

עבודת גמר – Microsoft Server

-סמואל קים-

שם מלא : סמואל קים

מקצה : Microsoft Servers

מרצה : בנימין כהן

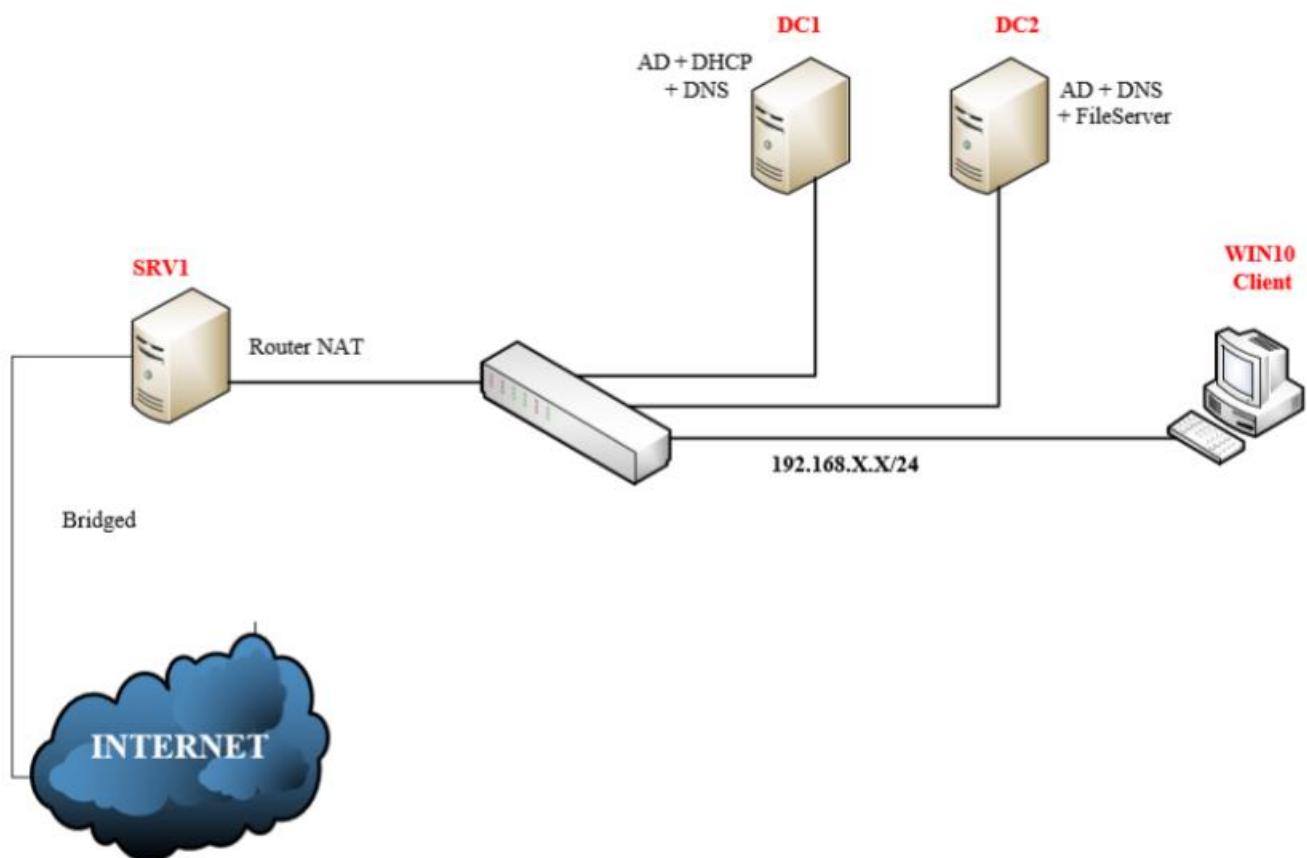
תאריך הגשה : 10.2.2024

לפני שמתחלים בעבודתנו, علينا יש לעירוך תוכנית מדוקיקת כדי לא ליתקל בשגיאות בעתיד או נמשיך בסדר כזה:

4	הכנות המعبدת
8	Domain Controller
24	צרוֹף המחשבים ל- Domain
25	PAT / NAT
33	DHCP
44	ניהול השרת מרוחק
49	DNS
68	Roaming Profile
77	שיטופים ומיפויים – שרת קבצים
93	הקשחת התחנות
101	מדיניות סיסמאות בארגון
102	BONUS
104	עבודת חקר

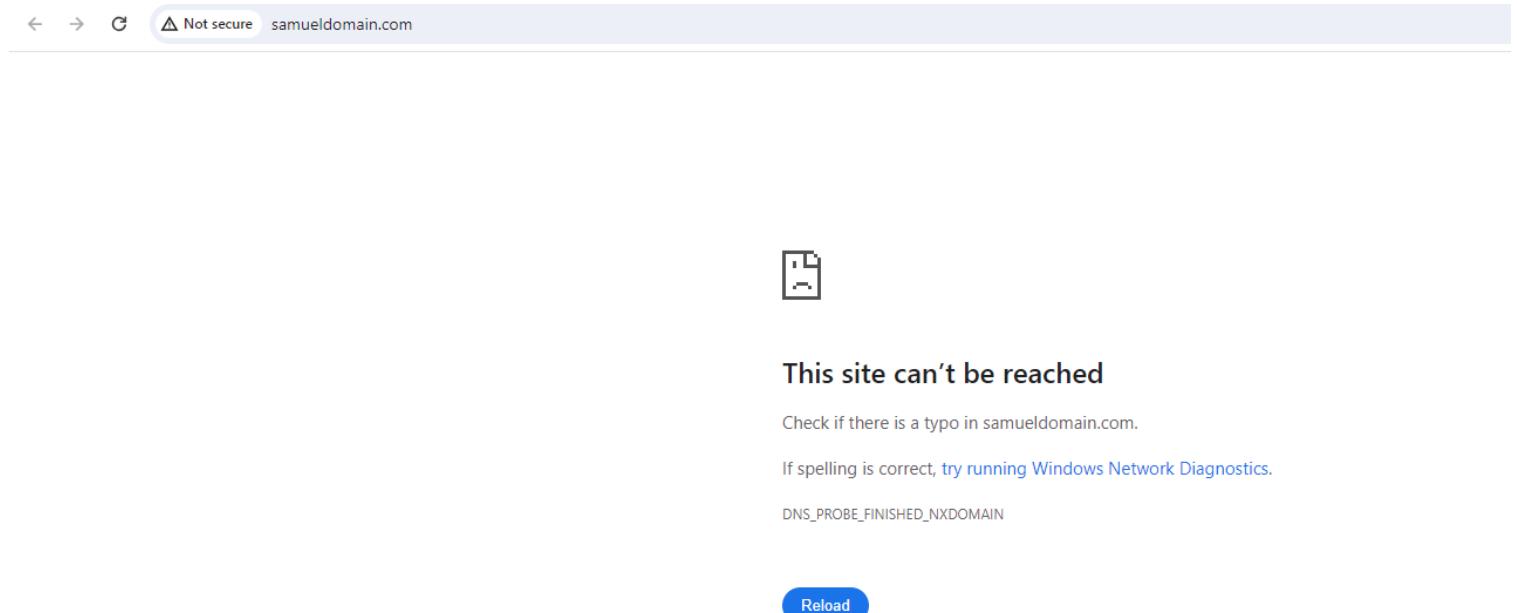
כז נראה הטופולוגיה שלנו בה נעבד, יש לנו שני שרתים DC מחשב (Win 10) ושרת SRV1 שיעבוד כנתב בטופולוגיה שלנו, הוא יתרגם כתובות פרטיות לכתובות ציבוריות לפי פרוטוקול PAT

- DC או Domain Controller אחראי על אימומת והרשאה של משתמשים ומחשבים בדומיין. הנה משאבים כגון קבצים ומדפסות, שכפל מידע בין בקרים תחום שונים כדי להבטיח זמינות ואמינות גבוהה של הרשת.



- הכנות המעבדה -

- עכשוначיל לתכנן, יצרתי קובץ חדש שבו מתוארת תוכנית המכונות העובדות אפשר לראות אותו בעמוד הבא , נבדק בתוכנת VMware
- מצאתי גם שם דומיין ובדקתי את זמינותו באינטרנט, הדומיין פנוי, אפשר לחת אותו :



- יש אפשרות לראות את זה בקובץ נפרד שליחתי

IP Range: 192.168.116.50-100 /24 Admin user name: Avocado

Admin Password: 1234qweR

FQ Domain Name: samueldomain.com

1st DC:

Name: samdc1 OS Version: Microsoft Server 2019

IP: 192.168.116.200 / 24 DG: 192.168.116.254

DNS 1: 192.168.116.200 DNS 2: 192.168.116.201

Roles: DC, DNS, AD, DHCP

2nd DC:

Name: samdc2 OS Version: Microsoft Server 2019

IP: 192.168.116.201 /24 DG: 192.168.116.254

DNS 1: 192.168.116.200 DNS 2: 192.168.116.201

Roles: AD, DNS, File Server

NAT-SRV

Name: samnat OS Version: Microsoft Server 2019

IP: 192.168.116.254 / 24 DG: -

DNS 1: 192.168.116.200 DNS 2: 192.168.116.201

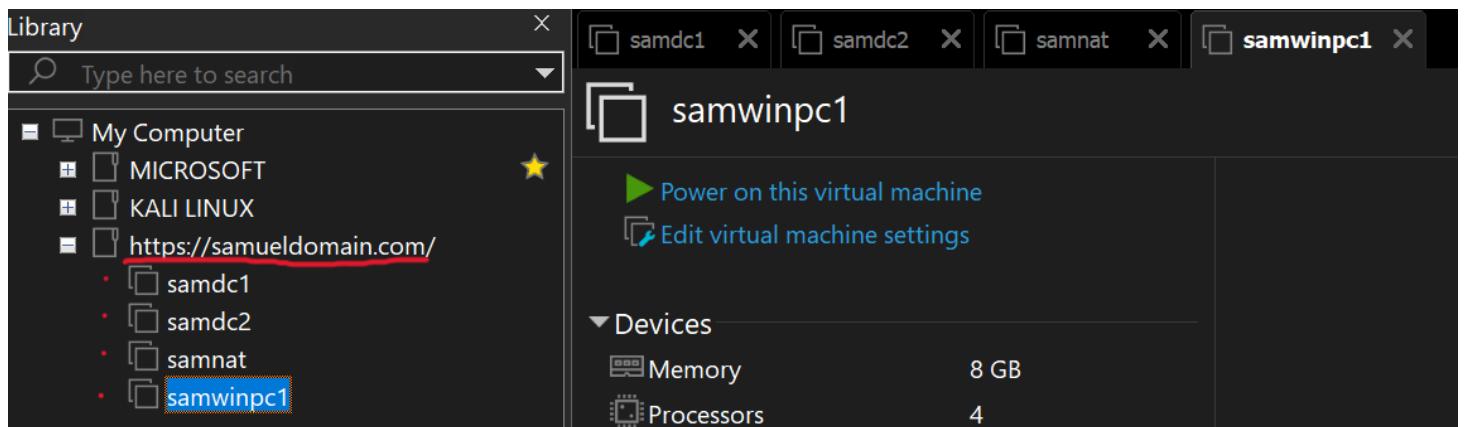
Roles: Router - NAT

- הכנות המעבדה -

Domain: samueldomain.com

Passwords: 1234qweR (All Profiles)

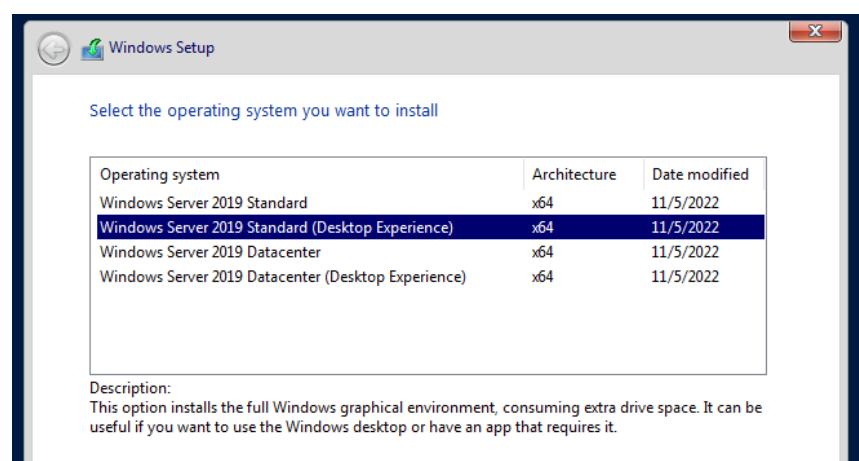
- מכונות וירטואליות מוכנות, כעת נעבר להתקנת ISO במכשירים קובץ Windows



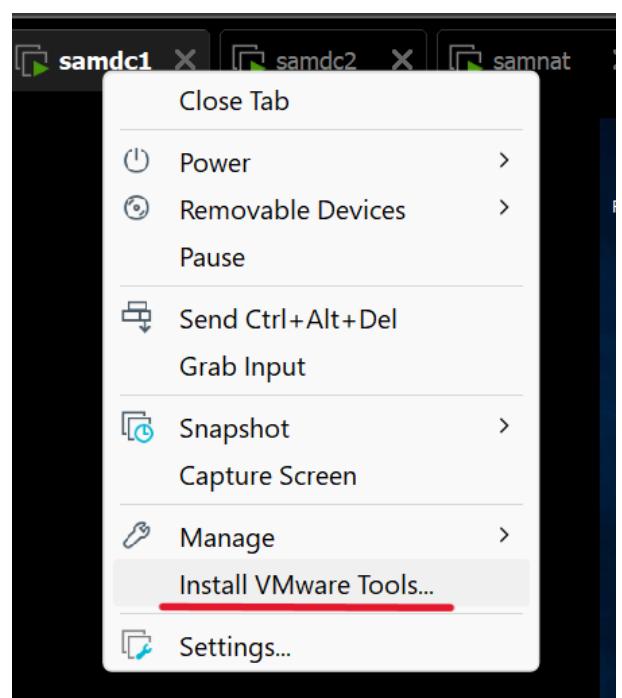
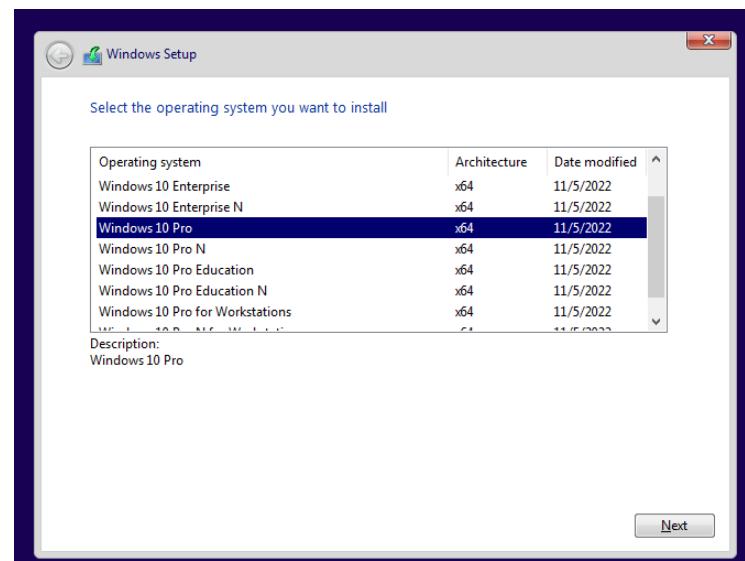
- הכנות המעבדה -

- כעת אנו נמצאים ב PRE Installation על המכונות שלנו, מגדירים את השפה \ שעון הנכוון מיקום ומתקינים את הדרייבר של VMtools אל כל המחשבים

Server DC 1, 2 & NAT:

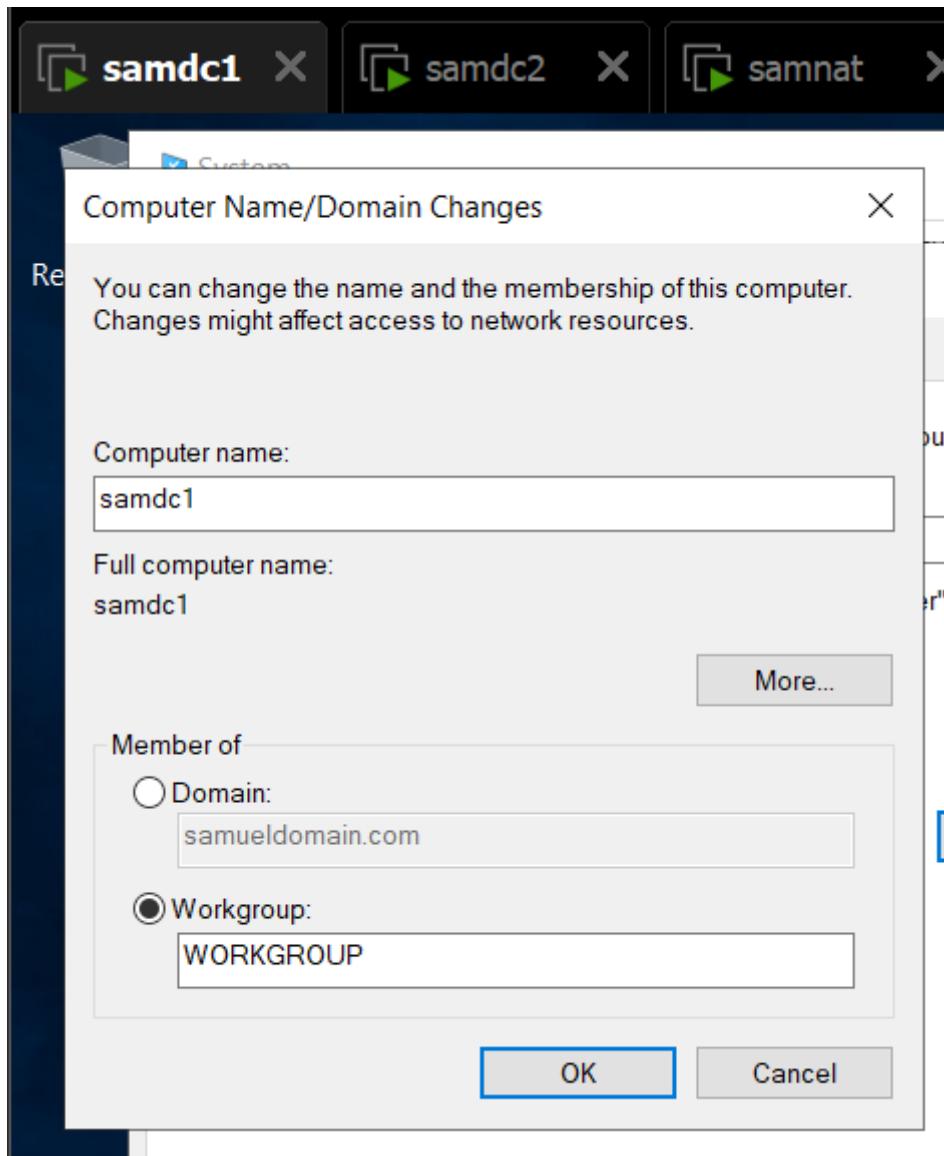


Windows 10 :



- Domain Controller -

קודם כל, בואו נוסיף את שם המחשב - אנחנו עדים לא יכולים להוסיף אותו לדומיין כי שום דבר לא מוגדר

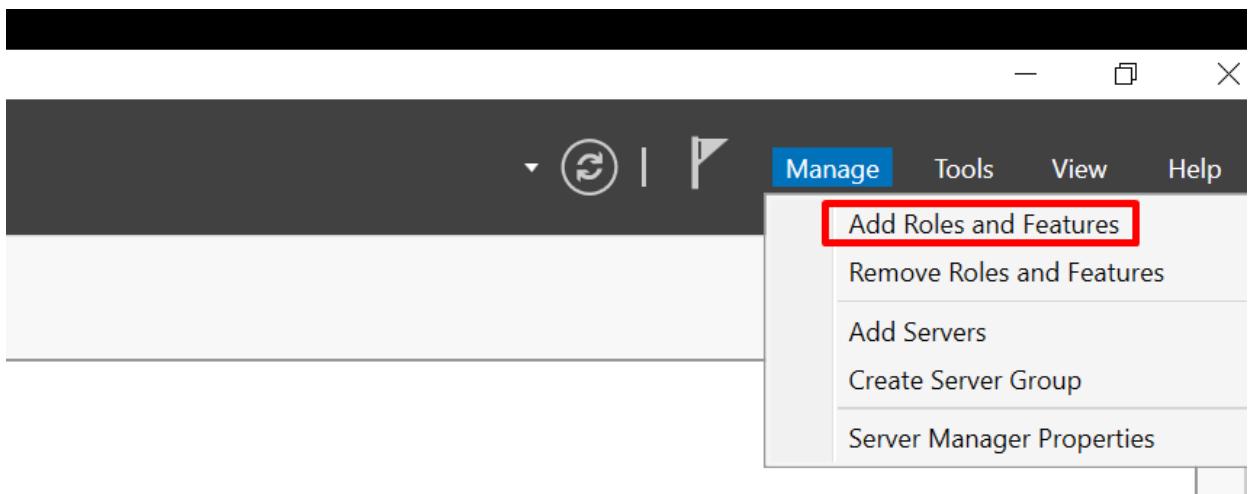


- Active Directory (AD) הוא שירות ספריות שפותח על ידי Microsoft המשמש בסביבת Windows לניהול משתמשים, מחשבים, קבוצות ומשאבים אחרים ברשת. זהו מסד נתונים מרכזי המאחסן מידע על אובייקט רשות ותכונותיהם. Active Directory מספקת גישה אחורית למשאבים, ניהול מדיניות אבטחה וaimot משמשים בראשת ארגונית.

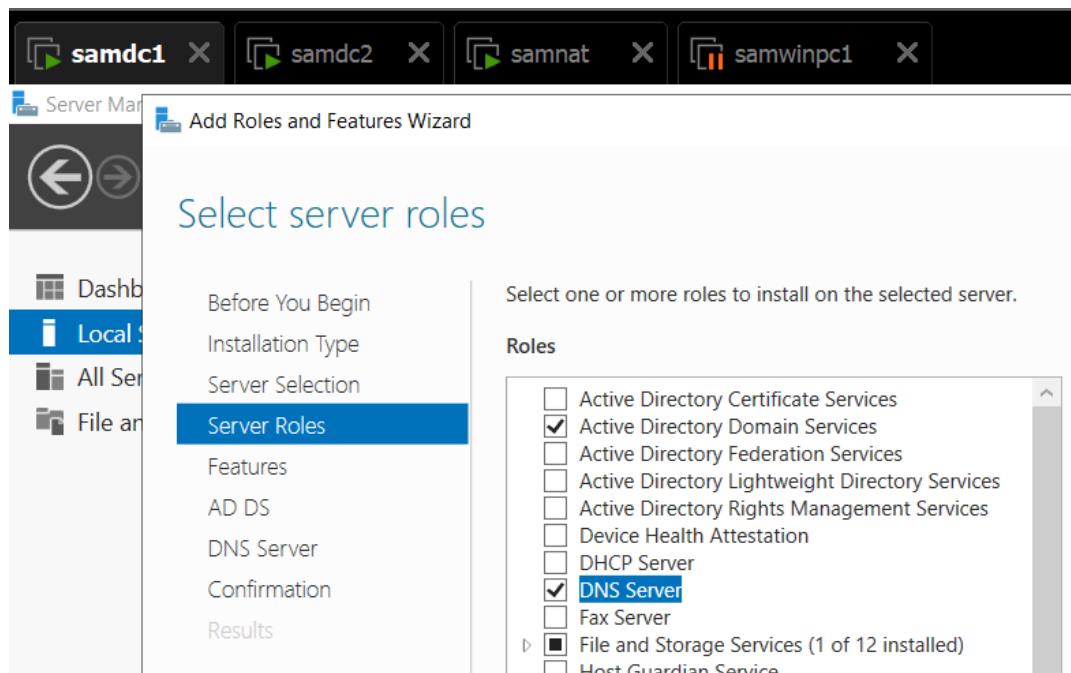
- Domain Controller -

DNS Server \ Domain Controller להפוך את DC1

- כآن ב Server Manager נקצתה את DC1 כ PDC השרת הראשי שמנהל את הכול בתחום שלנו. ניצור Forest חדש, וגם נוסיף Active Directory לניהול דומיין ונփוך אותו לשרת DNS גם כך שכל המכשירים ברשת ייגשו אליו תחילת

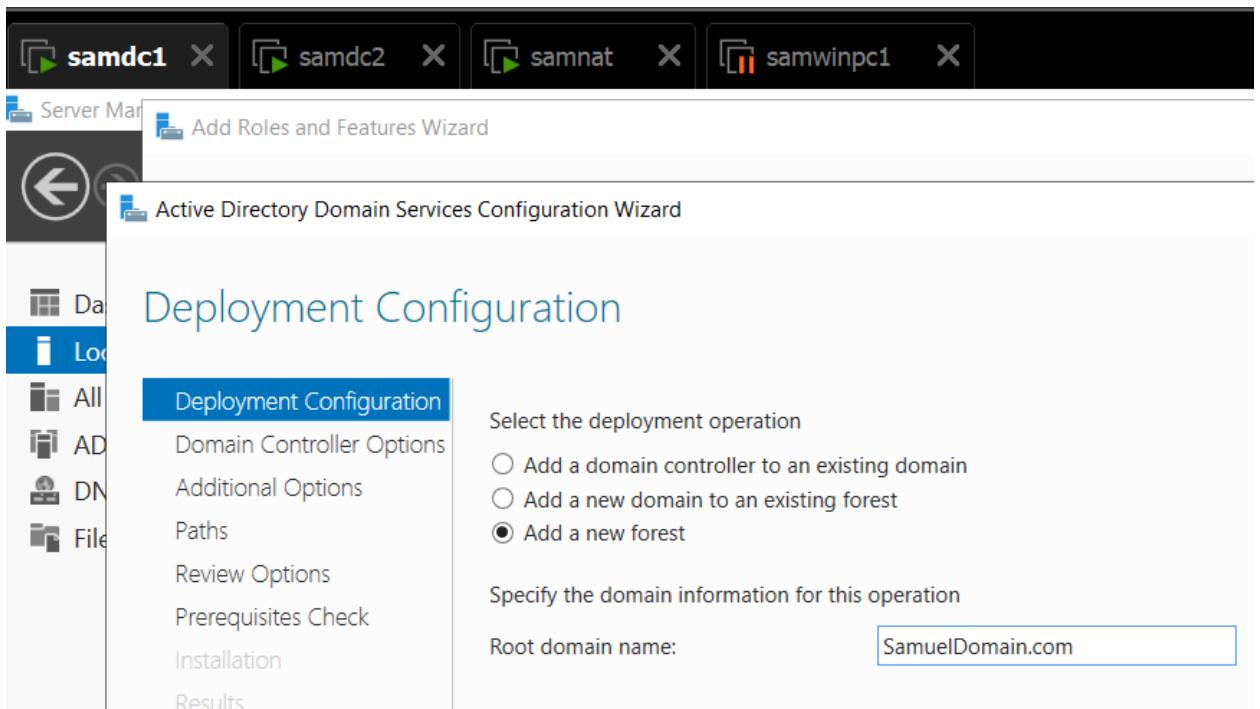


- בManage נתקין את כל הרחבות ותפקידים עבור השירותים שלנו



- Domain Controller -

- 創建一個新的 forest 和域，沒有域控制器



- 在這一步，你將會選擇要部署的森林、域或控制器。通常情況下，我們會選擇「Add a new forest」，並為新森林設置根域。

Paths

TARGET SERVER
samdc1

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths

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

Database folder:	C:\Windows\NTDS	...
Log files folder:	C:\Windows\NTDS	...
SYSVOL folder:	C:\Windows\SYSVOL	...

- Microsoft Active Directory "Forest" 是一個由多個域組成的樹狀結構，每個域都有自己的域控制器。

- Domain Controller -

”

לפניהם המשך, אני רוצה לנטרל את המנהל הנוכחי למטרות אבטחה, מכיוון שה SID-שלו ידוע לכולם והડומיין שלנו עשוי להיות בסיכון

- הSID (Security Identifier) הוא מזהה אבטחה ייחודי המוקצה לכל אובייקט במערכת Windows

Copy Object - User

Create in: SamuelDomain.com/Users

First name:	Avocado	Initials:
Last name:		
Full name:	Avocado	
User logon name:	avocado	@SamuelDomain.com
User logon name (pre-Windows 2000):	SAMUELDOMAIN\	avocado

Server Manager ▶ Dashboard

Active Directory Users and Computers

File Action Help

Name Type Description

Administrator	User	Built-in account for admin...
Allowed ROD...	Security Group	Members in this group c...
<u>Avocado</u>	User	
Cert Publishe...	Security Group	Members of this group a...
Cloneable D...	Security Group	Members of this group t...
Denied ROD...	Security Group	Members in this group c...
DnsAdmins	Security Group	DNS Administrators Group
DnsUpdatePr...	Security Group	DNS clients who are per...

Avocado Properties

Published Certificates Member Of Password Replication

Security	Environment	Sessions
General Address Account	Profile Telephone	
Remote Desktop Services Profile		COM+

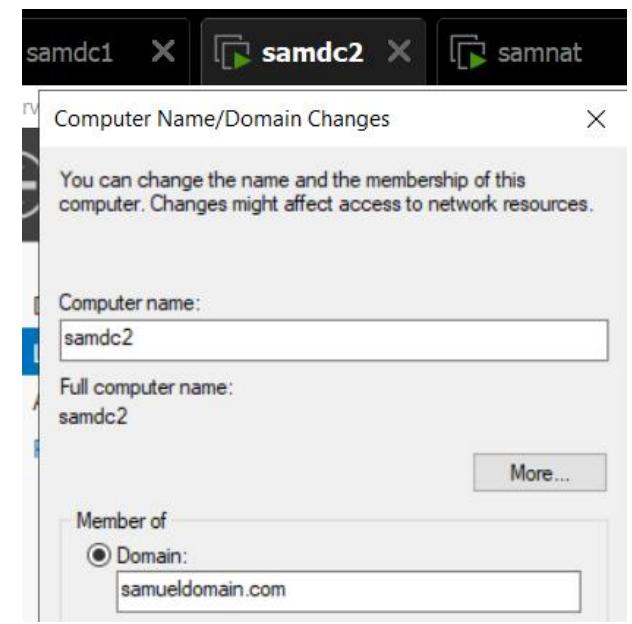
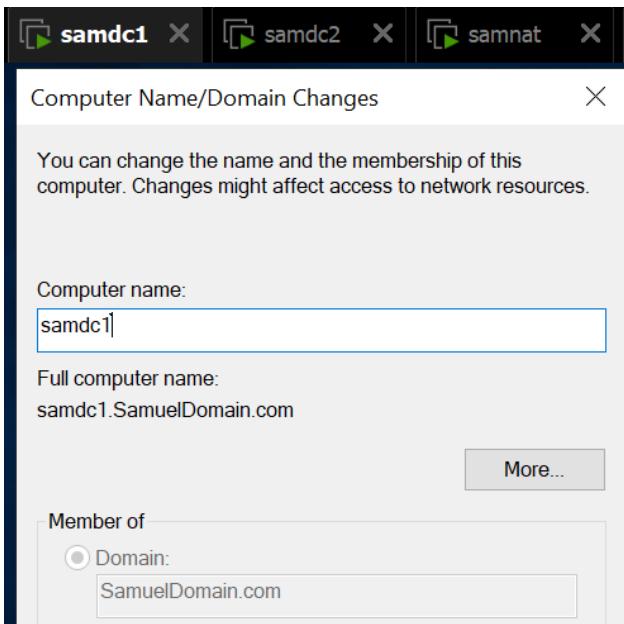
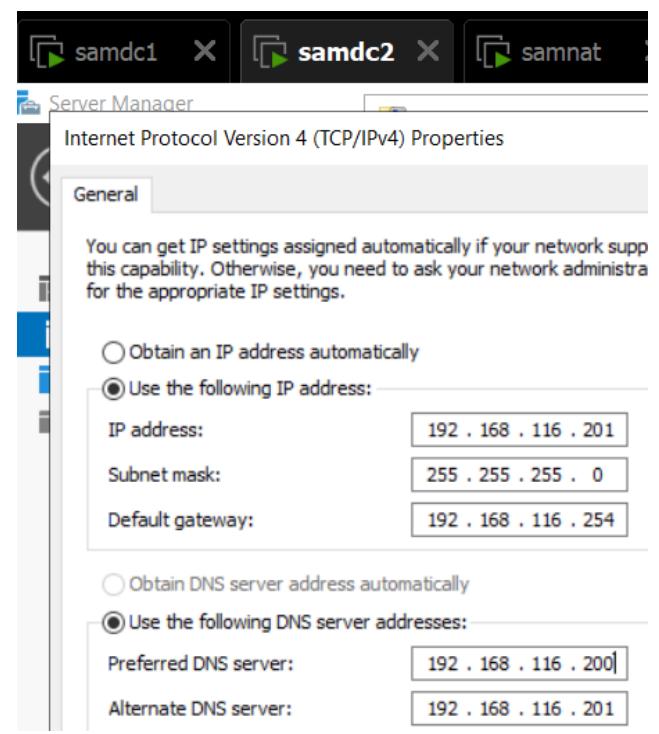
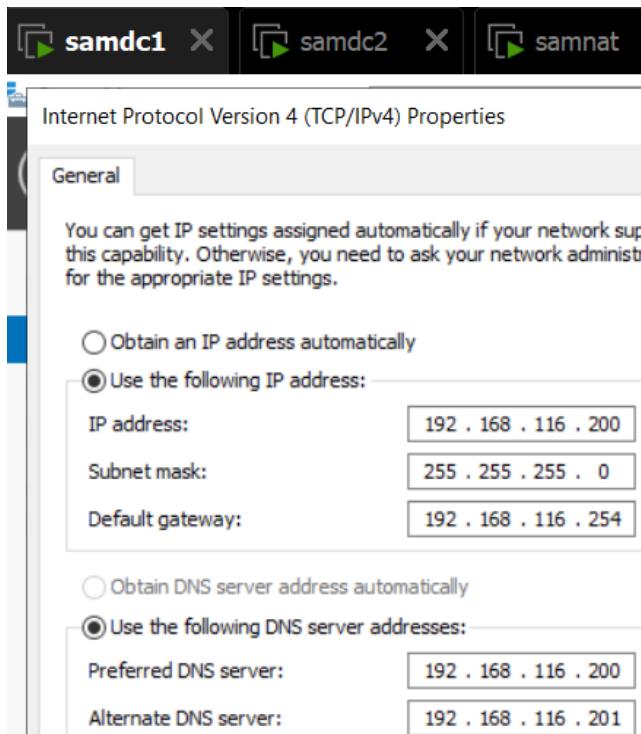
Attributes:

Value
<not set>
CN=Person,CN=Schema,CN=Configuration,DC=Samuell... top; person; organizationalPerson; user 36648ea3-df1a-4d31-a889-026c633c610f S-1-5-21-1637162184-846909169-1922183574-1103 <not set>

- Domain Controller -

- צרף את DC2 ל-Domain- הנדר אותו כשרת DC נוסף
RID Master. הנדר אותו כשרת החזיק בתפקיד Domain

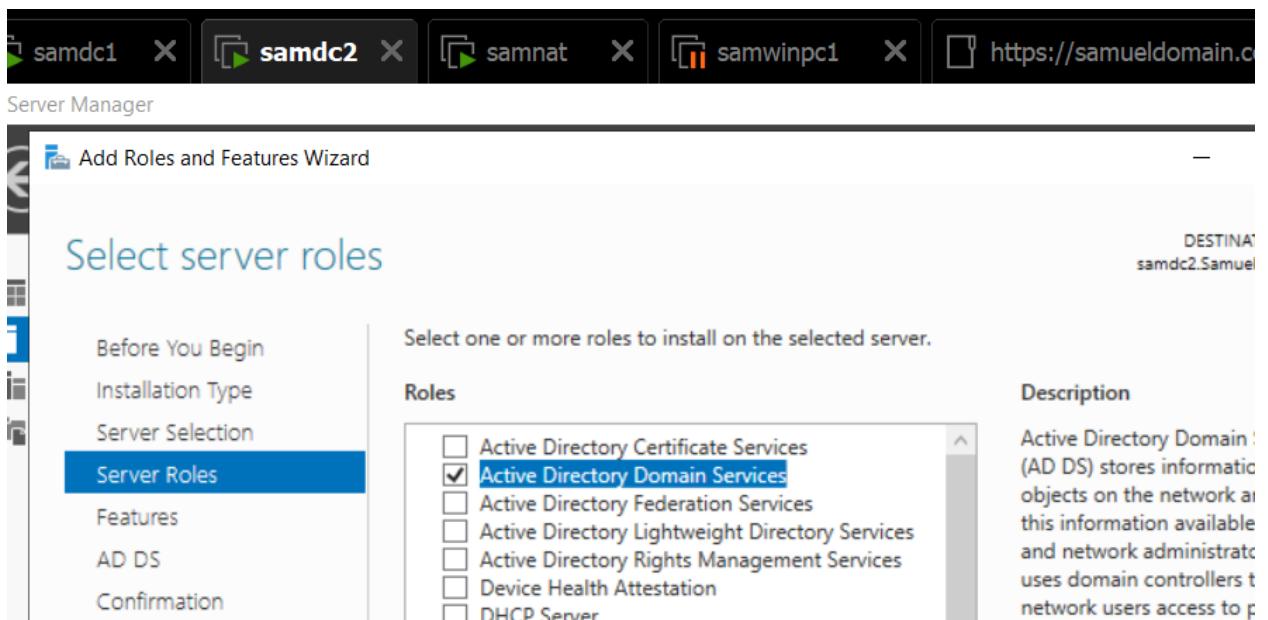
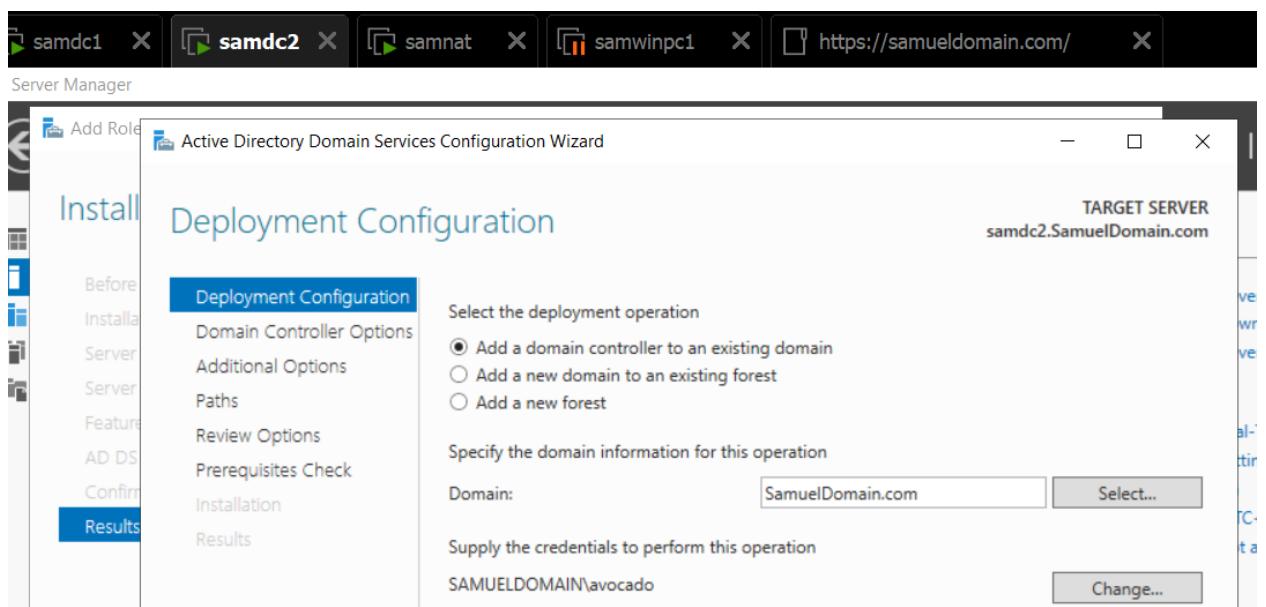
- מוסיפים כתובות סטטי ומחברים את DC2-1 לדומיין



– Domain Controller –

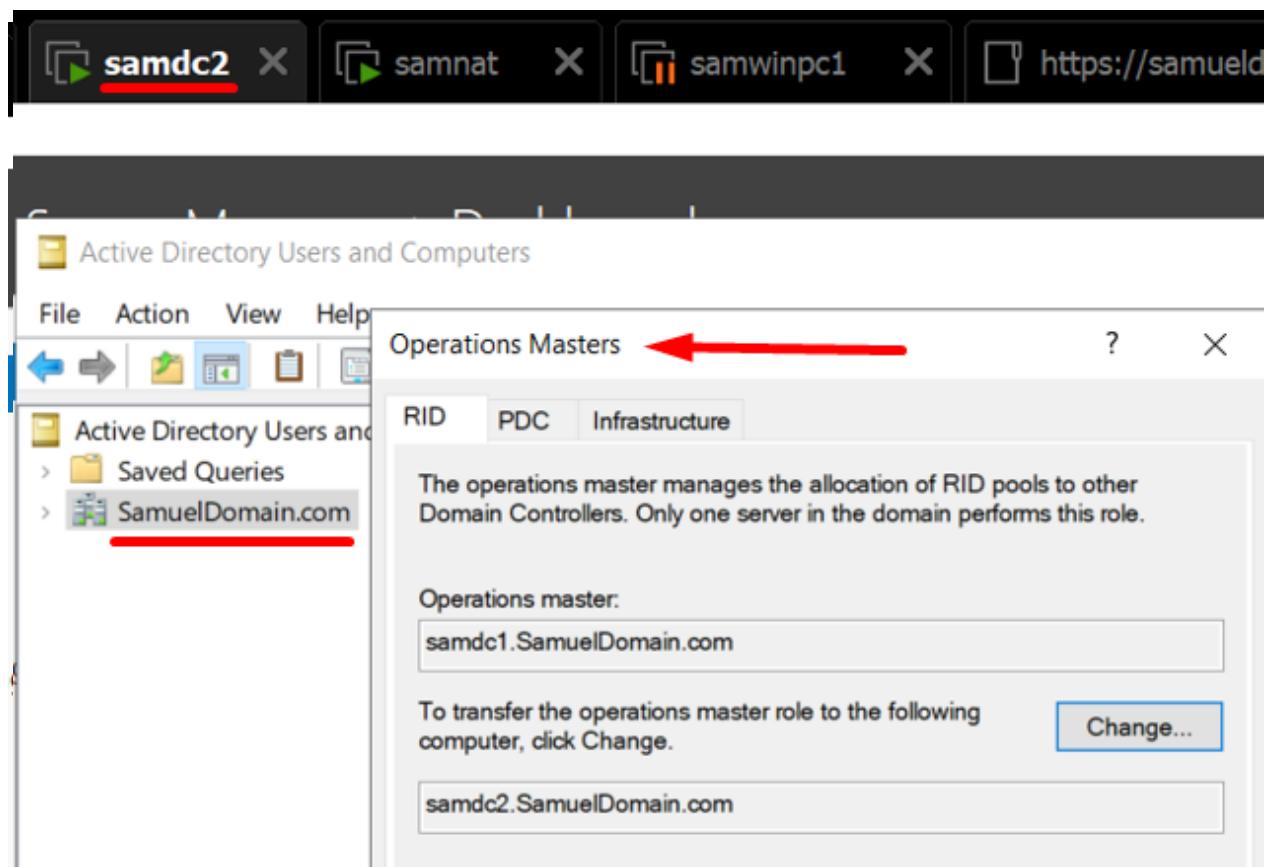
- לאחר ההצטרפות לדומיין, עלינו להתקין AD בשרת השני על מנת לחלק את העומס ובלב זה להוסיף את תפקיד RID Master לייצור מזהים ייחודיים לאובייקט בתחום Active Directory

- מוסיפים שרת DC2 ל FOREST הקיים



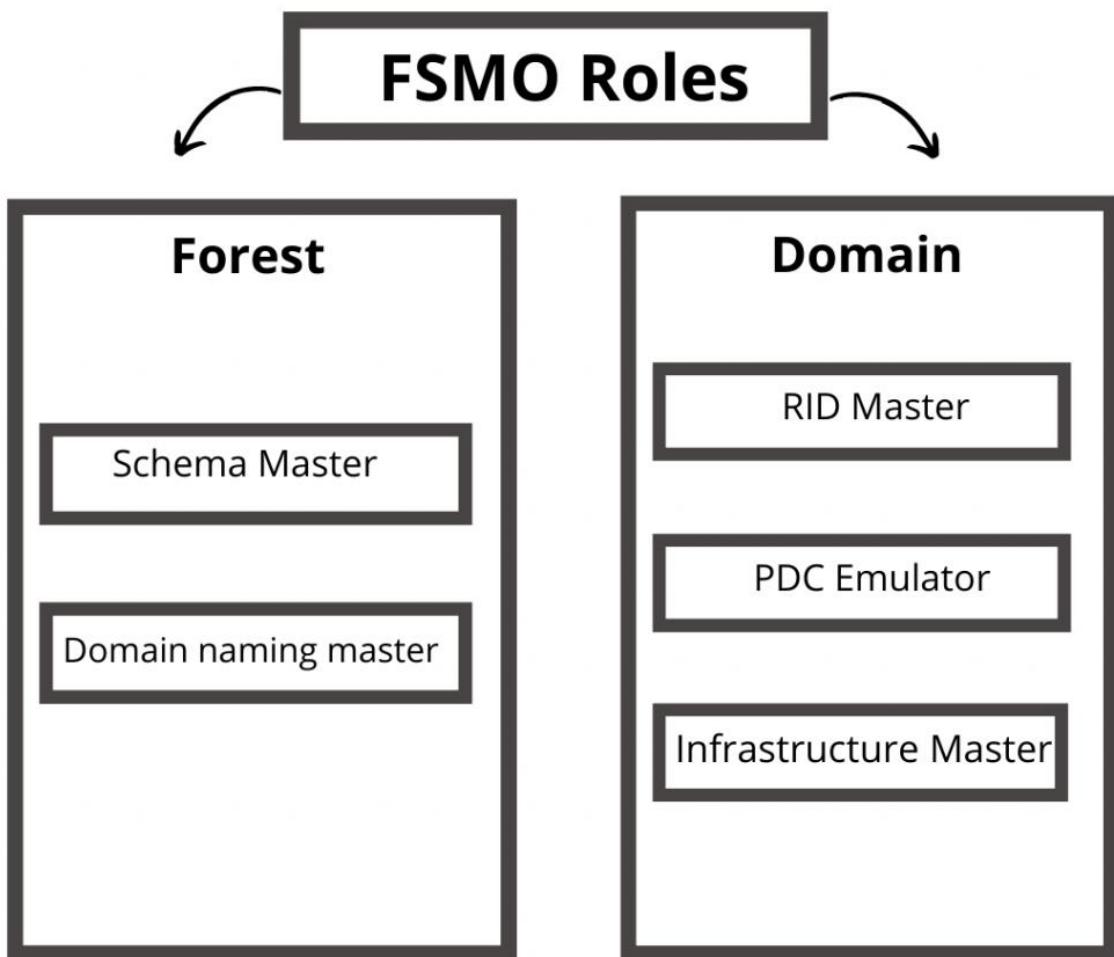
- Domain Controller -

- ולאחר לחיצה על כפתור CHANGE, השרת השני שלנו מקבל את התפקיד של RID MASTER



- RID Master (Relative Identifier Master) הוא אחד מתפקידיו (FSMO) ב-Active Directory שאחראי על הנפקת מזהים ייחסיים (IDs) בדומיין. IDs משמשים לייצירת SIDs (מזהים אבטחה) ייחודיים עבור כל אובייקט חדש, דיברנו עליהם בעבר

- **FSMO (Flexible Single Master Operations)** הוא קבוצה של תפקידים בשירות הספריות של Active Directory המנהלות פעולות הדורשות בקרה ותיאום מרכזיים בתחום סביבת Active Directory. כל תפקיד FSMO אחראי לביצוע פונקציות ספציפיות בתחום תחום או ערך של Active Directory כולל תפקידים כמו PDC, Schema Master, Domain Name, RID Master • תפקידים אלו עוזרים להבטיח עקביות Emulator וכו. תפקידים אלו עוזרים ל证实 עקביות ויעילות של פעולות בסביבת Active Directory



- Domain Controller -

- צור שני (OU) organizational unit (OU) האחד עבור מחלקת Sales והשני עבור מחלקת Sys_Admins.
- צור שני משתמשים חדשים בשם user1 ו- user2 (עובד מחלקת Sales).
- צור שני משתמשים נוספים בשם user3 ו- user4 (עובד מחלקת Sys_Admins).
- צור קבוצה בשם Sales והכנס לתוכה את המשתמשים user1 ו- user2.
- צור קבוצה בשם Sys_Admins והכנס לתוכה את המשתמשים user3 ו- user4.
- הכנס את קבוצת Sys_Admins כחברה בקבוצת Domain Admins

- **אנו יוצרים שתי קבוצות של שני אנשים ומוסיפים למנהל הדומיין SysAdmins**

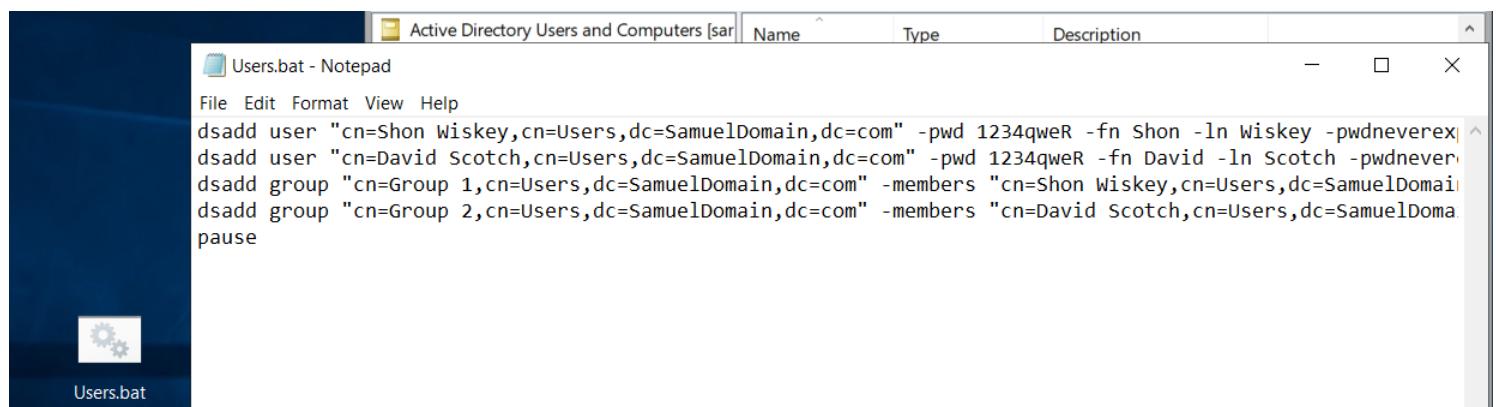
The screenshot shows the Active Directory Users and Computers management console. At the top, two group properties are displayed: 'Sales_group Properties' and 'SysAdmins_group Properties'. Both windows show tabs for Object, Security, Attribute Editor, General, Members, Member Of, and Managed By. In the 'Members' tab of the Sales_group window, two users (User 1 and User 2) are listed under the 'SamuelDomain.com/Sales' container. In the 'Members' tab of the SysAdmins_group window, two users (User 3 and User 4) are listed under the 'SamuelDomain.com/Sys_Admins' container.

