

## תרגיל מעבדה 1 : תרגול סביבת ACTIVE DIRECTORY

בתור מנהלי הרשת של חברת TestLab התבקשתם להקים את אתר החברה בניו יורק, החברה הינה חברת Startup קטנה ולכן כרגע היא תכיל שני שרתי DC, ע"מ לחסוך במשאבים הוחלט ששרת אחד יהיה שרת CORE, את ניהול הדומיין תבצעו מהמשרד שלכם ממחשב החברה בו מותקנת מע' הפעלה ווינדוס 10. זיכרו שזהו הדומיין הראשון ביער הראשון. על מנת לחסוך רפליקציות מיותרות החלטתם לבצע IFM מהאתר בת"א לניו יורק. כמו כן קיבלתם משימה להכניס מספר רב של משתמשים ובחרתם לעשות זאת באמצעות קובץ CSV ו-Powershell. התבקשתם מבחינת רגולציה להעביר את התפקיד של domain - schema master naming אל השרת בניו יורק.

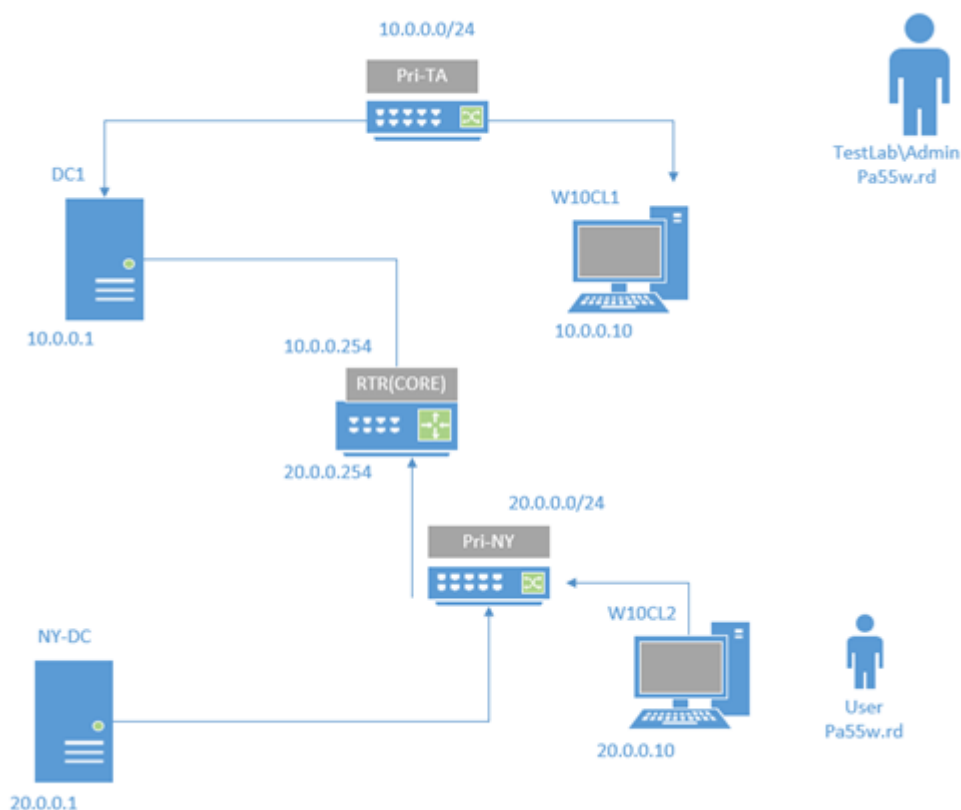
### בחלק זה של המעבדה תבצעו :

התקנה והקמה של דומיין, התקנת שרת DC, ביצוע IFM, העברת FSMO ROLES, חיבור מכונת ווינדוס 10 לדומיין והתקנת RSAT

### בחלק השני של המעבדה תבצעו :

הגדרות אתר (חיבור ורפליקציה), הגדרות קבוצות אבטחה והרשאות NTFS

### סכימה של הרשת שלנו (לאחר הרצת הסקריפטים)

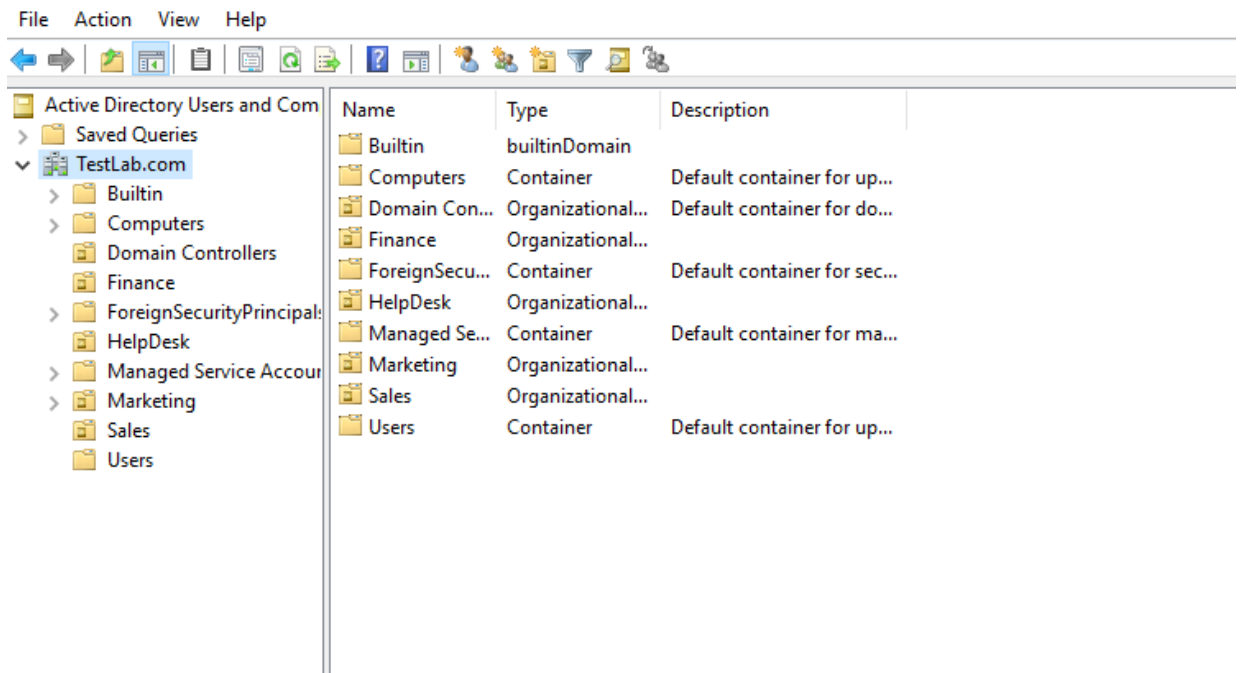


## תרגיל ראשון יצירת משתמשים מקובץ CSV

הסבר צעד אחר צעד כיצד לבנות את קובץ ה-CSV עבור יצירת משתמשים באופן אוט' בדומיין

שלב א': יצירת OU בדומיין :

באמצעות PS או בכלים גרפיים ניצור את היחידות הארגוניות שיכילו את המשתמשים שלנו



שלב ב': יצירת 100 משתמשים בצורה רנדומלית

האתר יוצר משתמשים בצורה רנדומלית: <https://www.fakenamegenerator.com/>

The screenshot shows the 'Order Bulk Identities' form on the Fake Name Generator website. The form includes a 'SPIN' wheel and a 'CONGRATULATIONS' message. The form steps are:

- Step 1 - Read and agree to terms of service**: ☒ I agree to the terms of service and understand that all generated information is fake.
- Step 2 - Choose output format and compression**:
  - Output Format: Comma separated (.csv)
  - Compression: .zip
- Step 3 - Choose name sets, countries, gender, and age**:
  - Name set: American, Arabic, Australian, Brazil, Chechen (Latin)
  - Country: Switzerland, Tunisia, United Kingdom, United States, Uruguay
  - Gender: Male: 50%, Female: 50%
  - Age: 20 - 65 years old
- Step 4 - Choose fields to include**:
  - Don't include these: Username, Password, Browser user agent, Telephone number, Telephone country code, Mother's maiden name, Birthday (m/d/yyyy), Age, Tropical zodiac, Credit card type
  - Include these: Given name, Surname, City, Street address

בחרתי שם, שם משפחה עיר, רחוב את כל השאר נשלים באקסל ... אני בוחר מאה משתמשים  
ע"מ לקבל את רשימת המשתמשים בצורה בטוחה – אני מכניס מייל מזויף שנוצר לי באתר הזה :

<https://emailfake.com>

## Fake Email Generator with your domain

You can write username and write or search domain that you like

test@work4uber.us



Copy

Waiting new emails for:

test@work4uber.us



All emails are displayed on this page automatically and instantly.

Address is valid (uptime 1 day)

נעתיק את כתובת המייל ונזין אותה באתר :

### Step 5 - Enter quantity & choose delivery options

You are allowed to have three (3) orders in the queue at a time.


Estimated wait: 10 minutes

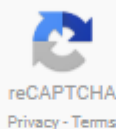
Quantity:  (Maximum: 50,000)

E-mail address:

### Step 6 - Type captcha

Tip: Sign in to avoid typing the captcha for future orders.

 I'm not a robot



Place your free order >>

נמתין לקבלת המייל שמאשר שהרשימה הוכנה להורדה :

From	Subject	Time (UTC)
jacob@fakenamegenerator.com	Your Fake Name Generator order is ready	2018-01-08 09:12:21

To: test@work4uber.us  
From: jacob@fakenamegenerator.com (sender info)  
Subject: Your Fake Name Generator order is ready  
Received: 2018-01-08 09:12:21 (3 sec.)

Delete Message

**FAKE NAME GENERATOR™**

**Your free order is ready**






Thank you for your recent order of generated identities from the [Fake Name Generator!](#)



Your freshly generated names can be downloaded at:  
<http://www.fakenamegenerator.com/pickup.php?order=d4277f66>

Your order will be available for 14 days. If you run into any problems, please do not hesitate to email us. We are happy to help in any way we can!

