

מטלת גמר – Microsoft Server

שקלד אוריאל ברמי – 213164379

CSPP86

מדריך – בנימין כהן

תאריך ההגשה: 01/02/2024



לפני שאתחל ביצוע המלאכה, ארצה לקיים סדר, איך לעבוד נכון, אקיים כל מטריה כסוג של "פרק" בעבודה זו.

הכנת מעבדה:

1. התקנת מכונות ורטואליות חדשות

הגדרת דומיין קונטROLר:

2. הפיכת DC1 לדומיין קונטROLר ויאנאו סרבר + שיום דומיין + שימוש מחשבים

3. צירוף DC2 לדומיין והפיכתו לserver rid master

צירוף מחשבים לחומיין:

4. צירוף וינדוז 10 וסרבר 1 לדומיין ושינוי שם שליהם לפי תנאים

המשר הגדרת דומיין קונטROLר:

5. יצירת שבי OU

6. יצירת משתמשים בתוך OU

7. יצירת קבועות והכנסת משתמשים אליהם בתוך OU

8. שימוש בפקודות לטובת יצירת יזרים ועוד...

פרופיל משתמש:

9. יצירת פרופיל נודד למשתמש שיירנו קודם

10. פתיחת אופציה למנהל הרשות לכיסיה לתיקית הפרופיל בשרת.

פתיחה אופציה לגישה ברשות האינטרנט והגדרת סרבר 1 כתוב שלם:

11. הגדרת סרבר 1 כתוב

:DHCP

12. התקנה כוללת של DHCP

הגדרת DNS:

13. הגדרת כל המחשבים לשימוש בדיאנאו של DC1

14. הפניות

15. הגדרת זונים

16. יצירת CNAME

17. יצירת ובדיקה של ראנד רובין

ניהול השירות מרוחק:

18. מתן האופציה `sys_admins` להגדרת שירותי מוינטוס 10.

19. מתן RDP לשרת DC1 לעזרך מחוץ לארגון.

הקשחת התחנות:

20. שימוש כללי ב-Group Policy

מדיניות סיסמה:

21. יצירת מדיניות סיסמה לפי תנאים ספציפיים

בונוס:

22. יצירת מדיניות סיסמה מוקלה

שיתופים ומיפויים:

23. הגדרת DC2 כשרת קבצים ומיפויים

עובדת חקר/מאמרה:

24. מאמר - מדיניות הסיסמה: איך מיקרוסופט ואסוס מגינות על המשתמשים שלהם?

תוכן עניינים

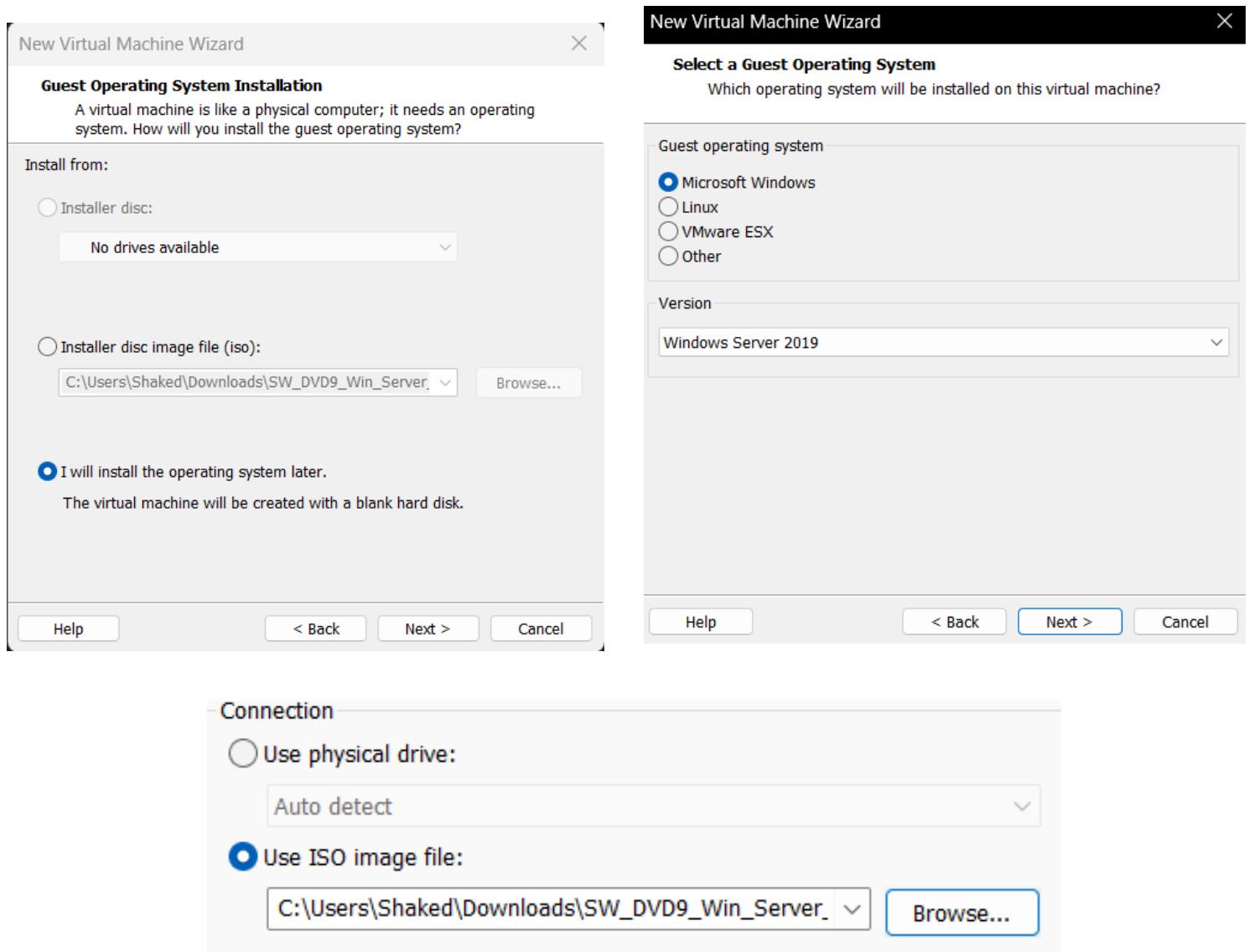
הכנת המעבדה	5.....
הגדרת VMWare Tools	11.....
הגדרת Domain Controller	14.....
הפיכת DC1 לדומיין קונטרולר DNS ו-SMB סרבר	14.....
צירוף DC2 לדומיין	21.....
הגדרת DC2 כ-rid master	22.....
יצירת שני יחידות ארגוניות	23.....
יצירת משתמשים חדשים, תחת היחידות הארגוניות	24.....
יצירת 2 קבוצות, והכנסת משתמשים אליהם	25.....
יצירת 2 חשבונות משתמש אחרים על ידי שימוש בפקודות DSADD	27.....
יצירת 2 קבוצות אחרות על ידי שימוש בפקודות DSADD	28.....
הכנסת חשבונות לקבוצות, רק על ידי פקודות	29.....
יצירת עשרה חשבונות על ידי סקריפט, שמשתמש בפקודת DSADD	30.....
יצירת יחידה ארגונית + חשבון משתמש חדש + קבוצה חדשה רק על ידי פקודות	31.....
יצירת עשרה חשבונות חדשים על ידי סקריפט מבוסס PowerShell	32.....
בדיקות שרת ה-DC, שהכל תקין, ושלל השינויים מסתנכרנים.	33.....
צירוף המחשבים לדומיין	34.....
פרופיל משתמש	35.....
יצירת פרופיל משתמש נודד לחשבון שיצרנו בתרגילים הקודמים	35.....
בדיקה שהפרופיל אכן נודד	37.....
שינויי ההגדרות, בכדי לתת לאדמינים, לגשת לתיקיית פרופיל	38.....
בדיקה שוב שהפרופיל אכן תקין ונודד	39.....
שינויי פרופיל, לפרופיל מנדרורי	41.....
הגדרת ניתוב - PAT	42.....
הגדרת סרבר 1 להיות נתב, ואפשר PAT	42.....
הגדרת DHCP Server	51.....
מתן כתובת IP קבועה ל-DC1 והתקנת DHCP SERVER עליו	51.....
הגדרת DHCP SCOPE	54.....
הגדרת החראות בטוחה DHCP	55.....
הגדרת תוקף לכל כתובת בטוחה	56.....
הגדרת רואוטר, בהגדרות טווח של DHCP	57.....
בדיקה קישוריות	59.....
יצירת Failover Cluster	62.....
הגדרת DNS Server	64.....
וידעו שלל המחשבים מוגדרים להשתמש באותו של DC1	64.....

65.....	הגדרת מעבר לשרת DNS חיצוני
66.....	חסימת אתר Facebook בארגון
67.....	ויזוא שוינדוס 10 קלינט שלו, יכול לתרגם את הכתובת של גוגל, בעזרת NSLOOKUP
68.....	הגדרת Stub Zone
70.....	יצירת ZONE מסווג Primary, ולאחר מכן, ליצור Zone Secondary
73.....	יצירת CNAME לשרת DC2
75.....	יצירה ובדיקה של ראנד רובין
82.....	ניהול השירות מרוחק
82.....	אפשר למחוקת Sys_Admns לנהל את השירותים מה Windows Client
87.....	ביצוע השטלות עם משתמש Sys Admins
91.....	מתן האופציה לעובד מחוץ לארגון להתחבר עם פורט 5588
93.....	הקשחת התחנות
93.....	חסימה של Control Panel למי שלא Sys Admins
97.....	חסימה של שימוש CMD למי שלא Sys Admins נמצא בתוך
99.....	חסימה של דיסק אונ-לי
100.....	יצירת תנאי, שיאפשר למשתמש Sys Admin, להיות minin, בכל מחשבי הארגון
103.....	התקנת תוכנה על גבי כל מחשבי הארגון ללא מעורבות אדם
106.....	מדיניות סיסמה
107.....	מטלת בונו
109.....	שיתופים ומיפויים
109.....	הגדרת DC2 כשרת קבצים
110.....	הגדרת Home Folder לחמשה משתמשים
112.....	יצירת תיקייה משותפת ב2cp
113.....	מיפוי כונן רשות
115.....	יצירת תיקייה משותפת נוספת בשם סקריפט
116.....	יצירת מסכה, והגבלה שמיירת קבצי AVI
121.....	מאמר בנווע למединיות סיסמה – שקד אוריאל ברמי - איך מיקרוסופט ואסוס מגינות על המשמשים שלהם

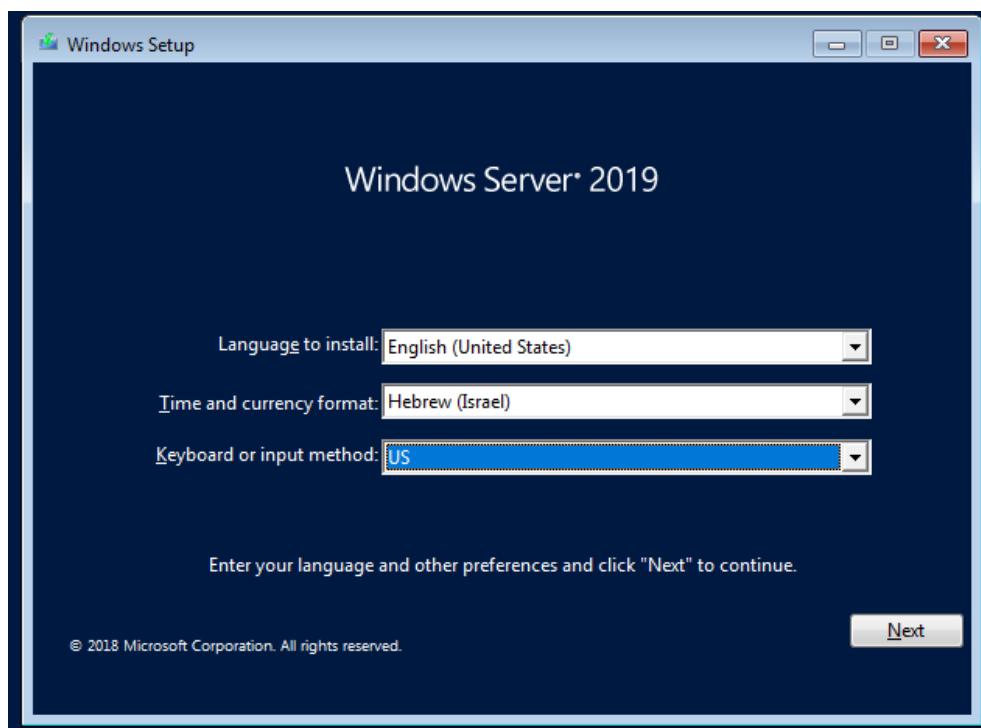
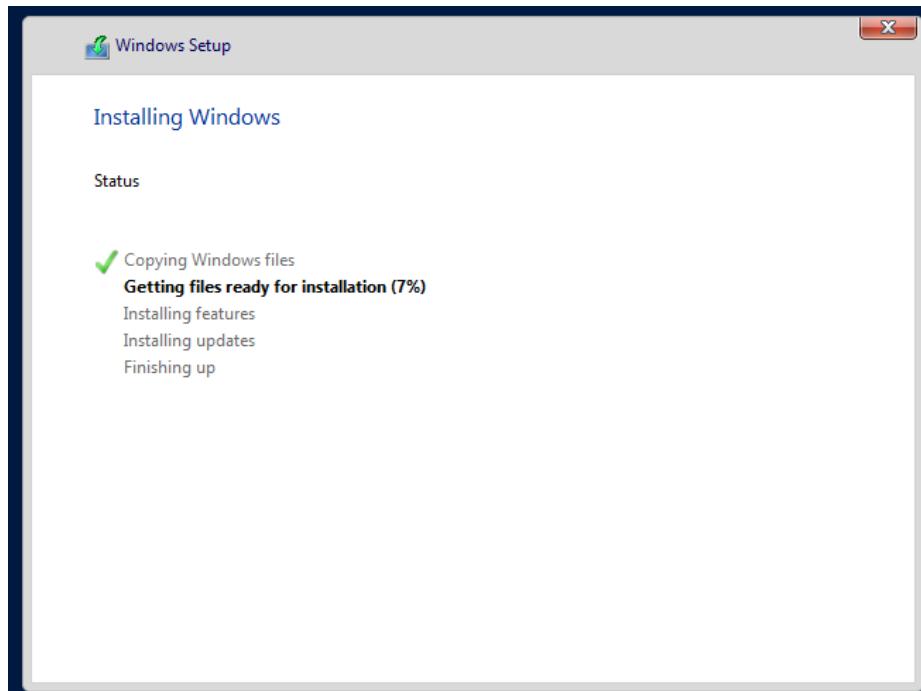
הכנות המבוקשת

יש להתקין מכונות וירטואליות חדשות לשלוטין ולא להשתמש במכונות שהוגדרו במהלך המקצועה.

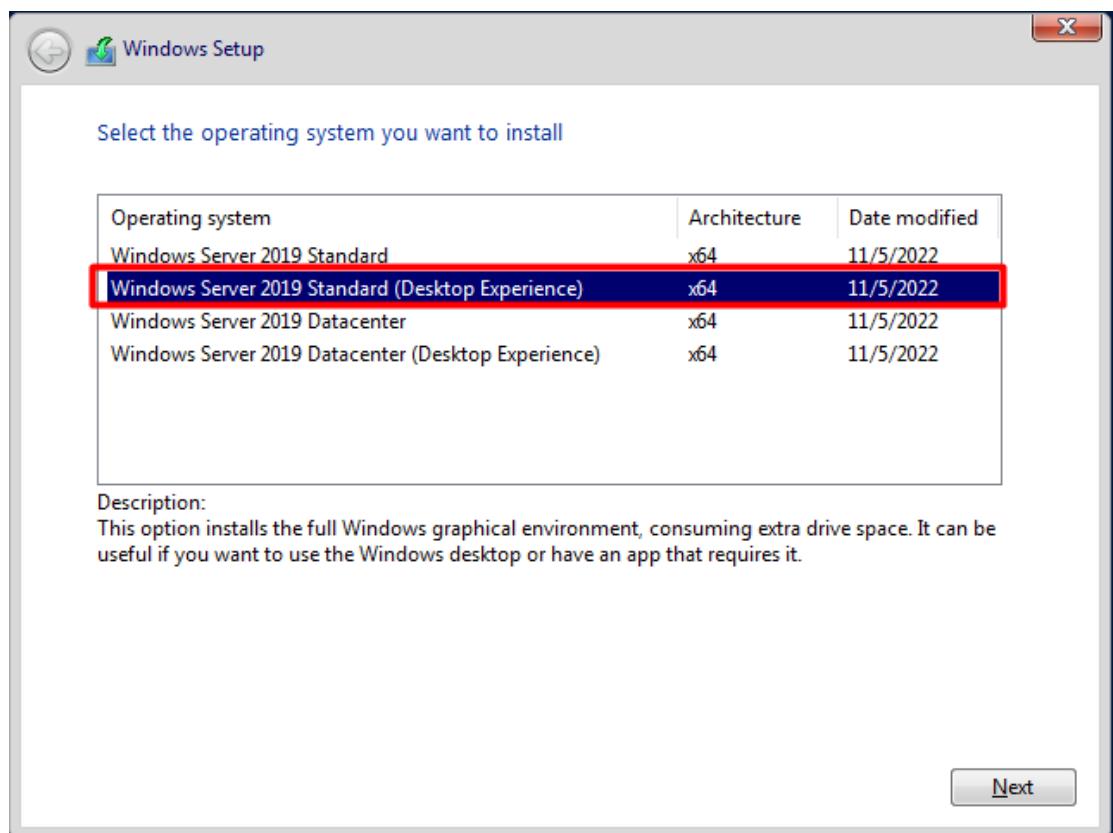
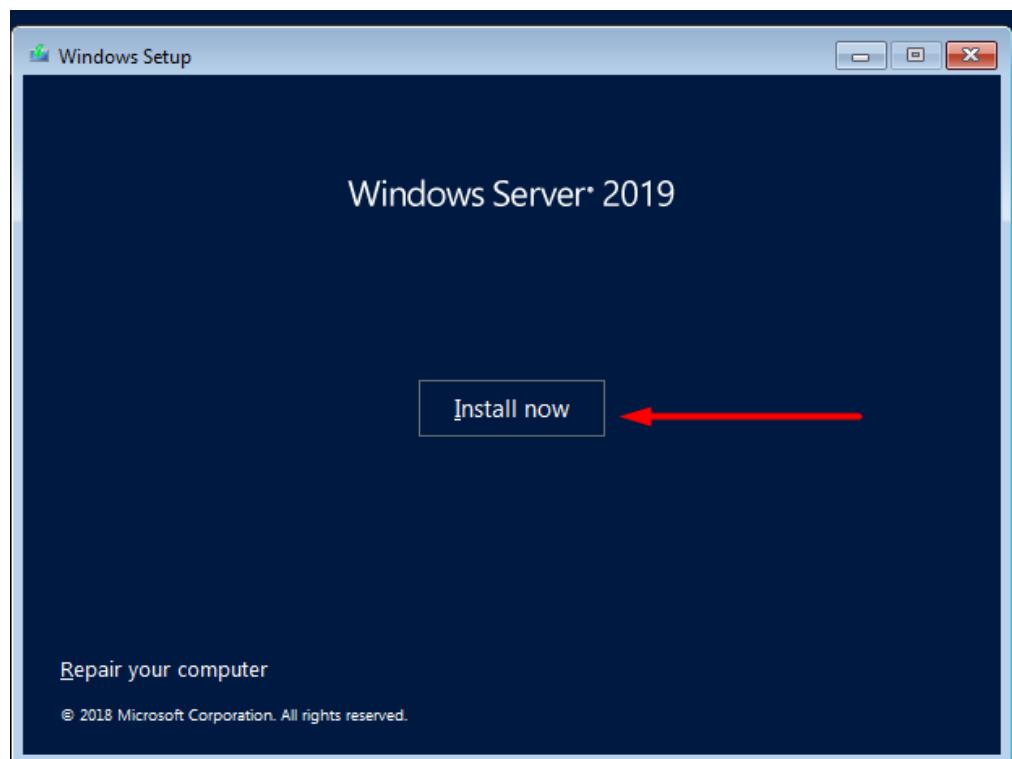
נתחיל בהתקנת DC1, לתוכה Windows Server 2019, המיעודה במיוחד לשימוש בשירותים.



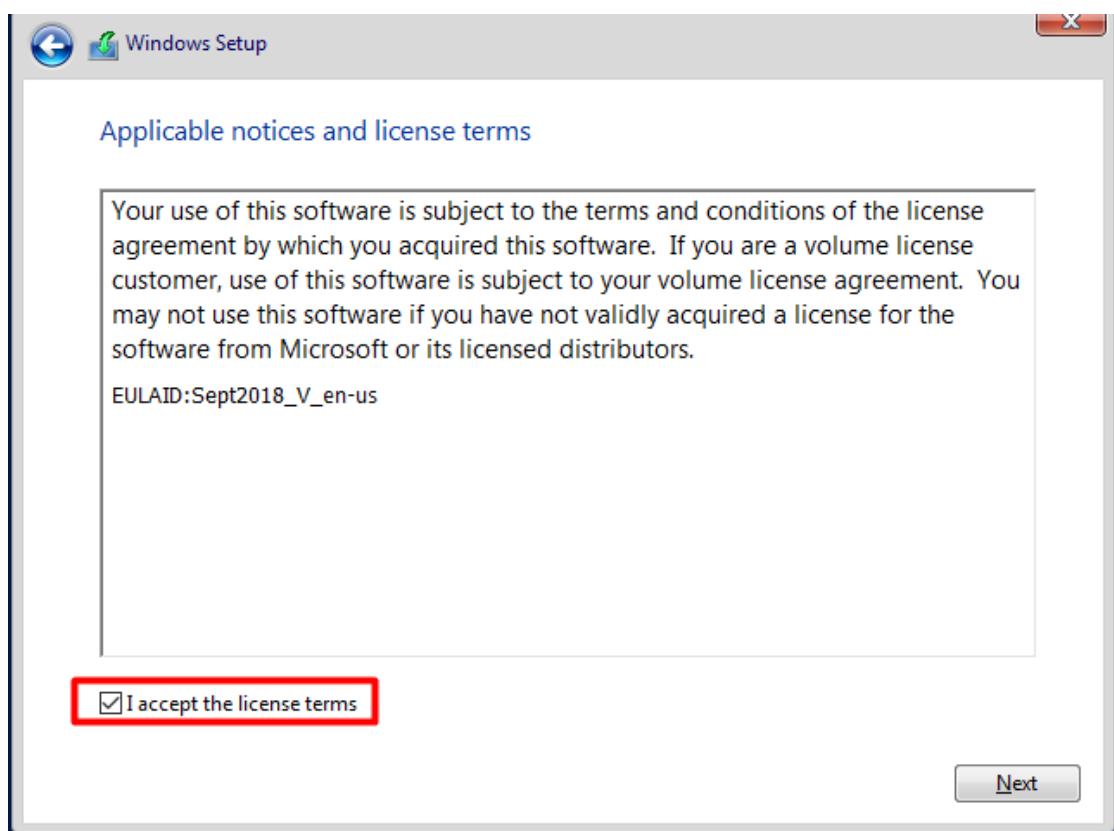
כעת נעשה את התקינה של המערכת הפעלה עצמה



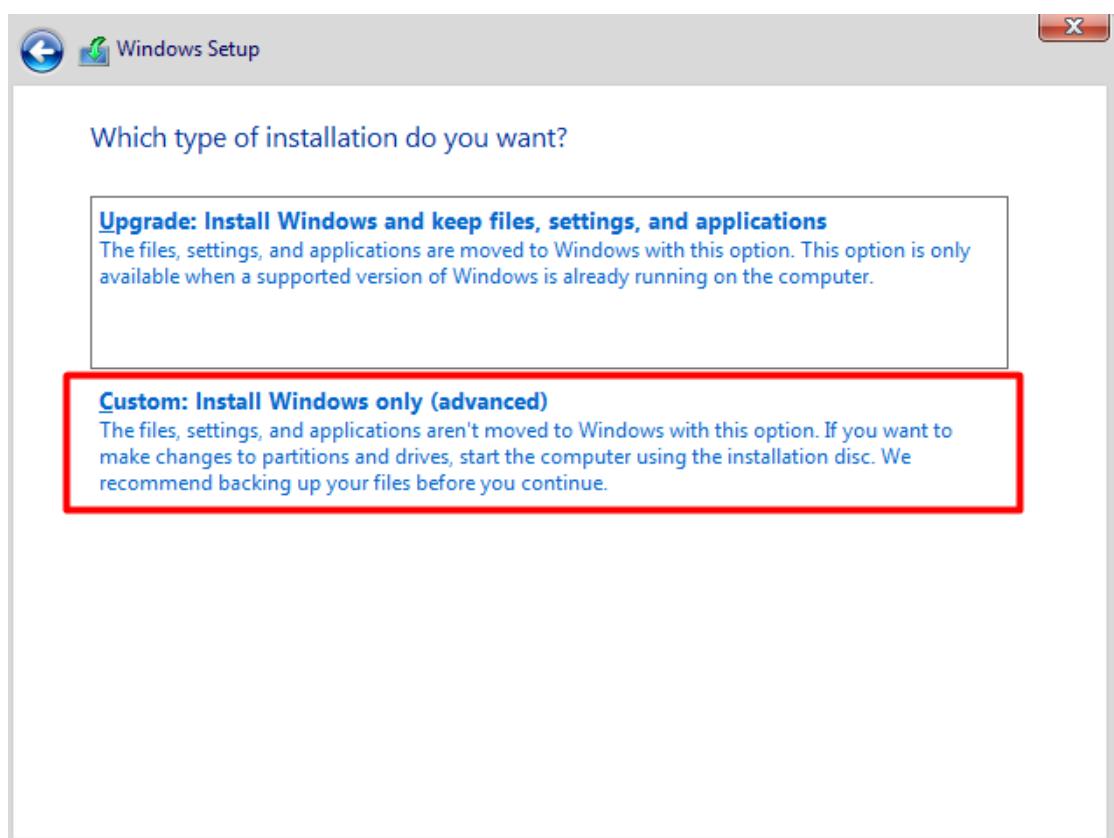
נלחץ על Install Now



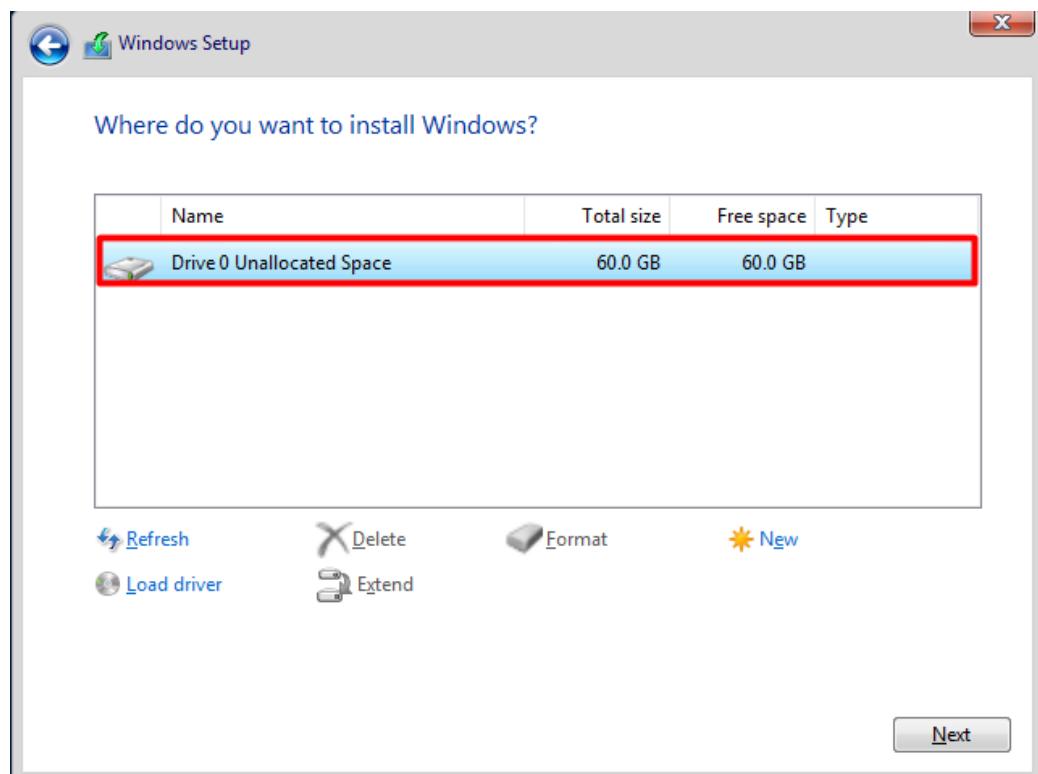
נוכחים לתקנון, לתנאים שמייקרוסופט מציבים לנו לשימוש



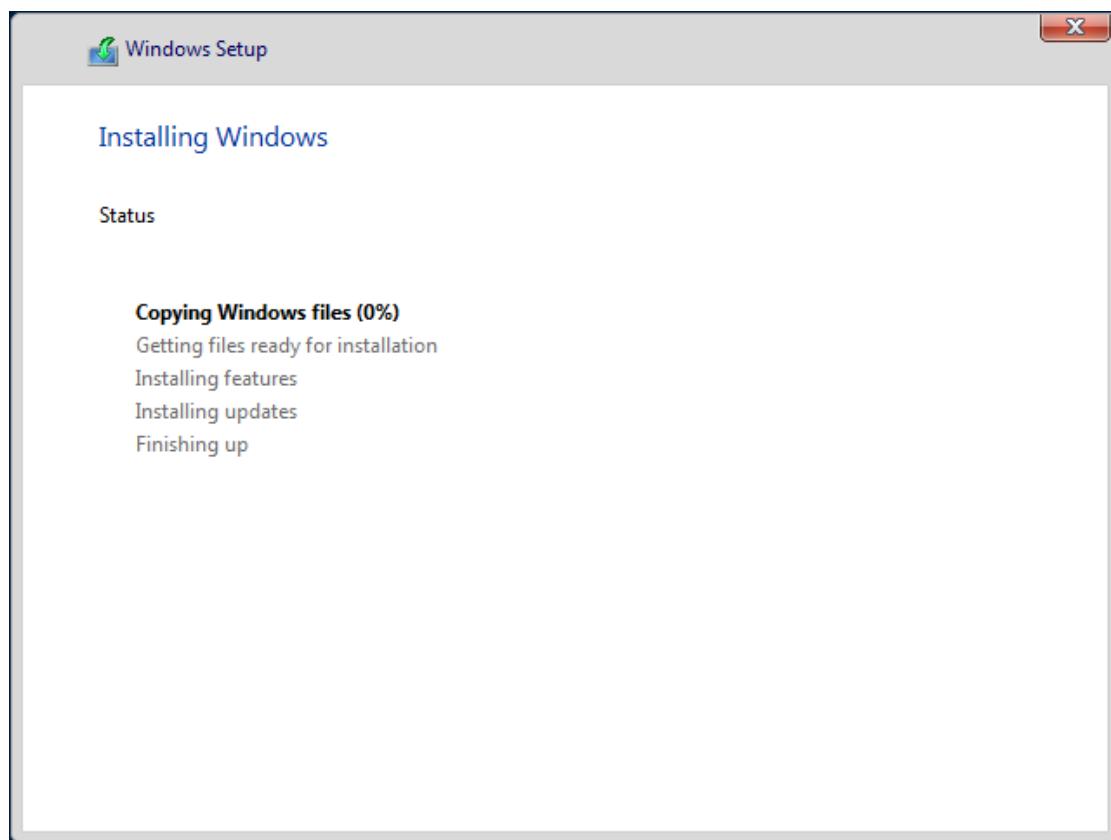
נבחר בモודル



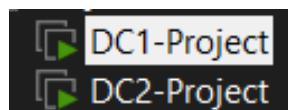
נבחר כונן, שעלי' נתקין את הווינדואס סרבר



ונתן לו להתקין

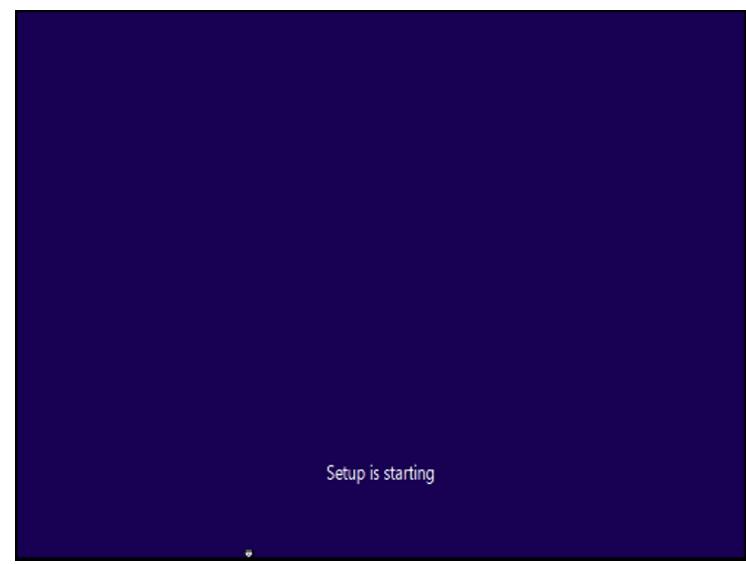


כעת יש לנו מערכת Windows Server 2019 מוכנה, נעשה את אותה התקינה בדיק לc2p, אוטם שלבים בדיק כמו בשלבים הקודמים, ונשאר עם חווית שולחן העבודה, כי נרצה בשלב מאוחר יותר להפוך אותו לשרת קבצים.

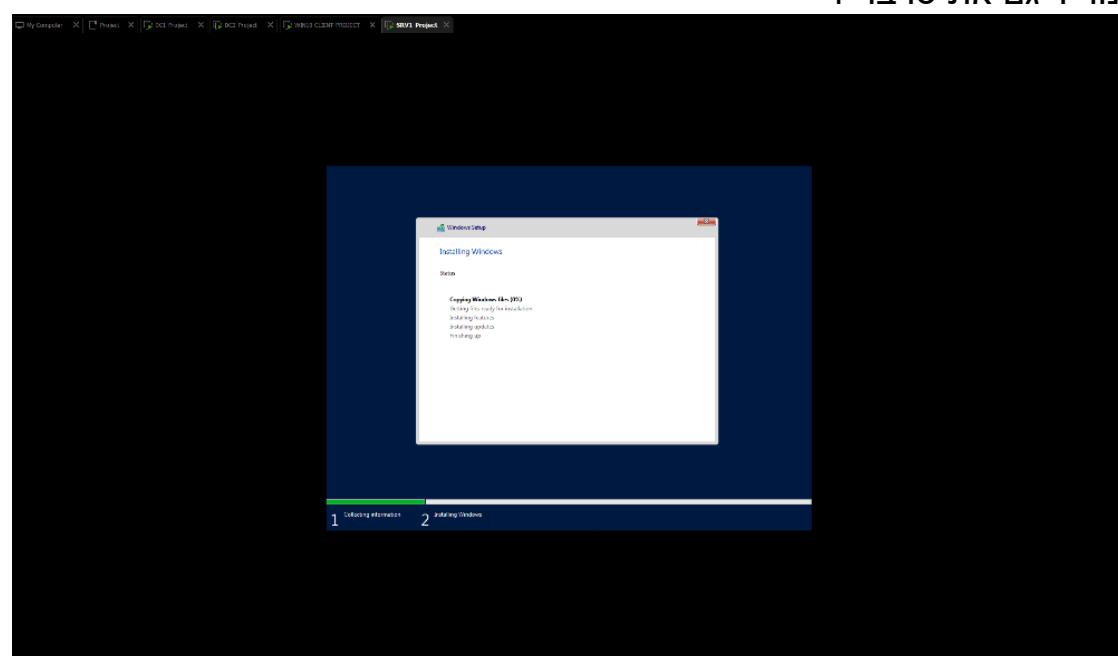


כעת יש לנו שני DC

כעת נגדיר ווינדוס 10 קליינט, ממש כמו בטופולוגיה



נוריד גם את סרבר 1



הגדרת VMWare Tools

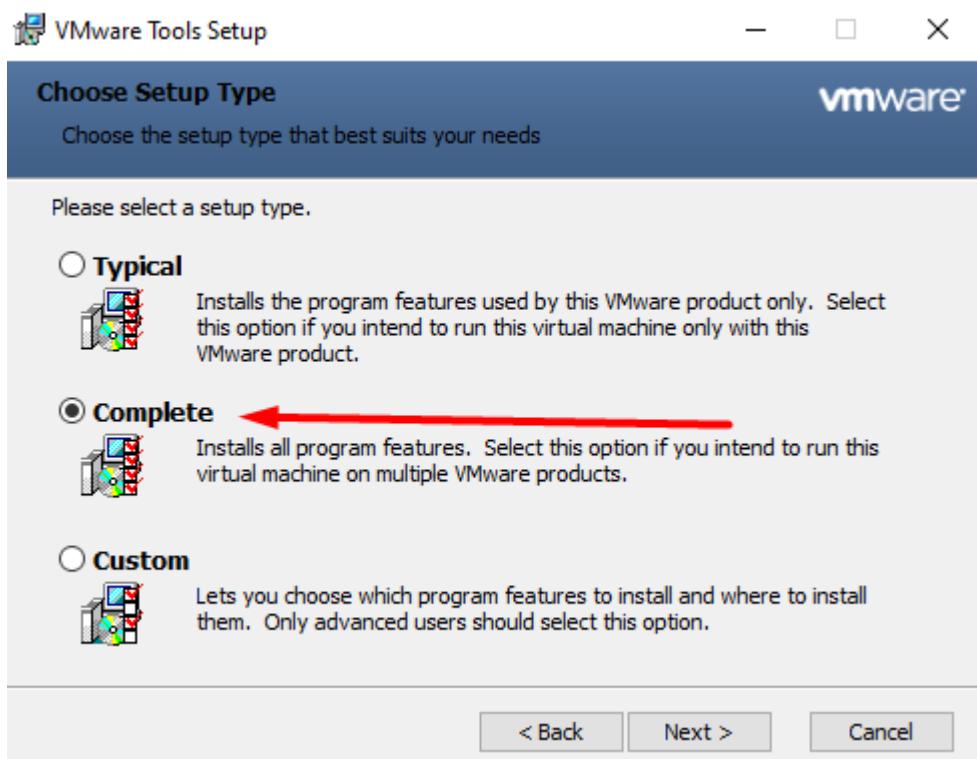
VMWARE Tools זה בעצם סט של דרייברים, למערכות הפעלה שלנו, בכך שיכלו לזרוץ כמו שציריך, לדוגמה, רזולוציה גבוהה, ביצועים טובים, חיבור ללא שנעשה, ועוד.

דבר ראשון נכנס למכשף ההתקנה של VMWare Tools

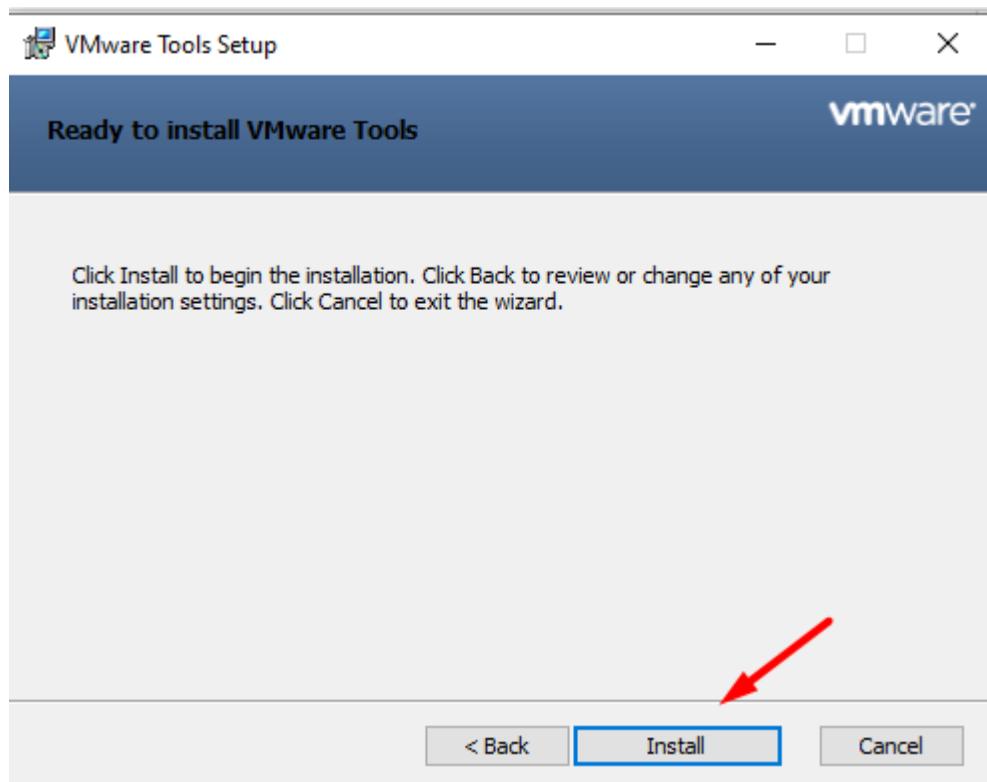


נבחר בהתקנה Complete

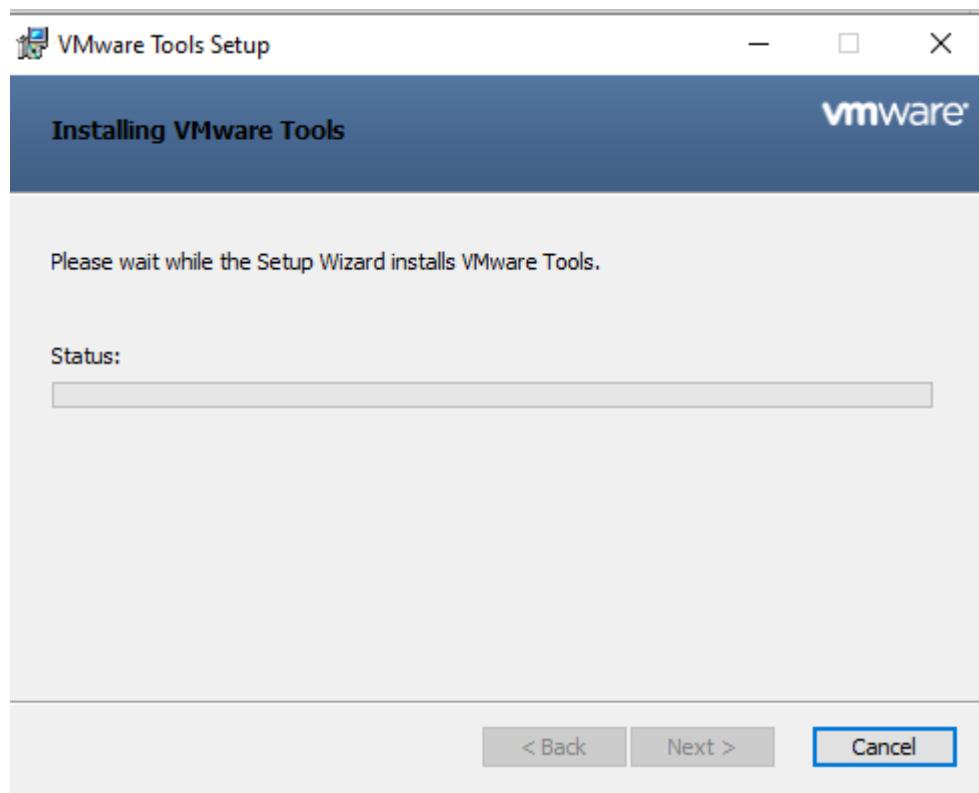
מה שההתקנה תעשה, היא תתקין את כל מה שיש ל-tools להציג



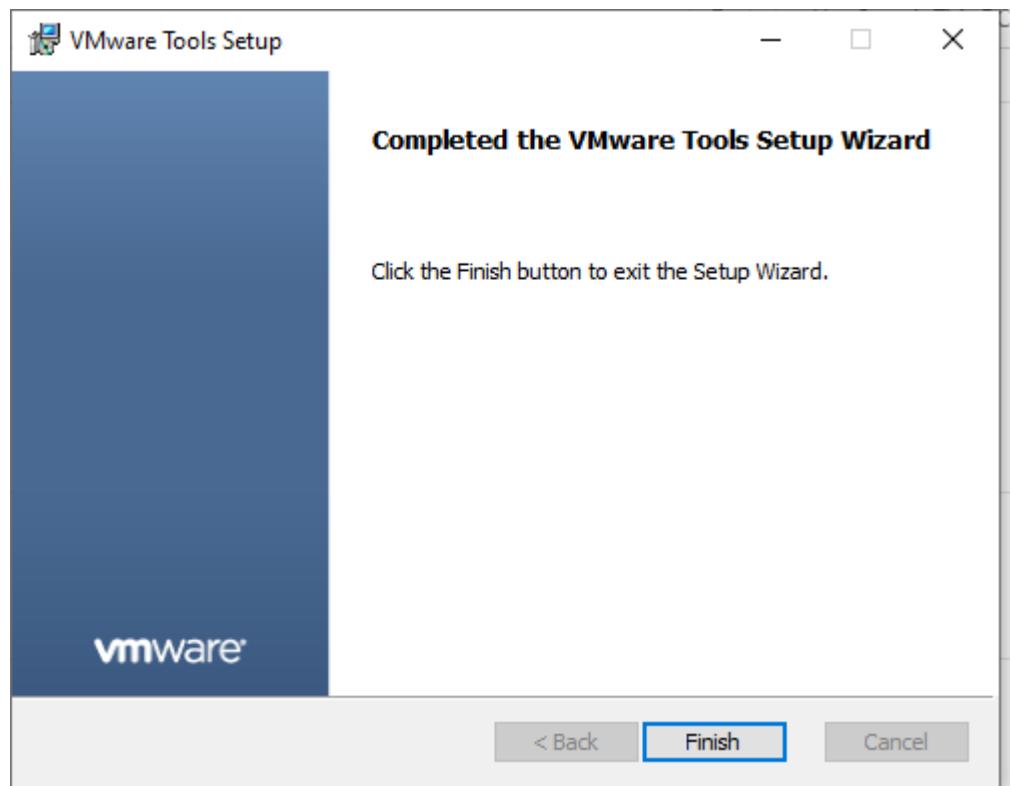
install על כל



לנו מתקין זה צעת



כעת סיום הוריד VMWare Tools, נוכל להמשיך בעבודתנו



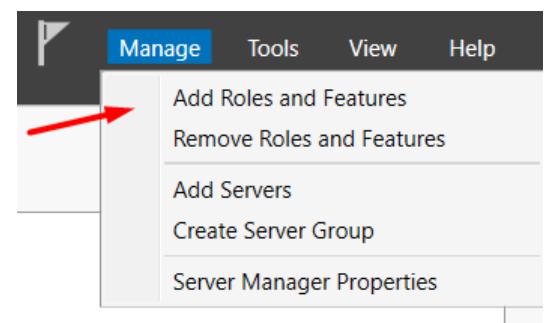
הגדרת Domain Controller

הפייה DC1 לדומיין קונטROLר DNS ו-SERVER
כעת נצורך להגדיר דומיין, נתנהל לפי ההנחיות שניתנו לנו
ההנחיות:

- שימוש ה-Domain והמחשבים לפי הפורמט הבא:
 - שם ה-Domain צריך להכיל את השם של הסטודנט. למשל: סטודנט בשם אבי אברהם – שם ה-Domain יהיה avi.xyz.net / avi.com / avi และ וכו'
 - שם המחשבים צריך להכיל את שם ה-Domain + המחשב. למשל: avi-pc1 / avi-xyz-pc1
- בשביל לבצע את זה, נצורך ללקת להגדרות דומיין קונטROLר ונעשה את המטלה הראשונה

.DNS Server -ו Domain Controller

נתחיל בלהסביר מה זה דומיין קונטROLר, הוא שירות אשר מנהל את הדומיין בארגון, זאת אומרת שמאחסן את כל המידע על המחשבים, המשתמשים, ניהול הרשאות DNS Server, זה השירות שמקשר בין שמות דומיינים לבין כתובות IP



از נלך ל-1cd ונוועה כרא:

Add Roles and Features Wizard

Before you begin

DESTINATION SERVER
WIN-LIFFTRSDT6S

Before You Begin

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

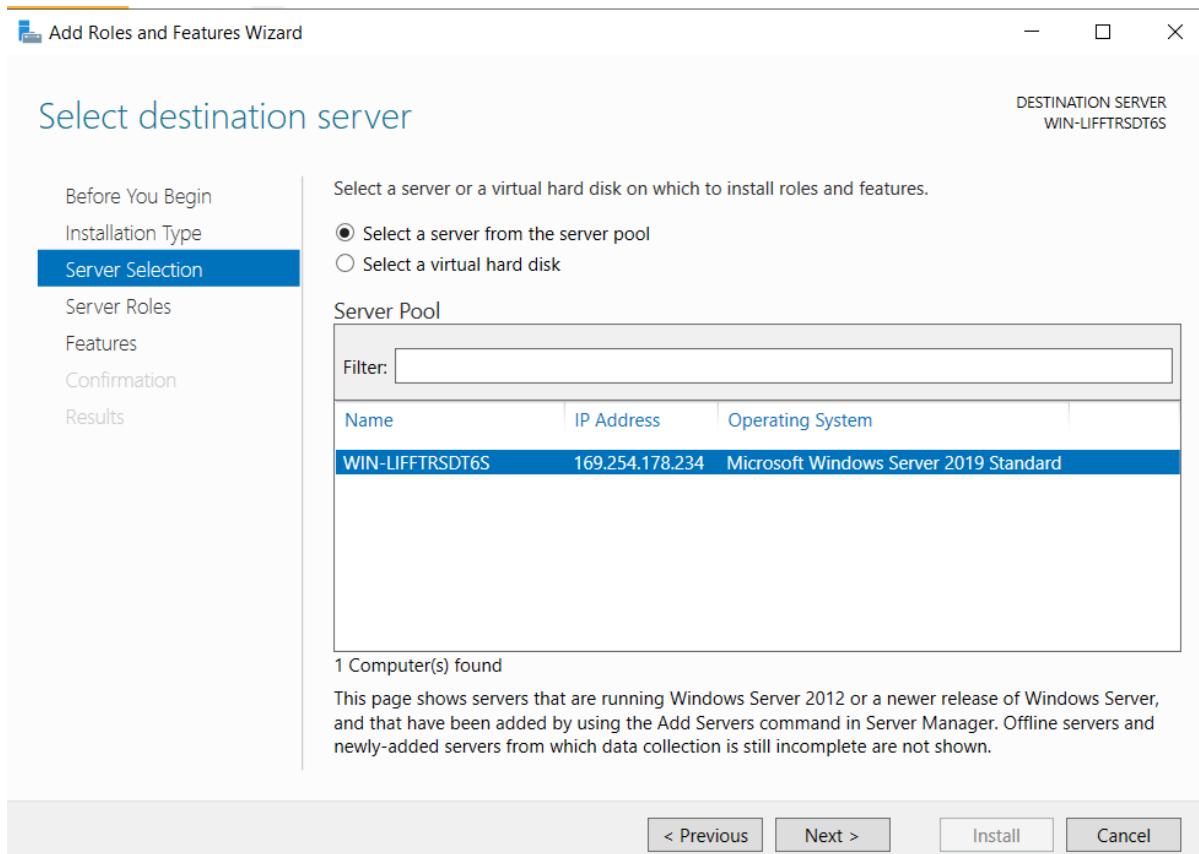
To continue, click Next.

