תרגיל מעבדה 2: תרגול סביבת ACTIVE DIRECTORY

בתור מנהל IT בחברת TESTLAB , קיבלת הוראה ממנכ"ל החברה להקים תשתית IT עבור סניף קטן של החברה אשר יוקם בארה"ב

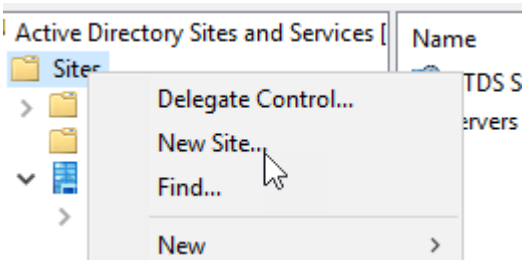
במעבדה שלנו ע"מ לדמות אתר אמיתי – נשתמש בשתי רשתות שונות ונחבר אותן באמצעות ראוטר.

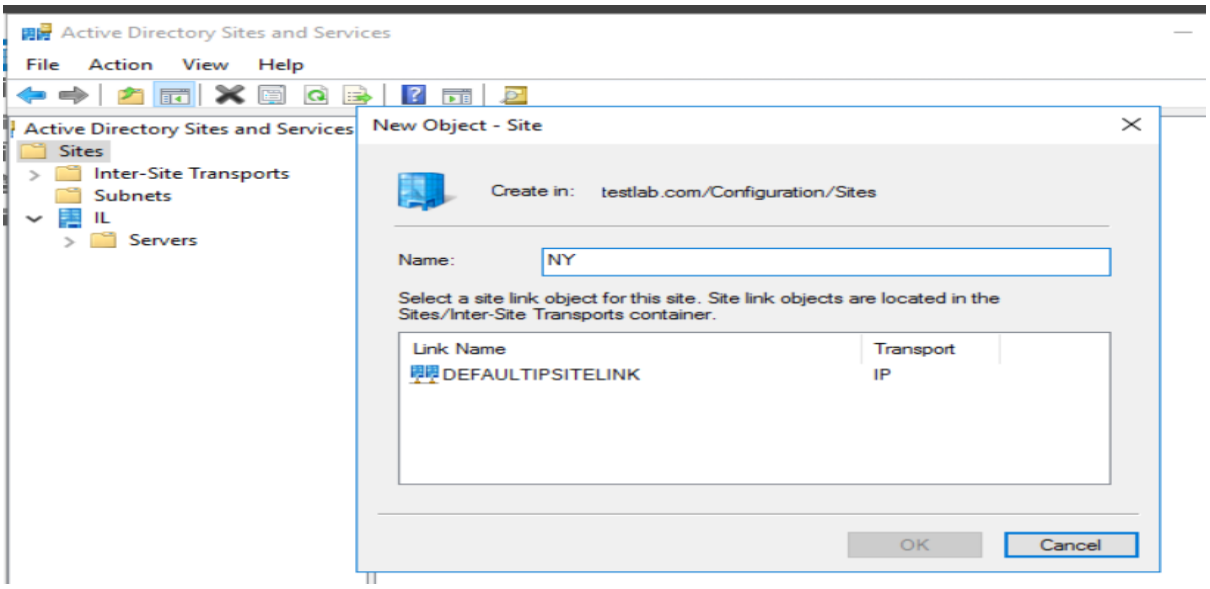
כמו כן נבצע מספר בדיקות רפליקציה , נגדיר קבוצות אבטחה והרשאות NTFS

שלב א : הגדרת SITE

בשרת DC1 , ניכנס לממשק AD sites and services ונשנה את שם אתר ברירת המחדל ל-IL

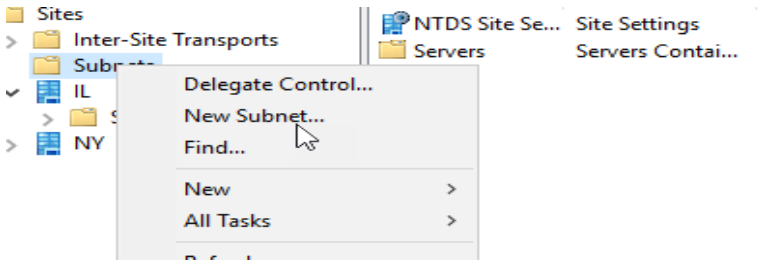
כעת נגדיר אתר חדש עבור האתר של NY



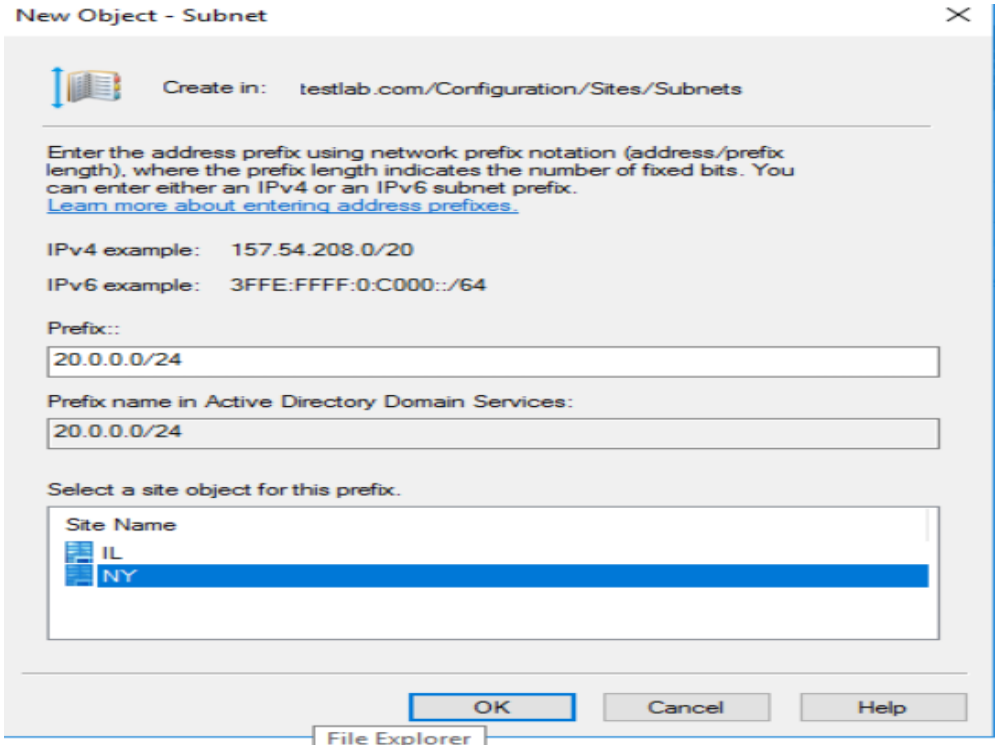


נבחר להשתמש בחיבור ברירת המחדל (היות ויש לנו רק נק' חיבור יחידה כרגע)

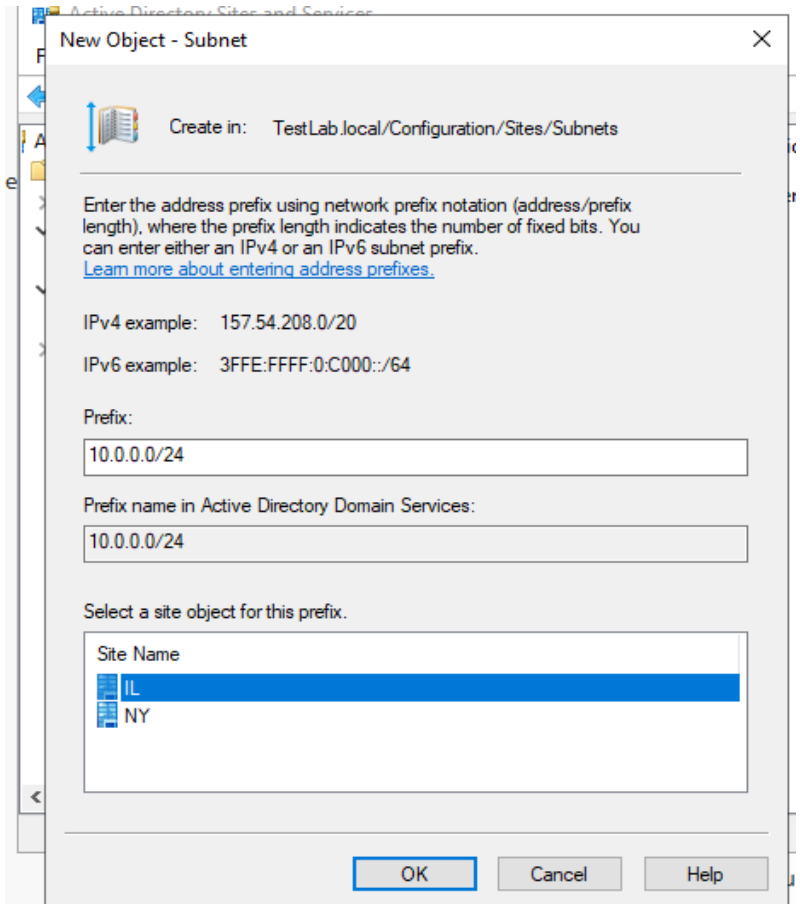
נגדיר עבורו את ה-SUBNET חדש



בהגדרות נרשום את כתובת הרשת של NY : 20.0.0.0.24 ונבחר באתר NY

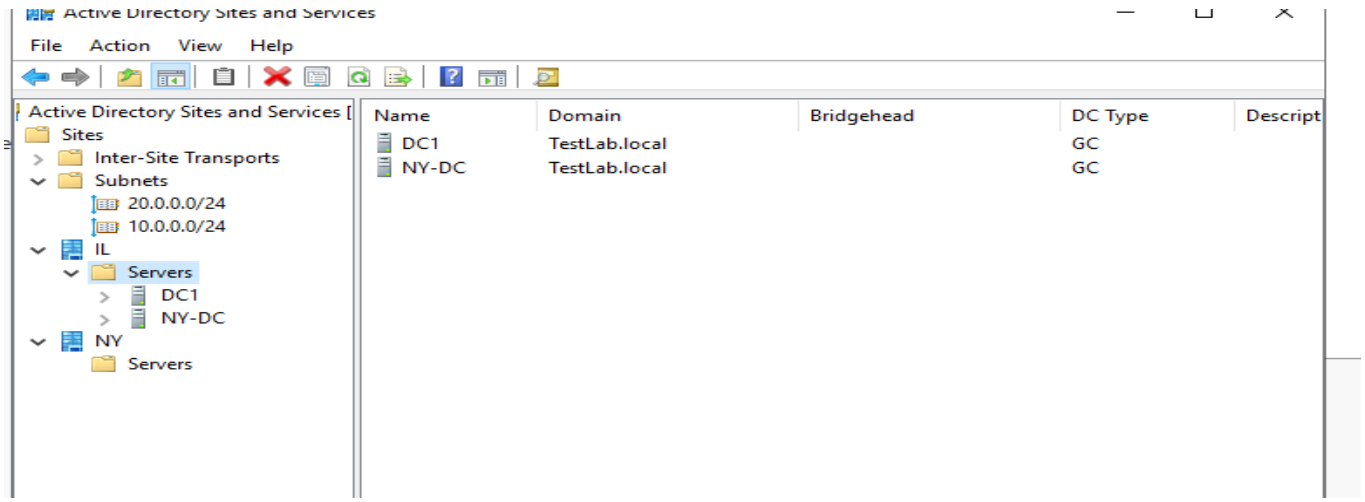


נחזור על התהליך הפעם נגדיר עבור IL את ה-SUBNET של 10.0.0.0 /24

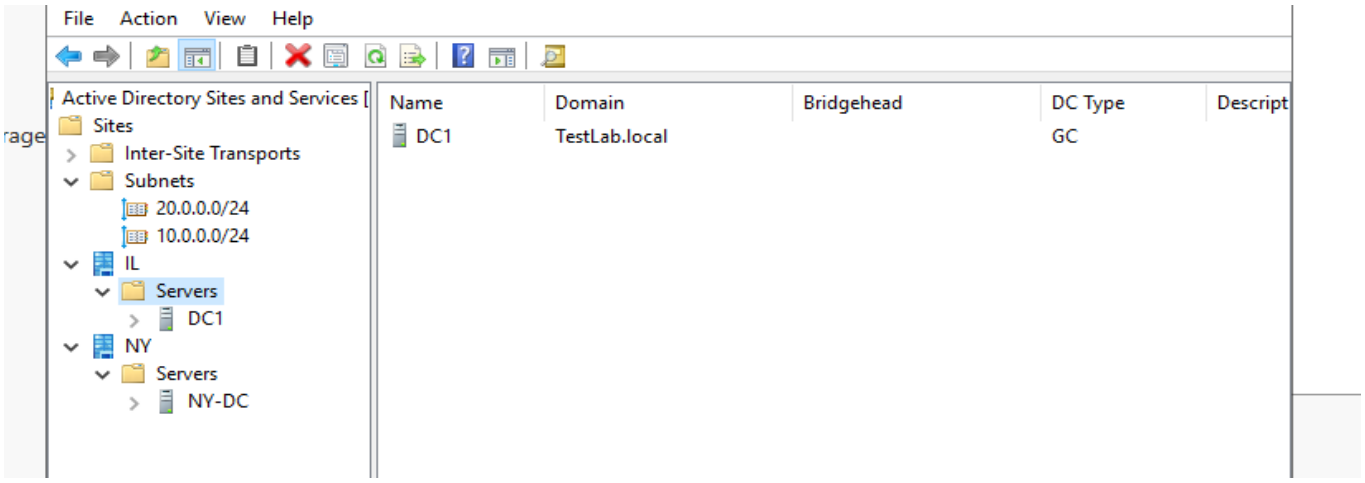


בשלב זה נגרור את השרת של NY שכרגע יושב בישראל אל האתר ב-NY

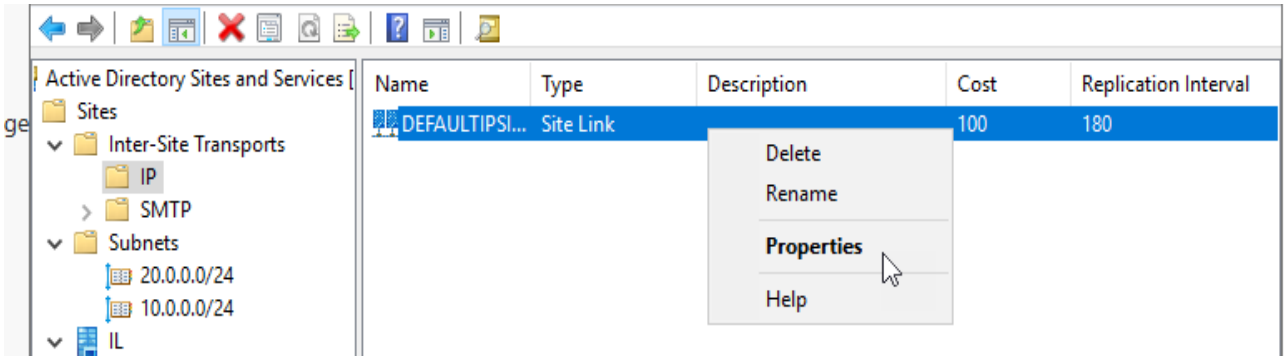
לפני :



