
SeeSecurity
Microsoft Servers
SOC OPERATOR & INCIDENT RESPONDER
SOC
CYBER SECURITY PREPARATION PROGRAM
CSPP
Name: Alexnader Chait
T.Z: [redacted]
Educator: Binyamin Cohen
Date: 01.29.2024
קורס למתחילים בסייבר
CSPP
מבואות סייבר
ניהול רשתות ובקר SOC
Microsoft Project

תוכן עניינים

אפשר ללחוץ על המספרים בדי להגיע לעמודים הרצויים, אם אין מספר אז התתי סעיפים נבאותו עמוד

29- הגדרת DHCP server

- 30 ▪ תן ל-DC1 כתובת IP קבועה והתקן עליו שרת DHCP.
- 31 ▪ הגדר Scope שמחלק 50 כתובות.
- 32 ▪ הגדר Lease של 8 שעות.
- ▪ הגדר Address Exclusions של חמש כתובות ראשונות מתוך ה- Scope.
- 33 ▪ הגדר DHCP Options לחלוקת DNS (שהוא DC), Router (שהוא SRV1) ו suffix על שם הדומיין.
- 34 ▪ בדיקת קישוריות - בדוק ש- WIN10 מקבל IP בצורה אוטומטית מהשרת DHCP ובדוק שיש Ping בין כל המחשבים. בדוק שניתן לבצע Ping מ- SRV1 לאינטרנט.
- 35 ▪ צור Failover cluster עם שרת DC2 (ניתן לבטל את הפעולה לאחר סיום ההגדרה במידה ויש צורך)

40- הגדרת DNS server

- 40 ▪ וודא שכל המחשבים מוגדרים להשתמש ב- DNS של DC1.
  לא לשכוח להגדיר ידנית בכרטיס Bridged של SRV1 להשתמש ב- DNS של DC.
- 41 ▪ הגדר Forwarding לשרת DNS חיצוני (8.8.8.8).
- 43 ▪ הגדר Conditional Forwarders או Primary Zone ל- facebook.com במטרה למנוע מהעובדים לגלוש facebook במהלך יום העבודה.
- 46 ▪ הכנס ל- WIN10 והשתמש ב- nslookup כדי לוודא שהשרת מצליח לתרגם את הכתובות google.com
- 47 ▪ הגדר Conditional Forwarders ל- Google.com – יש להעזר בפקודה nslookup ולצרף צילום מסך של פלט הפקודה.
- 48 ▪ הגדר Stub Zone ל- yahoo.com
- 49 ▪ צור ZONE מסוג Primary – איזה שם שתרצה – צור לZONE הזה בשרת Secondary Zone DC2
- 51 ▪ צור CNAME לשרת DC2 או לרשומה אחרת לבחירתך, לשם שהוא שונה מהשם המקורי של השרת – בדוק שזה עובד (PING מהתחנה לשם החדש)
- 54 ▪ צור ובדוק Round Robin ל 2 רשומות שמפנות לכתובת רנדומלית (לא CNAME)

56- פרופיל משתמש

- 56 ▪ צור פרופיל משתמש נודד לחשבון שיצרנו בתרגילים הקודמים
- 60 ▪ בדוק שהפרופיל אכן נודד ממחשב למחשב
- 62 ▪ שנה את ההגדרות כך שמנהל הרשת יוכל להכנס לתיקיית הפרופיל בשרת (Domain Admin)
- 65 ▪ בדוק שוב שהפרופיל אכן תקין ונודד ממחשב למחשב
- 66 ▪ שנה את הגדרות הפרופיל כך שהוא יהיה מנדטורי – כלומר – לא ניתן יהיה לשנות שום דבר בפרופיל

68- שיתופים ומיפויים – שרת קבצים

- 68 ▪ הגדר **את שרת** DC2 **כשרת קבצים – (התקנת Role)** {במידה ושרת DC2 הותקן כ Server Core ניתן להגדיר ששרת הקבצים יהיה שרת DC1 }
- 70 ▪ **Home Folder** - הגדר לכ 5 חשבונות Home Folder. עליך לוודא כי כל משתמש נגיש ל-Home folder שלו בלבד.
- 75 ▪ שיתוף תיקייה - צור ב- DC2 תיקיה משותפת בשם DATA. {במידה ושרת DC2 הותקן כ Server Core ניתן להגדיר בשרת DC1 }
- ▪ צור בתוך התיקייה קובץ txt.
- 76 ▪ ניהול הרשאות - דאג לכך שאלו יהיו הרשאות הגישה לתיקייה המשותפת:
  הרשאת Modify לקבוצת Sys_Admins.
  הרשאת Read & execute לקבוצת Sales.
  זכור כי הרשאות שיתוף הינן הרשאות משולבות.
- 77 ▪ מיפוי כונן רשת - מפה את התיקייה לכל המשתמשים ובדוק שההרשאות שלהם נכונות. את הבדיקה בצע דרך WIN10.
- 81 ▪ צור תיקייה משותפת נוספת ב-DC2 בשם Script. {במידה ושרת DC2 הותקן כ Server Core ניתן להגדיר בשרת DC1 }
- 80 ▪ תן הרשאת Modify לקבוצת Everyone.
  צור בתוכה קובץ Batch שהמשתמש יפעיל ושיבצע את מיפוי תיקיית data ככונן הרשת עבור המשתמש (השתמש בפקודה net use).
- 82 ▪ צור מכסה Quota לנפח השימוש של כל משתמש בתיקיות ה Home Folder עד 5GB ומנע מהמשתמשים לשמור קבצי AVI בתיקיות אלו.

84- הקשחת התחנות

השתמש ב- Group Policy כדי להקשיח את התחנות עבודה על-ידי:

- 85 ▪ מניעת גישה של משתמשים שאינם עובדי Sys_Admins ל-Control Panel.
- 86 ▪ מניעת גישה של משתמשים שאינם עובדי Sys_Admins ל-CMD.
- ▪ מניעת שימוש של כלל המשתמשים ב-Disk-on-key.
- 88 ▪ צור Policy שמאפשר למחלקת Sys_Admins להיות בקבוצת Administrators המקומית של כל מחשבי הארגון (זהירות!)
- 90 ▪ הגדר ע"י GPO התקנה של תוכנה ע"ג מחשבי הארגון ללא מעורבות אדם.

91- מדיניות סמאות בארגון:

צור מדיניות סמא לפי התנאים הבאים:

- 91 ▪ אורך סמא 8 תווים
- ▪ מחייב שילוב של מספר סוגי תווים
- ▪ לא ניתן להשתמש ב 4 סמאות אחרונות
- ▪ תוקף סמא 75 ימים.

92- עבודת חקר / ניתוח:

- 92 ▪ כתוב מאמר / מחקר / סיכום – במילים שלך בנושא "*בחינת אבטחת מידע ומדיניות פרטיות*", בהתבסס על נושאים שנלמדו במהלך המקצה (למשל: מדיניות סמא, מדיניות חיבור מרחוק, ניהול זהויות, עבודה עם הרשאות לקבצים ותיקיות ברשת וכו')
  במסגרת המחקר עליך לחקור ולנתח את הנהלים הנוכחיים של מיקרוסופט בנושאי אבטחת מידע ומדיניות פרטיות. עליך להשוות אותם לנהלים של חברות אחרות ולבחון את השפעותיהם על המשתמשים והארגונים.
- ▪ יש להצמד לנושאים שנלמדו במהלך המקצה ולהרחיב אותם ככל האפשר.
- ▪ פרק זה צריך להיות לפחות 3 עמודים (750-1000 מילים לפחות)
- ▪ יש לציין מה המקורות בהם נעזרת ומהו התוכן אותו קיבלת מכל מקור. (AI כמו ChatGPT, אתרים באינטרנט, מיקרוסופט וכו')

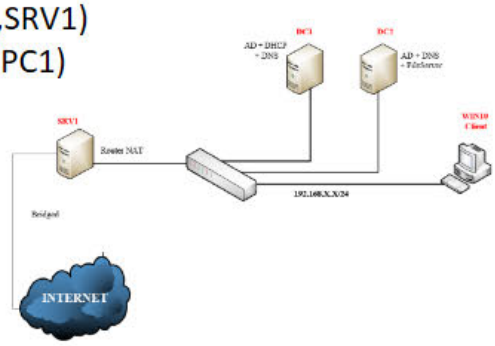
93- <u>אתגר</u>- *נקודות בונוס (לא נכלל במאמר של הקורס): צור מדיניות סמא מקיפה ו שונה לעובדי מחלקת* Sales *בלבד.*

Part 1 - Lab Setup

The Lab Setup step is crucial since were creating the foundation of our network, it's important to install everything correctly in order to avoid future issues

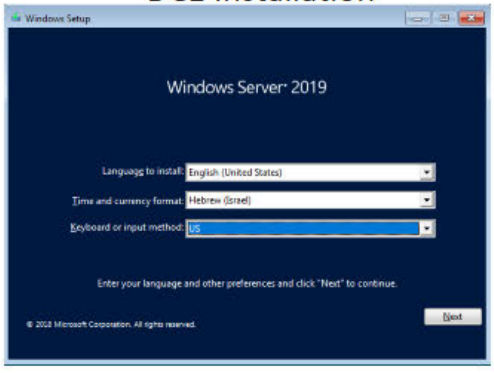
I'm going to create 4 new virtual machines according to this following topology

Three machines will use the windows server 2019 OS (DC1,DC2,SRV1)
One machine will act as the client and use the Windows 10 OS (PC1)
This will be the foundation of our network



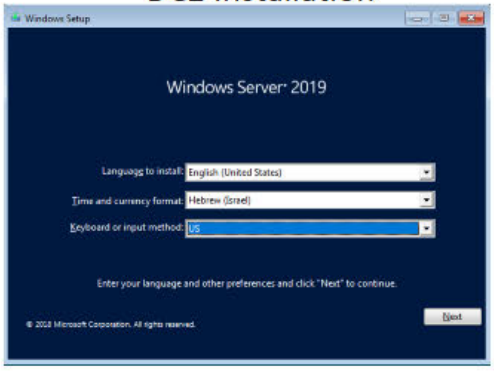
DC1 will be used for the AD+DHCP+DNS roles
DC2 will be used for the AD+DNS+Fileserver roles
SRV1 will be used as the Router/NAT/PAT
PC1 will be used as the client (Windows10)
We will also install VMware tools on all the machines for better functionality

DC1 Installation



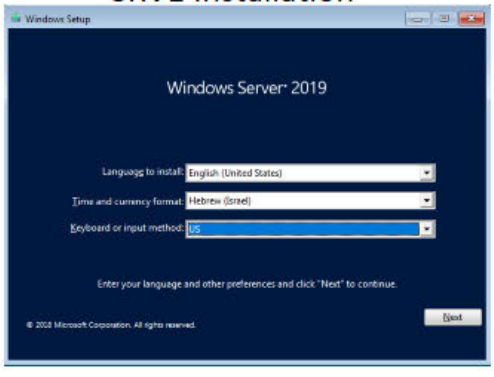
Computer name	alexDC1
Workgroup	WORKGROUP
Operating system version	Microsoft Windows Server 2019 Standard
Hardware information	VMware, Inc. VMware20,1

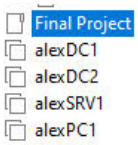
DC2 Installation



Computer name	alexDC2
Workgroup	WORKGROUP
Operating system version	Microsoft Windows Server 2019 Standard
Hardware information	VMware, Inc. VMware20,1

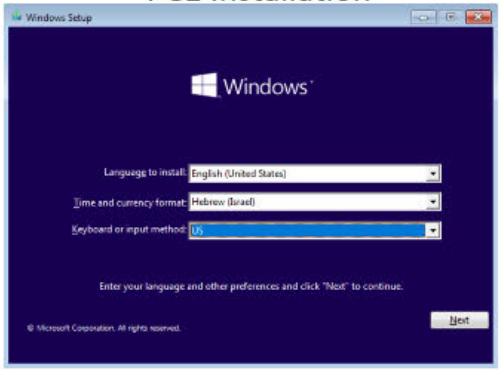
SRV1 Installation





Computer name	alexSRV1
Workgroup	WORKGROUP
Operating system version	Microsoft Windows Server 2019 Standard
Hardware information	VMware, Inc. VMware20,1

PC1 Installation



Device name	alexPC1
Edition	Windows 10 Pro

All systems are now installed

This first step is important because it allows me to have an active network that can communicate while I work at expanding and configuring the network

Starting up, I will configure the starting IP addresses according to this plan (DG is subject to change according to the progress of the project) I'll start with a DG of 192.168.0.2 (VMware default option)

פרופיל חברה:

מס' עובדים /משתמשי מחשב: 1

מס' המחשבים הניידים: 0 , מס' המחשבים הניידים: 0 מחלקות ארגוניות: 3

מדיניות אבטחה מיוחדת – אם יש:
תחנות מוקשחות ומדיניות סמה ע"י GPO

IP Range: 192.168.0.0 - 255 /24 Admin user name: bozo

Admin Password: **********

FQ Domain Name: alex.net

1st DC:

Name: alexDC1 OS Version: windows server 2019

IP: 192.168.0.200 /24 DG: 192.168.0.254

DNS 1: 192.168.0.200 DNS 2: 192.168.0.201

Roles: DNS, DHCP, AD,

2nd DC:

Name: alexDC2 OS Version: windows server 2019

IP: 192.168.0.201 /24 DG: 192.168.0.254

DNS 1: 192.168.0.200 DNS 2: 192.168.0.201

Roles: DNS, AD, Fileserver,

NAT-SRV

Name: alexSRV1 OS Version: windows server 2019

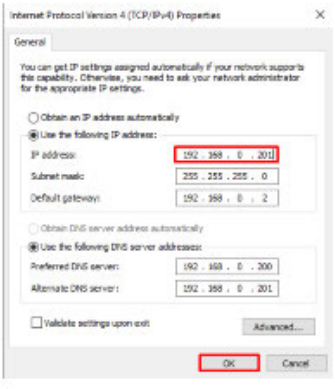
IP: 192.168.0.202 /24 DG: 192.168.0.254

DNS 1: 192.168.0.200 DNS 2: 192.168.0.201

Roles: Router, Nat, Pat,

DC1 IPv4

DC2 IPv4



SRV1 IPv4

PC1 IPv4

The reason this works, is because I'm using the VMware built-in Virtual Network Editor, which allows me to use a virtual network That I have created, is this case the Subnet Address is 192.168.0.0

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.159.0
VMnet8	NAT	NAT	Connected	-	192.168.0.0

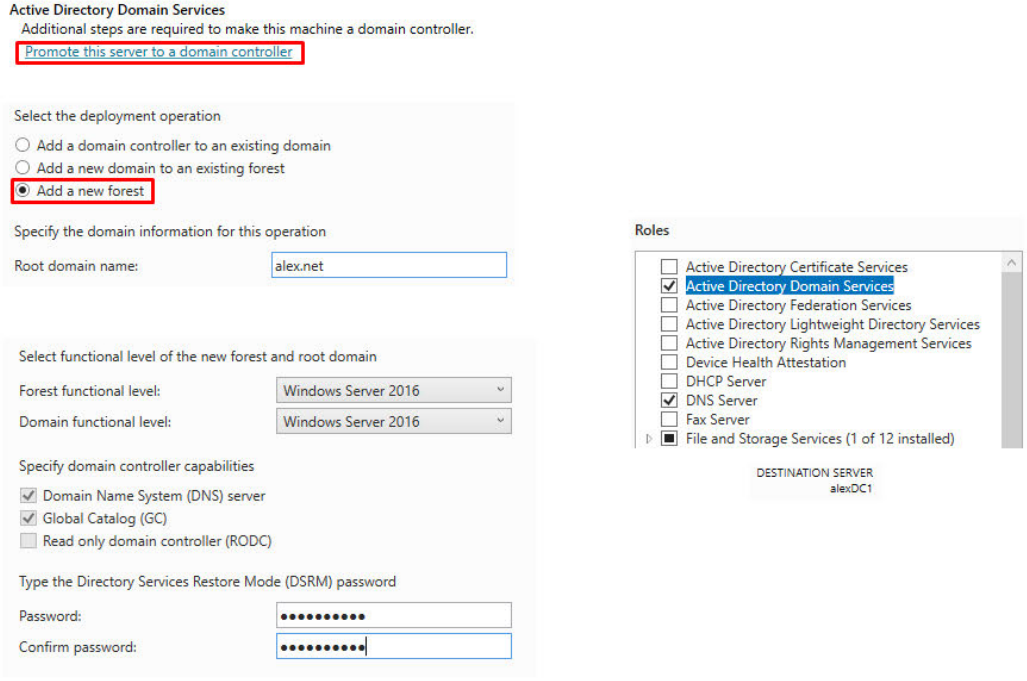
Part 2 - Domain Controller Configuration

Establishing a domain controller in the initial phases of setting up a new network using VMware is essential.

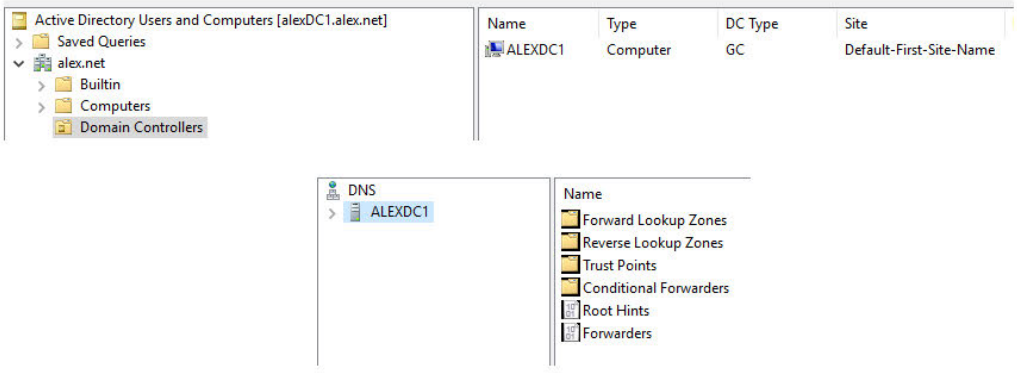
This server plays a pivotal role in creating a centralized system for user authentication, managing security policies, and overseeing network resources. It forms the backbone of a Windows Active Directory environment, ensuring efficient administration, streamlined user access, and robust network security.

Three machines will use the windows server 2019 OS (DC1,DC2,SRV1) One machine will act as the client and use the Windows 10 OS (PC1)

This will be the foundation of our network, Here I'm adding new forest and creating a new domain named alex.net

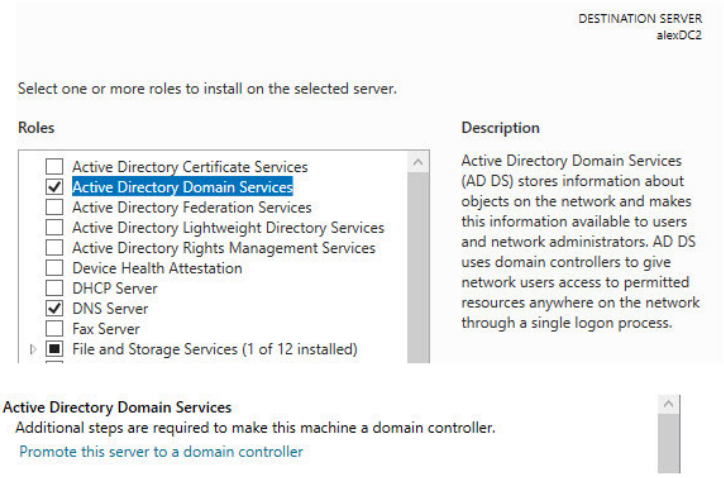


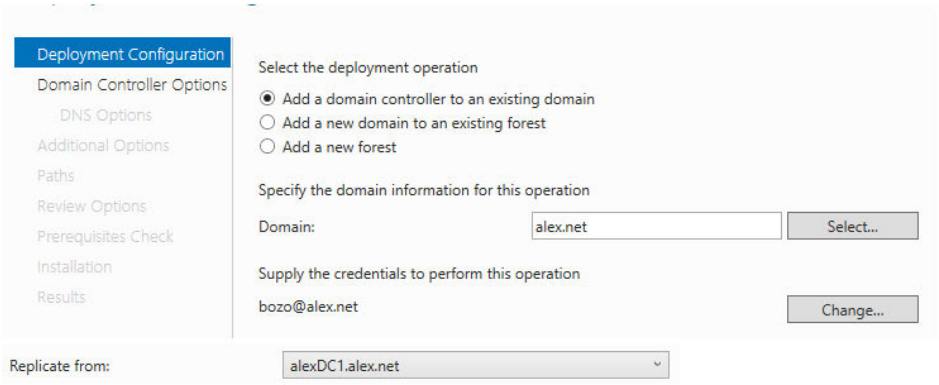
Here we can see that DC1 is now a domain controller & a DNS server



We'll do a similar process on DC2 to add it to the domain as domain controller

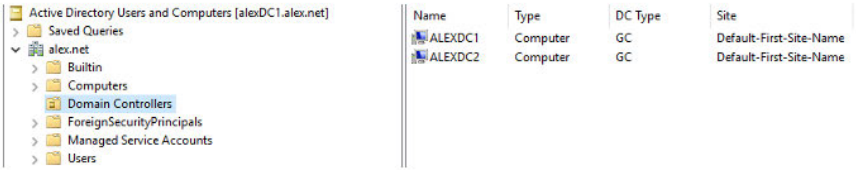
We'll do a similar process on DC2 to add it to the domain as domain controller



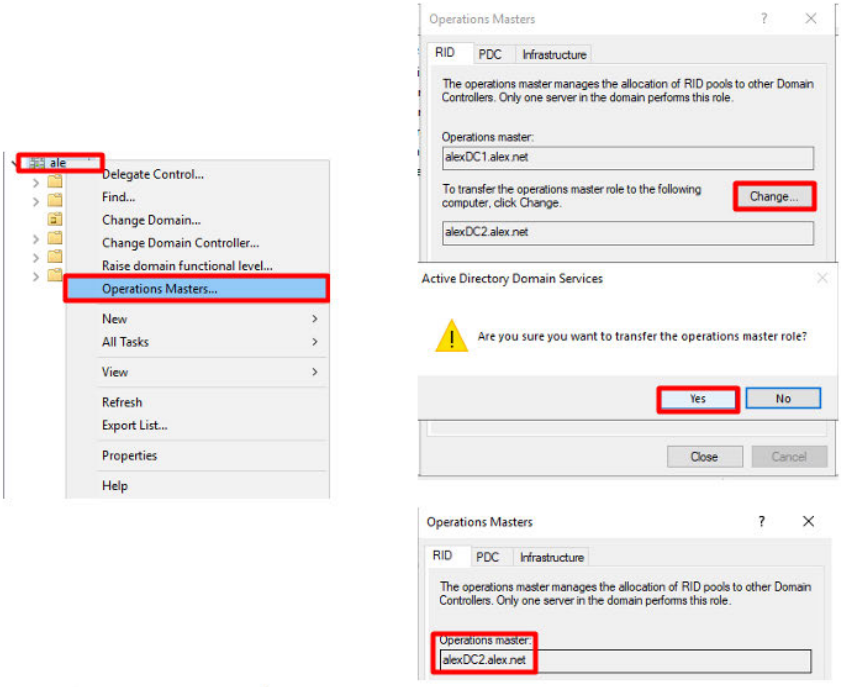


Here we can see that now DC2 is part of the alex.net domain

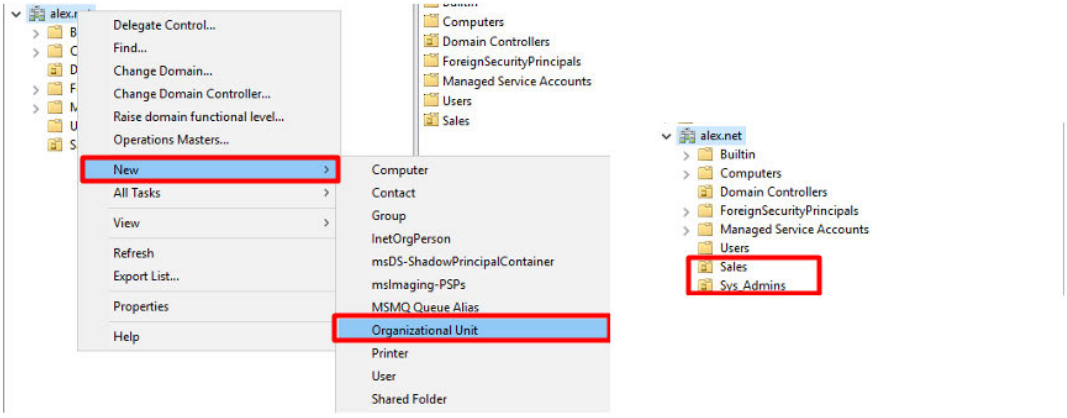
Here we can see that the new DC2 server is also a part of the alex.net domain as a domain controller



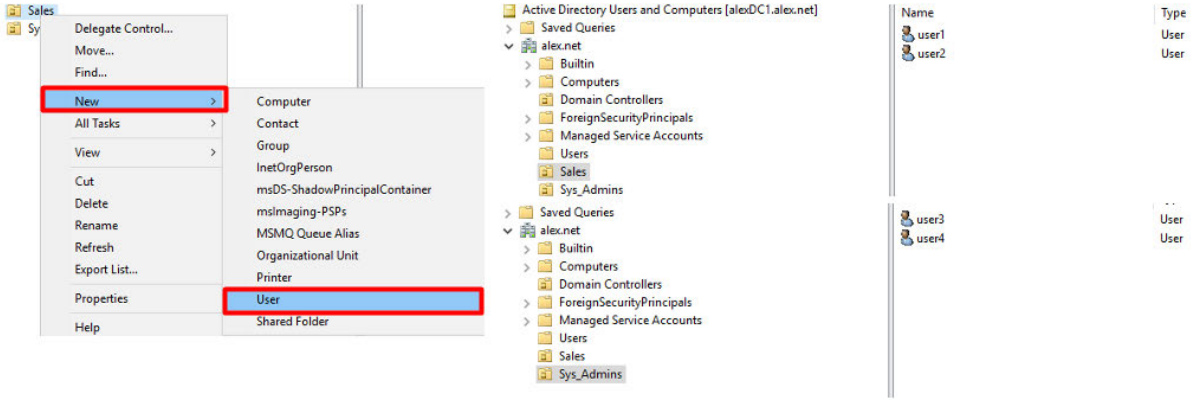
The rid master role is being transfer from DC1 to DC2, The RID Master role in Active Directory manages the creation of unique identifiers (SIDs) for objects, ensuring each has a distinct identifier within the domain.



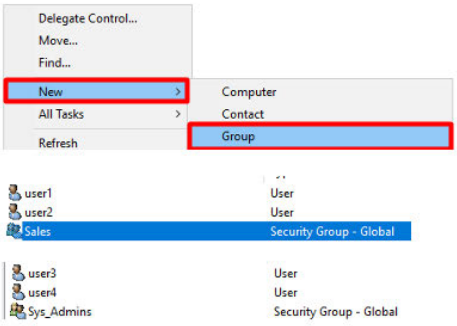
Here I'm creating two new OU's
OUs (Organizational Units) in Active Directory are containers used to organize and manage objects, such as users, groups, and computers, within a domain.

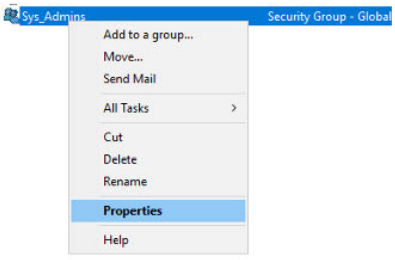


Here I'm creating two users for the Sales OU, and two users for the Sys_Admins OU

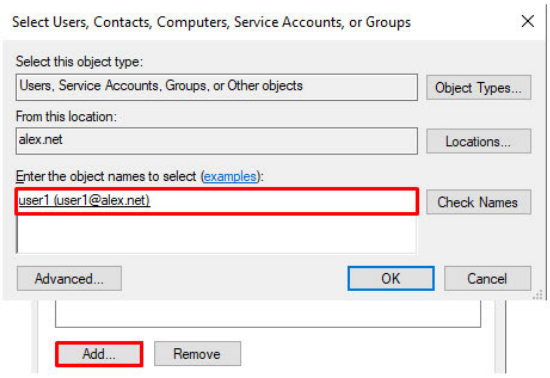


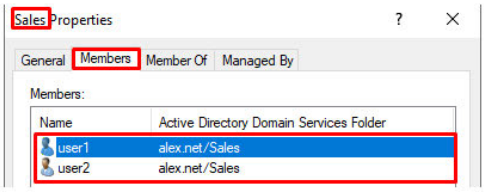
I'm creating two groups, one group is called Sales which will include user1+user2 One group is called Sys_Admins will will include user3+user4

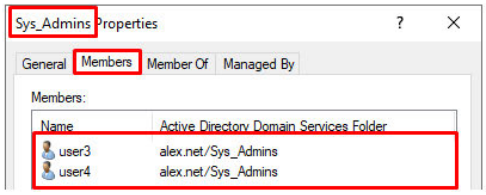




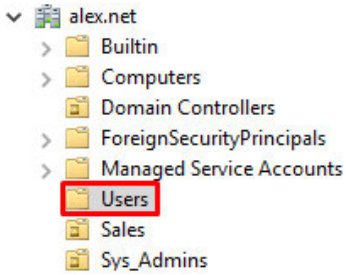
Here we can see that we have two groups with two users,
User1+User2 are members of the Sales group
User3+User4 are members of Sys_Admins group

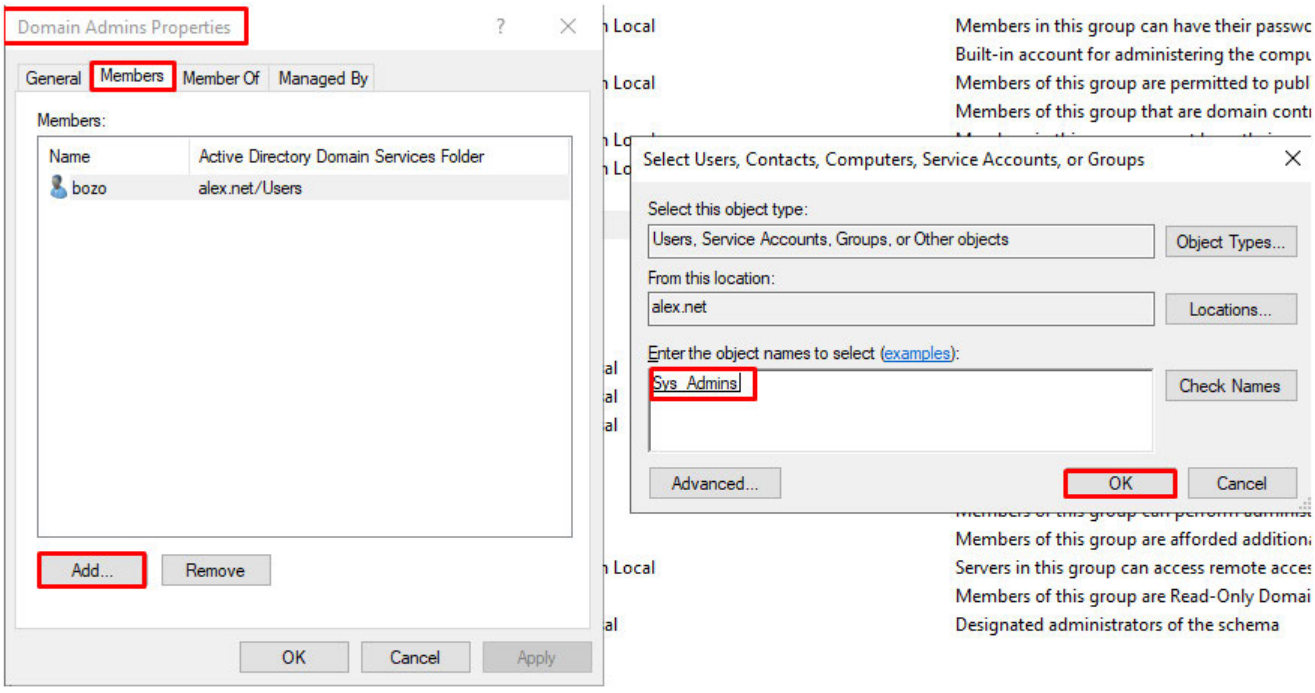




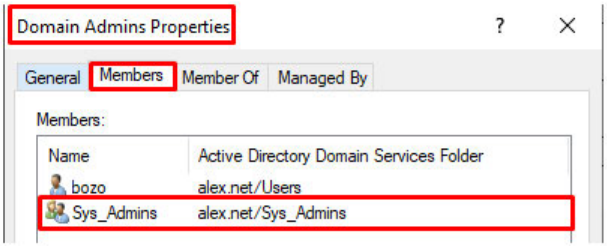


I'll be adding the group Sys_Admins which has users3+user4 to the domain admins Group





Here we can see that the Sys_Admins are also members of the Domain Admins group



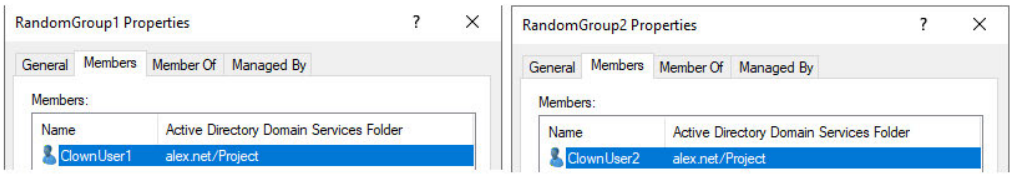
I'm going to create two users + two groups by using DSADD commands, this script will create both including a new OU named Project

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> # Adjusted script with unique names
>>
>> # Define names
>> $OUName = "Project"
>> $Group1Name = "RandomGroup1"
>> $Group2Name = "RandomGroup2"
>> $User1Name = "ClownUser1"
>> $User2Name = "ClownUser2"
>>
>> # Create the OU
>> dsadd ou "OU=$OUName,DC=alex,DC=net"
>>
>> # Create the groups
>> dsadd group "CN=$Group1Name,OU=$OUName,DC=alex,DC=net" -samid $Group1Name
>> dsadd group "CN=$Group2Name,OU=$OUName,DC=alex,DC=net" -samid $Group2Name
>>
>> # Create the users
>> dsadd user "CN=$User1Name,OU=$OUName,DC=alex,DC=net" -samid $User1Name -upn "$User1Name@alex.net" -fn Clown -ln One -
pwd P@ssw0rd!123
>> dsadd user "CN=$User2Name,OU=$OUName,DC=alex,DC=net" -samid $User2Name -upn "$User2Name@alex.net" -fn Clown -ln Two -
pwd P@ssw0rd!123
dsadd succeeded:OU=Project,DC=alex,DC=net
dsadd succeeded:CN=RandomGroup1,OU=Project,DC=alex,DC=net
dsadd succeeded:CN=RandomGroup2,OU=Project,DC=alex,DC=net
dsadd succeeded:CN=ClownUser1,OU=Project,DC=alex,DC=net
dsadd succeeded:CN=ClownUser2,OU=Project,DC=alex,DC=net
PS C:\Users\Administrator>
```

Here I'll put in the two users and two groups I just created into different groups using commands only

```
PS C:\Users\Administrator> # Add users to groups
>> Add-ADGroupMember -Identity "RandomGroup1" -Members "ClownUser1"
>> Add-ADGroupMember -Identity "RandomGroup2" -Members "ClownUser2"
PS C:\Users\Administrator>
```

We can see that ClownUser1 is a member of RandomGroup1, ClownUser2 is a member of RandomGroup2



Here I'm using a script that creates 10 users and puts them in the OU named Project

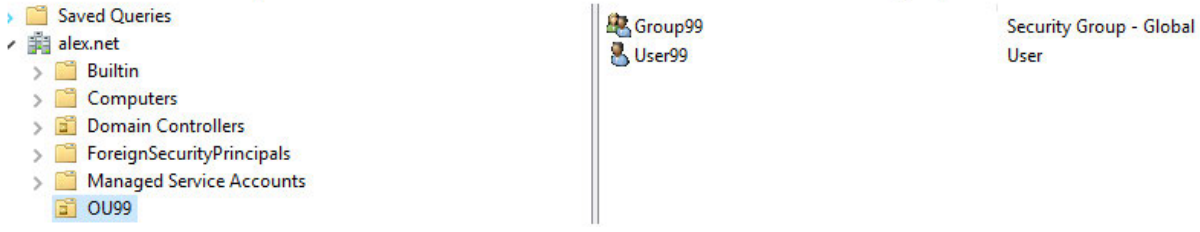
```
>> for ($i = 1; $i -le 10; $i++) {
>>     dsadd user "CN=Clown$i,OU=Project,DC=alex,DC=net" -samid clown$i -upn clown$i@alex.net -fn Clown -ln $i -pwd P
@ssw0rd!123
>> }
dsadd succeeded:CN=Clown1,OU=Project,DC=alex,DC=net
dsadd succeeded:CN=Clown2,OU=Project,DC=alex,DC=net
dsadd succeeded:CN=Clown3,OU=Project,DC=alex,DC=net
dsadd succeeded:CN=Clown4,OU=Project,DC=alex,DC=net
dsadd succeeded:CN=Clown5,OU=Project,DC=alex,DC=net
dsadd succeeded:CN=Clown6,OU=Project,DC=alex,DC=net
dsadd succeeded:CN=Clown7,OU=Project,DC=alex,DC=net
dsadd succeeded:CN=Clown8,OU=Project,DC=alex,DC=net
dsadd succeeded:CN=Clown9,OU=Project,DC=alex,DC=net
dsadd succeeded:CN=Clown10,OU=Project,DC=alex,DC=net
PS C:\Users\Administrator>
```

We can see that the script is working and 10 new users have been added to the project group

Here I'm using a powershell based script that Creates a new OU,Group,User

```
PS C:\Users\Administrator> # Create OU
>> New-ADOrganizationalUnit -Name "OU99" -Path "DC=alex,DC=net"
>>
>> # Create Group
>> New-ADGroup -Name "Group99" -GroupScope Global -Path "OU=OU99,DC=alex,DC=net"
>>
>> # Create User
>> New-ADUser -Name "User99" -SamAccountName "User99" -UserPrincipalName "User99@alex.net" -GivenName "User" -Surname
 "99" -Path "OU=OU99,DC=alex,DC=net" -AccountPassword (ConvertTo-SecureString "P@ssw0rd!123" -AsPlainText -Force) -En
abled $true
PS C:\Users\Administrator>
```

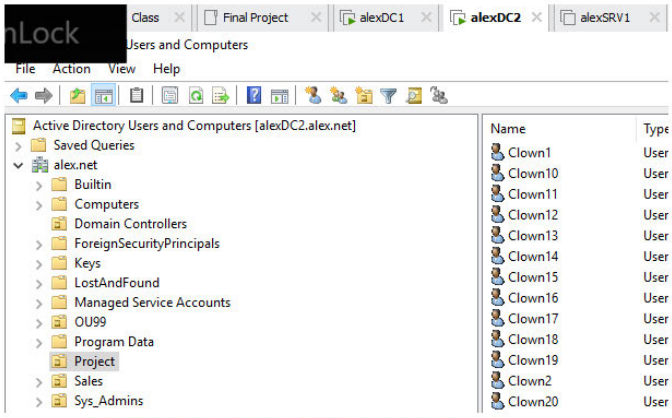
We can see the script was successful and a new OU named OU99 was formed with a new group and user



I'm using a powershell based script that creates 10 users with the given name Clown, the script will put the new users in Project

```
PS C:\Users\Administrator> # Loop to create 10 users
>> for ($i = 11; $i -le 20; $i++) {
>>     $username = "Clown$i"
>>     $userUPN = "$username@alex.net"
>>
>>     New-ADUser -Name $username -SamAccountName $username -UserPrincipalName $userUPN -GivenName "Clown" -Surname $
i -Path "OU=Project,DC=alex,DC=net" -AccountPassword (ConvertTo-SecureString "P@ssw0rd!123" -AsPlainText -Force) -Ena
bled $true
>> }
PS C:\Users\Administrator>
```

I'll Check if all the changes in the AD are synchronized with both DC servers




```
PS C:\Users\Administrator> repadmin /replsummary
Replication Summary Start Time: 2024-01-26 10:09:41

Beginning data collection for replication summary, this may take awhile:
  .....