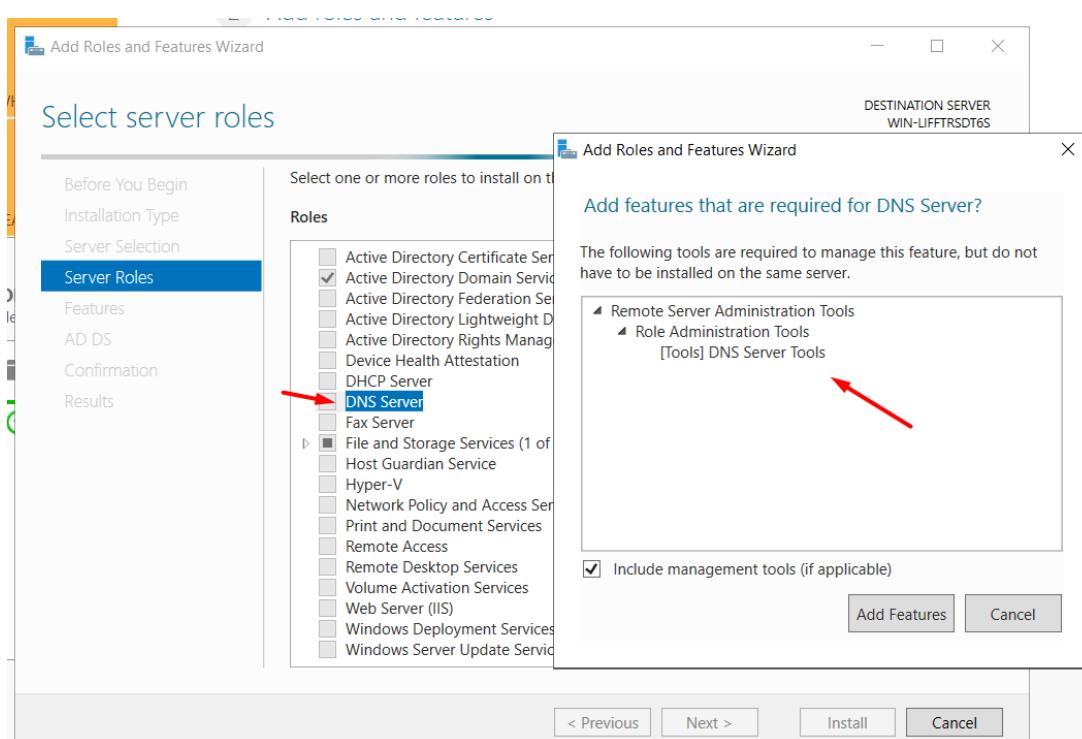
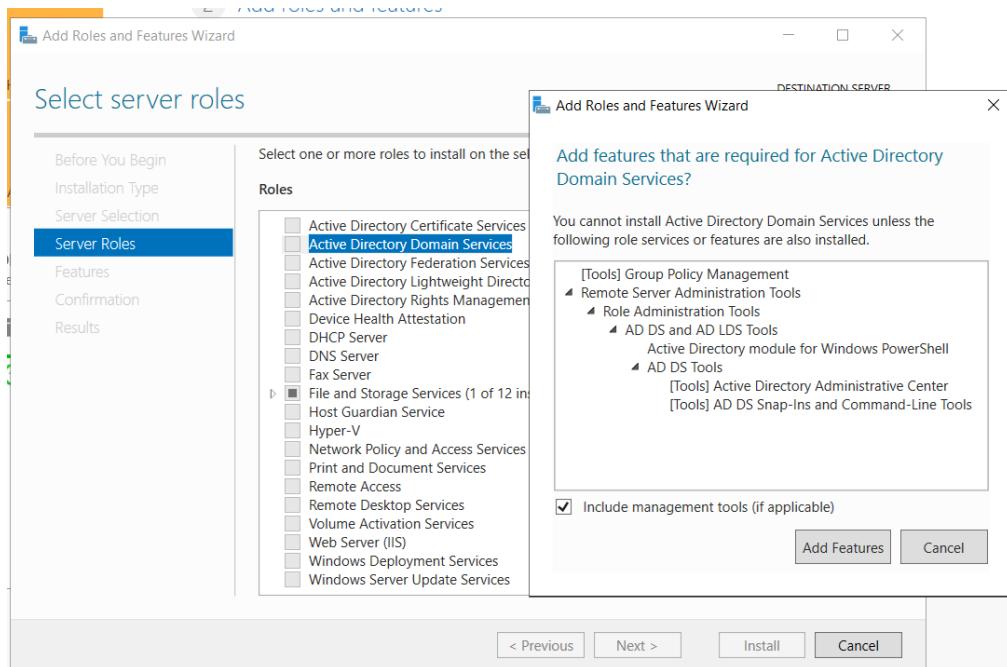
כעת נפתח לנו המחשב, נצטרך לעשות נקסט

Skip this page by default

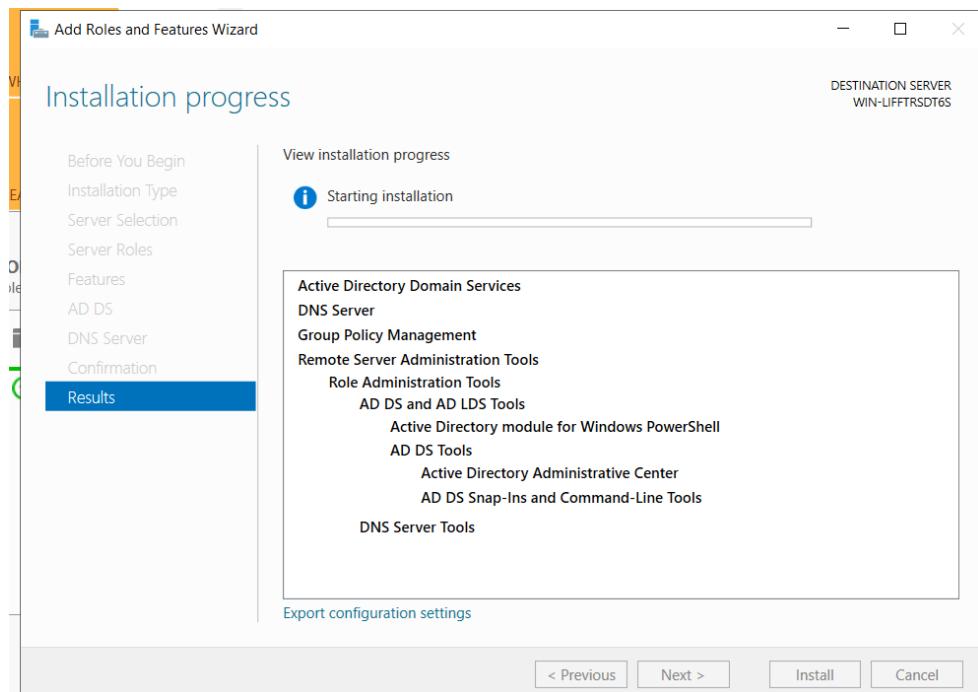
< Previous Next > Install Cancel

נבחר בסרבר, כМОבן שעדין אין שם, כי לא נתנו לו שם עדין, ניתן לו שמוים עם הדרומי

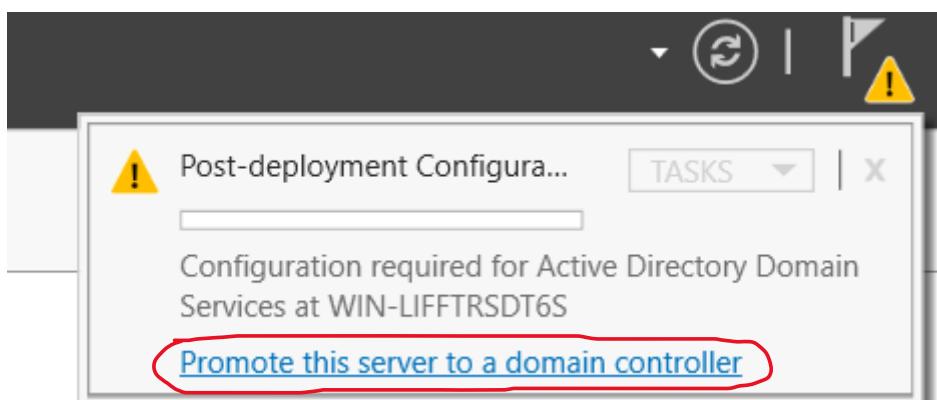




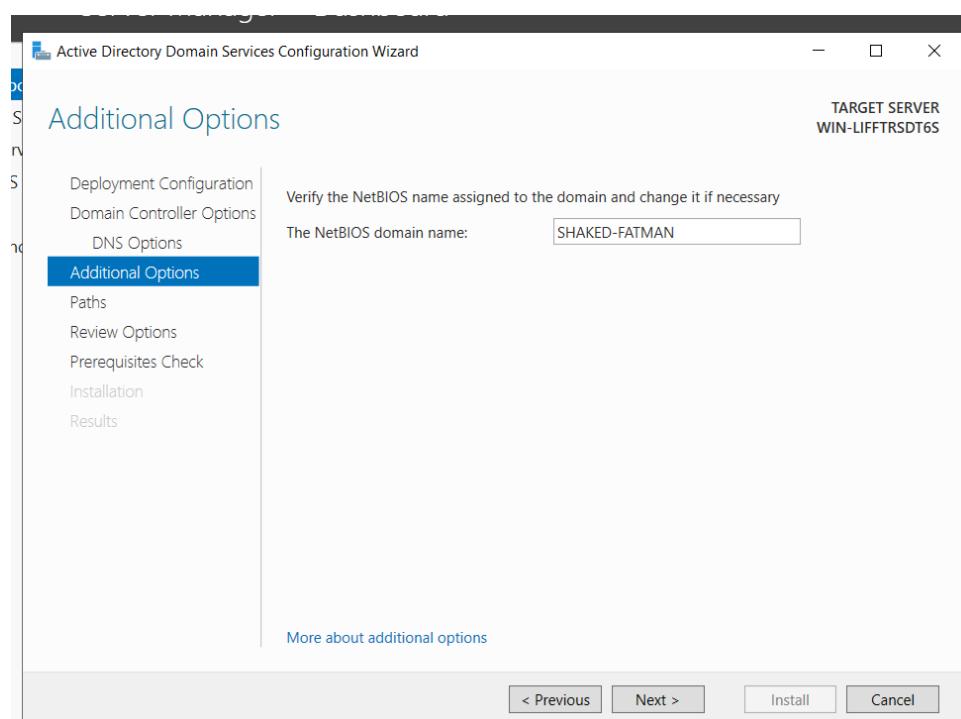
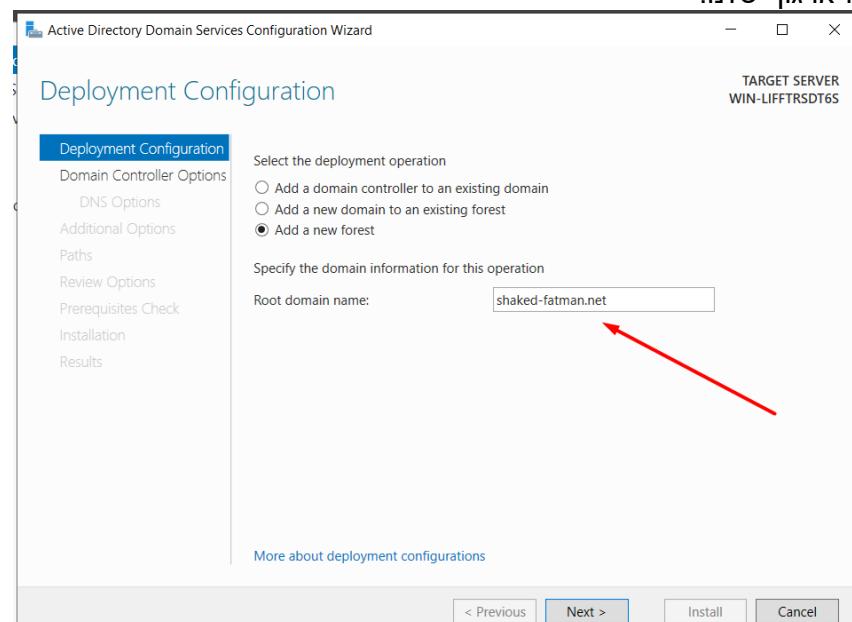
כעת אנחנו מתקינים את הכלים של שירות דומיין ודיאנוואו.



כעת נעשה את ההגדרות של דומיין קונטROLLER

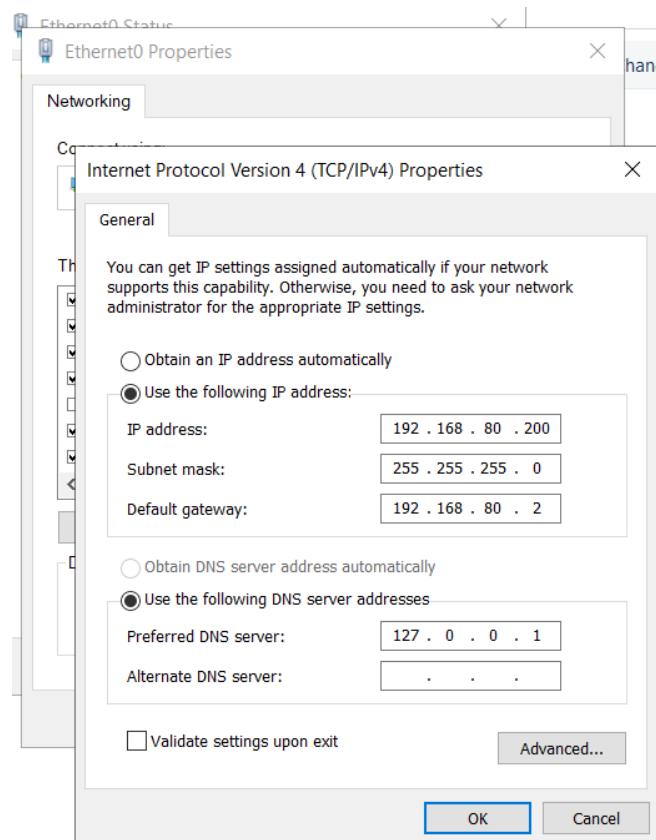


כעת ניצור דומיין חדש, דומיין זה שמו ייחודי, שמצוה אותו, אצלנו זה יהיה כביכול תחום של ה"ארגון" שלנו.



כעת נעשה Next בלי הפסקה פשוט, והמחשב יעשה Restart.

נתן כתובת IP קבועה ומסודרת, ל-dc1

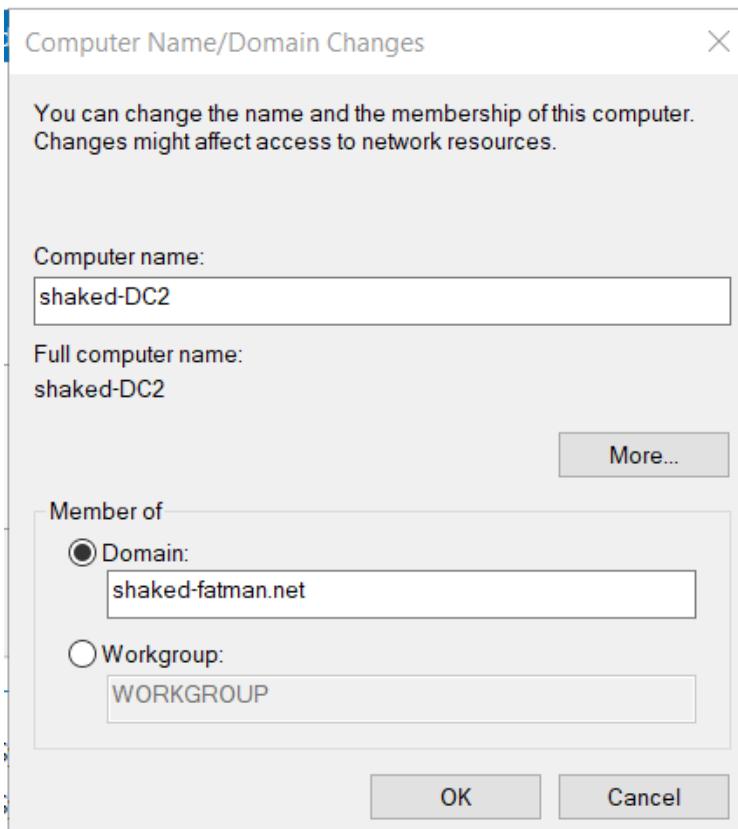


וגם ניתן לשנות שם יפה ל-dc1

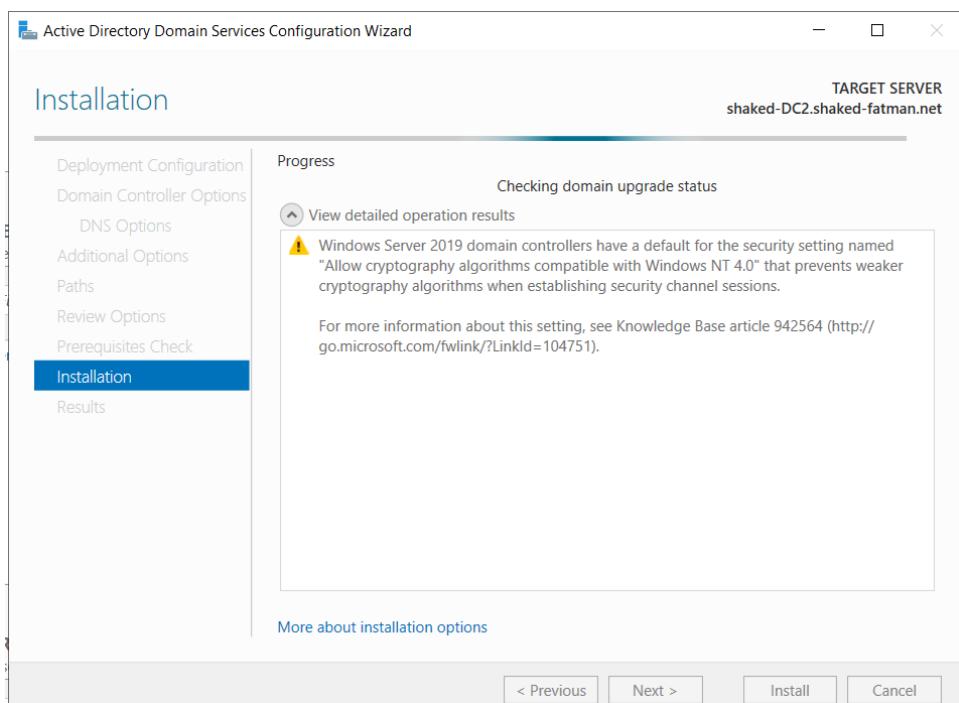
Full computer name: shaked-fatman-DC1.shaked-fatman.net

צרוף DC2 לדומיין

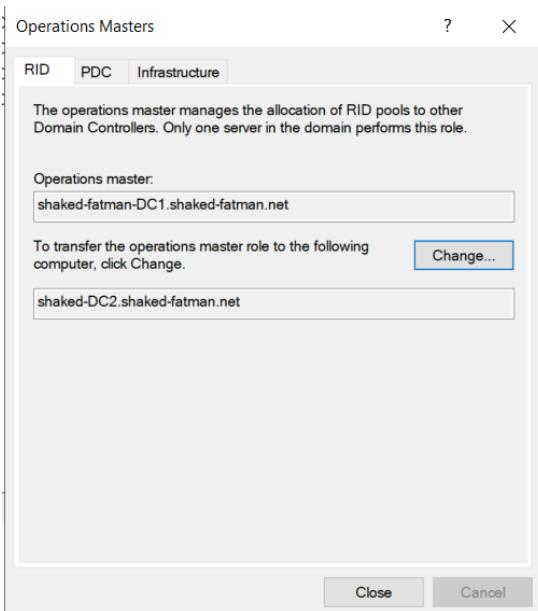
צרף את DC2 ל Domain – הגדר אותו כשרת החזיק בתפקיד Domain Master



כעת נלך ל DC2, נתן לו שם, ו לחבר אותו לדומיין



נתקין לו דומיין
סרביסץ, בצד שיכל
להיות דומיין
קונטROLLER הכרוא.



הגדרת RID master DC2

כעת נשנה את RID MASTER ל dc2

RID מאסטר זה כמו מנהל של רשות. הוא אחראי על כל המחשבים והמכשורים ברשות, ואיך הם מתחברים אחד עם השני. הוא גם אחראי על האבטחה של הרשות

The operations master manages the allocation of RID pools to other Domain Controllers. Only one server in the domain performs this role.

Operations master:
shaked-DC1.shaked-fatman.net

To transfer the operations master role to the following computer, click Change...
Change...

shaked-DC2.shaked-fatman.net

Operations Masters

Active Directory Domain Services

The operations master role was successfully transferred.

OK

Microsoft-Windows-DNS Client Events System 23/01/2024 16:32:37

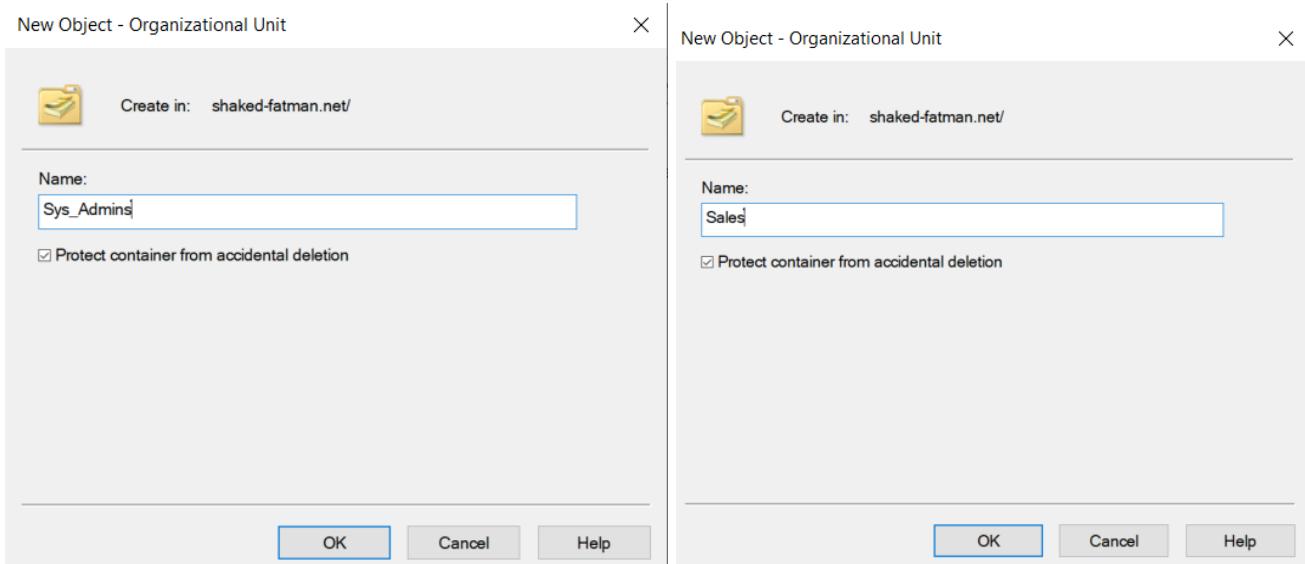
יצירת שני יחידות ארגוניות

▪ צור שני (OU) organizational unit

האחד עבר מחלקת Sales והשני עבר מחלוקת Sys_Admins

יחידות ארגוניות ב Windows Server משמשות כדי לארגן משתמשים

צרכי דרך DC1 שתי יחידות ארגוניות, לבקשתם.



Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational Unit	Default container for do...
ForeignSecur...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...
Sales	Organizational Unit	
Sys_Admins	Organizational Unit	

יצירת משתמשים חדשים, תחת היחידות הארגונית

- צור שני משתמשים חדשים בשם user1 ו- user2 (עובד מחולקת Sales).
- צור שני משתמשים נוספים בשם user3 ו- user4 (עובד מחולקת Sys_Admins).

נוצר תחת היחידה הארגונית של Sales, 2 משתמשים כמו שקבעו, את יוצר אחד ואת יוצר

Left Dialog (User2):
Create in: shaked-fatman.net/Sales
First name: User2 Initials:
Last name:
Full name: User2
User logon name: User2 @shaked-fatman.net
User logon name (pre-Windows 2000): SHAKED-FATMAN\user2
< Back Next > Cancel

Right Dialog (User1):
Create in: shaked-fatman.net/Sales
First name: User1 Initials:
Last name:
Full name: User1
User logon name: User1 @shaked-fatman.net
User logon name (pre-Windows 2000): SHAKED-FATMAN\user1
< Back Next > Cancel

ונעשה את אותו הדבר, רק במחלקה הארגונית של Sys Admins, ניצור את יוצר 3 ויוצר 4

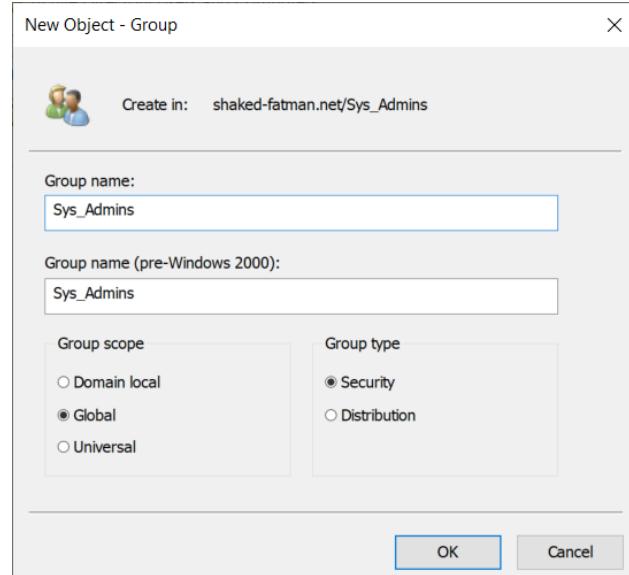
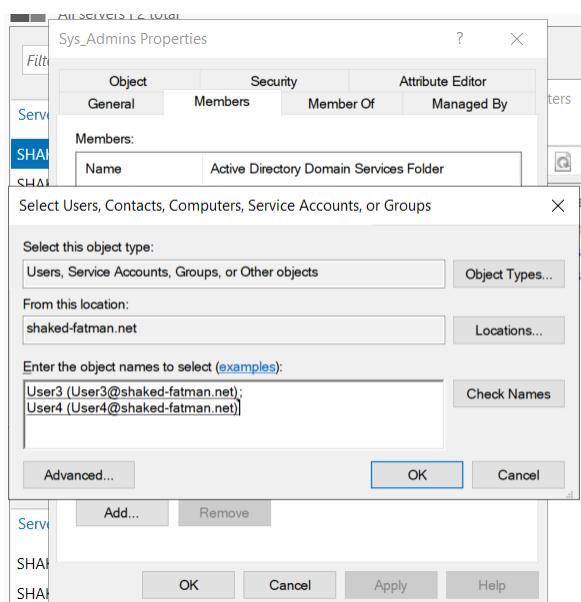
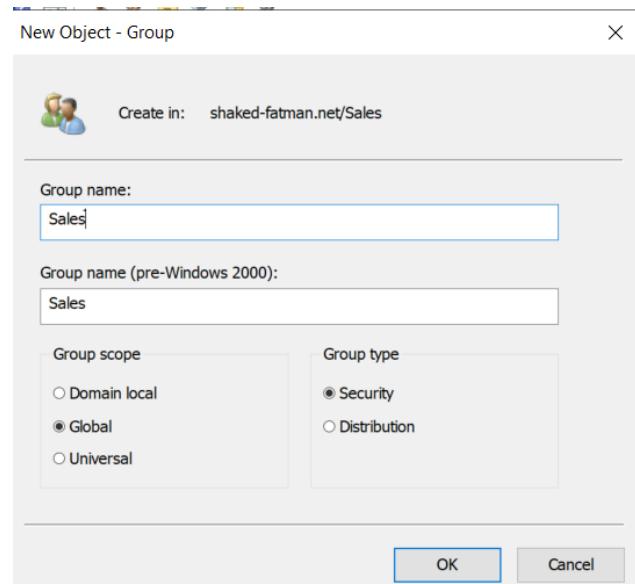
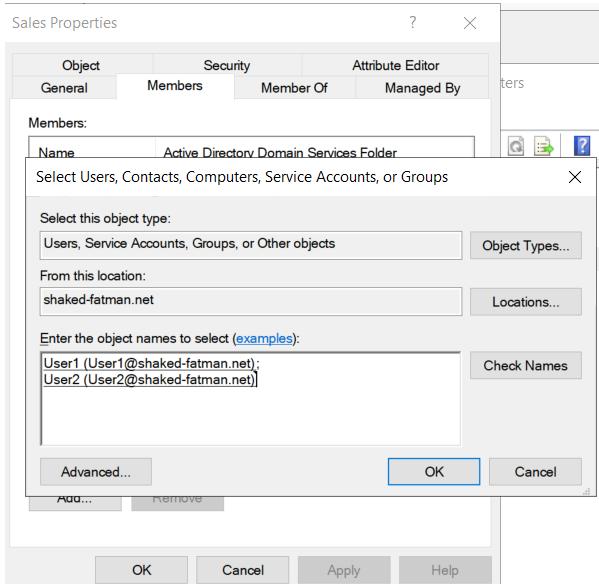
Left Dialog (User4):
Create in: shaked-fatman.net/Sys_Admins
First name: User4 Initials:
Last name:
Full name: User4
User logon name: User4 @shaked-fatman.net
User logon name (pre-Windows 2000): SHAKED-FATMAN\user4
< Back Next > Cancel

Right Dialog (User3):
Create in: shaked-fatman.net/Sys_Admins
First name: User3 Initials:
Last name:
Full name: User3
User logon name: User3 @shaked-fatman.net
User logon name (pre-Windows 2000): SHAKED-FATMAN\user3
< Back Next > Cancel

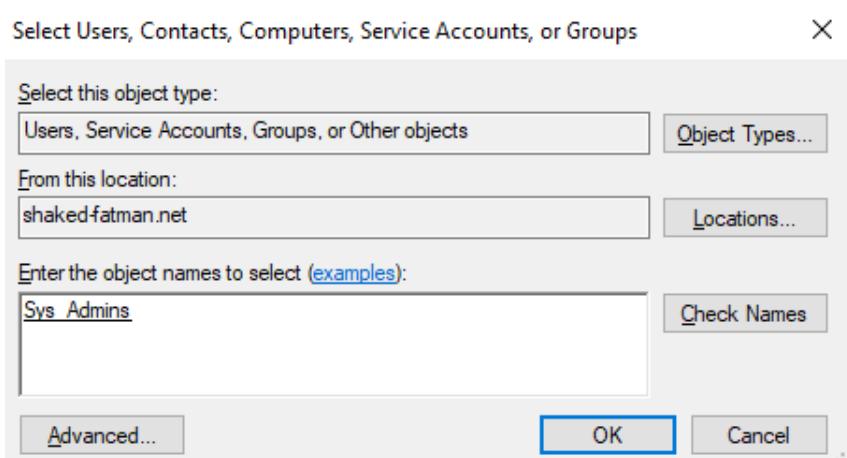
יצירת 2 קבוצות, והכנסת משתמשים אליהם

- .user2 -> user1
- .user4 -> user3
- .Domain Admins -> Sys_Admins

כעת ניצור קבוצות בתוך היחידות הארגונית, ונכנס לתוכם משתמשים, כMOVEDן לפי ההנחיות שהתבקשו.



כעת נוסיף את Sys Admins ל- Domain Admins



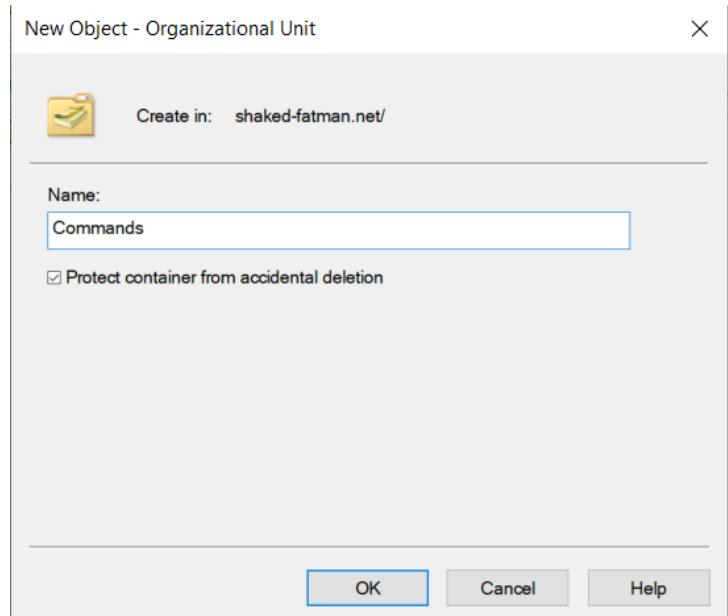
מה שביצם יקרה מרגע זה ואילך, בaczem Sys Admins הם לא סתם קבוצה, בaczem הם יכולים לשמש להם גישה לביצוע הפעולות.

יצירת 2 חשבונות משתמש אחרים על ידי שימוש בפקודות DSADD

▪ צור 2 חשבונות משתמש אחרים ע"י שימוש בפקודות DSADD

כעת נוצר עוד 2 חשבונות בעזרת פקודות, רק שנכניסו אותם לתוך סקיורייטי גראף שנקבע לו "קומנדו", אך ורק לטובות סדר.

פקודה DSADD היא פקודה שמשמשת ליצירת אובייקטים באקטיב דירקטורי. היא יכולה לשמש ליצירת משתמשים, מחשבים, קבוצות, יחידות ארגניות, ואובייקטים אחרים.



הרצתי את הפקודות הרשומות מטה בצד שיעבוד לך!

```
Administrator: Windows PowerShell
Copyright © Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> dsadd user "CN=user5,OU=commands,DC=shaked-fatman,DC=net" -samid user5 -upn user5@shaked-fatman.net -fn User -ln 5 -display "User 5" -pwd Abcd123
dsadd succeeded:CN=user5,OU=commands,DC=shaked-fatman,DC=net
PS C:\Users\Administrator>
PS C:\Users\Administrator> dsadd user "CN=user6,OU=commands,DC=shaked-fatman,DC=net" -samid user6 -upn user6@shaked-fatman.net -fn User -ln 6 -display "User 6" -pwd Abcd123
dsadd succeeded:CN=user6,OU=commands,DC=shaked-fatman,DC=net
PS C:\Users\Administrator>
```

בשתי הפקודות, ניתן לראות את המשתנים הבאים:

CN - Common Name: זהו שם המשתמש או הקבוצה.

OU - Organizational Unit: זהה תקיה ב- Active Directory המכילה משתמשים או קבוצות.

DC - Domain Component: זהו שם החלק של הדומיין.

יצירת 2 קבוצות אחרות על ידי שימוש בפקודות DSADD

צור 2 קבוצות אחרות ע"י שימוש בפקודות DSADD

עת ניצור 2 קבוצות חדשות לגמרי, אחת בשם שוארמה והשנייה בשם קbab, להן הכוחה שהכל עובד והפקודות



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright <C> Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> dsadd group "CN=shawarma,OU=commands,DC=shaked-fatman,DC=net"
dsadd succeeded:CN=shawarma,OU=commands,DC=shaked-fatman,DC=net
PS C:\Users\Administrator> dsadd group "CN=kebab,OU=commands,DC=shaked-fatman,DC=net"
dsadd succeeded:CN=kebab,OU=commands,DC=shaked-fatman,DC=net
PS C:\Users\Administrator>
```

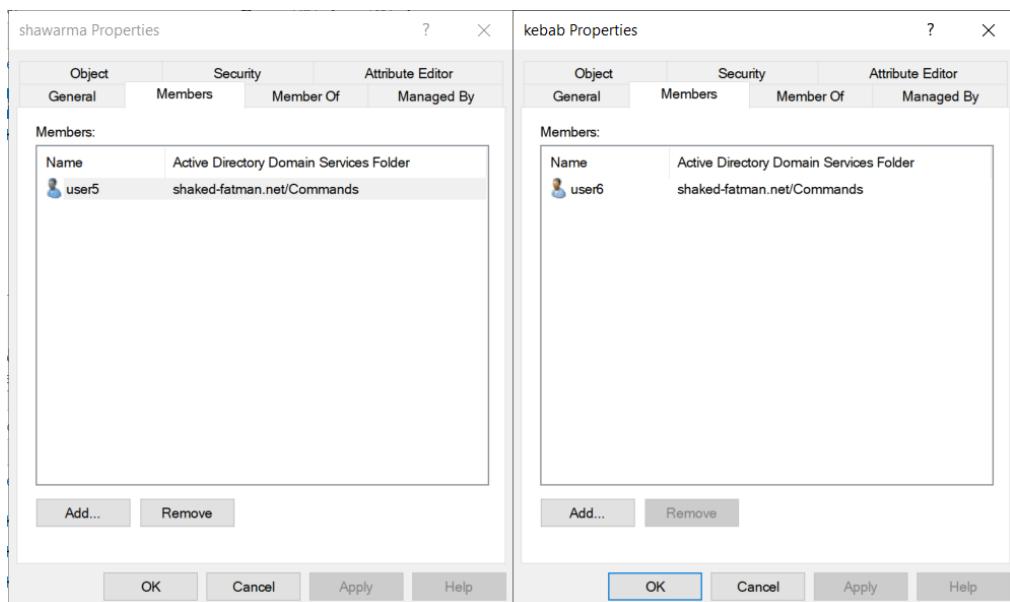
Name	Type
kebab	Security Group - Global
shawarma	Security Group - Global
user5	User
user6	User

- הכנסת החשבונות לקבוצות, רק על ידי פקודות
- הכנס את החשבונות לקבוצות השונות (ע"י פקודות בלבד)

השתמשתי בpowershell, בשבייל להוסיף את החשבונות לקבוצות
השתמשתי בpowershell, בשבייל להוסיף את החשבונות לקבוצות
השתמשתי בpowershell, בשבייל להוסיף את החשבונות לקבוצות
השתמשתי בpowershell, בשבייל להוסיף את החשבונות לקבוצות

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

PS C:\Users\Administrator> dsmod group "CN=shawarma,OU=commands,DC=shaked-fatman,DC=net" -addmbr "CN=user5,OU=commands,DC=shaked-fatman,DC=net"
dsmod succeeded:CN=shawarma,OU=commands,DC=shaked-fatman,DC=net
PS C:\Users\Administrator> dsmod group "CN=kebab,OU=commands,DC=shaked-fatman,DC=net" -addmbr "CN=user6,OU=commands,DC=shaked-fatman,DC=net"
dsmod succeeded:CN=kebab,OU=commands,DC=shaked-fatman,DC=net
PS C:\Users\Administrator>
```



יצירת עשרה חשבונות על ידי סкриיפט, שמשתמש בפקודה DSADD

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

cut ניצור סкриיפט, שמשתמש בלולאה, וגם בפקודת DSADD שתcin ל' Users מ-20-30, בעזרת סיסמה קבועה, ליחידה שהוראים לה Commands, cut אראה את הפקודה והוכחה שעובד כמובן.

```
[Administrator: Windows PowerShell]
Windows PowerShell
Copyright <C> Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> $ou = "OU=commands,DC=shaked-fatman,DC=net"
PS C:\Users\Administrator> $password = "Abcd123"
PS C:\Users\Administrator> for ($i = 20; $i -le 30; $i++) {
    >>> $username = "user$i"
    >>> dsadd user "CN=$username,$ou" -samid $username -upn "$username@shaked-fatman.net" -fn User -ln $i -display "User $i" -pwd $password
    >>>
dsadd succeeded:CN=user20,OU=commands,DC=shaked-fatman,DC=net
dsadd succeeded:CN=user21,OU=commands,DC=shaked-fatman,DC=net
dsadd succeeded:CN=user22,OU=commands,DC=shaked-fatman,DC=net
dsadd succeeded:CN=user23,OU=commands,DC=shaked-fatman,DC=net
dsadd succeeded:CN=user24,OU=commands,DC=shaked-fatman,DC=net
dsadd succeeded:CN=user25,OU=commands,DC=shaked-fatman,DC=net
dsadd succeeded:CN=user26,OU=commands,DC=shaked-fatman,DC=net
dsadd succeeded:CN=user27,OU=commands,DC=shaked-fatman,DC=net
dsadd succeeded:CN=user28,OU=commands,DC=shaked-fatman,DC=net
dsadd succeeded:CN=user29,OU=commands,DC=shaked-fatman,DC=net
dsadd succeeded:CN=user30,OU=commands,DC=shaked-fatman,DC=net
```

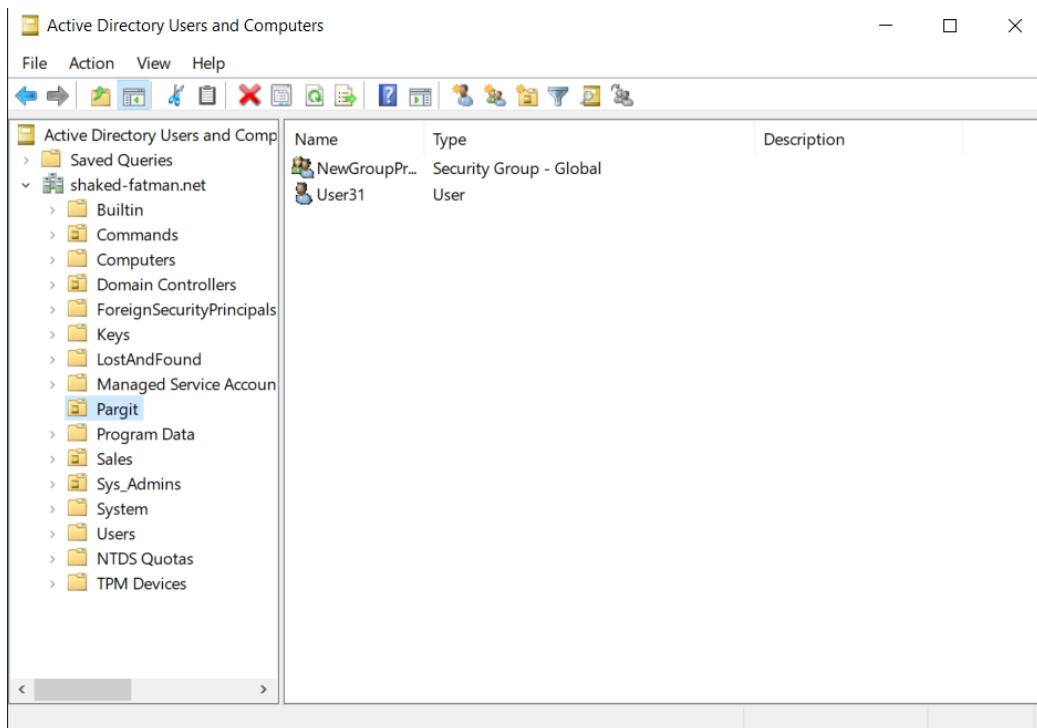
Name	Type	Description
kebab	Security Group - Global	
shawarma	Security Group - Global	
user20	User	
user21	User	
user22	User	
user23	User	
user24	User	
user25	User	
user26	User	
user27	User	
user28	User	
user29	User	
user30	User	
user5	User	
user6	User	

**יצירת יחידה ארגונית + חשבון משתמש חדש + קבוצה חדשה רק על ידי פקודות
צור OU חדש + חשבון משתמש חדש + קבוצה חדשה ע"י פקודות ב PS**

הסקריפט הזה יוצר קבוצה חדשה בשם "NewGroupProjectYes" ביחידת הארגון .
היחידה בכללי זמינה בכל הדומיין, ביחד עם החשבון החדש והקבוצה.
ניצור סקריפט אחד, שיעשה את כל זה, להלן הפקודה והוכחה שעובדת.

