M.C.S.E

Microsoft Certified Solution Expert

BY: AYMAN FOUAD SHOKRY
Email: ayman_shokry22@hotmail.com

Introduction

Difference between cisco and Microsoft:

There 2 kinds in this field

Connectivity	Control / management
Cisco IOS Is for build network inside firm from routers and switches and manage it with protocols.	Windows M.S Is for manage users and system on devices with group policy and monitoring.

Windows client 7,8,10

Ways of install win client:

1- **Bootable CD/DVD**
2- **Bootable USB**

Notes:

These 2ways won't be helpful in case we need install win in firm or company so we need faster way to do it is use hiren boot with image of win.

How to make hiren boot usb:

Open win setup usb program.

Choose bootice > parts manage >reformate usb disk.

Choose align to 1mb > next

Choose format option NTFS >choose quick format.

Mark on 4th choice which have .ISO.

Choose the file ISO of hiren.

3- **Imaging**

Is because we can't copy and paste the win system because we will can't paste in the cluster 0 in the HDD manually.

So the image going to be the righteous way for it install the files in its place.

Notes:

Any program we going to use out of Microsoft software's going to be "third party ".

There 2 tools for make image.

1st is Norton ghost

2nd is Acronis

How to use both tools

Norton Ghost	Acronis
Hiren tool > backup tool >Ghost Norton Ok > local > partition “to image for create “ “ from image to use exist” Must be identical H.W	Hiren tool >backup tool > Acronis > ok Create image > disk 2 pri ACT > next till end Restore to use exist image Must be identical H.W

4- Remote installing service

And its deleted now and no one use it and came in replace of it Ghost Server.

And also it’s deleted from MCSE course.

A+, Electronics

HHD

HDD Bad Sectors:

1- Physical bad sector :

It happens cause of chromo oxide “CrO2” are get less on the platter “disk media “

For solve this problem we use DLG “Data Life Guard “or “Dr Norton “

Notes:

As long as chromo oxide be less it be harder to fix and as it be large it be easier in fix cause programs are use the exist around it and fix the affected areas .

2- Logical bad sector : “ Cross link”

It happens because 2 bits be written in the same spot on platter so it made HDD can’t define which one it work so HDD stop load the Operating system.

For solve it we use HDD regenerator which in the hiren program.

Difference between compatible, original, server devices:

MCSE

File System

When file be written on cluster place it divide it on the cluster sizes 4k or 16k so if file has 20k amount it going to take 5 clusters size of 4k size and in 16 going to take 2 clusters size , but the 2nd cluster which have 12k free it won't be unable to use .

In the same time when file be written on platter it happened randomly cause platter moves with 7500 RPM and pin moves forward and backward .. So data never be written organized.

Every data has number for can recognize it again and for recognize the file again it need

FAT "File Allocation Table"

And that how virus can destroy file … by accessing the FAT and delete or destroy it.

- **Definition of File system :**

Is utility for use to access on HDD.

- **Allocation Tables :**

FAT	FAT32	NTFS "new tech File system"
- Up to 4GB - Dual boot	- Up to 32GB - Dual boot	- Up to 2 Tera - Dual boot 1-permission 2-encryption 3-compression 4-qouta

- History of Microsoft :

Bill Gates start his work in Apple Corporation in the beginning as programmer then he stole the code of DOS idea and leave.

Then he start his own business and made DOS 1,2,3,4 they all failure then made 5, 6, 7 and they success.

But wasn't good enough until 1995 made Windows 95, but it kept have problems,

1st it was 16 bit/APP

2nd its working wiz MS.DOS sub dos in restarting.

3rd haven't good security or arrangement for corporations.

In 1998 Microsoft made windows 98 and said its 32Bit/APP, until Java Company discover it's wrong

And that windows still work wiz only 16Bit/APP but in double way 16 for sent and 16 for receive.

But it keep the same 16Bit/APP.

In the same time at 1990 company name New Technology made them first operating system NT1 , 2 and 3 failed but NT 4 success in 1995 and all companies and corporations start use it cause its features were great for them from users and security and log files and not depending on MS DOS and work stations and servers .

1999 Microsoft bought New Technology Company and made them most real success windows 2000 NT 32bit/APP.

DOS	
1	16bit/app
2	16bit/app
3	16bit/app
4	16bit/app
5	16bit/app
6	16bit/app
7	16bit/app

Microsoft		
3.1	90	16b/a
3.11	94	16b/a
Win 95	95	16b/a
Win98	98	32b/a
Win me	99	32b/a
Win NT	2000	32b/a

Notes:

Bit/Application: is the road which carry data sent and receive from user to system to H.W and as road is have more size as it be faster and better.

New Technology is the company which invented the NTFS. 16b/a

NTFS

Permissions

As you see NTFS permissions must think direct in **"Who - Doing - What? "**

- Is feature responsible for ..,

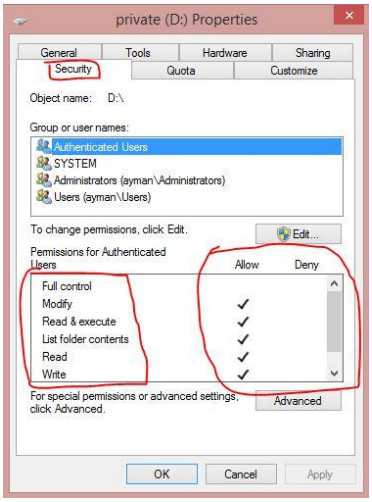
Modify: can delete and R/W but not add users.

Read: open file "Read only " .

Write: add files and R/W .

Full control: have all control.

User account	Permission
	1. Full control 2. Modify 3. Read 4. Write



- User Account :-

1. Local User Account :

Reside in SAM file "Security Account Manager ".

Is the file which has all users' security that be on the local device can't share same users with other device cause it going to have different SAM which not have the files and difference S.ID.

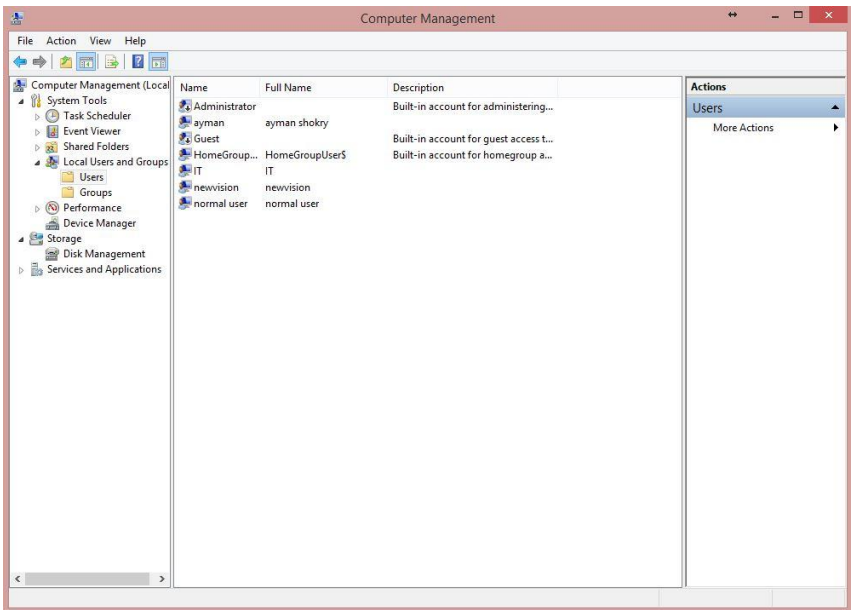
S.ID: Security identifier.

2. Domain User Account :

Reside in A.D "Active directory ".

Is for make many users for logging from any device and go check A.D instead of SAM local computers.

3. Built in User Account:



Is the users which is being created by default in windows system “Administrator, Guest “.

Notes:

When we get message error “Access denied “be sure is cause of permission.

Administration have almost control of permission and can give permissions to users.

Users have limited control depending on permissions it getting.

A) NTFS permission level:

1 - File

2 – Folder

3 – Partition

B) NTFS permission accumulative :

If User A has permission Read and permission in Group has Write

So user A when enter folder going to have R+W permission.

C) Deny override any other permission:

If user A have full control permission inside group, and we want make user A dun have permission to Read some folder.,

We give this user A Deny on read.

By that priority be with deny be before than full control so user A will can’t read the folder even it has full control in the group.

NTFS permission Inheritance:

Is the main partition or folder have some permissions,

Then the sub folders going to be inheritance the same of the main,

You can't change or edit in the sub folders,, but can only add more permissions.

For solve this is change Advanced security for new folder unmark on inheritance permission object.

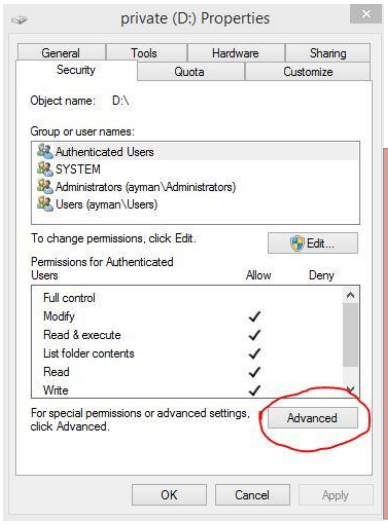
Steps:

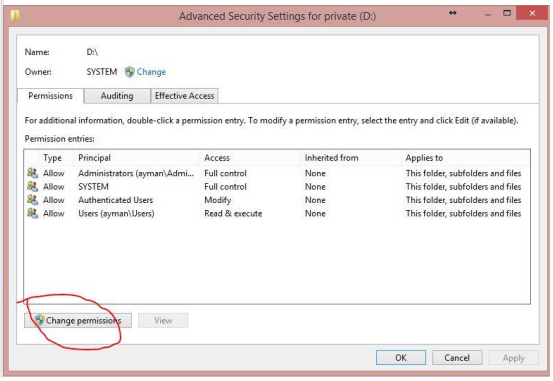
Properties -> security -> advanced security setting -> change permission -> unmark.

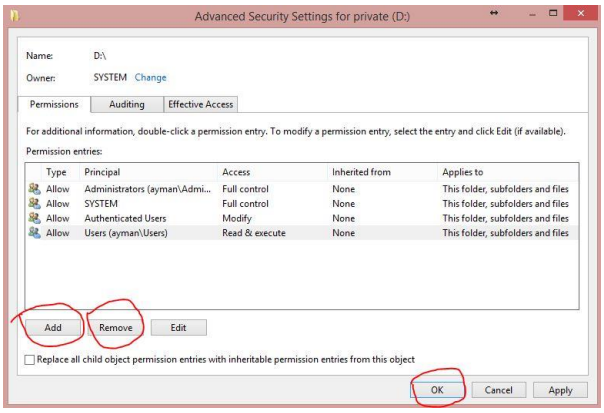
Choose add "for keep permission as it is but with your control"

Or choose remove and clear "for delete the permissions and add manual over new ".

Press ok.







NTFS

Special permissions

Is feature have more control to folders and users.

Let's say if there company have 500 users and we want to make them read only 1 folder for each user and in the same time make 5 admins can have full control on all partitions with its sub folders.

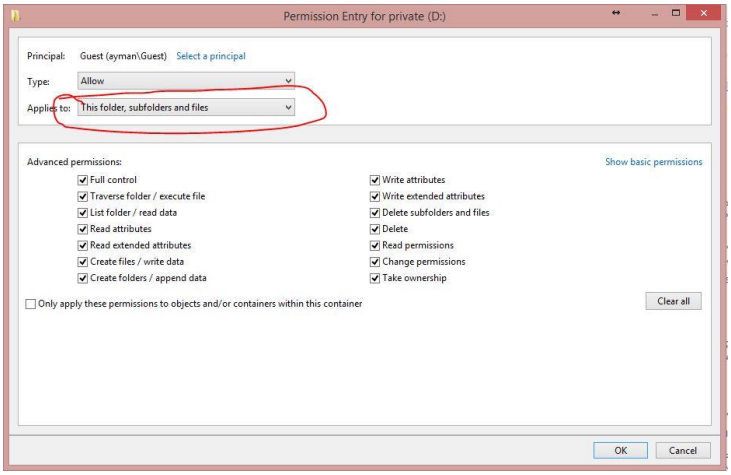
With normal permissions is very hard cause will have to give deny to 495 users manually and that going to waste too much time and won't be 100% occurred.

So we use special permission for control and manage these kind of cases.

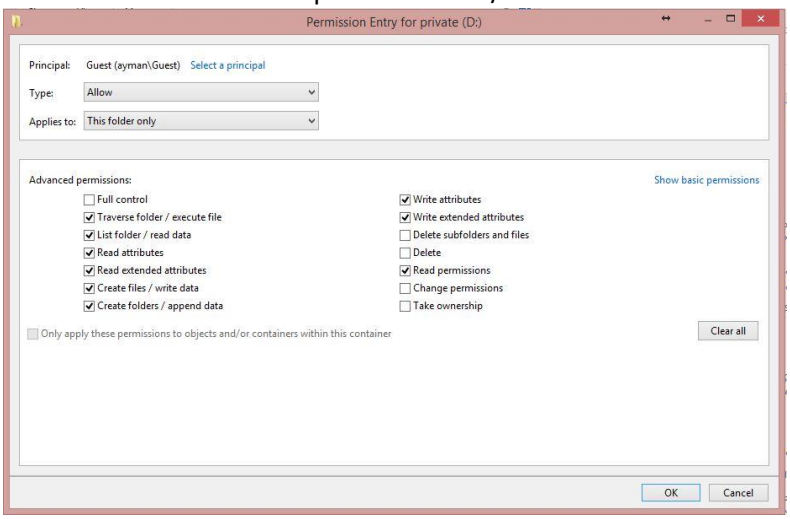
Ex:

Company have 5 departments "HR has R/W, IT has R/W and R on the partition, Sales have R only, Help desk have R for whole partition, Admins has full control ".

1st we will set for admin F.C to partition and Subfolders.

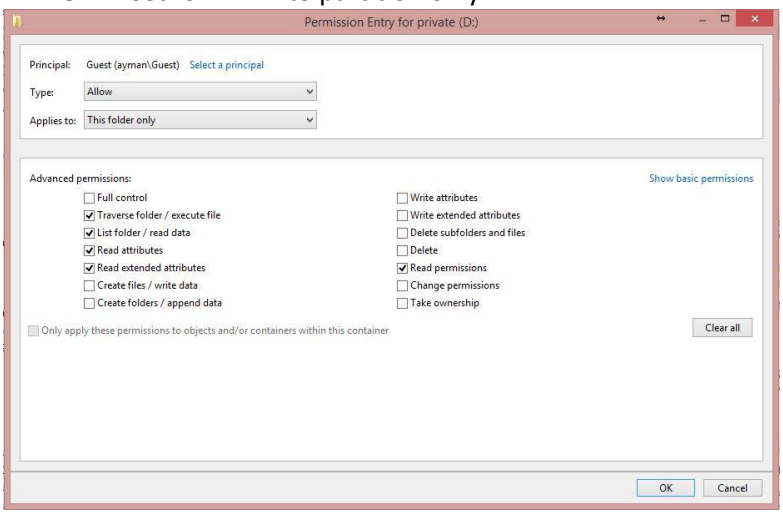


2nd we will set for HR R to partition and R/W for HR folder.



3rd we will set for sales R to sales folder only.

4th we will set for H.D R to partition only.



NTFS

Quota

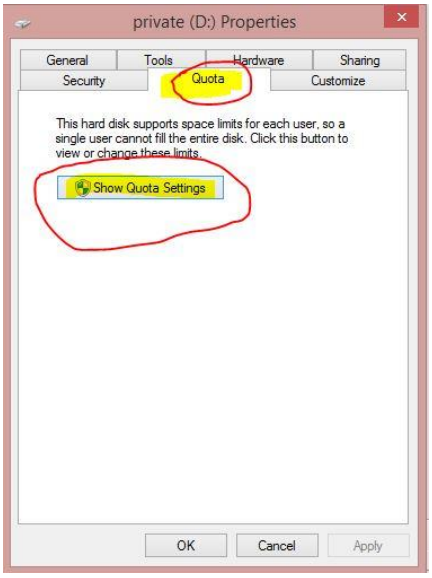
Quota:

Is for give limited space on partitions for users.

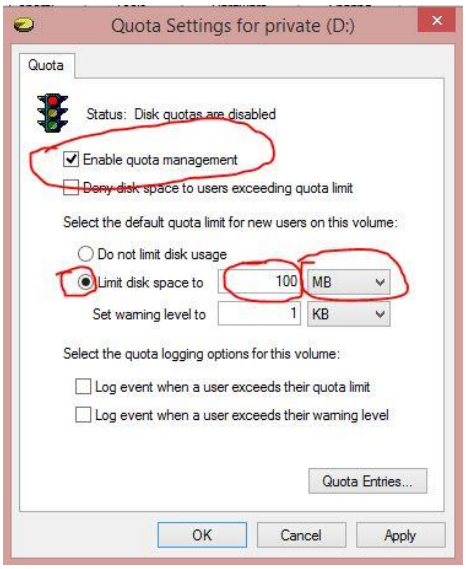
We also use quota for reduce high usage on HHD and control the Backup.

- **Steps** :

1st we going to enable the quota “partition properties > quota > show quota settings > check mark “enable quota management

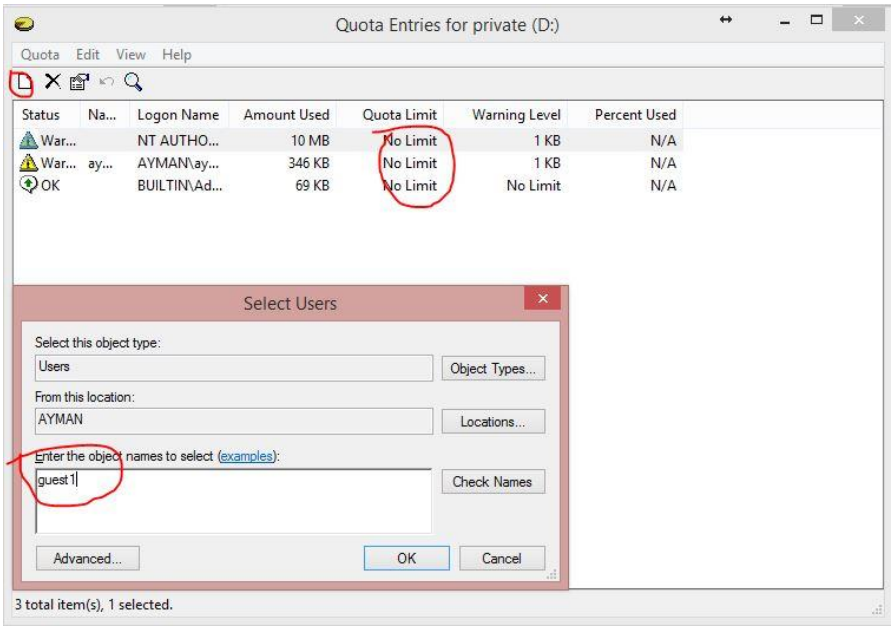


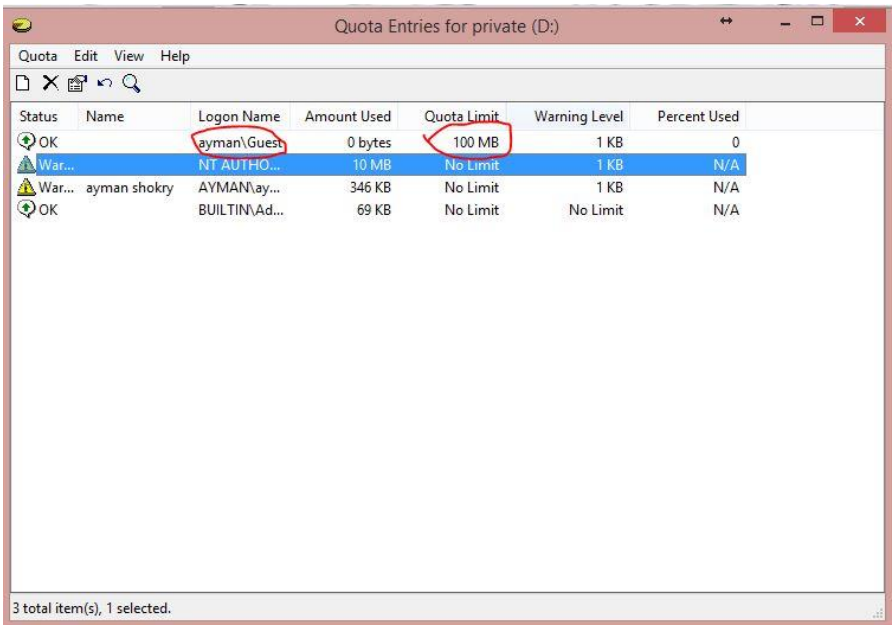
Choose limit disk space to “100 mb”



2nd when we need more space we going to “quota entries (will appear window of quota)

For add users we press on add and type username”.





This feature can work with users which has Read/ write or modify or full control permissions and not with Read only cause it won't need space for use on HDD anyway.

NTFS

Compression

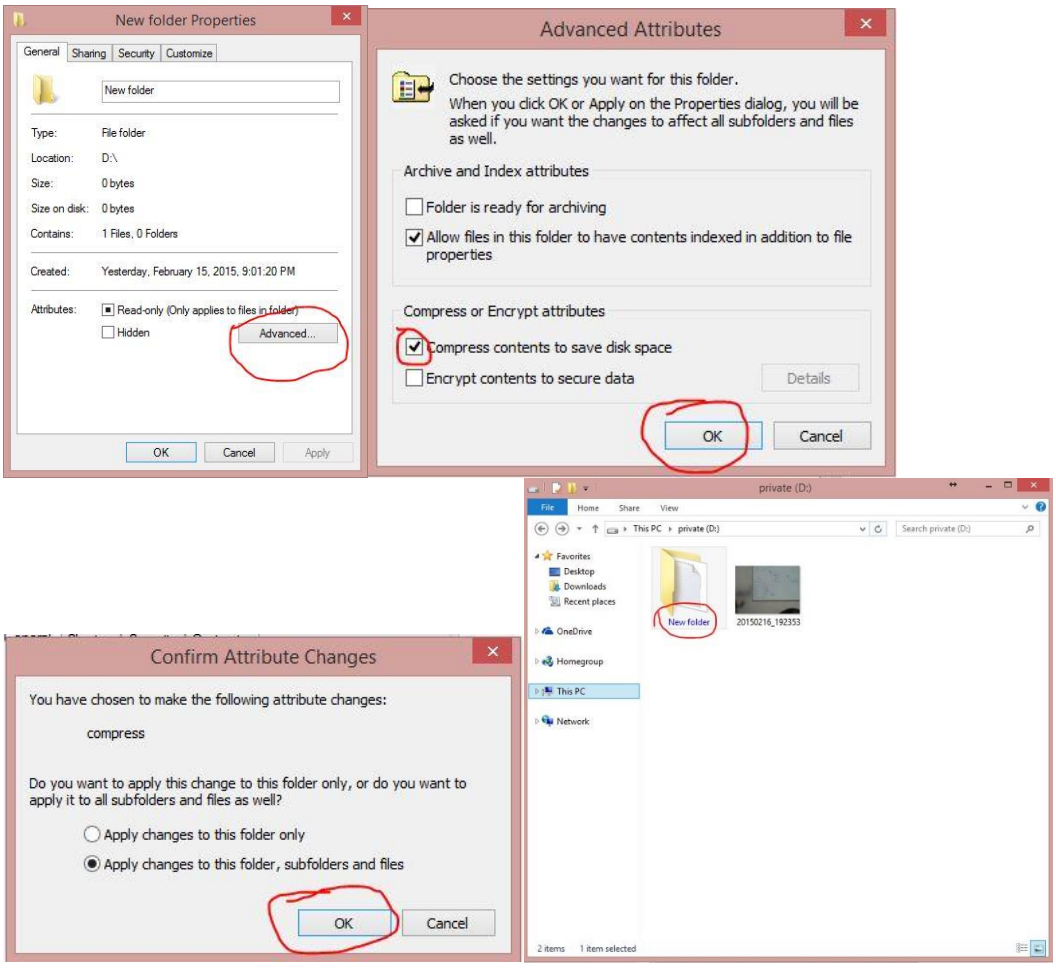
Compression:

Is for make folder has automatically compressing as per we are adding files inside it.

Steps:

Right click on folder > properties > advance > check mark on: compress contents to save disk “.

Folder name color will be change for blue color.



Notes :

File compressing is bad for computers processor cause as long as its in use its loading on it.

NTFS

Encryption

Is for make encryption on folder or file and that away from permission.

Encryption can be made by “owner “.

Decryption can be made by “owner, recovery agent”.

