

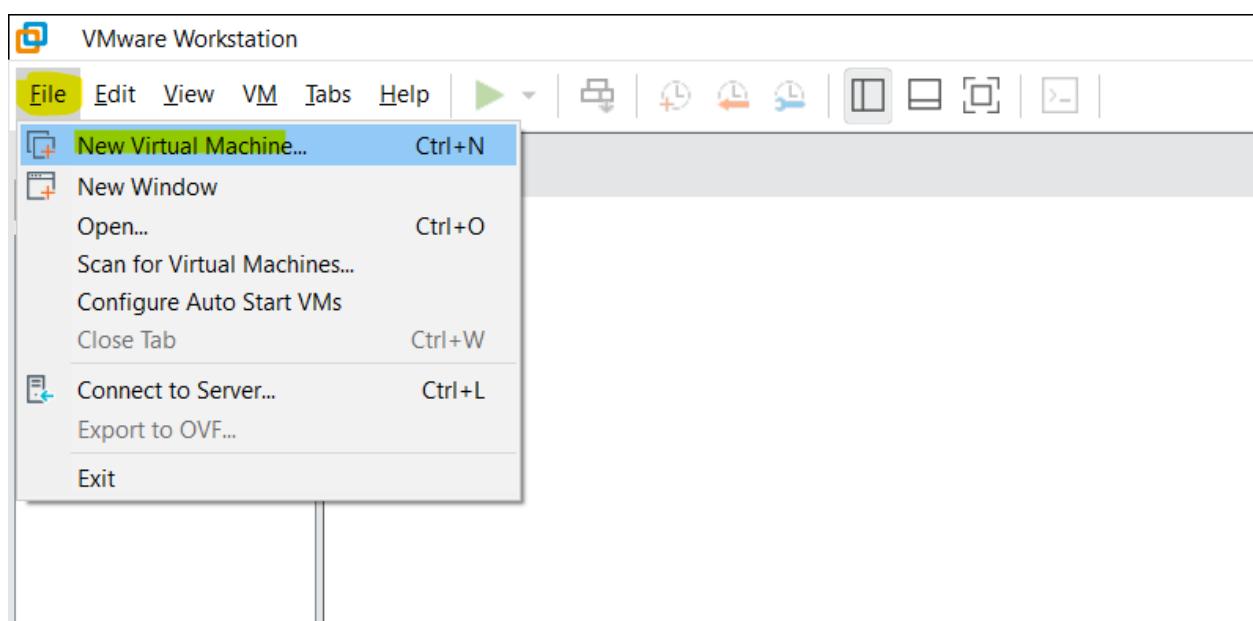
MCSA



By : Mostafa Mahmoud Bahgat

LinkedIn: <https://www.linkedin.com/in/mostafaamahmoud>

هنسخدم برنامج VMware Workstation : Install عشان نعمل ال



1- هنفتح VMware file ومن هنختار New Virtual Machine

New Virtual Machine Wizard

X

vmware
WORKSTATION
PRO™

17

Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

Typical (recommended)

Create a Workstation 17.5 or later virtual machine in a few easy steps.

Custom (advanced)

Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

open it in a tal

Help

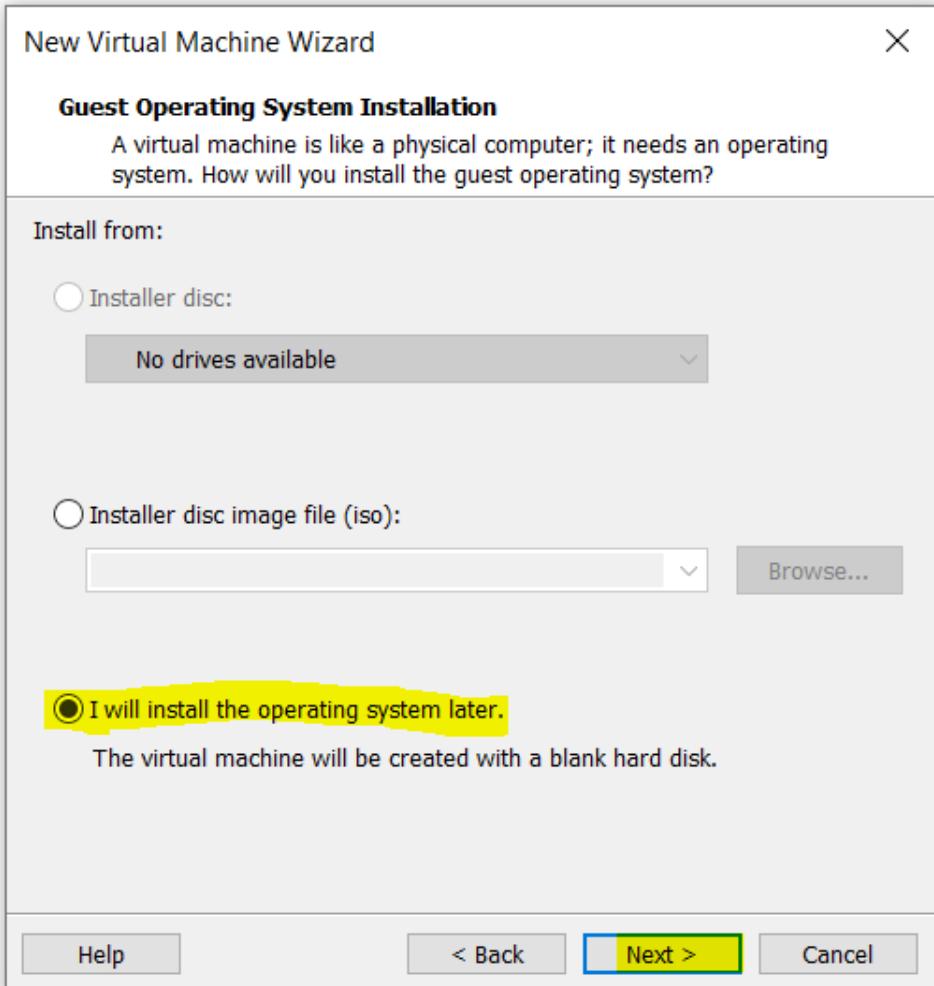
< Back

Next >

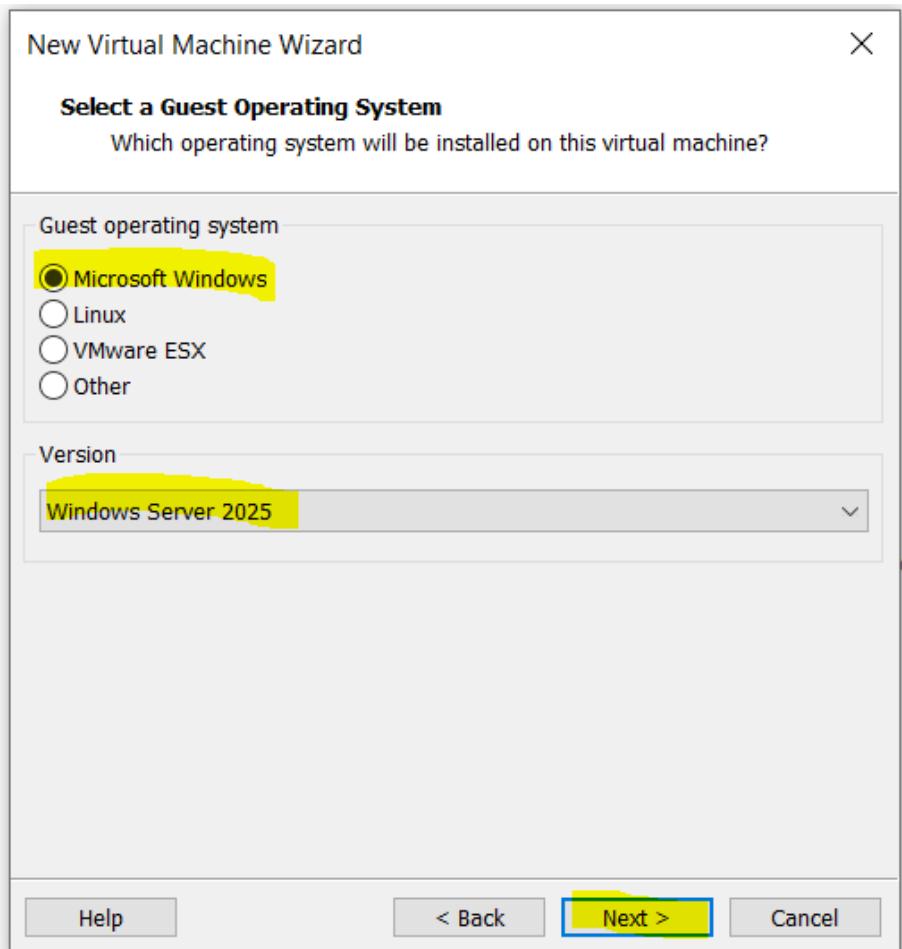
Cancel

Typical - هنختار 2

--



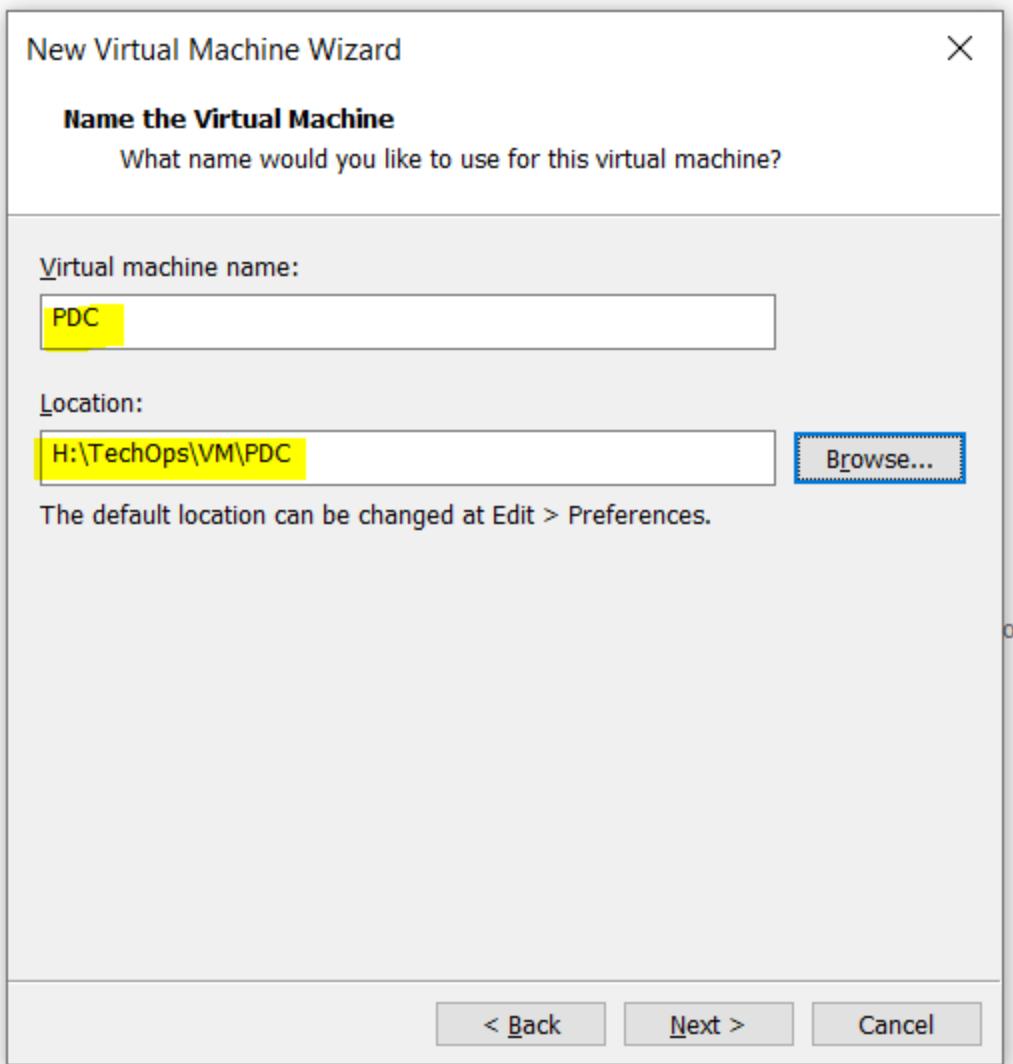
I Will install the os later - 3 هنختار --



open it in a tab.

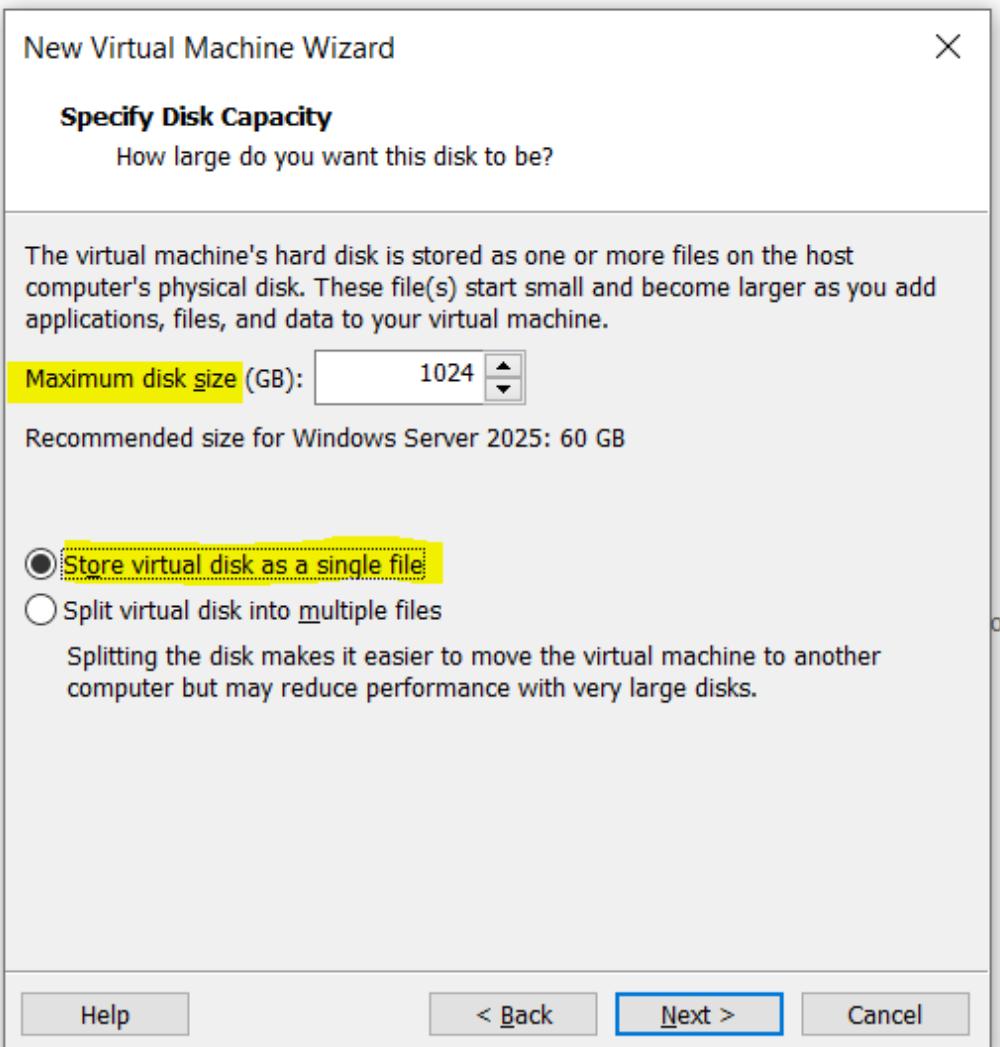
4- هنختار ال Version MS Windows : OS وال هنختاره Windows Server 2025

--



5- هحدد ال name الخاص بال VM وحدد ال path الخاص بال VM (كل ملفات وما يخص ال vm هيكون في ال path دا علي جهازك)

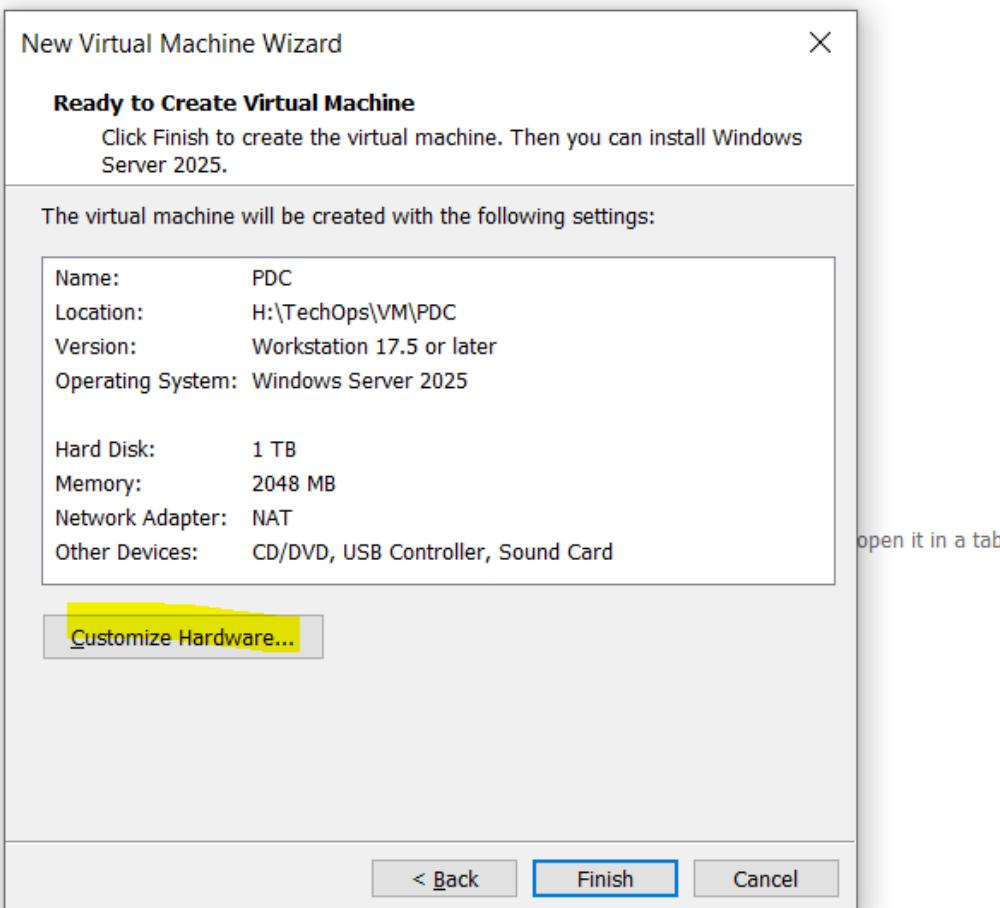
--



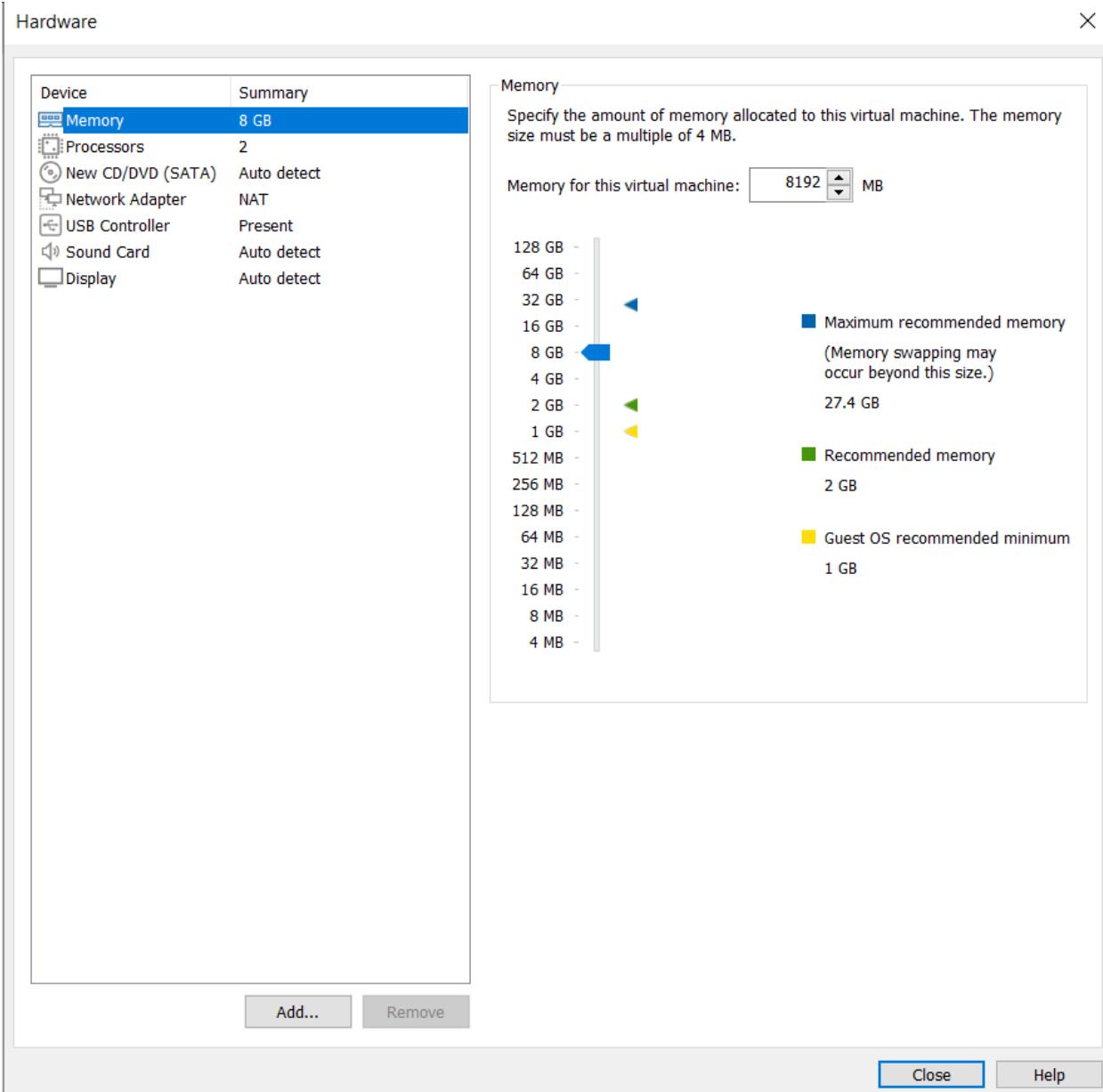
6 – بحدد بعد كدا مساحة ال Disk ، وبيكون فيه option بيفولك عاوزه single file ولا

ال Disk ال single file كله هيكون اك file واحد لو disk هيكون متقسم لاكثر من file

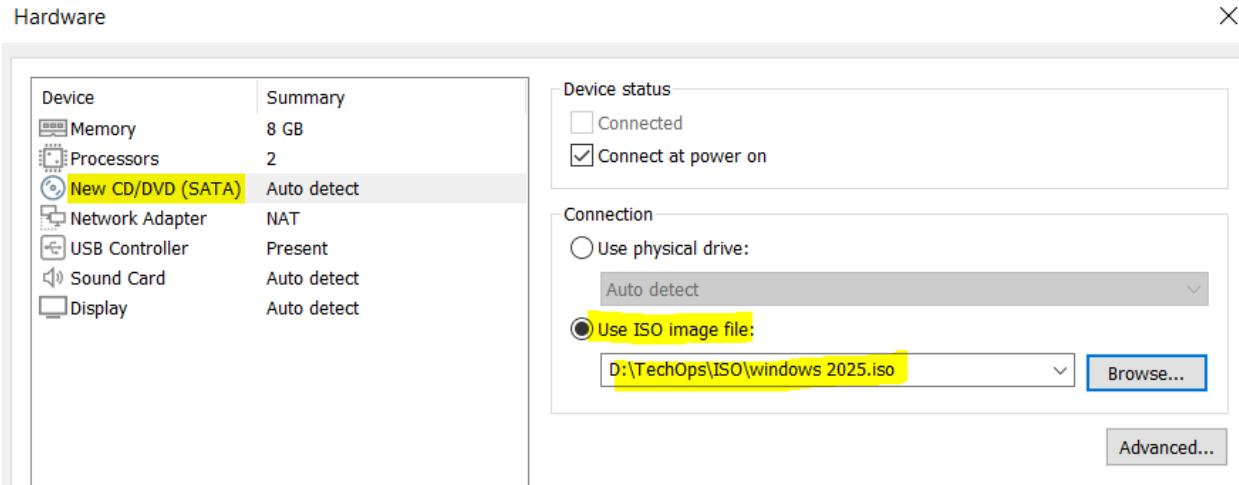
--



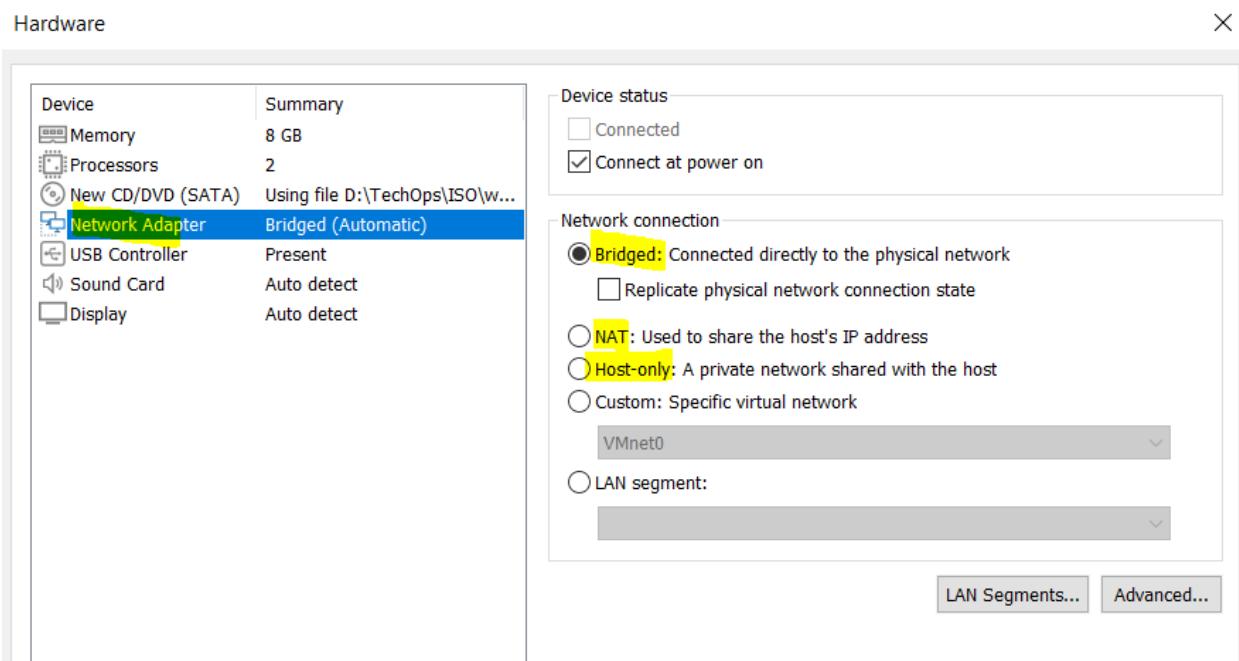
7- بعد کذا هختار customize hardware



8- بعد کدا بحدد ال Config الخاصه بال VM دي زي ال RAM وال CPU وال Network



9- في ال CD/DVD هنا بختار ال iso ال هعمل Boot منها



10 - في ال Network Mode في عندنا 3 Mode

- هنا ال VM هتسحب IP من ال Network الفعليه بتاعتي وال VM هنكون كانها جهاز فعلي معايا في ال Network

- هنا خياد IP لكن NAT فمش هقدر يوصل للوصل لل Network بتاعتي بس هيطلع انترنت عادي

- هنا بيتم انشاء شبكة خاصه بين الجهاز المضيف وال VM فقط ف ال VM مش هطلع انترنت ولا هقدر توصل لل Network بتاعتي لكن تقدر تشووف ال جهاز المضيف واي VM تاني تكون Host-only

New Virtual Machine Wizard

X

Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Windows Server 2025.

The virtual machine will be created with the following settings:

Name: PDC
Location: H:\TechOps\VM\PDC
Version: Workstation 17.5 or later
Operating System: Windows Server 2025

Hard Disk: 1 TB
Memory: 8192 MB
Network Adapter: Bridged (Automatic)
Other Devices: 2 CPU cores, CD/DVD, USB Controller, Sound Card

[Customize Hardware...](#)

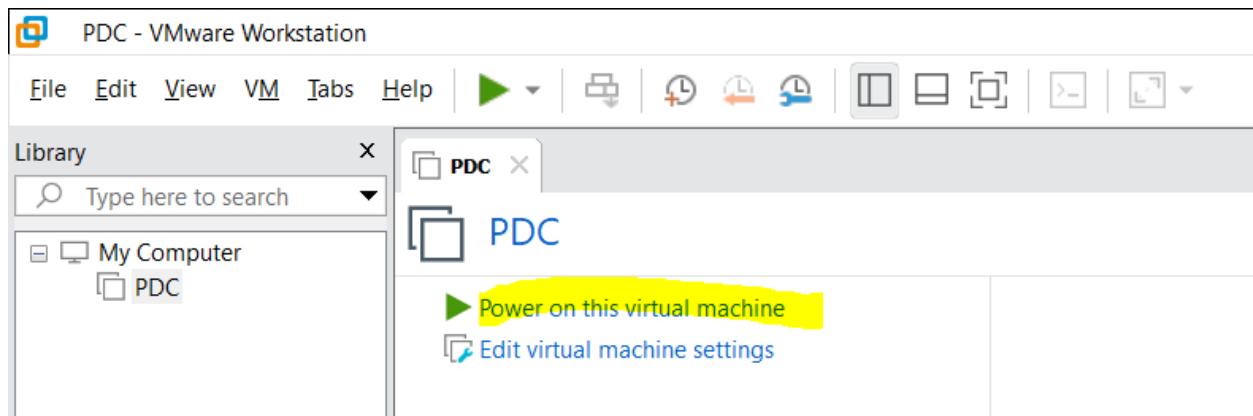
< Back

Finish

Cancel

11 – بعد تعديل ال Config هتضغط Finish

--



12- هنلاقي ال VM ظهرت معاك ف تعمل Power on وتبداً تتبع خطوات ال Install

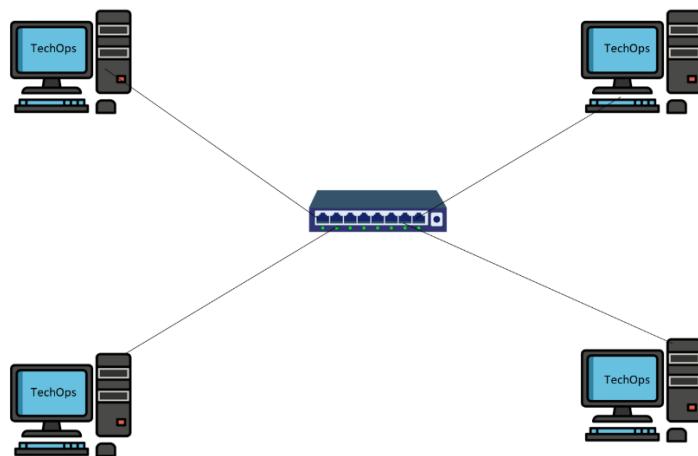
ملحظه (اول ما تشغلي ال VM اضغط بالماوس داخل ال VM واضغط زر المسطره عشان نقدر نعمل boot من ال iso)

Active Directory Installation

الاول خلينا نتكلم عن Model 2 من الاجهزة

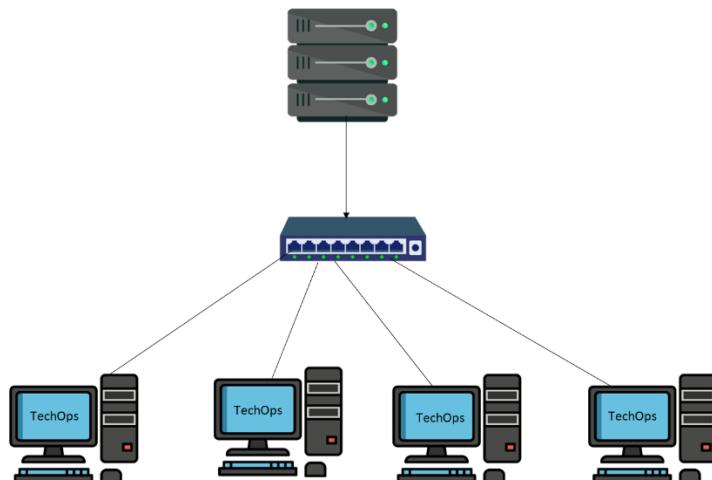
هذا بيكون peer-to-peer : ودا بيكون Workgroup - 1

هنا بيكون كل جهاز مستقل بذاته ، تخزين ال accounts بتكون على نفس الجهاز



هذا بيكون Client-Server : ودا بيكون Domain - 2

هنا يتم التحكم في جميع الاجهزة من خلال ال Active Directory Domain Controller يعني فيه
– يتم تخزين ال accounts مركزيا وبالتالي يمكن للمستخدمين عمل login من اي جهاز داخل ال Network – التحكم في اعدادات الاجهزه والمستخدمين من خلال ال Group Policy



تعال نفرق بين المصطلحات ال Domain Controller وال Active Directory

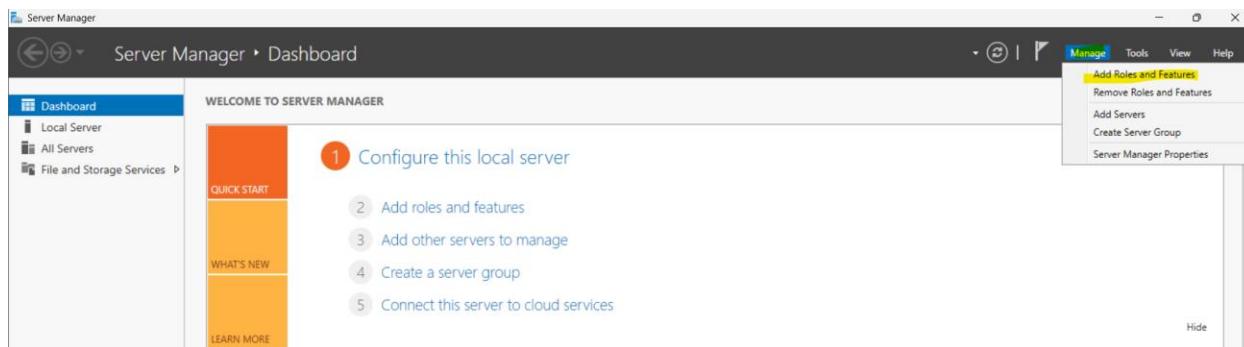
Domain: دا النطاق ال هيكون فيه كل الاجهزه ال هقدر اتحكم فيها

Active Directory: دا الجهاز ال physical ال هيتحكم في الاجهزه

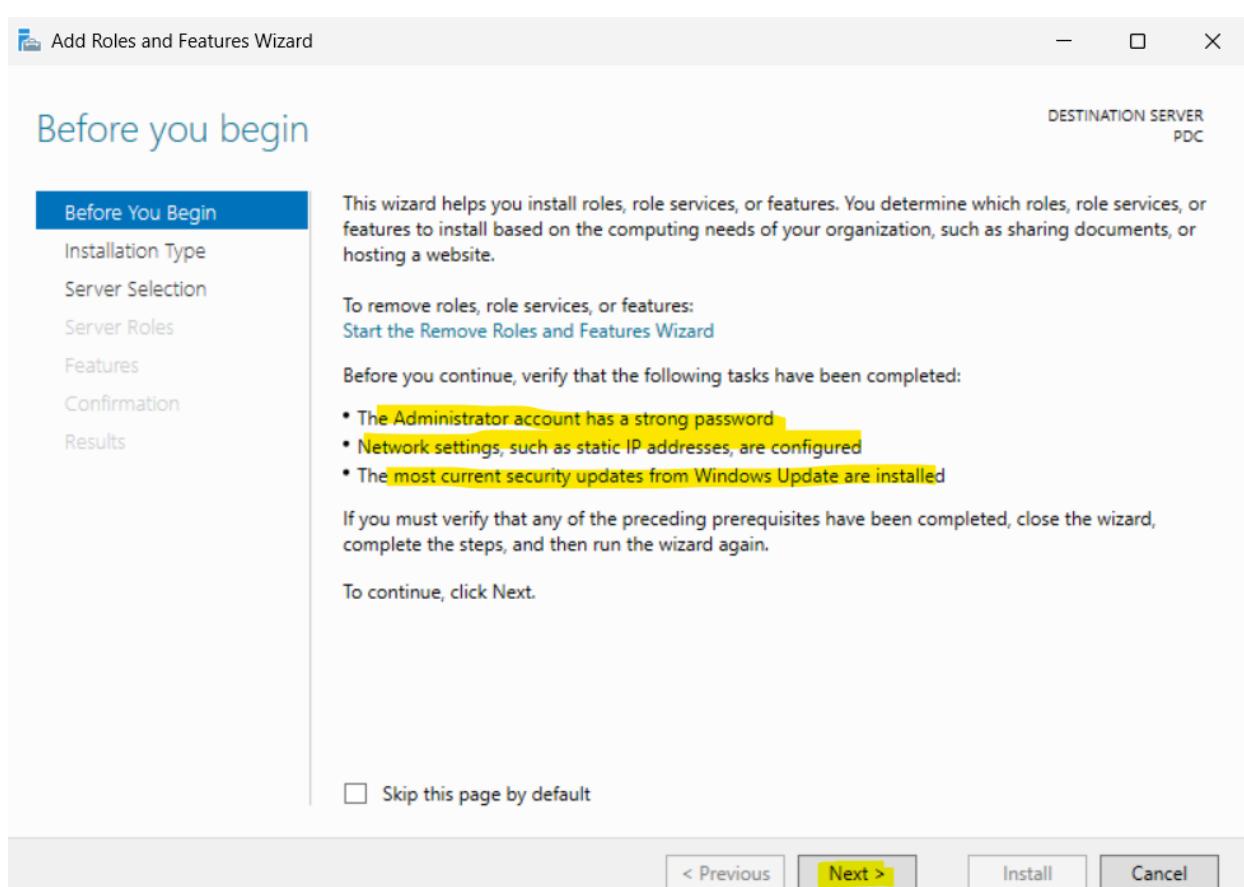
Domain Controller: دي ال service المطلوب انها تنسطب على السيرفر عشان يتحول لل AD

--

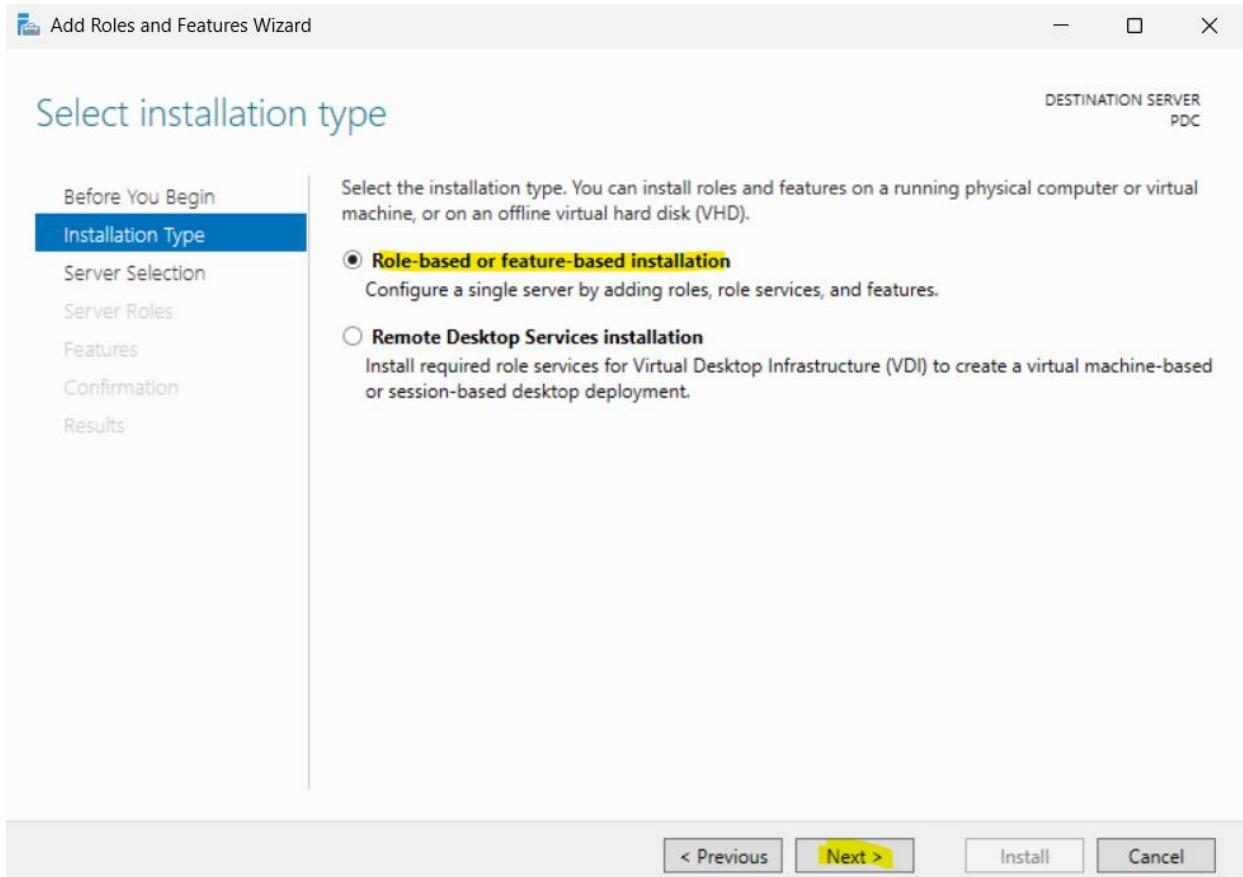
: Install Active Directory Domain Controller



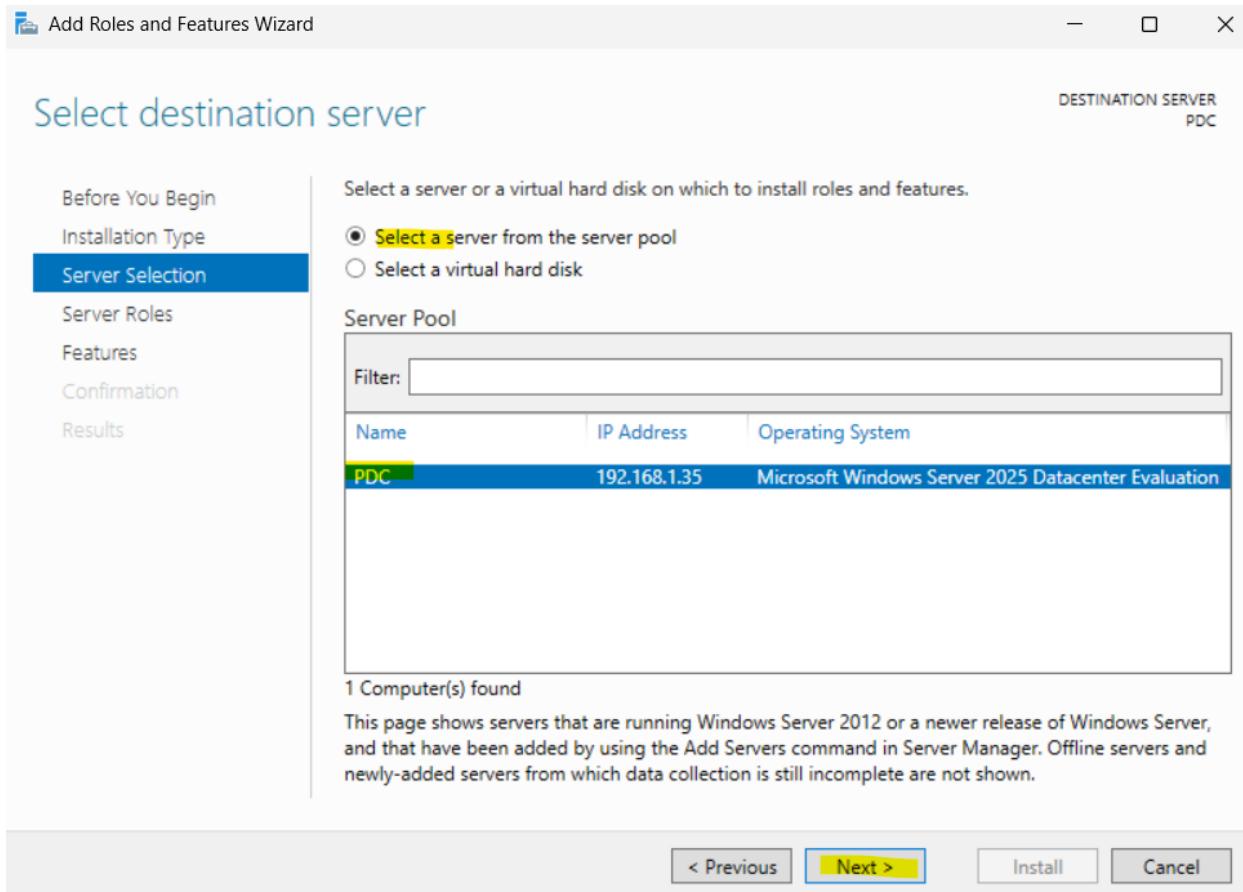
1 – من هنختار Add Roles and Features Manage



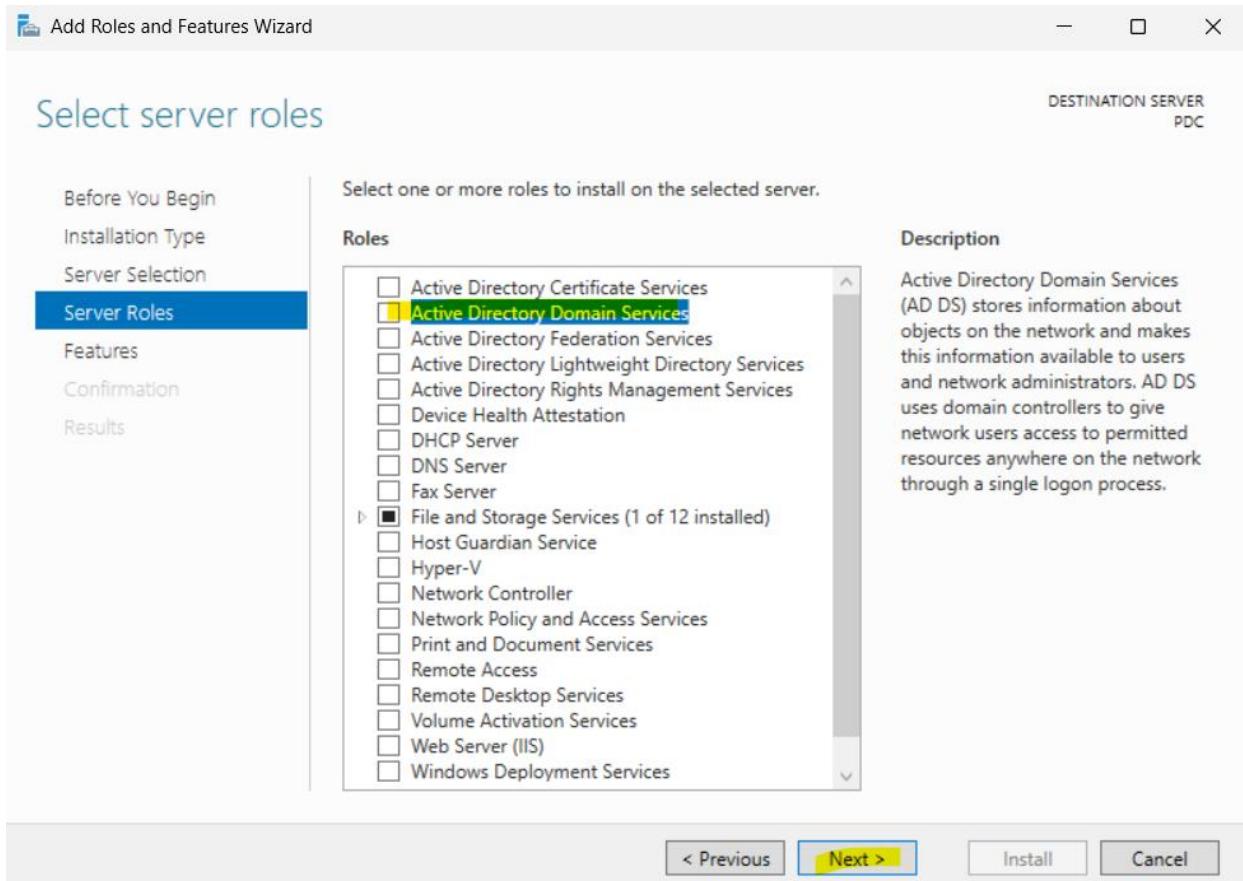
next -2 هو هنا بيقولك على الحاجات الاساسية ال هتعملها قبل م تعمل Add service



3- هنختار **Role-based or feature-based installation**

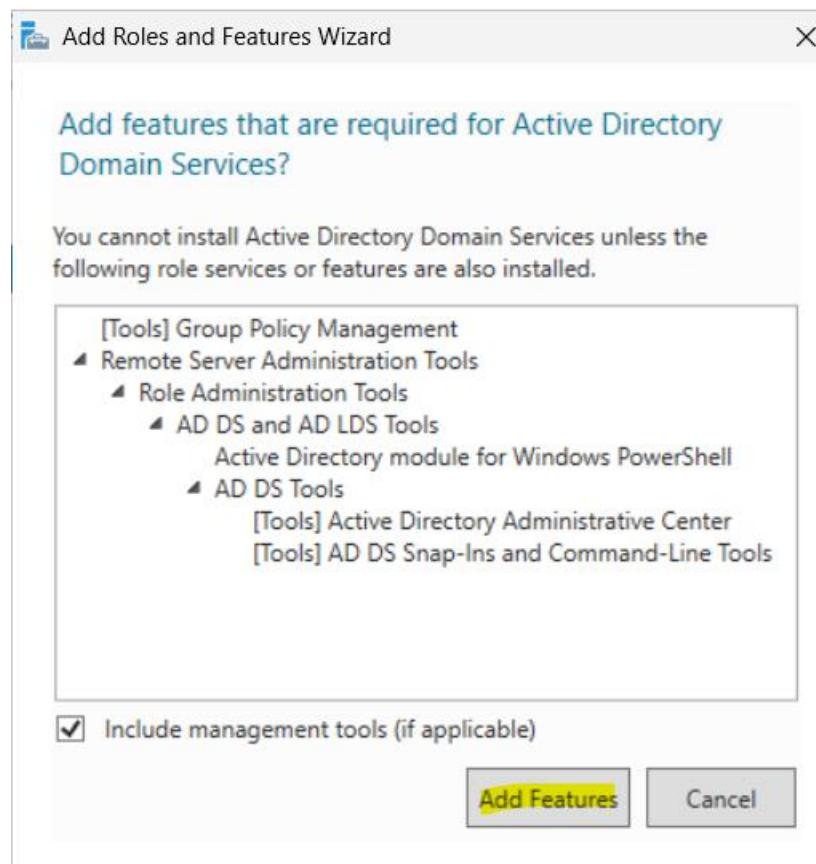


4 – هنختار السيرفر وبعد كدا next



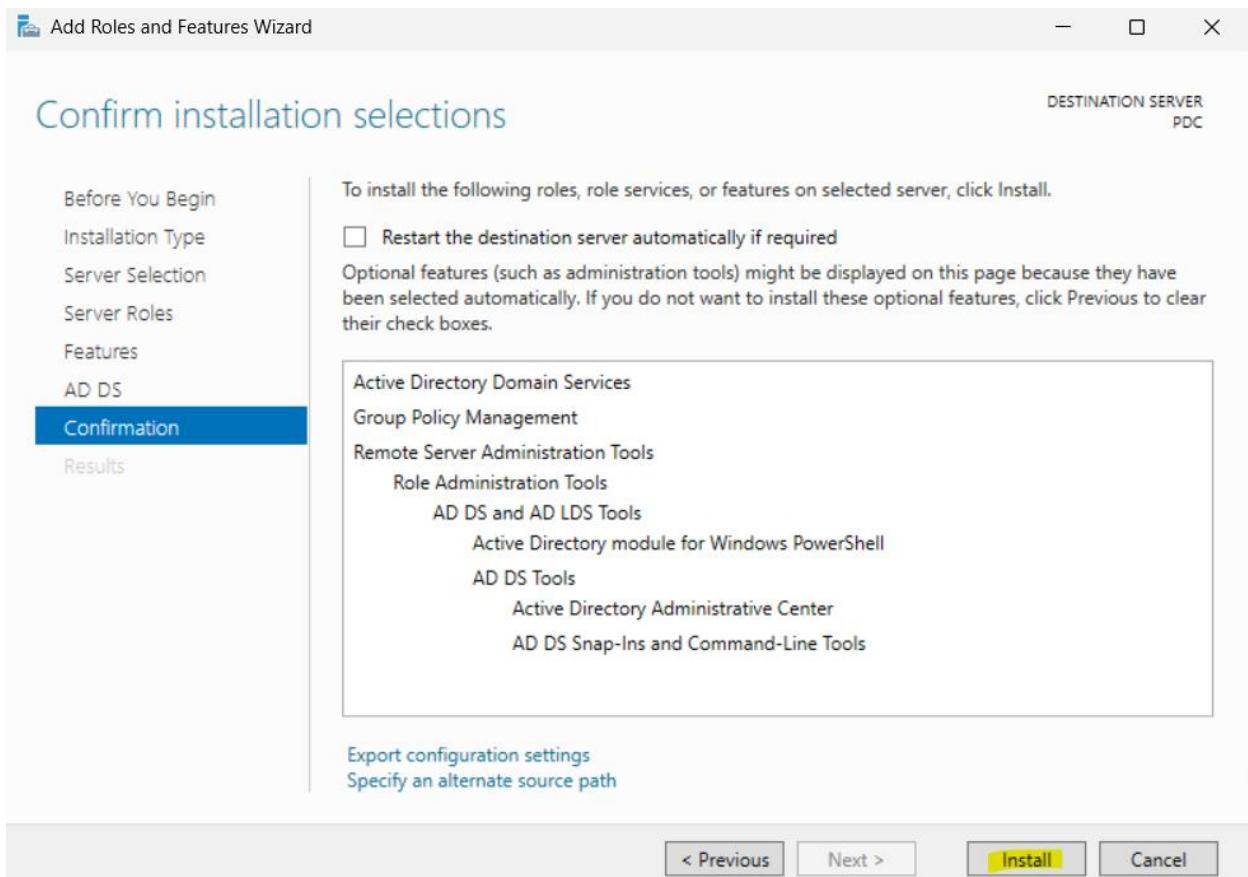
5- هنختار Active Directory Domain Services

--



6- لما نختارها هيطلعنا ال features الاساسيه الازمه لتسطيب ال service فهنضغط على Add Features وبعد كدا تكمل ال next الموجودة لحد ما متوصل لآخر خطوه وهي ال install

--

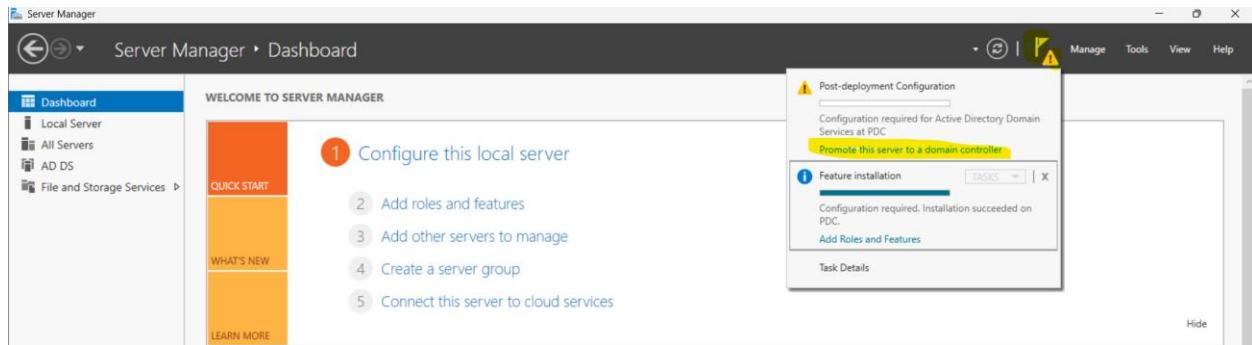


7 - وهذا دي اخر خطوه فهعمل **Install**

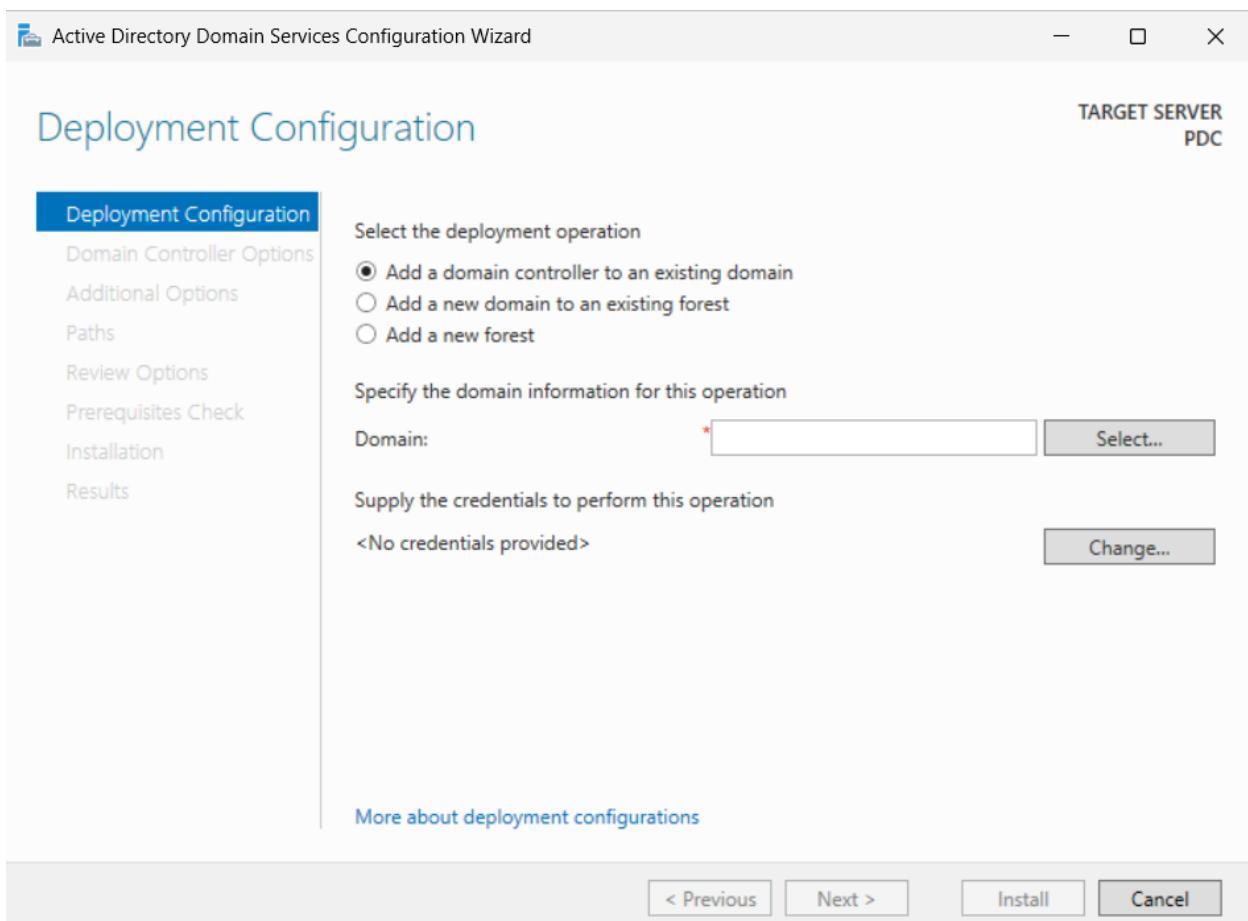
كدا عملنا **Service** install لـ اسمها **Active Directory Domain Services**

الخطوه ال بعد كدا هنحول السيرفر لـ **DC**

Active Directory Domain Services configuration

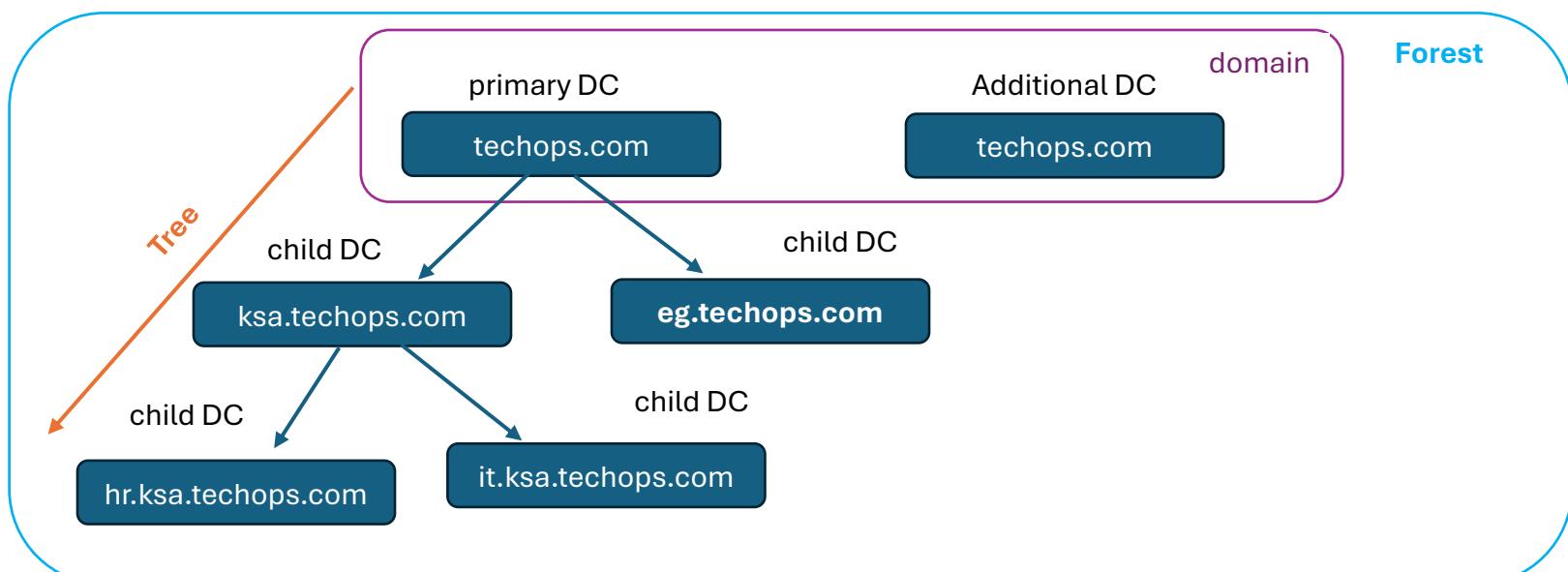


1- من ال هنختار من اى promote this server to a domain controller notification



2- هيطلع عندي ال wizard دا تعال نشرح الفرق بين ال 3 deployment operation

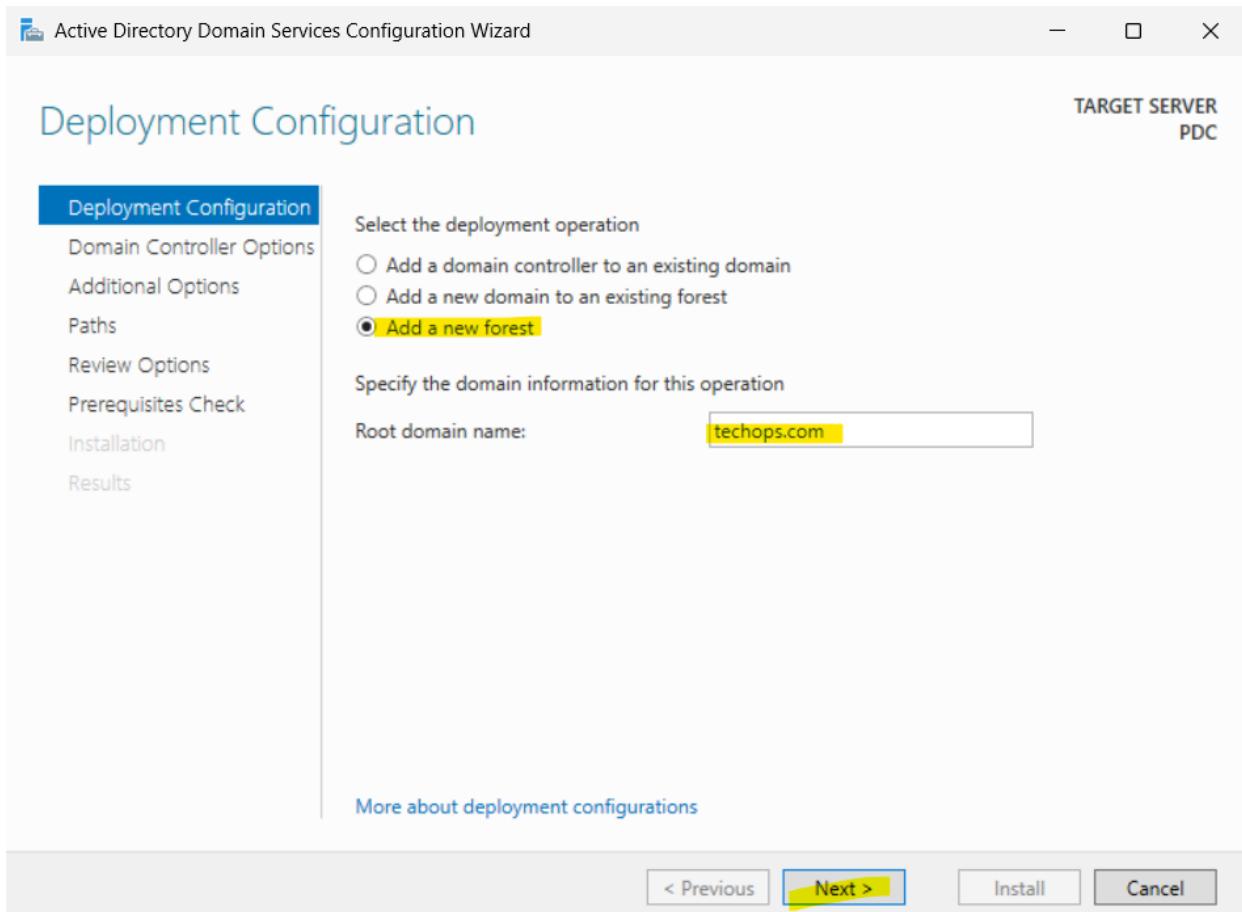
قبل ما نتكلم عن الفرق بينهم تعال نشرحهم ونفهمهم واحده واحده



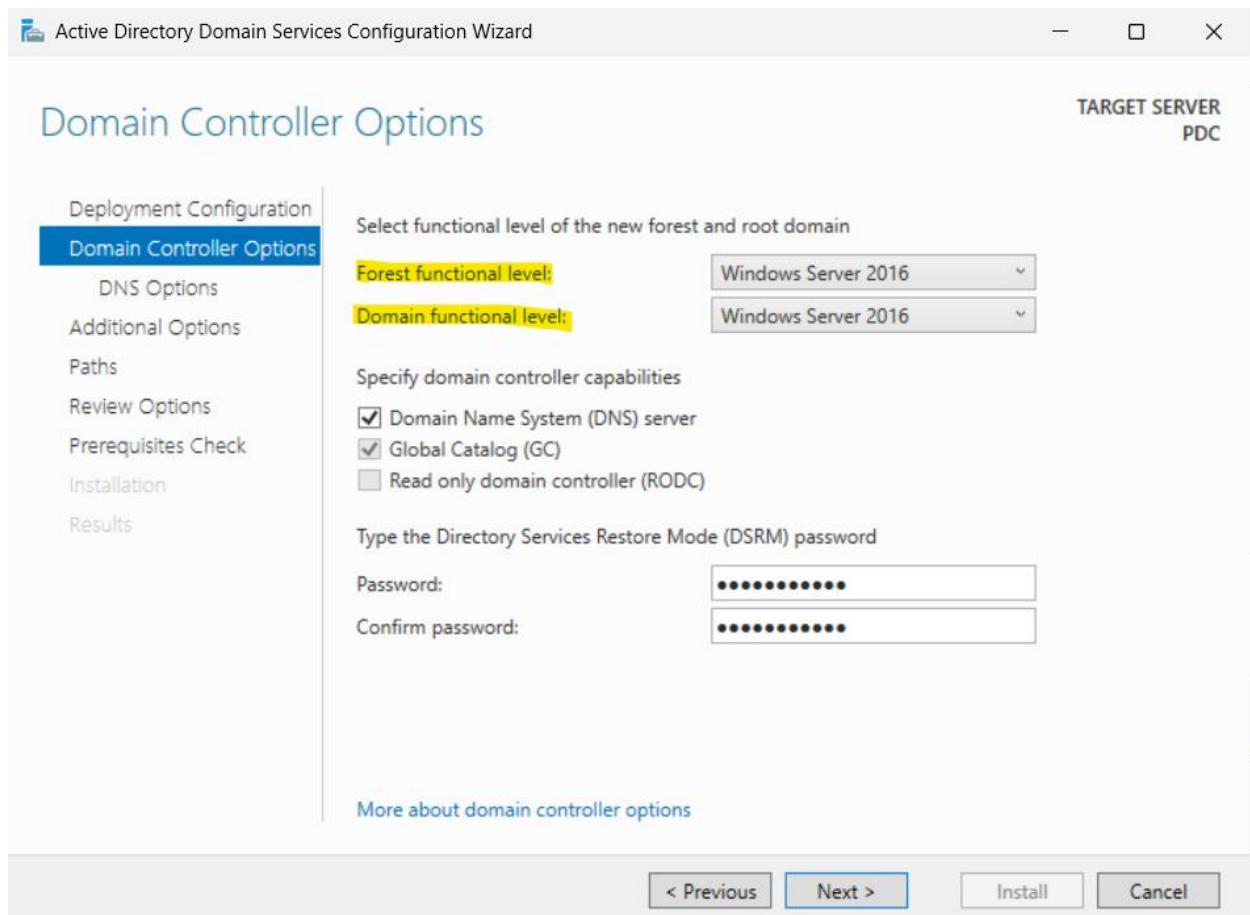
Additional : دا يقصد بيه ال Add a domain controller to an existing domain -

child : دا يقصد بيه ال Add a new domain to an existing forest -

primary : دا يقصد بيه ال Add a new forest -



3- بما اننا لازم بنعمل domain جديد يبقى هنختار Add a new forest واتكتب اسم الدومين بتاعي



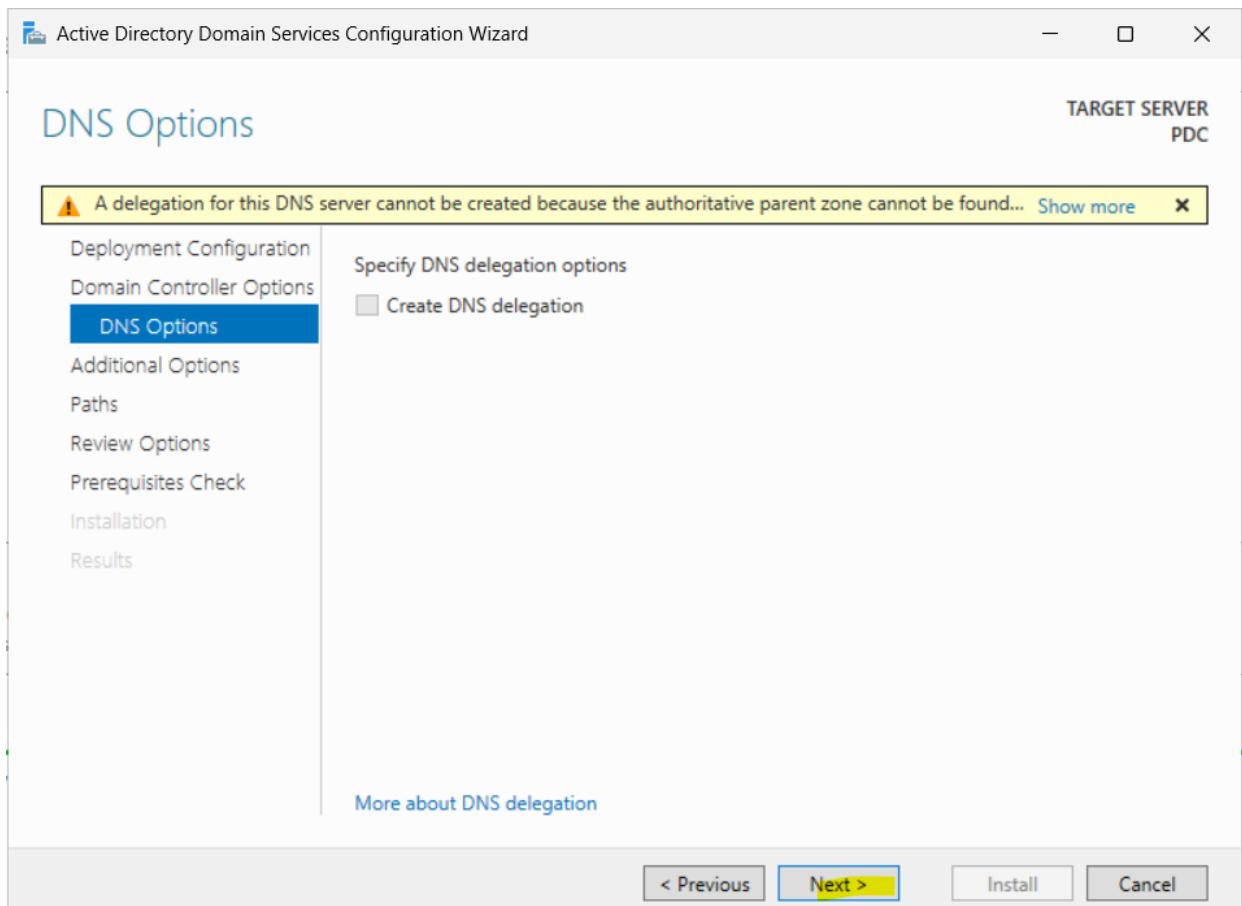
4- بنختار ال domain function level وال forest functional level

دا اقل operating system داخل ال forest ينفع يتحول DC داخل ال forest بتابعی (اقل os هينزل علي ال child)

دا اقل operating system داخل ال forest ينفع يتحول DC داخل ال domain بتابعی (اقل os هينزل علي ال Additional domain)

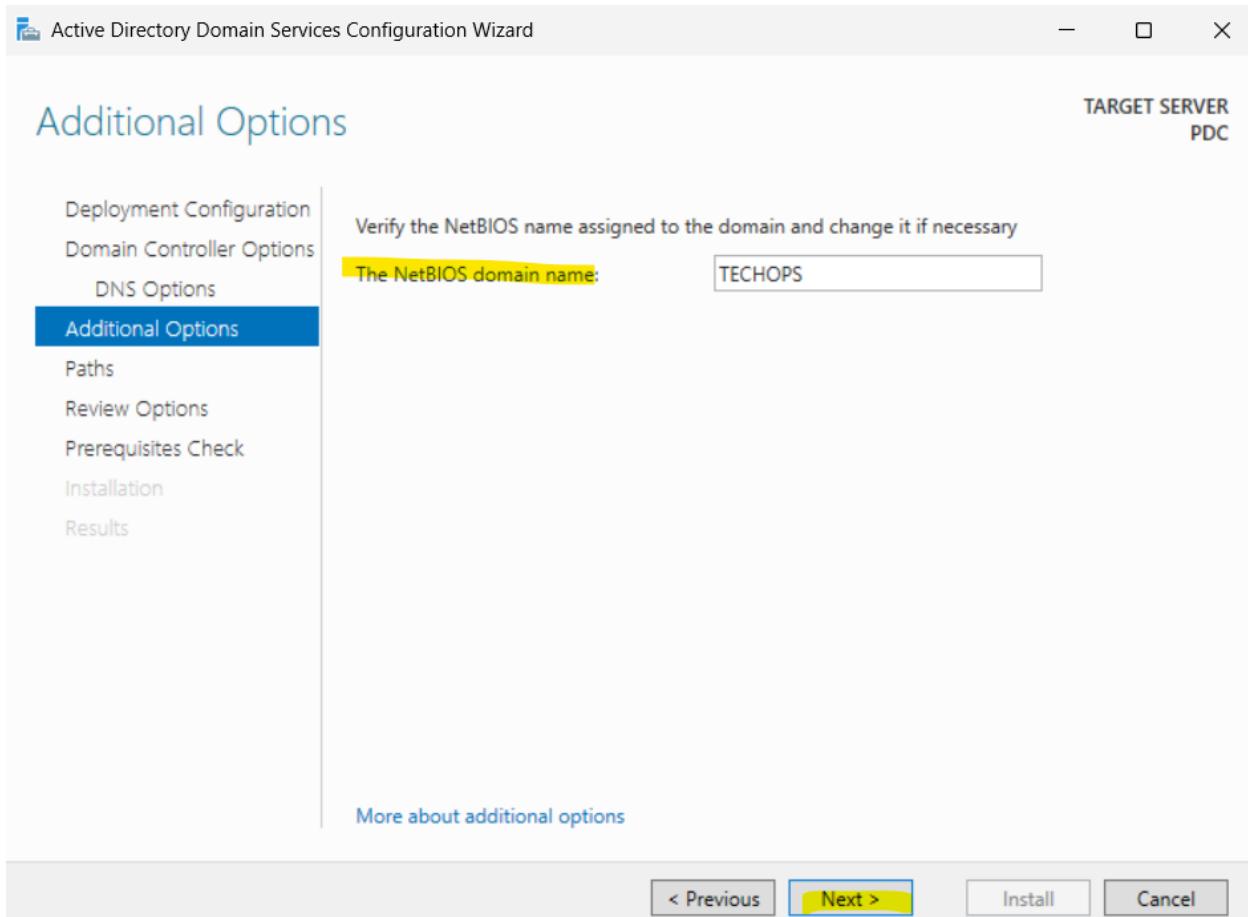
بعد كدا بيقولك انه هيسطب ال DNS ودا لانه اساسي في ال DC والا جهزه بعد كدا هتعمل join من خالله

بعد كدا بيقولك ان السيرفر دا هيكون GC ودا لانه هو اول domain عندي

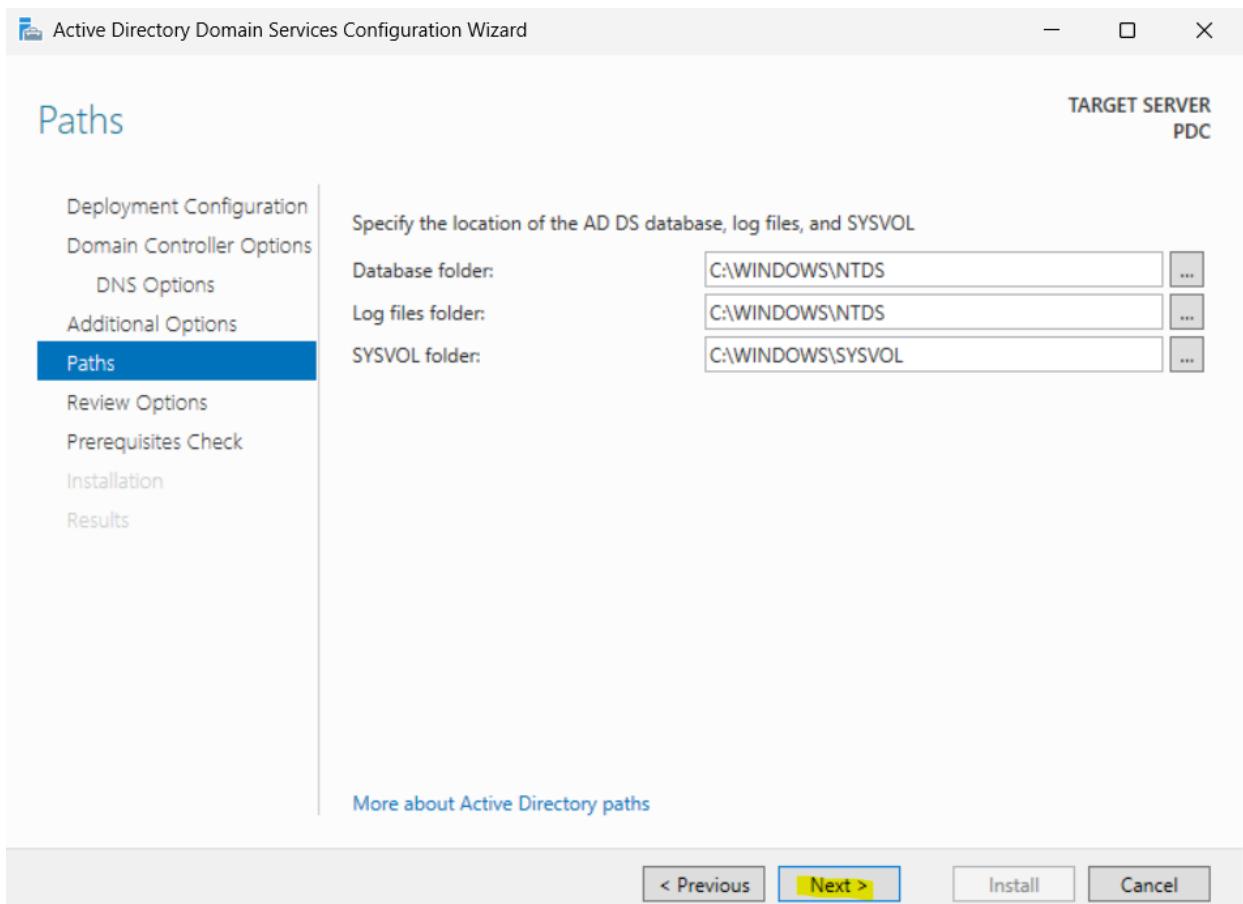


next -5

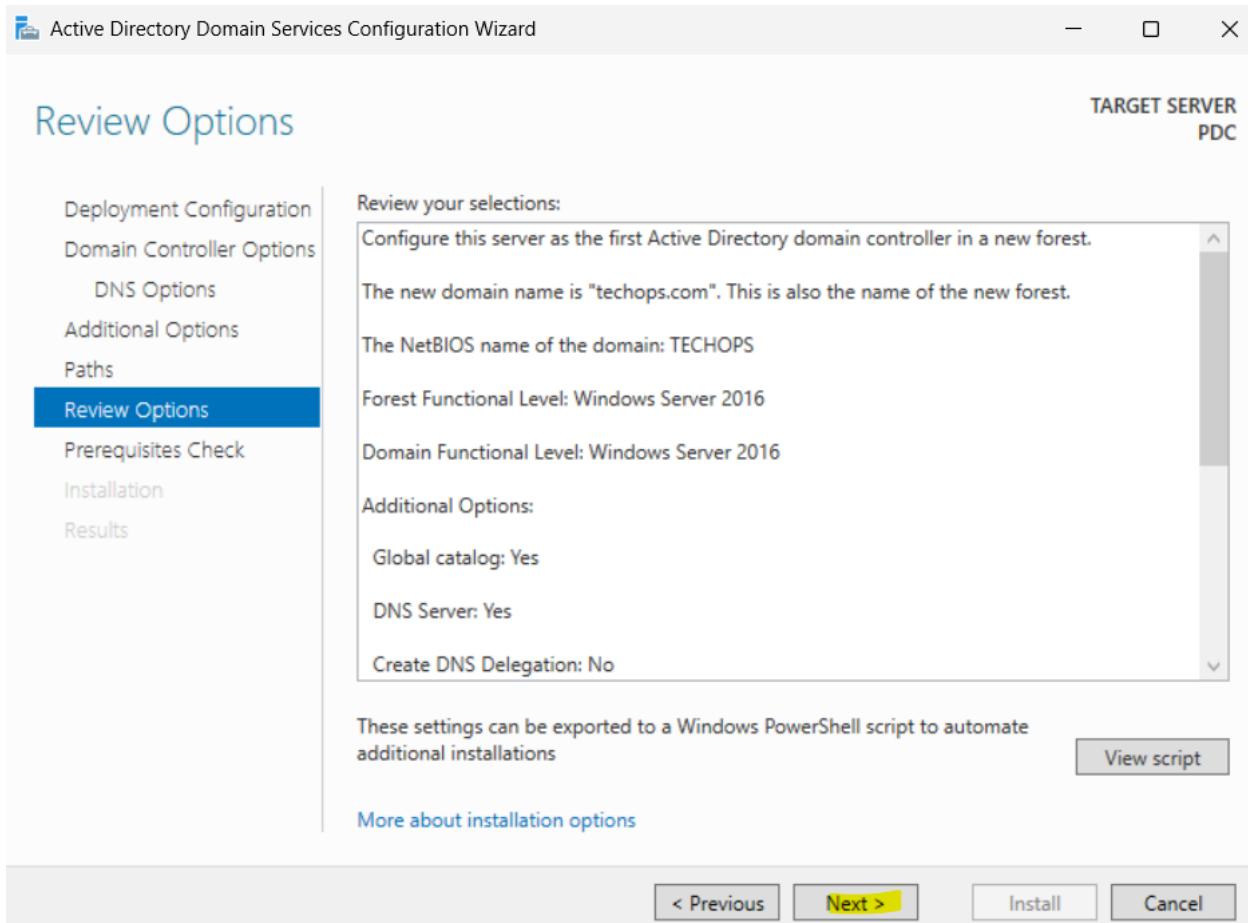
--



6- Next : هو هنا بيقولك ال NetBIOS name هيكون اي join اي لازمه ال net bios name ؟ دا عشان لو عندك اجهزه قديمه في ال network و هتعملها netbois فهيكون من خلال ال domain



next -7 : هنا بيوضلك ال paths الخاصه بال db و logfile و sysvol



next -8

Active Directory Domain Services Configuration Wizard

Prerequisites Check

TARGET SERVER
PDC

All prerequisite checks passed successfully. Click 'Install' to begin installation.

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

Rerun prerequisites check

View results

This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "techops.com". Otherwise, no action is required.

If you click Install, the server automatically reboots at the end of the promotion operation.

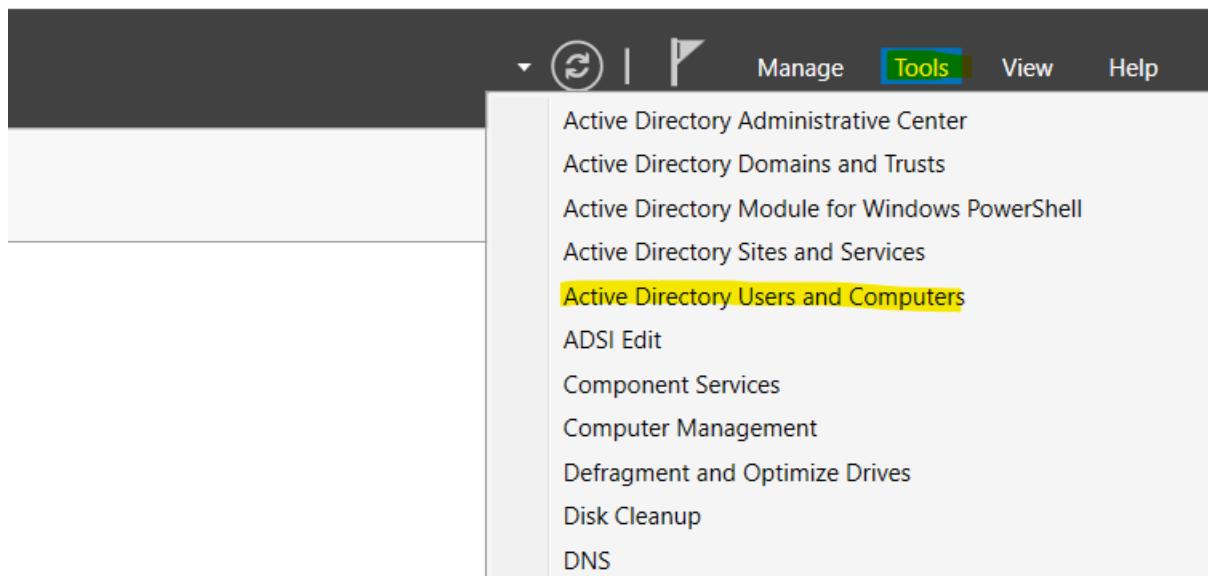
More about prerequisites

< Previous Next > **Install** Cancel

install -9

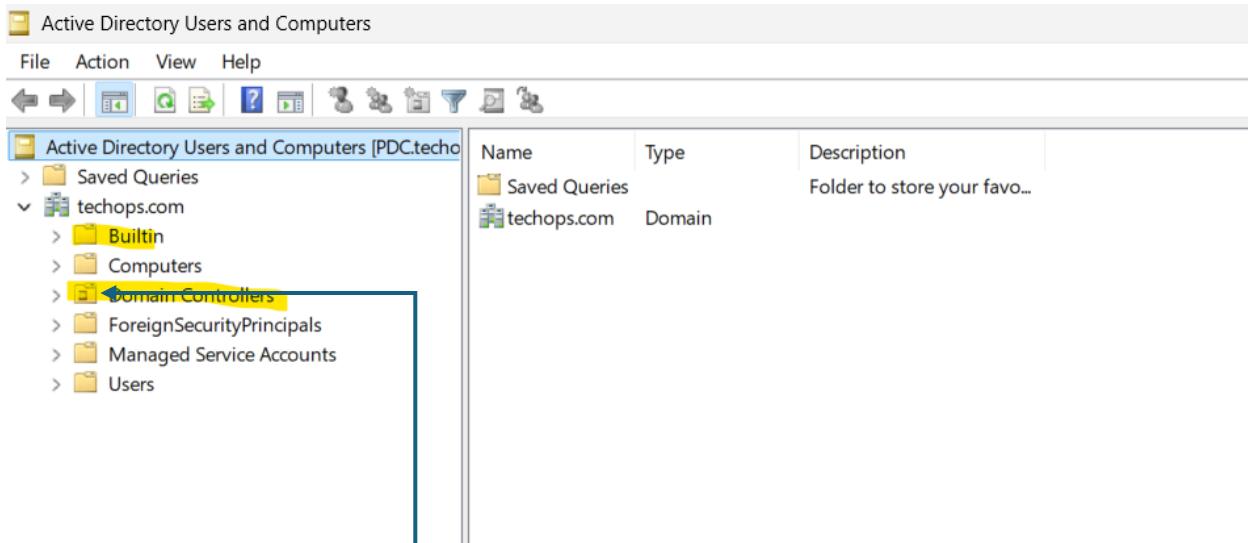
Join Domain

قبل ما نعمل join نشوف كل ما يخص ال users and group



عشان نفتح ال AD Users and Computers الخاص بال users من Tools هنختار Console

--



هلاقی فتح معانا بالشكل دا ، وعاوزك تفرق بين حاجاتين هنا ال organization Unit(OU) وال Container

OU مميز ان بيكون فيه علامه ع المربع الاصفر

ودا يستخدمه لك عمليه تنظيميه داخل ال AD

بقدر اطبق من خلال Group policy او Permissions على OU معينه او تطبيق
ال ال AD داخل ال AD ، لا يمكن تطبيق ال GP عليه بشكل مباشر
بتحتوي على Objects مثل ال user وال computer لكنه لا يوفر نفس التنظيم والاداره التي توفرها
ال OU

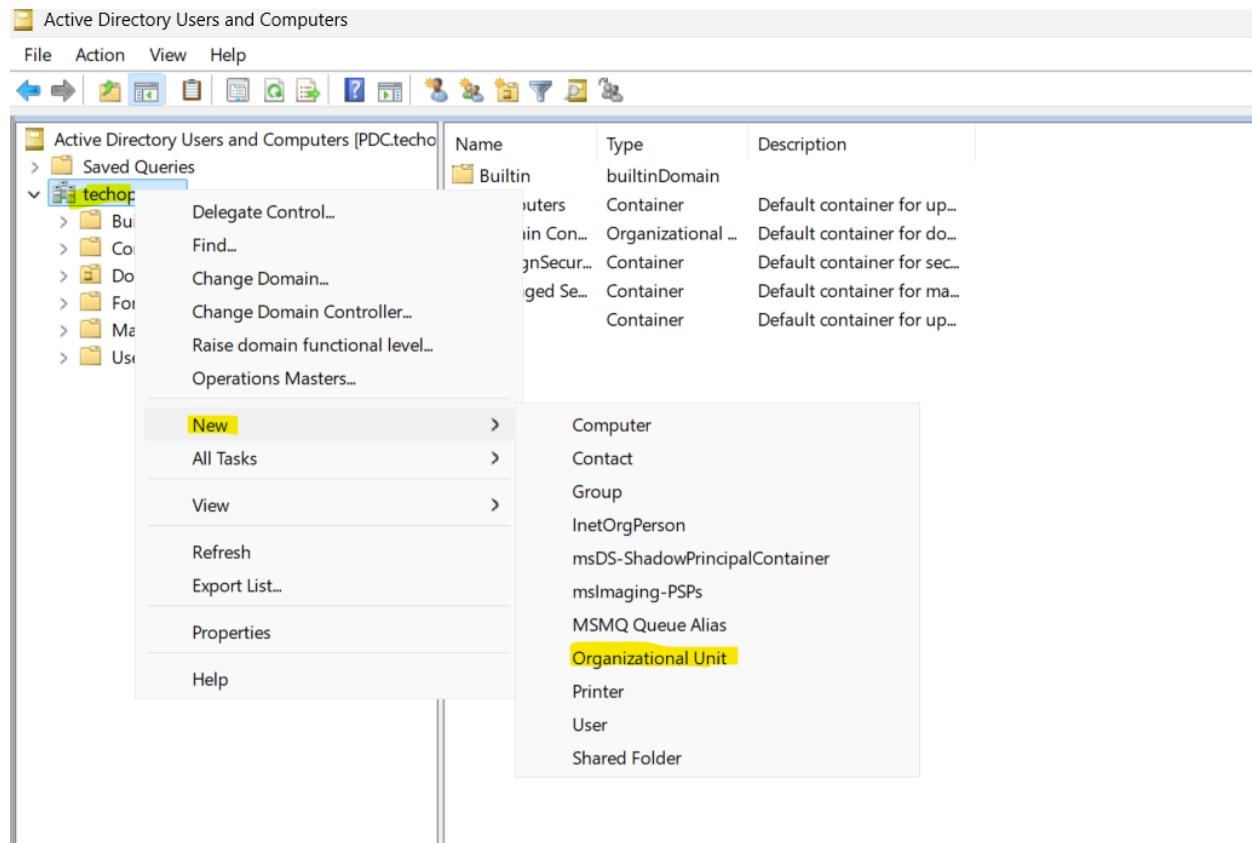
بعض الـ Containers الافتراضية في Active Directory

Users: يحتوي على حسابات المستخدمين الافتراضية.

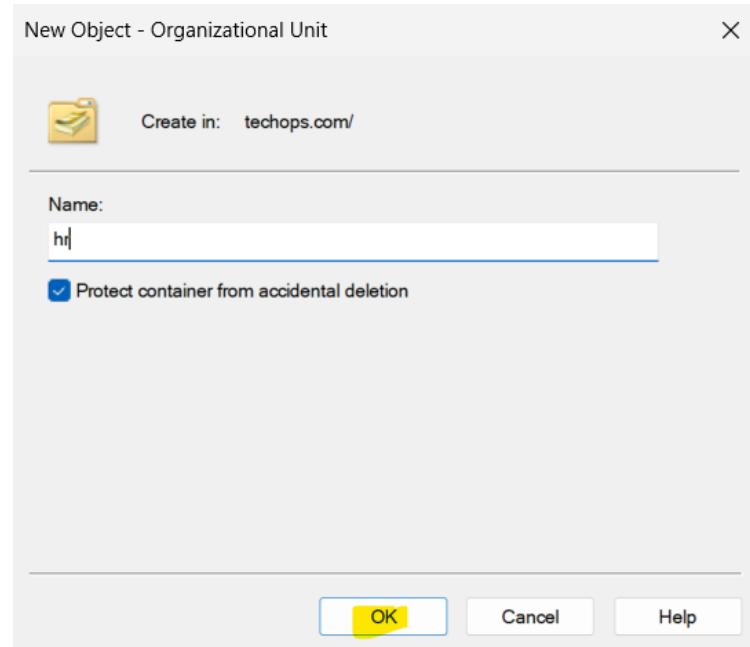
Computers: يحتوي على الأجهزة التي يتم ضمها (Joined) إلى الدومين.

Builtin: يحتوي على المجموعات الأمنية المدمجة (مثل Administrators و Users).

طیب از ای نعمل ل OU ؟



Click على اسم ال Domain New هنختار من و من



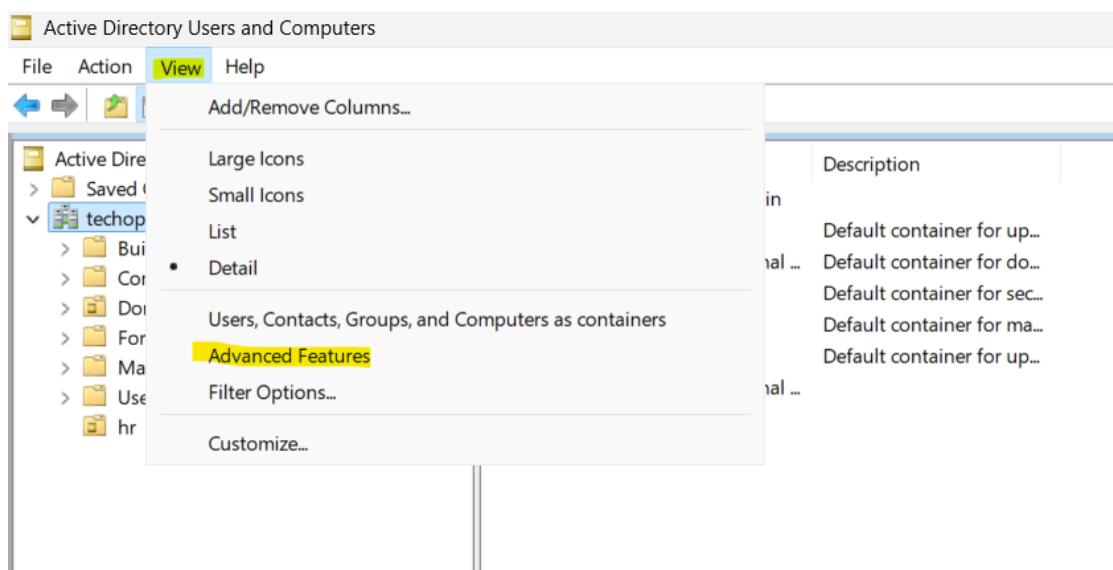
بعد كدا بكتب اسم ال OU ال عاوزه واضغط OK

--

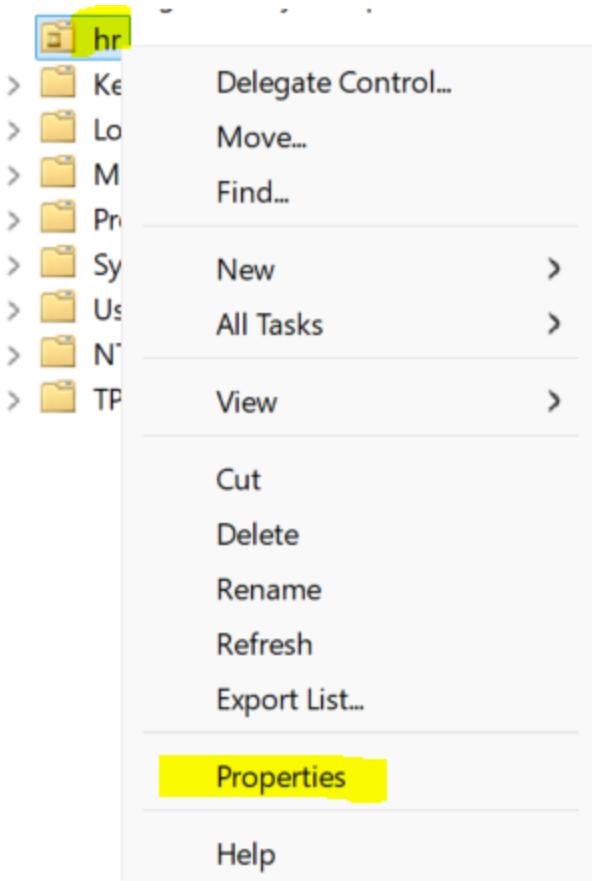
طيب ازاي احذف ال OU ؟

وانا بعمل create كان في جمله Protect container from accidental deletion كنت عامل عليها check الجمله دي معناهااني بحمي ال OU دا من الحذف ال غير المقصود طيب لو عاوز احذفها

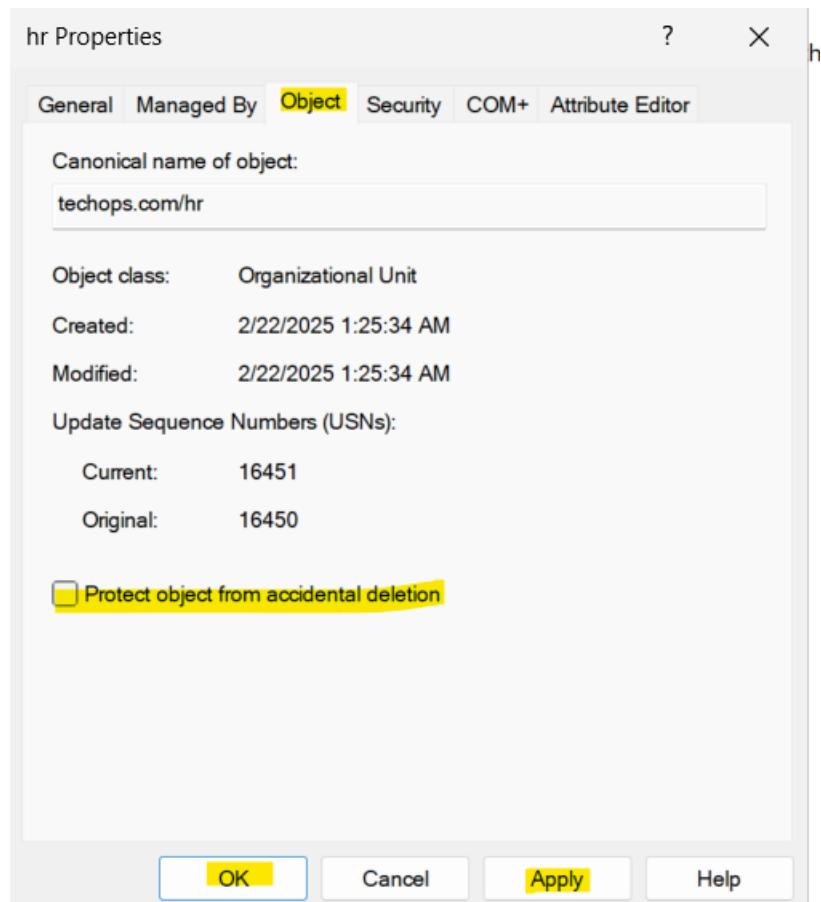
؟



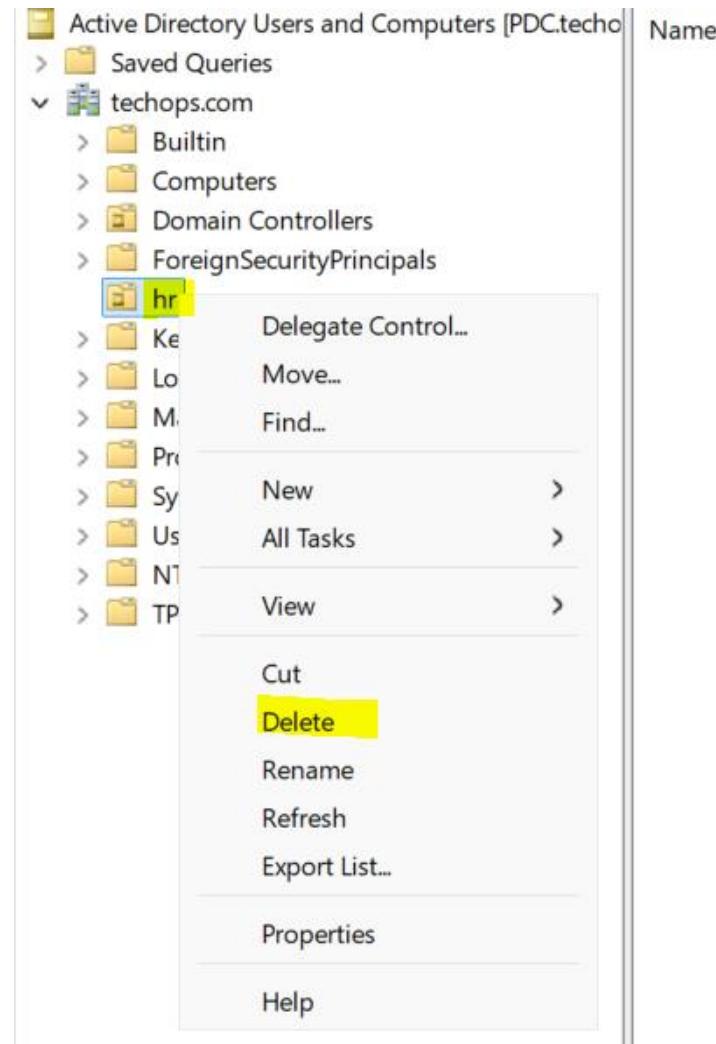
من View هنظهر ال advanced features



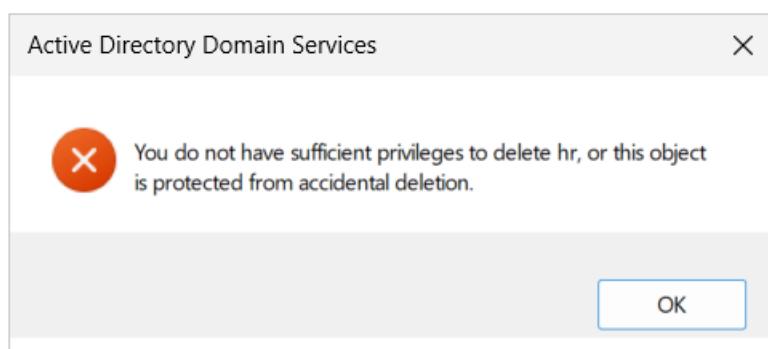
ومن ال OU ال عاوز احذفها هختار ال properties بتاعتها



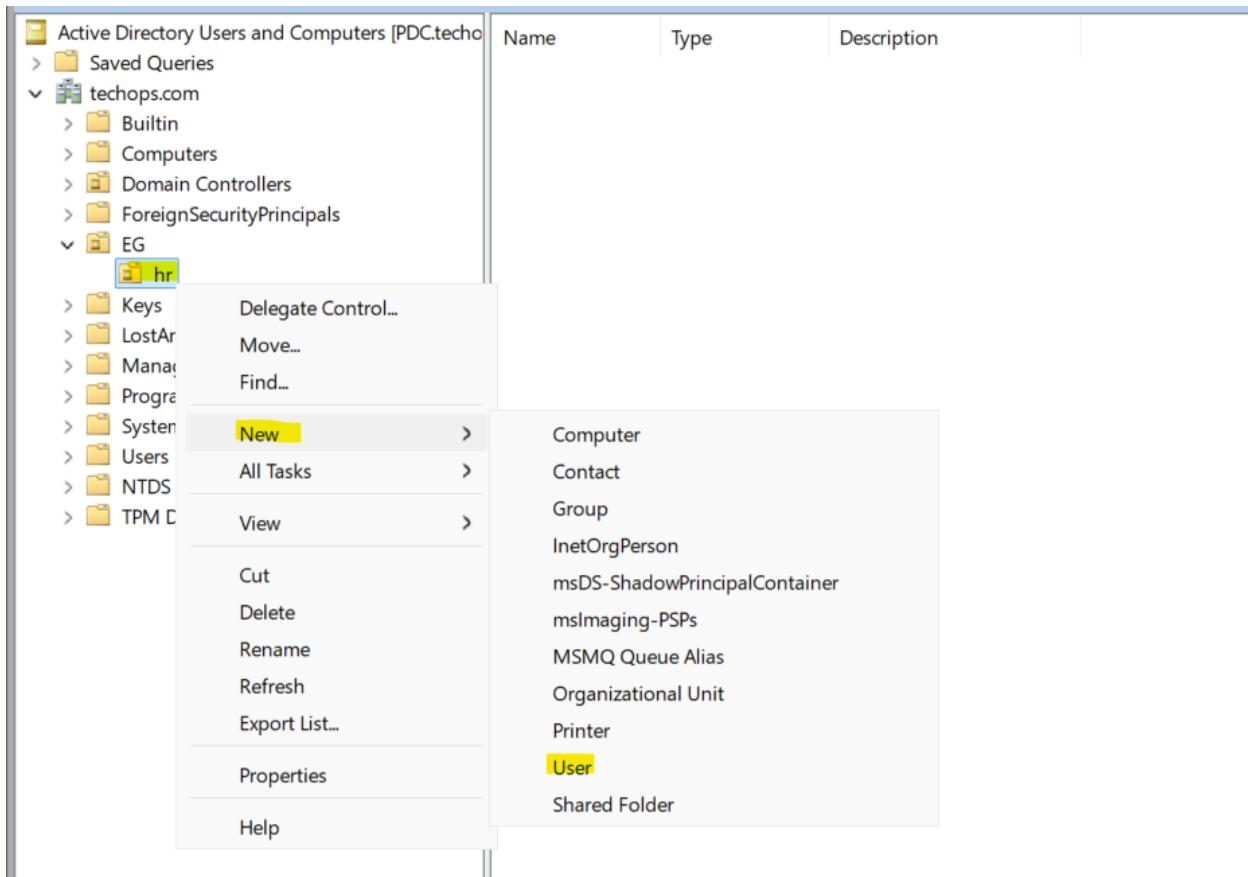
هناقي في حاجه اسمها object لو فتحنها هناقي فيها نفس الخيار الخاص بالحذف هنشيل من عليه ال
apply ونعمل check



بعد كدا هنروح على ال OU ونضغط delete فهتتحذف معانا
لو معملناش الخطوات دي وعملنا delete عطول بيطعلنا ال error دا :



طيب سريعا تعال نشوف بنعمل create لـ user ازاي :



من ال OU هختار new ومنها اختار user

--

New Object - User

X



Create in: techops.com/EG/hr

First name:

mostafa

Initials:

Last name:

mahmoud

Full name:

mostafa mAhmoud

User logon name:

mostafa

@techops.com

User logon name (pre-Windows 2000):

TECHOPS\

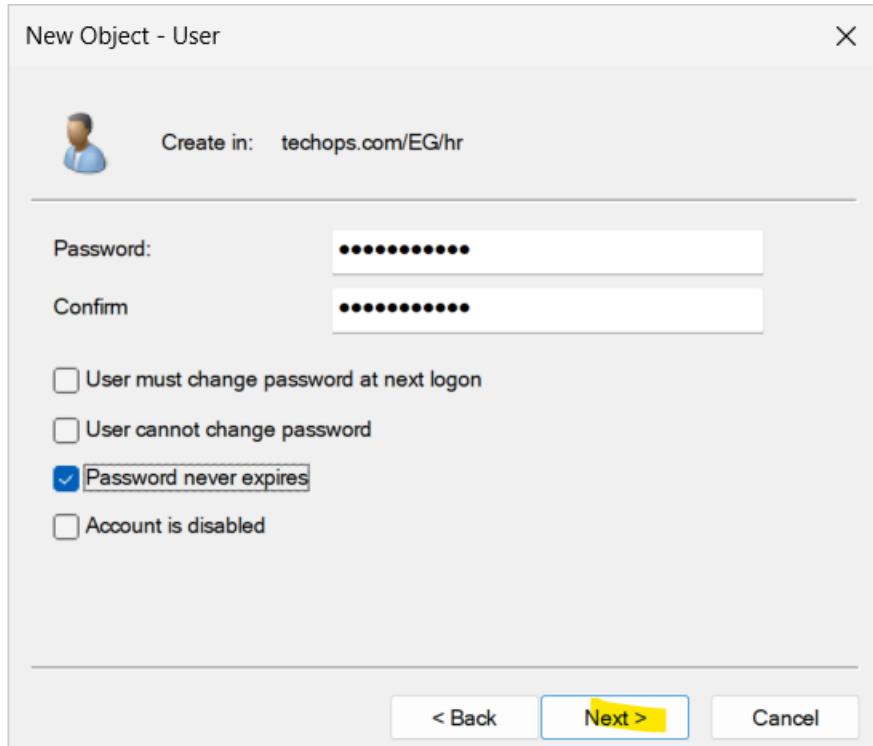
mostafa

< Back

Next >

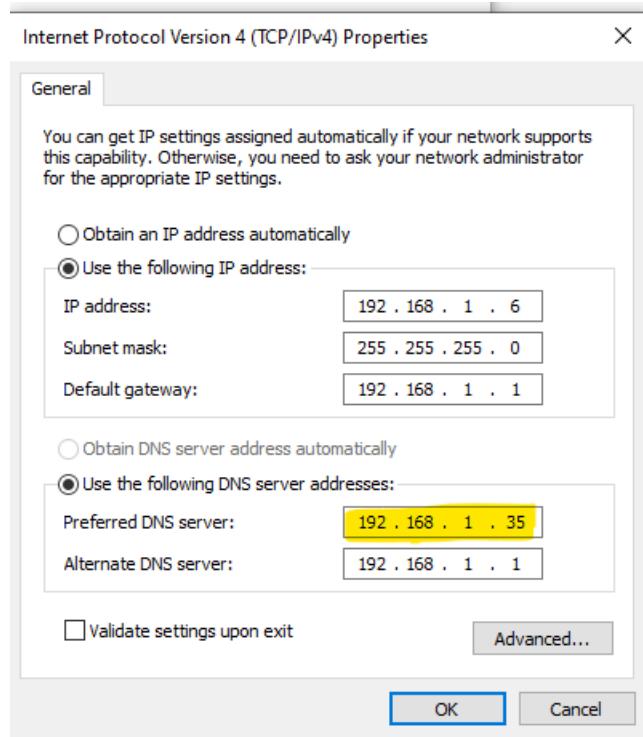
Cancel

بكتب اسم ال user وال logon name واضغط next

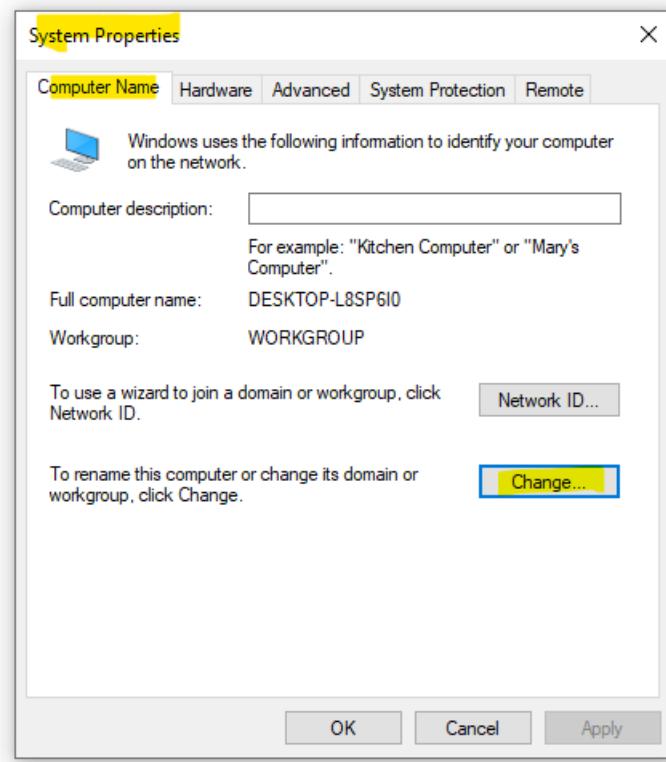


بعد كدا بكتب ال password ، وتعال نفهم كل جمله من دول
password : هنا بجبر ال user انه يغير ال User must change password at next logon
بتاعته بعد اول logon
password : عكس الاولى وهي ان ال user مقدر يغير ال User cannot change password
password : مش هيكون فيه وقت محدد للتغيير ال Password never expires
عادي
account disable : هنا بعمل disable لـ user دا ولو عملت ال Account is disabled
هيقدر يعمل logon

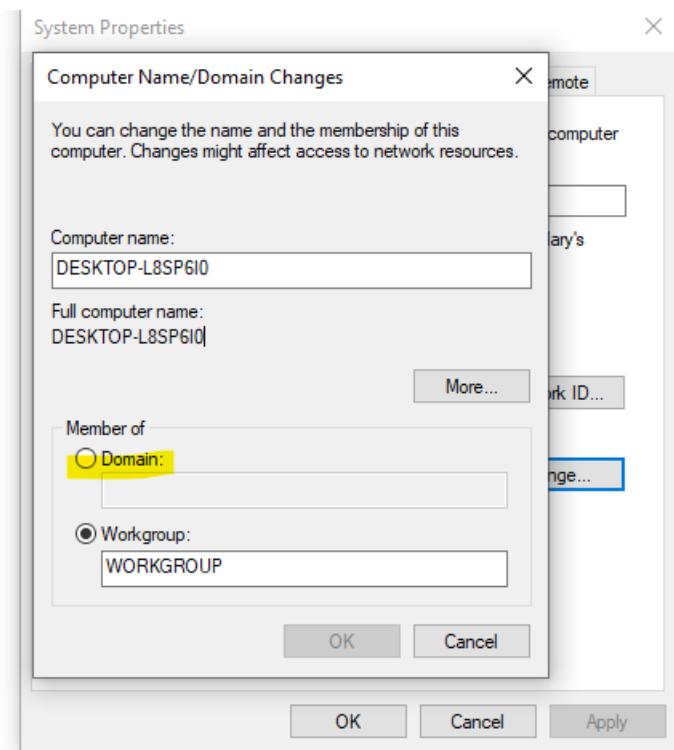
طیب از ای بقا اعمل join لل domain ؟



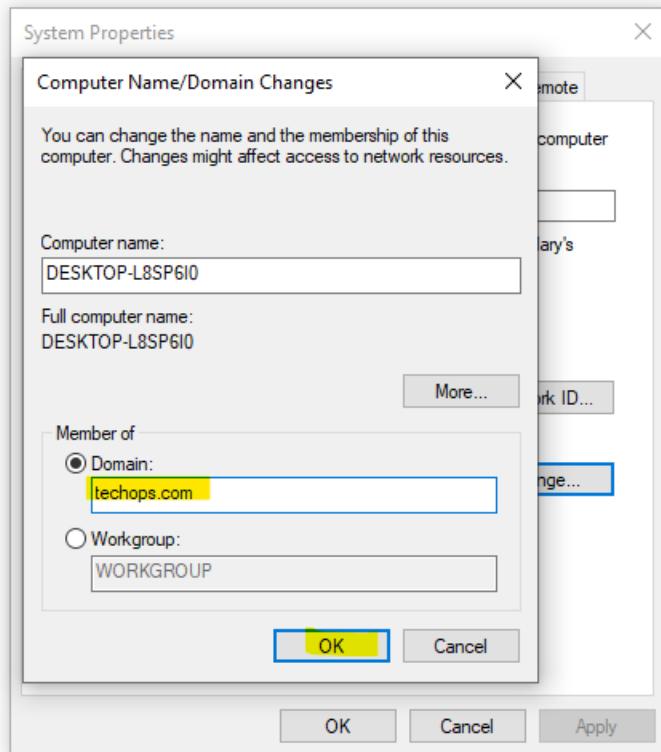
اول حاجه بظبط ال DNS لازم يكون ال IP الخاص بال domain في ال Client عند ال ف انا عندي ال IP بتاع ال domain 192.168.1.35 بتاع ال client ضفته في ال dns



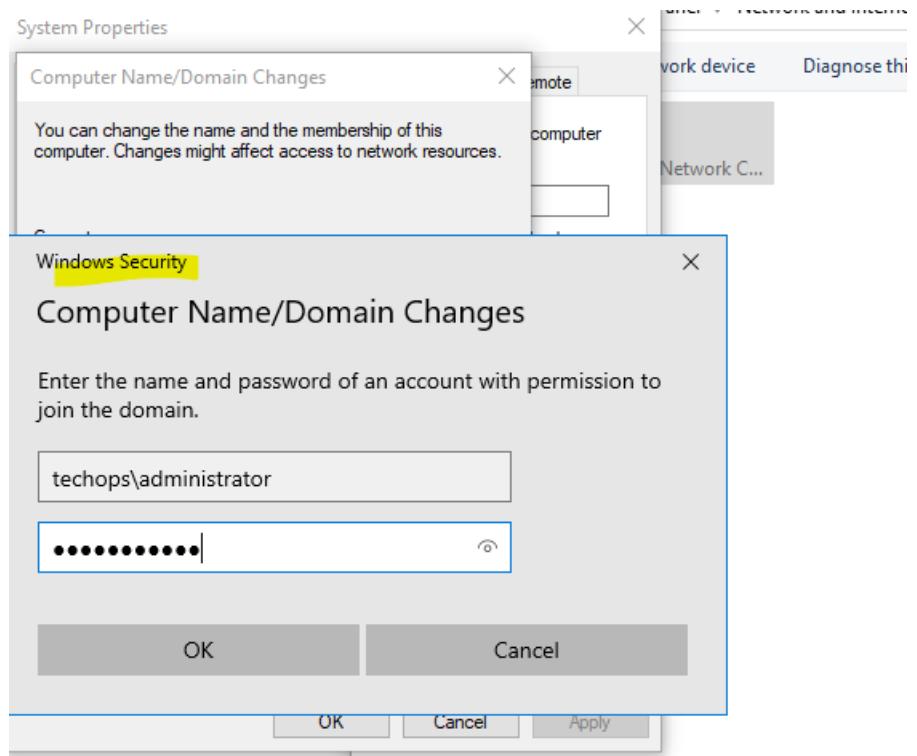
بعد كدا هفتح ال system properties و هروح على ال computer name واضغط change



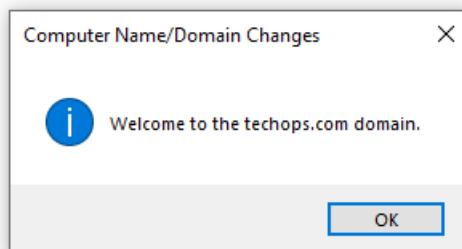
هذا بدل ما هو member of Domain هنختاره workgroup



هناكتب اسم ال domain بتاعنا



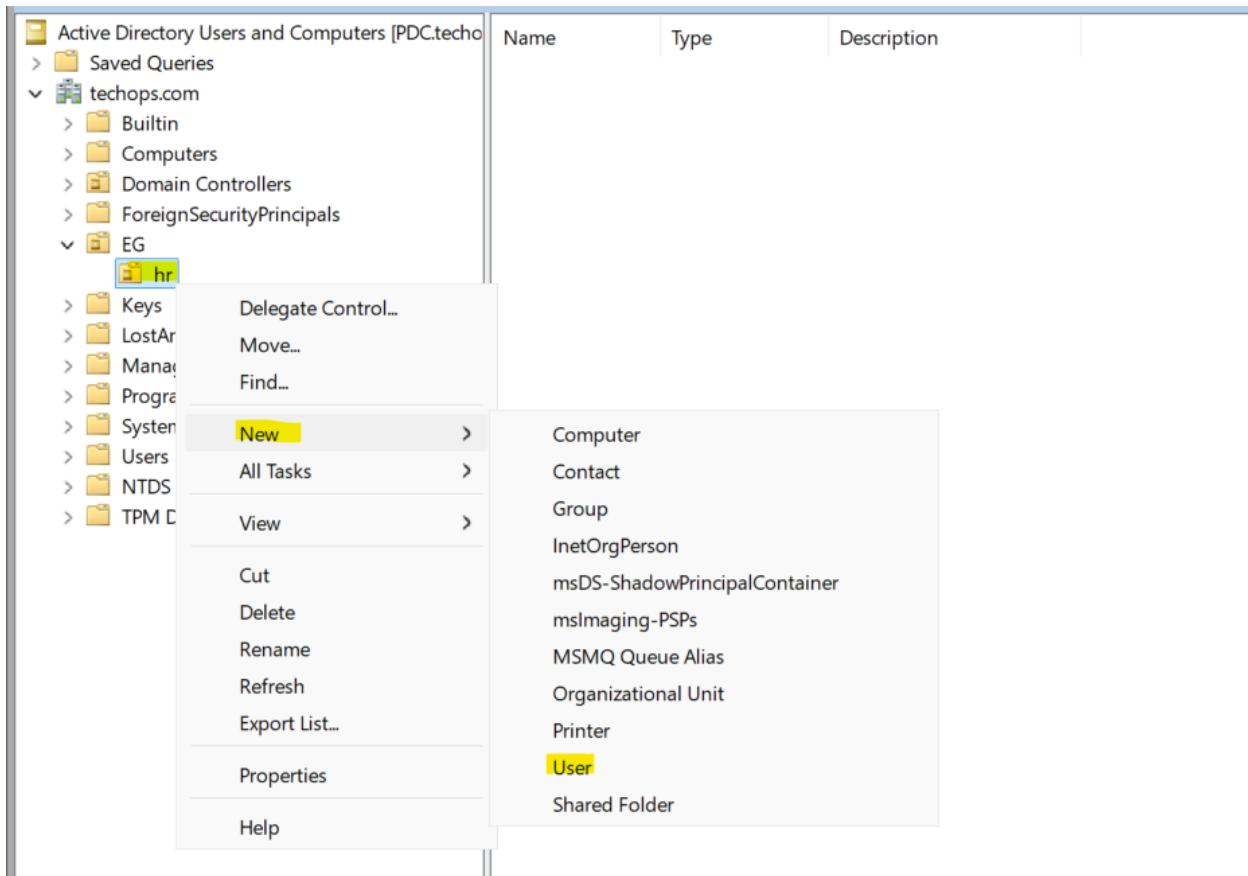
هیطلب مني ال user وال password ال هعمل بيهم join لل domain وفالغالب بيكون ال user ال
لكن user العادي يقدر يعمل join by default لحد 10 اجهزه فقط



بعد م اكتب ال user وال password واضغط ok هيت عمل join للجهاز دا داخل ال domain بعد
كدا لازم اعمل restart

Create Users

ازاي نعمل User لـ create



من ال OU هختار new ومنها اختار user

--

New Object - User

X



Create in: techops.com/EG/hr

First name:

mostafa

Initials:

Last name:

mahmoud

Full name:

mostafa mAhmoud

User logon name:

mostafa

@techops.com

User logon name (pre-Windows 2000):

TECHOPS\

mostafa

< Back

Next >

Cancel

بكتب اسم ال user وال logon name واضغط next

New Object - User X

Create in: techops.com/EG/hr

Password: ······

Confirm ······

User must change password at next logon

User cannot change password

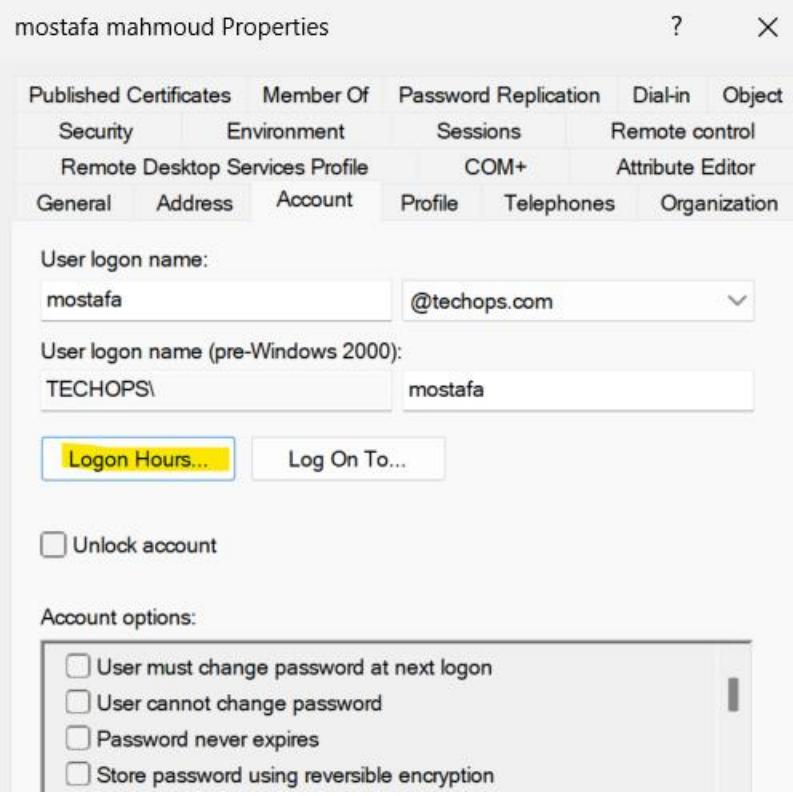
Password never expires

Account is disabled

[< Back](#) Next > [Cancel](#)

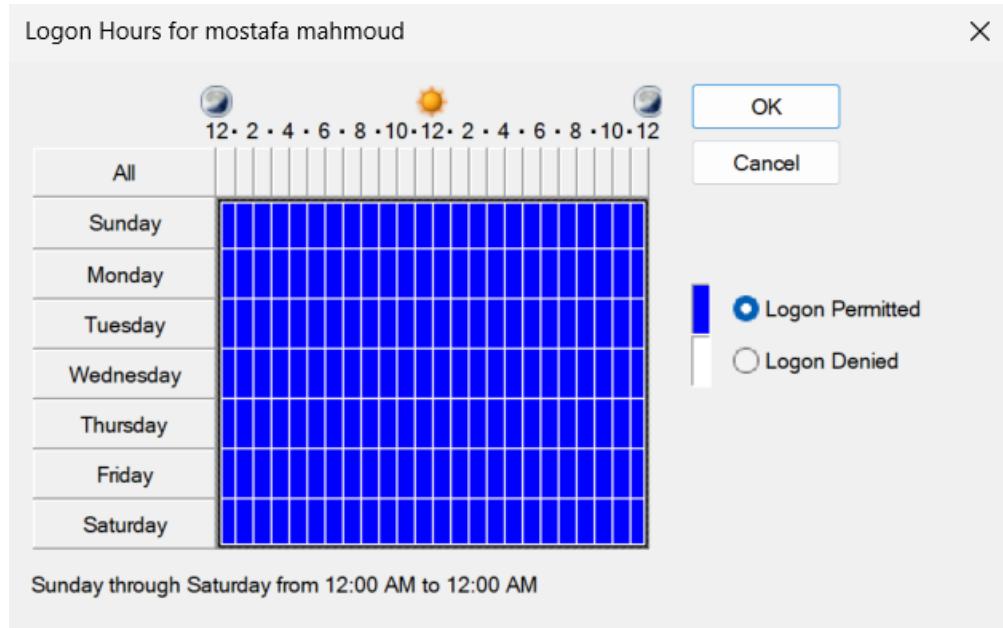
بعد كدا بكتب ال password

وبكدا عملنا User create لـ

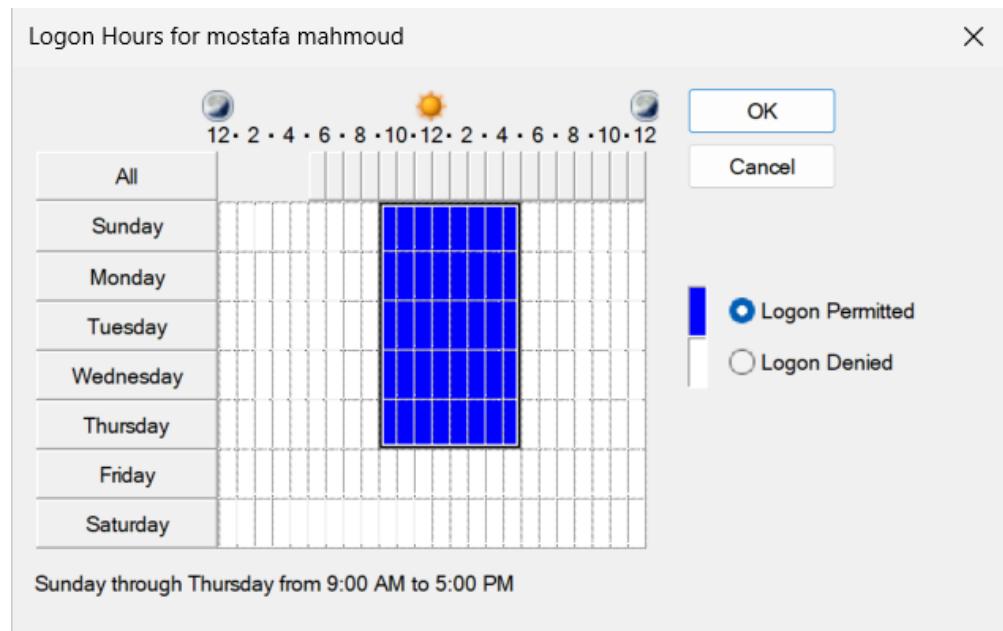


من ضمن الحاجات المهمة في ال account هي ال logon hours

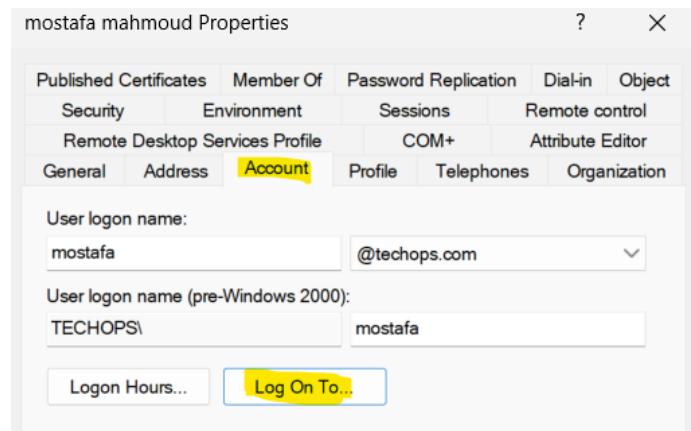
ومن خلالها بقدر اتحكم ان ال user يعمل logon في وقت محدد فقط



في الاساس بتكون ان ال user يقدر يعمل logon في اي وقت لكن انا اقدر اعدل ال config دي

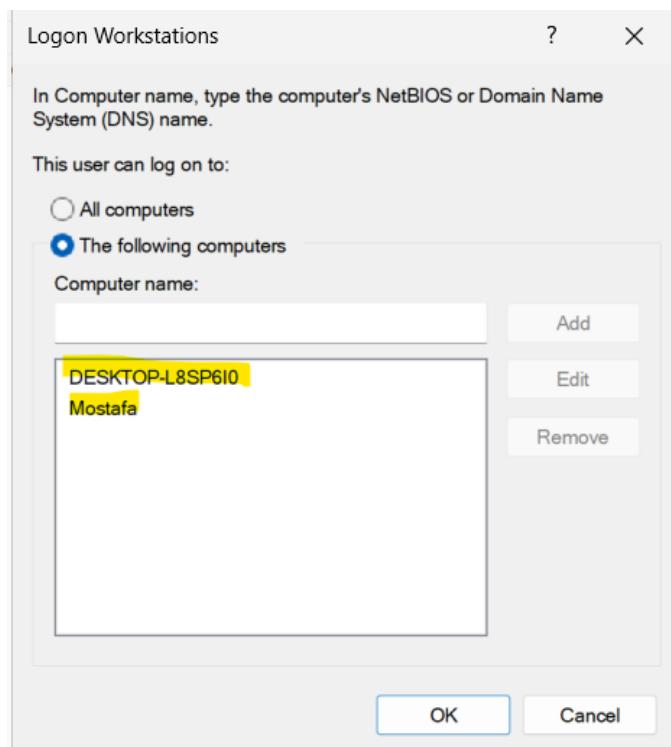


هذا ال user مش هيقدر يعمل logon غير من الاحد للخميس من الساعه 9الصبح للساعه 5 المغرب ال هو وقت العمل فقط اي وقت خارج الوقت المحدد مش هيقدر يعمل logon

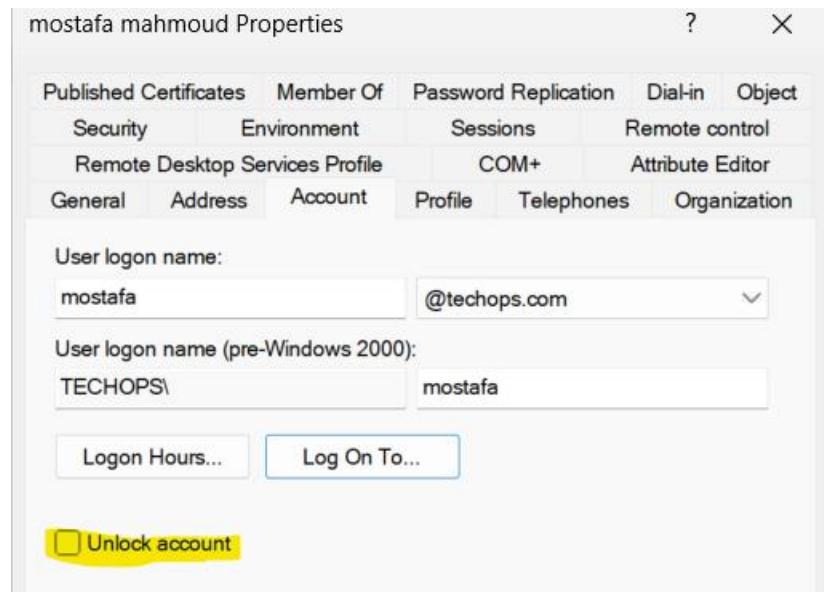


في حاجه اسمها log on to

ال user بيقدر يعمل logon على اي جهاز member من ال domain By default من خلال ال Log On To اقدر احدد مجموعه أجهزه فقط هي دي ال هي عمل عليها logon اي حاجه تاني لا ميقدرش يعمل عليها logon

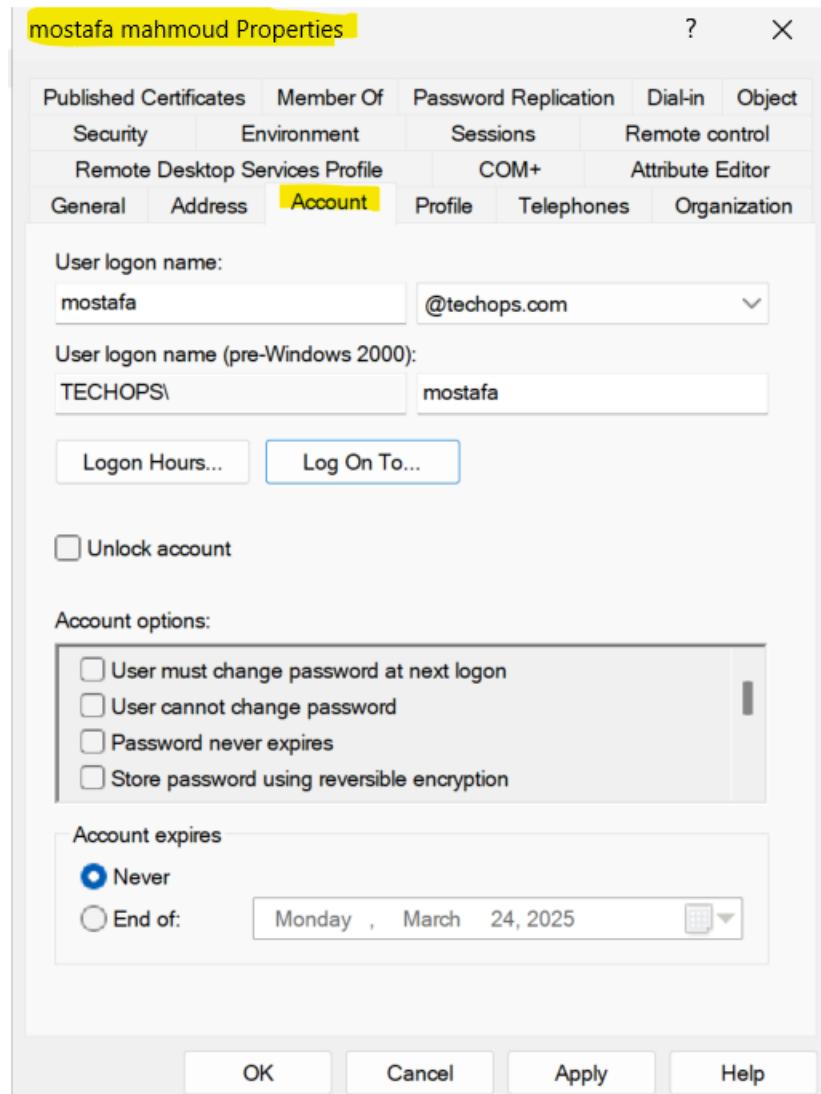


هيقدر يعمل logon فقط على الاجهزين دول فقط



ال unlock account دي بستخدمها ف اي ؟

مثلا بكون عامل GP ان لو ال user كتب ال password 3 مرات في خلال 10 دقائق ان ال account بتاعه يحصله lock ، لو هو فعلا ال user بس كان ناسي ال password ف ساعتها هنيجي على ال unlock account ونهعمل check عليها بحيث ان ال unlock account ميفضلش lock طول المده ال انا محددها

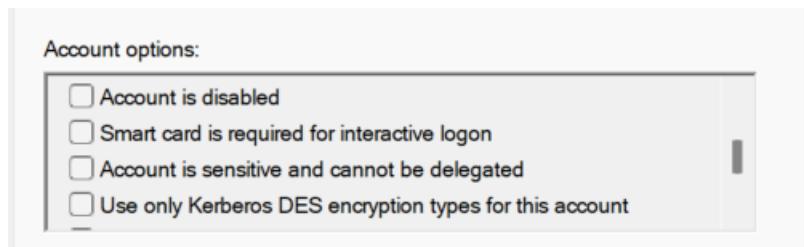


لو فتحنا ال properties الخاص بال user دا ودخلنا علي ال tab ال اسمها account
 هنلاقي ال logon name الخاصه بال user
 وهنلاقي ال account options وتعال نشرحها واحده واحده :

password : هنا بجبر ال user انه يغير ال User must change password at next logon
 بتاعته بعد اول logon
 password : عكس الاولي وهي ان ال user مقدر يغير ال User cannot change password

مش هيكون فيه وقت محدد لتعتير ال password هفضل شغاله دايما عادي

وهنا غلط جدا اننا نعمل check او نفعطها طيب اي السبب؟ لأن كل حاجه داخل بيئه ال domain هي passwords encryption ومنها ال reversible password الخاصه بال Users ف هنا لو فعلت دي ف بقولها اظهوري ال password ب encryption وبما ان ال password فهظور عكس ال encryption وبالنالي ال password هيكون واضح ومفهوم clear text

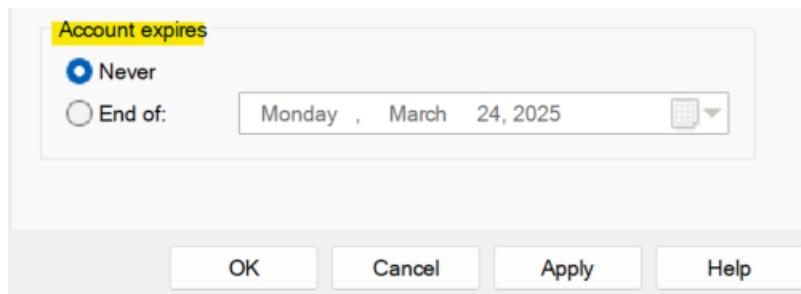


هنا بعمل disable لـ account دا ولو عملت مش user disable : Account is disabled هيقدر يعمل logon

هنا لو فعلتها ال user مش هيعرف يعمل Smart card is required for interactive logon الا لما يستخدم ال Smart Card الخاصه بيه logon

لو فعلته فـ account لا يمكن استخدامه في عمليات ال Delegation (هنشرحها بالتفاصيل فيما بعد)

باقي ال options خاصه بالتشغير وانواعه ولو هتسخدم حاجه معينه منهم



واخيرا في account expires اسمه option

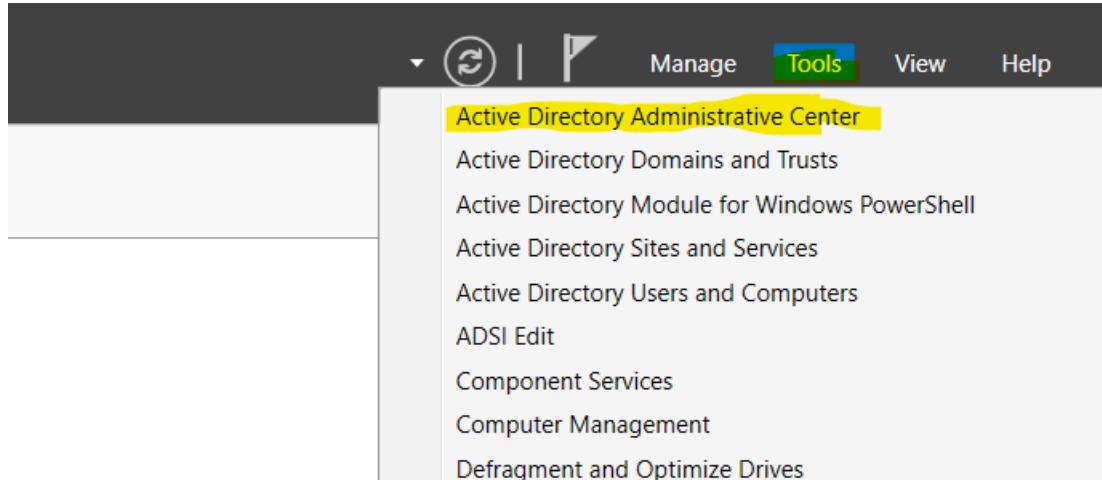
هنا لو عاوز احدد وقت معين ان ال account expire دا يحصله

طيب هل دا ممكن استخدمه ؟

اه ، ول يكن في موظف تابع لجهه خارجيه هيكون متواجد مده 3 أشهر فقط في شركتك هنا تقدر تحدد الوقت
ال هيكون ال account expire دا عشان ميقدرش يستخدمه تاني او لو ماشي ليه ال account يفضل موجود .

