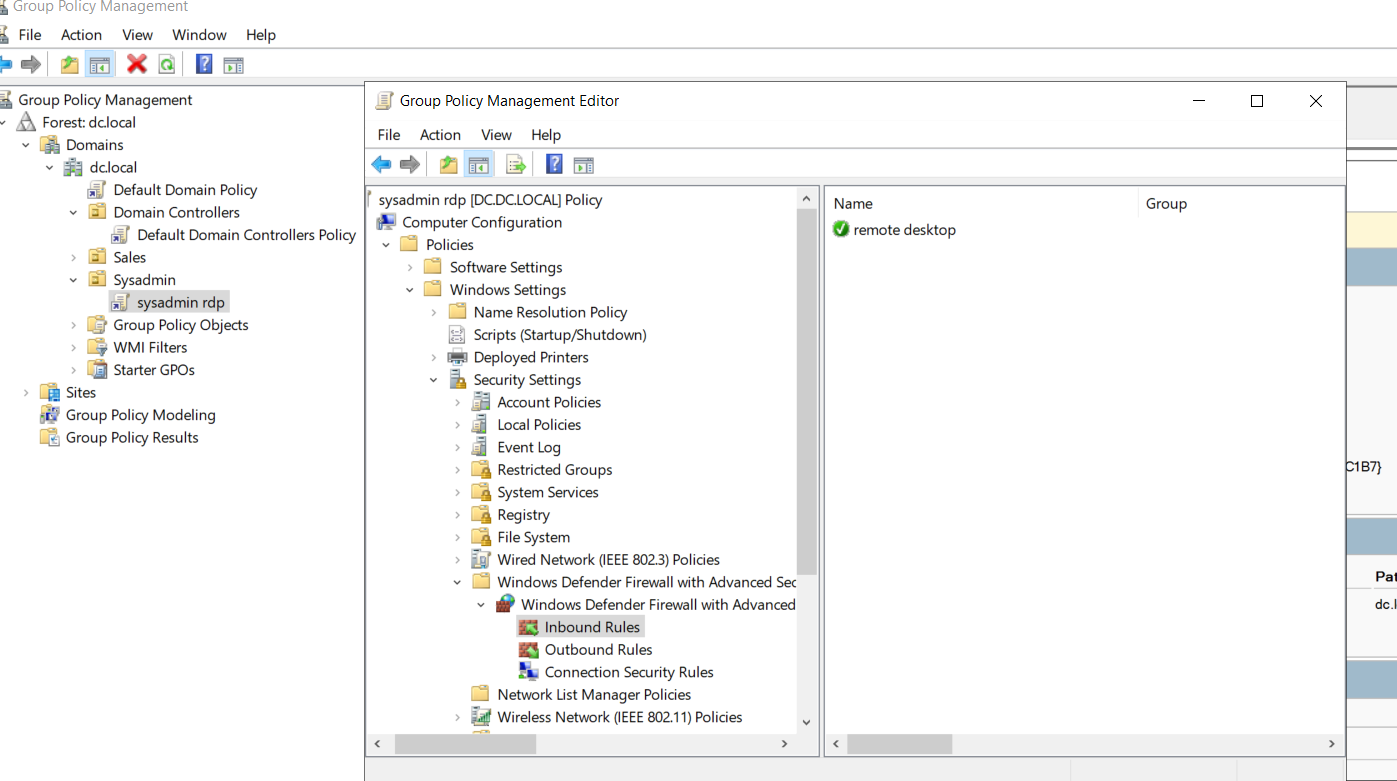
Search for the folder we want and finish, and the folder will poop up to the pc driver list.

Now we allso check that the premissions didn’t chanched . and that’s all .

