

الجانب العملي لشهادات MCSA 2008 / 2012 / 2016



إعداد أ. عبدالسلام صالح الراشدي
2019

 abdelsalam.elrashdi@gmail.com

 facebook.com/abdelsalam.elrashdi

الجانب العملي لشهادات MCSA 2008_2012_2016 الجزء الثاني

الرجاء تحميل الجانب العملي لشهادات MCSA 2008_2012_2016 الجزء
الاول من موقع كتب

<https://www.kutub.info/search?search=%D8%B9%D8%A8%D8%AF%D8%A7%D9%84%D8%B3%D9%84%D8%A7%D9%85+%D8%A7%D9%84%D8%B1%D8%A7%D8%B4%D8%AF%D9%8A>

18-Active Directory

يعتبر Active Directory أو Active Directory Domain Services أساس شبكات الدومين في مايكروسوفت ، وهو عبارة عن قاعدة بيانات لكل موارد الشبكة Resources والخدمات Services والمستخدمين Users

بحيث أنك تستطيع من خلاله عمل تحكم مركزي Central Administration بكل هذه الأجزاء في الشبكة وعمل Domains و بنية الشركة الهيكلية Hierarchical organization structure وغيرها ، والتحكم بالصلاحيات ال authorization and authentication .

إذا حملت النظام Windows Server دون تثبيت اي Rule عليه ، وعملت له انضمام للشبكة Join فيسمى Member Server، اما اذا حملت نظام التشغيل فقط فيسمى standalone Sever.

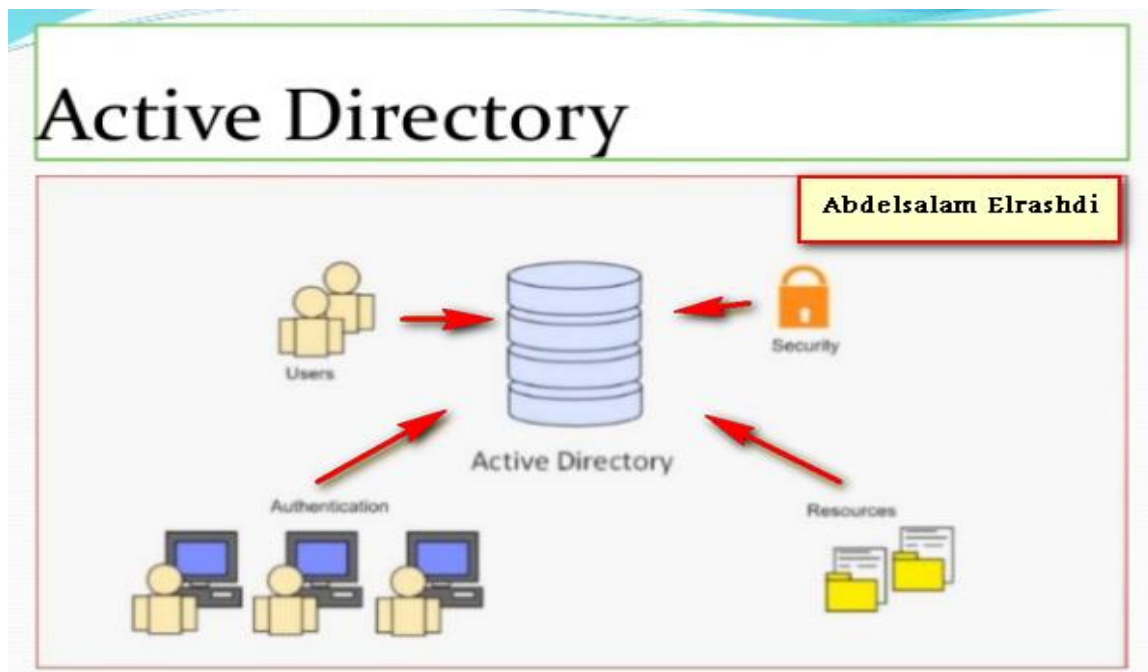
إذا Domain Controller يعتبر Server يخزن فيه قاعدة بيانات ال Active Directory وتحفظ في ملف يسمى ntds.nit ”

اما المجال Domain فهو عبارة عن اسم منطقي غير ملموس يحتوي بداخله على جميع العناصر الرئيسية مثل .active dirctoe,y,domain controller,ou,users,computers,printers,folders,...etc

وللتوضيح أكثر نتخيل ان الدومين هو دولة ليبيا على سبيل المثال والمساحة الجغرافية الحقيقية التي توجد بها ليبيا هي domain controller والسجل المدني الذي يحتوي علي المعلومات الخاصة بالليبيين والاجانب الموجودين داخل ليبيا هو Active directory.

Active Directory is essential to any Microsoft network built on the client-server network model—it allows you to have a central sever called a Domain Controller (DC) that does authentication for your entire network.

Instead of people logging on to the local machines they authenticate against your D Active Directory stores data as objects. An object is a single element, such as a user, group, application or device, such as a printer. Objects are normally defined as either resources -- such as printers or computers -- or security principals -- such as users or groups.

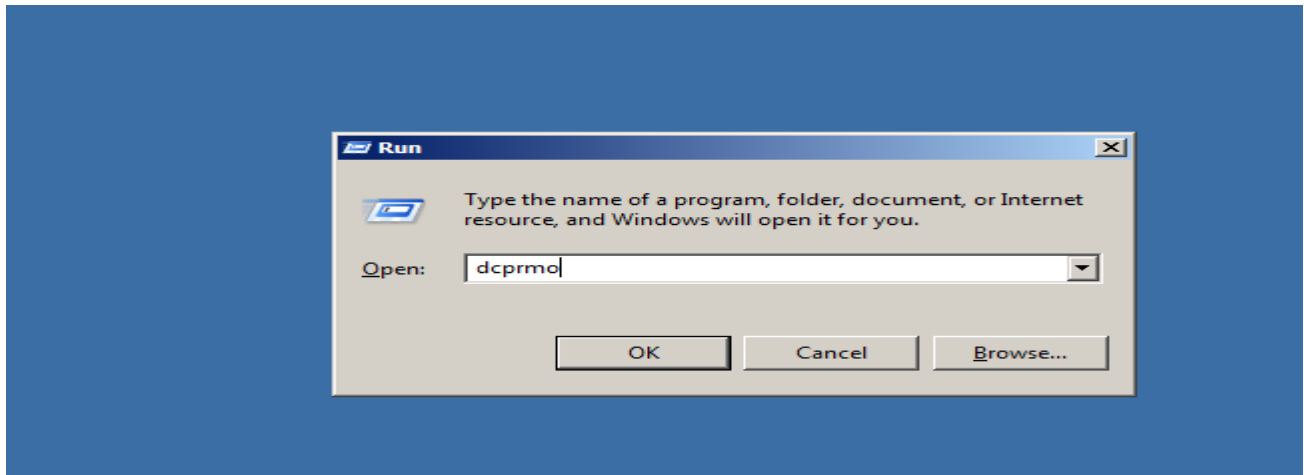


18.1- Install active directory on windows server 2008 r2

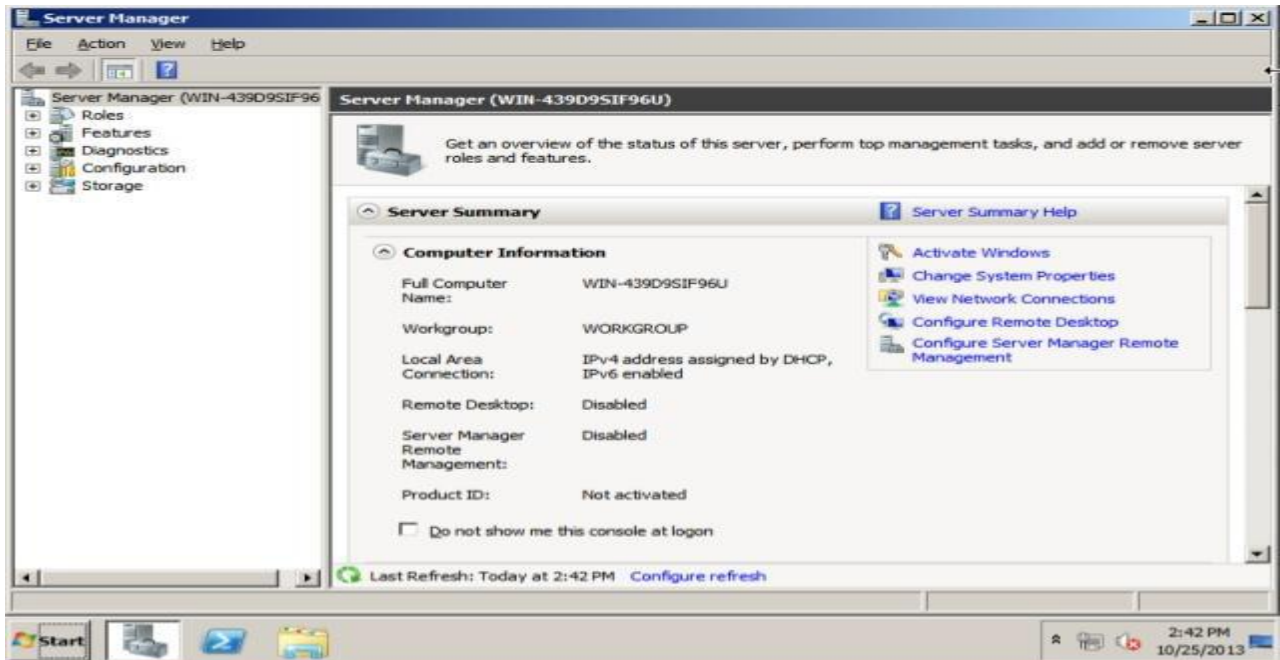
You have two ways to install the active directory

first one :-

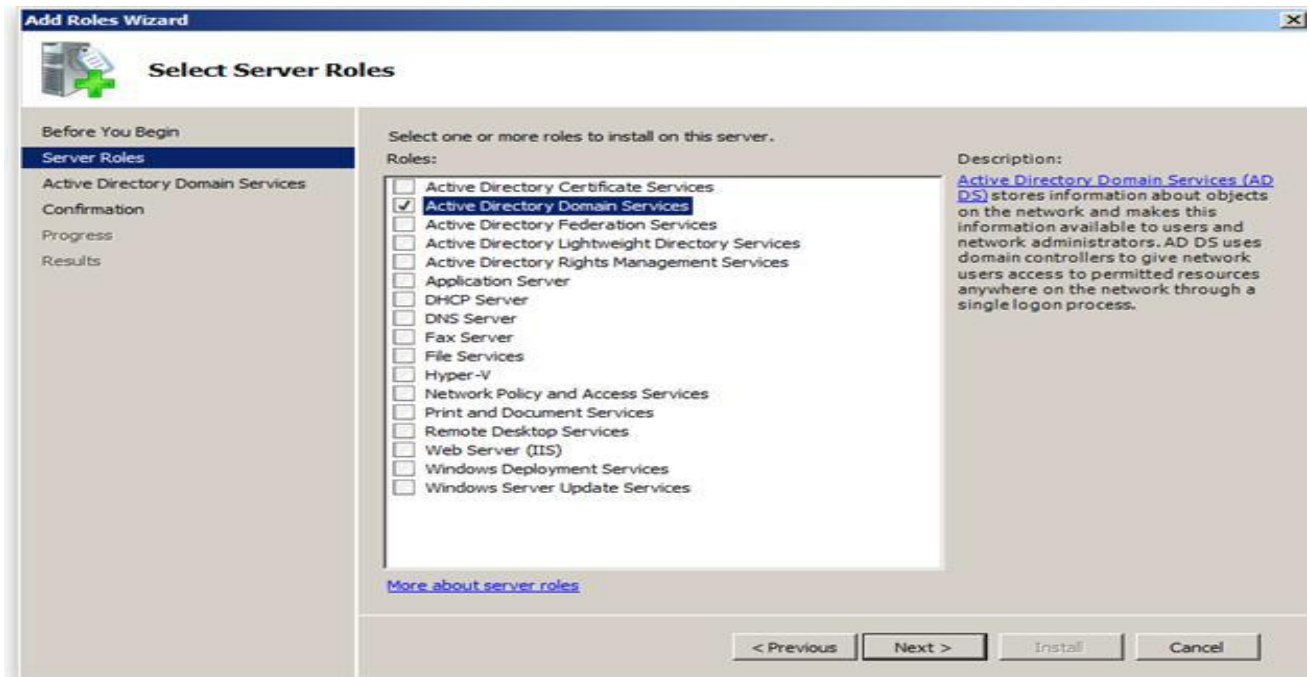
open the run then type dcpromo



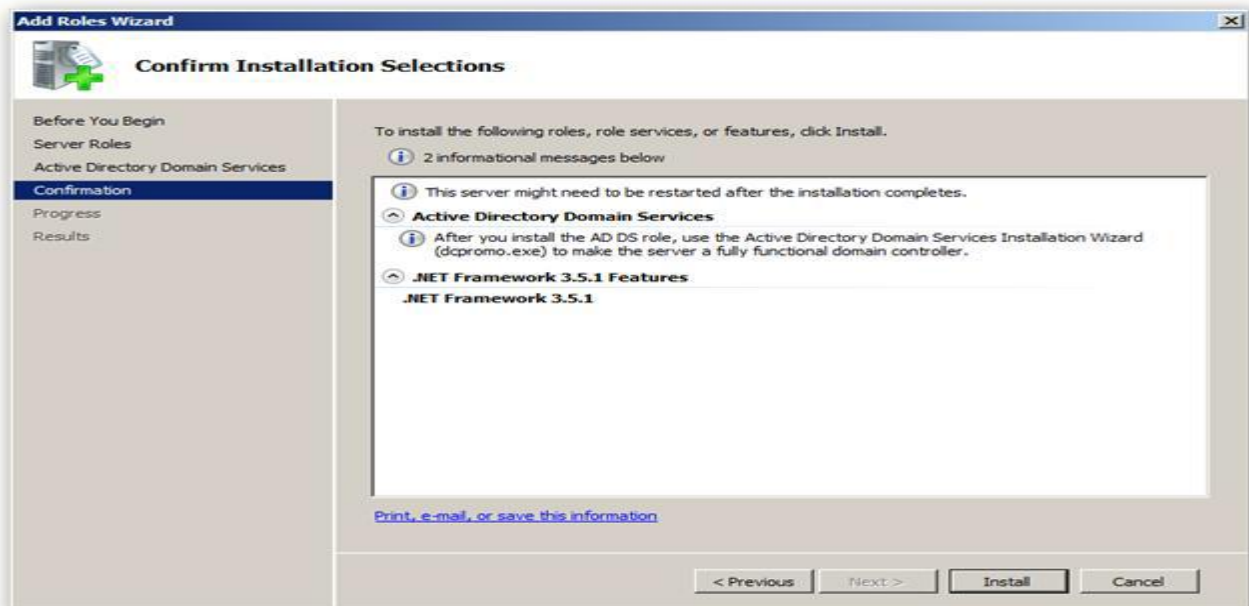
Second one :- Open Server Manager and click on roles, this will bring up the Roles Summary on the right hand side where you can click on the Add Roles link. hoice image place



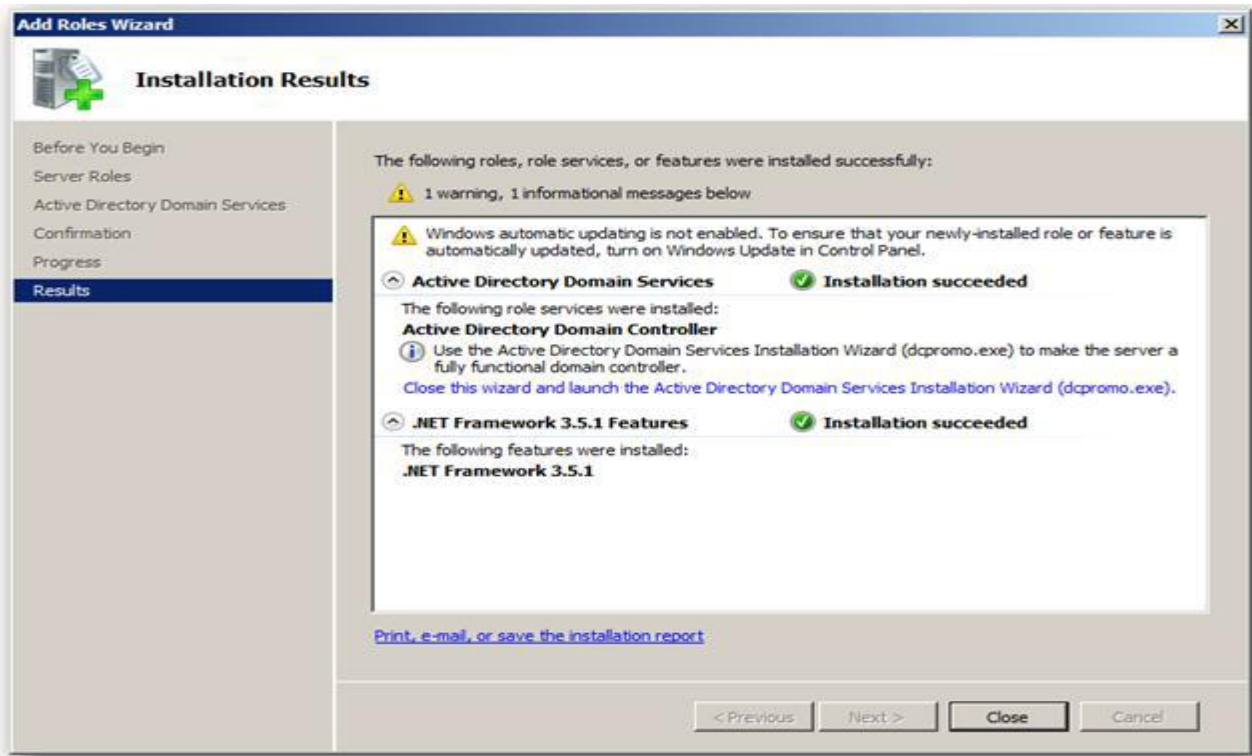
This will bring up the Add Roles Wizard where you can click on next to see a list of available Roles. Select Active Directory Domain Services from the list, you will be told that you need to add some features, click on the Add Required Features button and click next to move on.



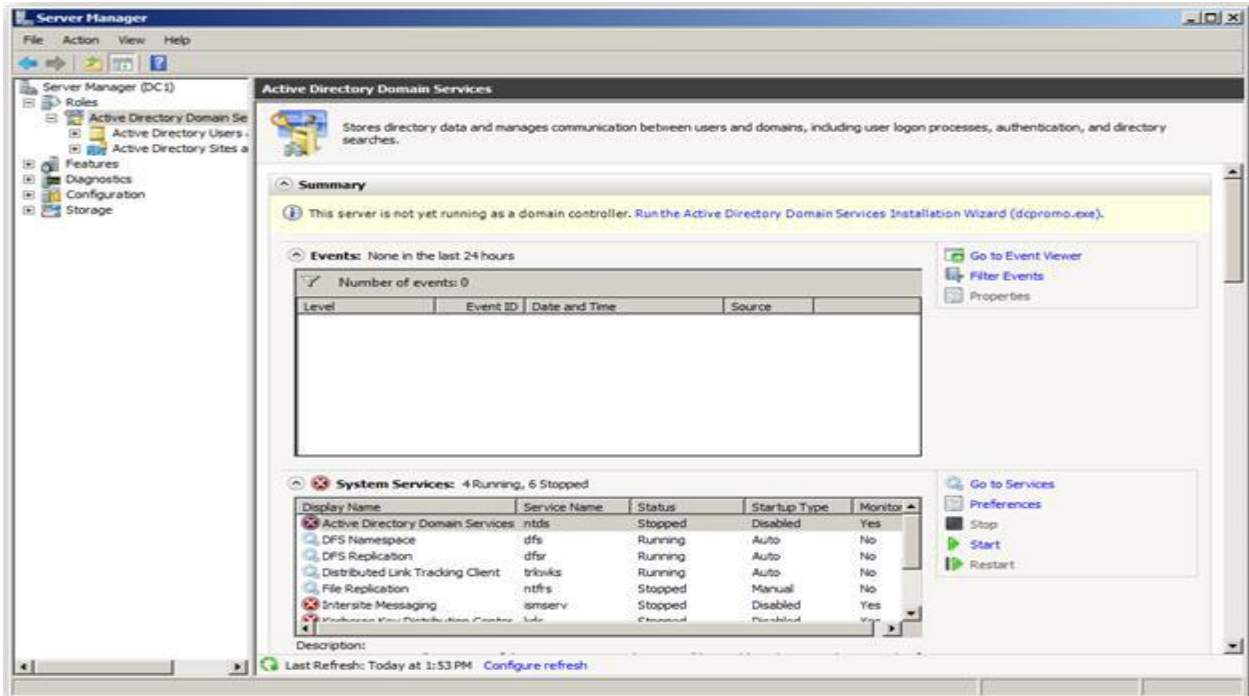
A brief introduction to Active Directory will be displayed as well as a few links to additional resources, you can just click next to skip past here and click install to start installing the binaries for Active Directory.



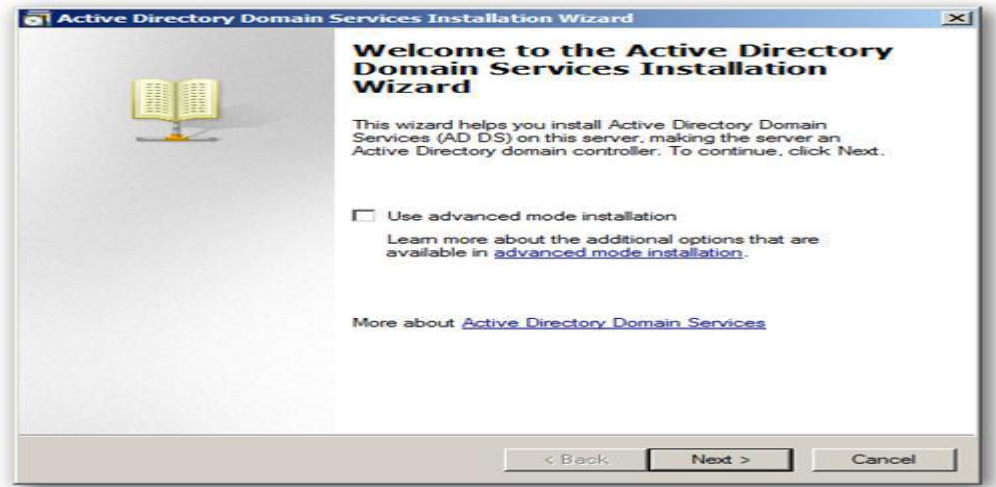
When the installation is finished you will be shown a success message, just click close



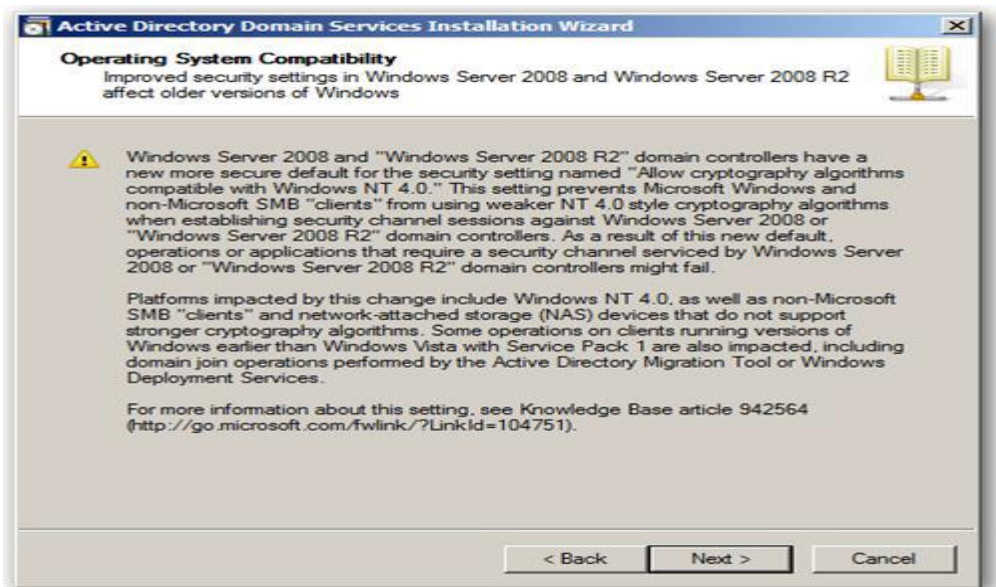
Open up Server Manager, expand Roles and click on Active Directory Domain Services. On the right hand side click on the Run the Active Directory Domain Services Installation Wizard (dcpromo.exe) link.



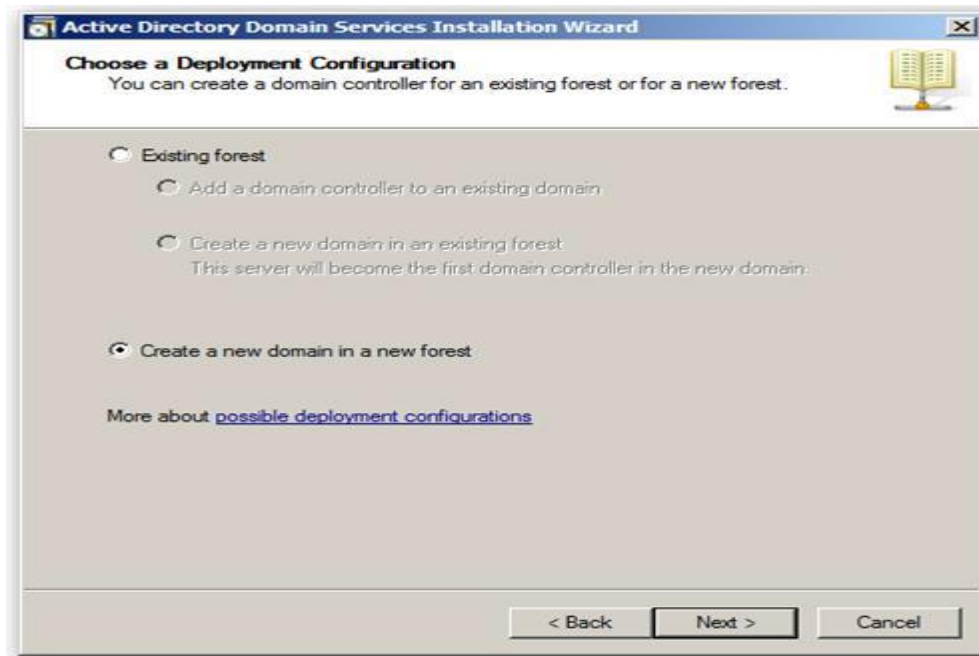
This will kick off another wizard, this time to configure the settings for you domain, click next to continue.



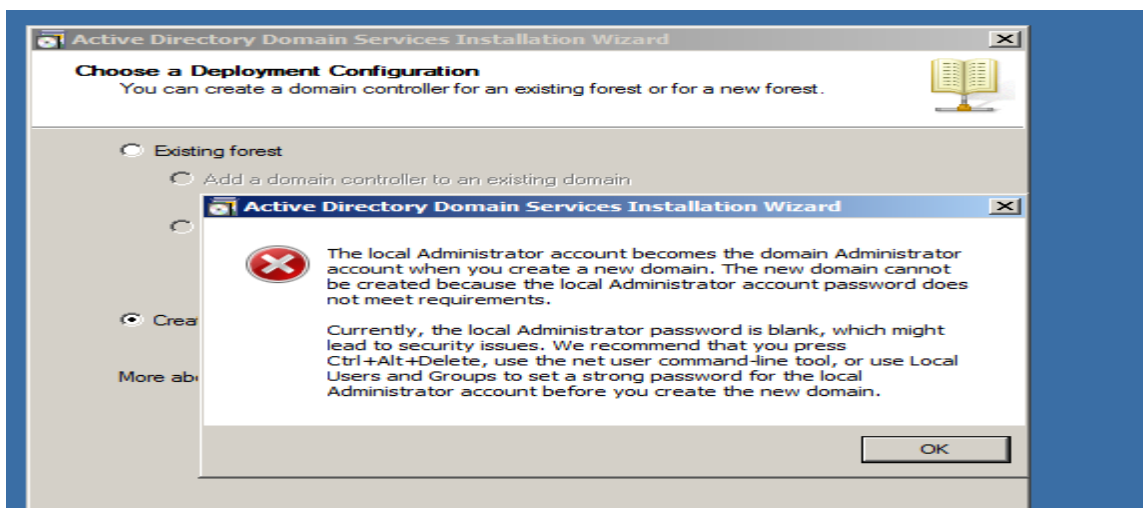
The message that is shown now relates to older clients that do not support the new cryptographic algorithms supported by Server 2008 R2, these are used by default in Server 2008 R2, click next to move on.



Choose to create a new domain in a new forest.



This message will appear if your username
(administrator) not have complexity password

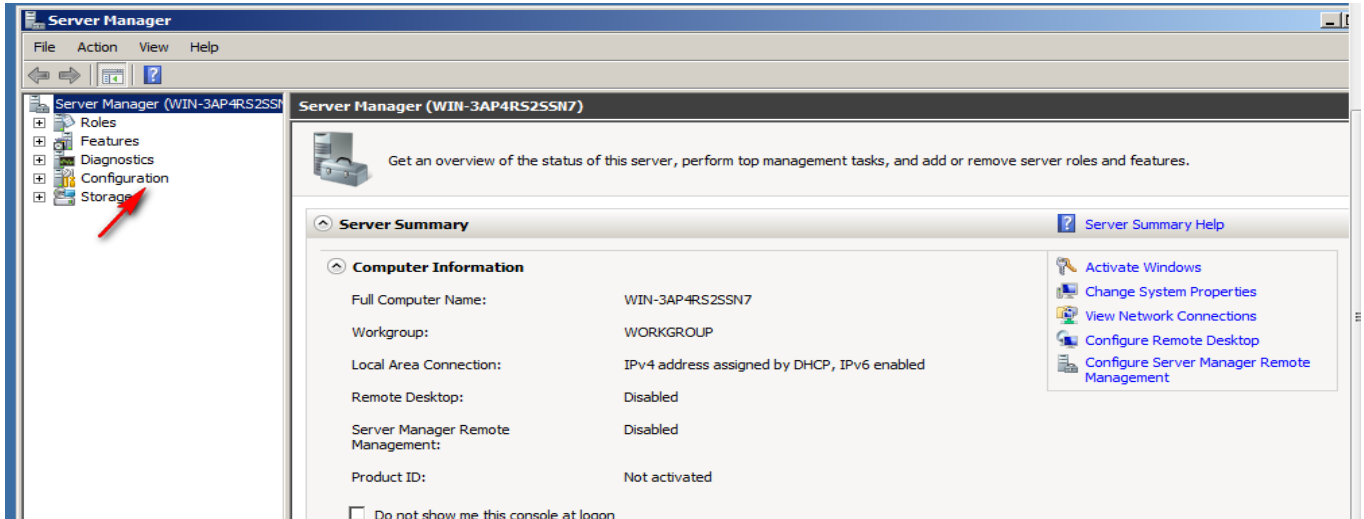


الرسالة السابقة تظهر عندما لا يوجد باسورد معقد يحتوي علي حروف ورموز وارقام للادمين
Administrator

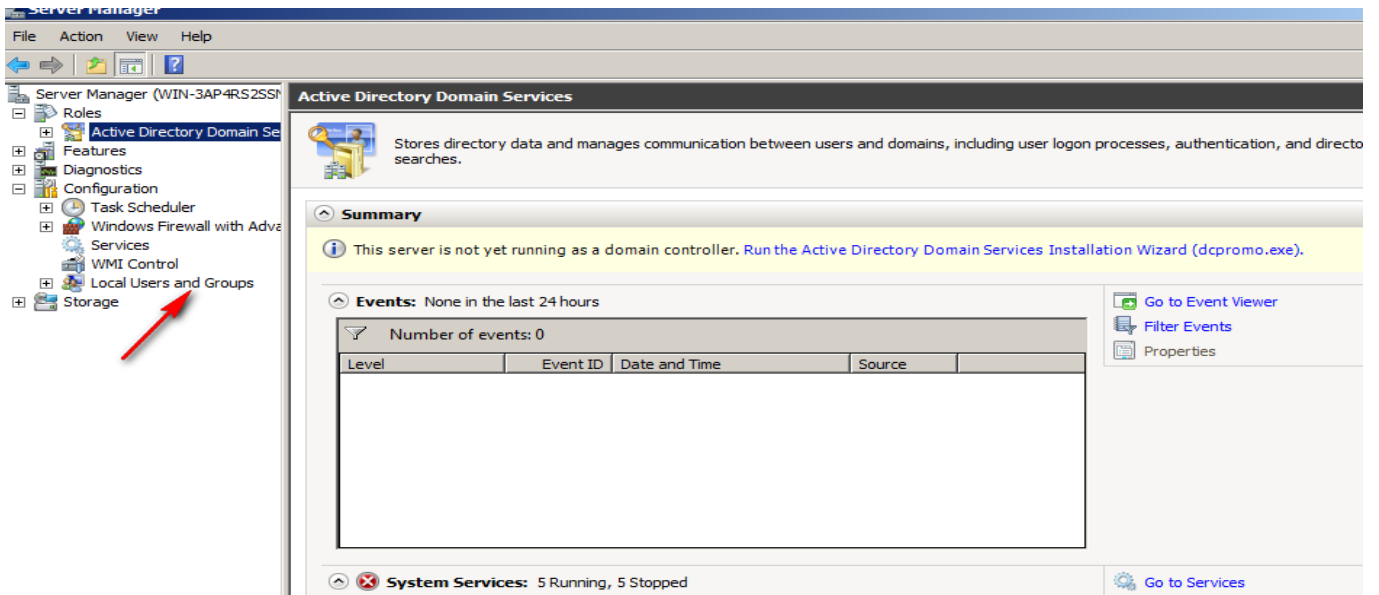
ولعمل باسورد معقد للادمن يجب علينا اتباع الاتي:

Open server manager

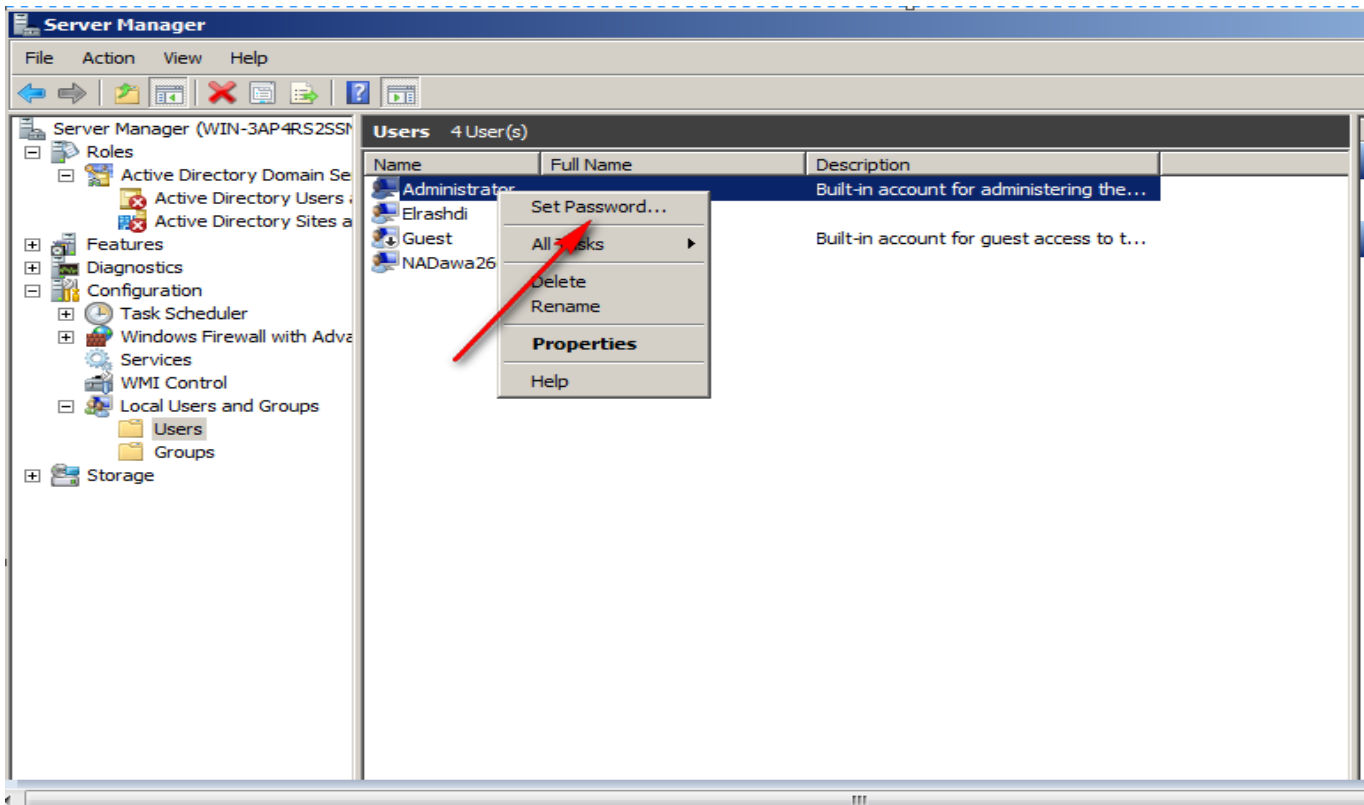
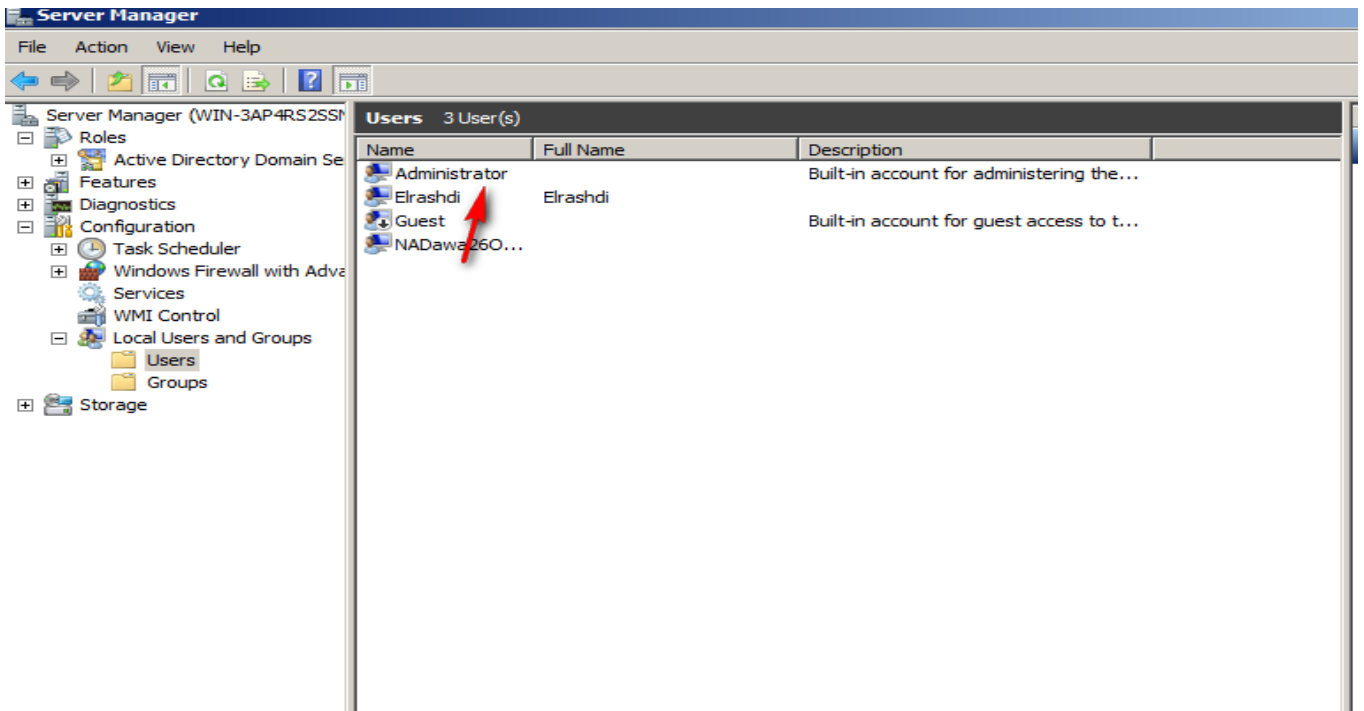
Manage computer



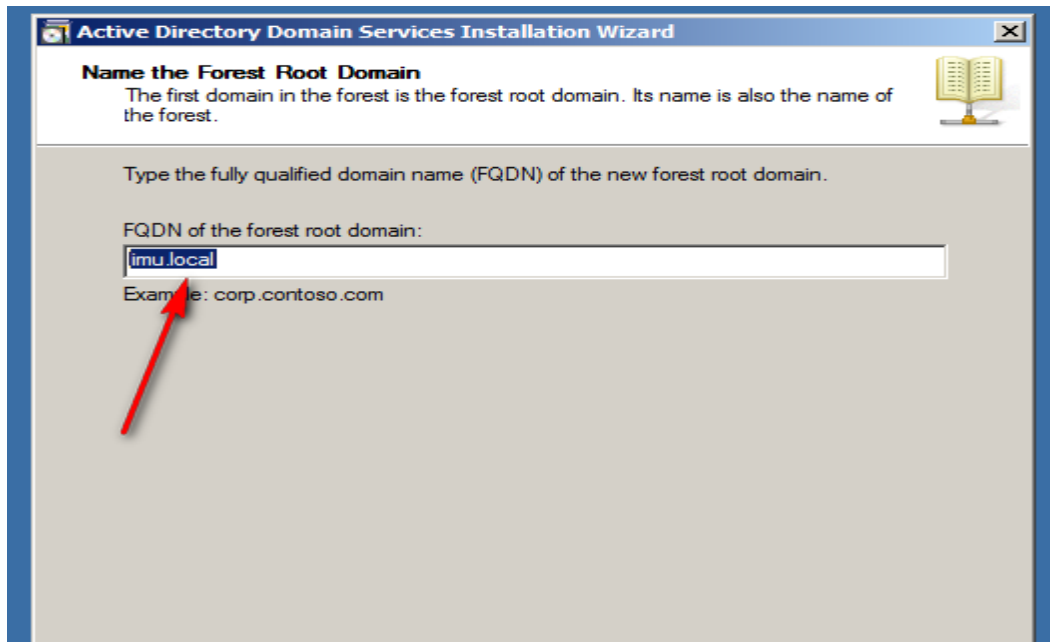
Create users



Create users



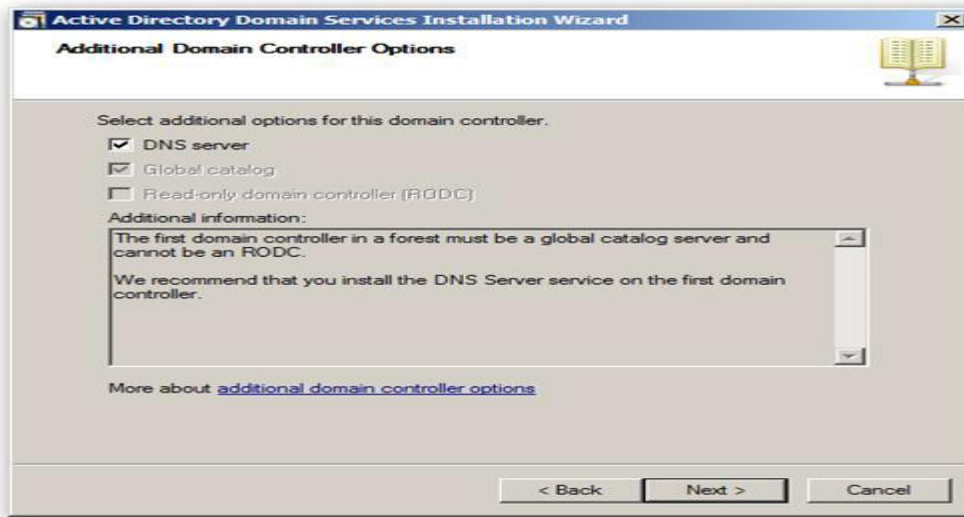
Now you can name your domain, we will be using a limu.local domain



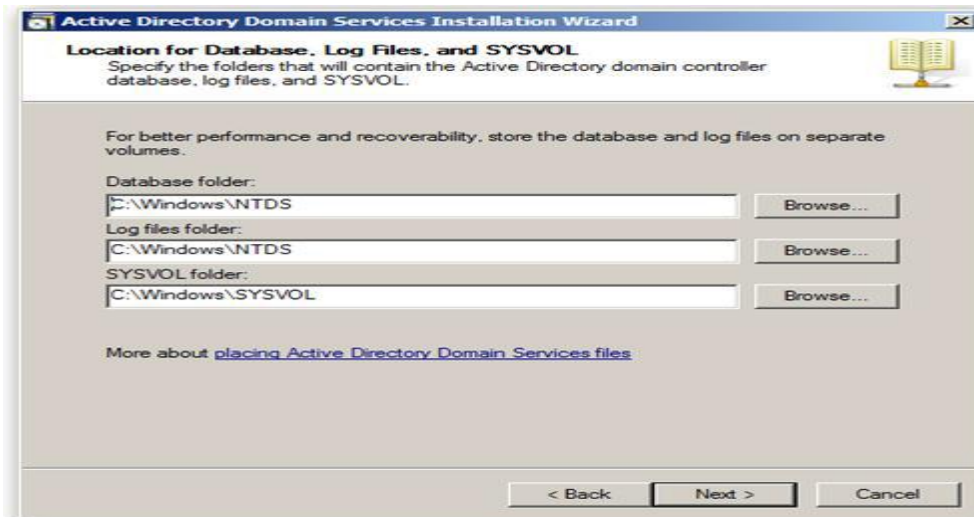
Since this is the first DC in our domain we can change our forest functional level to Server 2008R2.



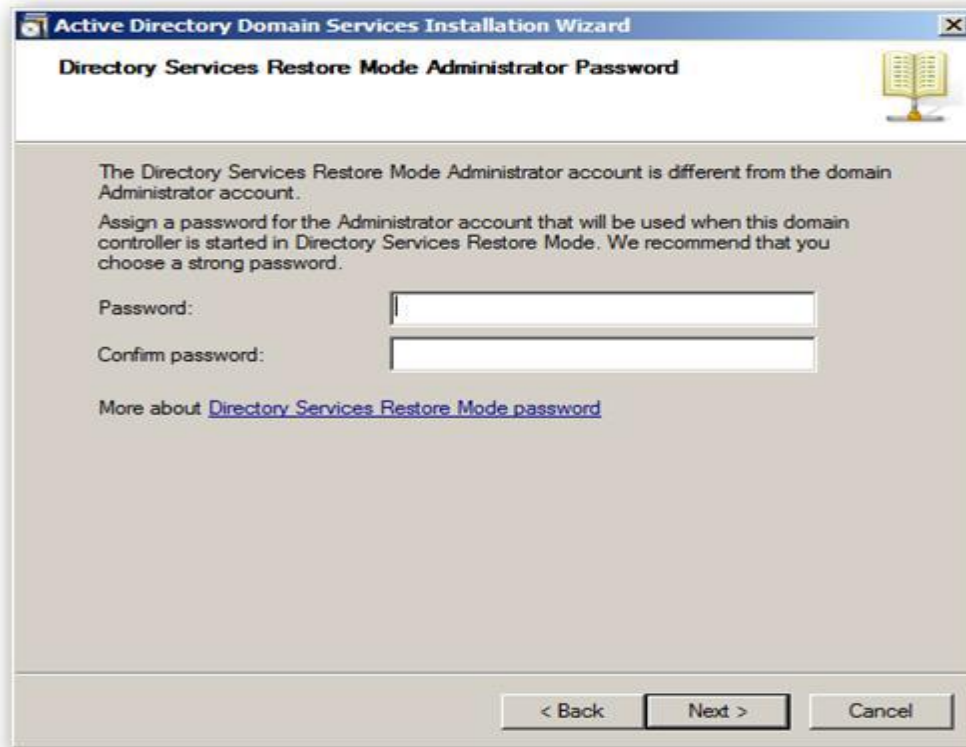
We want to include DNS in our installation as this will allow us to have an AD Integrated DNS Zone, when you click next you will be prompted with a message just click yes to continue.



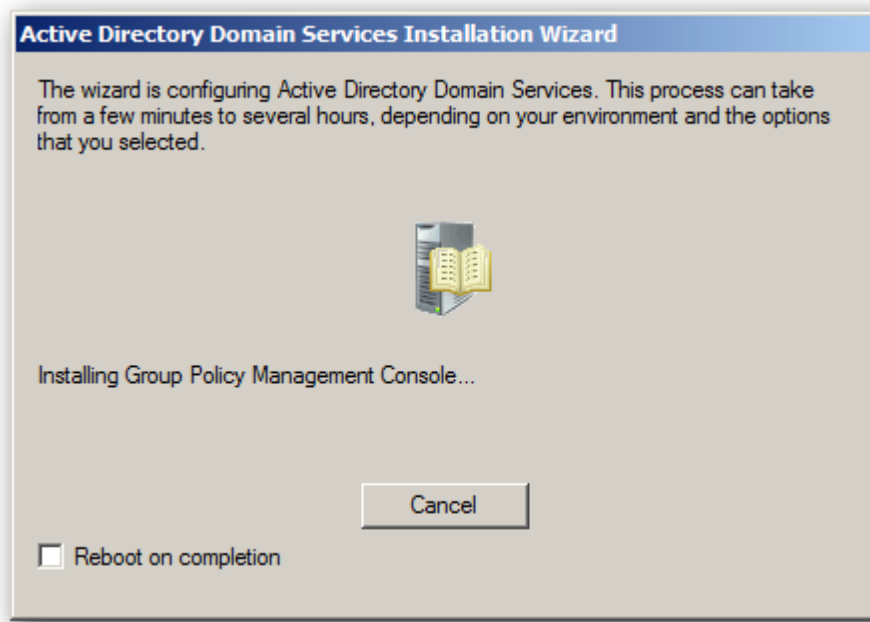
you will need to choose a place to store log files, it is a best practice to store the database and SYSVOL folder on one drive and the log files on a separate drive, but since this is in a lab environment I will just leave them all on the same drive



Choose a STRONG Active Directory Restore Mode Password and click next twice to kick off the Configuration



You will be able to see what components are being installed by looking in the following box



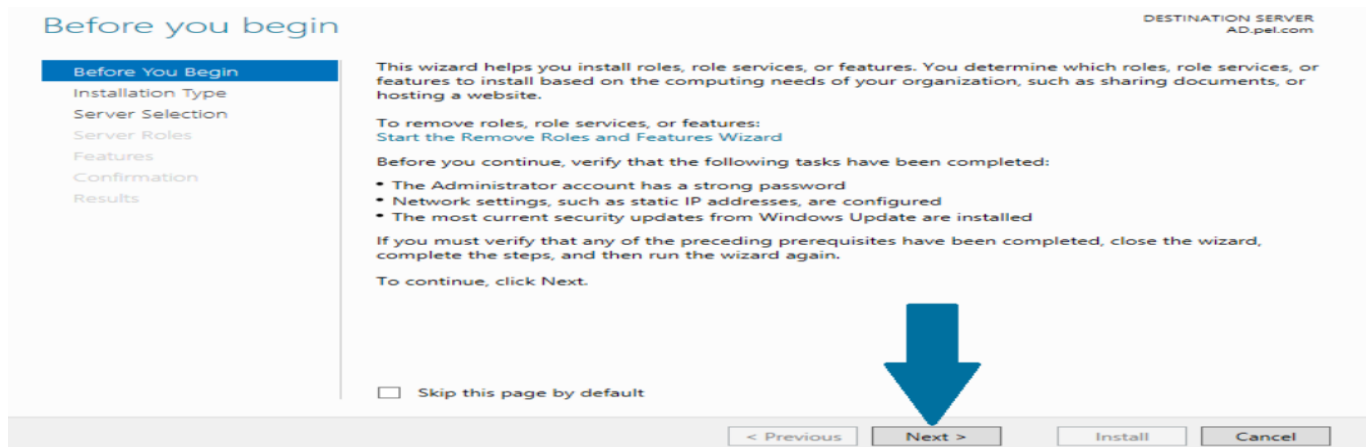
When its done you will be notified and required to reboot your PC.



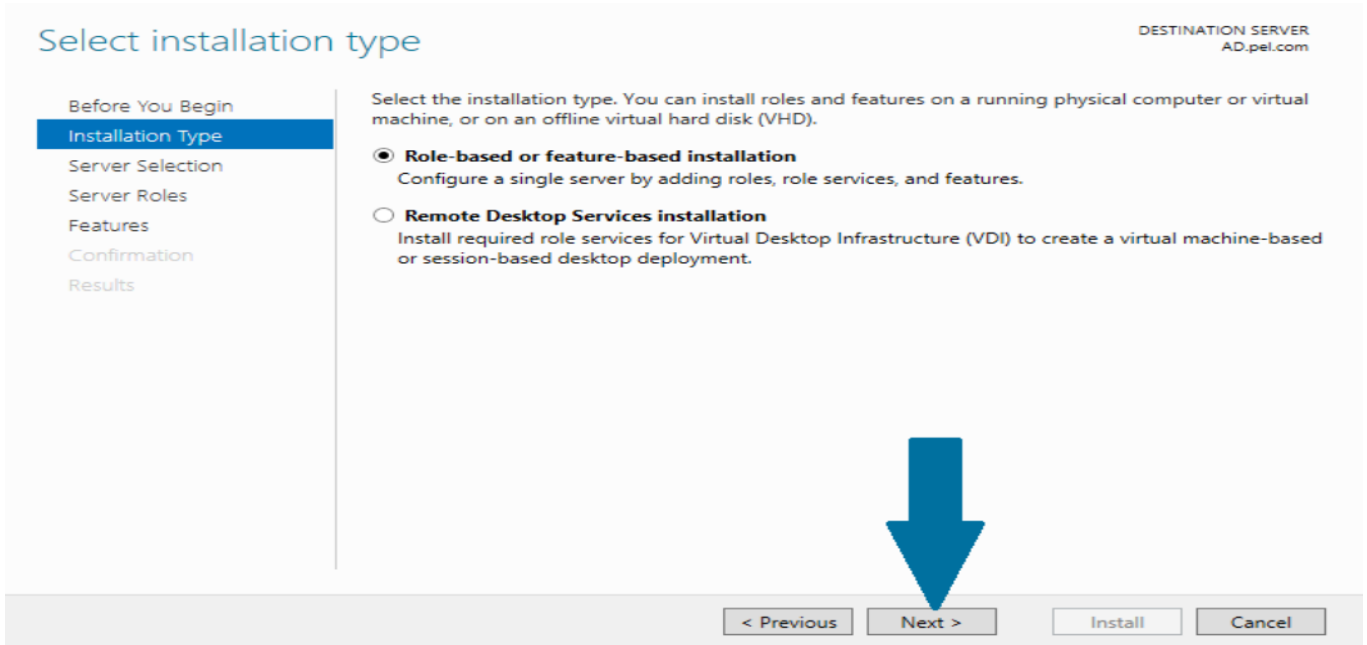
18.2- Active directory on windows server 2012

start "Server Manager" Choose "Add roles and features" Click through the wizard until "Features"

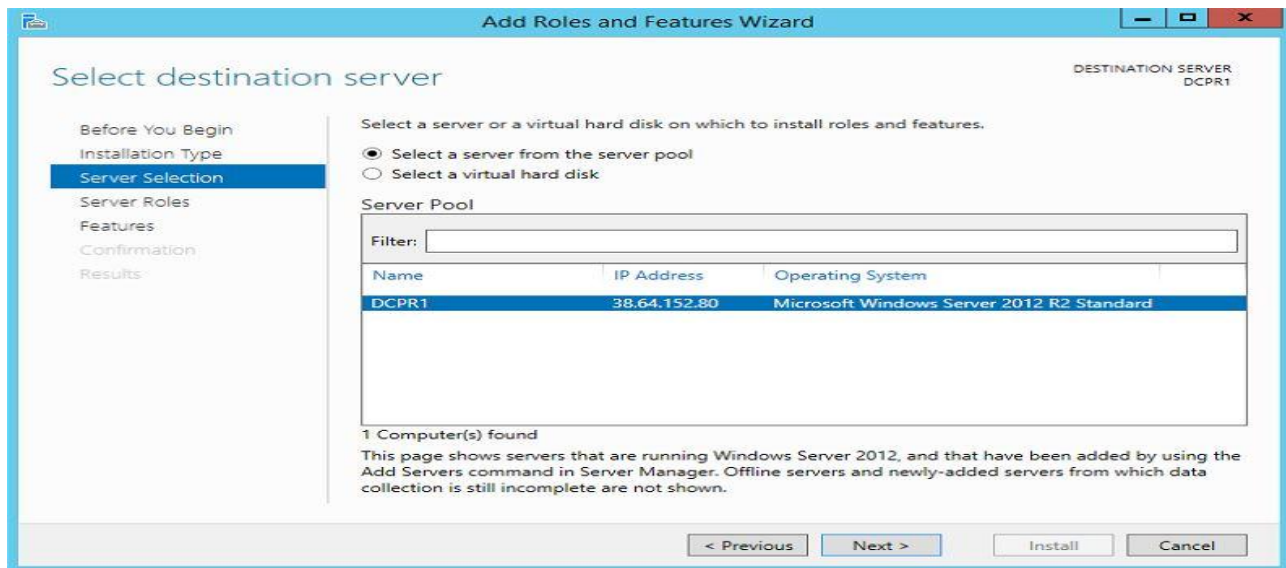
Go to "Remote Serer Administration Tools" and expand it Select "AD DS and AD LDS Tools"



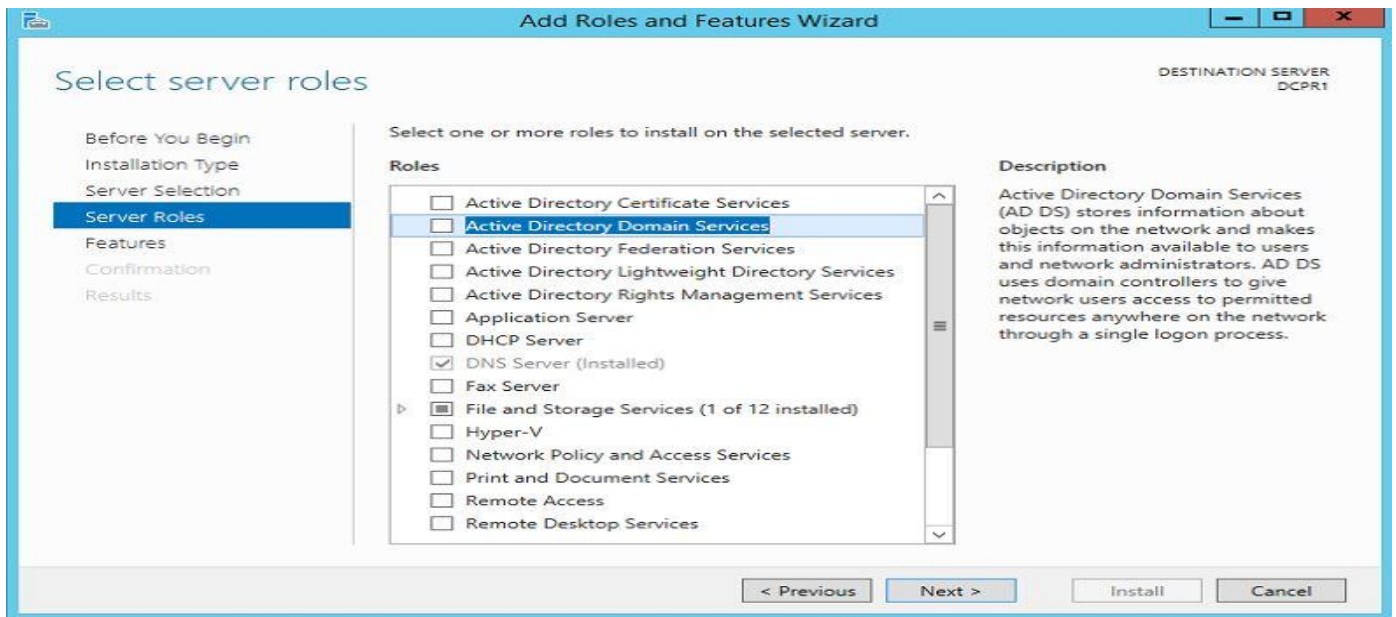
In next window keep "Role-based or feature-based installation" default selection and click on next.



In next window we can select which server to install role. In our case it will be local. So keep the default selection and click on next.



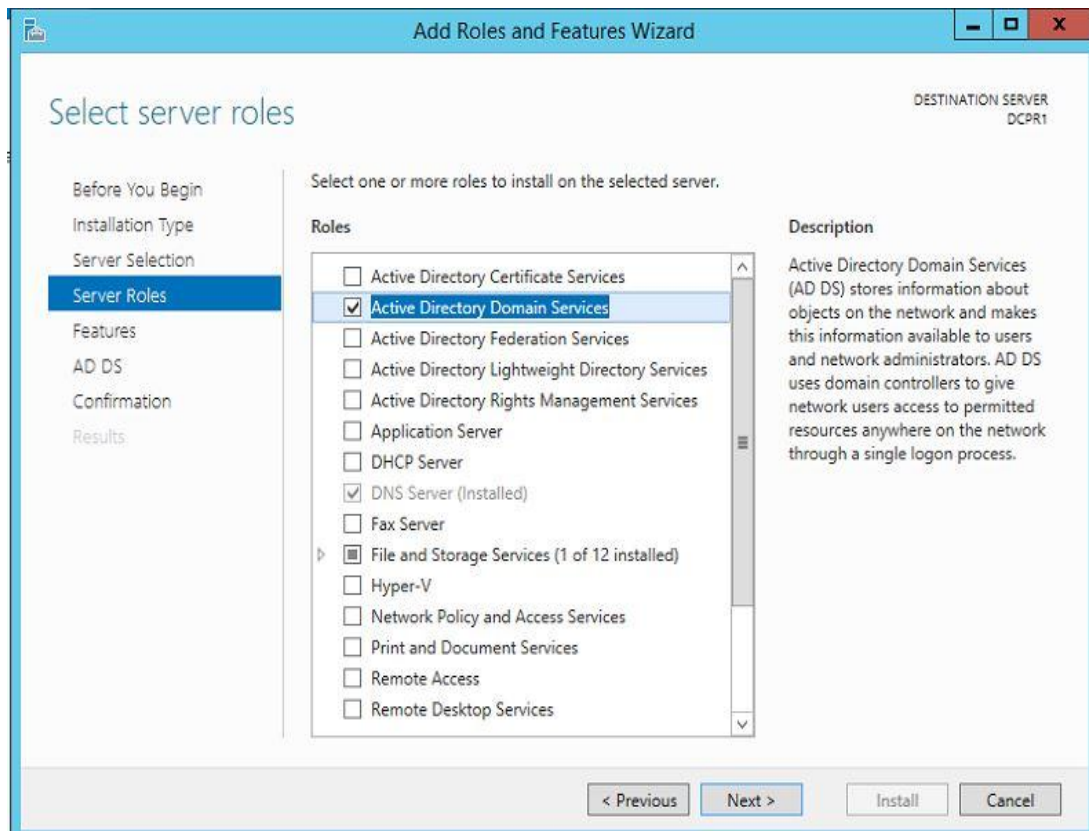
In next window it gives option to select the roles. select and click on tick box "Active Directory Domain Services"



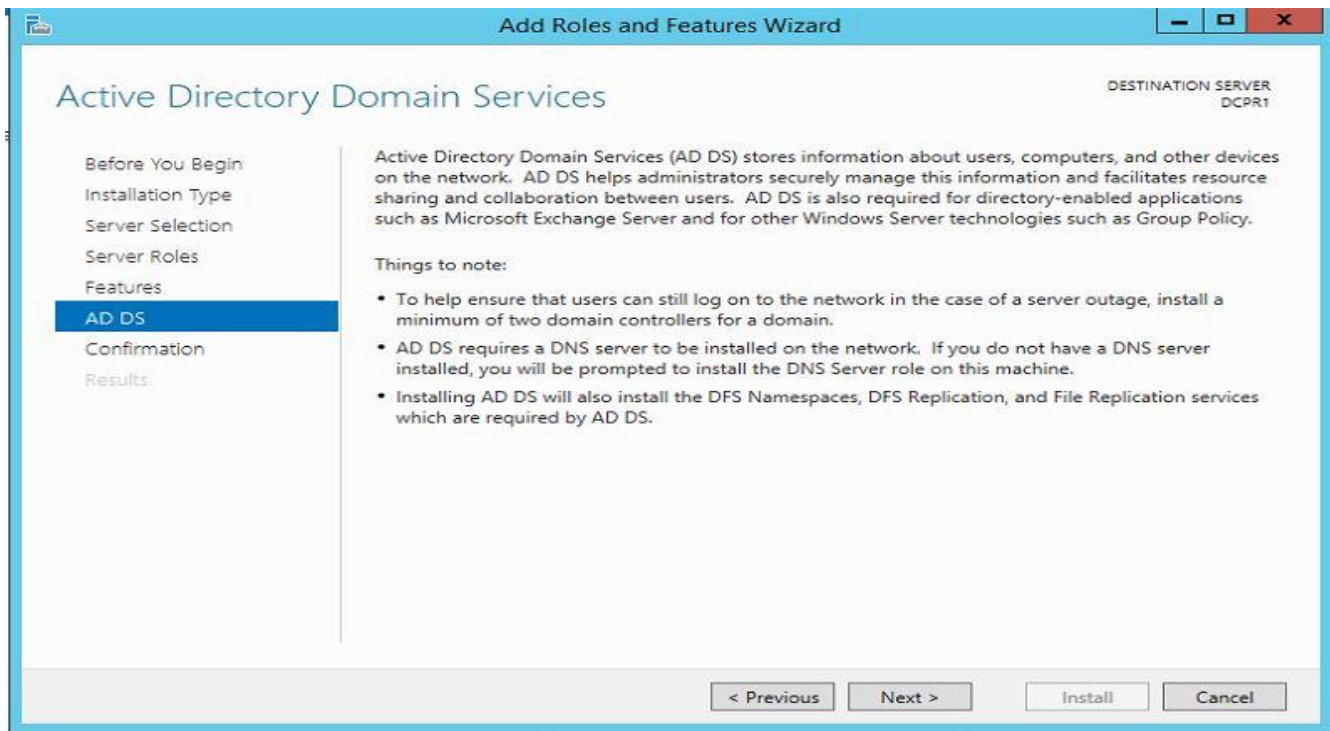
then it will prompt window to indicate the additional feature installations related to selected role. click on "Add Features" to continue.



Then in next window click on next to continue



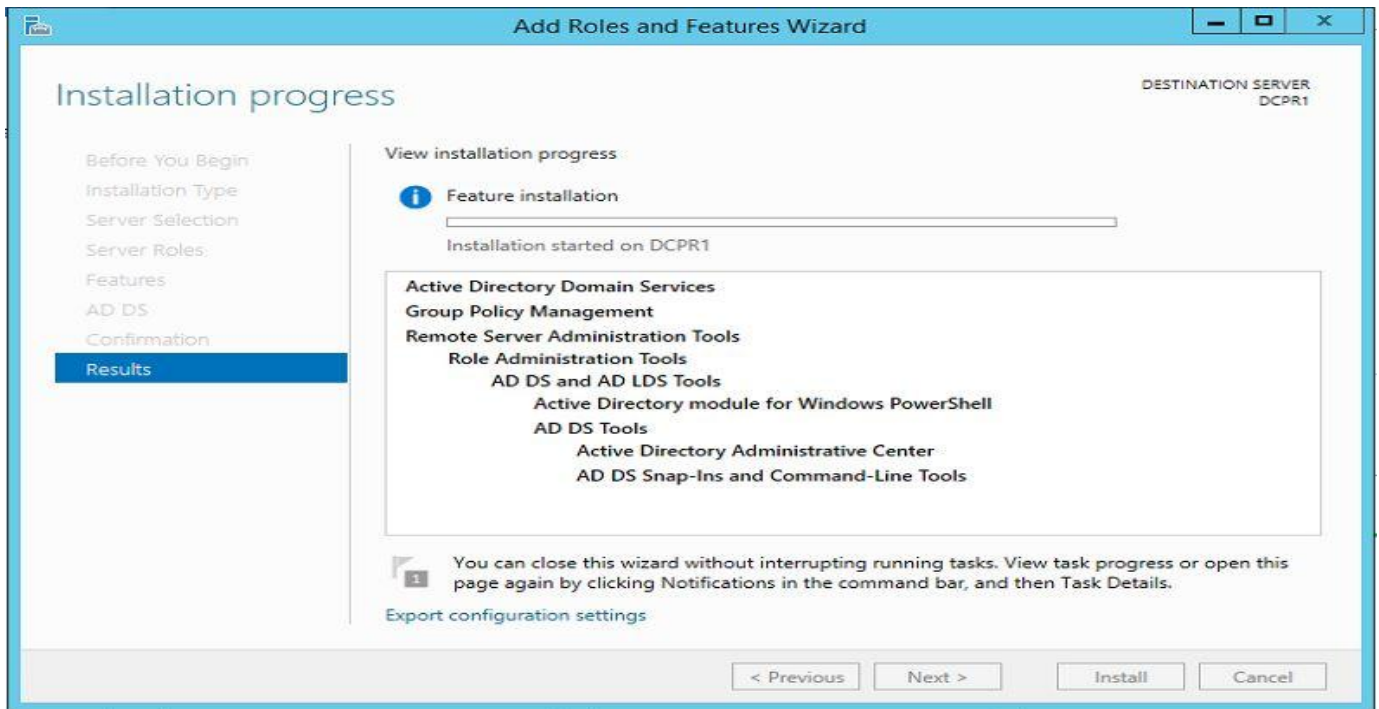
In next window it give brief description about the AD service. click on next to continue.



In next window it gives brief about the installation. click on "install" to start the installation.

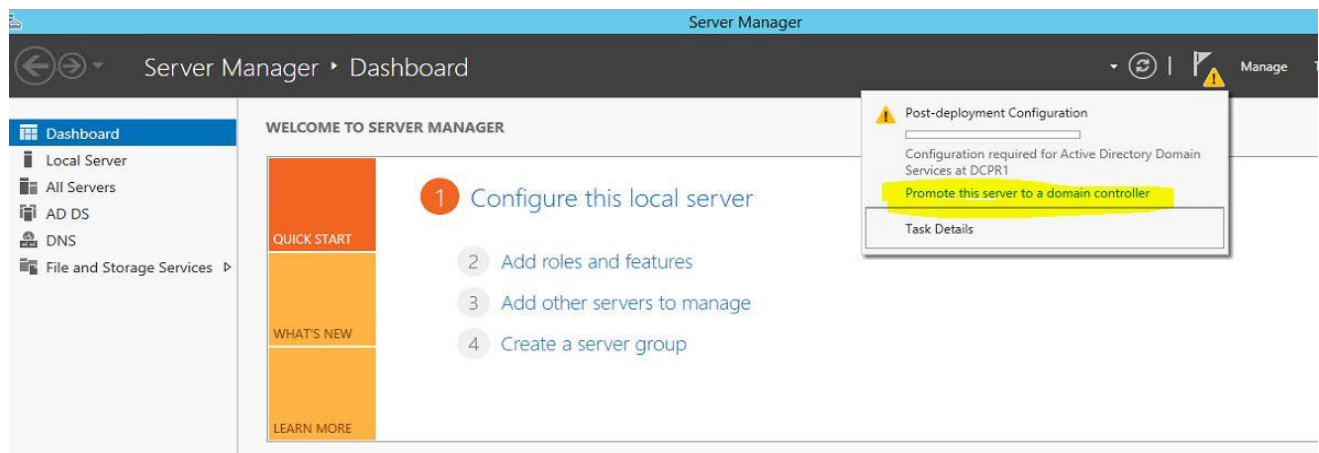


In next window it will begins the service install and we have to wait till it finish.

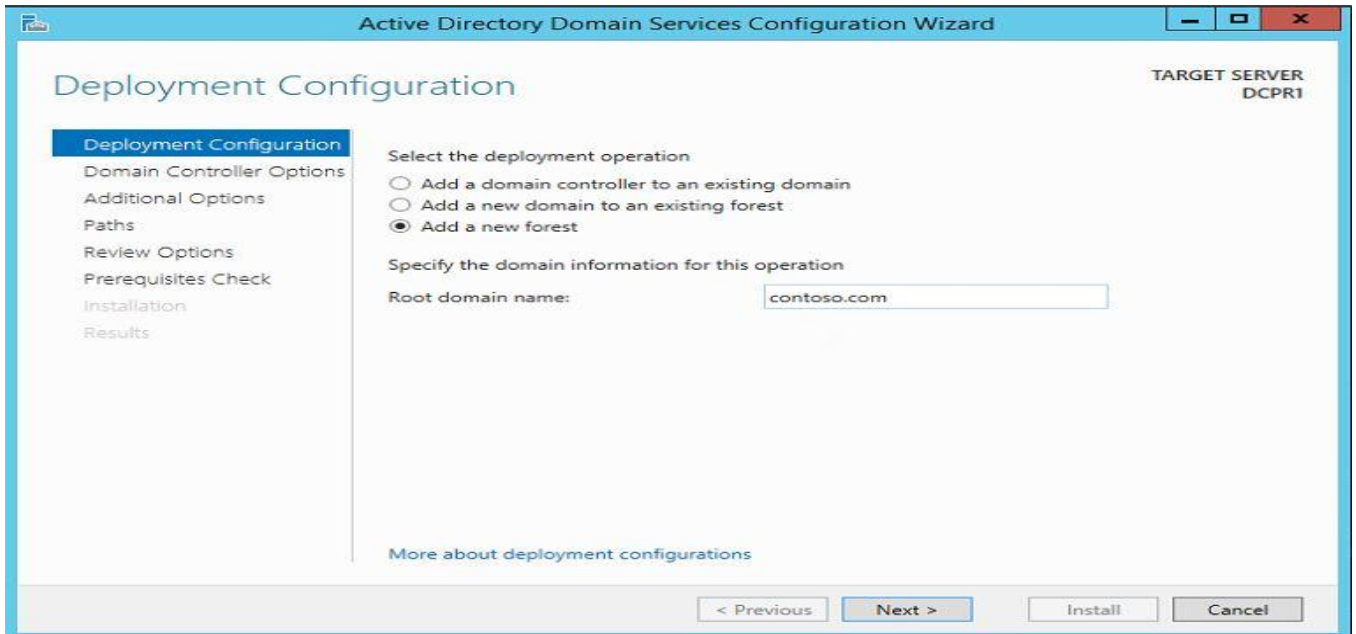


Once it finish click on "close" to exit from the wizard. then next step is to reboot the server to complete the installation

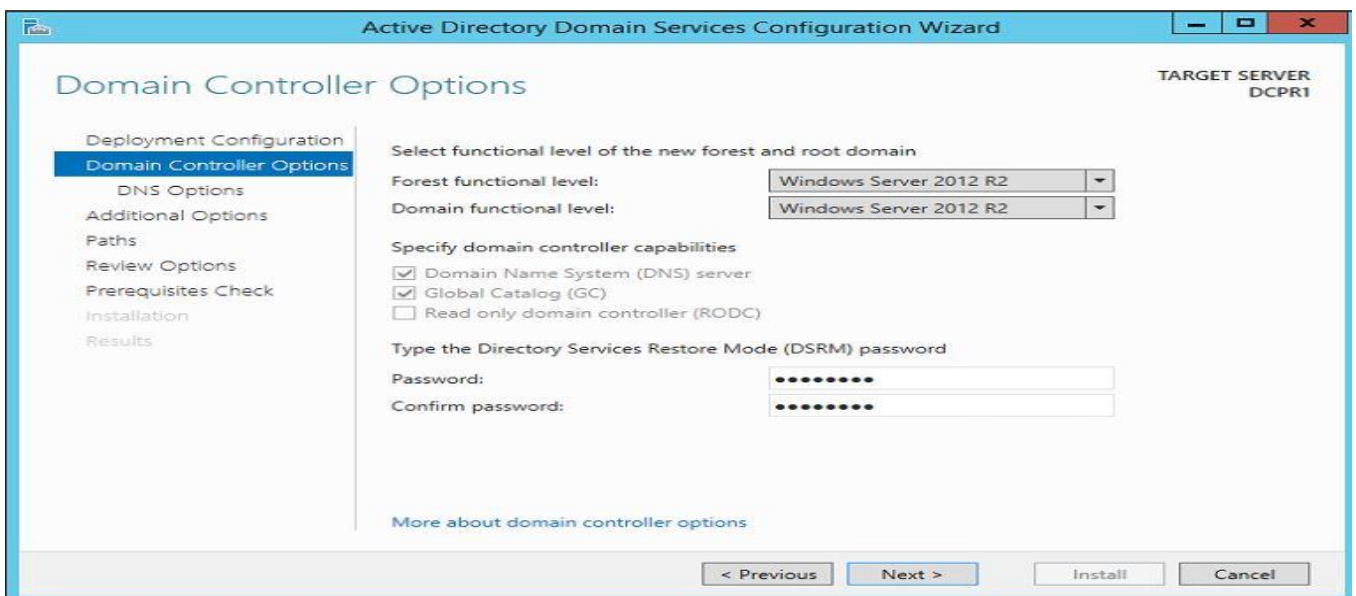
After that completes we need to start on the DC setup. to start that open the "Server Manager" and click Task flag on right hand corner. then it will list option as below picture. click on "promote this server to a domain controller" option (highlighted with yellow in picture)



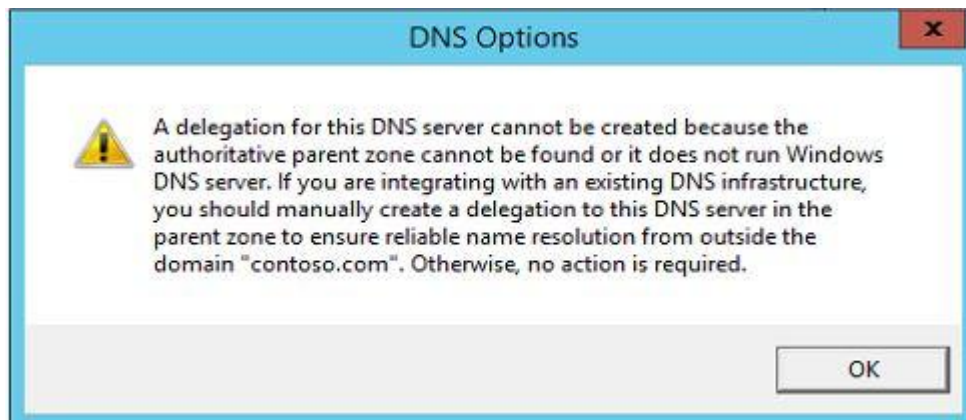
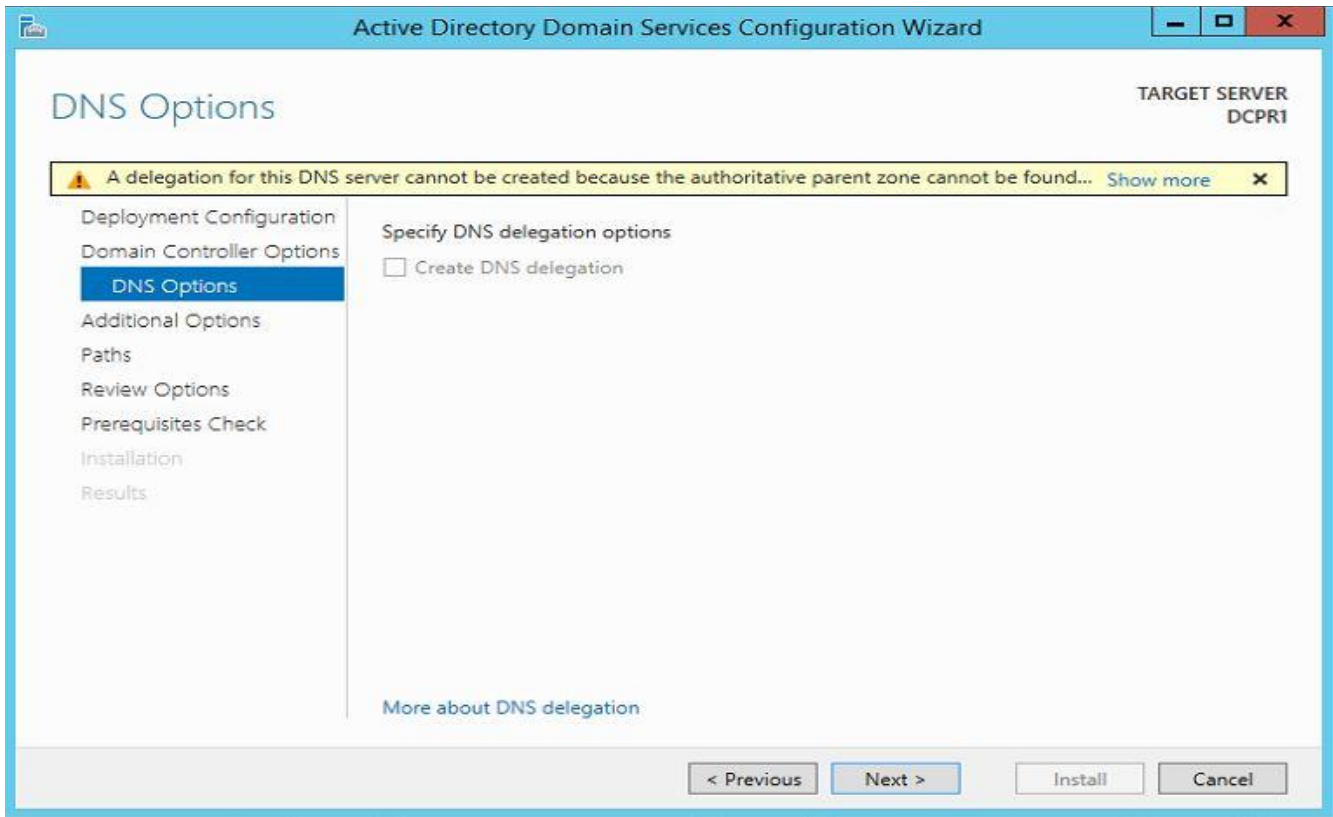
Then it starts the DCPROMO wizard. on the first window since its going to be new forest i have selected option "Add a new forest" and i typed the domain name "contoso.com" which i will be using on the forest. once fill the info click on "next" to continue.



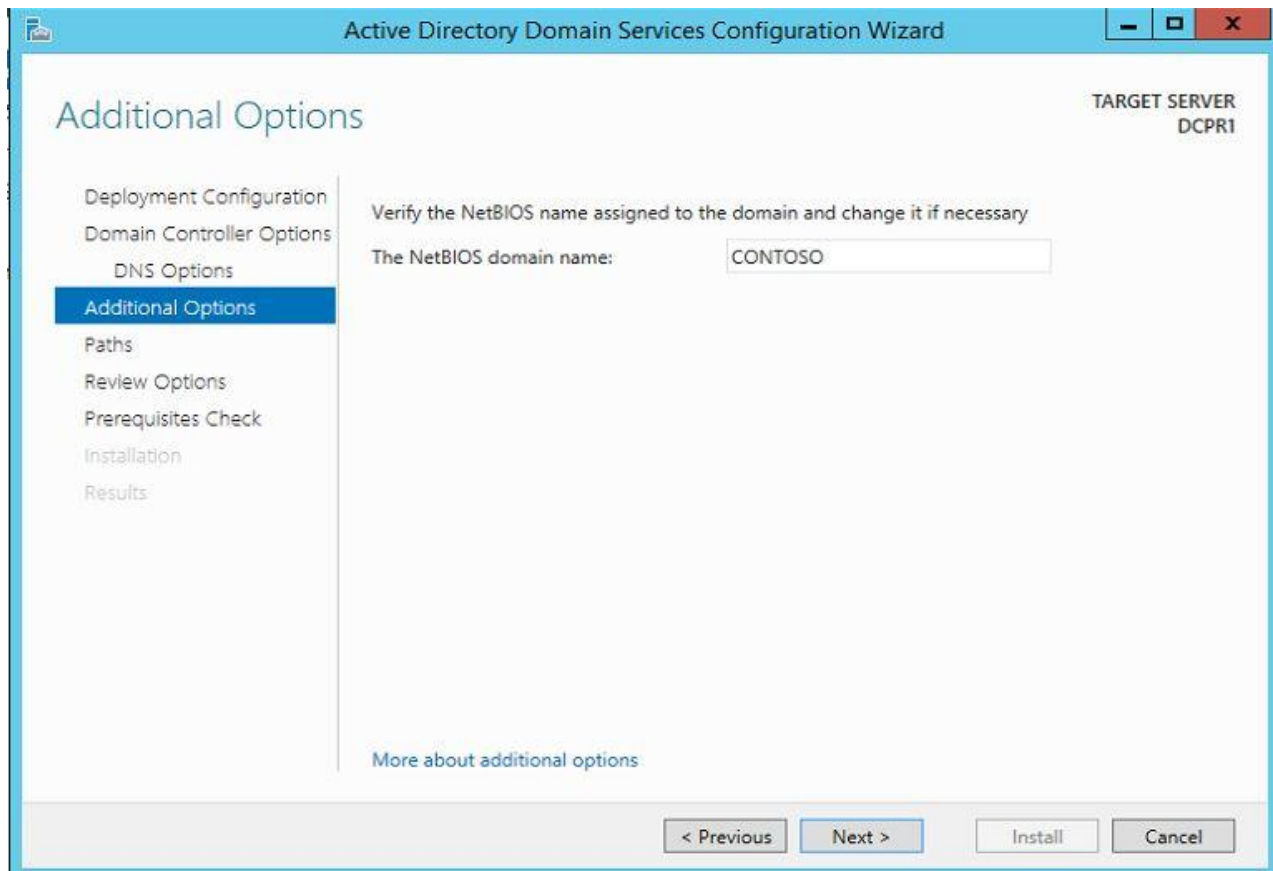
In next window we can select the forest and domain functional levels. i will keep it default. then in domain controller capabilities its by default selected DNS server and Global Catalog as its first DC in the forest. then we need to defined password to use in DC recovery. click on next to continue.



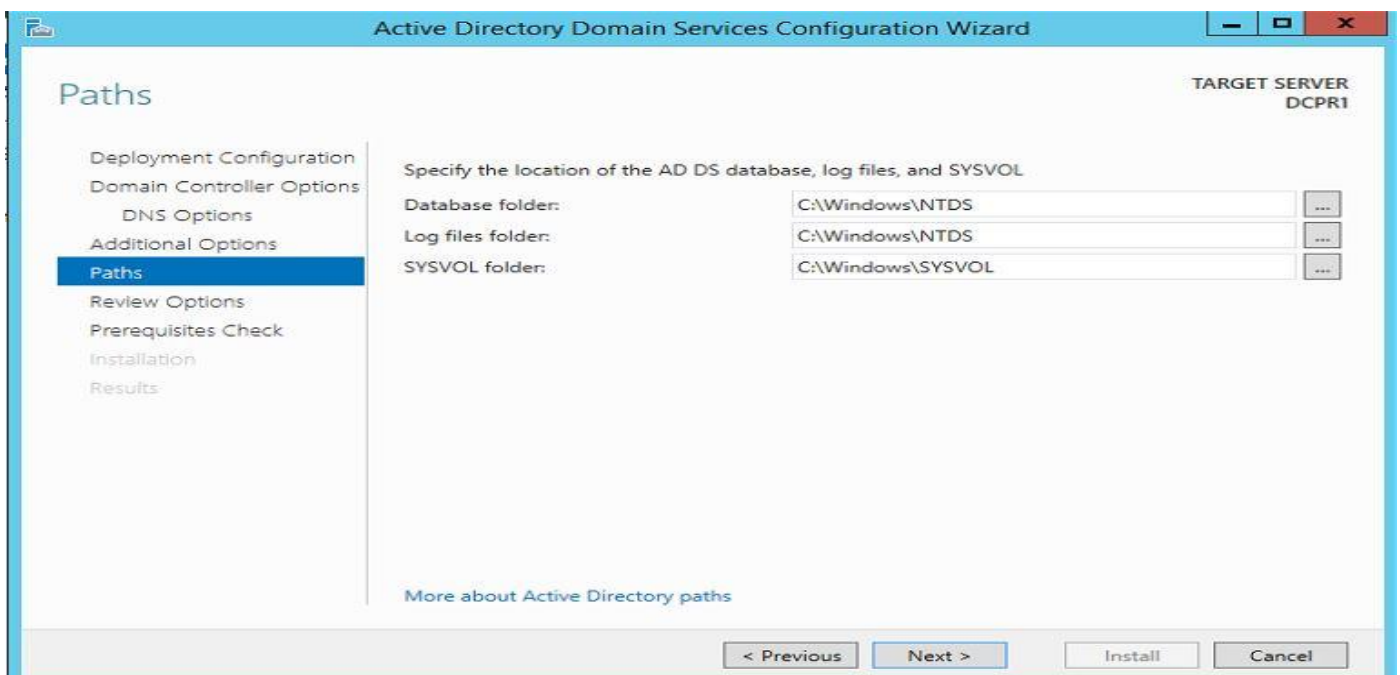
In next window it will give following error but it can be ignore. click on next to continue.



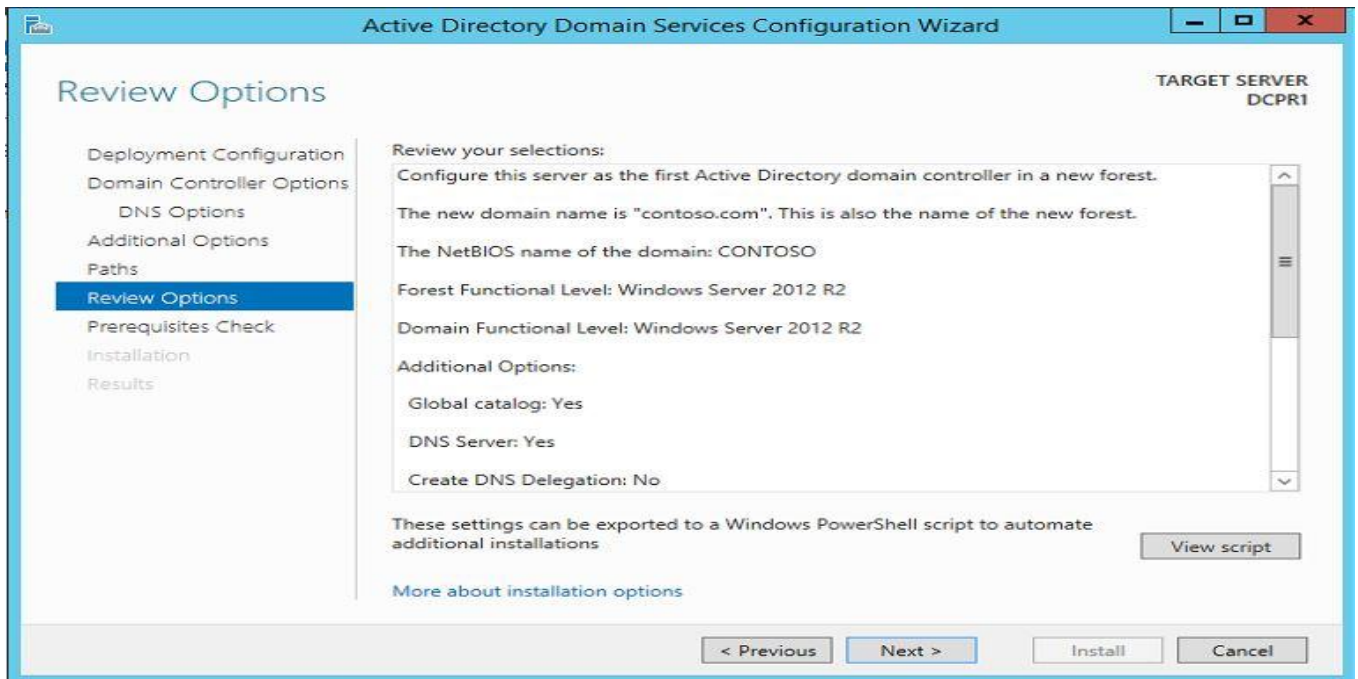
In next window it ask for the netbios name. we can keep it default and click on next to continue.



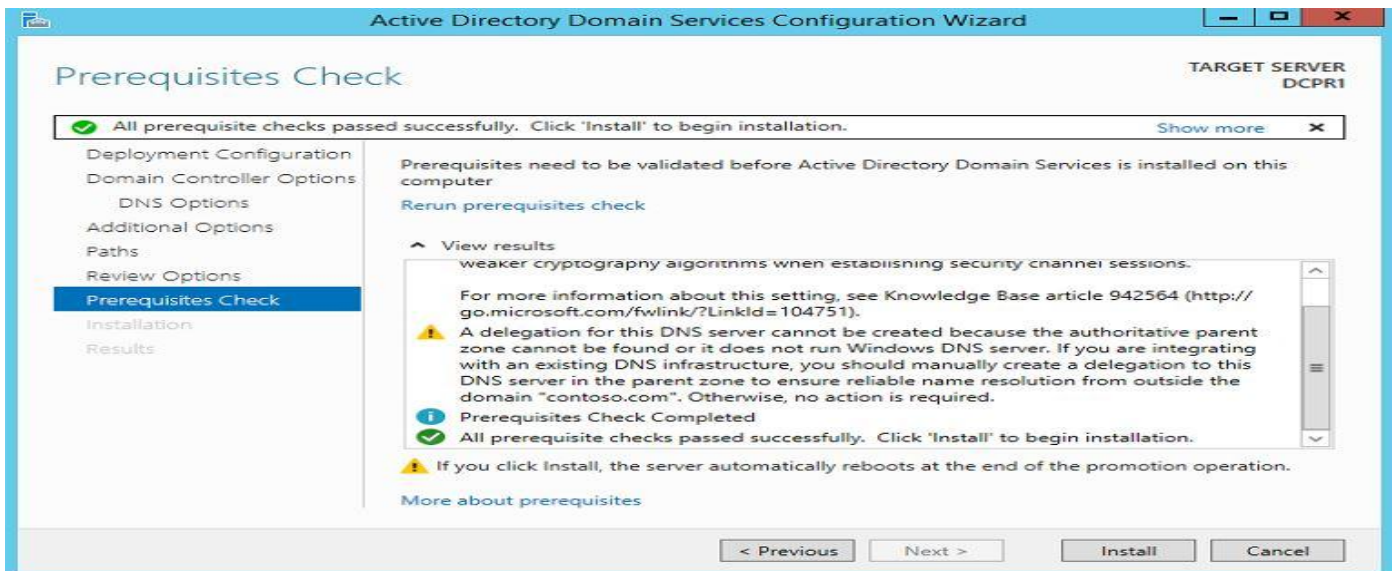
In next window it give option to change file paths for AD database, log files and SYSVOL files. we can change the paths or keep them defaults. once changes are done click on next to continue.



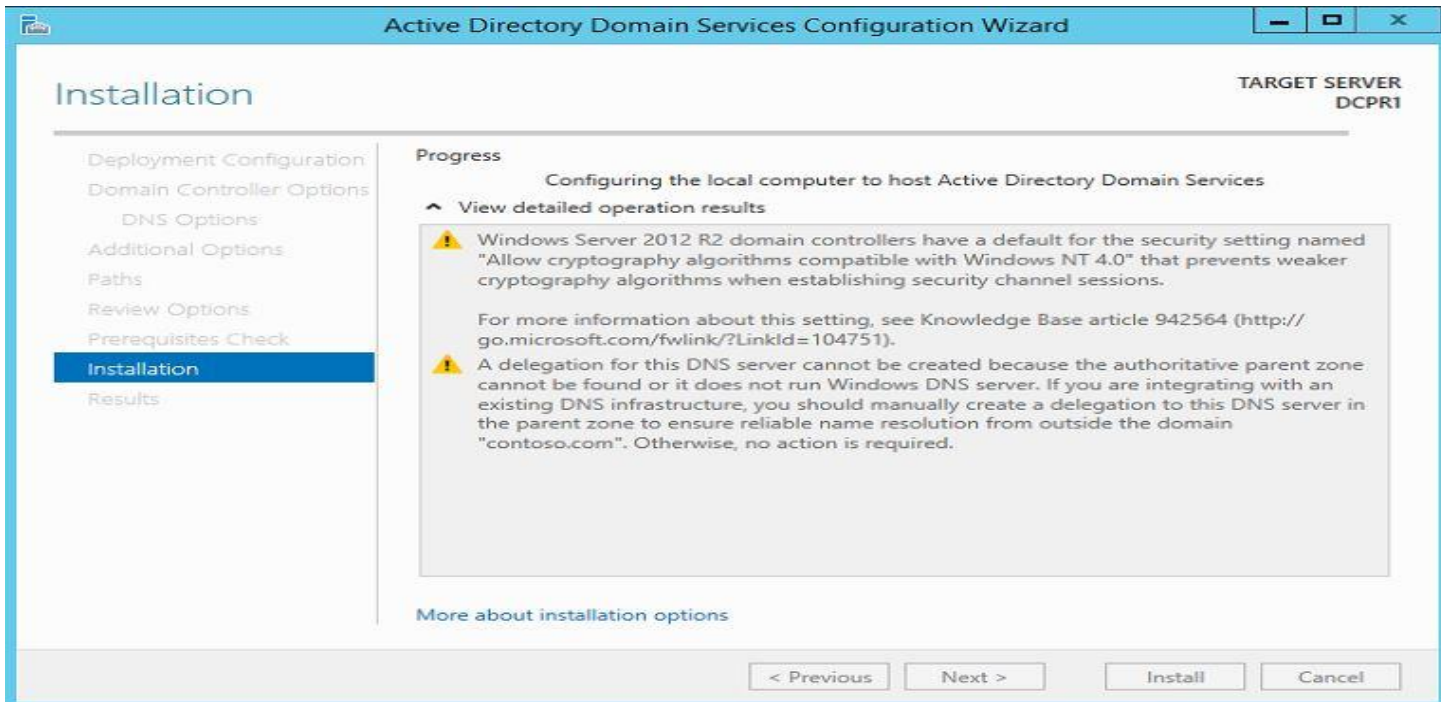
In next window it gives description about the installation. click on next to continue.



In next window it will run system check and verify system is compatible with the selected installation. once test completes successfully click on install button to begin the installation. if its passes any critical errors those needs to be address before the installation begin.



then it will start the install and we need to wait till it finishes.

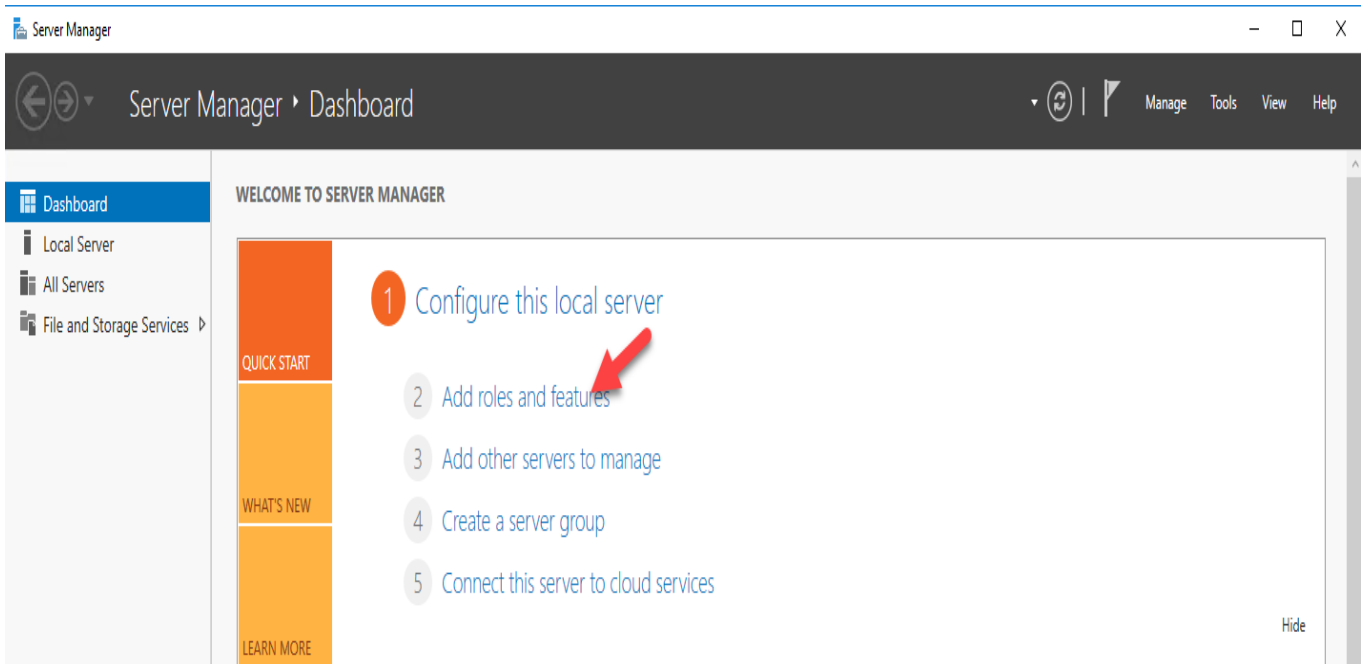


Once its complete the install it will automatically reboot the server.

18.3- Install active directory windows server 2016

تحميل active directory داخل windows server 2016

Then on server manager click on add roles and features



Before you begin

Before You Begin

- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

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

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

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

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

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

To continue, click Next.

Skip this page by default

< Previous

Next >

Install

Cancel

Select installation type

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

- Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.
- Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous

Next >

Install

Cancel

Select destination server

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

- Select a server from the server pool
 Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
REBELTEST-PDC01		Microsoft Windows Server 2016 Datacenter

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous

Next >

Install

Cancel

Select server roles

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

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

Roles

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

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

< Previous

Next >

Install

Cancel

Select server roles

- Before You Begin
- Installation Type
- Server Selection
- Server Roles**
- Features
- Confirmation
- Results

Add Roles and Features Wizard

Add features that are required for Active Directory Domain Services?

You cannot install Active Directory Domain Services unless the following role services or features are also installed.

- [Tools] Group Policy Management
- ▲ Remote Server Administration Tools
 - ▲ Role Administration Tools
 - ▲ AD DS and AD LDS Tools
 - Active Directory module for Windows PowerShell
 - ▲ AD DS Tools
 - [Tools] Active Directory Administrative Center
 - [Tools] AD DS Snap-Ins and Command-Line Tools

Include management tools (if applicable)

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

-

Select server roles

- Before You Begin
- Installation Type
- Server Selection
- Server Roles**
- Features
- AD DS
- Confirmation
- Results

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

Roles

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

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

-

Add Roles and Features Wizard

DESTINATION SERVER
REBELTEST-PDC01

Select features

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

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

Features	Description
<input checked="" type="checkbox"/> .NET Framework 3.5 Features (1 of 3 installed)	.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
<input checked="" type="checkbox"/> .NET Framework 4.6 Features (2 of 7 installed)	
<input type="checkbox"/> Background Intelligent Transfer Service (BITS)	
<input type="checkbox"/> BitLocker Drive Encryption	
<input type="checkbox"/> BitLocker Network Unlock	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Client for NFS	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Direct Play	
<input type="checkbox"/> Enhanced Storage	
<input type="checkbox"/> Failover Clustering	
<input checked="" type="checkbox"/> Group Policy Management	
<input type="checkbox"/> Host Guardian Hyper-V Support	
<input type="checkbox"/> I/O Quality of Service	
<input type="checkbox"/> IIS Hostable Web Core	
<input type="checkbox"/> Internet Printing Client	
<input type="checkbox"/> IP Address Management (IPAM) Server	
<input type="checkbox"/> iSNS Server service	

< Previous **Next >** Install Cancel

Add Roles and Features Wizard

DESTINATION SERVER
REBELTEST-PDC01


Active Directory Domain Services

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

 Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
[Learn more about Azure Active Directory](#)
[Configure Office 365 with Azure Active Directory Connect](#)

< Previous **Next >** Install Cancel

Installation progress

DESTINATION SERVER
REBELTEST-PDC01

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

View installation progress

i Feature installation

Installation started on REBELTEST-PDC01

Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

i You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)

< Previous

Next >

Close

Cancel

Installation progress

DESTINATION SERVER
REBELTEST-PDC01

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

View installation progress

i Feature installation

Configuration required. Installation succeeded on REBELTEST-PDC01.

Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

i You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

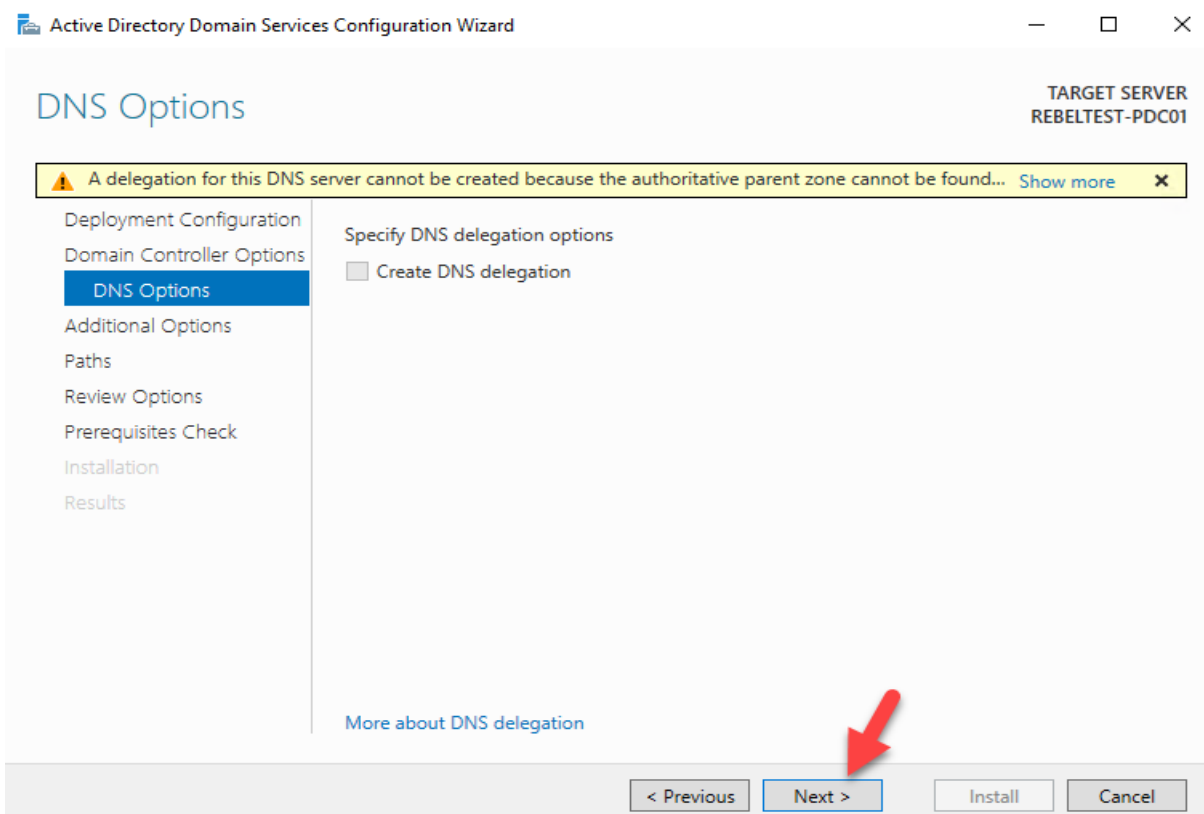
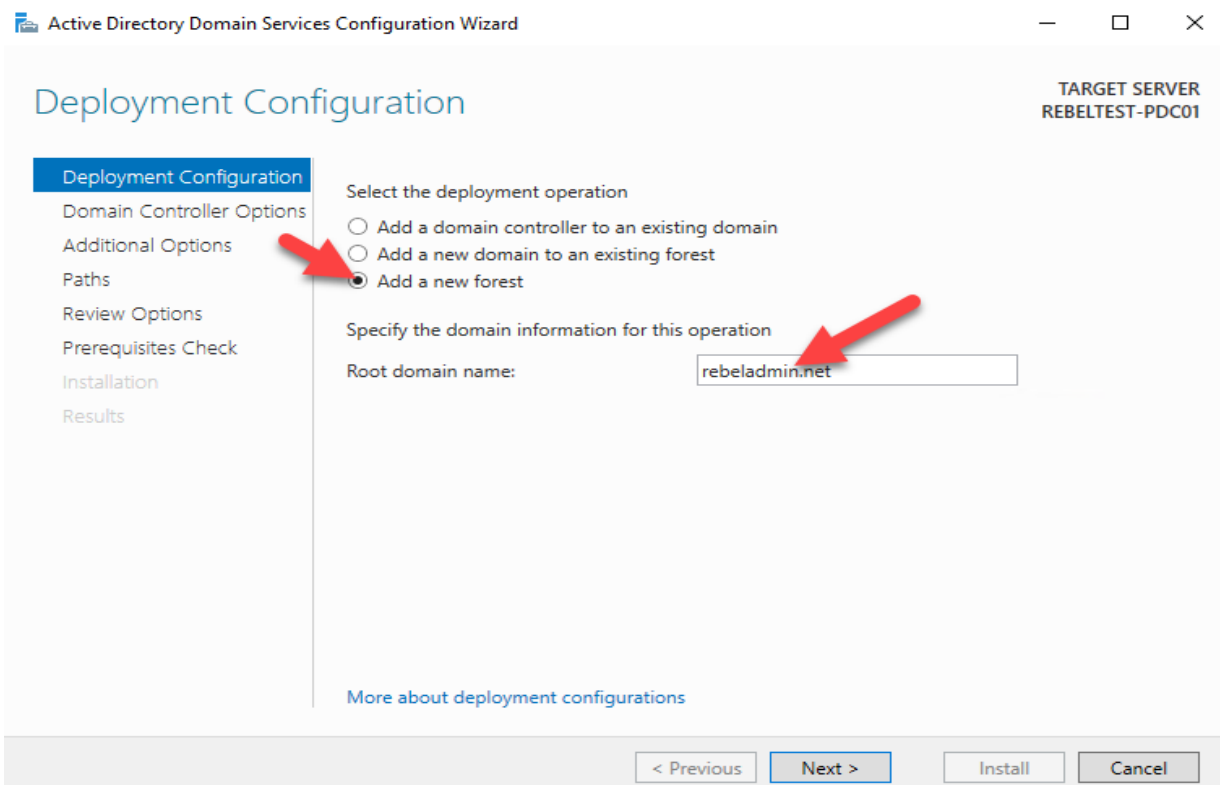
[Export configuration settings](#)

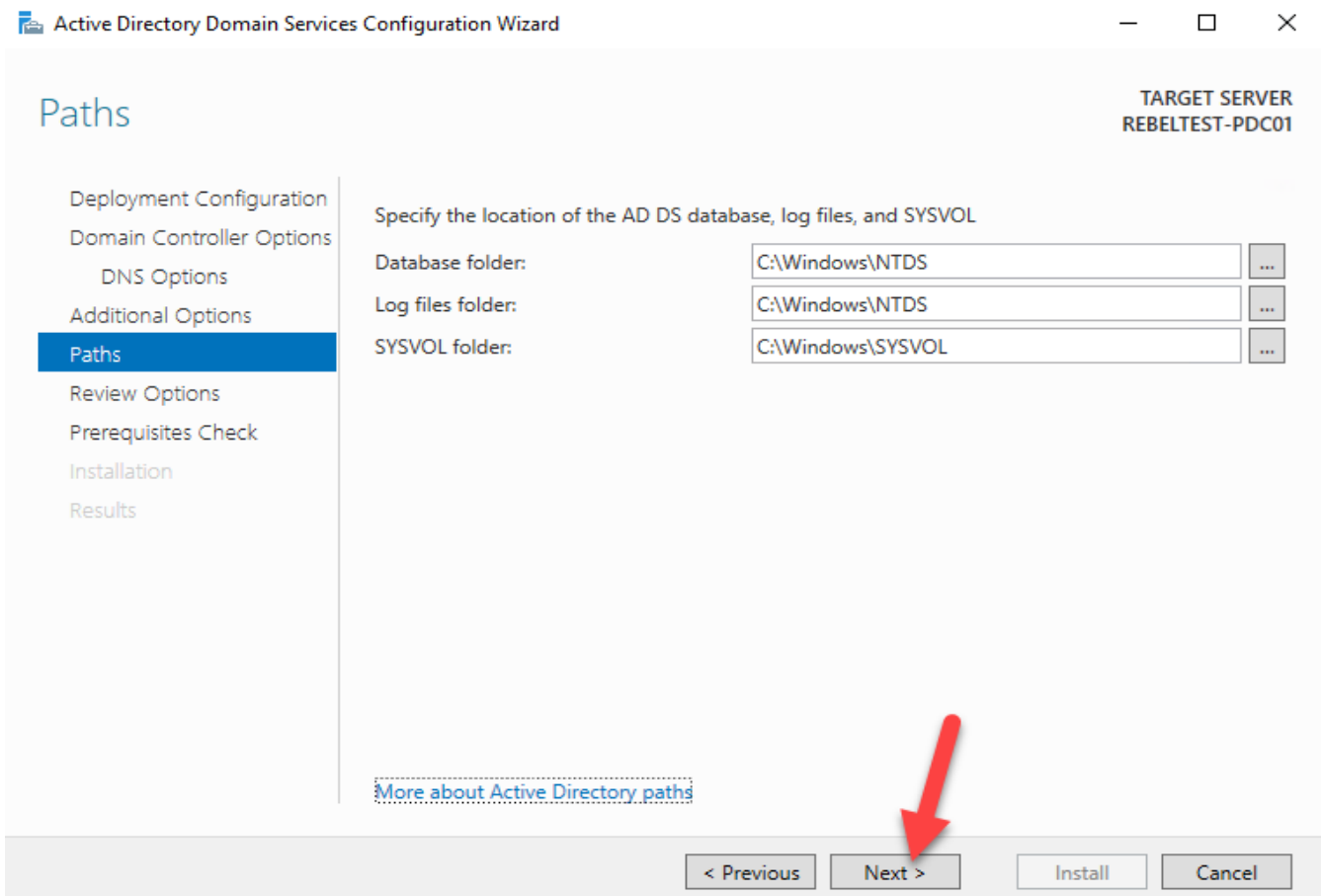
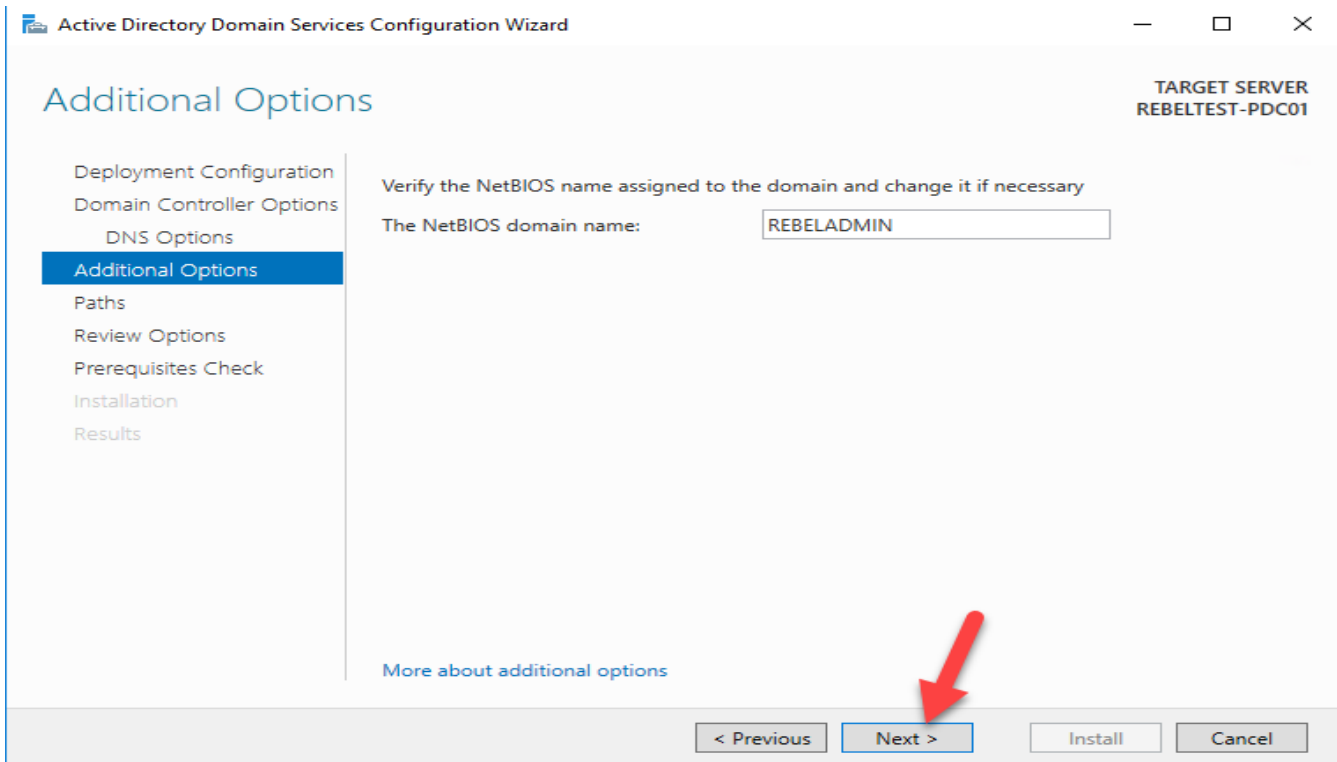
< Previous

Next >

Close

Cancel





Review Options

TARGET SERVER
REBELTEST-PDC01

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

Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "rebeladmin.net". This is also the name of the new forest.

The NetBIOS name of the domain: REBELADMIN

Forest Functional Level: Windows Server 2016

Domain Functional Level: Windows Server 2016

Additional Options:

- Global catalog: Yes
- DNS Server: Yes
- Create DNS Delegation: No

These settings can be exported to a Windows PowerShell script to automate additional installations

View script

[More about installation options](#)

< Previous

Next >

Install

Cancel

Prerequisites Check

TARGET SERVER
REBELTEST-PDC01

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

Show more

- 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

- ⚠ Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).
- ⚠ 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 "rebeladmin.net". 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

Installation TARGET SERVER
REBELTEST-PDC01

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

Progress
Checking if Group Policy Management Console needs to be installed...

View detailed operation results

⚠ Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).

⚠ 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 "rebeladmin.net". Otherwise, no action is required.

[More about installation options](#)

< Previous Next > Install Cancel

10- Add object (users,group,OU,computers) in active directory

إضافة (users,group,OU,computers) داخل active directory

الوحدة التنظيمية (OU) organizational unit وهي تشبى المجلد أي بمعنى انها تقوم بتنظيم Active directory الي مجموعة من OUs على حسب الاقسام الموجود في ال domain وذلك تسهل عملية البحث والاضافة والتعديل داخل Active directory.