في console تاني للتعامل مع ال Users وهو ال

Active Directory Administrative Center



لما بعمله open بلاقيه بالشكل دا :

A screenshot of the Active Directory Administrative Center Overview page. The left sidebar shows navigation links for Active Directory, Overview, Dynamic Access Control, Authentication, and Global Search. The main content area is titled "WELCOME TO ACTIVE DIRECTORY ADMINISTRATIVE CENTER" and includes links to learn more about the center, use the Active Directory module for Windows PowerShell, find answers on the Active Directory Forum, deploy Dynamic Access Control, get Microsoft Solution Accelerator, and deploy Authentication Policies and Silos. At the bottom, there are "RESET PASSWORD" and "GLOBAL SEARCH" sections.

طيب از اي نصيف User من خلاله ؟

WELCOME TO ACTIVE DIRECTORY ADMINISTRATIVE CENTER

Find in this column

Find in this column

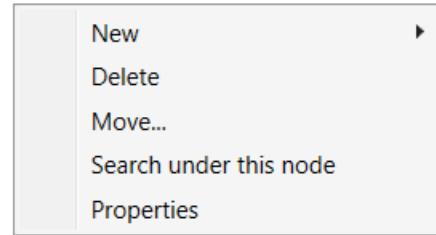
- Builtin
- Computers
- Domain Controllers
- EG
- ForeignSecurityPrincipals
- Keys
- LostAndFound
- Managed Service Accounts
- NTDS Quotas
- Program Data
- System
- TPM Devices
- Users

من ال domain name بتابعك اختيار ال OU ال عاوزها ول يكن هختنار ال EG/hr

Name	Type	Description
mostafa mahmoud	User	

هتلaciها فتحت بالشكل دا

Name	Type	Description
 mostafa mahmoud	User	



اضغط click في اي مكان فاضي هنظهر لك ال options New ومنها اختار User

هناقي كل ال options الخاصه بال user في screen واحده وتقربيا دي افضل حاجه في ال AC

طيب لو عاوز اعمل delete ل user ؟
تعال الاول نشوف قيمه اسمها SID اختصار ل Security Identifier : ودا عباره عن قيمه unique ، يتم تعينه لكل object داخل ال Active Directory
يبقى ال SID يستخدم لتعريف ال objects بشكل فريد داخل ال Domain
بيكون بالشكل دا :

SID: S-1-5-21-4111435051-1387456246-770560793-1105

ال S يرمز الي Security Identifier
ال 1 يرمز الي رقم الإصدار
ال 5 يرمز الي السلطة التي أصدرت SID (في أغلب الحالات تكون Windows NT Authority)
ال 21-4111435051-1387456246-770560793 دا معرف ال domain او الجهاز
ال 1105 دا معرف ال user او group داخل ال domain

وال SID دا ال domain بيعامل معه
وليكن هتعمل access معين ل user معين علي ال share folder دا بيتم ربطه بال username وليس ال SID
وبالتالي لو حذفت user اسمهوليكن ahmed ال معرف ال user بتاعه 1105 وعملت user جديد بنفس الاسم ه يكون user مختلف تماما لانه ه يكون له SID جديد

Name	Type	Description
ahmed	User	Copy... Add to a group... Disable Account Reset Password... Move... Open Home Page Send Mail
mostafa mAhmoud	User	All Tasks > Cut Delete Rename Properties Help

هنعمل delete لـ user ال اسمه ahmed ودا ال SID الخاص بيـه هو 1105

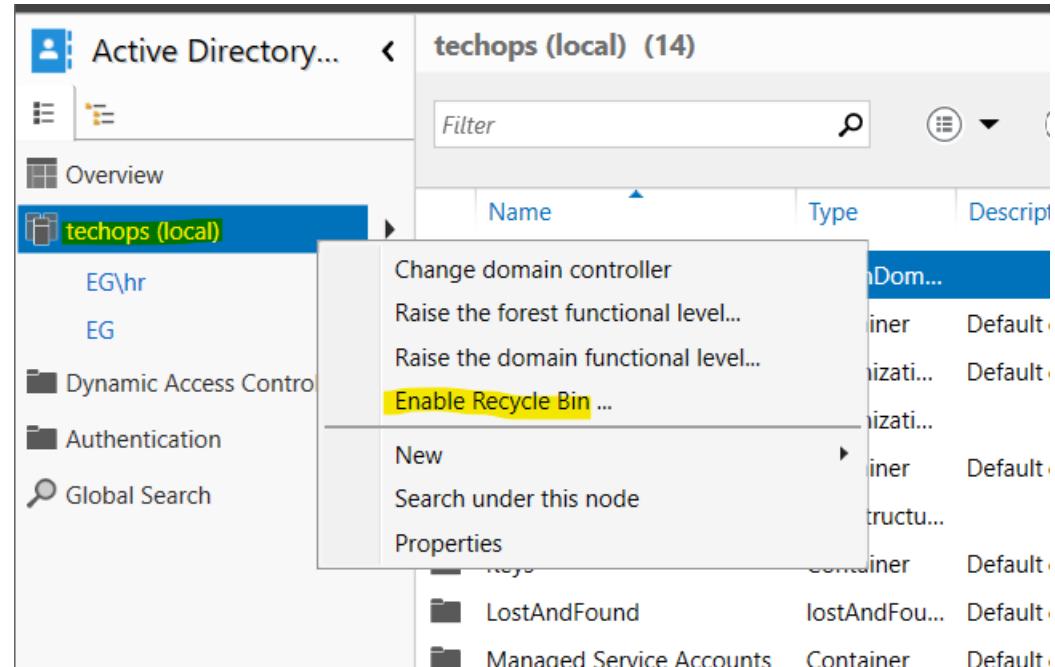
Name	Type	Description
ahmed	User	
mostafa mAhmoud	User	

بعد كدا هنعمل user جديد بنفس الاسم وتعال نشوف ال SID الخاص به

SID: S-1-5-21-4111435051-1387456246-770560793-1106

ال SID بقت مختلفه لأن الاول كان 1105 ودلوقت بقا 1106

طيب ازاي اعمل recovery لل user ال اتمسح ؟
 في ال features اسمها Recycle Bin في Administrative admin center خاصه بال windows server 2008R2 ودي بدأت بدأ من domain 2008R2 يكون domain function level وبالتالي ال طيب افعلها ازاي ؟



بعد ما نفتح ال administrative admin center هنضغط على اسم ال domain ونختار Enable Recycle Bin
 طيب هل الاول user عملناها ينفع نعمله recovery لا لأننا فعلنا ال recycle bin بعد ما حذفناه لكن لو دلوقت حذفنا ال user ول يكن عندي user اسمه Mohamed ال SID بتاعه

mohamed

Account	Account First name: mohamed Middle initials: Last name: Full name: * mohamed User UPN logon: mohamed @ techops.com User SamAccountName logon: techops \ mohamed <input type="checkbox"/> Protect from accidental deletion Log on hours... Log on to...	Account expires: <input checked="" type="radio"/> Never <input type="radio"/> End of [] Password options: <input checked="" type="radio"/> User must change password at next log on <input type="radio"/> Other password options <input type="checkbox"/> Microsoft Passport or smart card is required for interactive log on <input type="checkbox"/> Password never expires Encryption options: Other options:
Organization	Display name: mohamed Job title:	
	Modified: 2/23/2025 10:11:04 AM Created: 2/23/2025 10:11:04 AM Object class: User Canonical name: techops.com/EG/hr/mohamed Last log on: <Not Set> Last bad log on: <Not Set> Log on count: 0 Bad password count: 0 Update sequence numbers (USN): Current: 24616 Original: 24610 User account control: 0x200 GUID: 9205d544-7b65-4a0b-bf95-ae335290ddde SID: S-1-5-21-4111435051-1387456246-770560793-1102 Password last set: <Not Set> Password expiration: <Expired>	

OK Cancel

هعمله delete

Active Directory...

Overview

techops (local)

- EG\hr
- EG
- Dynamic Access Control
- Authentication
- Global Search

hr (1)

Name	Type	Description
mostafa mahmoud	User	

مبقاش موجود عندي لانه اتعمله delete

The screenshot shows the Active Directory Users and Computers interface. The left navigation pane is visible with options like Overview, techops (local), EG\hr, EG, Dynamic Access Control, Authentication, and Global Search. The main pane displays the 'techops (local) (15)' view. A table lists various objects with columns for Name, Type, and Description. The 'Deleted Objects' container is highlighted in blue. Below the table, a section titled 'Deleted Objects' provides details: Object class: Container and Description: Default container for deleted objects.

Name	Type	Description
Builtin	builtinDom...	
Computers	Container	Default container for upgr...
Deleted Objects	Container	Default container for delet...
Domain Controllers	Organizati...	Default container for dom...
EG	Organizati...	
ForeignSecurityPrincipals	Container	Default container for secur...
Infrastructure	infrastructu...	
Keys	Container	Default container for key o...
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Container	Default container for man...

Deleted Objects

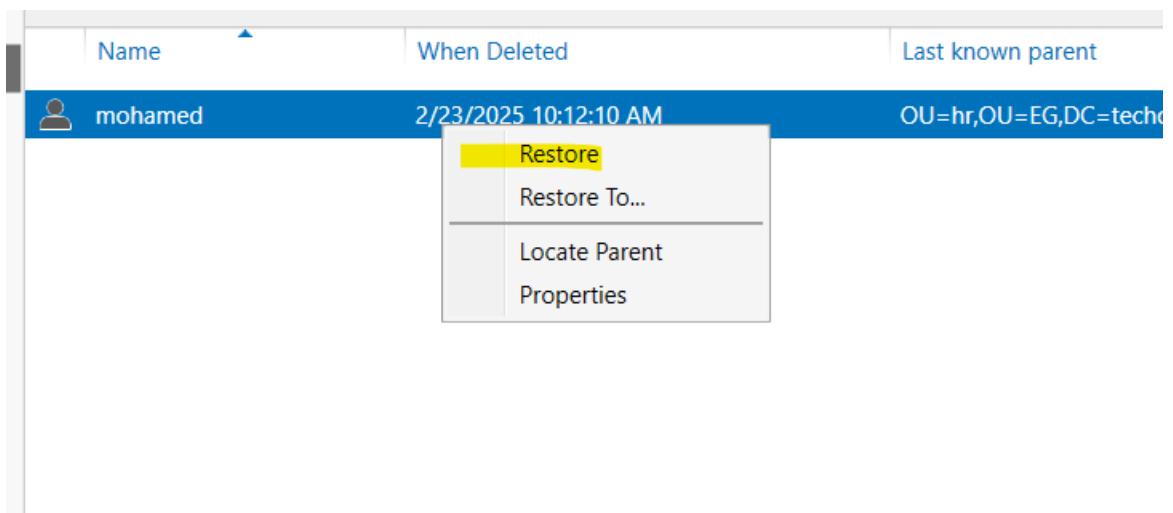
Object class: Container
Description: Default container for deleted objects

لو ضغطنا على اسم ال domain وفتحناه هنلاقي في حاجه جديد ظهرت اسمها Deleted Objects

The screenshot shows the Active Directory Users and Computers interface. The left navigation pane is visible with options like Overview, techops (local), Deleted Objects, EG\hr, EG, Dynamic Access Control, Authentication, and Global Search. The main pane displays the 'Deleted Objects (1)' view. A table lists the deleted object with columns for Name, When Deleted, Last known parent, Type, and Description. One entry is shown: mohamed, deleted on 2/23/2025 10:12:10 AM, with a parent of OU=hr,OU=EG,DC=techops,DC=com and Type User.

Name	When Deleted	Last known parent	Type	Description
mohamed	2/23/2025 10:12:10 AM	OU=hr,OU=EG,DC=techops,DC=com	User	

لو فتحناها هنلاقي ال user ال اتعمله delete



عليه واختار restore لو عاوز ترجعه للمكان ال كان فيه Click

او restore to لو هترجعه في مكان ثاني

او لو عاوز تعرف هو كان موجود فين هنختار locate parent

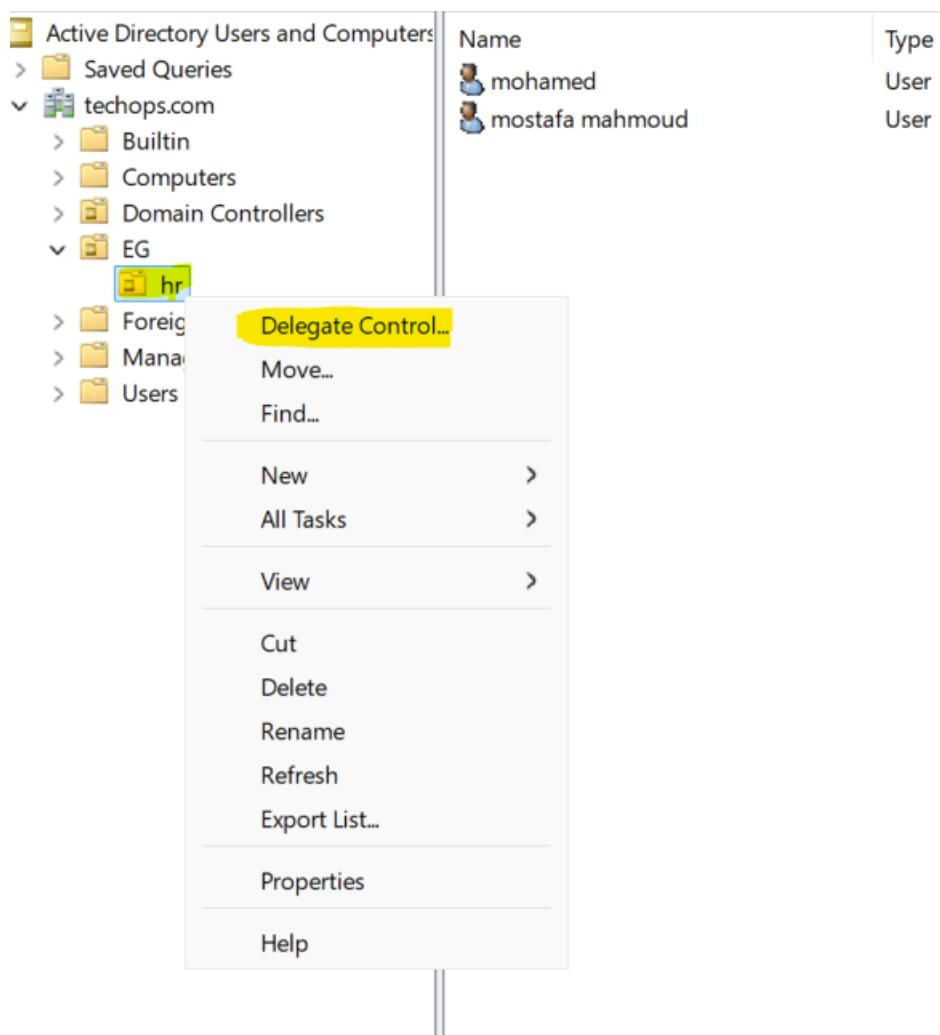
A screenshot of the Active Directory Users and Computers console. The left navigation pane shows 'Active Directory...' and several containers like 'techops (local)', 'EG\hr', 'Deleted Objects', 'EG', 'Dynamic Access Control', 'Authentication', and 'Global Search'. The 'Deleted Objects' container is currently selected. The main pane displays a table with columns: Name, Type, and Description. Two users are listed: 'mohamed' (User type) and 'mostafa mahmoud' (User type). Both users are highlighted in blue.

كدا حصله restore بعد ما كنت عملته delete

Create User Delegation

ال Delegation : هو التفويض بمعنى اني منح User permission معين لـ User معين لتنفيذ مهمه معينه او عمل objects mange لـ User معين انه يقدر يعمل على reset password كل domain group بتابع اي اخليه administrator على كل domain container او على OU معين delegation ممكن اطبقه على كل او على OU معين

طيب ازاي ابدا اعمل ال user delegation لـ user معين ؟



من ال OU هختار Delegate Control

--

Delegation of Control Wizard

Welcome to the Delegation of Control Wizard



This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.

To continue, click Next.

< Back

Next >

Cancel

Help

Next

--

Delegation of Control Wizard

Users or Groups

Select one or more users or groups to whom you want to delegate control.



Selected users and groups:

Add...

Remove

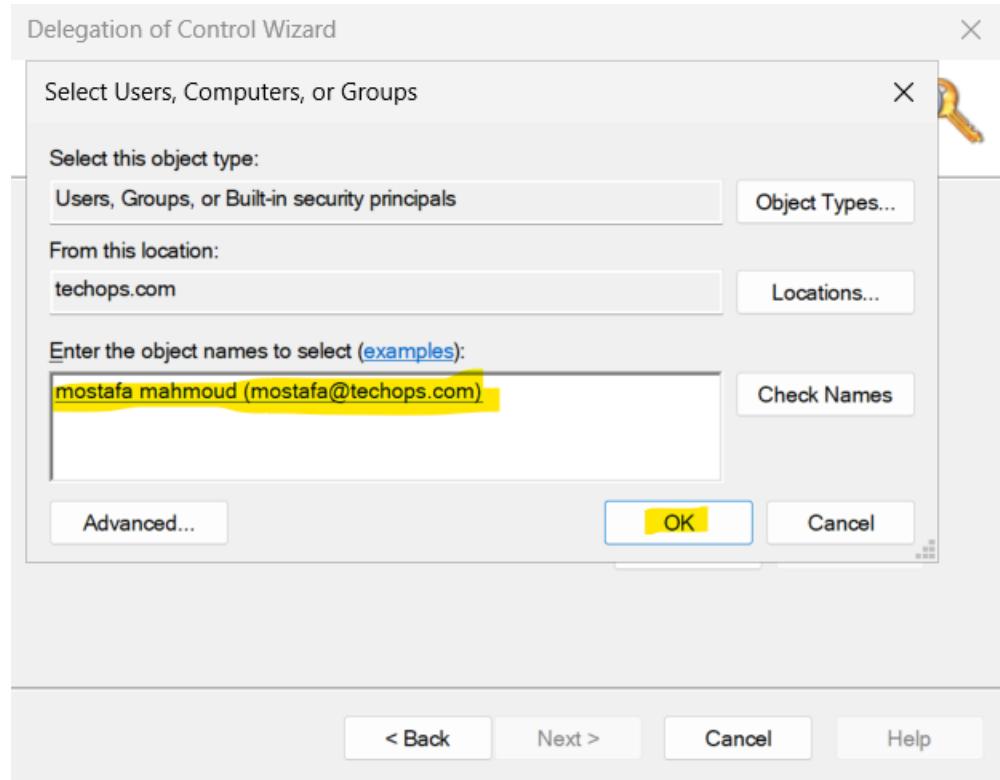
< Back

Next >

Cancel

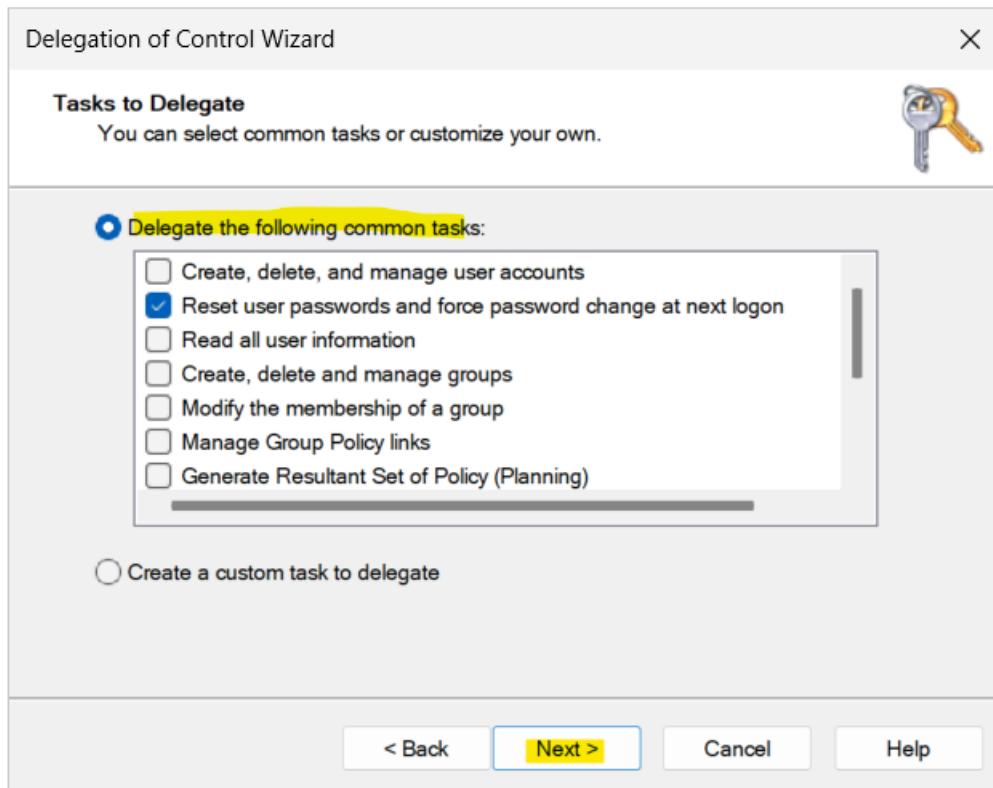
Help

Add



بضيف ال user ال عاوز اعمله delegation وبعده كدا ok ثم Next

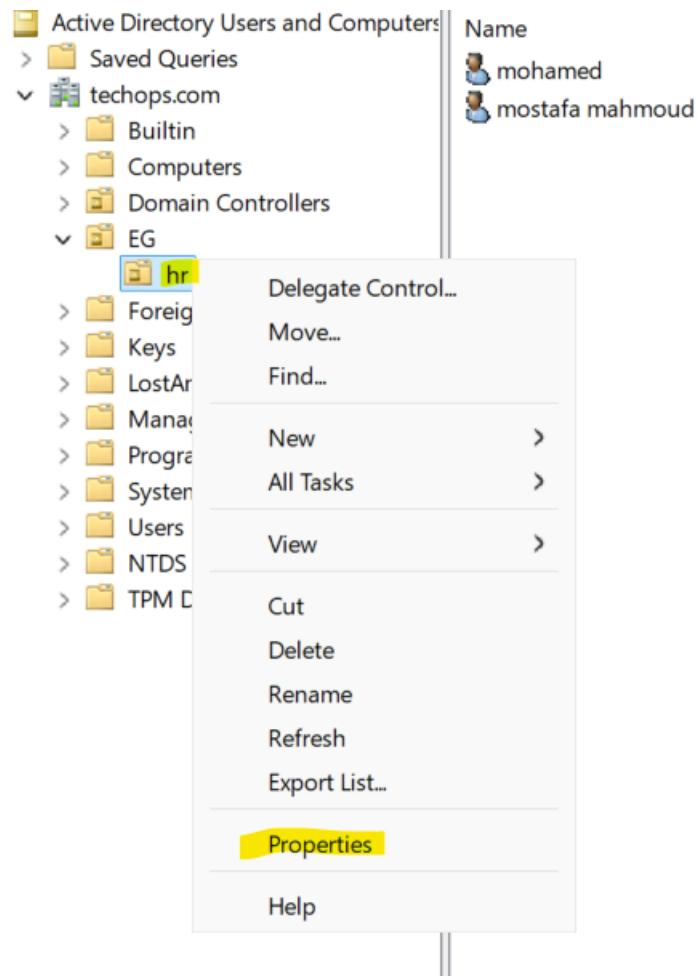
--



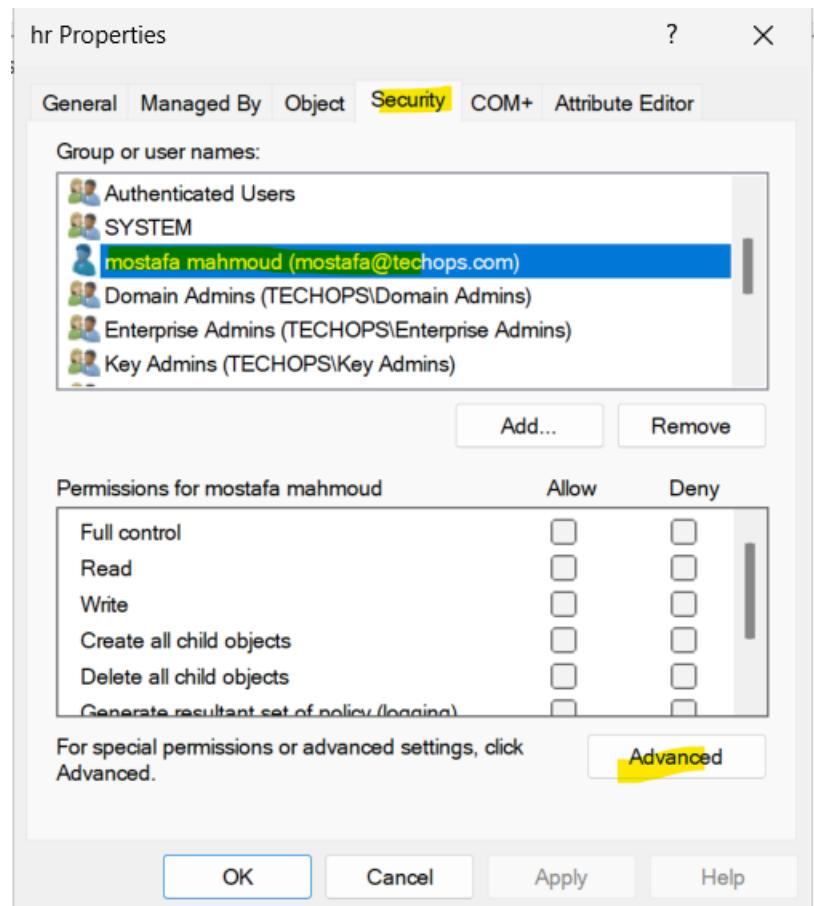
بعد کدا بحدد ال reset password ال user دا یقدر یعملها و هنا اختارت ال delegation task

--

طیب ازای اعمل Remove لل delegation ؟



من ال OU هنختار properties



ومن ال security هناقي ال user ف هنروح على Advanced

Advanced Security Settings for hr

Owner: Domain Admins (TECHOPS\Domain Admins) [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Principal	Type	Access	Inherited from	Applies to
Everyone	Deny	Special	None	This object only
mostafa mahmoud (mostafa@t...)	Allow	Reset password	None	Descendant User objects
mostafa mahmoud (mostafa@t...)	Allow		None	Descendant User objects
Account Operators (TECHOPS\A...)	Allow	Create/delete InetOrgP...	None	This object only
Account Operators (TECHOPS\A...)	Allow	Create/delete Compute...	None	This object only
Account Operators (TECHOPS\A...)	Allow	Create/delete Group o...	None	This object only
Print Operators (TECHOPS\Print ...)	Allow	Create/delete Printer o...	None	This object only
Account Operators (TECHOPS\A...)	Allow	Create/delete User obj...	None	This object only
Domain Admins (TECHOPS\Do...)	Allow	Full control	None	This object only
ENTERPRISE DOMAIN CONTRO...	Allow	Special	None	This object only

Add Remove Edit Restore defaults

Disable inheritance

OK Cancel Apply

هعمل remove لـ permissions بتاع ال user دا

Remote management

في اكتر من طريقة تقدر تعمل بيها servers لـ remote management

زي اي ؟

DOS - 1 : ودي بتكون عن طريق ال

RDP - 2 : ودي اختصار ل remote desktop protocol ودا أشهرهم

server manager - 3

windows admin center - 4

mmc - 5

powershell - 6

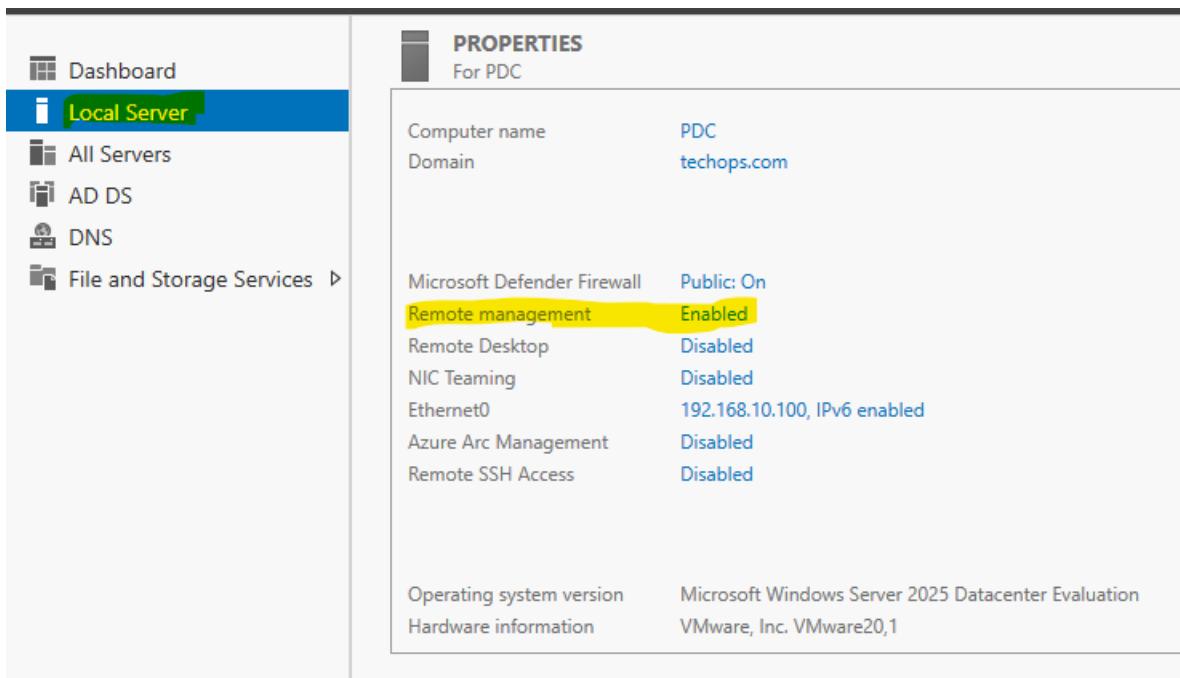
طيب هنركز في شرحنا على الأشهر والأهم وهو ال RDP :

أول حاجة ازاي افعل ال RDP على ال server ؟

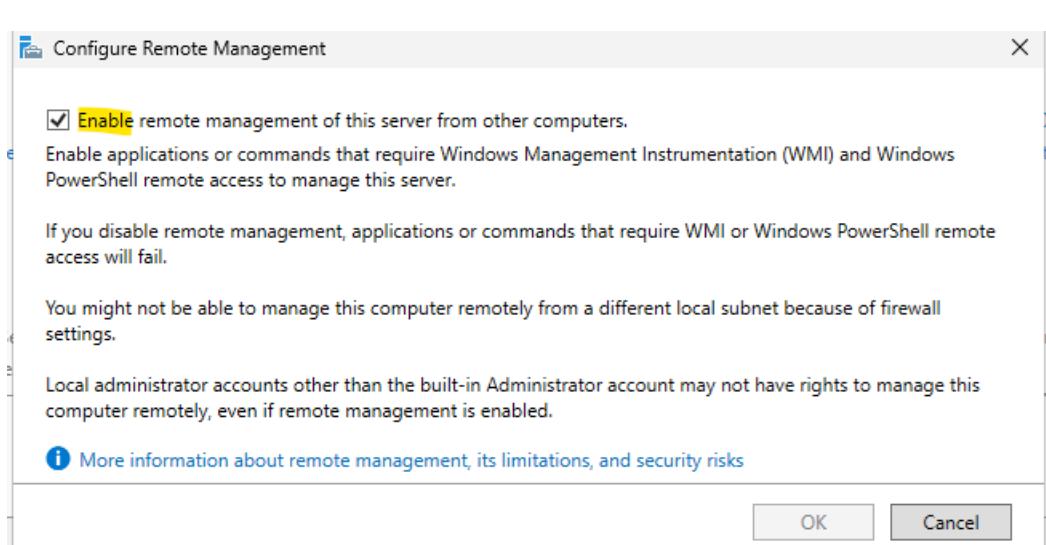
لكن هناخد فكره عن كل واحده :

Windows Remote Management : اختصار ل WinRM – 1

GUI



من ال Remote Management بفتح ال Local server هلاقي ال Server manager



فهي كدا Enable

كدا جاهز اعمل RM على السيرفر ال اسمه pdc
ف لو روحت على pc مثلاً وعاوز اعمل command اسمه ipconfig بس كانى بعمله على ال pdc

علي ال PC بفتح ال CMD ك administrator

```
C:\Users\Administrator.TECHOPS>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . . . . . : 
  Link-local IPv6 Address . . . . . : fe80::ea35:dade:6108:e1ed%3
  IPv4 Address. . . . . : 192.168.10.150
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 

C:\Users\Administrator.TECHOPS>winrs -r:pdc.techops.com ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . . . . . : 
  Link-local IPv6 Address . . . . . : fe80::b3fb:ba83:d378:c21b%9
  IPv4 Address. . . . . : 192.168.10.100
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 

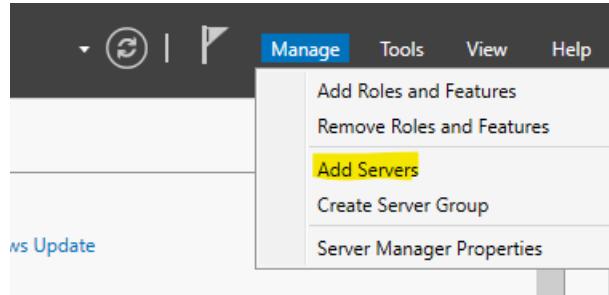
C:\Users\Administrator.TECHOPS>
```

اول command عادي بعمله ع pc ال انا موجود عليه دلوقت فال ip بتاعه 150
لكن تاني command بقوله نفذلي الامر دا علي السير ال اسمه pdc وبالتالي جاب ال ip بتاع ال pdc
ال هو 100

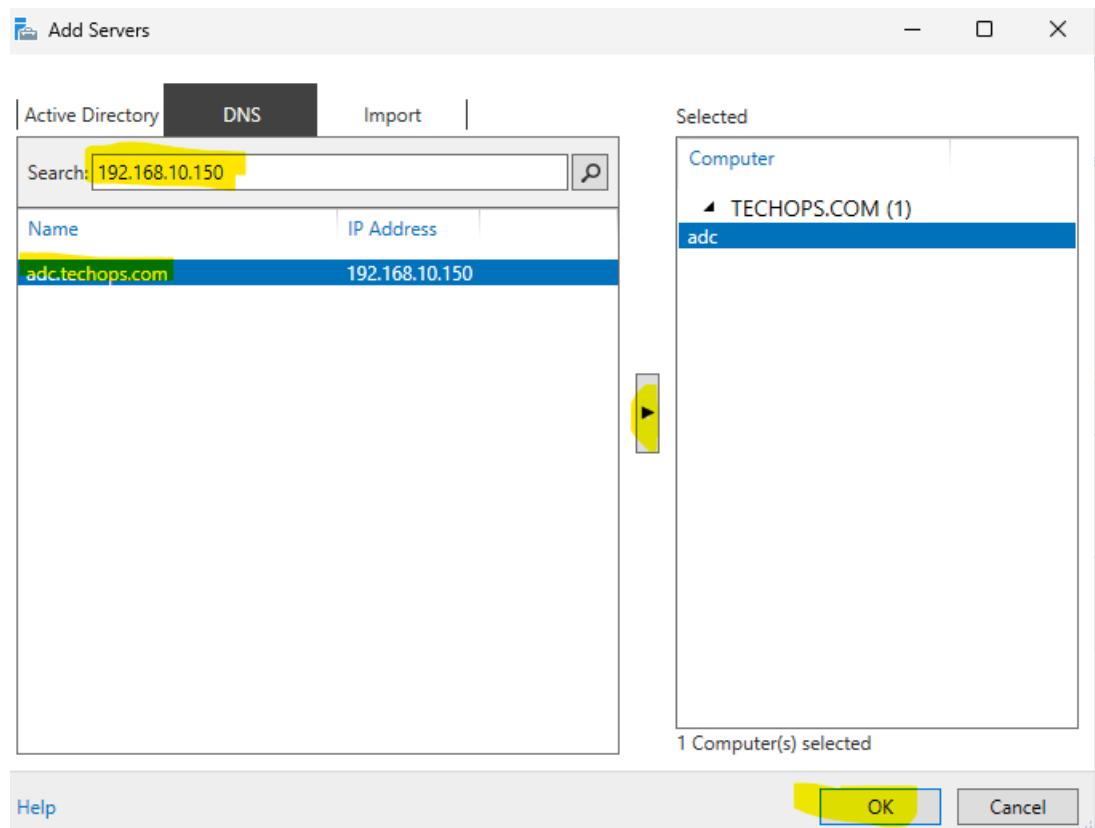
ال هو دا : Server Manager -2

The screenshot shows the Windows Server Manager interface. The left sidebar is titled "Local Server" and lists "All Servers", "AD DS", "DNS", and "File and Storage Services". The main pane displays the "PROPERTIES" for the "PDC" role. It includes sections for "Computer name" (PDC), "Domain" (techops.com), "Microsoft Defender Firewall" (Public: Off, Remote management: Enabled), "Operating system version" (Microsoft Windows Server 2025 Datacenter Evaluation), and "Hardware information" (VMware, Inc. VMware20,1). On the right, there are sections for "Last installed updates" (Windows Update, Last checked for updates: Today at 6:11 PM), "Microsoft Defender Antivirus" (Real-Time Protection: On, Feedback & Diagnostics, IE Enhanced Security Configuration: On, Time zone: (UTC-08:00) Pacific Time (US & Canada), Product ID: Not activated), and "Processors" (AMD Ryzen 7 5700U with Radeon Graphics, Installed memory (RAM): 5.66 GB).

طب ازاي استخدمه ؟



من manage هعمل Add Servers



عمل add لـ server ok manage اعمله عاوز انا لـ

Servers

All servers | 2 total

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
ADC	192.168.10.150	Online - Performance counters not started	3/11/2025 6:28:37 PM	00492-10000-00001-AA467 (Activated)
PDC		Add Roles and Features Restart Server	/2025 6:27:54 PM	00492-10000-00001-AA489 (Activated)

EVENTS
All events | 39 to

Server Name	Date and Time
ADC	3/11/2025 6:19:53 PM
ADC	on 3/11/2025 6:19:40 PM
ADC	3/11/2025 6:19:40 PM
ADC	3/11/2025 6:17:53 PM
ADC	3/11/2025 6:12:53 PM
ADC	on 3/11/2025 6:07:53 PM
ADC	on 3/11/2025 6:06:53 PM

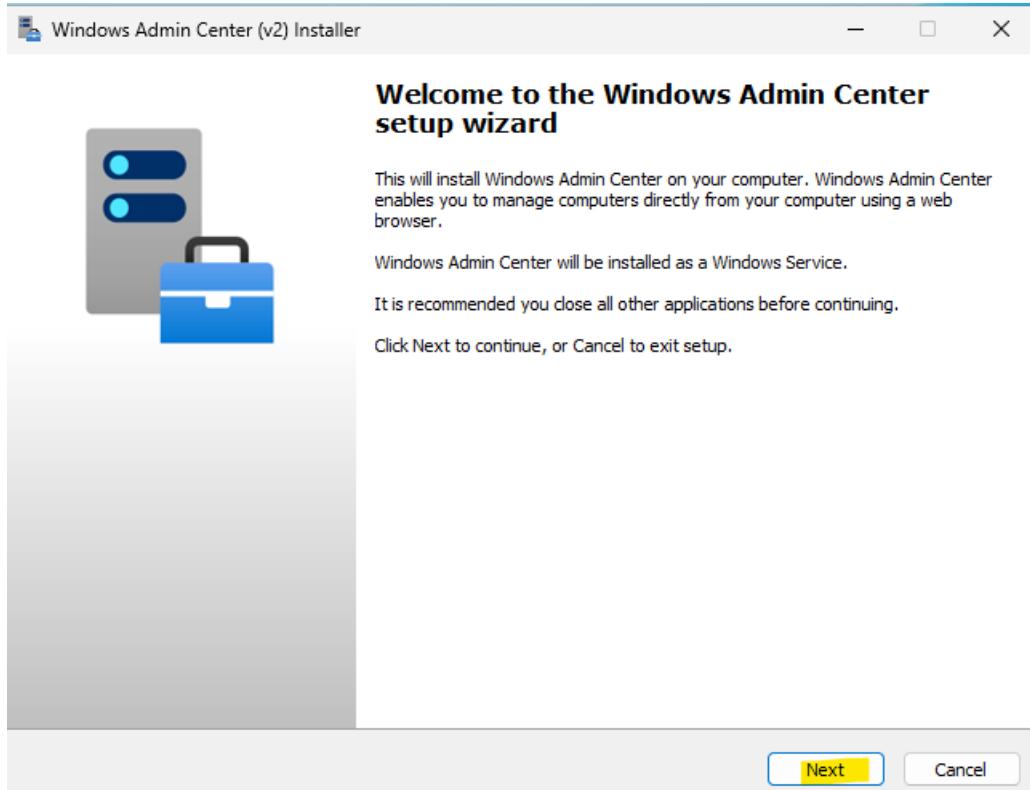
SERVICES
All services | 24:

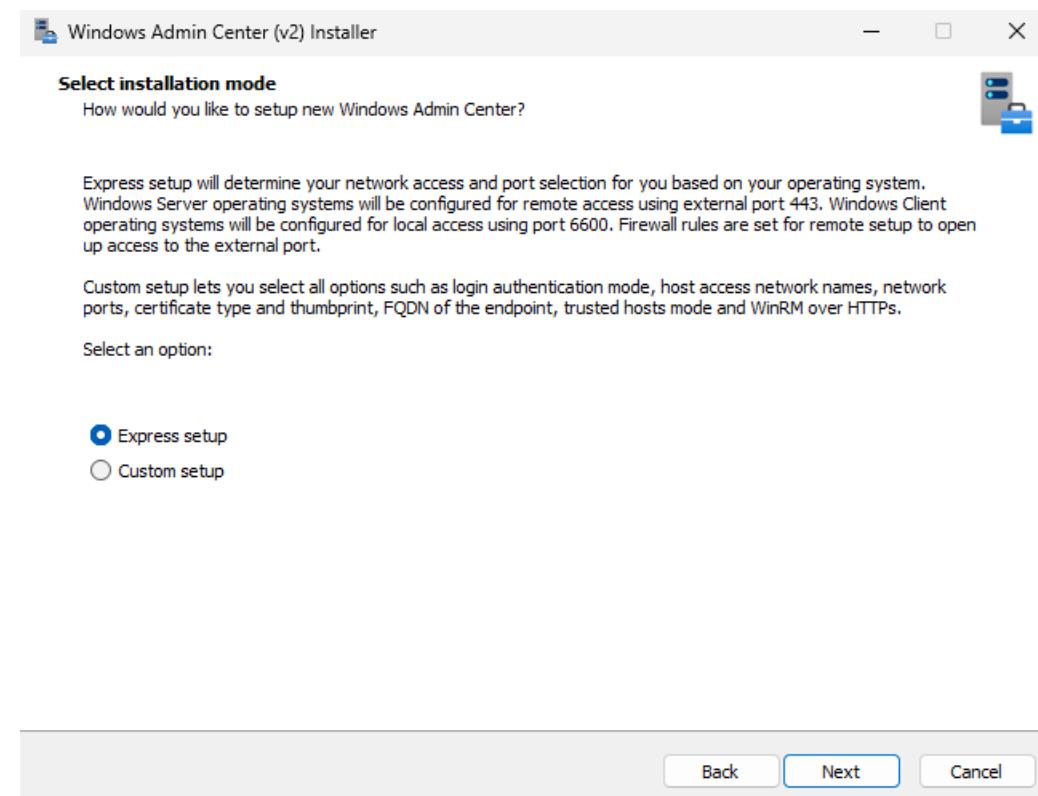
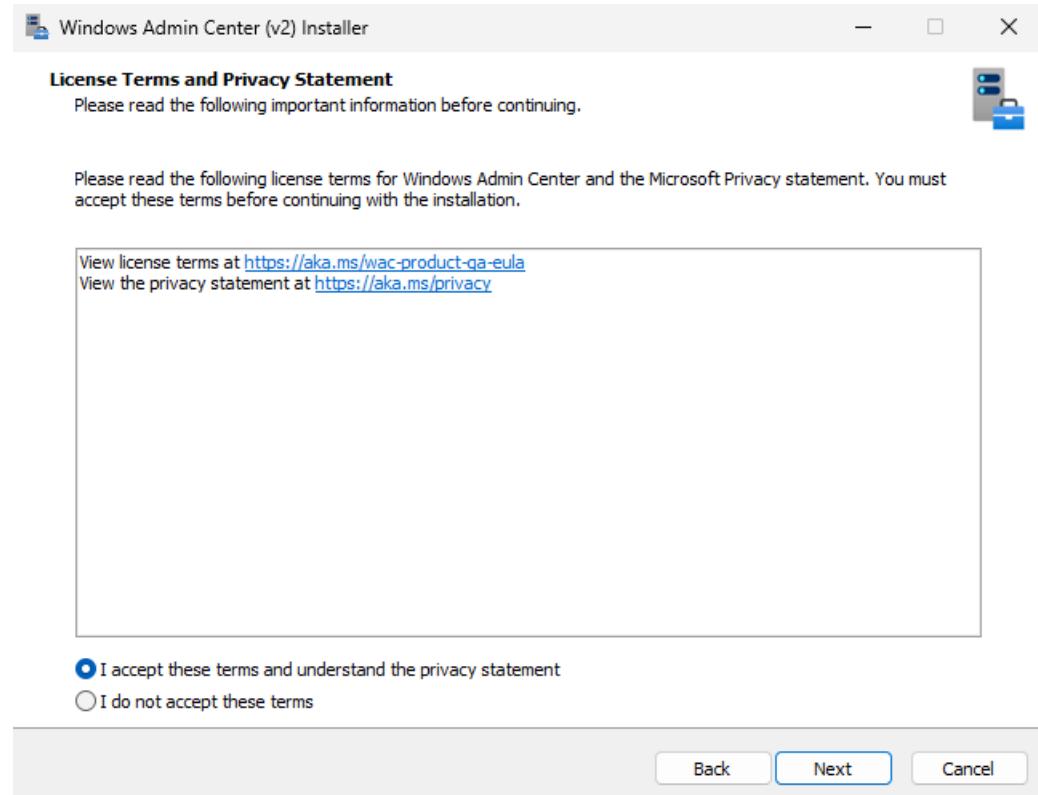
Server Name	Status	Start Type
ADC	Running	Automatic (Delayed Start)

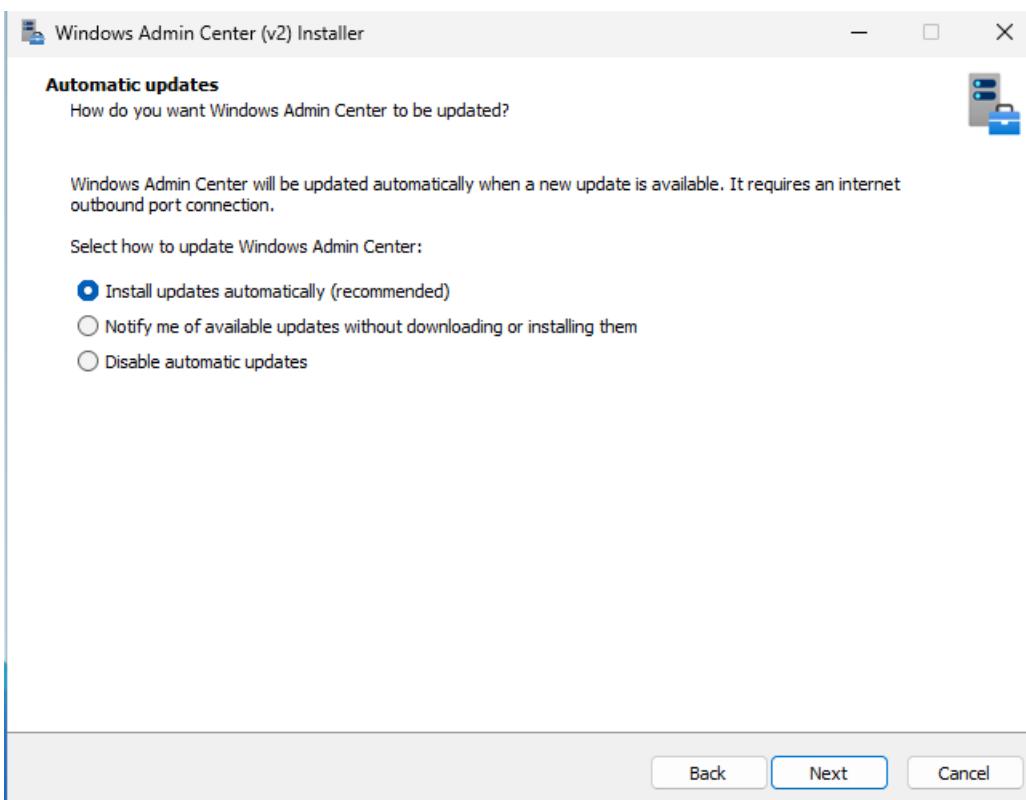
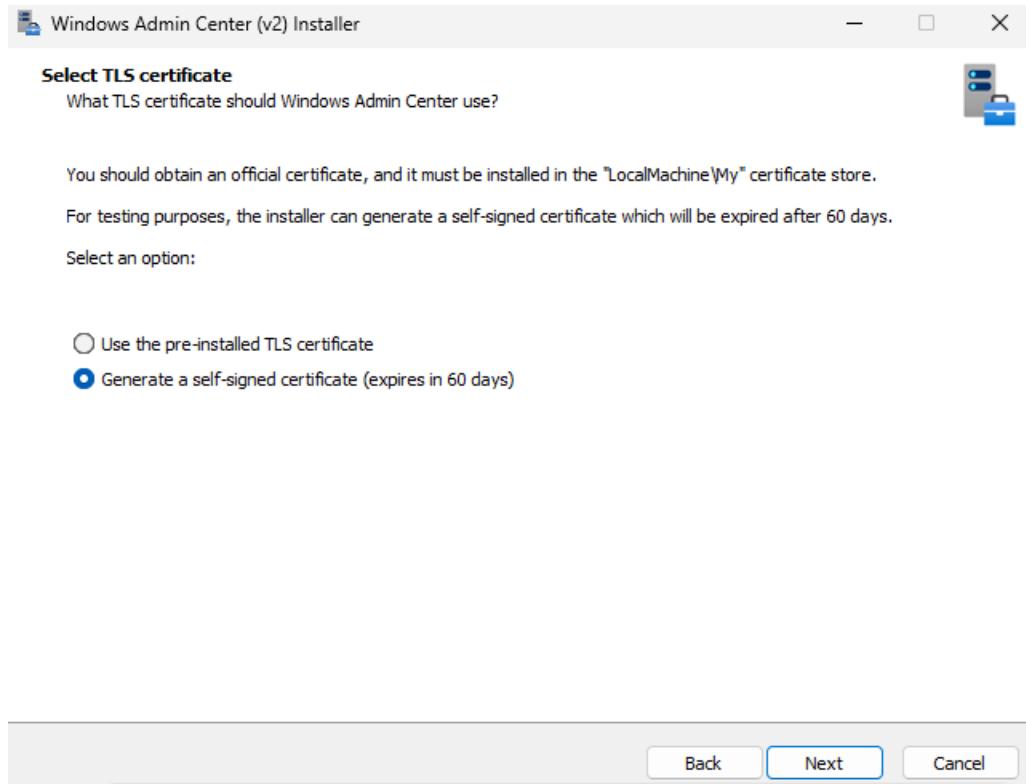
ومن All Servers هلاقی ال ADC وادر اعمله manage

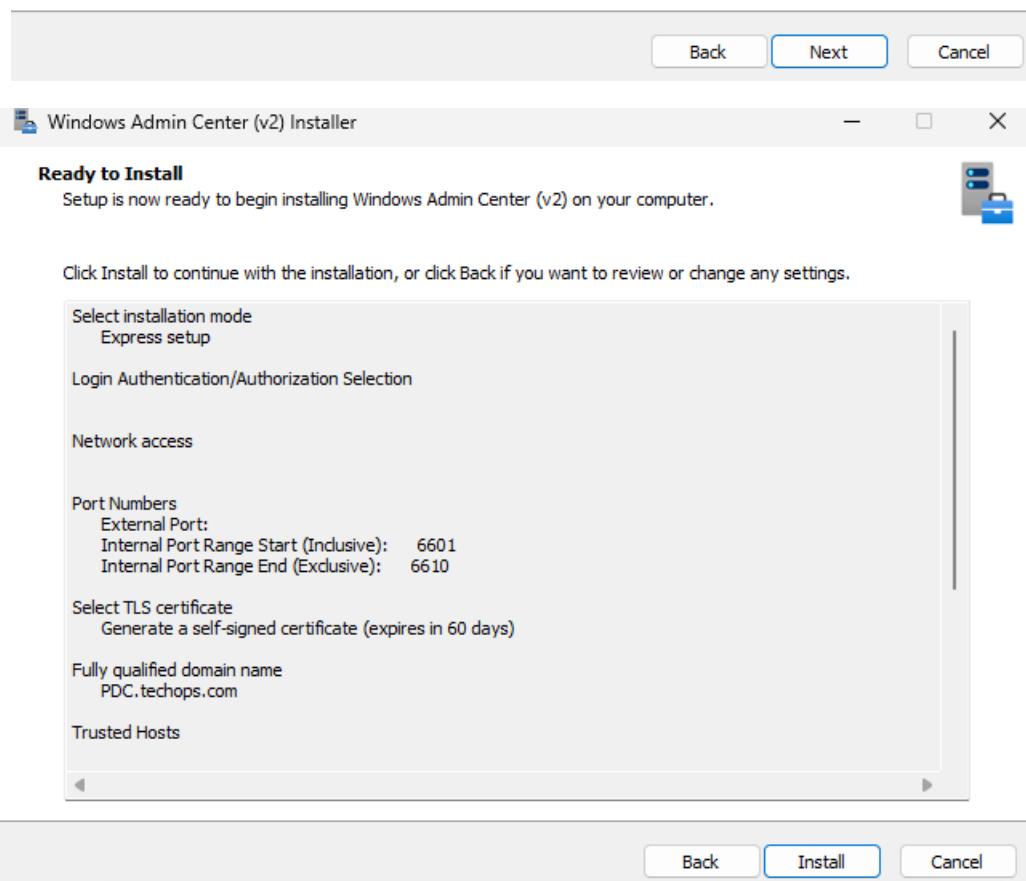
Windows Admin Center : WAC -3
و دا قائم على ال web (من المتصفح)

هو ال app بتعمله download وinstall









Windows Admin Center | All connections ▾ Microsoft

Windows Server 2025 is now generally available! Explore the latest updates that improve security, performance, and flexibility. Consider upgrading today. [Learn more ↗](#) [X](#)

[Add](#) [Connect](#) [Manage as](#) [Remove](#) [Edit Tags](#) [→ Connect to Arc](#)

<input type="checkbox"/> Name ↑	Type	Last connected	Managing as	Azure Arc Status	Tags
mostafa_Gateway	Windows PCs	Never	NTECH\mostafa.mahmoud	Unknown	

1 item [⟳](#) [Y](#) [🔍](#)

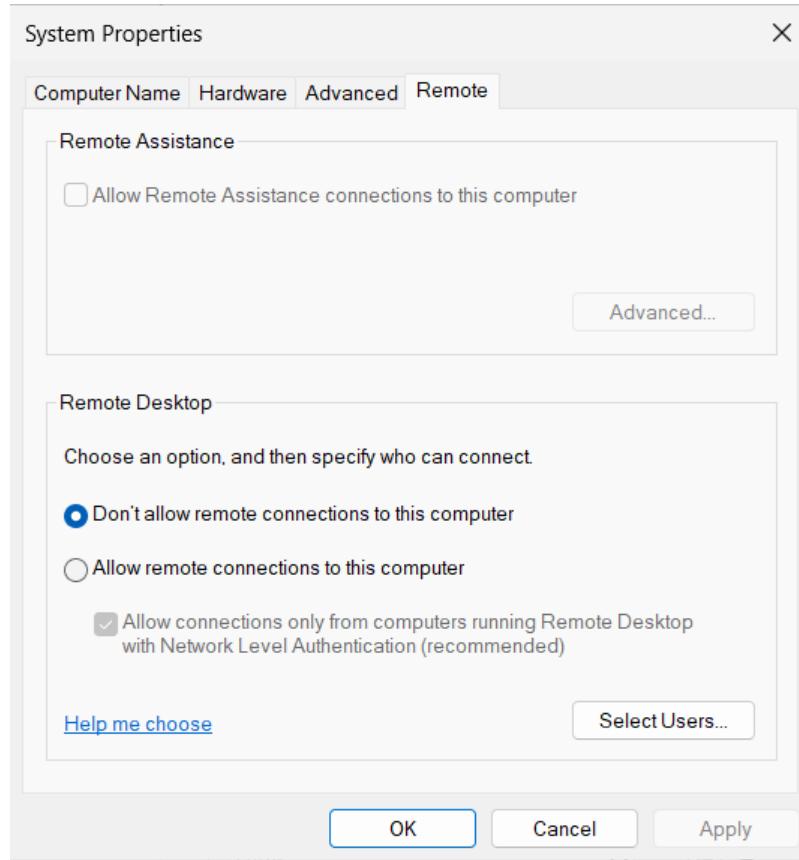
بنكتب ال ip وال port ونعمل login Add لـ servers

هندا ال : RDP

The screenshot shows the Windows Server Manager interface. The left sidebar has a 'Local Server' section selected. The main area is titled 'PROPERTIES For PDC' and displays various system settings:

Setting	Value
Computer name	PDC
Domain	techops.com
Microsoft Defender Firewall	Public: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet0	192.168.1.35, IPv6 enabled
Azure Arc Management	Disabled
Remote SSH Access	Disabled
Operating system version	Microsoft Windows Server 2025 Datacenter Evaluation
Hardware information	VMware, Inc. VMware20,1

من ال remote desktop هنفتح ال local server ونختار ال server manger



هناقيها Allow و هنختار don't allow

ال option ال هو

Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

لما بعمله allow بقوله ان يسمح فقط للاجهزه التي تستخدم ال Network Level Authentication فقط انها تقدر تعمل remote access

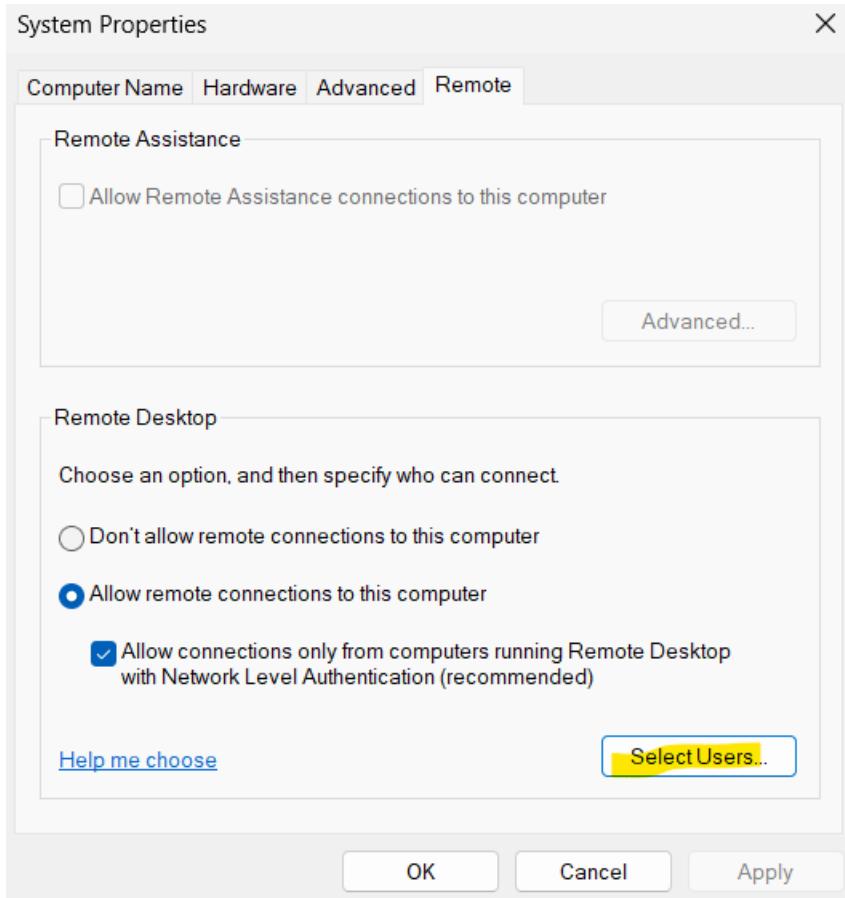
تفله في حاله واحده وهي لو بتعمل remote access من جهاز قديم زي windows xp لانه مش بـ support Network Level Authentication ال كله windows 7 لكن من Network Level Authentication support

Network Level Authentication

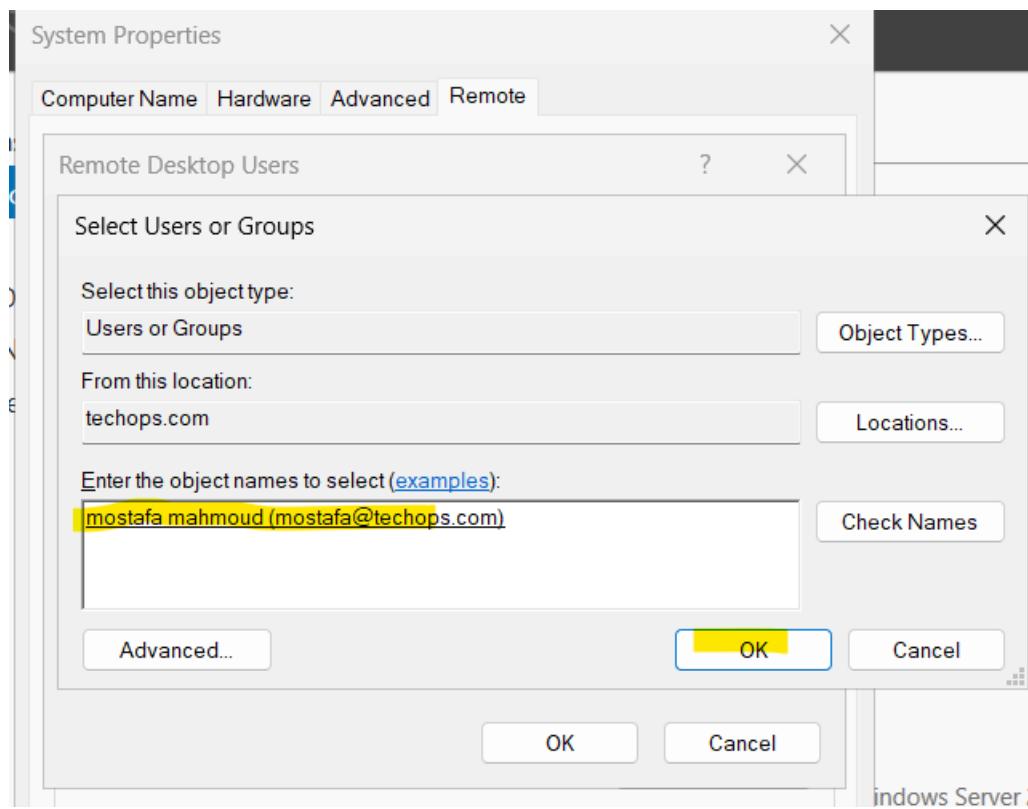
طيب اي الفائده منه ؟

بيحميني من هجمات معينه زي ال Brute Force لانه بيمنع ال connection قبل ان تتم عمليه ال Authentication

طیب لو عاوز اضیف user معین هو ال يقدر يعمل : remote access

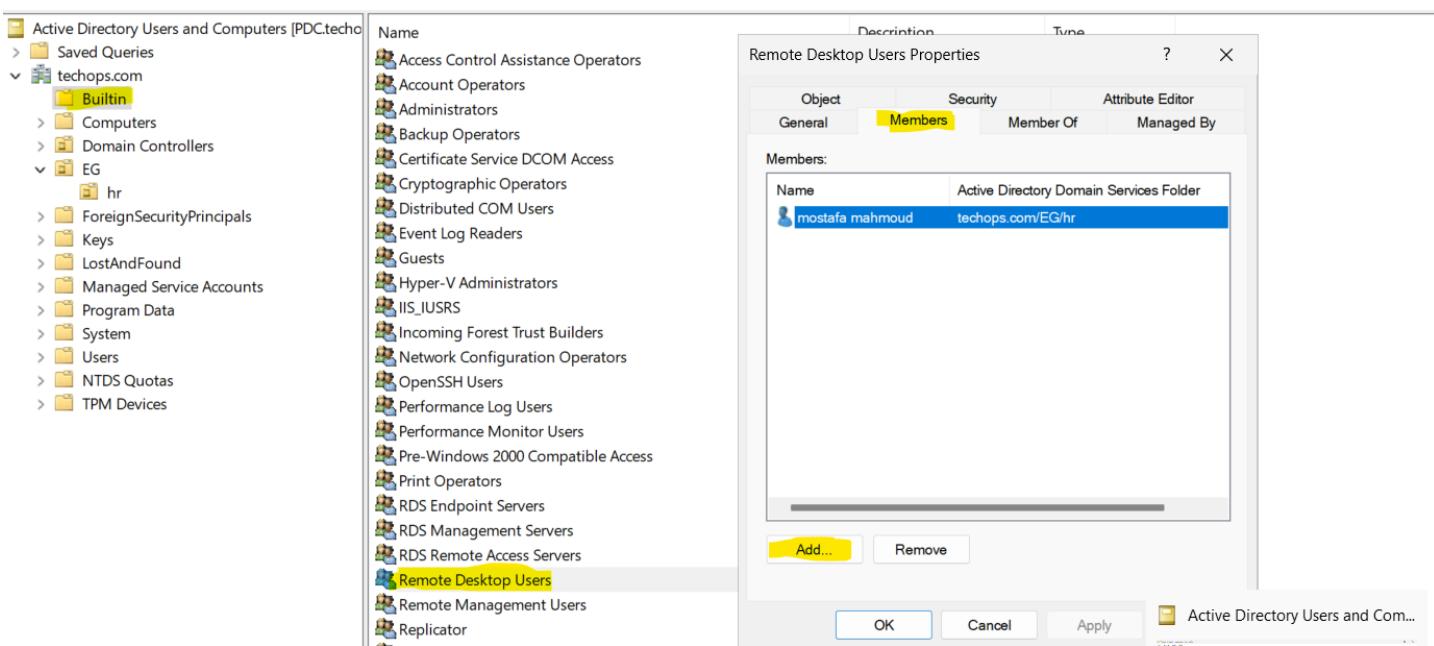


من نفس ال Select Users هختار console --



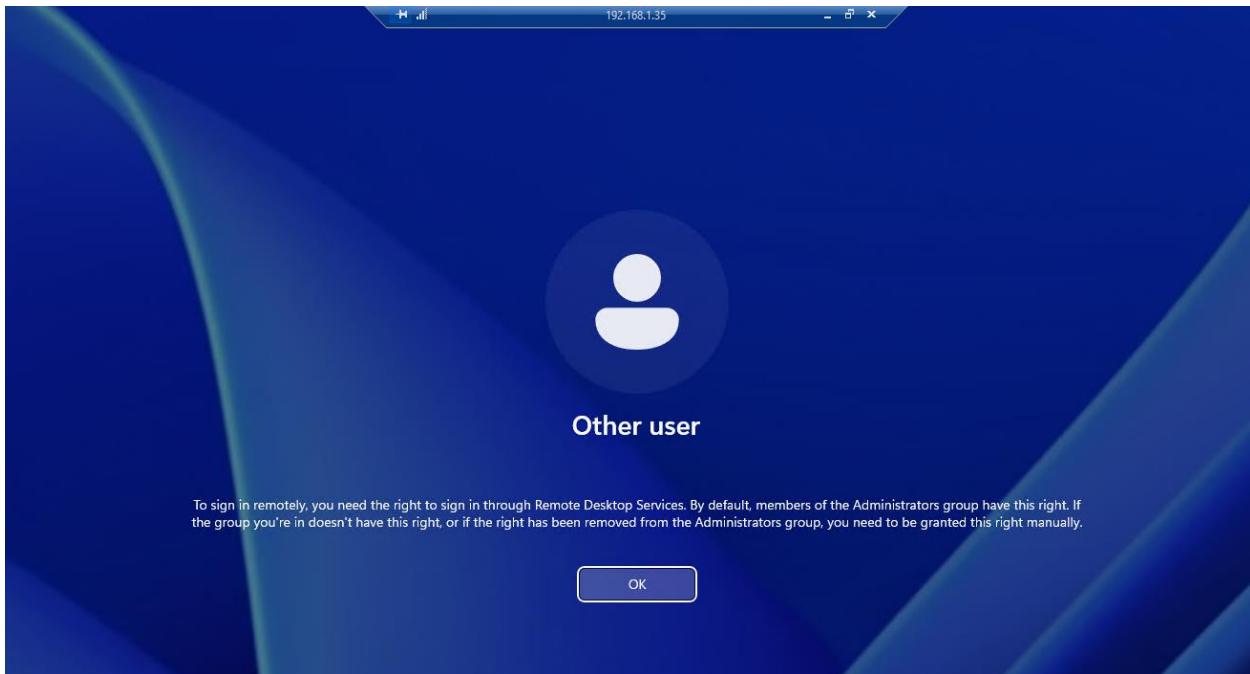
وختار ال user ال عاوزه

--
في طریقه کمان

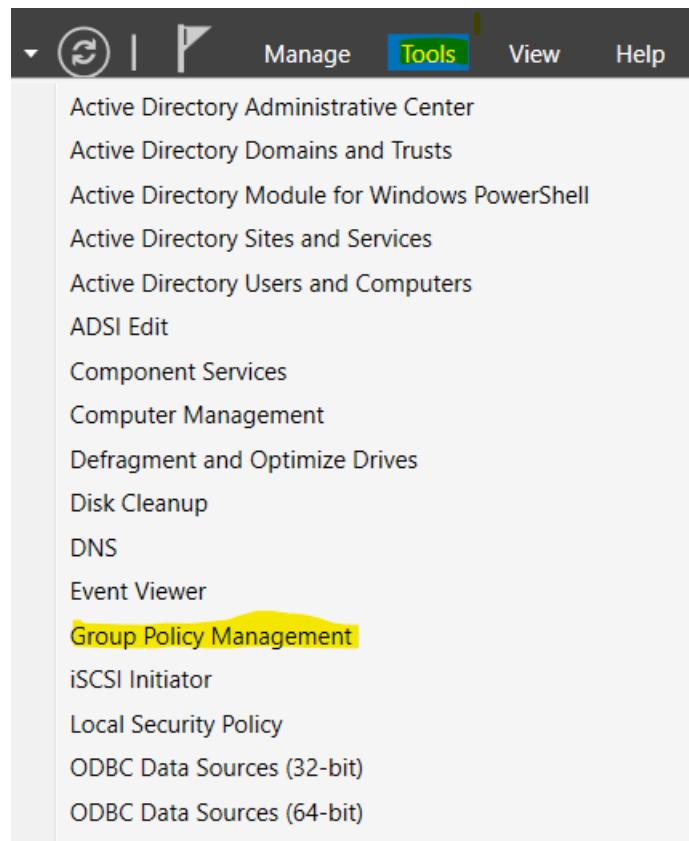


من ال Group users and group هختار ال container ومنه هختار ال Group واعمل Members او remove منها هروح علي ال Remote Desktop users اسمها ، ونلاحظ ان ال user ال صفتة في الخطوه السابقة ظهر هنا

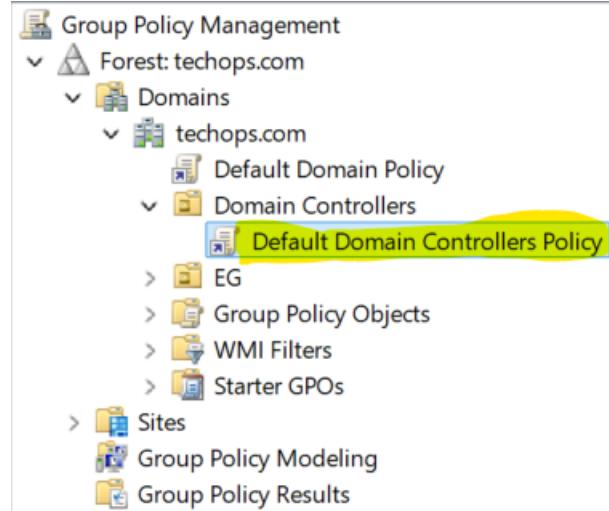
طيب بعد م ضفت ال user ال اسمه mostafa هل اقدر اعمل بيه ؟ remote access
لا لان ال server دا domain controller وال user ال اسمه mostafa عادي وفي
الا user login على ال domain server by default policy تكون بتكون سوا
remote او locally



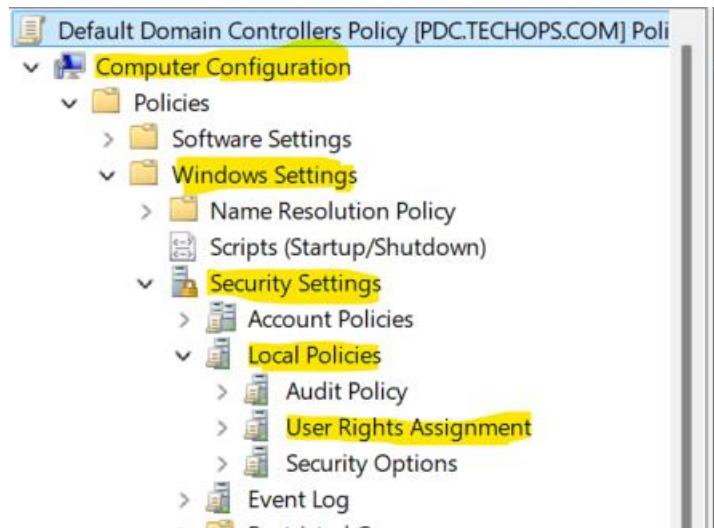
طيب ازاي اخليه يقدر يعمل login ؟
من ال group policy بقدر اعدلها :



من ال tools هروح على group policy management



هروح على ال Default domain controllers policy

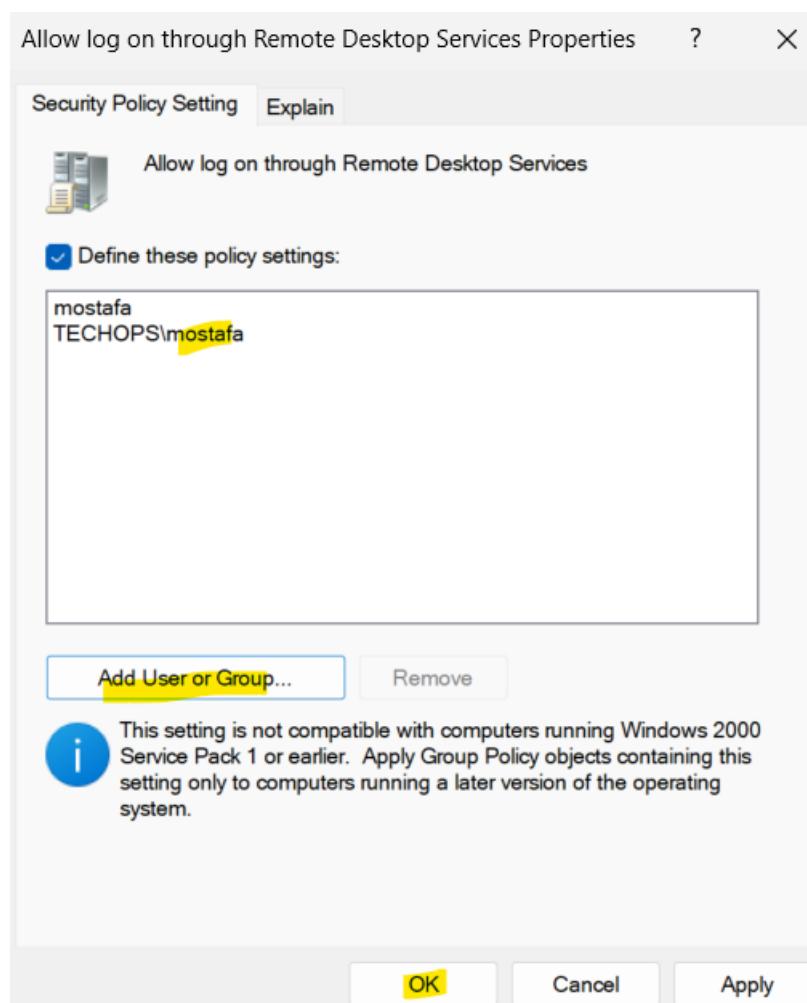


هروح على ال Windows Settings ومنها هروح على computer configuration

وهختار منها ال Local Policies ومنها هختار ال Security Settings ومن ال User Rights Assignment

The screenshot shows the 'Computer Configuration' node expanded, with 'Policies' selected. Under 'Policies', 'User Rights Assignment' is highlighted. A context menu is open over this item, with 'Allow log on through Remote Desktop Services' being the selected option.

وبعد كذا هختار ال allow logon through Remote Desktop Services



واخيرا هختار ال user واعمل ok

طيب لو دلوقت روحت عملت logon هيفتح معاليا ؟

لا لانه ال policy لسه مسمعتش وعشان تسمع في اكتر من طريقة

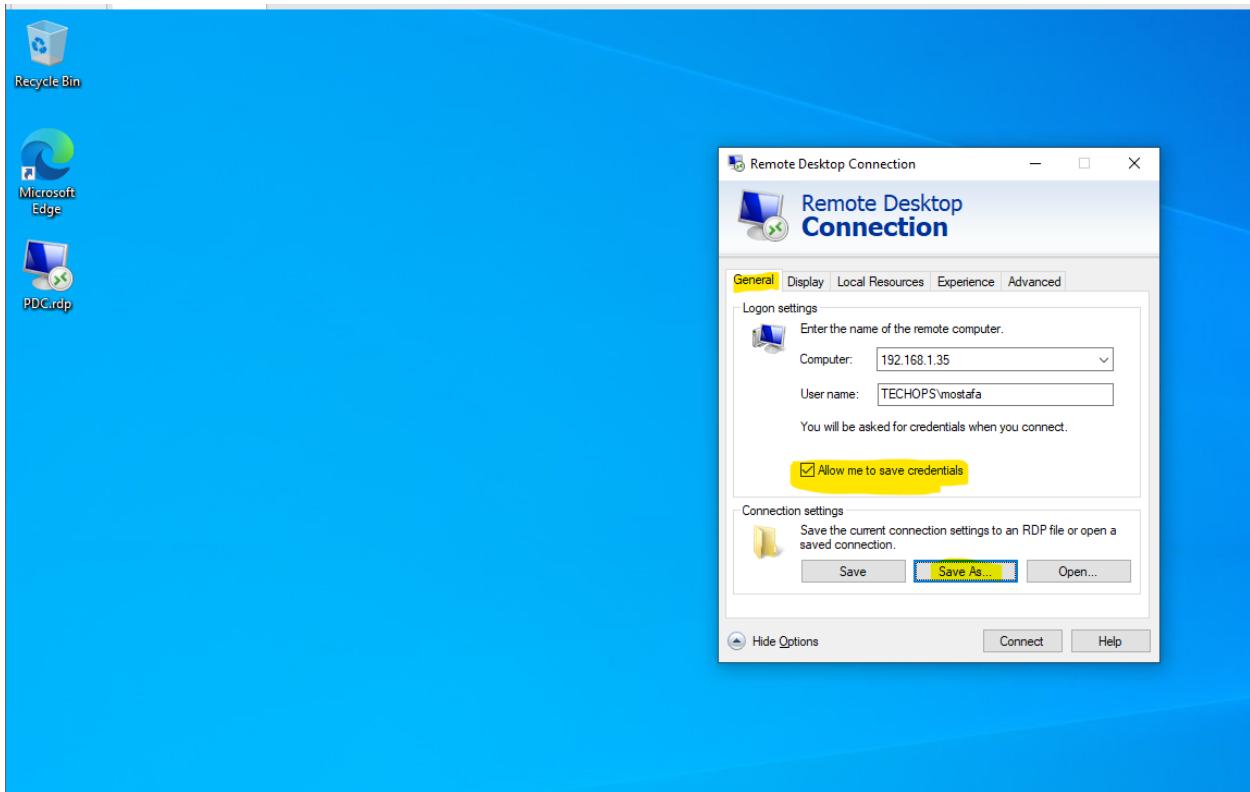
انك تعمل لـ server restart

او انك تزوج على ال CMD وتكتب الامر دا

gpupdate /force

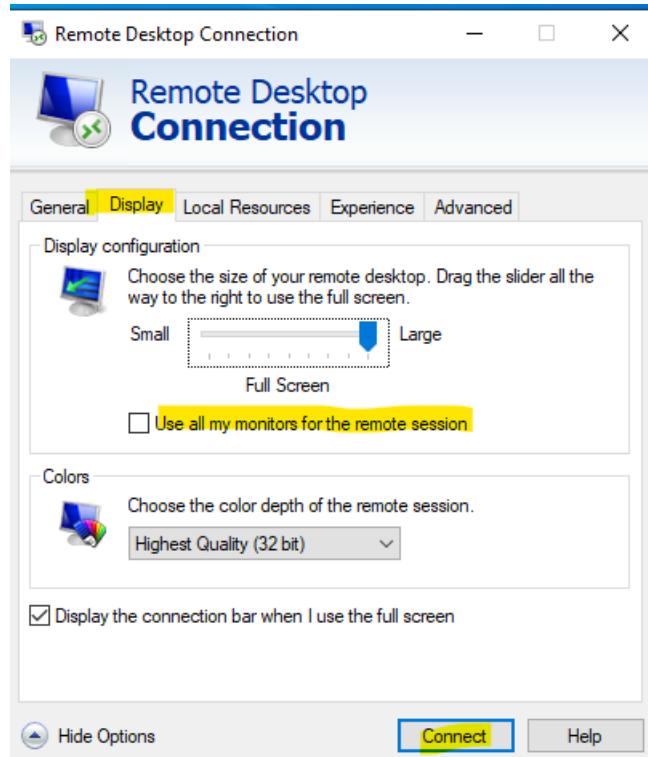
```
C:\Users\Administrator>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