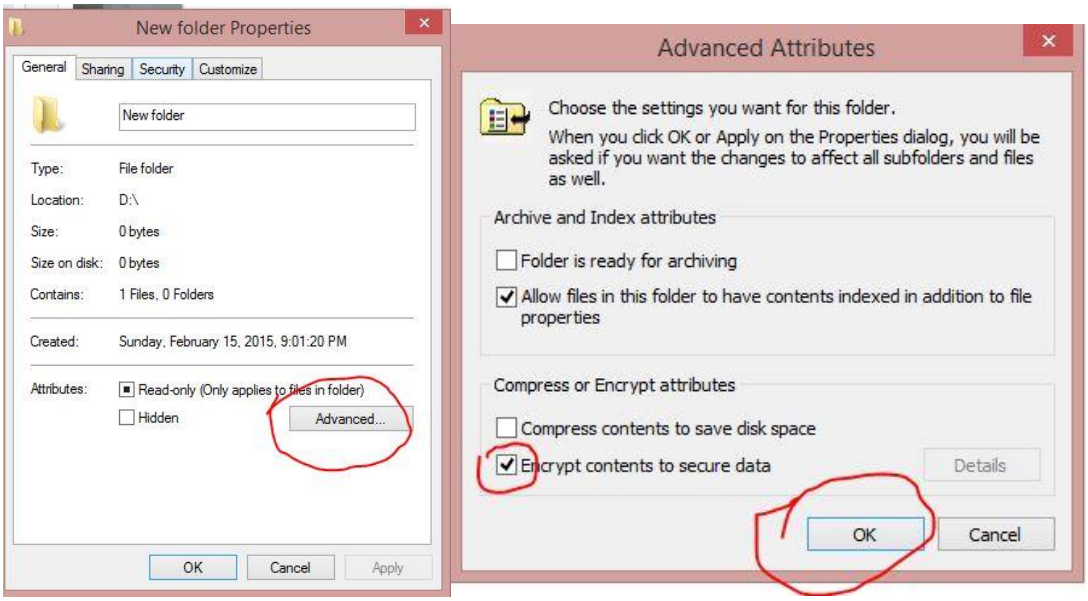
Problem is we can’t depend on permission because as windows system changes all permission will be under control of new windows administrator.

But encrypted folders won’t be able to access because S.ID will be changed so no owner or recovery agent will be able for decrypted or accessing.

Steps:

Right click > properties > advanced > check mark on “encrypt contents of secure”

Color of folder name will be changes for green color.



Standard:

Can’t use compression and encryption in the same time in the same folder.

Standard for "permission, encryption, compression"

In copy and cut from folder to folder and in the same partition, or from partition to partition.

Between " partition to partition"			**Within " folder to folder"**	
Copy	**Cut**		**Copy**	**cut**
Inheritance	Inheritance		Inheritance	Remain the same

EX:

When we have partition D and partition E

Partition D has (HR folder compressed with R permission) and (admin folder with R/W permission).

Partition E has (IT folder compressed with F.C permission) and (H.D folder has modify permission).

- When folder HR moves to IT E:// it will have permission of E:// F.C and modify also will not be compressed,

When HR moves to admin will be the same compressed.

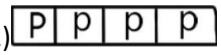
Disk Management

1) Basic disk :

A primary : "up to 4 partitions "

B extended: "logical drivers "

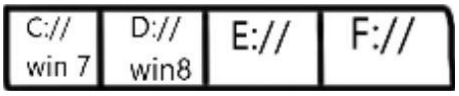
Types:

1) 

2) 

3) 

4) 



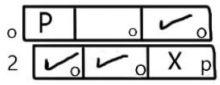
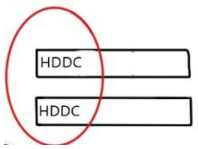
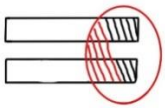
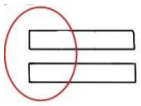
Notes:

When we delete all partitions first partition we going to create going to be automatically primary.

Hard Disk types:

IDE, Sata , SCSI

2) Dynamic disk:

RAID	Mirrored	Stripes	Spanned	Simple
Min 3HDD Max 32 HDD 	Min 2HDD Max 32HDD 	Min 2HDD Max 32HDD 	Min 2HDD Max 32HDD 	Min 1HDD Max 32HDD 
Fault tolerance	Fault tolerance	No fault tolerance Win 8,10 support only this types	No fault tolerance Win 8,10 support only this types	No fault tolerance Win 8,10 support only this types

Introduction in Active Directory

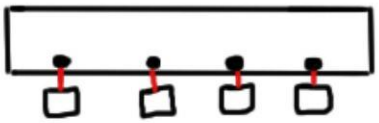
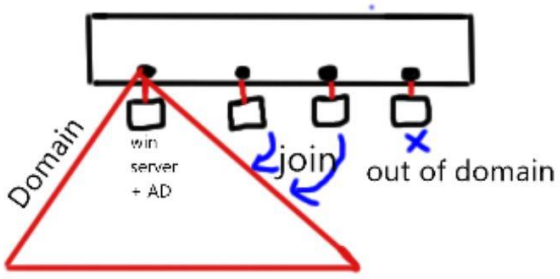
Notes:

- Win 2008 can only work with " full , core"
- Win 2012 can work with " full, core, midi"
- Win 2012 can change from full to core or midi while it's working.

Full: is using full windows programs and features**.**

Core: is working with DOS and save 75% of device performance.

Midi: is working with DOS and full system with less performance.

Work Group	Domain
 - Server/ client - Stand alone - All computers are peers; no computer has control over another computer. - Each computer has a set of user accounts. To use any computer in the workgroup, you must have an account on that computer. - There are typically no more than ten to twenty computers. - All computers must be on the same local network or subnet.	 • One or more computers are servers. Network administrators use servers to control the security and permissions for all computers on the domain. This makes it easy to make changes because the changes are automatically made to all computers. • If you have a user account on the domain, you can log on to any computer on the domain without needing an account on that computer. • There can be hundreds or thousands of computers. • The computers can be on different local networks.

Pc Roles:

	Operating system	Role
Client	Professional Servers	Ask for service
Server	Win server + service	Provide service
Domain controller	Win server + A.D	Manage control

Requirements for Active directory:

1- Win server.
2- NTFS partition.
3- Free space 250mb.
4- DNS server.
5- Static ip “running NIC”.
6- Add “A.D” role.

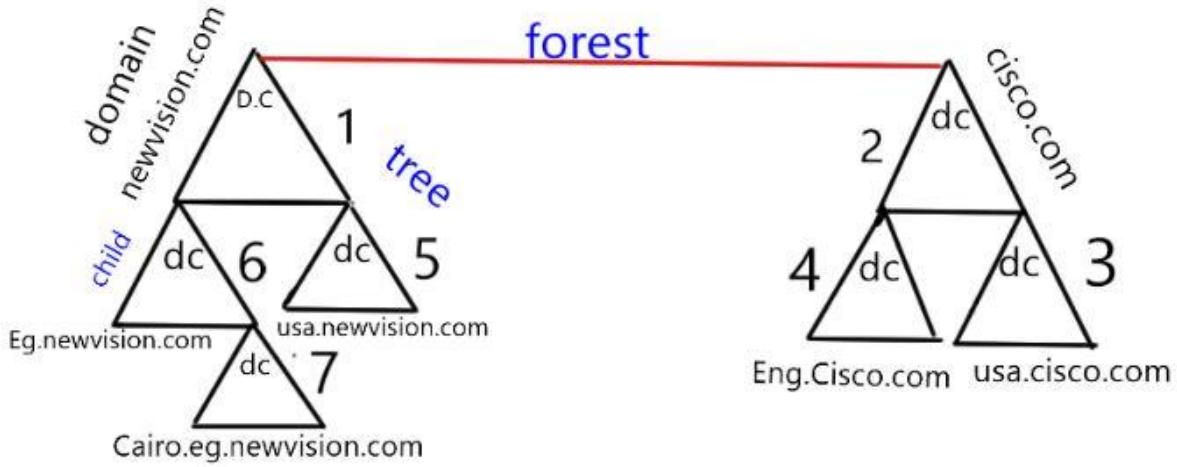
Notes:

For add A.D in win 2008 press Run “DC promo”.

For add A.D in win 2012 from “server manager”.

Network structure

Network structure	
Logical N.S	**Physical N.S**
- Domain - Tree - Child - Forest	- Domain controller - Site



Notes:

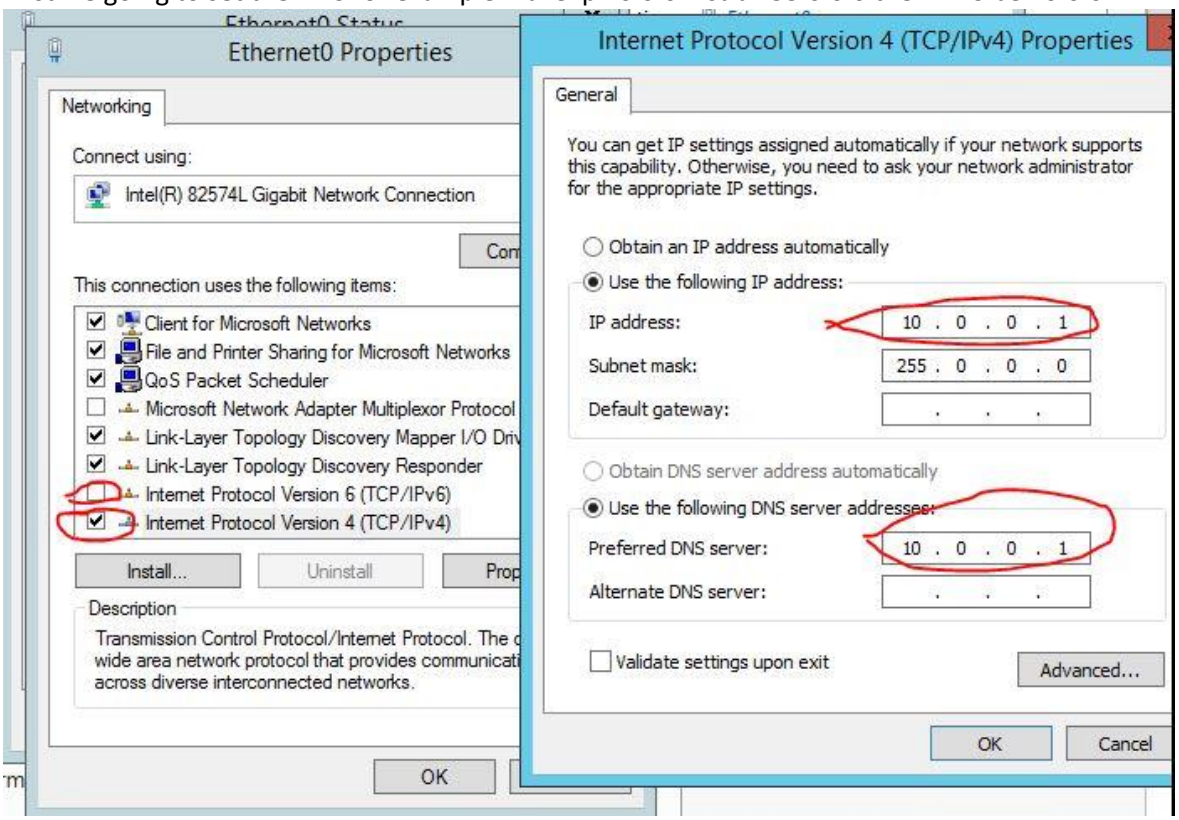
1) Domain which is the main root of tree and forest and parent.
2) Domain of new tree and child's and belong to #1 forest.
3) 4) Child domains are belong #2 domain and belong to #1 forest.
5) 6) Child's domains belong to #1 domain.
7) Child of #6 domain and belong to #1 domain tree.

- Every domain work alone and controlling its users. But all domains are connected to other and they can ping or share files, printers with each other even separated.

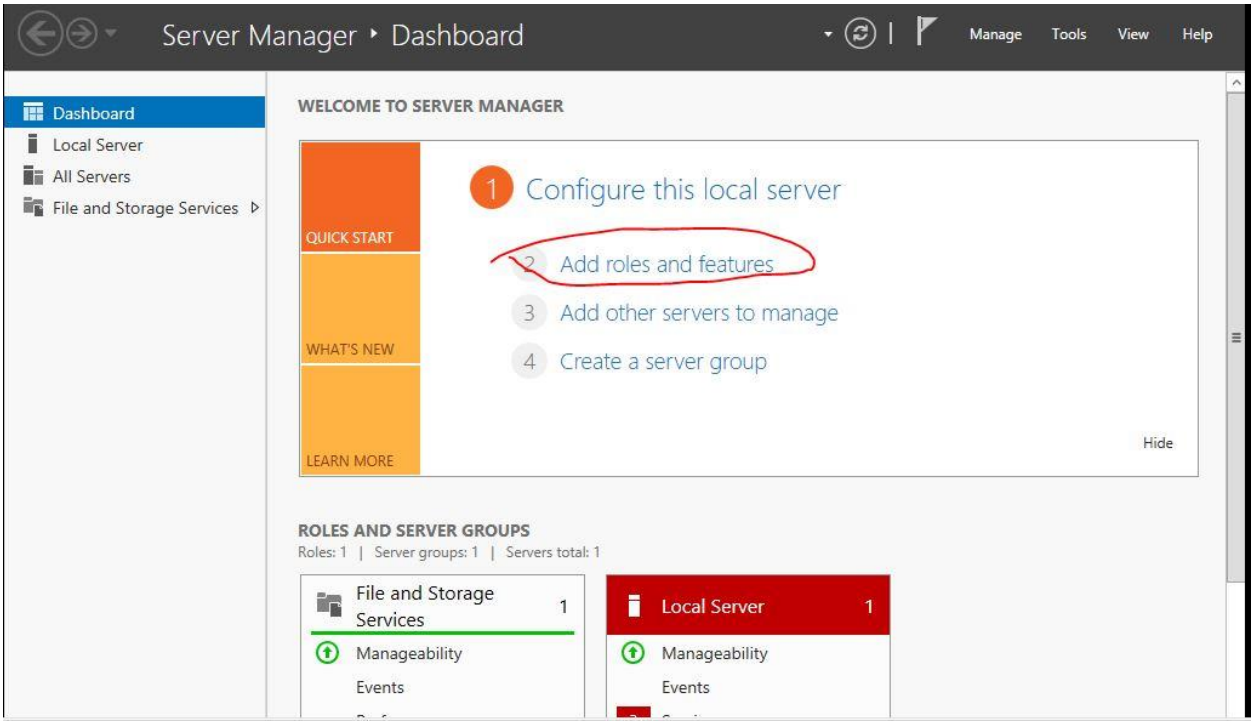
Steps in win server 2012

Steps for create Domain:

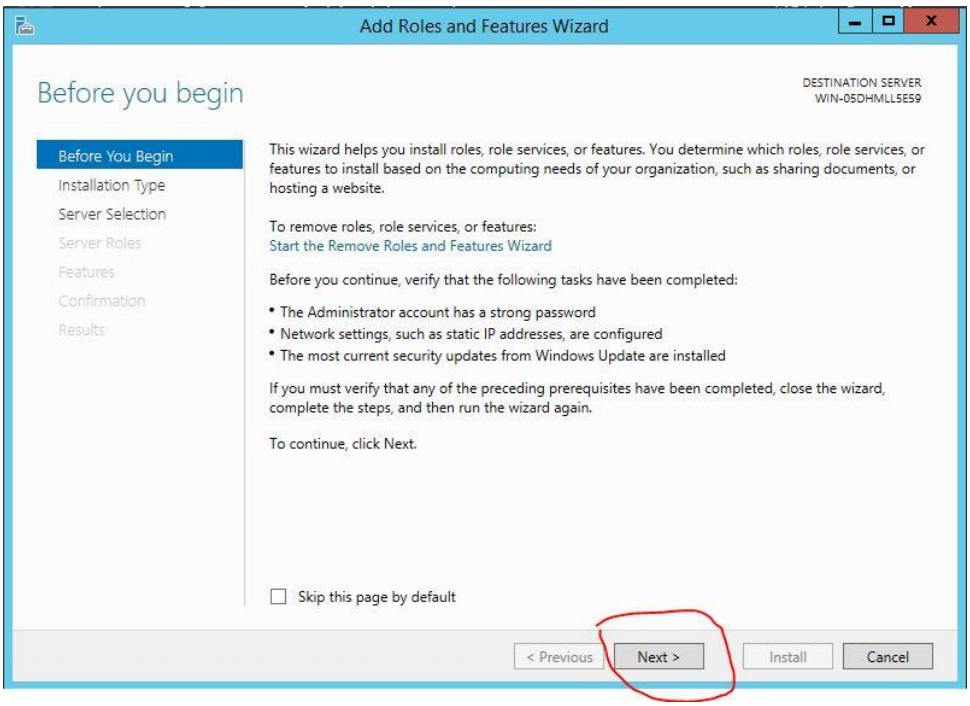
First we going to set the DNS for example make ip 10.0.0.1 sub 255.0.0.0 then DNS be 10.0.0.1

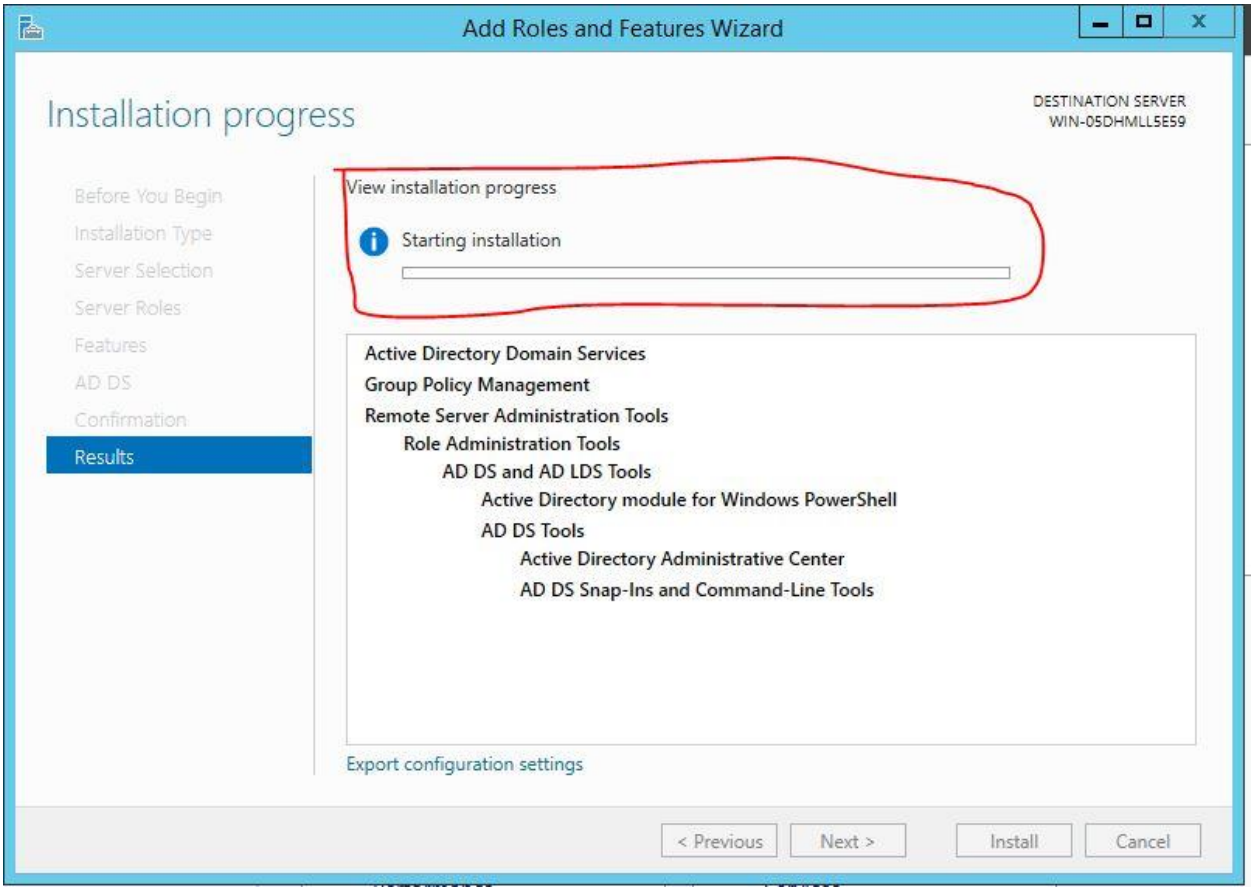


Then press Add role and features from server manager

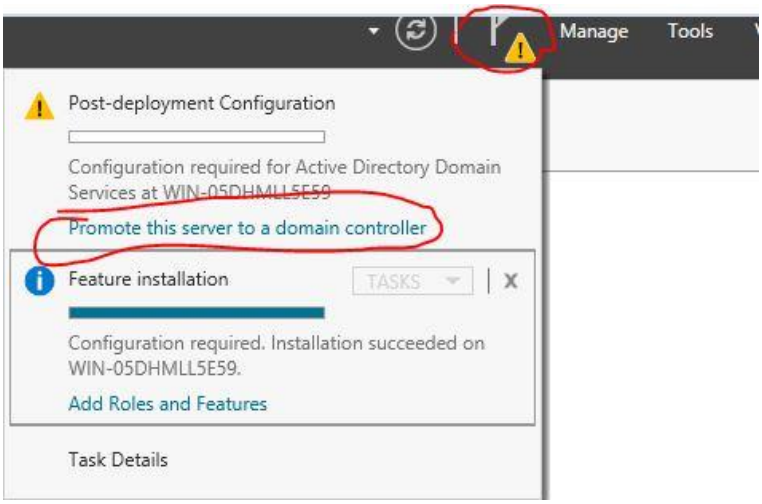


Press next 5 times then press install

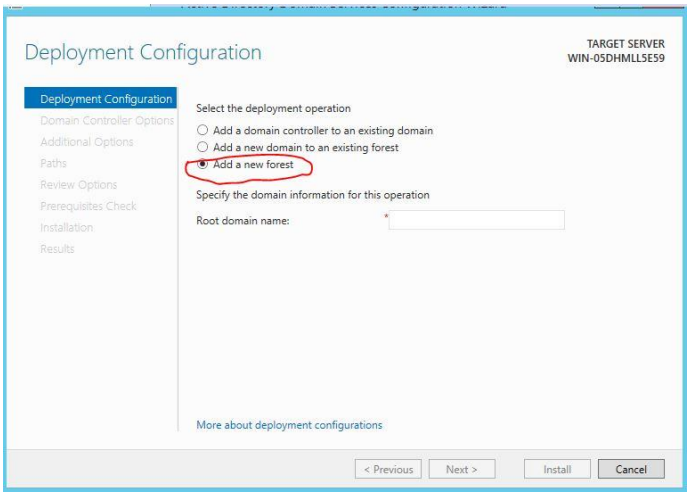




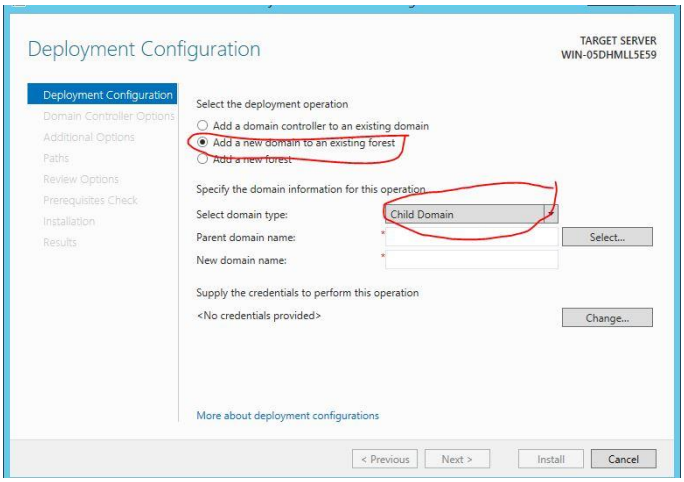
After installation finish will see this caution mark press on it and then press on promote this server



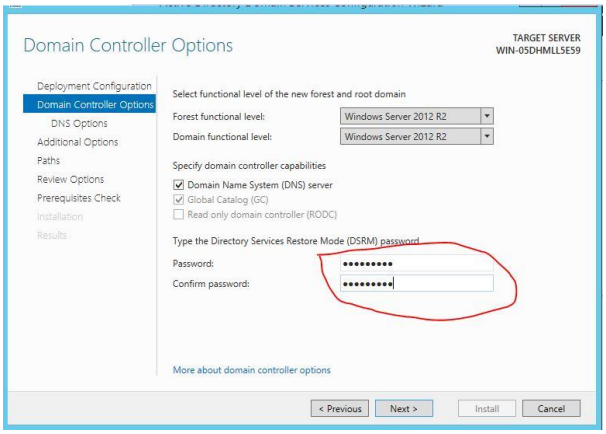
Press on add new forest for create new Domain

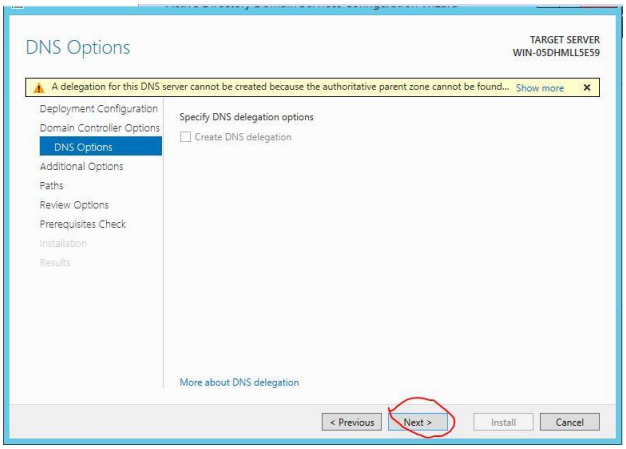


Press on new domain to existing forest for add child or tree. And sure must type domain name and the new domain name.