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

C:\Users\Administrator>$baseDN = "DC=shaked-fatman,DC=net"
C:\Users\Administrator>$ou = "Pargit"
C:\Users\Administrator>$user = "User31"
C:\Users\Administrator>$group = "NewGroupProjectYes"
C:\Users\Administrator>$password = "R0ad123"
C:\Users\Administrator>New-ADOrganizationalUnit -Name $ou -Path "DC=shaked-fatman,DC=net"
C:\Users\Administrator>New-ADUser -SamAccountName $user -UserPrincipalName "$user@shaked-fatman.net" -GivenName "User" -Surname "31" -DisplayName "User 31" -Name $user -Path "OU=$ou,$baseDN" -AccountPassword (ConvertTo-SecureString -AsPlainText $password -Force) -Enabled $true
C:\Users\Administrator>New-ADGroup -Name $group -GroupScope Global -Path "OU=$ou,$baseDN"
```



יצירת עשרה חשבונות חדשים על ידי סкриיפט מבוסס PowerShell

צור 10 חשבונות חדשים ע"י script מבווס PS

ניצור 10 חשבונות חדשים על ידי סкриיפט, הסקרייפט יהיה מצורף למטרה בתמונה, כמוובן, הוכחה שהכל עובד. הסקרייפט יצר לנו עשרה חשבונות חדשים, וכמוובן שהשתמשנו בPowerShell.

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

PS C:\Users\Administrator> $ErrorActionPreference = "SilentlyContinue"
>>> $ou = "Pargit"
>>> $password = "Shadid123"
>>> $ouPath = "OU=$ou,DC=shaked-fatman,DC=net"

>>> New-ADOrganizationalUnit -Name $ou -Path "DC=shaked-fatman,DC=net" -ErrorAction SilentlyContinue

>>> for ($i = 40; $i -le 50; $i++) {
>>>     $username = "user$i"
>>>     $displayname = "User $i"
>>>
>>>     New-ADUser -SamAccountName $username -UserPrincipalName "$username@shaked-fatman.net" -Name $username -GivenName "User" -Surname $i -DisplayName $displayname -Path $ouPath -AccountPassword (ConvertTo-SecureString -AsPlainText $password -Force) -Enabled $true
>>> }
>>> $ErrorActionPreference = "Continue"
>>>

PS C:\Users\Administrator>
```

Name	Type
NewGroupPr...	Security Group - Global
User31	User
user40	User
user41	User
user42	User
user43	User
user44	User
user45	User
user46	User
user47	User
user48	User
user49	User
user50	User

בדיקות שרתים DC, שהכל תקין, וshall ה שינויים מסתנכרנים.

- **בדוק shall ה שינויים ב AD מסונכרנים בין 2 שרתים DC**

כעת נבדוק shall ה שינויים שביצעו בהחלת נשמרו גם בDC

בתמונה לעיל ניתן לראות את DC1 ובתמונה מטה נראה את DC2, ואנו נראה את הדברים כי אחורוניים שעשינו, בשביל לוודא שהכל התעדכן.

ניתן לראות שבאמת הכל קיים.

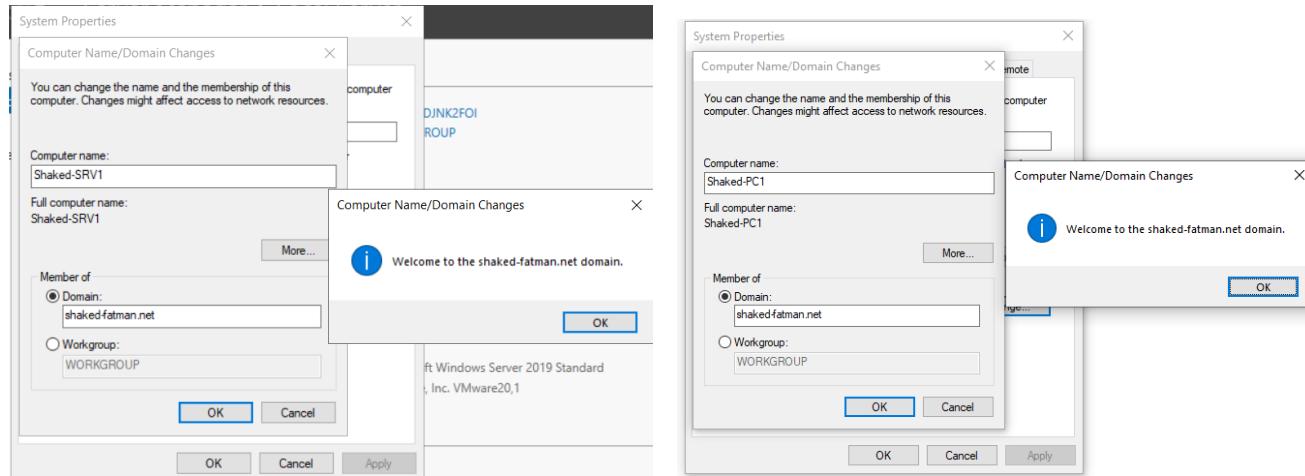
Name	Type	Description
NewGroupP...	Security Group - Global	
User31	User	
user40	User	
user41	User	
user42	User	
user43	User	
user44	User	
user45	User	
user46	User	
user47	User	
user48	User	
user49	User	
user50	User	

Name	Type	Description
NewGroupP...	Security Group - Global	
User31	User	
user40	User	
user41	User	
user42	User	
user43	User	
user44	User	
user45	User	
user46	User	
user47	User	
user48	User	
user49	User	
user50	User	

צירוף המחשבים לדומיין

צירוף המחשבים ל-Domain
▪ צירוף את SRV1 - WIN10

כעת נחבר את וינדוז 10 ורבר 1 שהתקנו קודם, לדומיין שלנו, לא כתבתי את השם המלא של הדומיין, מאחר וקפיצה לי שגיאה, שהשם ארוך מדי, אז כתבתי את השם שלו, בכל אופן, כדי להוכיח, שאני זה שיצר את הפרויקט



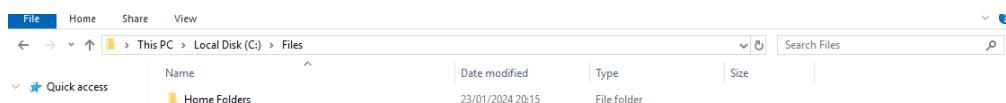
לאחר צירוף מחשבים לדומיין המחשבים יהיו מנוהלים על ידי Active Directory של הארגון.

פרופיל משתמש

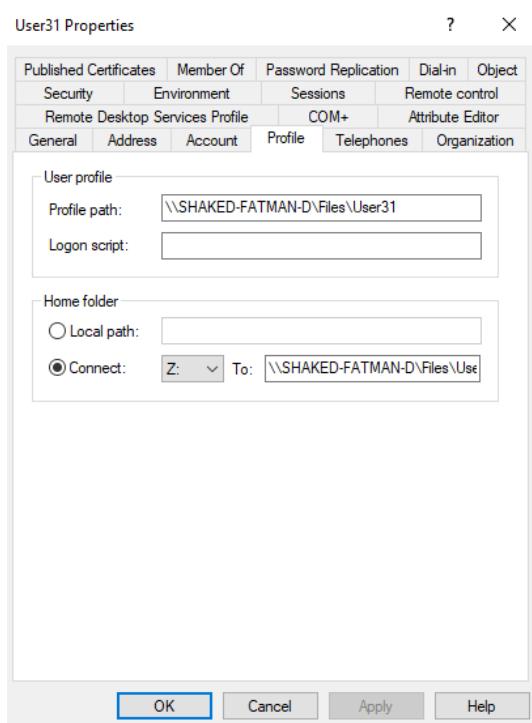
יצירת פרופיל משתמש נודד לחשבון שיצרנו בתרגילים הקודמים פרופיל נודד זה מקום בו המחשב שומר את הגדרות שלך, כמו שולחן העבודה, הרקע, והתוכנות שאתה מתקן. אם אתה משתמש בפרופיל נודד, אתה יכול להיכנס למחשב אחר ולראות את אותן הגדרות בדיק, או בקיצור ממש כמו לקחת את המחשב שלך לכל מקום

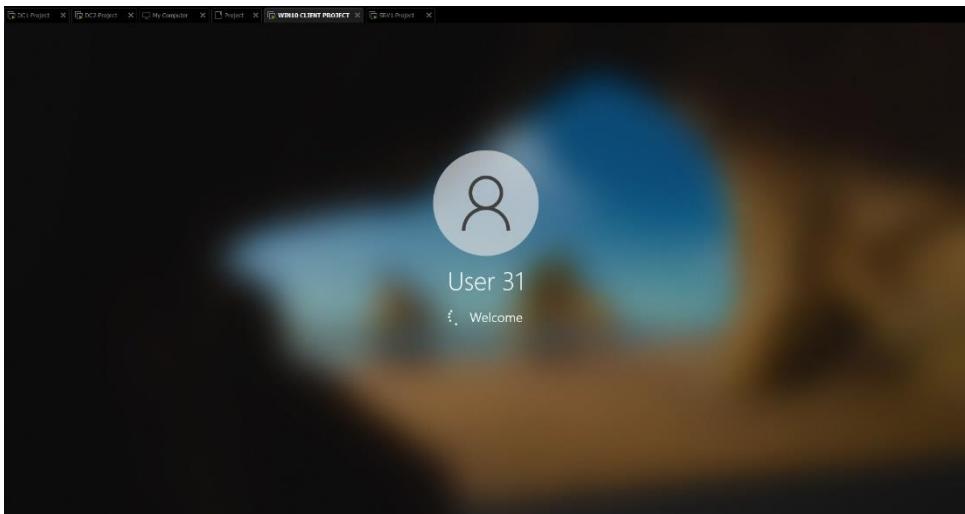
צור פרופיל משתמש נודד לחשבון שיצרנו בתרגילים הקודמים

בשביל ליצור פרופיל משתמש נודד, נצטרך תיקיה משותפת.



נשתק עתה עם כל היוזרים
ונכתב את הפרופיל לתיקיה, כדי שיוכל להיות משותף.



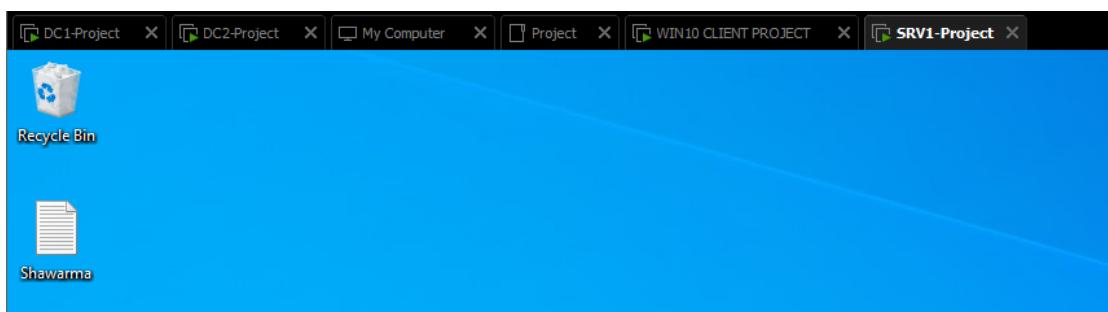
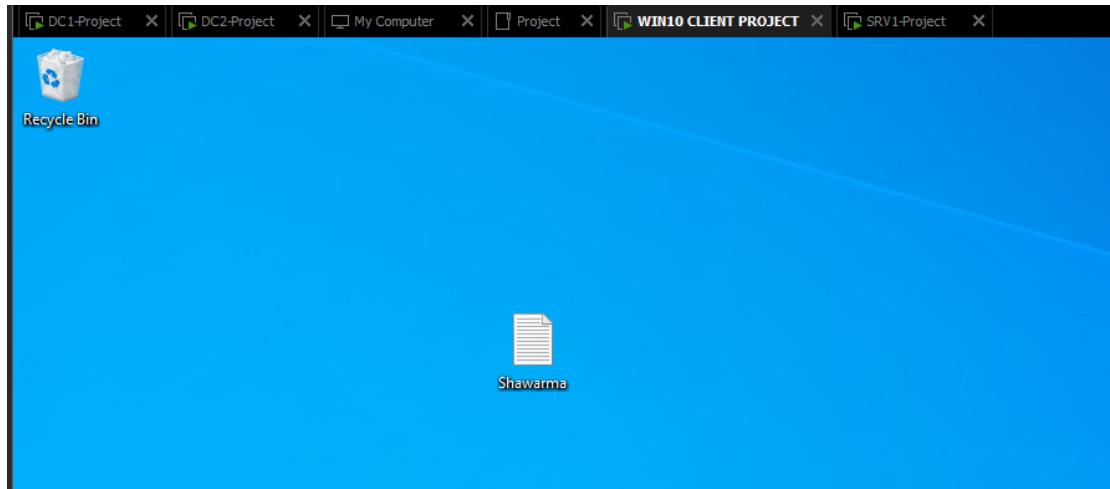


ונitinן לראות
שהפרופיל עובד

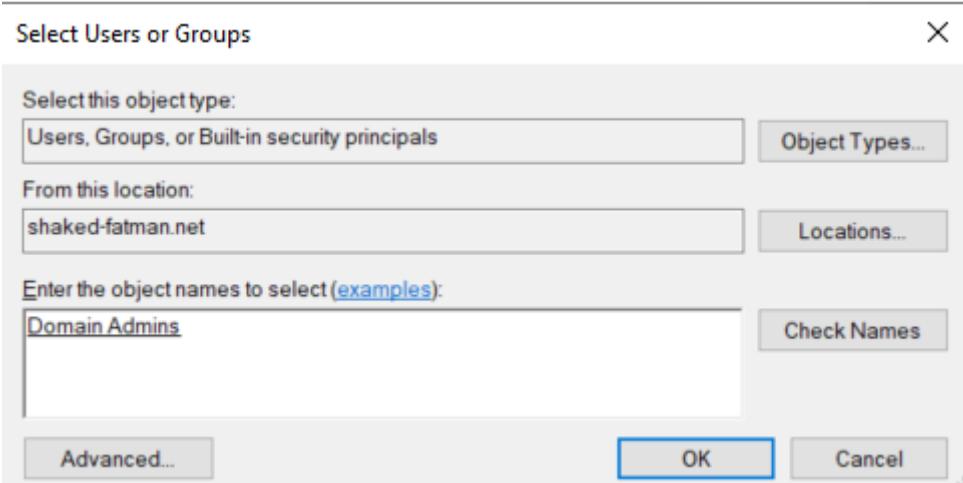
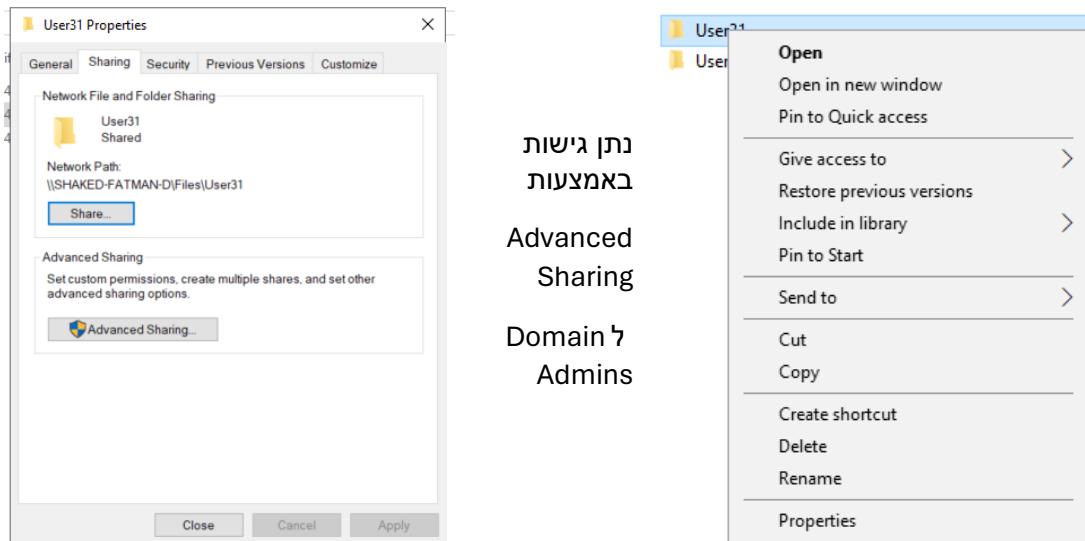
בדיקות שהפרופיל אכן נודד

▪ בדוק שהפרופיל אכן נודד ממחשב למחשב

לטובות הבדיקה, אוצר קובץ טיקסט חדש, נקרא לו בסתם שם, נגיד, שוארמה, ונבדוק אם נראה אותו במחשב אחר, כאשר נתחבר לפרופיל



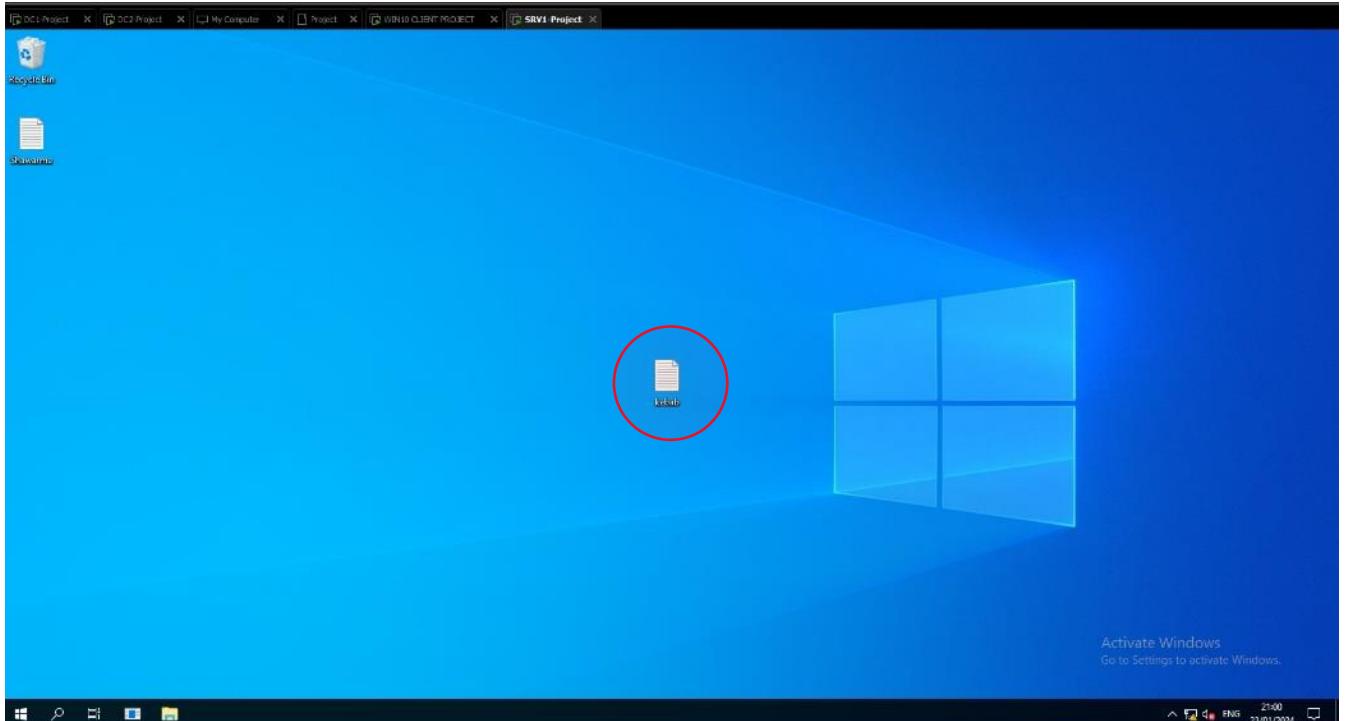
שינויי ההגדרות, בכדי לחת לאדמינים, לגשת לティקיות הפרופיל
 • שנה את ההגדרות כך שמנהל הרשות יוכל להכנס לティקיות הפרופיל בשרת (Domain Admin)



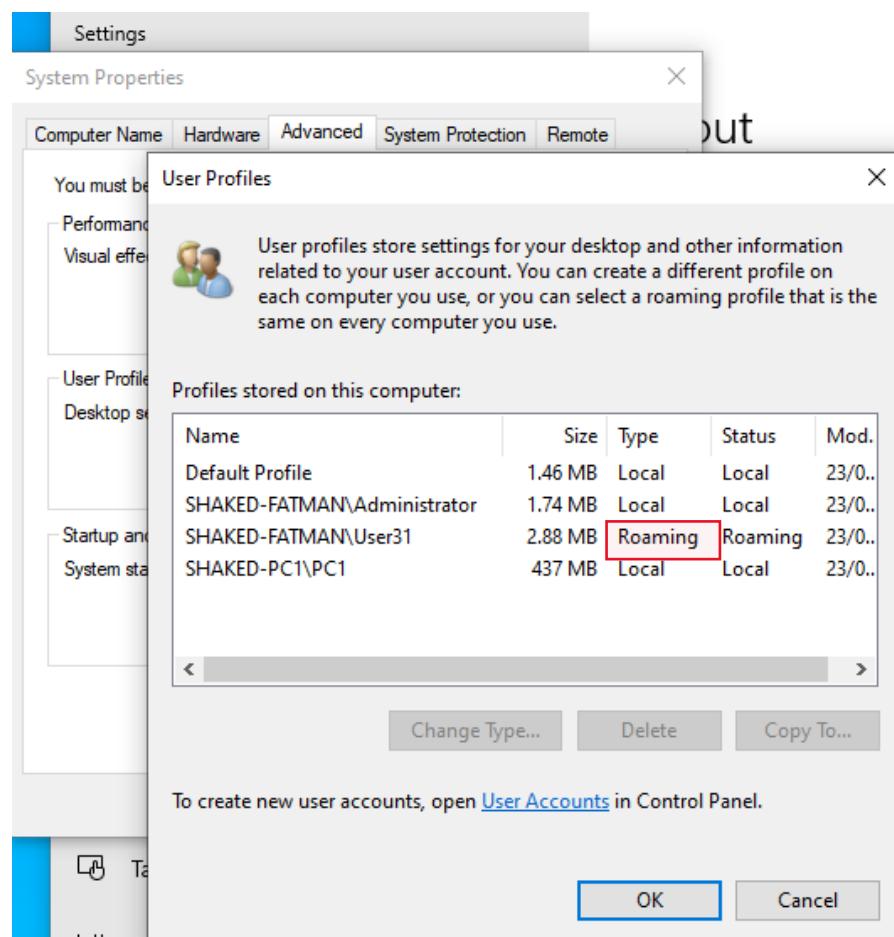
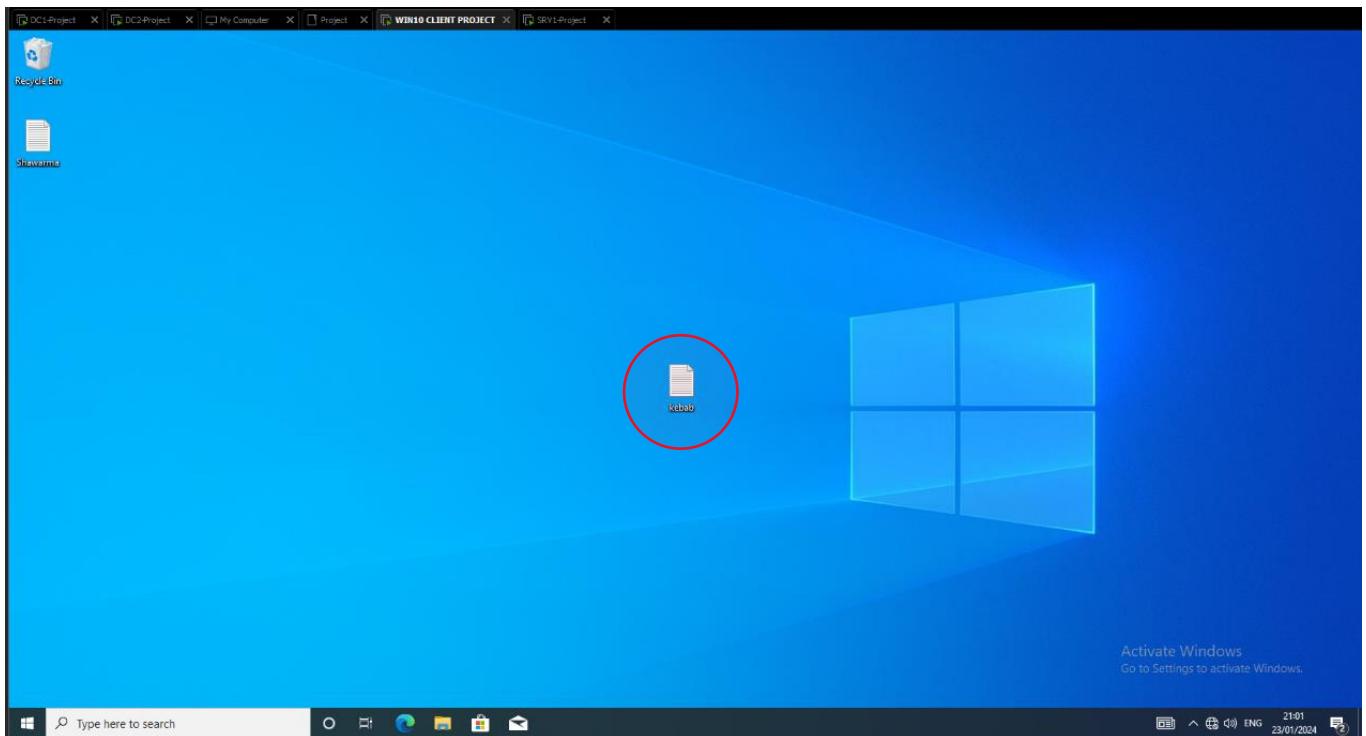
בדיקות שוב שהפרופיל אכן תקין ונולד

- **בדיקה שוב שהפרופיל אכן תקין ונולד ממחשב**

ניצור עוד קובץ, נקרא לו קבב.

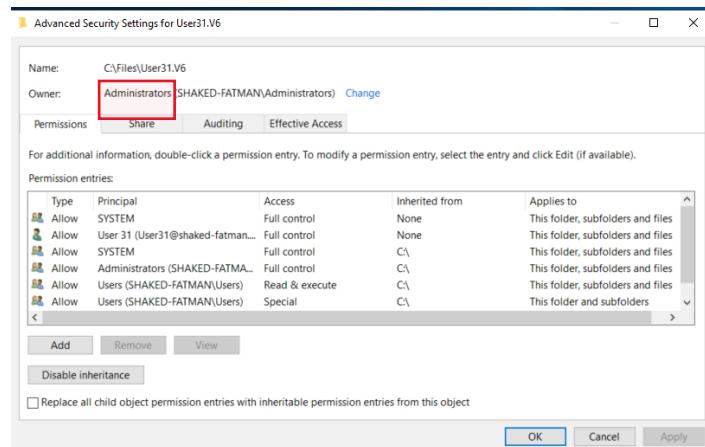


ונitin לראות שהפרofil אכן תקין ונodd.



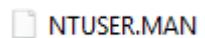
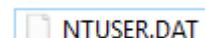
שינוי ה profiel, ל profiel מנדטורי

שנה את הגדרות ה profiel כך שהוא יהיה מנדטורי – כמובן – לא ניתן יהיה לשנות שום דבר ב profiel

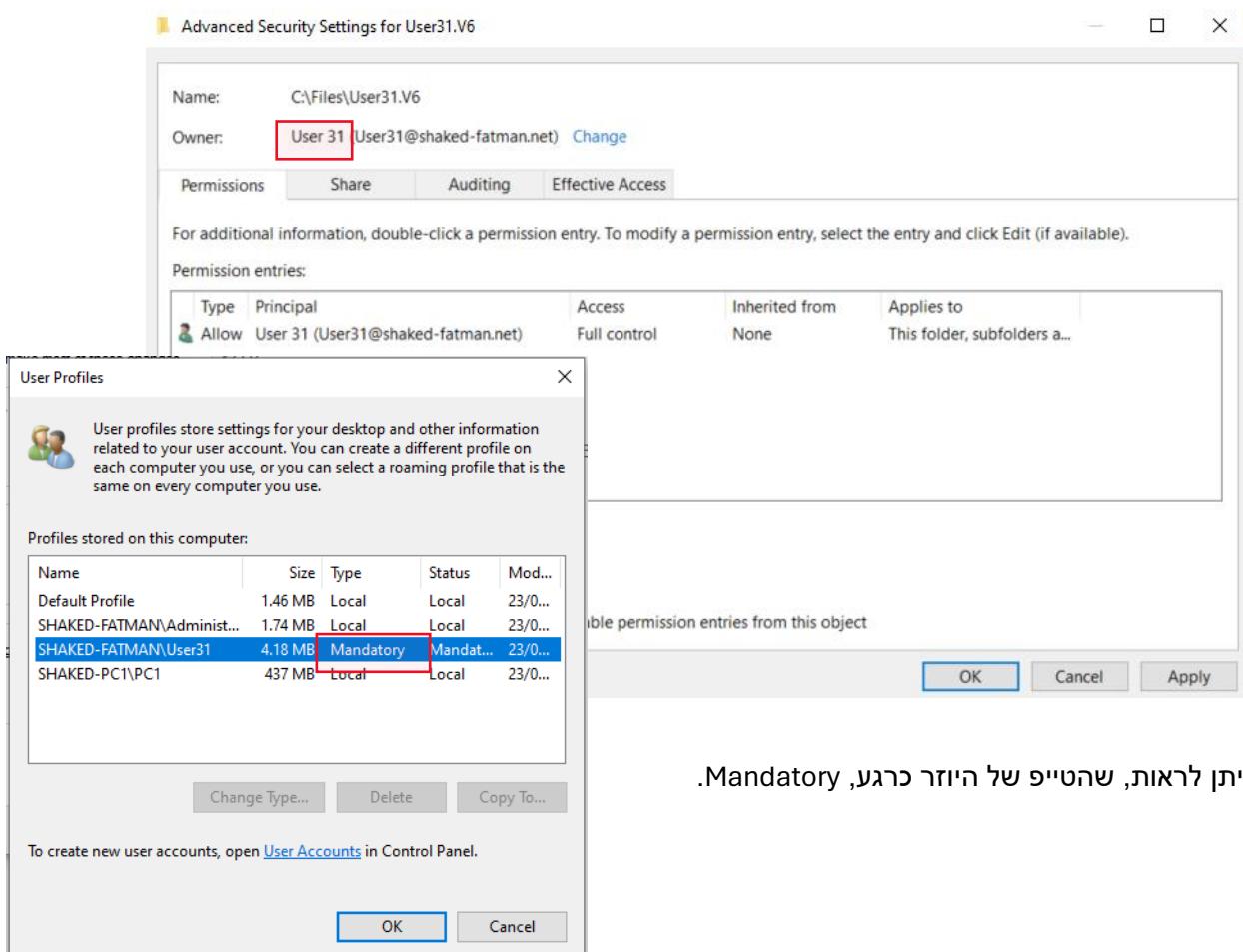


cutת נונה מנוקודה DAT לנוקודה MAN

שינוי זה הופך את קובץ ה profiel ל קריאה בלבד, מה שאומר שהמשתמש לא יכול לבצע שינויים קבציים לקובץ זה.



נחזיר את ה בעלות ל USER ו נמחק גישות



. ניתן לראות, שהטיפ של היוזר כרגע, Mandatory.

הגדרת ניתוב ו- PAT

הגדרת סרבר 1 להיות נטב, ואפשר PAT

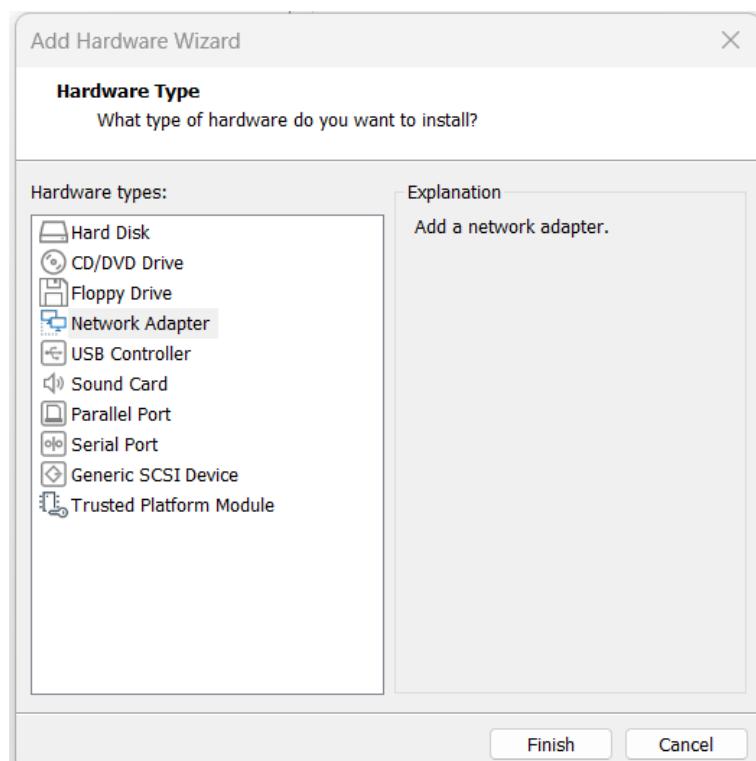
כאשר סרבר 1 יהיה נטב, הוא יהיה השרת, שמוסמך אותנו לרשות האינטרנט, PAT הוא קיצור של Port Address Translation. זו היא טכנולוגיה המאפשרת למחשבים שמחוברים לנטב להתחבר לרשות האינטרנט באמצעות כתובת IP אחת, הוא גם מתרגם כתובות IP פרטיות, לכתובות IP ציבוריות.

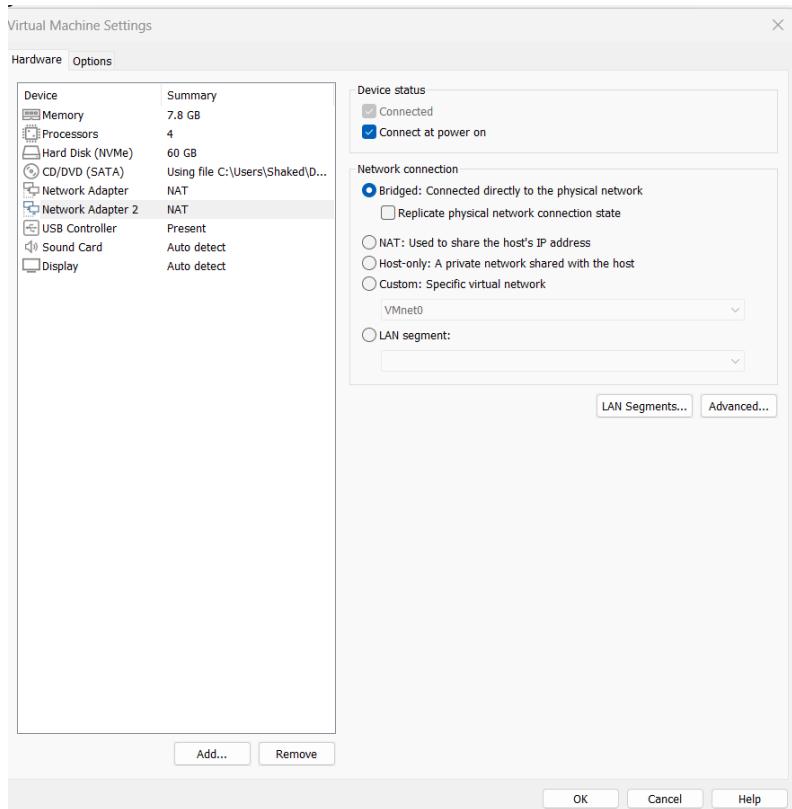
הגדרת ניתוב ו- PAT

- הגדר את SRV1 להיות נטב ואפשר לו לבצע PAT.
- בדיקת קישוריות לאינטרנט – וודא שכל המחשבים גולשים באינטרנט.

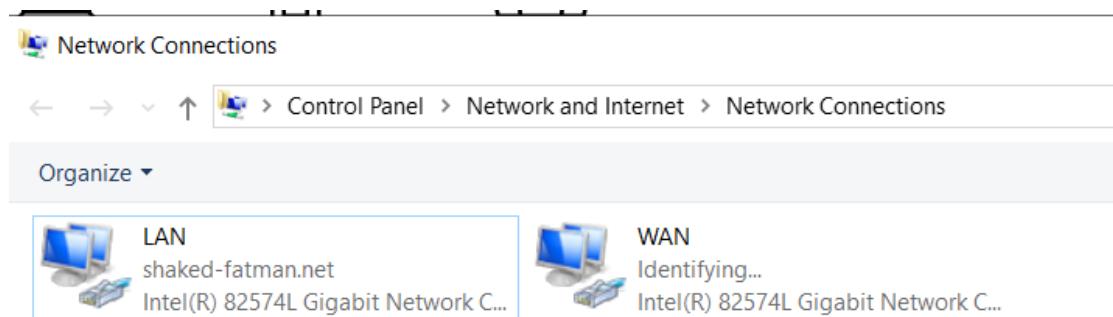
בשביל לאפשר את גלישת הרשת בסרבר 1, נדרש להווסף כרטיס רשת במערכת הווירטואלית, לצורך Bridged

להלן התהליך של הוספה כרטיס רשת





כעת ניתן לראות שיש לנו שתי רשתות על סרבר 1, שינוי שמות לטובת הנוחיות שלנו.



8.8.8.8 ש לנו כעת פינג שעבוד

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

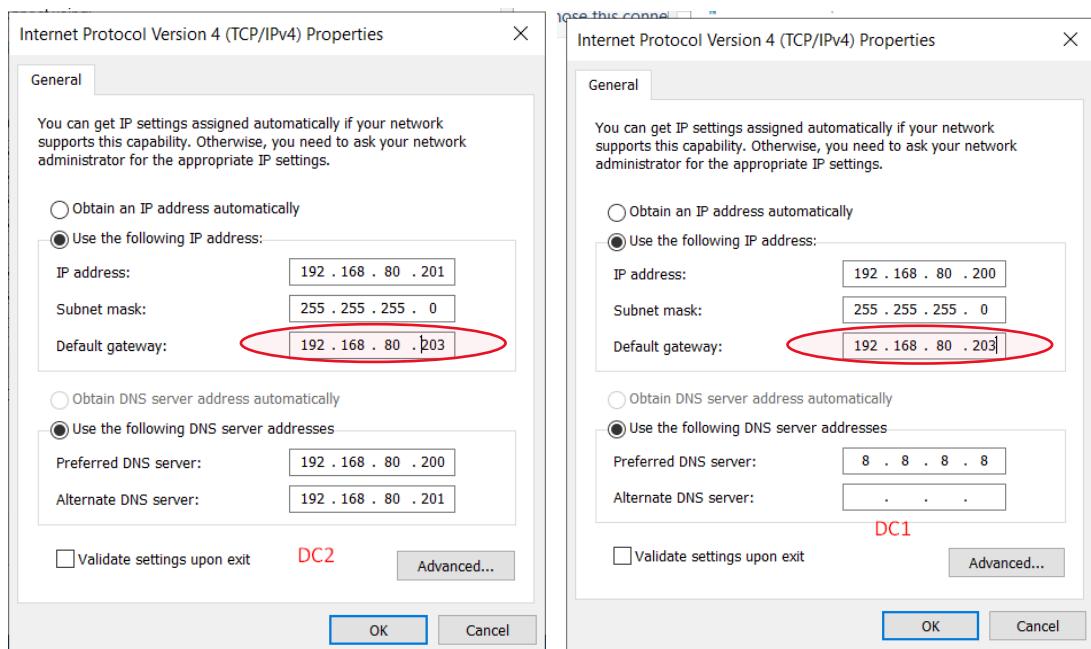
C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=6ms TTL=118
Reply from 8.8.8.8: bytes=32 time=4ms TTL=118
Reply from 8.8.8.8: bytes=32 time=6ms TTL=118
Reply from 8.8.8.8: bytes=32 time=5ms TTL=118