Source DSA          largest delta    fails/total %%   error
 ALEXDC1                    10m:46s    0 /   5    0
 ALEXDC2                    11m:01s    0 /   5    0

Destination DSA     largest delta    fails/total %%   error
 ALEXDC1                    11m:01s    0 /   5    0
 ALEXDC2                    10m:45s    0 /   5    0
```

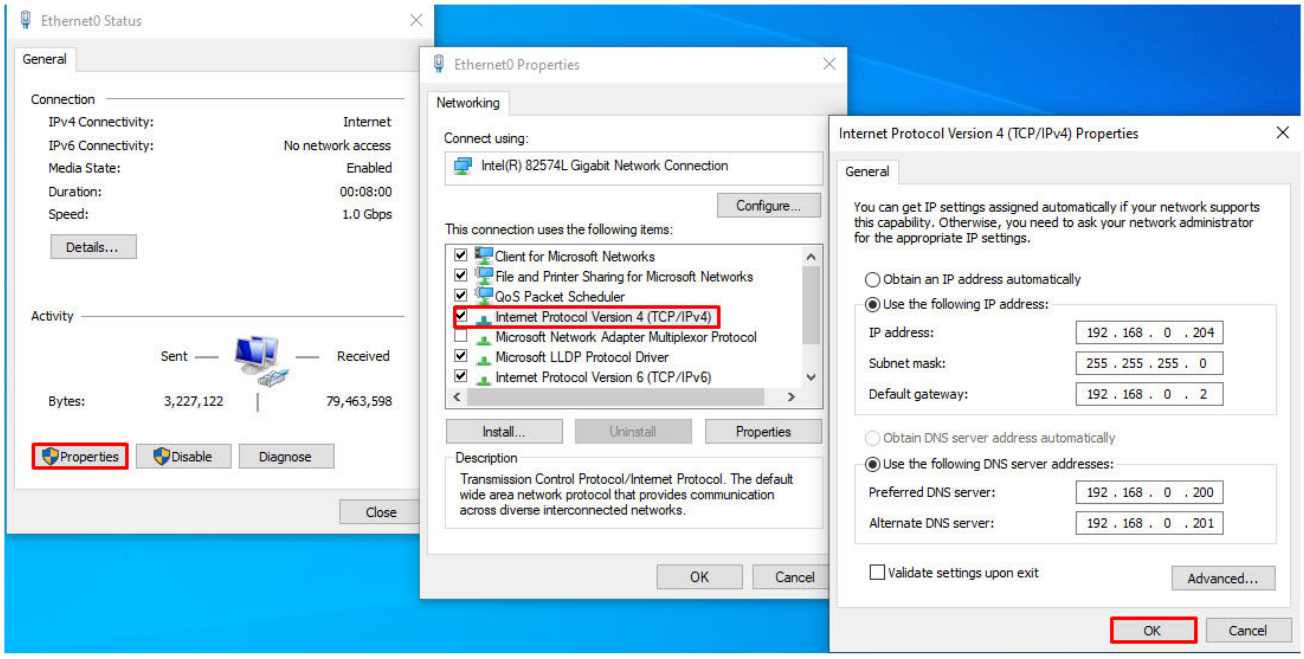
Here we can see that DC2 also has all the new Data, and we also check with a replication summary, it shows that everything is functioning.

Part 3 - Adding SRV1+Windows 10 to Domain

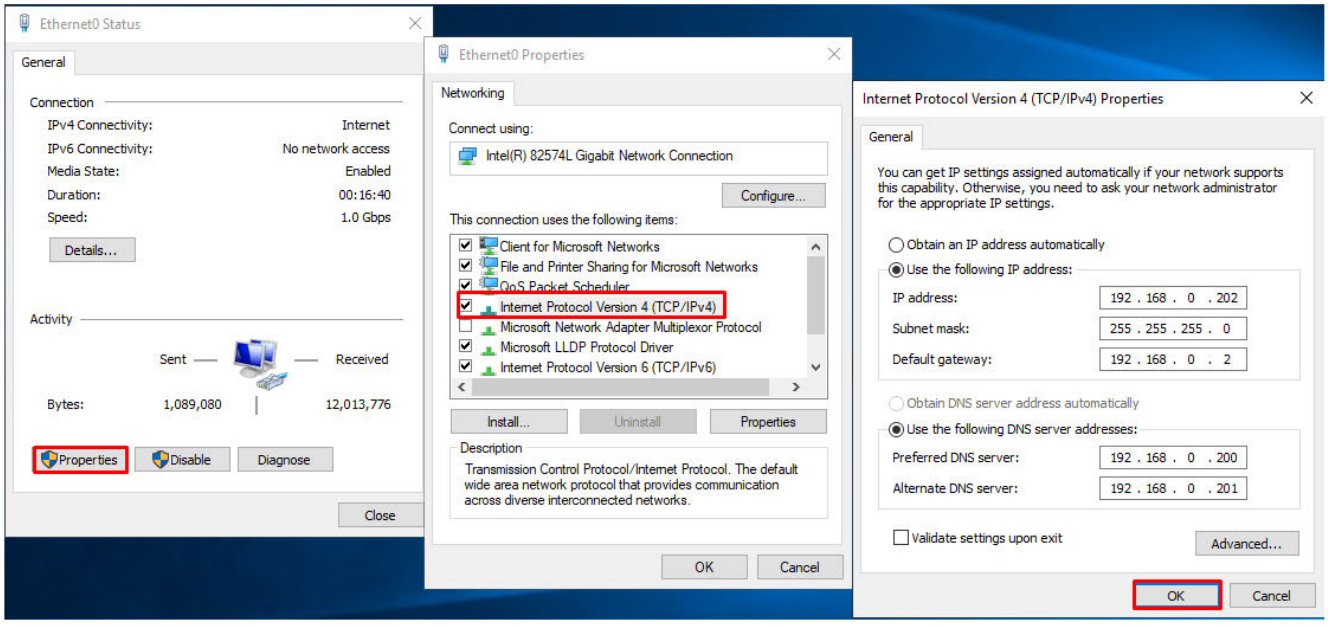
Adding clients and servers to a local network ensures users can access and share resources, fostering collaboration, centralization, and improved efficiency.

First we need to make sure that the alexPC1 and alexSRV1 are able to communicate with DC1 & DC2 in order to add them to the domain

Here I'm configuring SRV1 so it will communicate with DC1/DC2



Here I'm configuring PC1 so it will communicate with DC1/DC2

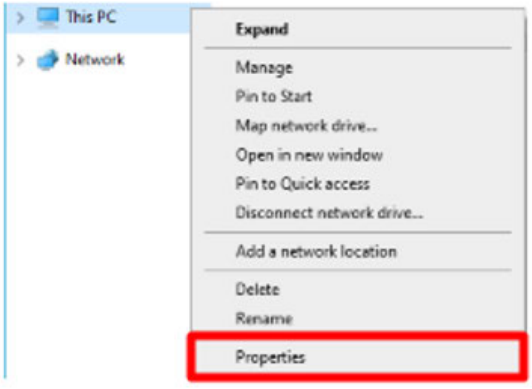


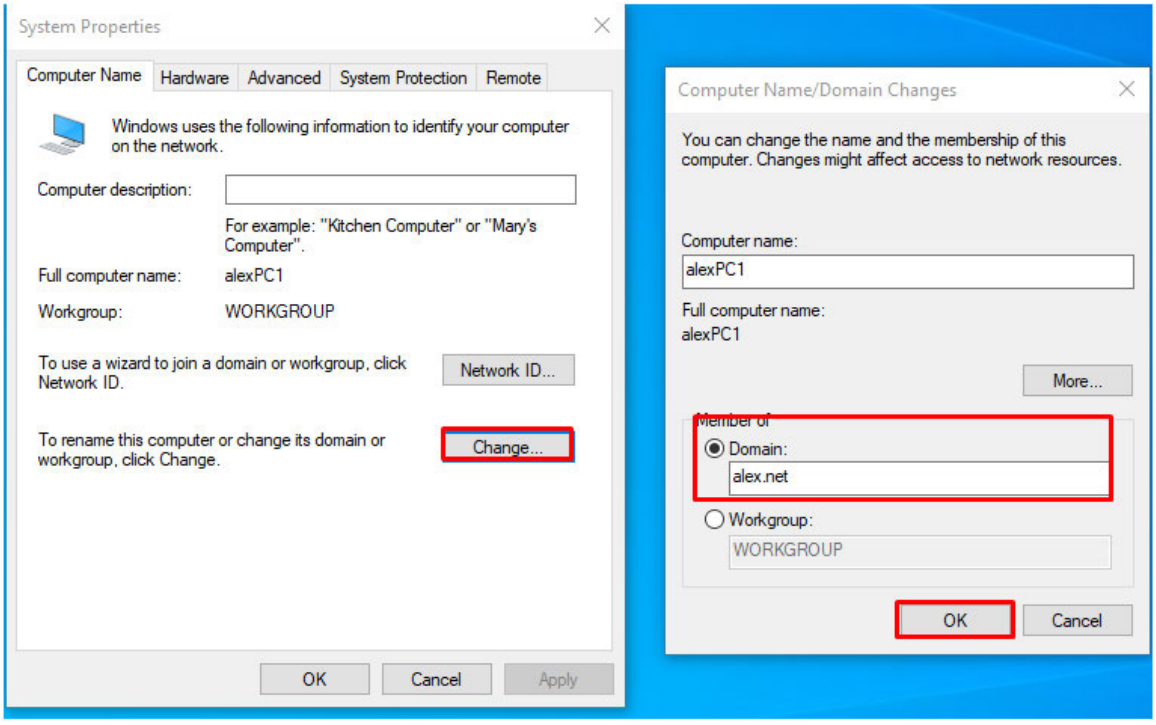
```
C:\Users\alexPC1>ping 192.168.0.200

Pinging 192.168.0.200 with 32 bytes of data:
Reply from 192.168.0.200: bytes=32 time<1ms TTL=128
Reply from 192.168.0.200: bytes=32 time<1ms TTL=128
Reply from 192.168.0.200: bytes=32 time<1ms TTL=128
Reply from 192.168.0.200: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\alexPC1>ping 192.168.0.201

Pinging 192.168.0.201 with 32 bytes of data:
Reply from 192.168.0.201: bytes=32 time<1ms TTL=128
Reply from 192.168.0.201: bytes=32 time<1ms TTL=128
Reply from 192.168.0.201: bytes=32 time<1ms TTL=128
Reply from 192.168.0.201: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\Administrator>ping 192.168.0.200

Pinging 192.168.0.200 with 32 bytes of data:
Reply from 192.168.0.200: bytes=32 time<1ms TTL=128
Reply from 192.168.0.200: bytes=32 time<1ms TTL=128
Reply from 192.168.0.200: bytes=32 time<1ms TTL=128
Reply from 192.168.0.200: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 192.168.0.201

Pinging 192.168.0.201 with 32 bytes of data:
Reply from 192.168.0.201: bytes=32 time<1ms TTL=128
Reply from 192.168.0.201: bytes=32 time<1ms TTL=128
Reply from 192.168.0.201: bytes=32 time<1ms TTL=128
Reply from 192.168.0.201: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

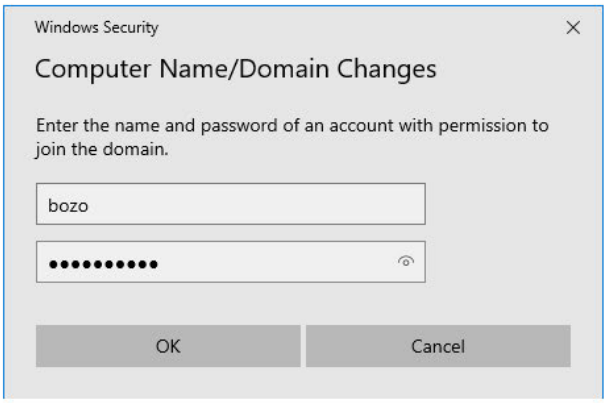
Now that we established that SRV1 & PC1 are able to communicate it's time to add them to the domain

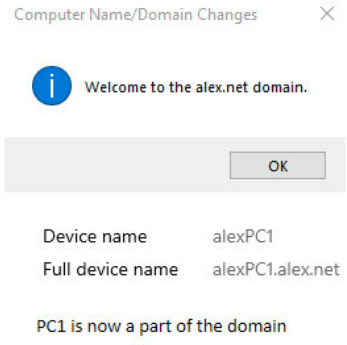
I'll start with adding PC1 to the domain by going to System Properties and changing from Workgroup to alex.net which is the domain name





Here we'll input the domain admin credentials in order to add PC1 to the domain



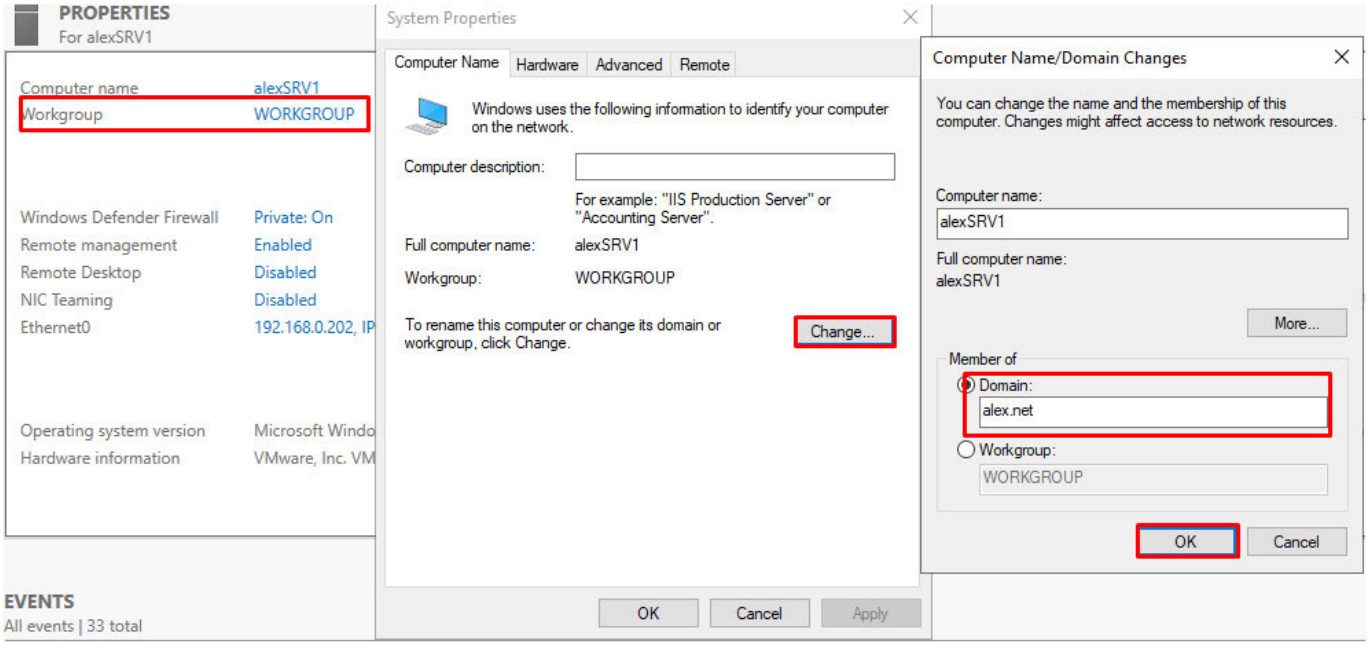


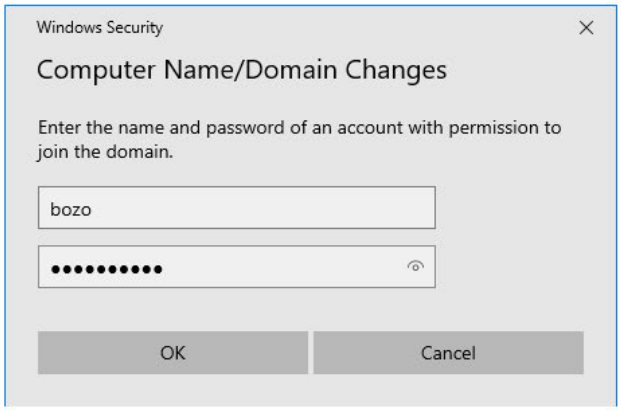
PC1 is now a part of the domain

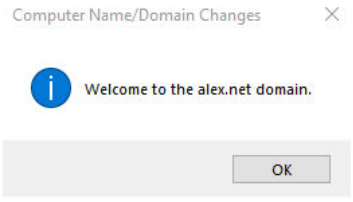
Now let's make sure that we can see the new alexPC1 from the domain controller & active directory

WE CAN! :)

Now lets repeat the same process with alexSRV1 and add it to the alex.net domain

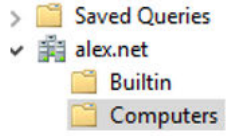






SRV1 is now a part of the domain

Now let's make sure that we can see the new alexSRV1 from the domain controller & active directory

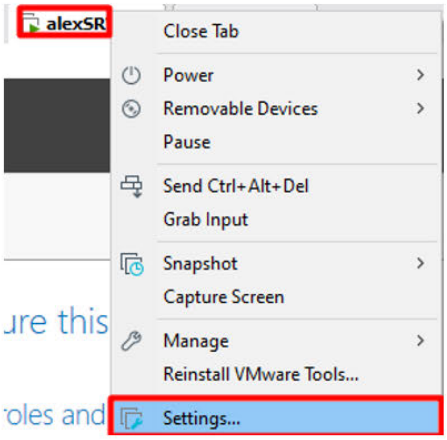


We seem both PC1 and SRV in active directory of alex.net Domain

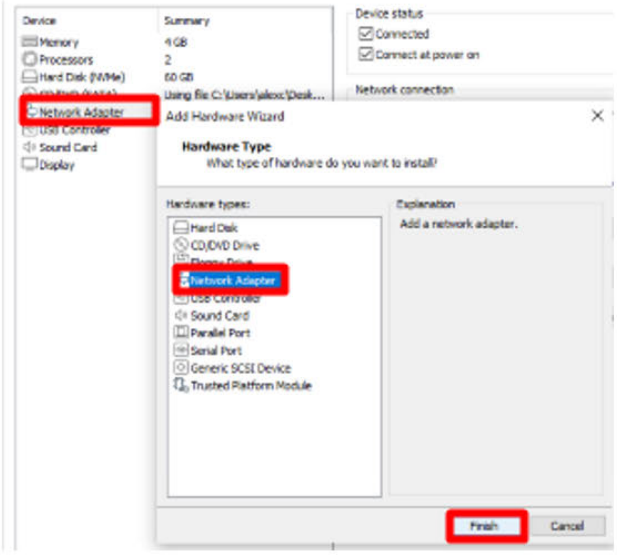
Part 4 - SRV1 Routing & NAT/Pat Configuration

The role of a NAT (Network Address Translation) router with PAT (Port Address Translation) is to enable multiple devices on a local network to share a single public IP address for internet communication. PAT assigns unique port numbers to each connection, allowing multiple devices to use the same public IP simultaneously. This enhances security, conserves public IP addresses, and facilitates internet access for local devices.

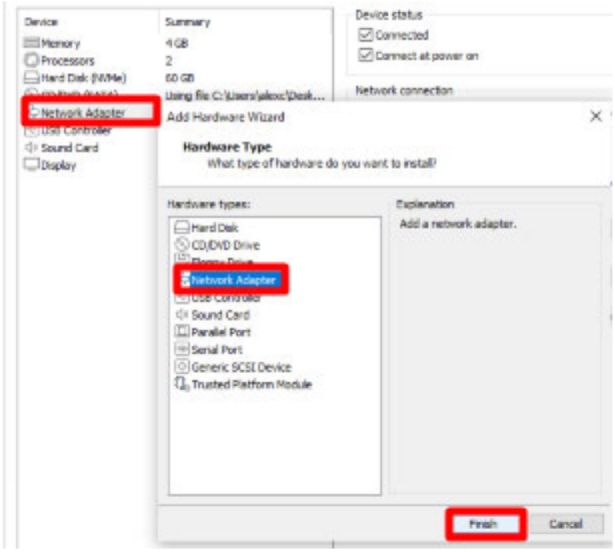
First I'll begin with making sure I have two network types which are NAT & Bridged
LAN Will be used for our local network (LAN), and the bridged will be used for the external Network. (WAN)



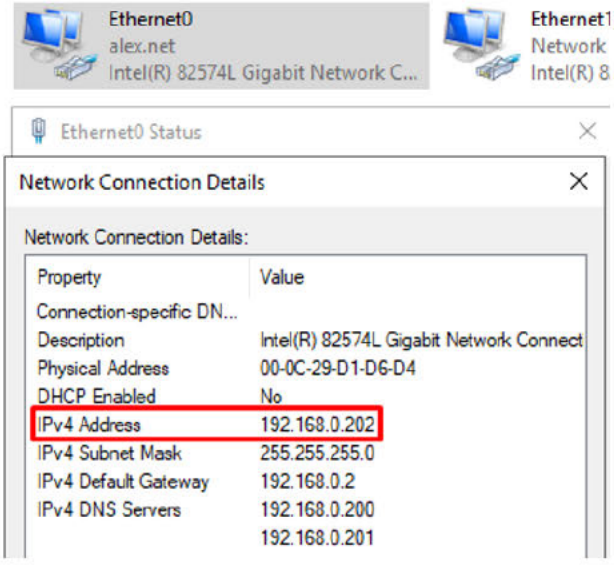
Since there's no Bridge option I'll need to add it

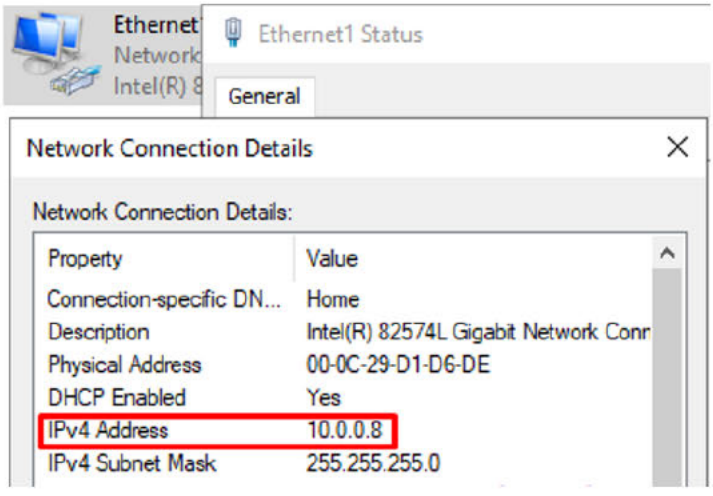


Now I have two Network Adapters, NAT & Bridged



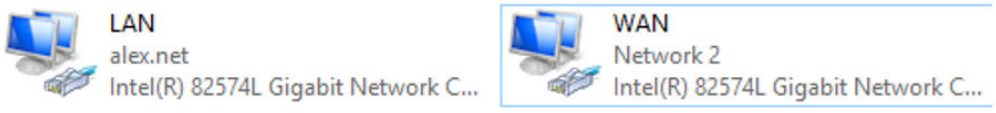
In the next step, well identify and rename both our networks on SRV1 according to their type (LAN/WAN)



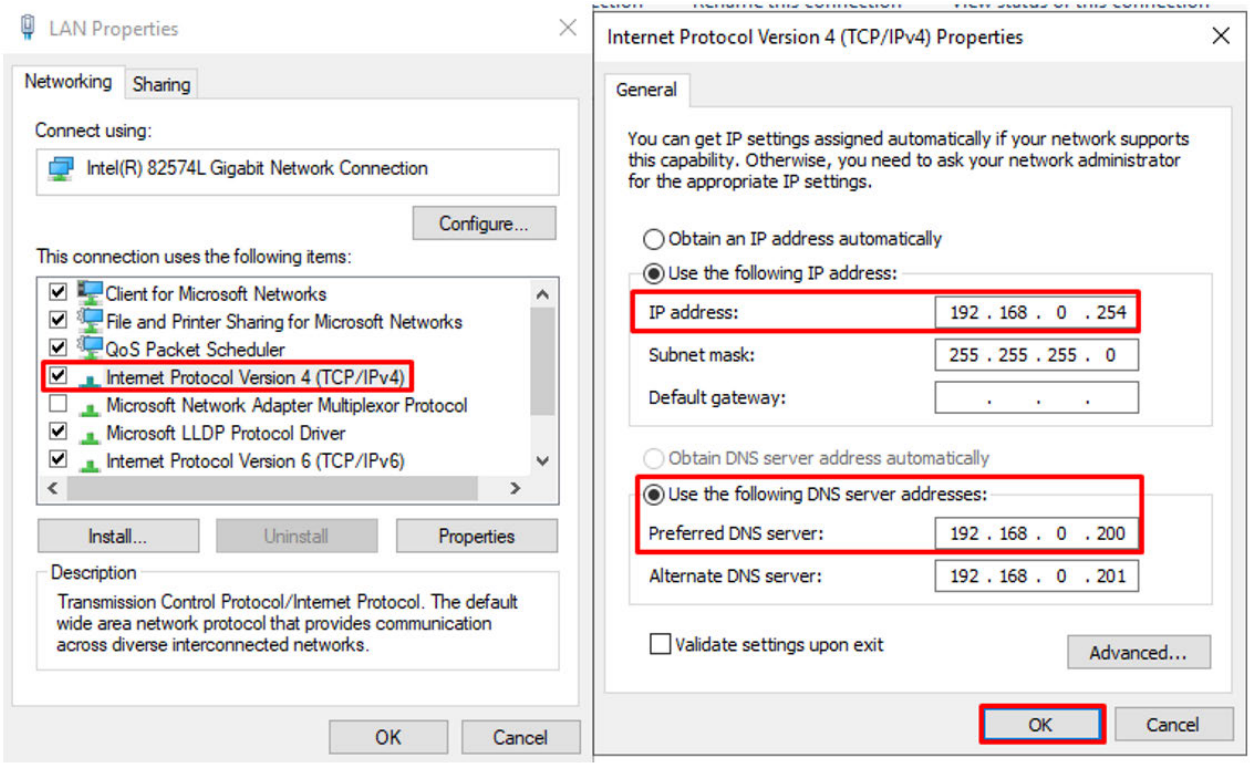


Here we can see that Ethernet0 is the LAN/NAT and that Ethernet 1 is the Bridged/WAN since Ethernet 0 is using the local network IP address, and the Ethernet 1 isn't

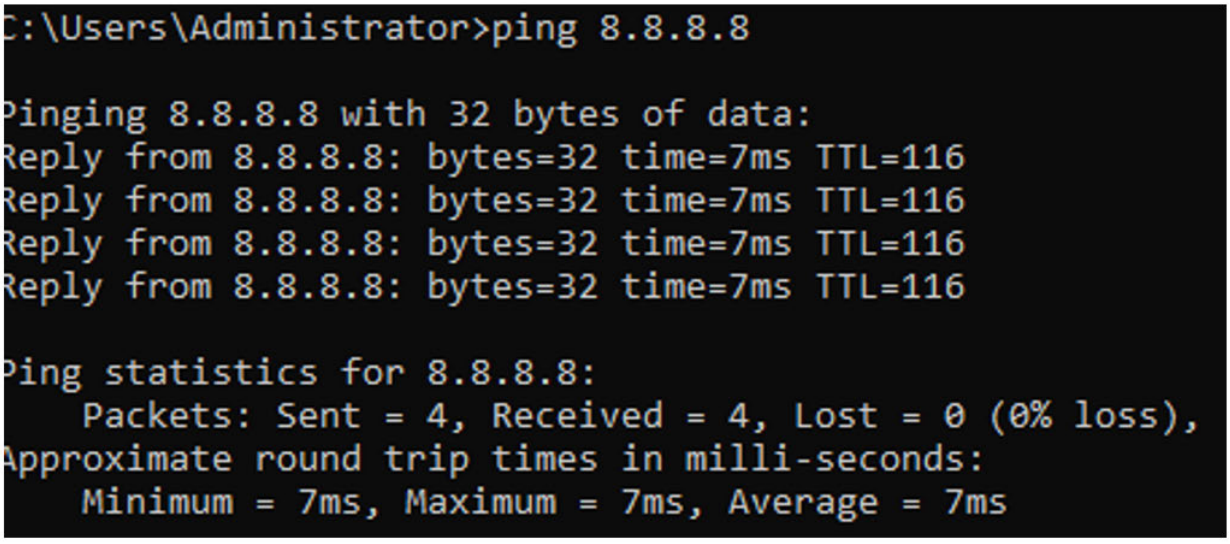
Now I'll rename accordingly, Ethernet0 will be named LAN, and Ethernet1 will be named WAN



The next step is configuring the LAN adapter and giving it an address of 192.168.0.254 which will act the default gateway for the rest of the local network

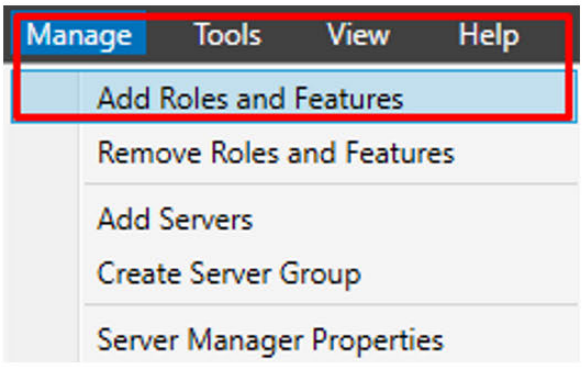


Let's ping google to see if we have Internet on SRV1 after the changes

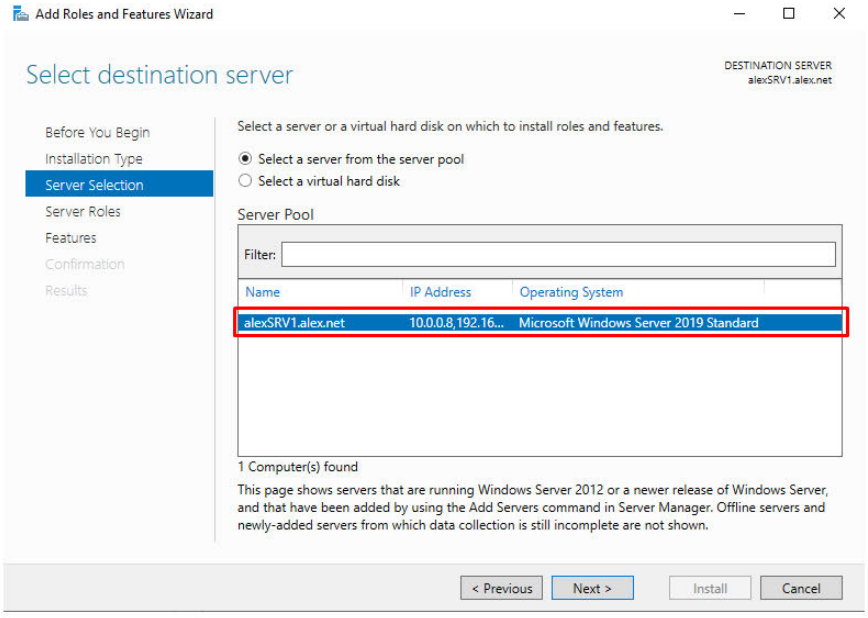


Ping is successful, SRV1 has internet connectivity

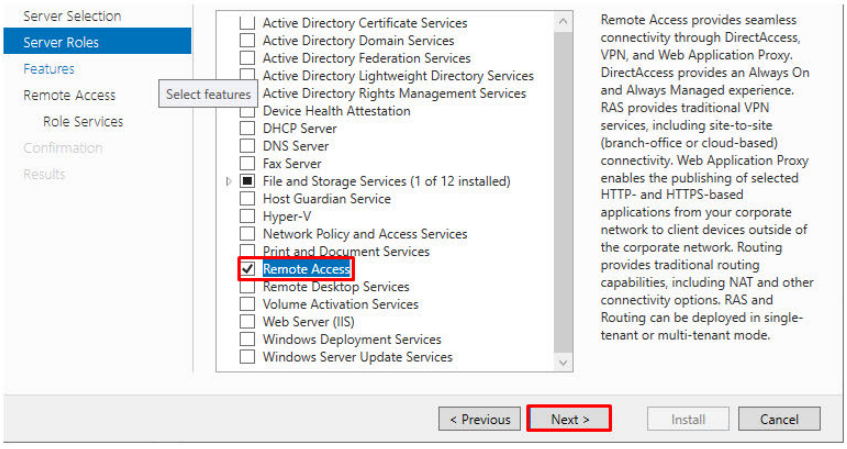
LAN & WAN are now configured, since WAN is an ISP or "outside" adapter we don't configure it.
The next step is adding the remote access role (RRAS), which will allow SRV1 to be used as a router/NAT/PAT



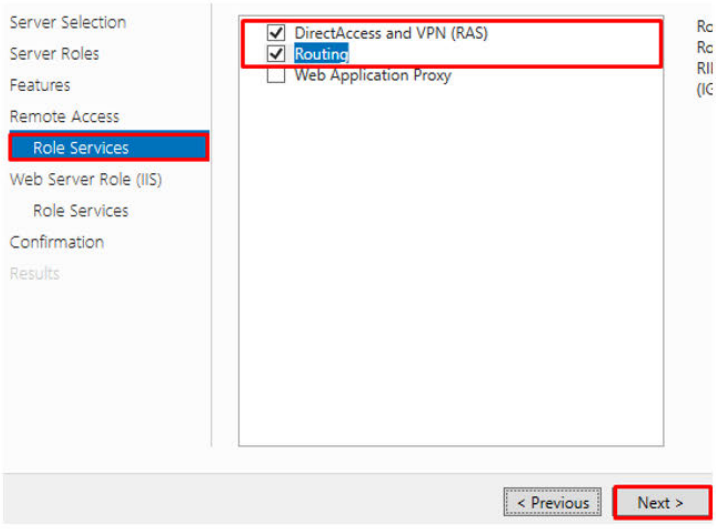
Select SRV1



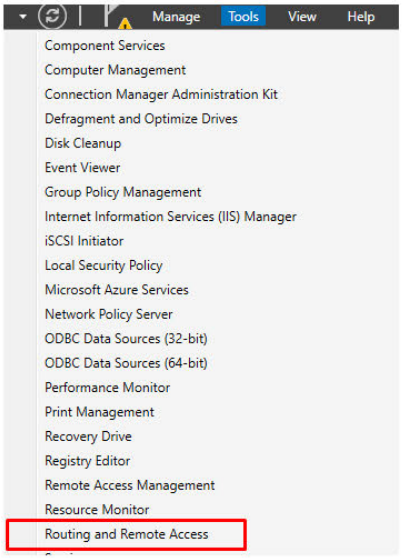
Here we select the Remote Access role



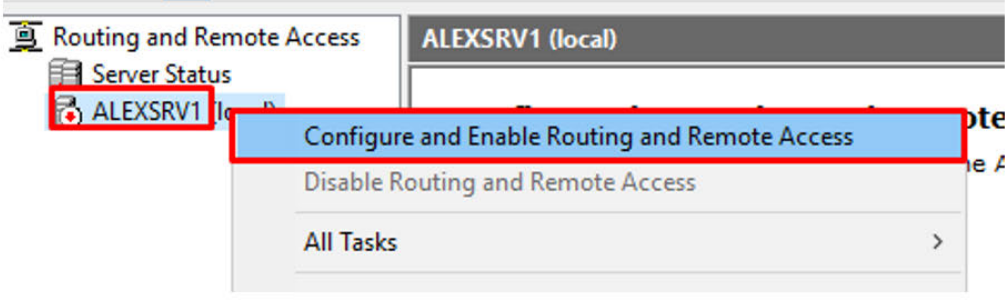
Selecting the Routing/Direct Access & VPN role services



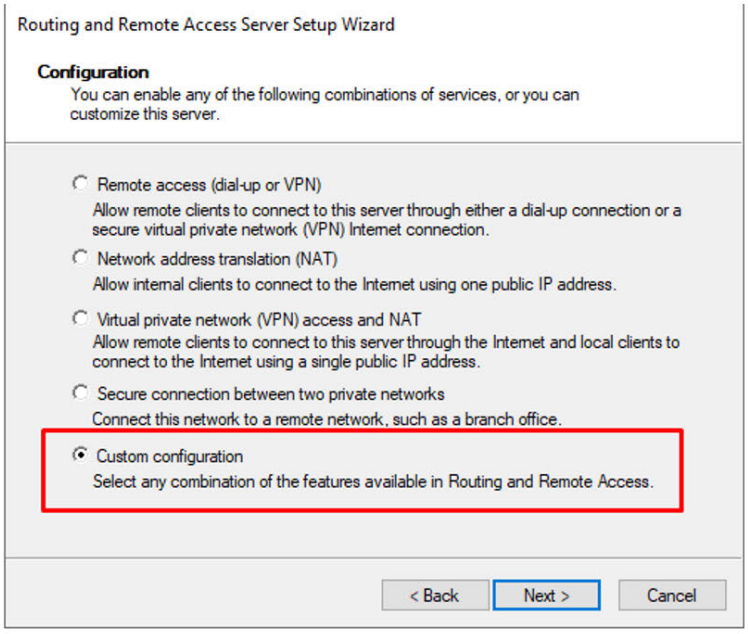
Now that the installation is complete will go to the routing & remote access



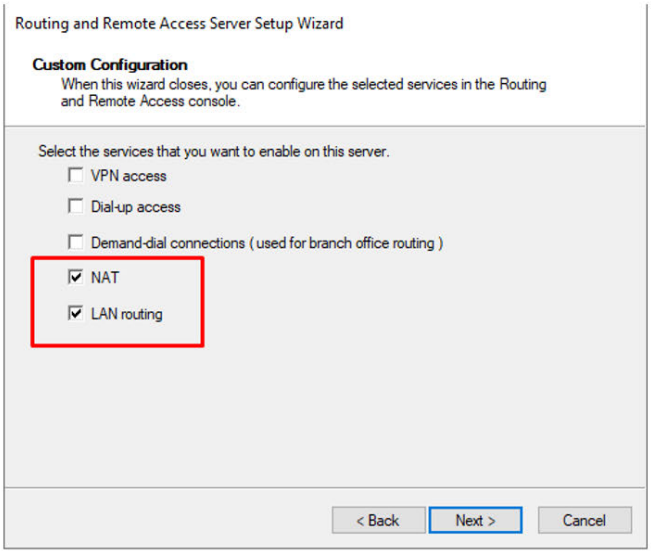
Next step is configuring SRV1



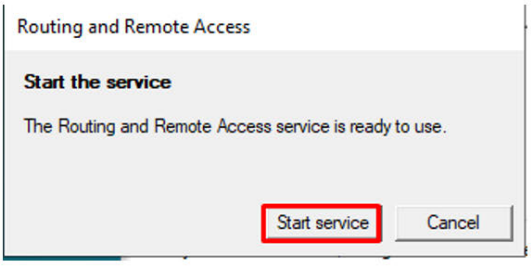
I'll select the custom configuration option since the other ones are not suitable