المجموعة group وهي عبارة عن تجمع مجموعة من المستخدمين users يشتركون في طبيعة العمل فبدل من تطبيق امر معين على كل مستخدم على حد نقوم بتطبيق الامر على المجموعة فيتم تطبيق هذا العمل بشكل تلقائي على جميع المستخدمين داخل هذه المجموعة.

organizational unit (OU). An OU can contain computers, users, user groups, and other network objects. Usually, an OU is used for the purpose of grouping things for administrative purposes, such as delegating administrative rights and assigning policies to the group as a single unit.

Group	User/ Session	Description
Account Operators		<p>A built-in group that exists only on domain controllers. By default, the group has no members. By default, Account Operators have permission to create, modify, and delete accounts for users, groups, and computers in all containers and organizational units (OUs) of Active Directory except the Builtin container and the Domain Controllers OU. Account Operators do not have permission to modify the Administrators and Domain Admins groups, nor do they have permission to modify the accounts for members of those groups.</p>
	Administrator	<p>A user account for the system administrator. This account is the first account created during operating system installation. The account cannot be deleted or locked out. It is a member of the Administrators group and cannot be removed from that group.</p>
Administrators		<p>A built-in group . After the initial</p>

installation of the operating system, the only member of the group is the Administrator account. When a computer joins a domain, the Domain Admins group is added to the Administrators group. When a server becomes a domain controller, the Enterprise Admins group also is added to the Administrators group. The Administrators group has built-in capabilities that give its members full control over the system. The group is the default owner of any object that is created by a member of the group.

Anonymous

A user who has logged on anonymously.

Authenticated Users

A group that includes all users whose identities were authenticated when they logged on. Membership is controlled by the operating system.

Backup Operators

A built-in group. By default, the group has no members. Backup Operators can back up and restore all files on a computer, regardless of the permissions

that protect those files. Backup Operators also can log on to the computer and shut it down.

Batch

A group that implicitly includes all users who have logged on through a batch queue facility such as task scheduler jobs. Membership is controlled by the operating system.

Cert Publishers

A global group that includes all computers that are running an enterprise certificate authority. Cert Publishers are authorized to publish certificates for User objects in Active Directory.

Cert Server Admins

Certificate Authority Administrators - authorized to administer certificates for User objects in Active Directory.
(Domain Local)

Cert Requesters

Members can request certificates
(Domain Local)

Creator Group

A placeholder in an inheritable ACE.

When the ACE is inherited, the system replaces this SID with the SID for the primary group of the object's current owner. The primary group is used only by the POSIX subsystem.

Creator
Owner

A placeholder in an inheritable access control entry (ACE). When the ACE is inherited, the system replaces this SID with the SID for the object's current owner.

Dialup

A group that implicitly includes all users who are logged on to the system through a dial-up connection. Membership is controlled by the operating system.

DnsAdmins
(installed with DNS)

Members of this group have administrative access to the DNS Server service. This group has no default members.

DnsUpdateProxy
(installed with DNS)

Members of this group are DNS clients that can perform dynamic updates on behalf of other clients, such as DHCP servers. This group has no default

members.

Domain Admins

A global group whose members are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers.

Domain Admins is the default owner of any object that is created in the domain's Active Directory by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.

Domain Computers

A global group that includes all computers that have joined the domain, excluding domain controllers.

Domain Controllers

A global group that includes all domain controllers in the domain. New domain controllers are added to this group automatically.

Domain Guests

A global group that, by default, has only one member, the domain's built-in Guest

account.

Domain Users

A global group that, by default, includes all user accounts in a domain. When you create a user account in a domain, it is added to this group automatically.

Enterprise Admins

A group that exists only in the root domain of an Active Directory forest of domains. It is a universal group if the domain is in native mode, a global group if the domain is in mixed mode. The group is authorized to make forest-wide changes in Active Directory, such as adding child domains. By default, the only member of the group is the Administrator account for the forest root domain.

*Enterprise
Controllers*

A group that includes all domain controllers in an Active Directory service forest of domains. Membership is controlled by the operating system.

Everyone

A group that includes all users, even guests. Membership is controlled by the

operating system.

In Windows XP and later, the Anonymous Logon security group has been removed from the *Everyone* security group: see [Q278259](#) and the group policy [Let Everyone permissions apply to anonymous users](#)

Group Policy
Creators Owners

A global group that is authorized to create new Group Policy objects in Active Directory. By default, the only member of the group is Administrator. The default owner of a new Group Policy object is usually the user who created it. If the user is a member of Administrators or Domain Admins, all objects that are created by the user are owned by the group. Owners have full control of the objects they own.

Guest

A user account for people who do not have individual accounts. This user account does not require a password. By default, the Guest account is disabled.

Guests	A built-in group. By default, the only member is the Guest account. The Guests group allows occasional or one-time users to log on with limited privileges to a computer's built-in Guest account.
HelpServicesGroup	XP - Group for the Help and Support Center
<i>Interactive</i>	A group that includes all users who have logged on interactively. Membership is controlled by the operating system.
KRBTGT	A service account that is used by the Key Distribution Center (KDC) service.
<i>Local System</i>	A service account that is used by the operating system.
<i>Network</i>	A group that implicitly includes all users who are logged on through a network connection. Membership is controlled by the operating system.
Network Configuration	Members of this group can make changes to TCP/IP settings and renew

Operators	and release TCP/IP addresses on domain controllers in the domain. This group has no default members.
<i>Nobody</i>	No security principal.
Performance Monitor Users	Members of this group can monitor performance counters on domain controllers in the domain, locally and from remote clients without being a member of the Administrators or Performance Log Users groups.
Performance Log Users	Members of this group can manage performance counters, logs and alerts on domain controllers in the domain, locally and from remote clients without being a member of the Administrators group.
Power Users	A built-in group. By default, the group has no members. This group does not exist on domain controllers. Power Users can create local users and groups; modify and delete accounts that they have created; and remove users from the

Power Users, Users, and Guests groups. Power Users also can install most applications; create, manage, and delete local printers; and create and delete file shares.

Pre-Windows 2000
Compatible Access

A backward compatibility group which allows read access on all users and groups in the domain. By default, the special identity Everyone is a member of this group. Add users to this group only if they are running Windows NT 4.0 or earlier.

Principal Self
or
Self

Principal Self
or
Self

A placeholder in an ACE on a user, group, or computer object in Active Directory. When you grant permissions to Principal Self, you grant them to the security principal represented by the object. During an access check, the operating system replaces the SID for Principal Self with the SID for the security principal represented by the object.

Print Operators

A built-in group that exists only on

domain controllers. By default, the only member is the Domain Users group. Print Operators can manage printers and document queues.

RAS and IAS Servers

Servers in this group are permitted access to the remote access properties of users. A domain local group . By default, this group has no members. Computers that are running the Routing and Remote Access service are added to the group automatically. Members of this group have access to certain properties of User objects, such as Read Account Restrictions, Read Logon Information, and Read Remote Access Information.

Remote Desktop Users

XP - Members in this group are granted the right to logon remotely

Replicator

In NT 4 domains, this group was called Replicators and is used by the directory replication service. In 2K/XP the group is present but is not used. Do not add users to this group.

Schema Admins

A group that exists only in the root domain of an Active Directory forest of domains. It is a universal group if the domain is in native mode , a global group if the domain is in mixed mode . The group is authorized to make schema changes in Active Directory. By default, the only member of the group is the Administrator account for the forest root domain. Because this group has significant power in the forest, add users with caution.

Server Operators

A built-in group that exists only on domain controllers. By default, the group has no members. Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back up and restore files; format the hard disk of the computer; and shut down the computer.

Service

A group that includes all security principals that have logged on as a service. Membership is controlled by the

operating system.

Terminal Server

Users

A group that includes all users who have logged on to a Terminal Services server. Membership is controlled by the operating system.

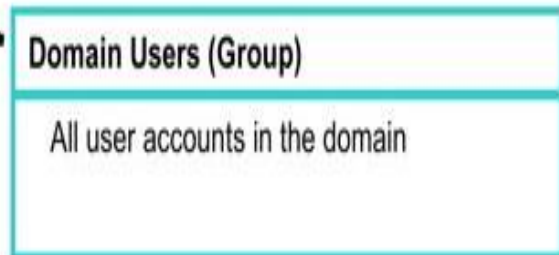
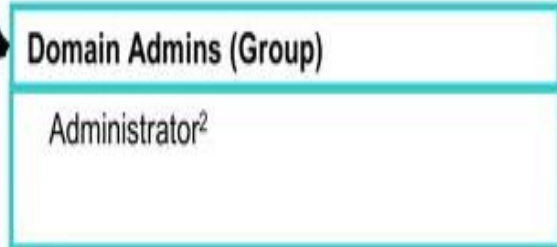
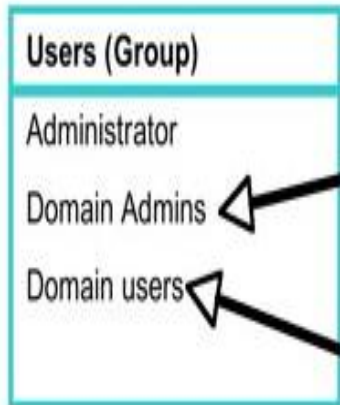
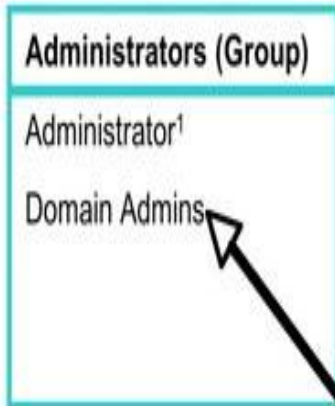
Users

A built-in group. After the initial installation of the operating system, the only member is the Authenticated Users group. When a computer joins a domain, the Domain Users group is added to the Users group on the computer. Users can perform tasks such as running applications, using local and network printers, shutting down the computer, and locking the computer. Users can install applications that only they are allowed to use if the installation program of the application supports per-user installation.

Default Admin Users and Groups:

----- Machine(s) -----

----- Domain -----



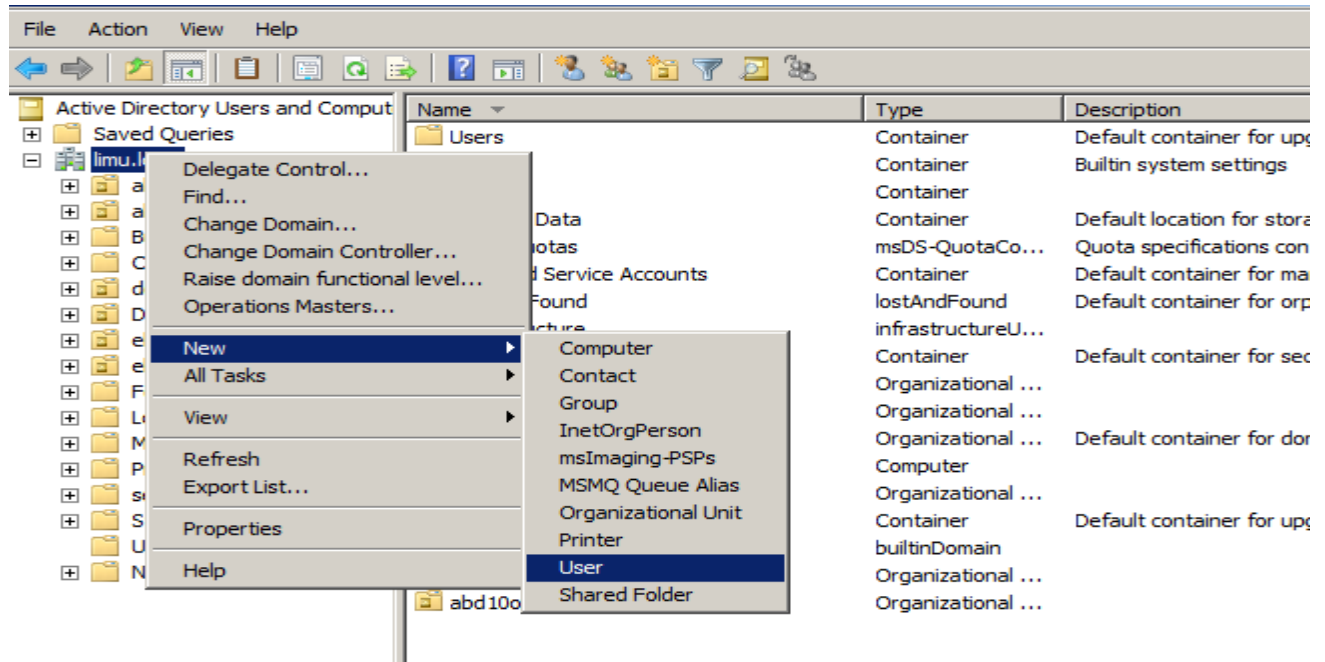
The arrows indicate automatic memberships that happen when a machine joins a domain.

1 = Local Administrator

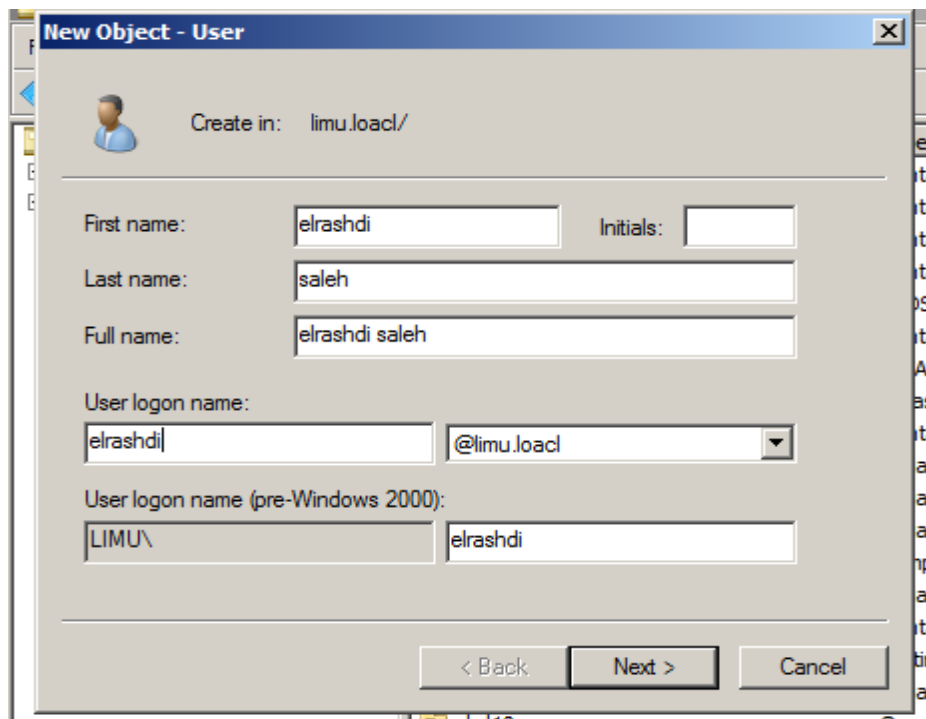
2 = Domain Administrator

19.1- Add objects (users,group,OU,computers) in active directory windows server 2008

إضافة (users,group,OU,computers) داخل active directory في windows server 2008



Create user

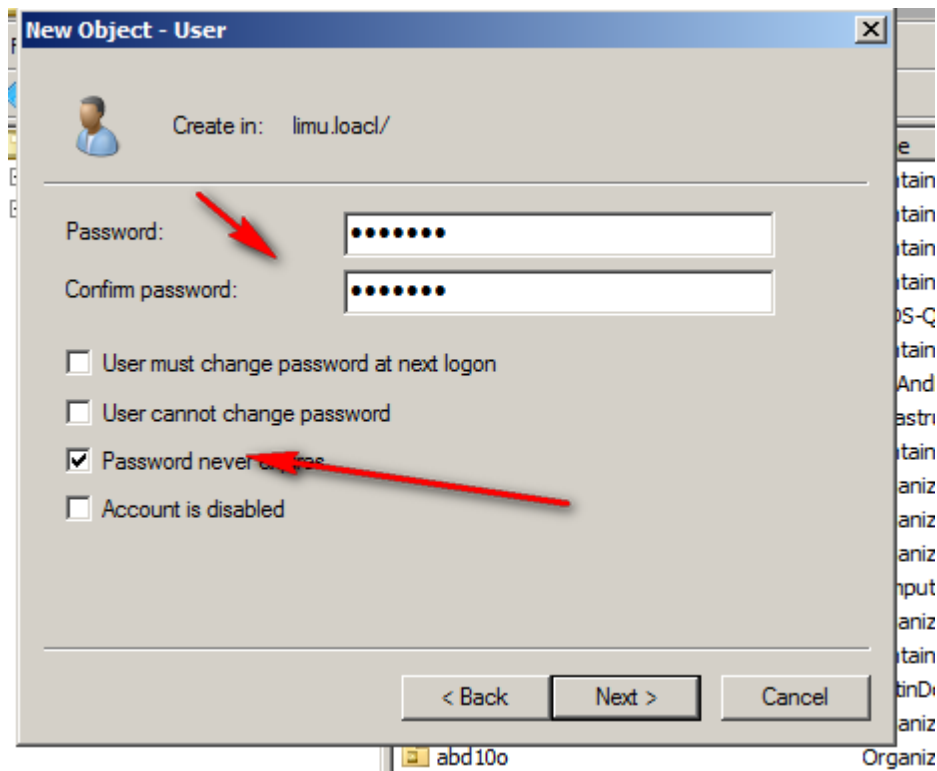


Set password

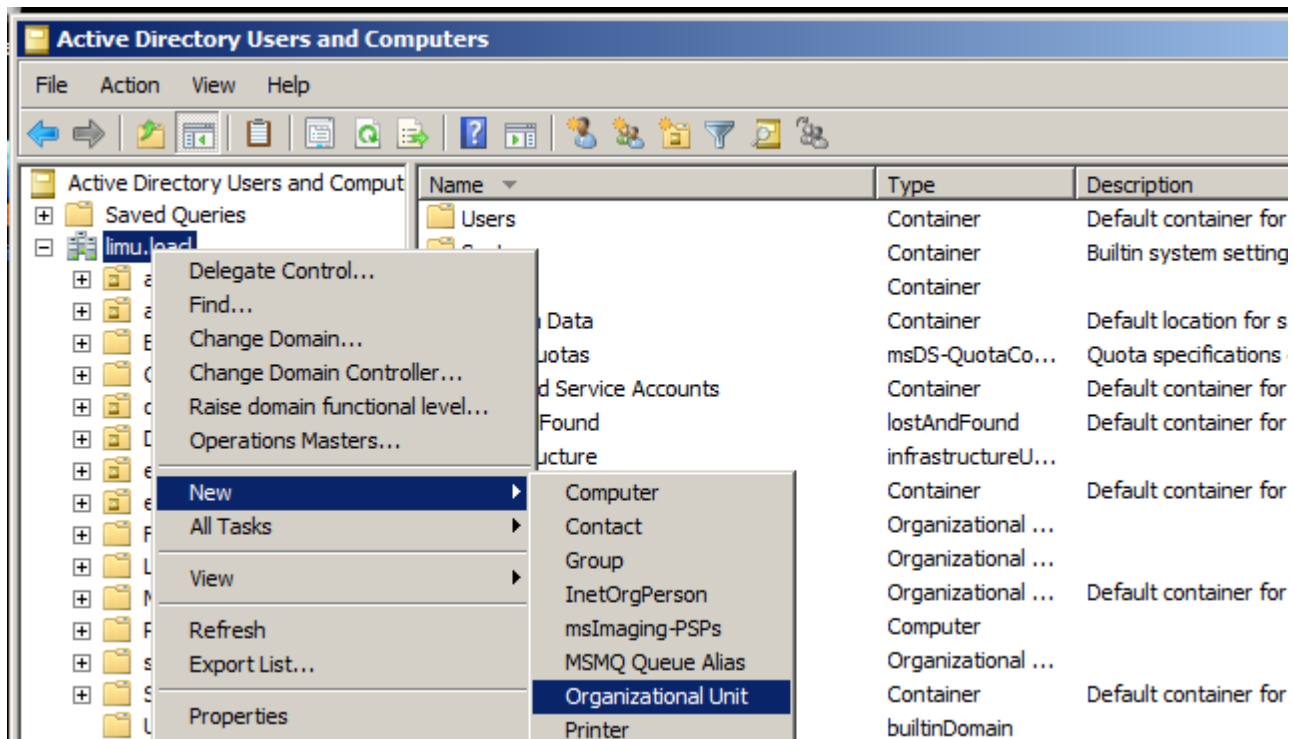
The screenshot shows the 'New Object - User' dialog box in the 'Password' step. The 'Create in' field is set to 'limu.local/'. There are two password input fields, both containing seven dots. Below the fields are four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (unchecked), 'Password never expires' (checked), and 'Account is disabled' (unchecked). At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'. Two red arrows point to the 'Password:' label and the 'Password never expires' checkbox.

The screenshot shows the 'New Object - User' dialog box in the 'Name' step. The 'Create in' field is set to 'limu.local/'. There are four text input fields: 'First name' (elrashdi), 'Last name' (saleh), 'Full name' (elrashdi saleh), and 'User logon name (pre-Windows 2000)' (LIMU\). There are also two dropdown menus: 'Initials' (empty) and 'User logon name' (@limu.local). At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

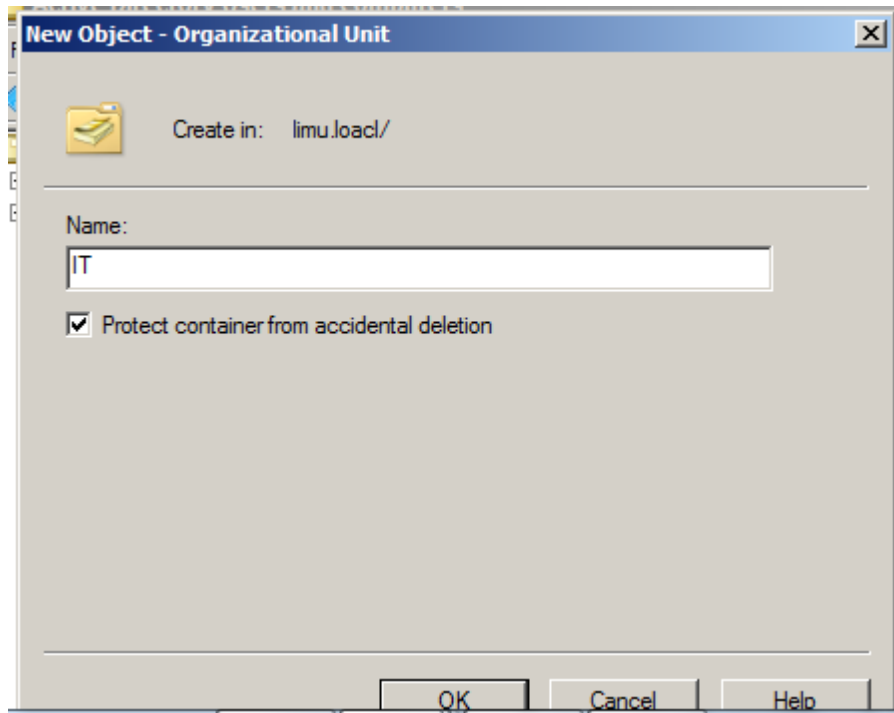
Set password



Create OU

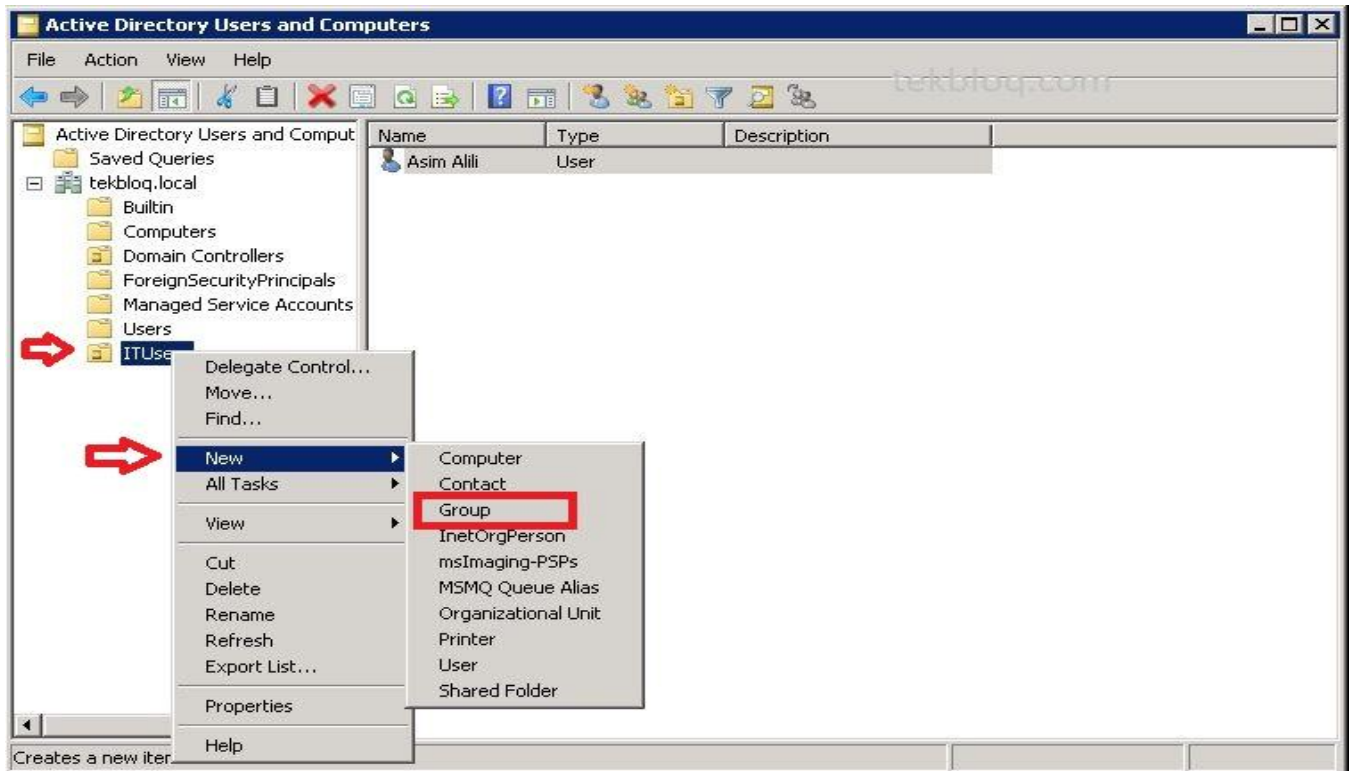


Create OU



Create group

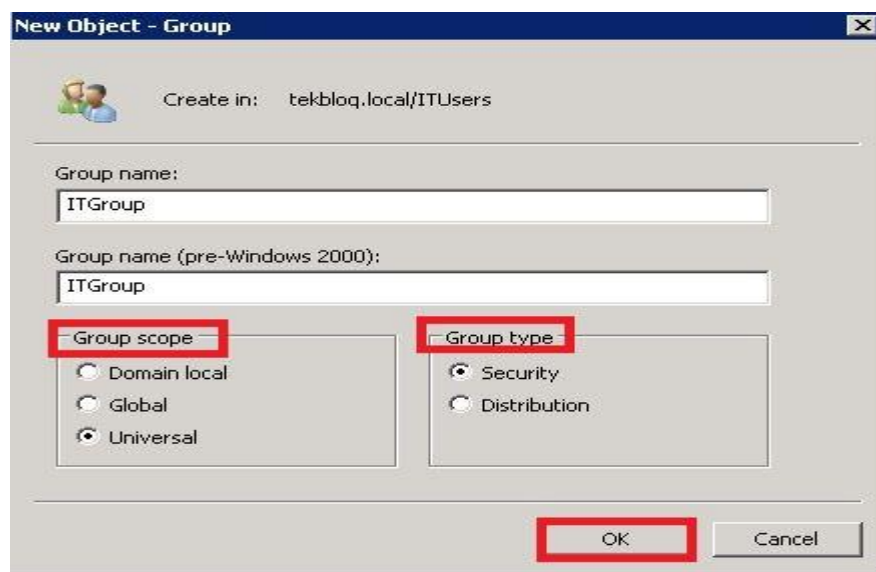
To create group right click on ITUsers OU and Click New and then click Group:



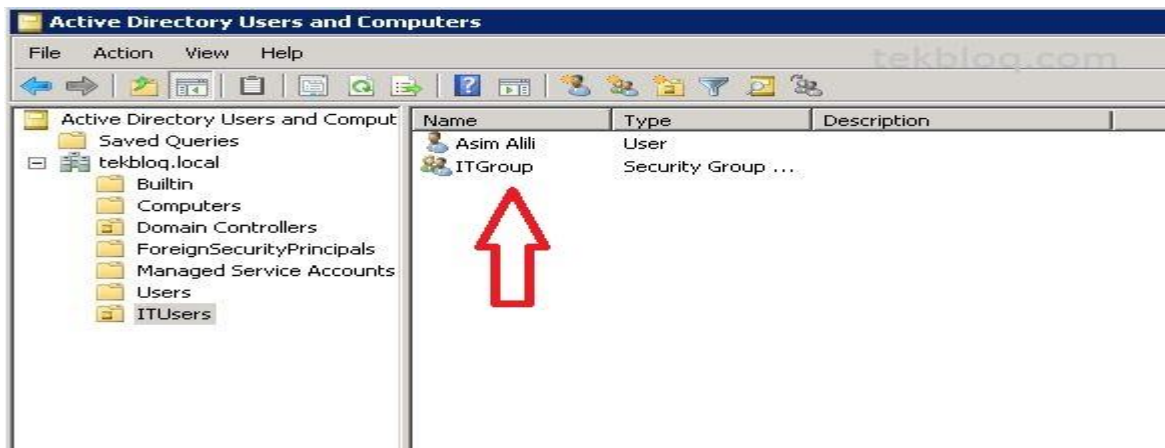
Type group name , Group scope and type for that and click OK:

The Group type indicates whether the group can be used to assign permissions to other network resources, such as files and printers. Both security and distribution groups can be used for e-mail distribution lists.

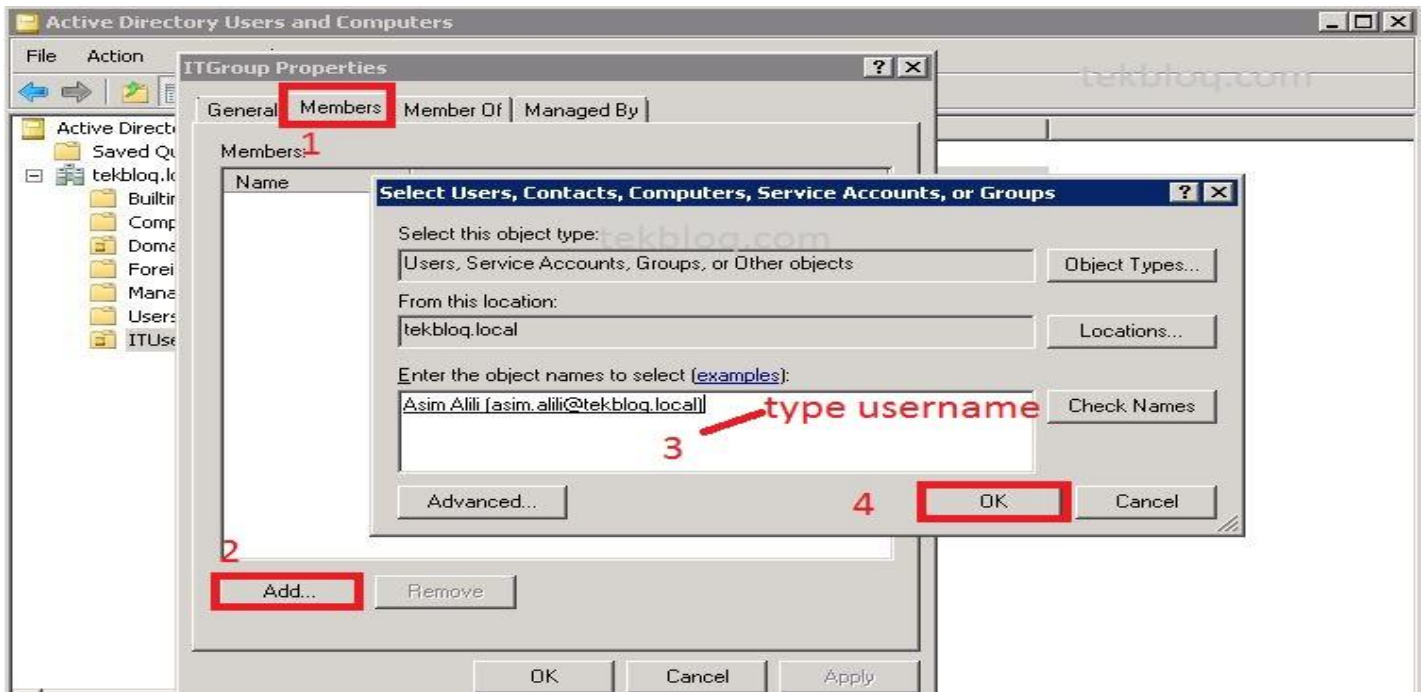
The Group scope determines the visibility of the group and what type of objects can be contained within the.



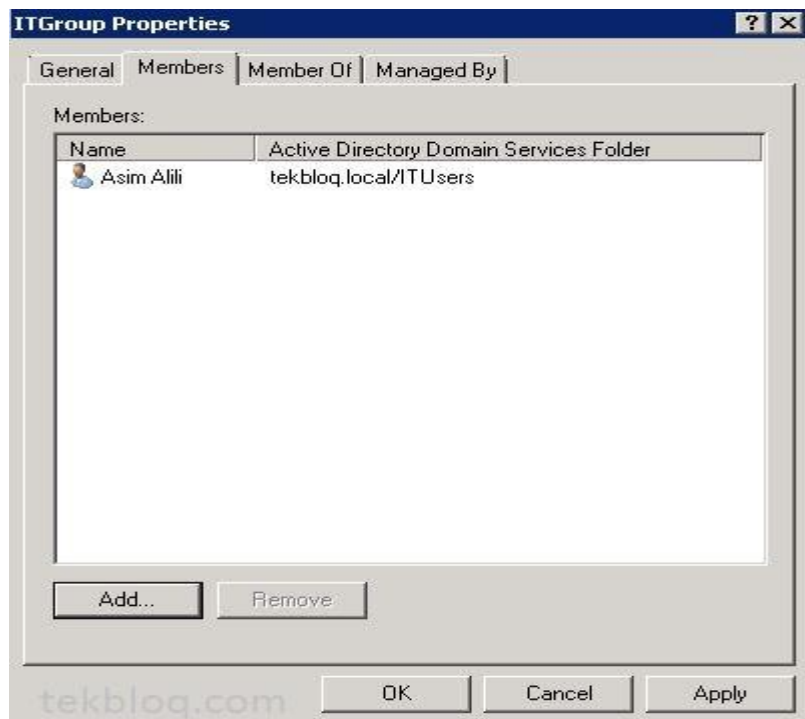
ITGroup group created:



To add member to that group double-click on that groups and click Members, click Add and type name for that user and click OK

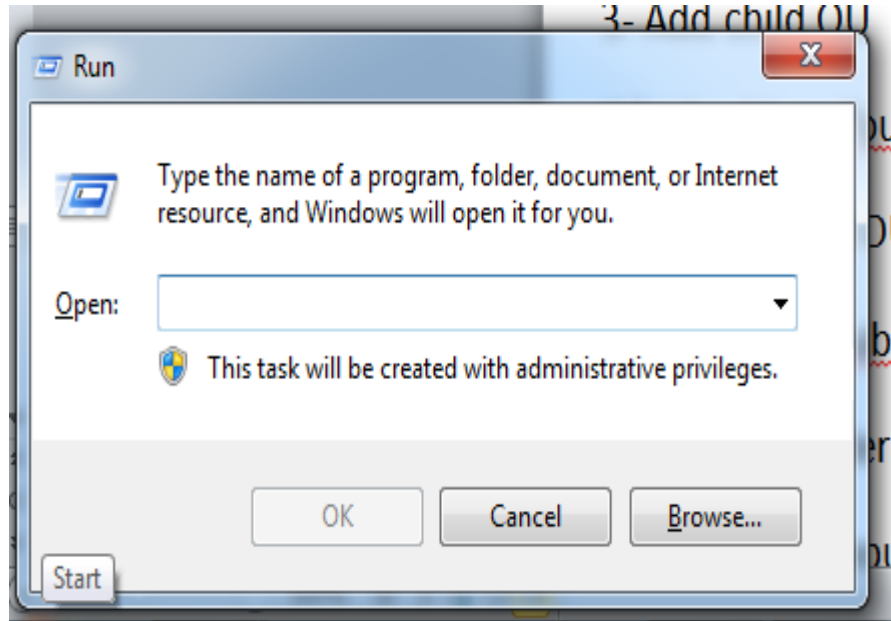


And click OK:

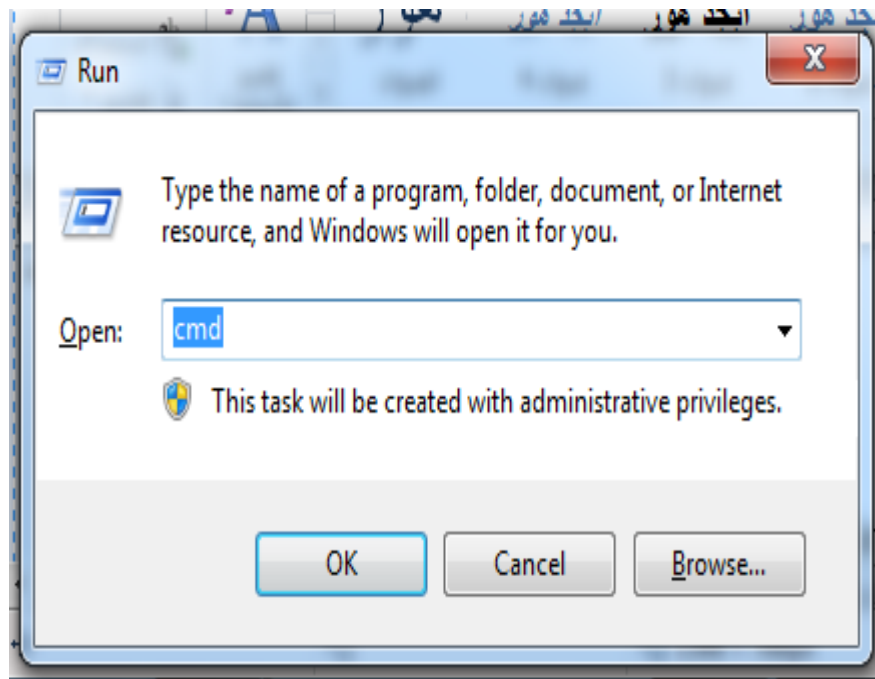


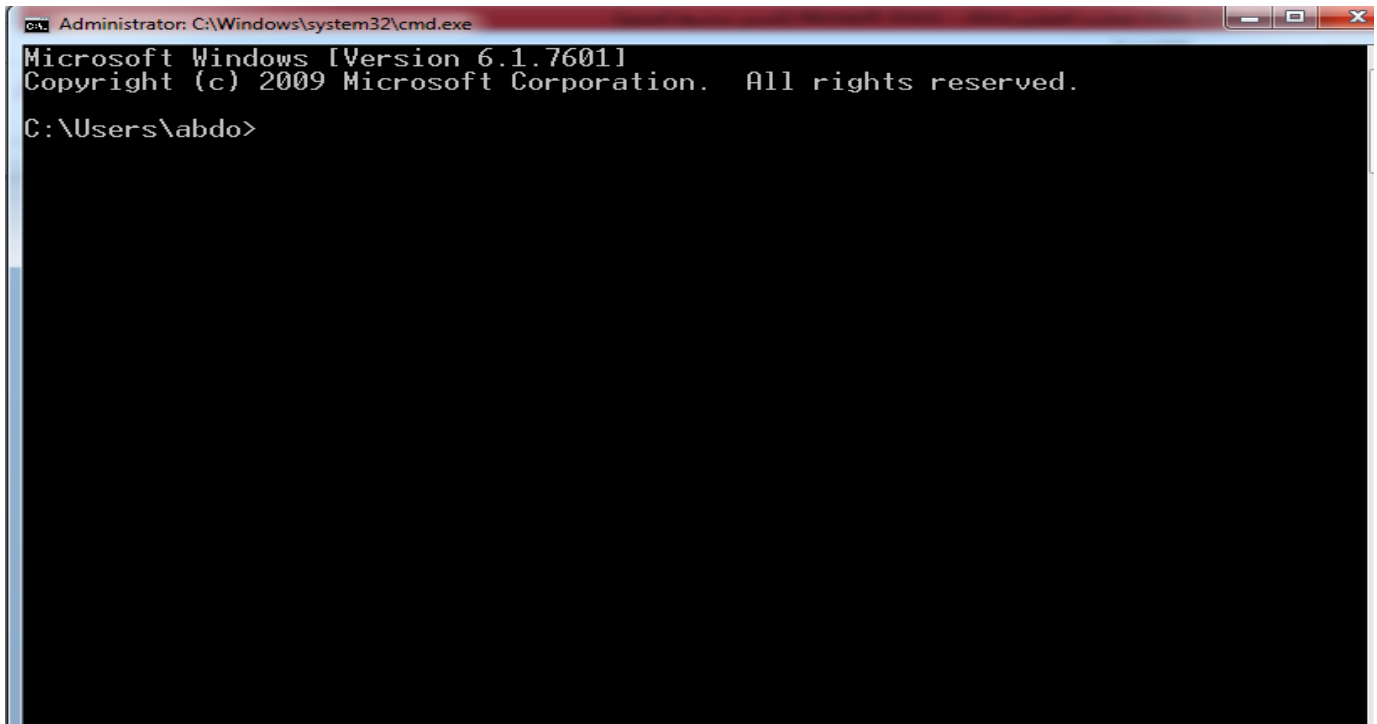
19.1.1- create objects in active directory in windows server 2008 by using command line

Open run



Type cmd





```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.76011
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\abdo>
```

Type those commands

```
C:\> dsadd ou "ou=Elrashdi,dc=limu,dc=local"
```

2- Delete OU

```
C:\>dsrm "ou=Elrashdi,dc=limu,dc= local "
```

3- Add child OU

```
C:\>dsadd ou "ou=abdo,ou=Elrashdi,dc=limu,dc=local"
```

4- Delete child OU

```
C:\>dsrm "ou=abdo,ou=Elrashdi,dc=limu,dc=local"
```

5- Add computer to active directory

```
C:\>dsadd computer "cn=com1,cn=computers,dc=limu,dc= local "
```

6- Delete computer

```
C:\>dsrm "cn=com1,cn=computers,dc=limu,dc= local "
```

7- Add user to active directory

```
C:\>dsadd user "cn=A.Elrashdi,cn=users,dc=limu,dc= local " -fn abdel salam -ln saleh -pwd  
P@sw0rd -samid A.Elrashdi -upn A.Elrashdi@limu.local
```

8- Delete user from active directory

```
C:\>dsrm "cn=A.Elrashdi,cn=users,dc=limu,dc=local"
```

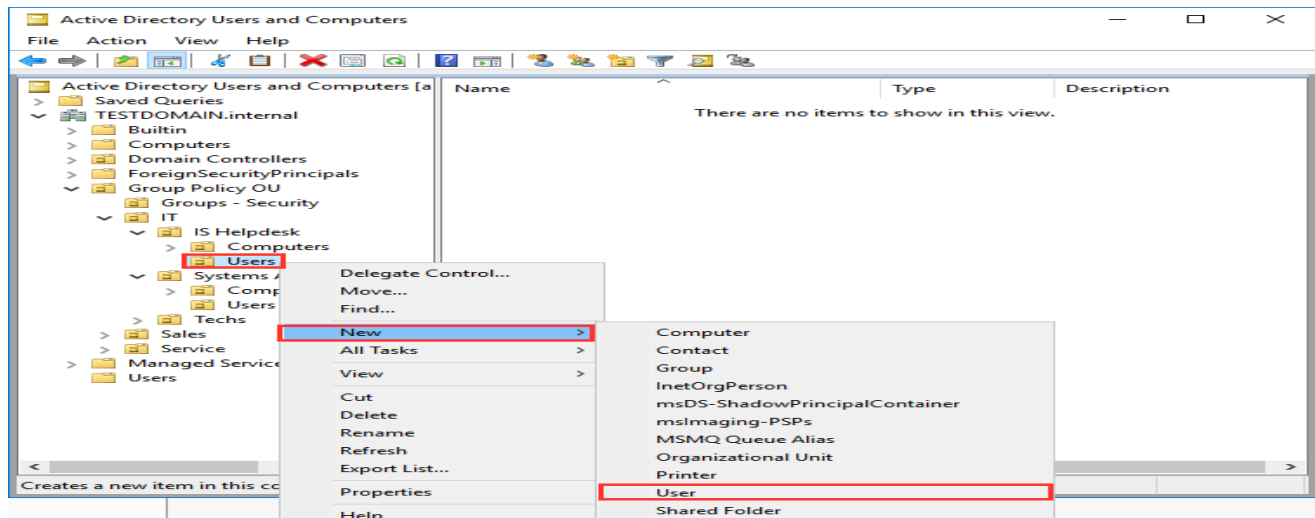
19.2- Add objects (users,group,OU,computers) in active directory windows server 2016

Creating AD Users and Groups – Standard User Accounts

Go through and setup all of the remaining user accounts for the environment and place them in the proper OUs. Remember, use the **Copy** feature as much as possible after setting up one user.

Navigate to **Group Policy OU | IT | Helpdesk | Users**

Right-click **Users** and select **New | User**



- Fill in the information

New Object - User

Create in: N.internal/Group Policy OU/IT/IS Helpdesk/Users

First name: Joe Initials:

Last name: Smith

Full name: Joe Smith

User logon name: jsmith @TESTDOMAIN.internal

User logon name (pre-Windows 2000): TESTDOMAIN\ jsmith

< Back Next > Cancel

Type a password twice.

Leave the User must change password at next logon enabled

New Object - User

Create in: TESTDOMAIN.internal/Group Policy OU/IT/IS Hel

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

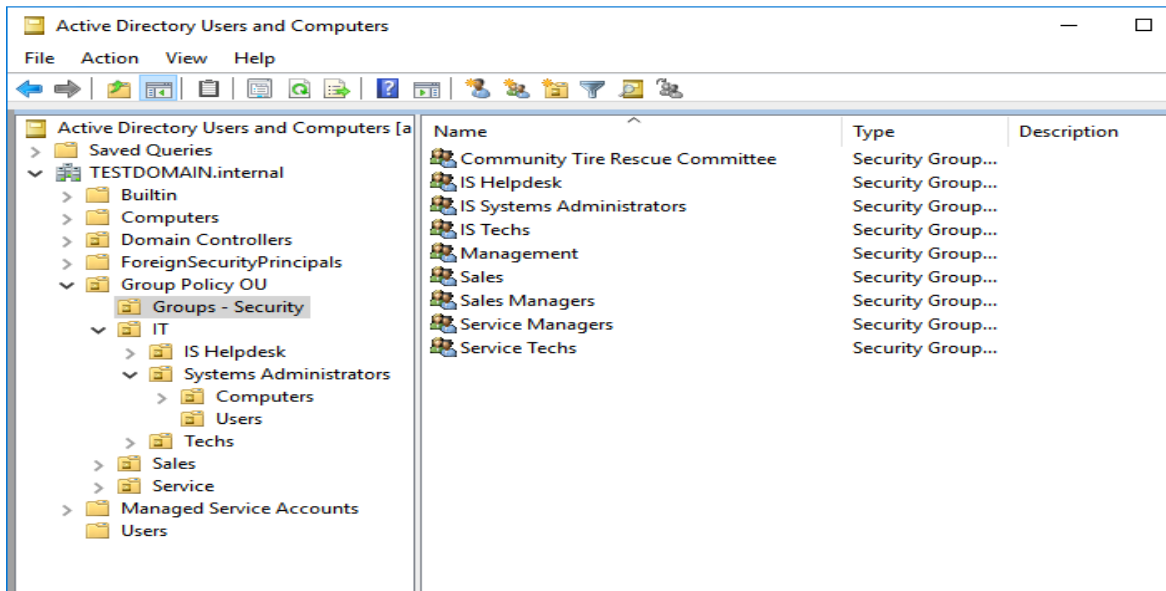
Account is disabled

< Back Next > Cancel

Finish creating the users and placing them into the proper OUs.

Creating AD Users and Groups – Groups

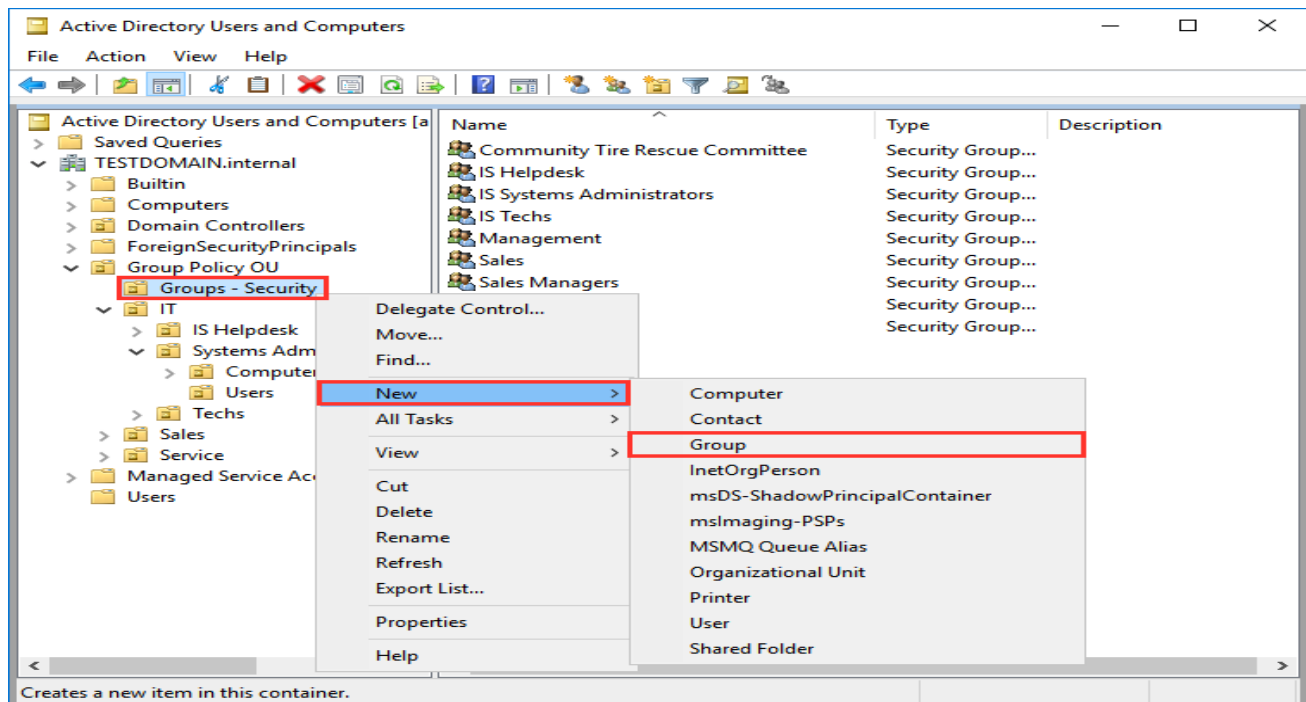
Finally, let's create some groups and assign the associated people to them.



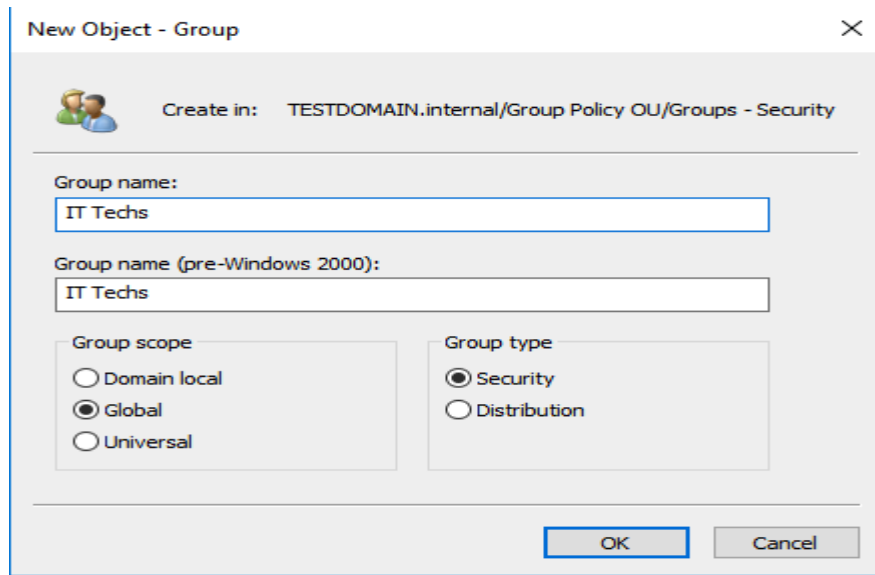
Navigate to Group Policy OU | Groups – Security

Right-click Groups – Security

Select New | Group

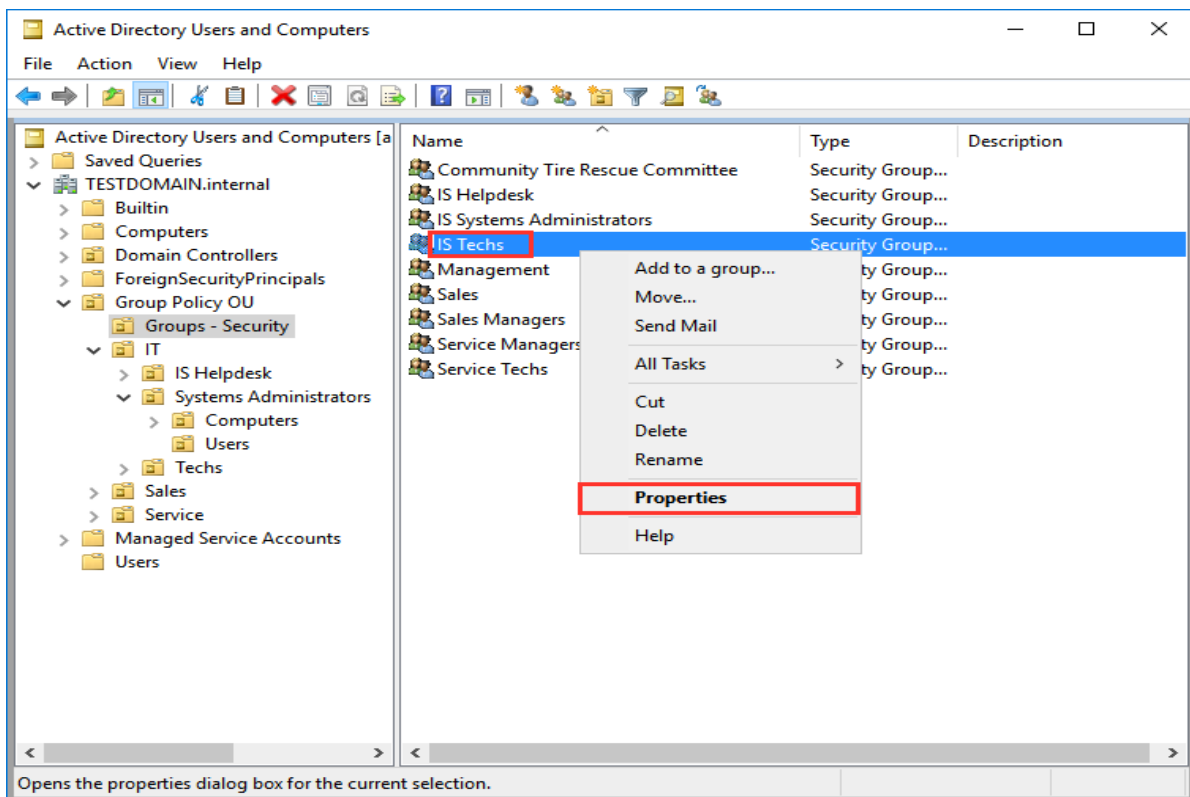


Fill in the information. For this one, I am calling this group IT Techs

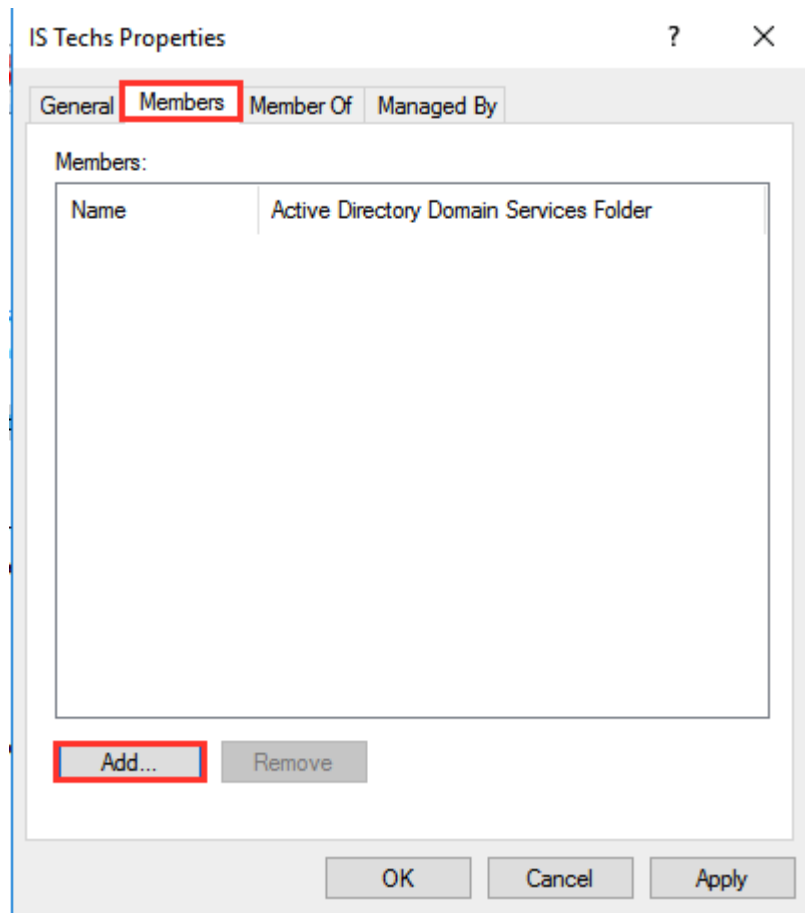


Now that the group is created, let's add a member to it.

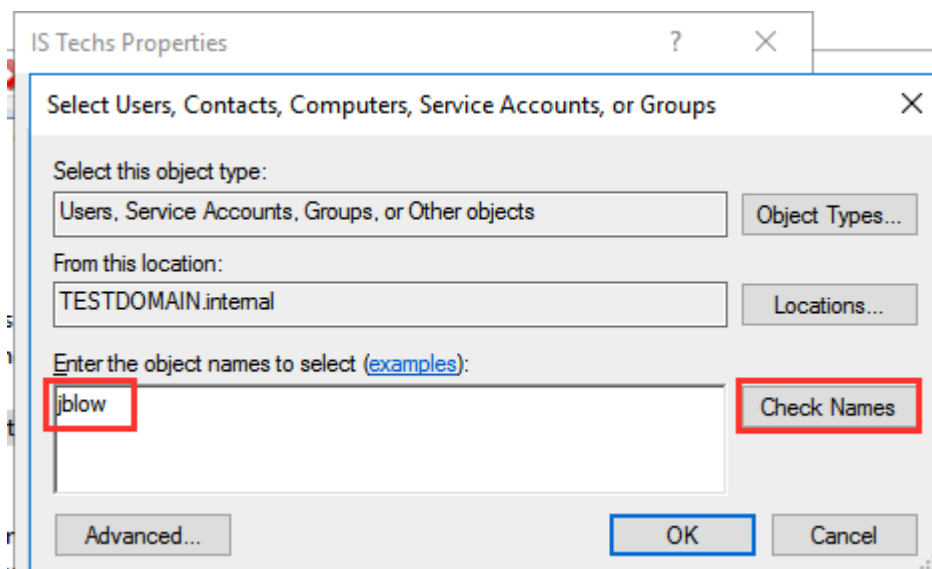
Right-click the IS Techs group and select Properties



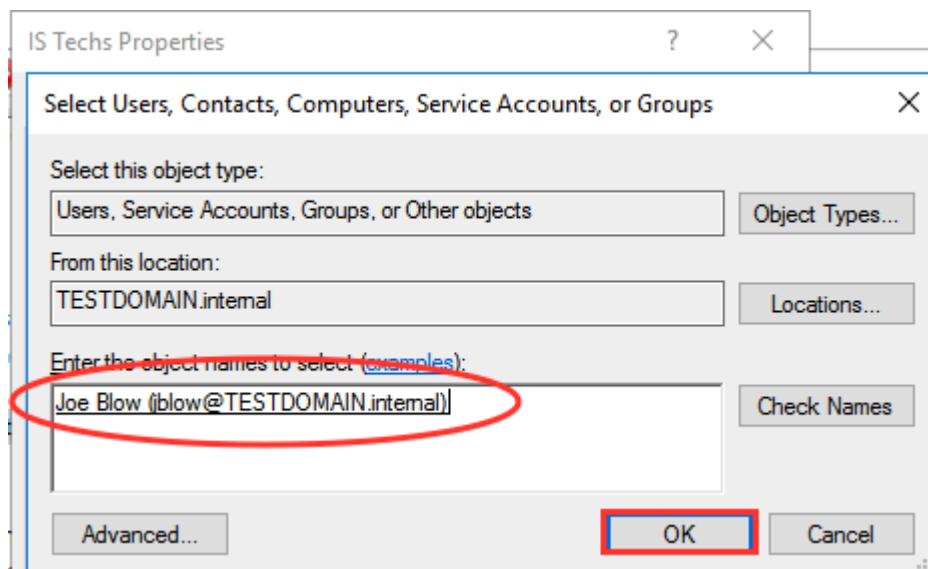
In the Members tab, select Add.



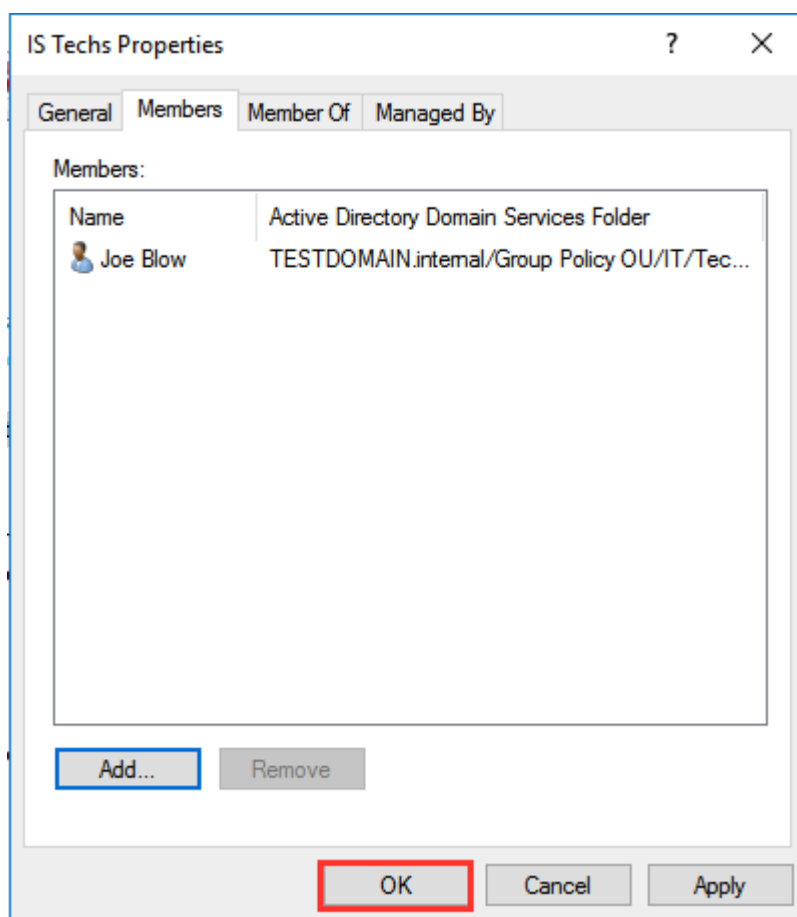
Type the username and select **Check Names**.



When the system finds the account, you will see the full account details. Select **OK**.



Select **OK** when finished adding users to the group.



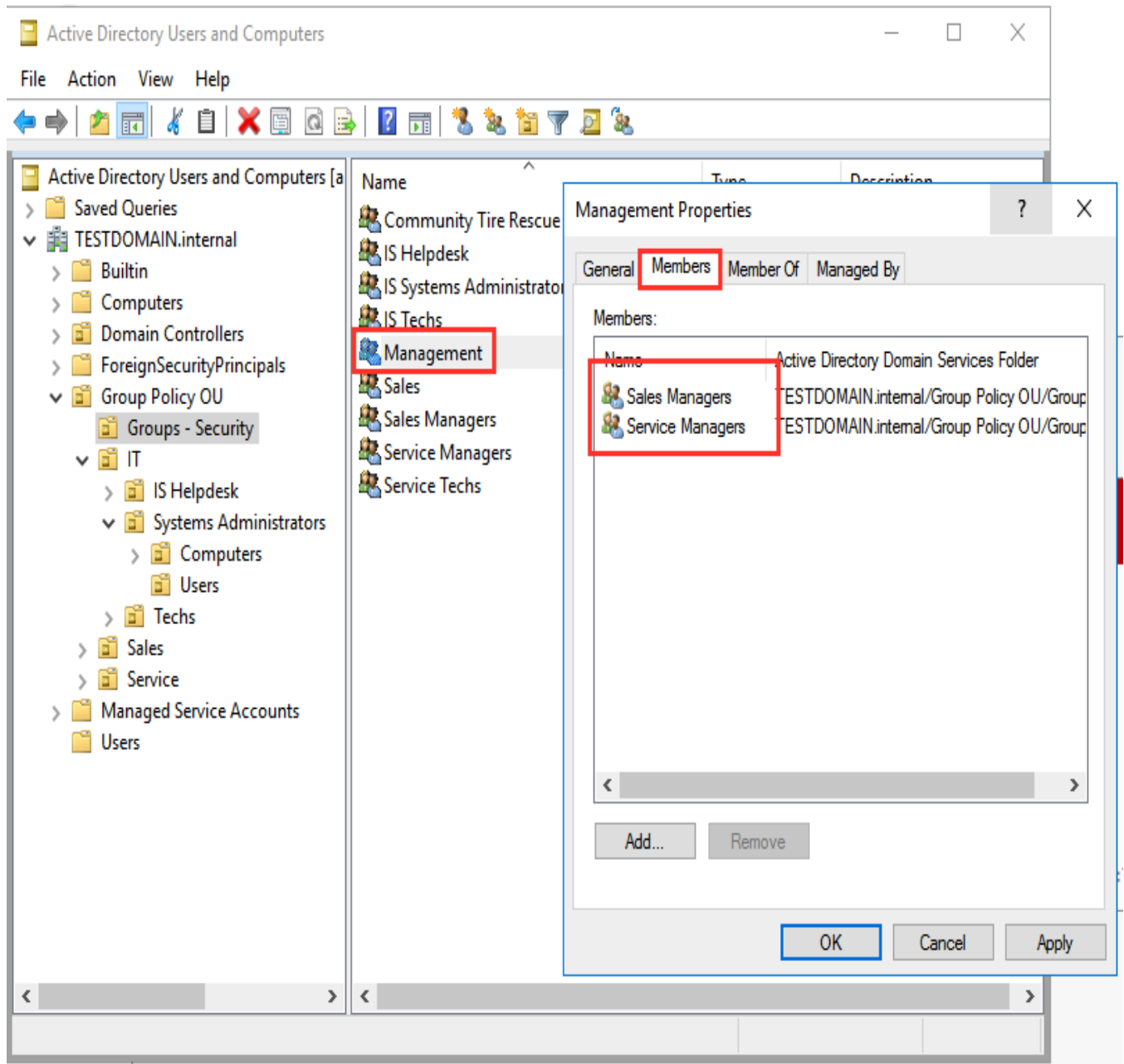
When finished, let's nest a couple of groups within another group.

This example, we have two Managers groups: **Sales** and **Service Managers**. We want to add those groups to a **Management** group.

Right-click the **Management** group and select **Properties**.

In the **Members** tab, click **Add**, type the names of the groups, and add them to the group.

It should look like this:



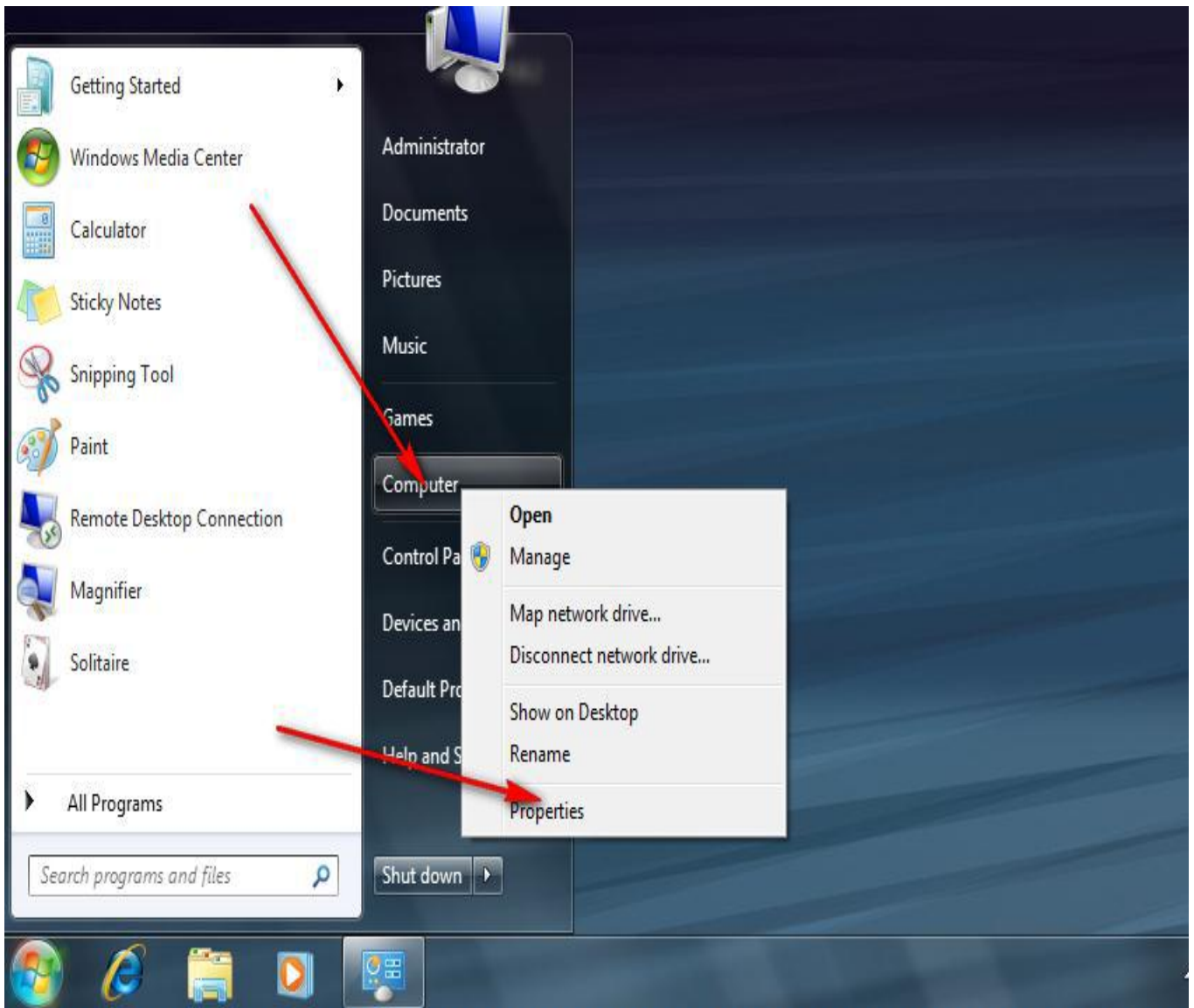
That's it for this one! We have a foundation for our environment! Stay tuned for our next tutorial in the series!

20-Join computers to domain controller

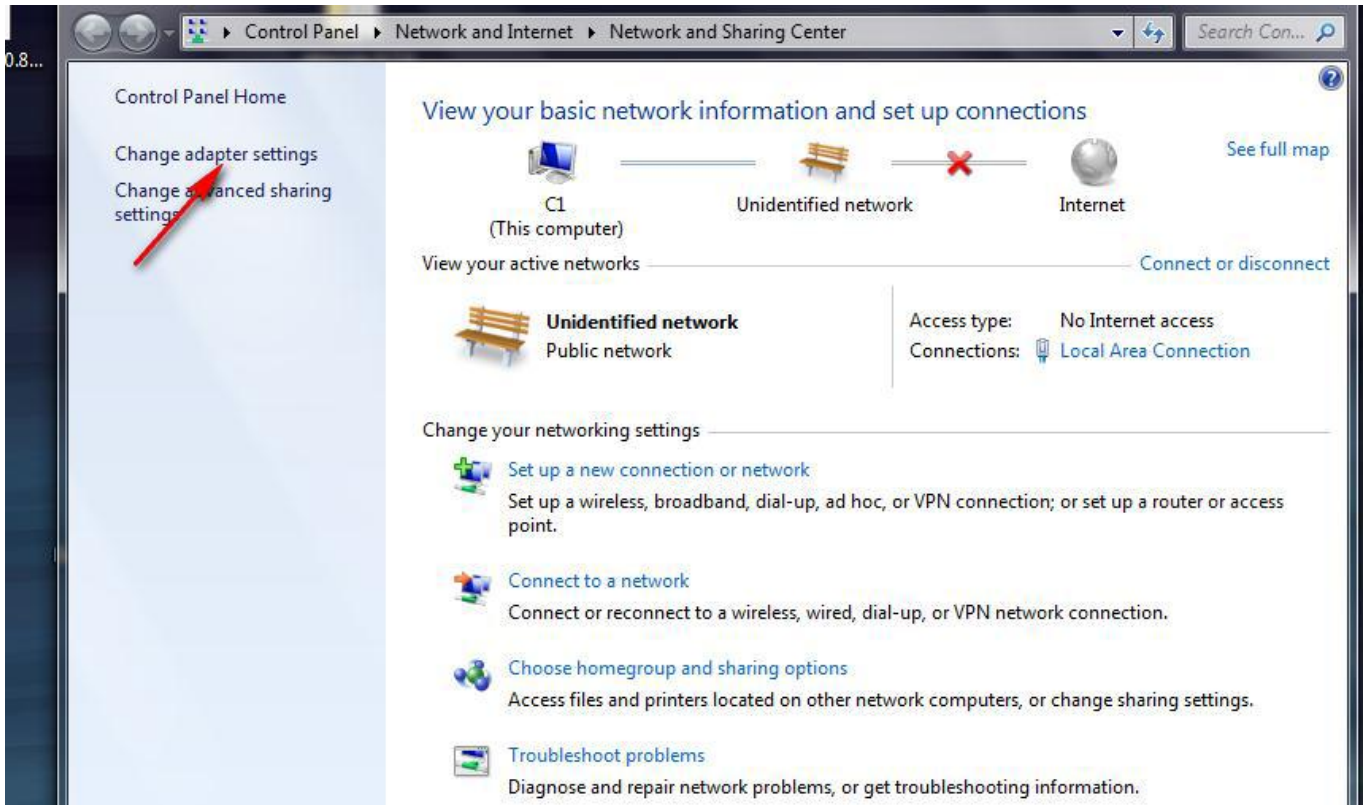
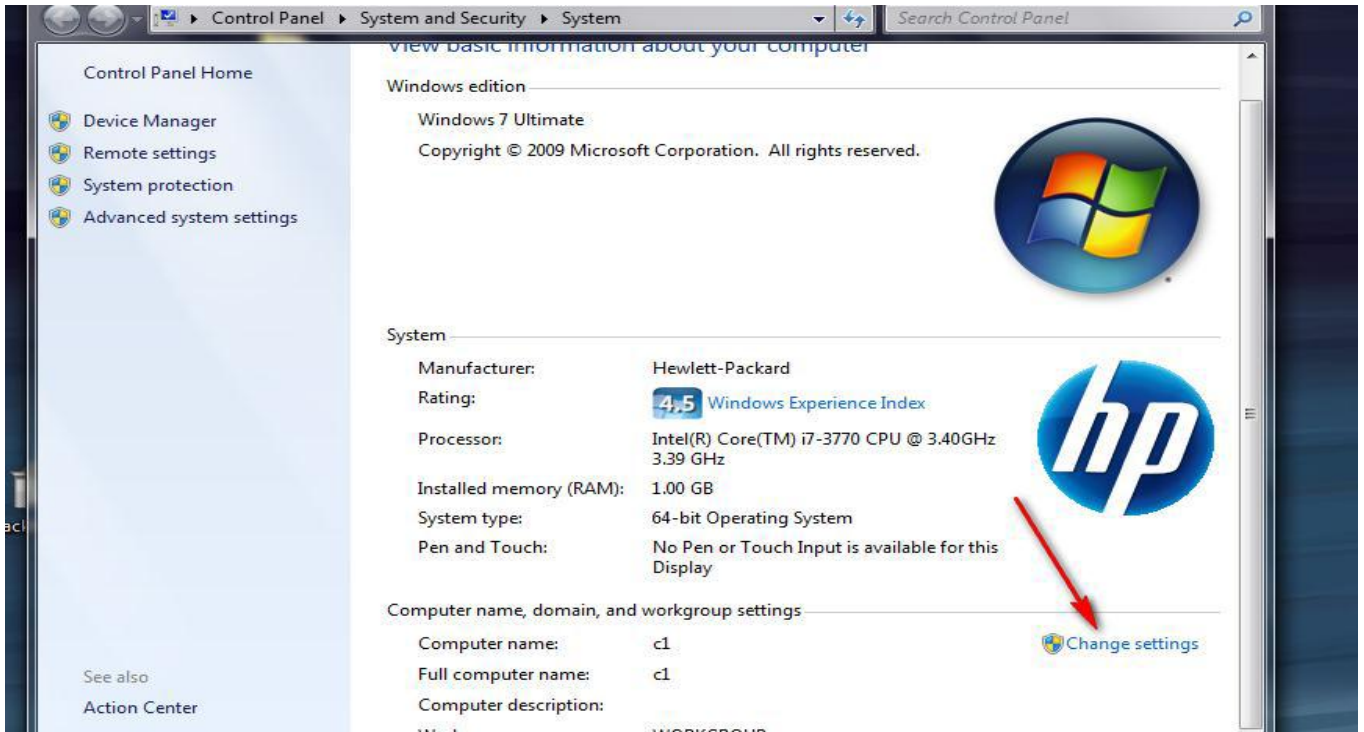
لكي نستطيع التحكم في جميع الاجهزة الموجودة في الشبكة فيجب علينا اضافة جميع الاجهزة داخل الدومين الذي تم انشائه مسبقا والصور التالي توضح كيفه اضافة الاجهزة داخل الدومين

Before join computer to domain you have to check connectivity

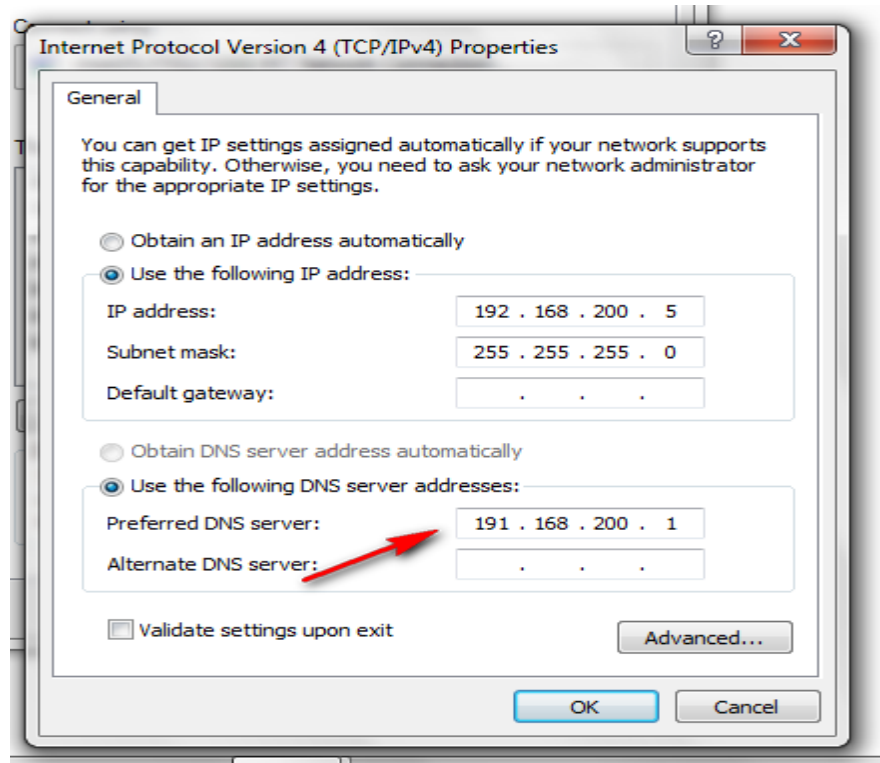
between server and Clint and put DNS on the Clint



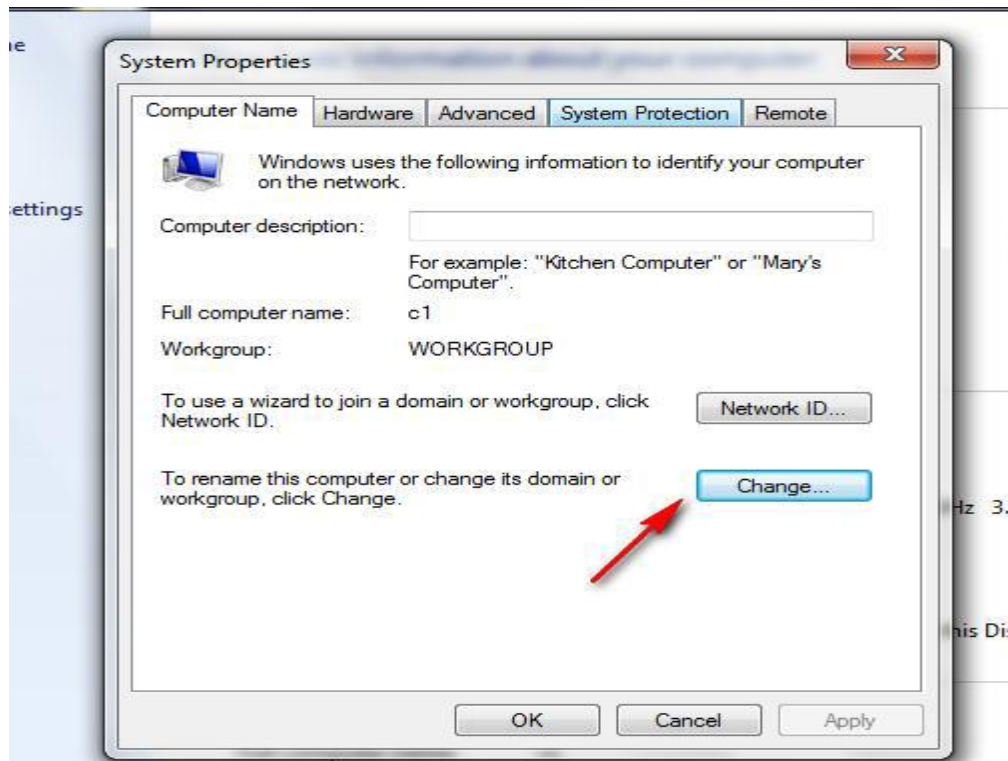
Join computer to domain



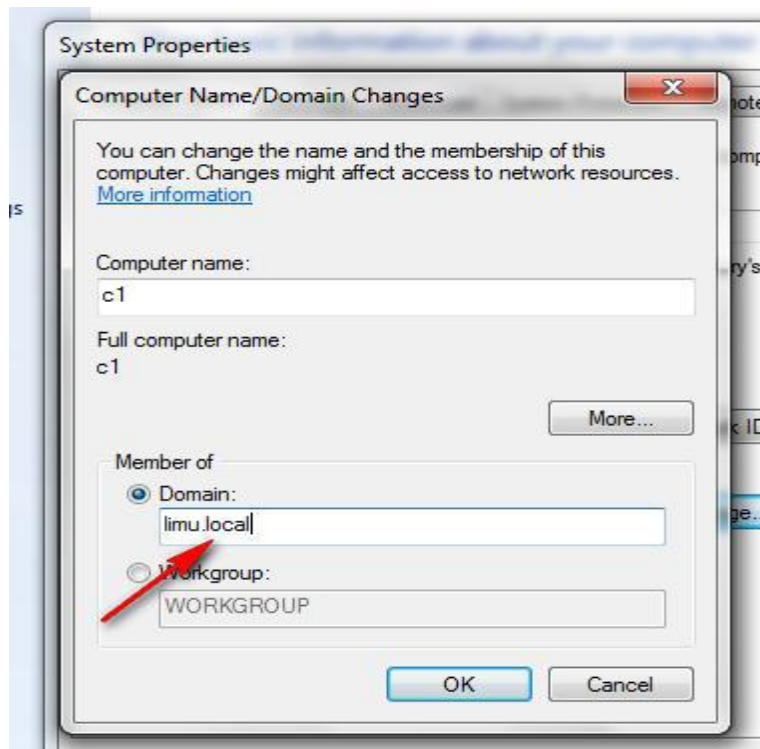
Put the Ip of DNS server



Join computer to domain



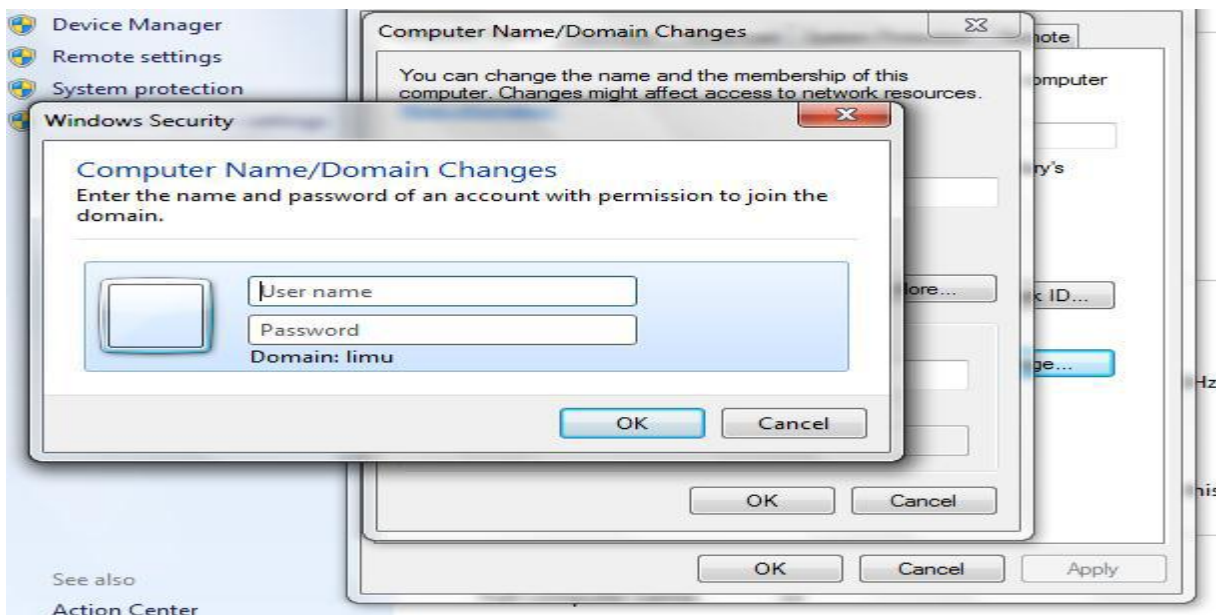
ادخال اسم الدومين



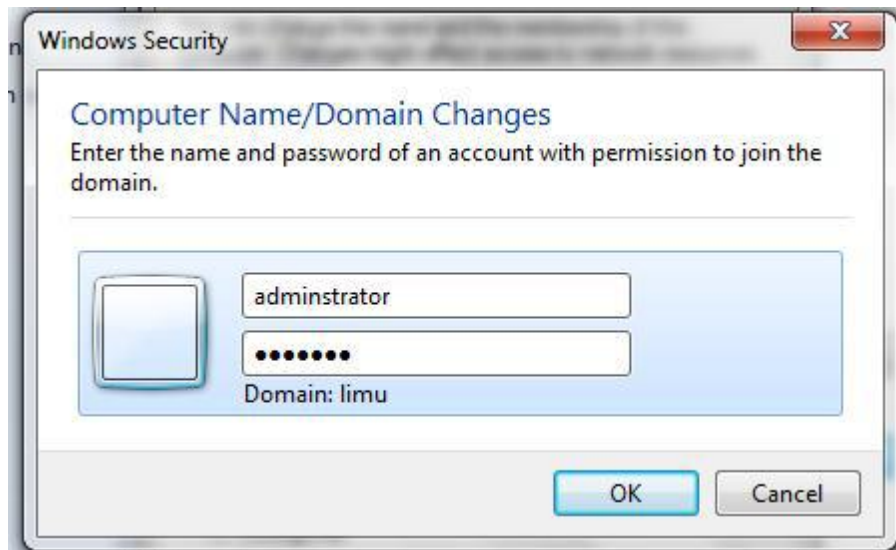
You have to type username and password

that already save in active directory

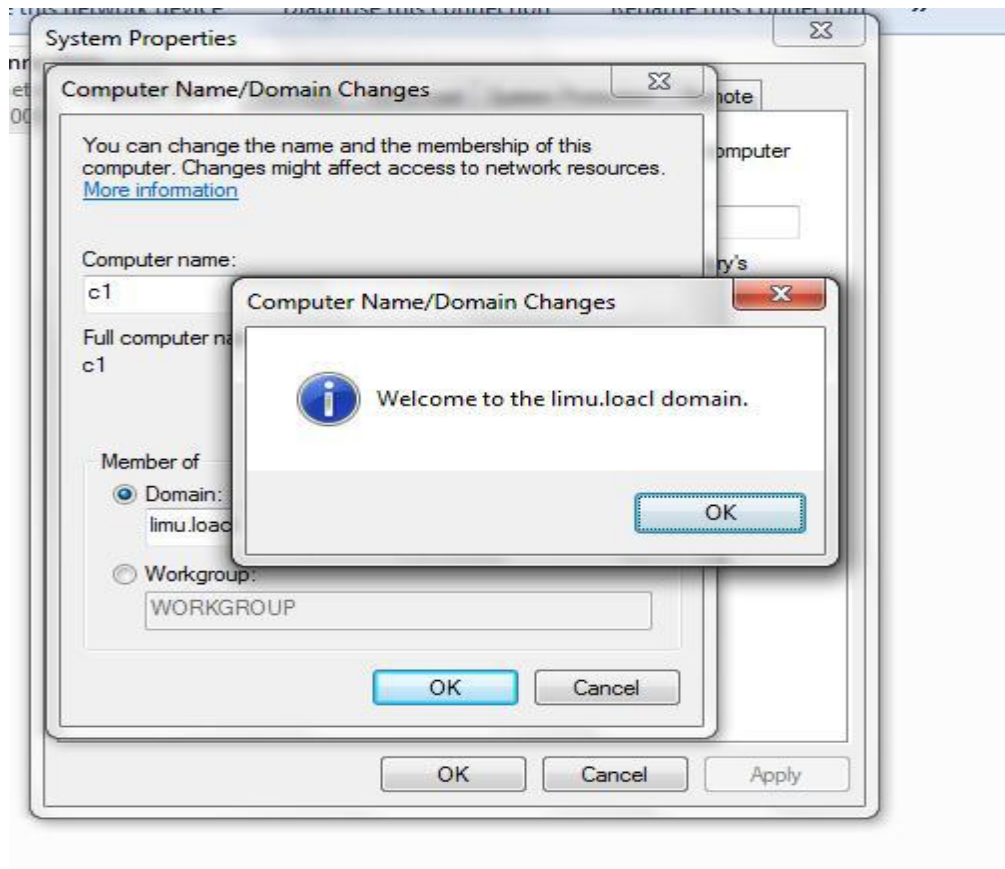
ادخال اسم مستخدم موجود داخل الدومين



Type username and password



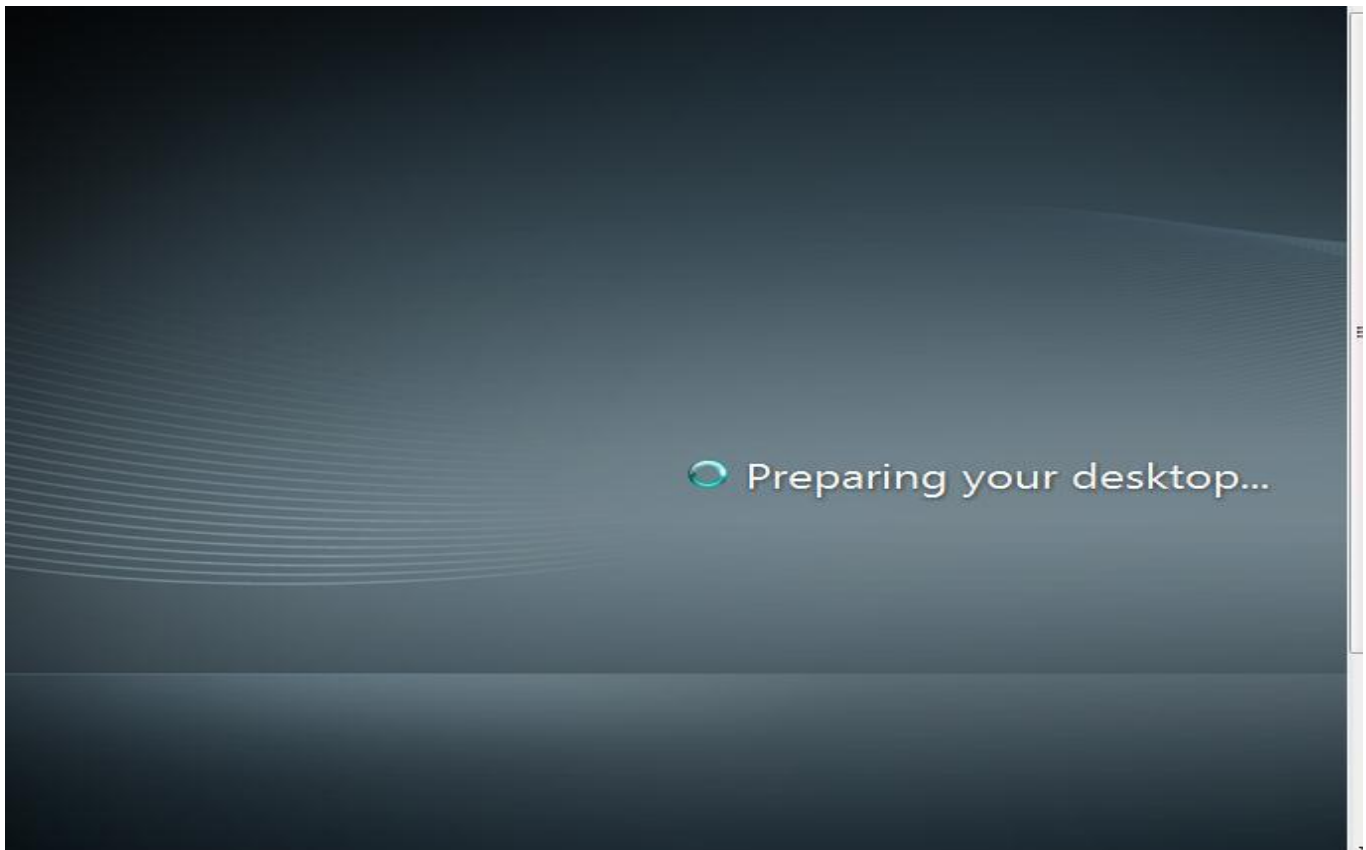
Now computer is joined



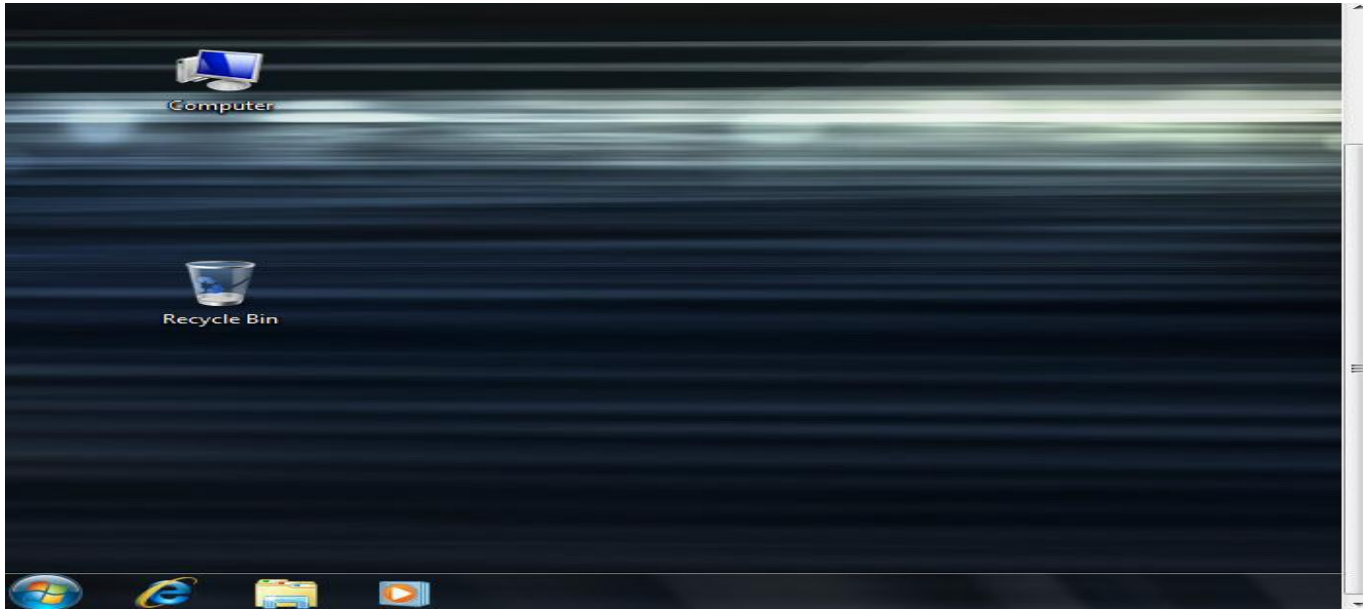
After restart the computer you have type limu\ then an f username and password to login



Now preparing the desktop



Now preparing the desktop

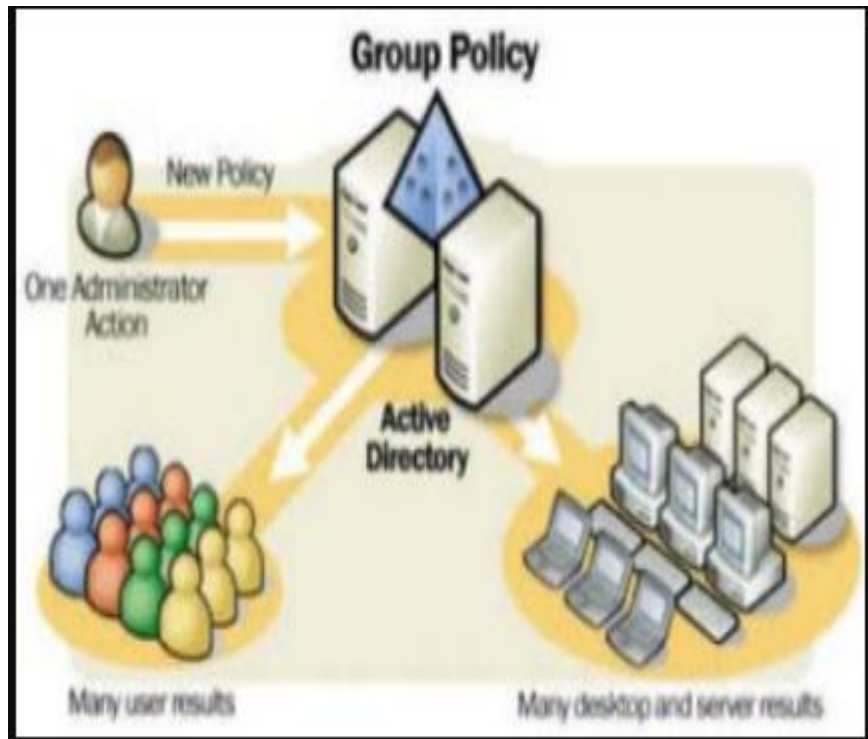


21-Group policy in windows server

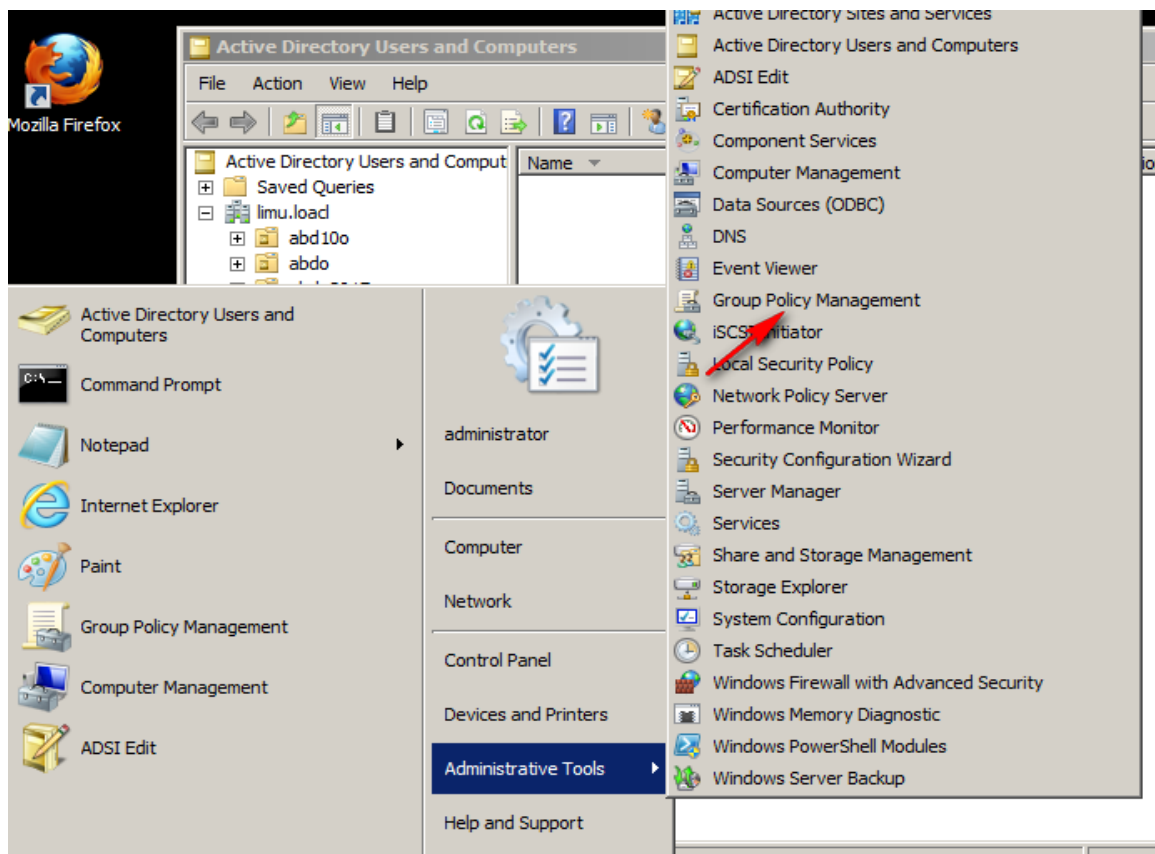
بكل بساطة هي عبارة عن اداة تنشيط من خلالها قواعد تتيح التحكم في المستخدمين والموارد والاتصال بحيث تمنع او تسمح بناء على ما يريده مدير النظام. مثلا اريد ان اسمح للمستخدم بالوصول الى الاقراص الصلبة وامنع غيره من ذلك واسمح للمستخدم بتغيير خلفية سطح المكتب وامنع باقي المستخدمين، واسمح للمستخدم ومشاركة والوصول الى الملفات المشتركة وامنع غيره الخ....

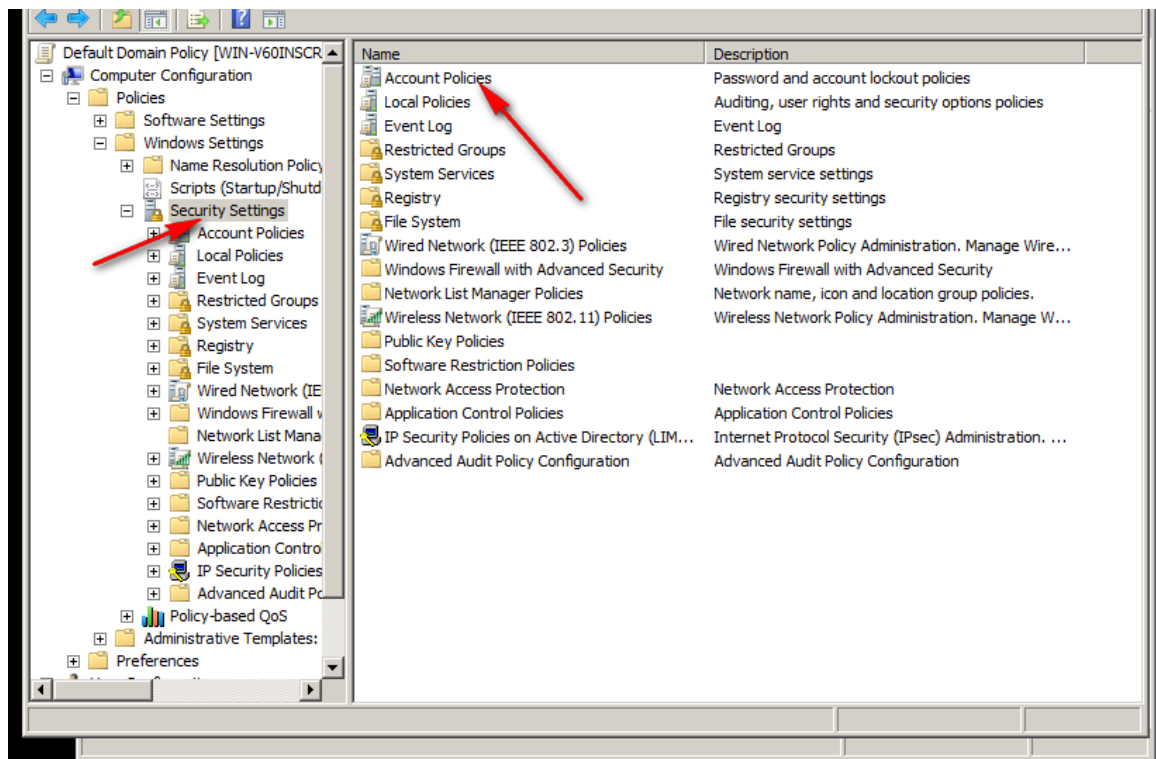
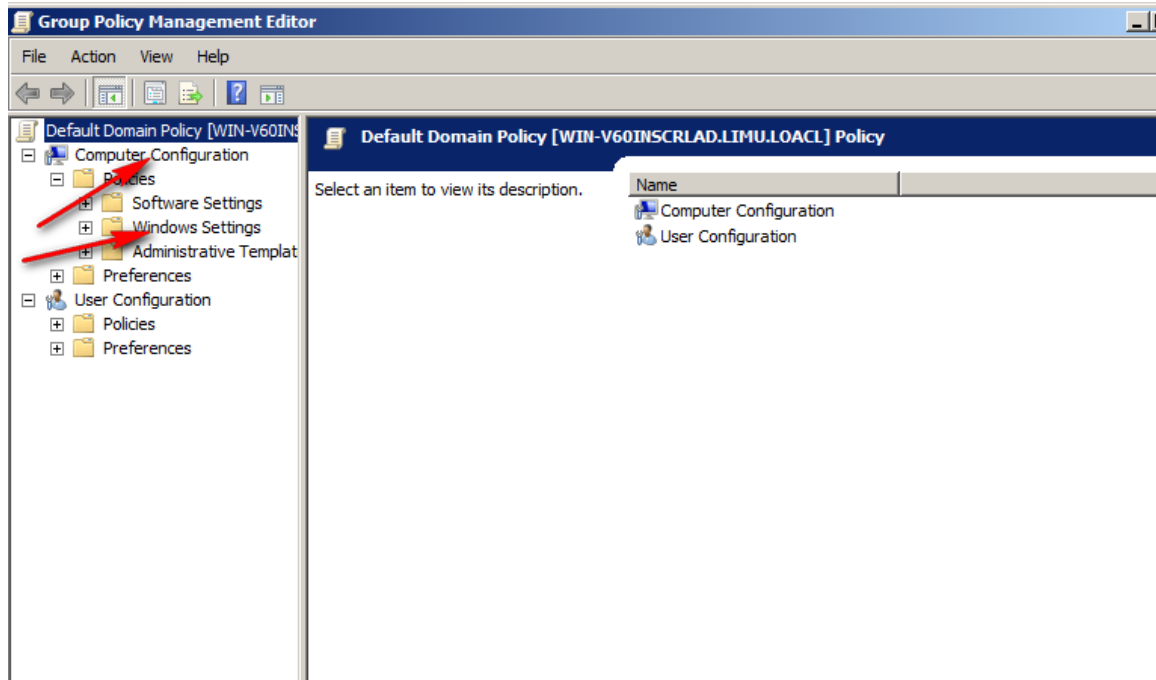
Group Policy is a hierarchical infrastructure that allows a network administrator in charge of Microsoft's Active Directory to implement specific configurations for users and computers. Group Policy can also be used to define user, security and networking policies at the machine level.

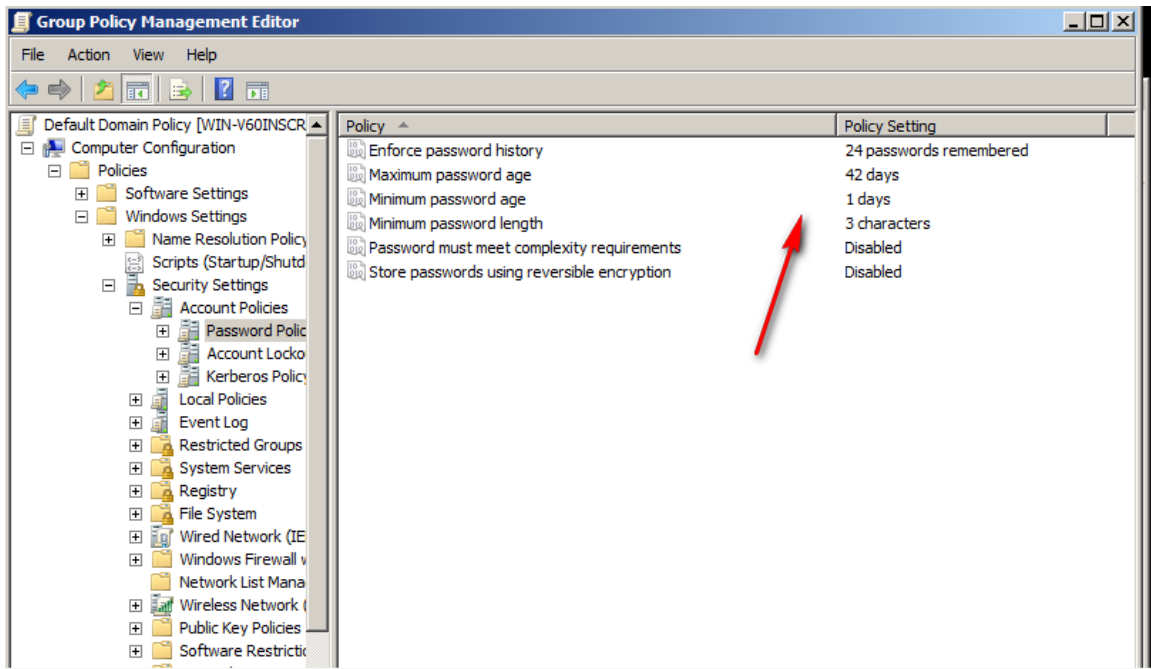
Group Policy is a feature of the Microsoft Windows NT family of operating systems that controls the working environment of user accounts and computer accounts. Group Policy provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. A version of Group Policy called Local Group Policy ("LGPO" or "LocalGPO") also allows Group Policy Object management on standalone and non-domain computers.