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 = 6ms, Average = 5ms

C:\Users\Administrator>
```

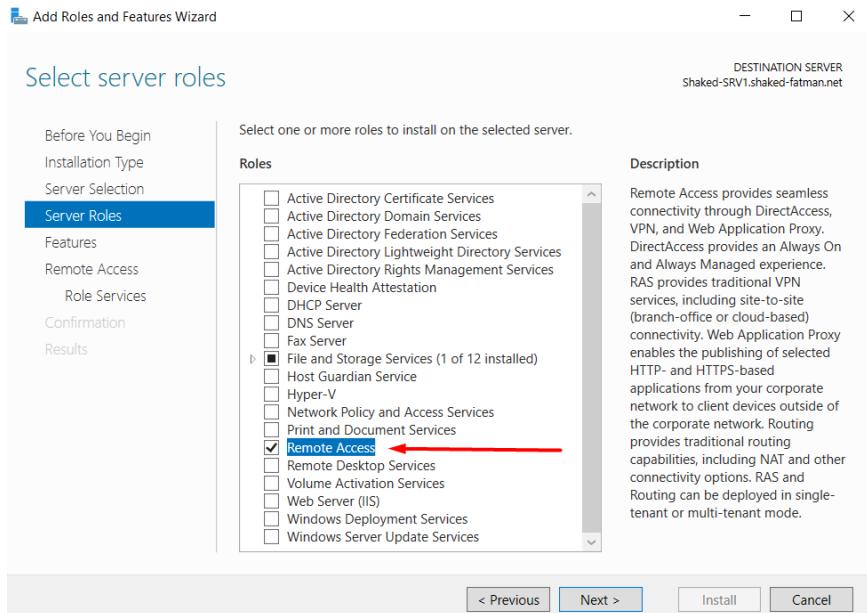
כעת נשנה בכל המחשבים את ה gateway אל סרבר 1, לאחר והוא הנטב שלנו.



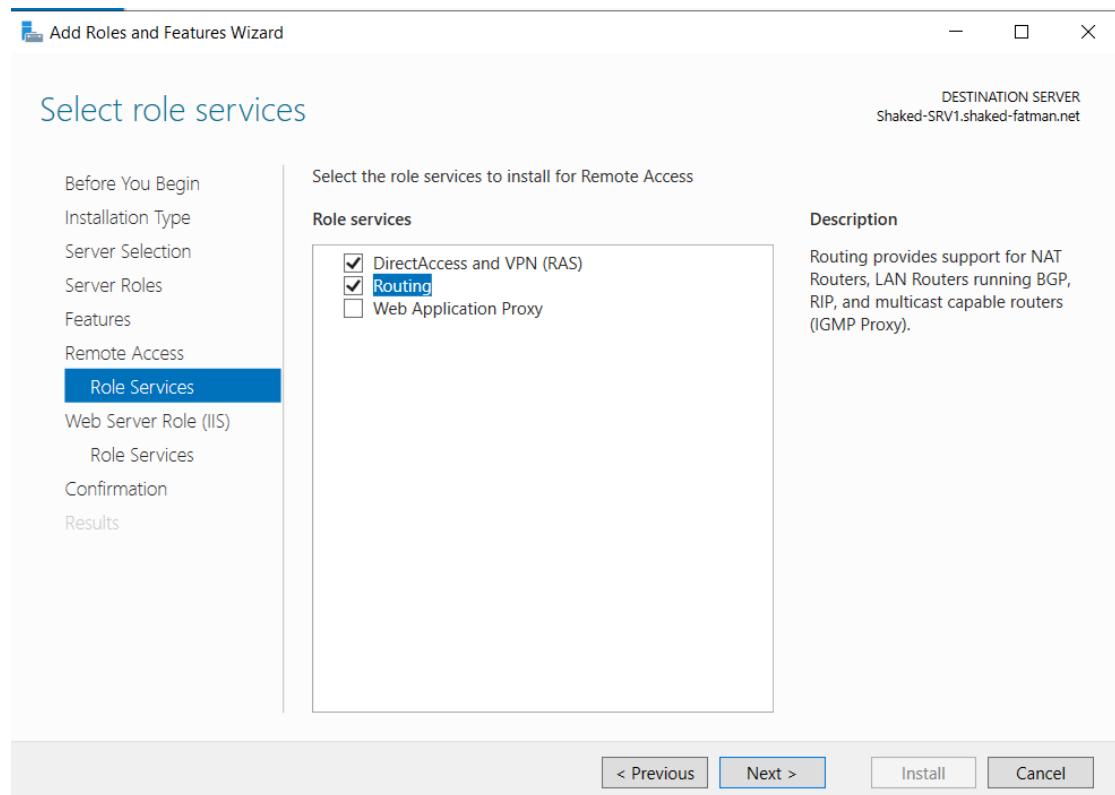
ונctrיך להפעיל Routing לסרב

מה שיאפשר לנו להיות נתב שלנו

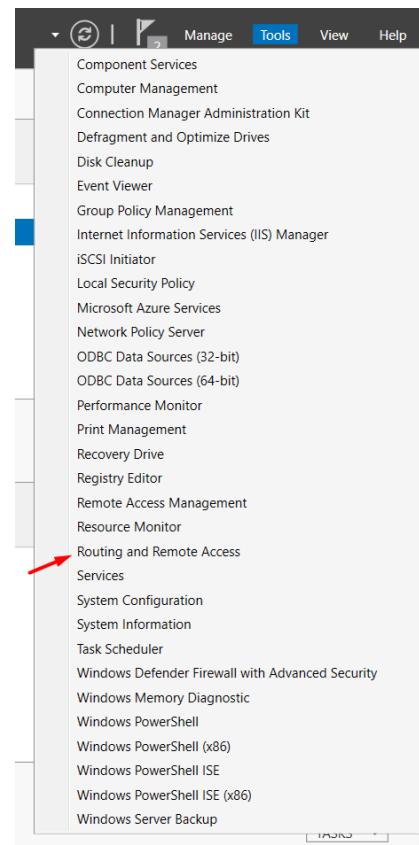
נוריד לסרב את Routing Access



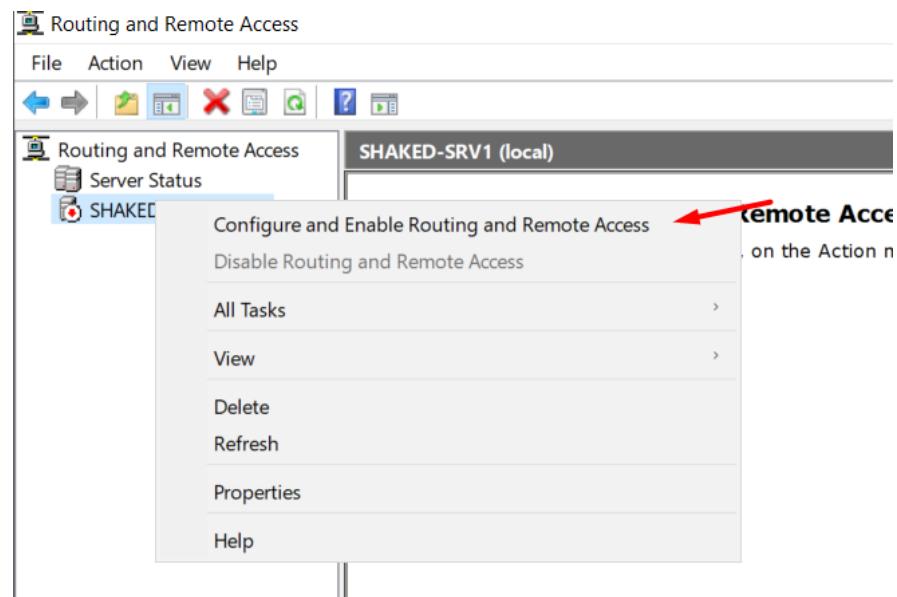
וריד Routing



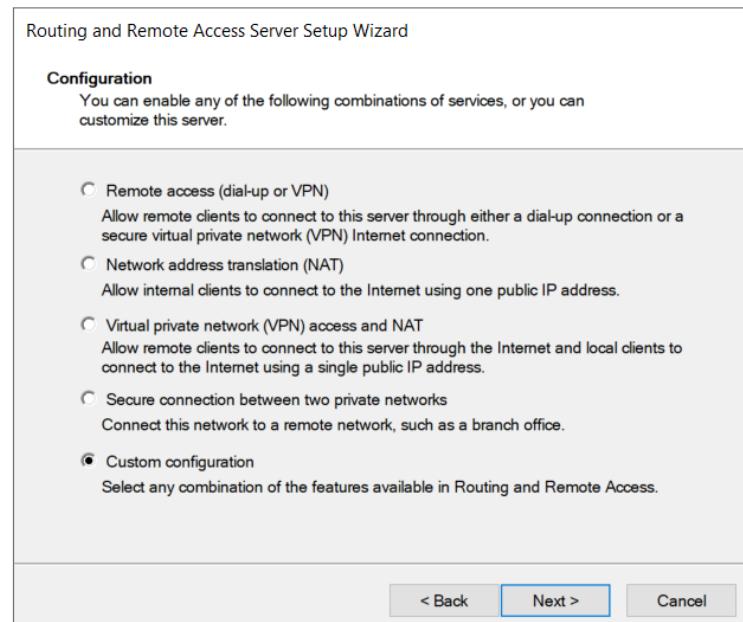
כעת נכנס ל- Routing and Remote Access



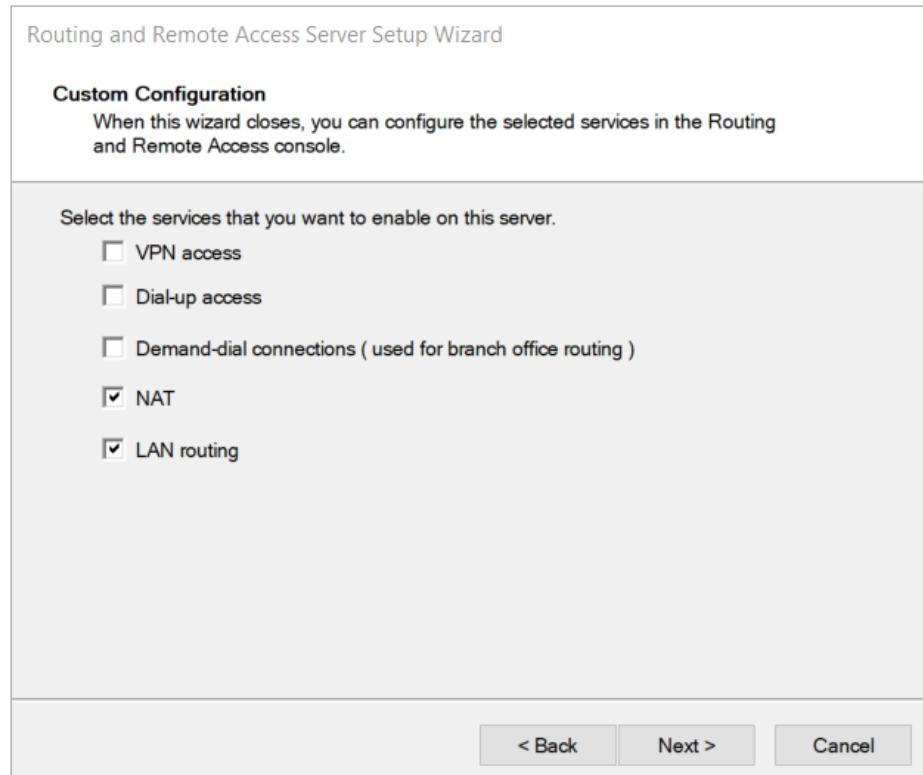
כעת נצטרך להפעיל לו Routing, מה שיפר容 את האופציה להיות הנתוב שלנו ברשות.



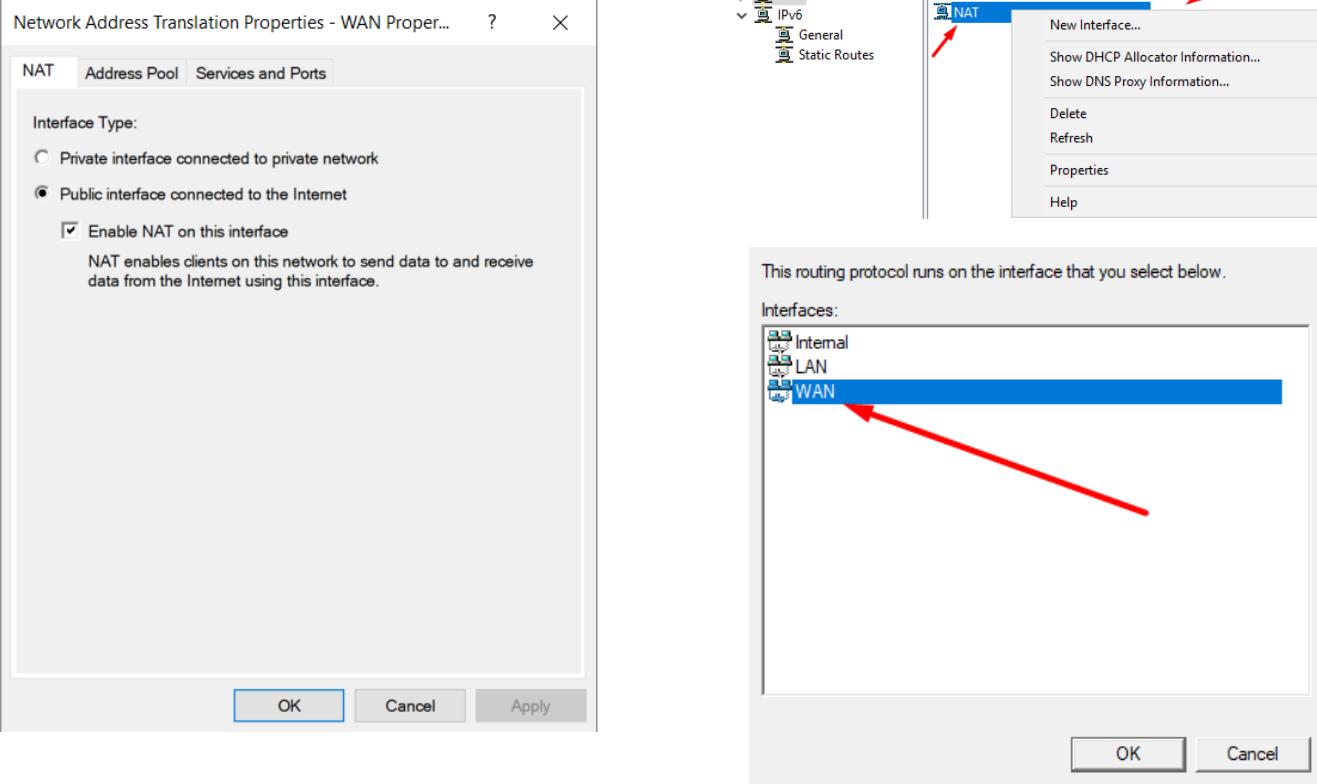
נבחר ב-custom



כעת נגדיר לו שאנו חונכו צריכים NAT



כעת נגדיר WAN כחדר NAT חדשה



כעת ניתן לראות שעובד הפינגים ב-DC

The screenshot displays three separate Windows Command Prompt windows, each showing the output of a ping command to the IP address 8.8.8.8. The results are color-coded to identify the source host:

- Top Window (DC2):** Shows ping results from a host named "SHAKED-FATMAN". The statistics show 0% loss with an average round trip time of 5ms.
- Middle Window (DC1):** Shows ping results from a host named "Administrator". The statistics show 0% loss with an average round trip time of 6ms.
- Bottom Window (PC1):** Shows ping results from a host named "Administrator". The statistics show 0% loss with an average round trip time of 6ms.

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

C:\Users\Administrator.SHAKED-FATMAN>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data: DC2
Reply from 8.8.8.8: bytes=32 time=5ms TTL=117
Reply from 8.8.8.8: bytes=32 time=5ms TTL=117
Reply from 8.8.8.8: bytes=32 time=6ms TTL=117
Reply from 8.8.8.8: bytes=32 time=6ms TTL=117

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 6ms, Average = 5ms

C:\Users\Administrator.SHAKED-FATMAN>

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=6ms TTL=117

Ping statistics for 8.8.8.8: DC1
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 6ms, Average = 6ms

Microsoft Windows [Version 10.0.19045.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 8.8.8.8

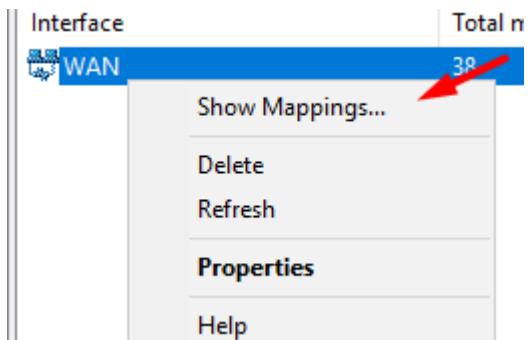
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=6ms TTL=117
Reply from 8.8.8.8: bytes=32 time=7ms TTL=117
Reply from 8.8.8.8: bytes=32 time=5ms TTL=117 PC1
Reply from 8.8.8.8: bytes=32 time=6ms TTL=117

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 7ms, Average = 6ms
```

בשביל PAT נוצר לשים זמנית ל`1cc`, בשביל לבדוק רק שעבוד, נשים DNS
8.8.8.8

Use the following DNS server addresses:
 Preferred DNS server: **8 . 8 . 8 . 8**
 יש לנו PAT!

וכנו לטבלת PAT



SHAKED-SRV1 - Network Address Translation Session Mapping Table

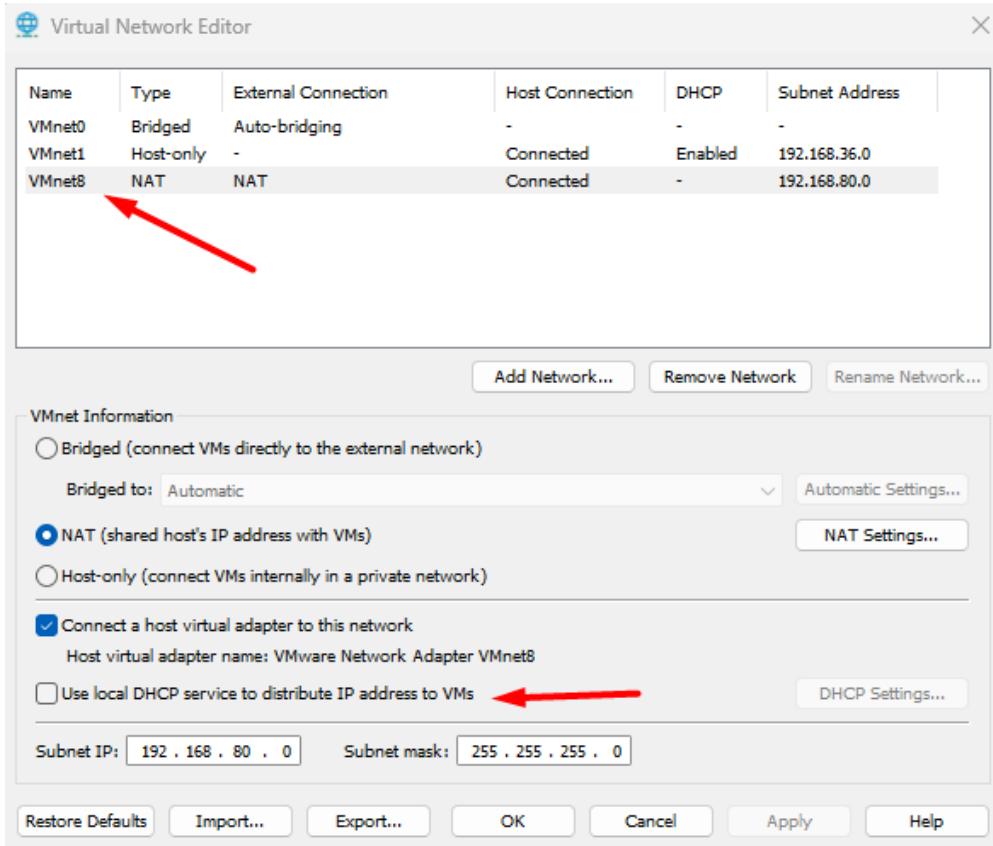
Protocol	Direction	Private address	Private port	Public Address	Public Port	Remote Address	Remote Port	Idle time
UDP	Outbound	192.168.80.202	58.261	10.100.102.162	62.919	8.8.8.8	53	30
UDP	Outbound	192.168.80.202	53.207	10.100.102.162	62.920	8.8.8.8	53	30
UDP	Outbound	192.168.80.202	59.268	10.100.102.162	62.921	8.8.8.8	53	29
UDP	Outbound	192.168.80.202	56.088	10.100.102.162	62.923	8.8.8.8	53	27
UDP	Outbound	192.168.80.202	53.567	10.100.102.162	62.927	142.251.37.68	443	10
UDP	Outbound	192.168.80.202	63.349	10.100.102.162	63.349	8.8.8.8	53	26
UDP	Outbound	192.168.80.202	50.734	10.100.102.162	62.929	142.251.37.67	443	10
UDP	Outbound	192.168.80.202	57.348	10.100.102.162	62.930	8.8.8.8	53	25
UDP	Outbound	192.168.80.202	52.783	10.100.102.162	62.932	8.8.8.8	53	24
UDP	Outbound	192.168.80.202	55.257	10.100.102.162	62.934	8.8.8.8	53	23
UDP	Outbound	192.168.80.202	64.239	10.100.102.162	64.239	8.8.8.8	53	23
UDP	Outbound	192.168.80.202	61.010	10.100.102.162	62.937	8.8.8.8	53	22
UDP	Outbound	192.168.80.202	64.939	10.100.102.162	62.938	8.8.8.8	53	17
UDP	Outbound	192.168.80.202	62.421	10.100.102.162	62.939	8.8.8.8	53	17
UDP	Outbound	192.168.80.202	51.919	10.100.102.162	62.940	8.8.8.8	53	17
UDP	Outbound	192.168.80.202	54.757	10.100.102.162	62.941	8.8.8.8	53	16
UDP	Outbound	192.168.80.202	60.343	10.100.102.162	62.943	8.8.8.8	53	13
UDP	Outbound	192.168.80.202	61.699	10.100.102.162	62.945	8.8.8.8	53	13
UDP	Outbound	192.168.80.202	57.385	10.100.102.162	62.947	8.8.8.8	53	13
UDP	Outbound	192.168.80.202	58.477	10.100.102.162	62.948	8.8.8.8	53	13
UDP	Outbound	192.168.80.202	50.565	10.100.102.162	62.952	8.8.8.8	53	12
UDP	Outbound	192.168.80.202	60.178	10.100.102.162	62.954	8.8.8.8	53	12
UDP	Outbound	192.168.80.202	52.241	10.100.102.162	62.956	8.8.8.8	53	12
UDP	Outbound	192.168.80.202	60.671	10.100.102.162	62.957	8.8.8.8	53	11
UDP	Outbound	192.168.80.202	58.888	10.100.102.162	62.960	8.8.8.8	53	10
UDP	Outbound	192.168.80.202	59.500	10.100.102.162	62.962	8.8.8.8	53	10
UDP	Outbound	192.168.80.202	61.124	10.100.102.162	62.964	8.8.8.8	53	10
UDP	Outbound	192.168.80.202	52.154	10.100.102.162	62.966	8.8.8.8	53	9
UDP	Outbound	192.168.80.202	59.334	10.100.102.162	62.968	8.8.8.8	53	9
UDP	Outbound	192.168.80.202	52.884	10.100.102.162	62.970	8.8.8.8	53	7
UDP	Outbound	192.168.80.202	54.706	10.100.102.162	62.977	8.8.8.8	53	5
UDP	Outbound	192.168.80.202	58.636	10.100.102.162	62.980	8.8.8.8	53	5
UDP	Outbound	192.168.80.202	54.986	10.100.102.162	62.981	8.8.8.8	53	5

הגדרת DHCP Server

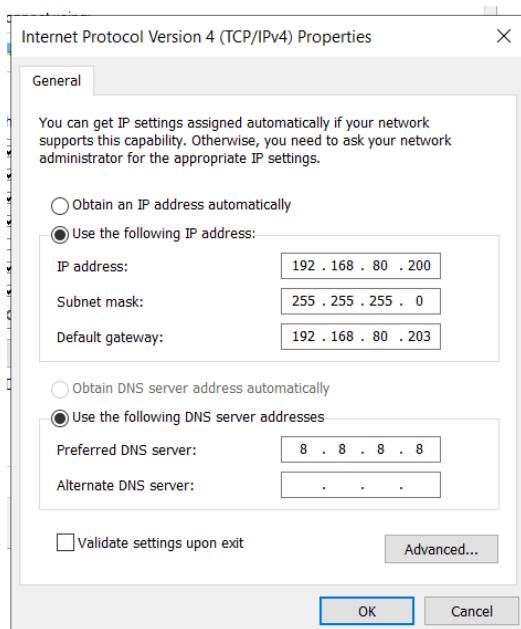
- מתן כתובת IP קבועה ל-DC1 והתקנת DHCP SERVER עליו.
- תנן ל-DC1 כתובת IP קבועה והתקן עליו שירות DHCP.

בחלק זה נתקין DHCP, זה המלצר של הרשתות. הוא ממלצר לכולם כתובת IP לפני שנתיחיל נctrar לCBCOT את DHCP של VMWARE.

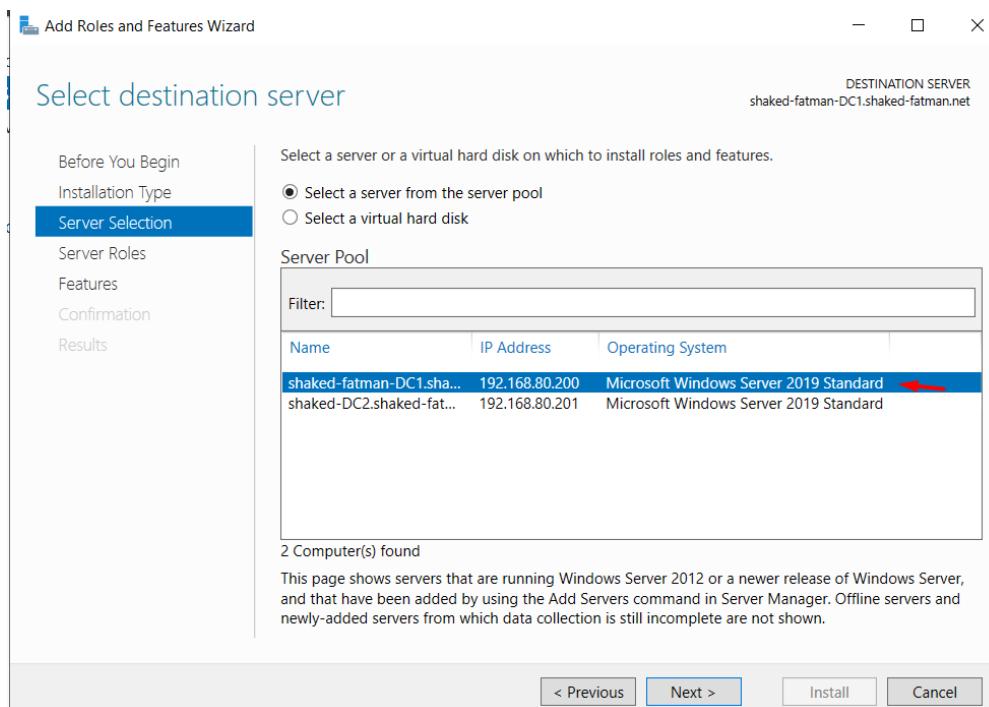
ניגש לחלונית "Edit", בתוכנת שארט, ומלחץ על הבחירה בשם "Virtual Network Editor".



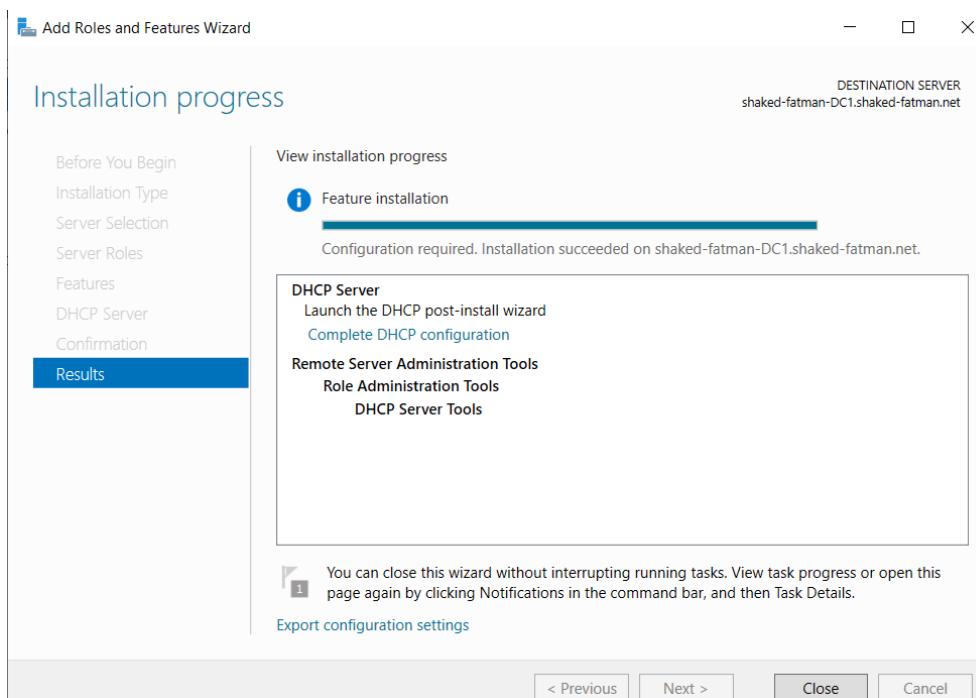
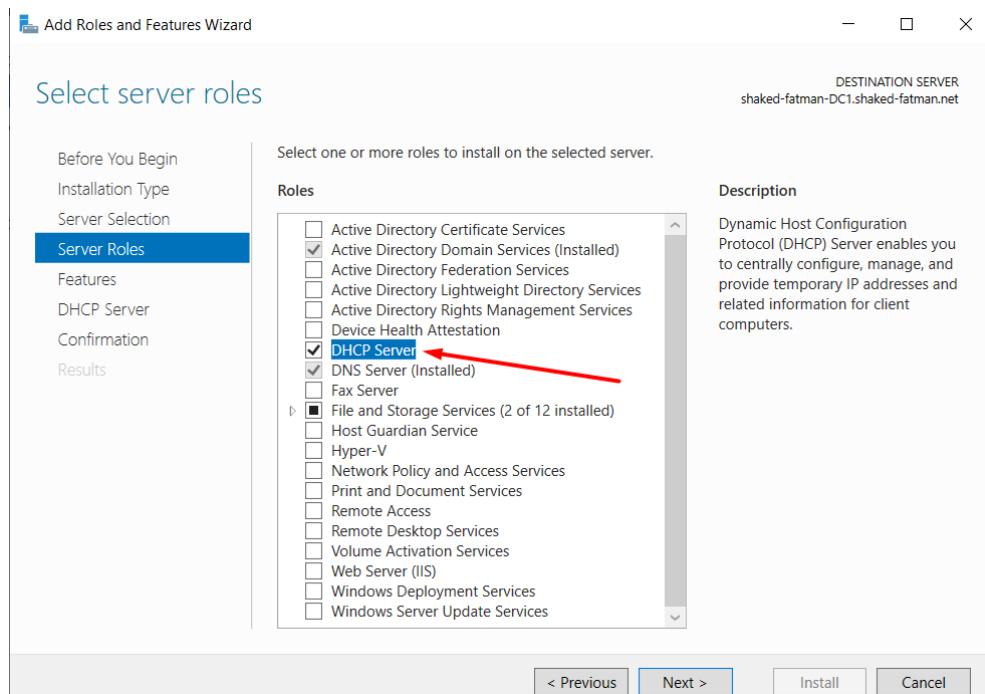
ויריאנו של dc כתובות קבועה



כעת נתקין שרת DHCP Role



נمشיך בהתקנה



הגדרת DHCP SCOPE

טווח DHCP הוא קבוצה של כתובות IP שנitin "להעניק" למחשבים ברשת מקומית

הגדיר Scope שמחلك 50 כתובות.

New Scope Wizard

נקרא לאם Scope טווח של כהה

Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: 

Description:

< Back **Next >** Cancel

New Scope Wizard

ונתן לאם Scope טווח של 50 כתובות

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.



Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:
End IP address:

Configuration settings that propagate to DHCP Client

Length:
Subnet mask:

< Back **Next >** Cancel

הגדרת החרגות בטווח DHCP

- **הגדר Address Exclusions של חמיש כתובות ראשונות מtower ה-Scope.**

החרגות כתובת, זה כביכול תחילה של סינון כתובות, פה אנחנו אומרים לו, "את החמש כתובות הראשונות, אל תתן לאף אחד, תשמור אותם לעצמך!".

נתנו חמיש כתובות ראשונות עם החרגות מtower Scope

New Scope Wizard

Add Exclusions and Delay

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

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

Start IP address: End IP address:

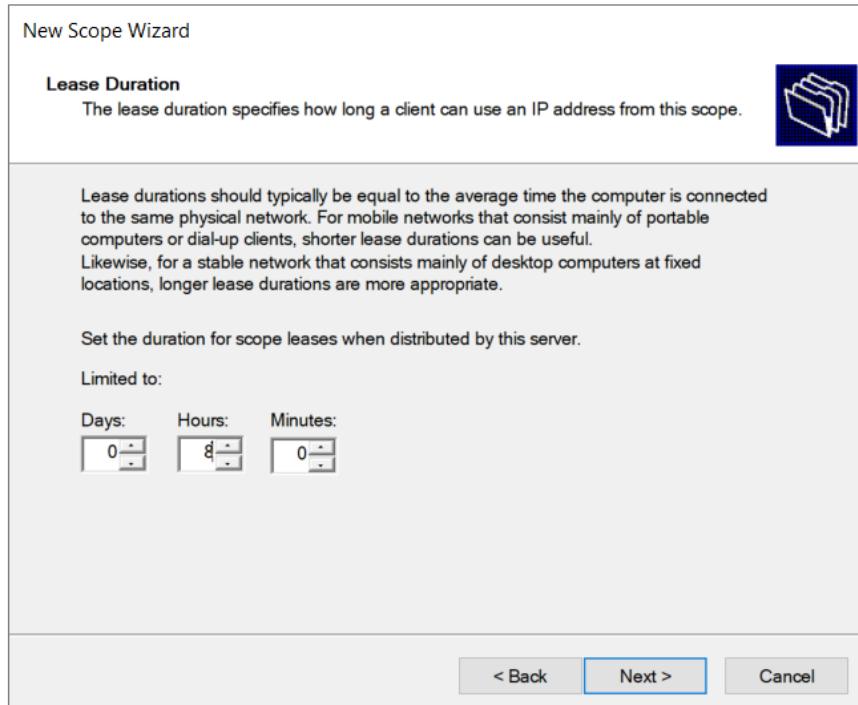
Excluded address range:
192.168.80.100 to 192.168.80.105

Remove

Subnet delay in milli second:
0

< Back Next > Cancel

הגדרת תוקף לכל כתובות בטווח



הגדיר Lease של 8 שעות.

ניתן לכל כתובות 8 שעות, כביכול
משכירים כתובות ברשות למשך גג 8
שעות.

נבדק שהכל עובד ב-PC

```
Administrator: C:\Windows\system32\cmd.exe
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : shaked-fatman.net
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address . . . . . : 00-0C-29-AF-98-4B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8355:2296:8aba:1af8%3(PREFERRED)
IPv4 Address. . . . . : 192.168.80.106(PREFERRED) ←
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, 23 January 2024 22:16:36
Lease Expires . . . . . : Wednesday, 24 January 2024 6:16:35
Default Gateway . . . . . :
DHCP Server . . . . . : 192.168.80.200
DHCPv6 IID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-41-6F-66-00-0C-29-AF-98-4B
DNS Servers . . . . . : 192.168.80.200
                                         192.168.80.201
NetBIOS over Tcpip. . . . . : Enabled

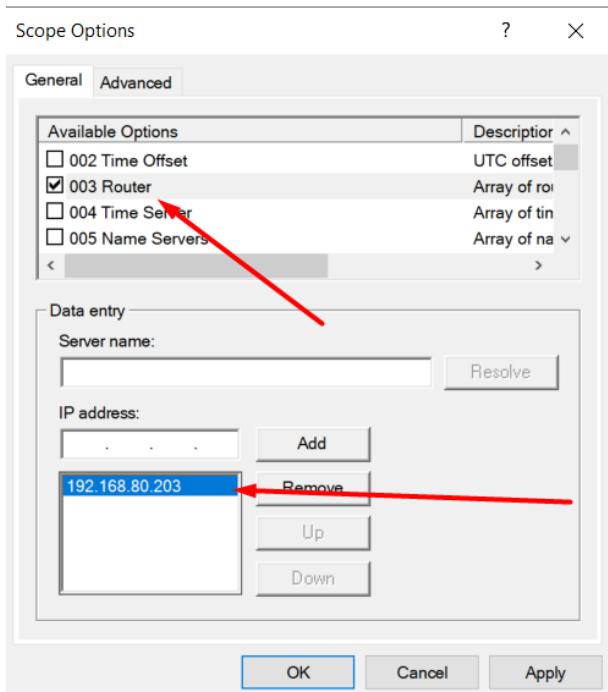
Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : E0-2E-0B-D2-2C-5F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

C:\Users\Administrator>
```

הגדרת רוטר, בהגדירות טווח של DHCP

- הגדיר DHCP Options לחולקת DNS (שהוא Router) | suffix (SRV1) על שם הדומיין.
- בדיקה קישוריות - בדוק ש- WIN10 מקבל IP בצורה אוטומטית מהשרת DHCP ובודק שיש Ping בין כל המחשבים. בדוק שניתן לבצע Ping מ- SRV1 לאינטרנט.

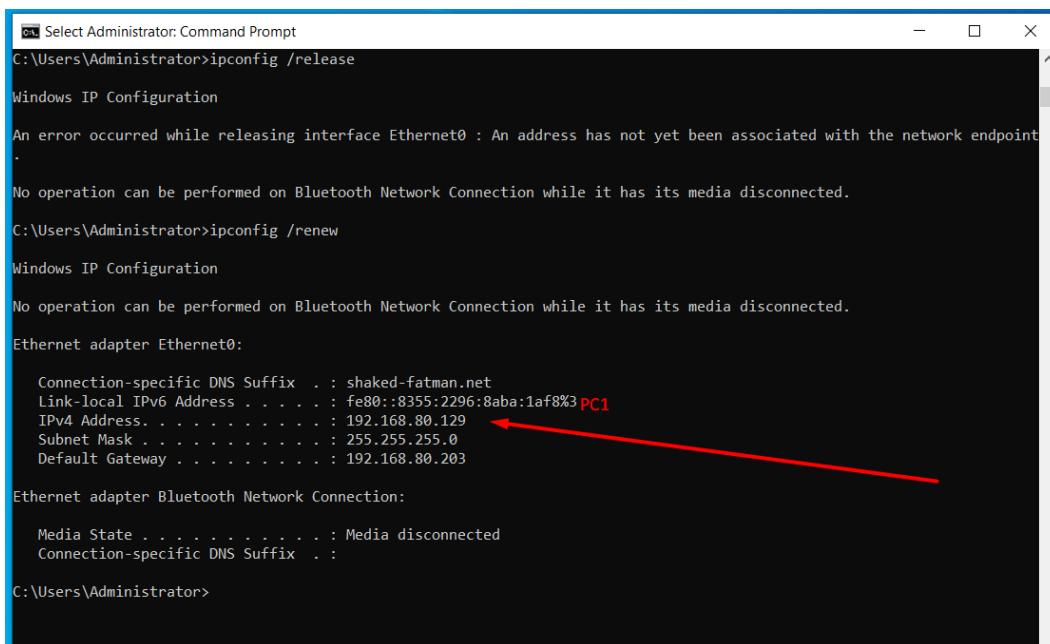


כעת נגדיר בפאות Router, שהוואר שלנו זה SRV1

נראה שיש חלוקת DNS וSuffix על שם ה-Domain

006 DNS Servers	Standard	192.168.80.200	None
015 DNS Domain Name	Standard	shaked-fatman.net	None

הפעלת DHCP על PC1, ועובד, ניתן לראות שעובד, לאחר שיש את ה gateway שרצינו שהוא



```
C:\Users\Administrator>ipconfig /release

Windows IP Configuration

An error occurred while releasing interface Ethernet0 : An address has not yet been associated with the network endpoint
.

No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

C:\Users\Administrator>ipconfig /renew

Windows IP Configuration

No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : shaked-fatman.net
Link-local IPv6 Address . . . . . : fe80::8355:2296:8aba:1af8%3 PC1
IPv4 Address . . . . . : 192.168.80.129
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.80.203

Ethernet adapter Bluetooth Network Connection:

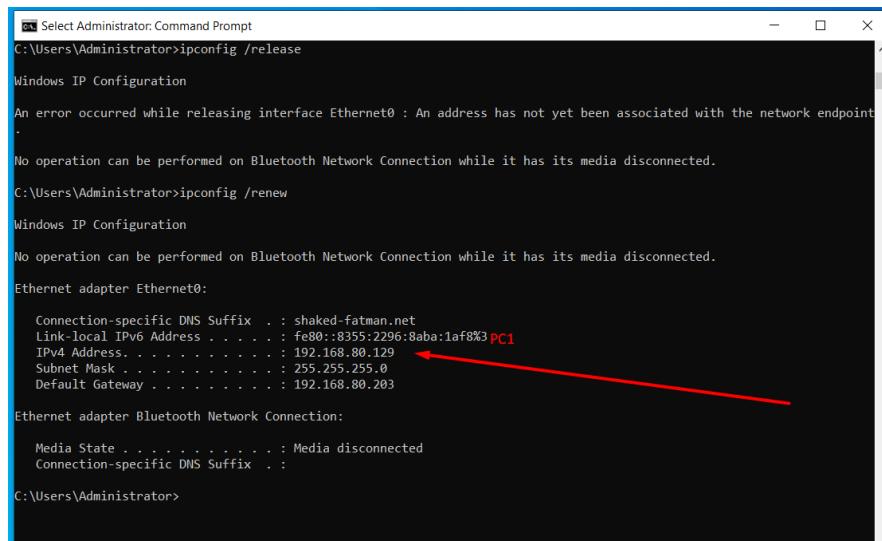
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\Administrator>
```

בדיקות קישוריות

בדיקת קישוריות - בדוק ש-WIN10 מקבל IP בצורה אוטומטית מהשרת DHCP ובודק שיש Ping בין כל המחשבים. בדוק שניתן לבצע Ping מ-SRV1 לאינטראנט.

כמו שהראיתי קודם, PC1 מקבל כתובת DHCP



```
C:\Users\Administrator>ipconfig /release
C:\Users\Administrator>ipconfig /renew
Windows IP Configuration

An error occurred while releasing interface Ethernet0 : An address has not yet been associated with the network endpoint.

No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

C:\Users\Administrator>ipconfig /renew
Windows IP Configuration

No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet0:

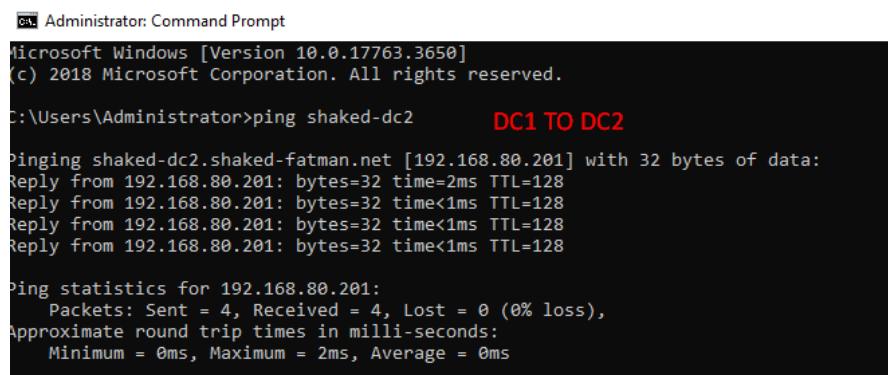
  Connection-specific DNS Suffix . : shaked-fatman.net
  Link-local IPv6 Address . . . . . : fe80::8355:2296:8aba:1af8%3
  IPv4 Address . . . . . : 192.168.80.129
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.80.203

Ethernet adapter Bluetooth Network Connection:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

C:\Users\Administrator>
```

נבדק果然 שהמחשבים עושים Ping אחד לשני

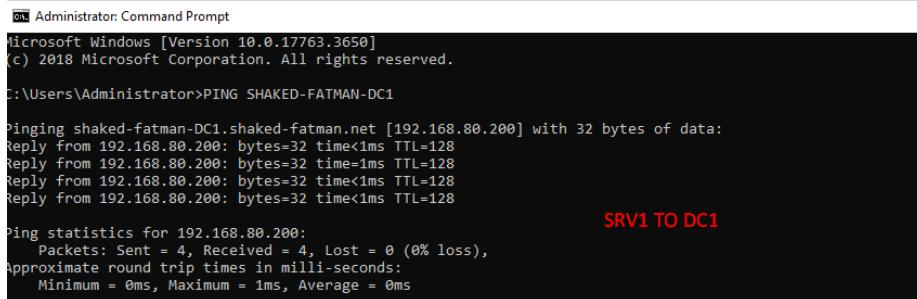


```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping shaked-dc2          DC1 TO DC2

Pinging shaked-dc2.shaked-fatman.net [192.168.80.201] with 32 bytes of data:
Reply from 192.168.80.201: bytes=32 time=2ms TTL=128
Reply from 192.168.80.201: bytes=32 time<1ms TTL=128
Reply from 192.168.80.201: bytes=32 time<1ms TTL=128
Reply from 192.168.80.201: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.80.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
```



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

C:\Users\Administrator>PING SHAKED-FATMAN-DC1

Pinging shaked-fatman-DC1.shaked-fatman.net [192.168.80.200] with 32 bytes of data:
Reply from 192.168.80.200: bytes=32 time<1ms TTL=128
Reply from 192.168.80.200: bytes=32 time=1ms TTL=128
Reply from 192.168.80.200: bytes=32 time<1ms TTL=128
Reply from 192.168.80.200: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.80.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

ניתן לראות שPC לא עושה פינג לשrv1

```
C:\Users\User3>ping shaked-srv1

Pinging shaked-srv1.shaked-fatman.net [192.168.80.203] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.80.203:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

בשביל שייעבוד, נצטרך לכבות את הפירול.

```
[Administrator: Windows PowerShell
Windows PowerShell
Copyright <C> Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
```

חומרת אש (Firewall) היא מערכת אבטחת רשות המנתרת ו管理办法 את תובורת הרשות הנכנסת והיצאת.

במקרה של PC1 ו-SRV1, חומרת האש חסמה את התקשרות בין שני המחשבים.

כאשר ביטלנו את חומרת האש, היא כבר לא חסמה את התקשרות בין שני המחשבים. לכן, הצלחנו לבצע פינג מ-PC1 לשrv1.

cut הping עובד

```
C:\Users\User3>ping shaked-srv1

Pinging shaked-srv1.shaked-fatman.net [192.168.80.203] with 32 bytes of data:
Reply from 192.168.80.203: bytes=32 time<1ms TTL=128
Reply from 192.168.80.203: bytes=32 time<1ms TTL=128
Reply from 192.168.80.203: bytes=32 time=2ms TTL=128
Reply from 192.168.80.203: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.80.203:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

פינג מ2cp לוינדי 10

```
Administrator: Command Prompt
C:\Users\Administrator.SHAKED-FATMAN>ping 192.168.80.129

Pinging 192.168.80.129 with 32 bytes of data:
Reply from 192.168.80.129: bytes=32 time=1ms TTL=128
Reply from 192.168.80.129: bytes=32 time<1ms TTL=128
Reply from 192.168.80.129: bytes=32 time=1ms TTL=128
Reply from 192.168.80.129: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.80.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

cut נבצע פינג מ1cp לרשת האינטרנט, וניתן לראות, שאנו חנו מקבלים תגובה בחזרה.