I'll select NAT/Routing since the other ones are not suitable

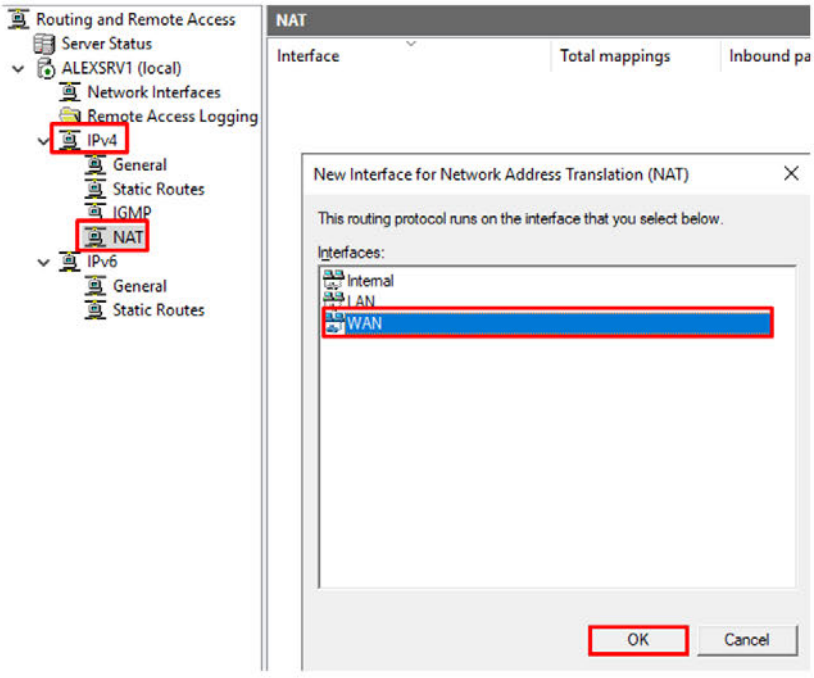


I'll start the service

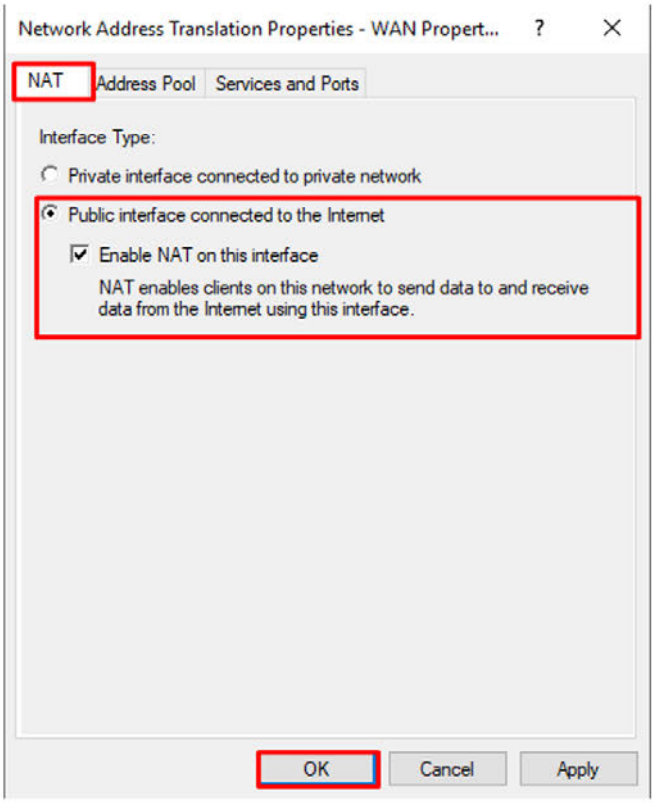


The next step is adding a new interface in the Routing & remote access tool
The new interface will be added in IPV4 NAT interface

I will add a new NAT interface on the WAN

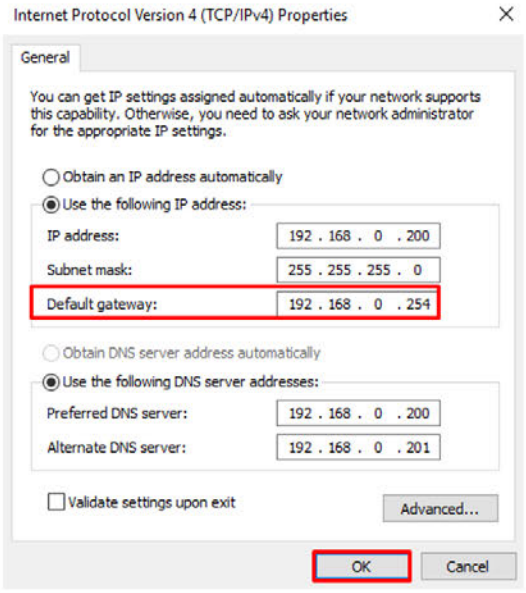


Here we can get the best of both worlds, basically it's a public interface that also enables clients on this network to use the internet using this interface

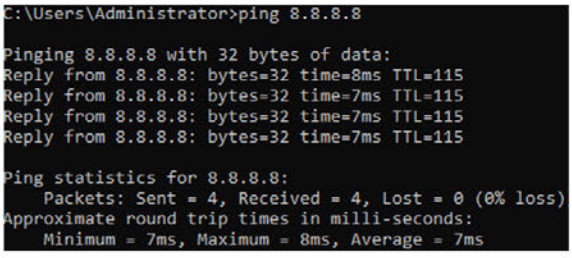


Right now SRV1 should be fulfilling his role as a router, let's check all of our systems to see if we when change the default-gateway to 192.168.0.254 (SRV1) they will have an internet connection

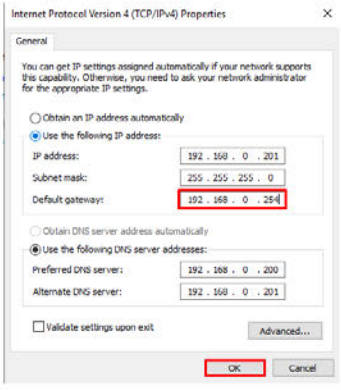
I'll start with checking DC1

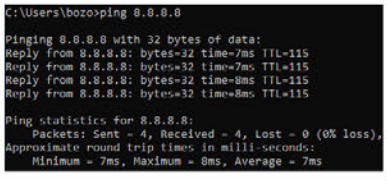


Use the ping command to check if the internet is connected properly, I'll ping 8.8.8.8 (google)

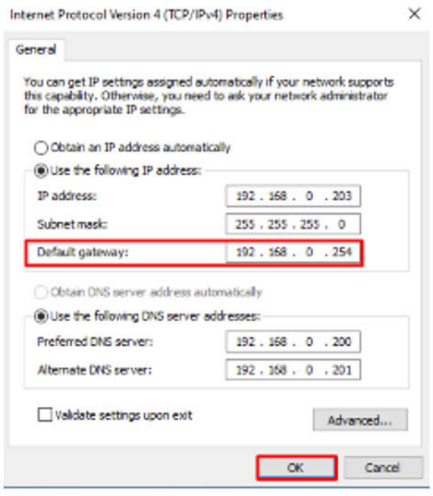


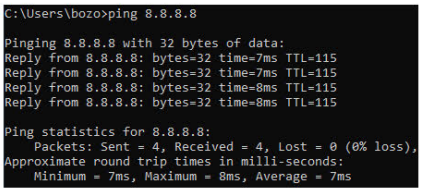
Now I'll do the same for alexPC1 & alexDC2, I'll also check alexSRV1 internet connection
First I'll check PC1 after changing the default-gateway



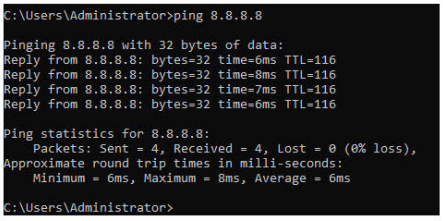


Good we have connection, now I'll do the same for DC2



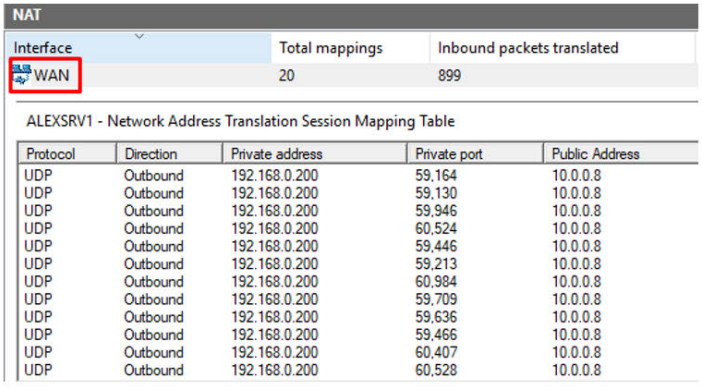


DC2 also has connection, finally I'll check if SRV1 has connection as well



All 4 systems have connection and are able to use the internet after the changes I've made

We can also see the mappings on SRV1



DC1 is configured to use the default gateway of your NAT server (192.168.0.254), and DC1 is able to access the internet, this indicates that Port Address Translation (PAT) configuration is working.

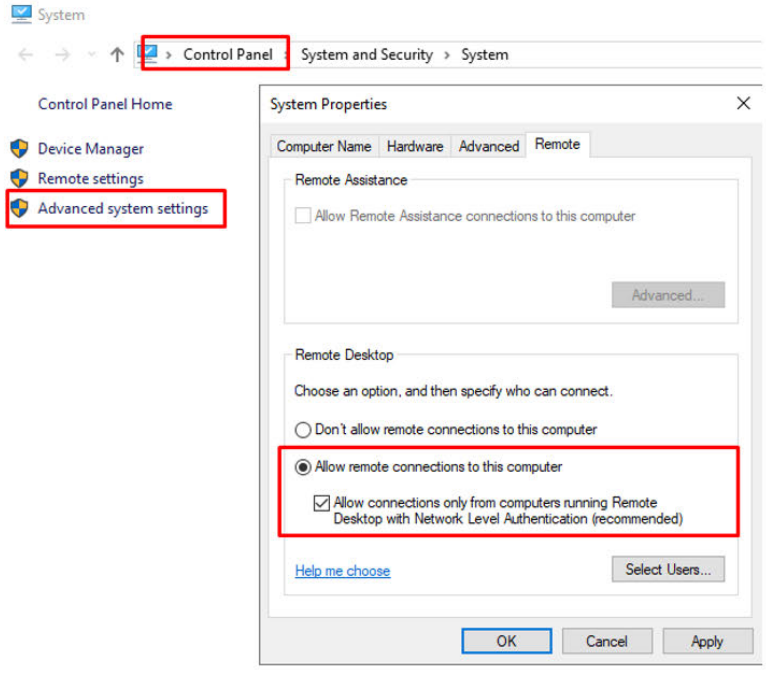
Using the NAT server as the default gateway means that DC1 outbound traffic is being translated by the PAT functionality, allowing it to share the NAT server's public IP address for internet access. This is a typical scenario when PAT is correctly configured, and devices on the local network can successfully access the internet through the NAT server.

Part 5 - Remote Server Management

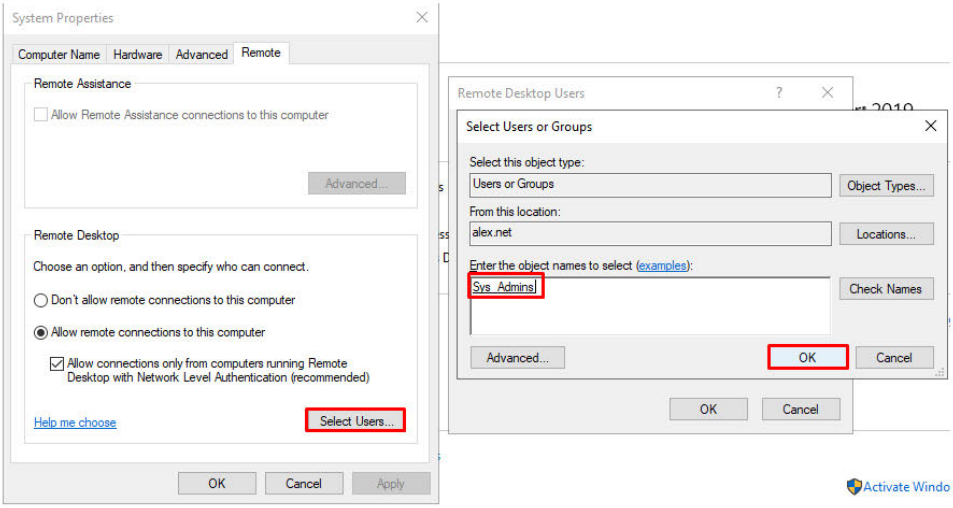
Remote access server management allows administrators to manage servers from anywhere, troubleshoot issues remotely, enhance security, efficiently apply updates, and minimize downtime. It is used for quick and secure access to servers, especially for tasks like troubleshooting, updates, and maintenance, regardless of physical location.

In this part I will allow the Sys_Admins to manage the servers from alexPC1 (Windows 10s) using Remote Desktop

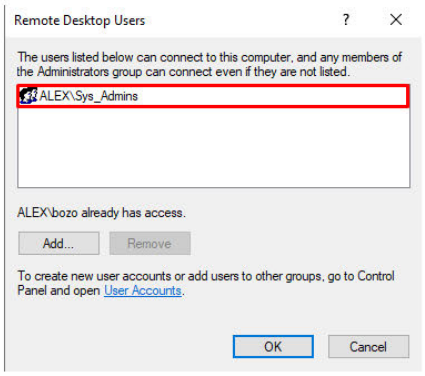
First I will configure all three servers to make them accessible remotely
I'll start with DC1, after going into system in the control panel, than advanced system settings
I will select the "Allow remote connections on this computer option"

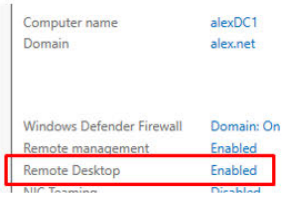


Now I will add the Sys_Admins group to have remote desktop authorization

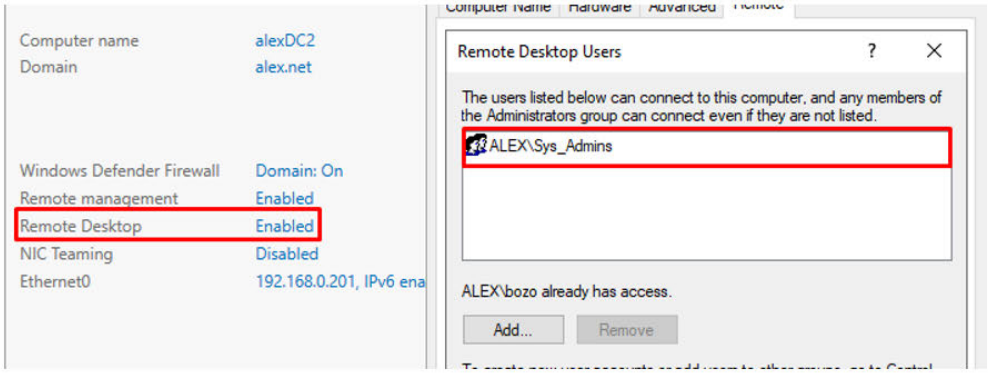


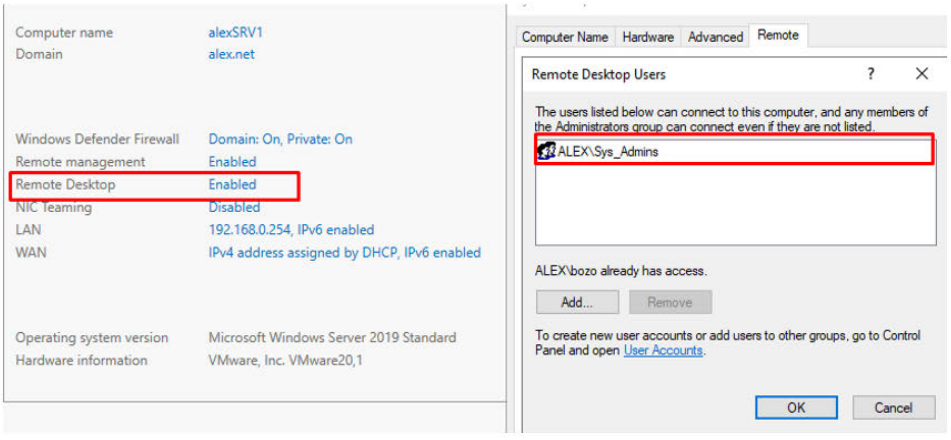
I can see that now the Sys_Admins group can connect to this computer (Remote Desktop Users) and we can see that the remote desktop option is enabled





I will now repeat the exact same process I've just done to DC1 to DC2 & SRV1

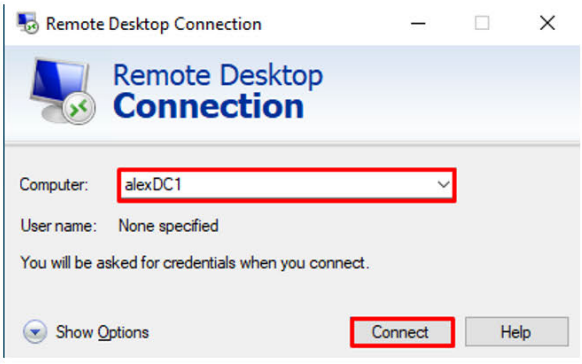




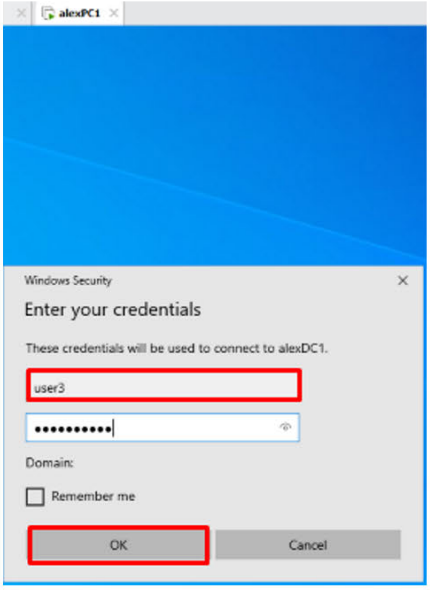
Both DC2 & SRV1 are now configured with remote access & authorized specifically for the Sys_Admins group

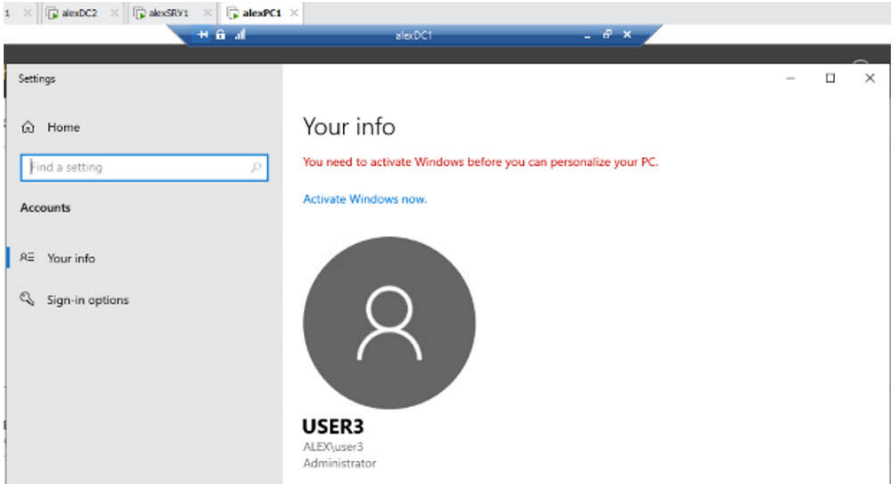
Now I can test to see if the configuration worked, I'm going to login from alexPC1 (WIN10) with a Sys_Admin user (user3) and see if I'm able to get remote access successfully for all three servers

First I'll login to PC1 with the username - user3 who is a part of the Sys_Admin group that has remote access privileges
I'll start with gaining access remotely to DC1, using remote desktop connection

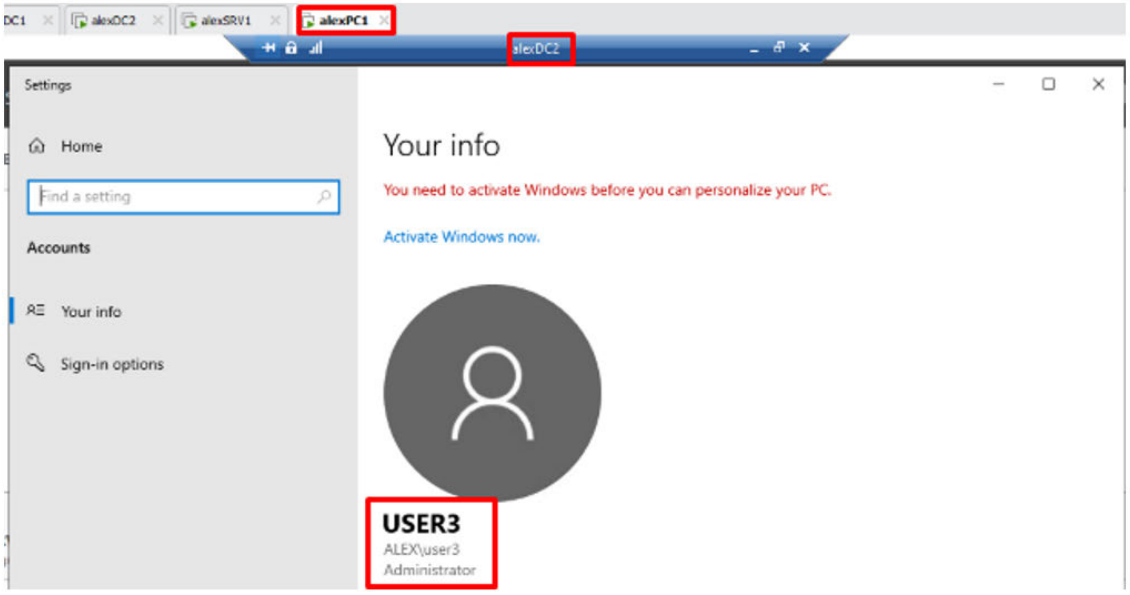


I will now enter the user3 credentials to remotely access DC1

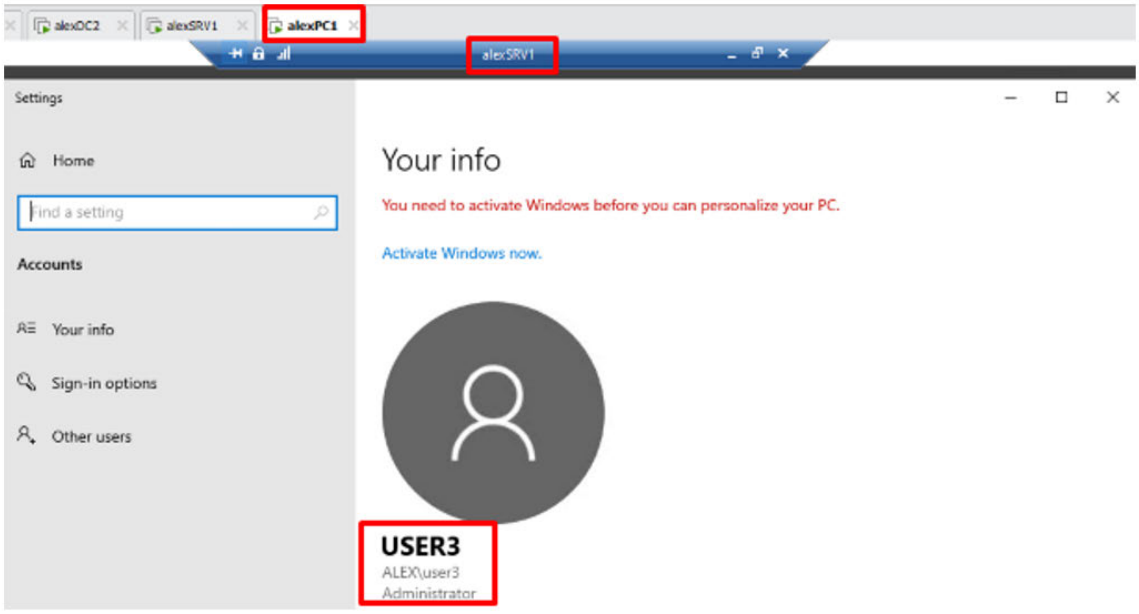




Remote access has worked for user3 from PC1 (WIN10) to DC1, I will repeat the exact same process for DC2 & SRV1



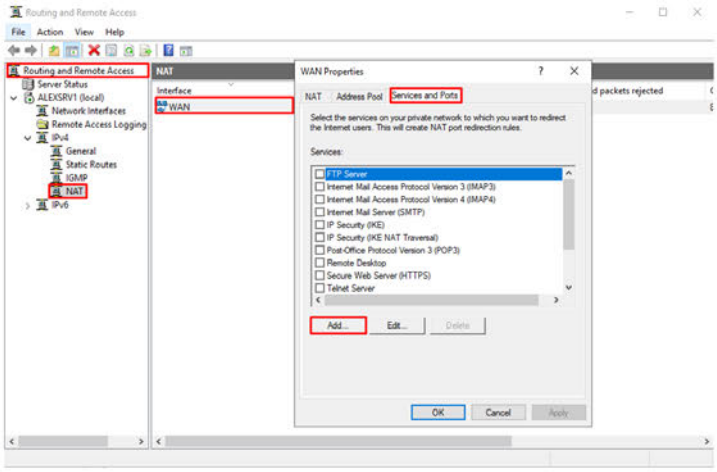
The same process has worked for DC2 & user3 is able to remotely manage it



The same process has worked for DC3 & user3 is able to remotely manage/access it

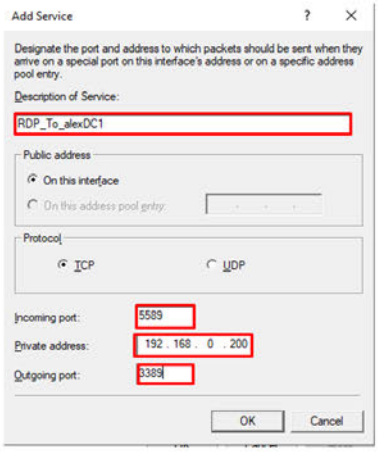
Next, I will allow RDP for server DC1 for a worker outside the organization, from port 5588 to port 3389 in the server

To do this I need to go back to SRV1 and go to the routing and remote access tool



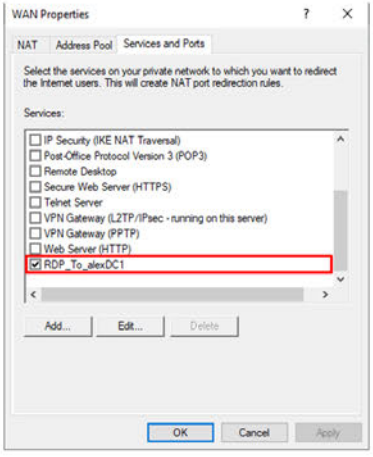
RDP (Remote Desktop Protocol) allows remote control of a computer over a network, commonly used for remote administration and troubleshooting in networking.

I will add a new service/ports on my WAN interface in IPv4 NAT

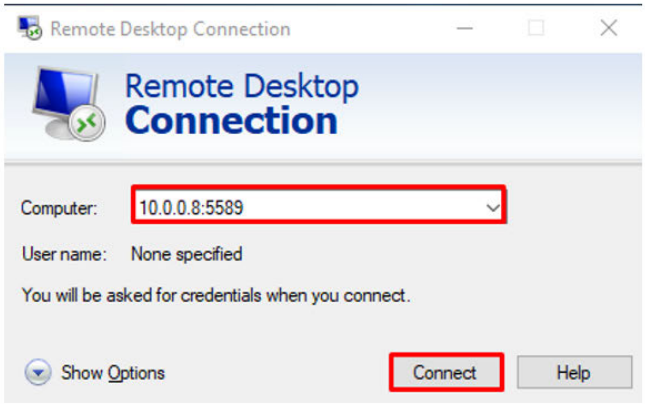


Changing the incoming port for RDP to 5589 while keeping the outgoing port as 3389 means that RDP_to_DC1 now uses a non-default port for external connections. This modification is a security measure, often used to obfuscate RDP access and reduce exposure to potential threats targeting the default port (3389).

The service is now active, which means we have allowed a worker that works outside the local network to use this secure service



Now let's test with the IP address of 10.0.0.8:5589 (WAN) and see if we can remotely access DC1



The connection is successful

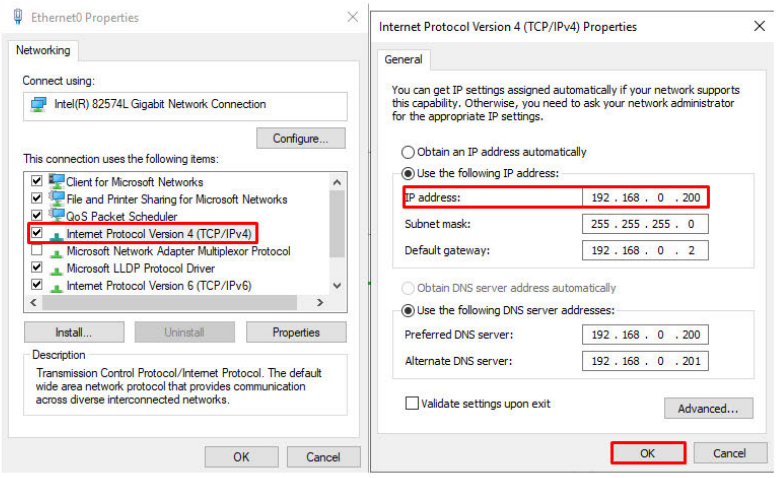
re this local server

Part 6 - Installment & Configuration of DHCP

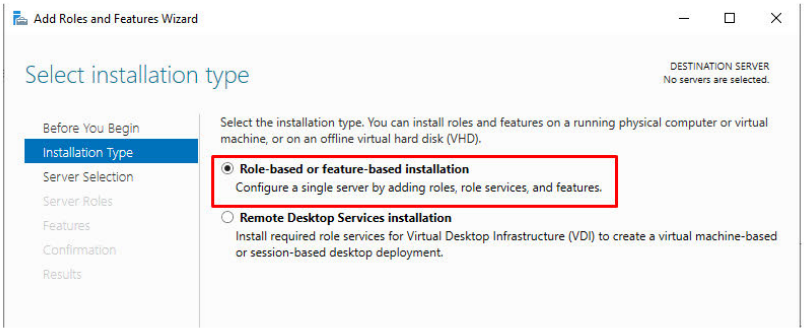
Dynamic Host Configuration Protocol (DHCP) is a network protocol that automates the assignment of IP addresses and other network configuration parameters to devices on a network. Its primary role is to simplify and streamline the process of connecting devices to a network by dynamically assigning IP addresses, subnet masks, default gateways, and other essential parameters.

DHCP plays a crucial role in simplifying network management, reducing the likelihood of configuration errors, and facilitating the efficient allocation of IP addresses. It is a fundamental component for modern networks, ensuring a streamlined and automated process for device connectivity.

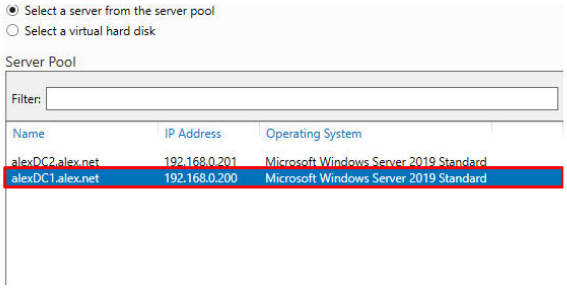
In this part I will be installing and configurating DHCP on the alexDC1 domain controller, first I'll start by giving DC1 a static IP address, followed by the installation of the DHCP server



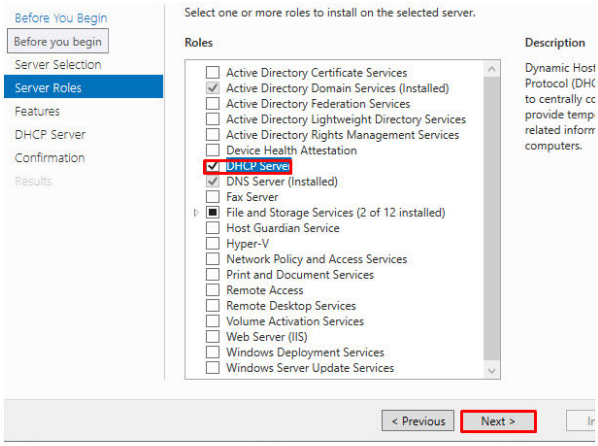
Now that we've made sure that DC1 has a static IP address we can begin the installation of the DHCP role



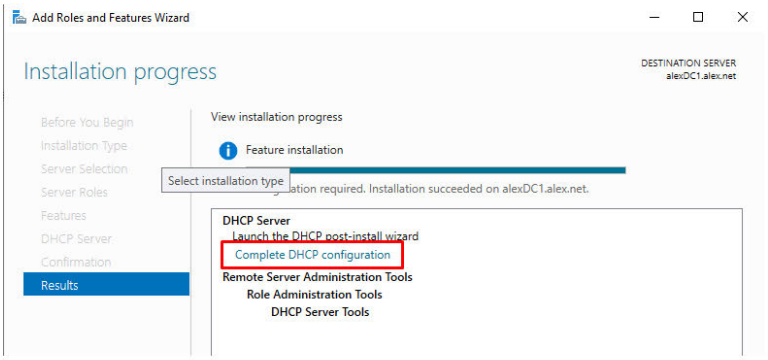
Here I'll select the DC1 server since its the designed DHCP server



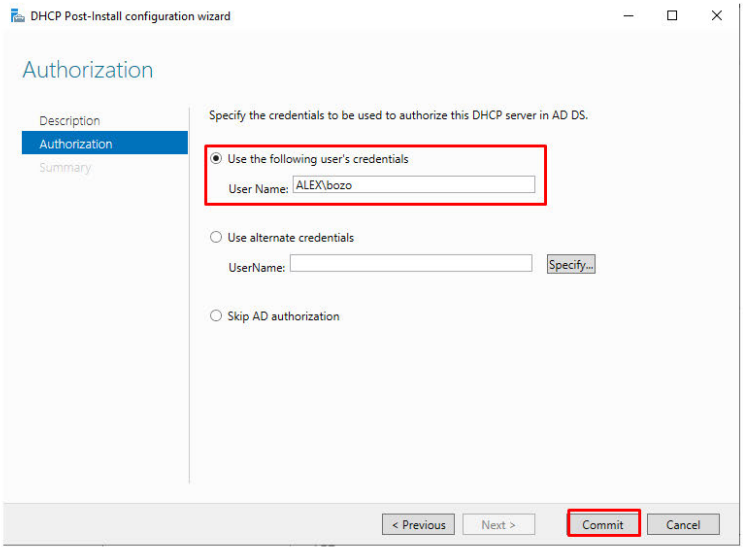
Selecting the DHCP role for installation

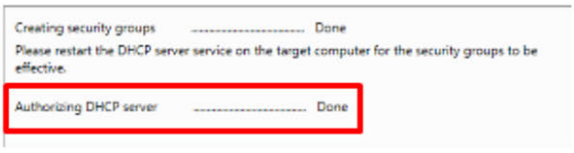


Completing DHCP Configuration



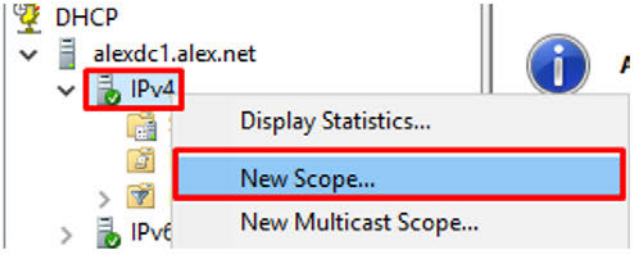
Providing the proper credentials for authorization



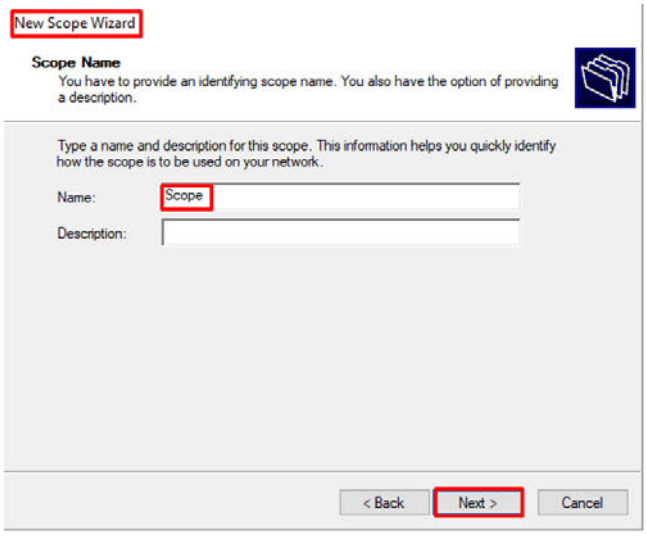


Now that I'm done installing the DHCP server on DC1, I can begin with the configurations
Let's start with configuring a scope that gives out 50 IP address.