**Share**  
Have a friend or co-worker that needs the Fake Name Generator? Let them know!



**Unserialize**  
Quickly unserialize JSON and PHP serialized data online.  
[Learn more: Unserialize](#)



 **FakeNameGenerator.com\_d4277f66**  
 **FakeNameGenerator.com\_d4277f66**

נלחץ על הקישור ונוריד את הרשימה , נפתח את הקובץ המכוון וניגש לעריכה באקסל

Name

 FakeNameGenerator.com\_d4277f66  
 FakeNameGenerator.com\_d4277f66

FakeNameGenerator.com\_d4277f66 - Excel

GivenName	Surname	City	StreetAddress
Troy	Clayton	Seattle	1201 Union Street
Martha	Giddens	Arcadia	1287 Oakdale Avenue
Oscar	Moore	Newburg	1879 Fairfield Road
Jared	Williams	Oakland	3502 Clifford Street
Valerie	Carolina	Long Beach	2919 Clarence Court
Kathleen	Castro	Norcross	764 Mount Olive Road
Robert	Smith	Longview	3775 Scenicview Drive
Susan	Ford	Newport News	4316 Tenmile
Erika	Proctor	Harleysville	978 Burning Memory Lane
Jeffrey	Jobe	Irving	3930 Stoney Lane
Anthony	Mitchell	Norfolk	881 Jefferson Street
Kurt	Pickell	Goodlettsville	4616 Buffalo Creek Road
John	Hensley	Brentwood	4247 Feathers Hooves Drive
Susan	Boissonneault	Memphis	4215 Mapleview Drive
Nancy	Flores	Little Ferry	2318 Desert Broom Court
David	Bain	Paramount	953 Thompson Street
Daniel	Melendez	Forsyth	136 Twin House Lane
Robert	Hill	New York	3657 Oakwood Avenue
Mary	McCroskey	Fieldton	2842 Hilltop Drive
Benny	Babb	Monsey	1460 Pallet Street
Jennie	Therrien	Phoenix	1069 Griffin Street
Lawrence	Tom	Rocky Mount	1261 Green Acres Road
Carol	Beal	Warren	3955 Cherry Ridge Drive
Renata	Bryant	Overland	973 Rodney Street

מעט קריאה על הפקודה : New-ADuser תראה לנו שיש המון פרמטרים - חלקם דרושים וחלקם אופציונליים :

<https://technet.microsoft.com/en-us/library/ee617253.aspx>

אנו נשתמש לצורך הסקריפט במספר פרמטרים :

SamAccountName - שם האובייקט ב-AD – בקובץ אקסל ייקרא SAM

DisplayName – שם התצוגה – בקובץ אקסל ייקרא DISP

Path – מיקום האובייקט – בקובץ אקסל ייקרא - PATH

Department – מחלקה (שם זהה ל-OU) – בקובץ אקסל DEP

City - עיר מגורים –

Password - סיסמה – בקובץ אקסל PASS (בקובץ נדין את הסיסמה Pa55w.rd)

UserPrincipalName – שם ה LOGON שלו מכיל כבר את שם הדומיין - בקובץ אקסל UPN

GivenName	Surname	City	StreetAddress	SAM	UPN	DISP	DEP	PATH	PASS
Troy	Clayton	Seattle	1201 Union Street						
Martha	Giddens	Arcadia	1287 Oakdale Avenue						
Oscar	Moore	Newburg	1879 Fairfield Road						
Jared	Williams	Oakland	3502 Clifford Street						

בחברה שמות המשתמשים מורכבים מכל השם הפרטי + אות ראשונה של שם המשפחה

בעמודה SAM השתמשתי בפונקציה הבאה :

<https://support.office.com/en-us/article/Video-CONCATENATE-Function-in-Excel-2616d904-7410-4885-90db-a95f5bce6915?ui=en-US&rs=en-US&ad=US>

	GivenName	Surname	City	StreetAddress	SAM	UPN	DISP	DEP
1	Troy	Clayton	Seattle	1201 Union Street	=CONCATENATE(A2,LEFT(B2,1))			
2	Martha	Giddens	Arcadia	1287 Oakdale Avenue				

צור מחרוזת טקסט המכילה את כל מה שכתוב בתא A2 והוסף את האות הראשונה מצד שמאל של תא B2 .

העתקה פשוטה תביא לנו את הרשימה הבאה :

	GivenName	Surname	City	StreetAddress	SAM
1	Troy	Clayton	Seattle	1201 Union Street	TroyC
2	Martha	Giddens	Arcadia	1287 Oakdale Avenue	MarthaG
3	Oscar	Moore	Newburg	1879 Fairfield Road	OscarM
4	Jared	Williams	Oakland	3502 Clifford Street	JaredW
5	Valerie	Carolina	Long Beach	2919 Clarence Court	ValerieC
6	Kathleen	Castro	Norcross	764 Mount Olive Road	KathleenC
7	Robert	Smith	Longview	3775 Scenicview Drive	RobertS

ניגש ליצור את העמודה UPN שהיא זהה ל-SAM רק מכילה את שם הדומיין שלנו : "@testlab.local" (בתמונה הכיתוב שונה)

F2	=CONCATENATE(E2,"@Testlab.com")					
	A	B	C	D	E	F
1	GivenName	Surname	City	StreetAddress	SAM	UPN
2	Troy	Clayton	Seattle	1201 Union Street	TroyC	TroyC@Testlab.com

קח את מה שכתוב בעמודה SAM ותוסיף לו את הסיומת של הדומיין שלנו

נבצע העתקה לכל הקובץ

ונמשיך לעמודה הבאה : DISP

DisplayName – יורכב מהשם הפרטי+רווח+שם משפחה ולכן ניצור אותו בצורה הבאה :

	A	B	C	D	E	F	G	H	I
	GivenName	Surname	City	StreetAddress	SAM	UPN	DISP	DEP	PATH
1	Troy	Clayton	Seattle	1201 Union Street	TroyC	TroyC@Testlab.com	=CONCATENATE(A2," ",B2)		

הכנסנו שלושה ערכים – שם פרטי, ערך של רווח , שם משפחה

G2	=CONCATENATE(A2," ",B2)								
	A	B	C	D	E	F	G	H	I
1	GivenName	Surname	City	StreetAddress	SAM	UPN	DISP		
2	Troy	Clayton	Seattle	1201 Union Street	TroyC	TroyC@Testlab.com	Troy Clayton		
3	Martha	Giddens	Arcadia	1287 Oakdale Avenue	MarthaG	MarthaG@Testlab.com	Martha Giddens		
4	Oscar	Moore	Newburg	1879 Fairfield Road	OscarM	OscarM@Testlab.com	Oscar Moore		
5	Jared	Williams	Oakland	3502 Clifford Street	JaredW	JaredW@Testlab.com	Jared Williams		

את הערך מחלקה ניתן בצורה שירותית לפי המחלקות שלנו : אני חילקתי 25 משתמשים לכל מחלקה .

היות והמחלקה מקבילה בשמה ל-OU נוכל להשתמש בערך שלה ליצירת הנתבי :

(בתמונה הערך שונה) =CONCATENATE("OU=",H2,"",DC=Testlab,DC=LOCAL")

=CONCATENATE("OU=",H2,"",DC=Testlab,DC=Com")												
GivenName	Surname	City	StreetAddress	SAM	UPN	DISP	DEP	PATH	PASS			
Troy	Clayton	Seattle	1201 Union Street	TroyC	TroyC@Testlab.com	Troy Clayton	Sales	=CONCATENATE("OU=",H2,"",DC=Testlab,DC=				
Martha	Giddens	Arcadia	1287 Oakdale Avenue	MarthaG	MarthaG@Testlab.com	Martha Giddens	Sales	Com")				
Oscar	Moore	Newburg	1879 Fairfield Road	OscarM	OscarM@Testlab.com	Oscar Moore	Sales	CONCATENATE(text1, [text2], [text3], [text4], ...)				
Jared	Williams	Oakland	3502 Clifford Street	JaredW	JaredW@Testlab.com	Jared Williams	Sales					

חשוב מאוד לא לשכוח את הפסיק לפני DC

בערך PASS נעתיק לכולם את הסיסמה Pa55w.rd - בתמונה הערך שונה

Charles												
GivenName	Surname	City	StreetAddress	SAM	UPN	DISP	DEP	PATH	PASS			
Troy	Clayton	Seattle	1201 Union Street	TroyC	TroyC@Testlab.com	Troy Clayton	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Martha	Giddens	Arcadia	1287 Oakdale Avenue	MarthaG	MarthaG@Testlab.com	Martha Giddens	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Oscar	Moore	Newburg	1879 Fairfield Road	OscarM	OscarM@Testlab.com	Oscar Moore	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Jared	Williams	Oakland	3502 Clifford Street	JaredW	JaredW@Testlab.com	Jared Williams	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Valerie	Carolina	Long Beach	2919 Clarence Court	ValerieC	ValerieC@Testlab.com	Valerie Carolina	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Kathleen	Castro	Norcross	764 Mount Olive Road	KathleenC	KathleenC@Testlab.com	Kathleen Castro	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Robert	Smith	Longview	3775 Scenicview Drive	RobertS	RobertS@Testlab.com	Robert Smith	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Susan	Ford	Newport News	4316 Tenmile	SusanF	SusanF@Testlab.com	Susan Ford	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Erika	Proctor	Harleysville	978 Burning Memory Lane	ErikaP	ErikaP@Testlab.com	Erika Proctor	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Jeffrey	Jobe	Irving	3930 Stoney Lane	JeffreyJ	JeffreyJ@Testlab.com	Jeffrey Jobe	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Anthony	Mitchell	Norfolk	881 Jefferson Street	AnthonyM	AnthonyM@Testlab.com	Anthony Mitchell	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Kurt	Pickell	Goodlettsville	4616 Buffalo Creek Road	KurtP	KurtP@Testlab.com	Kurt Pickell	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
John	Hensley	Brentwood	4247 Feathers Hooves Drive	JohnH	JohnH@Testlab.com	John Hensley	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Susan	Boissonneault	Memphis	4215 Mapleview Drive	SusanB	SusanB@Testlab.com	Susan Boissonneault	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Nancy	Flores	Little Ferry	2318 Desert Broom Court	NancyF	NancyF@Testlab.com	Nancy Flores	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
David	Bain	Paramount	953 Thompson Street	DavidB	DavidB@Testlab.com	David Bain	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Daniel	Melendez	Forsyth	136 Twin House Lane	DanielM	DanielM@Testlab.com	Daniel Melendez	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Robert	Hill	New York	3657 Oakwood Avenue	RobertH	RobertH@Testlab.com	Robert Hill	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Mary	McCroskey	Fieldton	2842 Hilltop Drive	MaryM	MaryM@Testlab.com	Mary McCroskey	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Benny	Babb	Monsey	1460 Pallet Street	BennyB	BennyB@Testlab.com	Benny Babb	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Jennie	Therrien	Phoenix	1069 Griffin Street	JennieT	JennieT@Testlab.com	Jennie Therrien	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Lawrence	Tom	Rocky Mount	1261 Green Acres Road	LawrenceT	LawrenceT@Testlab.com	Lawrence Tom	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Carol	Beal	Warren	3955 Cherry Ridge Drive	CarolB	CarolB@Testlab.com	Carol Beal	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Renata	Bryant	Overland	973 Rodney Street	RenataB	RenataB@Testlab.com	Renata Bryant	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Michael	Salgado	Salt Lake City	4259 Hickory Street	MichaelS	MichaelS@Testlab.com	Michael Salgado	Sales	OU=Sales,DC=Testlab,DC=Com	Pa\$5w0rd			
Paulette	Parra	Huntsville	4172 Marcus Street	PauletteP	PauletteP@Testlab.com	Paulette Parra	Finance	OU=Finance,DC=Testlab,DC=Com	Pa\$5w0rd			
Cathy	Yarborough	Yorba Linda	4823 Sunny Day Drive	CathyY	CathyY@Testlab.com	Cathy Yarborough	Finance	OU=Finance,DC=Testlab,DC=Com	Pa\$5w0rd			
Erik	Moffit	Greenville	1050 Deer Haven Drive	ErikM	ErikM@Testlab.com	Erik Moffit	Finance	OU=Finance,DC=Testlab,DC=Com	Pa\$5w0rd			
Harold	Stradford	Chicago	4825 Jadewood Drive	HaroldS	HaroldS@Testlab.com	Harold Stradford	Finance	OU=Finance,DC=Testlab,DC=Com	Pa\$5w0rd			
Jeremy	Allen	Jacksonville	4236 Railroad Street	JeremyA	JeremyA@Testlab.com	Jeremy Allen	Finance	OU=Finance,DC=Testlab,DC=Com	Pa\$5w0rd			
George	Dismukes	Frederick	3709 Agriculture Lane	GeorgeD	GeorgeD@Testlab.com	George Dismukes	Finance	OU=Finance,DC=Testlab,DC=Com	Pa\$5w0rd			
Holly	Hewitt	Hempstead	2012 Stanley Avenue	HollyH	HollyH@Testlab.com	Holly Hewitt	Finance	OU=Finance,DC=Testlab,DC=Com	Pa\$5w0rd			
Calvin	Sanders	Jersey City	2429 Central Avenue	CalvinS	CalvinS@Testlab.com	Calvin Sanders	Finance	OU=Finance,DC=Testlab,DC=Com	Pa\$5w0rd			
Albert	Landreth	Westland	498 Lakeland Terrace	AlbertL	AlbertL@Testlab.com	Albert Landreth	Finance	OU=Finance,DC=Testlab,DC=Com	Pa\$5w0rd			
Mariah	Bigham	Waverly Hall	4994 Hart Country Lane	MariahB	MariahB@Testlab.com	Mariah Bigham	Finance	OU=Finance,DC=Testlab,DC=Com	Pa\$5w0rd			
Hye	Boyd	Julesburg	3696 Shobe Lane	HyeB	HyeB@Testlab.com	Hye Boyd	Finance	OU=Finance,DC=Testlab,DC=Com	Pa\$5w0rd			
Charles	George	Everett	1246 Stockert Hollow Road	CharlesG	CharlesG@Testlab.com	Charles George	Finance	OU=Finance,DC=Testlab,DC=Com	Pa\$5w0rd			
Bruce	Badger	Smithville	77 Rafe Lane	BruceB	BruceB@Testlab.com	Bruce Badger	Finance	OU=Finance,DC=Testlab,DC=Com	Pa\$5w0rd			