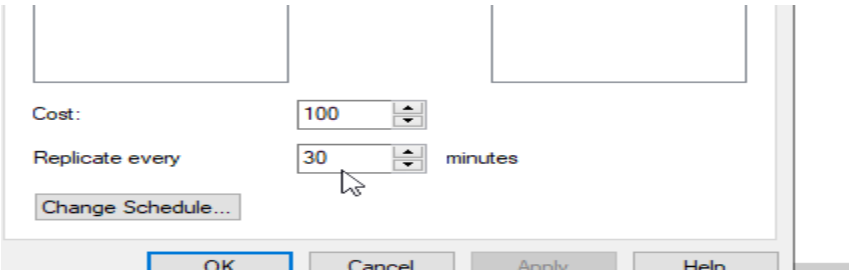
נתעלם מהאזהרה ונגיע למצב הבא :



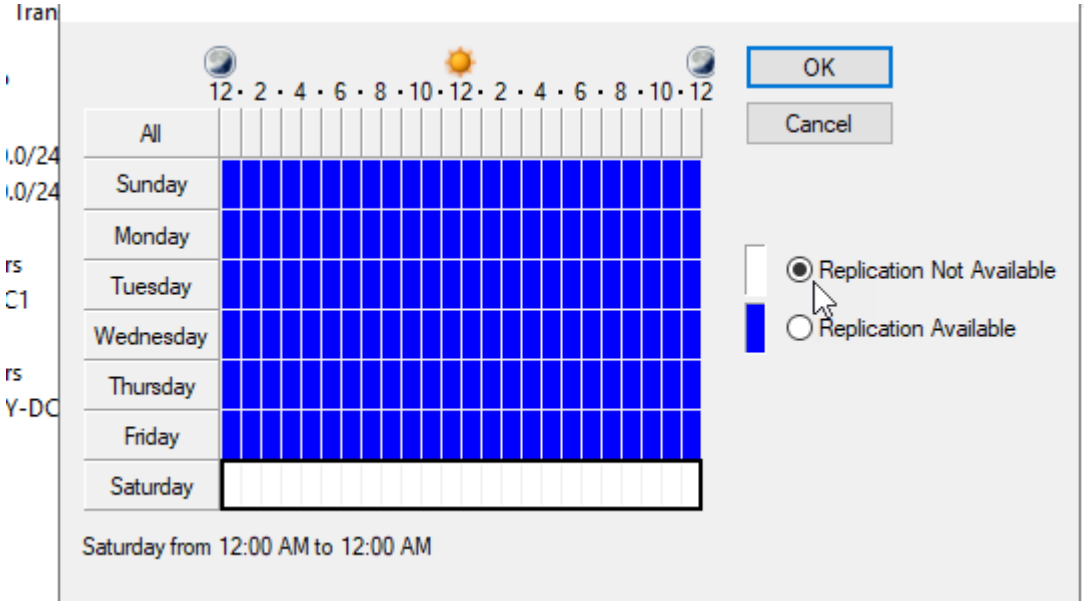
נעמוד על Inter-Site Transports נבחר ב-IP ניגש למאפייני חיבור ברירת המחדל :



נגדיר רפליקציה כל חצי שעה ובימי שבת ללא רפליקציה



בימי שבת לא תהיה רפליקציה :



שלב ב : הגדרת רפליקציה באתר

נבצע מספר בדיקות לבדיקת רפליקציה

בשרת NY-DC נתחבר כ-ADMIN ניכנס לממשק POWERSHELL ונצור משתמש חדש לבדיקה :

"New-Aduser -Name "testu - יווצר לנו משתמש לא פעיל בקונטיינר USERS

```
C:\Users\admin> New-ADUser -Name "testu"
```

נשתמש בפקודה : Get-ADReplicationAttrubuteMetadata על מנת לראות אילו מאפיינים התרפלקו ובאיזה שרת

נזין את ה-DN של המשתמש ואת השרת מולו נבצע את הבדיקה :

```
icationAttributeMetadata

PS C:\Users\admin> Get-ADReplicationAttributeMetadata -Object "cn=testu,cn=users,dc=testlab,dc=local" -Server nydc
PS C:\Users\admin> Get-ADReplicationAttributeMetadata -Object "cn=testu,cn=users,dc=testlab,dc=local" -Server ny-dc

AttributeName                                  : objectCategory
AttributeValue                                 : CN=Person,CN=Schema,CN=Configuration,DC=TestLab,DC=local
FirstOriginatingCreateTime                     :
IsLinkValue                                    : False
LastOriginatingChangeDirectoryServerIdentity   : CN=NTDS Settings,CN=NY-DC,CN=Servers,CN=NY,CN=Sites,CN=Configuration
                                                 ,DC=TestLab,DC=local
LastOriginatingChangeDirectoryServerInvocationId : 93262e5e-22dc-410a-a3ce-471b5e12f290
LastOriginatingChangeTime                      : 7/11/2021 10:24:31 AM
LastOriginatingChangeUsn                       : 12477
LastOriginatingDeleteTime                      :
LocalChangeUsn                                 : 12477
Object                                         : cn=testu,cn=users,dc=testlab,dc=local
Server                                         : NY-DC.TestLab.local
Version                                        : 1
```

נקבל רשימה ארוכה עם מאפיינים שעברו עדכון והשרת בו בוצע העדכון

נרשום את אותה הפקודה הפעם נזין בשם השרת את DC1 :

```
PS C:\Users\admin> Get-ADReplicationAttributeMetadata -Object "cn=testu,cn=users,dc=testlab,dc=local" -Server dc1
Get-ADReplicationAttributeMetadata : Directory object not found
At line:1 char:1
+ Get-ADReplicationAttributeMetadata -Object "cn=testu,cn=users,dc=test ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (:) [Get-ADReplicationAttributeMetadata], ADIdentityNotFoundException
    + FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityNotFoundException,M
   icrosoft.ActiveDirectory.Management.Commands.GetADReplicationAttributeMetadata

PS C:\Users\admin>
```

קיבלנו שגיאה כי טרם בוצעה רפליקציה והאובייקט לא נמצא שם,נבצע סנכרון יזום באמצעות הפקודה repadmin

נכתוב : repadmin /replicate dc1 ny-dc1 "dc=testlab,dc=local"

נוכל לראות שלאחר מכן הפקודה הצליחה היות והאובייקט הועבר גם לשרת בישראל.

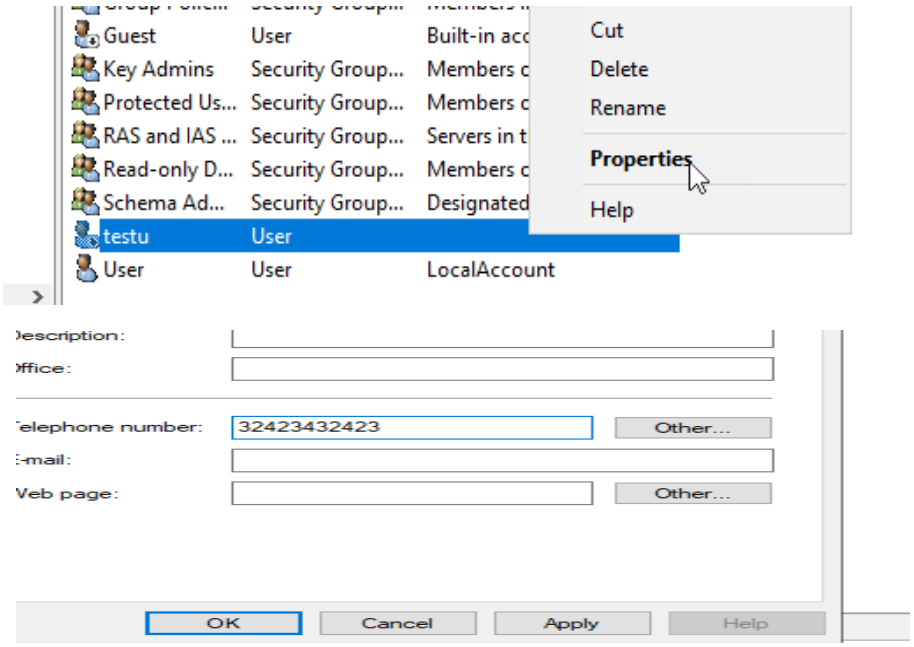
```
    The naming context specified for this replication operation is invalid.

PS C:\Users\admin> repadmin /replicate dc1 ny-dc "dc=testlab,dc=local"
Sync from ny-dc to dc1 completed successfully.

PS C:\Users\admin> Get-ADReplicationAttributeMetadata -Object "cn=testu,cn=users,dc=testlab,dc=local" -Server dc1


AttributeName                                : objectCategory
AttributeValue                               : CN=Person,CN=Schema,CN=Configuration,DC=TestLab,DC=local
FirstOriginatingCreateTime                   :
IsLinkValue                                  : False
LastOriginatingChangeDirectoryServerIdentity : CN=NTDS Settings,CN=NY-DC,CN=Servers,CN=NY,CN=Sites,CN=Configuratio
                                               ,DC=TestLab,DC=local
LastOriginatingChangeDirectoryServerInvocationId : 93262e5e-22dc-410a-a3ce-471b5e12f290
LastOriginatingChangeTime                    : 7/11/2021 10:24:31 AM
```

ניגש לאתר בישראל נעמוד על המשתמש testu ממשק ACTIVE DIRECTORY USERS , ניגש למאפיינים ונשנה לו את מספר הטלפון



נזין מספר טלפון כלשהו נשמור ונצא

ב-NY-DC ממשק POWERSHELL נכתוב את הפקודה הבאה :

Repadmin /showobjmeta ny-dc1 "cn=testu,cn=users,dc=testlab,dc=local"

```
PS C:\Users\admin> repadmin /showobjmeta ny-dc "cn=testu,cn=users,dc=testlab,dc=local"

21 entries.
Loc.USN                          Originating DSA  Org.USN  Org.Time/Date        Ver Attribute
=======                          =============== ========= =============        === =========
  12477                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 objectClass
  12477                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 cn
  12477                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 instanceType
  12477                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 whenCreated
  12477                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 nTSecurityDescriptor
  12477                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 name
  12478                                 NY\NY-DC     12478 2021-07-11 10:24:31    2 userAccountControl
  12478                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 codePage
  12478                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 countryCode
  12478                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 dBCSPwd
  12478                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 logonHours
  12478                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 unicodePwd
  12478                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 ntPwdHistory
  12478                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 pwdLastSet
  12478                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 primaryGroupID
  12477                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 objectSid
  12478                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 accountExpires
  12478                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 lmPwdHistory
  12477                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 sAMAccountName
  12477                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 sAMAccountType
  12477                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 objectCategory
0 entries.
Type    Attribute     Last Mod Time                          Originating DSA  Loc.USN Org.USN Ver
======= ============  =============                         ================ ======= ======= ===
        Distinguished Name
        ==============================

PS C:\Users\admin>
```

נרשום את אותה הפקודה הפעם עם שרת DC1 נוכל לראות את השינוי שבוצע בשרת DC1 ואת המאפיין ששונה :

```
PS C:\Users\admin> repadmin /showobjmeta dc1 "cn=testu,cn=users,dc=testlab,dc=local"

22 entries.
Loc.USN                          Originating DSA  Org.USN  Org.Time/Date        Ver Attribute
=======                          =============== ========= =============        === =========
  28975                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 objectClass
  28975                                   IL\DC1     28975 2021-07-11 10:40:52    1 cn
  29013                                   IL\DC1     29013 2021-07-11 10:47:47    1 telephoneNumber
  28975                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 instanceType
  28975                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 whenCreated
  28975                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 nTSecurityDescriptor
  28975                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 name
  28975                                 NY\NY-DC     12478 2021-07-11 10:24:31    2 userAccountControl
  28975                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 codePage
  28975                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 countryCode
  28975                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 dBCSPwd
  28975                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 logonHours
  28975                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 unicodePwd
  28975                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 ntPwdHistory
  28975                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 pwdLastSet
  28975                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 primaryGroupID
  28975                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 objectSid
  28975                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 accountExpires
  28975                                 NY\NY-DC     12478 2021-07-11 10:24:31    1 lmPwdHistory
  28975                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 sAMAccountName
  28975                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 sAMAccountType
  28975                                 NY\NY-DC     12477 2021-07-11 10:24:31    1 objectCategory
0 entries.
Type    Attribute     Last Mod Time                          Originating DSA  Loc.USN Org.USN Ver
======= ============  =============                         ================ ======= ======= ===
        Distinguished Name
        ==============================
```

נבצע בדיקה לגבי המאפיין :

נכתוב בשורת הפקודה :

```
PS C:\Users\admin> repadmin /replicate ny-dc dc1 "dc=testlab,dc=local"
```

נבצע רפליקציה הפעם משרת dc1 אל שרת ny-dc

נחזור עם הפקודה :

```
PS C:\Users\admin> Get-ADReplicationAttributeMetadata -Object "cn=testu,cn=users,dc=testlab,dc=local" -Server ny-dc
```