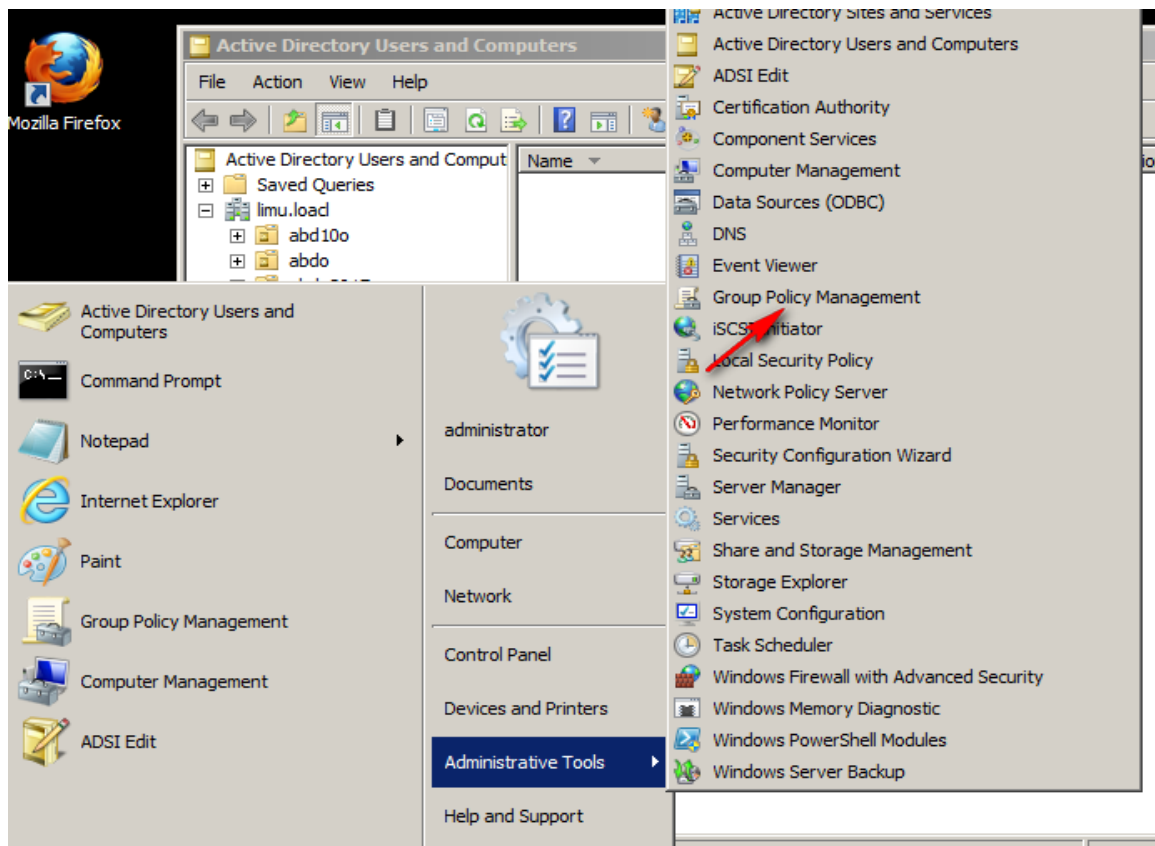
21.1- Apply Password policy in window server 2008

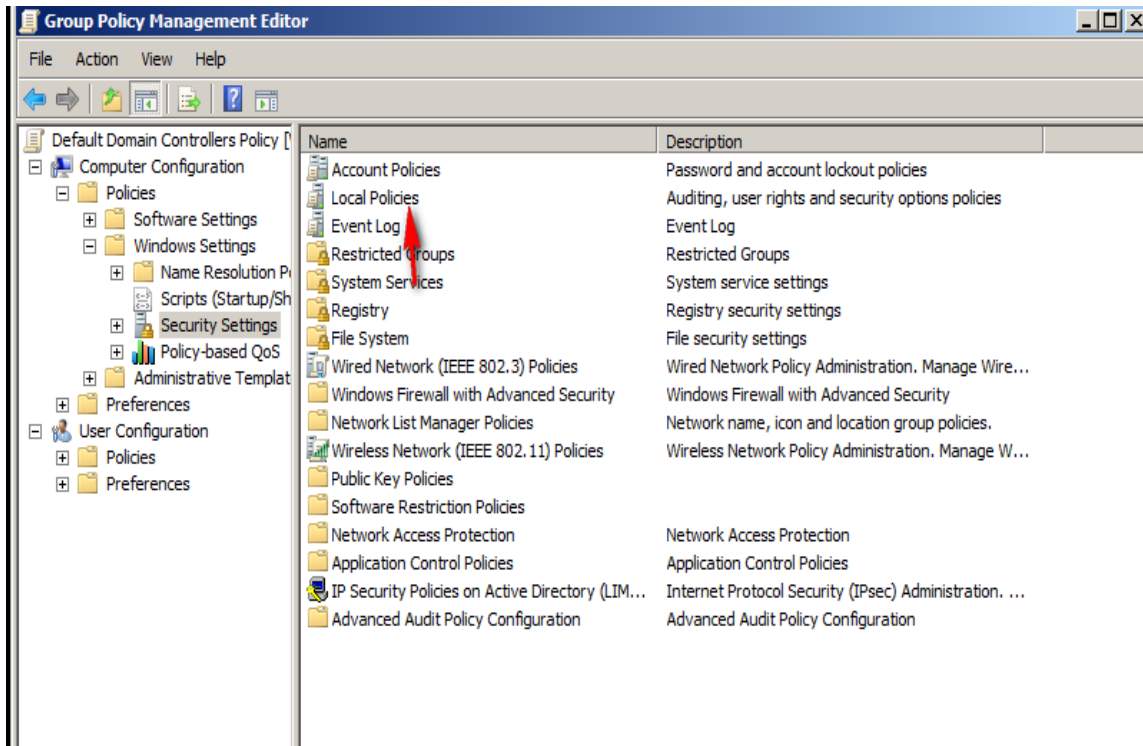
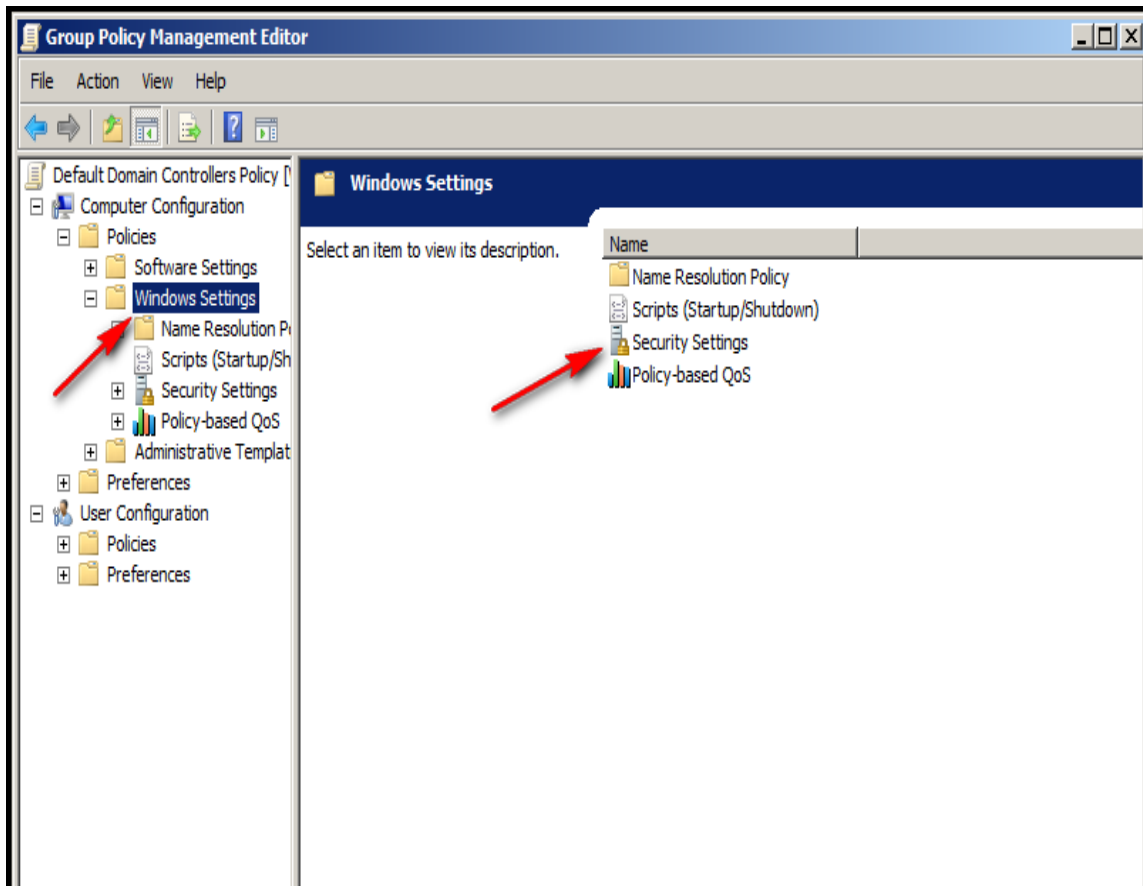


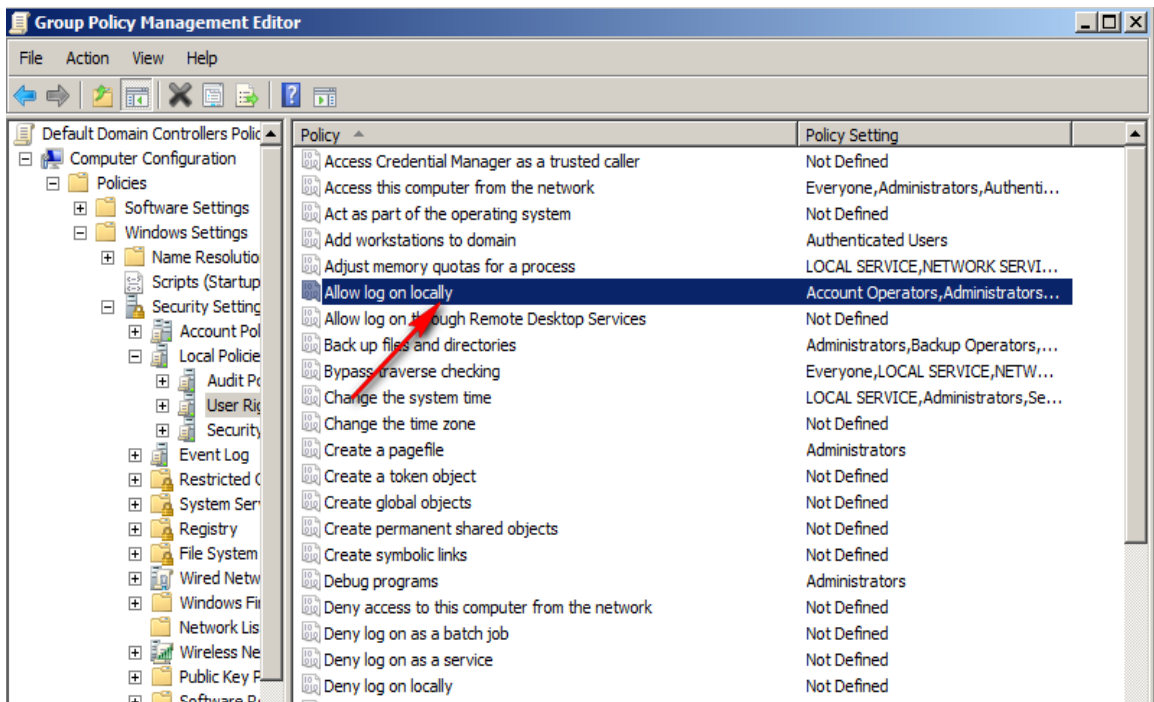
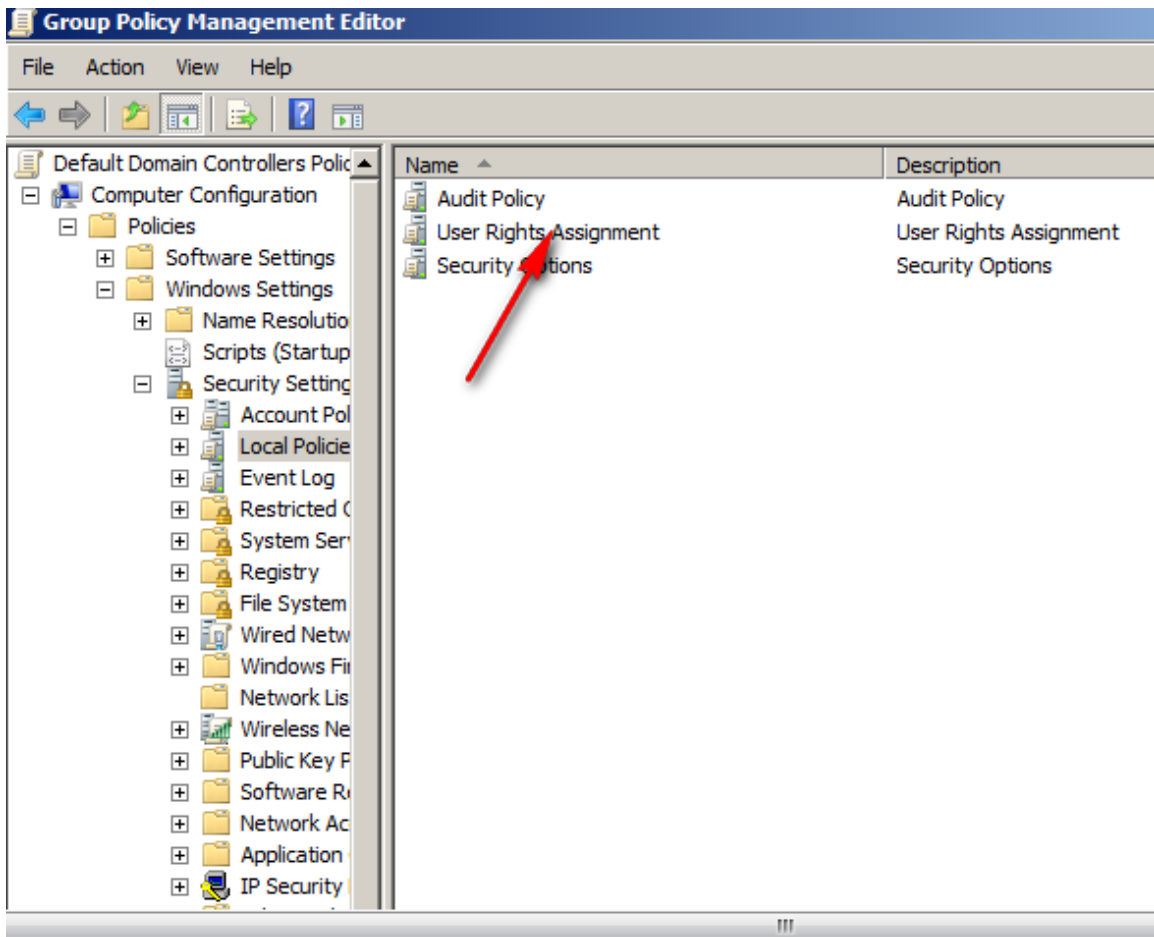


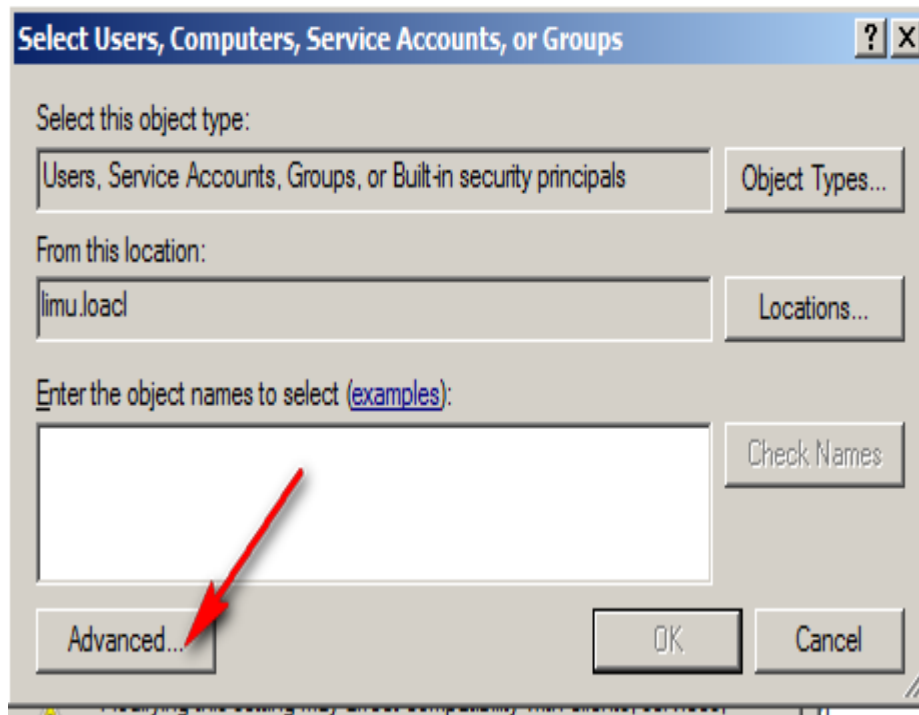
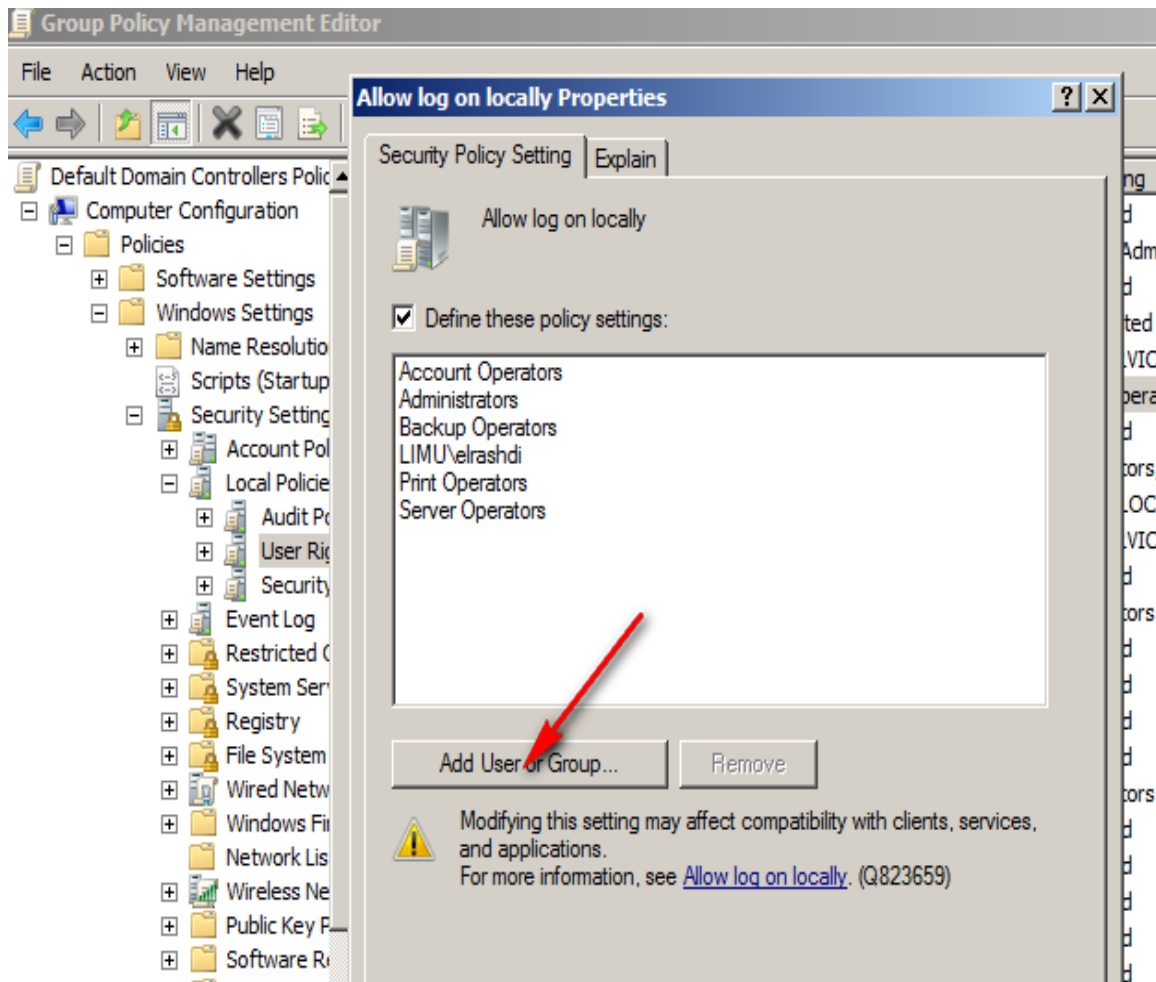


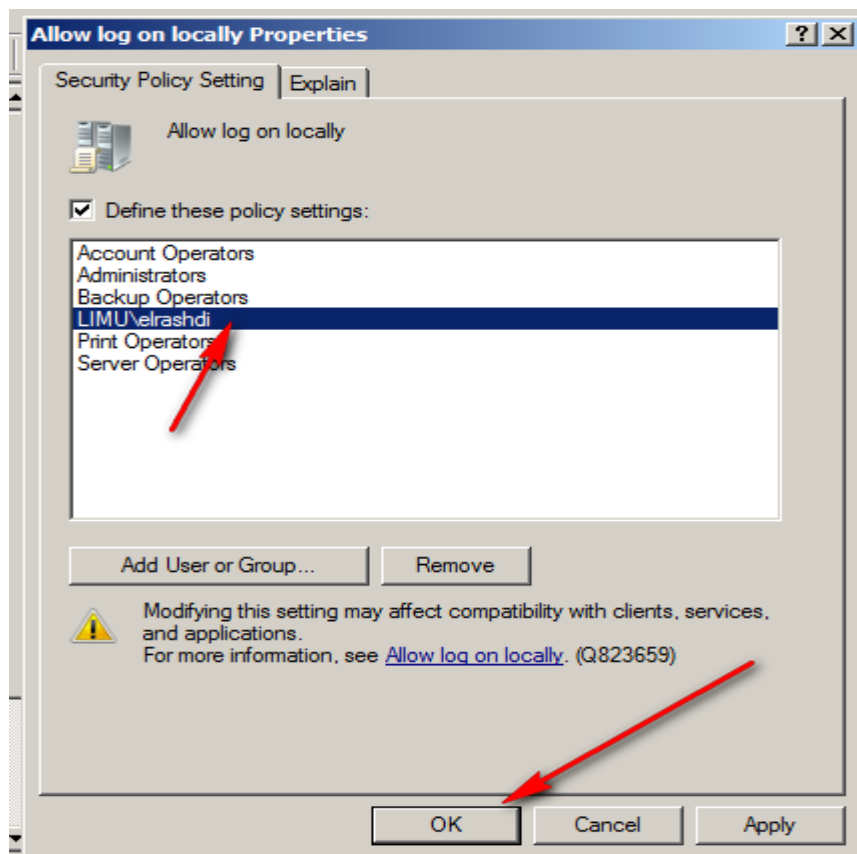
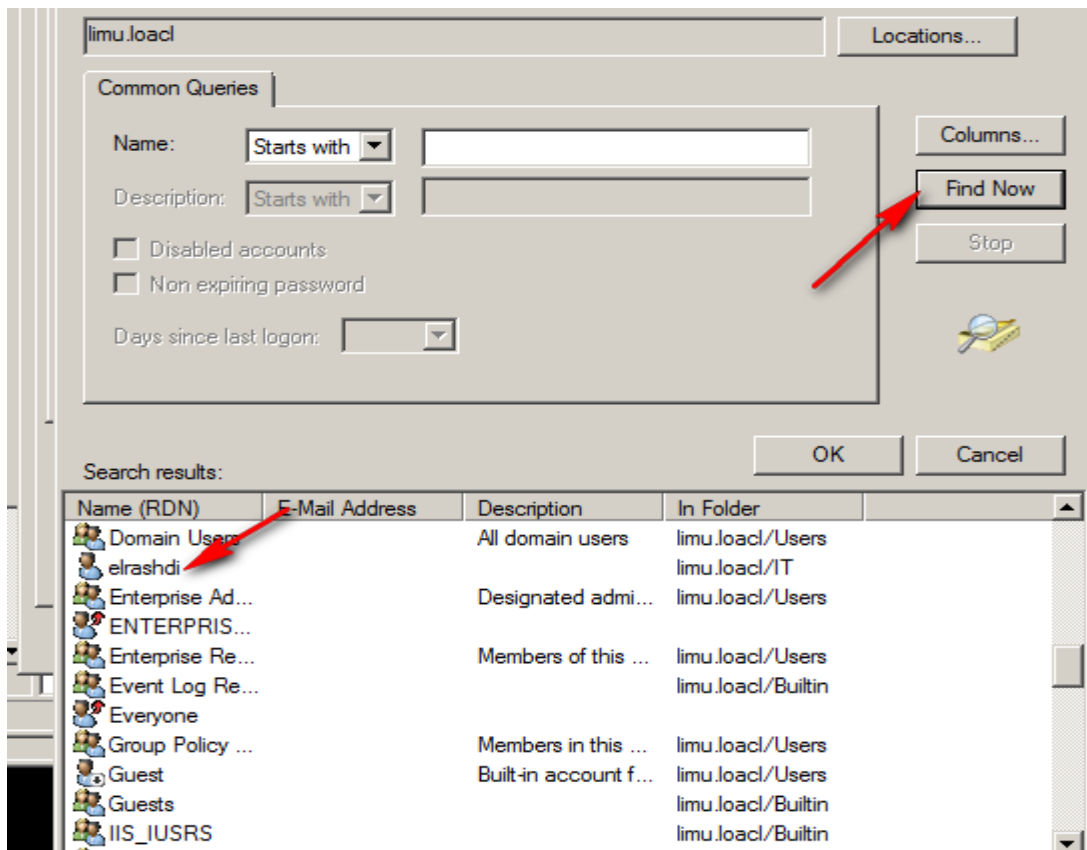
21.2- Allow user to connect locally on domain controller







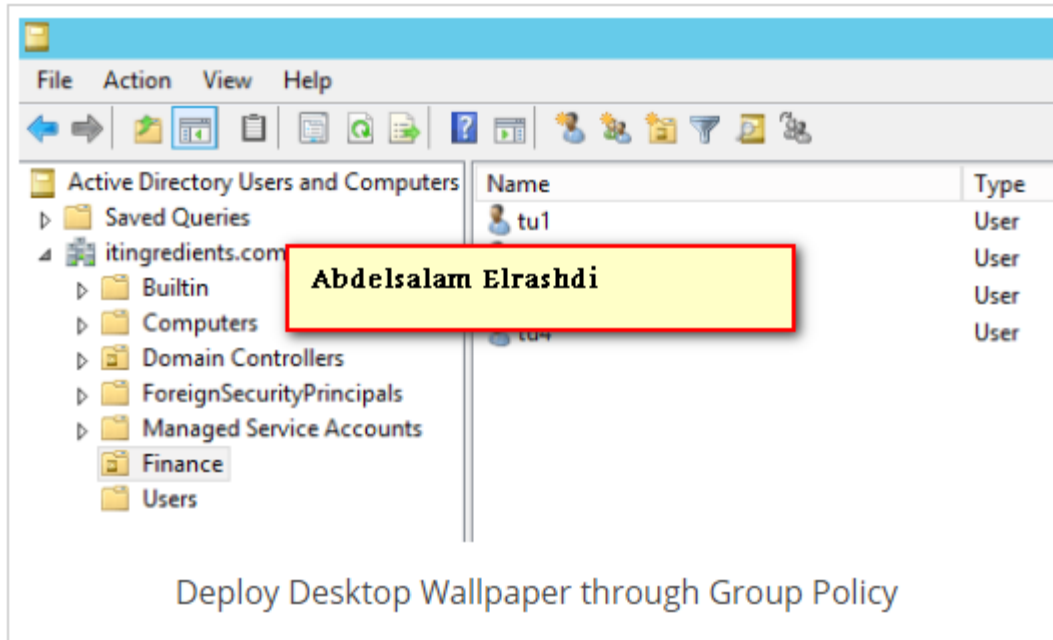




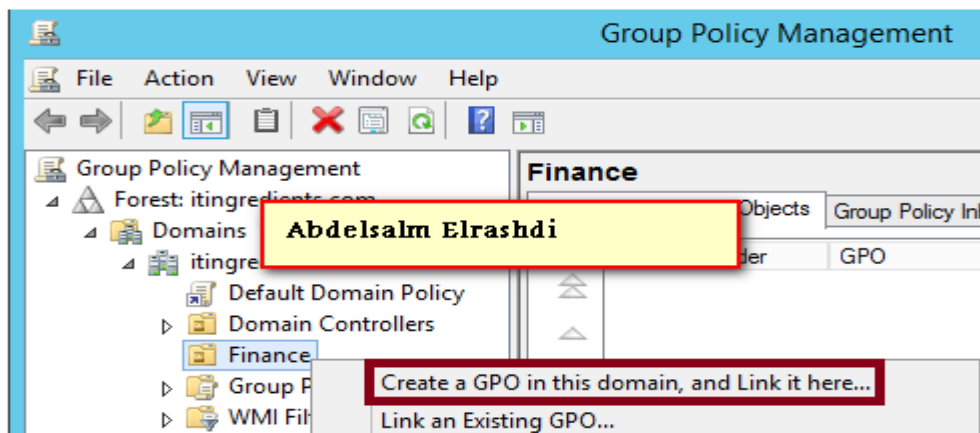
21.3- Change Desktop Wallpaper by Group Policy in Server 2012 R2

تغير خلفية سطح المكتب عن طريق القروب بولسي

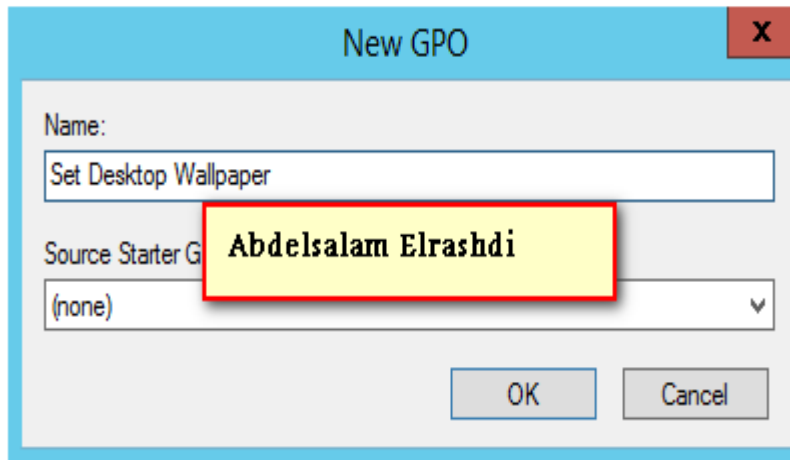
We have created an Organizational Unit (OU) naming “Finance” and added some users in the OU



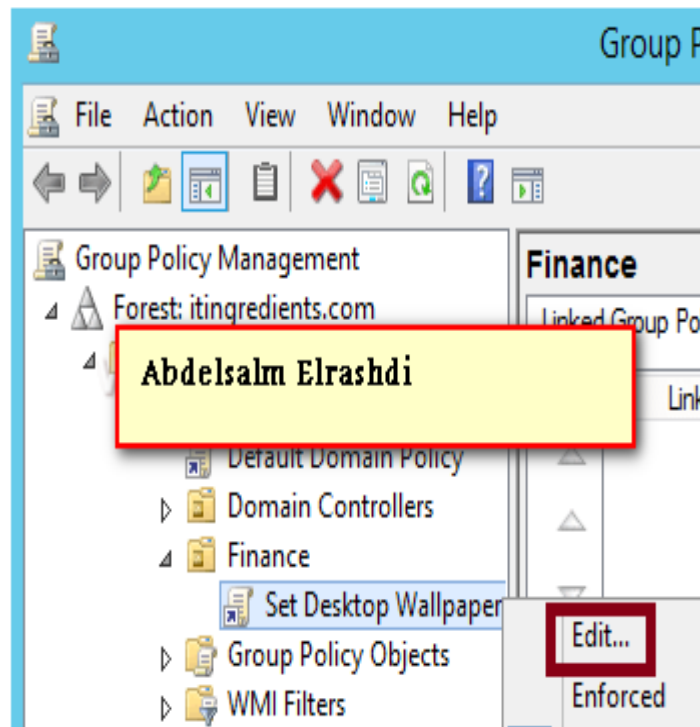
Open GPMC (Group Policy Management Console), right click on the OU “Finance” and then click on “Create a GPO in this domain, and Link it here”



On New GPO console, enter the name of group policy object. In this practical, the name of our GPO is “Set Desktop Wallpaper“. Click on Ok.

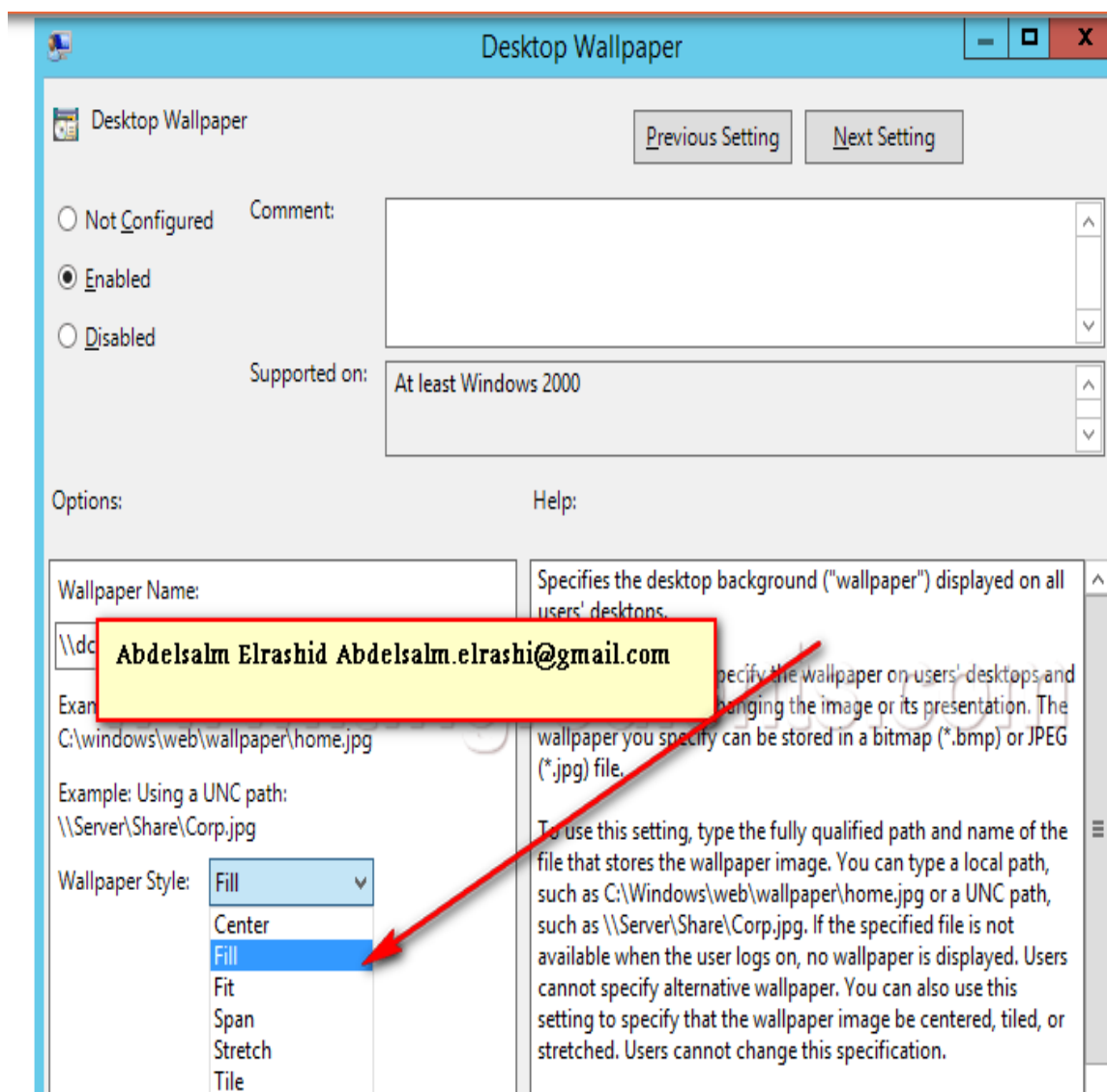


To deploy desktop wallpaper through Group Policy, right click on the GPO “Set Desktop Wallpaper” and click on “Edit” to modify the GPO settings. Default Group Policy Objects are blank templates, we have to define the policy to make it work.



To Set Desktop Wallpaper via Group Policy, on Group Policy Management Editor Console, under User Configuration expand Policies then expand Administrative Templates. Under Desktop, click on Desktop to expand all policies. Now double click on Desktop Wallpaper to open its settings.

Under Desktop wallpaper console, we have to give the fully qualified path and name of the file that stores the wallpaper image. If the specified file is not available when the user logs on, no wallpaper is displayed. Moreover, users cannot specify alternative wallpaper. Select Enabled to enable the policy and specify the UNC path \\dc01\share\wallpapers\wall01.jpg. You can also use the setting to specify that the wallpaper image be centered, tiled, or stretched. Users cannot change this specification.



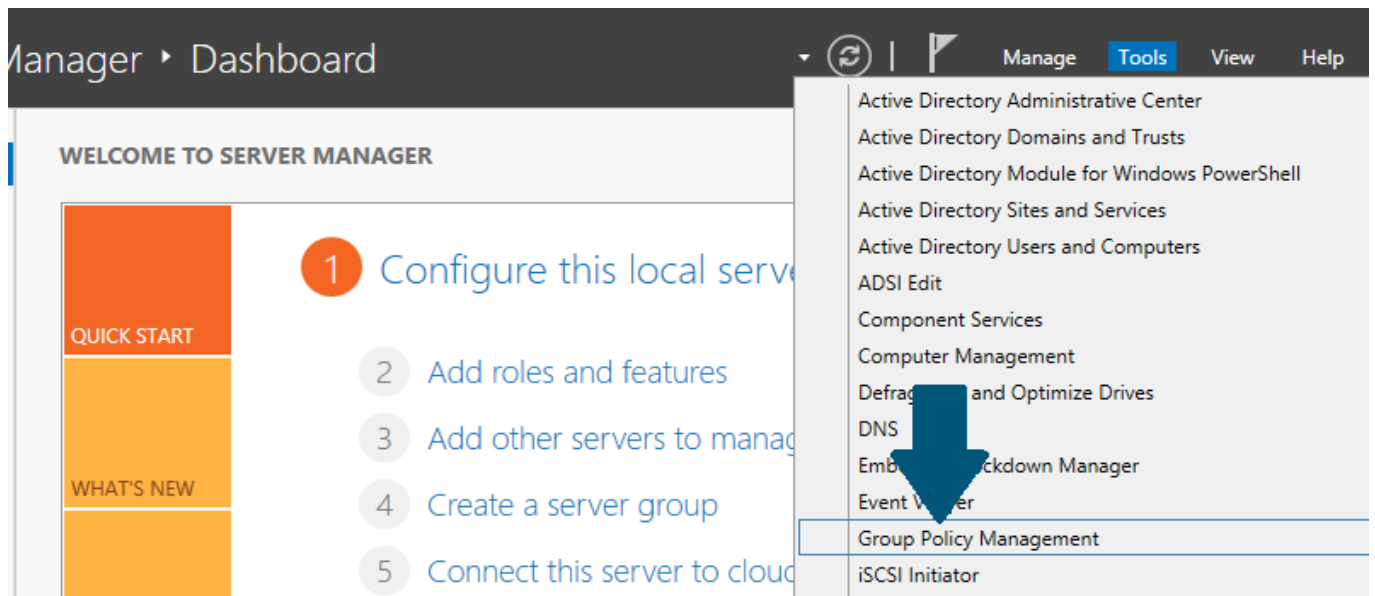
Now go to the client machine and login with the Domain User. You can see new Desktop Wallpaper would be deployed for the all the users created in Finance OU.

21.4- Hide C Drive Using Group Policies in Active Directory on Windows Server 2012 R2

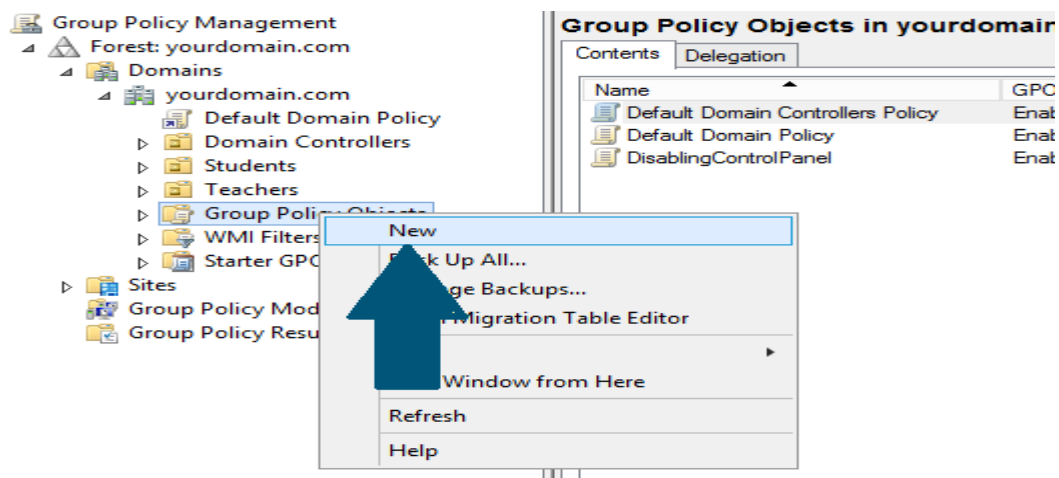
إخفاء القرص الصلب C على جهاز معين

Creating a Group Policy Object

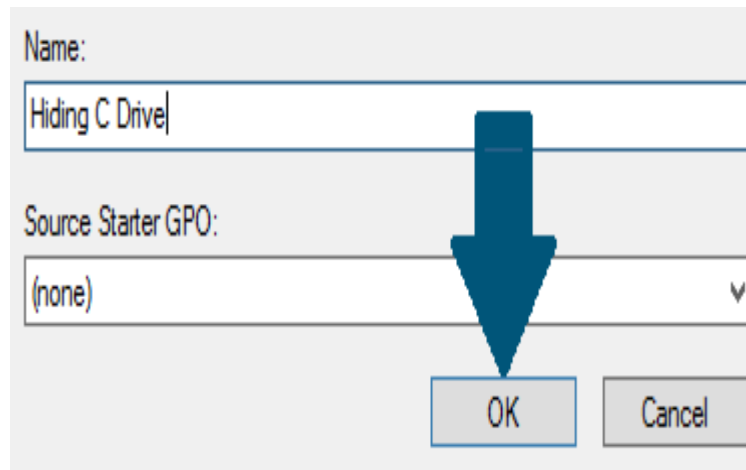
Open server manager dashboard and click **Group Policy Management**.



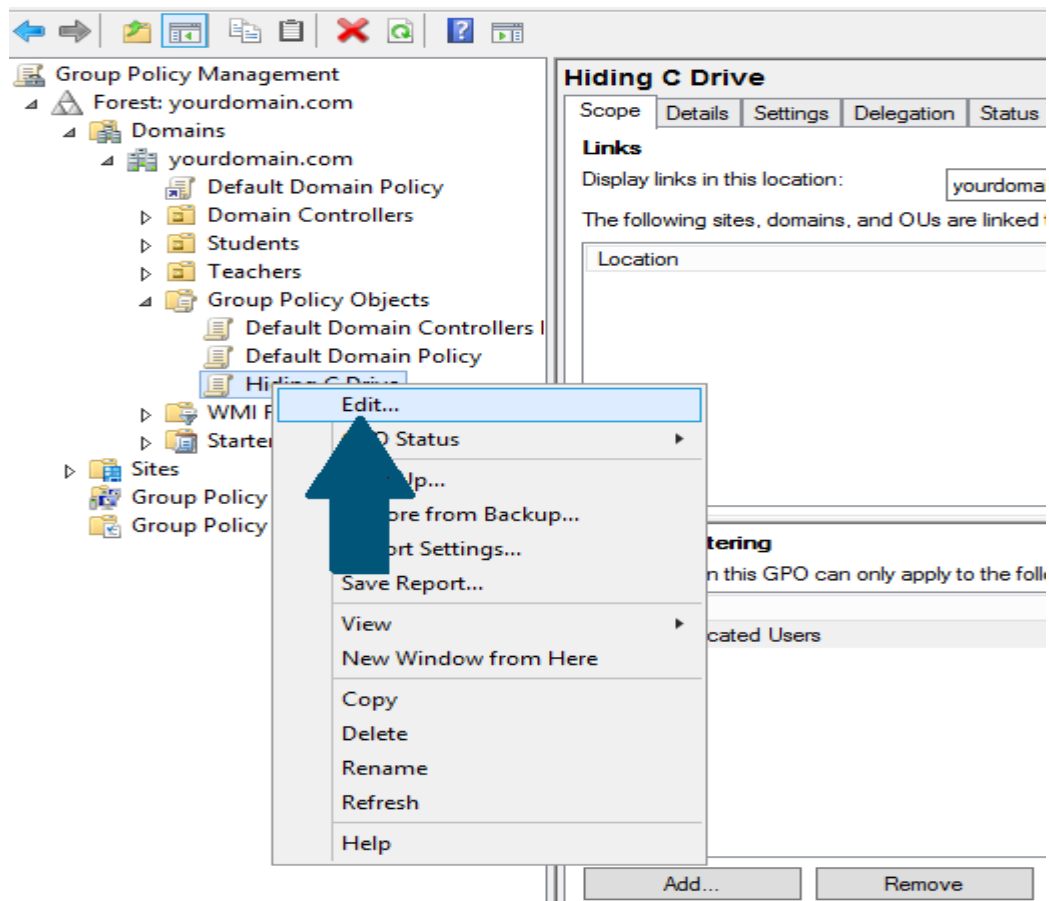
Expand the Tree: <domain name> node and right-click **Group Policy Objects**. Click **New**.



Provide a meaningful name and click **OK**.



Right-click the GPO (Group Policy Object) you created in above step and click **Edit**.



Go to **User Configuration > Administrative Template > Windows Components > File Explorer**. Right-click **Hide these specified drives in My Computer** and click **Edit**.

Windows Components

- Add features to Windows 8.1
- App runtime
- Application Compatibility
- Attachment Manager
- AutoPlay Policies
- Credential User Interface
- Desktop Gadgets
- Desktop Window Manager
- Digital Locker
- Edge UI
- File Explorer**
- File Revocation
- IME
- Instant Search
- Internet Explorer
- Location and Sensors
- Microsoft Management Console
- NetMeeting
- Network Projector
- Network Sharing
- Presentation Settings
- Remote Desktop Services
- RSS Feeds
- Sound Recorder
- Tablet PC
- Task Scheduler
- Windows Calendar
- Windows Color System

File Explorer

Hide these specified drives in My Computer

Edit [policy setting](#)

Requirements:
At least Windows 2000

Description:
This policy setting allows you to hide these specified drives in My Computer.

This policy setting allows you to remove the icons representing selected hard drives from My Computer and File Explorer. Also, the drive letters representing the selected drives do not appear in the standard Open dialog box.

If you enable this policy setting, select a drive or combination of drives in the drop-down list.

Note: This policy setting removes the drive icons. Users can still gain access to drive contents by using other methods, such as by typing the path to a directory on the drive in the Map Network Drive dialog box, in the Run dialog box, or in a command window.

Setting	State
Common Open File Dialog	
Explorer Frame Pane	
Previous Versions	
Turn off the display of thumbnails and only display icons.	Not configured
Turn off the display of thumbnails and only display icons on...	Not configured
Turn off the caching of thumbnails in hidden thumbs.db files	Not configured
Do not display the Welcome Center at user logon	Not configured
Turn on Classic Shell	Not configured
Display confirmation dialog when deleting files	Not configured
Location where all default Library definition files for users/m...	Not configured
Disable binding directly to IPropertySetStorage without inter...	Not configured
Turn off Windows Libraries features that rely on indexed file ...	Not configured
Disable Known Folders	Not configured
Turn off display of recent search entries in the File Explorer s...	Not configured
Allow only per user or approved shell extensions	Not configured
Start File Explorer with ribbon minimized	Not configured
Turn off the display of snippets in Content view mode	Not configured
Do not track Shell shortcuts	Not configured
Maximum number of recent items to display	Not configured
Remove CD Burning feature	Not configured
Turn off caching of thumbnails	Not configured
Remove UI to change menu	Not configured
Remove UI to change keyboard	Not configured
Remove DFS tab	Not configured
Hide these specified drives in My Computer	Not configured

Choose **Restrict C drive only** and click **Apply** and then **OK**.

Hide these specified drives in My Computer

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

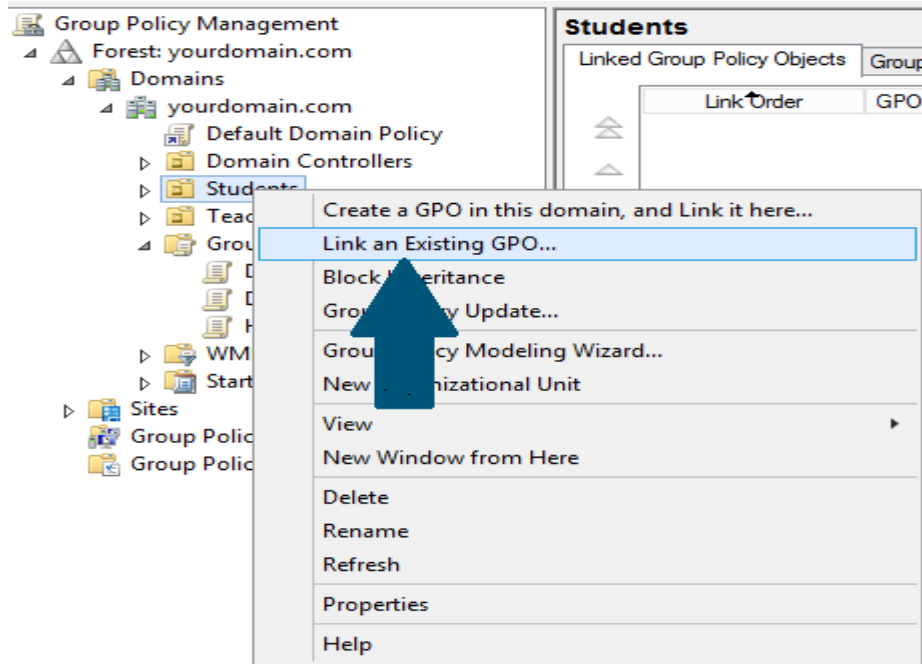
Supported on: At least Windows 2000

Options: **Restrict C drive only**

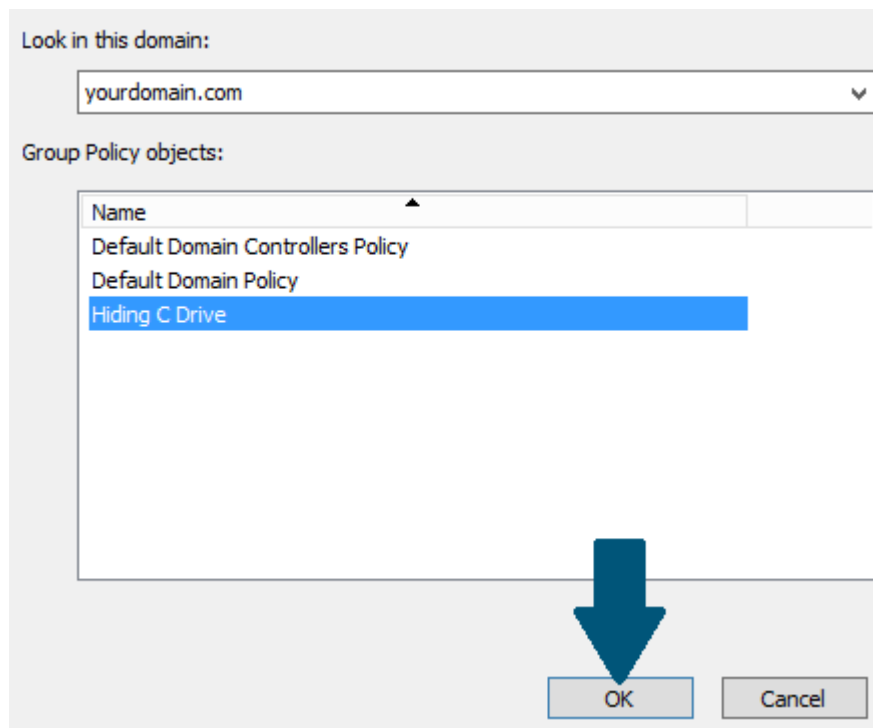
Help: This policy setting allows you to hide these specified drives in My Computer. This policy setting allows you to remove the icons representing selected hard drives from My Computer and File Explorer. Also, the drive letters representing the selected drives do not appear in the standard Open dialog box. If you enable this policy setting, select a drive or combination of drives in the drop-down list.

Linking a GPO (GroupPolicy Object) to an OU (Organisational Unit)

Right-click the OU (In my case it is Students) you need to apply the policy and click **Link an Existing GPO**.

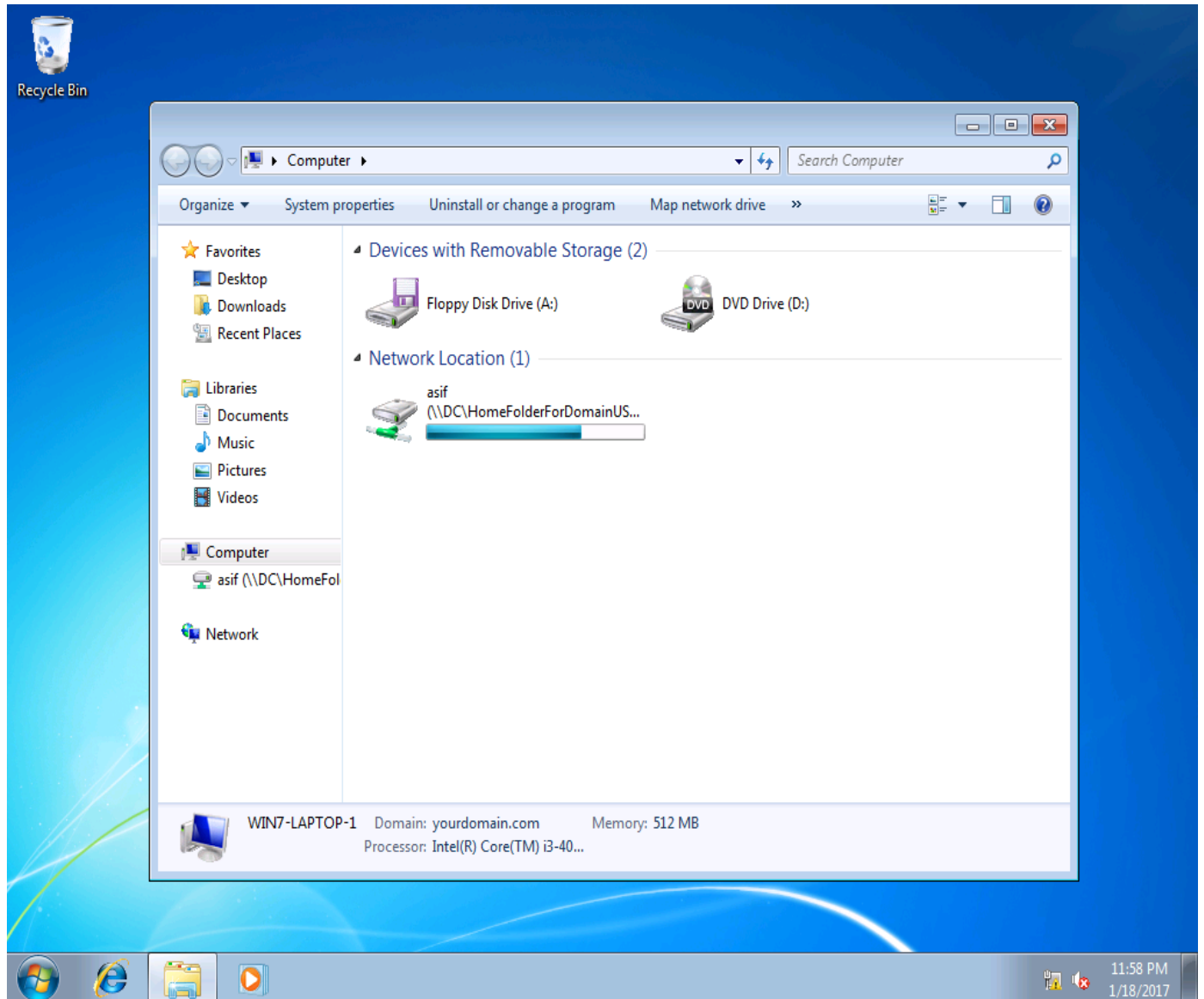


Choose the GPO you created in above steps and click **OK** and you are done.



Testing the Group Policy

Login to a client machine with a user and you will notice there is no C drive in My Computer. Make sure the user is from OU you chose in above steps.



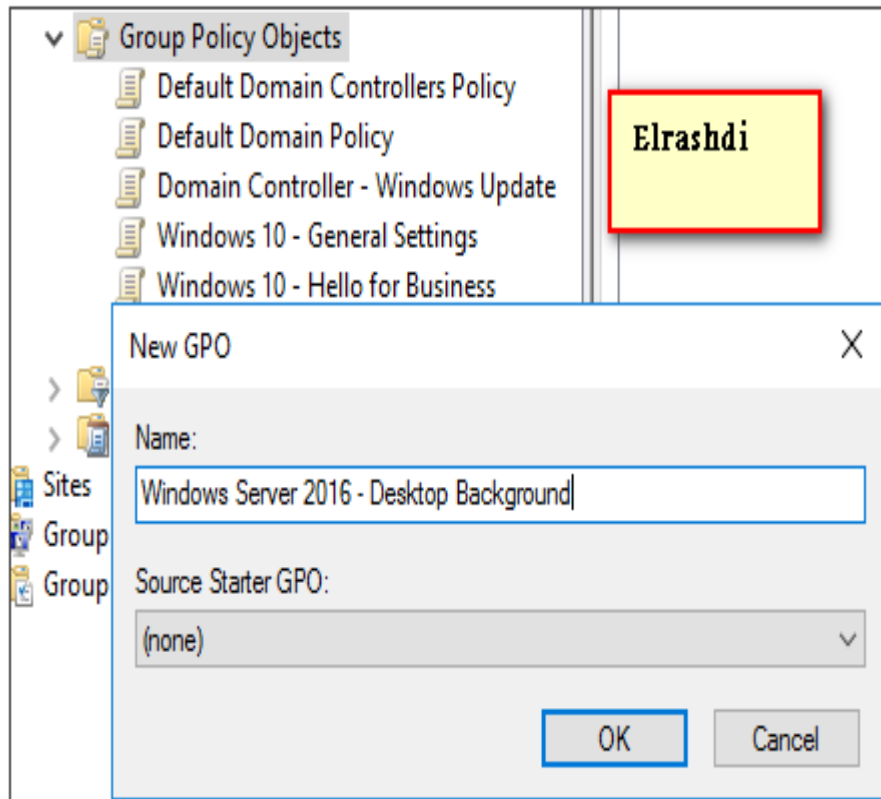
21.5- Changing the desktop background using Group Policy in windows server 2016

تغير خلفية سطح المكتب عن طريق قروب بولسي windows server 2016

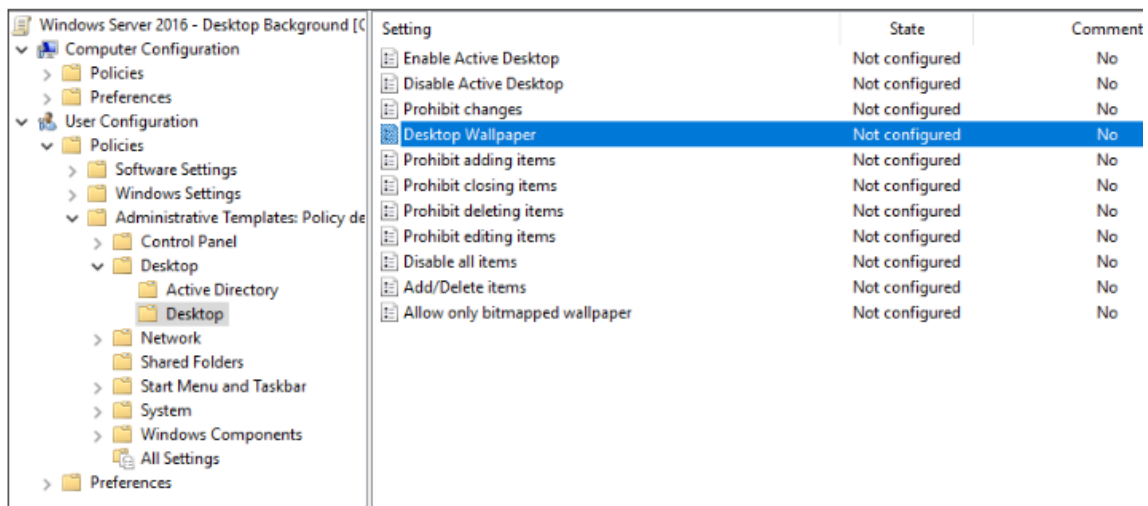
Group Policy Configuration

Right, lets fire up Group Policy Management.

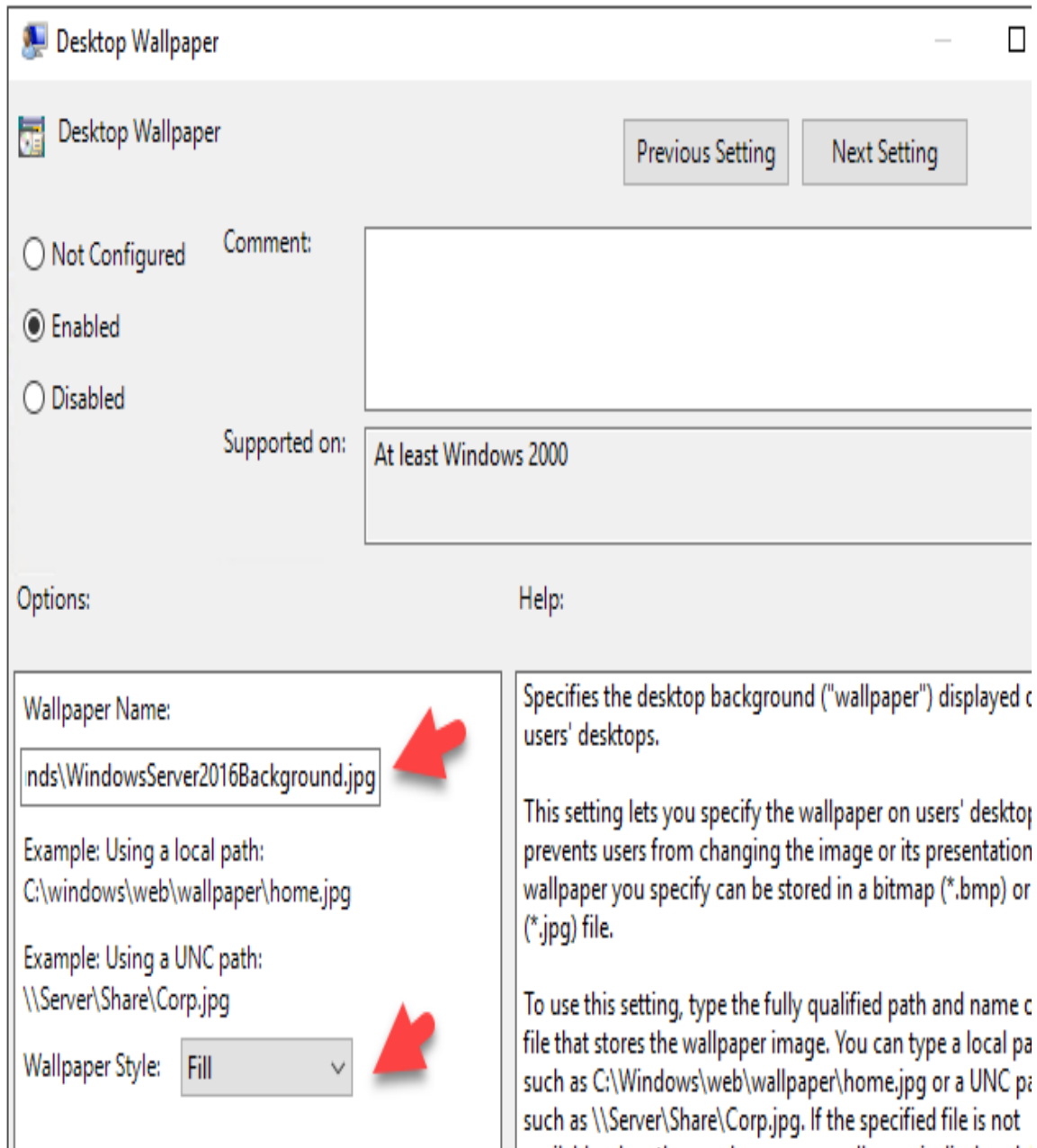
To start with we'll create a new Group Policy Object, I'll call it "Windows Server 2016 – Desktop Background"



The policy setting that we want to edit is under "User Configuration" -> "Policies" -> "Administrative Templates" -> "Desktop" -> "Desktop" -> "Desktop Wallpaper"



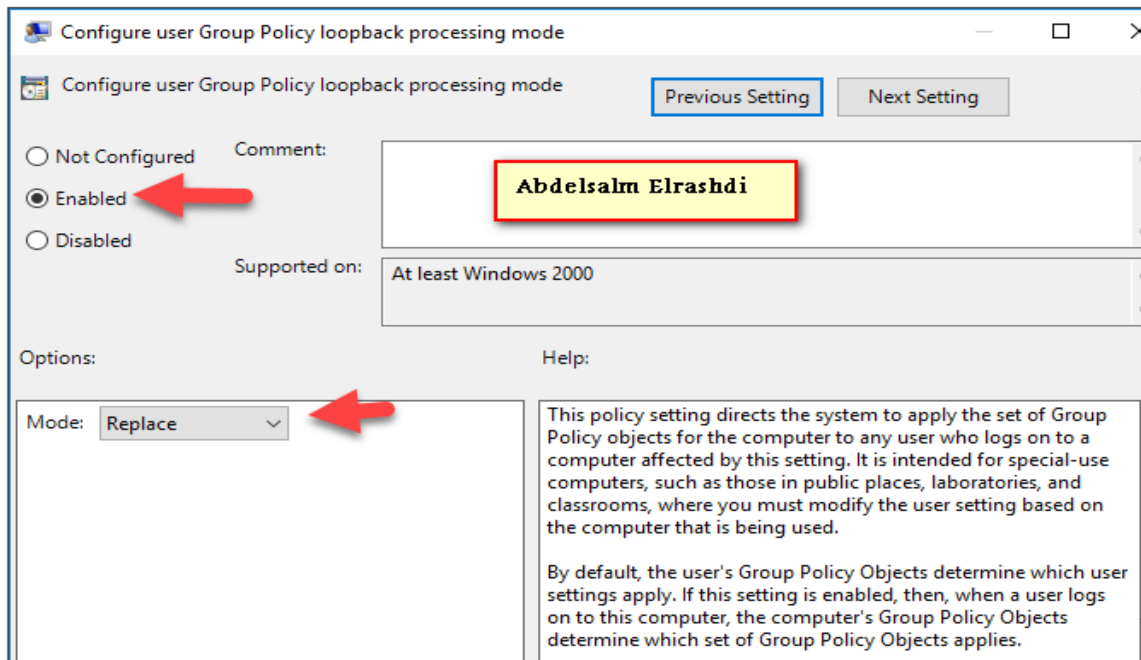
Double click the “Desktop Wallpaper” setting



- Click “Enable”
- Set the wallpaper name to the UNC of the location of your desktop image file i.e. \\domain.com\NETLOGON\Backgrounds\WindowsServer2016Background.jpg
- Set the “Wallpaper style” to “Fill”

- Click “OK”

Within the same GPO navigate to “Computer Configuration” -> “Policies” -> “Administrative Templates” -> “System” -> “Group Policy” and locate the GP setting called “Configure user Group Policy loopback processing mode”

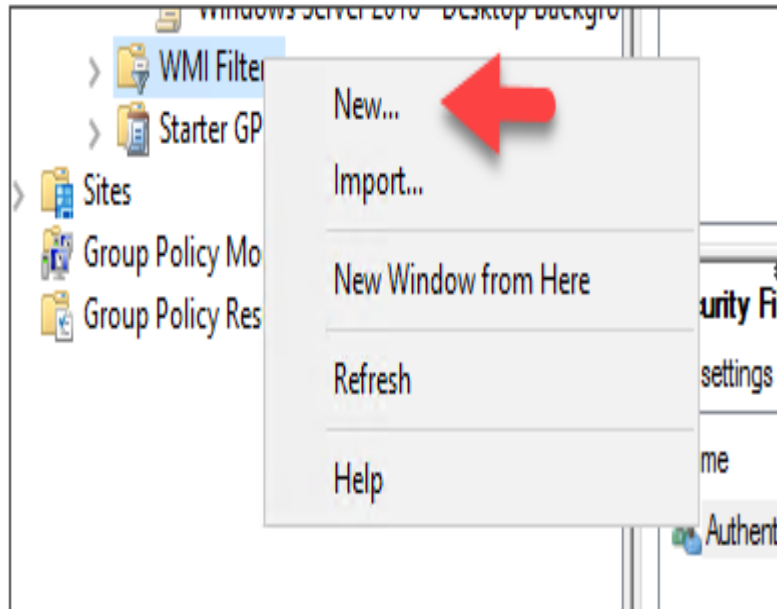


Enable this setting and change the “Mode” to “Replace”

The reason for this setting is to ensure that the “User Configuration” settings are applied to the server when the user logs in. If this setting isn’t configured the policy won’t get applied to the server because the GPO is only associated to a OU with server (computer) objects. Once done we can close this window and return to the Group Policy Management screen.

Ok, as mentioned above this GPO is going to be applied to the server OUs however I suspect that your server OUs also contain Windows 2008/2012/2012R2 servers and you don’t want a Server 2016 desktop applied to these servers. To stop this from happening we can create a WMI filter that’ll single out Server 2016 servers.

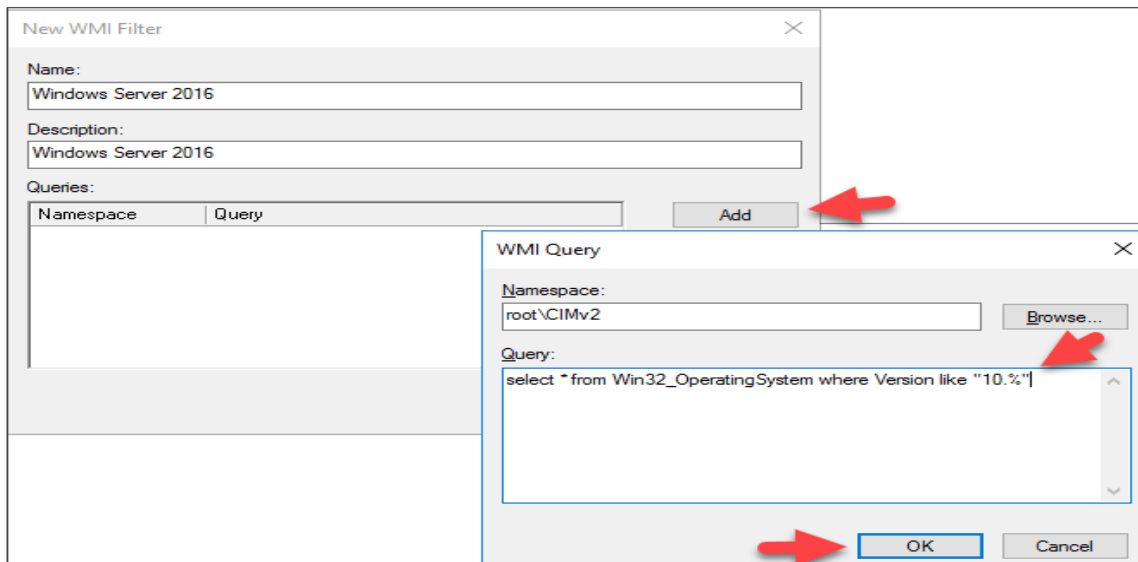
So...from Group Policy Management find “WMI Filters”, right click it and select “New”



Give it a name and description i.e. “Windows Server 2016”

In the queries window click “Add” and add the following query

*select * from Win32_OperatingSystem where Version like “10.%”*

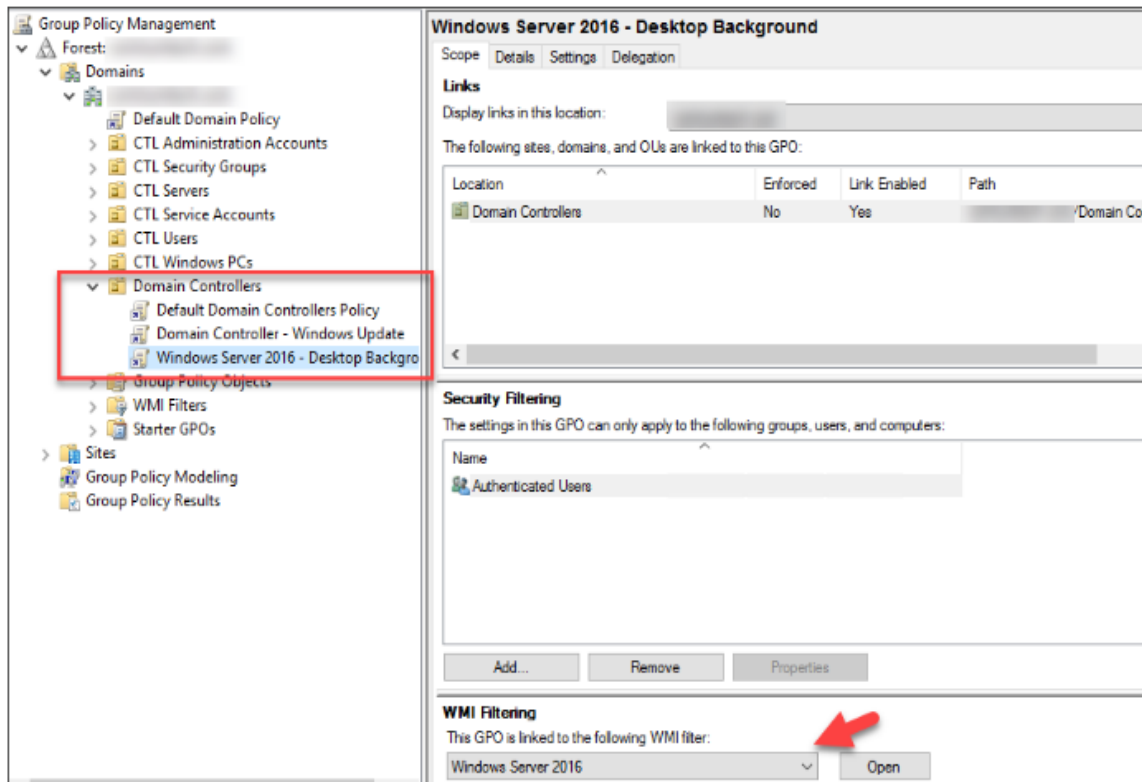


This query will ensure that the OS version is 10 (i.e. Server 2016) and won't apply to any OS versions below this. Click “OK” and click “Save” to exit the WMI filter window.

Applying the GPO

Ok, so we have our nice new GPO created, the background image on the server and finally a WMI filter created to ensure that only 2016 Servers get the new background.

We just need to apply this GPO to the OU container that houses the servers, in my example I am targeting the DCs. Then we need to set the WMI filter on the GPO to be the one we just created above.



All needs to be done now is to run GPUPDATE on the servers. Log off and log back in and see that nice new background!

22-Delegation in windows server

اعطاء تفويض او صلاحيه للمستخدم او مجموعة من المستخدمين على مستوى الدومين او container او OU

Delegation is one of the most important security features of Active Directory Domain Services.

Delegation enables a higher administrative authority to grant specific administrative rights for

containers and subtrees to individuals and groups. Domain administrators, with broad authority over large segments of users, are no longer required.



22.1- Delegation in windows server 2008

تفويض او صلاحيات علي طريق windows server 2008

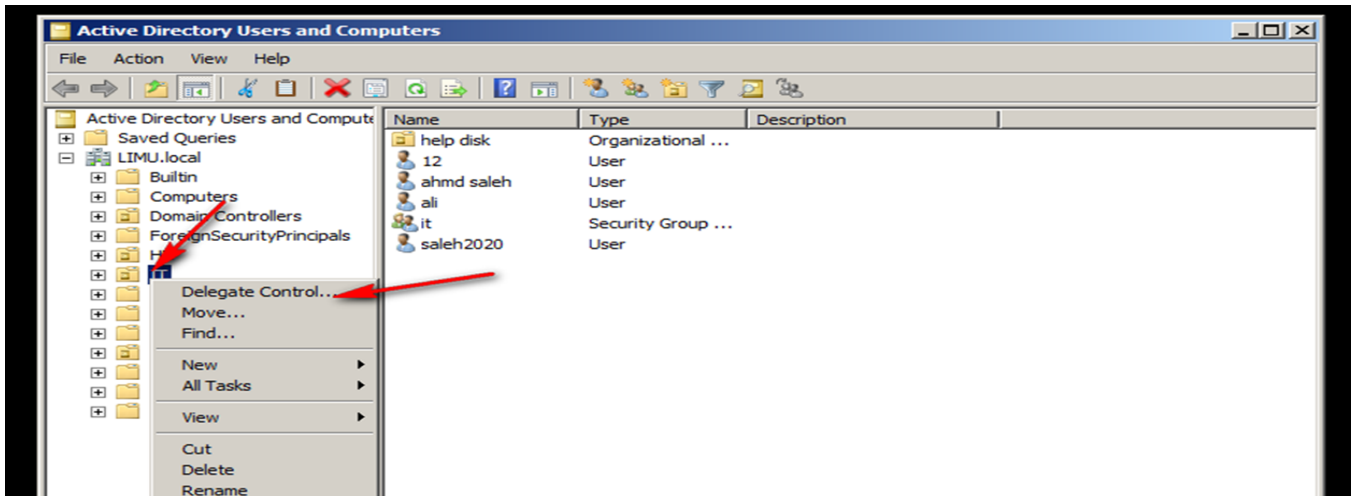
You can use the Delegation of Control Wizard to assign special permissions.

The following permissions can be set with one click:

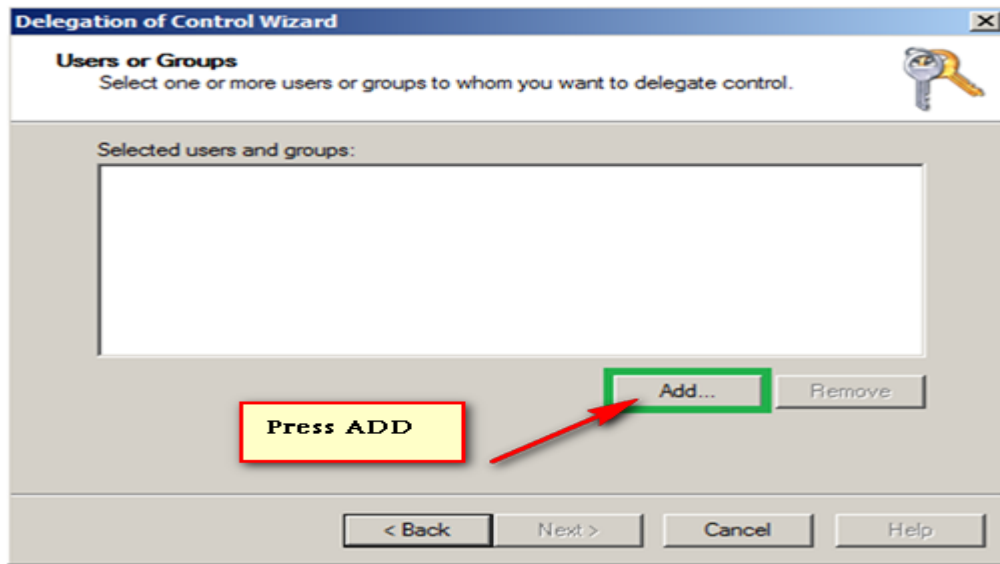
- Create, delete and manage user accounts
- Reset user passwords and force password change at next logon
- Read all user information
- Create, delete and manage groups
- Modify the membership of a group
- Manage Group Policy links
- Generate Resultant Set of Policy (Planning and Logging)
- Create, delete and manage inetOrgPerson accounts
- Reset inetOrgPerson password and force password change at next logon
- Read all inetOrgPerson information

Active Directory Delegation wizard

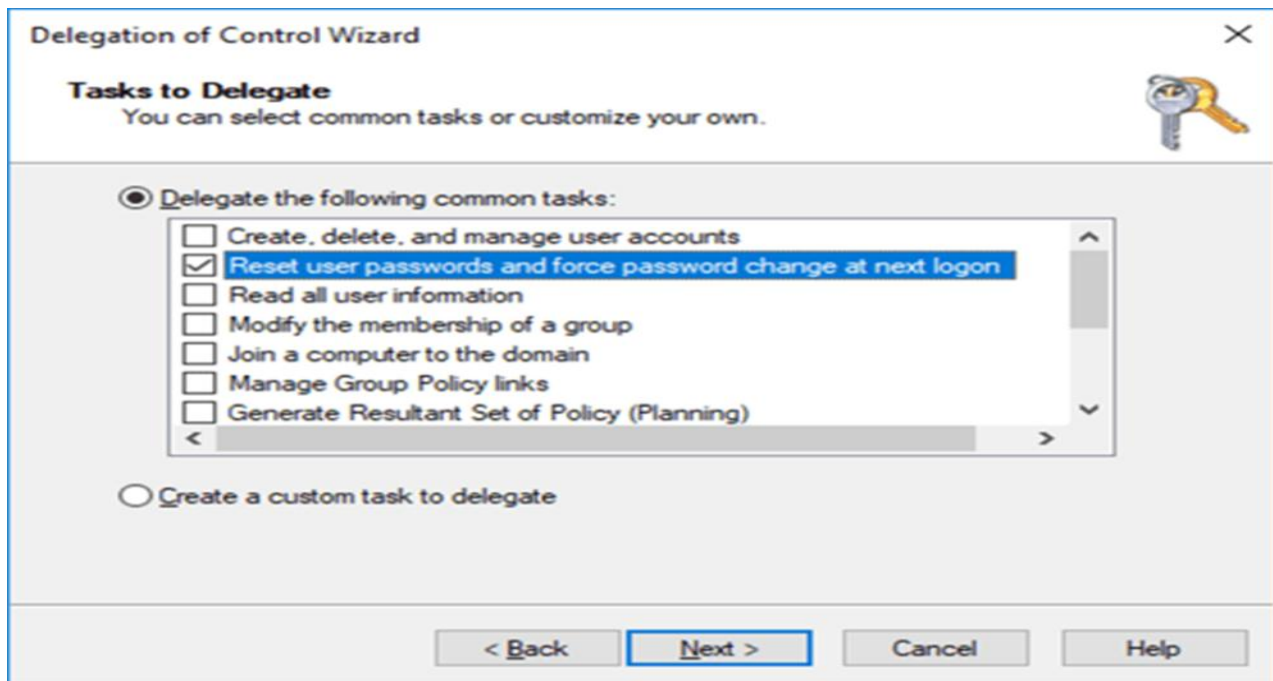
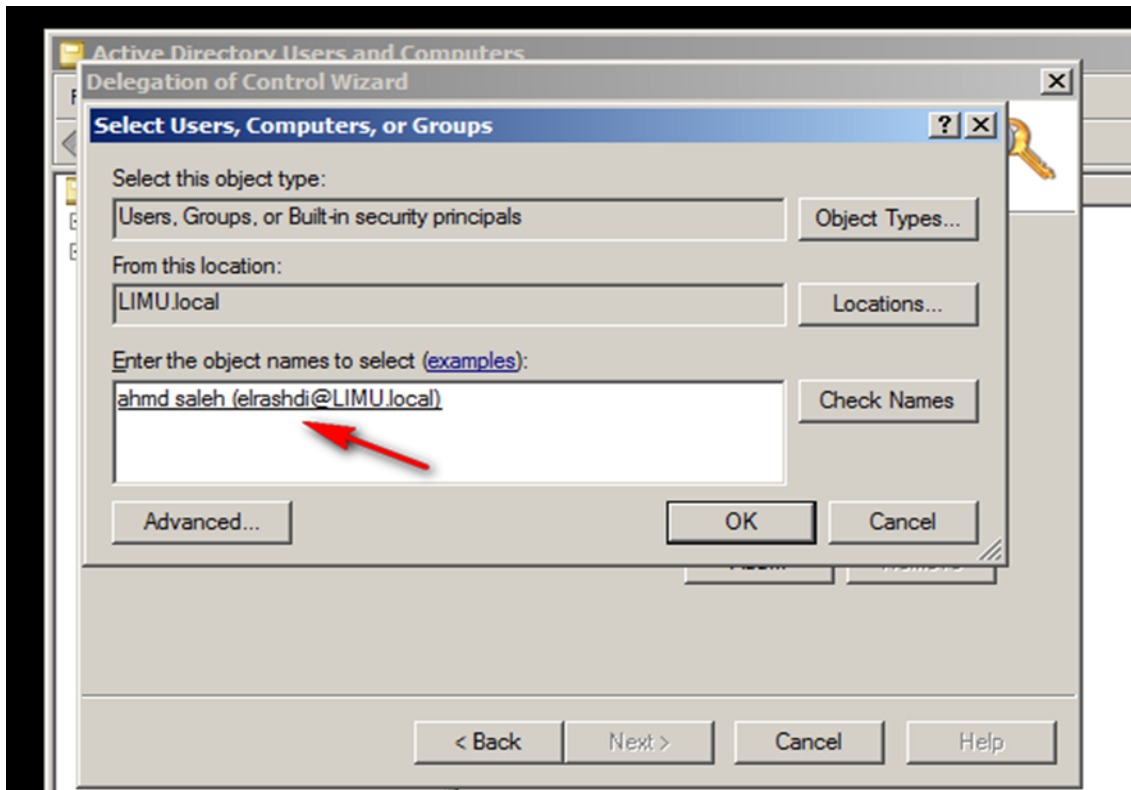
This wizard is available when you open Active Directory Users and Computers console and select Organizational Unit (OU) or domain on which you want to start delegating privileges. Click right mouse button and choose “Delegate Control...” option. You should see a wizard



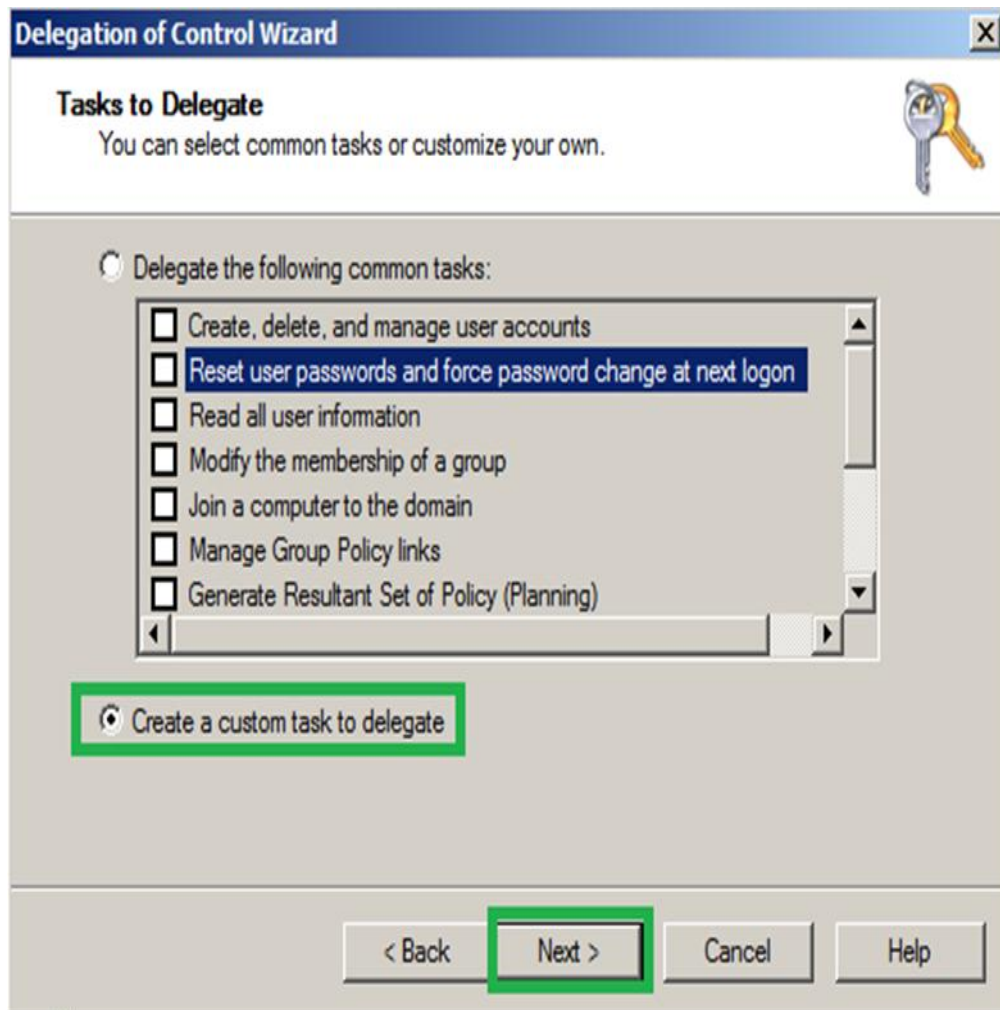
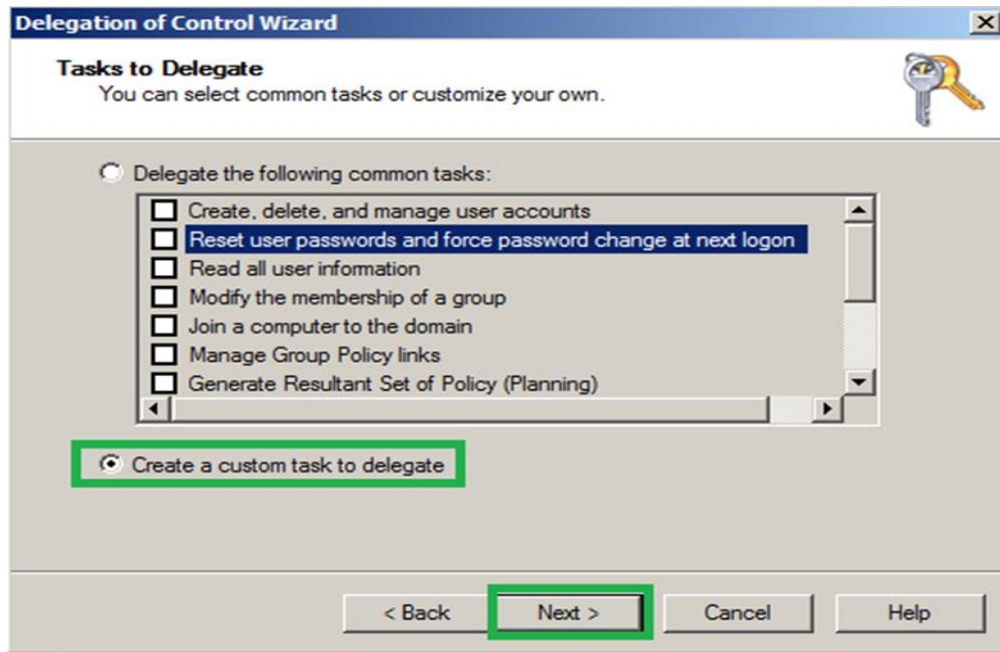
Follow with the wizard and choose desired options. At the first screen, you will be prompted for user or group to which you want to grant permissions.



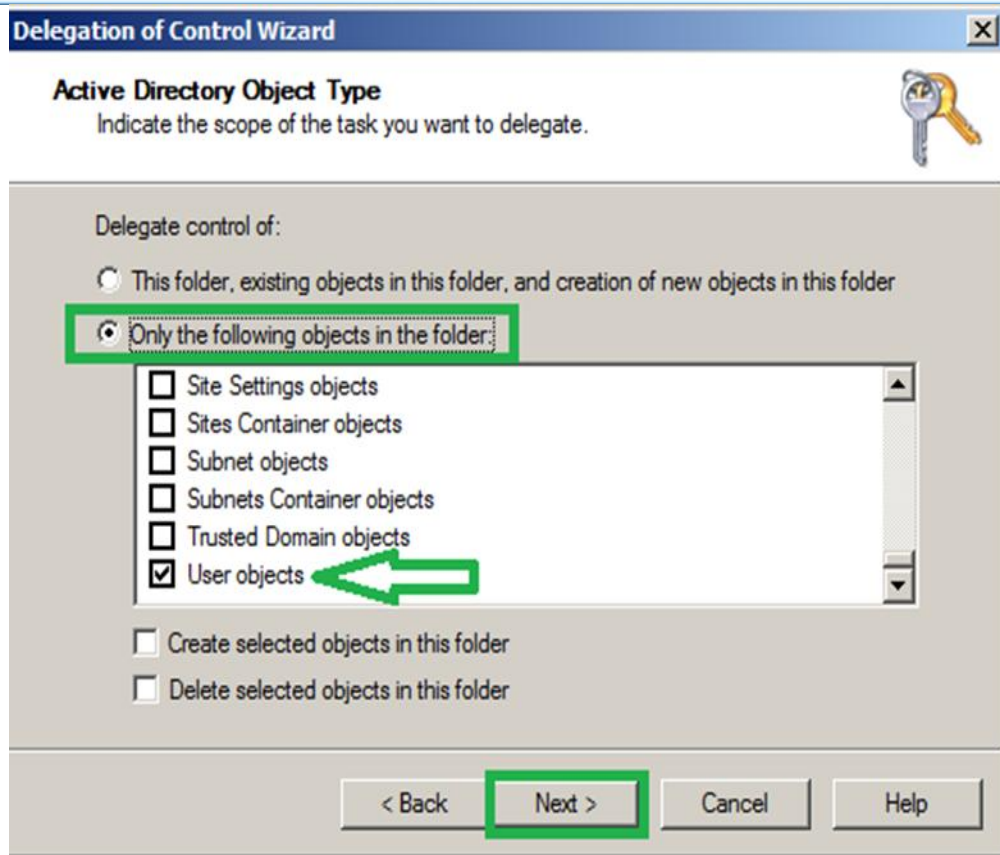
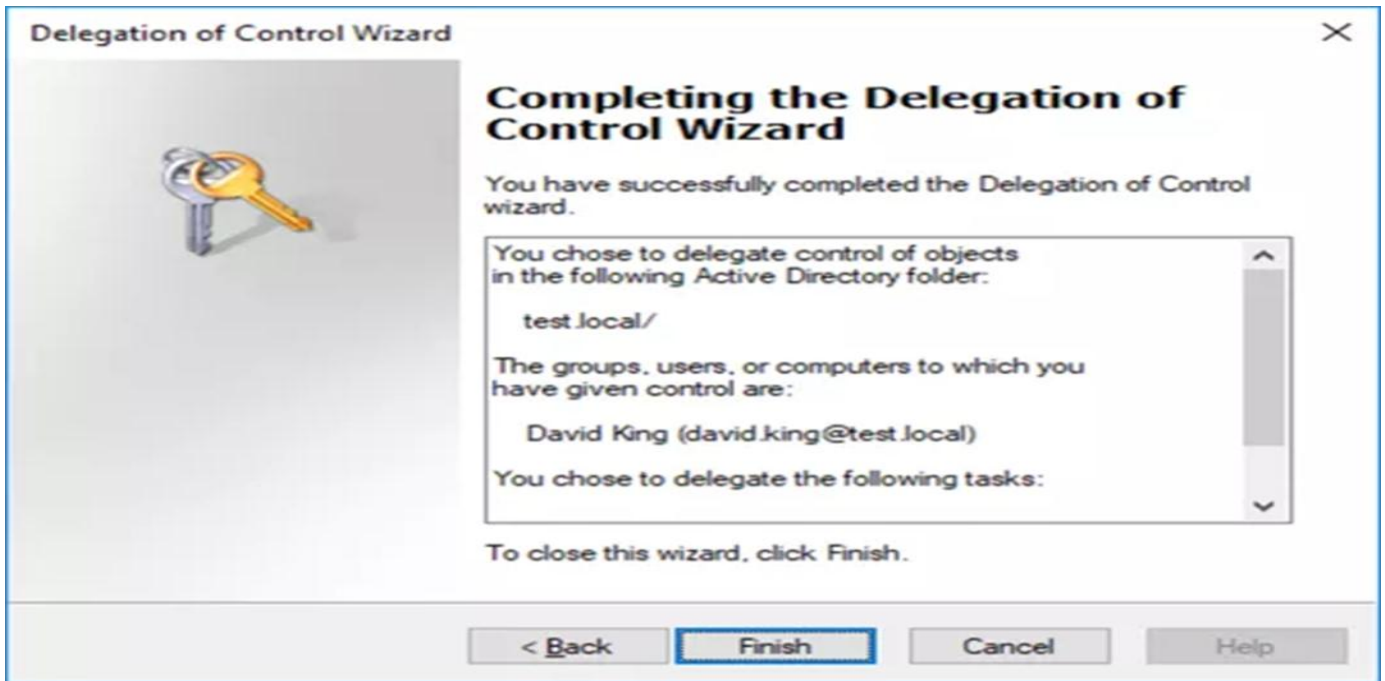
Note! It is good practice to not add users directly in Delegation Control wizard. Instead of adding them directly, please create dedicated group and grant permission to it. Put each user who requires permissions into that group.



In case that you want to create a custom task to delegate, choose the second option and click “Next” button



choose “Only the following objects in this folder” option and select appropriate object(s) from the list



22.2- Delegation in windows Server 2012

تفويض او صلاحيات علي طريق windows server 2012

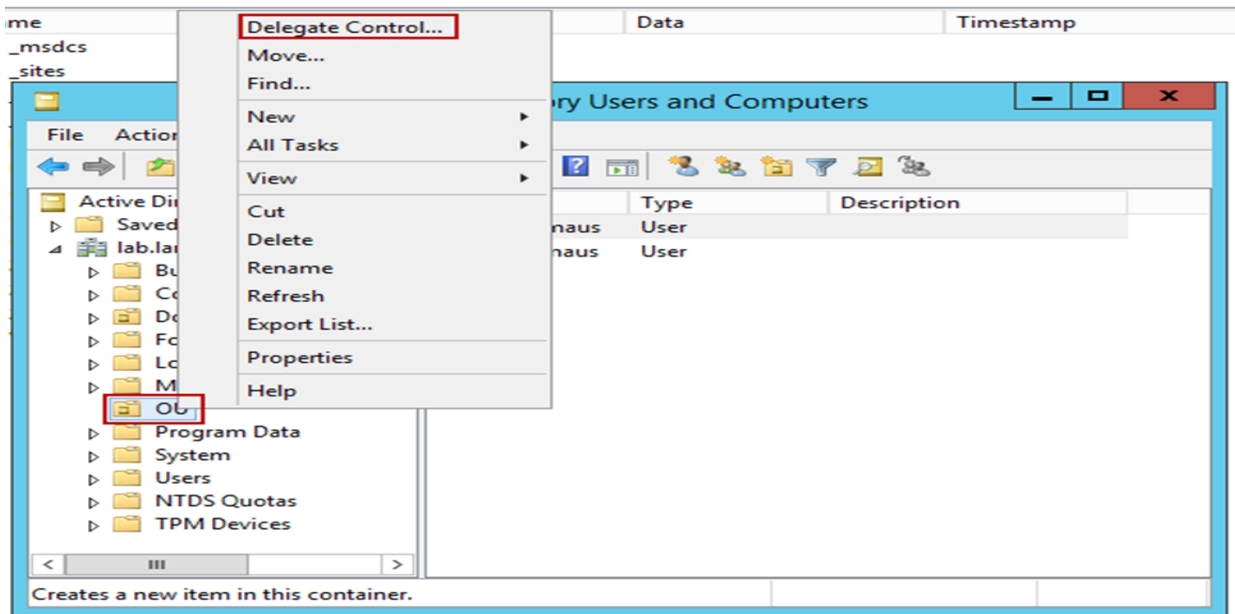
You can use the Delegation of Control Wizard to assign special permissions.

- The following permissions can be set with one click:
- Create, delete and manage user accounts
- Reset user passwords and force password change at next logon
- Read all user information
- Create, delete and manage groups
- Modify the membership of a group
- Manage Group Policy links
- Generate Resultant Set of Policy (Planning and Logging)
- Create, delete and manage inetOrgPerson accounts
- Reset inetOrgPerson password and force password change at next logon
- Read all inetOrgPerson information

Here is an example.

In Users and Computers click on a OU or group with the right mousekey.

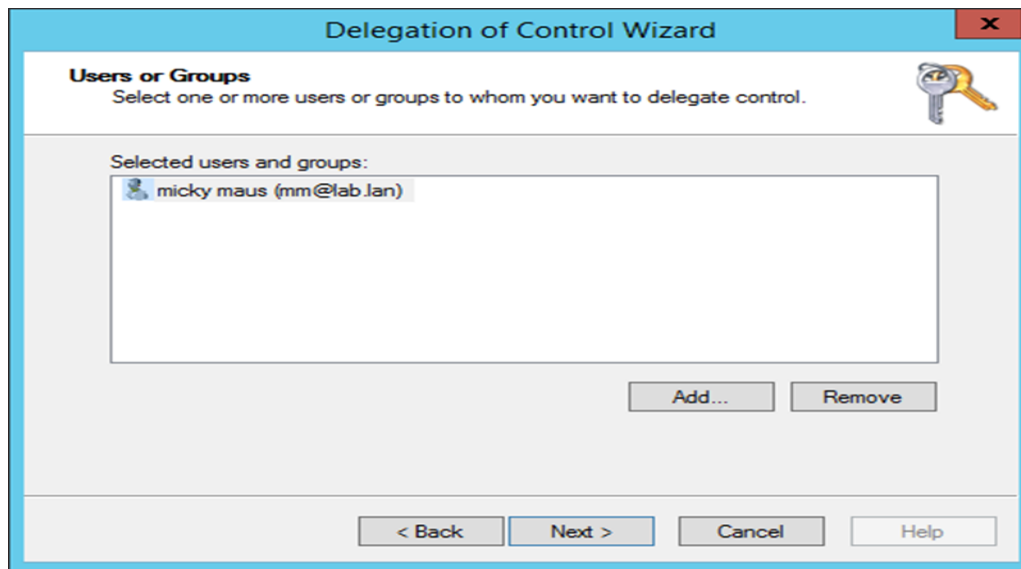
Click "Delegate Control"



The "Delegation of Control Wizard" starts

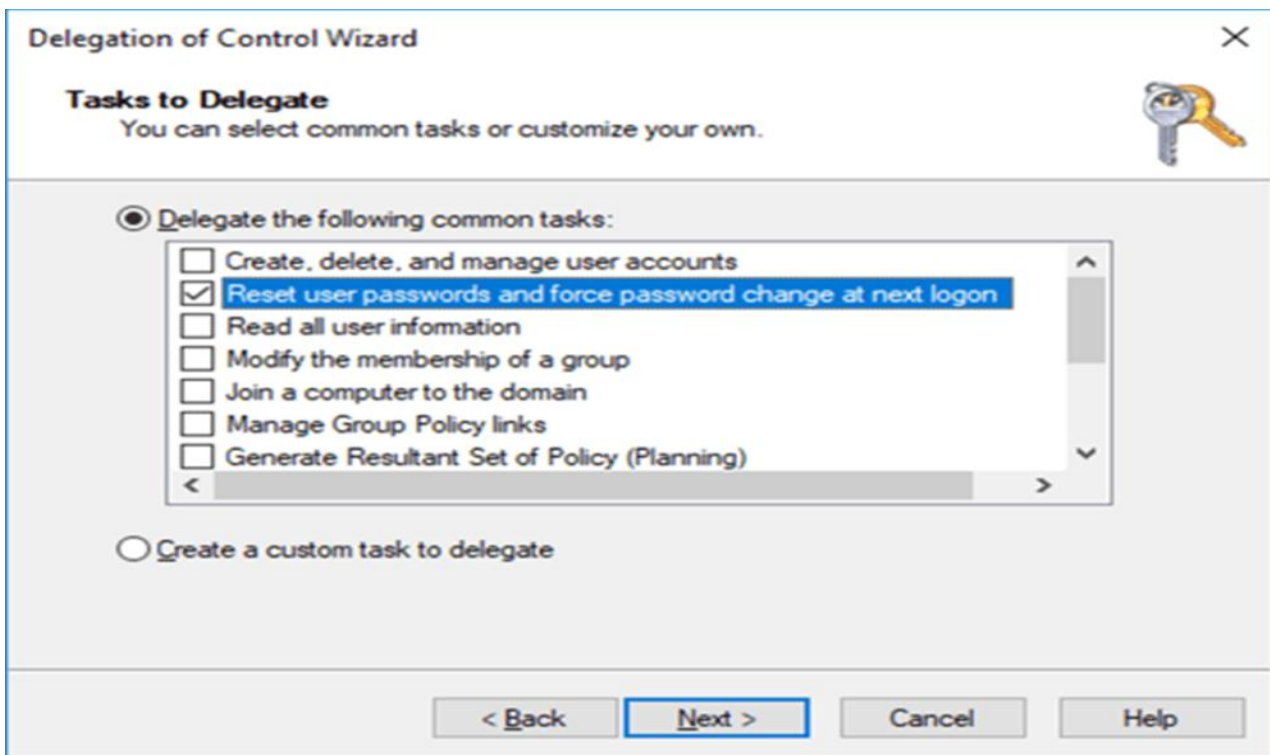
Click "Next"

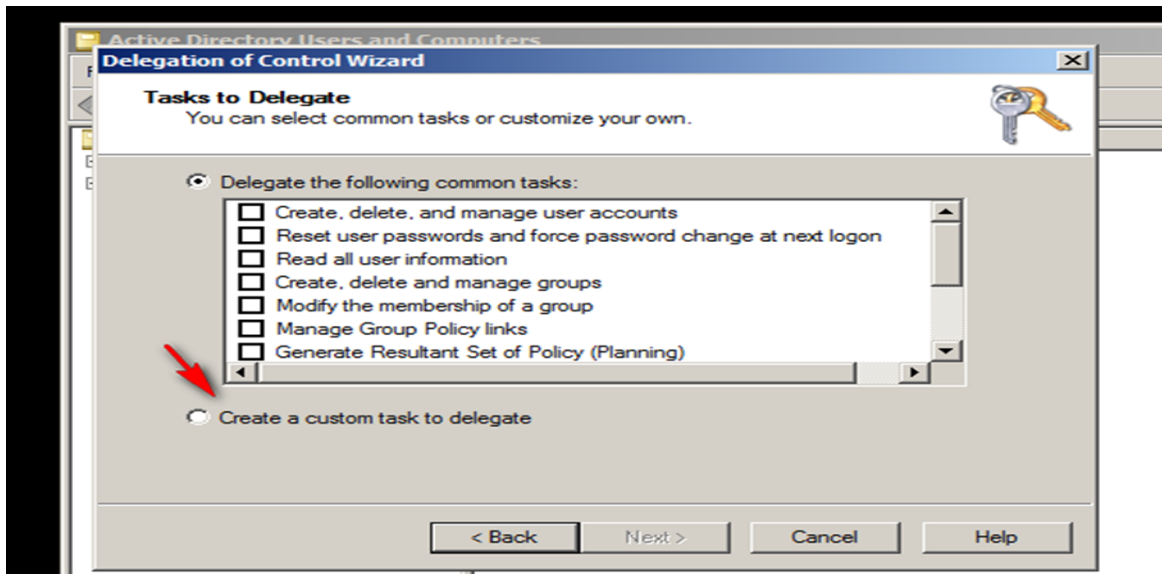
Select a User or Group



Click "Next"

Select the rights you want to delegate





23- Security and Sharing windows server

the difference between share permissions and file permissions; essentially they refer to the security setting that a user may have on a local server, versus a folder or file shared on that server. In short, share permissions apply to files or folders shared over the network and file permissions are used to restrict a user who is logged onto that machine. Figuring out how these permissions combine was a pain in NT, however Microsoft has included an effective permissions tool with XP and Windows Server 2003. Just click on the shared file or folder in Explorer, choose the Security tab, click Advanced, and then choose the tab for Effective Permissions.

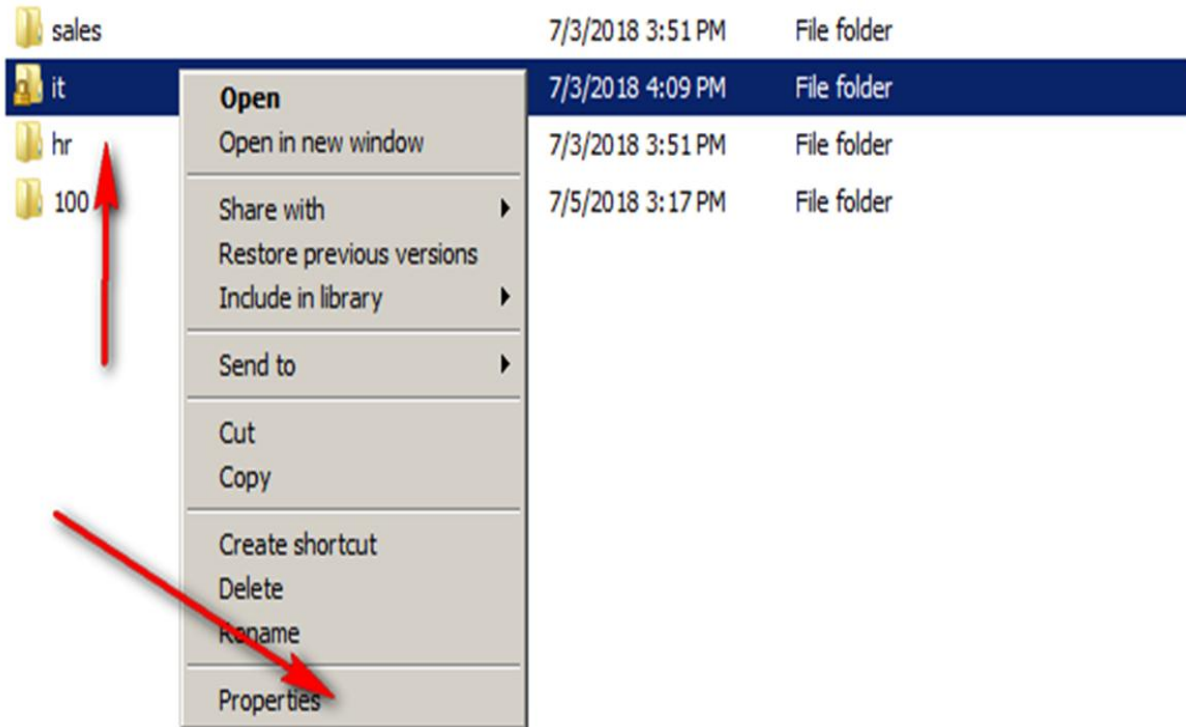


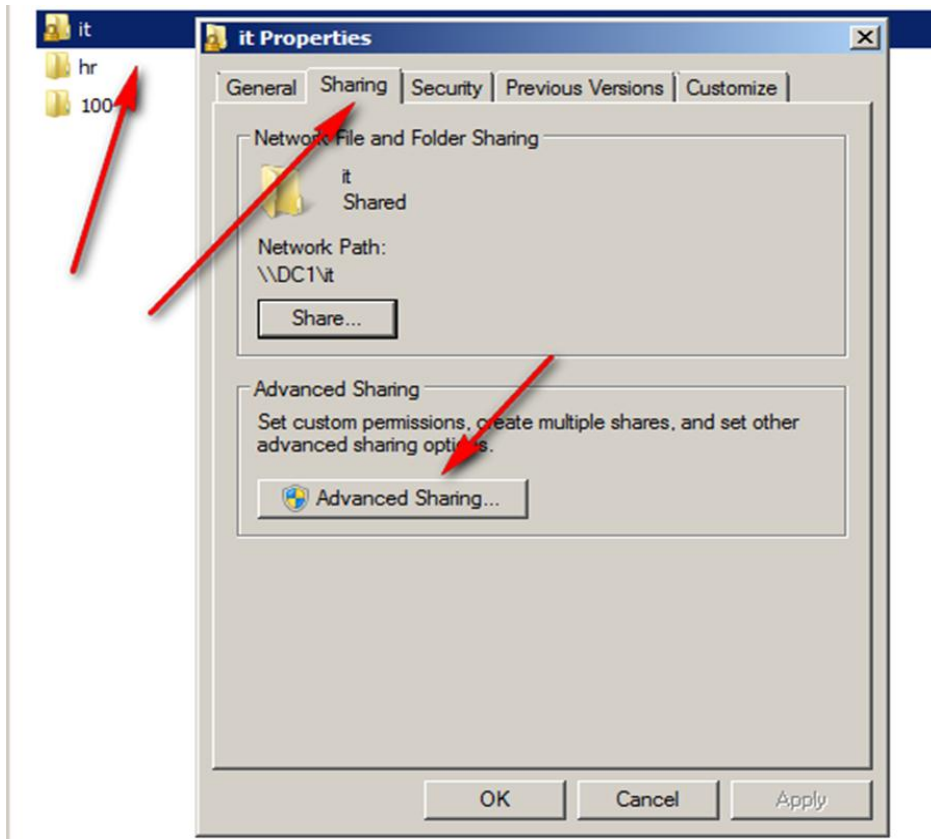
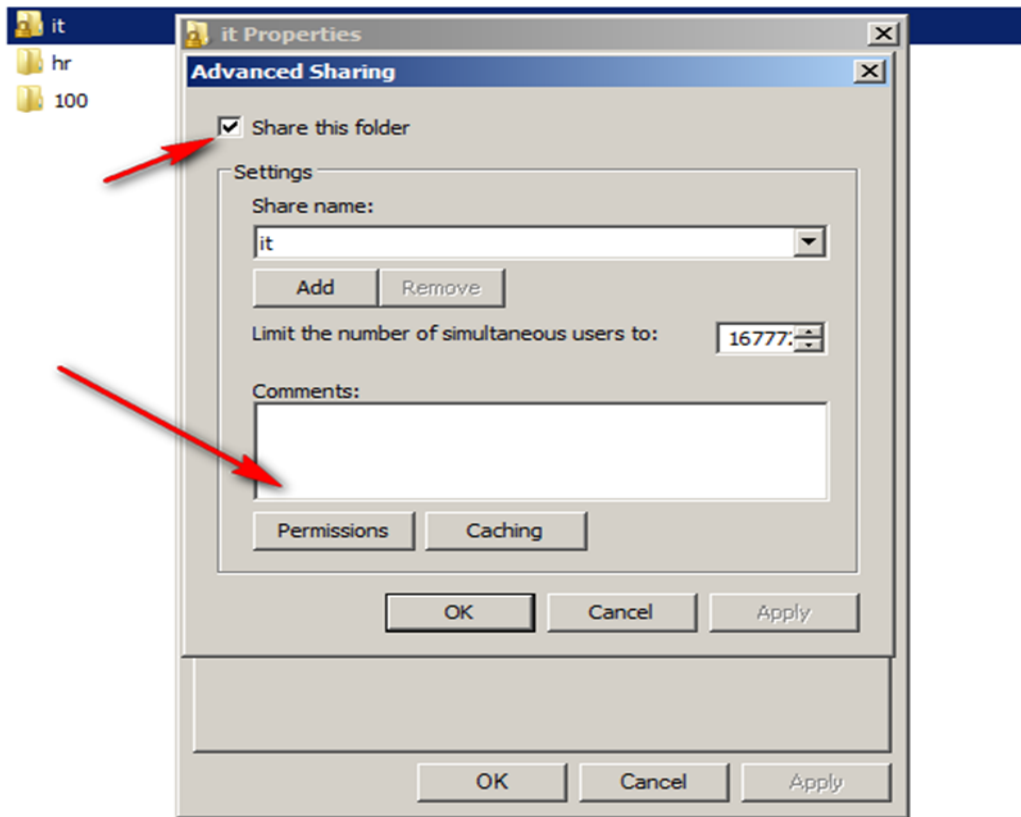
23.1- Security and Sharing windows server 2008

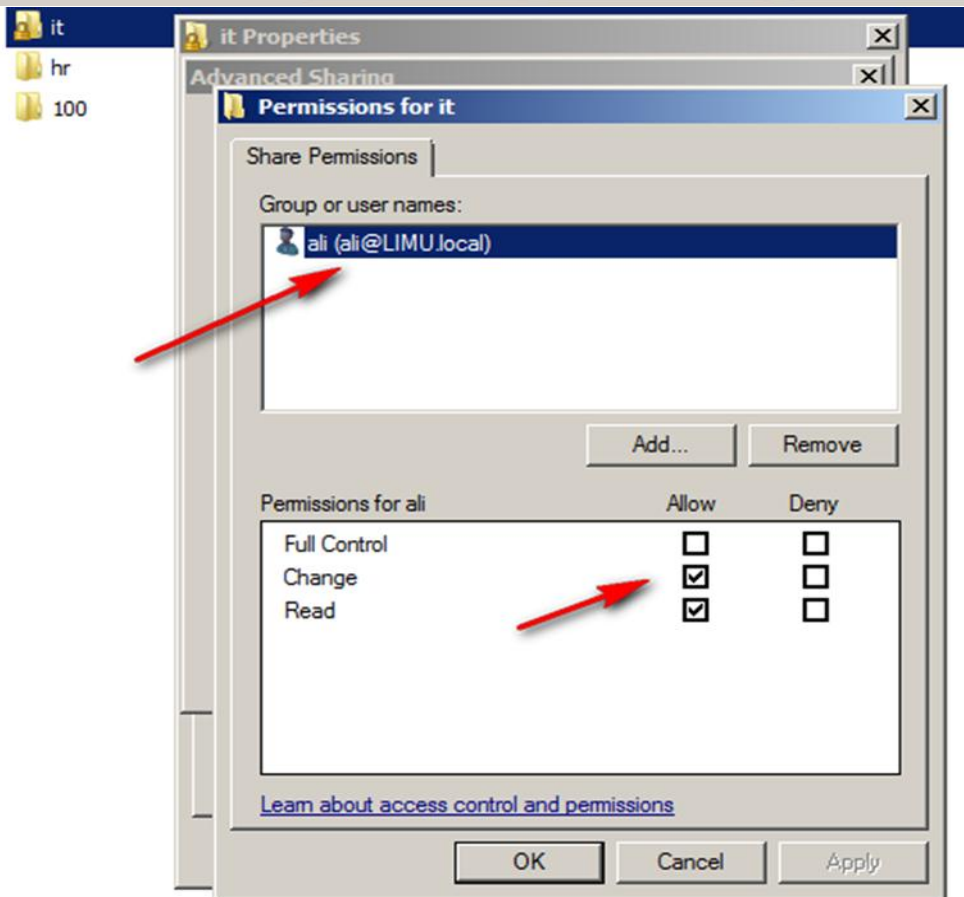
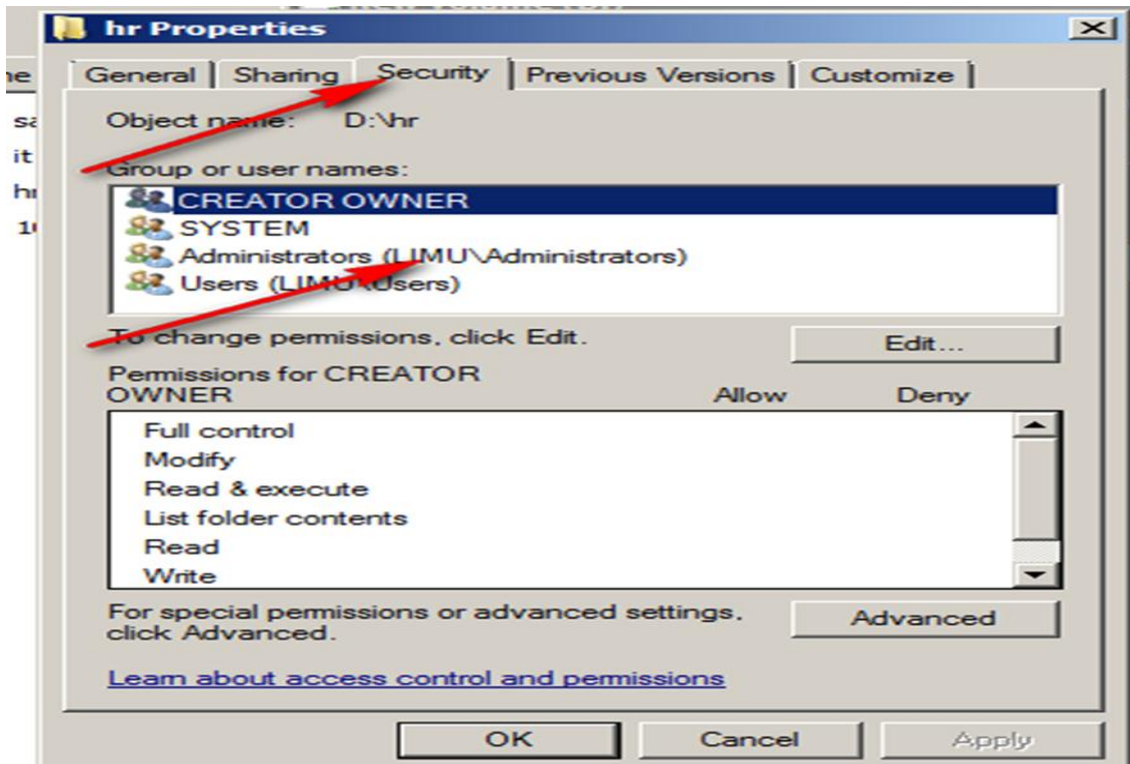
عملية Security وهي عبارة عن طريقة معين لحماية المجلدات من الدخول الغير مصرح بها لحماية هذا المجلد او الملف بحيث يتم تحديد الاشخاص المخول لهم بدخول ايضا الصلاحيات المحدد لكل شخص.

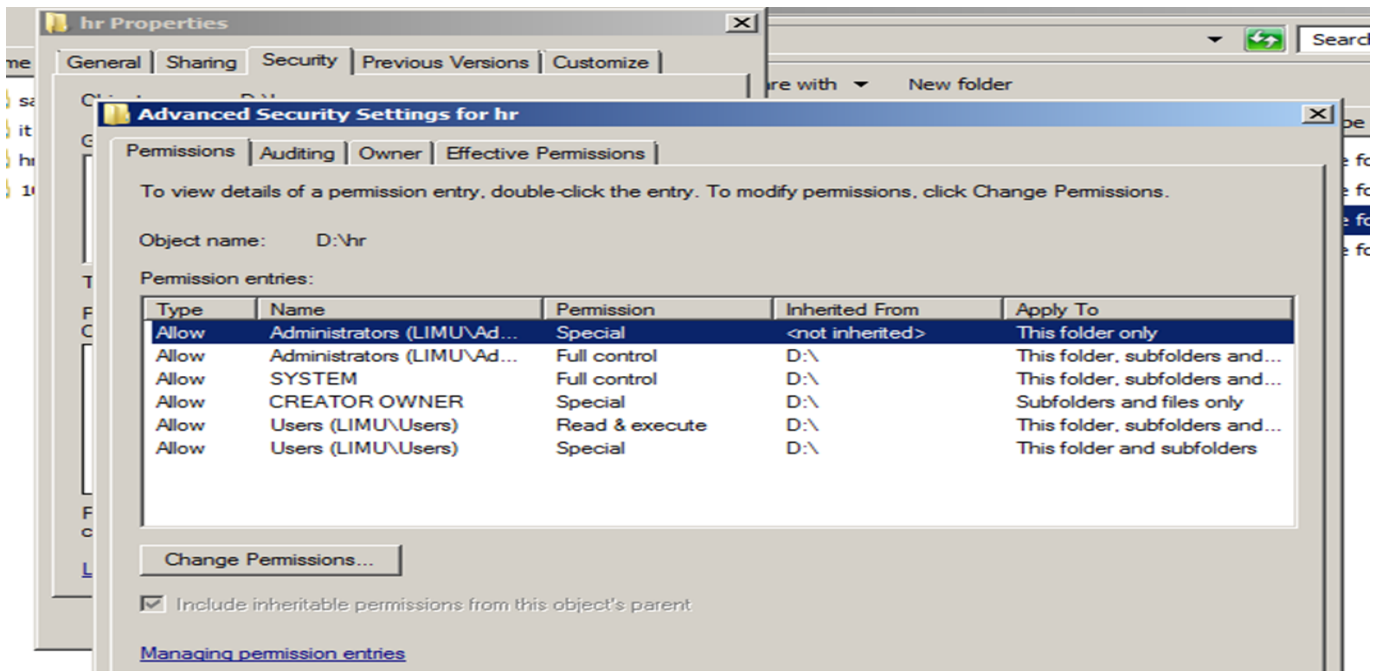
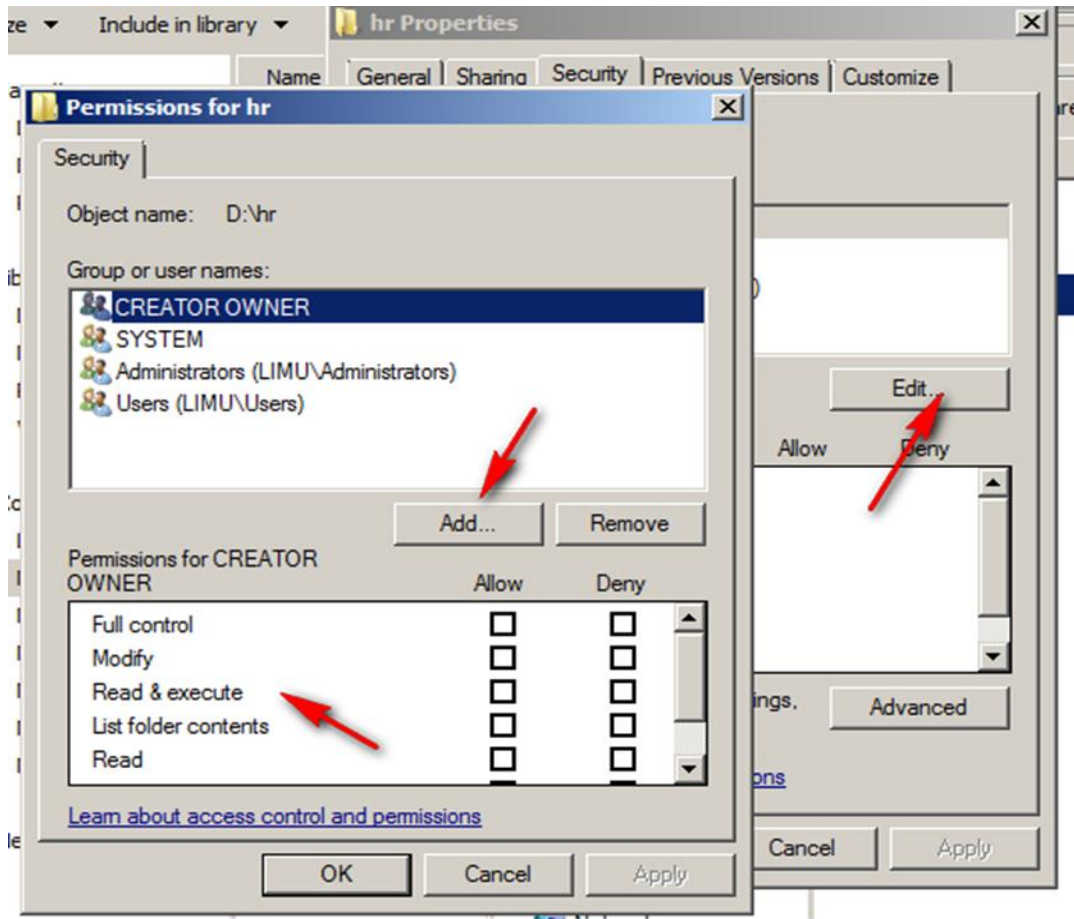
مع ملاحظة ان عملية الامن عادة تطبق عندما يدخل مستخدم عندها صلاحية بعمل login علي السيرفر.