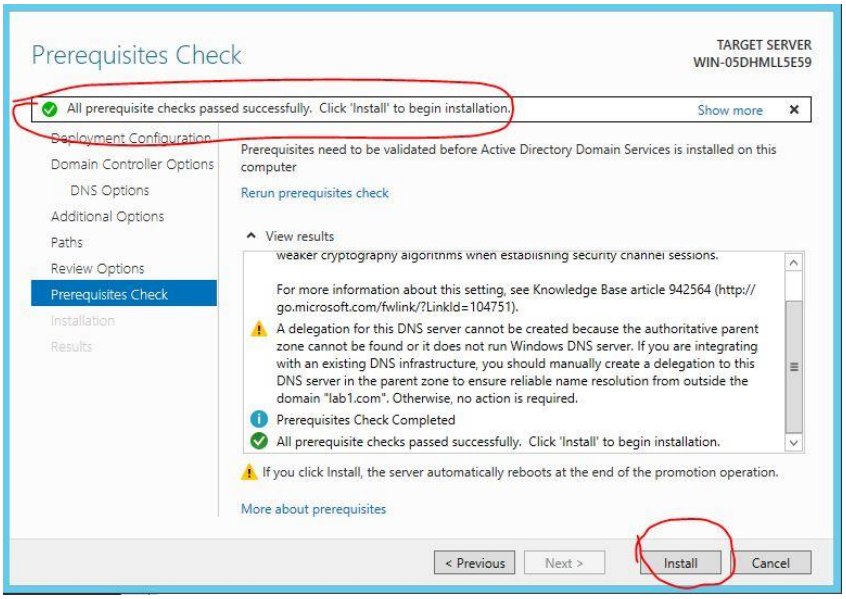


Set password and then press next



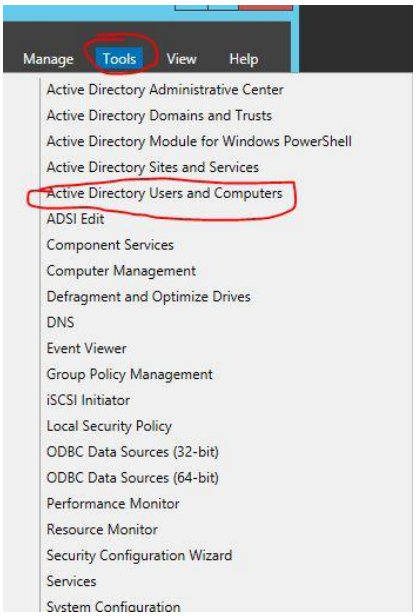


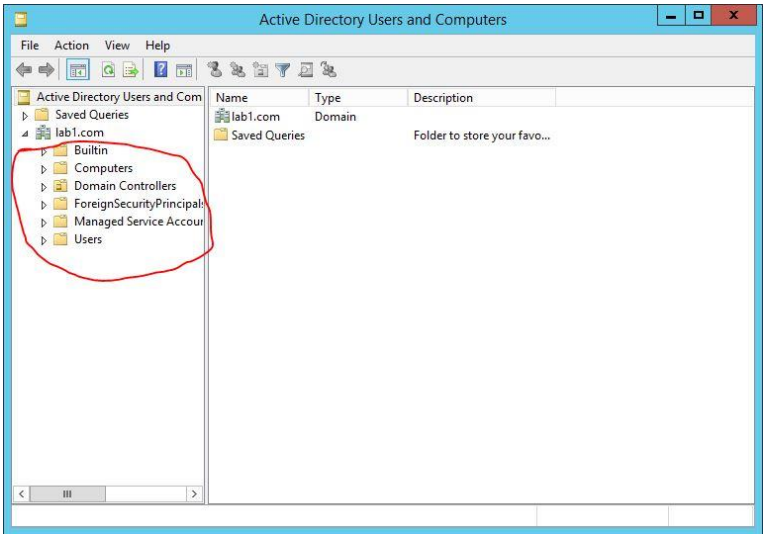
Must see all is fine and no x marks.. Then press install.



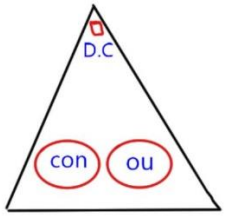
Device will restart for it activate.

Now u have Domain





Organization unit "OU"

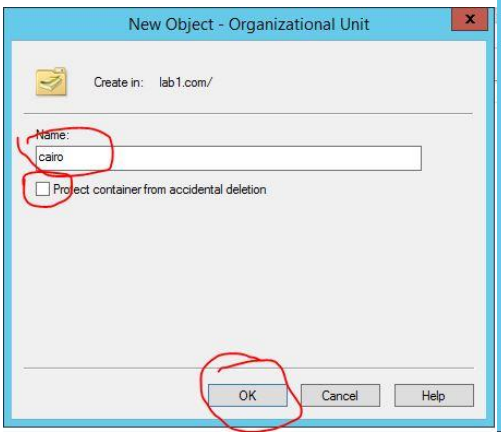
Container	Organization unit
Save only users and computers files without Appling policies.	Can save users and computers files and able to apply policies, create departments and users. 

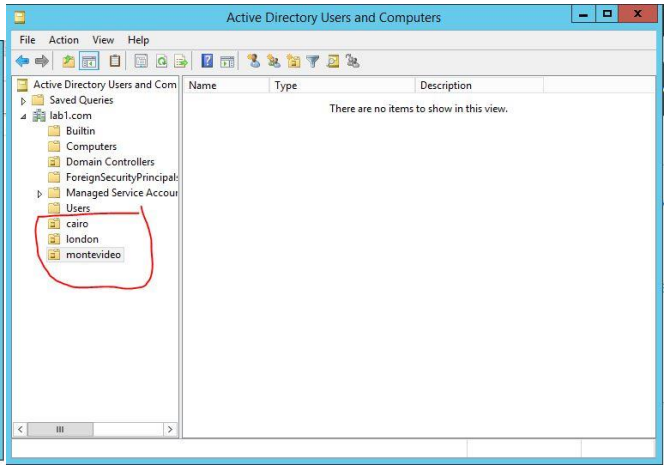
Notes:

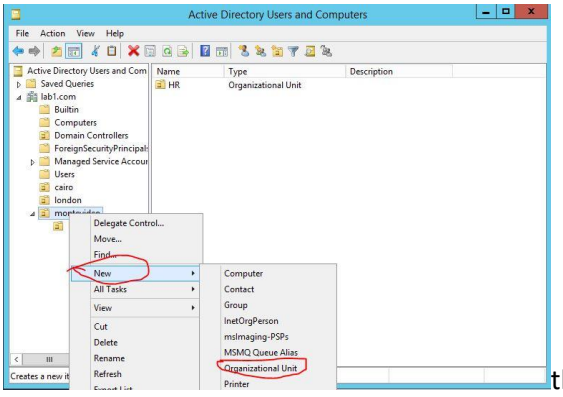
- We can use Ou when we have company with branches with the same protocols and same stable standards.
- If not then we have other option is create domain for each department or branch, but it going to be increase the expenses of IT department cause it going to need increase the IT team.
- If have problem with the current exist domain we need the CEO agreement for establish new domain.

EX:

Company Lab1 has 3 branches with departments. For create new OU







then we start create users and add policies.

Domain object

- **Domain object:**

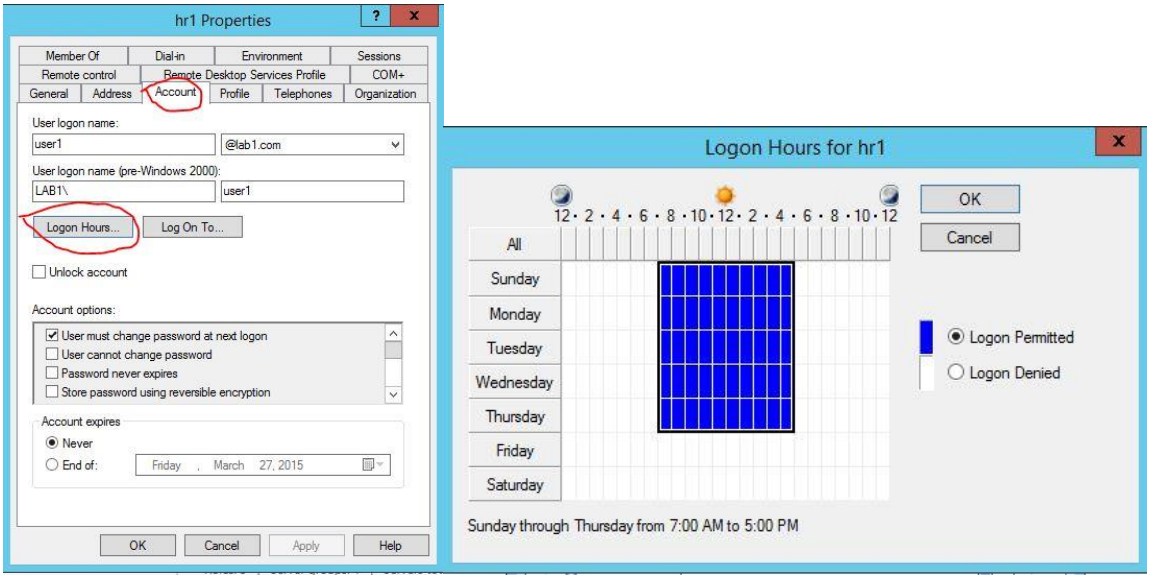
1) User account 2) computers account

After join domain with users a computer account would be created in container file.

Notes:

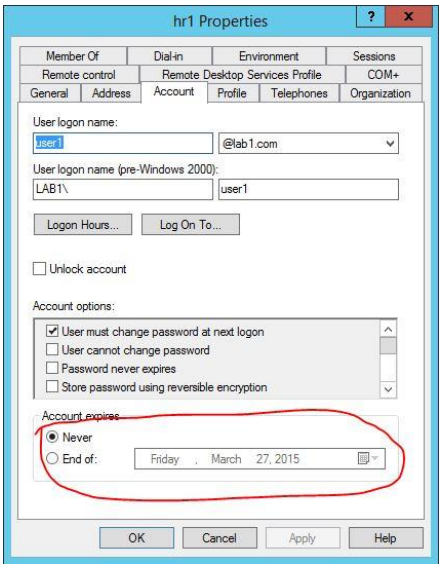
- User can login from any device in the same domain but just not be the domain controllers.
- For make user enter from specific computer and specific duration shift..

Steps: user properties > accounting tab > set time > set computer.



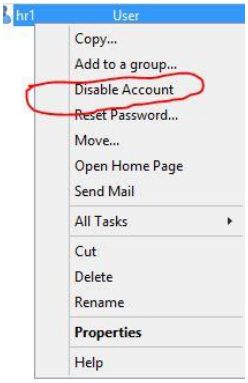
- For make user have expire date for specific user for employers which work part time contracts.

Steps: user properties > accounting tab > expired date set.



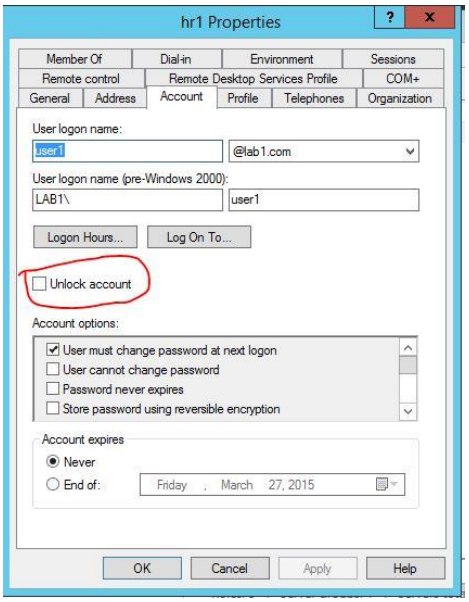
- For disabled/ enable users

Steps: right click > enable / disable.



- When user account type his password 3 times wrong it going to be locked.

Steps: user account tab > press unlock.



- For apply policies on user must give him option for he create his own password for can judge on him incase something wrong happened because only him have his own pw.

Steps: from its option while making new user account.

Group policy object "G.P.O"

- What the difference between user rights and permissions?

User rights: is on system at general EX" can't add user, change clock".

User permissions: is on specific object or folder EX" printer, file".

- **G.P.O History:**

It started with new technology corporation with system policy it like group policy but it's not categories, so when we need to search in whole policy for find what we want, but it didn't success in make advertisements for NT operating system until Microsoft hijacked the New technology, and then they edit the system policy and made categories for policies EX" Desktop, administration, etc.." then they called it Group policy object.

We not need to save all policies in our brain, enough we know the tools and how we do it perfectly.

G.P.O contents of:

%	**Computer configuration**	%	**User configuration**
-50% -90% -10%	- Deploy s.w" s.w settings" - Deploy security "win settings" - Adjust desktop setting" admin. Temp"	-50% -10% -90%	- Deploy s.w " s.w settings" - Deploy security " win settings" - Adjust desktop settings "admin. Temp"

Notes:

- Group policy able you for control everything from your device.
- Computer configuration is for apply on common.
- User configuration is for apply policy for specific users.
- For access G.P.O have 2 ways :
- 1st run > gpedit.msc
- 2nd run > mmc >file> add snap in. " Microsoft management console"
- Can't apply policy on computers on common and then apply user configuration for except it.
- Even windows professional client has G.P.O.
- G.P.O is little bit like roaming what we apply on user will find it in any computer we going to use.
- Computer settings policy will be difference that any user will find the policy of computers.

- **G.P.O levels:**

1) Site
2) Domain
3) OU
4) local

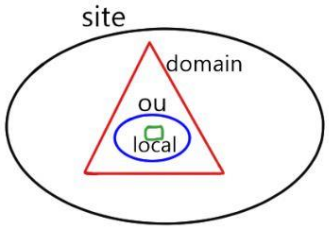
- **For start site or domain or OU.**

Steps:

Server manager > tools tab > group policy management.

That how we can add policy on site or domain or OU

Local from mmc or gpedit.msc.



G.P.O conflicts:

There priorities for levels while applying policies.

" 1) OU 2) domain 3) site 4) local"

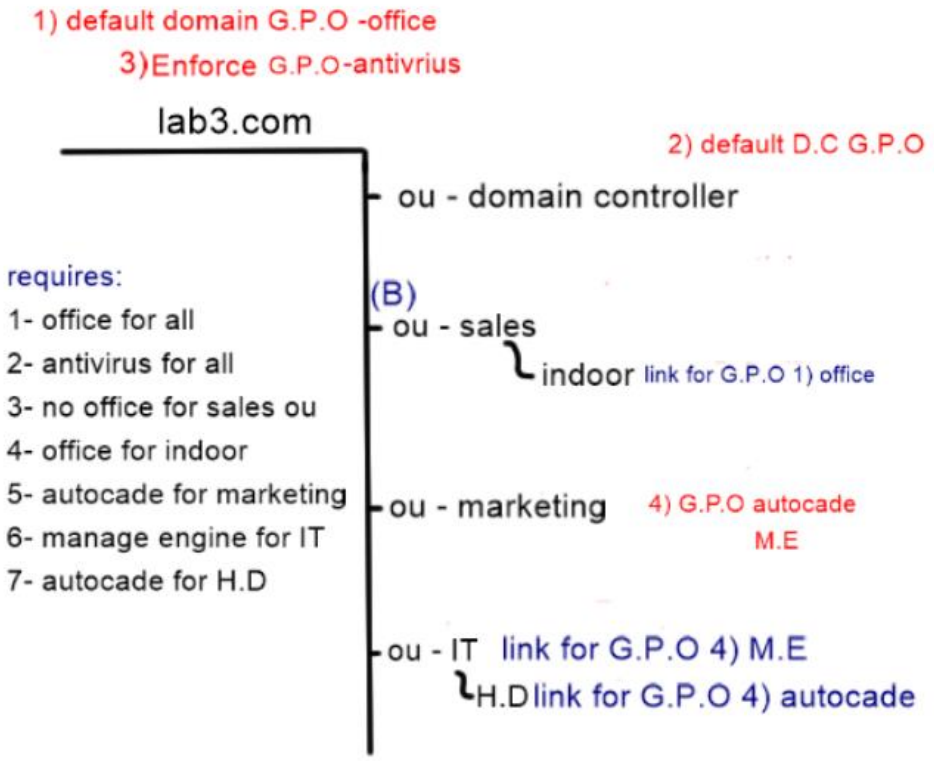
For example hen we have wallpaper policy on "Site with red " and " blue on domain" " green on OU" " orange on local".

Then which going to apply is the policy on OU.

- Local can apply it policy only when it's out of site and domain

- **Standard**:
  When we're in enterprise we must use the most less G.P.O.
  Ex: better use 200 G.P.O than 2000 G.P.O as it give me my needs.
  Reason: as per G.P.O increase the traffic on network because every 90 mins the group policy make update and it refresh and load all the G.P.O the enable and the disabled features.

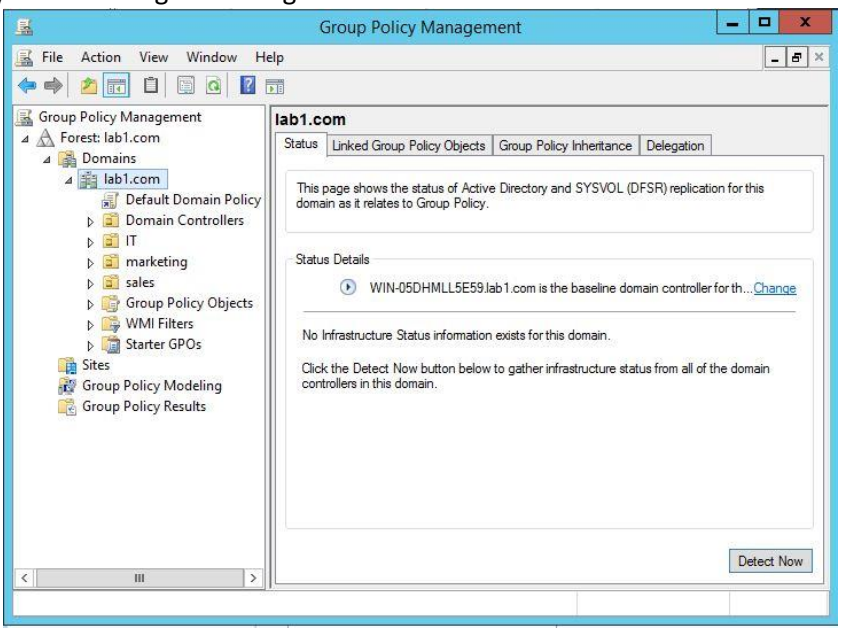
Scenario 1:



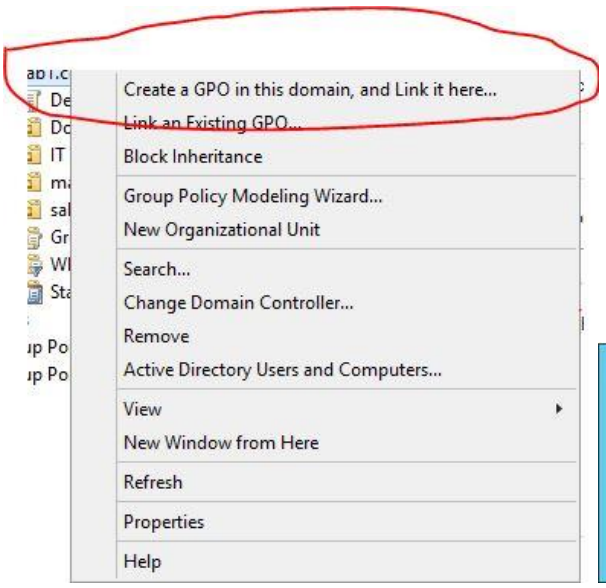
- **Description:**

- 1) Deploy office and antivirus and it going to use inheritance for deploy on all Ou's.
- 5) Deploy AutoCAD for marketing and H.D
- Use block for sales Ou don't get office but H.D wont inheritance the office.
- Deploy G.P.O antivirus on sales and it will inheritance to indoor.
- Deploy G.P.O management engine.

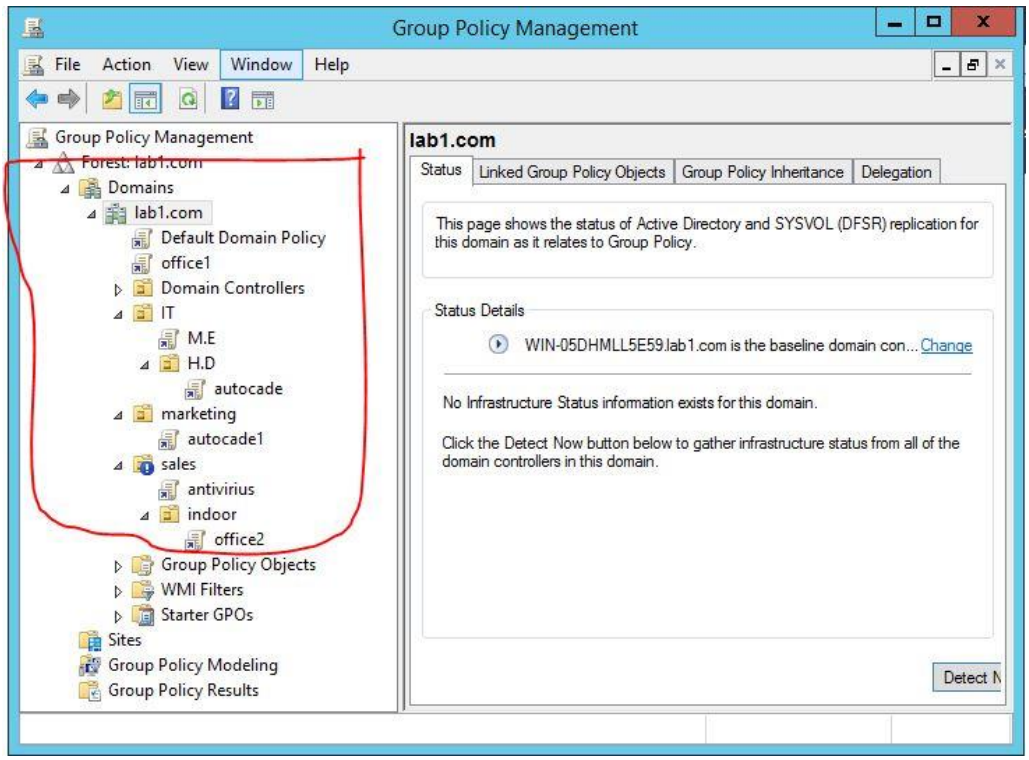
- **Steps**:



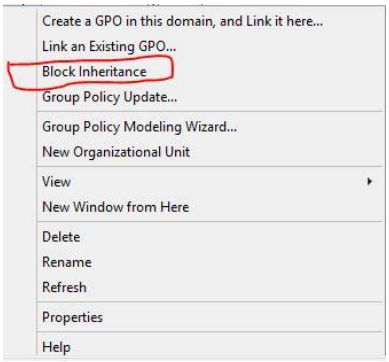
Create G.P.O


Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Active Directory Users and Computers...
View
New Window from Here
Refresh
Properties
Help


New GPO
Name:
office
Source Starter GPO:
(none)
OK
Cancel


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: lab1.com
Domains
lab1.com
Default Domain Policy
office1
Domain Controllers
IT
M.E
H.D
autocade
marketing
autocade1
sales
antivirius
indoor
office2
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
lab1.com
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
This page shows the status of Active Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.
Status Details
WIN-05DHMLL5E59.lab1.com is the baseline domain con... Change
No Infrastructure Status information exists for this domain.
Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.
Detect N

Make block for sales Ou



- **Steps for make block:**

Server manager > tools > group policy management > choose sales Ou > properties > block inheritance.

- **Group policy update:**

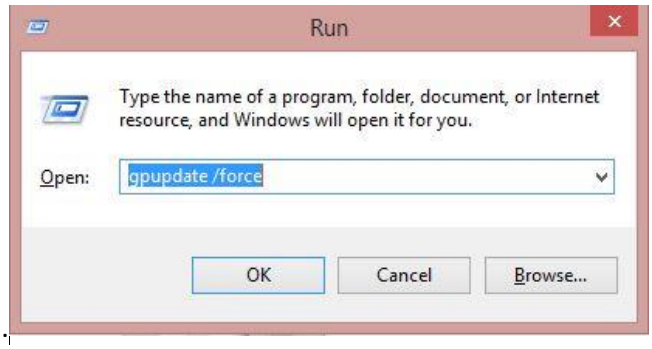
Is update happens every 90 min's or restarting if on computer but if on OU user will be every 90 min's

Or logging and logoff.