נוכל להבחין שהמאפיין טלפון השתנה והשינוי בוצע בשרת DC1

```
AttributeName                                  : telephoneNumber
AttributeValue                                 : 32423432423
FirstOriginatingCreateTime                     :
IsLinkValue                                    : False
LastOriginatingChangeDirectoryServerIdentity   : CN=NTDS Settings,CN=DC1,CN=Servers,CN=IL,CN=Sites,CN=Configuration,DC=Tes
                                                 tLab,DC=local
LastOriginatingChangeDirectoryServerInvocationId : dcf5bfca-1e1d-43c0-85a2-c79e118fc1ad
LastOriginatingChangeTime                      : 7/11/2021 10:47:47 AM
LastOriginatingChangeUsn                       : 29013
LastOriginatingDeleteTime                      :
LocalChangeUsn                                 : 12514
Object                                         : cn=testu,cn=users,dc=testlab,dc=local
Server                                         : NY-DC.TestLab.local
Version                                        : 1
```

כמו כן נוכל להבחין בשעת השינוי , בצורה זו נוכל לבצע מעקב לשינויים שבוצעו במאפיינים של AD באתרים השונים

מומלץ לעבור על המאמר הבא הנוגע לפקודה : repadmin

https://social.technet.microsoft.com/wiki/contents/articles/50788.active-directory-repadmin-tool.aspx#Initiate_replication_event_between_two_replication_partners

הסבר לגבי הפקודה : DCDIAG לביצוע דיאגנוסטיקה :

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731968(v=ws.11)

https://theitbros.com/dcdiag/

התקנת Active Directory Replication Status ToolL

נוריד את הכלי מהקישור הבא :

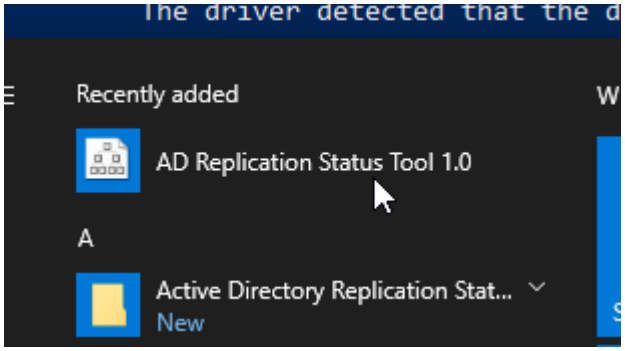
https://www.microsoft.com/en-us/download/details.aspx?id=30005

הסבר על הממשק :

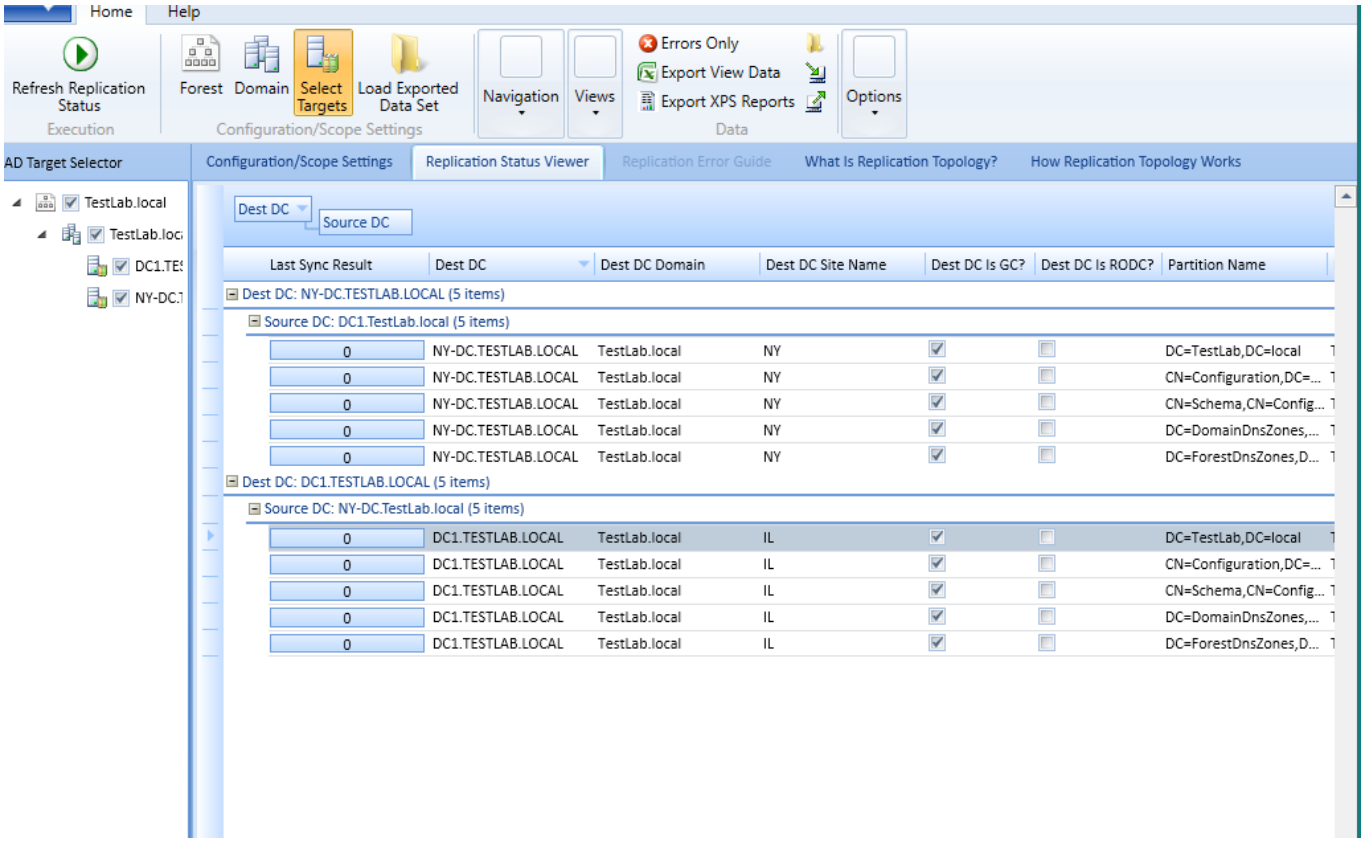
https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/get-use-active-directory-replication-status-tool

נתקין אותו על שרת ב-NY

ניגש ונריץ את הכלי :



נוכל לראות שהרפליקציה תקינה ואין תקלות :



תרגיל יצירת AD TRUSTS

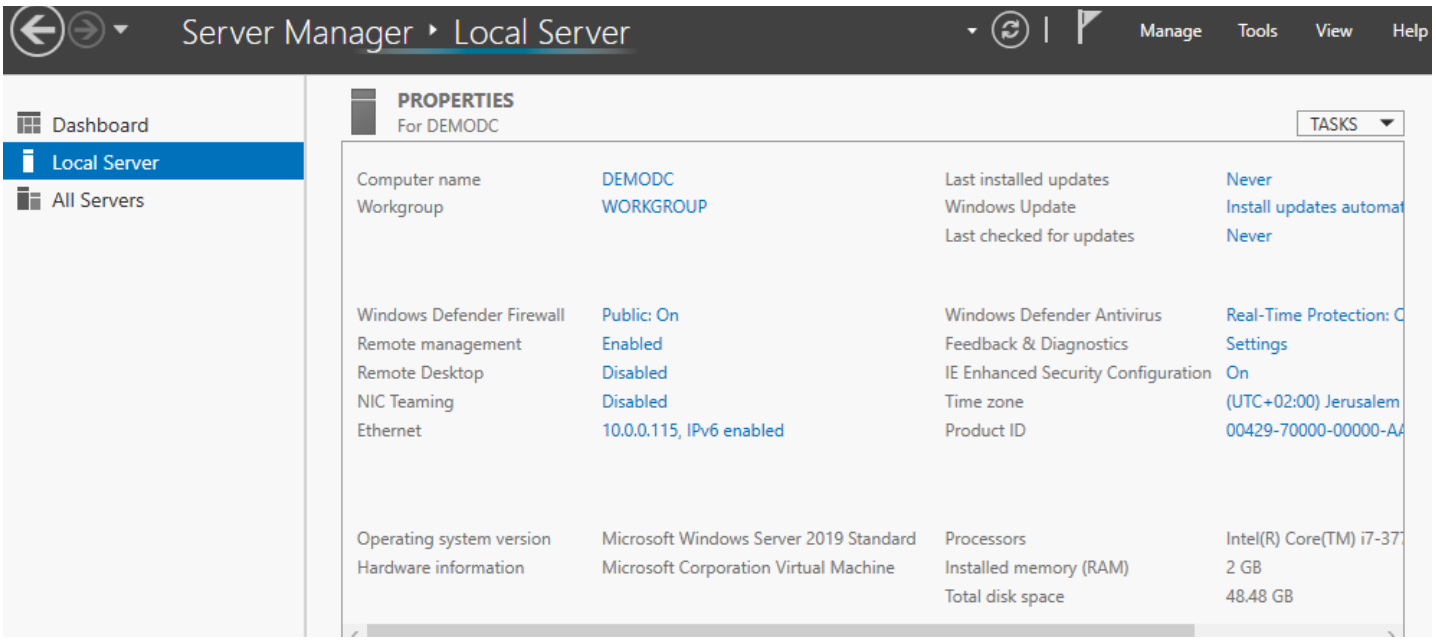
חברת TESTLAB החלה בשיתוף פעולה עם חברת שיווק בשם DEMOLAB , בתור מנהל הרשת בחברת TESTLAB התבקשת ליצור תשתית המאפשרת למנהלי המכירות בחברת DEMODC גישה לתיקייה בשרת הקבצים ב-TESTLAB. היות ושיתוף הפעולה בין החברות הינו הדוק וישנה הכרות עם מנהל הרשת בחברה השניה החלטת ליישם AD FOREST TRUST

שלב א : הקמת החברה DEMODC

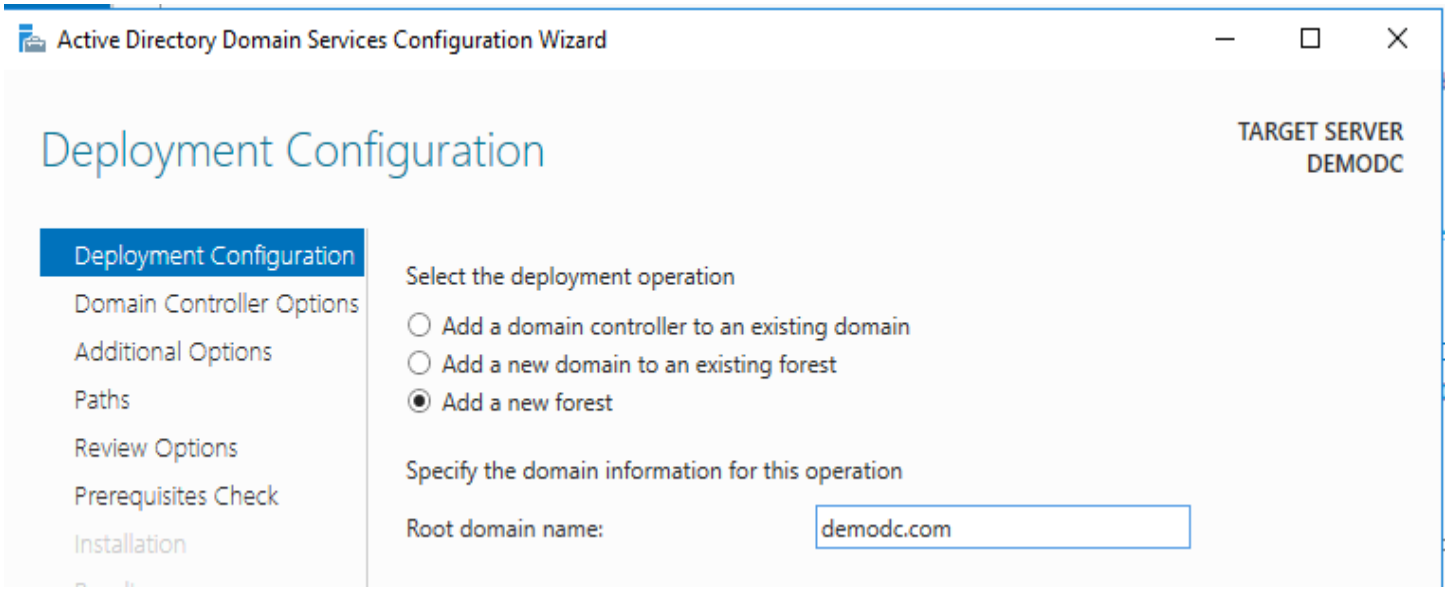
נתקין שרת חדש נשנה את שמו ל-DEMODC , את שם המנהל המקומי ל -Admin ונחבר אותו לסוויץ' הוירטואלי של ת"א

נגדיר כתובת IP : 10.0.0.115/24 (במצב רגיל כתובת ה-IP הייתה מכתובת רשת שונה לגמרי , אך אנו בתנאי מעבדה)