```
C:\Users\Administrator>
```



لو ضغطت علي ال show option هيفتحي ال options
ف اقدر اعمل save لـ connections واقدر عمل save لـ credentials نفسها زي الموجوده على
ال desktop

--

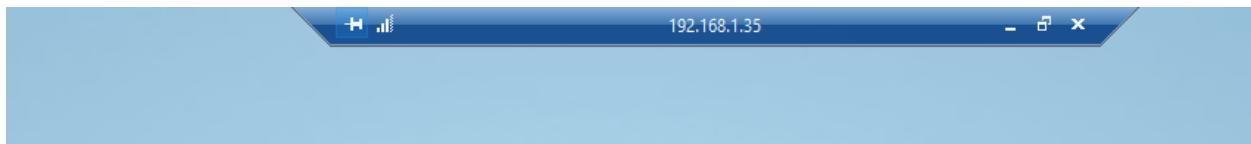


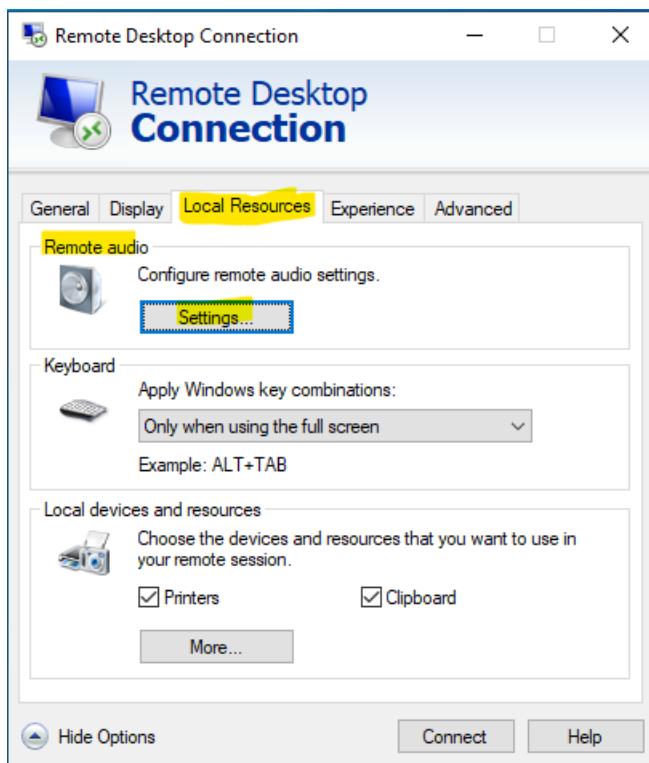
في ال display : بقدر اتحكم ف ال size الخاص بال remote desktop وكمان في ال color depth

وفي عندي option اسمه use all my monitors for the remote session :

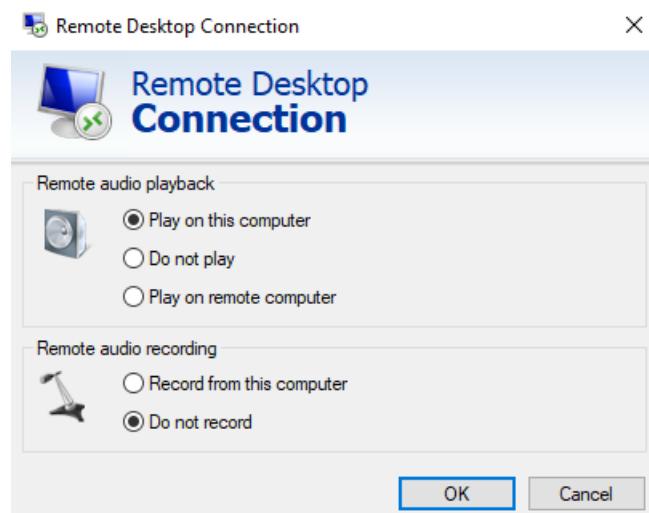
ودي عشان لو موصل اكتر من شاشه علي الالابتوب وعاوز ال session بتاع ال rdp دي تظهر علي كل الشاشات

ال last option ال اخير ال اسمه : Display the connection bar when I use the full screen :
لو لغيته ف مش هيظهر معليا ال bar الازرق دا :





ال Local resources setting هتلaci دی : ال audio روحت علي



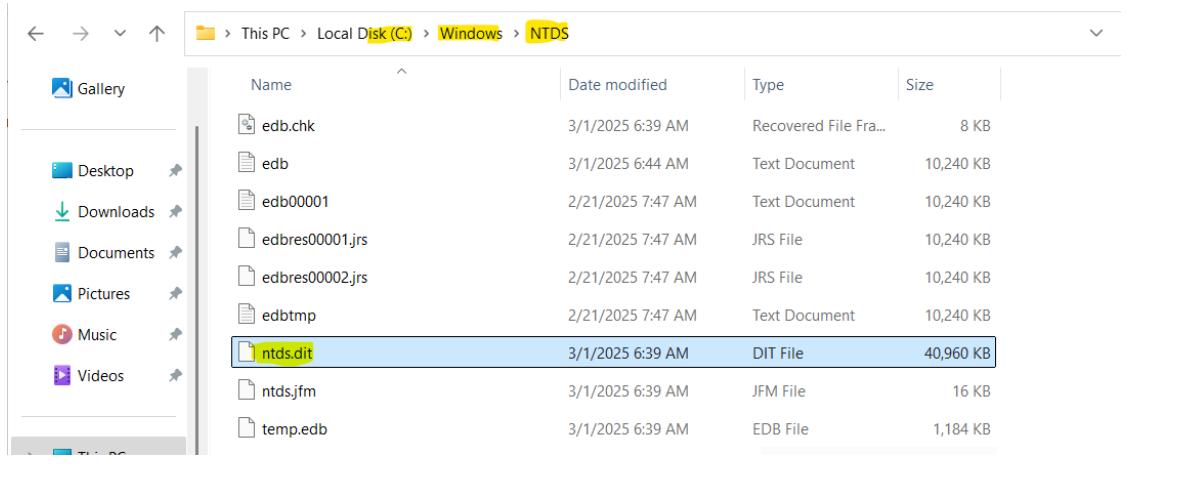
هنا لو فيه صوت شغال عندك

يشغله علي جهازك فقط – ميشغلهوش – يشغله علي ال remote computer

Active Directory Partitions

: NTDS دا خل ال active directory بالي ال هي ال Database

وال NTDS بتكون موجوده في ال path دا : C:\Windows\NTDS



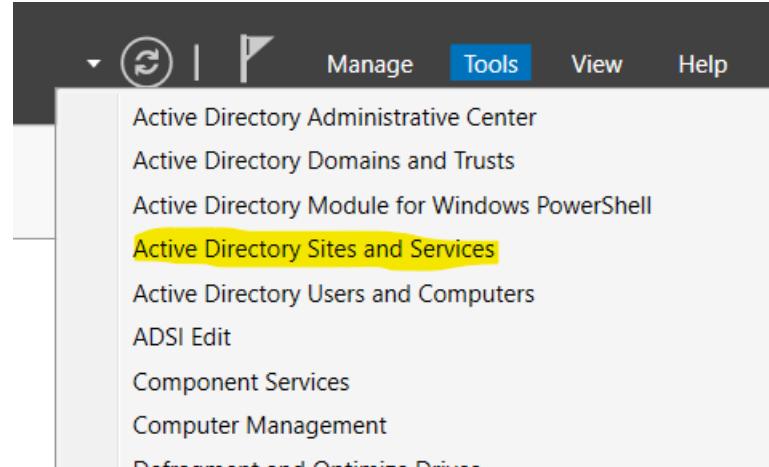
ودا ال بيتحزن فيه ال Domain partition -1
ال اقدر اعمل manage console من خلاله لـ AD users and computers

AD users and computers

The screenshot shows the Active Directory Users and Computers (ADUC) snap-in interface. The left pane displays the navigation tree for the domain PDC.techops.com, including containers like Saved Queries, techops.com, and various organizational units (OU)s such as BuiltIn, Computers, Domain Controllers, EG, hr, ForeignSecurityPrincipals, Keys, LostAndFound, Managed Service Accounts, Program Data, System, and Users. The right pane lists the users under the 'Users' container:

Name	Type	Description
mohamed	User	
mostafa mahmoud	User	

ودا بيعبر عن ال Configuration partition -2 في مكان ثاني وبالتالي ال console manage من خالله لل AD sites and services هو Configuration partition



من tools اختار AD Sites and Services

The screenshot shows the Active Directory Sites and Services management console. The left pane shows the navigation tree under 'Active Directory Sites and Services [PDC.techops.com]'. The 'Sites' node is expanded, showing 'Inter-Site Transports', 'Subnets', 'Default-First-Site-Name' (which is also expanded to show 'Servers' and 'PDC'), and 'DNS Settings'. The right pane displays a table of site settings:

Name	Type	Description
DNS Settings	msDNS-Server...	
NTDS Settings	Domain Contro...	

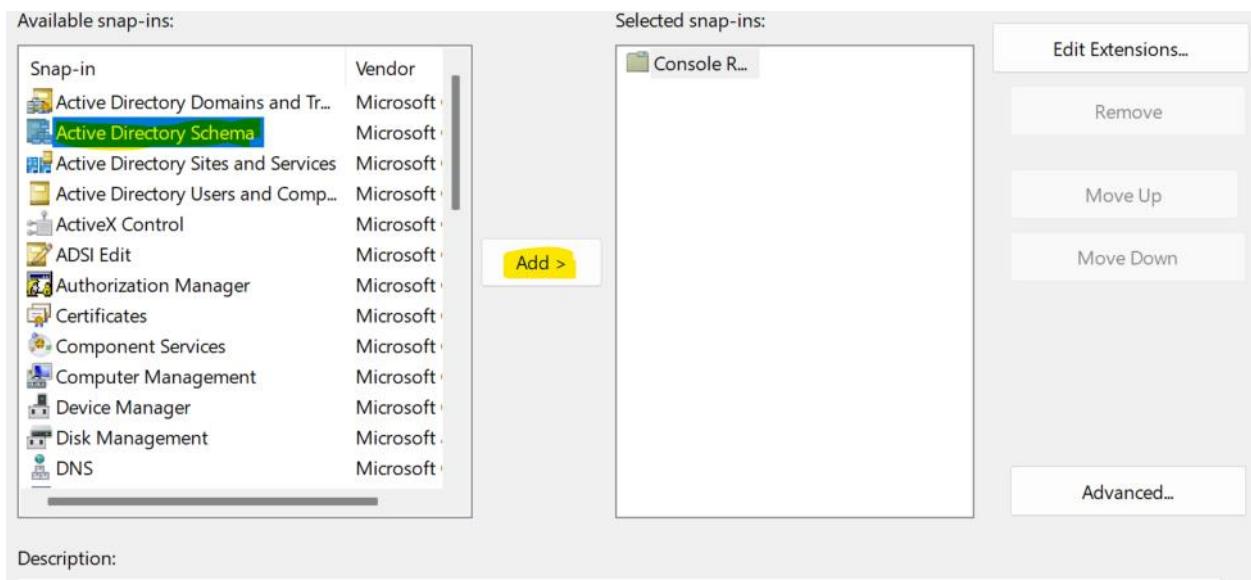
هلاقیه بالشكل دا اقدر بقا اضيف site تاني يكون فيه ال ADC ودا لو عندي اكتر من فرع مثلا

ودا بيعبر عن ال Design الخاص بال AD يعني مثلاً تعریقات ال Schema partition -3 وال console الخاصه بال AD وال Attributes objects لل Snap-in هو ال schema console لازم اضيف ال schema الخاص بال

طيب ازاي اعمل كدا ؟

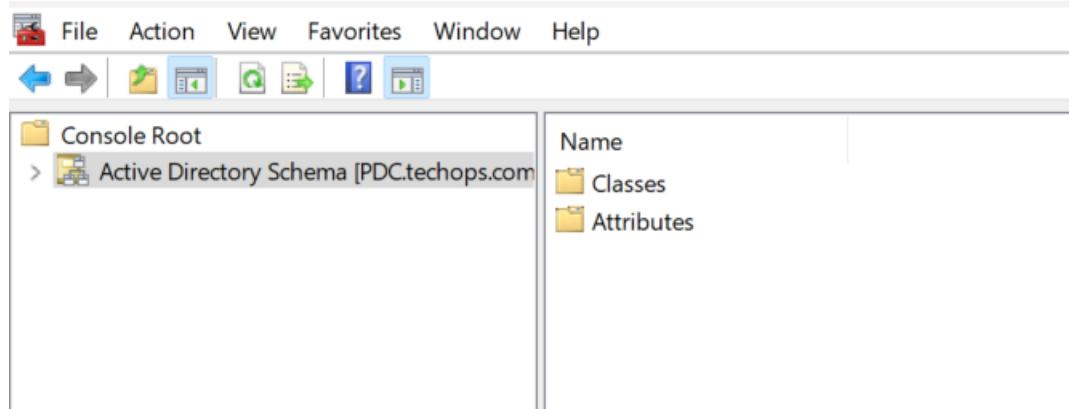


هتفتح ال Snap-in وتكلب ال command دا عشان تضيف ال



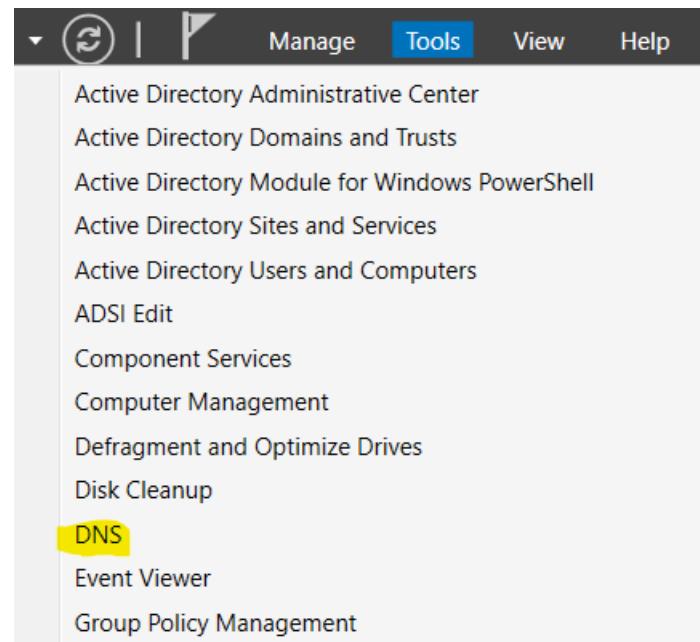
عمل Add لـ AD Schema

--



كدا تم اضافتها وتقدر تعدل ال object مثلا بتاع Attributes معين

يسخدمه التطبيقات والخدمات التي تحتاج إلى تخزين البيانات بشكل Application partition -4
موزع عبر الـ AD ولكن دون تكرارها إلى كل Domain Controller وأشهرهم ال DNS
يعني ال DNS لازم يكون على ال PDC لكن مش لازم يكون نازل على ال ADC
وال Console ليها DNS



من tools هختار ال DNS

The screenshot shows the Windows DNS Manager interface. On the left, the navigation pane displays the following tree structure:

- DNS
- PDC
 - Forward Lookup Zones
 - _msdcs.techops.com
 - techops.com
 - _msdcs
 - _sites
 - _tcp
 - _udp
 - DomainDnsZones
 - ForestDnsZones
 - Reverse Lookup Zones
 - Trust Points
 - Conditional Forwarders

The 'techops.com' node is selected, indicated by a blue border. On the right, the details pane shows a table of records for the zone:

Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[48], pdc.techops.com, host...	static
(same as parent folder)	Name Server (NS)	pdc.techops.com.	static
(same as parent folder)	Host (A)	192.168.1.35	2/22/2025
DESKTOP-L8SP6I0	Host (A)	192.168.1.6	2/22/2025
pdc	Host (A)	192.168.1.35	static

ب يكون الشكل دا

Additional Domain Controller

طيب ليه ممكن استخدم ال ADC ؟

1- اول حاجه بيتحققلي ال High Availability : في حاله ان ال PDC كان فيه عطل وتوقف عن العمل ، ال ADC بيستمر في تقديم خدمات زي ال Authentication وال Authorization دون انقطاع ودا بيقل من حدوث ال single point of failure في ال network

2- لو عندي عدد users كتير اقدر اوزع عمليات ال Authentication علي ال Loas Balancing ADC وال PDC

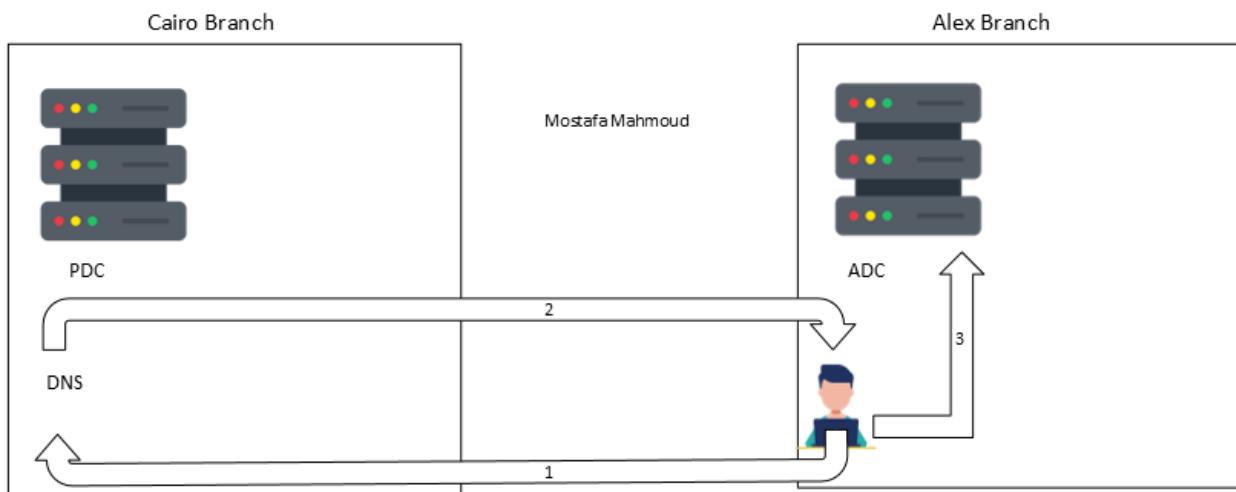
3- Disaster Recovery : في حاله حدوث عطل او فقدان لبيانات علي ال PDC يمكن لل ADC استعاده البيانات وضمان استمراريه العمل دون الحاجه الي اعاده بناء ال AD من البداية

4- Branch Office Support : لو عندي اكتر من فرع في اماكن متفرقه ف لو عملت ADC في كل فرع ف دا بيقل زمن الوصول الي ال Domain services وبالتالي الدنيا هتكون اسرع

5- Replication : المزامنه للتغيرات علي جميع ال DCs زي ال PDC وال ADC وبالتالي البيانات ال ه تكون علي الاتنين واحده ودا بيحافظ علي تناقض البيانات

6- طيب سوال : هل لازم اعمل Install لل DNS علي ال ADC ؟

تعال نفهم ال Auth بيتم ازاي وبعدين نجاوب



ال user موجود في alex branch هبروح لل DNS الخاص بال PDC وال PDC موجود في
ال Cairo branch وهي ساله انا هعمل auth من ال PDC ولا ال ADC فمثلا هبيقوله من ال ADC ، لكن
هنا المشكله ان ال user مازال بيروح يكلم ال DNS الخاص بال PDC

فالافضل انك تسطب ال DNS على ال ADC في حاله ان الاثنين في اماكن مختلفه طيب اي ال هستفاده
من ان اسطب ال DNS على ال ADC ؟

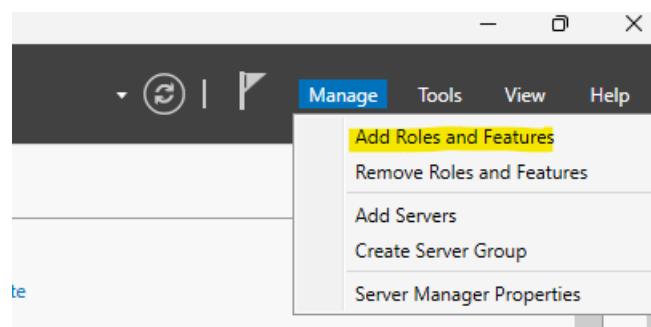
وهي تقليل زمن الوصول Latency Reduction

لو ال connection بين الفرعين انقطع ال users في
ال Alex يقدروا يستخدموا ال domain services وعمليات ال auth لكن لو مفيش DNS في
ال users مش هتقدر تعمل login

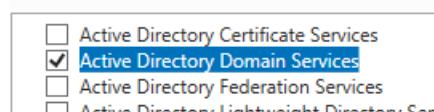
لو معنديش WAN Optimization Query على
ال DNS الموجود في cairo هتسنهلك ال Bandwidth ال بين الفروع

طيب از اي ابدا اعمل ال ADC ؟

اي account في ال SAM يعني على ال local Server ال هيتتحول ل ADC هيتخذ

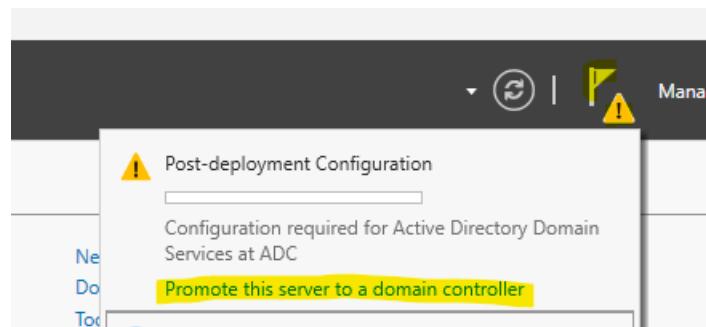


من manage على هروح Add Roles and Features

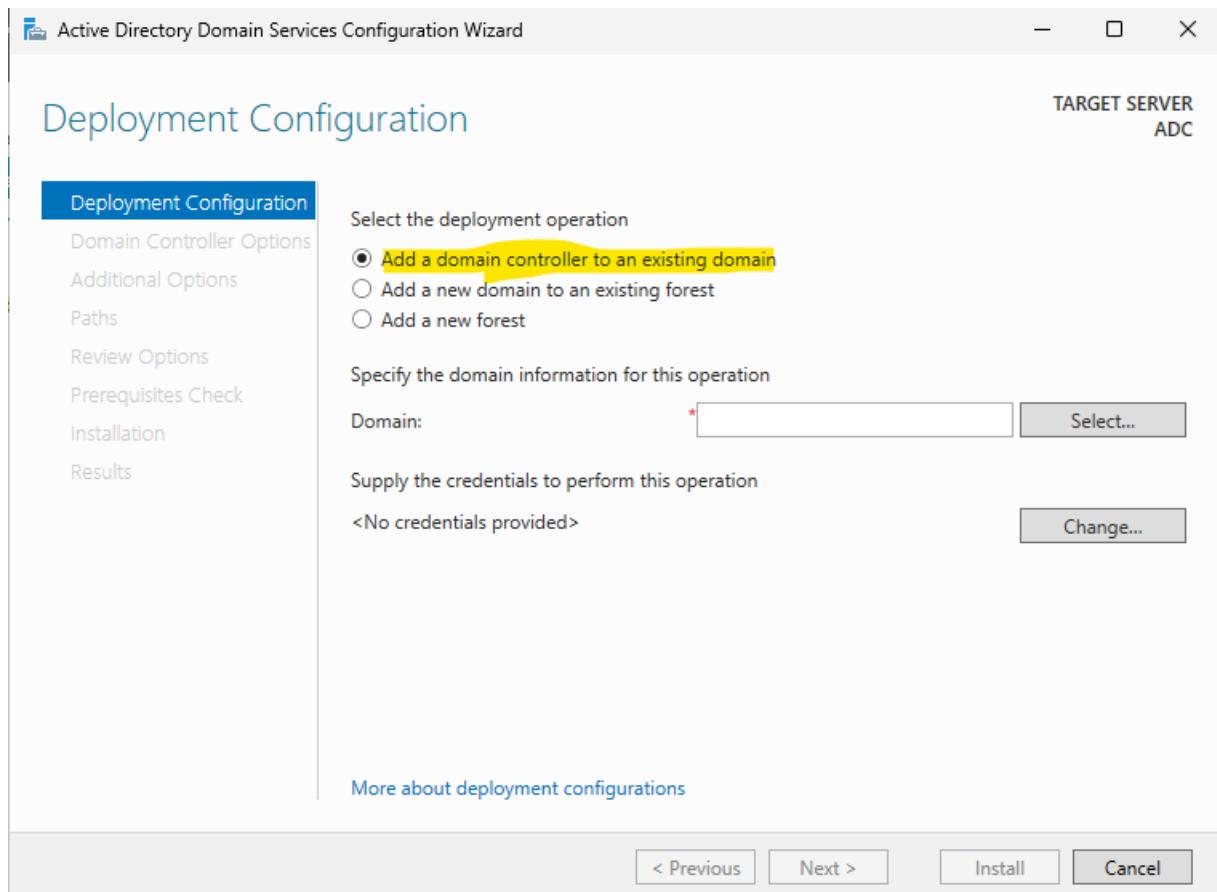


هختار ال Active directory Domain Services

بعد ال config install هبذا ال : config

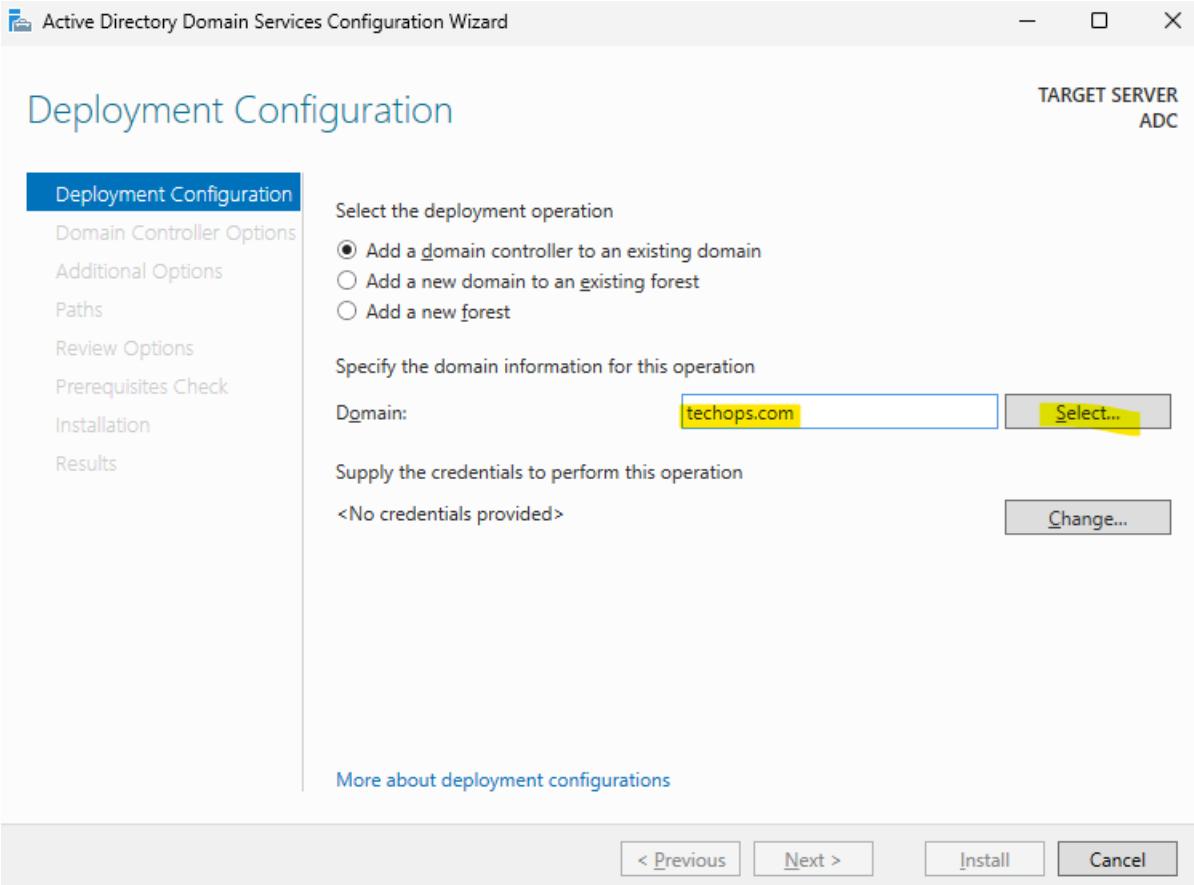


هفتح ال config console بال الخاص config



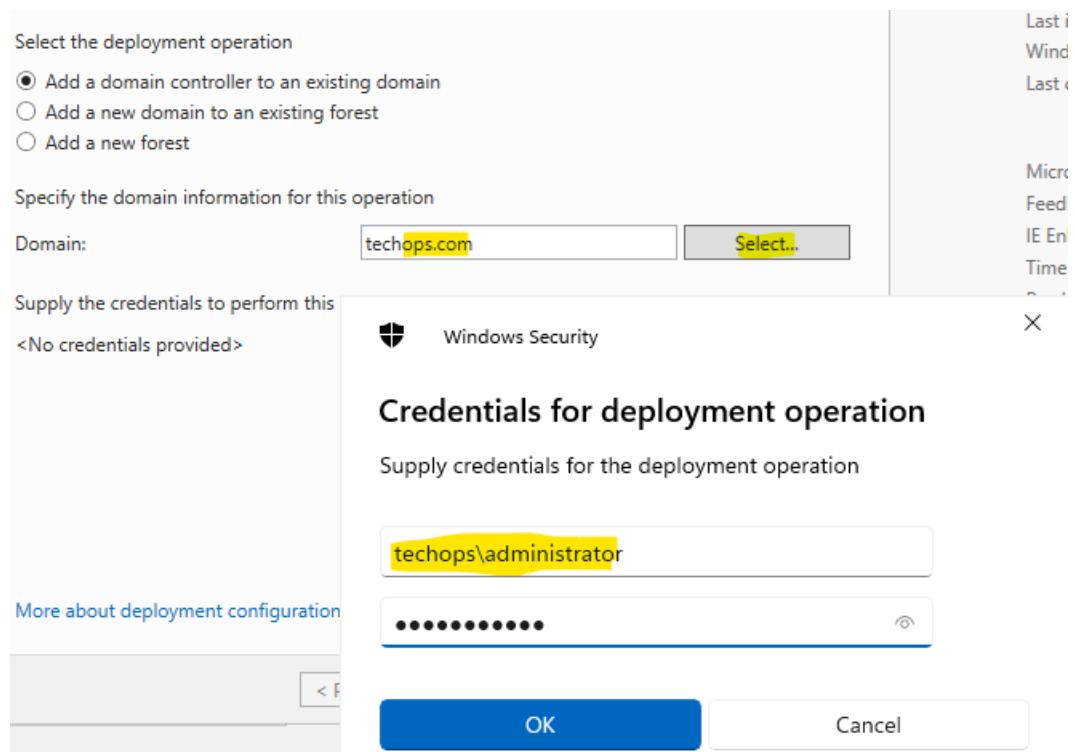
هختار اول اختيار ودا هنا بقولهاني عاوز اضيف Domain Controller في ال domain بتاعي ودا يقصد بيه ال ADC

--



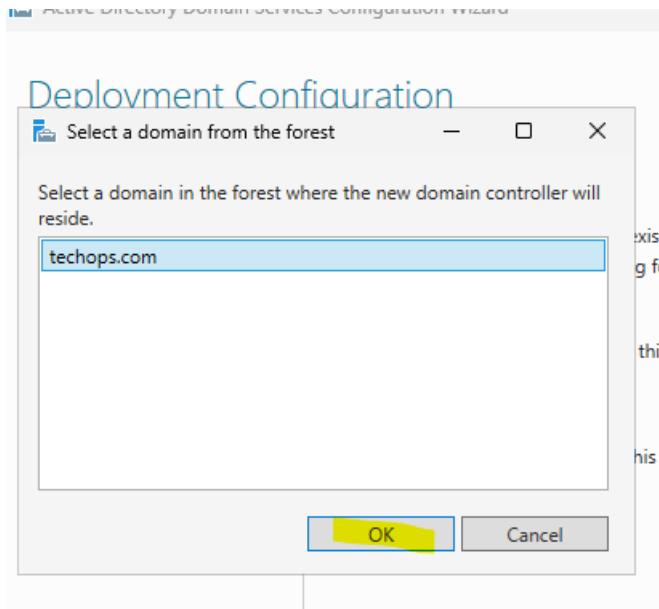
هڪتب اسم ال domain بتاعي ، ولازم طبعاً ابقي مرتبط ال ip وال dns على السيرفر دا

--

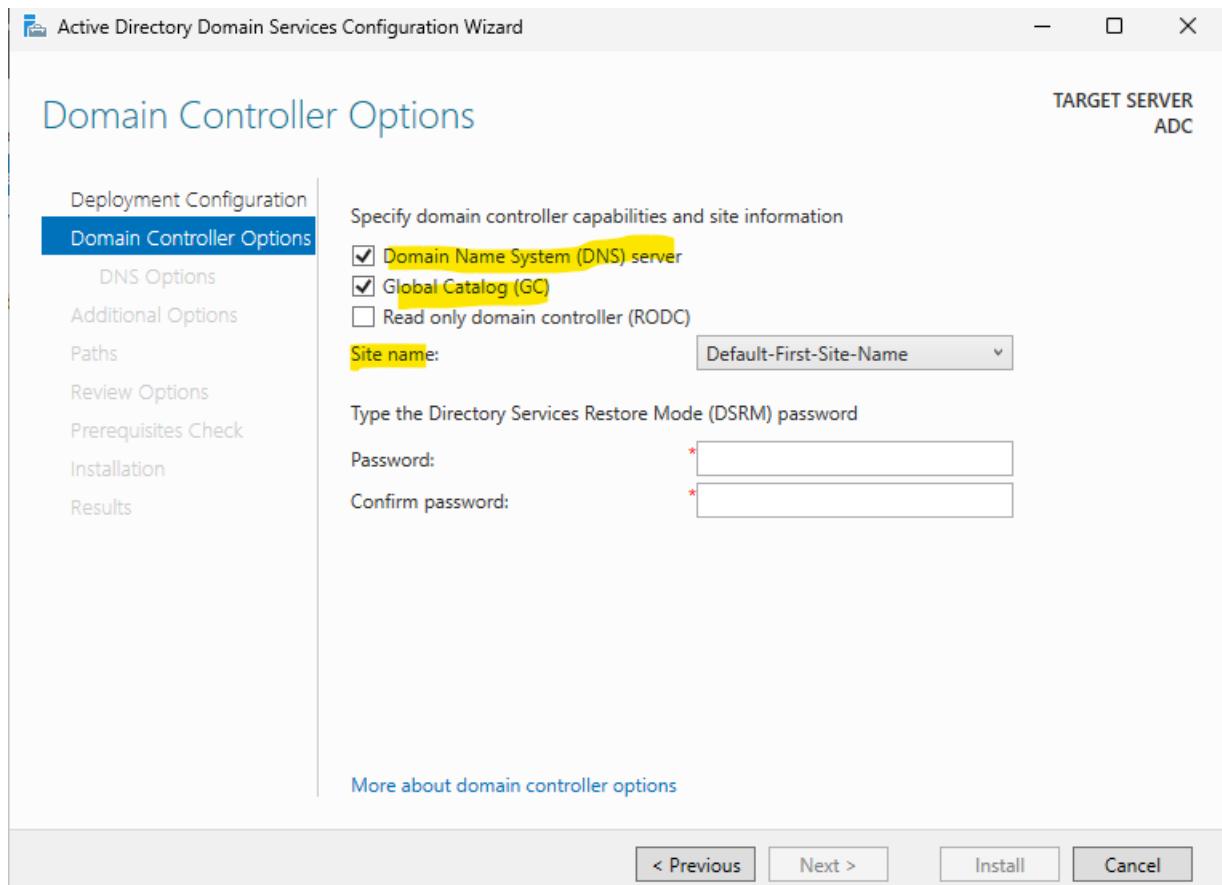


بعد لما اضغط select بيكولي اكتب ال user وال password

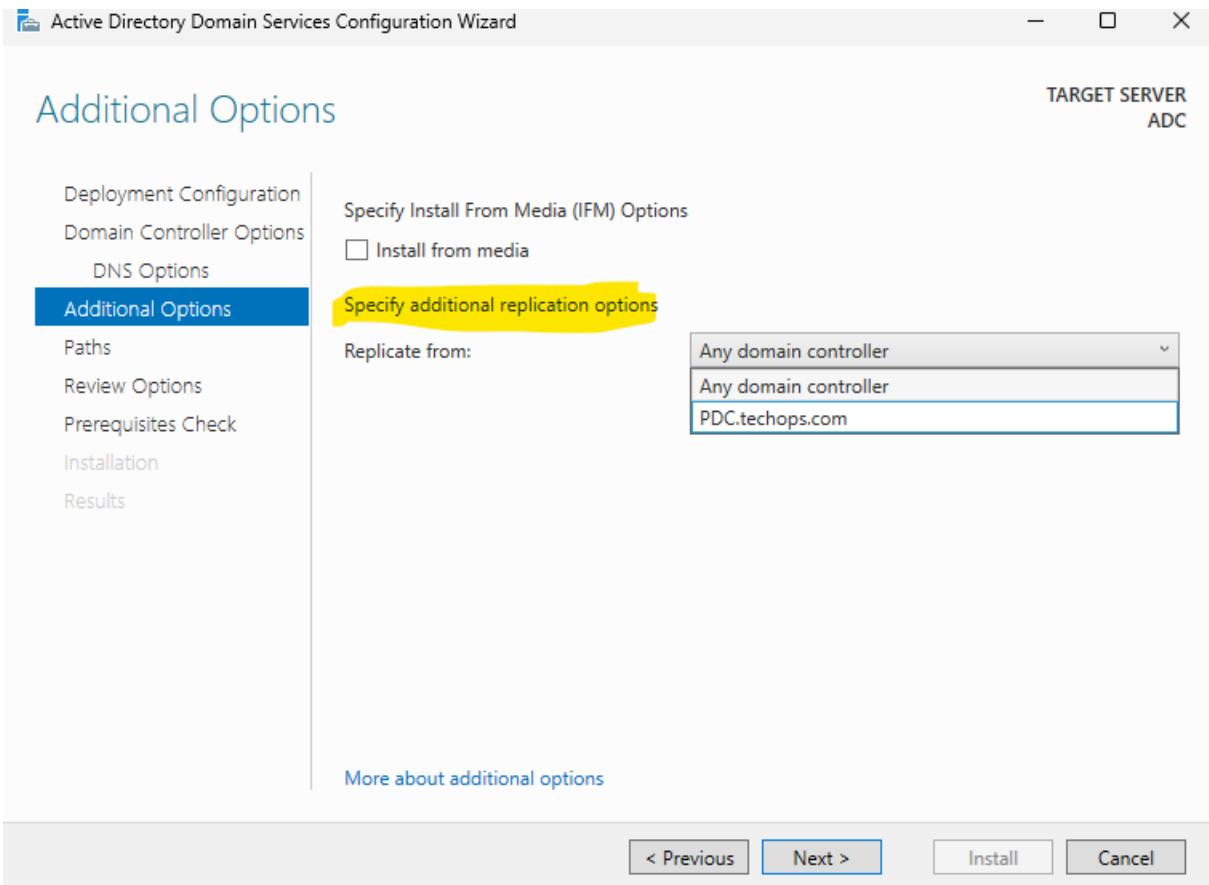
ال يقدر يعمل ADC هو ال Domain Admin



هلاقیه ظهر معايا فهختاره واضغط ok

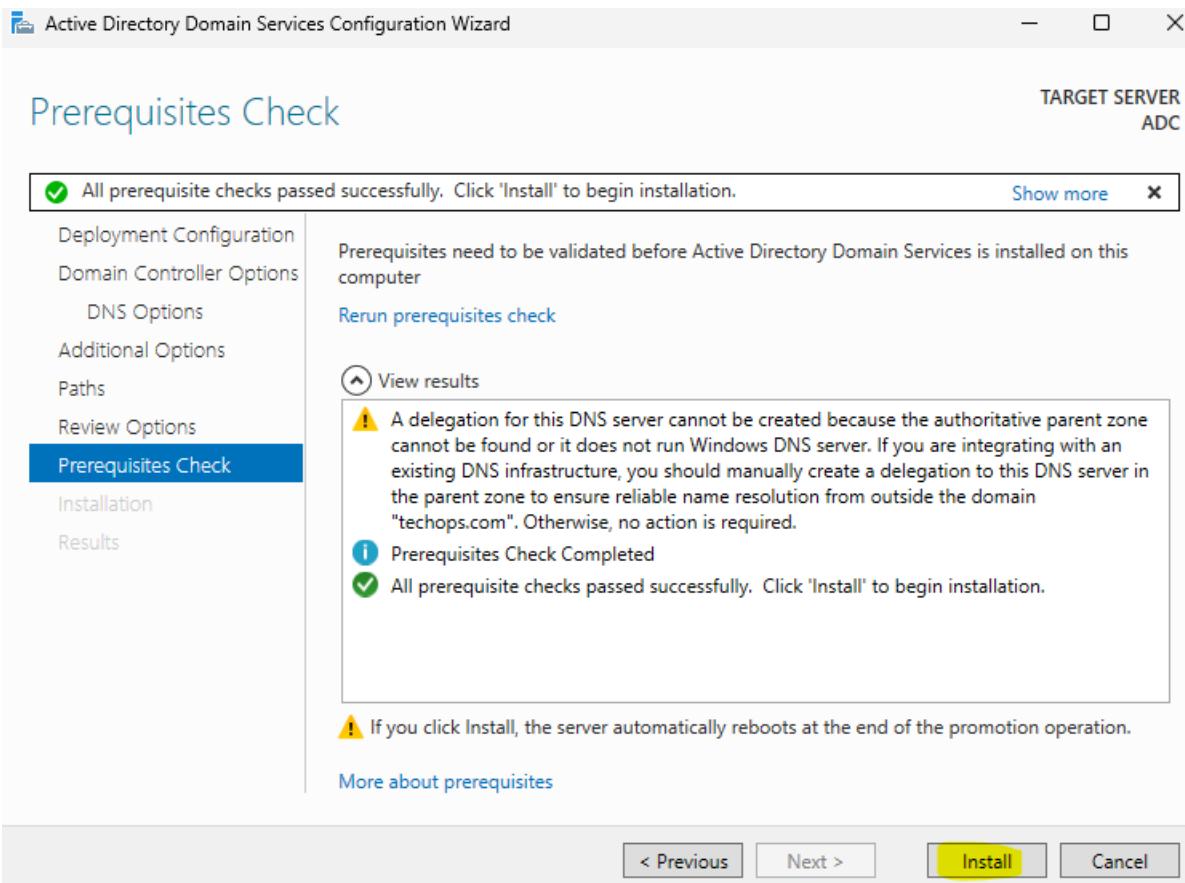


بختار اذا كنت تحتاج اسطب ال DNS ولا لا
وان ال server دا هيكون ك GC ولا لا
وبختار ال Site ال هيكون فيه ال ADC
وبعمل password لـ DSRM



هنا بيسالني ال Replication هيتمن انهي DC

--



بعد كدا لو الدنيا تمام هعمل ال **Install**

Operation Master Roles

في عدي 5 role

Domain naming master role -1

Schema master role -2

PDC emulator -3

RID -4

Infrastructure -5

ال Domain naming master role : دول server واحد فقط على مستوى ال schema .
ال forest يقوم بالوظيفتين دول

ال RID و PDC و Infrastructure : دول server واحد على مستوى ال Domain المسئول عن كل وظيفة
من دول



By default : ال 5 role سيكونوا على اول server في ال forest وهو ال PDC

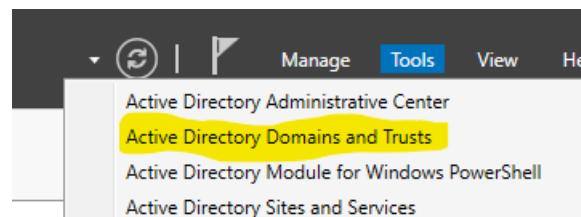
: Domain naming master role -1

مسؤال عن :

- forest داخل ال Domain naming
- domain name تكرار ال

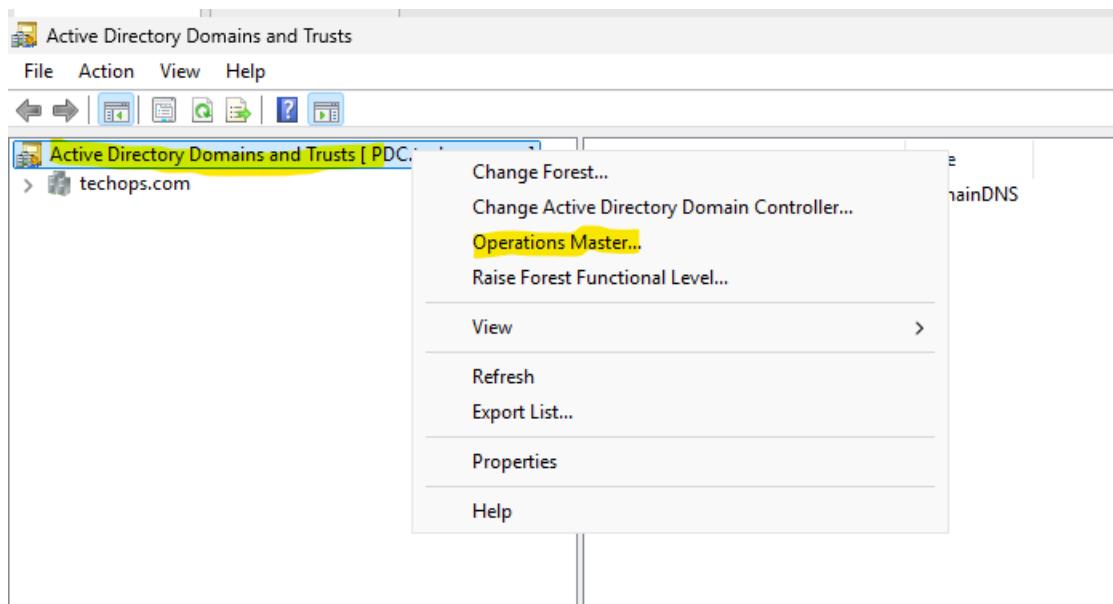
هل الوظيفه دي لو وقعت الدنيا هتفق ؟ لا ، هفضل شغال عادي لكن مش هتقدر تضيف DC غير لما
الخدمه دي ترجع

ودا زي م قولنا DC واحد فقط لكل Forest ال يلعب الوظيفه دي
طيب لو عاوز اعرف اين خاص بالوظيفه دي :

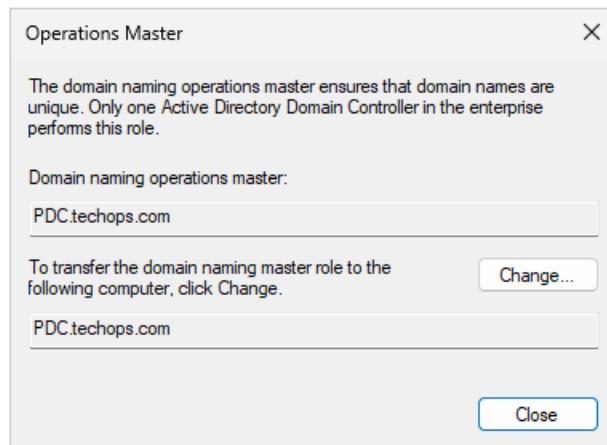


من tools هختار AD Domain and Trusts

--



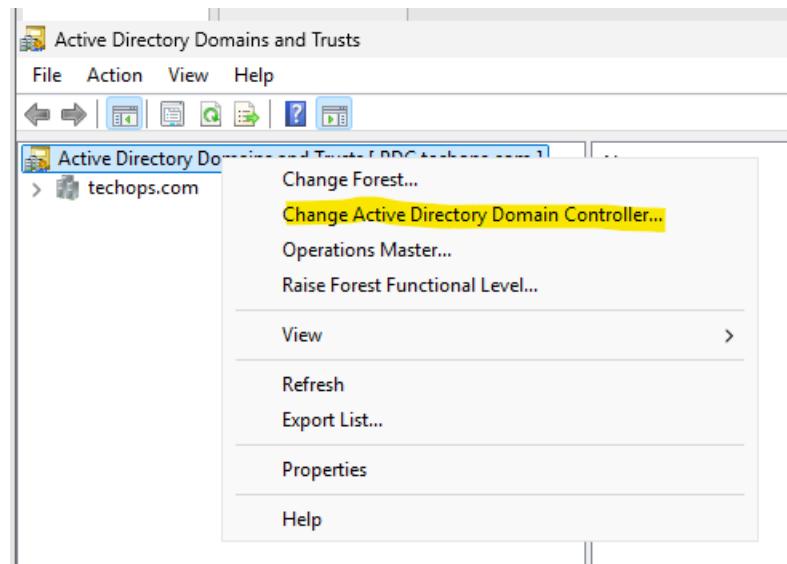
بعد کدا هختار Operation Master



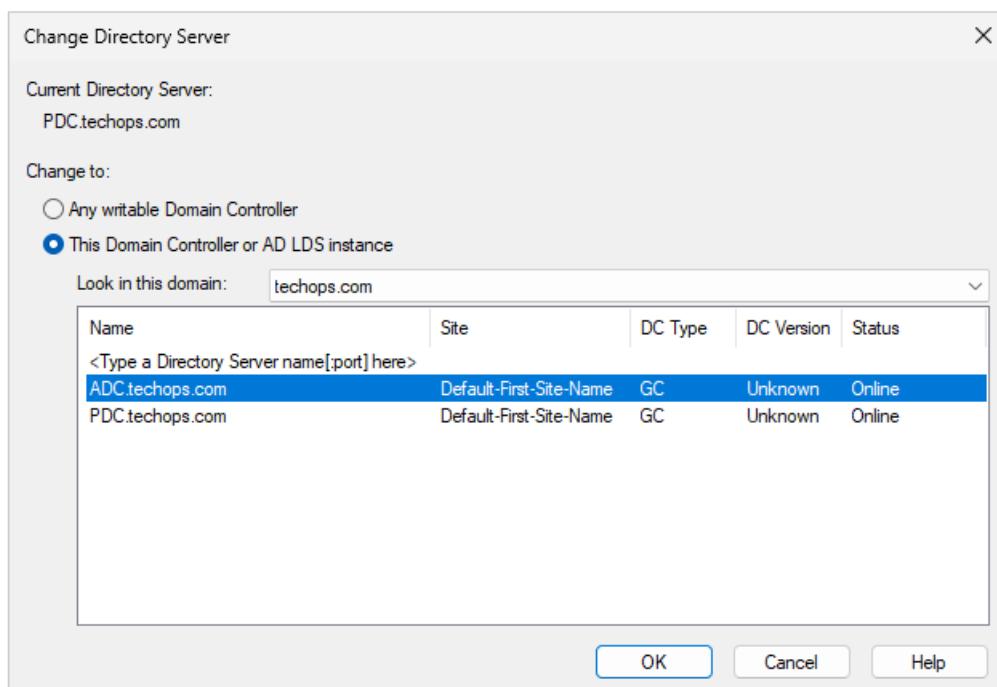
هلاقې ان ال PDC هو ال بیقوم بالوظیفه دي

--
طیب لو عاوز اغیره لل ADC ؟

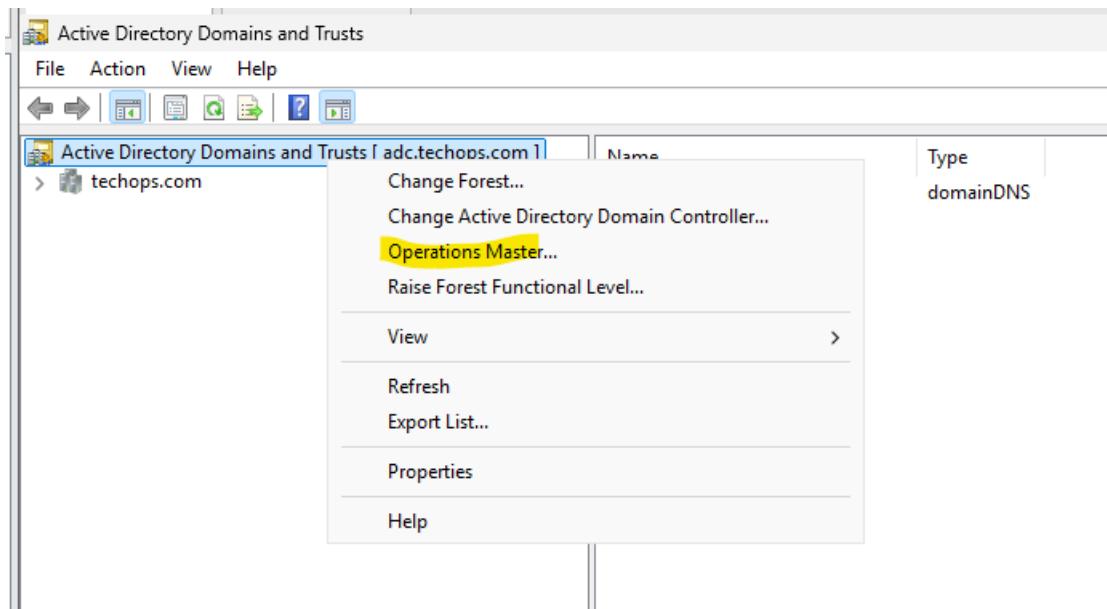
: نفس ال console



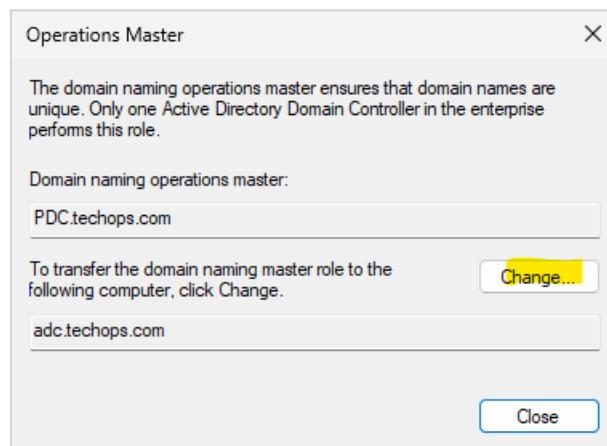
هختار change AD DC



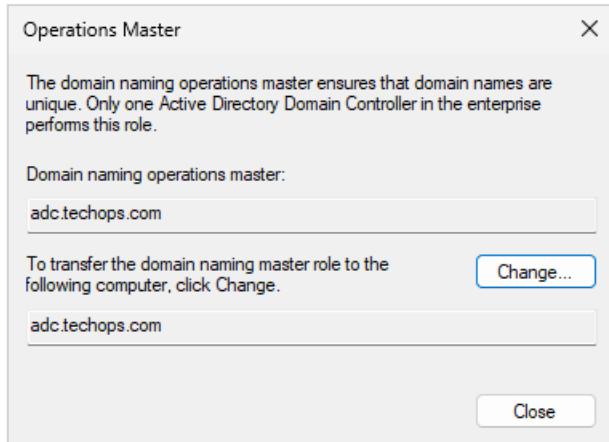
هختار ال ADC ، ف كانى حاليا بيص ع سيرفر ال ADC



هروح على ال operation master



وهي عمل change



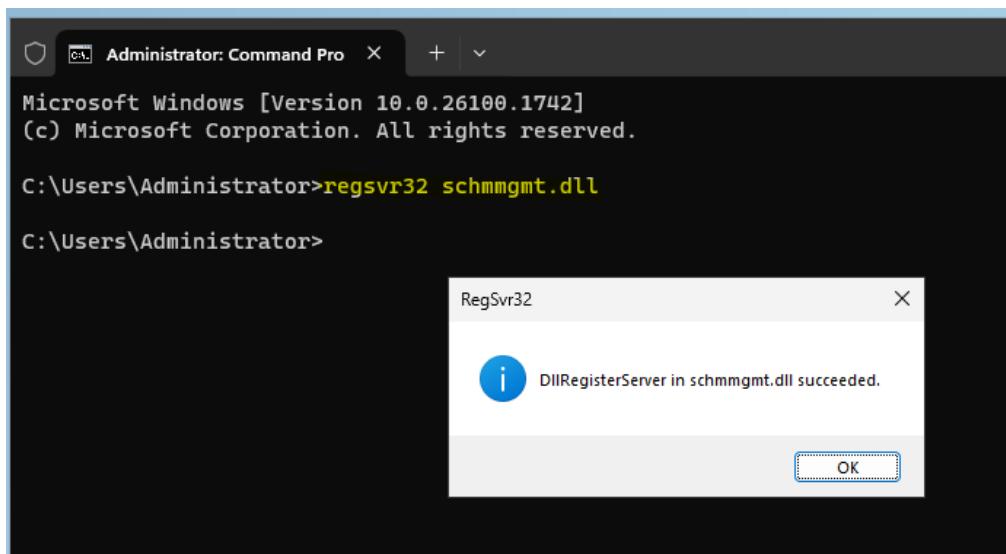
فهناشي اتغير لـ ADC

: Schema Master -2

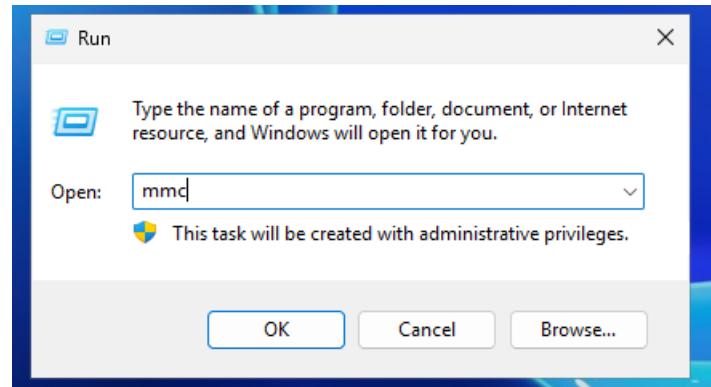
- بيتحكم في كل التعديلات على Active Directory schema يعني مثلاً لوعاوز اضيف attitude جديد ل object معين واتحكم في كل ال objects بتابع كل ال objects من خلال ال schema master

ودا زي م قولنا DC واحد فقط لكل Forest ال يلعب الوظيفه دي

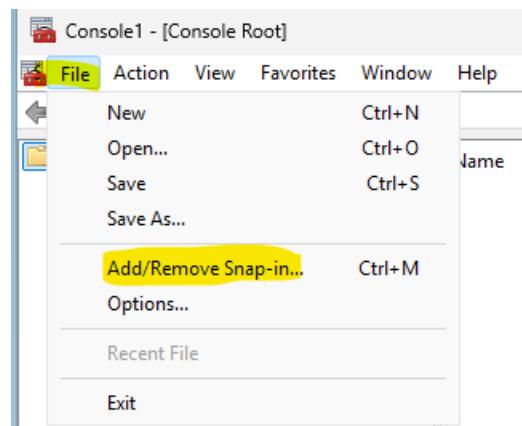
طيب ازاي اعرف اي server بيقوم بوظيفه ال schema



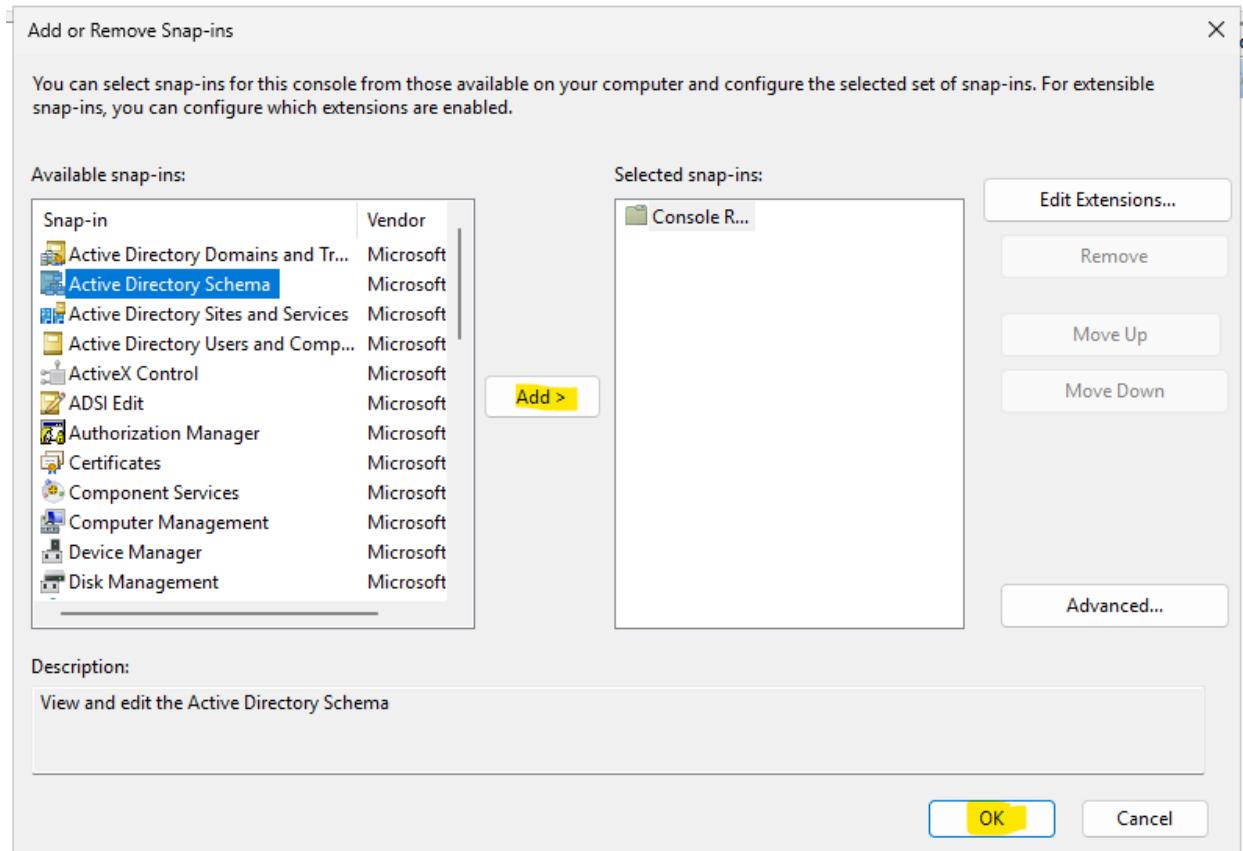
اول حاجه هنفعل ال console من خلال ال command دا في ال cmd



هفتاح ال mmc

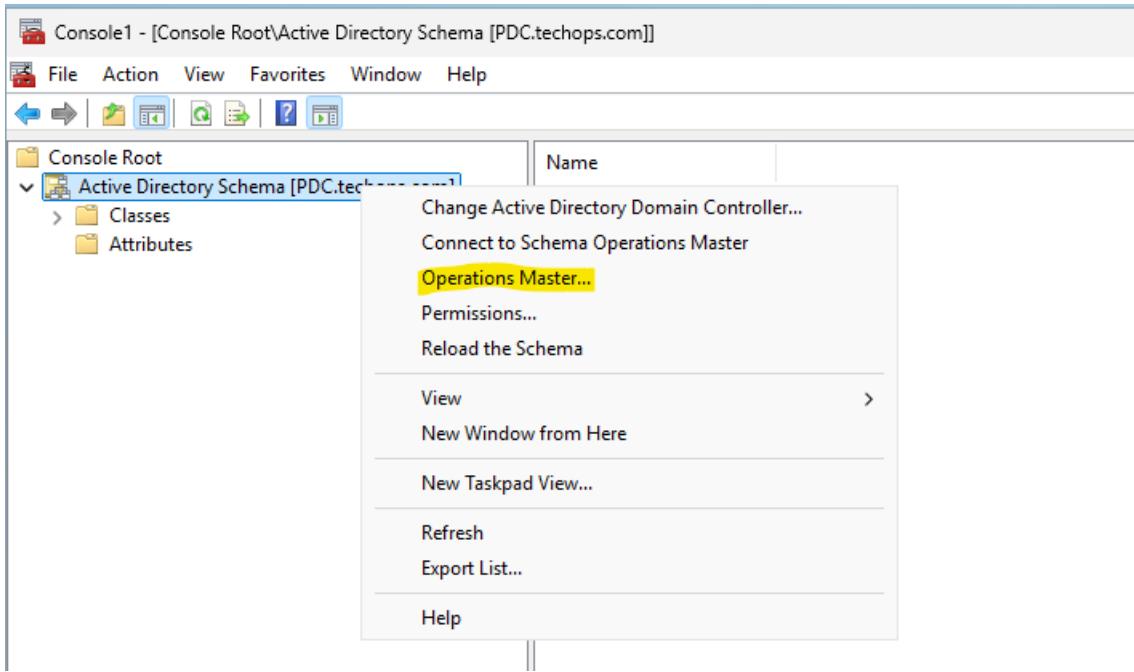


من file هنختار Add/remove Snap-in

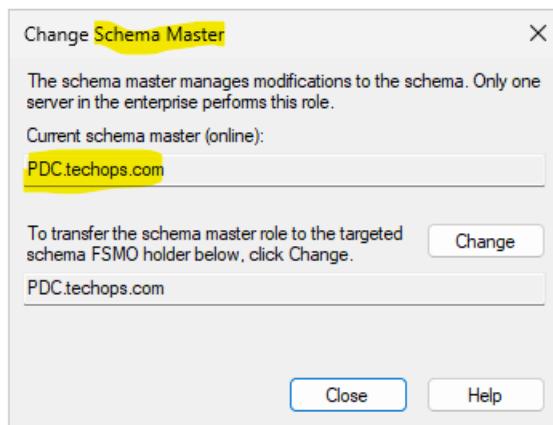


هتمل Add لـ AD Schema واضغط OK

--

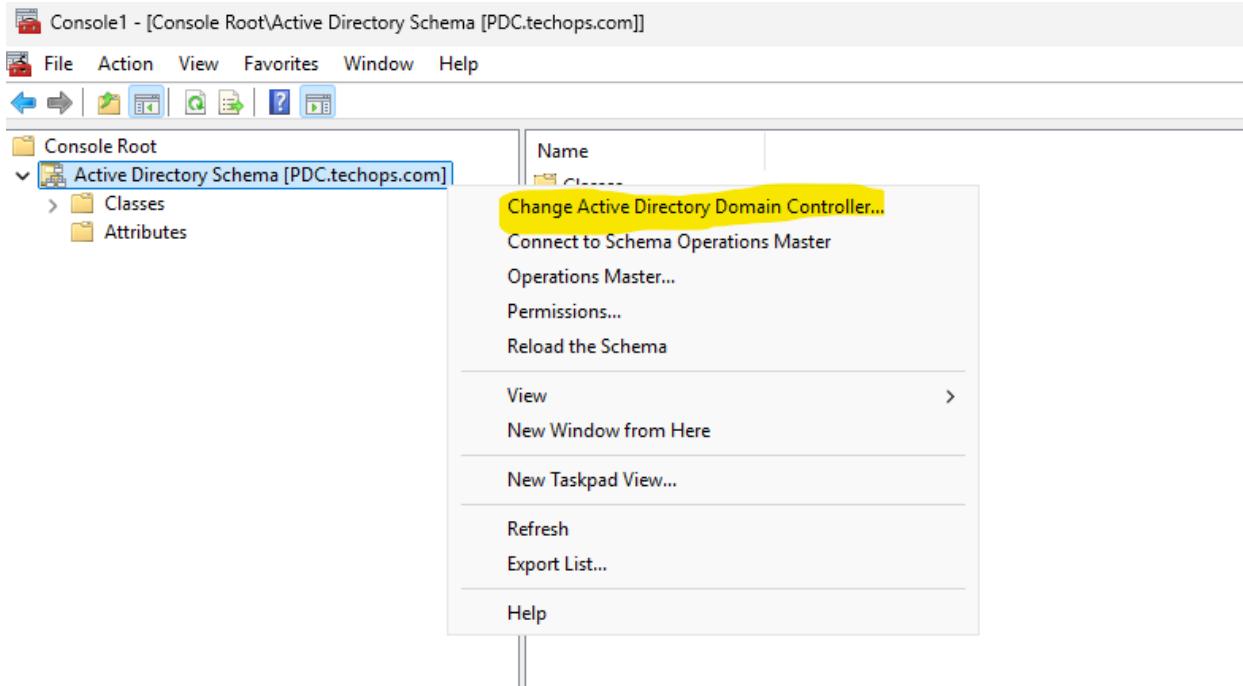


ومنها نختار Operations master

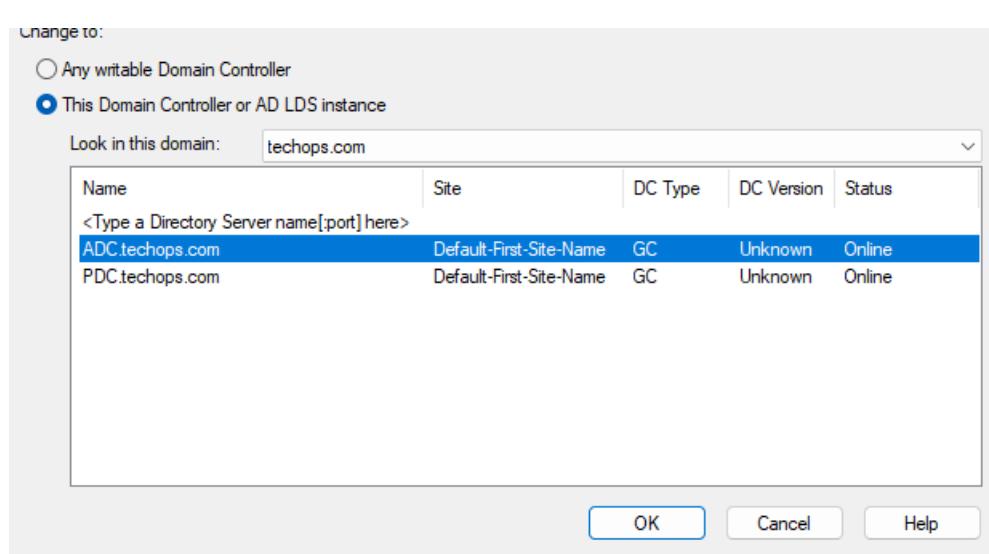


هناقي ان ال PDC هو ال يقوم ب وظيفه ال Schema

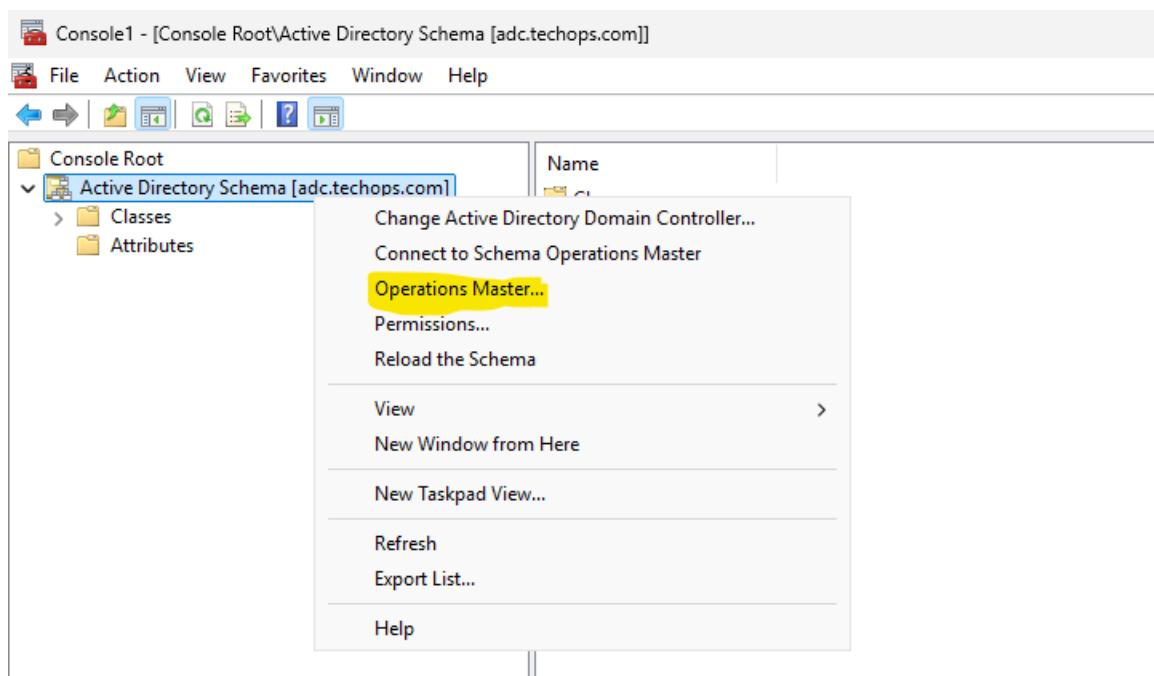
طيب ازاي اغير الوظيفه دي لـ ADC ؟



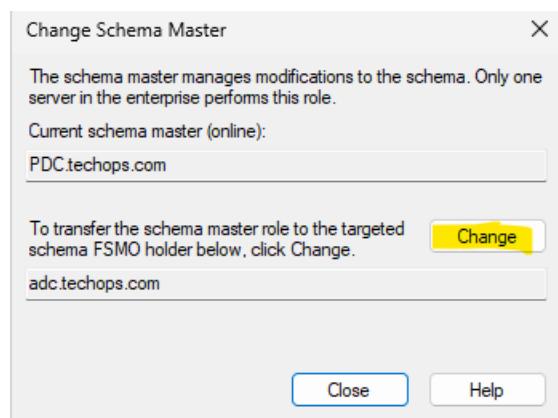
من نفس ال change ADDC هختار console



هختار ال ADC



بعد كذا هختار Operations Master



بعد كذا هعمل Change

Primary Domain Controller : اختصار ل PDC Emulator – 3

مسئوال عن :

- ال passwords ومعالجتها داخل ال domain بمعنى اذا قام المستخدم بتغيير ال password الخاصه بها ف ال PDC هو المسؤول عن تحديثها فورا
- ال Conflicts : بمعنى اذا تم انشاء او تعديل حسابات بنفس المعلومات علي اكثر من DCs ف ال PDC هو ال هيفصل في حل ال Conflicts دي
- Time Synchronization : جميع ال DCs في ال Domain يحصلون علي الوقت من ال PDC Emulator
- Group Policy Update : اي تحديث يتم اجراءه علي ال Group Policy يتم التعامل معه او لا عبر ال PDC Emulator قبل ان يتم نشره الي باقي ال DCs
- PDC Emulator يعمل داخل ال Domain Partition ، حيث يتم تحديث بيانات المستخدمين والمجموعات المتعلقة بكلمات المرور ، والسياسات الأمنية ، وعمليات التحقق من المصادقة

Relative Identifier : RID – 4

الوظيفه الاساسيه التي يقوم بيها هي ادارة تعيين ال Security Identifiers (SID) لل accounts داخلاً لل Domain objects

ال RID هو اخر جزء من ال SID وهو رقم فريد يتم تعيينه لكل object في ال AD مثل ال Users ف ال SID يتكون من جزأين رئيسيين :

جزء ثابت وهو ال Domain ID

وجزء متغير وهو ال RID

يعني مثلاً لو عندي SID بالشكل دا :

S-1-5-21-2143787207-2872493534-1719721540-1104

فان : Domain ID S-1-5-21-2143787207-2872493534-1719721540 هو ال RID

وال : 1104 ----> هو ال RID لهذا الحساب (ودا بيكون فريد لا يتكرر)

- هو المسؤول عن إدارة وتخصيص RIDs لكل Domain Controller داخلاً للدومنين ودا عشان ميحصلش اي تعارض في توزيع ال SID او ان 2DC يكون معاهم نفس ال SID

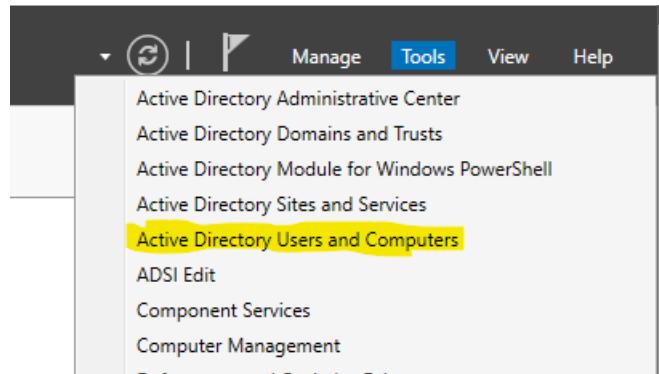
groups users ف ال Domain داخل ال Forest ف ال Infrastructure -5 وال computers تقدر تتفاعل مع بعض عبر ال Domains لكن المشكله هنا ان كل Domain له Database خاصه به

وهنا يجي دور ال Infrastructure Master Objects وهو انه بيضمن ان المعلومات الخاصه بال موجوده في ال Domains الاخرى تبقى محدثه عند استخدامها داخل ال Domain الحالي

- تحديث ال References : يعني مثلا لو تم تغيير اسم او حذف او نقل اي user object مثل user او domain في معين فال Infrastructure group يقوم بتحديث جميع ال DCs الاخرى في نفس ال Domains بالتغييرات دي حتى تبقى ال References صحيحه بين كل ال Domain

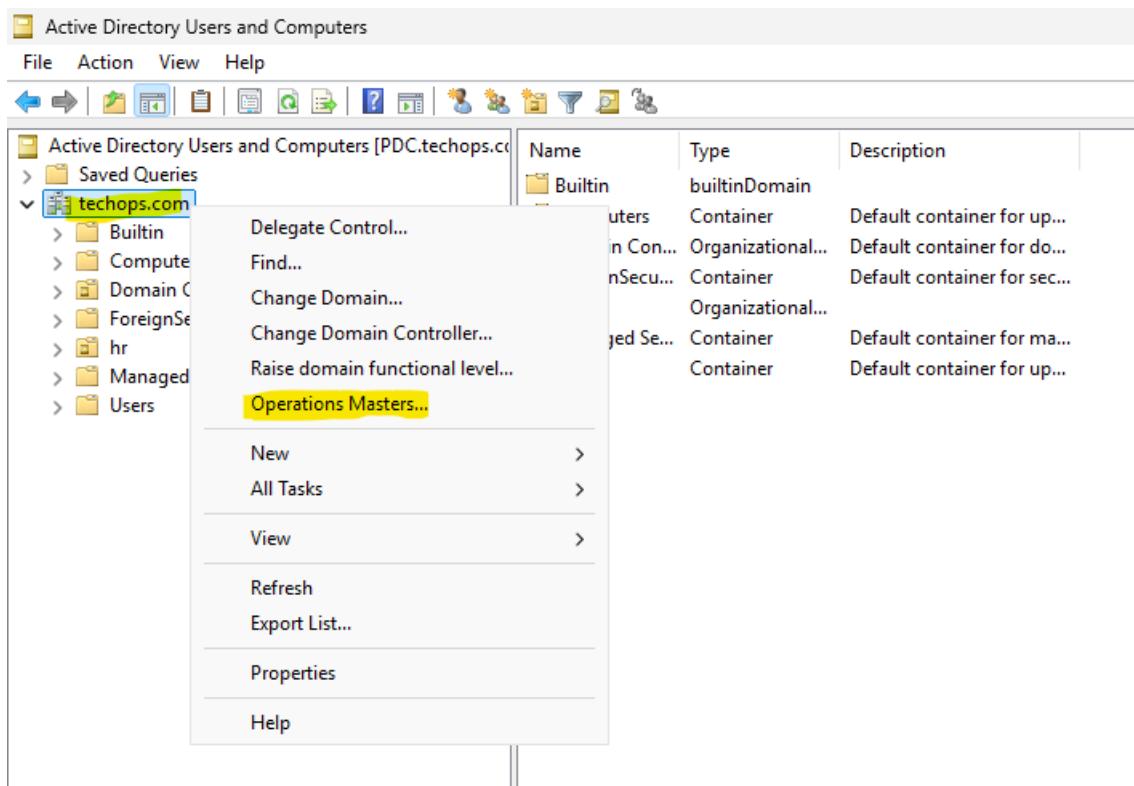
- اداره ال SID لـ users في ال Groups : بمعنى لو تم اضافه user من domain اخر لل domain الحالي ، فبيتم تخزين ال SID الخاص به داخل ال AD DB وبيكون ال مسؤوال عن تحديث ال SID دا لو حصله اي تغيير في ال Domain الاصلی

طيب عاوز اعرف مين ال server ال بيقوم بال 3 وظائف دول :

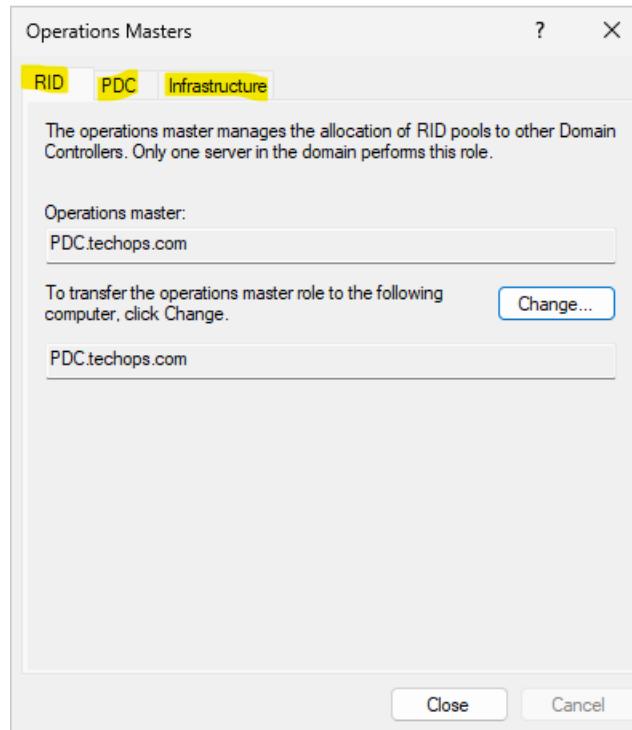


من ال Tools هفتح ال AD Users and Computers

--



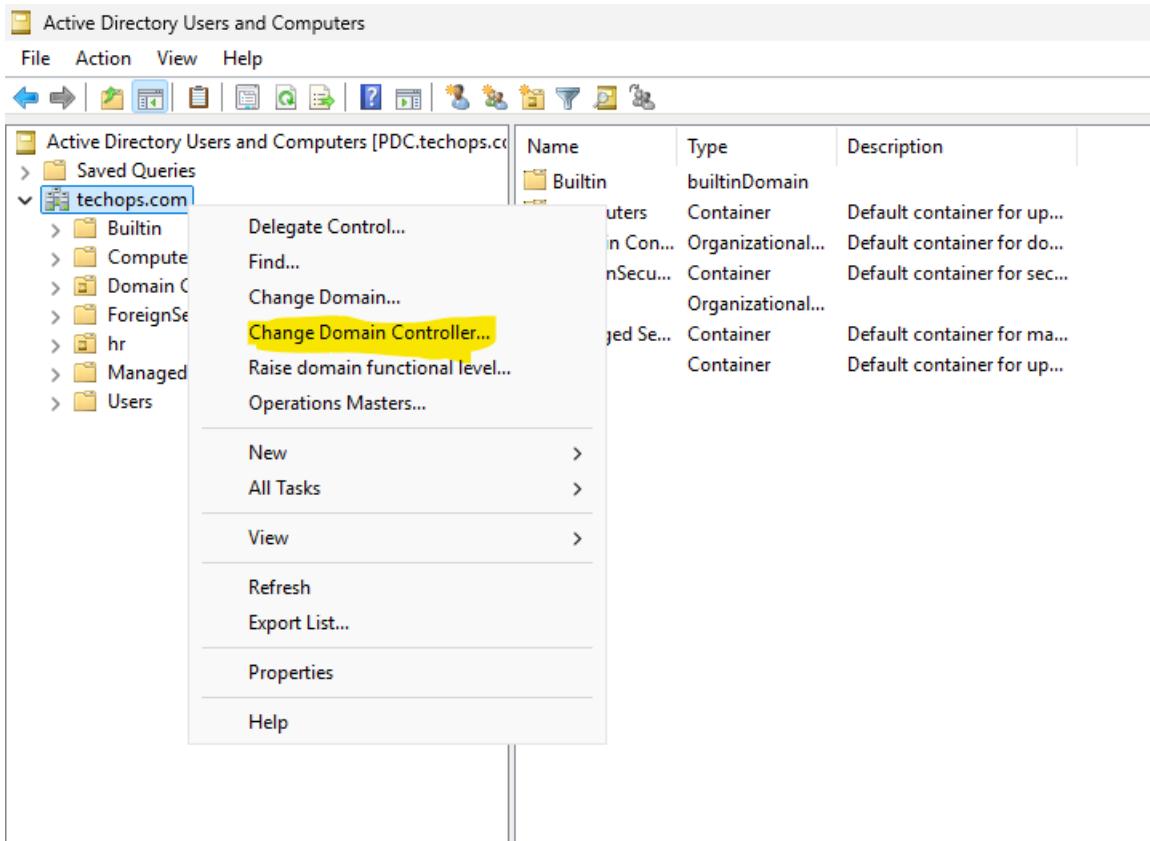
هروح على ال operations Master واختار Domain Name



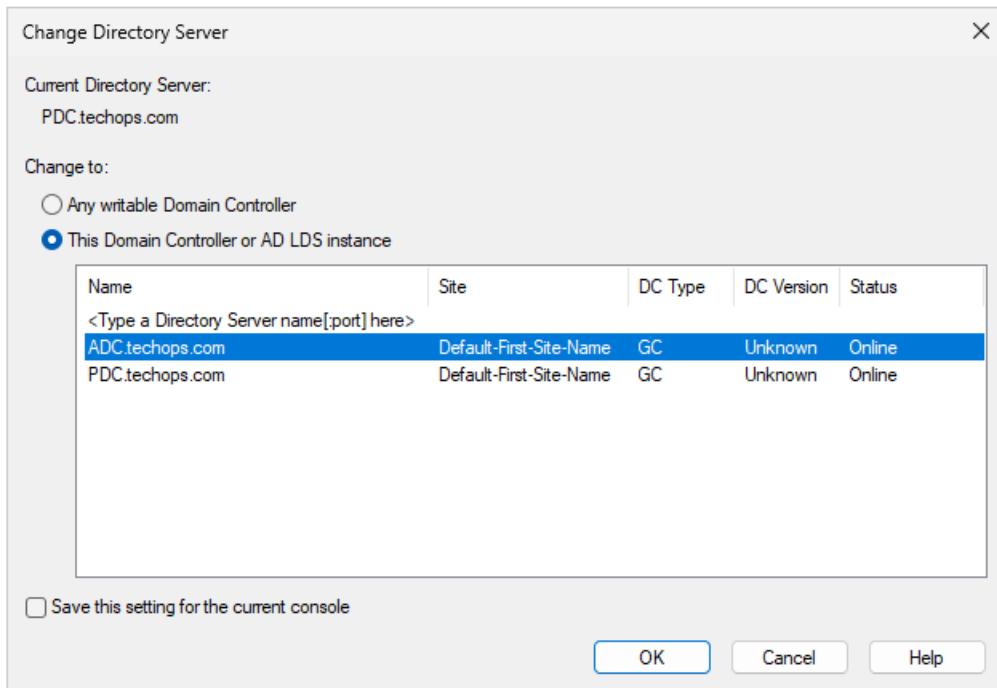
فهلاقي ال RID-PDC-Infrastructure واي ال server 3 ال بيقوم بالوظائف
بتاعتهم

طيب لو عاوز اغير ال server ال بيقوم بالوظيفه دي ؟

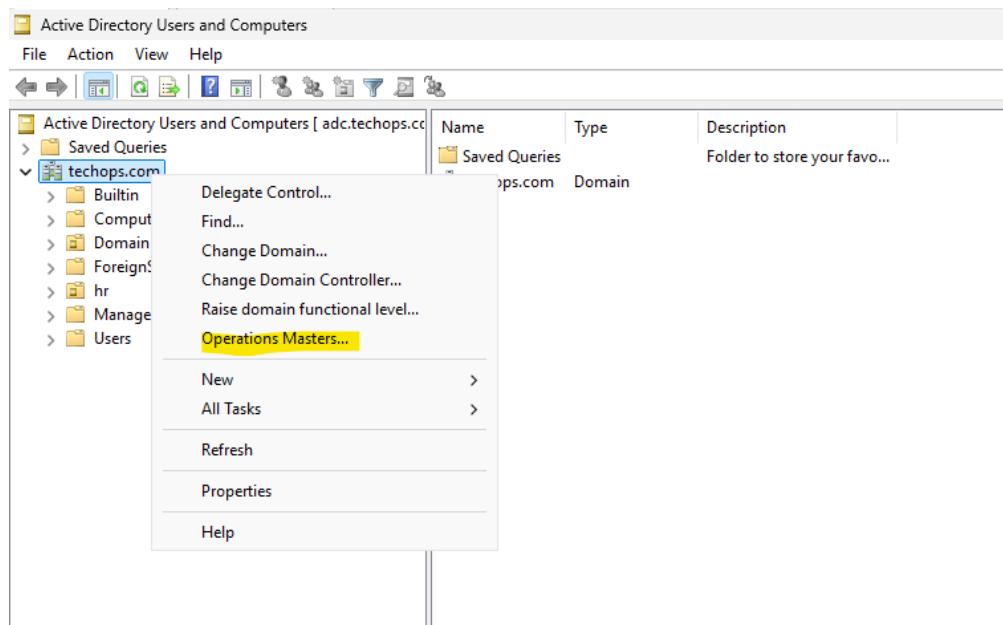
من نفس ال console ال هو ال AD Users and Computers



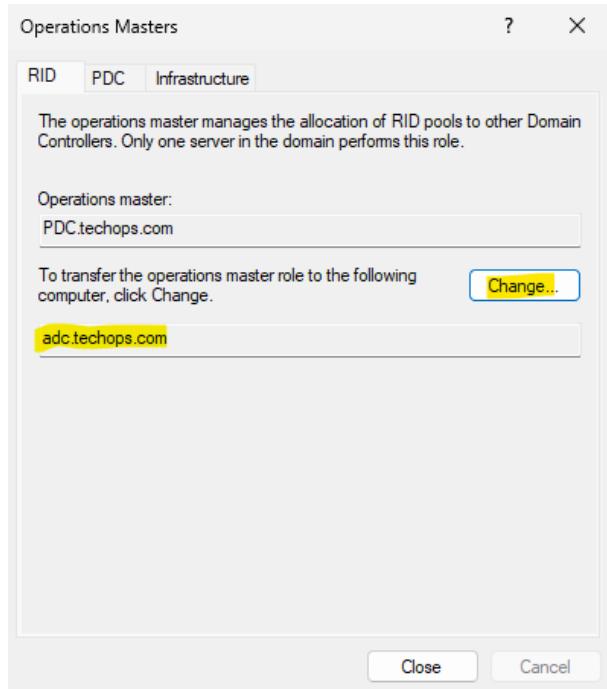
من ال هختار change DC Domain name



هختار ال ADC او السيرفر ال عاوز انقله ال Role لو عندي اكتر من ADC



بعد كدا من ال Domain name هختار Operation Masters



هتعمل change لل RID وبيكدا نقلت ال RID وخليت ال يقوم بالوظيفه دي هو ال ADC وليس ال Infrastructure مع ال PDC وال PDC وهكذا

--

طيب هل في طريقة اعرف بيهها اي ال servers ال بتقوم بالوظائف دي مره واحده؟
من ال cmd

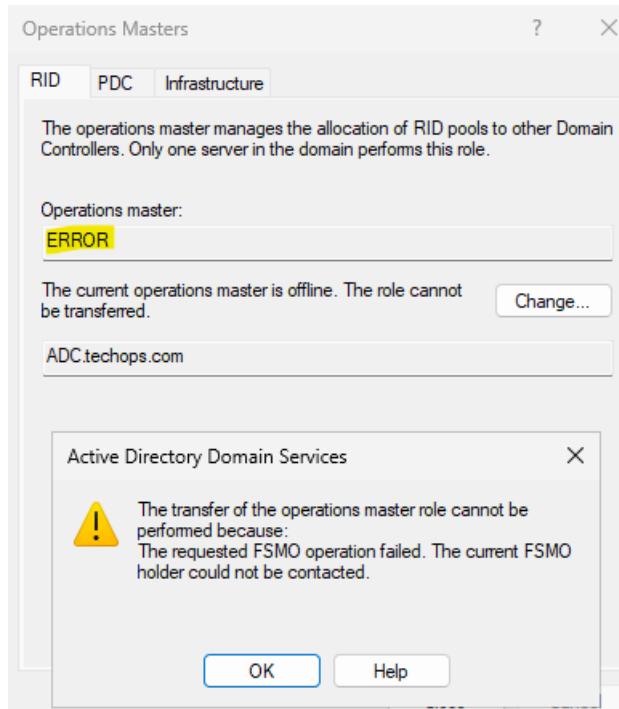
```
C:\Users\Administrator>netdom query fsmo
Schema master          PDC.techops.com
Domain naming master   PDC.techops.com
PDC                   PDC.techops.com
RID pool manager       PDC.techops.com
Infrastructure master  PDC.techops.com
The command completed successfully.
```

لو فتحنا ال cmd ك administrator وكتبنا ال netdom query fsmo command دا:
هناقيه بيعرض ال 5 role واي ال server ال بيقوم بالوظيفه دي وهنا ال PDC بيقوم بكل ال Role

احنا شوفنا لو عاوز انقل ال role من PDC بس ال ADC كان شغال ومهوش اي مشكله

طيب دلوقت ال PDC حصله اي مشكله ومبقاش شغال وبالتالي كل حاجه هنقف لانه هو ال بيقوم بال 5 role ف ازاي انقل ال Role دي لـ ADC عشان الدنيا ترجع تشتعل تاني ؟

مش هينفع بالطريقه ال كنا بنستخدمها وال PDC شغال ويعطيكي ال error دا



لانه مش قادر يوصل لـ PDC

فالحل هو ان هعمل Seize

طيب ازاي اعمل Seize

```
C:\Users\Administrator.TECHOPS>ntdsutil  
ntdsutil: roles  
fsmo maintenance: connections  
server connections: connect to server ADC  
Binding to ADC ...  
Connected to ADC using credentials of locally logged on user.  
server connections: quit
```

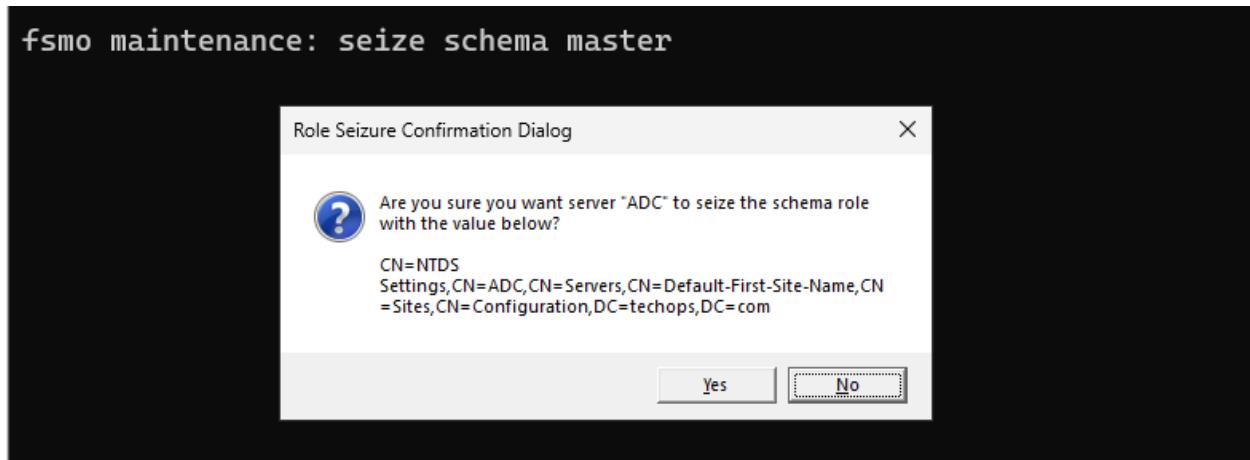
بشغل tool اسمها ntdsutil

منها بختار roles (لاني عاوز انقل ال roles)

بعد كدا بعمل connect على ال server ال عاوز انقل عليه ال FSOM Role وهو ف حالتي ال ADC

بعد كدا بطلع من ال connections وبكدا ال Seize يكون على ال server ال عملته عليه ADC وهو ال connect

--



بعد كدا بقوله عاوز اعمل seize لـ schema master او اي role هيطع ال log دا اضغط yes

```
fsmo maintenance: seize schema master
Attempting safe transfer of schema FSMO before seizure.
ldap_modify_sw error 0x34(52 (Unavailable)).
Ldap extended error message is 000020AF: SvcErr: DSID-0321053F, problem 5002 (UNAVAILABLE), data 1722