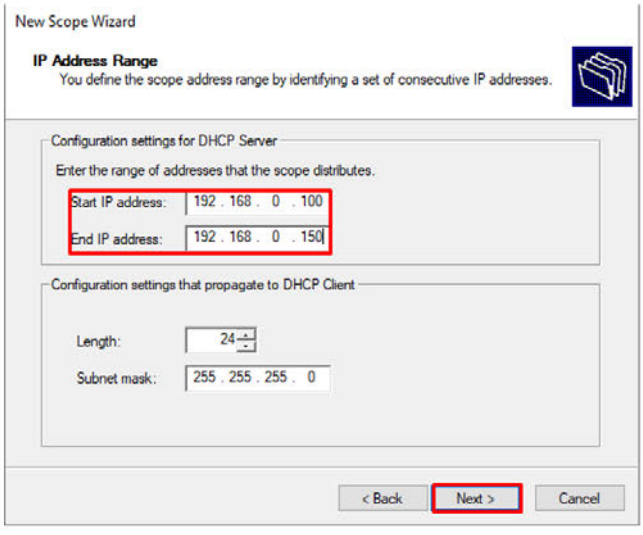
First I will create a new scope



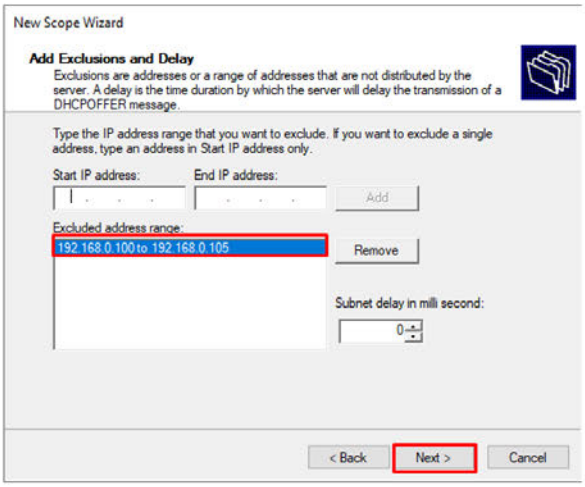
Naming the new scope, with a very creative name



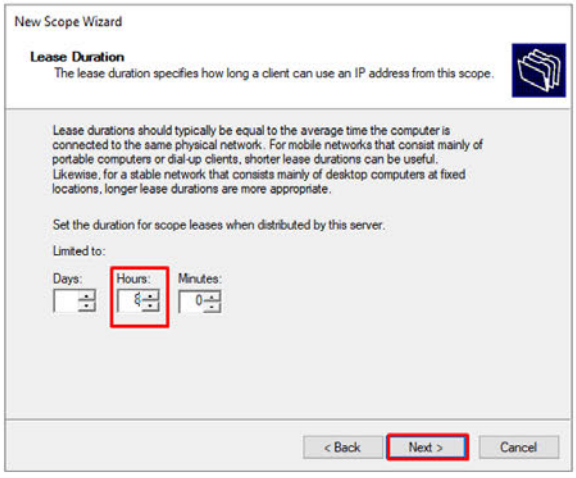
In the IP Address Range I'll define the scope by selecting a set of consecutive IP addresses, I have selected 192.168.0.100 to 192.168.0.150 which is 50.



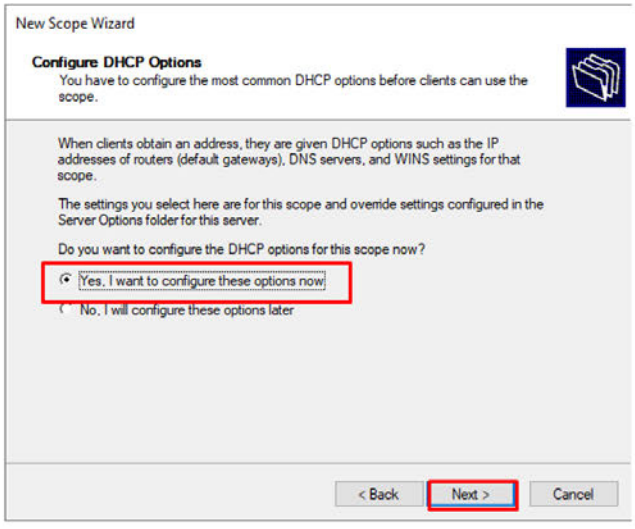
Now I'll configure Address Exclusions for the first 5 IP address of the Scope
the range of the Address Exclusions is - 192.168.100 to 192.168.105



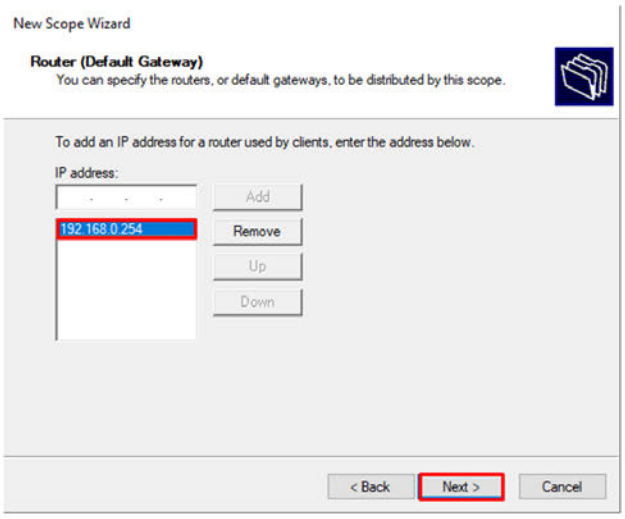
I'll also configure an 8 hour Lease



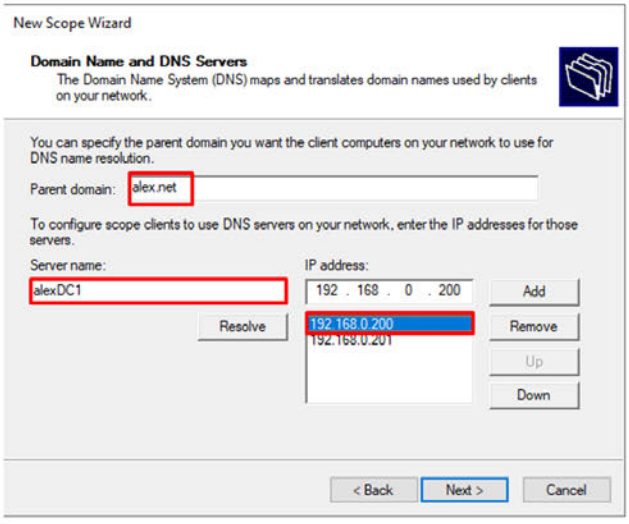
Now I'll begin the configuration of the DHCP options, I will configure DNS for a domain controller
router which is SRV1 and a suffix named after the domain



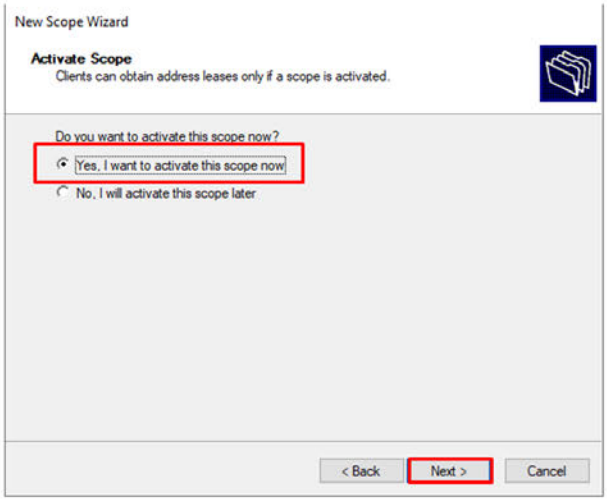
This part of the scope wizard allows the DHCP to distribute an IP address to the Router (SRV1)



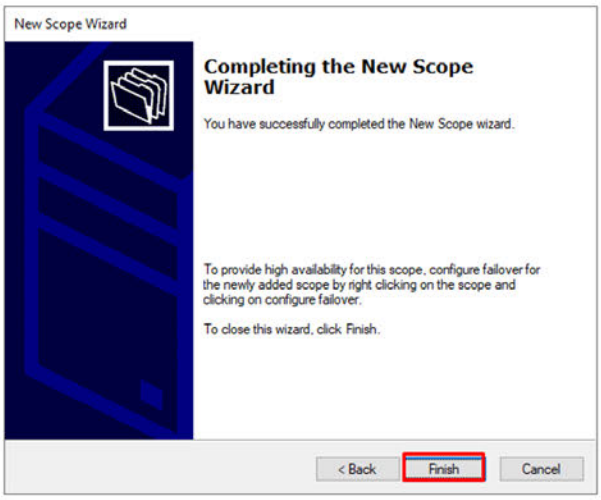
This part of the scope Wizard maps and translates domain names used by clients on my network
I will select DC1 as the first option



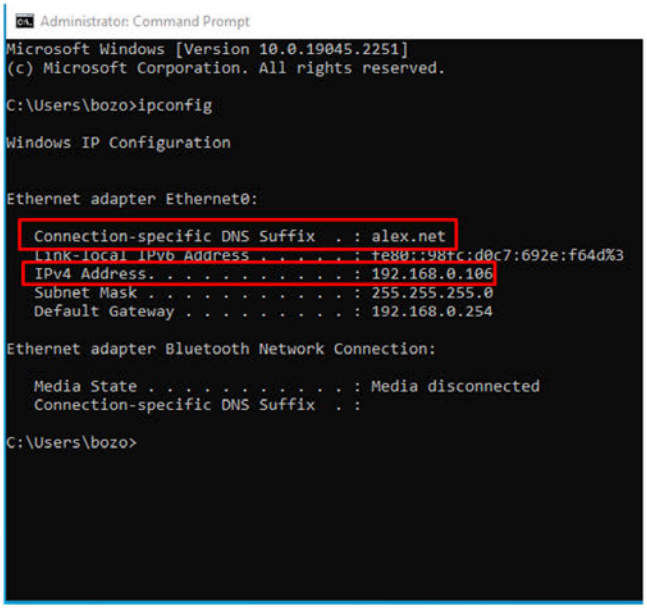
I will activate the scope now



The new scope installation is now complete

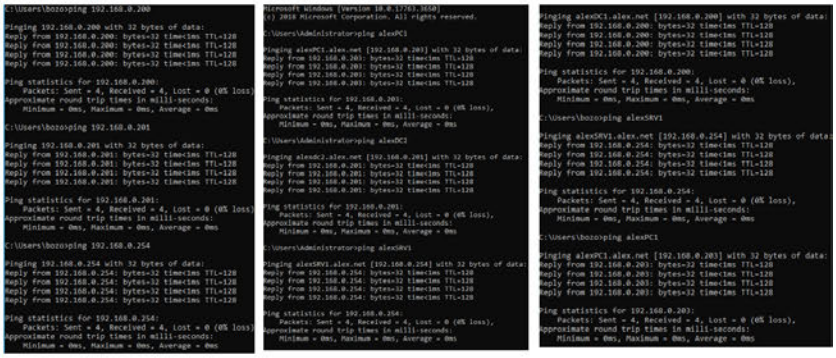


It's time to do a connectivity test
First I'll check that PC1 (WIN10) is getting his IP automatically from the DHCP server



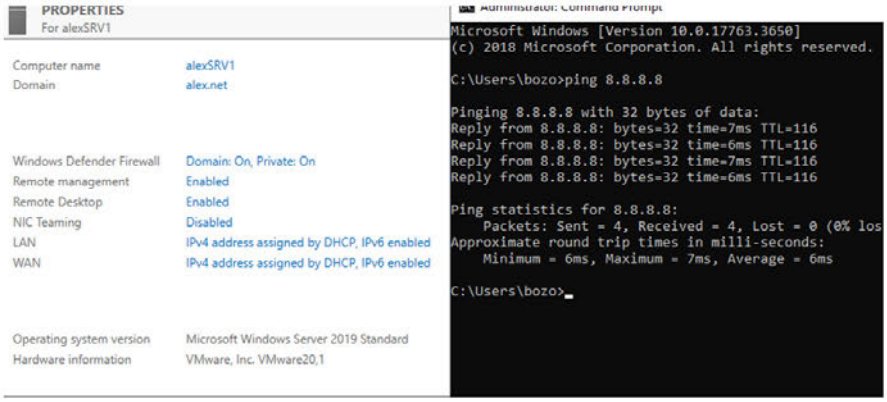
After using CMD we can see that the DNS Suffix is working, and the IP address is from the DHCP scope range which means it got it from the DHCP (auto)

Now I'll check that PC1 can ping all the other systems on the network, same for the other devices



All systems have connectivity and can communicate with each other after the changes

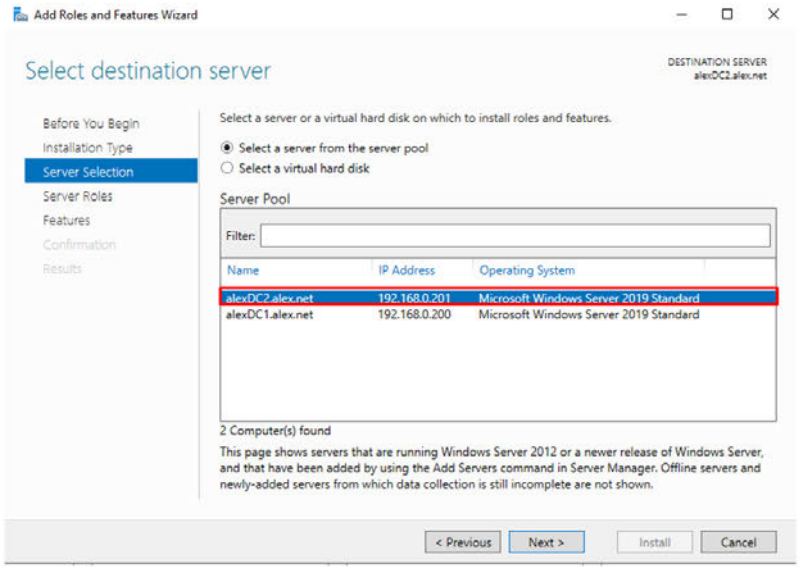
I'll also check if SRV1 can ping the internet



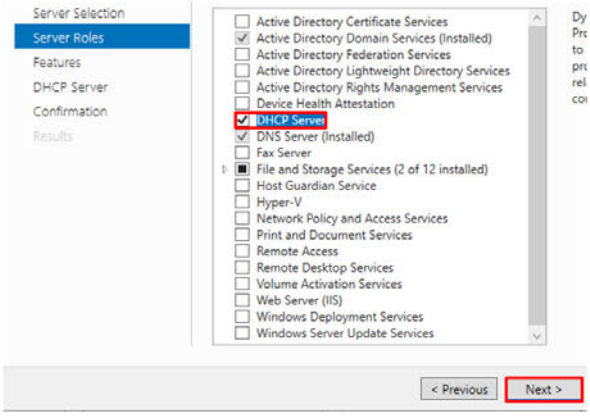
Ping is successful

Setting up a DHCP failover cluster:
A DHCP failover cluster ensures continuous DHCP service by allowing multiple servers to share the load and take over if one fails, providing high availability and fault tolerance.

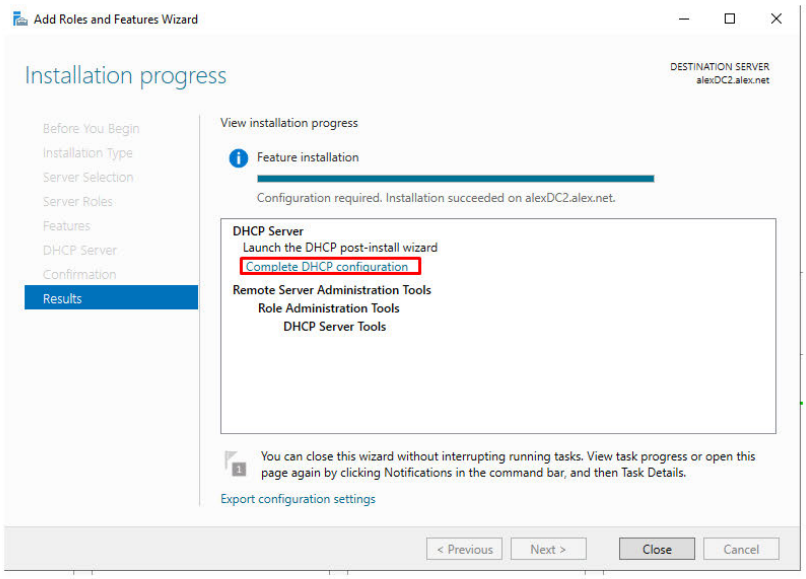
Now I'll create Failover Cluster using DC2, installing the DHCP role on DC2 the same way as I did with DC1 with the adds roles and feature wizard



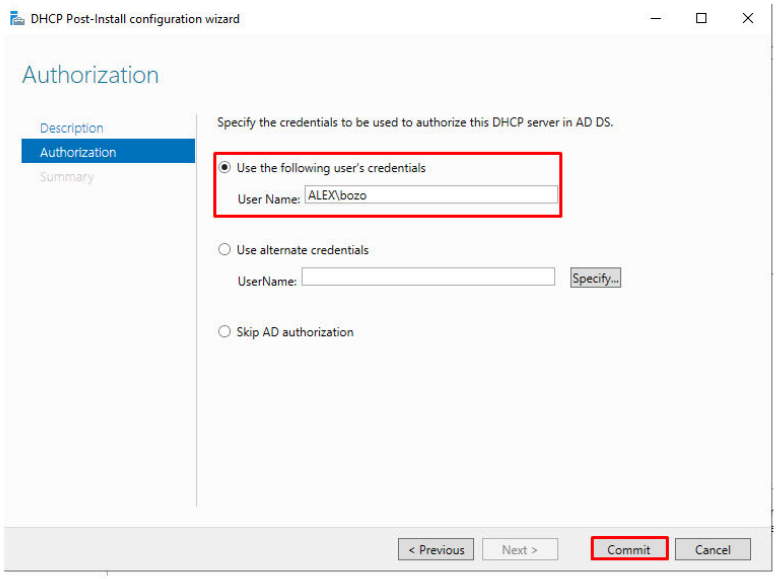
Selecting the DHCP server role on DC2

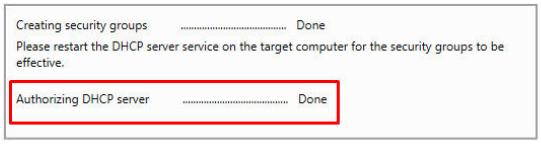


Select the complete DHCP Configuration



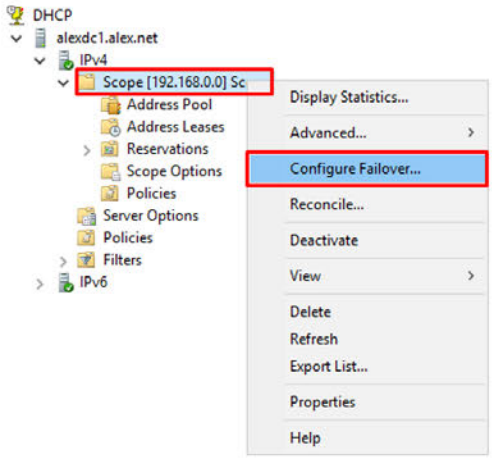
Commit authorization





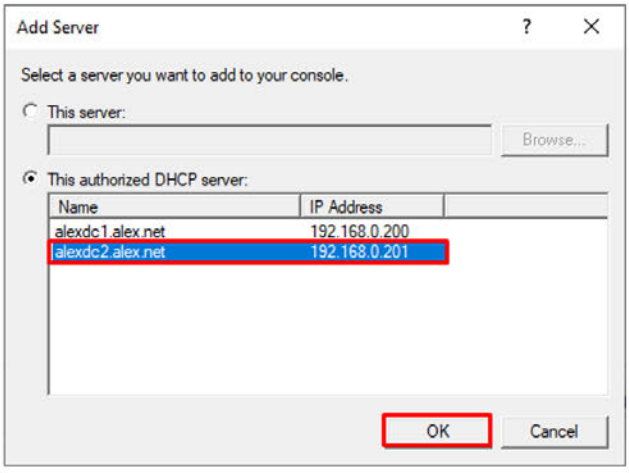
Now there are two active DHCP servers

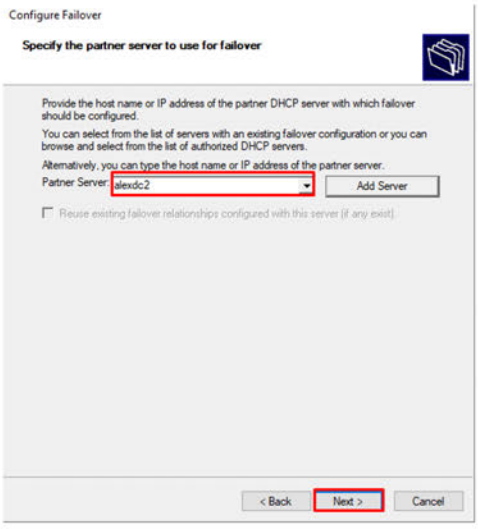
I'll configure the failover cluster



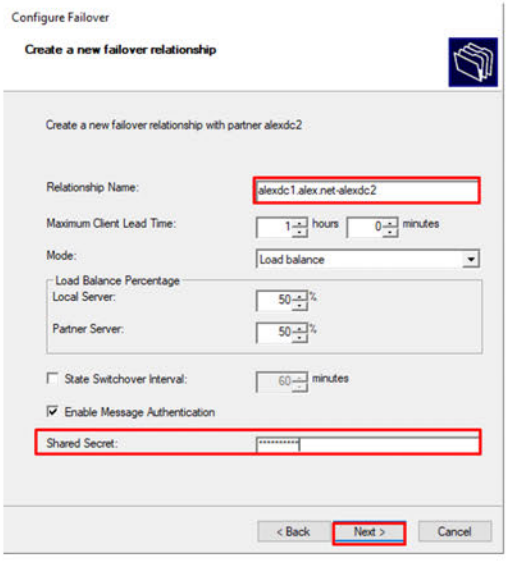
Select all Available scopes

I will select alexdc2 to use for failover

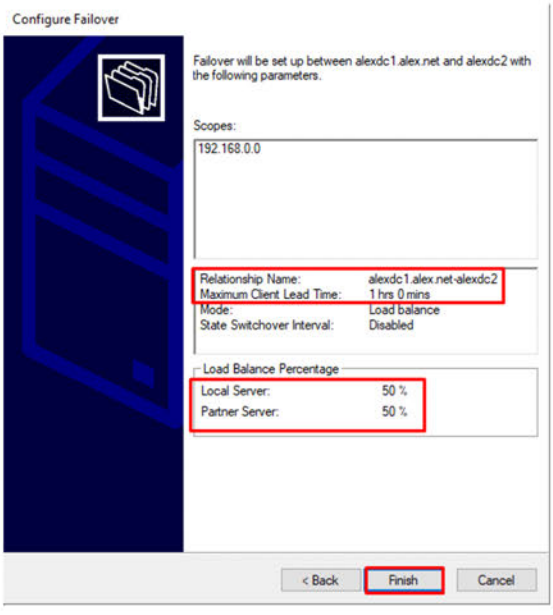




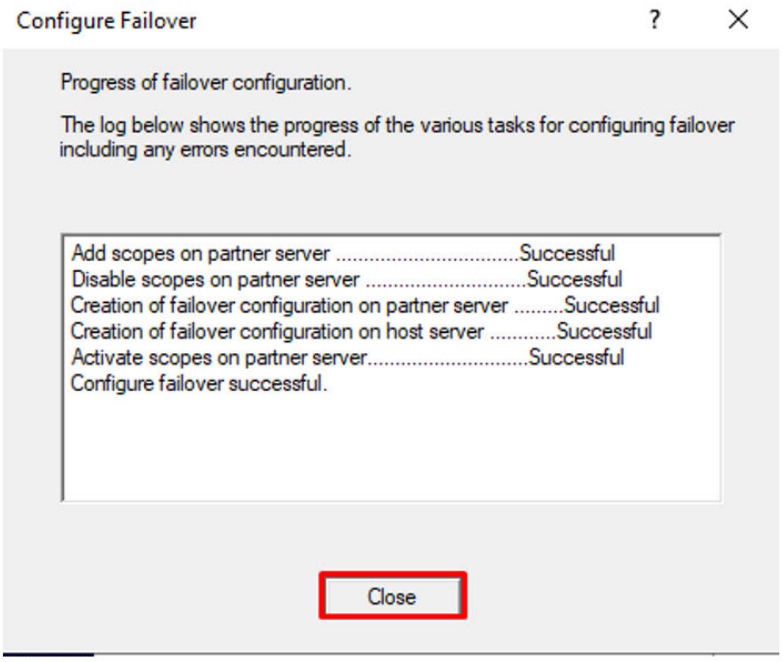
DC1 & DC2 now have a failover relationship, the load balance is 50/50



Failover will be set by the following parameters



Failover configuration is complete



Now I have better fault tolerance and load balancing on my network thanks to this failover configuration

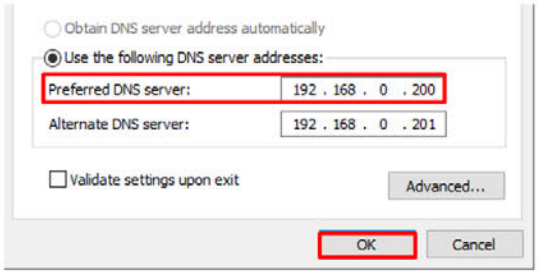
Part 7 - DNS Server Configuration

DNS is a system that translates readable domain names into IP addresses, enabling seamless internet communication.

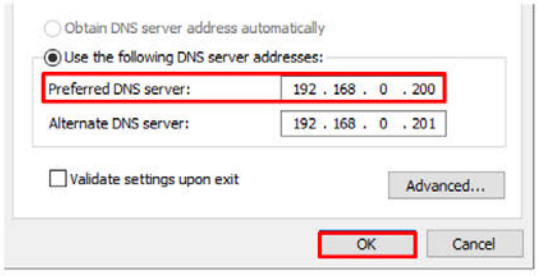
Configuring DNS servers on a local network is crucial for efficient name resolution, faster network performance, resource discovery, enhanced security, customization, and reduced dependency on external services. It facilitates smooth and secure communication within the network.

Starting up, I'll make sure the all of my systems are configured to use DC1 as their DNS which is 192.168.0.200

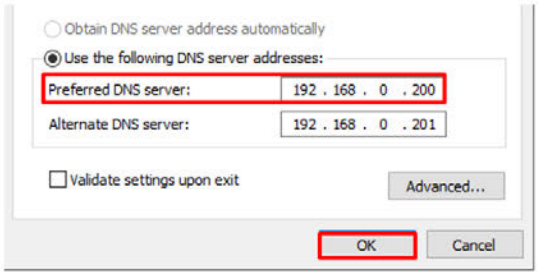
DC1 is using the correct DNS of DC1



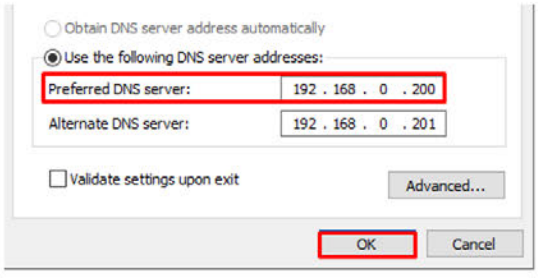
DC2 is using the correct DNS of DC1



SRV1 is using the correct DNS of DC1

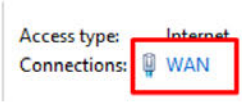


PC1 is using the correct DNS of DC1

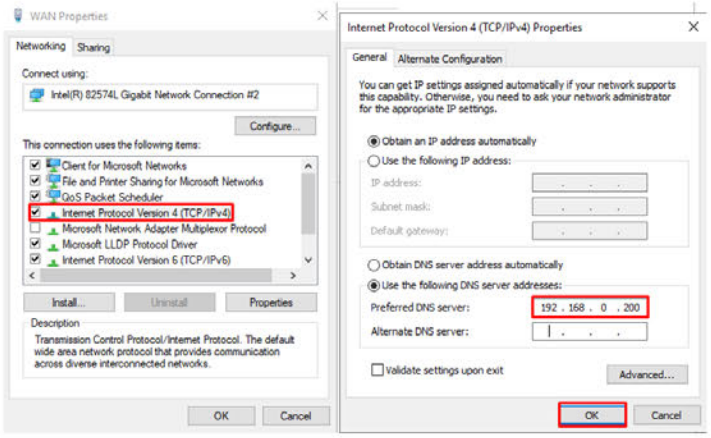


I'll also make sure that I manually configure the SRV1 bridged card to also use the DC1 DNS

Select the WAN connection since it's the bridged connection



Now adding the DC1 address to use as the DNS for the SRV1 bridged card



We can see that the LAN network is connected to the alex.net domain

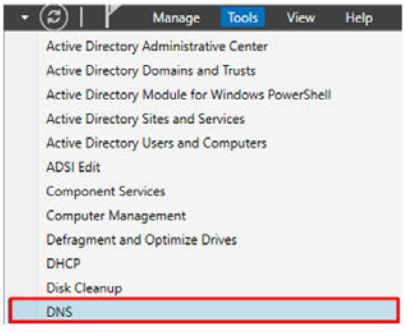
Forwarding in networking is the process of directing data packets to their destination based on the destination address. It optimizes data routing, interconnects networks, enables packet switching, and supports routing decisions for efficient and scalable communication.

In Active Directory DNS, forwarding directs unresolved DNS queries to external DNS servers, improving name resolution efficiency within and beyond the AD domain.

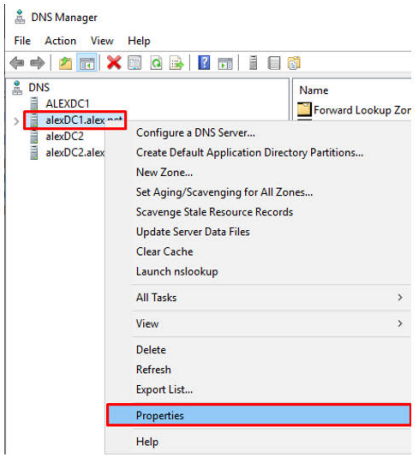
In DNS forwarding for security, administrators can configure DNS servers to use forwarders that filter and block access to specific websites. By directing DNS queries through these forwarders, malicious or unwanted websites can be identified and restricted, enhancing network security and controlling user access to specific content.

In Forwarding I'll start with configurating forwarding to an outside DNS server 8.8.8.8 (google)

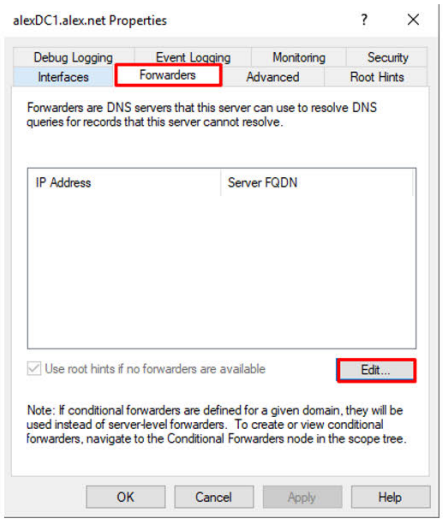
Tools, DNS manager on DC1



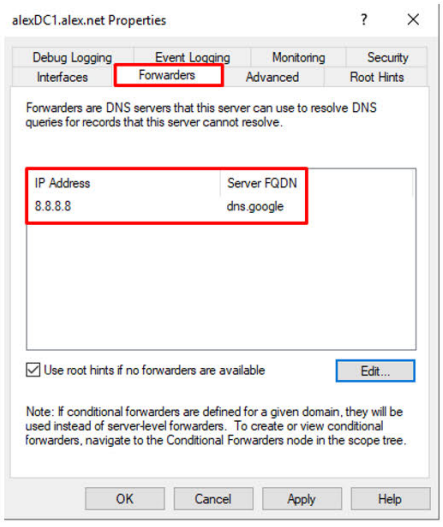
Select the alexDC1.alex.net DNS and go to Properties



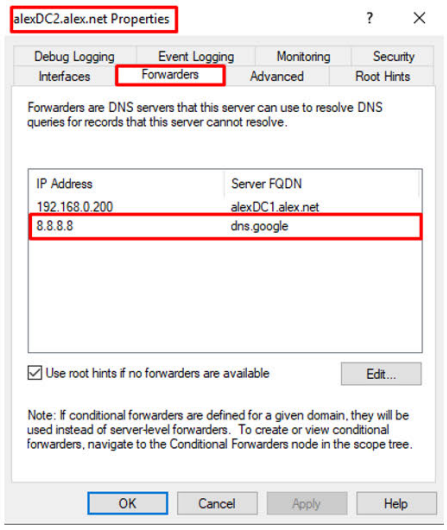
Click on Edit in Forwarders to add 8.8.8.8 (google DNS)



8.8.8.8 which is google DNS is now Forwarding for DC1

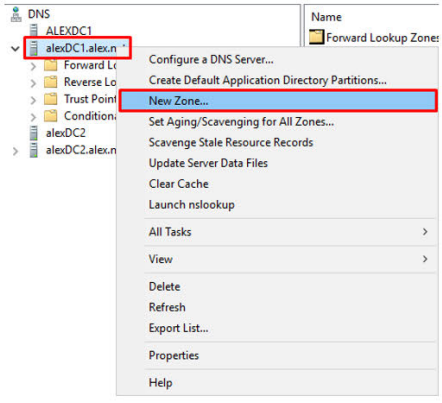


I'll do the exact same thing for DC2

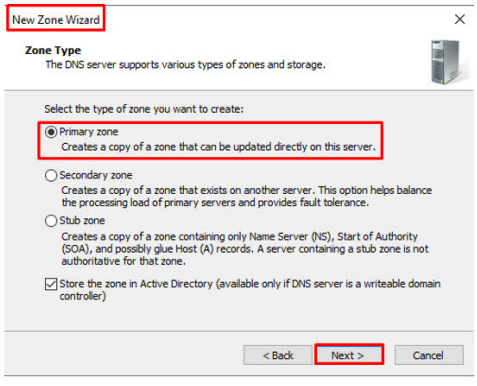


Next I will make Facebook.com a primary zone in order to prevent workers from using it during the workday

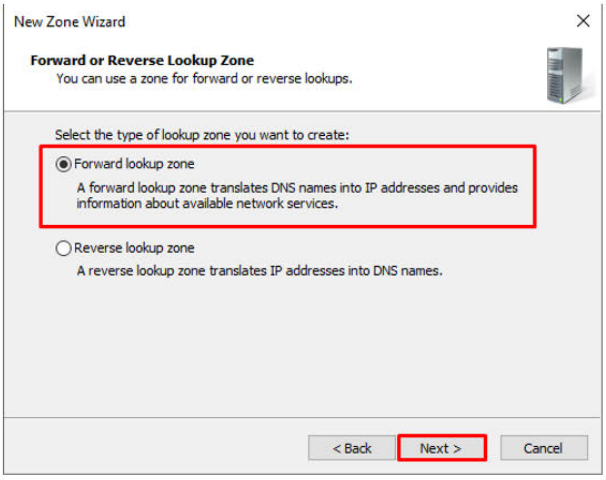
In the DNS manager I will create a new zone in DC1



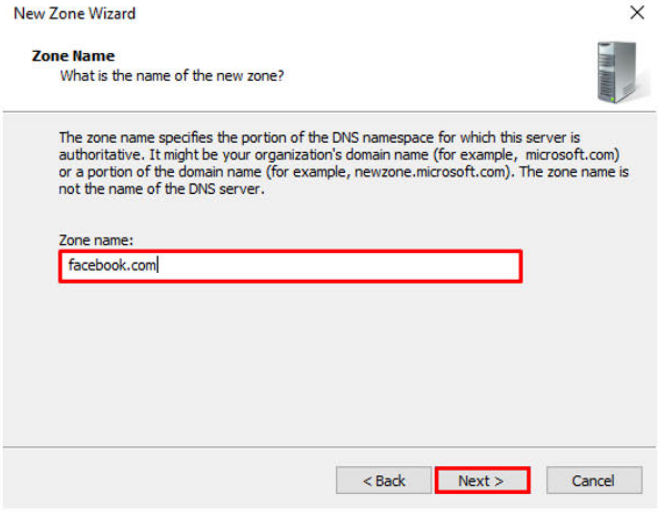
I'll select the Primary Zone in the New Zone Wizard



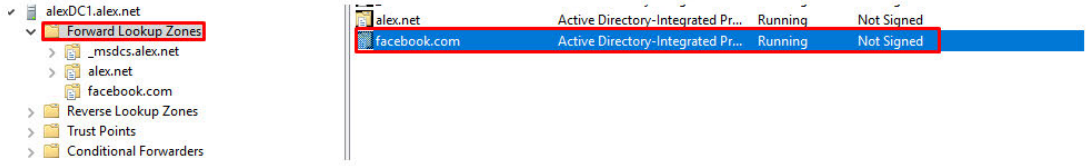
Select the Forward lookup zone



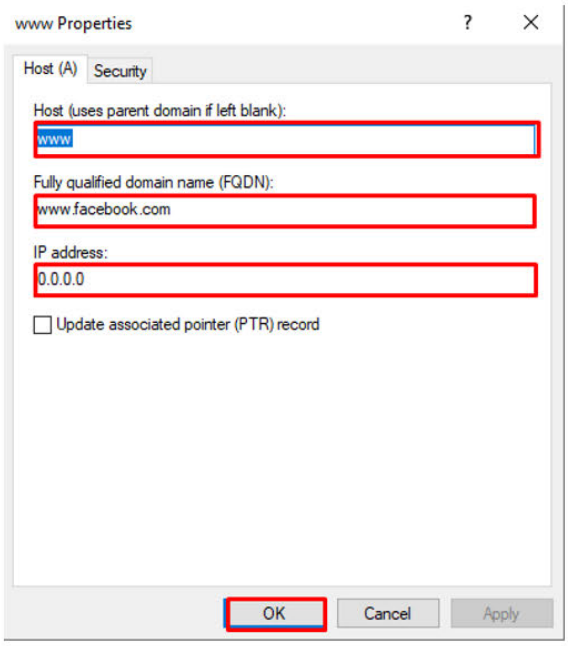
Zone name is facebook.com since we want prevent workers from using it



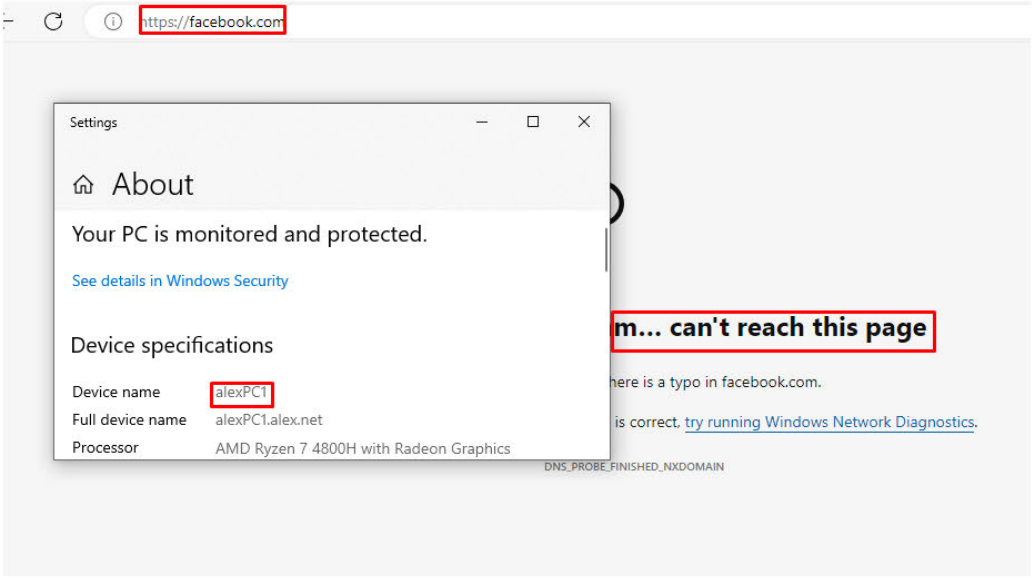
I'll go in the facebook.com Forward lookup zone



Now I'll create a new host with the IP address of 0.0.0.0, this action will send anyone trying to go to facebook.com To 0.0.0.0 instead of the real Facebook IP address which will prevent them from using Facebook

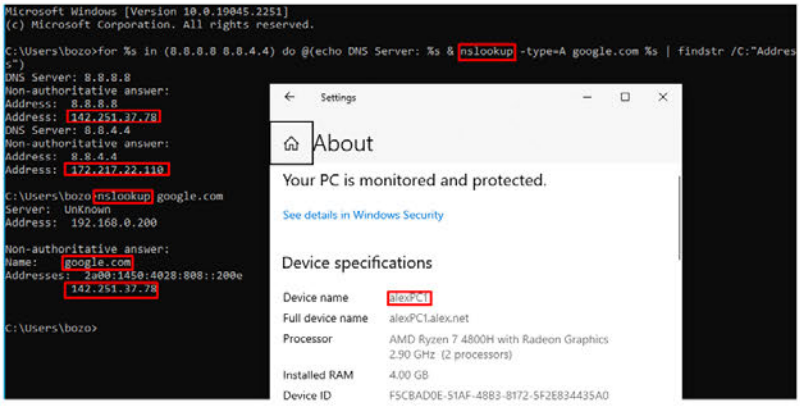


Now let's test on PC1 if he can use Facebook.com



Facebook.com is unreachable

Next I will use PC1 (WIN10) to see if it can translate google.com IP addresses using the nslookup command

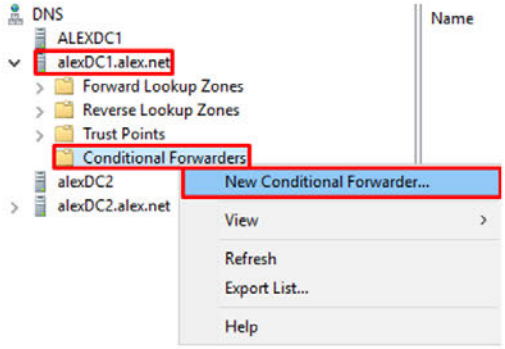


PC1 can translate google.com IP address using the lookup command

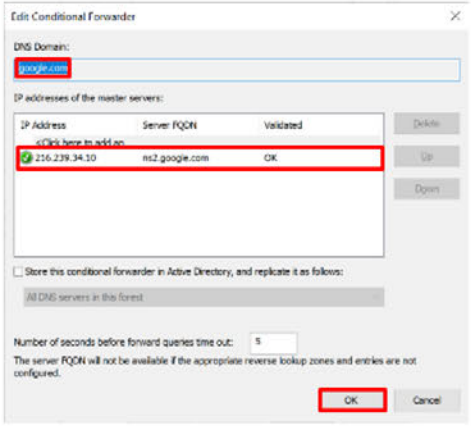
Next step I will configure conditional forwarders for google.com

A conditional forwarder in DNS directs queries for specific domain names to designated DNS servers. It's useful for optimizing network traffic, handling split DNS scenarios, and enhancing security by routing queries for specific domains through designated servers.