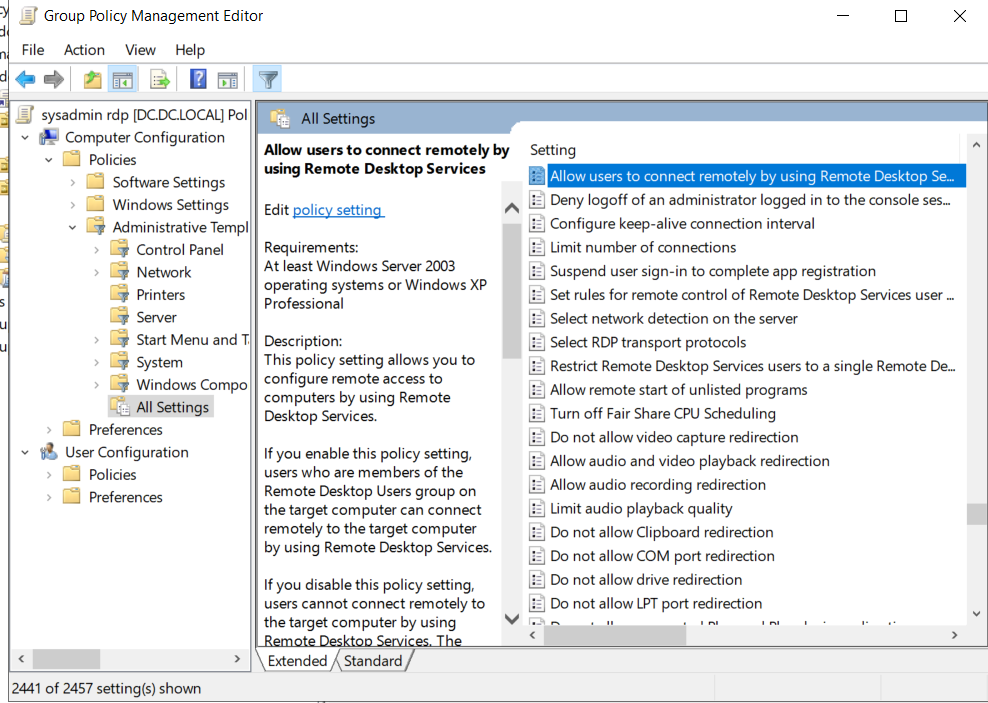
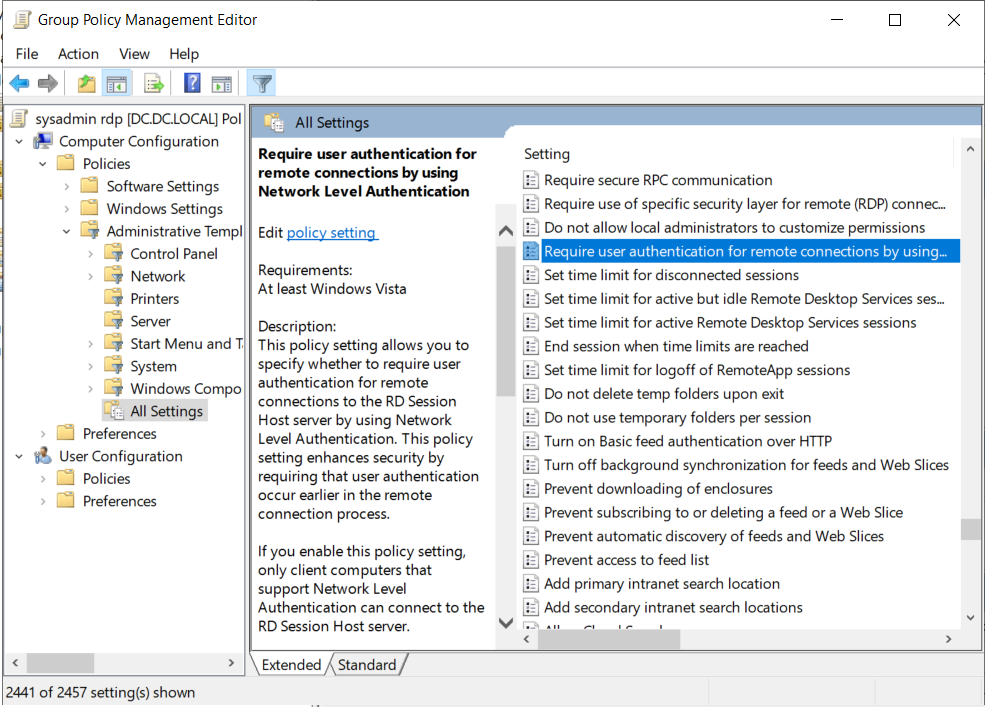


Remote desktop –

First of all , to all remote desktop between the pc's we need to allow it in the computre settings , by going to -my pc-> properies-> remote