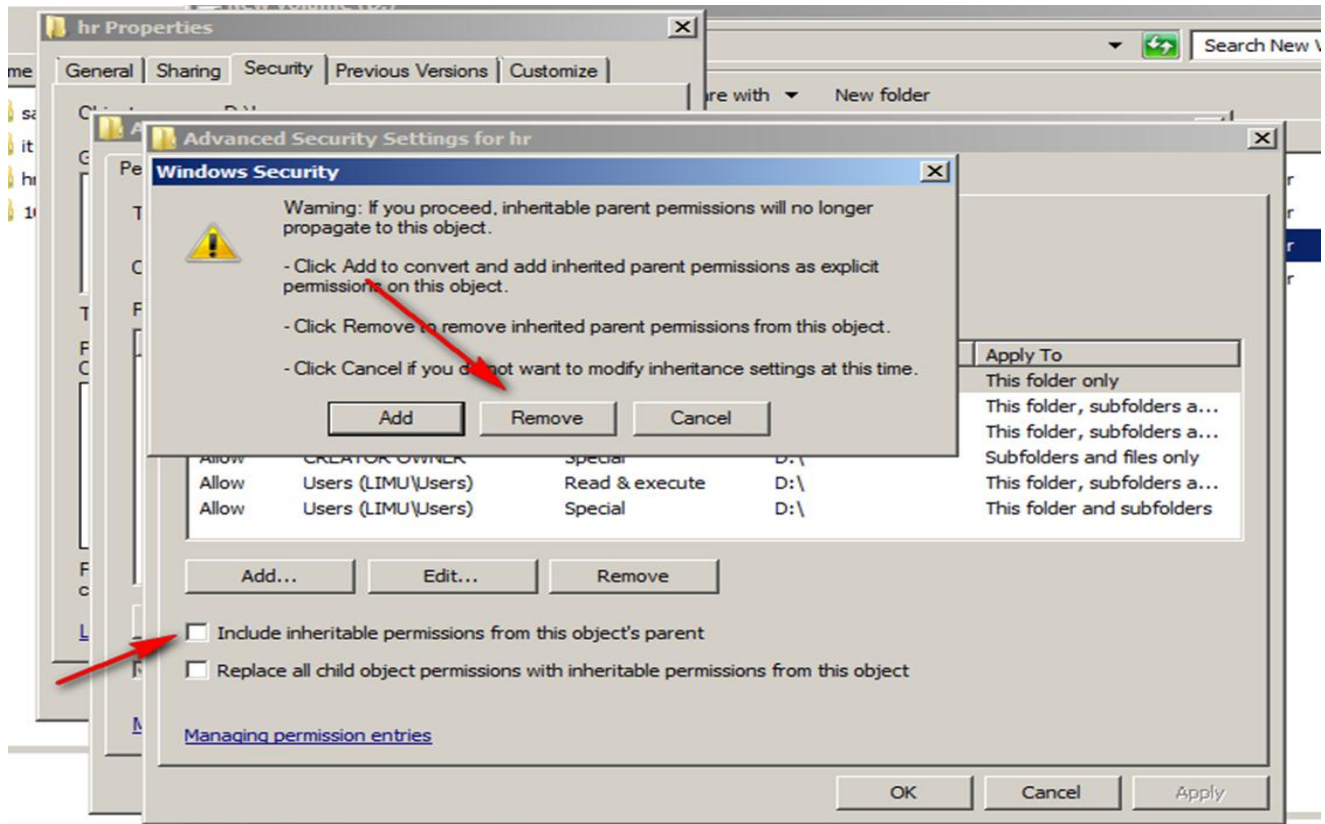
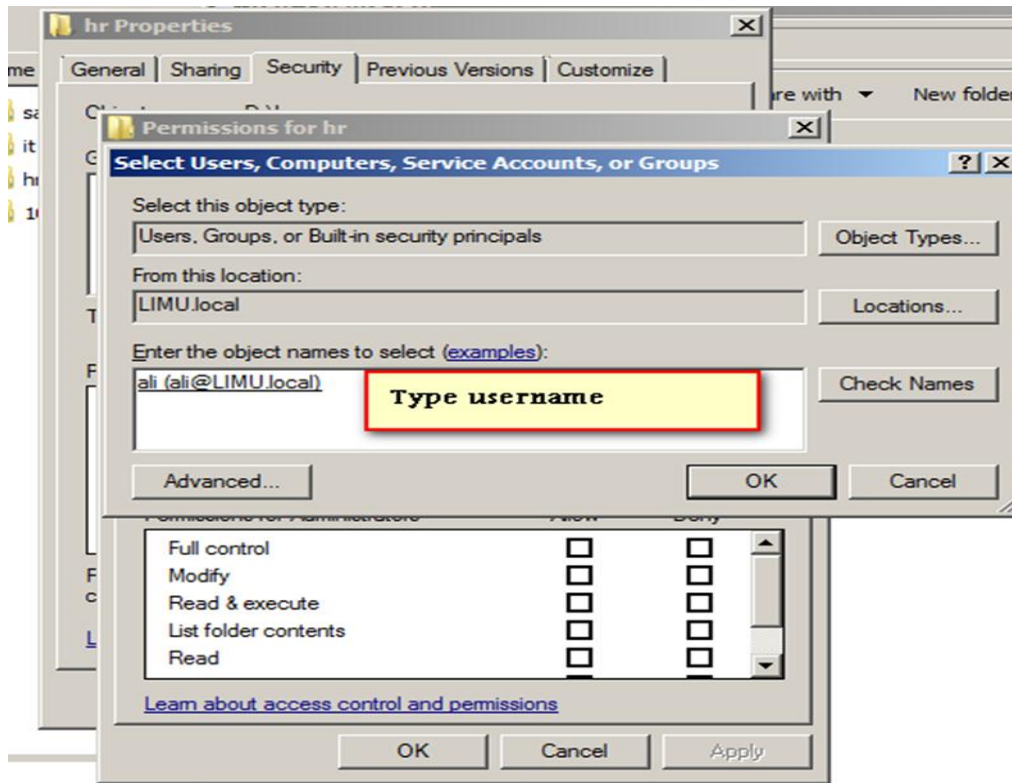
ام عملية Sharing وهي مشاركة هذا المجلد عن طريق الشبكة بحيث يمكن الوصول الي جميع المجلدات الموجودة داخل السيرفر عن طريق الاجهزة الاخرى داخل الشبكة كلا وفقا للصلاحيات المعطاة له عن طريق مدير الشبكة.

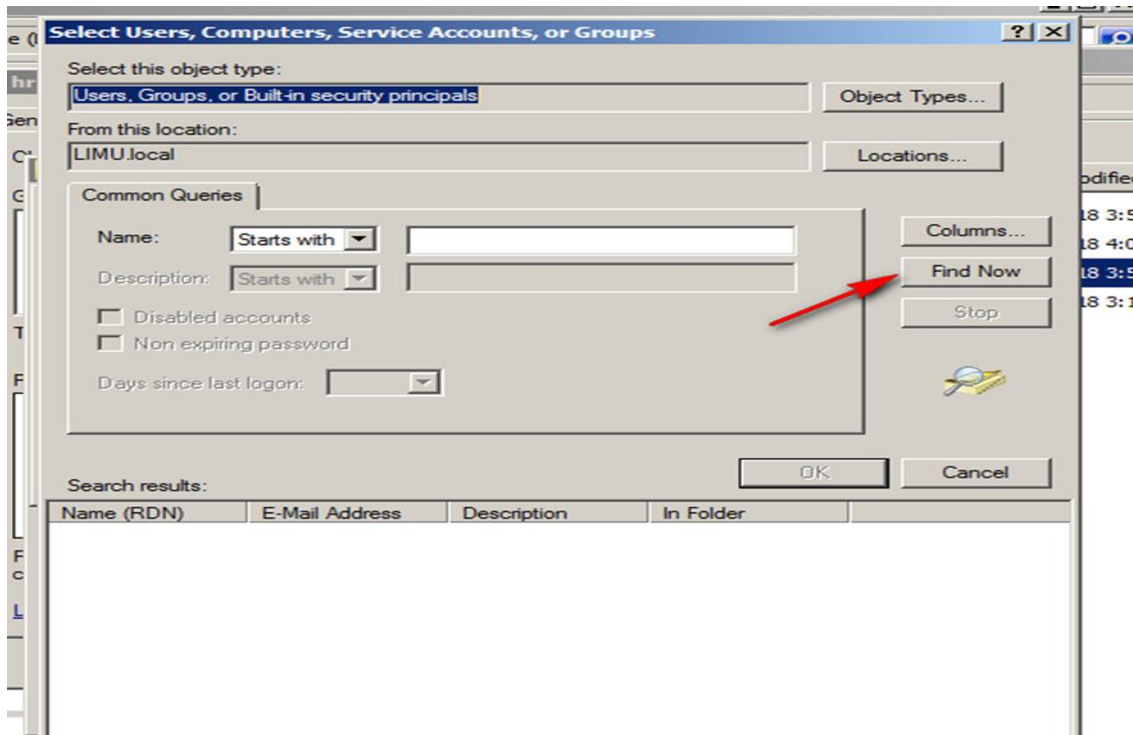
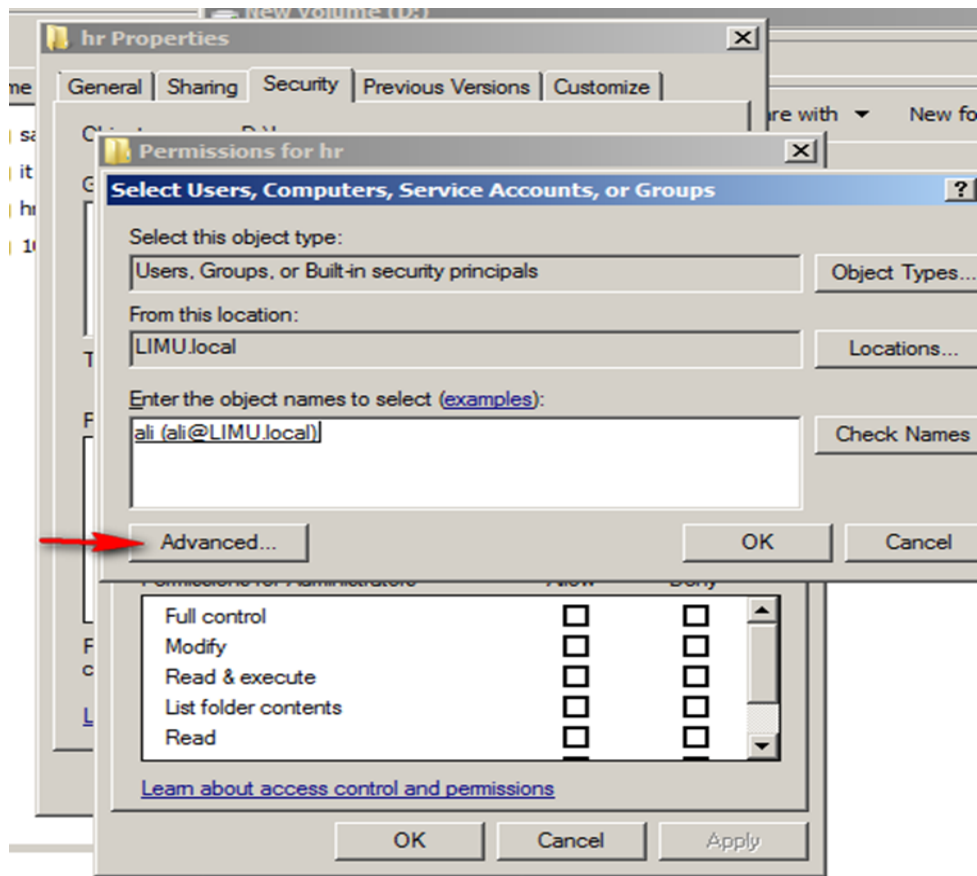


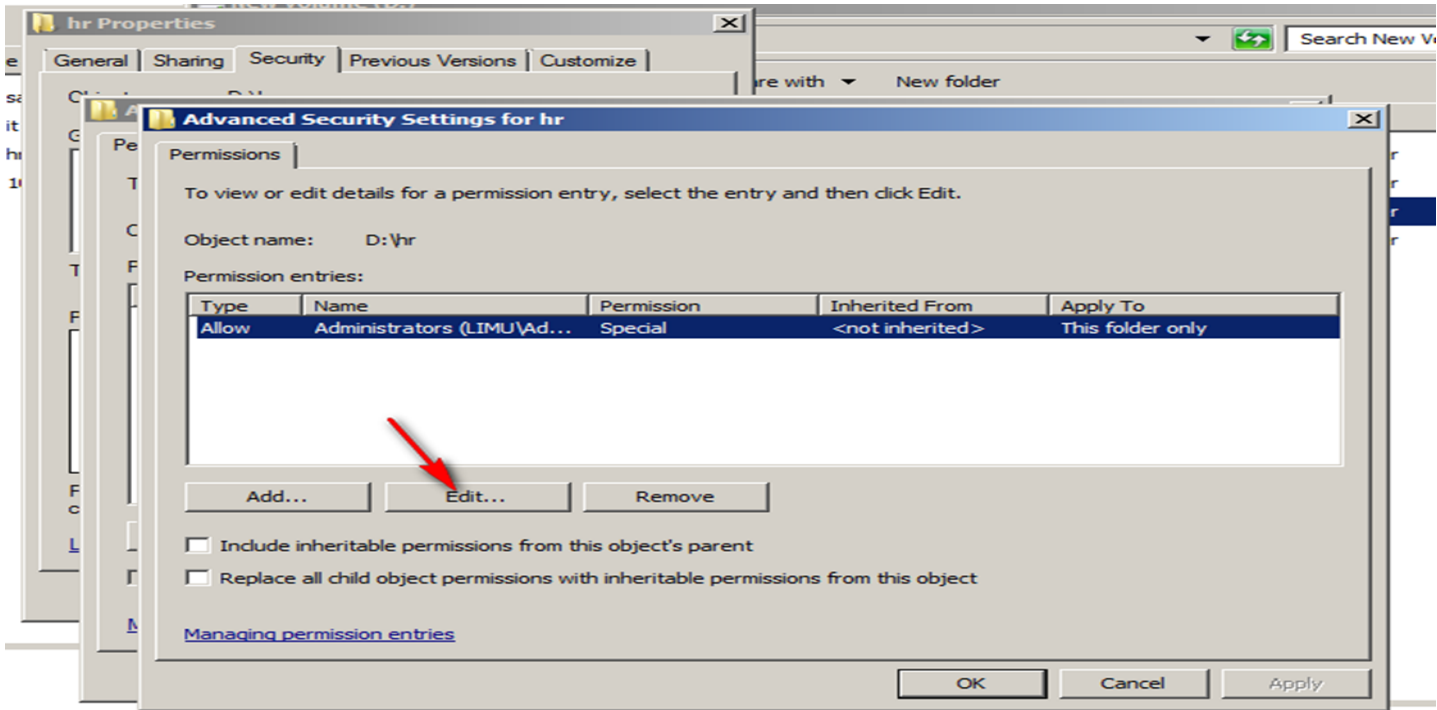
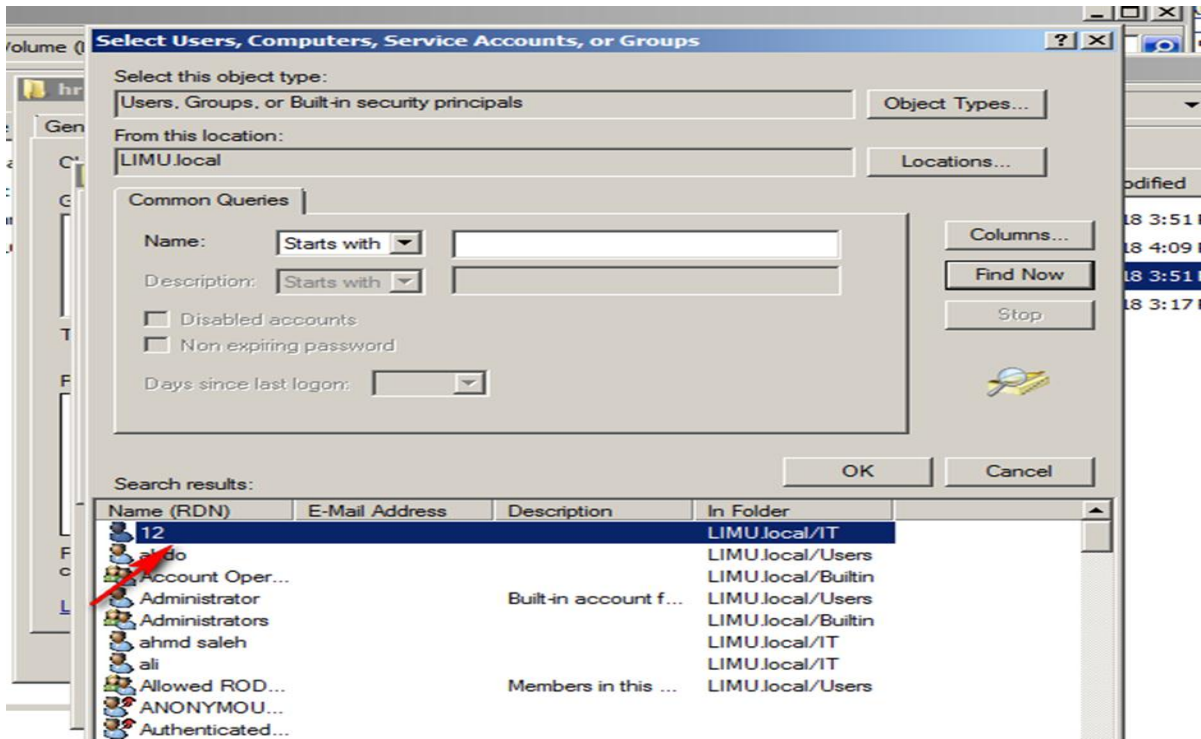


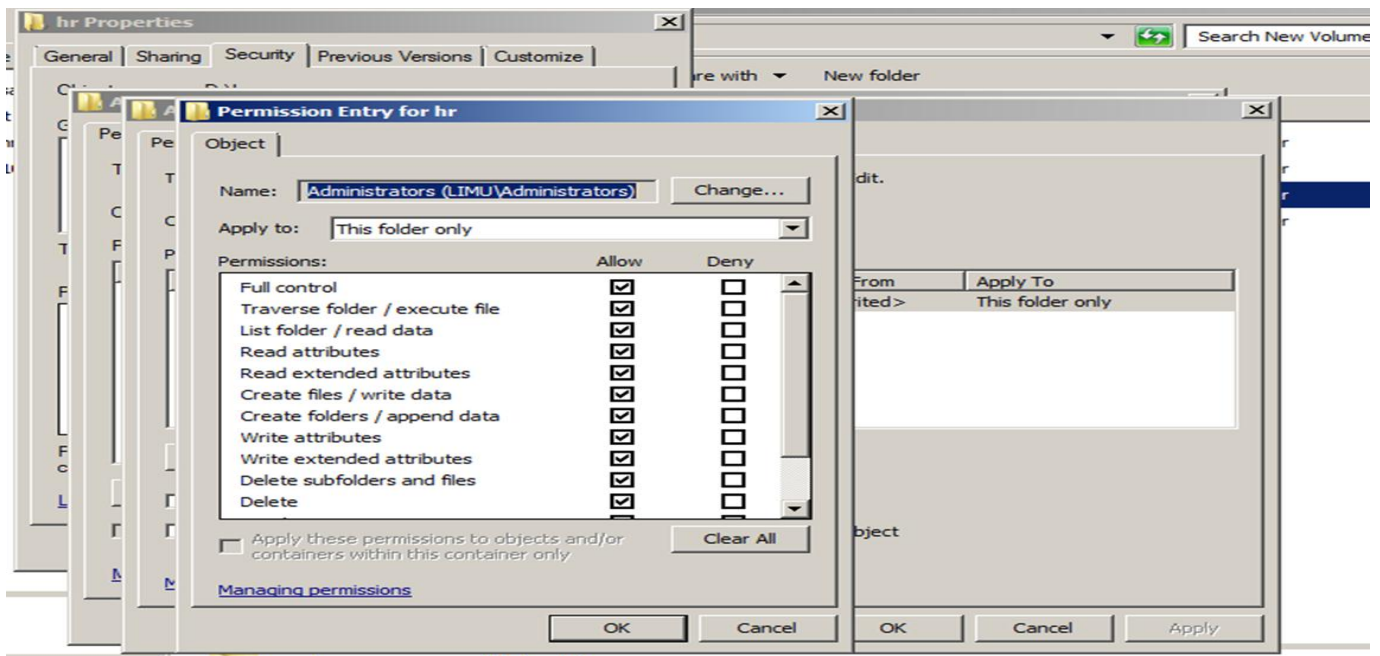










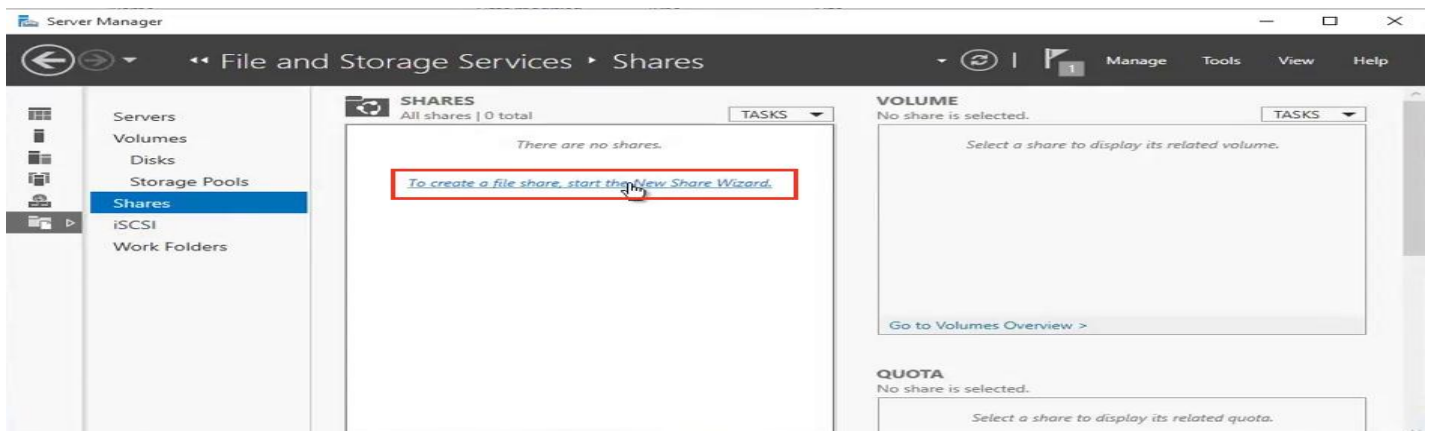


23.2- security and sharing in windows server 2016

Share Files and Folders in Windows Server

Before start sharing files make sure that the advanced sharing settings is configured correctly from control panel with firewall settings then select the folder you want to share. Here we will share files with File and Storage Services, it's already available in windows server by default.

Go to Server manager click File and Storage Services then click shares>tasks>New share to create a folder share on server.



New Share

Select a share profile for the folder you want to share then click Next.

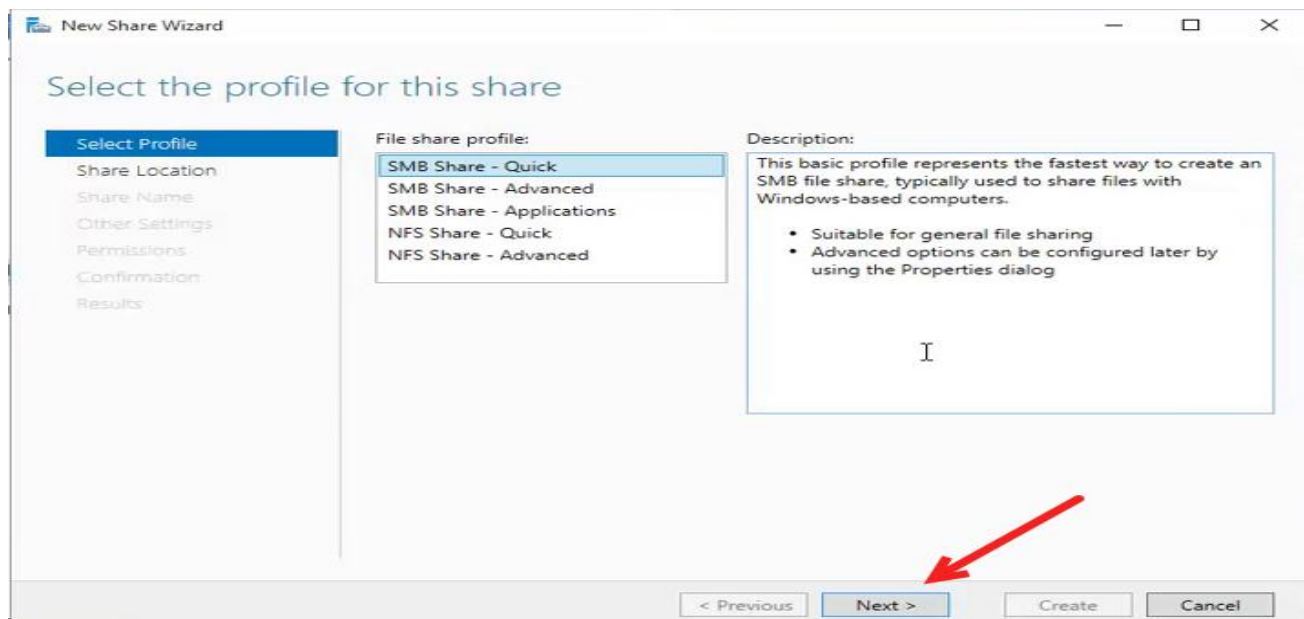
SMB Share Quick: (SMB) is the standard file sharing used by all versions of Windows. SMB Share Quick provides basic SMB sharing with full share and NTFS permission.

SMB Share Advanced: Provides SMB sharing with full share and NTFS permission and access to services provided by File Server Resource Manager.

SMB Share Application: Provides SMB sharing with settings suitable for Hyper-V and other applications.

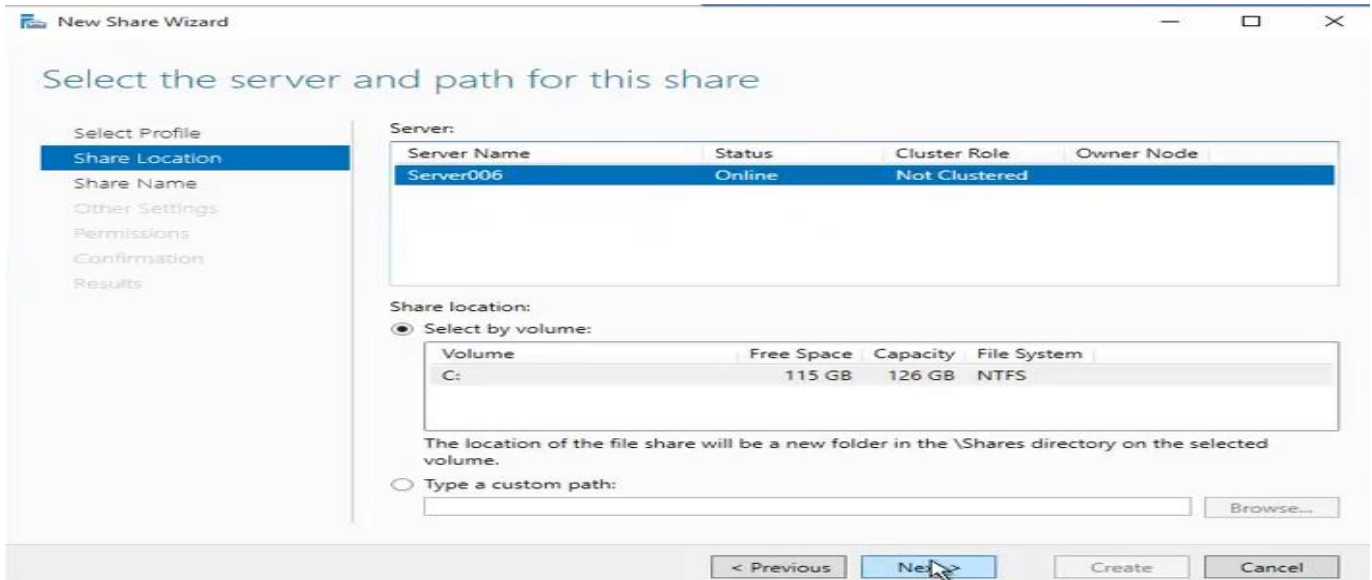
NFS Share Quick: (NFS) is the standard file sharing protocol used by most UNIX, Linux. NFS Share Quick provides NFS sharing with authentication permission and access to services provided by File Resource Manager.

NFS Share Advanced: Provides NFS Sharing with authentication and permission and access to services provided by File Resource Manager.



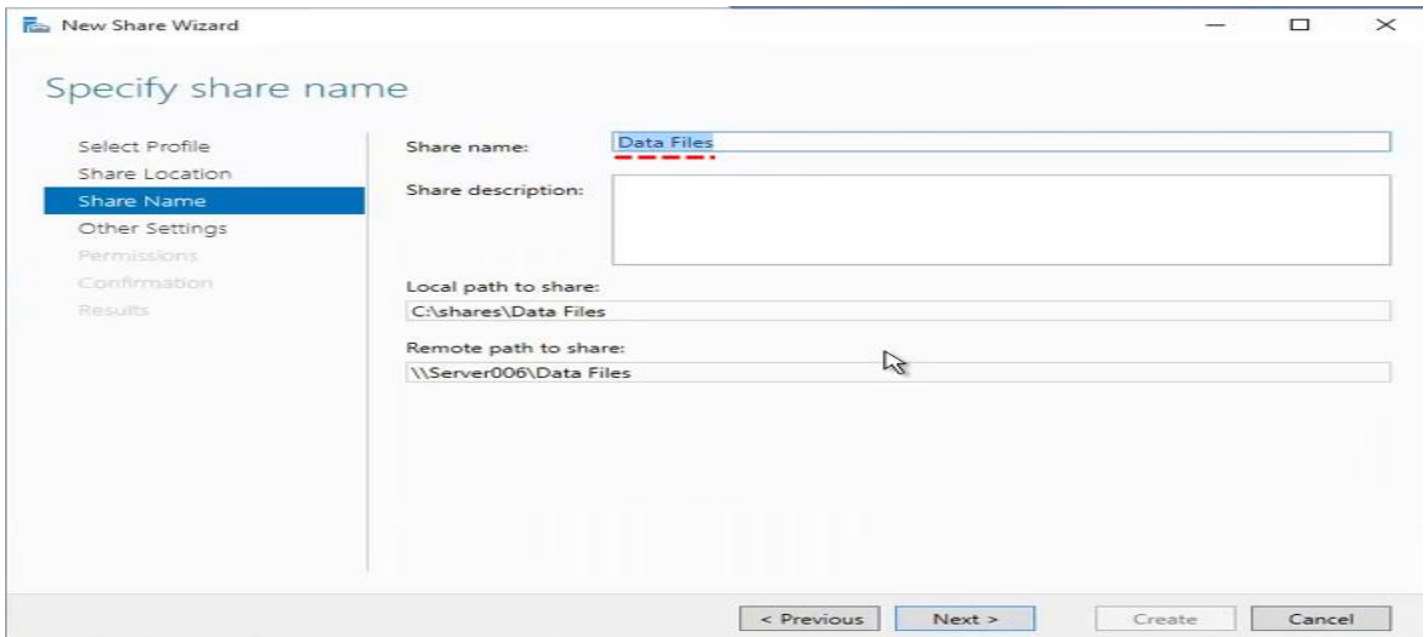
Share Profile

Now select the server and select a volume on the server or specify the folder path you want to share. To share a custom path, choose Type a custom path and browse the folder then click Next.



Share path

On the specify share name page, type a share name and click Next.



Share Name

Here you have to select the sharing options you need, if you don't know the definition read then mark them if required.

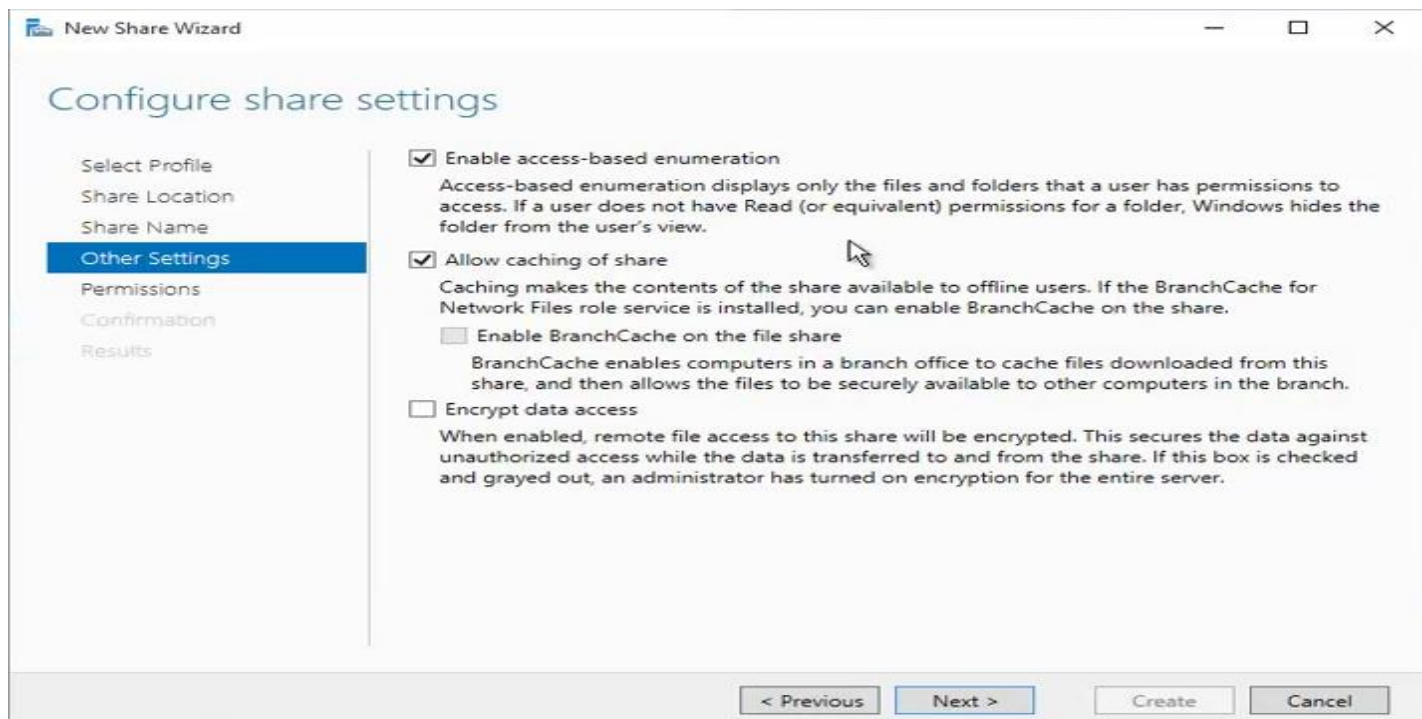
Select any or all of the following options:

Enable Access-Based Enumeration: Prevents users from seeing files and folders they do not have permission to access.

Allow Caching Of Share: Enables offline users to access the contents of this share.

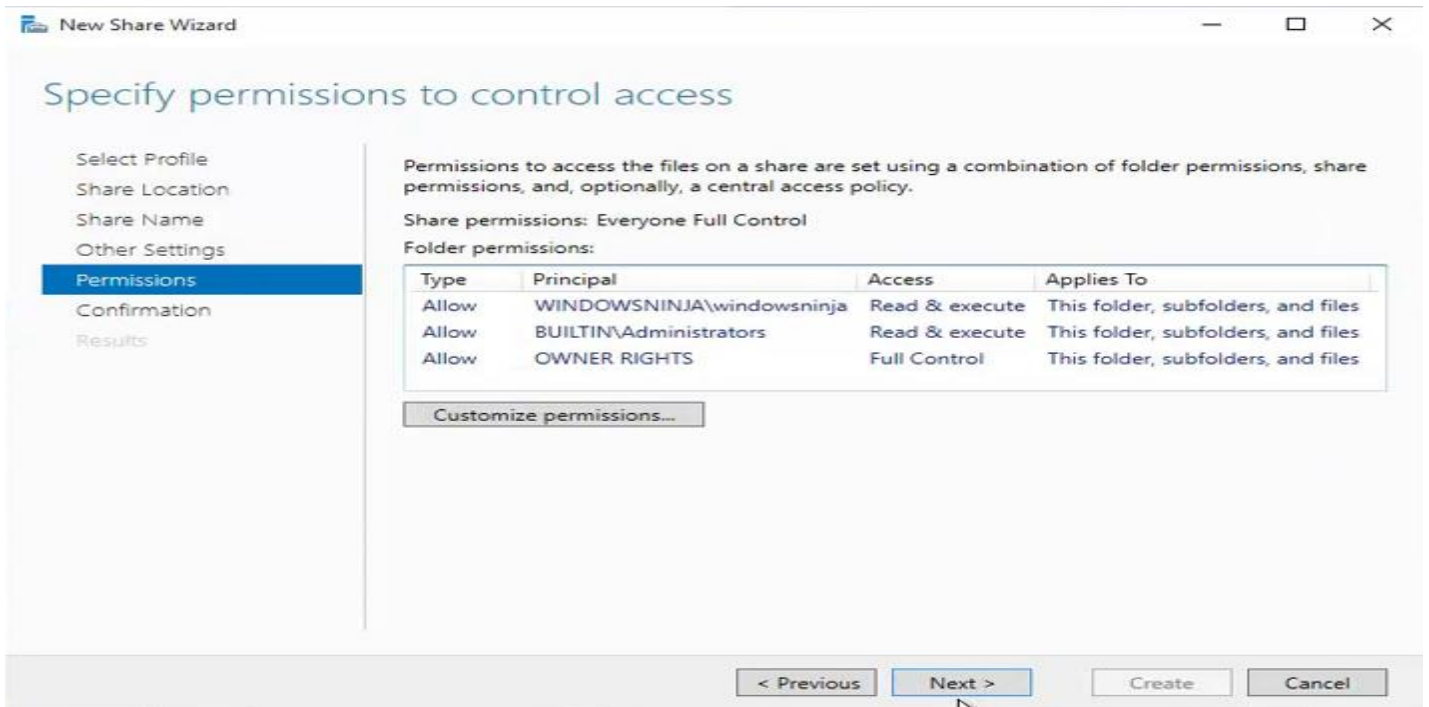
Enable BranchCache On The File Share: Enables BranchCache servers to cache files accessed from this share.

Encrypt Data Access: Causes the server to encrypt remote file access to this share.



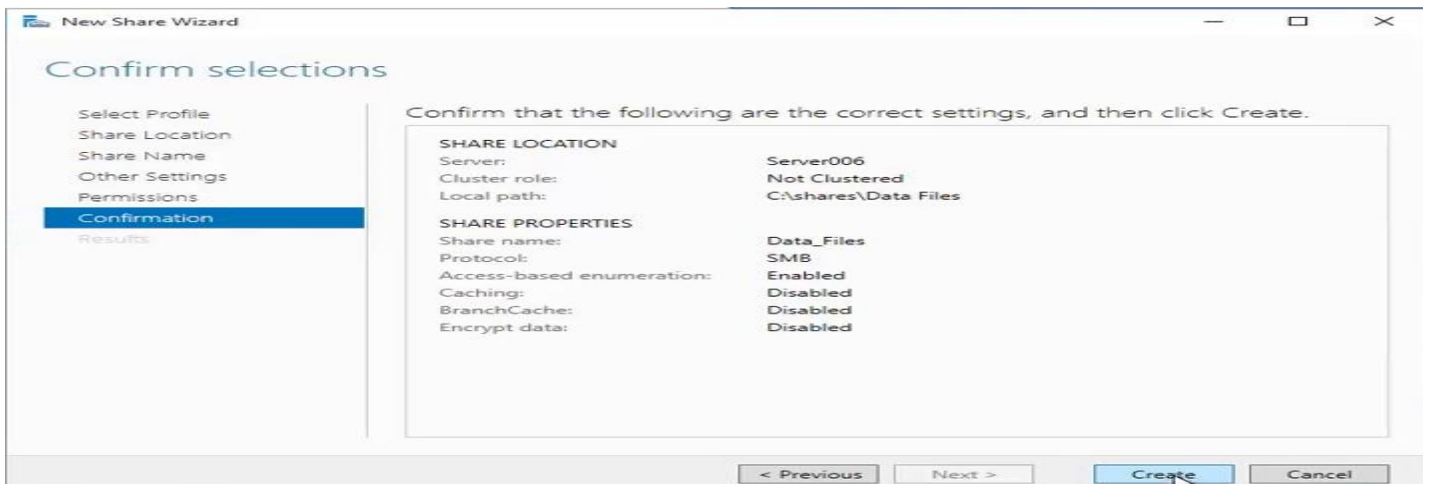
Configure Share Settings

Now Specify the permissions to control access read or write by clicking on Customize permissions then add, remove or change users permission and click Next.



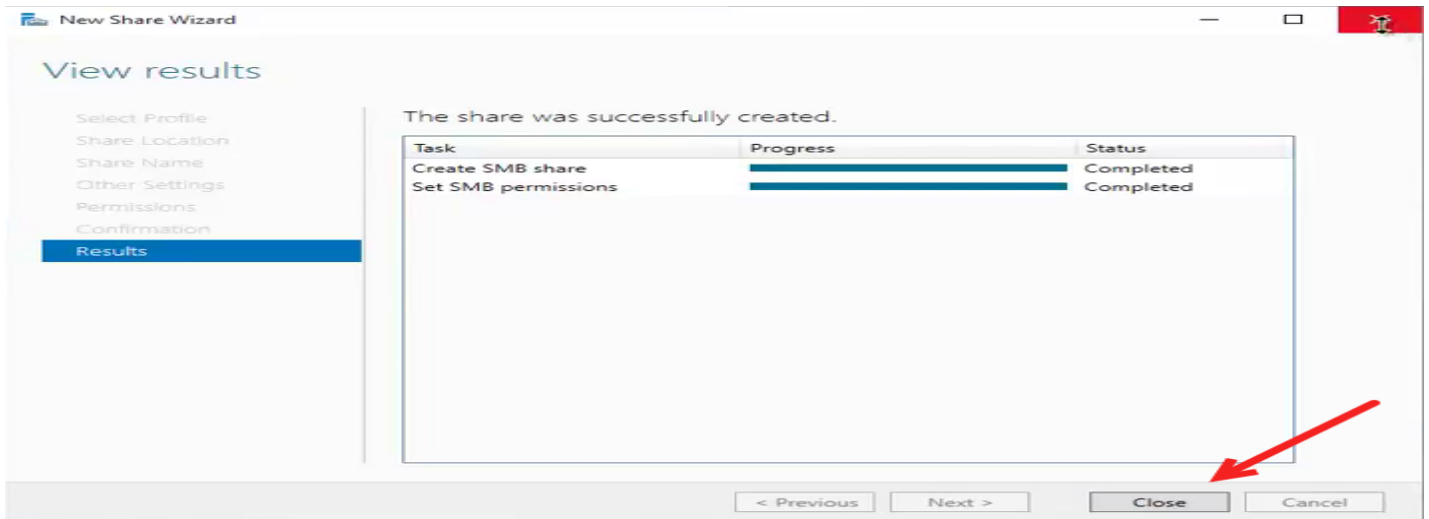
Permissions

Confirm that the shared settings are configured properly and click Create.



Confirmation

The share was created successfully with its appropriate permissions, click close.



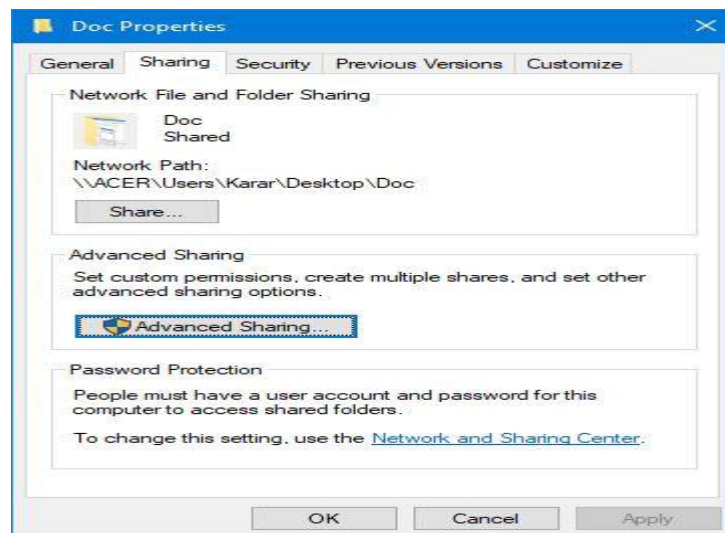
Shared

To check the folder shared go to Network>your computer then your shared files will be there.

Also you can see them by typing \\yourcomputername\ in the file explorer.

Configure file Shares using file Explorer

Navigate to the folder then right click and select Properties, click on sharing tab then click Advanced sharing.

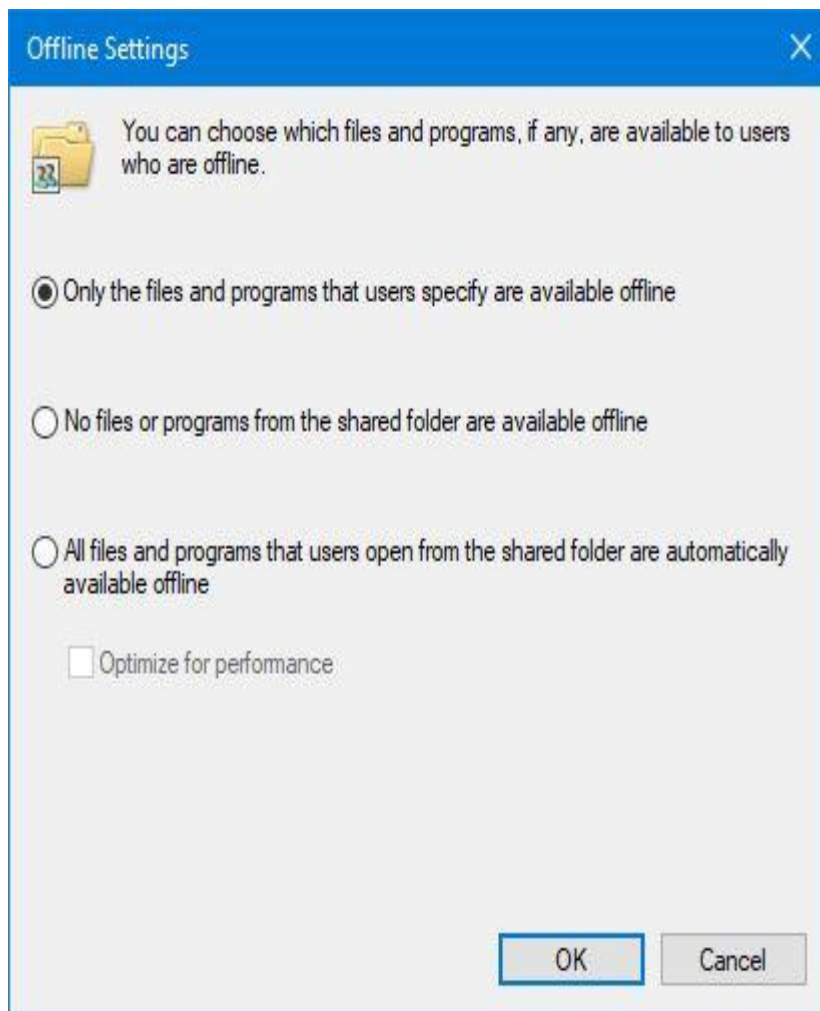


Sharing

Mark on Share this folder and enter a share name then click on permissions to add, remove or change permissions of users and click ok.

When the folder sharing is configured properly, click Apply then ok. Your folder will be shared successfully.

Also, you can manage caching of the folder by clicking on caching and select the one you want. (Caching enables offline files for the users those who have enabled offline files. You can choose if the folder should be available offline or not.



Offline Settings

All right, this was all about configured file shares in windows server 2016, hope it would be helpful and informative.

24-Install Remote Server Administration Tools (RSAT)

RSAT وهي اداء تسمح بتحميل جميع الخدمات الرئيسة الموجود داخل السيرفر مثل

windows) client ويندوز على Active directory users and computers, server manager, DNS,DHCP
(seven,8,10).

Remote Server Administration Tools (RSAT) enables IT administrators to remotely manage roles and features in Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008, and Windows Server 2008 R2 from a computer that is running Windows 10, Windows 8.1, Windows 8, Windows 7, or Windows Vista.

You cannot install RSAT on computers that are running Home or Standard editions of Windows. You can install RSAT only on Professional or Enterprise editions of the Windows client operating system

RSAT allows administrators to run snap-ins and tools on a remote computer to manage features, roles and role services. The software includes tools for cluster-aware updating, Group Policy management and Hyper-V management, as well as the Best Practices Analyzer.



RSAT runs on Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2 and Windows Server 2012.

How to Install Remote Server Administration Tools (RSAT) on Windows 7

After downloading either the 64-bit or 32-bit version, based upon your needs, you will then install it on any Windows 7 system that will be used to remotely manage your servers.

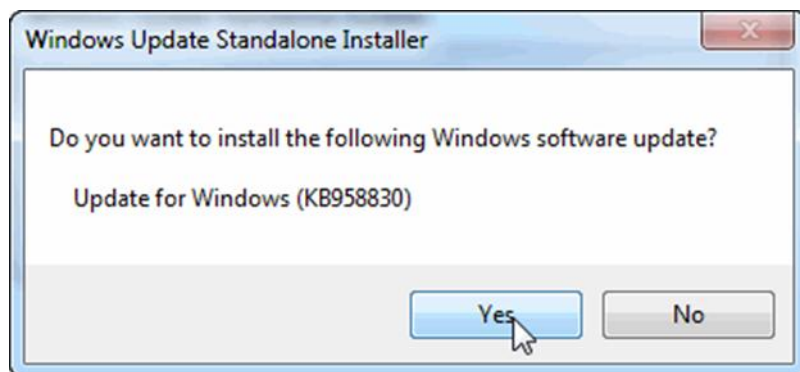
Note: In order to use RDP to manage your servers you do not need to install anything! The RSAT package will allow you to connect to the servers on your network as though you were using one of the tools on one of your servers, and allow you to perform all the management tasks on your network

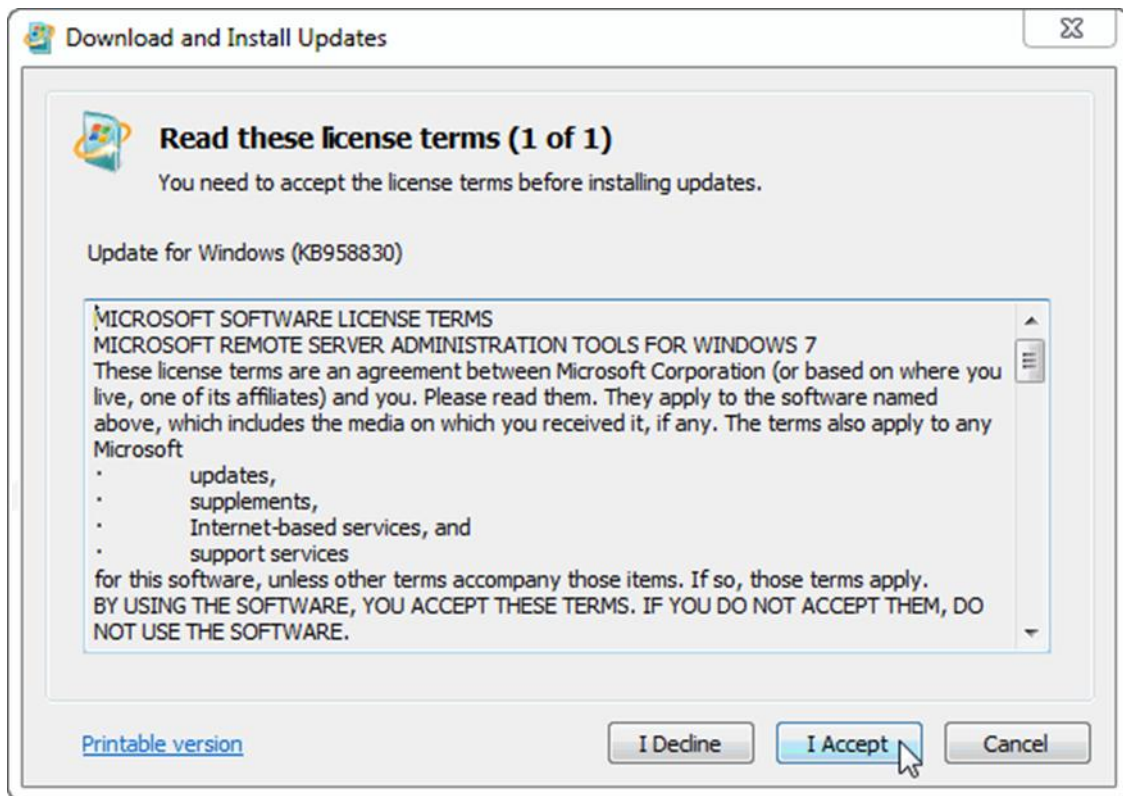
you must be either a member of the Administrators group on the computer on which you want to install the Administration Tools pack, or you must be logged on to the computer by using the built-in Administrator account.

Remote Server Administration Tools Installation Instructions;

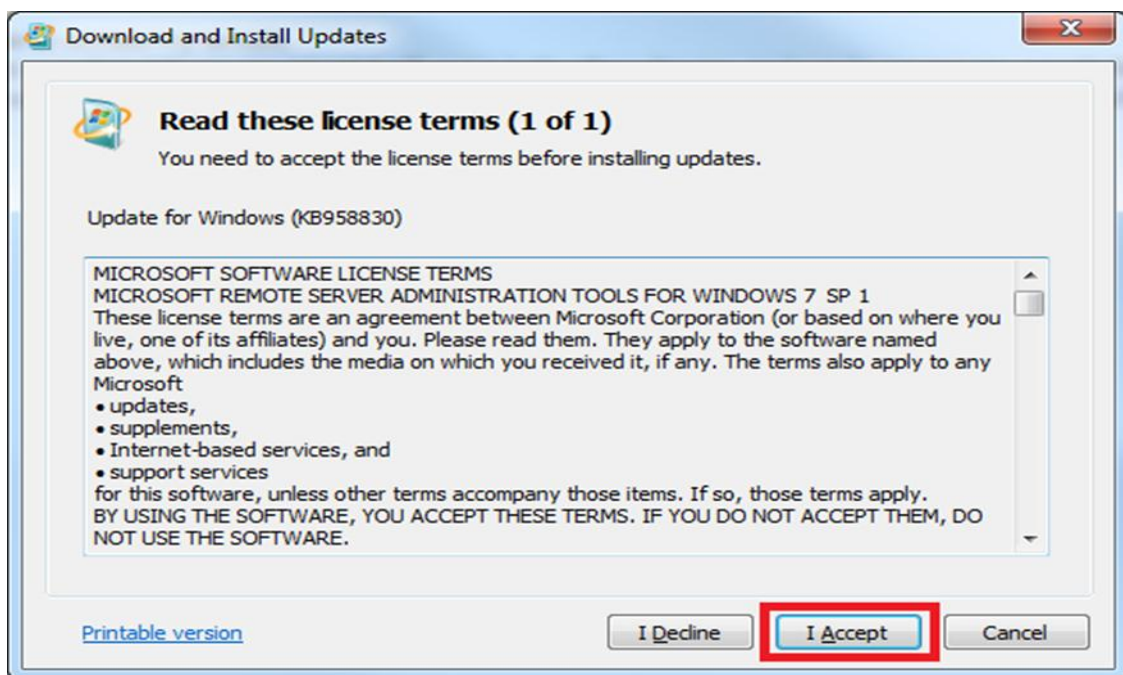
This article shows you how to download and install an important update in Windows 7. NOTE: All versions of Administration Tools Pack or Remote Server Administration Tools for Windows Vista with SP1 need to be removed from the computer before downloading this version. (Including copies in different languages)

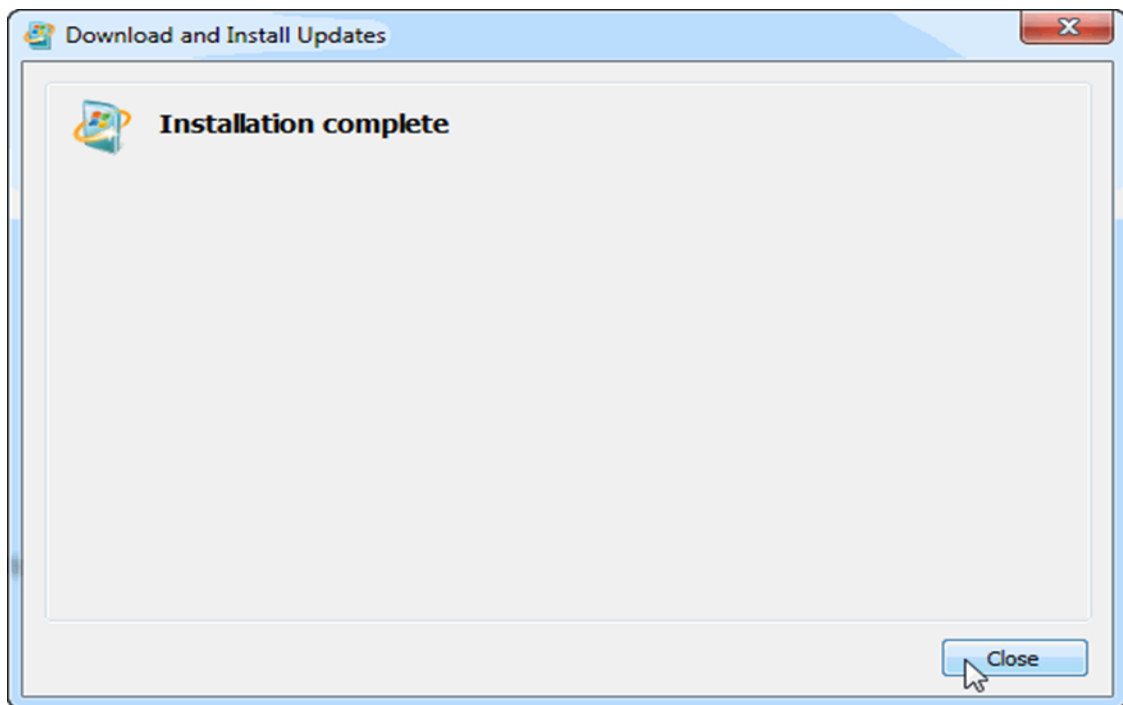
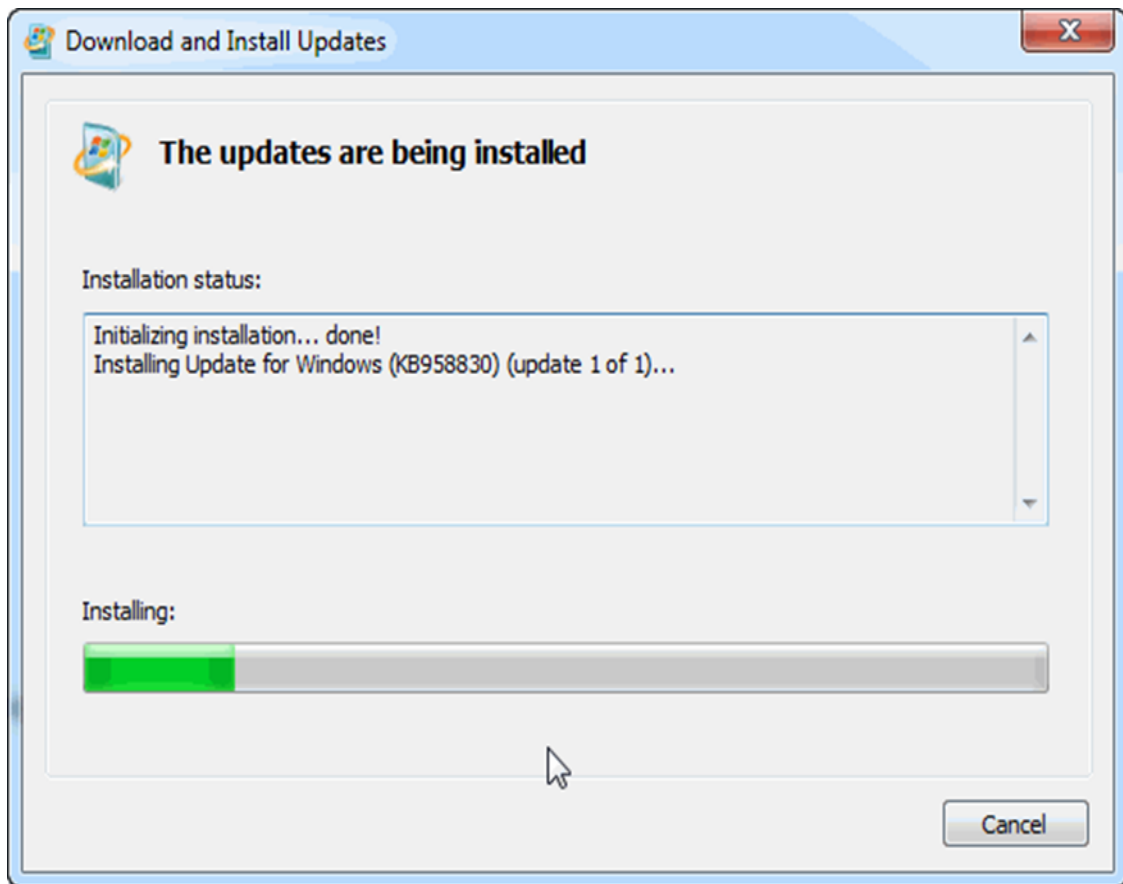
Double-click the downloaded file after choice the type version 64bit or 32bit to start the Remote Server Administration Tools for Windows 7 Setup Wizard. Follow all the steps through the installation (basically it's "Next" all the way to the "Finish" button...)



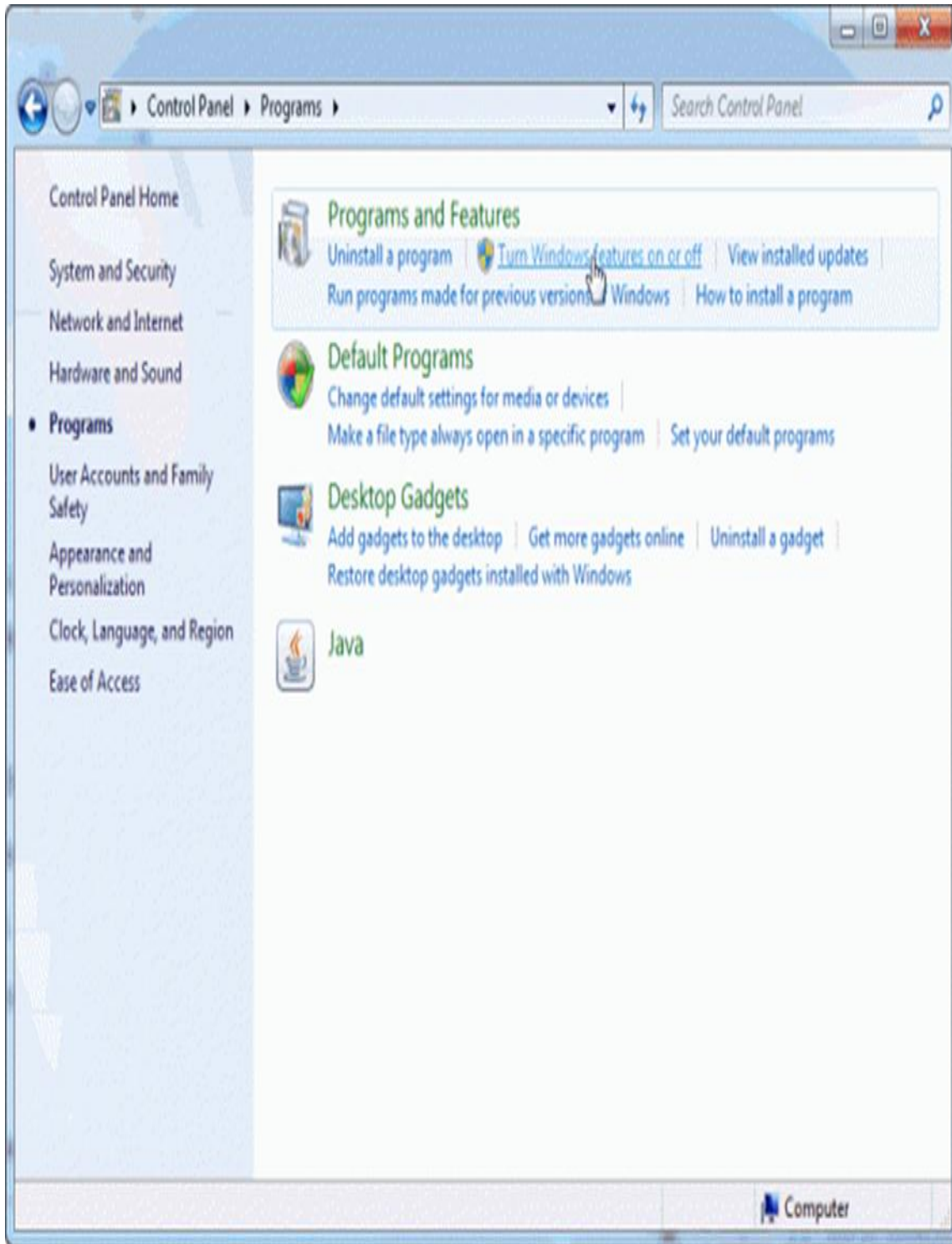


When you run the update package you will see this message, which explains that you are able to install an update – click ‘Yes’

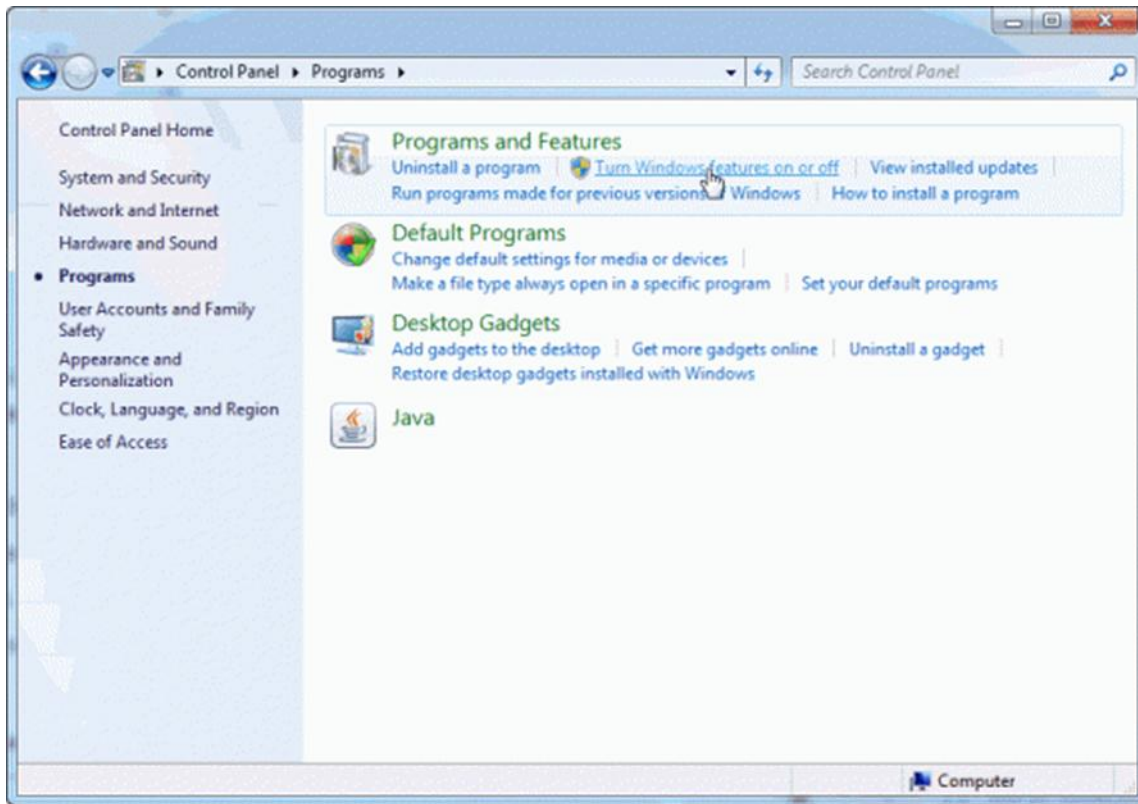




Next, click Start, click Control Panel, and then click Programs. In the Programs and Features area, click Turn Windows features on or off.



Next, click Start, click Control Panel, and then click Programs. In the Programs and Features area, click Turn Windows features on or off.



If you are prompted by User Account Control to enable the Windows Features dialog box to open, click Continue.

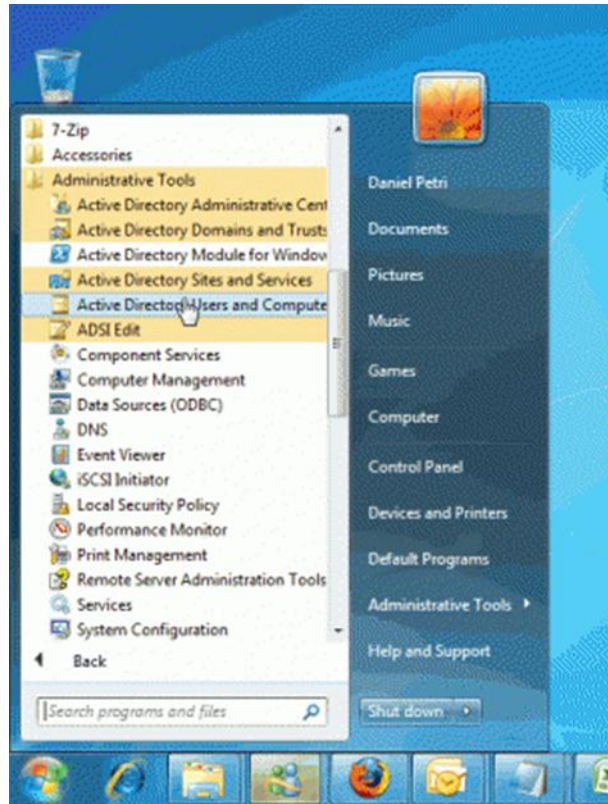
In the Windows Features dialog box, expand Remote Server Administration Tools. Select the remote management tools that you want to install. Click OK.

If the Start menu does not display the Administration Tools shortcut you will need to configure it:

Right-click Start, and then click Properties.

On the Start Menu tab, click Customize.

In the Customize Start Menu dialog box, scroll down to System Administrative Tools, and then select Display on the All Programs menu and the Start menu. Click OK. Shortcuts for snap-ins installed by Remote Server Administration Tools for Windows 7 are added to the Administrative Tools list on the Start menu.



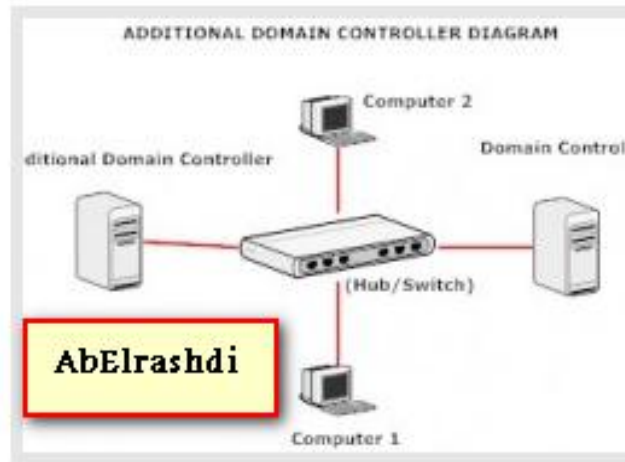
25-Additional Domain Controller

لماذا نحن نحتاج الي "نطاق اضافي" او Additional domain, الاجابة عن هذا السؤال بسيطة جدا اولاً لخدمات الوفرة او ال Services Redundancy او لتحسين المصادقة للنطاق في موقع بعيد او بالانجليزي for domain authentication improvement in remote site, حالة فشل ال server او توقفه عن العمل يكون لدينا واحدا اخر الذي يستطيع ان يقوم بجميع الخدمات والوظائف الخادم الاول

اولاً انت تحتاج الي تستطيع ال sever عليك بتفعيل خصائص كارت الشبكة لكي تبدأ عملية الترقية. كما ان ال domain controller server يتطلب static IP من نفس ال subnet او ال subnet routable او القابلة للتوجيه داخل الشبكة كما ان خدمات الدليل او ال Directory Services تعتمد علي DNS Servr وانت تحتاج الي الاشارة بشكل صحيح اين يتم تشغيل الخدمة. في مثالنا هذا ال additional server يستخدم DNS IP address 192.168.1.1 كما يوجد بالصورة في الاسفل:

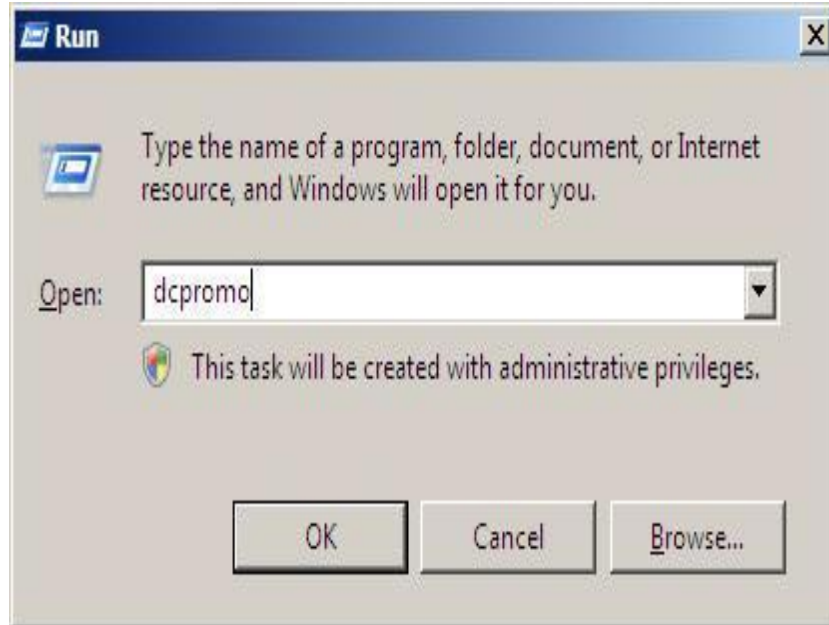
Why do we need to add additional Domain Controller? This answer is very simple: “for services redundancy” or “for domain authentication improvement in remote Site”.

- In case of server failure, we still have another one which can provide necessary services in our network, which avoids business discontinuity.

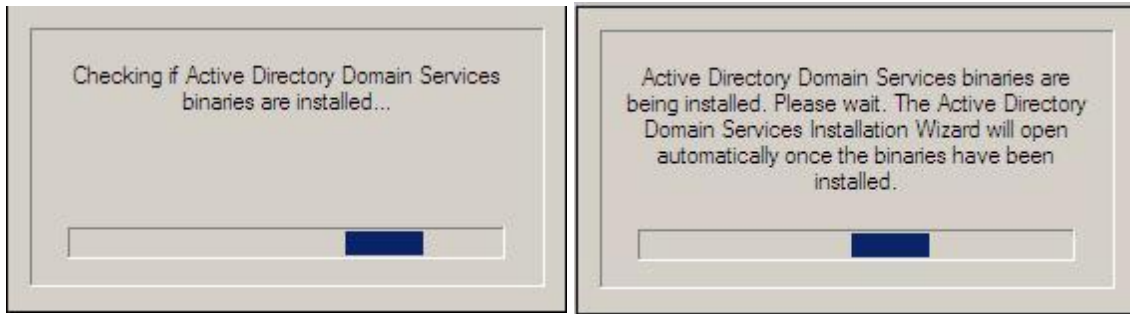


25.1- Install Additional Domain Controller windows server 2008

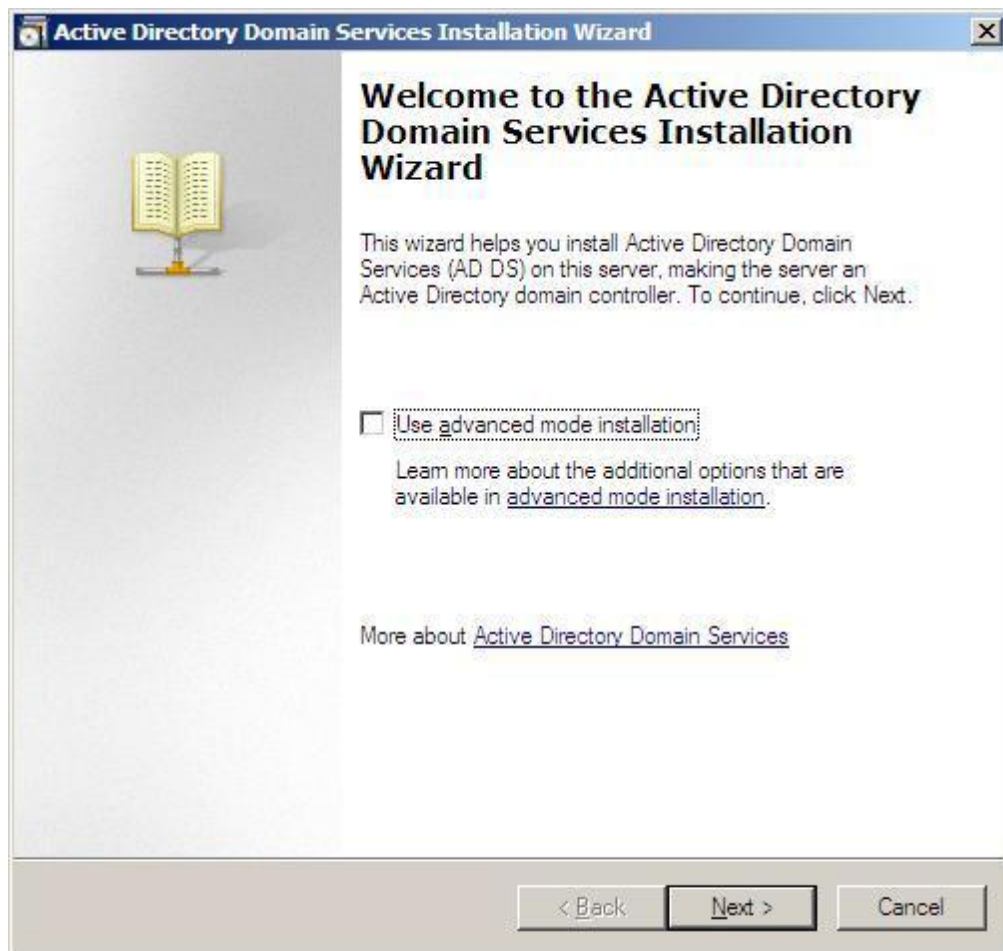
To set up an Additional Domain Controller, I will use the dcpromo.exe command. To use the command, click on Start > Run > and then write dcpromo > Click OK



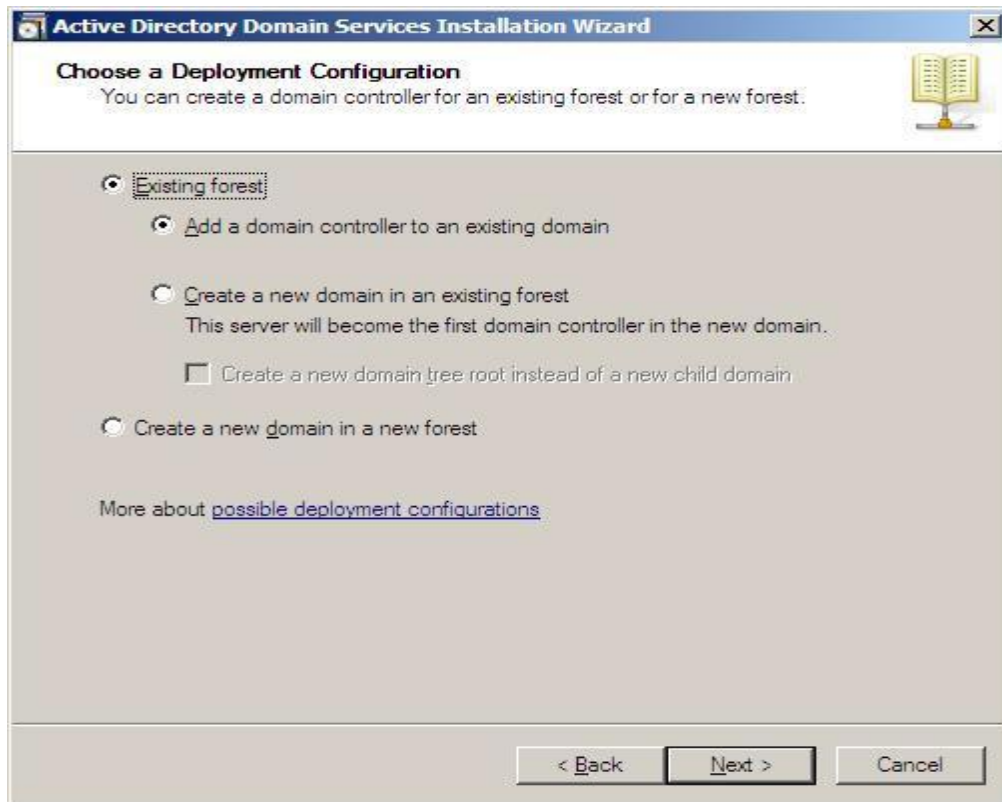
The system will start checking if Active Directory Domain Services (AD DS) binaries are installed, then will start installing them. The binaries could be installed if you had run the dcpromo command previously and then canceled the operation after the binaries were installed.



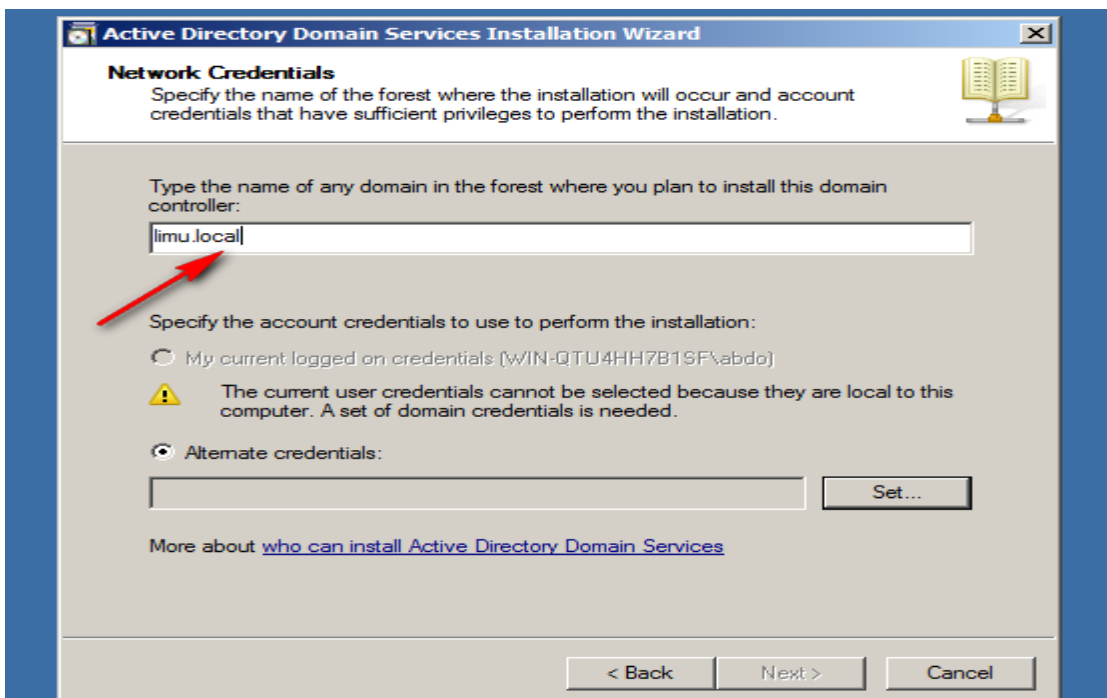
The Active Directory Domain Services Installation Wizard will start, either enable the checkbox beside Use Advanced mode installation and Click Next , or keep it unselected and click on Next



On the Choose a Deployment Configuration page, click Existing forest, click Add a domain controller to an existing domain, and then click Next.



On the Network Credentials page, type your domain name, my domain name is elmajdal.net (was set in the previous article) , so I will type LIMU.local



Additional Domain Controller

To set up an Additional Domain Controller, you will need an account that must be either a member of the Enterprise Admins group or the Domain Admins group. We have two options:

My Current logged on credentials (DomainName\Username or MachineName\Username)

Alternate credentials

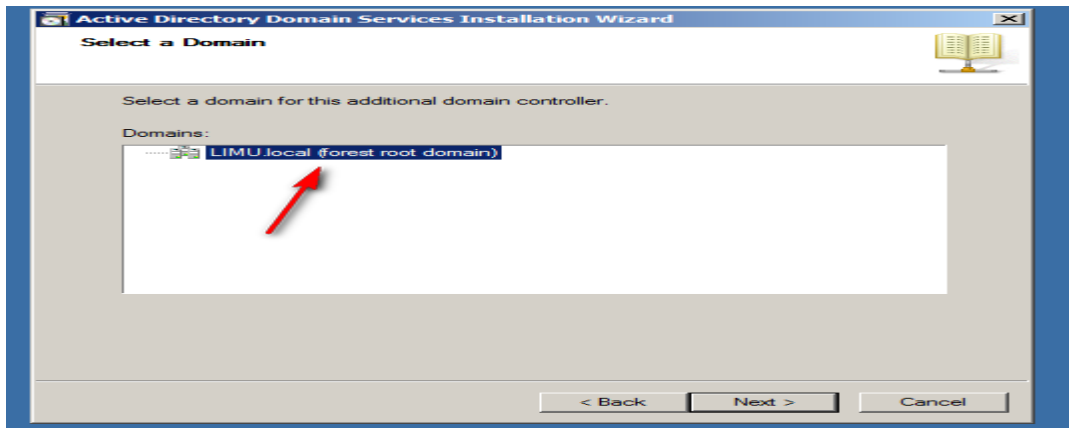
If you have previously joined this server to the domain and you are currently logged in to it with an Enterprise Admin/Domain Admin user, then you can use the first option (My current logged on credentials) . As you can see this option is grayed here, and the reason for this is below it. It is because I'm currently logged in with a local user, the machine is not a domain member. I'm left out with the second option: Alternate credentials

- To enter the Alternate credentials, click Set. In the Windows Security dialog box, enter the user name and password for an account that must be either a member of the Enterprise Admins group or the Domain Admins group > then click Next.

Enter the credentials



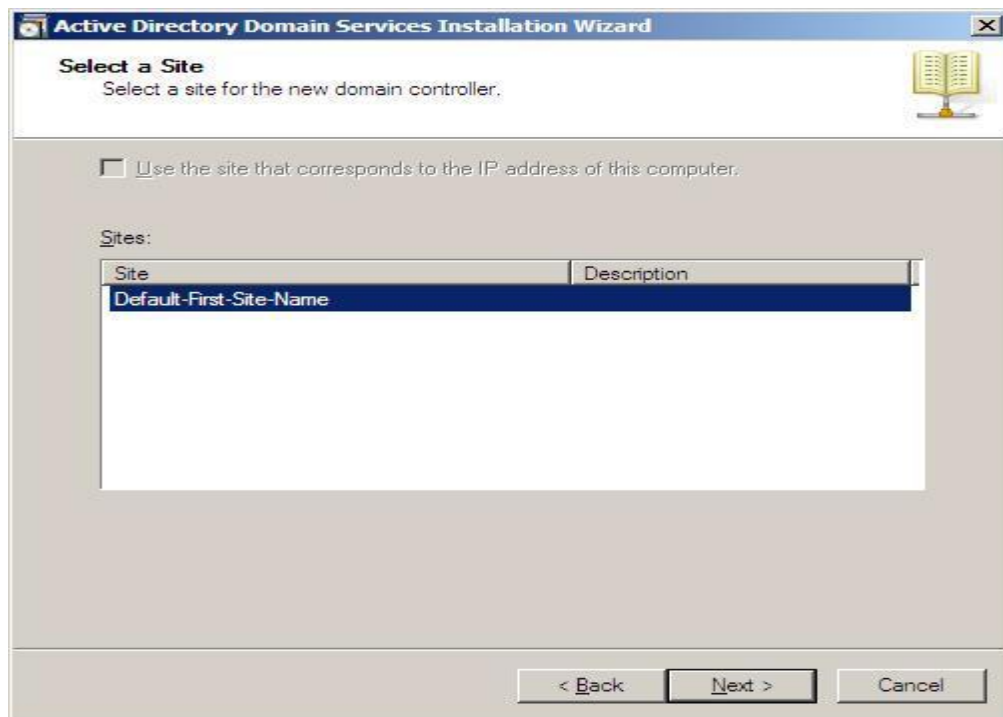
On the Select a Domain page, select the domain of the Additional Domain Controller, and then click Next, as I already have only one domain, then it will be selected by default



Select the site of domain controller

On the Select a Site page, either enable the checkbox beside Use the site that corresponds to the IP address of this computer, this will install the domain controller in the site that corresponds to its IP address, or select a site from the list and then click Next. If you only have one domain controller and one site, then you will have the first option grayed and the site will be selected by default as shown in the following image

Select the site of domain controller



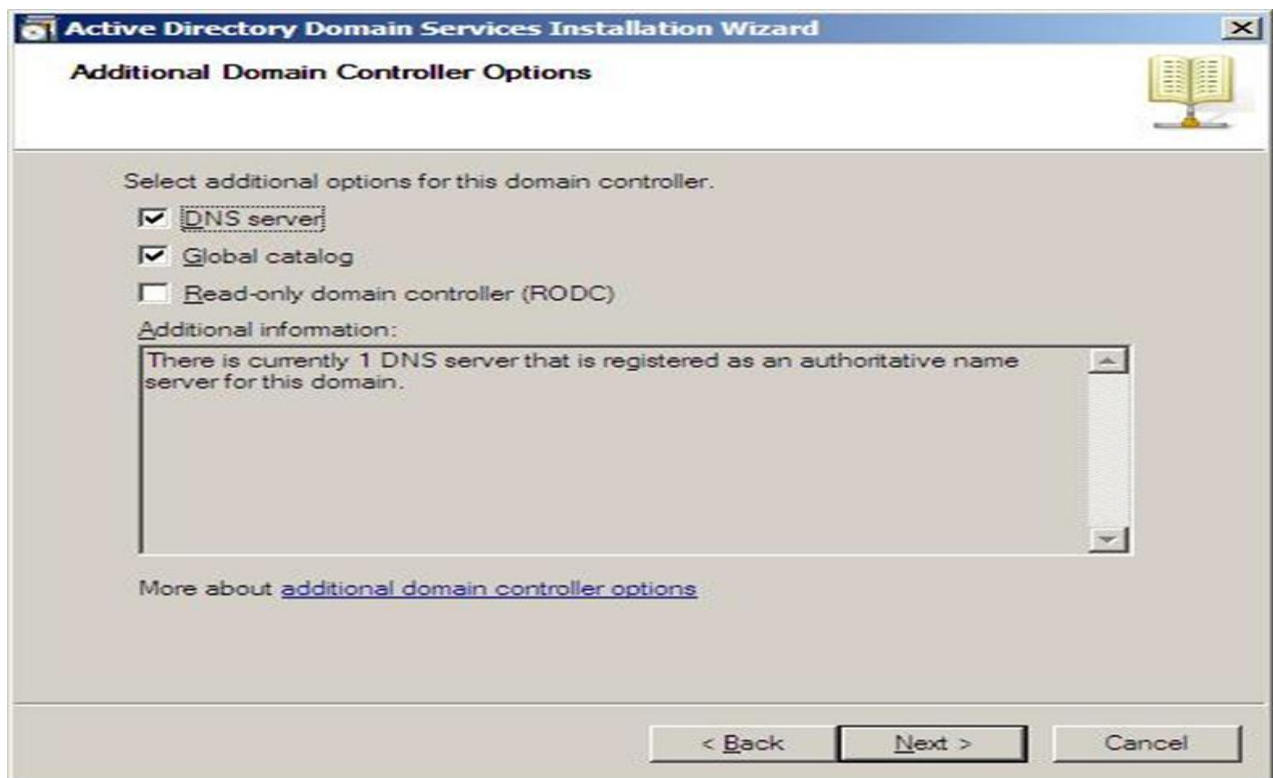
DNS and Global catalog

On the Additional Domain Controller Options page, By default, the DNS Server and Global Catalog checkboxes are selected. You can also select your additional domain controller to be a Read-only Domain Controller (RODC) by selecting the checkbox beside it

DNS and Global catalog

My primary domain controller is a DNS Server is well, and this can be verified by reading the additional information written in the below image, that there is currently 1 DNS server that is registered as an authoritative name server for this domain. I do want my Additional DC to be a DNS server and a Global catalog, so I will keep the checkboxes selected. Click Next

Additional Domain Controller



Select DNS

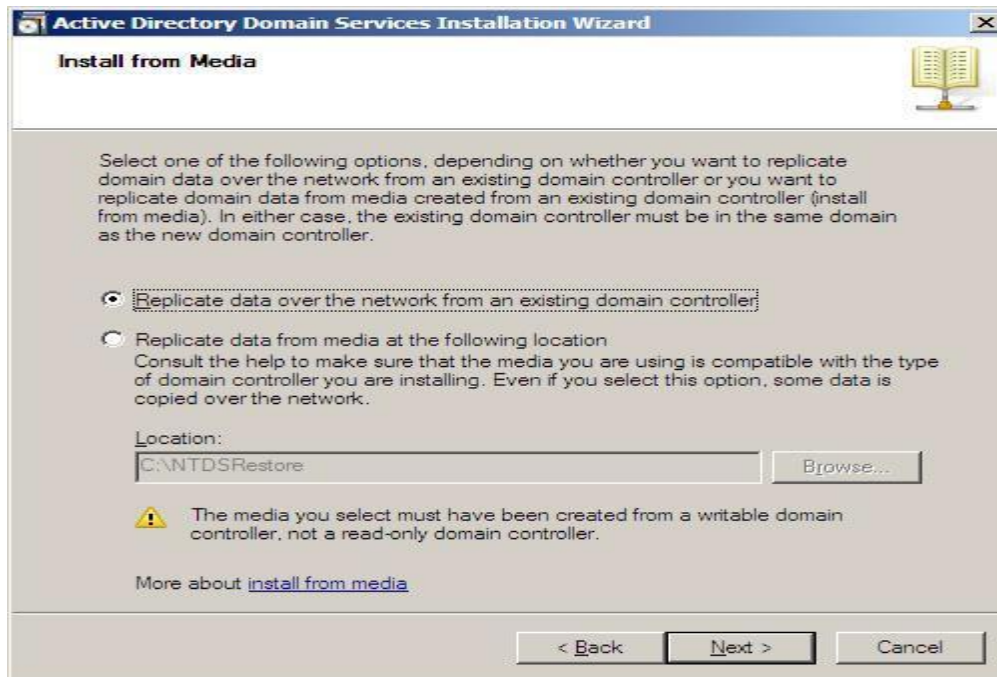
If you select the option to install DNS server in the previous step, then you will receive a message that indicates a DNS delegation for the DNS server could not be created and that you should manually create a DNS delegation to the DNS server to ensure reliable name resolution. If you are installing an additional domain controller in either the forest root domain (or a tree root domain) , you do not need to create the DNS delegation. In this case, you can safely ignore the message and click Yes.



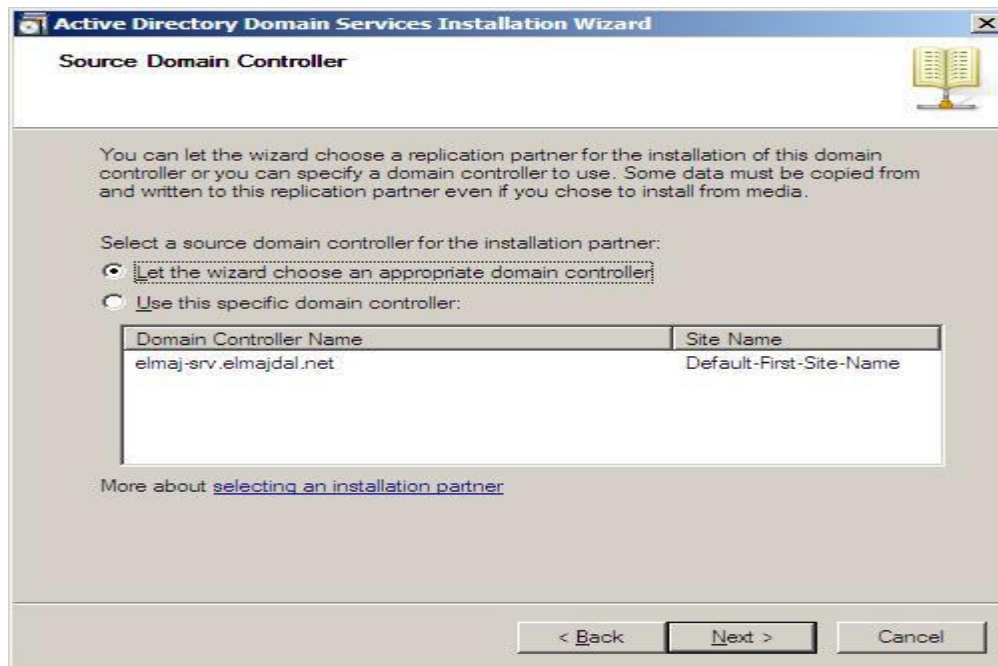
Install from media

In the Install from Media page (will be displayed if you have selected Use advanced mode installation on the Welcome page, if you didn't select it, then skip to step # 15), you can choose to either replicate data over the network from an existing domain controller, or specify the location of installation media to be used to create the domain controller and configure AD DS. I want to replicate data over the network, so I will choose the first option > click Next

Install from media



Select a source domain



Install read only control or not

If you want to choose from the list, any domain controller can be the installation partner. However, the following restrictions apply to the domain controllers that can be used as an installation partner in other situations:

A read-only domain controller (RODC) can never be an installation partner.

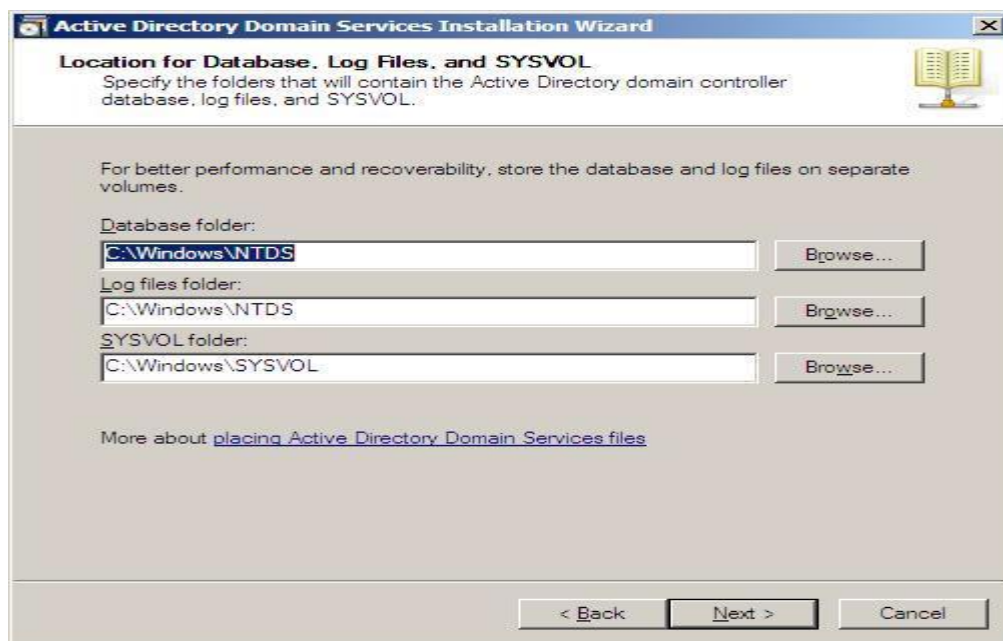
- If you are installing an RODC, only a writable domain controller that runs Windows Server 2008 can be an installation partner.

- If you are installing an additional domain controller for an existing domain, only a domain controller for that domain can be an installation partner.

Log file and sysvol

Now you will have to specify the location where the domain controller database, log files and SYSVOL are stored on the server. The database stores information about the users, computers and other objects on the network. the log files record activities that are related to AD DS, such information about an object being updated. SYSVOL stores Group Policy objects and scripts. By default, SYSVOL is part of the operating system files in the Windows directory Either type or browse to the volume and folder where you want to store each, or accept the defaults and click on Next

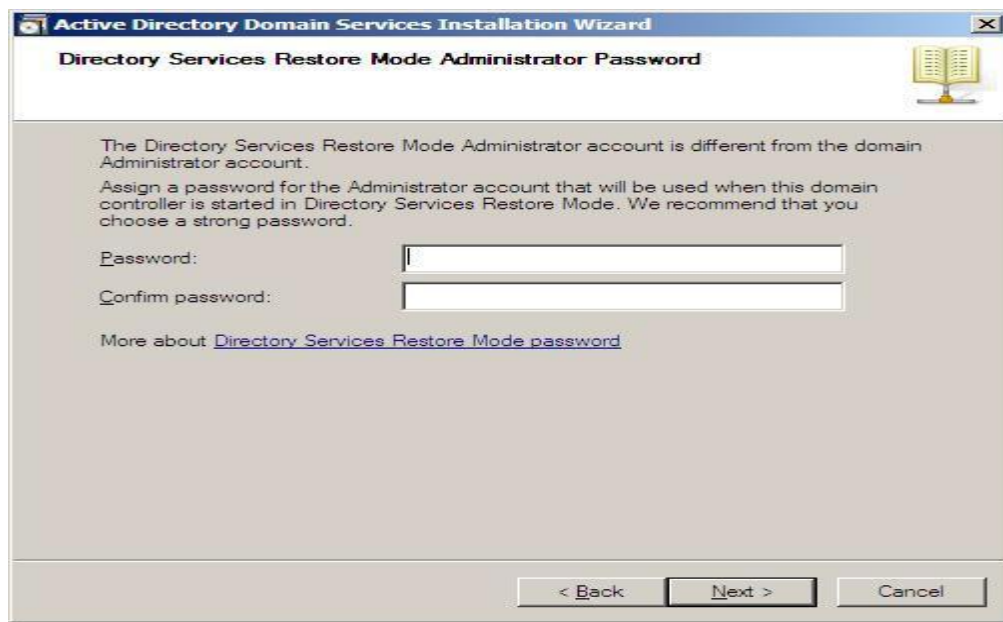
Finish installation



Backup and recovery

Note : Windows Server Backup backs up the directory service by volume. For backup and recovery efficiency, store these files on separate volumes that do not contain applications or other nondirectory files.

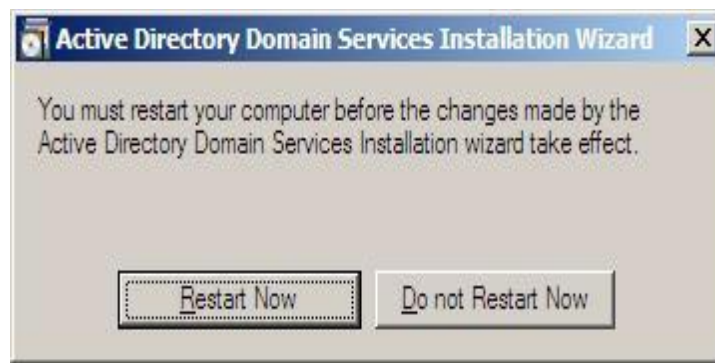
- In the Directory Services Restore Mode Administrator Password (DSRM) page, write a password and confirm it. This password is used when the domain controller is started in Directory Services Restore Mode, which might be because Active Directory Domain Services is not running, or for tasks that must be performed offline.



Finish installation

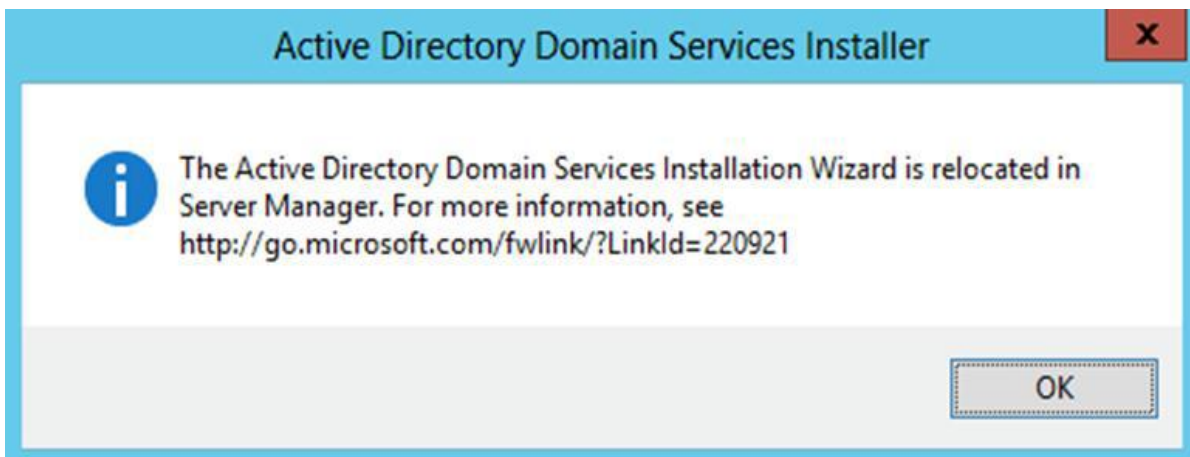
Summary page will be displayed showing you all the setting that you have set . It gives you the option to export the setting you have setup into an answer file for use to automate subsequent AD DS operations, if you wish to have such file, click on the Export settings button and save the file. Then click Next to begin AD DS installation

Active Directory Domain Services installation will be completed, click Finish, then click on Restart Now to restart your server for the changes to take effect



25.2- Add Additional Domain Controller to a windows Server 2012

When you try and run DCPromo from the explorer shell on Windows Server 2012, you will receive the following message “The Active Directory Domain Services Installation Wizard is relocated in Server Manager..

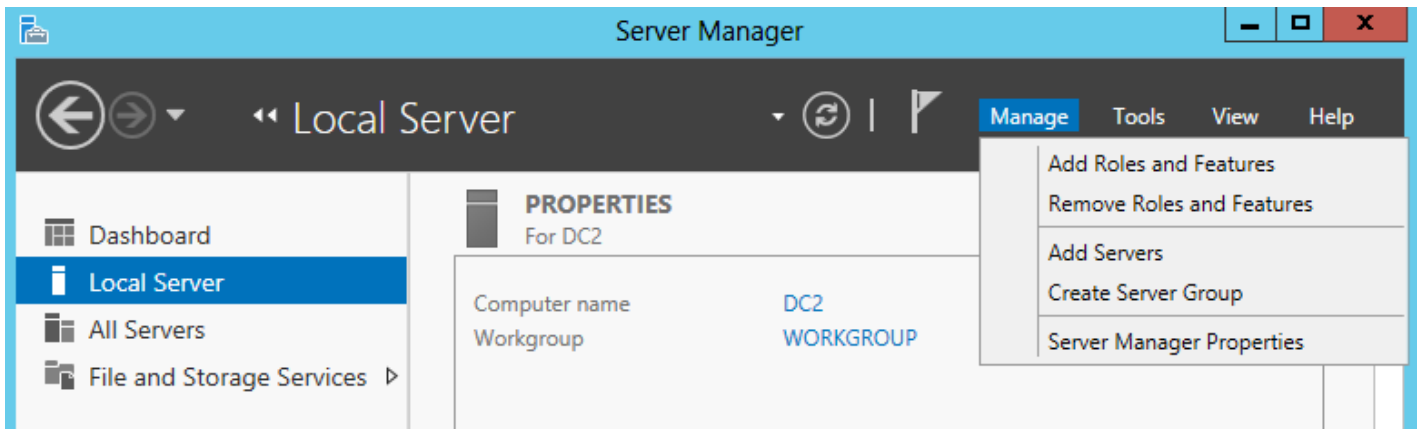


No DCPromo, what now?! DCPromo is deprecated in Windows Server 2012, so adding an additional Domain Controller is slightly different than in earlier versions. The new process is still straight forward, and the wizard will even extend the schema (to version 56) for you- meaning it's a one-stop process. Adding a Windows Server 2012 Domain Controller requires a Windows Server 2003 forest functional level or higher on your existing forest.

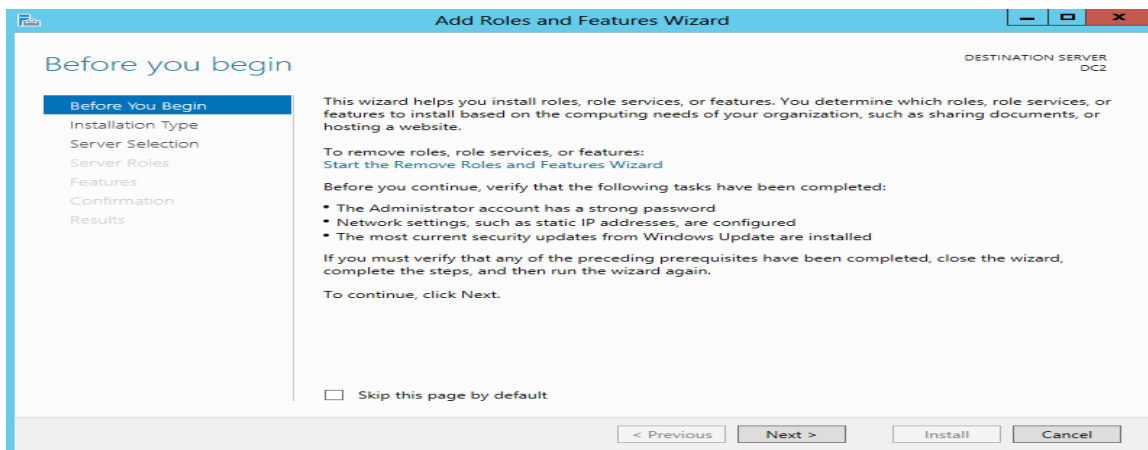
- Promoting a Server 2012 to a Domain Controller

- Open Server Manager, select Local Server on the left hand side then choose Manager -> Add roles and Features.

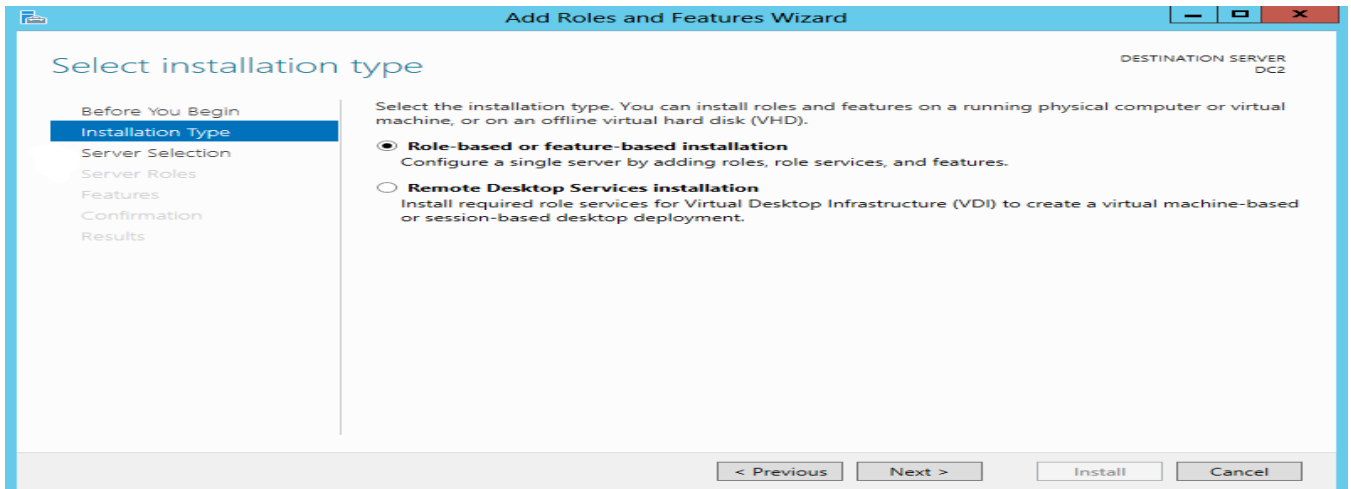
Add roles and features



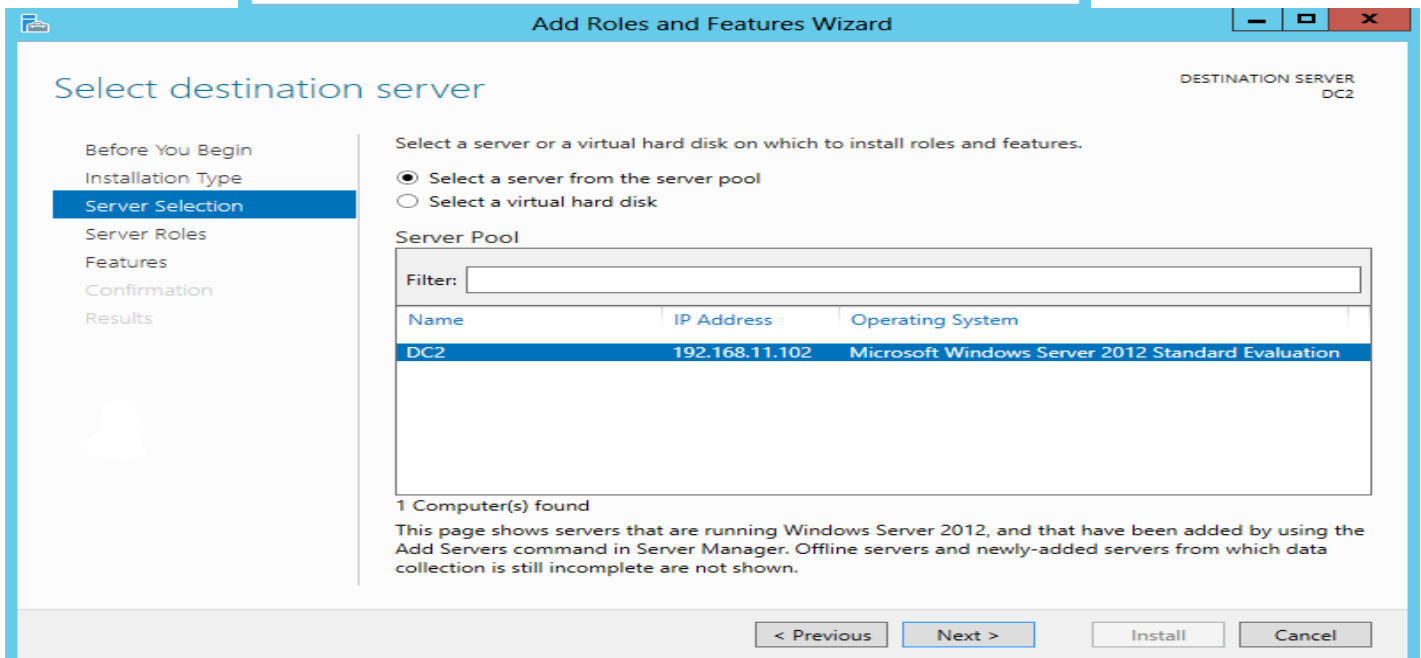
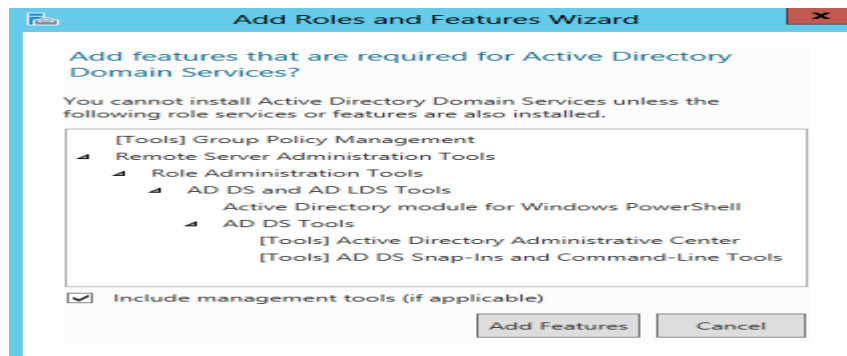
Add roles and features.