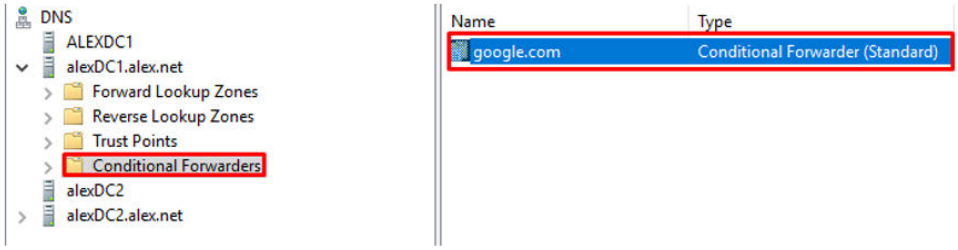
I'll create a new Conditional Forwarder



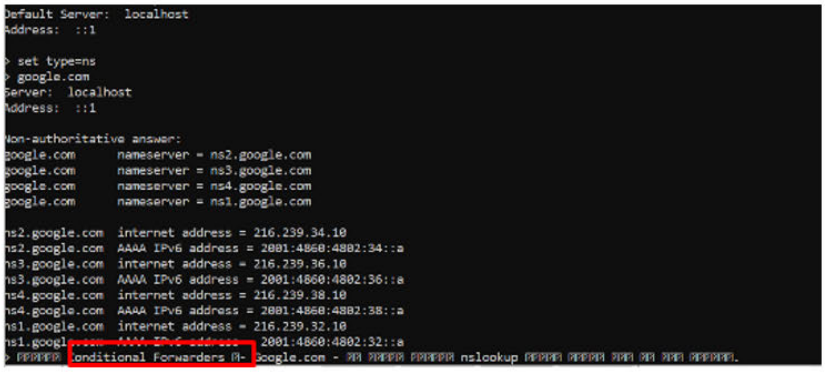
Adding google.com



I have a google.com Conditional Forwarder



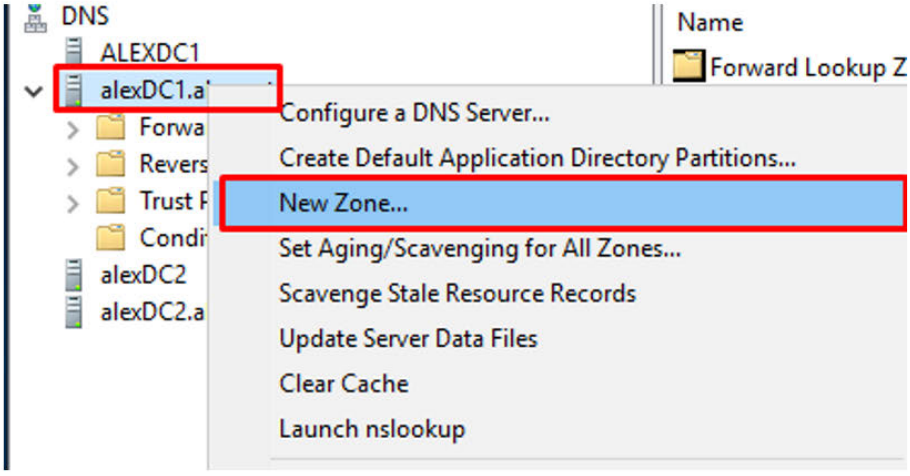
Using nslookup



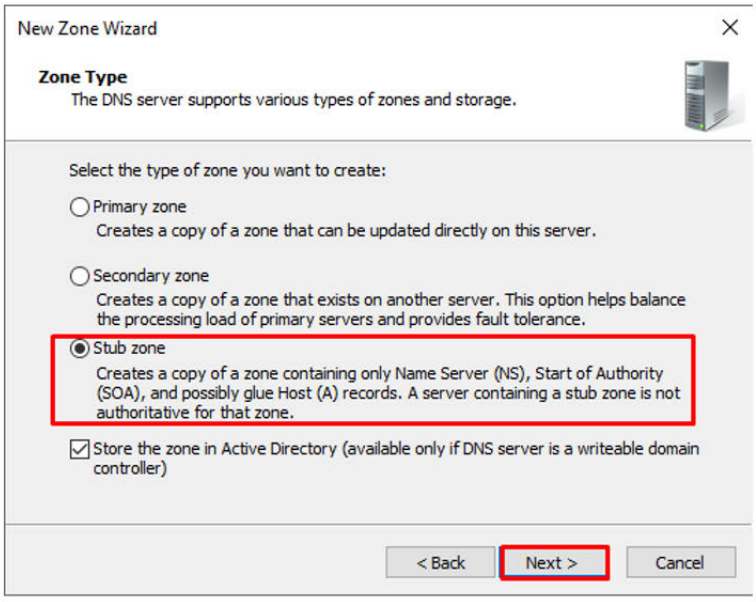
On the next task, I will configure a stub zone for Yahoo.com

A stub zone in DNS is used to optimize resolution by containing only essential information about authoritative name servers for a specific domain. It improves efficiency, isolates DNS queries, and enhances security in network environments.

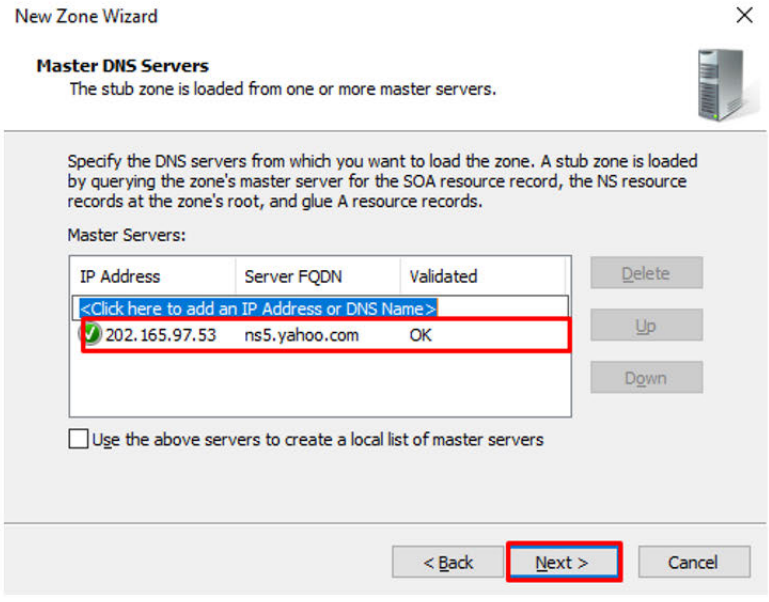
Starting by creating a New Zone



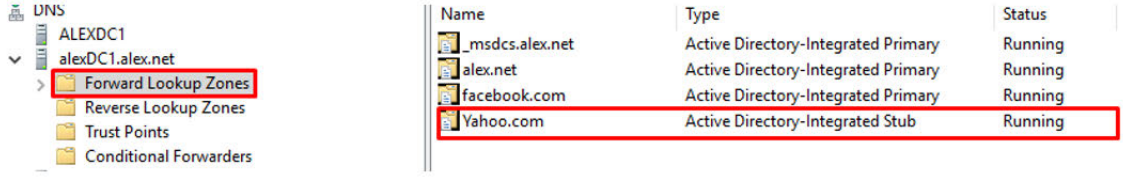
Select the Stub zone option



Using the ns5.yahoo.com address of 202.165.97.53



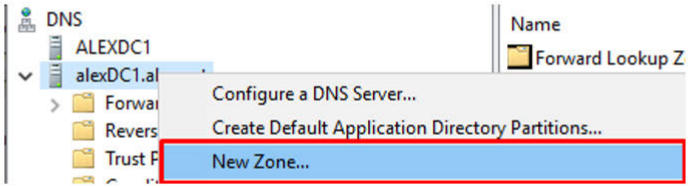
And now we can see that the Yahoo.com is running is configured as AD-Integrated Stub



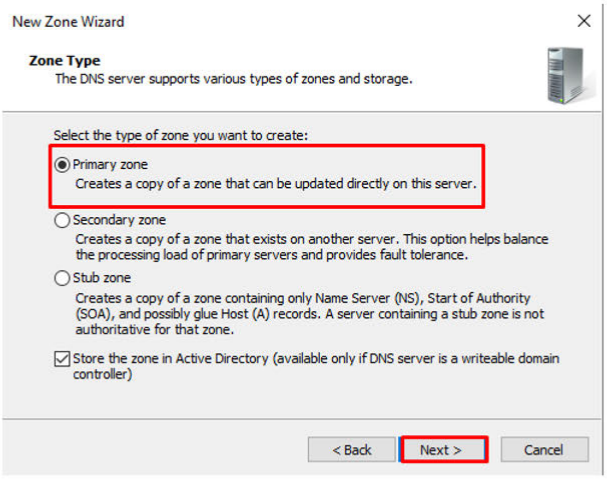
In the next part I will create a primary zone on DC1 named ShawarmaSucks, then I'll create a secondary zone on DC2 also named ShawarmaSucks

Primary zones in DNS are used for read-write access and are authoritative sources for DNS data. Secondary zones are used for read-only access and serve as backup copies, providing fault tolerance and load distribution. Primary zones are typically used for managing DNS records, while secondary zones are used for redundancy and improved performance in distributed network environments.

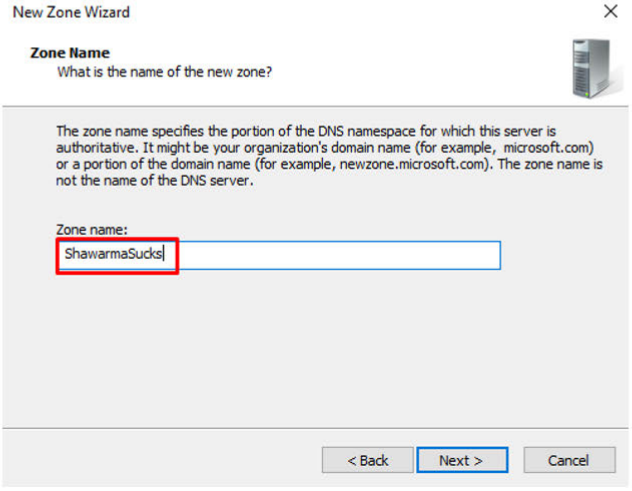
I'll start by creating a new zone on DC1



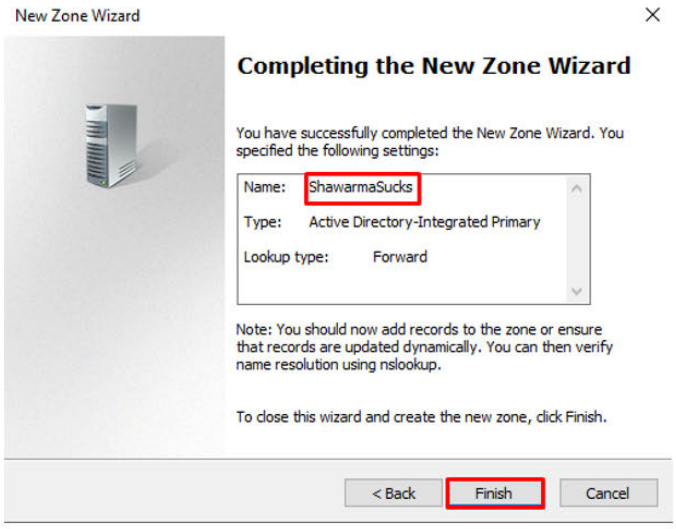
DC1 will be the Primary zone

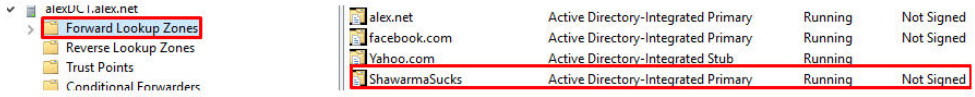


Will be named "ShawarmaSucks"

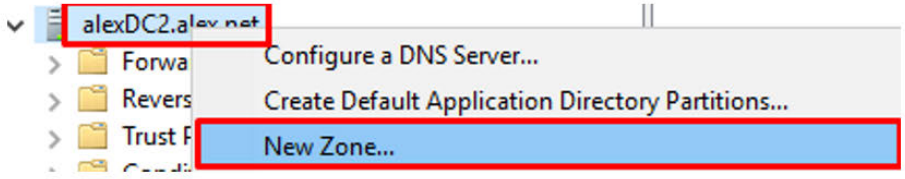


Finishing up the installation of the new primary zone

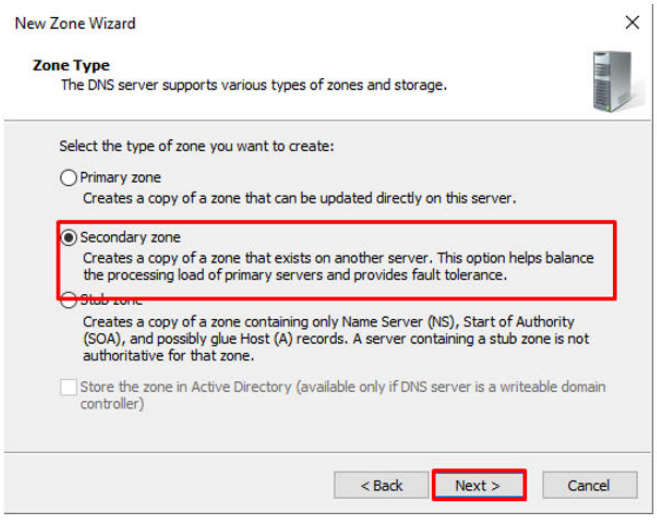




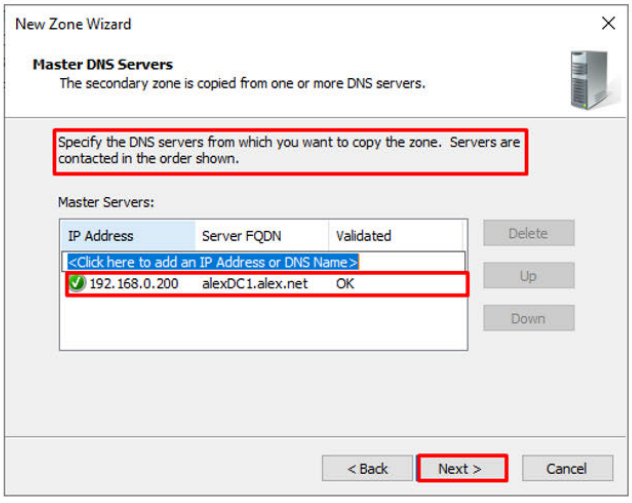
Next I will create a secondary zone named "ShawarmaSucks" on DC2



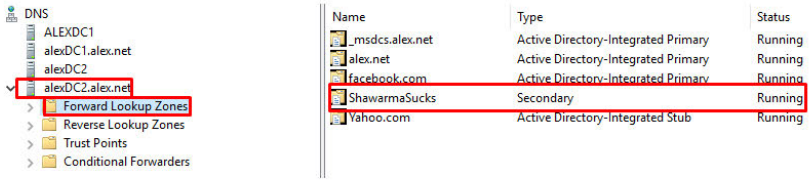
This time we will select Secondary Zone on DC2



I will copy the copy the Zone from DC1 or 192.168.0.200
since the secondary zone is copied from one or more DNS servers



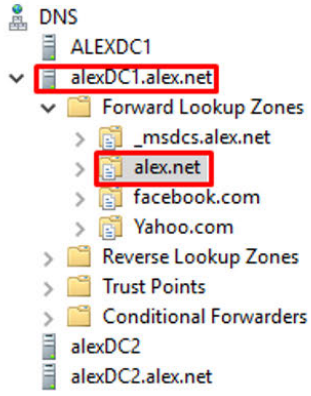
Finishing up the installation we can see that ShawarmaSucks is now also a secondary zone on DC2



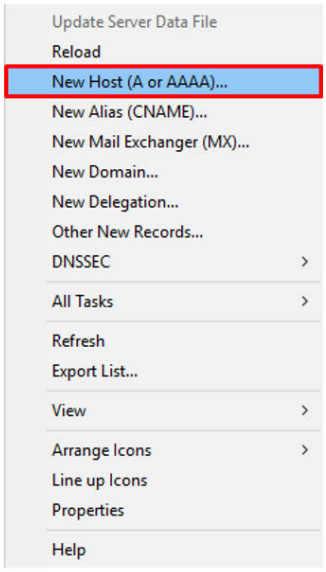
Next step I'll be creating a CNAME for DC1, naming it differently from its original name, I will than test if its working by pinging from PC1 to DC1 with its new name

A CNAME (Canonical Name) record in DNS is used to create an alias or nickname for an existing domain or subdomain. It is useful for simplifying domain management, facilitating changes, and creating flexible configurations.

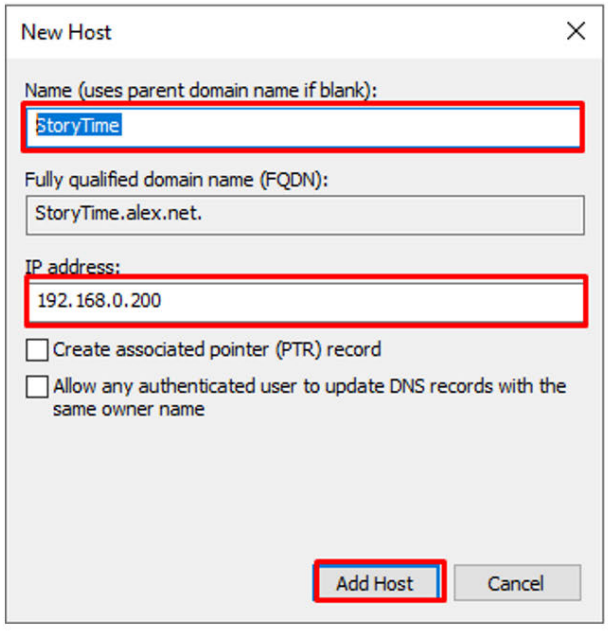
First I will go into the alex.net (my domain) in the DNS manager on DC1



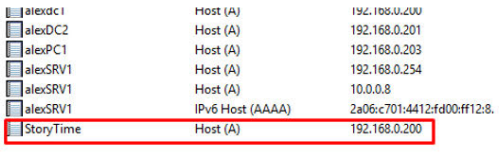
Here I will add a new Host for alexdc1 or 192.168.0.200



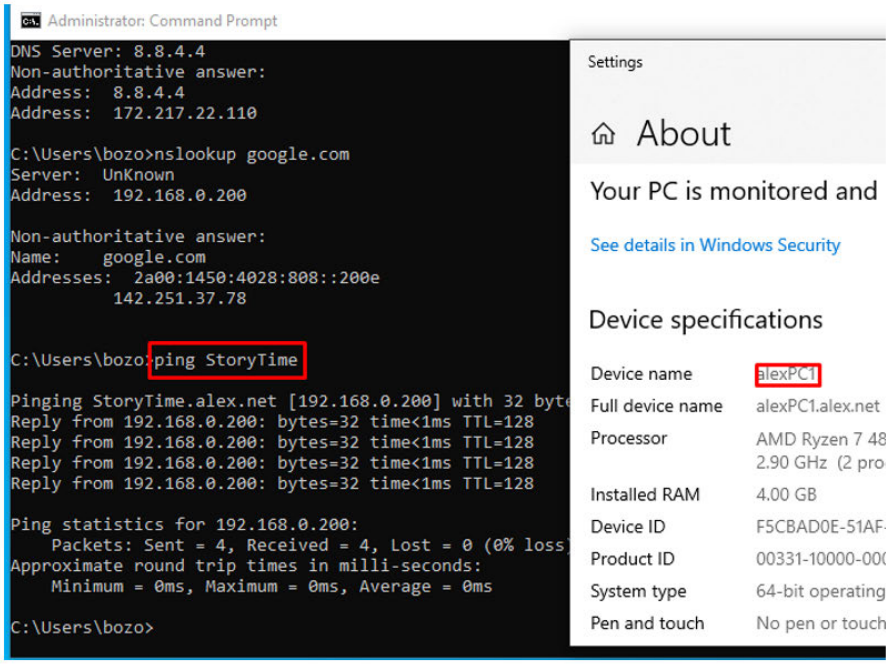
I will add a new host named StoryTime with the IP address of DC1 (192.168.0.200)



StoryTime is now a host



Now let's test on PC1 if it can reach "StoryTime" using the ping command

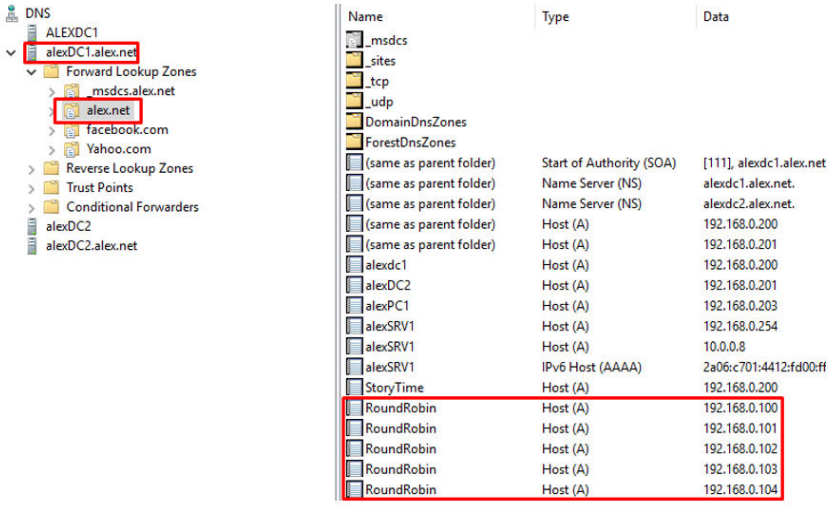


Ping is successful, DC1 can now be communicated with the CNAME StoryTime

Lasty in this part of DNS configurations I will create and test "Round Robin" to two addresses that forward to a random address

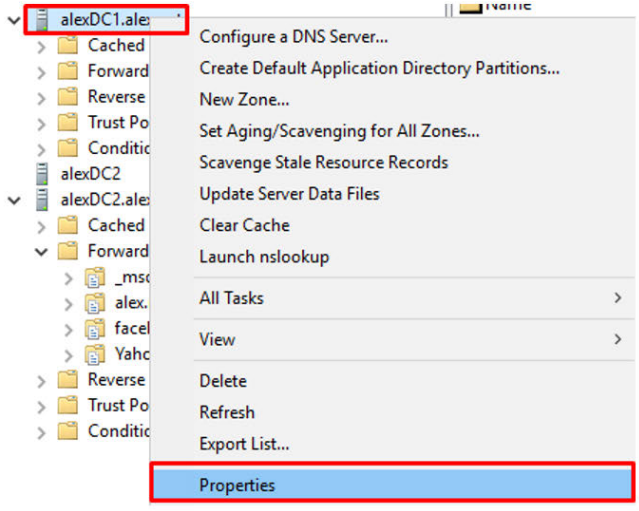
Round-robin is a DNS load balancing technique used to distribute requests among multiple servers in a rotating order. It is useful for achieving load distribution, preventing a single server from becoming a bottleneck, and improving overall system performance. Round-robin is typically employed when you want to distribute incoming network traffic evenly across multiple servers to optimize resource utilization and ensure high availability.

I'll start with creating 5 "AHost" entries in alex.net in DNS manager, I'll name them RoundRobin

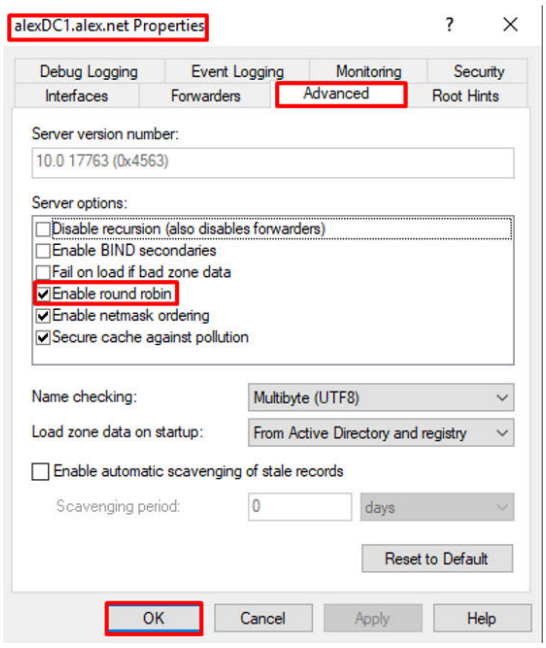


Now before we'll do the actual test with PC1, I'll need to check that RoundRobin is enabled

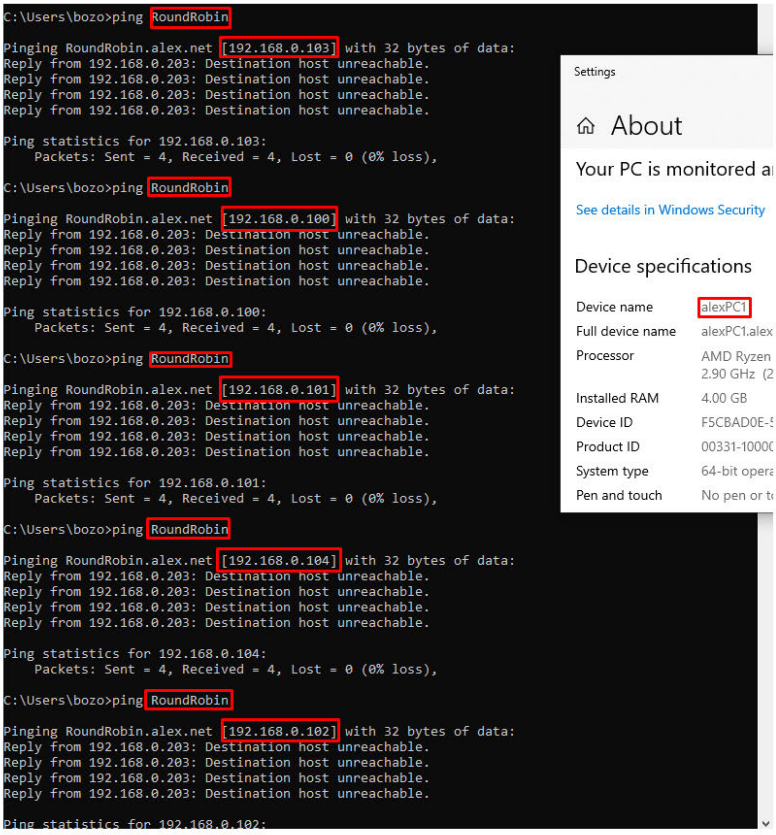
Go to Properties of DC1



Here we can see that RoundRobin is enabled which means that PC1 should get a different IP address each time it sends a ping to RoundRobin, in a rotation that load balances



I will be using PC1 (WIN10) to ping RoundRobin 5 times
it should rotate perfectly with a different IP address on each attempt



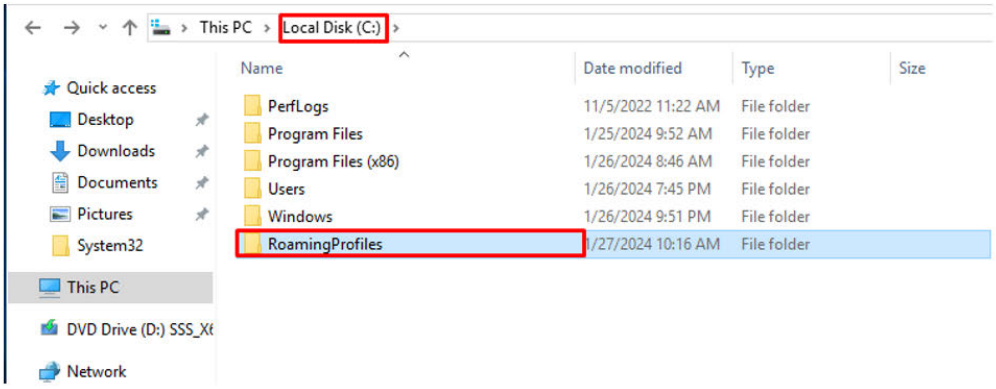
Round Robin is working properly, the rotations are providing load balancing

Part 8 - User Profile

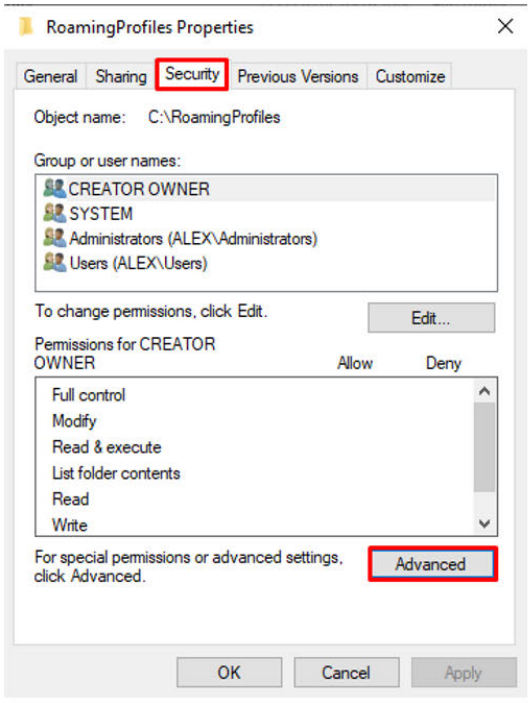
User profiles in Active Directory store personalized settings and configurations for individual users. They integrate with user accounts, providing consistency and security by enforcing policies, permissions, and restrictions. User profiles support mobility, allowing users to access their settings from any computer within the network.

Roaming Profiles: Enable users to access personalized settings on any network computer.
Mandatory Profiles: Provide a consistent, unmodifiable desktop experience for users.

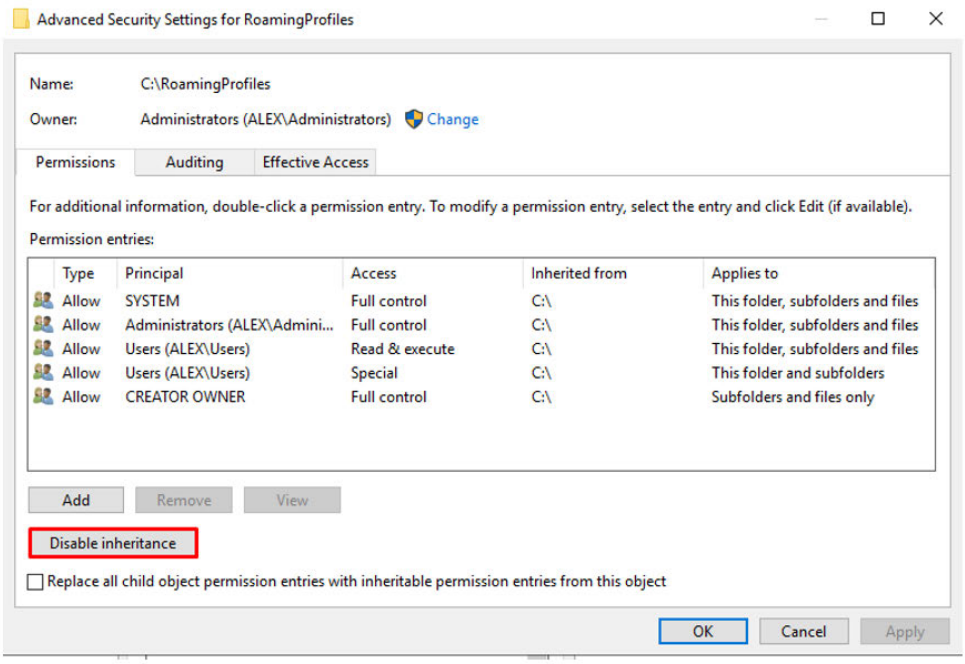
I'll start by creating a Roaming user profile to an account we have created in previous configurations
First, to create a roaming user profile I'll need to create a folder in DC1, I'll name it "RoamingProfiles"



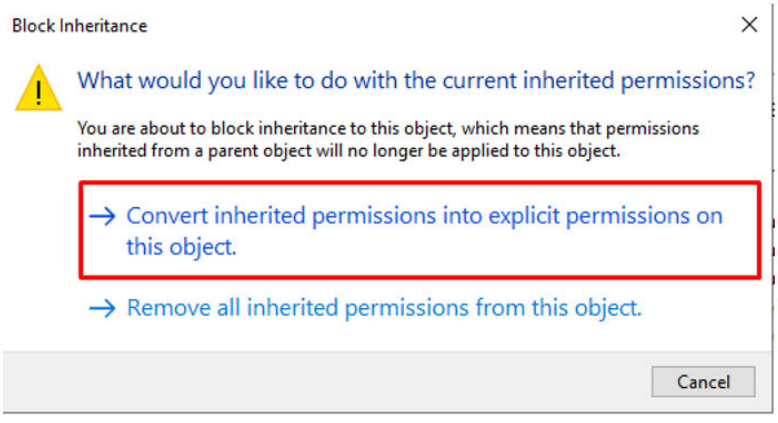
Now I will go to Security/Advanced on the RoamingProfiles folder



I will disable inheritance



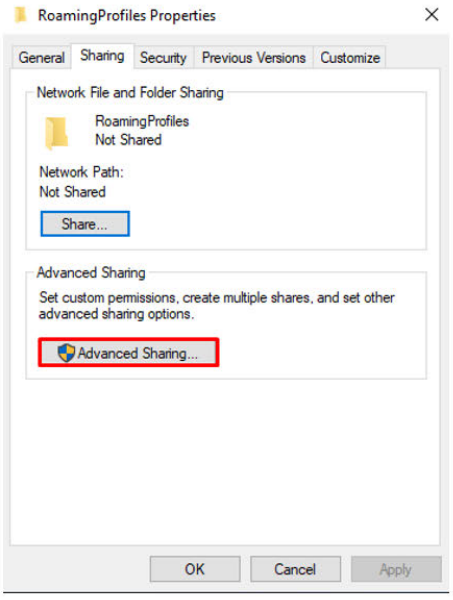
Disabling inheritance when creating roaming profiles ensures customized folder permissions improving security and access control.



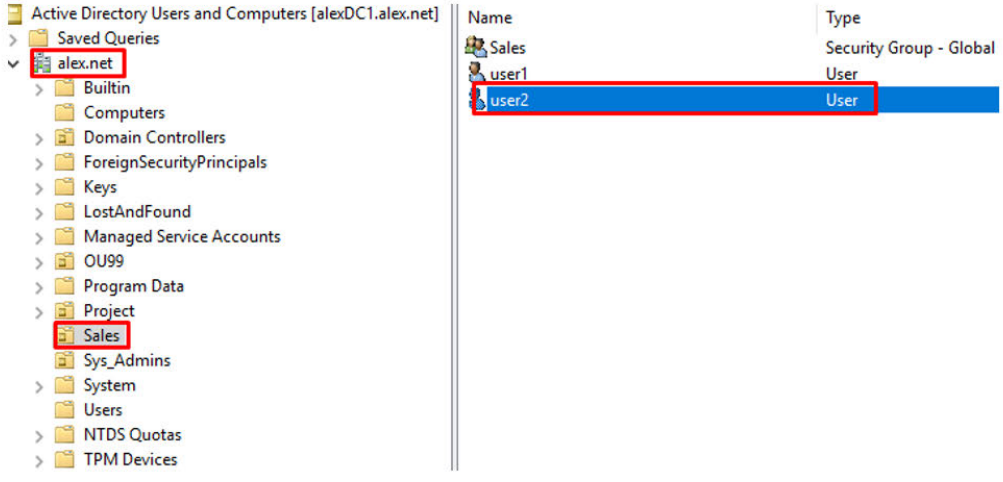
We can see that now it's changed to "Inherited from none"

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (ALEX\Admini...	Full control	None	This folder, subfolders and files
Allow	Users (ALEX\Users)	Read & execute	None	This folder, subfolders and files
Allow	Users (ALEX\Users)	Special	None	This folder and subfolders
Allow	CREATOR OWNER	Full control	None	Subfolders and files only

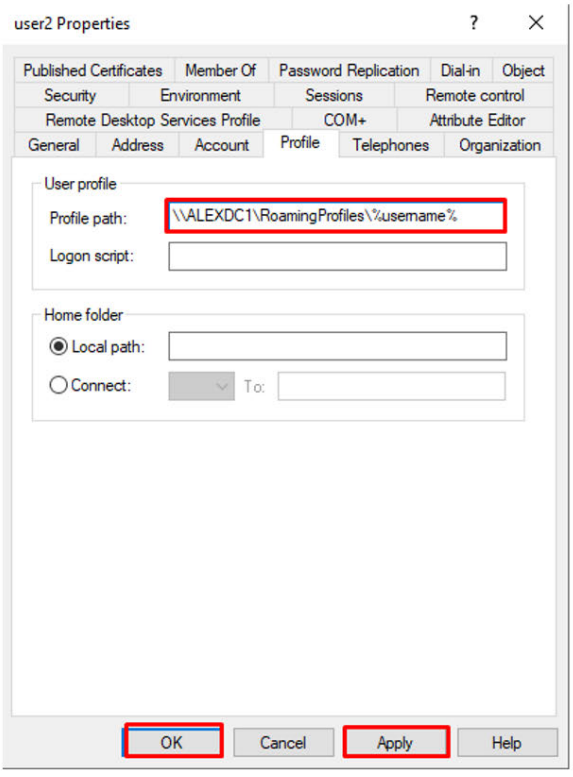
I will also share the folder, a roaming profile folder needs to be shared for seamless access across computers in a local network.