נקים שרת חדש , נתקין עליו את התפקיד של AD DS



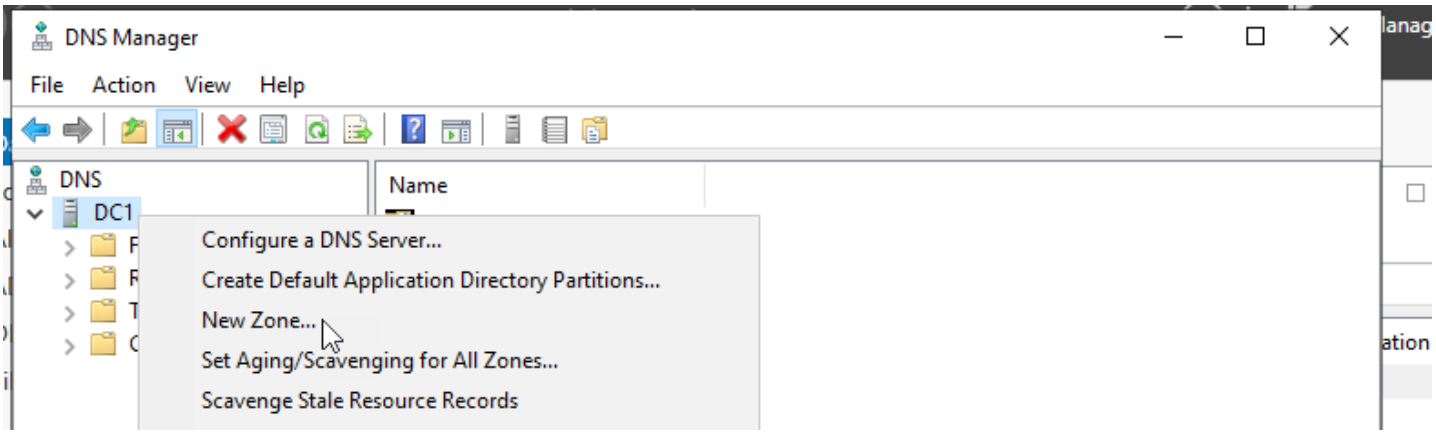
ונקדם אותו לשרת חדש ביער חדש



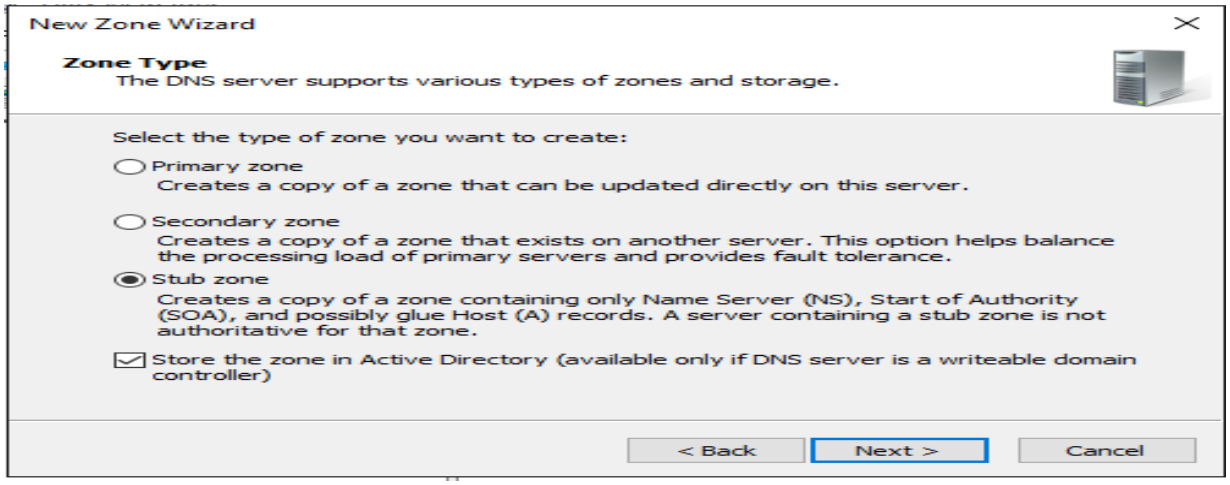
נעבור על שאר הפרטים ונבצע התקנה

שלב ב : הגדרות DNS בשני שרתי הדומיין ביערות השונים

ניגש לשרת ה-DNS שלנו DC1 בדומיין ונגדיר STUB ZONE (הסברים לגבי DNS יגיעו בהמשך)

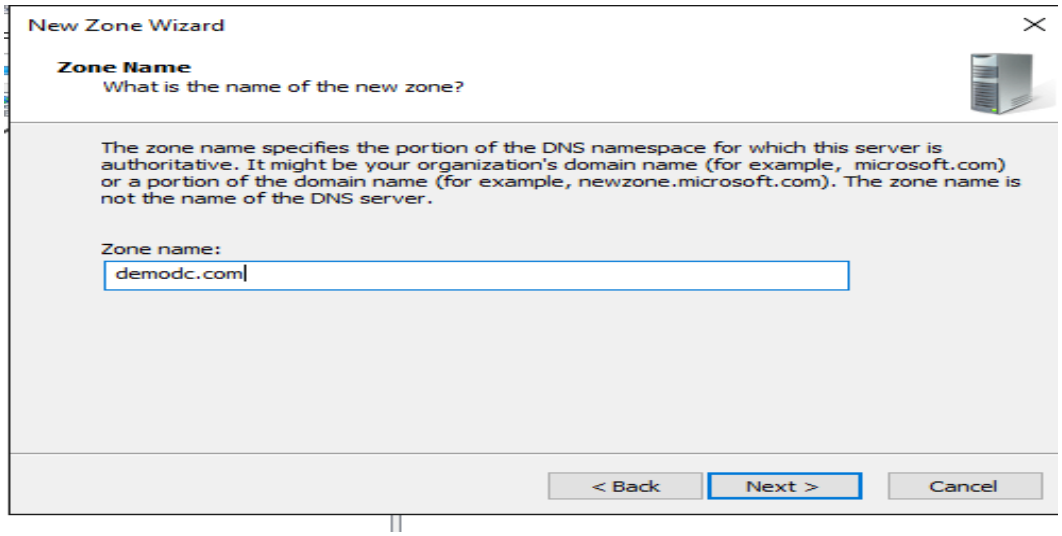


נעמוד על Forward Lookup Zones ונבחר ליצור Zone חדש מסוג STUB

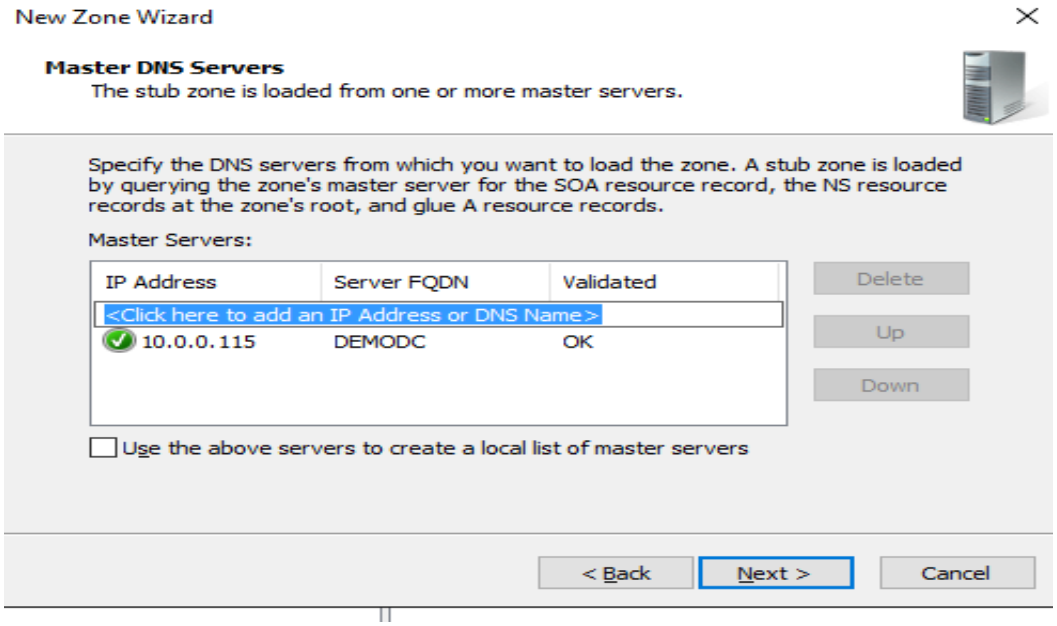


- Stub Zone - יאפשר לנו לקבל רק עותק חלקי של ה-DNS באתר השני , כלומר לא את כל האובייקטים שאותם נרצה לחפש אלא רק את שרתי הDNS בצד השני , זוהי הגדרה שימושית כאשר אין לנו יחסי אמון מלאים עם הארגון השני .

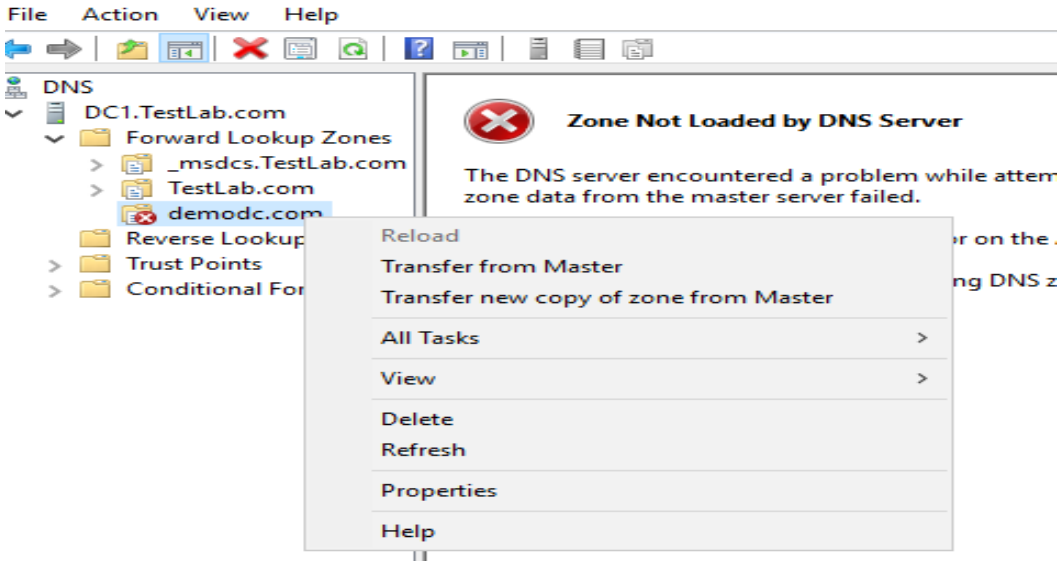
נזין את שם האתר :



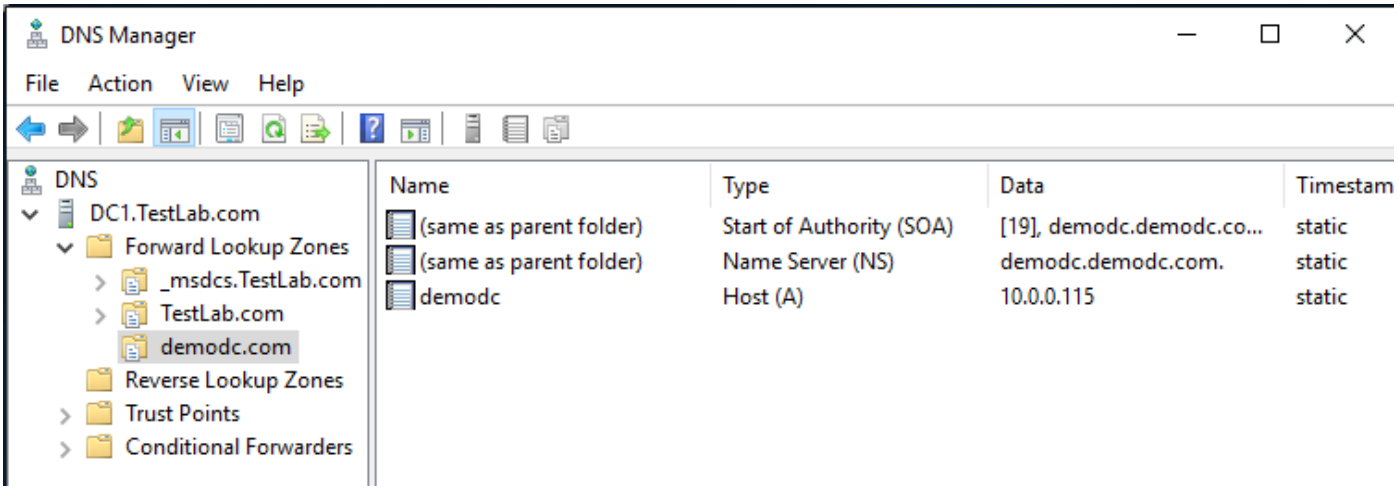
נקליד את כתובת שרת ה-DNS



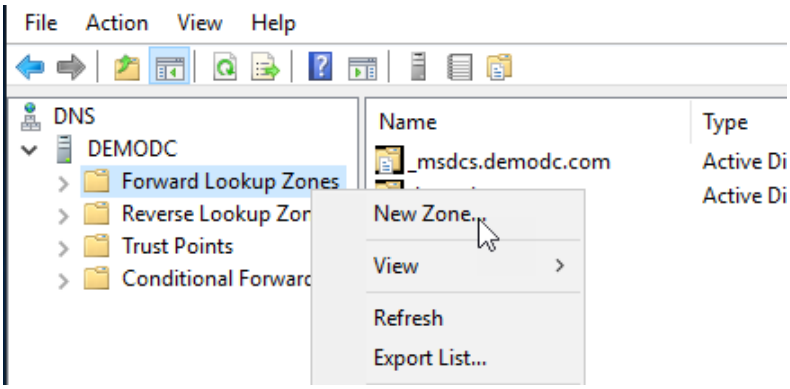
בסיום התהליך נעמוד על ה- STUB ZONE, ונלחץ על העבר מהמאסטר (העתק את הרשומות מהמקור)