נעת נשמור את הקובץ בתור CSV ונעתיק אותו למכונה הוירטואלית DC1

File folder11/22/2017 12:42 ...W10C1L1DISK (H:)

LIST

שם הקובץ:

CSV (Comma delimited)

שמור כסוג:

Add a title :Title

Add a tag :Tags

Oz :Authors

ביטול

שמור

כלים

הסתר תיקיות



## שלב ד: יצירת הסקריפט

כאשר הקובץ נמצא בשרת DC נוכל לפתוח את PS ISE ולכתוב את הסקריפט בשורה אחת:

```
Import-Csv C:\list.csv | foreach-object { New-ADUser -Name $_.SAM -UserPrincipalName $_.UPN -SamAccountName $_.SAM -GivenName $_.GivenName -DisplayName $_.DISP -Surname $_.Surname -Department $_.DEP -StreetAddress $_.StreetAddress -City $_.City -Path $_.PATH -AccountPassword (ConvertTo-SecureString $_.PASS -AsPlainText -force) -Enabled $True -PasswordNeverExpires $True -PassThru }
```

שימו לב שביצענו התאמה של העמודות ב-CSV למאפיינים של הפקודה New-ADUser – הסבר מפורט במעבדה שקיבלתם

בסקריפט השתמשתי במאפיין PassThru – ע"מ לראות את הפלט:

```
SID : 5-1-5-21-1501844496-3948599087-3361619076-1202
Surname : Mayes
UserPrincipalName : BillM@Testlab.com

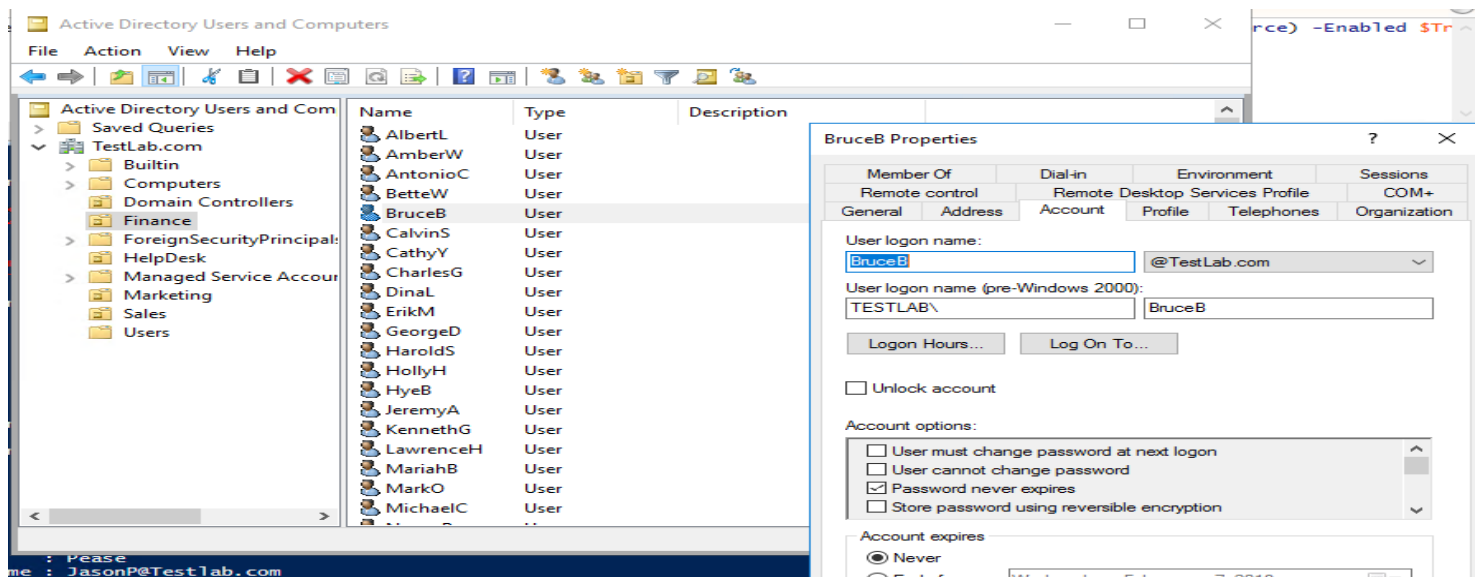
New-ADUser : The operation failed because UPN value provided for addition/modification is not unique forest-wide
At line:1 char:43
+ ... ch-object { New-ADUser -Name $_.SAM -UserPrincipalName $_.UPN -SamAcc ...
+ ~~~~~
+ CategoryInfo          : NotSpecified: (CN=RobertS,OU=M...=Testlab,DC=Com:String) [New-ADUser], ADException
+ FullyQualifiedErrorId : ActiveDirectoryServer:8648,Microsoft.ActiveDirectory.Management.Commands.NewADUser

DistinguishedName : CN=LynetteC,OU=Marketing,DC=Testlab,DC=Com
Enabled           : True
GivenName        : Lynette
Name             : LynetteC
ObjectClass      : user
ObjectGUID       : 4bcd3c05-7251-4e65-ab3f-b339d8497a0d
SamAccountName   : LynetteC
SID              : 5-1-5-21-1501844496-3948599087-3361619076-1203
Surname          : Calloway
UserPrincipalName : LynetteC@Testlab.com

DistinguishedName : CN=JasonP,OU=Marketing,DC=Testlab,DC=Com
Enabled           : True
GivenName        : Jason
Name             : JasonP
ObjectClass      : user
ObjectGUID       : 354fdada-b156-4c13-825a-16e3fb0b84a9
SamAccountName   : JasonP
SID              : 5-1-5-21-1501844496-3948599087-3361619076-1204
Surname          : Pease
UserPrincipalName : JasonP@Testlab.com
```

כמו שתוכלו לראות ישנן מס' התראות – ואם נקרא טוב נוכל להבין שהמשתמש לא נוצר כיוון שכבר קיים UPN כזה בדומיין ...

ניכנס לממשק הגרפי ונראה את המשתמשים בדומיין שלנו





בתור מנהל התשתיות בארגון החלטת לבדוק את האפשרות לחסוך רפליקציות ב-AD בזמן התקנת DC נוסף , בחרת להשתמש באפשרות לשכפל את ה-AD לקובץ בו אשר יישמש בשרת DC החדש כבסיס הנתונים וכל מה שיישאר לשרת החדש הינו להתעדכן בשינויים שחלו .

<https://technet.microsoft.com/en-us/library/cc770654.aspx>

בשרת DC1 ניכנס לממשק PowerShell עם הרשאות Administrator

ניצור תיקייה בשם C:\IFM

וניכנס לממשק ntdsutil

activate instance ntds

ifm

create full C:\ifm

```
PS C:\Users\Administrator> md C:\IFM

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          1/7/2018  10:15 AM             IFM

PS C:\Users\Administrator> ntdsutil
C:\Windows\system32\ntdsutil.exe: activate instance ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: ?

?                                - Show this help information
Create Full %s                  - Create IFM media for a full AD DC or an AD/LDS instance into folder %s
Create Full NoDefrag %s        - Create IFM media without defragmenting for a full AD DC or an AD/LDS instance i
er %s
Create RODC %s                 - Create IFM media for a Read-only DC into folder %s
Create Sysvol Full %s          - Create IFM media with SYSVOL for a full AD DC into folder %s
Create Sysvol Full NoDefrag %s - Create IFM media with SYSVOL and without defragmenting for a full AD DC into f
Create Sysvol RODC %s          - Create IFM media with SYSVOL for a Read-only DC into folder %s
Help                            - Show this help information
Quit                           - Return to the prior menu

ifm: create full C:\IFM
Creating snapshot...
Snapshot set {251092ce-01bd-422e-98ce-b8367e477038} generated successfully.
Snapshot {b8ae51c1-3e01-4669-a190-08401616549b} mounted as C:\$SNAP_201801071015_VOLUMEC$\
Snapshot {b8ae51c1-3e01-4669-a190-08401616549b} is already mounted.
Initiating DEFRAGMENTATION mode...
Source Database: C:\$SNAP_201801071015_VOLUMEC$\Windows\NTDS\ntds.dit
Target Database: C:\IFM\Active Directory\ntds.dit

Defragmentation Status (% complete)