```
SRV1-Project >
Administrator: Command Prompt
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=5ms TTL=118
Reply from 8.8.8.8: bytes=32 time=5ms TTL=118
Reply from 8.8.8.8: bytes=32 time=4ms TTL=118
Reply from 8.8.8.8: bytes=32 time=5ms TTL=118

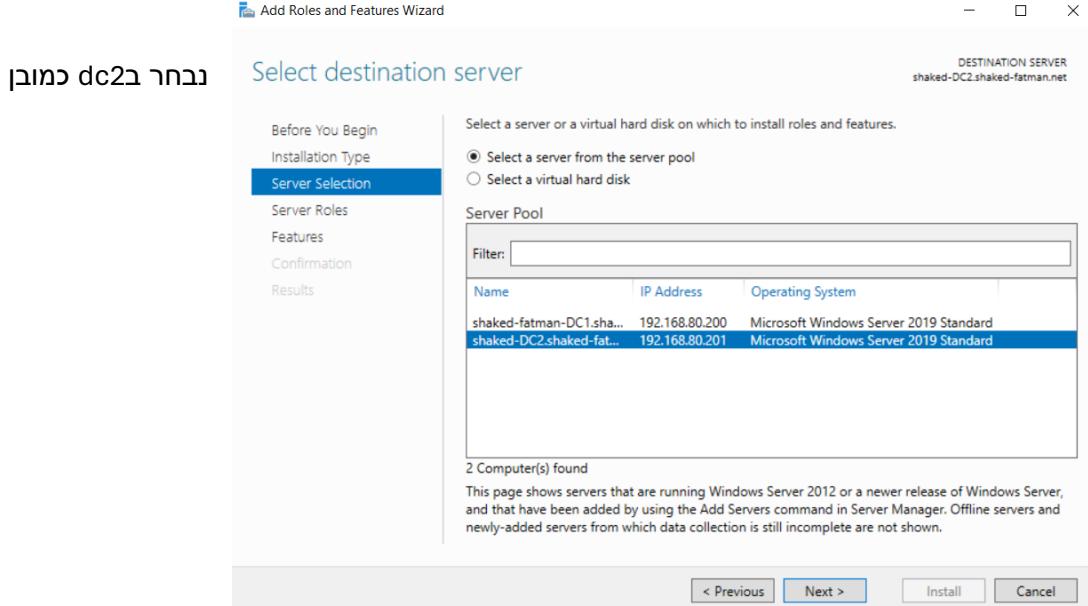
Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms
```

יצירת Failover Cluster

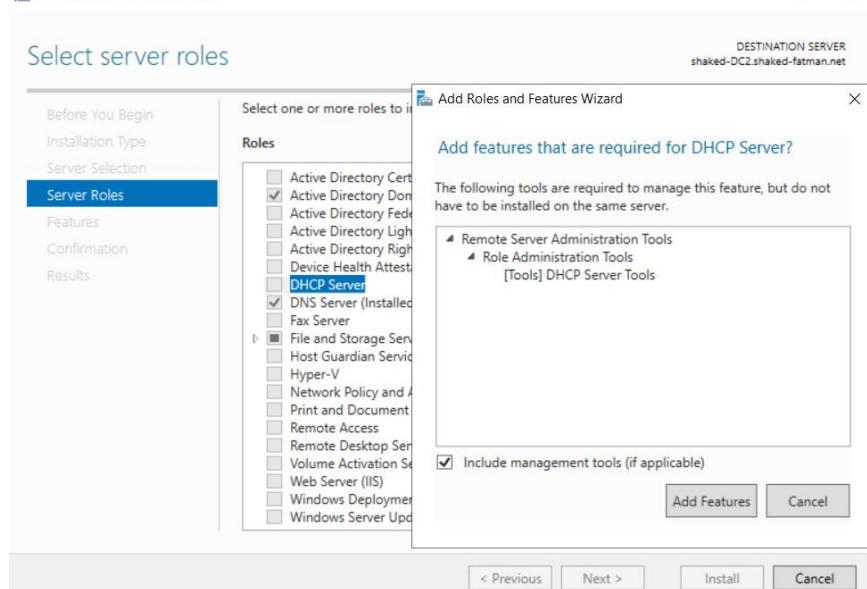
▪ צור ראשוןFailover cluster עם שרת DC2 (ניתן לבטל את הפעולה לאחר סיום ההגדרה במידה ויש צורך)

דבר ראשון נבון מה זה אומר, Failover Cluster זה קבוצה של שני או יותר שרתים המוחברים יחד כדי ליזור מערכת זמינה תמיד.

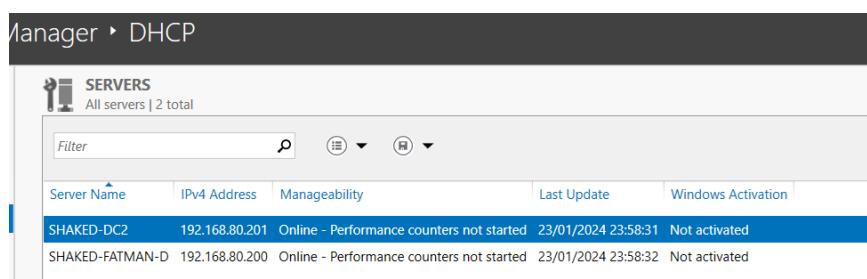
از נדרש להתקין DHCP על שרת DC2

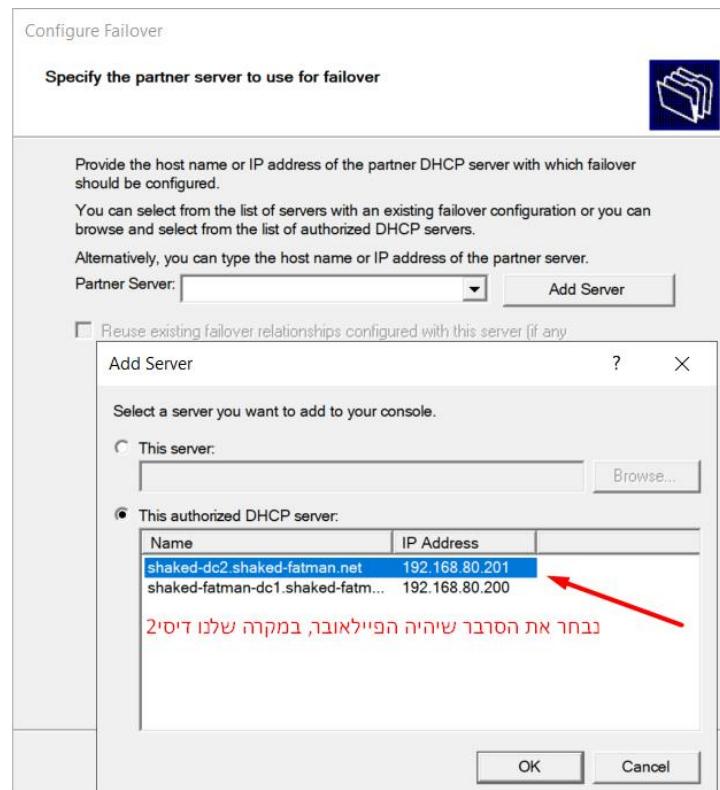
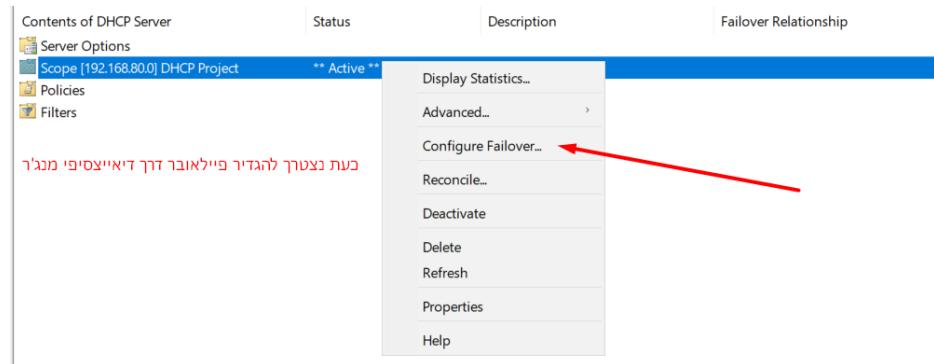


ונהפוך אותו לשרת DHCP

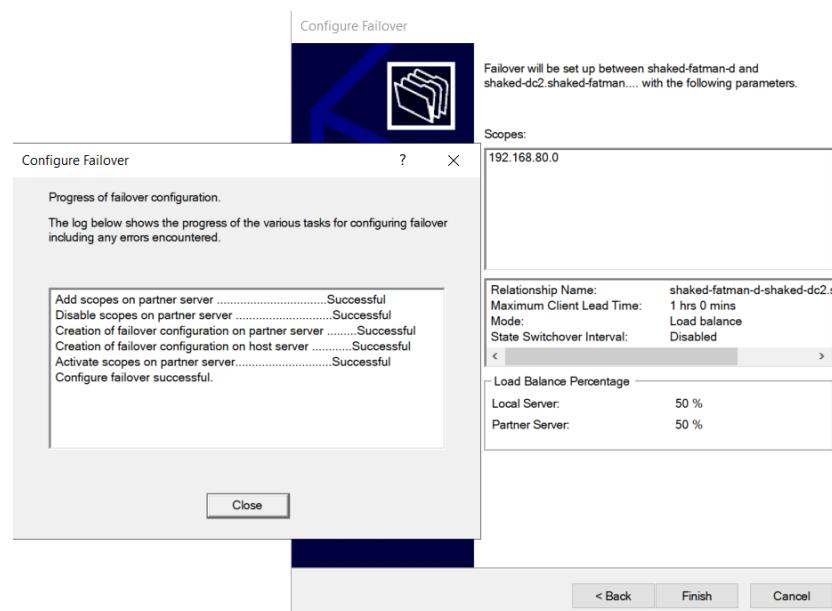


וכעת נראה גם את DHCP ב DC2





הצלחנו לעשות FailOver, עכשו במקרה
וגם במקרה/dc1 יהיה
מכובה, בכל אופן יהיה לנו
עוד שרת DHCP, ובראゴן
תמיד יהיה שירות כתובות
!.IP



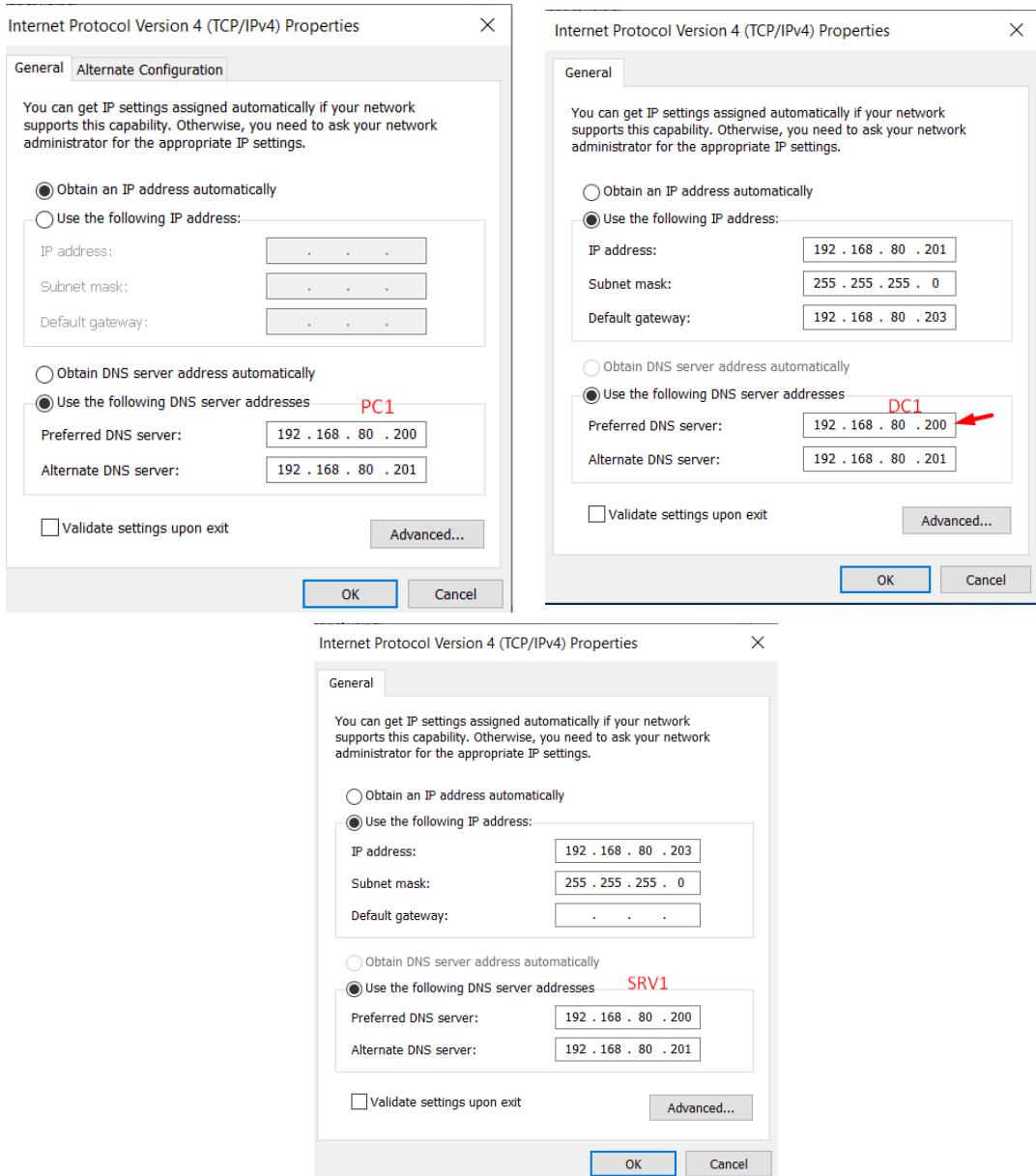
הגדרת DNS Server

DNS, בעצם יתרגם מכתובת במלילים, למספרים, כמו אני קשור, אתה לא תזכור מספר טלפון של אדם מסוים, תכתוב את השם שלו באני קשור לך, ותגיע אליו, אותו דבר DNS.

ויזואו שכל המחשבים מוגדרים להשתמש במקרה של DC1

ויזואו שכל המחשבים מוגדרים להשתמש ב- DC1 של DNS.

כעת נזודן שכל המחשבים ברשות שלנו מוגדרים להשתמש DNS של DC1, ואם לא, אז נשנה

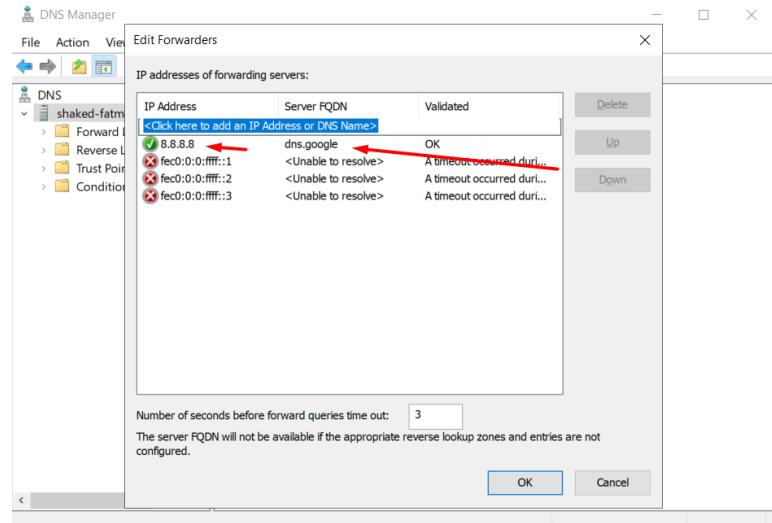


לאחר שווידאנו שאנו משתמשים בDNS של DC1, נוכל לעבור לשלב הבא

הגדרת מעבר לשרת DNS חיצוני

כעת, כאשר שרת DNS יקבל שאלתה שאין לו תשובה עליה, הוא יפנה לשרת DNS שנמצא בכתובת 8.8.8.8

הגדר Forwarding לשרת DNS חיצוני (8.8.8.8)

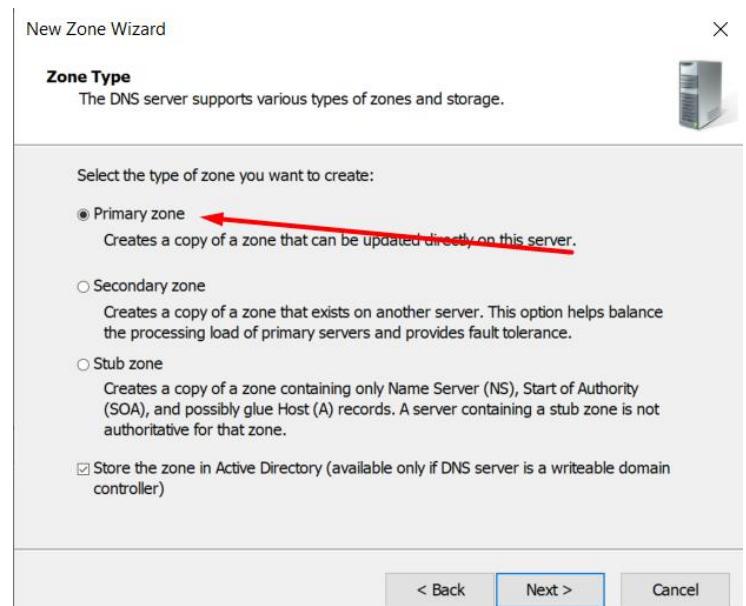
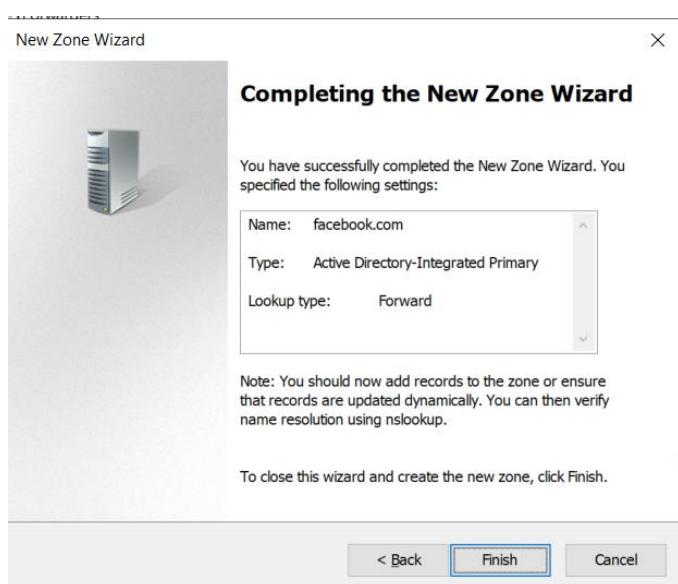


הגדרנו העברה
לשרת 8.8.8.8

חסימת אתר Facebook בארגון

הגדיר **Primary Zone** או **Conditional Forwarders** במתירה למנוע מהעובדים לגלוש **facebook.com** במהלך ים העבודה.

בוצע כעת חסימה לגילישה באתר Facebook



לאחר שפתחנו זונ, לא יעבוד לנו יותר.



מה שעשינופה, פתחנו בעצם Zone לאתר Facebook, אך לא הגדרנו NameServers, ולא הגדרנו בכלל כלום, מה שגורם למצב, שברגע שמנוטים לפנות לכתובת של Facebook, אנחנו מקבלים Error

- ויזדוא שווינטוס 10 קלינט שלנו, יכול לתרגם את הכתובת של גוגל, בעזרת NSLOOKUP
- הכנס ל-WIN10 והשתמש ב-nslookup כדי לוודא שהשרת מצליח לתרגם את הכתובות google.com

השרת הצליח לתרגם את הכתובת של גוגל בעזרת Nslookup

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

C:\Users\Administrator>NSLOOKUP GOOGLE.COM
Server: UnKnown
Address: 192.168.80.200

Non-authoritative answer:
Name: GOOGLE.COM
Addresses: 2a00:1450:4028:803::200e
           172.217.22.46
```

ביצעת את הפקודה "nslookup google.com" כדי לוודא שהשרת שלי יכול לתרגם את כתובת האתר של גוגל לכתובת IP.

התוצאות של הפקודה הראו שהשרת שלי מצליח לתרגם את הכתובת כראוי.

הגדרת Stub Zone

■ הגדר Stub Zone ל yahoo.com

ZONE DNS הוא עותק של STUB ZONE שבו יש רק את הרשומות הדרישות לייצירת קשר עם שרת DNS-הנ-גדר Yahoo, לכתובת של אתר yahoo.com.

נתיחיל מחייפוש Name Server

```
C:\Users\Administrator>nslookup
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

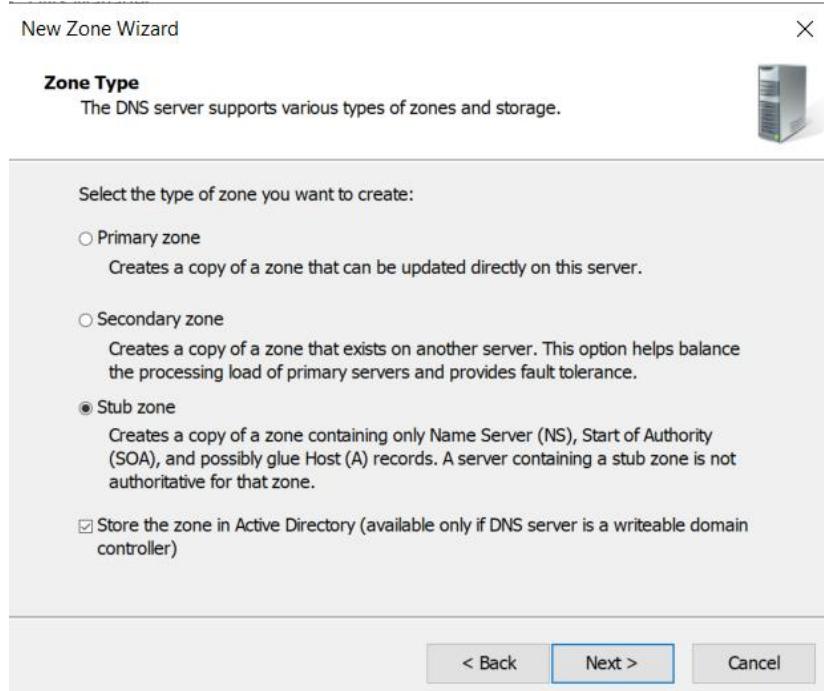
C:\Users\Administrator>nslookup
Default Server: UnKnown
Address: ::1

> 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 = ns5.yahoo.com
@yahoo.com      nameserver = ns1.yahoo.com
@yahoo.com      nameserver = ns3.yahoo.com

ns2.yahoo.com   internet address = 68.142.255.16
ns2.yahoo.com   AAAA IPv6 address = 2001:4998:1c0::7961:686f:6f21
ns4.yahoo.com   internet address = 98.138.11.157
ns5.yahoo.com   internet address = 202.165.97.53
ns5.yahoo.com   AAAA IPv6 address = 2406:2000:1d0::7961:686f:6f21
ns1.yahoo.com   internet address = 68.180.131.16
ns1.yahoo.com   AAAA IPv6 address = 2001:4998:1b0::7961:686f:6f21
ns3.yahoo.com   internet address = 27.123.42.42
ns3.yahoo.com   AAAA IPv6 address = 2406:8600:f03f:1f8::1003
>
```

לאחר שמצאנו את הנימם סרברס, ניצור סטאב זון חדש



The screenshot shows two windows side-by-side. On the left is the 'New Zone Wizard' in the 'DNS Manager' tool. It displays a list of 'Master DNS Servers' with one entry: 'ns1.yahoo.com' (IP 68.180.131.16). A red arrow points from the IP address in the list to the same IP address in the 'internet address' column of the nslookup command output on the right. On the right is a 'Command Prompt' window titled 'Administrator: Command Prompt - nslookup'. The command 'nslookup > yahoo.com' is run, and the output shows multiple entries for the 'yahoo.com' domain, including the master server 'ns1.yahoo.com' at IP 68.180.131.16.

IP Address	Server FQDN	Validated
<Click here to ... 68.180.131.16	ns1.yahoo.com	OK

```

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

C:\Users\Administrator>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 = ns5.yahoo.com
yahoo.com      nameserver = ns1.yahoo.com
yahoo.com      nameserver = ns3.yahoo.com

ns2.yahoo.com  internet address = 68.142.255.16
ns2.yahoo.com  AAAA IPv6 address = 2001:4998:1c0::7961:686f:6f21
ns4.yahoo.com  internet address = 98.138.11.157
ns4.yahoo.com  AAAA IPv6 address = 202.165.97.53
ns5.yahoo.com  internet address = 2406:2000:1d0::7961:686f:6f21
ns5.yahoo.com  AAAA IPv6 address = 68.180.131.16
ns1.yahoo.com  internet address = 2001:4998:1b0::7961:686f:6f21
ns1.yahoo.com  AAAA IPv6 address = 27.123.42.42
ns3.yahoo.com  internet address = 2406:8600:f03f:1f8::1003
>

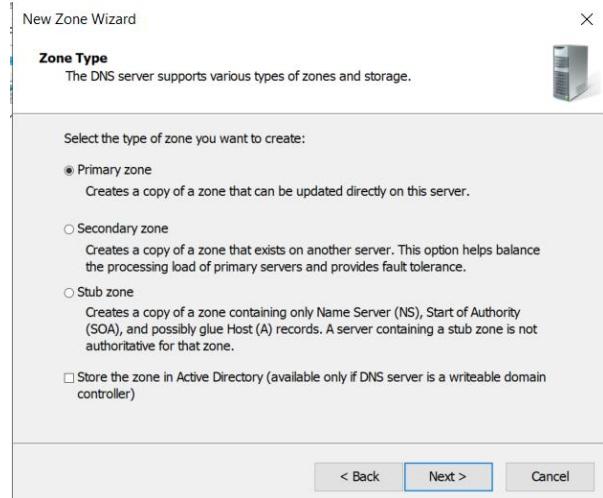
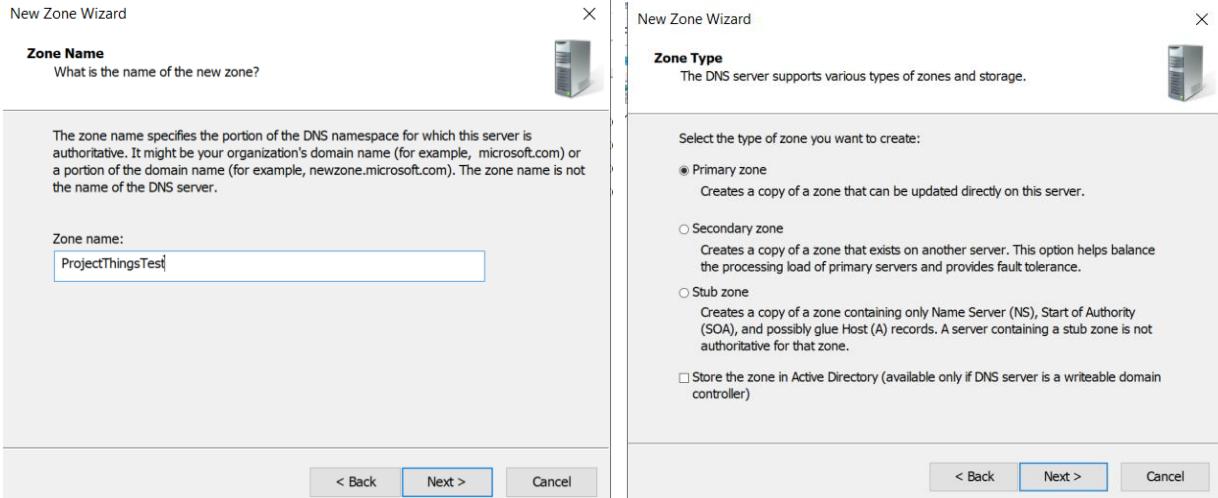
```

יצירת ZONE מסוג Primary, ולאחר מכן, ליצור Secondary Zone

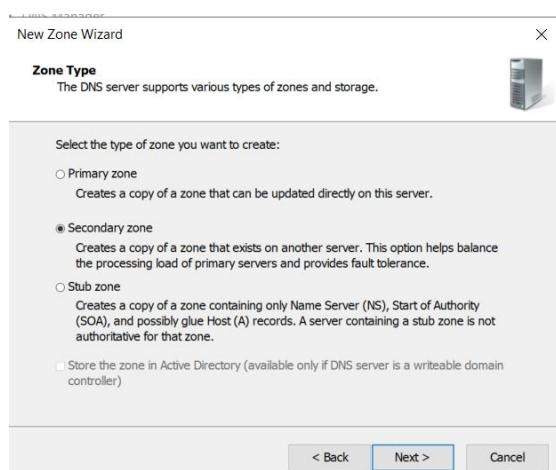
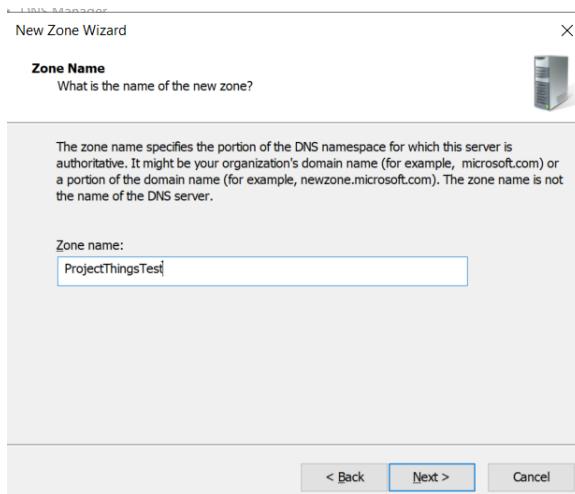
צור ZONE מסוג Primary – איזה שם שתרצה – צור לZONE זהה בשרת DC2

נתחיל בעצם ממערץ, שייהי בdc1

לහן השלבים

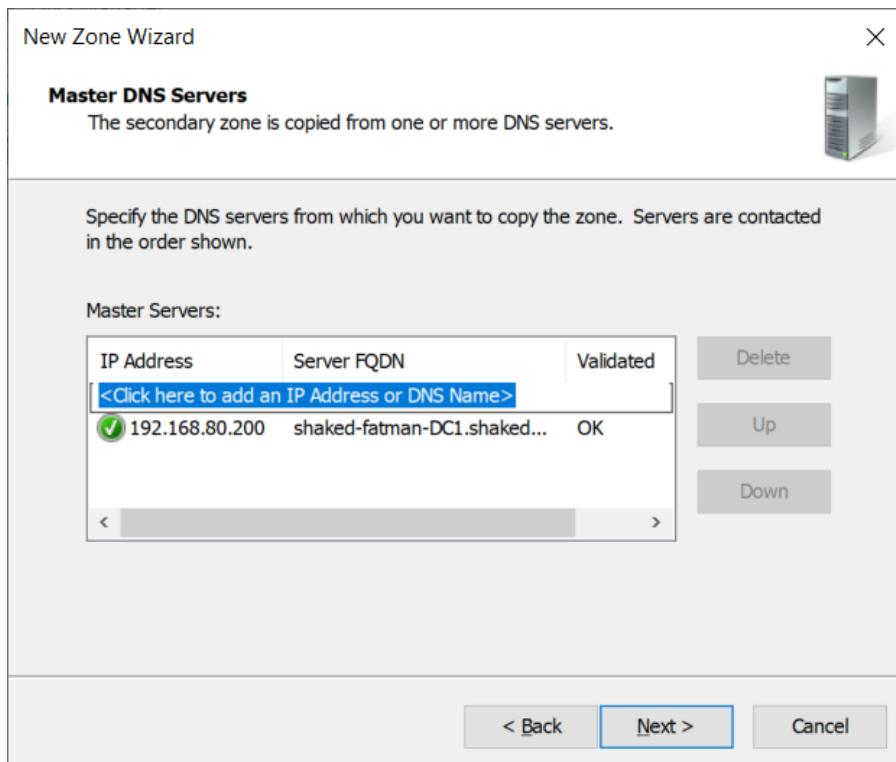


. לאחר שיצרנו Primary Zone בdc1, נלך/dc2, וניצור שם Secondary Zone

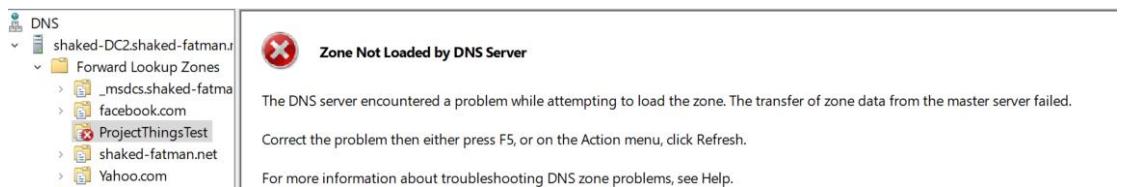


- הוא עותק של SERVER DNS של SERVER אחר. הוא משמש כדי לספק גיבוי ל-ZONE הראשית

כעת הוא שואל אותנו איפה zone, אז נגיד לו שהוא בdc1, בעזרה כתיבת כתובות האייפ' המוקומית שלו

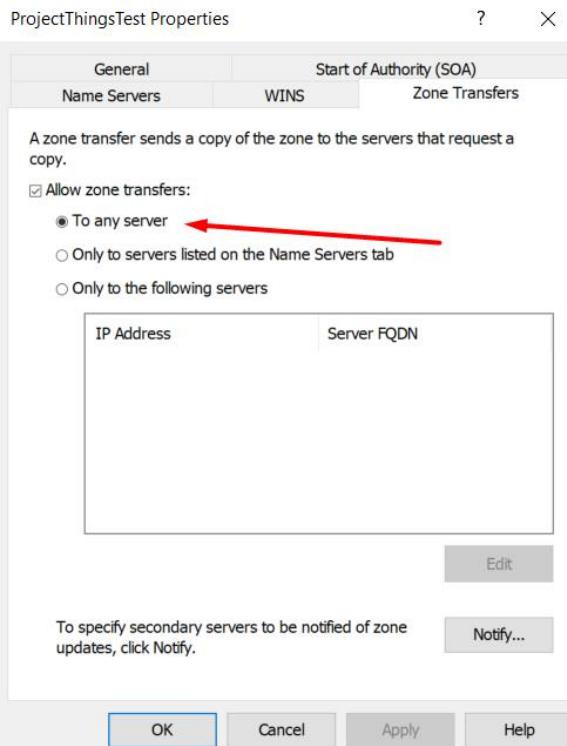


לאחר שנבצע נראה שיש שגיאה ושלא עובד, זה מאחר ולא אפשרנו לזמן לעבור לdc2

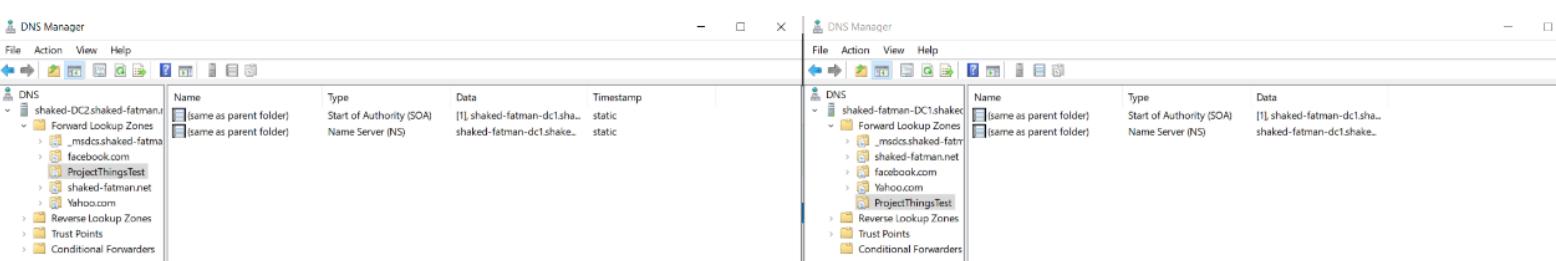


לאחר ששיםנו את ההגדירה, נראה שהכל עובד.

נפתחו העברותZONE לכל סרבר, הכל יעבד.



נכשו הכל עובד!



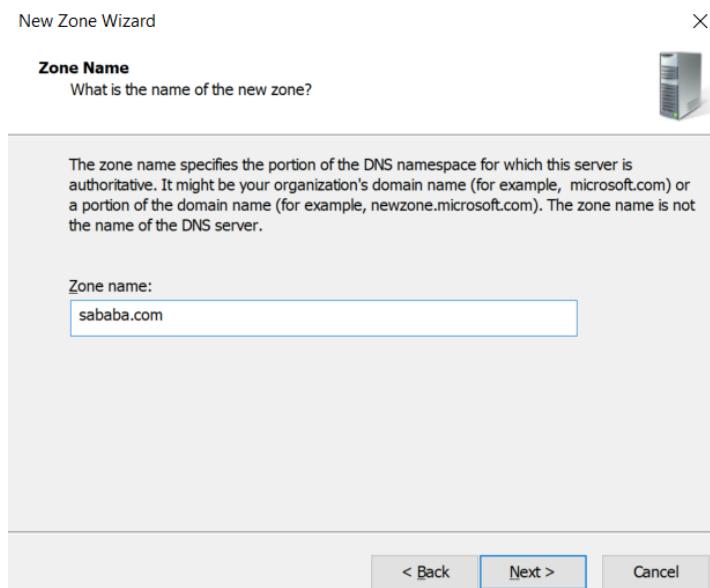
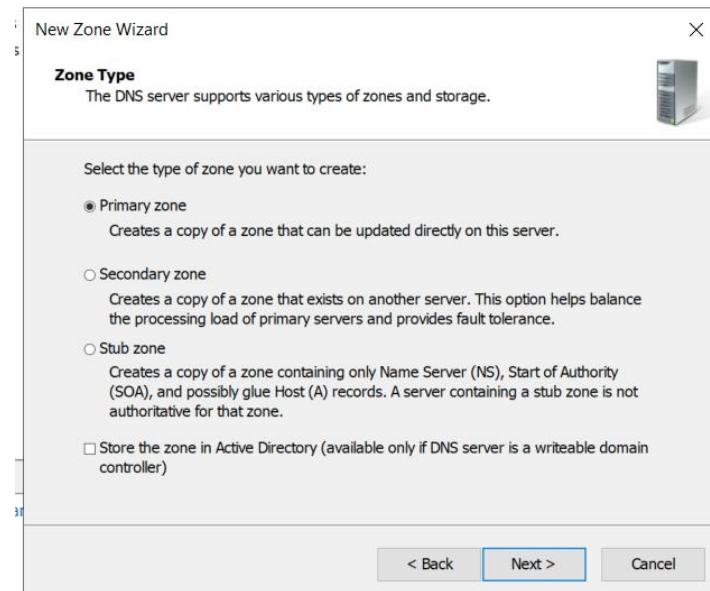
יצירת CNAME לשרת DC2

צור CNAME לשרת DC2 או לרשומה אחרת לבחירתך, לשם שהוא שונה מהשם המקורי של השרת –
בדוק שזהעובד (PING מהתחנה לשם החדש)

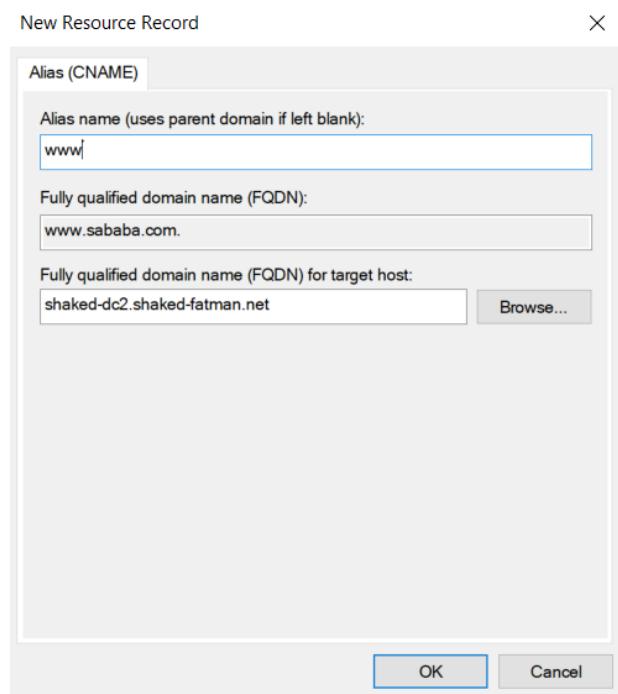
יצור CNAME שמכoon לשרת, ויתן לו שם, סבבה נקודה קום.

CNAME, זה סוג של רשומה, שמגדירה כינוי לשם דומיים, הרשומה מפנה את הדומיין, לכתובת דומיין אחרית.

יצור ZONE חדש ונקרא לו סבבה קום



כעת נוסיף בפנים Cname כמו שבקשו



כעת ניתן לראות שעובד

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

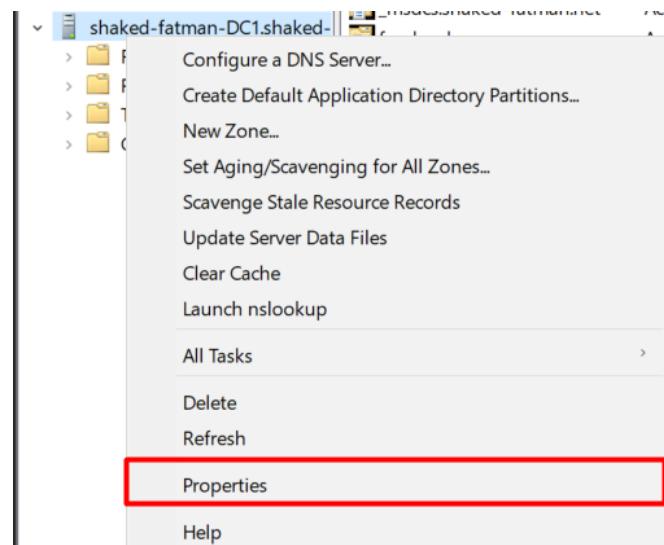
C:\Users\Administrator>ping www.sababa.com

Pinging shaked-dc2.shaked-fatman.net [192.168.80.201] with 32 bytes of data:
Reply from 192.168.80.201: bytes=32 time<1ms TTL=128
Reply from 192.168.80.201: bytes=32 time=1ms TTL=128
Reply from 192.168.80.201: bytes=32 time<1ms TTL=128
Reply from 192.168.80.201: bytes=32 time<1ms TTL=128

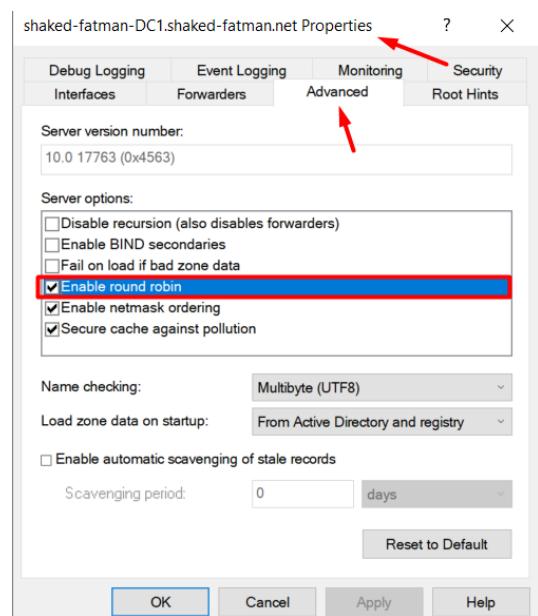
Ping statistics for 192.168.80.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

יצירה ובדיקה של ראונד רובין

- צור ובזוק Round Robin ל 2 רשומות שמשנות לכתובתRndomilit (לא CNAME) הוא אלגוריתם חלוקה מתחלף של משאיים בין מספר משתמשים או תהליכי דבר ראשון שנעשה, נפעיל Round Robin בc1 Properties

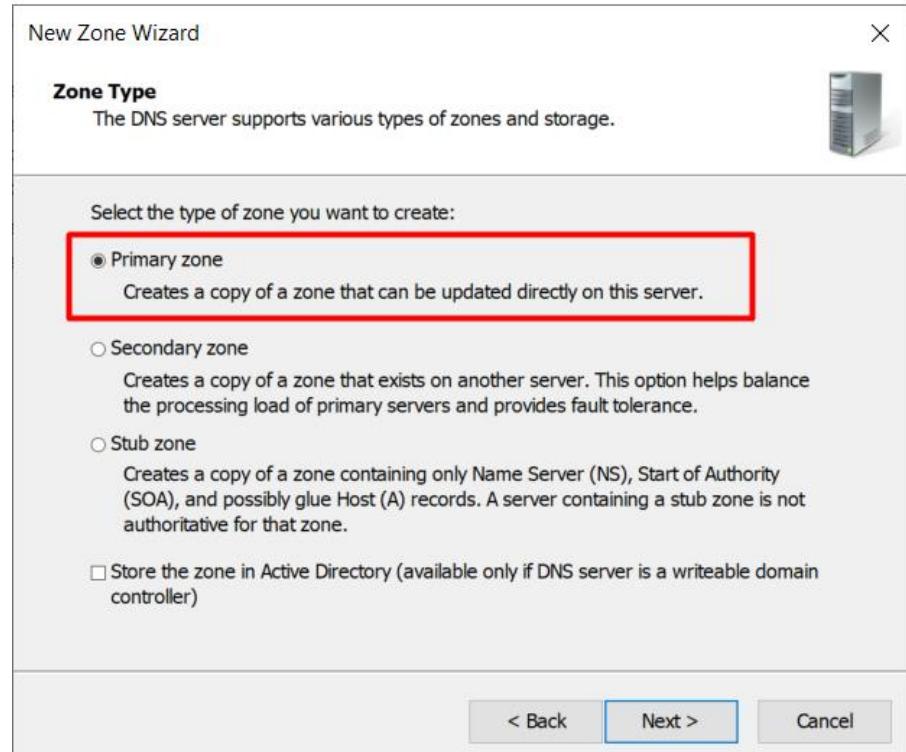


כעת נכנס ל'Advanced', ונעשה Advanced

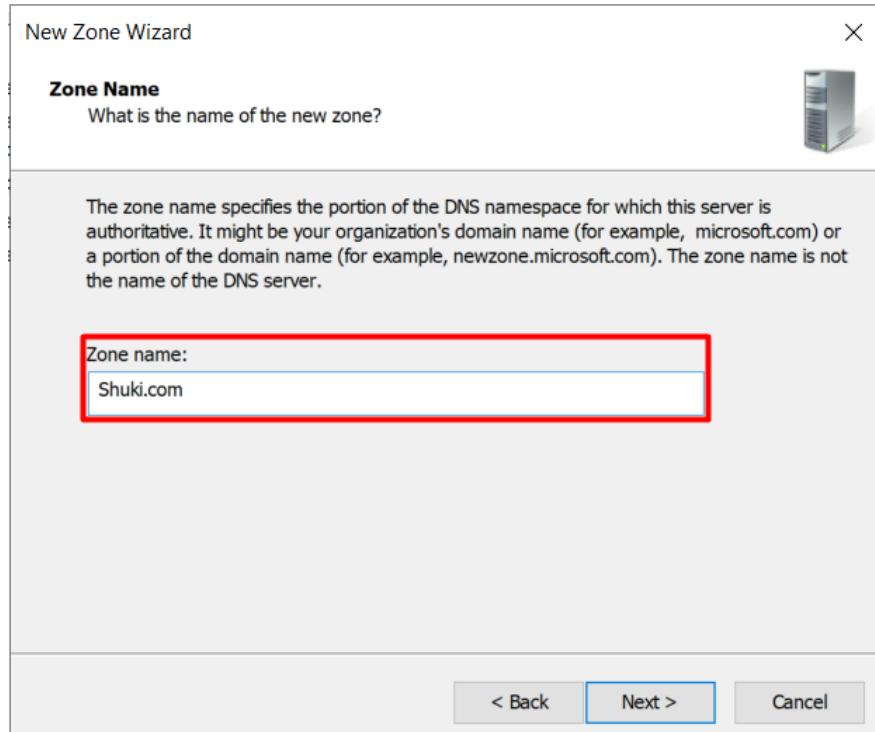


নি�וצר Zone חדש, ונקרא לו Shuki.com

נבחר ב-zone Primary

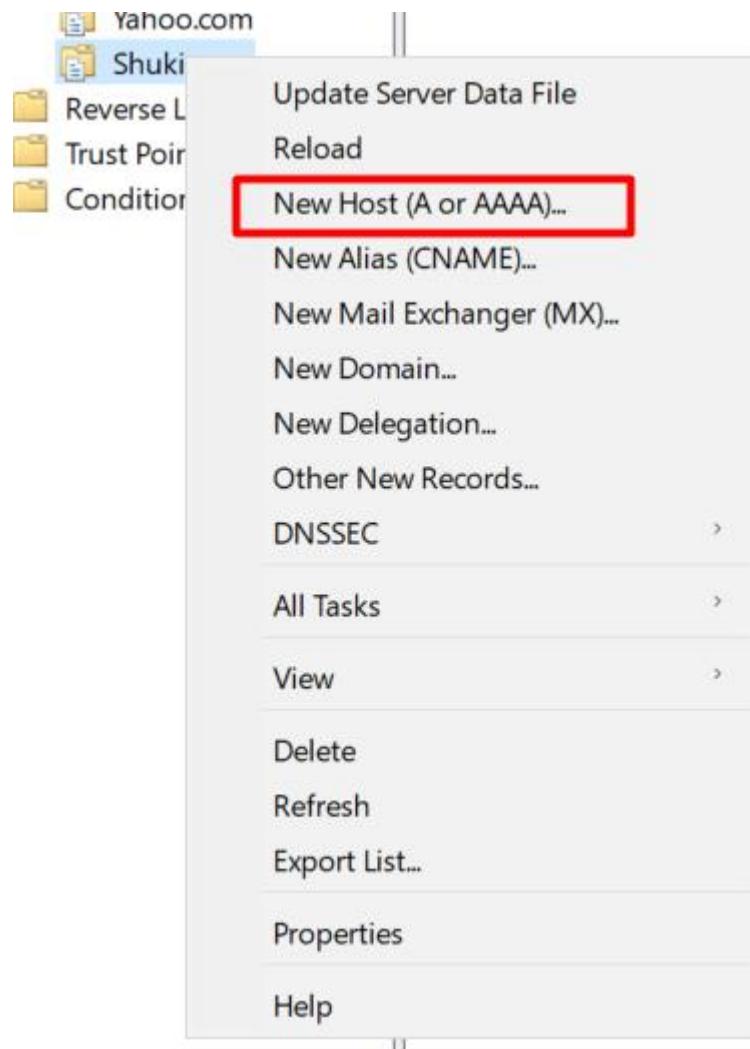


נקרא לו בשם שרצינו



כעת נוסיף שני (a) Host עם אותן השמות, אך עם כתובות רנדומליות לחלווטין.

נלחץ כפתור ימני על השם של הzone שלנו, ונלחץ על New Host



כעת ניתן שם לhost שלנו, נקרא לו Shukon

New Host X

Name (uses parent domain name if blank):
Shukon

Fully qualified domain name (FQDN):
Shukon.Shuki.com.