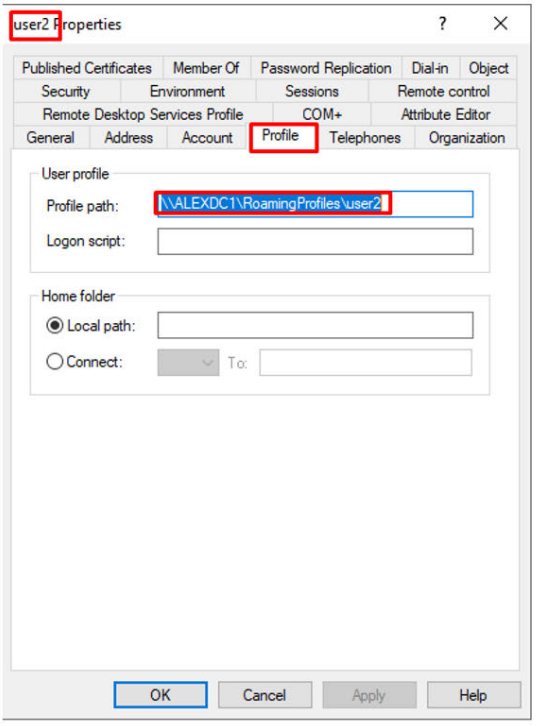
The next stage is configuring the Path to the user profile that I want to be a roaming profile, I will go into Active directory user & computer manager & than I'll select user 2 from the Sales OU



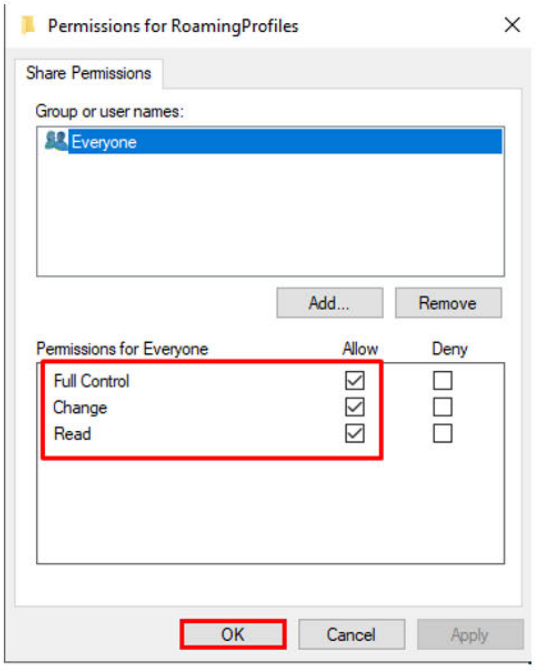
The next step is to paste the path of the folder to the user for whom I want to have a roaming profile. I will set up "user2" as the roaming profile, write the path of the folder I created earlier, and add "%username%" so that each user receives a folder with their name automatically.



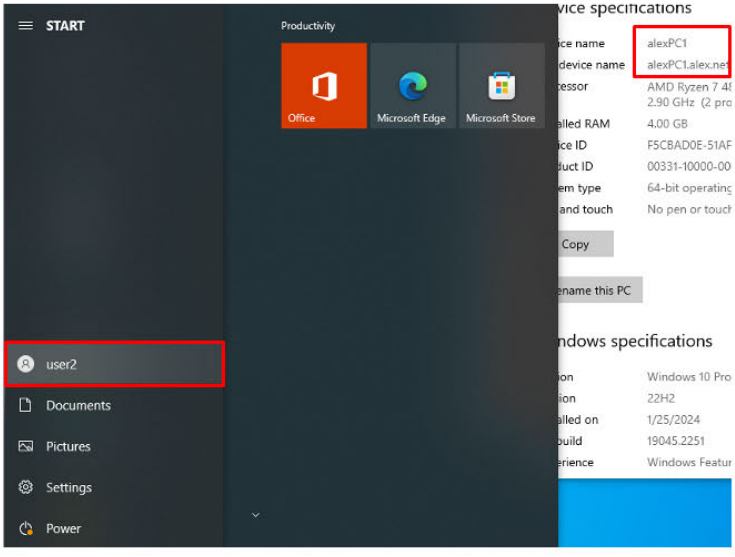
Now that I provided a path to the roaming folder you can see the username changing to user 2 after I click apply because it is updating from the DNS database



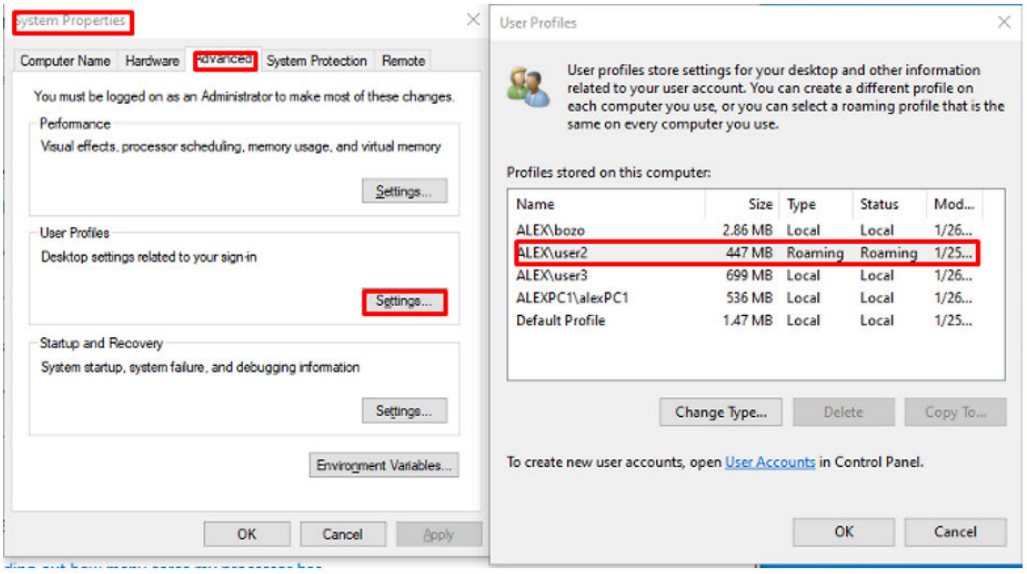
I will also give Permissions of full control to Everyone for the RoamingProfiles folder



I will now test to see if user2 is a roaming profile by logging in to PC1

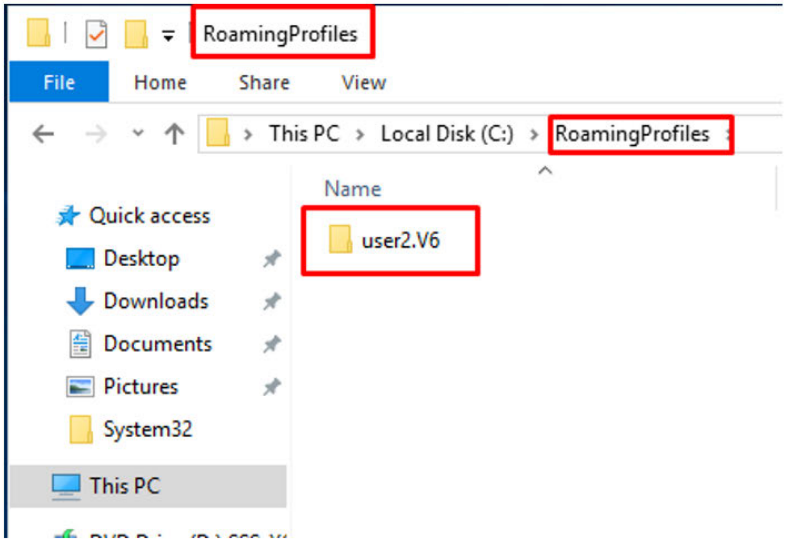


User2 was able to login in to PC1



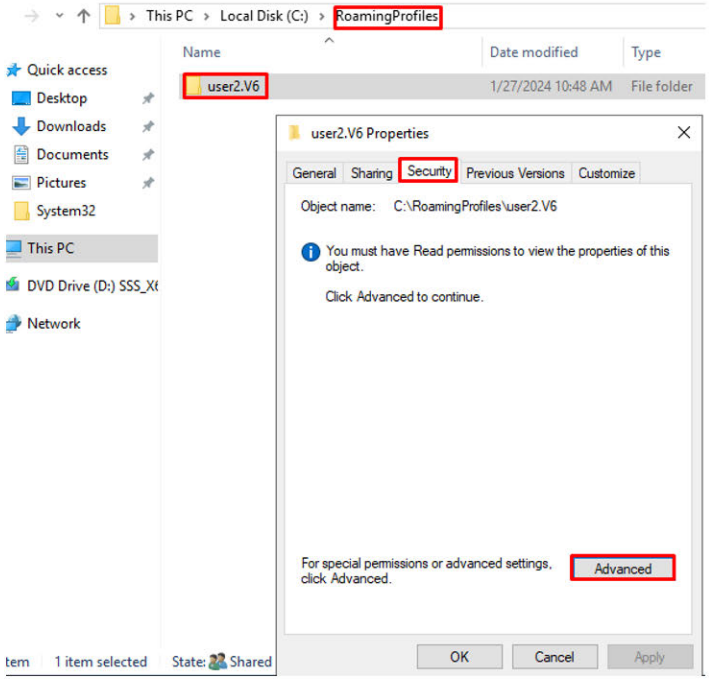
In the Advanced System Properties user profile settings we can also see that user2 has the roaming status

Additionally we can now see on DC1 that a new folder for user2 have been automatically created showing its working

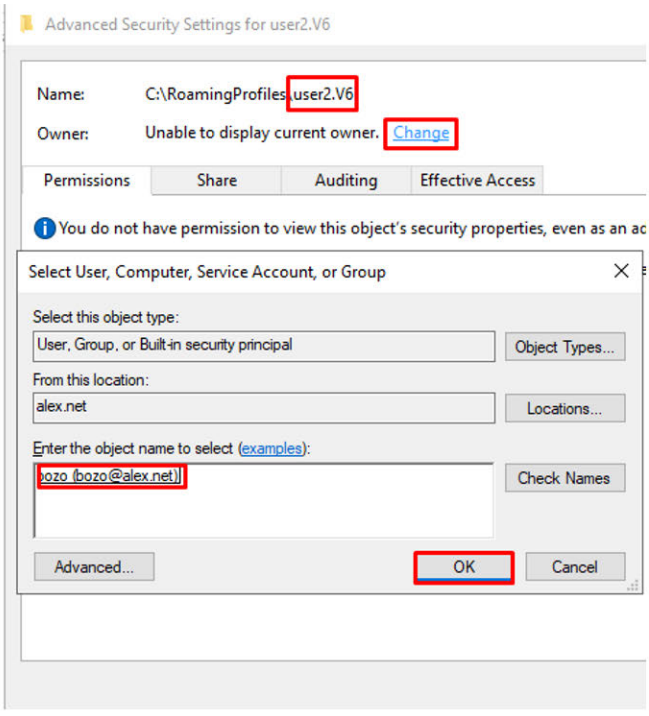


Next step I will give the domain admin the privileges to use users2 roaming profile,
I'll change the settings so that the network administrator can access the profile folder on the server (Domain Admin) > Verify that you can indeed log in with the profile after the changes made in the profile folder on the server > Through the Domain Admin

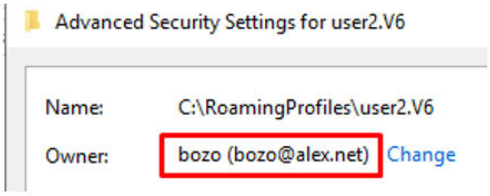
I'll also change the owner of the user2.V6 folder inside the RoamingFolder from user2 to Bozo, who is the Domain Admin. Now, Bozo can access the folder and is responsible for its sharing settings and permissions. After this change, the user user2 won't be able to access the folder, so grant user user2 access to the folder as well.



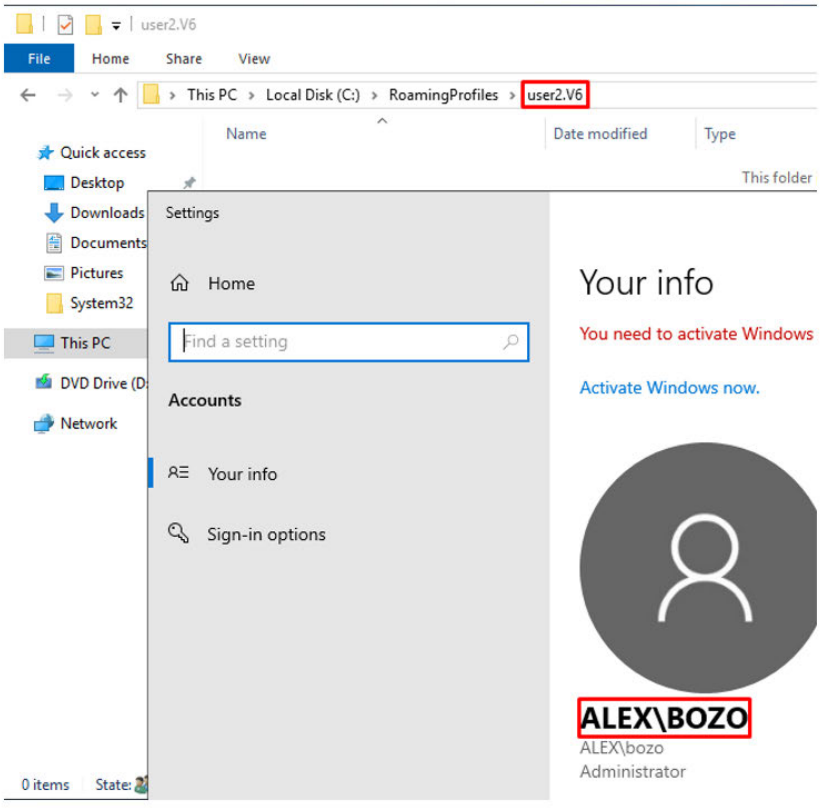
Will give ownership to the domain admin



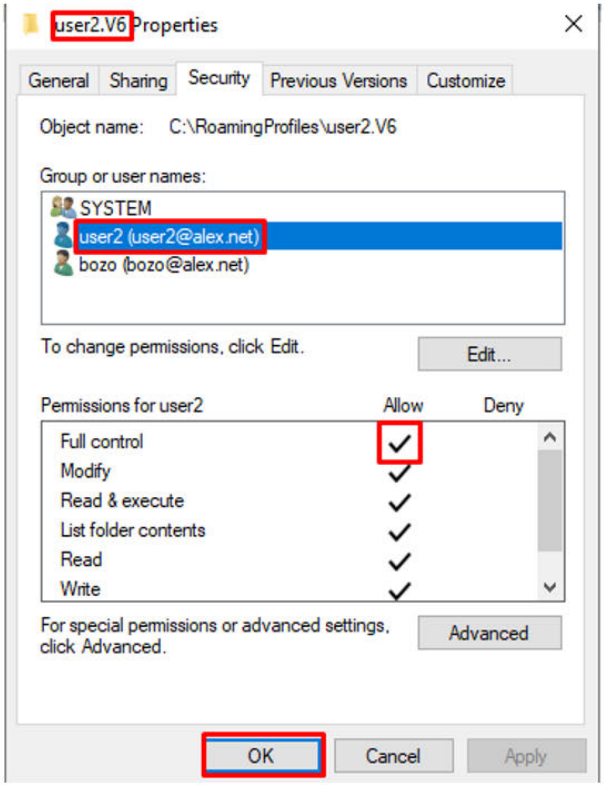
The owner is now the domain admin, mr bozo



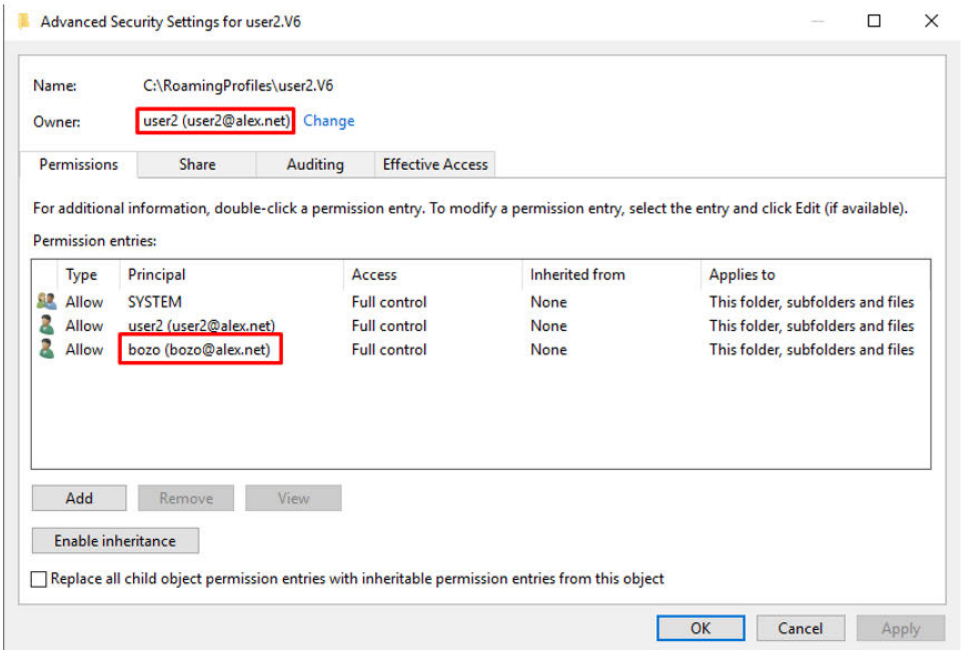
Bozo is able to get inside the folder of user2.V6



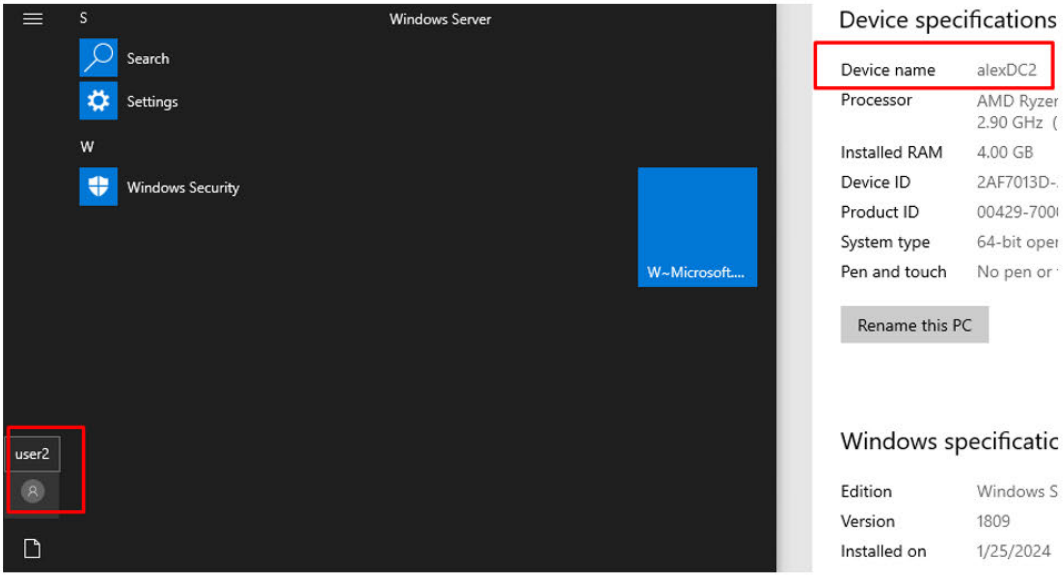
Will make sure that user2 still has permissions and access to his folder



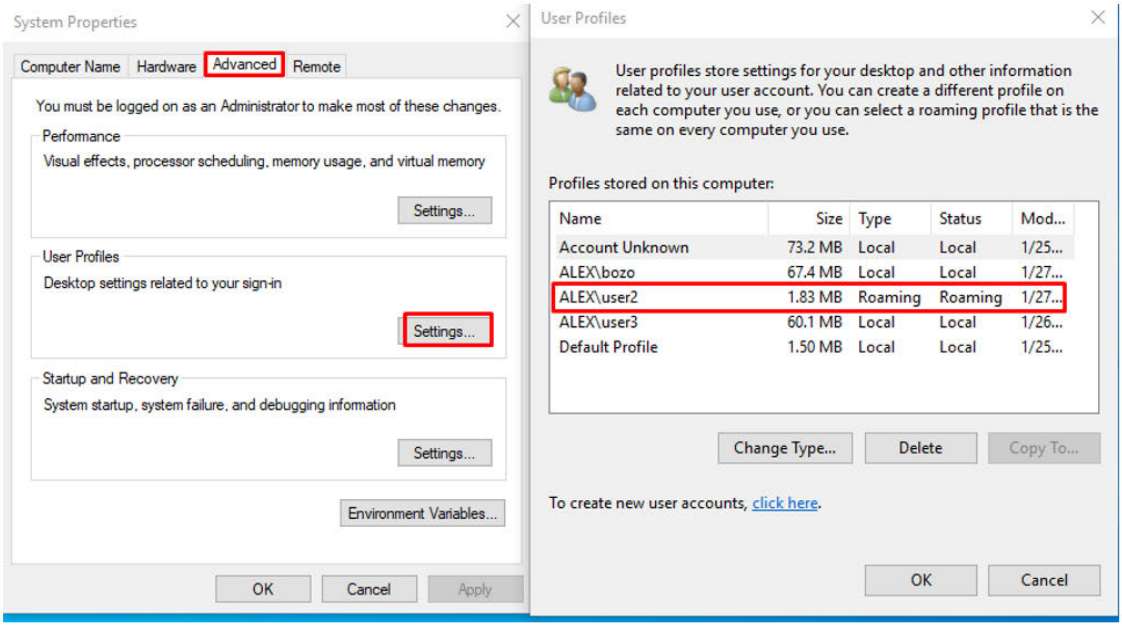
After bozo getting permissions, we gave the ownership back to user2



Now I'll check if user2 is still a roaming profile and working properly after the changes
This time I will use DC2 to check & not PC1, I'll login with user2 to DC2.



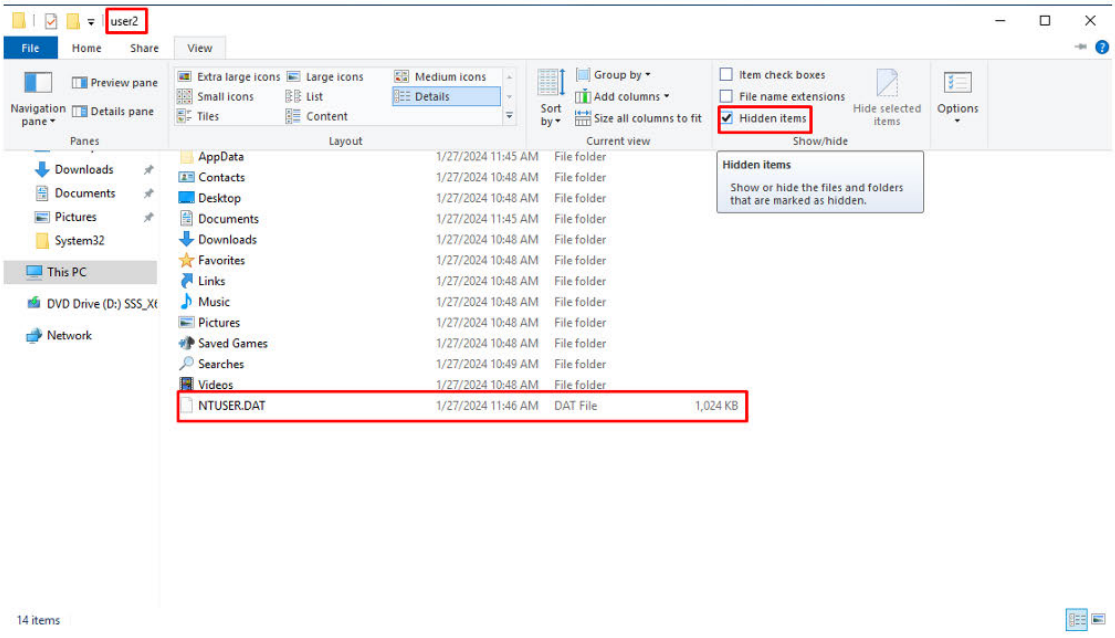
User2 is able to login to DC2, now let's verify if it's a roaming profile



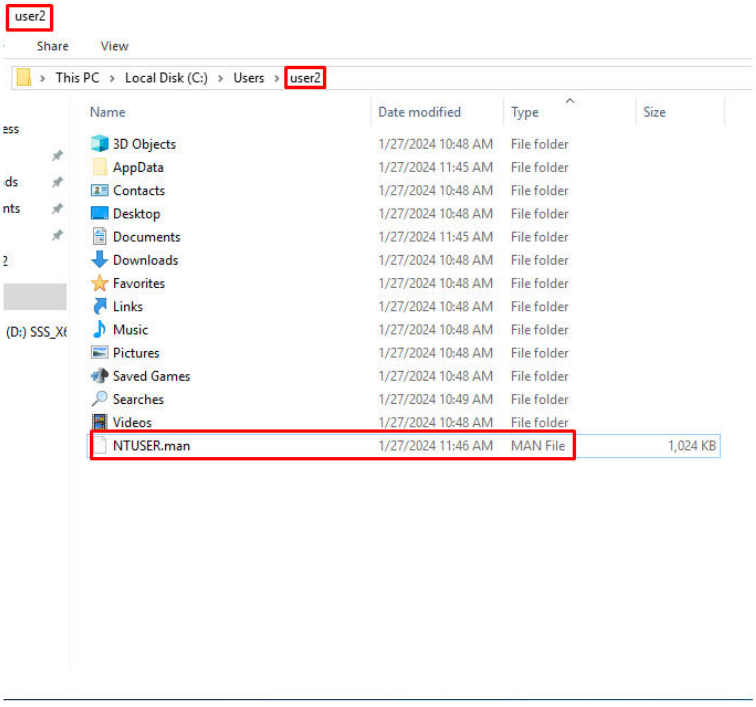
User2 is still a roaming profile and works properly after the changes

In the next step I will change user2 into a mandatory profile, Mandatory profiles make sure everyone sees the same desktop setup every time they log in. They're like a set template for a no-changing desktop experience, useful for keeping things simple and controlled.

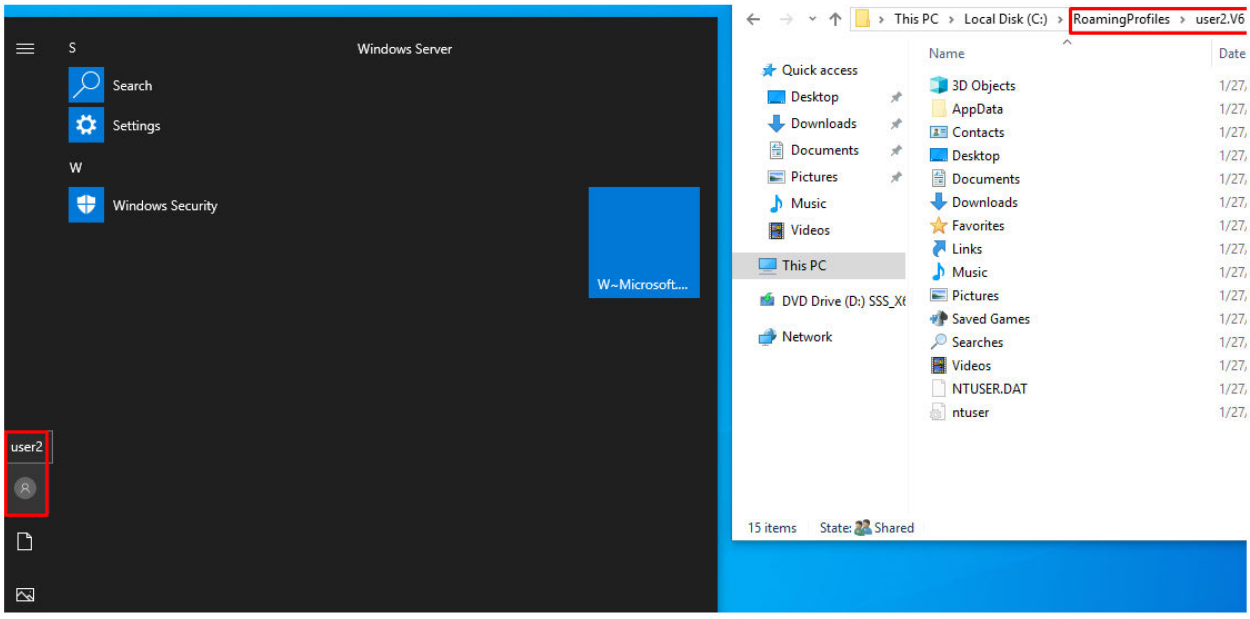
I'll Log in through the user Bozo, and change the file extension of user2 NTuser.DAT to .MAN. Which will make it Mandatory



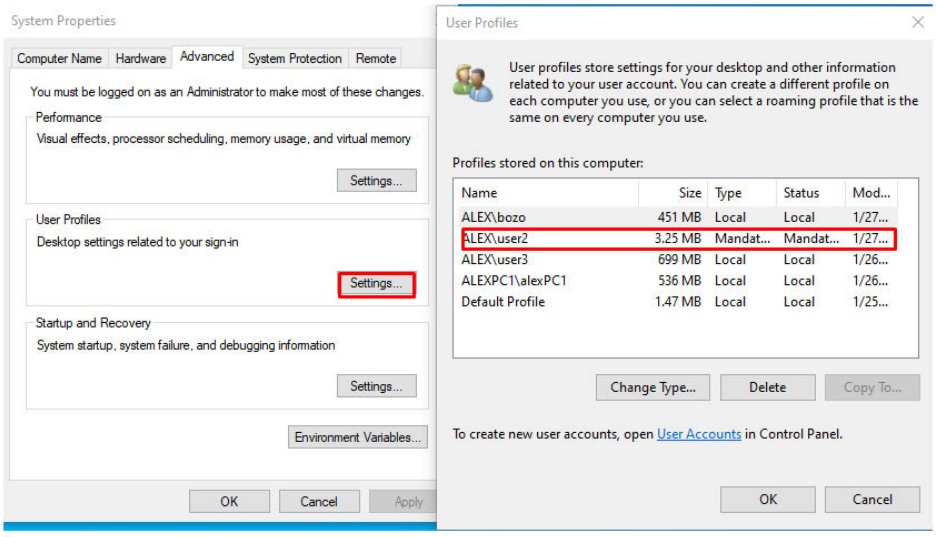
Now we change it to a .MAN file



User2 still has access to his folder after the changes



We can also see here that user2 is a mandatory profile now

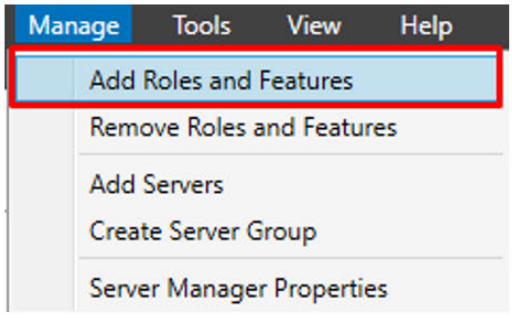


Part 9 - File Server Mapping & Sharing

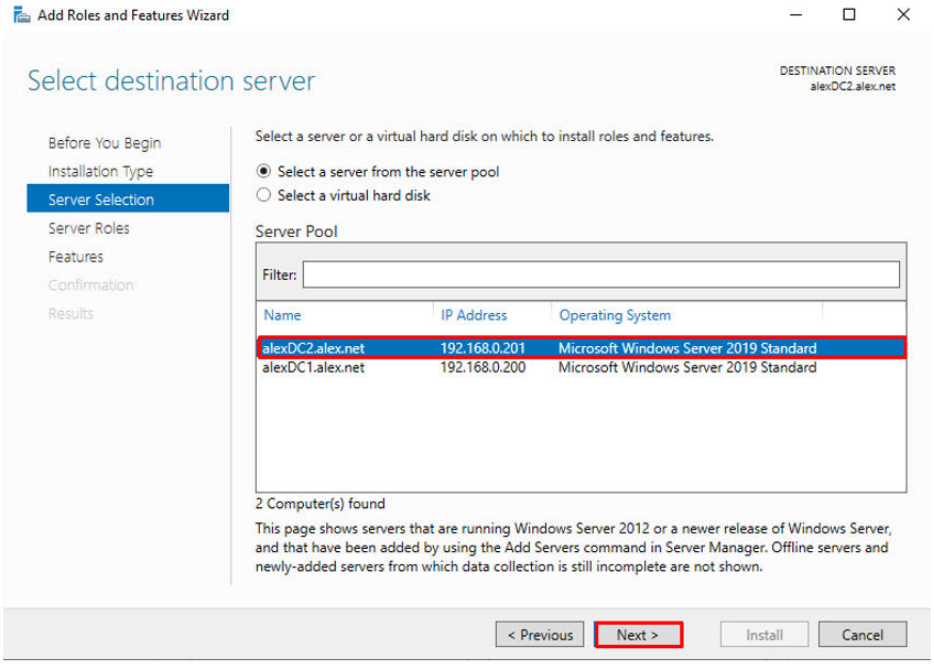
File Server Mapping and Sharing in networks offer centralized data storage, access control, enhanced security, collaboration support, simplified backup, resource optimization, and scalability. They are essential for efficient file management and collaborative work in networked environments.

A File Server in a network is like a boss for files. It keeps all the files in one place, controls who can access what, makes it easy for people to work together on files, and ensures that files stay safe and can be found even if something goes wrong. It's like the go-to guy for handling files in a group.

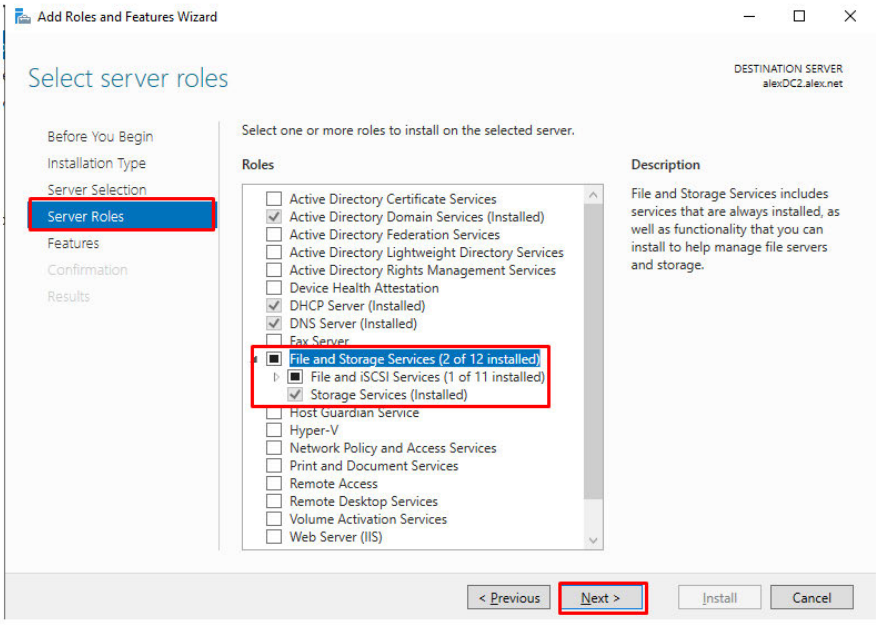
First I will begin with installing the File Server role on DC2



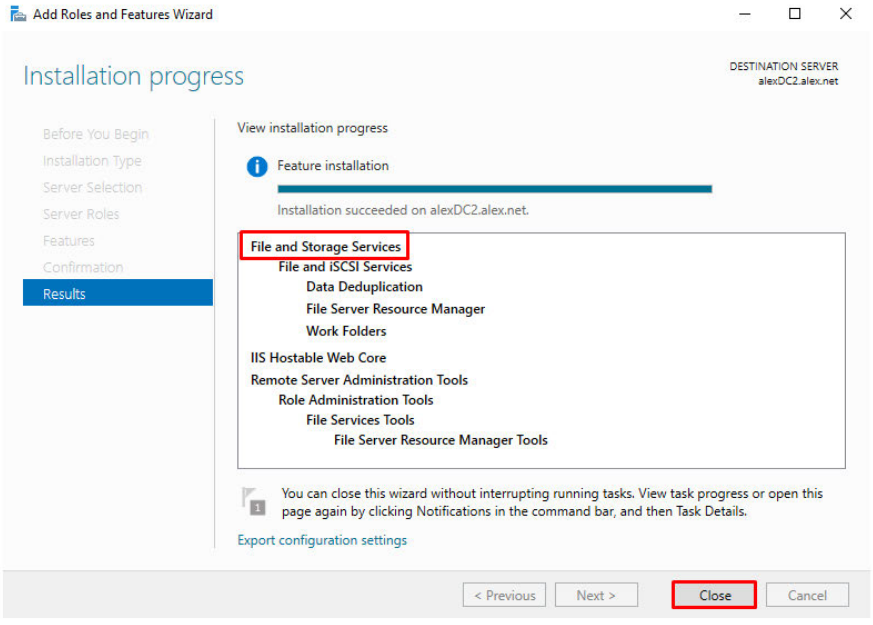
I'll select DC2 for the fileserver role



I'll select the File and Storage services role



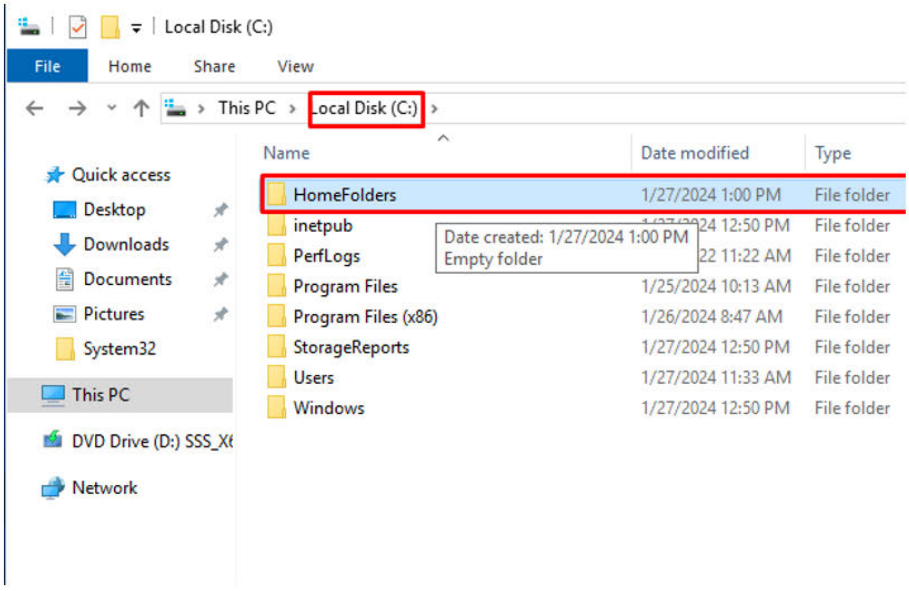
The role is now installed on DC2



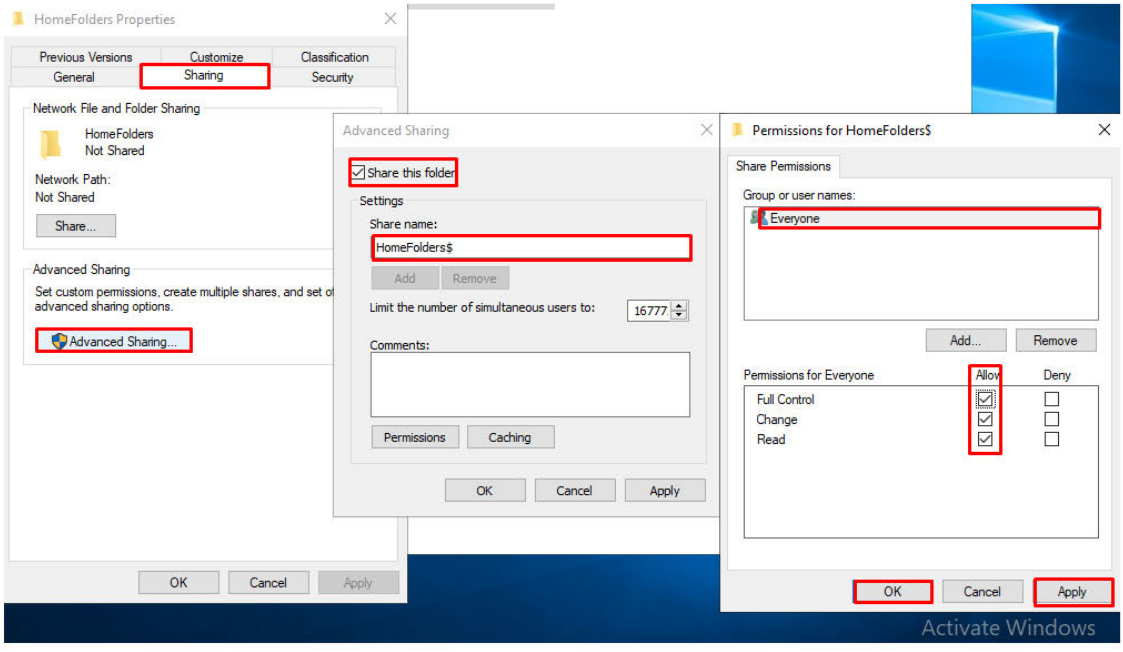
Next step is configuring an Home Folder for 5 users, I will also make sure that each user can only access his specific home folder.