Below these windows, the main Active Directory Users and Computers window is shown. On the left, a navigation pane lists various containers: Active Directory Users and Computers [sam], Saved Queries, SamuelDomain.com (which is expanded to show Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, Keys, LostAndFound, Managed Service Accounts, Program Data, System, Users, NTDS Quotas, TPM Devices, Sales, and Sys_Admins). On the right, a 'Select Groups' dialog box is open. It has fields for 'Select this object type:' (Groups or Built-in security principals), 'From this location:' (SamuelDomain.com), and 'Enter the object names to select (examples):' (Domain Admins). A red arrow points from the 'Domain Admins' entry in this field to the 'Check Names' button. Another red arrow points from the 'Check Names' button to the 'OK' button at the bottom right of the dialog box.

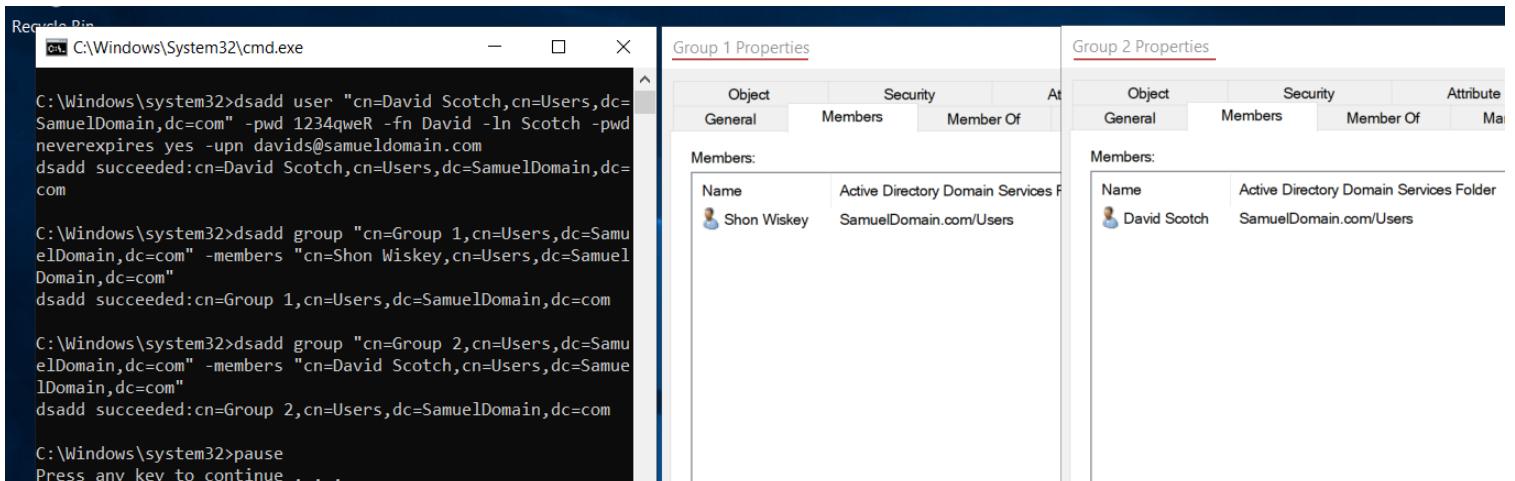
- Domain Controller -

- צור 2 חשבונות משתמש אחרים ע"י שימוש בפקודות DSADD
- צור 2 קבוצות אחרות ע"י שימוש בפקודות DSADD
- הכנס את החשבונות לקבוצות השונות (ע"י פקודות בלבד)

- החלטתי לעשות שלושה סעיפים בסקריפט אחד והחלטתי ליצר קבוצות עם משתמשים חדשים בكونטיינר של USERS



```
Active Directory Users and Computers [sar] Name Type Description
Users.bat - Notepad
File Edit Format View Help
dsadd user "cn=Shon Wiskey,cn=Users,dc=SamuelDomain,dc=com" -pwd 1234qweR -fn Shon -ln Wiskey -pwdneverexp
dsadd user "cn=David Scotch,cn=Users,dc=SamuelDomain,dc=com" -pwd 1234qweR -fn David -ln Scotch -pwdneverexp
dsadd group "cn=Group 1,cn=Users,dc=SamuelDomain,dc=com" -members "cn=Shon Wiskey,cn=Users,dc=SamuelDomain,dc=com"
dsadd group "cn=Group 2,cn=Users,dc=SamuelDomain,dc=com" -members "cn=David Scotch,cn=Users,dc=SamuelDomain,dc=com"
pause
```



```
Recycle Bin
C:\Windows\System32\cmd.exe
C:\Windows\system32>dsadd user "cn=David Scotch,cn=Users,dc=SamuelDomain,dc=com" -pwd 1234qweR -fn David -ln Scotch -pwdneverexp yes -upn davids@samueldomain.com
dsadd succeeded:cn=David Scotch,cn=Users,dc=SamuelDomain,dc=com

C:\Windows\system32>dsadd group "cn=Group 1,cn=Users,dc=SamuelDomain,dc=com" -members "cn=Shon Wiskey,cn=Users,dc=SamuelDomain,dc=com"
dsadd succeeded:cn=Group 1,cn=Users,dc=SamuelDomain,dc=com

C:\Windows\system32>dsadd group "cn=Group 2,cn=Users,dc=SamuelDomain,dc=com" -members "cn=David Scotch,cn=Users,dc=SamuelDomain,dc=com"
dsadd succeeded:cn=Group 2,cn=Users,dc=SamuelDomain,dc=com

C:\Windows\system32>pause
Press any key to continue . . .
```

Object	Security	Attribute
General	Members	Member Of
Members:		
Name	Active Directory Domain Services Folder	
Shon Wiskey	SamuelDomain.com/Users	

Object	Security	Attribute
General	Members	Member Of
Members:		
Name	Active Directory Domain Services Folder	
David Scotch	SamuelDomain.com/Users	

- בהתחלה הכתני פקודות שיצרוות משתמשים חדשים ומוסיפות אותם לקבוצה החדשה שנוצרה, אז שמתי את הפקודות האלה בקובץ טקסט שהוא אני מmirah לקובץ BAT, לסקריפט שלנו שיירץ את כל הפקודות אחת אחת

- Domain Controller -

סקריפט :

```
dsadd user "cn=Shon Wiskey,cn=Users,dc=SamuelDomain,dc=com" -pwd  
1234qweR -fn Shon -ln Wiskey -pwdneverexpires yes -upn  
shon@samueldomain.com
```

```
dsadd user "cn=David Scotch,cn=Users,dc=SamuelDomain,dc=com" -pwd  
1234qweR -fn David -ln Scotch -pwdneverexpires yes -upn  
davids@samueldomain.com
```

```
dsadd group "cn=Group 1,cn=Users,dc=SamuelDomain,dc=com" -members  
"cn=Shon Wiskey,cn=Users,dc=SamuelDomain,dc=com"
```

```
dsadd group "cn=Group 2,cn=Users,dc=SamuelDomain,dc=com" -members  
"cn=David Scotch,cn=Users,dc=SamuelDomain,dc=com"
```

pause

יוצר משתמשים חדשים בשם "שון וויסקי ודוד סקוטץ" בדומיין SamuelDomain.com

הפרמטרים :

cn= Name

dc= Domain Name

pwd- מגדיר את הסיסמה של המשתמש

fn- מגדיר את שם המשתמש

ln- מגדיר את שם המשפחה של המשתמש

pwdneverexpires yes- מציין שהסיסמה של המשתמש לעולם לא תפוג

upn- מגדיר את UPN- של המשתמש (User Principal Name) שהוא השם החלופי של המשתמש.

יוצר קבוצה חדשה בשם "קבוצת 1" בדומיין SamuelDomain.com".

הפרמטרים :

members- מצביע על חברי הקבוצה, במקרה זה "שון וויסקי ודוד סקוטץ"

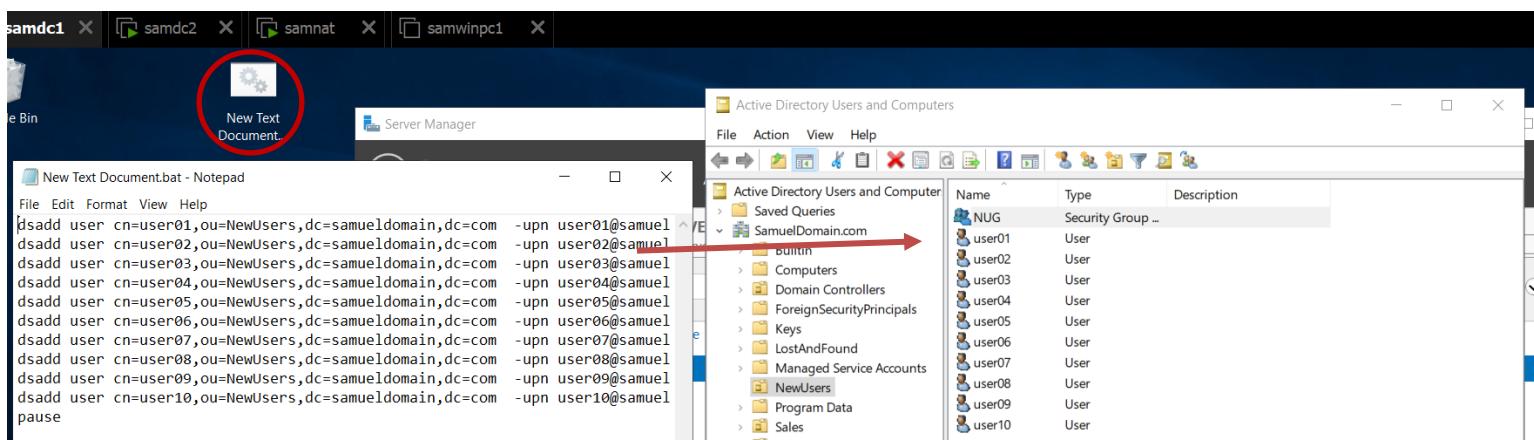
- Domain Controller -

צור 10 חשבונות ע"י שימוש בפקודות DSADD ליצירת ריבוי משתמשים (script)

- כעת נעשה את אותו הדבר עם תרגיל נוסף, רק שהפעם ניצור 10 משתמשים באמצעות כמעט כמעט פקודות

- יצרתי סקריפט ב EXCEL-ותרגמתי אותו לקובץ BAT כדי ליצור 10 משתמשים חדשים ב Active Directory

A	B	C	D	E	F	G
user01	dsadd user cn=user01,ou=NewUsers,dc=samueldomain,dc=com	-upn user01@samueldomain.com	-display user01	-pwd 1234qweR	-mustchpwd no	-hmdir \\SAMDC1\\HomeFolders\\\$username\$
user02	dsadd user cn=user02,ou=NewUsers,dc=samueldomain,dc=com	-upn user02@samueldomain.com	-display user02	-pwd 1234qweR	-mustchpwd no	-hmdir \\SAMDC1\\HomeFolders\\\$username\$
user03	dsadd user cn=user03,ou=NewUsers,dc=samueldomain,dc=com	-upn user03@samueldomain.com	-display user03	-pwd 1234qweR	-mustchpwd no	-hmdir \\SAMDC1\\HomeFolders\\\$username\$
user04	dsadd user cn=user04,ou=NewUsers,dc=samueldomain,dc=com	-upn user04@samueldomain.com	-display user04	-pwd 1234qweR	-mustchpwd no	-hmdir \\SAMDC1\\HomeFolders\\\$username\$
user05	dsadd user cn=user05,ou=NewUsers,dc=samueldomain,dc=com	-upn user05@samueldomain.com	-display user05	-pwd 1234qweR	-mustchpwd no	-hmdir \\SAMDC1\\HomeFolders\\\$username\$
user06	dsadd user cn=user06,ou=NewUsers,dc=samueldomain,dc=com	-upn user06@samueldomain.com	-display user06	-pwd 1234qweR	-mustchpwd no	-hmdir \\SAMDC1\\HomeFolders\\\$username\$
user07	dsadd user cn=user07,ou=NewUsers,dc=samueldomain,dc=com	-upn user07@samueldomain.com	-display user07	-pwd 1234qweR	-mustchpwd no	-hmdir \\SAMDC1\\HomeFolders\\\$username\$
user08	dsadd user cn=user08,ou=NewUsers,dc=samueldomain,dc=com	-upn user08@samueldomain.com	-display user08	-pwd 1234qweR	-mustchpwd no	-hmdir \\SAMDC1\\HomeFolders\\\$username\$
user09	dsadd user cn=user09,ou=NewUsers,dc=samueldomain,dc=com	-upn user09@samueldomain.com	-display user09	-pwd 1234qweR	-mustchpwd no	-hmdir \\SAMDC1\\HomeFolders\\\$username\$
user10	dsadd user cn=user10,ou=NewUsers,dc=samueldomain,dc=com	-upn user10@samueldomain.com	-display user10	-pwd 1234qweR	-mustchpwd no	-hmdir \\SAMDC1\\HomeFolders\\\$username\$



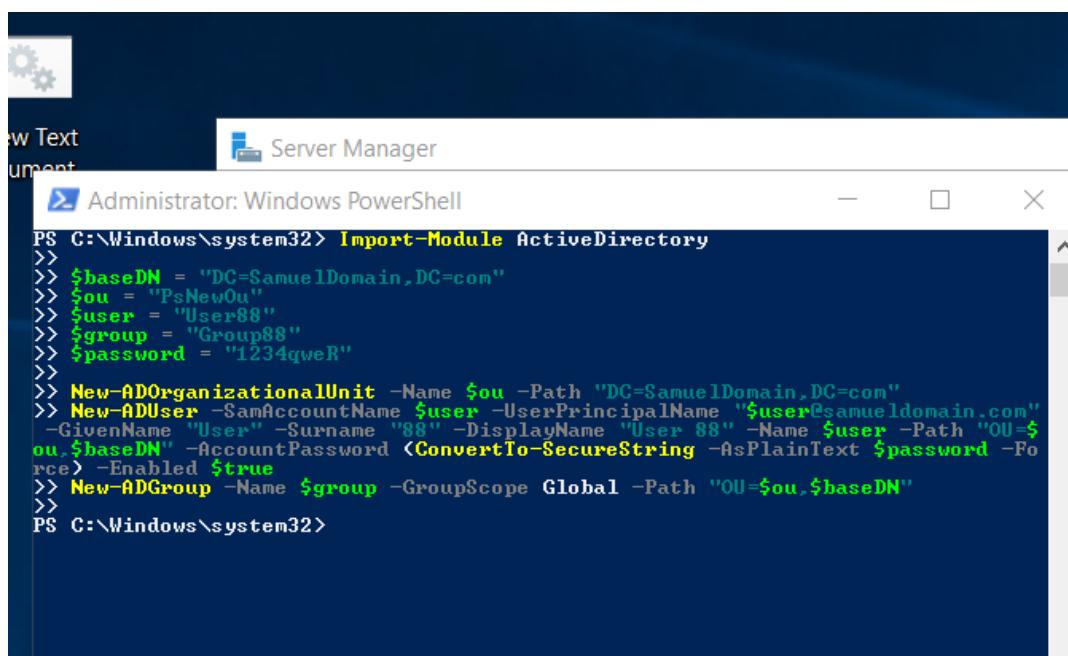
-pwd Password

-hmdir Home Directory

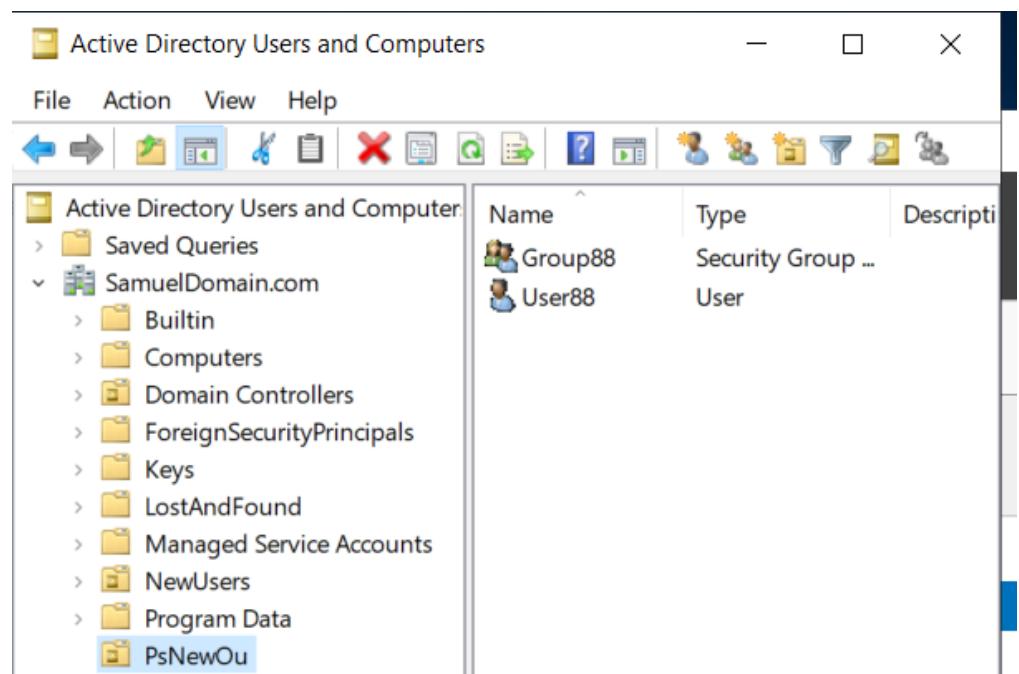
- Domain Controller -

צור OU חדש + חשבון משתמש חדש + קבוצה חדשה ע"י פקודות בPS

- באמצעות פקודות ב-Powershell - הוספהו משתמש חדש OU חדש וקבוצה אליה שייך המשתמש



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Import-Module ActiveDirectory
>>
>> $baseDN = "DC=SamuelDomain,DC=com"
>> $ou = "PsNewOu"
>> $user = "User88"
>> $group = "Group88"
>> $password = "1234queR"
>>
>> New-ADOrganizationalUnit -Name $ou -Path "DC=SamuelDomain,DC=com"
>> New-ADUser -SamAccountName $user -UserPrincipalName "$user@samueldomain.com"
-GivenName "User" -Surname "88" -DisplayName "User 88" -Name $user -Path "OU=$ou,$baseDN" -AccountPassword <ConvertTo-SecureString -AsPlainText $password -Force> -Enabled $true
>> New-ADGroup -Name $group -GroupScope Global -Path "OU=$ou,$baseDN"
>>
PS C:\Windows\system32>
```



Active Directory Users and Computers

Name	Type	Description
Group88	Security Group ...	
User88	User	

Active Directory Users and Computer

- Saved Queries
- SamuelDomain.com
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Keys
 - LostAndFound
 - Managed Service Accounts
 - NewUsers
 - Program Data
 - PsNewOu

פקודה זו תוענת את מודול ה Active Directory ומאפשרת לך להשתמש בו cmdlet PowerShell כדי לנהל את Active Directory מסקריפט של.

\$baseDN = "DC=SamuelDomain,DC=com"

מגדיר את ה- DN הבסיסי עבור הדומיין

\$ou = "PsNewOu"

מגדיר את השם של היחידה הארגונית החדשה (OU) בדומיין.

\$user = "User88"

מגדיר את שם המשתמש החדש.

\$group = "Group88"

מגדיר את שם הקבוצה החדשה.

\$password = "1234qweR"

מגדיר סיסמה למשתמש חדש.

New-ADOrganizationalUnit

твор ייחידה ארגונית חדשה בשם שצוין בתיב שצווין ב-Active Directory.

New-ADUser

твор משתמש חדש עם הפרמטרים שצוינו, כגון שם חשבון (SamAccountName), שם פרטי (UserPrincipalName) ושם משפחתי, שם תצוגה, נתיב (OU) כולל סיסמה והפעלת חשבון.

New-ADGroup

твор קבוצה חדשה עם הפרמטרים שצוינו, כגון שם, היקף קבוצה (GroupScope), נתיב (OU).

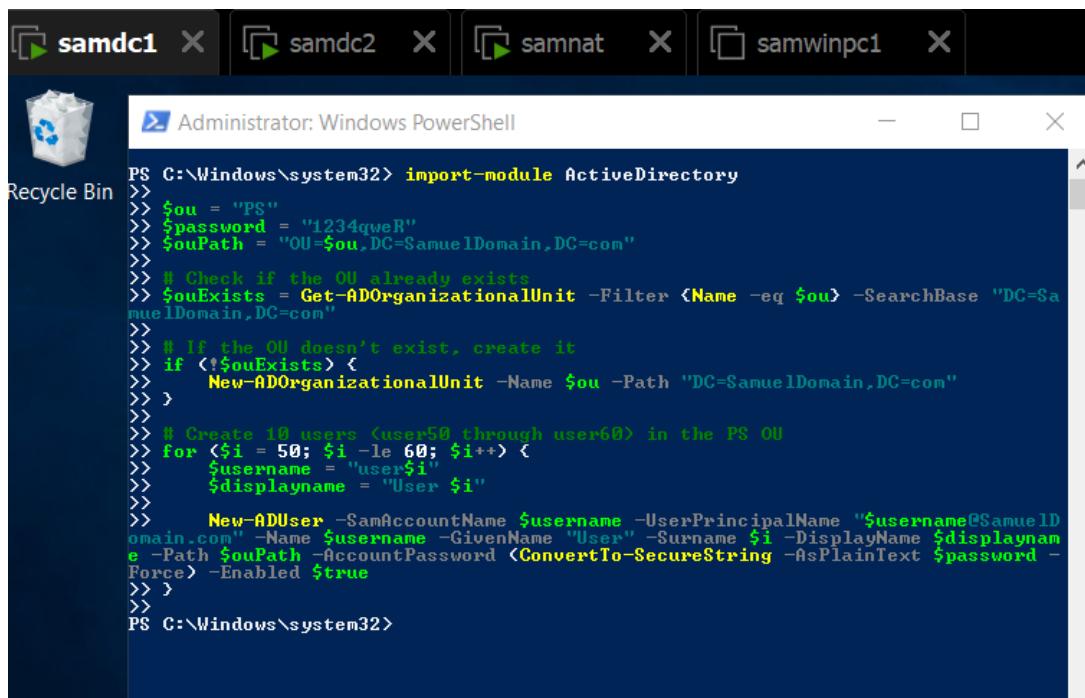
– Domain Controller –

צור 10 חשבונות חדשים ע"י script מbas סcript

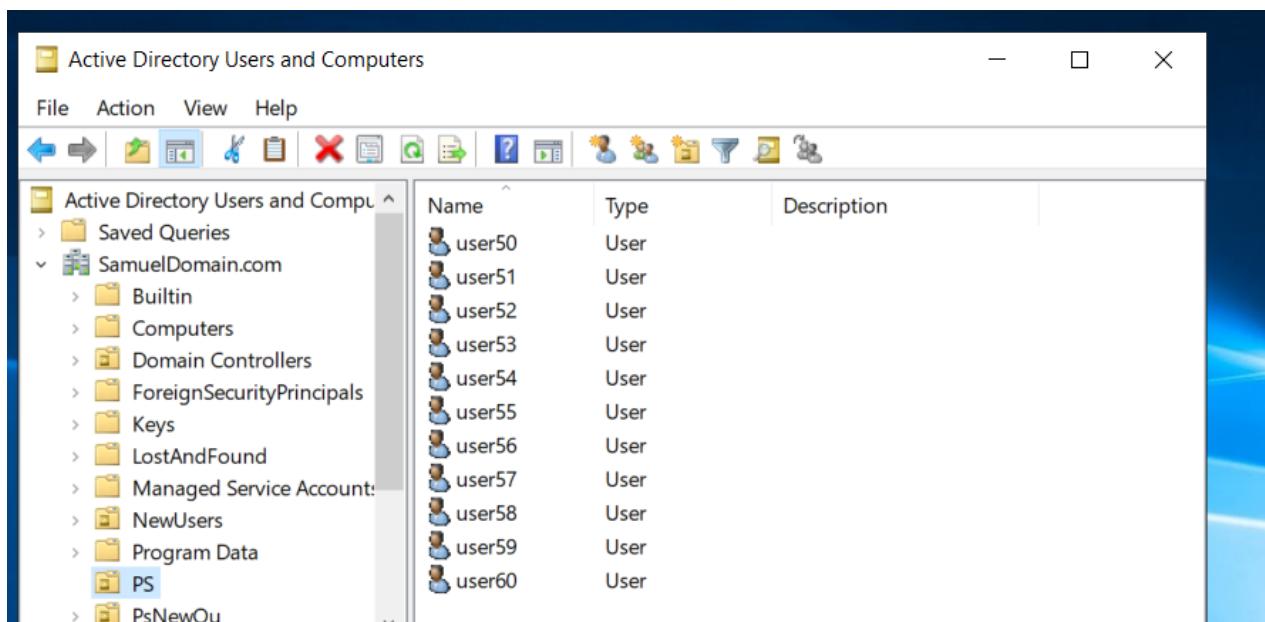
- כמעט אותו סקריפט כמו הקודם, רק כאן באמצעות פקודה מיוחדת, אנו יוצרים מהזור שיצר 10 משתמשים חדשים

`: { } for ($i = 50; $i -le 60; $i++)`

יציר loop ליצירת 10 משתמשים בשם "user50" עד "user60"



```
PS C:\Windows\system32> import-module ActiveDirectory
>>> $ou = "PS"
>>> $password = "1234qweR"
>>> $ouPath = "OU=$ou,DC=SamuelDomain,DC=com"
>>>
>>> # Check if the OU already exists
>>> $ouExists = Get-ADOrganizationalUnit -Filter {Name -eq $ou} -SearchBase "DC=SamuelDomain,DC=com"
>>>
>>> # If the OU doesn't exist, create it
>>> if (!$ouExists) {
>>>     New-ADOrganizationalUnit -Name $ou -Path "DC=SamuelDomain,DC=com"
>>> }
>>>
>>> # Create 10 users (user50 through user60) in the PS OU
>>> for ($i = 50; $i -le 60; $i++) {
>>>     $username = "user$i"
>>>     $displayname = "User $i"
>>>
>>>     New-ADUser -SamAccountName $username -UserPrincipalName "$username@SamuelDomain.com" -Name $username -GivenName "User" -Surname $i -DisplayName $displayname -Path $ouPath -AccountPassword (ConvertTo-SecureString -AsPlainText $password -Force) -Enabled $true
>>> }
>>>
PS C:\Windows\system32>
```

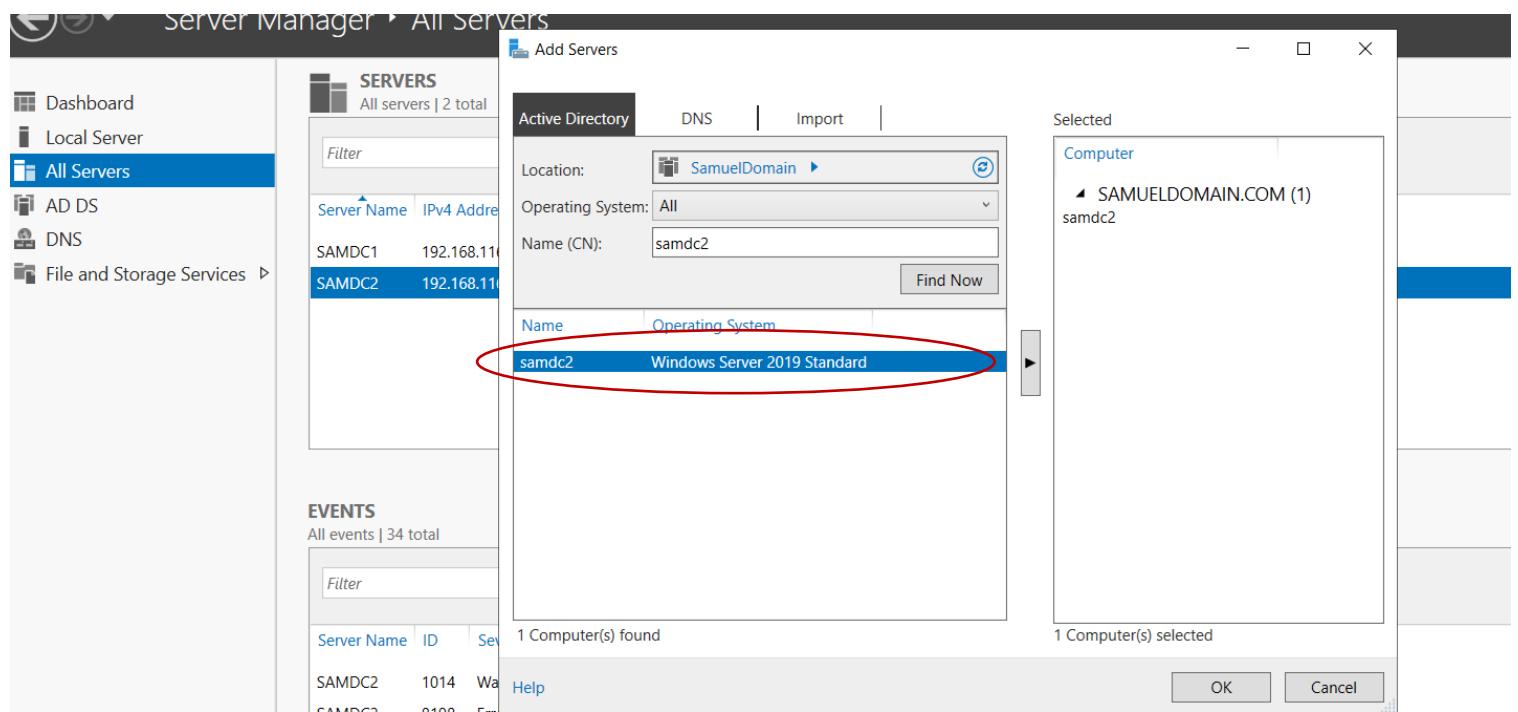


Name	Type	Description
user50	User	
user51	User	
user52	User	
user53	User	
user54	User	
user55	User	
user56	User	
user57	User	
user58	User	
user59	User	
user60	User	

- Domain Controller -

• בדוק של השינויים ב-AD מסונכרנים בין 2 שרתי DC

- הוספהו שרת שני לשרת הראשון ב-SERVER MANAGER כדי שאוכל לנהל את שניהם ביחד, וגם לבדוק אם AD מסונכרנת

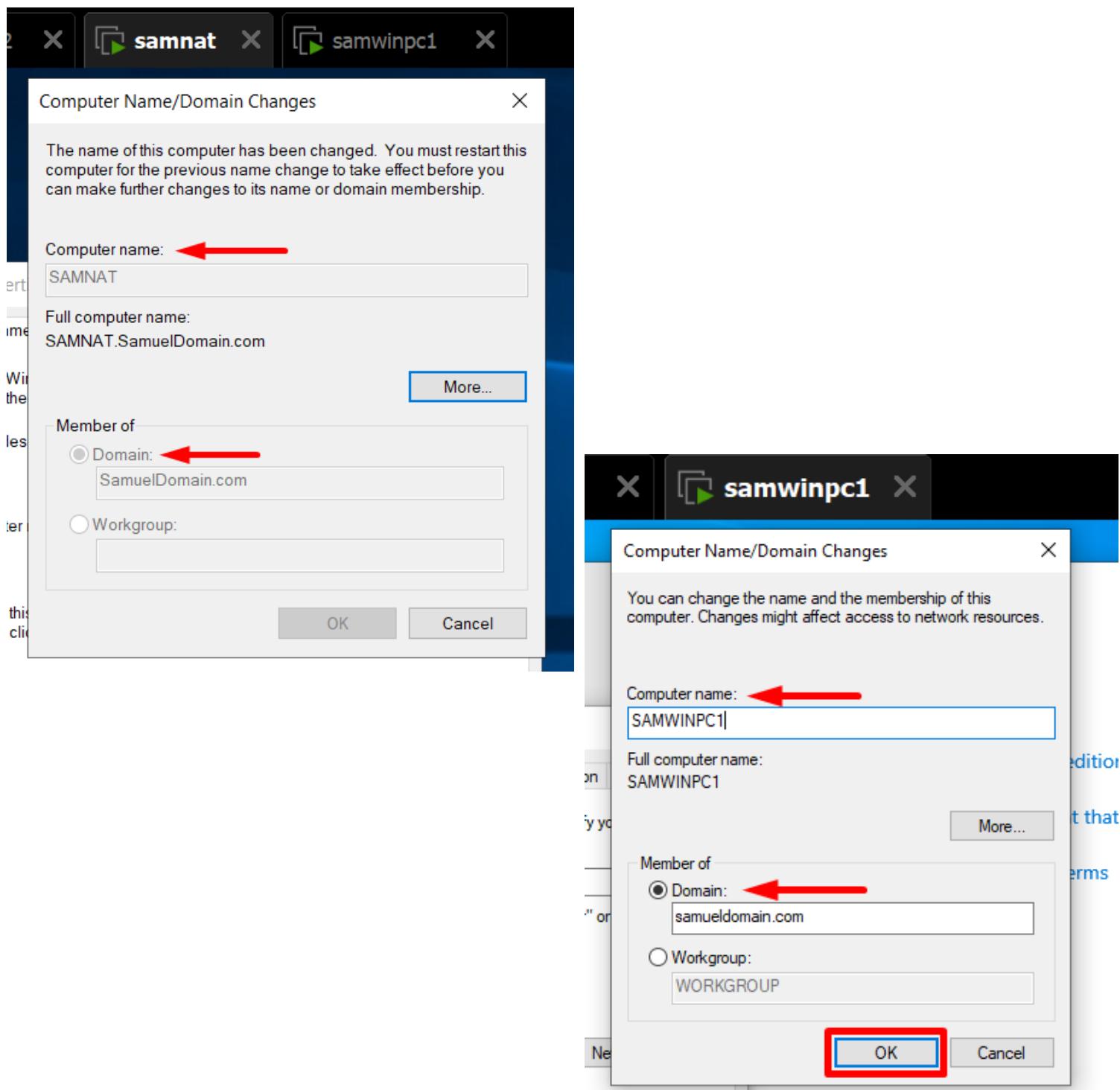


This screenshot shows two instances of the Active Directory Users and Computers (ADUC) console side-by-side. Both instances have the URL 'samdc1.SamuelDomain.com' in their titles. The left instance shows the 'samdc1' domain with several user objects listed. The right instance shows the 'samdc2' domain with similar user objects. Red arrows point from the bottom of the left window to a 'PS' object in the left tree and a 'PcNewOu' folder in the right tree, and from the bottom of the right window to a 'PS' object in the right tree and a 'PcNewOu' folder in the left tree, indicating synchronization issues between the two domains.

- צורף המחשבים ל- Domain



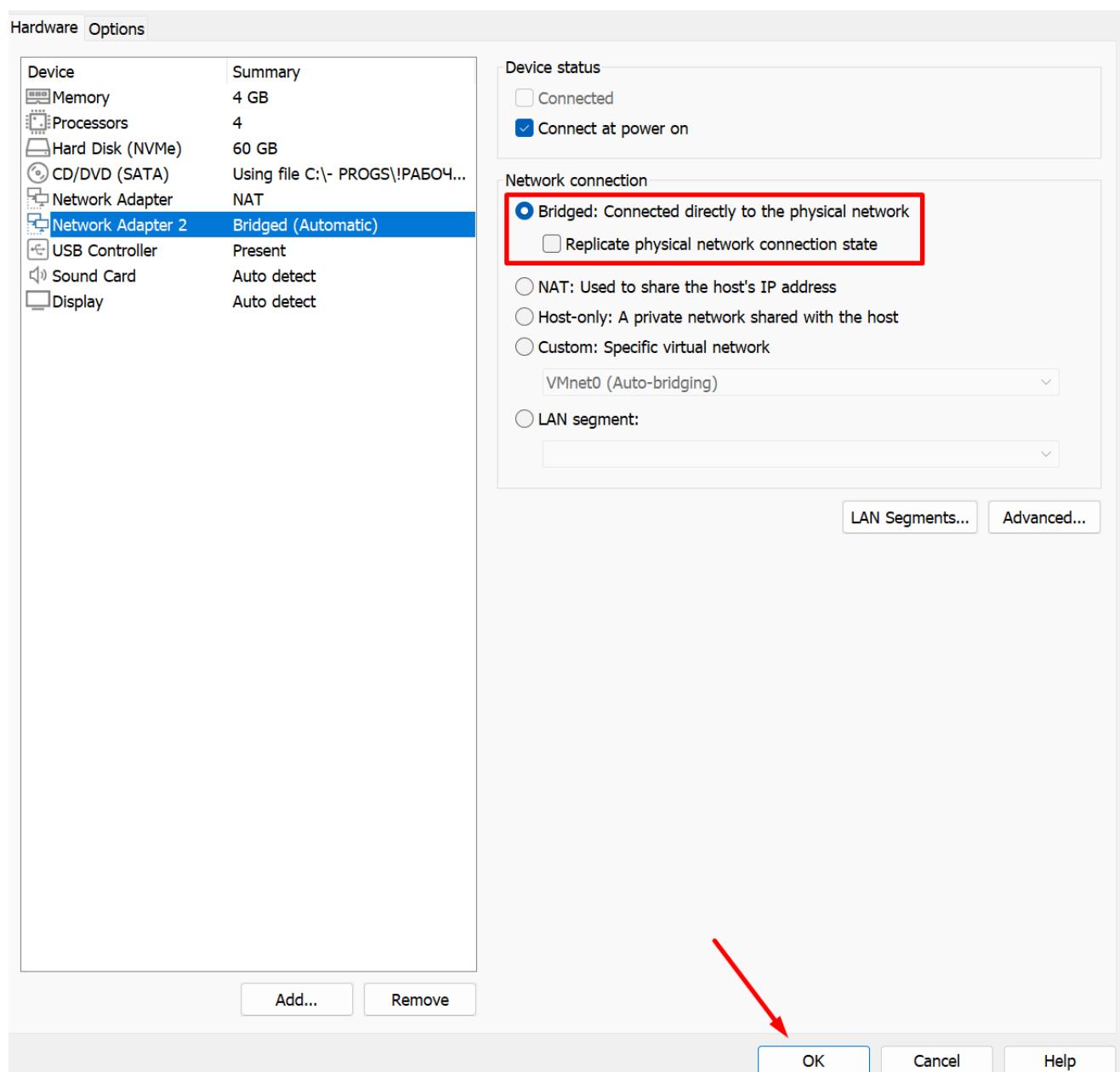
כבר הוספנו שרתים 2-DC1 ו- PC1 ל-SAMNAT



- PAT / NAT -

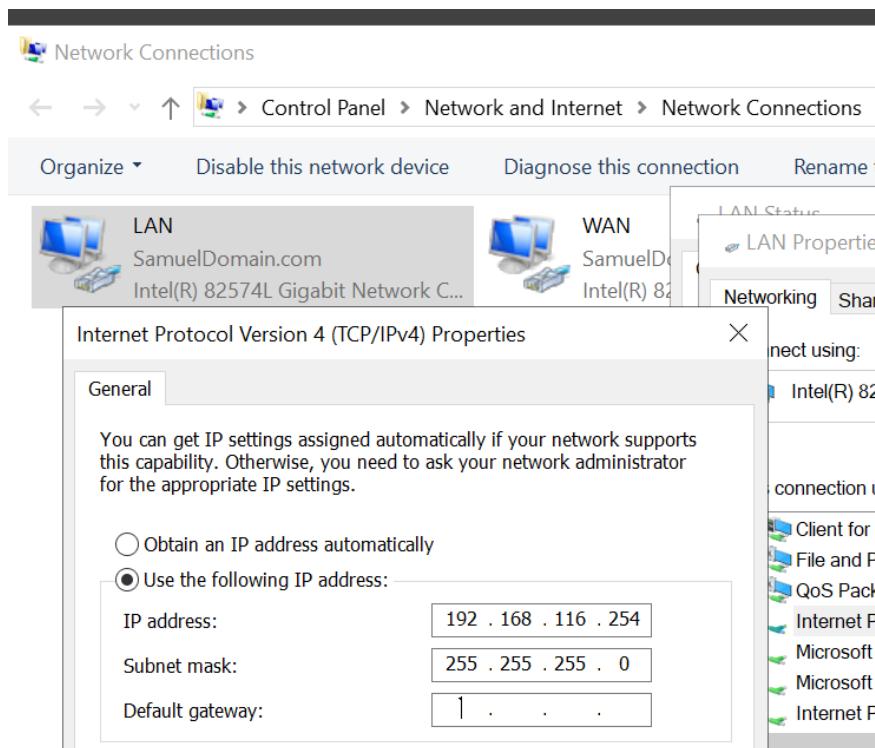
PAT הוא סוג של פרוטוקול NAT שמתרגם פורטים של התקנים בתוך רשת מקומית. זה מאפשר למספר מכשירים ברשות מקומית להשתמש באותה כתובת IP ציבורית, אך עם יציאות שונות כדי להבטיח שכל מכשיר מזוהה באופן ייחודי.

- כדי שהוא יעבוד בסימולציה שלנו, علينا יש להגדיר את התוכנית שלנו ולתת לשרת SAMNAT סיום להיות בין רשתות BRIDGE



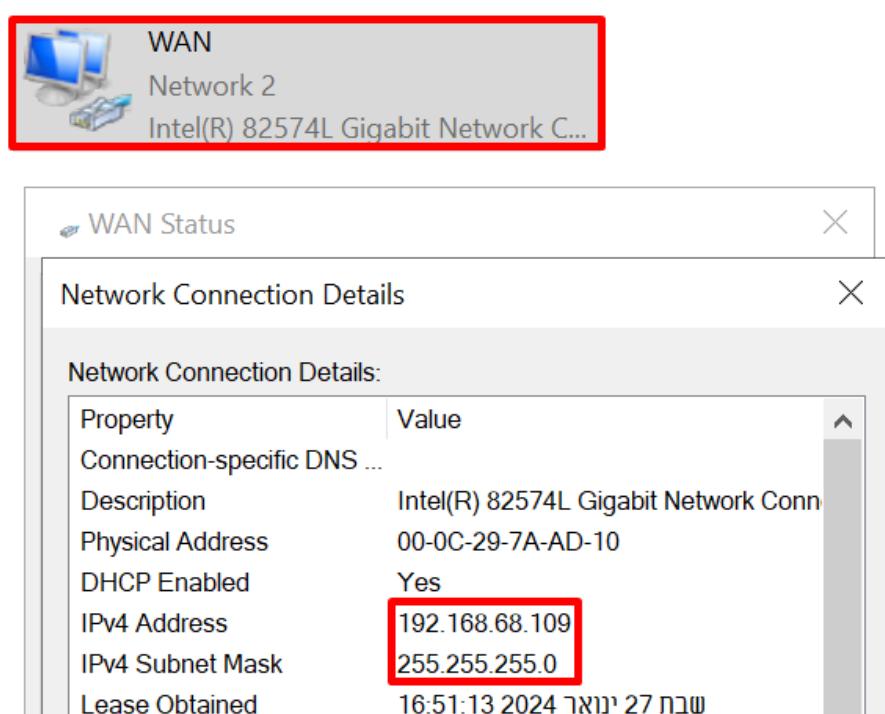
- PAT/NAT -

- כأن אנו יכולים לראות שיצרנו 2 כרטיסי רשת, משק אחד עבור לרשת המקומית שלנו, ואחד עבור לרשת החיצונית



כתובת של רשת שלנו

192.168.116.0 /24



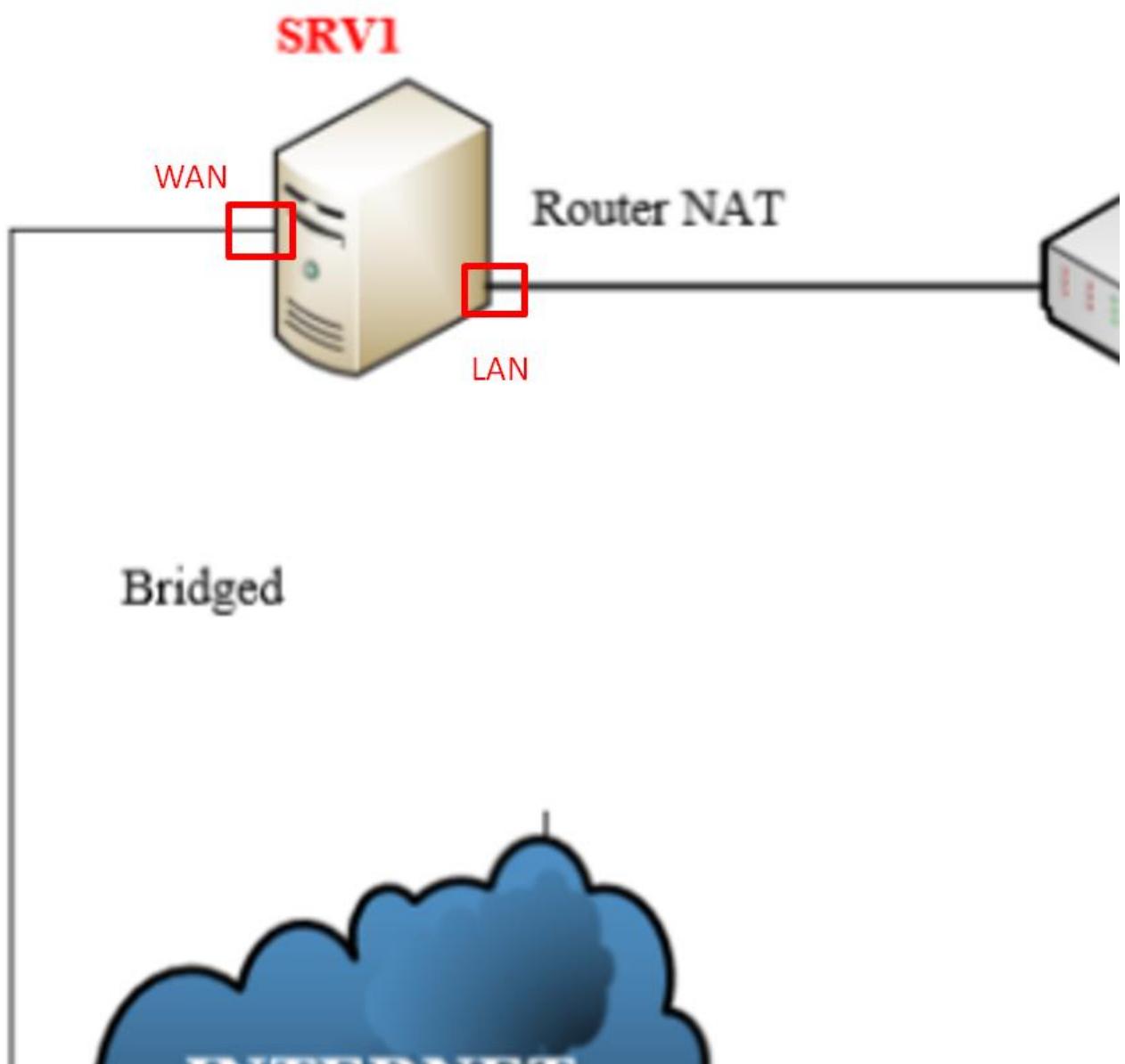
כתובת של רשת חיצונית

192.168.68.0 /24

- PAT/NAT -

• ונראה הכל ככה

השרת SAMNAT ישתמש כנתב



- PAT/NAT -

- כתת עליינו יש להתקין את פרוטוקול NAT בשרת שלנו.

Select server roles

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results

Select one or more roles to install on the selected server.

Roles

- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server
- Fax Server
- File and Storage Services (1 of 12 installed)
- Host Guardian Service
- Hyper-V
- Network Policy and Access Services
- Print and Document Services
- Remote Access**
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)
- Windows Deployment Services
- Windows Server Update Services

Description

Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.

< Previous **Next >** Install Cancel

DESTINATION SERVER
SAMNAT.SamuelDomain.com

Add Roles and Features Wizard

Select role services

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results

Select the role services to install for Remote Access

Role services

- DirectAccess and VPN (RAS)
- Routing**
- Web Application Proxy

Description

Routing provides support for NAT Routers, LAN Routers running BGP, RIP, and multicast capable routers (IGMP Proxy).

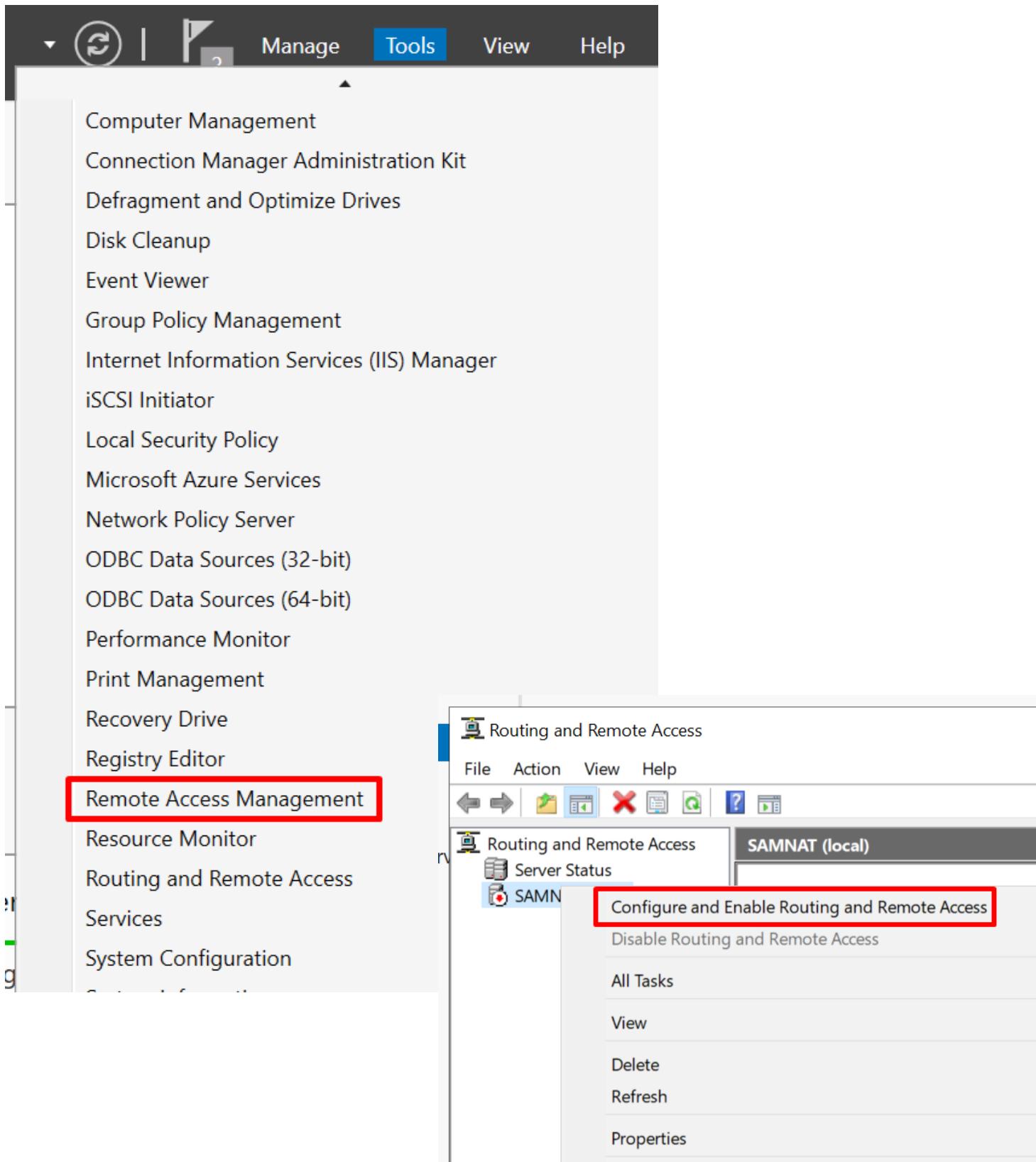
< Previous **Next >** Install Cancel

DESTINATION SERVER
SAMNAT.SamuelDomain.com

מורידים
ראוטינג

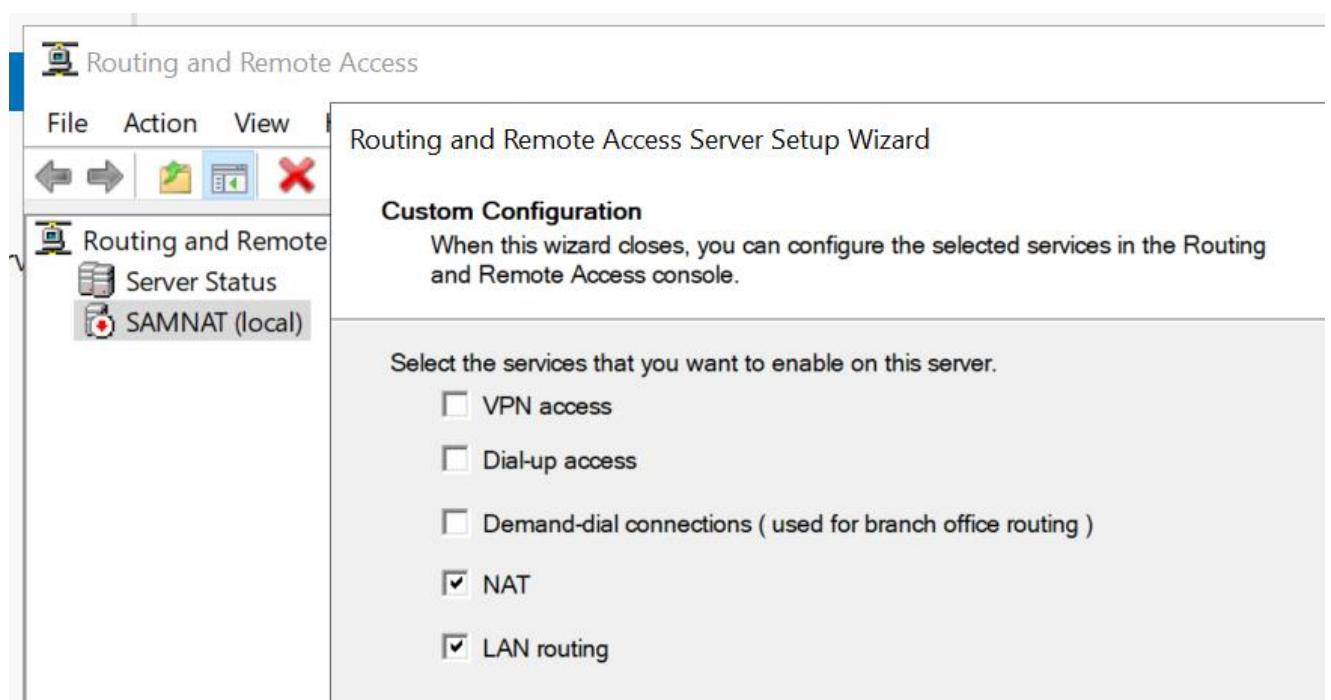
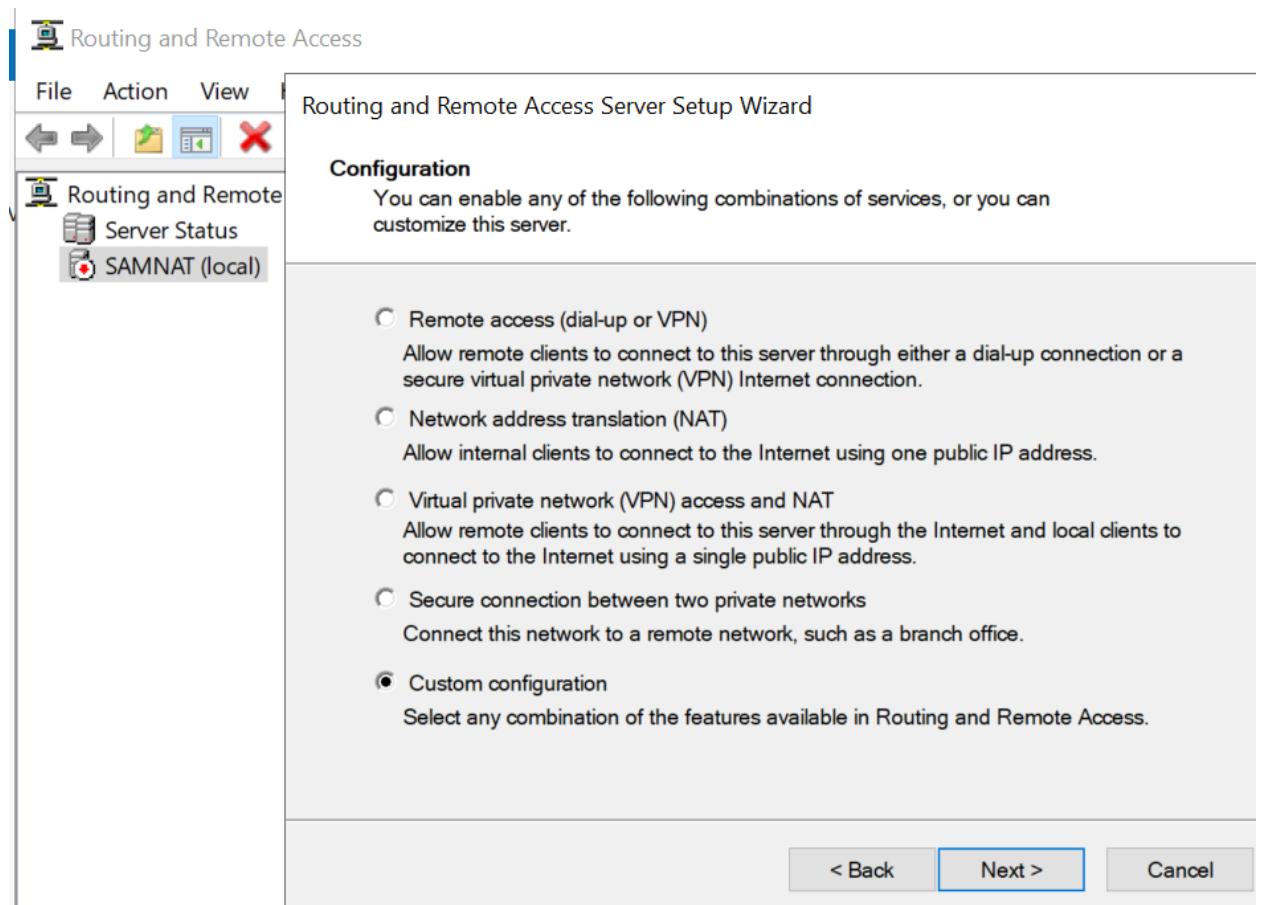
- PAT/NAT -

- כפי שאפשר לראות, פונקציית ניתוב הופיעה בכליים שלנו,
אז בואו נעבור להתקנה



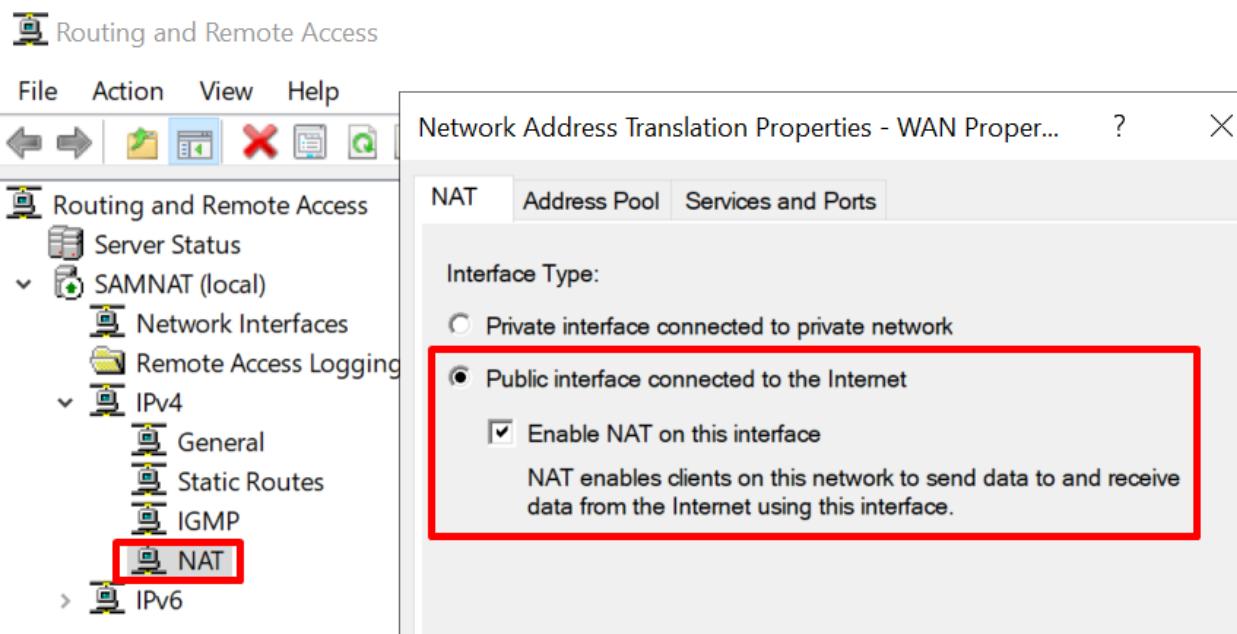
- PAT/NAT -

- אנו בוחרים התקנה CUSTOM מכיוון ששאר הfonקציות לא מעניינות אותנו, ובוחרים בפרוטוקול NAT גם את ניתוב של LAN



- PAT/NAT -

- אנו מפעילים את מערכת NAT-עצמה, בודקים את הפינג ורואים שהוא מגע לשרת גוגל משרת אחר שלנו DC1



nat X | samdc1 X | samdc2 X | samwinpc1 X

Command Prompt