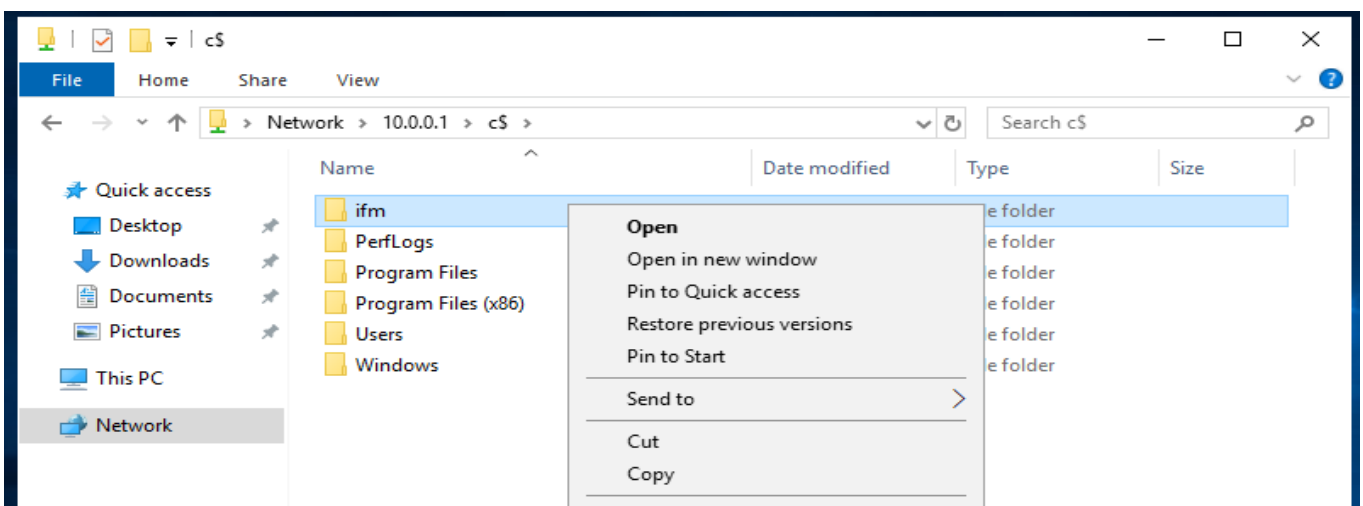
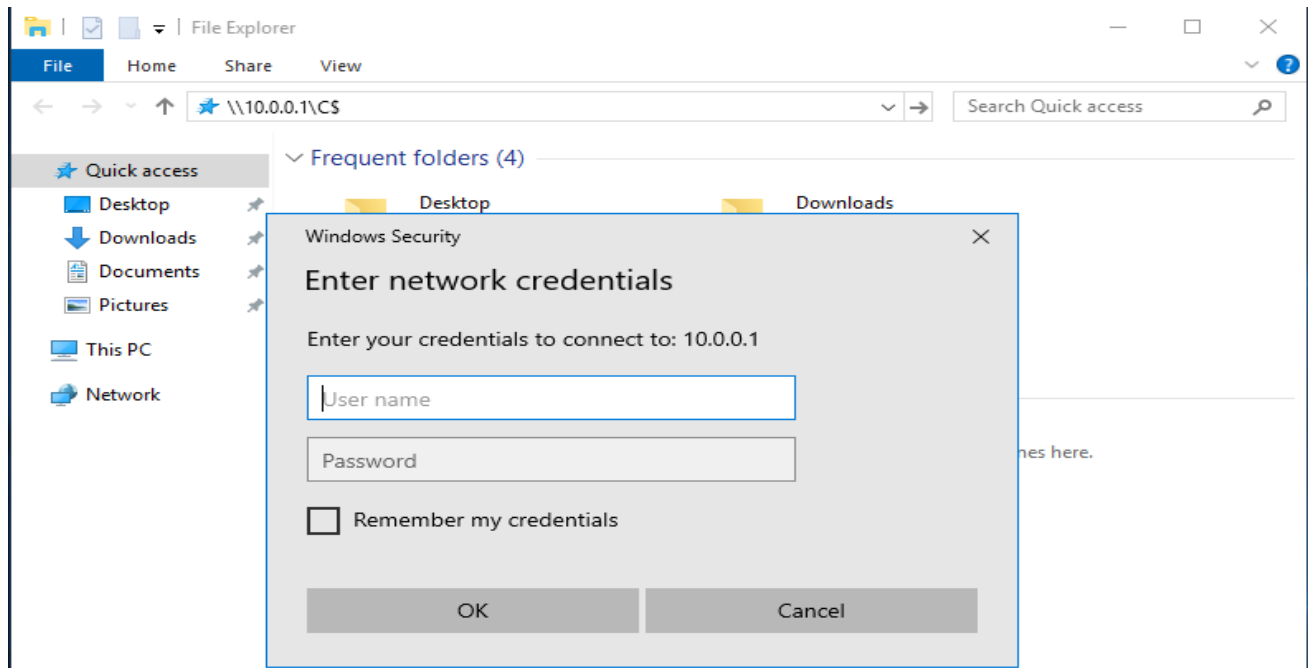
0   10  20  30  40  50  60  70  80  90 100
|---|---|---|---|---|---|---|---|---|---|
.....