Home folders are like personal lockers on a computer. They keep your stuff safe and make sure only you can access it. It helps organize your things, allows you to make your computer look and feel the way you want, and keeps everything in one place. Plus, if something goes wrong with your computer, your important stuff is backed up and can be easily fixed.

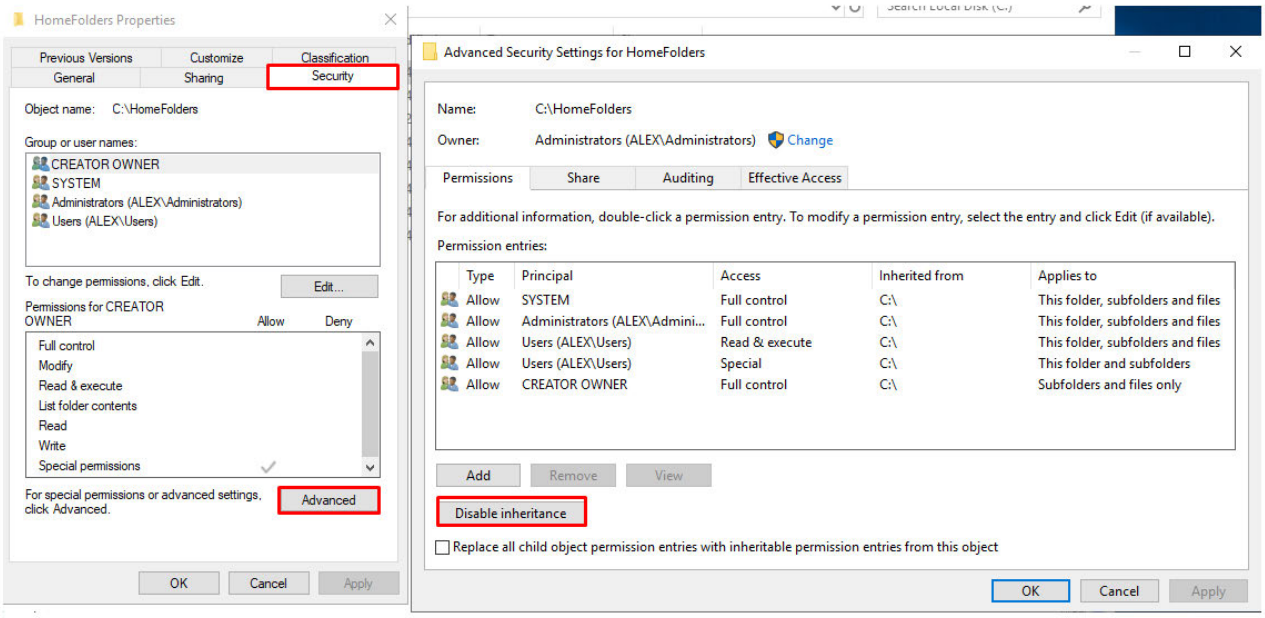
First step is creating a folder named "Home Folders" in DC2



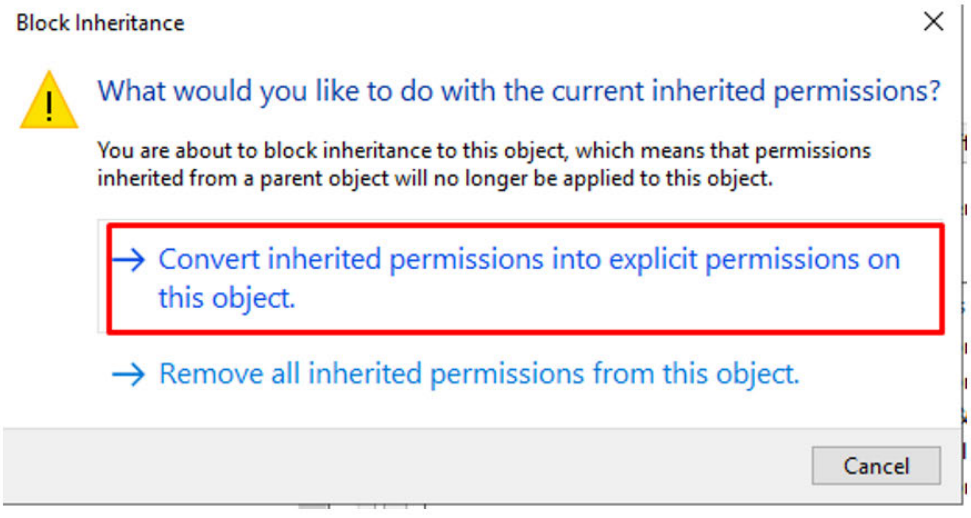
Going to the Sharing option on homefolders, I'm going to configure this folder that it can be used by everyone & I'm going to put a $ sign at the share name to make sure that users can't actually go to HomeFolder it self



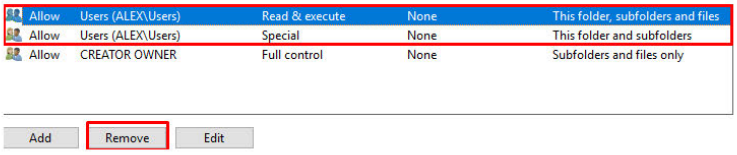
Next I will go to the security tab & click on the advanced option



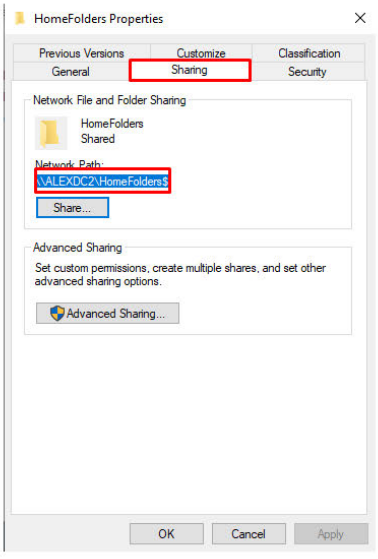
I will select Disable inheritance & click on Covert



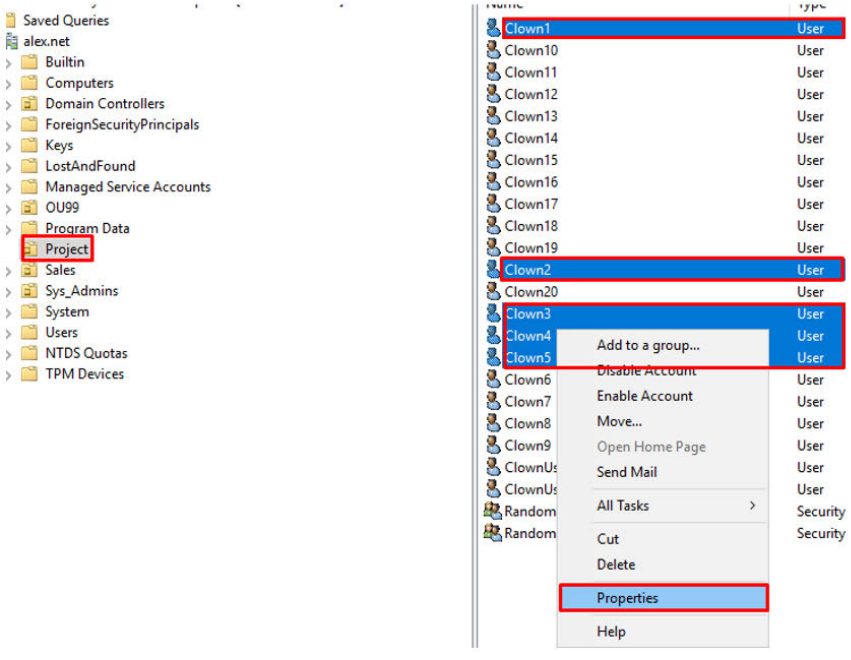
I will also remove both \User groups to avoid possible collisions & future issues



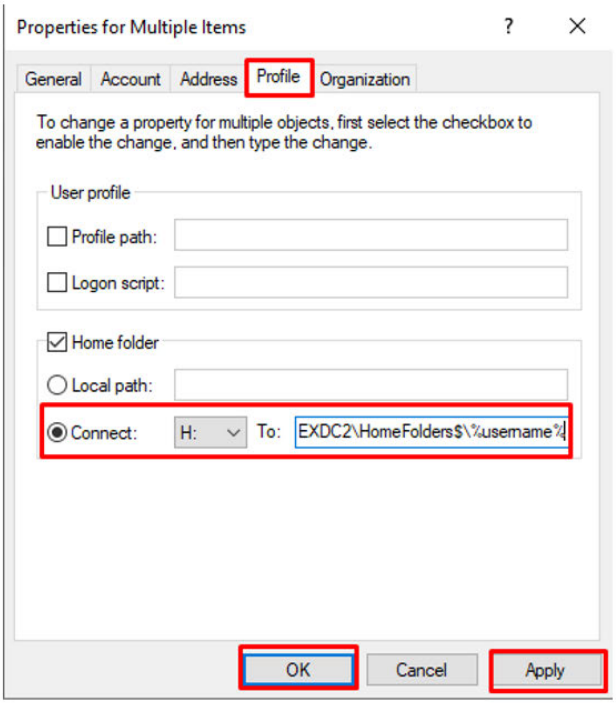
Now I will copy the folder path because I will need to for further user configurations



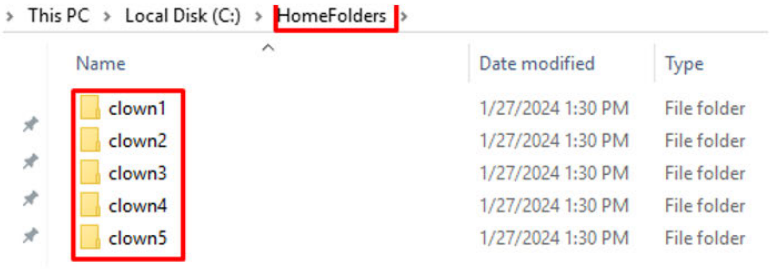
Now I will go to the active directory users & computers manager and select 5 users that will get an Home Folder
I'll select 5 users and give them all an Home Folder simultaneously



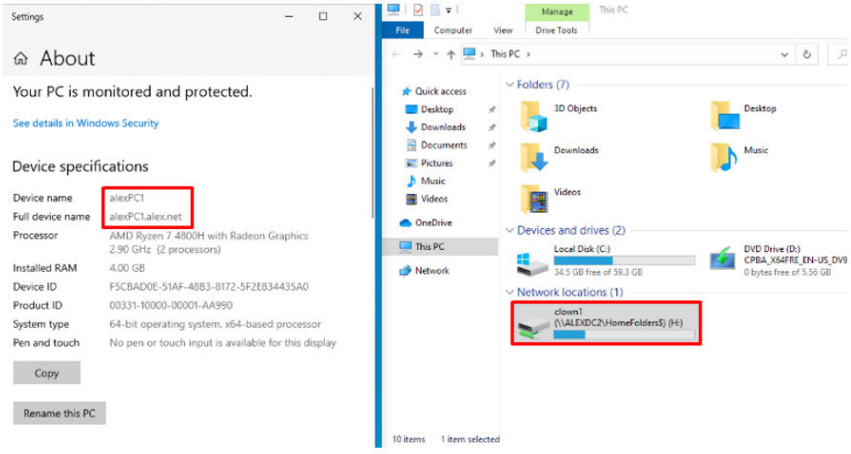
All 5 users will the H drive, I also added the %username% line at the end to give each user regardless of his username a Home Folder, after I click apply the username will turn into the login-name of each user



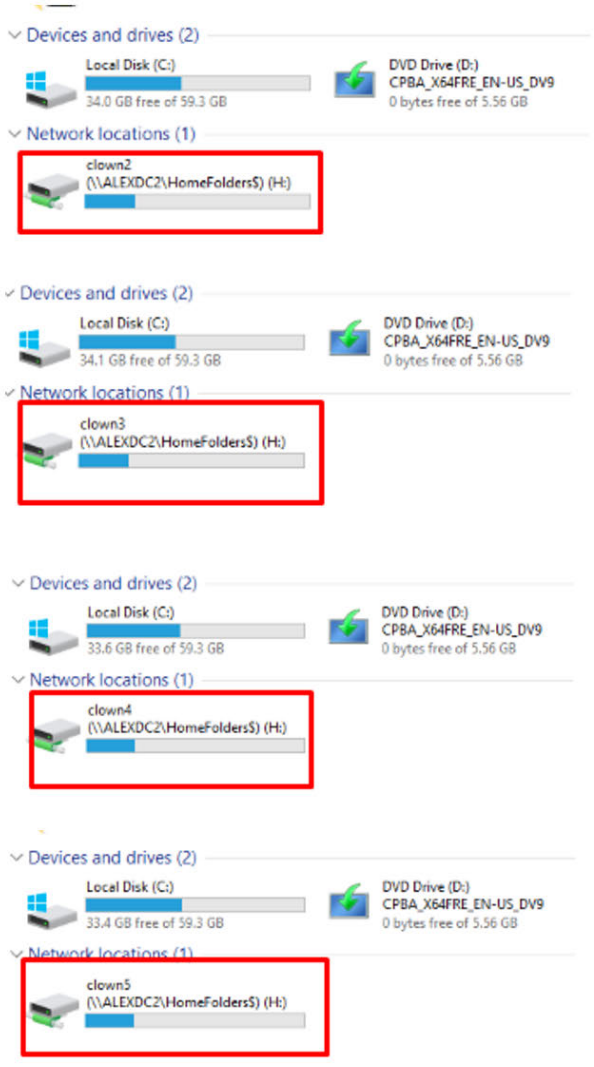
Here we can see that the 5 folders have been created after the previous action



Now I'll check if our 5 users can see only their folder from PC1
Starting with clown1



Yes, Now I'll do the same test for the other 4 users



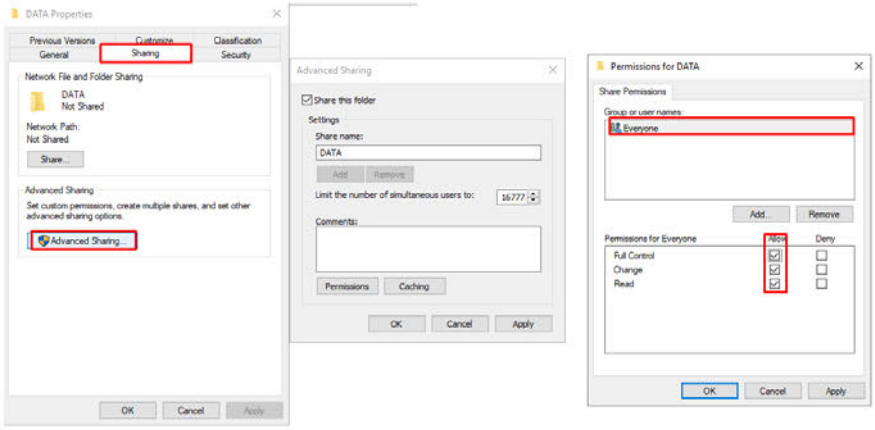
All 5 users are only seeing their own personal home folder from PC1 (WIN10)

Next step is folder sharing

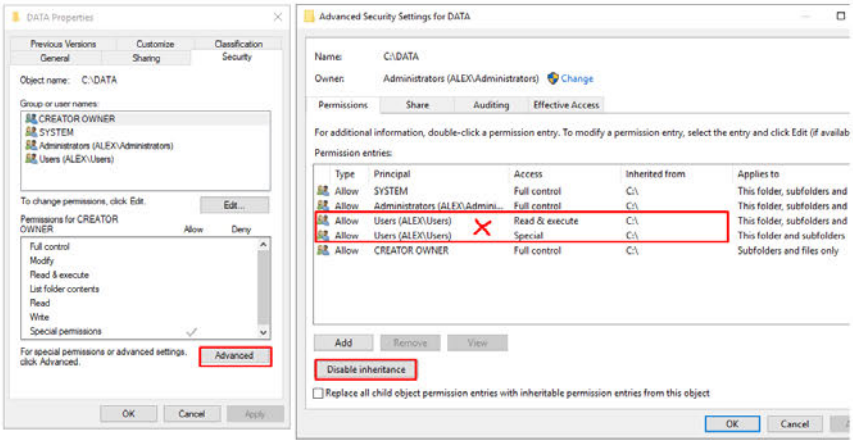
Folder sharing is a collaborative tool that allows multiple users to access, edit, and manage files in a centralized location. It enhances teamwork, ensures version control, and provides efficient access to the latest information. With features like access control and centralized storage, it's widely used in business collaboration, academic projects, file distribution, and remote work settings to streamline communication and improve overall efficiency.

I'll start by creating a folder in DC2 called DATA, inside that folder I will create an .txt file
I'll repeat a similar process I did before this with the creation of a shared folder configurations

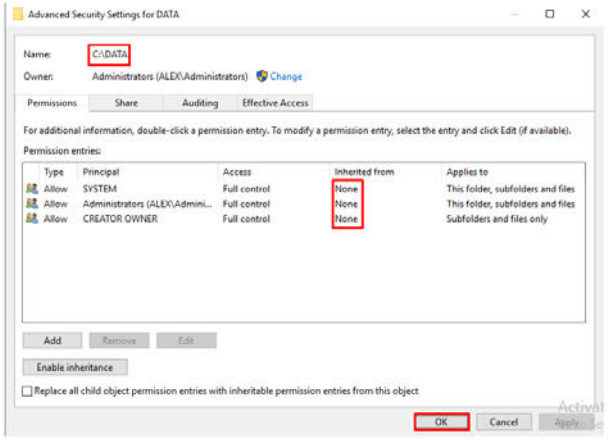
Same as before I'll allow everyone full control on this folder



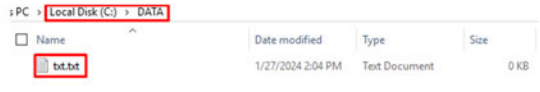
Again I will disable inheritance and remove both user groups from premissions



The basic configurations of the Shared folders are complete



Now I will create a .txt file inside the folder DATA in DC2



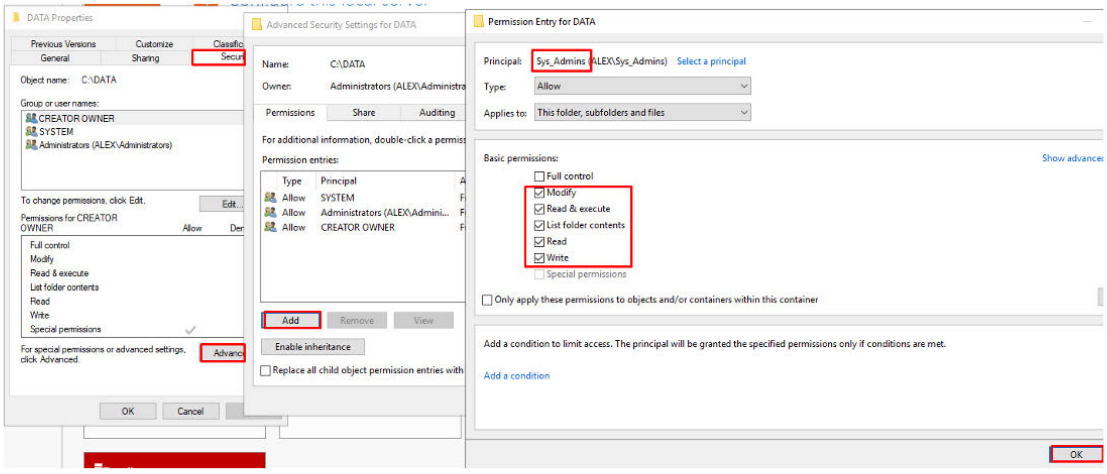
Next is permissions management

Permission management in network administration is vital for security, confidentiality, and resource optimization. It controls access, safeguards sensitive data, ensures compliance, maintains data integrity, and enhances network performance by allowing only authorized users to access specific resources based on their roles.

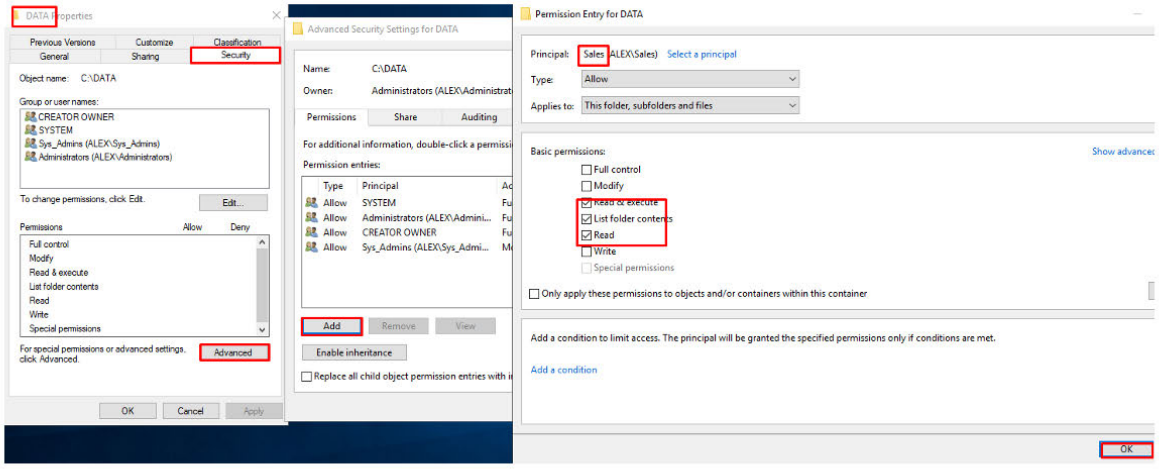
In this next part I will give the Sys_Admins group the modify permission

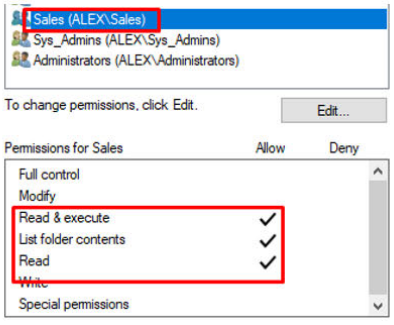
I'll also give the Sales group the Read & Execute permission

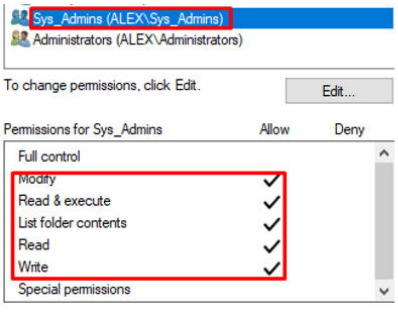
Here I'm giving the Sys_Admins the Modify permissions using the Advanced Security configuration on the DATA folder



I'll do the same with the Sales group, but I'll give them the Read & Execute permission only

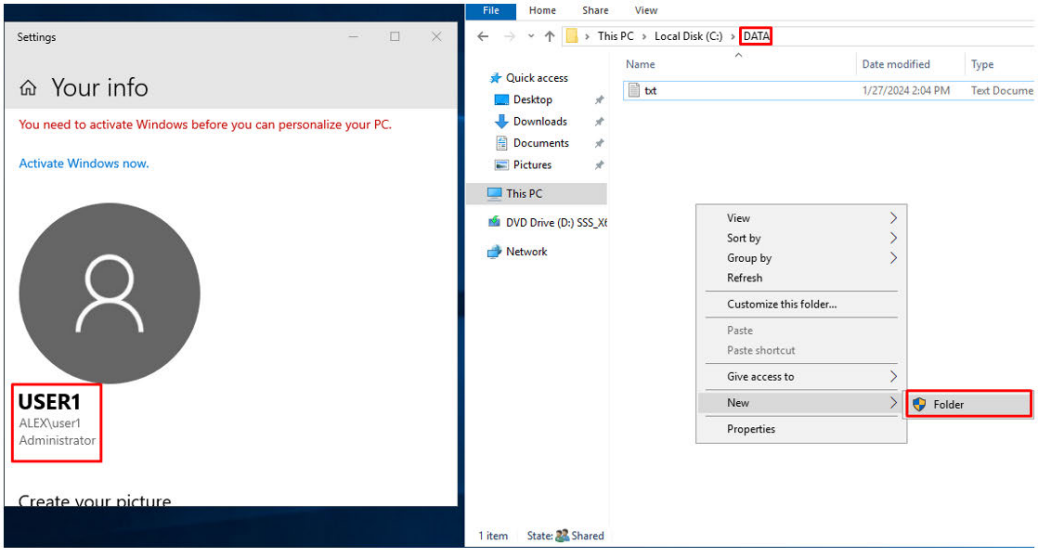


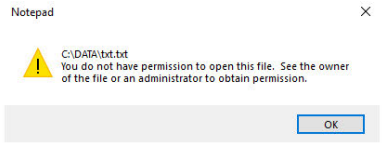




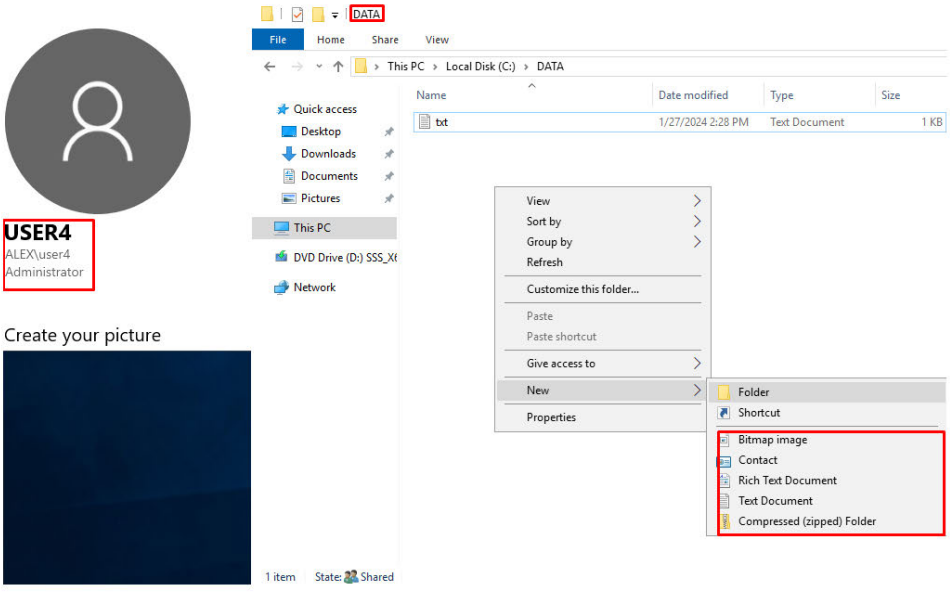
Now I'll check that user1 can only read & execute, compared to user4 that can modify (user1=sales, user4=Sys_Admins)

User1 permissions are working, he can only create a new folder and he can't modify the txt file





Now let's check user4 to compare

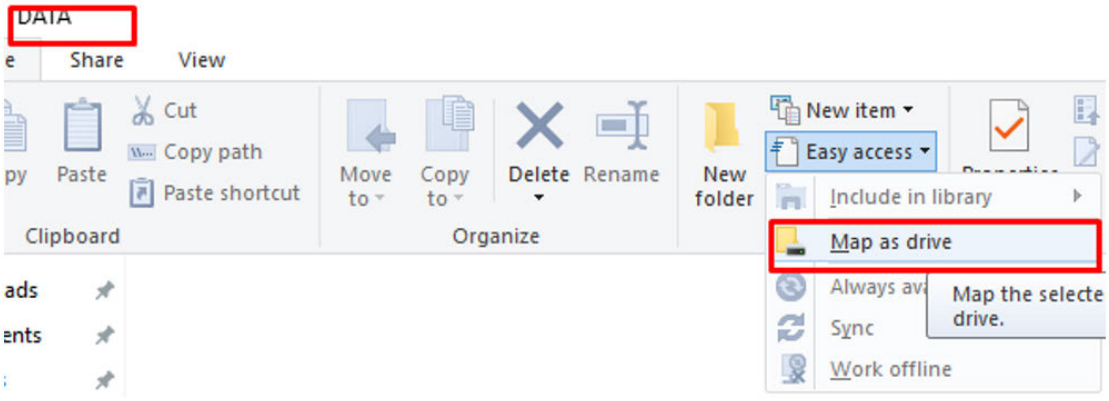


User 4 can edit and save the txt file, and he can create new documents, the permissions are working.

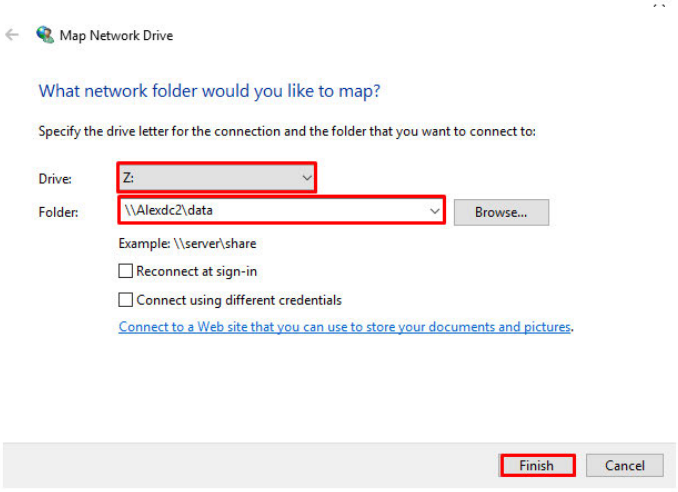
Drive mapping is useful for simplified access to network resources. It associates a network location with a drive letter, making it easier for users to navigate and work with files as if they were on a local drive. This method is employed to streamline file access, enhance user convenience, and facilitate collaboration, commonly used in networked environments for improved efficiency.

Now I'll map the folder as a drive

First I'll select the Map as drive option

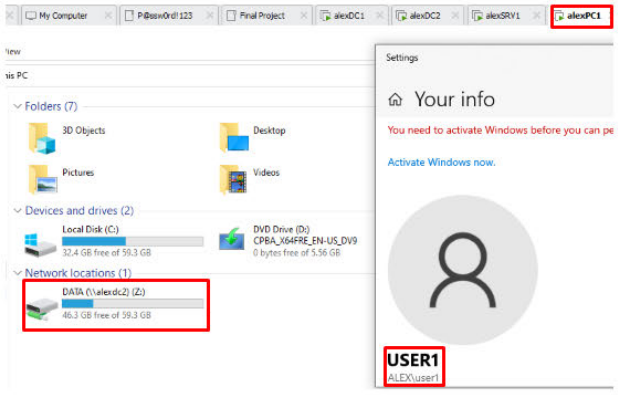


Now I'll select the proper path for the DATA folder on DC2, the drive letter will be Z

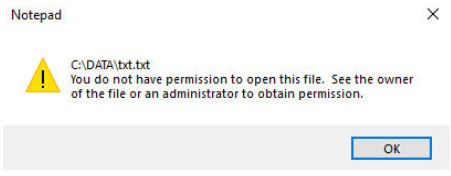


Now I'll connect from PC1 to see if the drive is visible and working properly for both the Sales & the Sys_Admins department

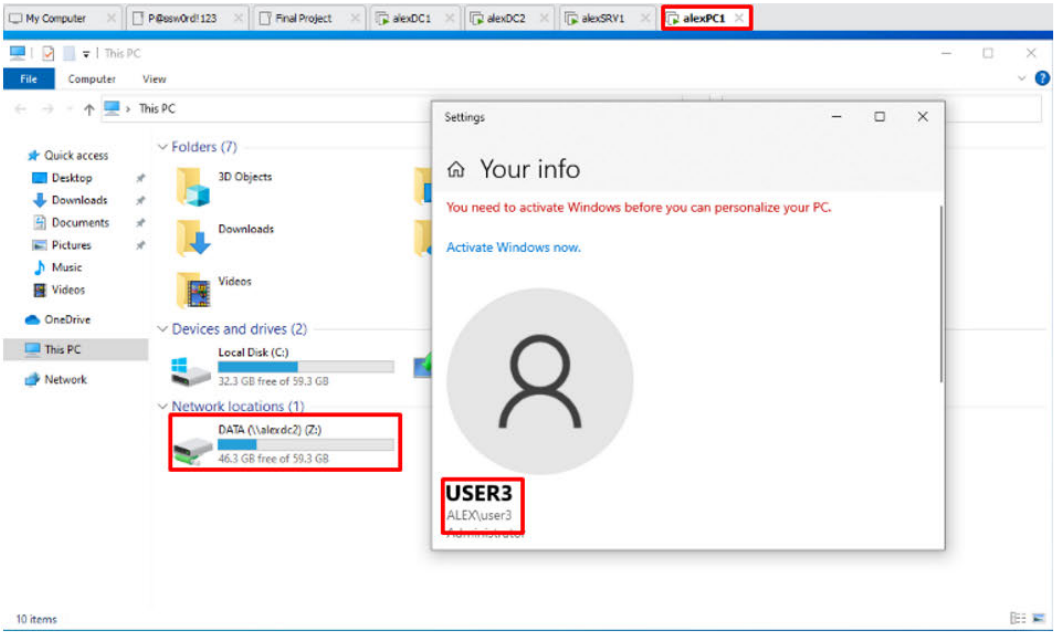
User1 is connected to PC1 & can see the DATA (Z) drive, his permissions are also working properly
User 1 is a part of the sales group



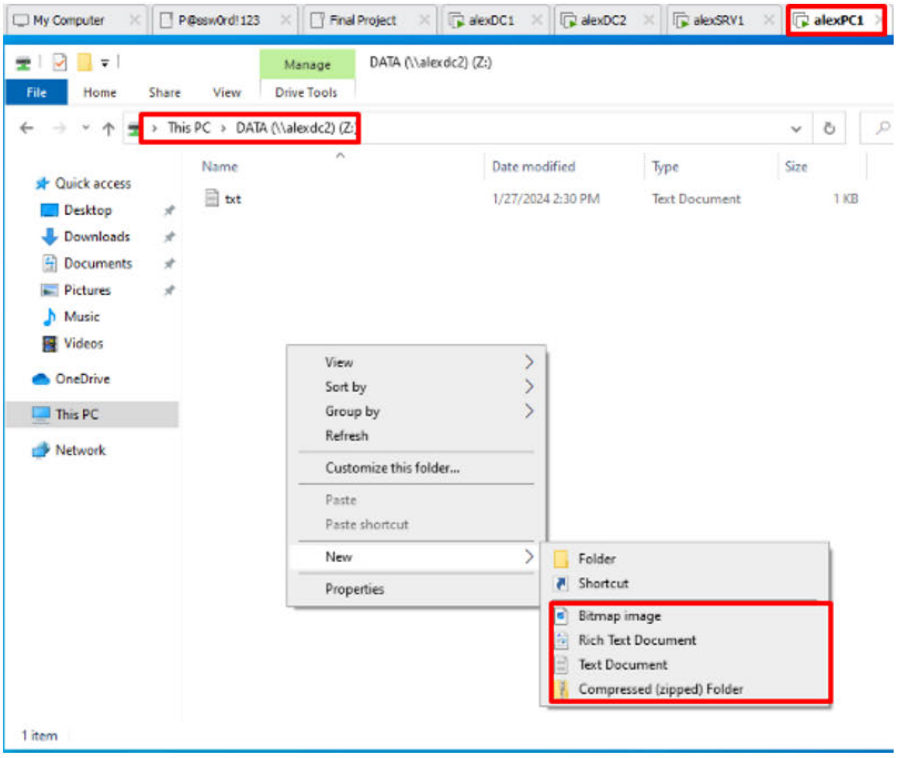
He still cannot save the txt file



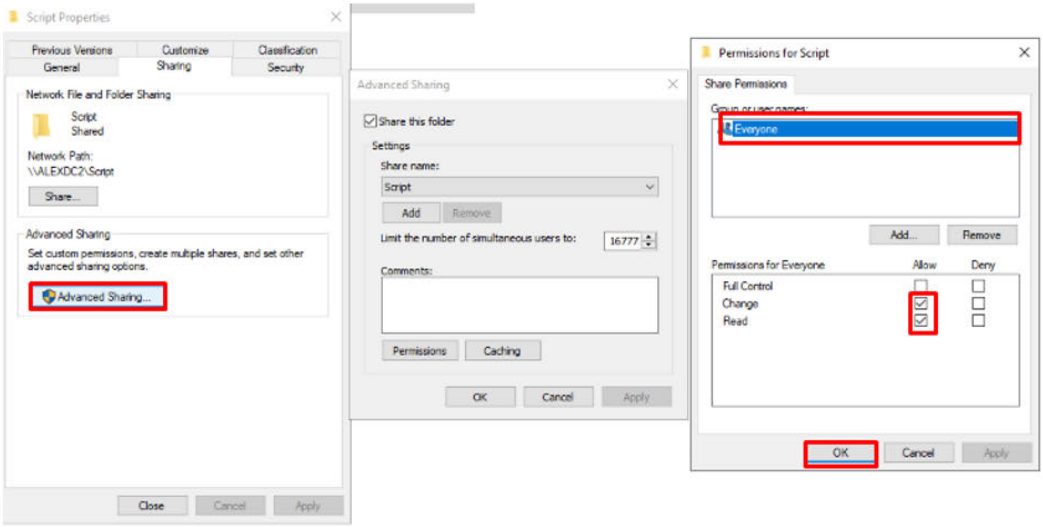
Now I'll try with user3 on PC1 (WIN10) user3 is a part of the sys_admins group



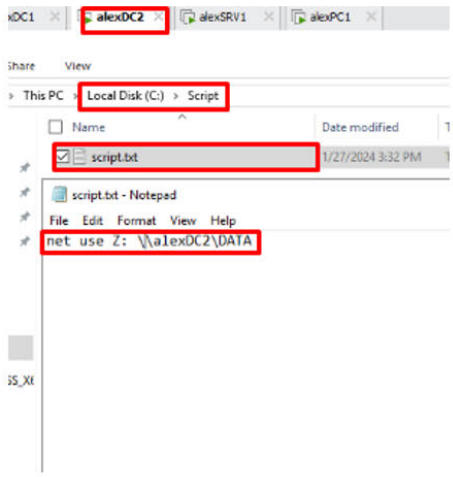
User3 can connect and use the DATA Z drive from PC1, he still has his permissions



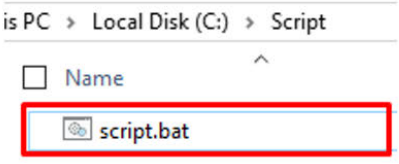
Next I will create another shared folder named Script, than I will a modify permission to the "everyone group"
I will repeat the exact same steps creating the last 2 shared folders on this project



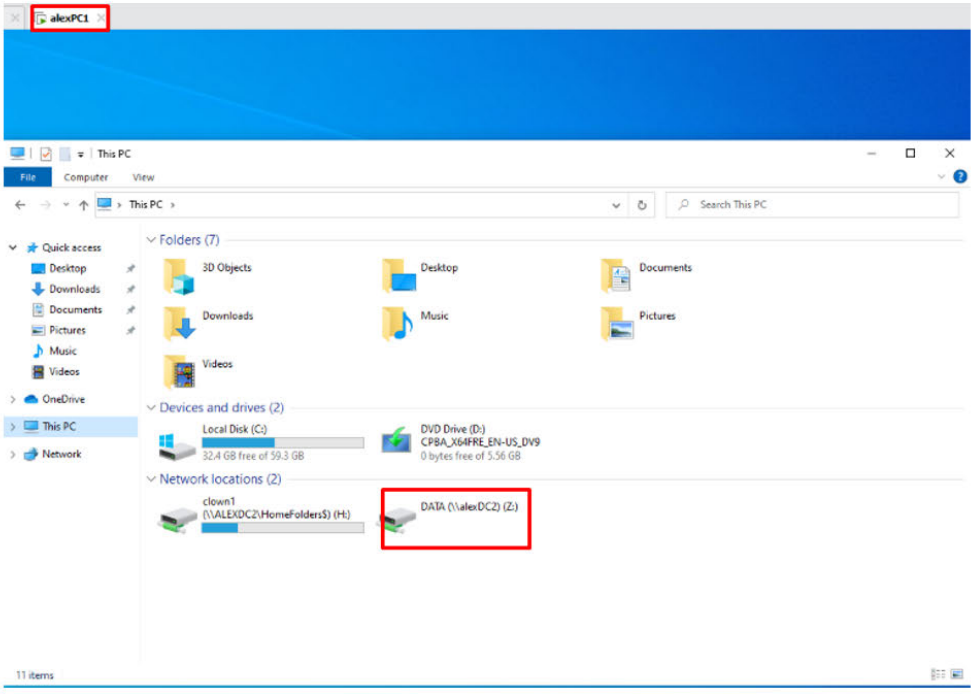
Next I will create the script inside the folder named Script, the script will make it easier for users to access the DATA folder



Now it's a script file after changing it to .bat from .txt



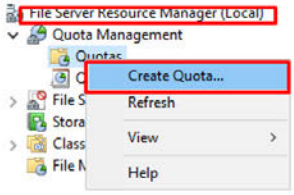
Let's test the script with a user and see if he gets a mapped drive
after running the script clown1 is able to see the DATA drive from PC1



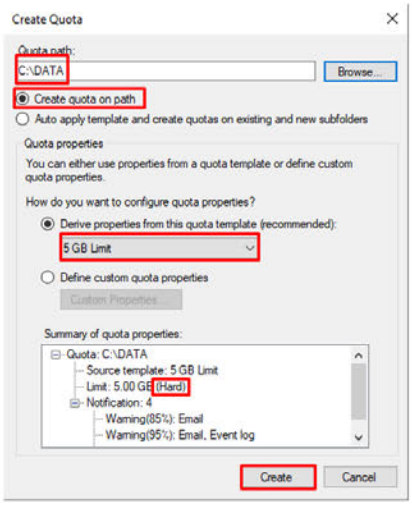
Next step I'm going to create a Quota on all the users of the Home Folder, the limit is going to be 5GB
I'm also going to prevent them from saving AVI files in these folders

Quotas are essential for managing folders and networks by preventing resource overuse, avoiding disk space exhaustion, enforcing fair usage, enhancing security, and ensuring compliance. They enable predictable planning, user accountability, and optimized system performance.