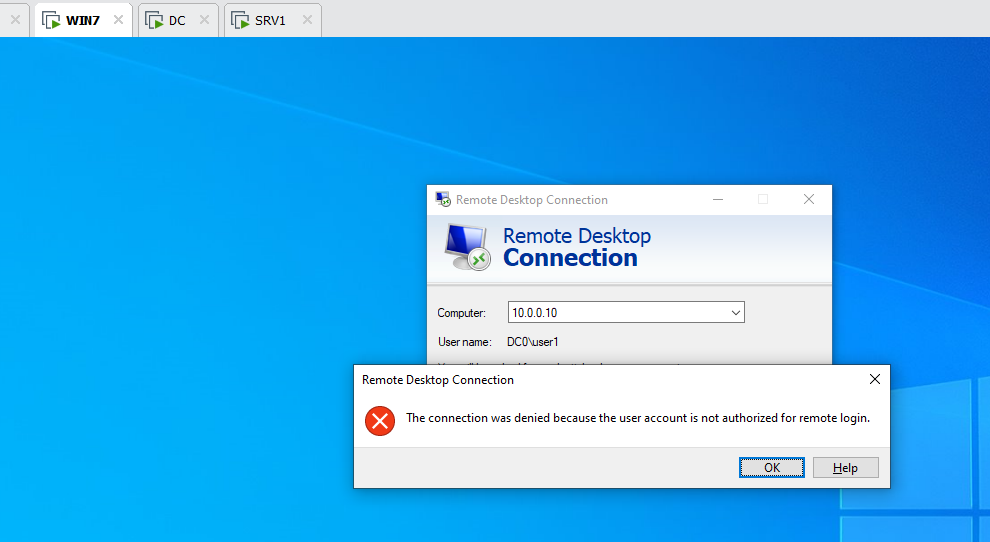
After I enable remote desktop , I crated new GPO for Sysadmin and sales group , Here I added a firewall rule that allows inbound connections to port 3389 (RDP PORT) on my Domain network.

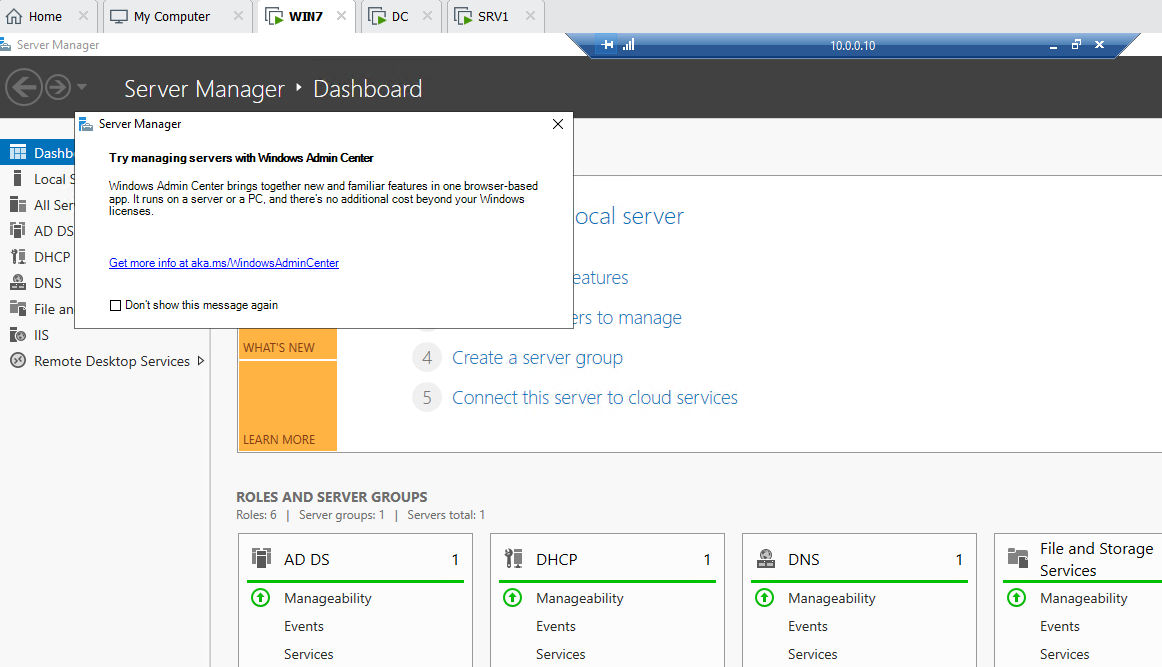
I enabled also “Allow users to connect remotely” option