```
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Avocado>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=5ms TTL=115
Reply from 8.8.8.8: bytes=32 time=5ms TTL=115
Reply from 8.8.8.8: bytes=32 time=5ms TTL=115
Reply from 8.8.8.8: bytes=32 time=4ms TTL=115

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms

C:\Users\Avocado>
```

- PAT/NAT -

- מחשבים אחרים :

PC1:

```
! samdc2 X || samwinpc1 X
Command Prompt
Microsoft Windows [Version 10.0.19045.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Win User>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=5ms TTL=115
Reply from 8.8.8.8: bytes=32 time=4ms TTL=115
Reply from 8.8.8.8: bytes=32 time=4ms TTL=115
Reply from 8.8.8.8: bytes=32 time=5ms TTL=115

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 5ms, Average = 4ms

C:\Users\Win User>
```

DC2:

```
! mdc1 X || samdc2 X || samwinpc1 X
Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Avocado>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=5ms TTL=115
Reply from 8.8.8.8: bytes=32 time=5ms TTL=115
Reply from 8.8.8.8: bytes=32 time=5ms TTL=115
Reply from 8.8.8.8: bytes=32 time=4ms TTL=115

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 5ms, Average = 4ms
```

- DHCP -



מה המשמעות של פרוטוקול זה באופן כללי ? הוא פרוטוקול רשות המקצה באופן אוטומטי כתובות IP ופרמטרים אחרים של רשות להתקנים בראשת, מה שמקל עליהם להתחבר לרשת ללא צורך בתצורה ידנית.

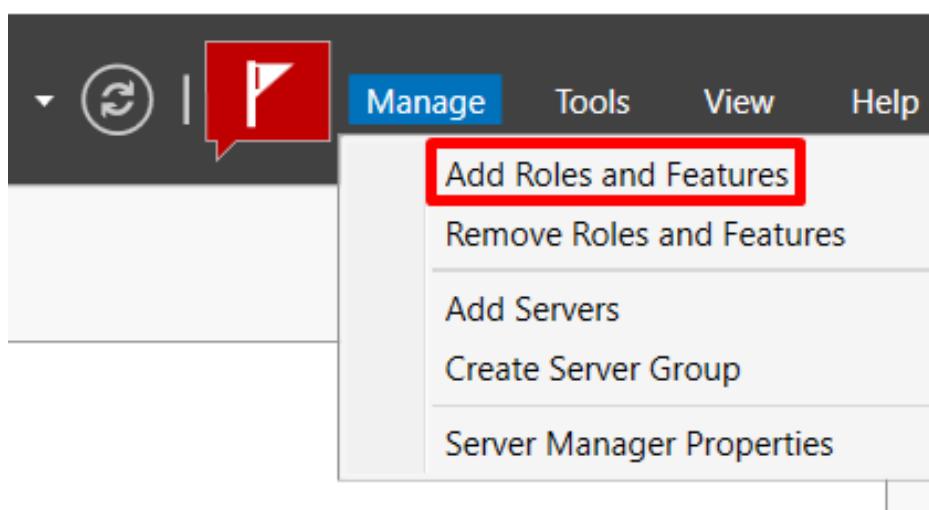
- ועכשו אנחנו נגידו את הפרוטוקול ב DC1-הגדרתי כתובות סטטיות בכל השירותים בתרגילים קודמות כדי למנוע התנגשויות כתובות ובסביל זמינות מתמדת לשירותים

תע 1- כתובת IP קבועה והתקן עליו שירות DC1

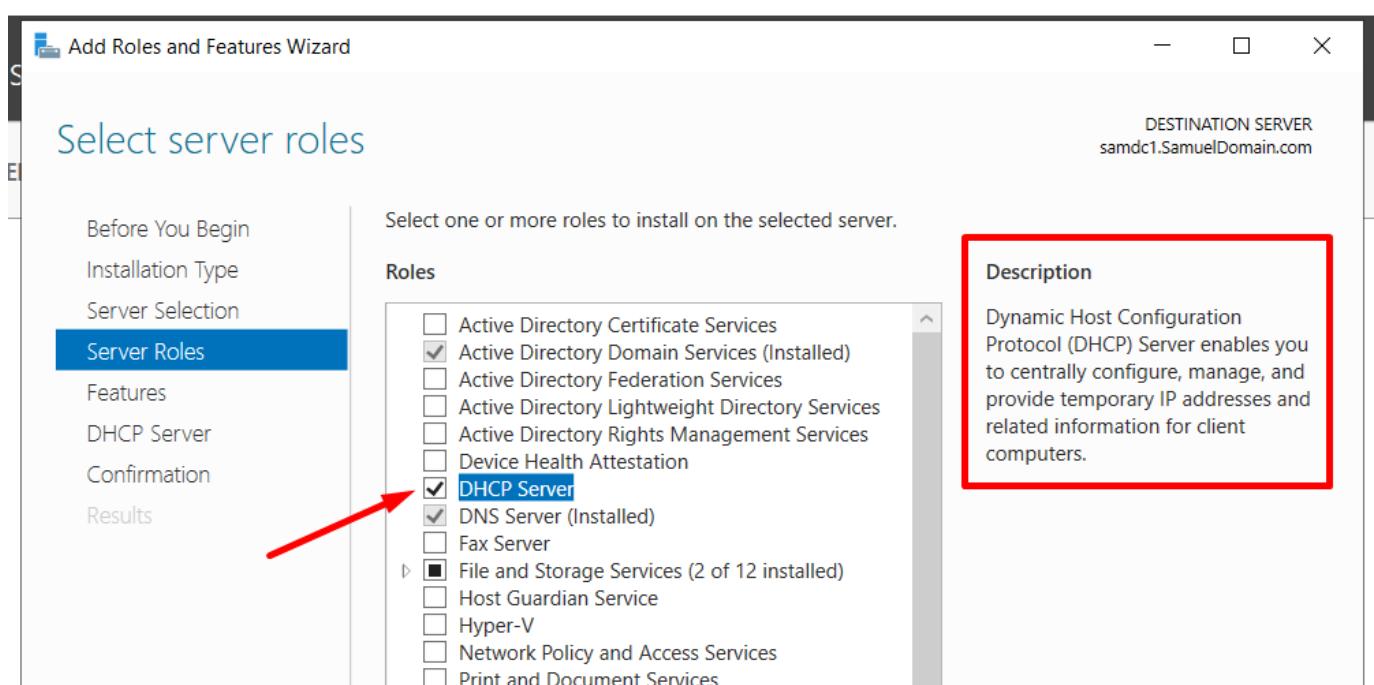
The figure consists of three side-by-side screenshots of Windows network configuration windows. Each window is titled 'Internet Protocol Version 4 (TCP/IPv4) Properties'.
1. The first window is for 'samnat' and shows the 'General' tab selected. It has two radio button options: 'Obtain an IP address automatically' (unchecked) and 'Use the following IP address' (checked). Below this are fields for 'IP address' (192.168.116.254), 'Subnet mask' (255.255.255.0), and 'Default gateway' (left empty). At the bottom are fields for 'Preferred DNS server' (192.168.116.200) and 'Alternate DNS server' (192.168.116.201).
2. The second window is for 'samdc1' and shows the 'General' tab selected. It has the same radio button options and field layout as the first window.
3. The third window is for 'samdc2' and shows the 'General' tab selected. It has the same radio button options and field layout as the first window.
In all three windows, the 'General' tab is selected, and the 'Use the following IP address' option is checked. The IP address is set to 192.168.116.200, the subnet mask to 255.255.255.0, and the default gateway to 192.168.116.254. The DNS tab is also visible in each window, showing the 'Use the following DNS server addresses' option selected with the preferred DNS server at 192.168.116.200 and the alternate DNS server at 192.168.116.201.

- DHCP -

- נעבר להתקנת תפקיד ה- DHCP עצמו על ידי התקנתו ב Server Manager



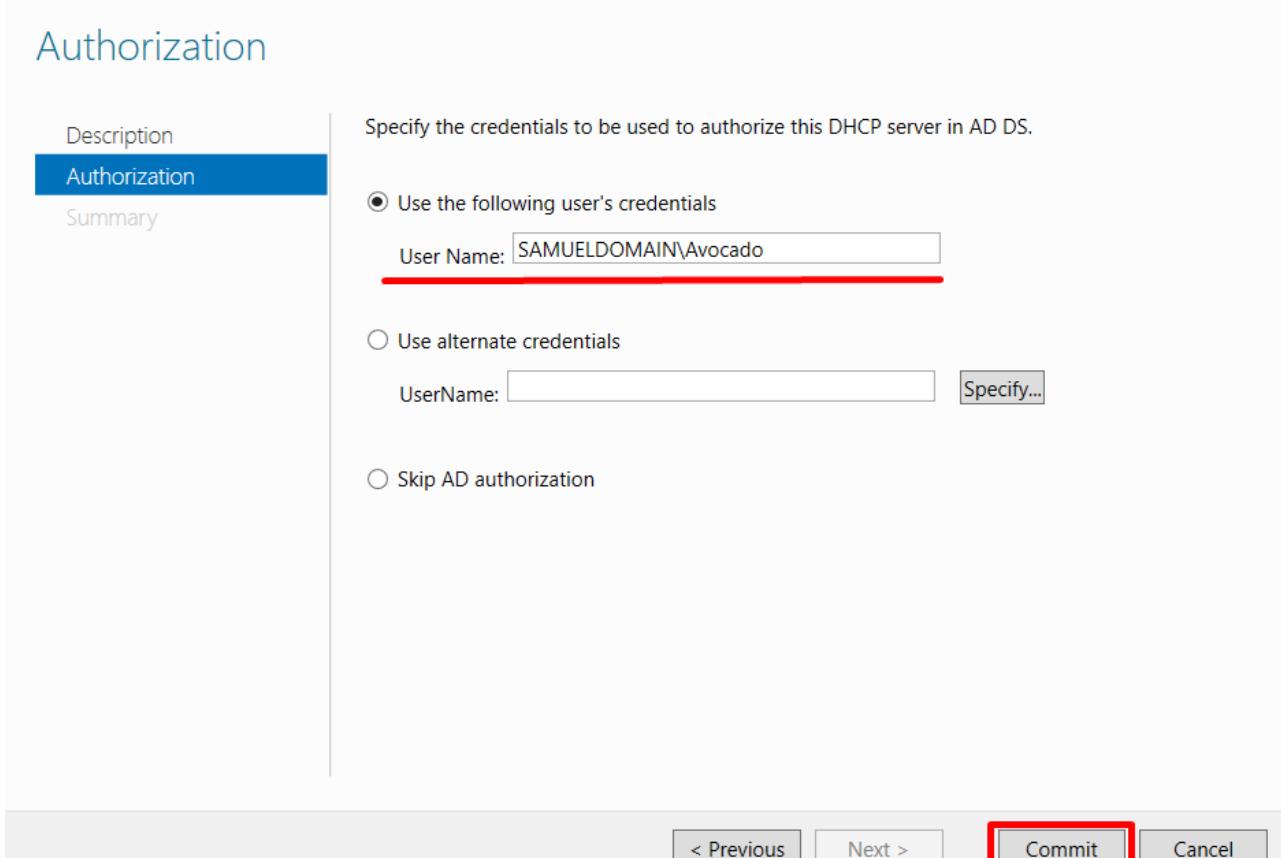
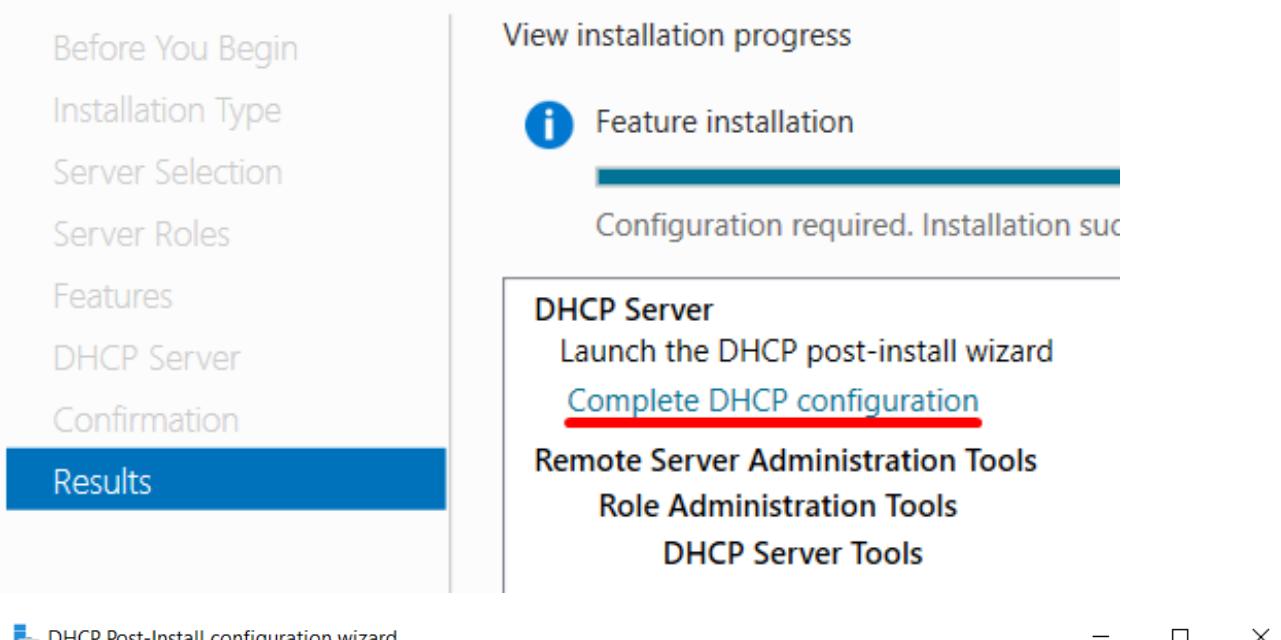
- מתקינים את ה תפקיד



- DHCP -

- לאחר ההתקנה, אנו ממשיכים להרשאת המנהל שלנו (אבותקו) בـ **DHCP Role**

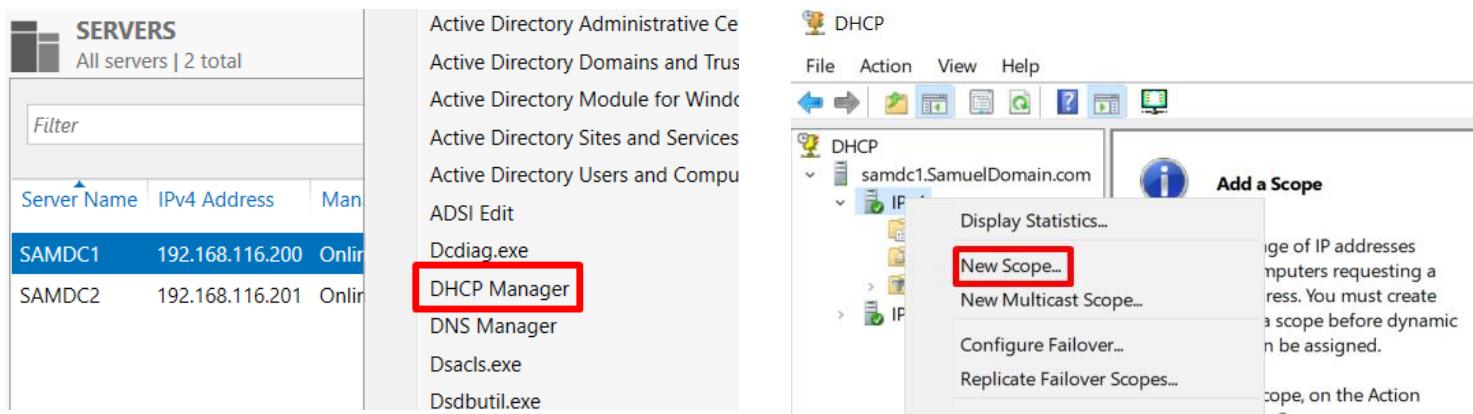
Installation progress



- DHCP -

הגדיר Scope שמחلك 50 כתובות

- כעת علينا ליצור מאגר כתובות ששותף על ידי DHCP

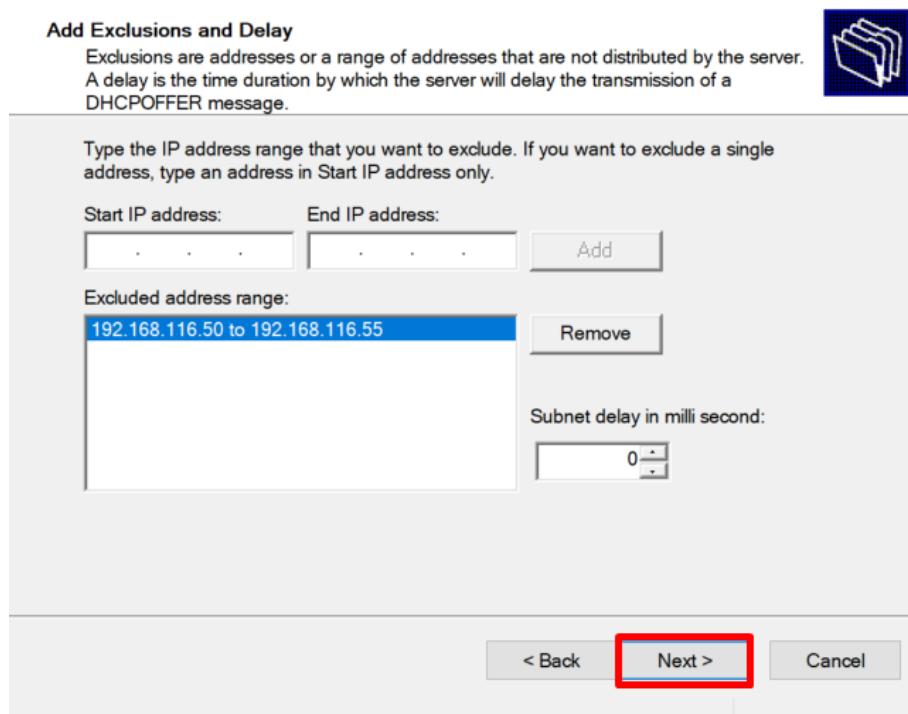


- DHCP -

הגדך של חמש כתובות ראשונות מתוך Scope-

- אנו לא כוללים 1+5 כתובות שהפרוטוקול יחלק ממאג'ר כתובות, למשל שירותים שפועלם ברכזיות וזקוקים לזמןנות מתמדת, אז כתובות הללו יהיו סטטיות

New Scope Wizard

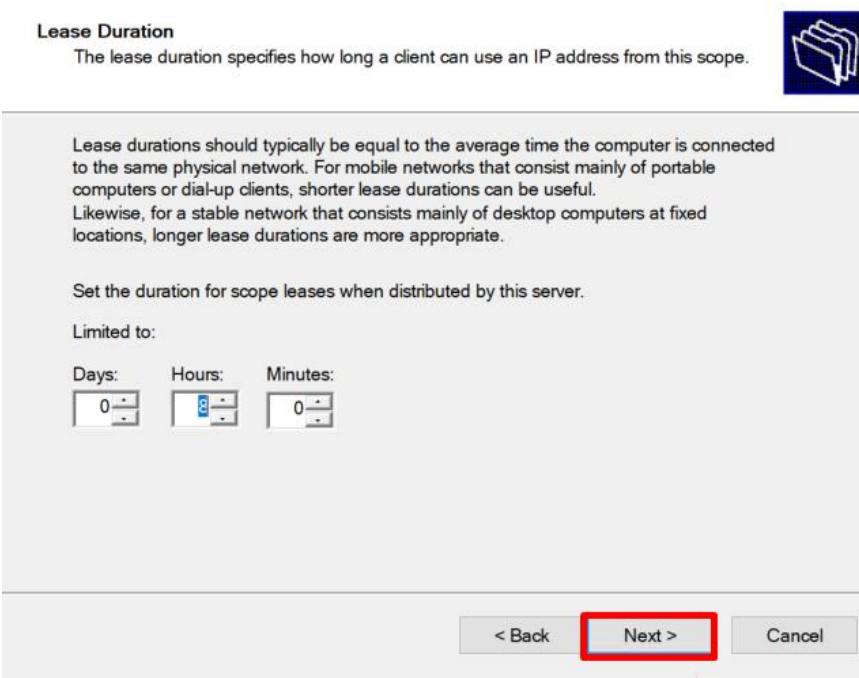


- DHCP -

- הגדך של 8 שעות Lease -

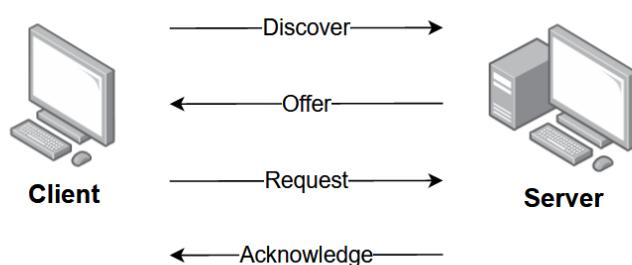
- אנו מגבילים את הכתובות בזמן, במקרה שלנו ל-8 שעות, ולאחר מכן DHCP חוזר שוב על התהליך שנקרא DORA

New Scope Wizard



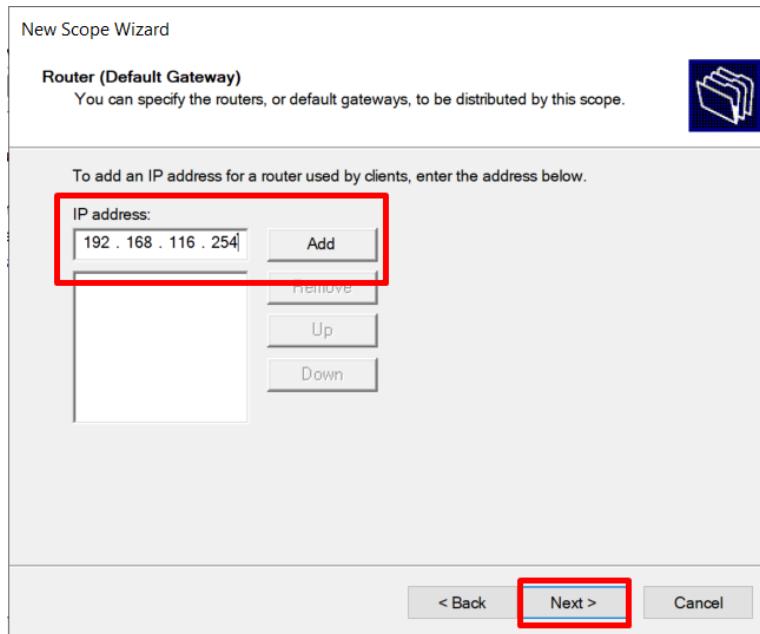
אבל למה אנחנו צריכים להגביל כתובות בזמן? ומהו תהליך DORA?

1. לדוגמה עוזב יכול לעזוב את תפקידו, אך הכתובת תישאר ובעגל זה הפרטוקול הוא דינמי ויש מוגבלת זמן לכל כתובות, חוץ מכתובות סטטי כמו בונוס, וזה אחת מהסיבות
2. תהליך DORA הוא רצף של שלבים בפרטוקול DHCP שבו הלקוח מבקש ומתקבל כתובת IP משרת DHCP

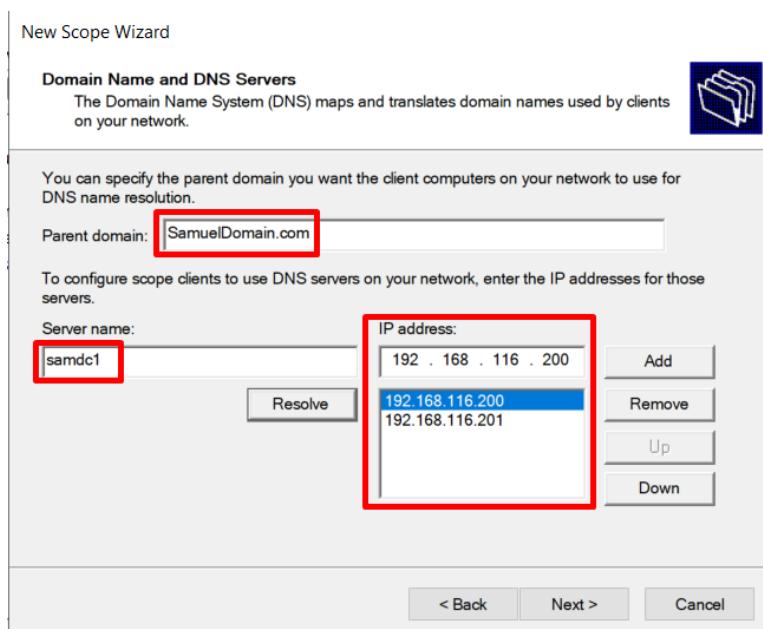


- DHCP -

- הגדכנו את כתובת Default Gateway שלנו, זה שרת SAMNAT שלו (נתב ברשת)



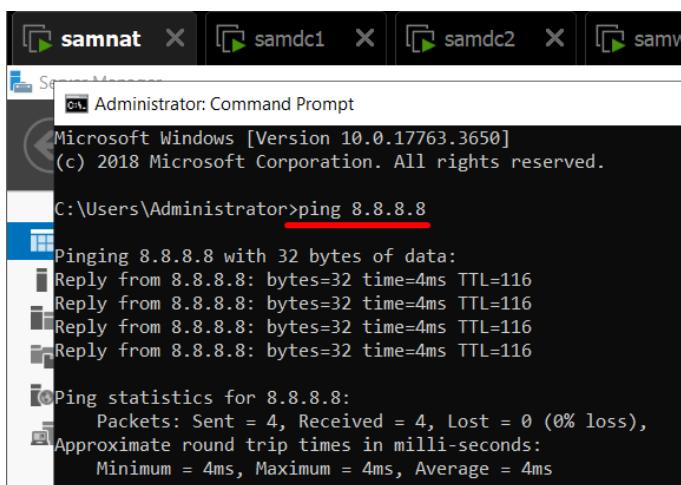
- מוסיפים את שרתי DNS-שלנו DC1-2 עם השמות שלהם



- DHCP -

בדיקה קישוריות – בדוק ש WIN10 מקבל IP בצורה אוטומטית
מחשרת DHCP ובזוק שיש Ping בין כל המחשבים. בזוק שניין לבצע Ping מ-SRV1 לאינטרנט.

- בזוקים אם חיבור לאינטרנט פועל על(SAMNAT)



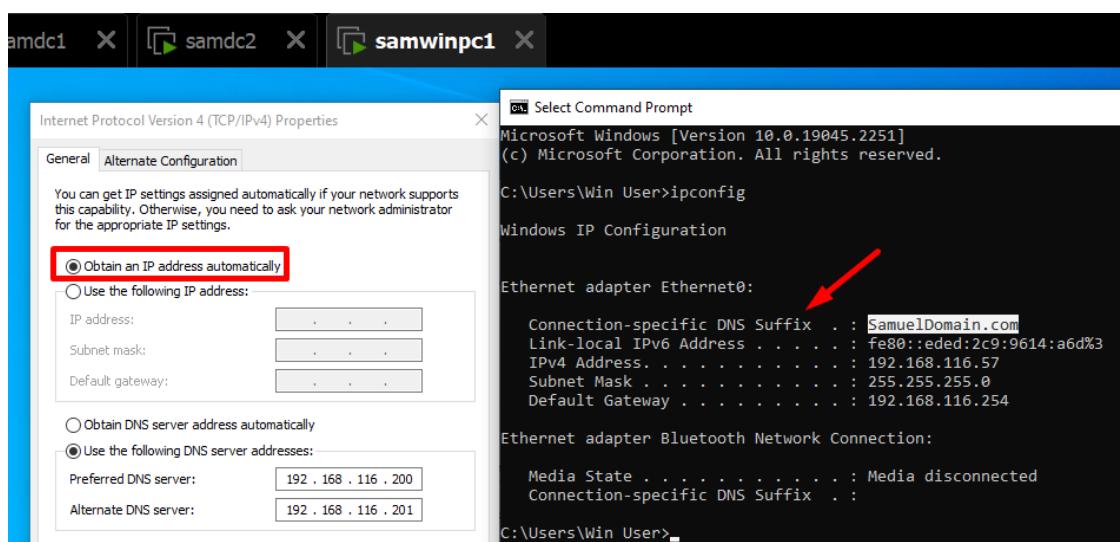
```
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=4ms TTL=116

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

- PC1 קיבל את הכתובת משרת DHCP אוטומטי



- DHCP -

- בדוקים אם יש חיבור בין כל המחשבים ברשת

```
C:\Users\Win User>ping samdc1

Pinging samdc1.samueldomain.com [192.168.116.200] with 32 bytes of data:
Reply from 192.168.116.200: bytes=32 time=1ms TTL=128
Reply from 192.168.116.200: bytes=32 time<1ms TTL=128
Reply from 192.168.116.200: bytes=32 time<1ms TTL=128
Reply from 192.168.116.200: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.116.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Win User>ping samdc2

Pinging samdc2.samueldomain.com [192.168.116.201] with 32 bytes of data:
Reply from 192.168.116.201: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.116.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Win User>ping samnat

Pinging samnat.SamuelDomain.com [192.168.116.254] with 32 bytes of data:
Reply from 192.168.116.254: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.116.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

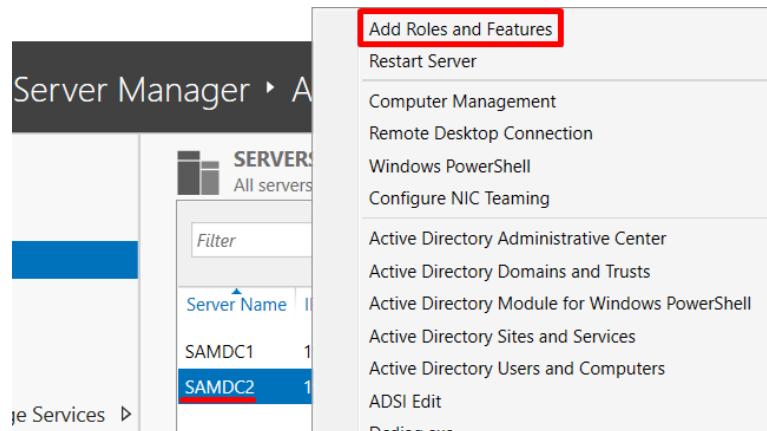
- DHCP -

צור DC2 עם שרת Failover cluster

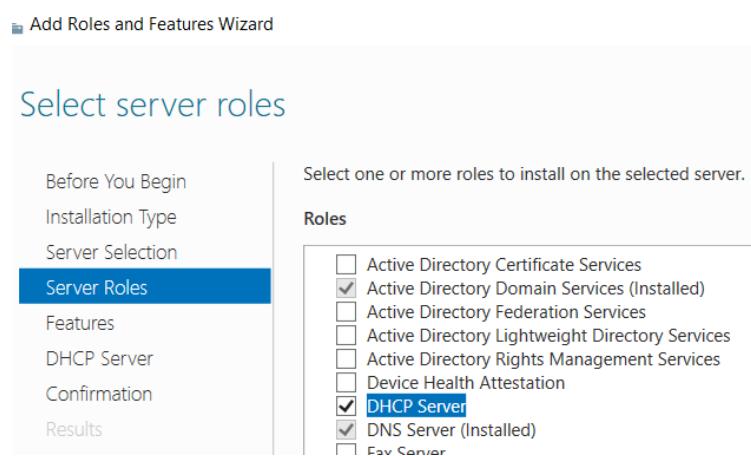
11

DHCP פירשו בדרך כלל קבוצה של שירותי DHCP המוגדרים בצורה כזו שאם אחד השירותים נופל אז שרת אחר לוקח אוטומטית על עצמו את האחריות על השירות ללקוחות. זה מבטיח המשכיות של שירות DHCP

- עכשו בואו נתקן את התפקיד הזה בשרת DC2

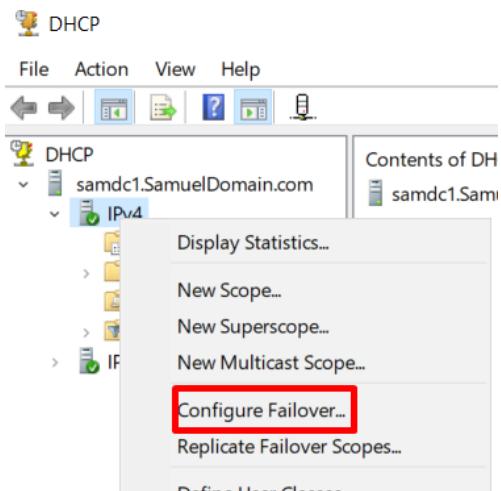


- ההתקנה היא בדיק כמו בשרת הראשון

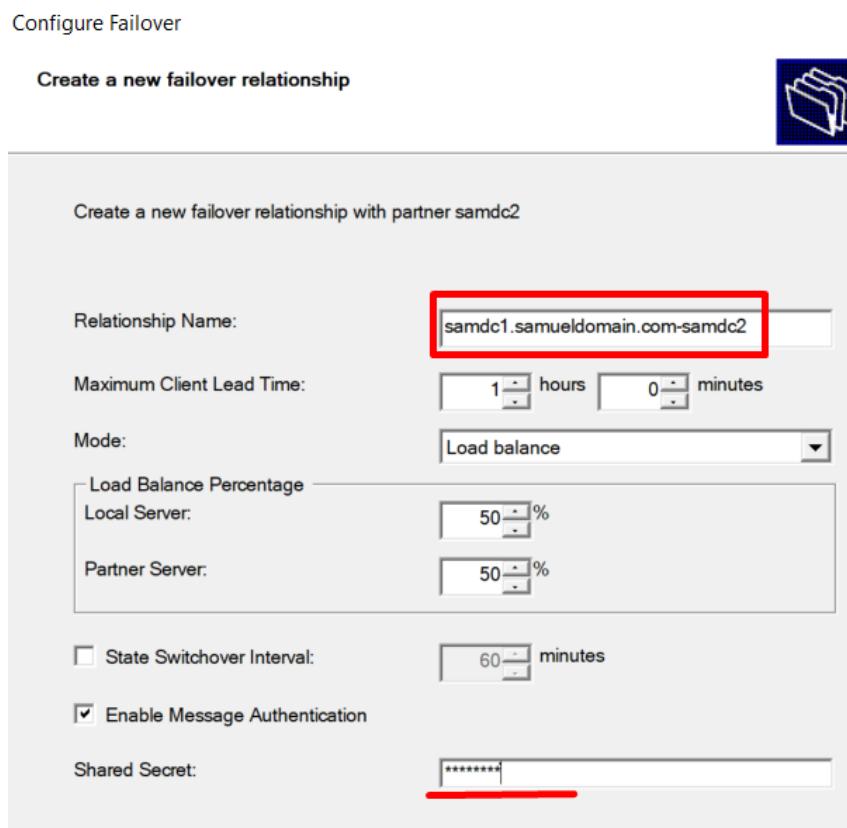


- DHCP -

- בשרת הראשון מוסיפים שרת השני



- אנו מקצים עומס ביניהם, ומגדירים סיסמה



- ניהול השירות מרוחק -



לפנינו נוצרו את קבוצת Sys_admins, בעת נגדיר עבורם גישה מרוחק לכל השירותים

אפשר למחוקת Sys Admins לנהל את השירותים
Remote Desktop, בעזרת WIN10

- bullet point **bullet point** בעת אנו הולכים לכל שרת, מאפשרים גישה מרוחק ומוסיפים את קבוצת ניהול שלנו מ-AD

SysAdmins_group Properties

Members:

Name	Active Directory Domain Services Folder
User 3	SamuelDomain.com/Sys_Admins
User 4	SamuelDomain.com/Sys_Admins

Server Manager

System Properties

Remote Desktop Users

Administrator already has access.

Add... Remove

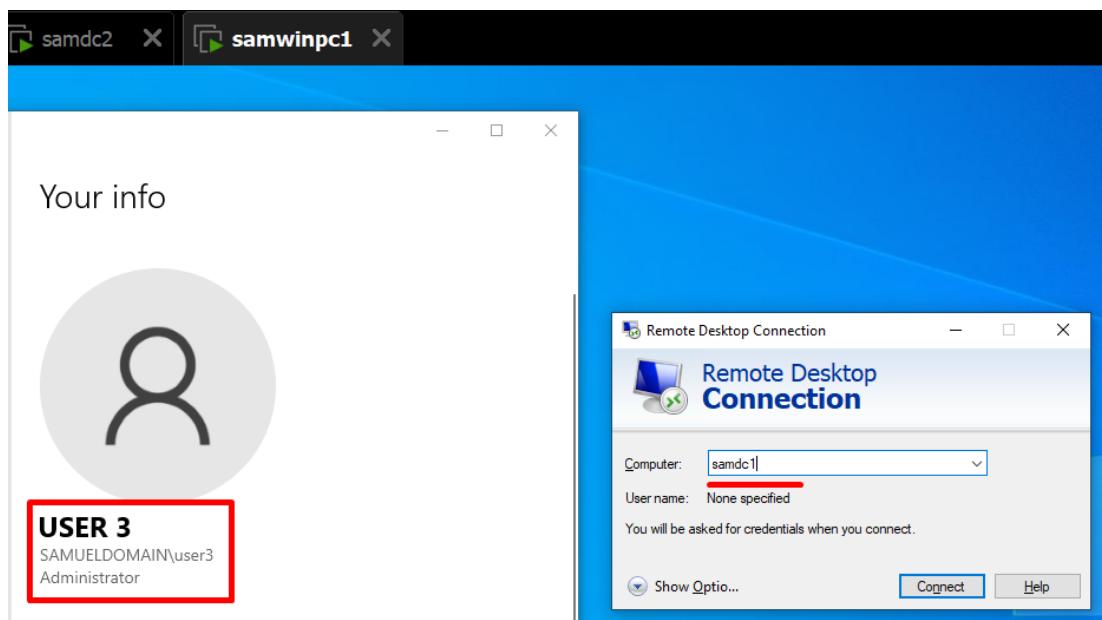
OK Cancel

See also

Product ID: 00429-70000-00000-AA282

- ניהול השירות מרוחק -

- נבדוק אם החיבור עובד ואני יכול להתחבר לשרתים דרך המستخدم USER 3 שהוא המנהל, דרך PC1



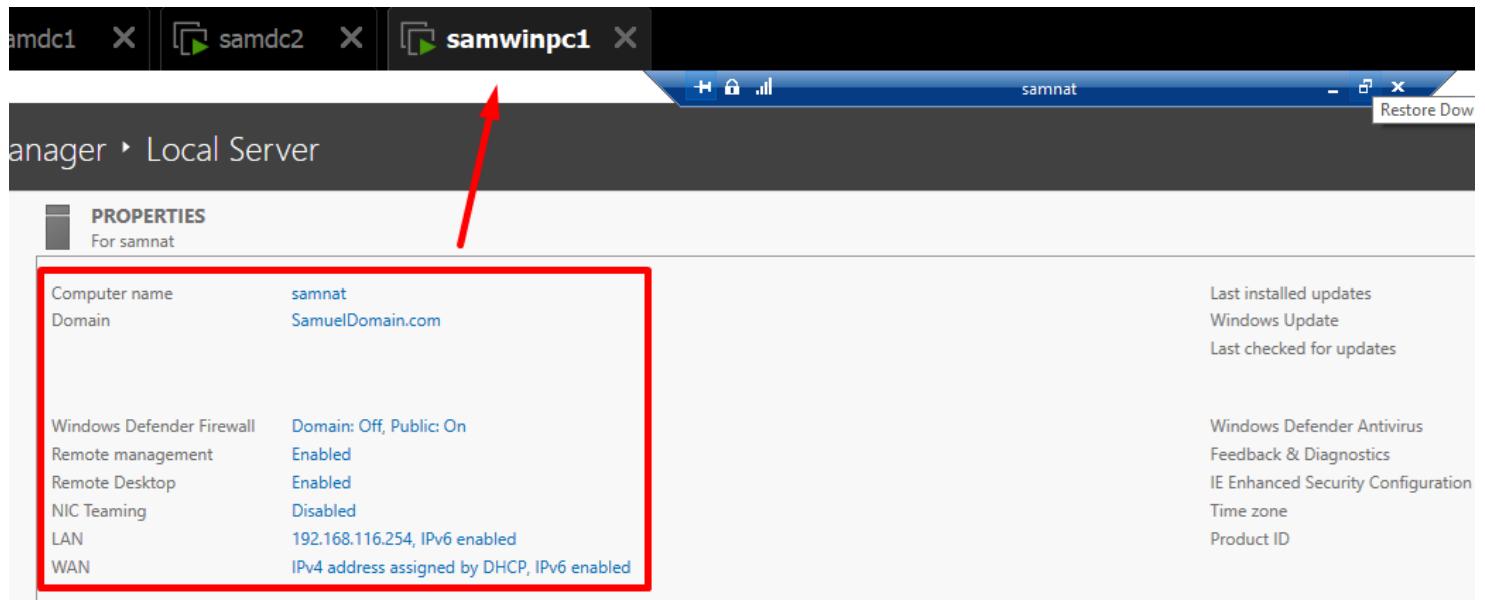
The screenshot shows the Windows Control Panel under 'Local Server' settings. It displays the properties for the computer 'samdc1'. The 'PROPERTIES' section includes:

Computer name	samdc1	Last installed updates
Domain	SamuelDomain.com	Windows Update
Windows Defender Firewall	Public: On	Last checked for updates
Remote management	Enabled	Windows Defender Antivirus
Remote Desktop	Enabled	Feedback & Diagnostics
NIC Teaming	Disabled	IE Enhanced Security Configuration
Ethernet0	192.168.116.200, IPv6 enabled	Time zone
		Product ID

The screenshot shows the Windows Control Panel under 'Local Server' settings. It displays the properties for the computer 'samdc2'. The 'PROPERTIES' section includes:

Computer name	samdc2	Last installed updates
Domain	SamuelDomain.com	Windows Update
Windows Defender Firewall	Domain: On	Last checked for updates
Remote management	Enabled	Windows Defender Antivirus
Remote Desktop	Enabled	Feedback & Diagnostics
NIC Teaming	Disabled	IE Enhanced Security Configuration
Ethernet0	192.168.116.201, IPv6 enabled	Time zone
		Product ID

- ניהול השירות מרוחק -



אפשר RDP לשרת DC1 לעובד מחוץ לארגון – מפורט 5588 לפורט 3389 בשרת.

- למטרות אבטחה, מגדרים פורט רנדומלי 5589 שתרגם לפורט של RDP לגישה מרוחק מרשת ה-WAN, כלומר מהמחשב הפיזי שלי
- ראשית עליינו יש לבדוק אם כתובת יש ל-Interface של SRV1 ב-WAN

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter LAN:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::2f4d:cb16:51e:885e%5
    IPv4 Address. . . . . : 192.168.116.254
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter WAN:

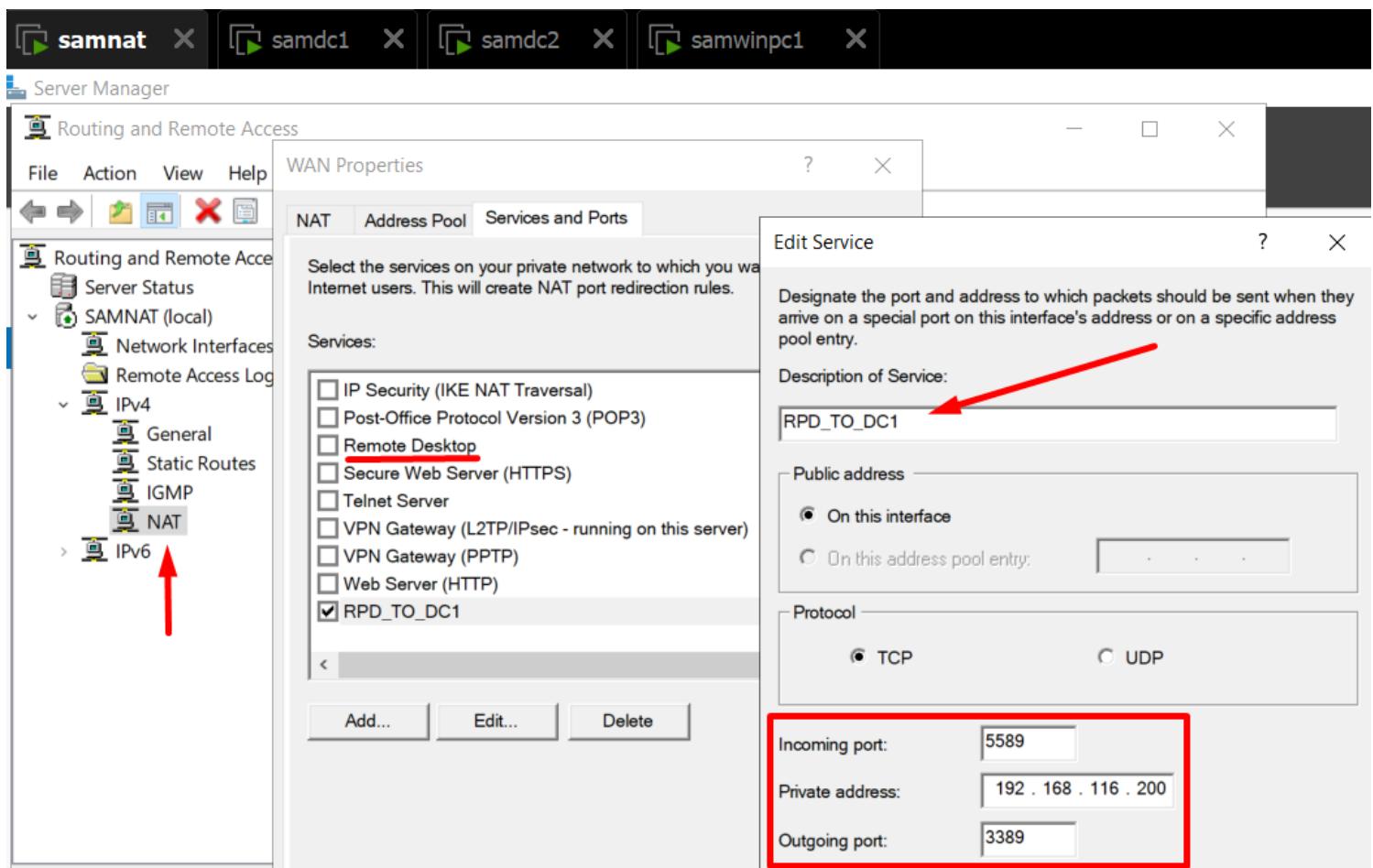
    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::6ff9:7aa1:de10:63c5%3
    IPv4 Address. . . . . : 192.168.68.109
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::52d4:f7ff:fe8a:92e0%3
                                         192.168.68.1
```