- **Steps for make update before 90min:**

1st normal way:

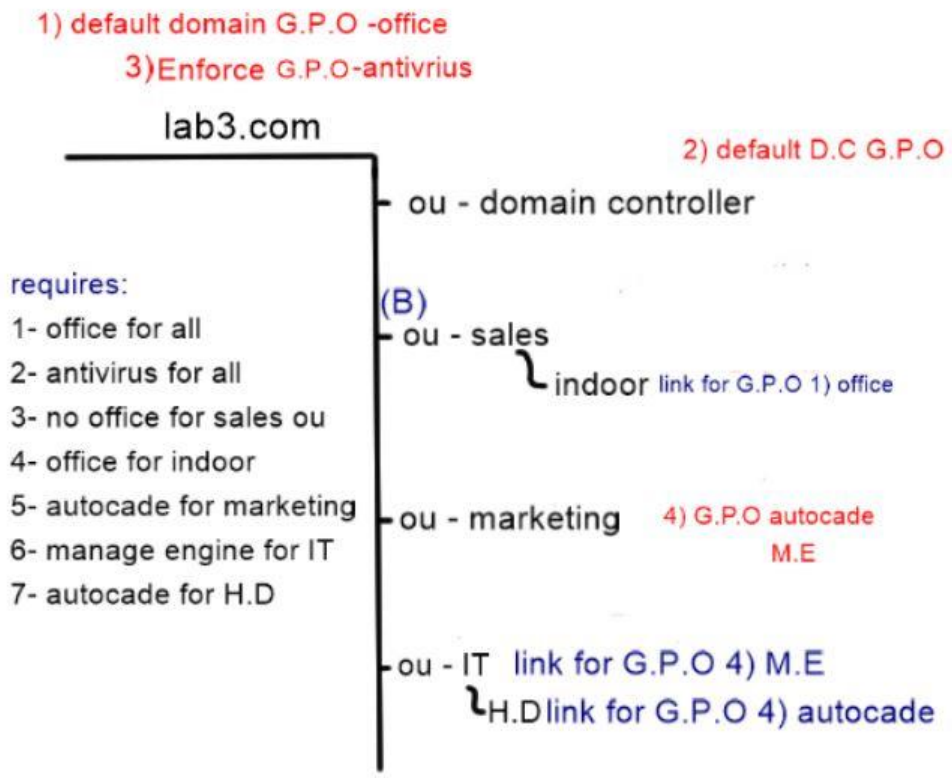
Run > type > "gpupdate /force.



2nd advanced way:

Run > type gpupdate /force/wait "time".

- **Scenario 2:**



- **Description**:

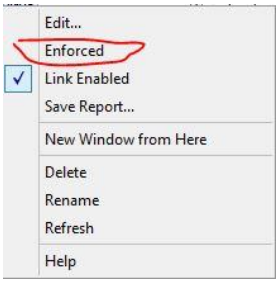
1. We already have 2 default G.P.O of domain and domain controller, so for we not use a lot of G.P.O we put in 1) default domain G.P.O office., and made 3) enforce for antivirus for it reach sales and indoor,
2. Made 4) G.P.O management engine and AutoCAD.
3. Now we just made 4 G.P.O only and it give us all our need from group policies, in the end is up to ever IT specialist " so don't save 1 way in make it".
4. Before you start create you must make design like pervious for see the best way to get your needs and G.P.O's.
5. For indoor ou have office we made link to get it from 1) default domain G.P.O.
6. Block option for Sales for it don't get office.
7. Made enforce for antivirus for it reach sales ou and indoor.
8. Made link for IT and H.D to get them G.P.O.

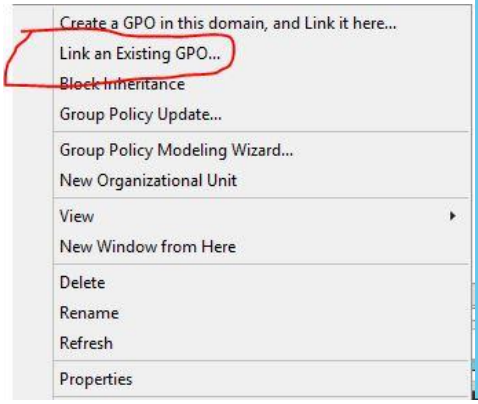
- **Enforce:**

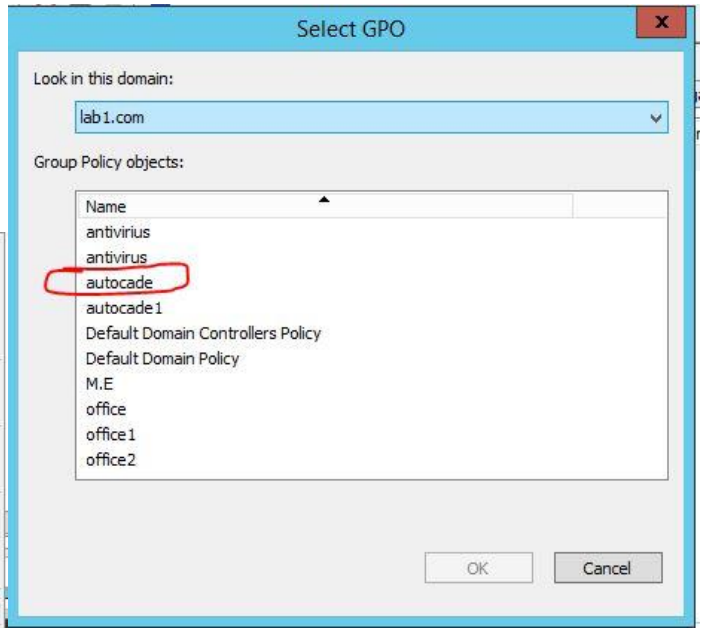
For deploy antivirus even block inheritance we use enforce for make antivirus don't be blocked on sales Ou and inherit to indoor.

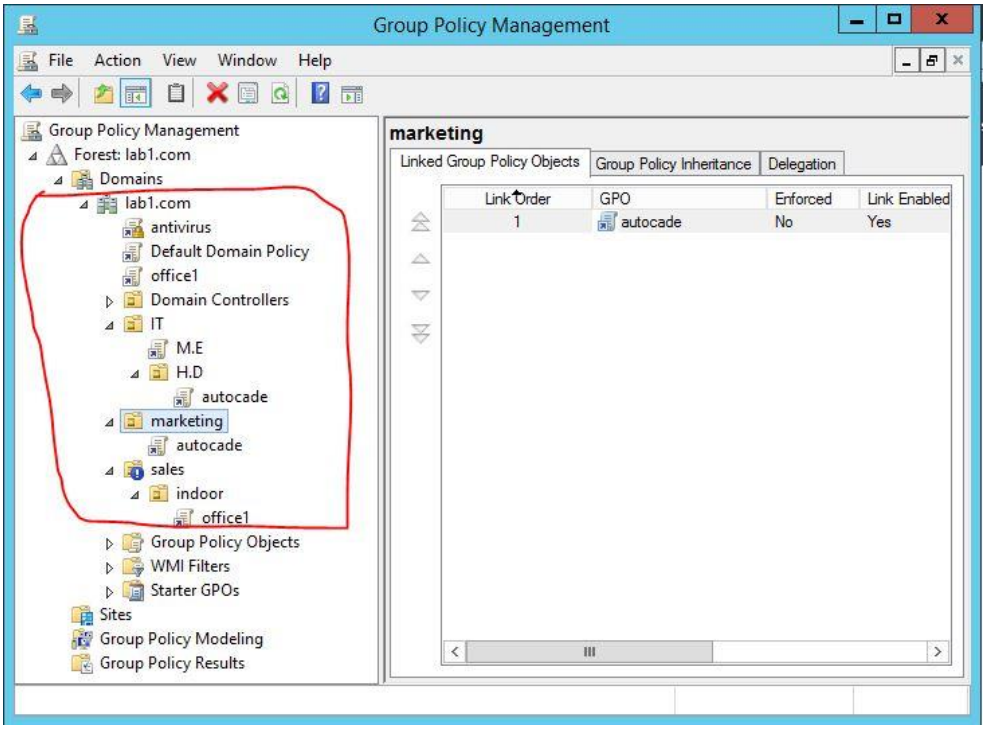
- **Steps:**

Server manager > tools > group policy management > choose sales Ou > properties > enforce.





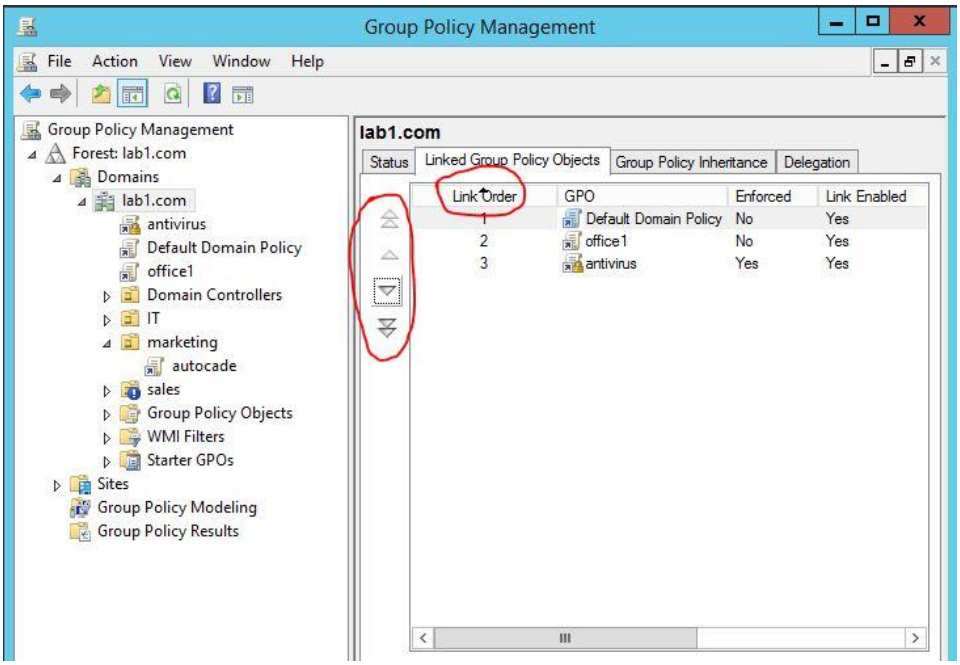




- **Link order:**

When we have 2 G.P.O have conflicts in order which going to be have priority to apply is which are in top of link order list.

For not use too much G.P.O we can use link way that if the G.P.O are already exist in other G.P.O will make link to direct it for it.



Notes:

- When the domain conflict happen in password G.P.O will deploy its policy and not the OU, because password level deploy on domain only.
- Expect when use domain/forest functional level 2008/2012.

- For disable G.P.O we press right click then unmark "link **enabled** "that will disabled until other action being taken.

G.P.O Editing:

There 3 options inside any policy "not configured, enable, disable"

- Not configured: is has no action but is on standby for any action taken.
- Enable: is make the policy activated.
- Disabled: is make policy not activated.

Ex:

When domain has G.P.O for hide control panel and is enabled and if in domain is not configured and is disabled on OU "what going to deployed is the OU".

If domain is not configured and is disabled on OU " the OU is going to deploy its G.P.O".

If is disabled on domain and not configured on OU "the domain is going to deployed its G.P.O"

DNS
Domain Name System

DNS:

1	DNS definition		
2	Types of names		
3	Host name		
4	Net bios name		
5	DNS process		
6	Host file		
7	LM file		
8	Types of query		
9	Root hints		
10	Installing DNS service		
11	Configuring DNS		
12	Forward lookup zone		
13	Reverse zones		
14	Types of zones		
15	Primary zone		
16	Secondary zone		
17	Stub zone		
18	Active directory integrate zone		
19	Creating zone		
20	Zone properties		
21	Server properties		
22	Zone transfer		
23	Forwarding		
24	Conditional forwarding		
25	Root zone		
26	Start of authority " AOS"		
27	Monitoring		
28	DNS records		
29	Host record		
30	PTR record		
31	Alias record		
32	Max record		
33	Backup		
34	Planned design		
35	DNS and active directory		
36	DNS requirement for A.D		
37	SRV		
38	Dynamic update		
39	Master browser		
40	suffix		

1) Definition: #1

DNS: is server for resolve name to IP.

EX: www.yahoo.com will be http://69.147.76.15

Host name & Net Bios name: #3, 4

Name			
Host name		**Net Bios name**	
EX: ayman.lab4.com	DNS	**Ex**: ayman Ayman.lab4.com	WINS

Notes:

- DNS is resolving name to IP, because you can't achieve site without add.
- Every dot in host name have it job for define the name and domain.
- Net bios name can write the full name like host name but dots won't have the same job for define the name and the whole going to be name for net bios.
- Until 2003 net bios name was use "WINS" for resolving it until 2008 it start use DNS.
- WINS: is windows internet naming system.
- Now days DNS resolving both host name and net bios name.
  But its use only the first 16 characters 1st 15 for name 16th is for service or tag or role.

- **DNS process: #5**

When u want enter yahoo website and type www.yahoo.com

1st it's going to check the device cache if it have the ip already or not.

For clear the cache list ">ipconfig/flushDNS"

2nd Host File: #6

It going to check it if didn't didn't find record in cache

Destination "system32 / drivers / etc"

3rd LM Host: #7

And is for check name in net bios names list

Destination "system32 / drivers / etc "

4th check DNS

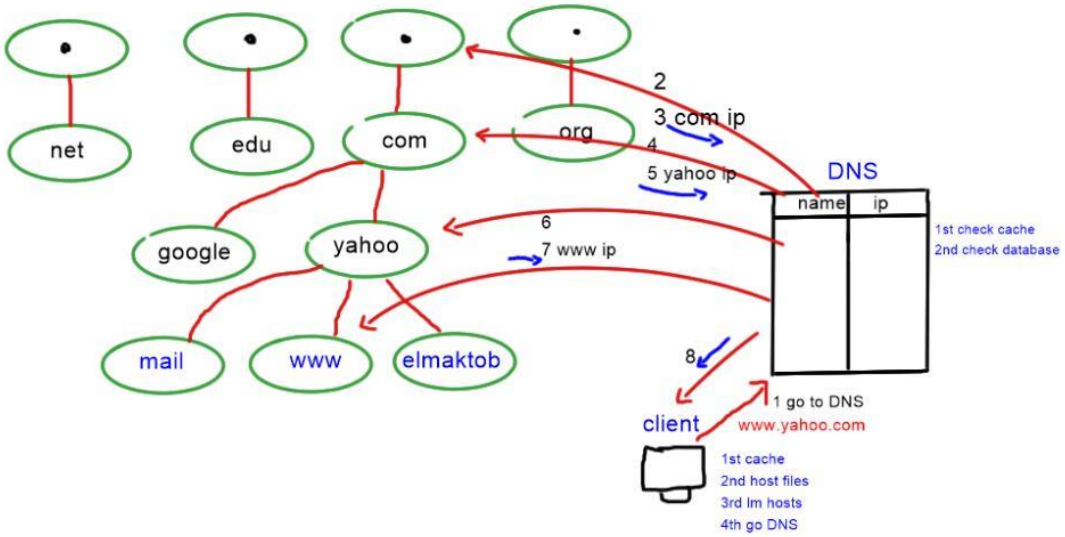
If last 3 steps didn't success in find the ip already by user pc it going to check it in the DNS

First it going to check the DNS cache then the Data base of DNS.

If it didn't success in find it it will go to the root hint the base of all servers.

- **Root Hint: #9**

Is the root and base of all servers Dot "."



- **Types of Query: #8**

1) Iterative query : " complete answer "

And is like when user ask DNS it Search and back with ip address to user.

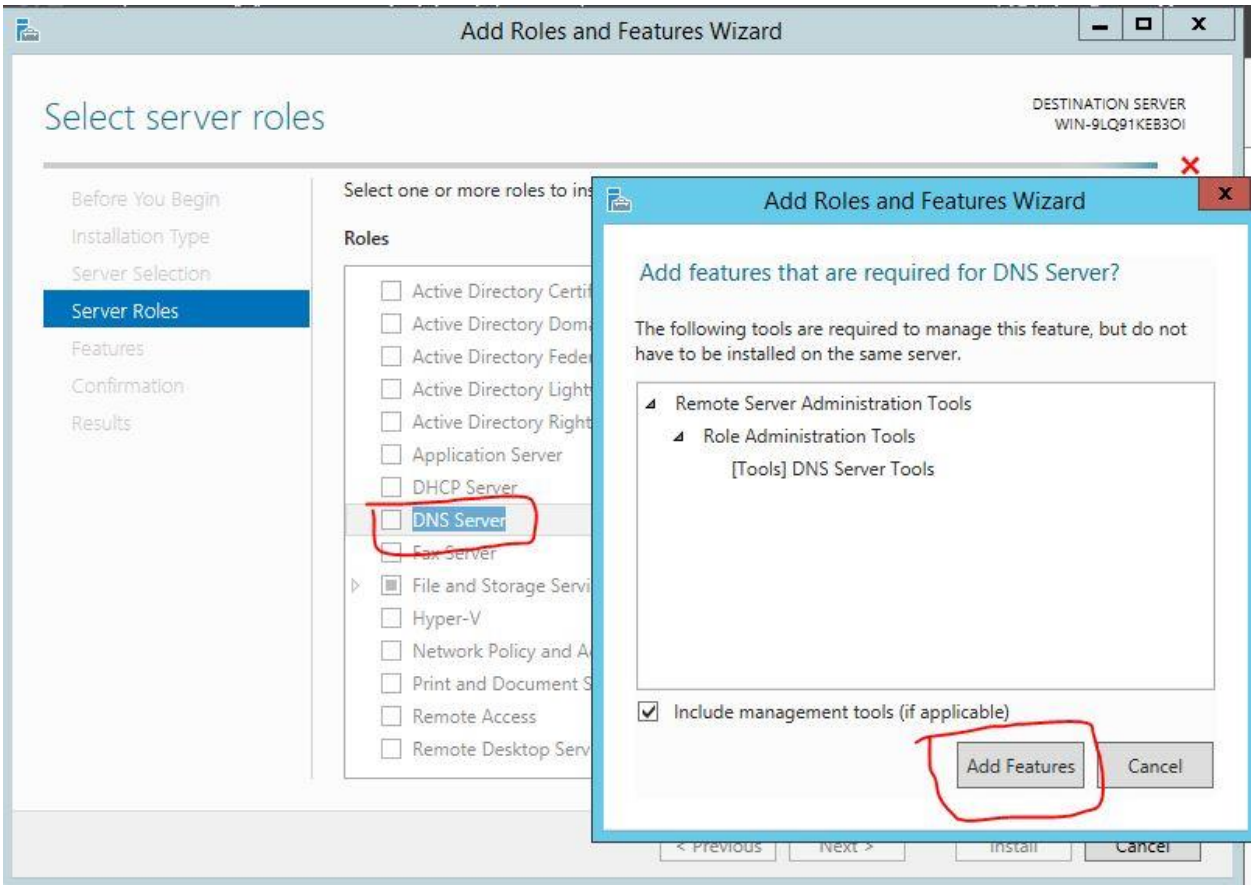
2) Recursive query: " best Answer"

And is like when DNS ask DNS it show it the best way to get the answer.

- **Installing DNS role: #10**

Steps: "server manager > add role > next > DNS> next > install "

Installing the DNS only not mean the service is work, must with configuration.



- **Forward zone : # 12**

Is for resolve name to IP " www.yahoo.com >http://69.147.76.15

- **Reverse zone: #13**

Is for resolve name to ip " http://69.147.76.15 > www.yahoo.com

Notes:

- **Forward lookup zone** must be the same of the domain for it work, and its preferring that before make it ask the manager for names and plan for work.
- **Reverse zone** must keep in the same network for it work.

- **Master browser: # 39**

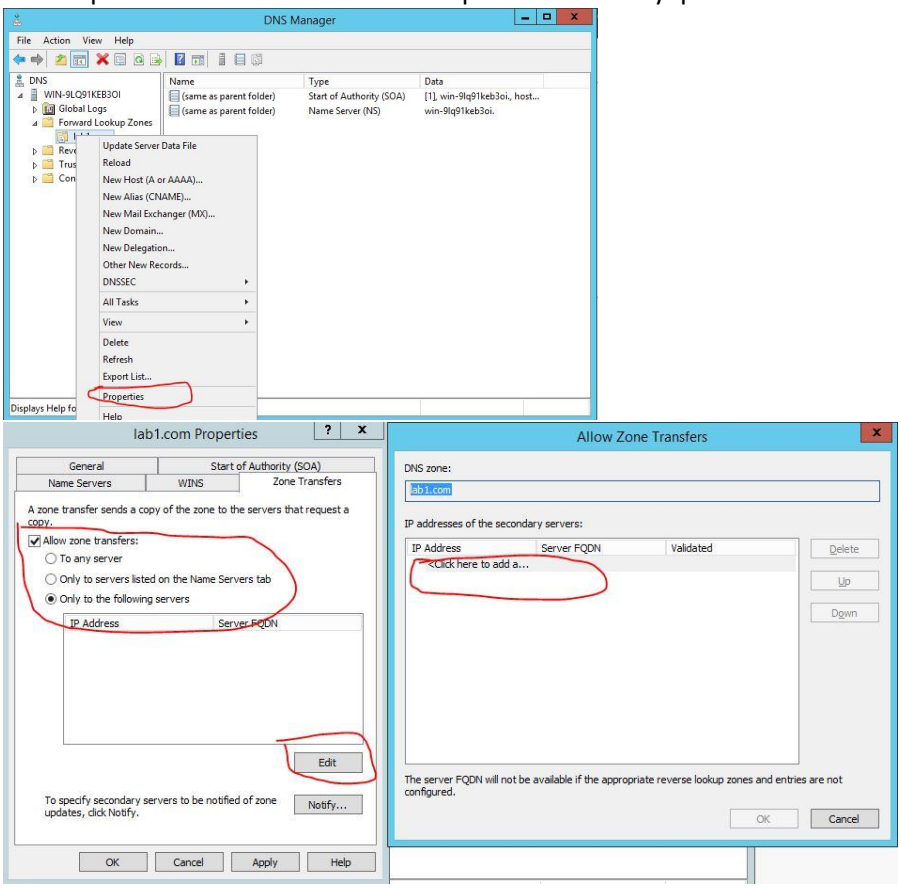
Is pc's in network they auto elect pc of them for be master browser nd it have role near of DNS in the network but automatically without configuration and by it you can run the ip of pc and open its shared folders for example.

DNS zones #14

Primary #15	Secondary #15	A.D integrated #18
- R/W version - Only 1 zone per topology - Can be installed on any server - " member , stand alone , D.C"	- Read only version - Unlimited zones - Can be installed on any server - " member , stand alone , D.C"	- R/W version - Unlimited zones - Can be installed on D.C only - Secure updates only

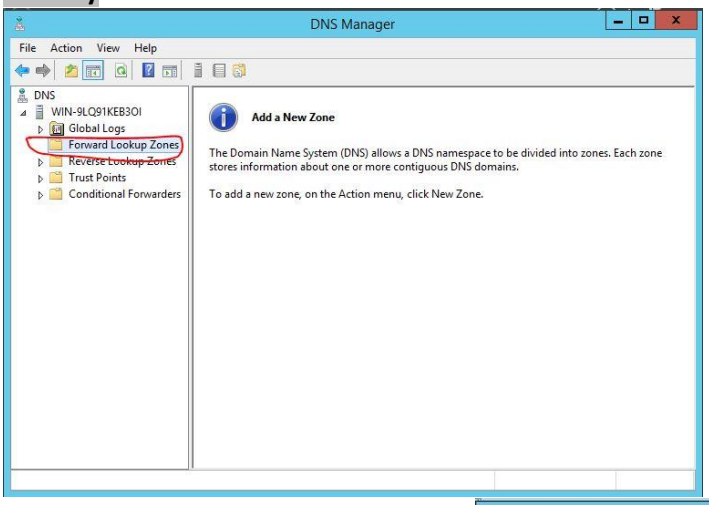
Notes:

- **Primary transfer** updates to other secondary.
- **Primary** can be installed on any server whatever is domain controller or standalone out of domain or member of domain.
- **For start transfer** must make in primary allow properties.
- **Steps**: right click on zone > properties > zone transfers > choose allow kind. there option to all servers or can add specific servers by ip.