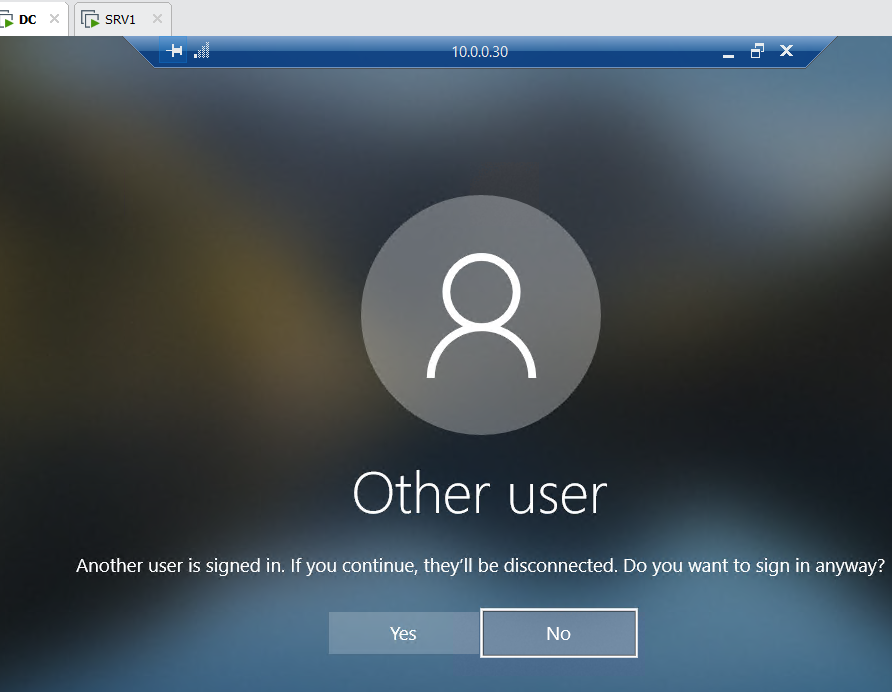
and to setup that only Sysadmin can remote desktop ,we will allow “user authentication'' do avoide sales group to remote desktop”

now to check ill use from sales group user1 and from Sysadmin user3 for remote desktop access

user 1(sales)

 user 3 ( Sysadmin)