Win32 error returned is 0x20af(The requested FSMO operation failed. The current FSMO holder could not be contacted.)
)
Depending on the error code this may indicate a connection,
ldap, or role transfer error.
Transfer of schema FSMO failed, proceeding with seizure ...
Server "ADC" knows about 5 roles
Schema - CN=NTDS Settings,CN=ADC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=techops,DC=com
Naming Master - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=techops,DC=com
PDC - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=techops,DC=com
RID - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=techops,DC=com
Infrastructure - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=techops,DC=com
fsmo maintenance:
fsmo maintenance:
fsmo maintenance: |
```

هيحاول ينقل ال role بالطريقه الطبيعي لكن مش هيقدر يوصل لـ PDC فهيعملها Seize وبكدا هكون نقلت اول role وهكذا مع باقي ال roles

Disk Management

فيه طرقتين لنقسام ال Disk

Basic -1

Dynamic -2

windows : ودا النوع ال basic -1

بitem تقسيمه الي 4 Partitions primary طب لو تحتاج اكتر من 4 ؟ التقسيمه هتكون كالتالي :

3 Primary

1 Extended

وبداخل ال Extended اقدر اعمل لحد 63 logical partition (اقدر اعمل لحد Logical volume)

ودا في حالة استخدام ال MBR (Master Boot Record)

وال MBR دا اول 512Byet في ال Disk وبيتقسام ل 3 حاجات :

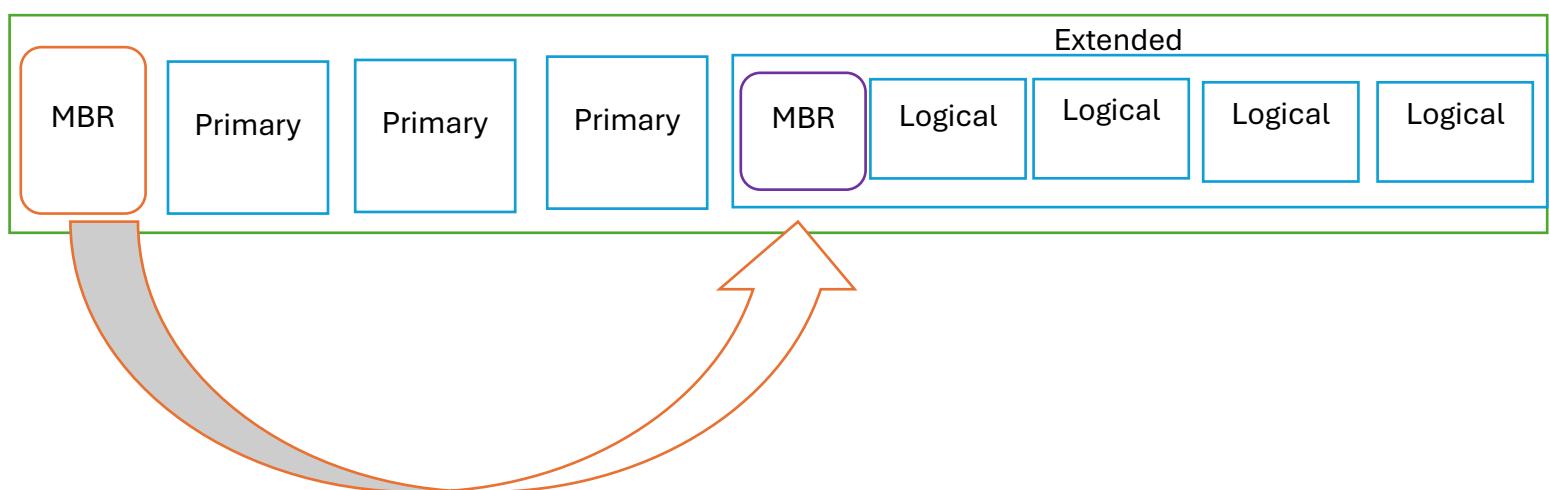
64 byte : دا بيكون بداخله معلومات عن كل ال partitions Partition table -

446 byte : يحتوي علي كود الاقلاع يعني دا ال بيقوم ال os بتاعي ومساحته Boot loader -

Magic number : هو عباره عن قيمه حجمها 2 byte من خلال هذه القيمه يتم التحقق من صحة ال MBR واذا

لم تكن هذه القيمه موجود يتعبر النظام ان ال MBR تالف

طيب ازاي ال MBR بيبقا شايف 4 partitions وانا ممكن يكون عندي لحد 63 logical ؟



ف ال MBR بيشوف ال Extended كله partition واحد فقط فهو بيشارو على mbr بيكون موجود في ال logical volume

طيب اي الفرق بين ال Extended Primary وال

ال Primary : دا القسم الرئيسي ال هيقلع منه نظام التشغيل بتاعي

قدر اعمل لحد 4 primary partition في ال MBR

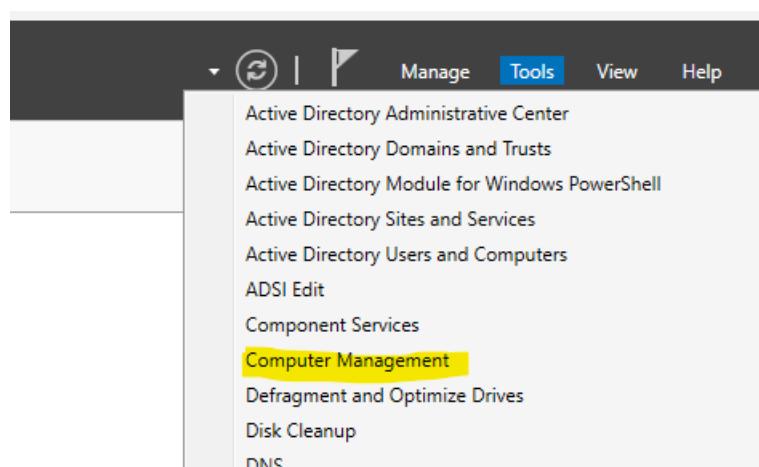
ال Extended : دا بيستخدم container بيشيل داخله ال logical volume

مقدرش استخدمه لتثبت نظام التشغيل

قدر اعمل لحد extended partition واحد فقط لكل Disk

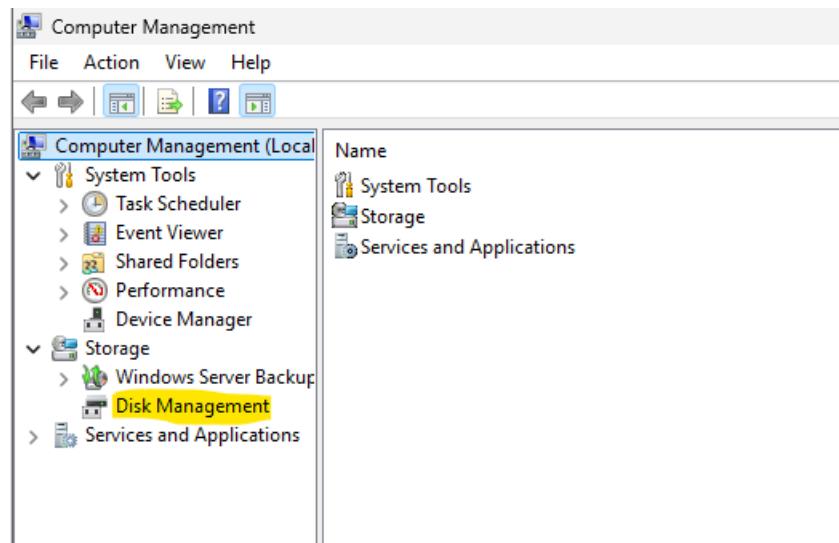
طيب ازاي نتعامل مع ال Disk ؟

من خلال Disk Management

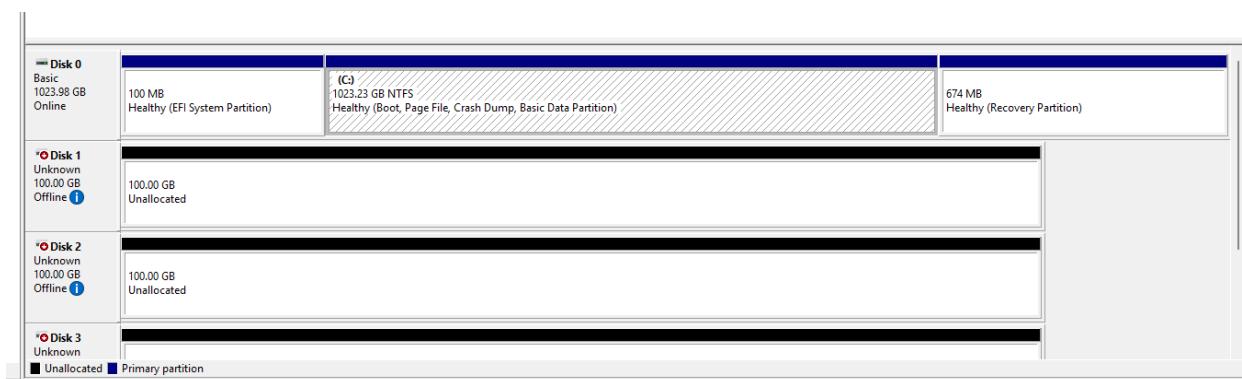


من Computer Management tools هختار

--



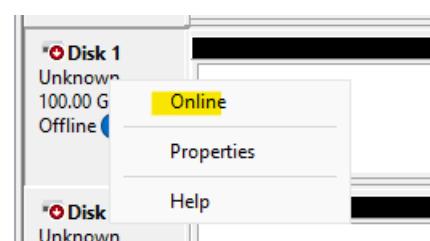
ومنه هنختار Disk Management



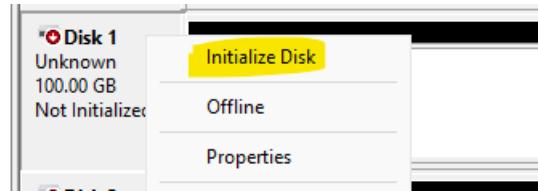
هناقی ال Disks ال عندي

طيب كدا Disk 0 هو بس ال online وشغال

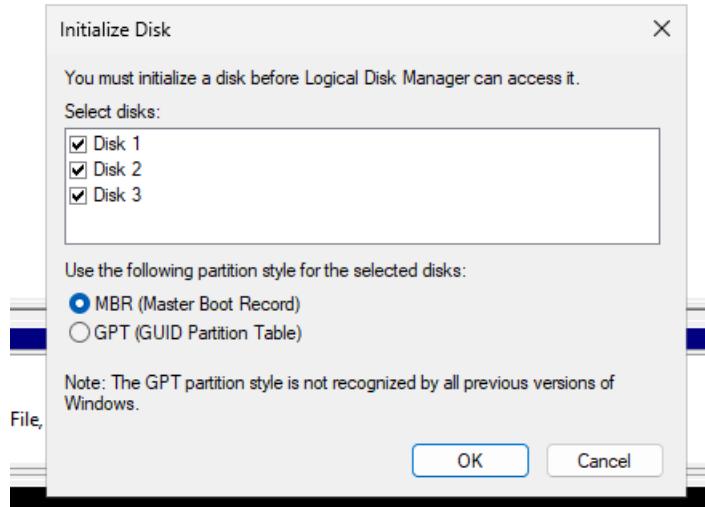
ازاي اجهز ال Disk عشان استخدمه ؟



على ال disk ونختار Click



بعد كدا هضغط click تاني وهضغط Initialize Disk



بعد كدا بختار ال Disk ال هعمله Initialize لأنني ضفت 3 disks جدد

وبعد كدا هختار MBR ولا GPT

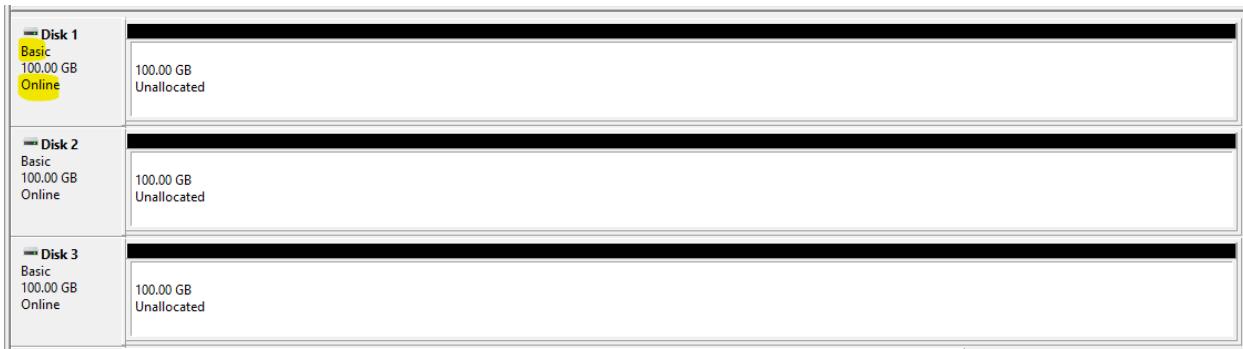
طيب اي الفرق بينهم ؟

ال : MBR

اقصي حجم لل Disk هو 2T – اقصي عدد لل Partitions هو 4- يدعم ال BIOS فقط

ال : GPT

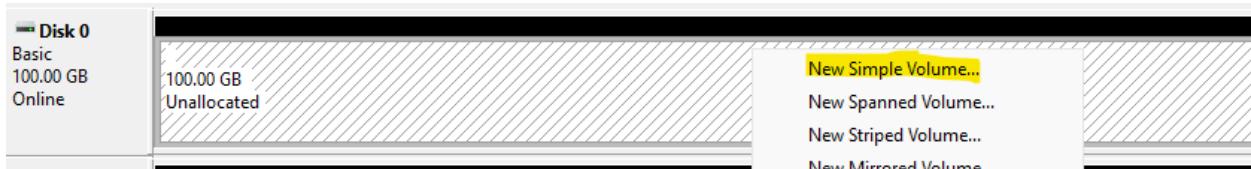
اقصي حجم لل Disk تقربيا 10ZB – اقدر اوصل لحد 128 primary partition – يدعم ال UEFI



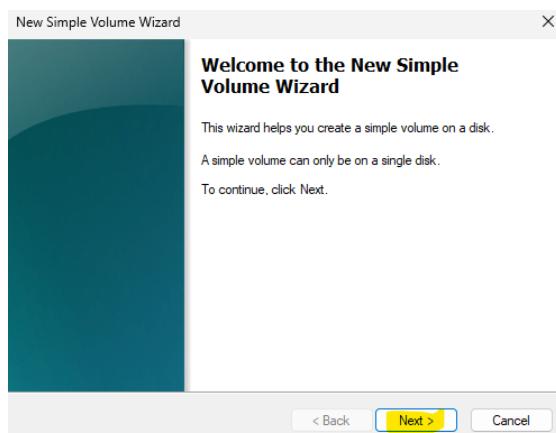
بعد كدا بقى **Basic** والنوع بناعه **online** دا ؟

--
طيب عاوز ابدا اشتعل على ال Disk دا ؟

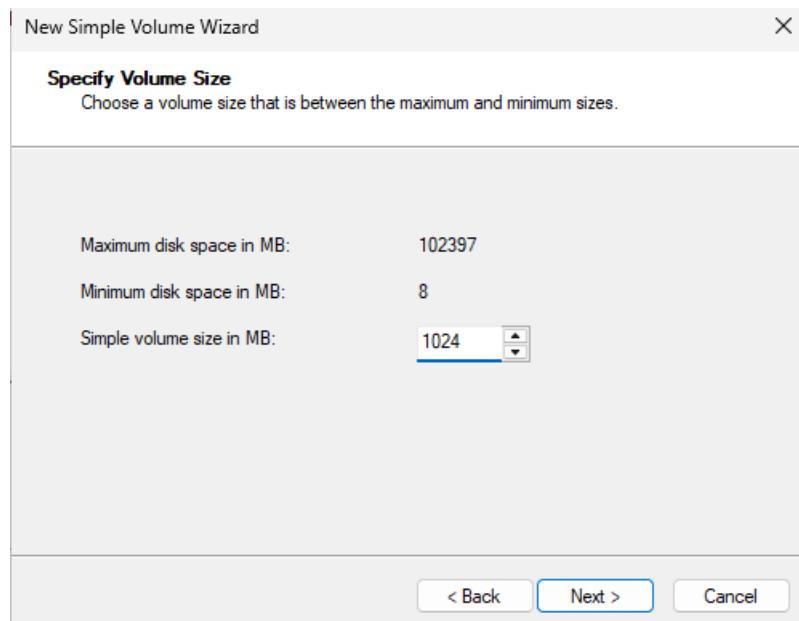
: partitions
هبدا اعمل



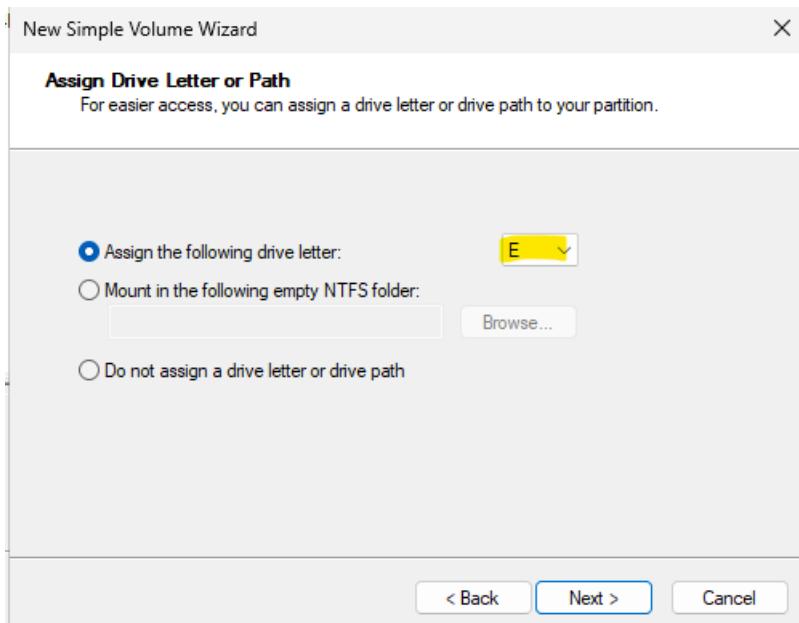
هضغط **New Simple Volume** على ال disk وختار click هختار



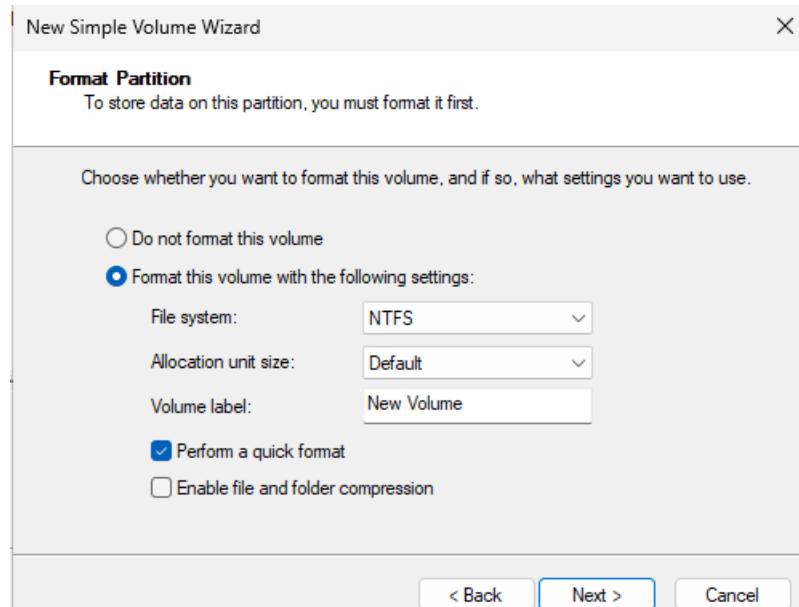
Next



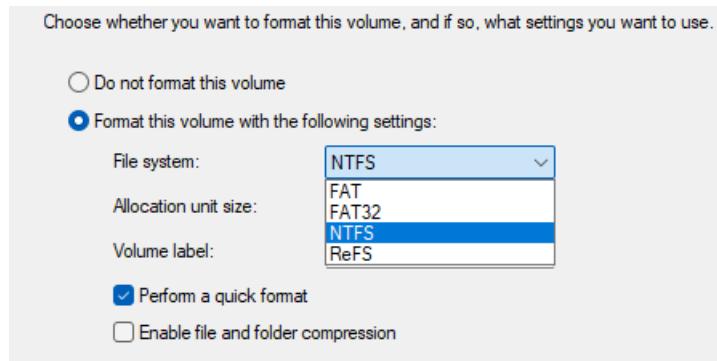
بعد كدا بحدد حجم ال partition بتاعي وهنا حده يكون 1 G



حدد Drive letter



بحد ال بتاعي وفي اكتر من نوع :



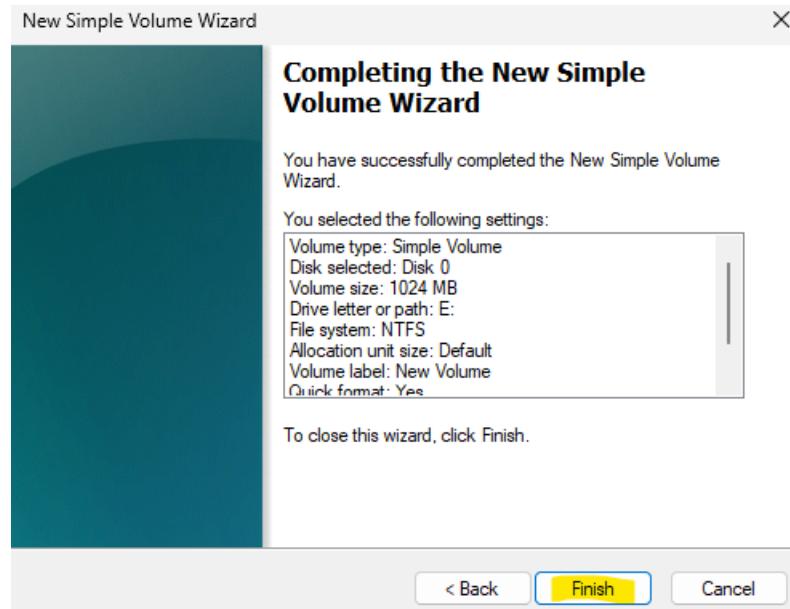
ودا نظام ملفات قديم وبيستخدم مع الاجهزه القديمه ، يدعم ال Disks صغيره الحجم ، لايدعم الملفات الكبيره

FAT -2 : اصدار محسن من FAT : حجم الملفات بتوصيل ل 4 GB وحجم ال partition بيصل ل 2TB ، بطئ في التعامل مع الملفات الكبيره ، لا يوفر صلاحيات وصول ولا يدعم التشفير ، يعني من التجزئة الي هي ال Fragmentation ودا بيسبب بطئ في الاداء

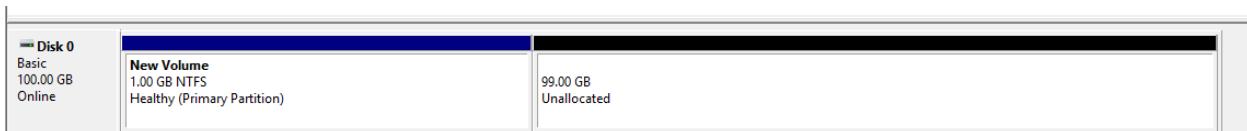
NTFS -3 : اختصار New Technology File System : يدعم ملفات تصل الي 16 اكتسابيات و partitions الى 8 بيتايات ، اسرع في قراءه وكتابه البيانات وخاصه مع الملفات الكبيره ، يدعم التشفير والتحكم في ال Permission

يقلل من ال Fragmentation

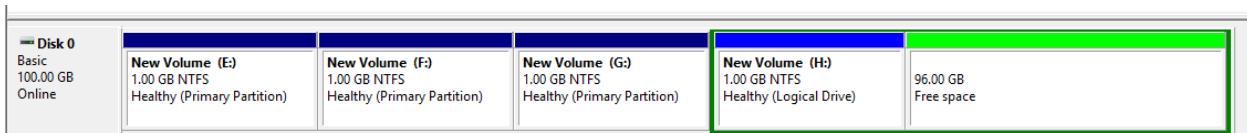
--



Finish



كدا عمل لـ `create partition` وبالتحديد `primary partition` هنكرر الخطوات دي 3 مرات كمان و هنشوف اي ال
هيحصل

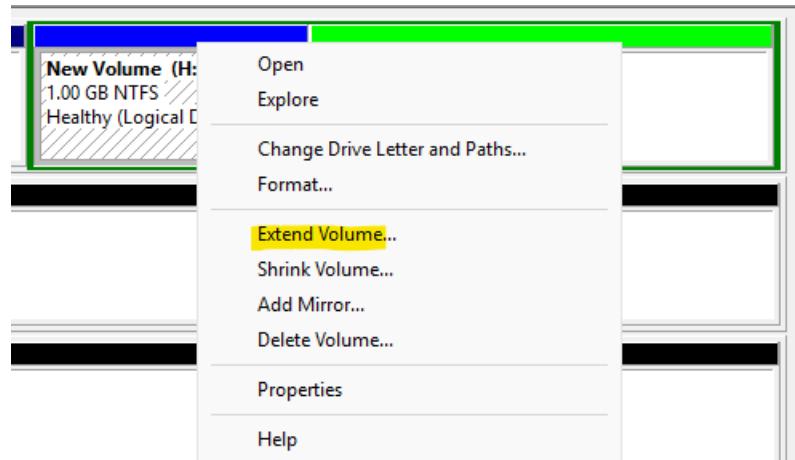


بعد ما عملت 3 كل واحد بحجم 1GB وجيت اعمل ال `partition` الرابع برضو بحجم 1GB
ف تلقائياً حولي كل المساحة المتبقية لـ `Extended Partition` وبداخله عمل create لـ `logical partition` بالحجم ال
كنت محدده وهو ال 1GB

طيب لو partition عندي المساحه كلها اتملت و عاوز ازودها ؟

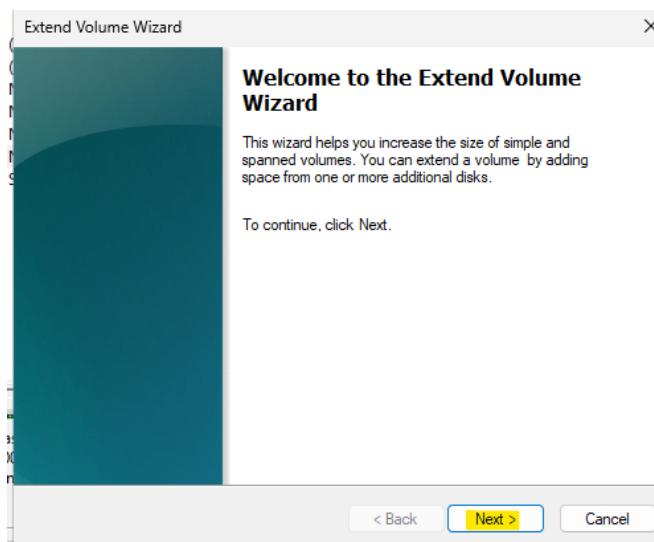
اقدر ازود لكن بشرط المساحه الفاضيه تكون موجوده جمبي عطول

يعني ف حالي مش هقدر ازود غير ال H partition

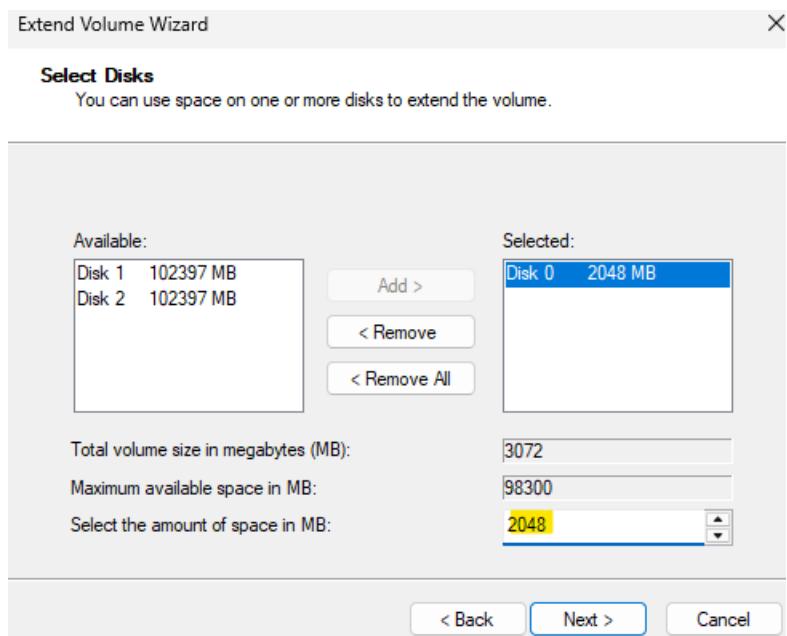


هروح على ال Partition واضغط click واختر Extend Volume

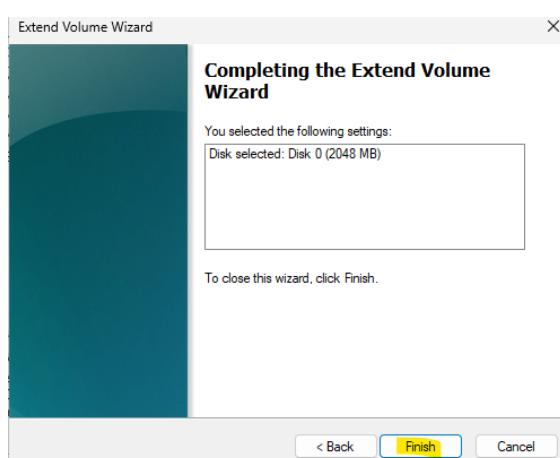
--



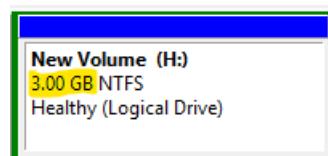
Next



کان 1GB و هزود عليه 2GB فهیظهر معايا مساحته ب 3GB

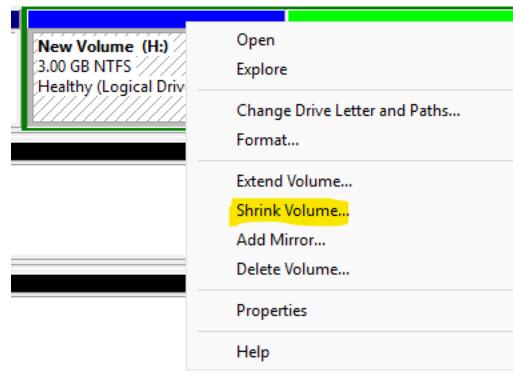


Finish

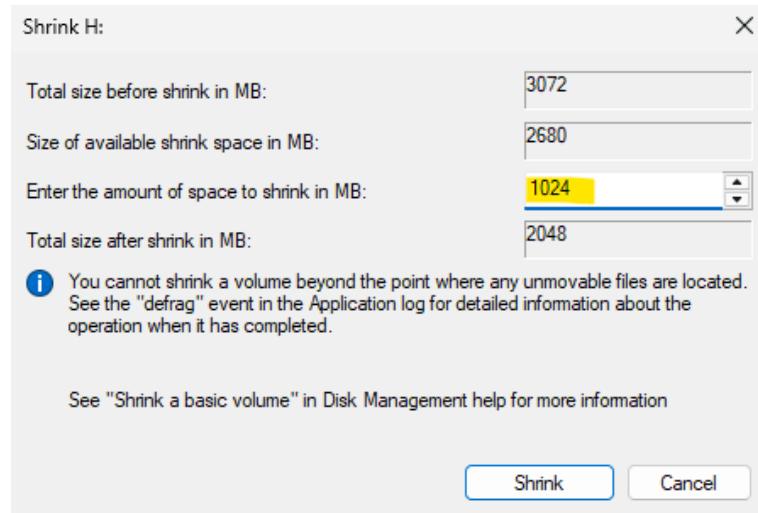


طيب لو هو بقا مساحته اكبر من ال يحتاجه وعاوز اخليه فقط 2G مش 3G ؟

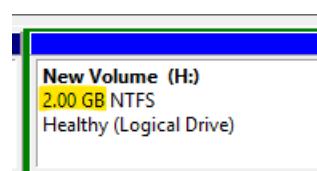
هعمل shrink



هضغط click ع ال partition وهختار Shrink Volume



هقوله عاوز اعمل shrink ل 1G

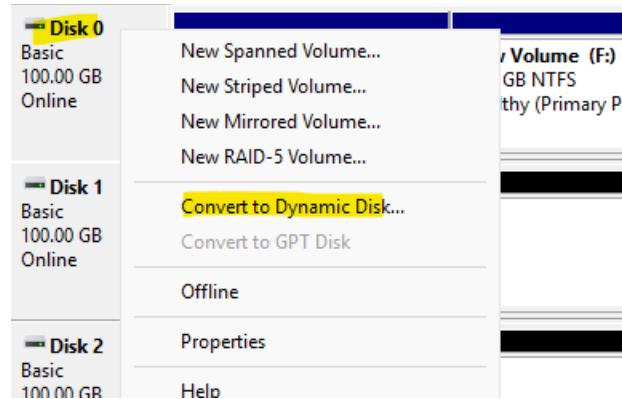


في ال partition هيفي 2GB وال free space 1GB هيروح لك

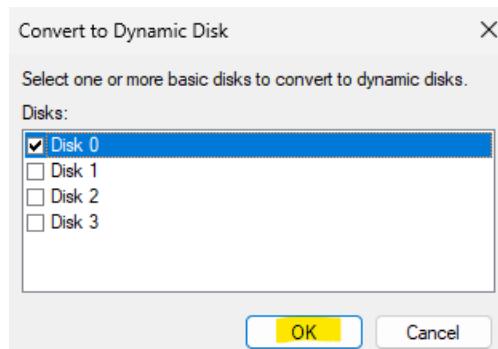
: dynamic في اكتر من نوع في ال Dynamic -2

Simple volume -1 : بعمله على واحد ، لا يوجد تحسن في الاداء او الحمايه ضد فقدان الداتا ، اقدر اعمل Disk partition من مساحه فاضيه متكتش جمبه عادي وممكن كمان اعملها من Disk ثاني غير ال Disk Extend ال هو فيه

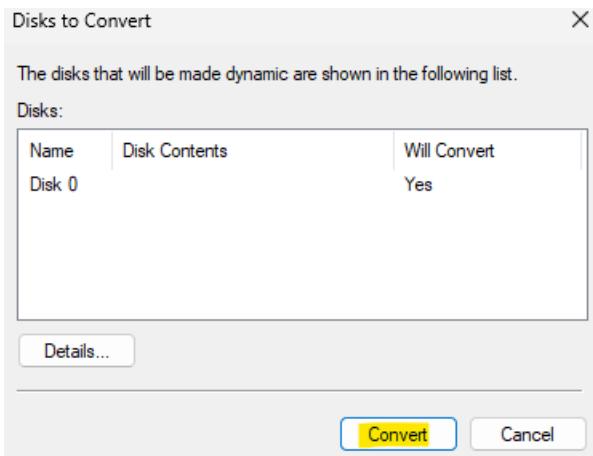
طيب ابدا استخدمه ازاي ؟



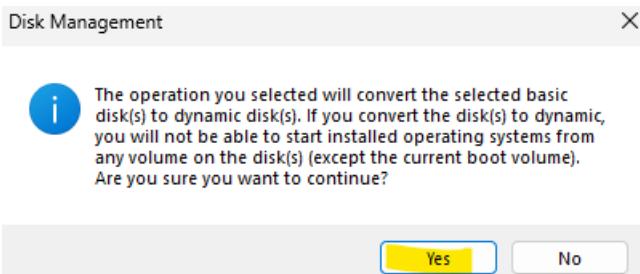
برو ح على ال Disk واضغط click واختار Convert to Dynamic Disk



اختر ال OK واضغط



واضغط بعد كدا على ال convert

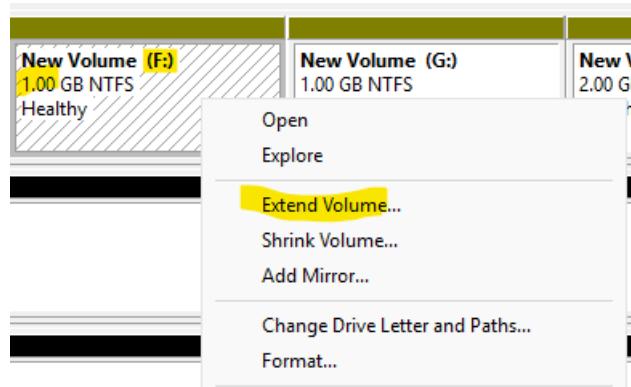


Yes

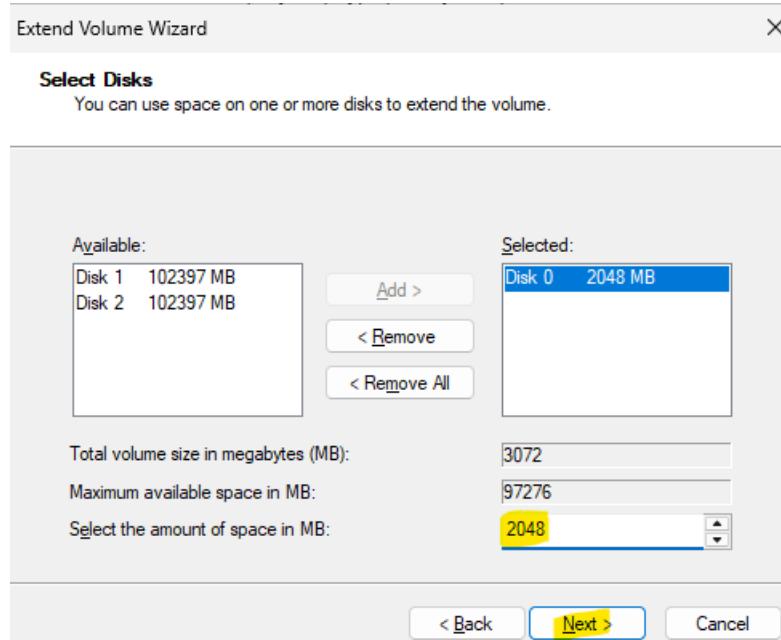
Disk 0 Dynamic 100.00 GB Online	New Volume (E) 1.00 GB NTFS Healthy	New Volume (F) 1.00 GB NTFS Healthy	New Volume (G) 1.00 GB NTFS Healthy	New Volume (H) 2.00 GB NTFS Healthy	95.00 GB Unallocated
Disk 1 Basic 100.00 GB Online	100.00 GB Unallocated				
Disk 2 Basic 100.00 GB Online	100.00 GB Unallocated				
Disk 3 Basic 1023.98 GB Online	100 MB Healthy (EFI System Partition)	(C) 1023.23 GB NTFS Healthy (Boot, Page File, Crash Dump, Basic Data Partition)			674 MB Healthy (Recovery Partition)
<input checked="" type="checkbox"/> Unallocated <input type="checkbox"/> Primary partition <input type="checkbox"/> Simple volume					

بقا ال Disk بقا partitions Dynamic وال simple volume عندي بقت من نوع

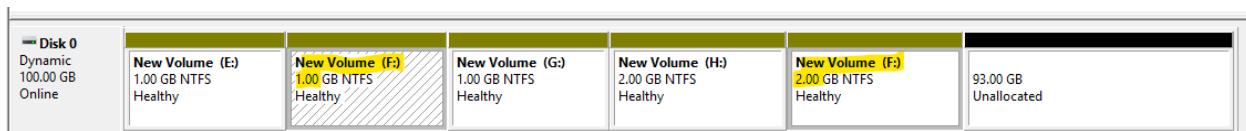
دلوقت اقدر اکبر مساحه اي partition رغم ان ال free



هروح على ال click وختار extend volume واختر partition



هو مساحته 1G فهزود عليه 2G هيقي مساحته 3G



هلاقي فيه partition جديد ظهر بس بنفس ال drive litter بالمساحه ال انا زودها



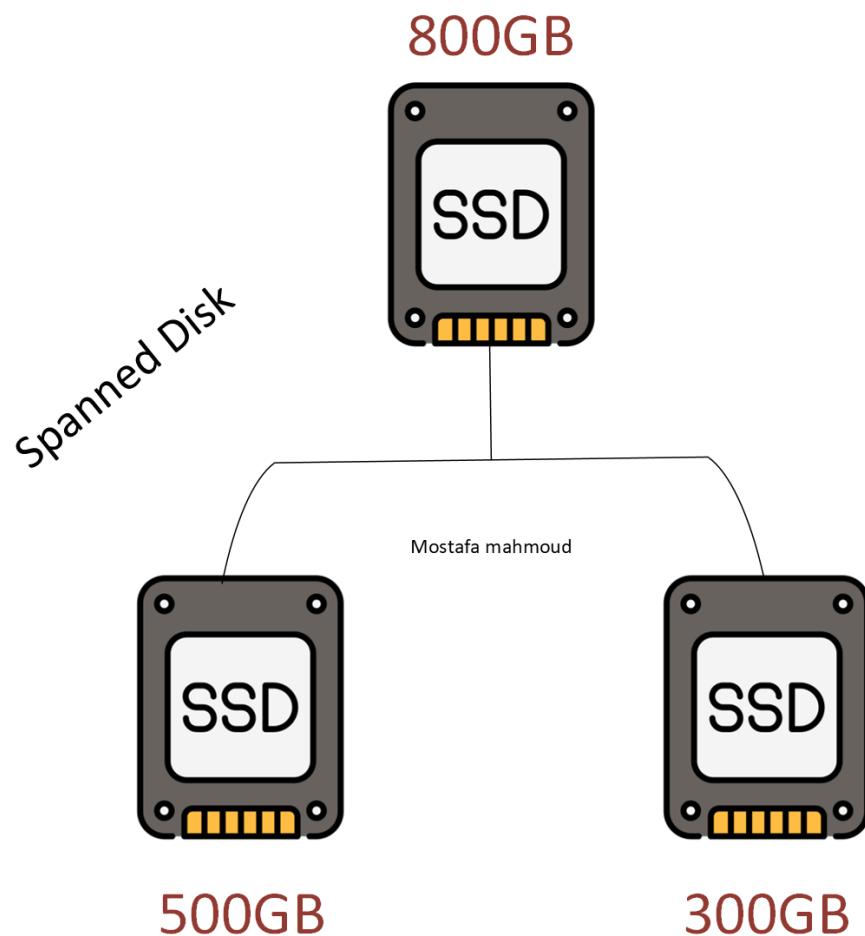
ولو روحت على ال partition هتلaci المساحه بتاعته بقت 3GB

النوع الثاني في ال : Dynamic

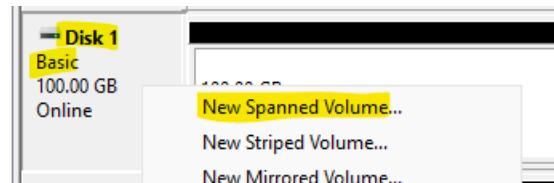
فكرته هنا اني بدمج اكتر من Disk مع بعض ويعامل معهم كاهم Disk واحد فقط ، بقى لازم اعمله على 2 Disk

معني لو عندي 2 كل واحد بحجم 500GB هدمج الاثنين مع بعض واتعمل معهم لك Disk واحد فقط مساحته 1TB

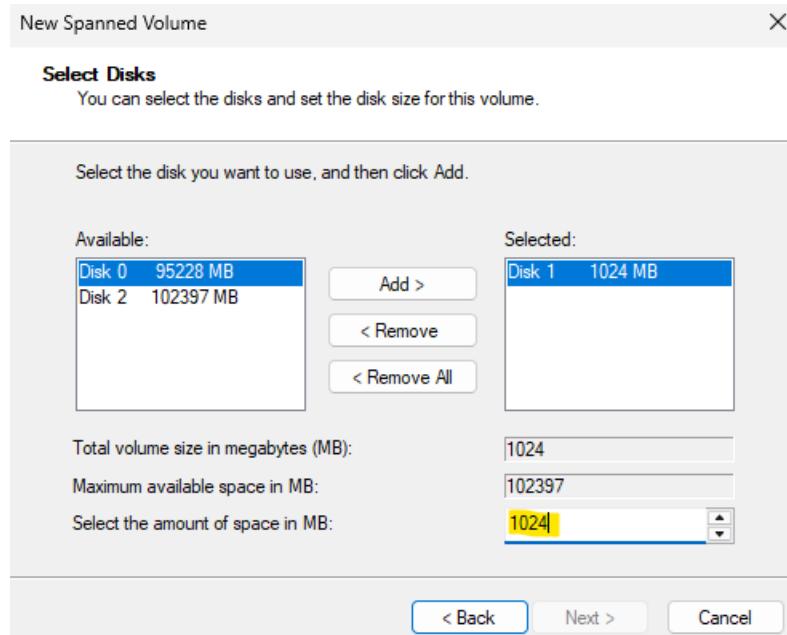
وهنا مش شرط ان الاثنين يكونوا نفس المساحه يعني ممكن واحد 500 واحد ثاني 200 لان الدانا بتكتب بالترتيب ع الاول يخلص يكتب على Disk الثاني ، لو حصله مشكله الدانا كله بتطير حتى ال على ال Disk ال مفهوش مشكله وبالتالي لا يوفر حمايه من البيانات ، وبستخدمه لو الهدف هي ازود مساحه التخزين



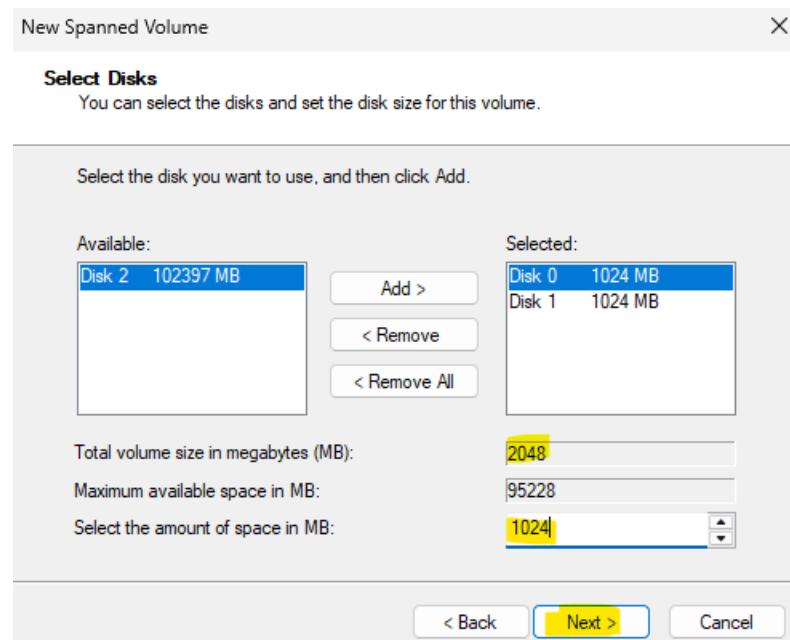
طيب اعمل کدا ازای ؟



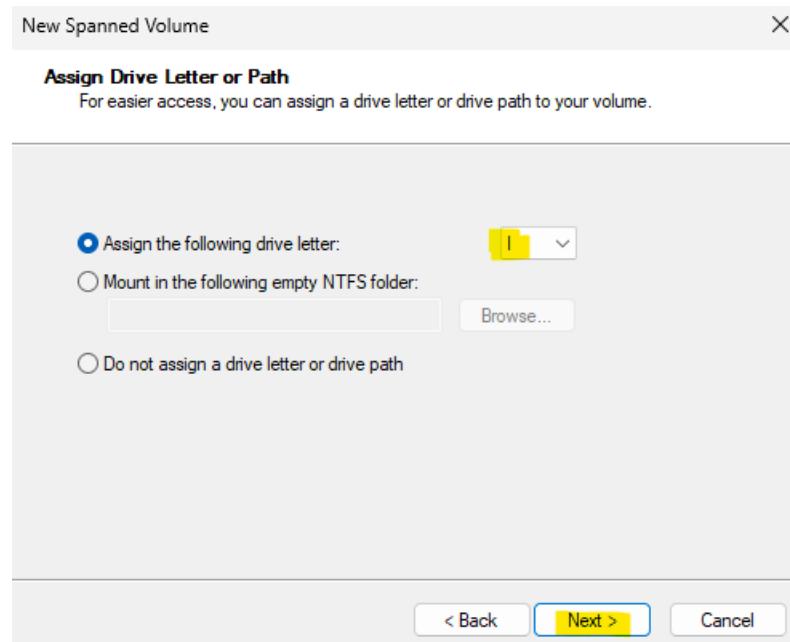
هروح على ال Disk و هضغط click و هختار New Spanned Volume



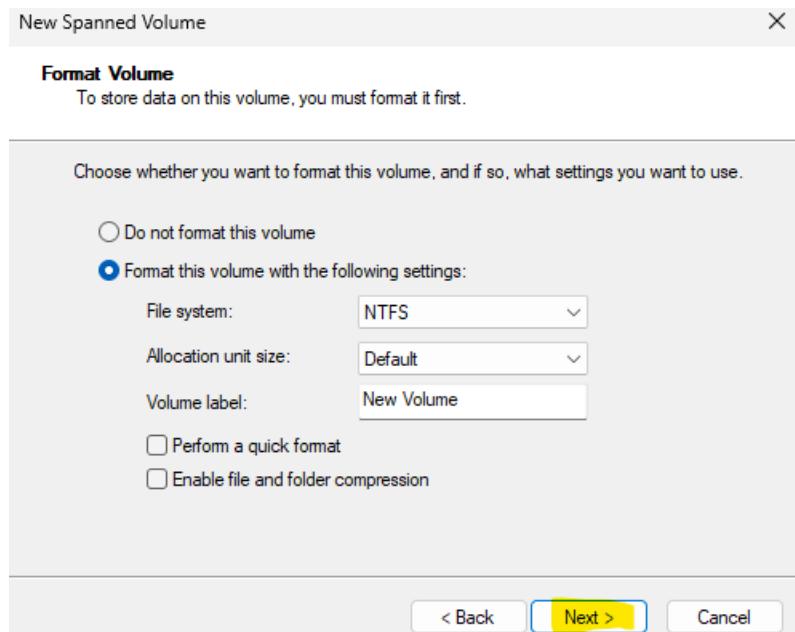
يقوله من Disk1 عاوز 1G لكن next غير مفعله طب ليه ؟ لانه لازم بشتغل على 2 Disks على الاقل



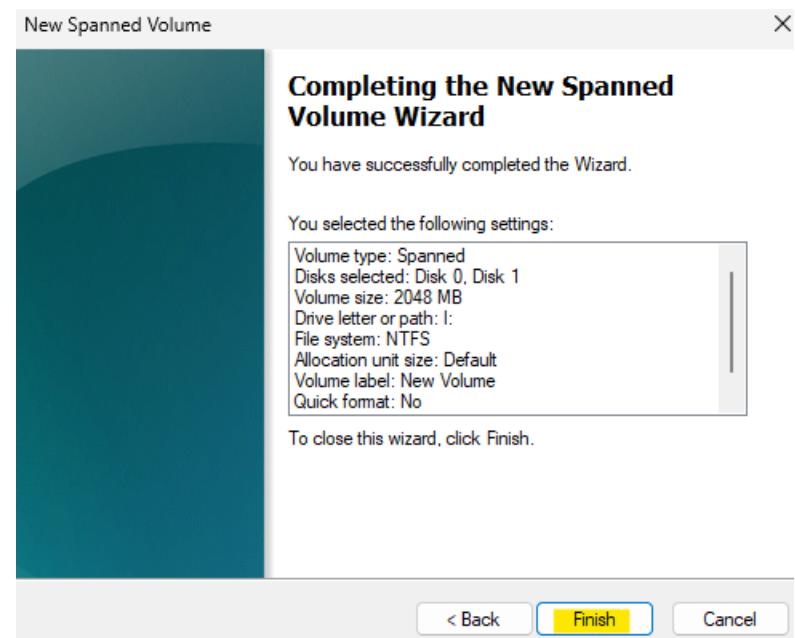
ضفت Disk کمان ، کدا من Disk0 هاخد 1GB و من Disk1 هعمل بينهم Spanned 1GB وبالتالي هيظهو وک واحد بمساحه 2G partition



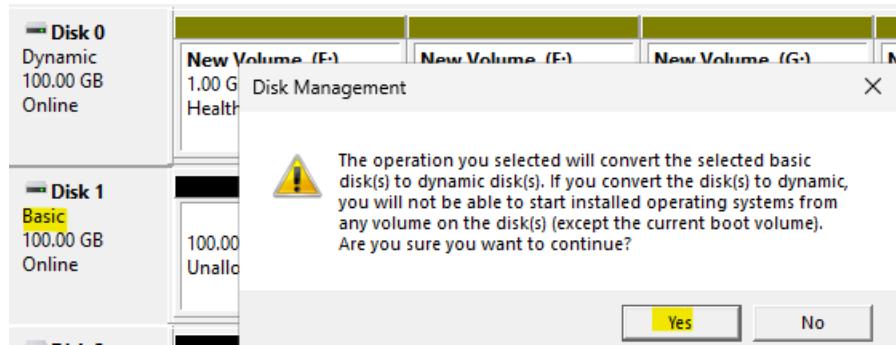
ختار ال Drive letter



Format ↴



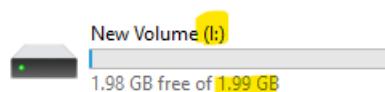
Finish



بيقولك ان Disk1 دا basic هولهولك dynamic عشان اقدر اعمل ال

Disk 0 Dynamic 100.00 GB Online	New Volume (E) 1.00 GB NTFS Healthy	New Volume (F) 1.00 GB NTFS Healthy	New Volume (G) 1.00 GB NTFS Healthy	New Volume (H) 2.00 GB NTFS Healthy	New Volume (I) 1.00 GB NTFS Healthy	92.00 GB Unallocated
Disk 1 Basic 100.00 GB Online	New Volume (I) 1.00 GB NTFS Healthy		99.00 GB Unallocated			
Disk 2 Basic 100.00 GB Online		100.00 GB Unallocated				
Disk 3 Basic 1023.98 GB Online	100 MB Healthy (EFI System Partition)	(C) 1023.23 GB NTFS Healthy (Boot, Page File, Crash Dump, Basic Data Partition)			674 MB Healthy (Recovery Partition)	
	■ Unallocated	■ Primary partition	■ Simple volume	■ Spanned volume		

ظهر عندي 1 partition لـ Disk0 من 1G و 1G من Disk1

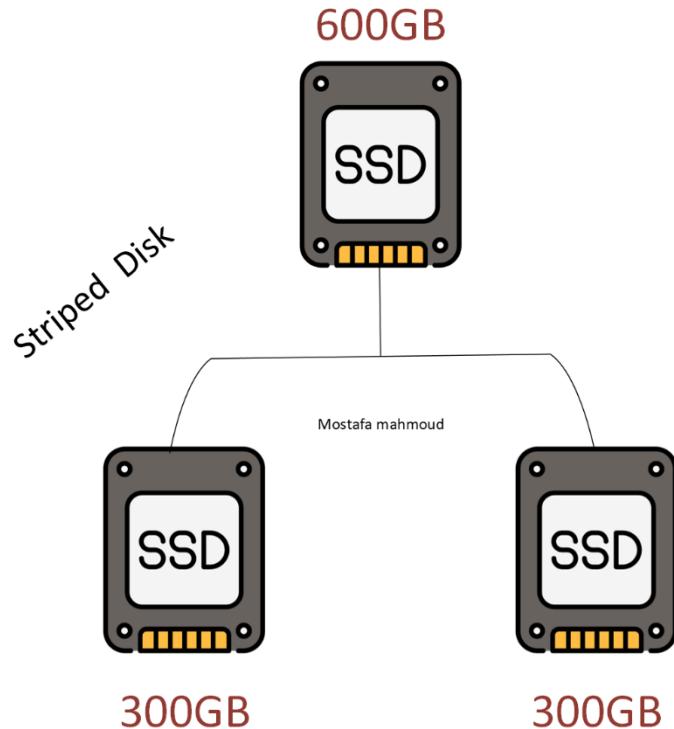


لو روحت على 1 partition هتلaci مساحته 2G

النوع الثالث من ال Dynamic

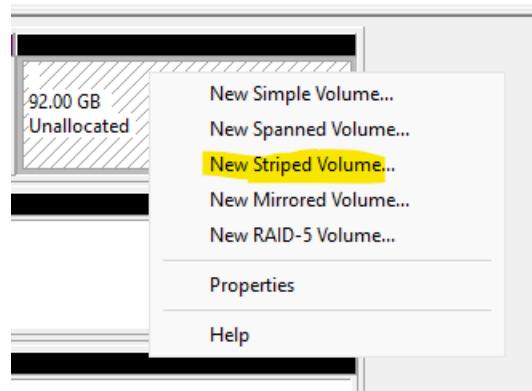
: RAID 0 ويسمى ب Striped Volume

نفس فكره ال Spanned لكن لازم مساحته الاتنين تكون متساوية والسبب انه بيوزع الداتا بين الاتنين مش بيكتب على disk الاول ويستتي يخلص ويروح يكتب على disk الثاني

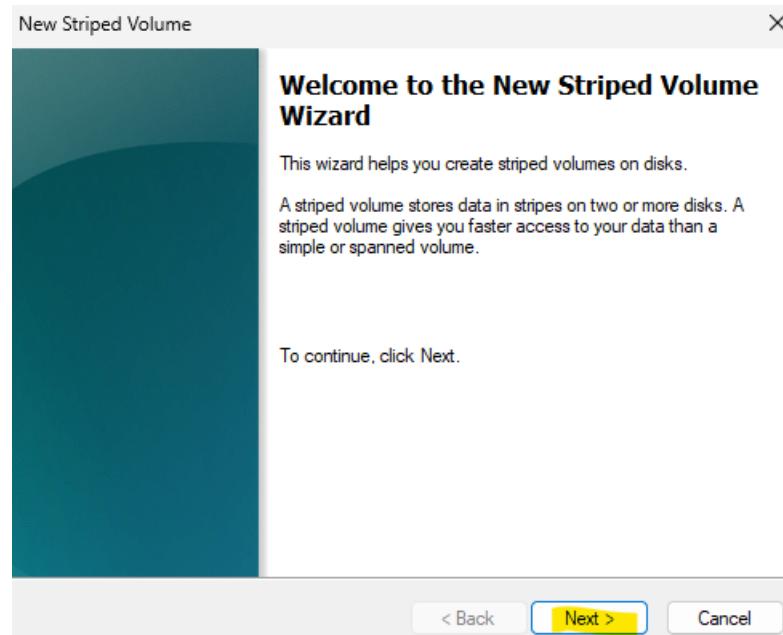


طلما ال Disk الاول 300GB فلازم الثاني يكون 300GB

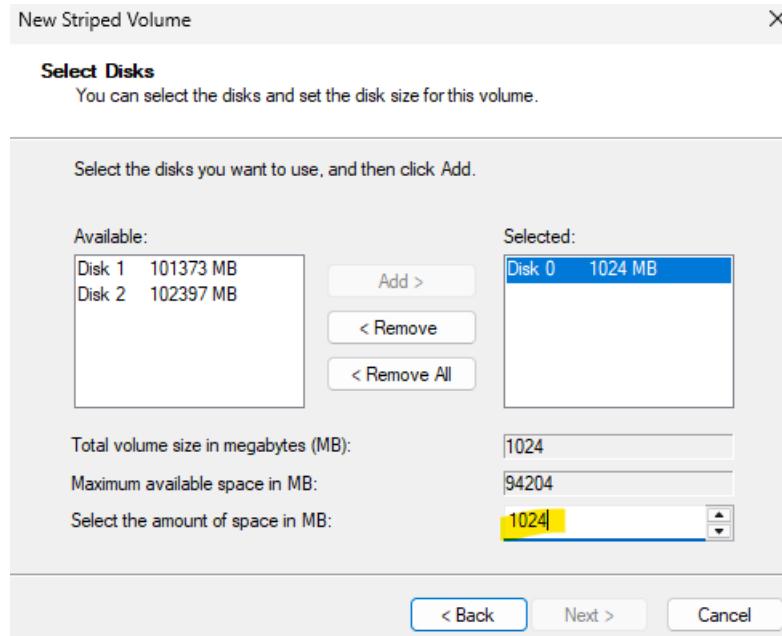
طيب ابدا استخدمه ازاي ؟



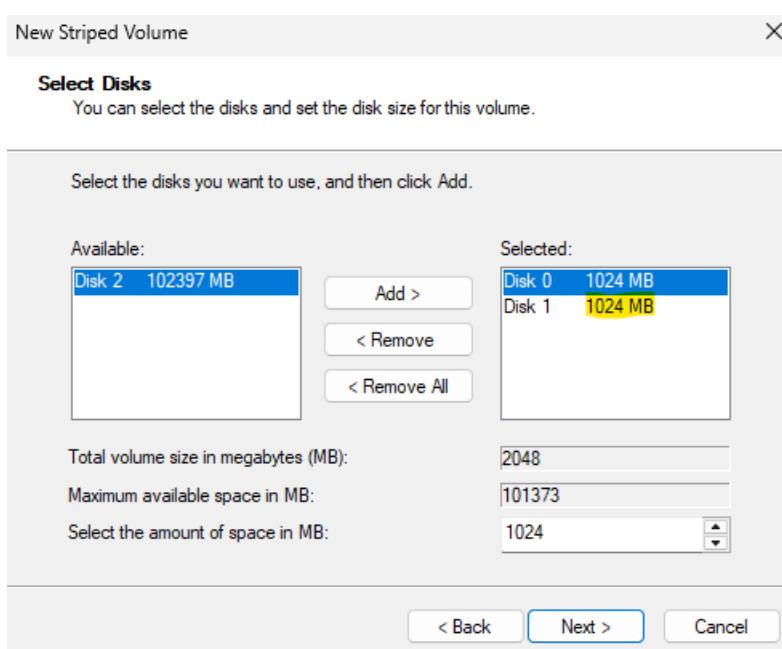
Click على ال مختار وختار New Striped Volume على الع'espace unallocated



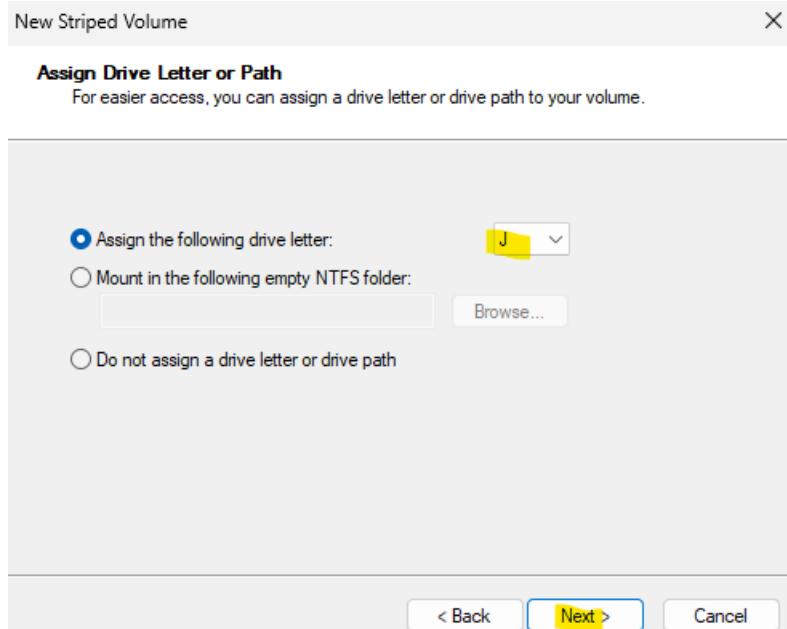
Click Next



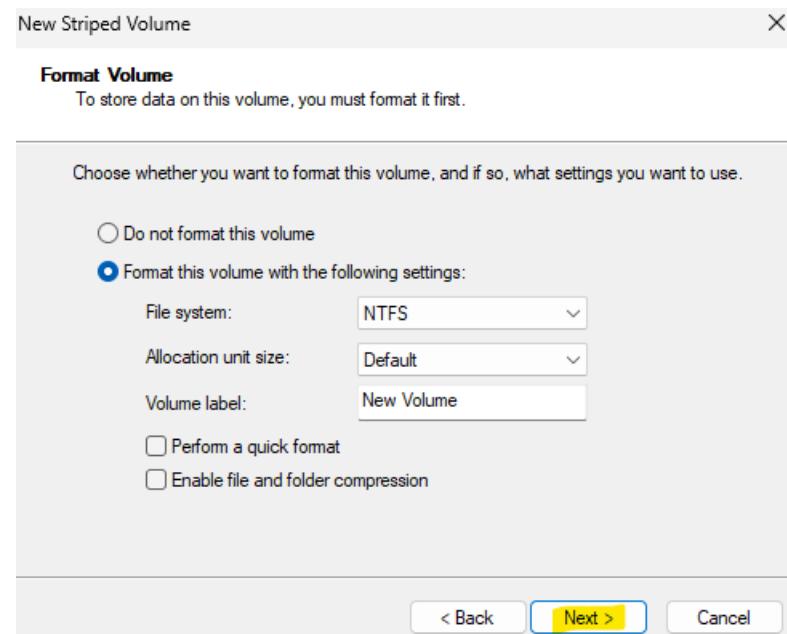
يقوله من 0 Disk عاوز 1GB وطبعا Next مش متفعل عشان لازم يكون في Disk 2 على الأقل



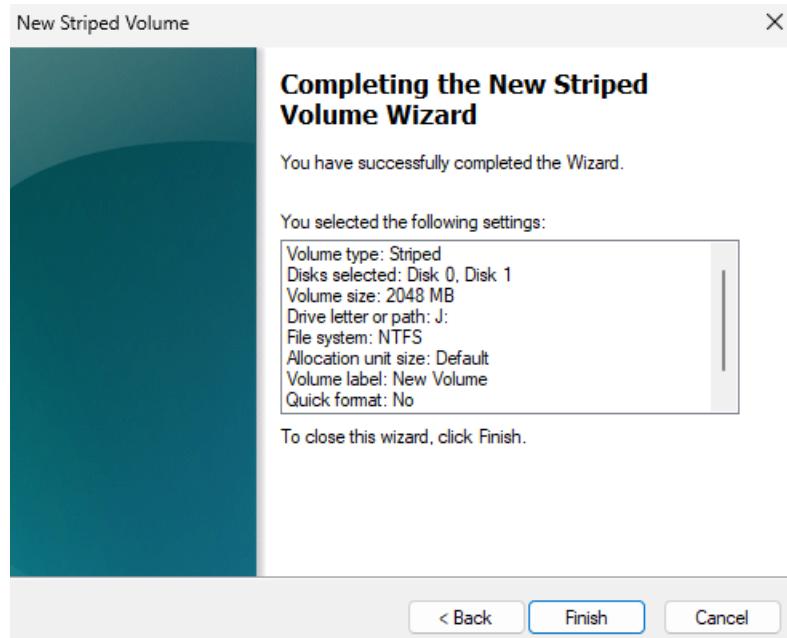
أول ما عملت Add ل Disk 1 هو مع نفسه حدد ال 1GB لأن زي م قولنا لازم مساحه الاثنين تكون متساوية



حدد بحده



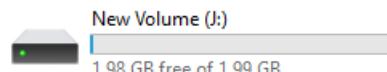
عمل بعده



Finish

Disk 0 Dynamic 100.00 GB Online	New Volume (E): 1.00 GB NTFS Healthy	New Volume (F): 1.00 GB NTFS Healthy	New Volume (G): 1.00 GB NTFS Healthy	New Volume (H): 2.00 GB NTFS Healthy	New Volume (I): 1.00 GB NTFS Healthy	New Volume (J): 1.00 GB NTFS Healthy	91.00 GB Unallocated
Disk 1 Dynamic 100.00 GB Online	New Volume (L): 1.00 GB NTFS Healthy	New Volume (J): 1.00 GB NTFS Healthy		98.00 GB Unallocated			

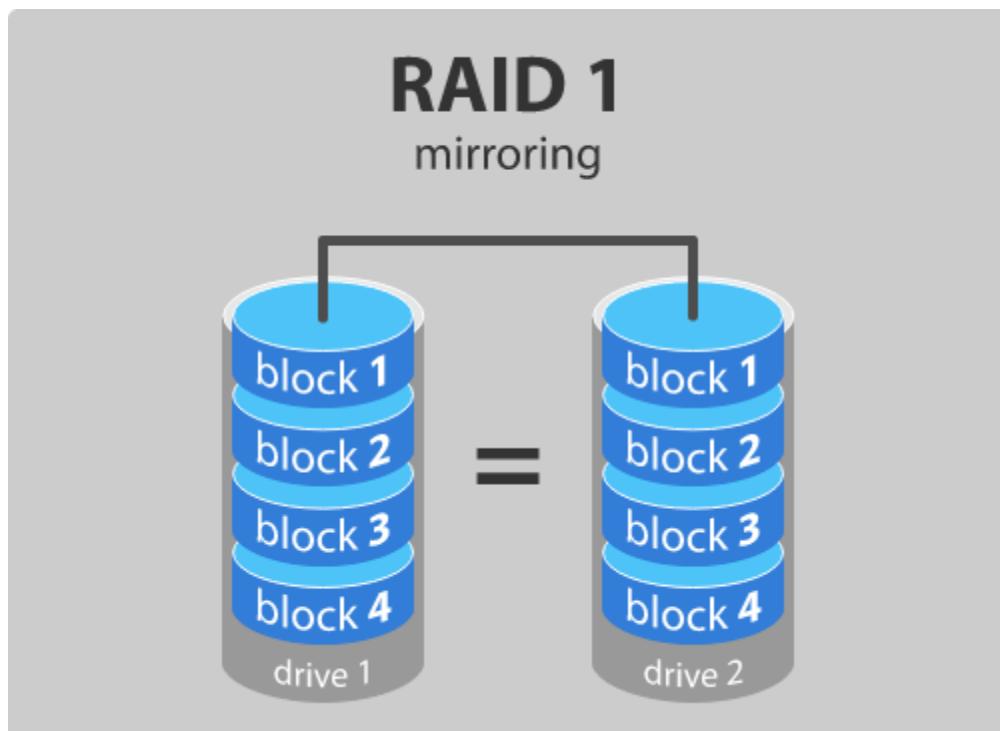
هلاقی عندي J عباره عن 1GB من Disk0 و 1GB من Disk1 partition



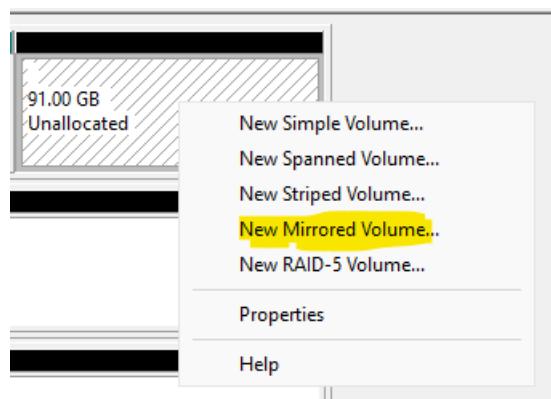
ولو فتحنا ال 2GB هلاقی مساحته partition

ويسمي ب RAID1 : لازم يكون علي 2Disk وال بيحصل بيتم تكرار الداتا علي ال Disk 2 يعني ال data الموجودة علي disk0 هي الموجودة علي disk1 ودا بعمله عشان لو فيه disk من الاثنين حصله مشكله ال data ميحصلهاش مشكله ، لكن هنا هىستهلاك ضعف المساحة ، ولازم يكون ال 2Disk بنفس المساحة

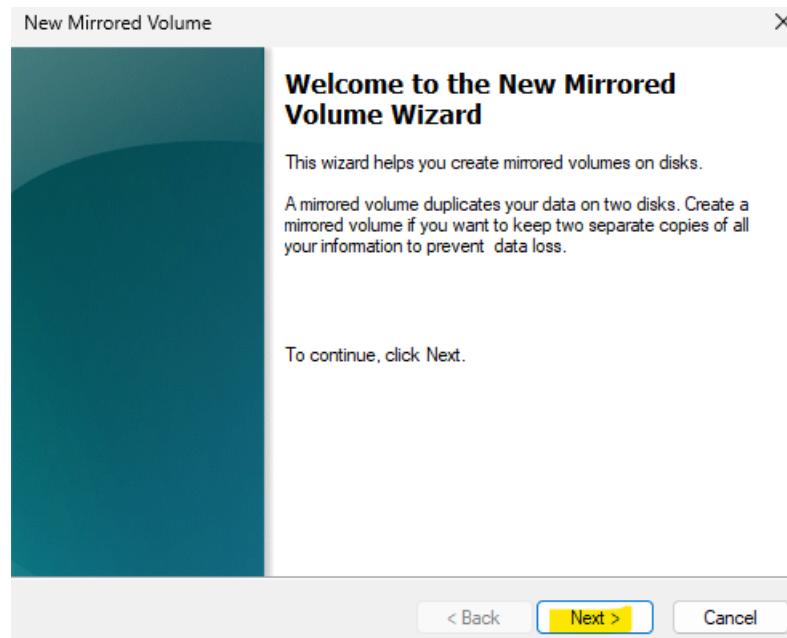
فلو عندي 2disk كل واحد فيهم 500GB هيظهروا في my computer لك واحد بروض بمساحة 500GB طب ليه مظهروش ب 1TB لأن الاثنين بيكتب عليهم نفس الداتا وهنا التركيز كله علي الحفاظ علي البيانات



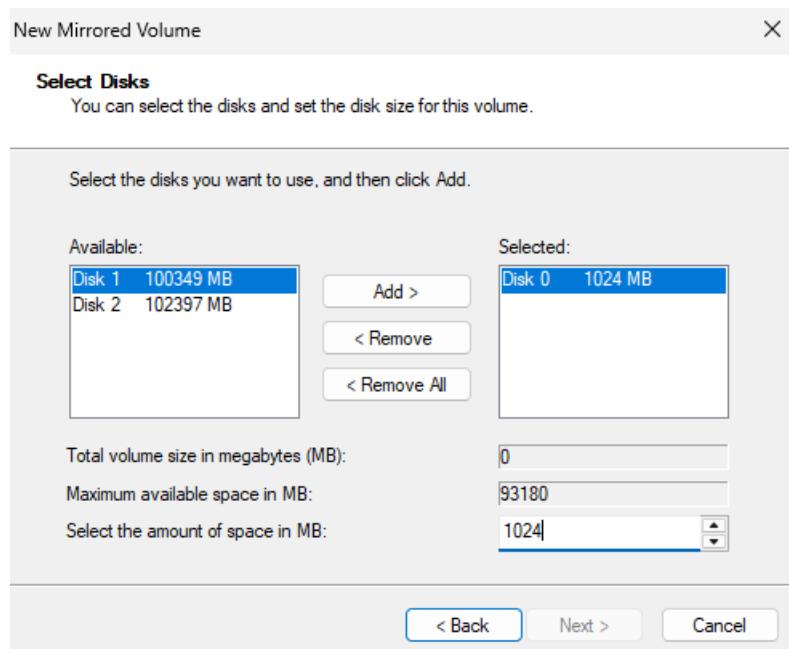
طيب ازاي ابدا اشتغل عليه ؟



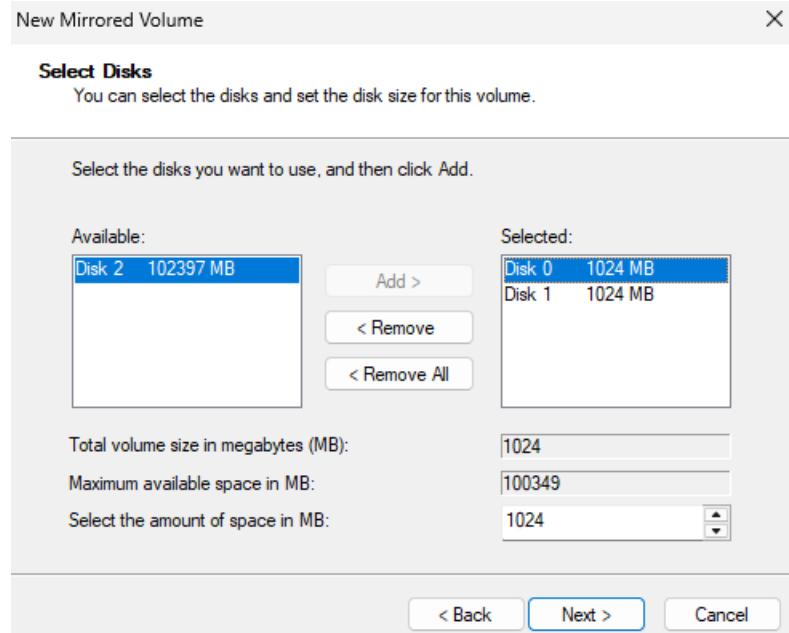
Click على ال وختار New Mirrored Volume في خيار العلامة المائية



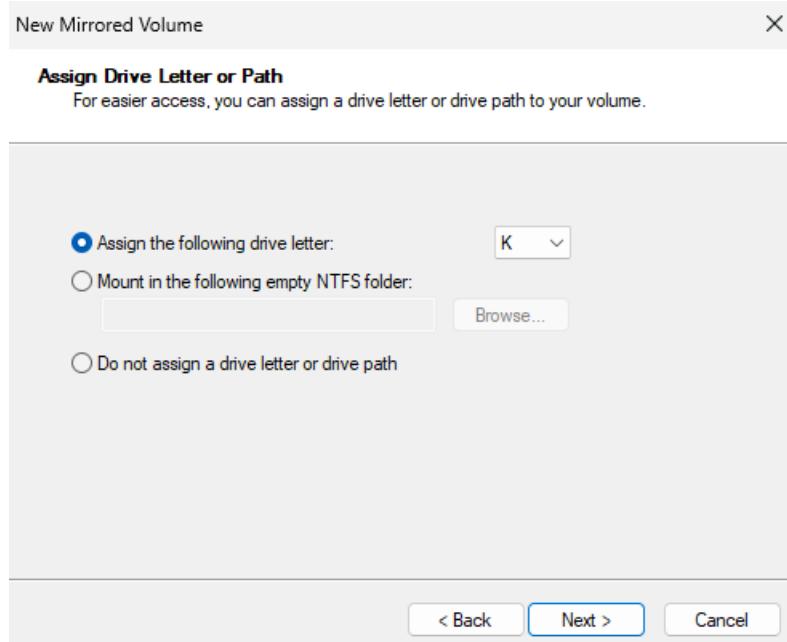
Click Next



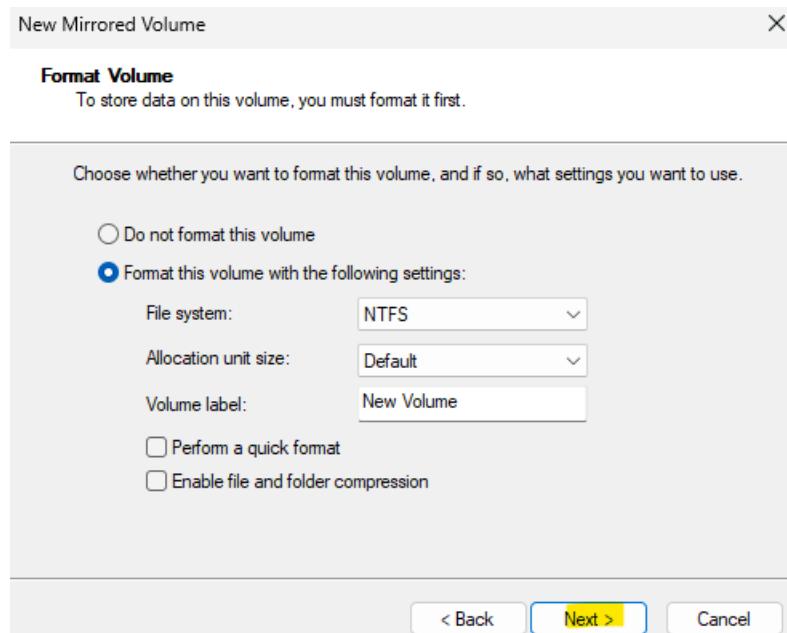
بقوله من 0 عاوز 1GB وطبعا Next مش متفعل عشان لازم يكون في Disk 2 على الأقل



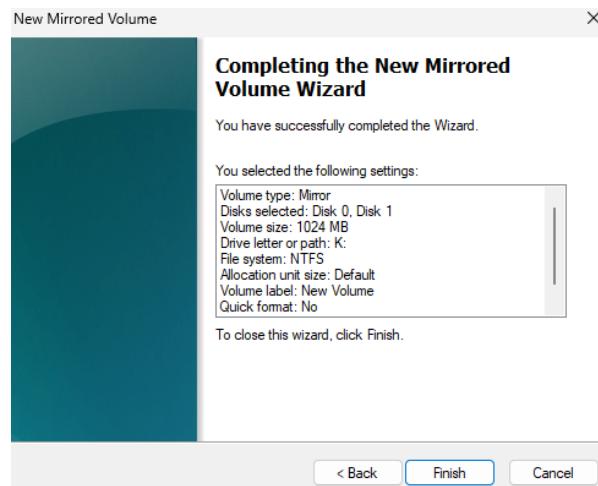
اول ما عملت Add ل Disk 1 هو مع نفسه حدد ال 1GB لان زي م قولنا لازم مساحه الاتنين تكون متساوية



Drive letter ↴



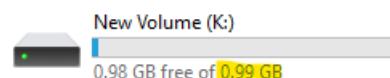
Format



Finish

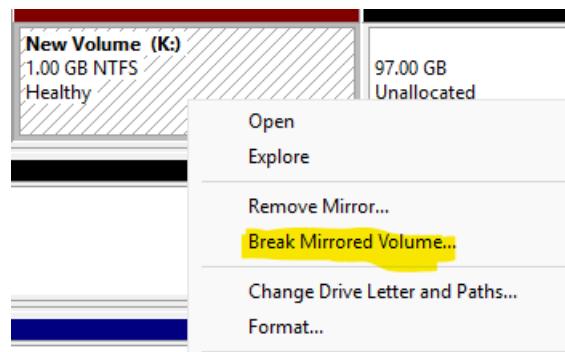
Disk 0 Dynamic 100.00 GB Online	New Volume (E) 1.00 GB NTFS Healthy	New Volume (F) 1.00 GB NTFS Healthy	New Volume (C) 1.00 GB NTFS Healthy	New Volume (H) 2.00 GB NTFS Healthy	New Volume (F) 2.00 GB NTFS Healthy	New Volume (I) 1.00 GB NTFS Healthy	New Volume (J) 1.00 GB NTFS Healthy	New Volume (K) 1.00 GB NTFS Healthy	90.00 GB Unallocated
Disk 1 Dynamic 100.00 GB Online	New Volume (L) 1.00 GB NTFS Healthy	New Volume (J) 1.00 GB NTFS Healthy	New Volume (K) 1.00 GB NTFS Healthy		97.00 GB Unallocated				
Disk 2 Basic 100.00 GB Online	100.00 GB Unallocated								
Disk 3 Basic 1023.98 GB Online	100 MB Healthy (EFI System Partition)	(C) 1023.23 GB NTFS Healthy (Boot, Page File, Crash Dump, Basic Data Partition)							674 MB Healthy (Recovery Partition)
CD-ROM 0 DVD 5.60 GB Online	SSS_X64FREE_EN-US_DV9 (D) 5.60 GB UDF Healthy (Primary Partition)								
■ Unallocated ■ Primary partition ■ Simple volume ■ Spanned volume ■ Striped volume ■ Mirrored volume									

بقا عندي 2Disk و هو عباره عن 1GB من Disk0 و 1GB من Disk1 partition k



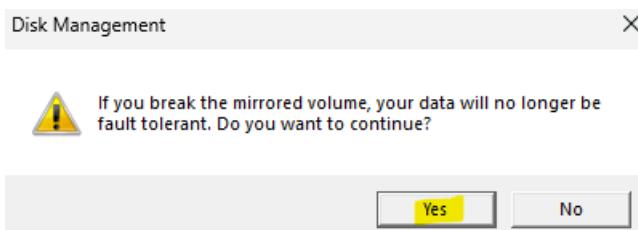
وفي my computer هنلاقيه ظهر ب 1GB فقط ودا لان الداتا هتكتب علي ال 2Disk

طيب لو فيه منهم Disk حصل فيه مشكله ، ممكن اجي افصلهم عن بعض بحيث يكون كل disk مستقل بالبيانات ال عليه



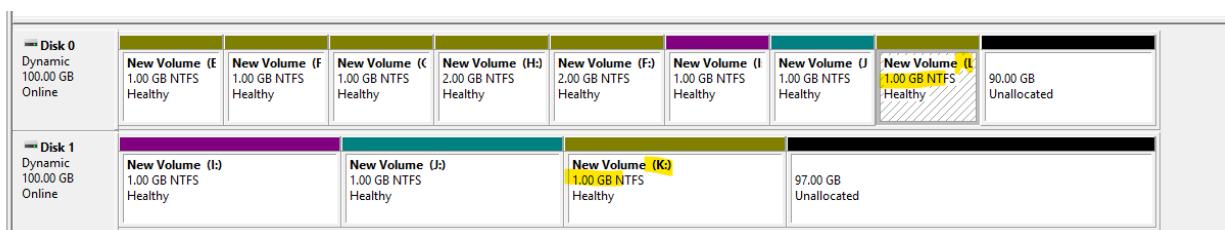
هروح على ال Break Mirrored Volume واعمل click mirror volume واختار

--



Yes

--

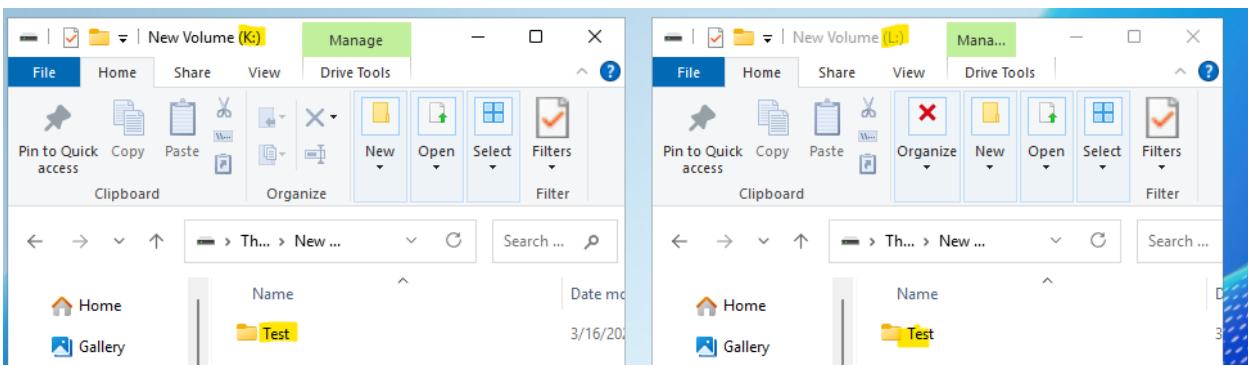


بتحولهم ل simple volume

--

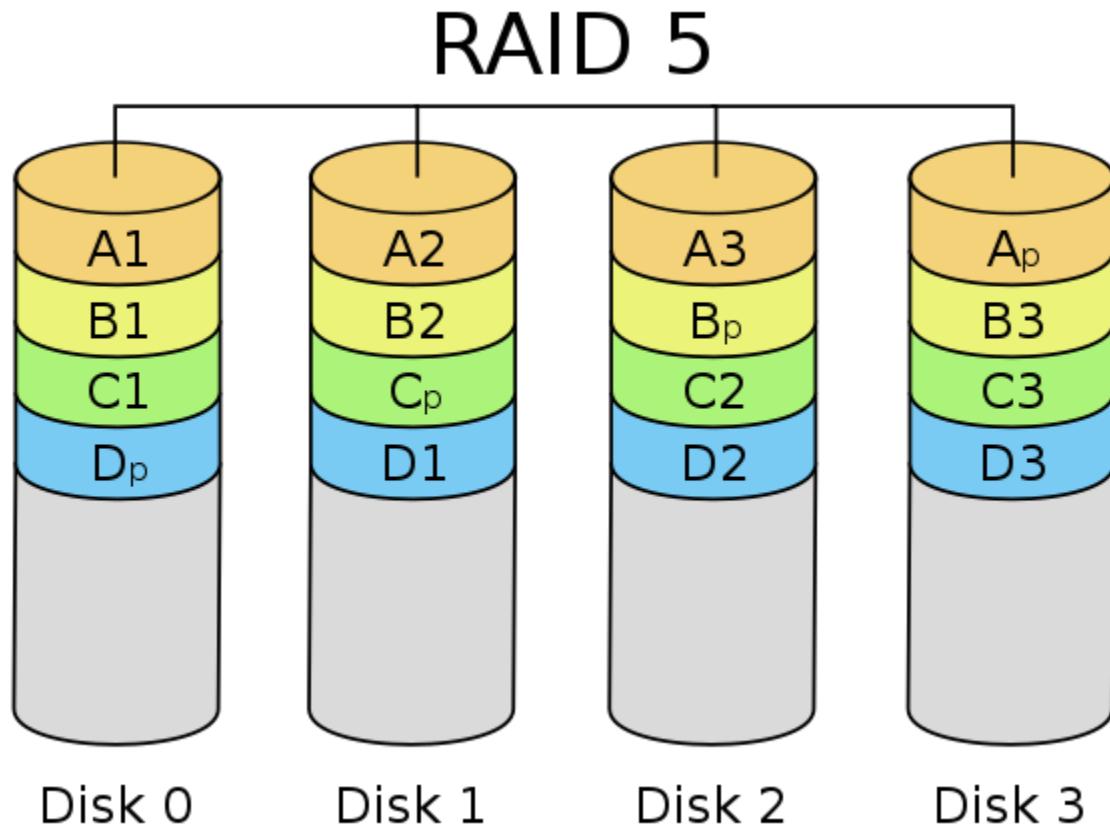


باقيهم انفصلوا عندي وكل واحد بقا disk لوحدة

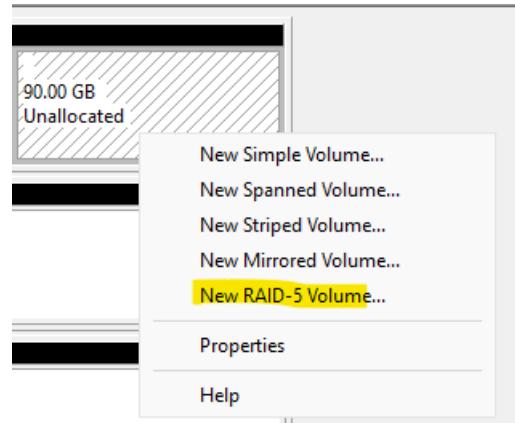


وكل واحد فيهم عليه نفس ال Data

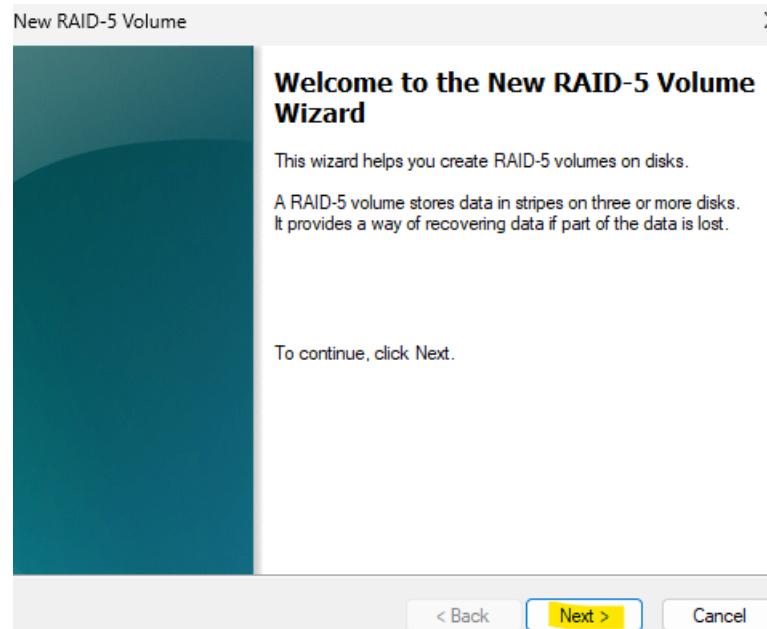
RAID 5 : بتعميل على 3Disk على الاقل ، الداتا بتكتب على 2Disk والثالث بيتسجل عليه معلومات ال parity ودى عن طريقها لو فيه مشكله وفقط لو غيرت ال Disk ال فيه المشكله كل الداتا هترجع زي ما كانت والمساحه بتظهر بعد مساحه ال الا ال disk ال هيكون عليه ال parity



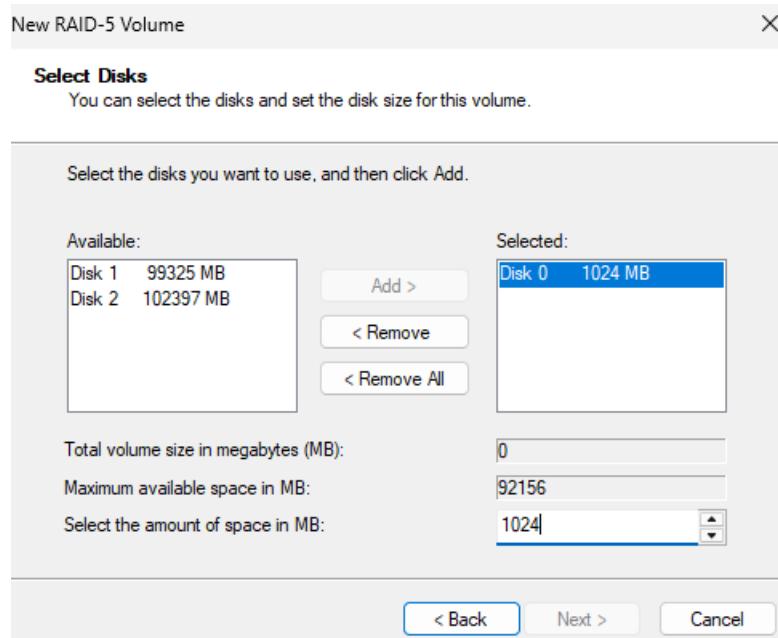
طيب ابدا استخدمه ازاي ؟



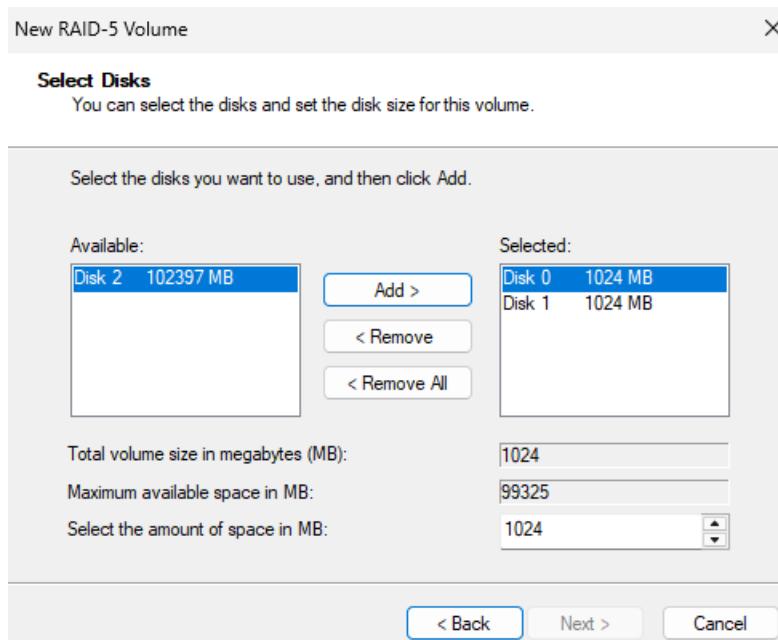
Click على الـ New RAID-5 Volume وختار unallocated space



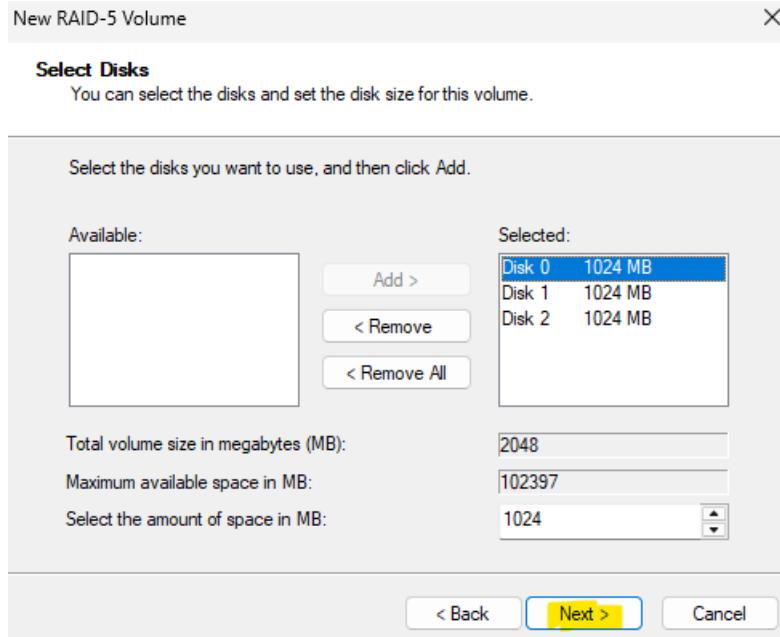
Next



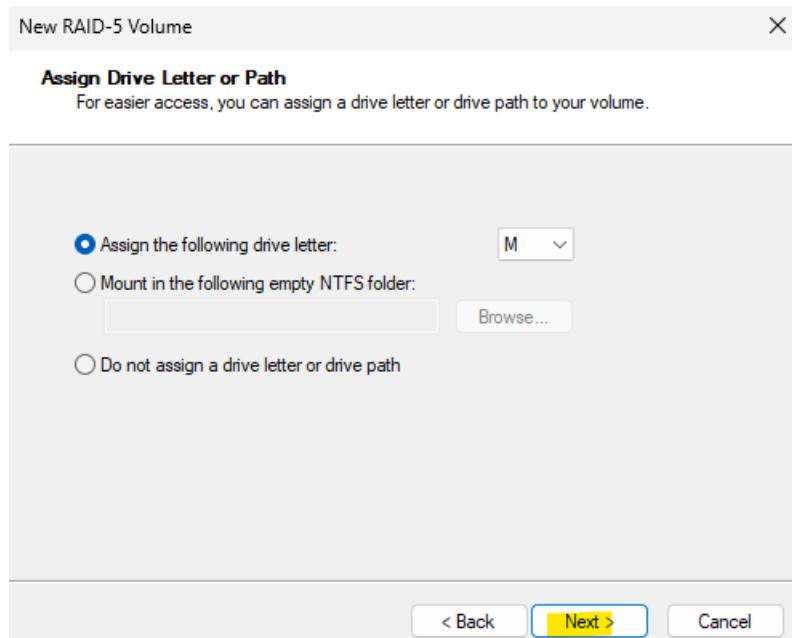
هضيف 1GB من Disk0 مش متفعله Next وطبعا



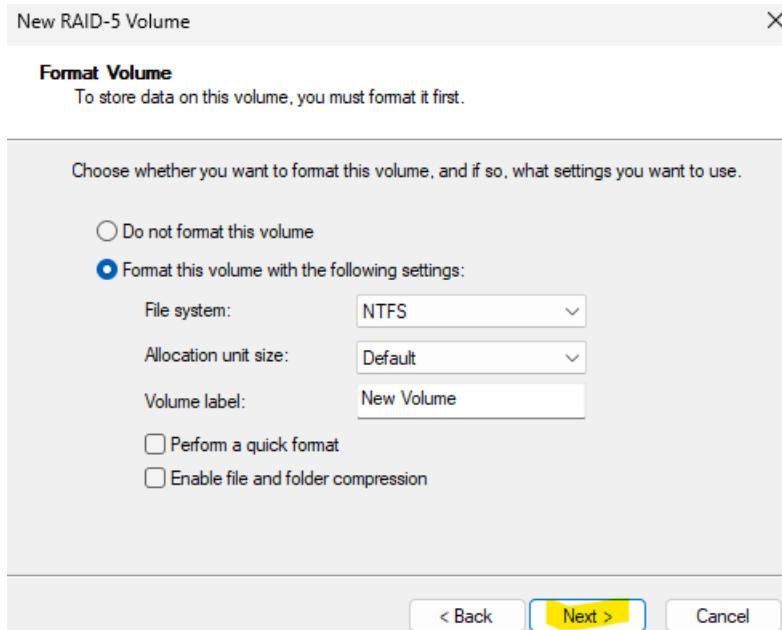
ضفت ال Disk1 بس برضو Next مش متفعله لأن قولنا اقل عدد من ال 3Disks هيكون RAID-5 مع Disk



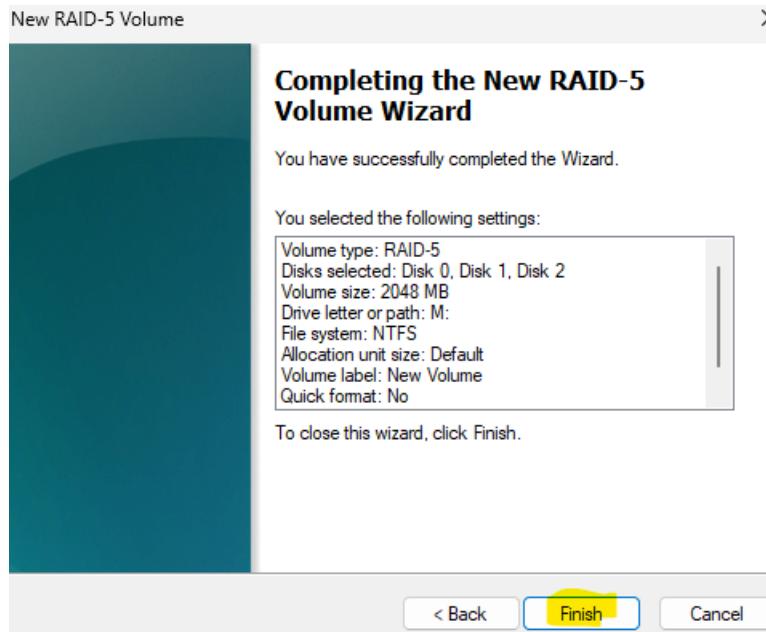
Next



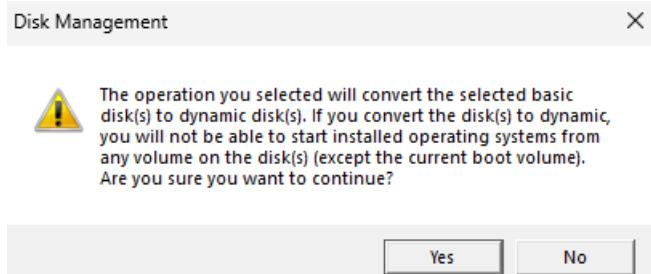
Drive letter ↴



Format



Finish

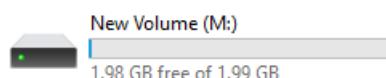


يقولي ان فيه disk basic النوع بتاعه هتحوله ل Dynamic

Yes

Disk 0 Dynamic 100.00 GB Online	New Volume 1.00 GB NTFS Healthy	New Volume 1.00 GB NTFS Healthy	New Volume 1.00 GB NTFS Healthy	New Volume (F) 2.00 GB NTFS Healthy	New Volume (F) 2.00 GB NTFS Healthy	New Volume 1.00 GB NTFS Healthy	New Volume 1.00 GB NTFS Healthy	New Volume 1.00 GB NTFS Healthy	89.00 GB Unallocated
Disk 1 Dynamic 100.00 GB Online	New Volume (I): 1.00 GB NTFS Healthy	New Volume (J): 1.00 GB NTFS Healthy	New Volume (K): 1.00 GB NTFS Healthy	New Volume (M): 1.00 GB NTFS Healthy		96.00 GB Unallocated			
Disk 2 Dynamic 100.00 GB Online	New Volume (M): 1.00 GB NTFS Healthy		99.00 GB Unallocated						
Disk 3 Basic 1023.98 GB Online	100 MB Healthy (EFI System Partition)	(C) 1023.23 GB NTFS Healthy (Boot, Page File, Crash Dump, Basic Data Partition)					674 MB Healthy (Recovery Part)		
CD-ROM 0 DVD 5.60 GB Online	SSS_X64FREE_EN-US_DV9 (D): 5.60 GB UDF Healthy (Primary Partition)								
	<input checked="" type="checkbox"/> Unallocated	<input type="checkbox"/> Primary partition	<input type="checkbox"/> Simple volume	<input type="checkbox"/> Spanned volume	<input type="checkbox"/> Striped volume	<input type="checkbox"/> RAID-5 volume			

بقا عندي واحد 1GB من Disk0 و 1GB من Disk1 و 1GB من Disk2 Partition M



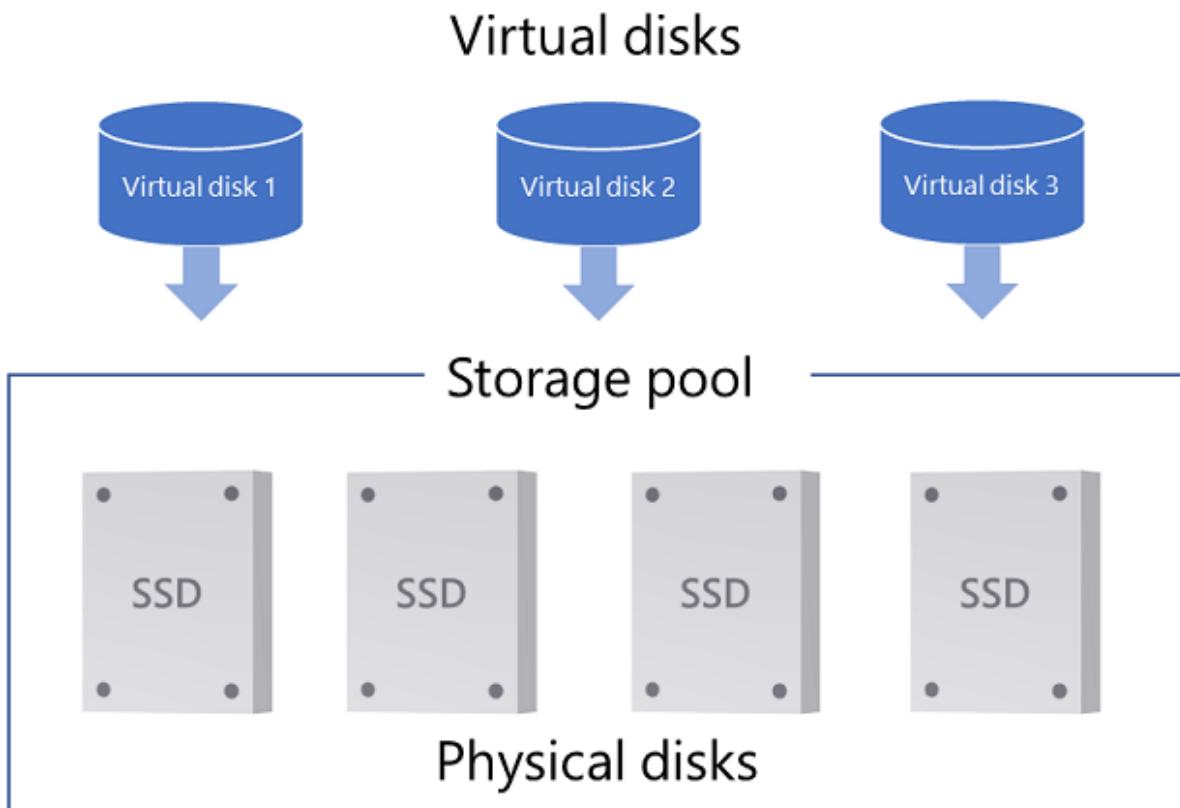
قولنا المساحة بتظهر بمجموع ال Disks الا ال disk ال بيكتب عليه ال parity

و بما ان كل disk مساحته 1GB يبقى ال هيظهروا 2GB

Storage Space

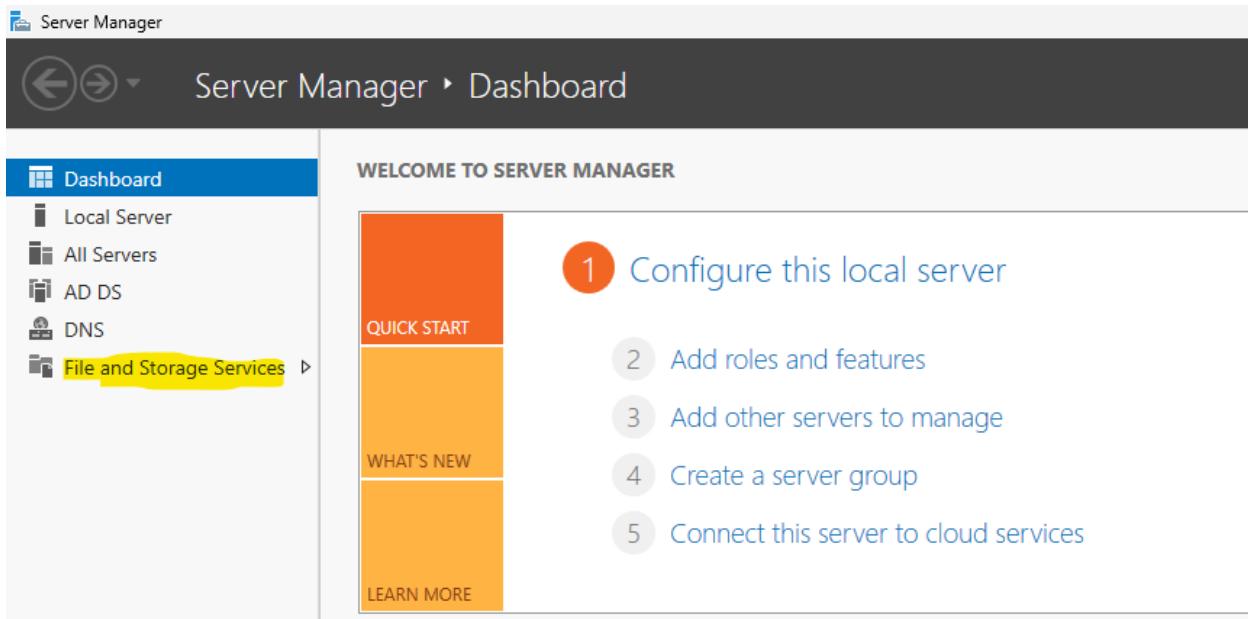
فكرة اني بجمع اكتر من disk في virtual volume

وال فكرة هي اني بجمع ال storage pool في physical disk ومن ال storage pool اعمل virtual disk ، ومش شرط يكونوا بنفس المساحة يعني ممكن يكون 500 disk create في 200 عادي



طيب ازاي ابدا استخدمه ؟

ولا لازم ال disk يكون unallocated يعني لسه متقسمش لاي partitions

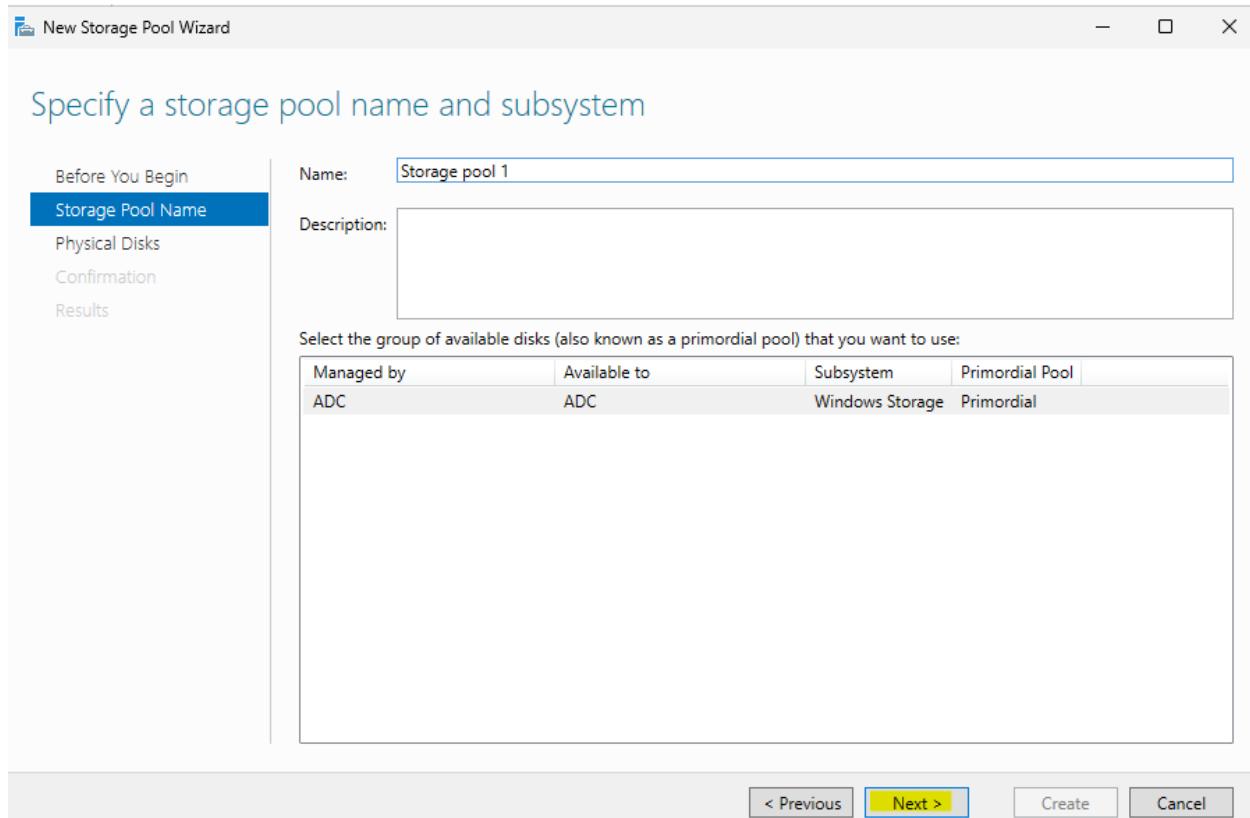


من ال هختار server manager

Name	Type	Managed by	Available to	Read-Write Server	Capacity	Free Space	Percent Allocated	Status
Windows Storage (1)	Primordial	Available Disks: ADC	ADC	ADC				

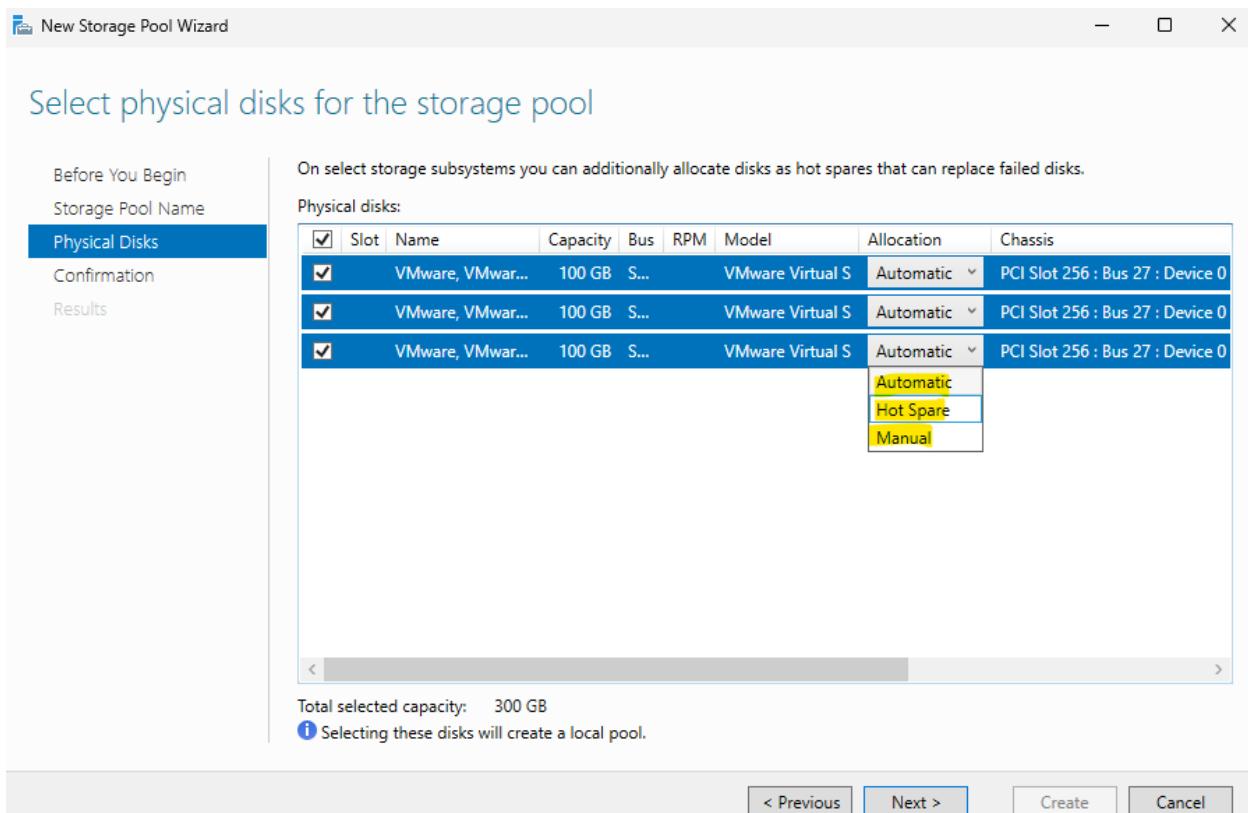
Slot	Name	Status	Capacity	Bus	Usage	Chassis
VMware, VMware Virtual S (ADC)	100 GB	SAS	Automatic	PCI Slot 256 : Bus 27 : Device 0 : Function 0		
VMware, VMware Virtual S (ADC)	100 GB	SAS	Automatic	PCI Slot 256 : Bus 27 : Device 0 : Function 0		
VMware, VMware Virtual S (ADC)	100 GB	SAS	Automatic	PCI Slot 256 : Bus 27 : Device 0 : Function 0		

فتح ال هلاقی عندي pool اسمها click هضغط على New Storage Pool



هڪتب Storage pool لل name

--



بعد كدا بحدد ال physical disk ال هتكون داخل ال storage pool

في ال allocation 3 type :

Automatic : يعني هيكون داخل ال pool ال بعملها دلوقت وهقدر استخدمه مباشره في عمليات ال read و ال write

Hot Spare : هيكون spare disk بمعنى انه مش هيستغل في ال pool عندي الا لو فيه disk حصل فيه مشكله وخرج برا الخدمه وقتها ال spare disk يدخل مكانه تلقائيا

Manual : شبه ال hot spare لكن هو مش هيستغل بشكل تلقائي لو حصل مشكله في ال disk لازم انت ال تدخل ب ايديك تشغله

On select storage subsystems you can additionally allocate disks as hot spares that can replace failed disks.

Physical disks:

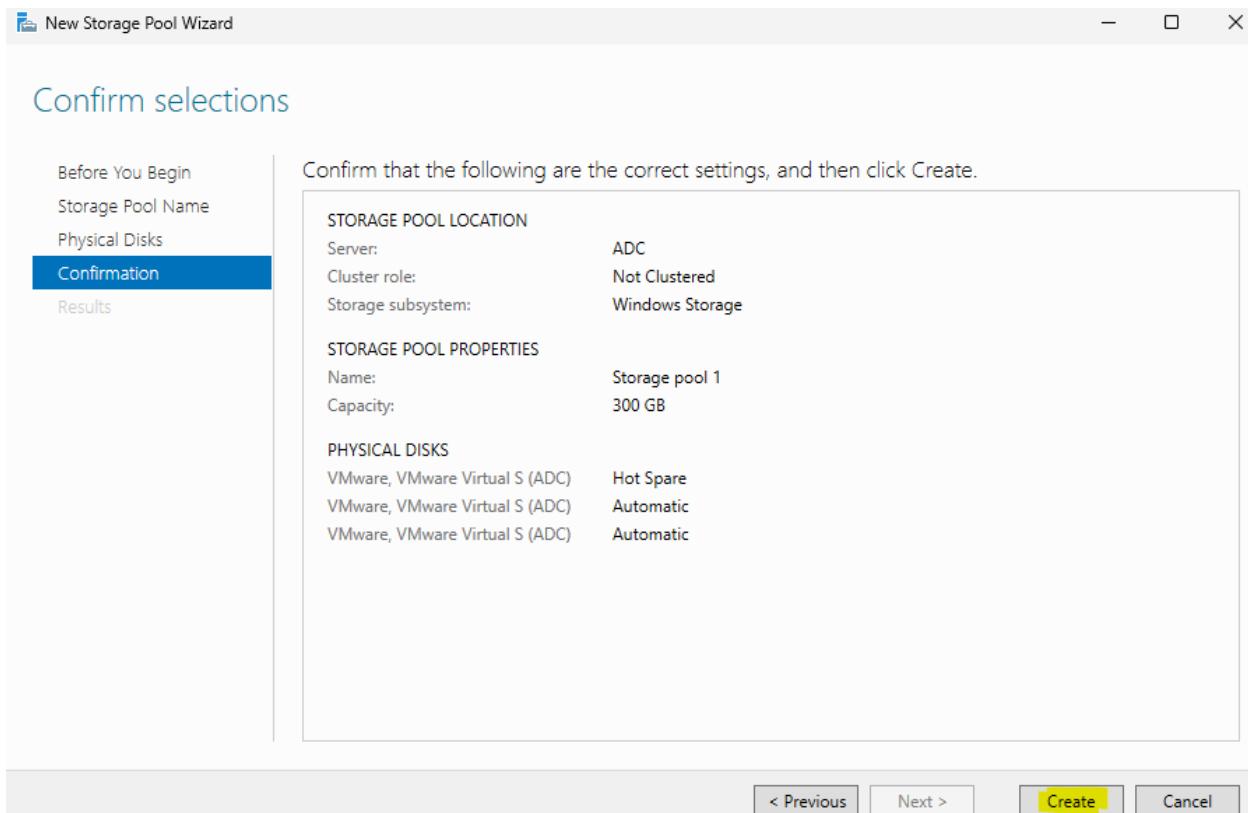
Slot	Name	Capacity	Bus	RPM	Model	Allocation	Chassis
<input checked="" type="checkbox"/>	VMware, VMwar...	100 GB	S...		VMware Virtual S	Automatic	PCI Slot 256 : Bus 27 : Device 0
<input checked="" type="checkbox"/>	VMware, VMwar...	100 GB	S...		VMware Virtual S	Automatic	PCI Slot 256 : Bus 27 : Device 0
<input checked="" type="checkbox"/>	VMware, VMwar...	100 GB	S...		VMware Virtual S	Hot Spare	PCI Slot 256 : Bus 27 : Device 0

Total selected capacity: 300 GB

 Selecting these disks will create a local pool.

هذا هو hot spare واحد

--



بعد كدا هنعمل create
وبكدا عملنا ال Storage pool

--
طيب دلوقت عاوزين نبدا نعمل virtual disk

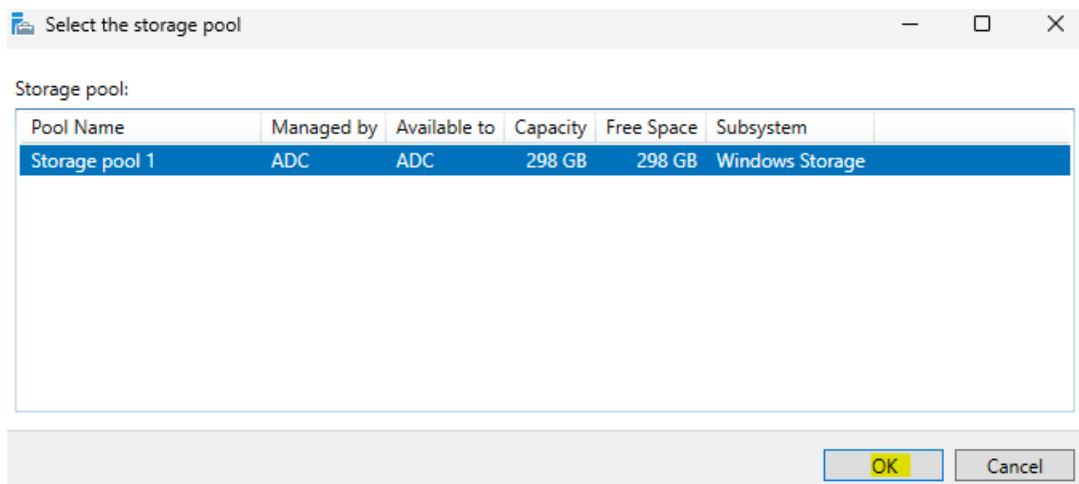
Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders

STORAGE POOLS
All storage pools | 1 total

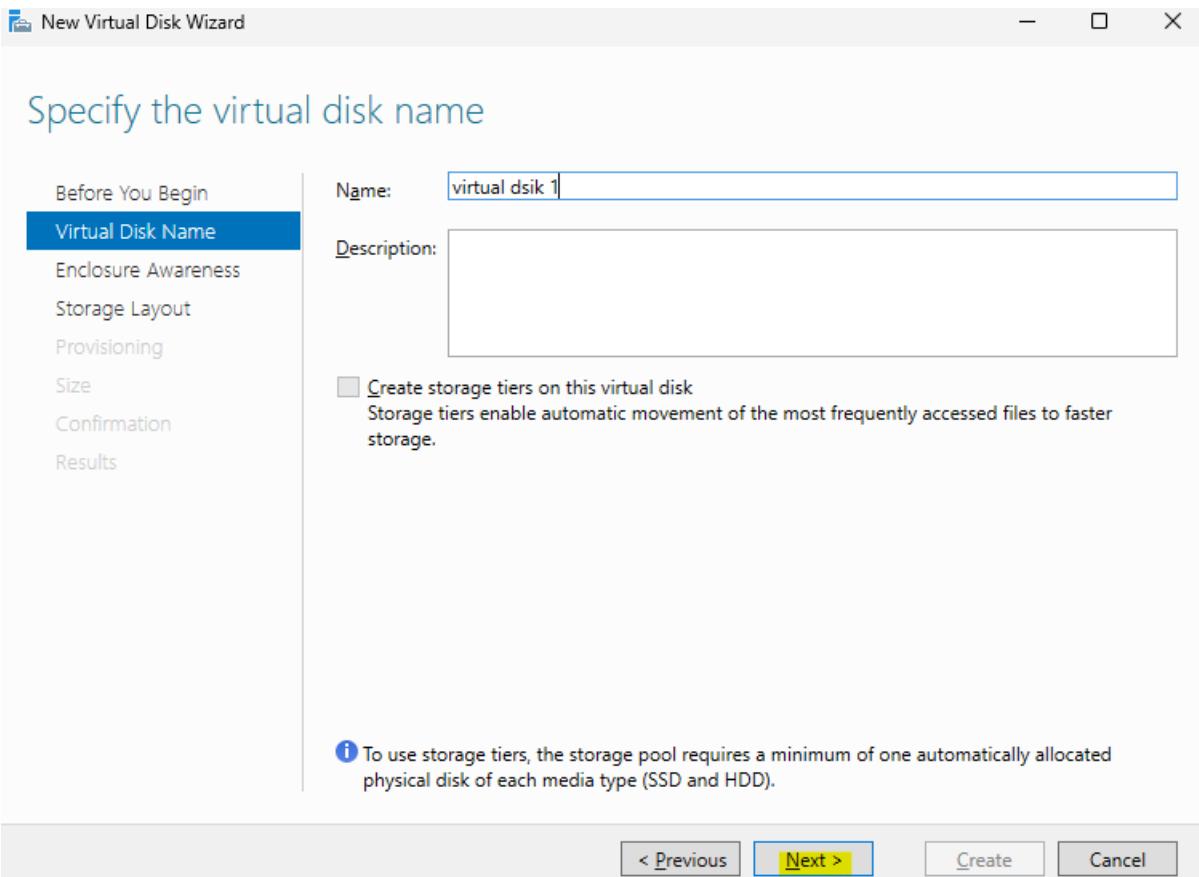
Name	Type	Managed by	Available
Windows Storage (1)	Storage pool	ADC	ADC
Storage pool 1	Storage Pool	ADC	ADC

Last refreshed on 3/16/20

علي ال storage pool وختار New virtual Disk Click

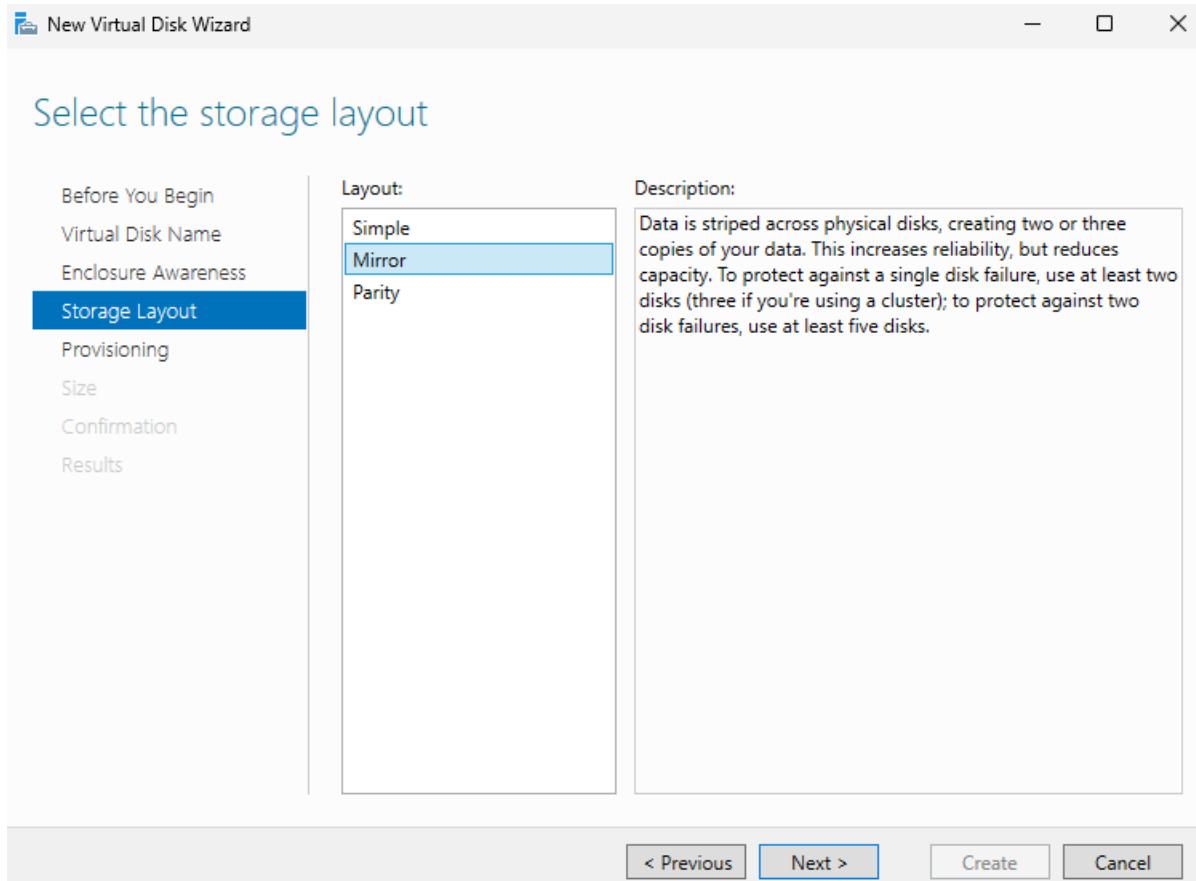


حدد ال pool و ok



Next ٿم next ٿم virtual disk ڦل Name

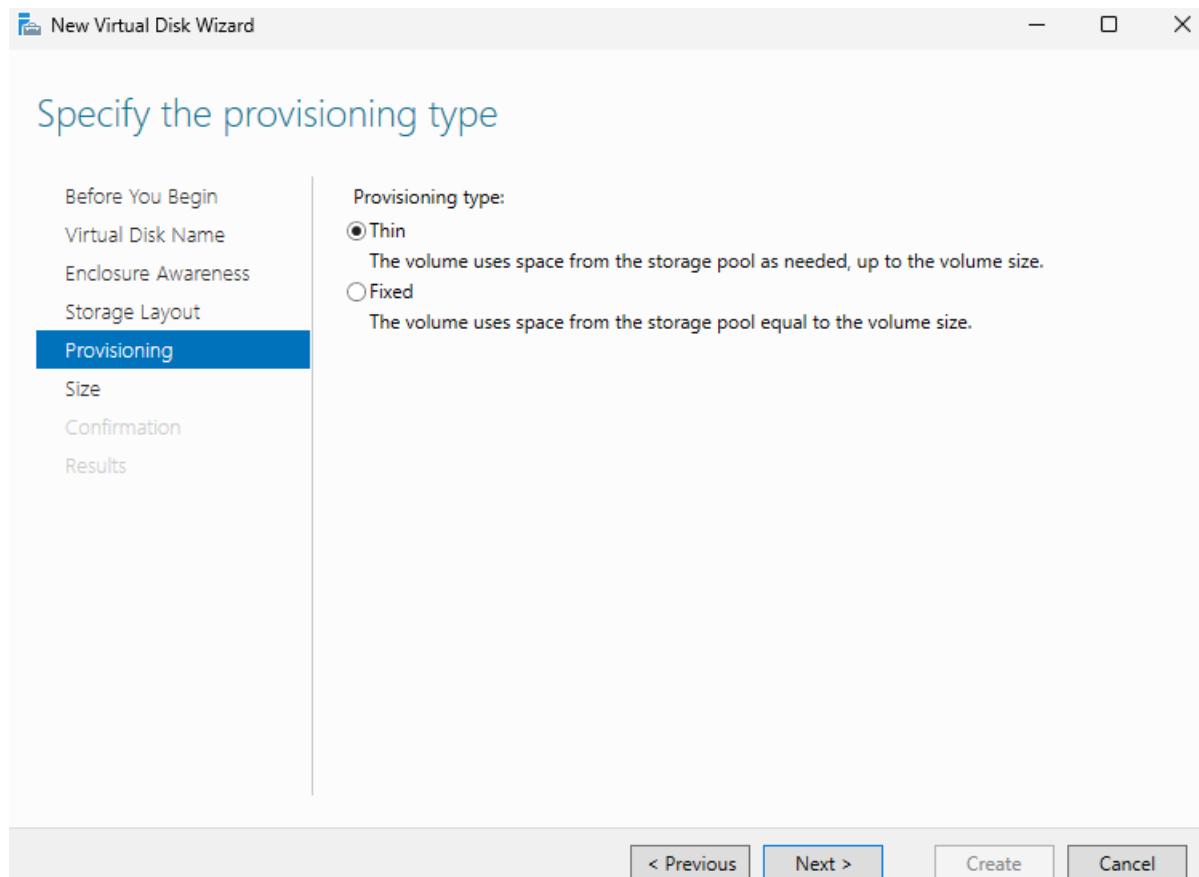
--



بحد ال storage layout ودي طريقة تنظيم البيانات على ال physical disk داخل ال RAID-5 pool وعندنا اكتر من نوع : simple – mirror

فهختار Next واضغط Mirror

--

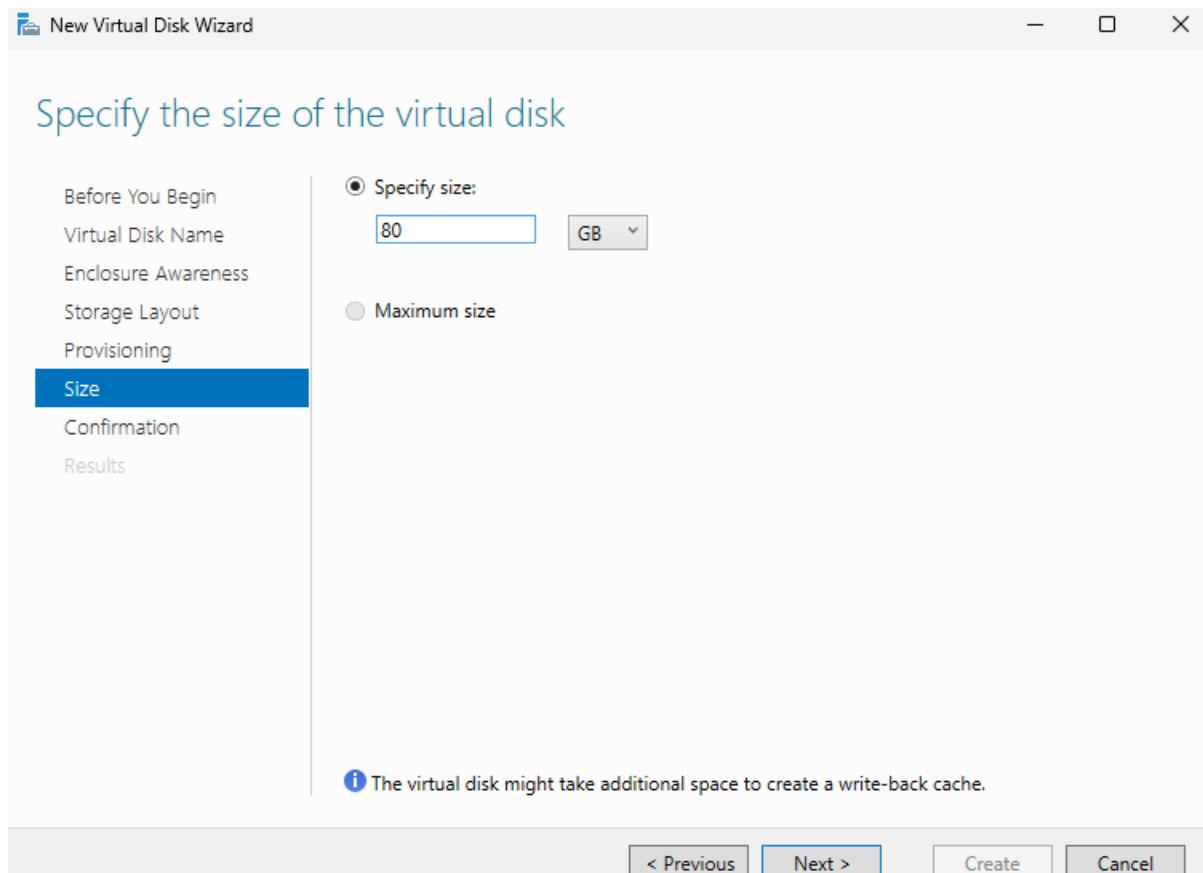


هنا هحدد نوع ال provisioning type وعندنا نوعين :

: ودا المساحه هتبدا ب صفر ويبدا تزيد كل ما اكتب data لحد ما اوصل للحجم ال انا هحددها في الخطوه ال بعدها

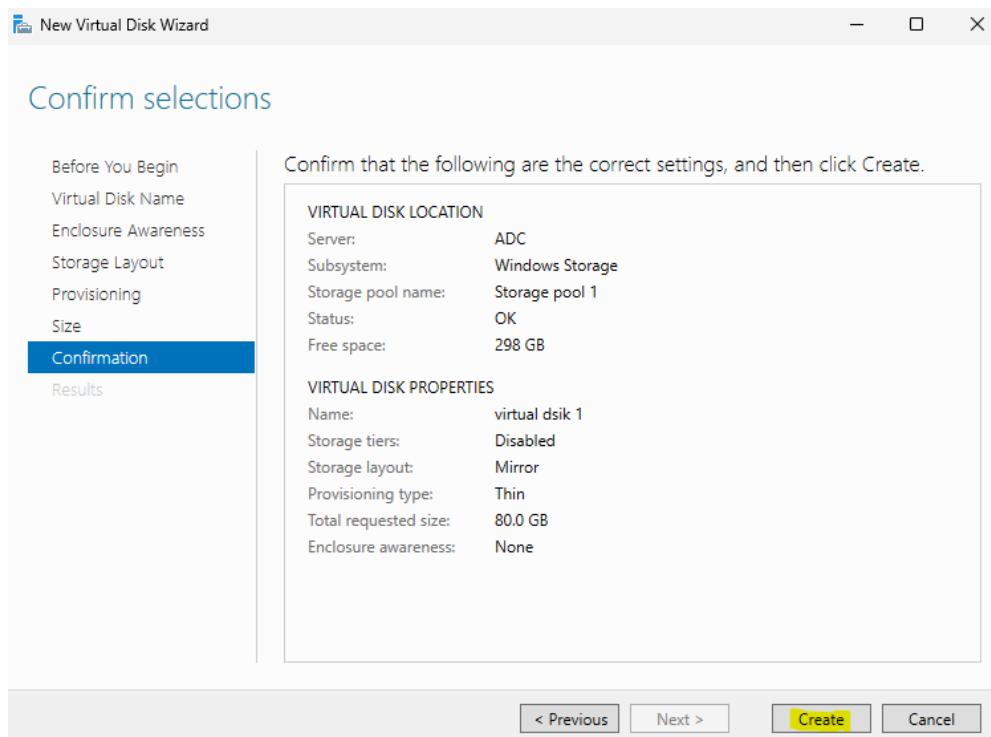
: ودا معناه اننا من البدايه بحجز مساحه معينه من ال disk سواء استخدمناها او لا

--



يحدد size

--



Create

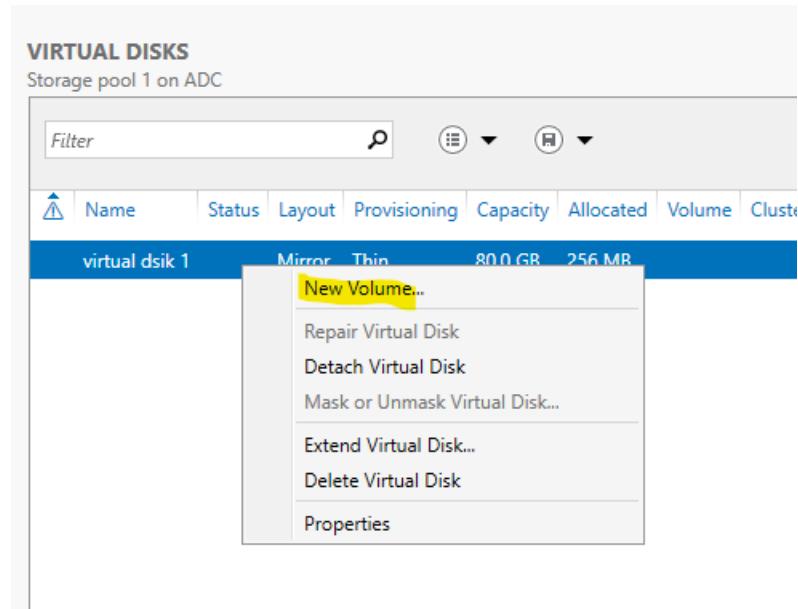
Name	Type	Managed by	Available to	Read-Write Server	Capacity	Free Space	Percent Allocated	Status
Storage pool 1	Storage Pool	ADC	ADC	ADC	298 GB	295 GB		

Name	Status	Layout	Provisioning	Capacity	Allocated	Volume	Clustered	Tiered	Write-Back Cache	Attached
virtual dsik 1	Mirror	Thin	80.0 GB	256 MB		1.00 GB				ADC

Slot	Name	Status	Capacity	Bus	Usage	Chassis
PCI Slot 256 : Bus 27	Device 0 : Function 0	SAS	Automatic			
PCI Slot 256 : Bus 27	Device 0 : Function 0	SAS	Automatic			
PCI Slot 256 : Bus 27	Device 0 : Function 0	SAS	Hot Spare			

هلاقي ال create اتعمله virtual disk عندي

طيب لو عاوز ابدا اعمل `create` ل virtual disk من ال volumes دا ؟



عليه و هختار New Volume Click

--

New Volume Wizard

Select the server and disk

Before You Begin

Server and Disk

Size

Drive Letter or Folder

File System Settings

Confirmation

Results

Server:

Provision to	Status	Cluster Role	Destination
ADC	Online	Not Clustered	Local

Refresh Rescan

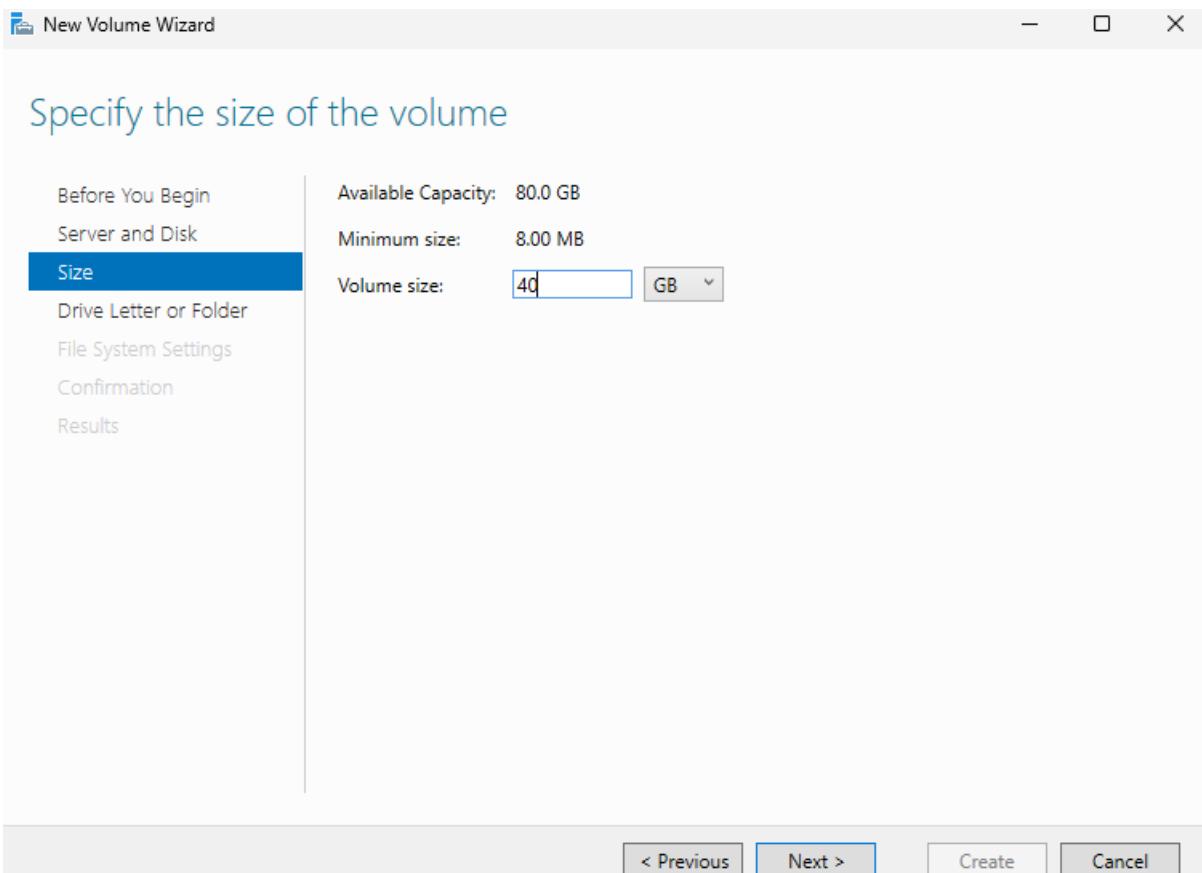
Disk:

Disk	Virtual Disk	Capacity	Free Space	Subsystem
Disk 0		100 GB	100 GB	
Disk 1		100 GB	100 GB	
Disk 2		100 GB	100 GB	
Disk 4	virtual dsik 1	80.0 GB	80.0 GB	Windows Storage

< Previous Next > Create Cancel

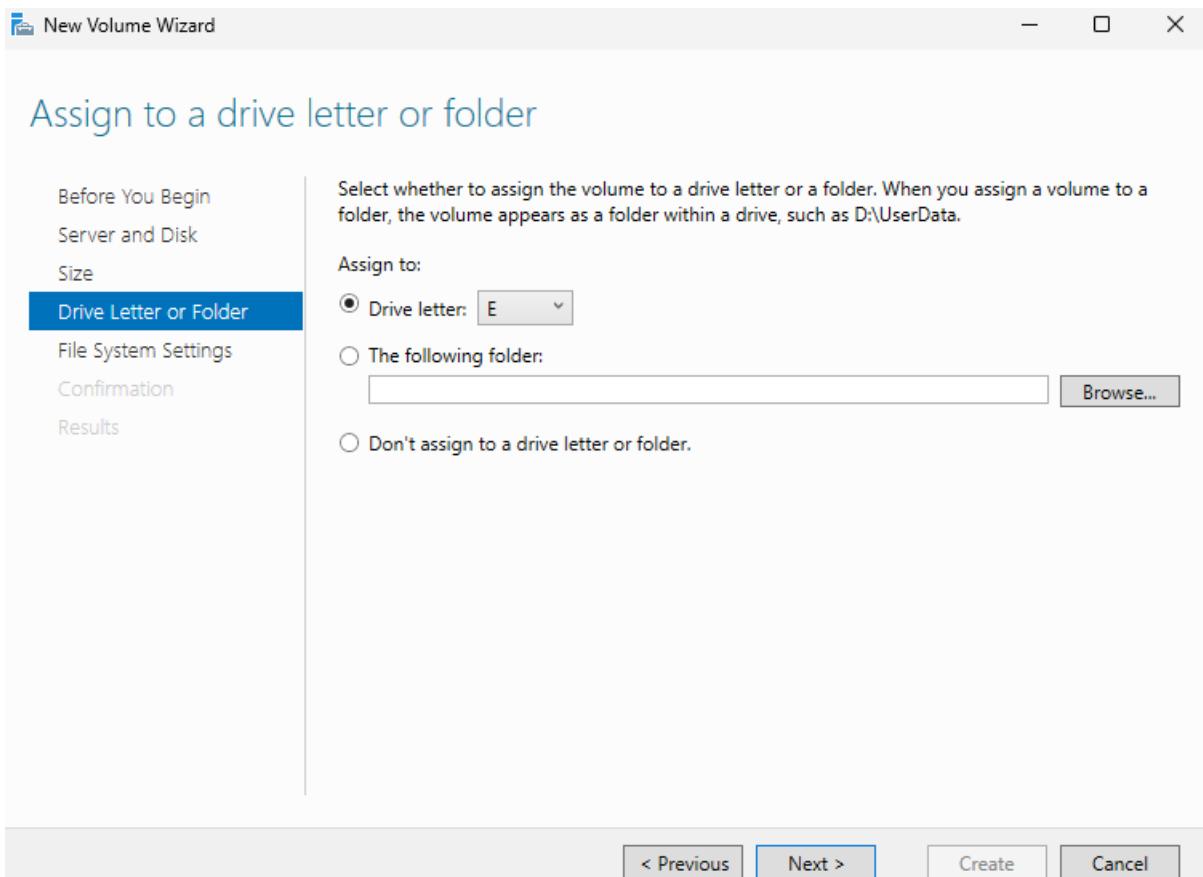
حدد ال virtual disk

--



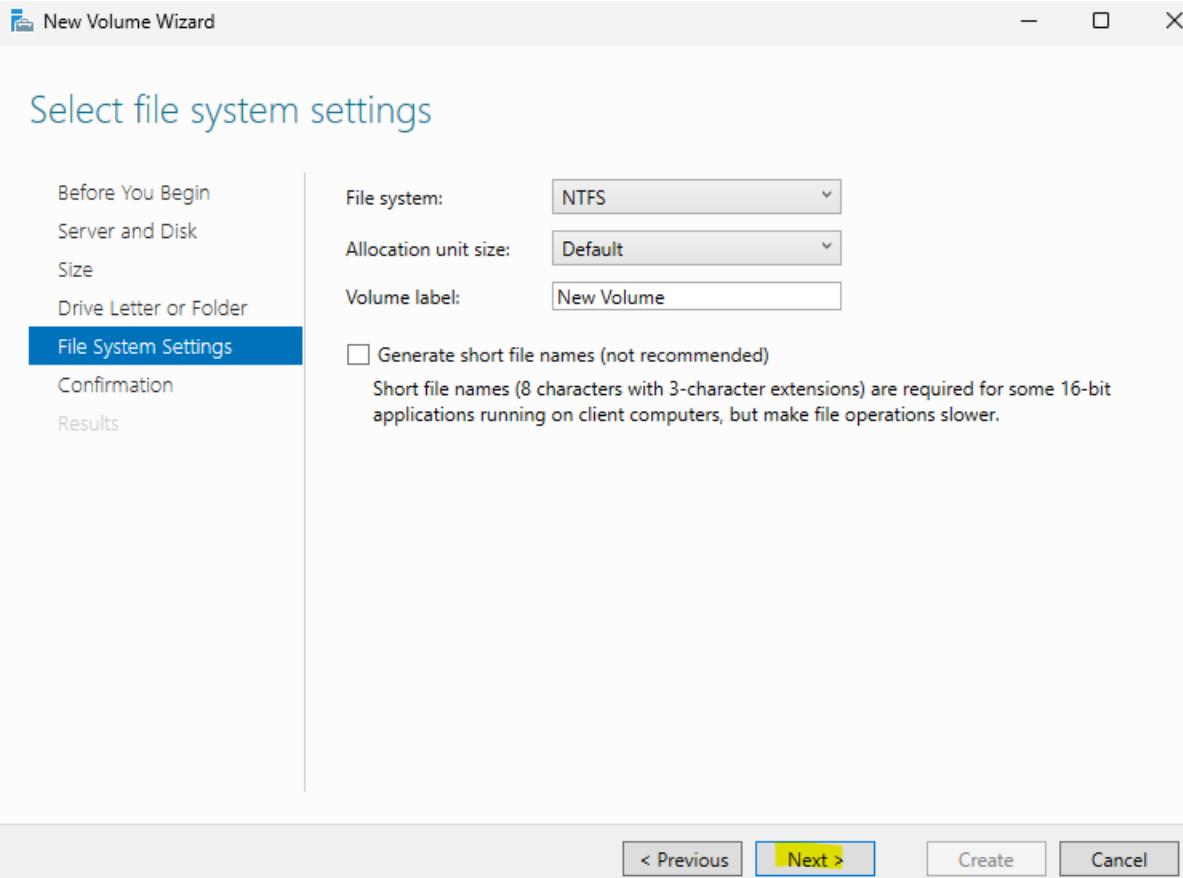
بقوله عاوز اعمل volume بمساحه 40GB

--



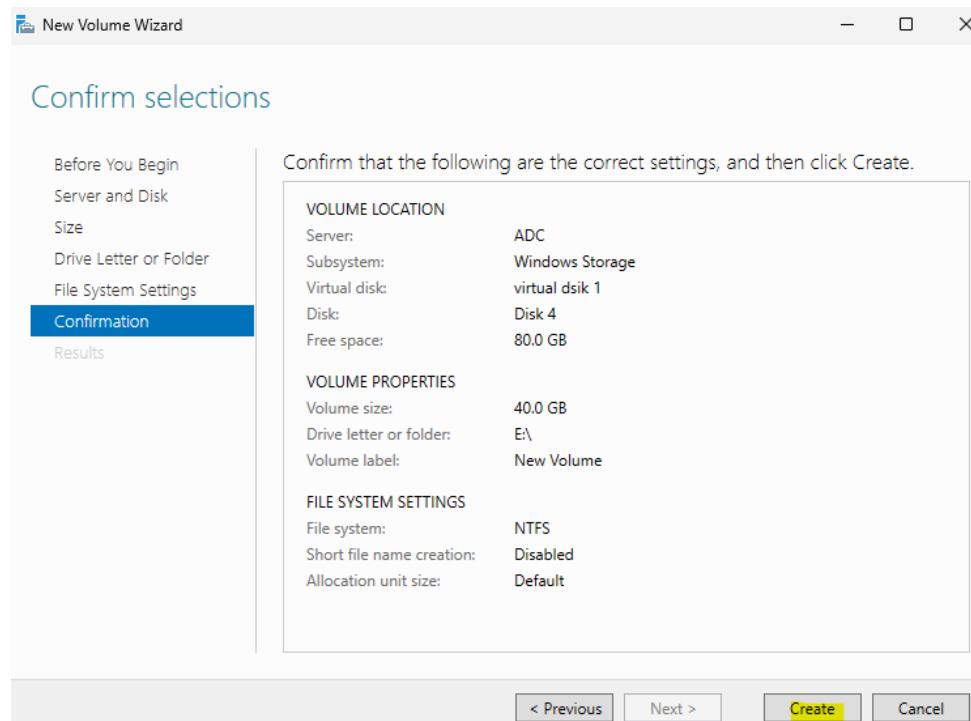
حدد الـ **drive letter**

--

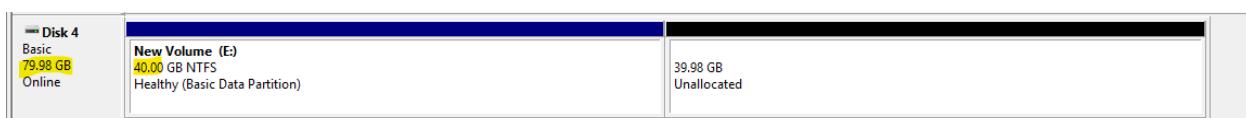


Format

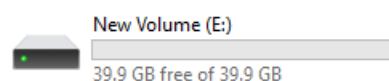
--



Create



لو روحت علي ال disk management هلاقي ال virtual disk ظهر وكانه disk عادي خالص
وقدر اتعامل معه وهلاقي كمان ال partition create ال عملته بمساحه 40GB



ولو روحت علي my computer ظهر معايا وقدر اكتب عليه data واتعامل
معه

iSCSI

هو **TCP/IP** Storage Network Protocol : هو Internet Small Computer System Interface network يُستخدم لنقل بيانات التخزين بين Servers و ال Storage Arrays عبر ال

بيشتعل ازاي ؟

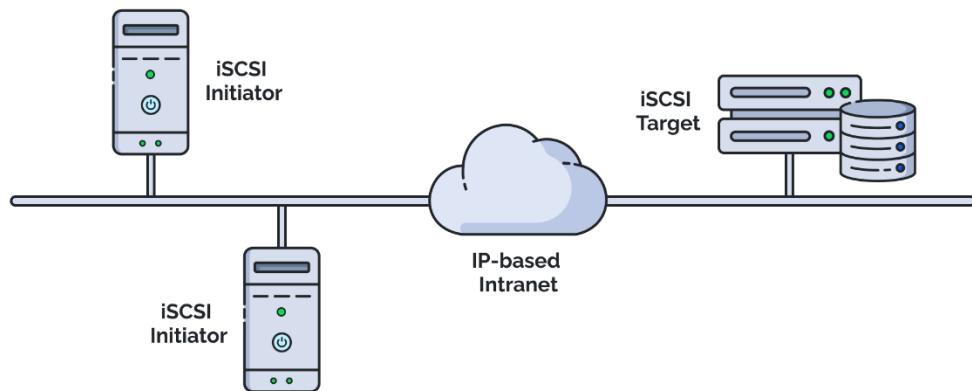
بيكون عندي

iSCSI Initiator -1 : ودا الجهاز الي تحتاج يوصل لـ storage ، ويكون بيعمله software او ان كارت ال iSCSI يدعم ال network

iSCSI Target -2 : دا الجهاز ال عليه ال storage سواء كان server او SAN storage او

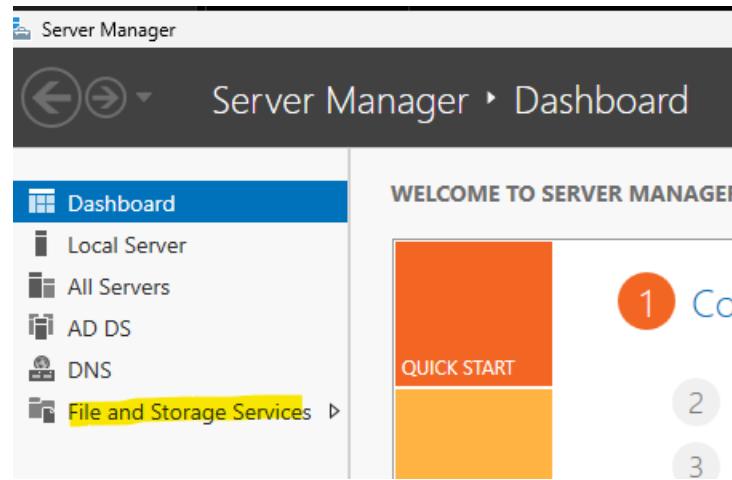
ولما يحصل connect بين ال **Initiator** وال **Target** يتم تخصيص وحدة تخزين لـ **Initiator**

وبيتم نقل البيانات عن طريق ال **TCP/IP**

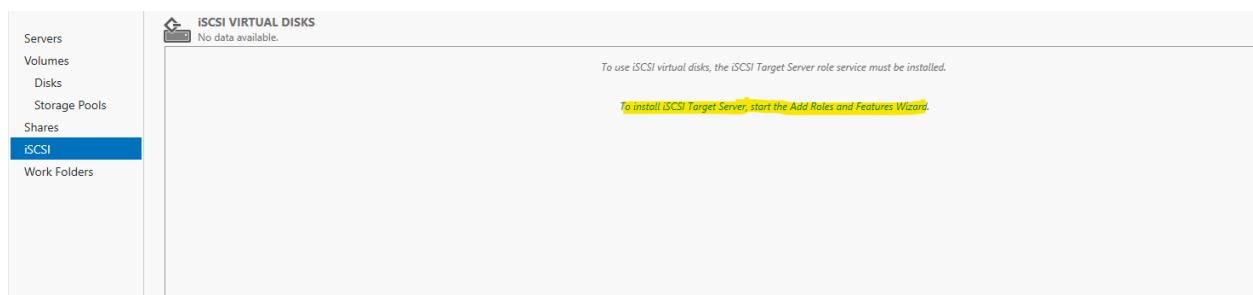


طيب ازاي ابدا استخدمه ؟

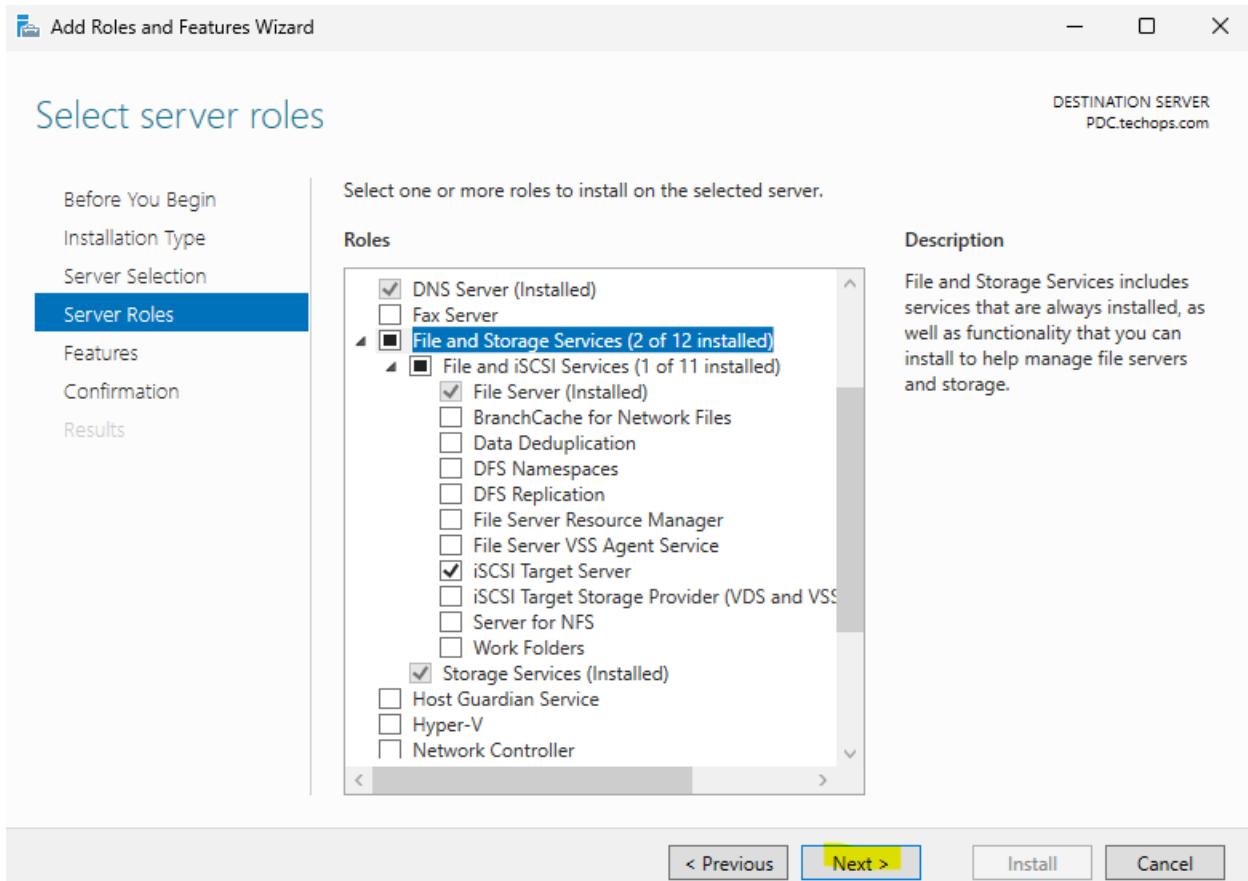
اول حاجه هست طب ال service على ال server



من ال File and Storage Services هروح ع server manager



هتفتح ال iSCSI ، هيقولك لازم تعمل install لـ role الاول ، اضغط على



هيفتح ال wizard دي وهو هيكون عامل Next ، اضغط Next ثم check على iSCSI Target Server ثم Install



بعد ال install العمل create on iSCSI virtual disk

New iSCSI Virtual Disk Wizard

Select iSCSI virtual disk location

iSCSI Virtual Disk Location

- iSCSI Virtual Disk Name
- iSCSI Virtual Disk Size
- iSCSI Target
- Target Name and Access
- Access Servers
- Enable authentication ser...
- Confirmation
- Results

Server:

Server Name	Status	Cluster Role	Owner Node
PDC	Online	Not Clustered	

Information: The list is filtered to show only servers with the iSCSI Target Server role installed.

Storage location:

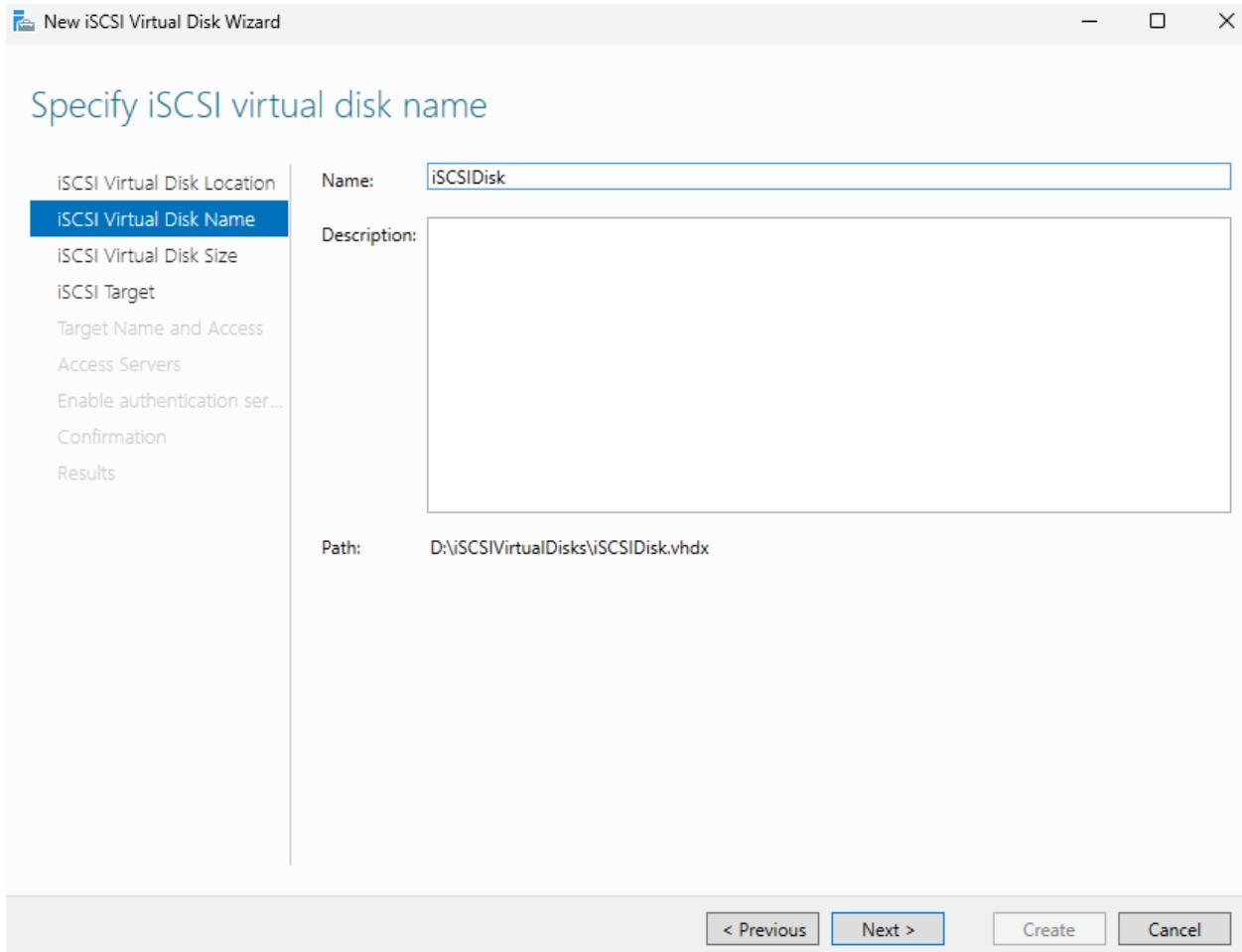
Select by volume:

Volume	Free Space	Capacity	File System
C:	1,001 GB	1,023 GB	NTFS
D:	500 GB	500 GB	NTFS

The iSCSI virtual disk will be saved at \iSCSIVirtualDisk on the selected volume.

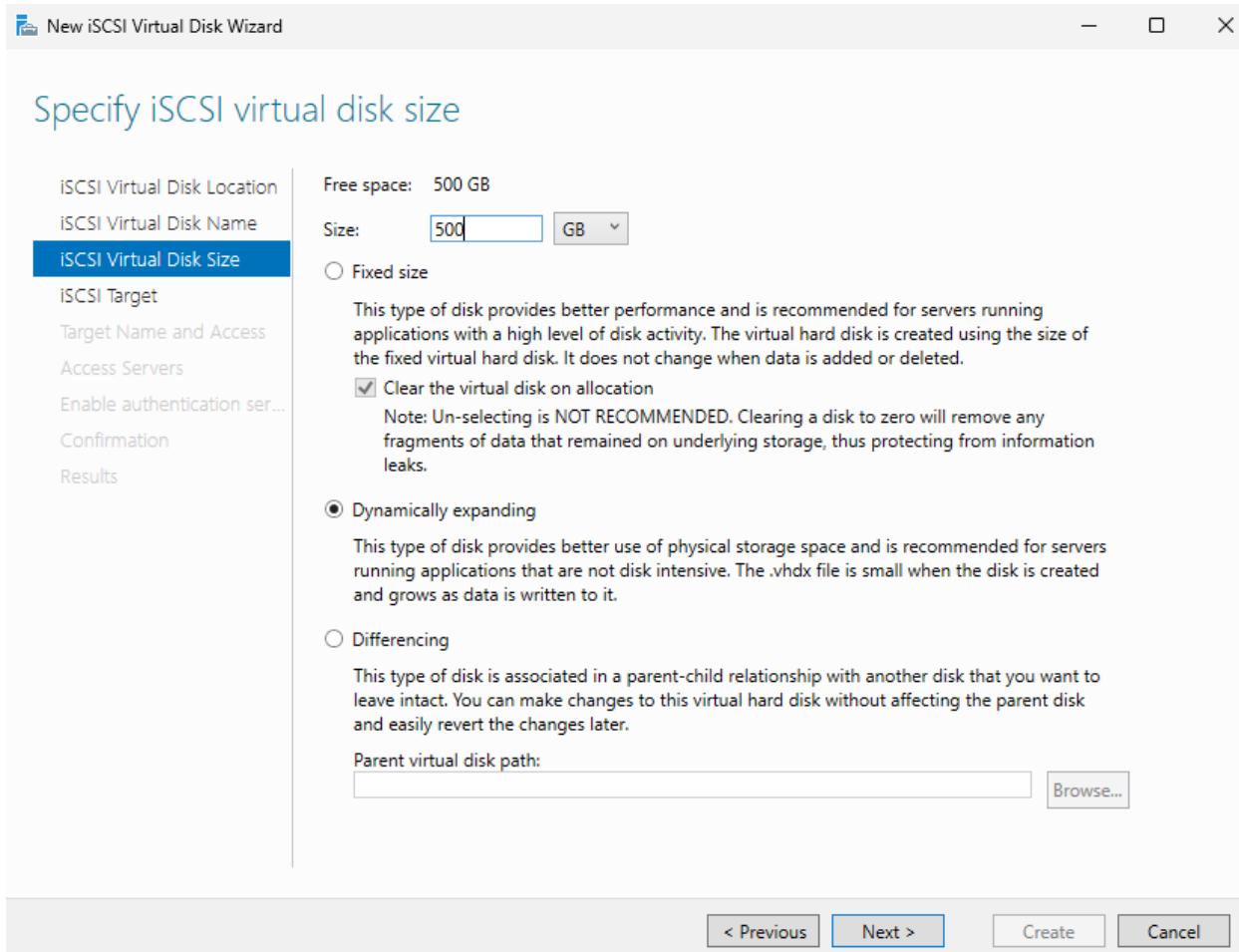
Type a custom path:

حدد ال disk ال هيتعمل منه ال iSCSI



path و ای Name

--

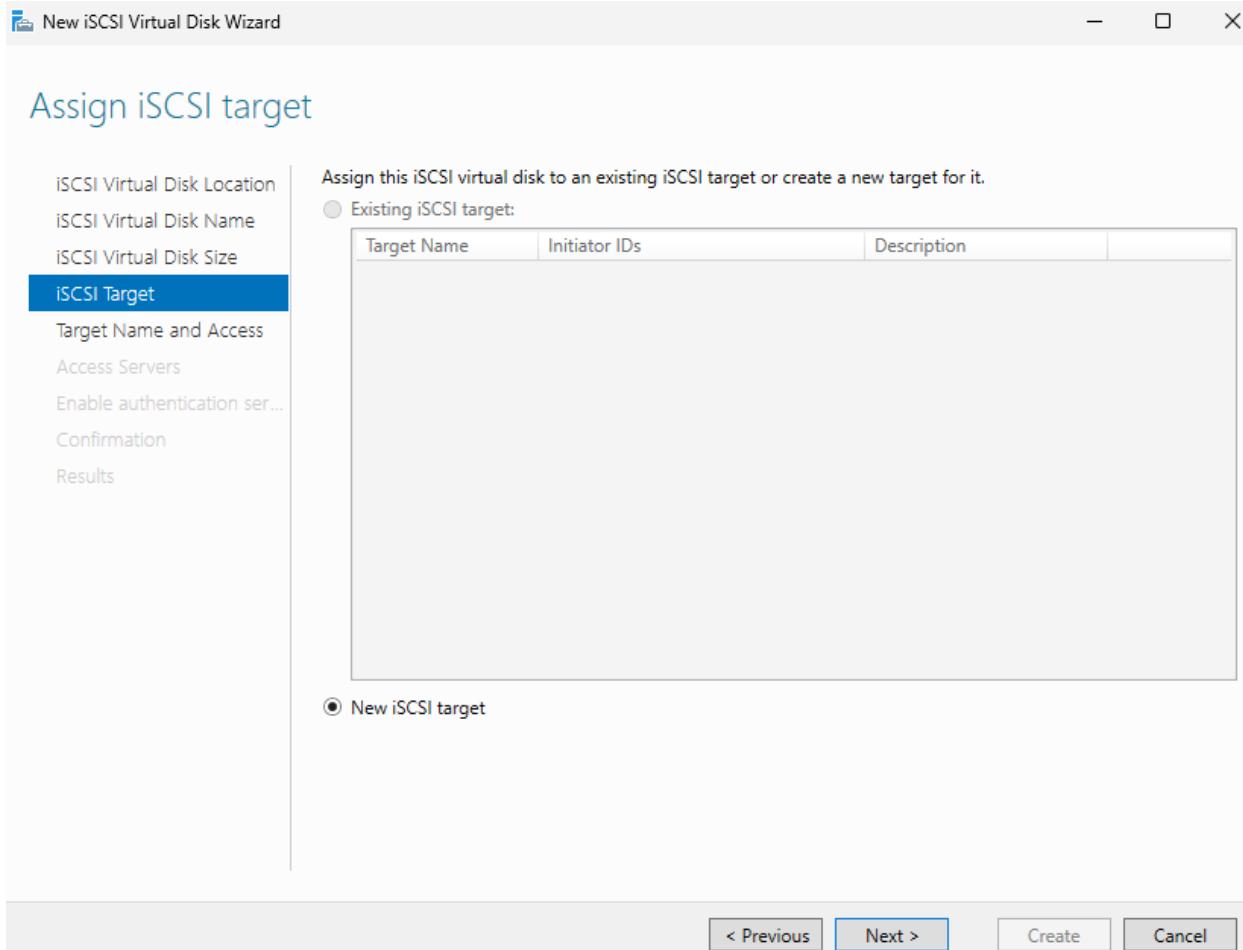


بحد ال space بناعتي

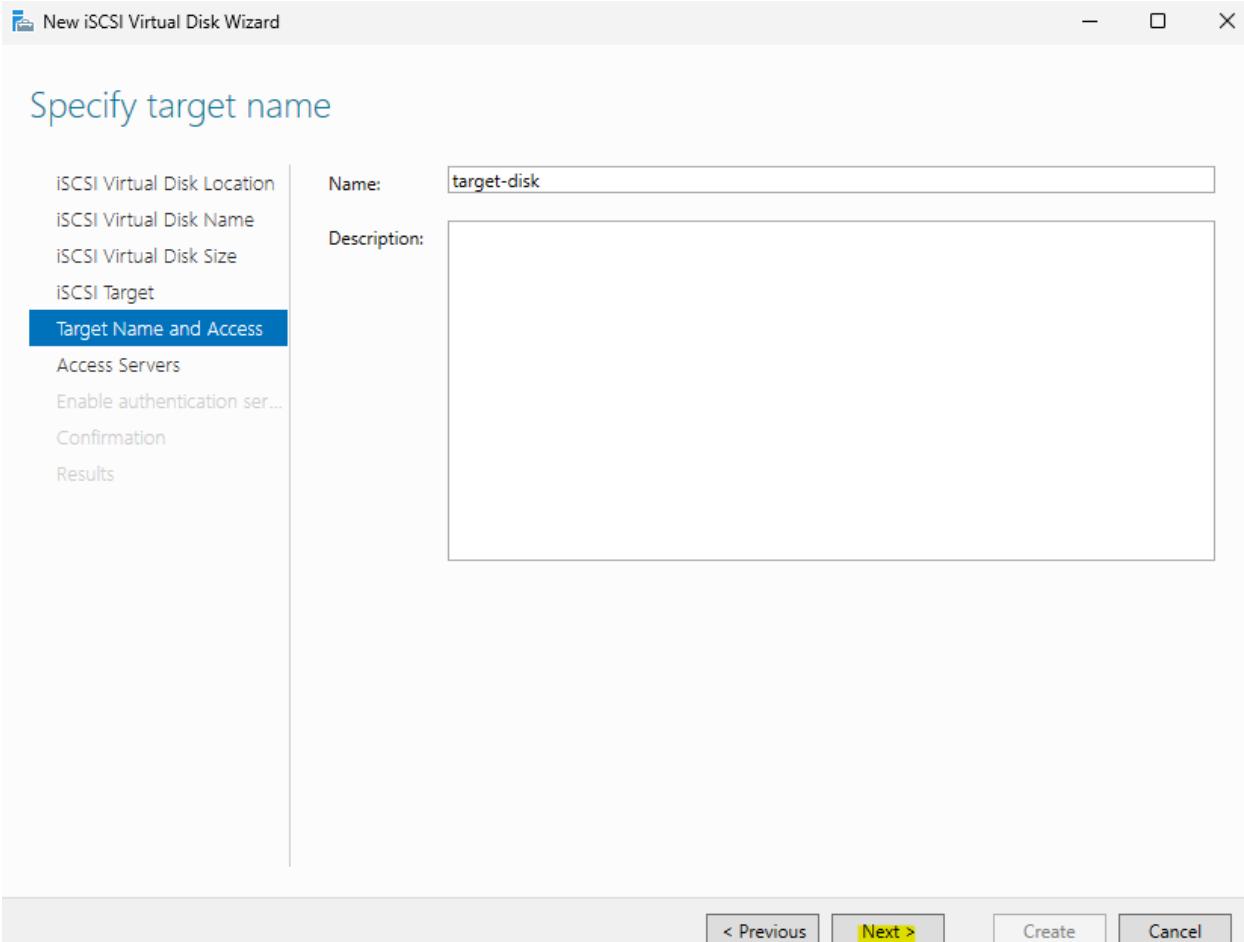
لو اختارت fixed ف هو هيعمل create ل virtual disk ويحجز له المساحة دي حتى لو مستخدماش

لو اختارت Dynamically expanding هبدا ب 0 وكل ما اكتب data عليه هيزيد

--

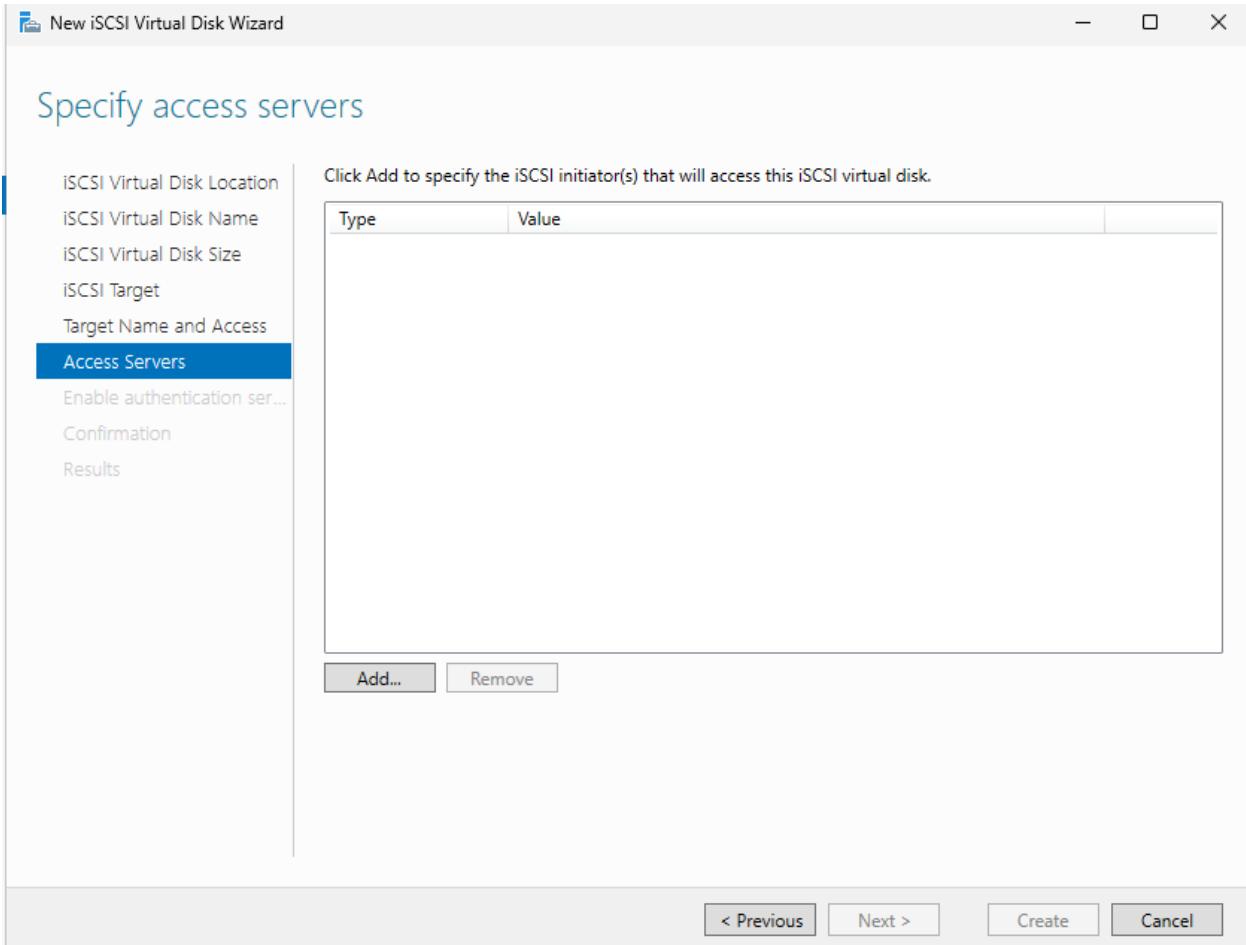


new iSCSI target جهش



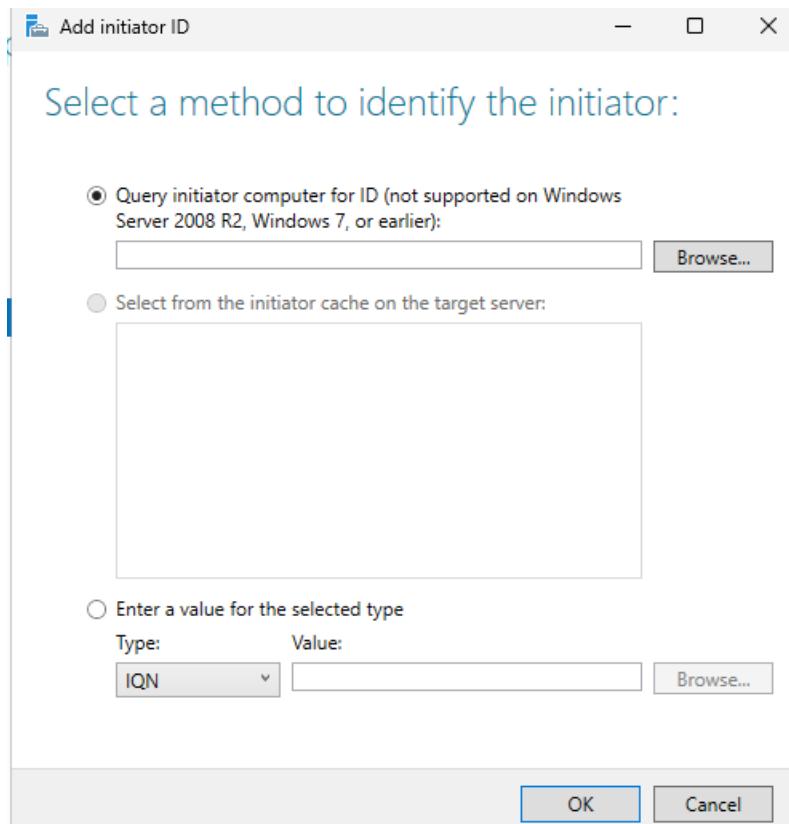
target name

--



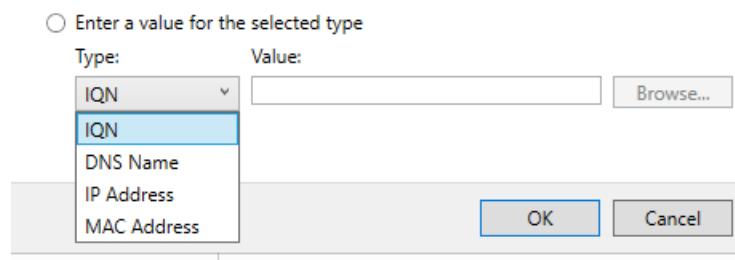
عمل Add لـ initiators

--



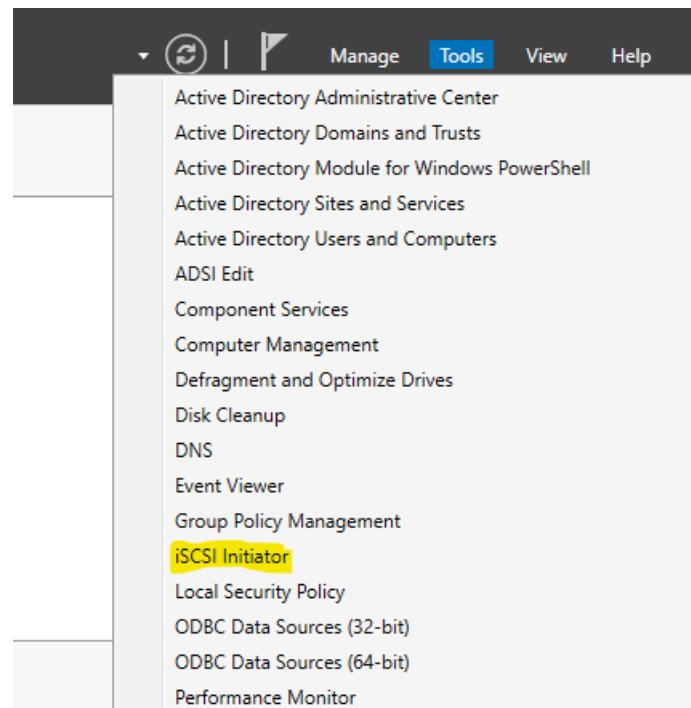
ف اکثر من طریقه : اني اضیفههم من عن طریق ال DC

او من اکثر من نوع تانی ال هما

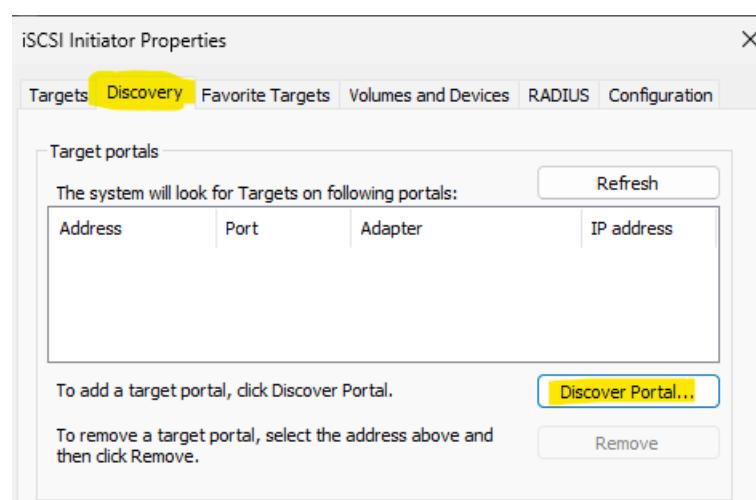


IQN اختصار ل iSCSI qualified name ، او IP او DNS Name او MAC

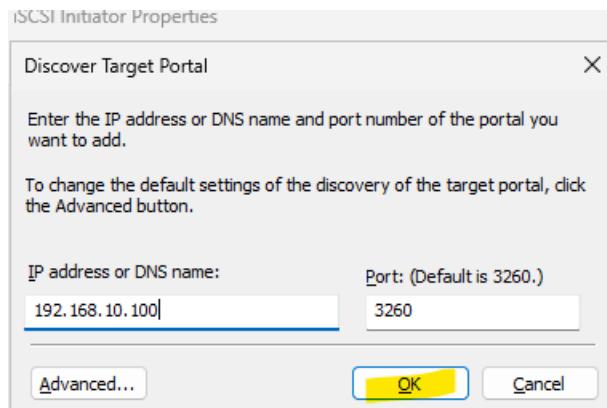
او تالت حاجه وهي ال initiator cache on the target server ودا من خلاله انا ال بروح علي ال target register داخل ال واخليه يعمل



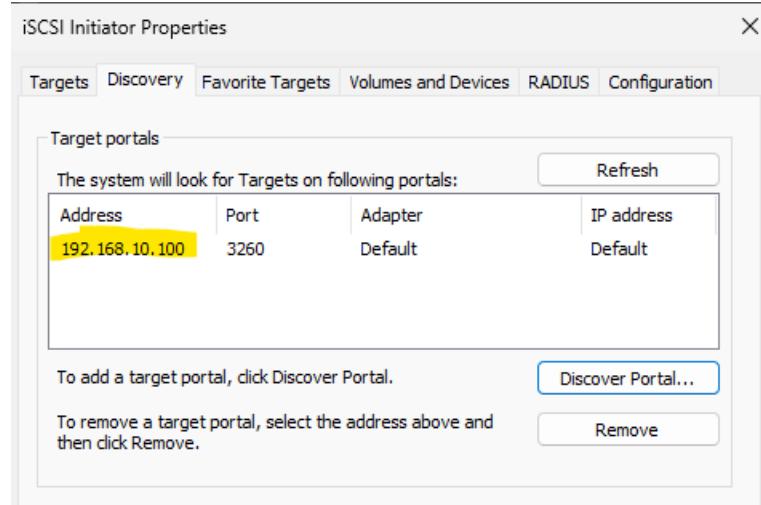
عند ال هفتح ال initiator tools واروح على server manger واختار iSCSI initiator



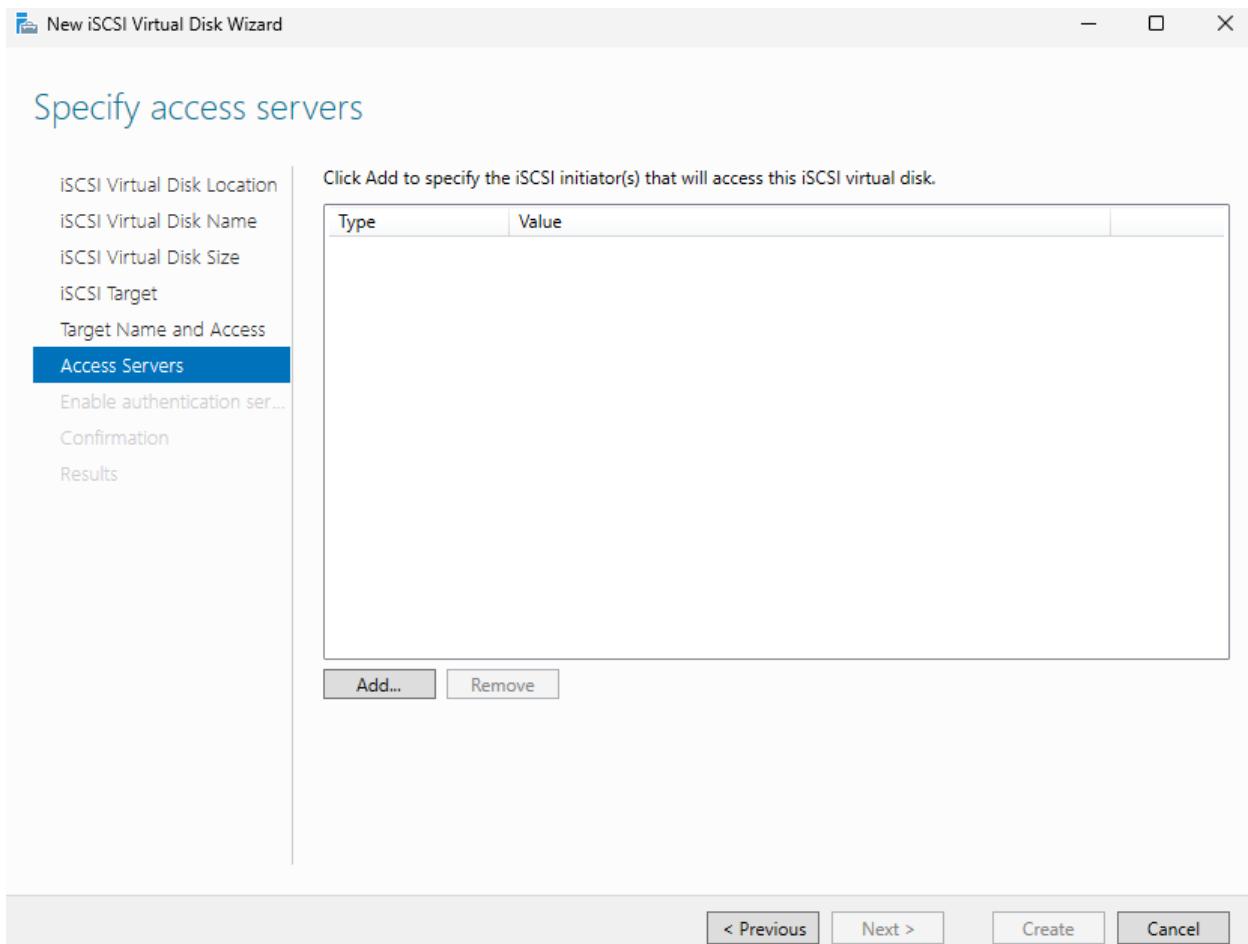
من Discover هفتح ال Discover portal



هكتب ال ip الخاص بال target

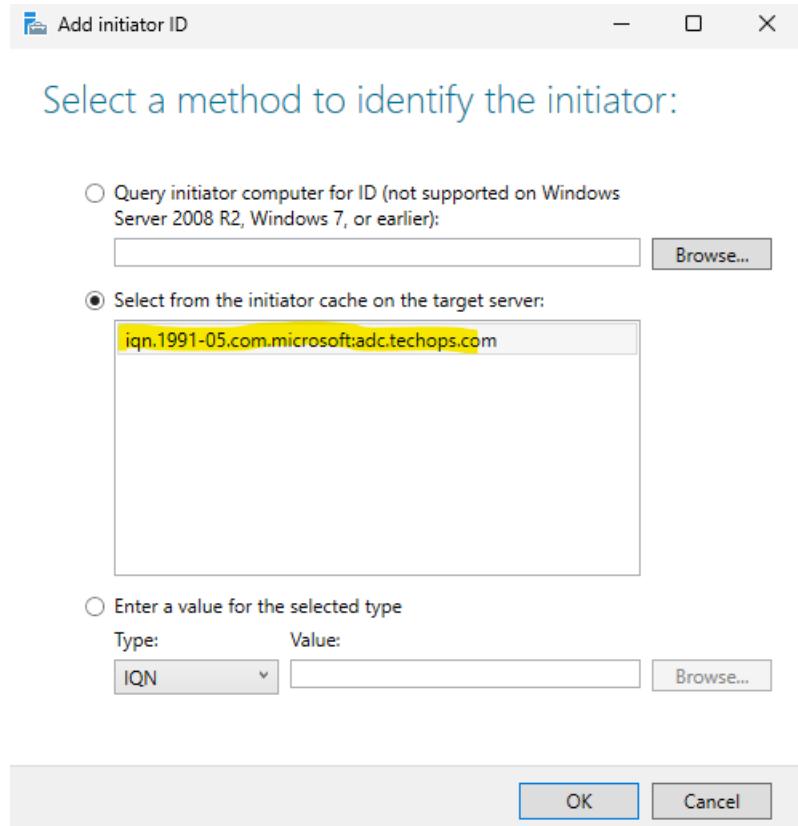


هلاقیه ظهر عندي



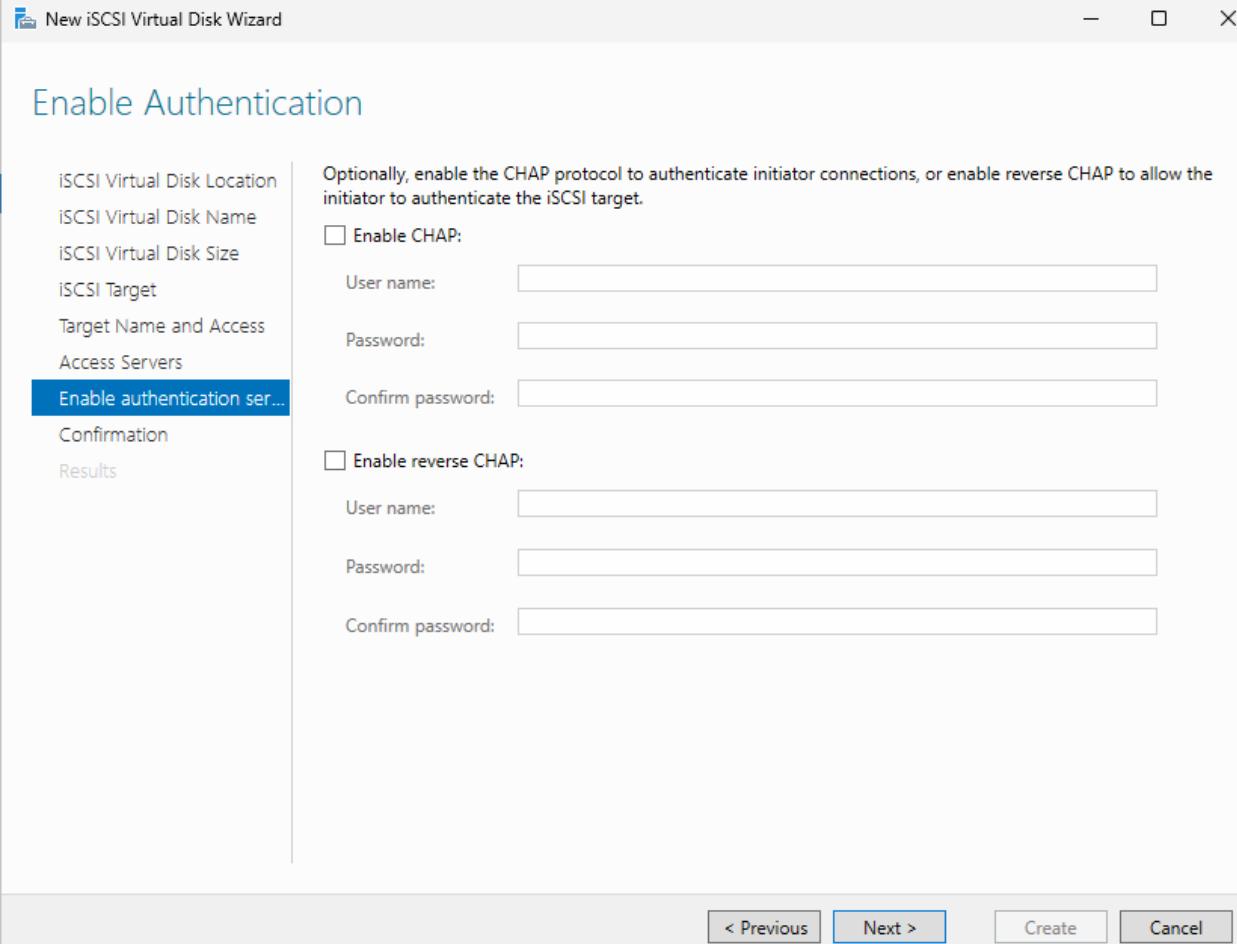
على ال target هروح امشي الخطوات واعمل add

--



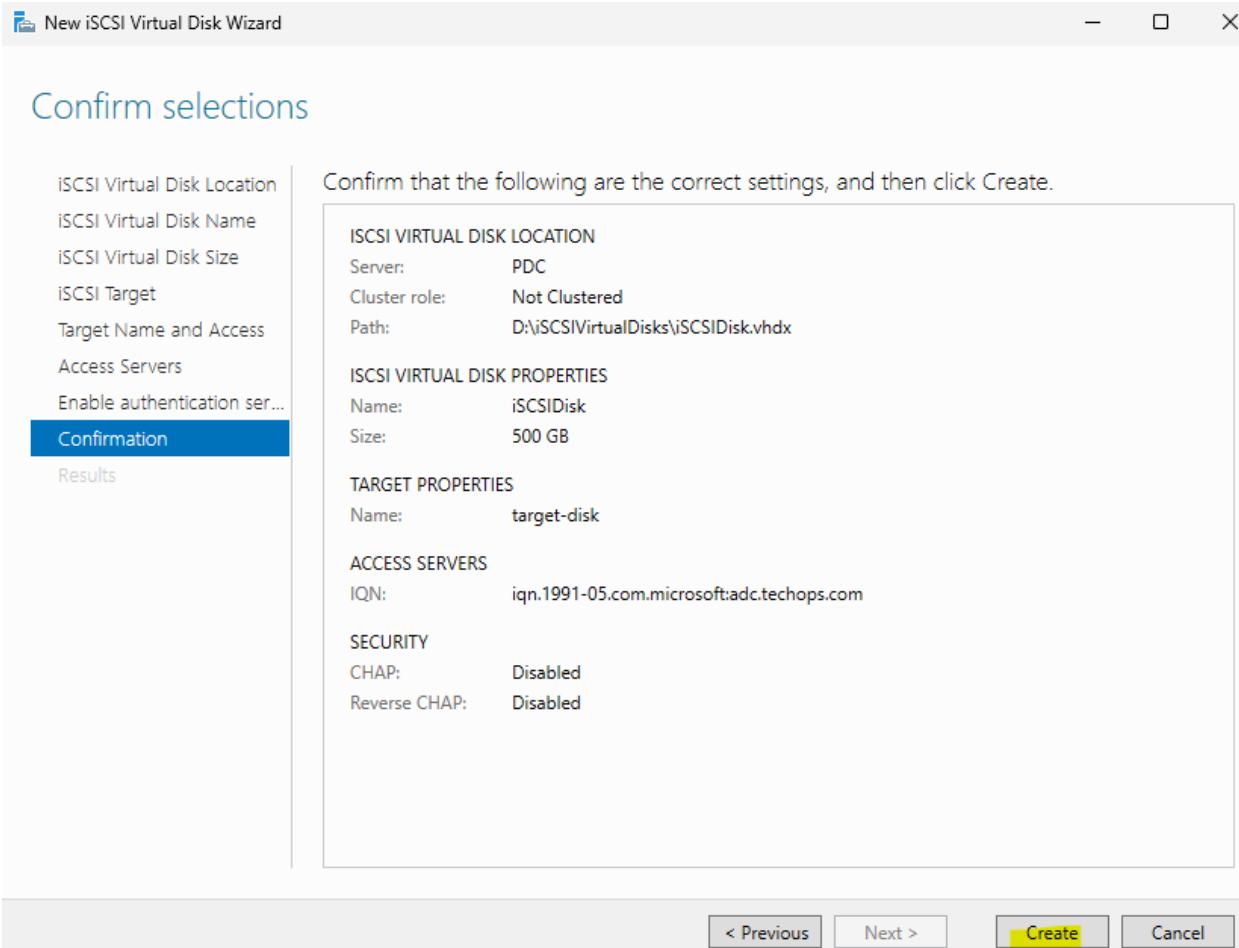
هتلافي ال initiator ظهر معایاف هو دا ال هختاره

--

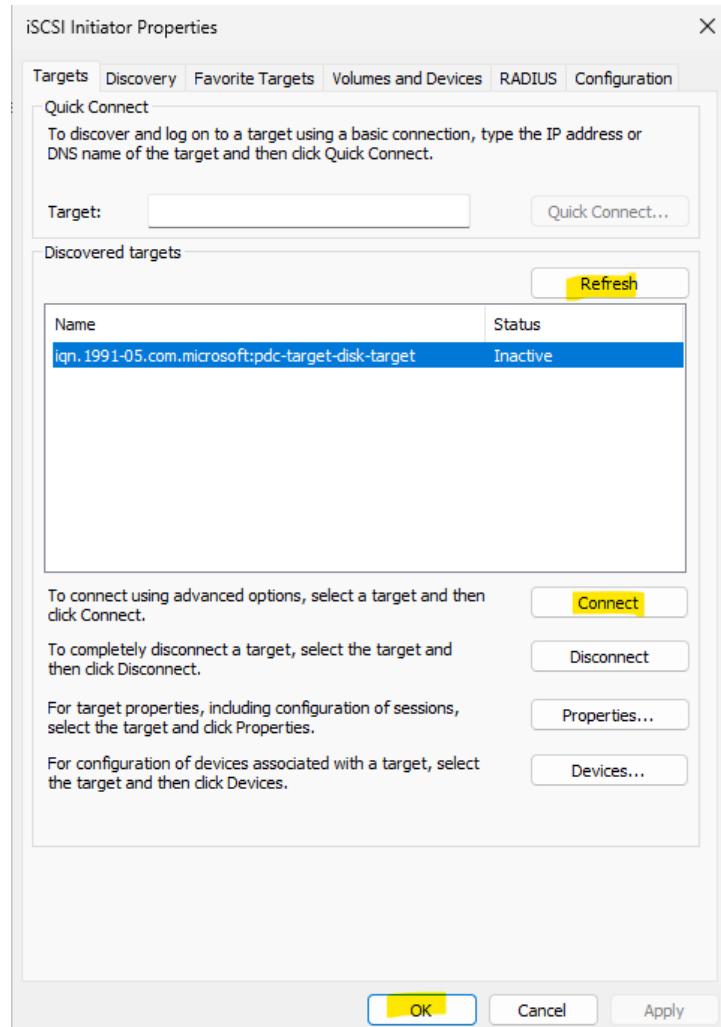


دي لو عاوز افعلاً auth عشان لما ال initiator يجي ينضم لـ target بطلب منه username and password

--

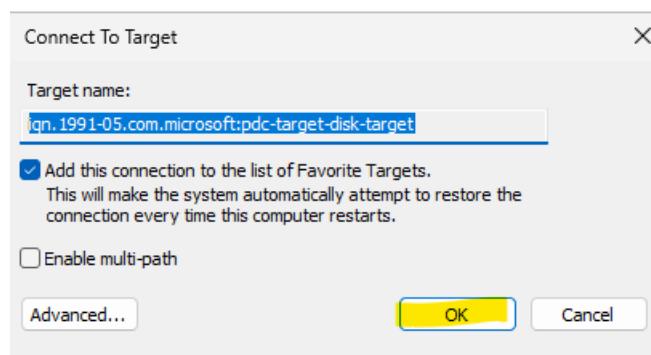


Create

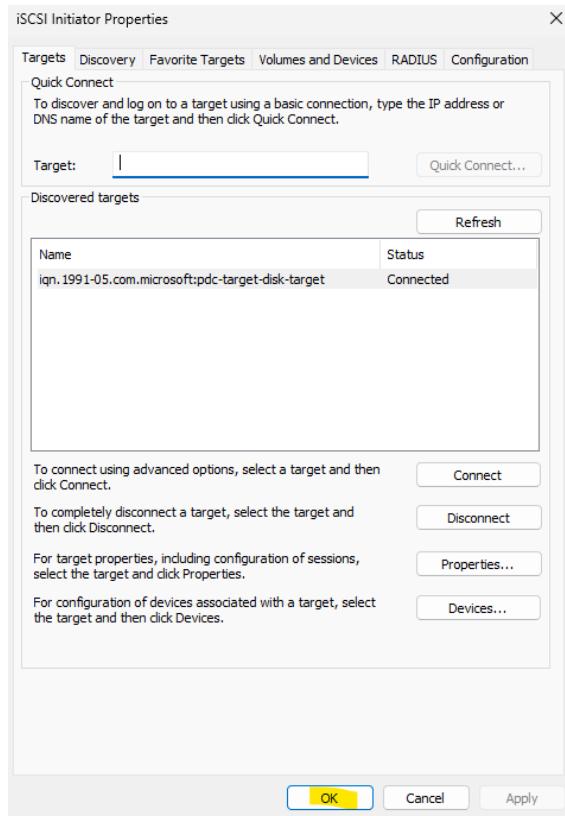


هرجع لـ initiator و هروح على ال targets اعمل بـ refresh target ظهر معايا ختاره وهعمل connect

--



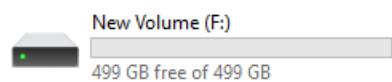
Ok



Ok



هلاقی disk ظهر عندي

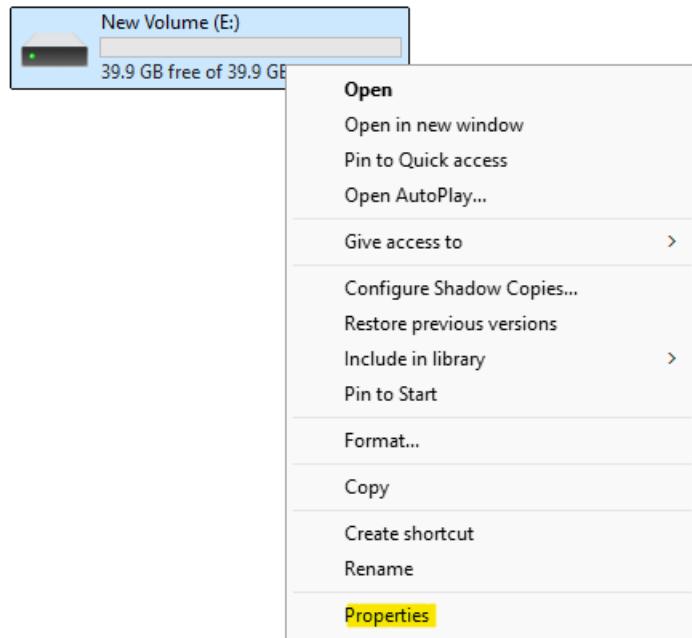


و هلاقیه بقی موجود عندي اک partition

NTFS Permissions

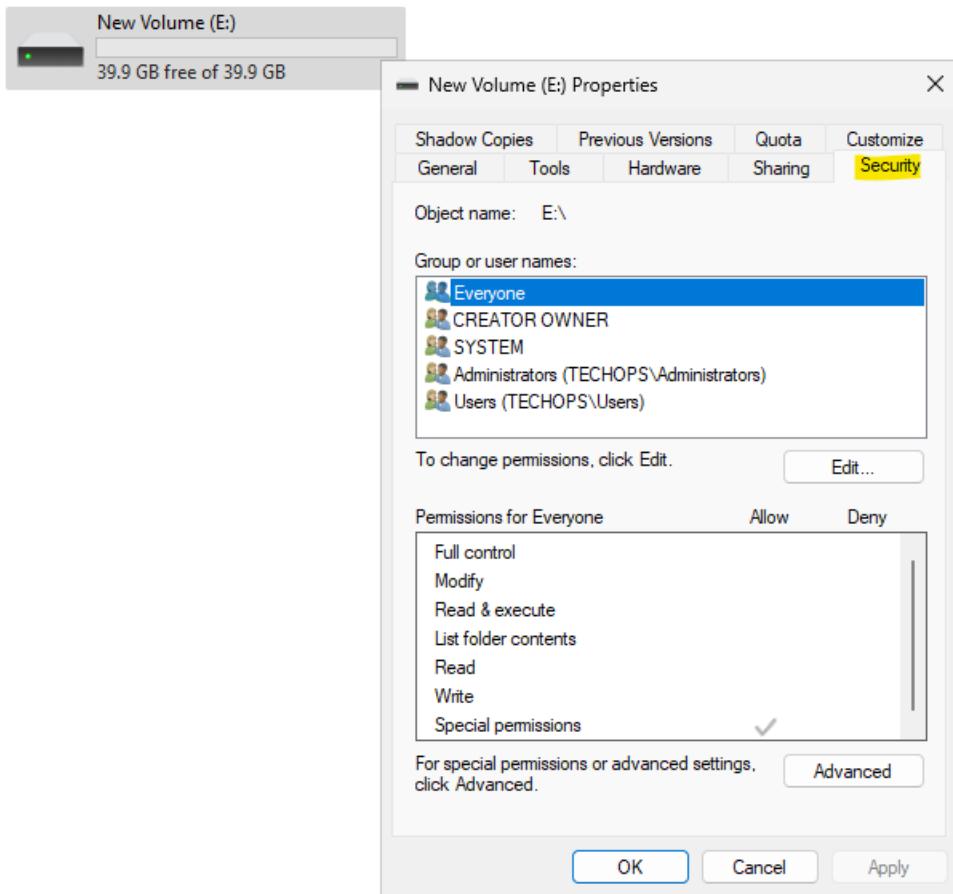
هي ال Access Control الخاصه بال Folders and Files الموجوده على partition ال
الخاصه بيها يكون على ال server locally Access NTFS وال يعني الناس ال هتدخل على
السيرفر local

طيب ابدا اعملها ازاي ؟



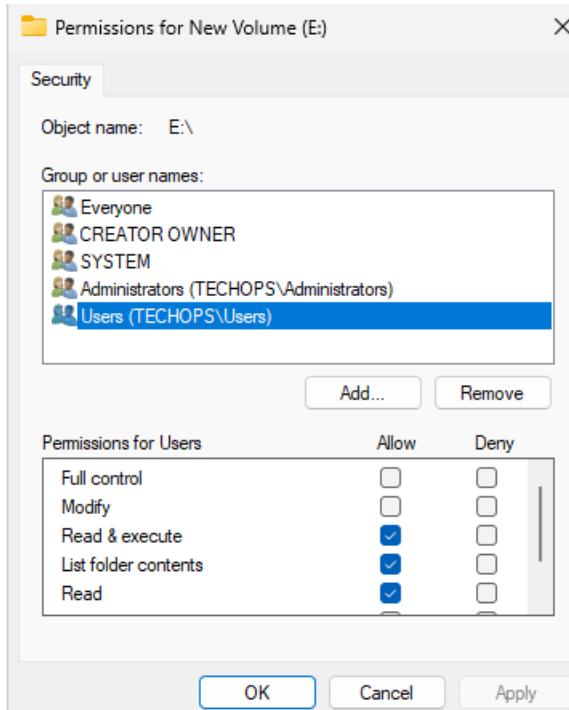
على ال partition وختار properties Click

--



هروح على Security هلاقی ال Access Control List هضغط على Edit

--



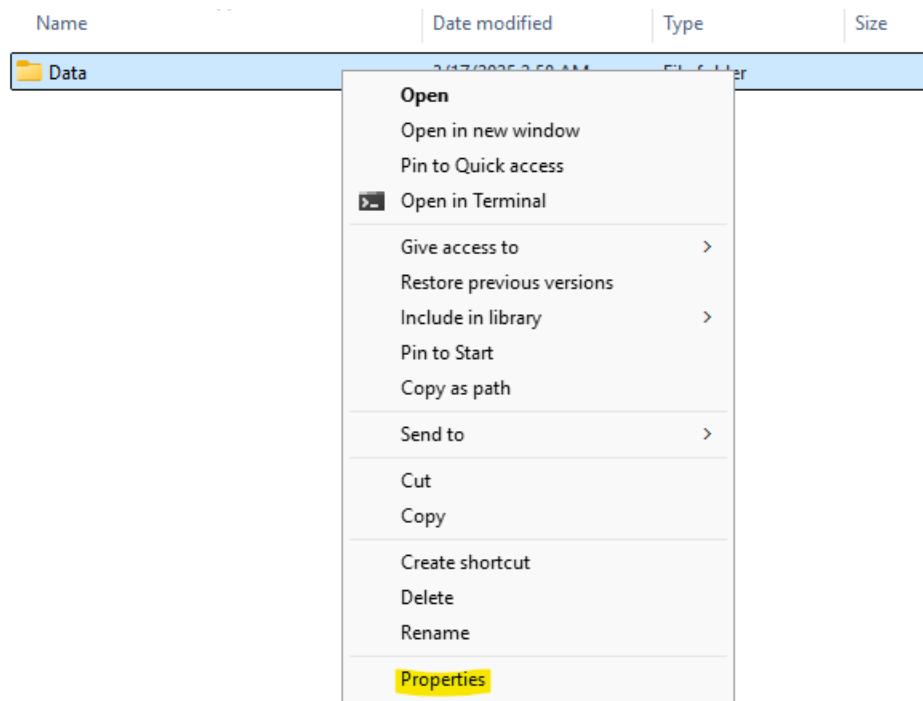
هلاقی ال config بالشكل دا

اقدر اعمل Add او group او user remove ل permission

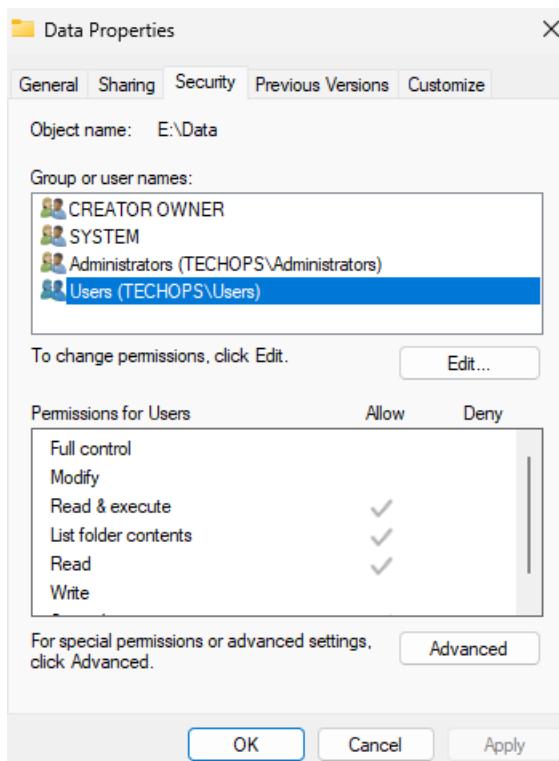
اقدر احدد ال permission بتاعتهم

--

طيب لو عندي folder داخل ال partition وعاوز اعدل ال permission بتاعته؟

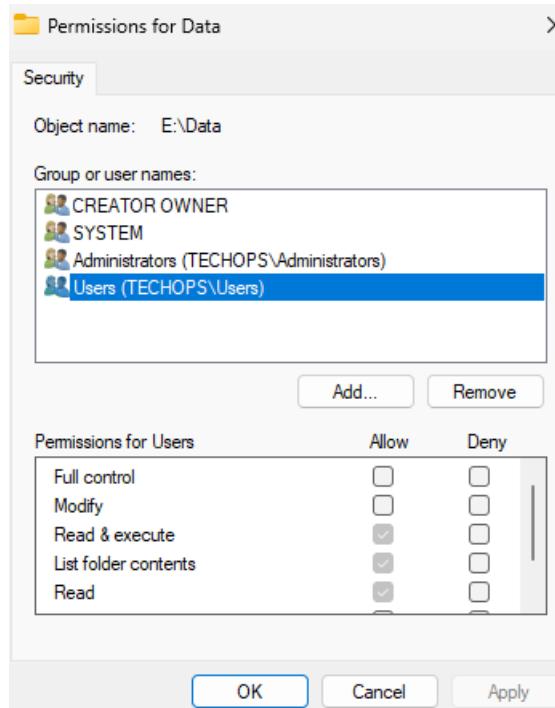


Click **Properties** و هختار **folder** ع ال



هروح علی Security هلاقی ال Edit Access Control List هضغط علی

--



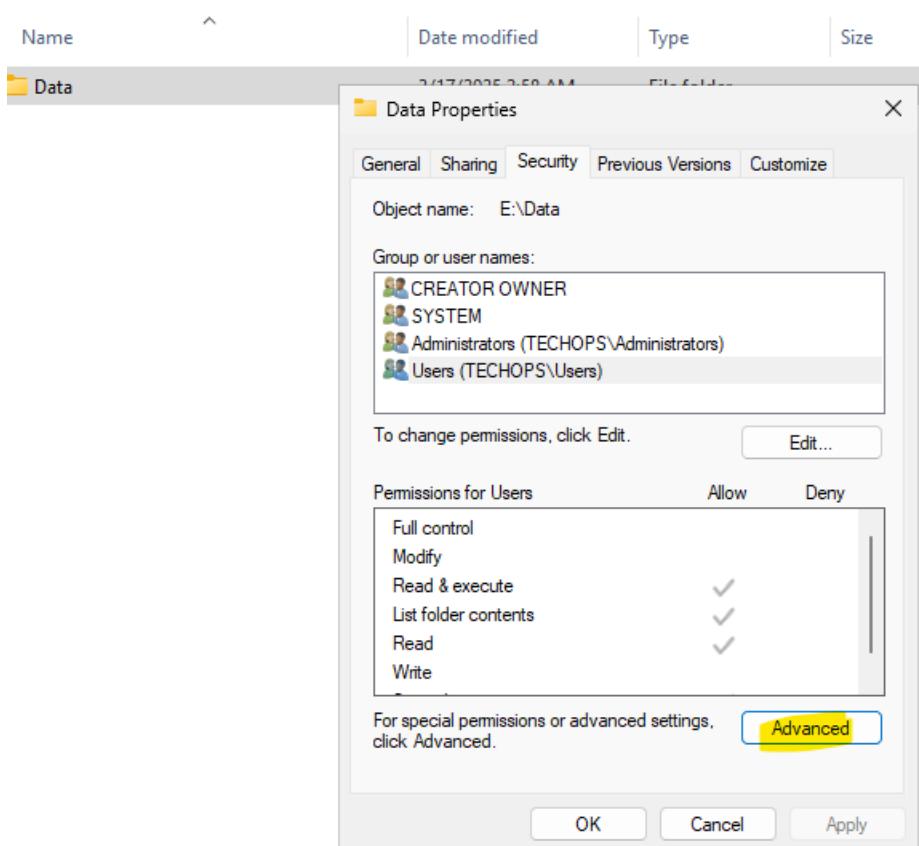
اقدر اعمل add او remove ل user او group

اقدر ادي permission لكن مش هعرف احذف permission موجوده طيب اي السبب؟

لان دى inheritance يعني ال folder واحد ال permission دى من ال parent بتعالو ال هو ال partition

طيب لو عاوز الغي ال inheritance دى ويكون ال folder مستقل ؟

This PC > New Volume (E:)



على ال folder هروح على ال security بقاعدته وفتح ال Advanced

--

Advanced Security Settings for Data

Name: E:\Data
Owner: Administrators (TECHOPS\Administrators) 

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

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

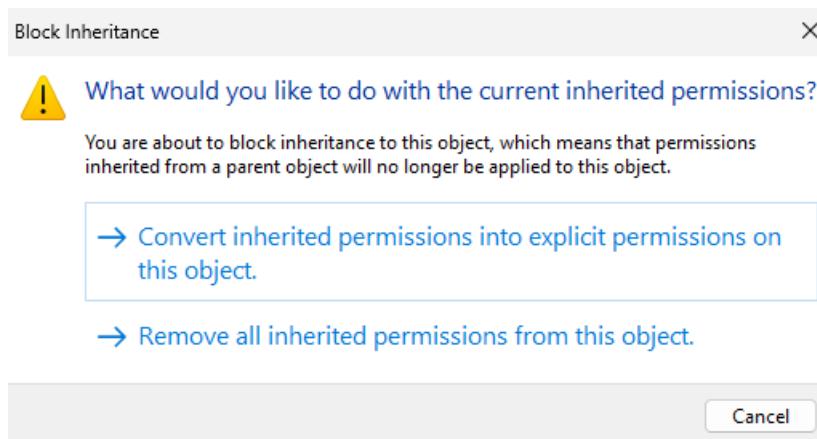
Add Remove View

Disable inheritance

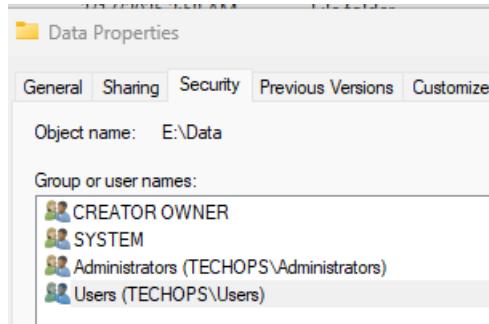
Replace all child object permission entries with inheritable permission entries from this object

OK Cancel Apply

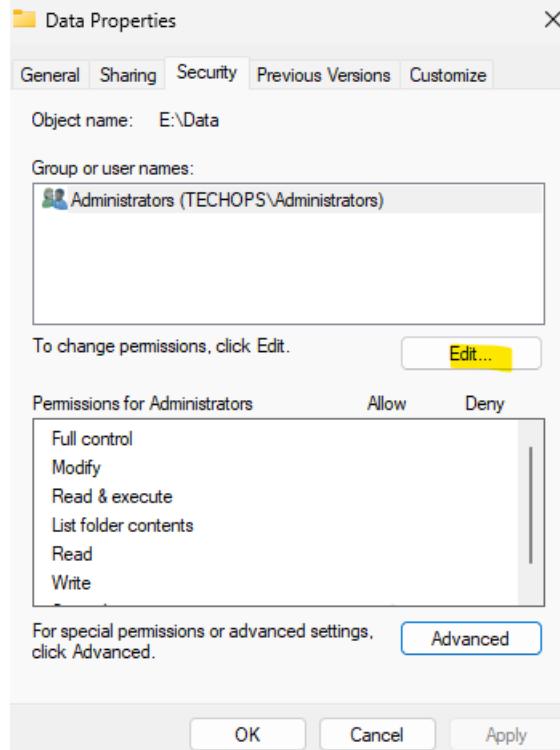
عمل هعمل



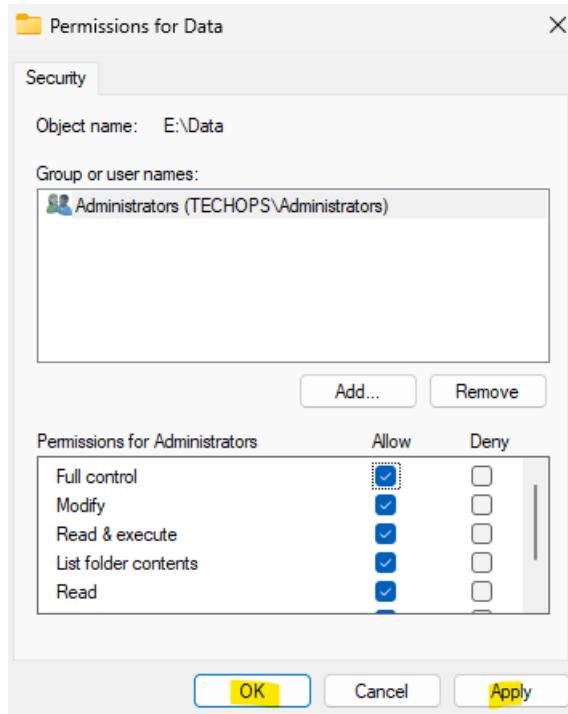
بىسالك ھيلギ ويخلې ال object زى ماھي ولا يمسحها وانت تعمالها من جدىد



ودي ال يقصد بيها ال object ال هما ال groups وال users وال معاهم ال permission



عملت administrator full control ظهرت remove عشان ادي edit لل



ok ثم Full control

--

طيب اي هي انواع ال permission ؟

هنا يقدر يفتح ال folder فقط يشوف ال بداخله List folder contents

يقراء فقط من غير ما يقدر يعدل Read

Read & Execute : يقدر يقراء ويقدر ينفذ ال files القابلة للتنفيذ يعني لو عندي file عباره عن bat يقدر ينفذه

Write : يقدر يعدل مقدر ش يحذف

Modify : يقدر يعدل ويحذف فقط

معه كل ال permission : Full control

--

ال permission تجميع يعني لو ال user في اكتر من group فيه group و فيه read واحد group و فيه read واحد group نفسه في ال 2 group ف ال permission بتاعتاه ه تكون 2 Groups لانه بيأخذ الاعلي بين ال read and write

لو فيه user موجود في group معين وال group read فقط وعاوز user معين داخل ال
read and ياخد ياخد read and write group
write

--

لو فيه user واحد allow و deny في نفس الوقت الاكثر تقييدا هو ال هيطبق يعني ال deny هو ال
هيطبق بمعنى لو فيه user في Group 2 الاول معه allow لل read and write
وال group الثاني معه deny لل user فقط ال user دا مش هيقدر يعدل لان ال هيطبق هو ال
deny لان دائما الاكثر تقييدا هو ال هيطبق write

Sharing Permissions

هي ال permission الخاصة بال sharing folders لكن ال معمولها Access control عبر ال network

عندی 3 type من ال sharing permission :

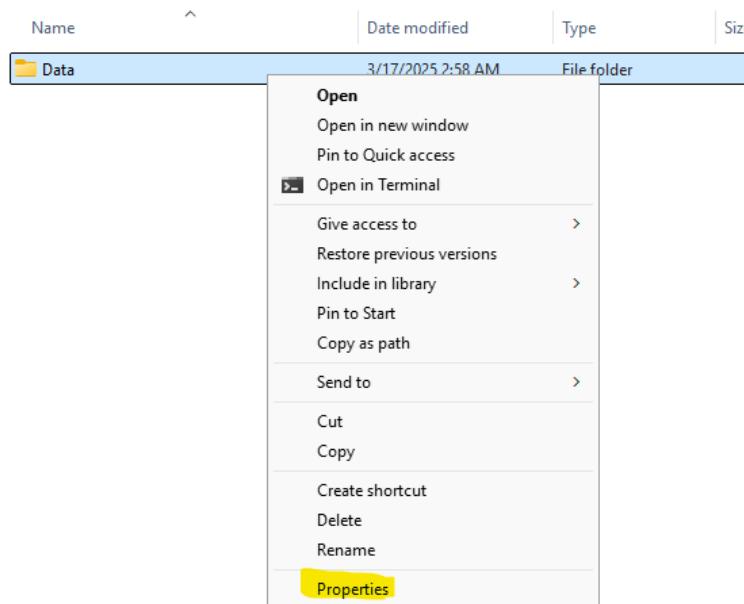
Read : ال user يقدر يفتح ال files ويعملها copy لكن لا يستطيع التعديل او الحذف
Change : ال user هيقدر يفتح ال files ويعملها copy و edit و delete
Full control : مع كل ال access حتى انه يقدر يغير ال permission نفسها

طيب لو انا مطبق ال Sharing permission هل بيأثروا ؟

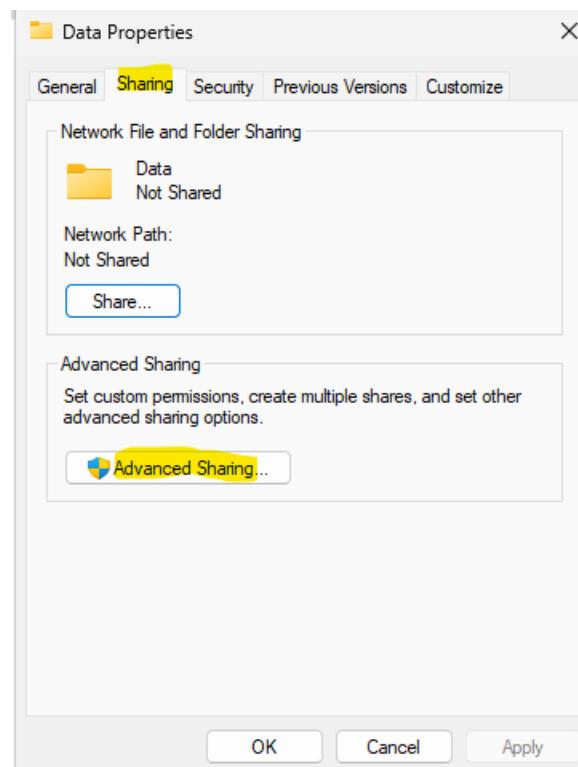
اه الاتنين بيأثروا في حاله ال sharing ، وال بيحصل ال permission الاكثر تعقيدا هي ال بتنطبق

يعني لو ال user معه write and read على ال NTFS permission و read بس على ال sharing permission فقط لانه هو الاكثر تعقيدا وهكذا

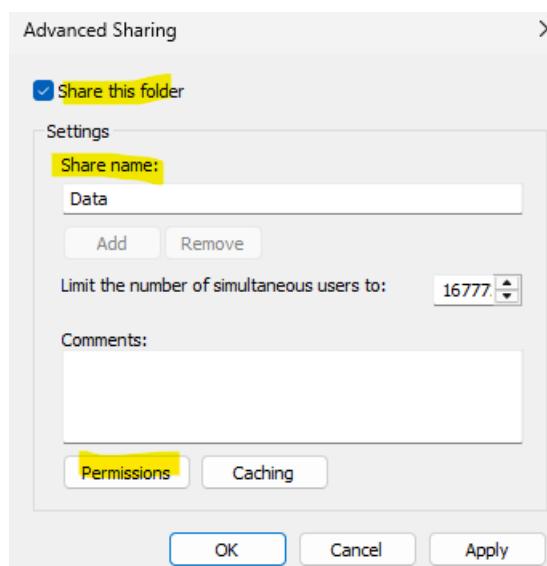
طيب ازاي اطبقه ؟



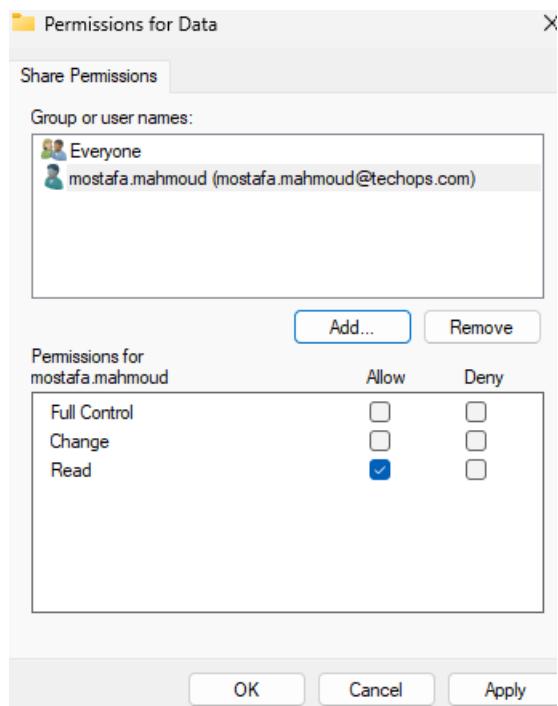
Click ع ال folder وختار properties



من sharing هختار Advanced



هعمل permission لـ share واديله name واروح علي ال enable

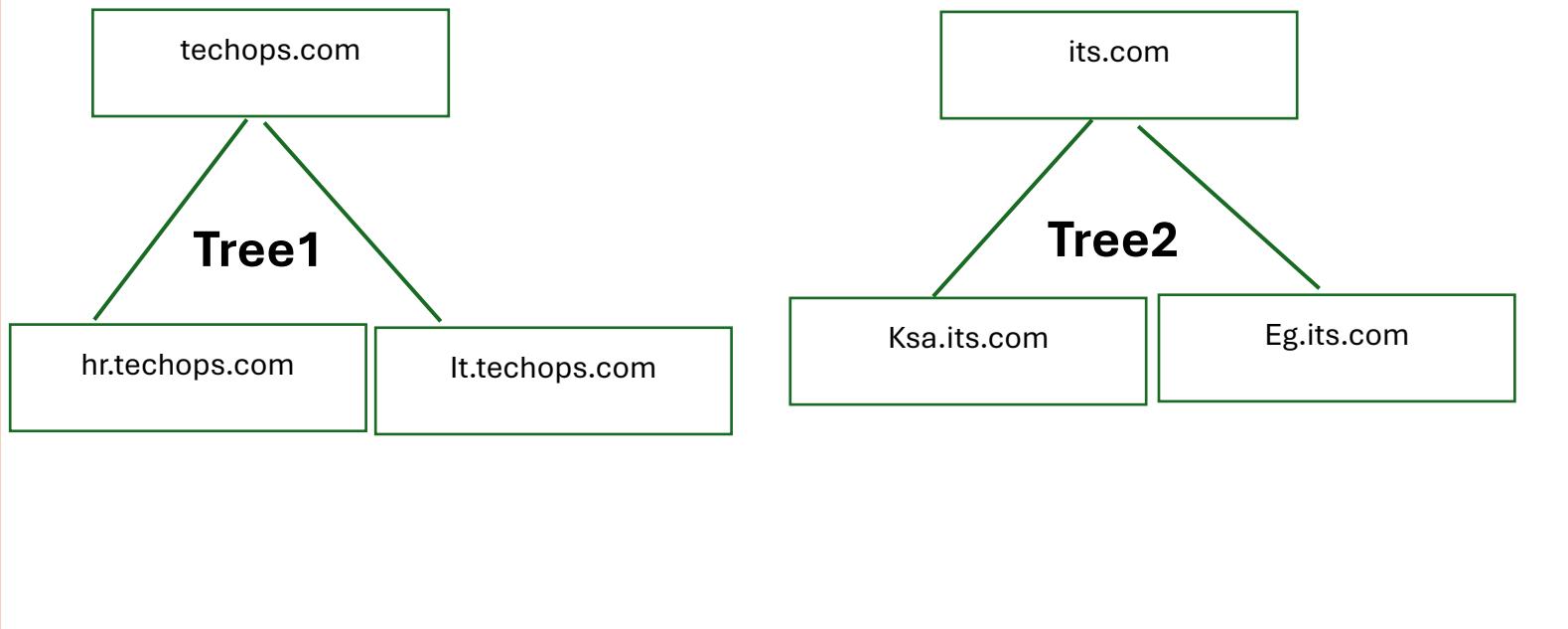


هحدد مثلًا ال user ال عاوز اديله access
واحدد ال ok access ثم

New Tree

هي مجموعة من ال Domains المرتبطة بعضها داخل نفس ال Forest

Forest



عندی ال Forest وهو أعلى مستوى في ال AD
وعندی 2 domains مختلفين وهما techops.com و its.com
طيب ليه سميناهم tree ؟ لأن تحت كل child domain فيه forest وبالتالي بيحصل عندی زي tree وعشان
كدا المستوى الأكبر اسمه forest يعني غابه لأن بيكون عندی اكتر من tree ف بيكونوا عندی forest

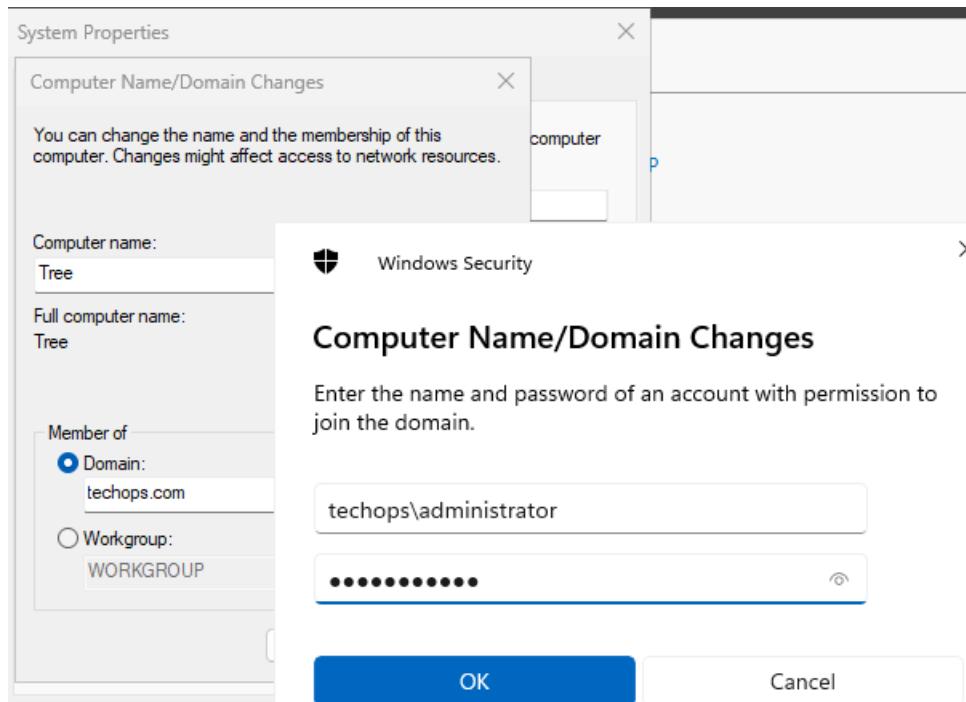
كل trees داخل ال forest بيتشارك في نفس ال Schema وال global catalog

طيب ازاي ابدا ابني tree عندي ؟

طيب احنا عندي ال domain بتاعنا ب اسم techops.com

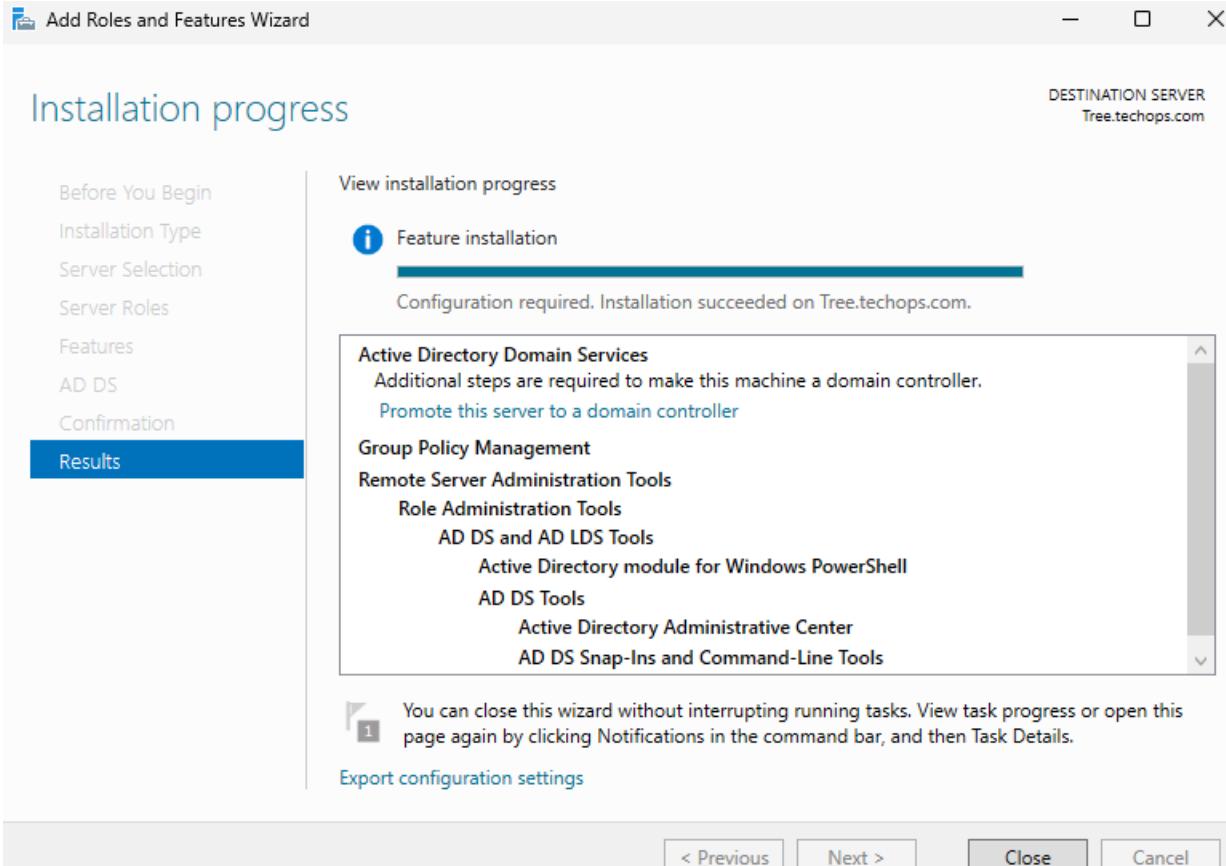
عاوزين نعمل tree يعني domain مختلف ب اسم مختلف وليكن its.com

--
هيكون عندي server تاني ال هو هيكون its.com



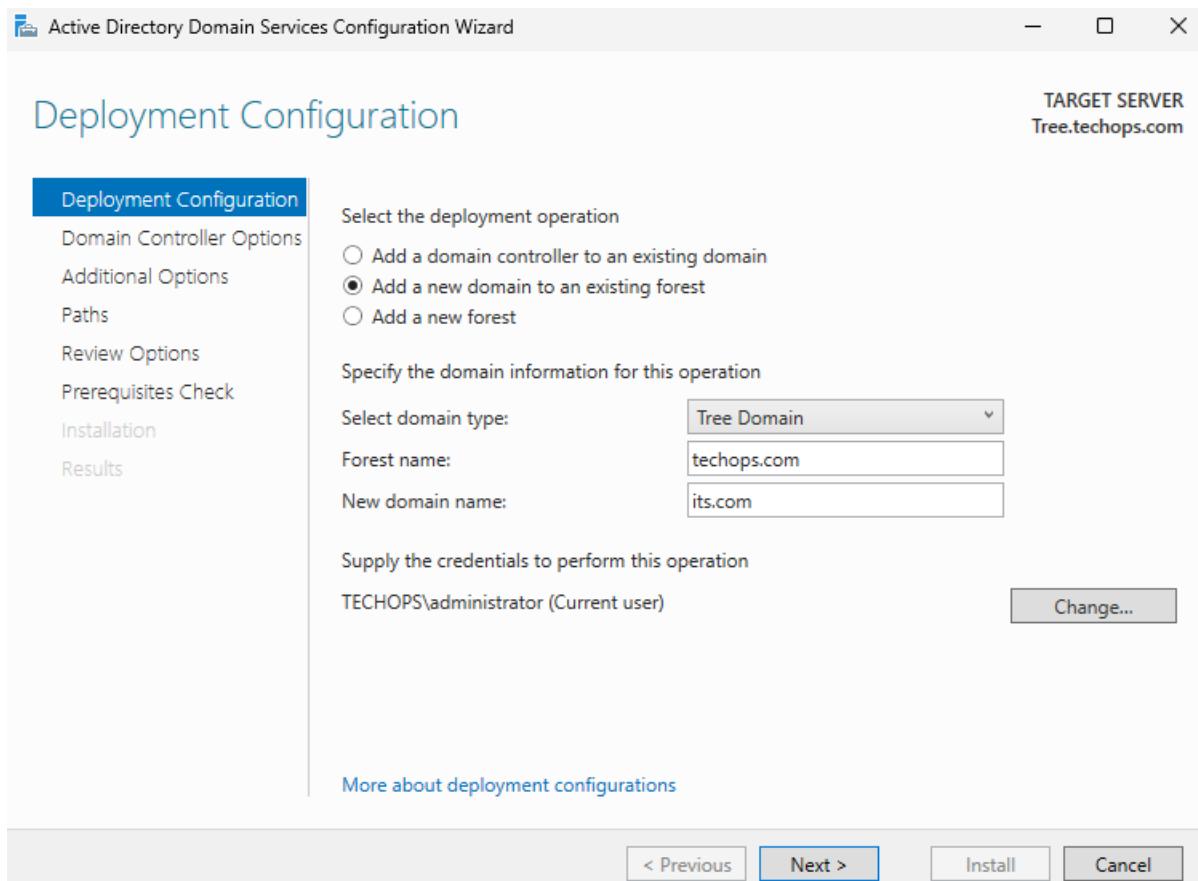
اول حاجه هعمله join لل domain بتاعي ال هو techops.com

--



تاني حاجه هست طب ال role ال هي AD domain Service عشان احوله ل DC

هدا اعمل server لل domain دا كانى بعمل new domain جديده بس هيكون في اختلافات في ال config



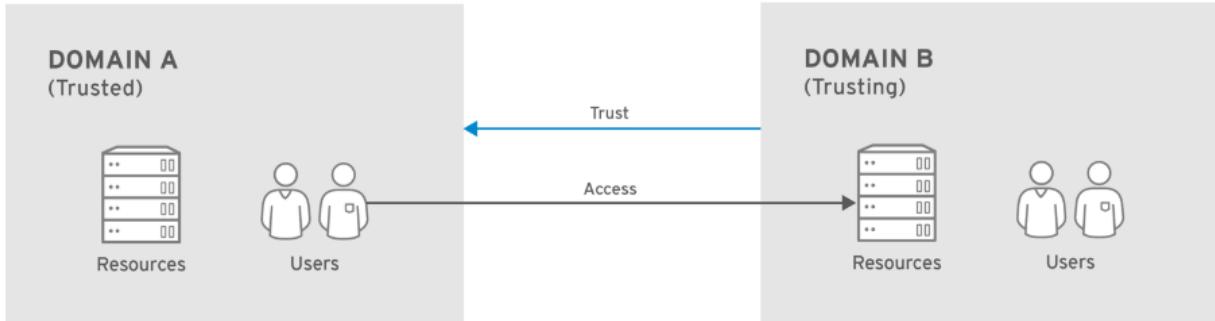
مش هعمل New forest لاني انا عاوز tree معايا في ال forest بتاعي
 ف هختار Add a new domain to an existing forest يعني عاوز اضيف domain في forest
 موجوده عندي
 بعد كدا هختار نوع ال domain هيكون tree
 بعد كدا بكتب forest name وف حالي هو techops.com
 وبعد كدا بكتب ال domain name الجديد ال انا عاوزه
 بعد كدا بكملي الخطوات بتاعتي عادي جدا

ملحوظه : لازم ال user ال هيعمل ال tree يكون موجود في group اسمها Enterprise Admins
 لان ال في ال group دي يقدر يعمل manage لـ DC ال في ال forest بالكامل لكن ال
 فقط يـ DC ال معه في نفس ال domain ال هما PDC وال ADC Admins

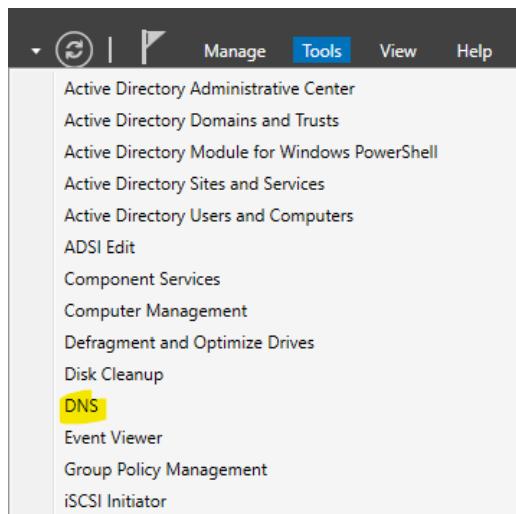
Trust Relationships

هو اني ببني trust بين domains مختلفه او forest مختلفه ، ودا بيسمح لـ users انهم يقدروا يعملوا على resources موجوده في forest مختلفه

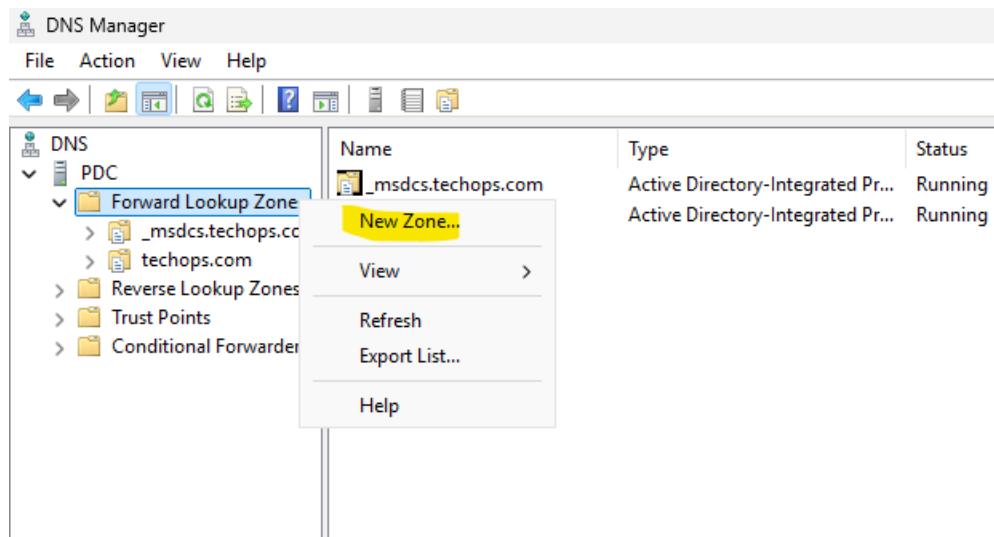
(بساطه هو عمليه التحقق من identity بين بيئات AD مختلفه)



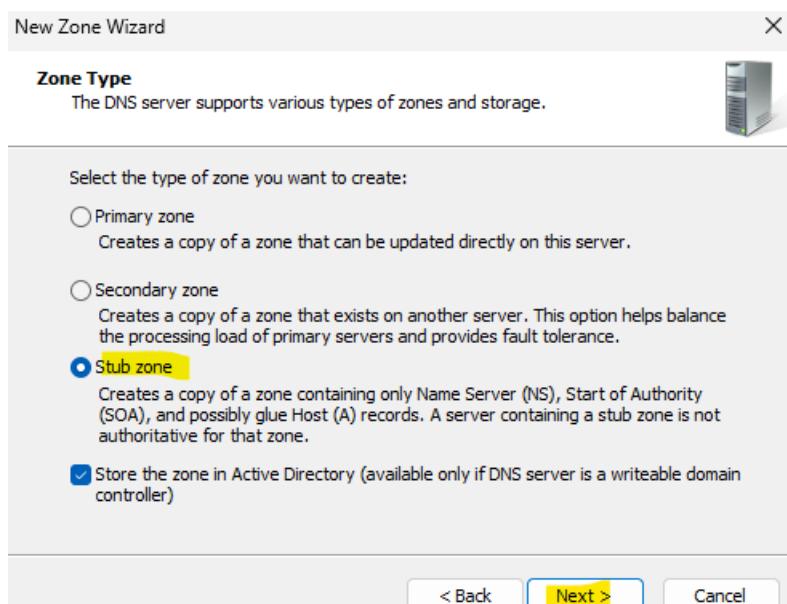
--
طيب ابدا استخدمه ازاي ؟



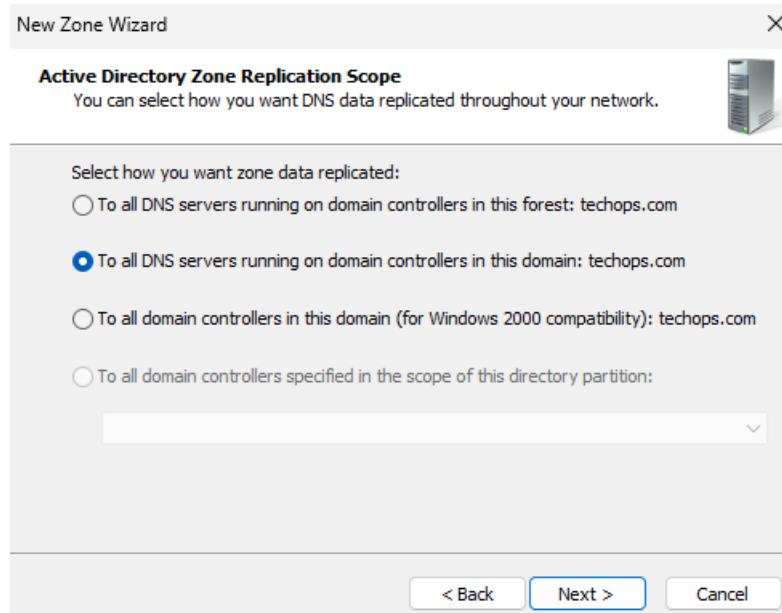
من ال server manager Tools هروح على DNS ومنها هفتح ال



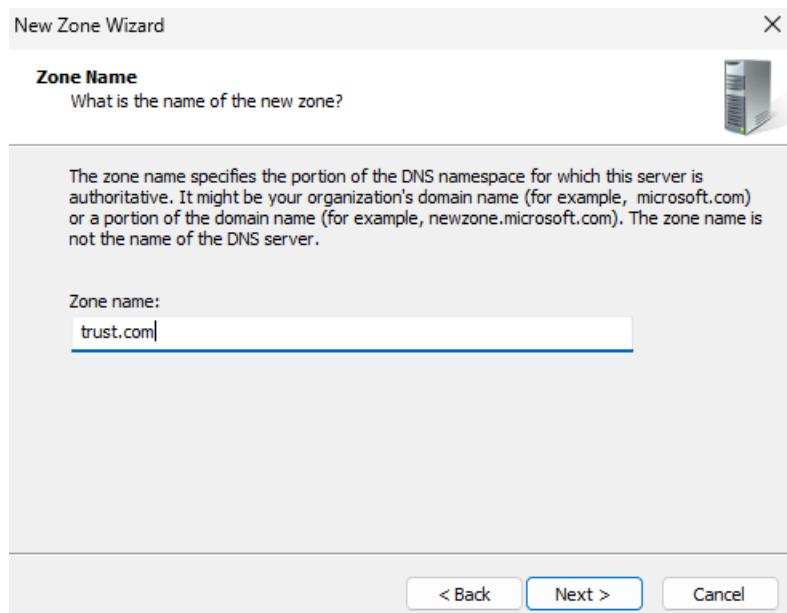
Click على ال domain name ومن على ال forward lookup zone هعمل New Zone



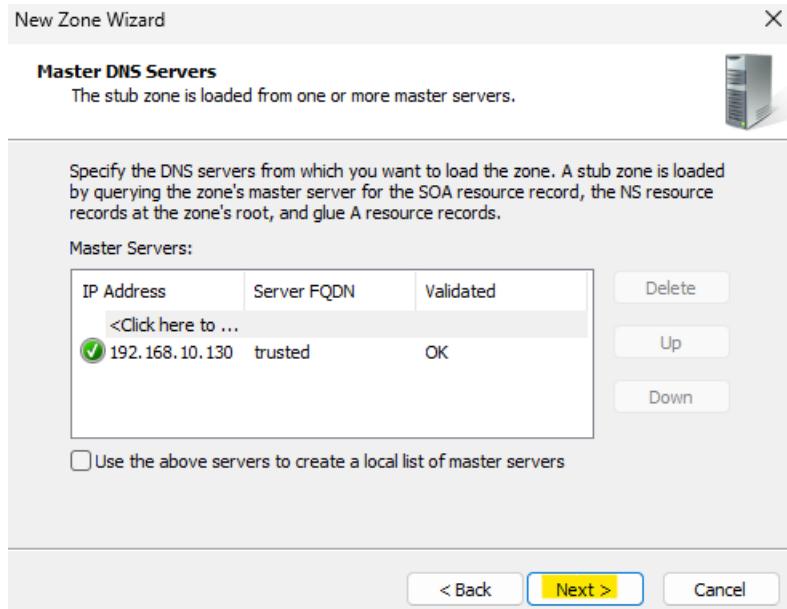
نوعه هيكون sub zone



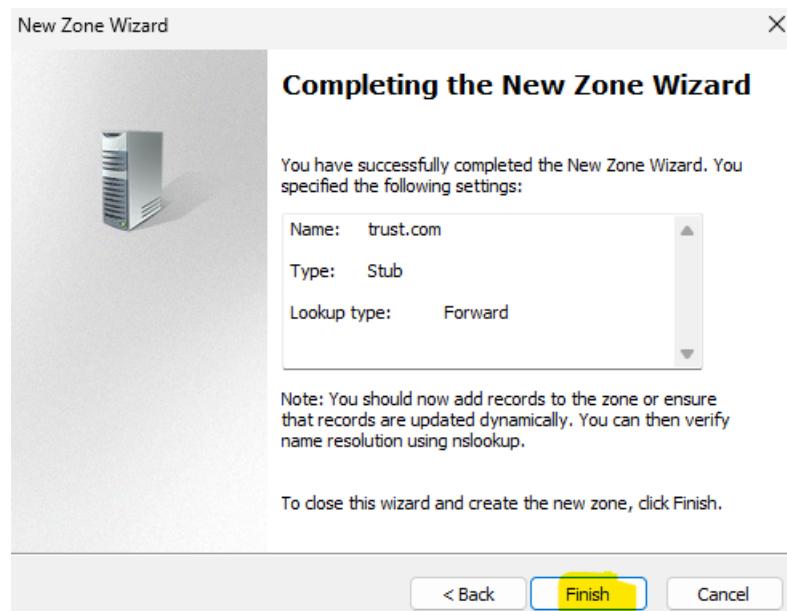
ال replication domain يكون على مستوى forest ولا على domain



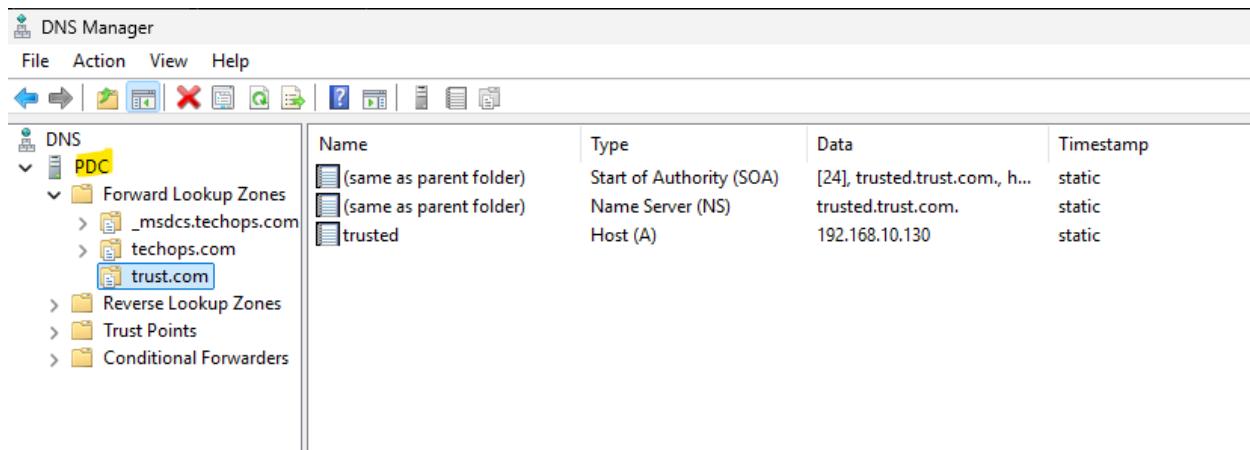
trust.com ال domain name zone name فبكتب ال عاوز اعمل معه trust وف حالي اسمه



هڪتب ال ip بتاع ال عاوز اعمل معه trust.com

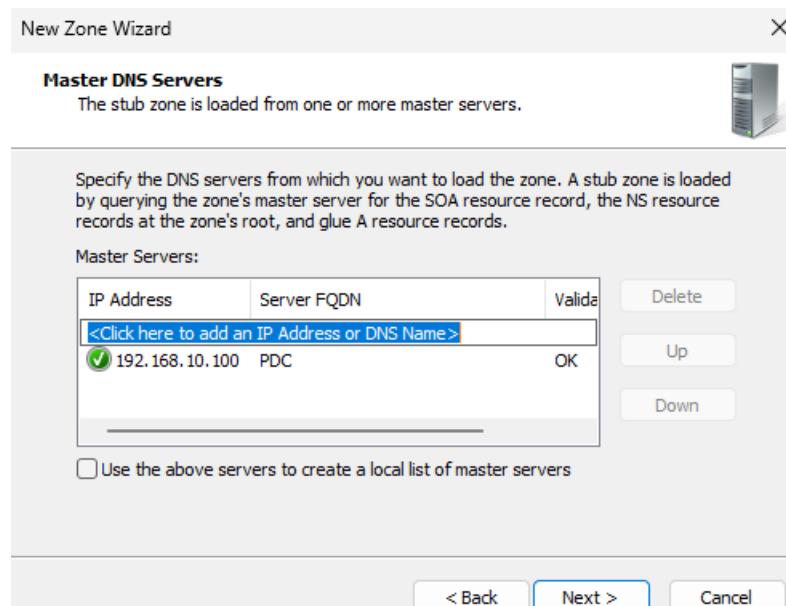


Finish



هلاقي ال بقى موجود لك zone trust.com عندي

--
وهكرر نفس الخطوات دي على ال domain ال اسمه trust.com عشان اعمل لل trust.com علني



علي ال trust zone عملت لـ PDC ال هو techops.com

--

The screenshot shows the Windows DNS Manager interface. On the left, the navigation pane displays a tree structure with 'DNS' at the root, followed by 'TRUSTED', 'Forward Lookup Zones' containing '_msdcs.trust.com' and 'techops.com', 'Reverse Lookup Zones', 'Trust Points', and 'Conditional Forwarders'. On the right, a table lists DNS records for the 'techops.com' zone:

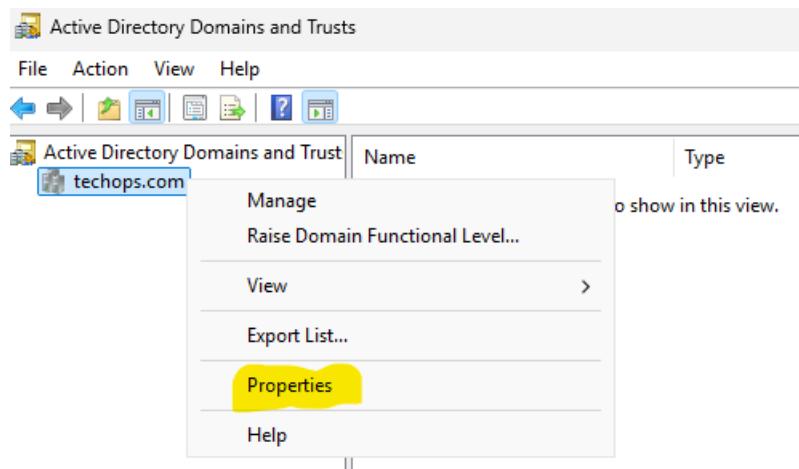
Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[305], pdc.techops.com, ...
(same as parent folder)	Name Server (NS)	adc.techops.com.
(same as parent folder)	Name Server (NS)	pdc.techops.com.
adc	Host (A)	192.168.10.150
pdc	Host (A)	192.168.10.100

هلاقیه بقی موجود عندي

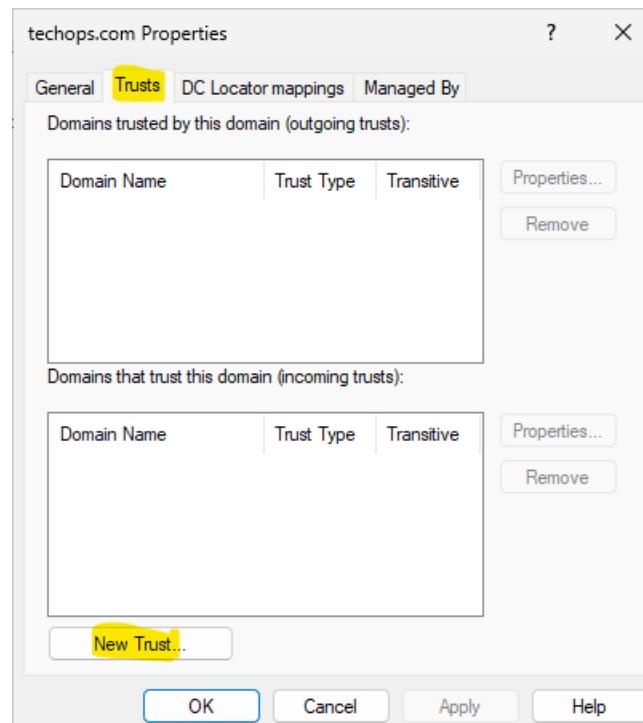
بعد کدا هعمل trust relationship لل build دا

The screenshot shows the 'Active Directory Administrative Center' window. The top navigation bar includes 'Manage', 'Tools', 'View', and 'Help'. Below the bar, a list of tools is displayed, with 'Active Directory Domains and Trusts' highlighted in yellow. Other options include 'Active Directory Module for Windows PowerShell', 'Active Directory Sites and Services', 'Active Directory Users and Computers', 'ADSI Edit', 'Component Services', and 'Computer Management'.

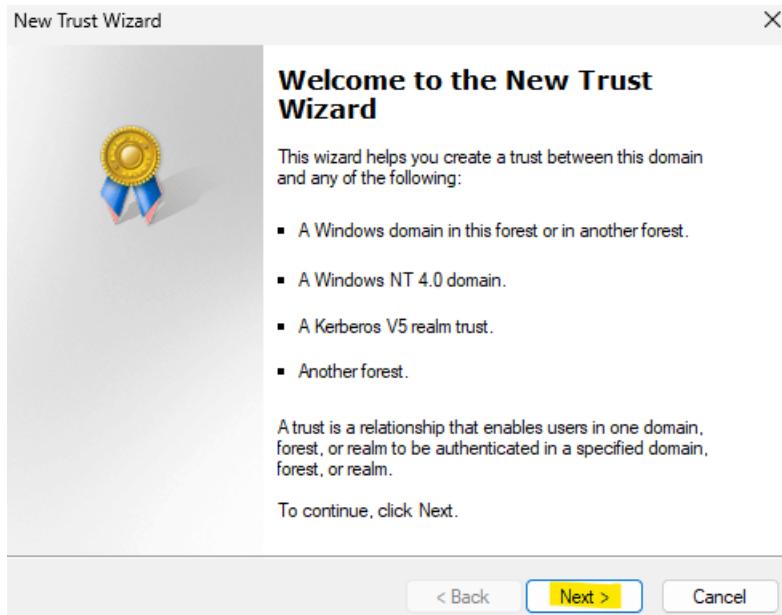
من tools هفتح ال AD Domain and trusts



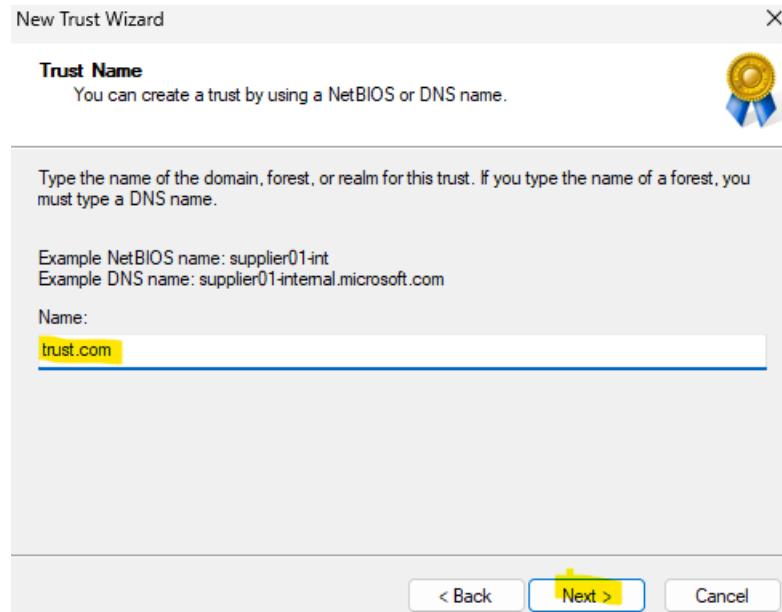
ع ال properties علی و هروح Click domain name



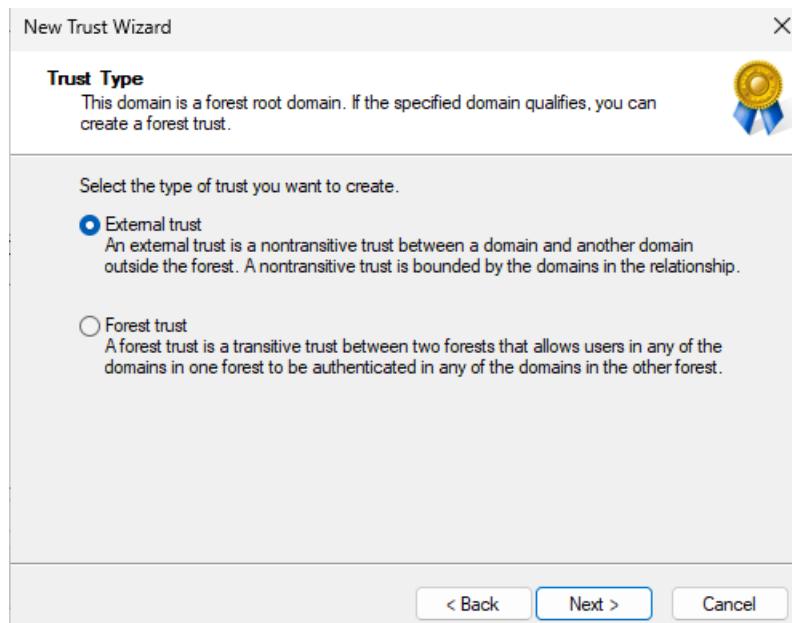
من properties علی و هروح trusts New trust و هعمل



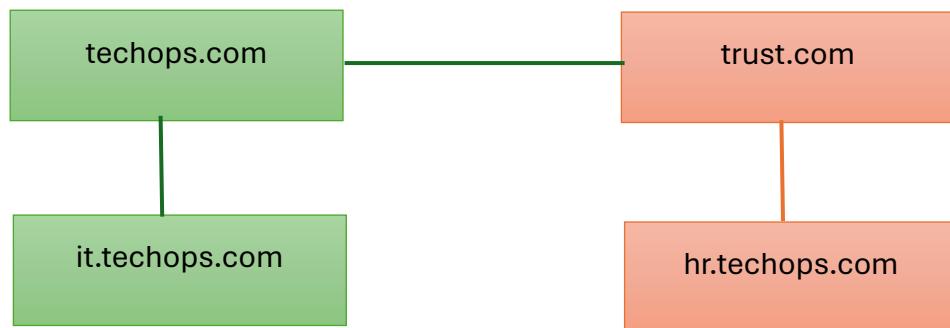
Next



ال trust مع domain العمل ال



ال type الخاص بال trust وفيه نوعين عندي :

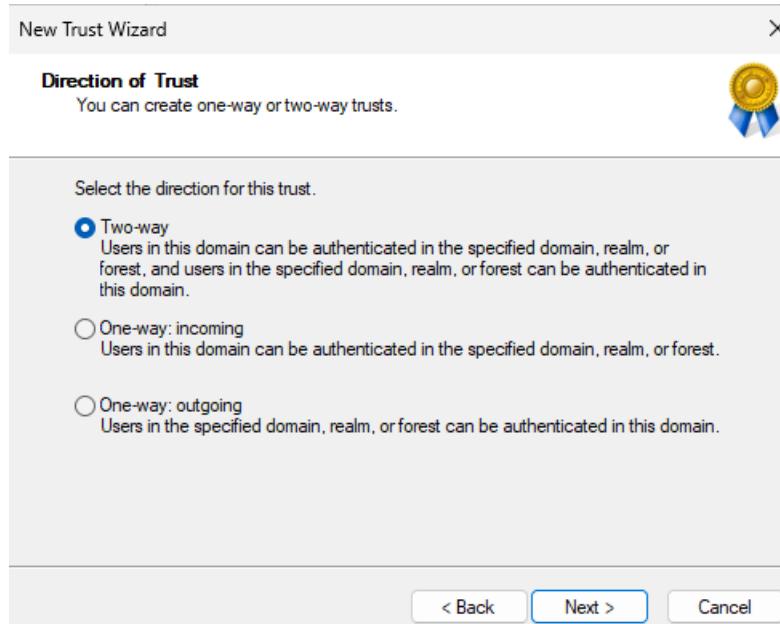


هنا ال trust هيكون بين ال tecops.com وال trust.com فقط ال تحتهم مش هيكون فيه بينهم trust ، يبقى هنا بيكون بين ال domains في forest مختلفه

هنا ال trust هيكون بين ال tecops.com وال trust.com وبعدين بين it.techops.com وال trust.com : Forest Trust -2

يبقى هنا ال trust هيكون بين forests مختلفه بالكامل hr.trust.com

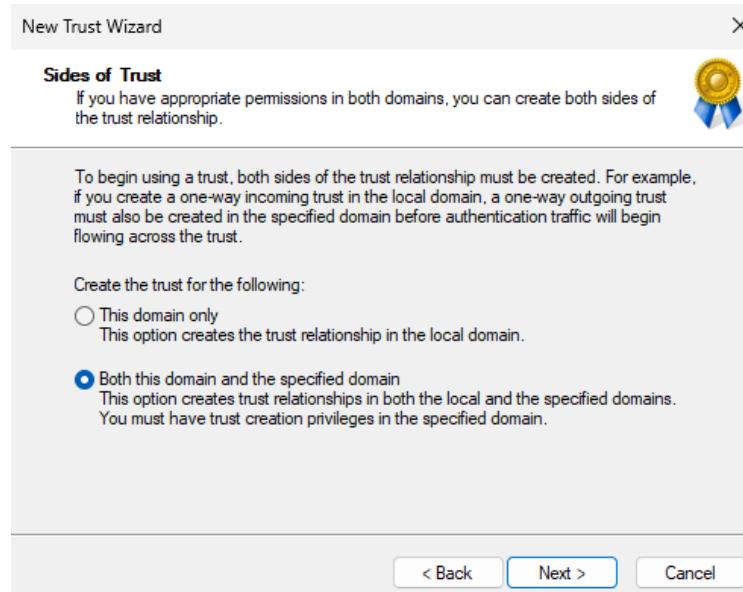
--



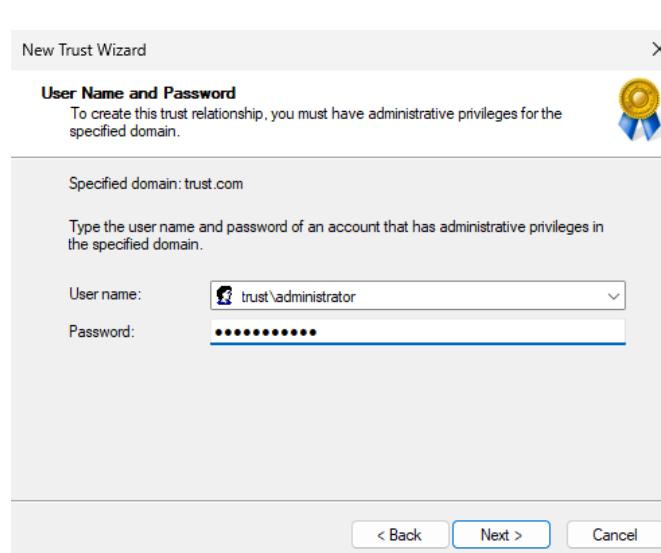
بعد كدا بحدد ال direction وفيه نوعين

- 1 : ودا معناه ان ال users الموجودين في techops.com يقدروا يعملوا access على ال resources الموجوده في trust.com والعكس ال users ال موجودين في trust.com يقدروا يعملوا access على ال resources الموجوده في tecops.com
- 2 : بحدد ان مثلا ال users الموجودين في techops.com يقدروا يعملوا access على ال resources الموجوده في trust.com ومعلمتش العكس

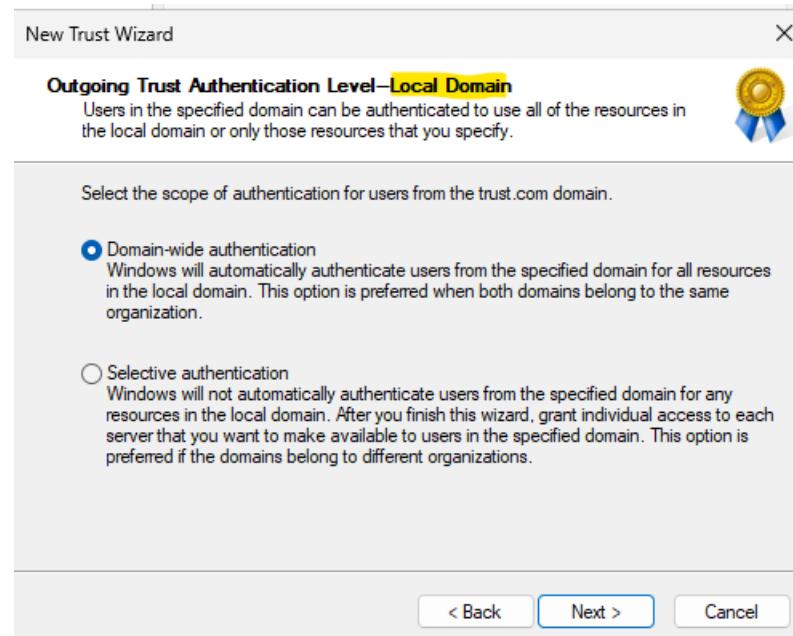
--



دي لو اختارتها ف كاني بطبق الخطوات دي على السيرفر دا فقط وبعد ما اخلص هروح على السيرفر الثاني اطبق عليه نفس الخطوات تاني
لو اختارت both كاني بطبق الخطوات على السيرفرين مره واحده
ف انا هنختار both



بيسالني علي ال username وال password الخاصين بالسيرفر الثاني ال هو trust.com ومن بعدها كل شاشه هتتكرر مرتين مره ل tecops.com ومؤهل

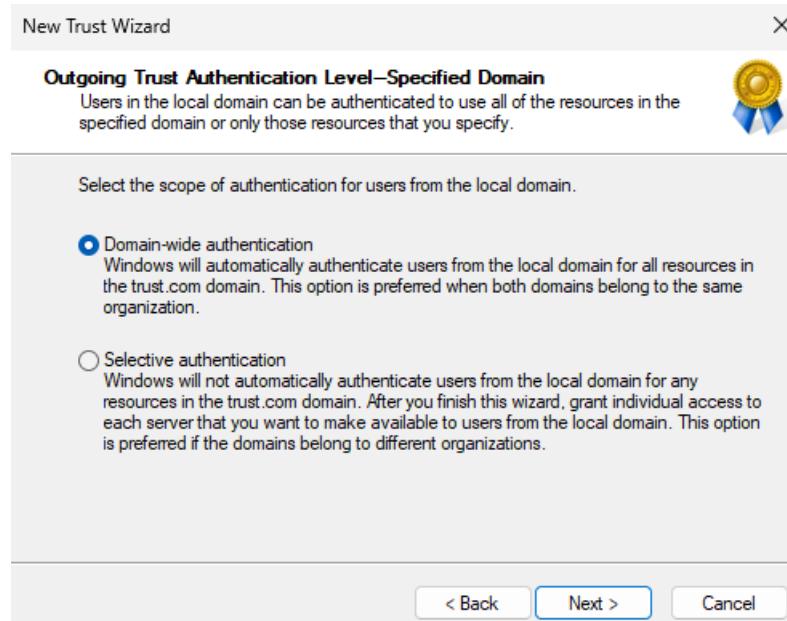


هنا بيسالني عن ال auth على ال local domain ال هو : techops.com

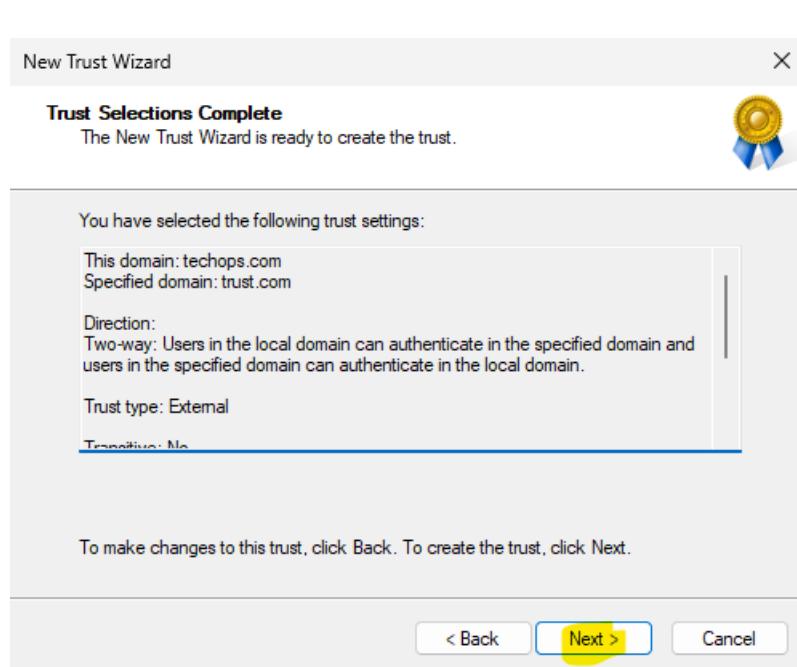
دي معانها ان كل users ال عند ال domain الثاني ال هو trust.com يقدرو يعملوا على كل ال موجوده على techops.com ال هو local domain access resources

هنا هحدد معينه هما ال يقدرو يعملهولها access مش كل ال resources : Selective auth

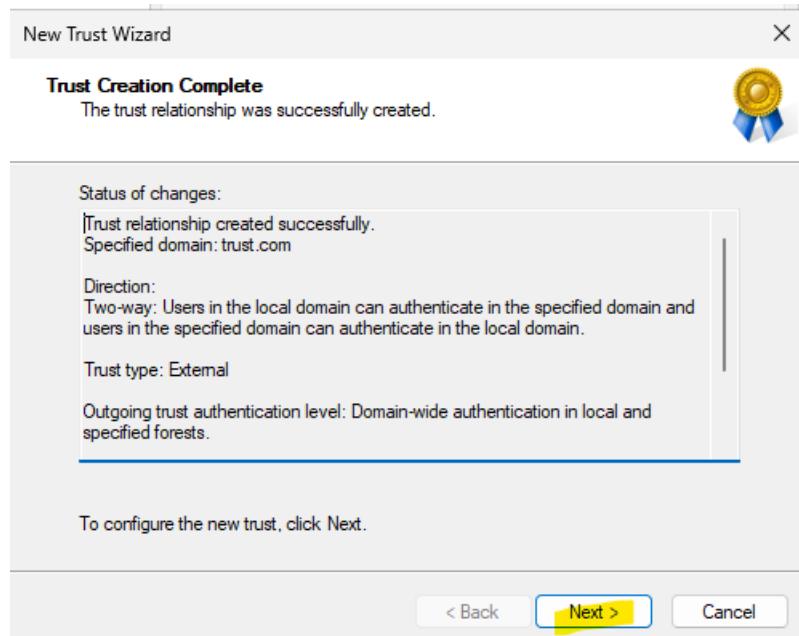
--



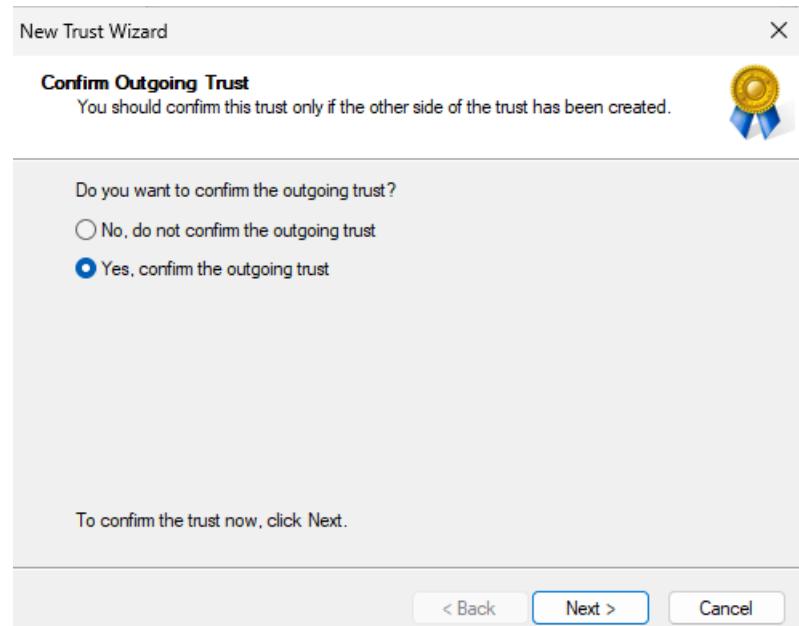
نفس الشاشه اتكررت لما عملت next عشان هنا هيسالني عن السيرفر الثاني ال هو trust.com : دي معانها ان كل users ال علي ال domain الاول ال هو techops.com يقدرو يعملوا على كل ال الموجوده علي ال domain الثاني ال هو truest.com access : هنا هحدد معينه هما ال يقدرو يعملو لها access مش كل ال resources : Selective auth



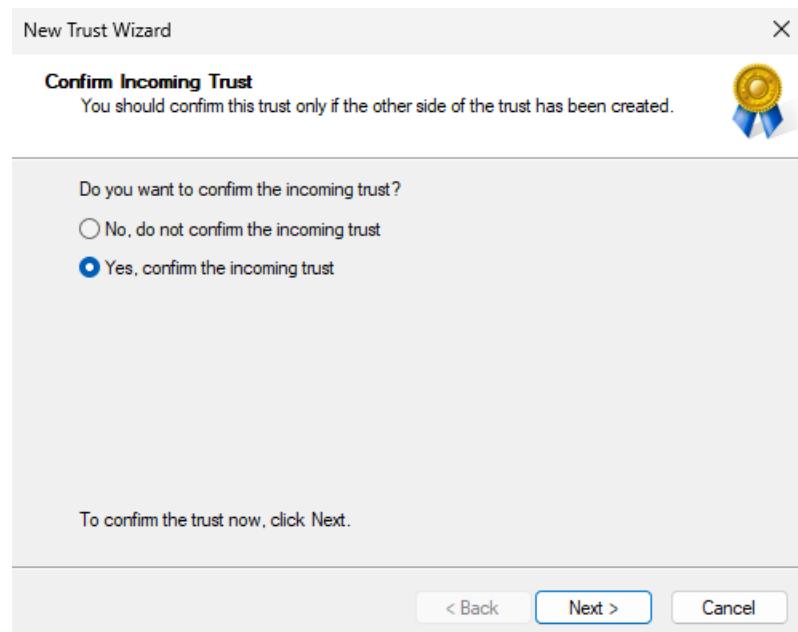
Next



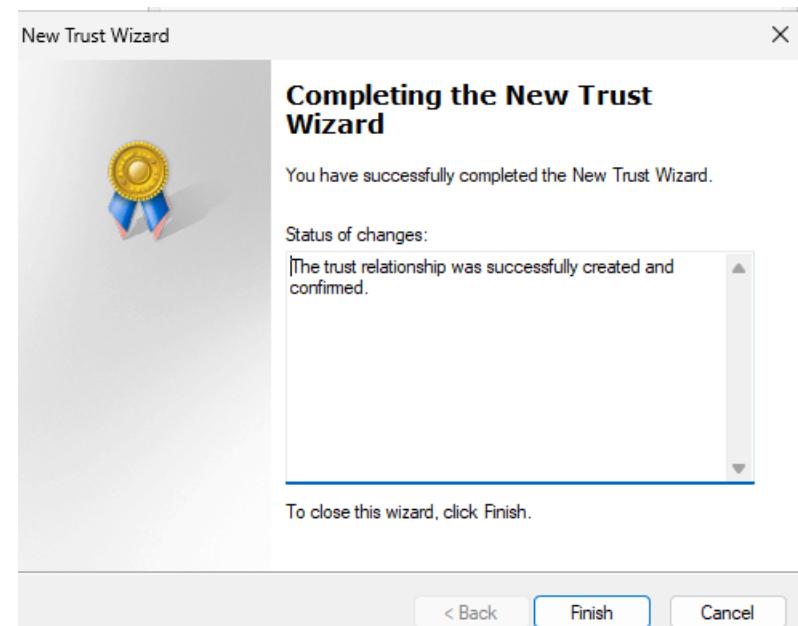
Next



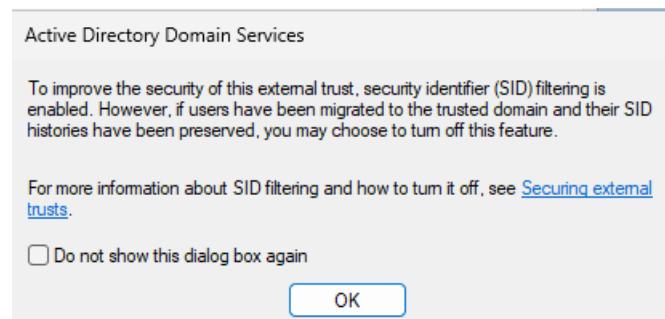
outgoing trust لـ confirm 



incoming trust ↴ confirm ↴



Finish



Ok

--

The dialog box is titled "techops.com Properties" and shows the "Trusts" tab selected. It displays two sections: "Domains trusted by this domain (outgoing trusts)" and "Domains that trust this domain (incoming trusts)".

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
trust.com	External	No

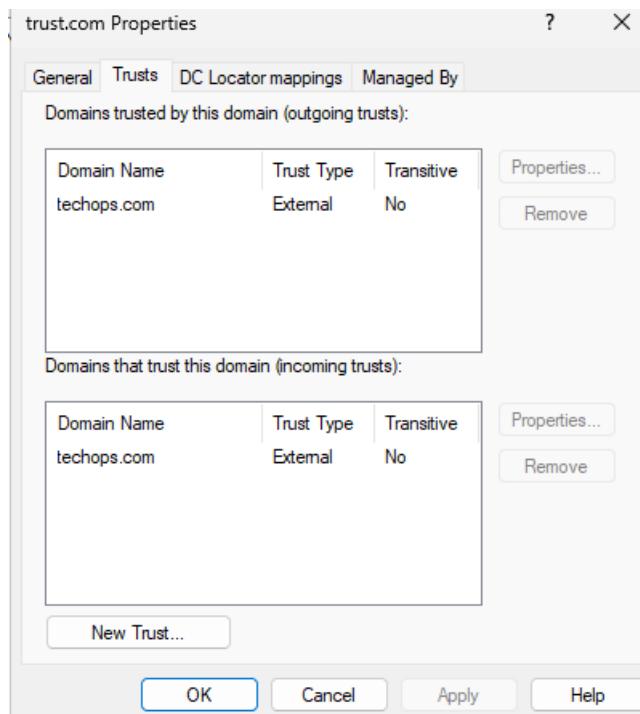
Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
trust.com	External	No

Buttons: Properties..., Remove, New Trust..., OK, Cancel, Apply, Help

هتلaci بقا ال trust.com موجود عندي في ال trusts مرتين في ال outgoing و ال incoming

--

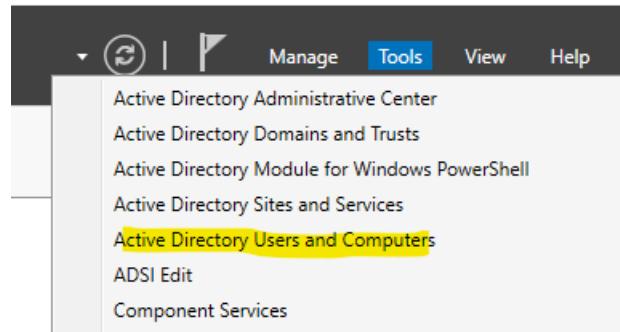


ولو روحت على trust.com وروحت على ال Domains and trusts وفتحت ال trusts هلاقي ان ال outgoing موجود وبرضو في ال incoming وال techop.com

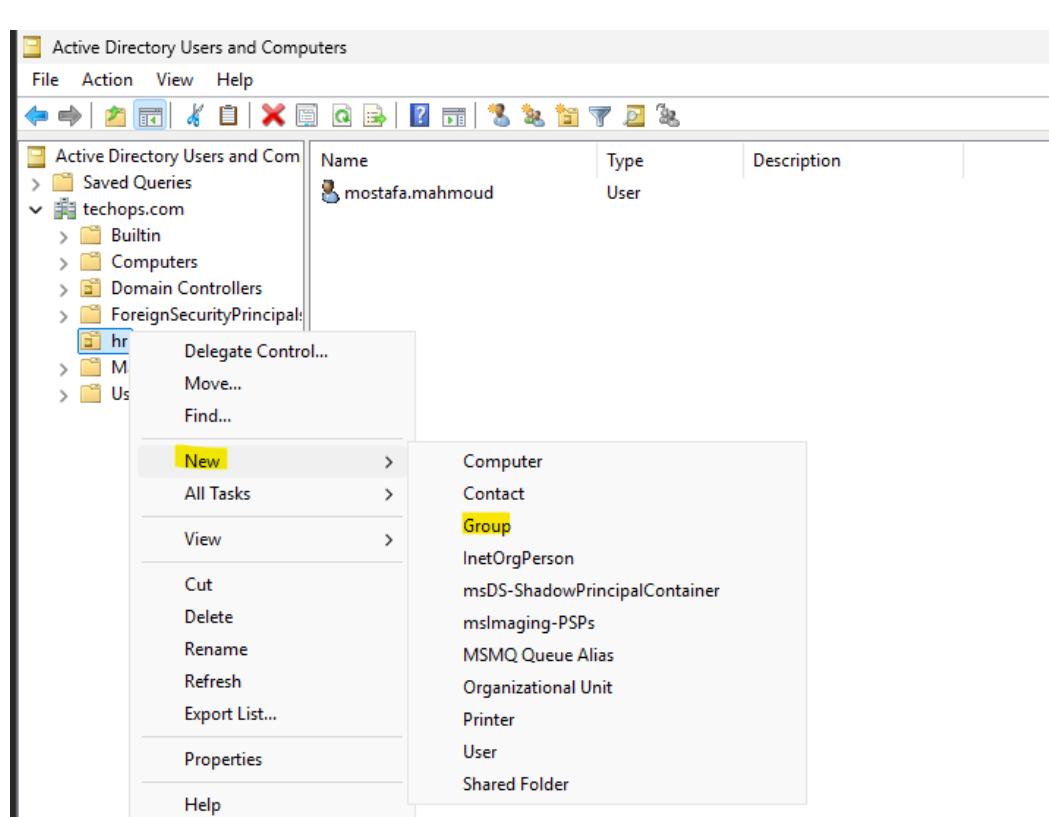
AD Groups

ال groups في ال Active directory هي طريقة لتنظيم وادارة ال users وال resources . ومن خلالها اقدر اطبق policies و permission على كل ال group بدل م اعمل permission لكل user

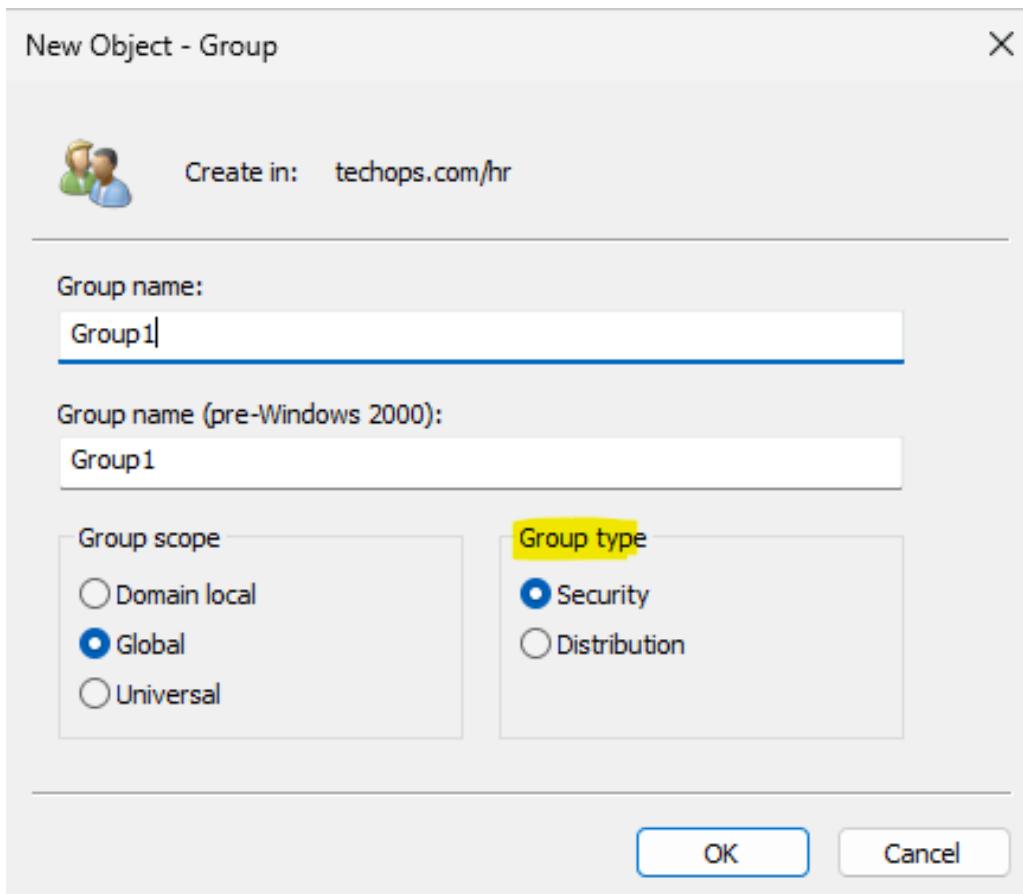
طيب ازاي اعمل create ل group ؟



من ال AD Users and computers هروح علي tools وافتح ال server manager



من المكان ال عاوز اعمل فيه ال group ول يكن ال OU ال اسمها hr هروح علي new واختار group



بعد كدا بحدد ال group type وعدي نوعين Group name

sharing permission : وهنا اقدر اطبق علي ال group سواء security -1 او NTFS permission -2 – اقدر اطبق عليها Group policy زى ال users . ودى polices بتطبق علي ال system Rights .

Distribution : دى بتسخدم في ال Exchange Server لتوزيع البريد الالكتروني علي ال group دا ككل ، يعني لو عاوز ابعت ايميل ل 100 موظف فبدل م ابعت ايميل لكل موظف ، لا هحطهم كلهم في group من نوع Distribution وابعدت الايميل لل group دا ف يوصل لكل users ال فيه ، نوع ال group دا مش بيكون ليه SID

بعد كدا بحدد ال Group scope ودى بتحدد 2 الاول هو ال users ال هسحبهم هيكونوا ع مستوي اي ال domain ولا child ولا trusted scop الثاني هو هقدر اطبق permission علي ال group دى لـ resources ال في انهي domain ، وفيه عندي اكتر من نوع :

هنا هقدر اسحب users من اي domain في ال Domain local -1 ، لكن مقدرش اطبق permission غير علي ال resources في ال trusted domain في ال domain بداعي فقط .

هنا مش هقدر اسحب users غير من ال domain بداعي فقط لكن اقدر اطبق permission على ال resources الموجوده علي اي domain في ال forest وكمان ال trusted domain

هنا اقدر اسحب ال users من اي domain معايا في ال forest و مقدرش اسحب من ال resources علي ال trusted domain الموجوده علي اي domain في ال forest وكمان ال trusted domain

Universal	Global	Domain Local	الميزة
✓	✓	✓	اضافه ال users من نفس Domain
✗	✗	✓	اضافه ال users من ال trusted domain
✓	✗	✓	اضافه ال users من اي forest domain
✓	✓	✗	امكانيه تعين ال permission علي ال resources في ال trusted domain
✓	✓	✗	امكانيه تعين ال permission علي ال resources الموجوده في forest

طيب استخدم انهي فلهم ؟ او اي الافضل

فيه نموذج بيستخدم اسمه IGDLA

Identity <--- I

global <---- G

Domain local <----- DL

Access <----- A

ودا بيقولك انك تضع ال users بداخل global group

ثم تضع ال Domain local group داخل global group

ثم تطبق ال Domain local group على ال access

بكدا هنستفاد بميزات النوعين

Group Policy

هي مجموعة من ال configuration and settings management التي تستخدم في ادارة وتحكم active directory windows في بيئة users accounts وال computers اعدادات ال

مميزاتها :

users devices على كل ال policy موحد one policy : Centralized Control -1

الاً password لجعل ال policy : اقدر اضع Network Security -2

الاً update apps وال : توزيع ال Update and Application Management -3

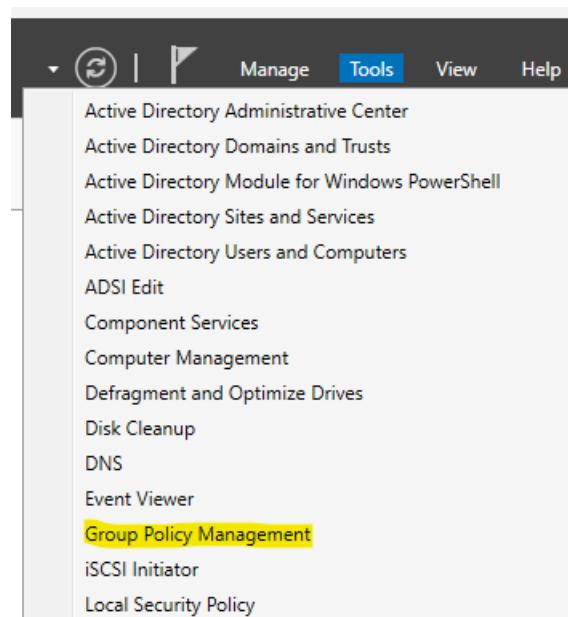
زى اني اعمل : Desktop Settings -4



هي بتطبق على ال OU او ال Domain او على مستوى ال Site

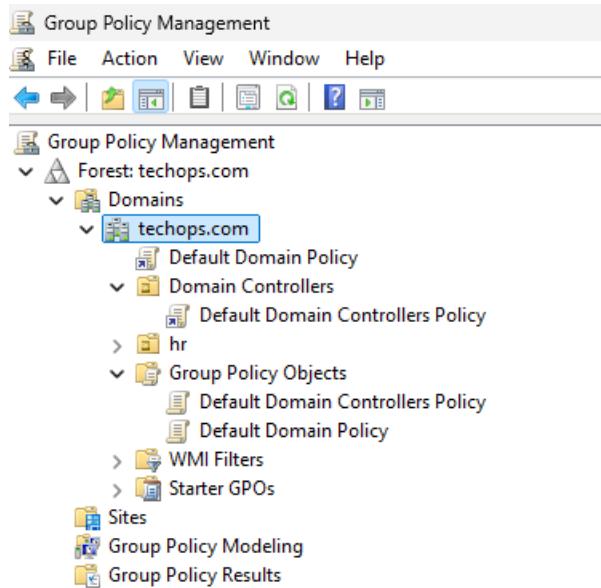
--

طيب ازاي ابدا اشوف ال GP ؟



من Tools هفتح Group Policy management

--



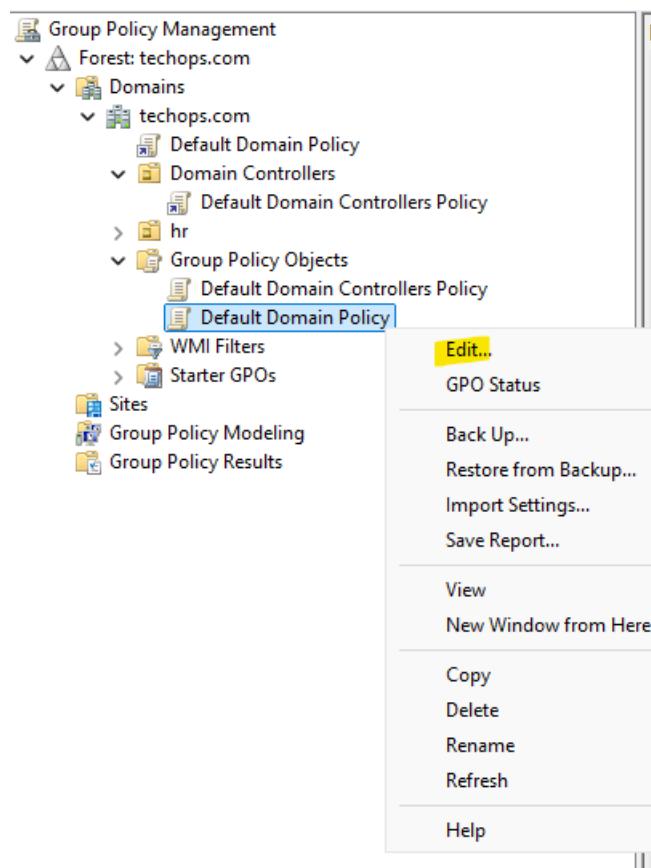
بلاقيها بالشكل دا ومن خلال الشكل هنالاحظ ان ال GP ممكن تطبق علي ال Domain ككل او علي OU او علي Site

كمان هنالاقى 2GP موجودين :

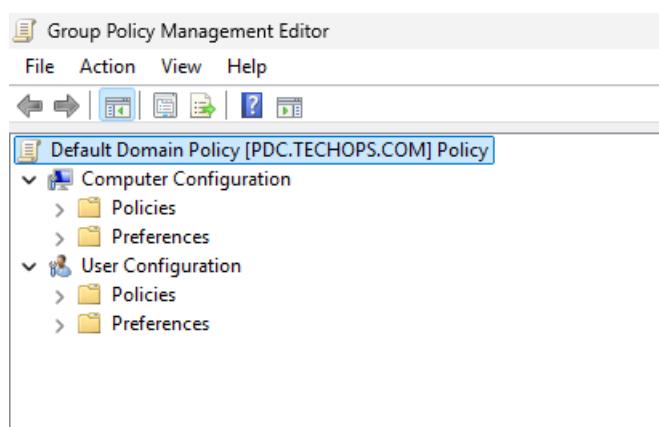
policy : ودي ال policy المطبقه علي ال Domain ككل زي مثلا ال Default Domain Policy الخاصه بال passwords ال هي الحد الادني من طول ال password ومدتها ومدي تعديتها

policy : ودي ال policy الطبقه علي جهاز ال DC نفسه زي ال Default Domain controllers Policy DC events لمراقبه ال Event Log Settings و ال User Rights Assignments

طيب خلينا في ال Default Domain Policy ونغير اعدادات ال passwords



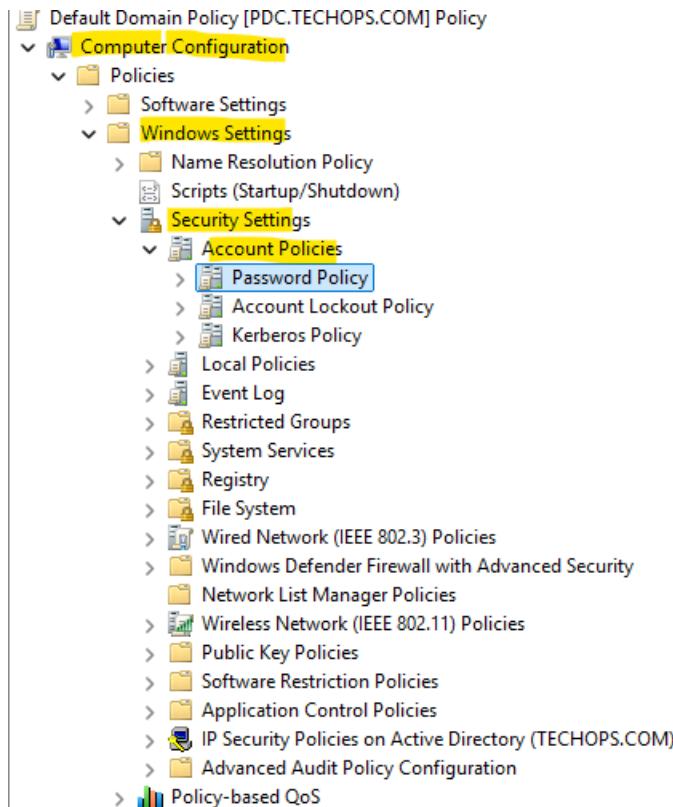
علي ال click هضغط Default Domain Policy وختار edit



اقدر اطبق ال policy علي حاجتين :

و دي ال هطبق على ال devices بعض النظر مين ال Computer Configuration policy .
ال داخل على ال user هيدخل على ال computer دا ال policy دا دي
هفضل مطبقه ، زي مثلا تعطيل ال USB

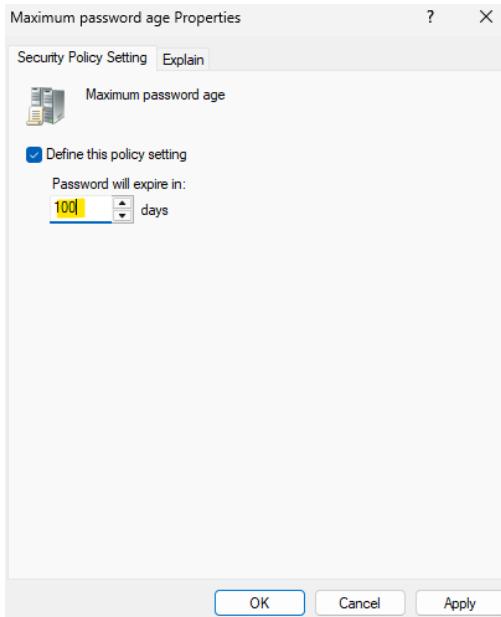
و دي ال المطبقه على ال user نفسه بغض النظر عن ال device : User Configuration
ال بيستخدمه مثلا تعطيل قائمة Run



طيب احنا محتاجين نعدل ال policy الخاصه بال password
هنفتح ال windows settings هختار منه computer config
من ال windows settings هختار security settings
من ال security settings هختار Account policies
من ال Account policies هنلقي ال password policy

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

هلاقي ال policies بال الخاصه passwords

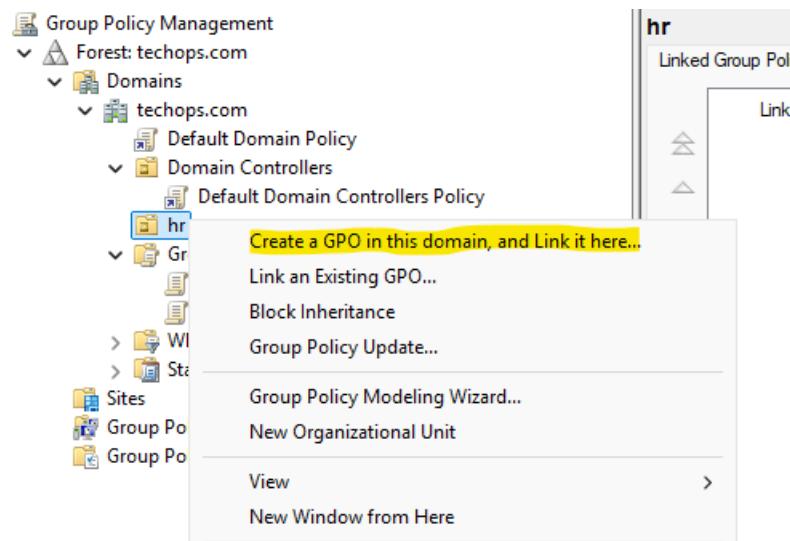


فمثلاً ممكن اعدل ال password expire من 42 يوم ل 100 يوم

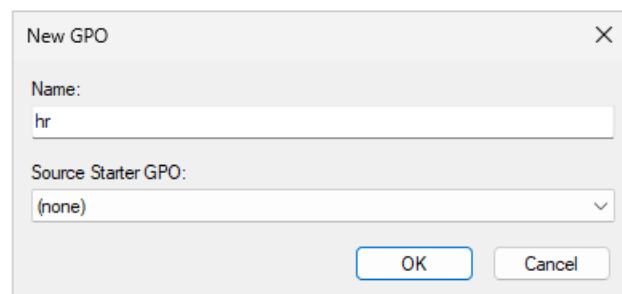
Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	100 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

طيب عاوز ابدا اطبق policy على ال OU ال اسمها hr ؟

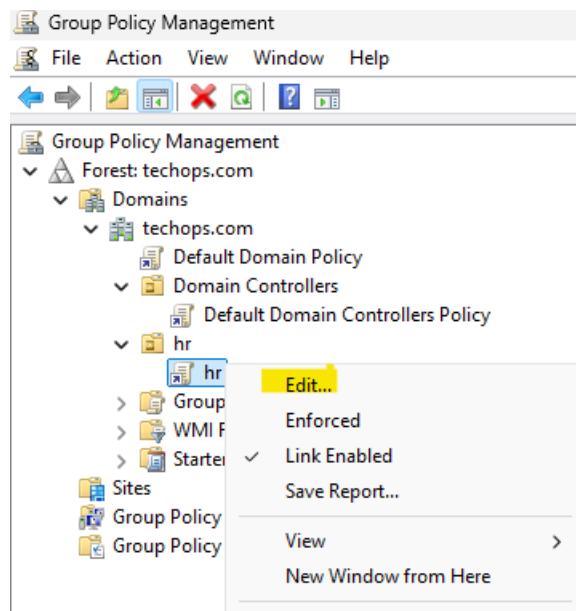
متلا عاوز امنع قائمه run ف ال users ال داخل ال OU دي مقدرش يفتح



Click على ال OU وختار اول اختيار عشان يعمل create و link في نفس الوقت



ال name الخاص بيها



Click على Edit و يعمل

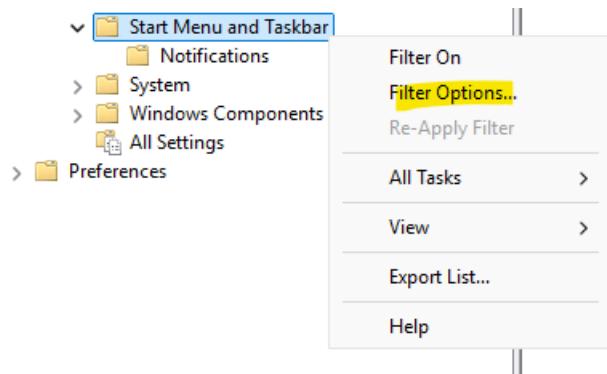
The screenshot shows the Group Policy Management Editor. On the left, the navigation pane displays the policy structure: 'hr [PDC.TECHOPS.COM] Policy / Computer Configuration / Policies / User Configuration / Policies / Administrative Templates: Policy definitions (ADI) / Start Menu and Taskbar / Notifications'. The right pane, titled 'Start Menu and Taskbar', lists various policy settings with their current state and comments. The table has columns for 'Setting', 'State', and 'Comment'.

Setting	State	Comment
Add Search Internet link to Start Menu	Not configured	No
Clear history of recently opened documents on exit	Not configured	No
Clear the recent programs list for new users	Not configured	No
Clear tile notifications during log on	Not configured	No
List desktop apps first in the Apps view	Not configured	No
Disable context menus in the Start Menu	Not configured	No
Remove Quick Settings	Not configured	No
Search just apps from the Apps view	Not configured	No
Add Logoff to the Start Menu	Not configured	No
Force Start to be either full screen size or menu size	Not configured	No
Go to the desktop instead of Start when signing in	Not configured	No
Gray unavailable Windows Installer programs Start Menu sh...	Not configured	No
Remove the People Bar from the taskbar	Not configured	No
Remove "Recently added" list from Start Menu	Not configured	No
Remove Personalized Website Recommendations from the ...	Not configured	No
Remove Recommended section from Start Menu	Not configured	No
Turn off personalized menus	Not configured	No
Lock the Taskbar	Not configured	No
Start Layout	Not configured	No
Add "Run in Separate Memory Space" check box to Run dial...	Not configured	No
Turn off notification area cleanup	Not configured	No
Remove Balloon Tips on Start Menu items	Not configured	No
Prevent users from customizing their Start Screen	Not configured	No
Remove and prevent access to the Shut Down, Restart, Sleep...	Not configured	No
Remove common program groups from Start Menu	Not configured	No
Remove Favorites menu from Start Menu	Not configured	No
Remove Search link from Start Menu	Not configured	No
Remove frequent programs list from the Start Menu	Not configured	No
Remove Games link from Start Menu	Not configured	No
Remove Help menu from Start Menu	Not configured	No
Turn off user tracking	Not configured	No
Remove All Programs list from the Start menu	Not configured	No
Remove Network Connections from Start Menu	Not configured	No
Remove pinned programs list from the Start Menu	Not configured	No

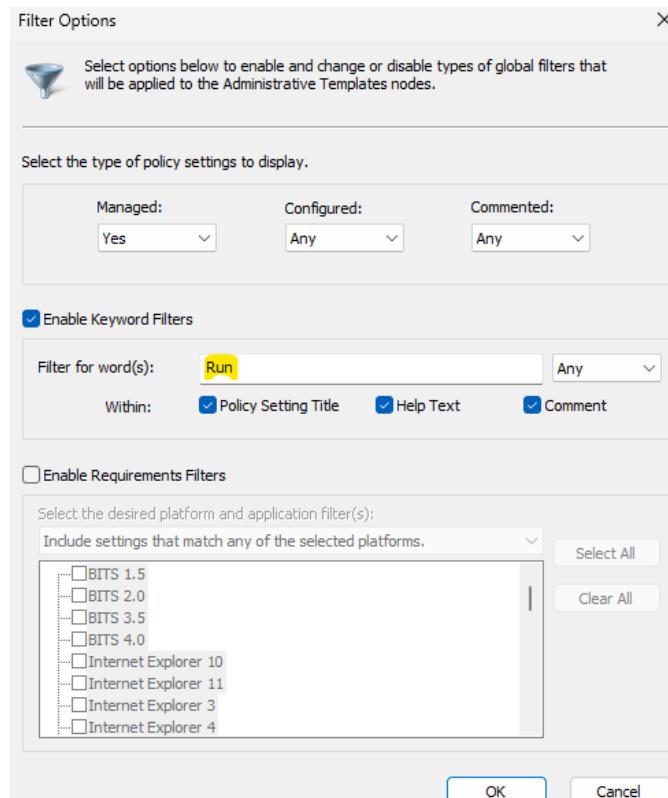
من User config policy هختار منها

ومن ال Administrative Start Menu and taskbar هختار

عندی filters كتير ف بدل ما ادور كتير ممكن اعمل options



filter options على ال start menu Click



بقوله اعرضلي كل ال policy ال فيها كلمة Run

hr [PDC.TECHOPS.COM] Policy

- Computer Configuration
- User Configuration
- Administrative Templates: Policy definitions (ADI)
 - Start Menu and Taskbar

Setting	State	Comment
Start Layout	Not configured	No
Add "Run in Separate Memory Space" check box to Run dia...	Not configured	No
Remove Run menu from Start Menu	Not configured	No
Show "Run as different user" command on Start	Not configured	No
Add the Run command to the Start Menu	Not configured	No

هیعرض کل ال فیها کلمہ Run مختار

Remove Run menu from start menu

Remove Run menu from Start Menu

Comment:

Not Configured

Enabled

Disabled

Supported on: Windows Server 2012 R2, Windows 8.1, Windows RT 8.1, Windows Server 2008, Windows Server 2003, Windows 7, Windows Vista, Windows XP, and Windows 2000

Options:

Help:

Allows you to remove the Run command from the Start menu, Internet Explorer, and Task Manager.

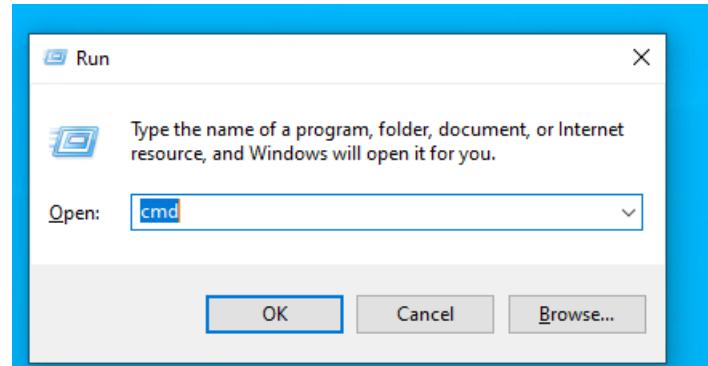
If you enable this setting, the following changes occur:

- (1) The Run command is removed from the Start menu.
- (2) The New Task (Run) command is removed from Task Manager.
- (3) The user will be blocked from entering the following into the Internet Explorer Address Bar:
 - A UNC path: \\<server>\<share>
 - Accessing local drives: e.g., C:
 - Accessing local folders: e.g., \temp>

Also, users with extended keyboards will no longer be able to display the Run dialog box by pressing the Application key (the

OK Cancel Apply

عمل Enable لے policy



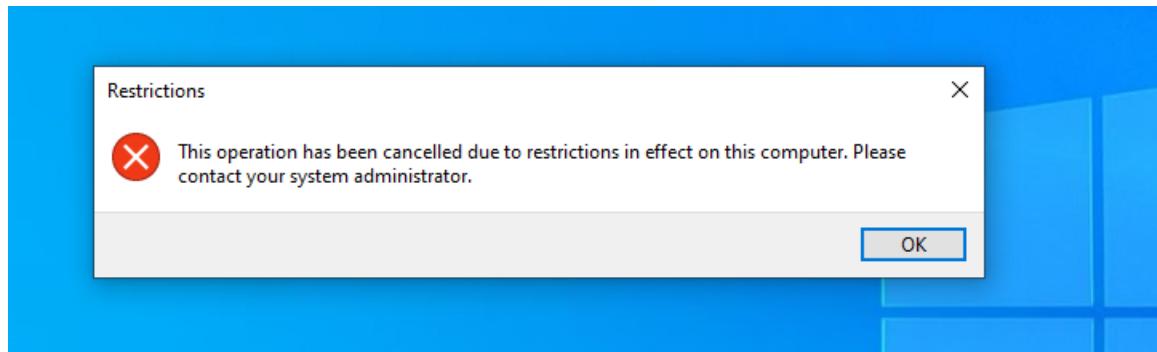
طيب عند ال user لسه بقدر افتح ال Run ؟
لان لسه ال محصلهاش update ف ممكن اعمل restart لل pc او اعمل gpupdate