נתחבר דרכו ונשתמש בפורט

5589

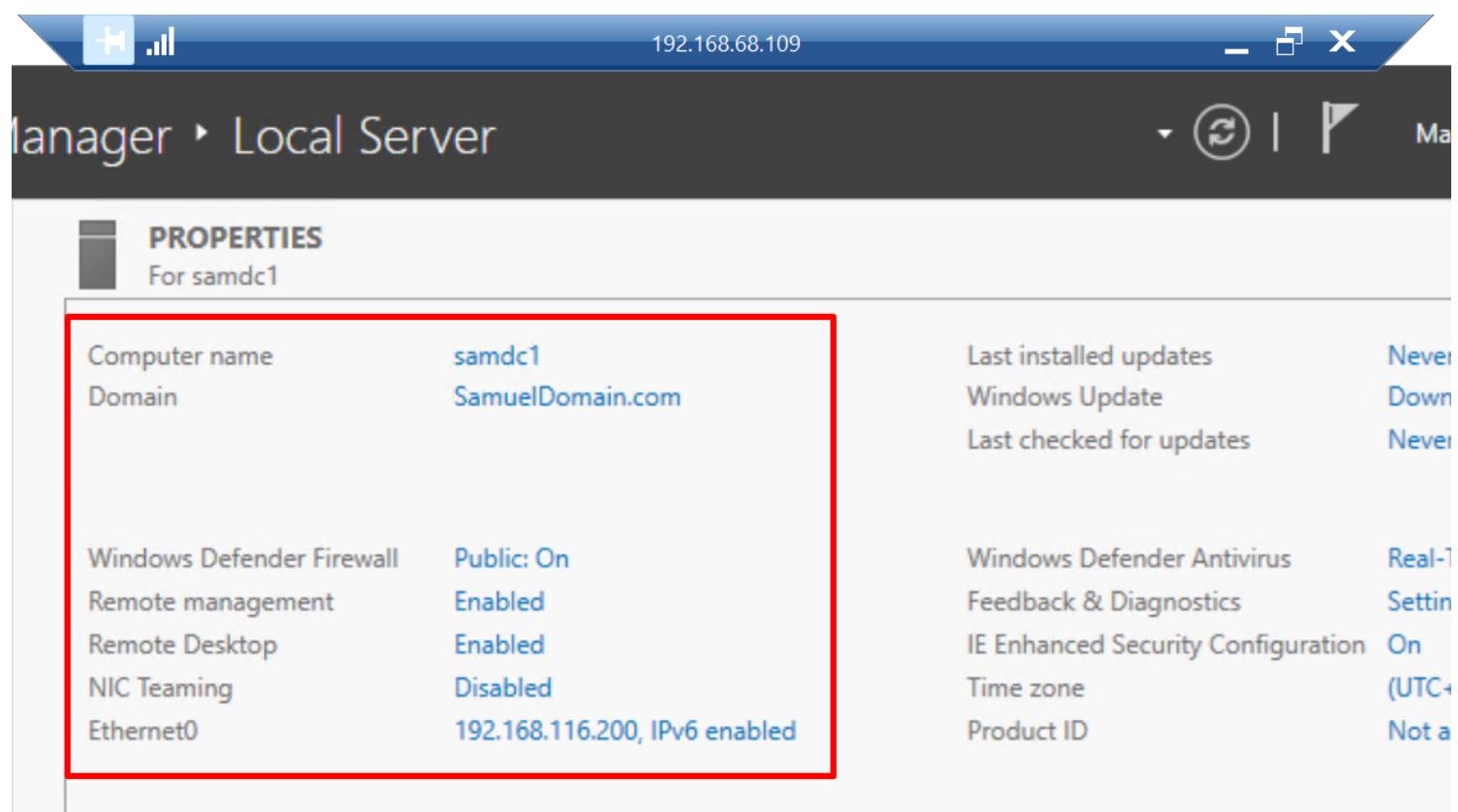
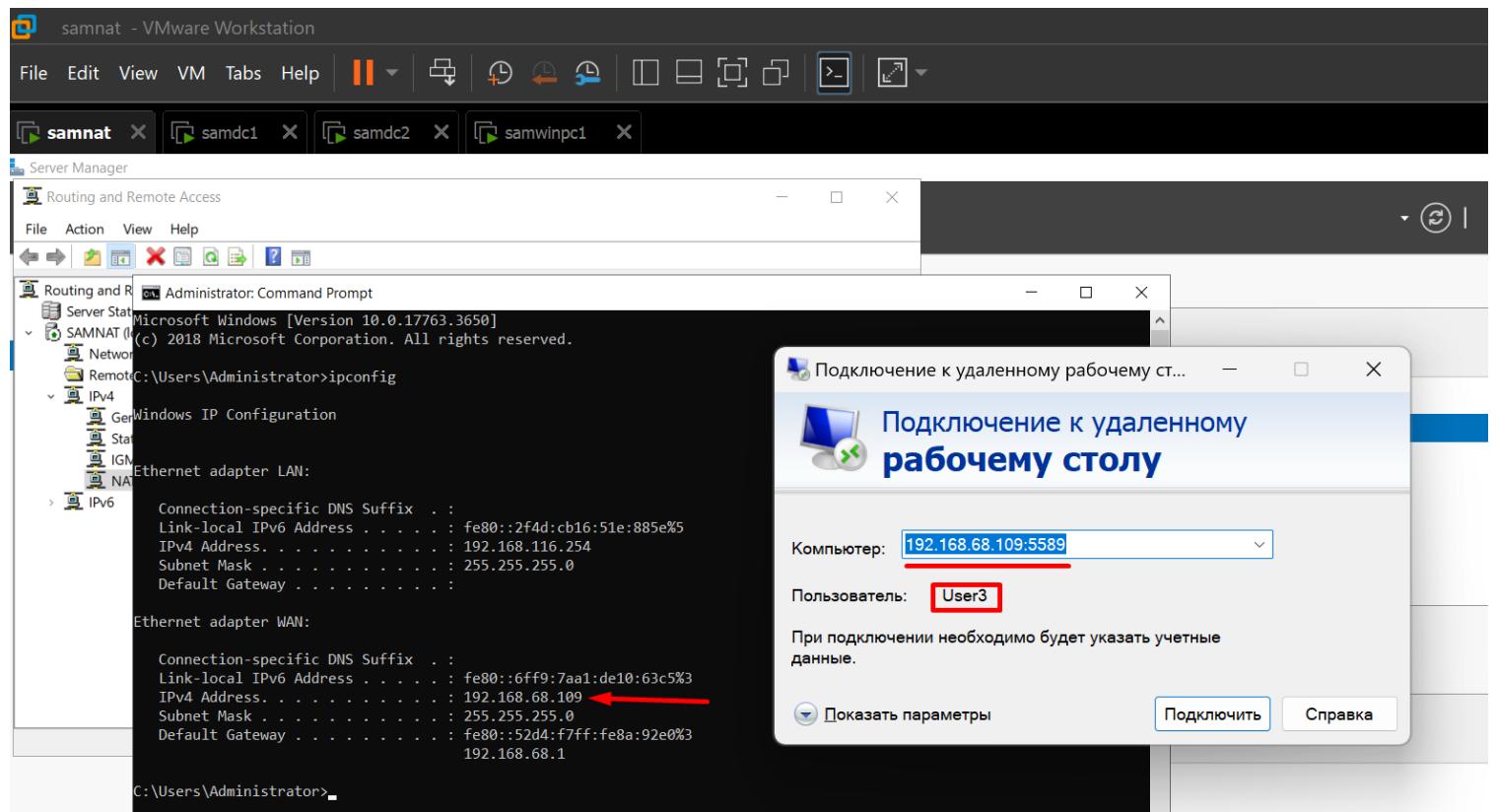
- ניהול השירות מרוחק -

- עכשו אנחנו עוברים להגדרות NAT ומוסיפים את השירות MCNISYS את כל הנטוונים הדרושים ובודקים אם הכל עובד



- ניהול השירות מרוחק -

- #### • בוא נבדוק אם הכל עובד

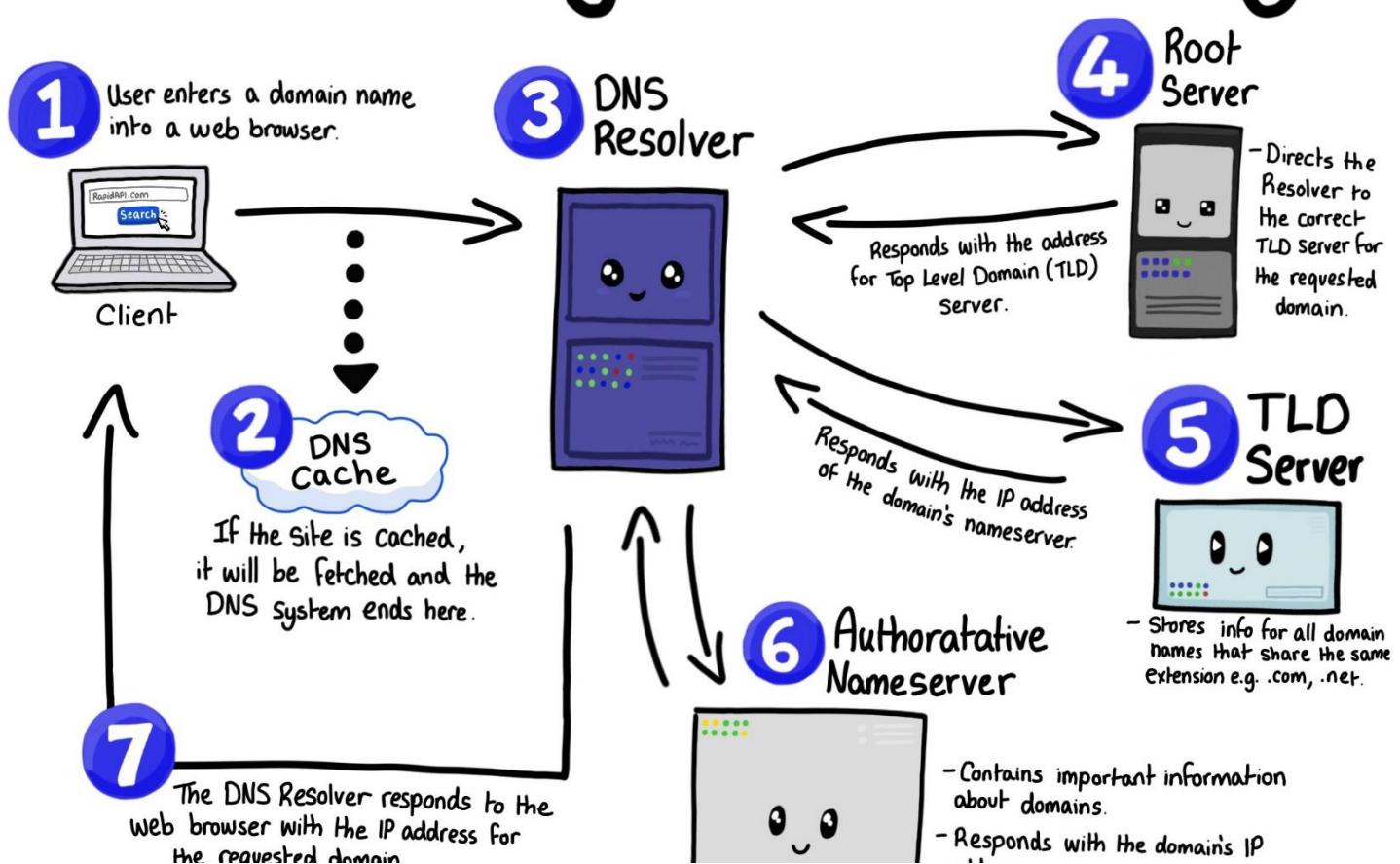


- DNS -

”

- הינה מערכת המתרגמת DNS (Domain Name System) -
שמות לדוגמה IP לכתובות SamuelDomain.com
- וקודם כל, כל בקשות ה-DNS מהרשות שלנו יישלחו ל-DC1,
- אבל אם אין מידע/cache של השרת, הבקשה תועבר לספק
ב-WAN וכן הלאה דרך היררכיית שרתים ה-DNS

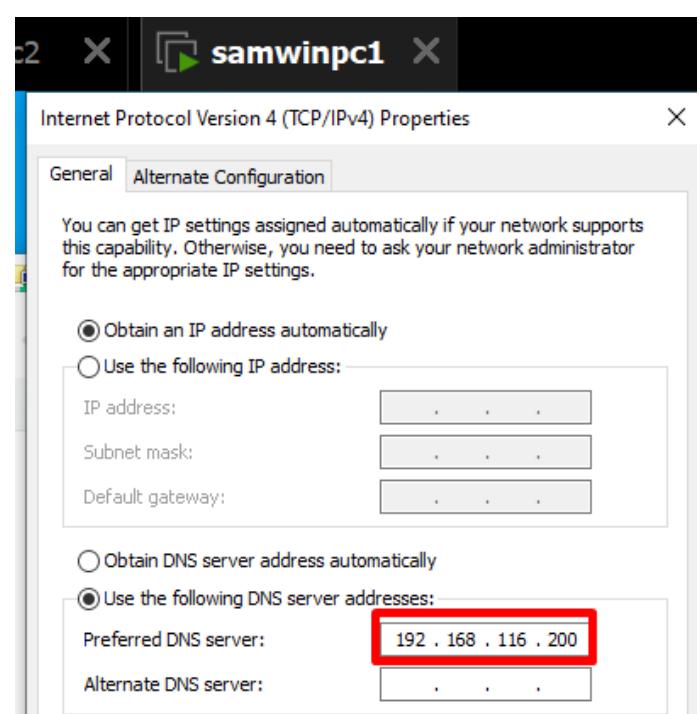
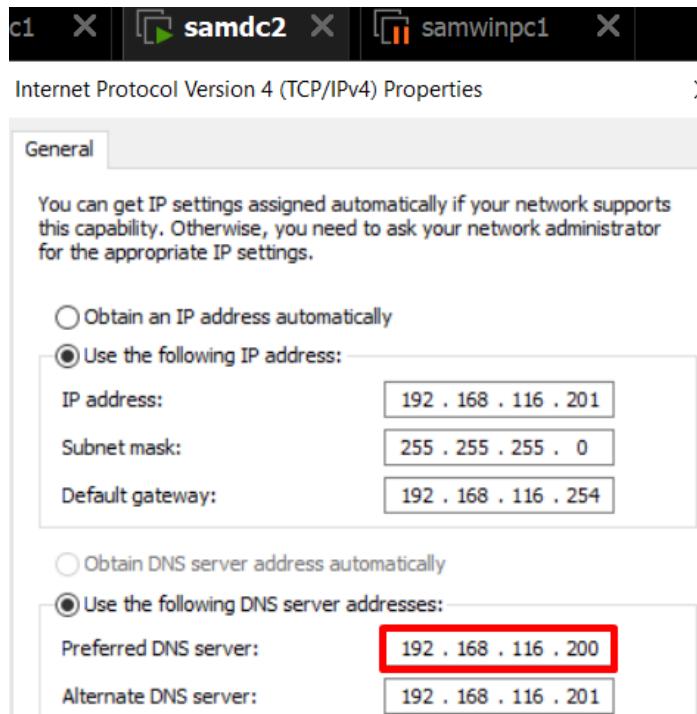
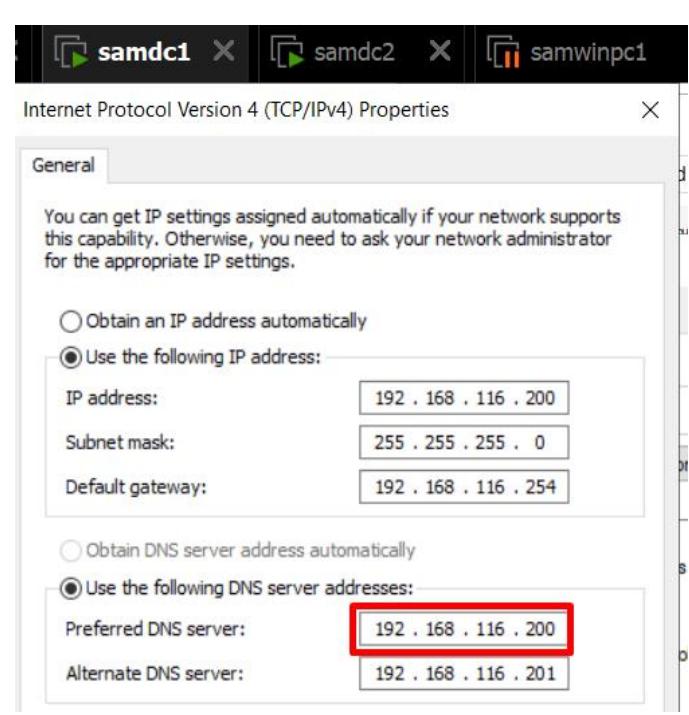
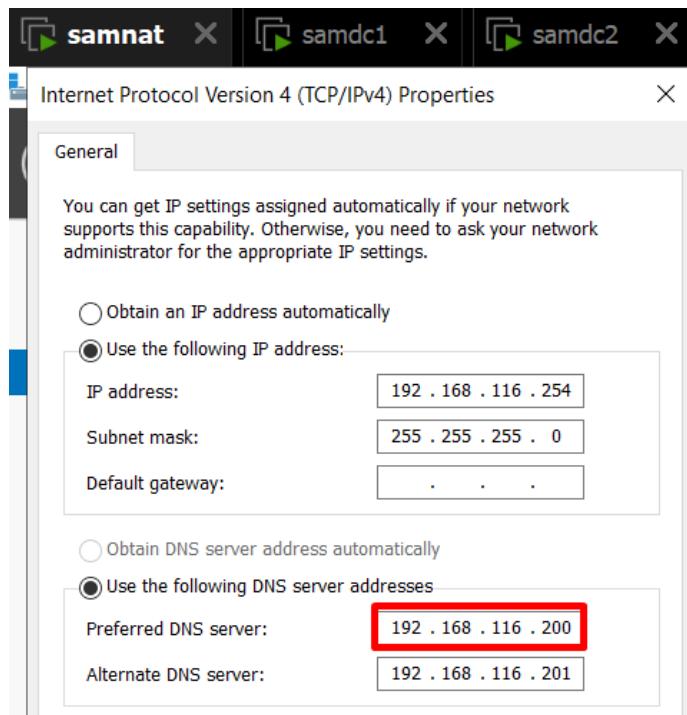
The DNS System Hierarchy



-DNS -

DNS שול DC1

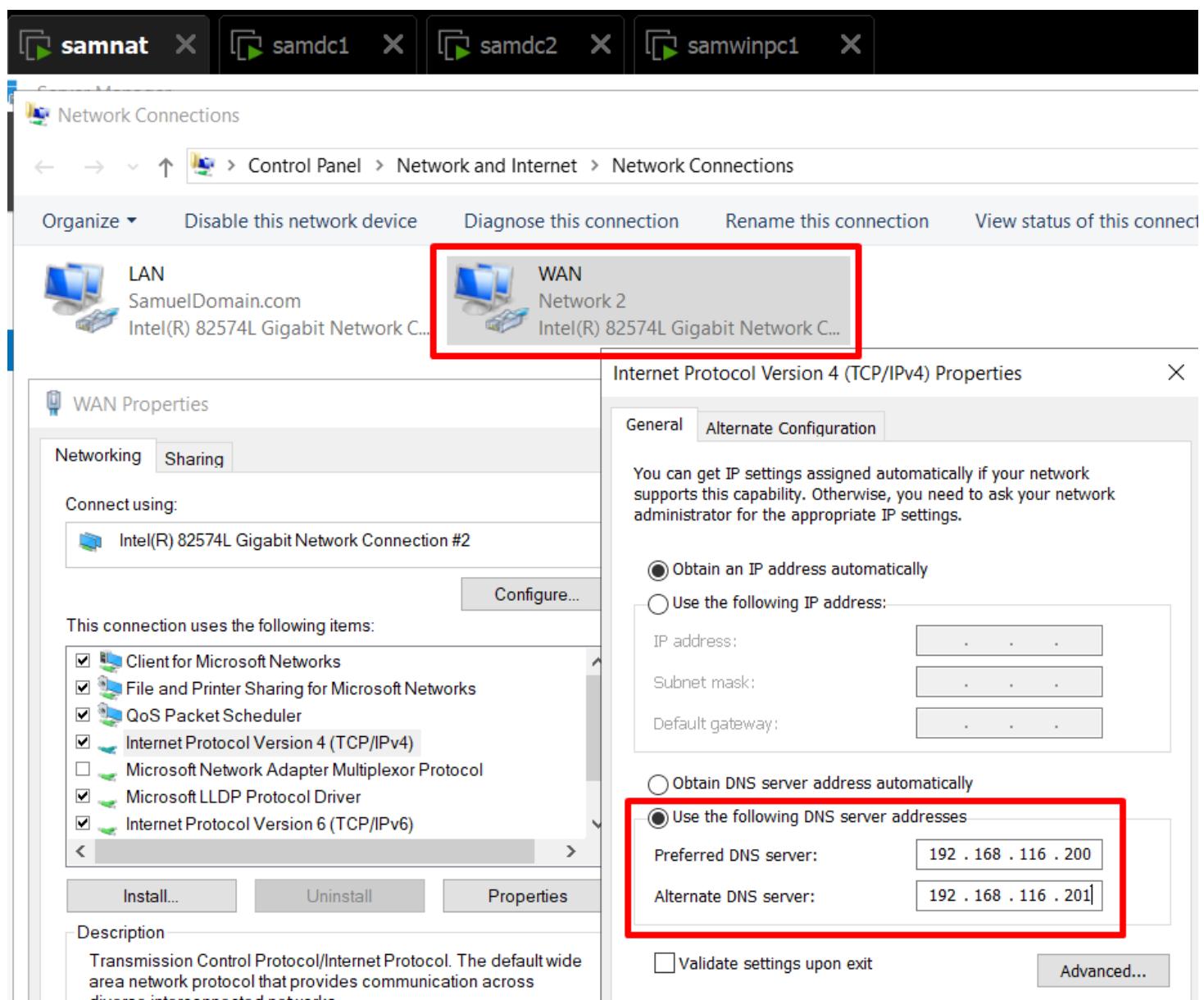
- קודם כל נבדק ששרת DNS-וינו מצוי בהגדרות הרשות של כל המחשבים



-DNS -

לא לשוכח להגדיר ידנית בכרטיס של DC לשימוש ב- DNS של SRV1

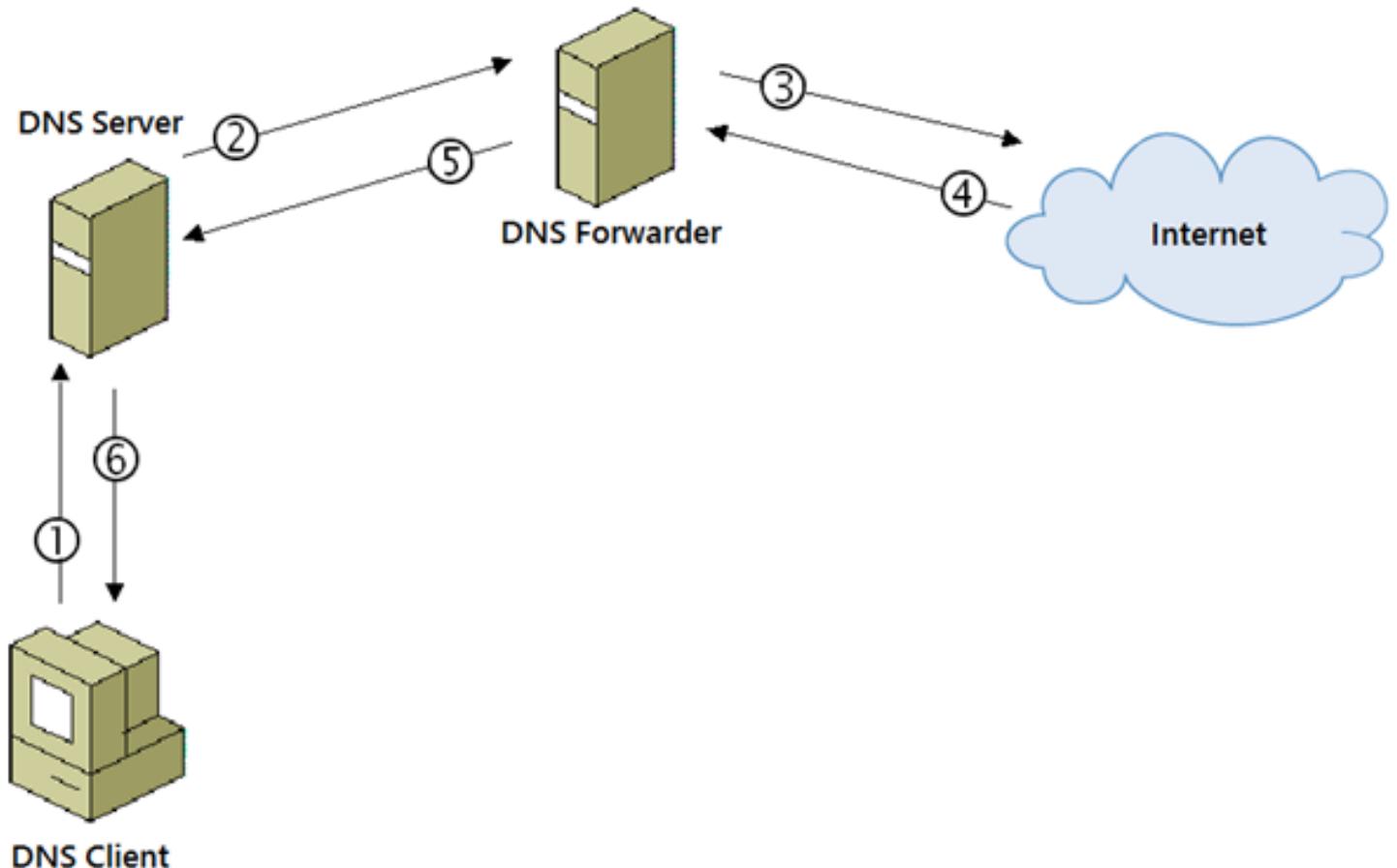
- אנו מכניסים את הכתובת של שרת DNS שלנו גם בכרטיס הרשות החיצוני



-DNS -

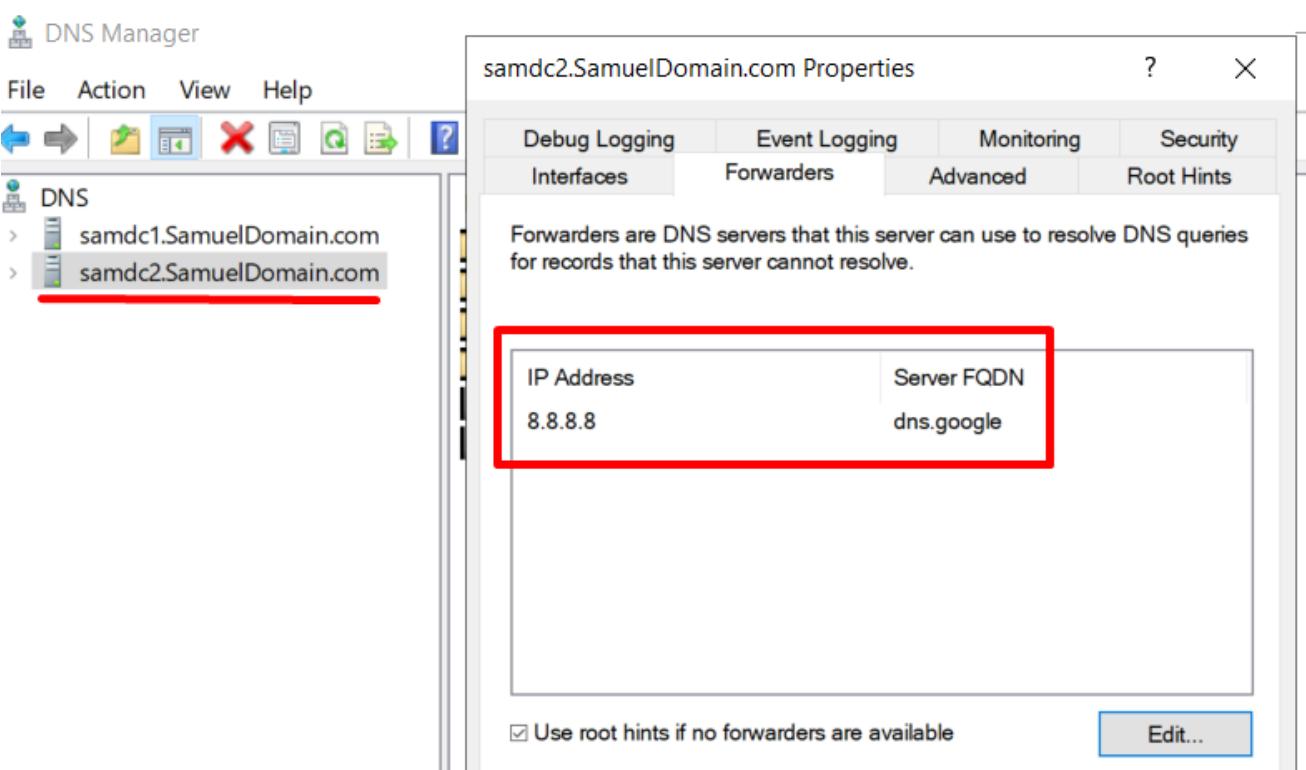
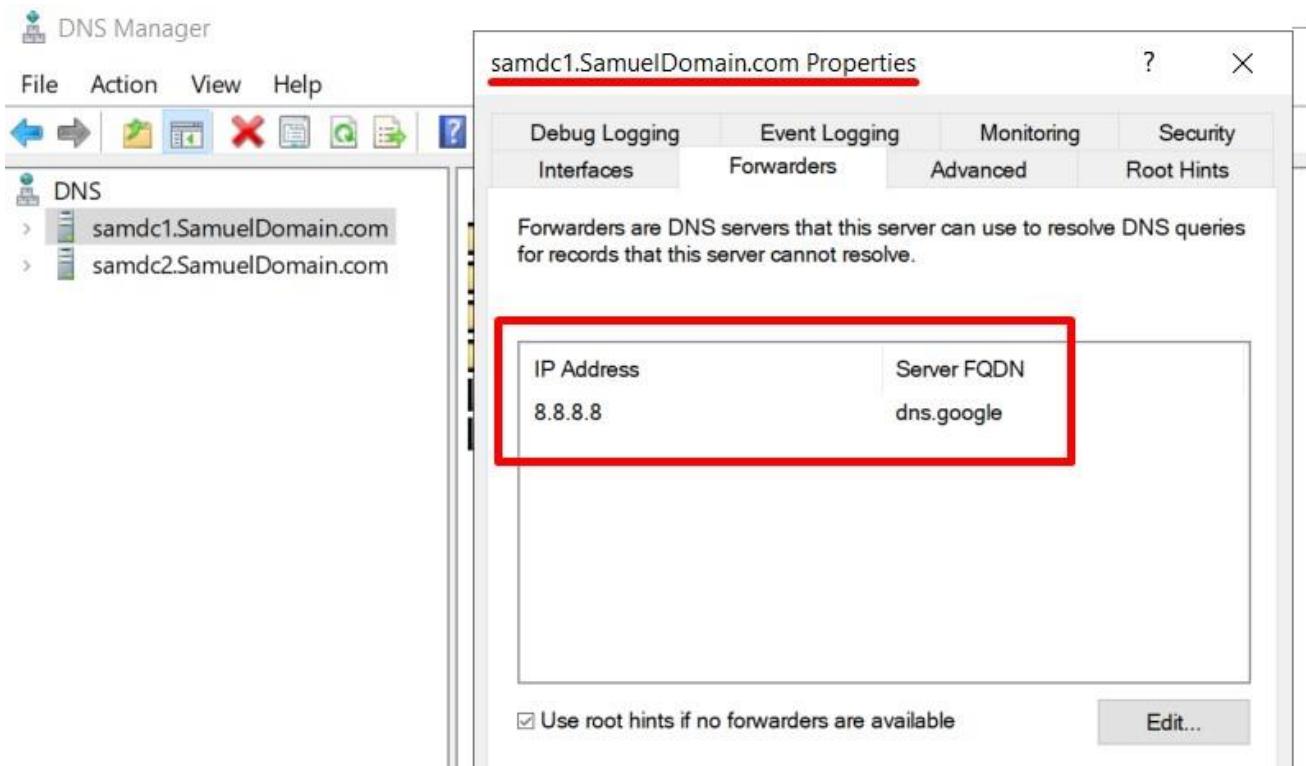
הגדך DNS Forwarding חיצוני (8.8.8.8)

ב-DNS FORWARDING הינה אפשרות לשירות DNS להעביר שאלות שמויות דומיין לשירות DNS אחר כאשר הוא אינו יכול לפתר את השאלה בעצמו. זה שימושי כאשר לשירות DNS אין מידע על הדומיין המבוקש ב-cache.



-DNS -

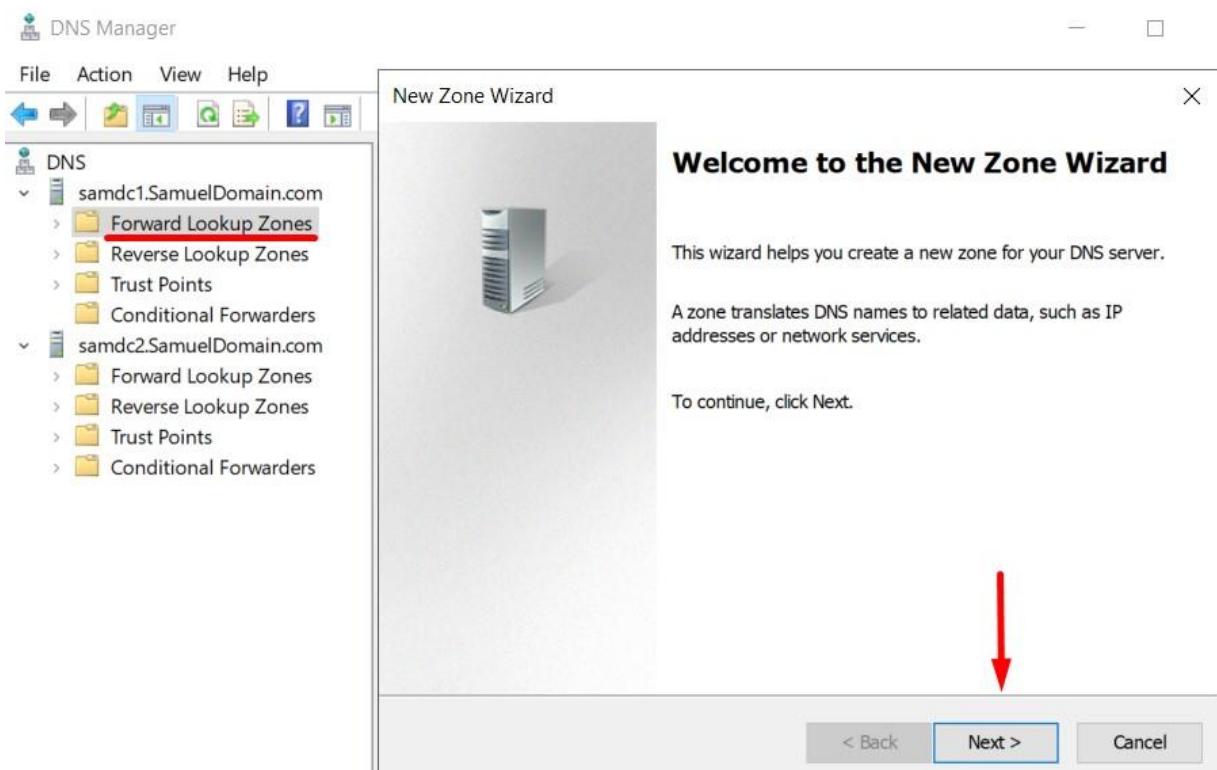
- אנחנו עוברים להדרות DNS MANAGER ובחלון אנחנו מוסיפים את שרת גוגל הידען
עשימים את אותו הדבר ב-DC2



-DNS -

הגדך ל-Primary Zone או Conditional Forwarders
Facebook.com במטרה למנוע מהעובדים לגלוש ב-
במהלך יום העבודה.

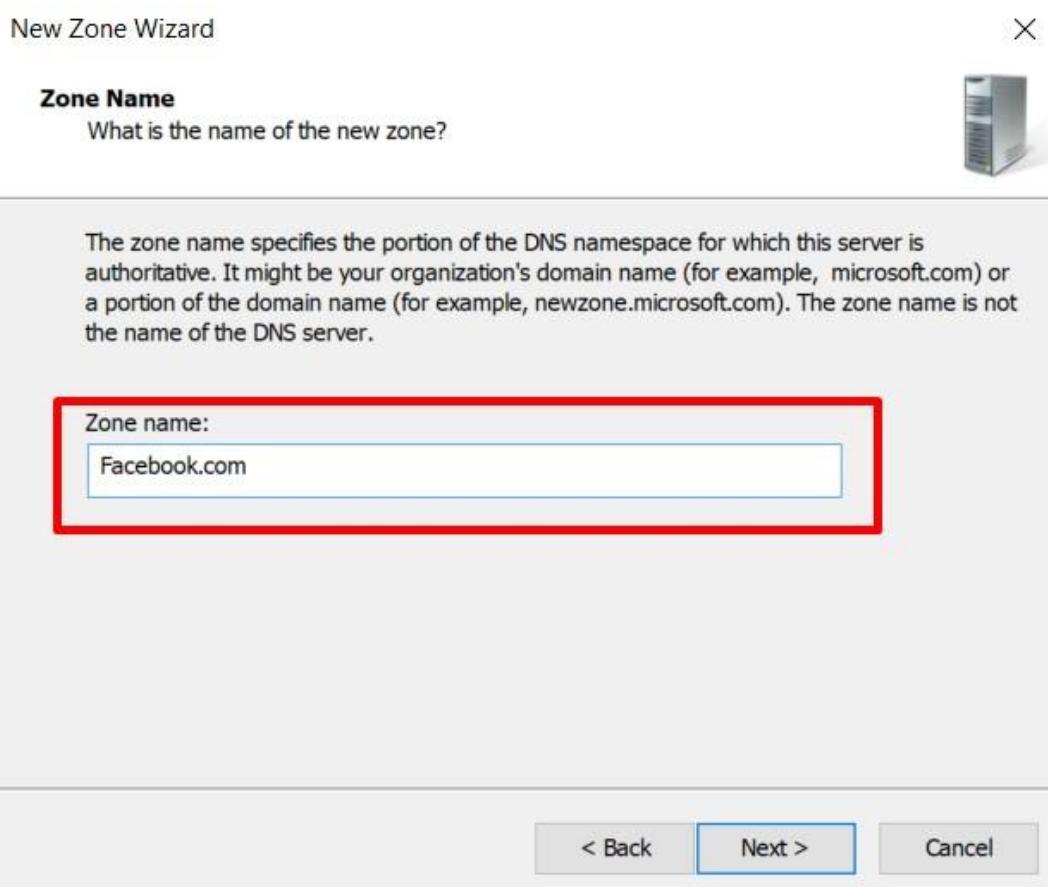
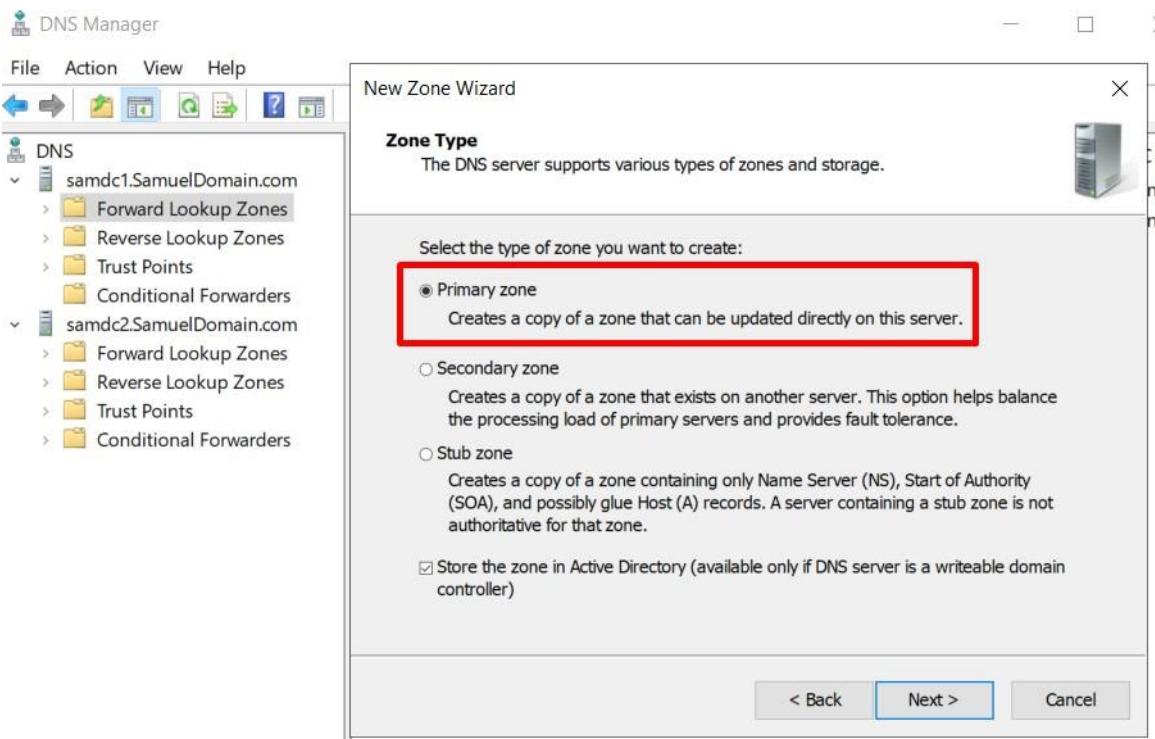
- מכיוון שהפרוטוקול מתרגם שמות דומיין, אנו נקצתה כתובת פייסבוק שגוייה ב-DNS MANAGER כדי למנוע מהעובדים להיות מושחים מעובודתם



: אזורים אלו מאחסנים רשומות יישירות בדיסק Primary zone שרת ה-DNS ומהווים מקור הסמכות לרשותם שליהם. ניתן לשנות אותם רק בשרת שבו הם מצויים.