Select first option

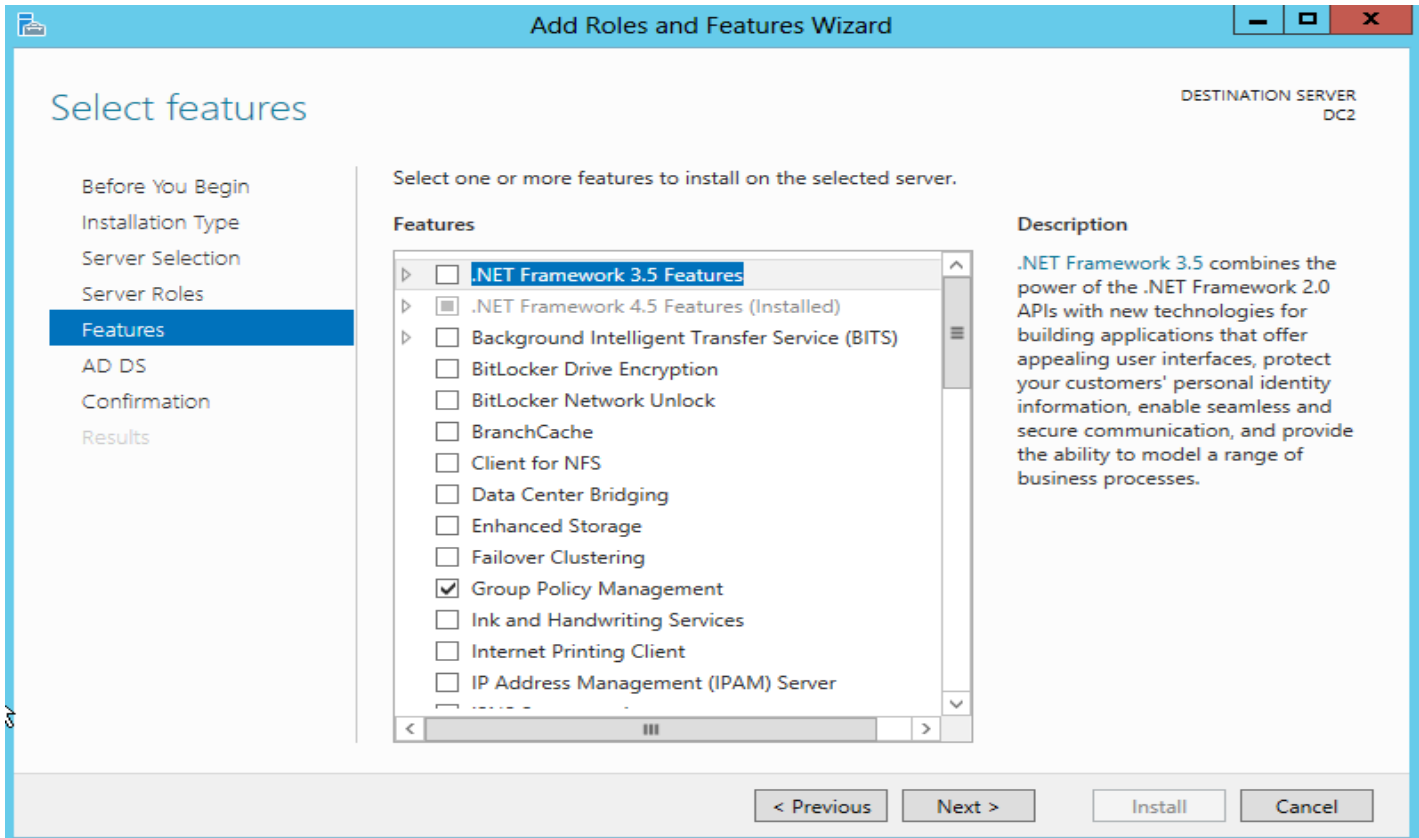


Select the server you wish to promote.

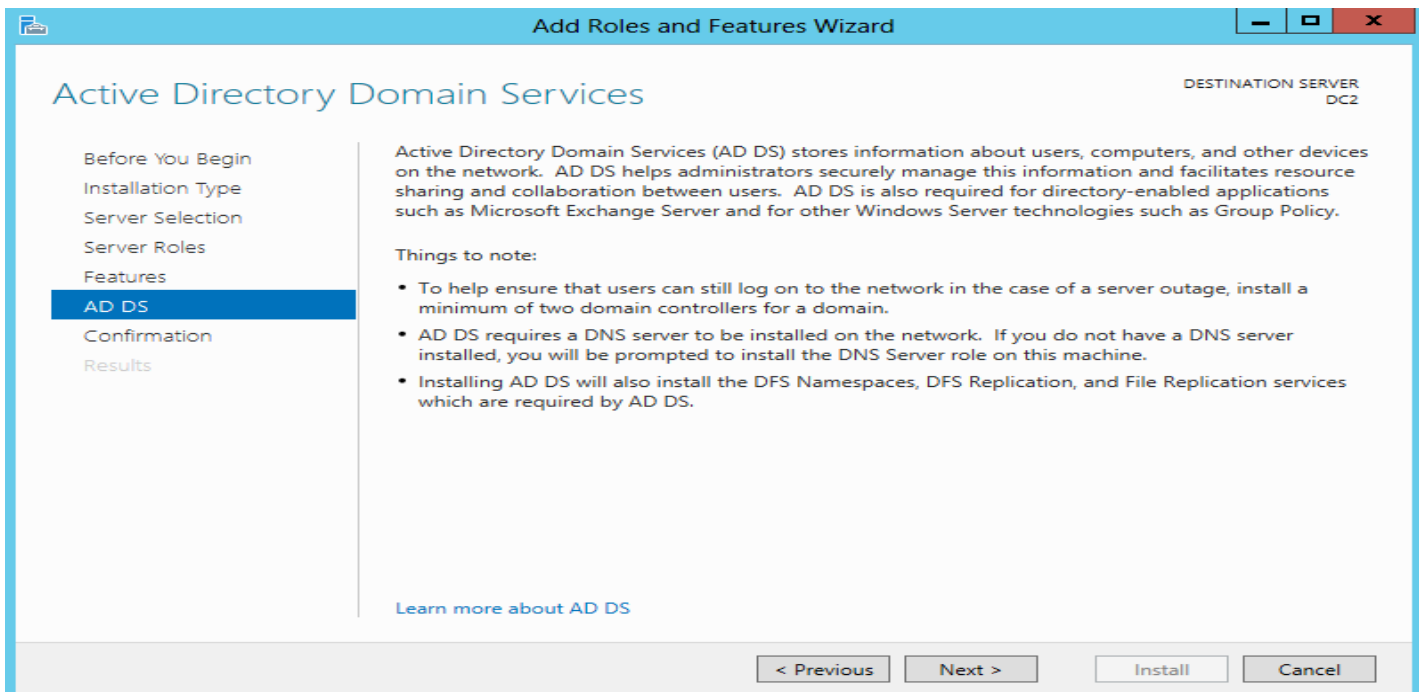


Click Add Features

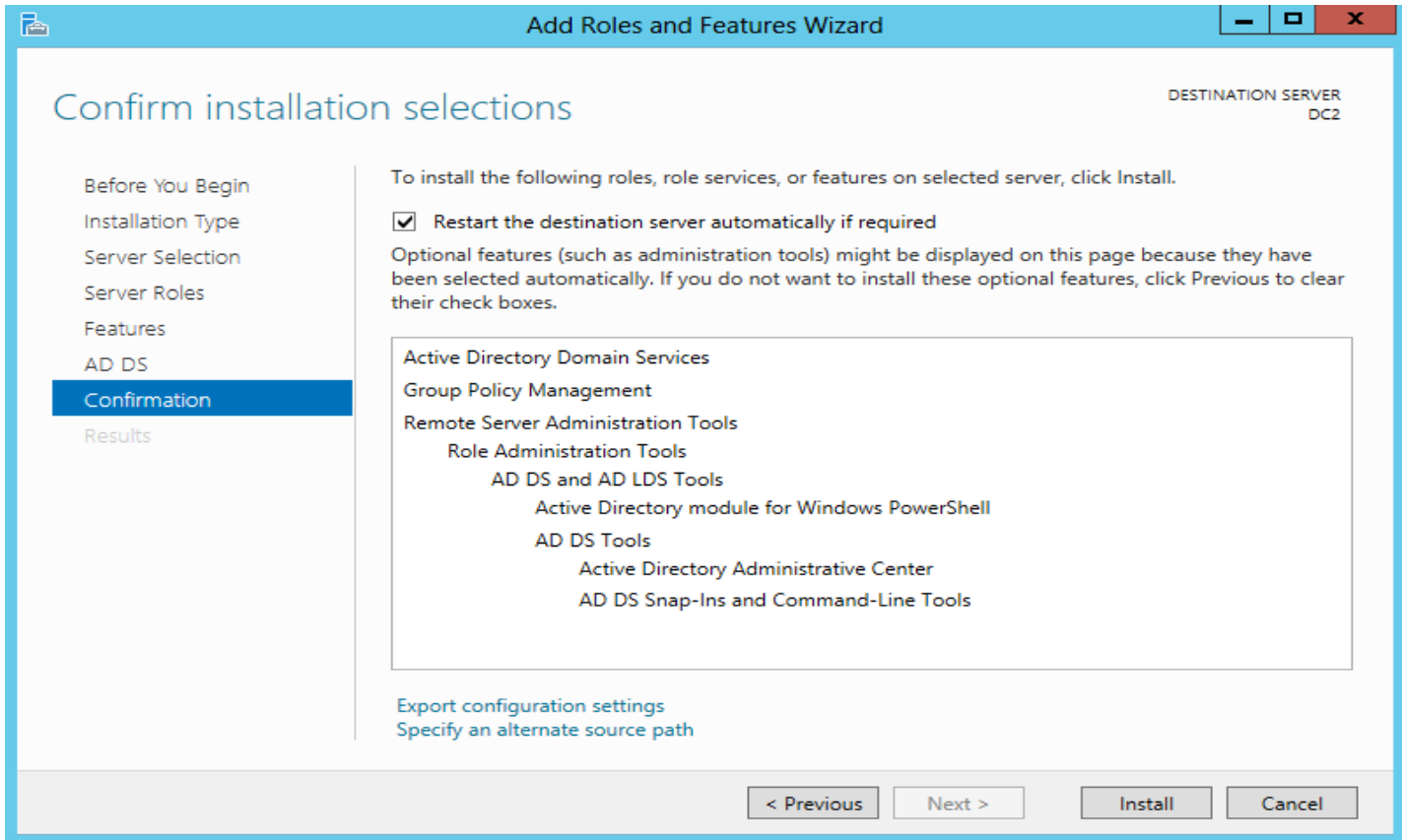
Add features



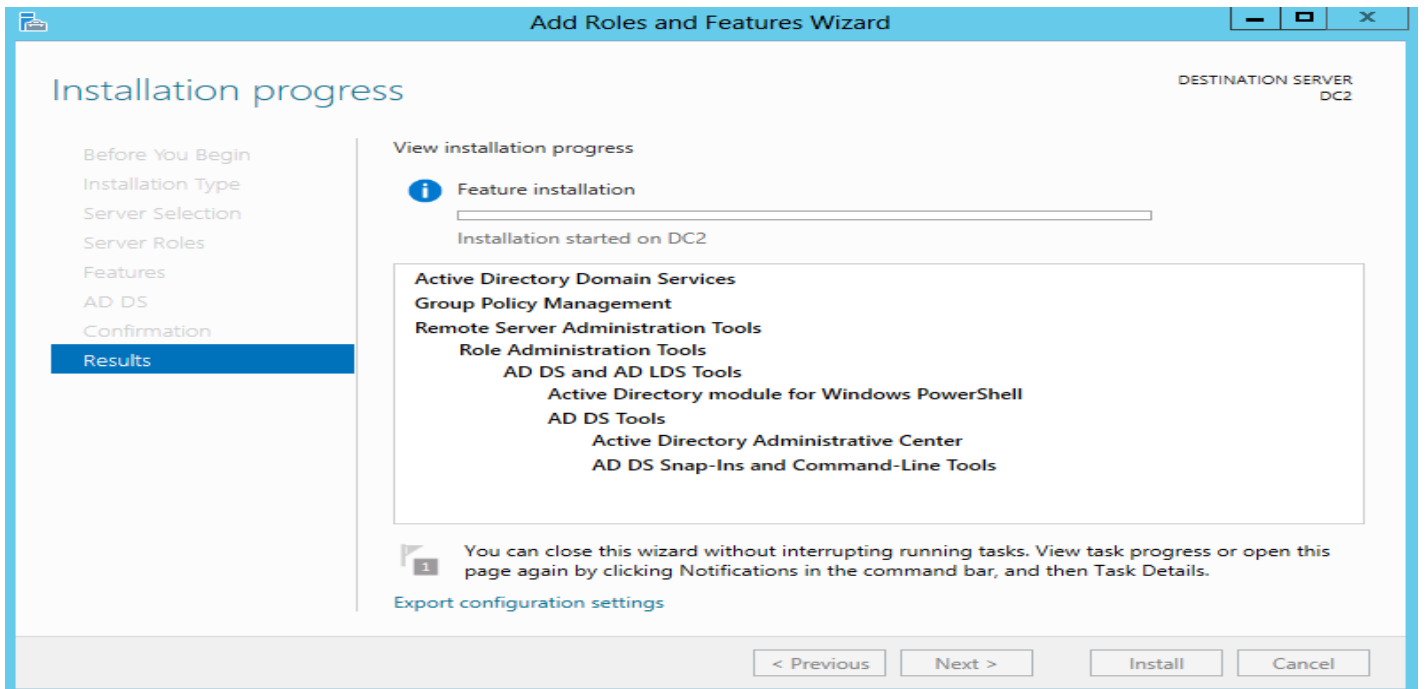
AD DS

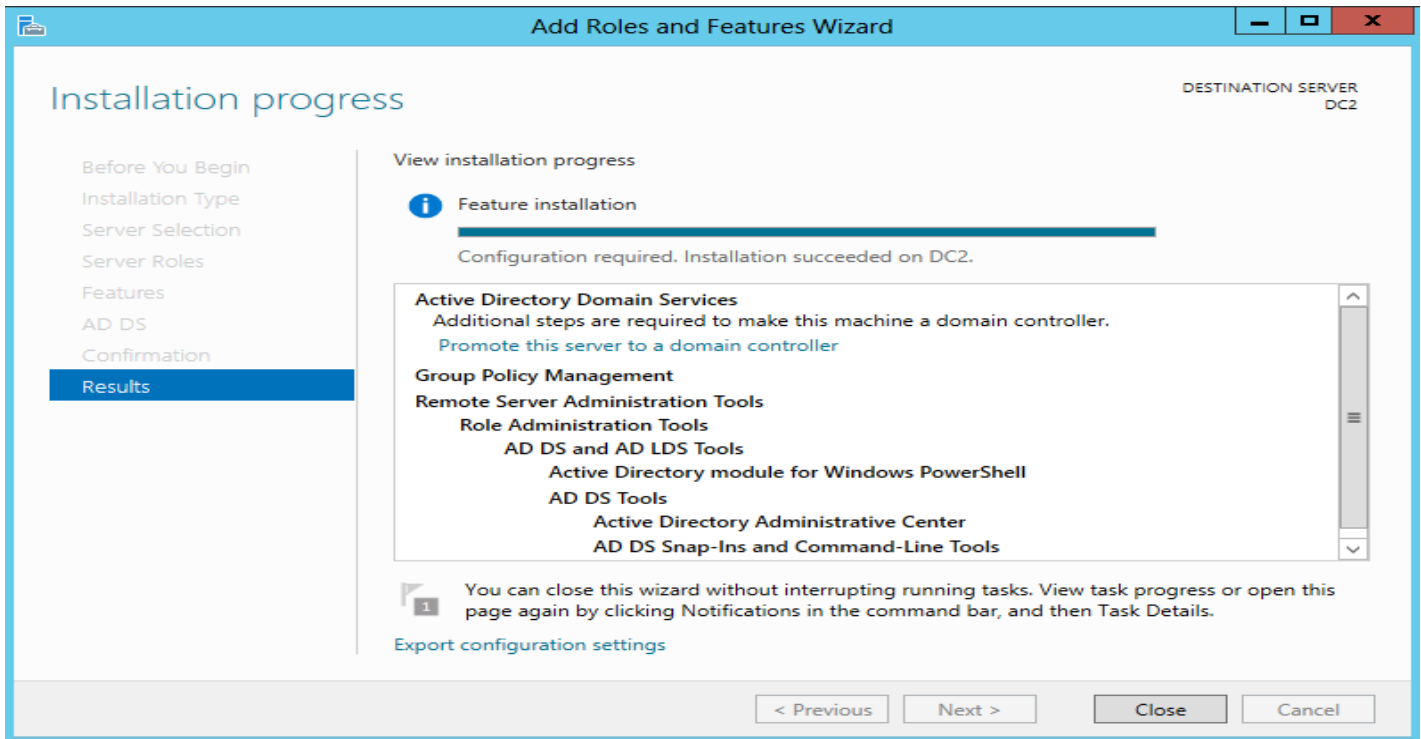


Confirmation

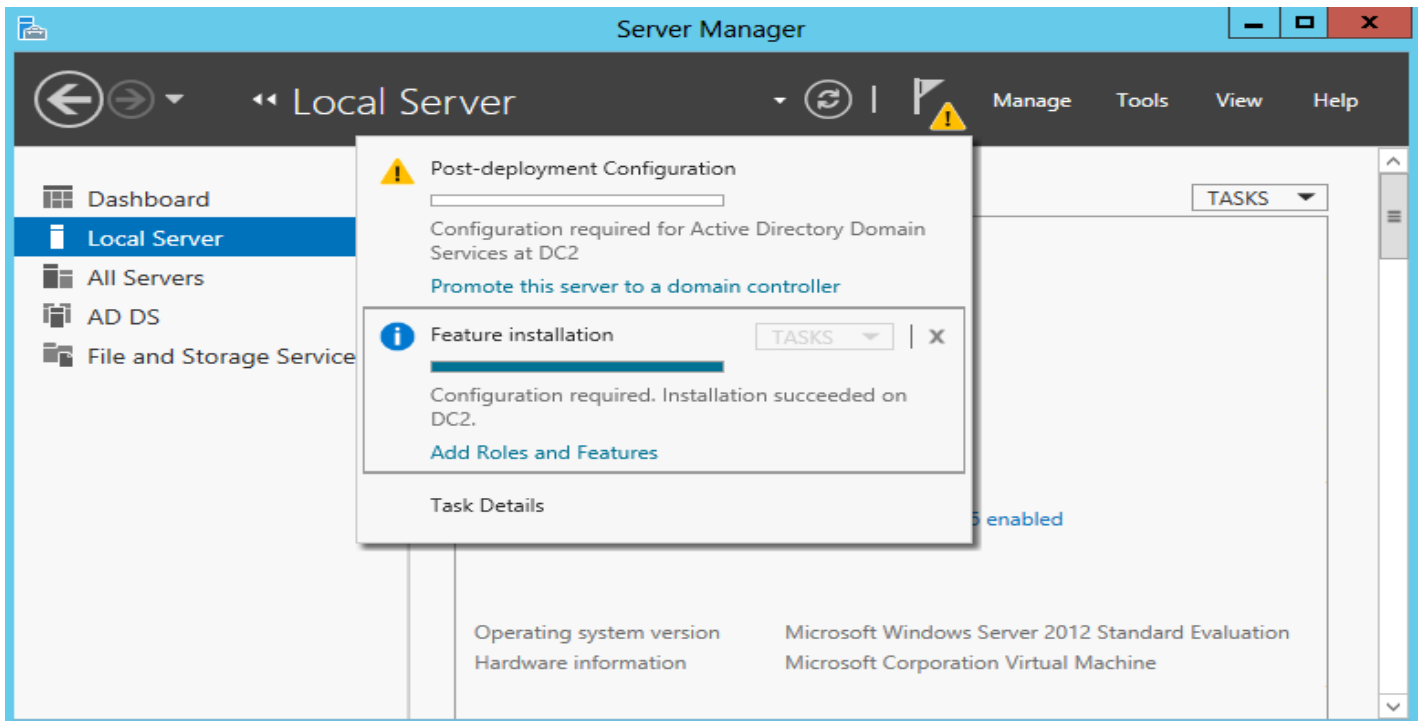


Results

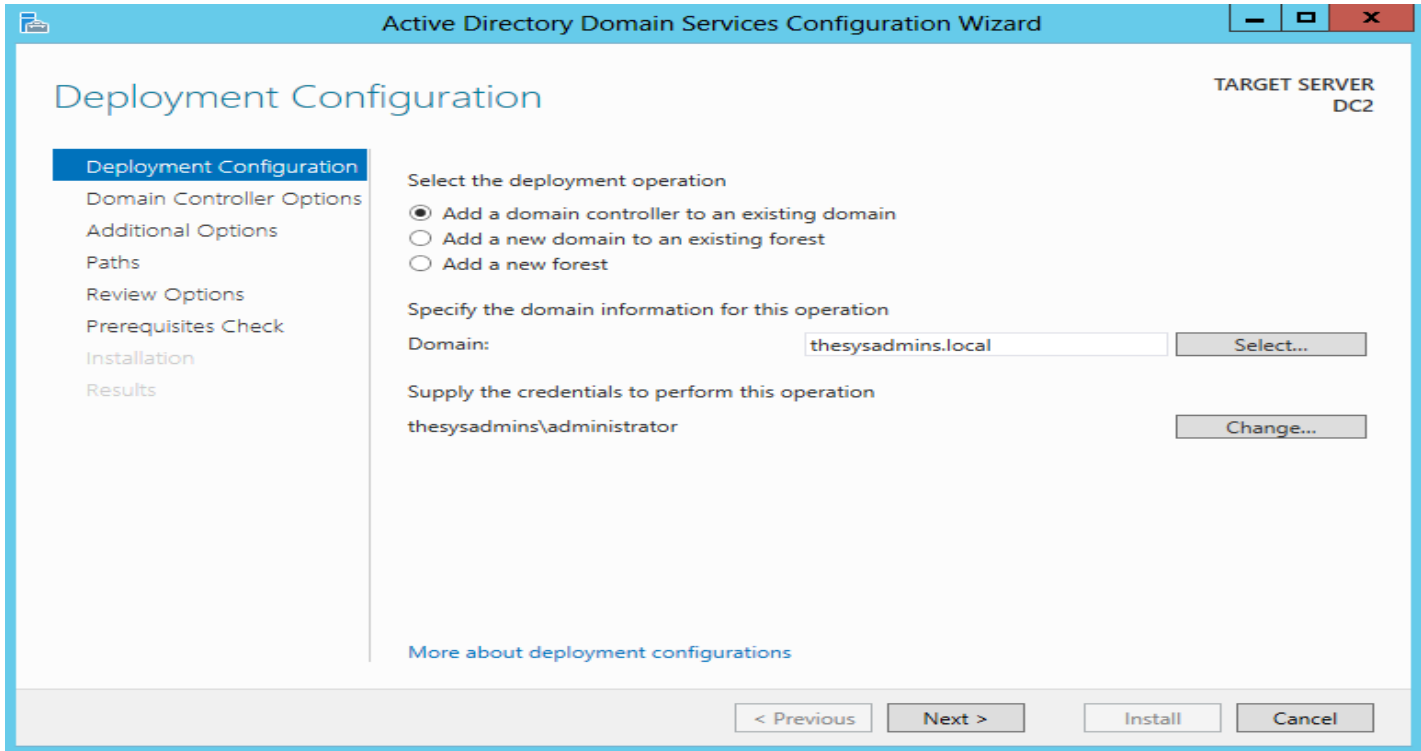




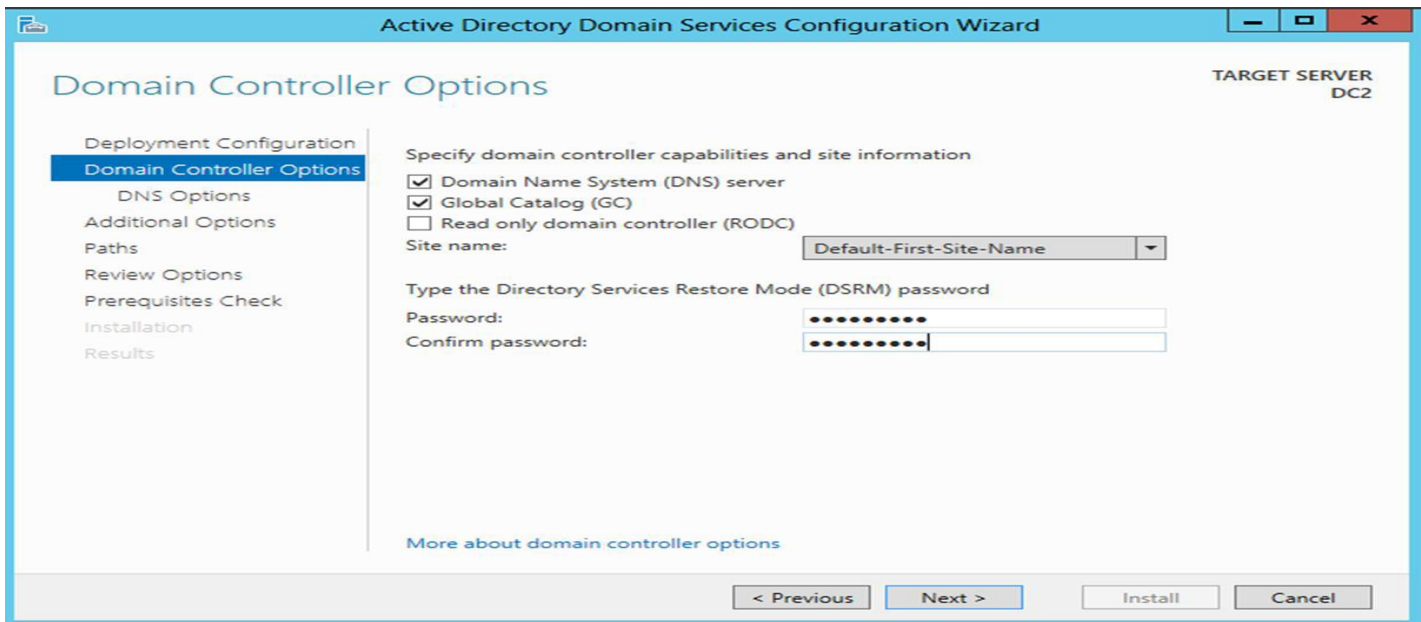
You'll now notice you have a notification, prompting you to promote this server to a domain controller.



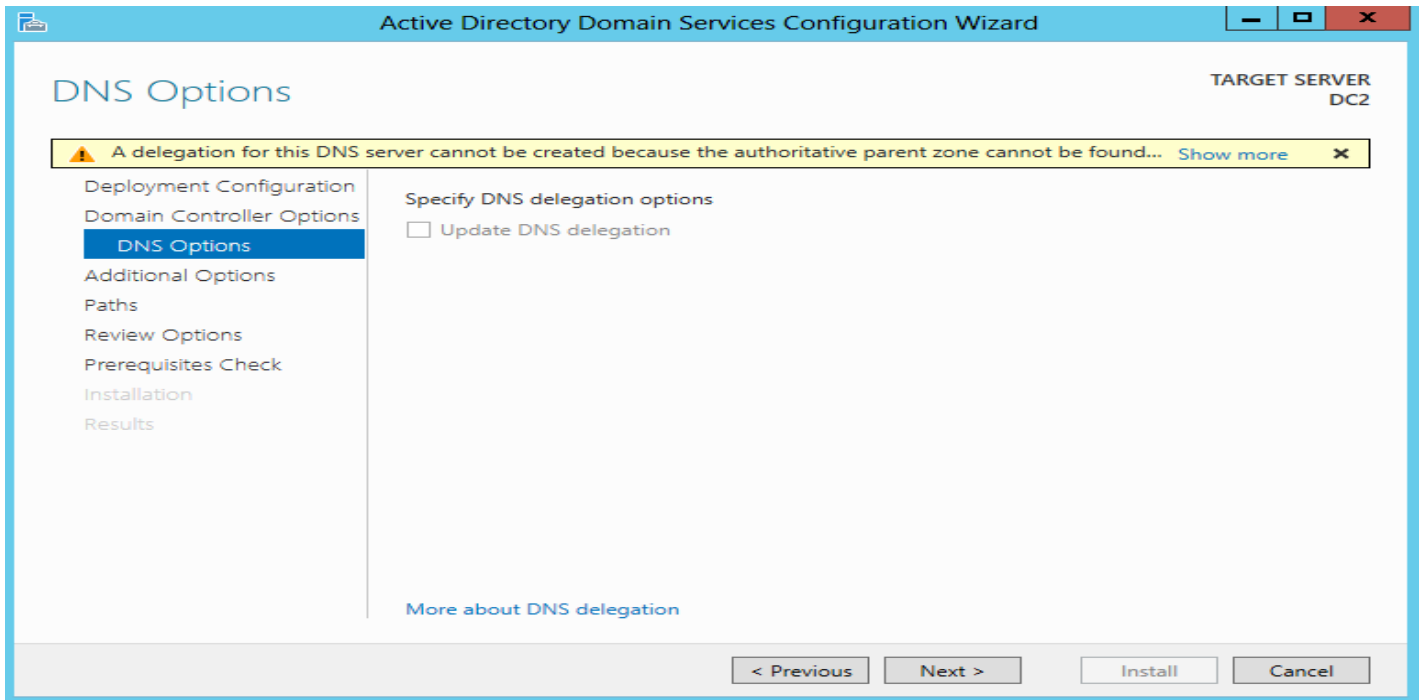
We are adding a domain controller to an existing domain, specify the domain and domain administrator credentials.



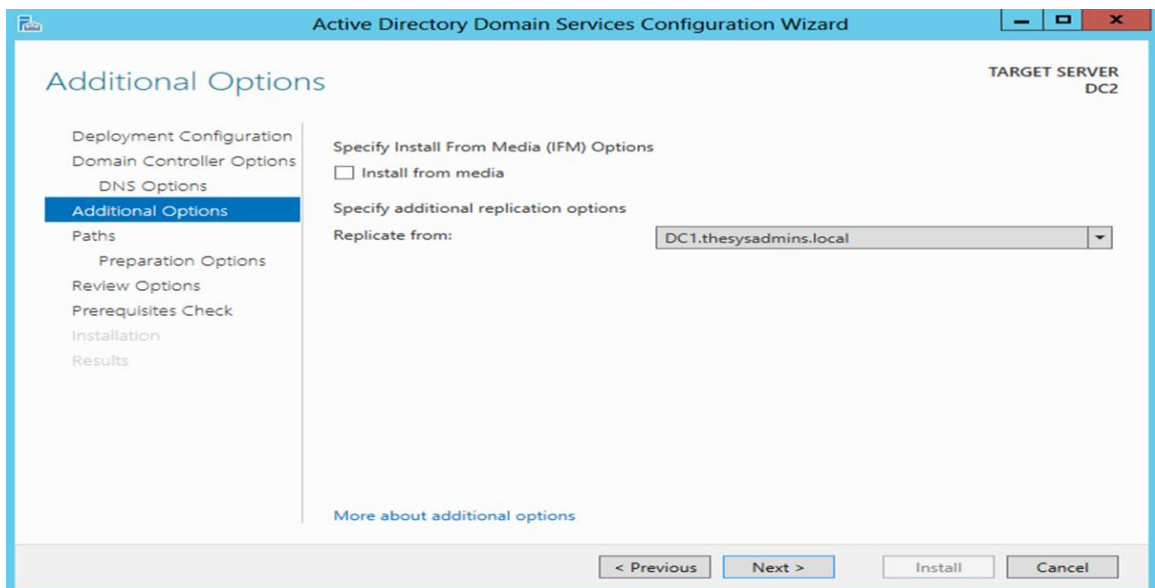
It will make the additional DC a DNS and GC by default, we do not want to make this a Read Only Domain Controller. You have the option to add the DC to a particular Site. Enter your DSRM password (as usual, keep this safe!).



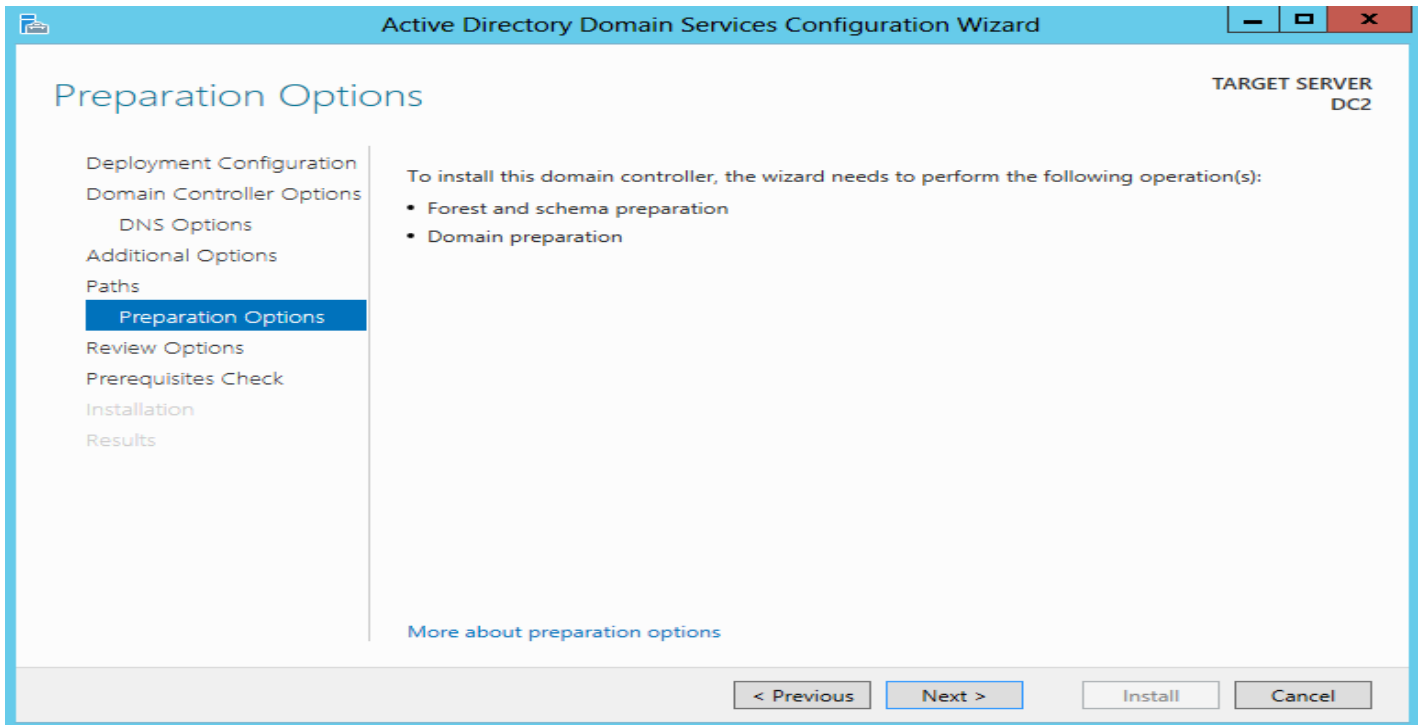
You can typically ignore the warning about DNS delegation, a more detailed explanation can be found here



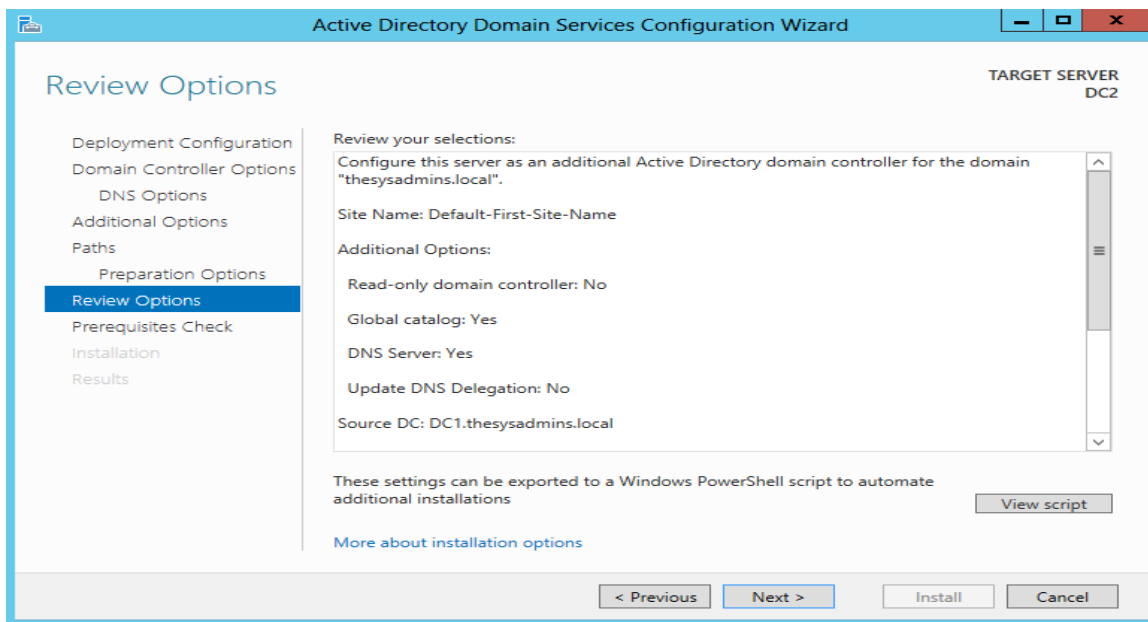
You can install from Media, which is useful if you are promoting a DC in a branch office with a poor connection- it will significantly reduce the initial Active Directory replication. You can specify a particular DC for the initial replication.



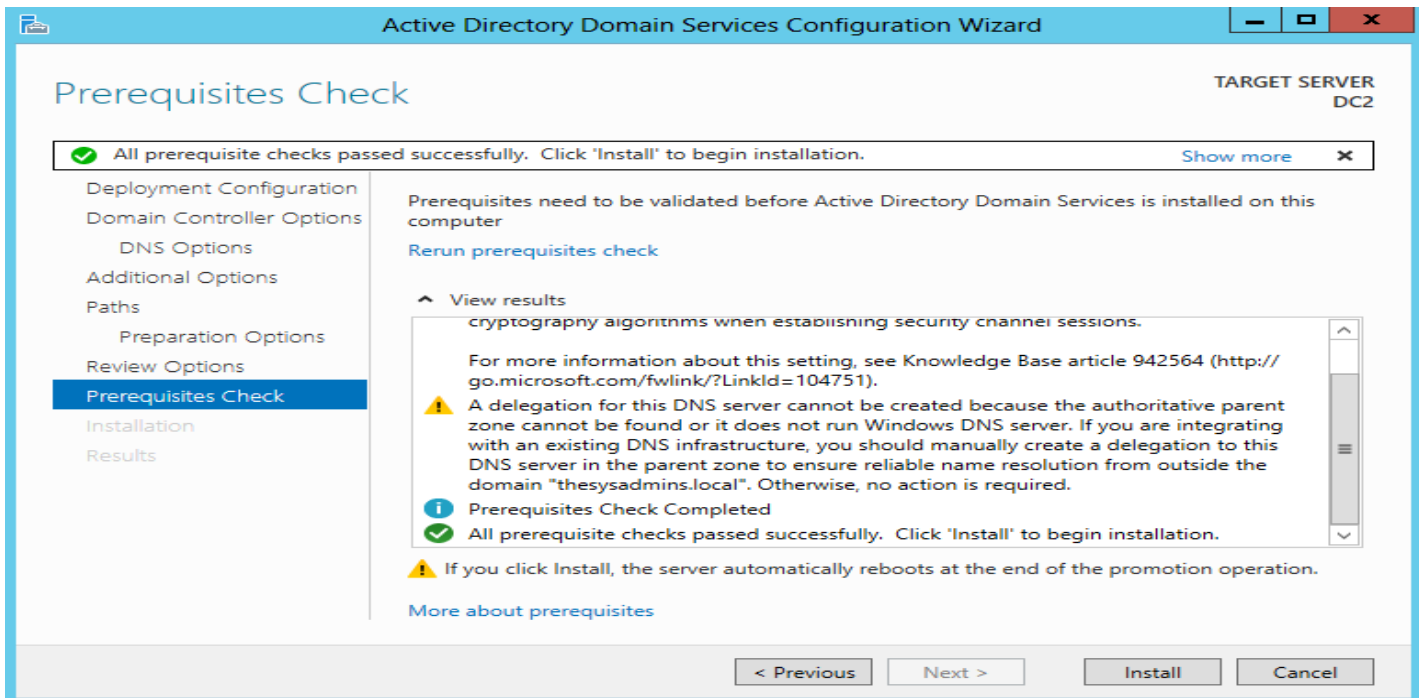
This screen tells us it will prepare the Forest, Schema and domain for us (Server 2012 uses Schema Version 56).



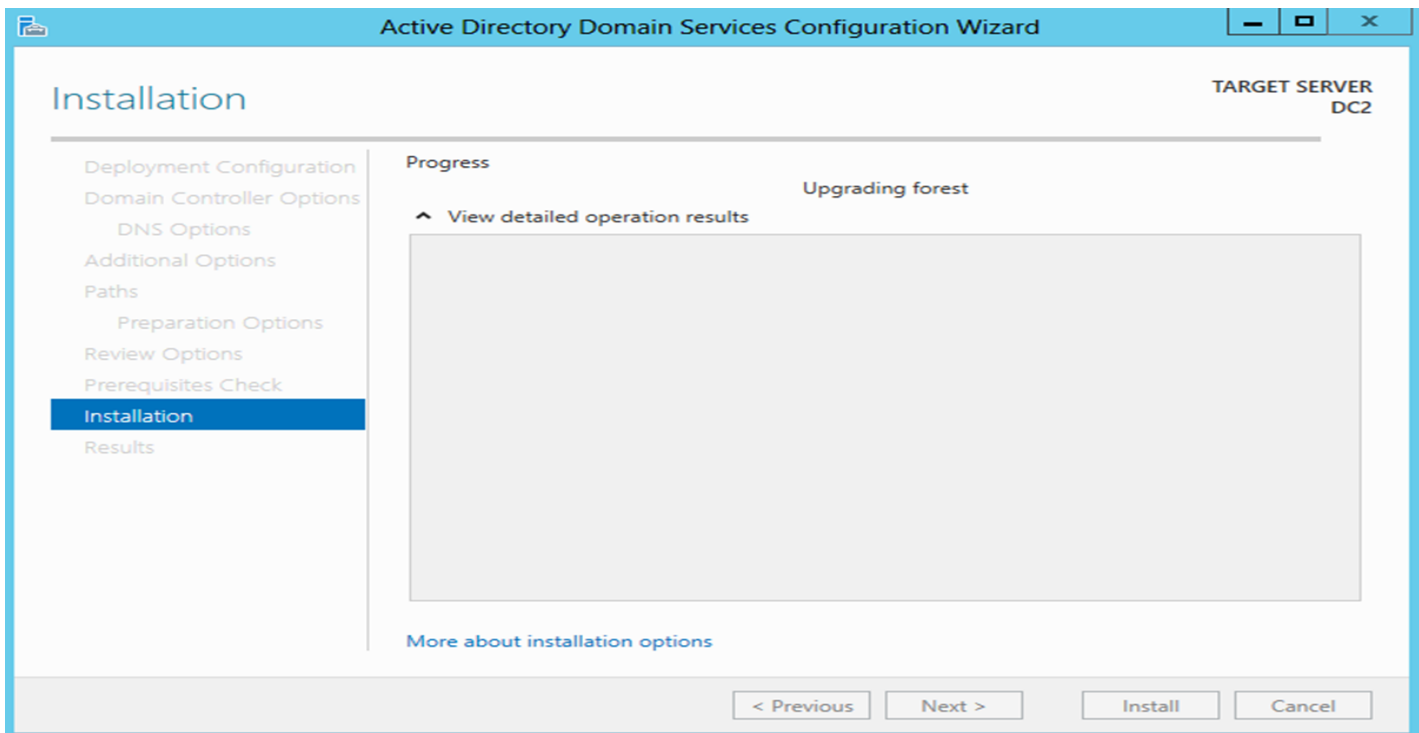
Review screen and option to view the Powershell script.



Click Install.



The install will tick over and when it has finished the server will be restarted.



25.3-Additional domain control in windows server 2016

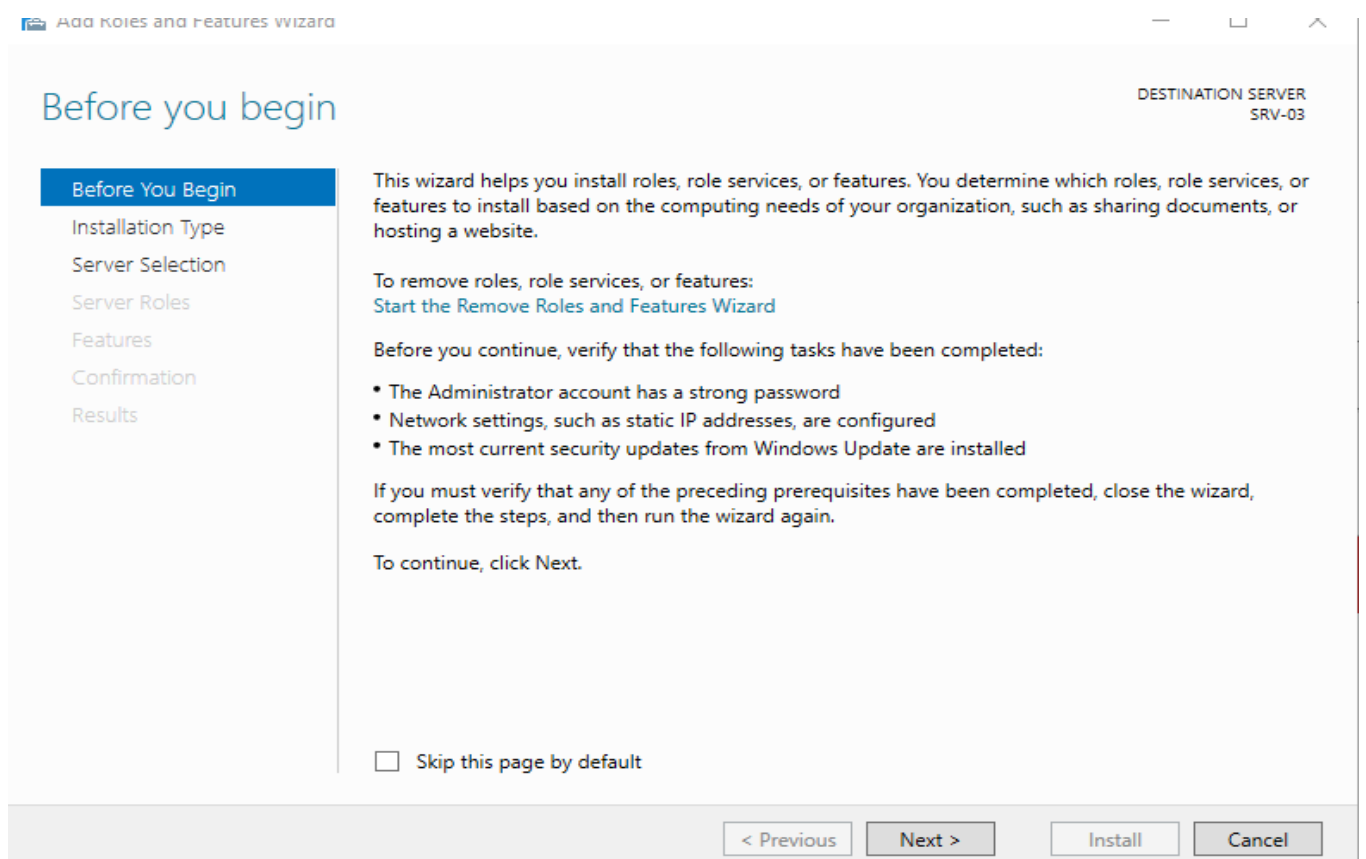
Prerequisites

- Static IP is configured
- Administrator account has strong password
- Firewall is turned off
- DNS server settings in TCP/IPv4 are correct and they are pointing to a domain controller

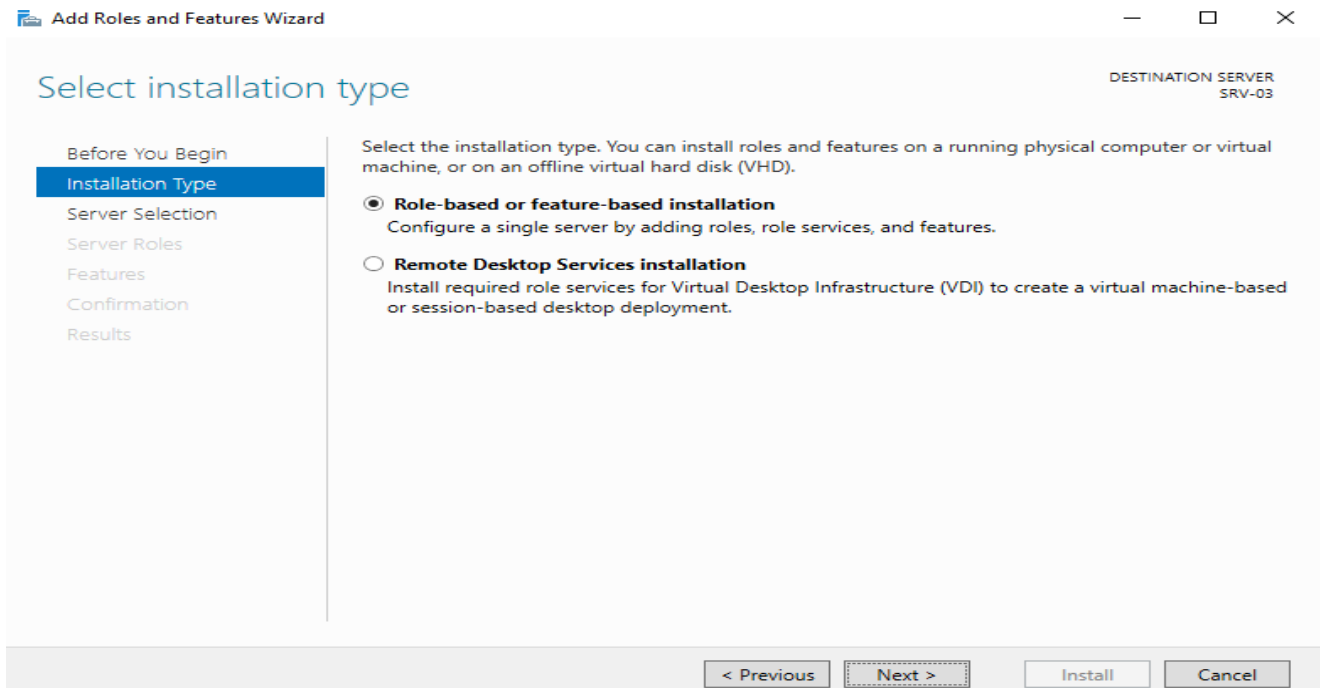
Add a New Domain in Existing Forest in Windows Server 2016

Open server manager dashboard and click Add roles and features.

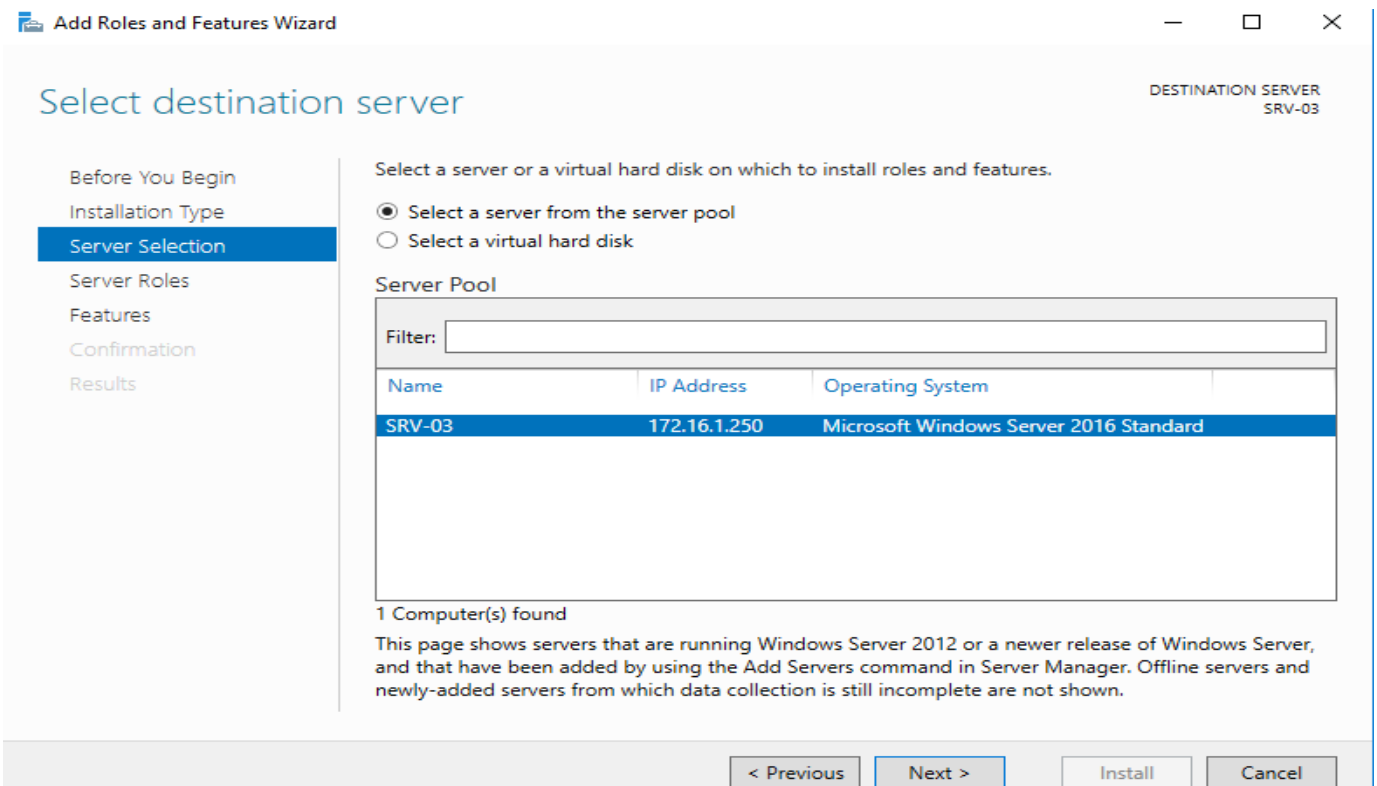
Read the prerequisites and click Next.



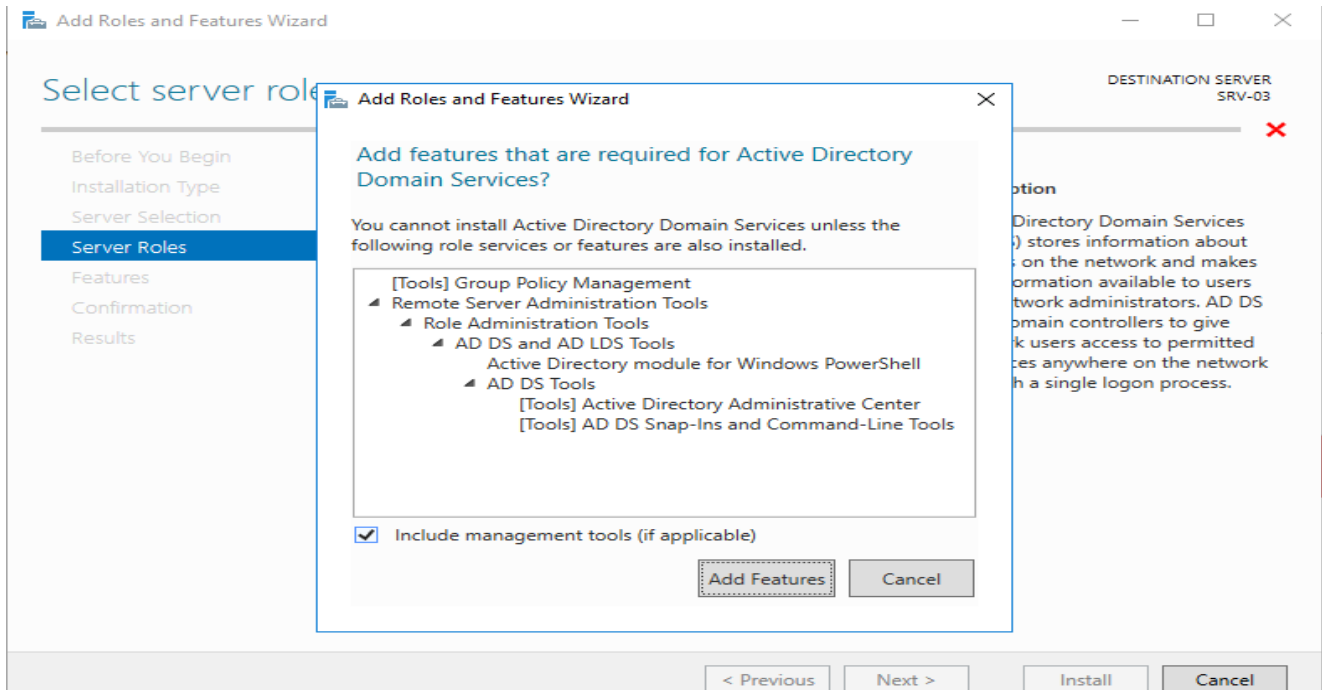
Choose Role-based or feature-based installation and click *Next*.



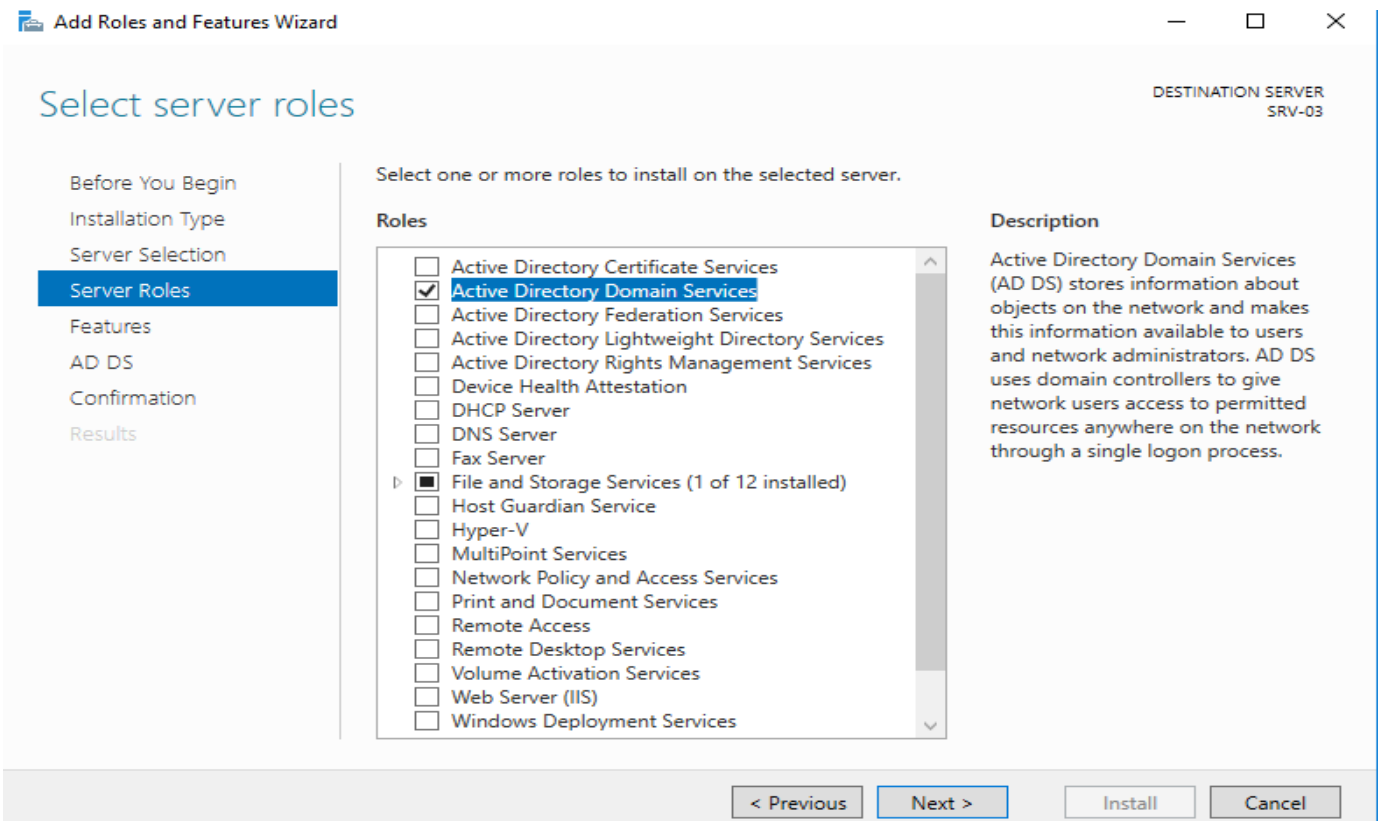
Choose the destination server on which you want to configure the new domain and click *Next*.



Choose Active Directory Domain Services from server roles. As soon as you check the server role, a new window pop up click Add Features.



Click Next.



Click Next.

Select features

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features**
- AD DS
- Confirmation
- Results

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

Features

- .NET Framework 3.5 Features (1 of 3 installed)**
- .NET Framework 4.6 Features (2 of 7 installed)**
- Background Intelligent Transfer Service (BITS)
- BitLocker Drive Encryption
- BitLocker Network Unlock
- BranchCache
- Client for NFS
- Containers
- Data Center Bridging
- Direct Play
- Enhanced Storage
- Failover Clustering
- Group Policy Management
- I/O Quality of Service
- IIS Hostable Web Core
- Internet Printing Client
- IP Address Management (IPAM) Server
- iSNS Server service
- LPR Port Monitor

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

< Previous Next > Install Cancel

Active Directory Domain Services

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD DS**
- Confirmation
- Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

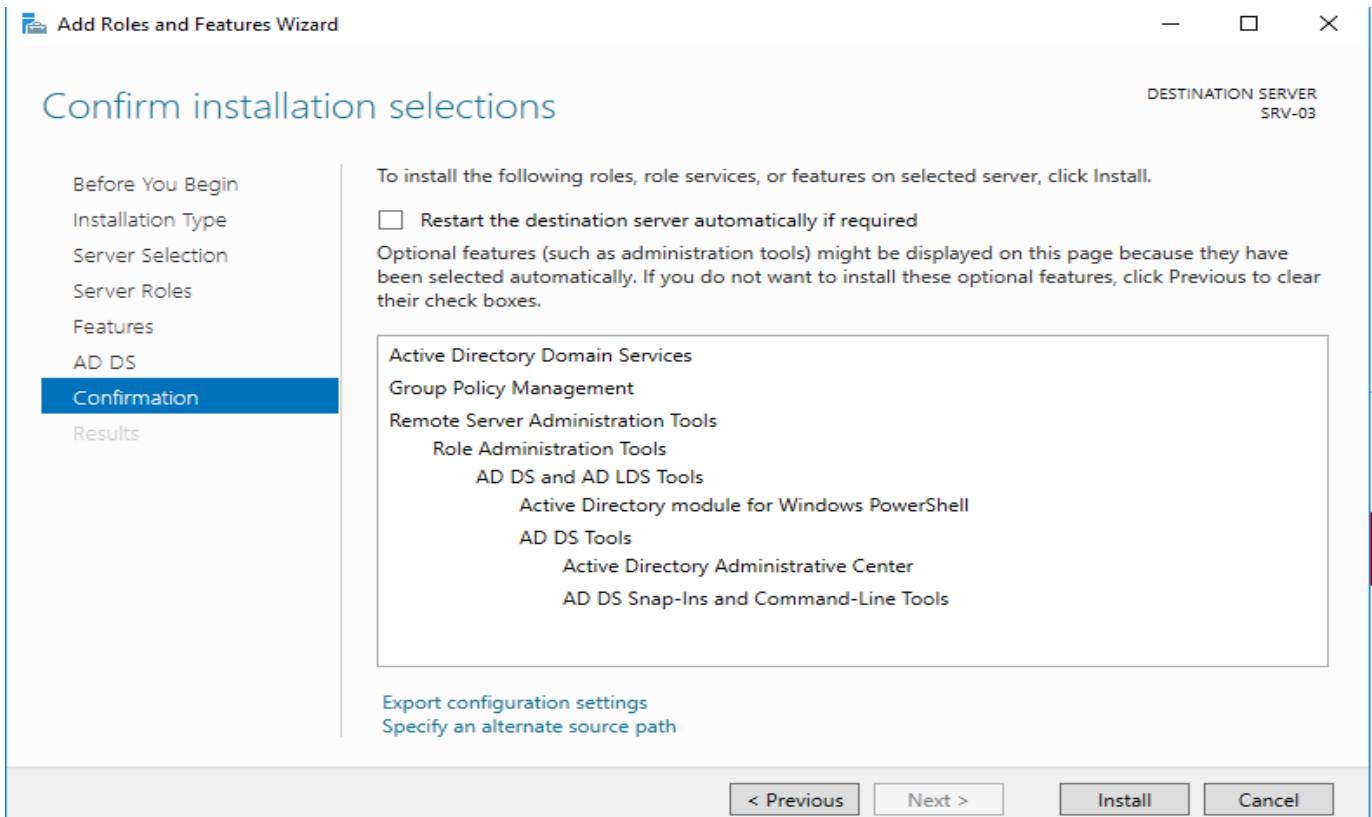


Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

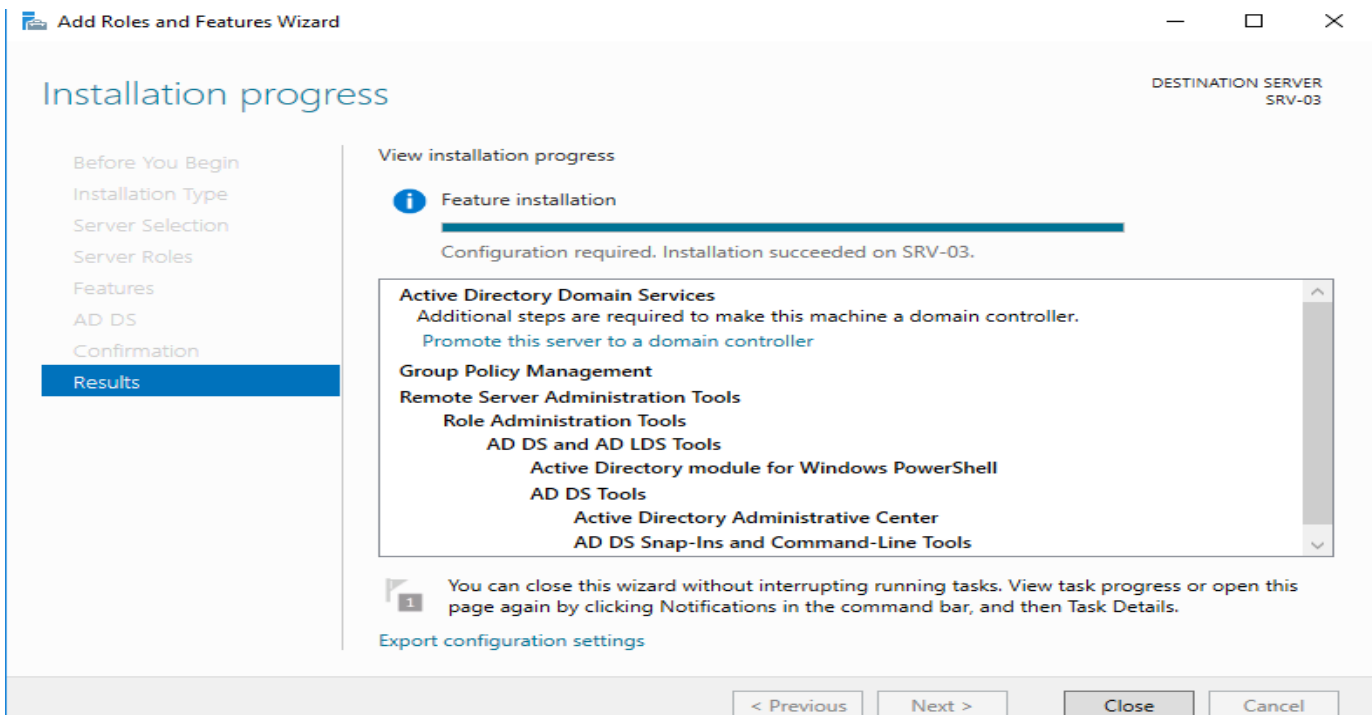
[Learn more about Azure Active Directory](#)
[Configure Office 365 with Azure Active Directory Connect](#)

< Previous Next > Install Cancel

Click Install and wait for an installation to finish. This may take several minutes to complete.



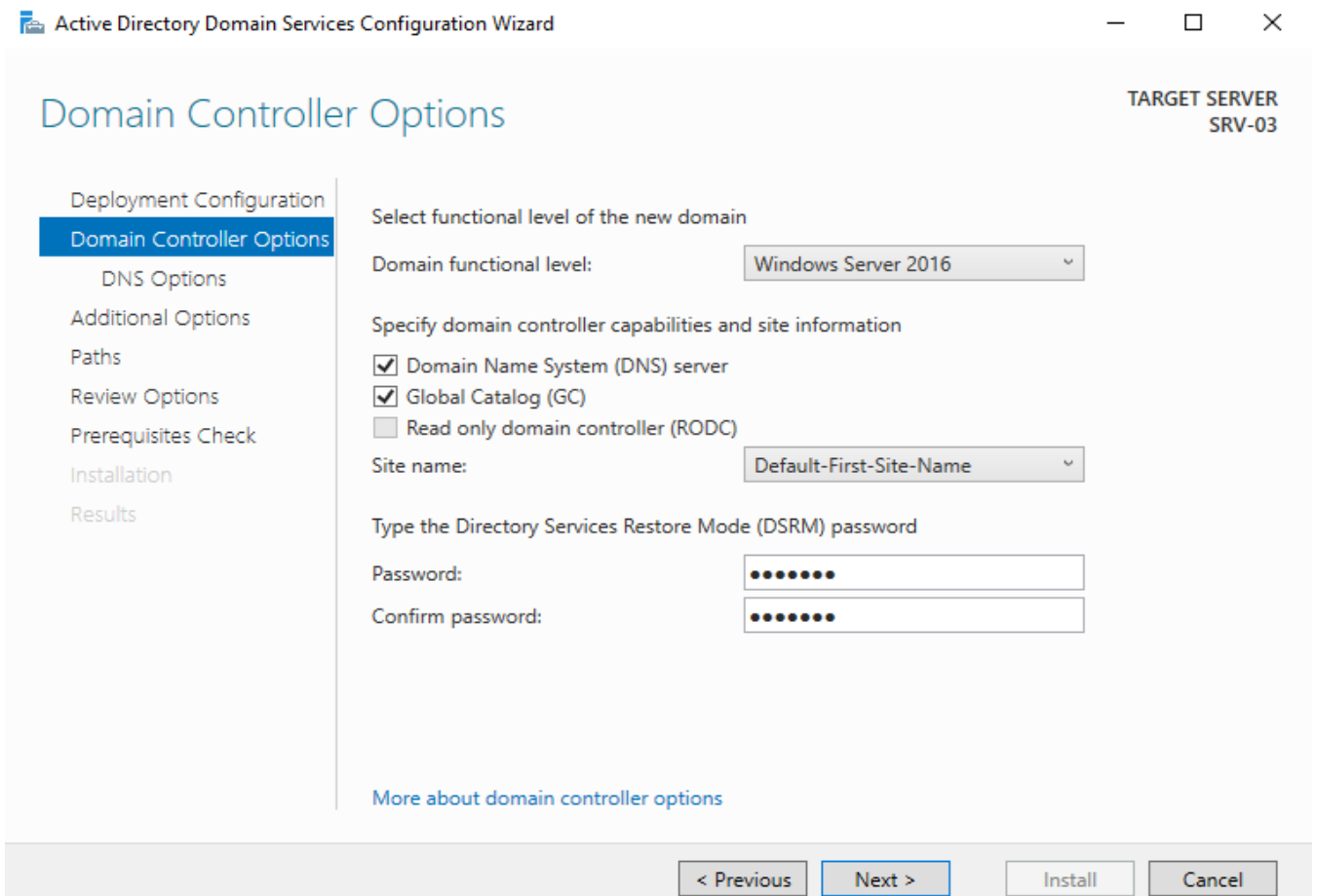
Click Promote this server to a domain controller.



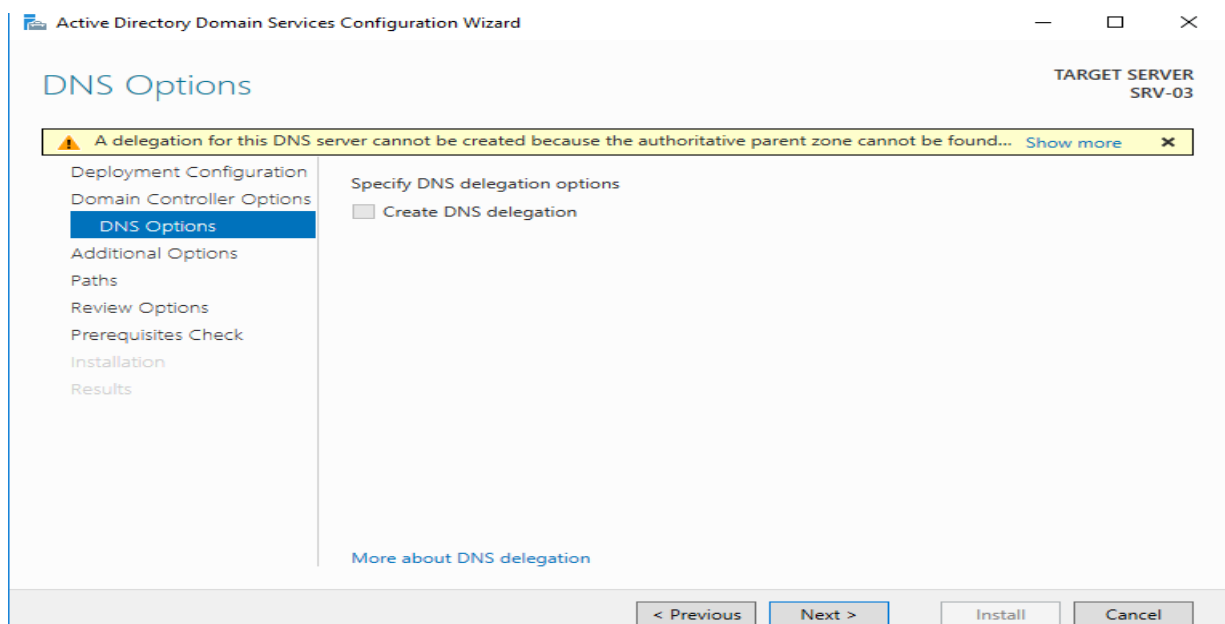
Choose to Add a new domain to an existing forest, and tree domain from domain type. Provide forest name, new domain name, and credentials of an account which is part of enterprise admin group. Click Next when you are done.

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the application name and standard window controls. The main window has a header with 'Deployment Configuration' and 'TARGET SERVER SRV-03'. A left-hand navigation pane lists steps: 'Deployment Configuration' (selected), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main area is titled 'Select the deployment operation' and contains three radio button options: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest' (which is selected), and 'Add a new forest'. Below this is the section 'Specify the domain information for this operation', which includes a 'Select domain type:' dropdown menu set to 'Tree Domain', a 'Forest name:' text box containing 'yourdomain.com', and a 'New domain name:' text box containing 'mydomain.com'. The next section is 'Supply the credentials to perform this operation', with a text box containing 'yourdomain\administrator' and a 'Change...' button. At the bottom of the wizard, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link for 'More about deployment configurations' is also visible.

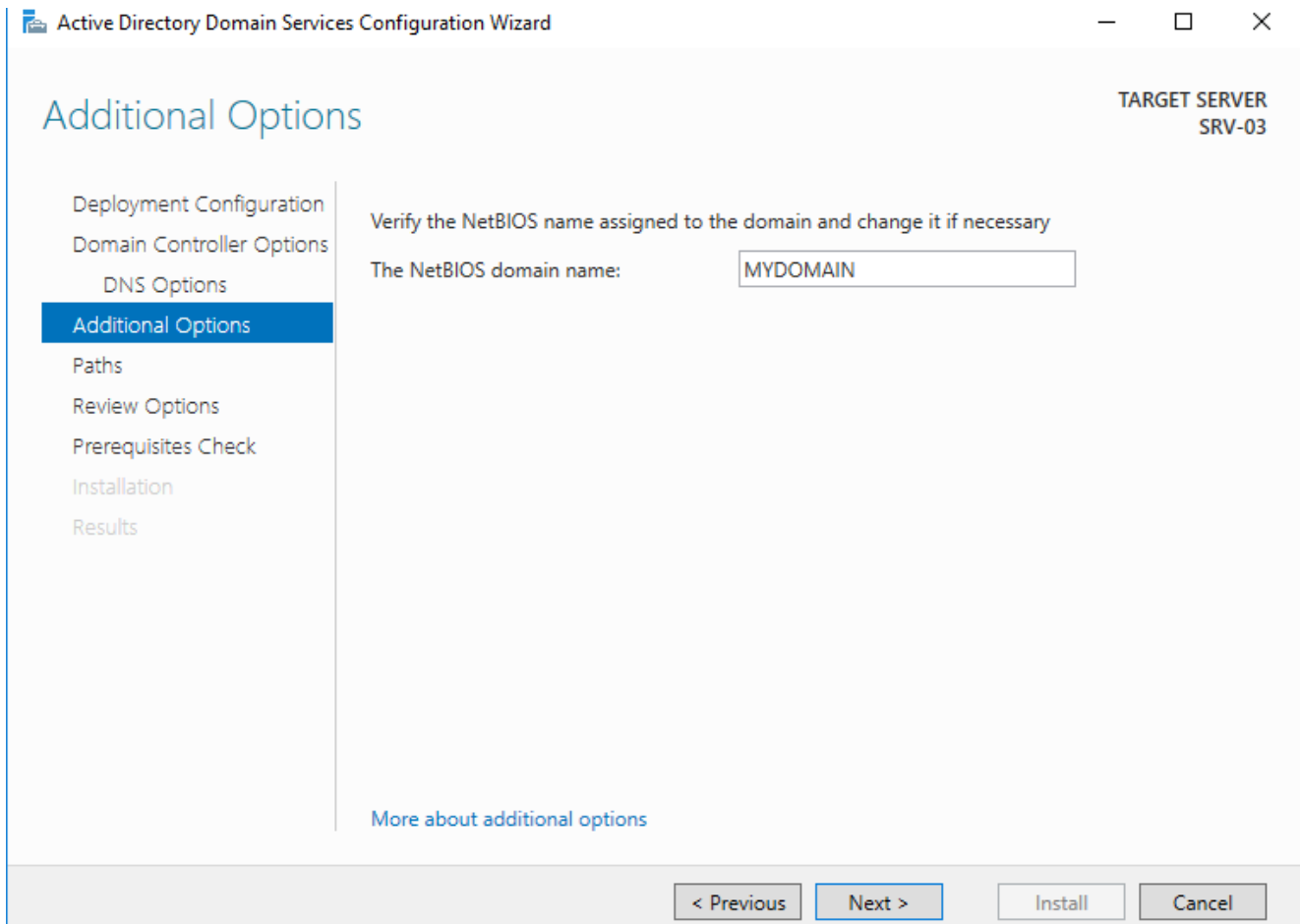
Provide Directory Services Restore Mode (DSRM) password and click Next. Keep the rest of the options as default while making sure the options for Domain Name System (DNS) Server and Global Catalog (GC) are checked.



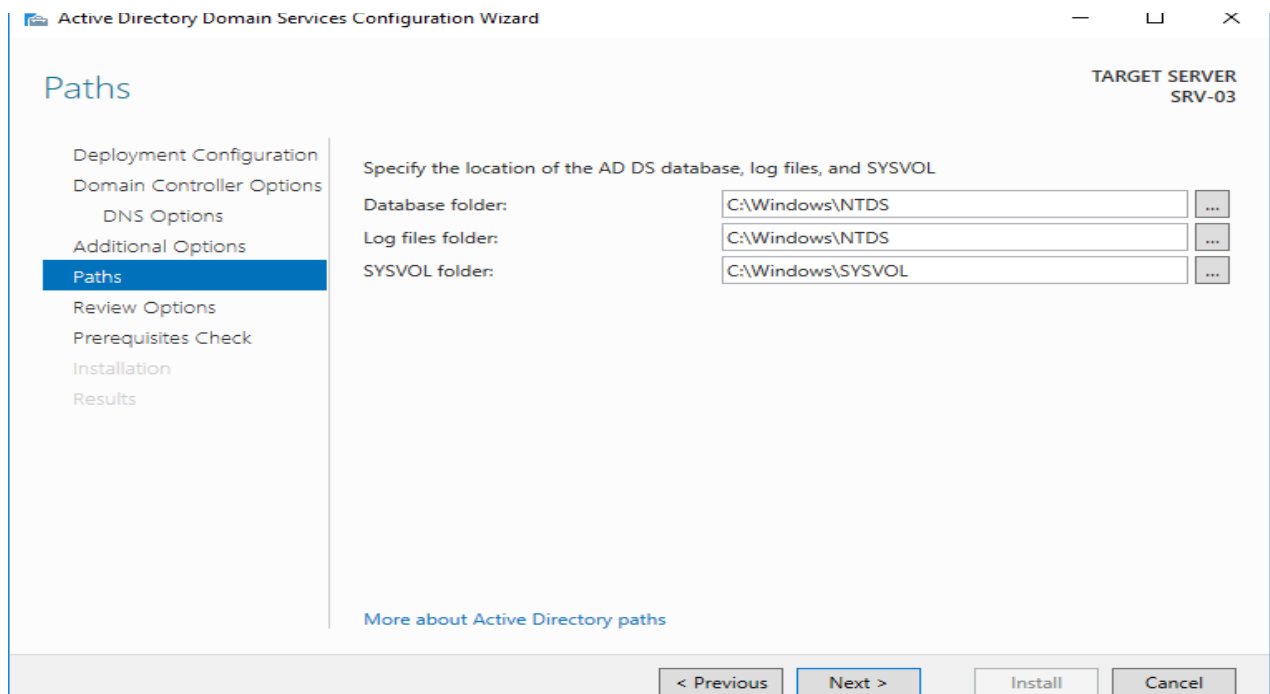
Ignore the warning and click Next.

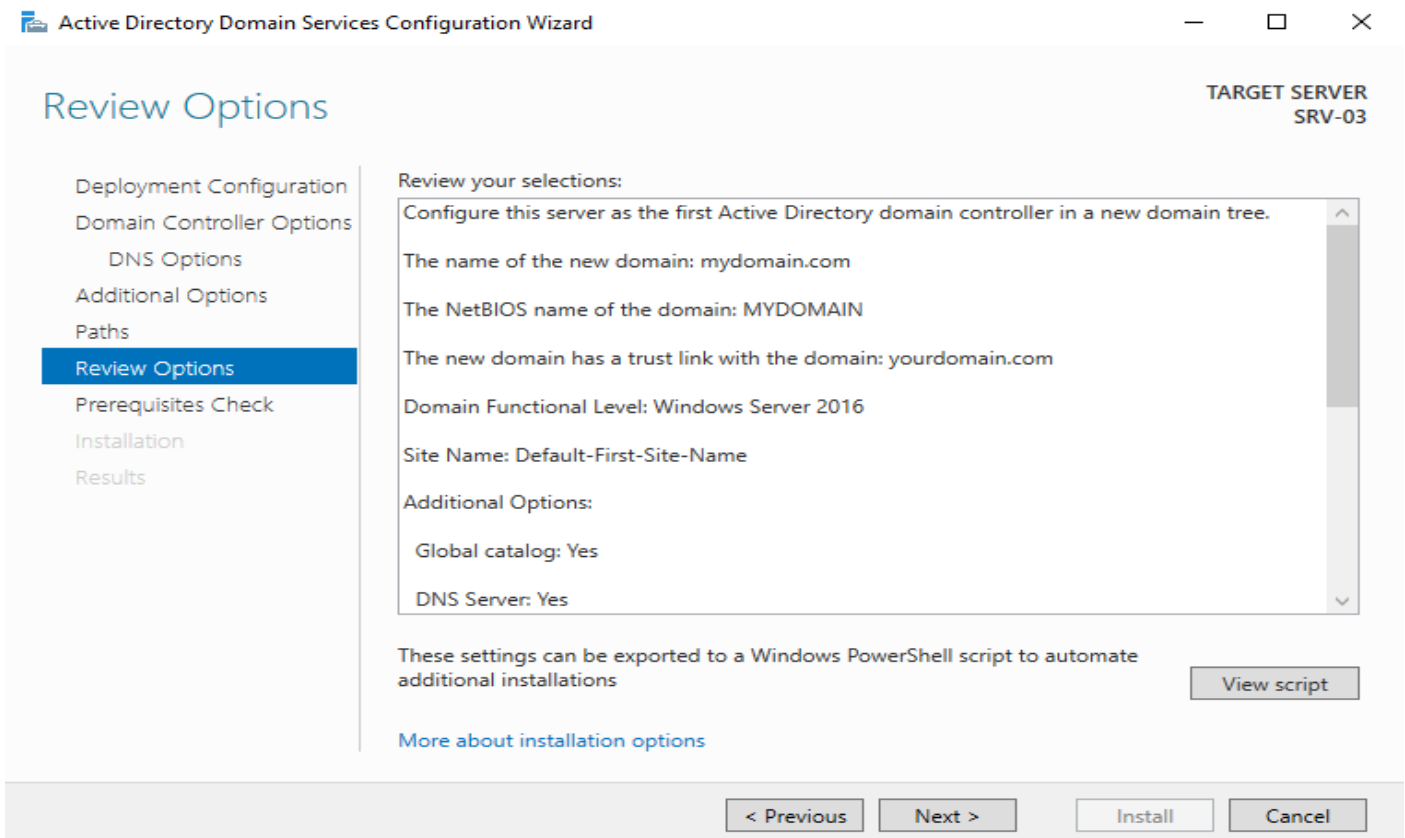


Click Next.

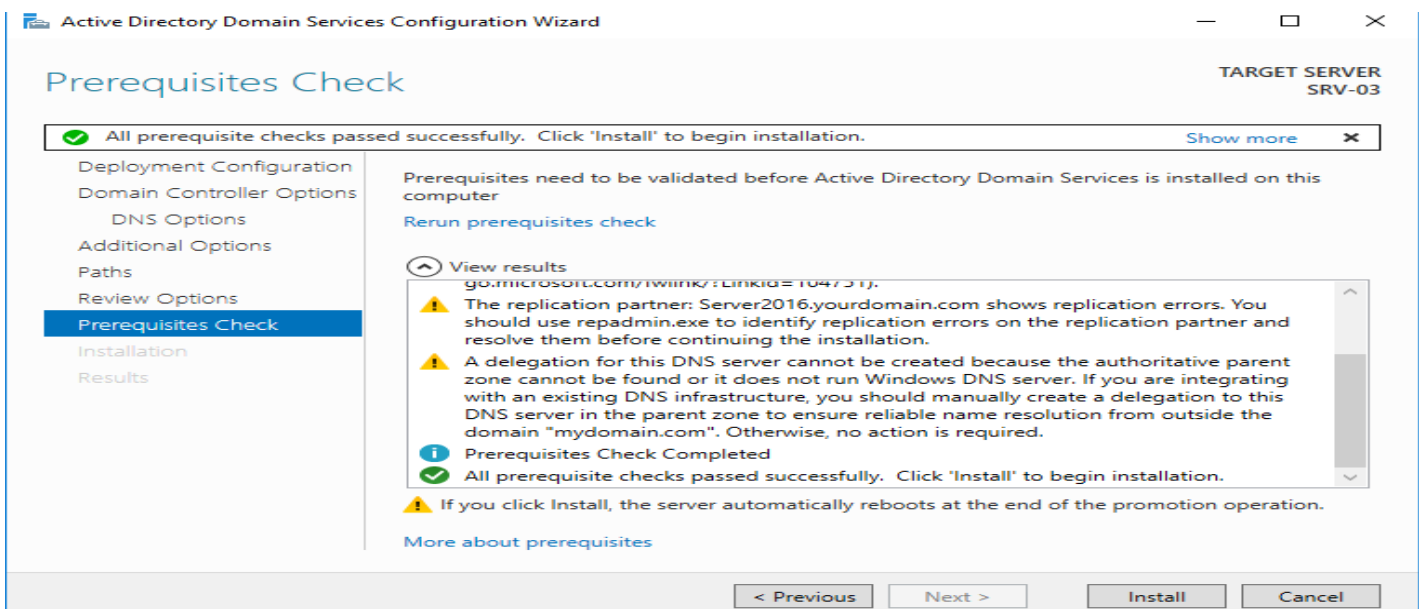


Click Next.





Click Install and wait for the configuration to finish. This may take several minutes to complete.



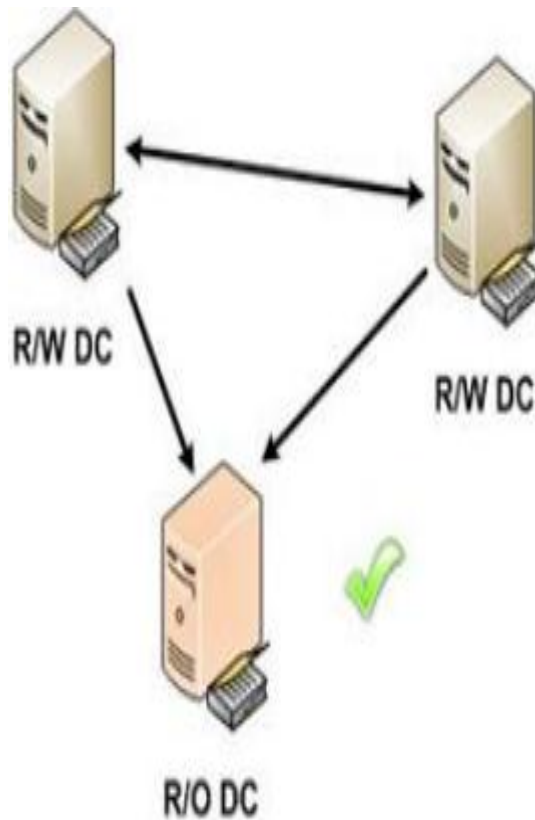
When you are done with configuration, the server will be rebooted automatically. After reboot, you can login with your domain admin account and start managing the new domain.

26-Read only domain controller

وحدة تحكم مجال للقراءة فقط (RODC) هو خادم يستضيف أقسام للقراءة فقط في قاعدة بيانات Active Directory ويستجيب لطلبات مصادقة الأمان.

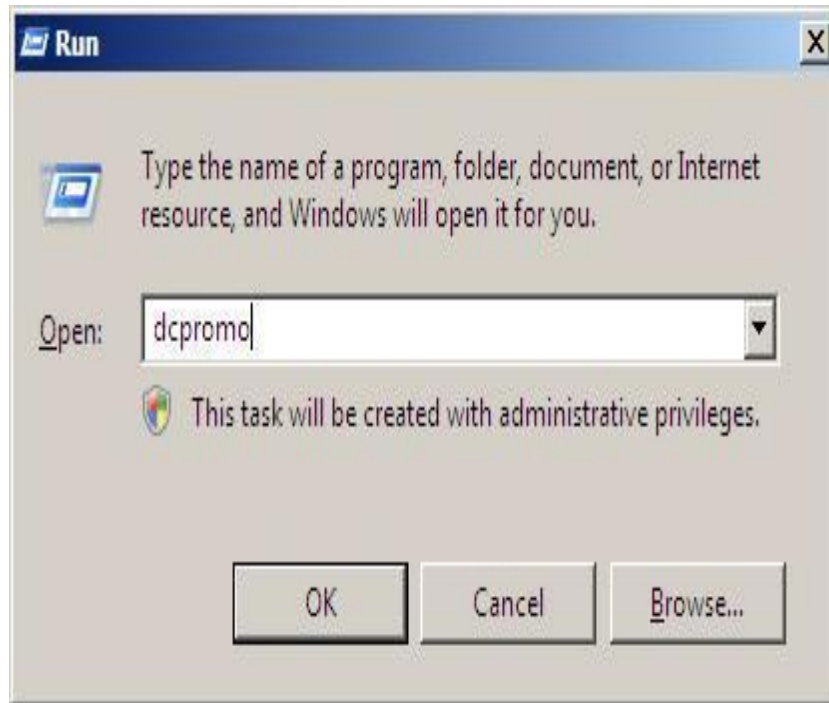
في وضع القراءة فقط ، يمكن لوحدة التحكم بالمجال الاستجابة للطلبات بسرعة أكبر نظرًا لأنه لا داعي للقلق بشأن معالجة التغييرات التي تحتاج إلى نسخها نسخًا متماثلًا إلى وحدات التحكم بالمجال الأخرى.

Why would you ever want to deploy RODCs? This domain controller mode is highly useful if you want to provide Active Directory authentication services in a location that is not adequately secure for a writable copy of your Active Directory database. Also, in read-only mode, the domain controller can respond to requests more quickly since it doesn't have to worry about processing changes that need to be replicated up to other domain controllers. It is also a good option if you have an application that performs best when installed on a domain controller. By running that application on an RODC rather than a regular domain controller, you don't run the risk that the DC will be inadvertently used by the application to make changes to your directory.

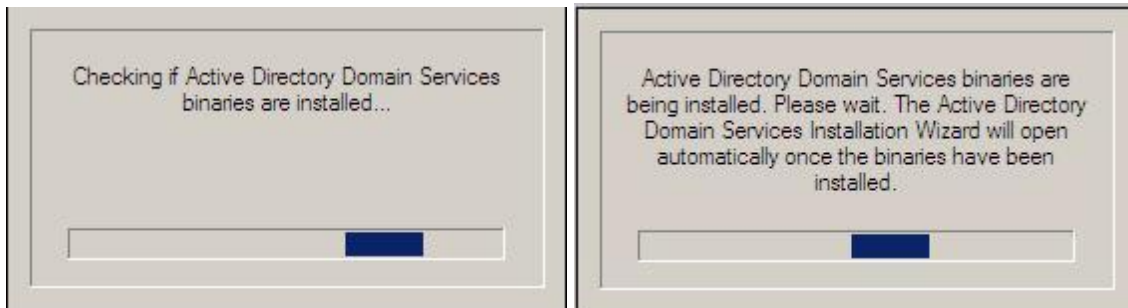


26.1- Read only domain controller in windows server 2008

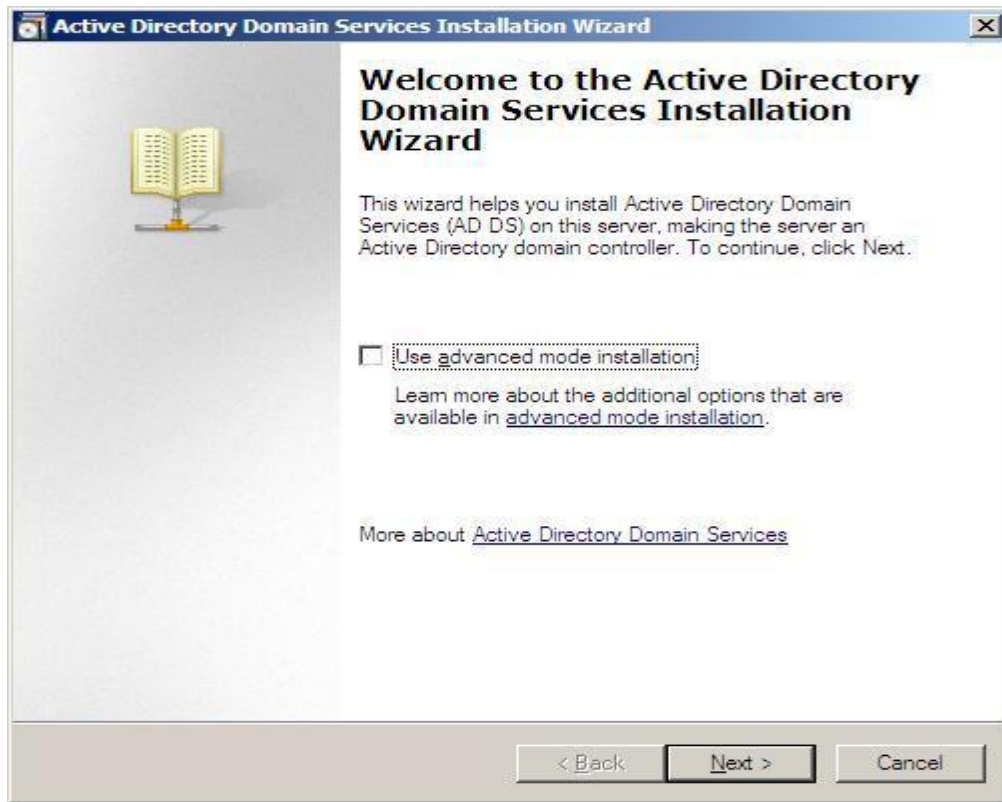
To set up an read only domain Controller, I will use the dcpromo.exe command. To use the command, click on Start > Run > and then write dcpromo > Click OK



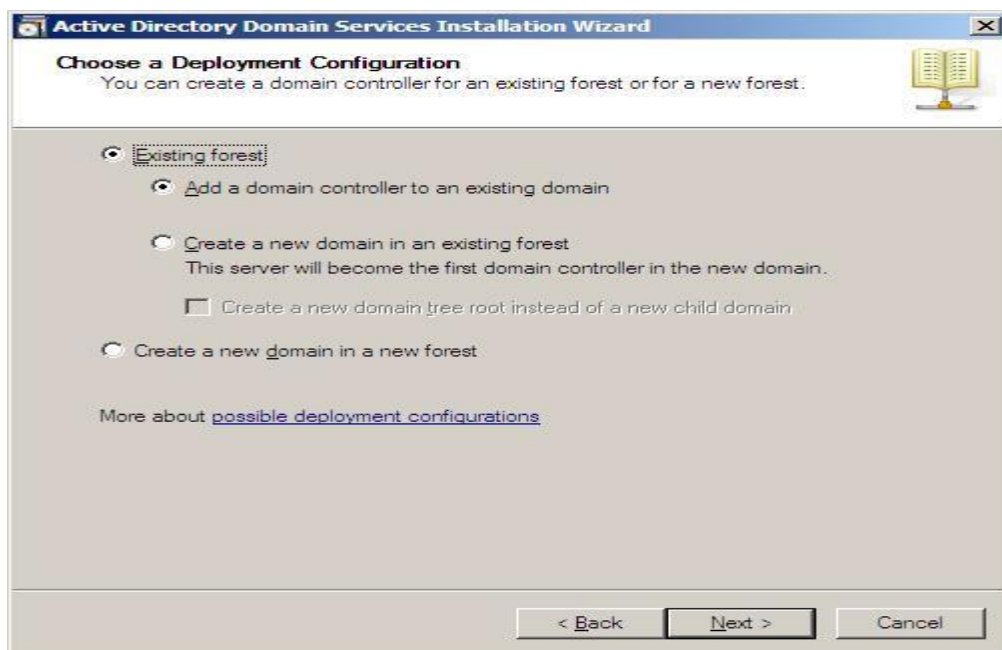
The system will start checking if Active Directory Domain Services (AD DS) binaries are installed, then will start installing them. The binaries could be installed if you had run the dcpromo command previously and then canceled the operation after the binaries were installed.



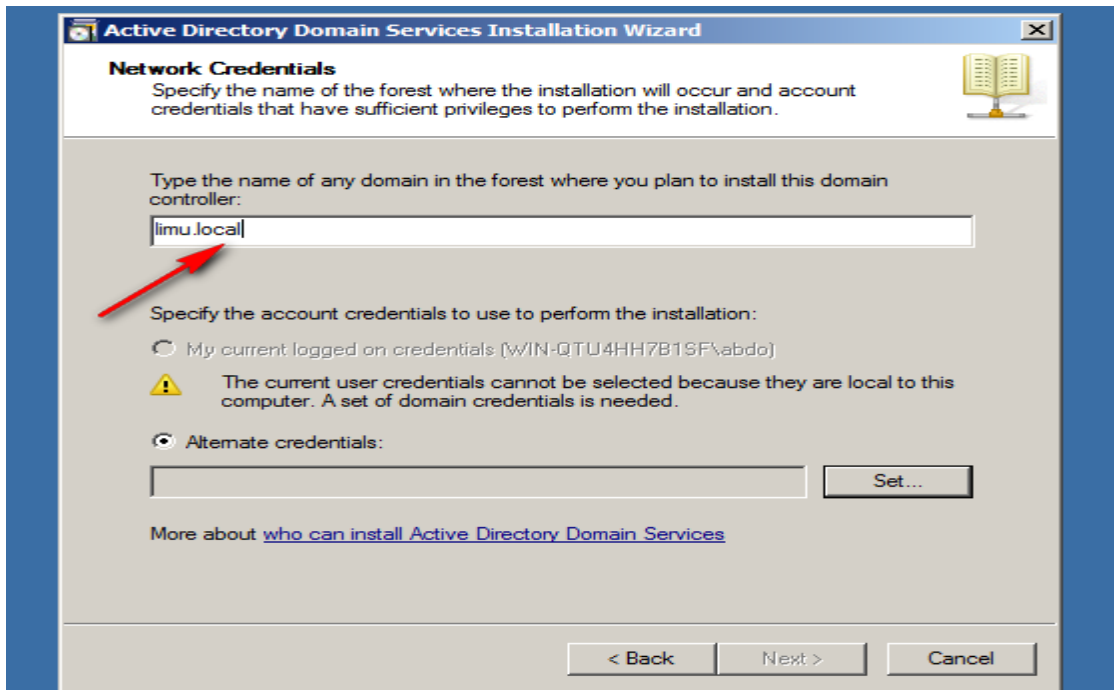
The Active Directory Domain Services Installation Wizard will start, either enable the checkbox beside Use Advanced mode installation and Click Next , or keep it unselected and click on Next



On the Choose a Deployment Configuration page, click Existing forest, click Add a domain controller to an existing domain, and then click Next.



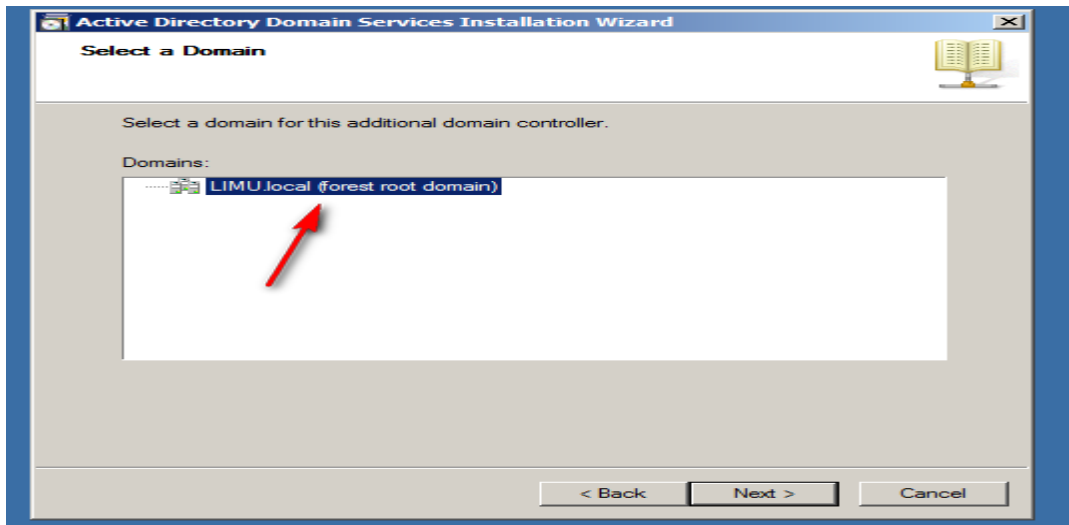
On the Network Credentials page, type your domain name, my domain name is elmajdal.net (was set in the previous article) , so I will type LIMU.local



Enter the credentials



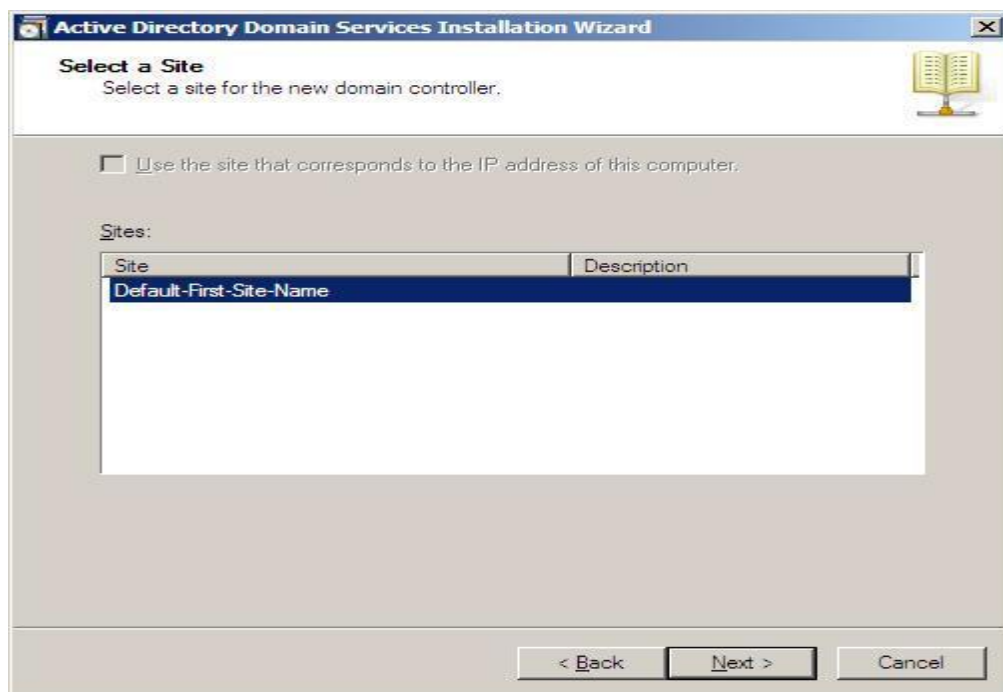
On the Select a Domain page, select the domain of the Additional Domain Controller, and then click Next, as I already have only one domain, then it will be selected by default



Select the site of domain controller

On the Select a Site page, either enable the checkbox beside Use the site that corresponds to the IP address of this computer, this will install the domain controller in the site that corresponds to its IP address, or select a site from the list and then click Next. If you only have one domain controller and one site, then you will have the first option grayed and the site will be selected by default as shown in the following image

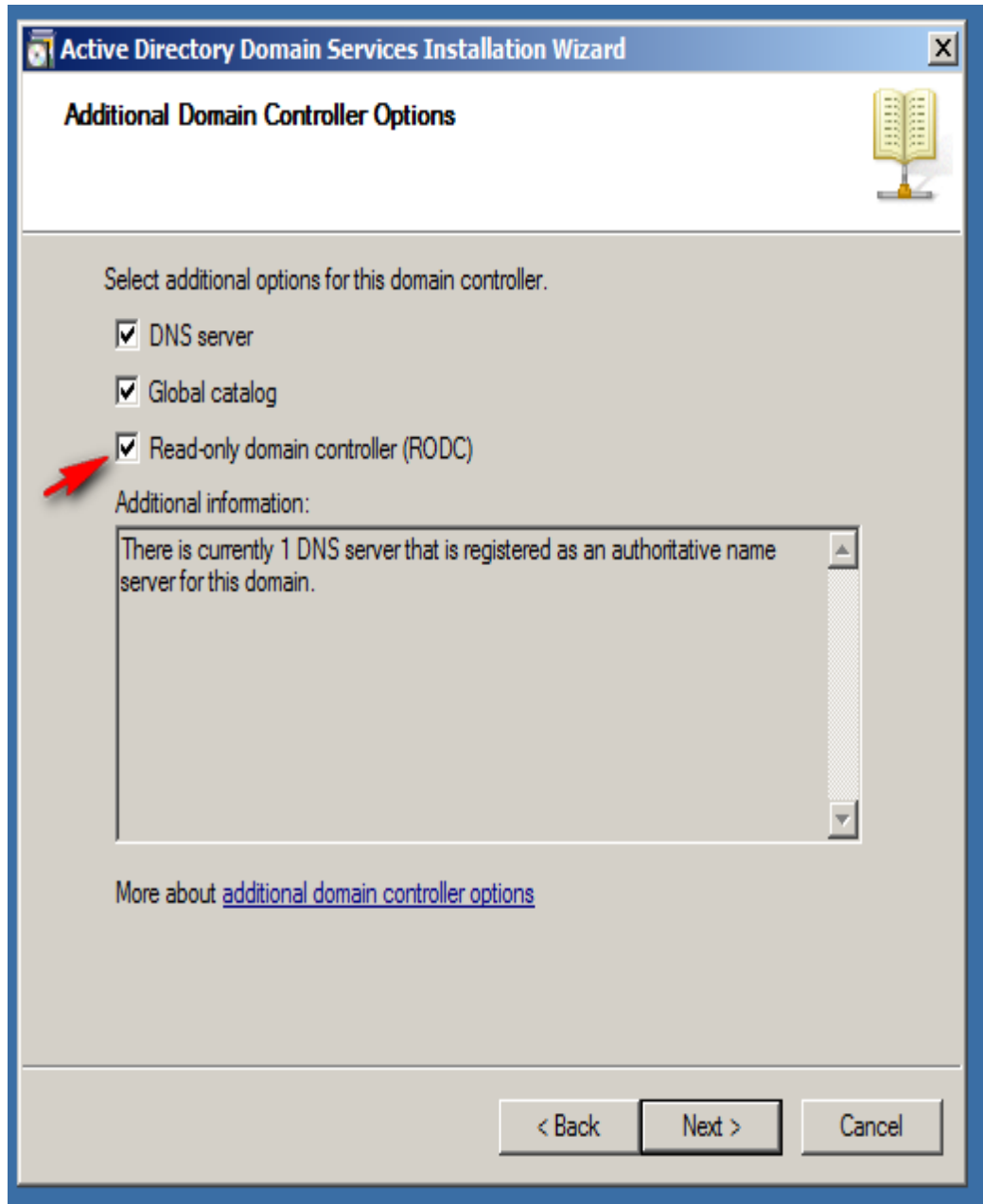
Select the site of domain controller



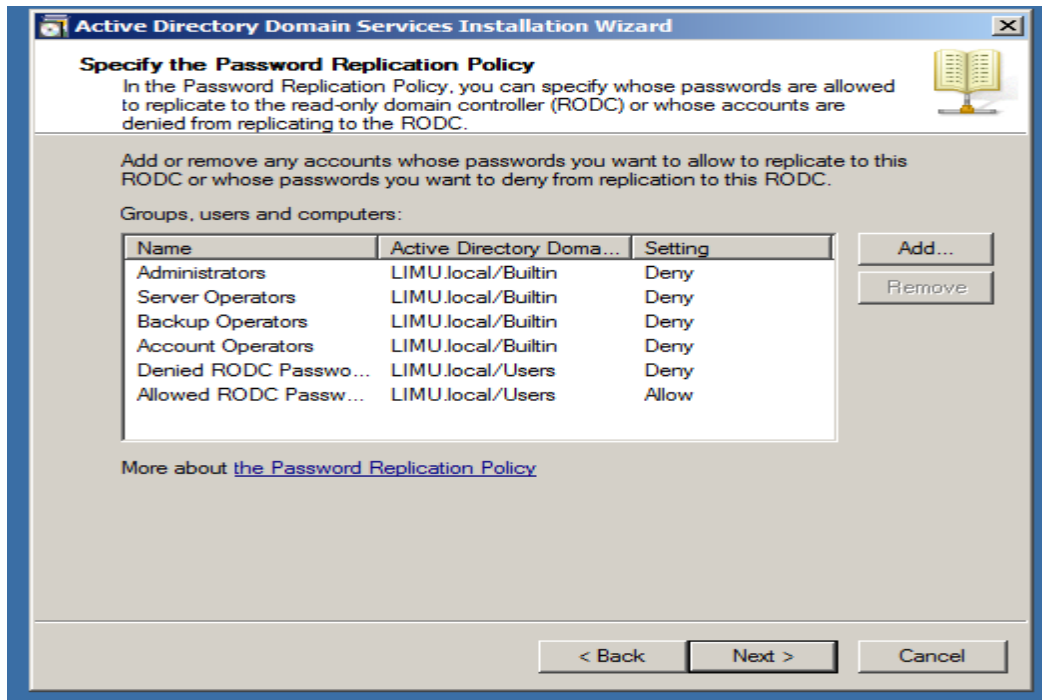
DNS and Global catalog

On the read only domain Controller Options page, By default, the DNS Server and Global Catalog checkboxes are selected. You can also select your additional domain controller to be a Read-only Domain Controller (RODC) by selecting the checkbox beside it.