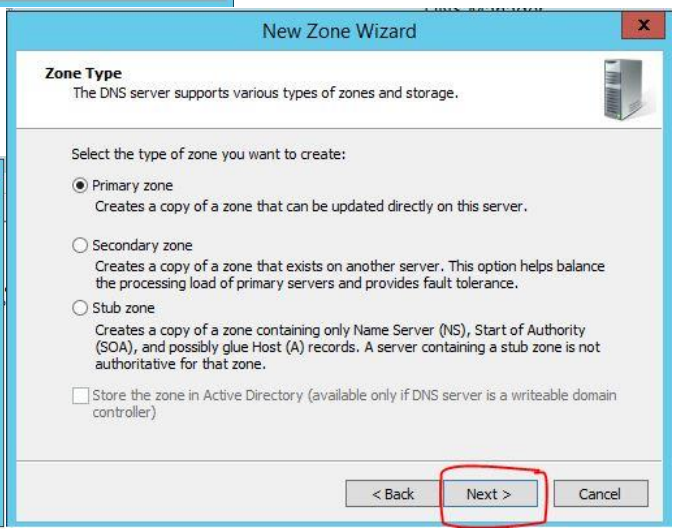


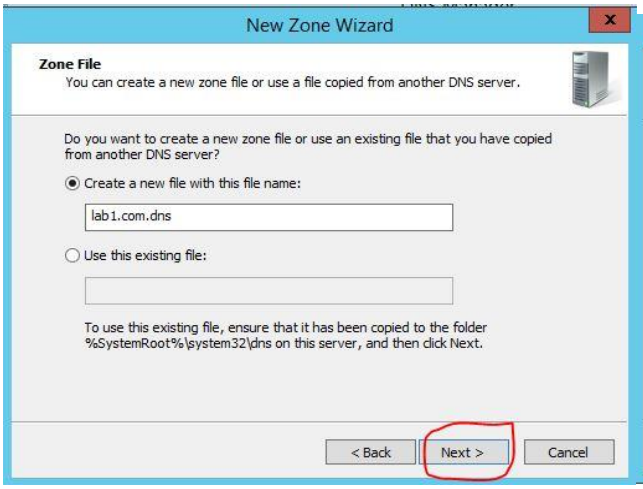
- **Secondary** zone must be have preferred DNS same ip of primary and the alternate DNS server is the same of your secondary ip.
- Sometimes firewall block the DNS transfers.
- **Primary** can make only one zone and others must be secondary.
- **Active directory integrated** can be installed unlimited only on domain controllers.
- **Active directory integrated** secure transfers updates only that mean it won't send all record list, just the updates.

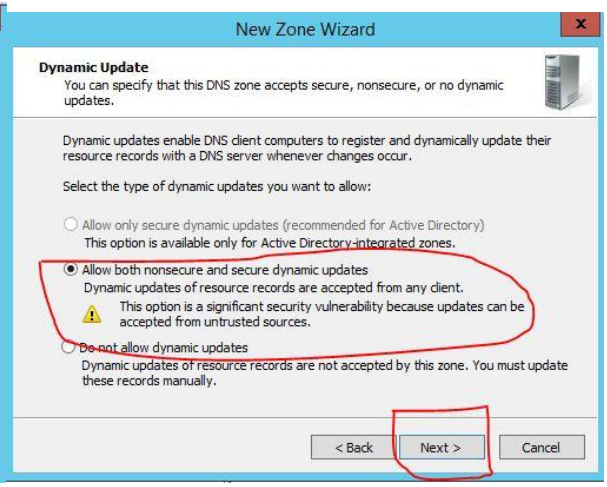
- **Primary**:


DNS Manager
File Action View Help
DNS
WIN-9LQ91KEB3OI
Global Logs
Forward Lookup Zones
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Add a New Zone
The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone stores information about one or more contiguous DNS domains.
To add a new zone, on the Action menu, click New Zone.

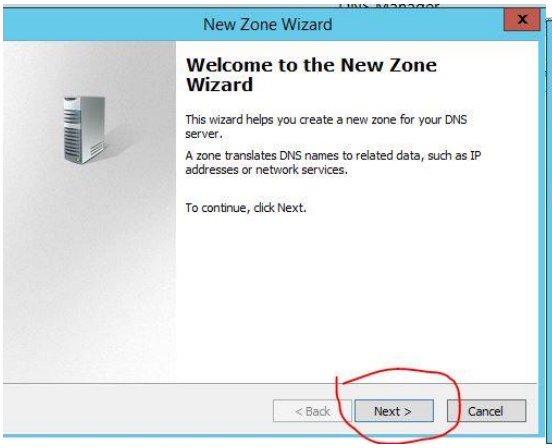

New Zone Wizard
Welcome to the New Zone Wizard
This wizard helps you create a new zone for your DNS server.
A zone translates DNS names to related data, such as IP addresses or network services.
To continue, click Next.
< Back
Next >
Cancel

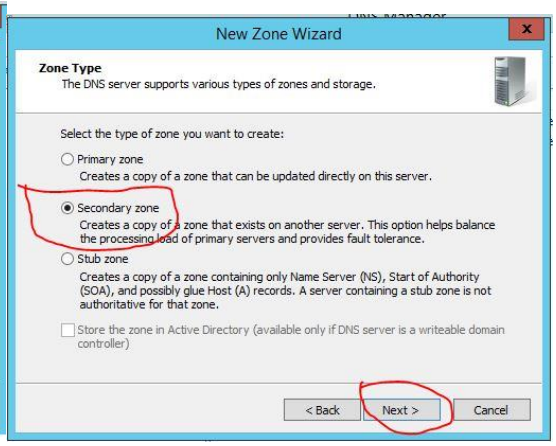

New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next >
Cancel


New Zone Wizard
Zone File
You can create a new zone file or use a file copied from another DNS server.
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?
Create a new file with this file name:
lab1.com.dns
Use this existing file:
To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.
< Back
Next >
Cancel

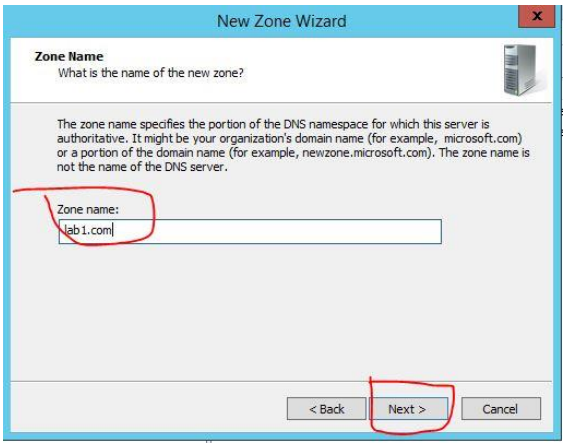

New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel

- **Secondary:**

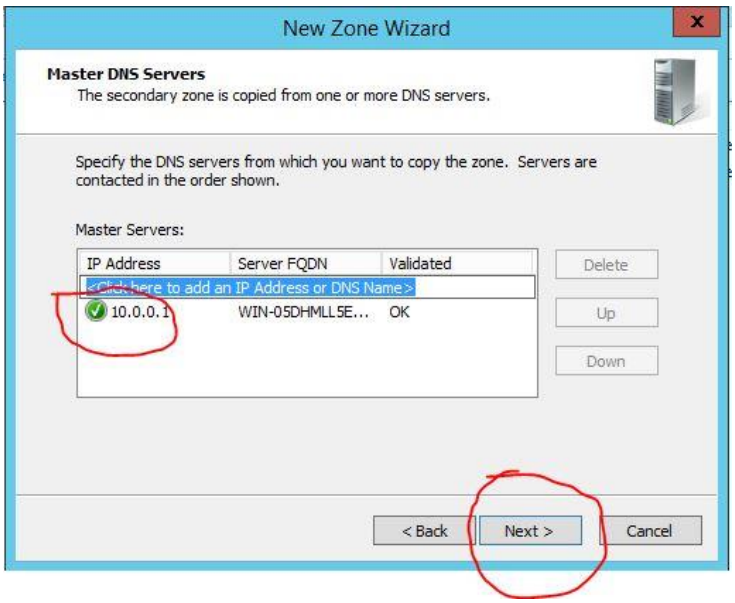




Here we write name of domain



Here we type the Ip of primary DNS



DNS

Active directory integrated

- **DNS requirements for A.D.I :**

1- At least 1 forward lookup zone.
2- Matching name space.
3- DNS supporting dynamic update
4- DNS supporting SRV “service”.
5- Suffix name “ is by enter computer name an press more and add domain”

- **Zone properties:**

General:

- **Status**: is for start or pause it.
- **Type**: which type of DNS need to change it “ primary or secondary or stub”
- **Dynamic update**: none or non-secure and secure for primary, and for integrated it has 1 more option is secure for users inside domain.
- **Aging**:

- **Zone transfer:**

Allow zones transfers::

A) To any server:

Is to transfer to any ip in network and is not secure.

B) Only to servers:

Is allow transferring to specific by name.

C) Only to the following:

Is by add specific ip's and allowing transfers most secured.

- **WINS**:

Using it forward lookup is for it go search in other DNS or Root hint.

Notes:

Don't replicated the record:

If want DNS not record the new ip had found.

- **S.O.A:**

1) Serial number:

It have the number of changes happens in DNS database and it appear more when have 2 A.D.I "sending incremental updates".

It sent updates only to the DNS and which control which has more mount of changes.

2) Primary server:

It have info about main DNS Server.

3) Responsible server:

It have info about DNS user.

4) Refresh interval:

Give specific time for check main DNS for updates.

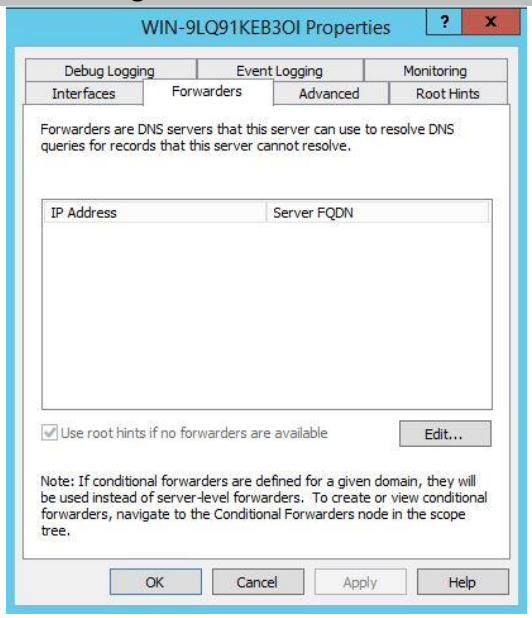
5) Retry interval:

Incase DNS didn't respond on it, it will continue work normally while keep checking by time had set before until 1 day pass on not responding it going to be expired .. And other DNS will stop work.

DNS

Forwarding

- **Forwarding**:



When want enter yahoo.com and it's not have it in DNS records and if not found it, it'll ask near DNS or Root hint.

Forward is give DNS 8.8.8.8 preferred DNS and 10.0.0.10 as alternate DNS so when going type for search something in internet it going to find it so fast as preferred DNS is 8.8.8.8.

But when want search in the local network it going to late a lot cause 8.8.8.8 going to search in the whole world until find inside your network.

So the best solution is forwarding options for avoid this issue.

Steps:

Server manager > DNS > name DNS > properties > forwards > add ip > edit for put time.

- **Conditional forwarding:**

Is when have other company with local domain, it going to use conditional forwarding by give it the DNS domain 20.0.0.10 and lab7.com the same steps but with 10.0.0.10.

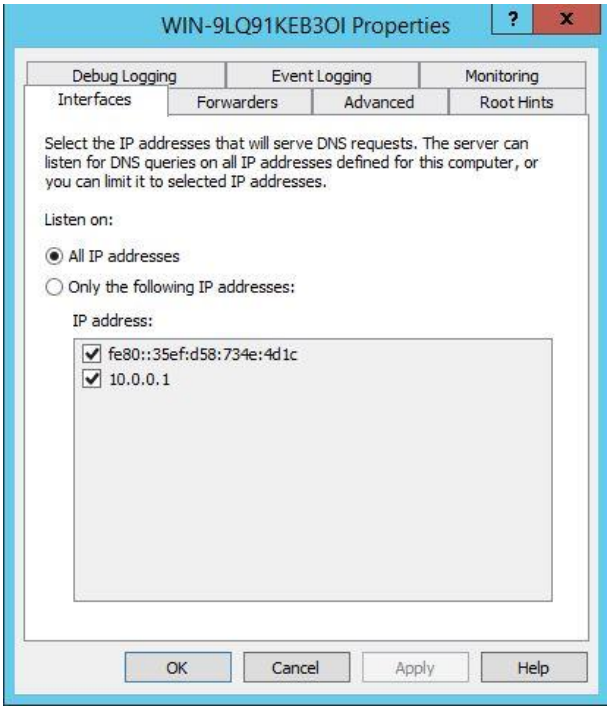
Steps:

Conditional forwarding > properties > new conditional forwarding.

DNS

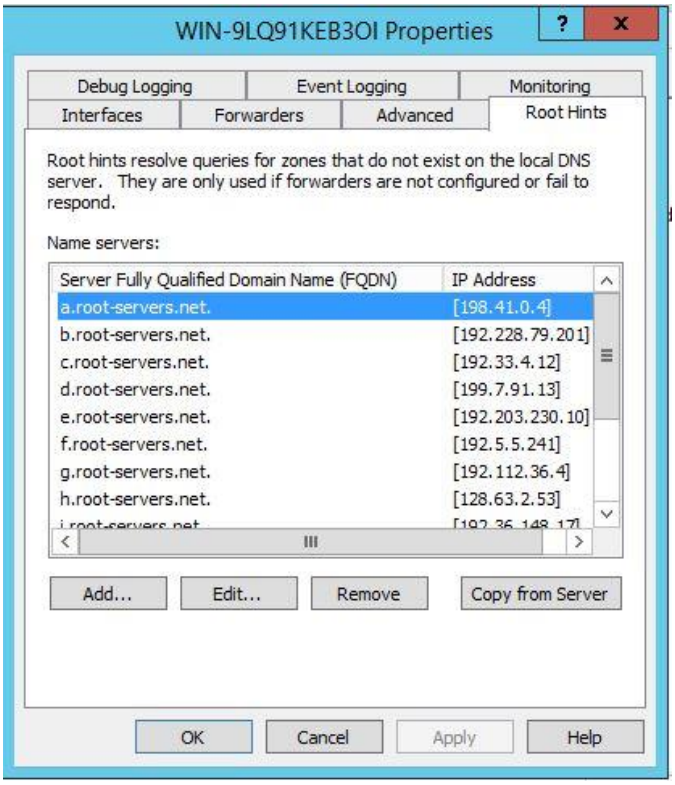
Server Properties

- **Interface**:



Is tab responsible for decide which ip listen to or ignore. Ip for all “and is listening and replaying to any DNS queries”. For specific ip’s “is for choose specific ip’s for listen to”.

- **Root hint:**

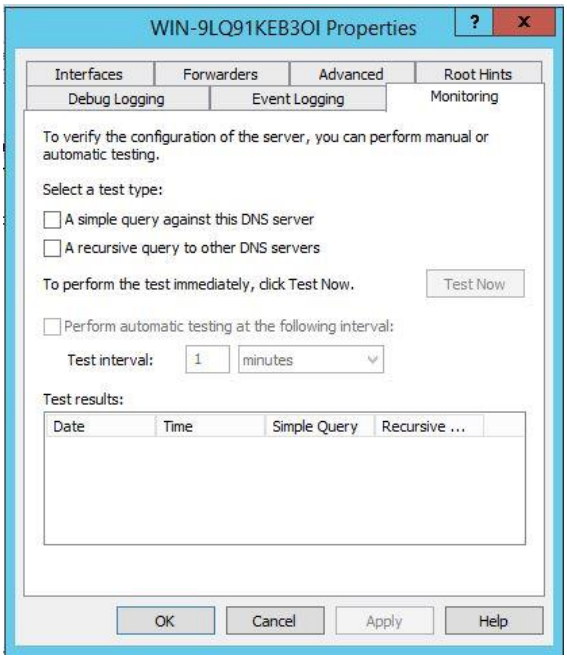


Is tab has the 13 servers which DNS go to, when it don't find in its record.

It be used when have private company or place and want to keep it secure and only listen and replay and don't receive queries from out the network.

So we create forward lookup zone "."(Root) and this going to disable the searching in root hints as it will be its own root hint.

- **Monitoring**:

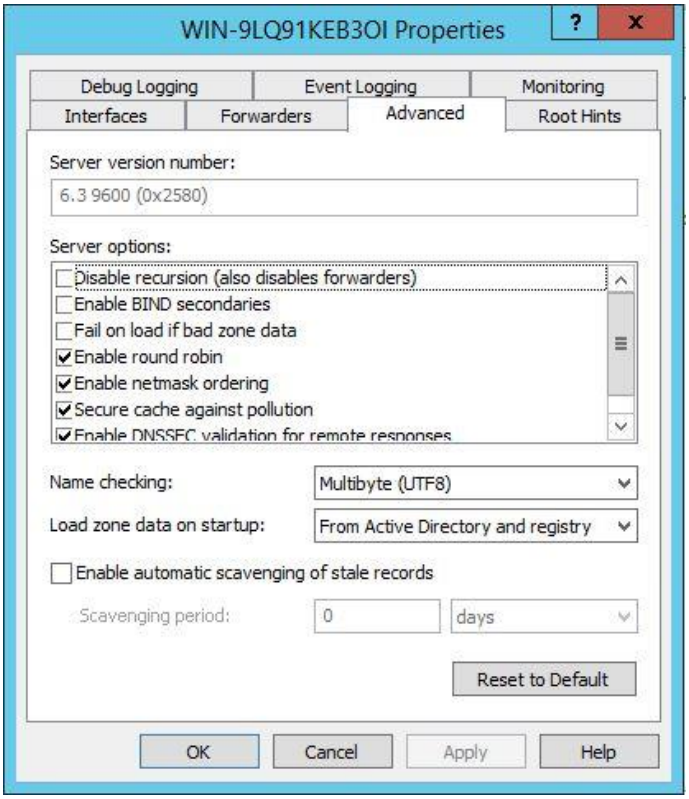


Is for test the DNS

Simple query: is for test the current DNS.

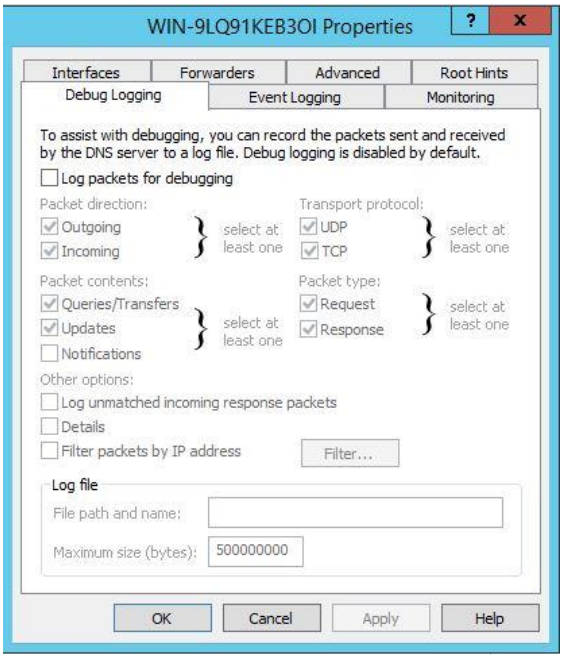
Executive query: is for test the forwarding DNS.

- **Advanced**:



- **Disable recursion "also forwarding** "Is for disable ask or receive forwarding p.s: before 2012 was able to choose 1 feature for disable it.
- **Enable BIND secondary's**: is for Linux o/s when secondary DNS be able for take records.
- **Fail on load if bad zone data**: if there bad records it will stop work.
- **Enable round robin:** is for rotate the ip's for not make traffic on record.
- **Enable net mask ordering**: is for make DNS check first before give the record for it be sure it work with the queries.
- **Secure cache against pollution**: is for keep cache always safe from bad records.
- **Enable DNSSE validation for remote responding**: is when have DNS in other site and is going to connect with our site this point for secure and make sure its safe.
- **Name checking**: it has the decoding type between DNS's.
- **Load zone data on startup**: is the distention of records if text has all records or create new or use it has public DNS.
- **Enable automatic scarving of state records**: when mark on it any expired DNS records will be deleted after 7 days.

- **Debug logging**:



Is tab work for monitor department and it's related with cisco with its packets direction and transport protocol, and what inside each packet and its types.

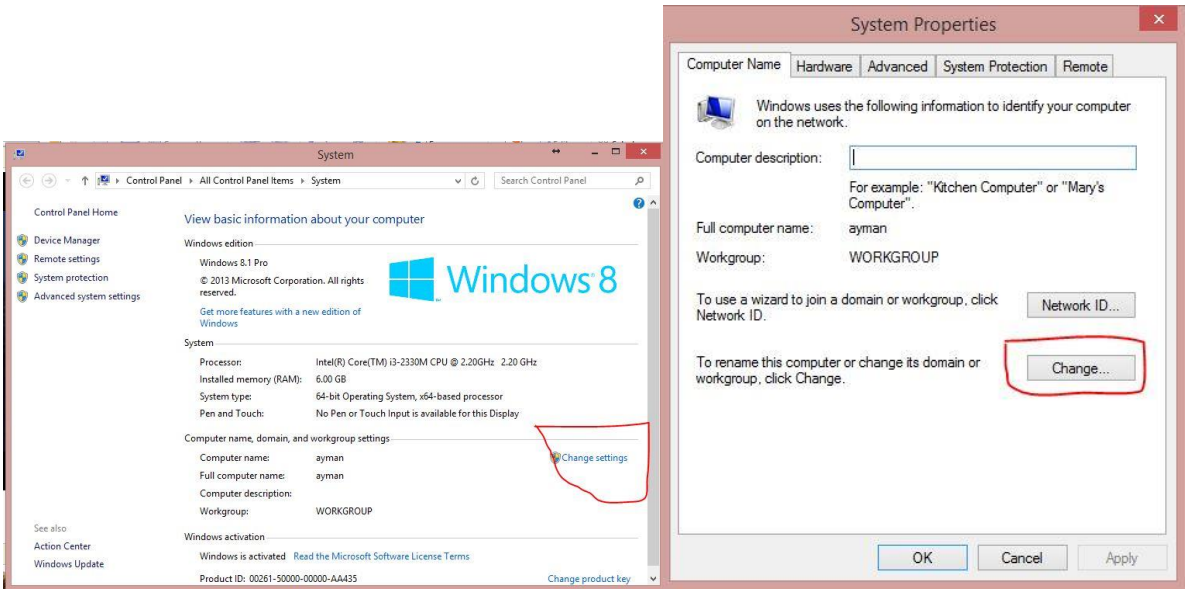
- **Suffix:**

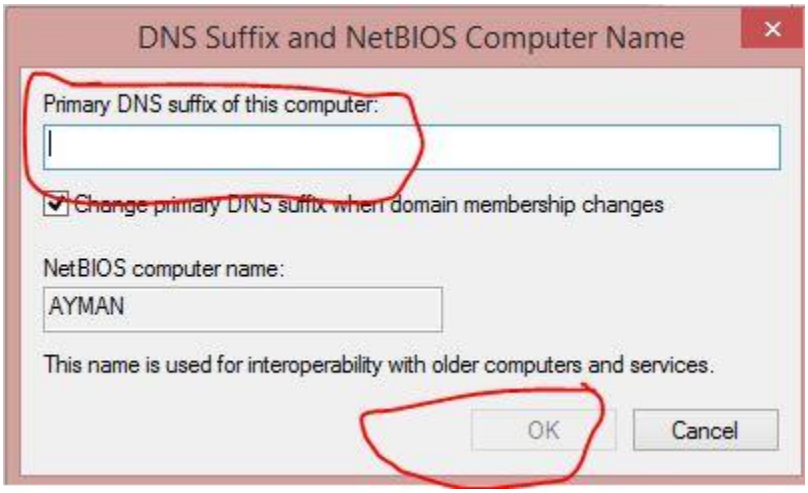
Is for make DNS device join domain even before it be exist, for make A.D when be configured it have the DNS primary work and replicate data with it.

Must be sure that DNS have the same name of domain which going to make it also the suffix name all must be match 100% or the whole process going to be failure.

Steps:

"My computer > right click > properties > change > more > type the suffix name > ok ".


System
Control Panel ▸ All Control Panel Items ▸ System
Search Control Panel
Control Panel Home
Device Manager
Remote settings
System protection
Advanced system settings
View basic information about your computer
Windows edition
Windows 8.1 Pro
© 2013 Microsoft Corporation. All rights reserved.
Get more features with a new edition of Windows
Windows 8
System
Processor: Intel(R) Core(TM) i3-2330M CPU @ 2.20GHz 2.20 GHz
Installed memory (RAM): 6.00 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display
Computer name, domain, and workgroup settings
Computer name: ayman
Full computer name: ayman
Computer description:
Workgroup: WORKGROUP
Change settings
See also
Action Center
Windows Update
Windows activation
Windows is activated Read the Microsoft Software License Terms
Product ID: 00261-50000-00000-AA435
Change product key
System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
Windows uses the following information to identify your computer on the network.
Computer description:
For example: "Kitchen Computer" or "Mary's Computer".
Full computer name: ayman
Workgroup: WORKGROUP
To use a wizard to join a domain or workgroup, click Network ID.
Network ID...
To rename this computer or change its domain or workgroup, click Change.
Change...
OK
Cancel
Apply


DNS Suffix and NetBIOS Computer Name
Primary DNS suffix of this computer:
Change primary DNS suffix when domain membership changes
NetBIOS computer name:
AYMAN
This name is used for interoperability with older computers and services.
OK
Cancel

DNS

Records

- **Host (A) record:**

Is for resolving name to ip.

- **Pointer (PTR) record:**

Is for resolving ip to name it work with reverse zone only.

- **Alias (Cname) record:**

Resolving name to name

Every website has two names (“host” newvision.microsoft.com), (“alias”www.microsoft.com) the same happen with FTP alias direct user to web server.

- **MX (Mail exchange):**

Is the same like Alias record just it have extra option is priority.

- **SRV(service) record:**

Resolving service to name and it work on D.C device.