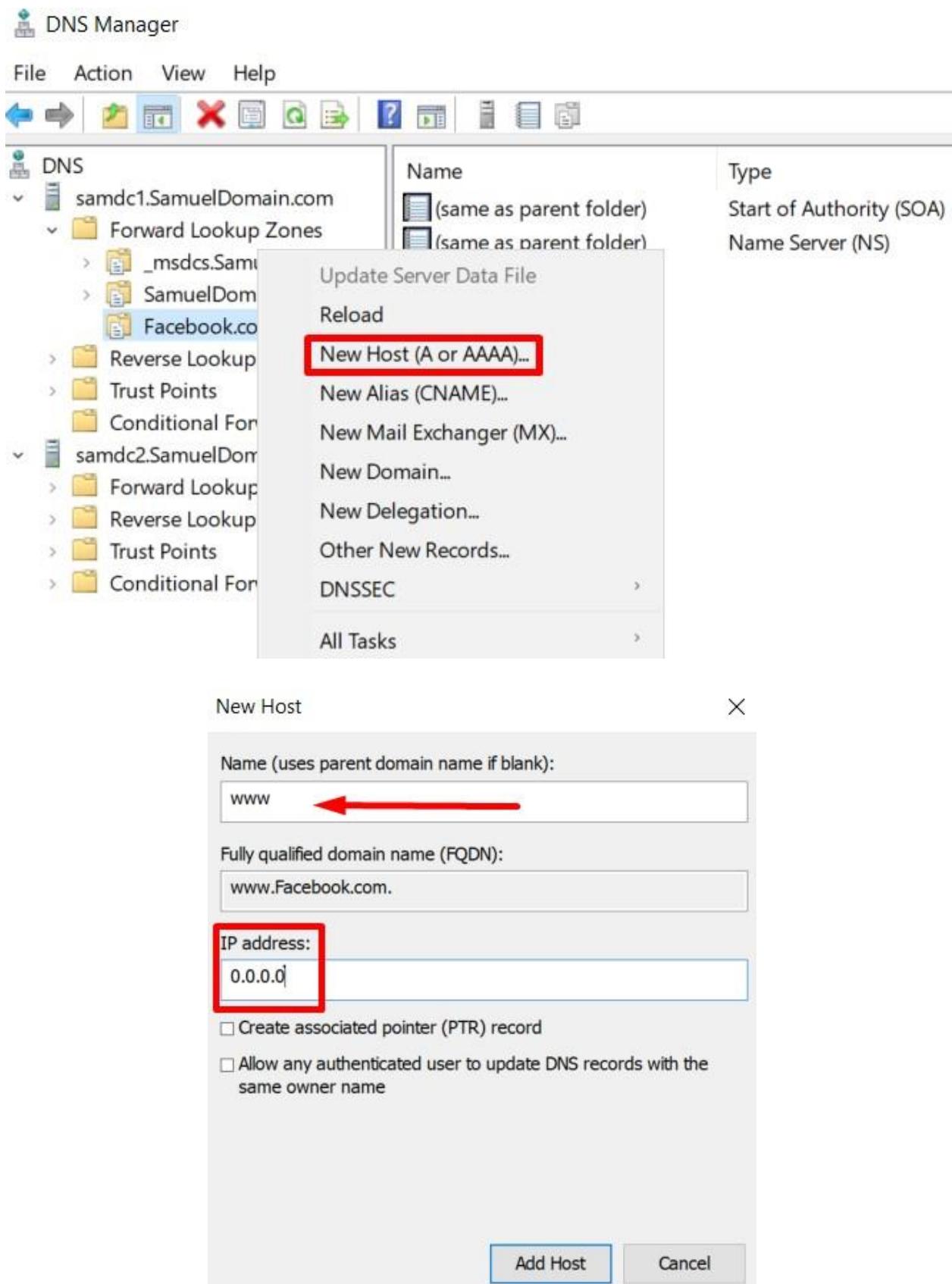
-DNS -

- אנו בוחרים באפשרות הראשונה ומוסיפים את הדומיין של פיסבוק



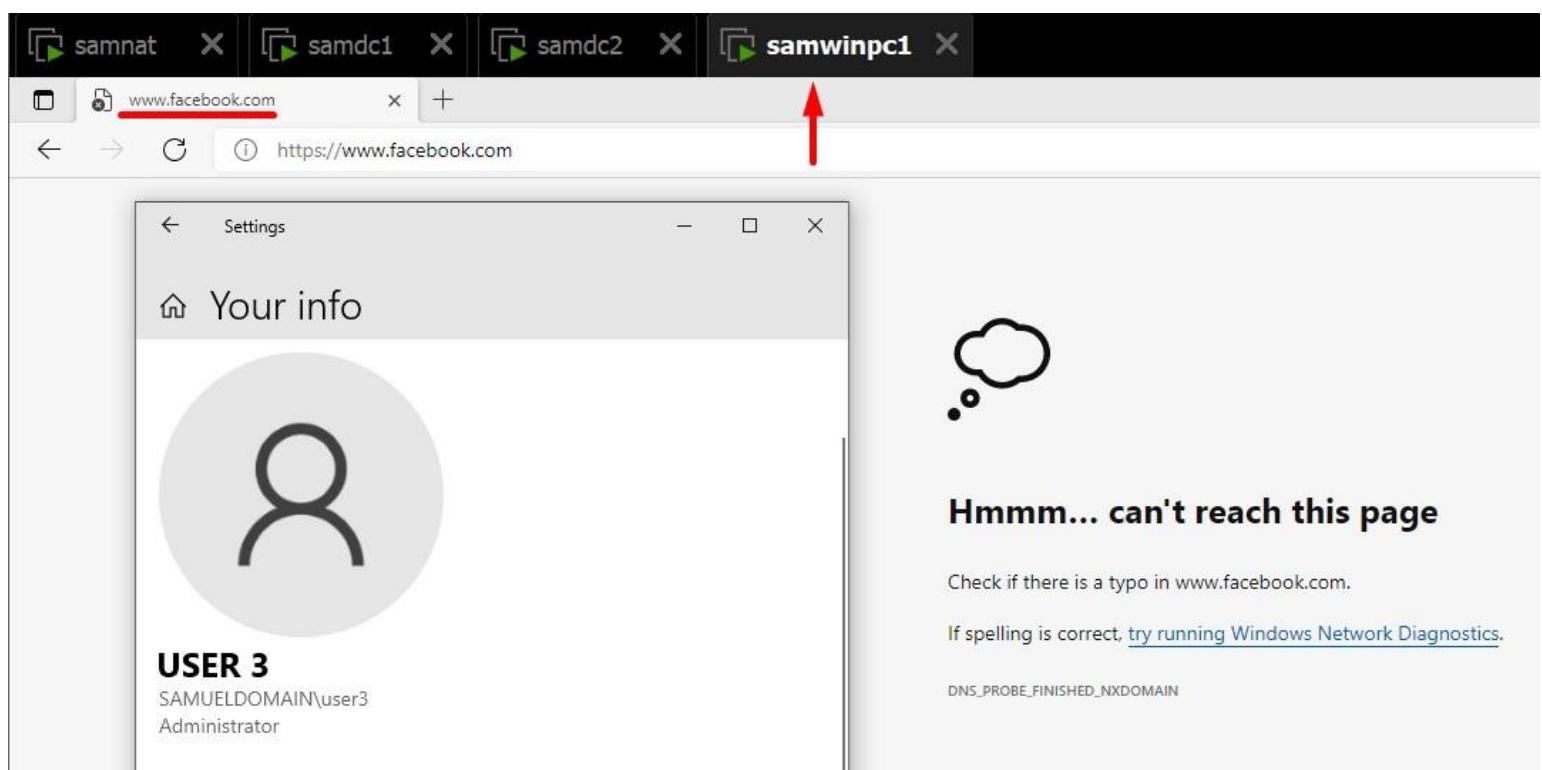
-DNS -

- לאחר הסיום התקינה של האזור החדש, אנו מוסיפים בו HOST שמו הוא למשל WWW, ונותנים לו כתובת שגوية!



-DNS -

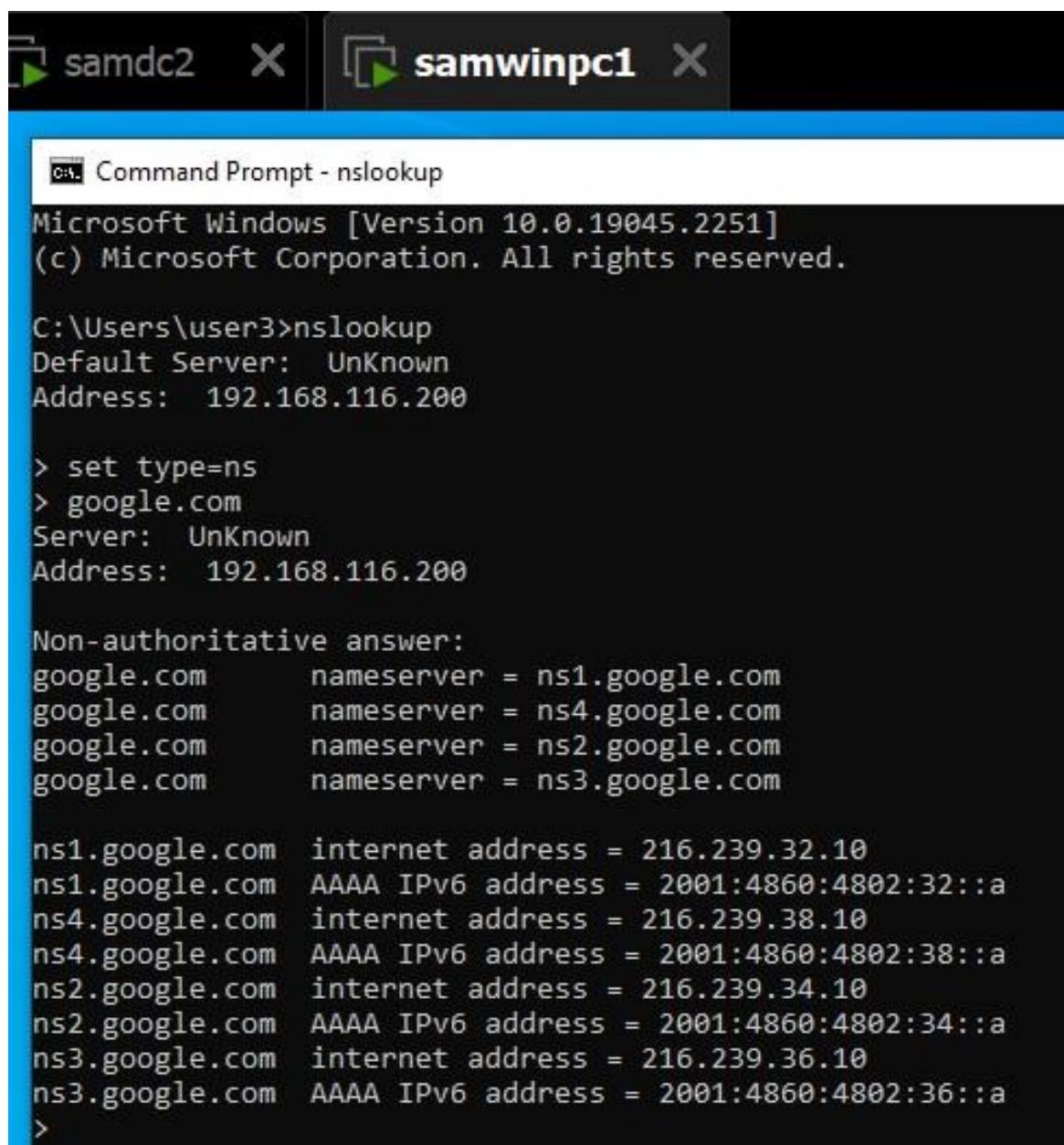
- ומקבלים את התוצאה על PC1 משרת ה-DNS



-DNS -

הכנס ל-WIN10ו השתמשב-nslookup כדי לוודא שהשרת מצליח לתרגם את הכתובות google.com

- אנו מקבלים כתובות של שרתים Google שזמינים לנו וגם את שמותיהם באמצעות הפקודה ns



```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.19045.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user3>nslookup
Default Server: UnKnown
Address: 192.168.116.200

> set type=ns
> google.com
Server: UnKnown
Address: 192.168.116.200

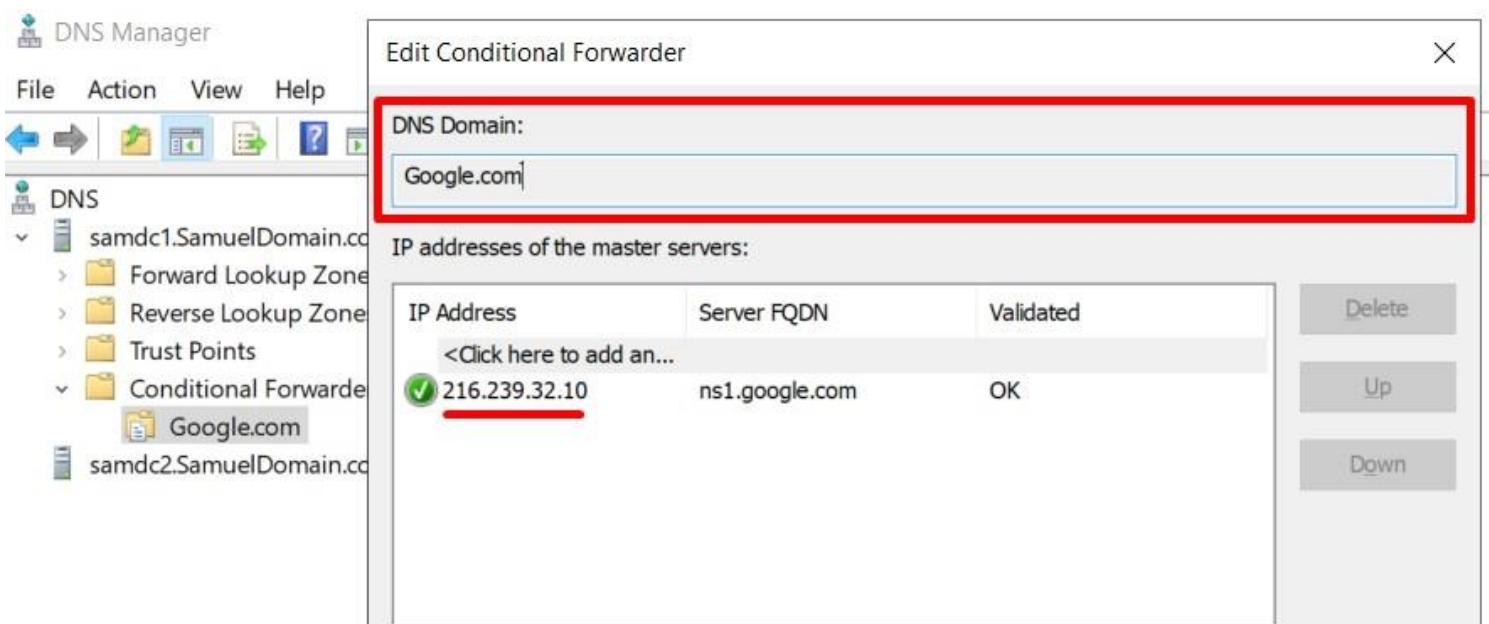
Non-authoritative answer:
google.com      nameserver = ns1.google.com
google.com      nameserver = ns4.google.com
google.com      nameserver = ns2.google.com
google.com      nameserver = ns3.google.com

ns1.google.com  internet address = 216.239.32.10
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  AAAA IPv6 address = 2001:4860:4802:38::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  AAAA IPv6 address = 2001:4860:4802:34::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  AAAA IPv6 address = 2001:4860:4802:36::a
>
```

-DNS -

הגדיר Google.com ל- Conditional Forwarders יש להעזר בפקודה nslookup ולצרכ צילום מסך של פלט הפקודה.

- עכשו ניצור CONDITION FORWARDING לגוגל, באמצעות השירותים שמצאו דרך CMD בתרגיל הקודם



-DNS -

הגדך yahoo.com ל-Stub Zone

- DNS ב-Stub Zone מכיל מידע על שרתים DNS של אזורים אחרים. הוא משמש להפניה מחדש של בקשות עבור דומיינים שאינם באזור המקומי לשרתים DNS אחרים כדי לקבל את המידע הרלוונטי
- נגידר אותו לדומיין של yahoo.com נבדוק את כתובות הדומיין הזמינים באמצעות CMD וניצור אזור חדש

█ Command Prompt - nslookup

```
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

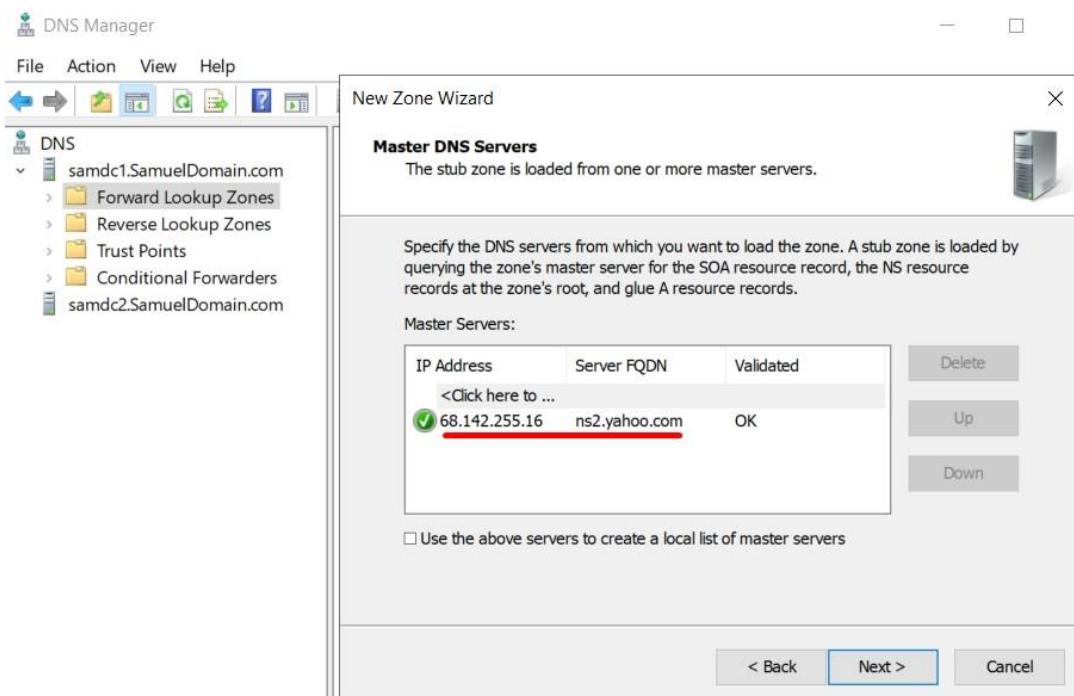
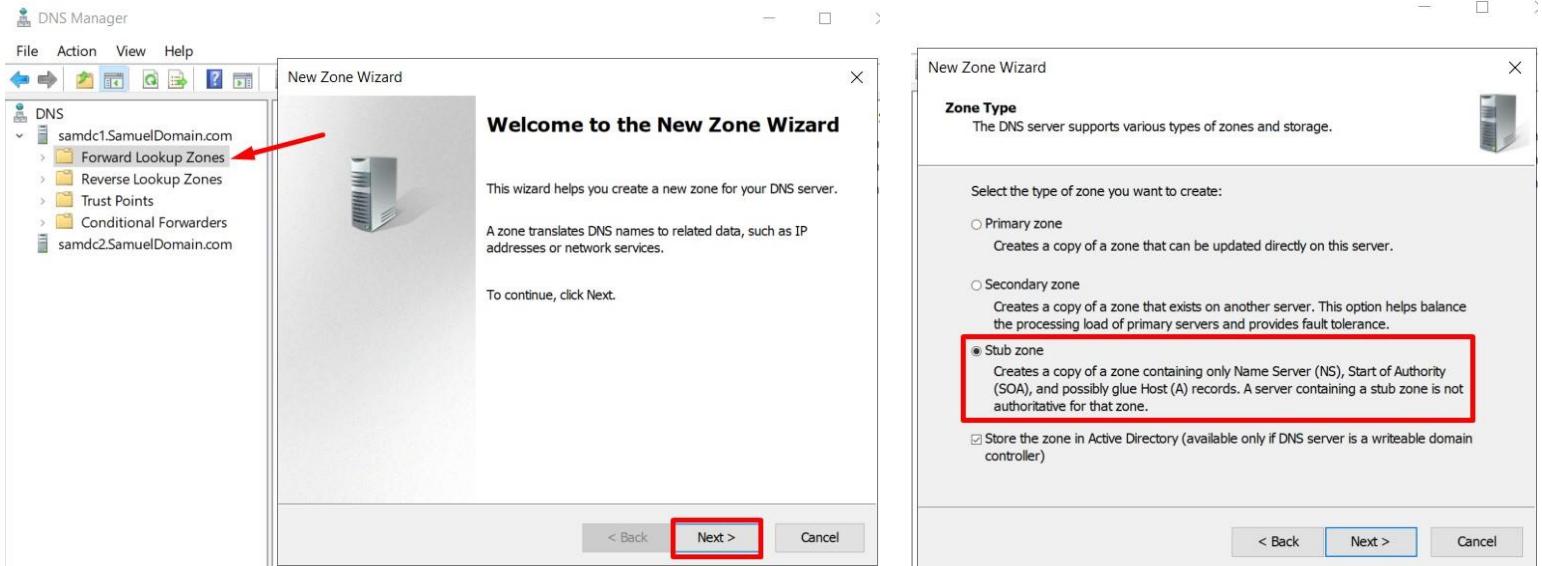
C:\Users\Avocado>nslookup
Default Server: UnKnown
Address: ::1

> set type=ns
> yahoo.com
Server: UnKnown
Address: ::1

Non-authoritative answer:  
yahoo.com      nameserver = ns2.yahoo.com
yahoo.com      nameserver = ns4.yahoo.com
yahoo.com      nameserver = ns3.yahoo.com
yahoo.com      nameserver = ns1.yahoo.com
yahoo.com      nameserver = ns5.yahoo.com
>
```



-DNS -



Name	Type	Status	DNSSEC Status
_msdcs.SamuelDomain.com	Active Directory-Integrated Primary	Running	Not Signed
Facebook.com	Active Directory-Integrated Primary	Running	Not Signed
SamuelDomain.com	Active Directory-Integrated Primary	Running	Not Signed
yahoo.com	Active Directory-Integrated Stub	Running	

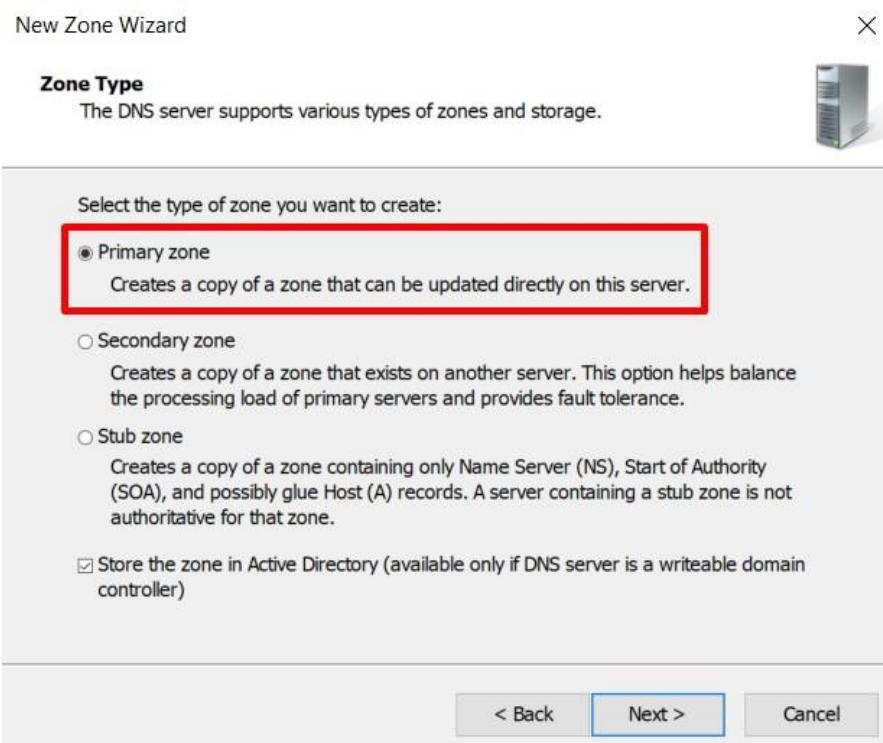
-DNS -

צורך ZONE מוגן – איזה שם שתרצה – צור ל Secondary Zone DC2 זיהה בשרת ZONE

ב-DNS הוא עותק של אזור משרת השני. הוא מתעדכן על ידי שכפול נתונים משרת ה-DNS הראשי ומספק fault tolerance בפעולת ה-DNS.

- אנחנו יוצרים אזור חדש ונותנים לו את השם SAM53

בהתחלת ניצור PRIMARY ZONE ב-DC1 ואז SECONDARY ZONE ב-DC2 עם אותו שם



DNS Manager

File Action View Help

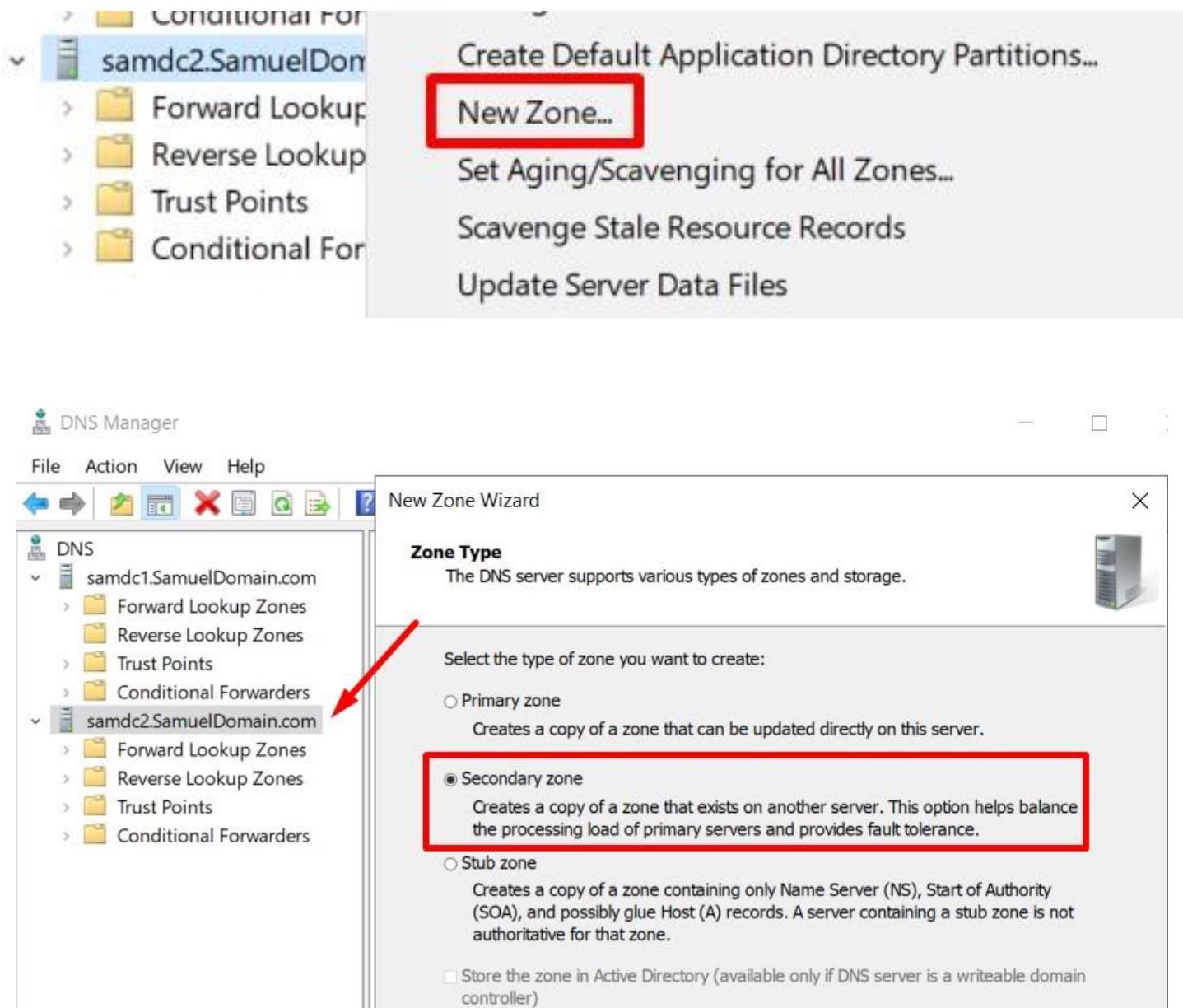
DNS

Name Type Status DNSSEC Status

_msdcs.SamuelDomain.com	Active Directory-Integrated Primary	Running	Not Signed
Facebook.com	Active Directory-Integrated Primary	Running	Not Signed
SamuelDomain.com	Active Directory-Integrated Primary	Running	Not Signed
yahoo.com	Active Directory-Integrated Stub	Running	
SAM53	Active Directory-Integrated Primary	Running	Not Signed

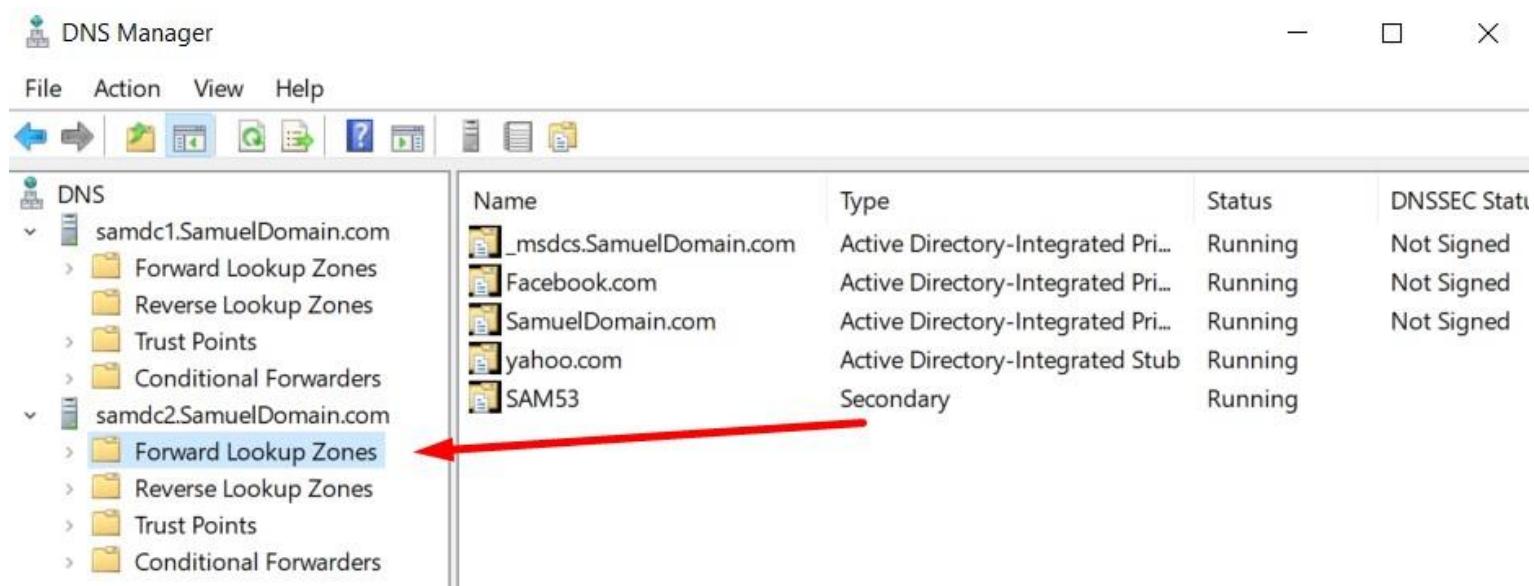
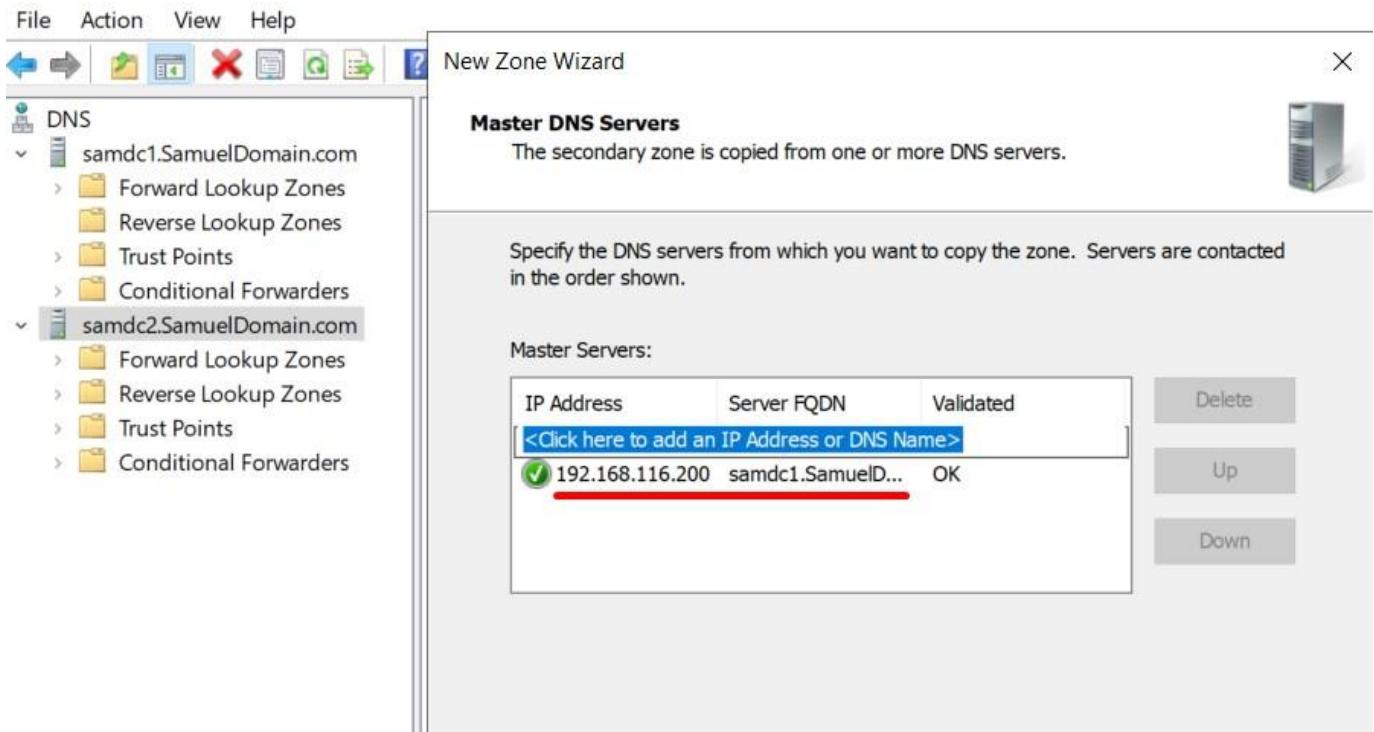
-DNS -

- **כעת נוסיף את SECONDARY ZONE ב-SAM53 עבר DC2**



-DNS -

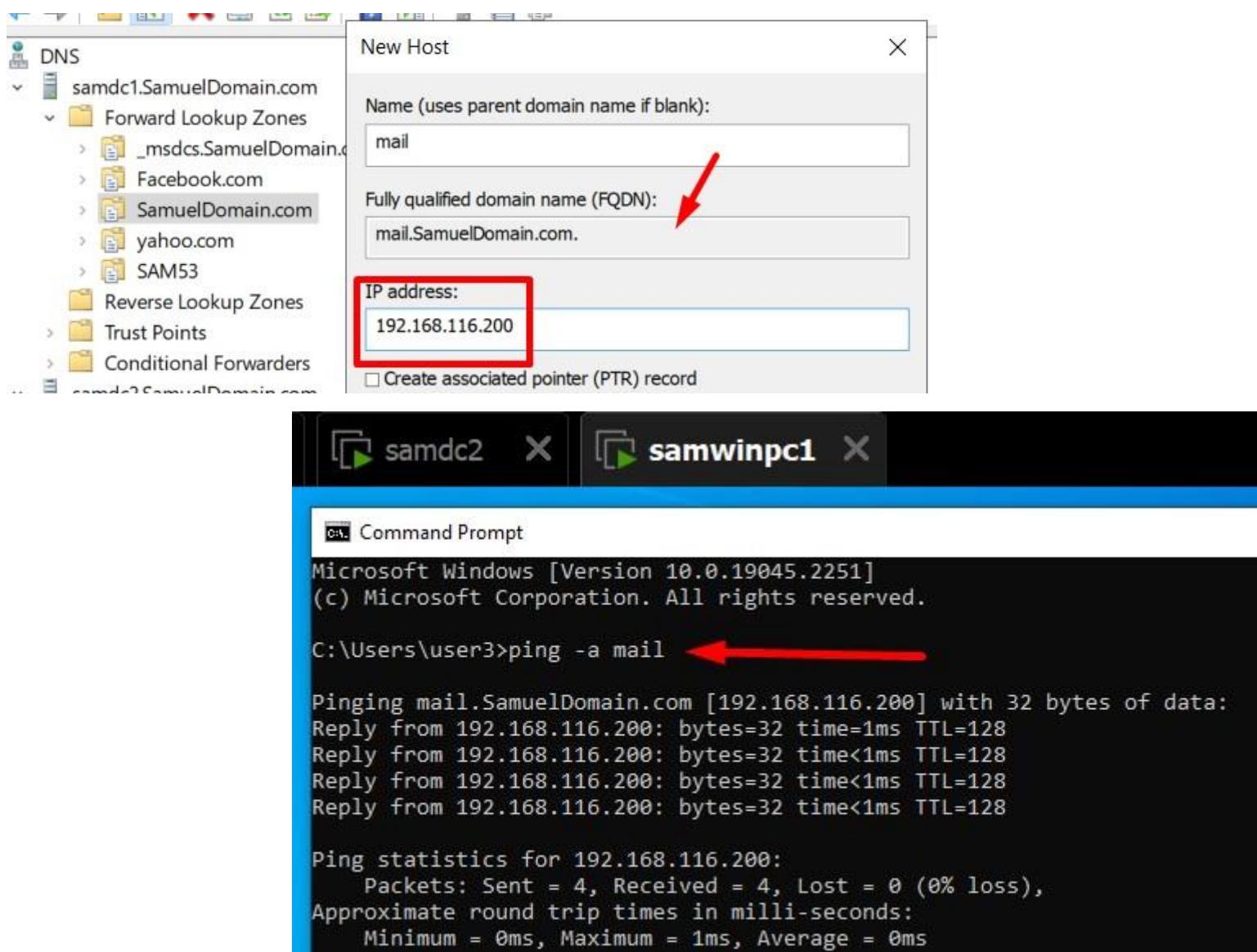
- מוסיפים את הכתובת PRIMARY של השרת שאנו רוצים להוסיף וליצור עותק שלה, במקרה שלנו זה DC1 או 192.168.116.200



-DNS -

צור CNAME לשרת DC2 או לרשומה אחרת לבחירתך לשם PING שהוא שונה מהשם המקורי של השירות – בדוק שזה עובד (מחתנה לשם החדש)

- DNS הוא סוג CNAME (CANONICAL NAME) – רשומה המשמש ליצירת "NICKNAME" עבור שמורות דומיין. זה מאפשר שם דומיין אחד להיות קישור לאחר דומיין.
- לדוגמה, אנחנו יכולים ליצור דומיין:
mail.samueldomain.com אבל זה לא יעבוד כי אין לנו שרת דואר
 - אנו מוסיפים HOST חדש לדומיין, מכניסים את הכתובת של ה-DC1 – DC1 ובודקים אם יש חיבור ואם שירות ה-DNS/CNAME פועל

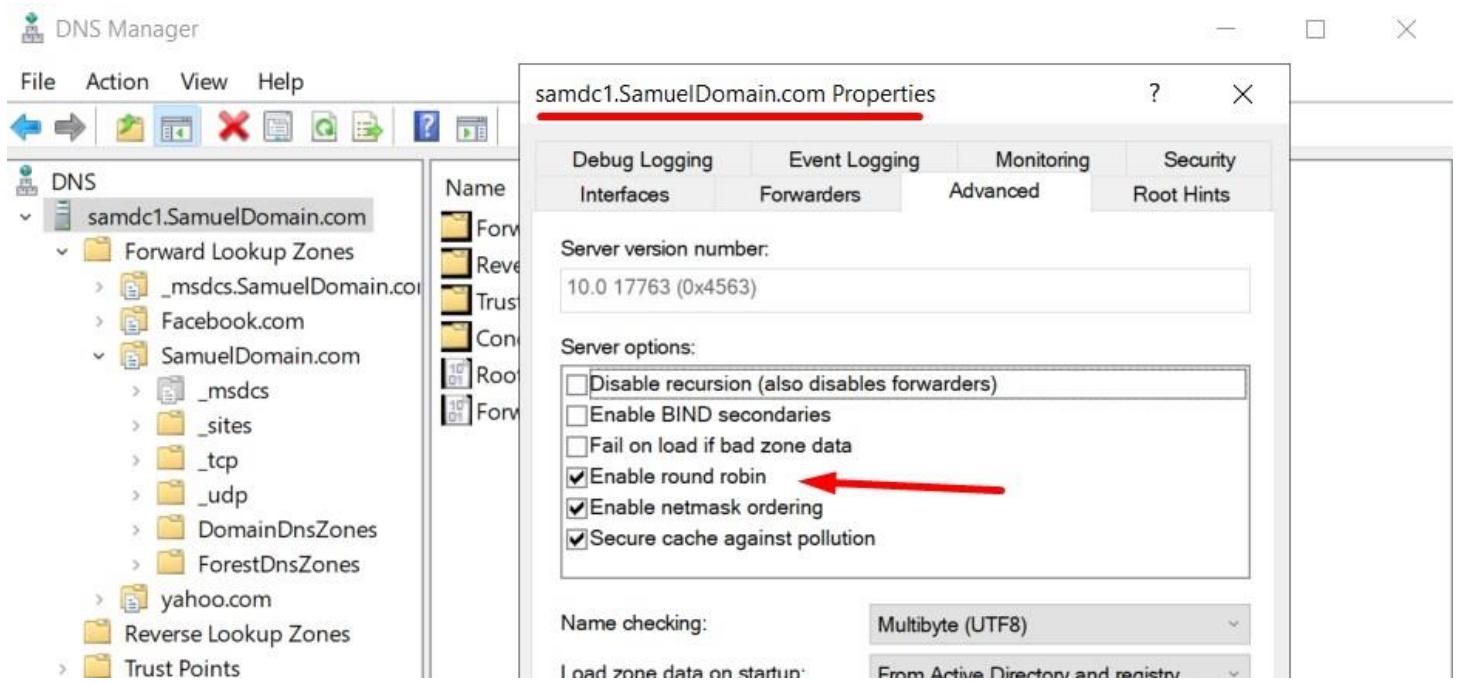
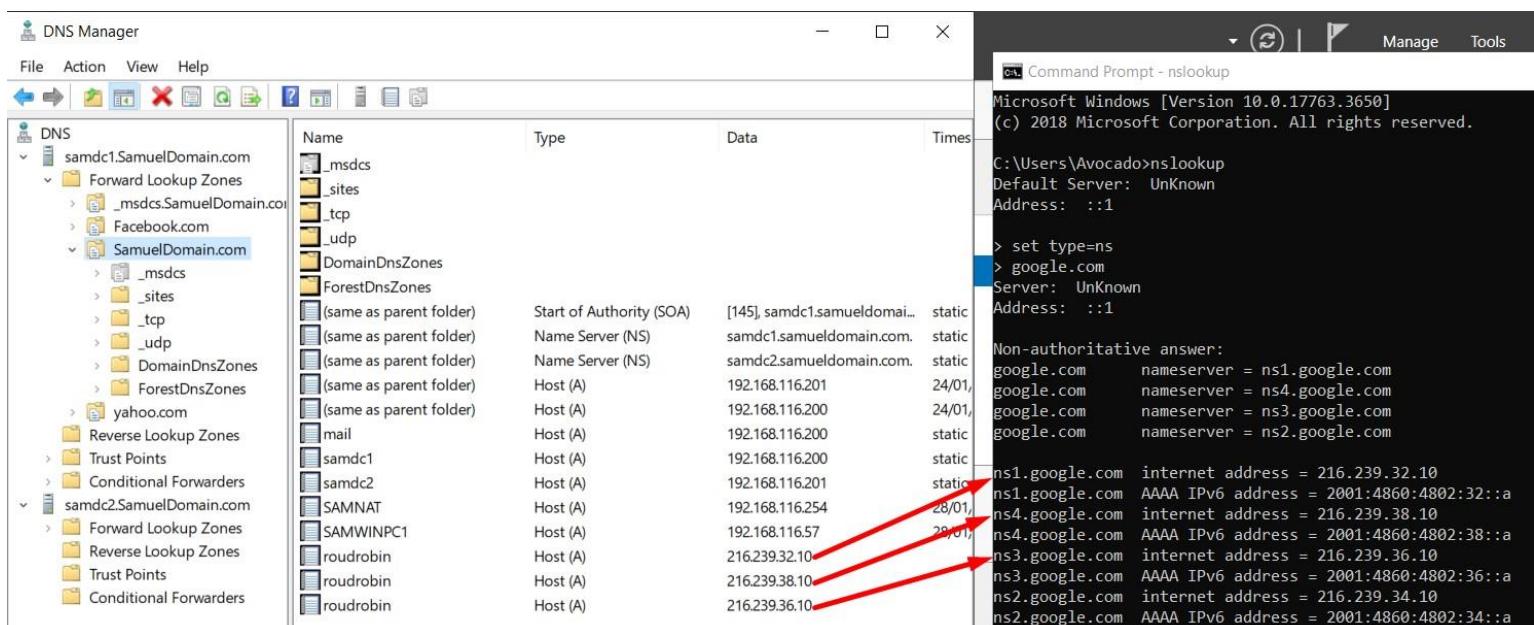


-DNS -

צור ובודק ל 2 רשומות שטףנות לכתובת Round Robin (CNAME) לנודמליות ולא

- DNS ב-Round Robin היא שיטת איזון עומסים. הוא מפיץ את העומס על פני מספר שרתים, ומשפר את הביצועים.
- קודם כל אני אזכיר HOSTS עם כתובות שונות אבל עם אותן שמות, למשל אקח שרתי גול, אפעיל את הפונקציה ROUD ROBIN בדומיין ובודק אם הפונקציה עובדת דריך

PC1



-DNS -

- איך נוכל לראות שהפונקציה עובדת, ועם כל בקשה משתנה כתובת HOST

```
C:\Users\user3>nslookup roudrobin.SamuelDomain.com
Server: UnKnown
Address: 192.168.116.200

Name: roudrobin.SamuelDomain.com
Addresses: 216.239.32.10 ←
           216.239.36.10 ←
           216.239.38.10 ←

C:\Users\user3>nslookup roudrobin.SamuelDomain.com
Server: UnKnown
Address: 192.168.116.200

Name: roudrobin.SamuelDomain.com
Addresses: 216.239.36.10 ←
           216.239.38.10 ←
           216.239.32.10 ←

C:\Users\user3>nslookup roudrobin.SamuelDomain.com
Server: UnKnown
Address: 192.168.116.200

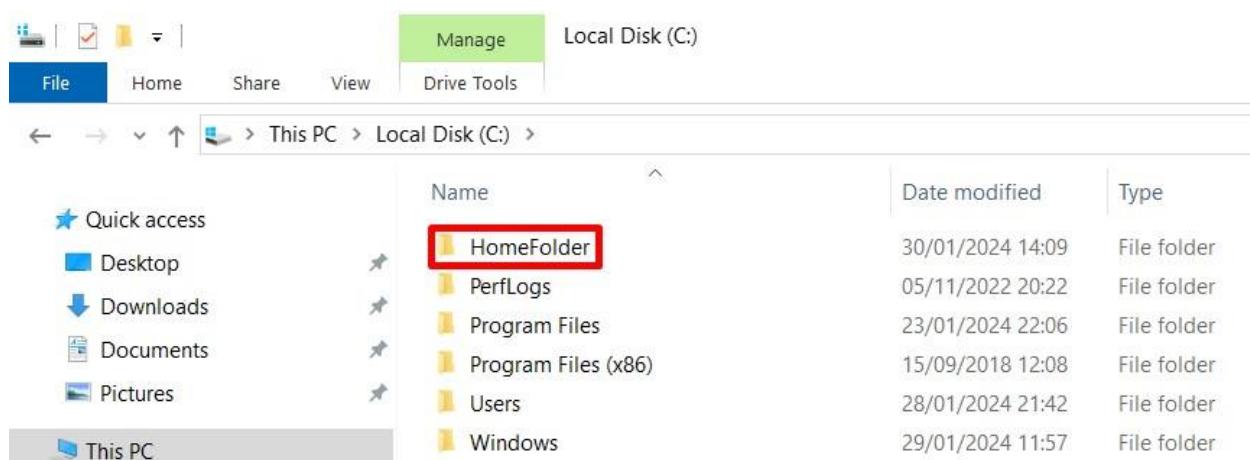
Name: roudrobin.SamuelDomain.com
Addresses: 216.239.38.10 ←
           216.239.32.10 ←
           216.239.36.10 ←
```

- Roaming Profile -

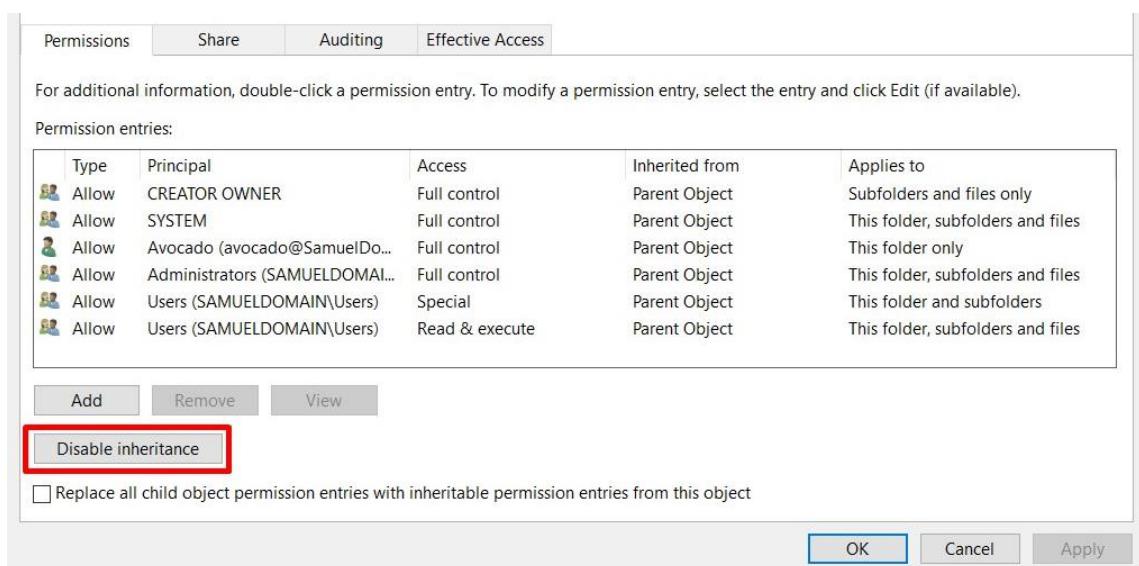
צורך פרופיל משותם נודד לחשבונן שיצרנו בתרגולים הקודמים

- מה זה פרופיל משותם? ומה הבדל בין חשבון משותם?
- PROFILE הוא חשבון משותם המכיל מידע להרשאה בראשת, ופרופיל הוא קבוצה של הגדרות ופרמטרים הקובעים את חווית המשתמש בעבודה עם מחשב. הפרופיל מכיל את הנתונים האישיים של המשתמש.
- עכשו נגיד פרופיל נודד לנידות מקסימלית, כך שהוא לא יהיה הקשור למחשב ספציפי, וכל הנתונים נשארו בשרת!