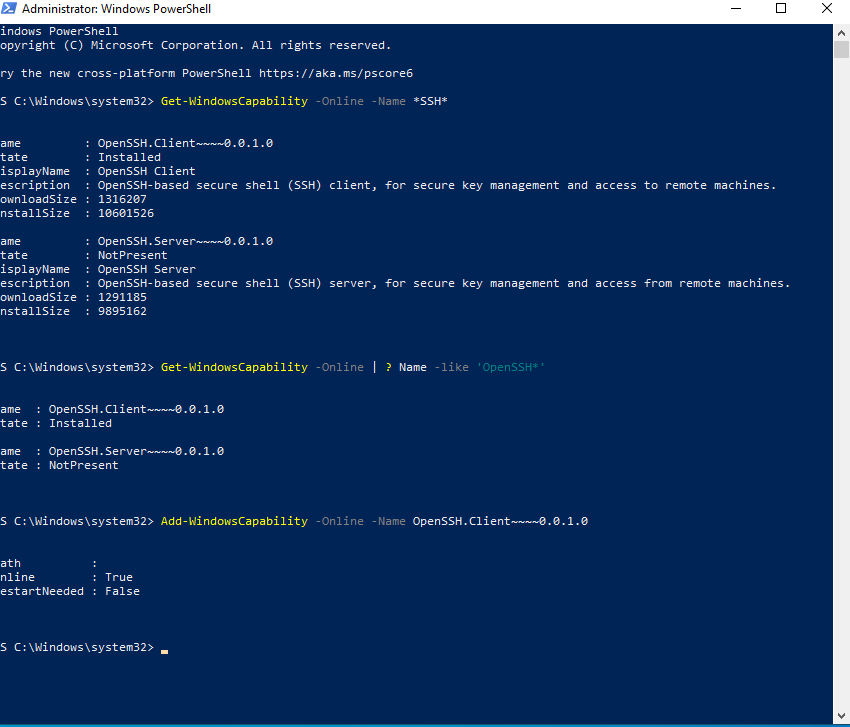


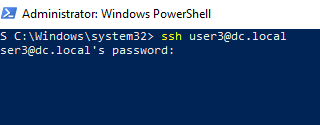
dc to user 

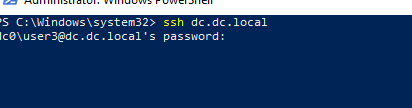
now we can see that all the remote desktop between all the sides are working

SSH REMOTE- SSH or Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH

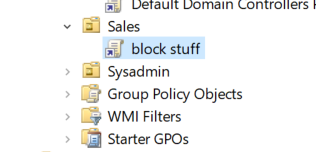
To install ssh from powershel as administrator we need the configuration , we can find it here [Installation of OpenSSH For Windows Server | Microsoft