```
C:\Users\mostafa.mahmoud>gpupdate
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\mostafa.mahmoud>
```

كدا بعمل update لل policy

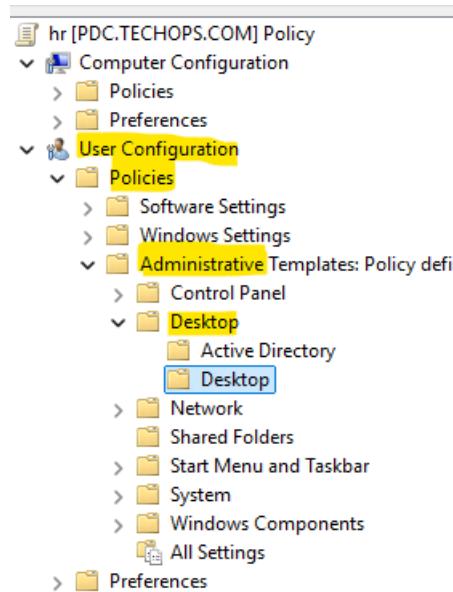
--



لما بفتح ال Run بعد ال update لل policy لما بفتح ال Run بعد ال update لل policy

طيب مثلًا عاوزين نغير ال wallpaper ونخليها واحده للكل ؟

لازم احط الصوره في folder يكون sharing



هروح على ال User Config ومنها policies

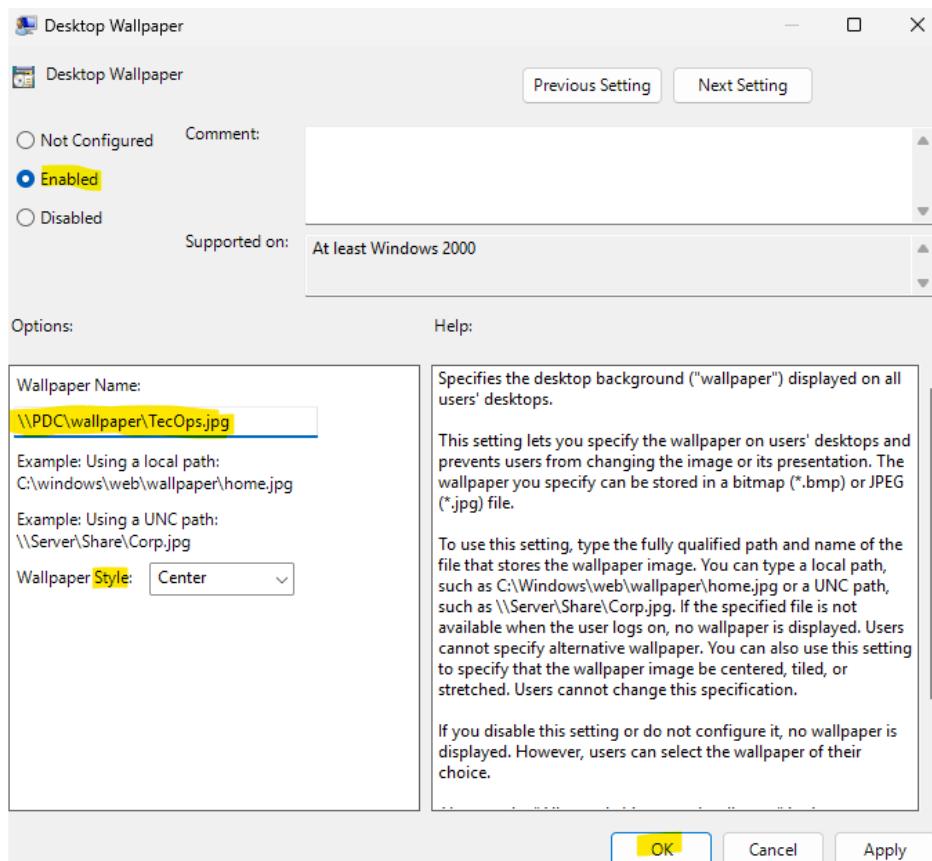
من Desktop policies ومنها هدخل لـ administrative

ومن desktop هختار desktop

--

Setting	State	Comment
Enable Active Desktop	Not configured	No
Disable Active Desktop	Not configured	No
Prohibit changes	Not configured	No
Desktop Wallpaper	Not configured	No
Prohibit adding items	Not configured	No
Prohibit closing items	Not configured	No
Prohibit deleting items	Not configured	No
Prohibit editing items	Not configured	No
Disable all items	Not configured	No
Add/Delete items	Not configured	No
Allow only bitmapped wallpaper	Not configured	No

هلاقي عندي Desktop wallpaper



عملها wallpaper style وبعد كدا هكتبle ال network path ال فيه الصوره وختار ال عاوزه



recycle Bin



Google
Chrome



TechOps

هنعمل gupdate و بعد كدا logout و تاني هنلاقي ال wallpaper اتغيرت

طيب تعال نوقف مثلاً ال USB ؟

The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane displays a tree structure of policies under 'hr [PDC.TECHOPS.COM] Policy'. Under 'Computer Configuration' > 'Policies' > 'Administrative Templates: Policy definitions (ADT)' > 'System' > 'Removable Storage Access', the 'Removable Storage Access' policy is selected. The right pane, titled 'Removable Storage Access', lists various settings with their current state and comments. The 'Removable Disks: Deny read access' setting is highlighted.

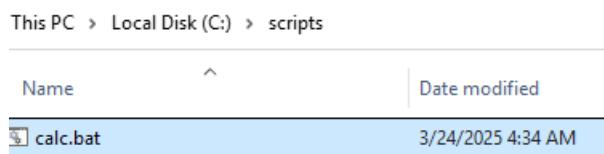
Setting	State	Comment
Set time (in seconds) to force reboot	Not configured	No
CD and DVD: Deny read access	Not configured	No
CD and DVD: Deny write access	Not configured	No
Custom Classes: Deny read access	Not configured	No
Custom Classes: Deny write access	Not configured	No
Floppy Drives: Deny read access	Not configured	No
Floppy Drives: Deny write access	Not configured	No
Removable Disks: Deny read access	Not configured	No
Removable Disks: Deny write access	Not configured	No
All Removable Storage classes: Deny all access	Not configured	No
Tape Drives: Deny read access	Not configured	No
Tape Drives: Deny write access	Not configured	No
WPD Devices: Deny read access	Not configured	No
WPD Devices: Deny write access	Not configured	No

من ال system policies ومنها administrative config ومنها user config
وتحت removable storage access system

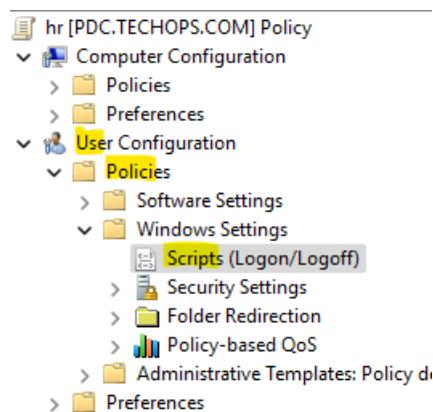
ومن ال RSA هنلقي ال removable Disk ودي ال يقصد بيهما ال USB وافق اعمل Deny لل
فقط او ال read فقط او الاثنين مع بعض

--

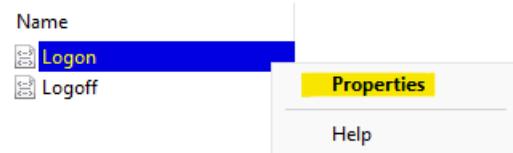
طيب مثلا لو عاوز انفذ scripts اول ما ال user يعمل logon ؟



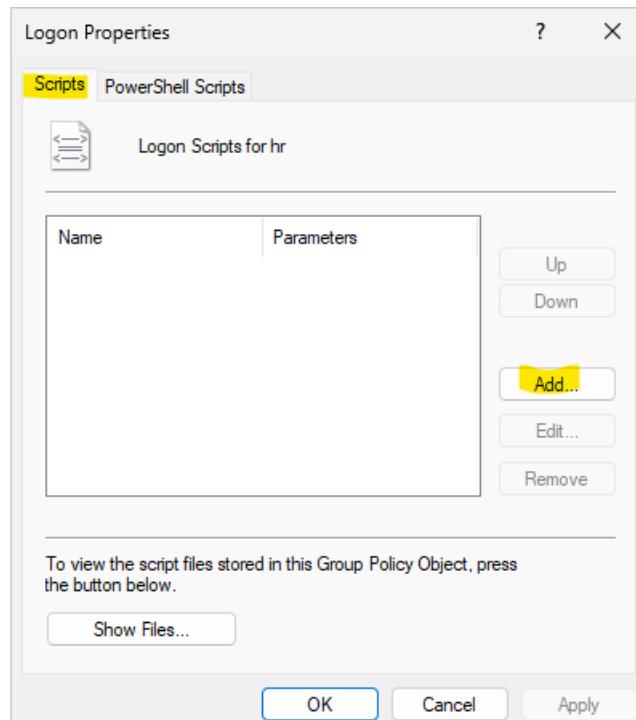
لو عاوز اعمل script يفتح ال calc اول ال user يعمل logon
هعمل file واتكتب فيه الامر calc وهمعمل save لـ file بالامتداد bat
ولازم ال folder يكون فيه sharing
يعني هو داخل folder اسمه scripts ف لازم يكون فيه sharing



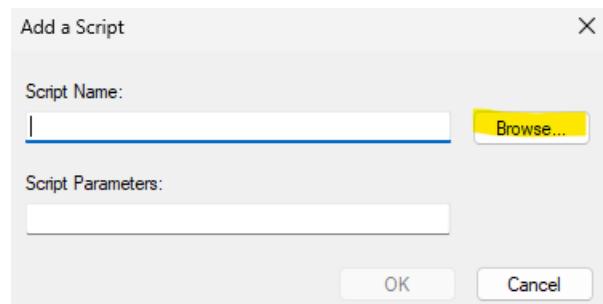
فتح ال windows settings policies ومنها فيه scripts



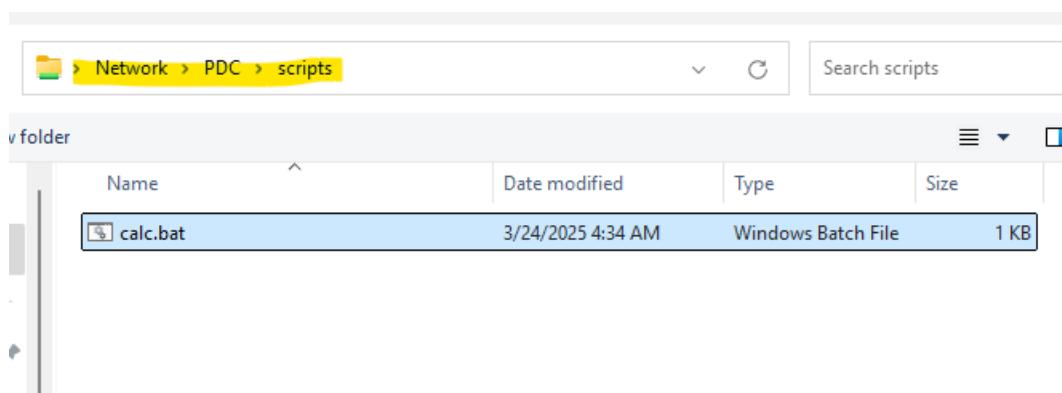
هقوله ال script بتنفذ لما اعمل logon اف هضغط click عليها وفتح ال properties



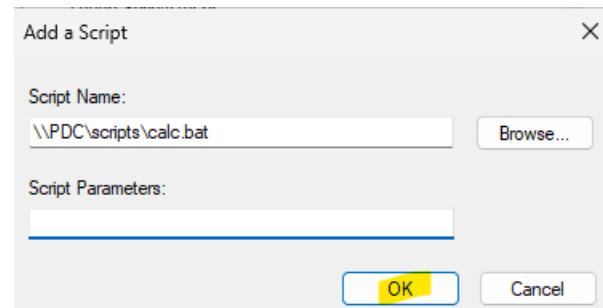
من Add scripts هعمل



بعد كدا هعمل browse



ختار ال script بتاعي بس من ال Network Path يعني مسار ال share بتاعه ال هو <\\PDC\\scripts>

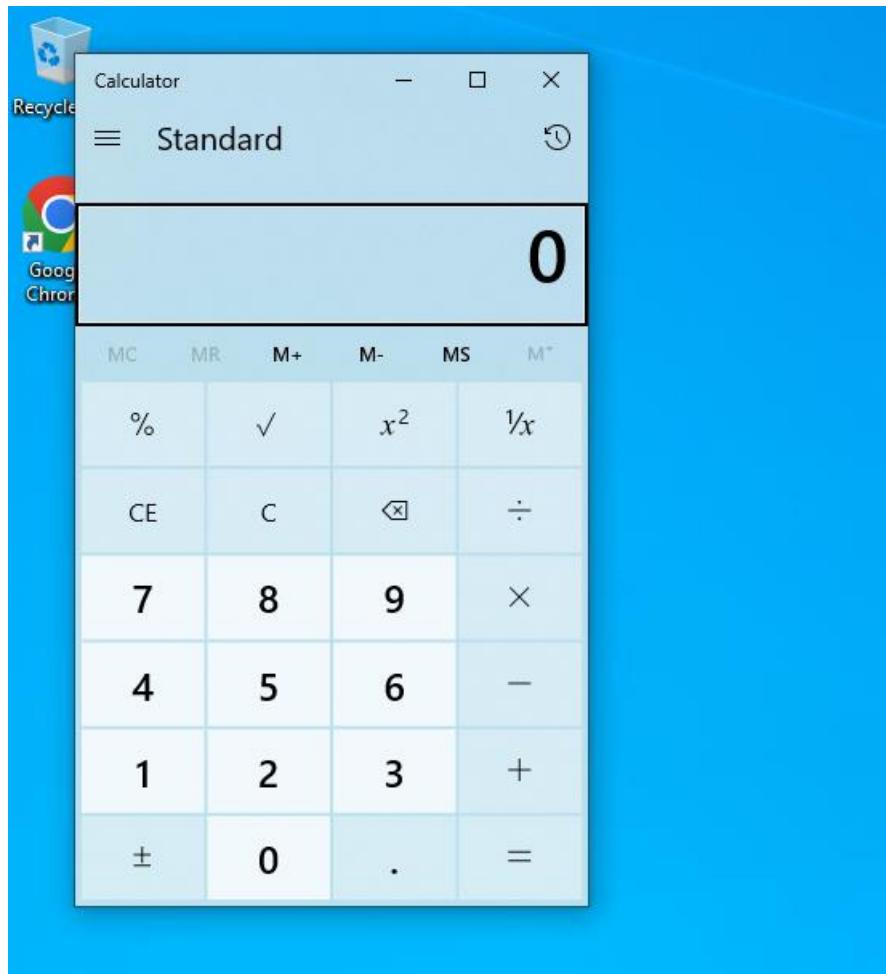


Ok