- **Backup**:

Destination **C:// windows > system32> DNS**

- **Design planned:**

Is put perfect plan for make downtime 0 and never be in risk.

- **Stub zone:**

Is responsible for be center of S.O.A in the huge firm which has a lot of DNS and all DNS go and ask for the final update S.O.A has been updated.

DHCP

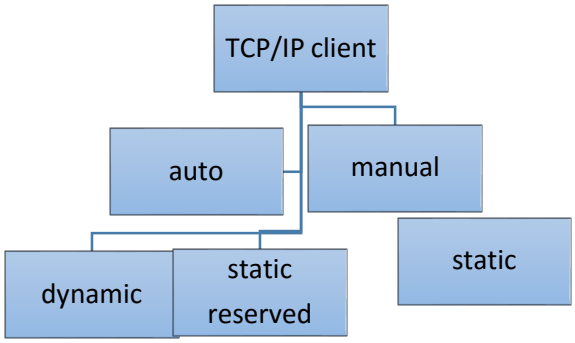
Dynamic Host Configuration protocol

- 1	- Definition	- 27	- Ipconfig /renew
- 2	- What does it used for	- 28	- Apipa
- 3	- DHCP clients	- 29	- Ipconfig /release
- 4	- How it works		
- 5	- Installing DHCP service “role”		
- 6	- Configuring DHCP		
- 7	- Creating scope		
- 8	- Exclusion		
- 9	- Lease duration		
- 10	- Scope options		
- 11	- Reservation		
- 12	- Authorization		
- 13	- Redmadanc		
- 14	- User class		
- 15	- Vendor class		
- 16	- Monitor		
- 17	- Backup		
- 18	- Server properties		
- 19	- Scope properties		
- 20	- Server option		
- 21	- Option 60 wds		
- 22	- Policy		
- 23	- Filter		
- 24	- Tcp/ip client		
- 25	- Boot p		
- 26	- DHCP relay agent		

- **DHCP definition:**

It assign the TCP/IP settings with Dynamic or Auto way.

- **TCP/IP client:**

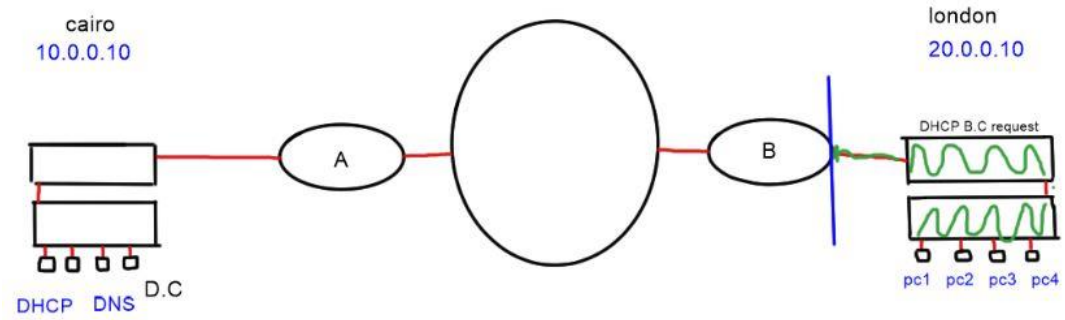


- **How it works:**

It work by give the DHCP the Ip Range and DNS and gateway, clients will send DHCP requests with B.C and then DHCP will replay on clients mac add with pole of Ip's Randomly.

- **Case1:**

2 branches and 1 has all servers "DHCP, DNS, D.C, etc" and other branch can't make DHCP request because router doesn't Support B.C.



Solution:

1st is Bootp is option in good manufacturing expensive routers which it able DHCP for receive B/C

But it won't work in that case because 2 branches not connected to same router directly.

2nd is DHCP relay agent it take clients requests from B router to DHCP server and back with the pole IP's.

- **Apipa**:

(Automatic Private **IP** Addressing) The Windows function that provides DHCP auto configuration addressing. **APIPA** assigns a class B **IP**address from 169.254.0.0 to 169.254.255.255 to the client when a DHCP server is either permanently or temporarily unavailable.

- **Ipconfig / release:**

For delete all ip's from device must use Command CMD "ipconfig /release".

- **Ipconfig /renew:**

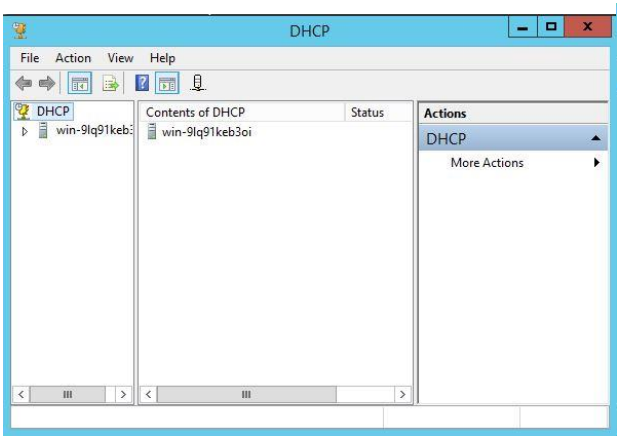
For make device take ip over again must use command CMD "ipconfig /renew".

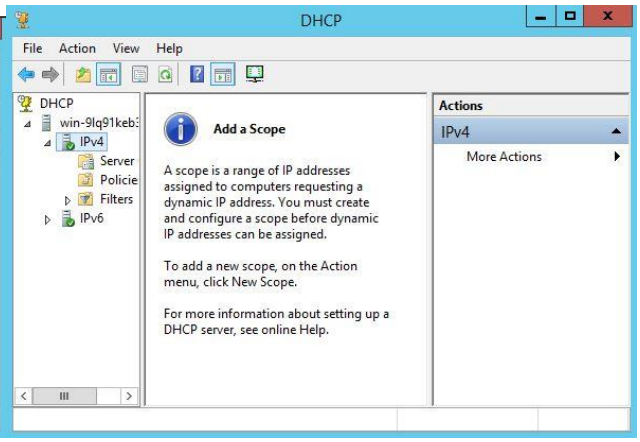
- **Installing DHCP:**

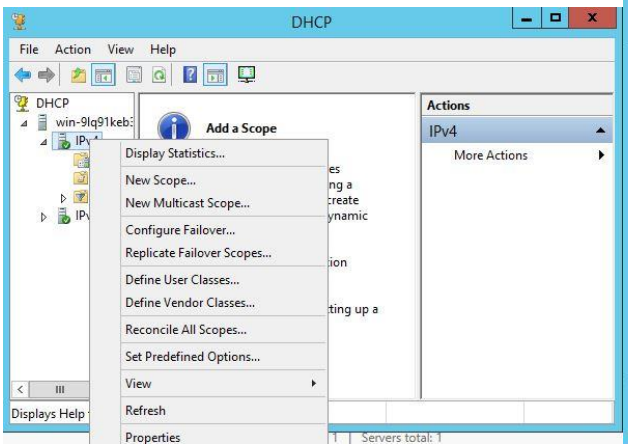
  Server manager > add role > DHCP > next > install
  The same like installing DNS

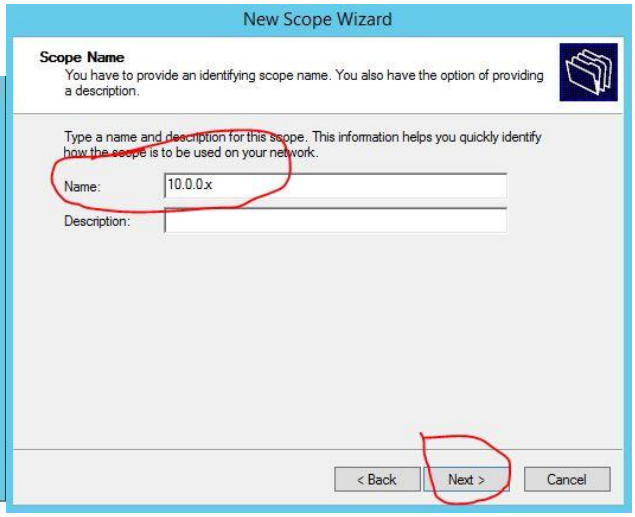
DHCP

Creating Scope



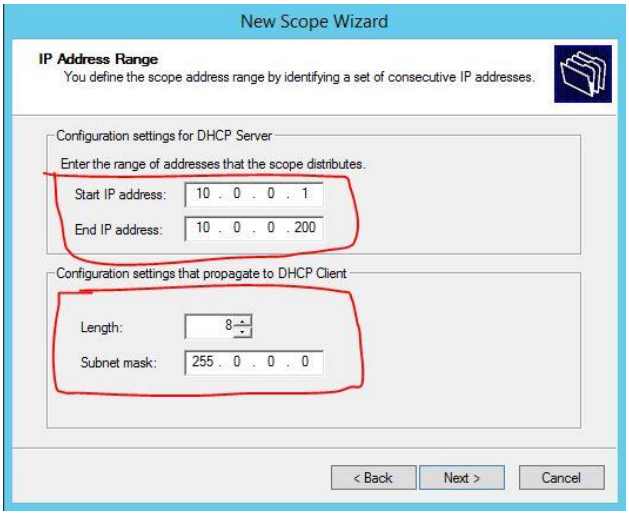






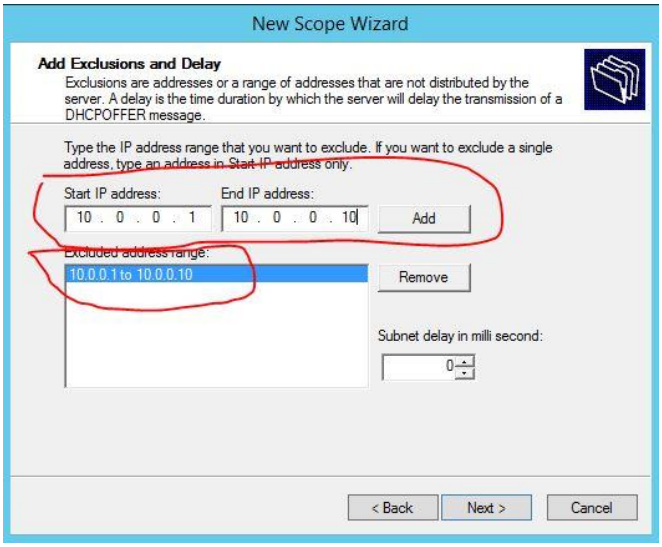
- **Ip address range:**

Is give ip address range for DHCP start make pole and share randomly with any client



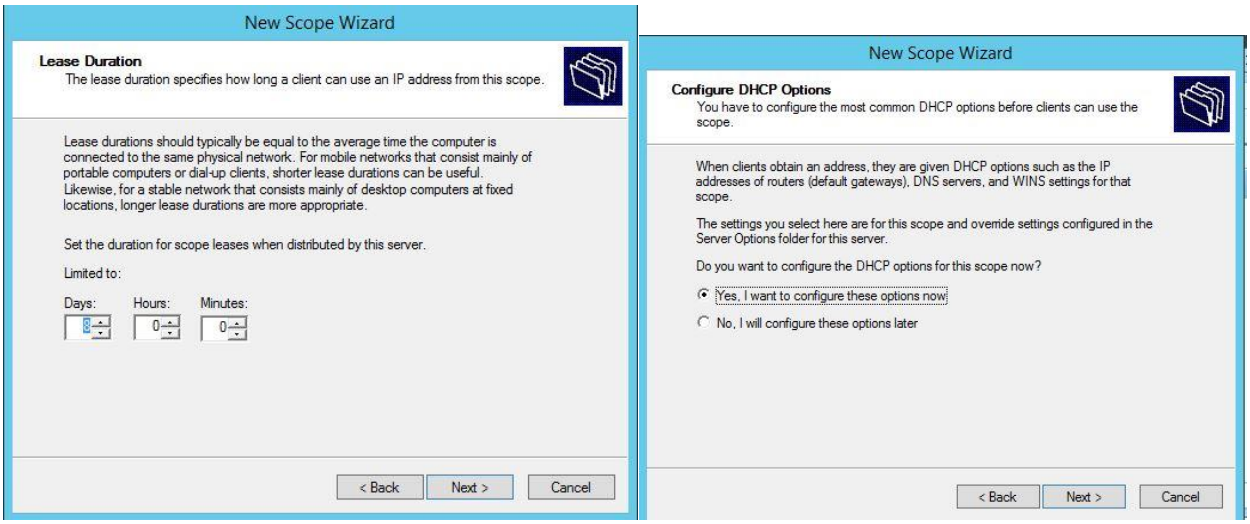
- **Add exclusions and delay:**

Is for avoid DHCP use the specific IP or range from use it in the DHCP pole for later can use these excluded IP's for main servers like DNS, D.C, etc.



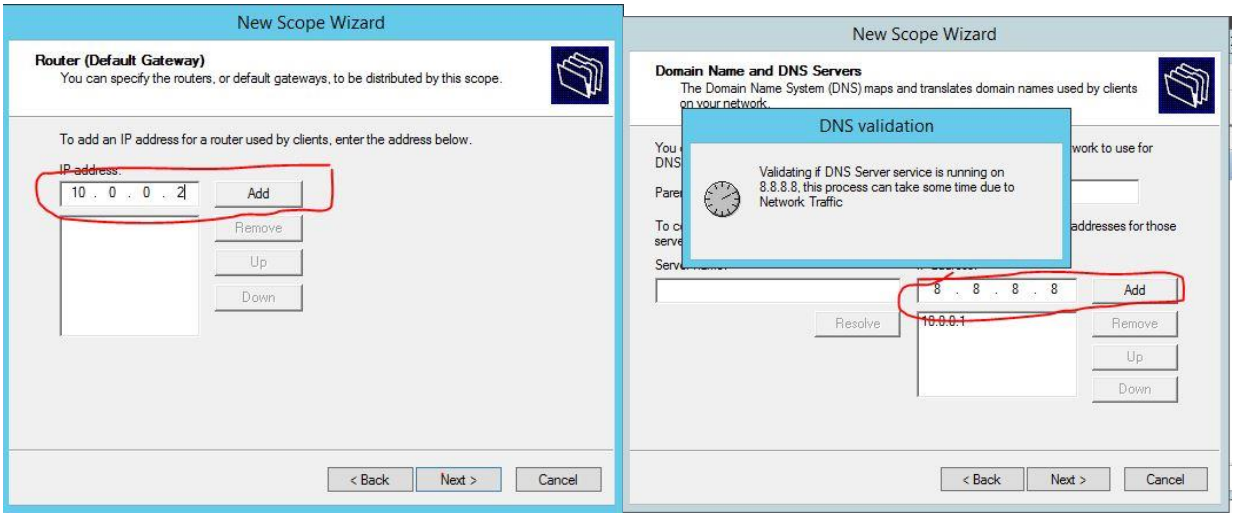
- **Lease duration:**

Is for make client when take ip DHCP reserve the ip for it don't be forever and be only for limited time because when have more clients than DHCP ip poles.



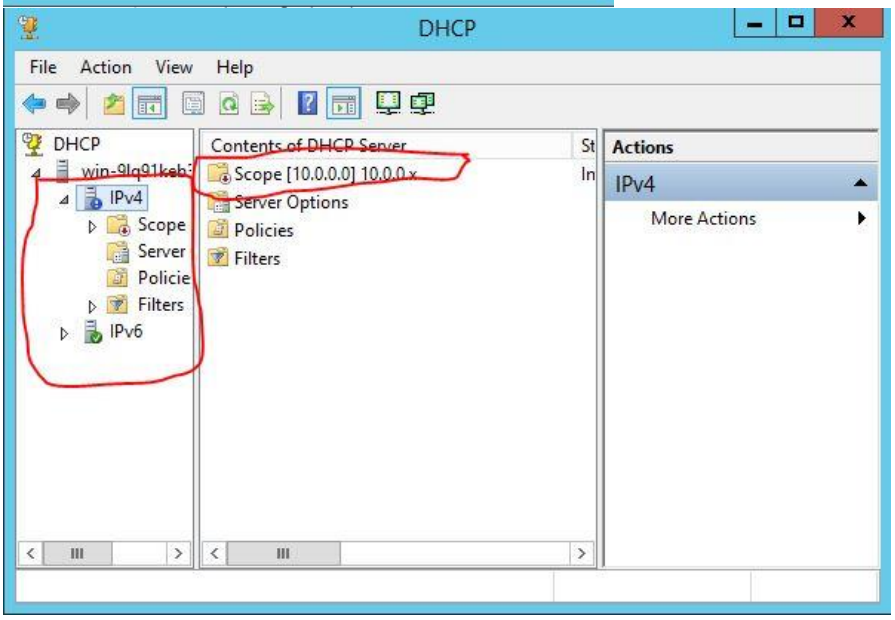
- **Domain name and DNS servers:**

Is add DNS ip's and must be aware with use primary ip or A.D.I in beginning then secondary ip and move up and down depending on priority.



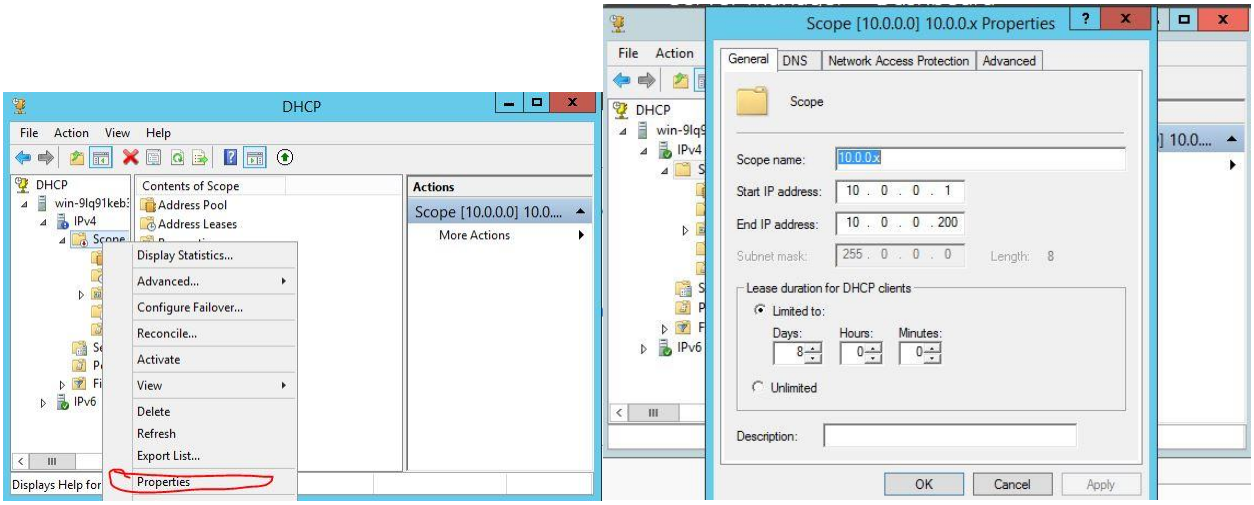
- **Activate scope:**

Is for activate scope later from scope options that because you maybe set the DHCP and will make it work later , so is not good make DHCP keep working and give ip's to useless clients and they use it for lease duration time.



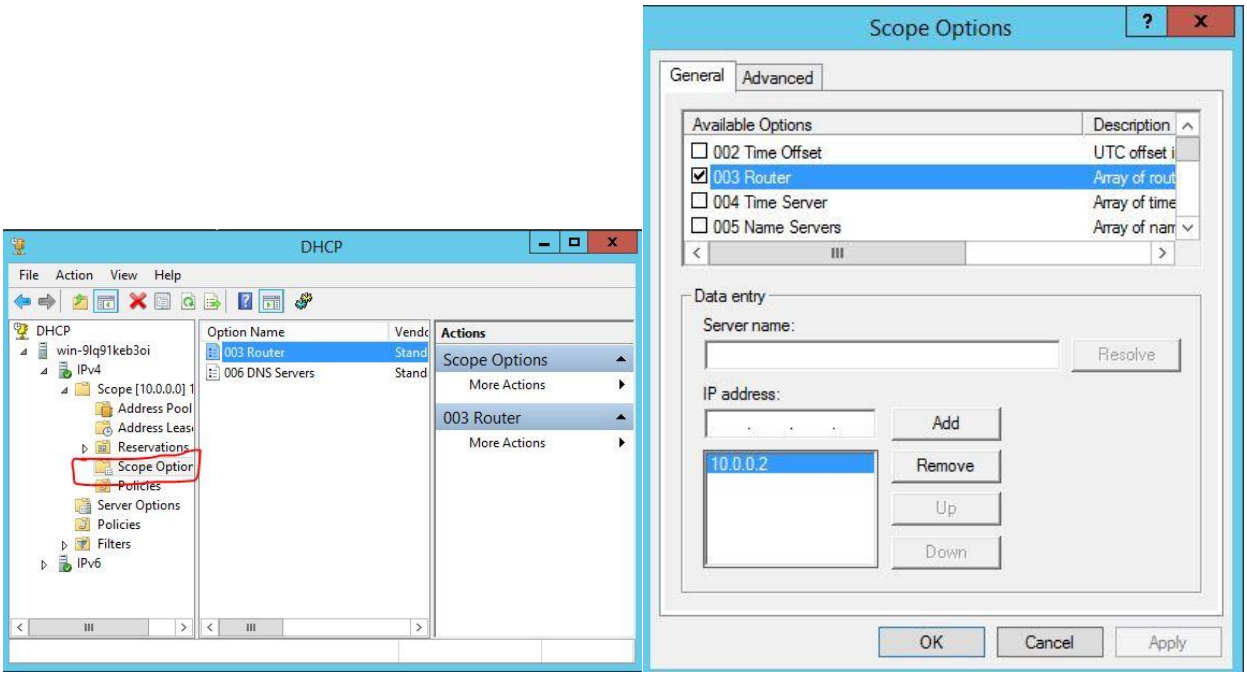
- **Scope properties:**

Can modify in IP range after creating it also in lease duration but cant in subnet, also it have extra option in lease duration it's unlimited.



- **Scope options:**

It have router and DNS servers.



- **Reservation:**

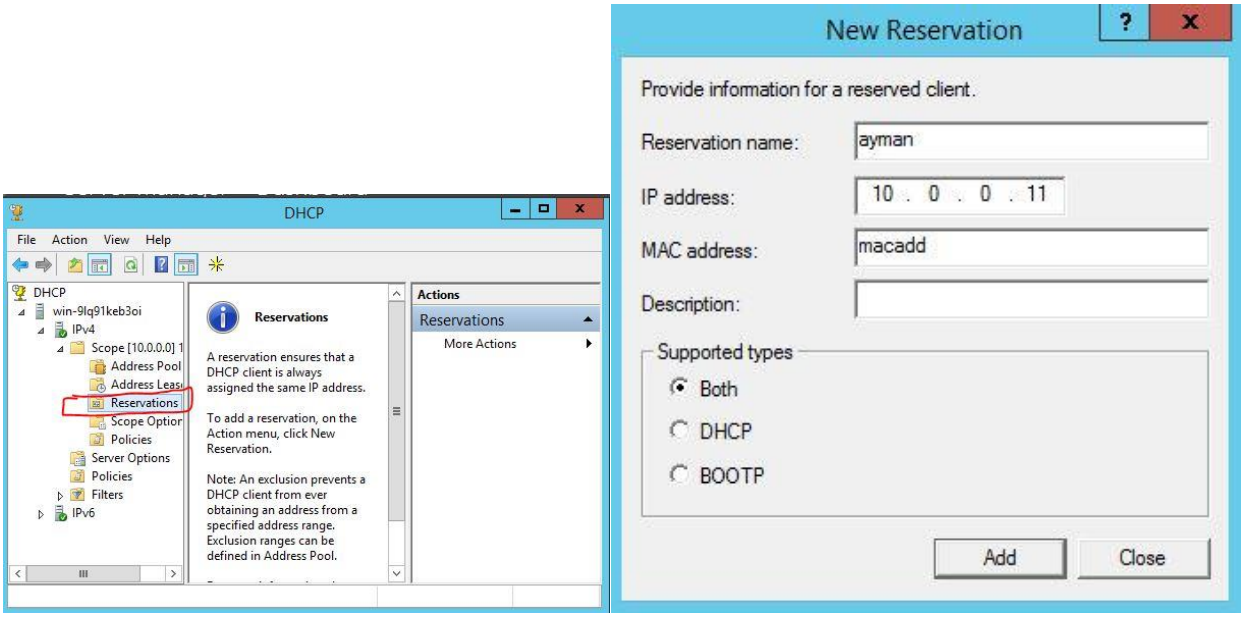
Steps: enter inside scope > reservation > right click > new reservation.

Add name and ip add mac address (without use Dash "-").

Reservation is for reserve ip and avoid DHCP for use it to random clients.

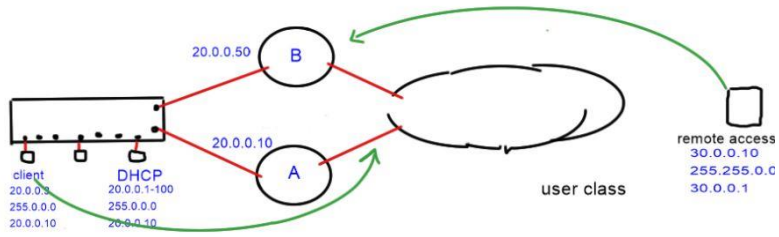
- **Supported types:**

- Both: its mix of DHCP and BOOTP and is the best option.
- DHCP: is when client in the same switch it can ask DHCP for IP.
- BOOTP: is for clients which re in other Switch for it use DHCP relay agent it calls BOOTP.