Docs](https://docs.microsoft.com/en-us/windows-server/administration/openssh/openssh_install_firstuse)

First, I installed OpenSSH on the Win7-Client through PowerShell and started the SSH service, in addition I set the SSH service to start automatic whenever the machine is online

After we install and setup port 22 we will try to connect with ssh to user 3

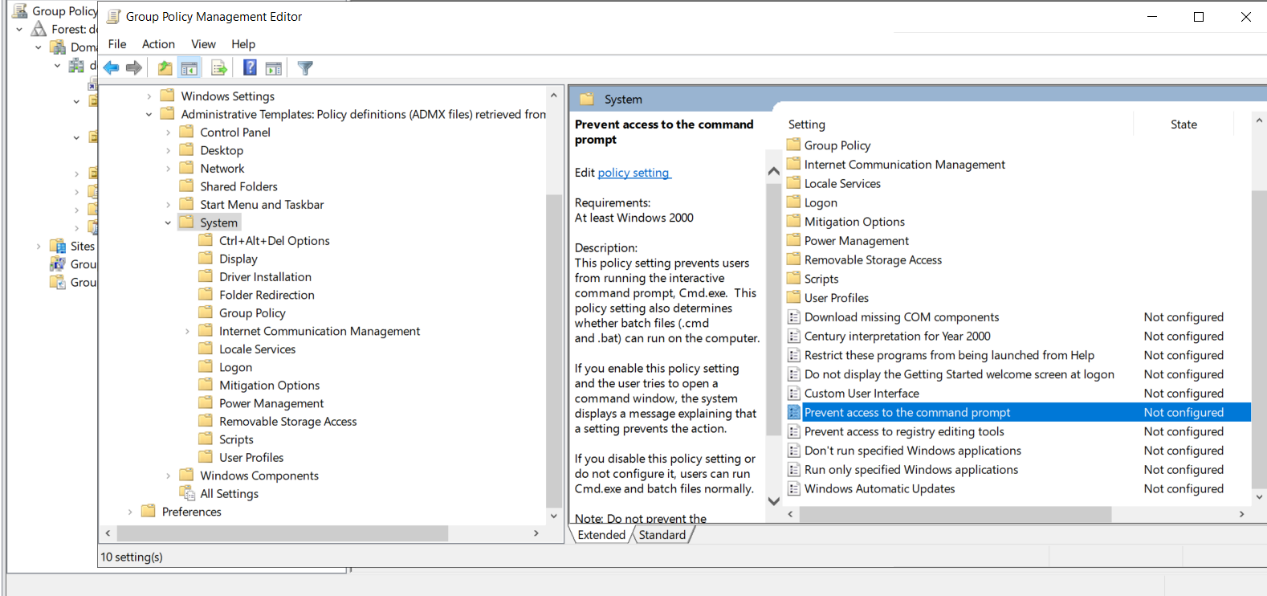
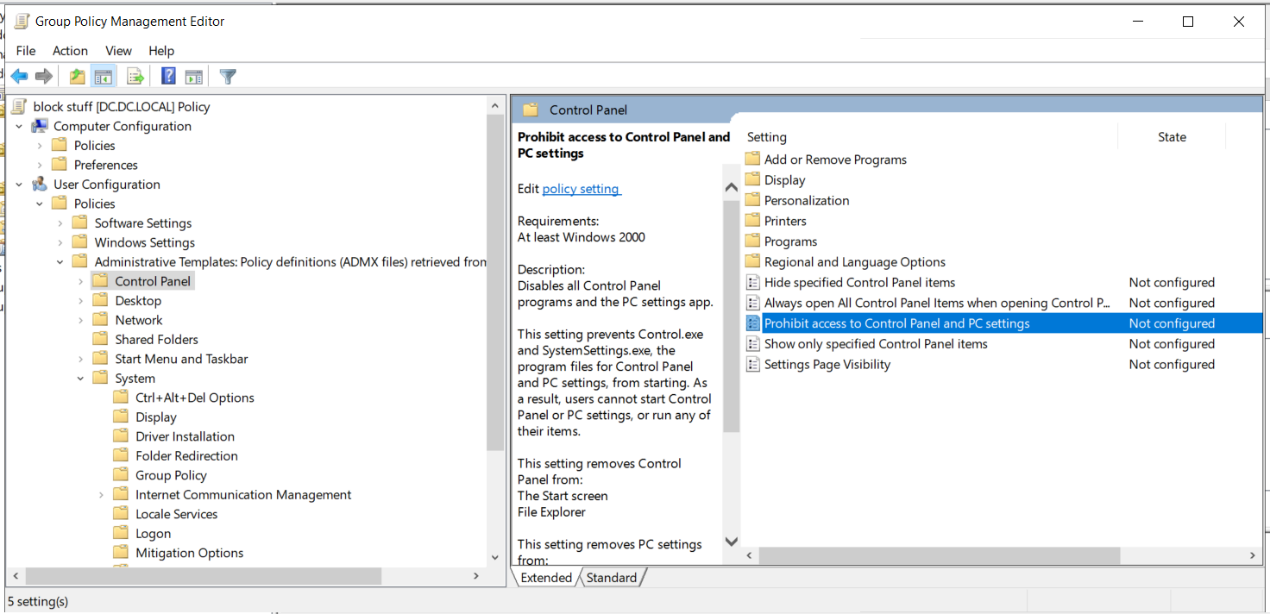
Like we see its asking for password that’s mean the connection its working 