Copying registry files...
Copying C:\IFM\registry\SYSTEM
Copying C:\IFM\registry\SECURITY
Snapshot {b8ae51c1-3e01-4669-a190-08401616549b} unmounted.
IFM media created successfully in C:\IFM
ifm:
```

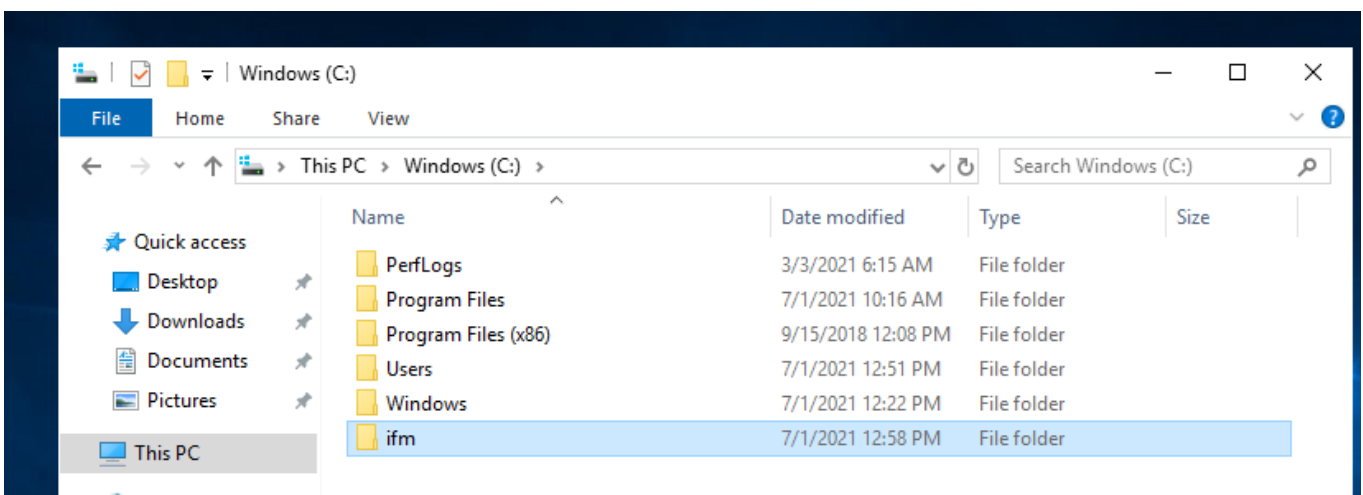
בסיום התהליך נבצע יציאה ע"י כתיבה של הפקודה quit פעמיים

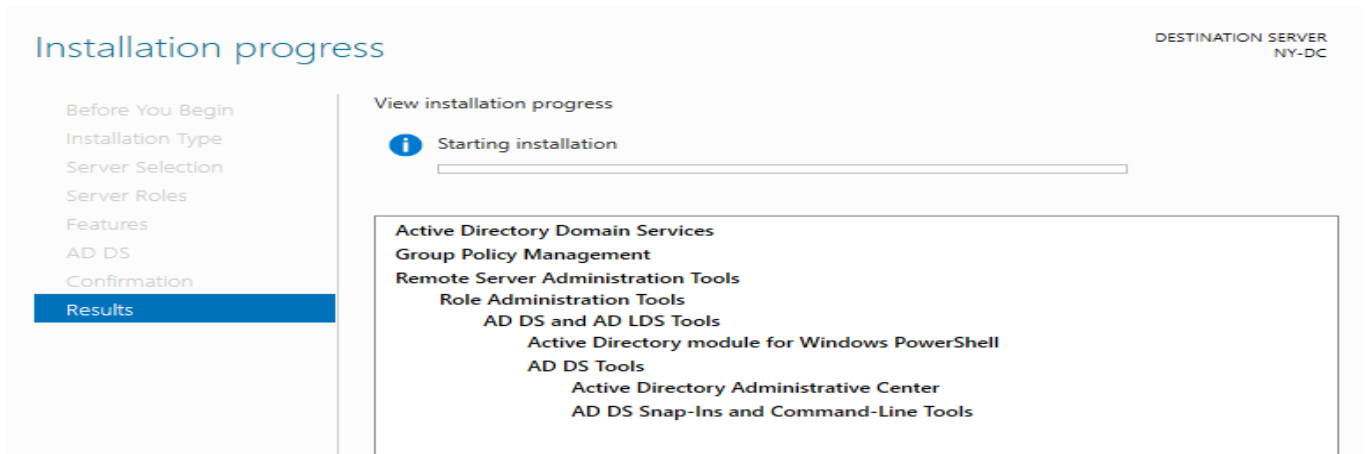
ניגש לתיקייה ונוודא שאכן נוצר לנו עותק של AD

ניגש אל המכונה NY-DC נתחבר עם המשתמש Administrator והסיסמה IPa55w.rd נעתיק לשם את תוכן התיקיה . ניכנס אל סייר הקבצים , נתחבר אל שרת DC1 באמצעות UNC PATH ונכניס את הרשאות Admin נסמן את התיקיה ונעתיק את כל תיקיית IFM אל הכונן המקומי

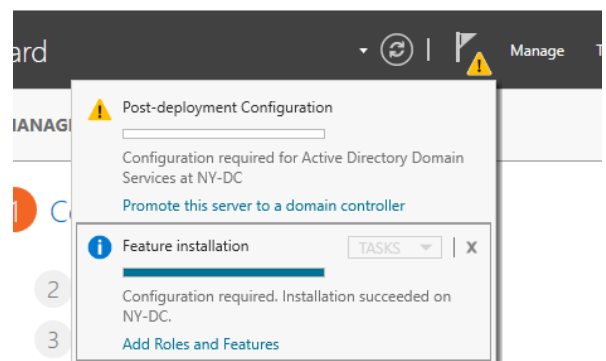


נבצע העתקה אל השרת המקומי

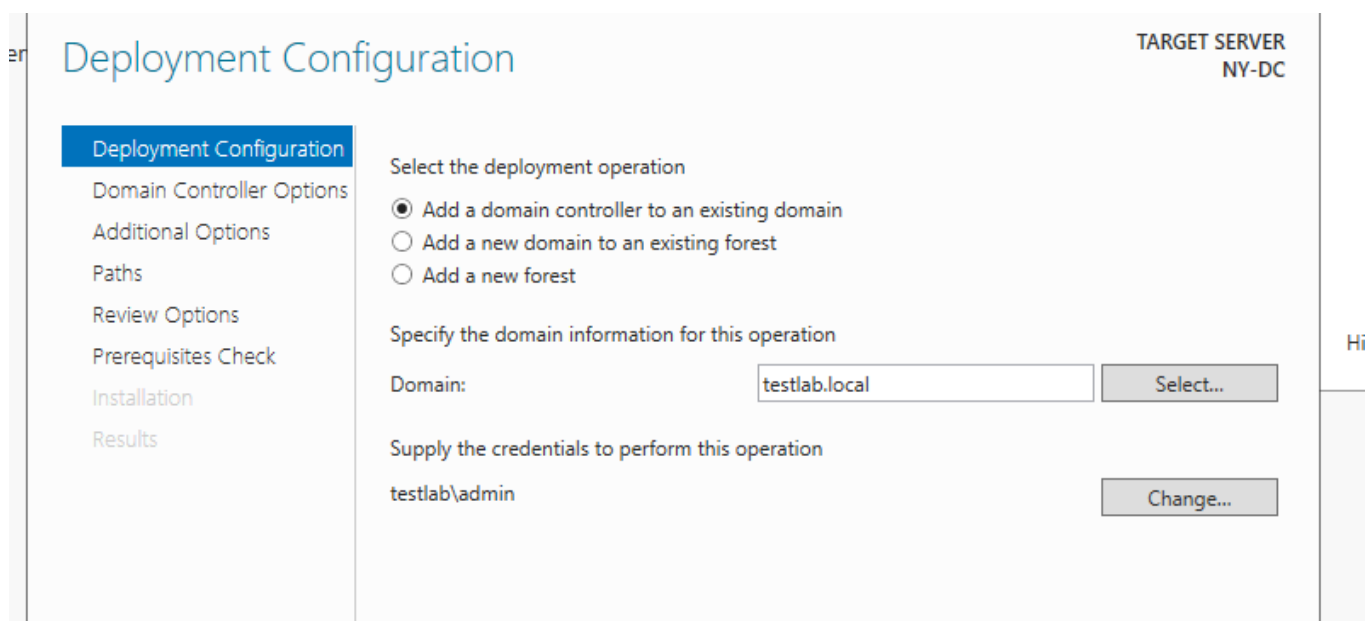
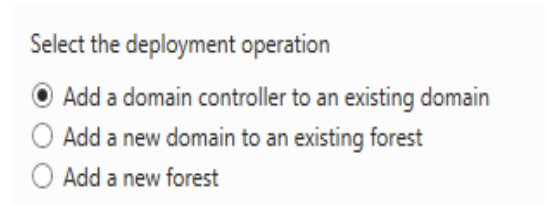




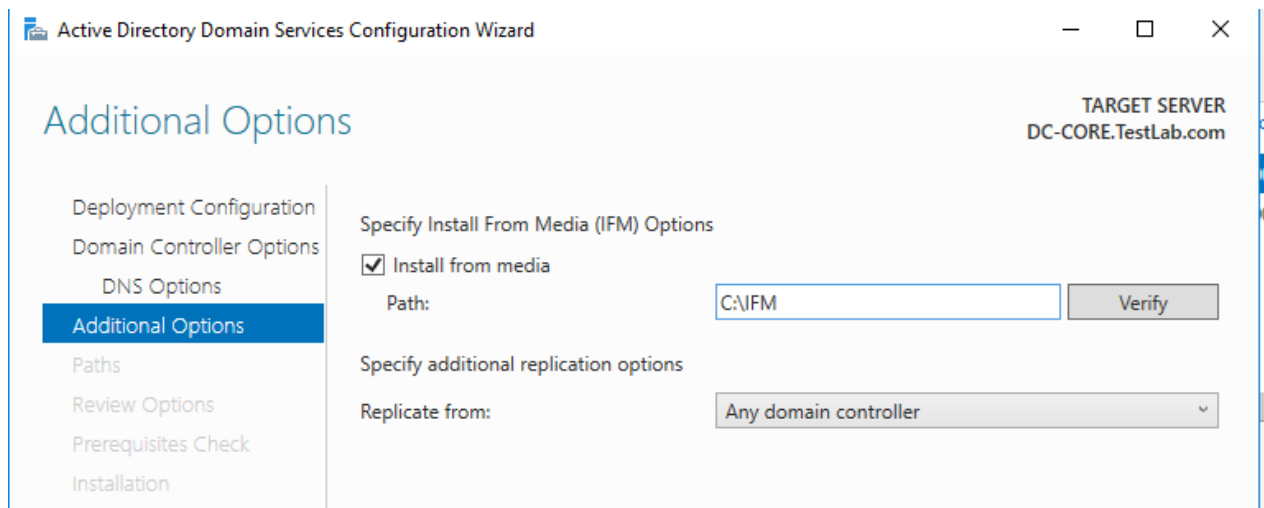
בסיום ההתקנה נהפוך את השרת לשרת DOMAIN CONTROLLER



אך הפעם נוסיף את השרת כשרת נוסף בדומיין קיים (שימו לב שבהגדרות כרטיס הרשת צריך להיות מוגדר DNS (10.0.0.1

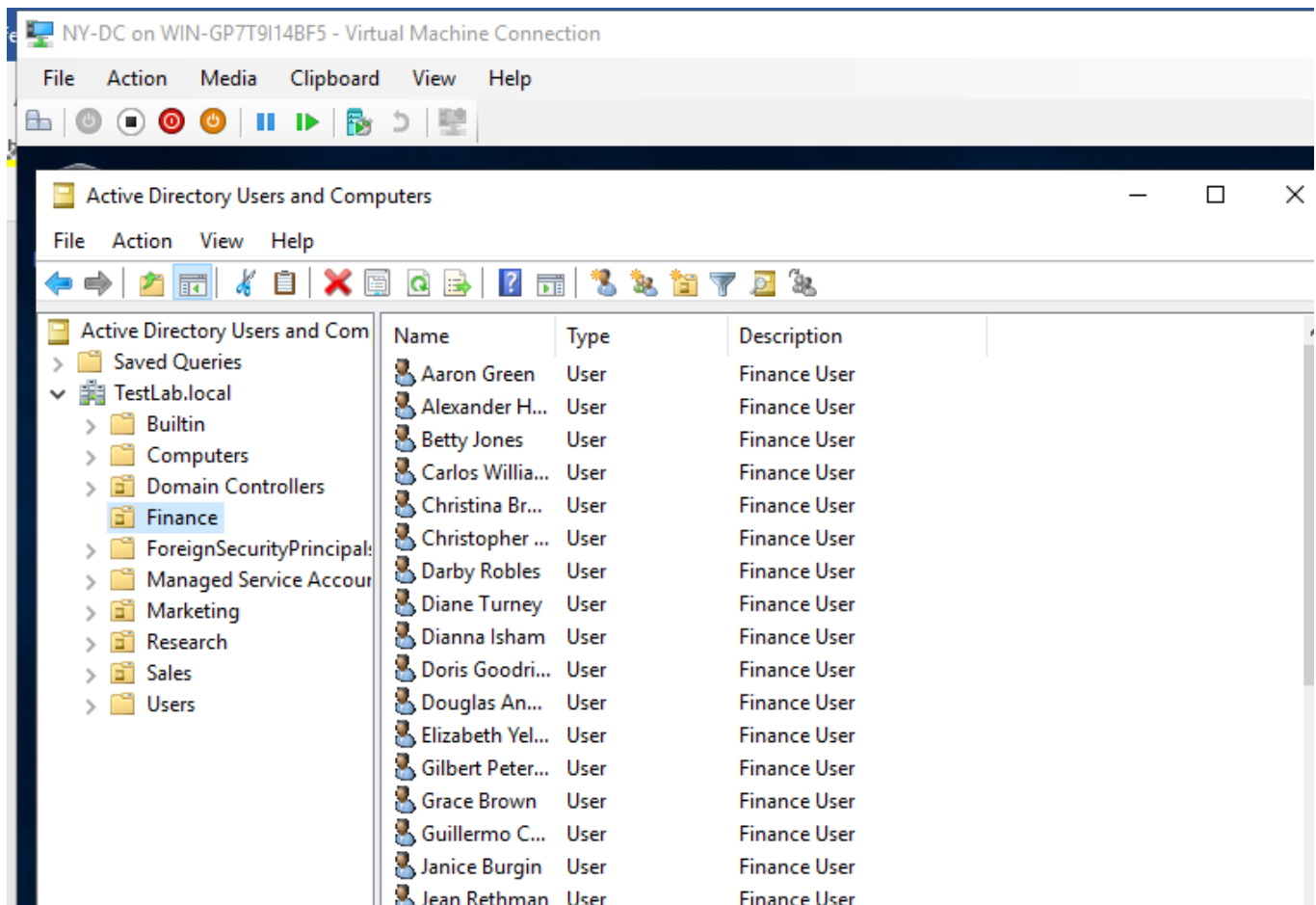


לאחר שגזין את ההרשאות וסיממת שחזור במסך אפשרויות נוספות נבחר לבצע התקנה ממדיה :



נוודא שההגדרות אכן תקינות ונלחץ על NEXT , נחכה לסיום הבדיקה ונבצע את ההתקנה

לאחר האתחול נודא שאכן כל המשתמשים עברו



## FSMO ROLES

ב- DC1 ניכנס לממשק POWERSHELL

כיוון ש DC1 הוא השרת הראשון ביער כל ה- FSMO ROLES מבוצעים על ידו. נבדוק באמצעות הפקודה :

Netdom query fsmo

```
PS C:\Users\Administrator> Netdom query fsmo
Schema master           DC1.TestLab.com
Domain naming master    DC1.TestLab.com
PDC                     DC1.TestLab.com
RID pool manager        DC1.TestLab.com
Infrastructure master    DC1.TestLab.com
The command completed successfully.

PS C:\Users\Administrator> _
```

או באמצעות POWERSHELL

```
PS C:\Users\Administrator> Get-ADDomain | Select-Object Name, InfrastructureMaster, PDCEmulator, RIDMaster
Name      InfrastructureMaster PDCEmulator  RIDMaster
-----
TestLab DC1.TestLab.com      DC1.TestLab.com DC1.TestLab.com

PS C:\Users\Administrator> Get-ADForest | Select-Object Name, SchemaMaster, DomainNamingMaster
Name      SchemaMaster  DomainNamingMaster
-----
TestLab.com DC1.TestLab.com DC1.TestLab.com
```

נבצע העברה של חלק מה- FSMO ROLES לשרת DC-NY - נשתמש בפקודות NTDSUTIL

<https://support.microsoft.com/en-us/help/255504/using-ntdsutil-exe-to-transfer-or-seize-fsmo-roles-to-a-domain-control>

ניתן לבצע זאת גם באמצעות ממשק גרפי או POWERSHELL:

[https://www.petri.com/transferring\\_fsmo\\_roles](https://www.petri.com/transferring_fsmo_roles)

<https://www.petri.com/manage-fsmo-roles-using-powershell>

נתחבר ל- DC-NY ונריץ ממנו את פקודת ntdsutil :

activate instance ntds

roles

? - ייתן לנו עזרה ונוכל לראות שיש לנו אפשרות לבצע Transfer או Seize

```

PS C:\Users\admin> ntdsutil
C:\windows\system32\ntdsutil.exe: activate instance ntds
Active instance set to "ntds".
C:\windows\system32\ntdsutil.exe: roles
fsmo maintenance: ?

? - Show this help information
Connections - Connect to a specific AD DC/LDS instance
Help - Show this help information
Quit - Return to the prior menu
Seize infrastructure master - Overwrite infrastructure role on connected server
Seize naming master - Overwrite Naming Master role on connected server
Seize PDC - Overwrite PDC role on connected server
Seize RID master - Overwrite RID role on connected server
Seize schema master - Overwrite schema role on connected server
Select operation target - Select sites, servers, domains, roles and naming contexts
Transfer infrastructure master - Make connected server the infrastructure master
Transfer naming master - Make connected server the naming master
Transfer PDC - Make connected server the PDC
Transfer RID master - Make connected server the RID master
Transfer schema master - Make connected server the schema master

fsmo maintenance:

```

נבחר להעביר את ה- Schema master ואת Domain Naming Master

ראשית נתחבר לשרת באמצעות Connections

```

fsmo maintenance: Connections
server connections: ?