נוצר תקיה שבה יהיו נתוני הפרופיל נודד בשרת DC1

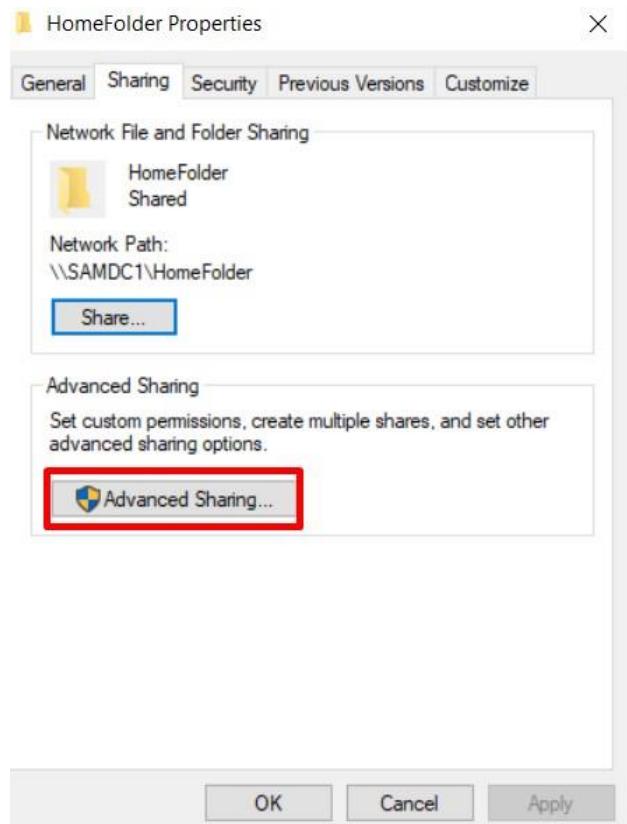


- מבטלים את הפונקציה INHERITANCE של התקיה כדי לשנות הרשות ולקבל שליטה מלאה



-Roaming Profile -

- כעת אנו משתפים אותה ומגדירים הרשותות לEveryone

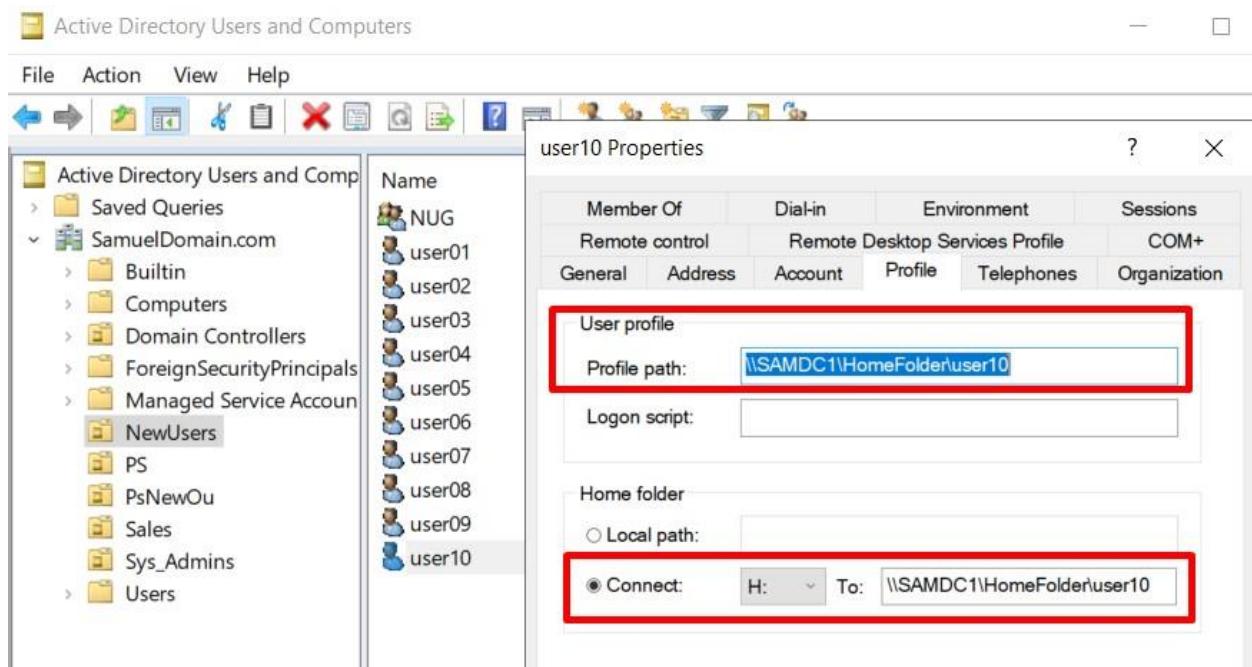


The screenshot shows the 'Advanced Sharing' dialog box for the 'HomeFolder' share. In the 'Permissions for Everyone' section, the 'Full Control' checkbox is checked under the 'Allow' column. The 'Change' and 'Read' checkboxes are also checked under the 'Allow' column.

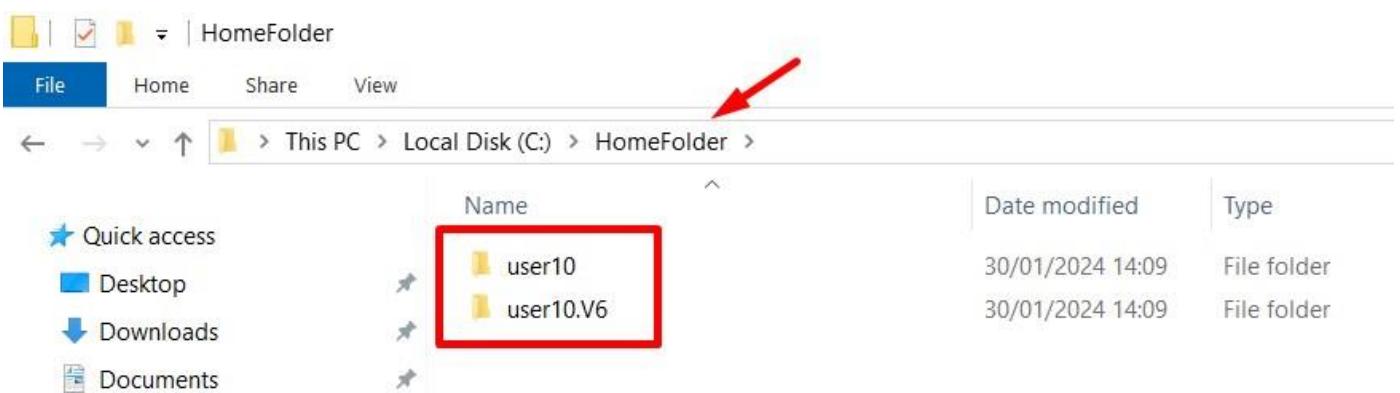
Permissions for Everyone	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Change	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>

-Roaming Profile -

- עוברים להגדרות החשבון ב-AD ומוסיפים את הנתיב לティקיה החדשה

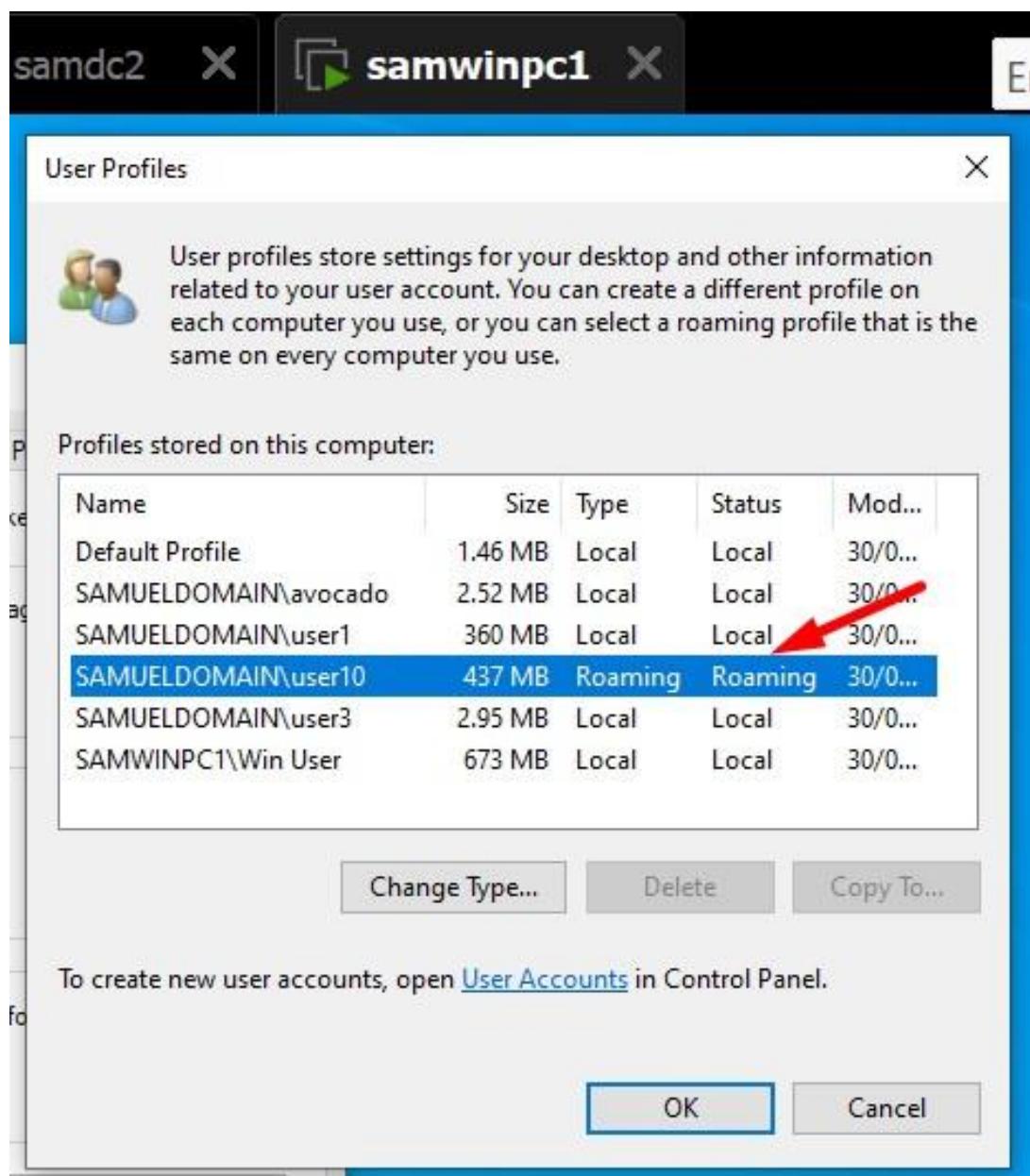


- לאחר הרשאה הראשונה של המשתמש ב-PC1, אפשר לראות שבתיקיה HomeFolder נוצרה תיקייה האישית של המשתמש



-Roaming Profile -

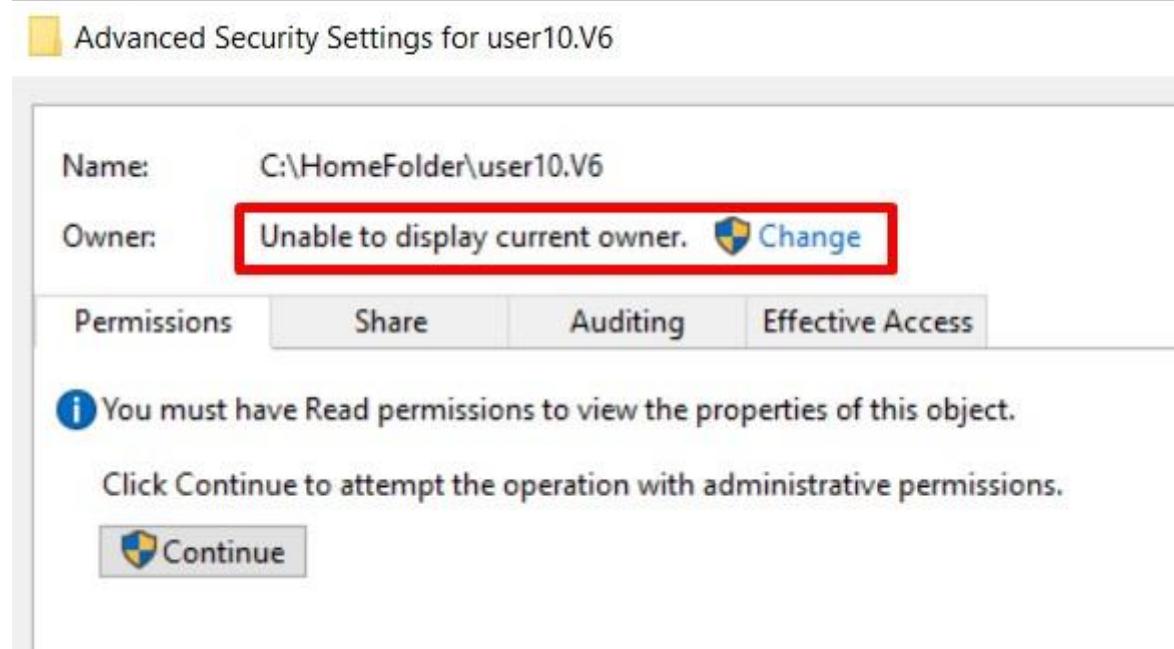
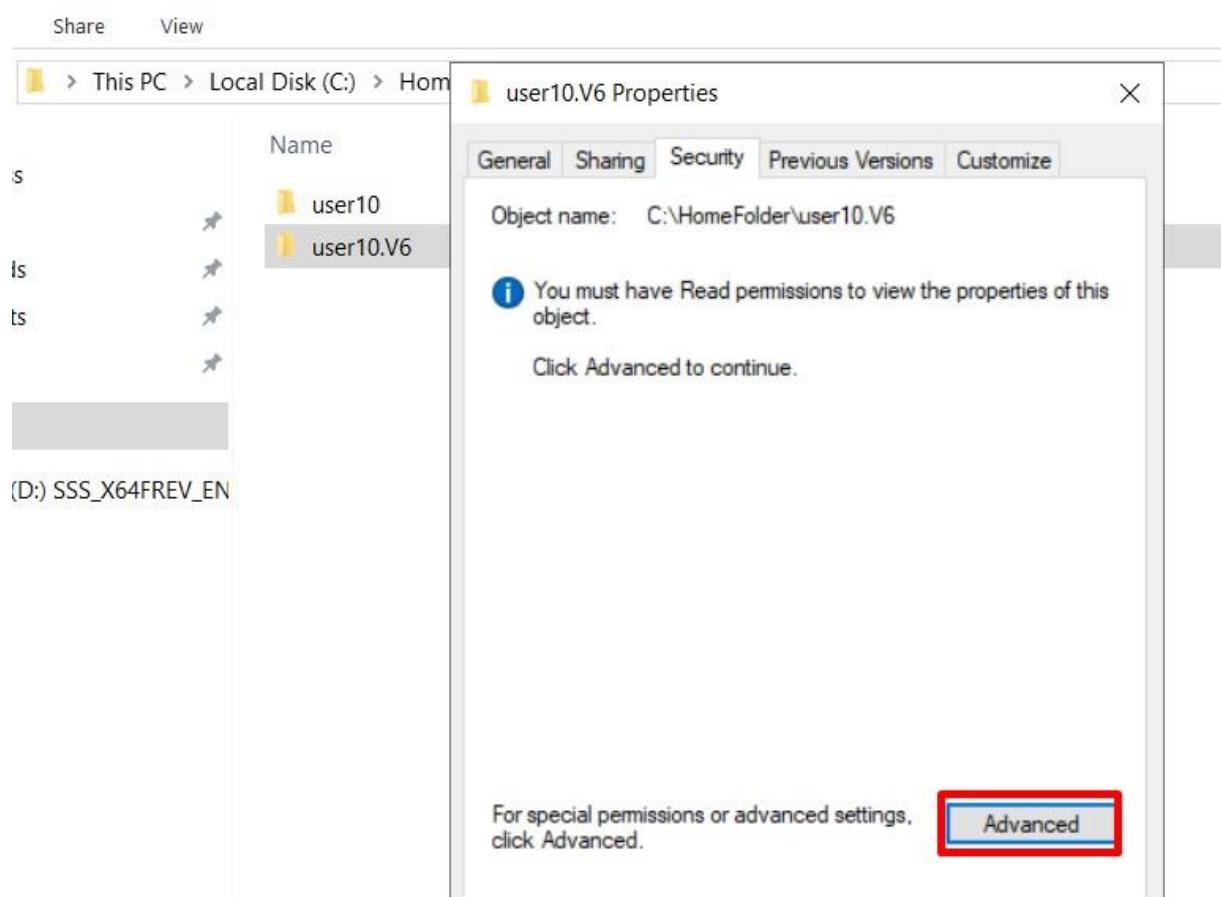
- בהגדרות משתמש המחשב אפשר לראות לראות של USER10 יש כרופיל נודז



-Roaming Profile -

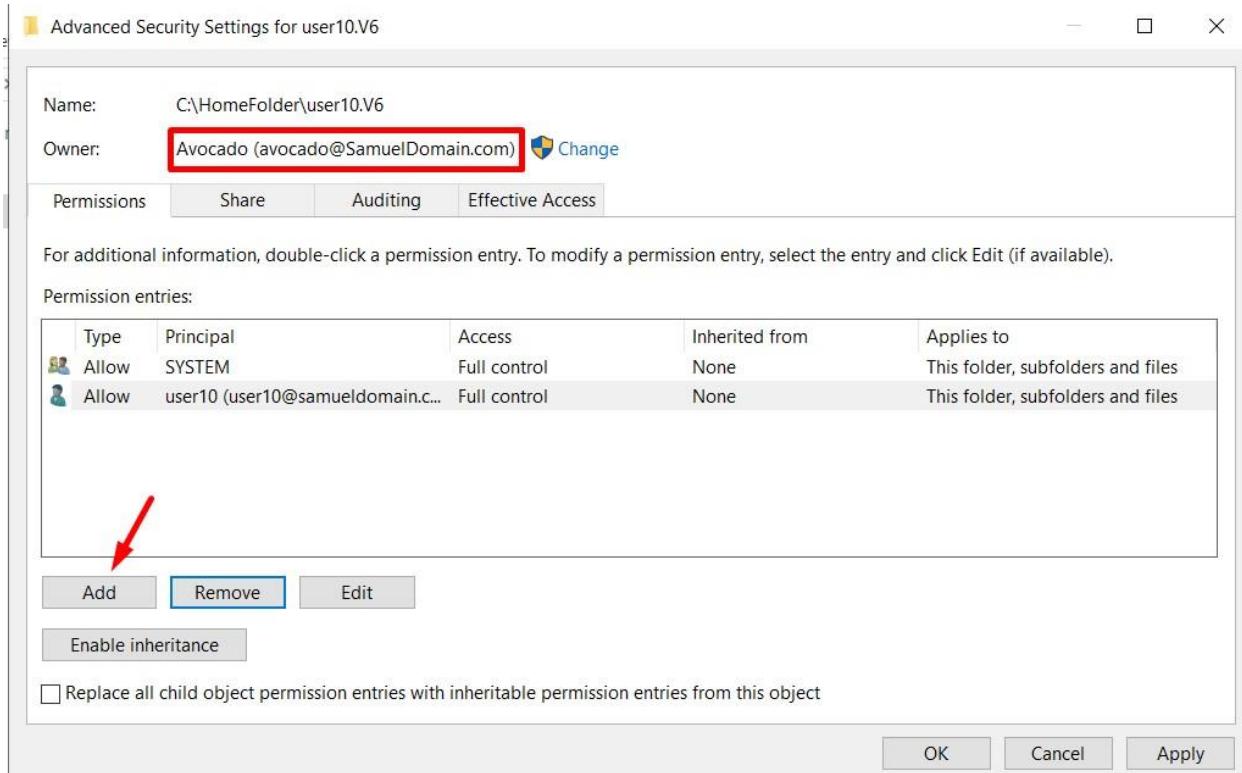
שנה את ההגדרות כך שמנהל הרשות יוכל להכנס לתיקייה
הפרופיל בשרת (Domain Admin)

- עכשו אנו צריכים לשנות את הרשות כך שרק לאדמין תהיה גישה לתיקיה . אבל בשביל זה חייב להוסיף אותו כבעליים של התיקיה כדי לתת אפשרות זו זאת.

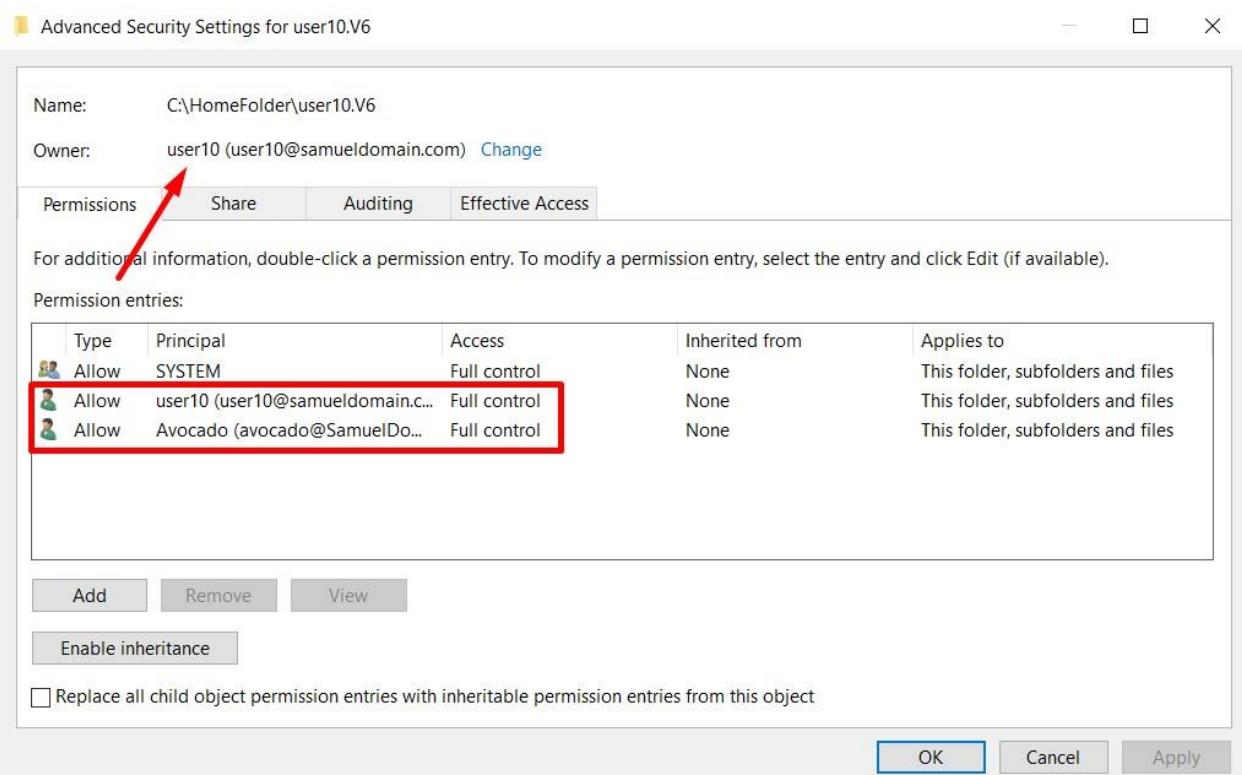


-Roaming Profile -

- מוסיפים את AVOCADO כבעליים של התקינה

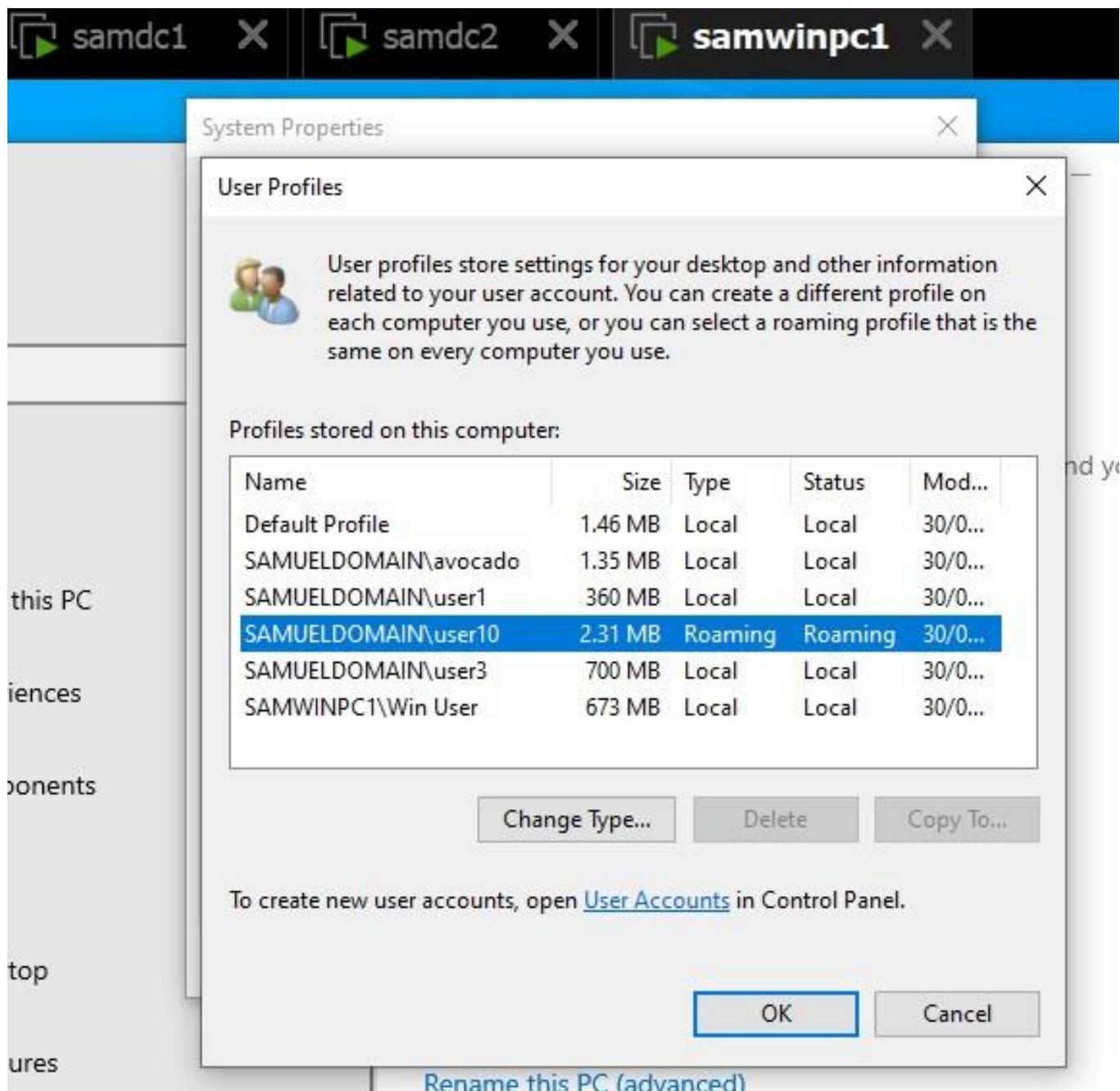


- נותנים לו הרשות של FULL CONTROL, ומוחזירים את USER10 כבעליים



-Roaming Profile -

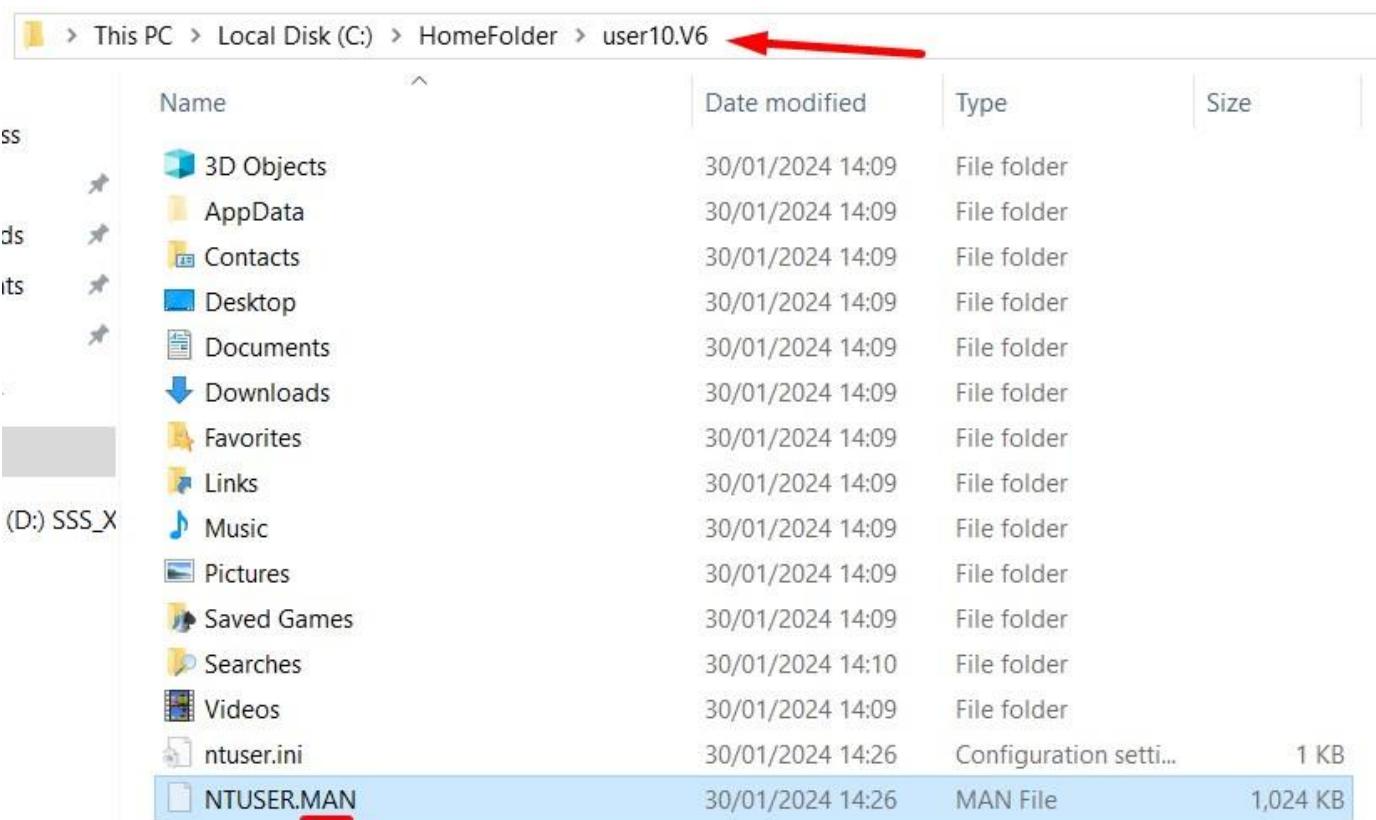
- בדוקים שהפרופיל עובד והוא ממשיך להיות נודד



-Roaming Profile -

שנה את הגדרות הפרופיל כך שהוא יהיה מנדטורי – כלומר – לא
ניתן יהיה לשנות שום דבר בפרופיל

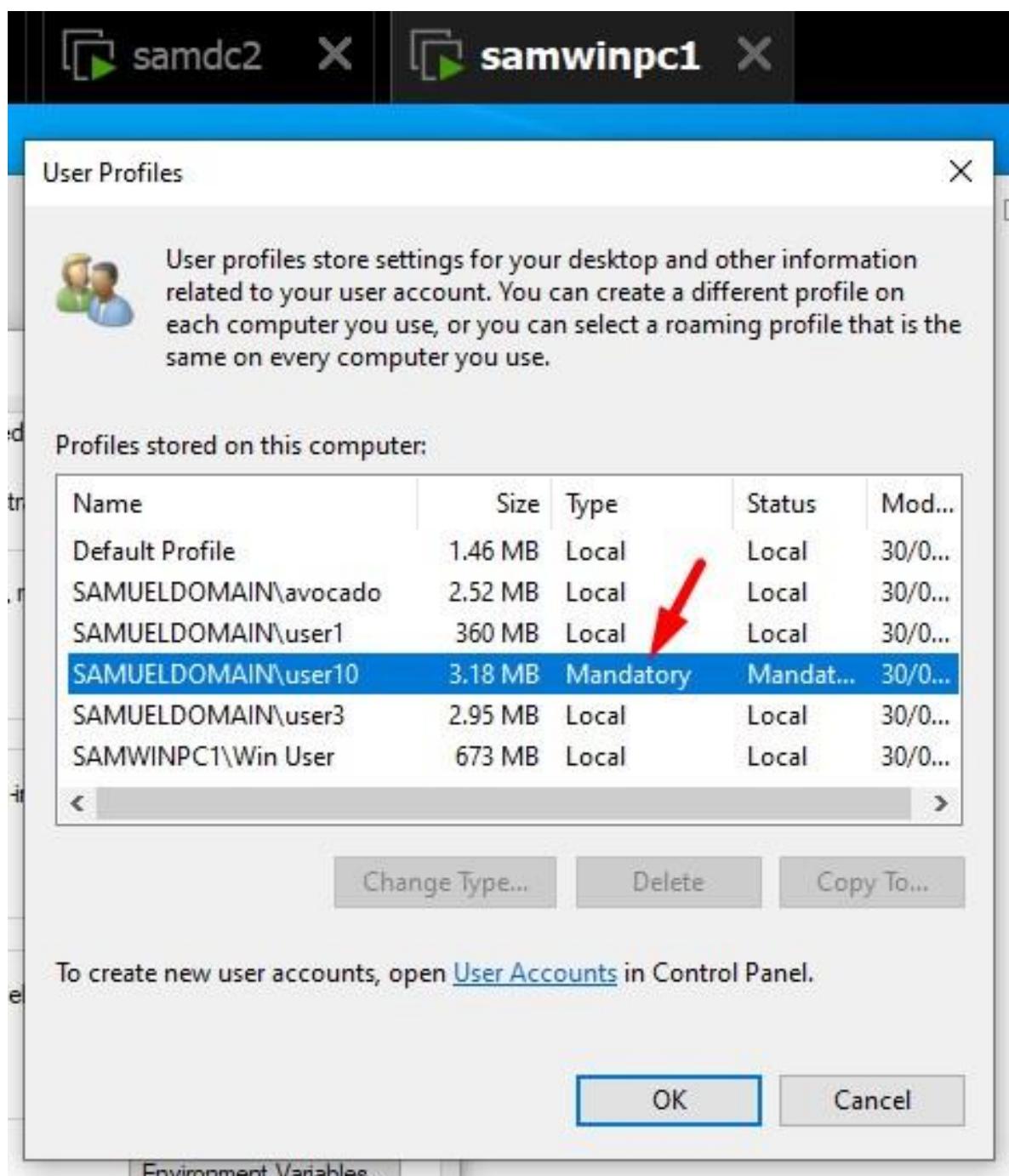
- פרוֹפִיל MANDATORY ב-Active Directory הוא סוג של פרוֹפִיל משתמש המאוחסן בשרת ואין לו אפשרות למשתמשים לבצע שינויים בהגדרות תוכן כדי כניסה או תוקן כדי עבודה.
- אנחנו צריכים לשנות את קובץ בתיקיית הпрофайл מ- NTUSER.DAT ל- NTUSER.MAN כדי להפוך את הпроֹפִיל לMANDATORY



	Name	Date modified	Type	Size
ss	3D Objects	30/01/2024 14:09	File folder	
ds	AppData	30/01/2024 14:09	File folder	
its	Contacts	30/01/2024 14:09	File folder	
	Desktop	30/01/2024 14:09	File folder	
	Documents	30/01/2024 14:09	File folder	
	Downloads	30/01/2024 14:09	File folder	
	Favorites	30/01/2024 14:09	File folder	
	Links	30/01/2024 14:09	File folder	
(D:) SSS_X	Music	30/01/2024 14:09	File folder	
	Pictures	30/01/2024 14:09	File folder	
	Saved Games	30/01/2024 14:09	File folder	
	Searches	30/01/2024 14:10	File folder	
	Videos	30/01/2024 14:09	File folder	
	ntuser.ini	30/01/2024 14:26	Configuration setti...	1 KB
	NTUSER.MAN	30/01/2024 14:26	MAN File	1,024 KB

-Roaming Profile -

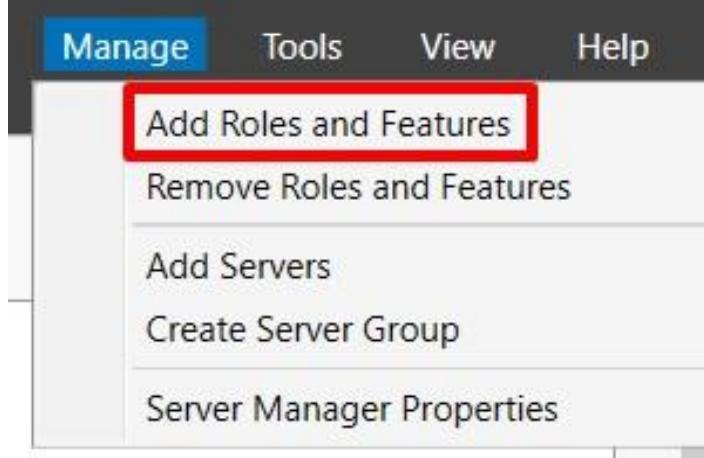
- **עכשו הпроfil הפץ להיות Mandatory**



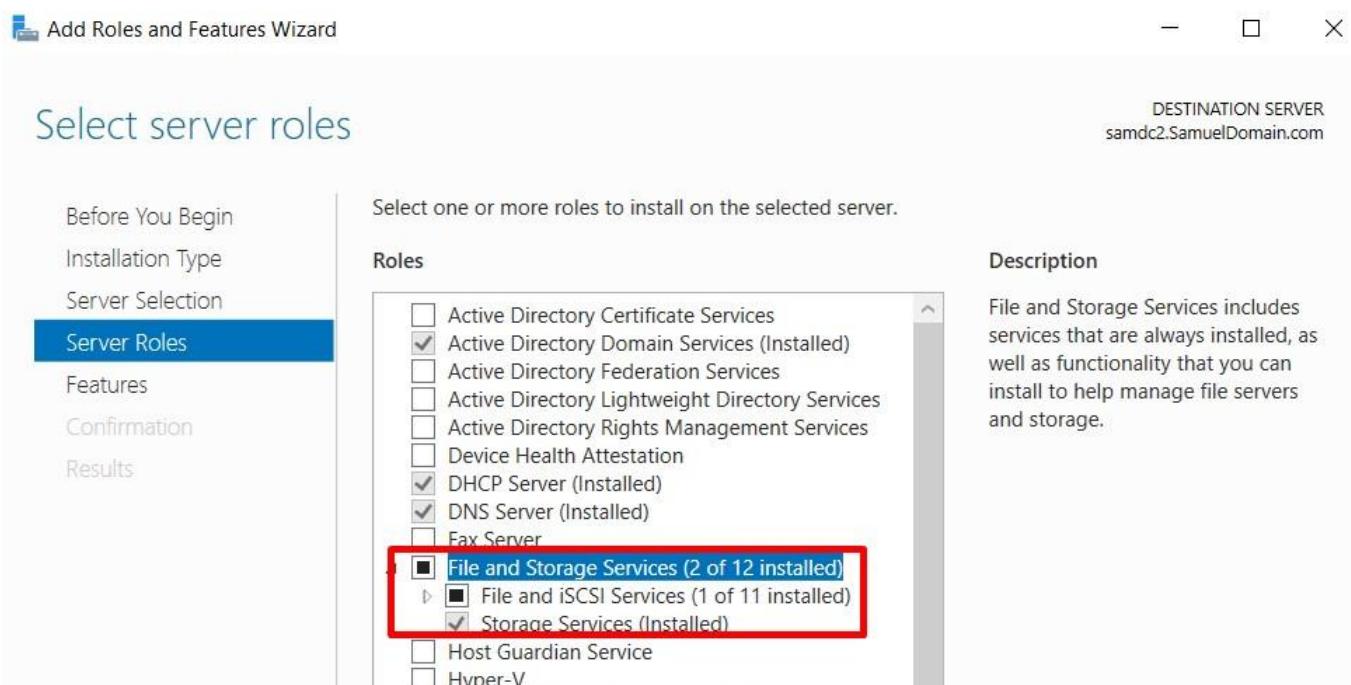
- שיתופים ומיפויים – שירות קבצים -

הגדרת שירות DC2 כשירות קבצים – (התקנת Role) {במידה ושרת הותקן כ Core Server DC2 ניתן להגדיר שירות הקבצים יהיה שירות DC1}

- שירות קבצים הוא מחשב ברשות המียวע לאחסן ולניהול קבצים ונתונים שאלייהם יש למשתמשים גישה.
 - MAPPING - הוא תהליך של מיפוי נתיב רשות לכונן במחשב המקומי. זה מאפשר למשתמשים לגשת במהירות למשאבים מרוחקים
- כתע עליינו להתקין את תפקיד השירות הקבצים ב-DC2



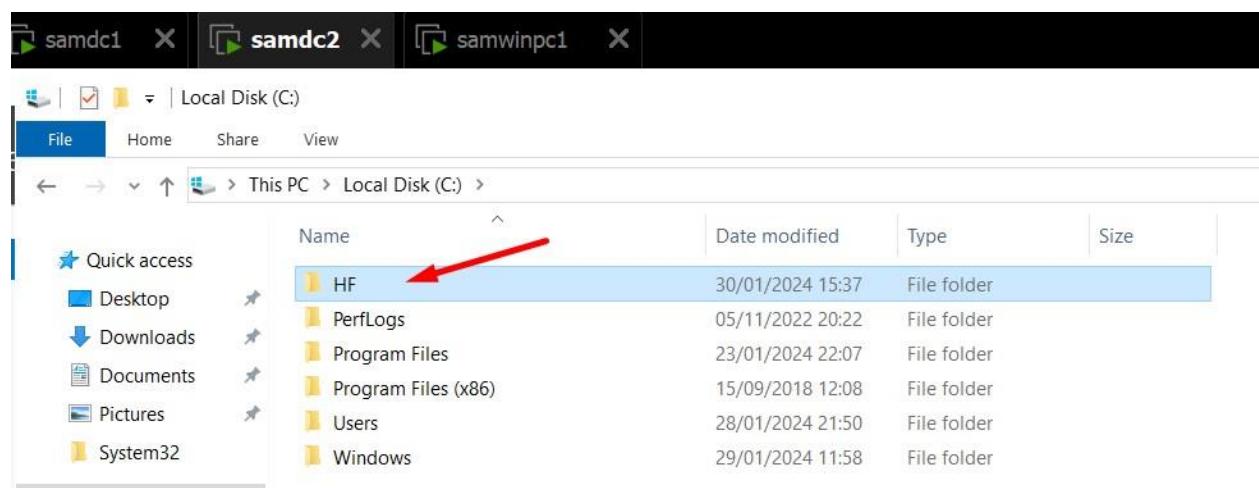
- מתקינים את התפקיד הזה וממשיכים להלאה



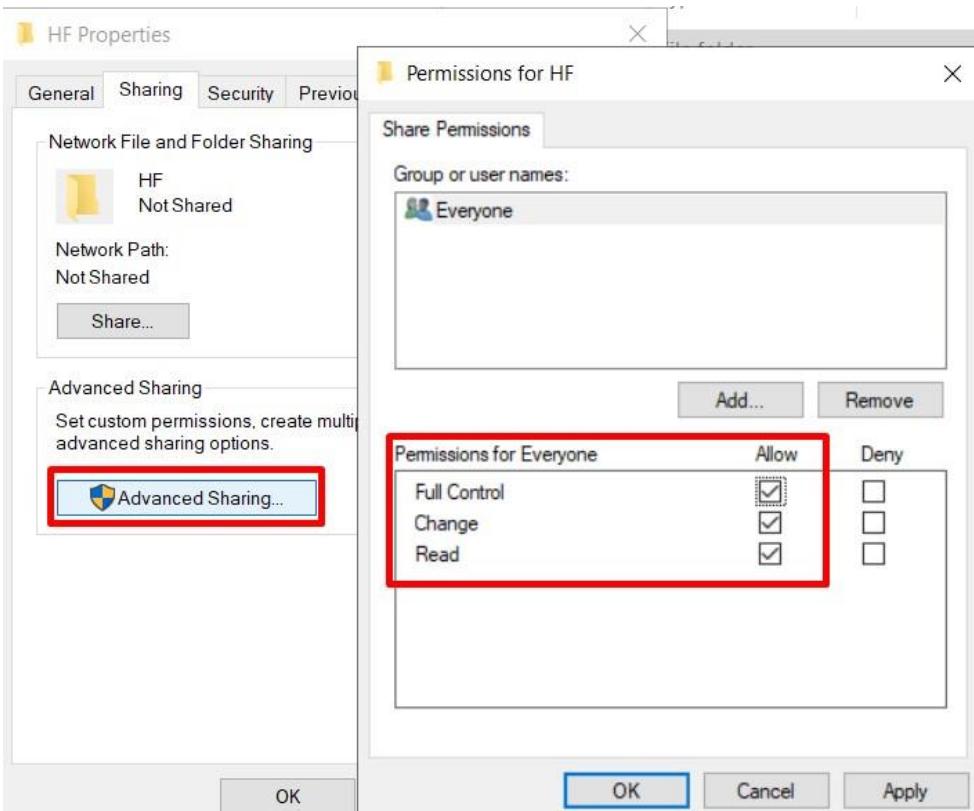
- שיתופים ומיפויים – שירות קבצים -

הגדיר לכ5 חשבונות *Home Folder*. عليك לוודא כי כל משתמש נגיש ל-*Home folder* שלו בלבד

- *HomeFolder* היא תיקייה מיוחדת בשירות קבצים המיעודת לאחסן נתונים אישיים וקבצים של משתמש ספציפי בסביבה ארגונית. לכל משתמש מוקצת תיקייה בית משלו שבה הוא יכול לשמר את הקבצים שלו
- קודם כל, בואו ניצור תיקייה חדשה בשירות הקבצים DC2

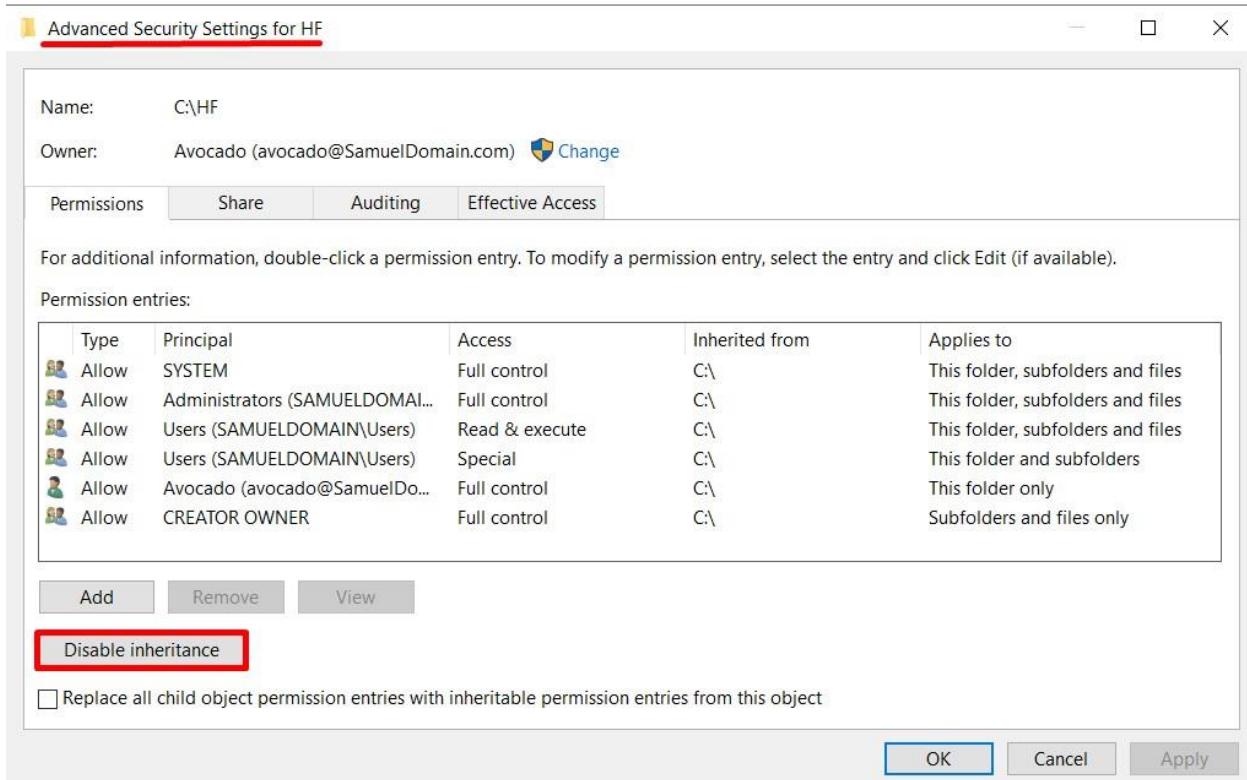


- עכשיו אנחנו צריכים לשתף אותה כדי שלמשתמשים יהיה גישה, אנחנו גם מגדירים הרשות לכולם



- שיתופים ומיפויים – שירות קבצים -

- מבטלים את הפקציה INHERITANCE של התיקיה כדי לשנות הרשות ולקבל שליטה מלאה



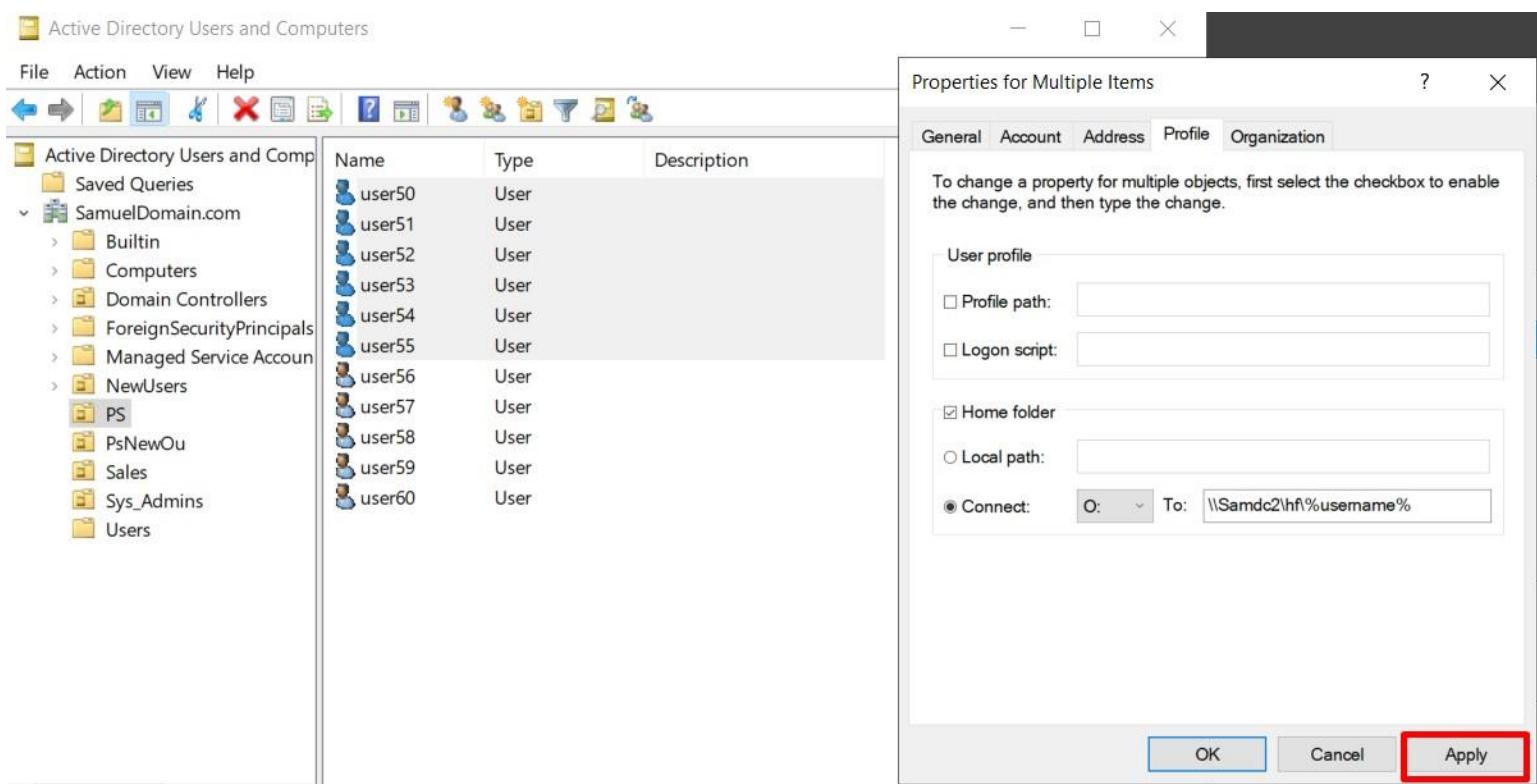
- משאים רק את ההרשאות הללו

Permission entries:

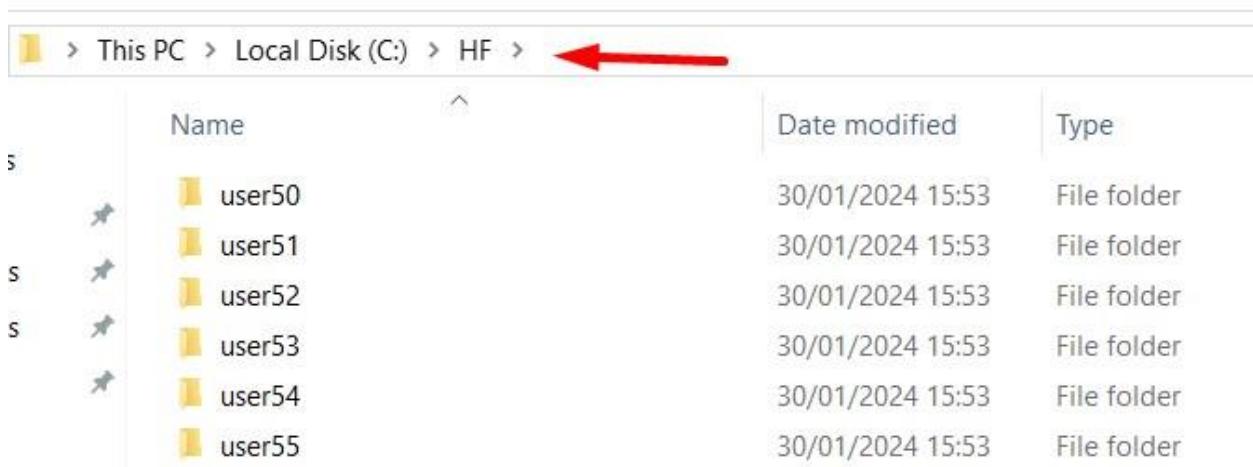
Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (SAMUELDOMAI...)	Full control	None	This folder, subfolders and files
Allow	Avocado (avocado@SamuelDo...)	Full control	None	This folder only
Allow	CREATOR OWNER	Full control	None	Subfolders and files only

- שיתופים ומיפויים – שירות קבצים -

- עוברים להגדרות החשבון של 5 משתמשים ב-AD ומוסיפים את הנתיב לתיקיה החדשה %username% הוא משתנה במערכות הפעלה של Windows
- שוחף אוטומטית בשם המשתמש הנוכן

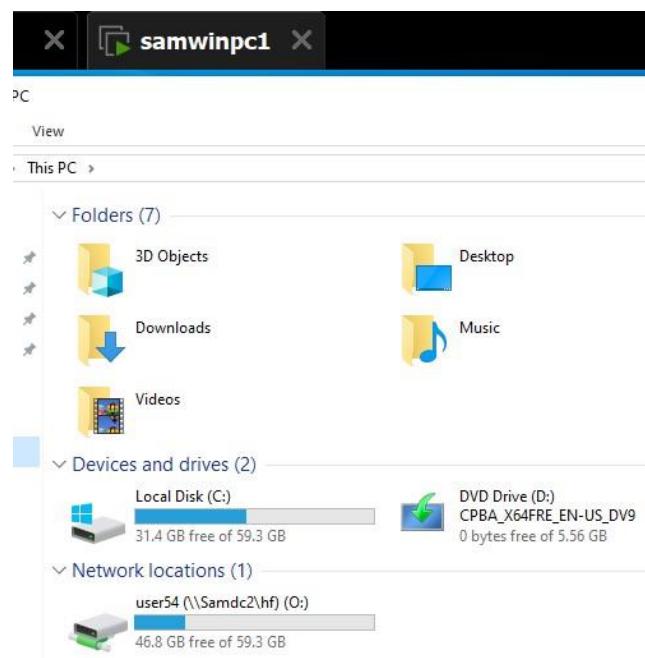
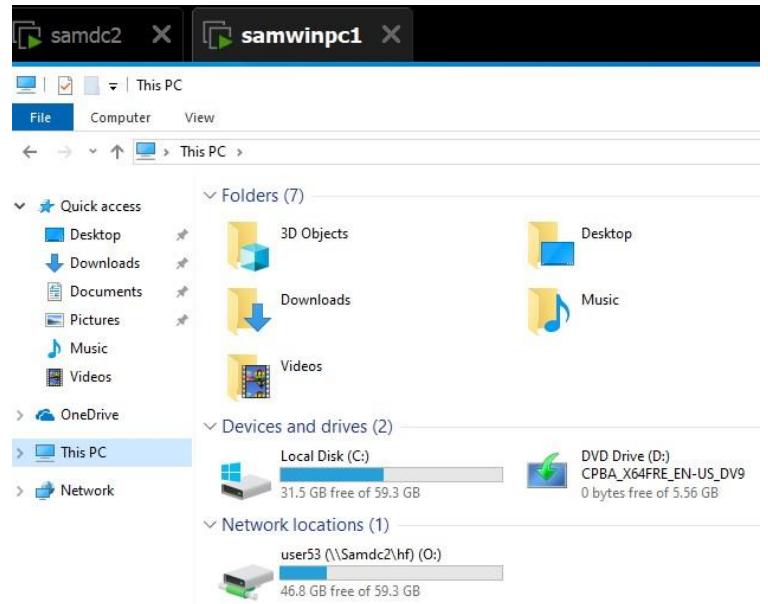
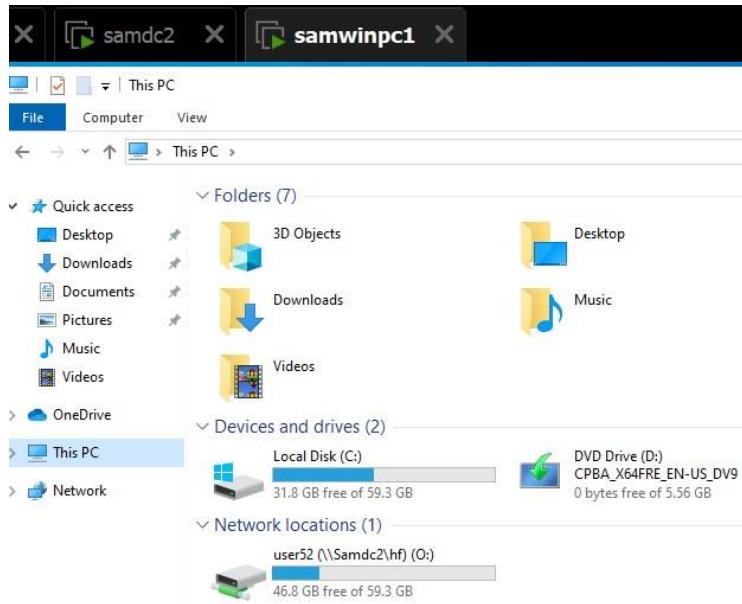
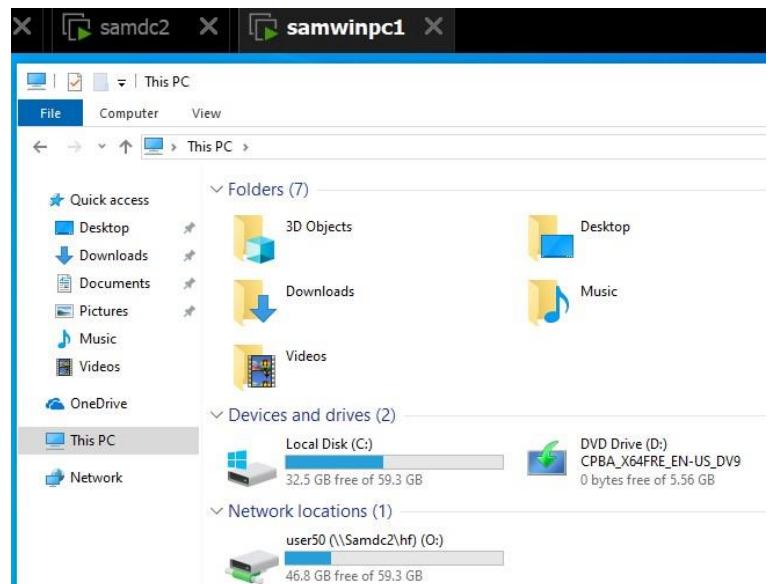
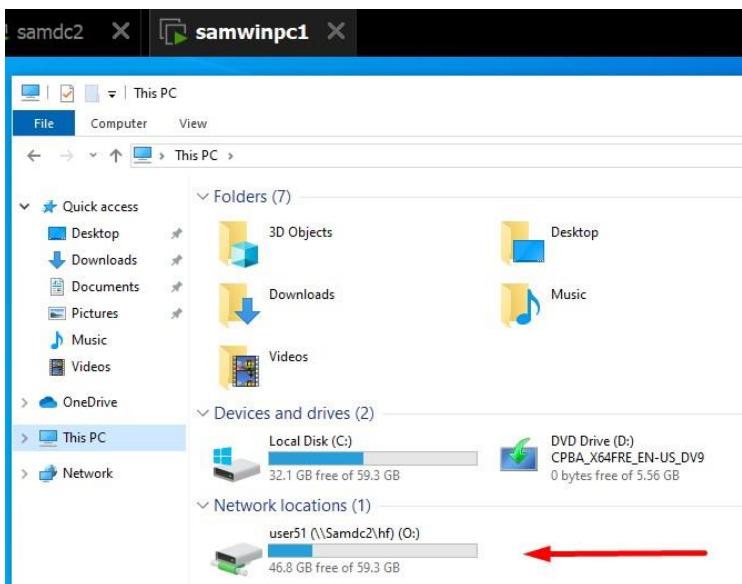


- כפי שאפשר לראות, תיקיות משתמש נוצרו אוטומטית בתיקיה HF



- שיתופים ומיופיעים – שירות קבצים -

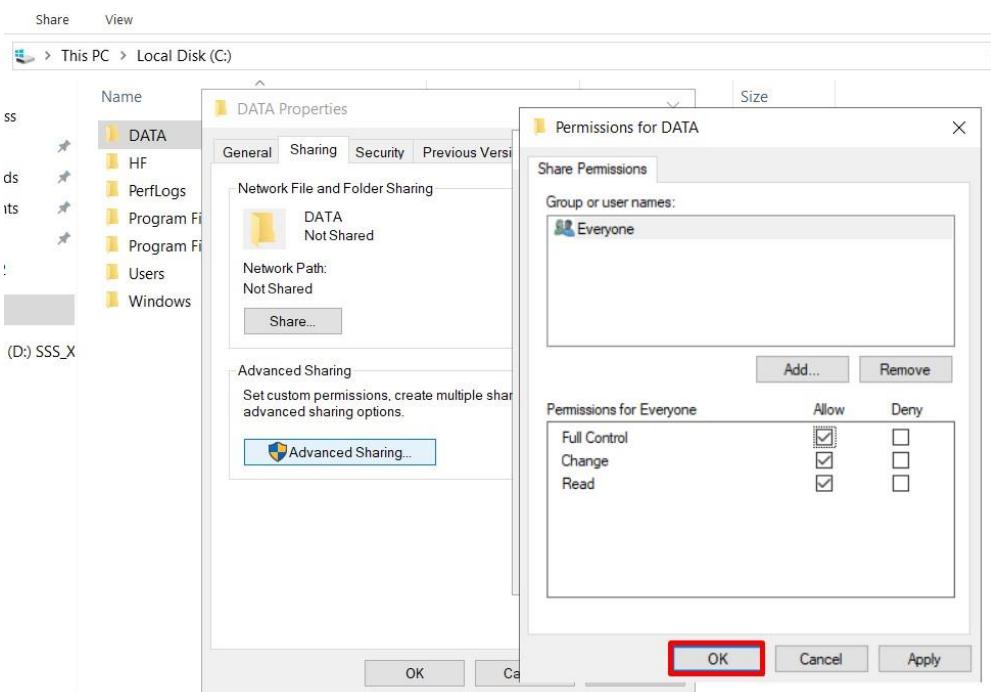
• בודקים שהדיםקים נוצרו



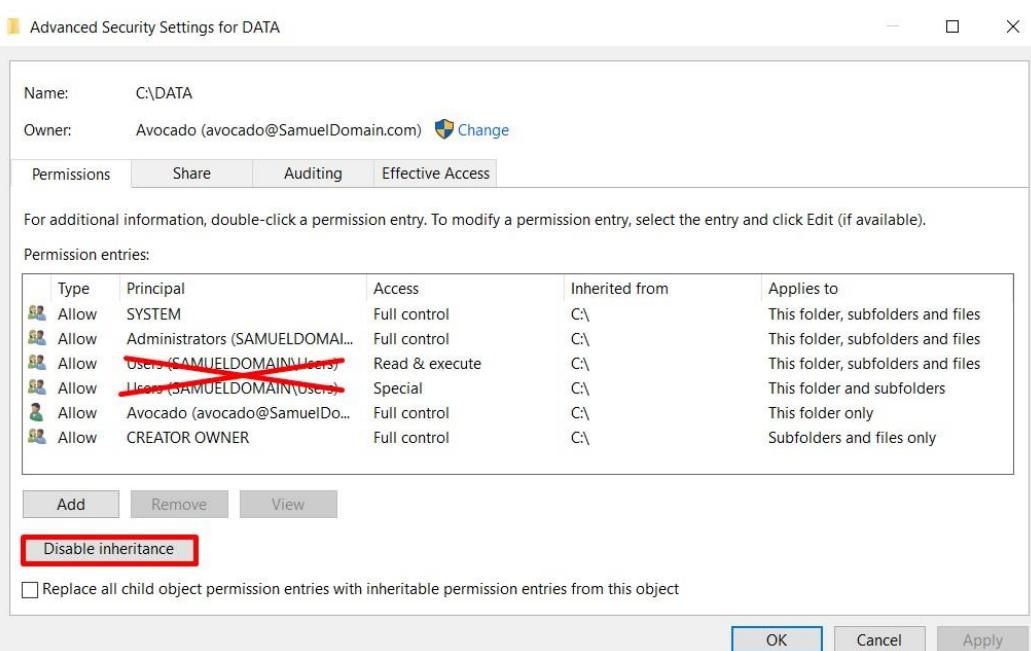
- שיתופים ומיפויים – שירות קבצים -

שיתוף תיקייה – צור ב-DC2 תיקייה משותפת בשם DATA . וצור בנתוך התיקייה קובץ txt

- אנו יוצרים תיקייה ב-DC2 ומשתפים אותה

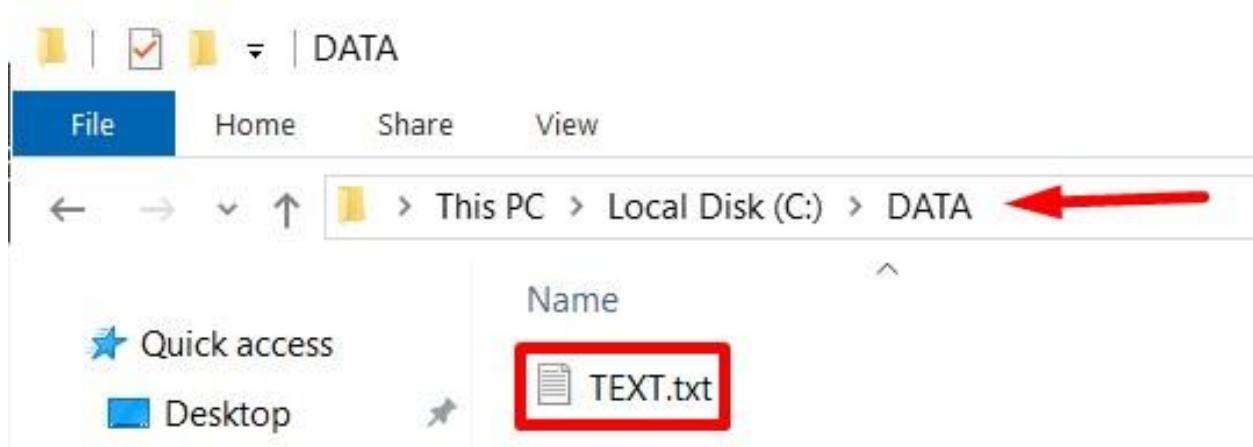


- מבטלים את הפעונציה INHERITANCE של התיקייה כדי לשנות הרשותות ולקבל שליטה מלאה



- שיתופים ומיפויים – שירות קבצים -

- אנו יוצרים מסמך טקסט בתיקיית DATA



- שיתופים ומיפויים – שירות קבצים -

ניהול הרשאות דאג לכך שהיו הרשותות הגישה לתיקייה המשותפת:

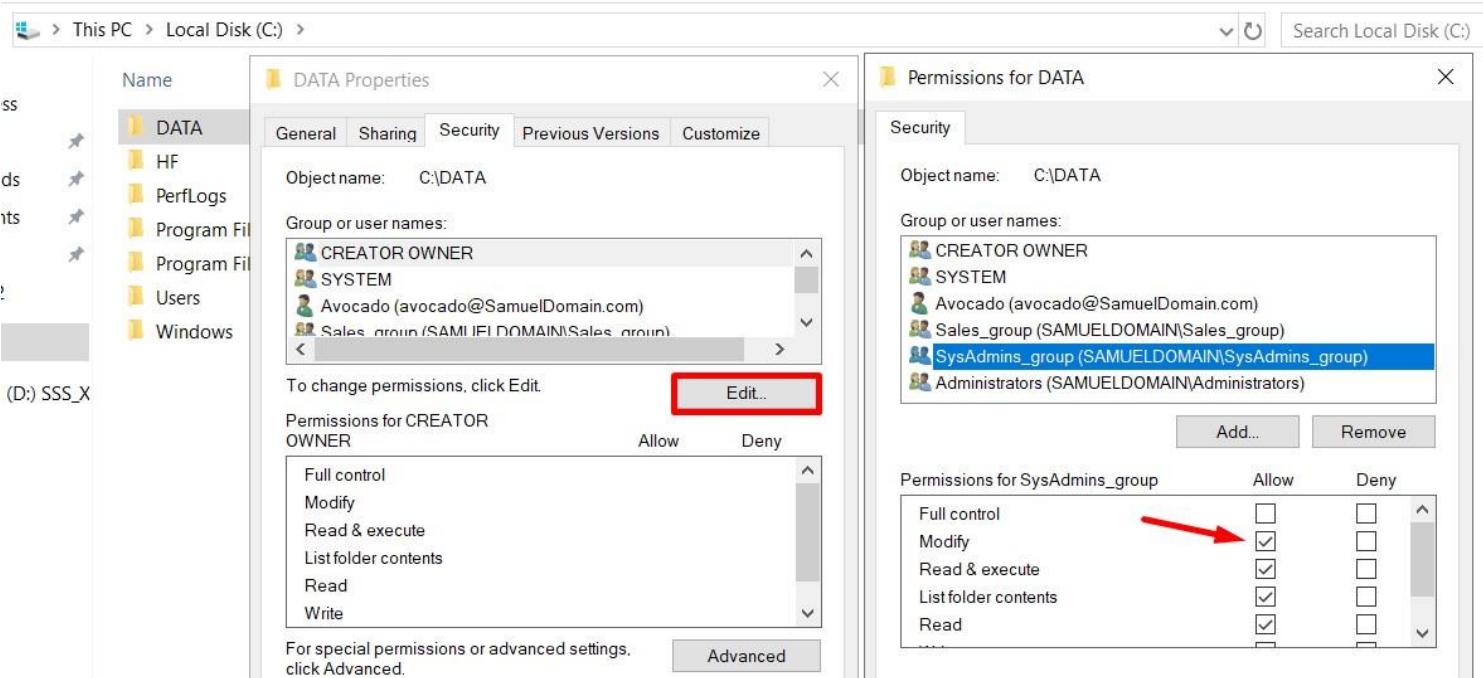
הרשאת Modify לקובוצת Sys Admins

הרשאת Read & execute לקובוצת Sales

זכור כי הרשותות שיתוף הינו הרשותות משולבות.

- בעת ניתן הרשותות לתיקייה לקובוצות שיצרנו קודם

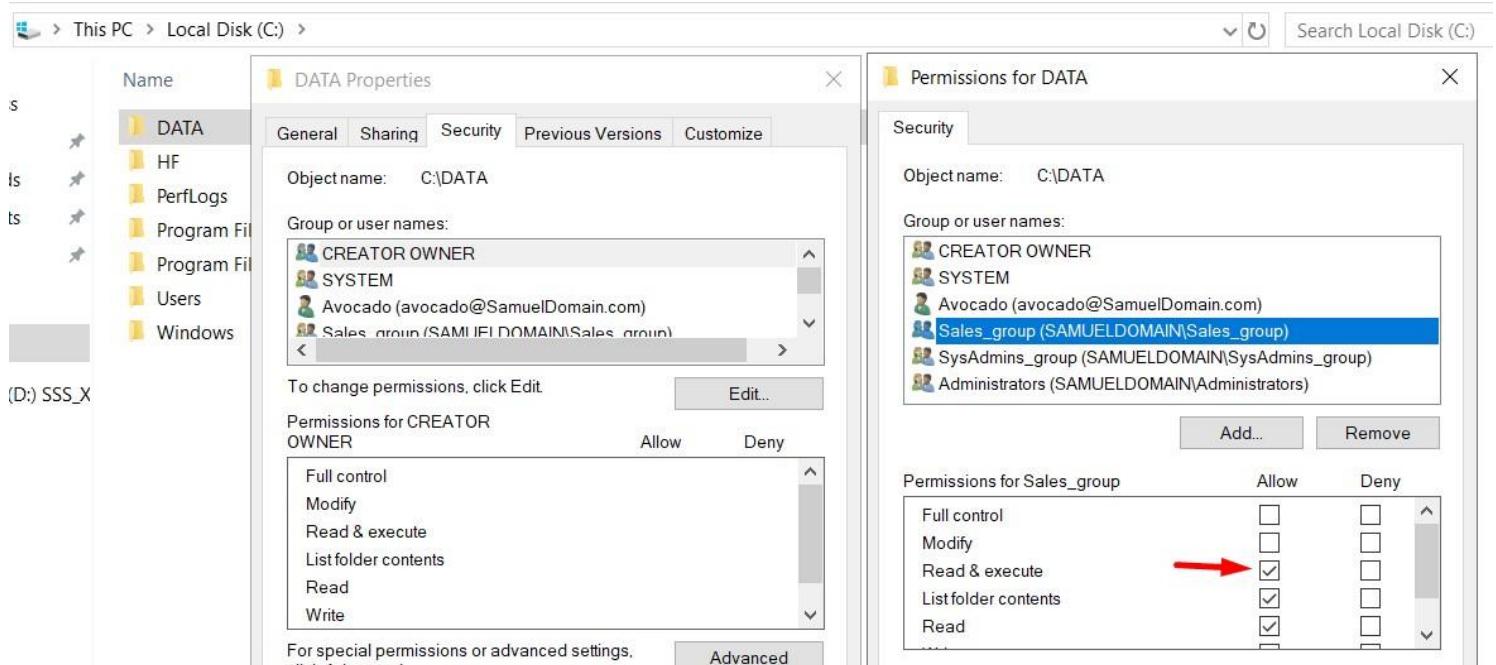
SysAdmins:



- ההרשאה "MODIFY" מעניקה לקובוצה זו את היכולת להציג, לשנות, להוסיף ולמחוק קבצים בתיקייה, כולל את היכולת לשנות תכונות של קבצים ותת תיקיות. הרשאה זו מעניקה לך גישה מלאה לתוכן התיקייה, למעט שינוי הרשותות על התיקייה עצמה ועל תוכנה.

- שיתופים ומיפויים – שירות קבצים -

Sales:

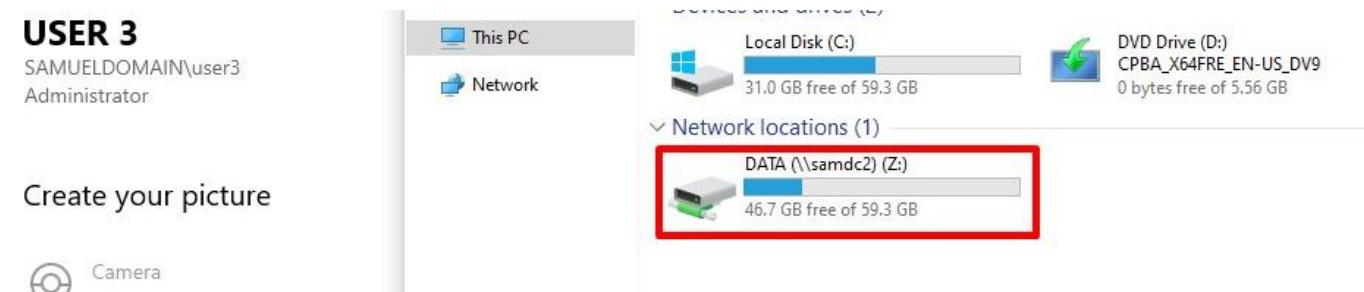
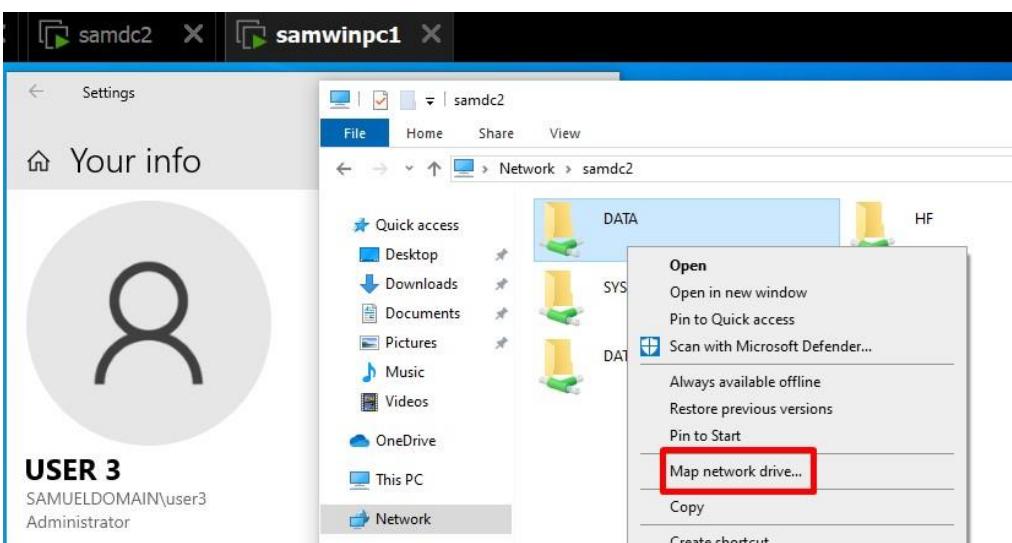
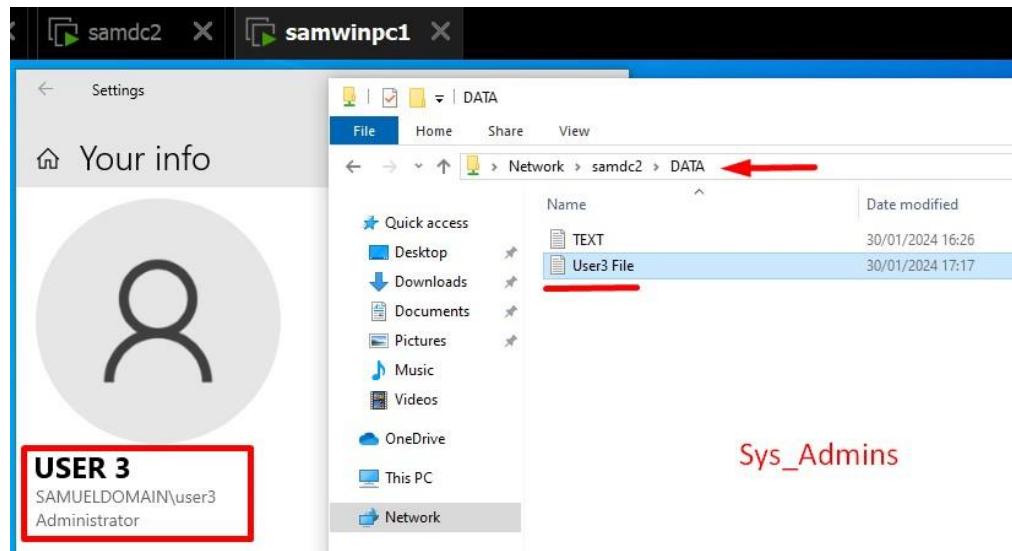


- הרשות "READ AND EXECUTE" משתמשים בעלי הרשאה זו יכולים לפתח ולקראן קבצים, כמו גם להפעיל קבצי הפעלה או תוכניות הנמצאות בתיקייה והם אינם יכולים לשנות קבצים או ליצור קבצים חדשים בתיקייה זו.

- שיתופים ומיפויים – שירות קבצים -

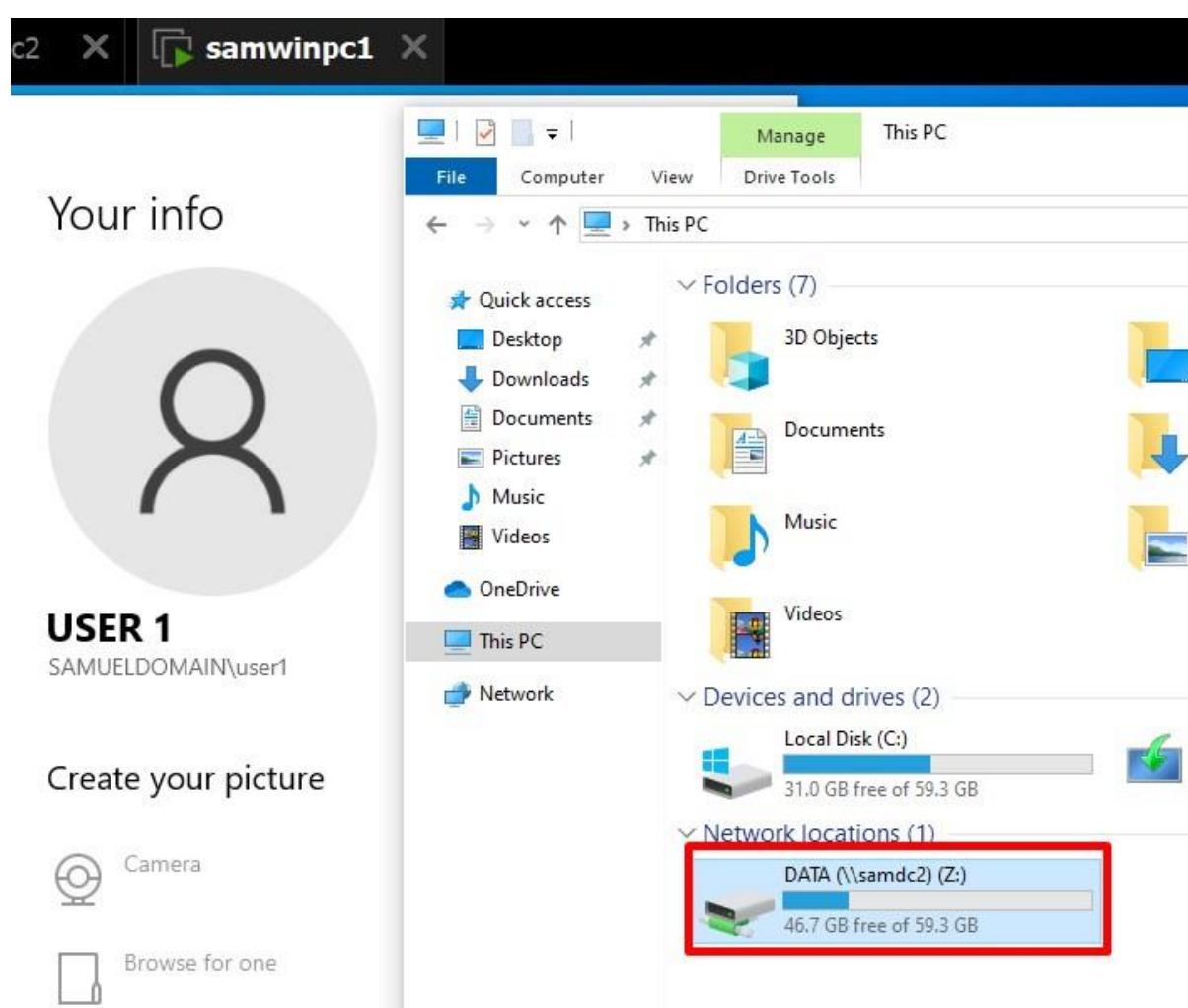
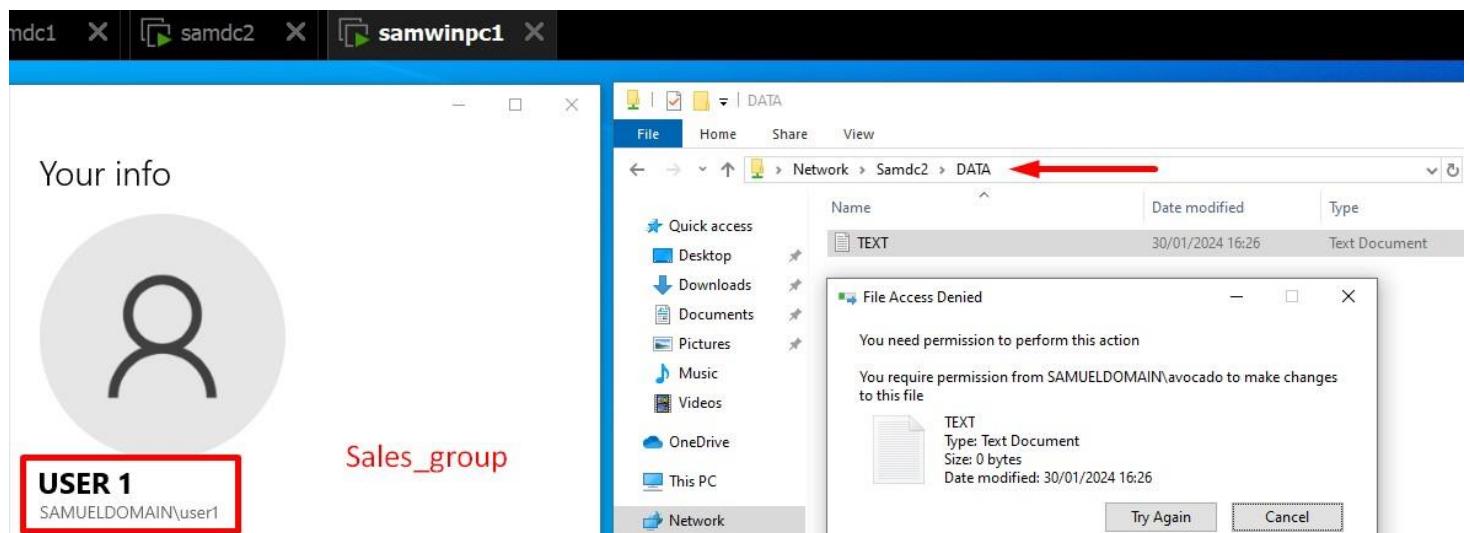
מייפוי כונן רשות-מפה את התיקייה לכל המשתמשים ובודק שההרשאות שלהם נכונות. את הבדיקה בצד WIN10

- אנו יוצרים קישור לדיסק ובודקים את הרשאות Sys_Admin
- יצרתי קובץ חדש משתמש של Sys_Admin



- שיתופים ומיפויים – שירות קבצים -

- לא הצלחתי למחוק את הקובץ TEXT ממשתמש Sales_Group

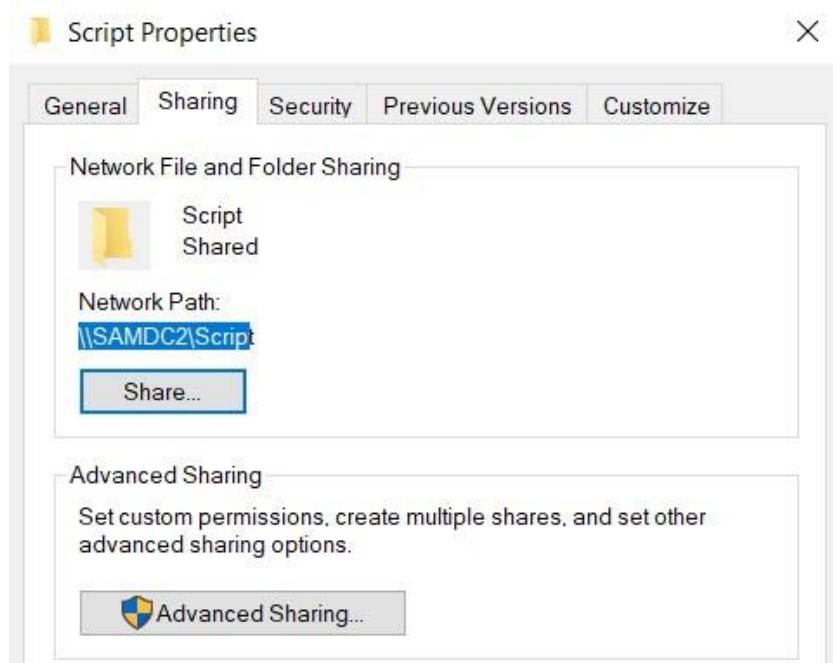
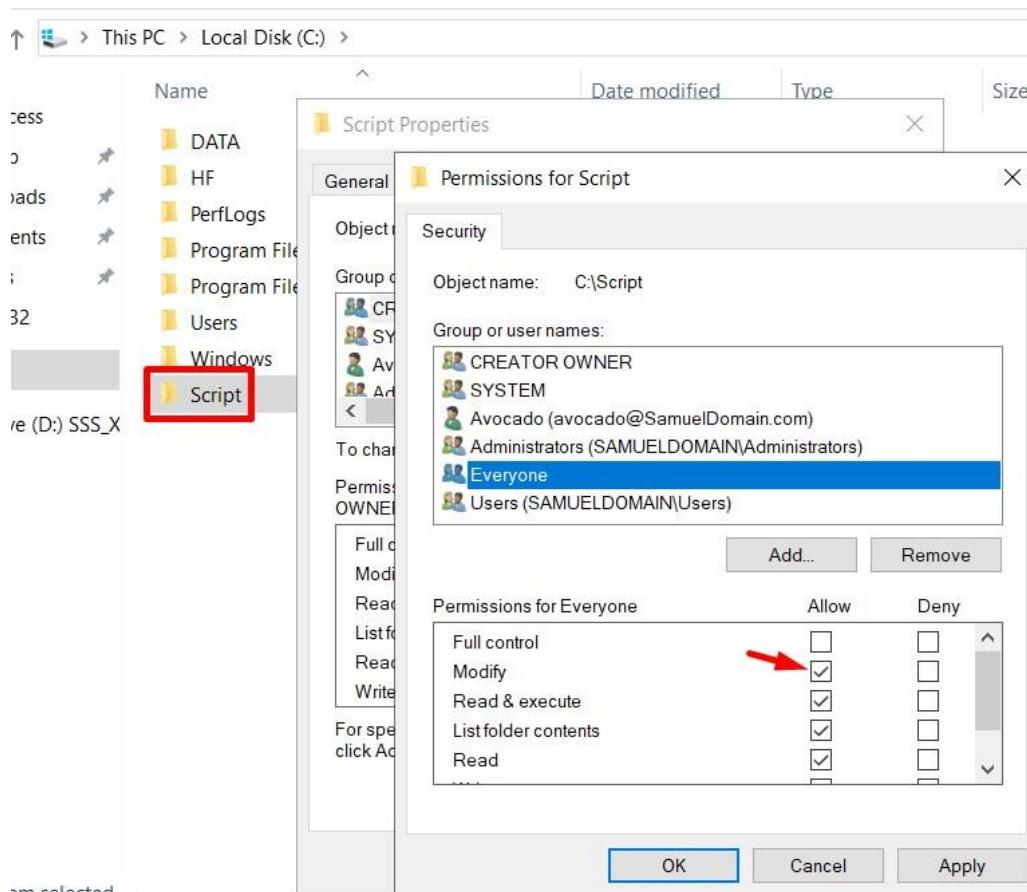


- שיתופים ומיפויים – שירות קבצים -

צור תיקייה משותפת נוספת ב-DC2 בשם DC2

תן הרשות Modify לקבוצה Everyone

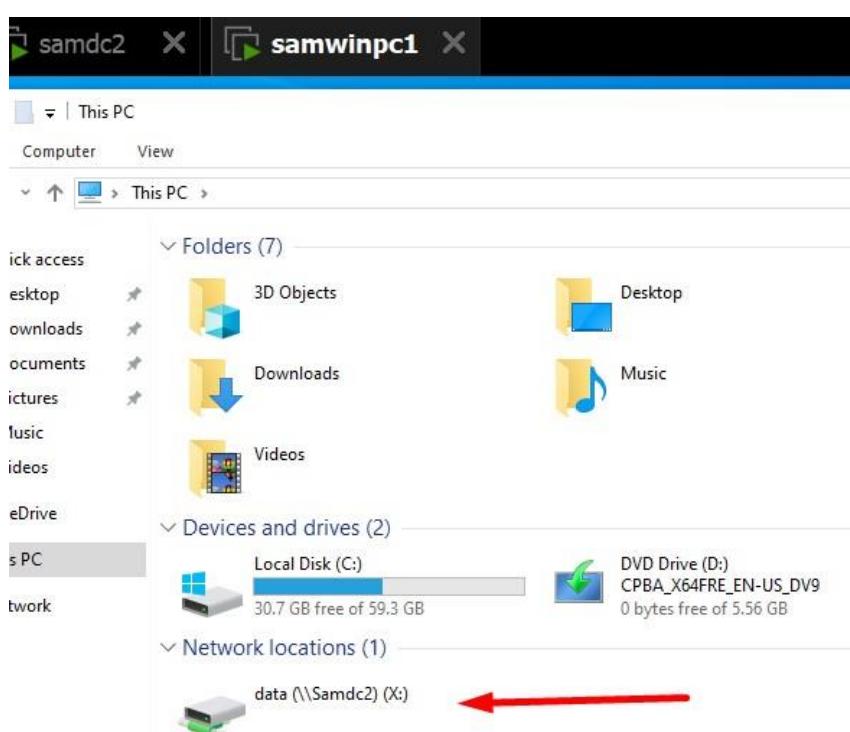
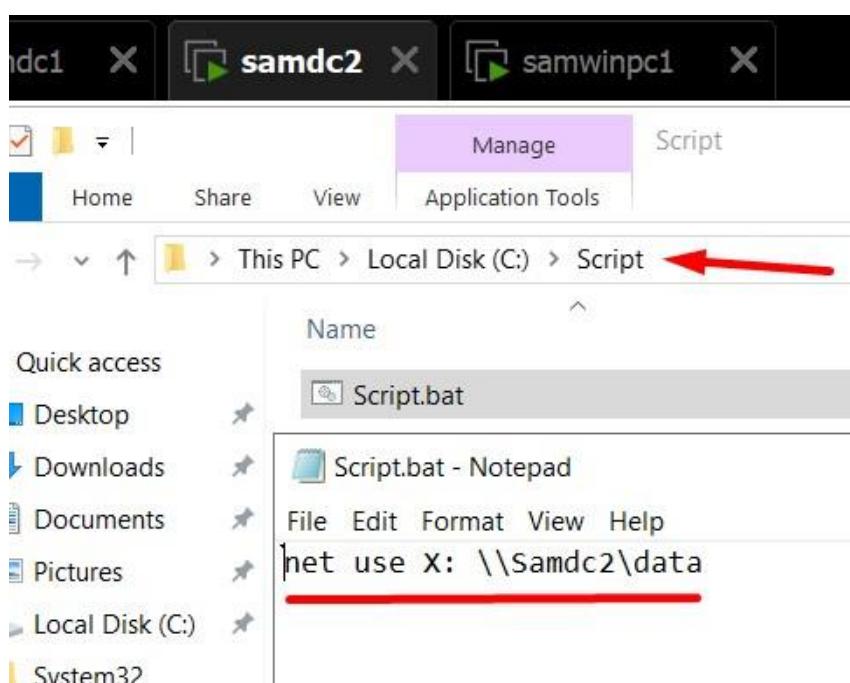
- אנו יוצרים תיקיה נוספת ונותנים הרשאה MODIFY למשתפים EVERYONE.



- שיתופים ומייפויים – שירות קבצים -

צור בתחום קובץ Batch שהמשתמש יפעיל ושייבצע את מייפוי
תיקיית data ככונן הרשות עבור המשתמש(השתמש בפקודה
use

- אנו יוצרים סקריפט שיפתח אוטומטית את תיקיית DATA בכונן X :
- עכשו למשתמשים יהיה קל יותר למצוא את הרתיקה הזו



- שיתופים ומיפויים – שירות קבצים -

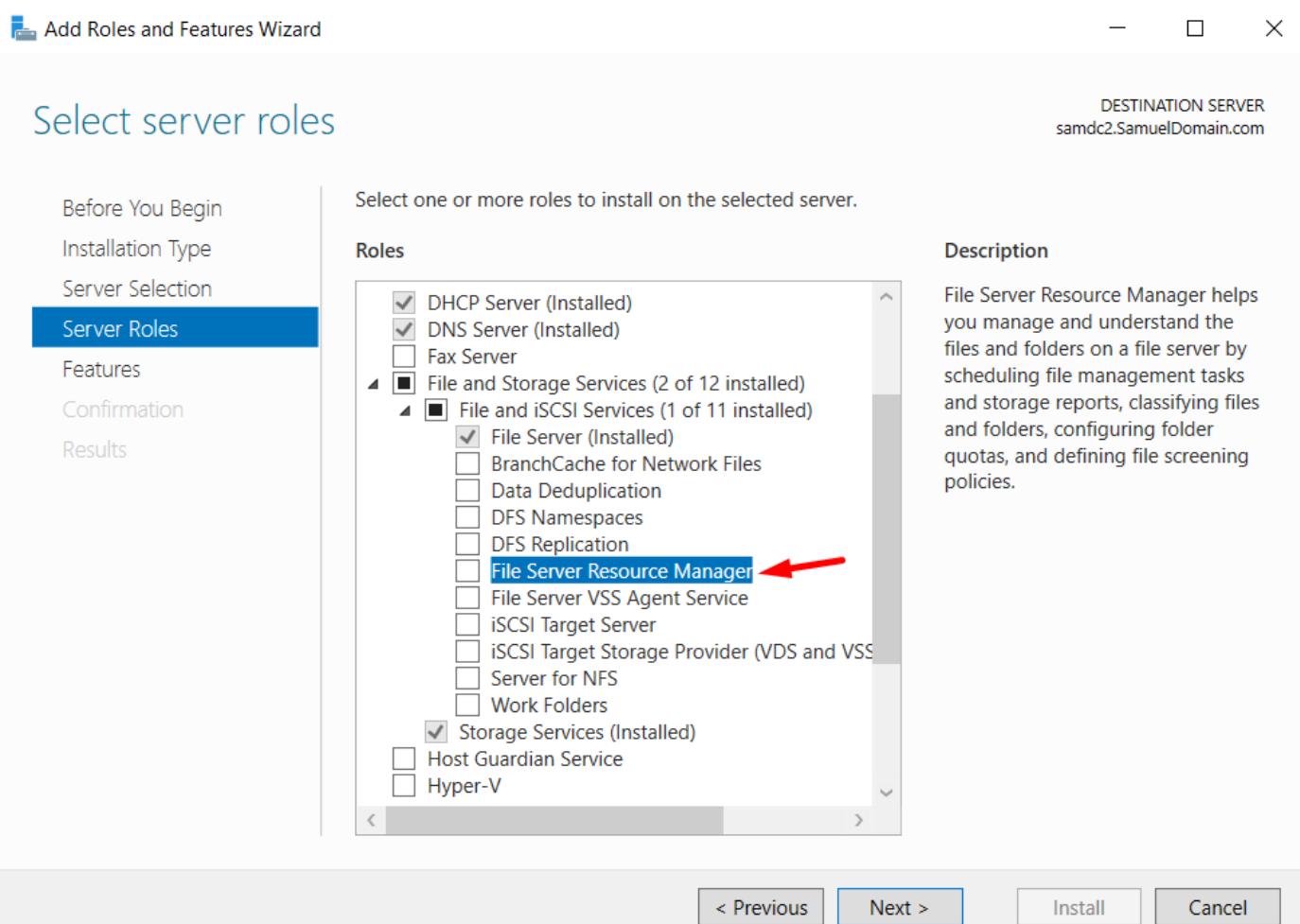
צור מכשה Quota לנפח השימוש של כל משתמש בתיקיות A VI Home Folder עד 5 GB ומנع מהמשתמשים לשמור קבצי AVI בתיקיות אלו.

- QUOTA ב-Active Directory, זהה בקרת גישה לשטח דיסק בשרת קבצים. הוא משמש להגבלת הנתונים שימושים או קבוצות משתמשים יכולים לאחסן בשרת קבצים.