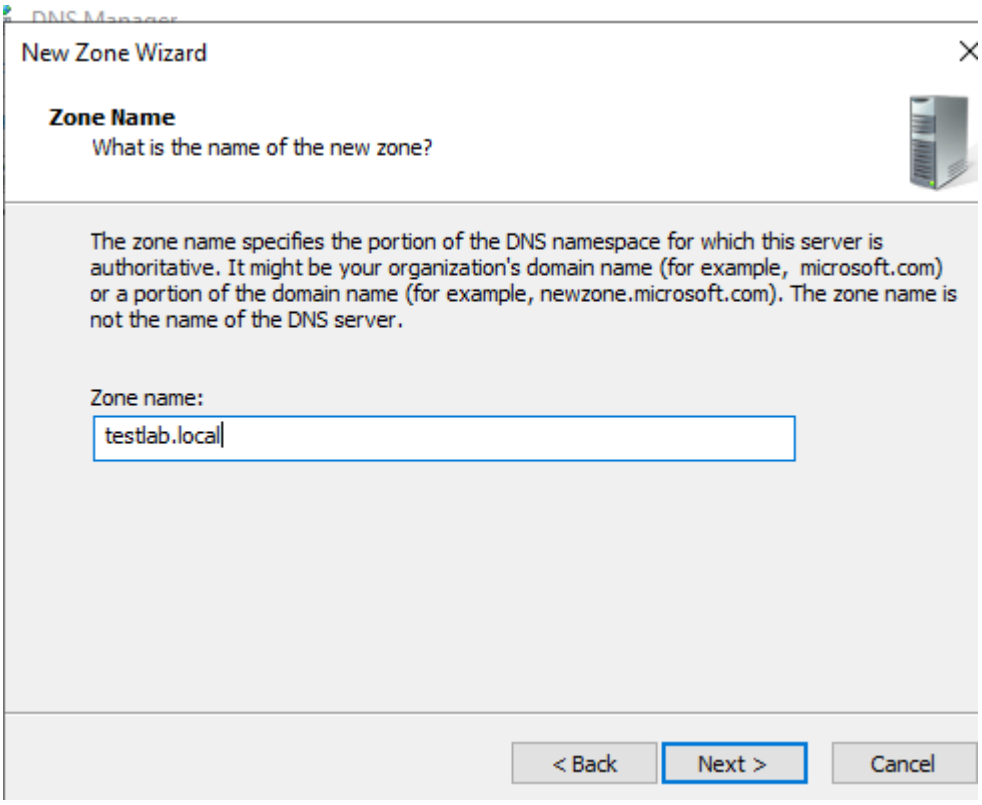


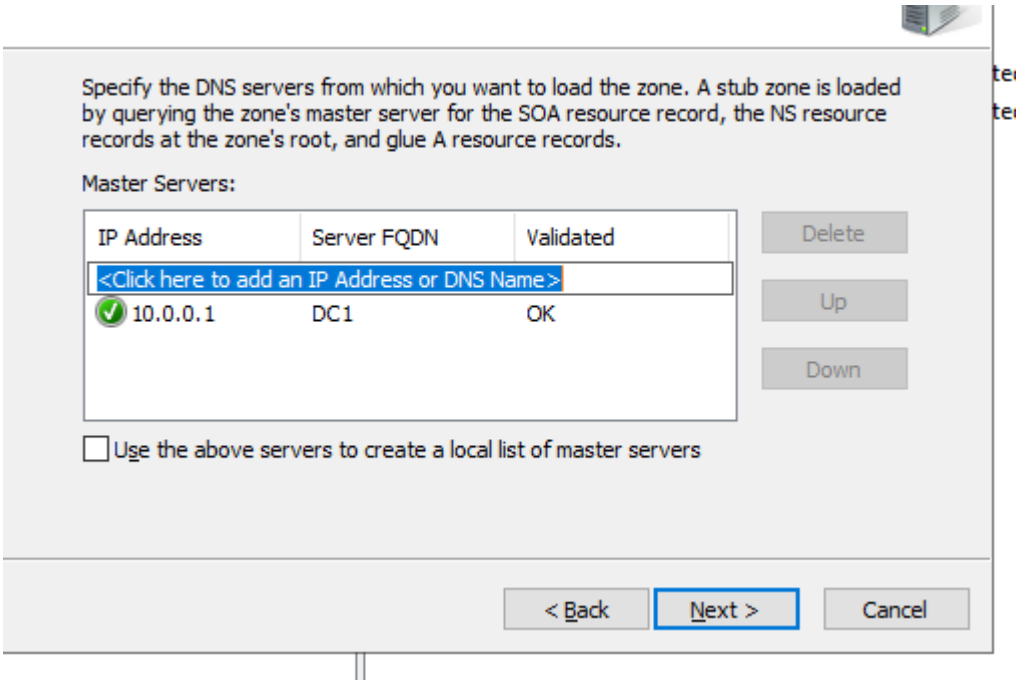
סיום מוצלח :



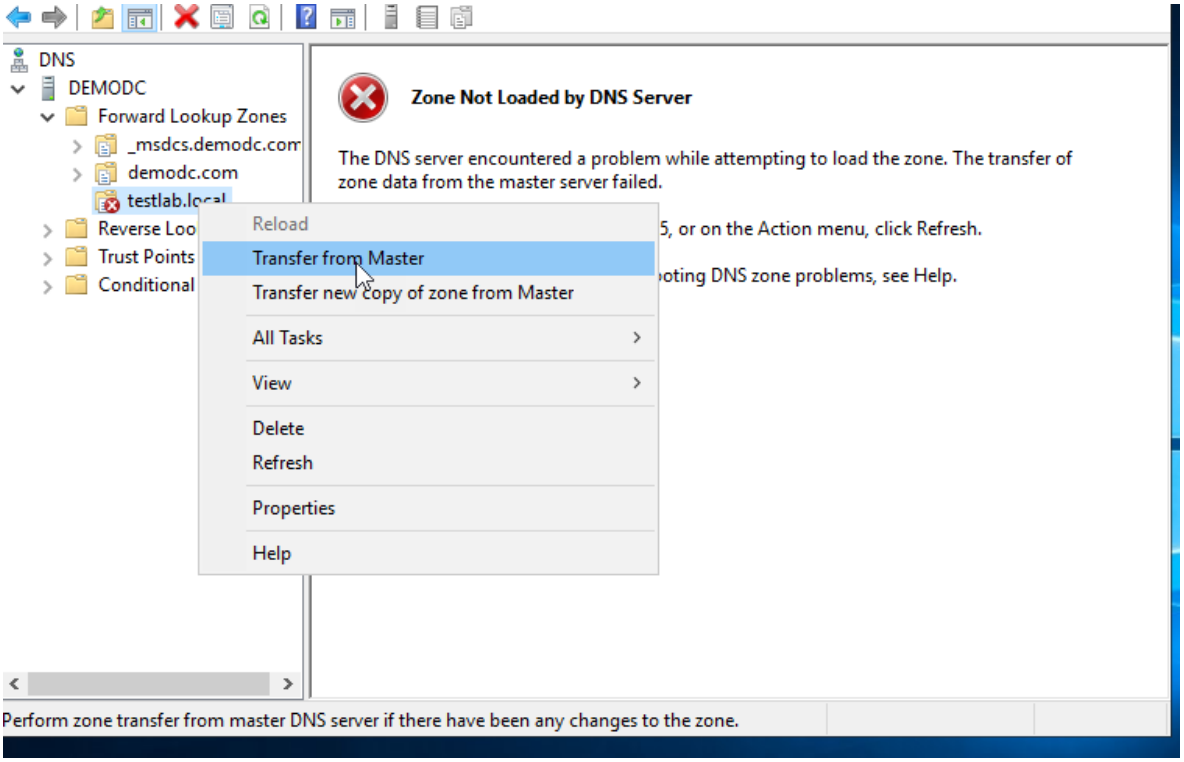
נעשה זאת גם בצד השני :ניגש לשרת DEMODC ונחזור על התהליך הפעם הפוך





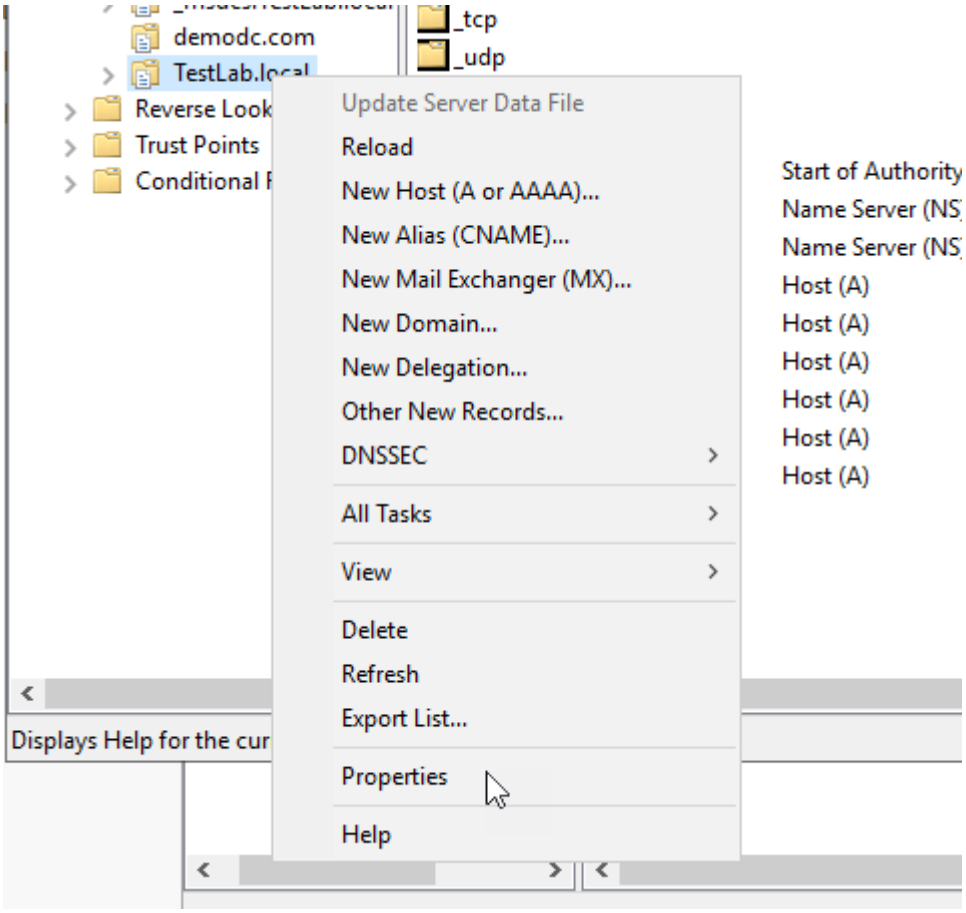


נבצע משיכה מהשרת :

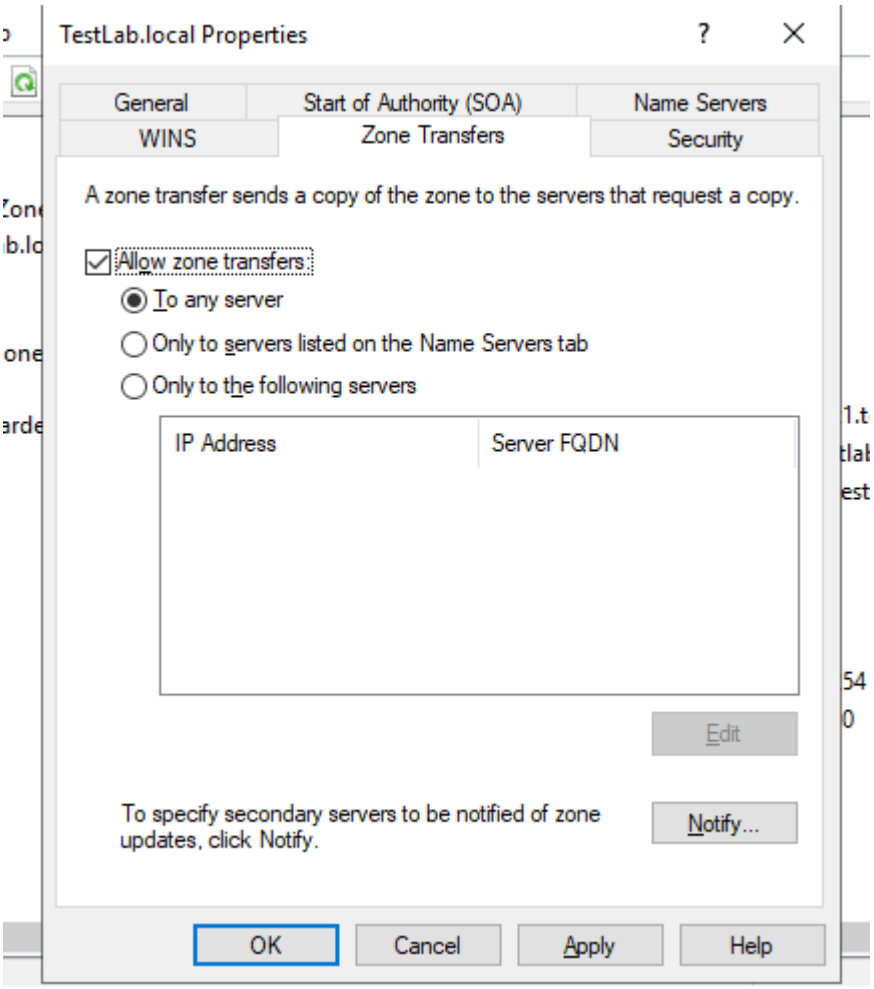


במידה והמשיכה לא מתבצעת ניגש לשרת DC1 ונבצע אישור לתהליך :

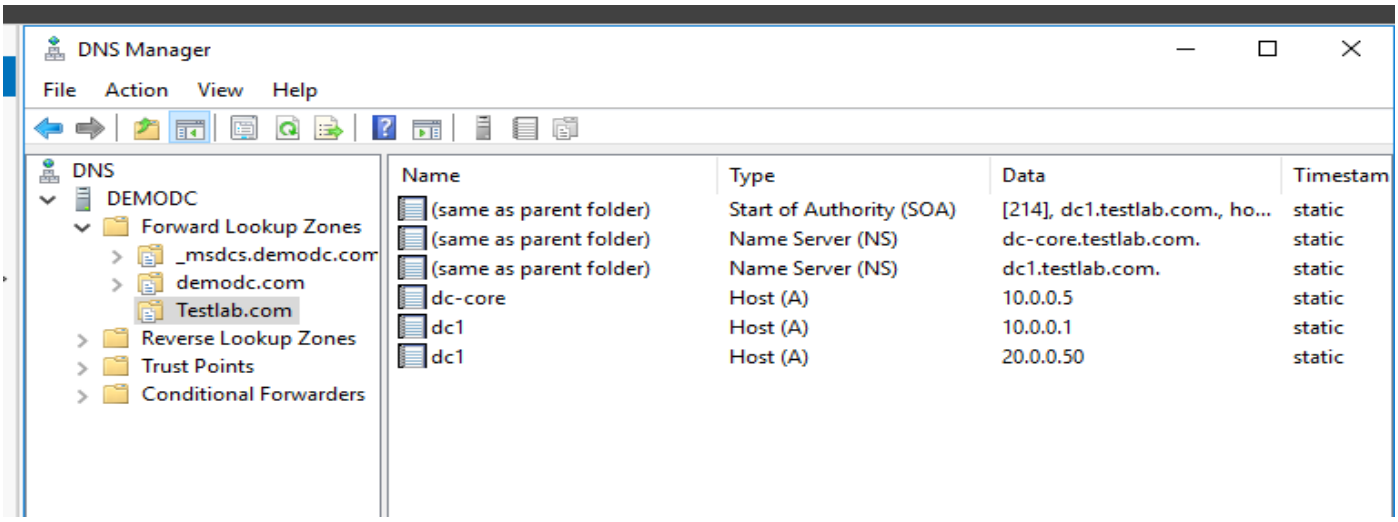
ניגש למאפייני ה-ZONE ונבחר לאשר העברת הרשומות לכל שרת (אנו עושים זאת היות ואנו בתנאי מעבדה, בסביבת ייצור היינו בוחרים את הכתובת של השרת מולו יבוצע התהליך)



בלשונית Zone transfers נבחר כל שרת :