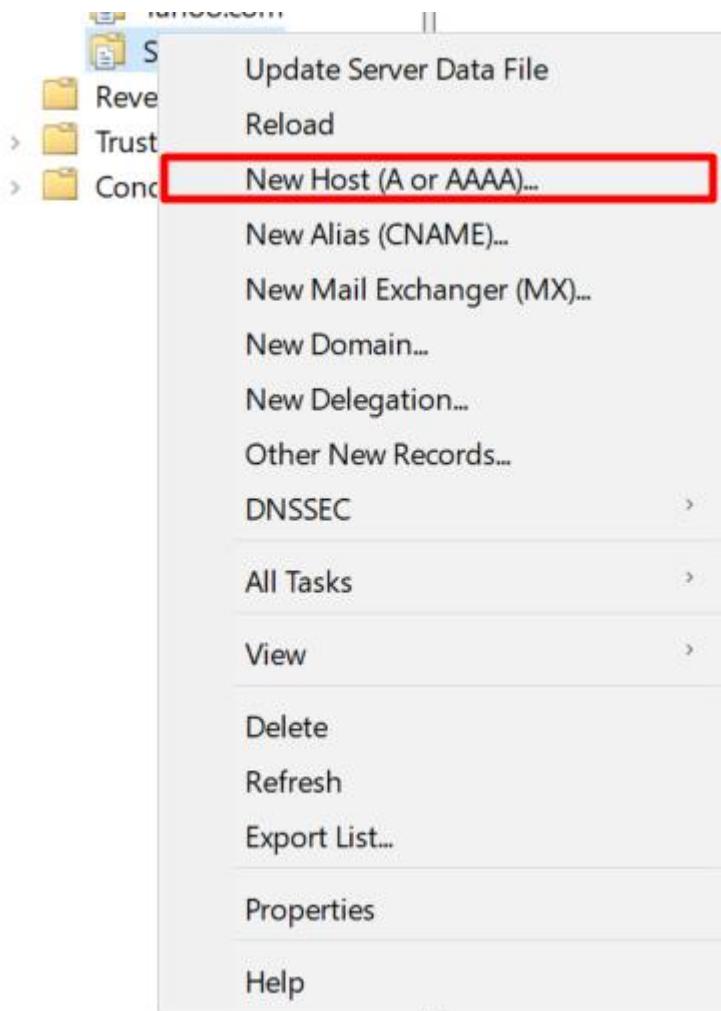
IP address:
192.168.80.41

Create associated pointer (PTR) record

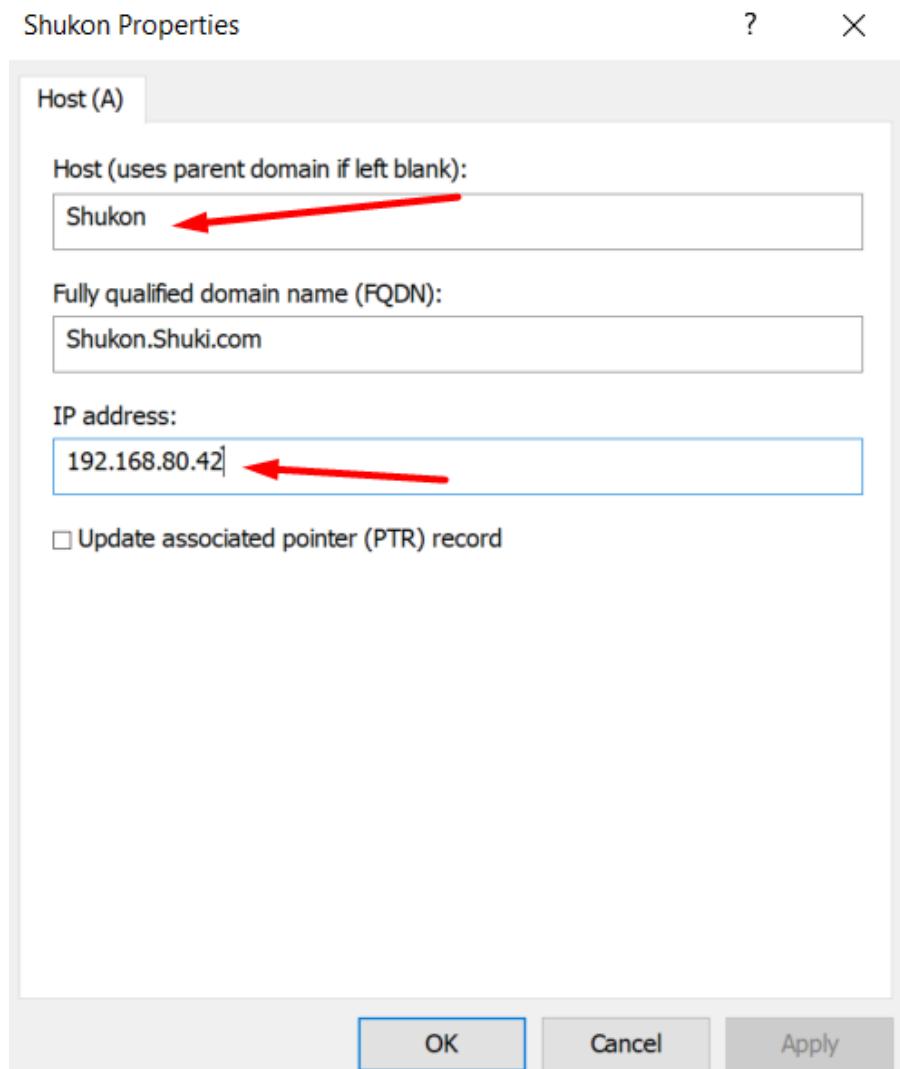
Add Host Cancel

וניצור עוד host, עם אותו השם, רק כתובות אחרות

בשביל זה נלחץ עוד פעם כפתור ימני על הZone, וגעשה New Host

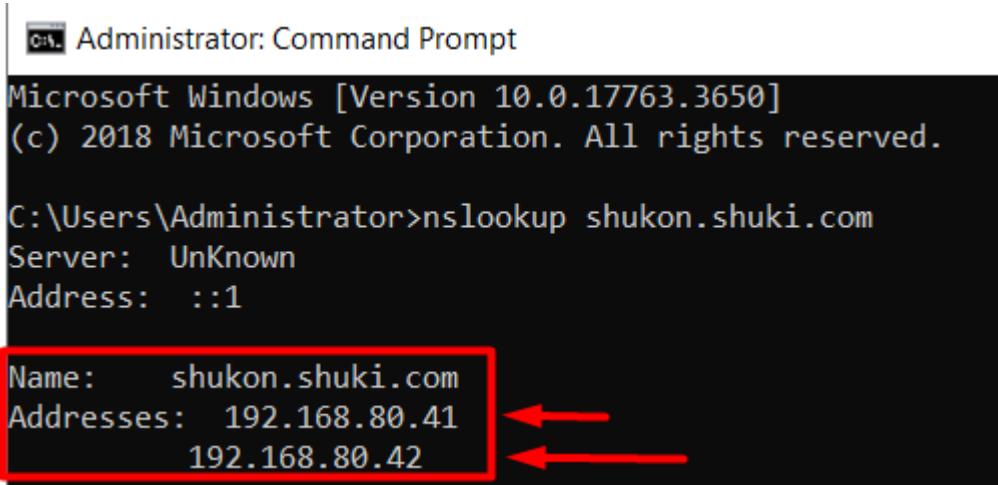


וניצור עוד Host, עם אותו השם, רק כתובות אחרת



כעת נבדוק Round Robin באמתעובד לנו

לטובת הבדיקה, נצטרך להריץ בשורת הפקודה nslookup shukon.shuki.com, אז זה יראה לנו איזה כתובות יש DNS, ל Shukon ,