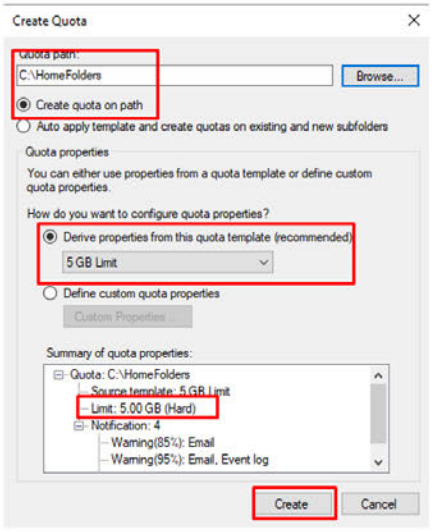
First I'm going to create a Quota in the file server resource management tool



Then I will apply the desired limit which is 5GB

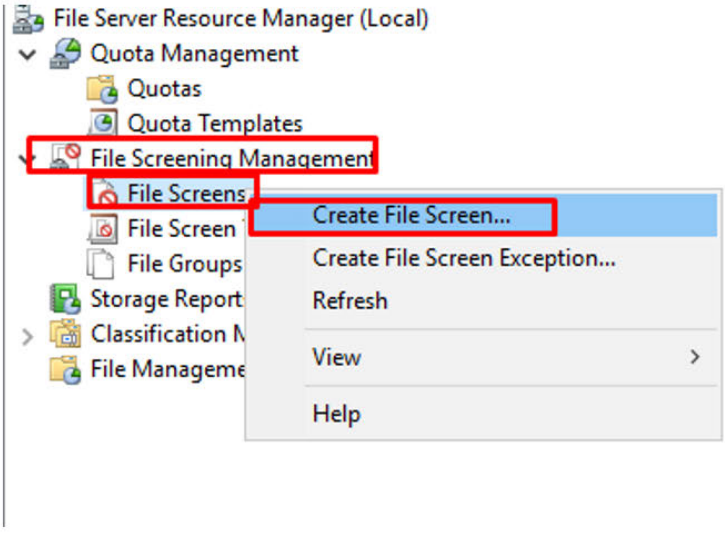


I have created a Quota for Home Folders with a 5GB hard limit using the file server management tool

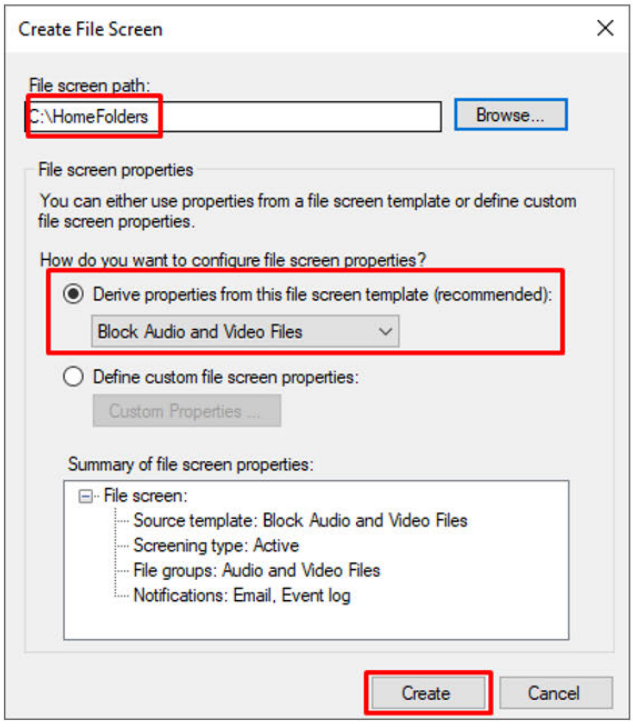


Next I will block the use of AVI files in these folders using the file server management tool

Creating a File Screen using the tool will allow me to block certain types of files



This will block AVI files from being used or saved inside the Home Folders location



Part 10 - Hardening Stations

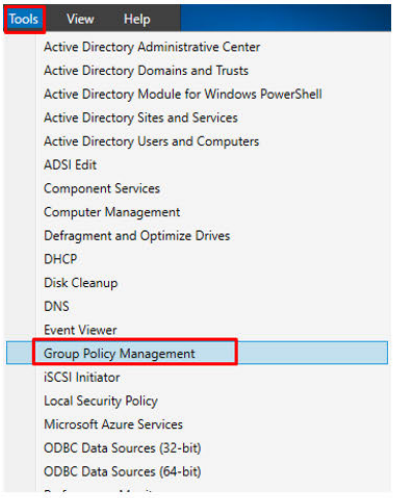
In cybersecurity, station hardening typically refers to the process of securing and strengthening network stations or devices to make them more resistant to cyber threats and attacks.

Like making computers tough so bad guys can't mess with them. It's like adding super locks, fixing weak spots, and keeping an eye out for any trouble. This helps keep important stuff safe and follows the rules.

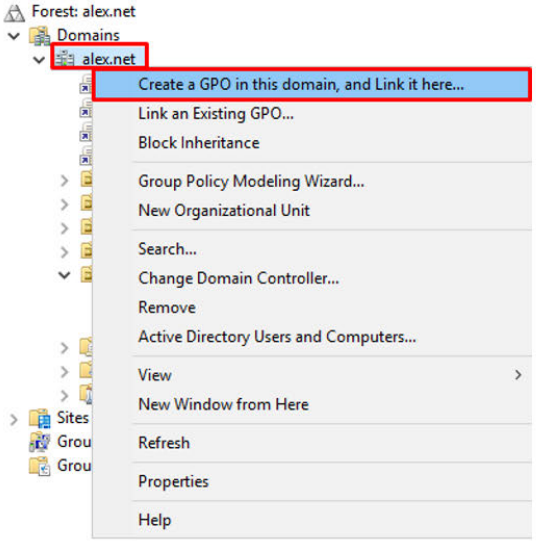
In this part I will use GPO or group policy to harder the workstations

First I will deny the access of those that are not in the Sys_Admins group to have access to the Control Panel or the CMD

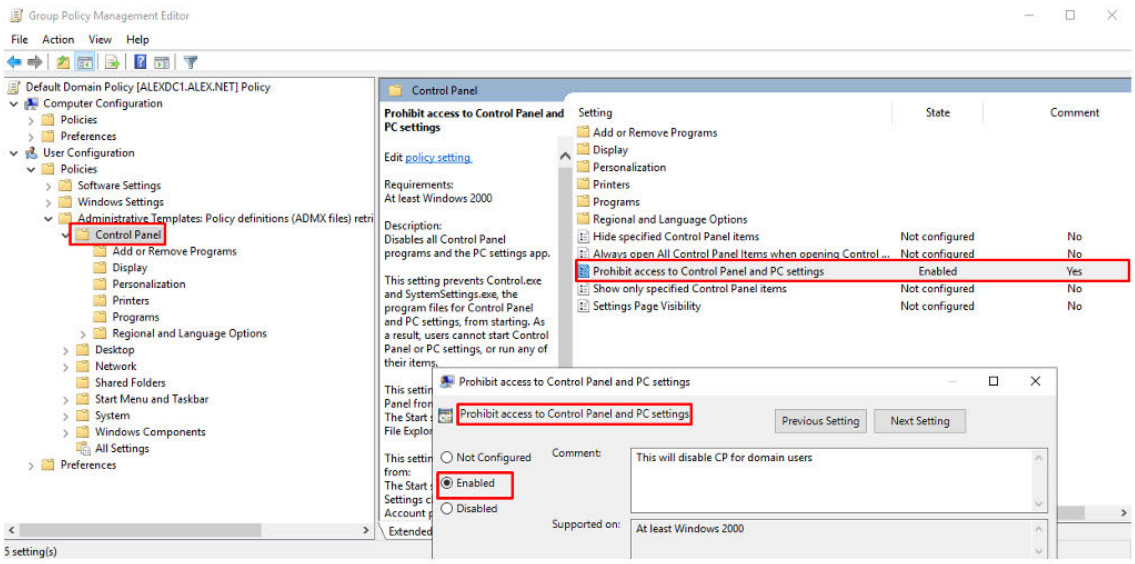
Starting up by opening the Group Policy Management tool



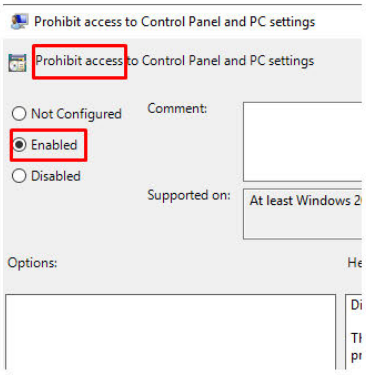
I'll create a GPO in the alex.net domain in Group Policy Objects

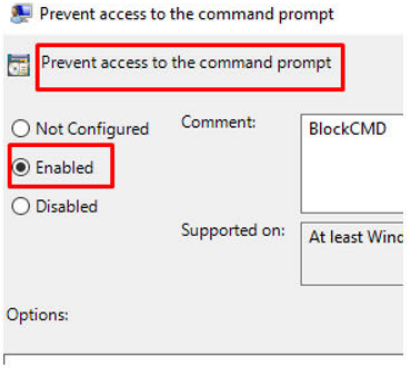


Here I'm enabling the GPO that prohibits access to Control Panel and PC Settings for domain users

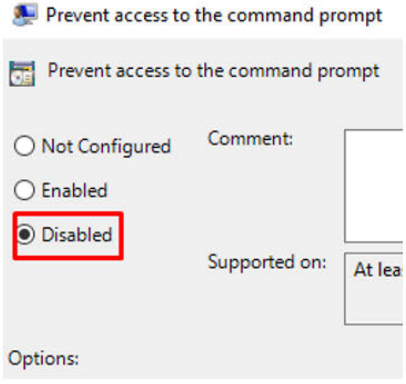


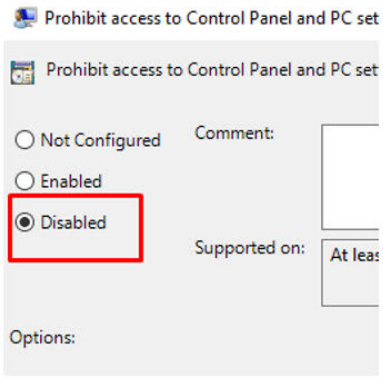
Domain policies (None SysAdmins)



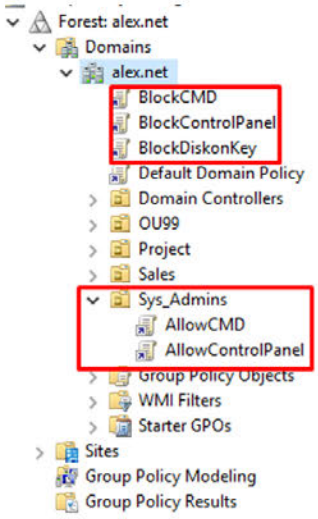


Sys_Admins GPO's policies, they have access to the CMD and the Control Panel, we will test this

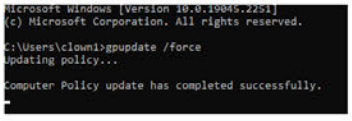




Here we can see an overview of the Policies, the top 3 will block CMD/CP/DiskonKey for the rest of the user Sys_Admins have their own policy which will allow them to use CMD+Control panel but will still block them from using a diskon key

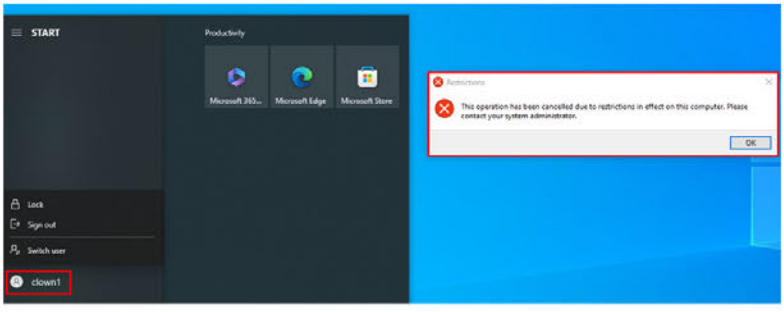


Clown1 testing, Clown1 is in sales and not a Sys_Admin, before the test I'll run a gpupdate /force command to force the GPO changes I've just made, I will test on PC1 (WIN10)

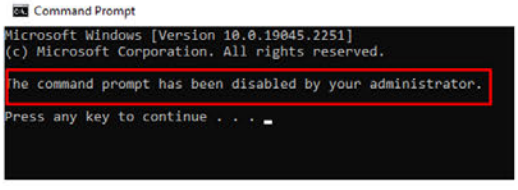


Now I'll takes Clowns1 ability to run the CMD or get into the control panel

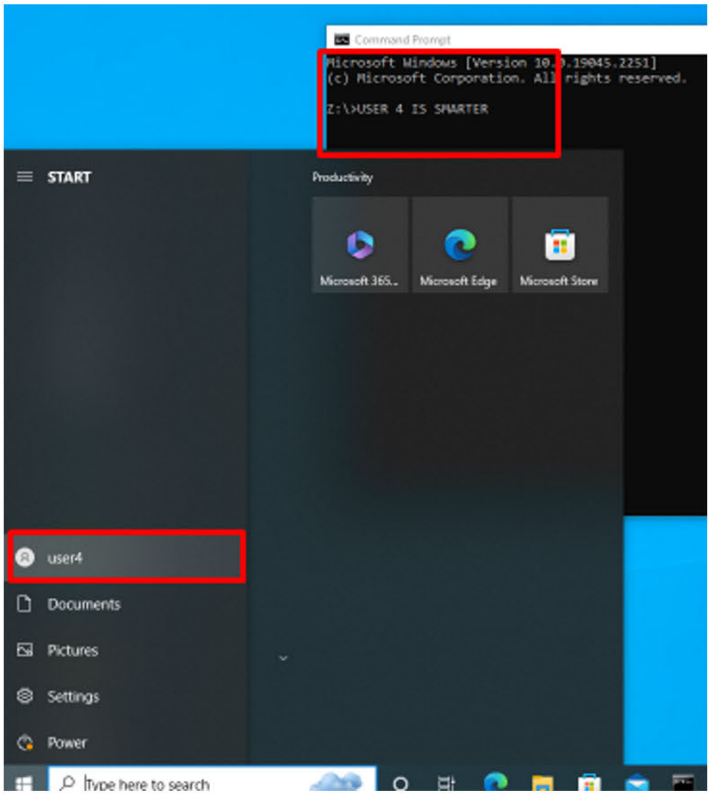
Clown1 cannot get into the control panel



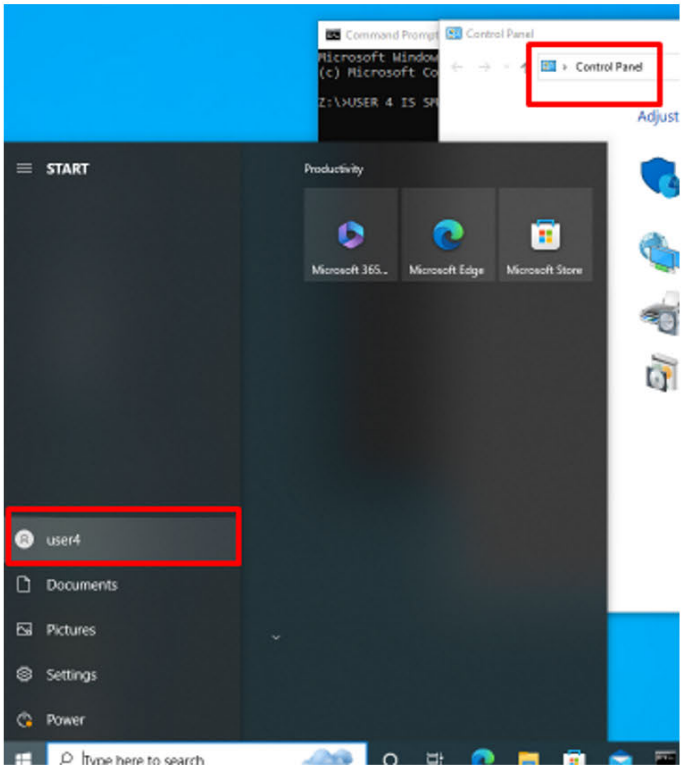
He also cannot use the CMD



Now I'll test an Sys_Admin user on PC1 (WIN10)
User 4 who's a member of the Sys_Admin group can use the CMD on PC1 unlike the loser Clown1 who wished he was in The Sys_Admin group



User4 who's a member of the Sys_Admin group can also use the Control Panel

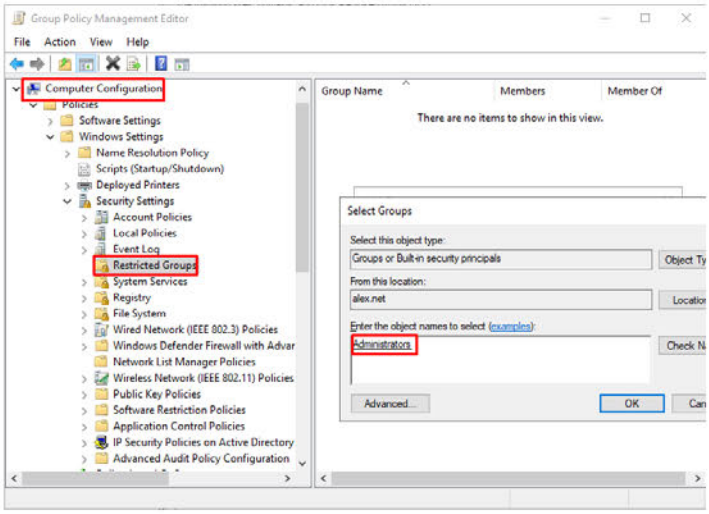


Now that we've established that being a Sys_Admins is awesome, I'll make it even better now

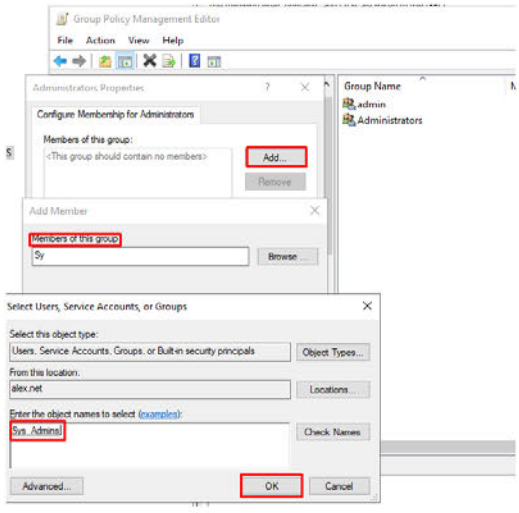
I'll make a policy that gives the Sys_Admins group to be in the Local Administrator group on all the systems in the network

Adding "Sys_Admins" to the local Administrators group via Group Policy simplifies administration, ensures consistent security, and provides centralized control, making it easier to manage and enforce security policies across all networked devices.

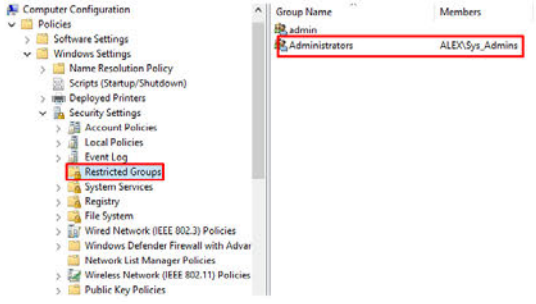
First I'll add the administrators group



Followed by the Sys_Admin group

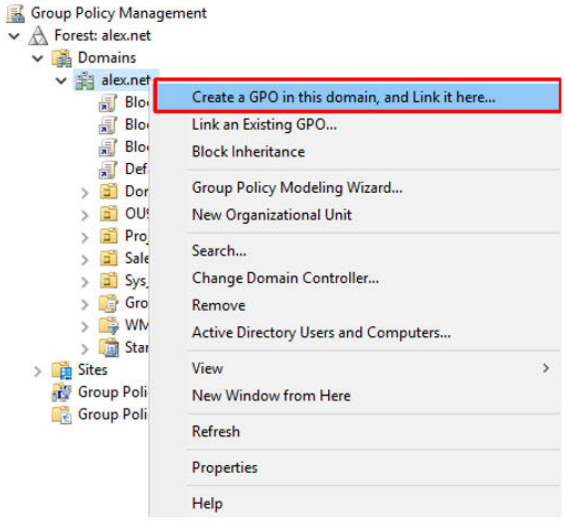


Now after I added the Sys_Admins to this group you can see they're members of Administrators

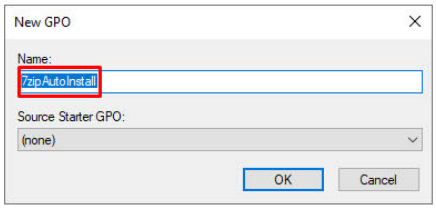


Now I will configure an automatic installation of 7-zip on all the systems on the servers without users doing it themselves
I'll be using GPO instead

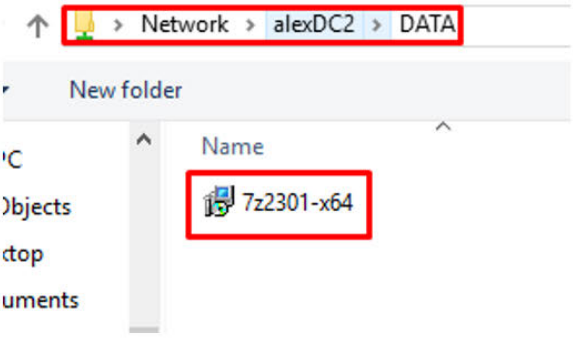
I have already download 7zip MSI installer and have placed it in the DATA folder
The next step is to create a new GPO



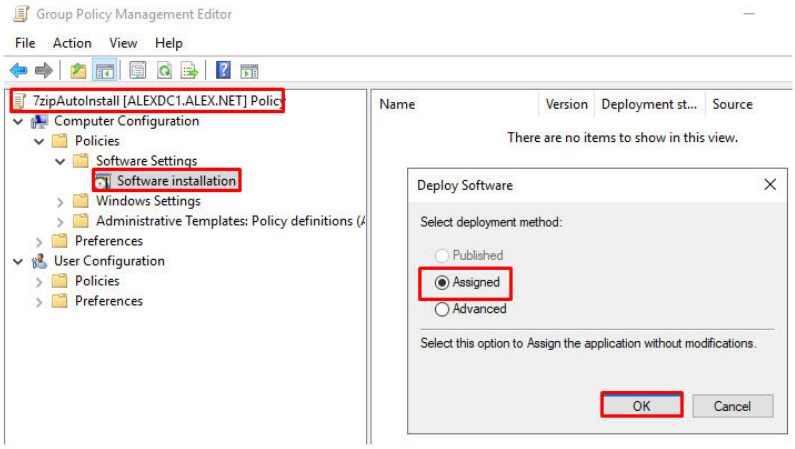
I'll name it 7zip auto install



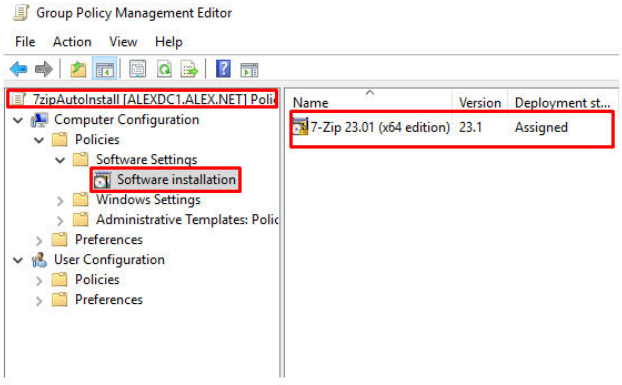
Select the MSI package that installs 7zip, from a network shared DATA folder



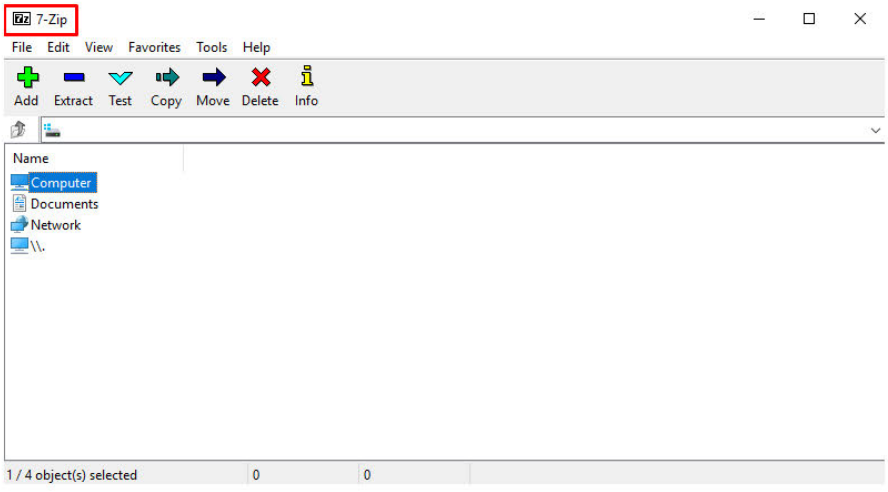
Choose the Assigned option for no human involvement



Installation is ready, lets test if this works, after force update GPO command



7Zip has been auto installed after restart



Part 11 - Organization Password Policy

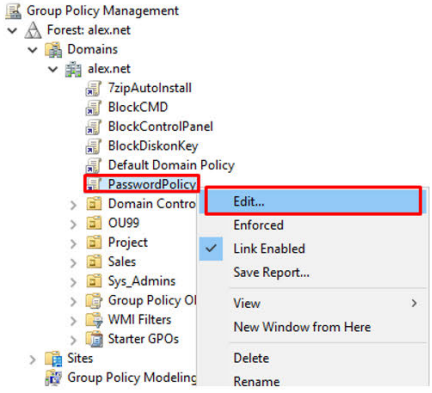
Organization password policies are vital for security, preventing unauthorized access, and compliance. They are applied during employee onboarding, regular password updates, access to systems, remote connections, compliance audits, and across third-party applications to maintain a consistent security posture.

They also minimize cybersecurity threats, and ensuring regulatory compliance. They are implemented during employee onboarding, periodic password updates, access to sensitive systems and networks, remote connections, compliance audits, and across diverse third-party applications.

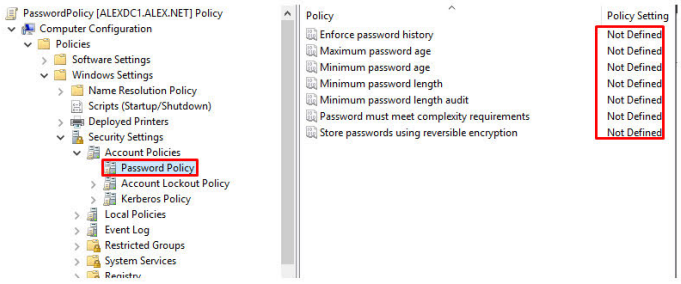
In this part I will create a password GPO that has strict password requirements

- Minimum length of 8
- Has to be a combination of letters/numbers/symbols/small & big letters
- Expires in 75 days
- 4 last passwords used cannot be used again

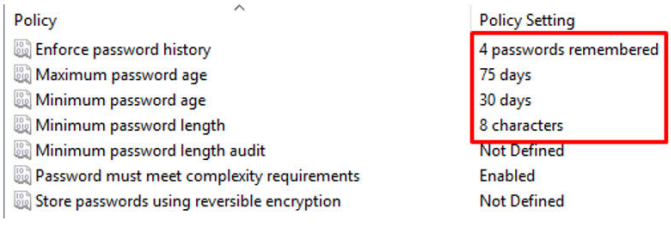
First I'll being by opening the GPO, then I will create a new GPO and click on edit



Expand the GPO in the GPMC and navigate to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy.



I will now configure according to the requirements



The GPO is now active, and the network is safer thanks to it.

Part 12 - Research/Analysis Article Project

Alright, Today, we're diving into the nitty-gritty of keeping our digital lives safe and on lockdown. You know, passwords, remote stuff, identity secrets, and who gets the secret access to our virtual house. Plus, we're throwing Microsoft into the ring and checking out how they're playing the game compared to the other players on the field. Ready?

I. Password Security: Okay, first up – the secret sauce to your digital life – passwords! Microsoft's got this party called Active Directory where they lay down the rules. They want us to create passwords that are like a maze for hackers. Think numbers, symbols, and all that, makes it really difficult to decrypt.

Now, others might throw in their own flavor. Some go full-on fortress mode with super strict rules like the financial industry or the military, while others might be more laid-back, letting you keep a much simpler "secret handshake" or password. everyone's got their password's own requirements, but the strictness can be totally different depending on various factors.

II. Remote Rendezvous: Ever had to work from your favorite couch or lazy chair? Microsoft's got your back with this Remote Desktop thingy. It's like a virtual tunnel that keeps your connection safe and sound. They're all about complex code, encryption, and multi-factor stuff to keep the digital bad guys at bay, while you can enjoy working from your home instead of driving 2 hours to work!

Counterparts, Well, they might have their own secret "recipe" for remote connections. Some go high-tech like Microsoft, while others might keep it simple like TeamViewer with much less security. It's a balancing act between staying secure and not making you jump through too many hoops of super-duper NSA levels of security.

III. Who's Who in the Digital World: Now, let's talk about who's who in this digital World. Microsoft's got this cool thing called Active Directory – it's like a guest list but for your computer. You can decide who's got the ticket and who's stuck outside, it's a great & relatively simple way to manage your virtual network!

What about the Industry Rivals? Oh, they've got their own guest lists. Some might use different tools like Azure or Jump cloud, but the goal is the same – keeping the riff-raffles out and letting the cool guys in. It's a bit like deciding who gets the backstage pass at a rock concert, unfortunately sometimes the bad guys do manage to sneak in.

IV. Permission Slip for Files and Folders: Time to talk about files and folders – the VIP area of your digital space. Microsoft uses this thing called NTFS. It's like the bouncer or a security guard at the mall, deciding who gets in and who's stuck in line. You've got the power to decide who's a part of your digital network.

Industry competitors like Apple or Google? Well, they have different rules for their digital hangouts. Some keep it exclusive, while others might let more people join in. It's all about finding the right balance between security and letting it roll.

V. Showdown: Microsoft vs. the Rest: So, how does Microsoft stack up against the competition? They're like the cool kid in school that everybody knows, but now there's a whole variety show out there now with plenty of choices. Some companies go for the "simple" design, while others bring out the fireworks.

Microsoft's always in the lab, cooking up new things to stay ahead of the game. But across the street, you've got companies doing their own thing trying to compete with the "big dog" sort to speak – the problem is that sometimes the "big dogs" like Microsoft, Apple and Google eat up their competition by buying them so it's difficult for new ground breaking ideas to grow.

VI. What It Means for Us: – the real stars of this digital drama. Microsoft wants us to follow the rules, but are they're trying to make it easy for us? what about Other companies? It's all about finding that sweet spot between keeping things locked down and not making us pull our hair out with insane levels of security and authentications, right now it seems like Microsoft is still leading the way when it comes to consistency and reliability compared to the rest, that's why they "own" the market

The impact on our day to day lives? Well, it depends on how well we know the rules and how much the big shots enforce them. Microsoft wants us to feel like we can move, not to feel like we're getting stuck in a mud.

Conclusion: To wrap it up, keeping our digital secrets safe is complicated, everyone are following the same basic principles of security but with their own unique set of design. Microsoft's got its style, but the competition have their own unique style as well, and they often don't mesh together, It's about making sure our personal passwords, remote connections, networks are safe, there are easy steps each person can take to do that.

So, who's doing it the best? Well, it depends on who's making us feel like the digital "VIP's" while keeping the attackers at bay.

(Sources - Google,Bard,ChatGPT,Brain)

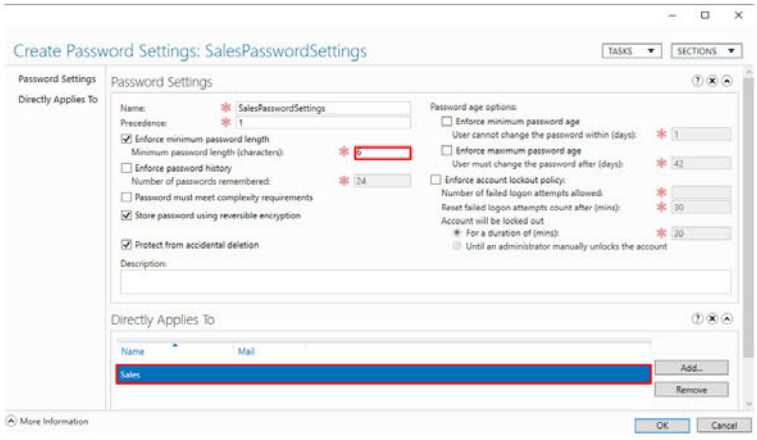
Part 13 - Bonus Challenge

I'll create a more forgiving password policy for the Sales group with these following parameters

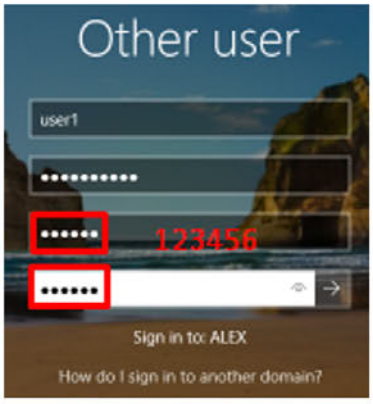
- Minimum length of 6

Remove complexity & Password History

I'll use the Active Directory administrative center on DC1 and configure



After resetting the user1 password he needs to enter a new one on his first login, I have entered a new password that meets the new requirements for him, which "123456" let's see if user1 is able to login with his new password on DC1



Success, user1 who's a member of Sales is able to login with a password of 123456 to DC1 after the changes