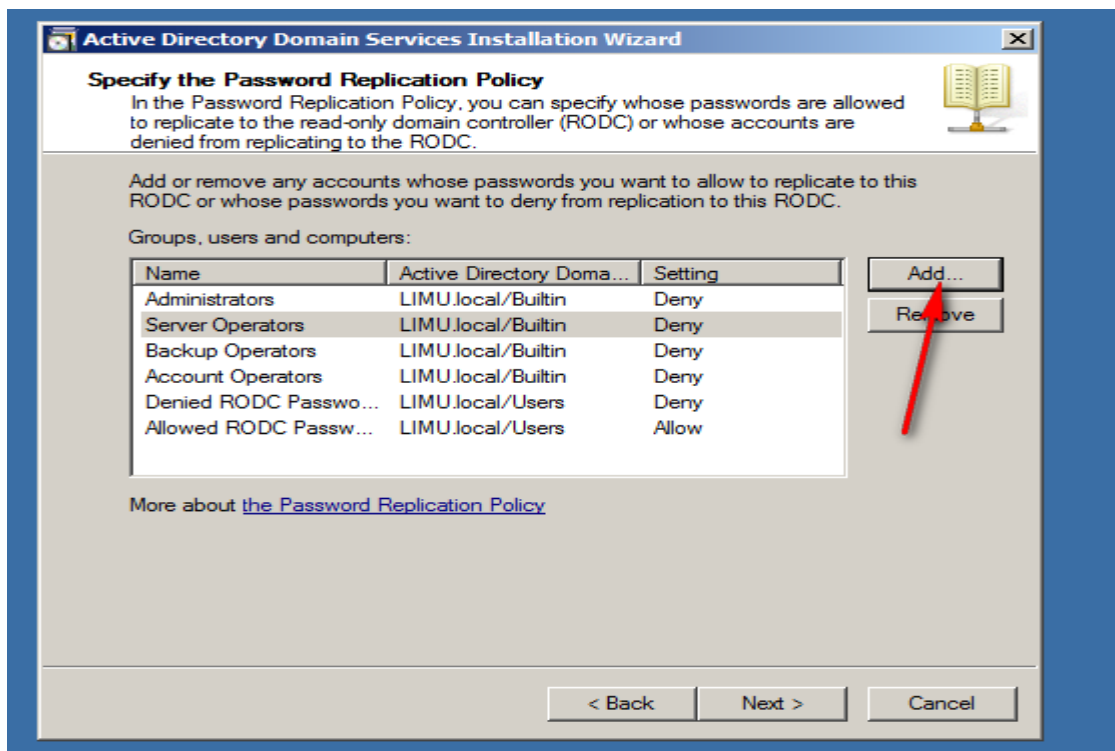
Read only domain controller



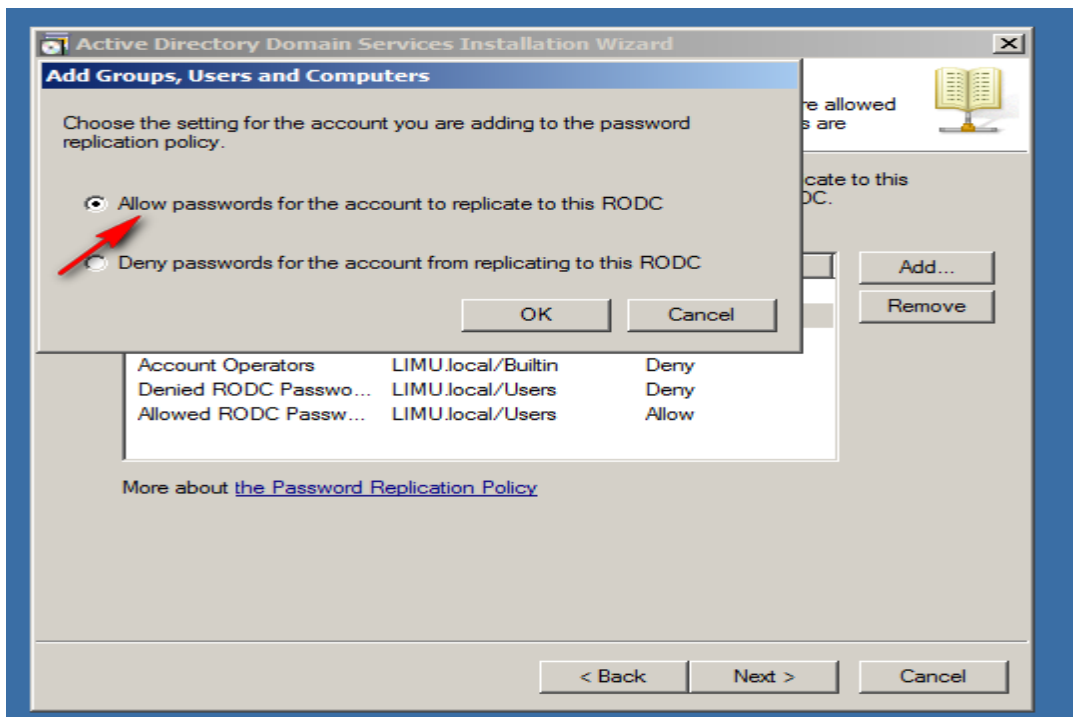
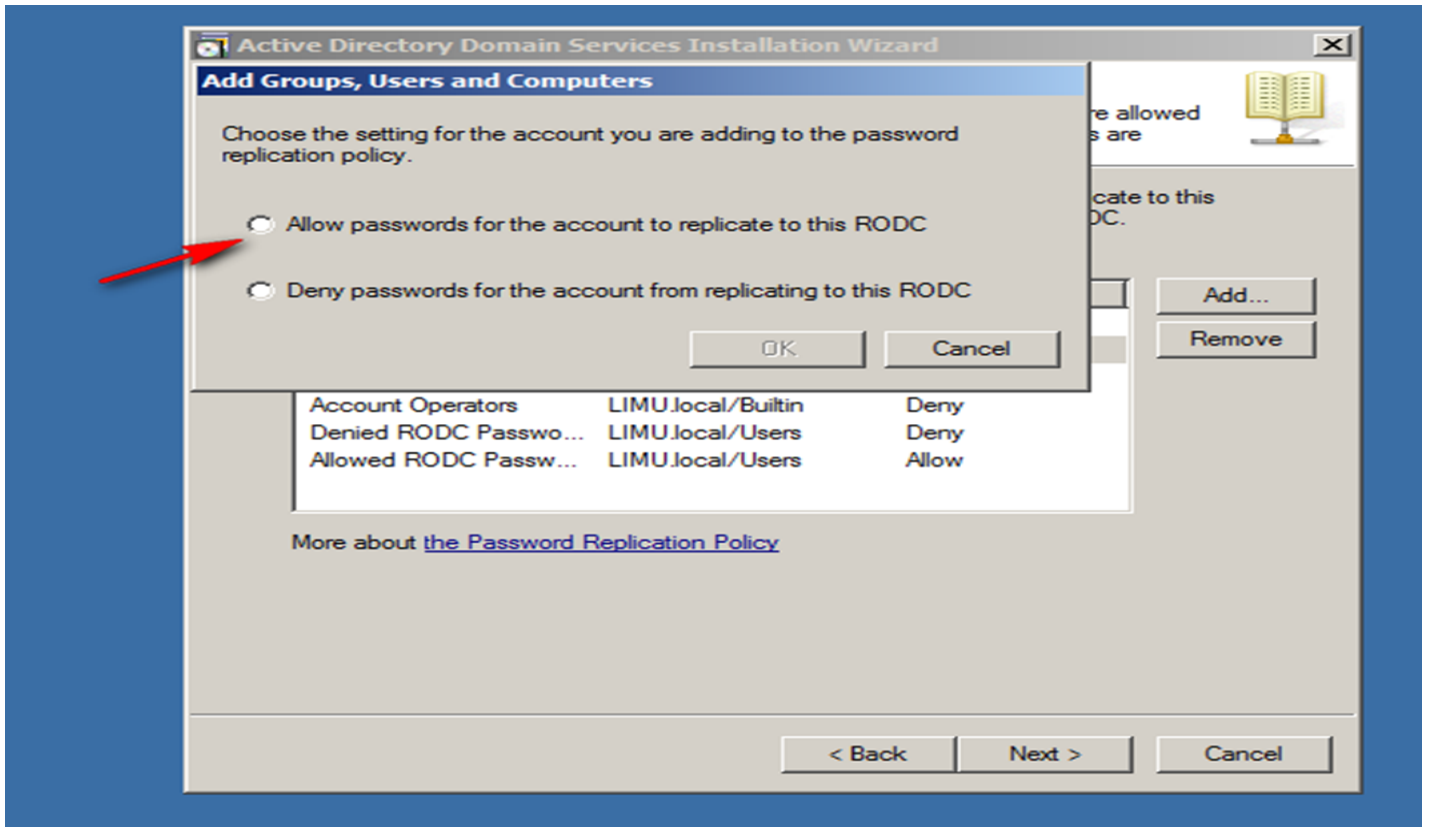
Specify the password replication

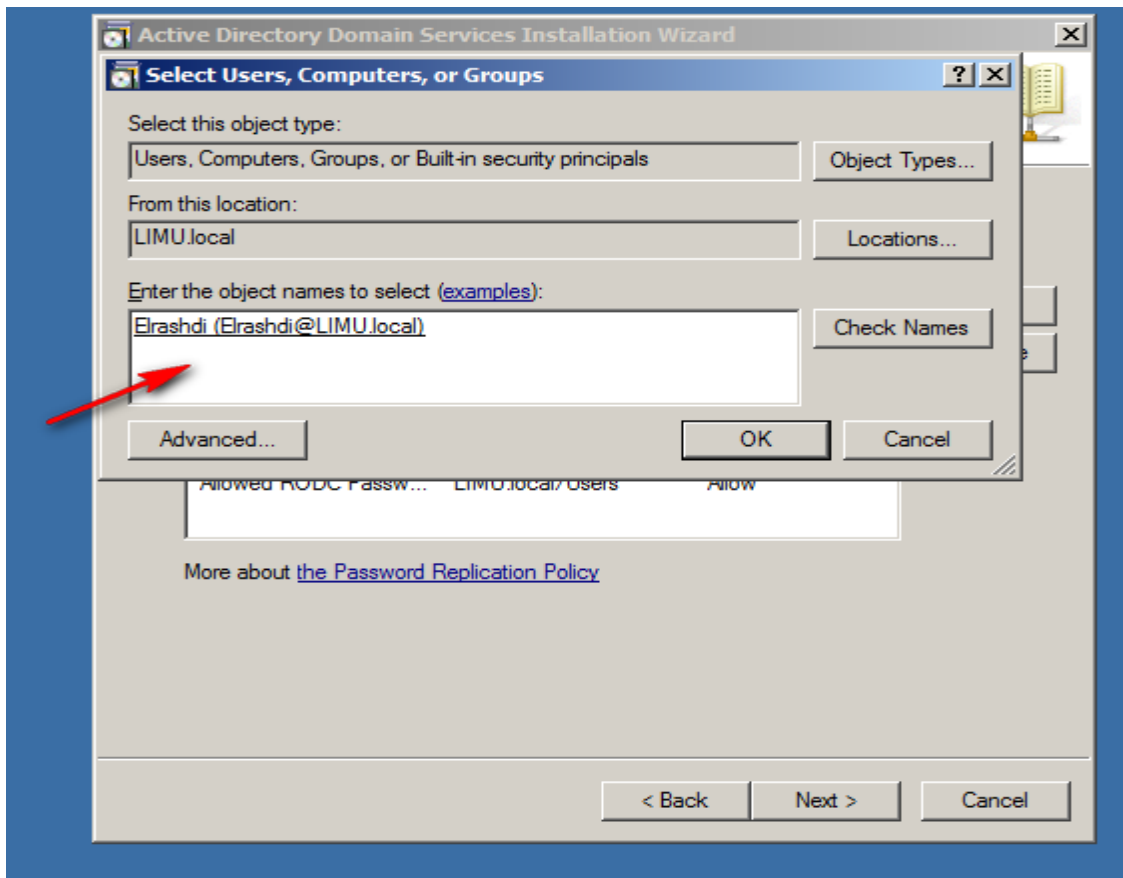
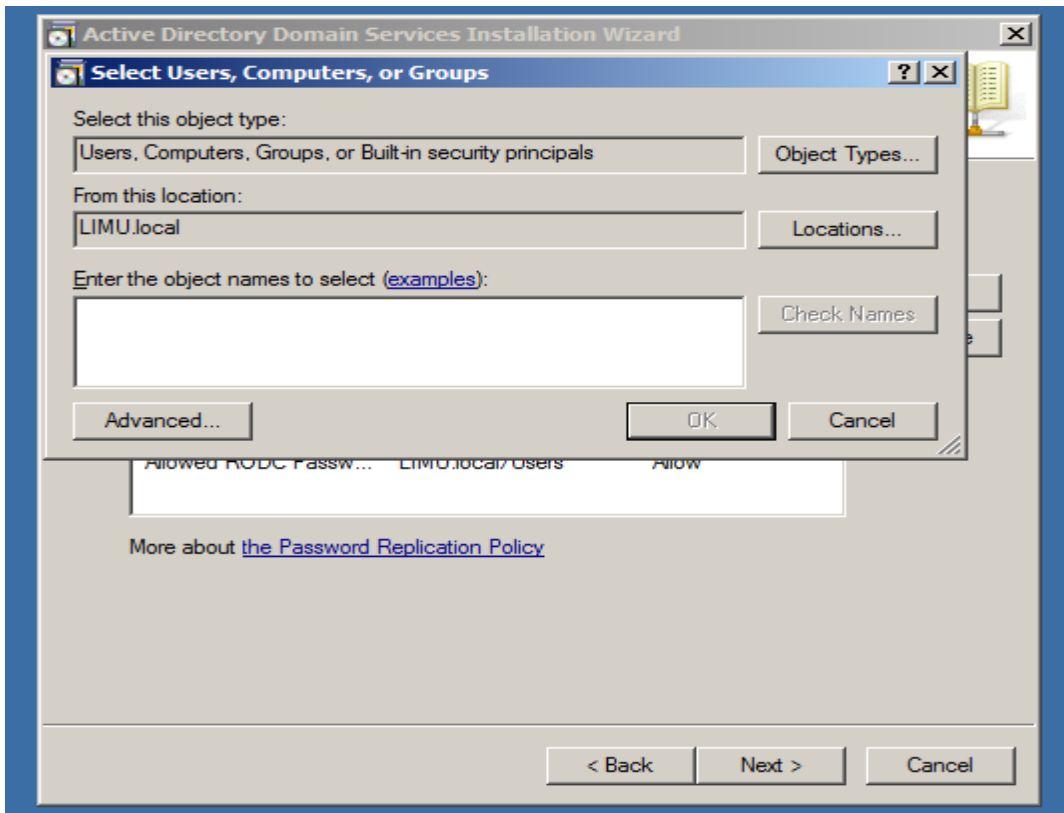


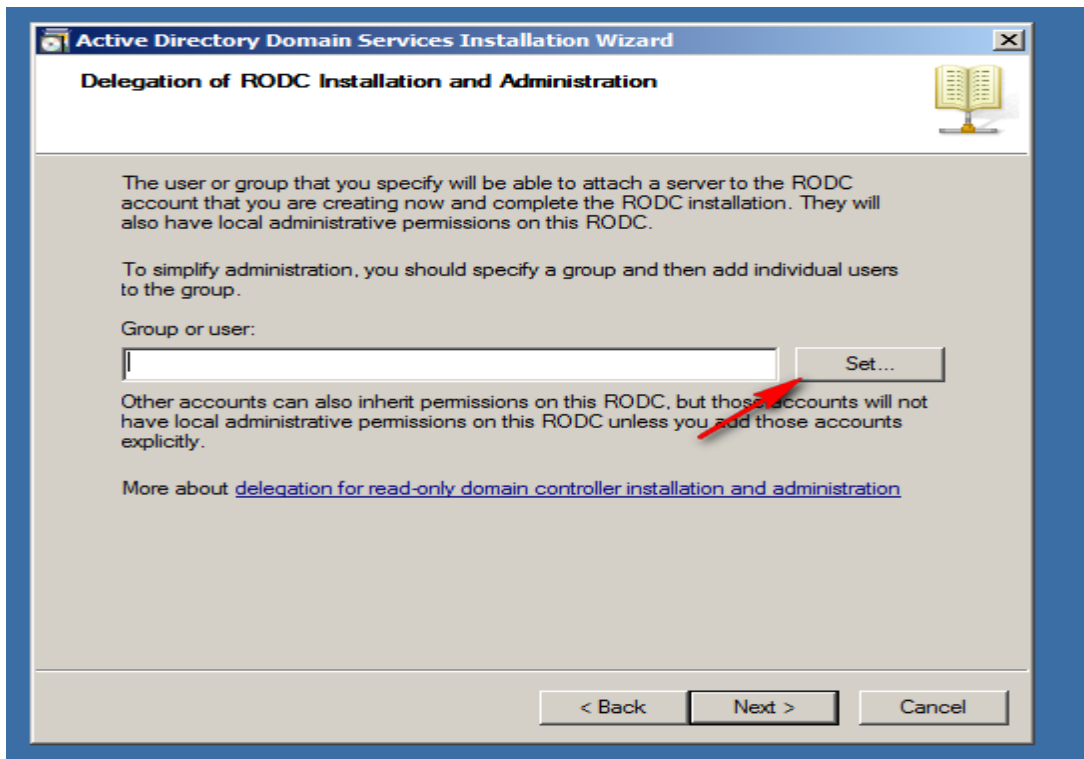
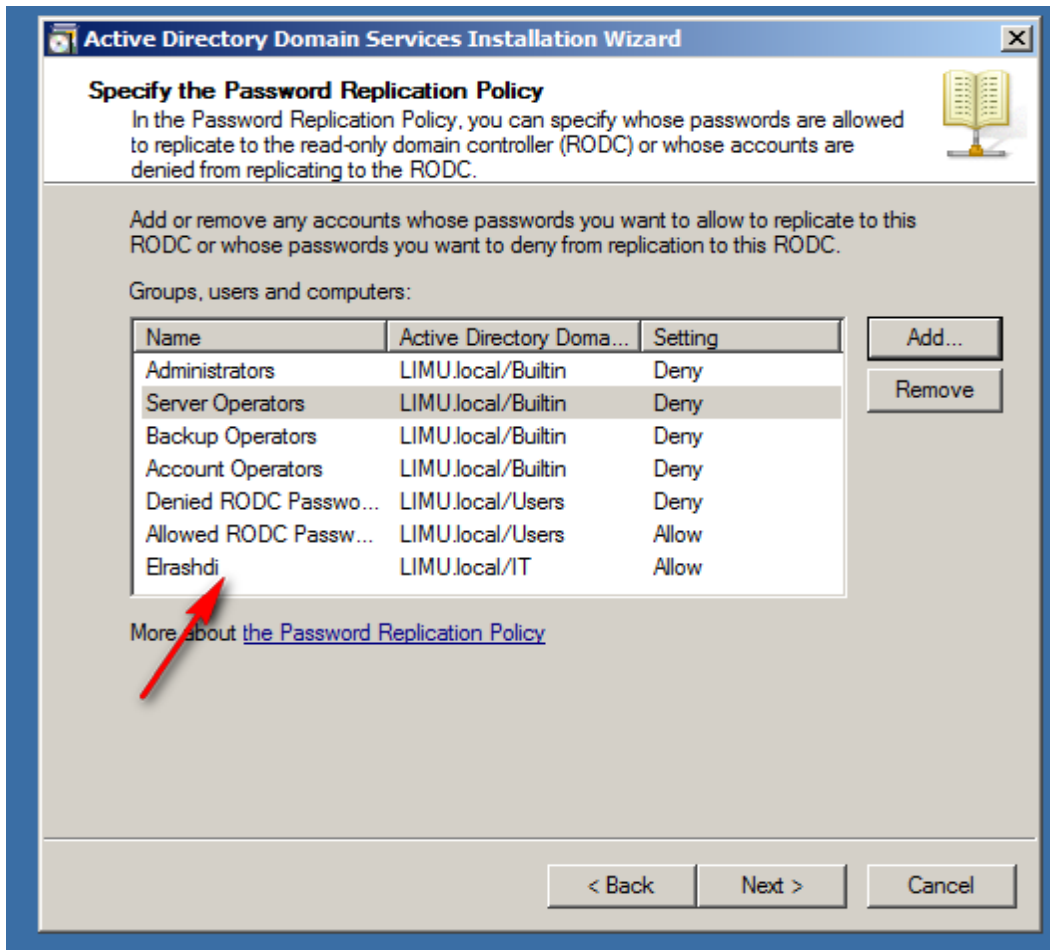
You can add specific user from original domain controller to read information from primal domain controller

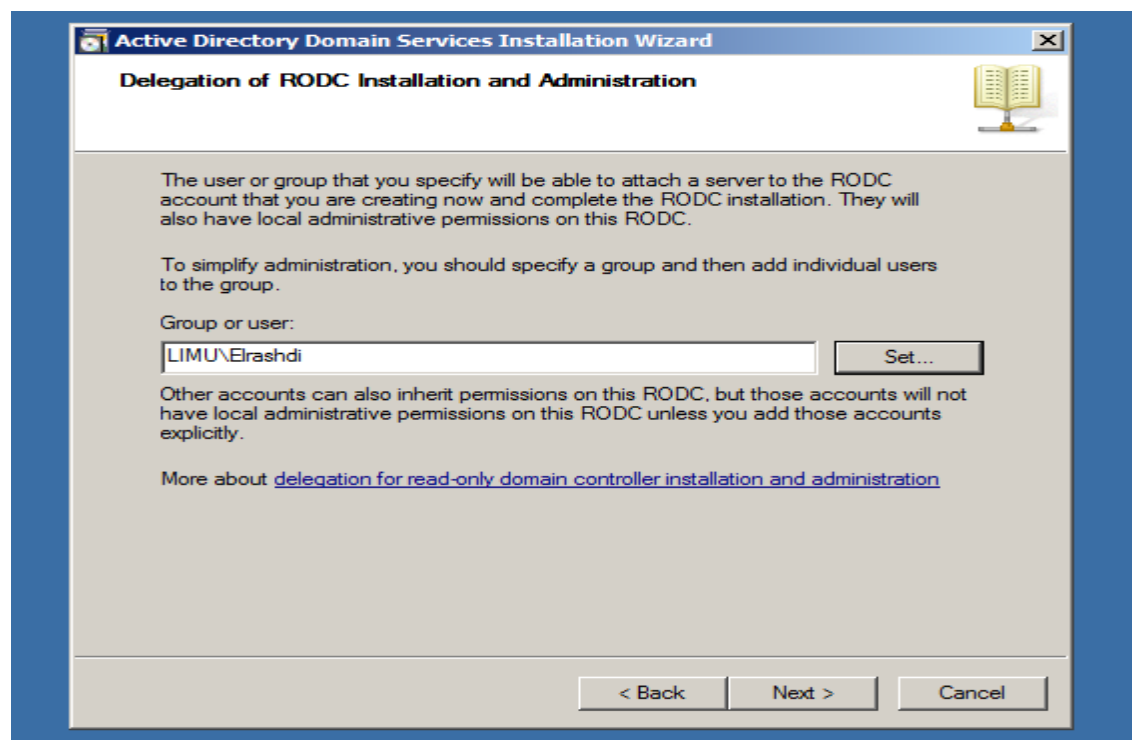
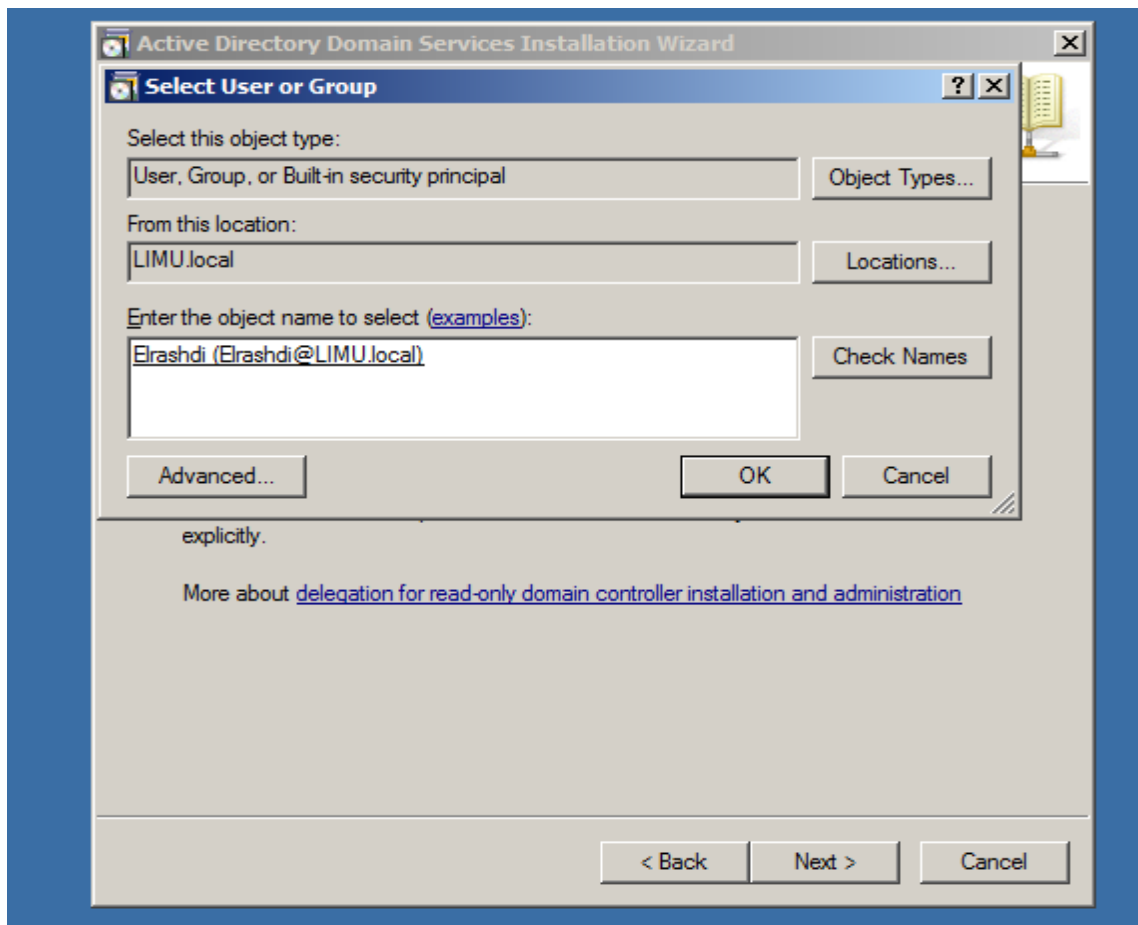


Select Specific user



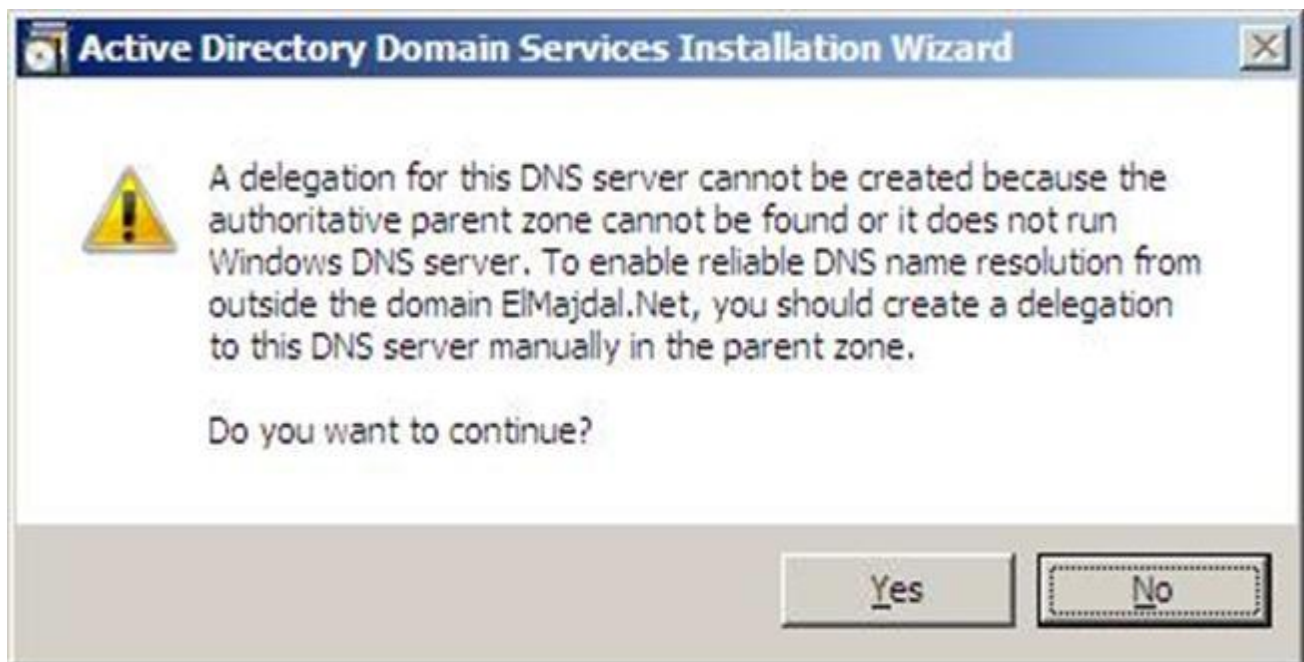






Select DNS

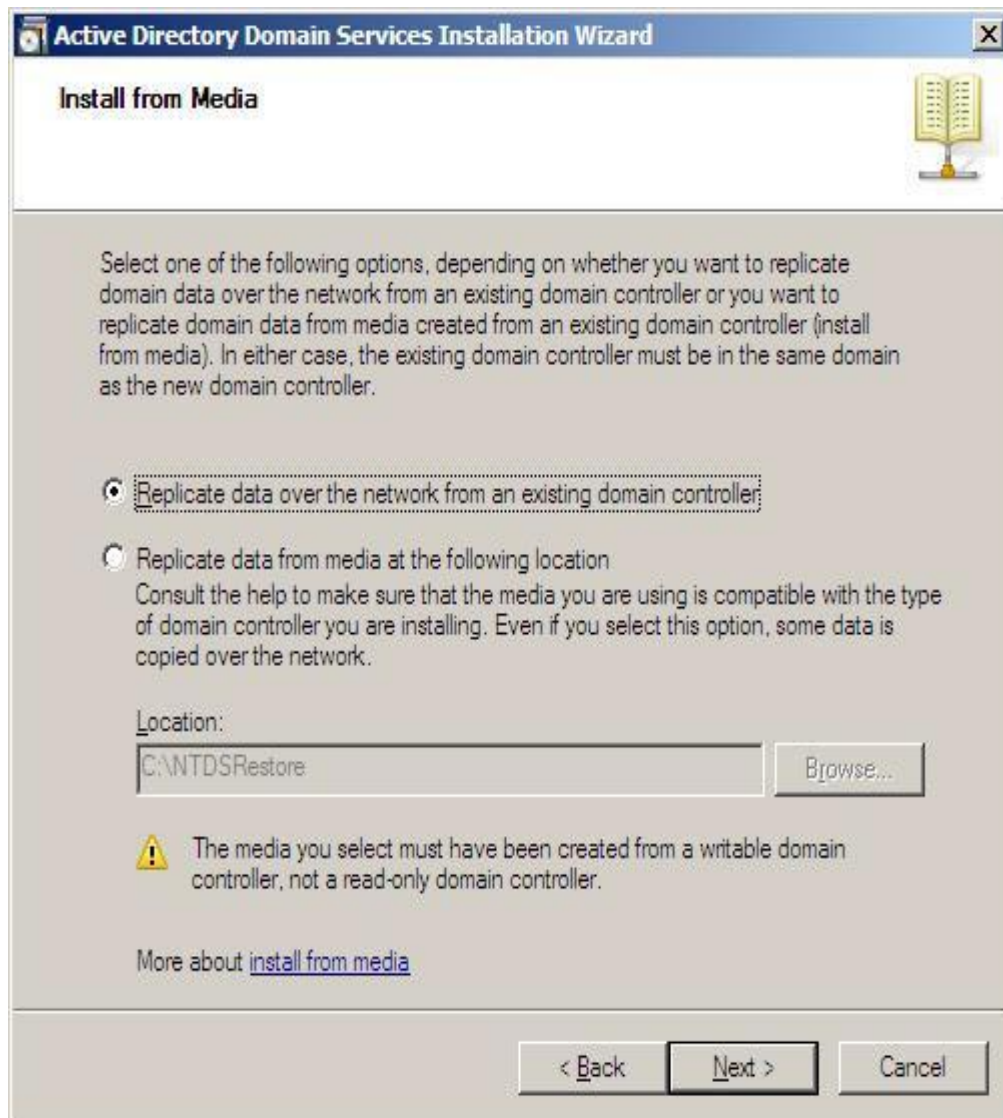
If you select the option to install DNS server in the previous step, then you will receive a message that indicates a DNS delegation for the DNS server could not be created and that you should manually create a DNS delegation to the DNS server to ensure reliable name resolution. If you are installing an additional domain controller in either the forest root domain (or a tree root domain) , you do not need to create the DNS delegation. In this case, you can safely ignore the message and click Yes.



Install from media

In the Install from Media page (will be displayed if you have selected Use advanced mode installation on the Welcome page, if you didn't select it, then skip to step # 15), you can choose to either replicate data over the network from an existing domain controller, or specify the location of installation media to be used to create the domain controller and configure AD DS. I want to replicate data over the network, so I will choose the first option > click Next

Install from media

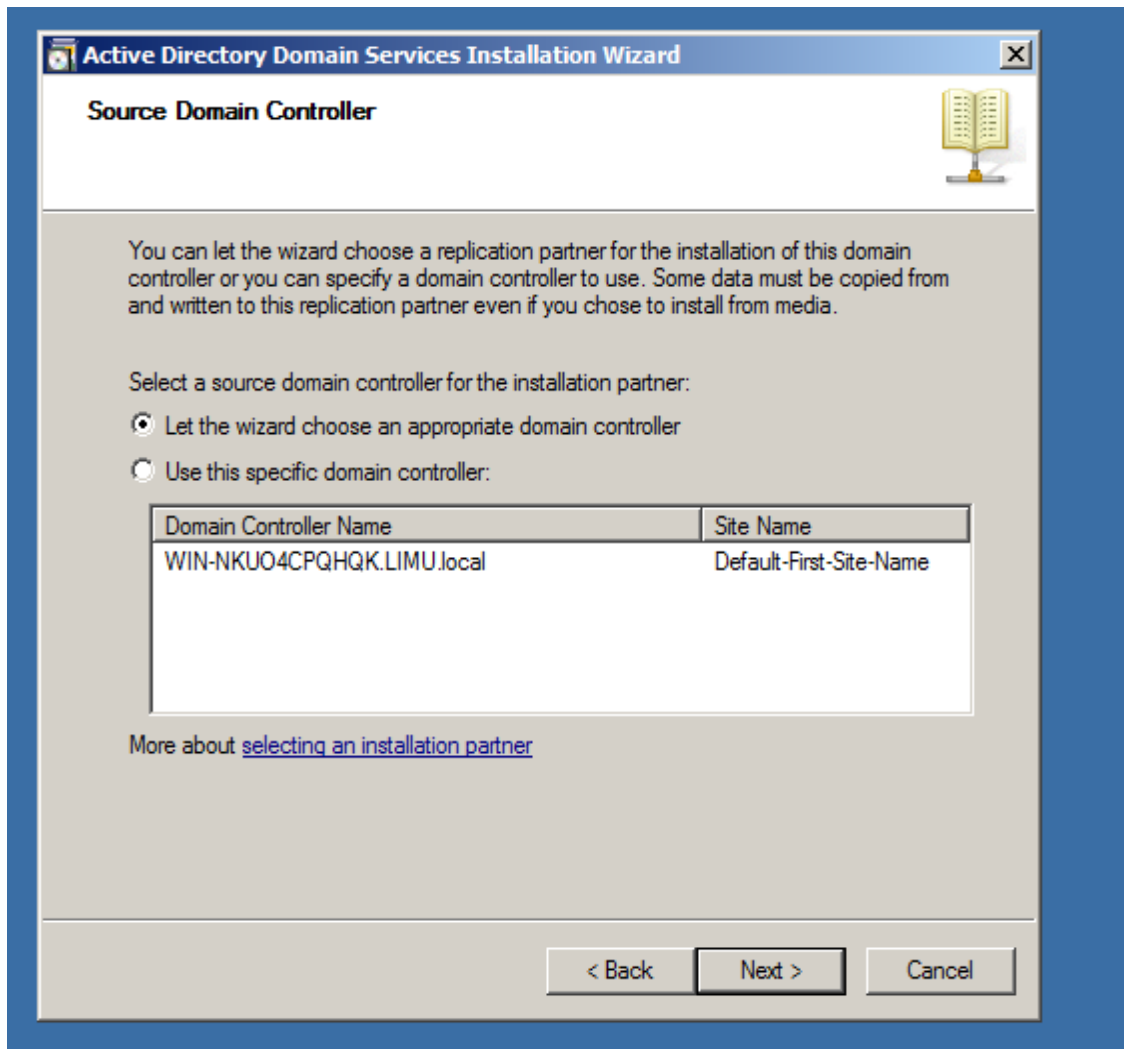


Select a source domain

On the Source Domain Controller page of the Active Directory Domain Services Installation Wizard, you can select which domain controller will be used as a source for data that must be replicated during installation, or you can have the wizard select which domain controller will be used as the source for this data. You have two options :

Let the wizard choose an appropriate domain controller Use this specific domain controller

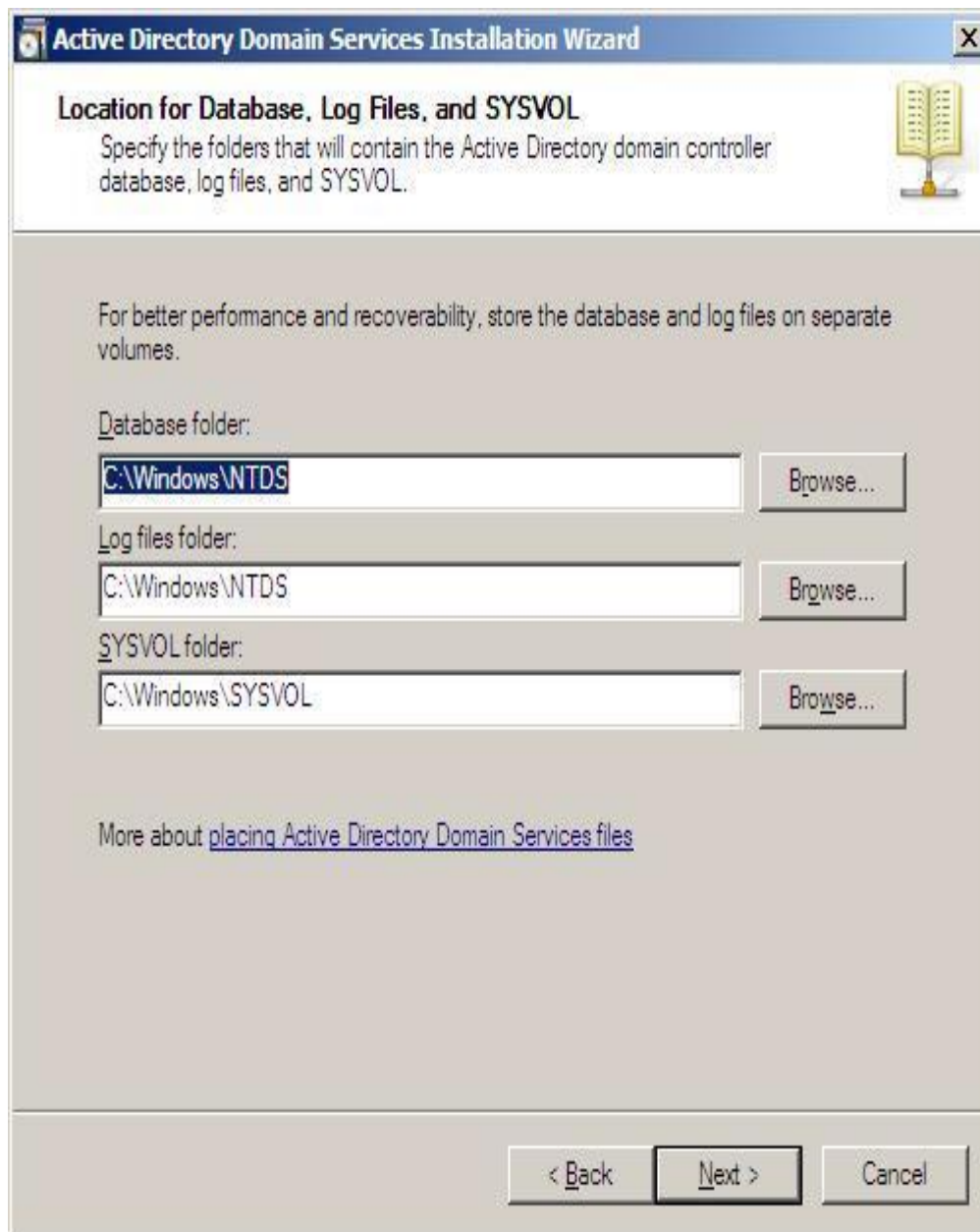
Select a source domain



Log file and sysvol

Now you will have to specify the location where the domain controller database, log files and SYSVOL are stored on the server. The database stores information about the users, computers and other objects on the network. the log files record activities that are related to AD DS, such information about an object being updated. SYSVOL stores Group Policy objects and scripts. By default, SYSVOL is part of the operating system files in the Windows directory Either type or browse to the volume and folder where you want to store each, or accept the defaults and click on Next

Finish installation



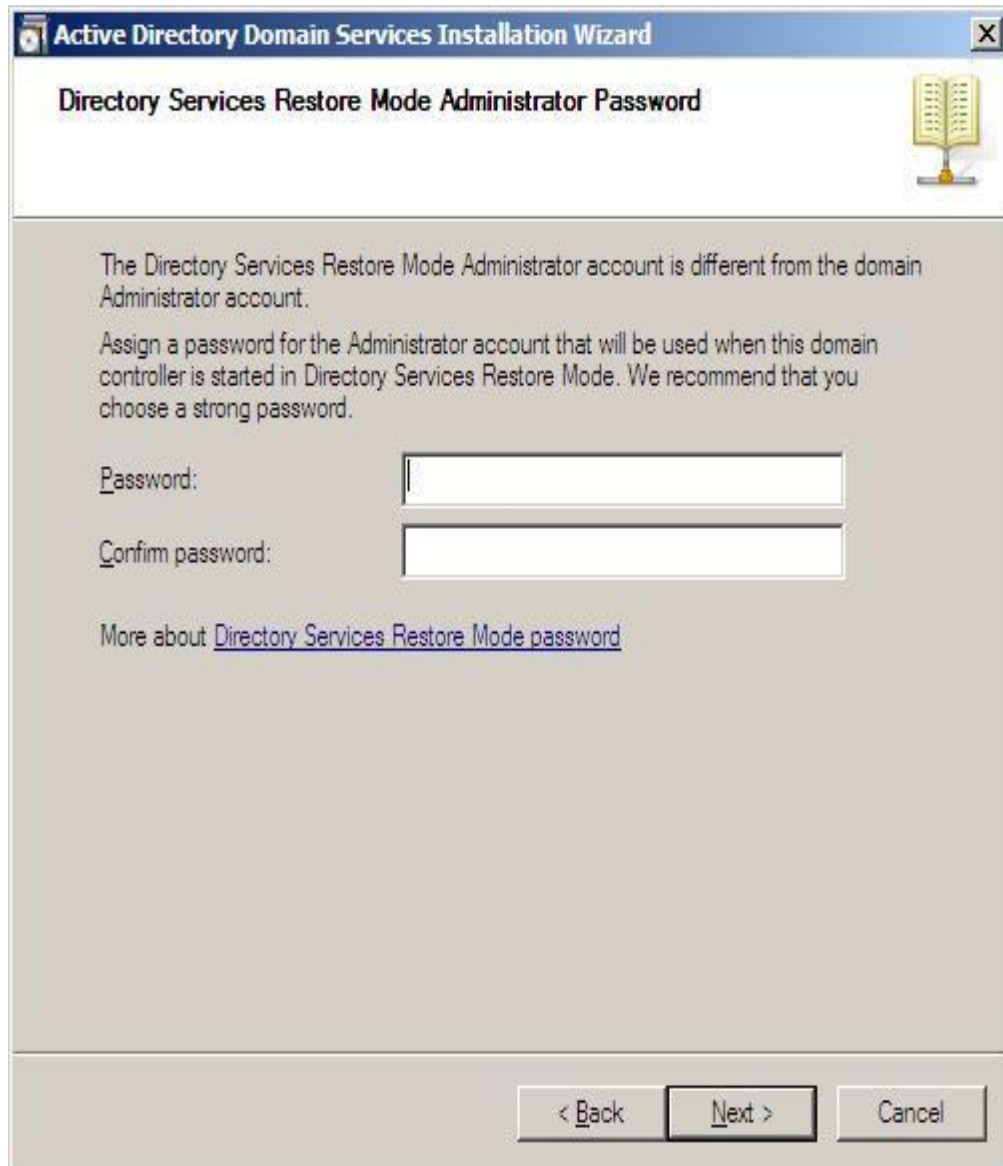
Backup and recovery

Note : Windows Server Backup backs up the directory service by volume. For backup and recovery efficiency, store these files on separate volumes that do not contain applications or other nondirectory files.

- In the Directory Services Restore Mode Administrator Password (DSRM) page, write a password and confirm it. This password is used when the domain controller is started in Directory Services

Restore Mode, which might be because Active Directory Domain Services is not running, or for tasks that must be performed offline.

Backup and recovery



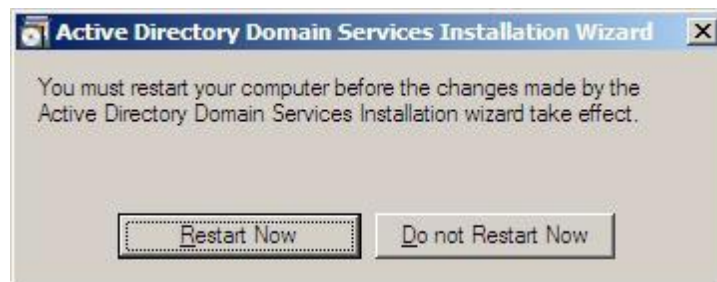
The screenshot shows a Windows wizard window titled "Active Directory Domain Services Installation Wizard". The current step is "Directory Services Restore Mode Administrator Password". The window contains the following text: "The Directory Services Restore Mode Administrator account is different from the domain Administrator account. Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password." Below this text are two input fields: "Password:" and "Confirm password:". At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

Finish installation

Summary page will be displayed showing you all the setting that you have set . It gives you the option to export the setting you have setup into an answer file for use to automate subsequent AD DS operations, if you wish to have such file, click on the Export settings button and save the file. Then click Next to begin AD DS installation

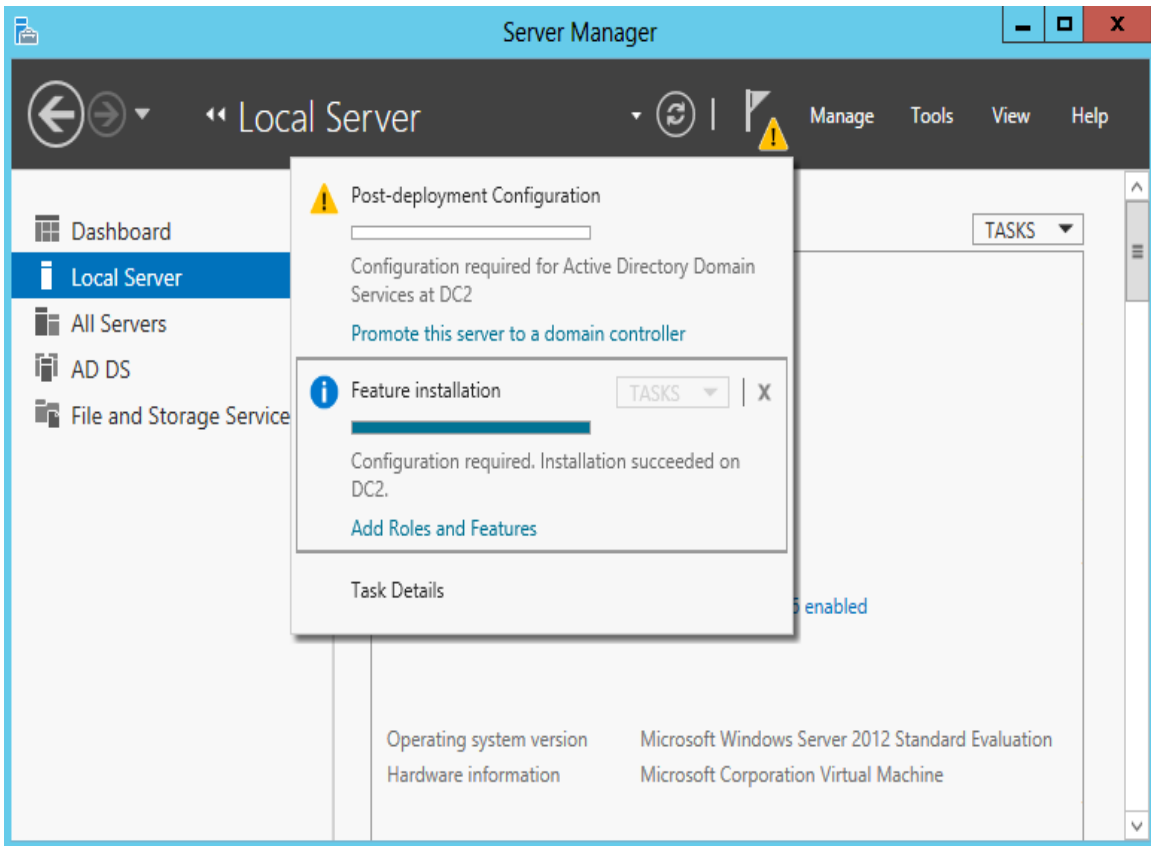
Finish installation

Active Directory Domain Services installation will be completed, click Finish, then click on Restart Now to restart your server for the changes to take effect

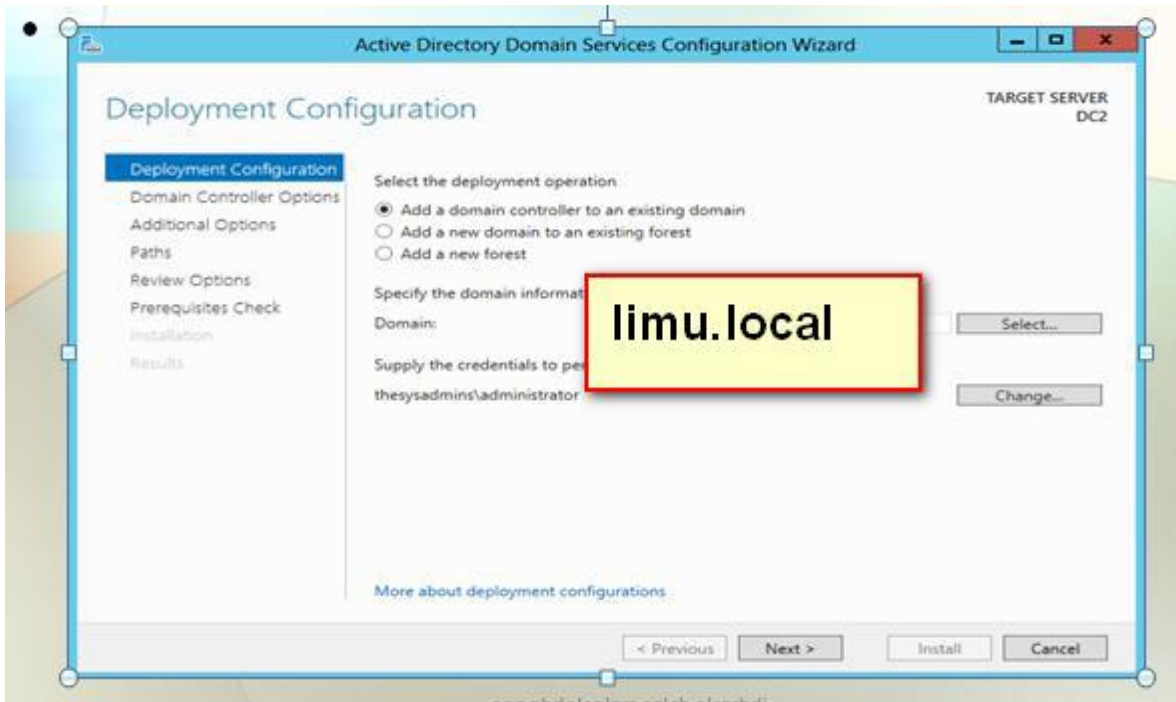


26.2- Read only domain control in windows server 2012

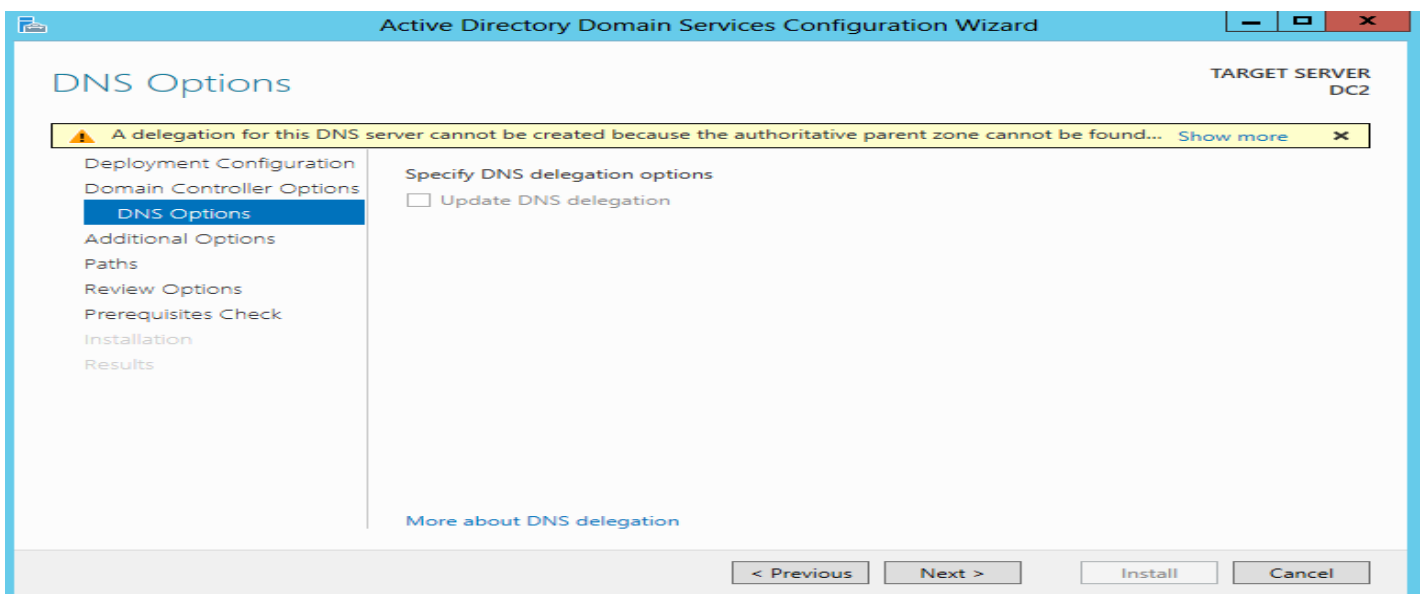
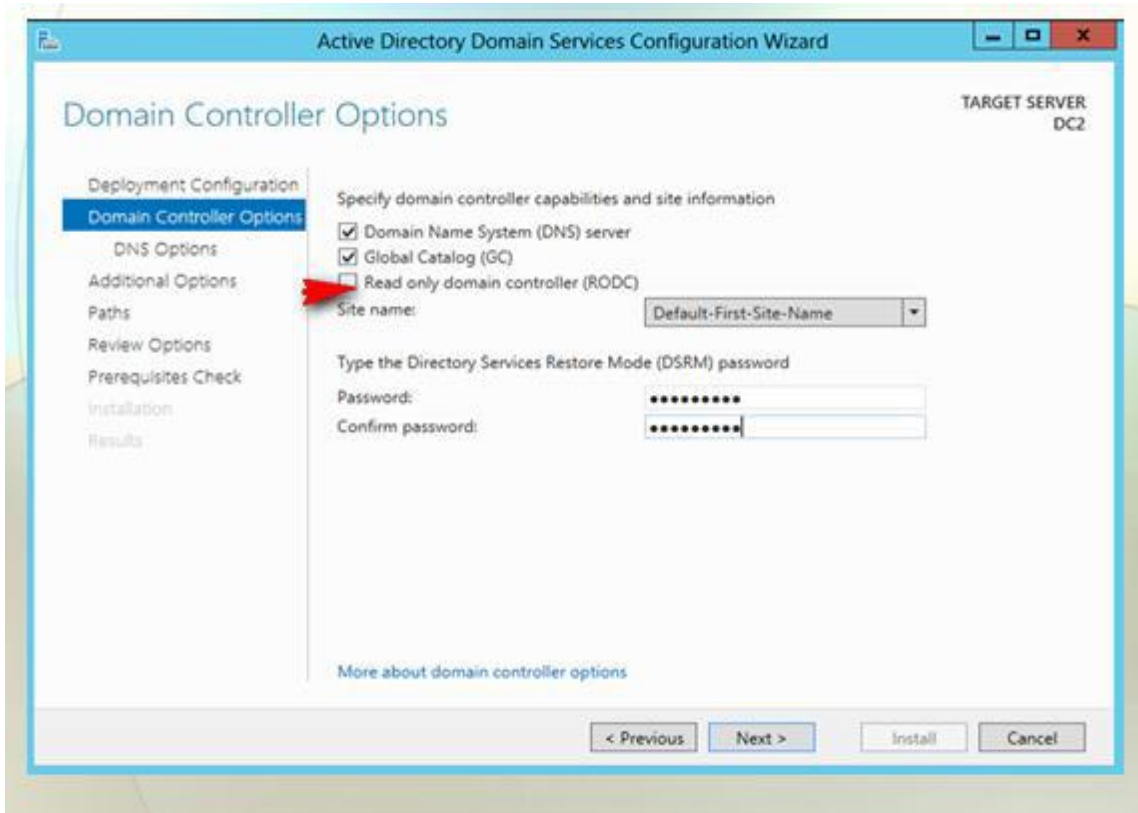
You'll now notice you have a notification, prompting you to promote this server to a domain controller.



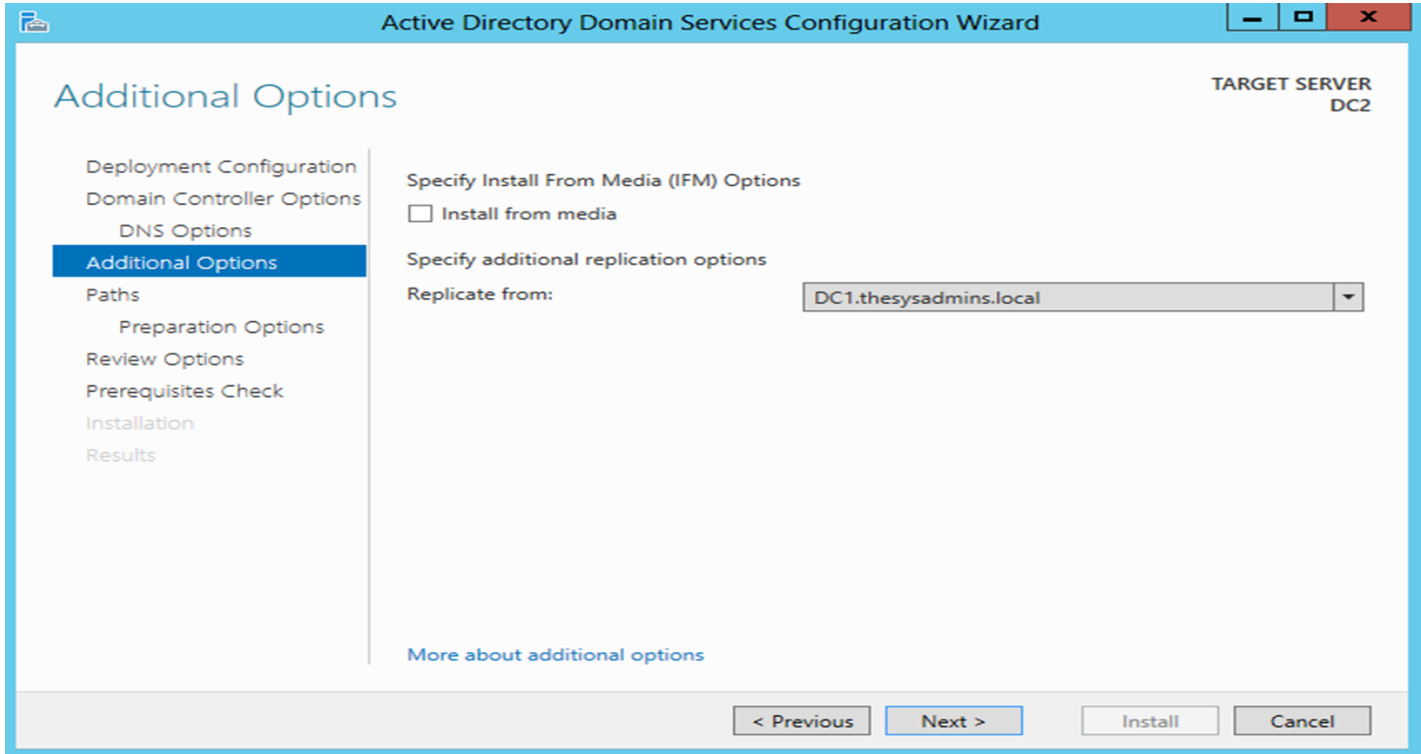
We are adding a domain controller to an existing domain, specify the domain and domain administrator credentials



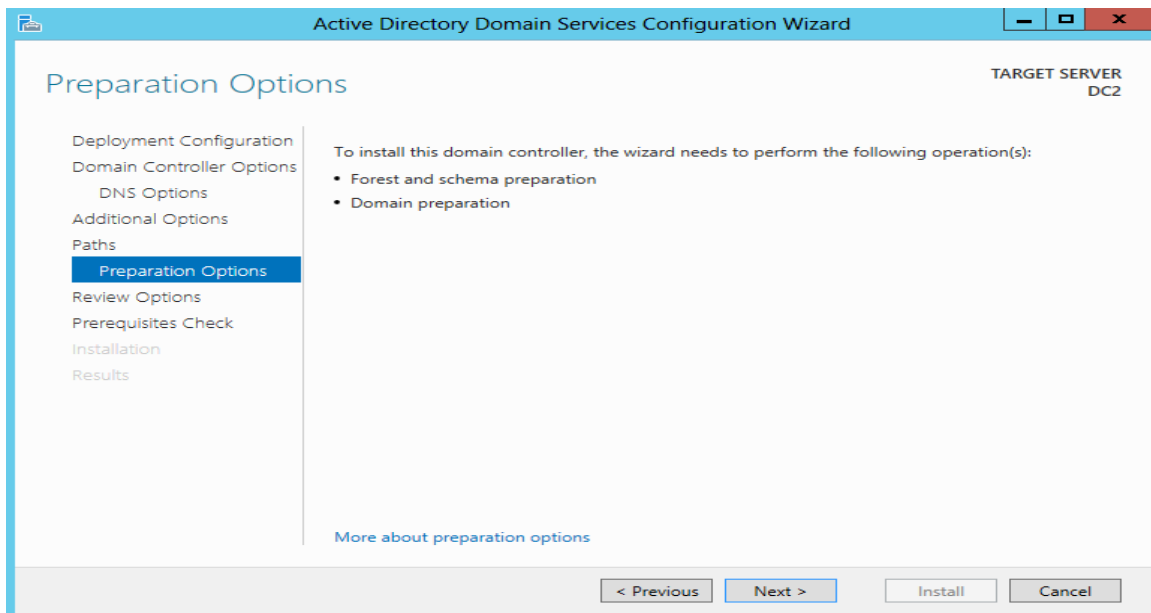
It will make the read only DC a DNS and GC by default, we do not want to make this a Read Only Domain Controller. You have the option to add the DC to a particular Site. Enter your DSRM password (as usual, keep this safe!).



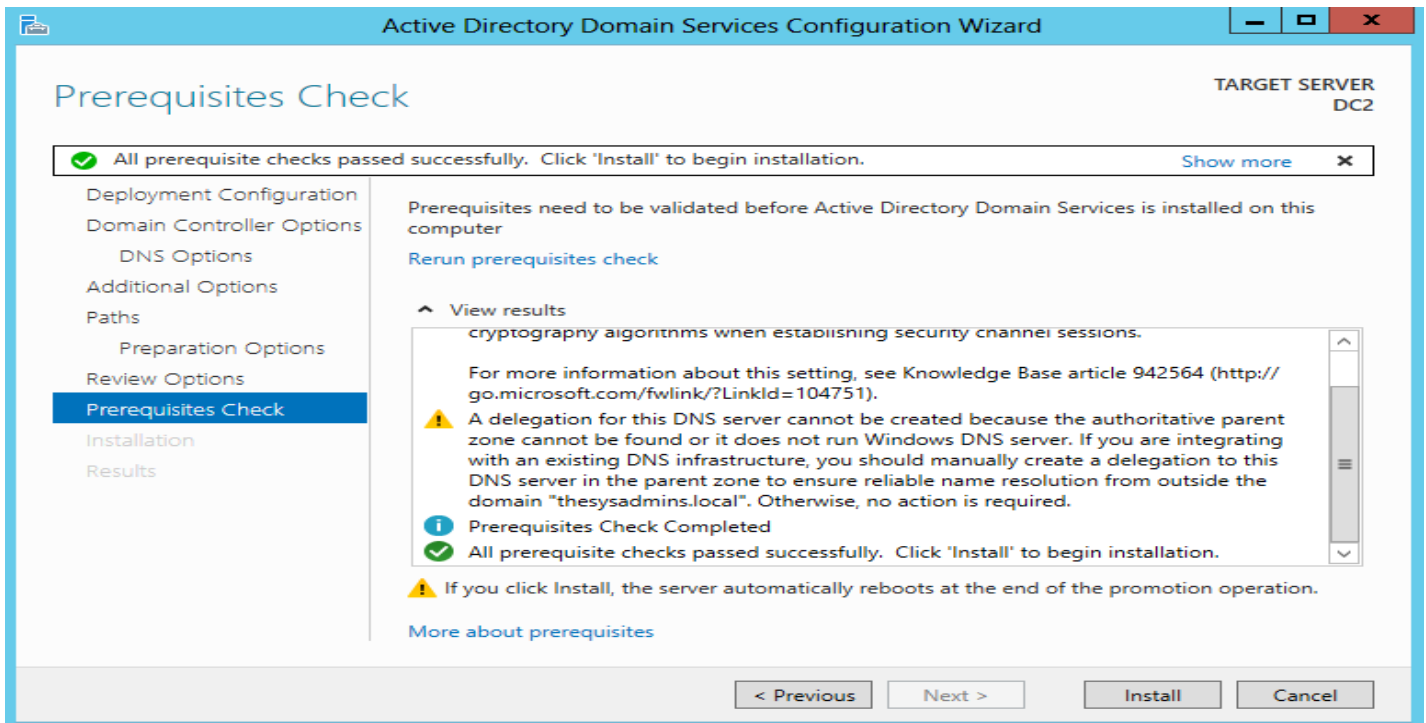
You can install from Media, which is useful if you are promoting a DC in a branch office with a poor connection- it will significantly reduce the initial Active Directory replication. You can specify a particular DC for the initial replication.



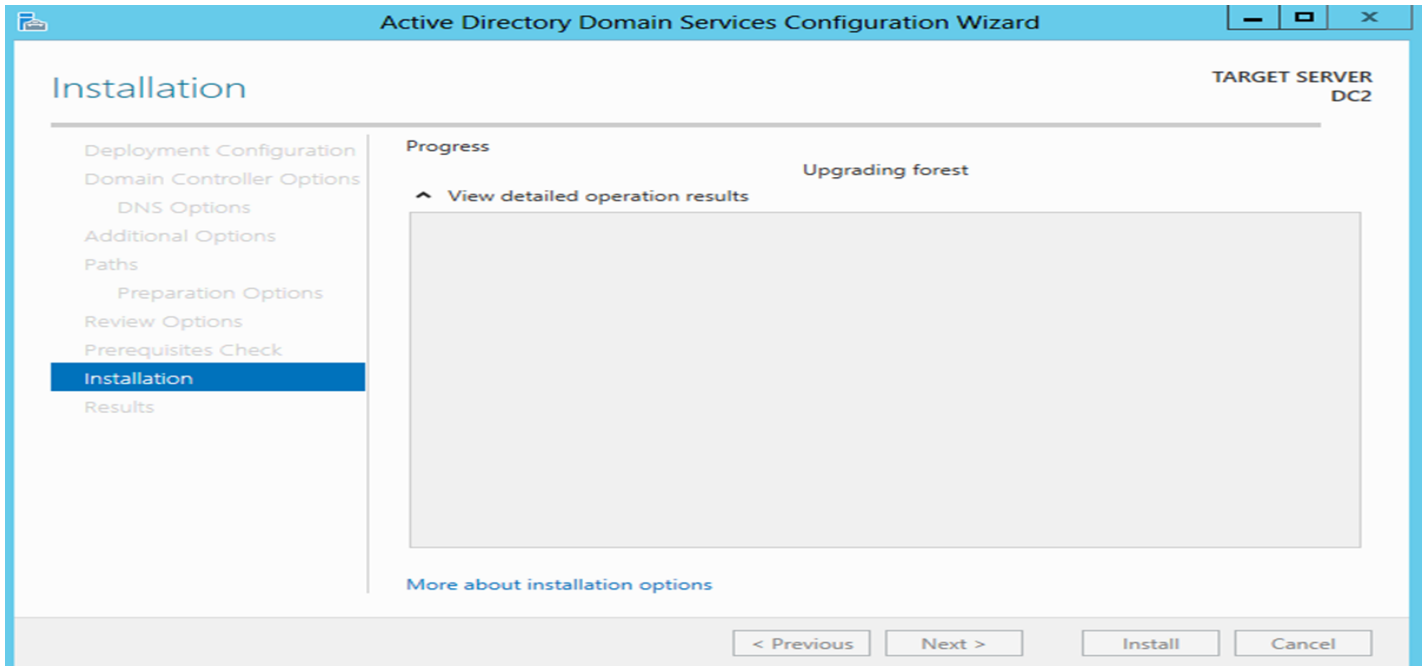
This screen tells us it will prepare the Forest, Schema and domain for us (Server 2012 uses Schema Version).



Click Install.



The install will tick over and when it has finished the server will be restarted.



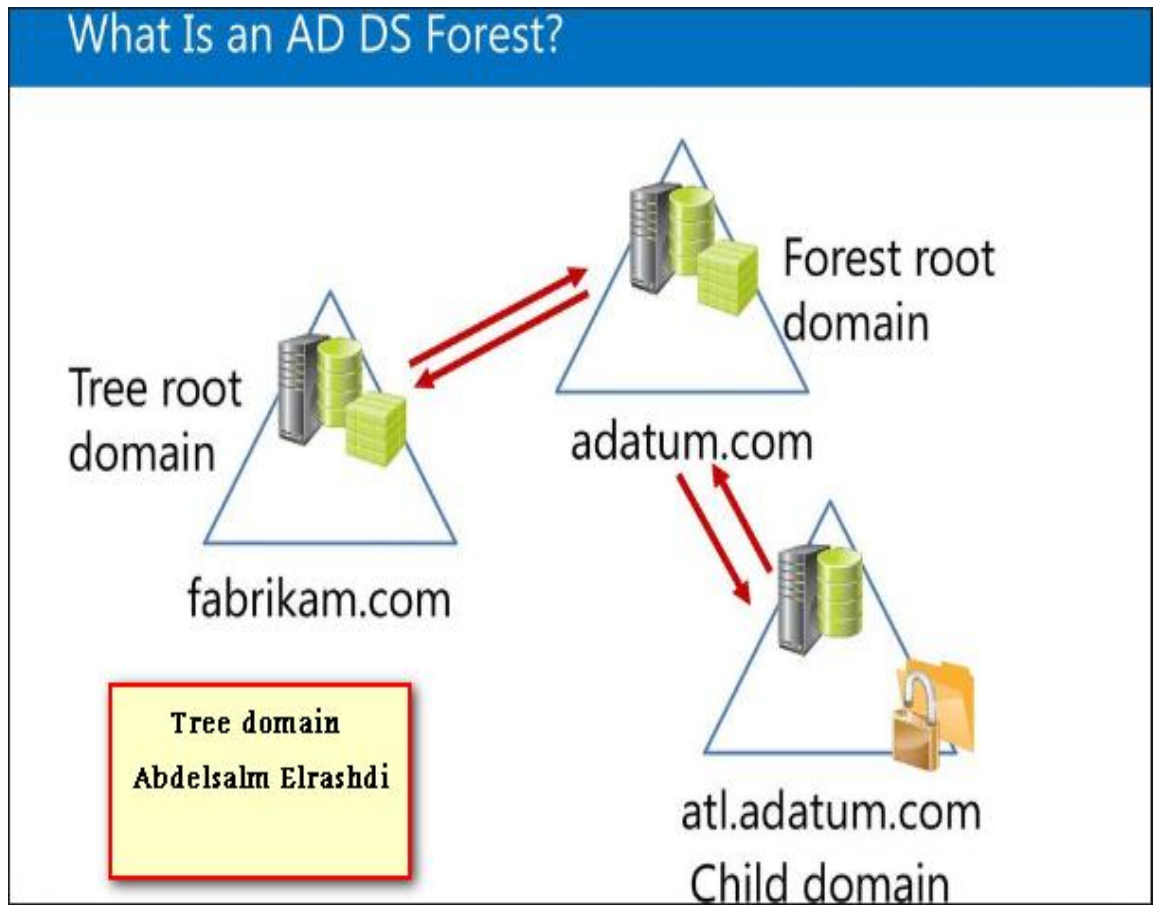
27- Tree Domain

تتكون شجرة المجال من عدة نطاقات تشترك في مخطط وتكوين شائعين ، مما يشكل مساحة اسم مجاورة. يتم أيضاً ربط المجالات في شجرة معاً بواسطة علاقات الثقة. الدليل النشط عبارة عن مجموعة واحدة أو أكثر من الأشجار.

A domain tree is made up of several domains that share a common schema and configuration, forming a contiguous namespace. Domains in a tree are also linked together by trust relationships. Active Directory is a set of one or more trees.

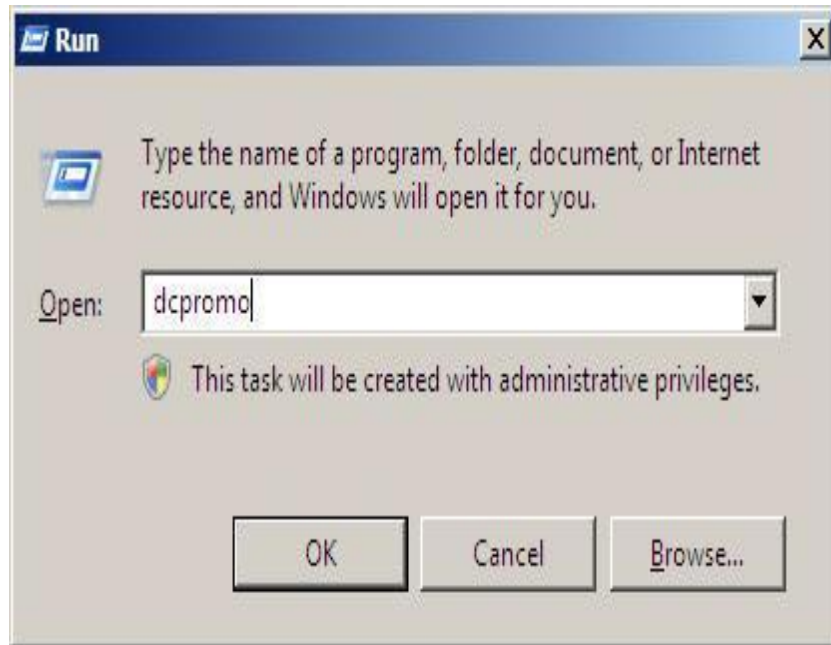
Trees can be viewed two ways. One view is the trust relationships between domains. The other view is the namespace of the domain tree. Child domain is a part of your main domain, if yahoo.com is your main domain then your sub domain will be mail.yahoo.com.

Domain Controller is simply a physical machine, on which you install your domain.

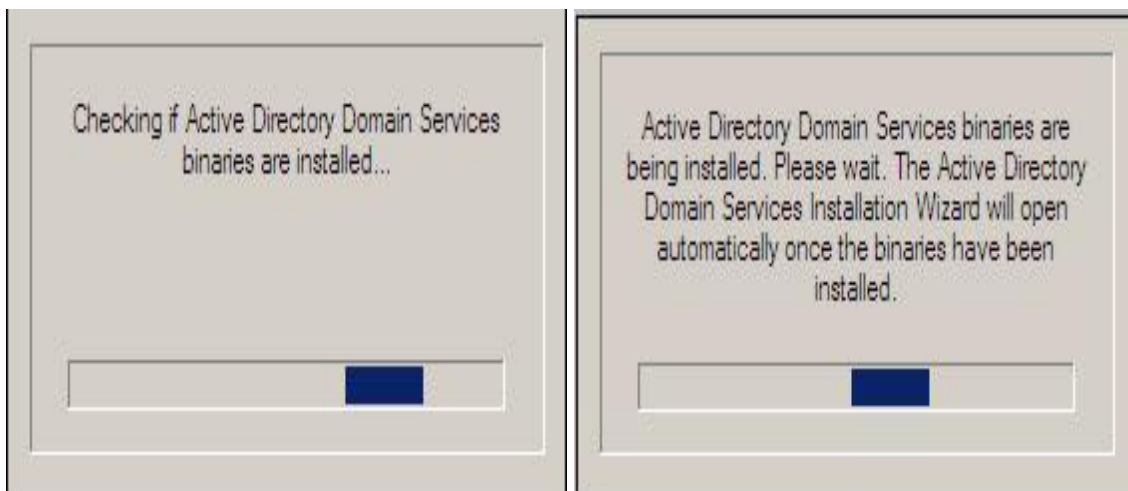


27.1- Install tree Domain in windows server 2008

To set up an tree Domain, I will use the dcpromo.exe command. To use the command, click on Start > Run > and then write dcpromo > Click OK



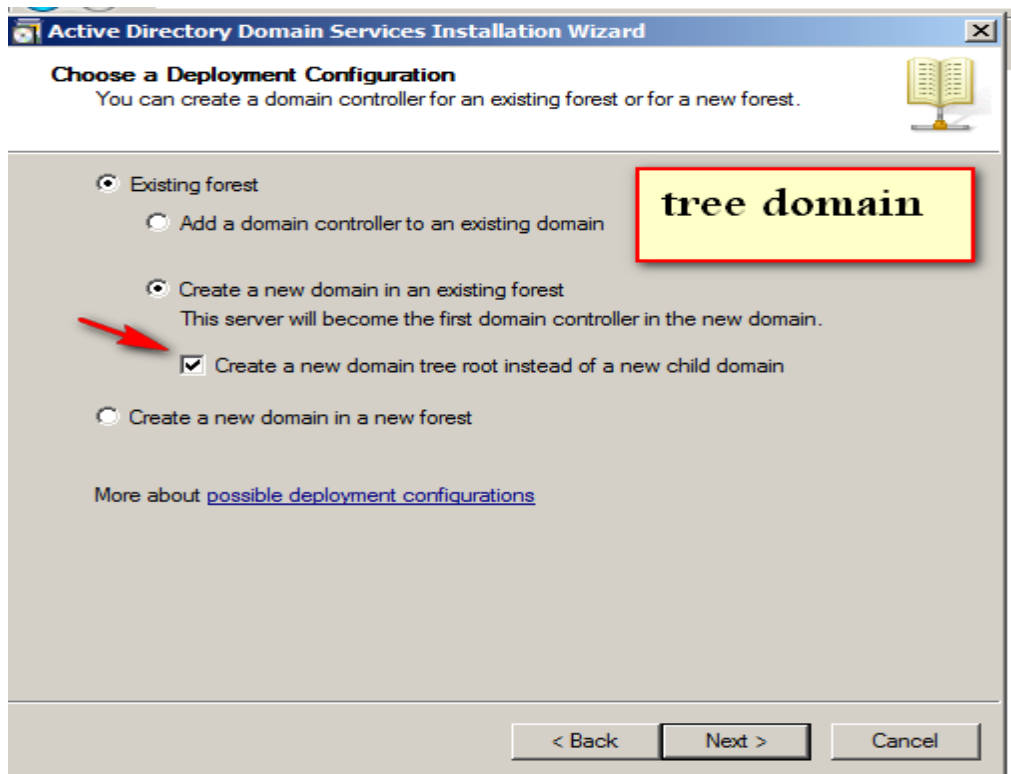
The system will start checking if Active Directory Domain Services (AD DS) binaries are installed, then will start installing them. The binaries could be installed if you had run the dcpromo command previously and then canceled the operation after the binaries were installed.



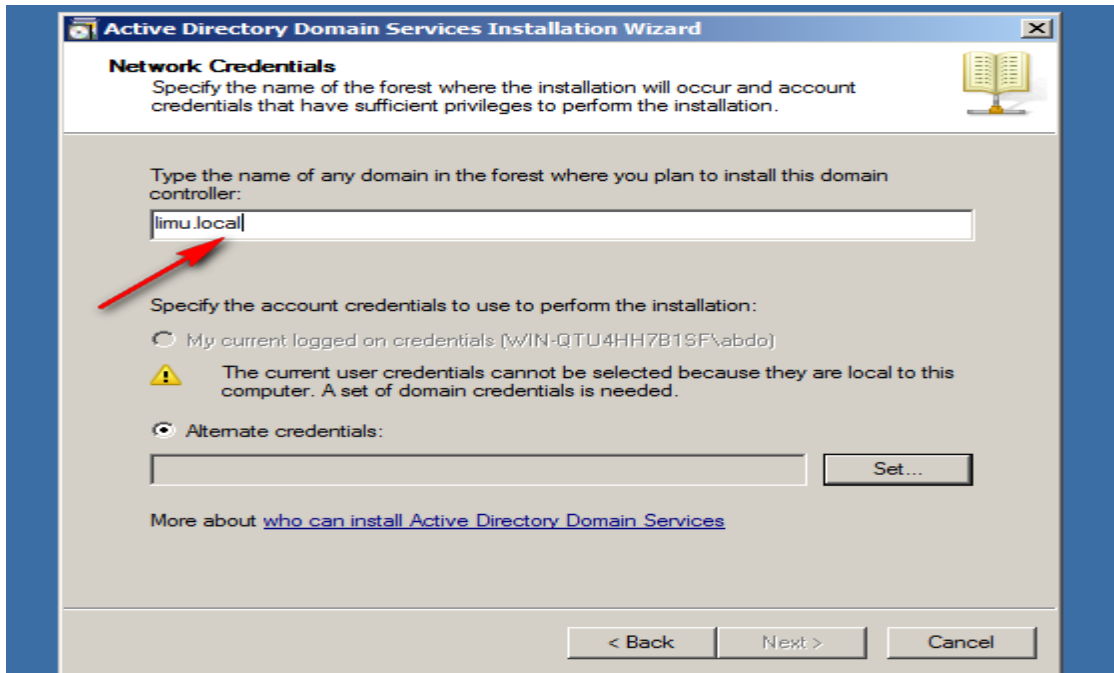
The Active Directory Domain Services Installation Wizard will start, either enable the checkbox beside Use Advanced mode installation and Click Next , or keep it unselected and click on Next



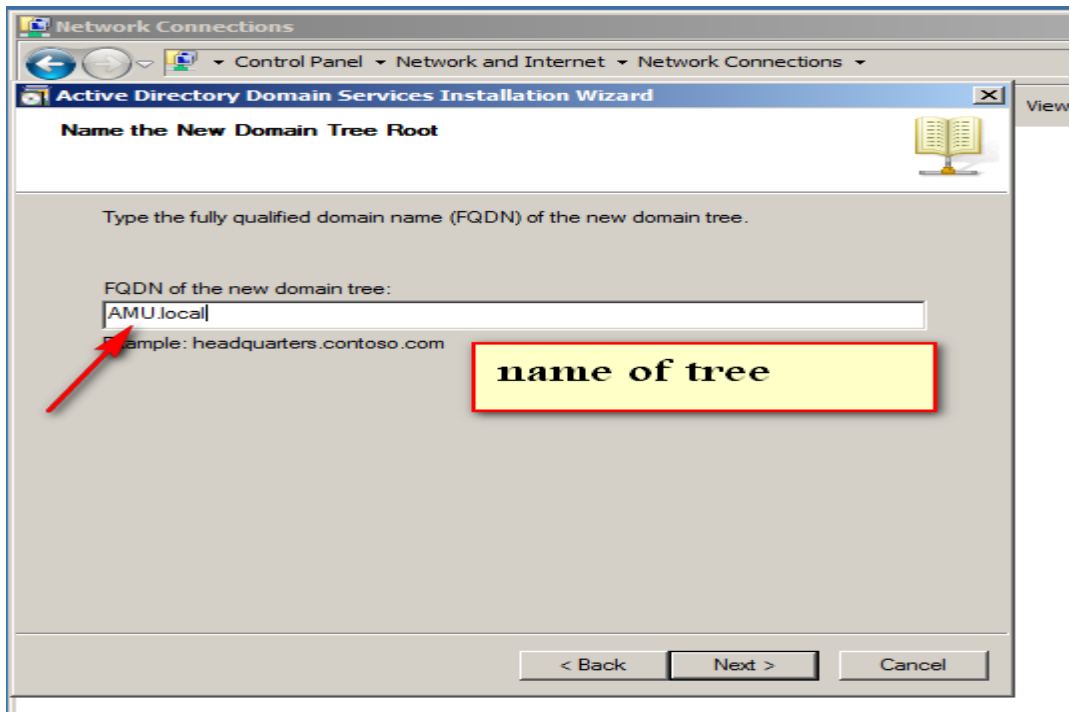
Select create a new domain tree root instead of a new child domain



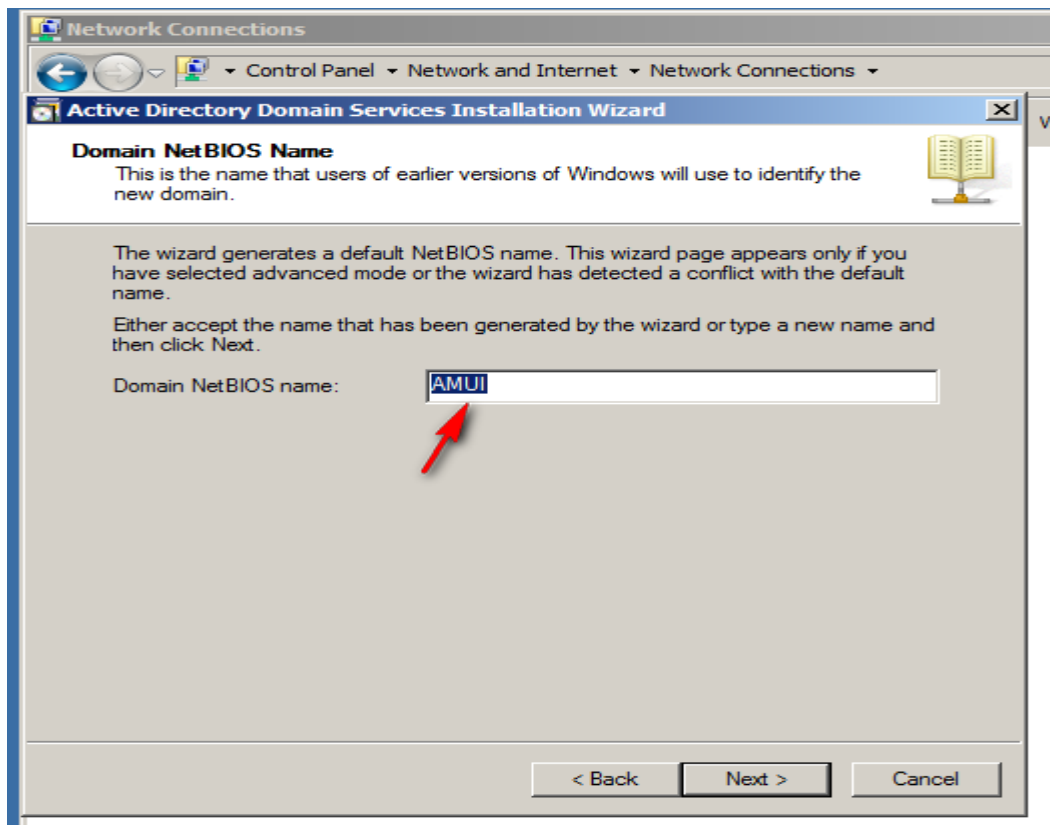
Write name of parent domain



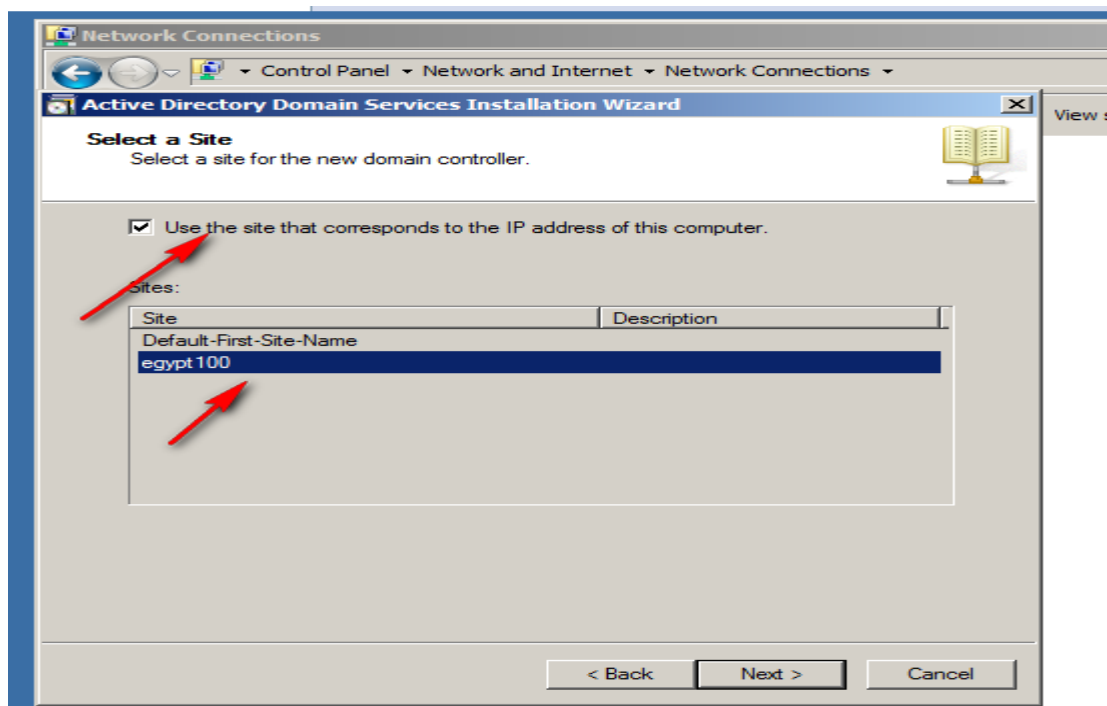
Name of tree



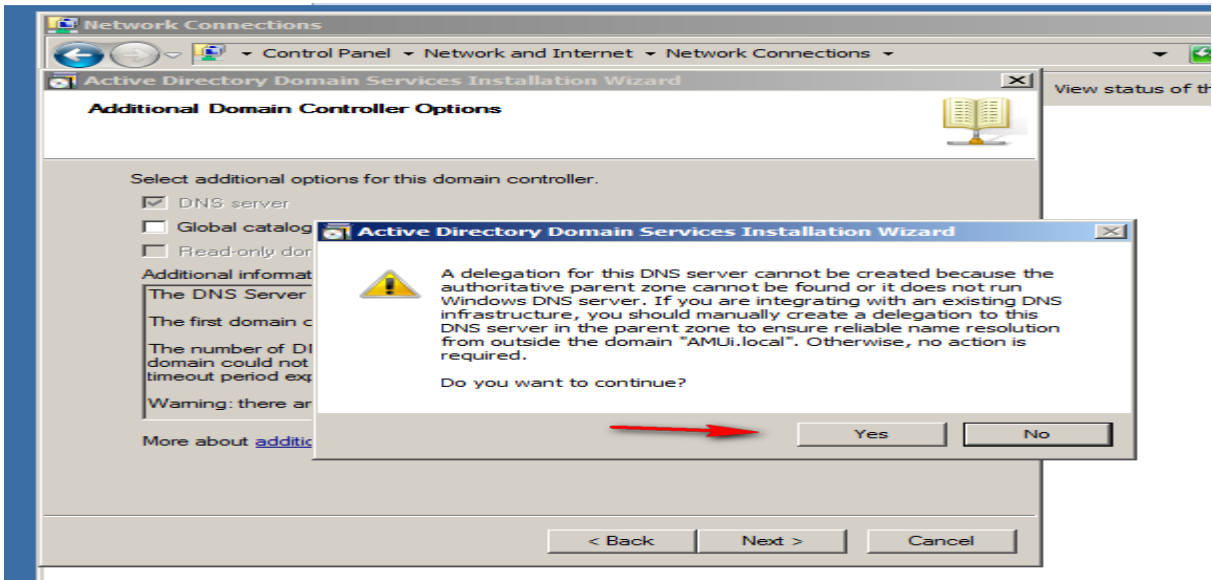
Domain Netbios name



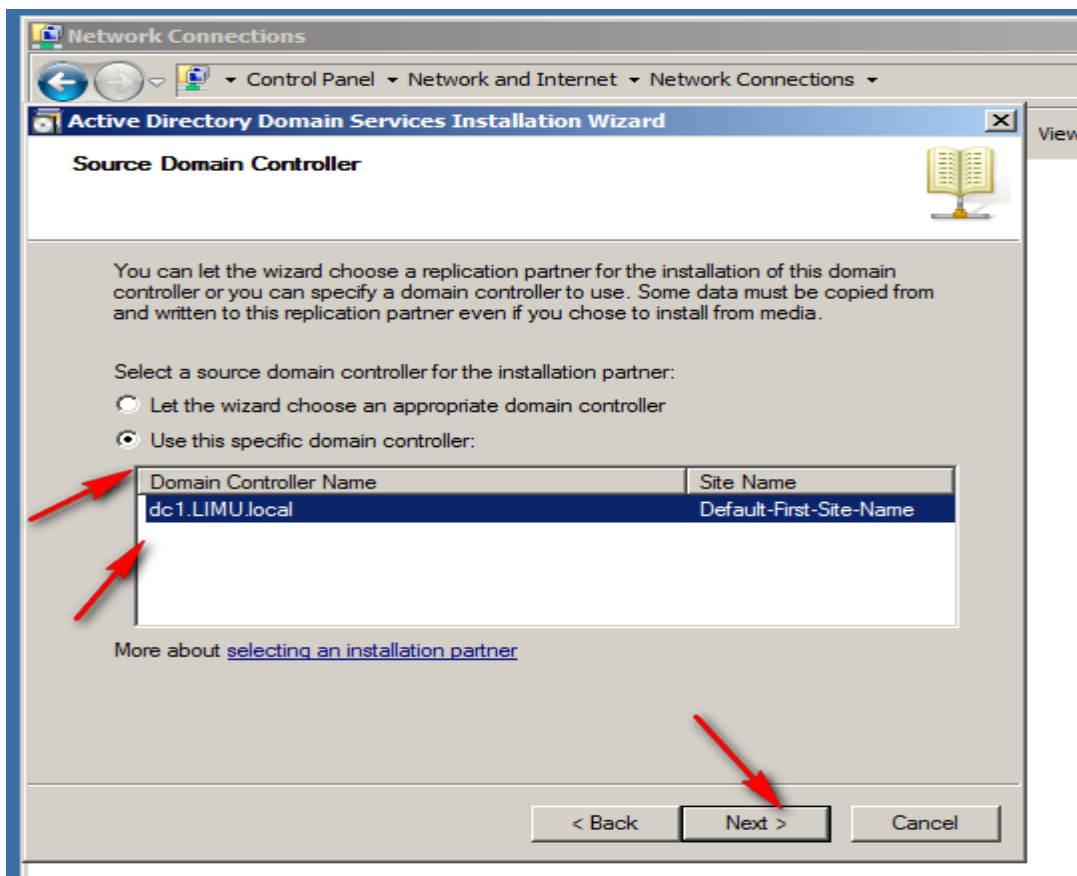
Select a site



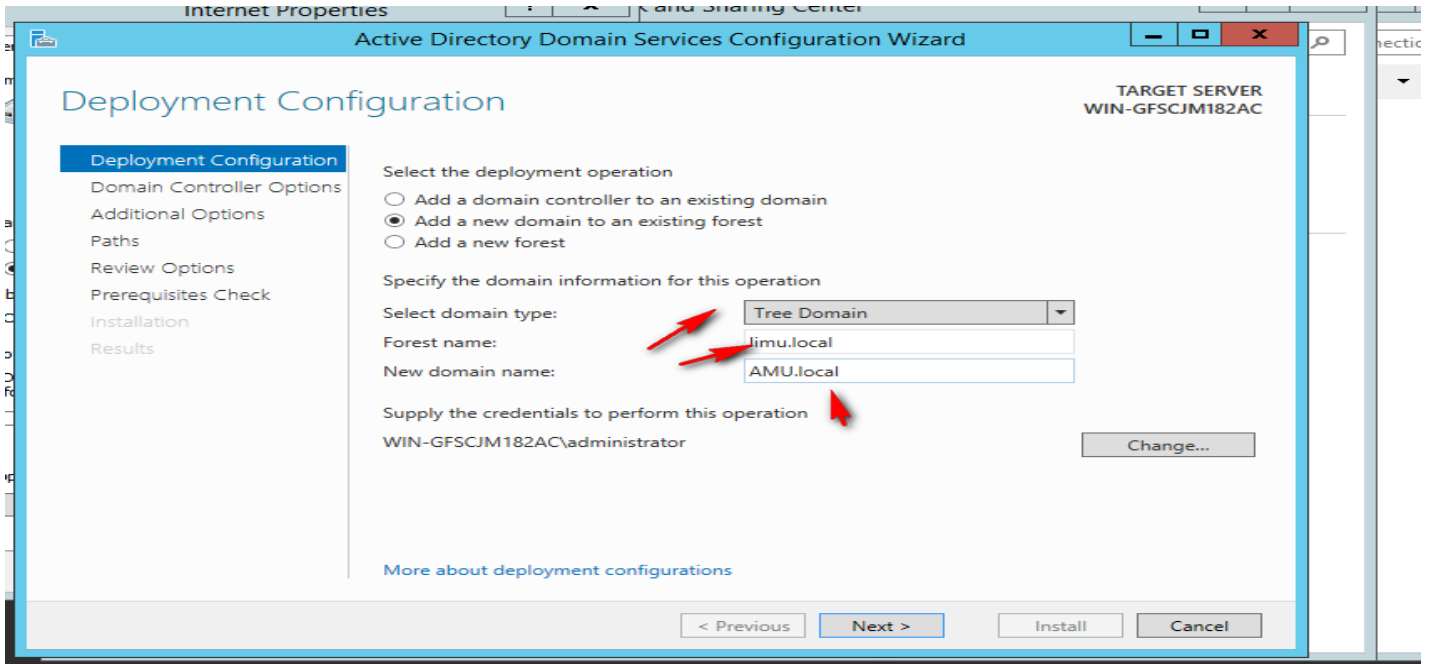
DNS



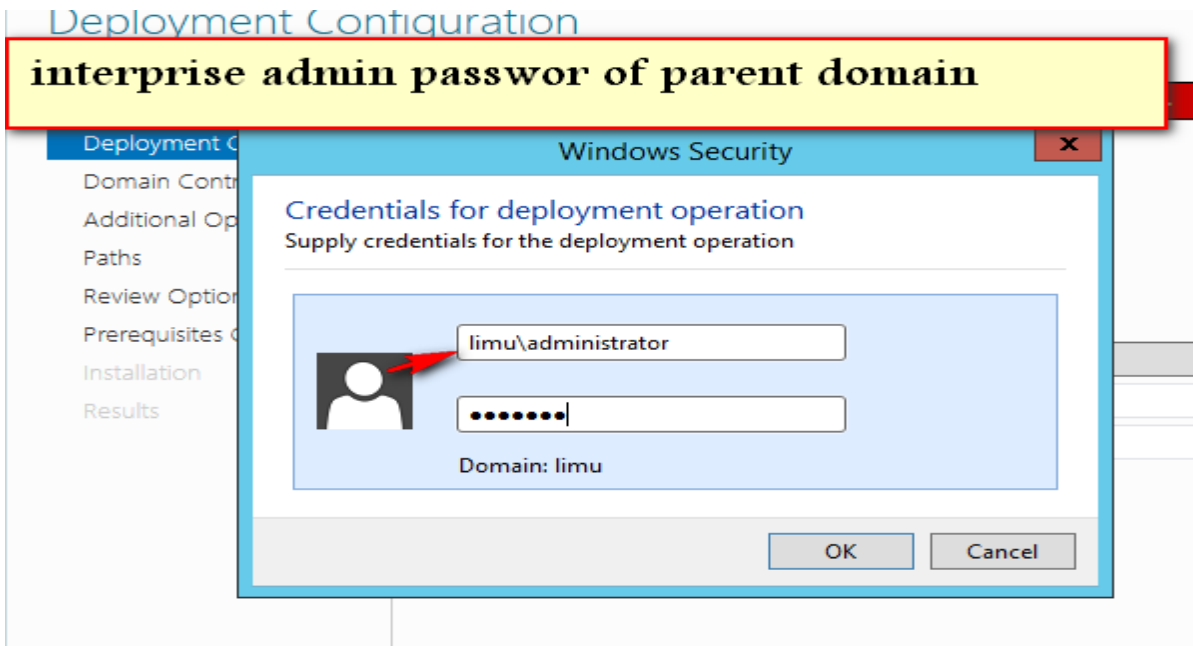
Source domain controller



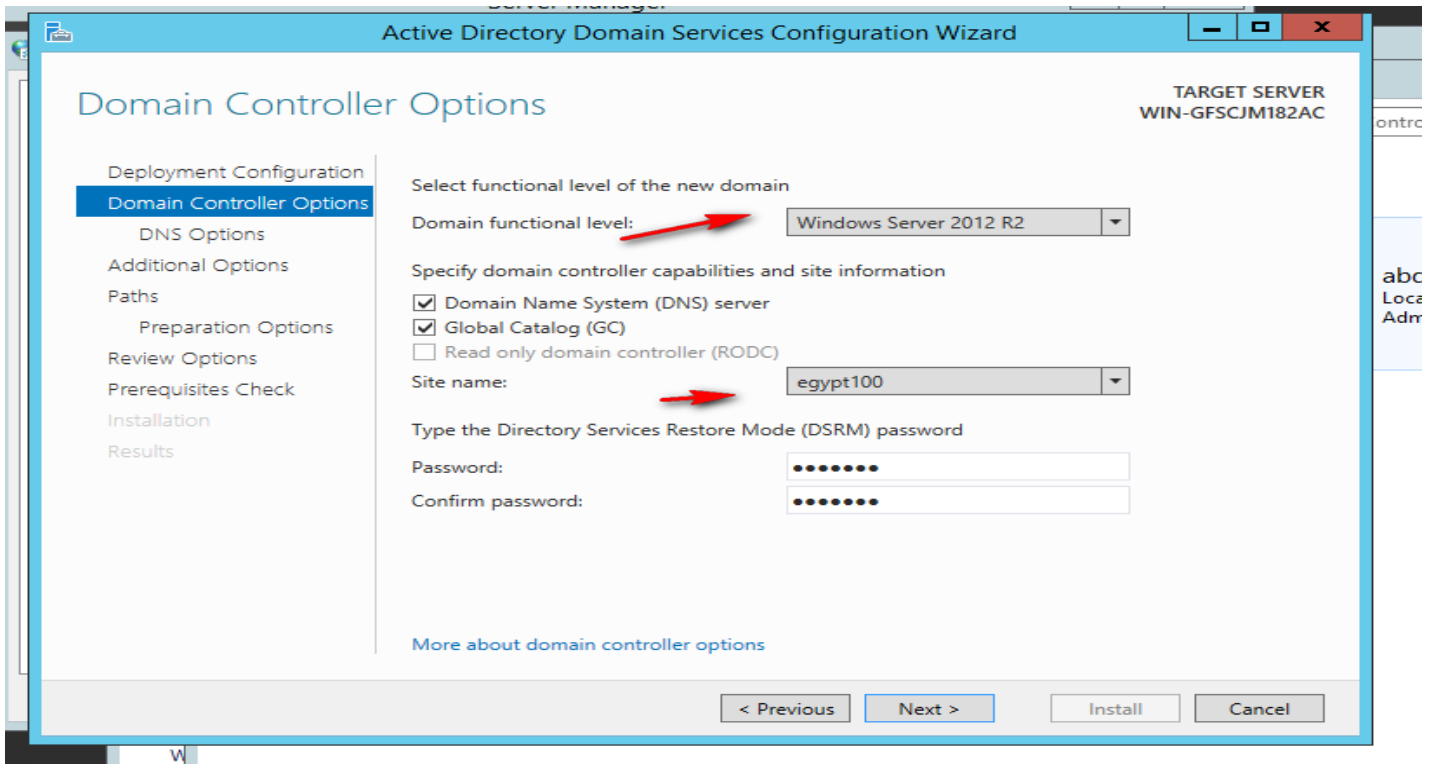
27.2- Install tree Domain in windows server 2012



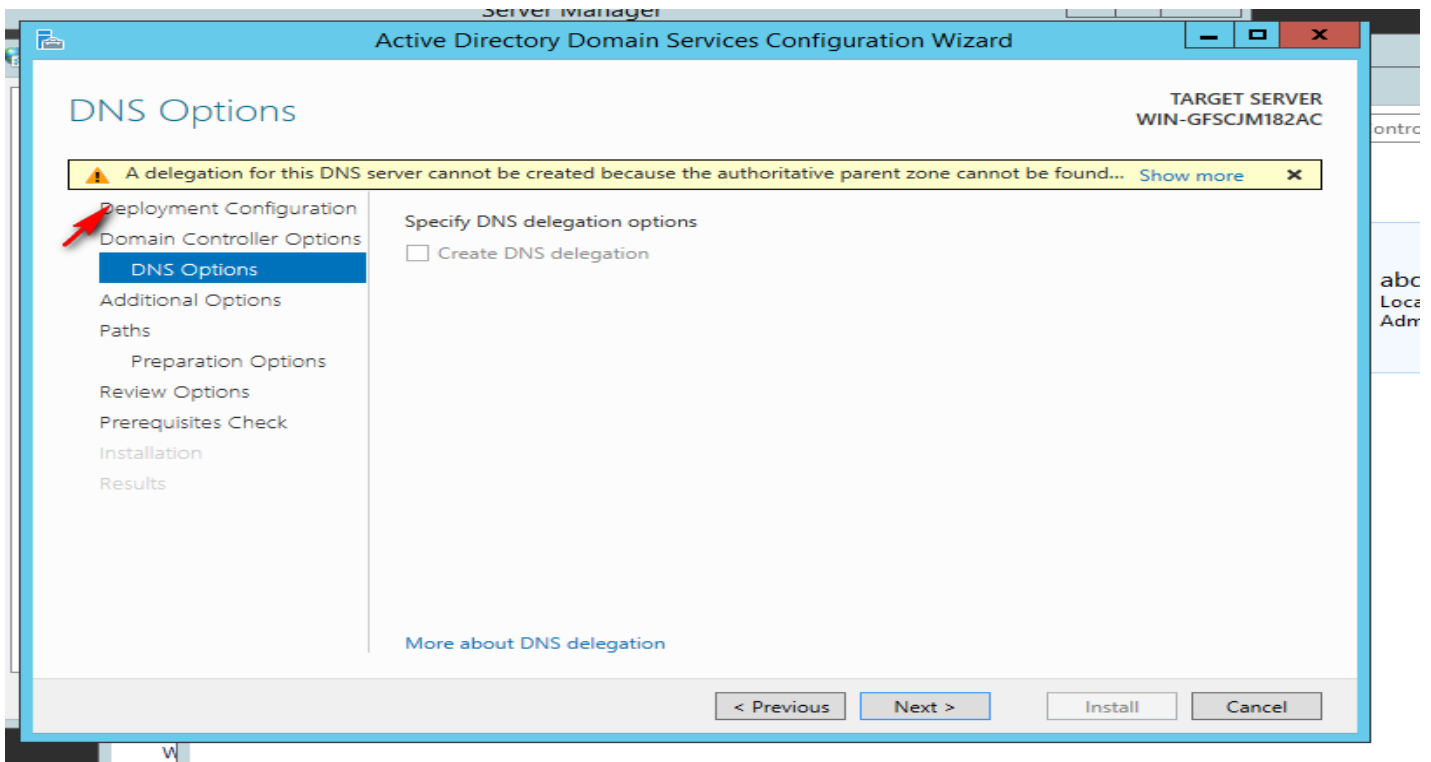
Enterprise admin password of parent domain



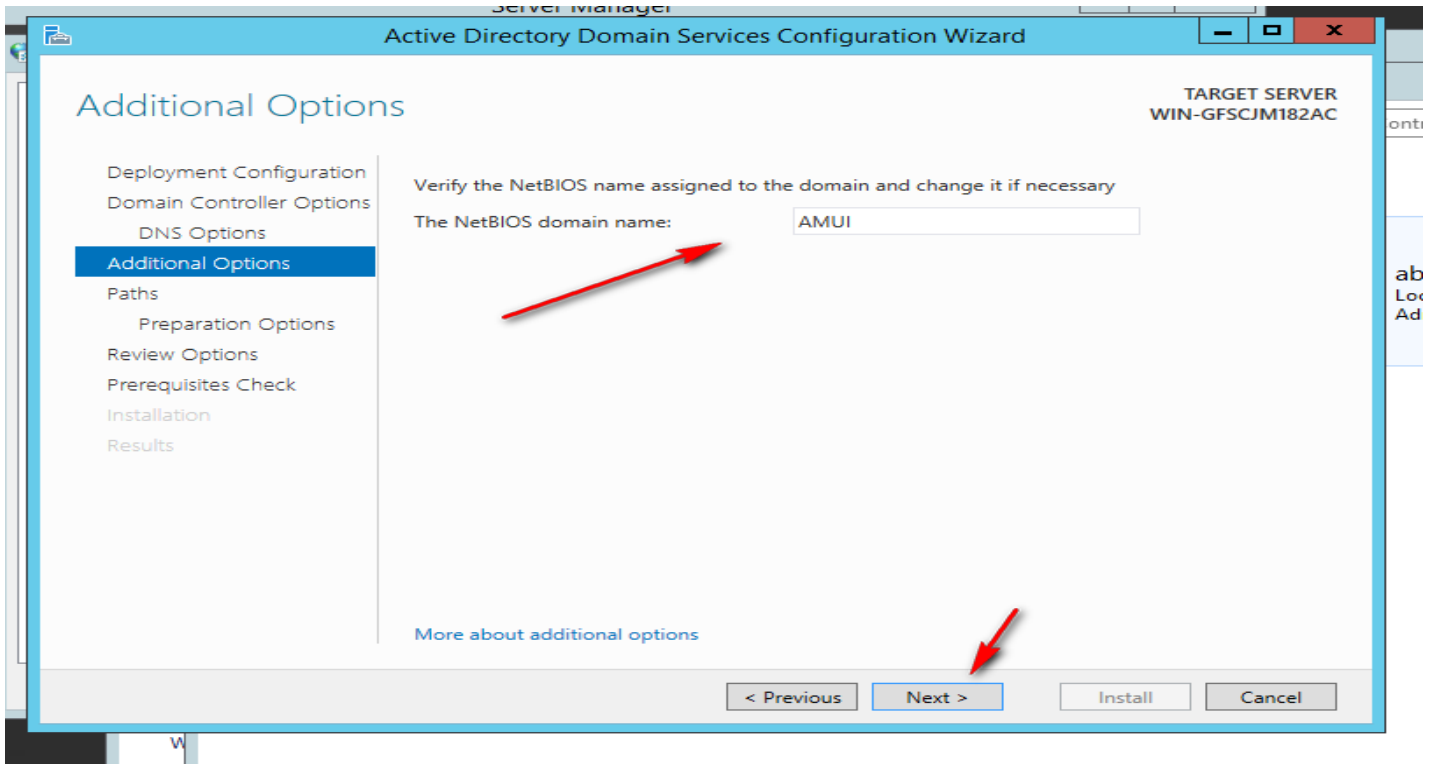
Select the following options



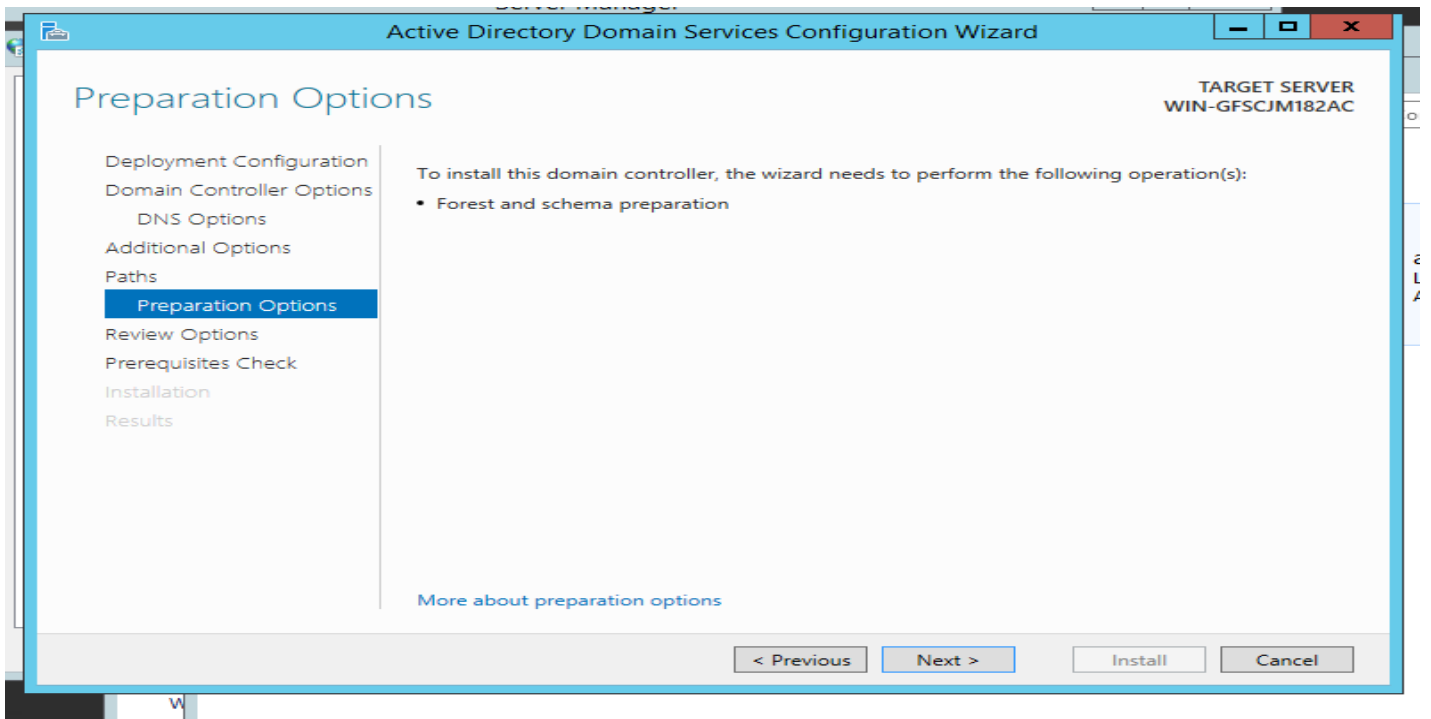
DNS



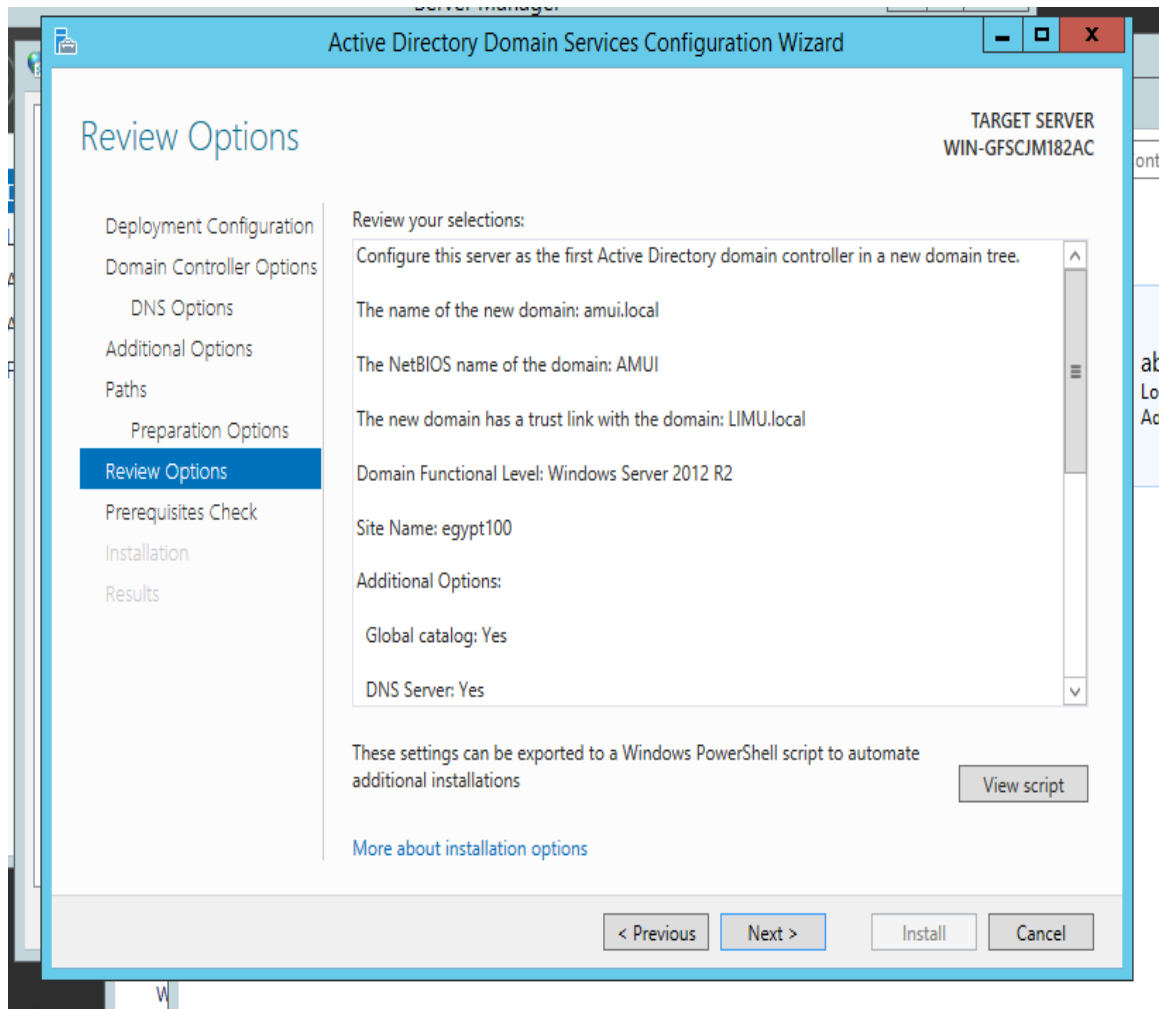
Netbios domain name



Next



Next then finish

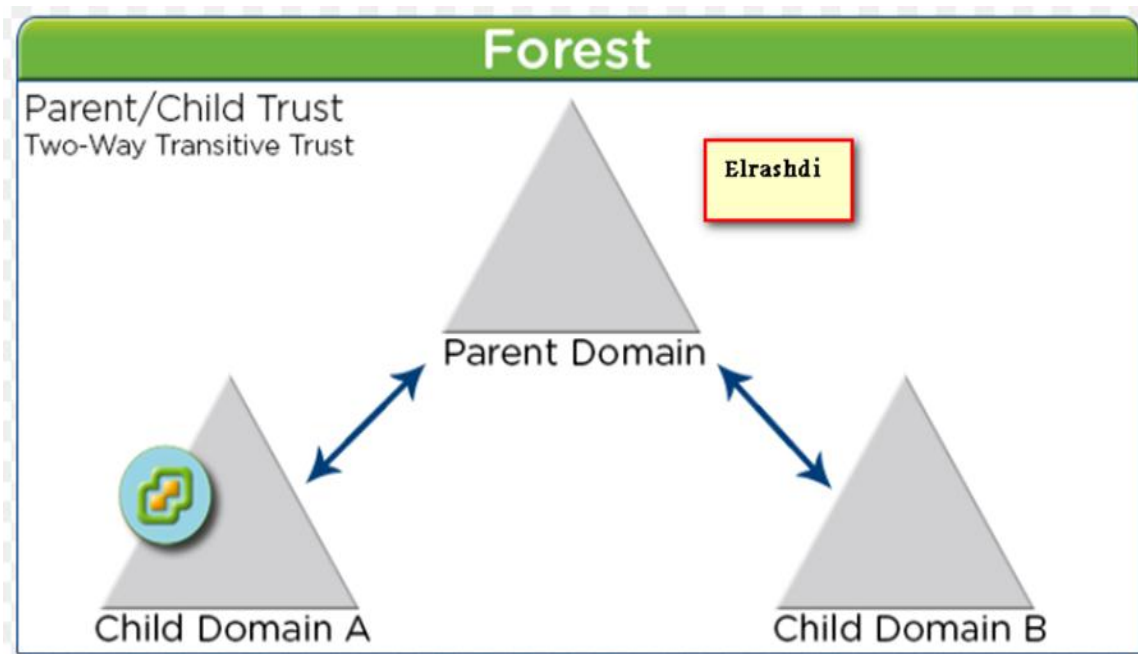


28-Child Domain

A child domain هو domain آخر ضمن أحد الأبوين في تسلسل هرمي في active directory النشط. سيرث نفس اسم مجال الرئيسي ويكون في نفس forest

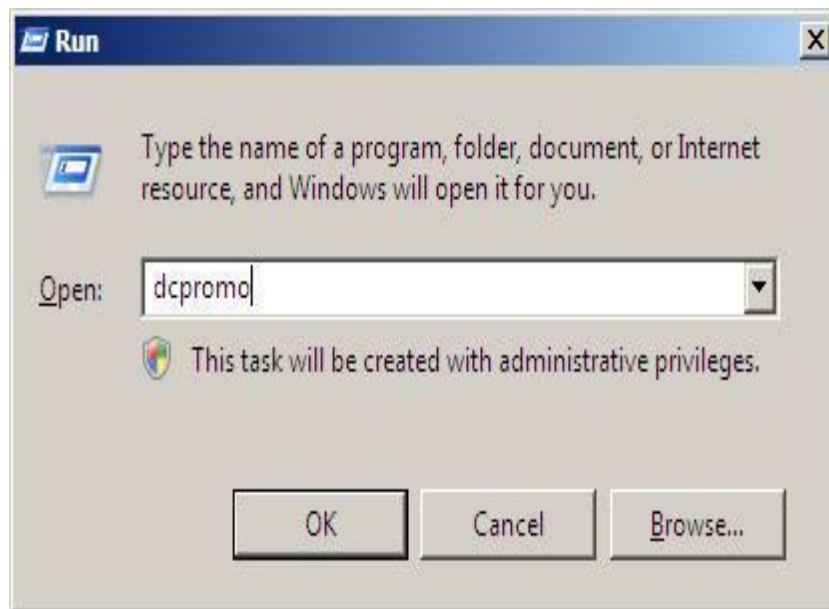
A child domain is another domain under a parent one in an active directory domain hierarchy. A child domain under a parent will inherit parent name and will in same forest

You require additional domains within your AD DS forest. If the new domain is to share a contiguous namespace with one or more domains, you need to create a new child domain.