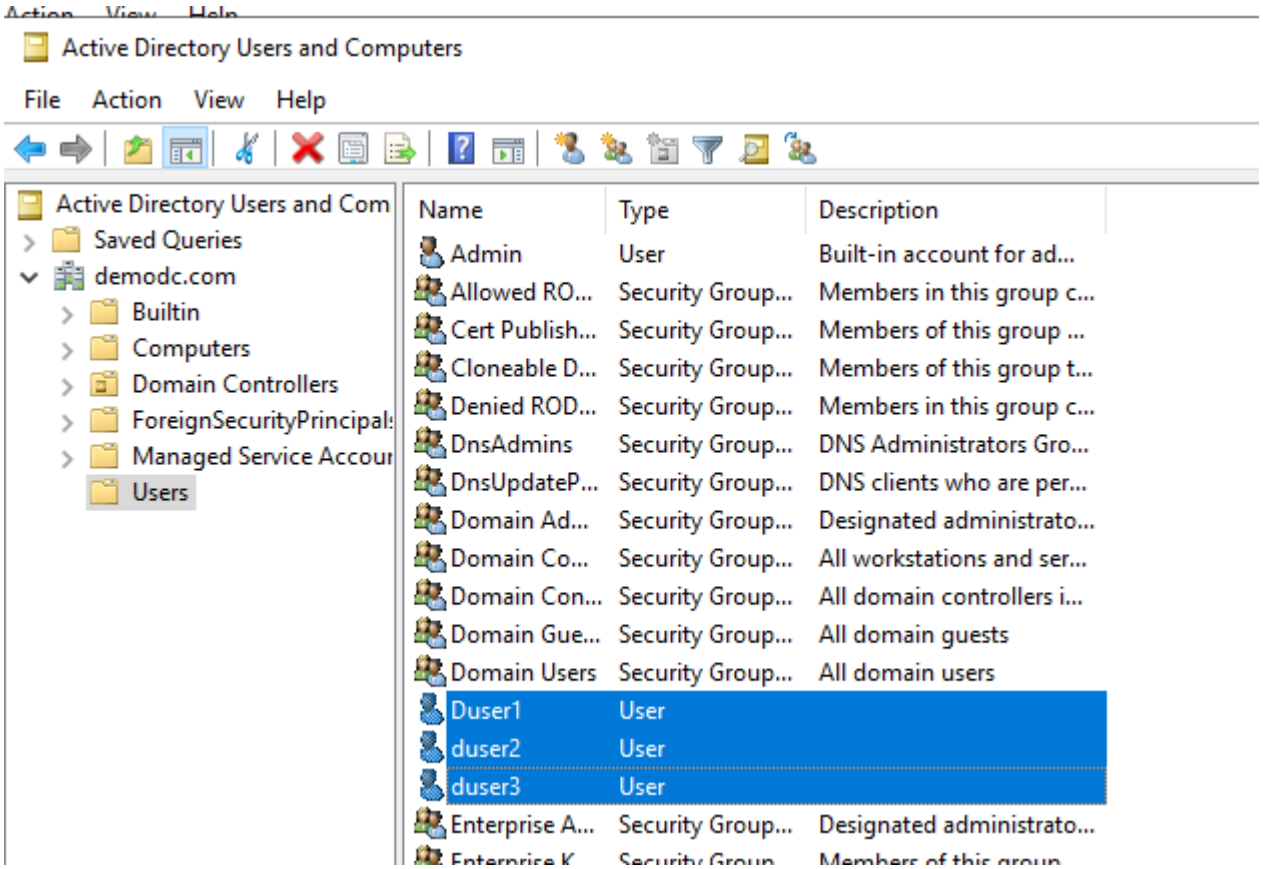


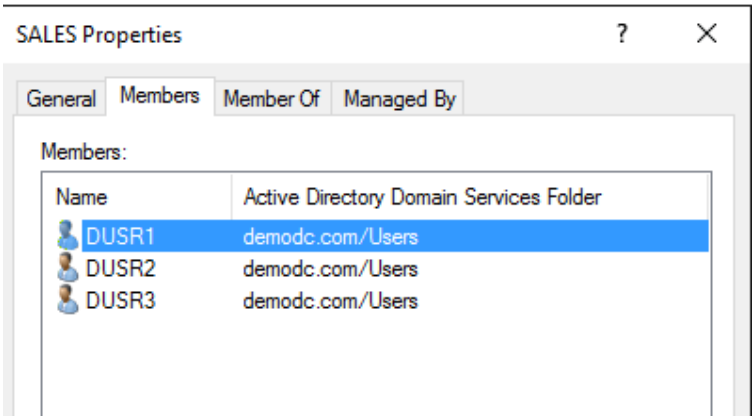
נחזור לשרת DEMOCD ונבצע את המשיכה



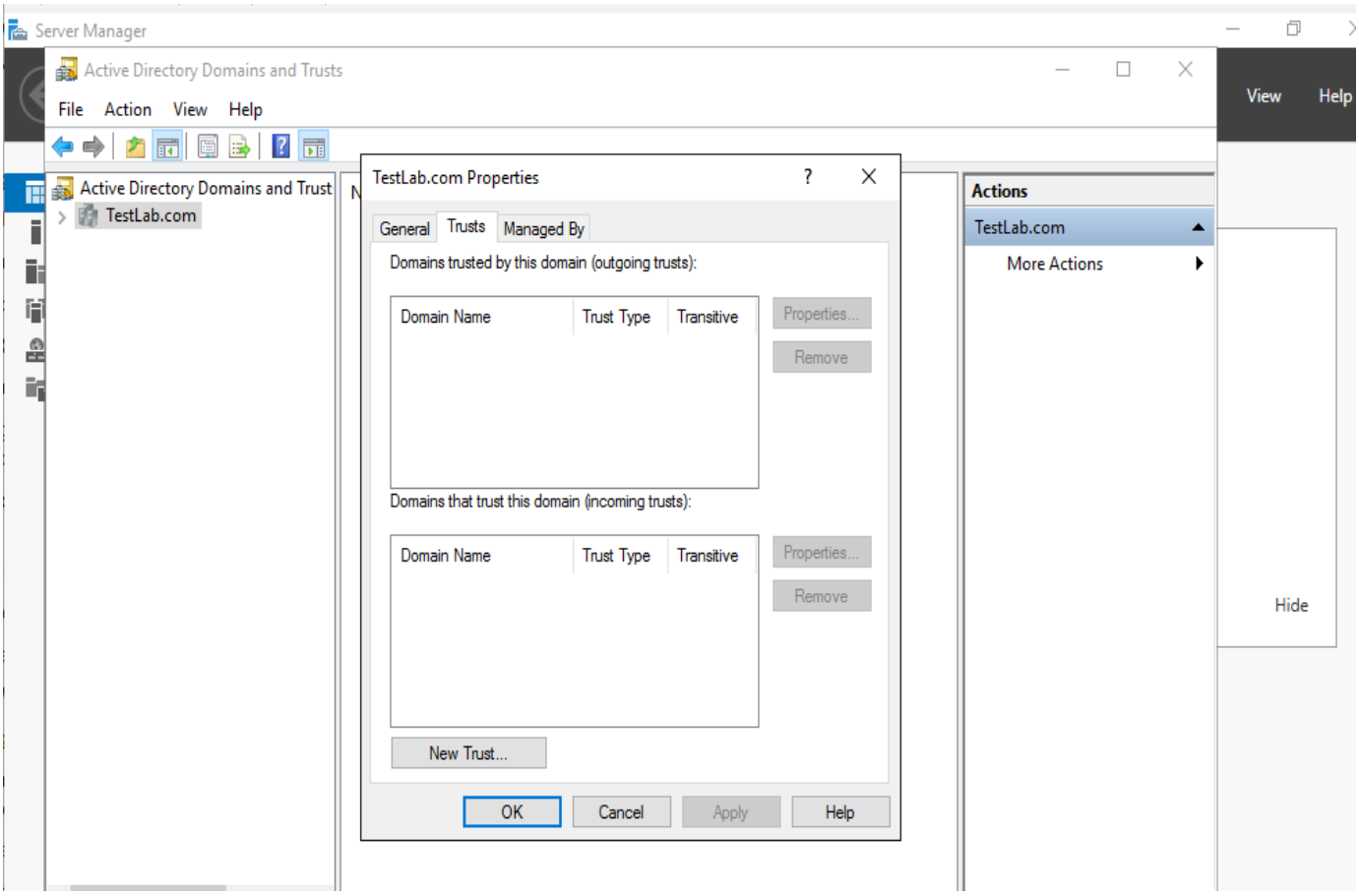
כעת נוכל לעבור לשלב הבא :

בממשק AD Users & Computers נגדיר שלושה משתמשים בשם DUSR1..3 עם הסיסמה Pa55w.rd, ניצור קבוצת SECURITY בשם SALES ונשייך אותם אליה

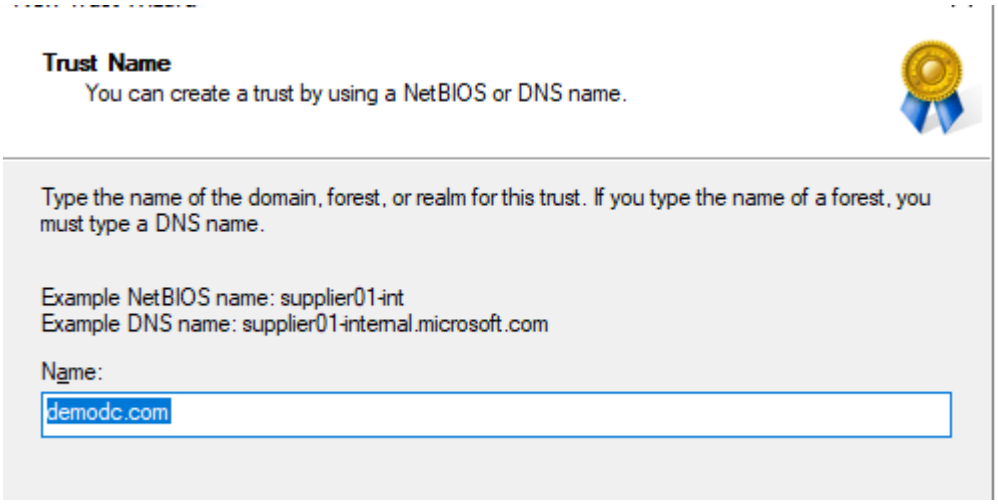




נעבור ל- DC1 וניכנס לממשק Active Directory Domain and Trusts נעמוד על מאפיינים וניכנס לטאב של TRUSTS