```
C:\Users\mostafa.mahmoud>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

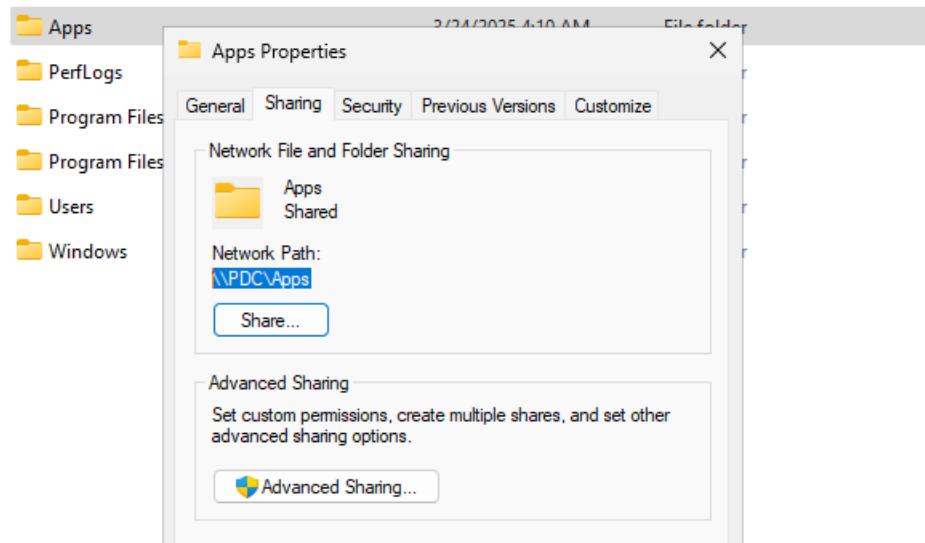
C:\Users\mostafa.mahmoud>
```

عند ال عمل update لـ client وبعد كدا نعمل logon و logout تانى

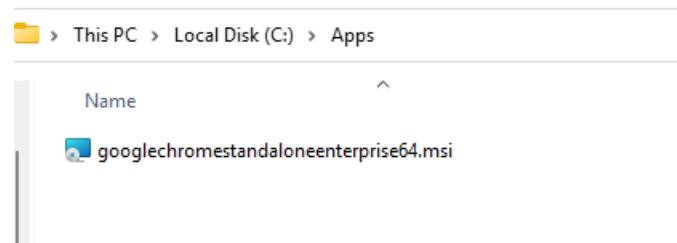


اول ما هتعمل logon هتلaci script تم تنفيذه وال calc افتحت

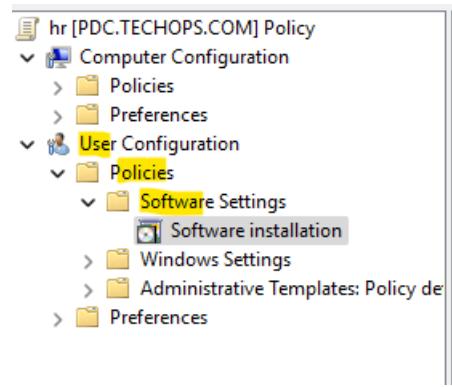
طيب لو عاوز اعمل applications install ل users معينه عند ال
اول شي لازم ال application install هيتعمله يكون بصيغه MSI
ولازم يكون داخل folder معموله sharing



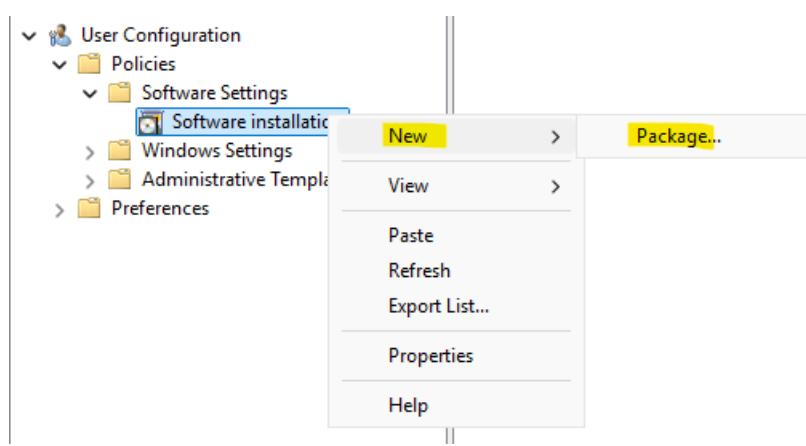
ف انا عندي share folder عملته



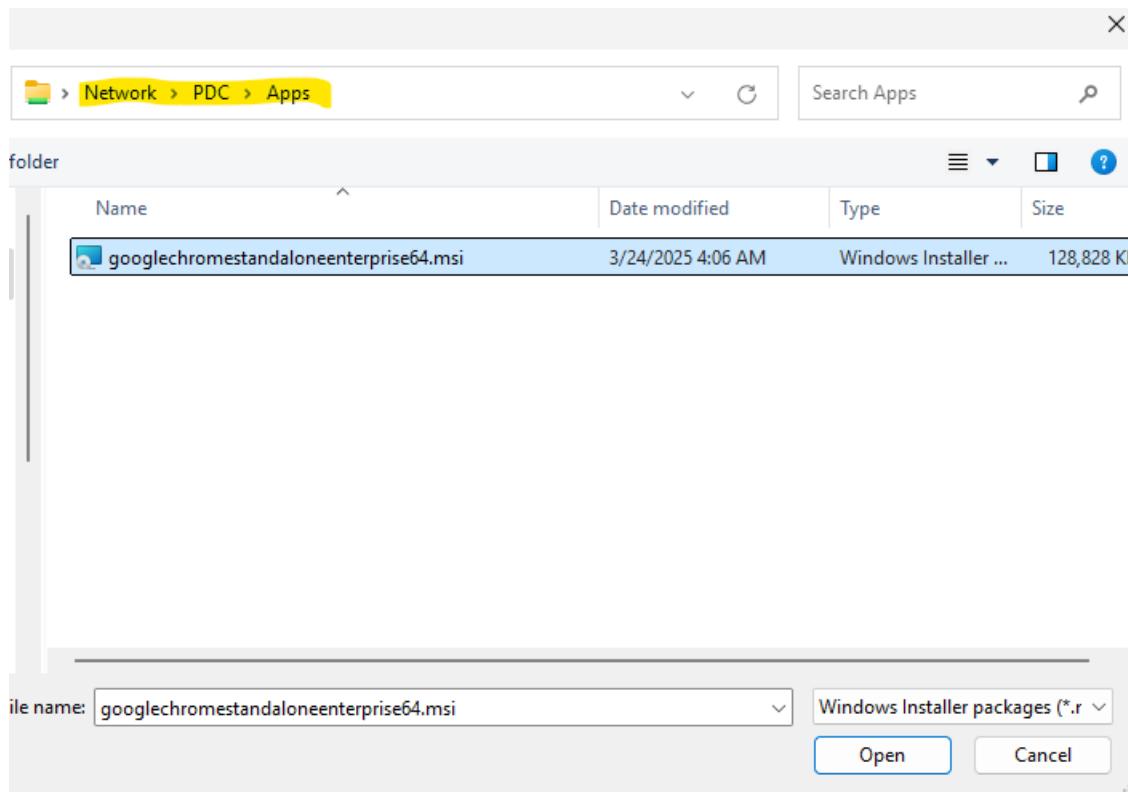
داخل ال folder عندي MSI بامتداد Google Chrome



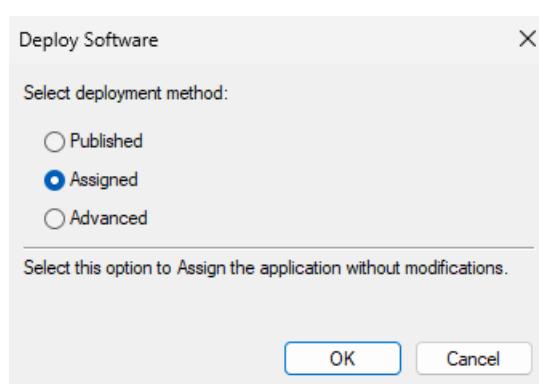
هروح على policies وفتح ال user config منها هلاقي
هلاقي software installation



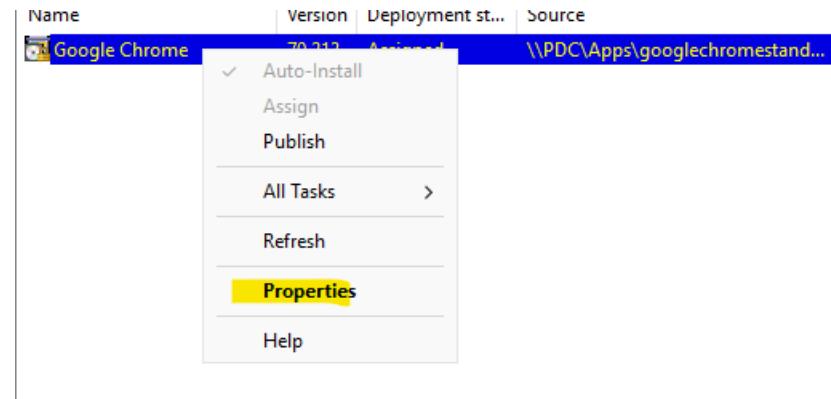
علي packages new وختار software installation Click



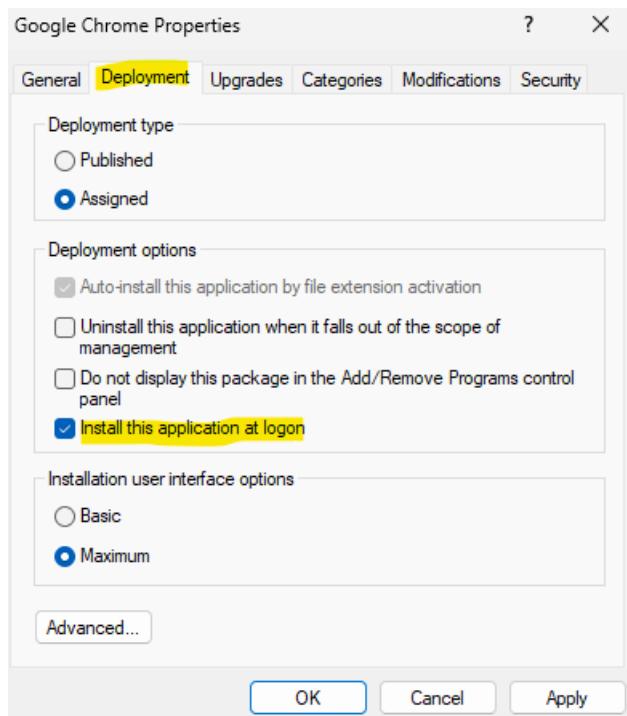
هختار ال application لكن من ال Network Path بتعايي ال هو كان \PDC\Apps



في ال Assigned هختار deploy



properties عليه و هختار Click



بعد كدا هدخل على Deployment check على Install this application at logon ومنها هعمل عمل user اول ما ال install وبكدا هيتعمله

```
C:\Users\mostafa.mahmoud>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

The following warnings were encountered during user policy processing:
The Group Policy Client Side Extension Software Installation was unable to apply one or more settings because the changes must be processed before system startup or user logon.
cy processing to finish completely before the next startup or logon for this user, and this may result in slow startup and boot performance.

For more detailed information, review the event log or run GPRESULT /H GPRReport.html from the command line to access information about Group Policy results.

Certain user policies are enabled that can only run during logon.

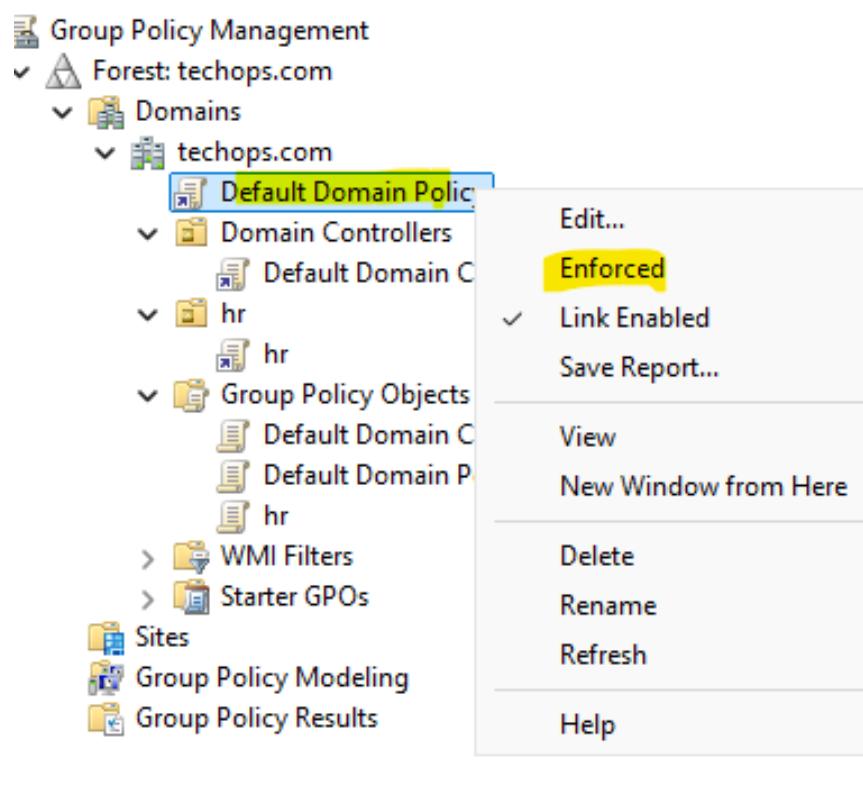
OK to log off? (Y/N) y -
```

من ال user لما عملت gpupdate /force بيقول ان عندك policy مش هتطبق غير لما تعمل application ال هو ال install لـ logon و logout



بعد ال logon اتعمله app install automatic

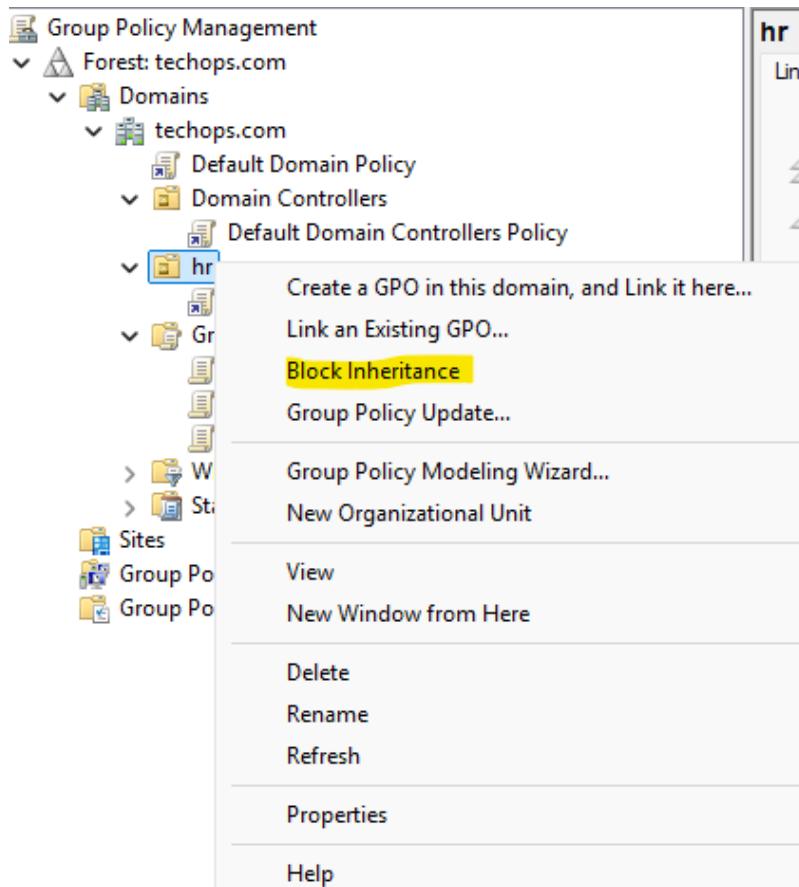
طيب لو بعد ما عملت ال GP على ال OU
و فيه تعارض بين ال GP ال على OU وال على ال Domain
لو عاوز ال Domain GP هي ال تتنفذ:



عليها و هختار Click

--

لو انت عاوز ال GP ال على ال OU هي ال هتطبق



Block Inheritance على ال OU وتعمل Click

طيب لو عاوز اعرف انا غيرت في انهي policy داخل ال GP دي ؟

The screenshot shows the Group Policy Management console. On the left, the navigation pane displays the following structure:

- Group Policy Management
- Forest: techops.com
- Domains
- techops.com
 - Default Domain Policy
 - Domain Controllers
 - Default Domain Controllers Policy
 - hr
 - Default Domain Controllers Policy
 - Default Domain Policy
 - hr
 - Group Policy Objects
 - Default Domain Controllers Policy
 - Default Domain Policy
 - hr
 - WMI Filters
 - Starter GPOs- Sites
- Group Policy Modeling
- Group Policy Results

The right pane shows the details for the 'hr' GPO. The 'Settings' tab is selected. The 'General' section includes tabs for Details, Links, Security Filtering, and Delegation. The 'Computer Configuration (Enabled)' section is expanded, showing the following sub-sections:

- Policies
- Software Settings
- Assigned Applications
- Windows Settings
- Scripts
- Administrative Templates

Data collected on: 3/24/2025 4:55:42 AM

No settings defined.

هفتح ال GP واروح علي ال setting بتاعتها هلاقي كل ال policies ال انا عدلت فيها

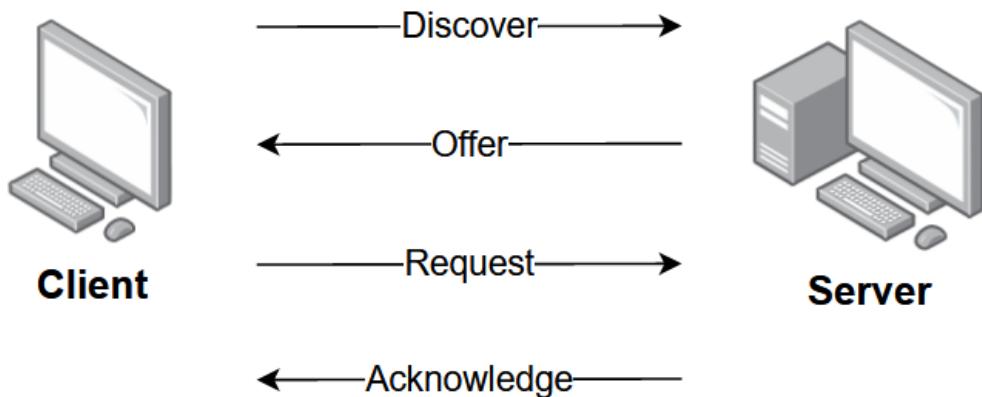
DHCP

اختصاراً DHCP Dynamic Host Configuration Protocol
ودا بيشتغل UDP على Port 67 و 68 و هنعرف ليه بيشتغل على 2 port
وال DHCP بيستخدم لتوزيع ال Network Configuration زى :

IP ➤
Subnet mask ➤
Default Gateway ➤
DNS ➤

طيب ازاي بيبدأ يوزع ال config دي ؟

ال process بتاعته بتمر ب 4 مراحل تعرف ب عملية ال DORA



- 1 : هنا ال DHCP Discover بيعت Broadcast عبر ال Client لجميع الاجهزه الموجوده والهدف منها البحث عن ال DHCP Server
- 2 : ال DHCP Offer لما توصله ال Discover بيعت ال offer بتاعه ودا بيحتوي على ال IP المتاح وباقى ال network config زى ال DNS وال Gateway
- 3 : وهنا ال DHCP Request Client بيعت DHCP Request لل Server بيؤكد انه تمام هيسخدم ال IP وال config الي تم ارسالها في ال offer
- 4 : ال DHCP Acknowledge : هنا ال Client بيؤكد انه تم تخصيص ال IP دا لل Client

و هنا نبدا نعرف ليه ال DHCP بيستخدم 2 port

DHCP Server 67 خاص بال

DHCP Client 68 خاص بال

--

لما ال client بياخذ ال ip من ال DHCP Server بيتم تعين له فترة تسمى بال Lease Time وبعد مرور 50% من المدة دي ال client بيحاول تجديد ال ip بشكل automatic وإذا لم يتم تجديده سيعاول مره اخره عندما يصل لـ 87.5% من الفترة

اذا لما يتستطيع ال client تجديد ال ip قبل انتهاء هذه المدة سيفقد ال ip الخاص به وسوف يحاول طلب ip جديد

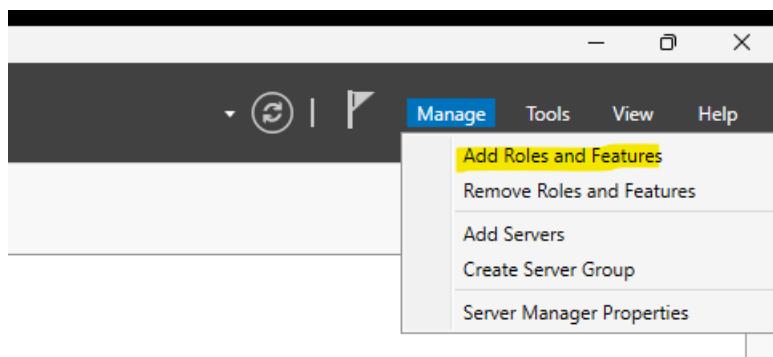
مدة ال Lease Duration By default 8 ايام وطبعا اقدر اعدلها علي حسب ما اناحتاج

--

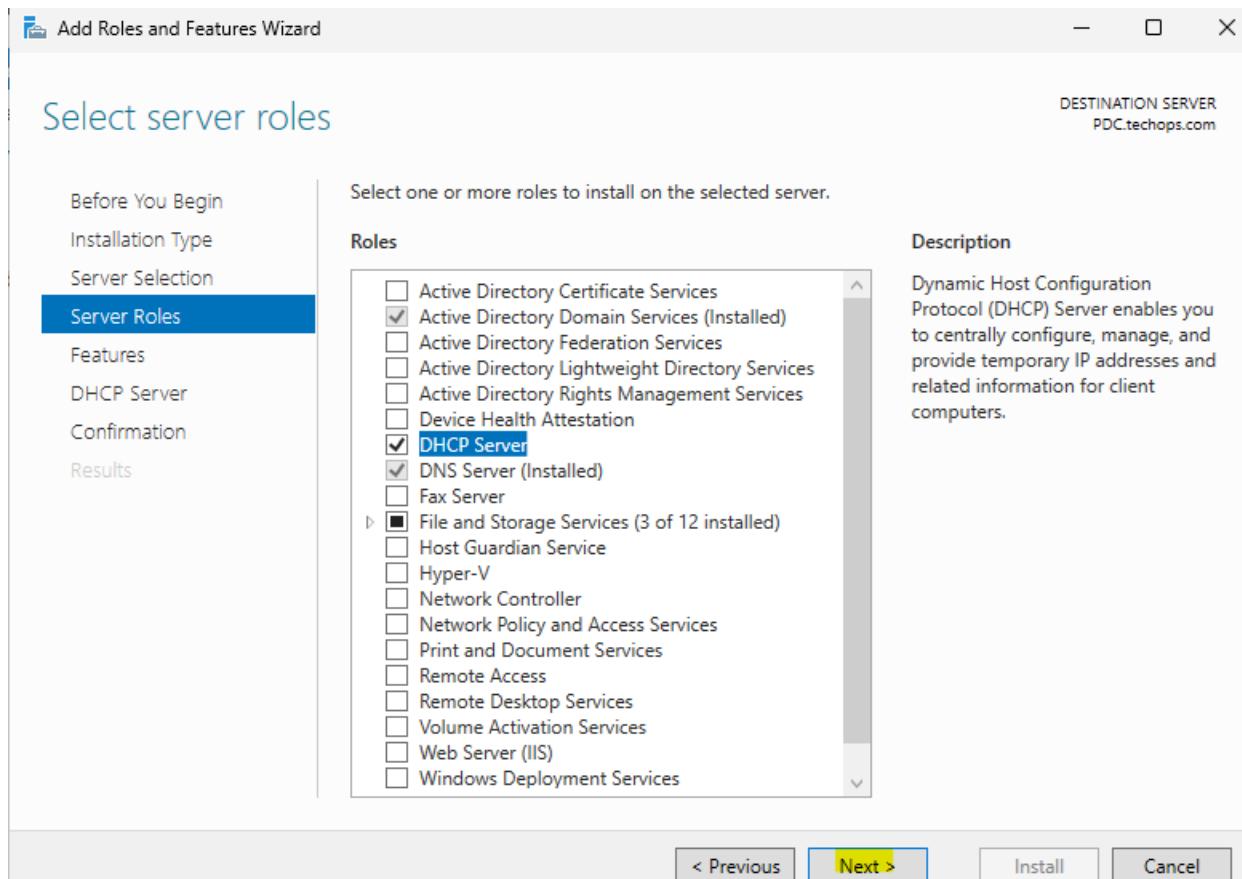
طيب ازاي ابدا استخدم ال DHCP ؟

كالعادة هنبدأ نسطب ال service الخاصه بيه

--

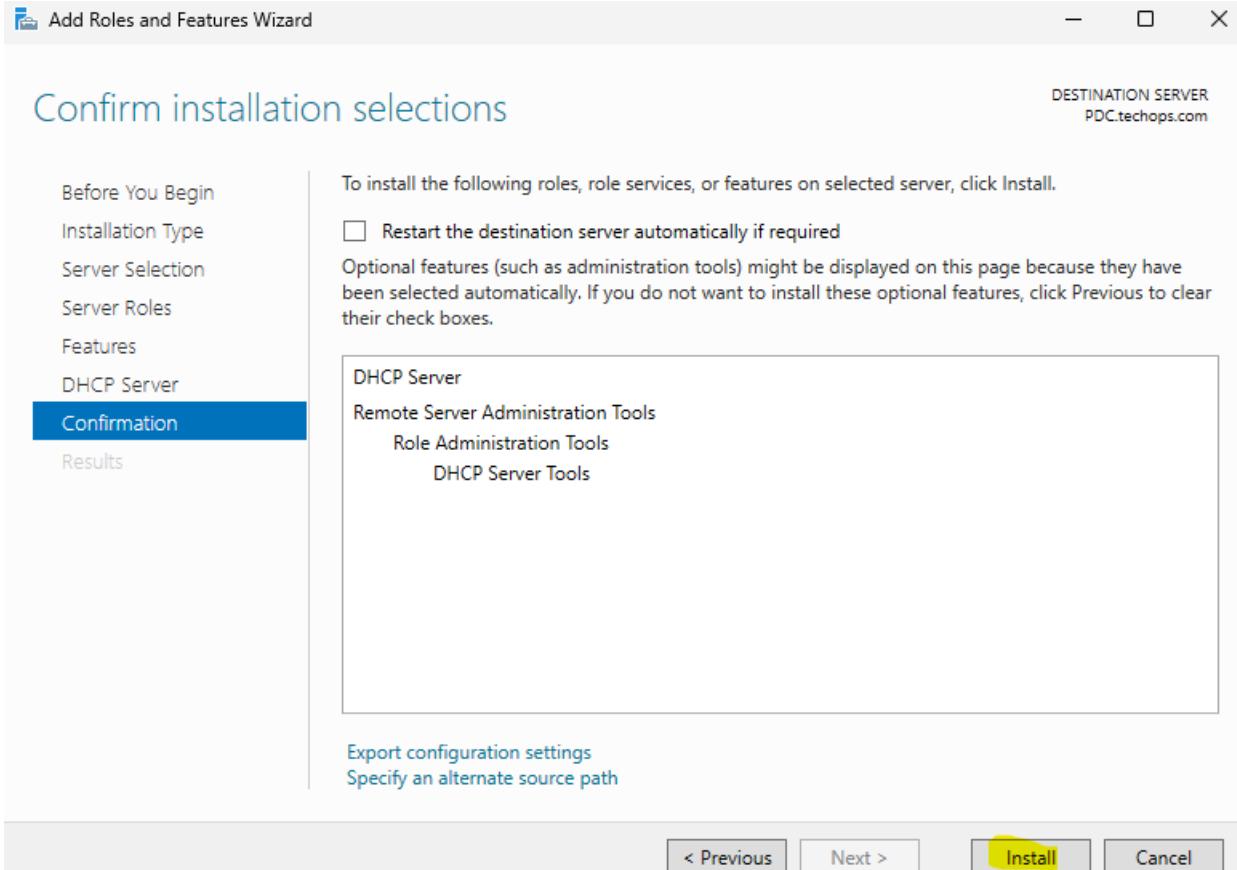


من ال Add Roles and Features وختار Manage هروح علي server manager



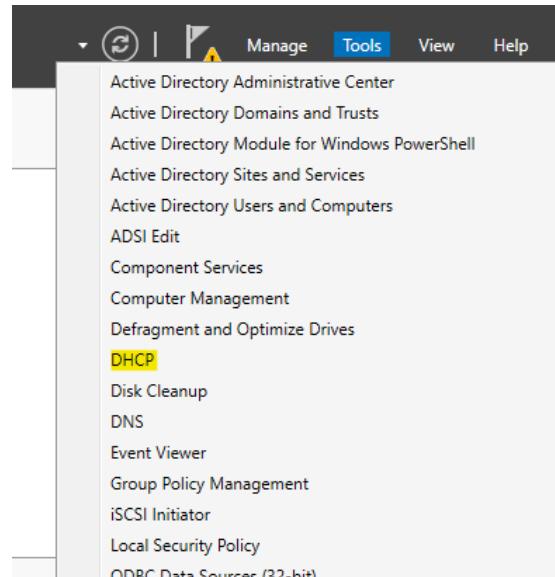
هختار ال DHCP Server

--

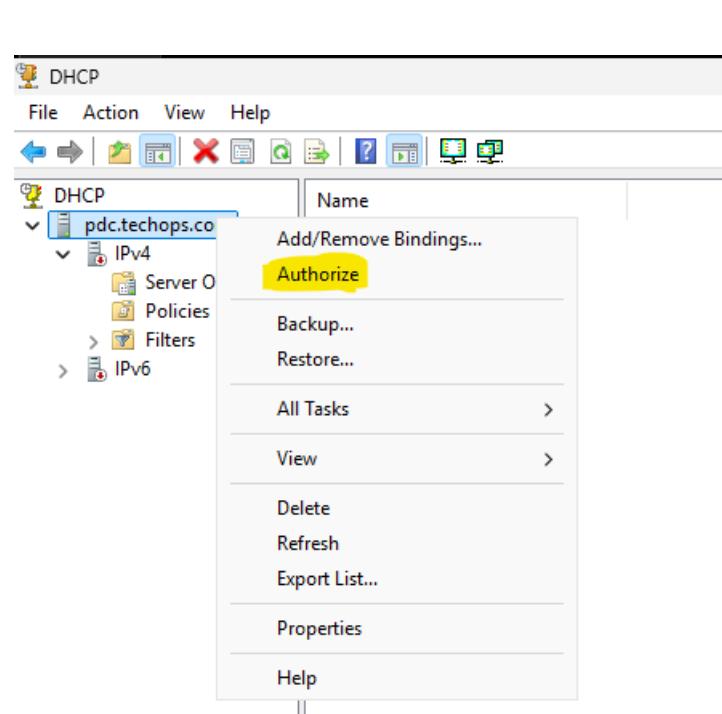


Install

بعد كدا هنبدأ نعمل ال config

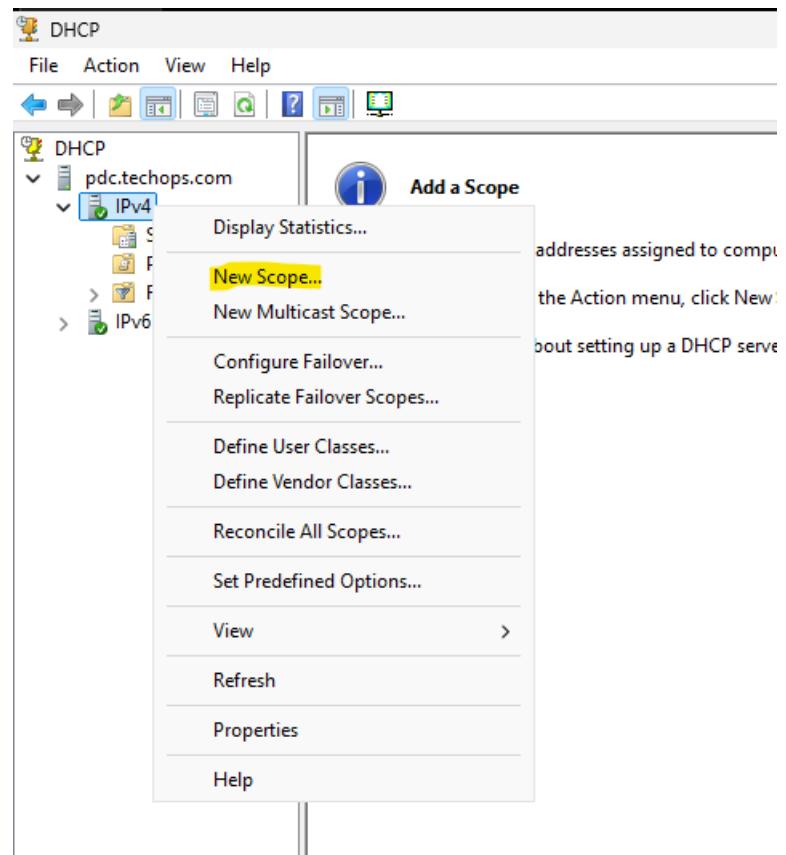


من Tools هنفتح ال DHCP



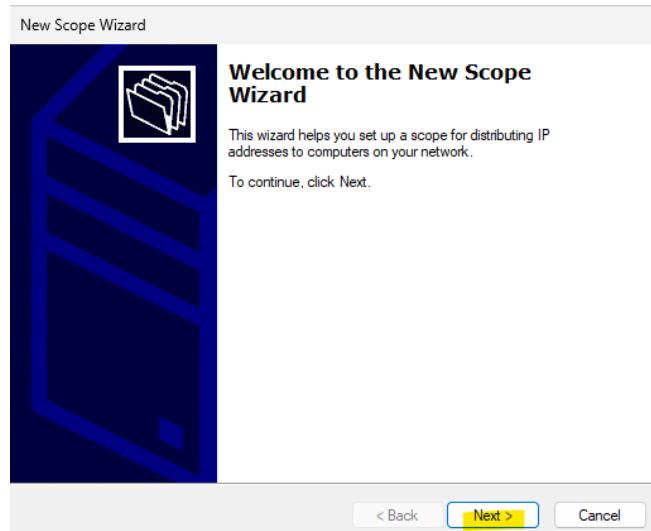
Authorize على ال domain name وختار Click

بعد كدا ببدا اعمل create لل scope بتاعتي ودي ال هتوزع ال config



New Scope على IPv4 وختار Click

--



Next

New Scope Wizard

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

نام و توصیف را بنویس

Next

New Scope Wizard

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

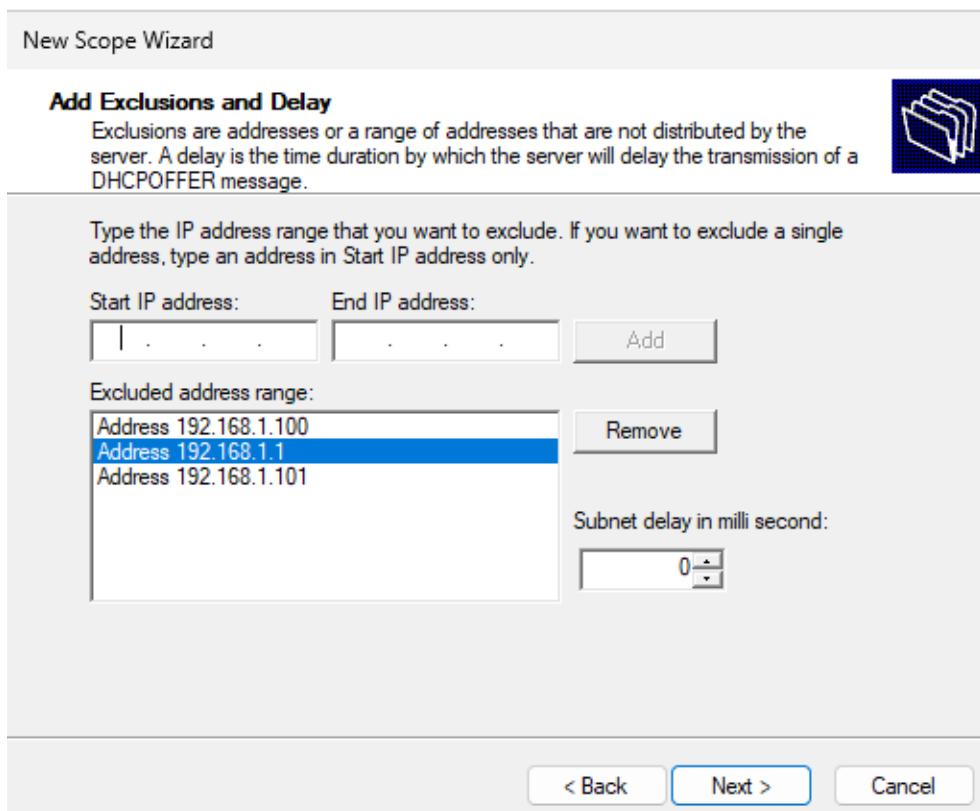
Next >

Cancel

بحدد ال start ip وال end ip

وبحدد ال subnet mask

--



هذا بعمل exclusions لبعض ال ips ال مش عاوز ال DHCP يوزعها
 زي ال router او ال firewall
 زي ip ال PDC وال
 ممكن كمان اعمل exclusions رنج معين من ال servers او ال printers استخدمهم static لـ

وهنا في حاجه اسمها subnet delay in milli second ودي عشان لو عندي اكتر من Server ف اكتر حدد مين ال يرد الاول على ال Client من خلالها يعني لو دا عاوزه هو ال يرد الاول هسيبيه 0 زي ما هو وعلى ال DHCP Server الثاني مثلا اخليها 100 milli second فمعني كدا الاقل هو ال هيرد اسرع

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

< Back

Next >

Cancel

ال Lease Duration يزيد ما قولنا ان تكون 8 ايام وتقدر تعديها زي ما انت تحتاج

--

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

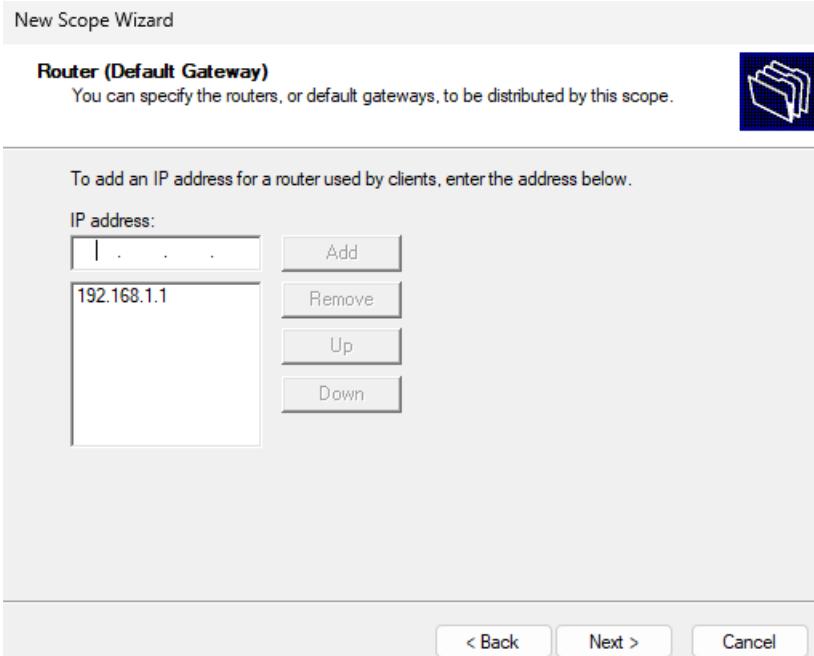
< Back

Next >

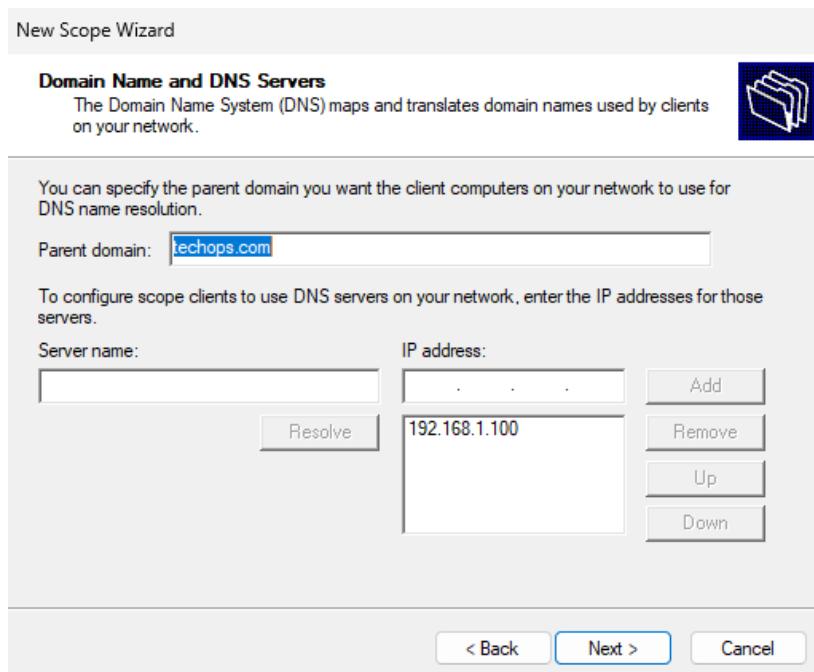
Cancel

هذا بيسالني اذا كنت تحتاج اضبط configuration تانيه ولا لا
فهقوله yes عشان نضبط ال subnet mask على الاقل
واكيد لو ال network طالعه انترنت فهحتاج اضبط ال DNS وال Gateway

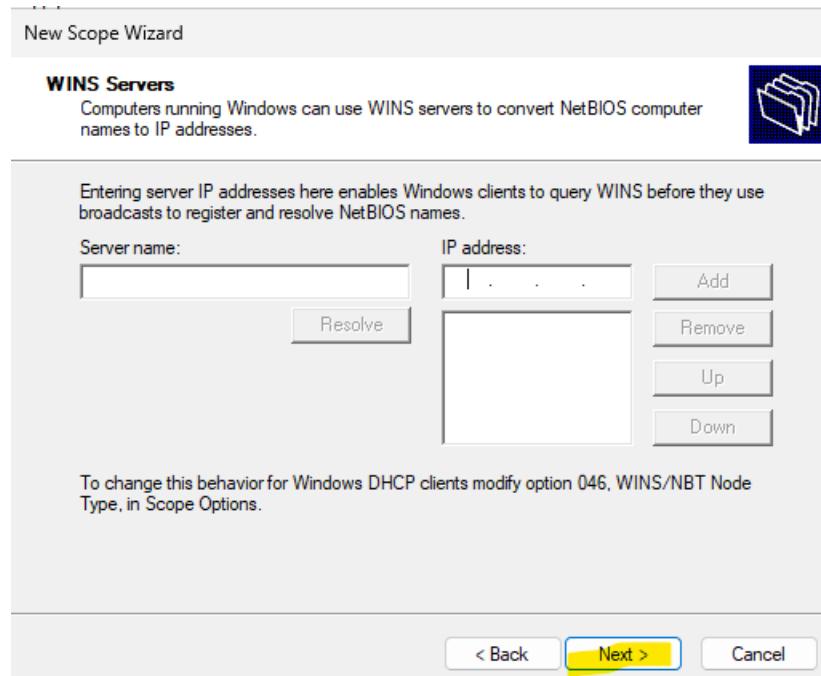
--



هنا بحدد ال **Gateway**

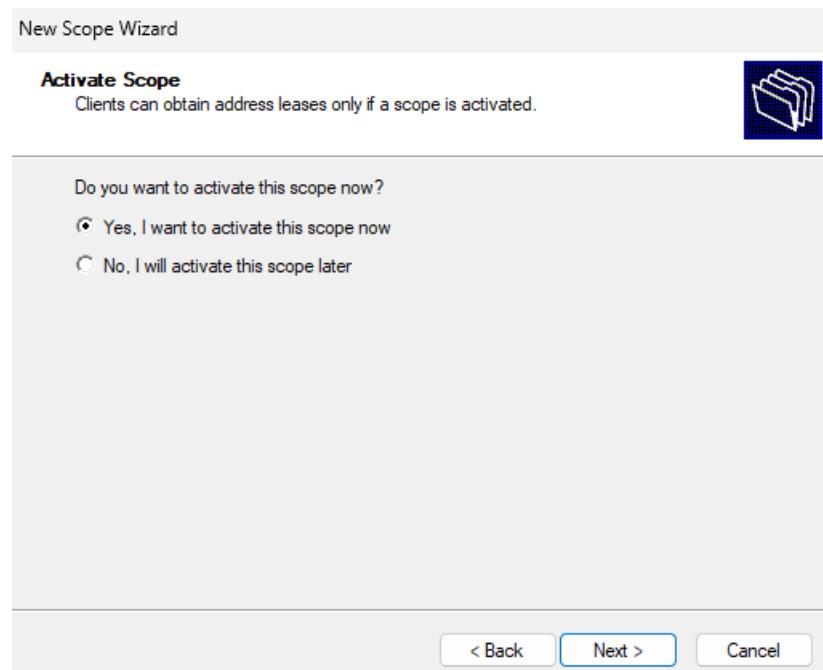


بحدد ال **DNS**



بیسالني عن ال WINS Server ودا سيرفر قديم ومش مستخدم حاليا كان مهمته بيوزع ال NetBIOS و Name

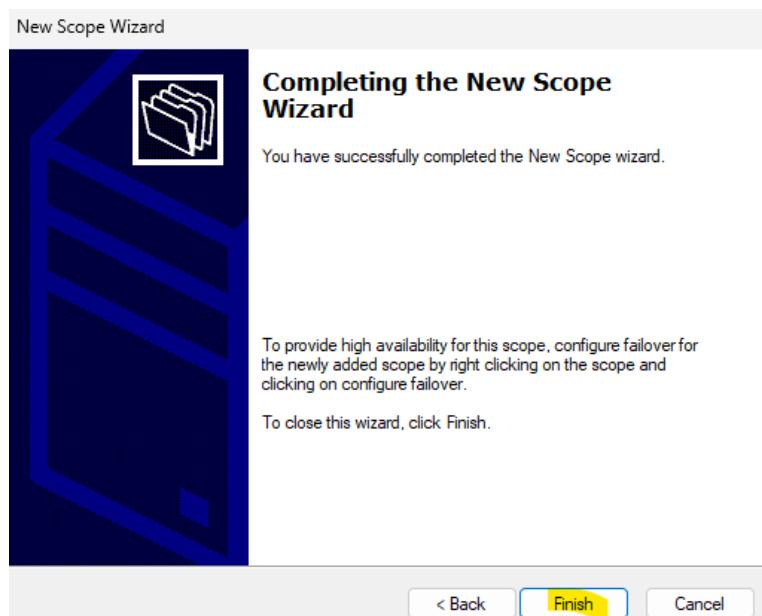
--



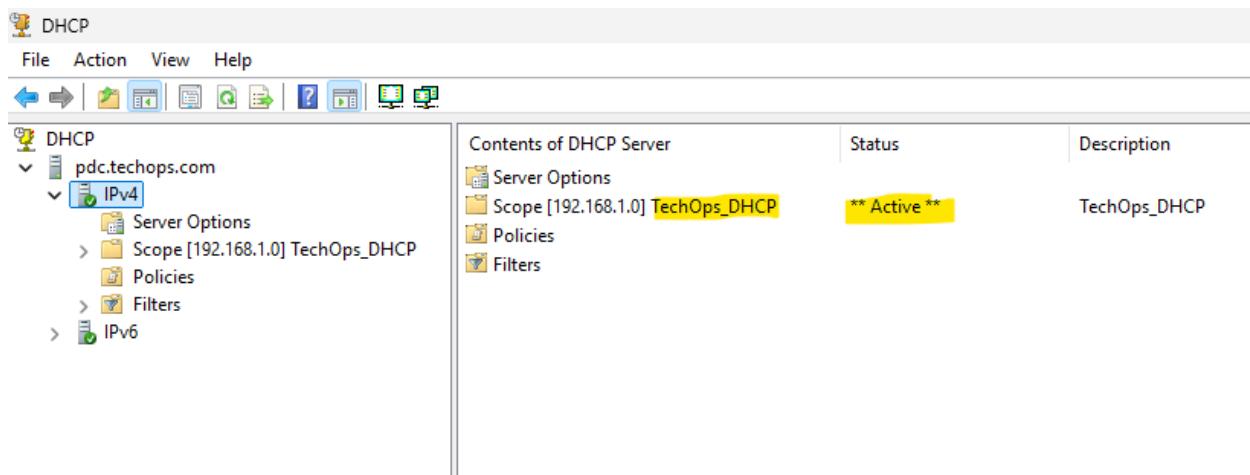
بیسانی هل يعمل activate لل scope دلوقت ولا لا

فهقوله yes عشان يعملها او enable active

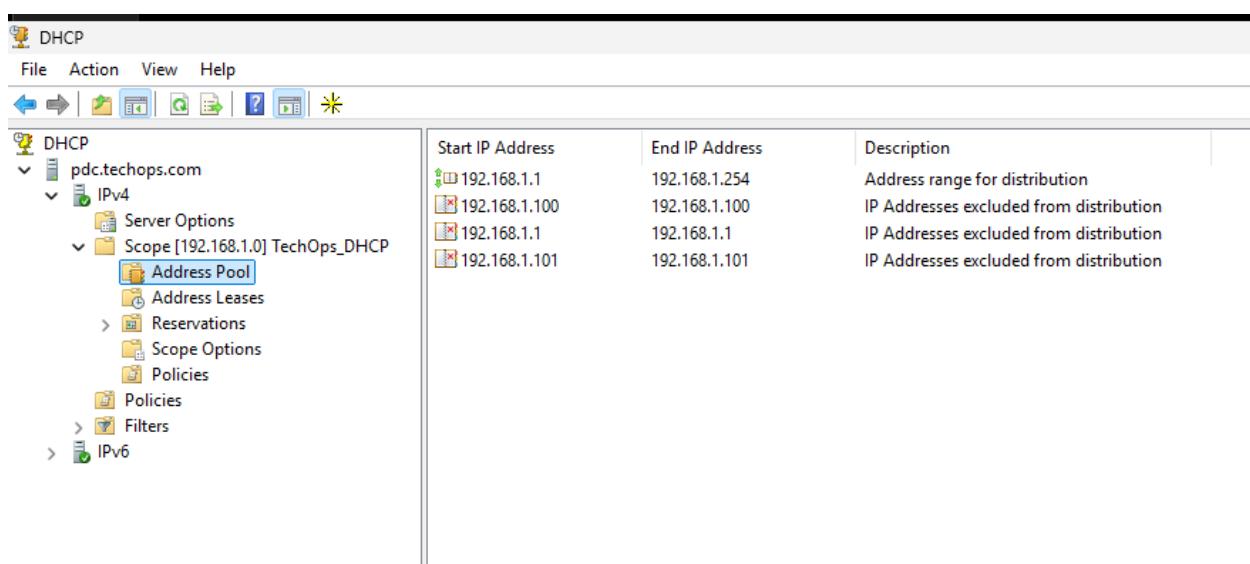
--



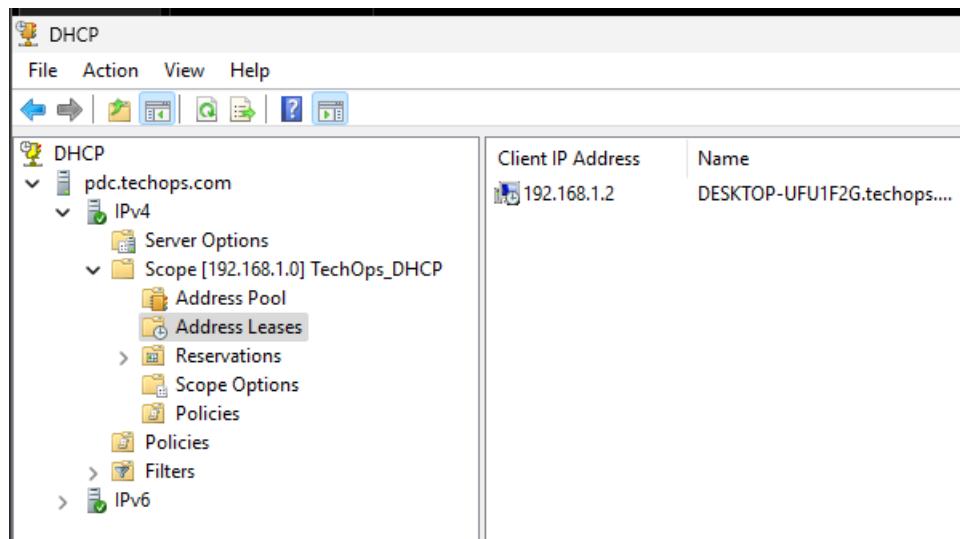
Finish



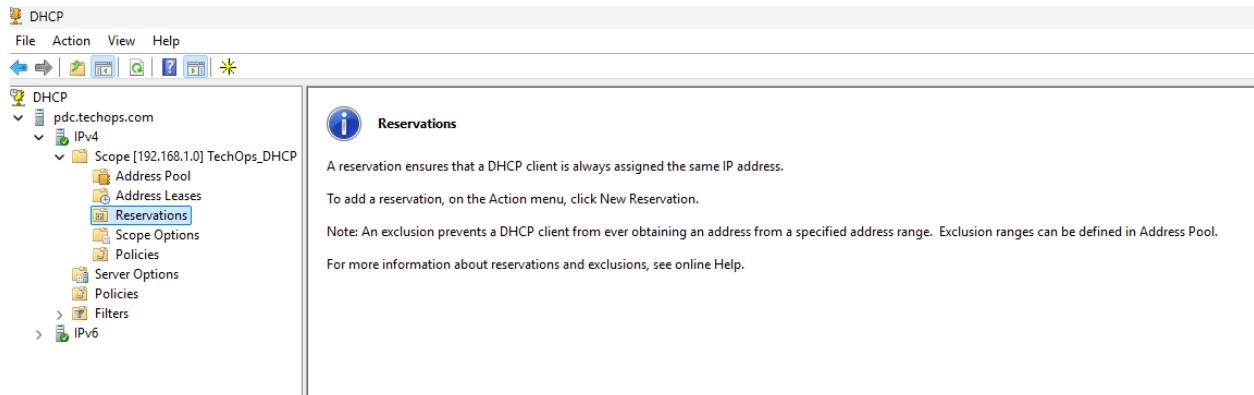
هلاقیها ظهرت عندي وبقت Active



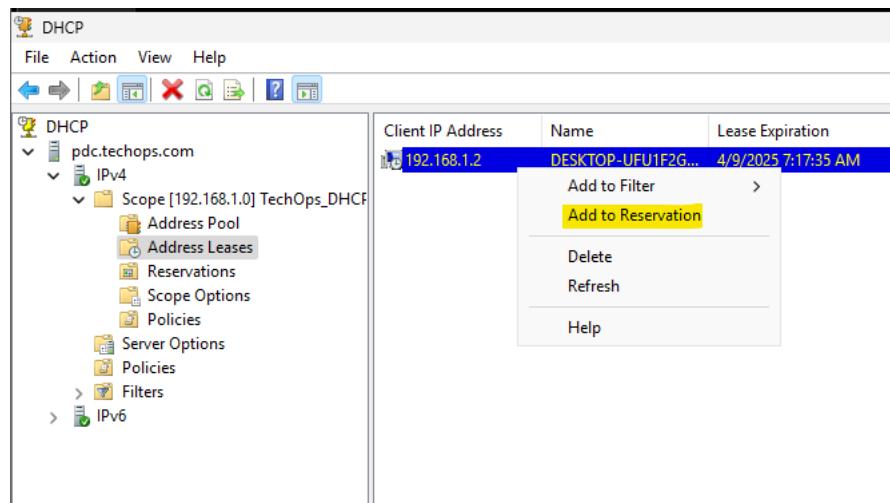
في ال Address Pool هتلaci ال Range ال هيتم توزيعه و هتلaci برضو ال ips ال معمولها
exclusions وتقدر تحذف من ال ip اي و تقدر تضيف ip يكون exclusions



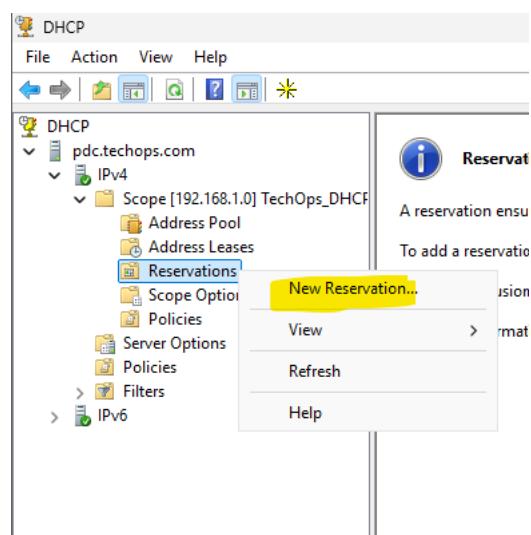
ال DHCP دى ال هيكون فيها ال clients ال سحبت ips من ال Address Leases



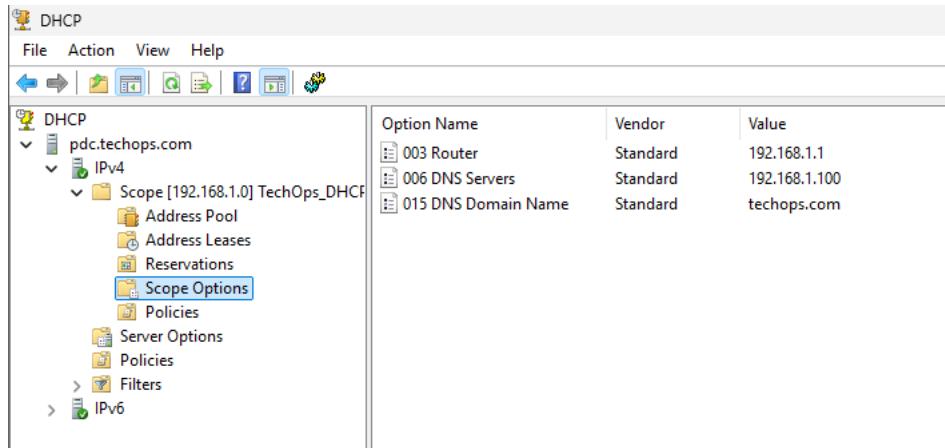
ال reservation ودا من خلله اقدر اربط IP معين ب MAC معين - بحيث ان كل ال Client ما يدخل يأخذ نفس ال IP المرتبط ب ال MAC بتاعه



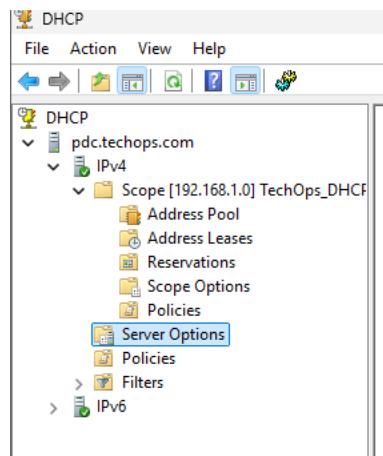
اقدر اروح على ال Client واعمل Add to Reservation



او اقدر اعمل New Reservation او واحدد ال IP وال MAC



ال Scope option دى ال عاوز اوزعها لل client زى ال DNS وال Gateway options

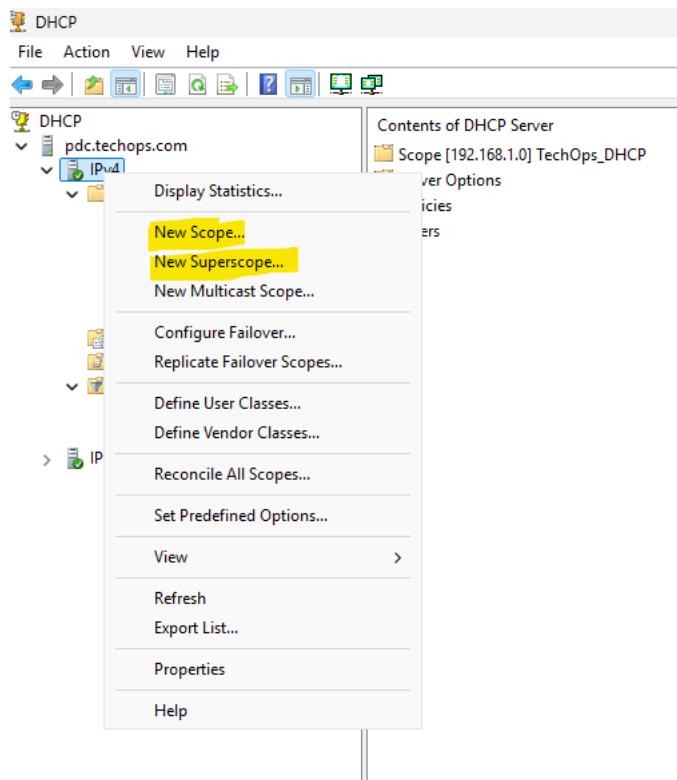


ال Server option : من خلالها لو عندي اكتر من scope وعاوز كل ال scopes ال عندي توزع معين ف بدل ما اعمله على كل scope واحده واحده ، ف انا بعمله مره واحده على ال server option

يبقى اي option موجود داخل ال server option هيطبق على اي scope عندي ؟

طيب في حالة التعارض بين ال scope option وال server option

ال scope option هي ال بتطبق ، السبب ؟ عشان ال scope option هي خاصه بال scope دى فقط هتعمل لـ override



لو روحت علي ال ipv4 هلاقي اني اقدر اعمل New scope

او new superscope ودي عباره عن اكتر من scope في مكان واحد ، ودي ممكن استخدمها لما يكون عندي اكتر من scope على نفس ال server ومن خلالها تقدر توزع على نفس ال network اكتر من subnet card

فممكن يكون عندي كارت شبكة فيه scope بتوزع

ips 192.168.1.50 – 192.168.1.200 وخلصت ال

وعاوز تضيف subnet مختلف وليكن

192.168.2.50 – 192.168.2.200

ف ال dhcp مش هيوزع من ال 2 subnet المختلفين غير لما يكونوا تحت superscope

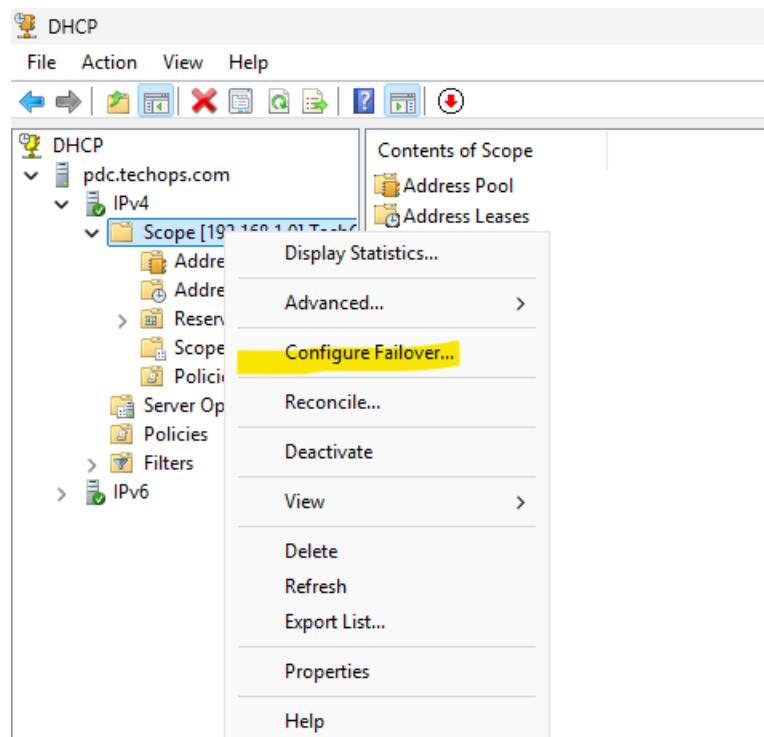
DHCP high availability

الفكره هنا ان بيكون عندي DHCP Server 2 بيوзуوا ال IPs ، وهنا لو فيه اي مشكله حصلت لاي
فيهم ال server الثاني هيفضل شغال وبالتالي ال service هتفضل شغاله ومش هيكون عندي
اي مشكله

و فيه عندي نوعين :

server : وهذا ال 2 server بيشتغلوا مع بعض بمعنى ان مثلا كل Load Balance mode -1
فيهم هيزع 50% من ال الموجوده عندي (active-active)
IPs : هنا الفكره بيكون server واحد فقط هو ال شغال ويوزع ال Hot Standby mode -2
باتاعتي كلها وال server الثاني بيكون standby له عشان لو حصله مشكله هو يبدا يشتغل فورا
(active-passive)

طيب ابدا استخدمه ازاي ؟



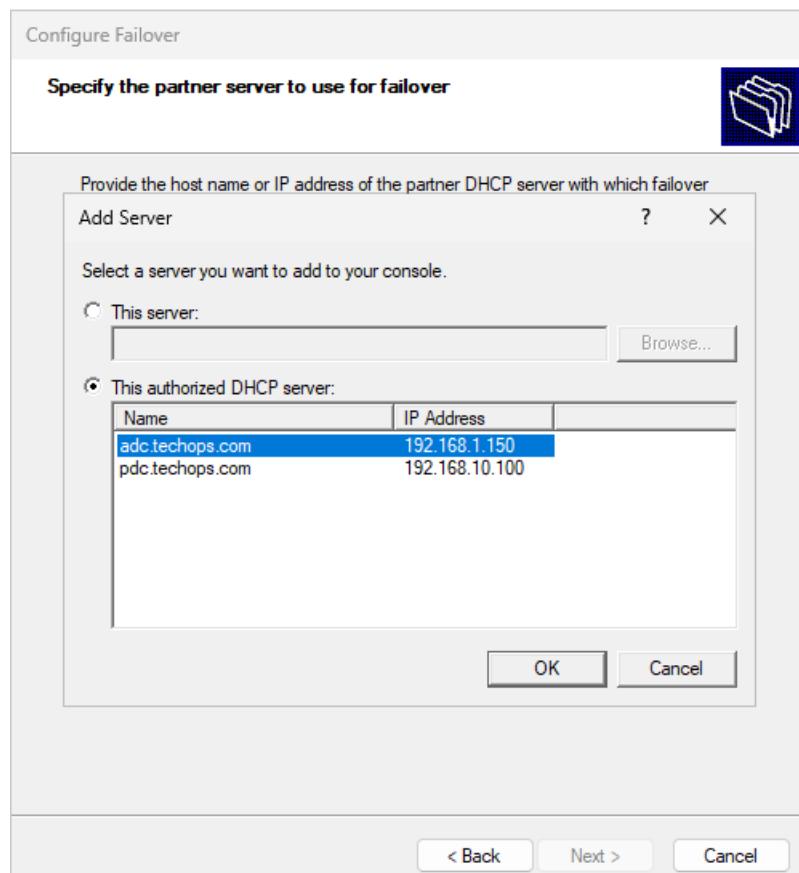
من ال DHCP بفتح IPv4 ومن ال scope ال عندي بختار Configure Failover

--



بتحدد ال Scope

--



بحدد ال sever الثاني ال هيكون معايا (ودا لازم يكون نازل عليه DHCP ومعمله authorize

--

Configure Failover

Specify the partner server to use for failover



Provide the host name or IP address of the partner DHCP server with which failover should be configured.

You can select from the list of servers with an existing failover configuration or you can browse and select from the list of authorized DHCP servers.

Alternatively, you can type the host name or IP address of the partner server.

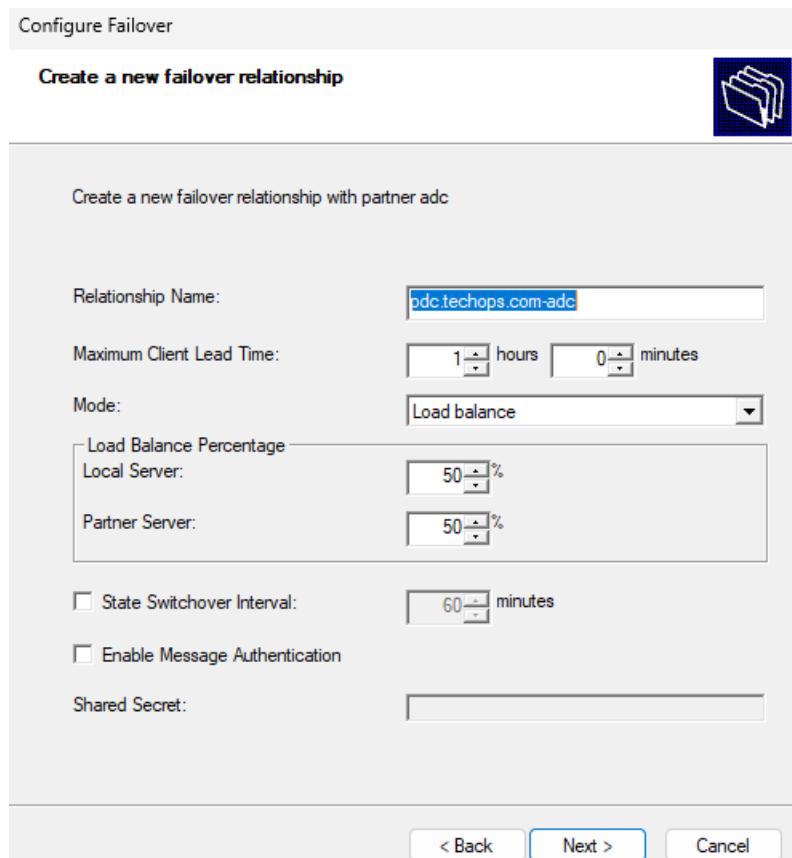
Partner Server:

Reuse existing failover relationships configured with this server (if any exist).

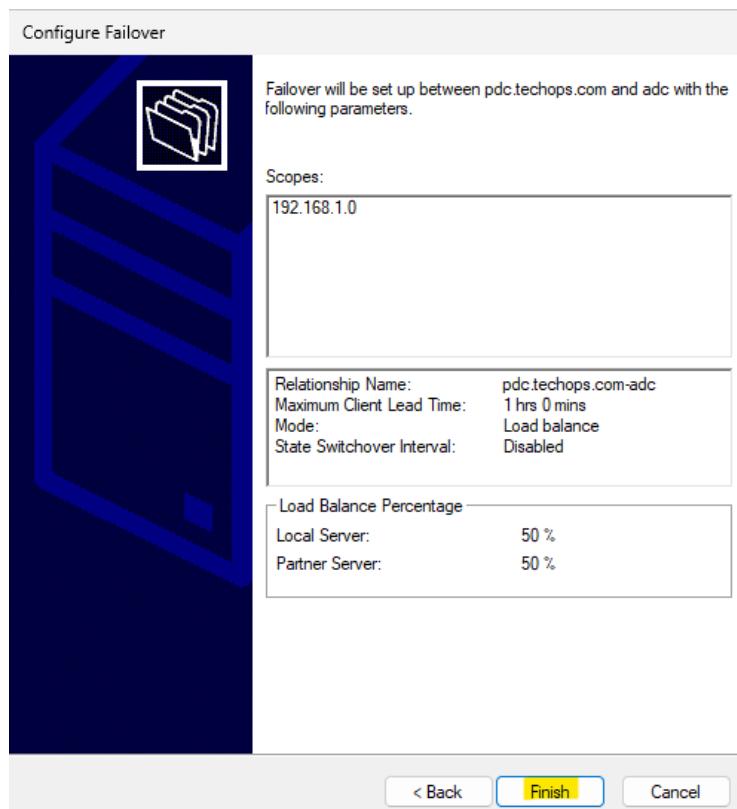
< Back Cancel

Next

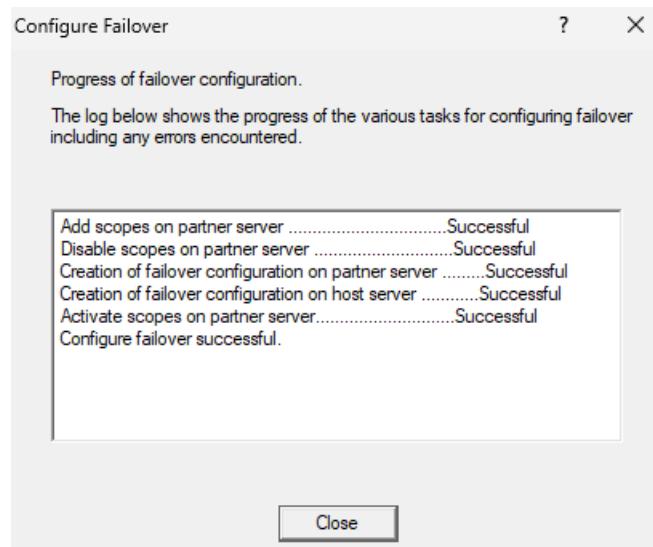
--



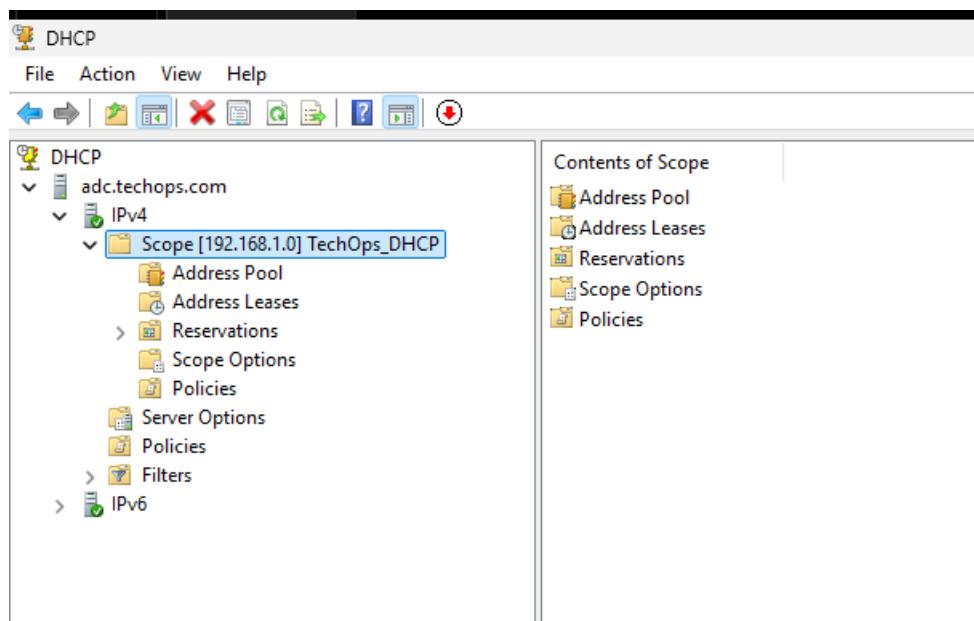
بعد كدا بيظهر ال relation ال هتكون مابينهم Relation name وبيكون اسم ال server الاول + اسم ال server الثاني (تقدر تعدله) : دي الفتره الي ال client يقدر يحتفظ بال IP(lease) فيها في حالهحصل توقف مؤقت في ال replication بين ال 2 server بعد كدا بتحدد ال Mode ولو هيكون LB في التوزيع بينهم هيكون ازاي ف هنا 50% لكل server بعد كدا فيه عندي ال State Switchover Interval ودي الفتره الي ال server الاساسي هيسنتماها قبل ما يفترض ان السيرفر الثاني Down دا هييفيدي ف اني لو فعلا السيرفر الثاني بقى down والسيرفر الاساسي فعل ال State Switchover Interval هياخذ هو ال full control وهو ال هيوزع ال IPs لوحده وكل دا هييفيدي انه ميحصلش IP Conflict



Finish



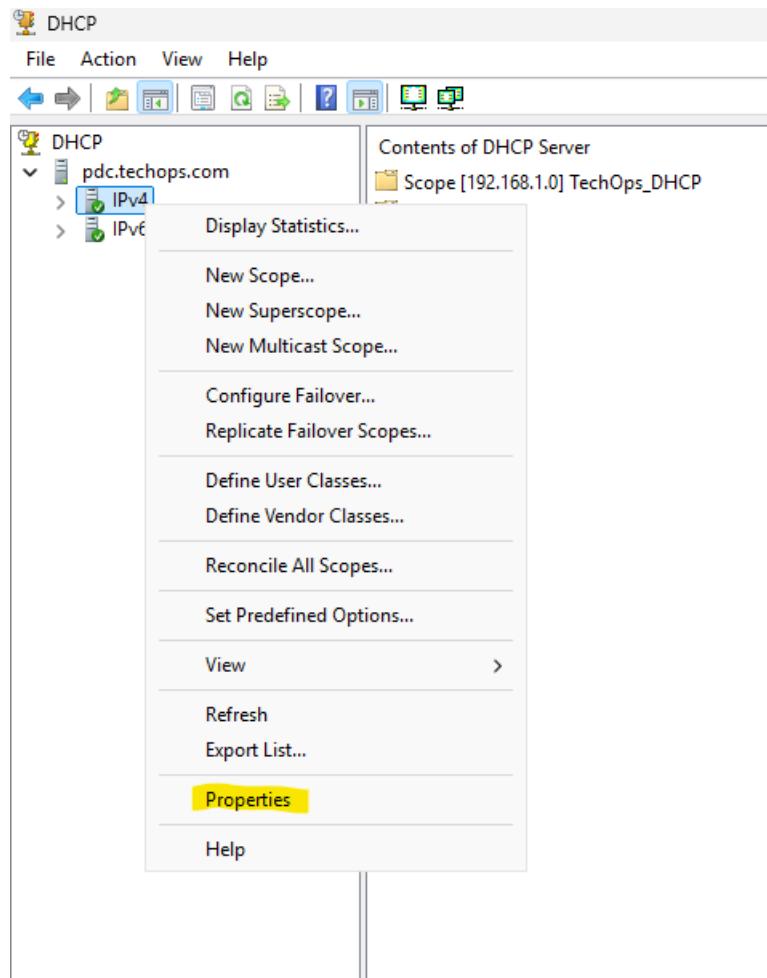
Successful All Tasks



لو فتحت ال DHCP على ال Server الثاني هلاقي ال Scope ظهرت

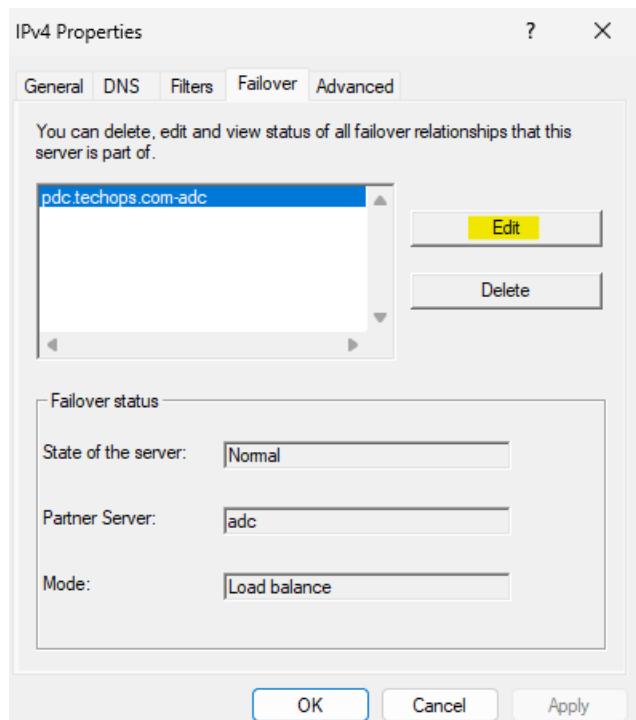
--
طيب لو محتاج اعمل edit على الكلام دا ؟

فتح ال DHCP على السيرفر الاول ال عملت عليه ال configuration



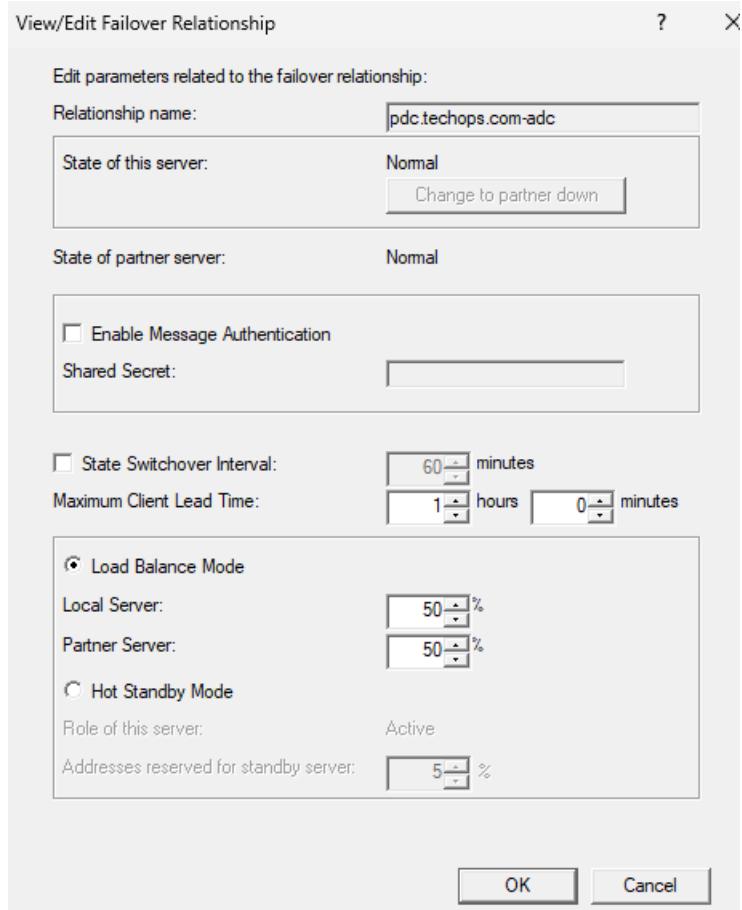
من IPv4 هفتح ال Properties

--



هختار ال edit واختار Relationship name

--

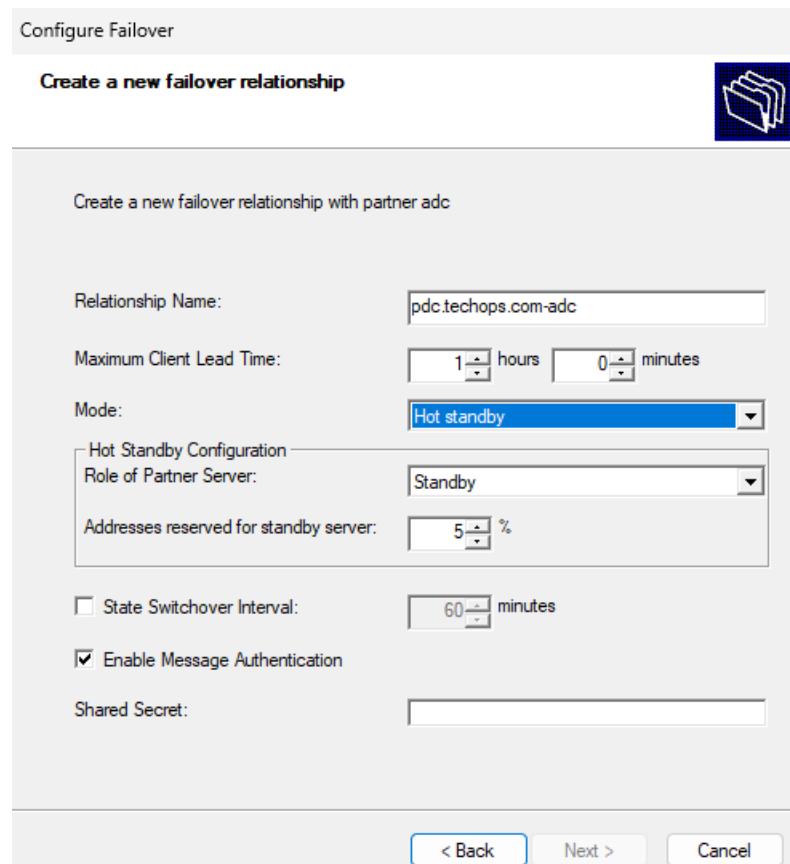


ومن ال page edit دا اكتر اعمل

--

طيب دلوقت شوفنا ال LB هنعمل ال Hot standby

نفس الخطوات



لكن في الخطوه دي بختار ال Mode يكون Hot standby يكون ال partner server هو ال active او ال standby وهذا اختيارته يكون ال standby وفي ال standby عرفنا انه مش هشتعل غير لما السيرفر الاول يحصله مشكله لكن اقدر احدد لل standby انه مثلا بقدر بوزع 5% فقط او اقللها او العينيها خالص

DNS

هو اختصار ل port 53 TCP/UDP شغال على Domain Name Server/system/service

هو نظام أو خدمة تقوم بترجمة Domains Names (مثل www.example.com) إلى عناوين IP (مثل 192.168.1.10)

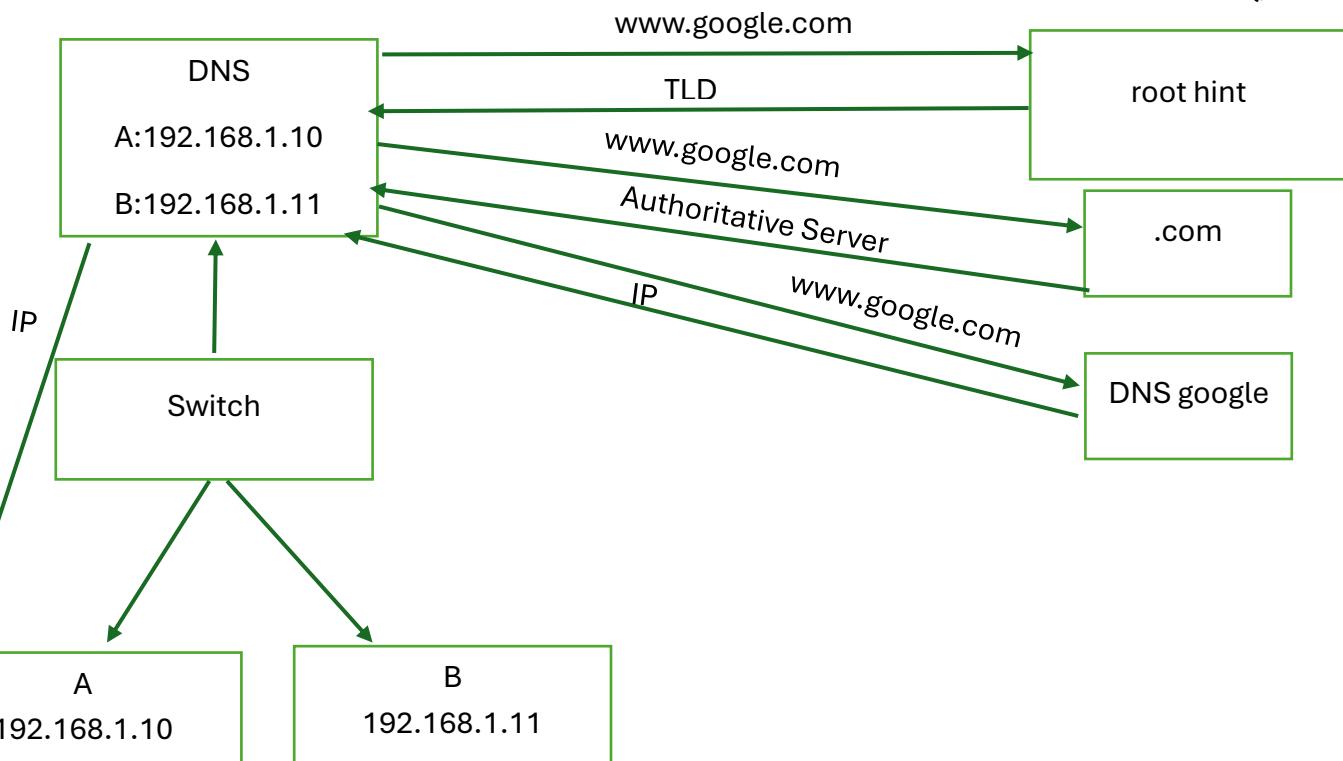
الفكرة من ذلك هي أنك لا تحتاج لحفظ عناوين IP طويلة ومعقدة للوصول إلى الموقع أو الخدمات على الإنترنت. بدلاً من ذلك، يمكنك استخدام اسم النطاق (مثل www.example.com) وخدمة DNS هي التي تقوم بترجمته إلى عنوان IP الصحيح

DNS يعمل بشكل مشابه تماماً لدليل الهاتف الذي يحتوي على أسماء الأشخاص وأرقام هواتفهم. عندما تبحث عن اسم شخص (أو ال Domain) يمكنك العثور على رقم هاتفه (أو عنوان ال IP) دون الحاجة لحفظ الرقم بنفسك

وبالتالي ال DNS يعتبر Service Locator لأنها بقدرة يحدد مكان ال Service بناءاً على ال IP بتاعه وبالتالي لما تروح تطلب [Domain name](http://www.example.com) فهو هيحدد ال IP

وبالتالي هيقوم بتوجيهك لل service المطلوبه

طيب اي ال بيحصل بالظبط ؟



هنا مثلاً لما جهاز A هيطلب google.com ال بيحصل التالي :

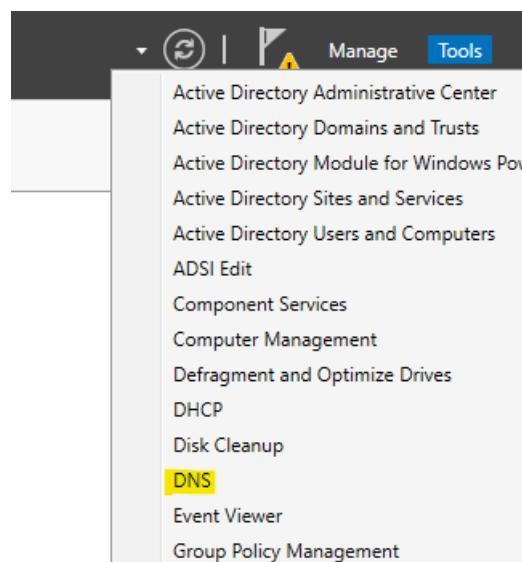
- 1 A بيعت لـ DNS Server في ال local network مثلًا
- 2 ال local DNS بيدور في الكاش ----> مفيش؟
- 3 يروح لـ root hint
- 4 ال root hint هيرد يقوله انه ميعرفش google.com لكن يعرف مين المسئول عنه وهذا بنسميه ال TLD اختصاراً لـ Top Level Domain زي (.com-.net-.org) ف ال root hint عدده معلوم عن كل ال Top level domain ف هيرد على DNS ويقوله ان ال .com هي المسئول عن ال google.com
- 5 google.com يروح لـ DNS Server ويسأله عن .com
- 6 .com يرد عليه ويقوله انه يروح لـ Authoritative Server الخاص بـ google.com
- 7 ال Authoritative Server يروح لـ DNS ويجيب منه ال IP النهائي
- 8 ال DNS بيعت ال IP لـ Client ال طلبه

وال server هو ال Authoritative Server عنده المعلومة النهائية عن ال domain name ، بتدور عليه ،

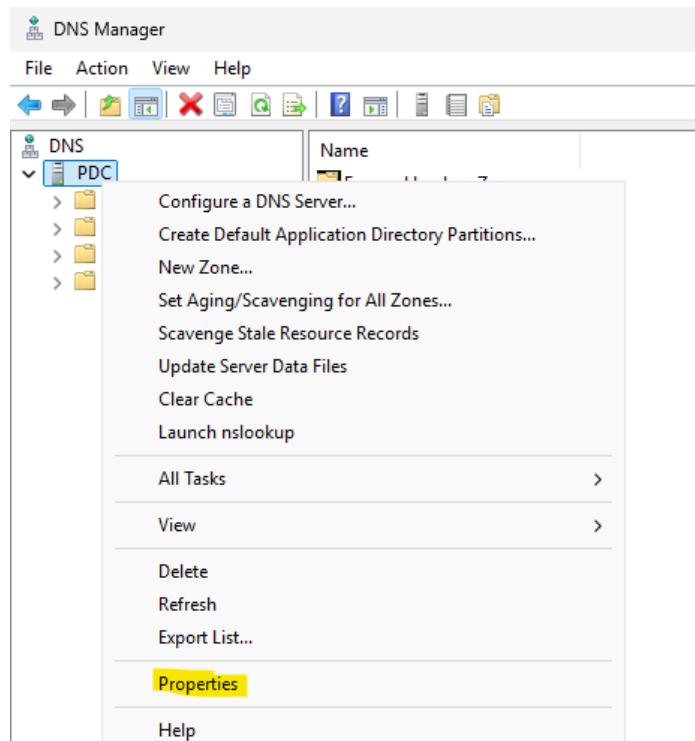
لما تسأل هو google.com ال ip بتاعه كام ؟

ال Authoritative Server هو ال هيرد يقولك انا المسئول عنه واتفضل ادي ال IP بتاعه كذا

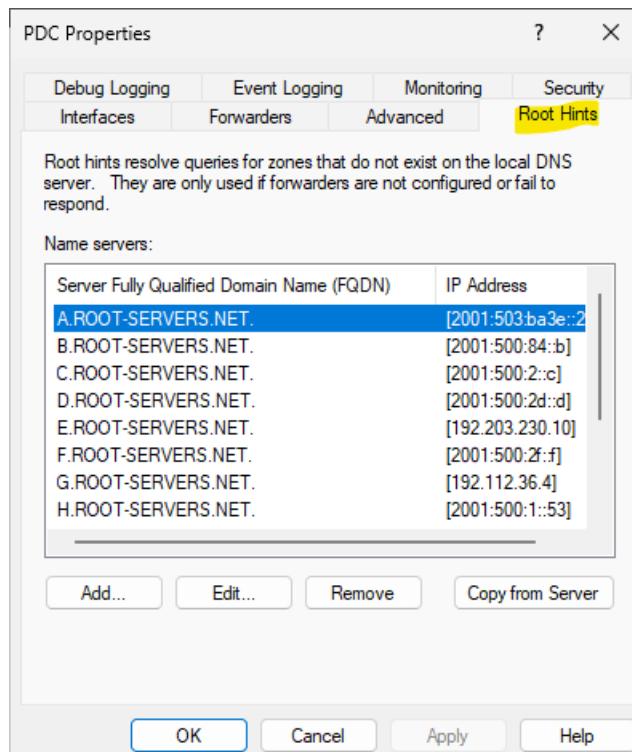
ازاي اشوف ال root hint ؟



من Tools هفت ح ال DNS



Click على ال domain name واختار properties

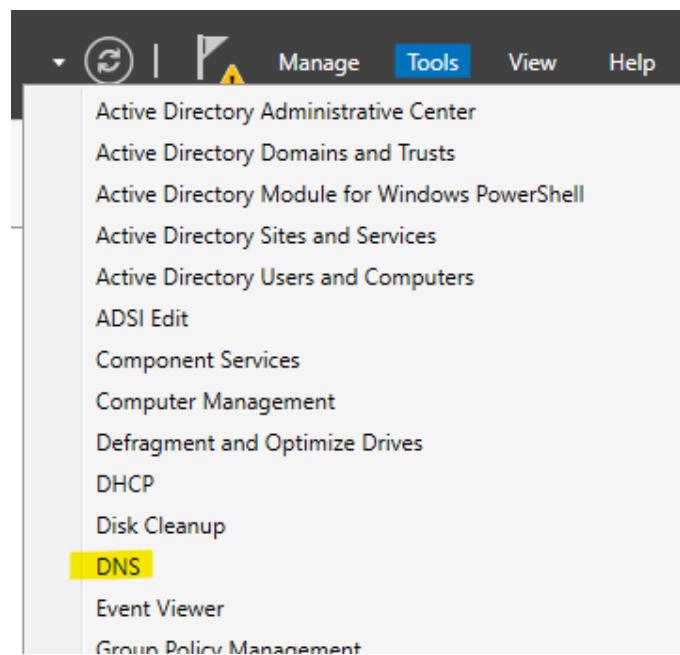


هلاقي عندي tab خاصه بال root hints

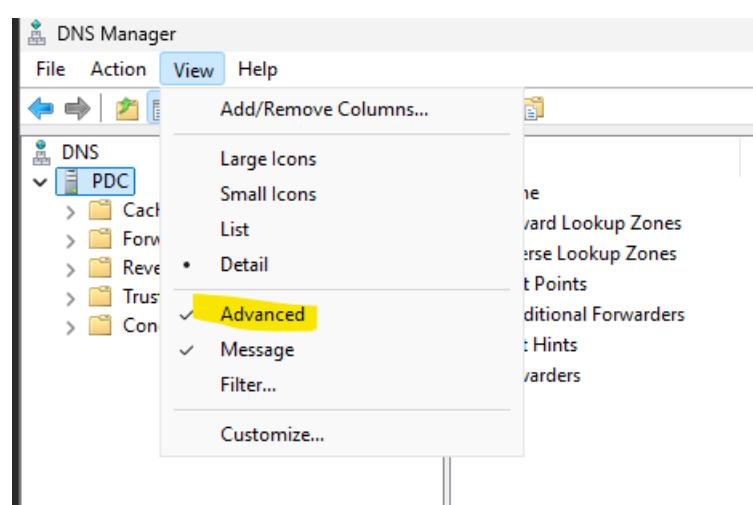
--

وال root hint هما عباره عن 13 super computers واسماءهم من ال A:M: وهو المسؤولين عن ال DNS على مستوى العالم

بitem تخزين المعلومات دي في الكاش عند client وعند ال DNS Server عشان اشوفها على ال DNS Server



من tools هتفتح ال DNS



من advanced view هنفع ال

DNS Manager

File Action View Help

Cached Lookups

Name	Type	Data	Timestamp
azure			
azure-dns			
bing			
google			
googleapis			
googleusercontent			
gstatic			
microsoft			
msftstatic			
msn			
(same as parent folder)	Name Server (NS)	e.gtld-servers.net.	static
(same as parent folder)	Name Server (NS)	b.gtld-servers.net.	static
(same as parent folder)	Name Server (NS)	a.gtld-servers.net.	static
(same as parent folder)	Name Server (NS)	d.gtld-servers.net.	static
(same as parent folder)	Name Server (NS)	i.gtld-servers.net.	static
(same as parent folder)	Name Server (NS)	f.gtld-servers.net.	static
(same as parent folder)	Name Server (NS)	j.gtld-servers.net.	static
(same as parent folder)	Name Server (NS)	k.gtld-servers.net.	static
(same as parent folder)	Name Server (NS)	c.gtld-servers.net.	static
(same as parent folder)	Name Server (NS)	g.gtld-servers.net.	static
(same as parent folder)	Name Server (NS)	h.gtld-servers.net.	static
(same as parent folder)	Name Server (NS)	l.gtld-servers.net.	static
(same as parent folder)	Delegation Signer (DS)	[19718][SHA-256][ECDSAP...]	static
(same as parent folder)	RR Signature (RRSIG)	[DS][Inception(UTC): 4/14...	static

في ال DNS هنلاقي ال cached lookups (بيتم تخزين المعلومه دي لمده يوم)

Cached Lookups

clients6			
l			
(same as parent folder)	Name Server (NS)	ns2.google.com.	static
(same as parent folder)	Name Server (NS)	ns1.google.com.	static
(same as parent folder)	Name Server (NS)	ns3.google.com.	static
(same as parent folder)	Host (A)	142.250.203.238	static
ns1	Host (A)	216.239.32.10	static
ns1	IPv6 Host (AAAA)	2001:4860:4802:0032:0000::...	static
ns2	Host (A)	216.239.34.10	static
ns2	IPv6 Host (AAAA)	2001:4860:4802:0034:0000::...	static
ns3	Host (A)	216.239.36.10	static
ns3	IPv6 Host (AAAA)	2001:4860:4802:0036:0000::...	static
ns4	A)	216.239.38.10	static
ns4	Host (AAAA)	2001:4860:4802:0038:0000::...	static
ogs	CNAME)	www.3.l.google.com.	static
play	A)	142.250.200.206	static
www	Host (A)	216.58.212.100	static

وهنا اقدر اعمل لحاجه معينه record

طیب علی ال client عاوز اشوف ال cached ؟

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

Windows IP Configuration

aefd.nelreports.net
-----
Record Name . . . . . : aefd.nelreports.net
Record Type . . . . . : 5
Time To Live . . . . . : 881
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record . . . . . : aefd.nelreports.net.akamaized.net

Record Name . . . . . : aefd.nelreports.net.akamaized.net
Record Type . . . . . : 5
Time To Live . . . . . : 881
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record . . . . . : a1851.dscg2.akamai.net

Record Name . . . . . : a1851.dscg2.akamai.net
Record Type . . . . . : 1
Time To Live . . . . . : 881
Data Length . . . . . : 4
Section . . . . . . . : Answer
```

هتفتح ال CMD وهنكتب ال command دا : ipconfig /displaydns

(بیتم تخزين المعلومه دي تقریبا لمده 20 دقیقه)

--

```
C:\Users\Administrator>ipconfig /flushdns  
Windows IP Configuration  
Successfully flushed the DNS Resolver Cache.  
C:\Users\Administrator>ipconfig /displaydns  
Windows IP Configuration  
  
C:\Users\Administrator>
```

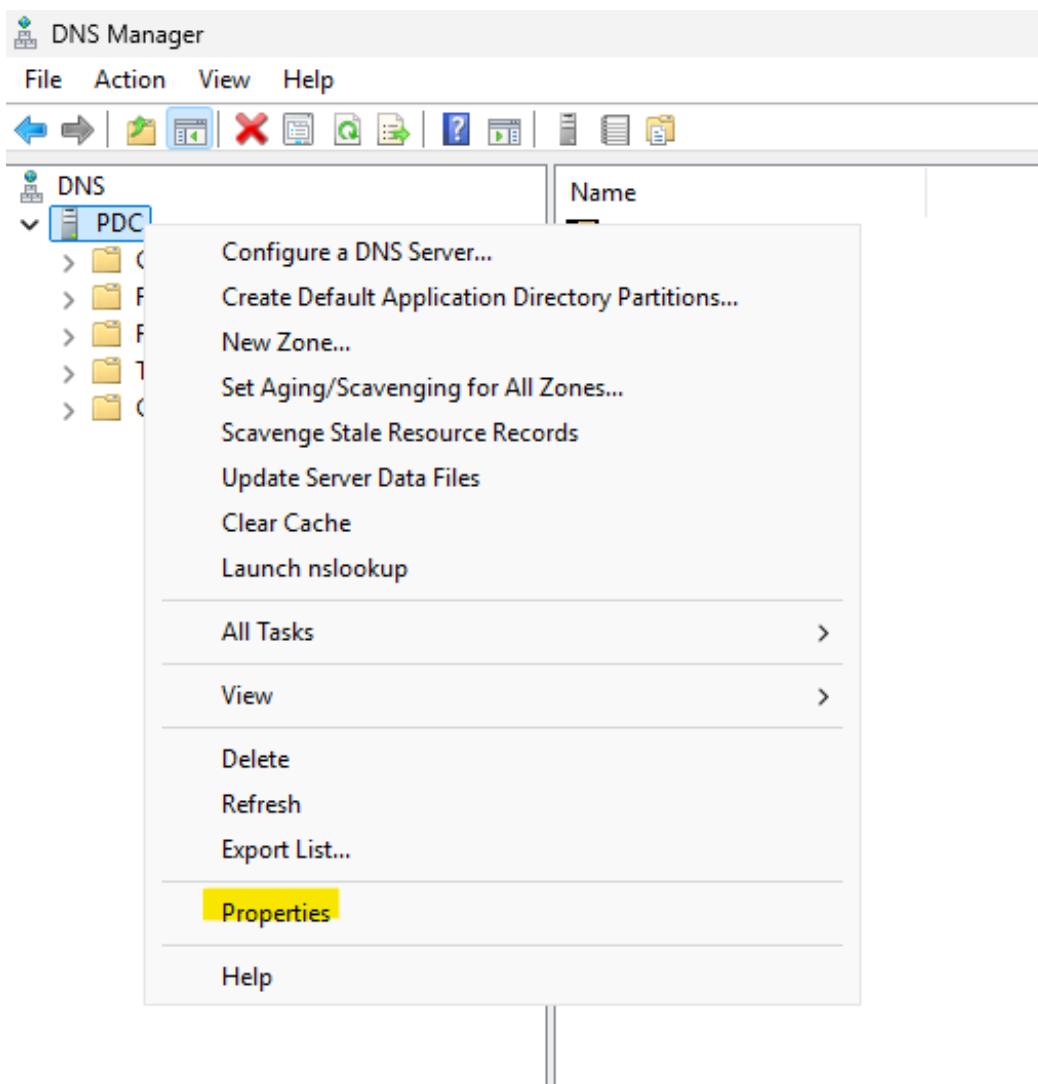
لو هتمسح ال Cache هتكتب ipconfig /flushdns لكن هنا بيمسح كل ال Cache مقدرش احذف معين ، وال record بيتم مسحه بعد انتهاء فتره ال TTL (Time To Live) ودي الفتره الي يقدر فيها ال DNS Server يحفظ بمعلومه ال record داخل ال Cache قبل ما يحذفها من عنده او يعتبرها منتهيه الصلاحيه ويطلبها من جديد

مثلا لما تسلله عن google.com يقول ال ip 192.168.1.60 والمعلومه دي صالحه لمده 300 ثانية بعدها ابقي اسالني تاني ف هها قيمه ال 300 دي اسمها TTL

بدل كل دا وبدل ما اني اخلي ال DNS Server بتاعي يروح يكلم ال root hints مباشر
لا ممكن اعمل حاجه اسمها DNS Forwarding

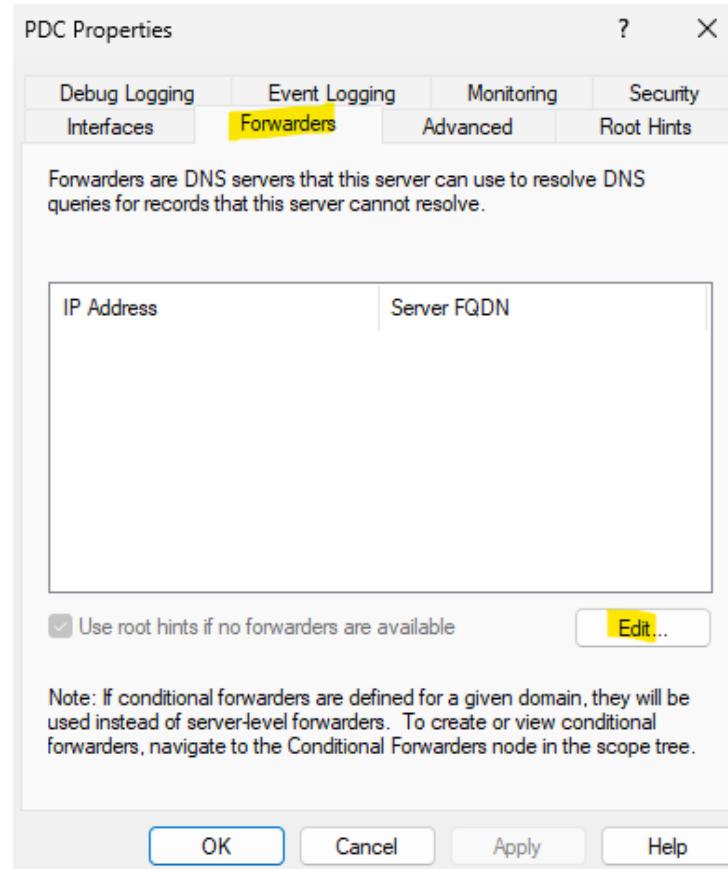
ودا كانبي يقول ال DNS Server لو مش عارف معلومه ال www.google.com روح ل DNS تاني (لو متعرفش المعلومه دي اسأل صاحبك يعلم وصاحبك دا بقا هو ال DNS Server manual) ودا احنا بنعمله او نضيفه Forwarding