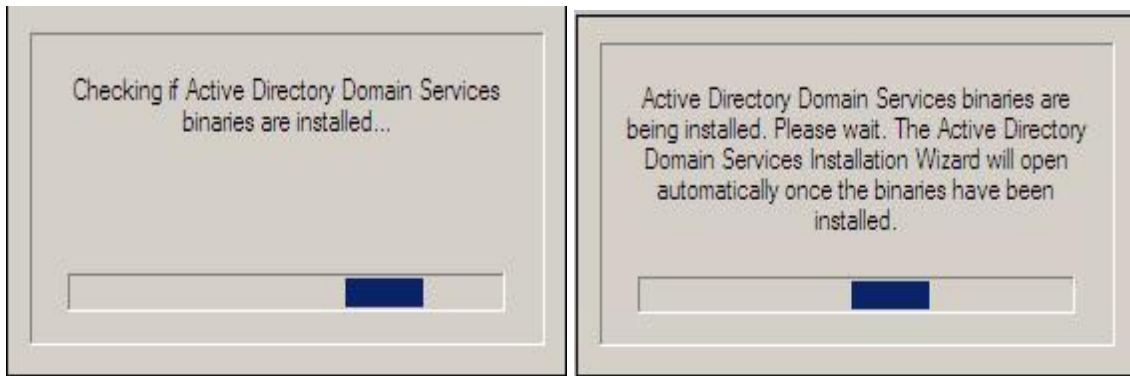


28.1- Child Domain in windows server 2008R2

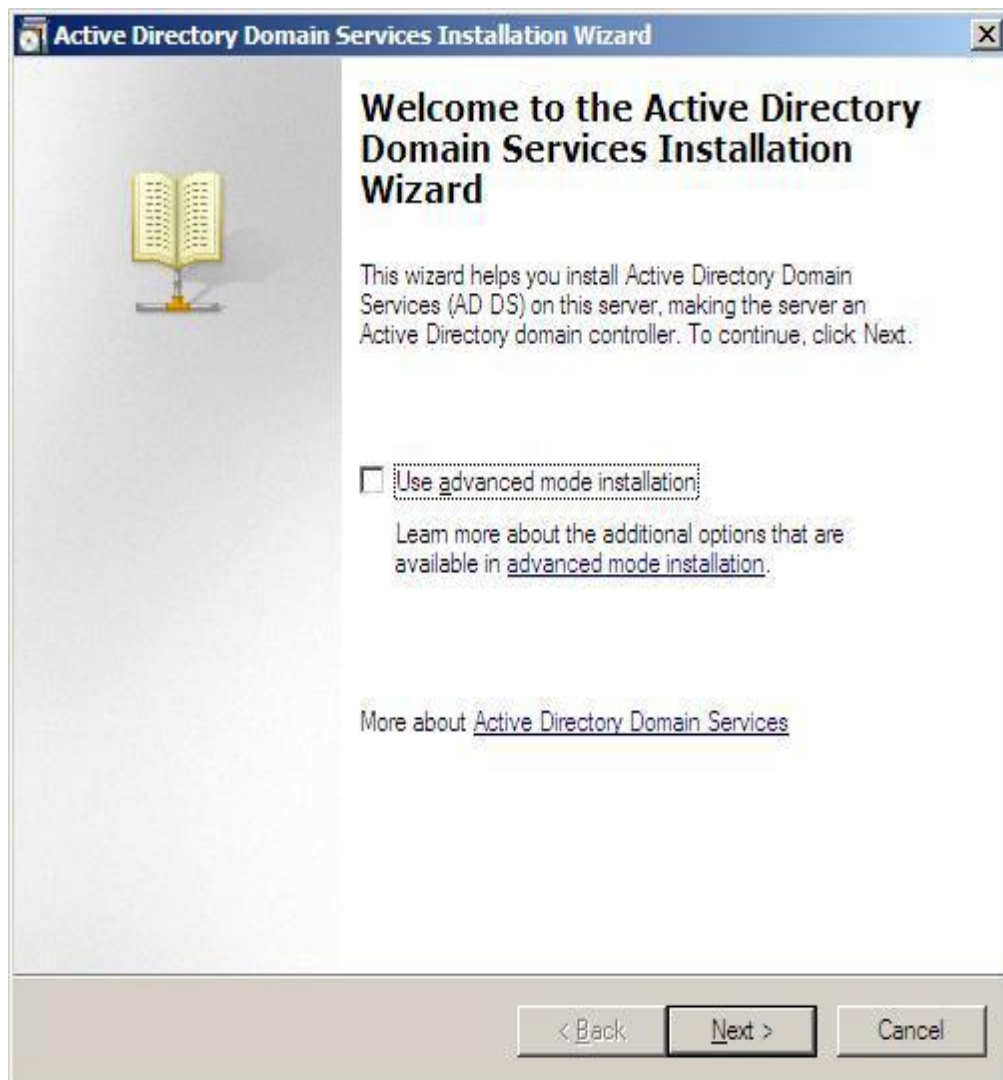
To set up an Additional Domain Controller, I will use the dcpromo.exe command. To use the command, click on Start > Run > and then write dcpromo > Click OK



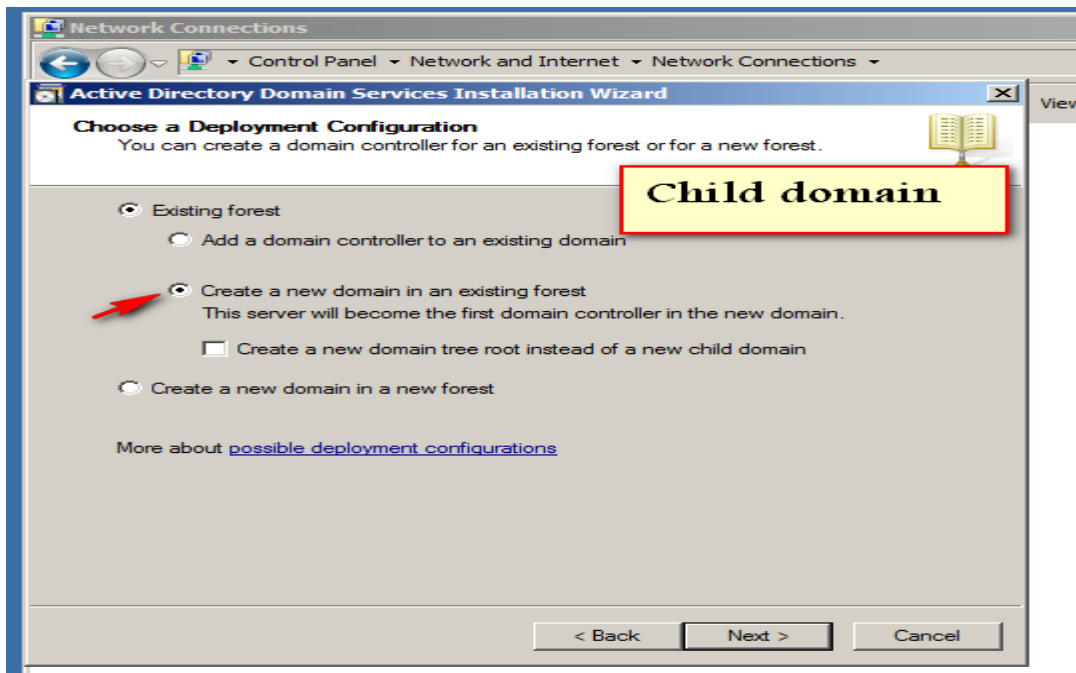
The system will start checking if Active Directory Domain Services (AD DS) binaries are installed, then will start installing them. The binaries could be installed if you had run the dcpromo command previously and then canceled the operation after the binaries were installed.



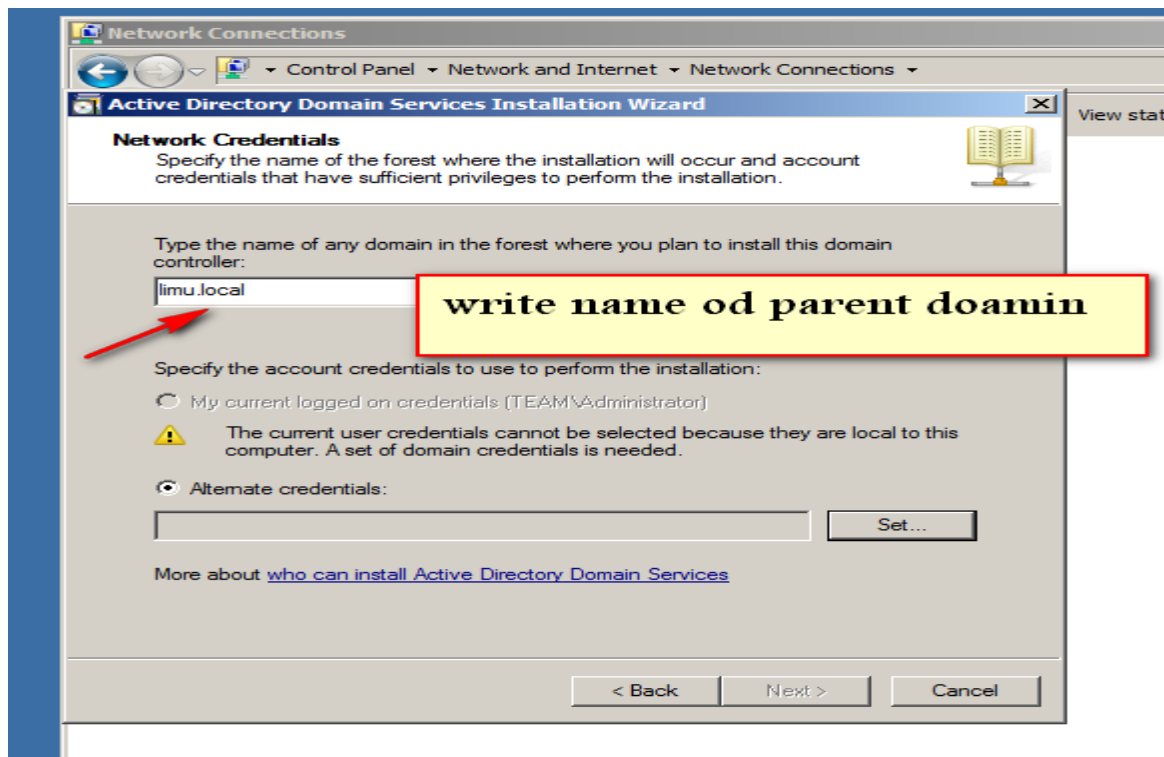
The Active Directory Domain Services Installation Wizard will start, either enable the checkbox beside Use Advanced mode installation and Click Next , or keep it unselected and click on Next



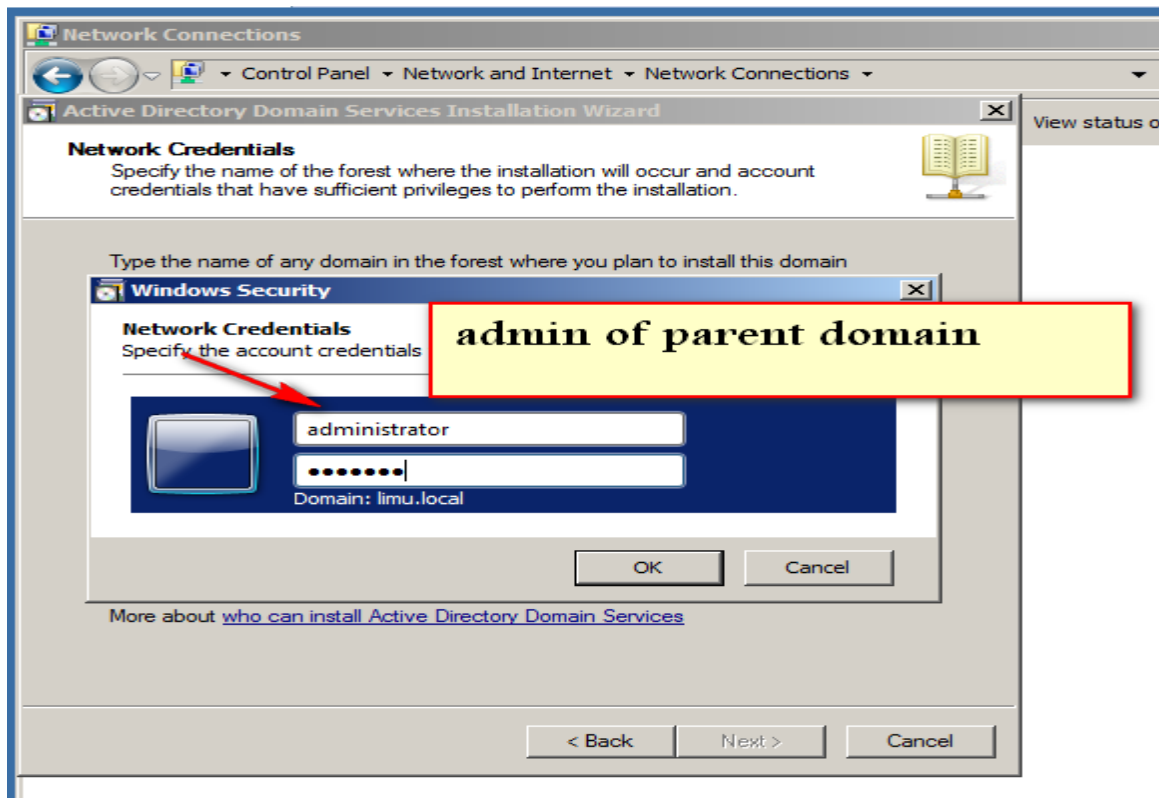
Choice create a new domain in existing forest



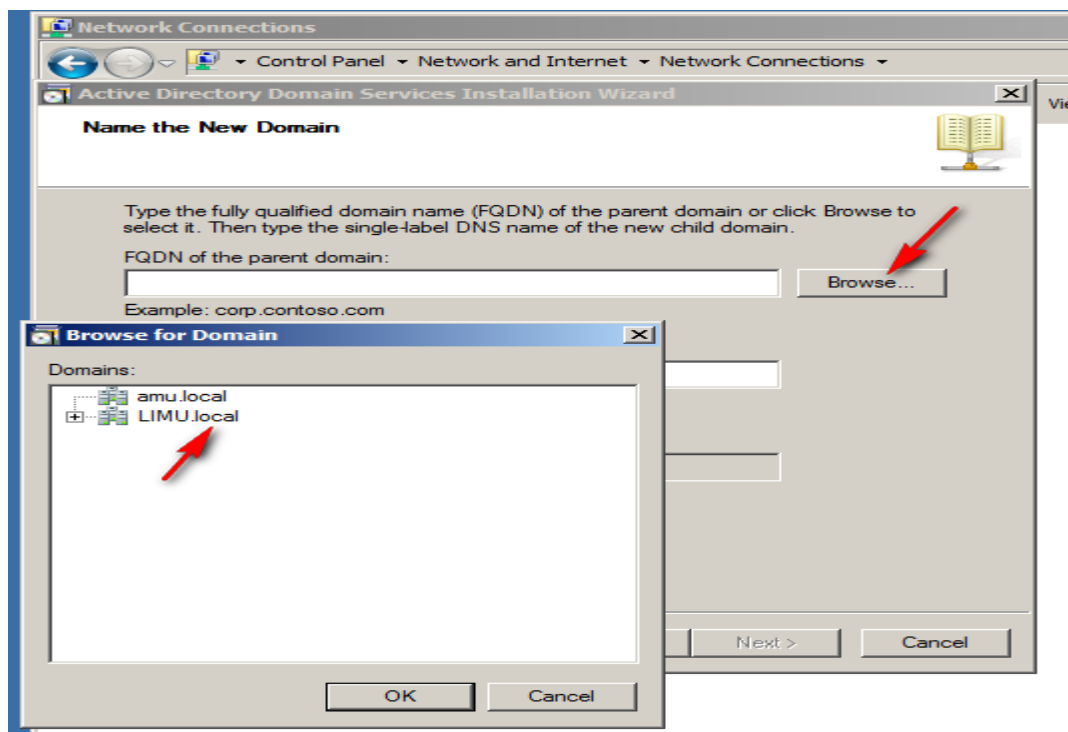
Write name of parent domain



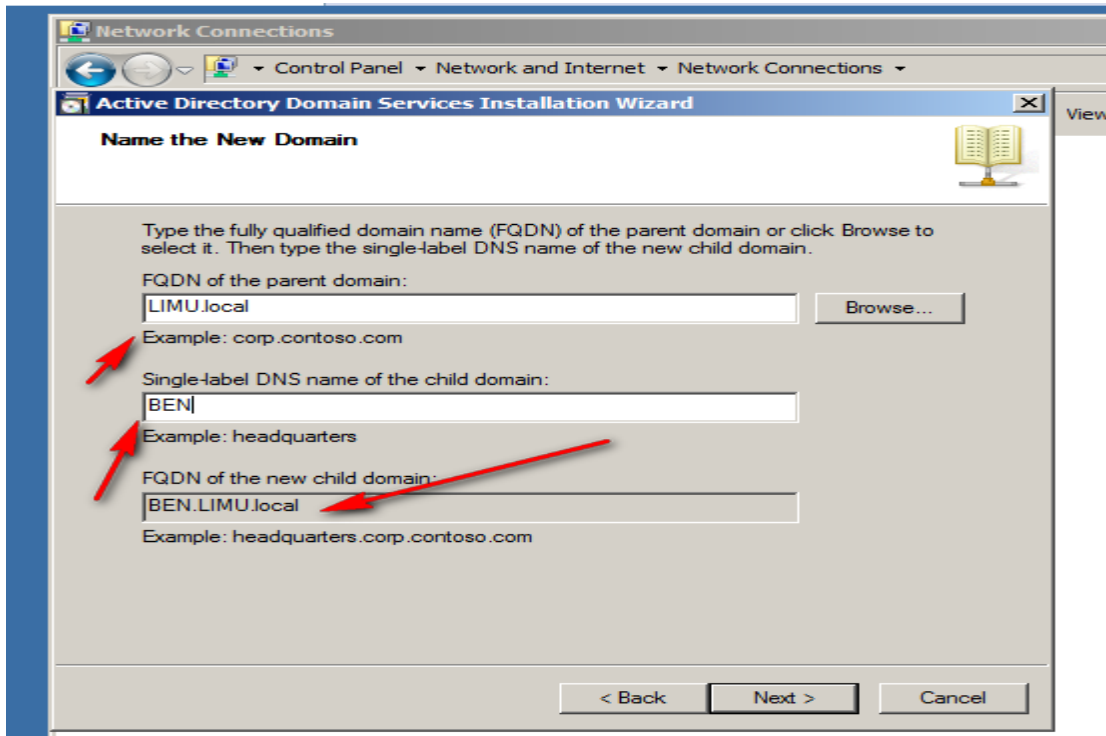
Click set then type enterprise admin of parent domain



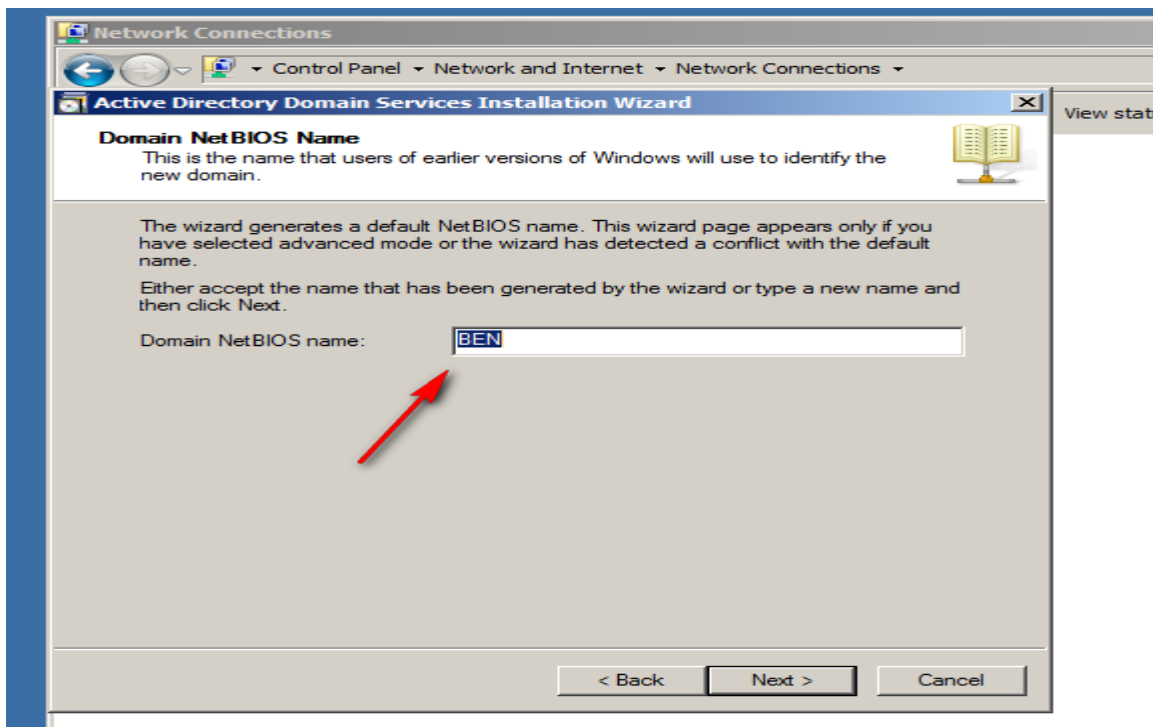
Browser then choice parent domain



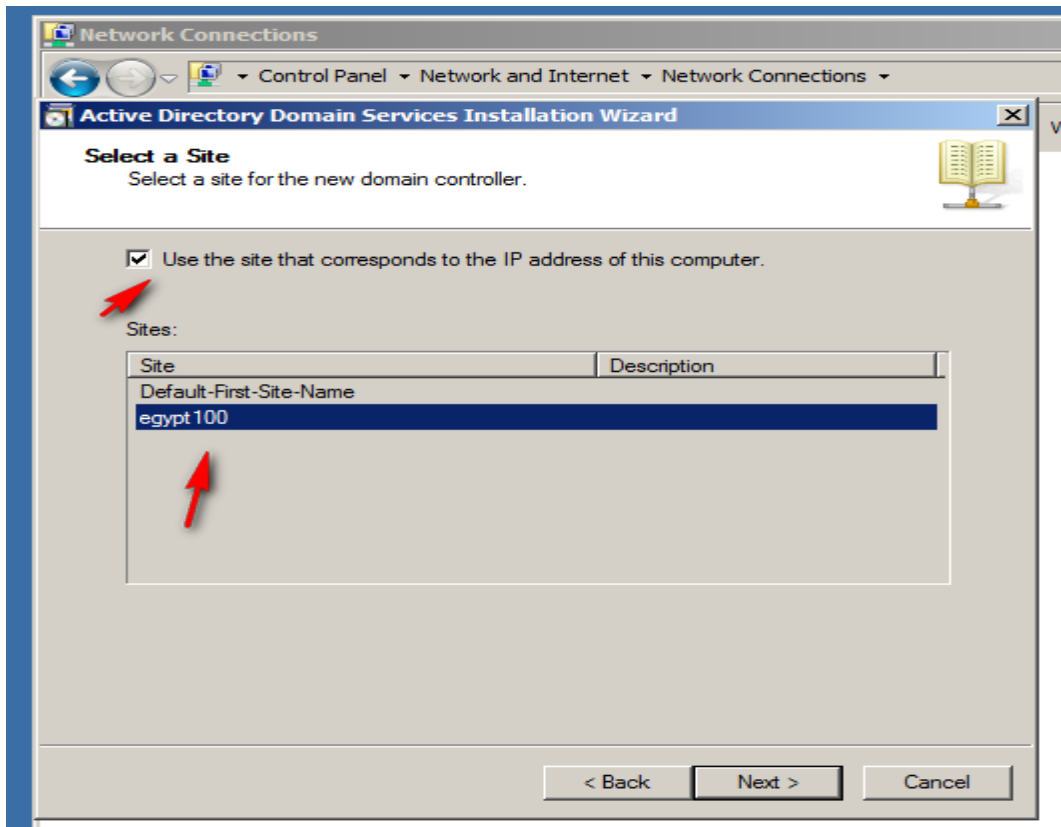
Type name of child domain



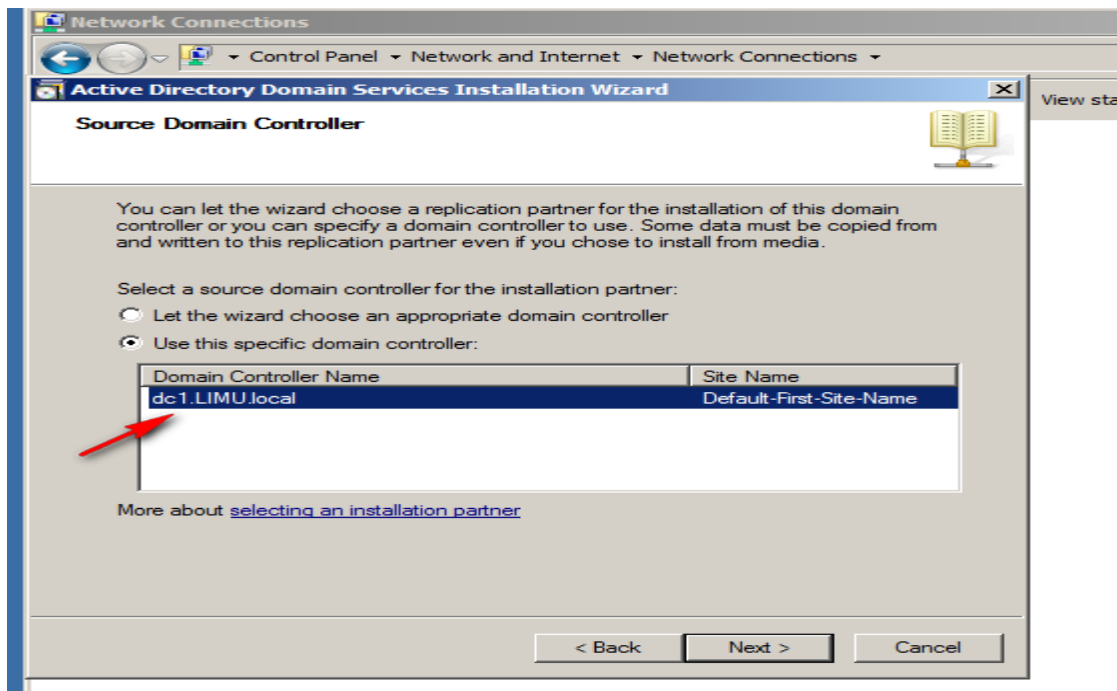
Domain Netbios name



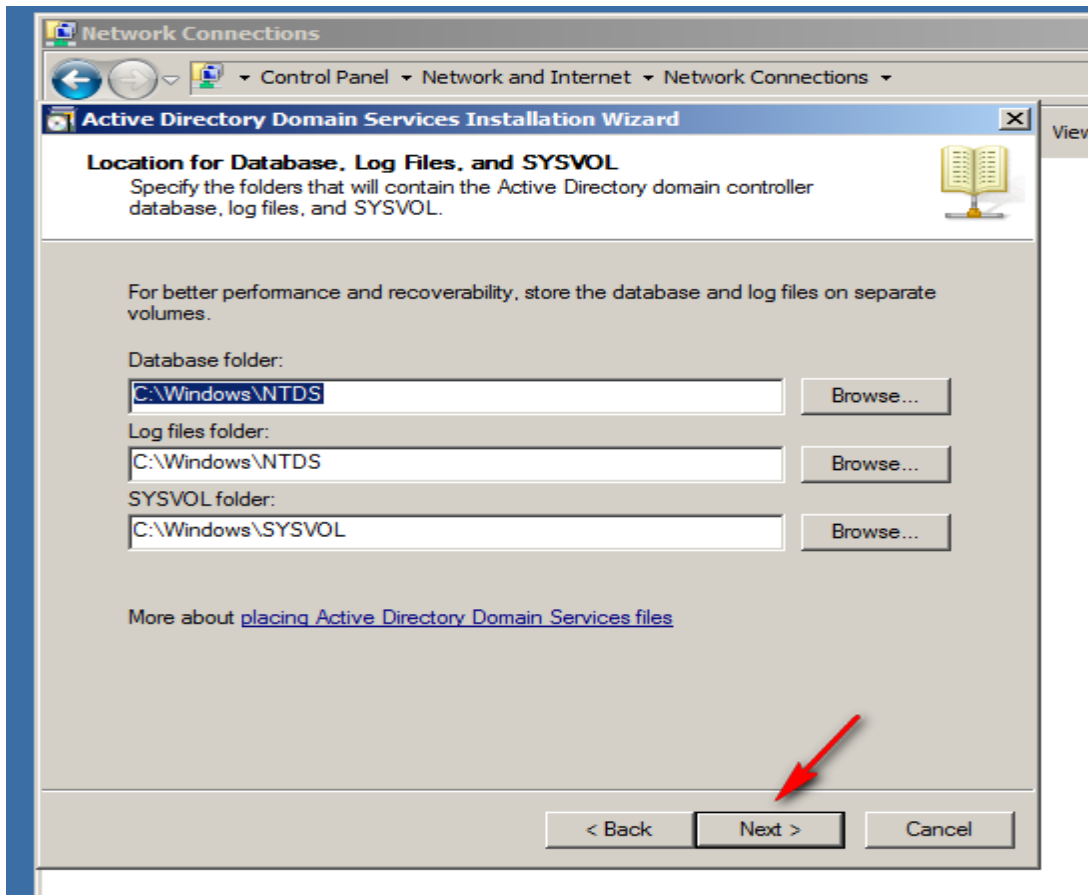
Select a site



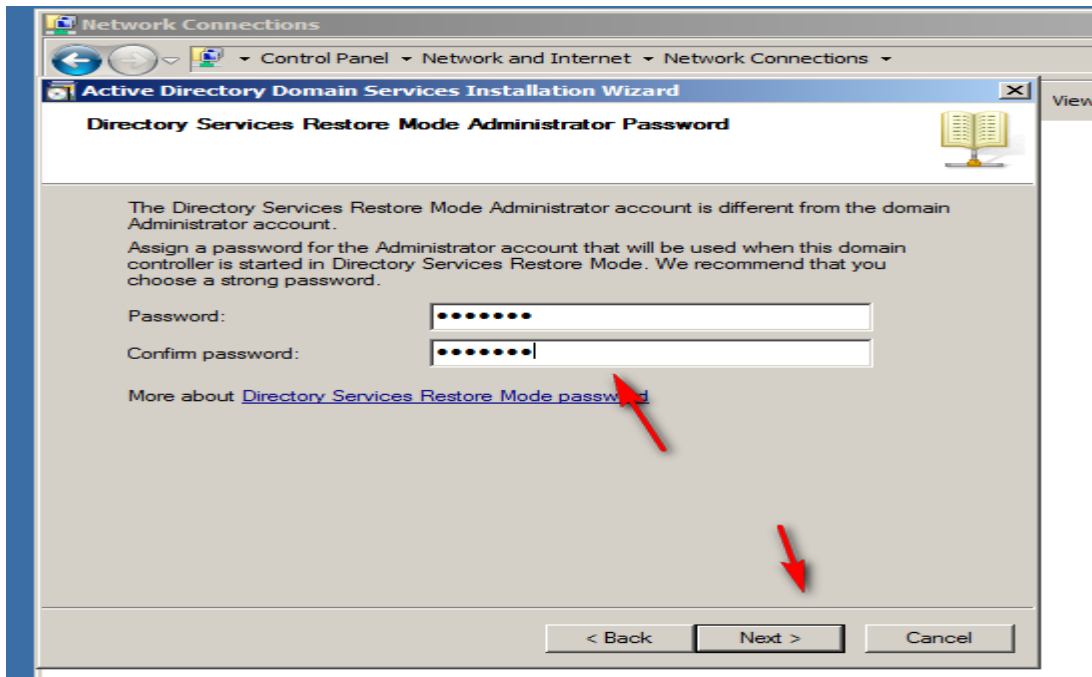
Source domain controller



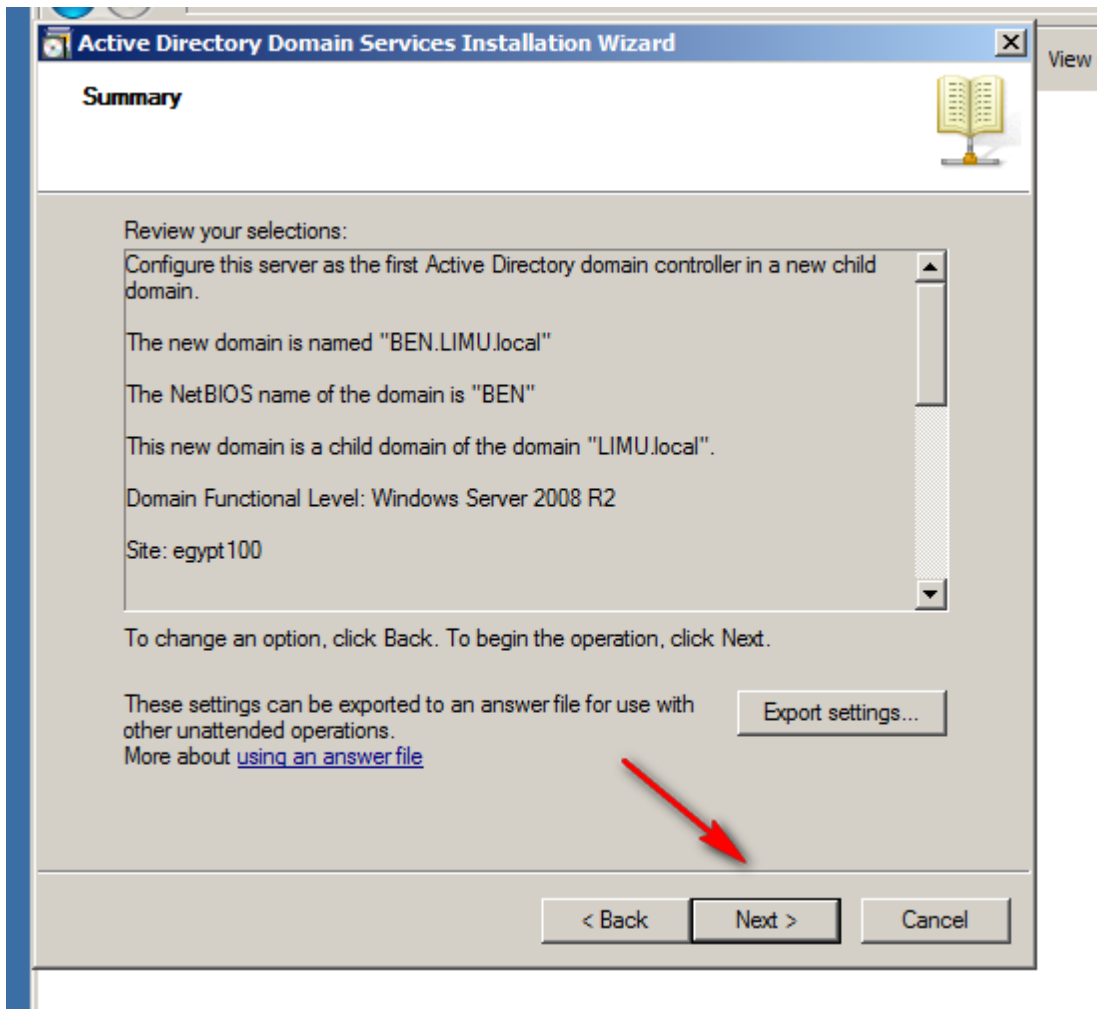
Log files and sysvol



Restore password

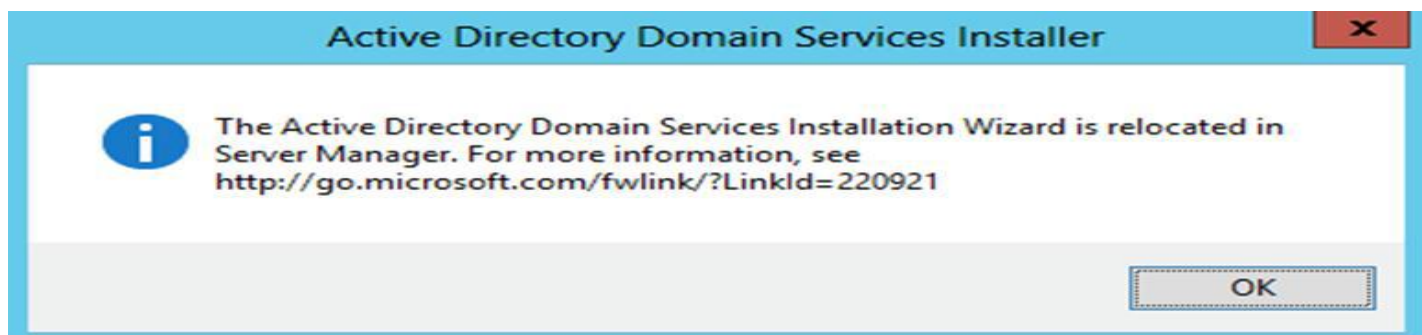


Summary

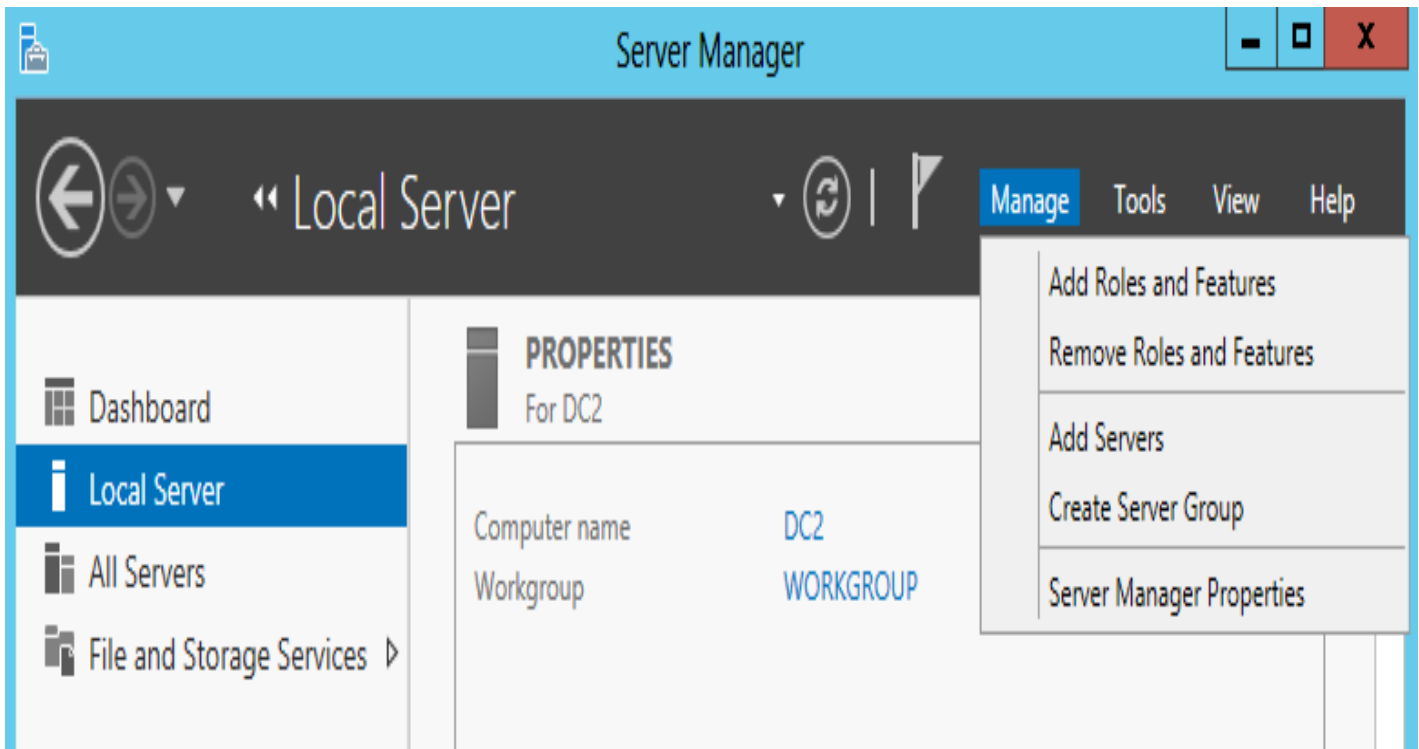


28.2- Child Domain in a windows Server 2012

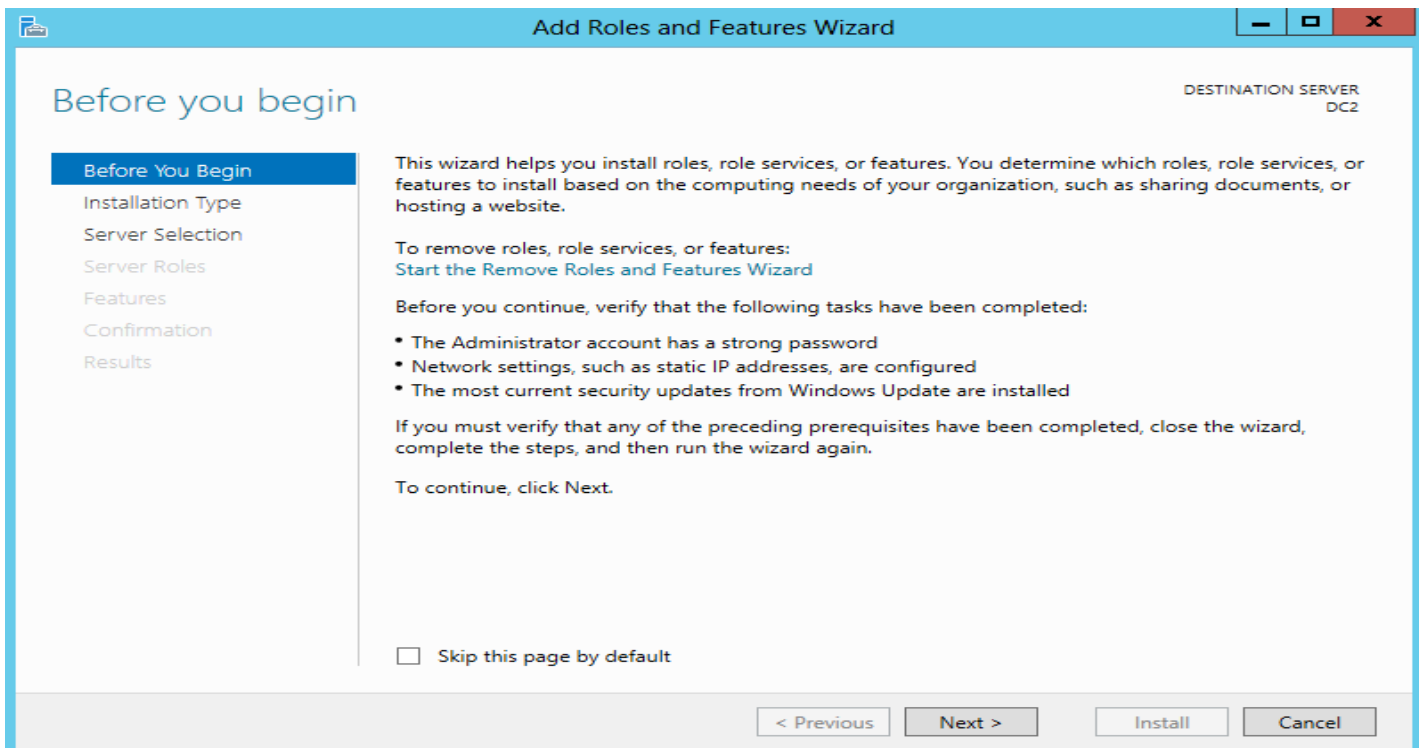
When you try and run DCPromo from the explorer shell on Windows Server 2012, you will receive the following message "The Active Directory Domain Services Installation Wizard is relocated in Server Manager. For more information.



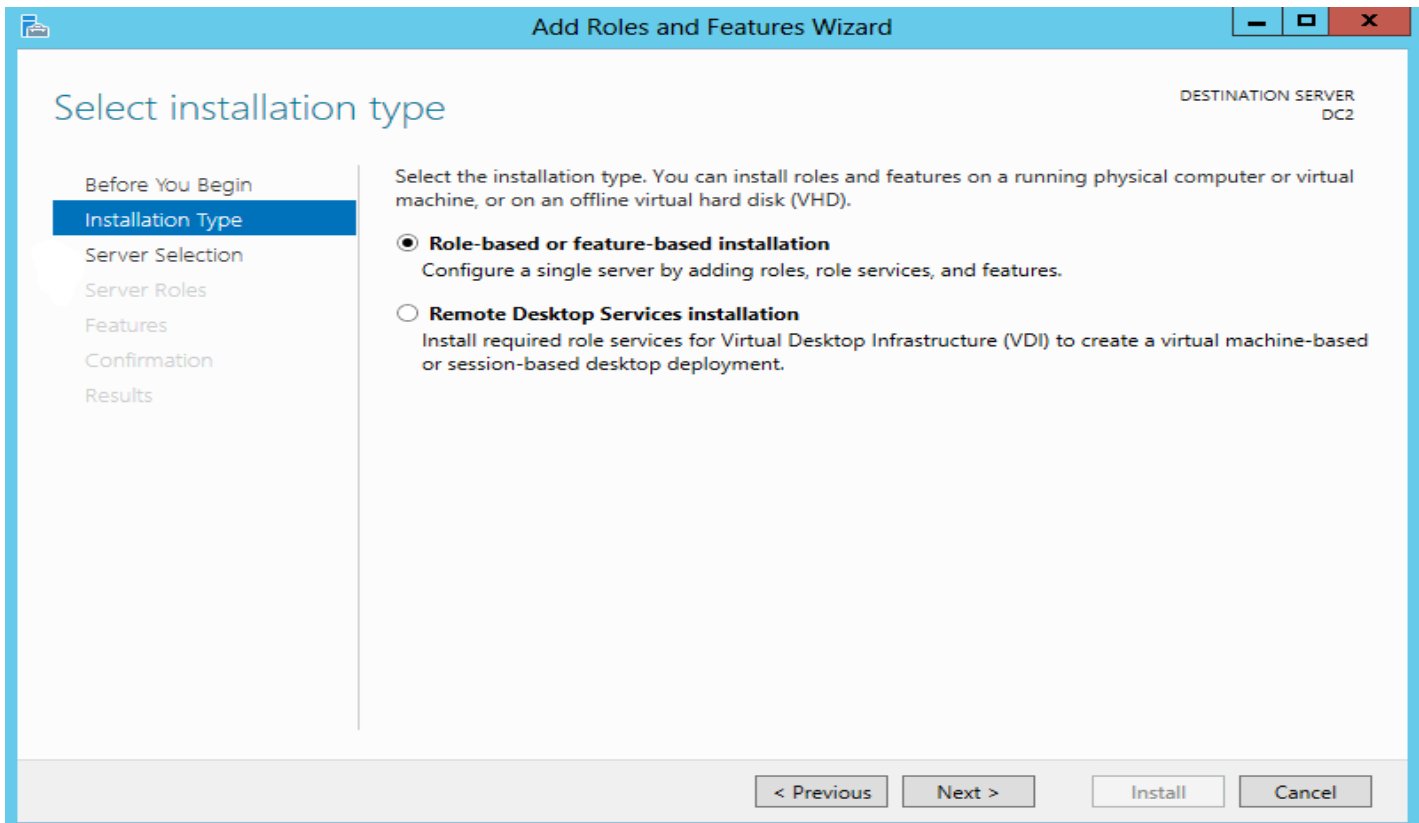
Add roles and features



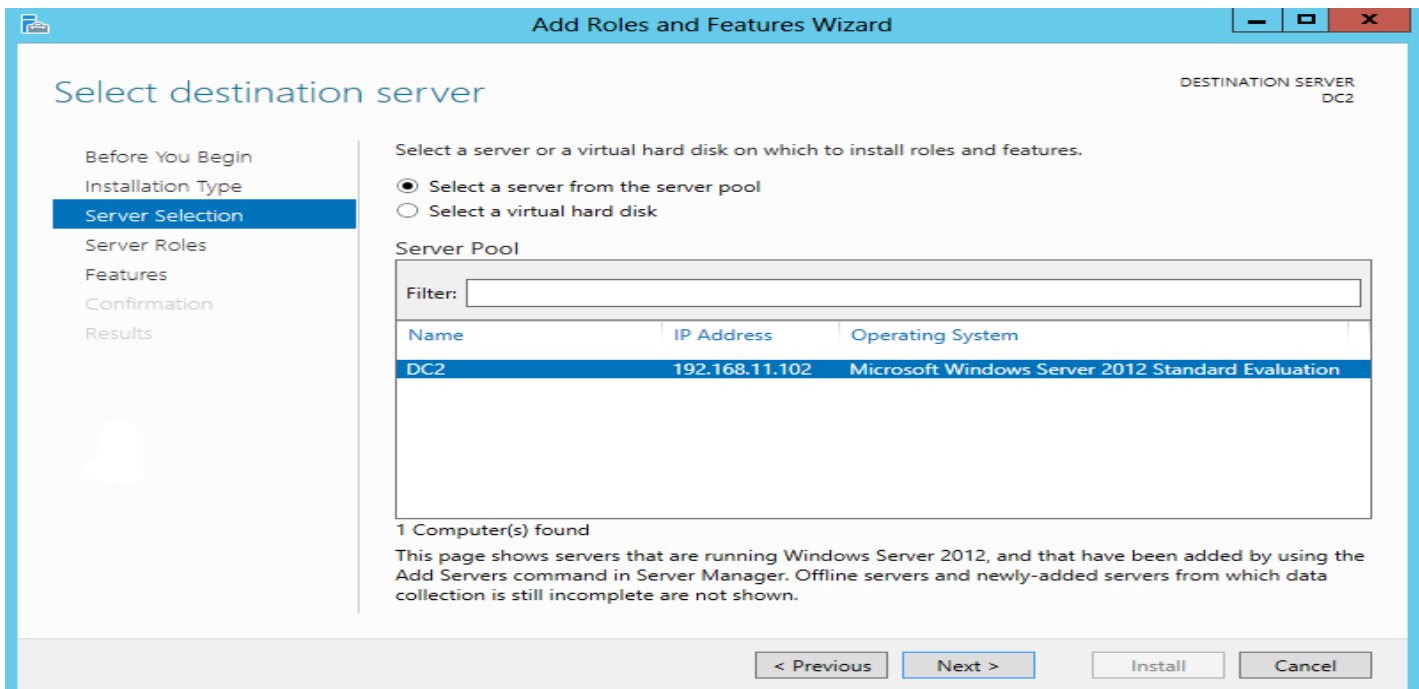
Add roles and features.



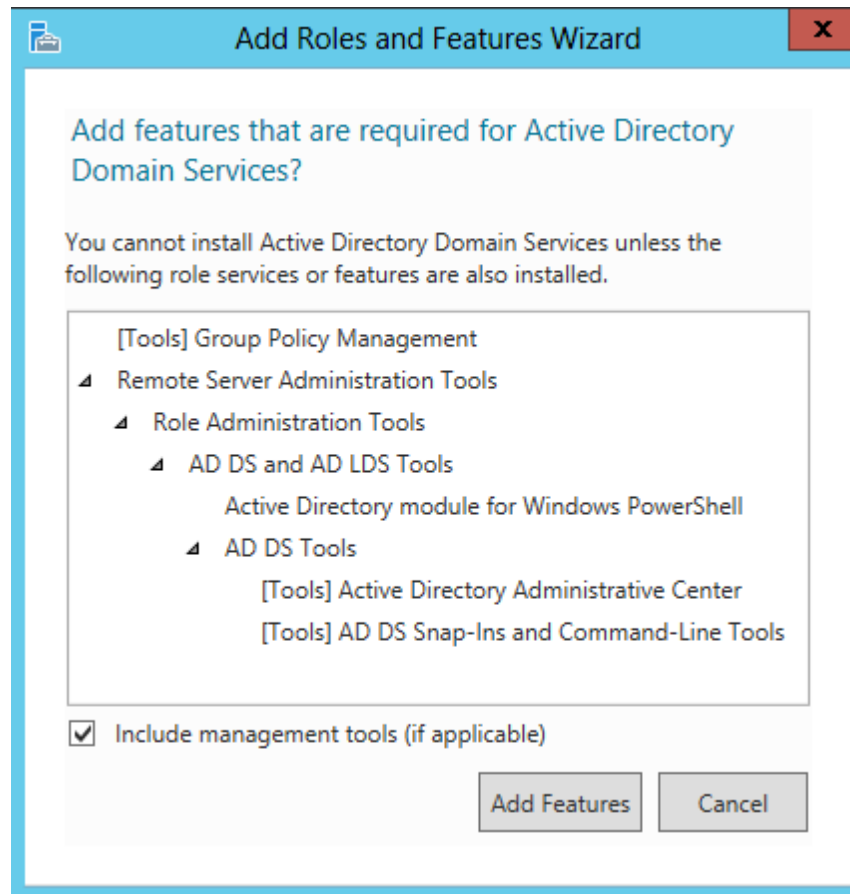
Select first option



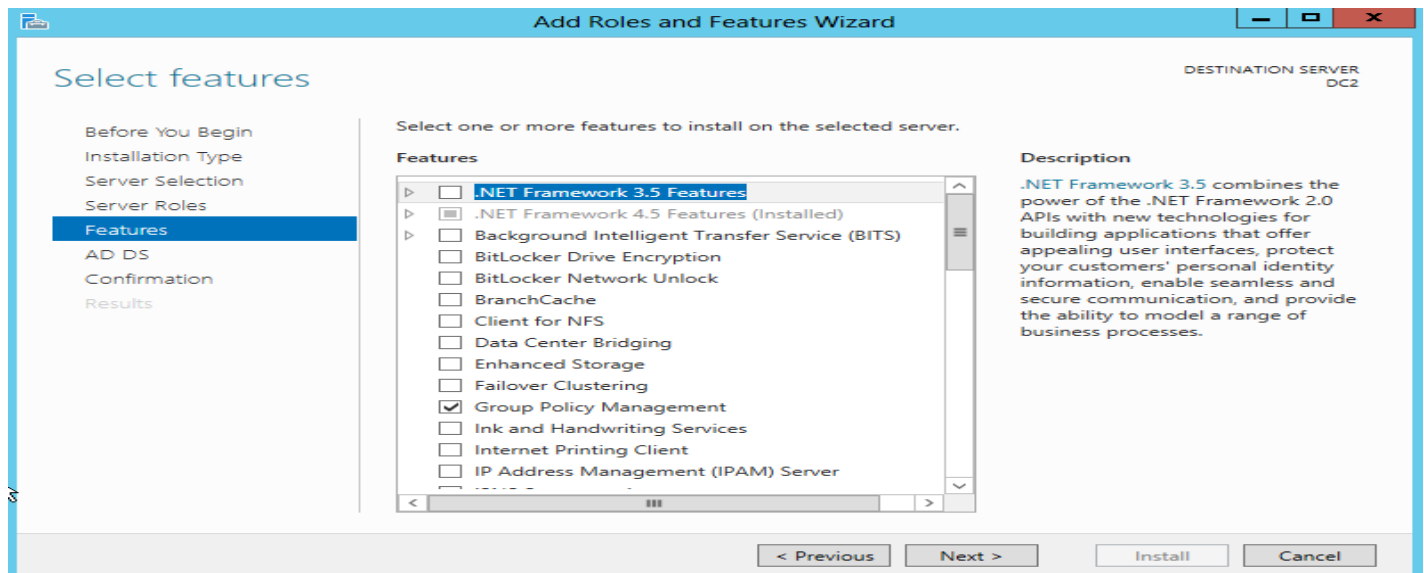
Select the server you wish to promote



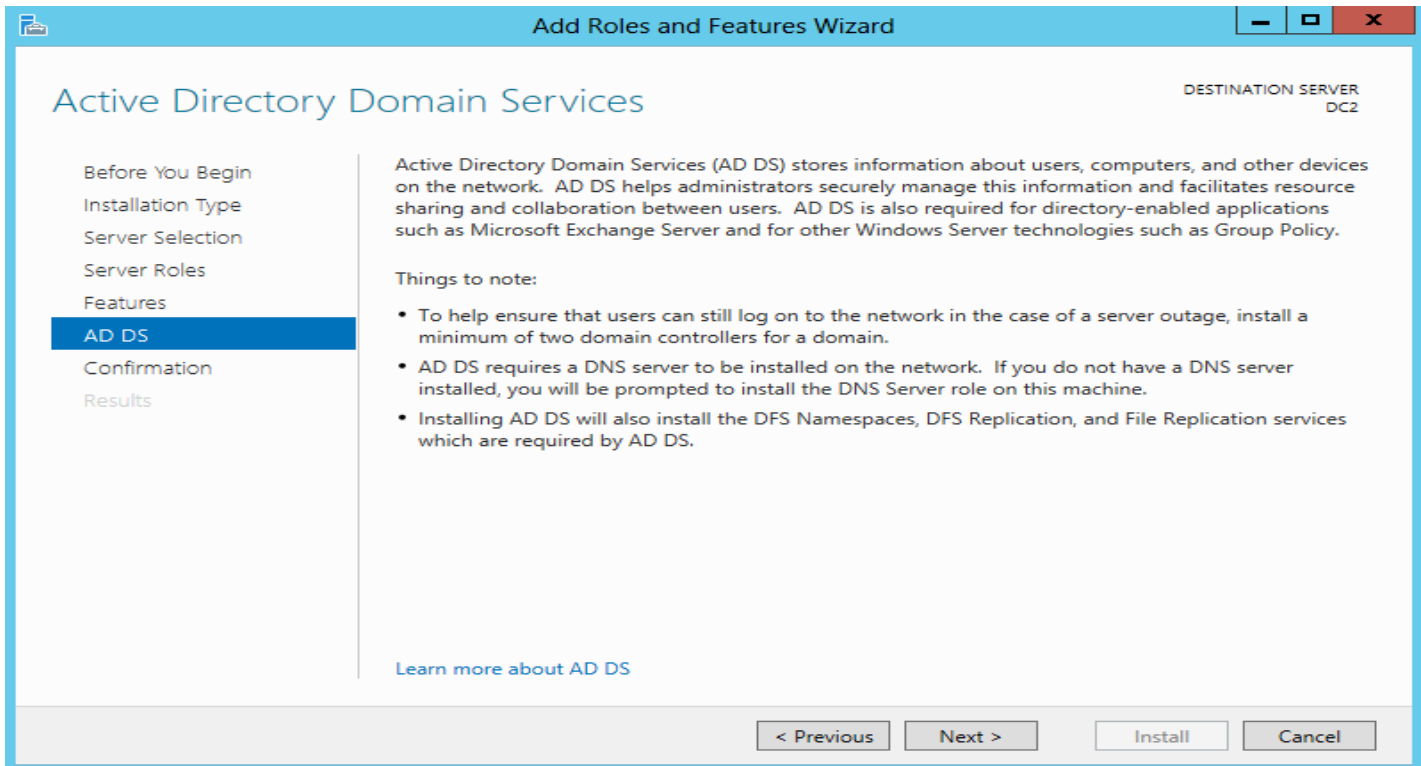
Click Add Features.



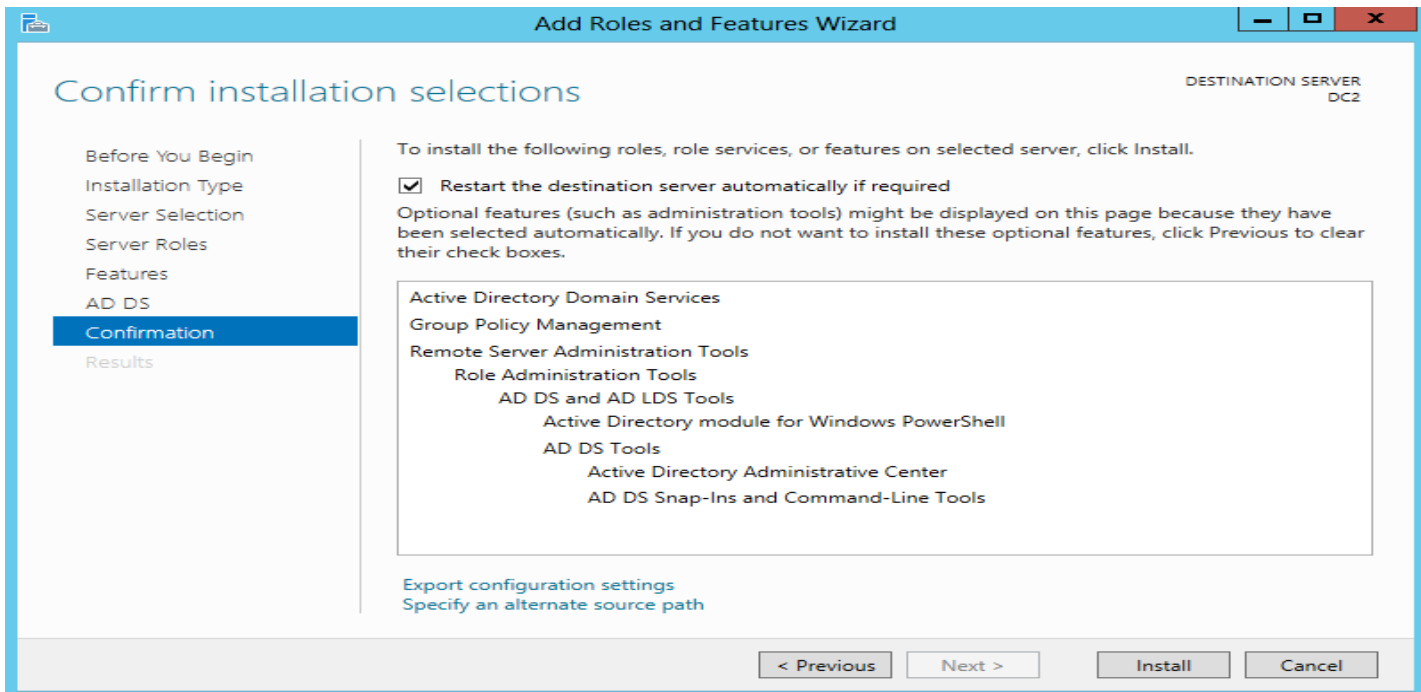
Add features



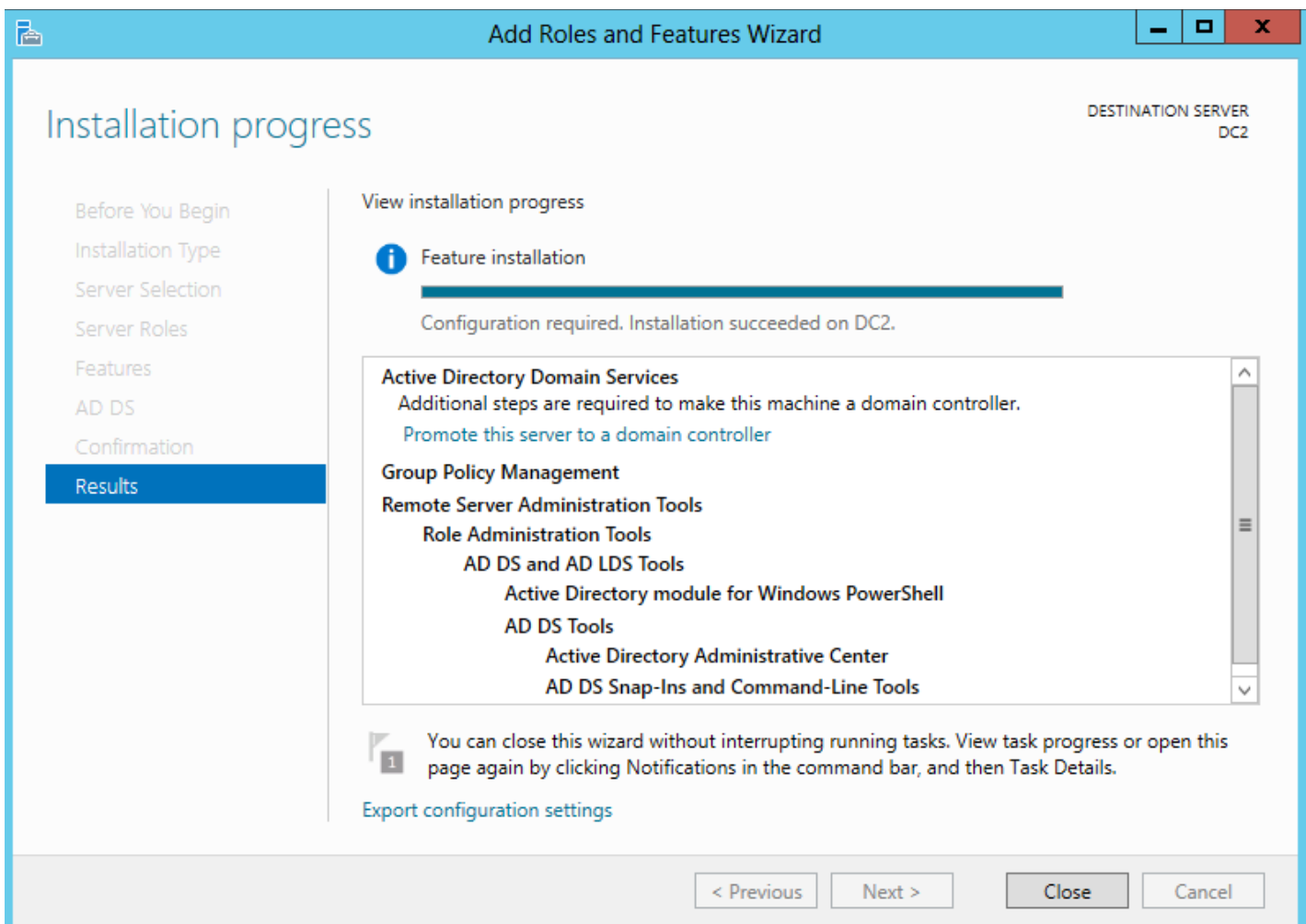
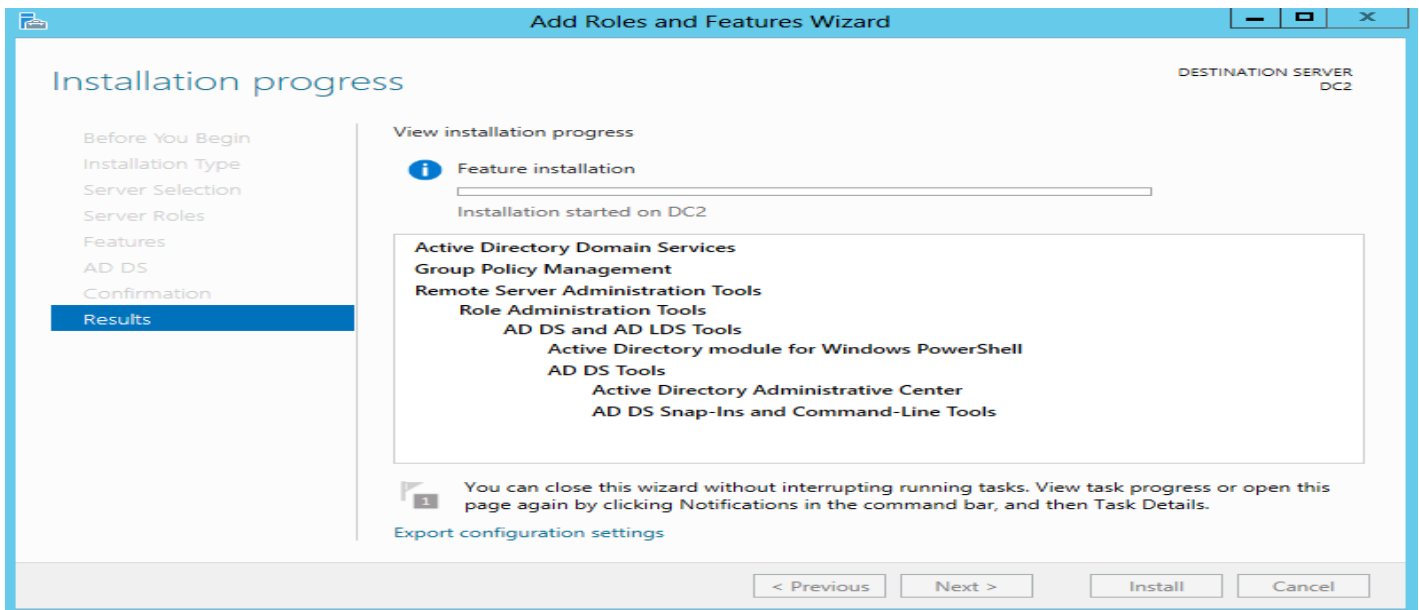
AD DS



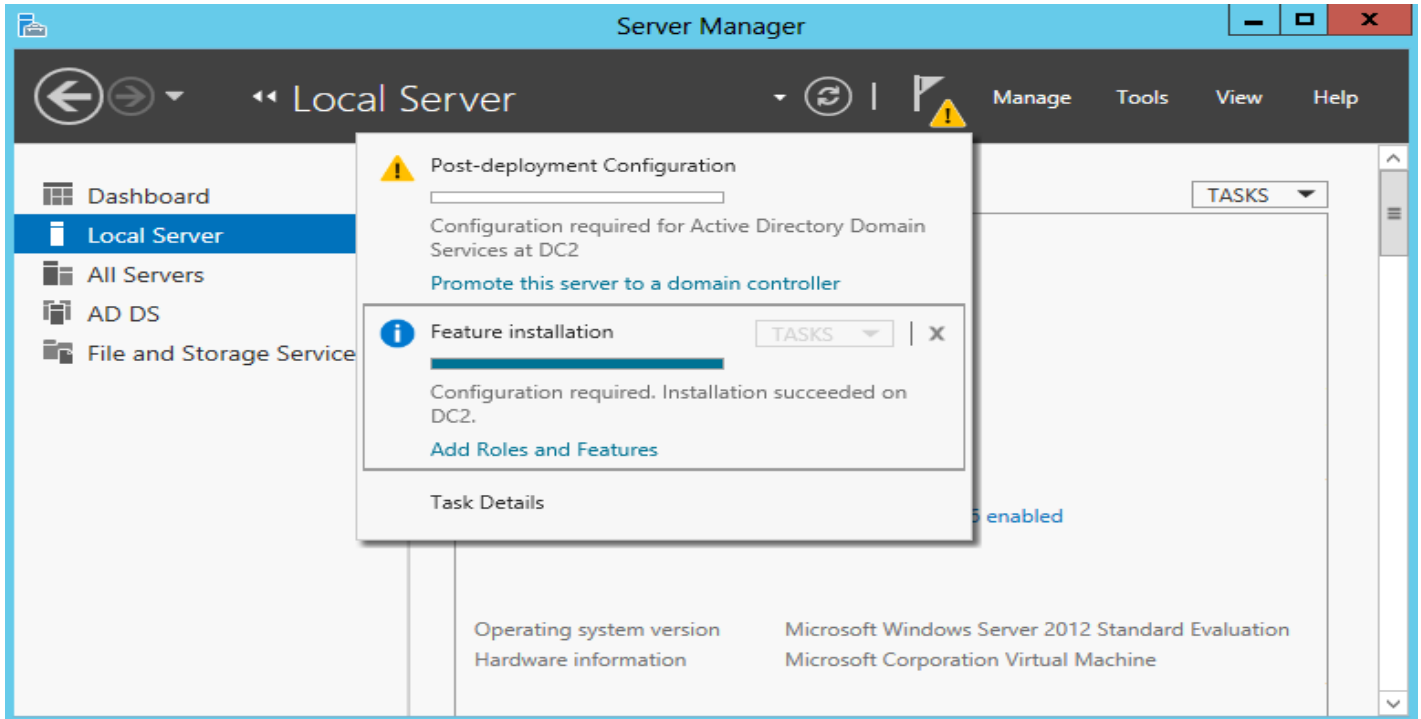
Confirmation



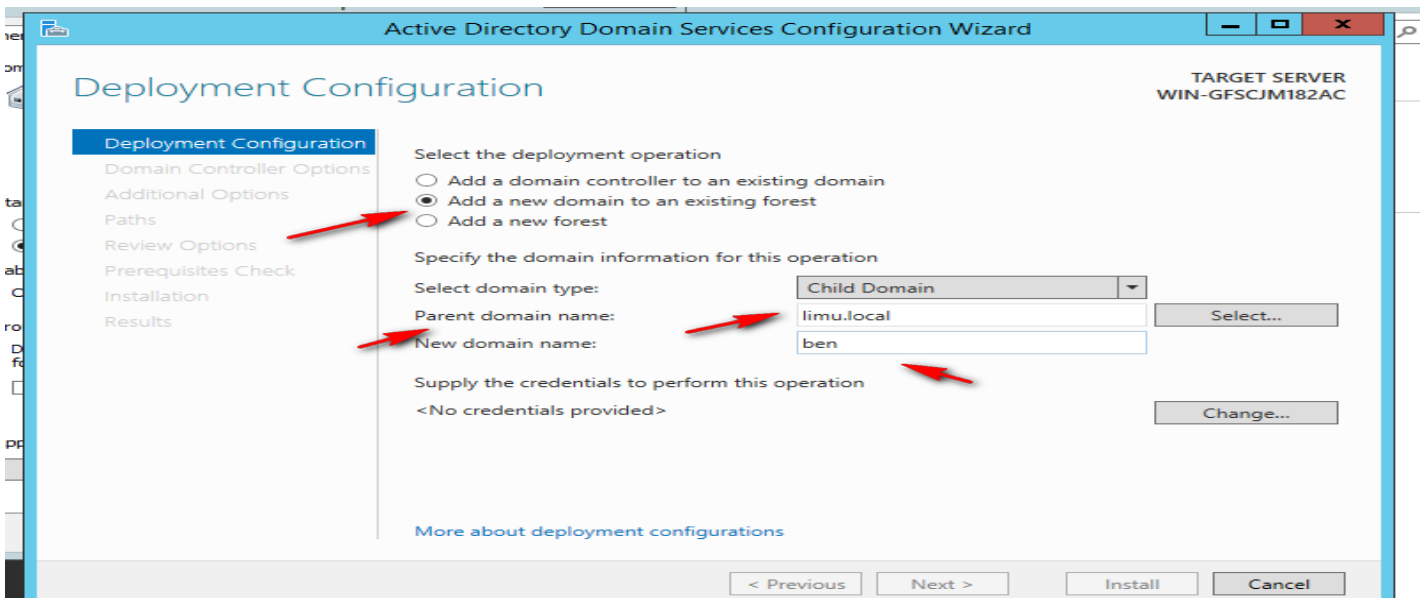
Results



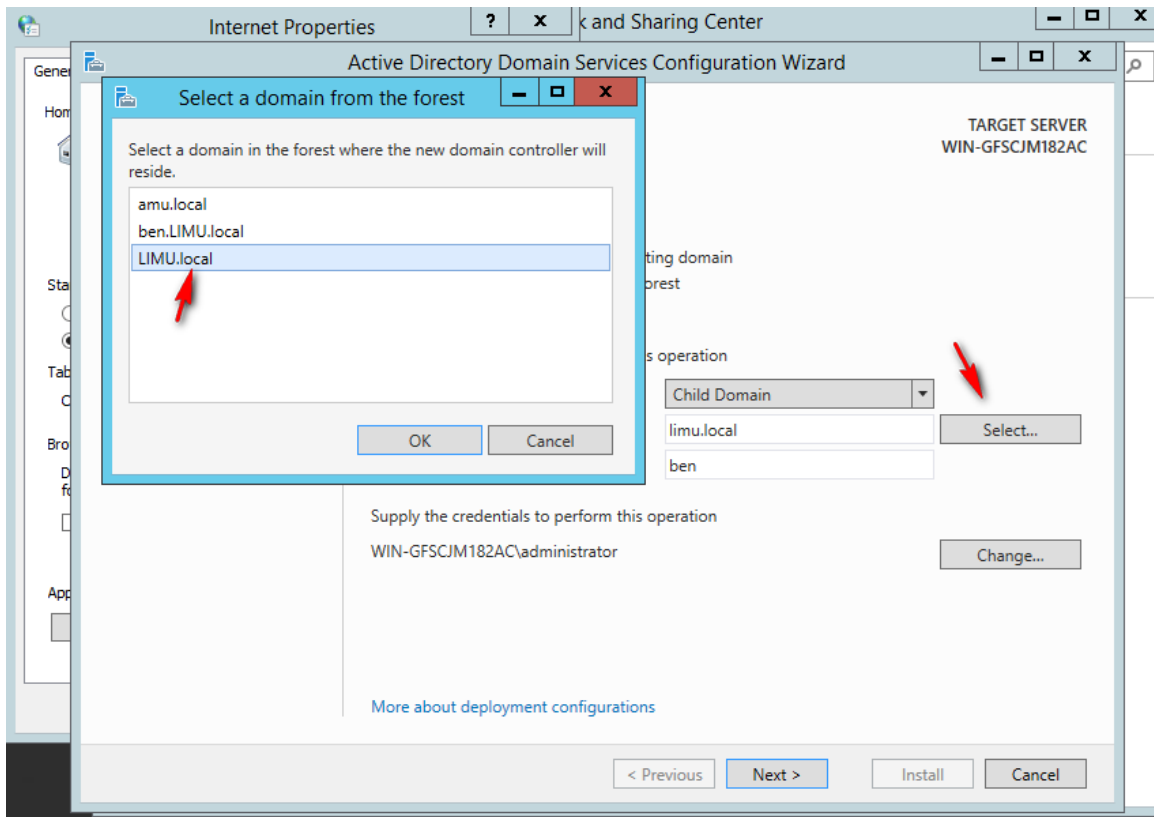
You'll now notice you have a notification, prompting you to promote this server to a domain controller.



Add a new domain to an existing domain



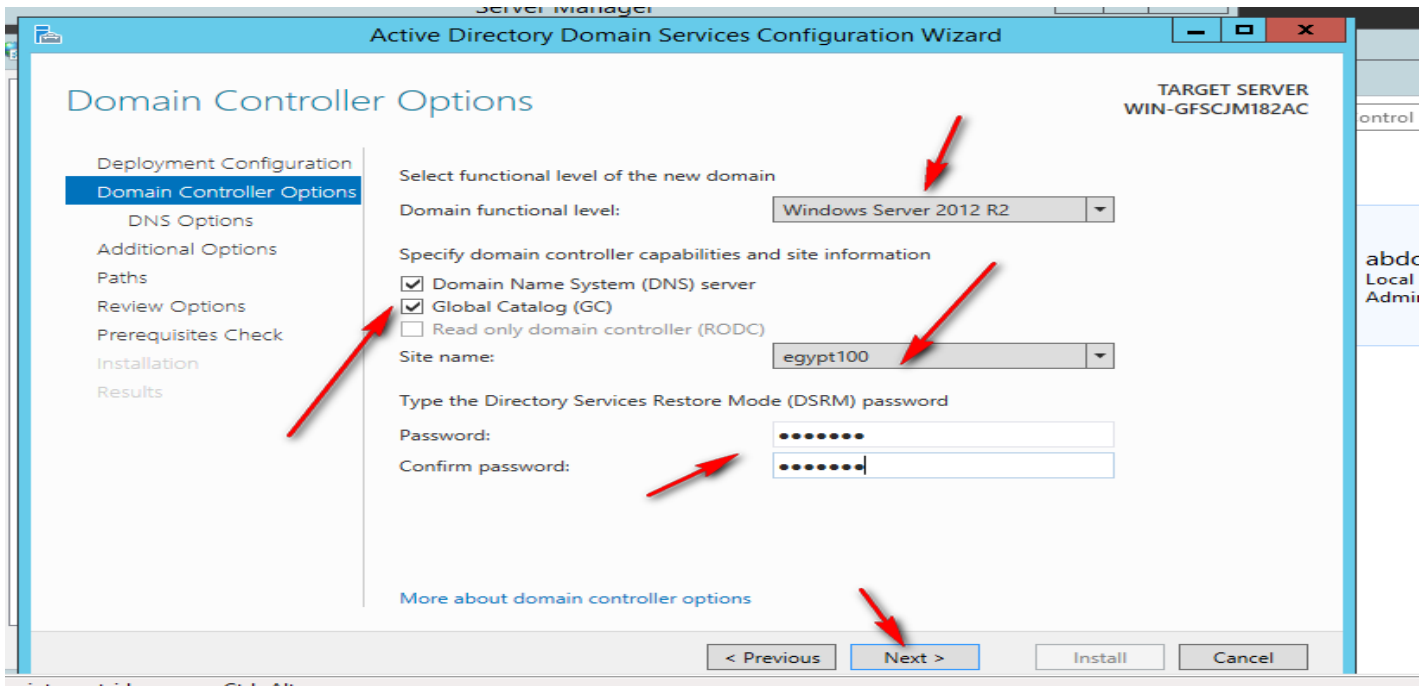
Select parent domain



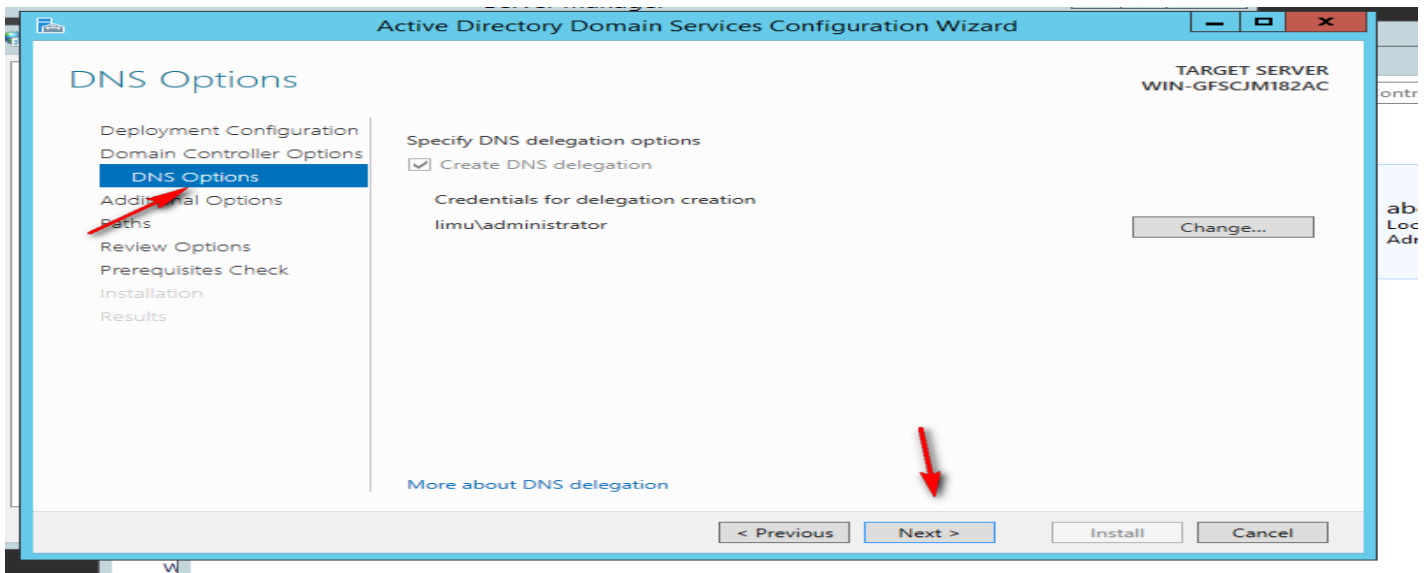
Type Enterprise password for admin



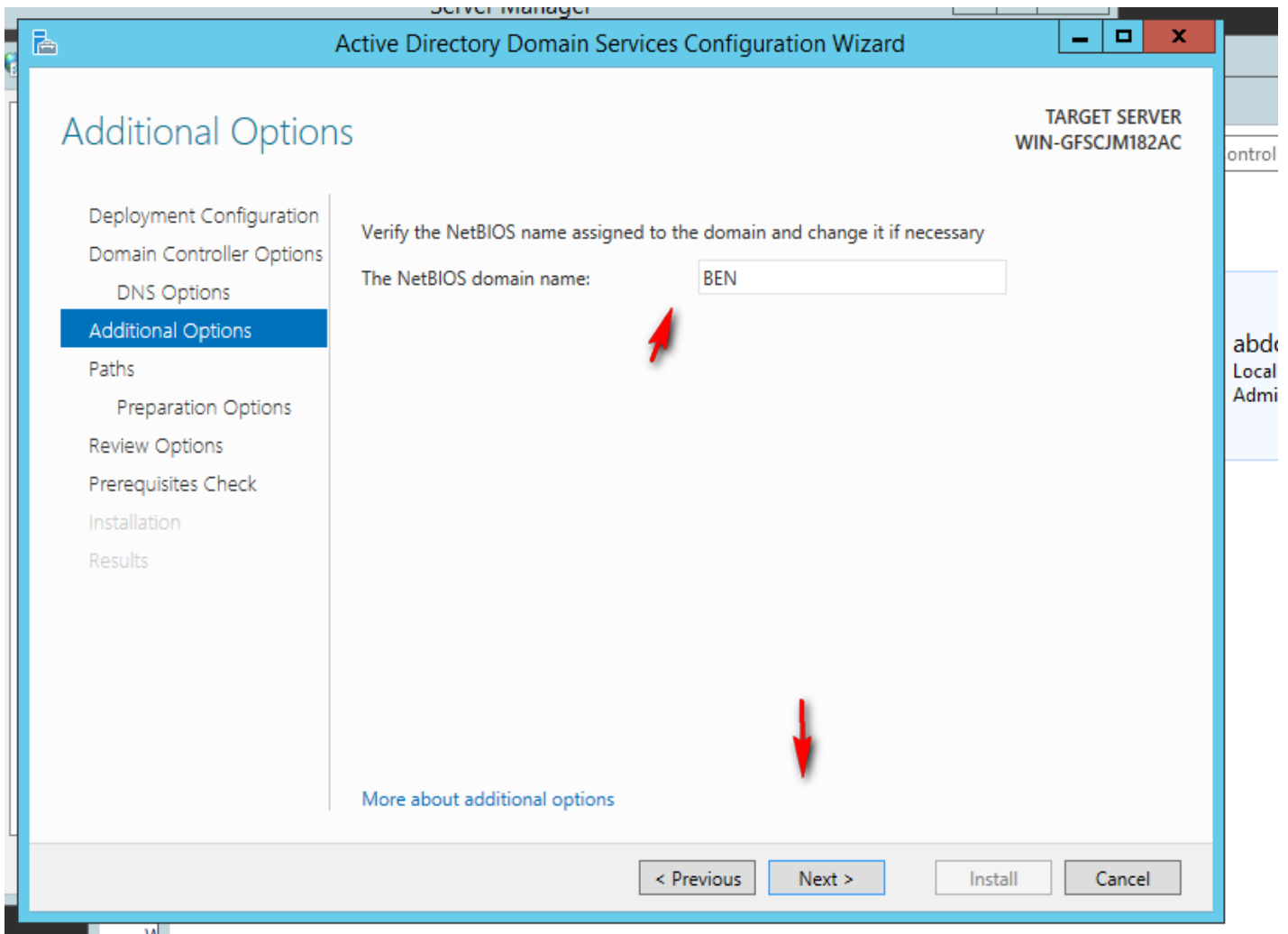
Choice the following then next



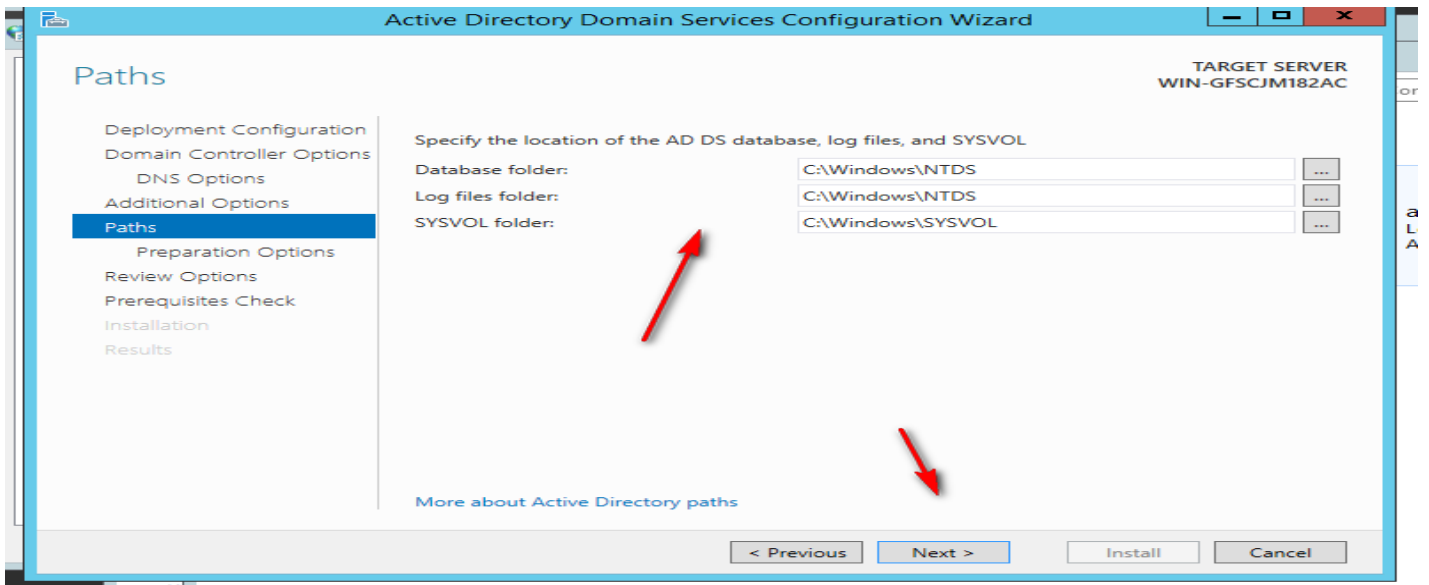
Next



Netbios domain name



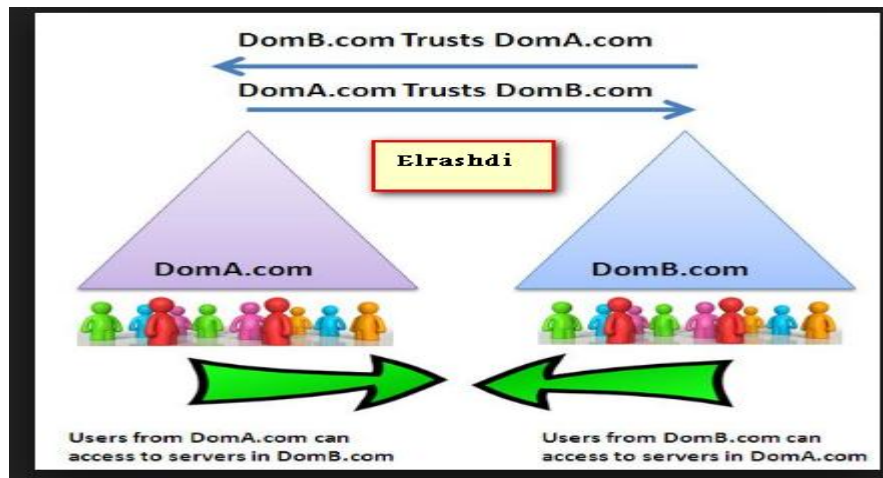
Next then finish



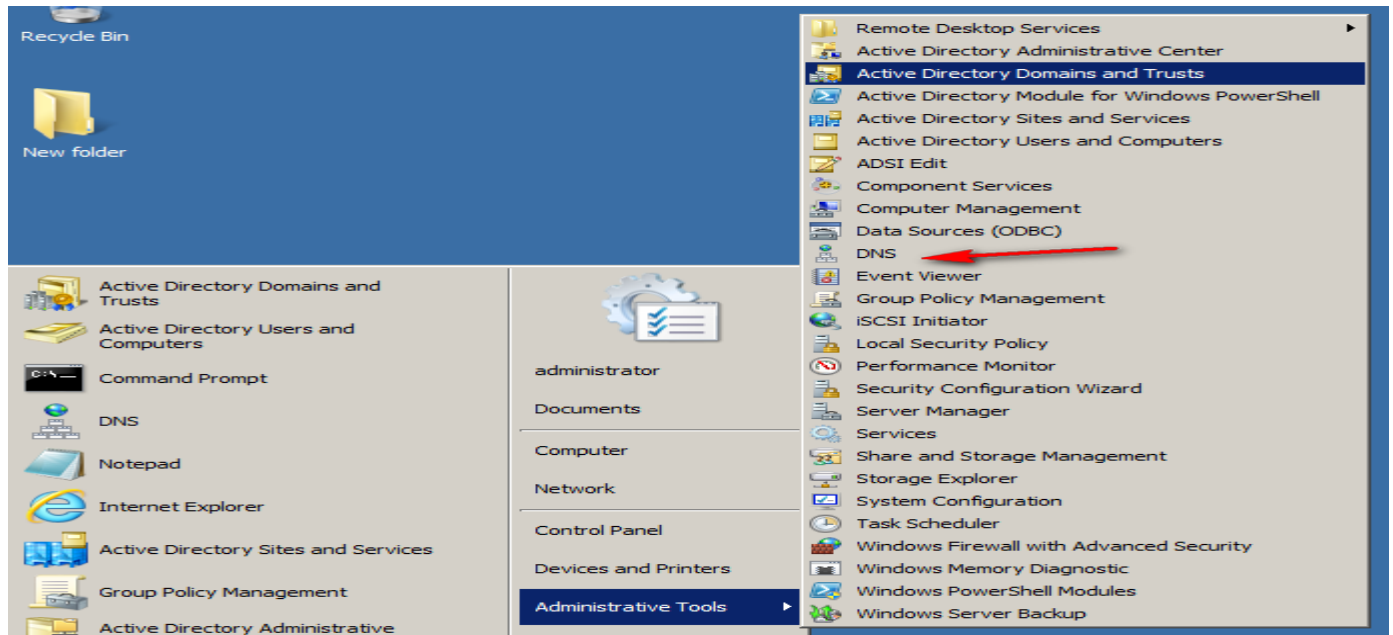
29-Trust between domains

احيانا يكون عندنا اكثر من مجال في forests مختلفة ونريد ان يكون هناك علاقة ثقة وتوثيقية بين هذه المجالات المختلفة بحيث يتم تبادل البيانات والمعلومات بشكل سلسل وبدون أي تعقيدات .

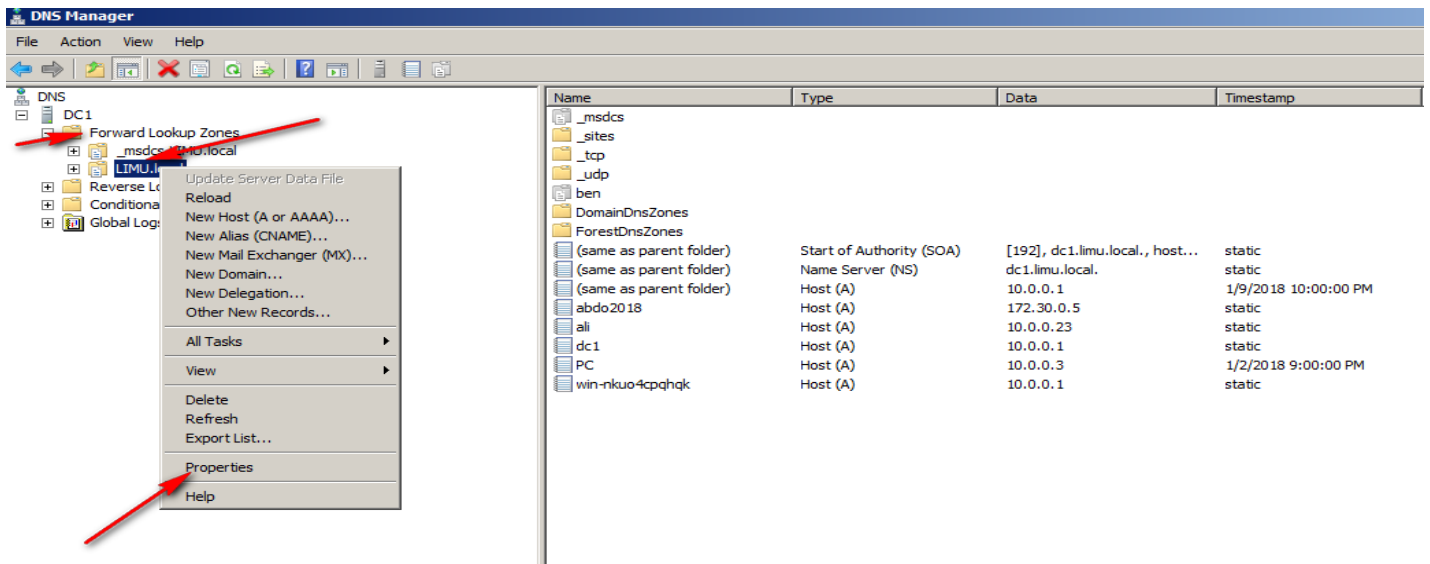
You can link two disjointed Active Directory Domain Services (AD DS) forests together to form a one-way or two-way, transitive trust relationship. You can use a two-way, forest trust to form a transitive trust relationship between every domain in both forests.



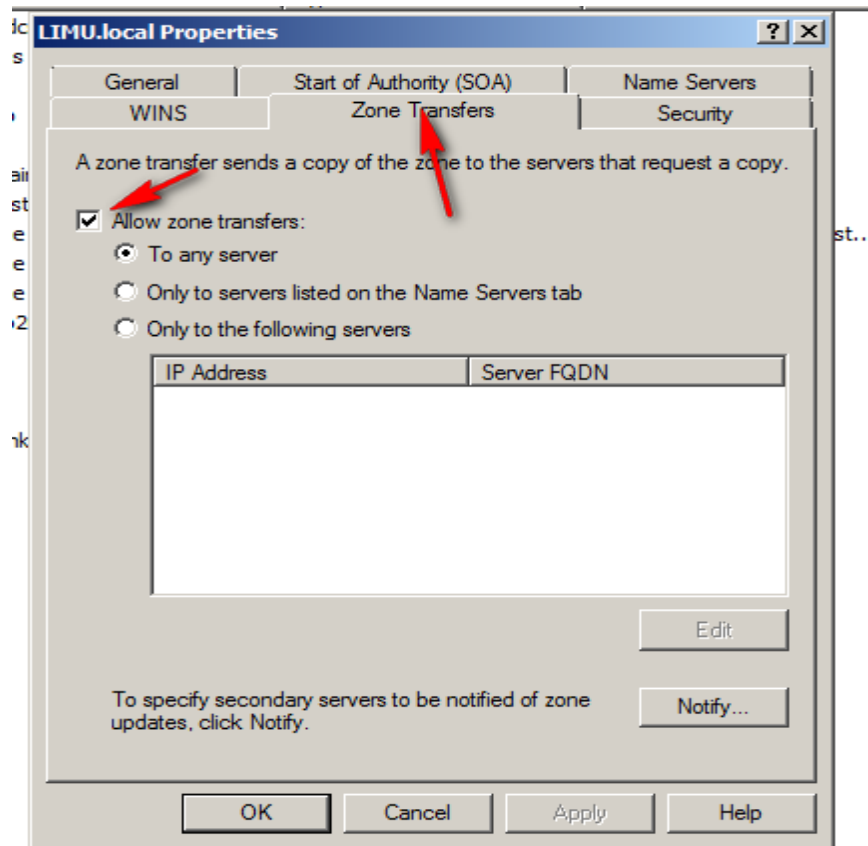
First open DNS



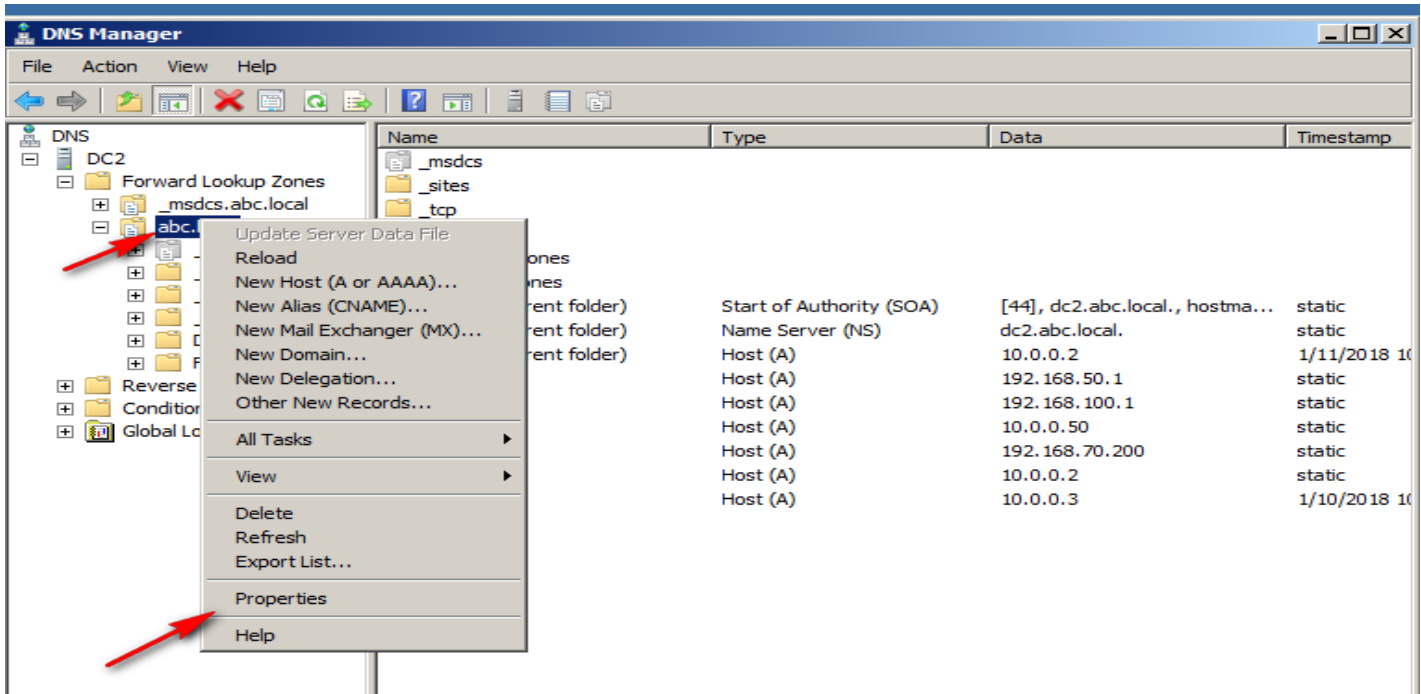
First on domain controller of limu domain Open forward lookup zones the properties of limu.local



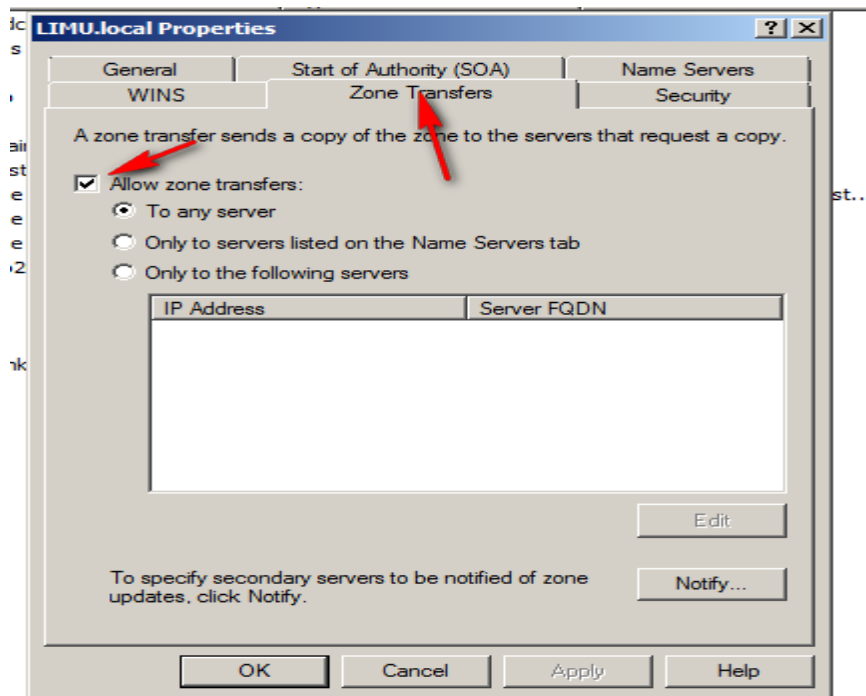
Zone transfers then allow zone transfers



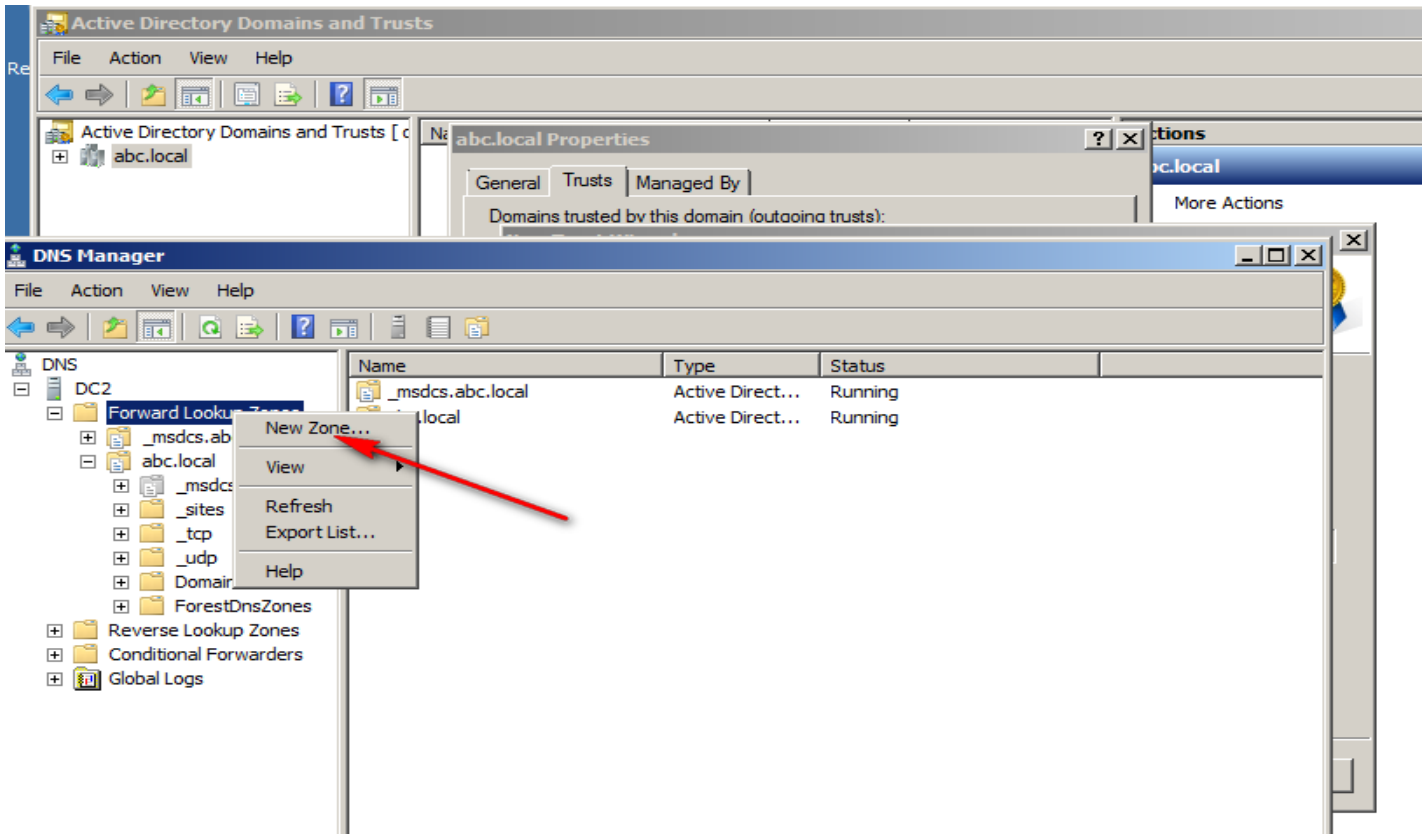
Second on domain controller of ABC domain Open forward lookup zones the properties of abc.local



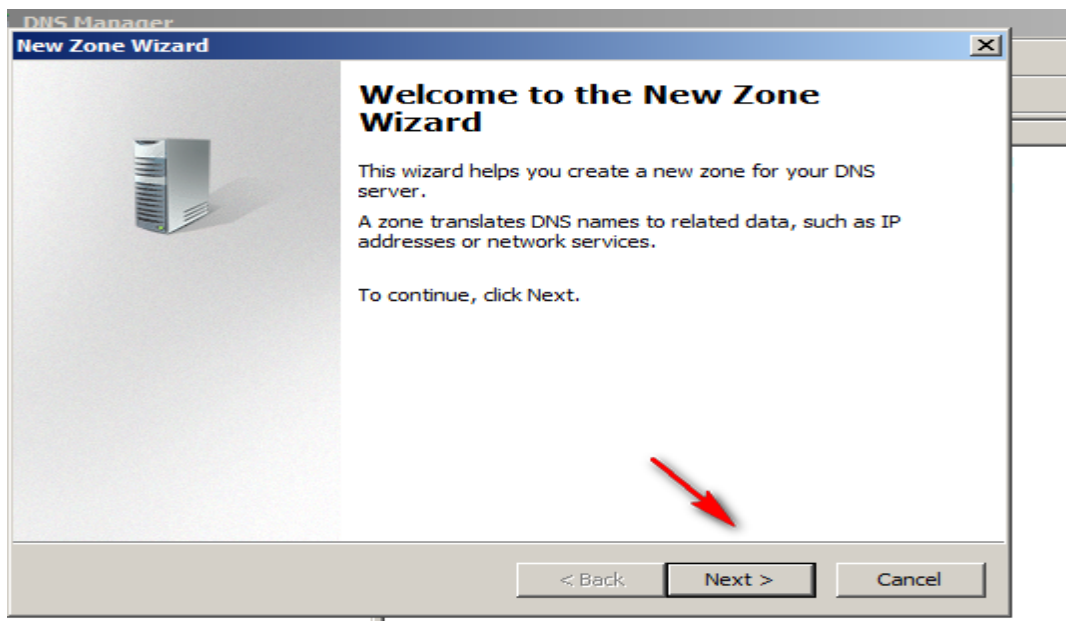
Zone transfers then allow zone transfers



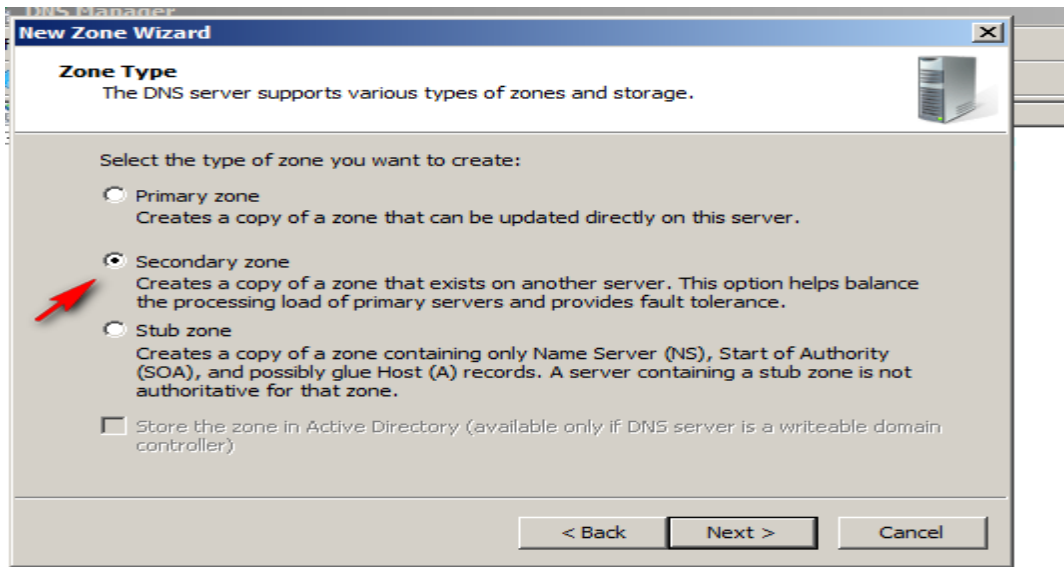
On abc domain Open the DNS then new zone



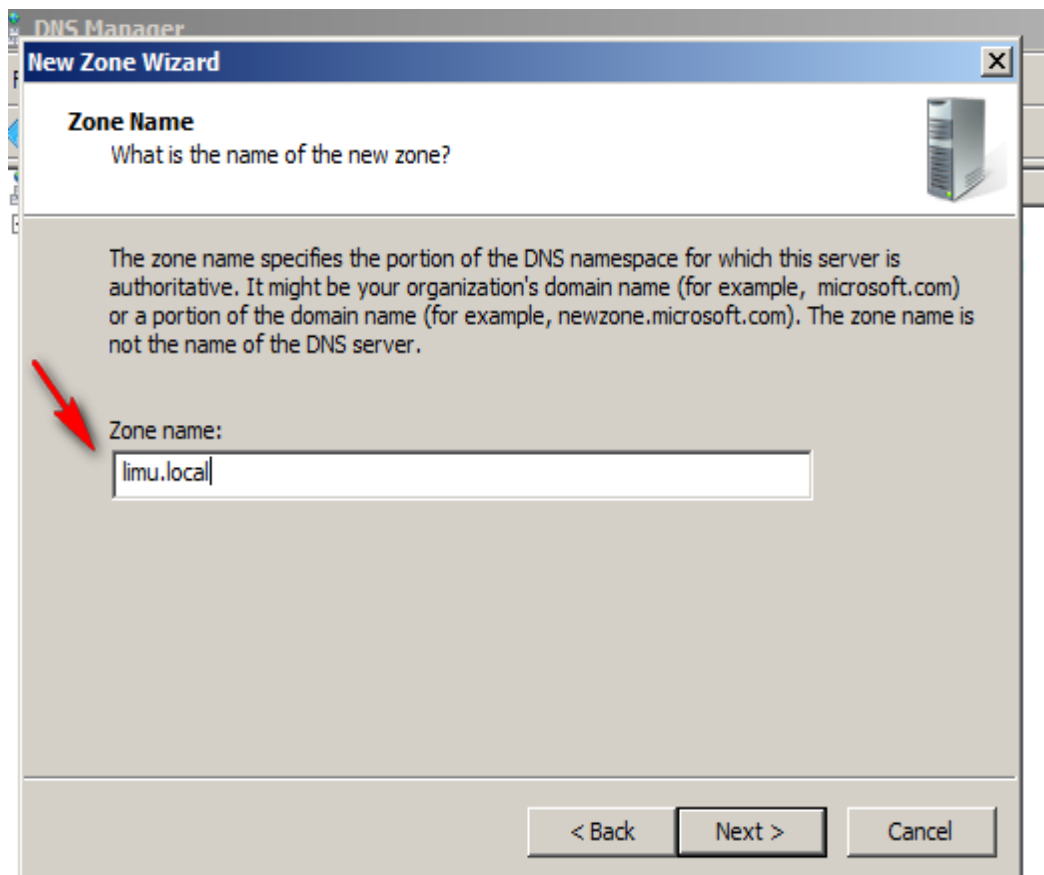
Next



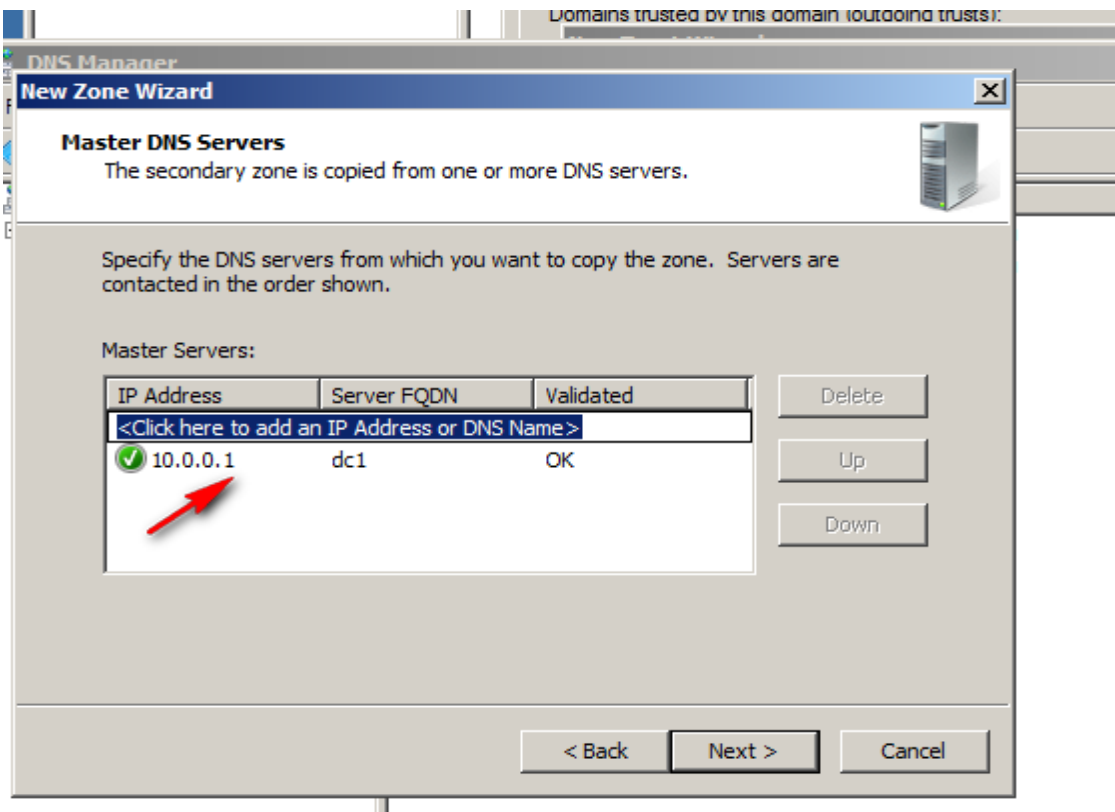
Secondary zone



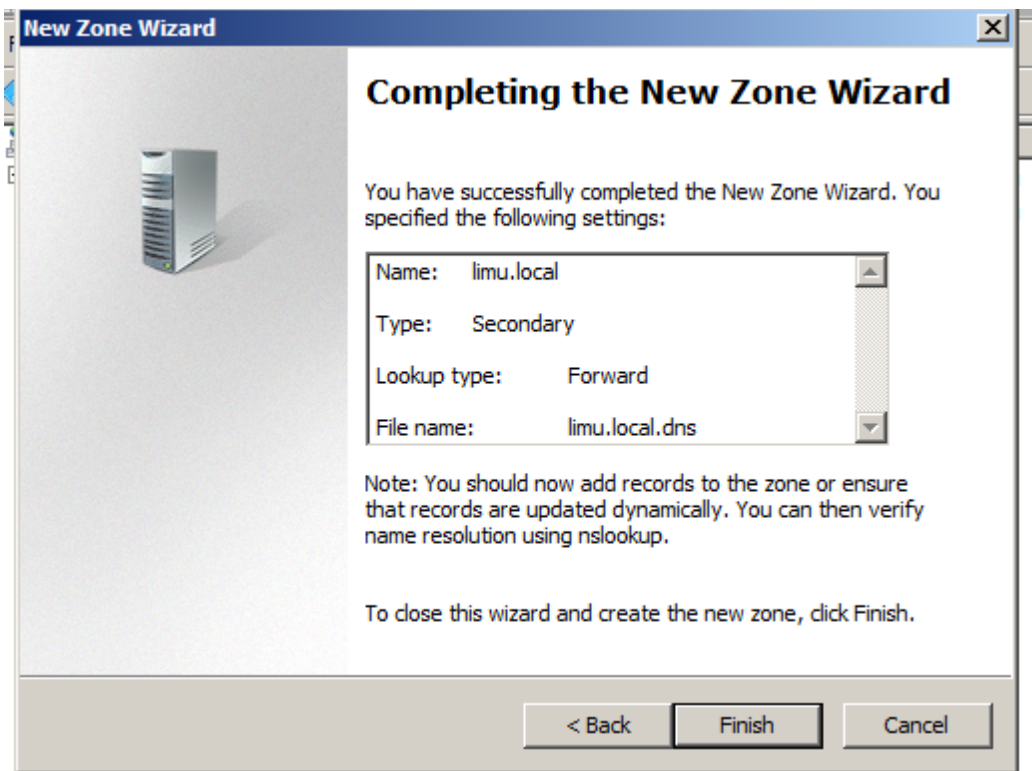
Type name of primer zone in another domain