עלינו יש להגביל את הזיכרון של התיקייה האישית ל-5 GB עבור כל משתמש ולאסור שמירת קבצי AVI

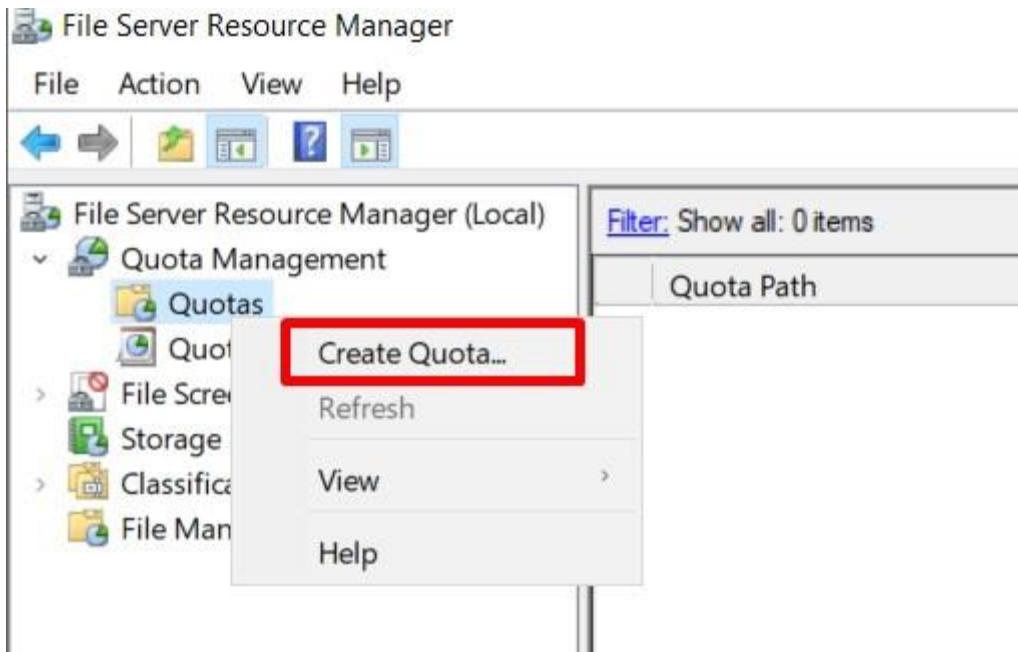
ו-AVI הוא אחד מפורמי הקבצים הנפוצים ביותר לאחסון אודיו ווידאו

- ראשית עלינו להתקין את התוסף של File Server Resource manager

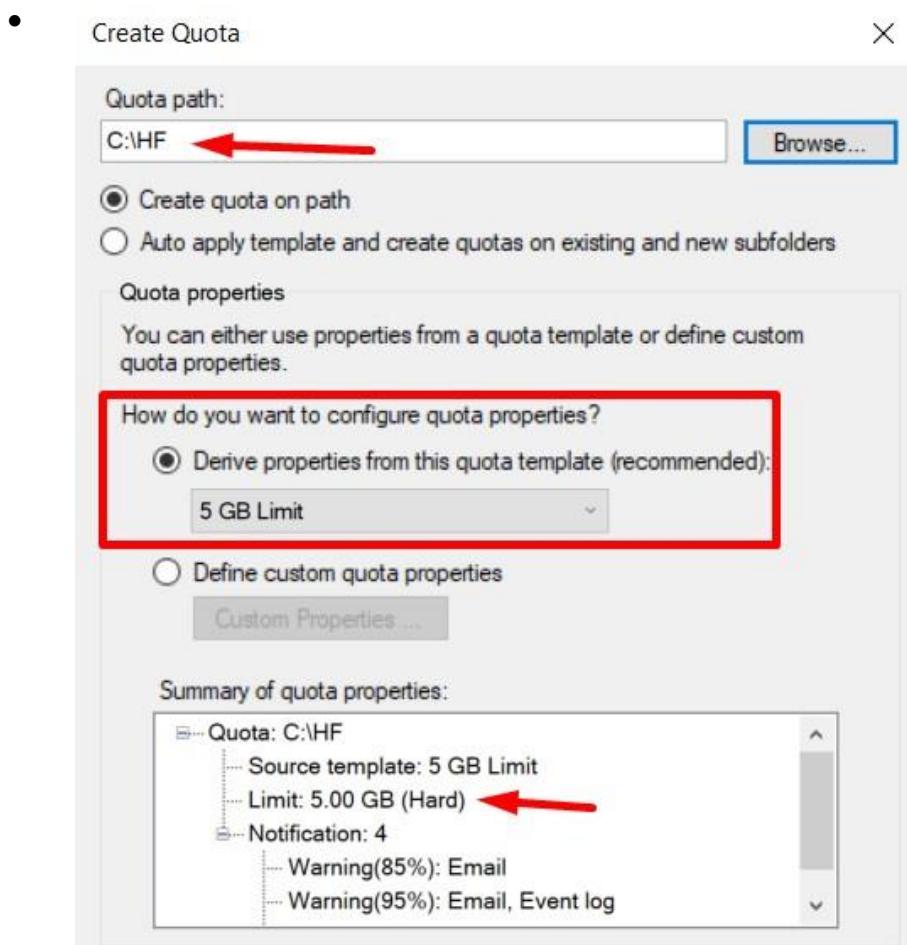


- שיתופים ומיפויים – שירות קבצים -

- לאחר ההתקנה, אנו עוברים למנהל הקבצים ויוצרים QUOTA

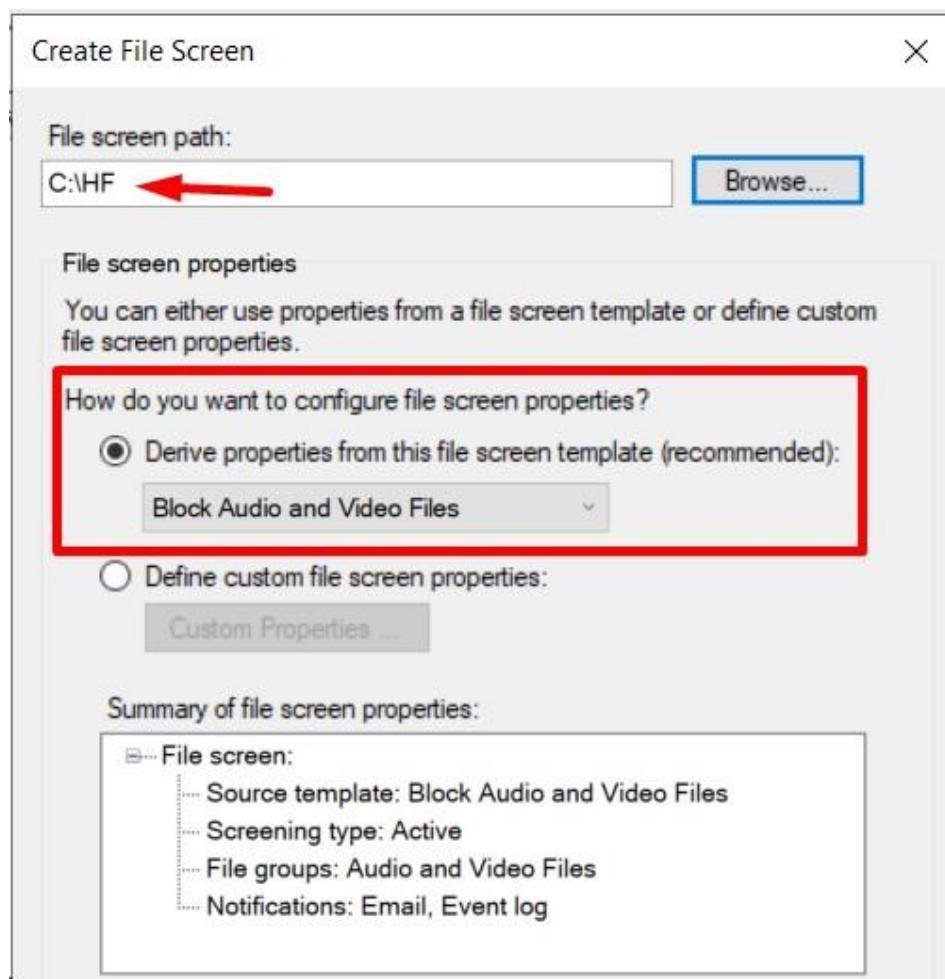
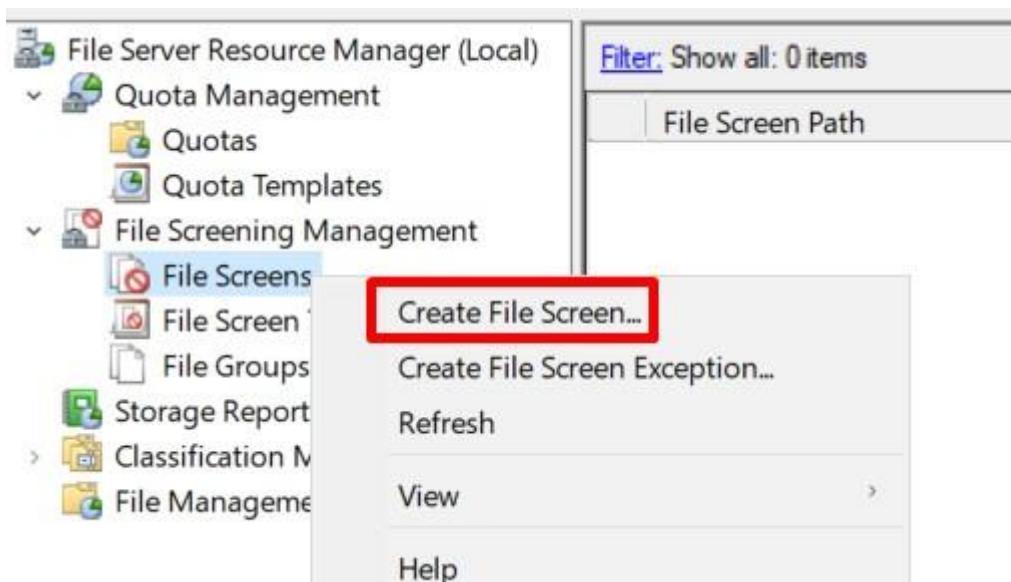


- אנו בוחרים את תקיות הבית של המשתמשים ומגבילים אותה ל-5 GB בשיטת HARD



- שיתופים ומיפויים – שירות קבצים -

- מצב HARD מונע מהמשתמשים לחרוג מהמגבלה שנקבעה על ידי חסימת ייצירת קבצים חדשים. מצב SOFT מאפשר לך לחרוג באופן זמני מ-QUOTA, אך מספק הודעה למנהל מערכת כאשר חריגת מהמגבלה
- עכשו אני אוצר נעלית קבצים AVI



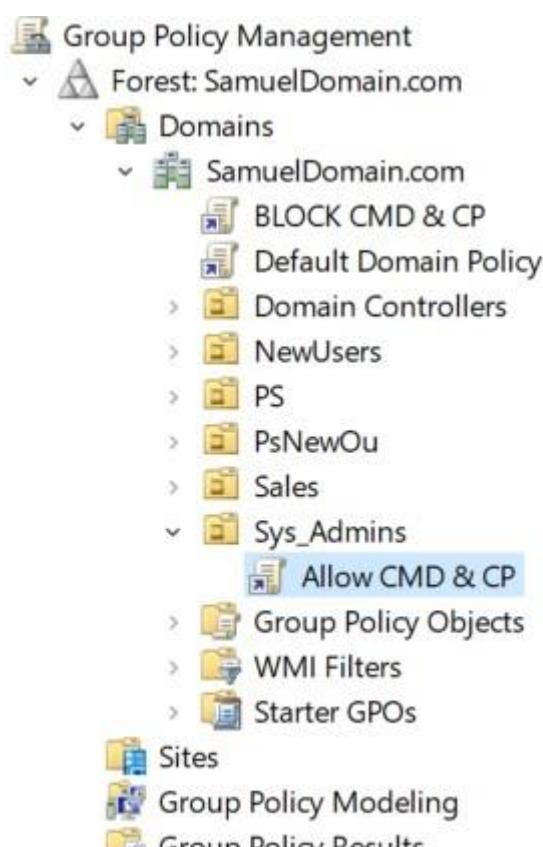
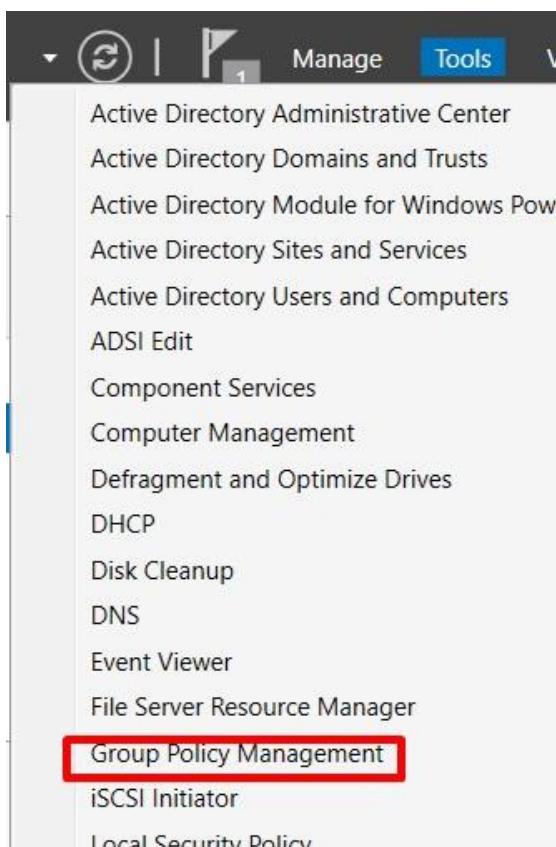
- הקשהת התchanות -

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

מניעת גישה של משתמשים שאינם עובדי Sys Admins
Control Panel

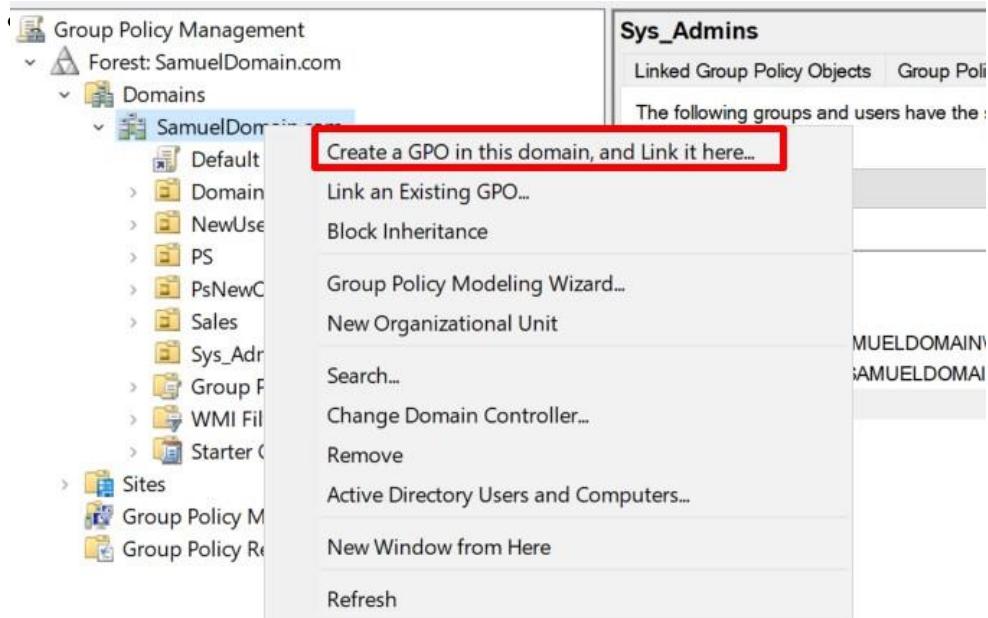
מניעת גישה של משתמשים שאינם עובדי Sys Admins
 Disk-on-key ב-

- כעת נאסר על גישה למשתמשים רגילים ל Control panel וCMD
- כעת נאסר על גישה לכל משתמשים ל Disk-on-key
- עם GPO ניהול מערכת יכול להגדיר סיסמאות למשתמשים, למנוע גישה לאתרים מסוימים, או להתאים אישית את שולחן העבודה של המחשב עם תוכניות וKİצורי דרכ רצויים. גם להגבר את האבטחה של החברה
- ראשית בווא נלך לשירות GPO



- הקשה התחנות -

• אנחנו יוצרים חדשה Policy



• אנו מוגבלים את השימוש בשורת CMD ובהגדרות מערכת הפעלה

The screenshot displays two Group Policy Objects (GPOs) in the 'Group Policy Management' console:

- BLOCK CMD & CP**: This GPO has a 'Control Panel' policy definition selected. The 'Edit policy setting' dialog for 'Prohibit access to Control Panel and PC settings' shows the 'Enabled' radio button selected. The 'Setting' pane lists various registry keys under 'Prohibit access to Control Panel and PC settings'.
- BLOCK CMD & CP [SAMDC1.SAMUELDOMAIN.COM] Policy**: This GPO has a 'System' policy definition selected. The 'Edit policy setting' dialog for 'Prevent access to the command prompt' shows the 'Enabled' radio button selected. The 'Setting' pane lists registry keys related to command prompt restrictions.

In both dialogs, the 'Enabled' radio button is highlighted with a red box. The 'Not Configured' and 'Disabled' options are also shown.

- הקשהת התchanות -

- אנו גם מאפשרים למנהל רשות פונקציות אלו

Prevent access to the command prompt

Prevent access to the command prompt

Not Configured Comment:
 Enabled
 Disabled →
Supported on: At least Wind

Prohibit access to Control Panel and PC setting

Prohibit access to Control Panel and PC setting

Not Configured Comment:
 Enabled
 Disabled →
Supported on: At least W

- > PS
- > PsNewOu
- > Sales
- ▼ Sys_Admins
 - Allow CMD & CP**
 - > Group Policy Objects
 - > WMI Filters
 - > Starter GPOs

- אנו יוצרים Policy חדשה ואוסרים על כל המחשבים להשתמש בכוננים חיצוניים

All Removable Storage classes: Deny all access

All Removable Storage classes: Deny all access

Not Configured Comment:
 Enabled →
 Disabled
Supported on: At least Wind

Group Policy Management

Forest: SamuelDomain.com

Domains

SamuelDomain.com

BLOCK CMD & CP

BLOCK Disk On Key

Default Domain Policy

Domain Controllers

NewUsers

PS

PsNewOu

Sales

Sys_Admins

Allow CMD & CP

Group Policy Objects

WMI Filters

Starter GPOs

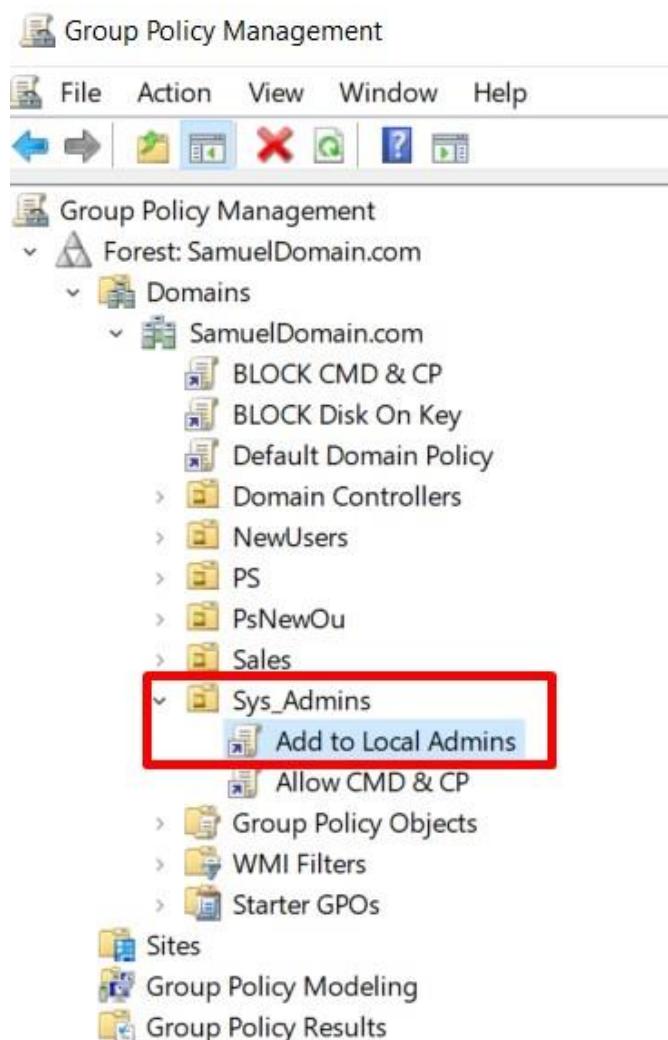
Sites

Group Policy Modeling

- הקשחת התchanות -

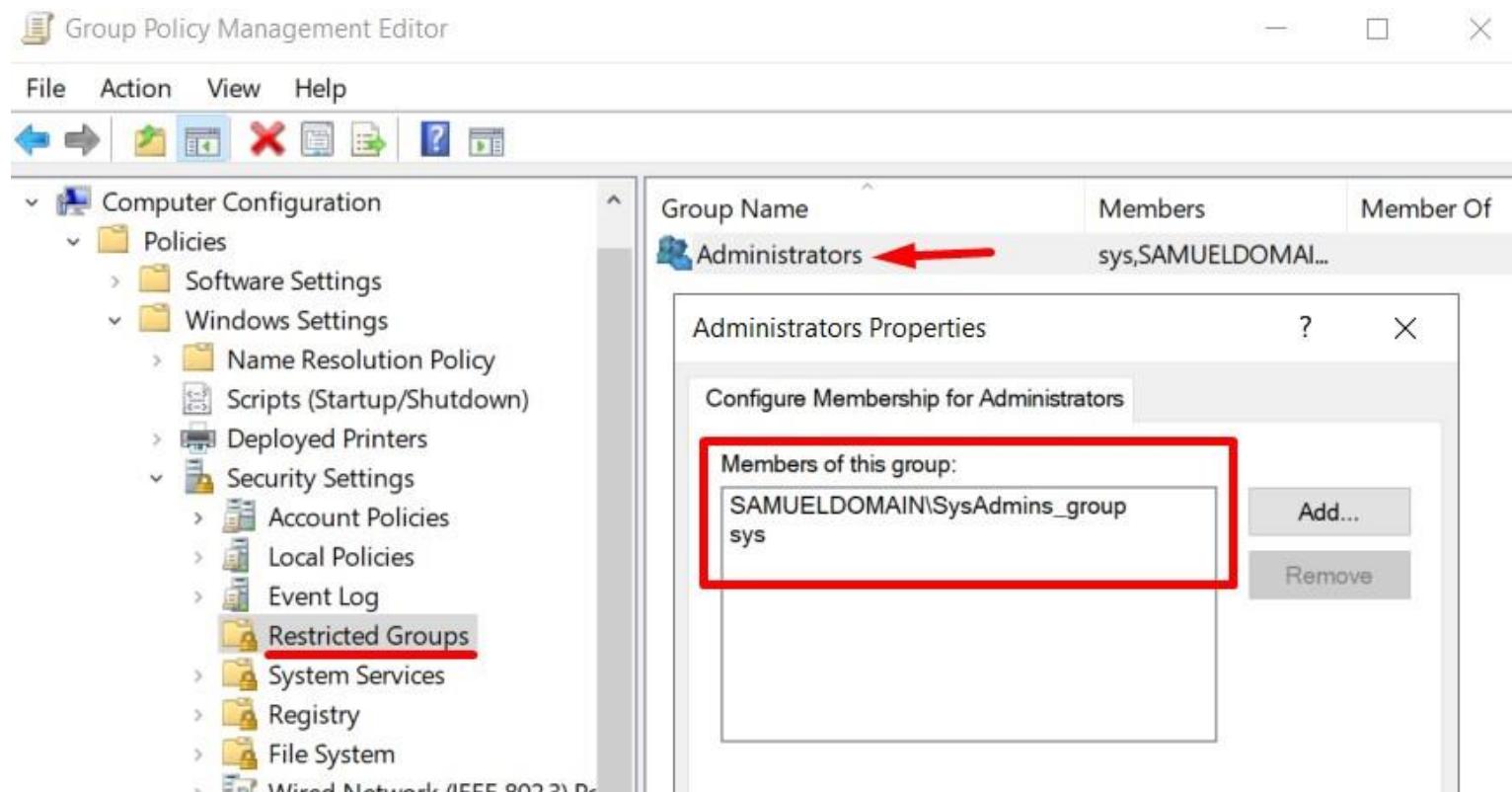
צור Policy שמאפשר למחלקת Sys Admins להיות בקבוצת המיקומית של כל מחשבי הארגון (זהירות!)

- כתעת אוצר POLICY שתוסיף את Sys Admins שלנו
למנהלים המקומיים של כל קבוצת המיצבים
- מנהלי מערכת : הם אחראים על ניהול, הגדרה ותחזוקה של רשות המחשבים בארגון. זה כולל ניהול שירותים, הגדרת ציוד רשת, הבטחת אבטחת הרשות
- מנהלי מערכת מקומיים : הם בדרך כלל אחראים לניהול מחשבים או תחנות עבודה בודדות. זה כולל התקנת תוכנה, הגדרת מערכת הפעלה
- לשם כך, עליינו ליצור POLICY חדשה, לאחר מכן להוסיף את כל המנהלים ורק לאחר מכן את מנהלי המערכת, כדי שום דבר לא יתאפשר ולא נאבד בטיעות את כל הזכויות



- הקשחת התchenות -

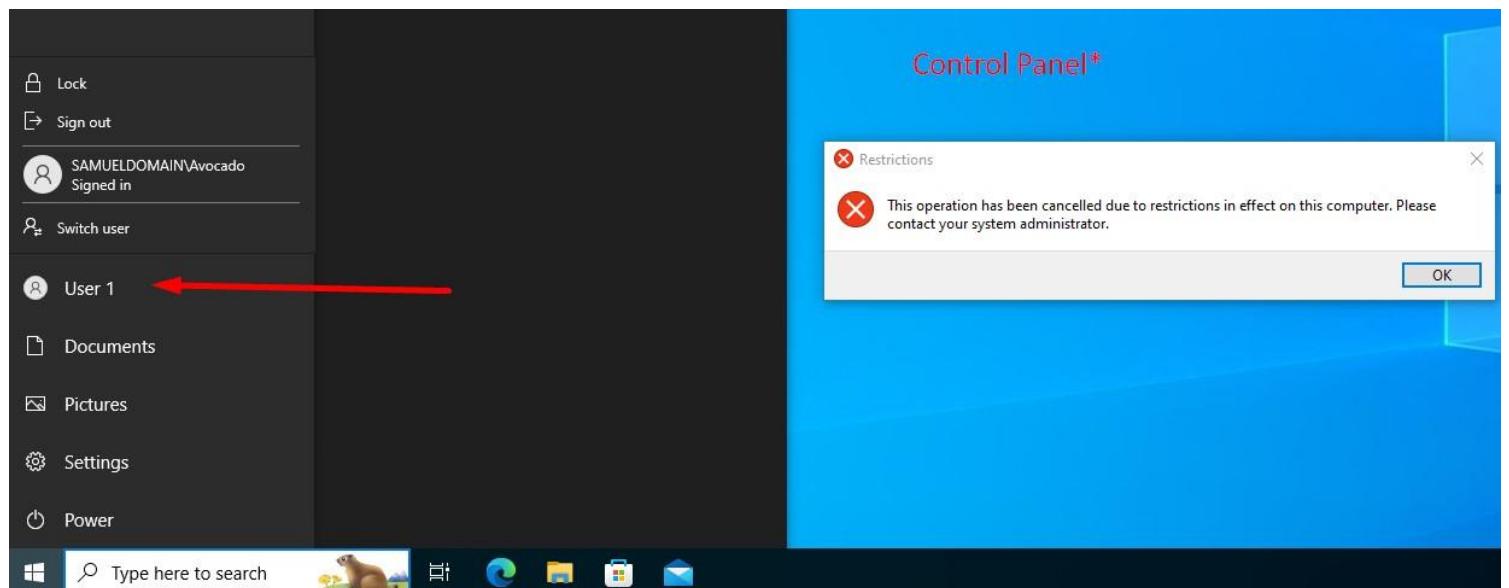
- אנחנו מוסיפים מנהלים ב Restricted Groups



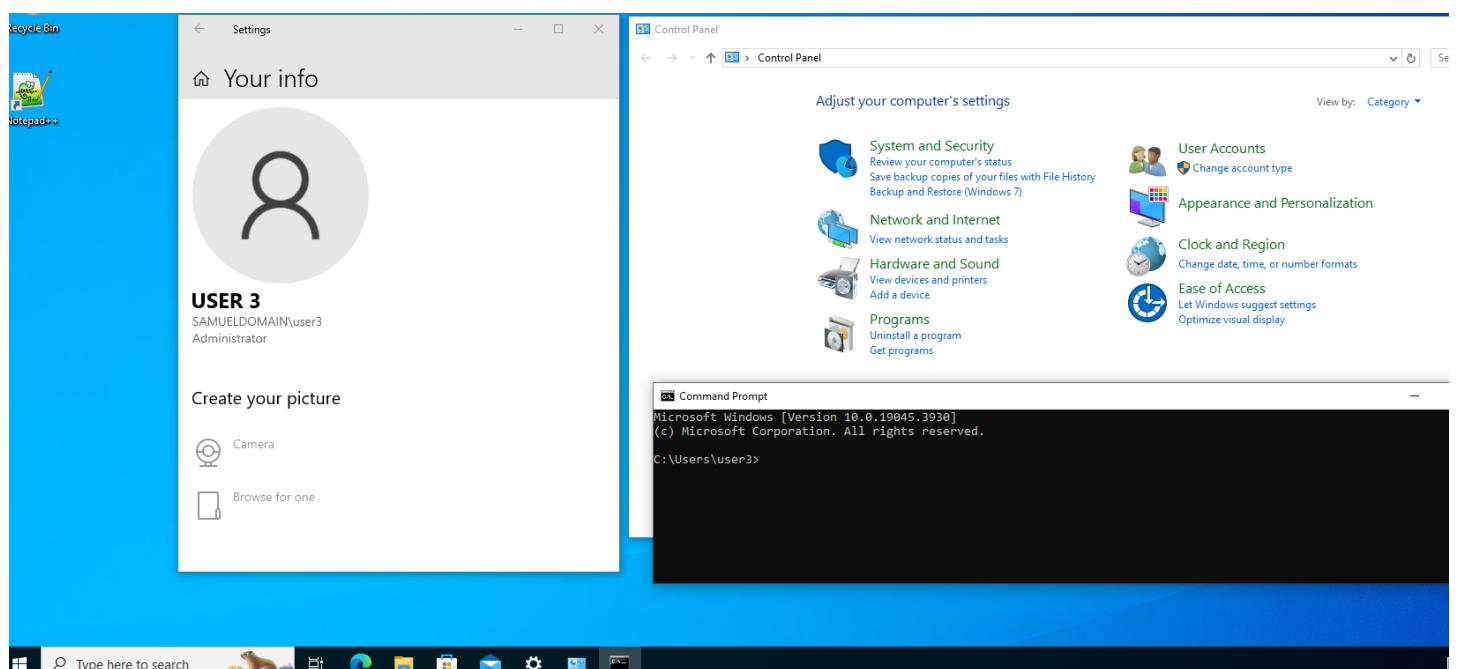
- הקשחת התchanות -

- איך שאפשר לראות שהمدיניות עובדות

Other Users:



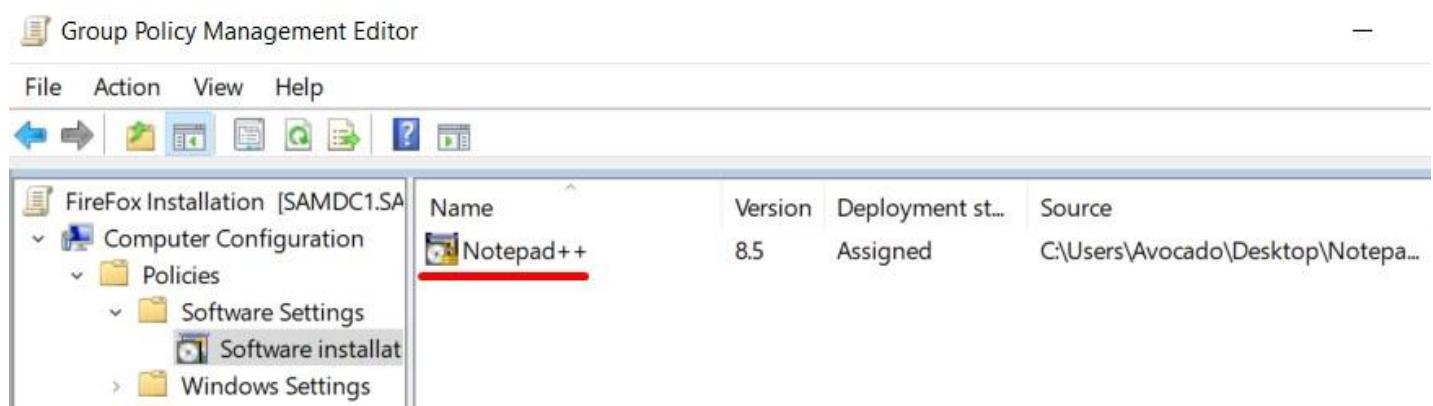
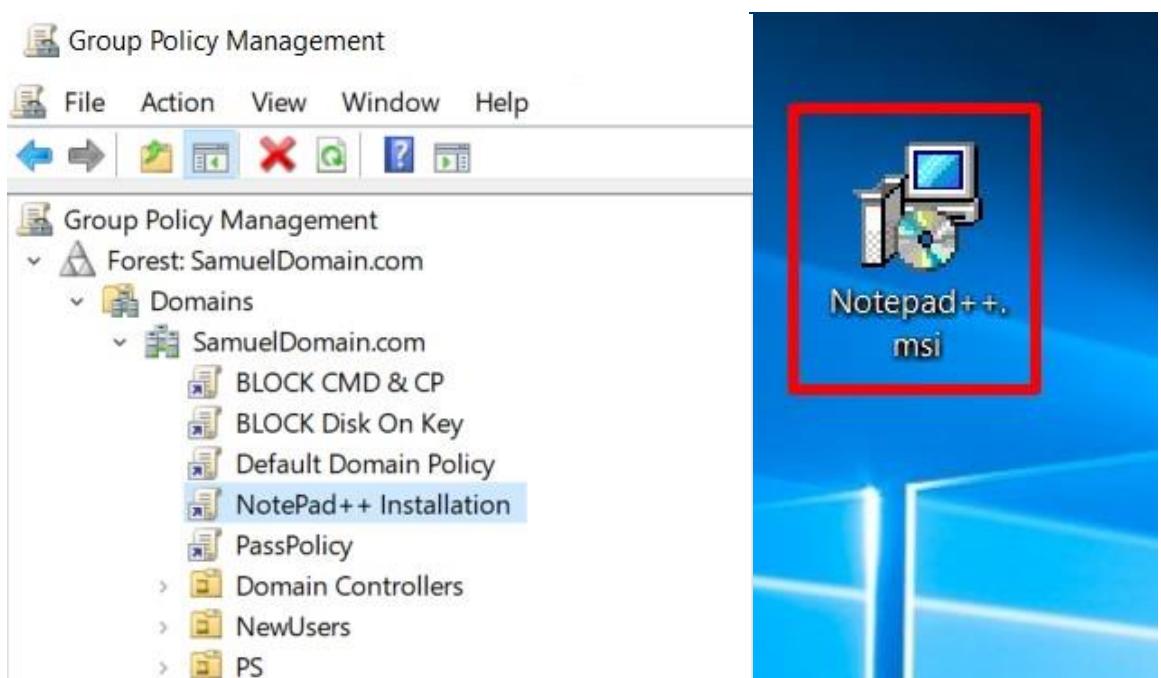
Sys_Admin:



- הקשהת התchanות -

הגדר עיי GPO התקינה של תוכנה עיי מחשבי הארגון ללא מעורבות אדם.

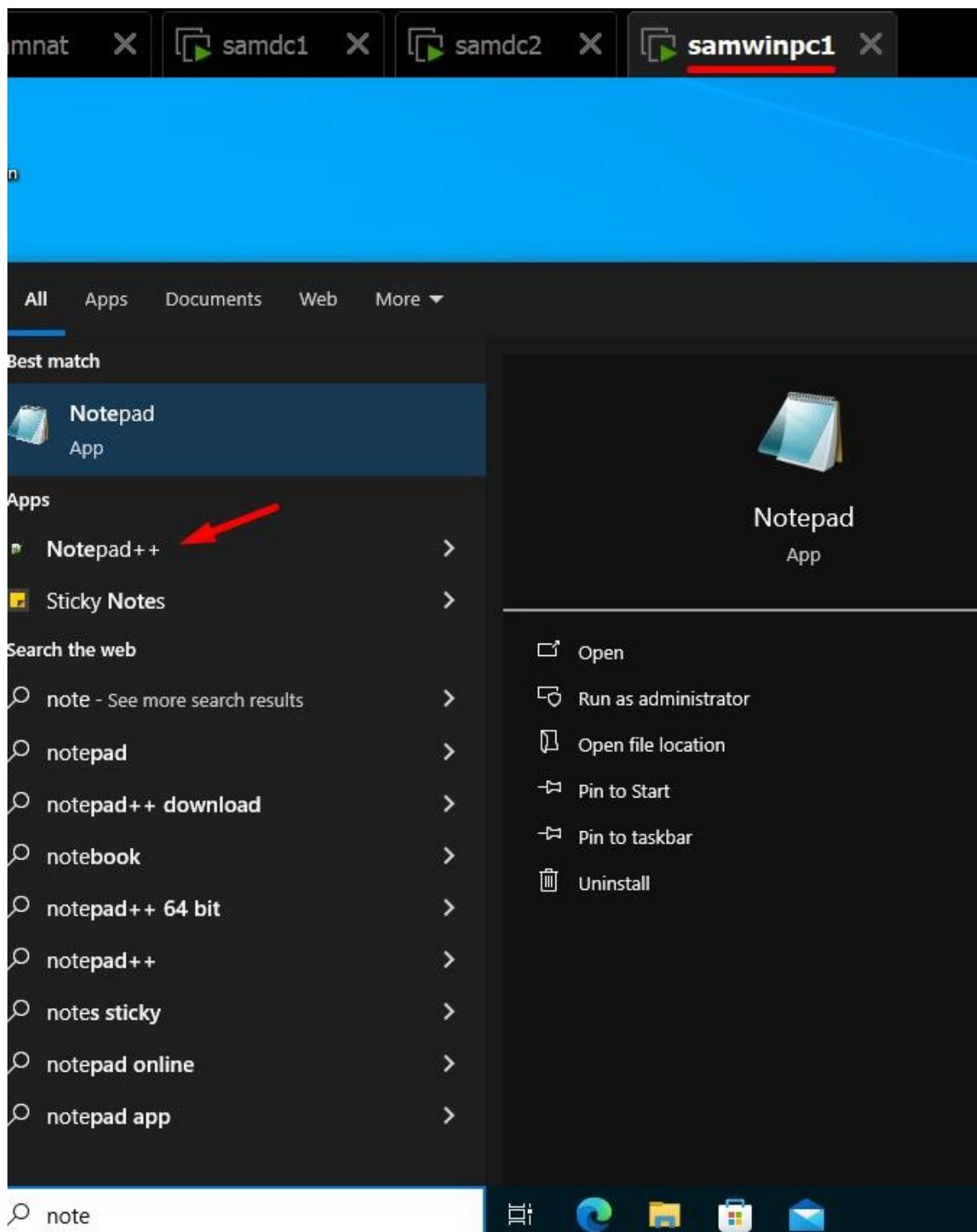
- בעת נוכל ליצור POLICY שתאפשר התקנת התוכנה על כל המחשבים בשיתוף רק אני ו-GPO
 - נתקין את Notepad++
 - אנו מורידים תחילה את התוכנית ויוצרים POLICY חדשה



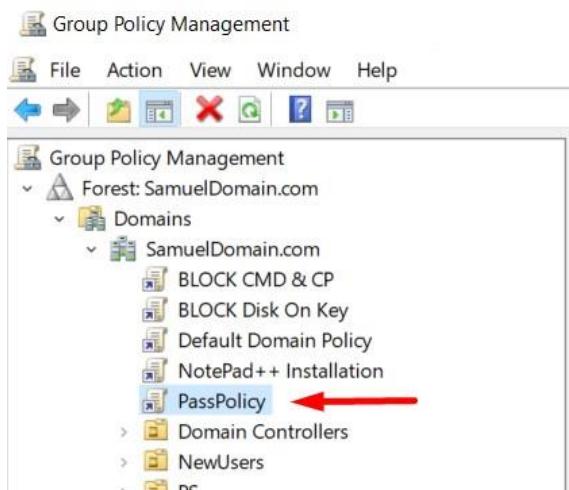
Name	Version	Deployment st...	Source
Notepad++	8.5	Assigned	C:\Users\Avocado\Desktop\Notepa...

- הקשחת התחנות -

- ובודקים שזה עובד על 1 PC



- מדיניות סיסמאות בארגון -



מדיניות סיסמאות בארגון:

צור מדיניות סיסמא לפי התנאים הבאים:

▪ אורך סיסמא 8 תווים

▪ מחייב שילוב של מספר סוני תווים

▪ לא ניתן להשתמש ב4 סיסמאות אחרונות

▪ תוקף סיסמא 75 ימים.

- מדיניות הסיסמאות של ארגון חשובה מאוד להבטחת אבטחה ומניעת גישה בלתי מורשית; נדרש לעקוב אחר כלליים מסוימים ביצירת סיסמה, מכיוון שיש ספריות שלמות לדוגמיה, שיכולים לנחש אותו

• **נשתמש גסO**

The screenshot shows the 'Group Policy Management Editor'. On the left, the navigation pane shows the 'Computer Configuration / Policies / Account Policies / Password Policy' path, with 'Password Policy' highlighted and a red arrow pointing to it. On the right, a table displays the policy settings:

Policy	Policy Setting
Enforce password history	8 passwords remembered
Maximum password age	75 days
Minimum password age	30 days
Minimum password length	8 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Not Defined

-BONUS -

צור מדיניות סיסמה מקילה / שונה לעובדי מחלקה Sales בלבך

- אני אצור מדיניות נפרדת לקבוצת המכירות, גודל סיסמה מקסימלי 10, תוקף סיסמה מקסימלי 100 ימים

The screenshot shows the Windows Group Policy Management console. On the left, a tree view shows 'SalesPassPolicy' under 'Sales'. A red arrow points from the text above to this node. The main pane displays a 'Policy' table with the following data:

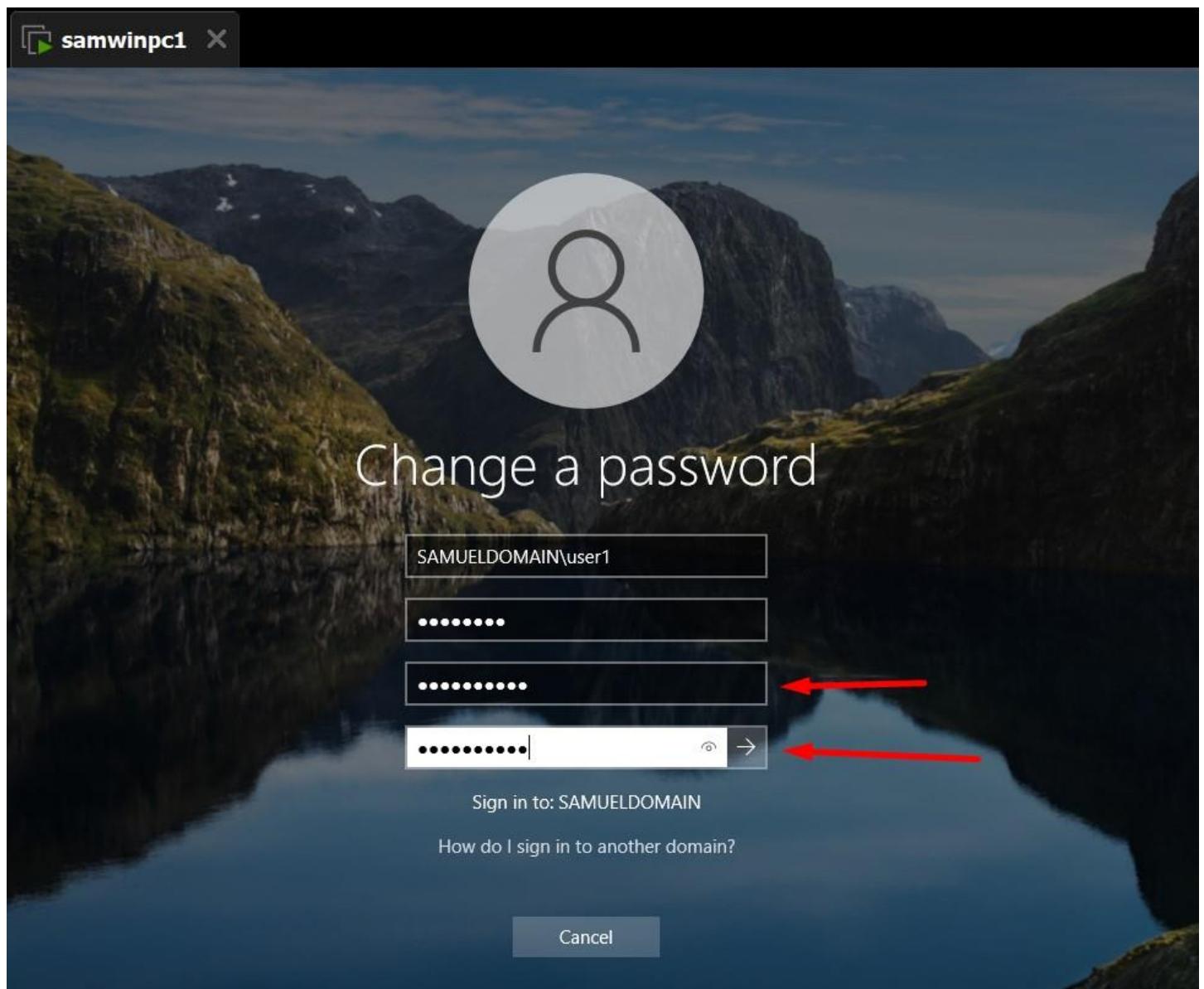
Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	100 days
Minimum password age	30 days
Minimum password length	10 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Not Defined

- אני מבטל את הגדרות המדיניות שקבענו קודם לכן בגלל
שאני לא יכול להיכנס להגדרות תחת משתמש מקבוצת
המכירות ולשנות את הסיסמה כדי להציג דוגמה 😊

The screenshot shows the Windows Group Policy Management console. A red arrow points from the text above to a context menu for a policy object named 'BLOCK CMD & C'. The menu options include 'Edit...', 'Enforced', 'Link Enabled' (which is highlighted with a red underline), 'Save Report...', 'View', and 'Run Windows from Here'. To the right, a 'BLOCK CM' properties window is open with tabs for 'Scope' and 'De'. Below it, a 'Run' dialog box is shown with the command 'gpupdate' entered in the 'Open:' field.

-BONUS -

- כעת, בהקשר למדייניות החדשה, אנו בוחרים את הסיסמה המתאימה!



- עבודה חקר -

בחינת אבטחת מידע ומדיניות פרטיות

במהלך המקרה למדנו הרבה נושאים לגבי Microsoft Active Directory והכליים שלו לניהול הארגון שבהם קיימים הרבה פרוטוקולים כמו Kerberos, NTFS, RDP, ACL, GPO ועוד הרבה דברים מעניינים. שונים מחשבונות, מדיניות קבוצתית ו עוד הרבה דברים מעניינים. היום במאמר זה ניגע בהם

- מדיניות סיסמה

מדיניות סיסמות ב Active Directory היא היבט של אבטחה שמטרתו להגן על מידע רגיש ומשאים ארגוניים. חשוב להבין את היבטים המרכזיים הבאים של מדיניות זו:

היבטים אלה של סיסמות, עליהם נדון בהמשך, מספקים רמת אבטחה מוגברת וסייעים בהגנה על נכסים ארגוניים מפני איומים שונים.

מורכבות סיסמות: הגדרת דרישות לשימוש בסוגים שונים של תווים (אותיות גדולות ואותיות קטנות, מספרים, סמלים) מה שהופך את הסיסמות לעמידות יותר בפני התקפות של brute force לדוגמה.

שינויים תקופתיים של סיסמה: דרישה לשינוי סיסמה תקופתיים עוזרת להפחית את הסיכון לדליפות סיסמה ומשפרת את אבטחת החשבון.

ההיסטוריה של סיסמות: הגבלת השימוש החוזר בסיסמות ישנות מסייעת במניעת נזודות תורפה הנגרמות בתוצאה משינוי תכוף של סיסמות לסיסמות דומות או חלשות.

נעילת חשבון: נעילת חשבון אוטומטית לאחר ניסיונות הת לחברות כושלים רבים מגנה מפני התקפות brute force.

כל אלו הם היבטים חשובים ליצור סיסמות שהשתמשנו בהן בפרויקט הזה, שיכלות לספק הגנה לprofil או חשבון אבל לא רק ב-Windows-Active Directory, אלא גם במערכות הפעלה או ספריות אחרות של חברות אחרות כמו OpenLDAP, FreeIPA וכו'

- מדיניות חיבור מרוחק

מדיניות גישה מרוחק ב-**Active Directory** היא קבוצה של כלליים והגדרות שנועדו להבטיח גישה מרוחק מאובטחת ויעילה למשאים ארגוניים כגון שרתים ומחשבים של החברה. בפרויקט זה נגענו בגישה מרוחק וניסינו להיכנס למחשבים מהרשות הפנימית ומהרשות החיצונית באמצעות פרוטוקול RDP.

(**RDP** – Remote Desktop Protocol) הוא פרוטוקול שפותח על ידי מיקרוסופט, בעזרתו, משתמשים יכולים לגשת למחשבים או שרתים מרוחקים.

אחד התכונות של RDP היא היכולת לשדר ממשק משתמש גרפי על גבי רשת. בנוסף, RDP מספקת הצפנה נתונים כדי להגן על סודיות המידע המועבר ברשות, והיא נתמכת גם בMagnitude מערכות הפעלה, כולל Windows, macOS ו-Linux, מה שמספק צדדיות וGamification בשימוש.

ישנם גם פרוטוקולי גישה מרוחק אחרים כגון TELNET, SSH וכן הלאה היבטים חשובים של המדיניות הם אימות והרשאה של משתמשים, הצפנה תעבורת להגנה על נתונים ובקרה גישה למעקב אחר פעילות המשתמש. מדיניות גישה מרוחק מוגדרת כהלכה מגנה על משאבי החברה מפני גישה בלתי מורשית ולאבטחת מידע

- הרשות לקבצים ותיקיות ברשות

בפרויקט זה, נגענו לעיתים קרובות בהרחבות הממלאות TPKID עצום בארגון Active Directory. מוביל להגדר נכוון את הרשות לקבצים והתיקיות, עלולות להיות אבטחה חמורות. הרשות מוגדרות בצורה שגوية עלולות להוביל לגישה בלתי מורשית של עובדים נתונים רגילים, דיליפות מידע או מחיקה בשוגג של קבצים חשובים. בנוסף, הרשות מוגדרות היטב מאפשרות לך ליעיל את תהליך העבודה עם הנתונים

גישה לקבצים ותיקיות. Active Directory משתמש בפרוטוקולי NTFS ו-ACL- כדי לשלוט

Windows NTFS היא מערכת קבצים סטנדרטית המשמשת במערכות הפעלה Windows המאפשרת להקצות רמות שונות של גישה לקבצים ולתיקיות למשתמשים ולקבוצות משתמשים. ACL היא רשימה של כללי הקובעים לאילו משתמשים או קבוצות יש גישה לקבצים או תיקיות מסוימים, ואילו פעולות הם יכולים לבצע בקבצים או תיקיות אלו.

Active Directory משתמש גם ב-LDAP לניהול הרשאות. הוא מספק דרך סטנדרטית לגשת לספריות כגון Active Directory, המאפשרת למנהל ממערכת ניהול הרשות עבר קבצים ותיקיות גם באמצעות ניהול מרכזי של Active Directory.

אתן פקודות בהן השתמשנו ליצור משתמשים חדשים ויחידות ארגוניות, למשל DSADD, משתמשות בעקרונות LDAP כדי ליצור אינטראקציה עם Active Directory וליצור אובייקטים חדשים בהתאם לפרמטרים שצינו. לפיכך, DSADD ו-LDAP קשורים קשר הדוק בהקשר של ניהול אובייקטים ב-Active Directory.

- מדיניות קבוצתית או GPO

עם GPOs מנהלי מערכת יכולים להגדיר הגדרות שונות, כגון מדיניות אבטחה, הגדרות רשות, ניהול תוכניות ושירותים והתאמות אישיות של ממש משתמש. זה עוזר להבטיח עמידה בתקני בטיחות וקלות שימוש.

מדיניות קבוצתית חלה על מיכלים ספציפיים של Active Directory, כגון דומיאנים, ייחדות ארגוניות או קבוצות, ומאפשרת לכך למנהל הגדרות על סמך מבנה הארגון שלו. במקרה זה, ל-GPO יש עדיפות, המאפשרת לכך לפטור התנגשויות בין הגדרות שונות.

באופן זה, מדיניות קבוצתית ב-Active Directory מספקת ניהול מרכזי וגייס של תכורות אבטחה ברחבי רשות Windows, מה שմ蹁ר את האבטחה והיעילות של הארגון כולו.