طيب ازاي اعمله ؟

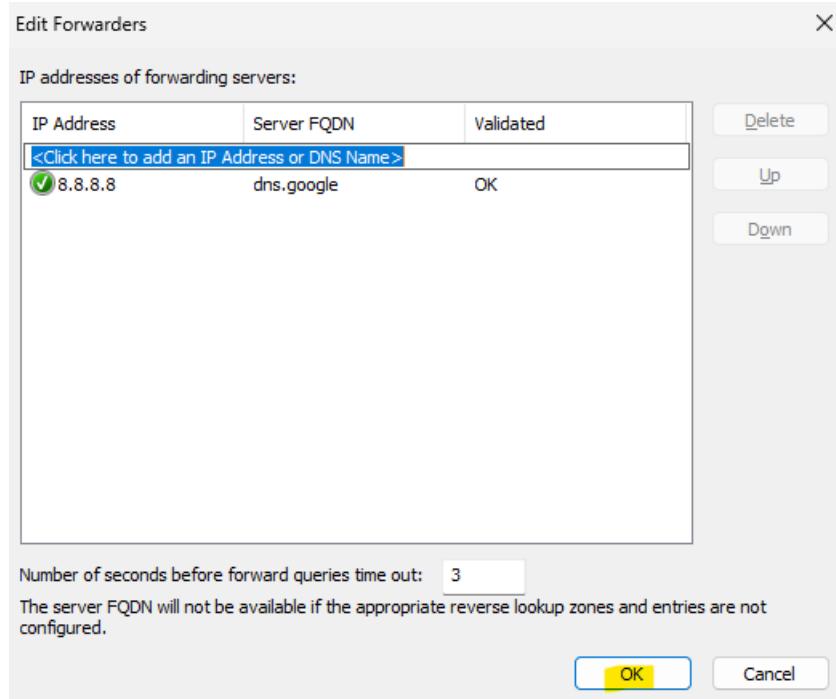


Click domain name ونختار properties على ال

--



هناقي ال Tab اسمها forwards وندخل على edit



ونضيف ال DNS Server و ok

--

لو جهاز A طلب A من ال DNS Server هو ال رد عليه بالمعلومه
يبقى ال DNS Server اسمه authoritative لو ال DNS Server راح سال ال DNS
non-authoritative او ال root hint يبقى في الحاله دي ال Forwarding
وال Authoritative دي معناها هو ال server ال بيملك المعلومه الاصليه عن domain معين
والمعلومه بتكون عنده في ال zone files بقى

دي معناها ان ال server جاب معلومه ال domain من server تاني زي ال Non-Authoritative Cache او ال Forwarding او حتى ال كانت متخزن في ال root hints

طيب ازاي اعرف انه رده Authoritative او Non-Authoritative
في عندي command tool او nslookup اسمه

```

C:\Users\Administrator>nslookup
Default Server: Unknown
Address: 192.168.223.2

> google.com
Server: Unknown
Address: 192.168.223.2

Non-authoritative answer:
Name: google.com
Addresses: 2a00:1450:4006:810::200e
           172.217.19.46

```

في ال CMD هكتب nslookup هيقولي ال DNS Server بتاعي
 لما اطلب google.com قالني انه هيرد عليا رد Non-Authoritative لأن المعلومه بتاع
 جالها من مكان تاني google.com

لما جهاز A بيعت لـ DNS server يساله على google.com بنسميه query
 وعندنا نوعين من ال Query

Recursive Query -1 : هنا client بيطلب من ال DNS Server المعلومه الخاصه بـ google.com وميرجعش غير بالمعلومه دي يعني تتصرف وتتجبهالي حتى لو مش عنده المعلومه دي يروح يسال ال root hint وهكذا لحد ما يرجعي بالمعلومه دي (يعني من الآخر هنقولي المعلومه يعني هنقولها)

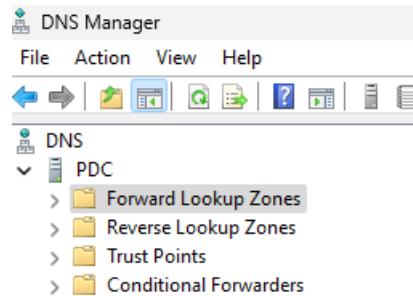
Iterative Query -2 : هنا ال DNS Server بيطلب من DNS Servers تانيه يدلوه على الطريق ، يعني ان ال DNS Server نفسه يروح يسال DNS Sever تاني هل انت تعرف معلومه google.com وهكذا لحد ما يصل للاجابه (بitem بين ال DNS Servers مش ال Client)

Non-Recursive Query -3 : لما يكون ال DNS Server عنده المعلومه اصلا سواء متخزن في ال cache او يكون هو المسؤول عن ال domain دا وبتاعلي هيكون عنده ال zone بتاعته فهيرد فورا برضو من غير ما يسال حد وبالتالي دا بيكون اسرعهم في الرد

لو ال Client طلب المعلومه من ال DNS Server وهو ال رد عليه مباشره بيقى كدا شغالين UDP لو ال DNS Servers سال DNS Sever تانيه بيقى كدا شغالين TCP

لو من Tools فتحنا ال DNS ه يكون بالشكل دا

طيب يعني اي كلمه zone ؟



دي معانها المكان الي بيتخزن فيه المعلومات الخاصه بال domain داخل ال DNS Sever وعنه ال files بتاعته وهو المسئوال عنها

طيب فيه نوعين عندنا ال Reverse lookup zones وال Forward lookup zones

دي معناها ان ال client هيجي بال name وعاوز ال IP

دارا ال client هيجيلي بال IP وعاوز name Reverse lookup zones

--

DNS Manager

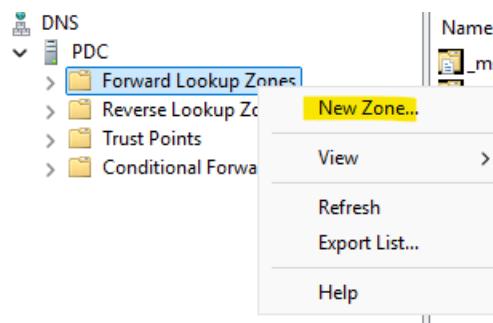
Name	Type	Data	Timestamp
_msdc			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
it			
(same as parent folder)	Start of Authority (SOA)	[535], pdc.techops.com, ...	static
(same as parent folder)	Name Server (NS)	adc.techops.com.	static
(same as parent folder)	Name Server (NS)	pdc.techops.com.	static
(same as parent folder)	Host (A)	192.168.223.131	4/14/2025 5:00:00 AM
(same as parent folder)	Host (A)	192.168.1.100	4/14/2025 12:00:00 AM
(same as parent folder)	Host (A)	192.168.1.150	4/10/2025 5:00:00 AM
(same as parent folder)	Host (A)	192.168.1.18	4/13/2025 9:00:00 AM
(same as parent folder)	Host (A)	192.168.223.128	3/20/2025 8:00:00 AM
(same as parent folder)	Host (A)	192.168.10.150	3/20/2025 7:00:00 AM
ADC	Host (A)	192.168.1.150	static
DESKTOP-UFU1F2G	Host (A)	192.168.1.2	4/1/2025 7:00:00 AM
pdc	Host (A)	192.168.1.100	static

تحت ال Forward lookup zones هلاقي ال domain name دا يكون فيه 2 record بيكونوا او لما بعمل ال DNS by default

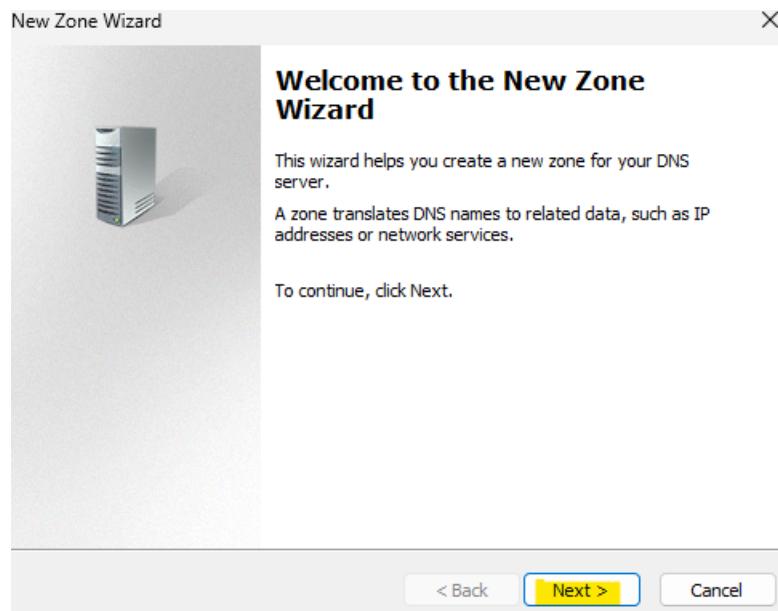
Start of Authority -1

Name Server -2

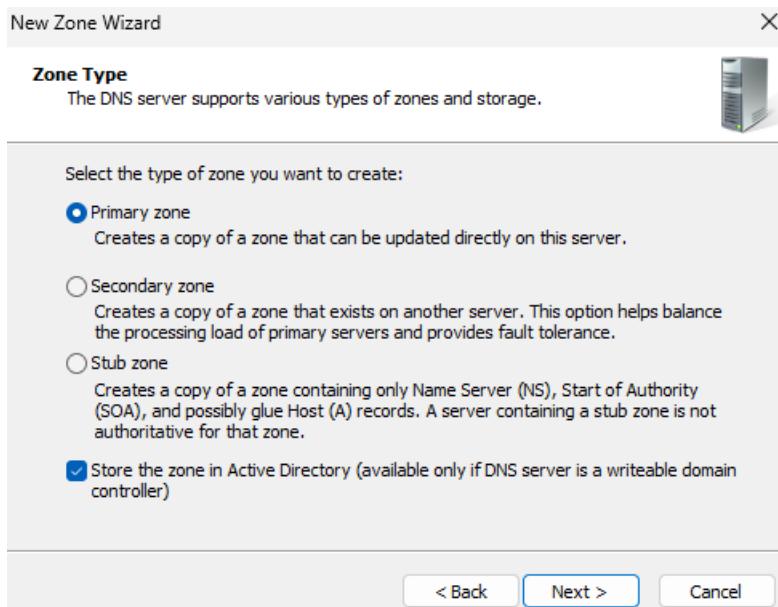
طيب لو عاوز اعمل New Zone



Click على ال new zone وختار Forward lookup zones



Next



--

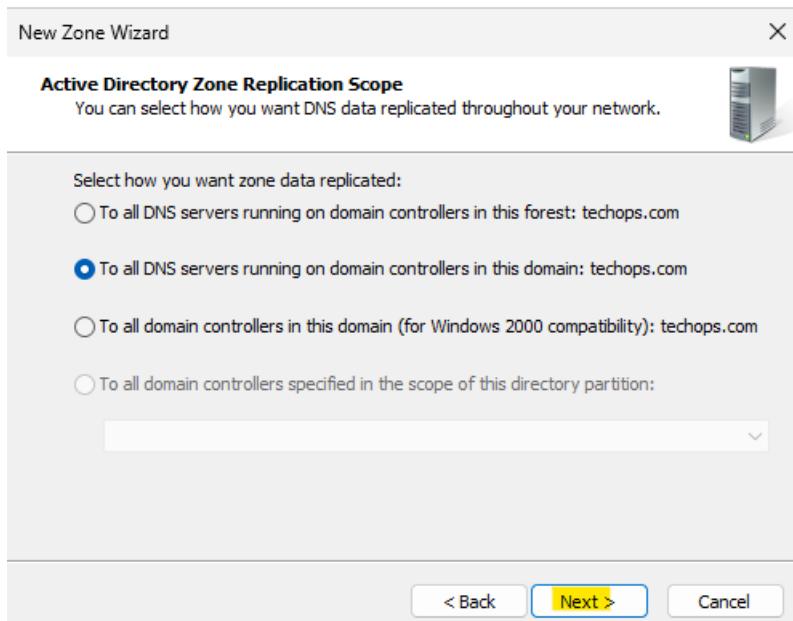
فيه عندي 3 انواع من ال Zones

Primary Zone -1 : هي الـ Zone الرئيسية اللي فيها البيانات الأصلية، و بتتعذر منها و السيرفر اللي عنده الـ Primary هو اللي بيملك الحق في التعديل

هي نسخه Primary من ال Read only بتعمل علشان Secondary Zone -2 أو (load balancing) تلقائياً عن طريق (redundancy)

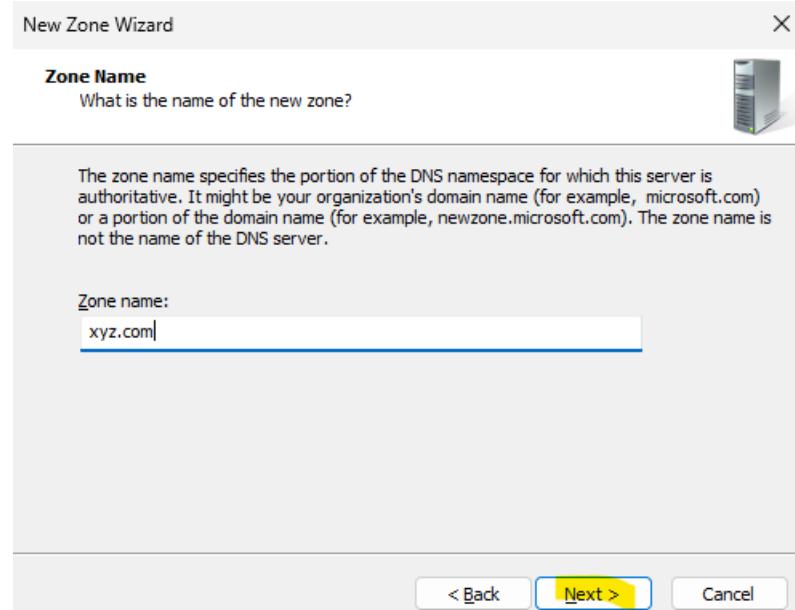
عملية اسمها Zone Transfer

نسخه مبسطه او خفيفه من ال zone و مش بتحتوي على كل البيانات، بس يحتوي على المعلومات الكافية علشان توصل للسيرفر الأساسي ال هو ال Authoritative VPN و مفيدة في بيئات فيها شبكات متفرعة او متصلة بعض عن طريق name server

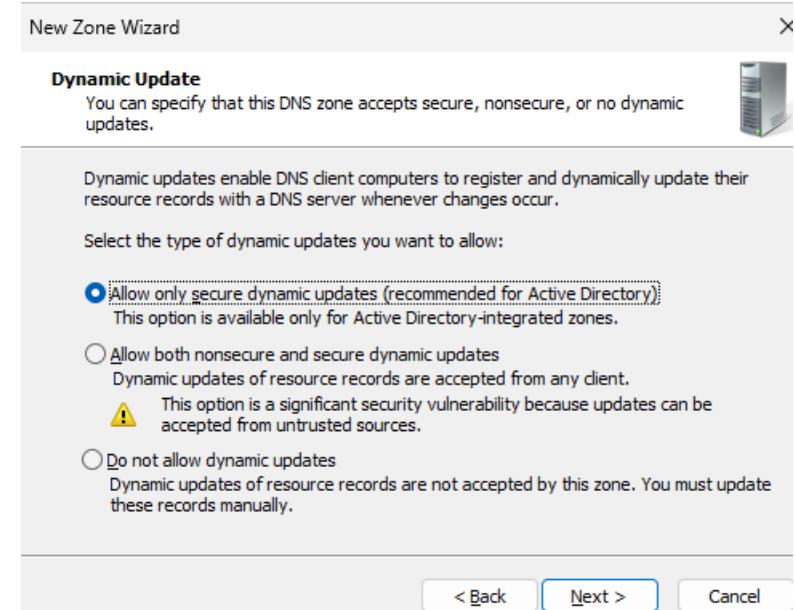


هذا بيسالني عن ال replication هيكون على مستوى ال forest ولا ال domain

--

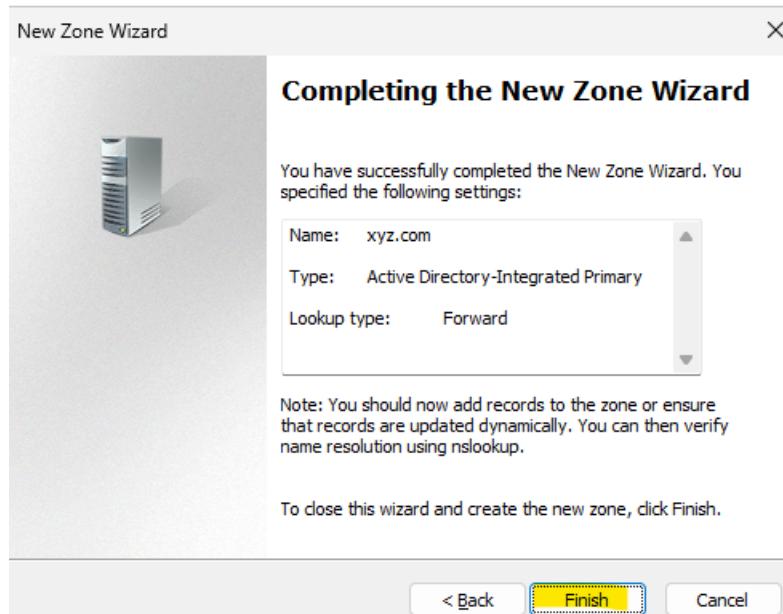


ال zone name



هنا يقول ان ال تبع ال Active Directory : فقط ال Allow only secure dynamic updates يقدر يعمل update في ال DNS

هنا الي تبع ال AD او ال HTI workgroup : Allow both
 مش هسمح لحد يعمل update وهذا ال administrator فقط ال هيدخل يعمل ال
 Do not allow manually بطريقه record



Finish

Name	Type	Status	DNSSEC Status	Key Master
_msdcs.techops.com	Active Directory-Integrated Pr...	Running	Not Signed	
techops.com	Active Directory-Integrated Pr...	Running	Not Signed	
xyz.com	Active Directory-Integrated Pr...	Running	Not Signed	

بقت موجوده عندي

طيب از اي ابدا اعمل Record ل create تحت ال zone دي ؟

في عندي اكتر من نوع record :

A Record -1 : اختصار ال Address Record : دا اشهر واهم نوع ودا وظيفته انه بيربط ال IP من نوع IPv4 ، يعني لما تكتب A record ال goole.com بقولك ال IP بتاعه 192.168.1.110 مثلا

AAAA Record -2 : نفس فكره ال A Record لكن خاص ب IPv6

MX Record -3 : Mail Exchange ودا خاص بالايميلات دا ال بيحدد لما تيجي تبعث ميل لحد معينه بيعته على الايميل الصح ، لو عندك mail.techops.com والايديات بتجيلك على MX Record ه يقول ان لو اي حد عاوز يبعث اي ميل علي @techops.com بيعته على ال mail.techops.com server

CNAME Record -4 او اختصار ال Canonical Name : دا alias name يعني لو عندي اسمه domain name techops-solution.com وآخره Alias ts.com يشاور علي techops-solution.com

او مثلا shop.techops.com يشاور علي www.techops.com وهكذا

NS Record او اختصار ال Name Server : ده اللي بيحدد مين السيرفر المسؤول عن ال domain ده يعني لما حد يسال من المسئول عن NS Record ال techops.com يرد ويقول ان ال DNS Server كذا هو المسئول عنه (يعني هو ال بيحدد ال domain لل Authoritative DNS Server)

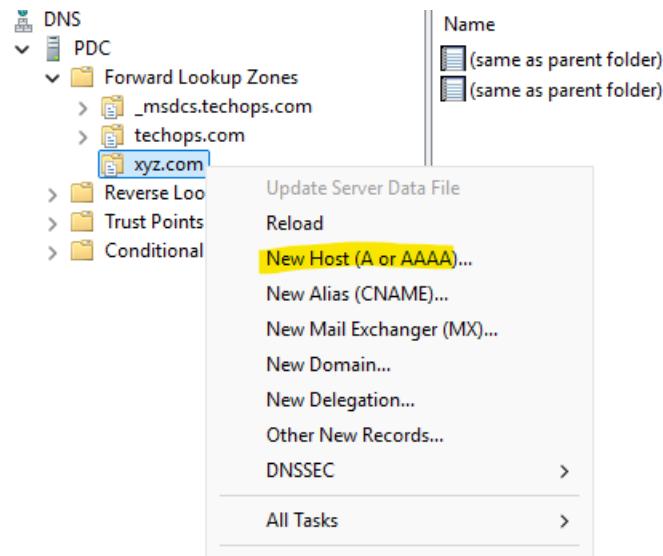
SOA Record او اختصار ال Start of Authority : ده أول Record بيتحط في ال Zone ودا ال يقول مين المسئول عن ال zone دي ، امتى اتعدلت ال zone ، وازاي تعامل مع ال Zone Transfer

PTR Record او A Record Pointer : ده عكس ال A Record يعني دا بتلله IP ويرجعلك ال name بتاعه ودا الموجود في ال Reverse Lookup

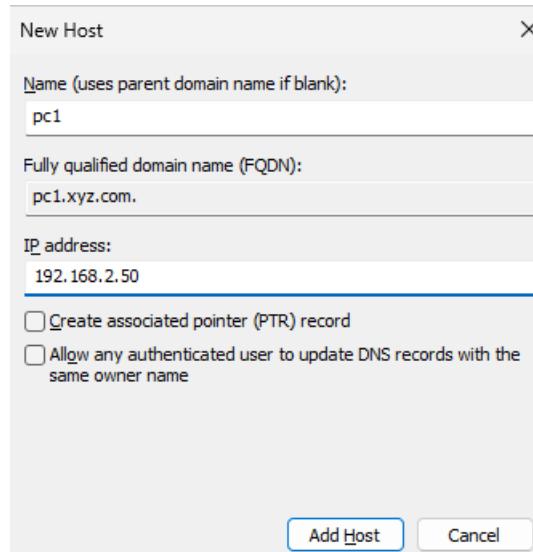
TXT Record : بيستخدم في التحقق من ملكيه ال Domain

SRV Record او اختصار ال Service location : دا بيقولك ان ال service المعينه دي شغاله على ال port دا بال server

TTL ودا ال هو ال Time to live : مش record في حد ذاته لكنه موجود مع كل record ودي الفتره الي هيتم حفظ المعلومه فيها في ال cache يعني لو ال TTL بيساوي 300 ثانية يعني ال DNS هيحتفظ بال record دا لمده 5 دقائق (ال هما ال 300 ثانية) وبعدها لو حد طلب منه تاني يسال تاني عن ال record دا



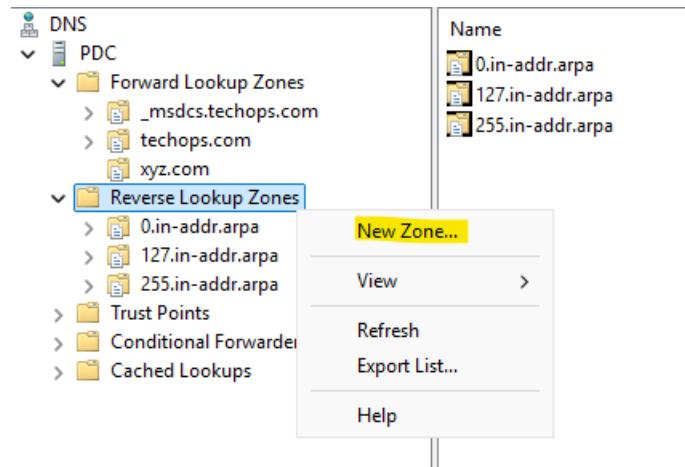
New Host على ال zone واختار Click



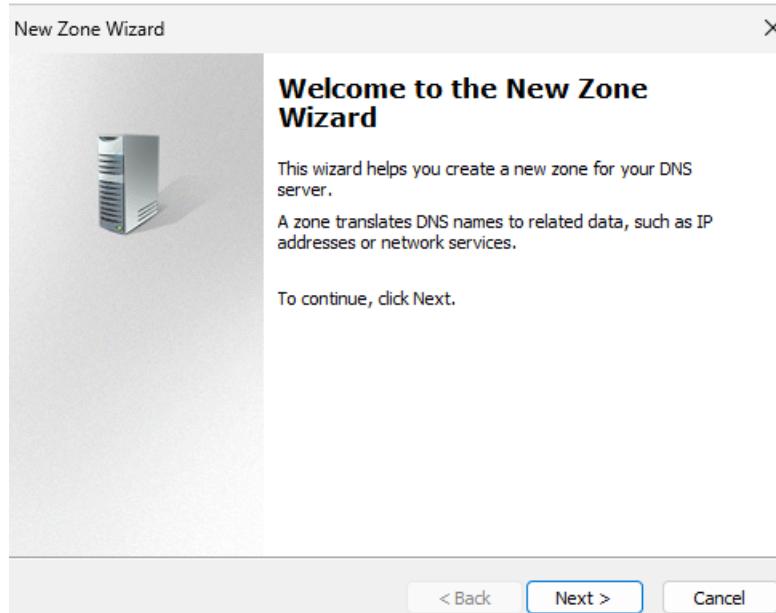
كدا صفت ال name دا : 192.168.2.50 وال ip بتاعه : pc1.xyz.com

عشان مثلا دا لو web sever وانا بكتب pc1.xyz.com يروح يشاور على 192.168.2.50 فيشتغل معابيا

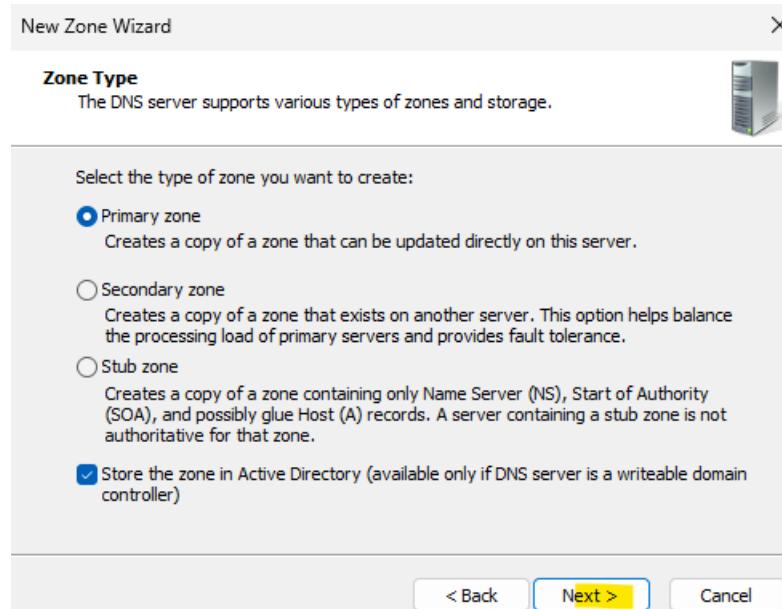
طیب فی ال : Reverse lookup zone



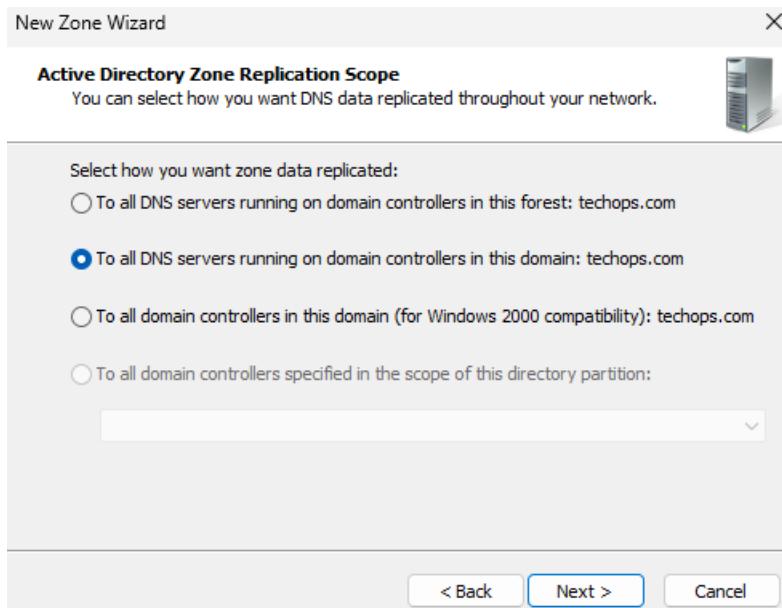
عليها و اختار Click new zone



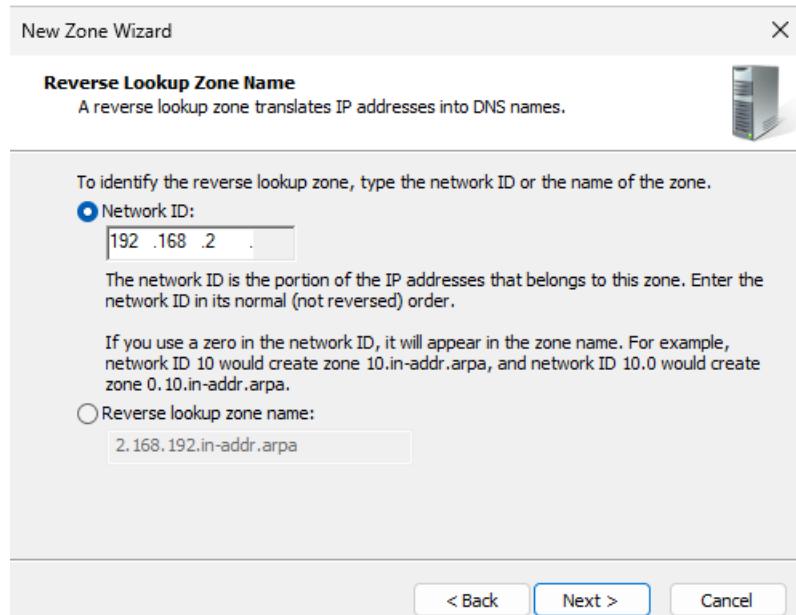
Next



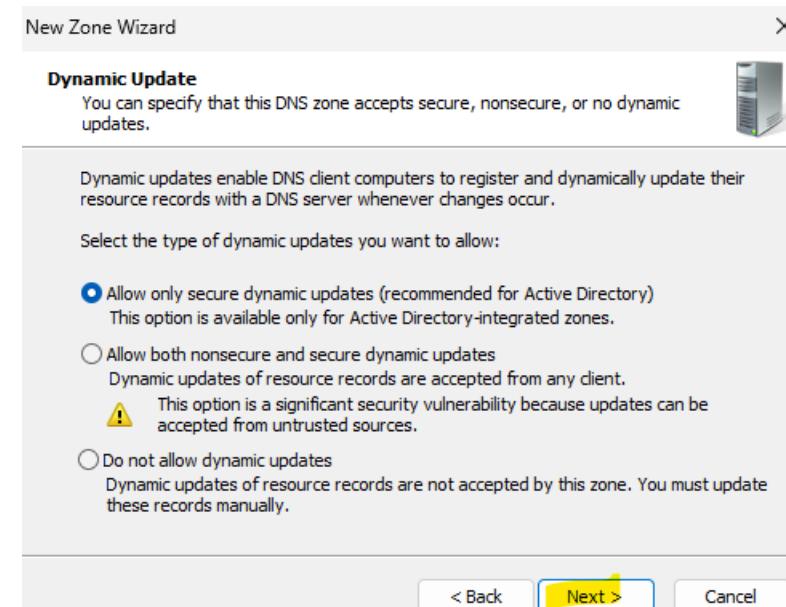
Next



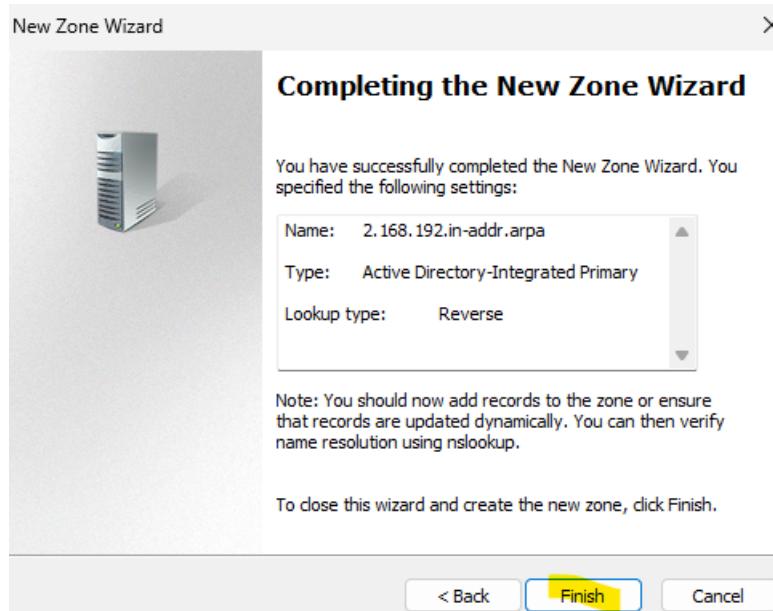
Next



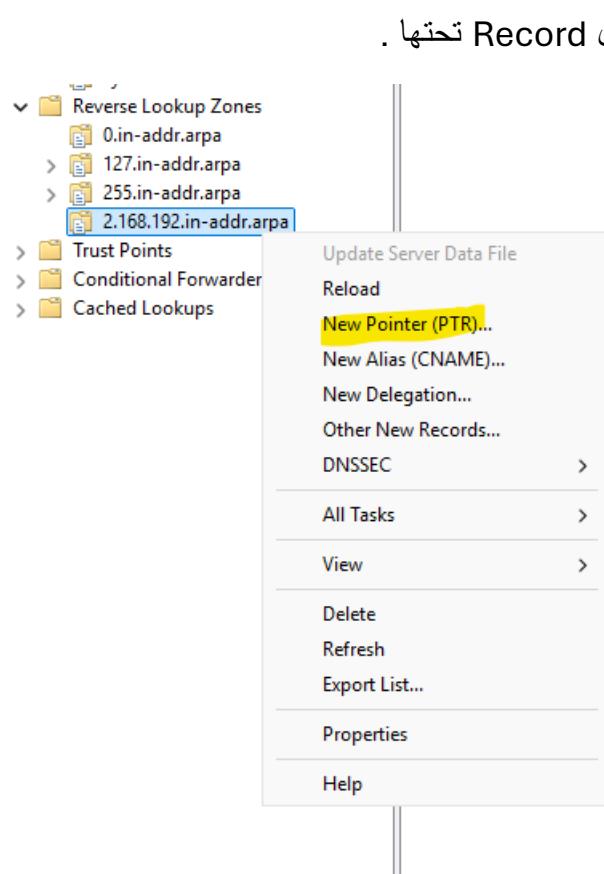
حدد ال network ID



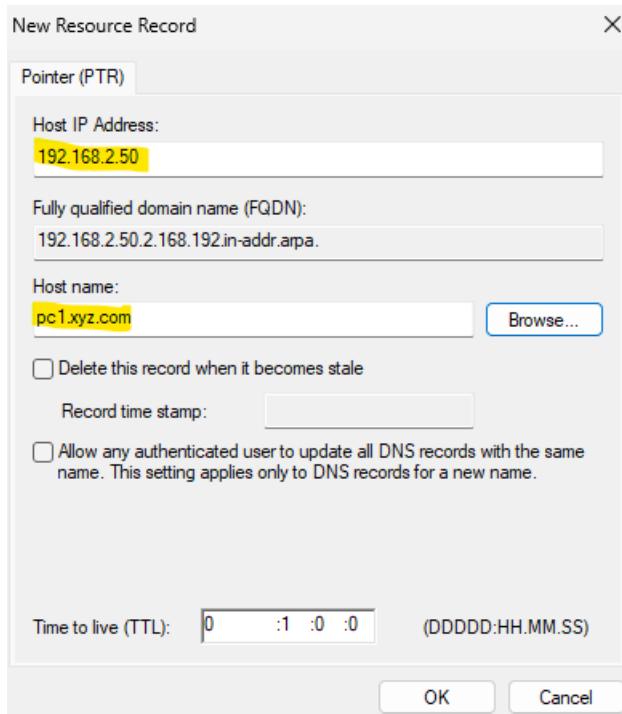
Next



Finish



زې ما عرفنا هنا هيكون PTR لان دا عکس ال A يعني دا هدیله Ip هيرجعلي ال name بتاعه



كتبت ال ip رجلي ال name

WDS Server

اختصاراً لـ Windows Deployment Services

يستخدم في عمل Network Deployment عن طريق الـ operating System دون الحاجة الي USB او CD

متطلباته ؟

-1 الـ server يكون Member من الـ domain

-2 DHCP : لتوزيع الـ IPs على الجهاز الذي تفلع عبر الشبكة

-3 DNS Server : عشان اقدر اوصل للـ domain

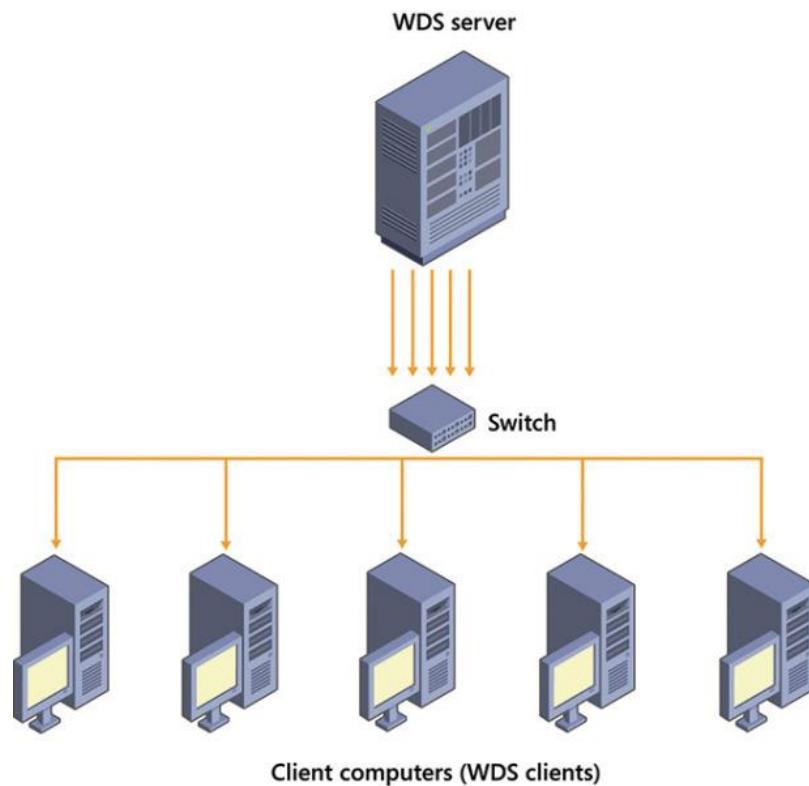
-4 NTFS : لازم الـ Partition عليه الـ image Files يكون NTFS

وطبعاً لازم الاجهزه بتاعتي اصلاً تكون بتدعم الـ PXE عشان اقدر اعمل boot من الـ Network

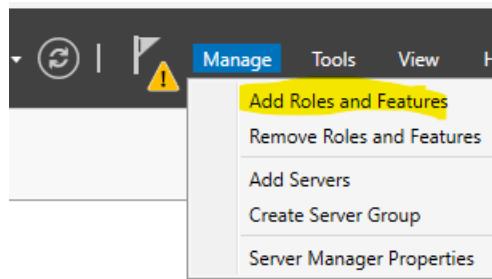
مكوناته ؟

-1 Boot image : تستخد لبدء تثبيت الـ OS وبتكون ماخوذة من قرص تثبيت الـ windows boot.win هو

-2 Install image : دي الـ Image الفعليه المراد تثبيتها install.win



طيب از اي ابدا اشتغل عليه ؟



هروج على Add Roles من manage

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

Roles	Description
<input checked="" type="checkbox"/> Active Directory Domain Services (Installed)	
<input type="checkbox"/> Active Directory Federation Services	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Device Health Attestation	
<input checked="" type="checkbox"/> DHCP Server (Installed)	
<input checked="" type="checkbox"/> DNS Server (Installed)	
<input type="checkbox"/> Fax Server	
<input checked="" type="checkbox"/> File and Storage Services (3 of 12 installed)	
<input type="checkbox"/> Host Guardian Service	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Network Controller	
<input type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	
<input type="checkbox"/> Volume Activation Services	
<input type="checkbox"/> Web Server (IIS)	
<input checked="" type="checkbox"/> Windows Deployment Services	
<input type="checkbox"/> Windows Server Update Services	

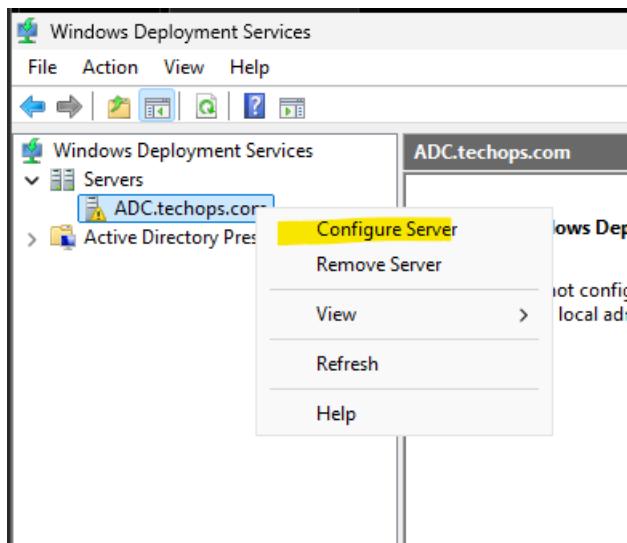
< Previous Next > Install Cancel

وهختار ال Windows Deployment Service

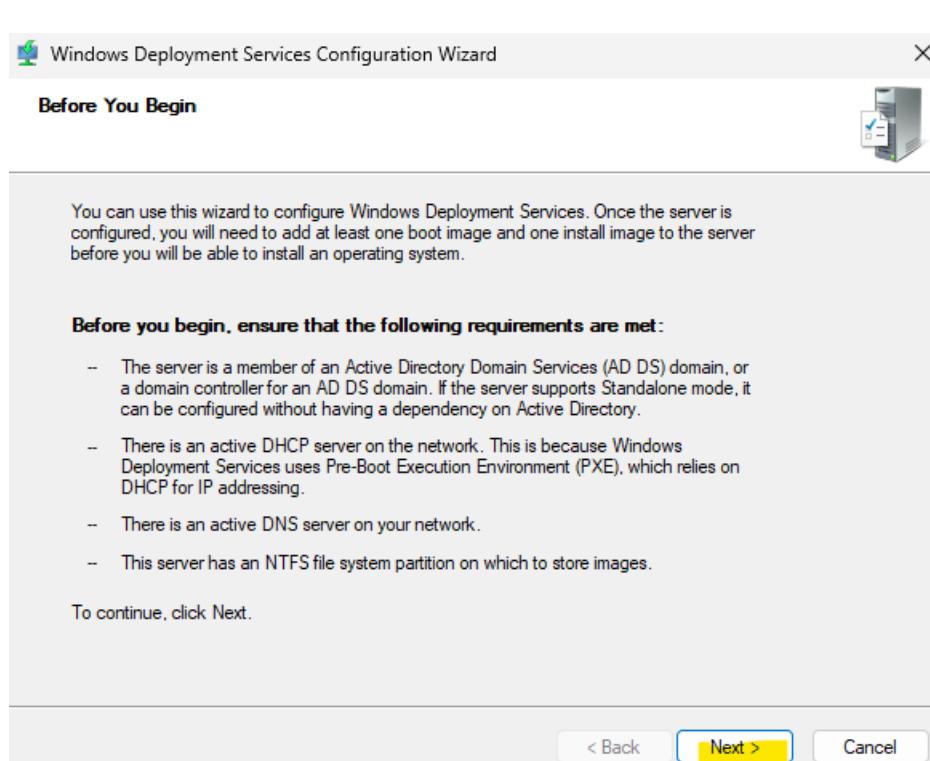
وبكدا عملت Install لـ Configuration Service ونبدا نعمل ال



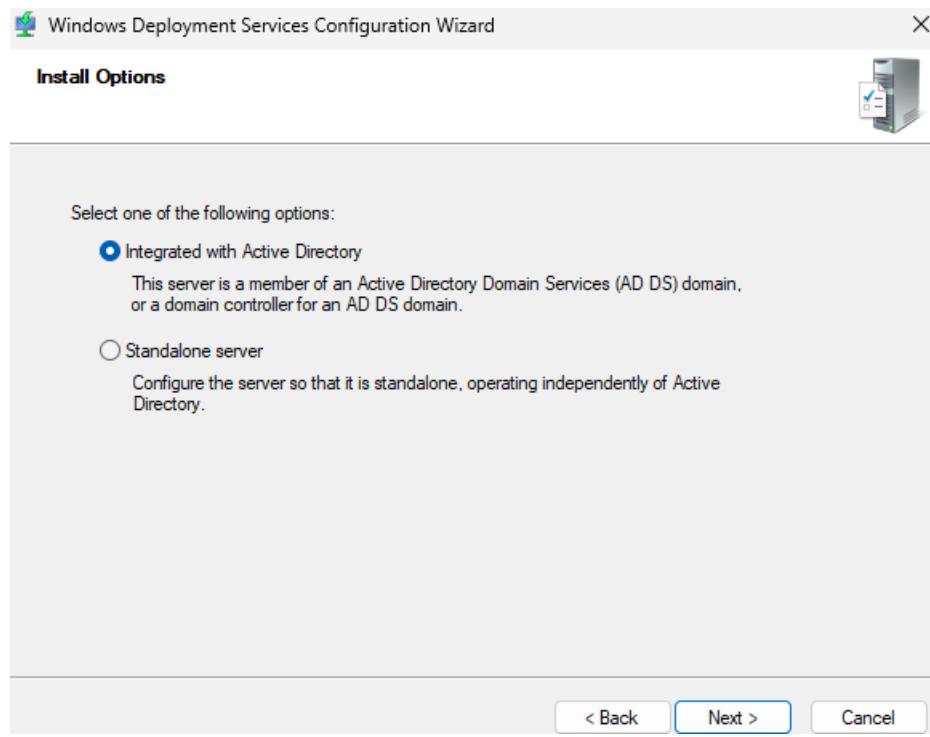
tools من open لها نعملها



هـنـضـغـط عـلـي الـ Cоnfigure Server وـنـخـتـار domain name

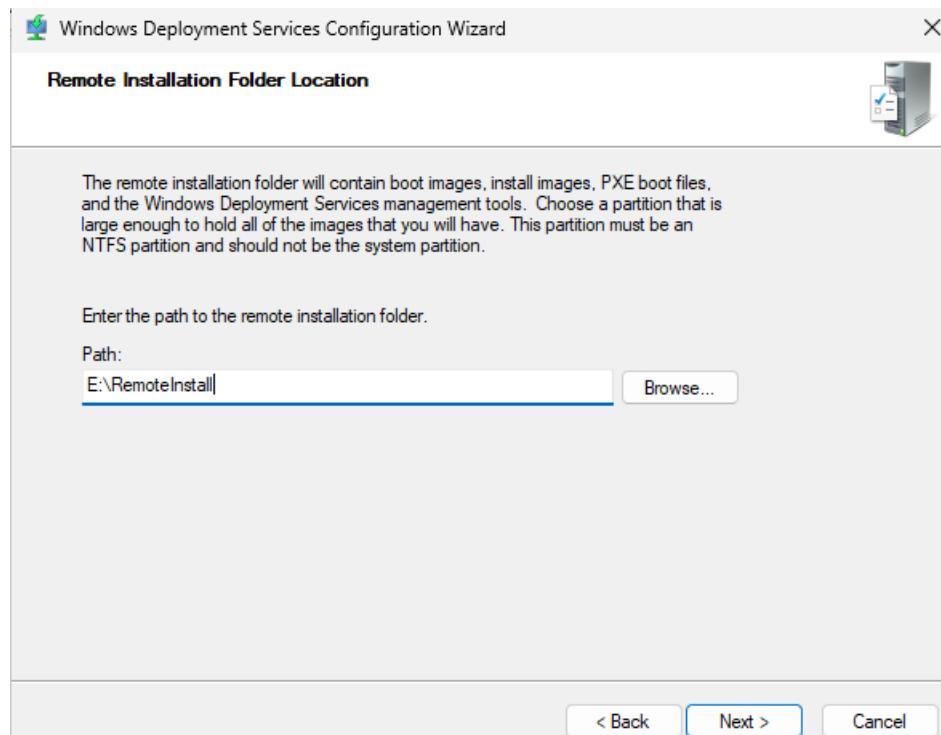


بـيـوـضـحـ الـمـتـطلـبـات الـ اـتـكـلـمـنـا عـنـهـا فـوـقـ

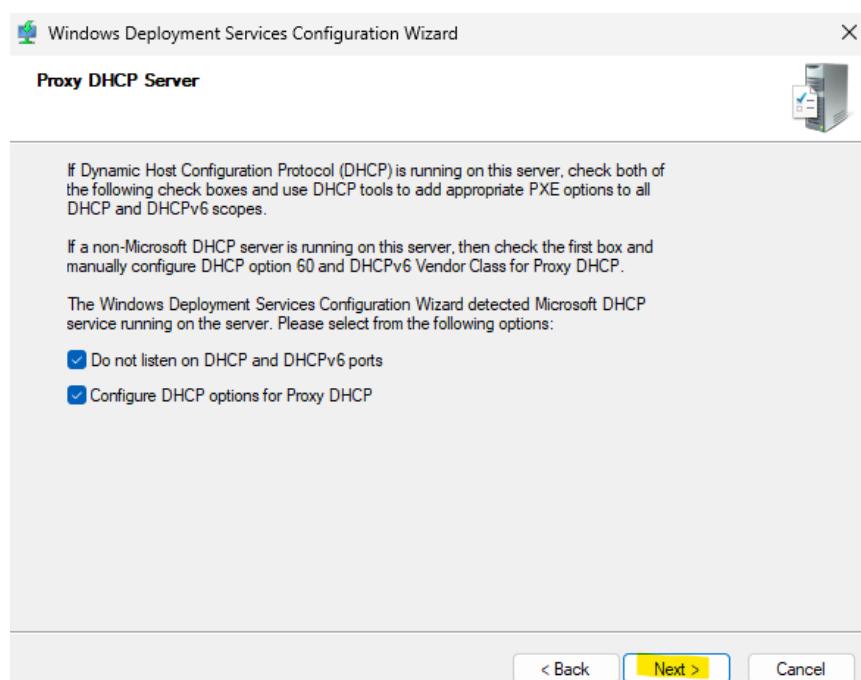


هختار **Integrated with Active Directory**

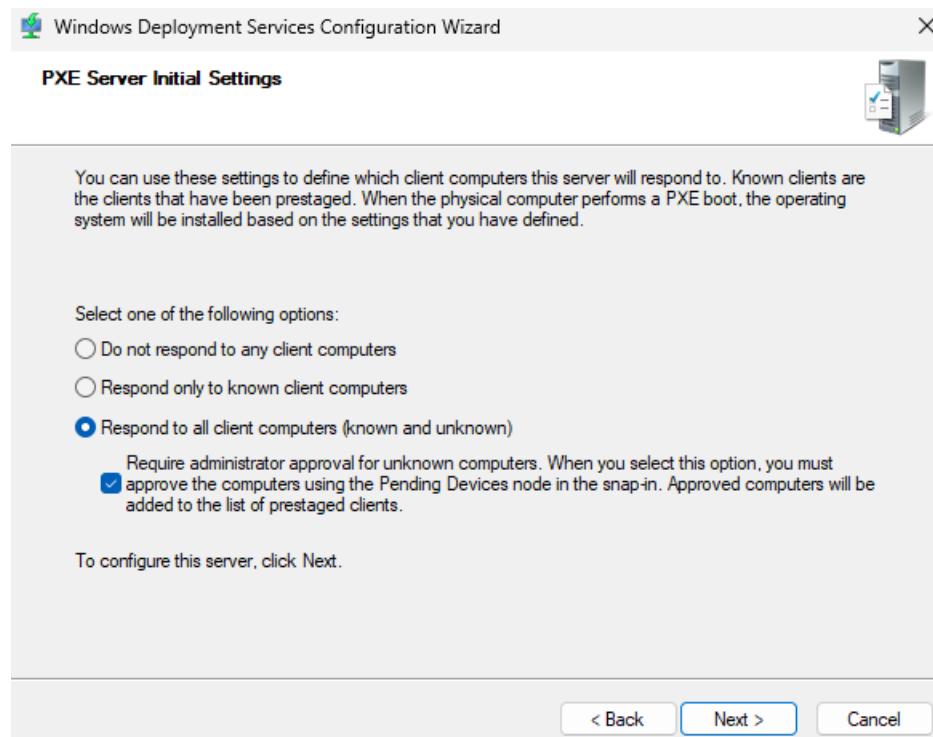
--



بنحدد ال remote installation folder



Next

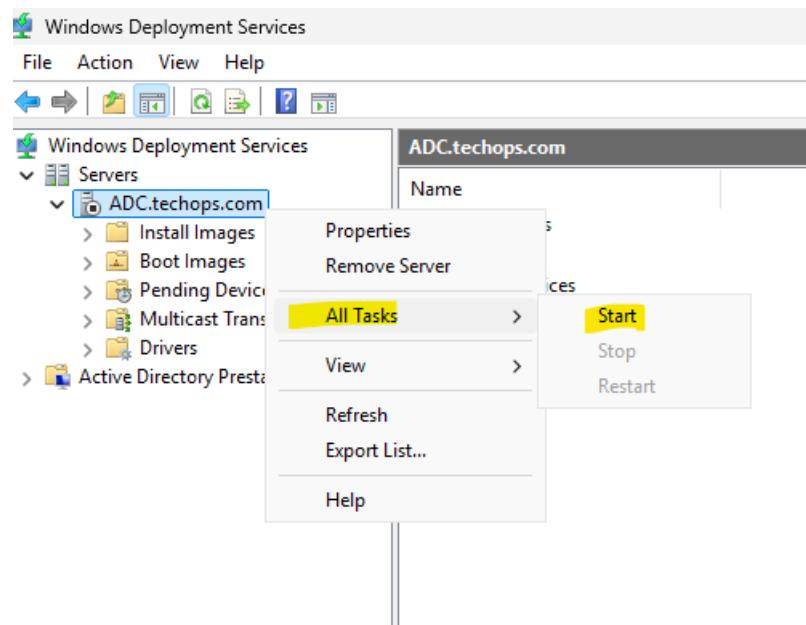


service : دی کدا محدش هيقدر يوصله كان ال
stop معولها

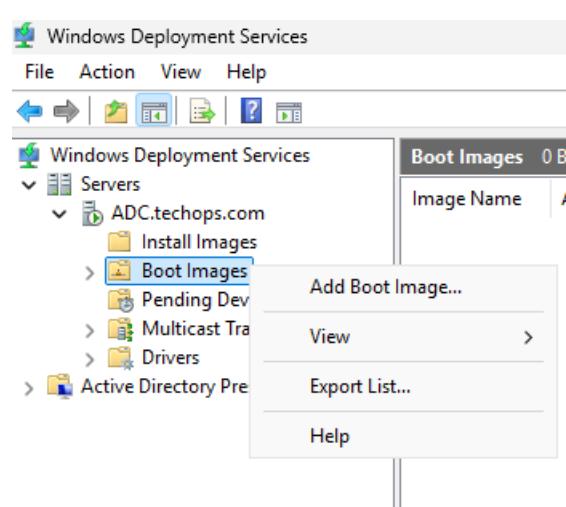
: لازم يكون الجهاز مضاف يدوياً مسبقاً في
Pre-staged device أو في Active Directory

: يستجيب للجميع ، لكن لازم تدخل ال password الخاصه
بال administrator approval for option ال اسمه unknown computers

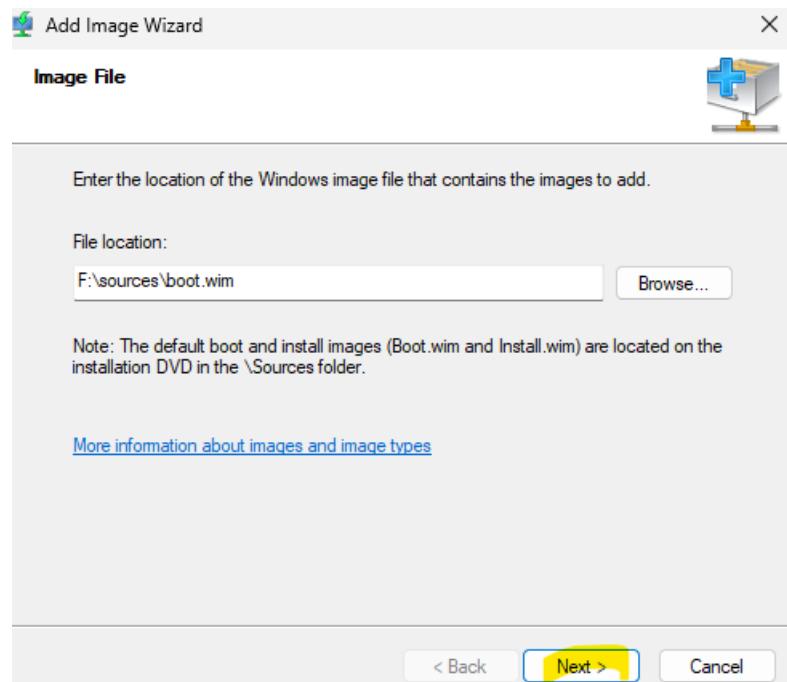
--



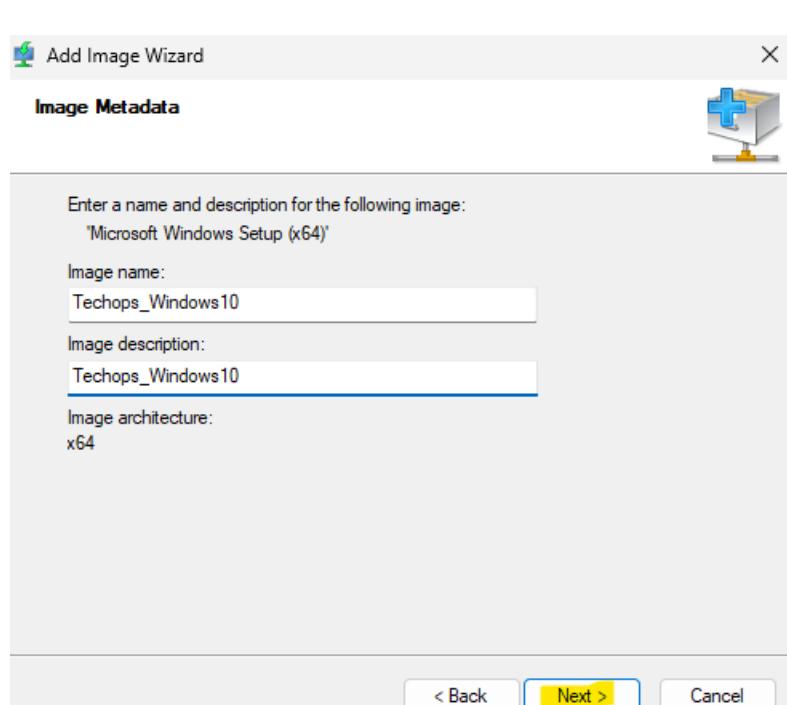
بیکون بالشکل دا هروج علی Start واعمل All tasks



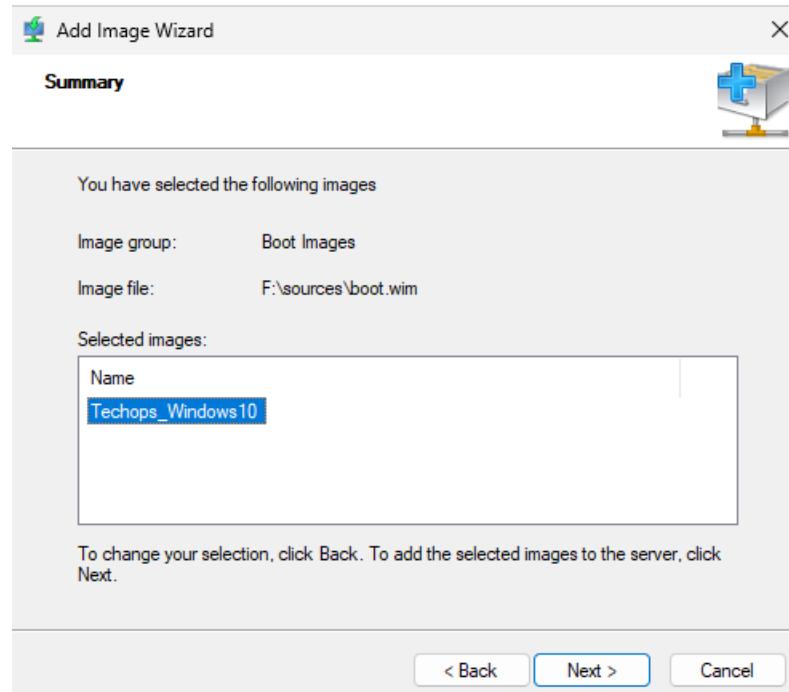
هعمل boot image ودي ال هعمل منها ال boot بتاعي



بحدد ال boot.wim في ال sources ب اسم boot image path

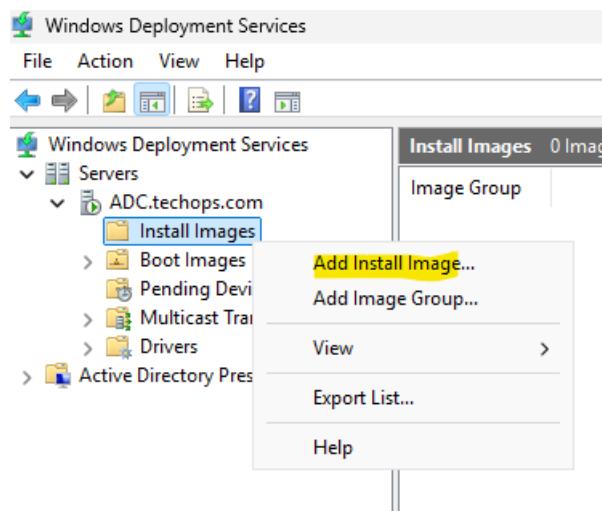


ال Image Name

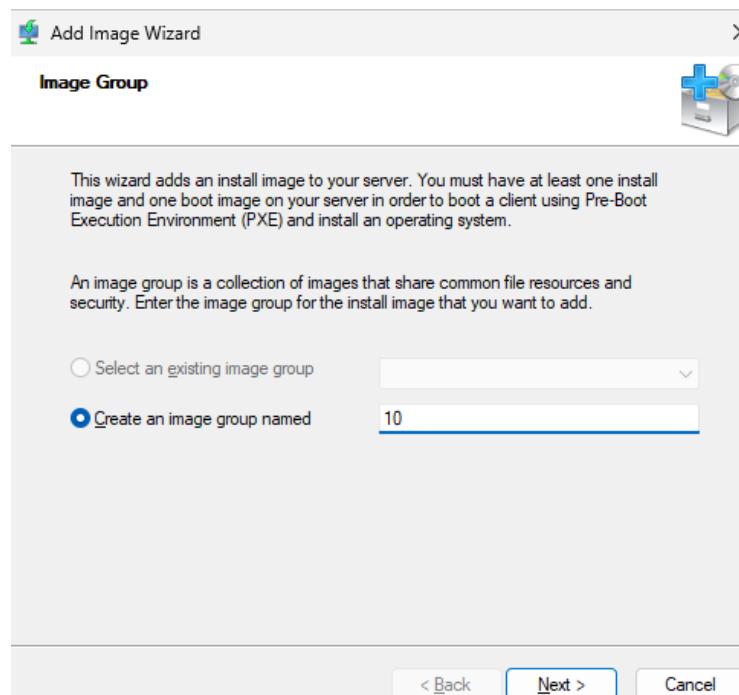


Next

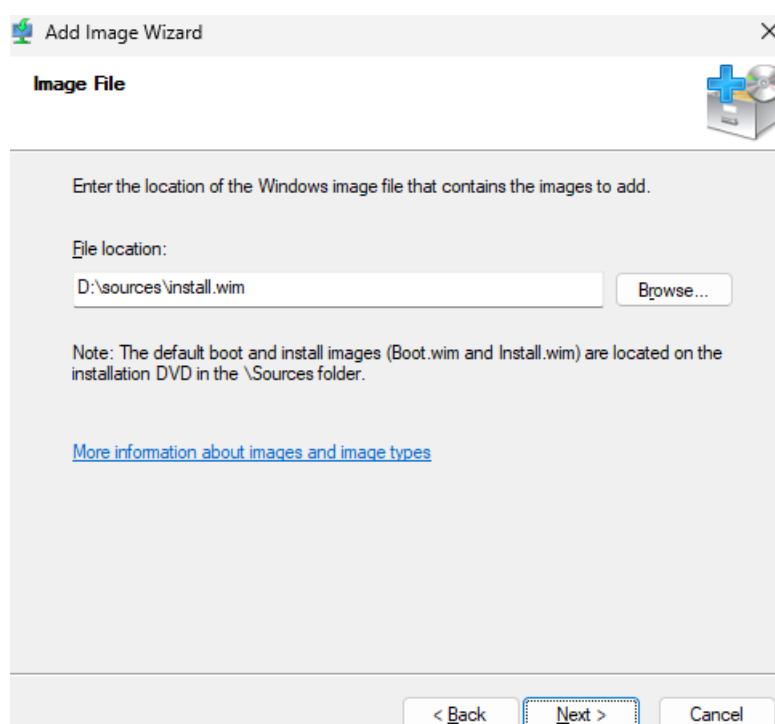
بعد كذا هنبدأ نعمل Install Image



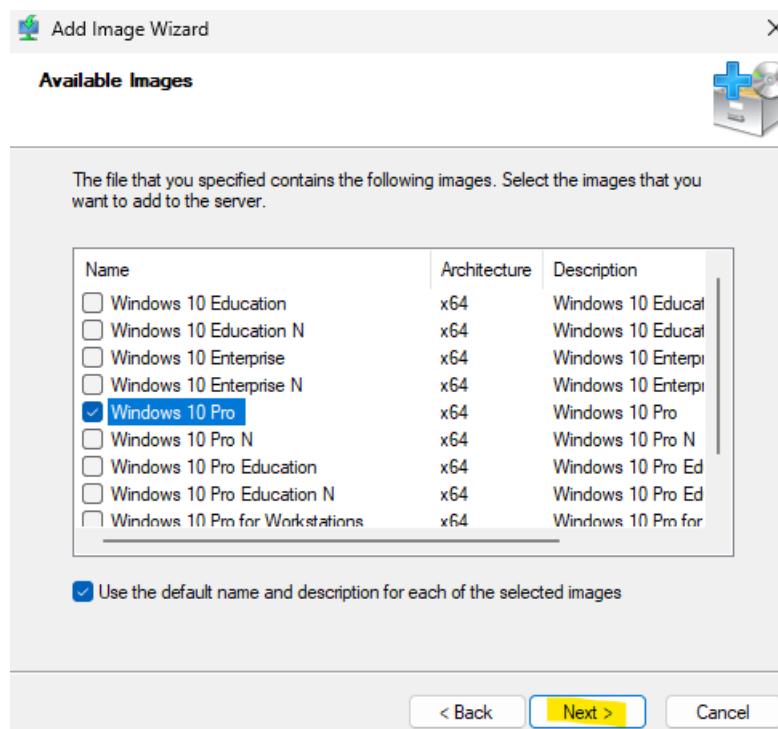
من Add Install Image هنختار install image



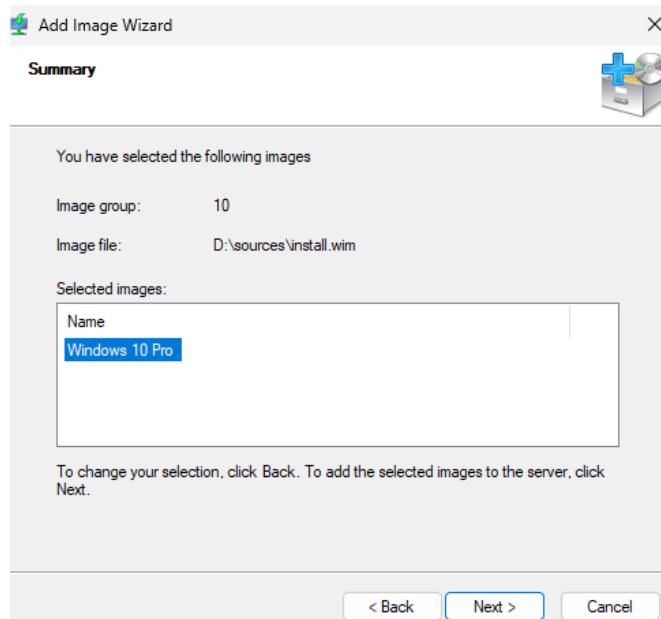
بنحدد ال image group عشان لو عندك اكتر من نسخه زي مثلا win10 , win11,win serv2025



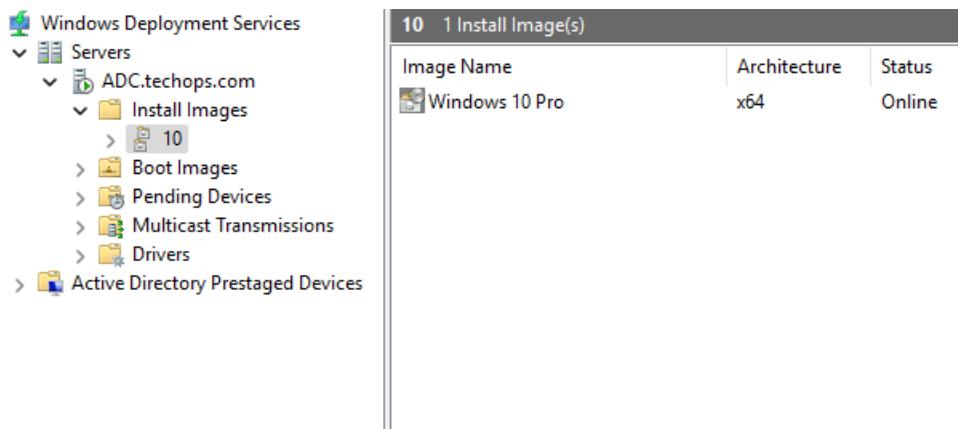
بعد كدا بتحدد ال Install.wim



بحدد انا عاوز اضيف انهي نسخه

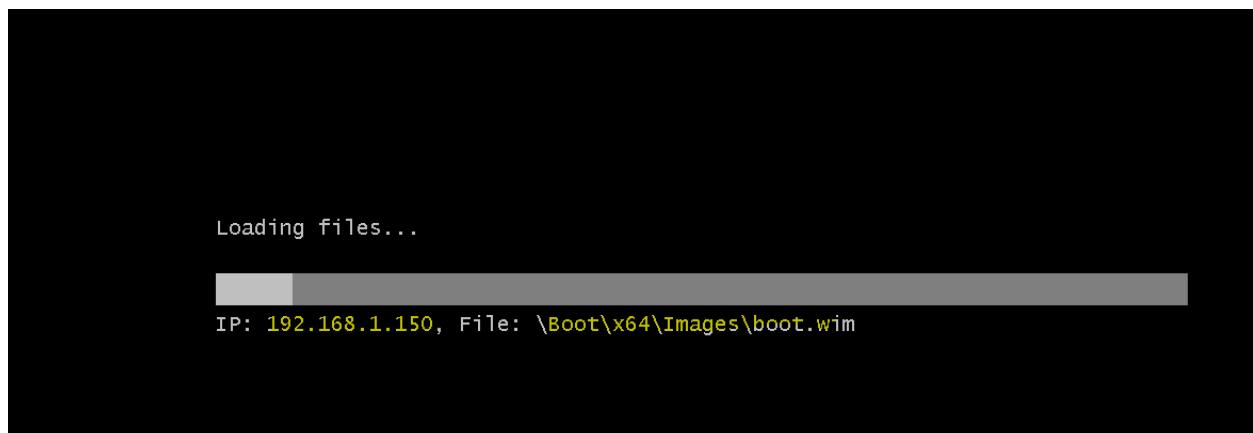


Next



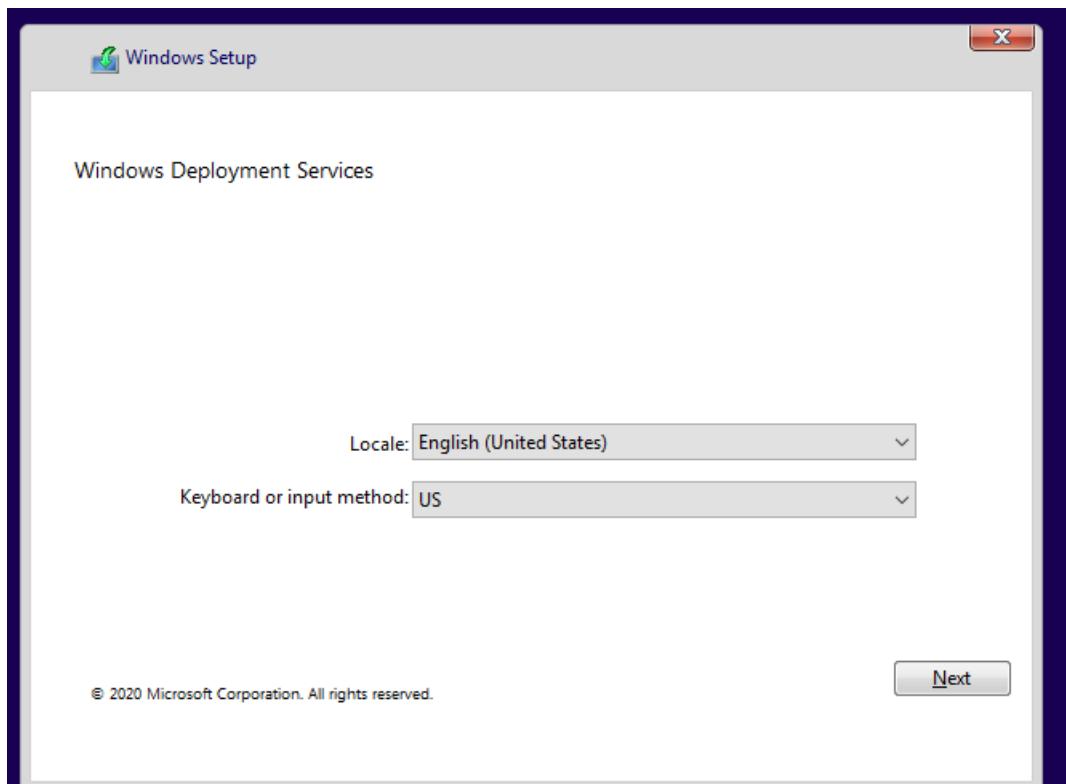
كدا بقت موجوده عندي

--
طيب ازاي نبدا نعمل os من النسخه دي؟
هنعمل vmware workstation ل vm على
وفي نخللها تعمل boot من ال network



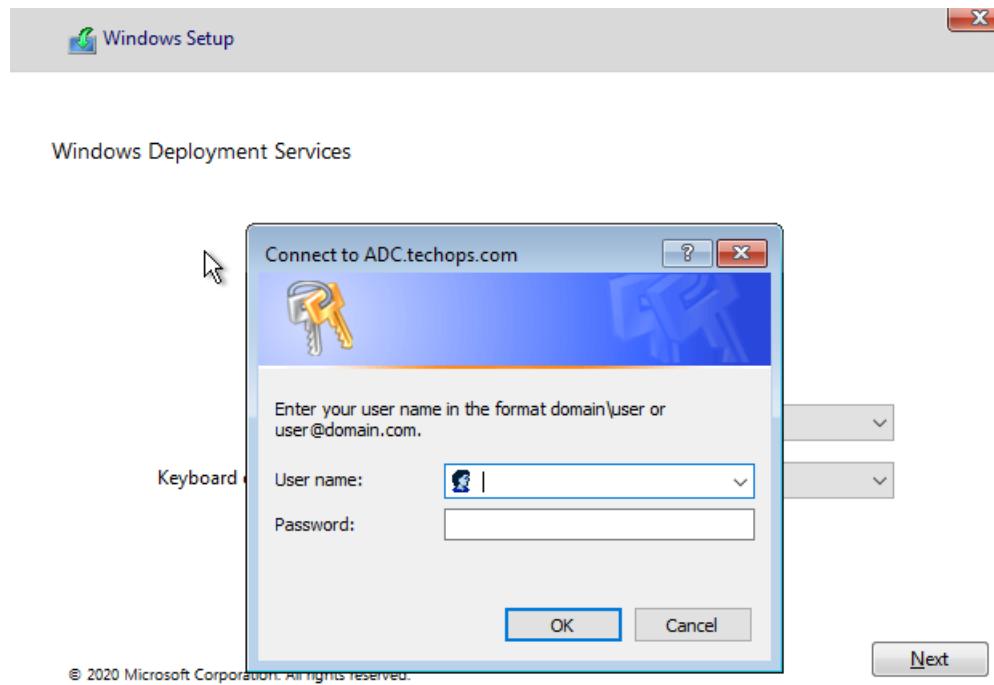
بعد ما عملت boot من ال network قدر انه ياخد IP من ال DHCP وقدر يوصل لـ WDS Server
ال هو 1.150 ودخل على ال path بتاع ال boot

--



وأبد الخطوات عادي

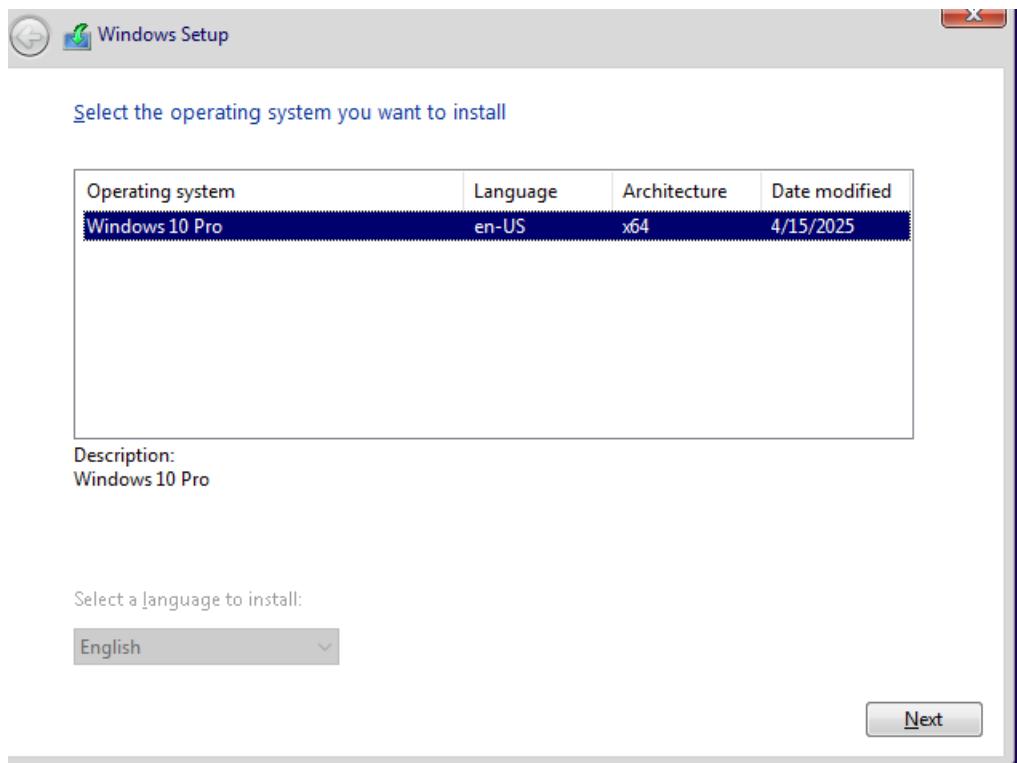
--



لكن لازم اكتب له ال upser وال password الخاصين بال administrator

--

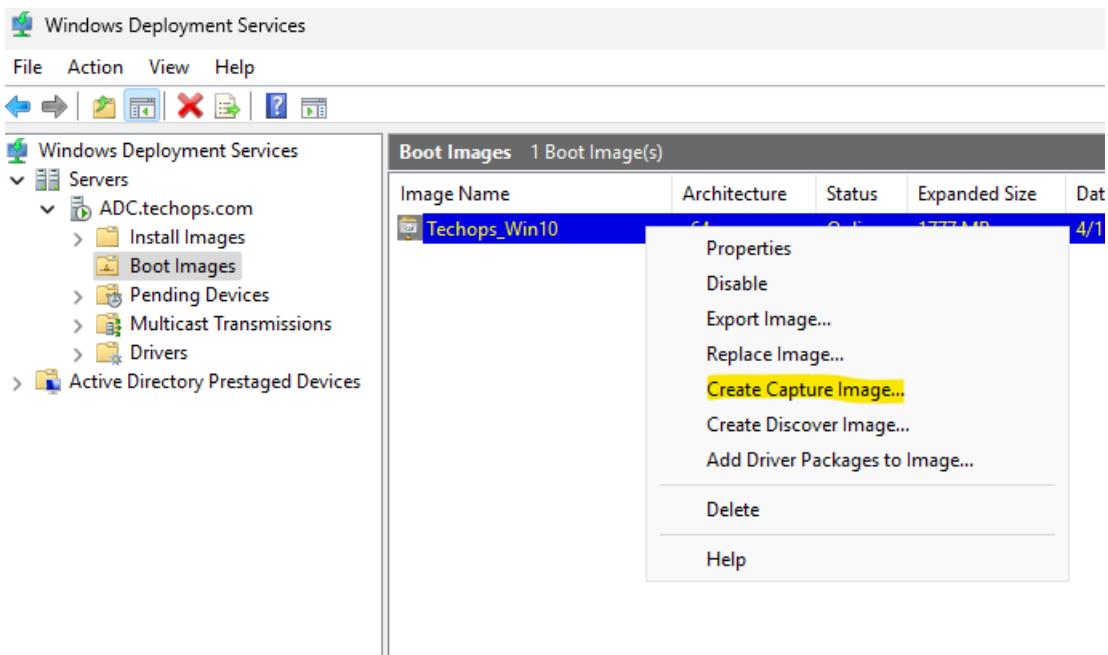
بعد كدا تكمل مراحل ال Install طبيعى خالص



النسخه ال كنت محددها ال هي win 10 pro

--

بعد ما عملنا ال os دا هنبدا في الخطوه الثانيه وهي اني هعمل install لـ app ال عاوزها واحد من النسخه دي image ارحطها علي ال WDS وهي دي ال هستخدمها فيما بعد



اول خطوه وهي اني هعمل image capture من ال image الذي عندي
من ال boot Image click على خيار create capture image

--

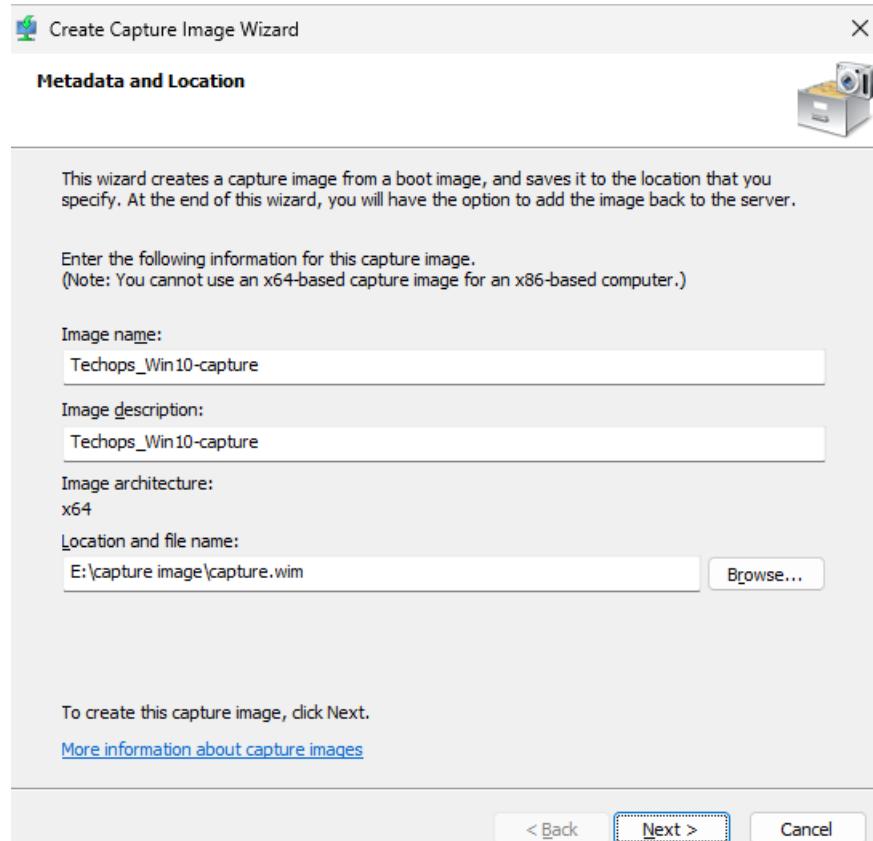
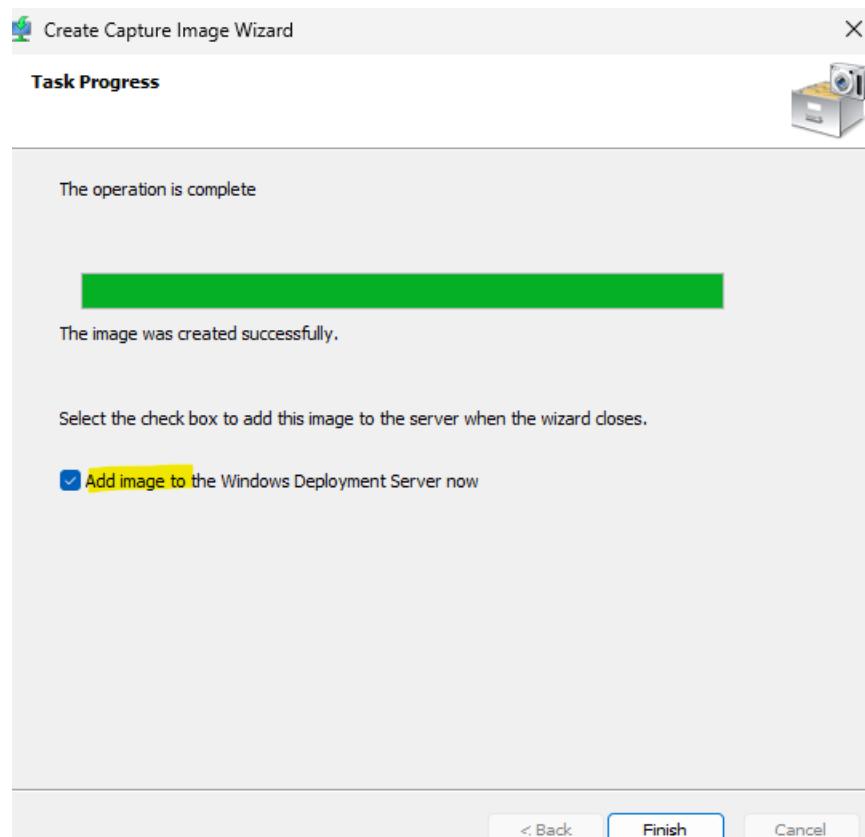


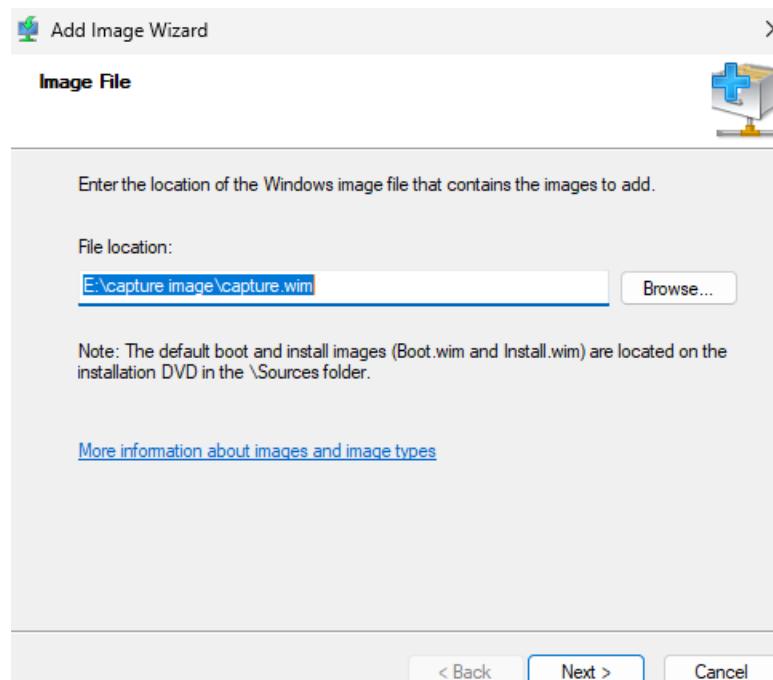
Image لـ path و Name

--

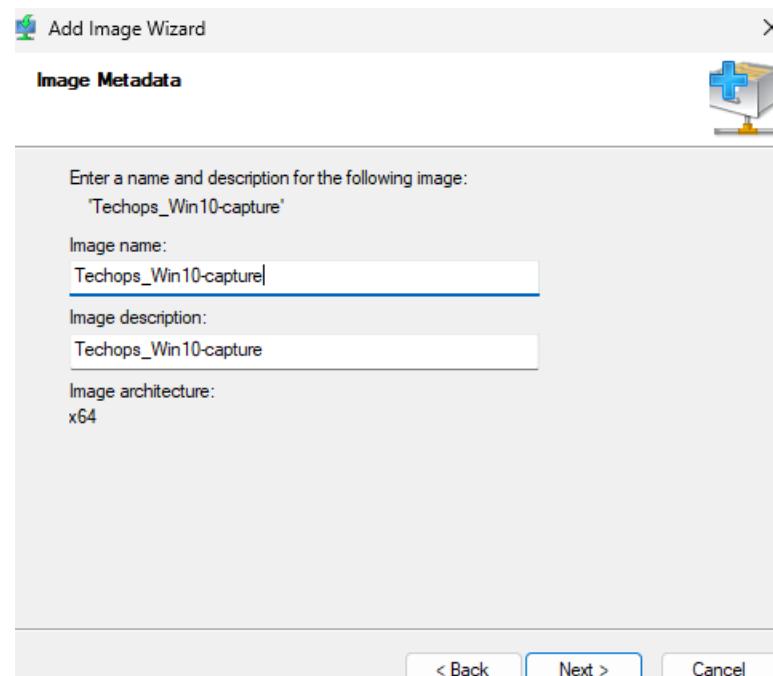


و هعمل check على ال box دا عشان ينزل ال image في ال WDS

--

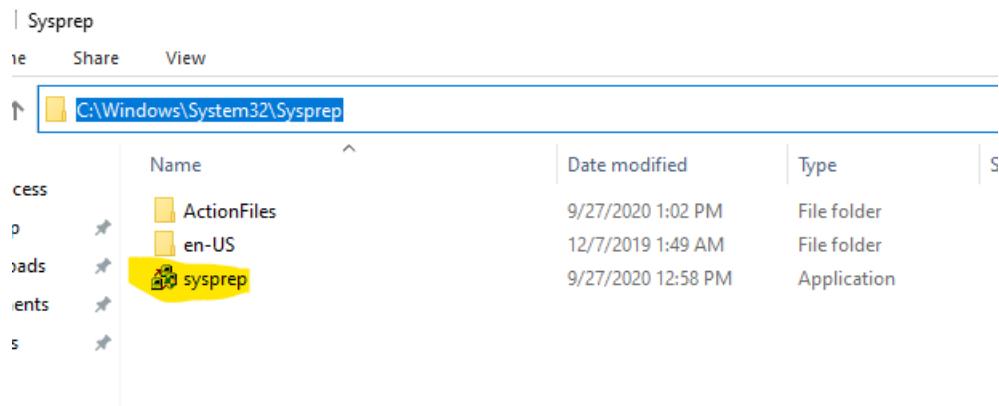


ال path

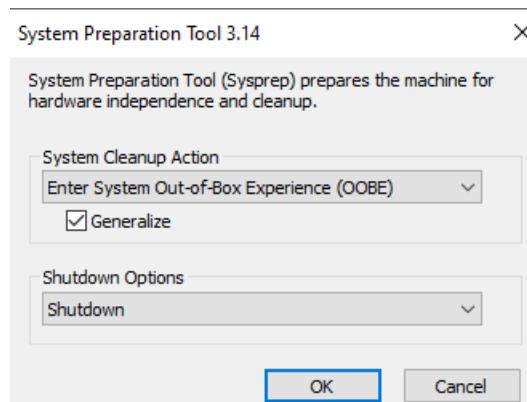


ال name دا بتاع os

تاني خطوه هنعمل Sysprep ودي عشان ال SID ميترersh على الاجهزه الي هينزل عليها ال OS دا



هندخل في ال path دا ونشغل ال sysprep



هختار ال configuration دى بعد ما يخلص ال shutdown هيحصل sysprep وانا بشغل ال vm

هختاراني اعمل boot من ال network واختار ال boot.wim الجديد الخاص بال capture

Windows Boot Manager (Server IP: 192.168.1.150)

Choose an operating system to start:
(Use the arrow keys to highlight your choice, then press ENTER.)

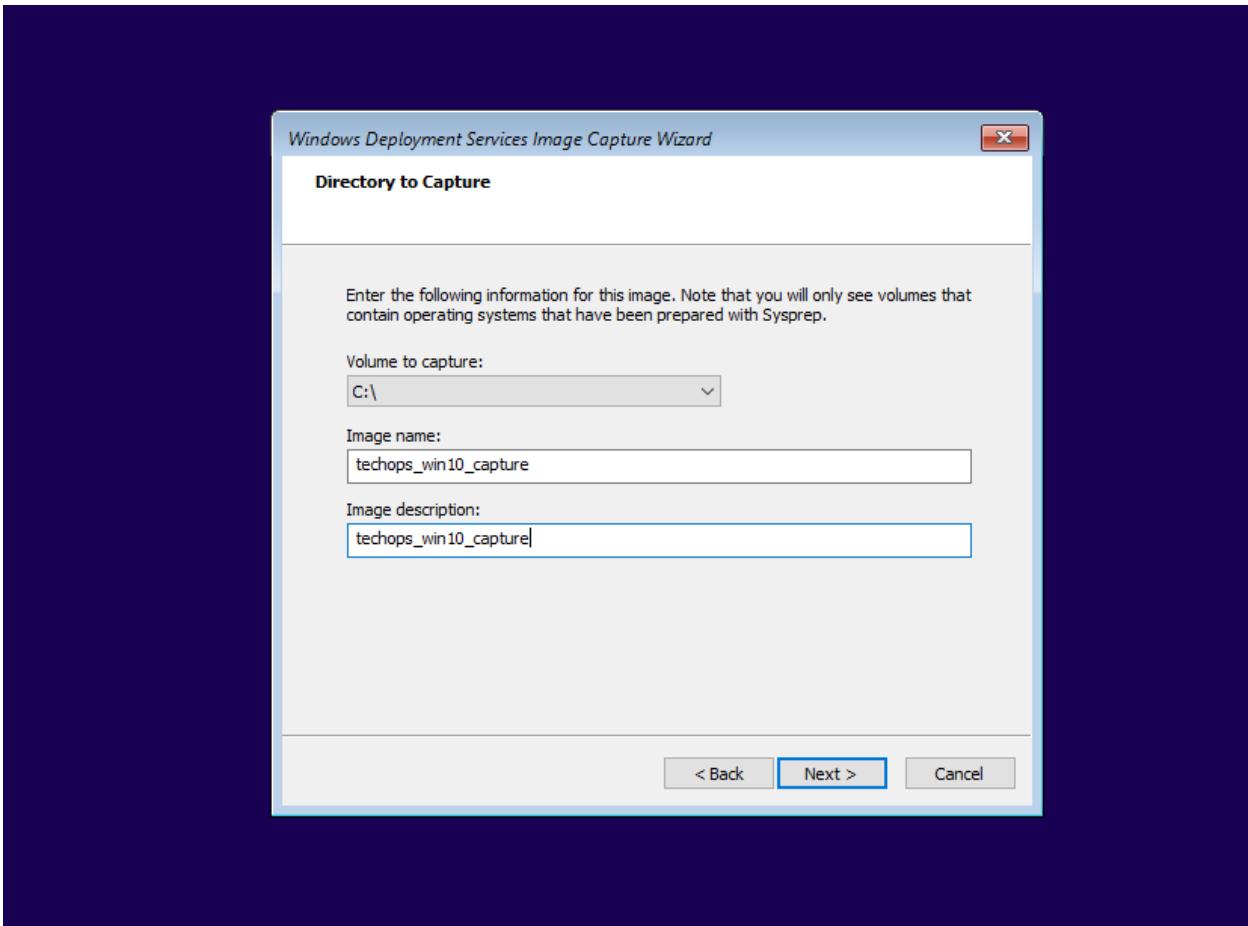
Techops_Win10
Techops_Win10-capture >

To specify an advanced option for this choice, press F8.

ENTER=Choose

ESC=Exit

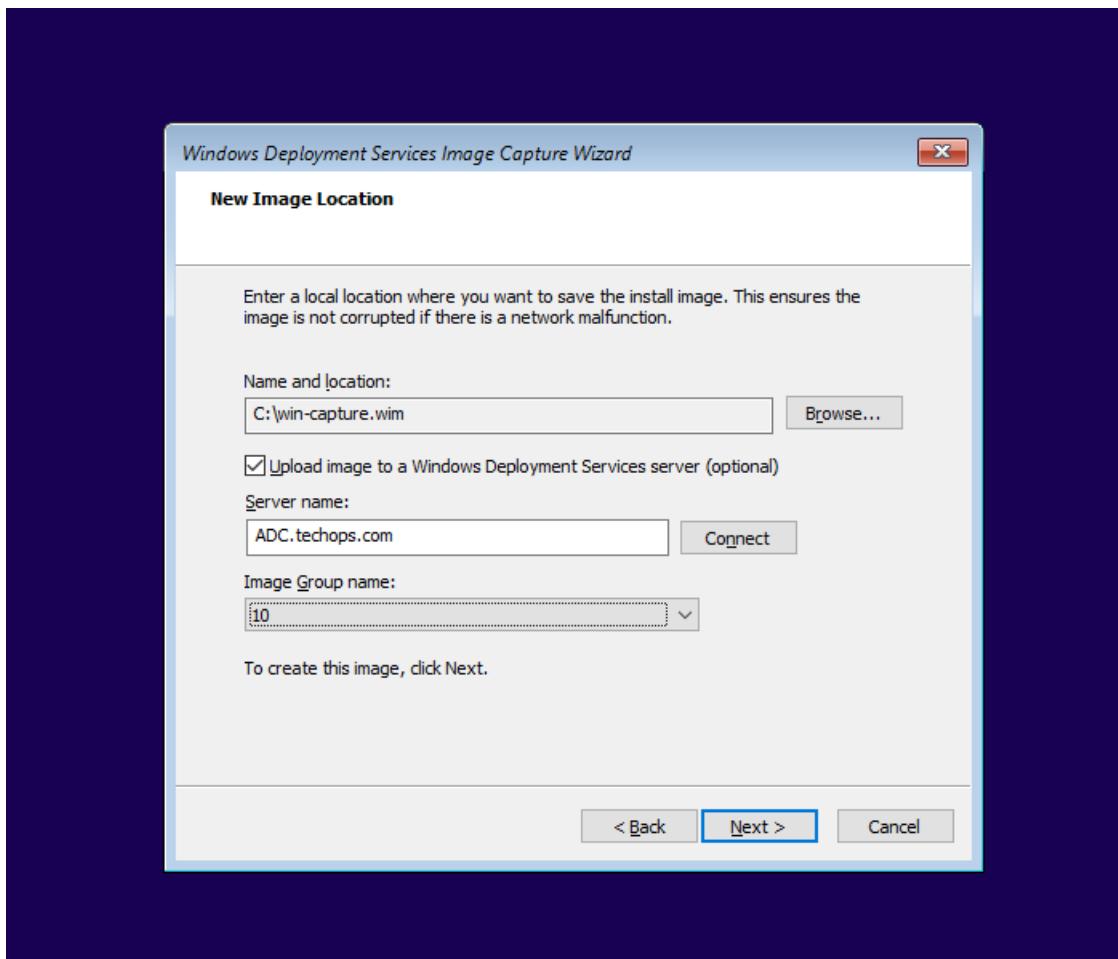
هختار النسخه ال capture --



بیسالنی ال Image دی هنکون فین

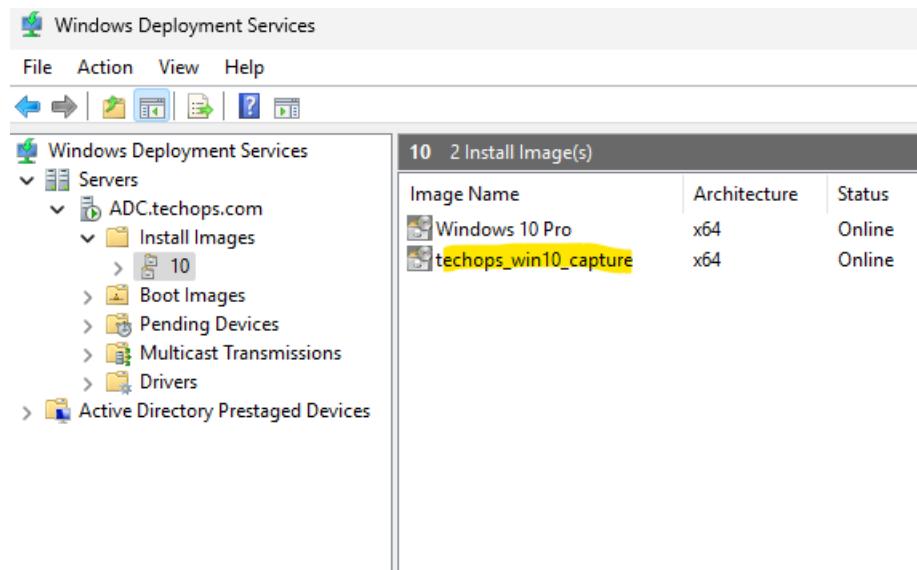
وال name بتاع ال Image دی

--



هیسالني عن ال path ال هتترمي فيه
وهو قوله ان يرفع ال image دي علي ال WDS
ف بيسالني عن ال server ف عملت عليه connect
بعد كدا بيسالني هحط ال image دى في انهي group داخل ال WDS Server

--



هتلقيها نزلت في ال Install Image على ال WDS Server

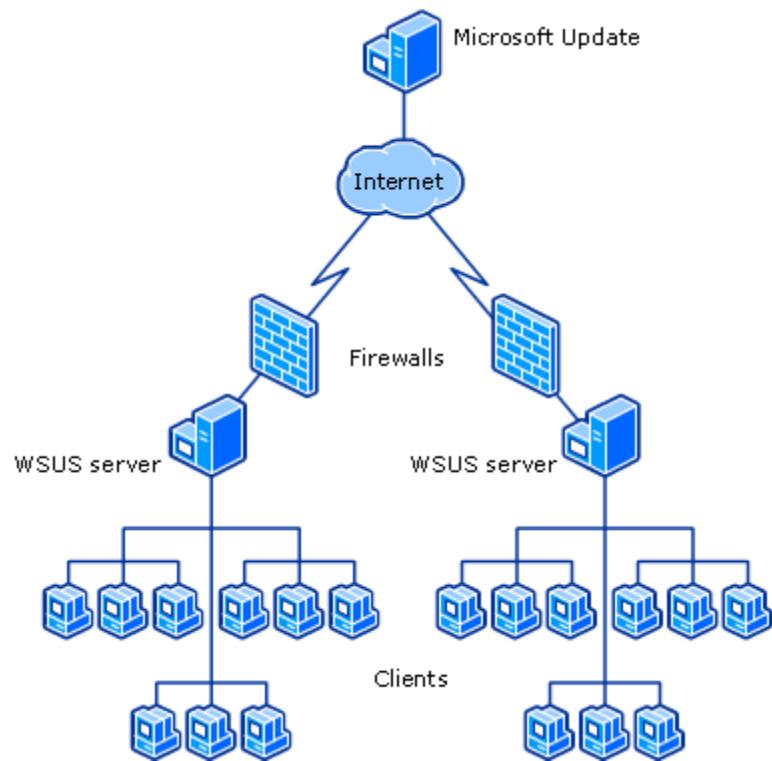
--

لما تيجي تعمل os من ال network وانت بتختار ال os بعد كدا هيجبلك عاوز
techops_win10_capture ولا Windows 10 pro

WSUS

اختصاراً لـ windows server update service

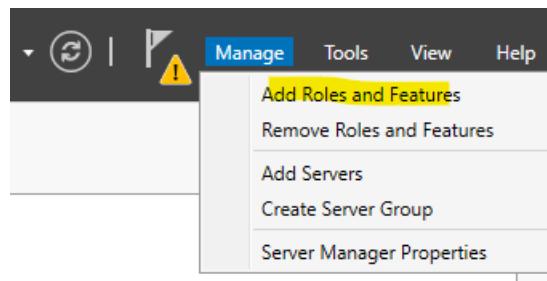
مهمته هي انه ي يعمل download لـ Microsoft update من Microsoft و يوزعها على الاجهزه ، بدل ما كل جاهز يحمل الـ Microsoft update مباشره من Microsoft



مكوناته ؟

- update : دا ال نفسه ال هيروح يعمل download لل WSUS Server -1
- DB : دي ال DB عشان يحفظ فيها ال configuration بتاعته WSUS Database -2
- updates manage : دي ال بتعمل منها web interface WSUS Console -3
- PCs Clients : ودي ال PCs الي هتوز عليها ال updates -4

ابدا استخدمه ازاي ؟



من Add Roles هروح علي Manage



هختار ال IIS وهي بتحتاج بعض ال services الثانيه ومنها ال Windows server update services
لان دا ال web server ال هنفتح من خلاله ال console

Select the role services to install for Windows Server Update Services

Role services

- WID Connectivity
- WSUS Services
- SQL Server Connectivity

هنا بيسالني عن ال DB ال هيحفظ فيها ال config
ال build-in DB دي WID connectivity
ال SQL Server خارجي : انت هنا هتحفظ ال config على SQL Server Connectivity

--

If you have a drive formatted with NTFS and at least 6 GB of free disk space, you can use it to store updates for client computers to download quickly.

If you need to save disk space, clear the check box to store updates on Microsoft Update; downloads will be slower.

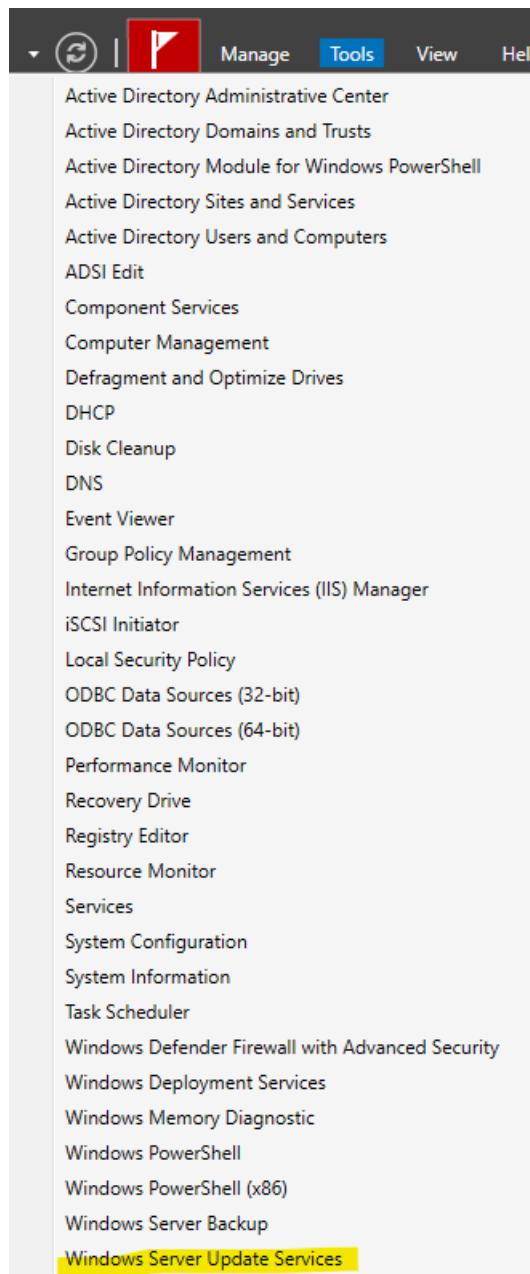
If you choose to store updates locally, updates are not downloaded to your WSUS server until you approve them. By default, when updates are approved, they are downloaded for all languages.

Store updates in the following location (choose a valid local path on PDC.techops.com, or a remote path) :
C:\WSUS\

هنا بيسالني عن ال path ال هينزل فيه ال update

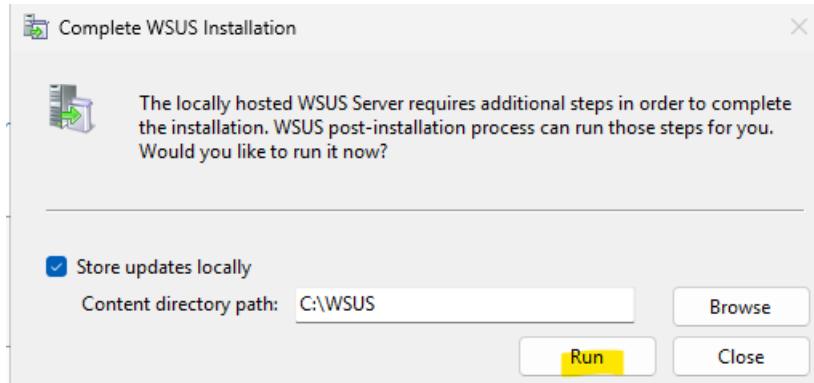
: config نبدا ال Install بعد ال

--

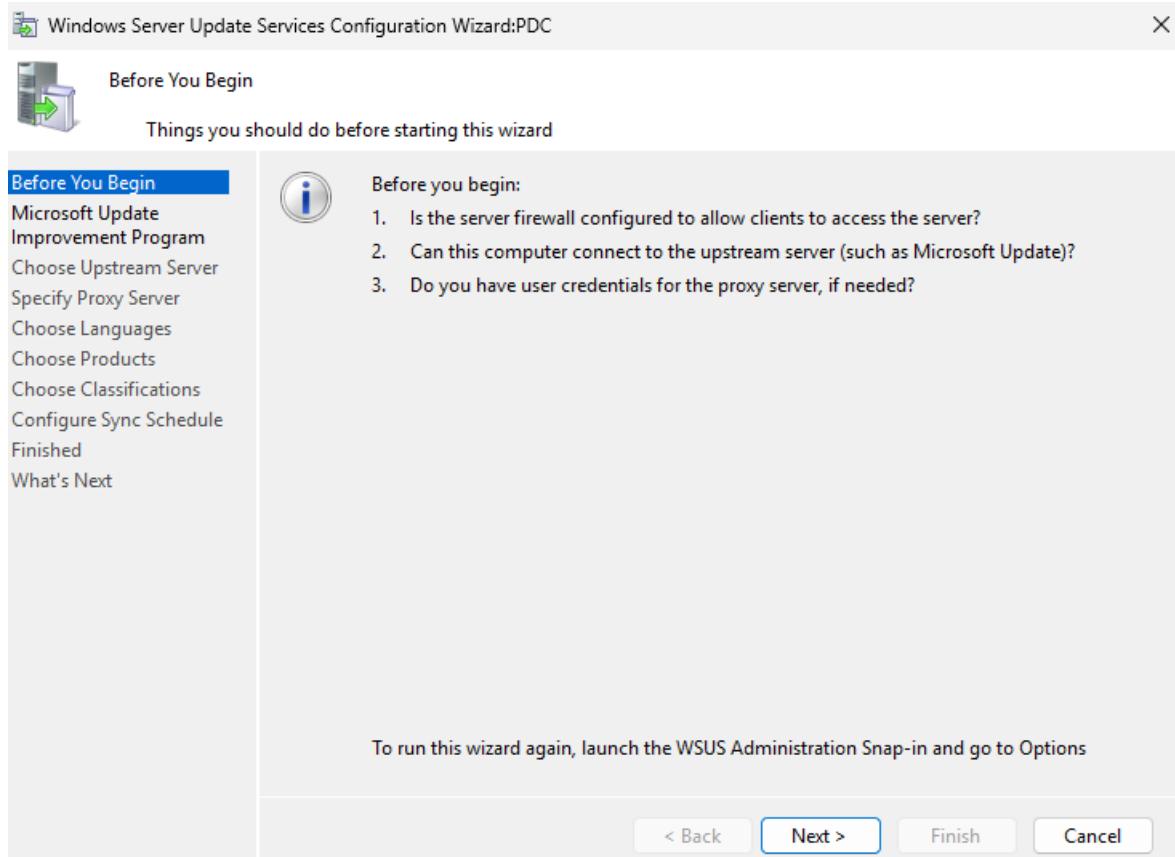


من tools هنختار WSUS

--



بتاكد ال path على click الثاني

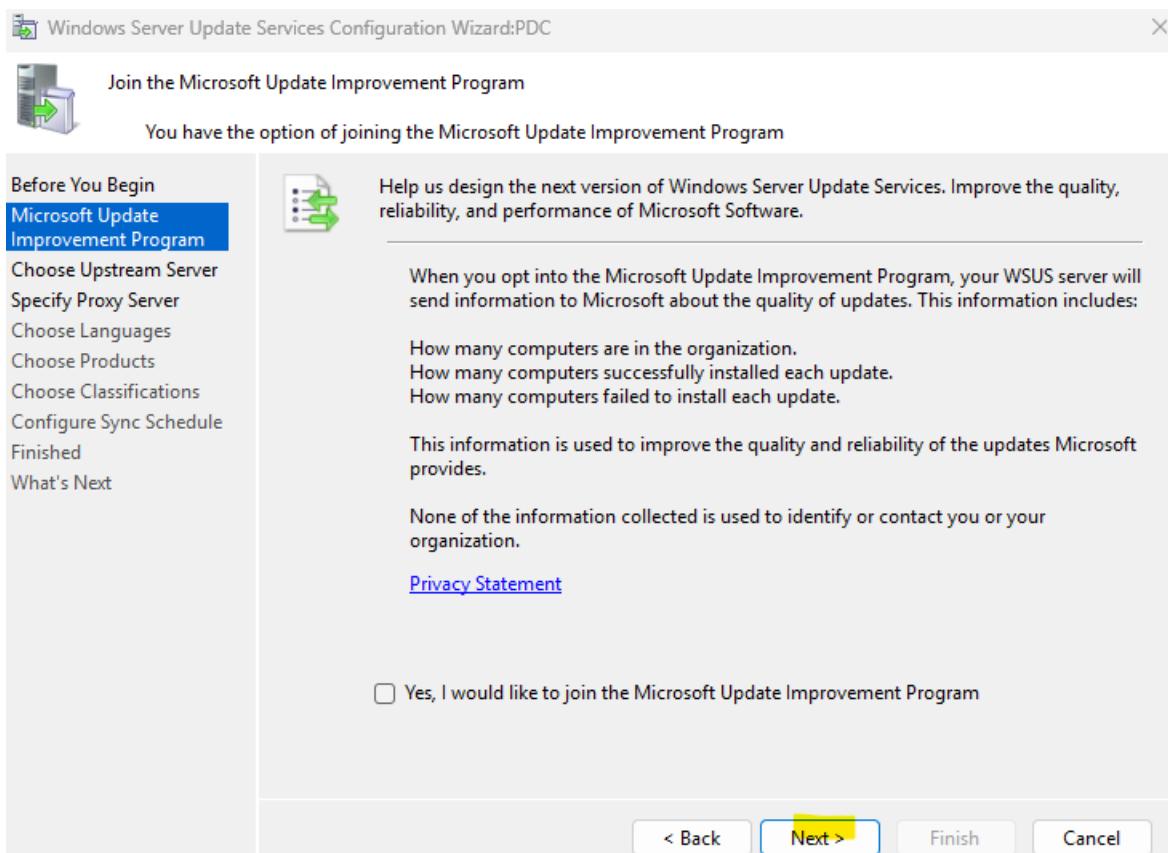


ببیدا ال config

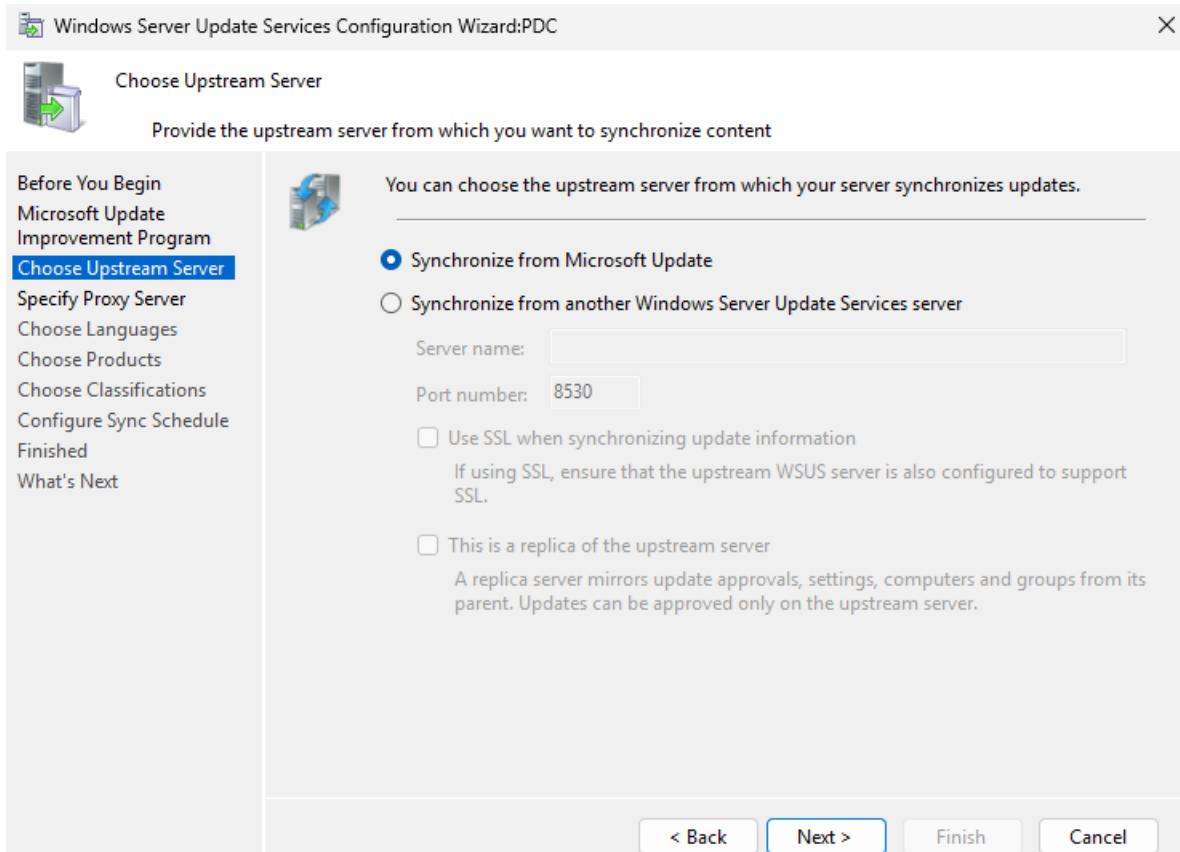
هنا بیعرفني قبل ما ابدا

1- اکون مظبط ال firewall عشان ال client یقدر یوصلی

- 2- ال المطلوبه تكون open ports
- 3- لازم ال server connect على ال up stream server وفي حالي هنا هو MS update (ممكن يكون server تاني يعني server ي Bibgib ال updates من server تاني وال server الثاني دا هو ال Microsoft Update (Bibgibها من Microsoft Update)
- 4- لو فيه proxy عندك فهل معاك ال credentials بتاعته

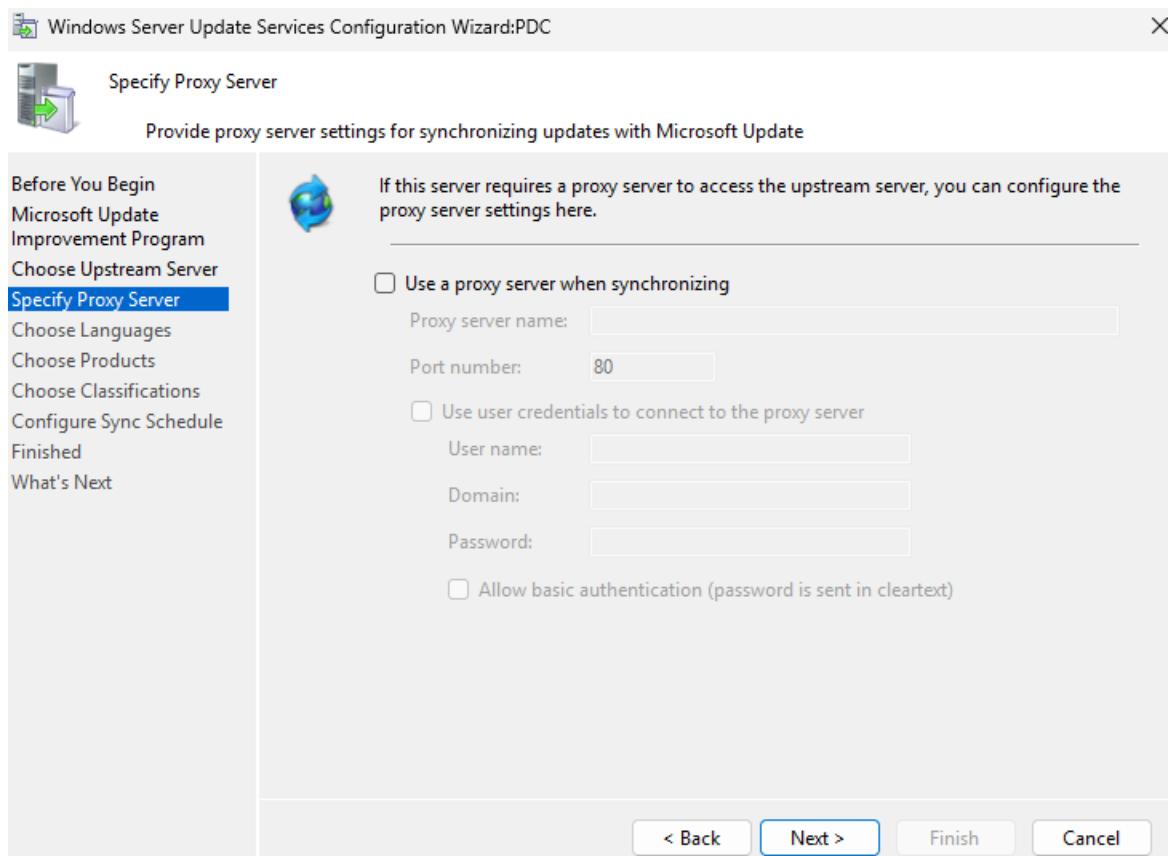


هنا MS بتسالك اذا كنت حابب تشارك معلومات عن ال updates ال انت بتستخدمها عشان يساعدوا في تحسين ال WSUS

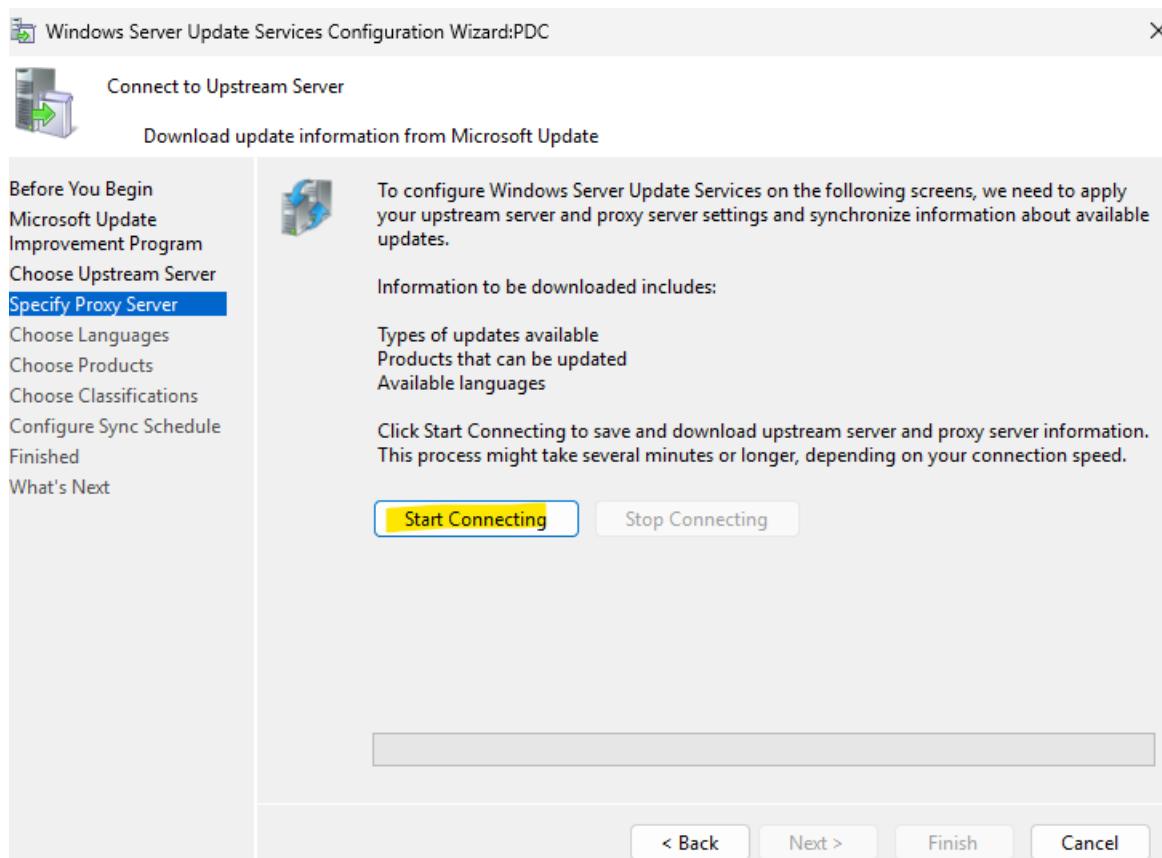


هنا بتشفو انت عاوز ال WSUS Server دا يعمل connect مع Microsoft Update مباشر ويجب منه ال Microsoft Update connect على WSUS Server تاني غير update ولا هتخليه يعمل