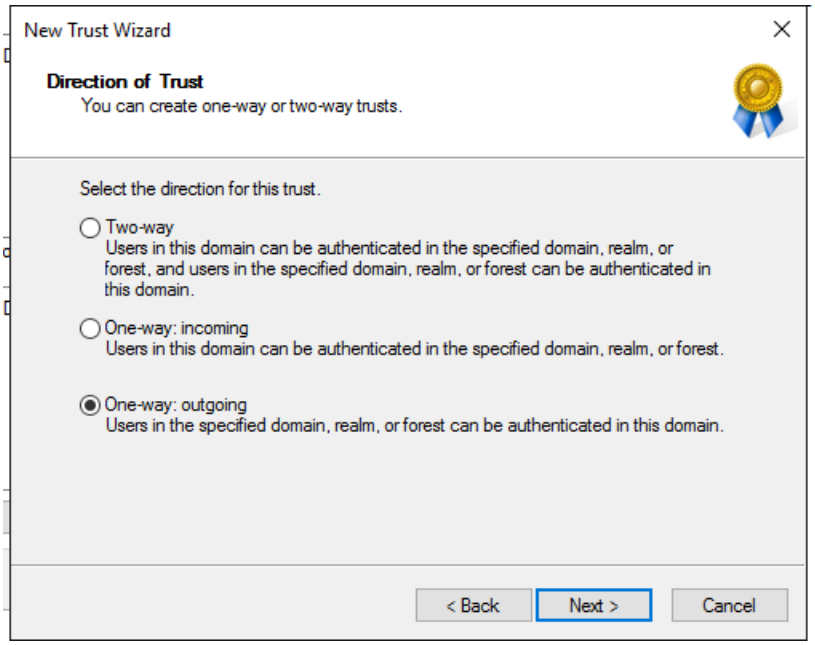


נבחר NEW TRUST, נעניק לו את השם demodc.com

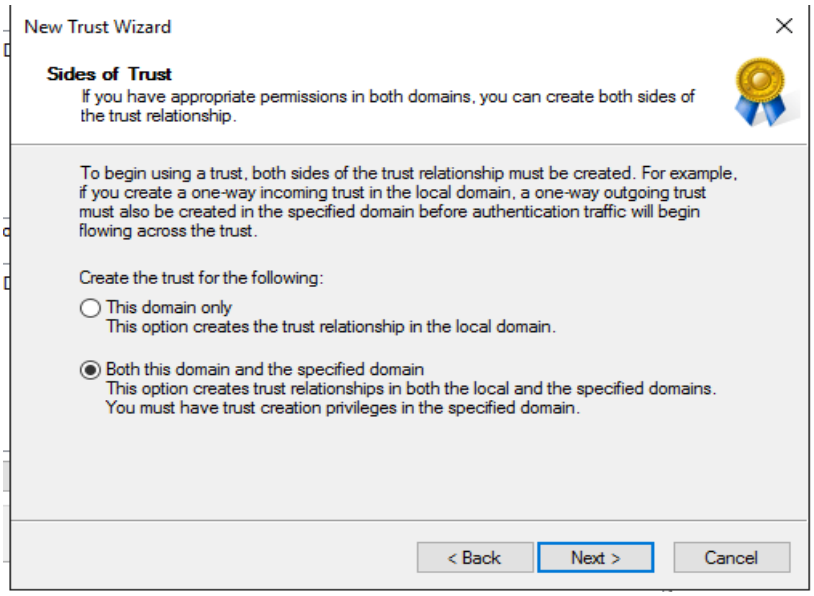


בסוג נבחר FOREST TRUST

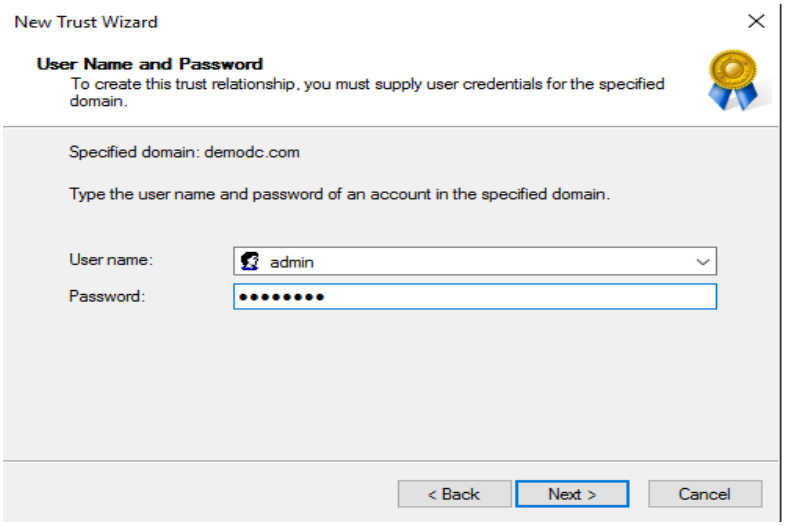
- נבחר את כיוון ה-Trust



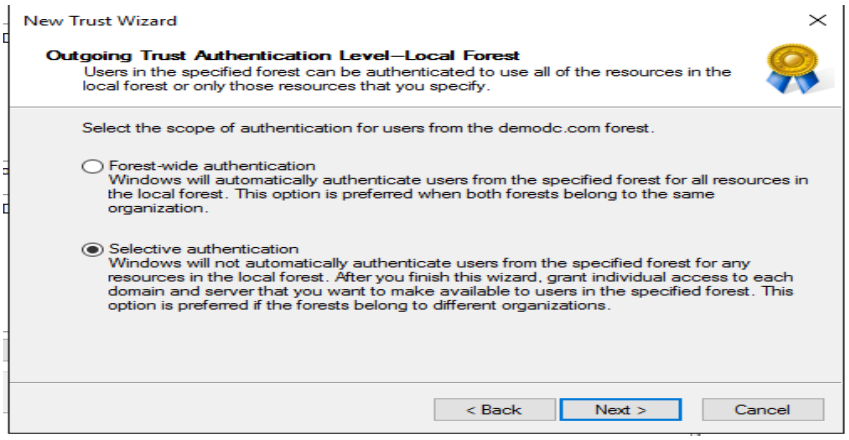
נבחר לבצע אימות מול שני הצדדים :



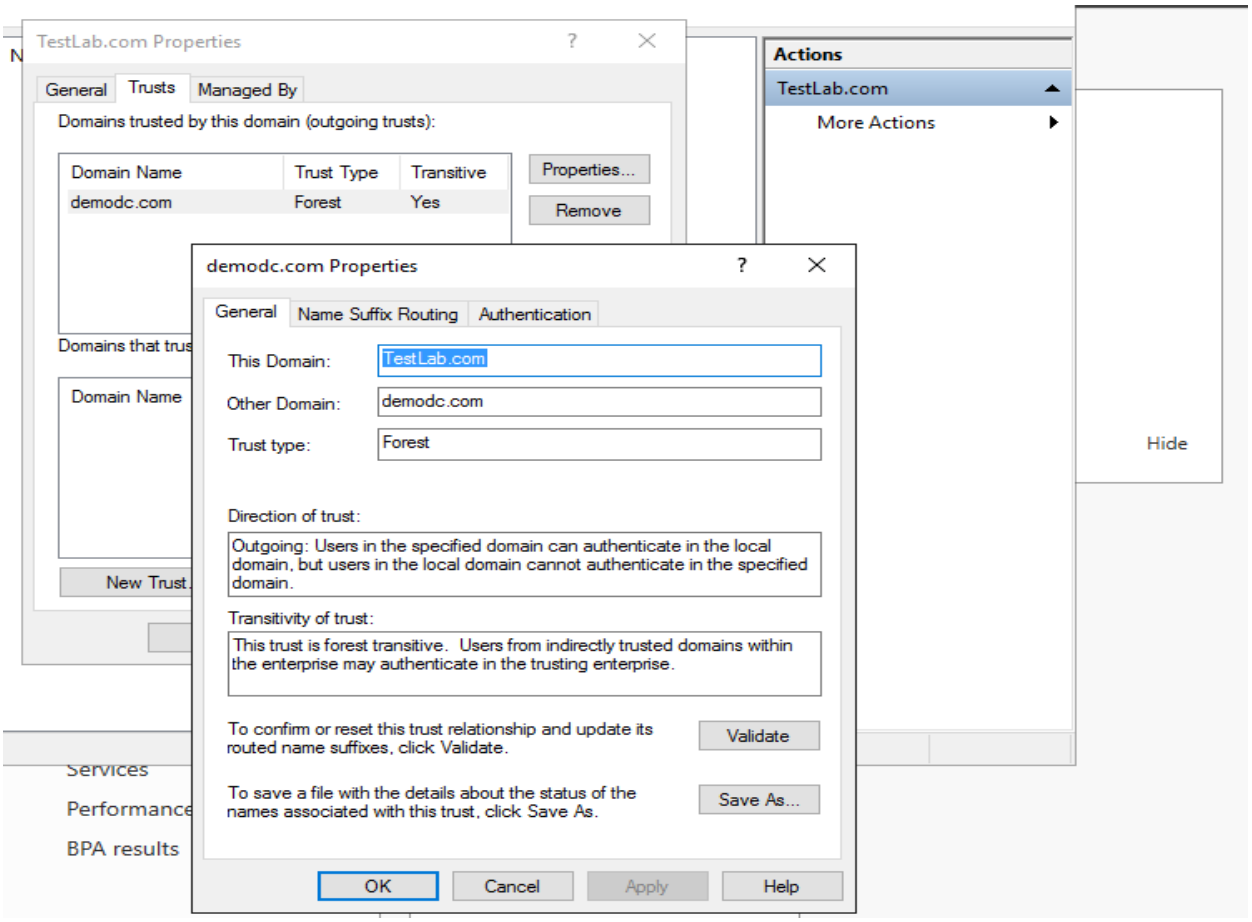
נזין את פרטי המנהל בדומיין השני :



נבחר אימות סלקטיבי כיוון שאנו רוצים להעניק רק לחברים בקבוצת SALES הרשאות

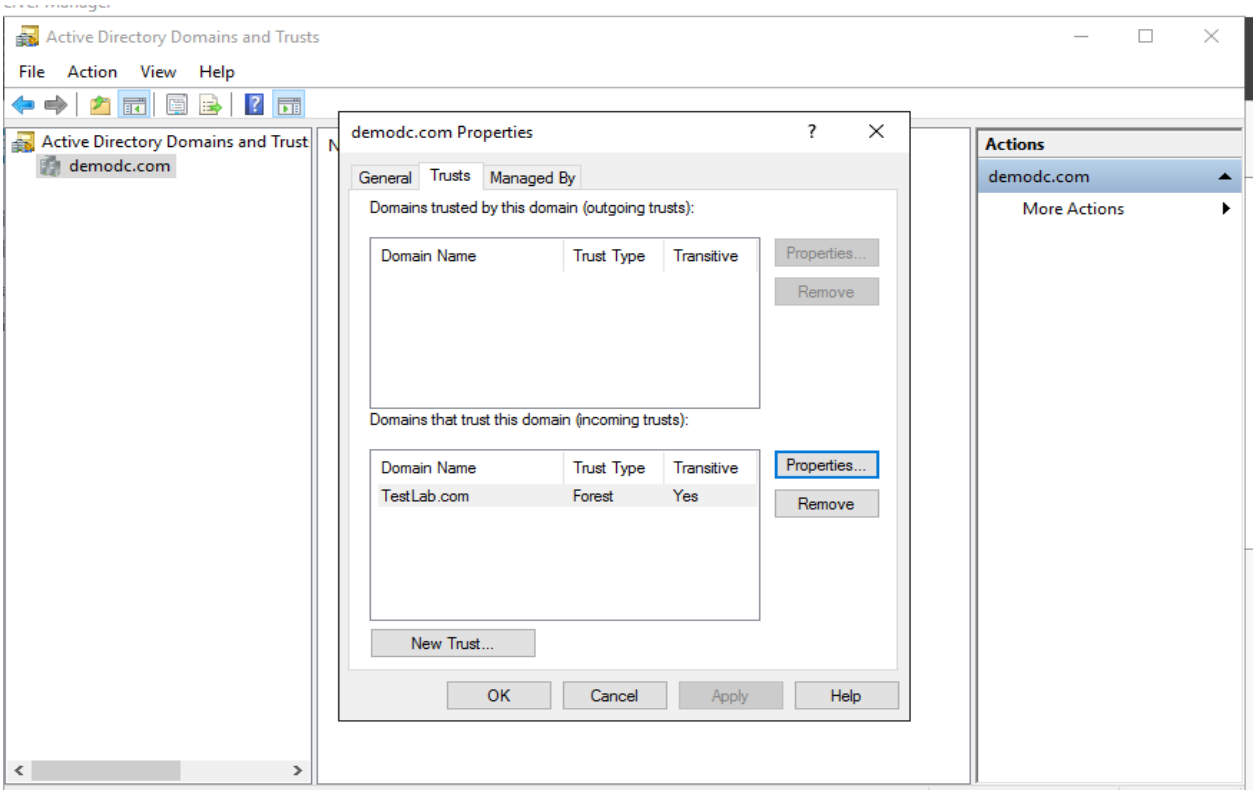


נלחץ NEXT עד לסיום ההתקנה , במסך הבא נעמוד על demodc.com נבחר מאפיינים

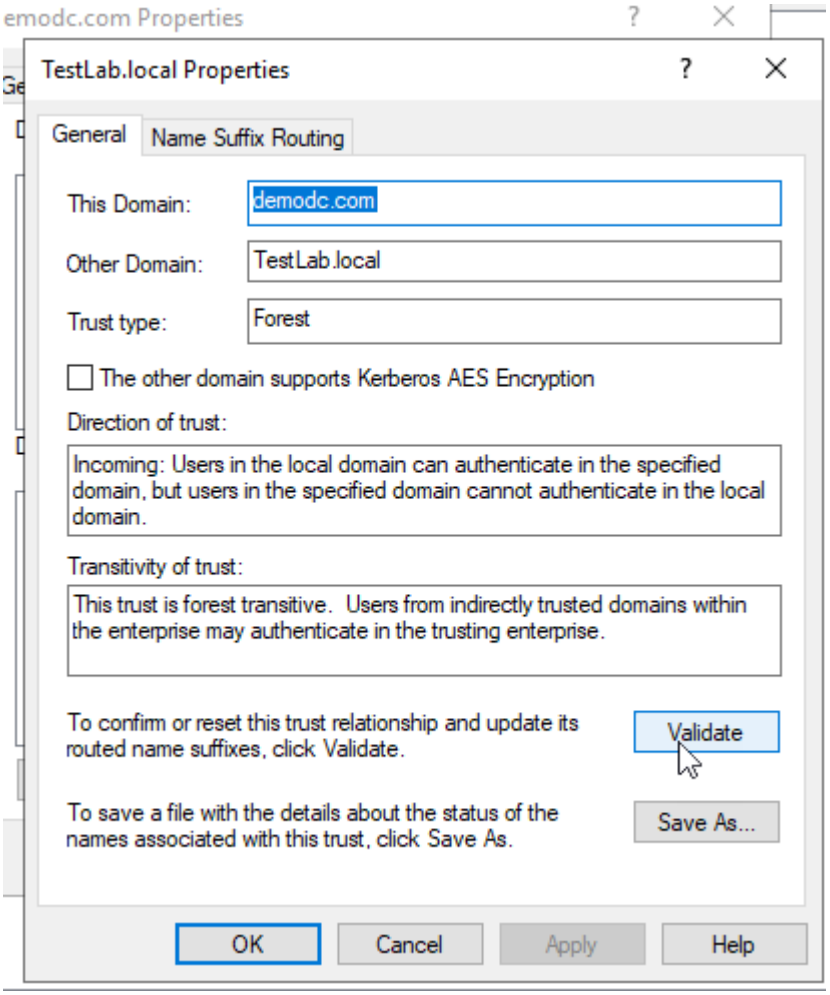


ונבחר VALIDATE ע"מ לוודא שהרישום אכן עבר כמו שצריך

נבצע את האימות גם בשרת השני DEMODC:

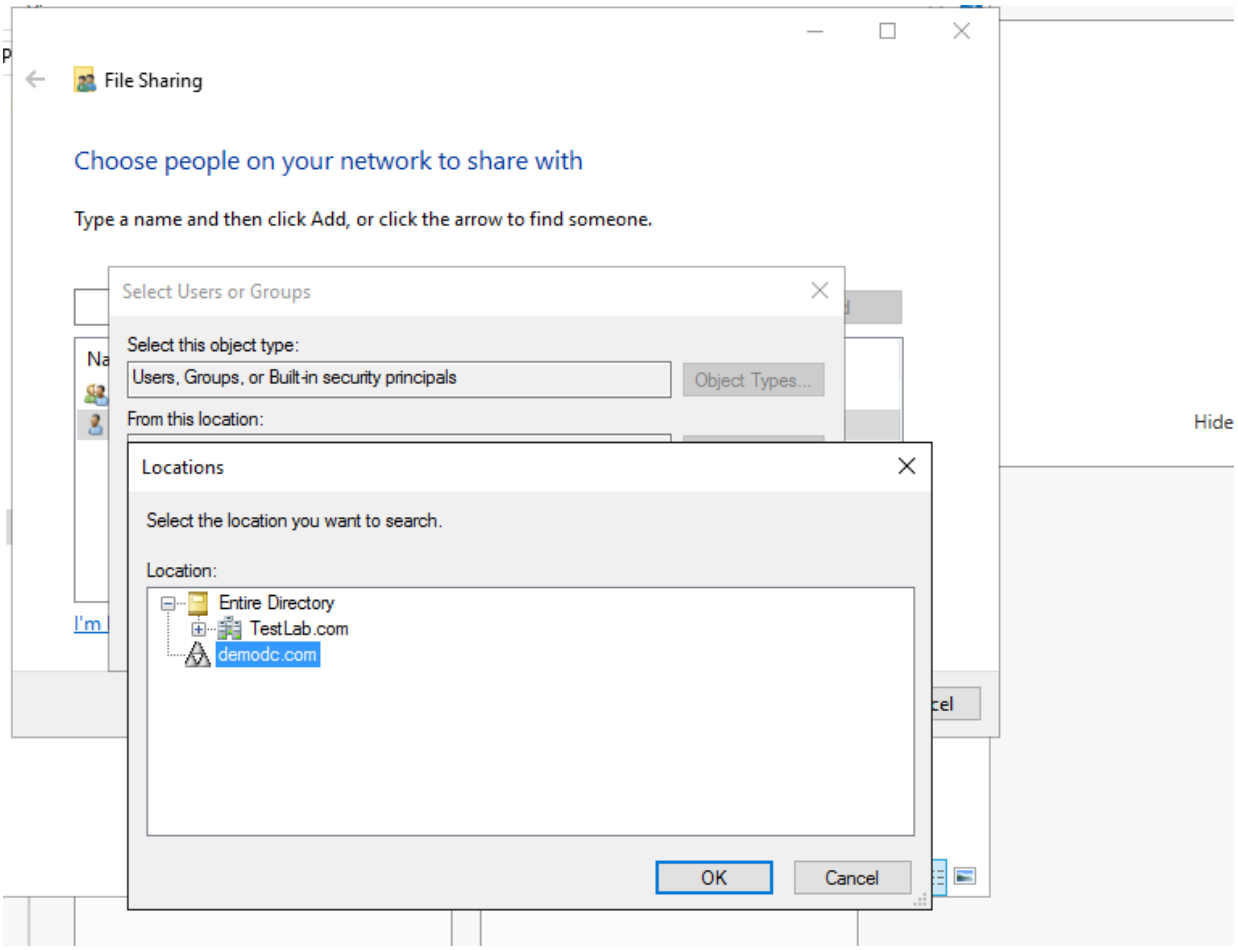


נזין את הרשאות המנהל בדומיין TESTLAB ונוודא שה TRUST פעיל

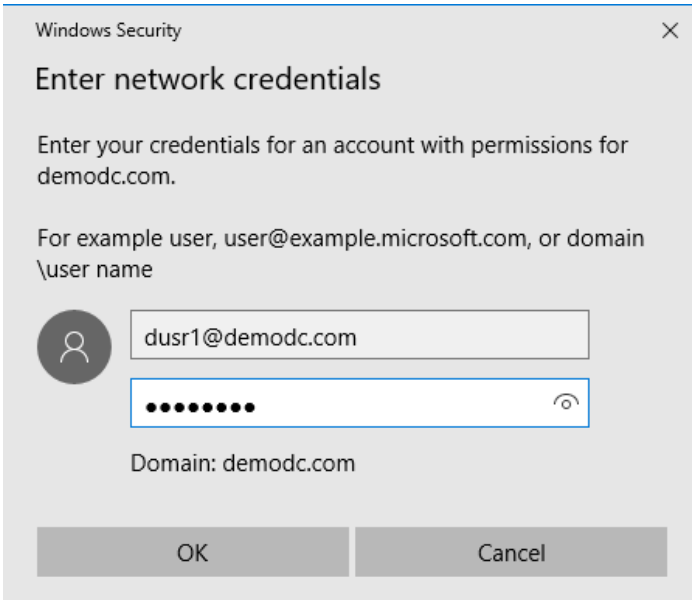


שלב ג : בדיקה של ה-TRUST

בשרת DC1 ניצור תיקייה משותפת ונשתף אותה עם הרשאות קריאה וכתיבה לקבוצת SALES בדומיין DEMODC



בהרשאות נבחר במיקום את הדומיין demodc.com נבחר את קבוצת SALES ונזין את ההרשאות של משתמש כלשהו בדומיין השני



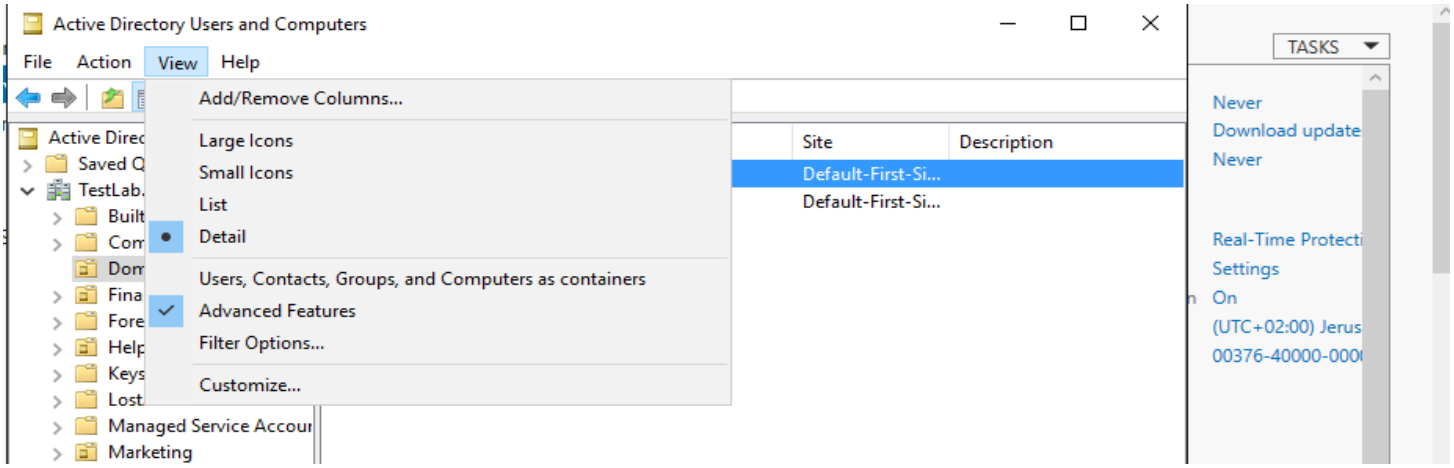
בשרת DEMODC נצרף את ה ADMIN לקבוצת SALES ונבצע בדיקה להתחברות ....

אנו עושים זאת כיוון שאין לנו מכונת קליינט ולמשתמשים רגילים אסור להתחבר לשרת – מי שרוצה יכול לצרף מכונת קליינט לדומיין החדש ולבצע בדיקה עם המשתמשים שיצרנו בסעיף הקודם

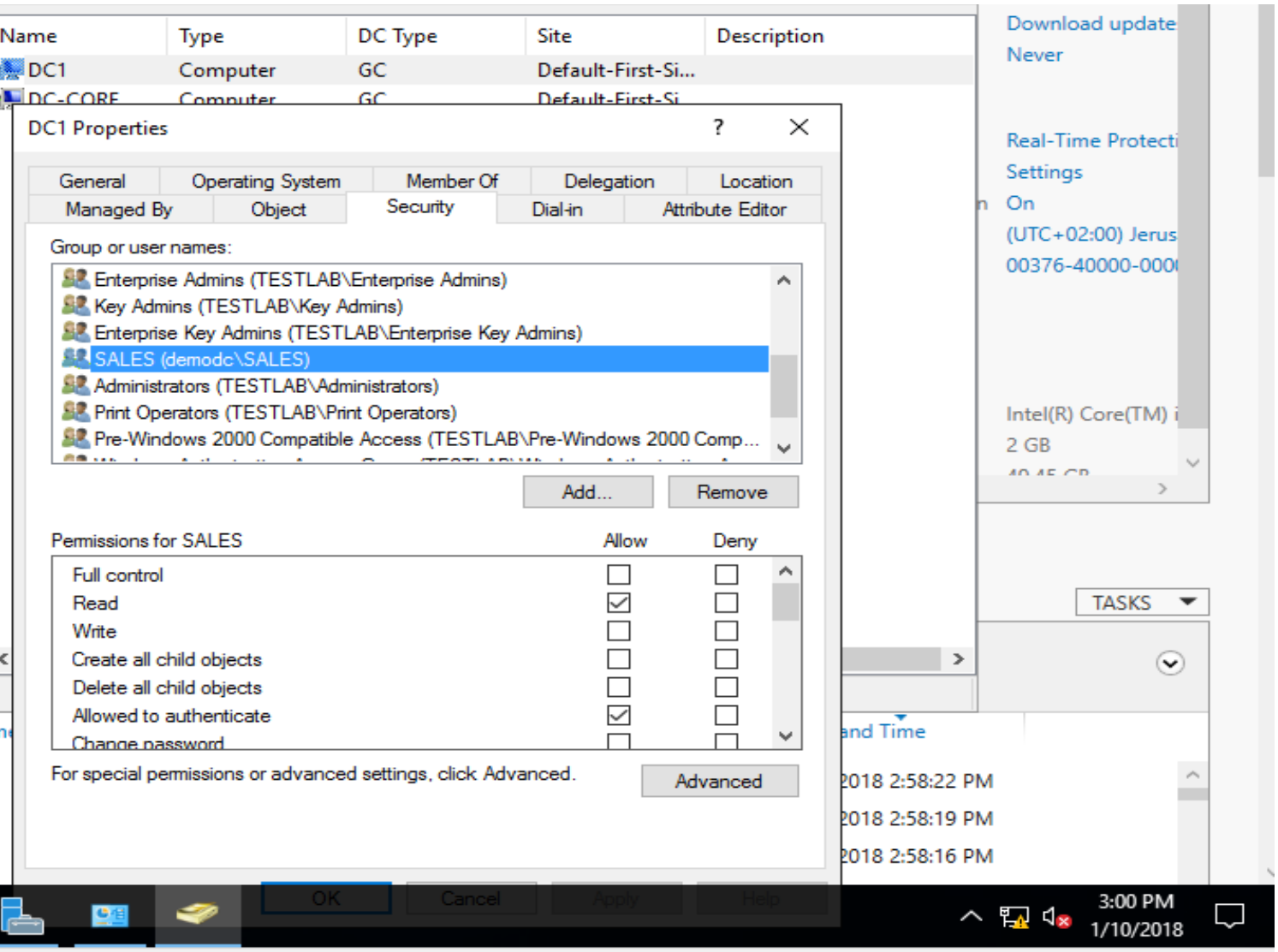
ביצוע הבדיקה :

היות ובחרנו אימות סלקטיבי , ניגש ל- AD Users & Computers

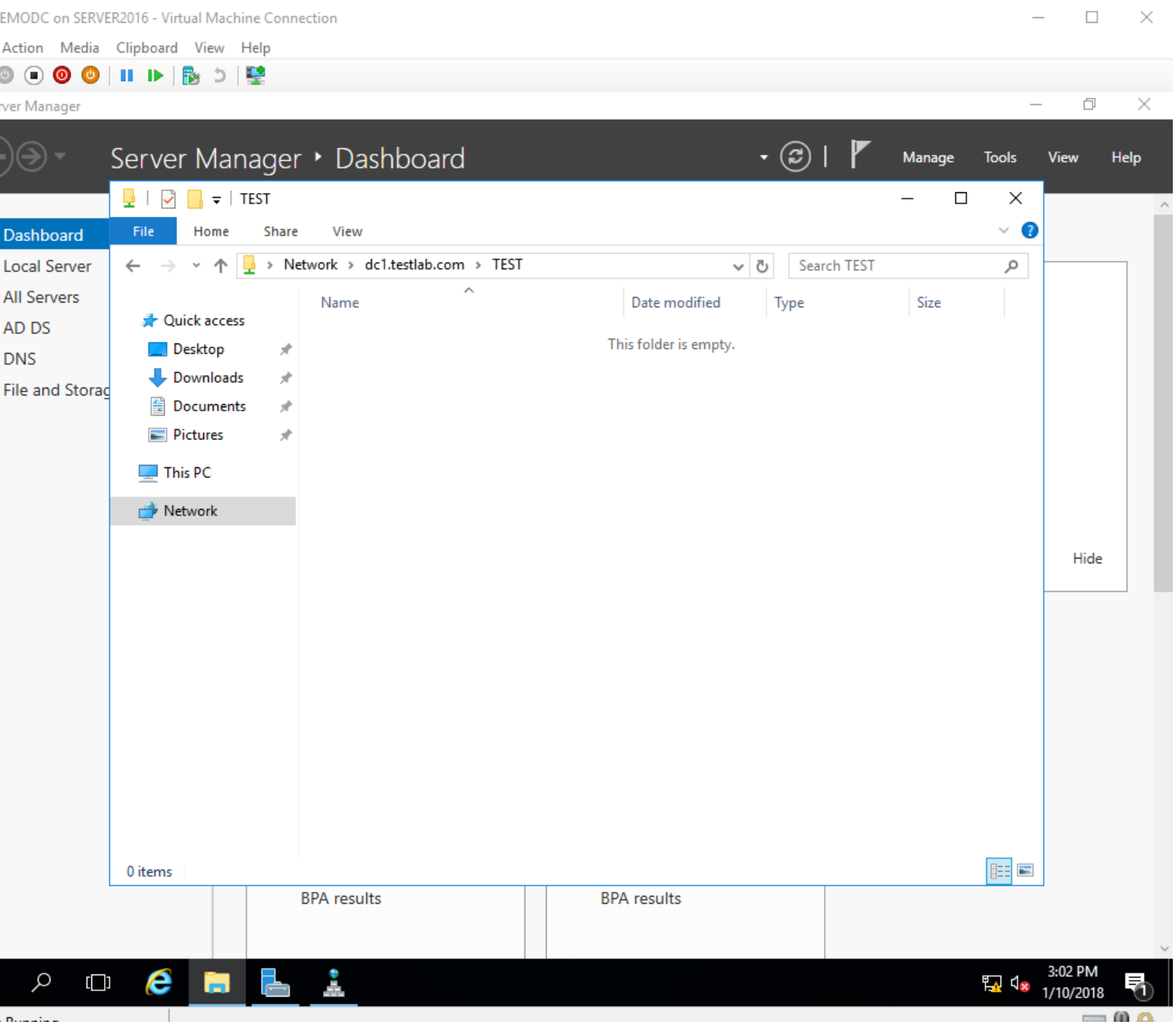
נסמן הצג אפשרויות מתקדמות



ניגש למאפיינים של שרת DC1 - נפתח את לשונית Security ונאפשר לחברי קבוצת SALES מ- DEMODC לבצע אימות מול השרת



נבצע בדיקה : ניכנס משרת DEMODC אל התיקייה בשרת DC1



בשלב זה ניתן למחוק את השרת DEMODC ולמחוק את ה-TRUST ואת ה-STUBZONE שכתוב ב-DNS

בחלק הבא נעסוק בהרשאות NTFS, הגדרות משתמשים , יצירת טמפלייט, הגדרות מחשבים, חשבונות מנוהלים והגדרת ADMIN CENTER