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

C:\Users\Administrator>nslookup shukon.shuki.com
Server: UnKnown
Address: ::1

Name:     shukon.shuki.com
Addresses: 192.168.80.41
           192.168.80.42
```

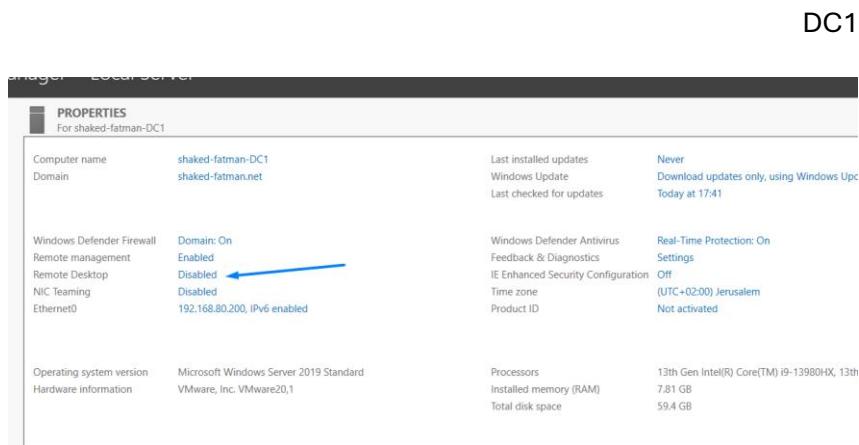
כעת ניתן לראות, שיש לנו את שתי הכתובות שיצרנו, זמינים לZone שיצרנו.

ניהול השרת מרוחק

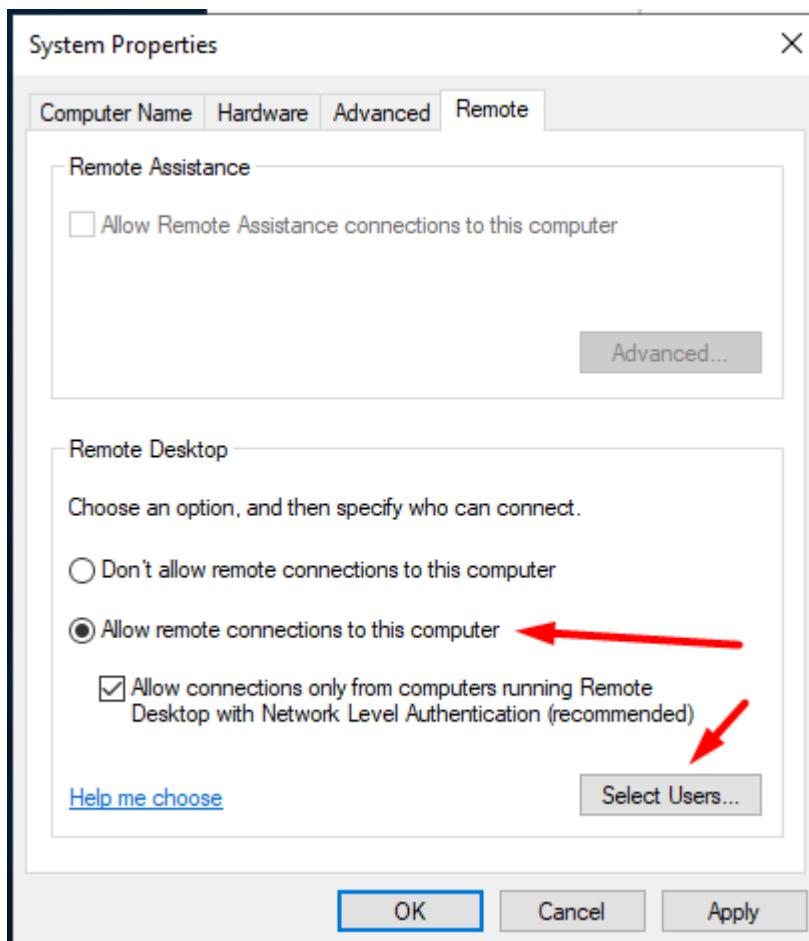
אפשרו למחוקת Sys/Admins לנהל את השירותים מWIN10.

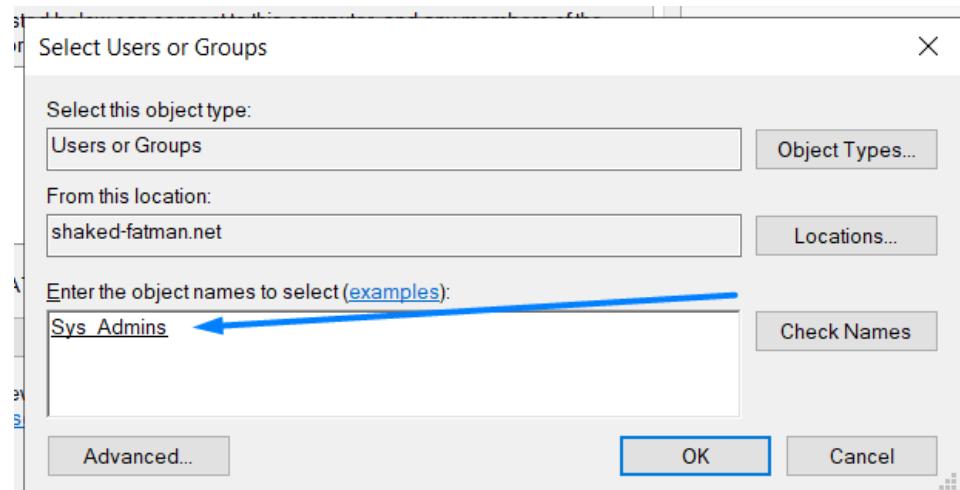
- אפשר למחוקת Sys/Admins לננהל את השירותים מWIN10, בעזרת Remote Desktop. הוא תוכנה שנותנת למשתמש להתחבר למחשב אחר מרוחק ולהשתמש בו כailo ישב מולו, או בKİצ'ור, משטלת עליו, הדבר געשה באמצעות פרוטוקול RDP, או בעברית פרוטוקול שלוחן עבודה מרוחק.

נפתח את האופציה בכל סרבר לSys/Admins

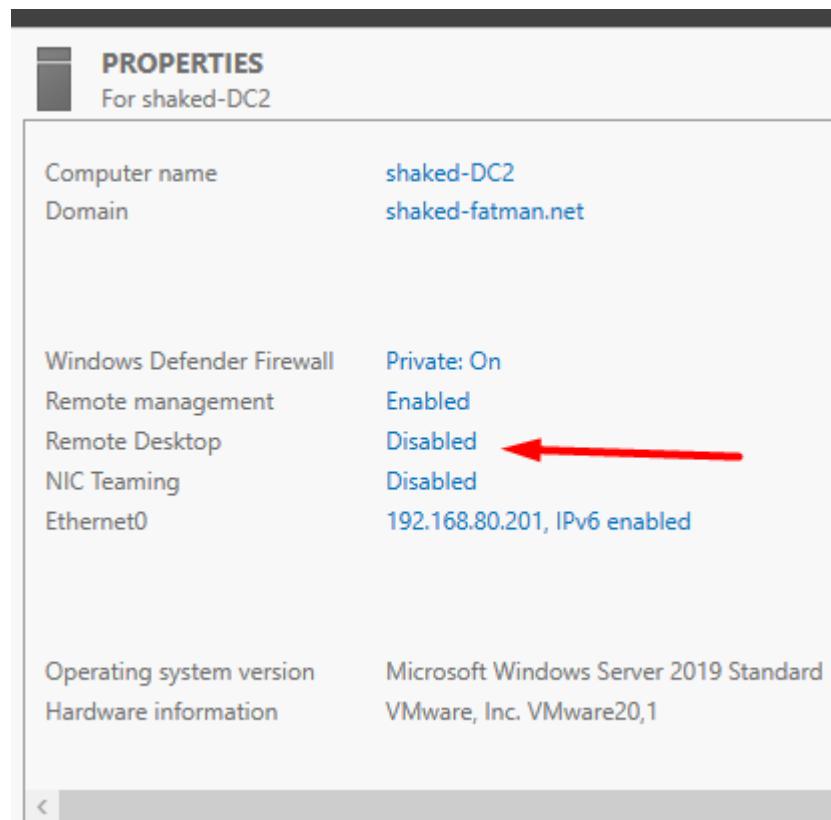


נפתח את האופציה לחיבור מרוחק, ונבחר בהסרים Sys/Admins

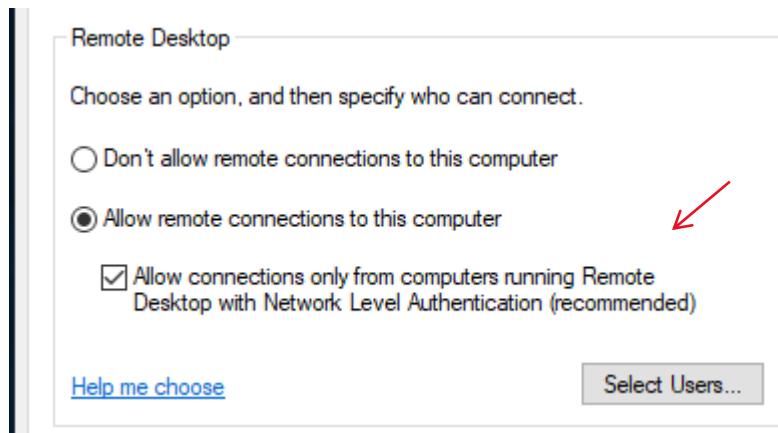




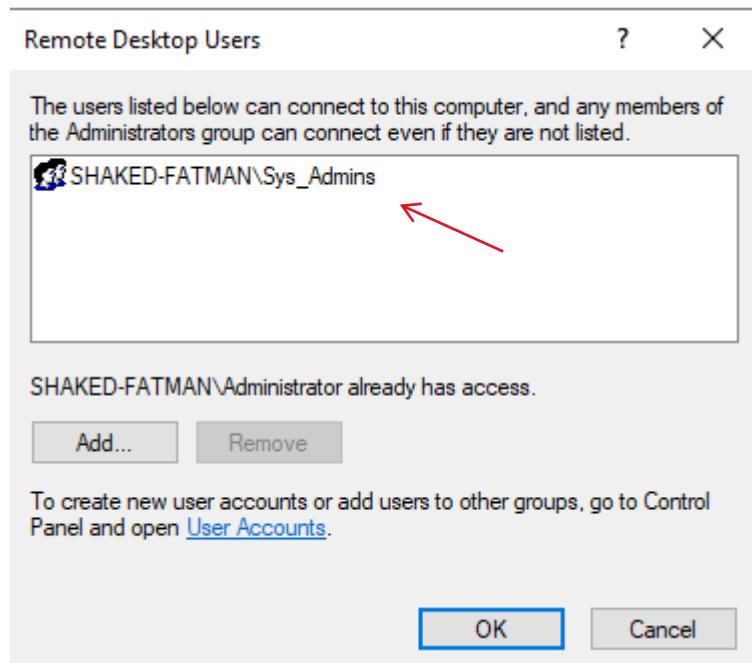
DC2

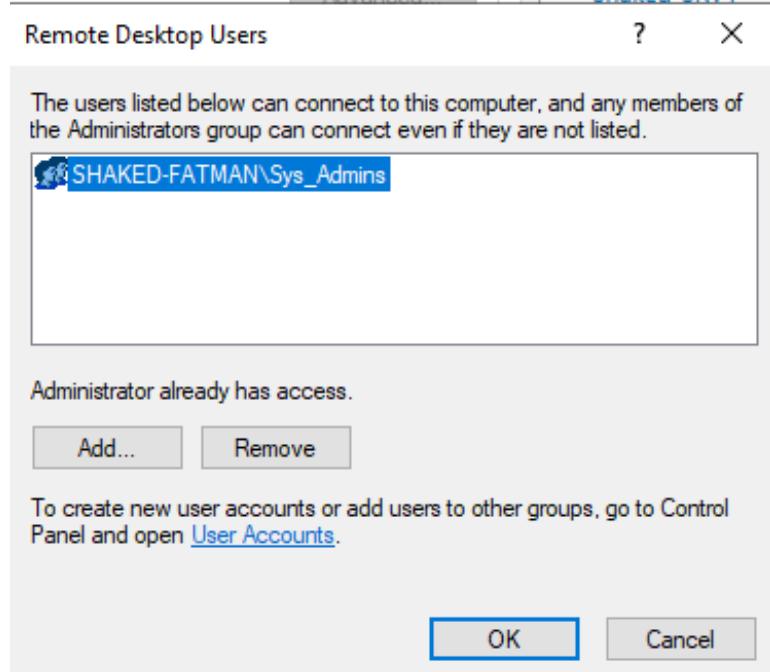
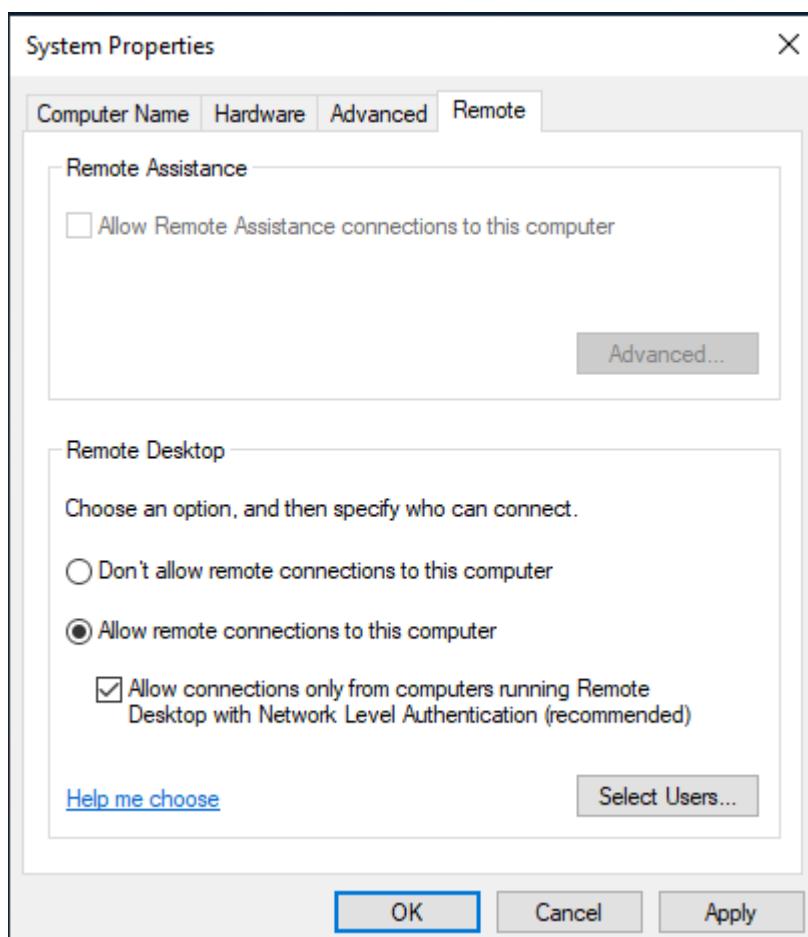


אפשר חיבור מרוחק



הנוסף את Sys_Admins

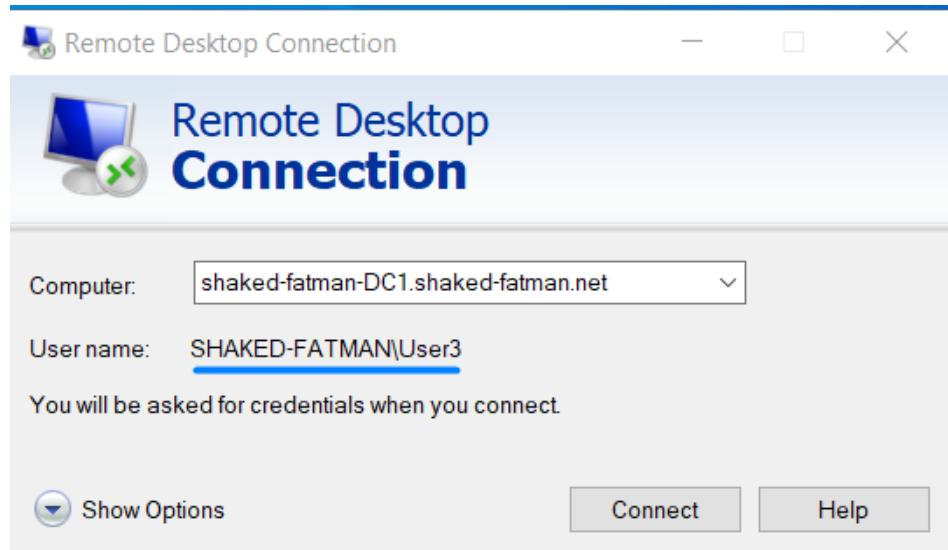




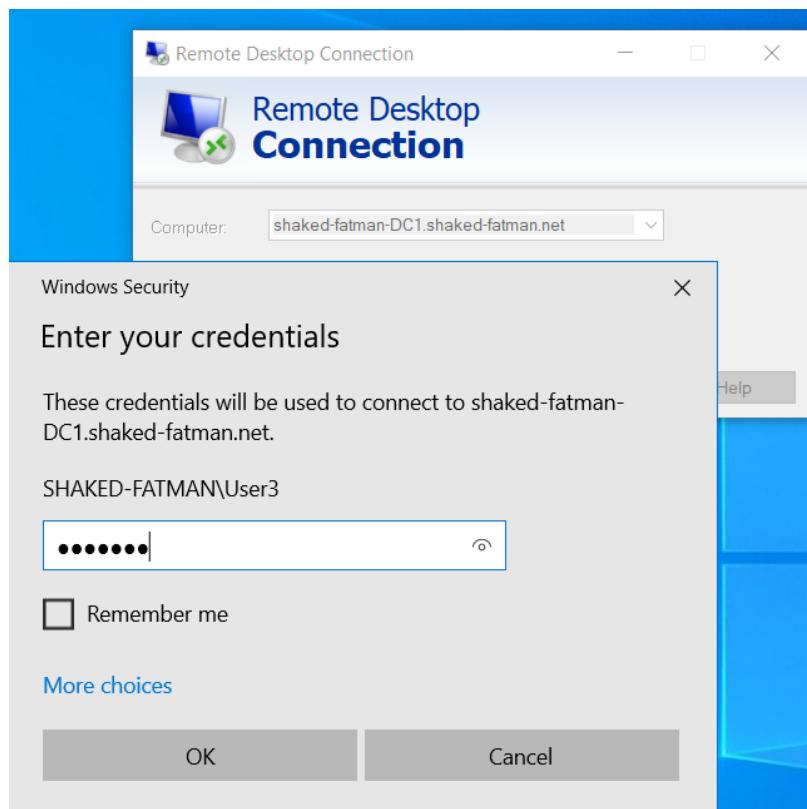
ביצוע השתלטות עם משתמש ממנהל Sys Admins

- בצע Login ל-WIN10 ובדוק שימושו של משתמש Sys_Administrators יכול לבצע השתלטות מופעלת.

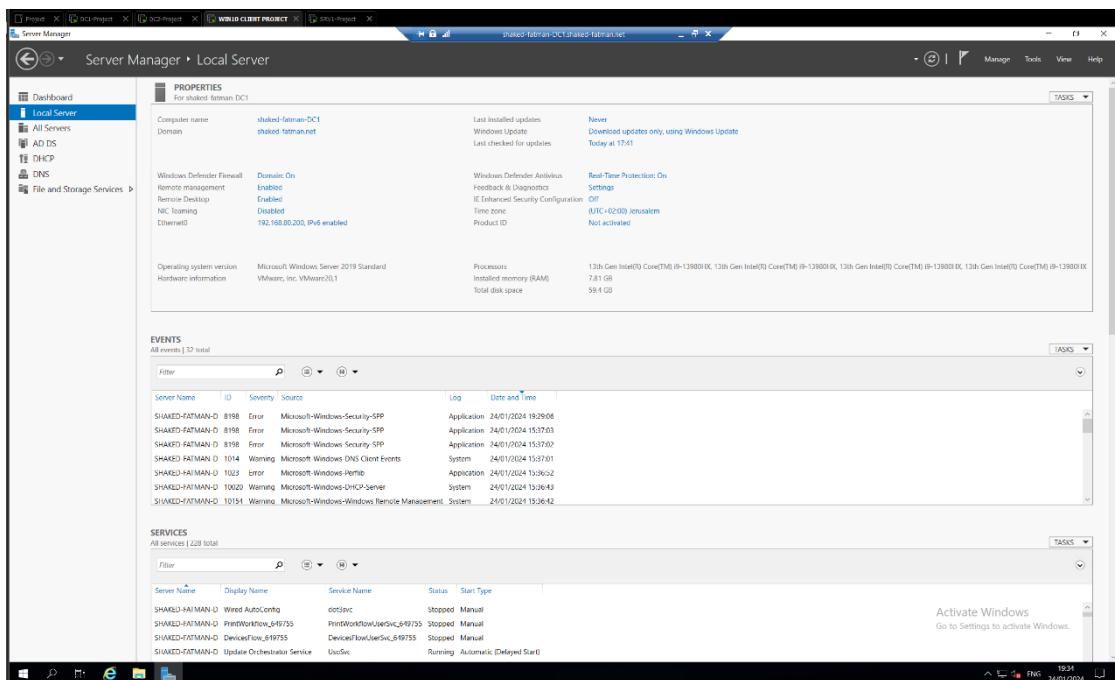
כעת נבדוק שמשתמש User 3 יכול להתחבר מווינדואס 10 ל-DC



נשימ את הסיסמה שלנו

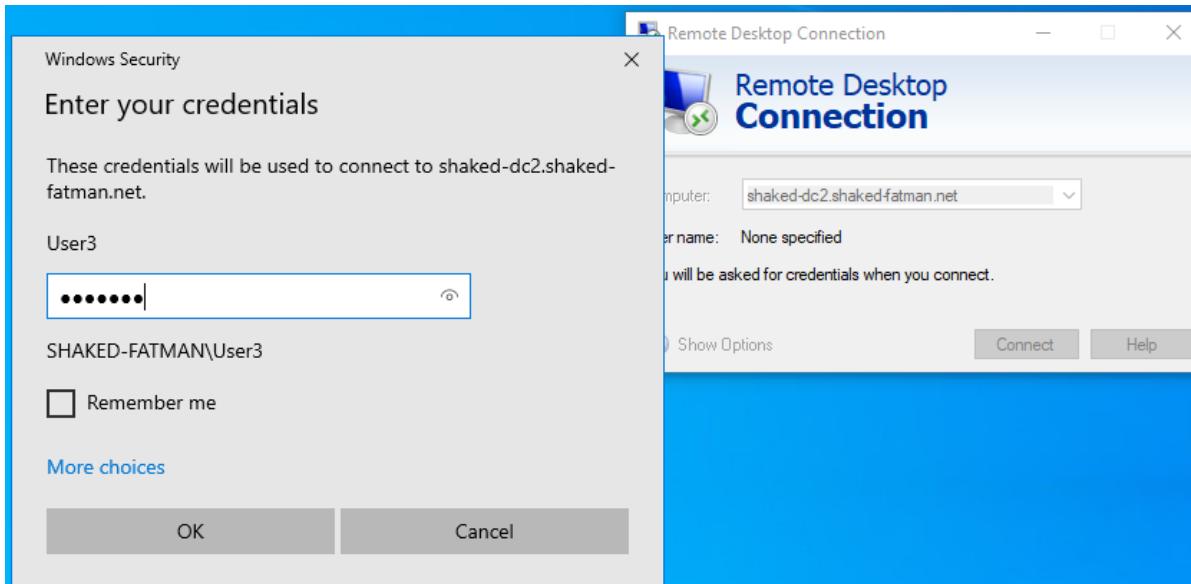


ניתן לראות חיבור מוצלח ל-dc1

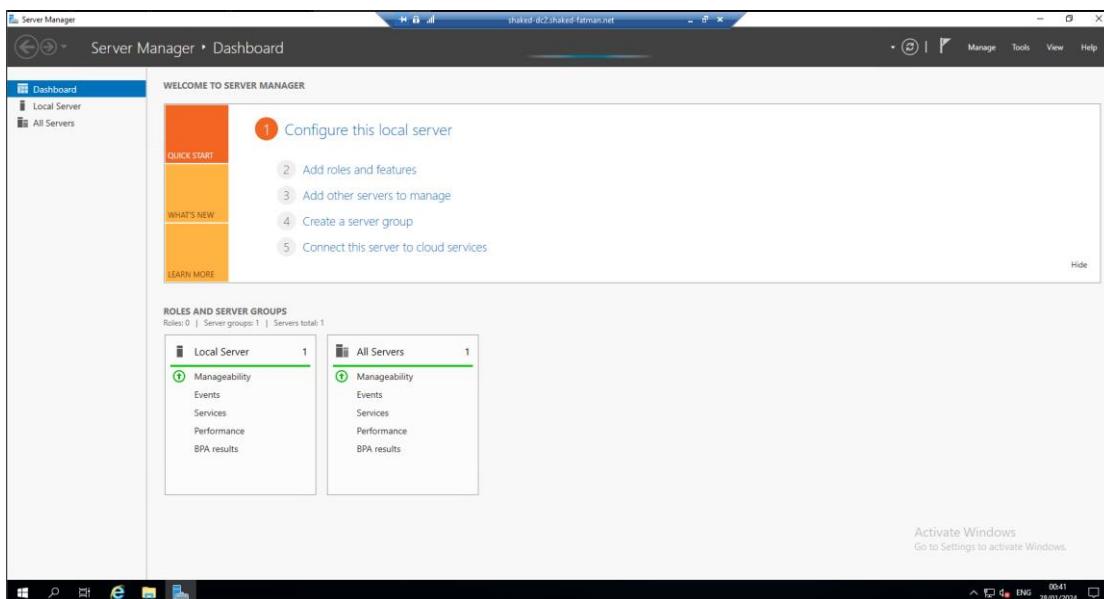


כעת נבדוק שיוור 3 יכול להתחבר מ 10.0.0.3 ל dc2

נשים את הפרטיהם של DC2

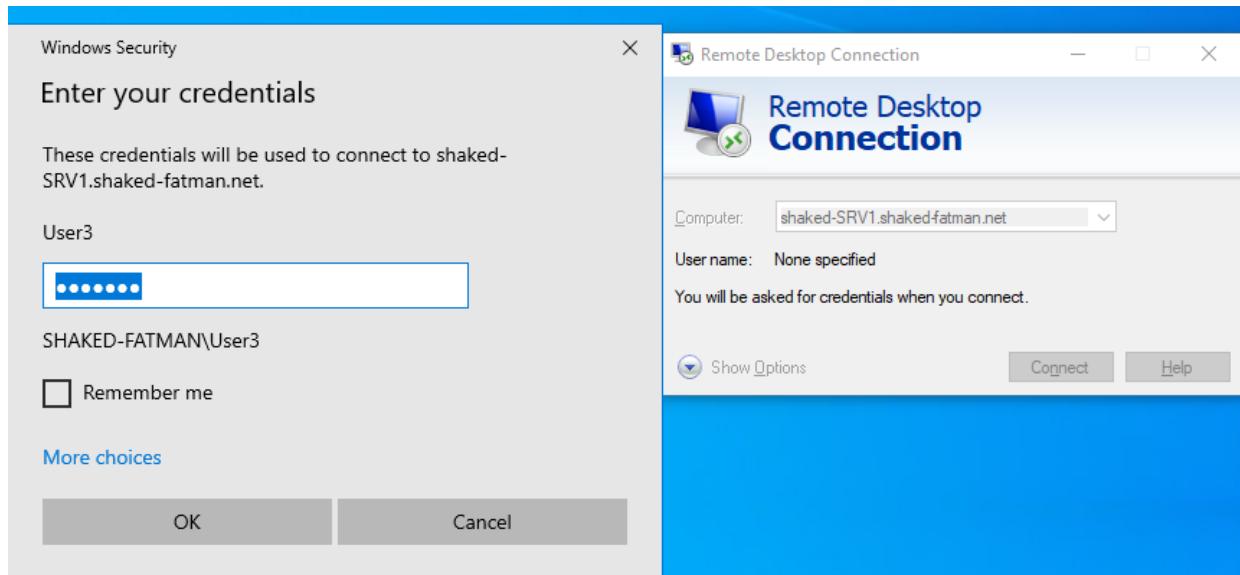


ונitin לראות חיבור מוצלח ל dc2

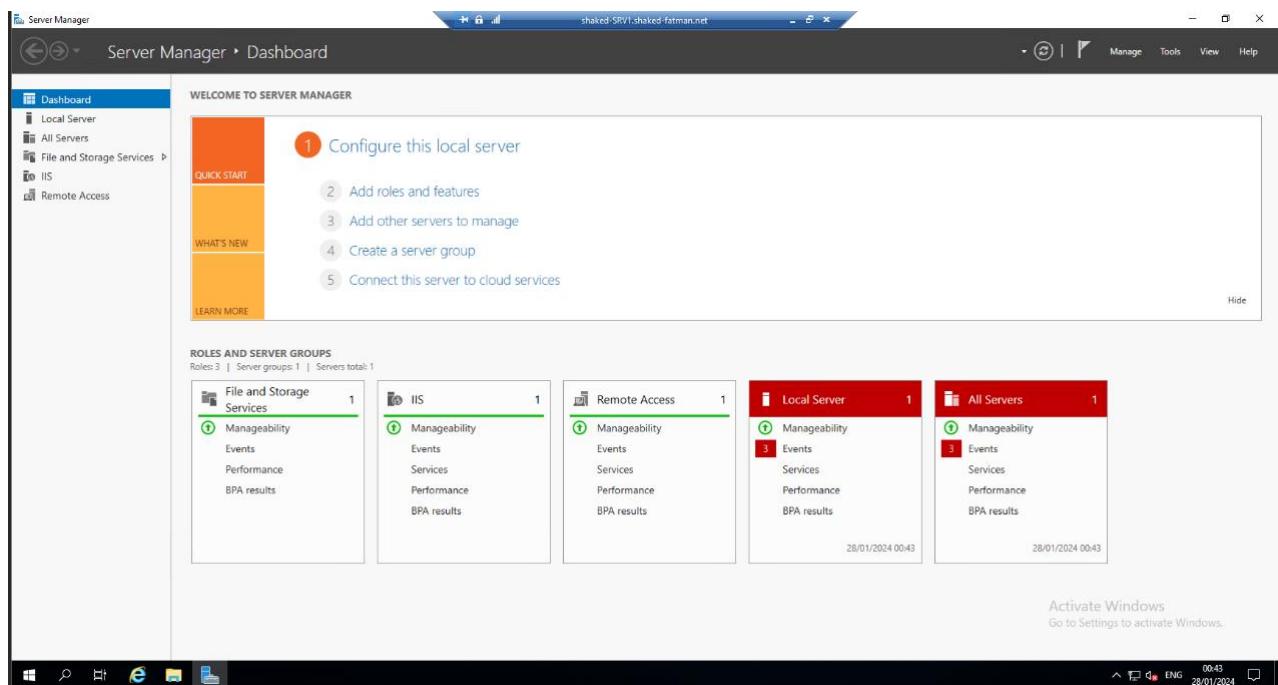


כעת נבדוק שיזר 3 יכול להתחבר מווינדוס 10 גם ל-SRV1

נשים את הפרטיהם של סרבר 1



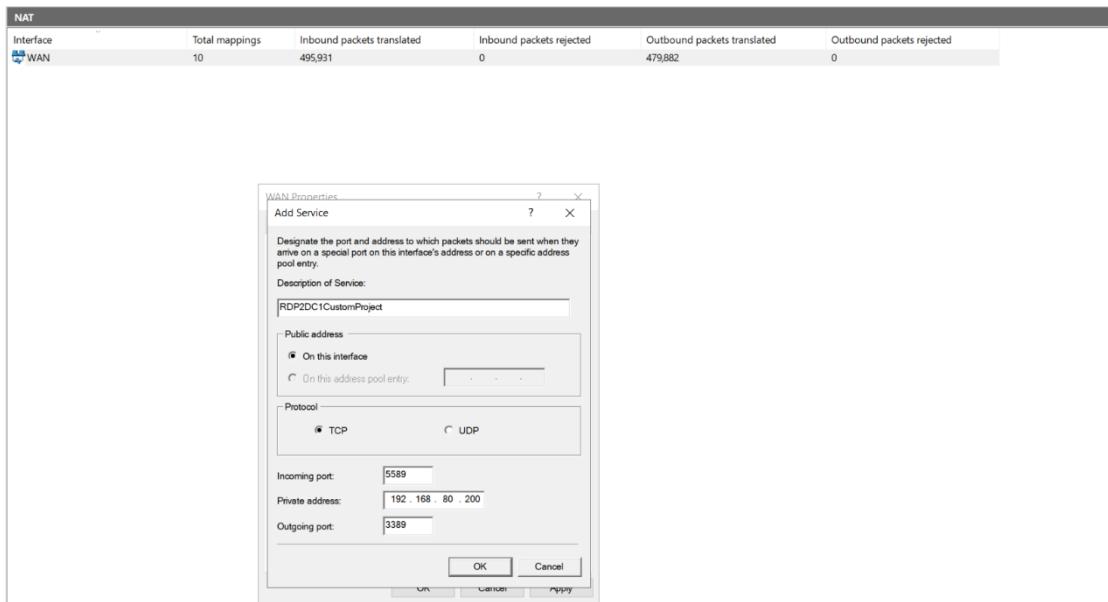
ונitinן לראות שהתחברנו ל-SRV1



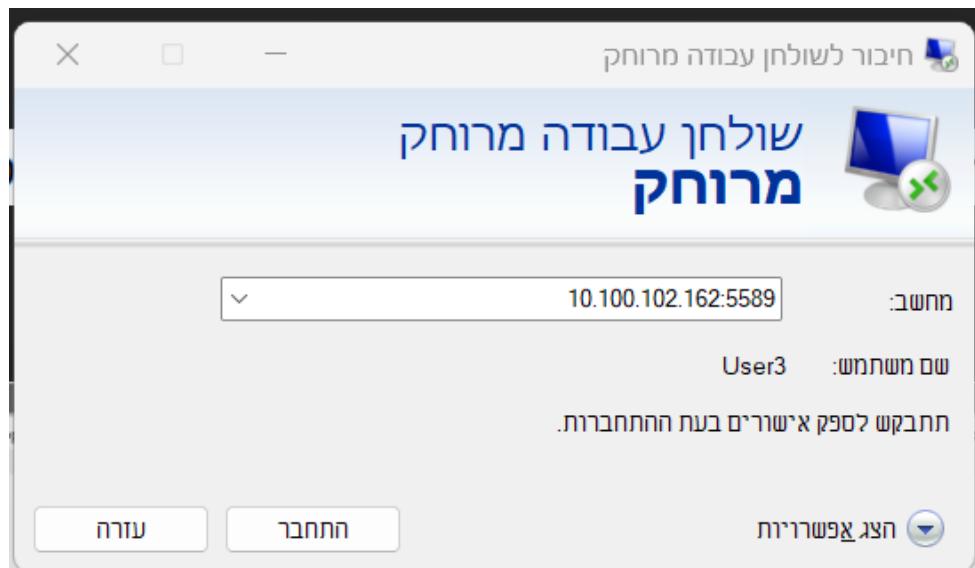
מתן האופציה לעובד מוחץ לארಗון להתחבר עם פורט 5588

- אפשר RDP לשרת DC1 לעובד מוחץ לארゴן – מפорт 5588 לפורט 3389 בשרת.

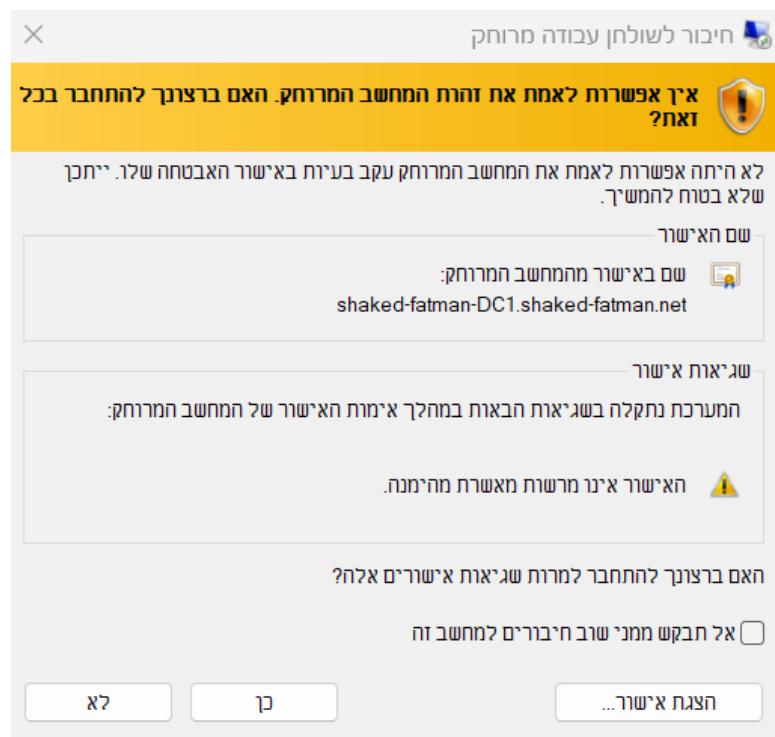
כעת נאפשר כניסה של פורט 5589 אל כתובת של DC1



כעת נלך לHost, המחשב הפיזי שמריץ את המכוניות הווירטואליות, וננסה להריץ דרכו (הכתובת, היא הכתובת פרטית וואן, של סרבר1)



קיבלונו את המסר הבא, נאשר.



ונחנו בפנים!

The screenshot shows the Windows Server Manager interface for a local server named "shaked-fatman-DC1". The left navigation pane includes options like Dashboard, Local Server, All Servers, AD DS, DNS, DHCP, File and Storage Services, and File and Storage Services. The main area displays the "PROPERTIES" tab for the selected server. It shows basic information such as Computer name (shaked-fatman-DC1), Domain (shaked-fatman.net), and Windows Defender Firewall status (Domain On). It also lists network interfaces, operating system version (Windows Server 2019 Standard), and hardware information (VMware, Inc. VMware201). The "EVENTS" tab shows a list of 32 events, mostly from Microsoft-Windows-Security-SPN, indicating various security and audit log entries. The "SERVICES" tab lists 258 services, including several Microsoft-Windows-Windows Remote Management services. A watermark for "Activate Windows" is visible in the bottom right corner.

הקשהת התהנות

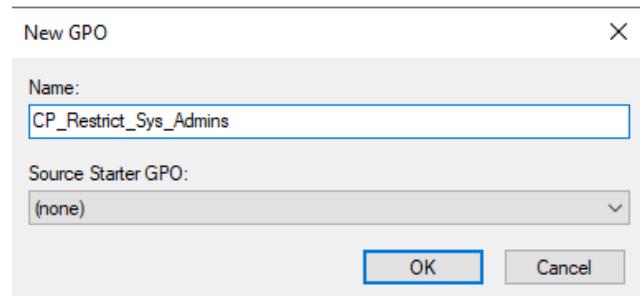
Group Policy הוא כלי שמאפשר למנהל לשלוט במחשבים בארגון שלהם. מאפשר למנהל להגדר חוקים שימושיים על אף מחשבים נראים, אף הם פועלים, ואף הם מאובטחים. לצורך הדוגמה, מנהל יכול להשתמש ב-Group Policy כדי להגדיר הגדרות של התקנים חיצוניים, חסימה של CMD לעובדים, חסימה של Control Panel, ועוד הרבה דברים.

חסימה של Control Panel למי שלא Sys Admins

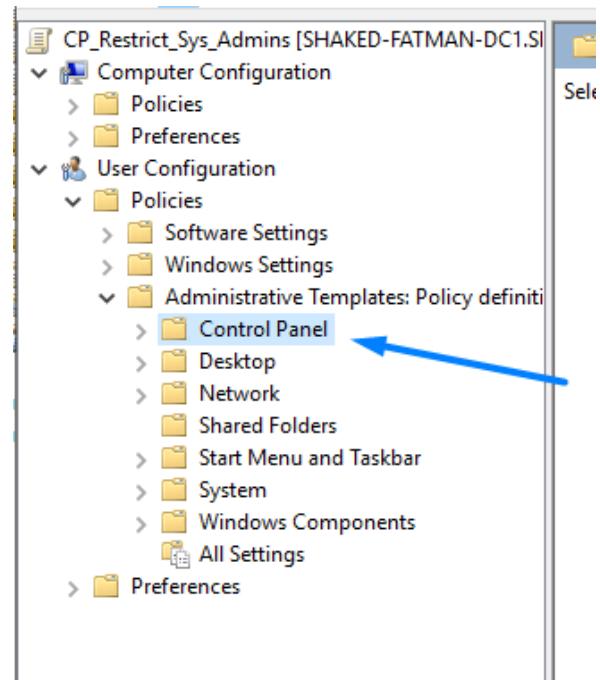
- **מניעת גישה של משתמשים שאינם עובדי Sys Admins ל-Control Panel**

הוא כלי שמאפשר למשתמש להתאים את מערכת הפעלה שלו לצרכי

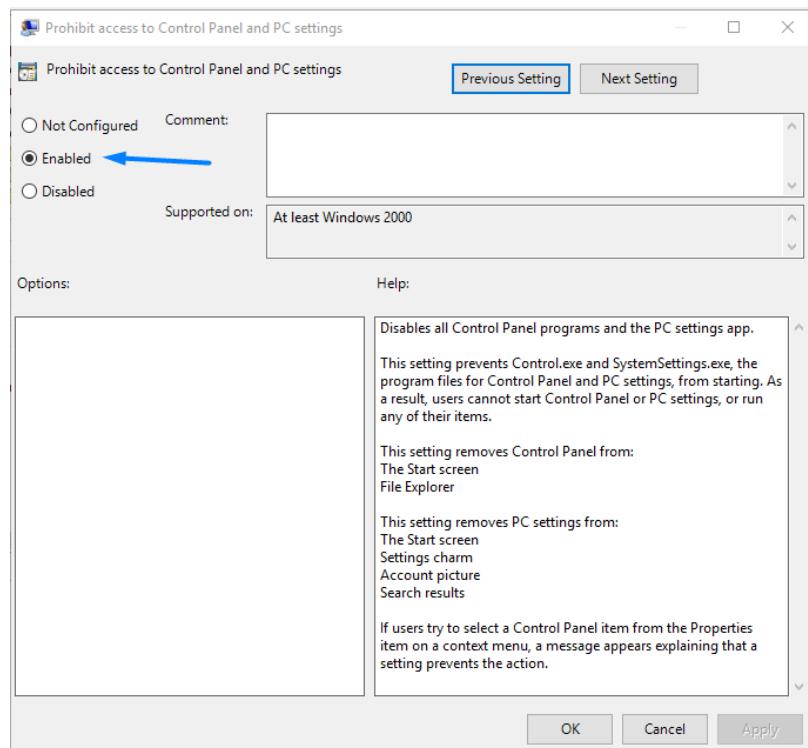
דבר ראשון שנעשה, זה יצירת Group Policy חדש



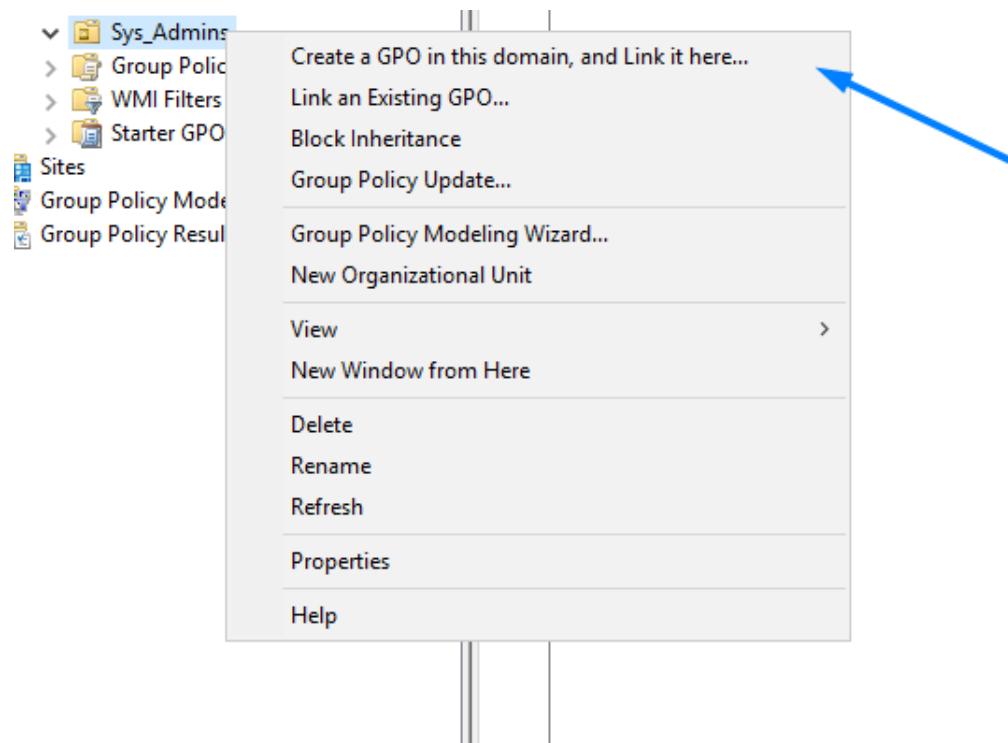
נכטו ל-**Templates** מוכנים, ונכנסו ל-**Control Panel**



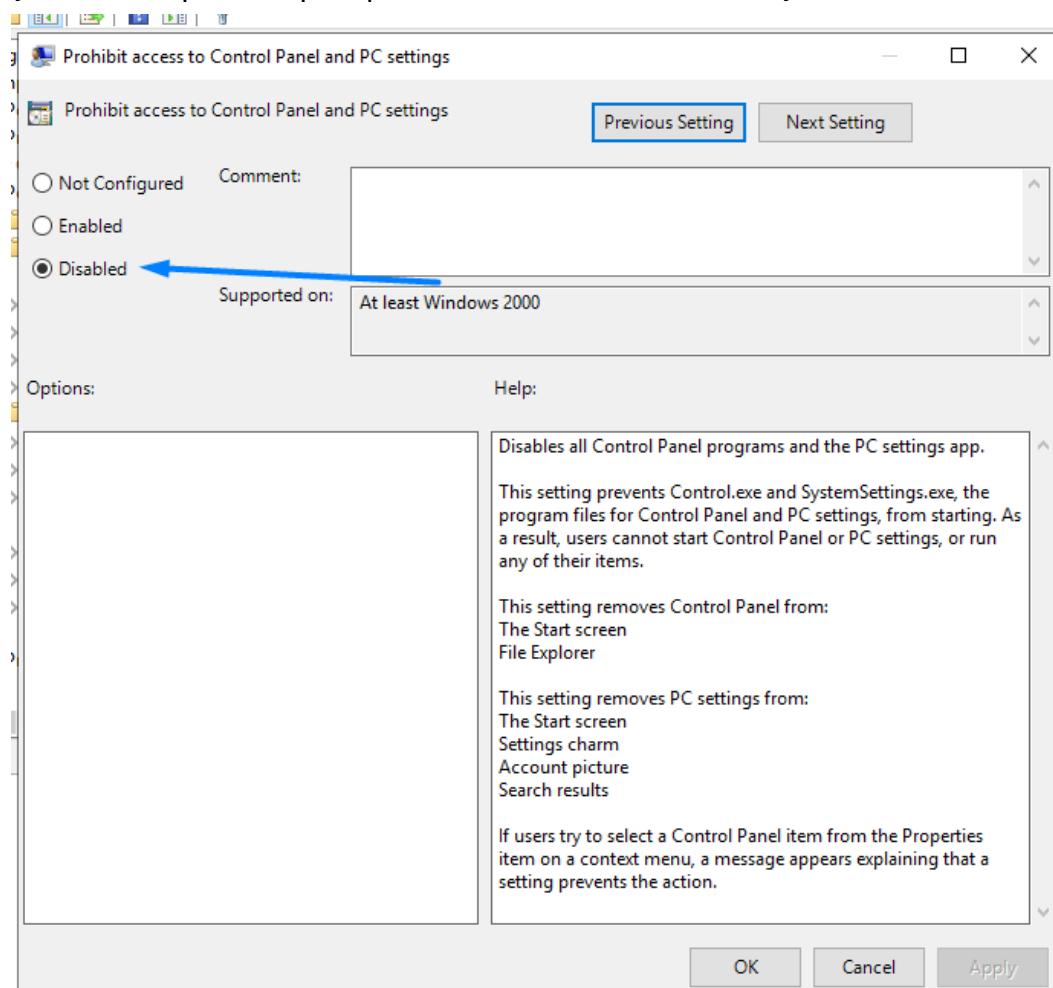
ונפעיל את ההגדרה הבאה



לאחר מכן נלך למשתמש Sys Admins וכן נזכיר ששם יהיה אפשרי לפתוח קונטROL פאנל

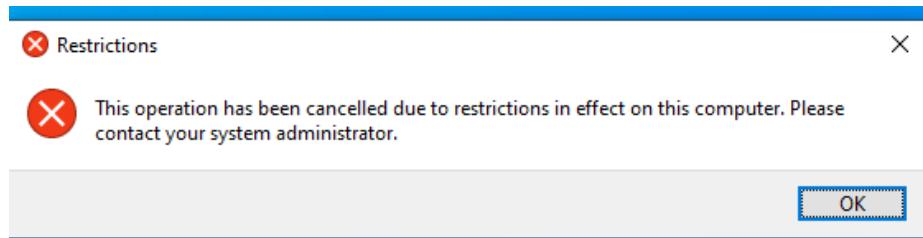


וככה פתחנו ל-Sys Admins Control Panel את הגישה ל-**Sys Admins**, בבדיקה ההפרק ממי שאין לו

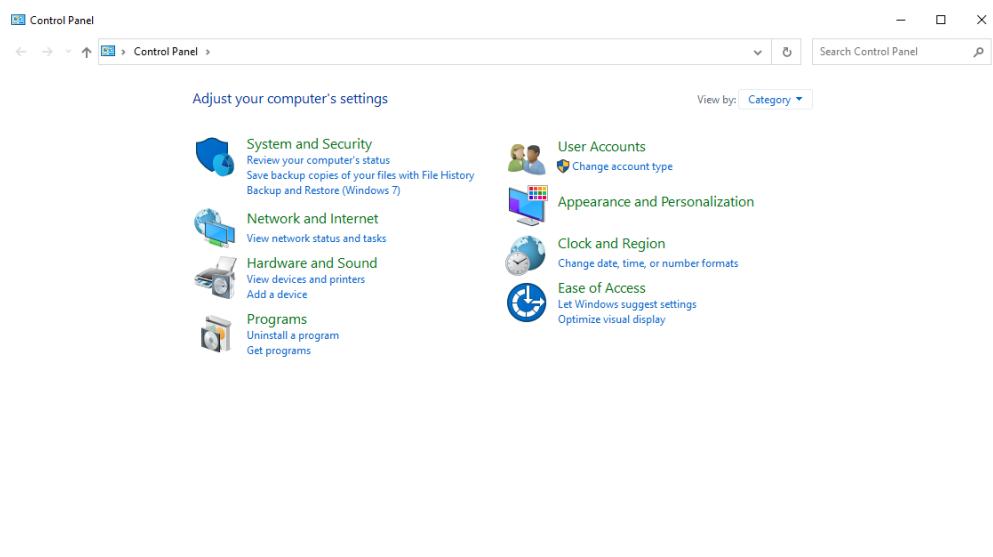


כעת נבדוק את זה, אם זה עובד, עם יוזר 3, יוזר 31 סתם נודד.

ב尤זר 31



ב尤זר 3:



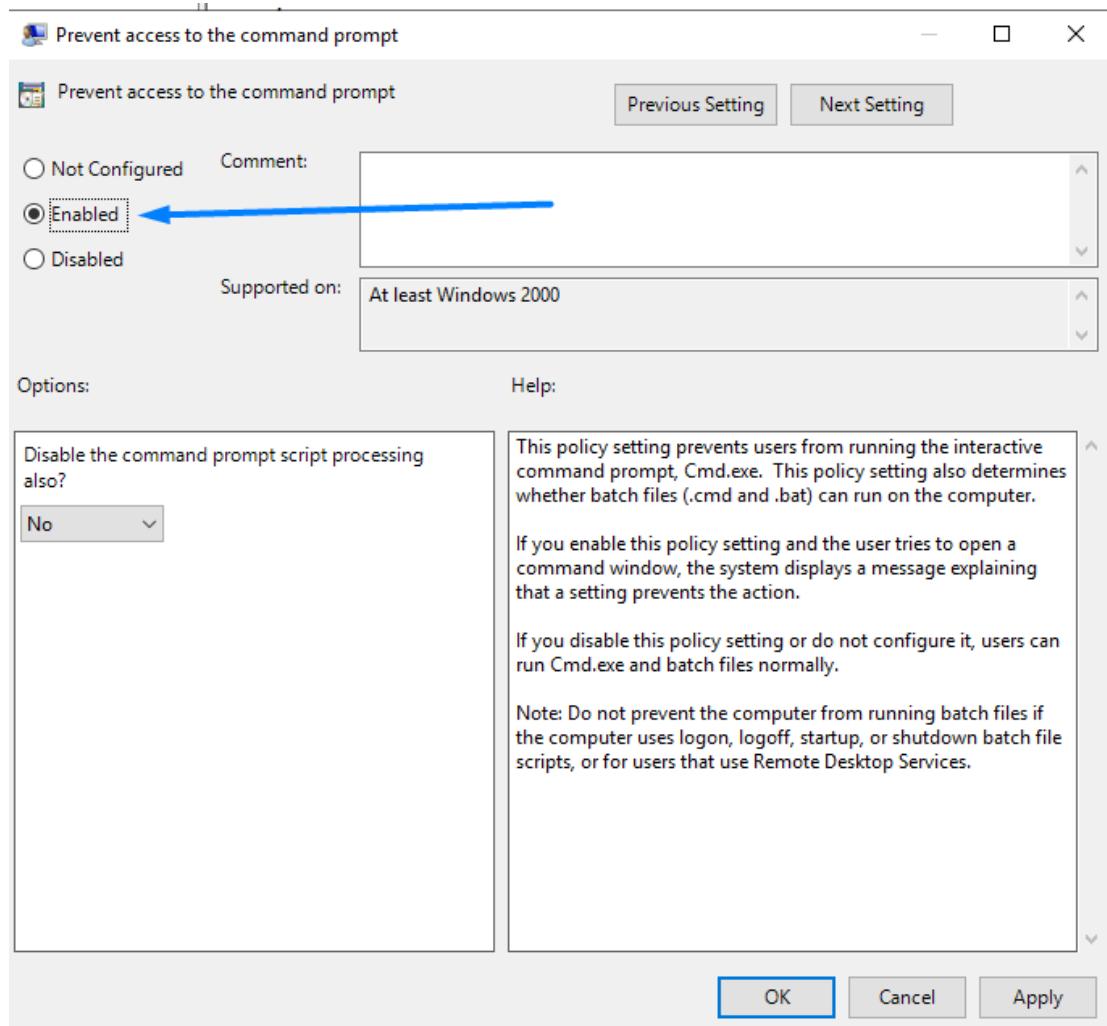
חסימה של שימוש CMD למי שלא נמצא בתחום Sys Admins

■ מניעת גישה של משתמשים שאינם עובדי Sys Admins ל-CMD.

לא בעיה, אותו עקרון כמו קודם, לחסום לכולם, ולפתח את האופציה ל-Sys Admins.

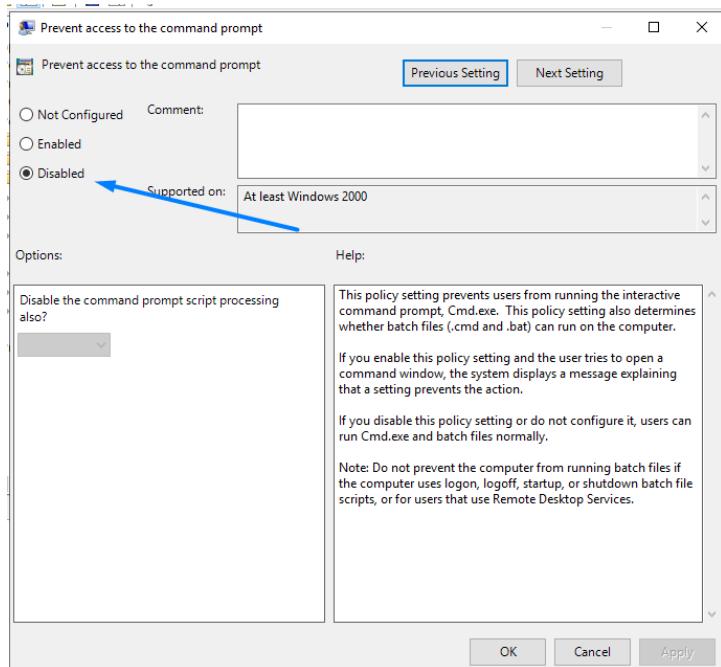
CMD זה ממשק שורת פקודה של Windows. הוא מאפשר להקליד פקודות בטקסט כדי לבצע משימות שונות.

נתחיל ביצירת GPO חדש, ובתוכו נפעיל את החסימה של CMD.

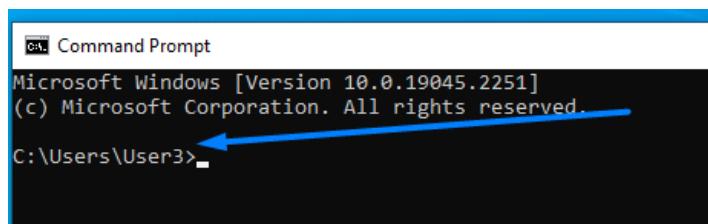


כעת נלך ל-Sys Admins, ונתן להם גישה ל-CMD.

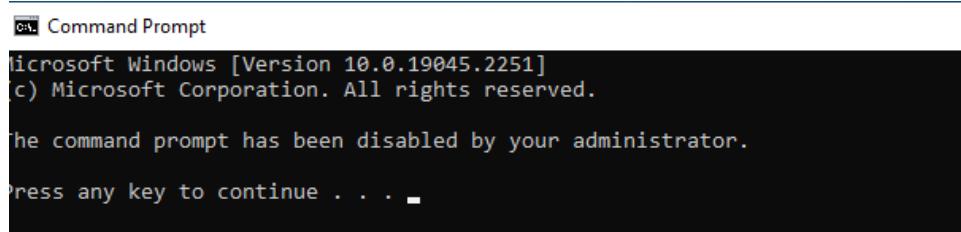
নিচৰ শেম GPO ছদ্ম, ওকেবা শেম ছসিমা.



כעת נשווה שוב בין יוזר3 ליווזר1



נביוזר...31



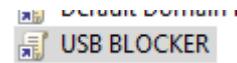
חסימה של דיסק און-קי

מניעת שימוש של כלל המשתמשים ב-Disk-on-key.

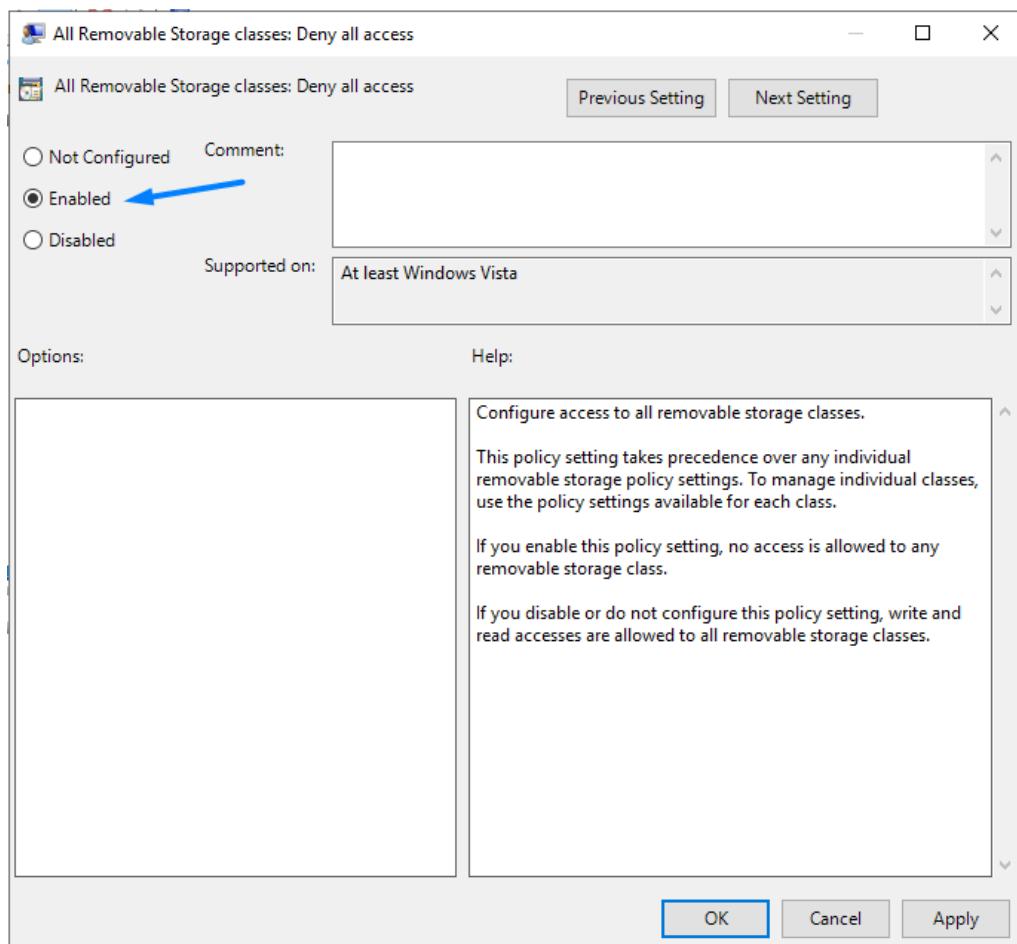
דיסק און-קי הוא מכשיר קטן וקל משקל שניתן להשתמש בו לאחסון נתונים. הוא מחובר למחשב באמצעות יציאת USB. דיסק און-קי יכול לשמש לאחסון מגוון קבצים.

חסימה של דיסק און-קי ב-GPO היא דרך למנוע משתמשי מחשב לחבר דיסק און-קי למחשביהם. אפשר להשתמש בחסימה זו כדי להגן על המחשבים מפני וירוסים, תוכנות זדוניות וכדומה.

יצור GPO חדש, נקרא לו USB בלוקר



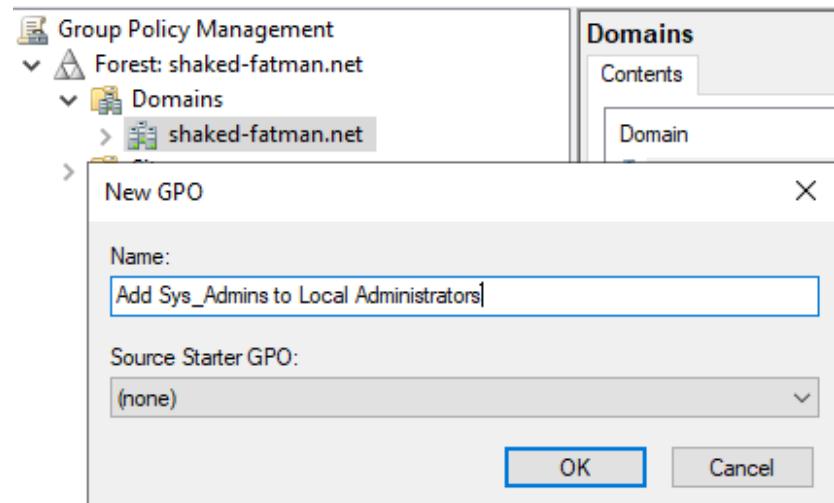
ונפעיל את ה政 Policy



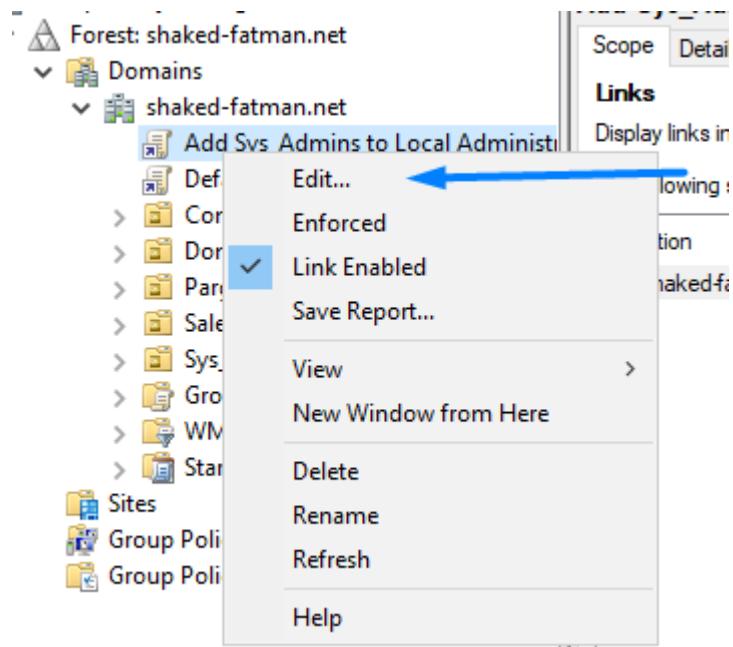
יצירת תנאי, שיאפשר להיות Admin, Sys Admins, בכל מחשיبي הארגון.

צורך Policy שמאפשר למחלקת Sys_Admins להיות בקבוצת Administrators המקומית של כל מחשיבי הארגון (זהירות!)

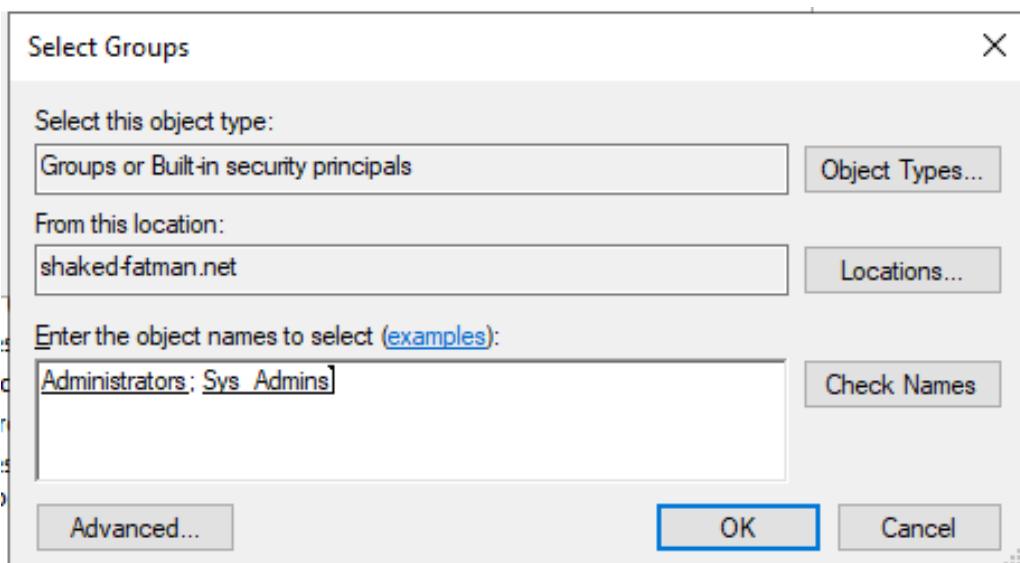
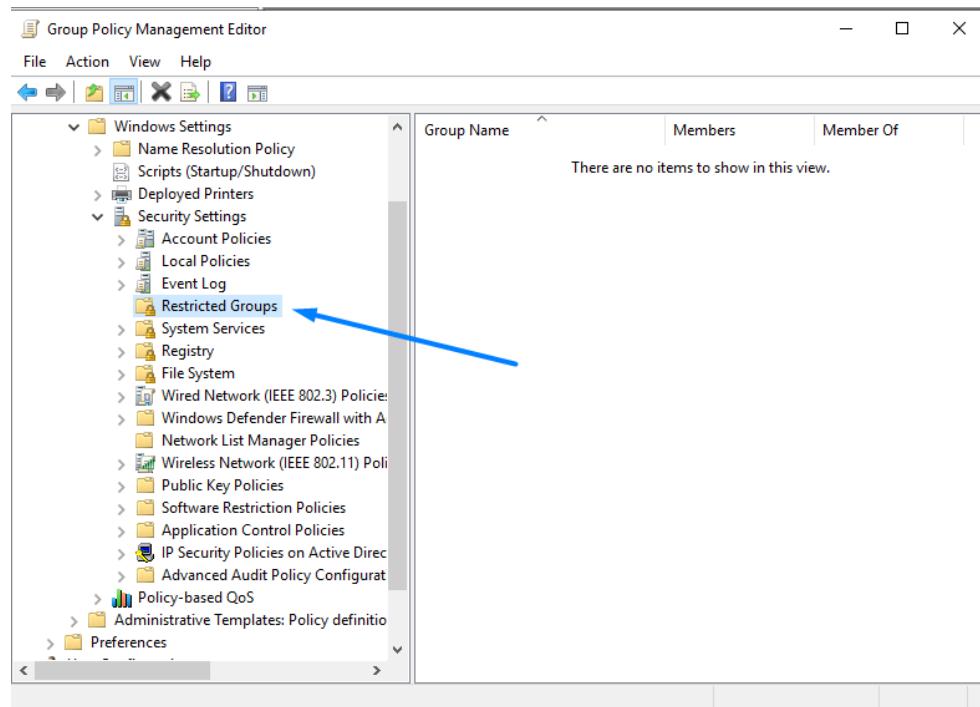
מוסיף GPO חדש, ונקרא לו ככה



ນלך לEDIT ונהריך אותו



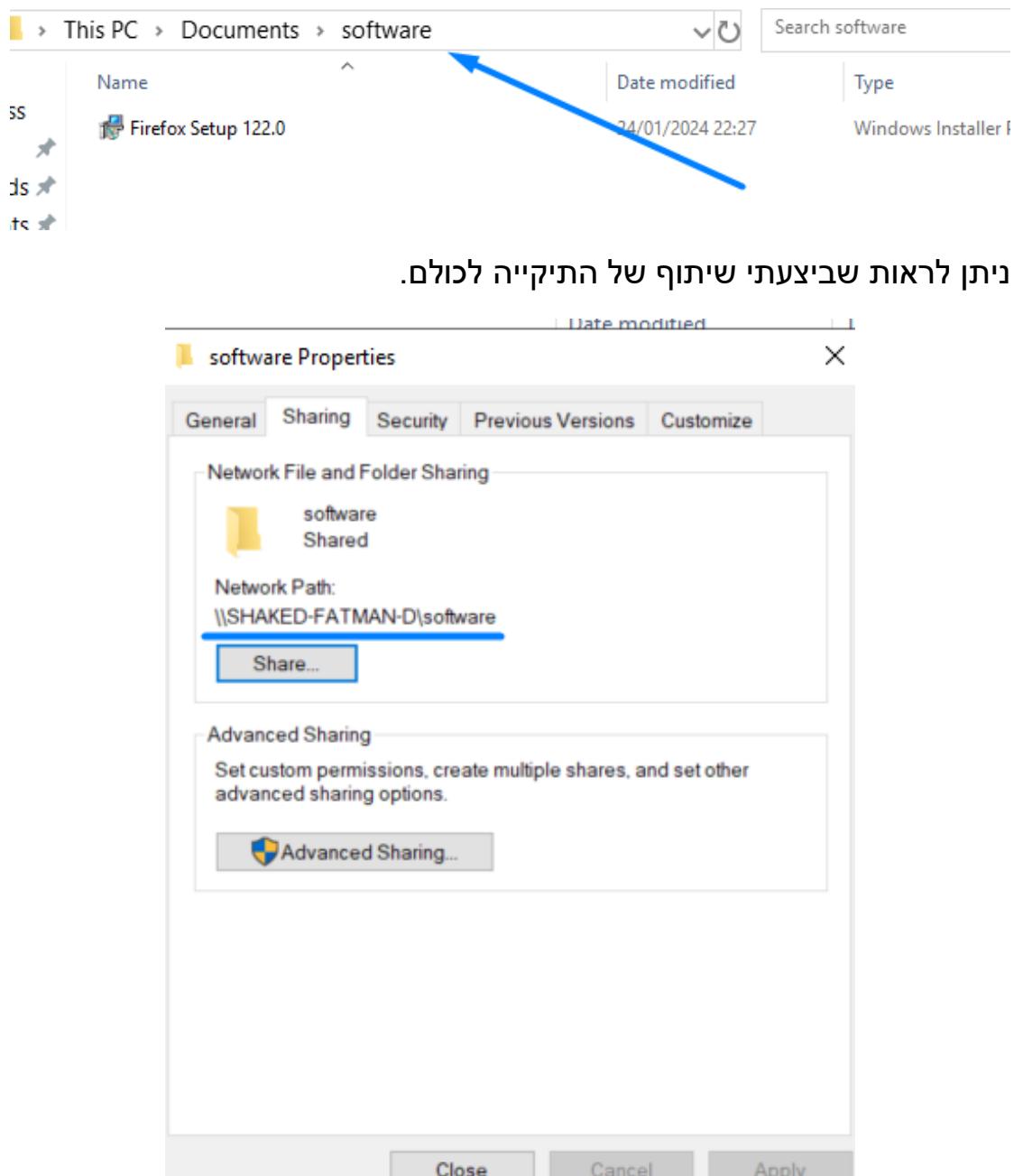
נגישות למשתמשים מוגבלים, Sys Admins, תחת Administrators, נספח



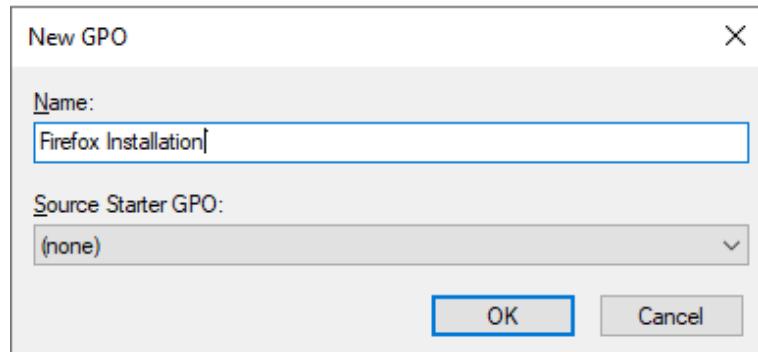
כעת יש לנו מסך עם אדמינים וINSI Sys Admins, גויסף את Sys Admins תחת Admins

The screenshot shows the 'Administrators Properties' dialog box. At the top, it displays two groups: 'Administrators' and 'SHAKED-FATMAN\Sys_Admin'. The main area is titled 'Configure Membership for Administrators'. Under 'Members of this group:', the entry 'SHAKED-FATMAN\Sys_Admin' is listed, with 'Add...' and 'Remove' buttons next to it. Below that, under 'This group is a member of:', there is a note: '<The groups to which this group belongs should not be modified>' followed by 'Add...' and 'Remove' buttons. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

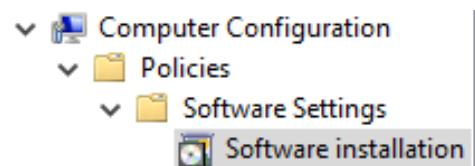
התקנת תוכנה על גבי כל מחשבי הארגון ללא מעורבות אדם.
 ■ הגדר ע"י GPO התקנה של תוכנה ע"ג מחשבי הארגון ללא מעורבות אדם.
 דבר ראשון צריך למצוא התקנת תוכנה שמשתמשה בהורדת MSI, להחטי את הדףן המקורי Firefox, ונשים אותו בתיקייה משותפת.



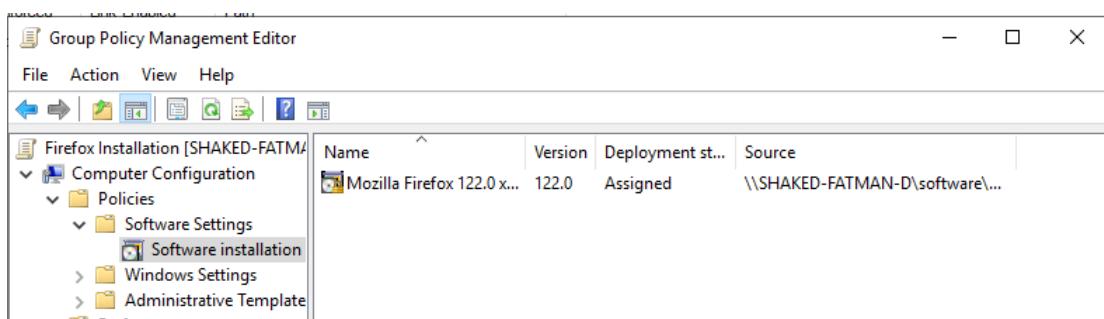
וניצור GPO חדש, נקרא לו התקנת FIREFOX.



נבחר בSoftware Installation.



מוסיף לההתקינה של Mozilla Firefox.



ונתן את הGPO לכלום בארגון

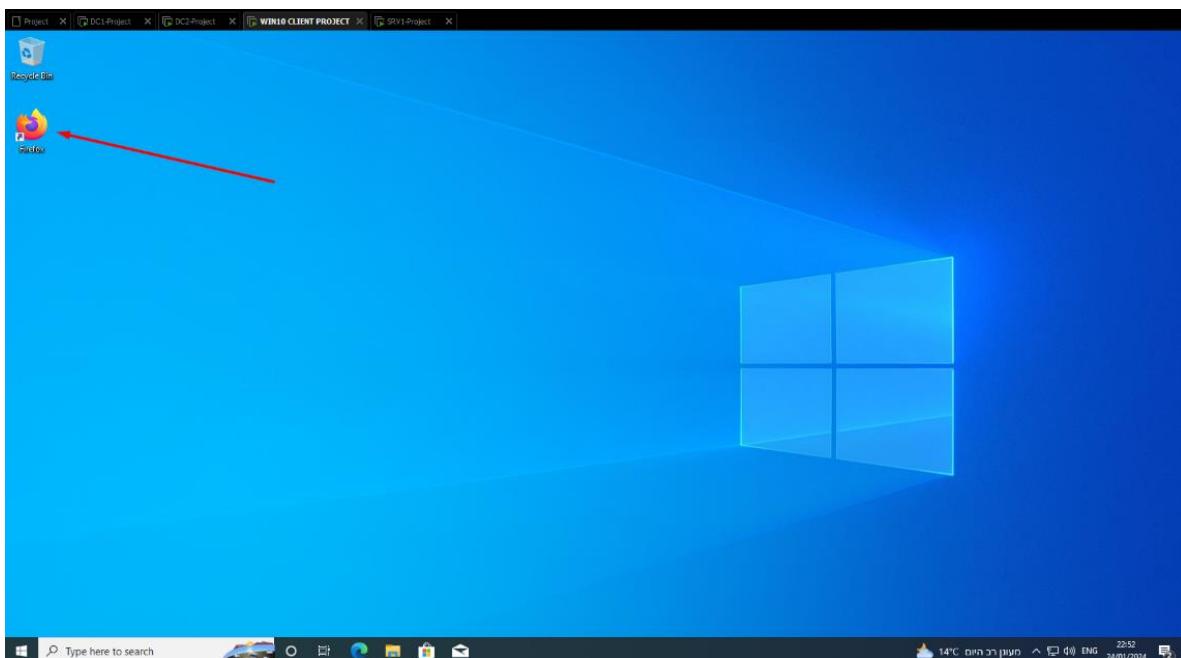
Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name



כעת נתחבר לפרויקט כלשהו רק כדי לבדוק שעובד, בוינדוז 10



ניתן לראות את Firefox פה, ללא מגע אדם!

מדיניות סיסמה

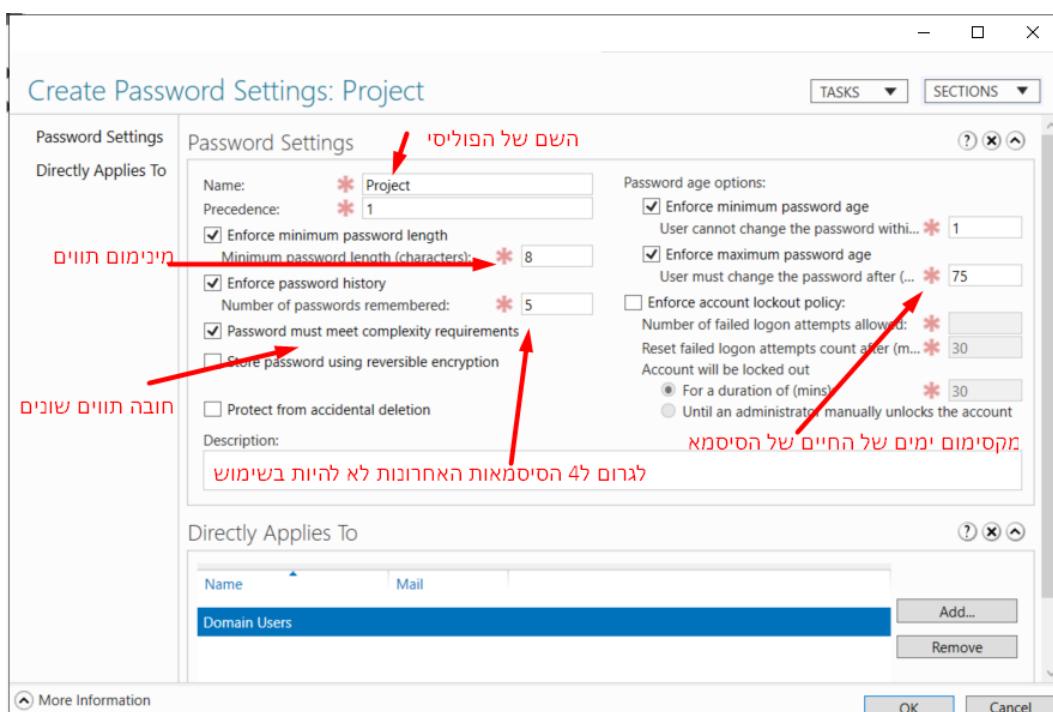
כעת נתchia את מדיניות סיסמה

מדיניות סיסמות בארגון:

צור מדיניות סיסמה לפי התנאים הבאים:

- אורך סיסמה 8 תווים
- מחייב שילוב של מספר סוגים תווים
- לא ניתן להשתמש ב 4 סיסמות אחרונות
- תוקף סיסמה 75 ימים.

כעת נגדיר Policy חדש נקרא לו פרויקט

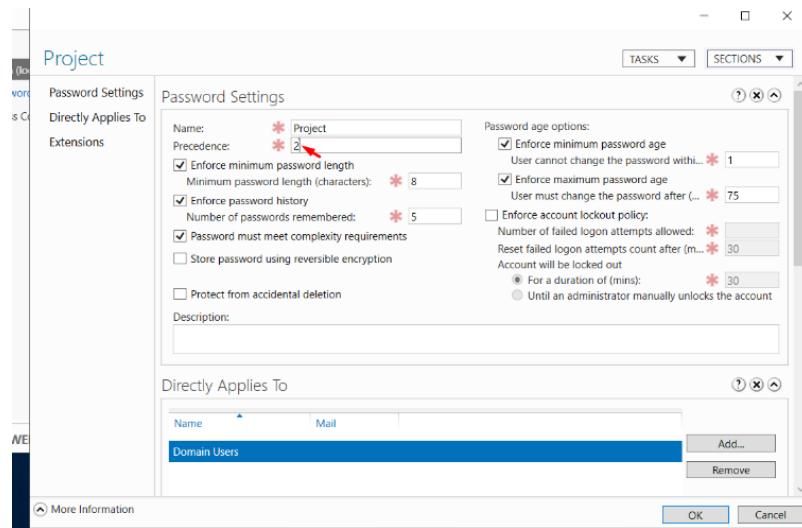


מטלת בונוס

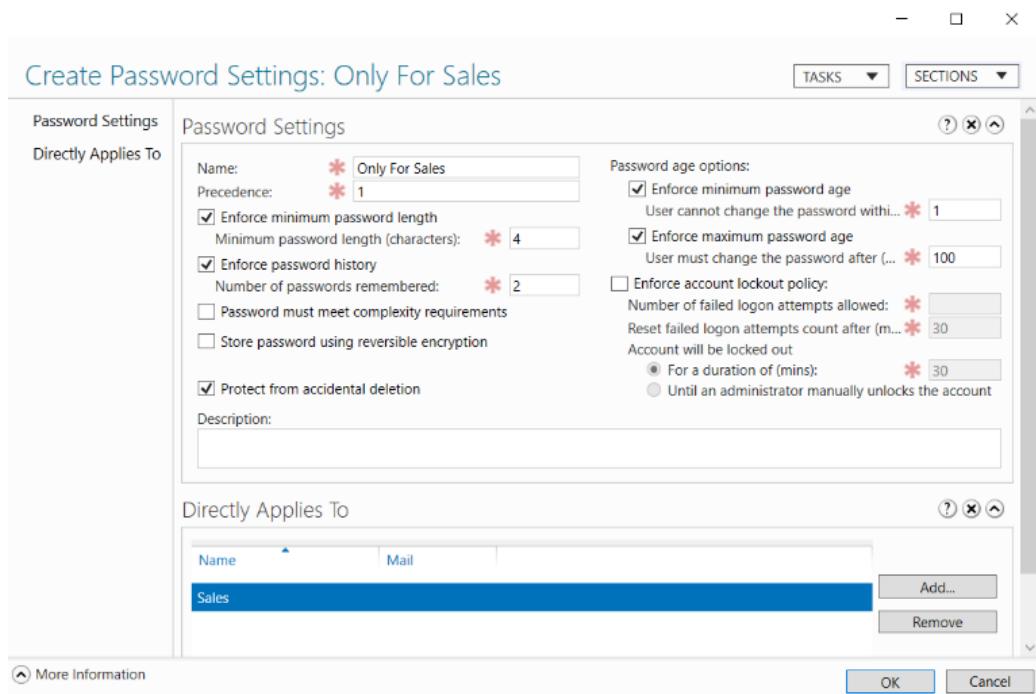
אם כבר אנחנו פה, נעשה את המטלת בונוס.

נוריד את Precedence של מה שעשינו קודם, ל2, ויצור חדש, נשים לו Precedence 1, אך ניתן את המדריניות סיסמאות אך ורק לSales. (Sales קובע את סדר ההעדפה של מדיניות סיסמאות. מדיניות עם Precedence גבוהה יותר תתגבר על מדיניות עם נמוך יותר)

להלן השינוי ל2:



להלן השינוי שביבענו, אך ורק למחלקה Sales, כתת מינימום תווים יהיה בשכילים 4, לעומת 8 לכולם, לא ניתן להשתמש בסיסמה האחורונה ששומשה, לעומת הגדרה שיש לכולם, שלא יכולים להשתמש ב-4 הסיסמות האחרונות, והמקסימום ימימן שסיסמה יכולה להיות קיימת לשימוש, היא מאה ימים, לעומת שבעים וחמשה של כולם. תנאים מקלים יותר ל-Sales בלבד כמובן.



להלן ניהול הסיסמות שיש לנו כרגע, לפי העדיפות.

	Name	Precedence	Type	Description
<input checked="" type="checkbox"/>	Only For Sales	1	Password S...	
<input checked="" type="checkbox"/>	Project	2	Password S...	

שיתופים ומיפויים

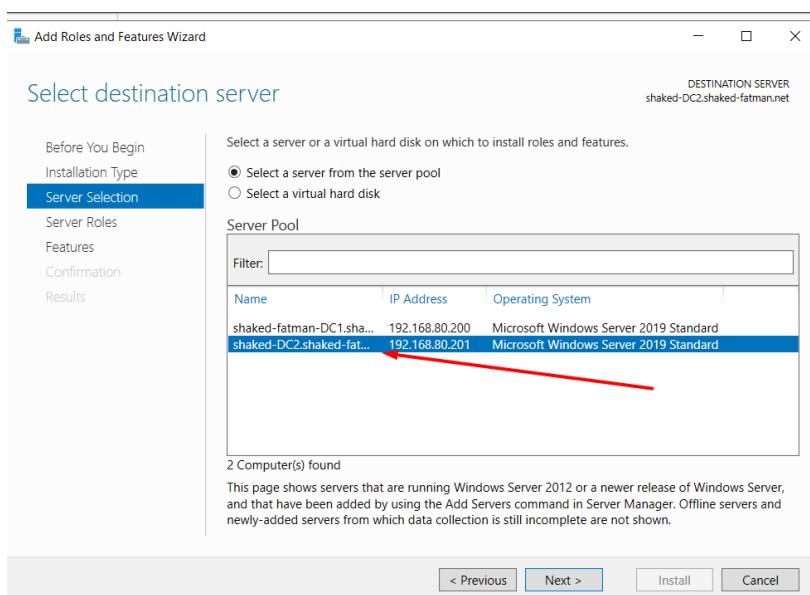
הגדרת DC2 כשרת קבצים

- הגדיר את שרת DC2 כשרת קבצים – (התקנות Role) { במידה ושרת DC2 הותקן כוותקן ניתן}
- להגדיר שרת הקבצים יהיה שרת DC1 }

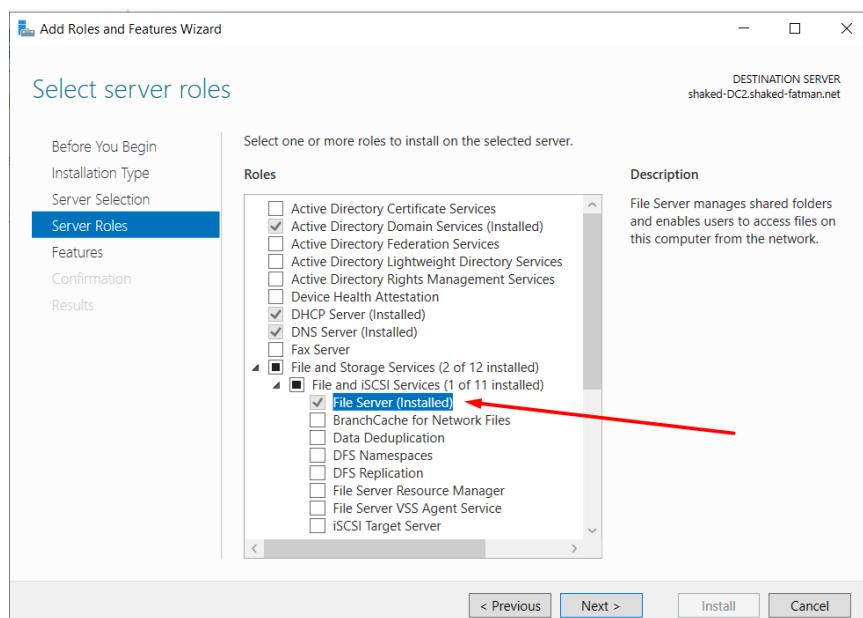
דבר ראשון שנעשה, זה הורדת רול של File Server.

טוב אז מסתבר שיש לי כבר את הרול אבל הצעדים להורדת הרול הם כאלה:

בחירת DC2



הורדת File Server

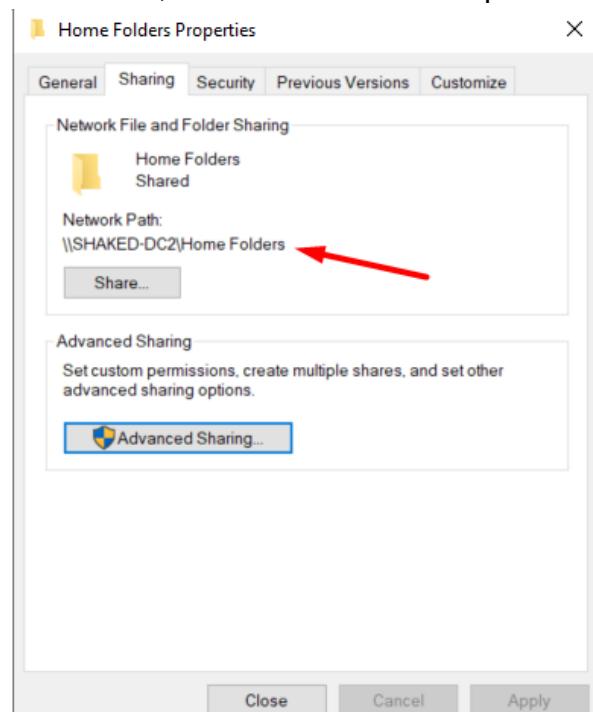


הגדרת Home Folder למשתמש

הגדרת Home Folder - הגדר לכ 5 חשבונות Home Folder. עליך לוודא כי כל משתמש נגיש ל-Home folder שלו בלבב.

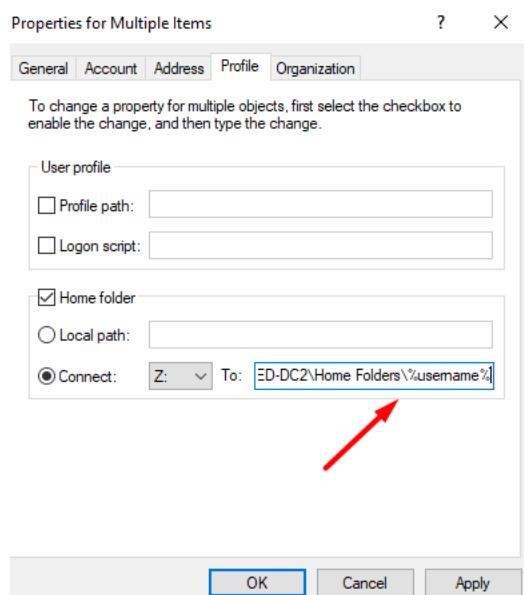
תיקית בית (Home Folder) היא תיקייה שבדרך כלל קיימת במערכות הפעלה שיש בהן הרבה משתמשים, שמכילות קבצים של משתמש כל שהוא במערכת. תיקית הבית היא מקום לאחסון קבצים אישיים של המשתמש.

עת הצורך ליצור Home Folder ב-dc2, וליצור לה שיתוף ברשות.



בחר חמשה משתמש

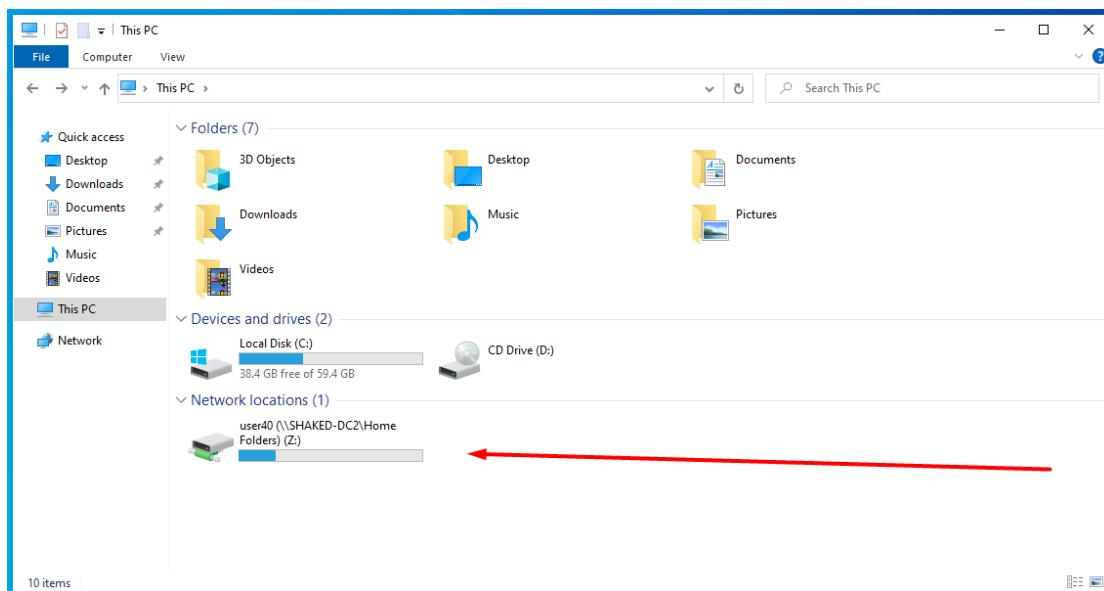
 user40	User
 user41	User
 user42	User
 user43	User
 user44	User



ונעשה שיפתח לכל USER, הום פולדר משולן %USERNAME% זה משתנה, שמכיל שם משתמש נכון, באופן אוטומטי, לאחר שנלחץ על אוקי', המערכת תיצור תיקית בית עבור כל המשתמשים שנבחרו

נתחבר ליזר 40

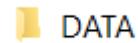
וכעת נראה שיש לנו תיקית בית במיוחד ליזר 40



יצירת תיקייה משותפת ב-DC2

- שיתוף תיקייה - צור ב- DC2 תיקייה משותפת בשם DATA. {במידה ושרת DC2 הותקן כ-NET-Server Core ניתן להגדיר בשרת DC1 קובץ txt} צור בתוך התיקייה קובץ txt.
- ניהול הרשאות - דאג לכך שגם היו הרשותות הגישה לתיקייה המשותפת: הרשות Modify לקבוצת Sys_Admins והרשות Read & execute לקבוצת Sales. צור כי הרשותות שיתוף הין הרשותות משולבות.