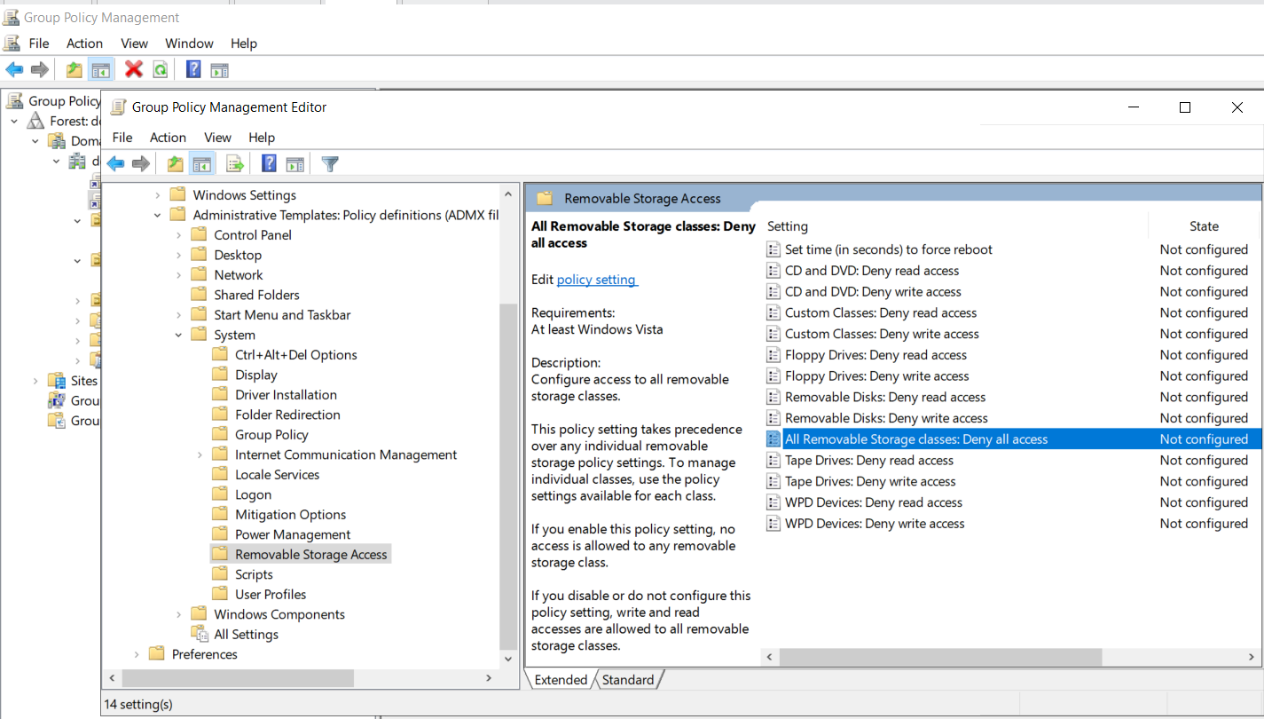
And like we see here I ssh from user 3 to the domain controller and it works