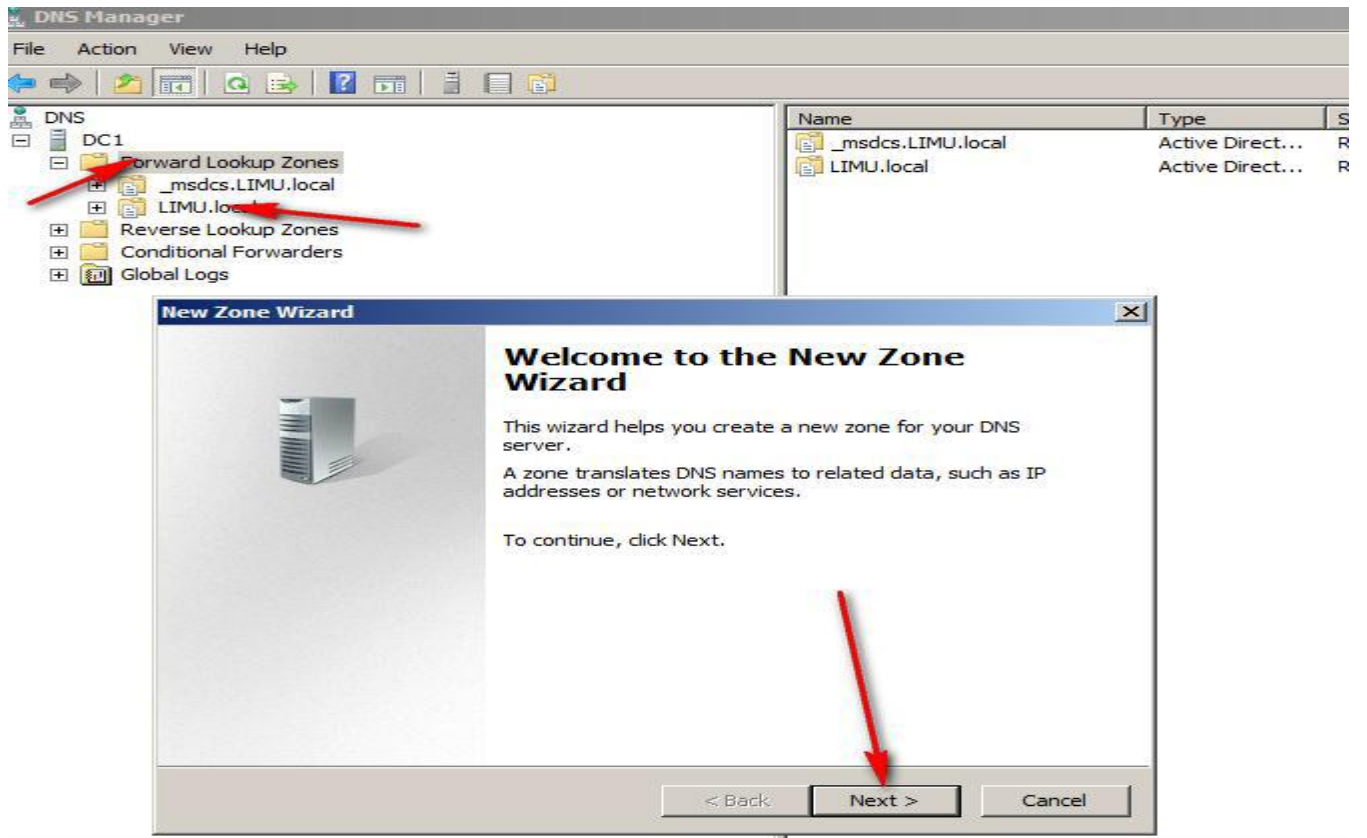
Ip address of another domain



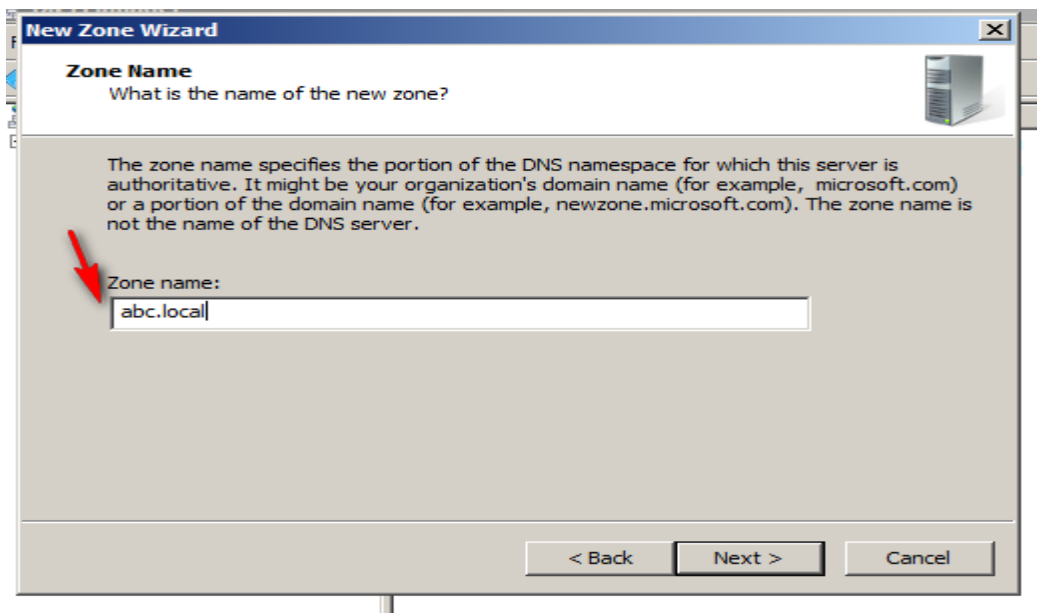
Finish



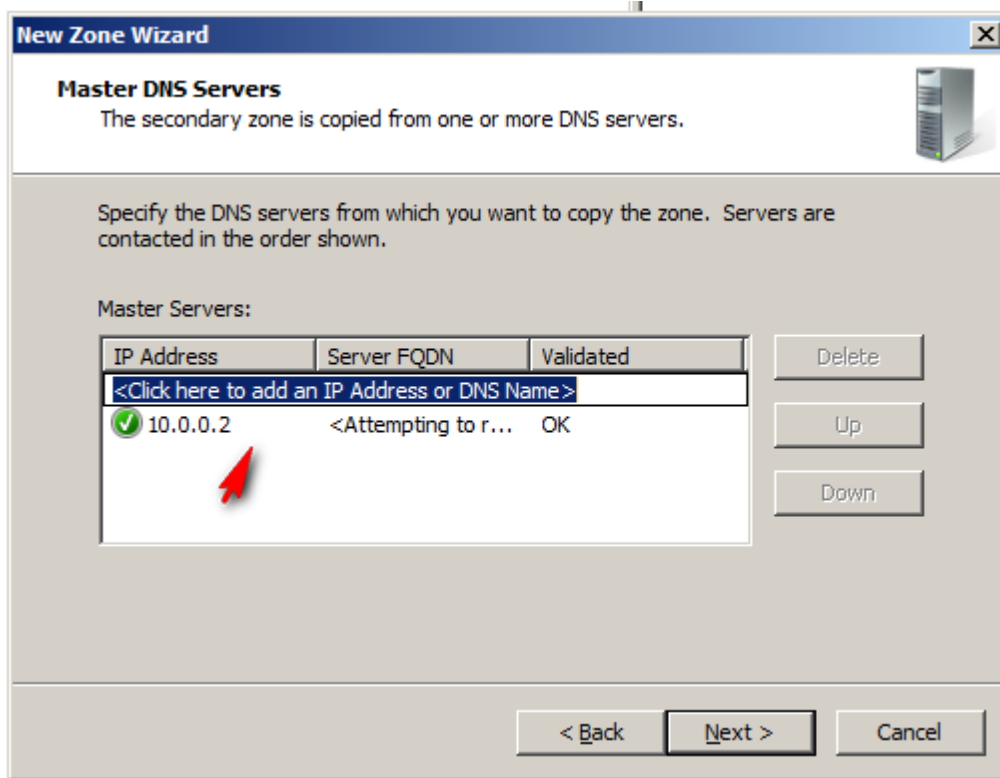
Same in limu.local domain



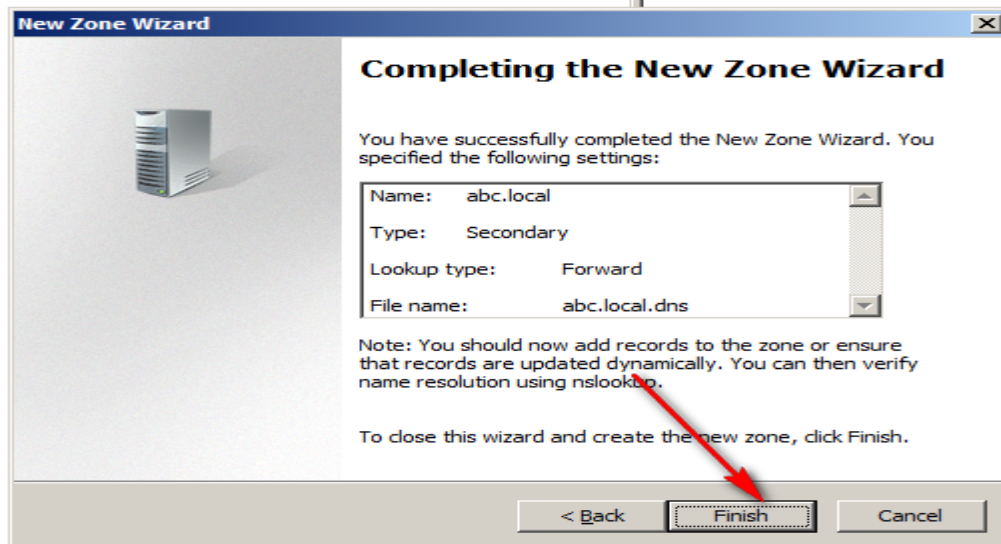
Zone name



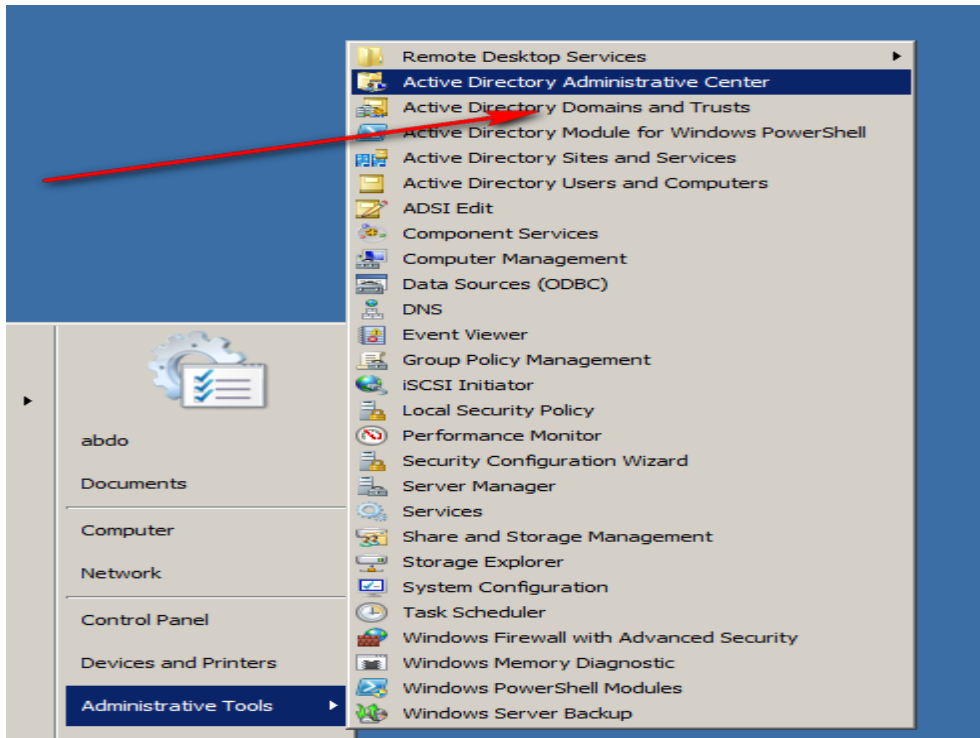
Ip address of another domain



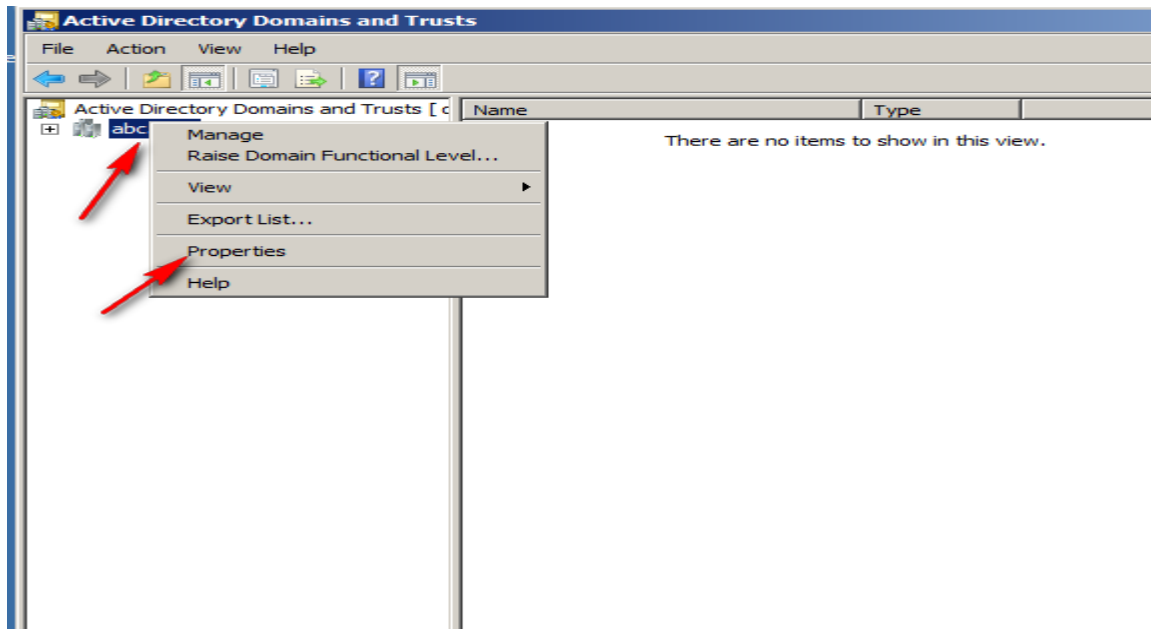
Finish



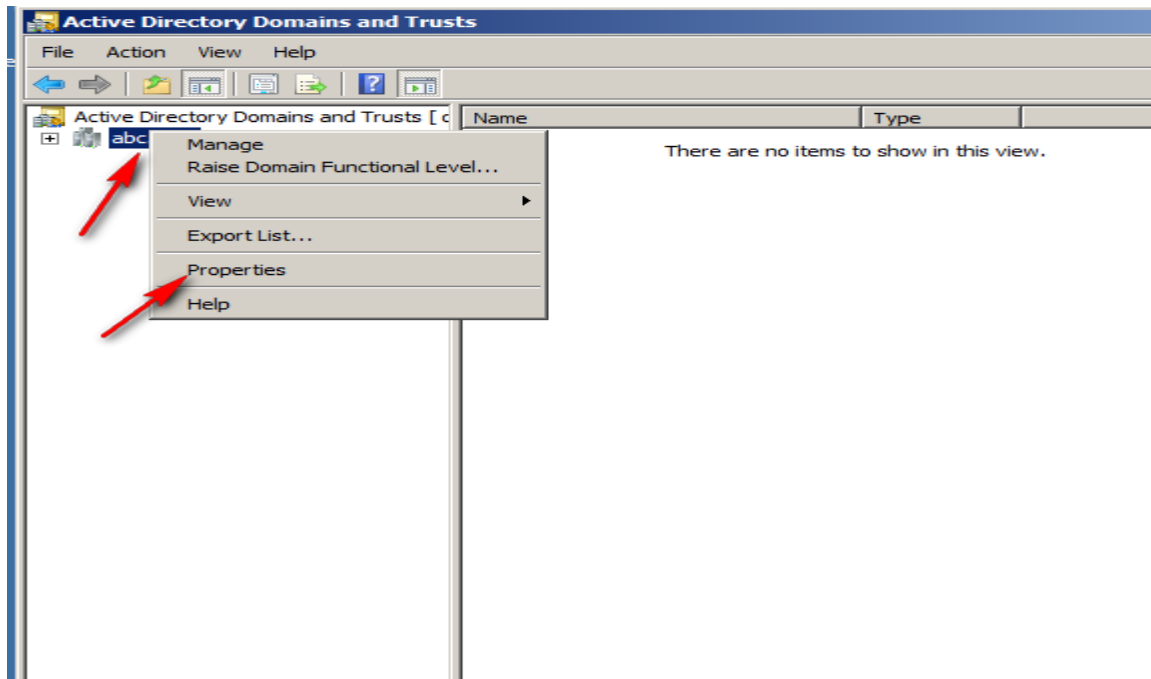
Open active directory domains and trusts



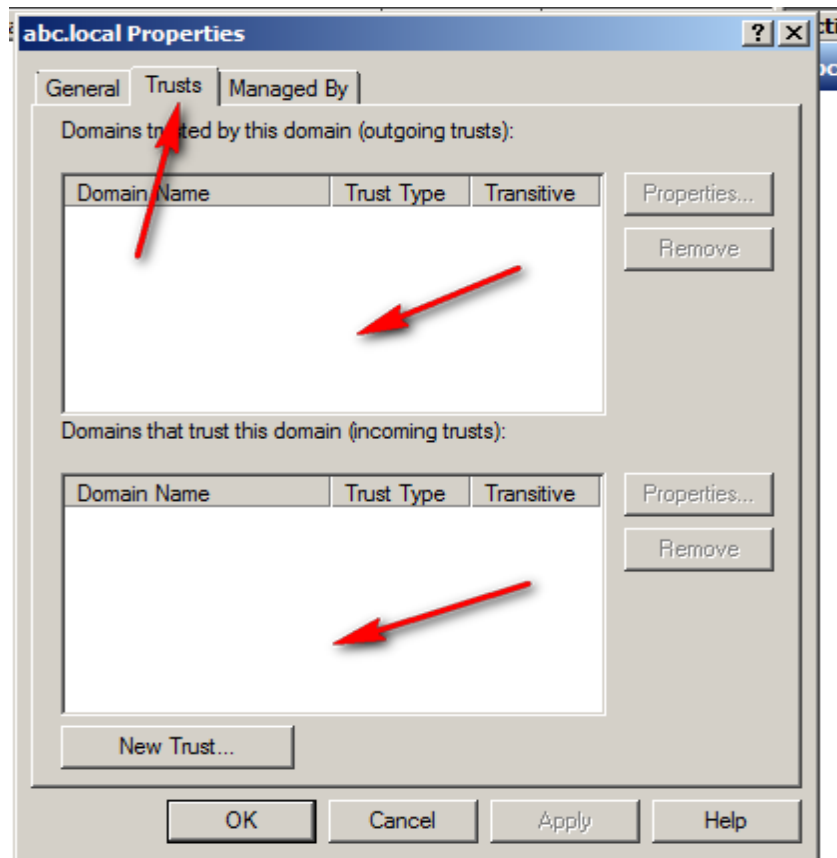
On abc domain Properties of abc.local



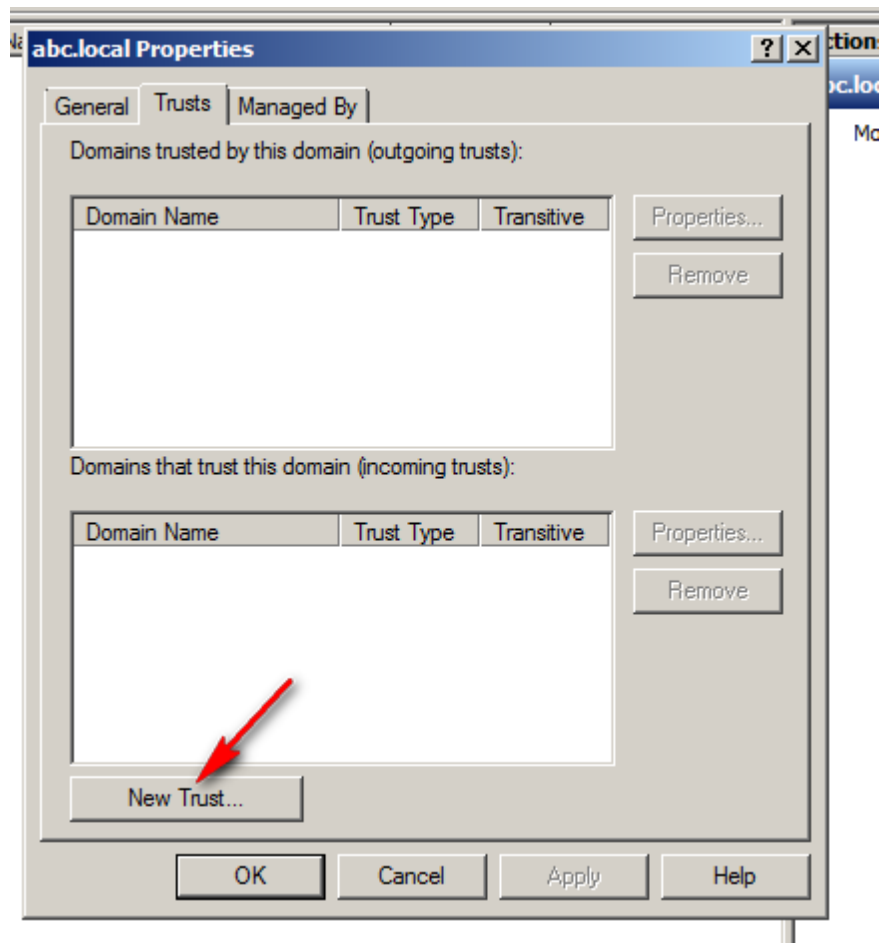
On abc domain Properties of abc.local



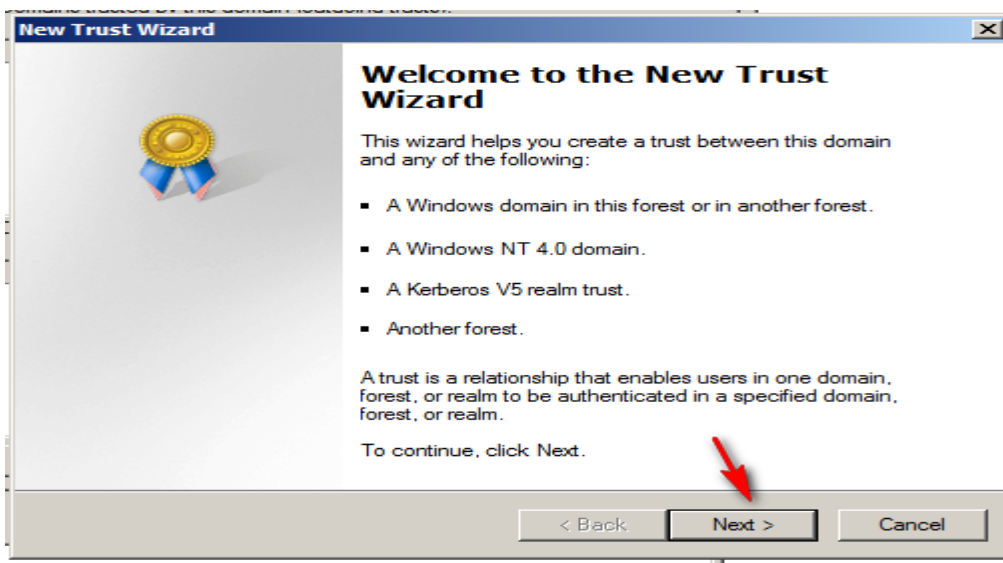
Trusts



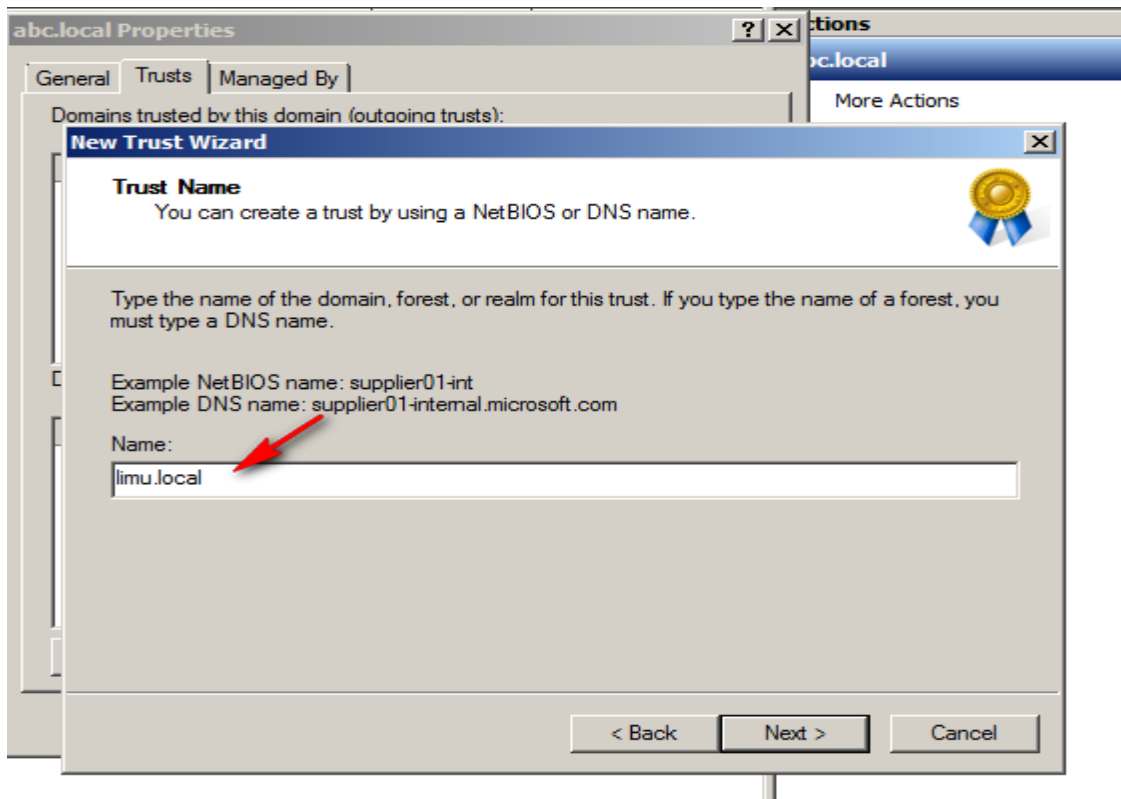
New trust



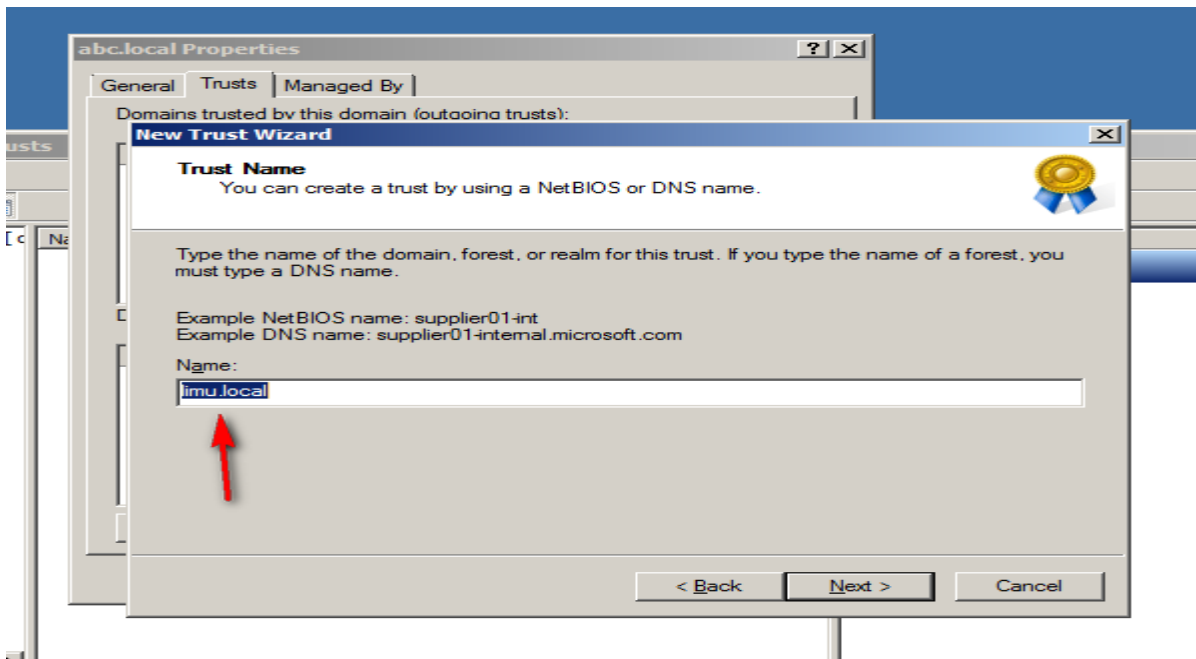
Next



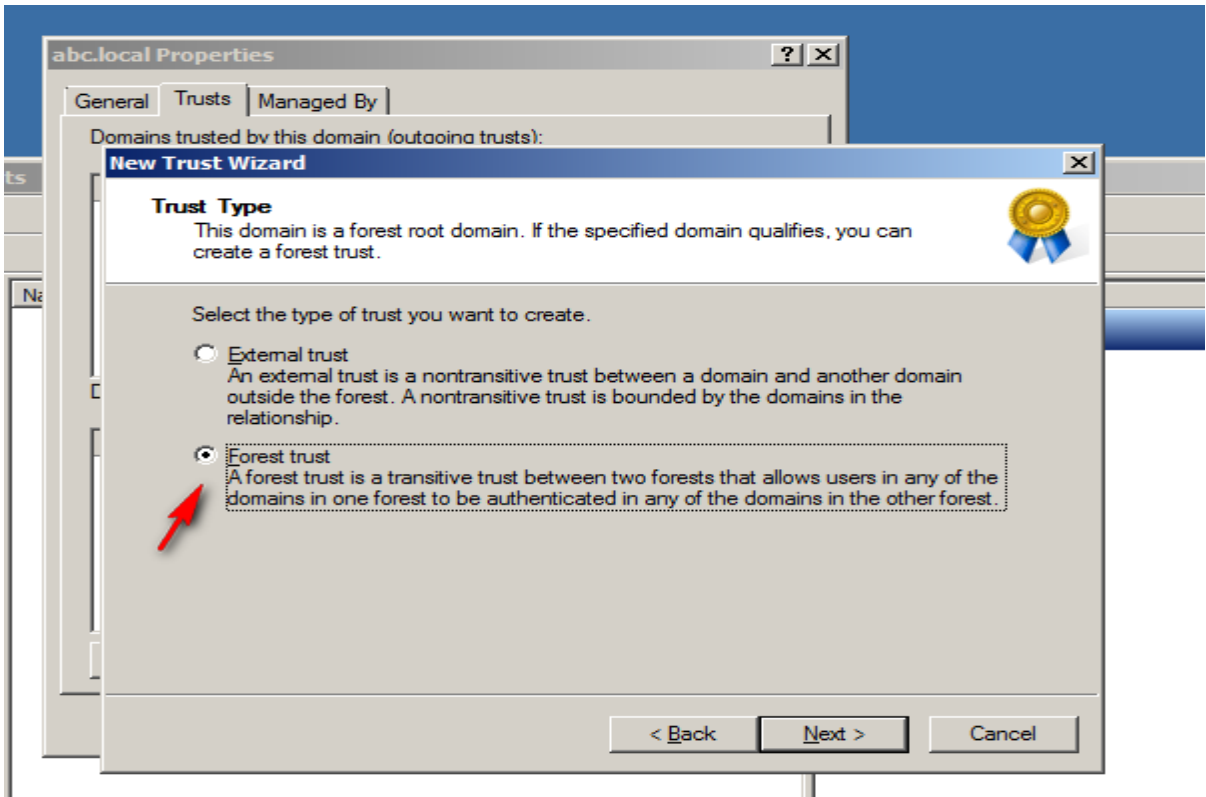
Type name of another domain



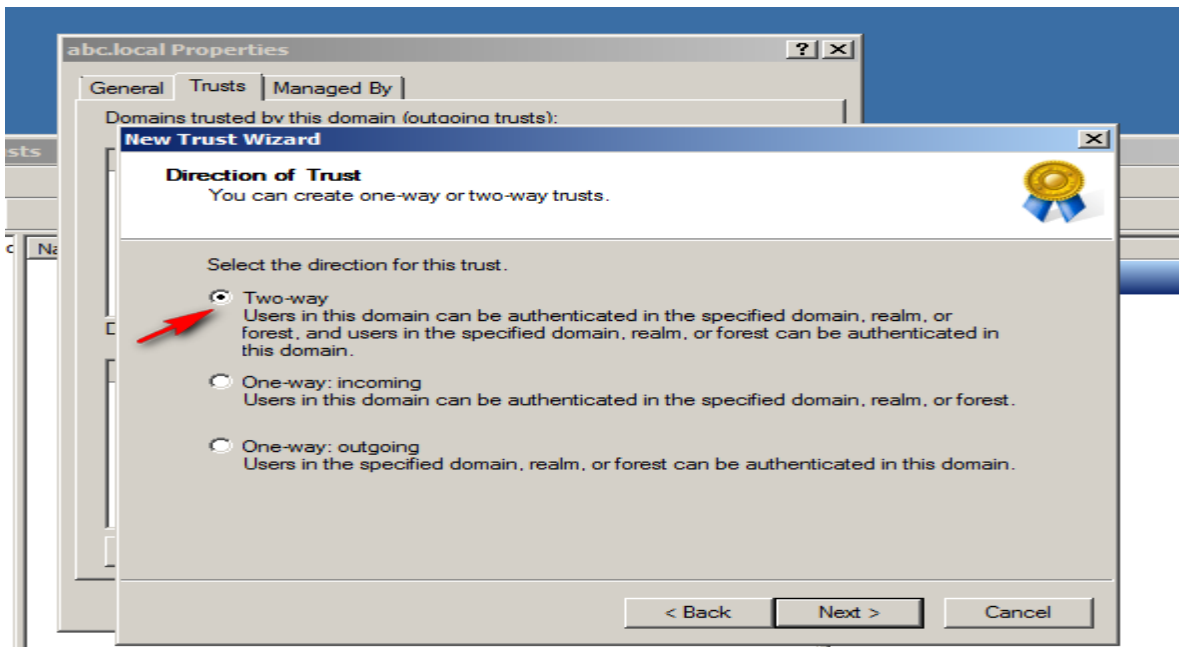
On abc domain complete the steps



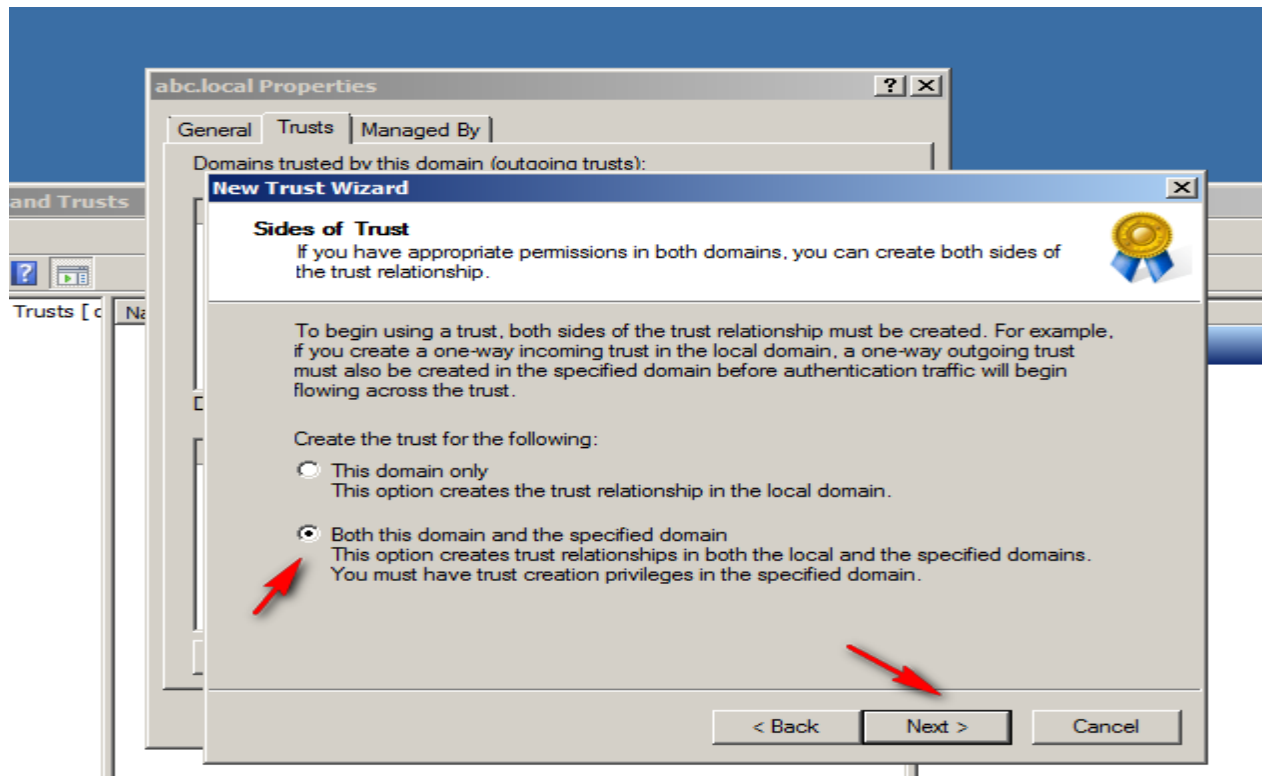
Forest trust



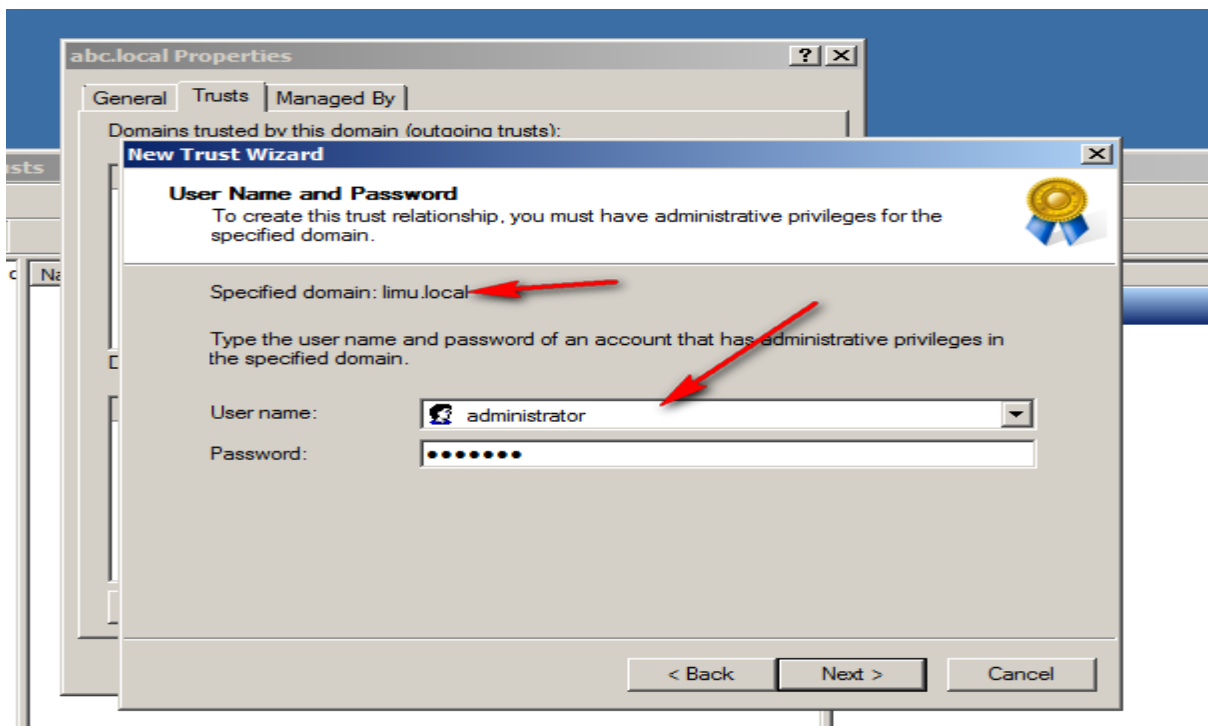
Two - way



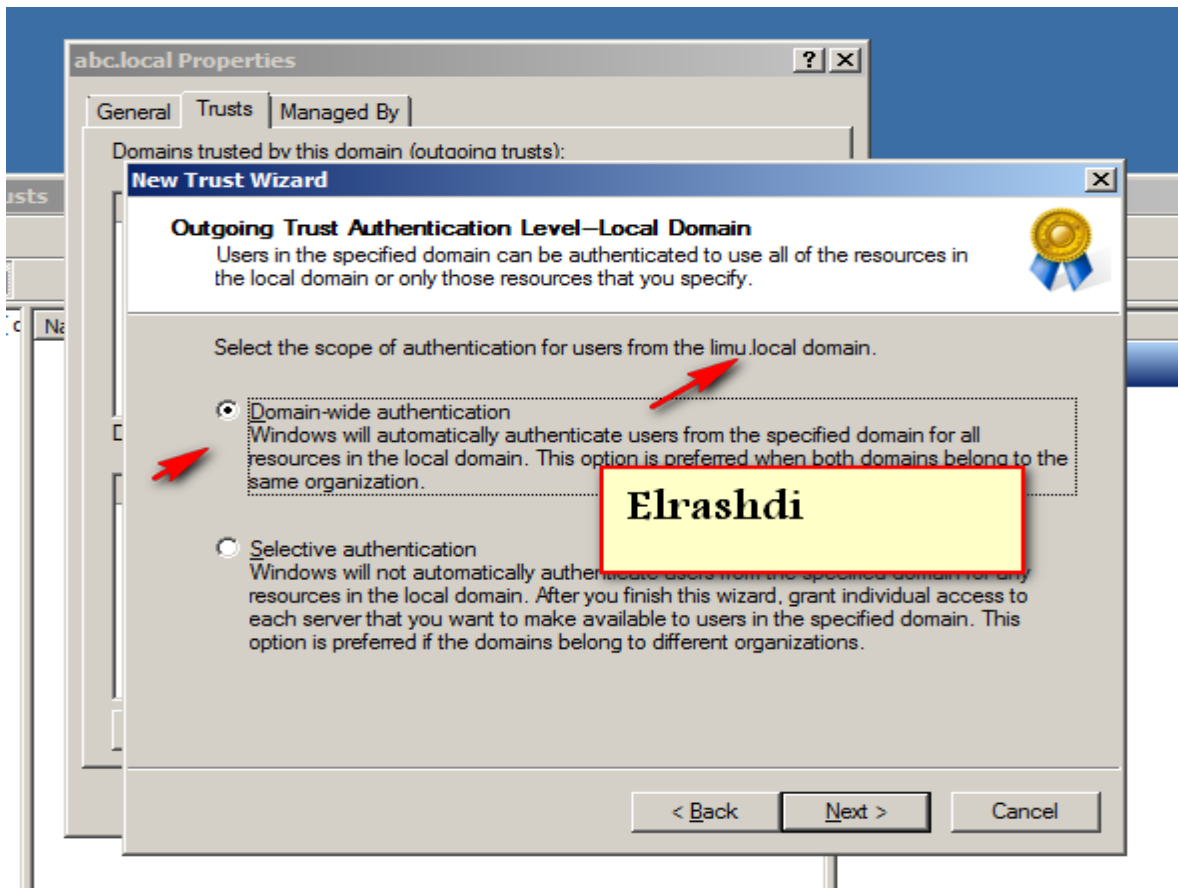
Both this domain and the specified domain



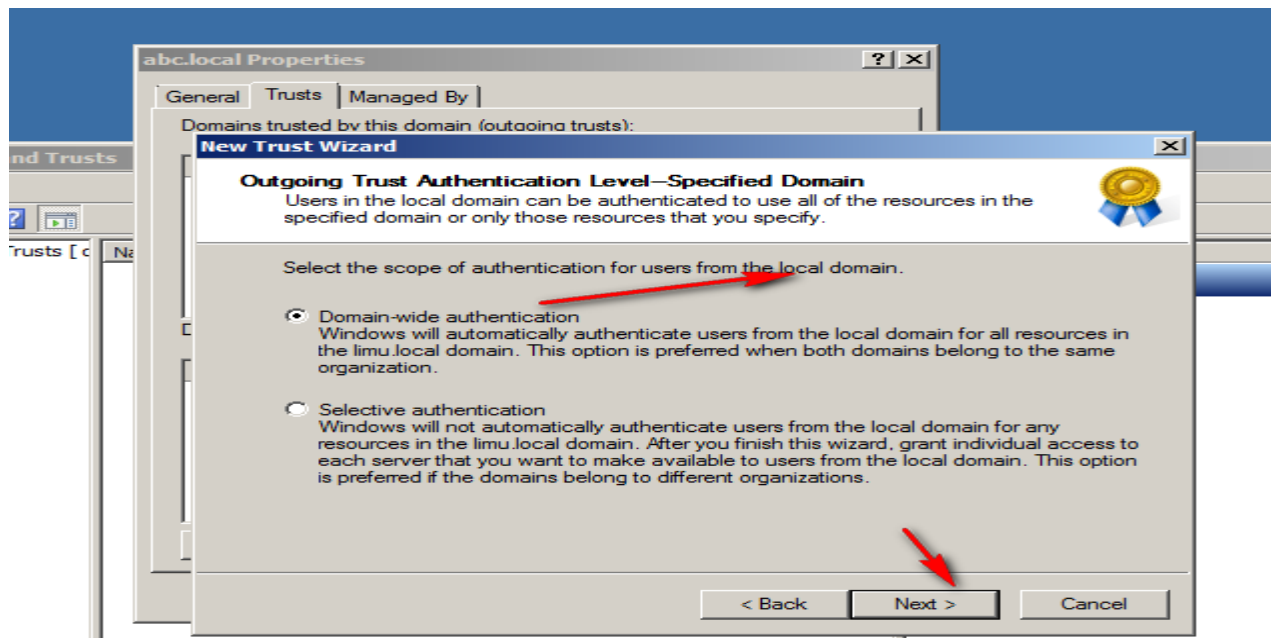
Type password of another domain



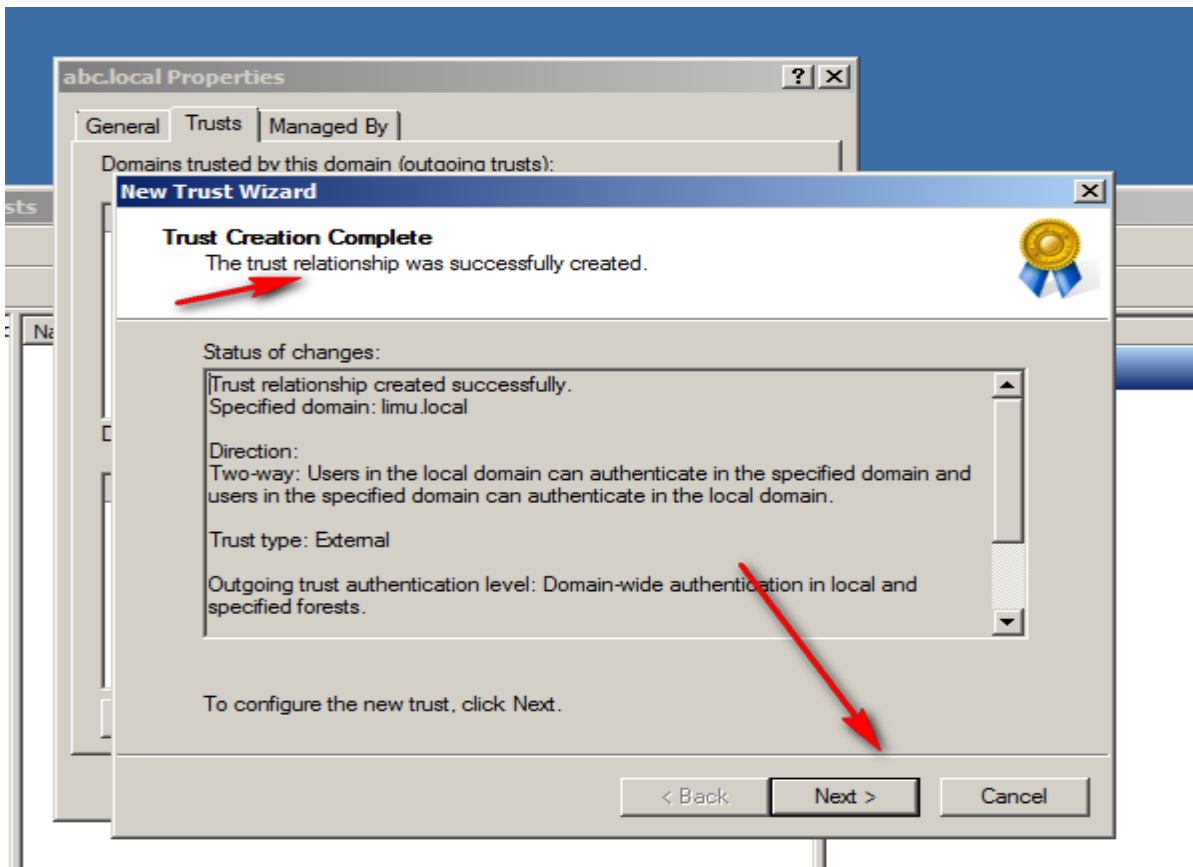
Domain-wide authentication for LIMU.local



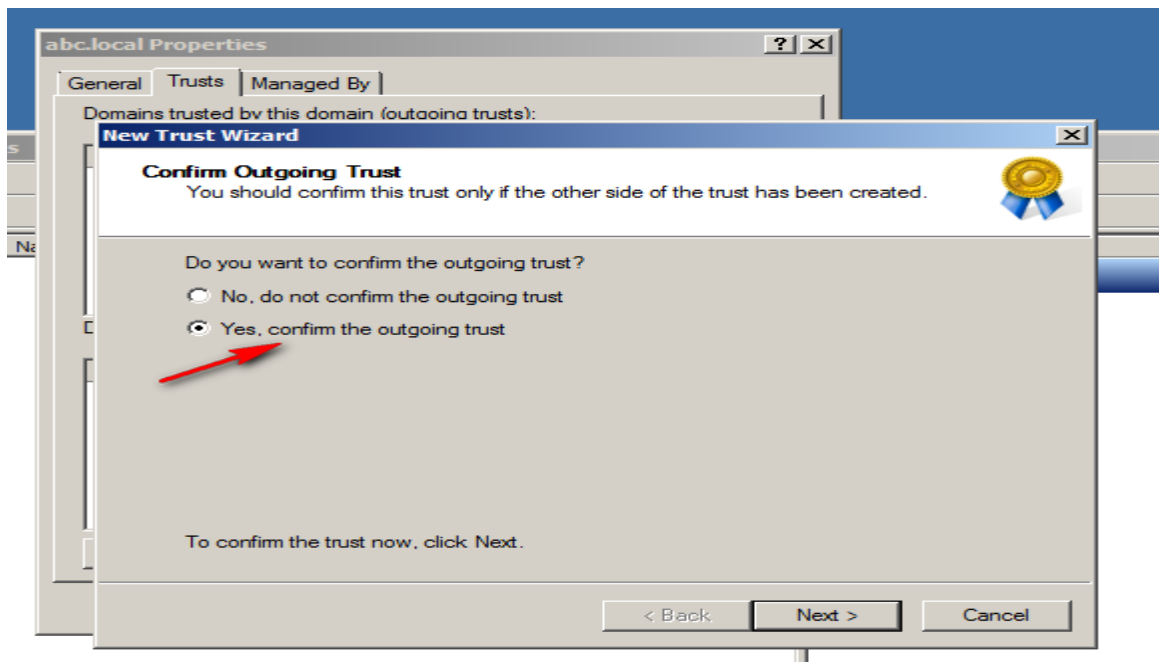
Also for local domain



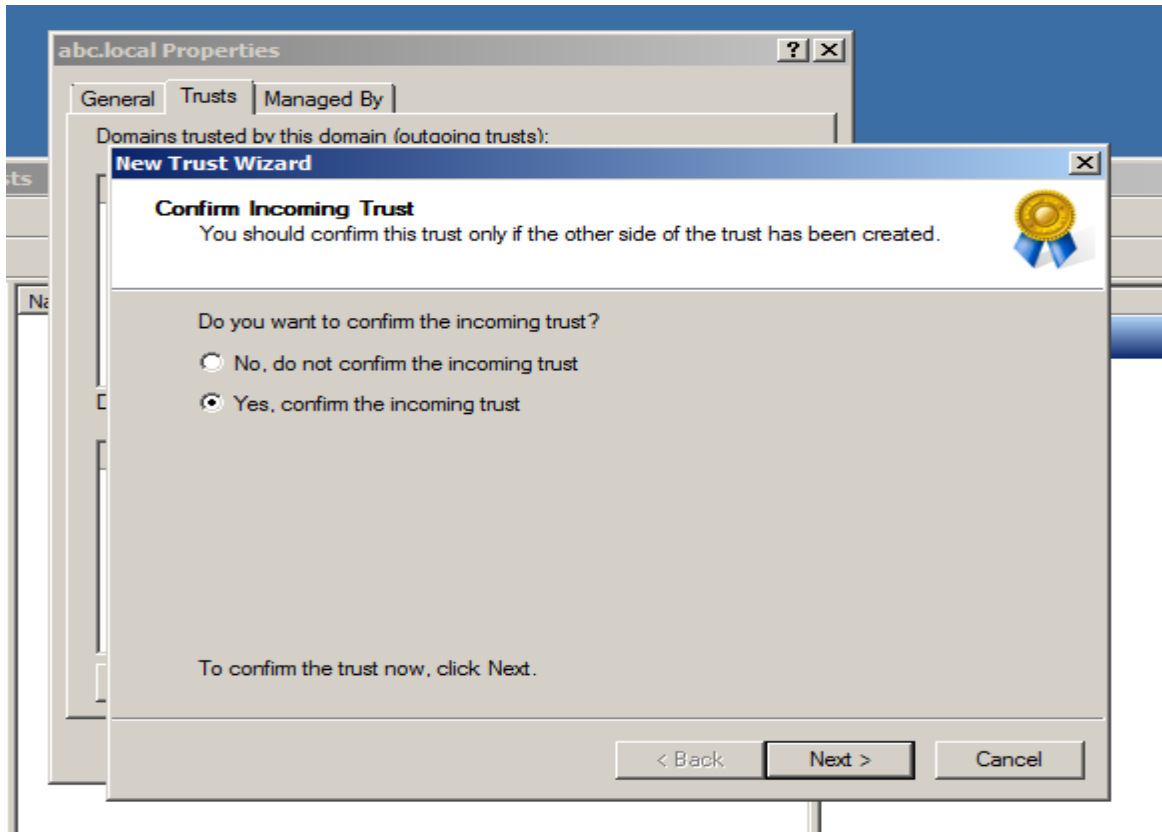
Trust complete



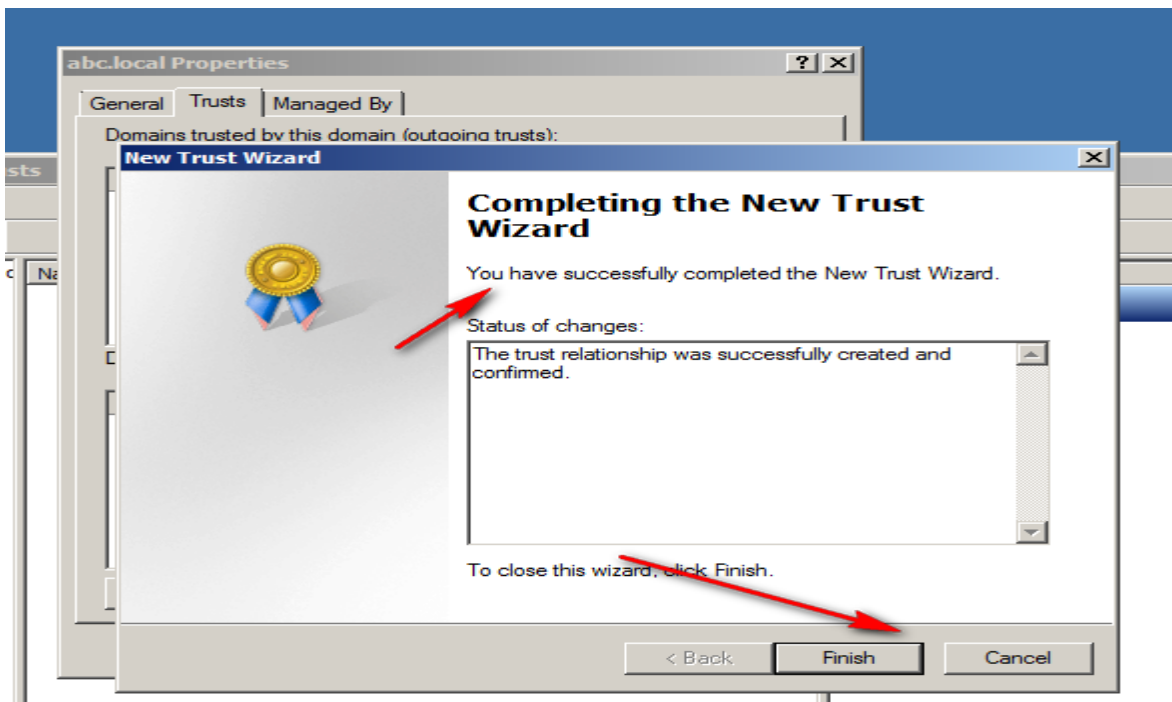
Yes confirm



Yes confirm



Finish



30-Backup windows server and active directory

من اهم الاشياء الذي يجب ان عملها لضمان استمرارية العمل في بيئة العمل الكبيرة هي عمل نسخ احتياطية لل windows server and active directory

Backing up Server 2008 Active Directory

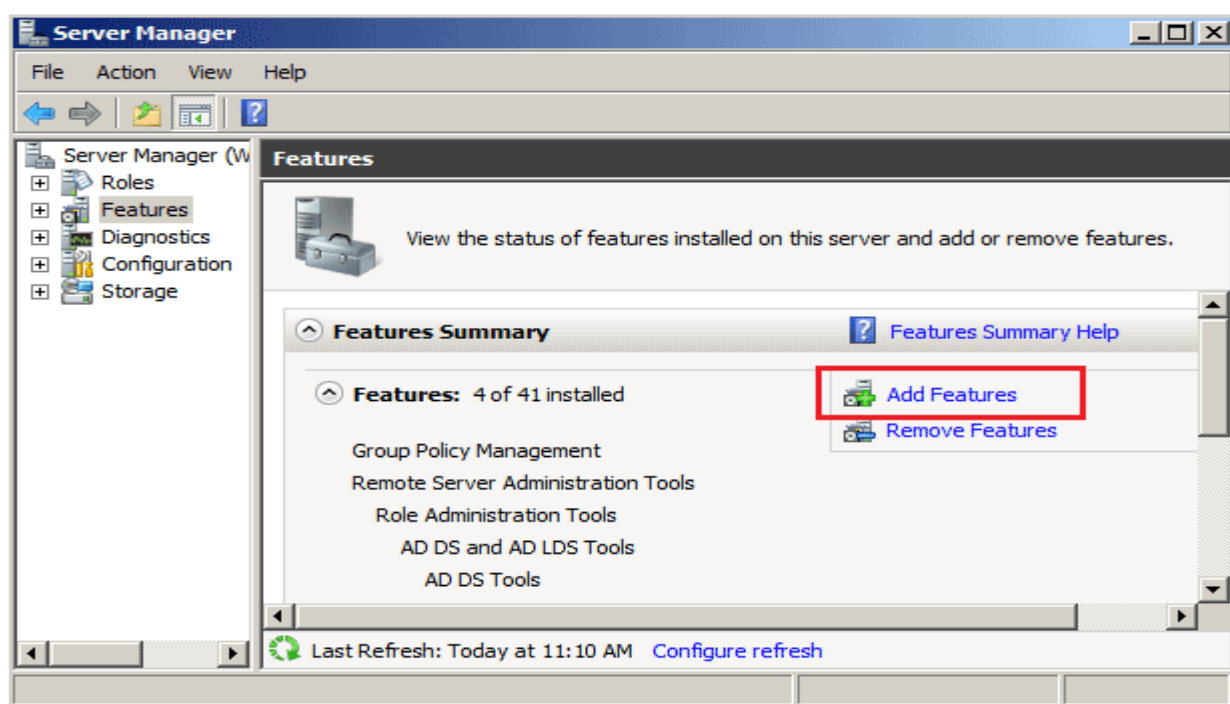
Now that we have the backup features installed we need to backup Active Directory. You could do a complete server backup, but what if you need to do an authoritative restore of Active Directory?

As you'll notice in Server 2008, there isn't an option to backup the System State data through the normal backup utility.

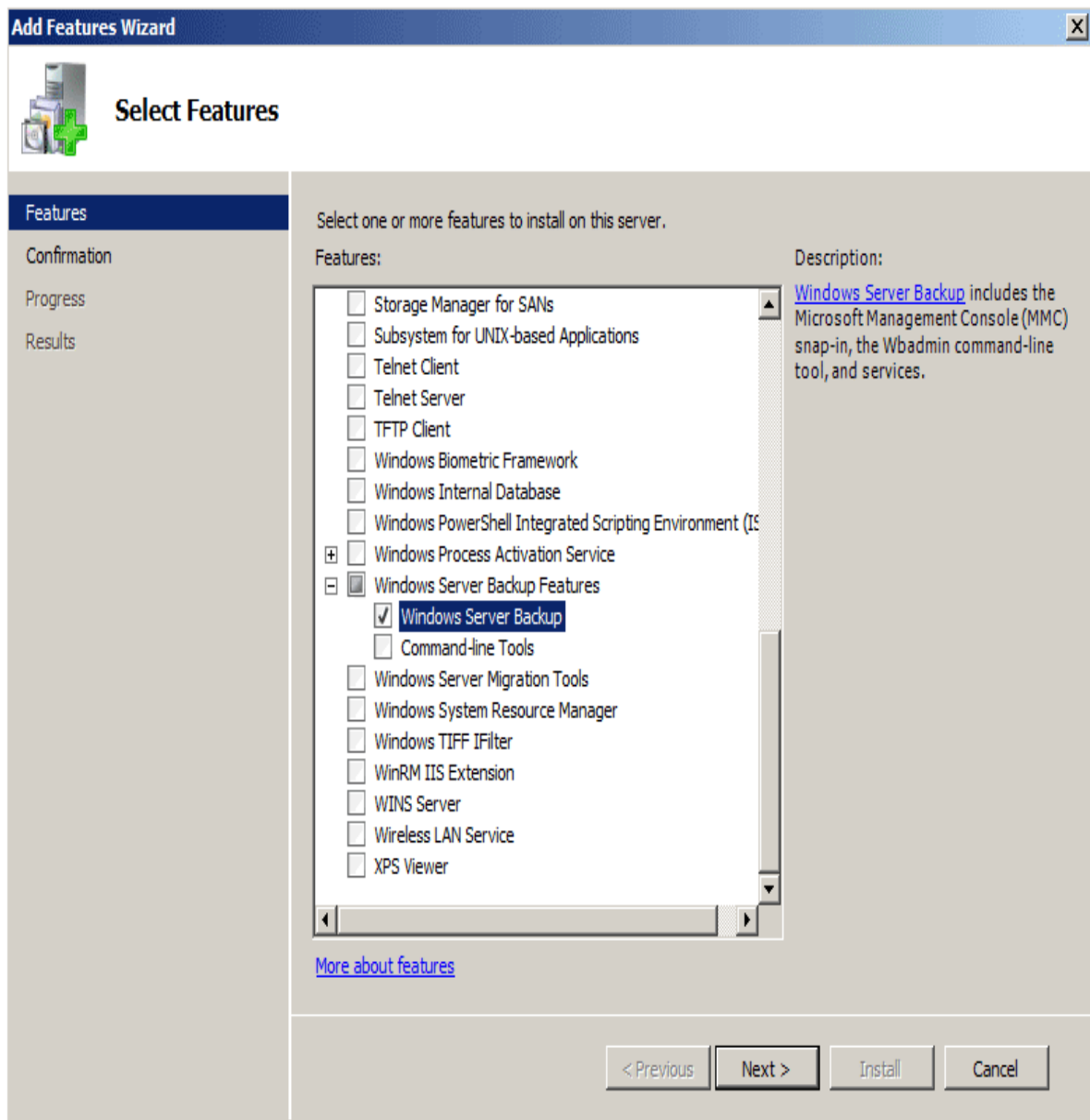
30.1- Install Windows Server Backup

Go to Start menu, and then select Administrative Tools, click on Server Manger.

Under Server Manager window, click on the **Add Features** link from the features summary section.



Select the **Windows Server Backup Features**, and then click on Next. The Command-line Tools allows you to perform a DC backup and recovery from the command line.

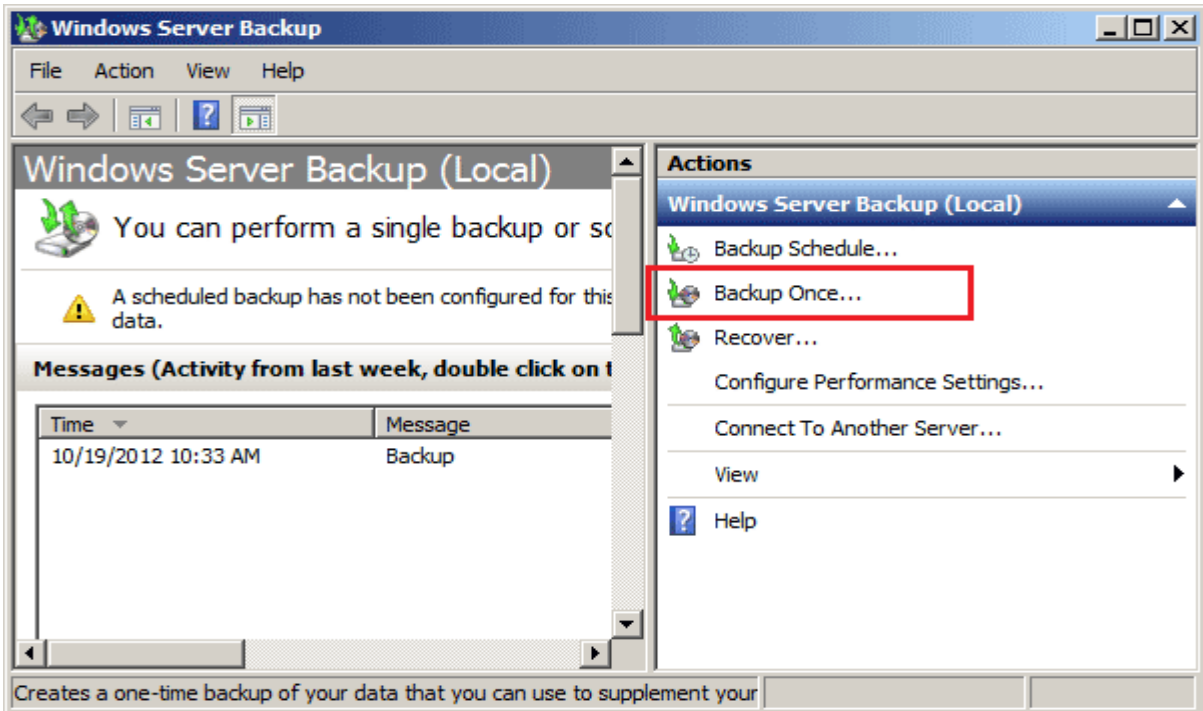


Backup Windows Server 2008 Active Directory

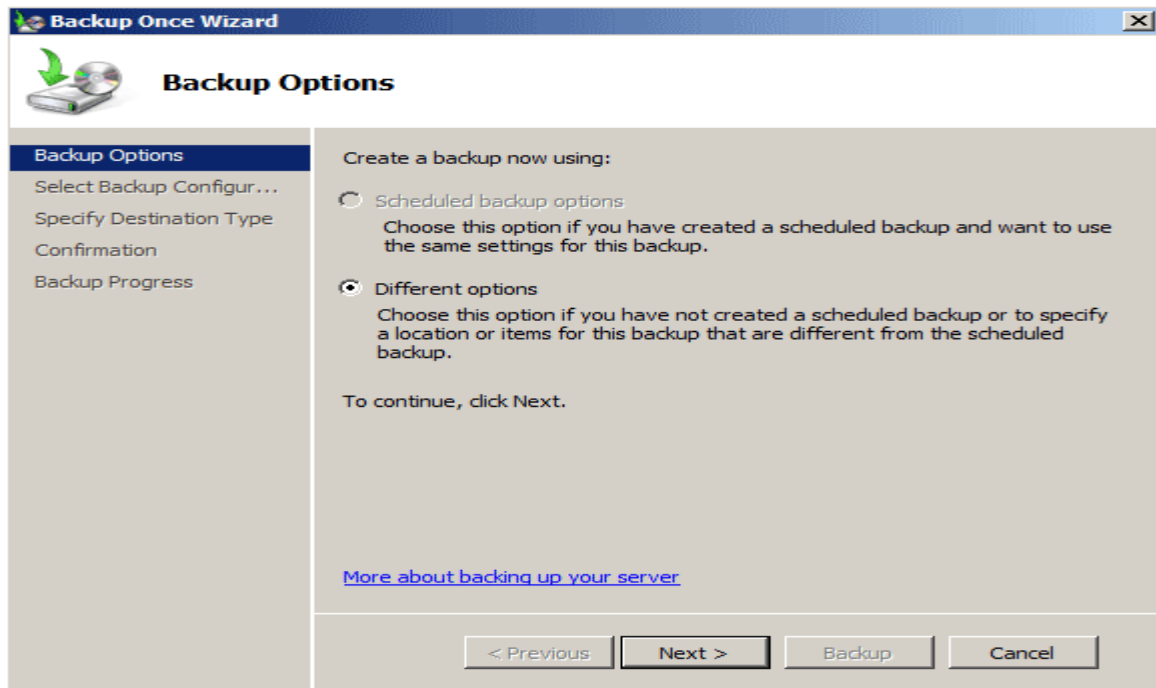
Now that we have Windows Server Backup installed lets perform our first backup of Active Directory in Windows Server 2008.

Go to Start menu, and then select Administrative Tools, click on Windows Server Backup.

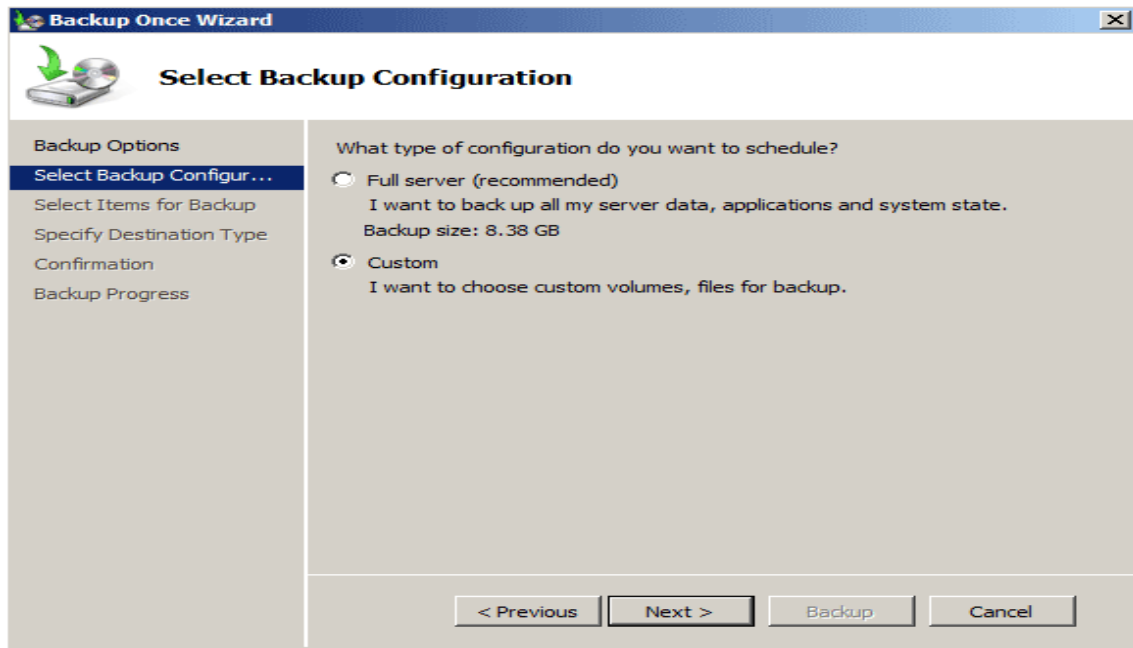
Select the **Backup Once** option to perform an immediate backup as illustrated in the screen below.



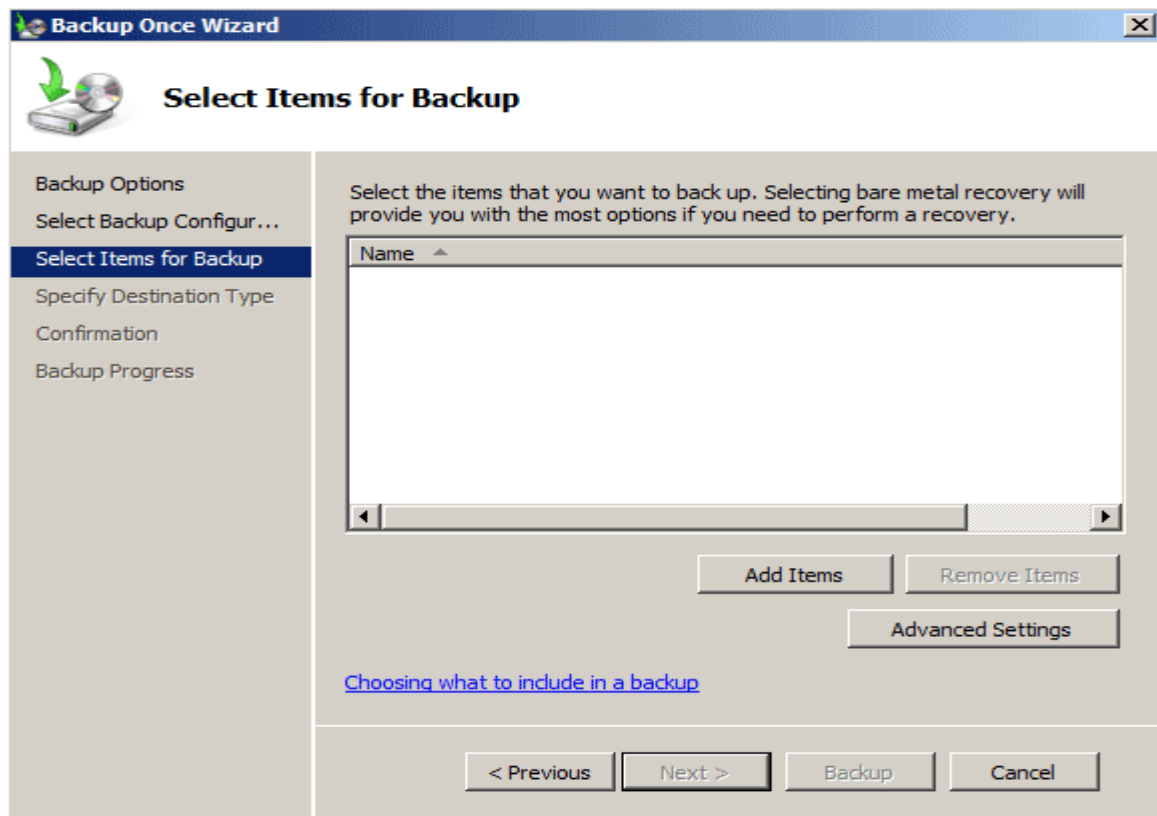
It will bring up the Backup Once Wizard, select **Different Options** and then click Next.



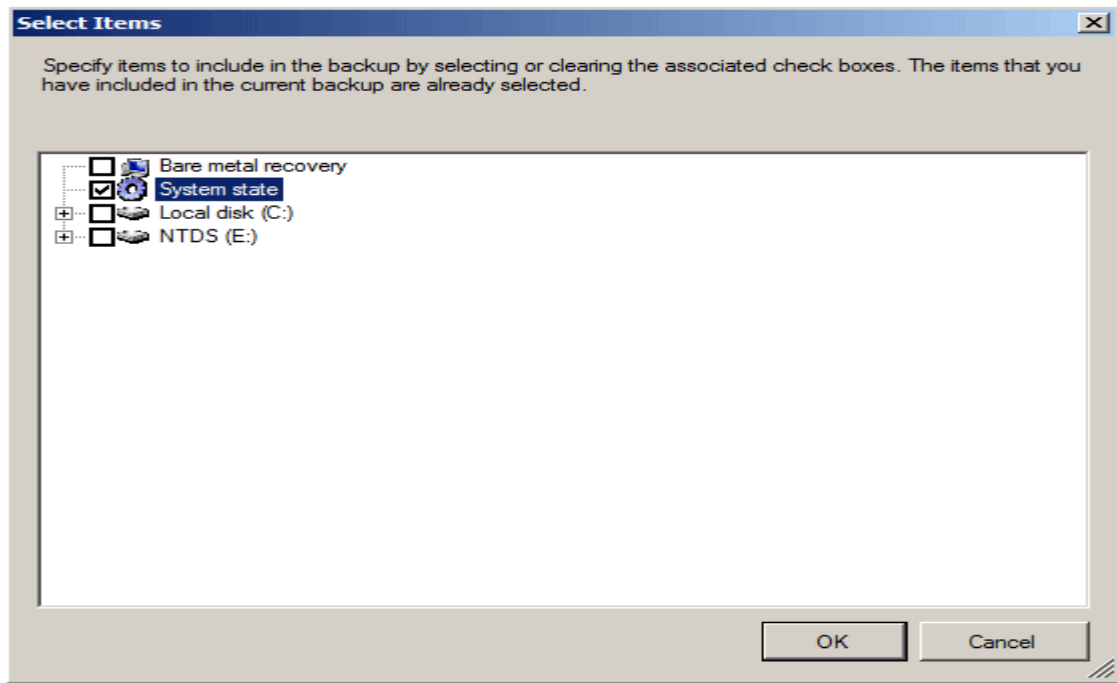
If you want to perform a full backup of your server, click on the Full server option. Now we're going to perform a system state backup, so we choose the Custom option.



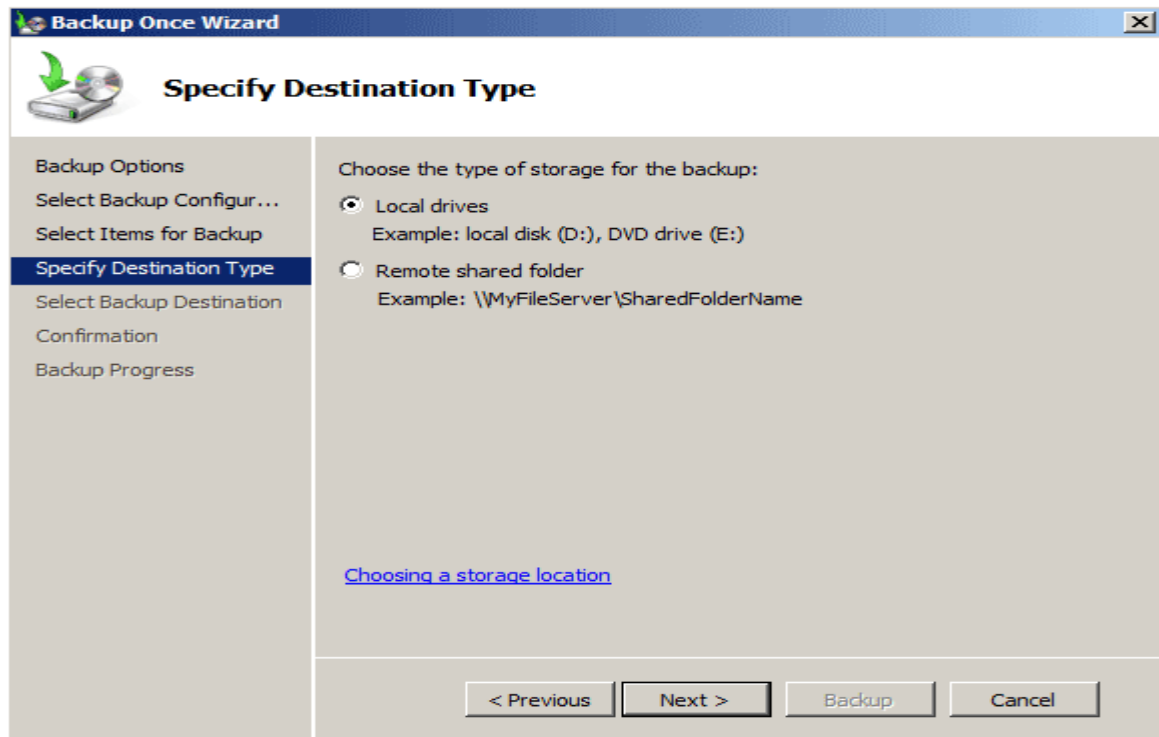
In the next window, you can customize the items you want to backup.



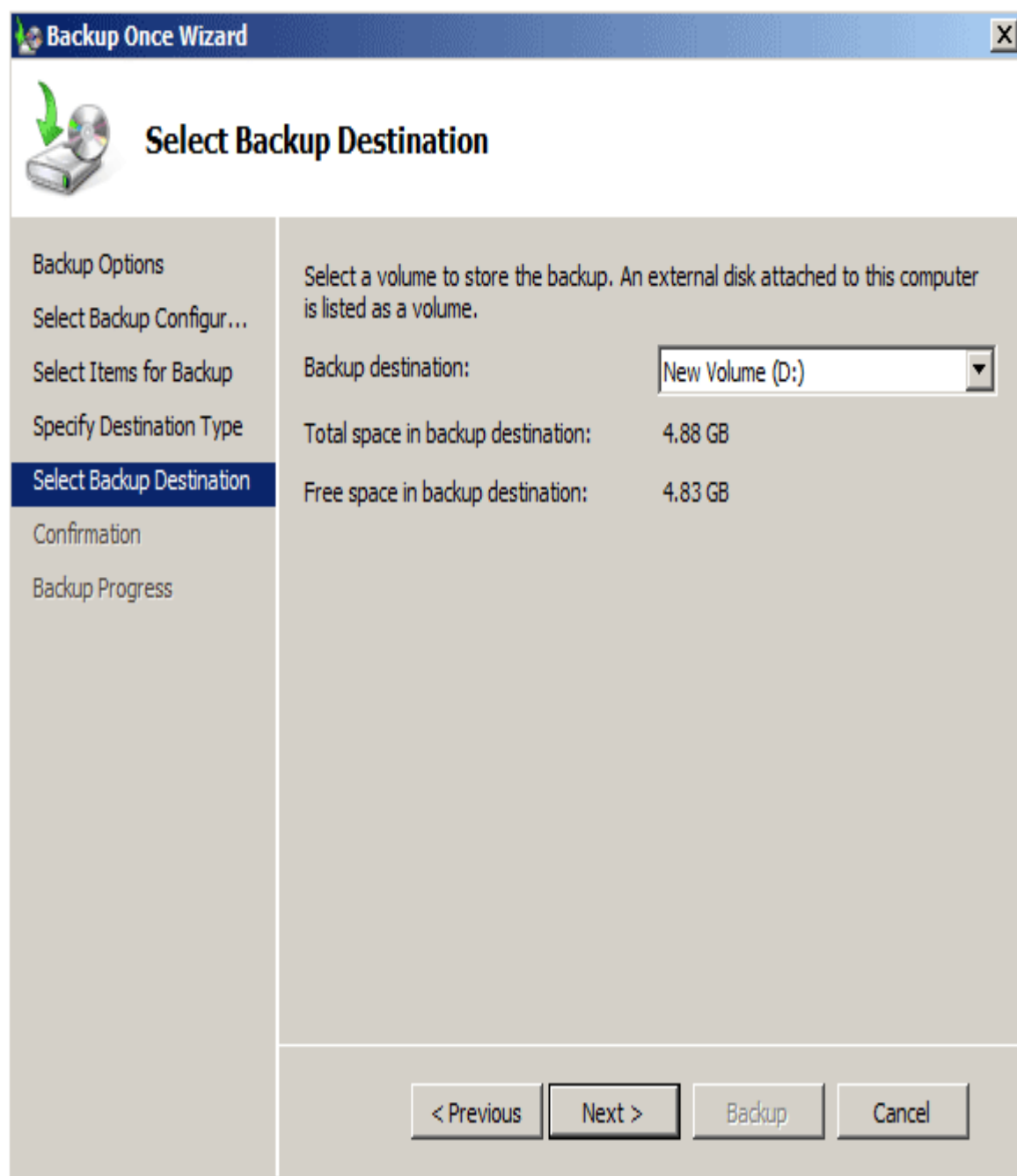
Click on Add Items button, check the System state option from the list. You can also choose to backup the entire NTFS volume on your computer.



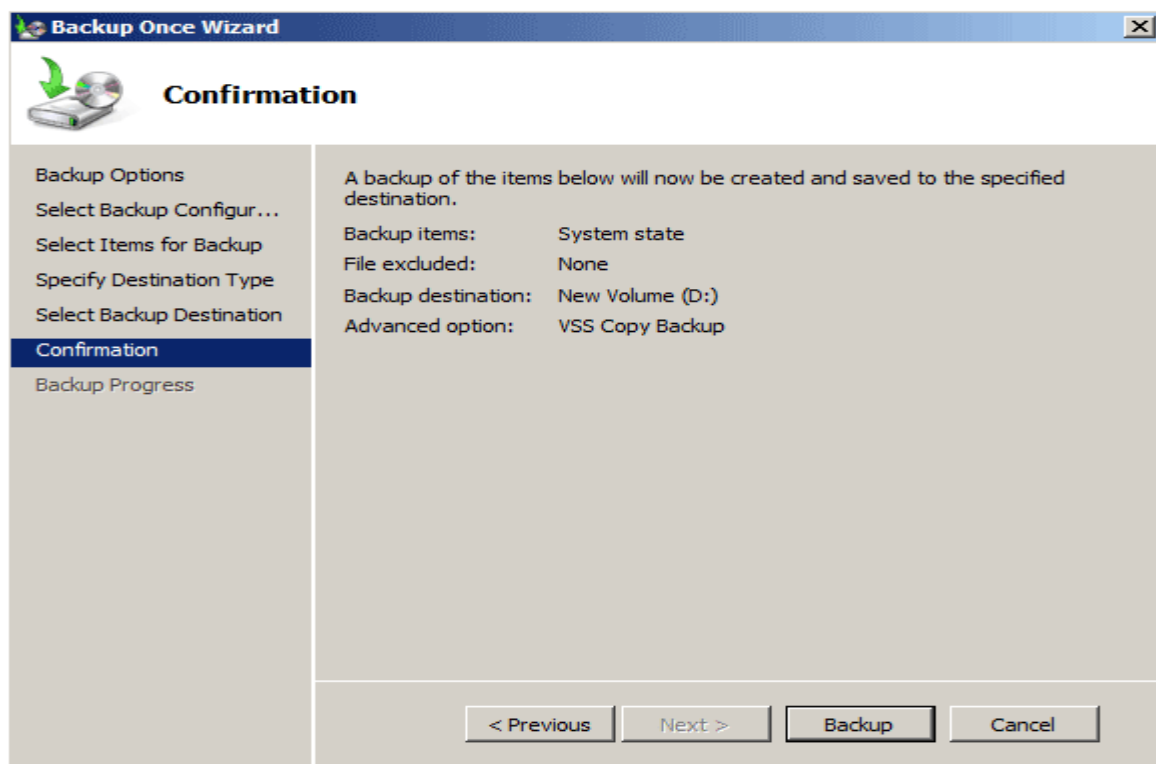
Specify the destination type for your backup. A system-state backup can't be performed directly to a network share so we have to choose the Local drives.



Next select a volume to store the backup. Windows Server Backup requires you to provide a separate target volume for the backup data. In single-volume server, you may need to shrink the existing partition to create a volume dedicated solely to backup data.



In the next window, confirm the options you have selected and then click on Backup.



If you want to script the backup process, or if you are backing up a server on a Server Core installation, you can use the WBADMIN.EXE command-line program. WBADMIN provides a complete set of options that perform essentially the same functions as the MMC snap-in, including performing a system state backup

```
Administrator: Command Prompt - wbadmin start systemstatebackup -backupTarget:d:
C:\Windows\system32>wbadmin start systemstatebackup -backupTarget:d:
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Starting to back up the system state [10/19/2012 4:04 PM]...
Retrieving volume information...
This will back up the system state from volume(s) Local Disk(C:),NTDS(E:) to d:.
Do you want to start the backup operation?
[Y] Yes [N] No Y

Creating a shadow copy of the volumes specified for backup...
```

30.2- Restore window server 2008

إعادة النسخة الاحتياطية التي تم اخذها مسبقا في حاله وجود مشكلة في window server 2008.

Start the computer by using the Windows Server 2008 DVD

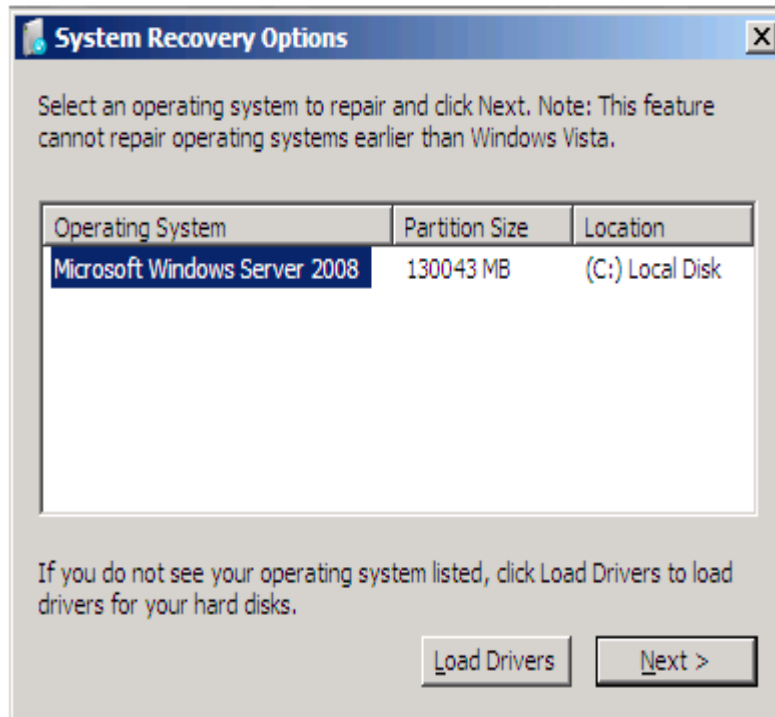
On the first screen Click Next.



Select the “Repair your computer” option in the lower-left corner of screen.

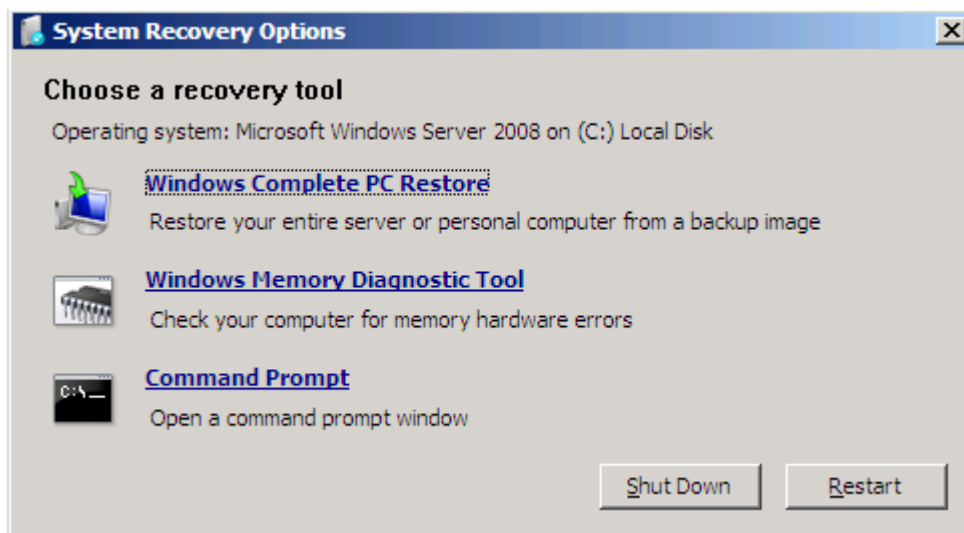


It will show you any currently installed operating systems. Click Next.

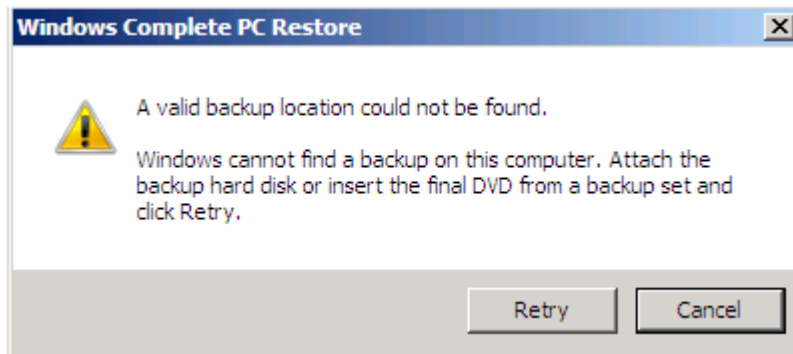


If this screen is blank you may have to load a third-party driver for your mass storage driver. You can click Load Drivers to load the mass storage driver from your USB flash drive.

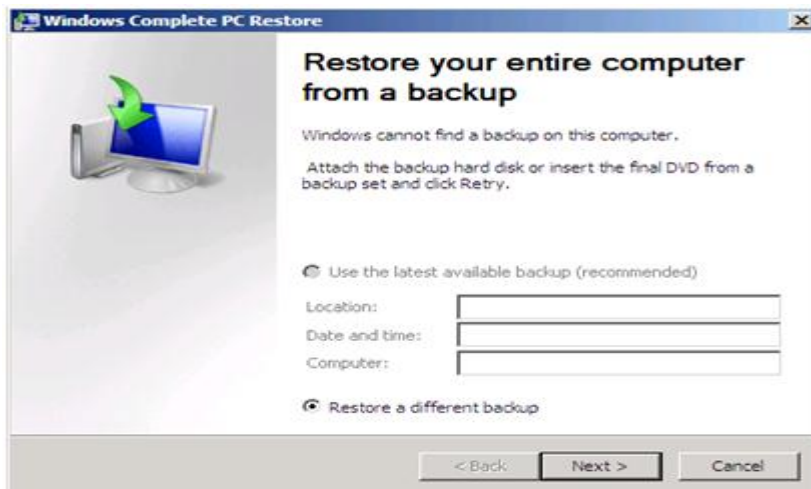
Click "Windows Complete PC Restore"



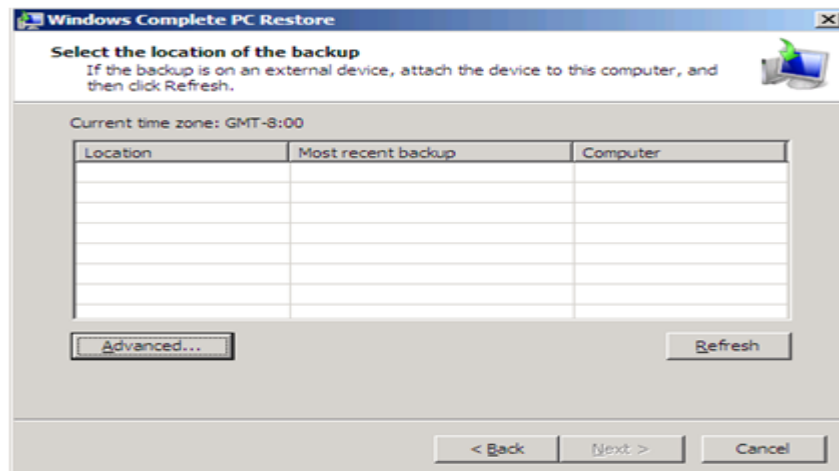
It will report “A valid backup location could not be found”. Click cancel.



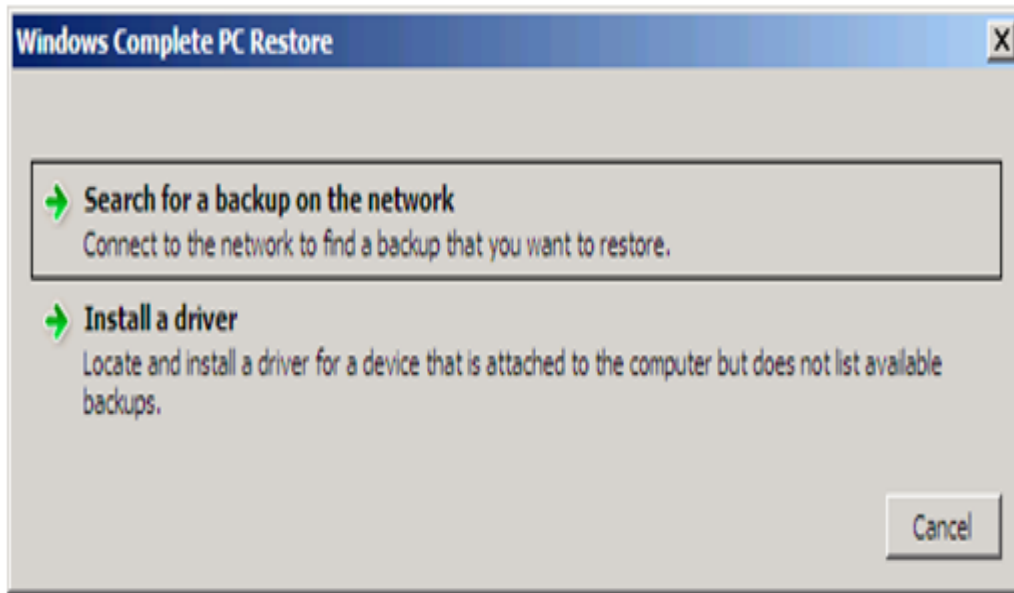
Select “Restore a different backup” then next.



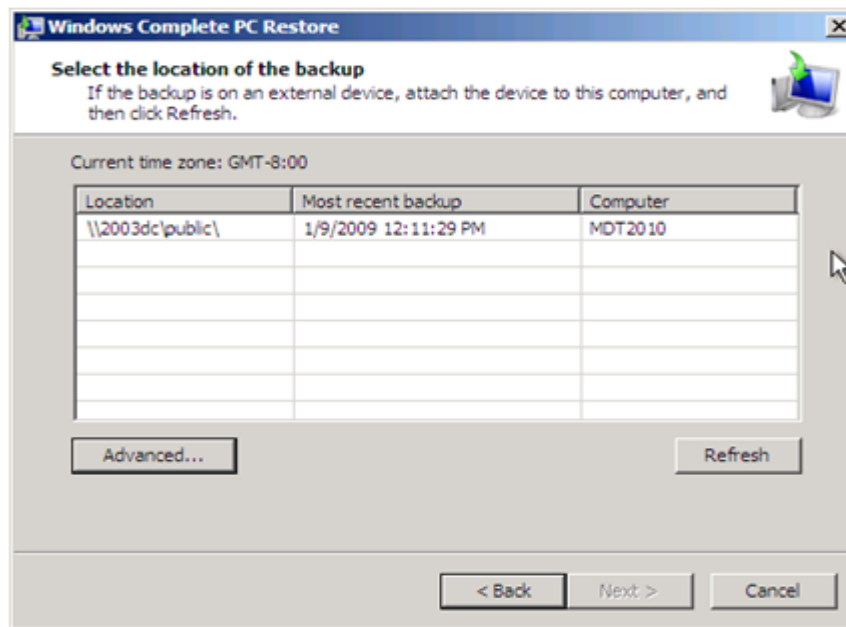
Click Advanced.



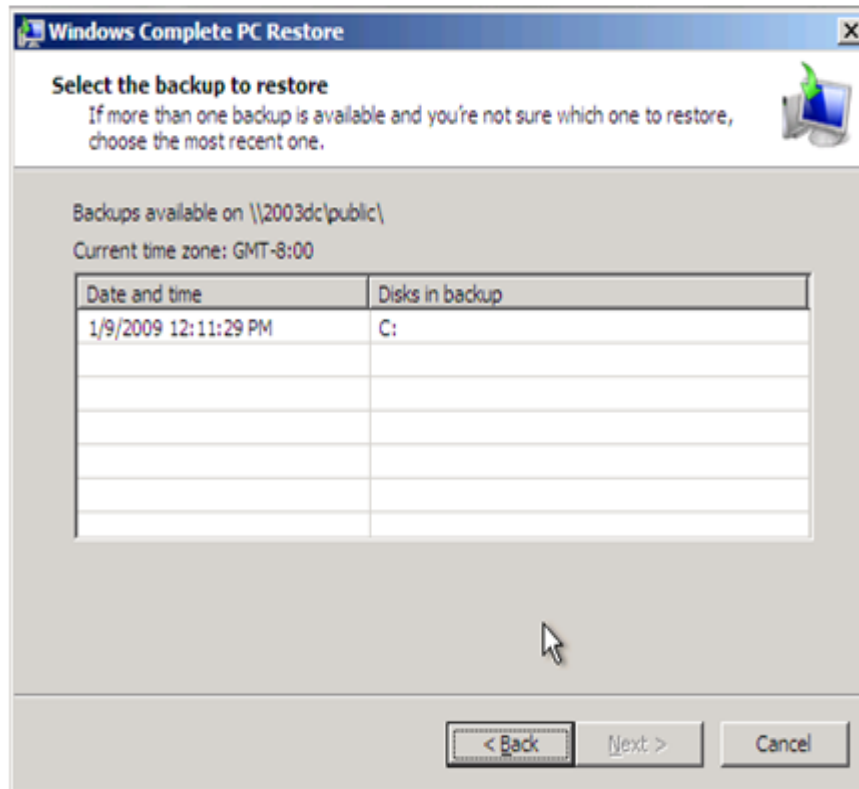
If the network adapter driver is included with Windows Server 2008 you can click “Search for a backup on the network. If the network adapter driver is not included you have to click “install a driver” and browse to your driver to load it. In my test I was using a Hyper-V virtual machine with the legacy network adapter. The legacy network adapter driver is in Windows Server 2008 so that it just works. The synthetic driver is not included.



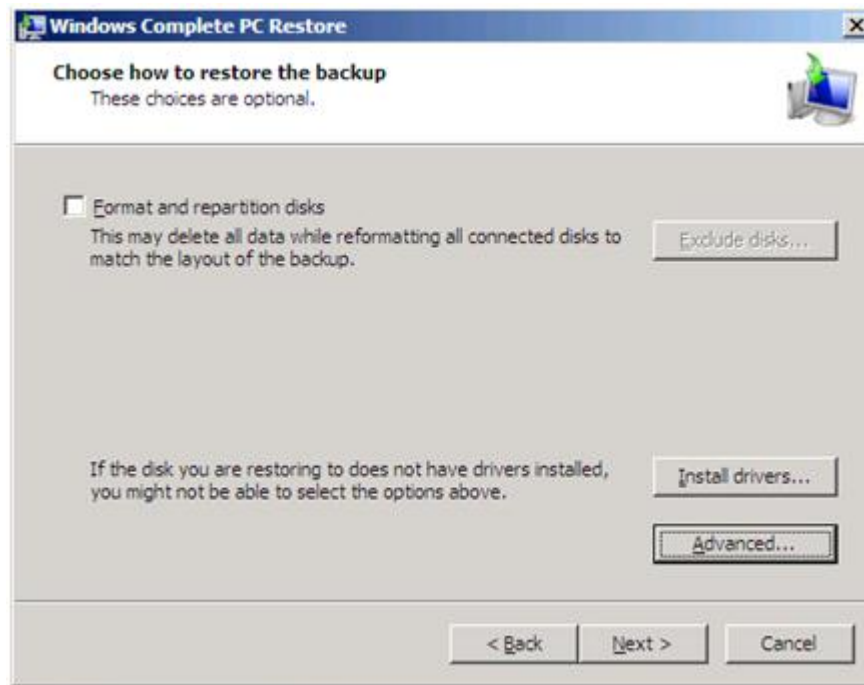
Select the backup listed and then click Next.



Select the backup then Next.

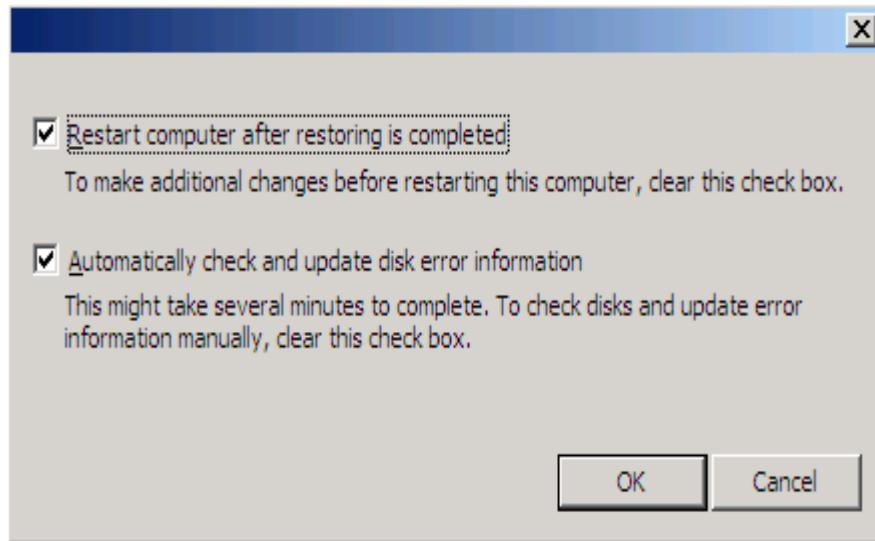


You are presented with the restore options.

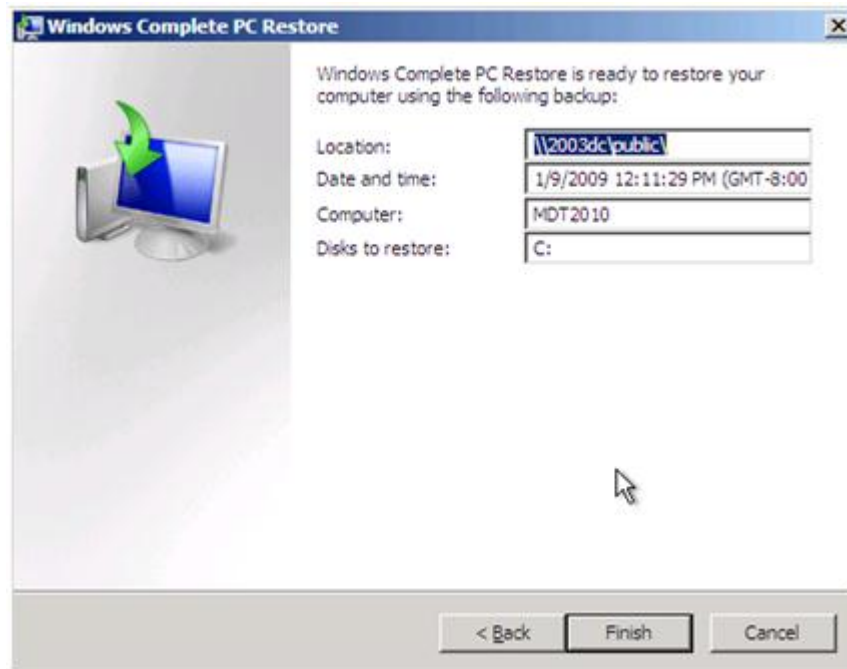


The exclude disks option enables you to exclude disks from the restore process.

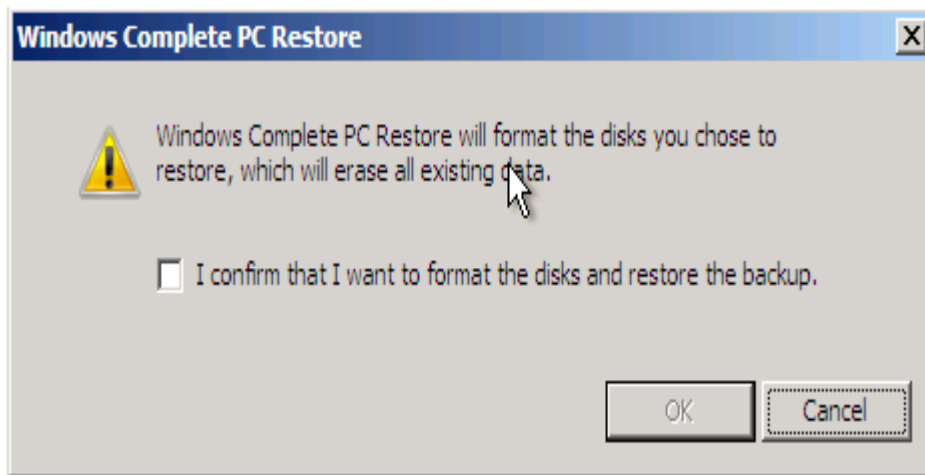
The advanced button has the following options.



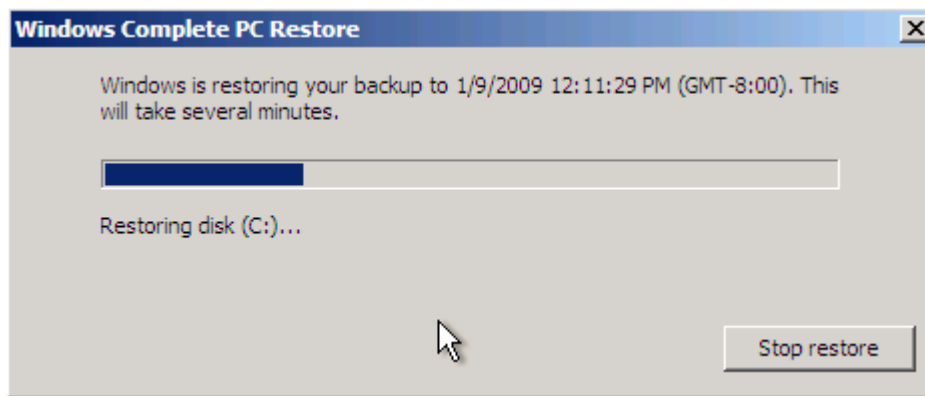
Click Finish to confirm the settings.



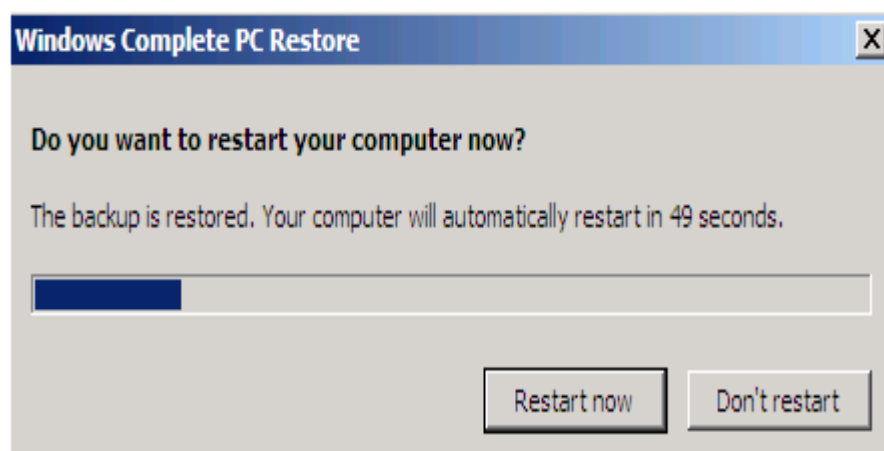
If you selected "Format and repartition disks" you are prompted with "Windows Complete PC restore will format the disks you chose to restore, which will erase all existing data". Click "I confirm that I want to format the disks and restore the backup".



You can monitor the progress through the final dialog box.

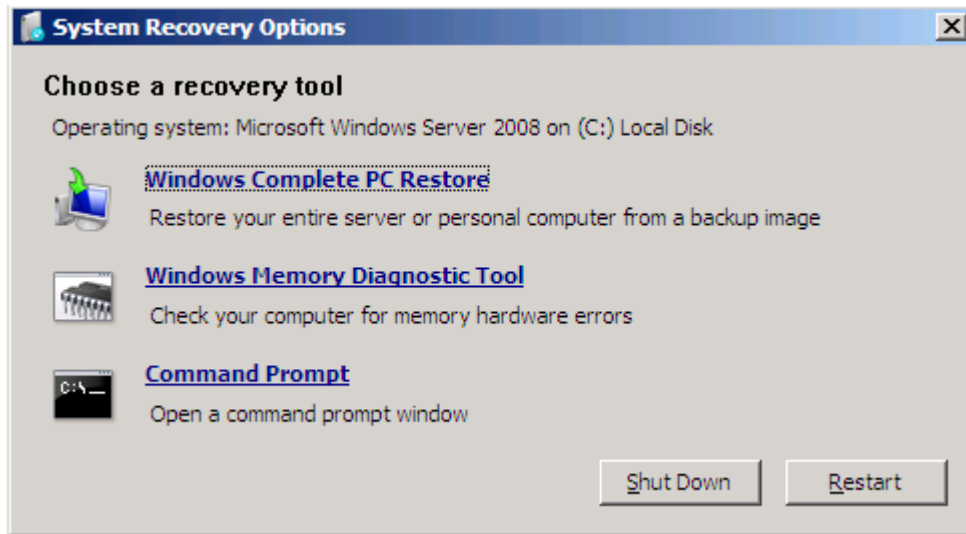


The restart will automatically occur or you can delay it.



For some scenarios, you may want to do this manually. The following lists the basic general steps to do this at the command prompt.

At the following screen select the “Command prompt” option.



The following subcommands for **wbadmin** provide backup and recovery functionality from a command prompt.

To configure a backup schedule, you must be a member of the **Administrators** group. To perform all other tasks with this command, you must be a member of the **Backup Operators** or the **Administrators** group, or you must have been delegated the appropriate permissions.

You must run **wbadmin** from an elevated command prompt. (To open an elevated command prompt, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.)

Subcommand	Description
Wbadmin enable backup	Configures and enables a daily backup schedule.
Wbadmin disable backup	Disables your daily backups.
Wbadmin start backup	Runs a one-time backup. If used with no parameters, uses the settings from the daily backup schedule.

Subcommand	Description
Wbadmin stop job	Stops the currently running backup or recovery operation.
Wbadmin get versions	Lists details of backups recoverable from the local computer or, if another location is specified, from another computer.
Wbadmin get items	Lists the items included in a specific backup.
Wbadmin start recovery	Runs a recovery of the volumes, applications, files, or folders specified.
Wbadmin get status	Shows the status of the currently running backup or recovery operation.
Wbadmin get disks	Lists disks that are currently online.
Wbadmin start systemstatercovery	Runs a system state recovery.
Wbadmin start systemstatebackup	Runs a system state backup.
Wbadmin delete systemstatebackup	Deletes one or more system state backups.

Subcommand	Description
Wbadmin start sysrecovery	Runs a recovery of the full system (at least all the volumes that contain the operating system's state). This subcommand is only available if you are using the Windows Recovery Environment.
Wbadmin restore catalog	Recovers a backup catalog from a specified storage location in the case where the backup catalog on the local computer has been corrupted.
Wbadmin delete catalog	Deletes the backup catalog on the local computer. Use this command only if the backup catalog on this computer is corrupted and you have no backups stored at another location that you can use to restore the catalog.

Reference

Microsoft press "Microsoft 70-410 - Installing and Configuring Windows Server 2012",",1/8/2013.

Microsoft press " Microsoft 70-411 - Administering Windows Server 2012",",1/8/2013.

Microsoft press " Microsoft 70-412 - Configuring Advanced Windows Server 2012 Services",",1/8/2013.

<https://www.computerworld.com/article/2588287/networking/networking-peer-to-peer-network.html>.

<https://www.thegeekstuff.com/2014/11/install-active-directory/>.

<http://www.mustbegeek.com/change-windows-desktop-background-using-group-policy/>.

<https://www.top-password.com/blog/how-to-backup-windows-server-2008-active-directory/>.

<https://blogs.technet.microsoft.com/askcore/2009/02/04/windows-server-backup-2008-restore-from-network-location/>.

<https://protechgurus.com/configure-lan-routing-windows-server-2016/>.

<https://whatismyipaddress.com/nat>.

<https://www.falconitservices.com/support/KB/Lists/Posts/Post.aspx?ID=77>

artic name " HOW TO INSTALL VPN ON WINDOWS SERVER 2016",

<https://www.thomasmaurer.ch/2016/10/how-to-install-vpn-on-windows-server-2016/>

" IP Addressing: DHCP Configuration Guide, Cisco IOS Release 15SY",

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/dhcp-relay-agent.html.last ,last visit Sep 10, 2018.

<https://www.slideshare.net/AdeelKhurram/what-is-active-directory-56059734>

<http://www.itingredients.com/deploy-desktop-wallpaper-group-policy-server-2012/>

" Delegating Administration by Using OU Objects", <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/delegating-administration-by-using-ou-objects>

" How to Configure and Enable Quota on Shared Folder Using File Server Resource Manager in Windows Server 2012 R2 ", <https://www.faqforge.com/windows-server-2012-r2/configure-file-server-resource-manager-windows-server-2012-r2/>.