- **User class:**

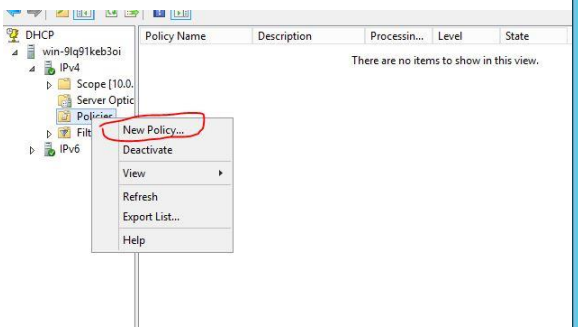
Is for when want scope option have extra option for specific user.

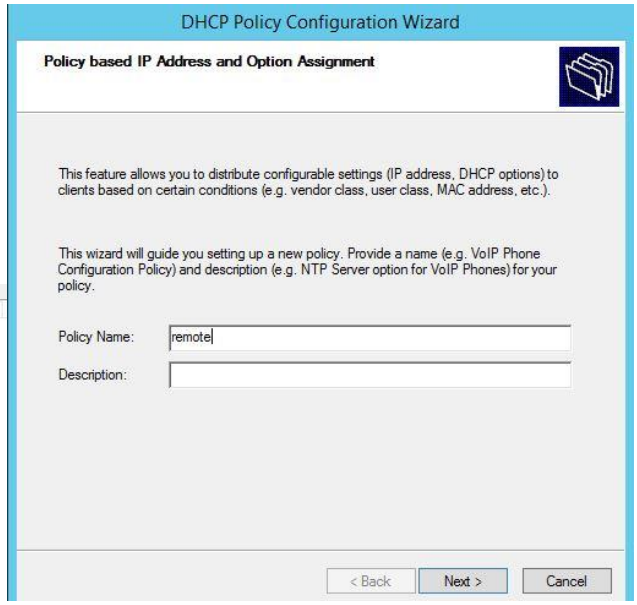


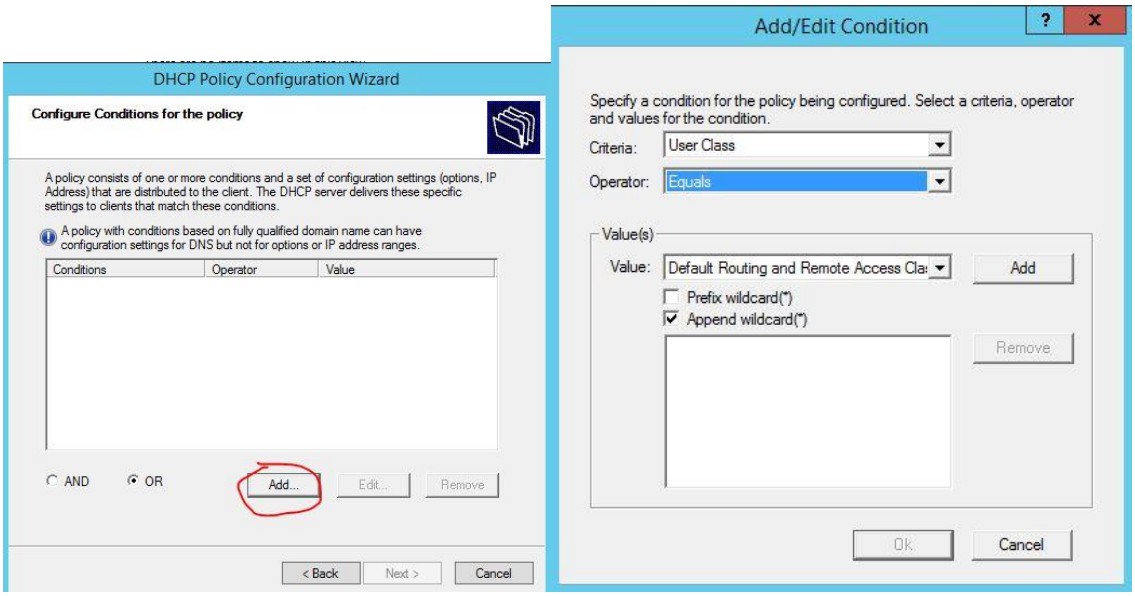
For example in the figure all clients inside range 20.0.0.x will have TCP/IP from DHCP to use 20.0.0.10 "Router A", but remote access users will use 20.0.0.50 "Router B"

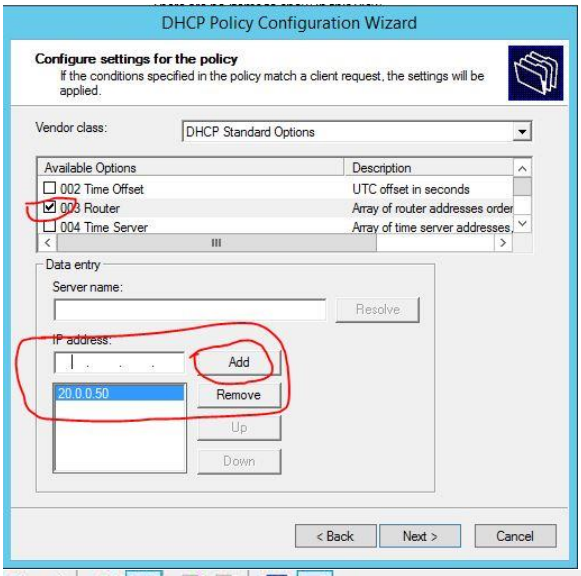
That can be done by user class in policies option.

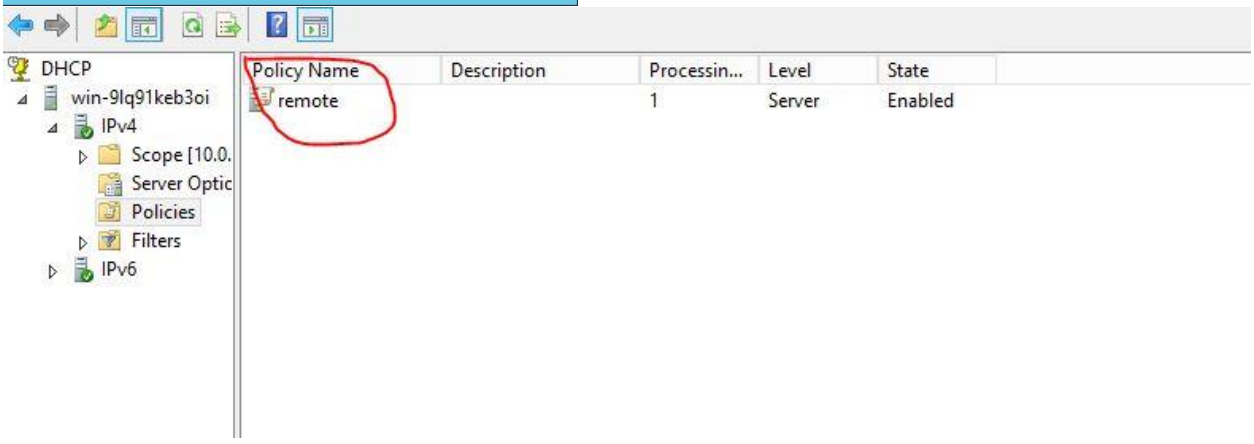
- **Step**: " policies> right click > new policy >type name > user class > choose (Default routing and remote access)> mark on append wild card






DHCP Policy Configuration Wizard
Configure Conditions for the policy
A policy consists of one or more conditions and a set of configuration settings (options, IP Address) that are distributed to the client. The DHCP server delivers these specific settings to clients that match these conditions.
A policy with conditions based on fully qualified domain name can have configuration settings for DNS but not for options or IP address ranges.
Conditions
Operator
Value
AND
OR
Add...
Edit...
Remove
< Back
Next >
Cancel
Add/Edit Condition
Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.
Criteria:
User Class
Operator:
Equals
Value(s)
Value:
Default Routing and Remote Access Cla
Add
Prefix wildcard(*)
Append wildcard(*)
Remove
Ok
Cancel

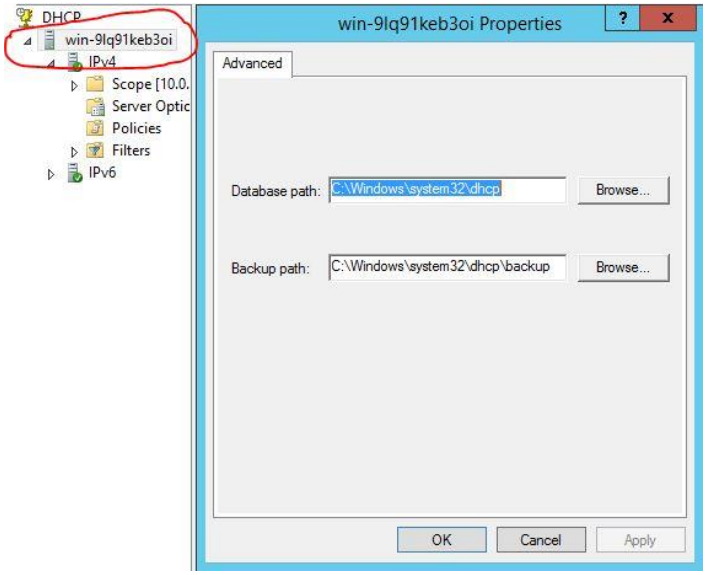

DHCP Policy Configuration Wizard
Configure settings for the policy
If the conditions specified in the policy match a client request, the settings will be applied.
Vendor class:
DHCP Standard Options
Available Options
Description
002 Time Offset
UTC offset in seconds
003 Router
Array of router addresses order
004 Time Server
Array of time server addresses
Data entry
Server name:
Resolve
IP address:
Add
20.0.0.50
Remove
Up
Down
< Back
Next >
Cancel


DHCP
win-9lq91keb3oi
IPv4
Scope [10.0.
Server Optic
Policies
Filters
IPv6
Policy Name
Description
Processin...
Level
State
remote
1
Server
Enabled

- **Vendor Class:**

Is give extra option by depending on the user operating system buuut is much better use user class instead of it cause not all operating system support this service

- **Server properties:**



- **Database path**: is the path of DHCP folder in device.
- **Backup path:** is the path of DHCP backup in device.

- **Advanced:**

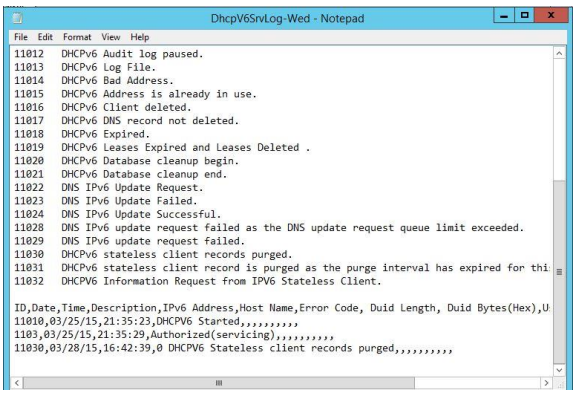
It assign IP for users out of range which using “BOOTP, DHCP or both”

Steps: scope>right click > properties > advanced tab

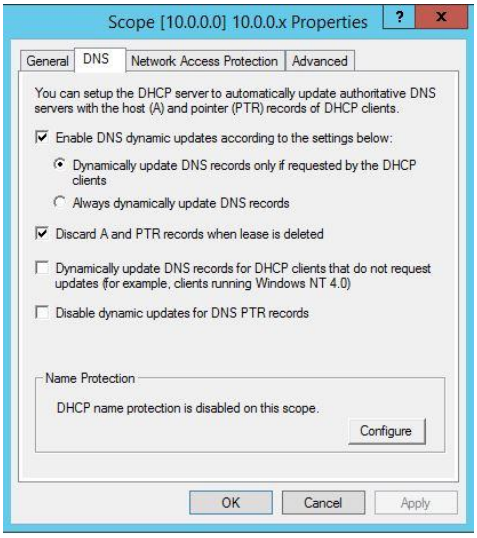
- **Monitor**:

Is folder has the files log of week with its all activity and its updating weekly

Path: C://>windows>system32>dhcp



- **Scope option "DNS Tab":**



As it's enabled it will keep always updated with clients with its last changes.

We disable it for publish a public DNS for secure it.

- **Dynamically update DNS records only if requested by the DHCP:**

Is make update only when clients request for the action.

- **Always dynamically update DNS records:**

Is for update always without depending on client request.

- **Discard A and PTR records when lease is deleted:**

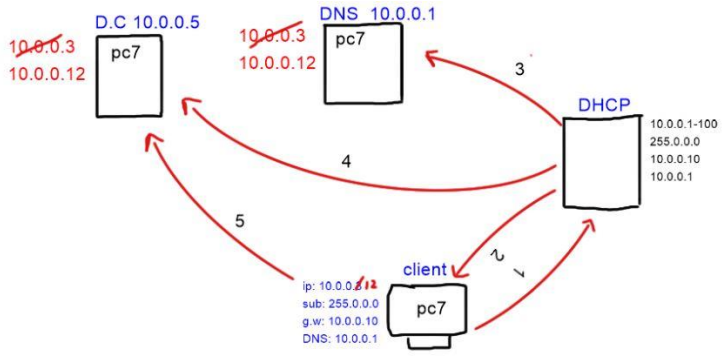
Is DHCP make DNS delete the expired leased records of Host A and PTR.

- **Dynamically update DNS records for DHCP clients that not request:**

Is for make updates for client which them O/S don't support request action.

- **Disable dynamic update for DNS PTR records:**

Is for disable the update option for only PTR records which resolving from reverse zone,



- **Backup:**

Is in the same folder of monitor we copy it for make backup.

- Path: C://>windows > system32 > dhcp > backup.

- **Server options:**

Is the same of scope options but for all scopes.

Incase these scope has different specific properties it will have priority before server option properties

- **Radiance:**

It make other DHCP for be backup increase the main DHCP server down.

So we 'll create other DHCP server and make the first main DHCP range " 1-~100" and the backup have range "101~200" for avoid conflicts and keep range covered.

For make DHCP respond on requests first must increase the delay.

- **Filter:**

Is option has allow or deny for client with mac address and make don't require nothing from DHCP server.

- **Authorized**:

Is for make DHCP authorized for no one can make fake DHCP and give Fake ip's and down the main DHCP.

It work only in domain or D.C, can't work while stand alone.

Must login as enterprise admin for can use it.

- **Multicast Scope**:

Is for use multicast with specific clients per them requests and it work with multimedia,

Is for not broadcasting the media with all clients because sure there clients not need that, also can't use unicast because it will take a lot of time to replay on each request in replay in share session.

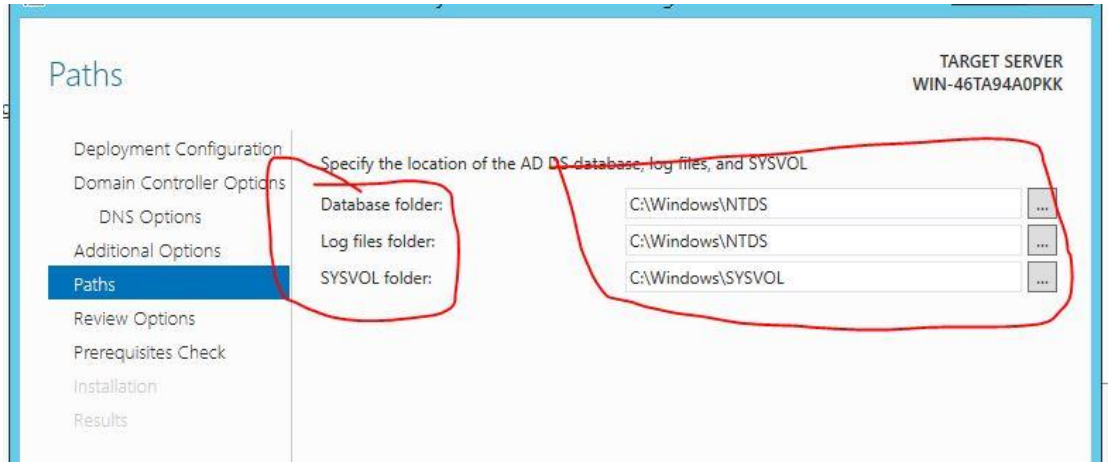
Notes and troubleshooting for A.D

- While installing A.D service will appear “Net Bios Name” sometimes normal or have “0” beside the name
  EX: lab3.com, lab3.com0
  Because NetBIOS name check the network if it have already the name exist if it found it already will add 0 if not it will not add nothing.

- **Data base:**

NTDS: it has the schema table, link table, data table in Active directory.

Sysvol: is responsible for save replicated data while it transferring from D.C to other in windows. And it need NTFS hard drive.



- **LADP**:

is protocol which take the query and move it and back with answer inside Domain .

- **Korbous** :

Is protocol responsible for secure any traffic happened inside the domain.

Notes:

As you see message **“ Domain controller an active directory could not contacted “** be sure is problem of DNS, also check the firewall sometimes it blocking it.

Windows deployment server

WDS

Is for deploy the windows O/S by the network card.

Server side	Client side
• WDS option 60 • A.D • DNS • DHCP	• Boot NIC • NIC supporting " PXE"

- **How it work :**

1st install the 4 roles WDS, AD, DNS, DHCP in the server side.

2nd configuring the 4 roles and insert windows CD/DVD for configuring WDS.

Steps:

"Server manager > WDS> install image > add install image > location "Browse" > sources > install. Win".

"Server manager > WDS> install image > add install image > location "Browse" > sources> boot. Win".

3rd make the target device boot from network boot for bios work on DHCP for obtain ip .

4th ask DNS for WDS IP.

5th network card start use image from server side.

Notes:

If there any problem or mistake in any role of server side the whole process going to failure totally.

PXE: is option able the network card obtaining and booting from bios and almost network cards have it.

Read only domain controller

RODC

Its option can be used in D.C for make it read only.

- It start with NT4 O/S then 2000 with Microsoft until now days, in NT4 it was have PDC"primary domain controller" and its R/W, also have the additional be BDC" backup domain controller" and its R only.
- But after 2003 it start be D.C "domain controller" and Add D.C "additional domain controller" both R/W

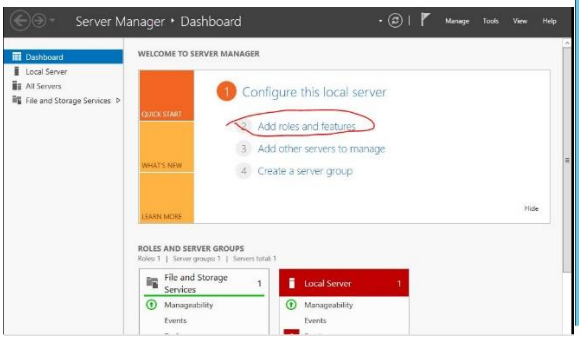
- Simply when have environment without security and away from IT head quarter control and must use additional D.C for deploy policies on users there but in the same time afraid from virus or get hacked and been infected in the database of D.C .

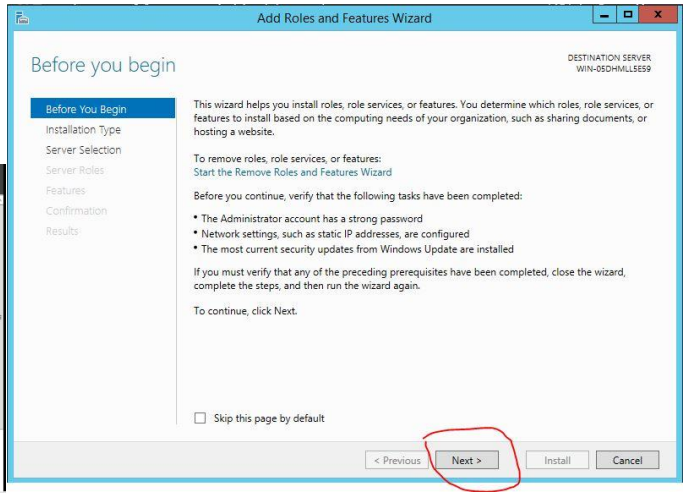
In that case the NT4 will be good because the additional be just back up read only so nothing can effect on the main database on the D.C.

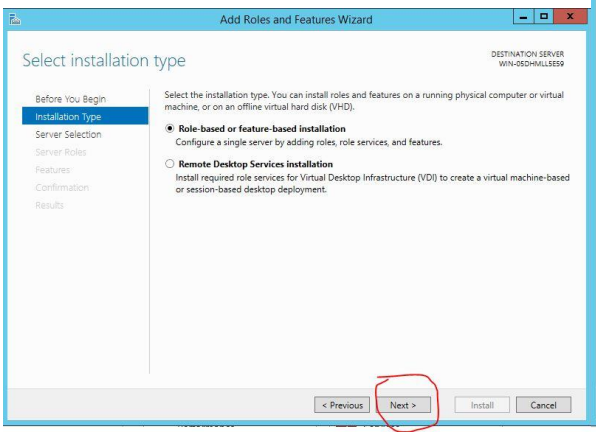
- But can use "RODC" option for make an additional domain controller have only read and not write so it will be more secure more controlled by D.C.

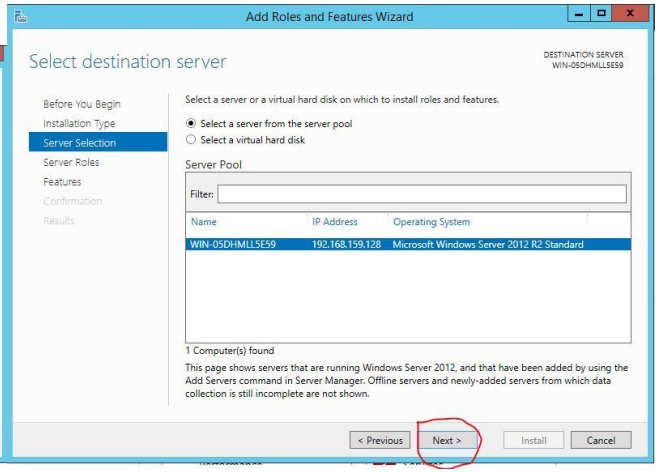
Steps:

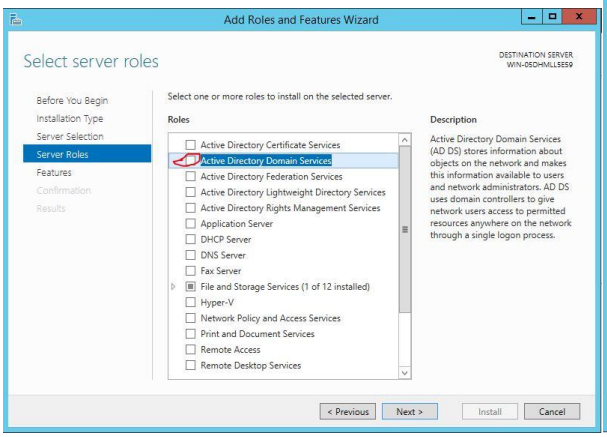
"Sever manager > add role> active directory > promote > make it to existing D.C > connect it to domain > check mark on "RODC" > install".