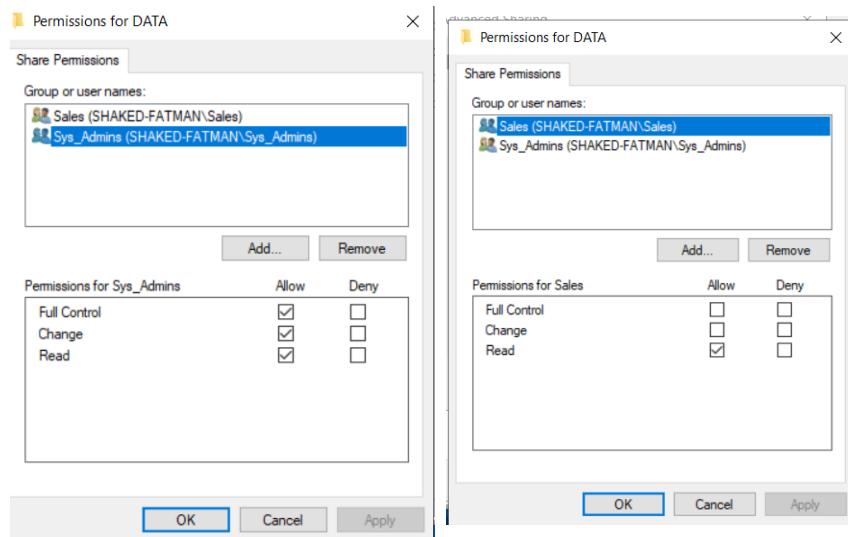
נוצר כעט תיקייה, נקרא לה DATA כמו שביקשו, כמובן שהכל יהיה על DC2



נוצר בתיקייה, קובץ טקסט

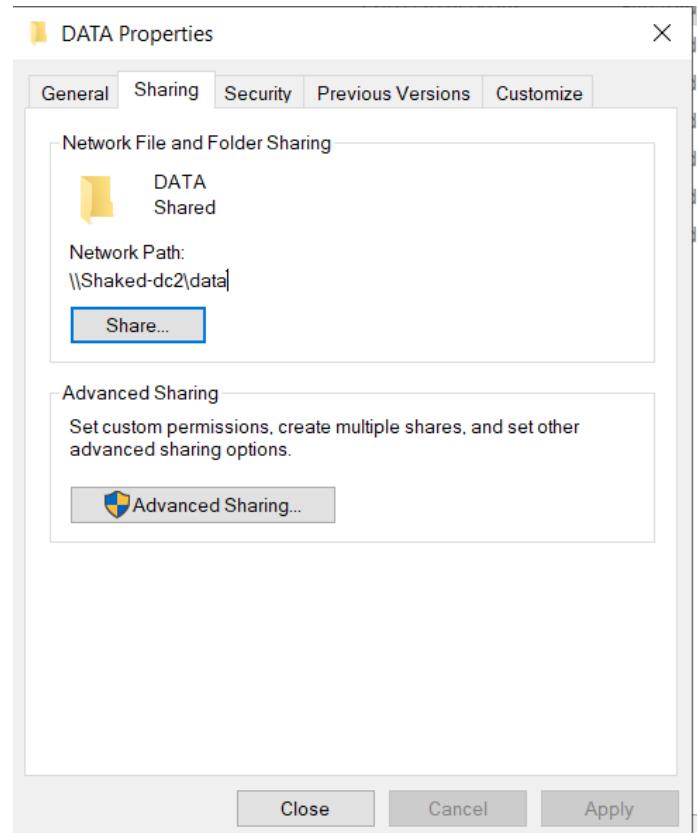


ניתן הרשותות כמו שהתבקשו בהנחיות

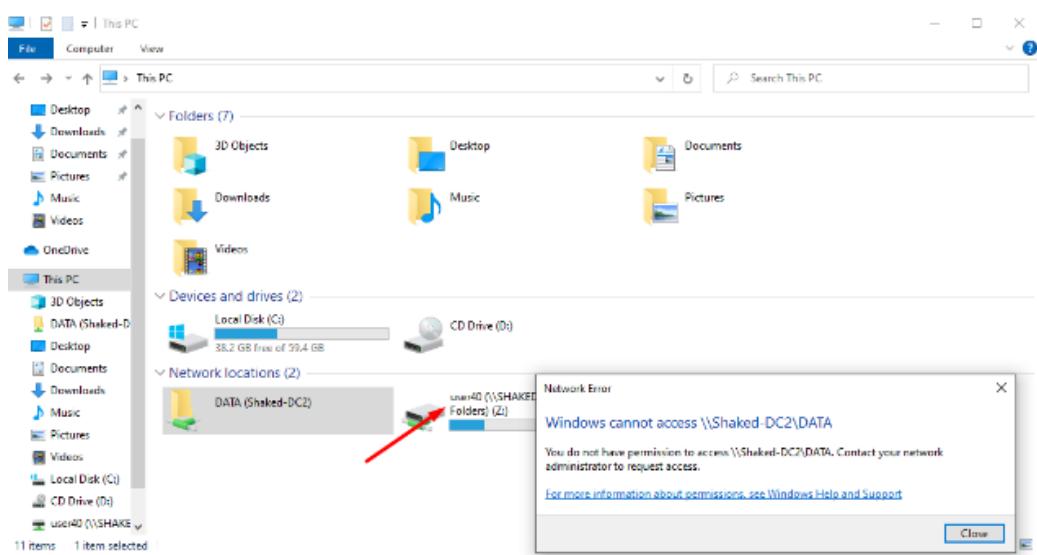


מיפוי כונן רשות

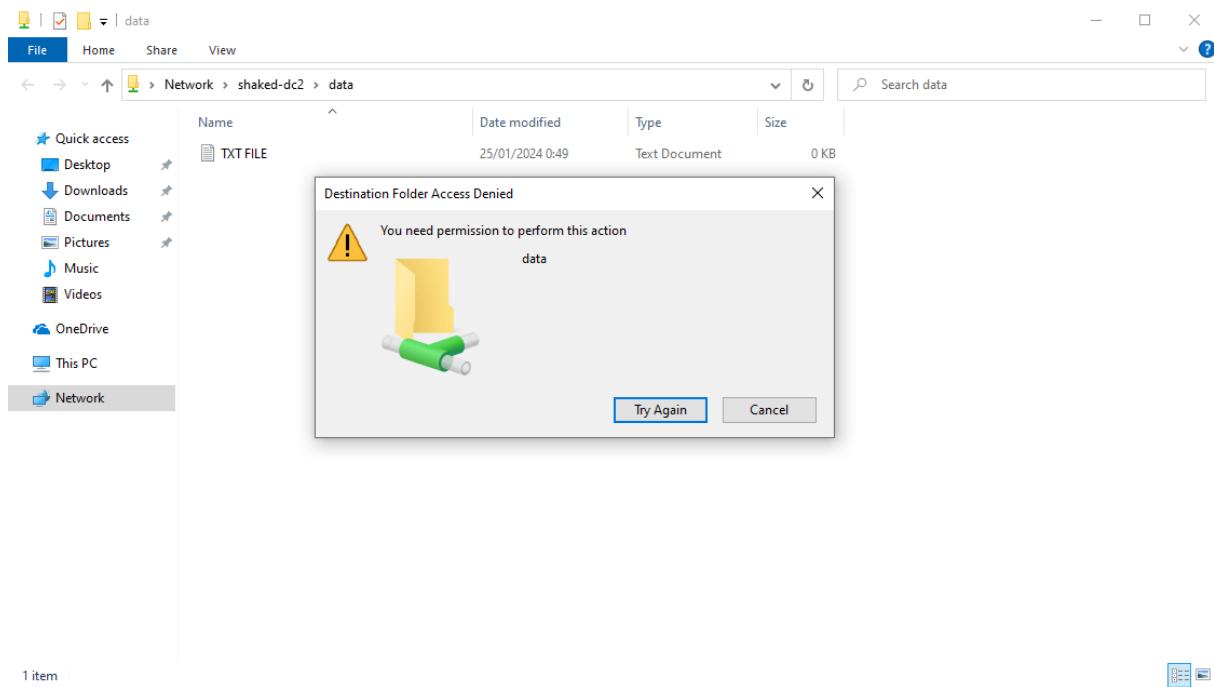
מיפוי כונן רשות - מפה את התיקיה לכל המשתמשים ובודק שההרשאות שלהם נכונות. את הבדיקה בוצע דרך WIN10.



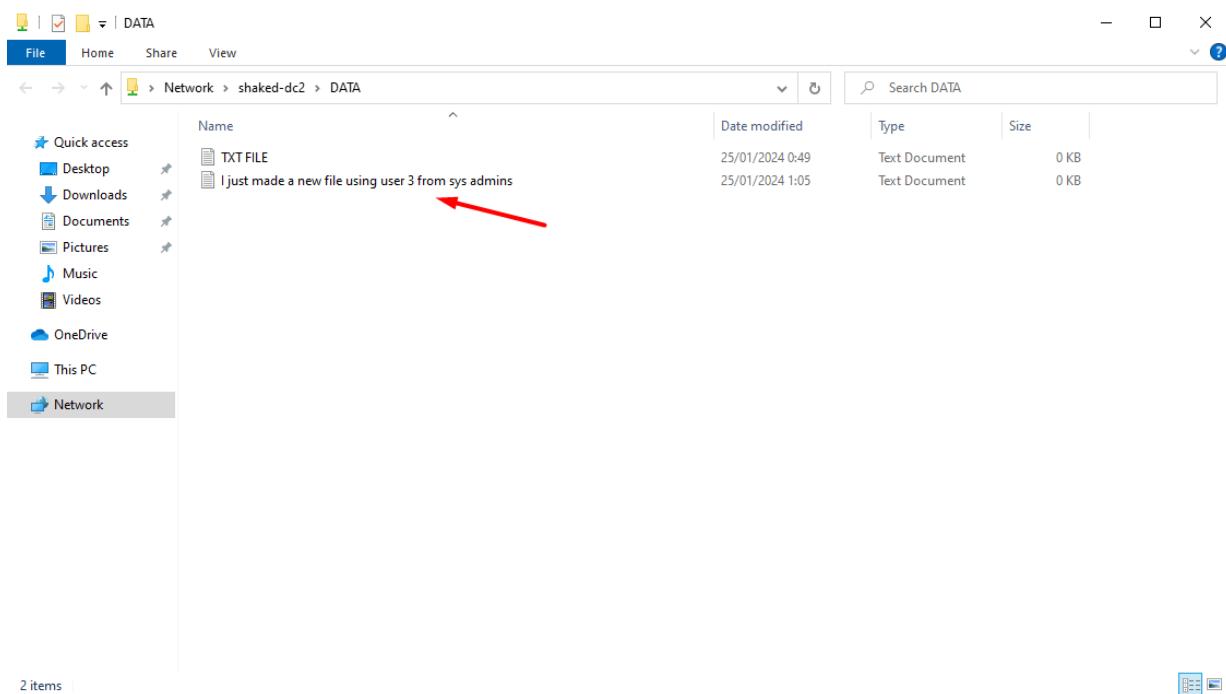
מיפויו את התיקיה לרשות, יוצר 40 לא נכנס לתיקיה, מאחר ואין לו הרשאות



דרך משתמש **Sales**, לא ניתן לבצע שינוי.



דרך משתמש **Sys Admins**, אפשר לעשות הכל.

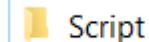


יצירת תיקייה משותפת נוספת בשם סקריפט

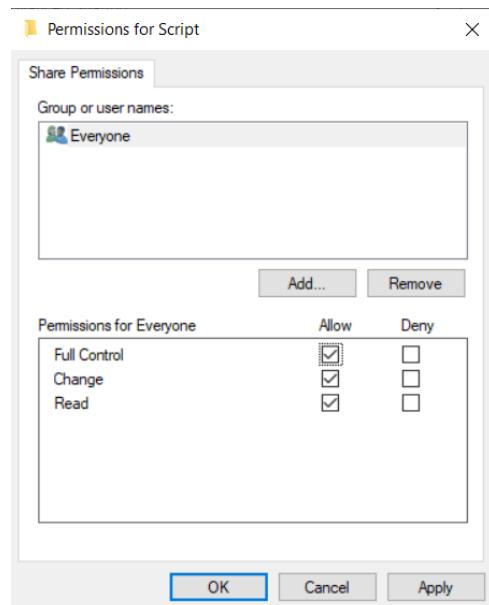
צור תיקייה משותפת נוספת DC2 בשם Script. {במידה ושרת DC2 הותקן כ Server Core ניתן להגדיר בשרת DC1}

תן הרשות Modify לקבוצת Everyone. צור בתוכה קובץ Batch שהמשתמש יפעיל ושיבצע את מיפוי תיקיית data ככונן הרשות עבור המשתמש (השתמש בפקודה net use).

נתחיל מייצרת תיקיה משותפת



ונתן לכלום גישה לעשוות הכל בתיקייה



כעת ניצור את הקובץ BAT, זה מה שייהי כתוב בקובץ



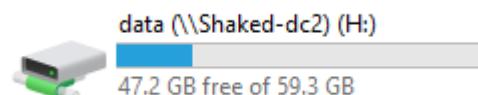
File Edit Format View Help
net use H: \\Shaked-dc2\data\

הקובץ:

Name

script.bat

עובד!



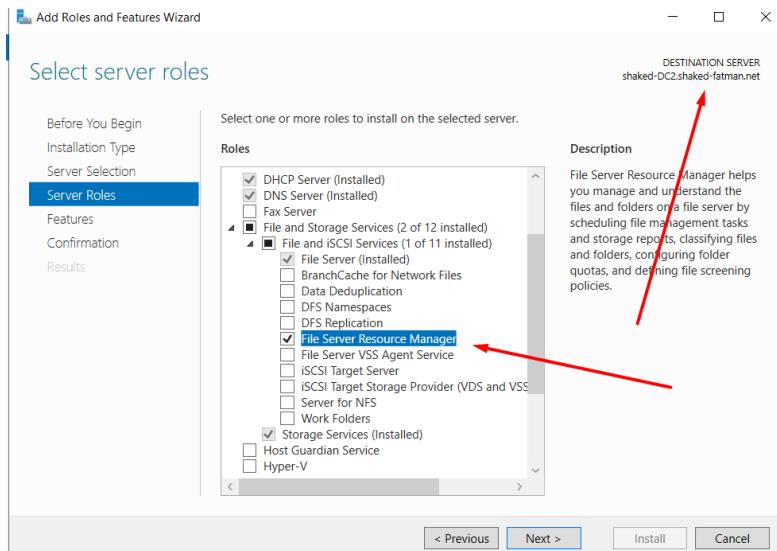
יצירת מכסה, והגבלת שמירה קבצי AVI

- צור מכסה Quota לנפח השימוש של כל משתמש בתיקיות ה Home Folder עד 5GB ומונע מהמשתמשים לשומר קבצי AVI בתיקיות אלו.

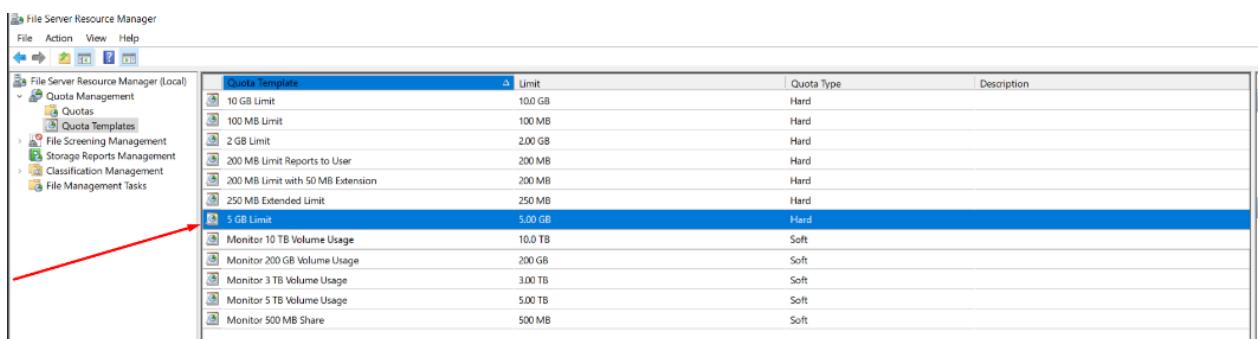
מה ש Quota יעשה, יגביל לכל משתמש, לשומר עד חמישה גיגה בית, בתיקית ההום פolder שלו.

נתחיל מיצירת המכסה

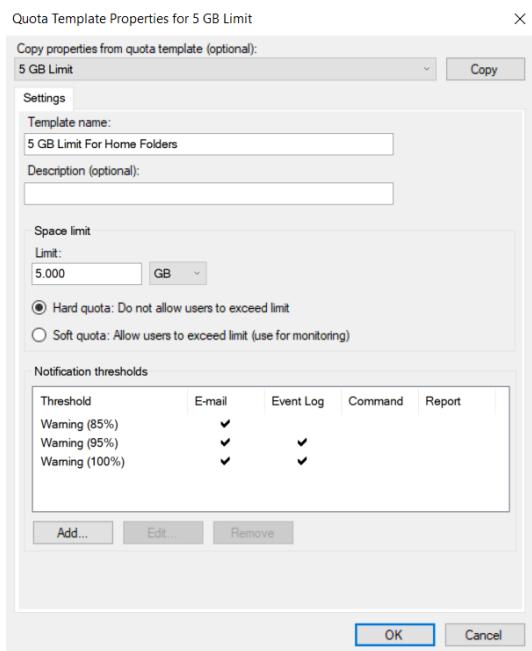
לצורך התחלת יצירת מכסות צריך להוריד DC2 ל File Server Resource Manager



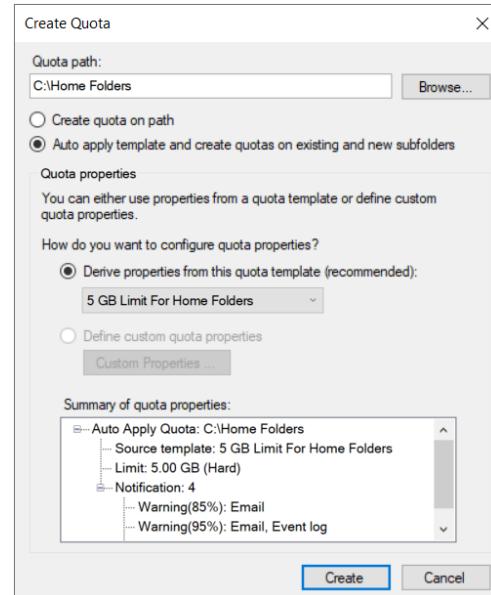
לאחר שהורדנו, נוכל לבחור בתבנית של 5 גיגה



נמשיך עם ההגדלה זו, בדיק מה שאנו צריכים



וביצור מגבלה נפרדת לכל משתמש.

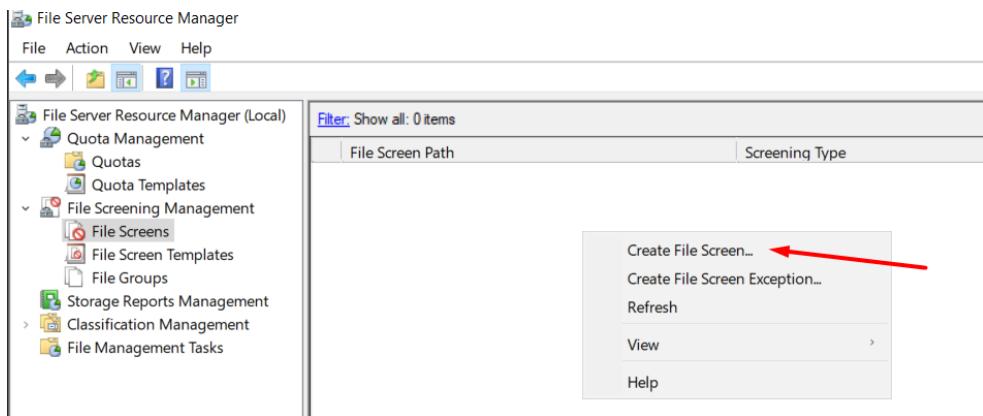


כעת ניתן לראות, שיש מגבלה לכל תיקייה, שיש לכל יוזר.

C:\Home Folders\user40	0%	5.00 GB	Hard	5 GB Limit For Home Folders	Yes
C:\Home Folders\user41	0%	5.00 GB	Hard	5 GB Limit For Home Folders	Yes
C:\Home Folders\user42	0%	5.00 GB	Hard	5 GB Limit For Home Folders	Yes
C:\Home Folders\user43	0%	5.00 GB	Hard	5 GB Limit For Home Folders	Yes
C:\Home Folders\user44	0%	5.00 GB	Hard	5 GB Limit For Home Folders	Yes

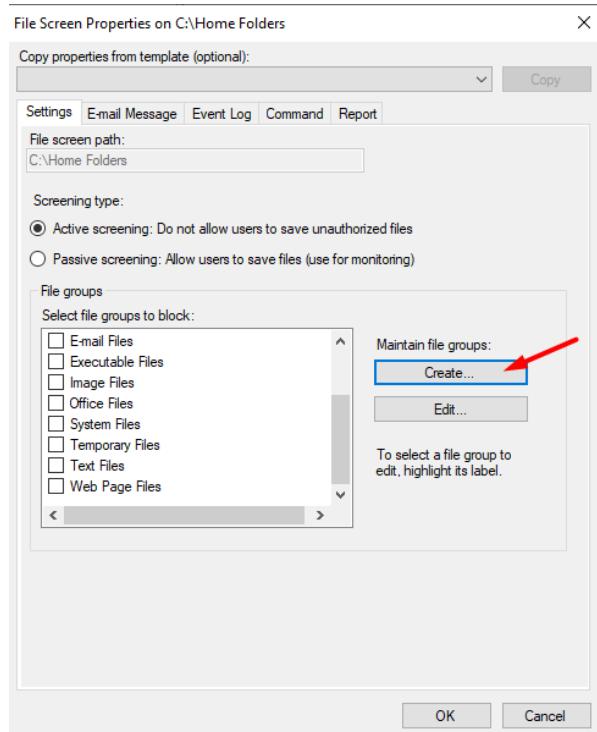
כעת נמנע את האופציה לשמר קבצי AVI

בכדי להתחיל, נctrar לפתוח File Screen חדש.

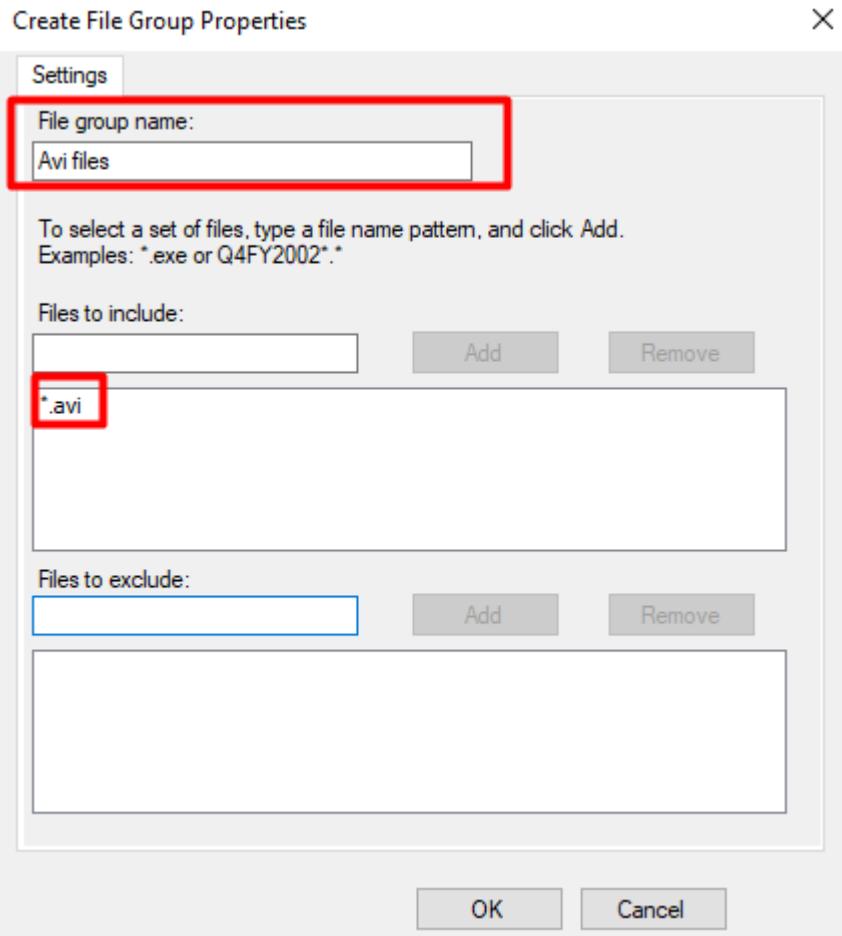


נctrar ליצור קבוצה חדשה, שתחסום קבצי AVI

נעשה Create



לאחר שיצרנו, יקופץ לנו חלון, שבו נצטרך להגדיר את הקובץ בקבוצה, נצטרך לכתוב כוכבית, ואז נקבעה וסימת הקובץ, בשביל שייעבוד לנו כראוי.



וניתן לו את הקבוצה של קבצי AVI

Create File Screen

File screen path: C:\Home Folders

File screen properties
You can either use properties from a file screen template or define custom file screen properties.

How do you want to configure file screen properties?

- Derive properties from this file screen template (recommended):
- Define custom file screen properties:

Summary of file screen properties:

- File screen: C:\Home Folders
- Screening type: Active
- File groups: Avi files
- Notifications:

File Screen Properties on C:\Home Folders

Copy properties from template (optional): Block Audio and Video Files

File screen path: C:\Home Folders

Screening type: Active screening: Do not allow users to save unauthorized files Passive screening: Allow users to save files (use for monitoring)

File groups

Select file groups to block: Avi files (highlighted with a red arrow)

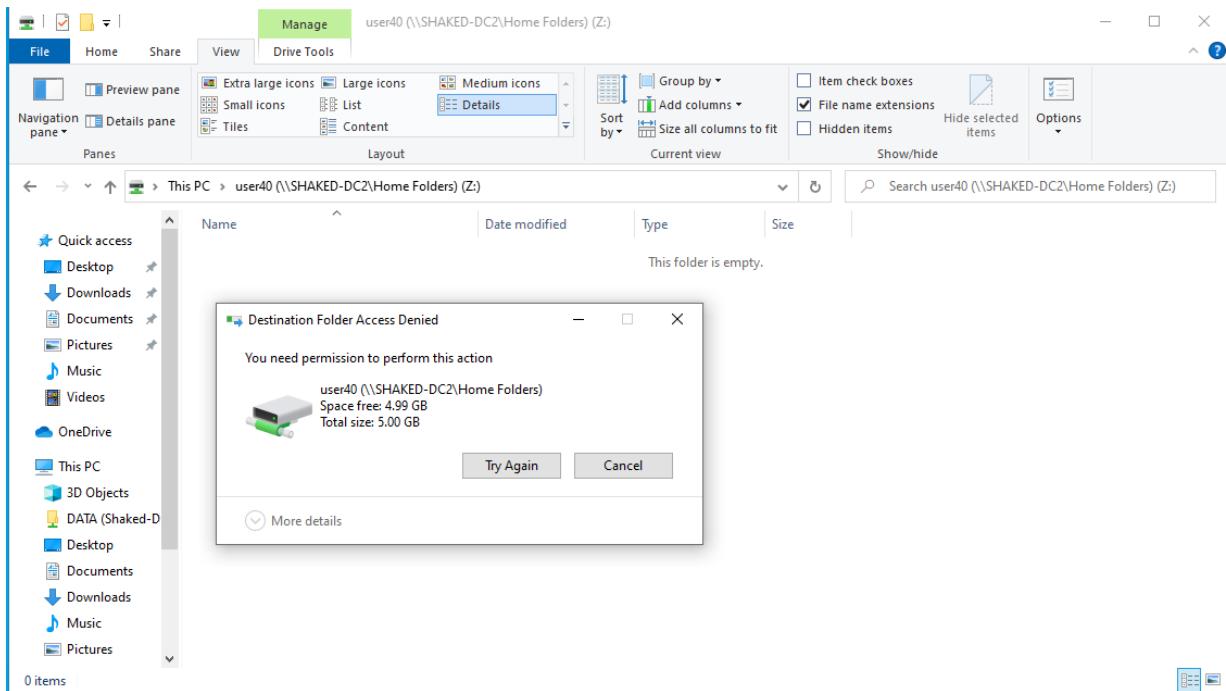
Maintain file groups:

To select a file group to edit, highlight its label.

הכינוטי מראש "ממש במקרה" קובץ AVI בוינדוז 10



ולא עובד! כמו שתכננו!



מאמר בנגע למדיניות סיסמה – שקד אוריאל ברמי - איך מיקרוסופט ואסוס מגינות על המשתמשים שלו

מדיניות סיסמה היא חלק חשוב מאבטחת המידע. סיסמות חזקות יכולות לעזור להגן על המשתמשים מפני פריצה. שתי חברות גדולות, מיקרוסופט ואסוס, משתמשות במדיניות סיסמה דומות. אך ככל אופן, יש כמה הבדלים מרכזים בין המדיניות שלהן.

אוריך הסיסמה

ההבדל המרכזי בין מדיניות הסיסמה של מיקרוסופט לאסוס הוא אוריך הסיסמה המינימלי. מיקרוסופט דורשת סיסמות באורך של לפחות 12 תווים, בעוד שאסוס דורשת סיסמות באורך של לפחות 8 תווים.

אוריך הסיסמה הוא גורם חשוב בשמירה על הסיסמה חזקה. סיסמות ארוכות יותר קשות יותר לפריצה. על פי מחקר של אוניברסיטת קנטבררי אשר נמצא זילנד, סיסמות באורך של 12 תווים או יותר הן הרבה פחות פראזות מסיסמות בעלות 8 תווים, בrama של סיסמות בעלות 12 תווים מוערכות להיות חזקות פי 13 מיליון מאשר סיסמות בעלות שמונה תווים, אם שתי החברות היו משכילות להשתמש בסיסמה בעלת 16 תווים לפחות, היה הרבה יותר קשה לפרוץ למשתמשים, על פי אותה אוניברסיטה שידרנו עליה קודם סיסמה של 16 תווים מוערכת חזקה פי 166 טריליאון מסיסמה של 8 תווים.

הדרישה של מיקרוסופט לשיסמות באורך של לפחות 12 תווים היא עילה יותר להגנה על המשתמשים מפני פריצה. עם זאת, היא עלולה גם להפוך את החיים למשתמשים מעט יותר מורכבים. סיסמות ארוכות יותר קשות לזכור, והרבה משתמשים ישתמשו במנהל סיסמות, ואם יהיה פרצת אבטחה לשרת של מנהל הסיסמות, יהיה אסון גדול, לאחר וכל המשתמשים שימושים במנהל סיסמות, יחו דליפה קשה של המידע שלהם, לגורמים נוספים בראשת, הרבה לא נוטים לחשב על זה, אך אם נסתכל על נתונים בפועל, לפי האתר HAVEIBEENPWNED, רק הם יודעים על 13 ביליאון חשבונות, והפרט הכל מפתיע זה שחצי מיליארד חשבונות, אשר הוזלפו באופן פתוח לרשות, הוזלפו מחברת פיסבוק העולמית!. מיותר לציין שמאח אחוז מהמשתמשים שחובנים הוזלף, חוות פריצה לפחות פעם אחת מנוקודת ההדלה, אז אכן דליפת מידע זה אופציית הגיונית, ושימוש במנהל סיסמות לא מומלץ.

הכללים לסוג הסיסמה

שתי החברות דורשות שישים סיסמות כדי לפחות גדולה, אותן קטנה, מספר וטו סימן. עם זאת, מיקרוסופט דורשת גם שישים סיסמות לא יהיה שם המשתמש של המשתמש, שמות של בני משפחה או חברים, מילים או ביטויים נפוצים, או רצף של תווים, אחר זה מורייד את העניין של סיכוי הפריצה למשתמש, אם הסיסמה תהיה אותו הדבר כמו שם המשתמש, זה קל מדי, ומתקפת ברוט פורס (ניסיון לפרוץ לחשבון על ידי ניסיון כל האפשרויות האפשריות לסיסמה), תהיה מיותרת.

הכללים הנוספים של מיקרוסופט יעילים יותר להגנה על המשתמשים מפני פריצה. עם זאת, הם עשויים גם להגביל את האפשרויות של המשתמשים ליצור סיסמות. לדוגמה, יתכן שהמשתמשים יתאפשרו לחשב על סיסמה חזקה שאינה שם המשתמש שלהם או מילה או ביטוי נפוץ.

השפעות על המשתמשים

המדיניות של מיקרוסופט ואסוס הן ייעילות להגנה על המשתמשים מפני פריצה. עם זאת, יתכן שהן יהפכו את החיים למשתמשים מעט יותר מורכבים.

אורק הסיסמה המינימלי של 12 תווים של מיקרוסופט עשוי להיות קשה לזכור עבור חלק מהמשתמשים. כמו כן, הכלל של מיקרוסופט שאסור על שימוש במידע קל לנחש עשוי להגביל את האפשרויות של המשתמשים לצירוף סיסמות.

ניתן להסתכל על כך ישירות בrama מאוד בסיסית, המדיניות של מיקרוסופט בהחלט בא להגן על המשתמשים יותר מאשר אסוס מפני פריצה, בכלל אופן, כלל שהסיסמא יותר ארוכה, ככל הנראה המשתמש יתקשה יותר לזכור את הסיסמה, מעבר לזכור של המשתמש, יש גם את היצירתיות שבאה לידי ביטוי כאשר אנו יוצרים סיסמות, ואם באים למשתמש עם תנאים "קשהים" מדי, יהיה קשה מאוד למשתמש ליצור סיסמה, במיוחד שהוא יזכור אותה.

השוואה למיניות סיסמה של הממשל האמריקאי

לפי בارد, הבינה המלאכותית של גול, למשל האמריקאי, יש את המדיניות החזקה ביותר בעולם, אך כאשר ישbstי וקראתו את המדיניות של הממשל האמריקאי, גיליתי שהיא ממש דומה לזה של מיקרוסופט, שניהם דורשים מהמשתמש 12 תווים לפחות, דרישות גם אחרות, כגון קטנה, מספר, וטו סימן, שניהם אוסרות להשתמש בשם המשתמש השם המשתמש, שמות של בני משפחה, או של קרוביים אחרים, אך בכלל אופן מה ההבדל העיקרי ביןיהן, הרי לא יכול להיות שלממשל האמריקאי ולמיקרוסופט יהיו את אותן הדרישות לסיסמה, אך הבנתי שהממשלה האמריקאית ממש פועלת בדרכים שונות, בכך שלא יהיה מידע איש בנסיבות, לדוגמה, הממשלה האמריקאית מציע הכשרות לאנשי IT ממשלתיים בנושא אבטחת מידע, בנוסף לכך, הממשלה האמריקאית משתמש בכלים טכנולוגיים כדי לבדוק את אבטחת הסיסמות של סוכניות ממשלתיות.

ולסיכום

הבנו שמדיניות הסיסמה של מיקרוסופט ואסוס הן ייעילות להגנה על המשתמשים מפני פריצה. עם זאת, הן עשויות גם להוות אתגר עבור המשתמשים. אבל הדרישה של מיקרוסופט לסיסמות באורך של לפחות 12 תווים היא יעה בהרבה יותר להגנה על המשתמשים מפני פריצה. עם זאת, היא גם דורשת מהמשתמשים לזכור סיסמה ארוכה יותר, מה שעלול להיות מתגרא. הכללים הנוספים של מיקרוסופט שאסורים על שימוש במידע שקל לנחש אותו גם הם יעלים יותר להגנה על המשתמשים מפני פריצה. עם זאת, הם גם מגבילים את האפשרויות של המשתמשים לצירוף סיסמות. מה שהבנו בכלל אופן, ומה שאני אישית למדתי במהלך כתיבת המאמר זהה, שיותר לא אסתכל אף פעם על הדרישות המינימליות שבקשיים ממוני, מהיום, משתמש במינימום 16 תווים בסיסמה.

מקורות מידע:

בארד

מה המדיניות סיסמה של חנות אסое היא כדרקון:

סיטוט אחרות

- הסיסמה חייבת להיות באורך של לפחות 8 תווים.
- הסיסמה חייבת להכיל לפחות 1 אות גדולה, 1 אות קטנה, 1 מספר ו-1 תו מיוחד.
- הסיסמה לא יכולה להיות שם המשתמש של המשתמש, או שמות של בני משפחה או חברים.
- הסיסמה לא יכולה להיות מיליה או ביטוי נפוצים.
- הסיסמה לא יכולה להיות מורכבת רק מרצף של תווים.

מה הנהלים הנוכחיים של מיקרוסופט מיקראוסופט

הנהלים הנוכחיים של מיקרוסופט ליצור סיסמאות חזקות הם כדלקמן:

- הסיסמה חייבת להיות באורך של לפחות 12 תווים.
- הסיסמה חייבת להכיל לפחות 1 אות גדולה, 1 אות קטנה, 1 מספר ו-1 תו מיוחד.
- הסיסמה לא יכולה להיות שם המשתמש של המשתמש, או שמות של בני משפחה או חברים.
- הסיסמה לא יכולה להיות מיליה או ביטוי נפוצים.
- הסיסמה לא יכולה להיות מורכבת רק מרצף של תווים.

למי יש את המדיניות סיסמה החזקה ביותר בעולם, לדעתך, ותתן לי פרטים.

לדעתי, ל-ממשלה אמריקאי יש את המדיניות סיסמה החזקה ביותר בעולם. המדיניות מחייבת את כל העובדים הפדרליים לשתמש בסיסמאות באורך של לפחות 12 תווים, כולל לפחות 1 אות גדולה, 1 אות קטנה, 1 מספר ו-1 תו מיוחד. סיסמאות לא יכולות להיות שם המשתמש של המשתמש, שמות של בני משפחה או חברים, מילים או ביטויים נפוצים, או רצף של תווים.

המדיניות של הממשלה האמריקאית היא עילוה מזו בדגנבה על סיסמאות מיפוי פיזיצית. מחקר של אוניברסיטת סטנפורד מצא כי סיסמאות באורך של 12 תווים או יותר הן פי 100 מיליאן חזקות יותר מסיסמאות באורך של 8 תווים.

המדיניות של הממשלה האמריקאית גם כן עילוה בהגבלה האפשרויות של התקפות פישינג. התקפות פישינג הן התקפות שבן האקרים מנוטם לנובב מידע איש על ידי שליחת דואר אלקטרוני מזויף. אם סיסמה מכילה מידע אישי, כגון שם של בן משפחה או תאריך הולדתו, האקרים יכולים להשתמש בכך כדי לנובב לפרטיו לחשבון.

עם זאת, המדיניות של הממשלה האמריקאית עשויה להיות קשה לממשכנים לזכור. סיסמאות באורך של 12 תווים או יותר הן 어렵ות יותר למסיכאות קצרות יותר, וזה יכול להיות קשה לזכור אותן.

אוניברסיטת קנטבררי שבניו זילנד:

[קישור למחקר בנוגע לארור סיסמאות](#)

אתר HAVEIBEENPWNED:

HAVEIBEENPWNED