GPO restriction-

I created new GPO under block stuff to disable users under Sales group to access control pannel and to the cmd.

So here I prevent to access the controll panel

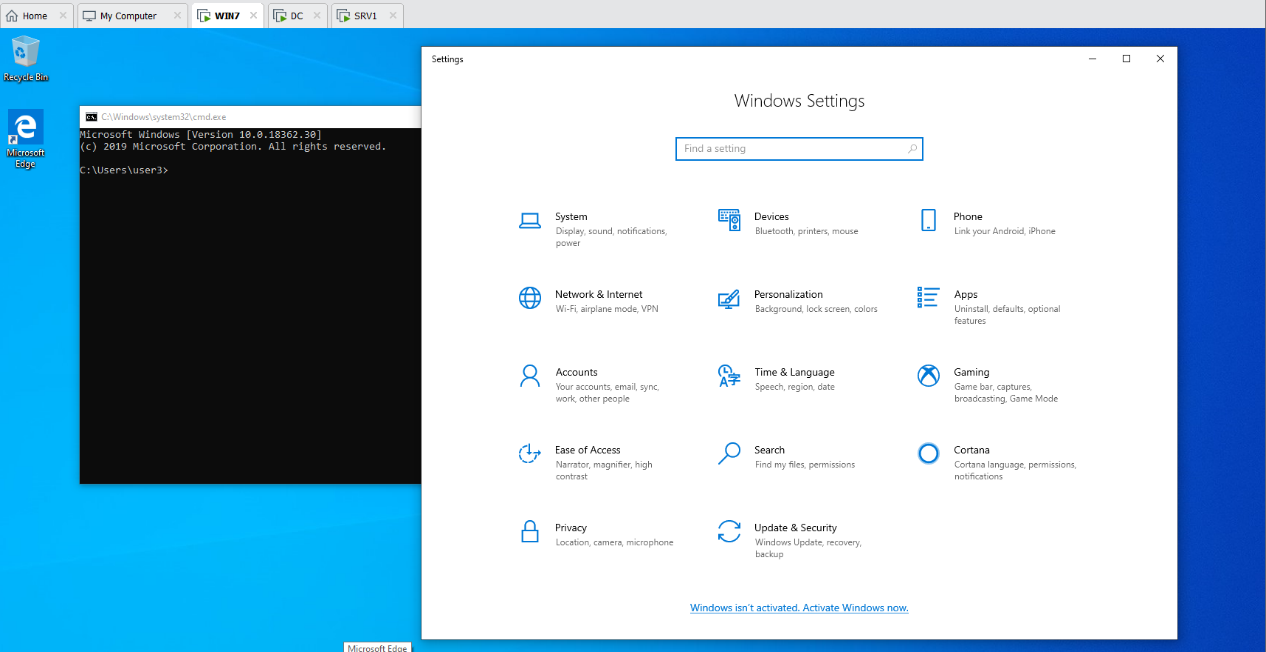
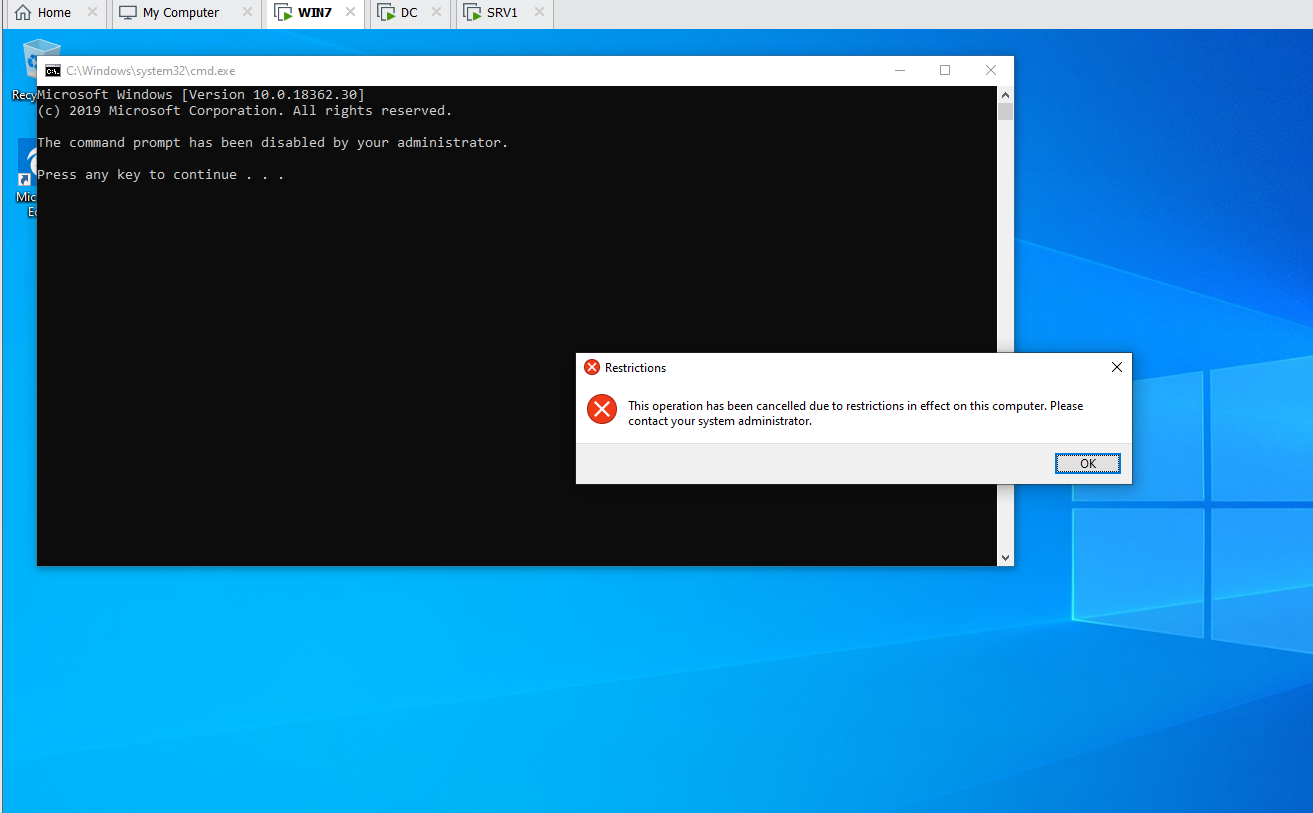
here I prevent to access the cmd

now I crated new GPO named disable USB access because I don’t want anyone to enter USB drive to the computers 

now to set all those policys we need to go to cmd and (gpupdate /force) to set the up .

now lets check the results , user 1 cant access the control pnael and cmd

and user 3 can access control panel and cmd

user 3 access  user 1 don’t have access to cmd and control panael that means my project is succesfuly done.

How my project was for me ?

It havent been hard but it took time because im busy all the time and the last weeks were very ruff for me , the project is good because its letting me to go back to all what we learned and setup all from the beginning , ill not lie there are few thing I still don’t get 100% like ssh

But with a little bit more learning every thing is possible , the classes where funny and it was more easy to learn that way and I hope my project its gonna be fine , I had a very good time with you uriel , u are very good teacher .thenks for all