? - Show this help information
Clear creds - Clear prior connection credentials
Connect to domain %s - Connect to DNS domain name
Connect to server %s - Connect to server, DNS name[:port number]
Help - Show this help information
Info - Show connection information
Quit - Return to the prior menu
Set creds %s1 %s2 %s3 - Set connection creds as domain %s1, user %s2,
                        pwd %s3. Use "NULL" for null password,
                        * to enter password from the console.

server connections:

```

נבצע חיבור לשרת אליו נרצה להעביר את התפקידים :

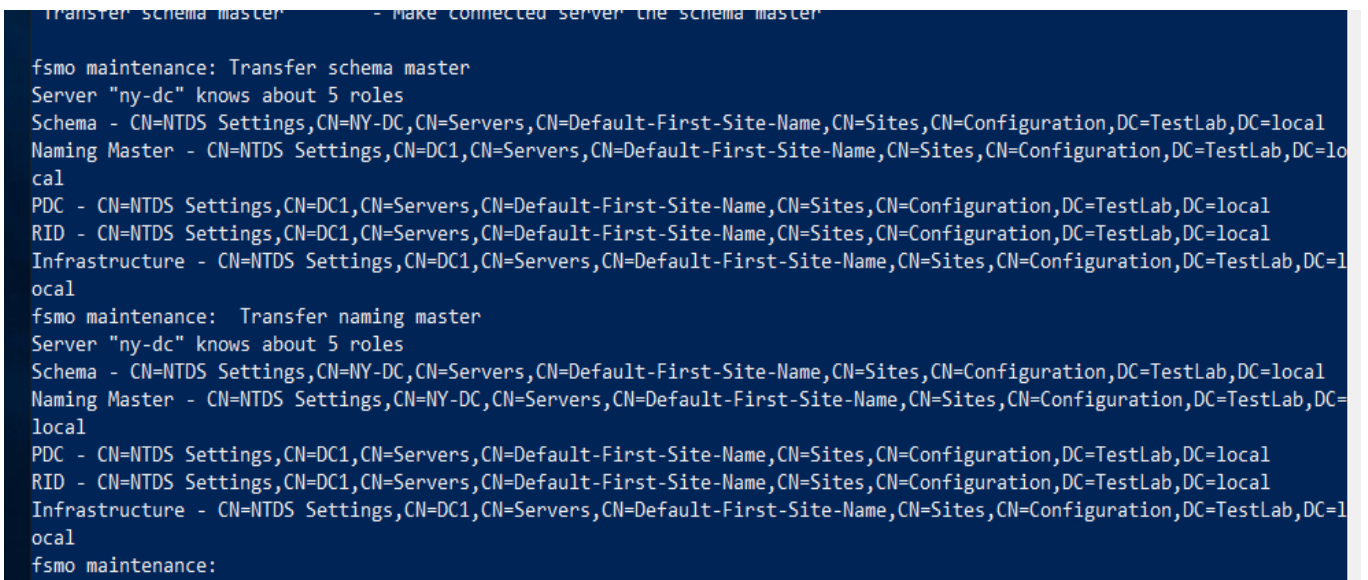
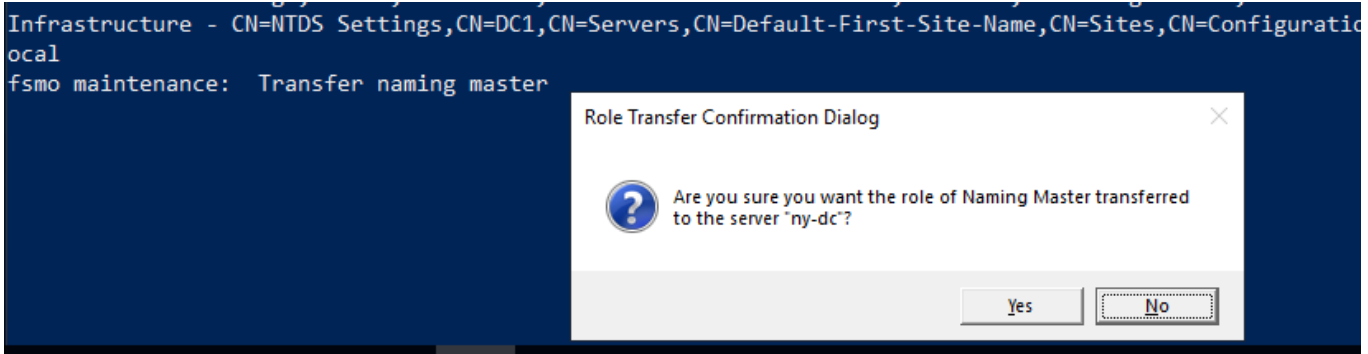
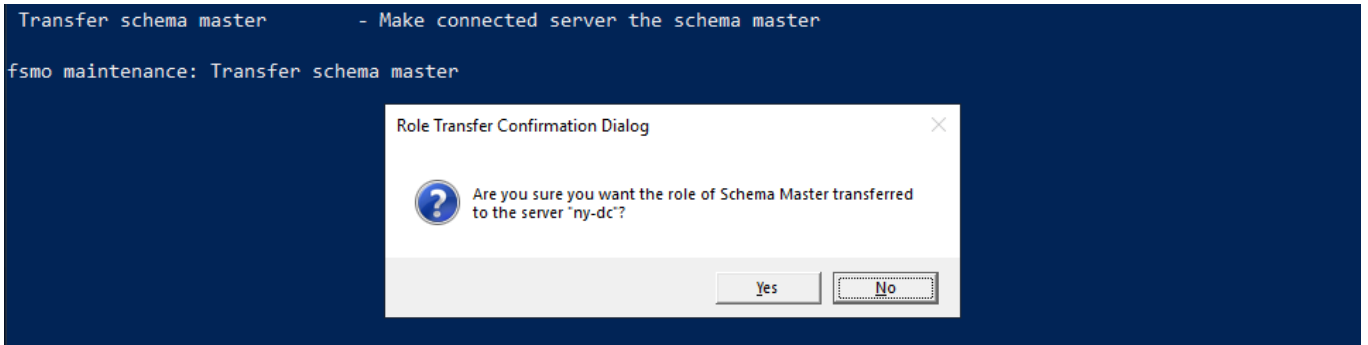
```

server connections: connect to server ny-dc
Binding to ny-dc ...
Connected to ny-dc using credentials of locally logged on user.
server connections:

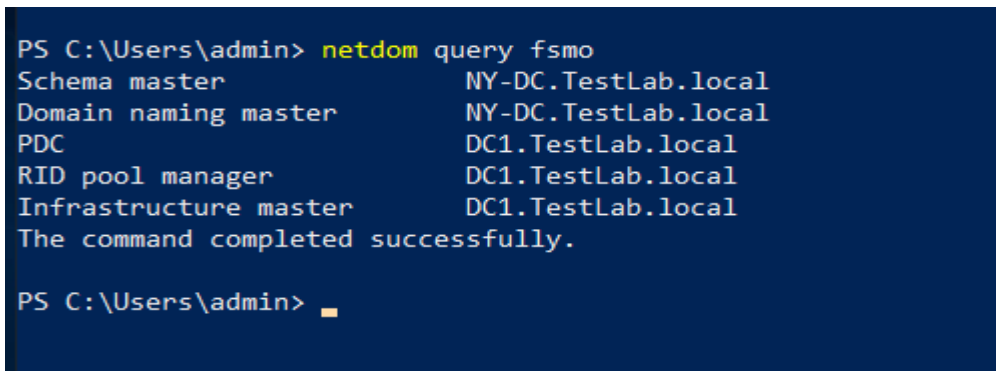
```



נכתוב quit ע"מ לחזור לתפריט הקודם ונבצע העברה – לאחר כל פעם נבצע אישור



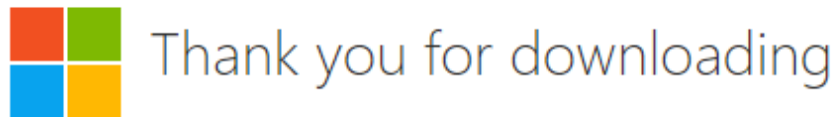
נצא מהממשק ונבצע בדיקה :



נוכל לראות שאכן עברו FSMO ROLES


על מנת שתוכל לבצע ניהול מרחוק מהמשרד שלך ולא תצטרך לרדת אל חדר השרתים הקפוא בכל פעם שתצטרך לבצע ניהול של השרתים, החלטת להתקין את כלי הניהול RSAT במחשב האישי שלך במשרד.

ניכנס לאתר של מייקרוסופט ונבצע הורדה של הכלי :



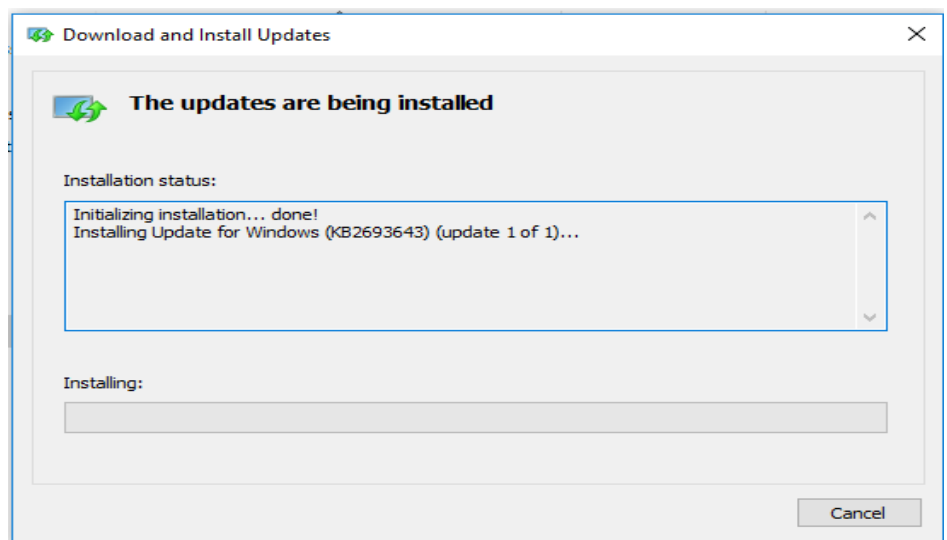
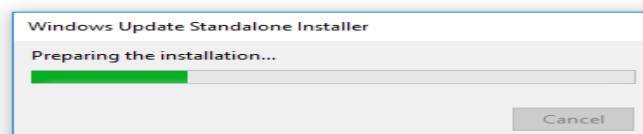
### Remote Server Administration Tools for Windows 10

If your download does not start after 30 seconds, [Click here](#)

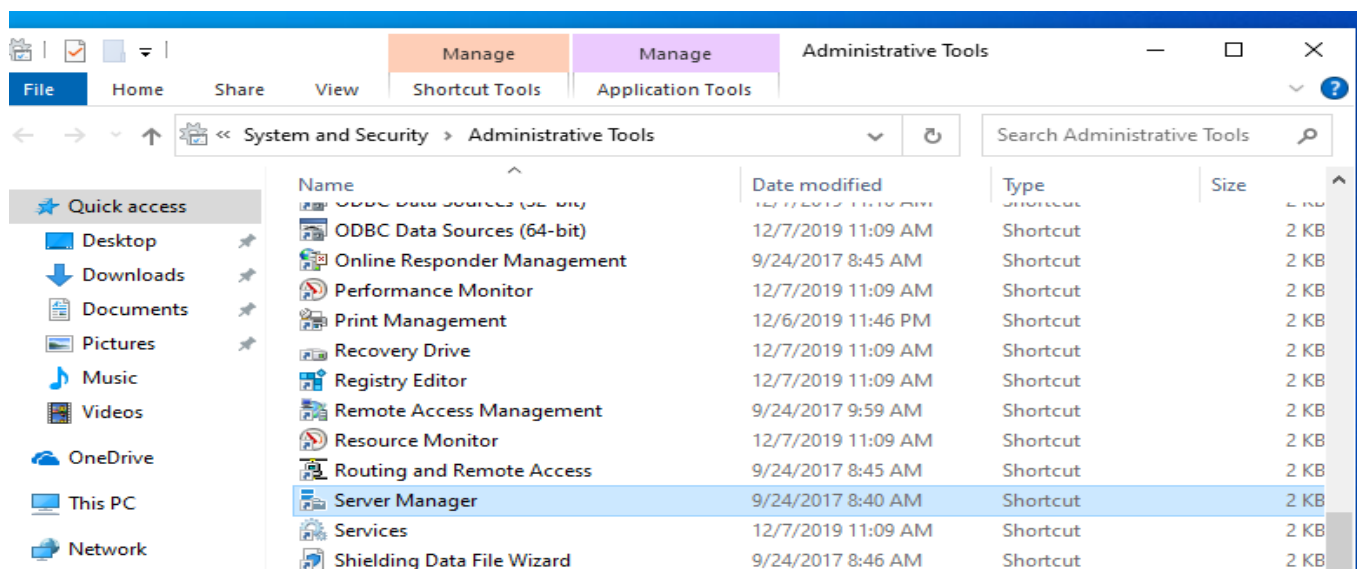
 [Install Instructions](#)

בדרך העדיפה עליך העבר אותו למכונה הוירטואלית ובצע התקנה

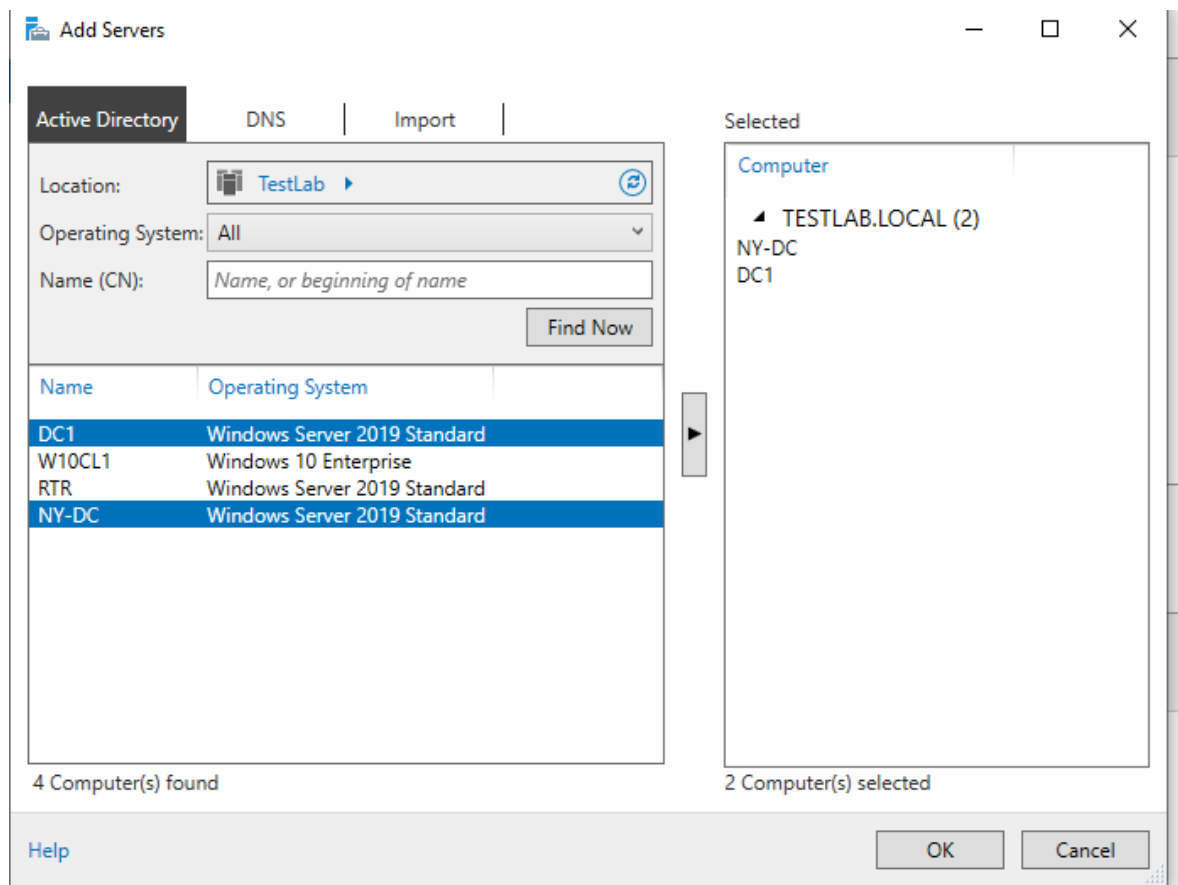
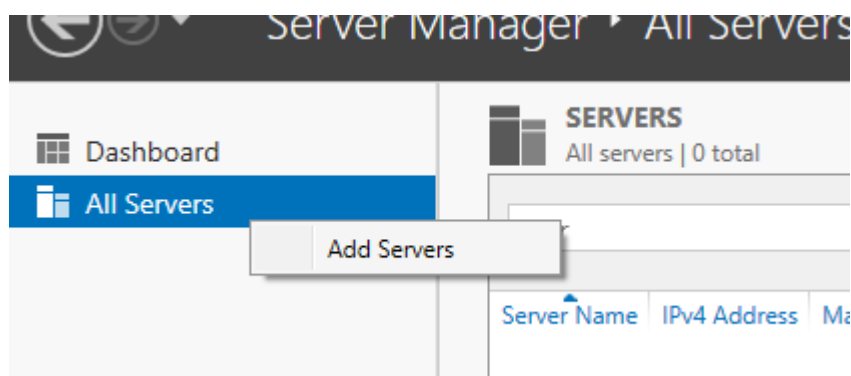
Name	Date modified	Type	Size
 WindowsTH-RSAT_TP5_Update-x64	9/25/2016 12:54 PM	Microsoft Update ...	93,153 KB



בסיום ההתקנה ניכנס למחשב כמנהל הדומיין ונפעיל את SERVER MANAGER



נוסיף את השרתים (הדבר מתאפשר כיוון שביצענו כניסה כמנהל הדומיין)



- במידה ואתה נתקל בתקלה באיתור שרת NY-DC הדבר נובע כיוון שבתחנה לא מוגדר ROUTER

**SERVERS**  
All servers | 2 total

Refresh failed More...

Filter

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
DC1	10.0.0.1	Online - Performance counters not started	7/1/2021 2:52:56 PM	00429-70000-00000-AA783 (Activated)
NY-DC	-	Target name resolution error	7/1/2021 2:52:26 PM	-

נגדיר את כרטיס הרשת :

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 10 . 0 . 0 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 0 . 0 . 254

☐ Obtain DNS server address automatically

נבצע רענון

**כעת ניתן לנהל מתוך הקליינט את הדומיין והשרתים**

**SERVERS**  
All servers | 2 total

TASKS

Filter

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
DC1	10.0.0.1	Online - Performance counters not started	7/1/2021 2:54:50 PM	00429-70000-00000-AA783 (Activated)
NY-DC	20.0.0.1	Online - Performance counters not started	7/1/2021 2:55:12 PM	00429-70000-00000-AA785 (Activated)

## ביצוע Domain off line join

לאחד המנהלים בסניף ניו יורק השוהה כרגע בחופשה, נגנב המחשב. המנהל רכש מחשב חדש ורוצה להתחבר אל הסניף באמצעות חיבור VPN. שרת ה-VPN הארגוני מאפשר כאמצעי אבטחה חיבור רק למחשבים המחוברים לדומיין. היות והמנהל יהיה נגיש לשרת DC רק בעוד שבועיים החלטת לבצע למחשב החדש Provision ולאפשר לו להתחבר לדומיין גם ללא צורך בתקשורת מול שרת DC

התחבר למכונת DC1 היכנס אל ממשק POWERSHELL וכתוב את הפקודה הבאה :

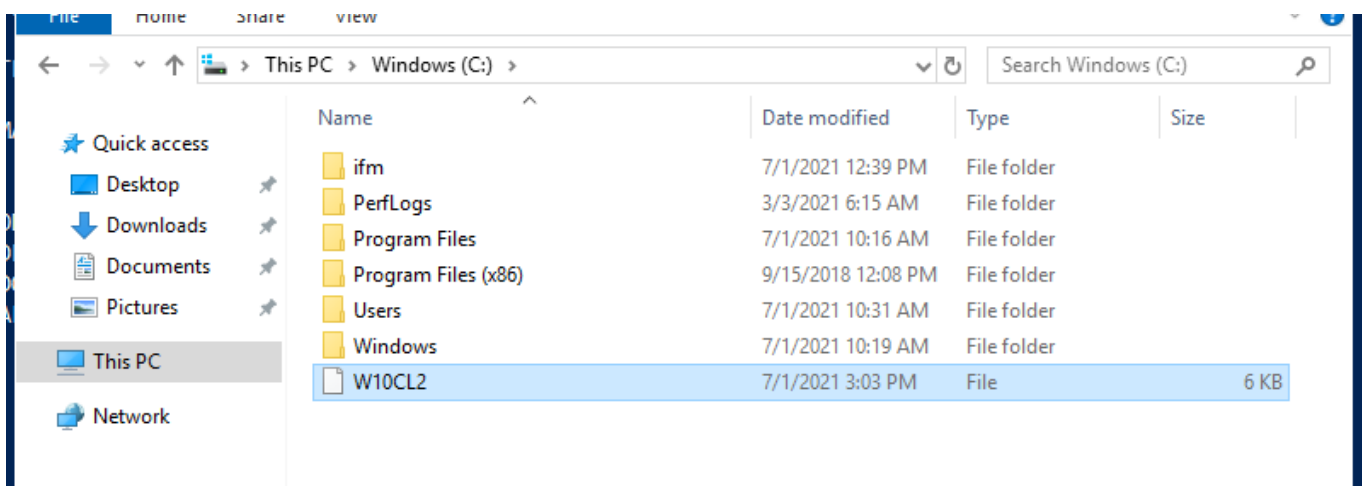
Djoin /provision /domain testlab.local /machine W10CL2 /savefile C:\W10CL2