--

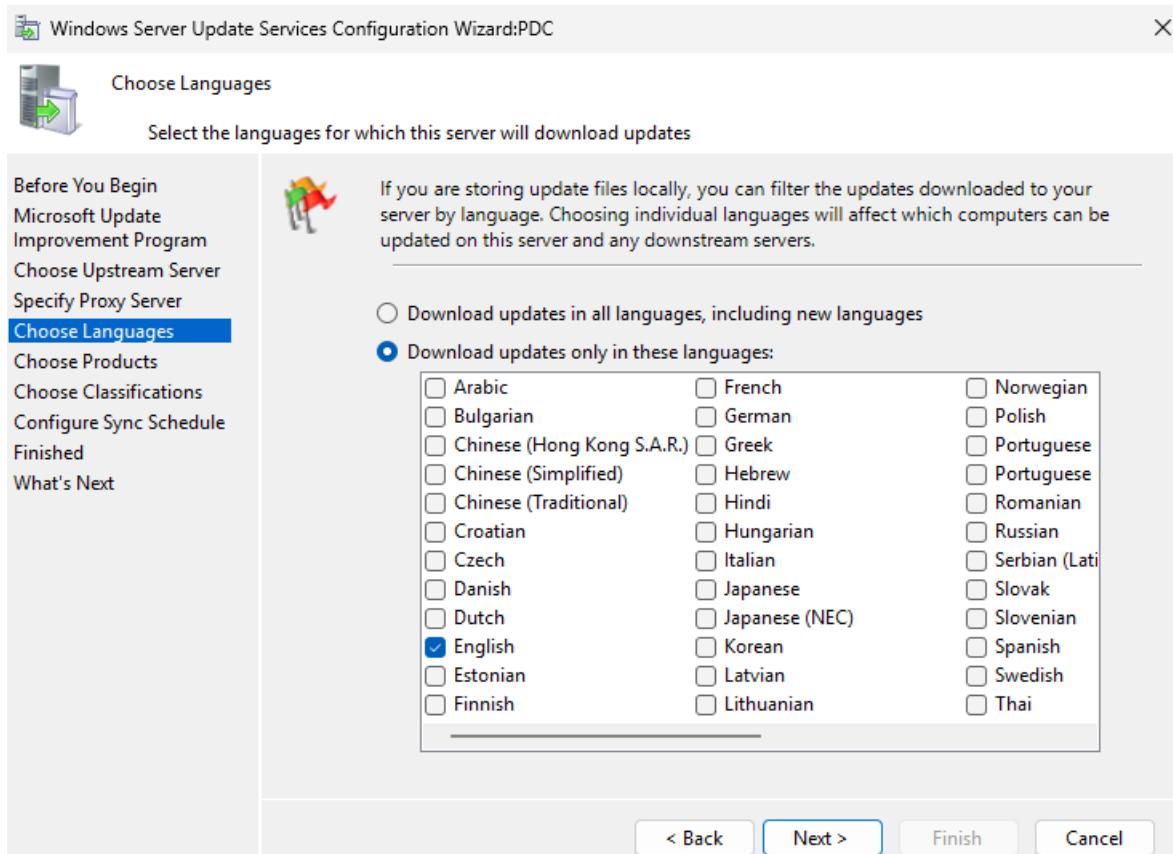


هنا لو انت عندك proxy server بتستخدمه هتعمل connect عليه بال credentials بتاعتك

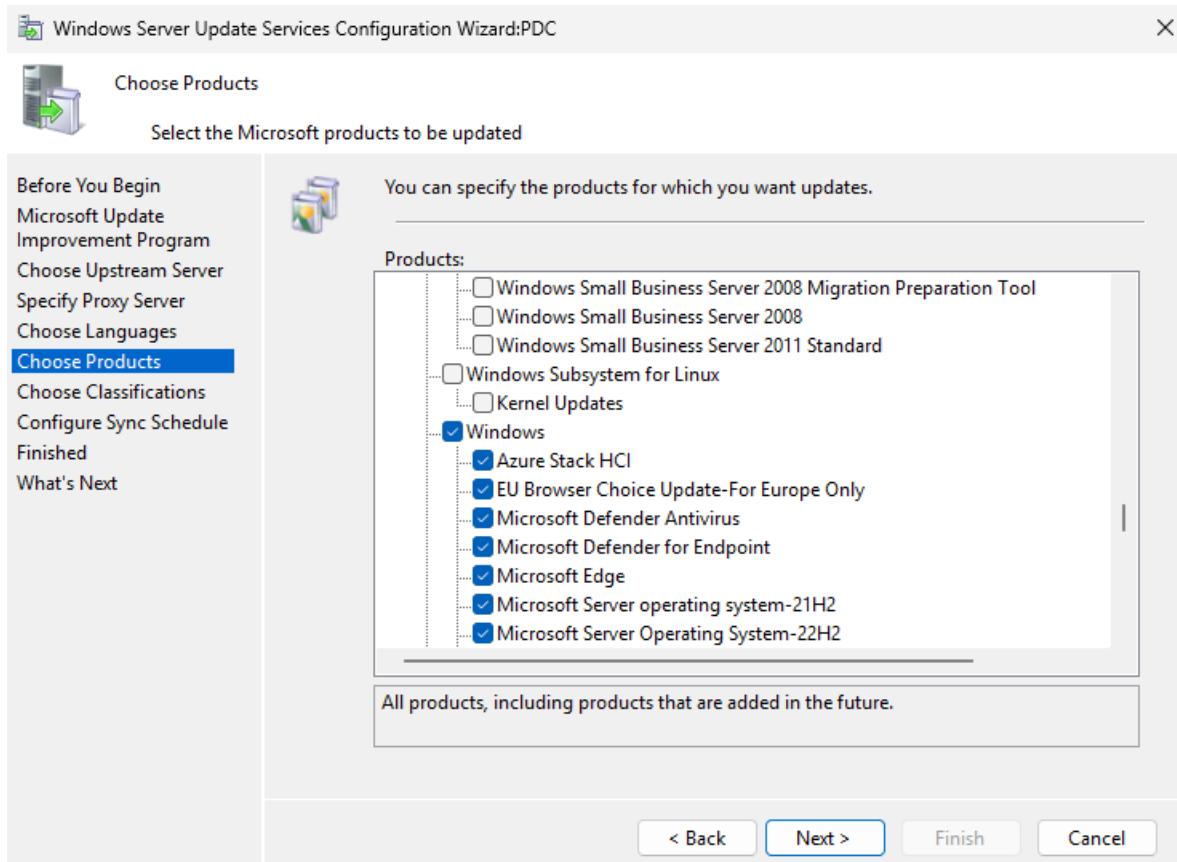


هنا هعمل start connecting وهذا مش هعمل download لـ update هو هنا هينزل معلومات عن ال updates المتاحة

--

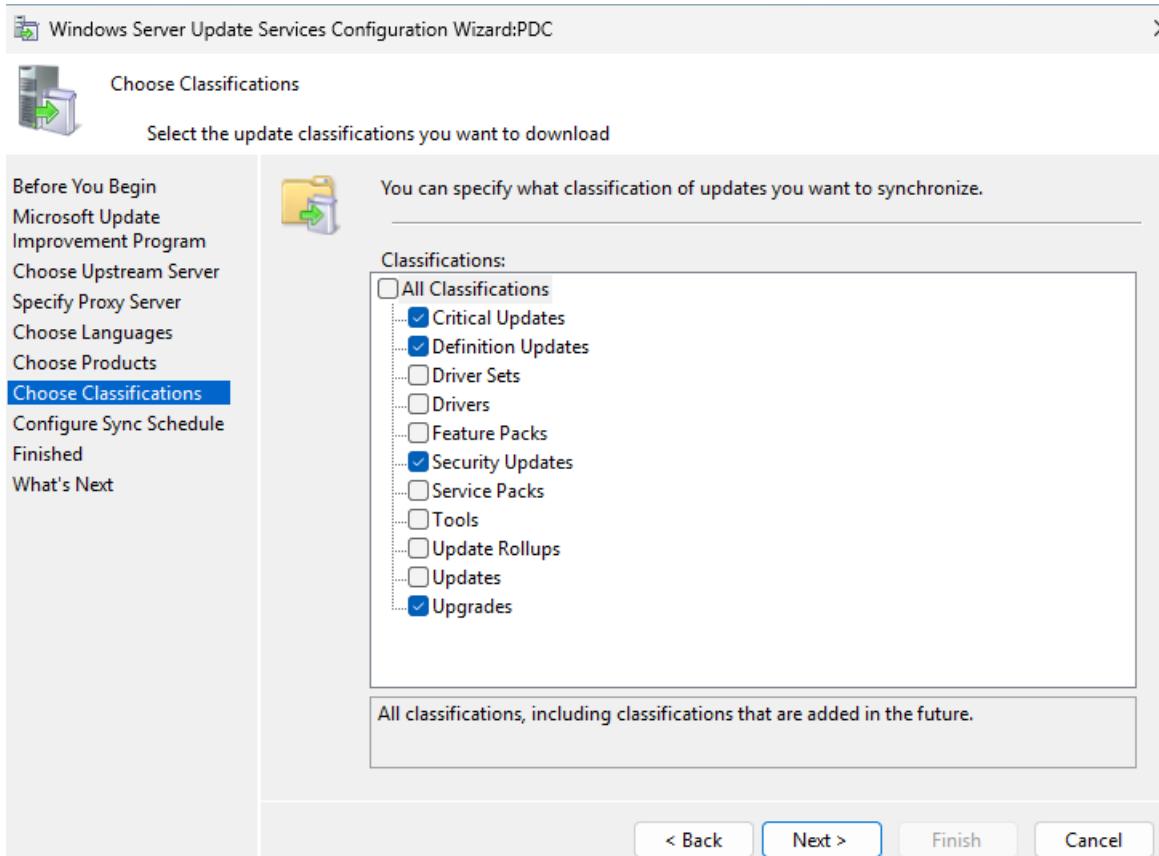


هذا يتحدد ال update بناء على Language



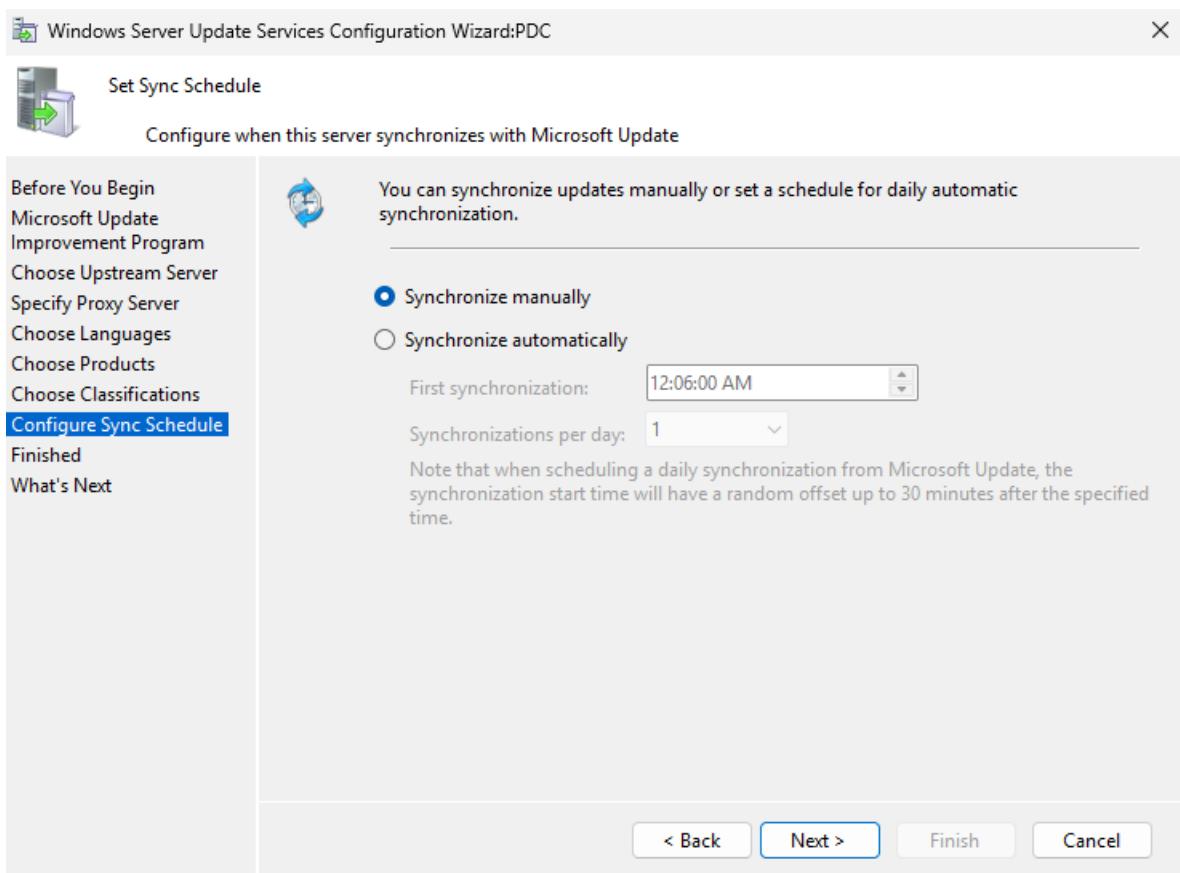
هذا يحدد الـ Product ليكون لا ي

--



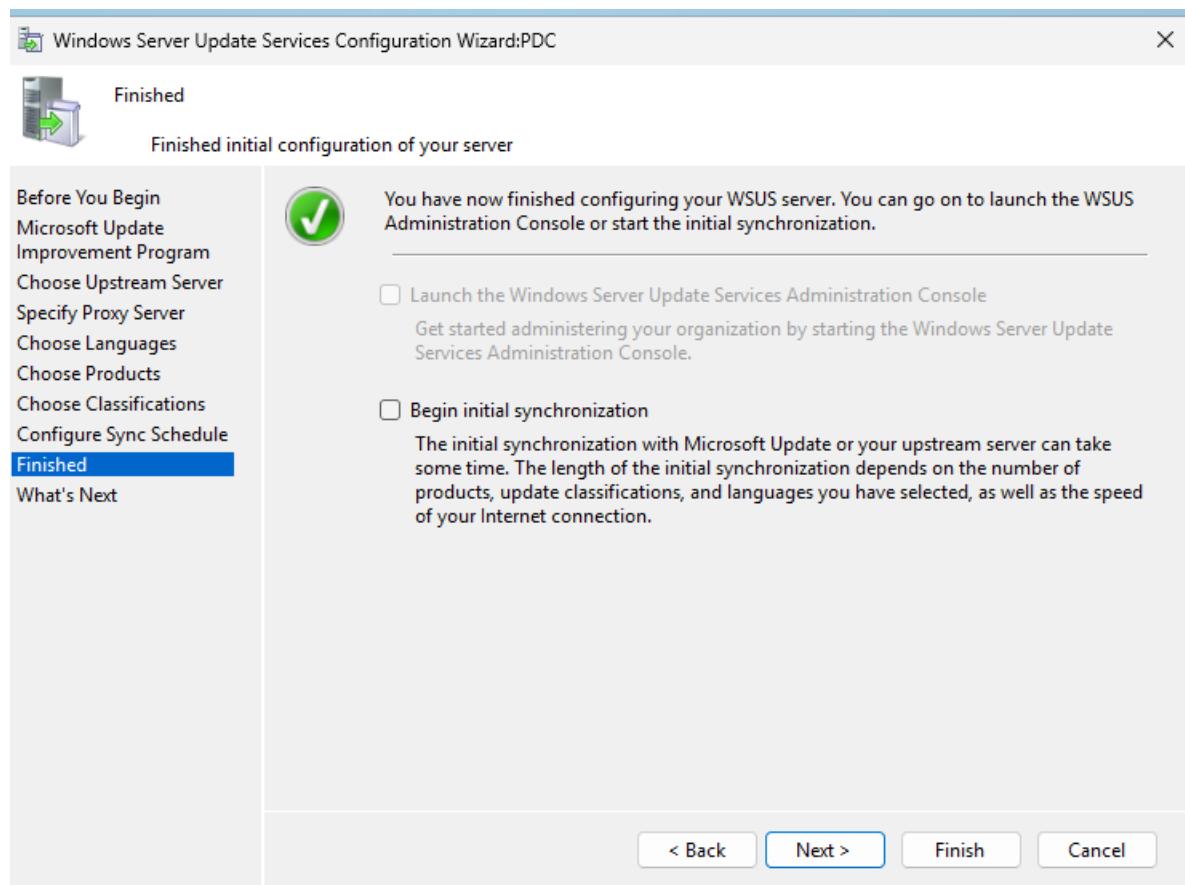
هذا يتحدد ال classifications يعني عاوز مثلا Critical Updates و Security Updates وهكذا

--

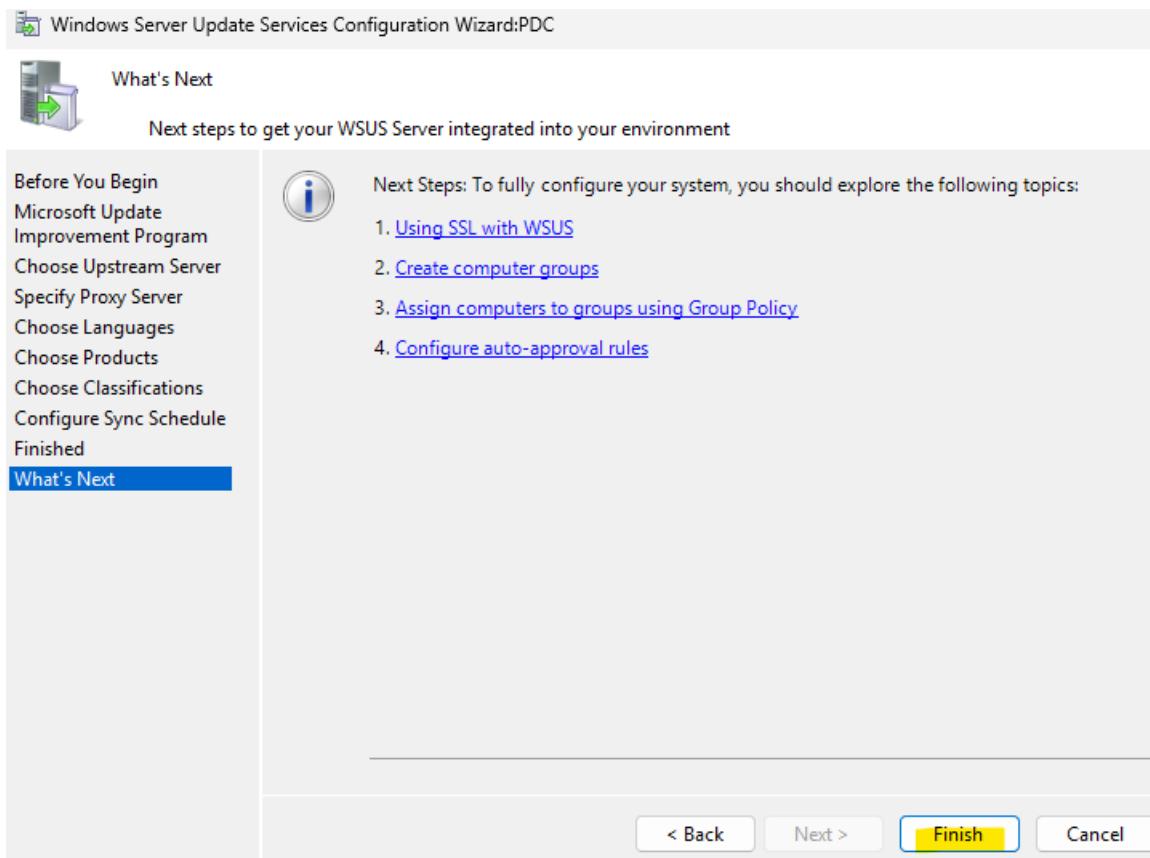


هنا بحدد امتي ال WSUS Server يروح يعمل sync مع MS update عشان يدور علي ال Updates الجديد

--

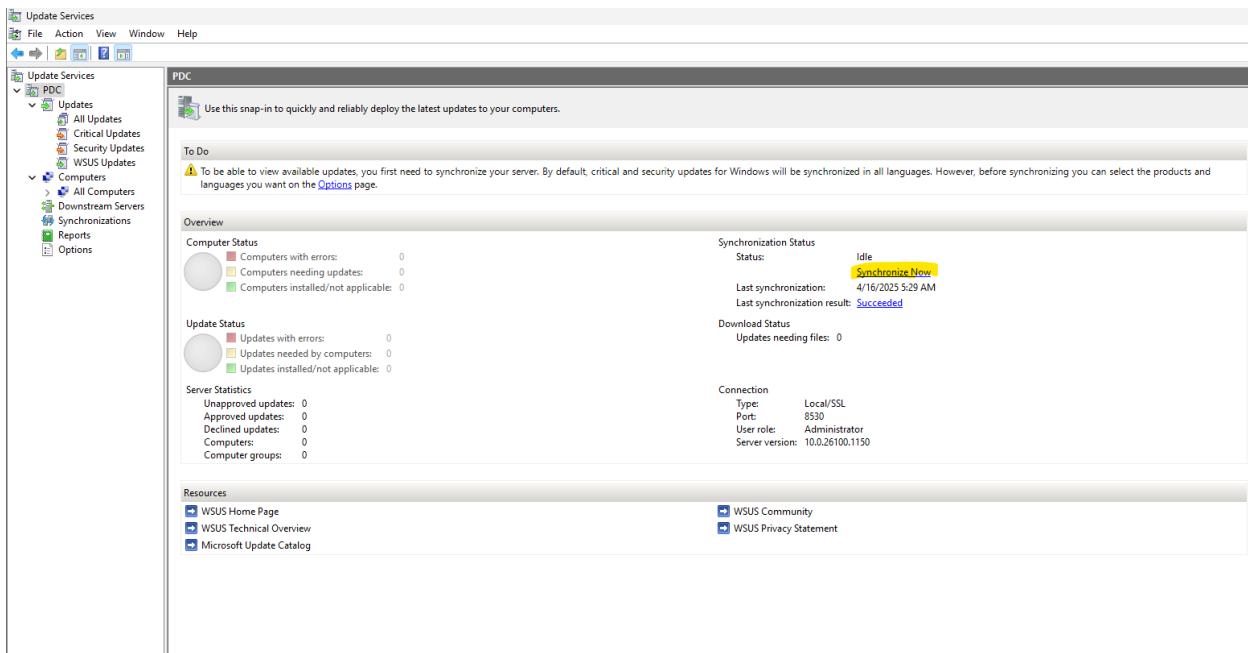


هنا ببسالني هتعمل sync دلوقت ولا من ال console فيما بع --



Finish

--

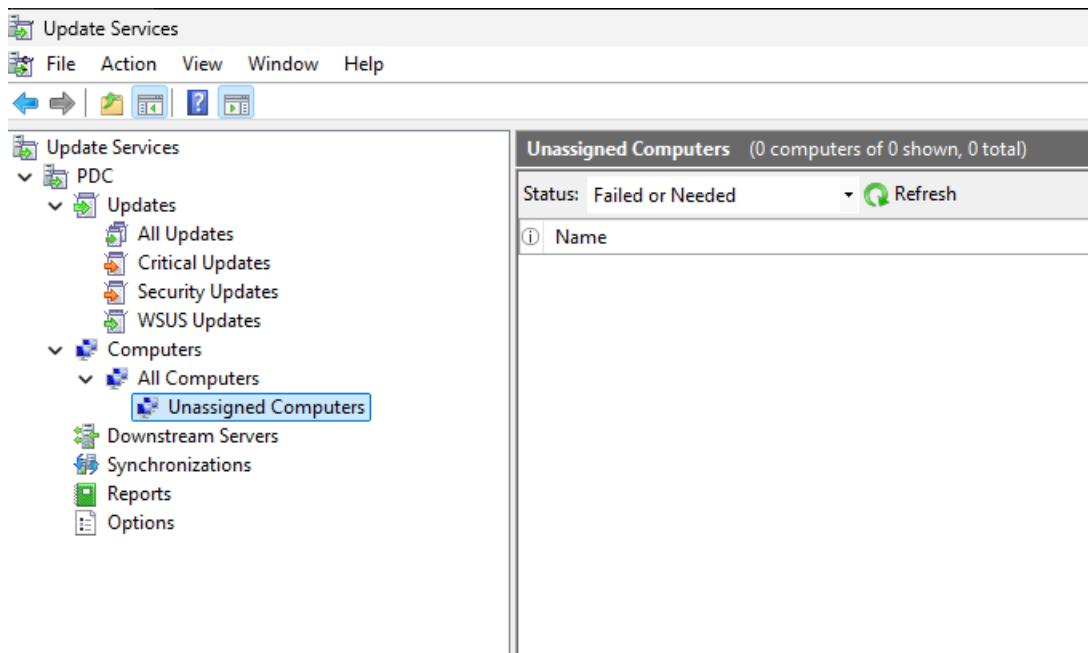


بعد كدا تقدر تعمل sync او تشوف ال critical update او security update و هكذا
وموضحي انه شغال ع port 8530

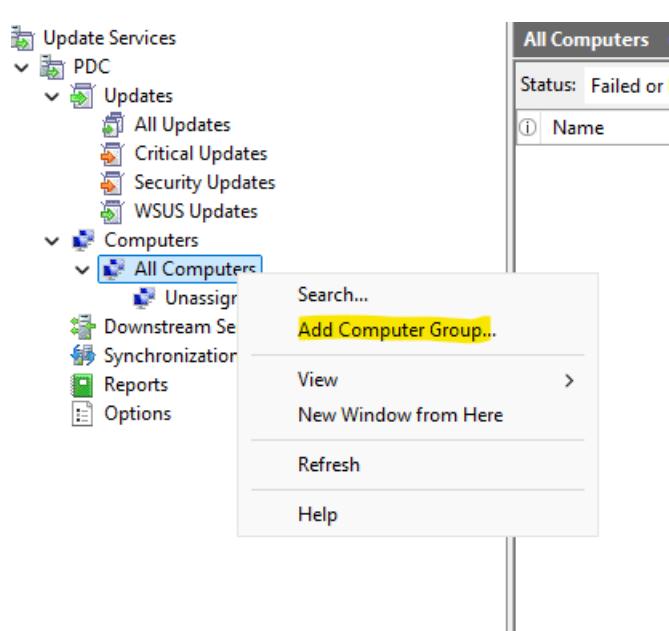
--
Synchronization Status
 Status: Synchronizing: 0%
[Stop Synchronization](#)
 Last synchronization: 4/16/2025 5:29 AM
 Last synchronization result: Succeeded
Download Status
 Updates needing files: 0

هنا بذات اعمل sync عشان يبدي معلومات ال updates المتاحه

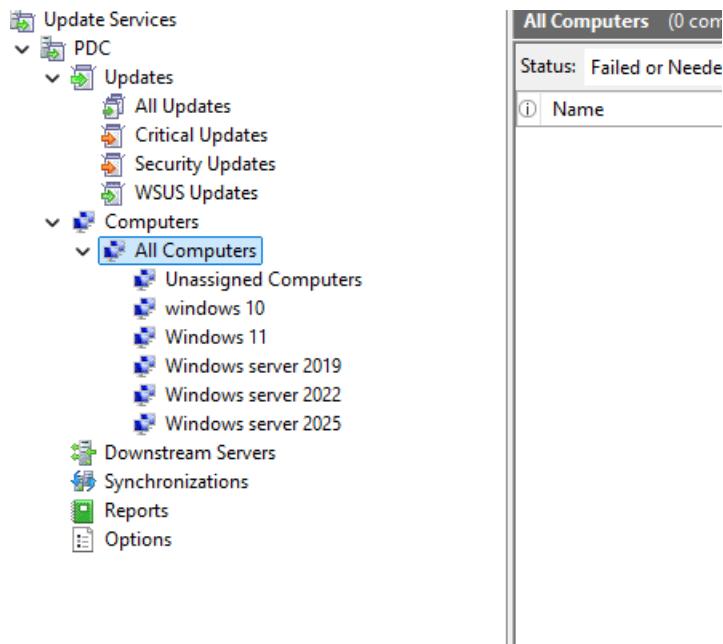
--



هذا سيتم تسجيل ال PCs ال بتسحب ال update من ال WSUS Server والافضل انك تقسمها groups



Click على Add Computer group واختار All Computers

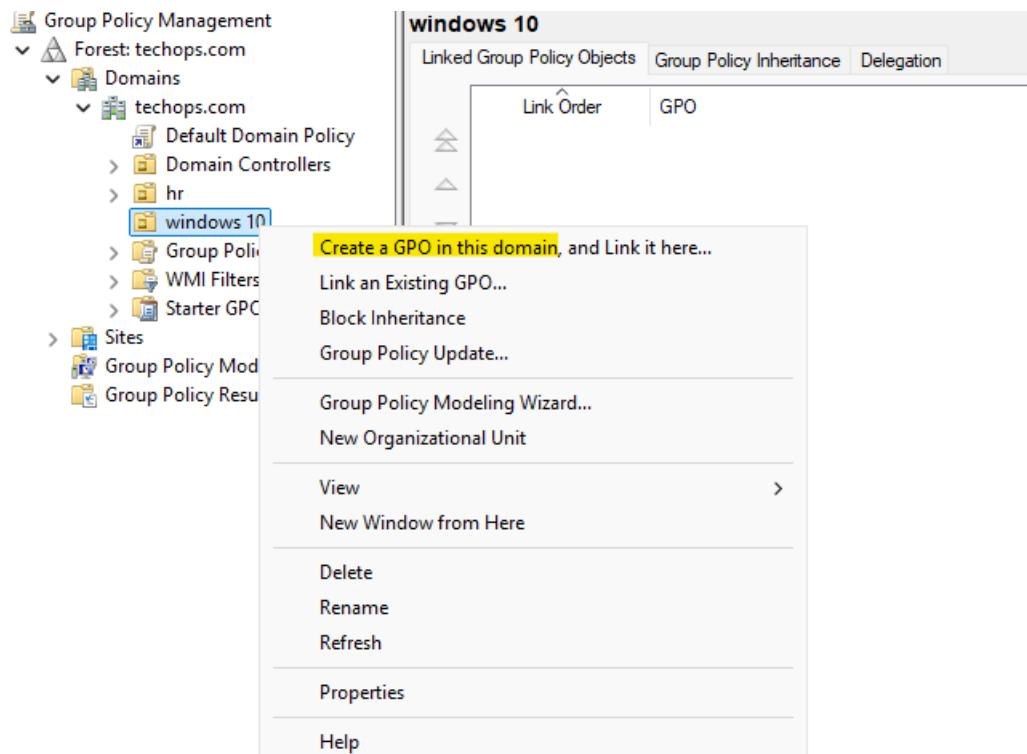


ه تكون بالشكل دا بحيث يكون من السهل عليك ان لو فيه update وعاوز تنزلها على win10 يعني تختار ال group ال اسمها windows 10

--

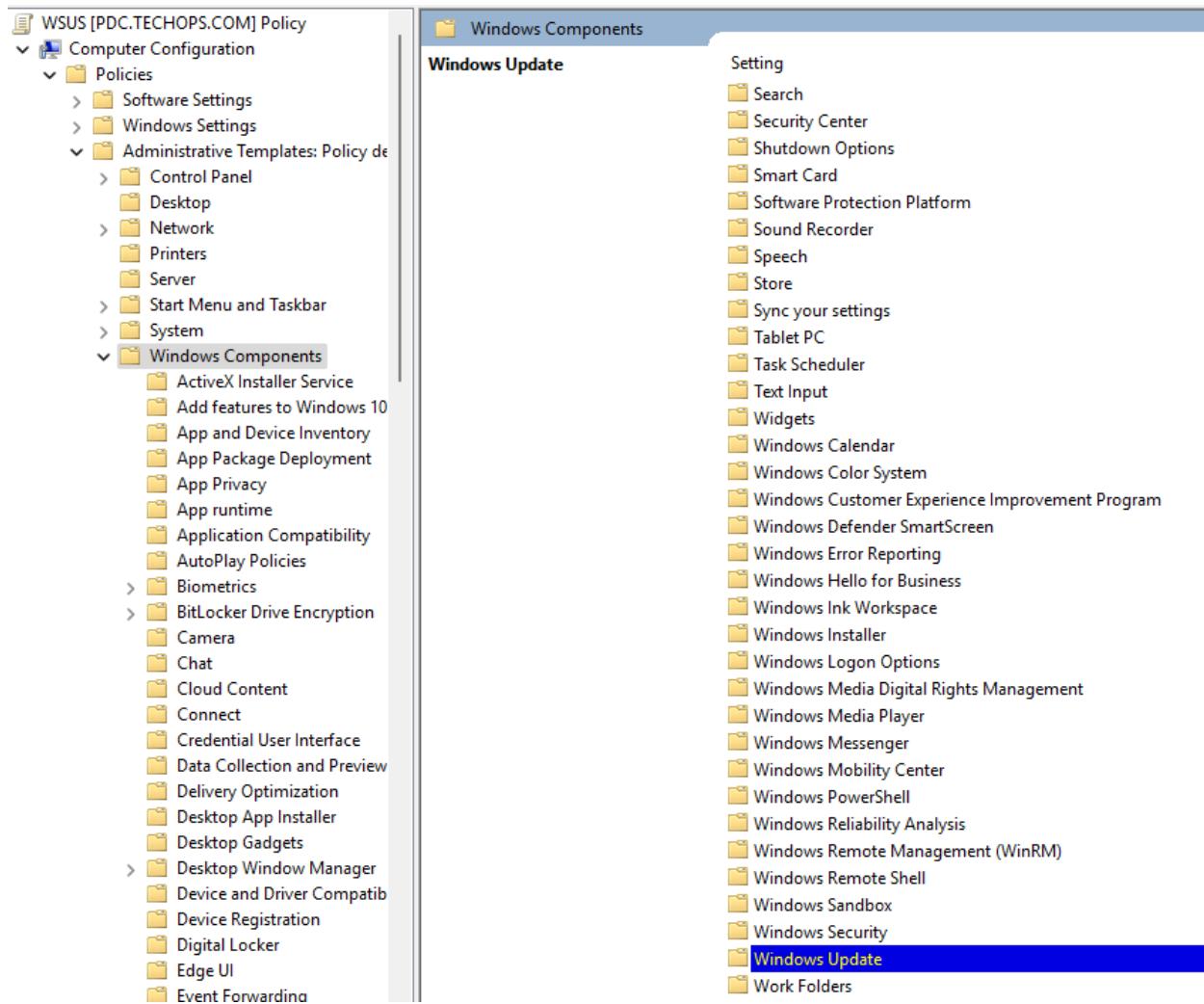
طيب ازاي ابدا اخلي ال PCs تسحب ال update

ممكن من خلال Group policy



علي ال OU ال عاوز اطبق عليها ال GP هعمل Create GP

--



هتعمل لـ GP edit

تحت ال administrative templates هندخل في ال Computer Configuration

تحتها هندخل في ال Windows Components

تحتها هنلاقي Windows Update

--

Manage updates offered from Windows Server Update Service			
Setting	State	Comment	
Specify intranet Microsoft update service location	Not configured	No	
Automatic Updates detection frequency	Not configured	No	
Do not connect to any Windows Update Internet locations	Not configured	No	
Enable client-side targeting	Not configured	No	
Allow signed updates from an intranet Microsoft update ser...	Not configured	No	
Specify source service for specific classes of Windows Updat...	Not configured	No	

تحت ال manage update offered from windows serve update service هندخل في windows update

هنعمل specify internet Microsoft update service location في edit

--

Specify intranet Microsoft update service location

Specify intranet Microsoft update service location

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled Supported on: At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excl

Options:

Set the intranet update service for detecting updates:

Set the intranet statistics server:

Set the alternate download server:

(example: https://IntranetUpd01)

Download files with no Url in the metadata if alternate download server is set.

Do not enforce TLS certificate pinning for Windows Update client for detecting updates.

Select the proxy behavior for Windows Update client for detecting updates:

Only use system proxy for detecting updates (default)

بتعميلها enable ويتحدد WSUS Server وال port بتاعه ، وتقدر لو عندك WSUS Server تاني تكتبه في ال alternate Server

Manage end user experience

Configure Automatic Updates

Edit [policy setting](#)

Requirements:
Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3 Option 7 only supported on servers of at least Windows Server 2016 edition

Description:
Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply

Setting	State	Comment
Turn off auto-restart for updates during active hours	Not configured	No
Specify active hours range for auto-restarts	Not configured	No
Allow updates to be downloaded automatically over metere...	Not configured	No
Enable features introduced via servicing that are off by default	Not configured	No
Configure Automatic Updates	Not configured	No
Specify deadline for automatic updates and restarts for qual...	Not configured	No
Specify deadline for automatic updates and restarts for feat...	Not configured	No
Remove access to "Pause updates" feature	Not configured	No
Remove access to use all Windows Update features	Not configured	No
Update Power Policy for Cart Restarts	Not configured	No
Display options for update notifications	Not configured	No

بعد كدا تحت ال manage and user experience هندخل في windows update ومنها هنعمل في edit

Configure Automatic Updates

Configure Automatic Updates

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on:

Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3 Option 7 only supported on servers of at least Windows Server 2016 edition

Options:

Configure automatic updating:

The following settings are only relevant if automatic updating is enabled:

Install during automatic maintenance

Scheduled install day:

Scheduled install time:

2 - Notify for download and auto install

3 - Auto download and notify for install

4 - Auto download and schedule the install

5 - Allow local admin to choose setting

7 - Auto Download, Notify to install, Notify to Restart

عملها واحد بقا enable

هنا الجهاز هيبيه ال user انه فيه update متاح بس مش هيحصله update الا لو ال user عمل عمل download لل update بتاع ال download هيحصل auto

هنا لو فيه update هيحصلها download مباشره دون موافقه ال user ، لما يحصل ال download هيصال ال user عوز تعمل install امتي

هنا لو فيه update هيحصلها download مباشره دون موافقه : Auto download and schedule the install ال user ، لما يحصل ال download ال install هيتم في الوقت ال انا احده

config : هنا بخلي ال pc بتاع ال local admin يقدر يعمل edit لـ setting بتاع ال update من خلال ال setting بتاع ال pc

هنا لو فيه update هيحصلها download مباشره Auto Download, Notify to install, Notify to Restart دون موافقه ال user ، لما يحصل ال download هيسال ال user عوز تعمل install امتي وال restart امتي

ف انا هنختار Auto download and notify for install

Manage updates offered from Windows Server Update Service			
Select an item to view its description.	Setting	State	Comment
	Specify intranet Microsoft update service location	Enabled	No
	Automatic Updates detection frequency	Not configured	No
	Do not connect to any Windows Update Internet locations	Not configured	No
	Enable client-side targeting	Not configured	No
	Allow signed updates from an intranet Microsoft update ser...	Not configured	No
	Specify source service for specific classes of Windows Updat...	Not configured	No

تحت ال manage update offered from windows serve update service windows update هندخل في automatic update detection frequency هنعمل في edit

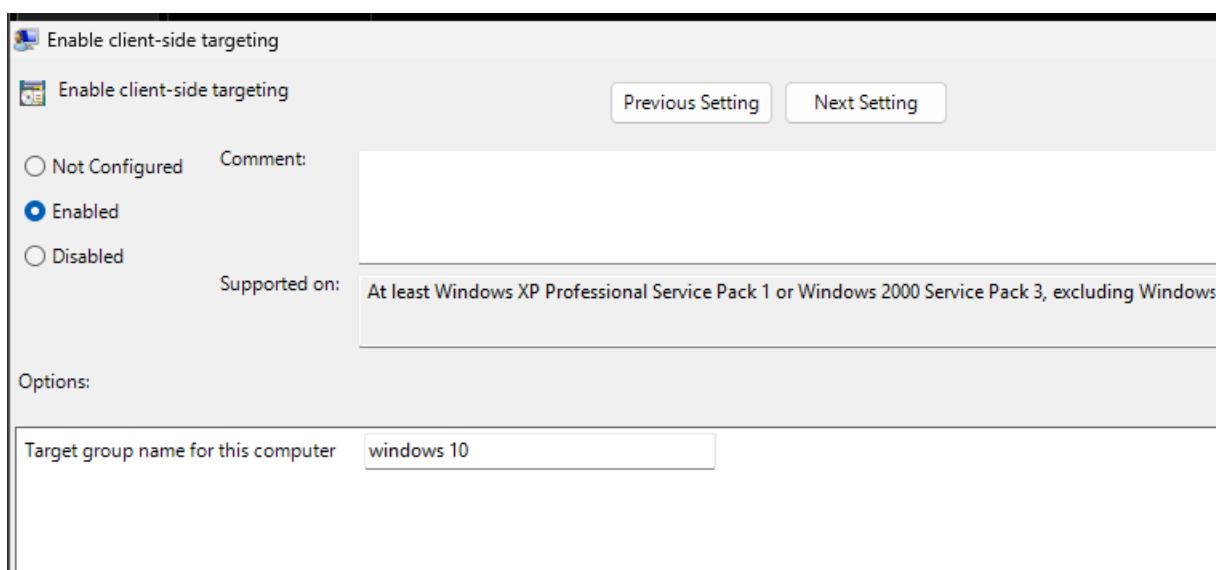
The screenshot shows the 'Automatic Updates detection frequency' policy settings. The 'Enabled' radio button is selected. The 'Supported on:' field indicates 'At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT'. In the 'Options:' section, the 'Check for updates at the following interval (hours)' dropdown is set to 96. A detailed help text is visible on the right side of the screen, explaining the policy's behavior based on the status (Enabled, Not Configured, or Disabled).

من المفترض ان client بيروح ل WSUS Server كل 22 ساعه يشوف فيه update ولا لا واقدر اعدل الوقت دا

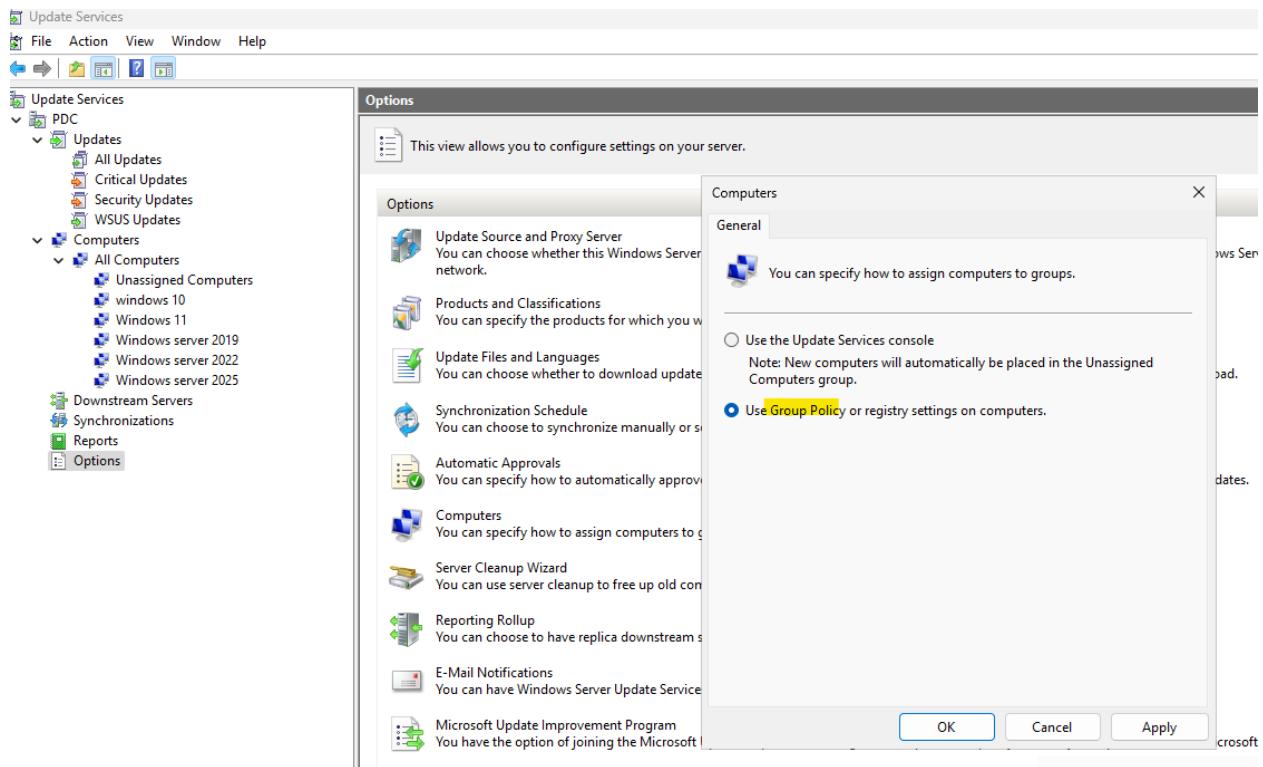
Setting	State	Comment
Specify intranet Microsoft update service location	Enabled	No
Automatic Updates detection frequency	Not configured	No
Do not connect to any Windows Update Internet locations	Not configured	No
Enable client-side targeting	Not configured	No
Allow signed updates from an intranet Microsoft update ser...	Not configured	No
Specify source service for specific classes of Windows Updat...	Not configured	No

تحت ال manage update offered from windows serve update service هندخل في windows update

هنعمل edit في Enable client-side targeting



هنا حدد ال group policy ال هتنزل فيه الاجهزه ال هيطبق عليها ال دا



واخير هروح علي ال WSUS Server وفي ال option computers ومنها هقوله ان الاجهزه بتعتني هتسمع عن طريق ال Group policy

طيب عاوزين نجرب نعمل update ل download

Update Services

File Action View Window Help

Update Services

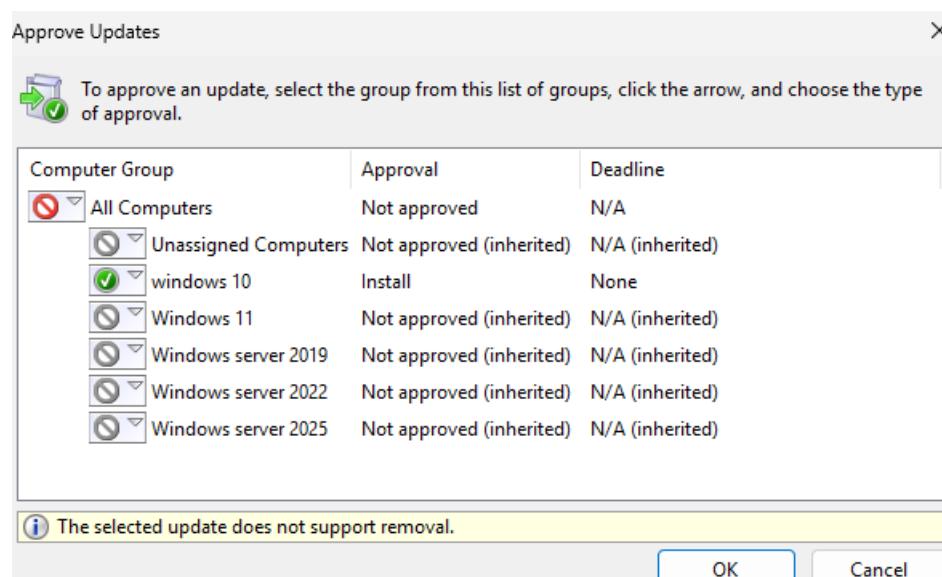
- PDC
- Updates
 - All Updates
 - Critical Updates
 - Security Updates
 - WSUS Updates
- Computers
 - All Computers
 - Unassigned Computers
 - windows 10
 - Windows 11
 - Windows server 2019
 - Windows server 2022
 - Windows server 2025
- Downstream Servers
- Synchronizations
- Reports
- Options

All Updates (59 updates of 59 shown, 59 total)

Approval: Unapproved Status: Any Refresh

Title	Actions
Windows XP Update Package, October 25, 2001	
814033: Critical Update	
Q329441: Critical Update	<ul style="list-style-type: none"> Approve... Decline Group By > Revision History File Information Status Report Help
814078: Security Update (Micro	
Q815487: Critical update for W	
Security Update for Windows X	
814078: Security Update (Micro	
Q811632: Critical Update (Wind	
810833: Security Update (Wind	
811493: Security Update (Wind	
813951: Update for Internet Explor	
814078: Security Update (Microsoft Jscript version 5.1, Windows 2000)	

علي ال update ال انا محتاجه click و هعمل approve

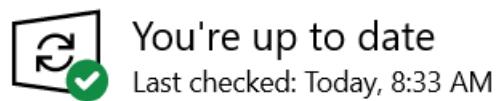


ببسالني عاوز تعمل ال update دا علي انهر group

windows 10 (1 computers of 1 shown, 1 total)				
Status:	Any	Refresh		
Name	IP Address	Operating System	Installed/Not Applicable	Last Status Report
desktop-ufu1f2g.techops.com	192.168.1.77	Windows 10 Pro	100%	4/16/2025 8:31 AM

بعد ما ال update يروح لـ client ال بينظهر معايا في ال group ال انا عملتها وحددها

--



You're up to date

Last checked: Today, 8:33 AM

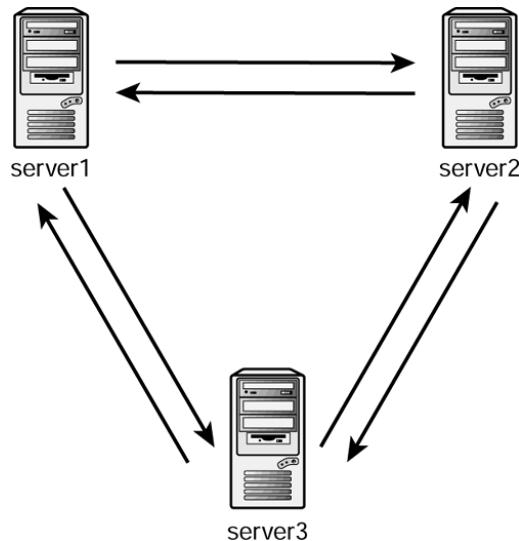
[Check for updates](#)

[Check online for updates from Microsoft Update](#)

وعلي ال client هنلاقي ال update اتسحب

Intra-Site Replication

هي عملية يتم من خلالها مزامنة التغييرات في قاعدة بيانات ال Active Directory بين جميع الموجوين داخل نفس ال site الموجوبين Domain Controllers



يتم استخدام بروتوكول يسمى RPC over IP

ال replication يكون تقريبا كل 15 ثانية

هو multi master replication يعني ان اي تعديل في اي server يسمع في كل ال DC

: يعني ال DC بينماك ان ال DB اكتسبت عند ال DC الثاني Accuracy

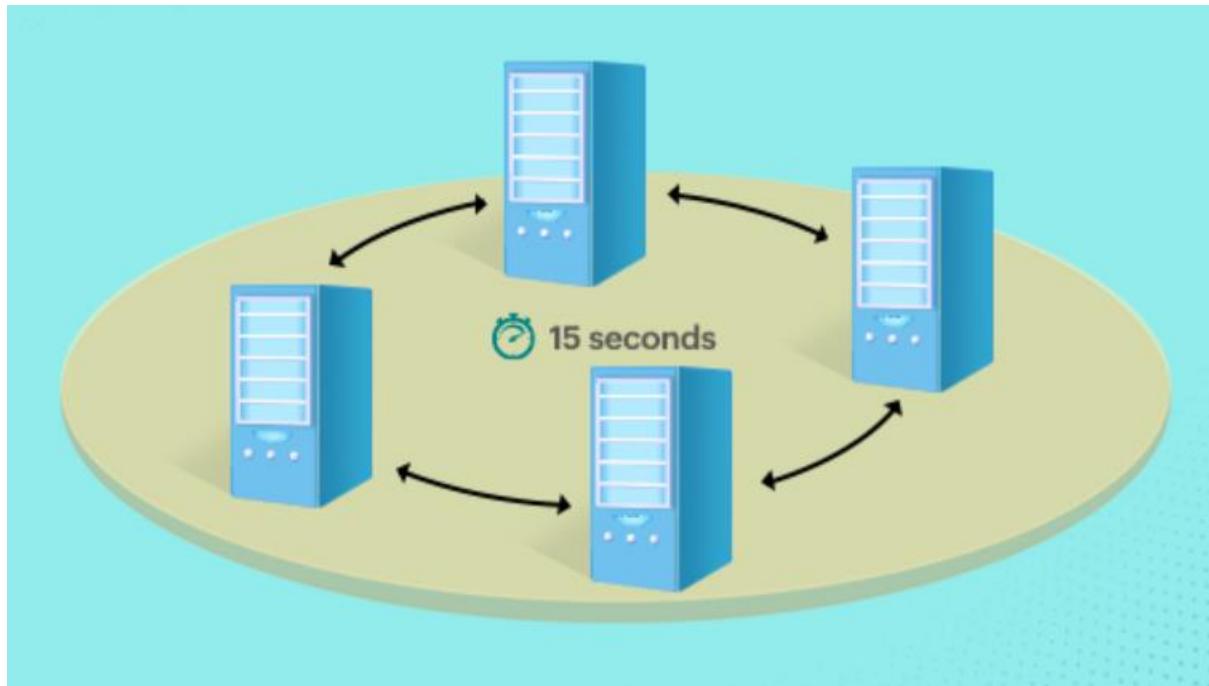
ال replication يتم بطريقه ال notification يعني ان ال DC اعلم بالتعديل بمجرد حدوثه

DC الثاني وبالتالي ال replication يتم بطريقه ال Pull يعني ان ال DC يحيط بمعلومات ال DC الثاني

الثاني انه تم تعديل تم في ال DC الثاني هو ال يروح يسحب التعديلات دي

DC1,DC2,DC3,DC4,DC5 ف DC بمعنى اني لو عندي اكتر من DC وليكن DC1 هيحصل ان DC1 هيبعد DC2 يروح يسحب التعديلات من DC1 وبعد كذا يبعد DC3 يسحب التعديلات من DC2 وهكذا

ال notify تكون بعد 15 ثانية من التعديل ولكن لو عندي اكتر من DC ف الاول هيكون بعد 15 ثانية وبعد كذا تزود 3 ثواني يعني ال DC الثاني بعد 18 ثانية وهكذا



replication يتم على مستوى ال Attribute-level and multi value replication object تم التعديل عليها فقط داخل ال attributes

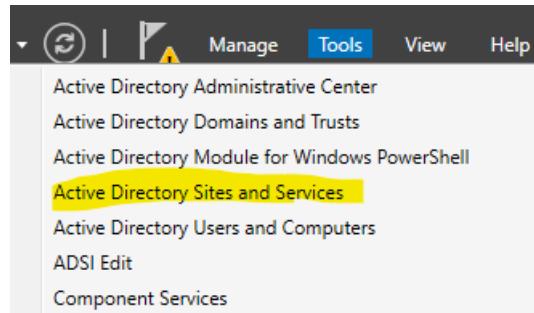
يتم تحديد مسارات ال replication باستخدام Knowledge Consistency Checker

ال KCC يقوم بإنشاء ring topology لضمان وصول كل ال DC إلى جميع التغييرات

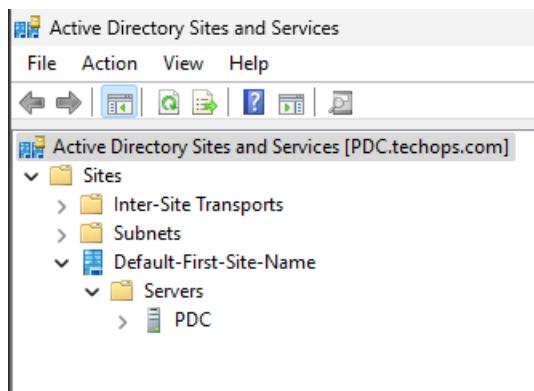
يبقى ال KCC هي المسئوله عن بناء ال Replication وبتخلي ال DC يعرف ال DCs الثانية ال معه في نفس ال Site

--

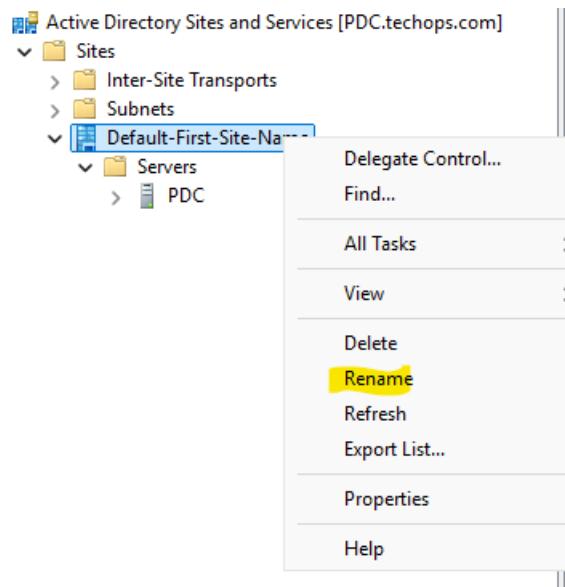
طيب از اي اعمل مثلا site rename لل site او اضيف site جديد ؟



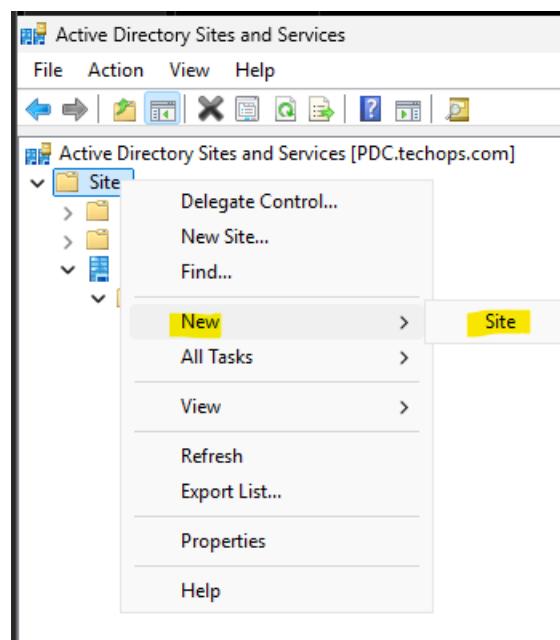
هنروح علي tools ونختار AD Sites and Services



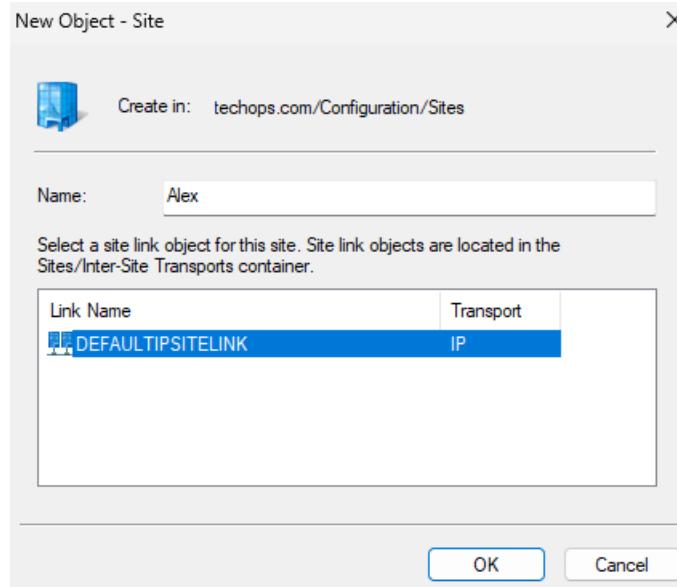
هتفتح بالشكل دا هيكون عندك ال default site وتحته ال DCs الموجوده وفي حالي مش عندي غير ال PDC



عشن اعمل change لـ site name واختار name على ال click

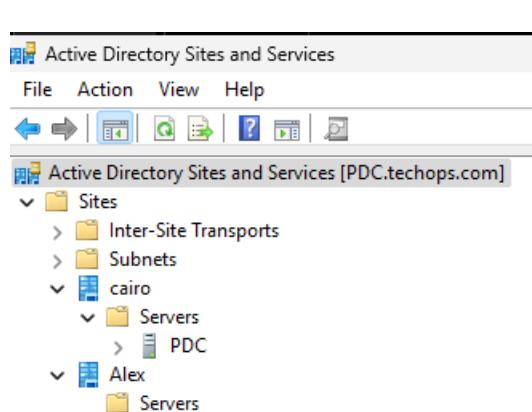


عشن اضيف site جديد على site click



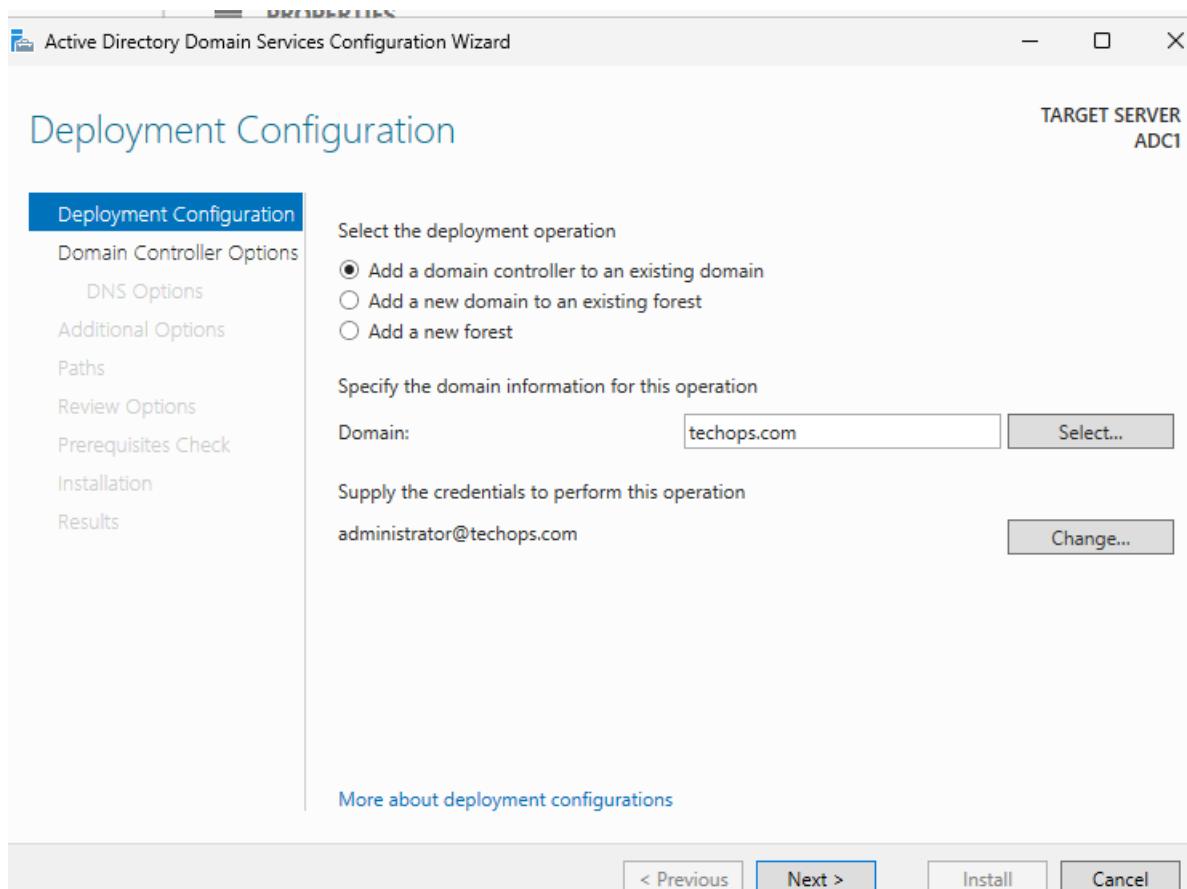
اكتب ال site name ال عاوزه وبعد كدا بختار ال link object وقدر اعمل اكتر من site link object هو اي ال link object دا طيب هو اي ال AD دا داخل ال AD يستخدم لربط لكثير من sites من خلال ما يعرف بال site link ، يبقى ال site link بيتم بين ال sites ال موجوده في مواقع مختلفه

طيب اي هو ال site link ؟ دا ال بيحدد طريقه ال connection بين ال sites وبعضها replication – تحديد افضل واسرع مسار لل replication schedule : هو site link يتم انشاءه تقائيا عند اضافه اكتر من site ودا بيستخدم في ال Inter site يعني ال replication بين المواقع المختلفه



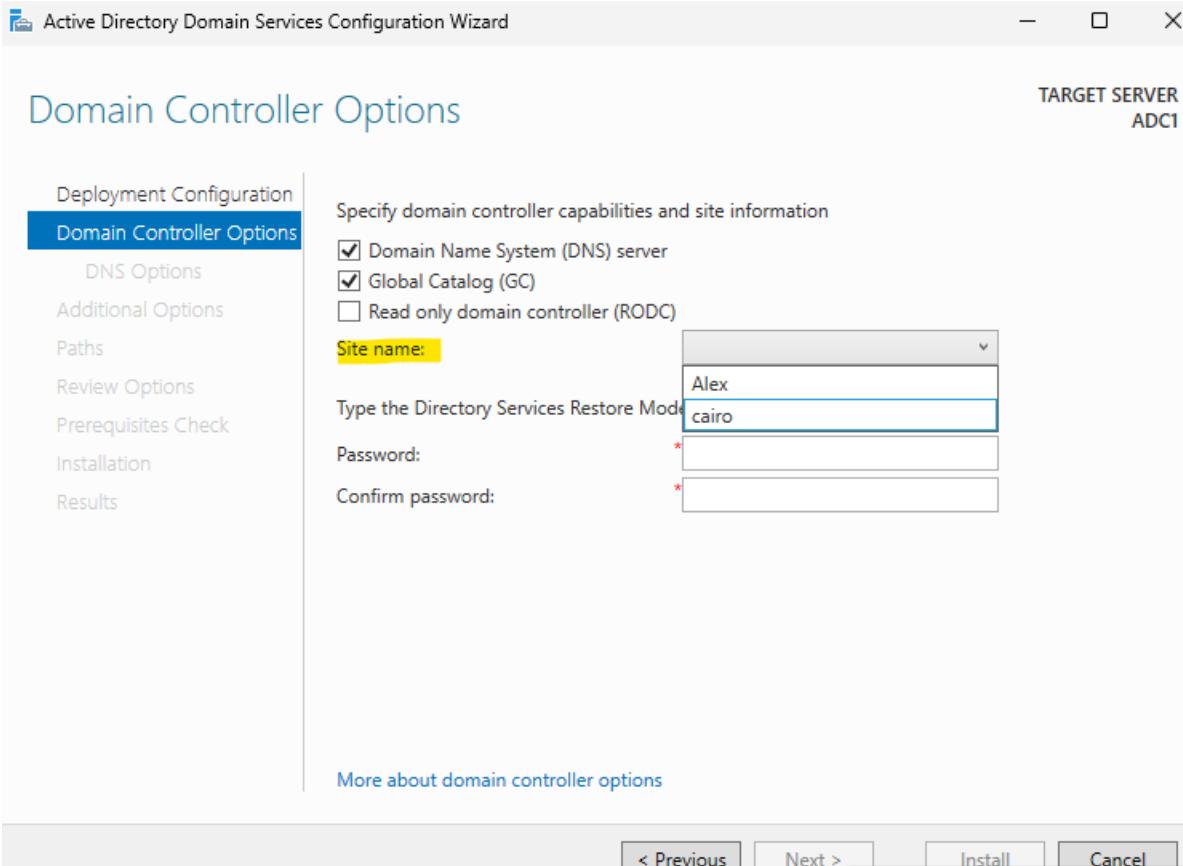
كدا بقى عندي Cairo – Alex 2 site وهما

دلوقت عاوزين نعمل ADC ويكون في ال site الاول مع ال PDC ال هو Cario ؟



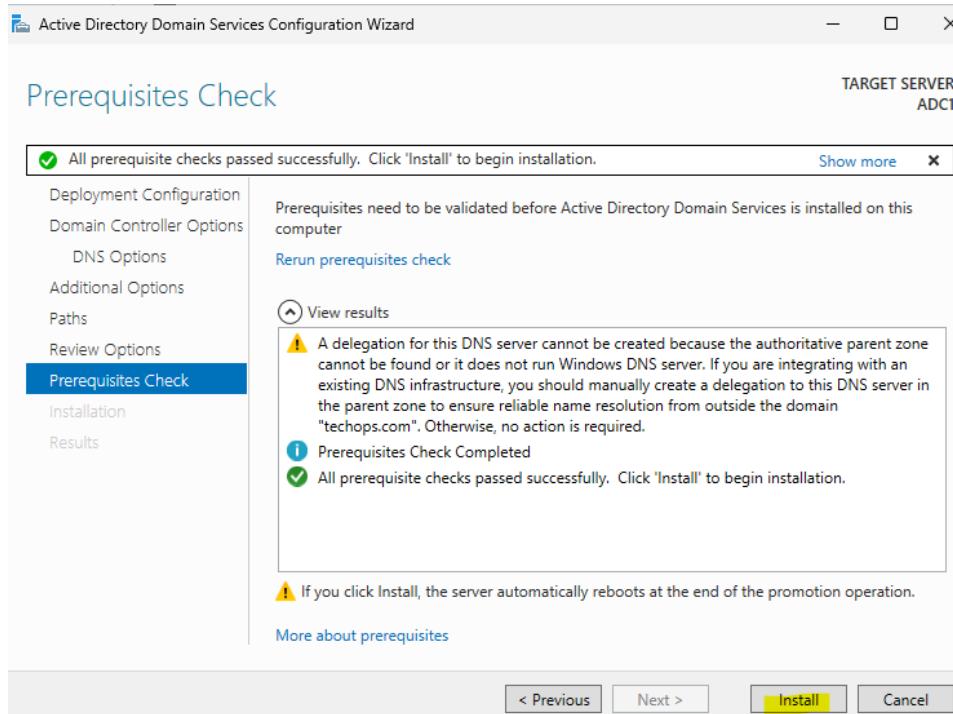
بنفس الطريقة ال اتعلمنها بعمل خطوات ال ADC
ختار هختار Add a dc to an existing domain واتكتب ال user بتاعي وال password

--

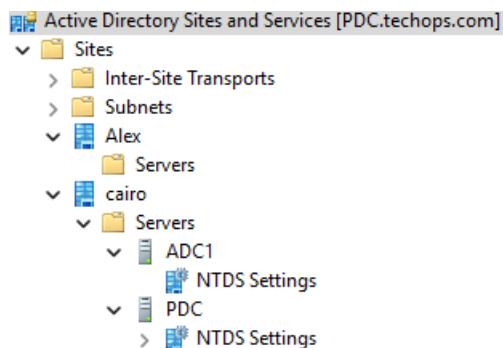


هنا بقى في ال site name بيقولي انت ال DC دا هتخليه في انهي ؟

--



بعد كدا نكمل باقي الخطوات ونعمل Install



بعد ال install لما تروح علي ال sites هتلقي ان ال ADC1 نزل في ال site ال احنا اخترناه وبقى عندي كذا replication site فيه PDC و ADC1 يبقى الاثنين في نفس ال site يبقى ال هتم بينهم ف 15 ثانية

طیب لو عاوزین نشوف ال replication partitions ال حصلها ؟

```
PS C:\Users\Administrator> repadmin /showrepl

Repadmin: running command /showrepl against full DC localhost
cairo\PDC
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: c6a59373-7c15-4d89-87c0-c7de2740096c
DSA invocationID: 932dfc7f-fd9d-41ab-a685-4fa76107d035

===== INBOUND NEIGHBORS =====

DC=techops,DC=com
    cairo\ADC1 via RPC
        DSA object GUID: 778594fc-78d7-460e-b98e-fe12f3a7749d
        Last attempt @ 2025-04-18 11:45:51 was successful.

CN=Configuration,DC=techops,DC=com
    cairo\ADC1 via RPC
        DSA object GUID: 778594fc-78d7-460e-b98e-fe12f3a7749d
        Last attempt @ 2025-04-18 11:49:18 was successful.

CN=Schema,CN=Configuration,DC=techops,DC=com
    cairo\ADC1 via RPC
        DSA object GUID: 778594fc-78d7-460e-b98e-fe12f3a7749d
        Last attempt @ 2025-04-18 11:45:51 was successful.

DC=DomainDnsZones,DC=techops,DC=com
    cairo\ADC1 via RPC
        DSA object GUID: 778594fc-78d7-460e-b98e-fe12f3a7749d
        Last attempt @ 2025-04-18 11:48:48 was successful.

DC=ForestDnsZones,DC=techops,DC=com
    cairo\ADC1 via RPC
        DSA object GUID: 778594fc-78d7-460e-b98e-fe12f3a7749d
        Last attempt @ 2025-04-18 11:48:48 was successful.

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

من ال powershell هكتب الامر دا : repadmin /showrepl

هنا ال 4 partitions حصلهم replication

اول partition ال هو من غير اسم دا ال domain partition

بعد كدا ال configuration partition

بعد كدا ال schema partition

وال application partition مقسم ل 2 واحد على مستوى ال domain وواحد على مستوى ال forest

وال application partition ظهر عشان انا وانا بعمل ال ADC اخترت اني اسطب ال DNS لو مكنتش سطبت ال DNS مكنش هيظهر لأن مكنش هيكون فيه اي application partition يستخدم ال replication وبتالي مكنش هيحصله replication لكن لما انا سطبت ال DNS عمل

--

طيب اي ال بيأثر علي ال replication ؟

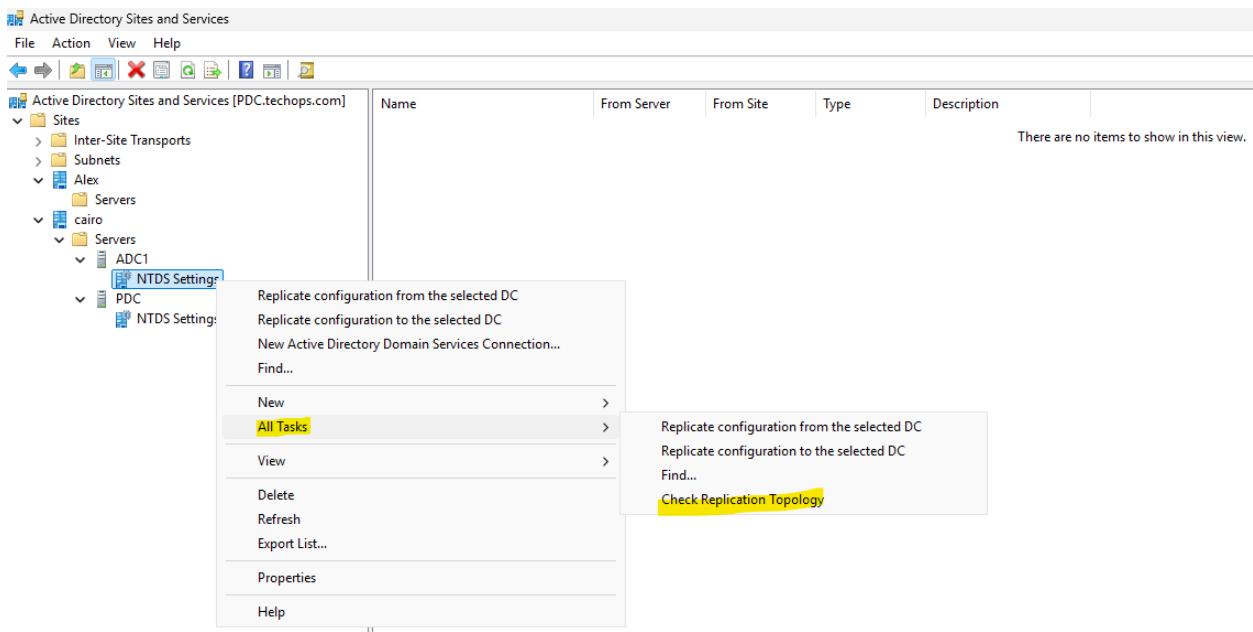
replication : دا بيمثل الاتصال الفعلي بين ال DCs بهدف عملية ال Connection object -1 يعني هو يقولي ان DC2 مثلًا بيأخذ replication من DC1 او العكس (يعني هو ال من خالله بتحصل عملية ال replication) ودا بيتم انشاءه بواسطه ال KCC

The screenshot shows the 'Active Directory Sites and Services' window for the 'PDC.techops.com' domain. On the left, the navigation pane displays the site structure: 'Sites' (Inter-Site Transports, Subnets), 'Alex' (Servers), and 'cairo' (Servers, ADC1, PDC). On the right, a table lists the 'Connection' objects:

Name	From Server	From Site	Type	Description
<automatically generated>	PDC	cairo	Connection	

هو دا ال connection تحت ال ADC1 في ال NTDS setting بنلاقى ال object وبيقولك ان ال ADC1 بيعمل replication من PDC نوع ال object دا connection

طيب لو لاي سبب ان ال connection دا اتحذف ؟



من هعمل all tasks ودي معنهااني بشغل ال service اسمه KCC وزي ما قولنا دي ال بتتنشي ال Connection object ف لما تشتعل هتنشي ال connection

--

ال tow-way one-way مش connection بتشتغل

ليه ؟ لان مثلا لما ال connection object اتحذف من ADC1 وروحت عملت عليه اي تعديل هيتم علي ال PDC لان ال connection بتاع ال PDC لسه شغال عادي

لكن لو عملت تعديل علي PDC مش هيسمع علي ال ADC1 ليه لان ال connection بتاع ADC1 اتحذف ومبقاش موجود

--

طيب لو افترضنا ال connection بين ال 2 DC موجود وكل DC عمل تعديل عكسي على نفس ال object لما ال connection يرجع انهي تعديل ال هيسمع ؟

آخر تعديل على ال object هو ال هيسمع ودا بسبب ال time stamp ودا تاريخ ووقت بيتم تسجيلهم مع كل تعديل يحصل على اي اي object داخل ال AD

وبالتالي لو PDC عمل تعديل الساعة 11

وال ADC1 عمل تعديل الساعة 11:30

ال AD بيروح لل time stamp يقارن بين التعديلات دي ويأخذ التعديل الحديث (آخر تعديل)

--

Failover Cluster

هو مجموعه من ال servers تعمل معا بغرض تحقيق مبدأ ال High Availability لـ servers وال services ، اذا توقف server عن العمل لاي سبب يقوم server اخر بالعمل بدلا منه بشكل تلقائي دون التاثير على الخدمة .

مكوناته :

- 1 : دي ال Nodes servers
- 2 : لازم يكون فيه shared storage بين ال servers عشان كلهم يكون عندهم نفس ال data
- 3 : دي رساله بتبعثها ال servers لبعض عشان يعرفوا انهم شغالين ولا في server توقف عن العمل
- 4 : دي الطريقة ال بيستخدمها ال failover cluster عشان يقرر مين ال يشغل ال Quorum او لو node down حصل مشكله في ال network cluster

يفضل يكون عندي اكتر من network card على ال server
domain Network card -1
storage Network card -2
(Heartbeat cluster) Network card -3

طیب ابدا اعمل ال Failover Cluster ازای؟

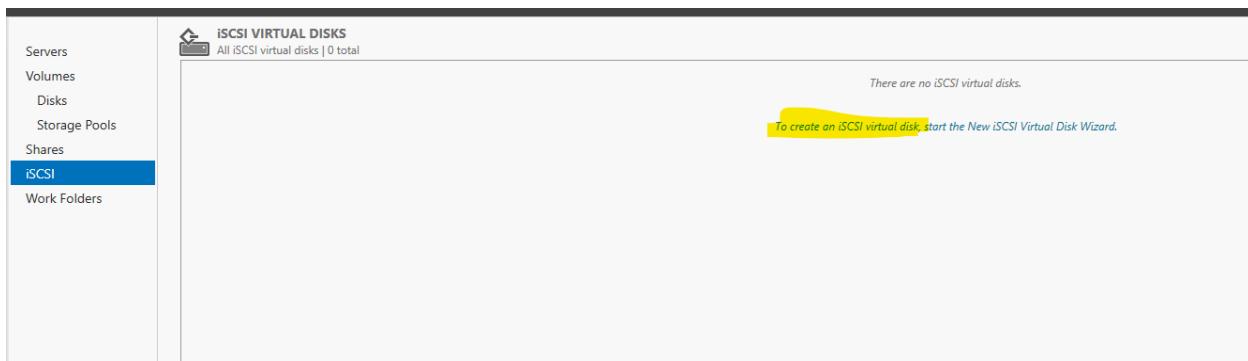
اول حاجه هبذا اظبط ال shared storage و هنستخدم ال iSCSI

The screenshot shows the Windows Server Manager interface. The left navigation pane is visible with items like Dashboard, Local Server (which is selected and highlighted in blue), All Servers, AD DS, DNS, File and Storage Services (which is also highlighted in yellow), and WDS. The right pane displays the 'PROPERTIES' for the 'Local Server'. It shows the computer name is 'PDC' and the domain is 'techops.com'. Under the 'File and Storage Services' section, it lists Microsoft Defender Firewall (Domain: On), Remote management (Enabled), Remote Desktop (Disabled), NIC Teaming (cluster), Domain (192.168.1.100, IPv6 enabled), and storage (192.168.2.100, IPv6 enabled).

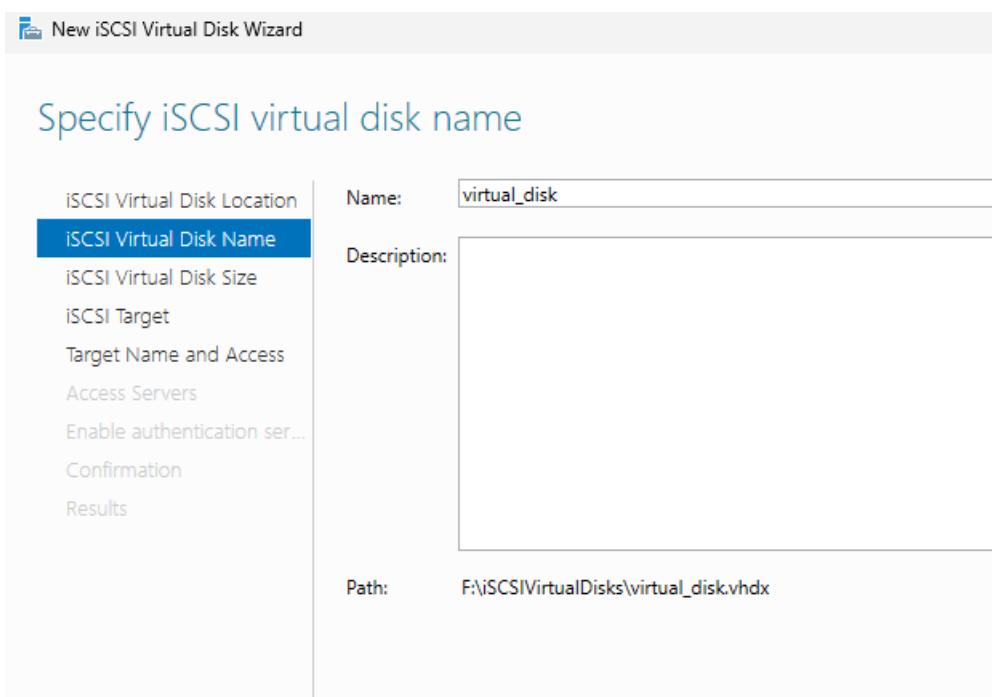
هنفتح ال file and storage

The screenshot shows the 'File and Storage Services' section under 'iSCSI'. The left navigation pane shows 'iSCSI' selected. The main pane displays 'iSCSI VIRTUAL DISKS' with the message 'No data available.' Below this, a note states 'To use iSCSI virtual disks, the iSCSI Target Server role service must be installed.' A link 'To install iSCSI Target Server, start the Add Roles and Features Wizard.' is present.

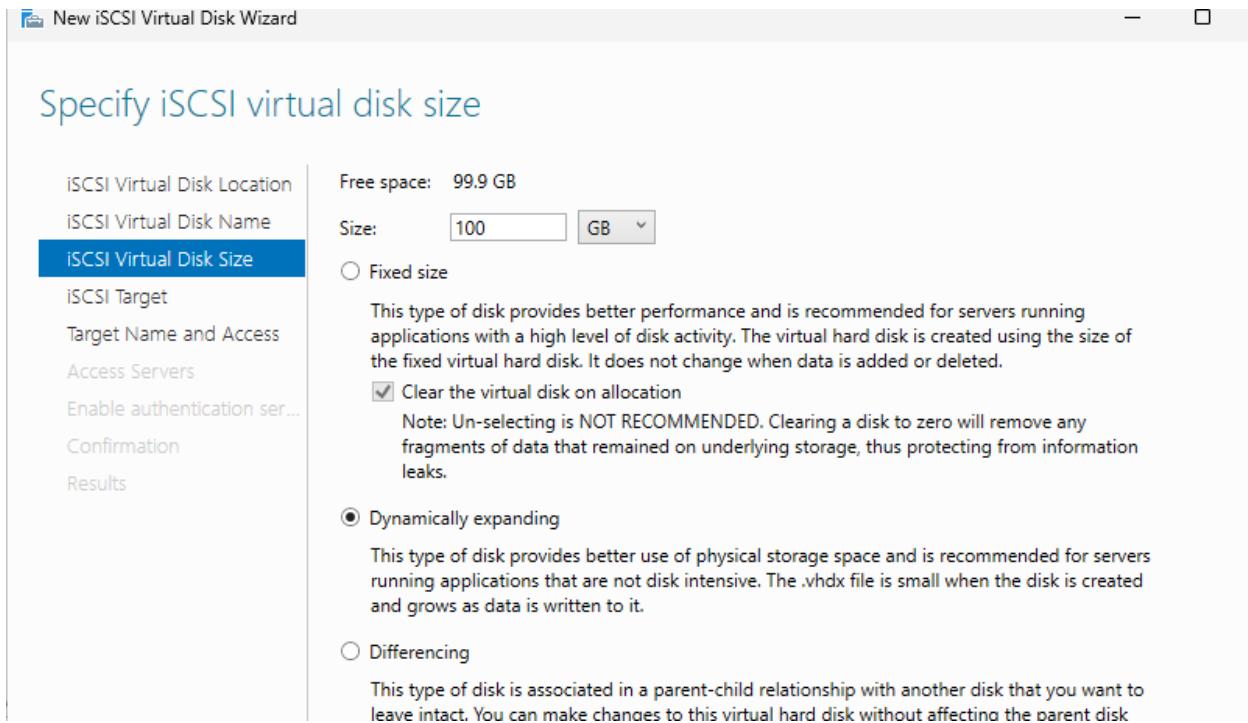
هنروح علي ال iSCSI و نعمل install لـ



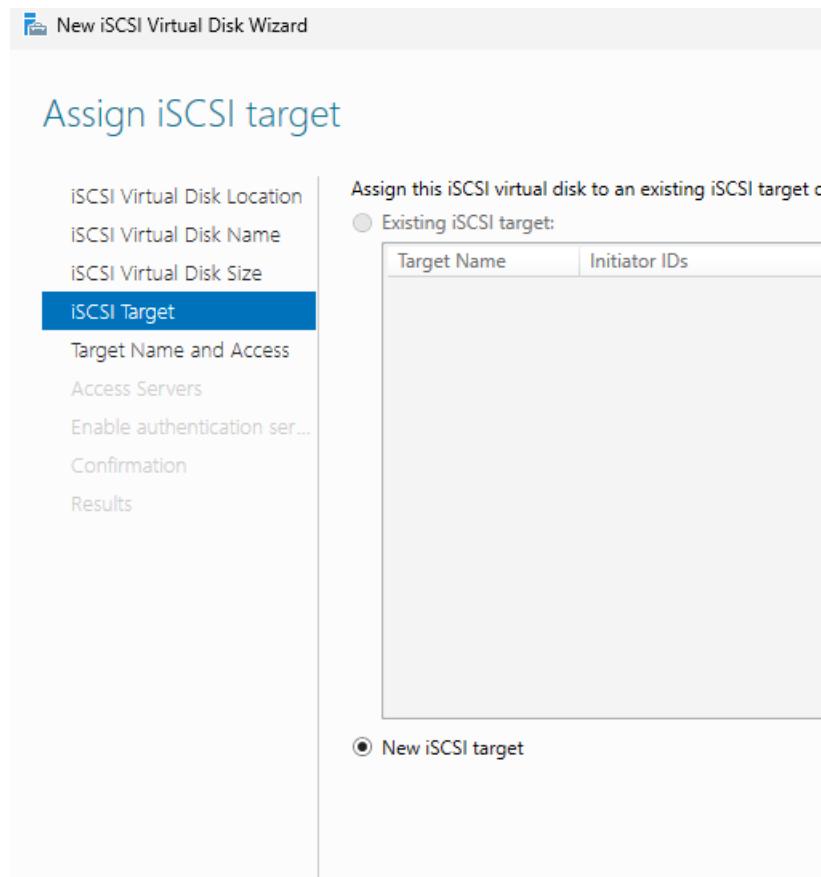
Virtual disk ل Create هعمل



VD ل Name



ال storage space ونوعها



عمل new target

--

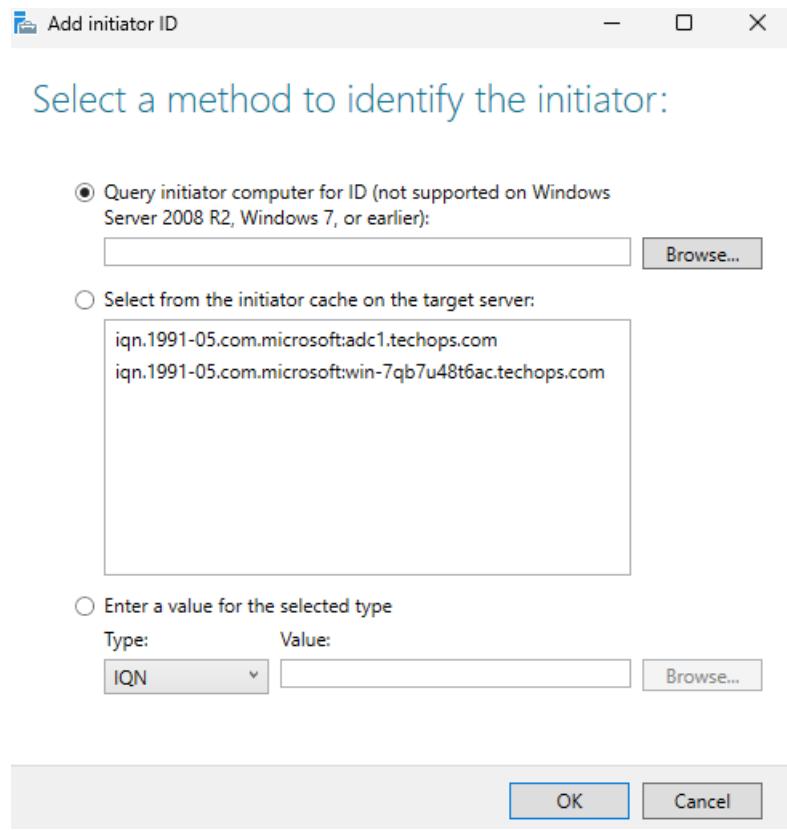
iSCSI Initiator Properties

Targets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration
Target portals					
The system will look for Targets on following portals:				Refresh	
Address	Port	Adapter	IP address		
192.168.1.100	3260	Default	Default		

iSCSI Initiator Properties

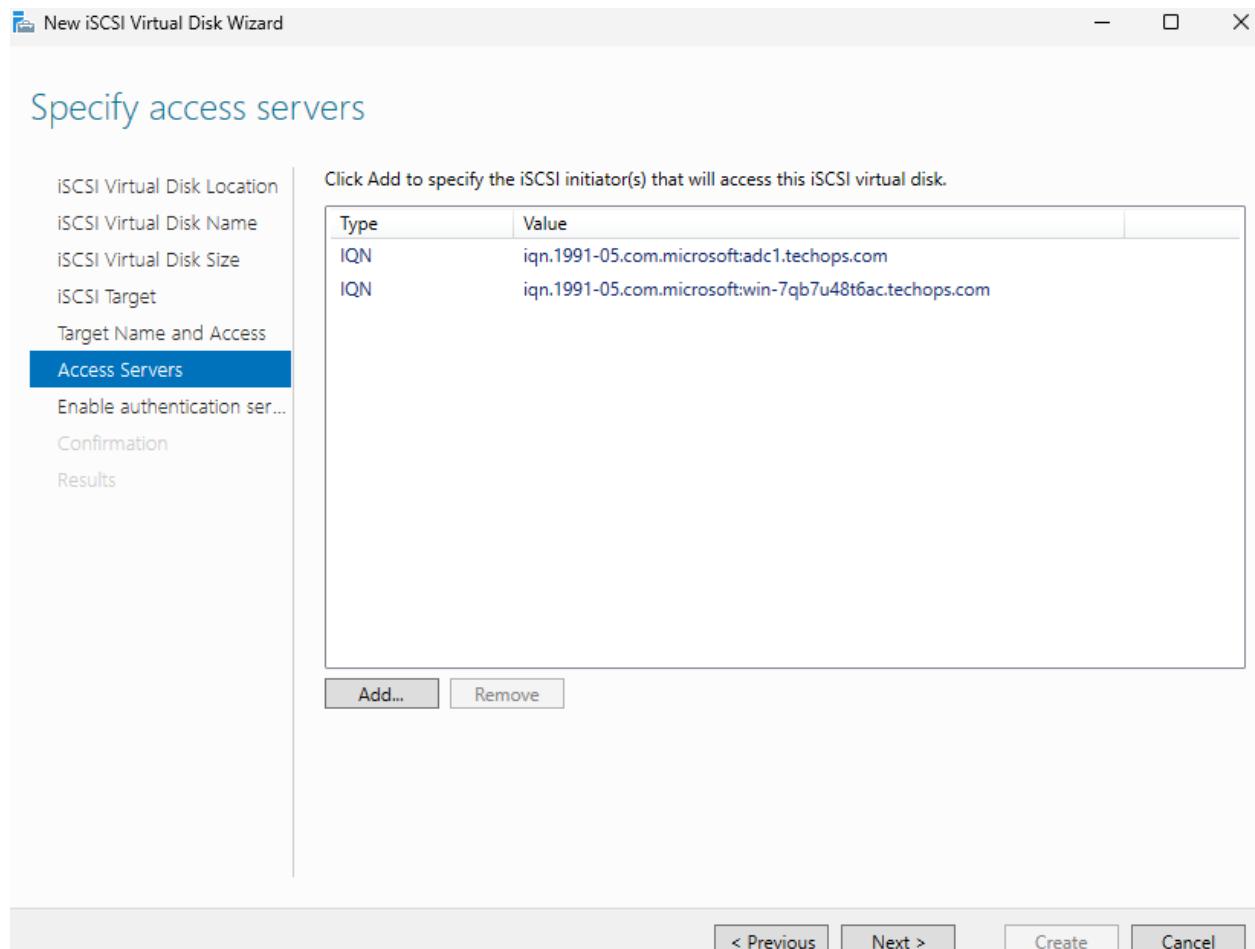
Targets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration
Target portals					
The system will look for Targets on following portals:				Refresh	
Address	Port	Adapter	IP address		
192.168.1.100	3260	Default	Default		

بعد كدا هروح على ال node 2 وافتتح ال iSCSI initiator واعمل discovery على ال ip الخاص بال iSCSI Target

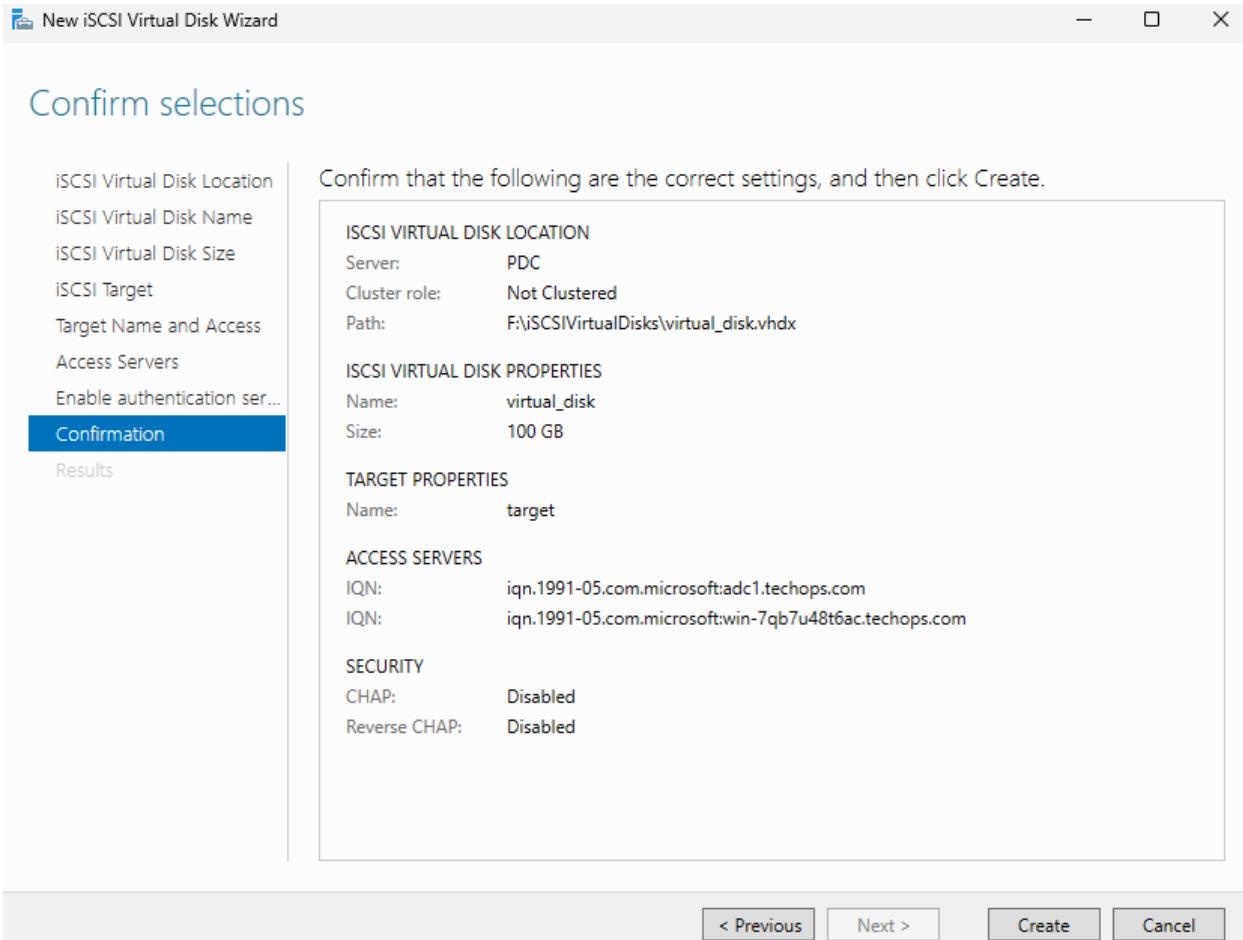


بعد كدا هرجع على ال SCSI Target هلاقيهم ظهروا عندي

--

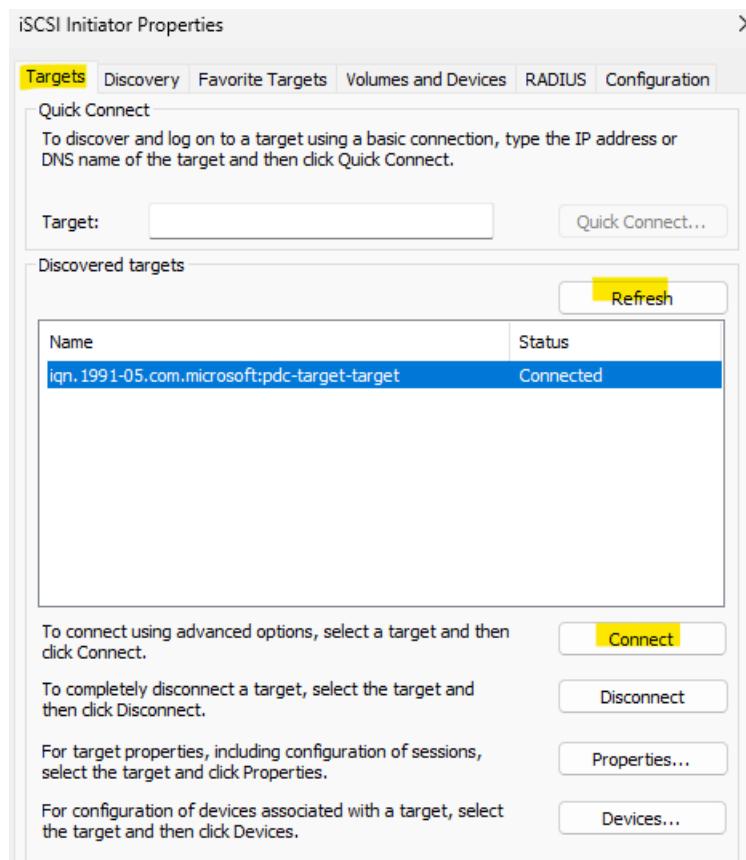


هعمل Add لـ 2 initiator



بعد كذا هعمل create

--



بعد كدا هنرجع علي ال initiator 2 ونروح علي target refresh نعمل بس target هنلاقي ال ظهر معايا هعمله connect (الخطوه دي هعملها علي ال 2 initiator)

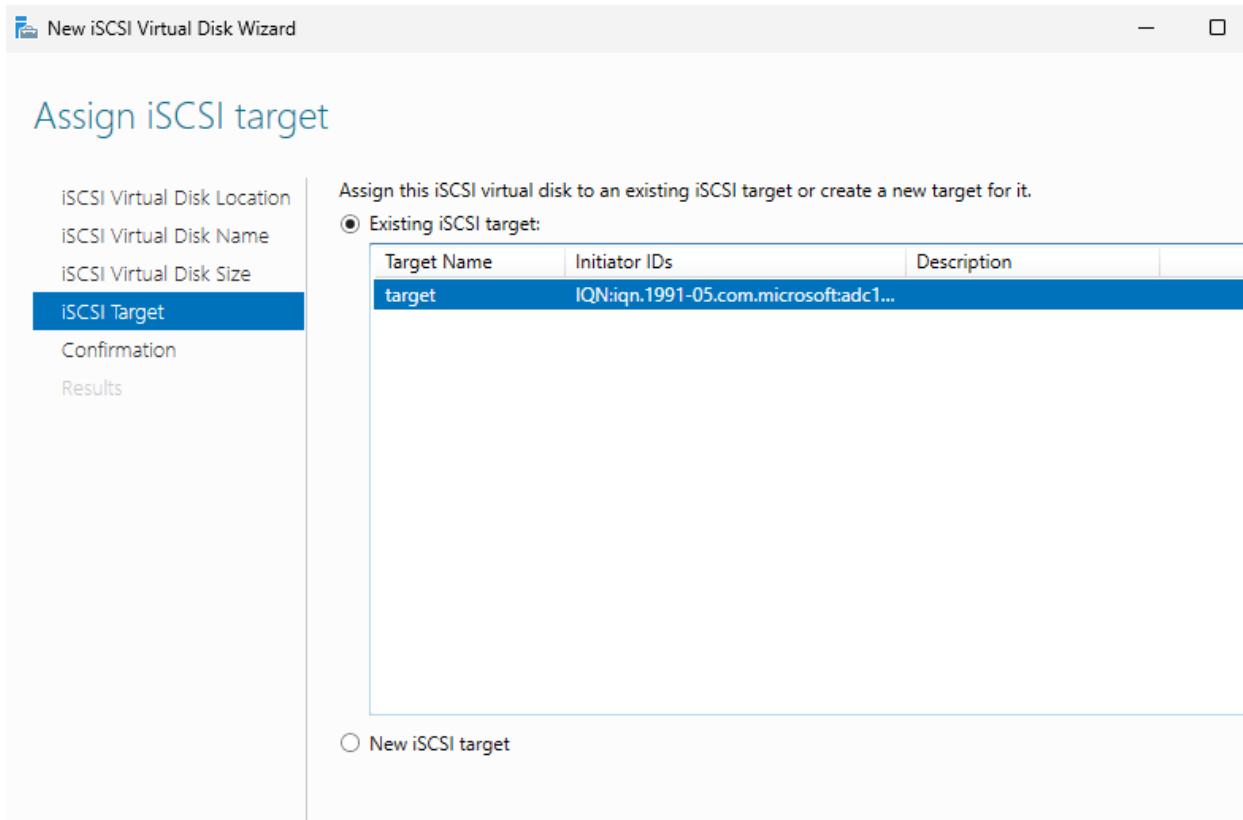
--

كدا جهزت ال 2 node shared storage علي ال

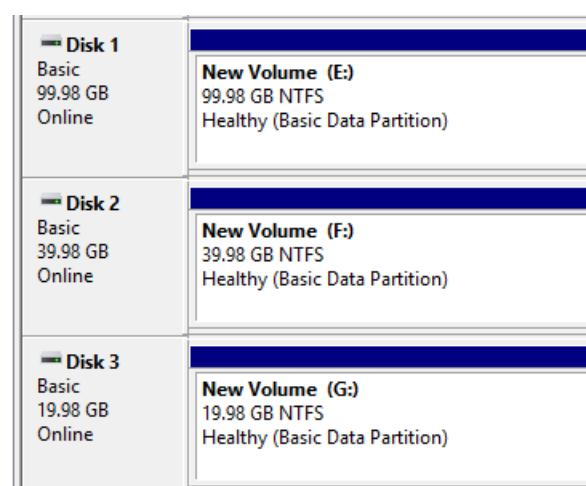
--

هكرر الخطوه دي واعمل disk 2 كمان

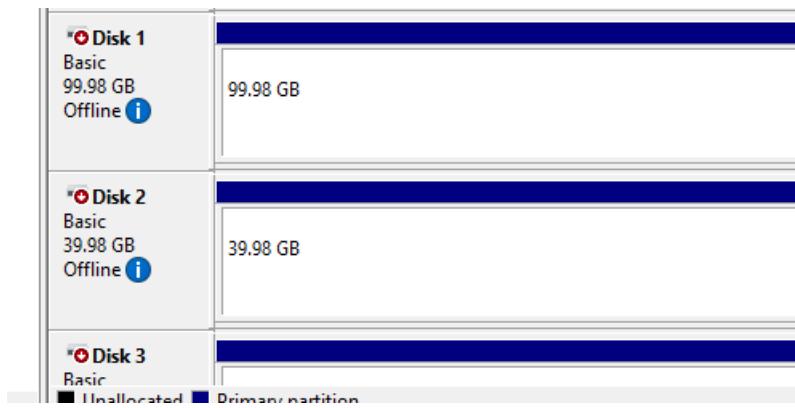
بس مش هعمل new target



في الخطوه دي هختار ال target ال احنا عملنها عشان مش كل شويا نروح عند ال initiator ونعمل config



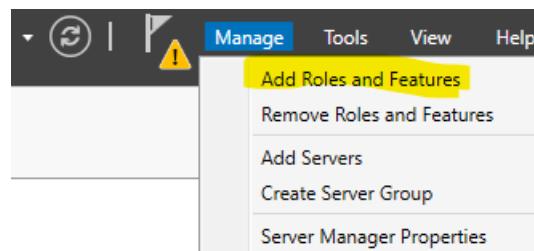
ضفنا 3 disk ، على 1 node اخلي ال 3 يكونوا online عادي



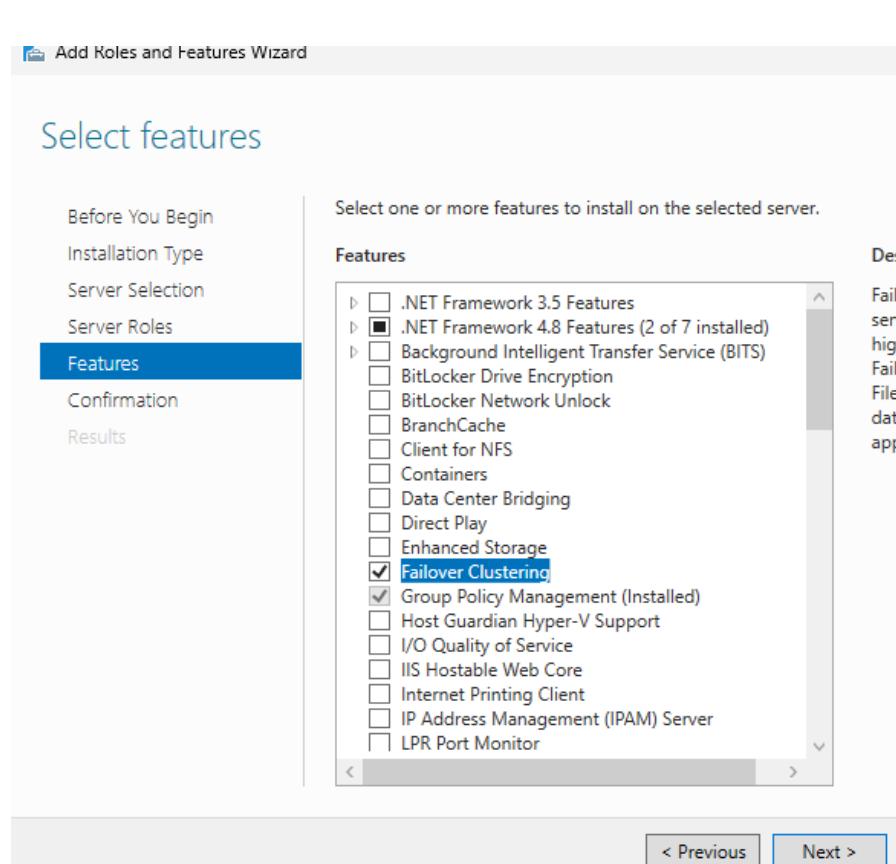
لكن على node 2 يكونوا offline

لاننا شغالين storage active/passive وبالتالي node 1 بس ال يستخدم ال storage ولو حصل مشكله
يسخدمهم (تجربا ان ال node 2 يكتبوا data في نفس الوقت فممكن يحصل مشكله لـ data)

تاني خطوه : نعمل failover cluster install لـ 2 node على ال

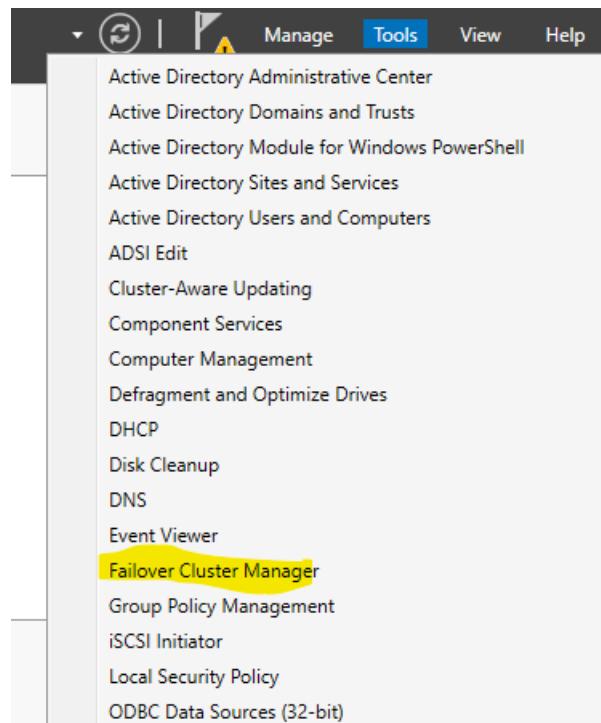


هنجعل add role and features



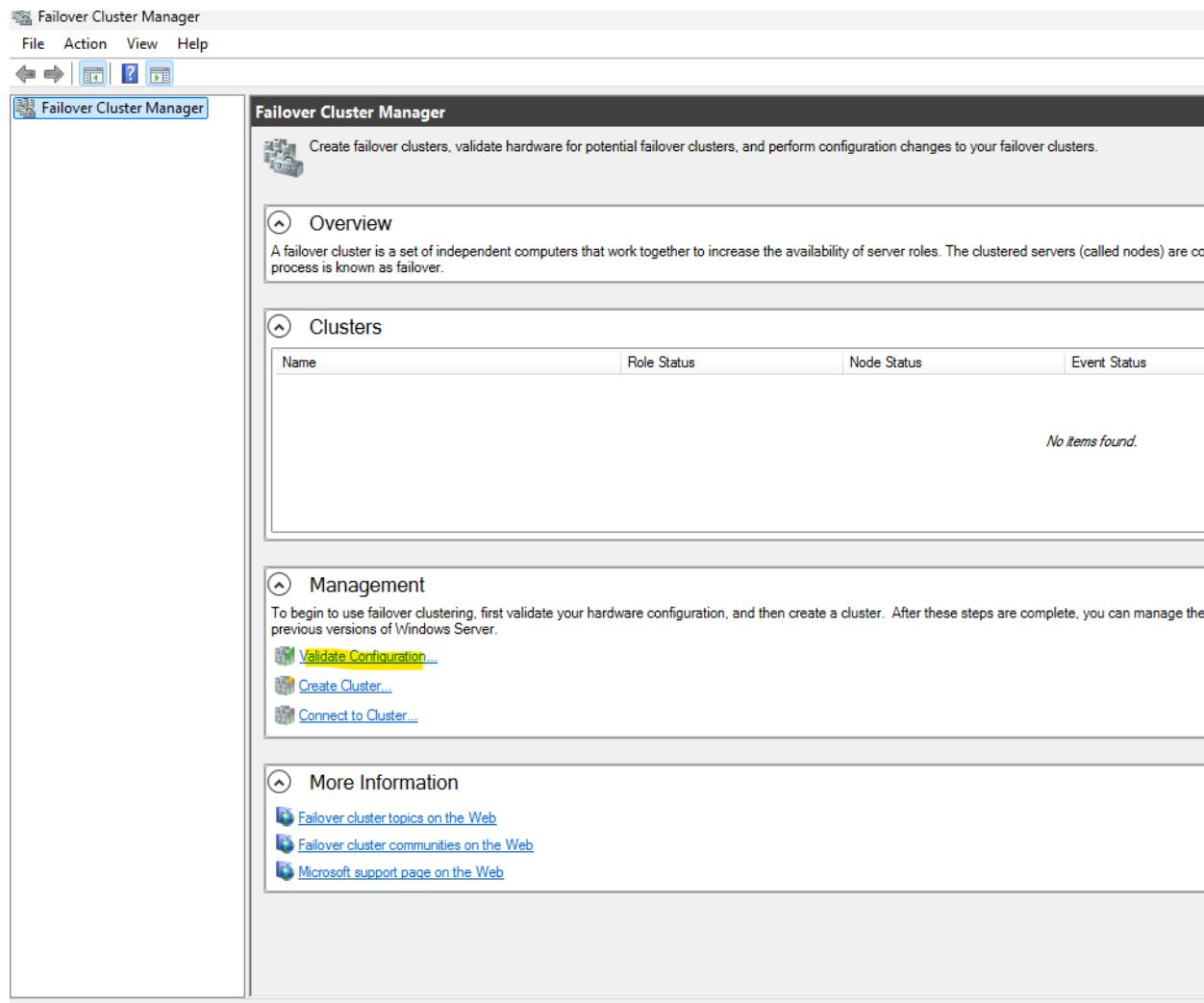
هختار feature failover clustering وبنظهر ك

وهكرر الخطوه مع node2



بعد که هنچ ال failover cluster manager

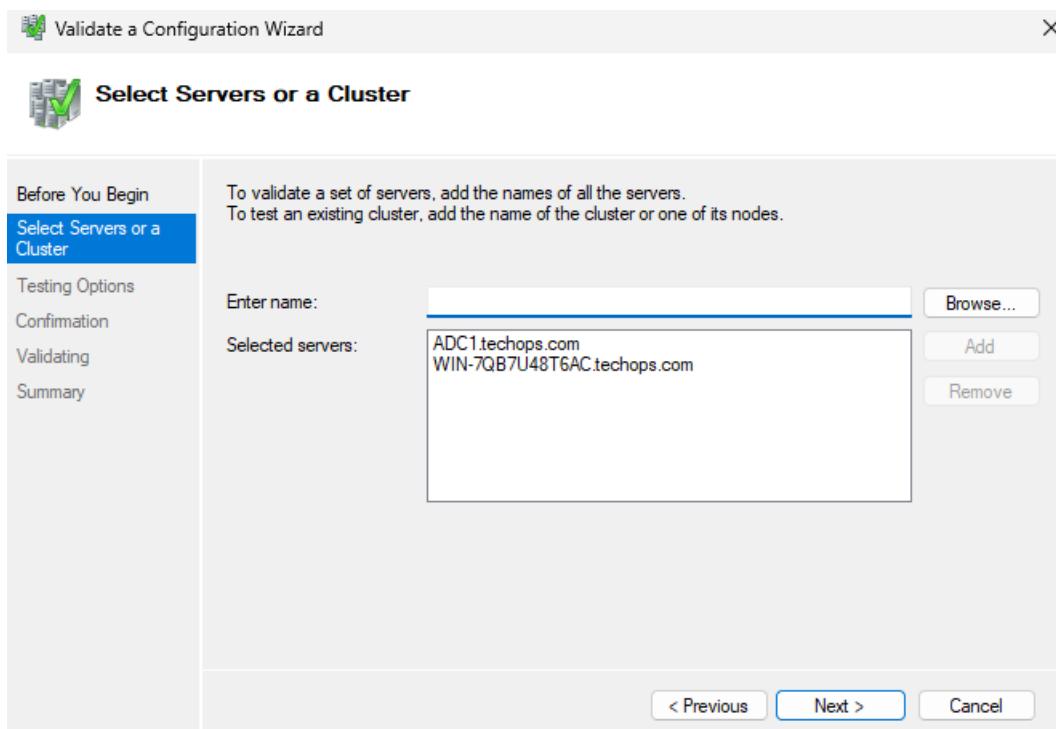
--



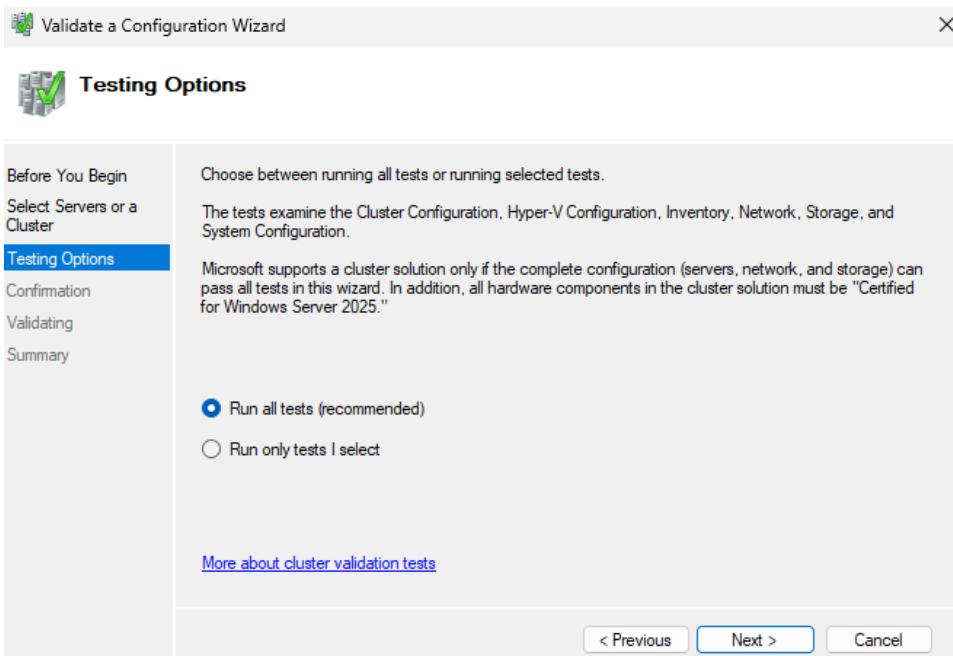
هيفتح بالشكل دا

ممكن اول حاجه اعملها هي ال validate لـ config عشان لو فيه اي config ناقصه يعرفي واعملها قبل ما ابدا

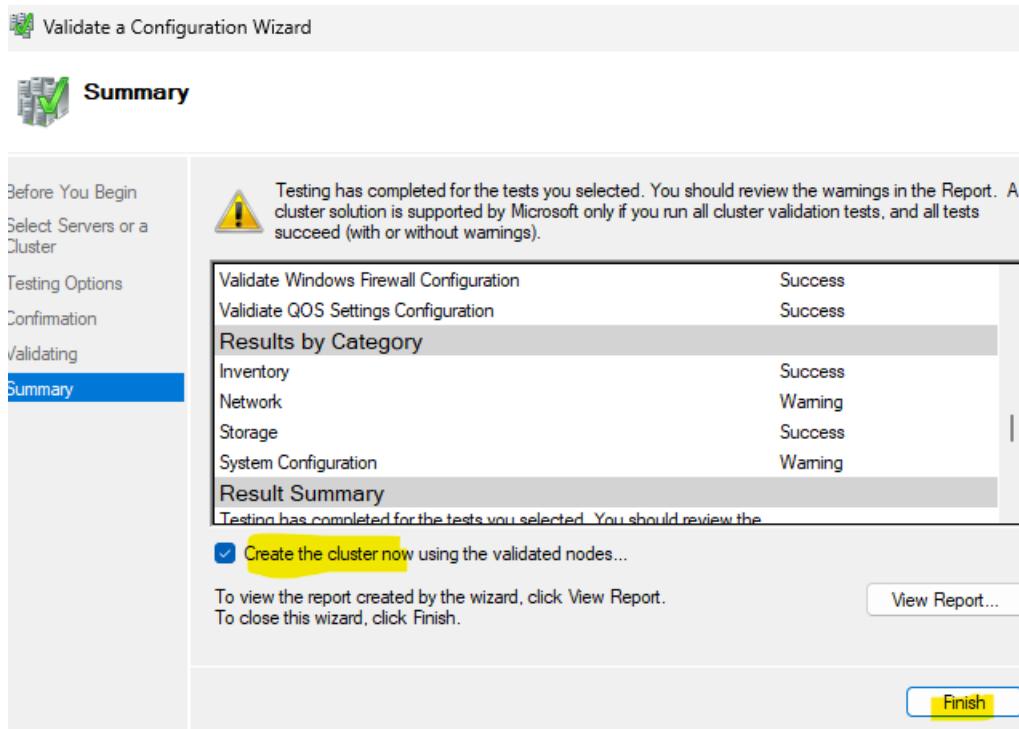
--



بیسالانی مین ال nodes ال هیكونوا فی ال cluster ف عدد 1 و 2 و node 2

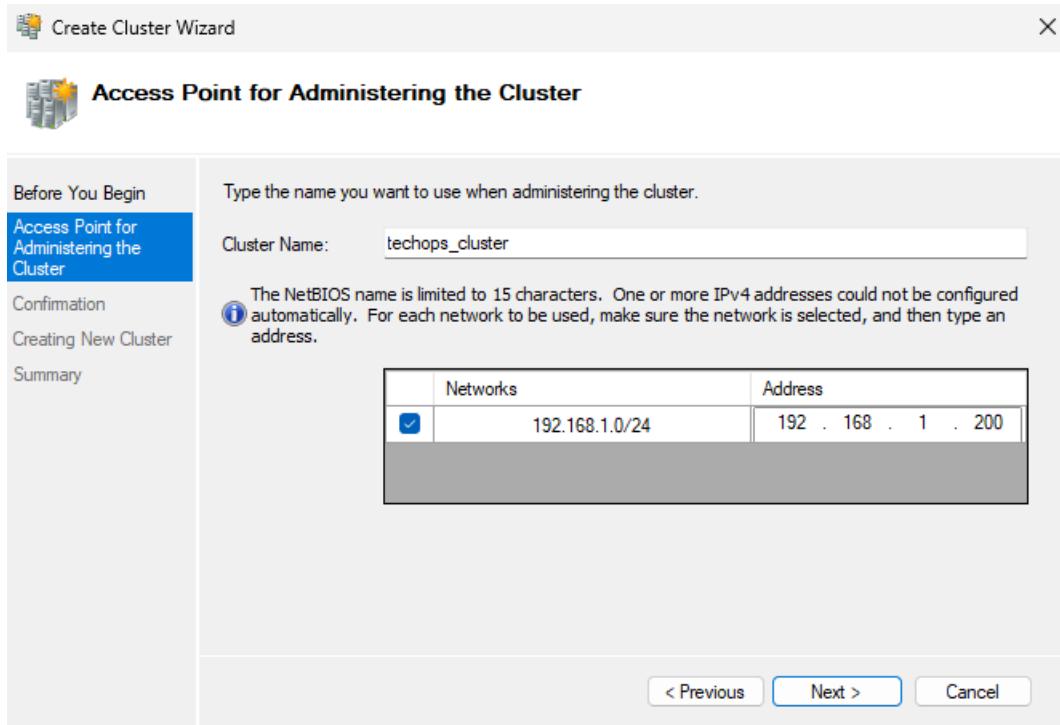


ختار run all test



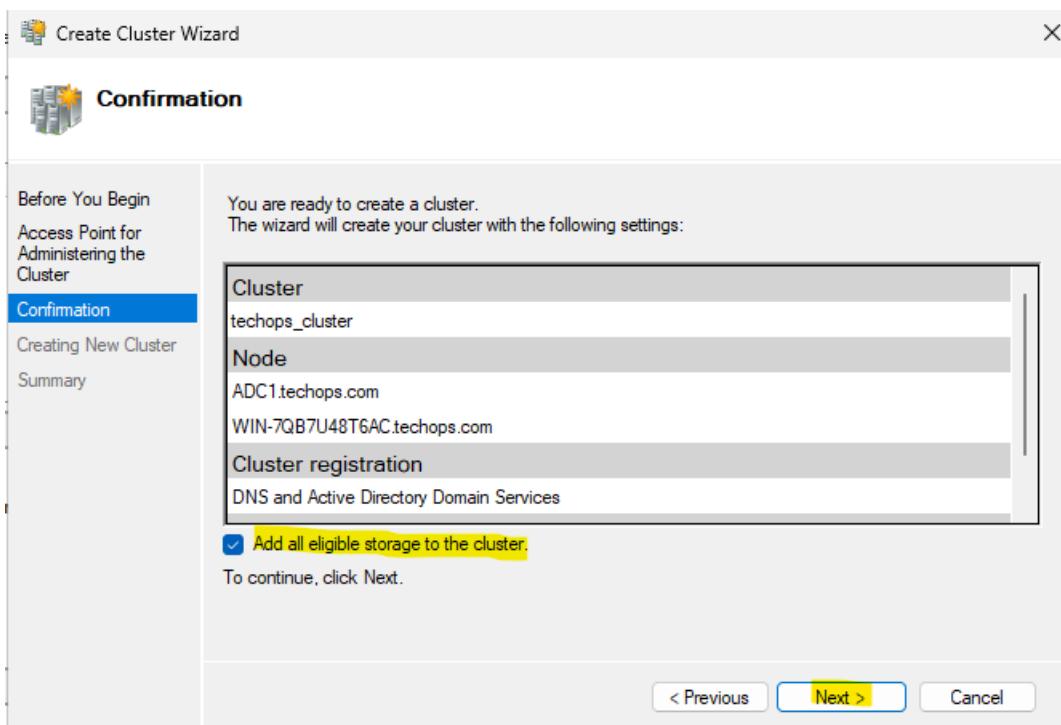
ال test تمام وجاهز اننا نبدا ال check ، cluster على ال عشان يفتحلي ال finish الخاص بال create اول ما اضغط console

--



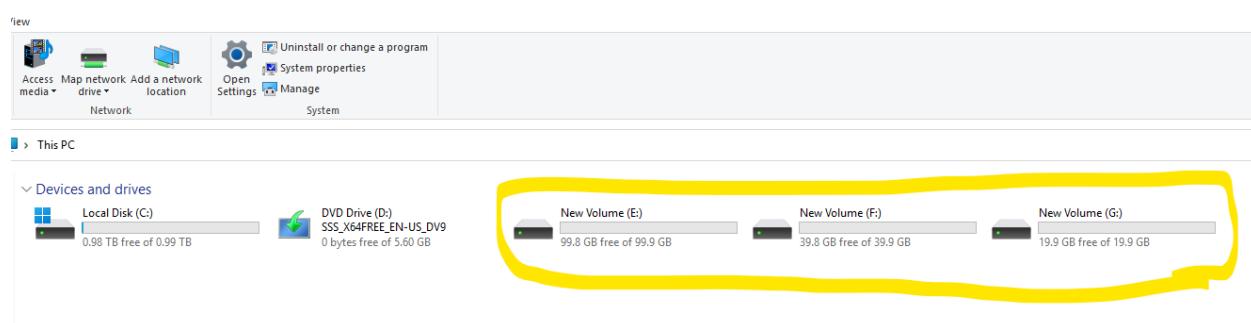
بیسانی هنا علی ال cluster name وال network ومش عندنا غير network واحدہ ف اخترنا ال دی ف سالنی عن ال address و ال address دا هیکون ال ip الخاص بال cluster ال هو عملنہ 192.168.1.200

--



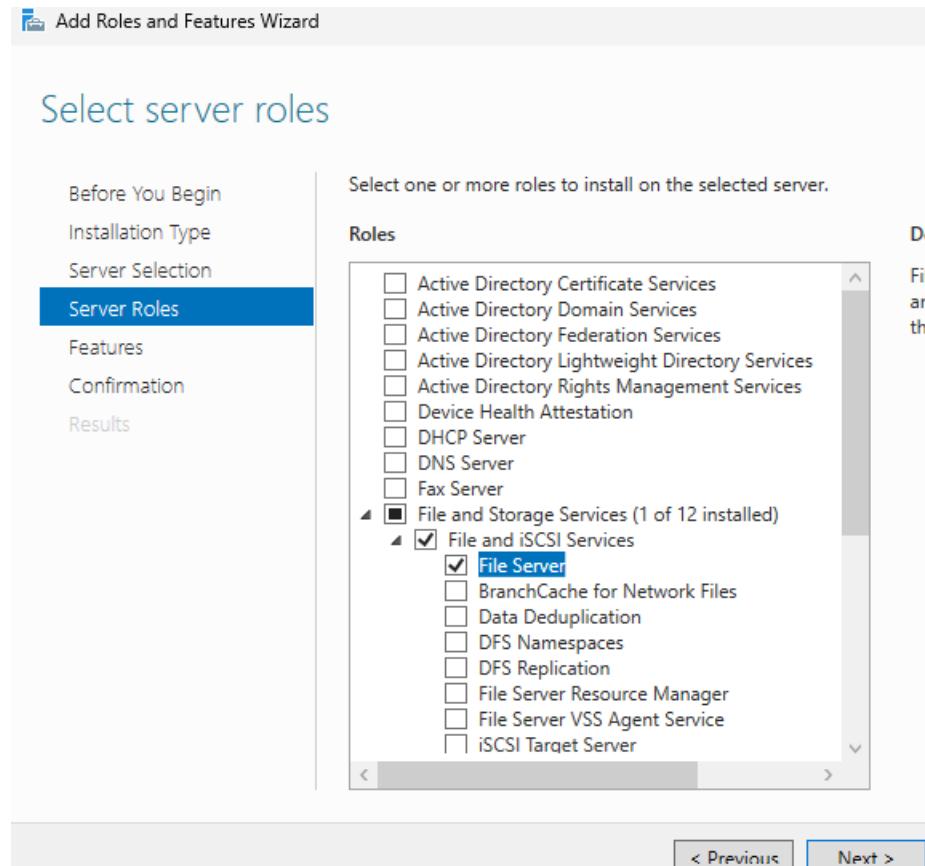
بعد كدا بيسالني هل اضفلك ال eligible storage ال عندك لـ cluster

ف هعمل check عليها ، وممكن اضافهم من ال console برضو



دا شكل ال partition add قبل ما اعملهم cluster لـ

كدا ال cluster failover جاهز واقدر اعمل service لاكثر من 2 node test على ال file sharing على ال 2 node installed دي تكون service فلازم ال file sharing على ال 2 node install ف هنعملها



هنعمل 2 node file server install لـ 2 node على ال