```
PS C:\Users\admin> djoin /provision /domain testlab.local /machine W10CL2 /savefile C:\W10CL2

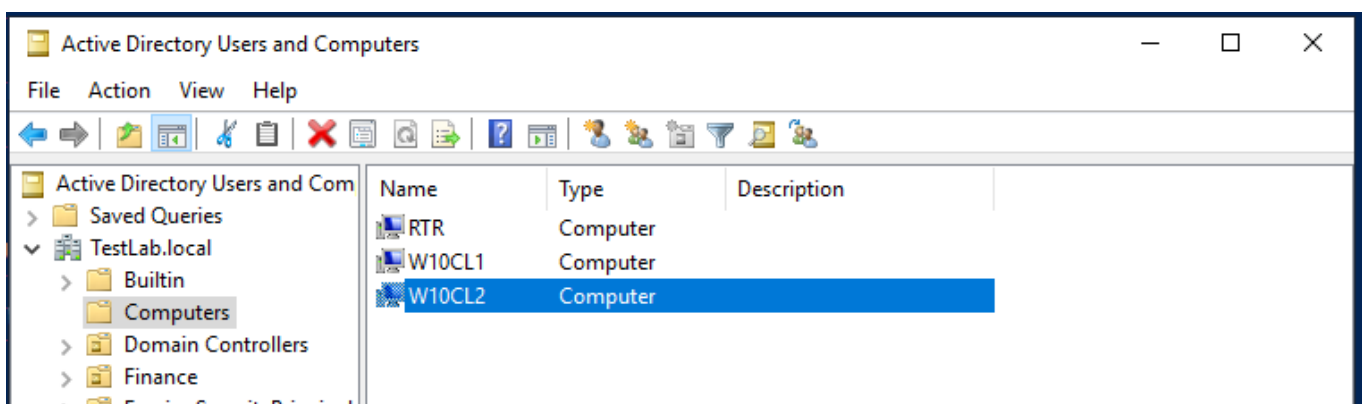
Provisioning the computer...
Successfully provisioned [W10CL2] in the domain [testlab.local].
Provisioning data was saved successfully to [C:\W10CL2].

Computer provisioning completed successfully.
The operation completed successfully.
PS C:\Users\admin>
```

נוכל לראות שבכונן נוצר לנו קובץ (הקובץ מכיל למעשה את הסיסמה שהייתה אמורה להיות מועברת בתהליך הצירוף לדומיין)

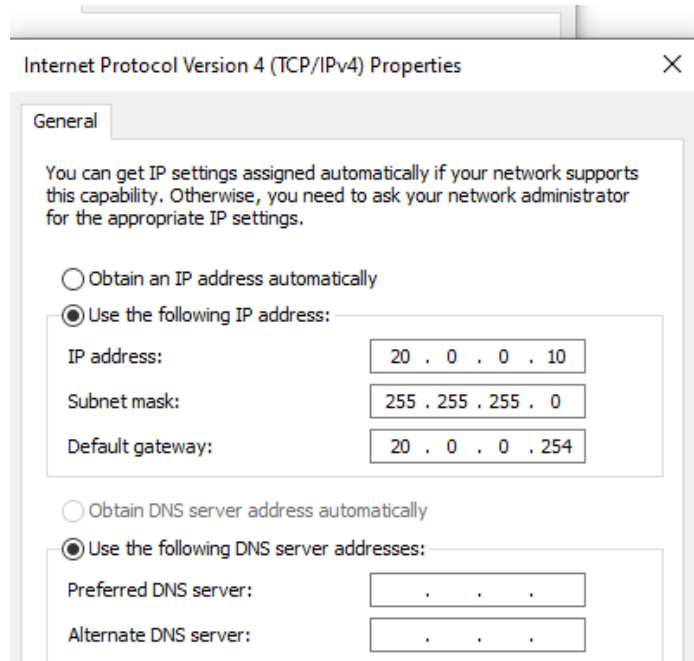


אם ניגש ל Active Directory נוכל לראות את המחשב שנוצר

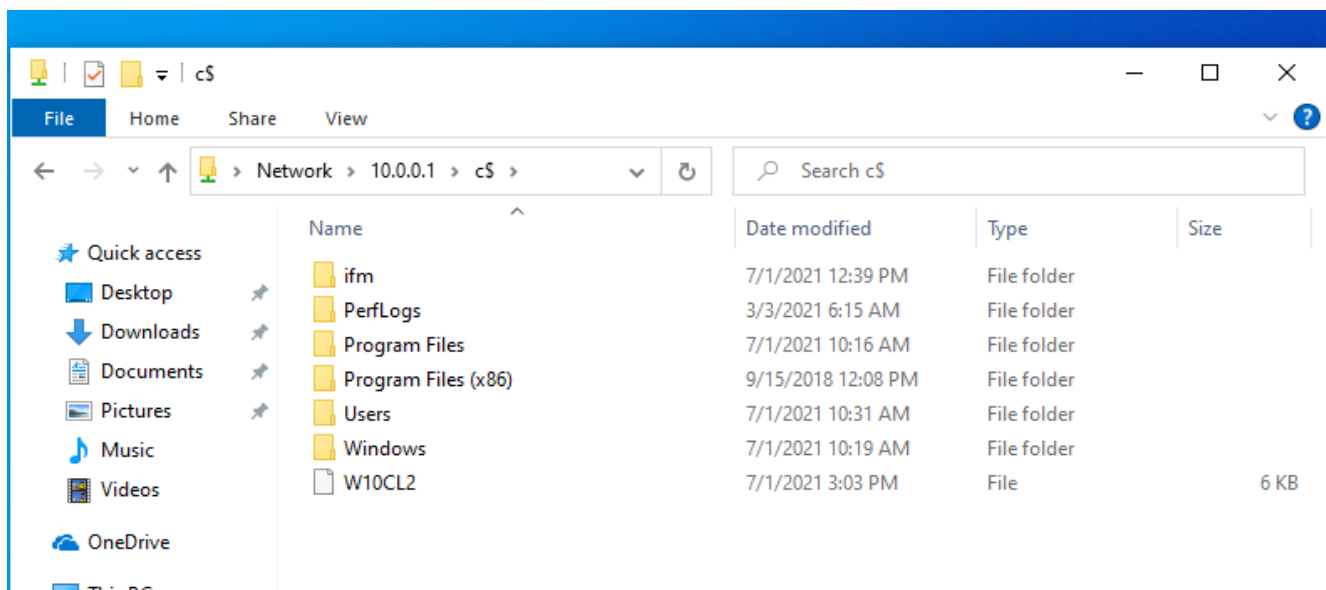


כעת נעבור למכונת W10CL2 נתחבר עם האדמין המקומי USER והסיסמה Pa55w.rd

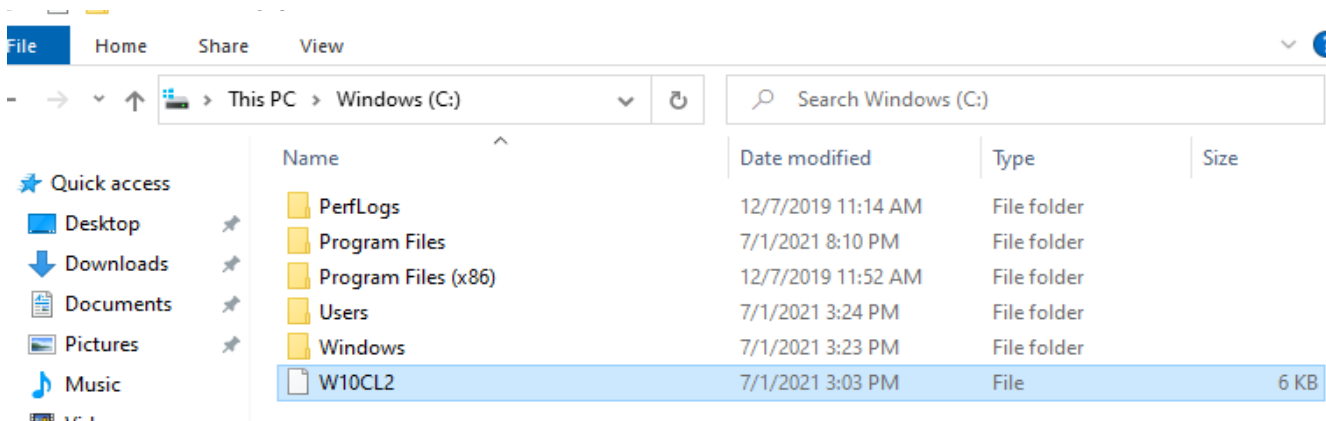
ניכנס להגדרות הרשת ונגדיר עבור המכונה Default Gateway – 20.0.0.254



בסייר הקבצים נתחבר אל הכונן של DC1 (בסביבה אמיתית היינו שולחים את הקובץ במייל)



נעתיק את הקובץ לכונן C המקומי שלנו





בשלב הבא ניכנס לממשק POWERSHELL כאדמין ונכתוב :

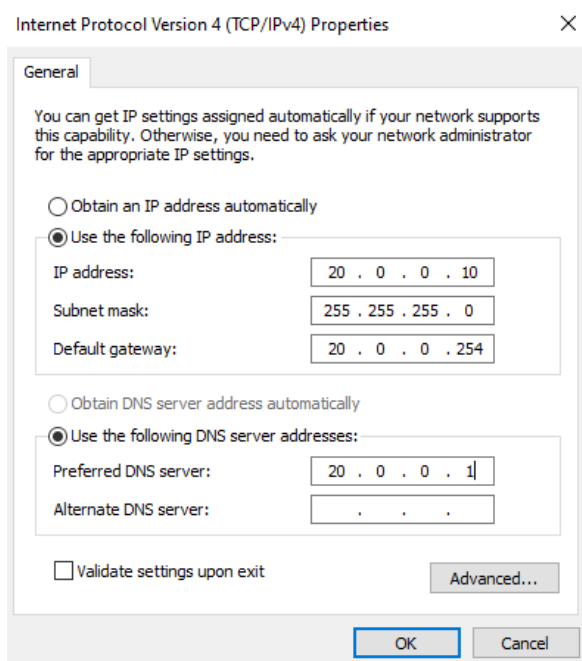
Djoin.exe /REQUESTODJ /LOADFILE C:\w10cl2 /WindowsPath C:\Windows /LOCALOS

```
PS C:\windows\system32> djoin.exe /REQUESTODJ /LOADFILE C:\W10CL2 /WindowsPath C:\Windows /LOCALOS
Loading provisioning data from the following file: [C:\W10CL2].

The provisioning request completed successfully.
A reboot is required for changes to be applied.
The operation completed successfully.
PS C:\windows\system32>
```

ע"מ שהשינויים ייכנסו לתוקף נבצע אתחול למע' ההפעלה

נתחבר שוב כ USER עם הסיסמה Pa55w.rd והפעם נגדיר עבור המכונה שרת DNS של ניו יורק וננסה להתחבר כמשתמש בדומיין



נבצע יציאה ונתחבר כמשתמש בדומיין – נתחבר כמשתמש aarong@testlab.local



החיבור הצליח היות והמכונה מאומתת בדומיין ויכולה לתקשר מול שרת ה-DC בניו יורק ...