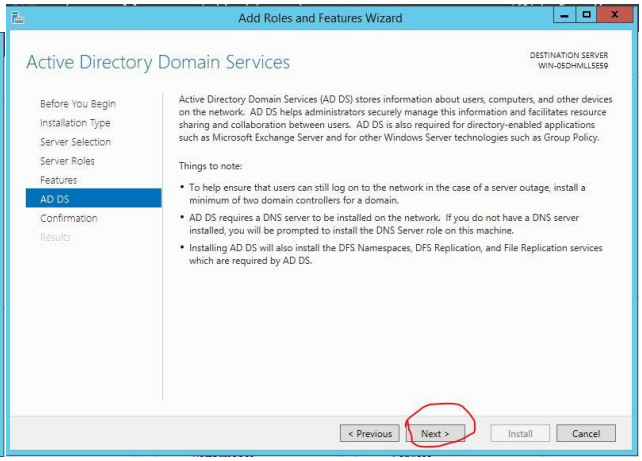


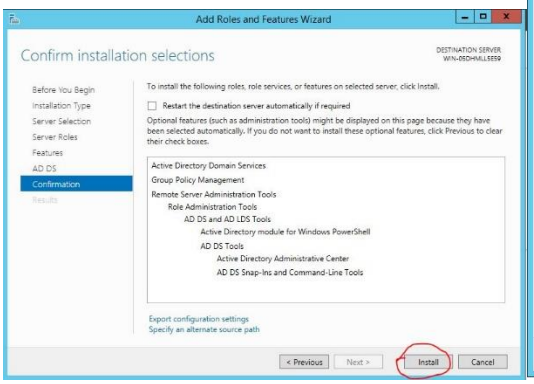


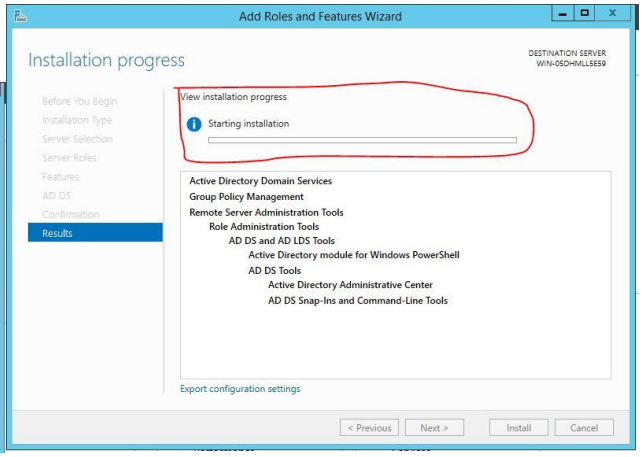

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
WIN-05DHMLL5E59
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, 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

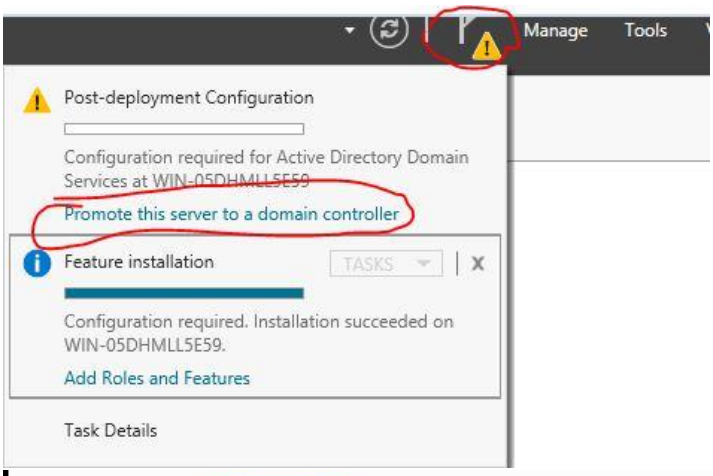

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
WIN-05DHMLL5E59
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
WIN-05DHMLL5E59
192.168.159.128
Microsoft Windows Server 2012 R2 Standard
1 Computer(s) found
This page shows servers that are running Windows Server 2012, 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

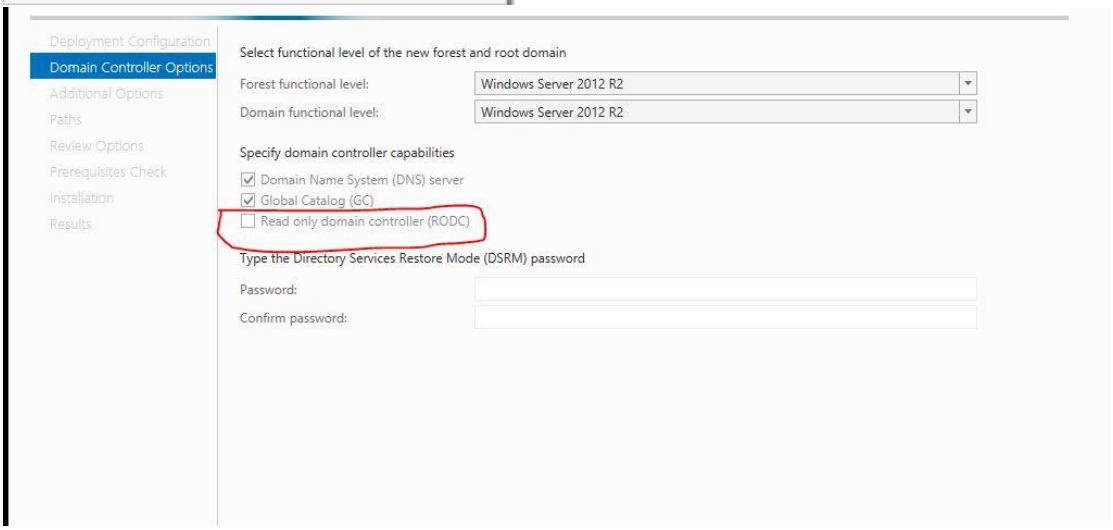

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-05DHMLL5E59
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
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


Add Roles and Features Wizard
Active Directory Domain Services
DESTINATION SERVER
WIN-05DHMLL5E59
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. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy.
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.
Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by AD DS.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
WIN-05DHMLL5E59
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
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
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN-05DHMLL5E59
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
View installation progress
Starting installation
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
Export configuration settings
< Previous
Next >
Install
Cancel





Notes:

In NT4 O/S when PDC be down the users going to be able work with the current BDC have already but not able for create or modify anything until make other PDC and give it the control.

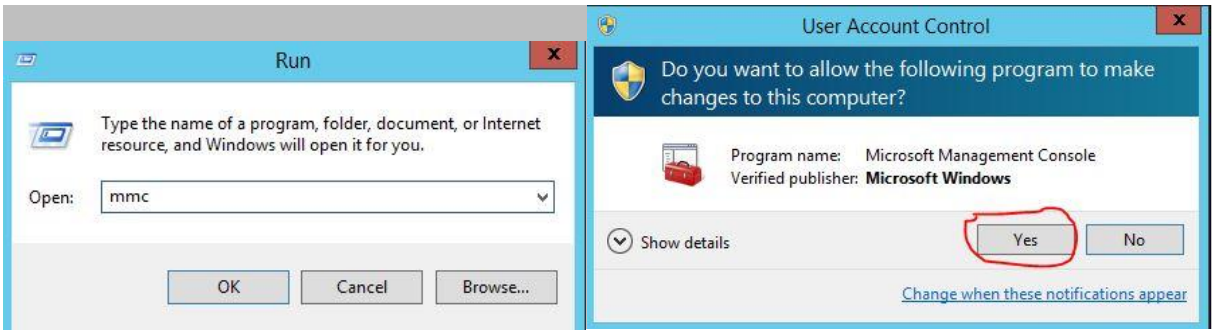
Delegation

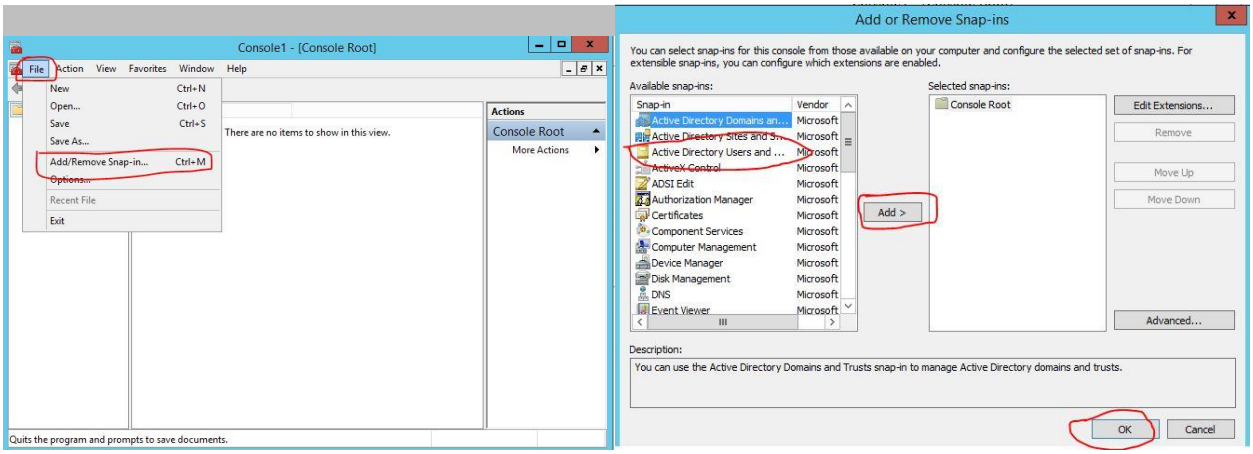
- Is give normal user some specific options for make specific tasks in active directory and reduce the pressure on the IT team and not waste them time in simple tasks like add or remove user or enable or disable.
- In the same time can't give the user full control access in the active directory, so we use for them taskpad view for make them control only the specific tasks they need.

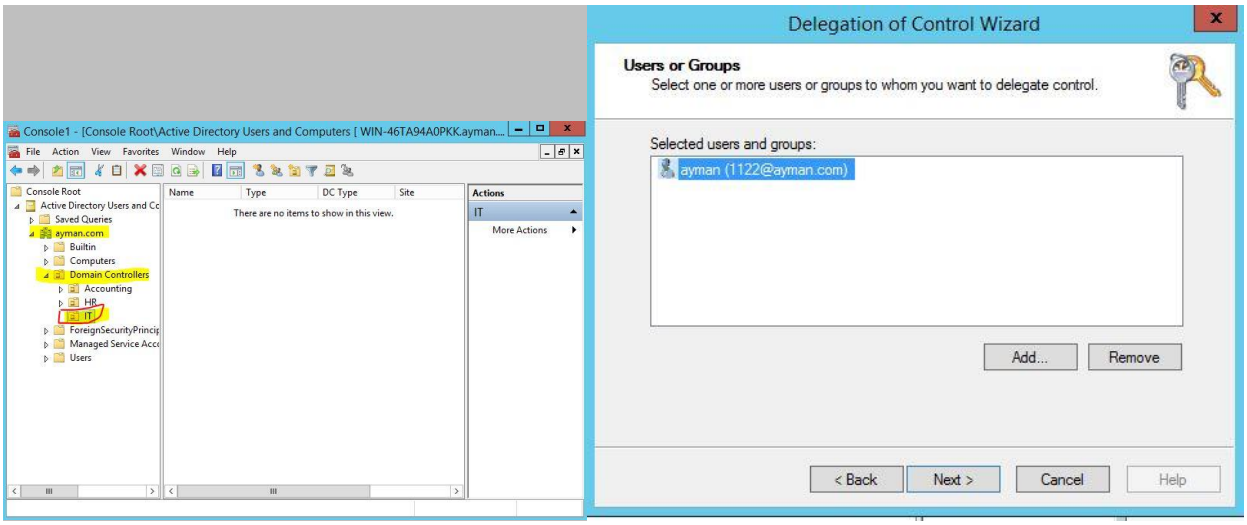
Steps:

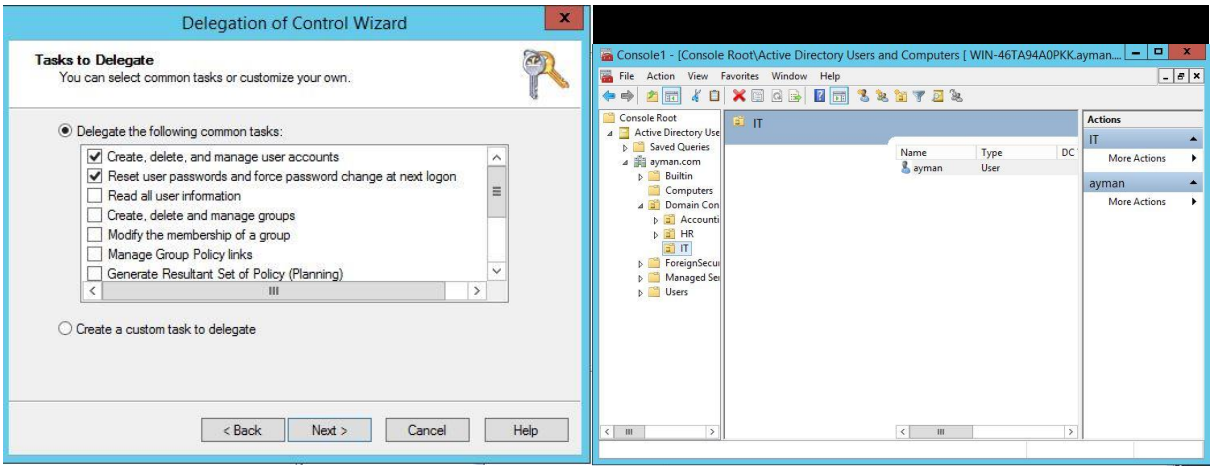
- **delegation**

"Run > type "mmc" > file > add / remove snap in > active directory and users > open > click n ou > right click > delegation > choose user > choose task > next > choose task ".





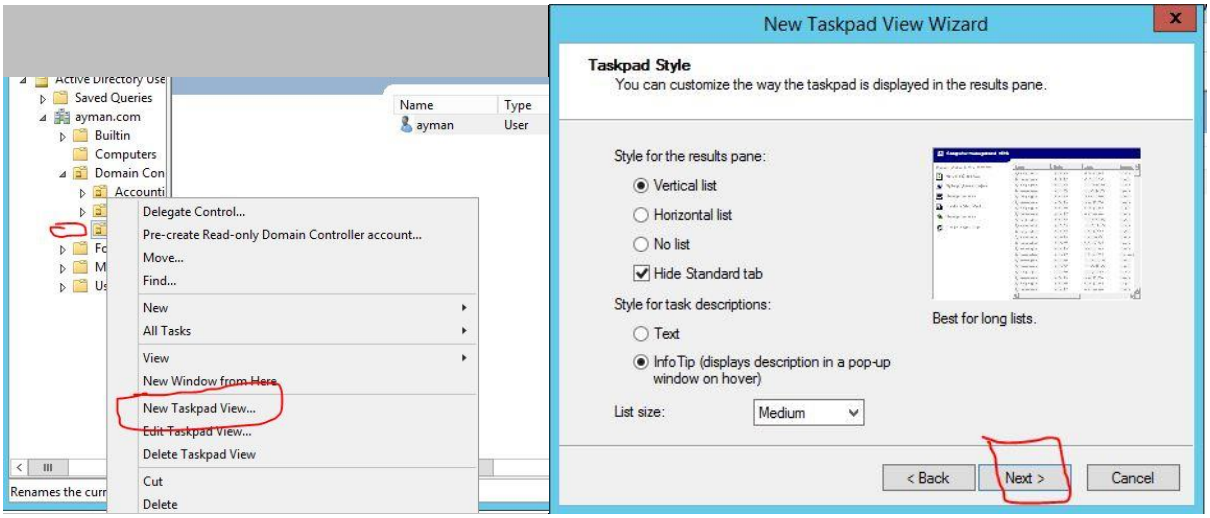

Console1 - [Console Root\Active Directory Users and Computers [WIN-46TA94A0PKK.ayman...
File Action View Favorites Window Help
Console Root
Active Directory Users and Co
Saved Queries
ayman.com
Builtin
Computers
Domain Controllers
Accounting
HR
IT
ForeignSecurityPrincip
Managed Service Acco
Users
Name Type DC Type Site
There are no items to show in this view.
Actions
IT
More Actions
Delegation of Control Wizard
Users or Groups
Select one or more users or groups to whom you want to delegate control.
Selected users and groups:
ayman (1122@ayman.com)
Add...
Remove
< Back
Next >
Cancel
Help

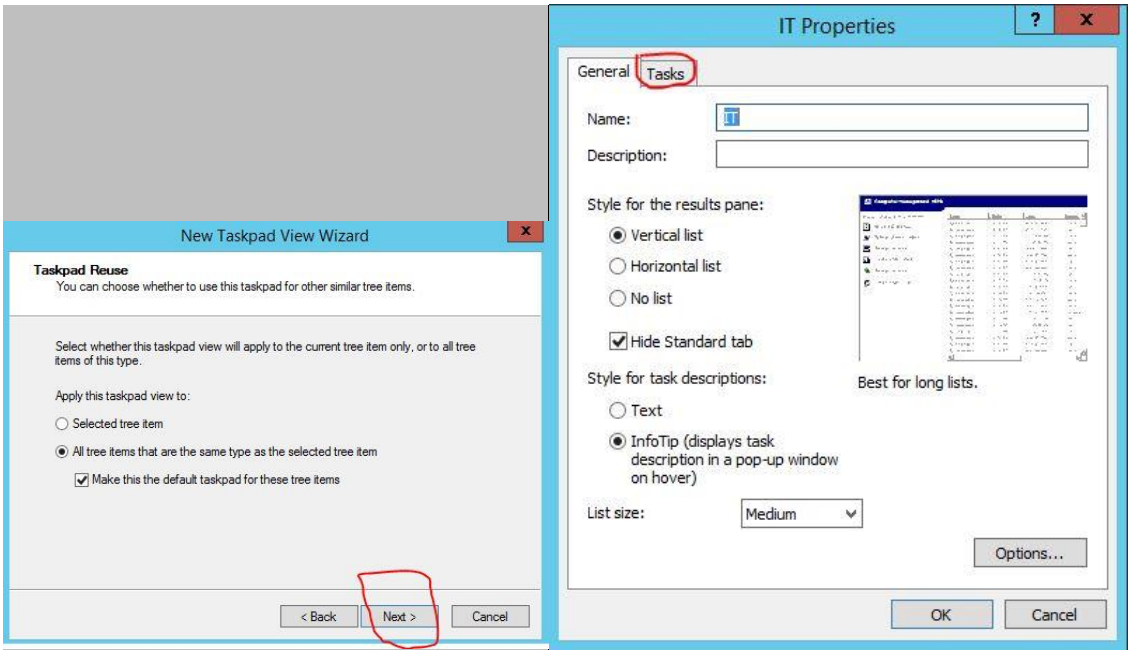

Delegation of Control Wizard
Tasks to Delegate
You can select common tasks or customize your own.
Delegate the following common tasks:
Create, delete, and manage user accounts
Reset user passwords and force password change at next logon
Read all user information
Create, delete and manage groups
Modify the membership of a group
Manage Group Policy links
Generate Resultant Set of Policy (Planning)
Create a custom task to delegate
< Back
Next >
Cancel
Help
Console1 - [Console Root\Active Directory Users and Computers [WIN-46TA94A0PKK.ayman...
File Action View Favorites Window Help
Console Root
Active Directory Use
Saved Queries
ayman.com
Builtin
Computers
Domain Con
Accounti
HR
IT
ForeignSecu
Managed Se
Users
IT
Name Type DC
ayman User
Actions
IT
More Actions
ayman
More Actions

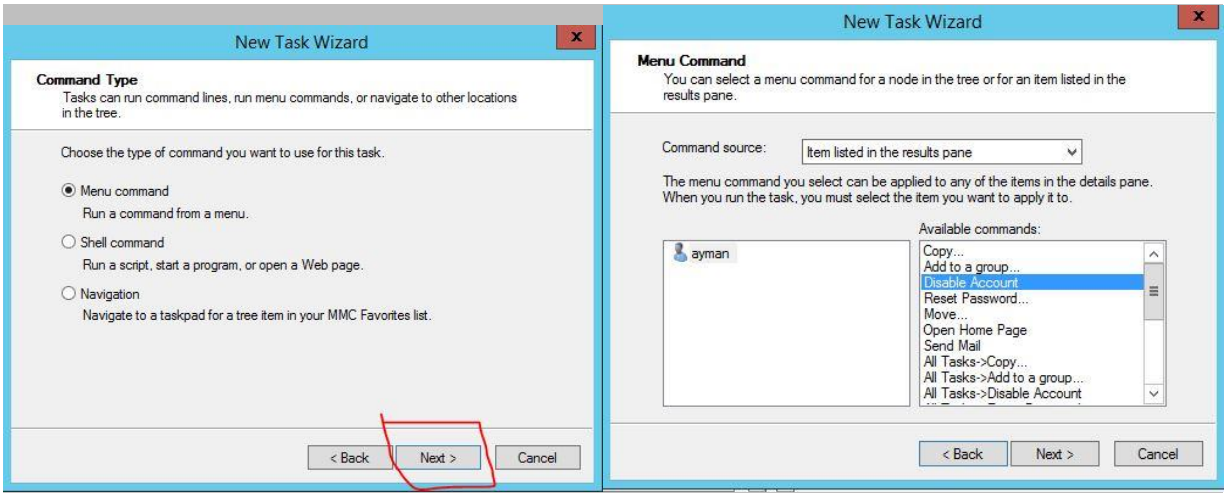
- **Taskpad view**

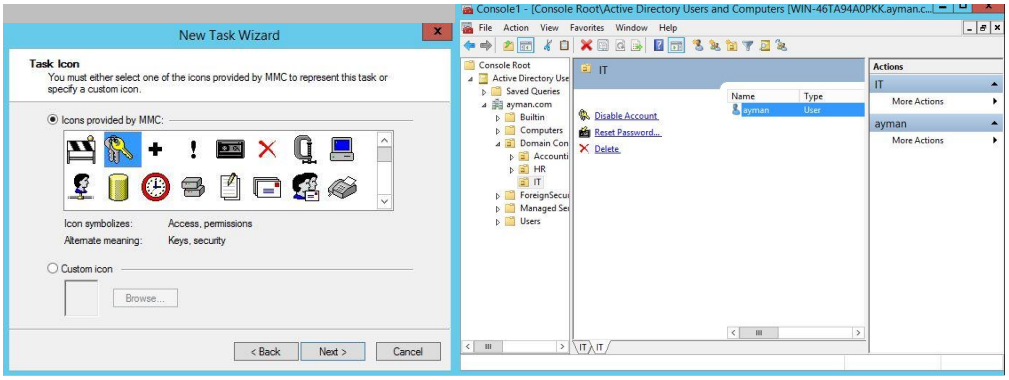
"right click on OU > new taskpad view > next > then right click on OU > edit taskpad> choose "task">

New > next > menu command >next > "choose command "> next choose icon > (check mark on when I finish run this wizard again)> finish."



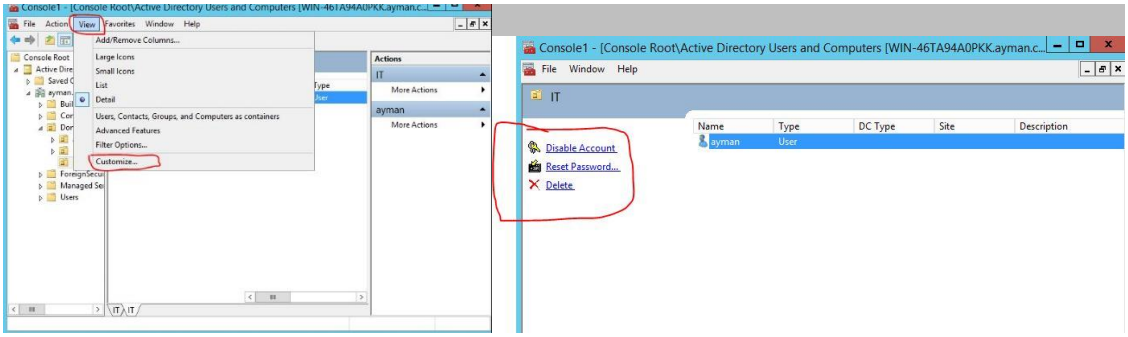






- **For users view only them specific tasks:-**

"Press on (View) > customize > un check mark on all options > ok > file > options > in console mode (choose user mode limited access single window) > ok > file > save (choose location) > send the console file by mail to users ".



Notes:

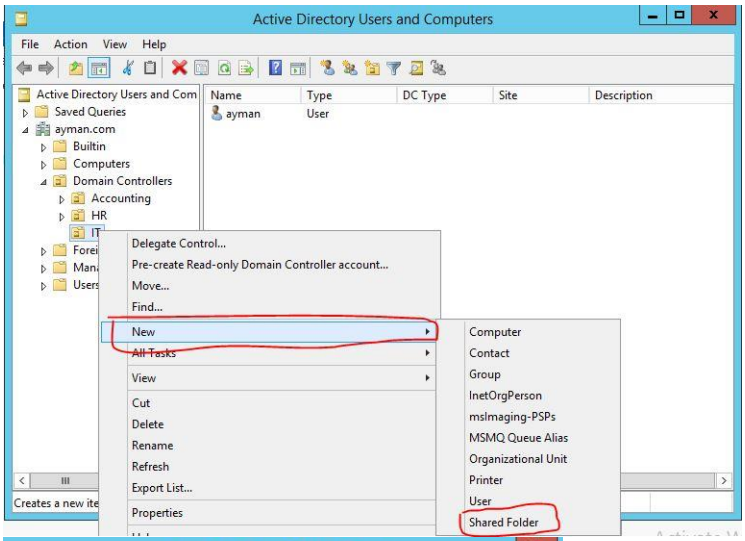
- Users which have delegations options will be the only users which can use the tasks options … normal users will can't open the hyperlinks.

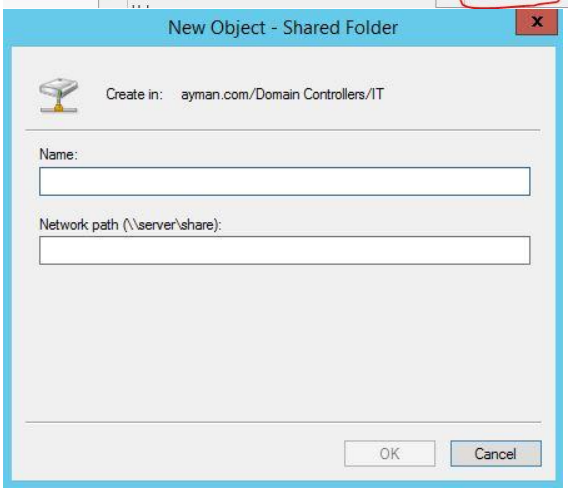
Publish resources

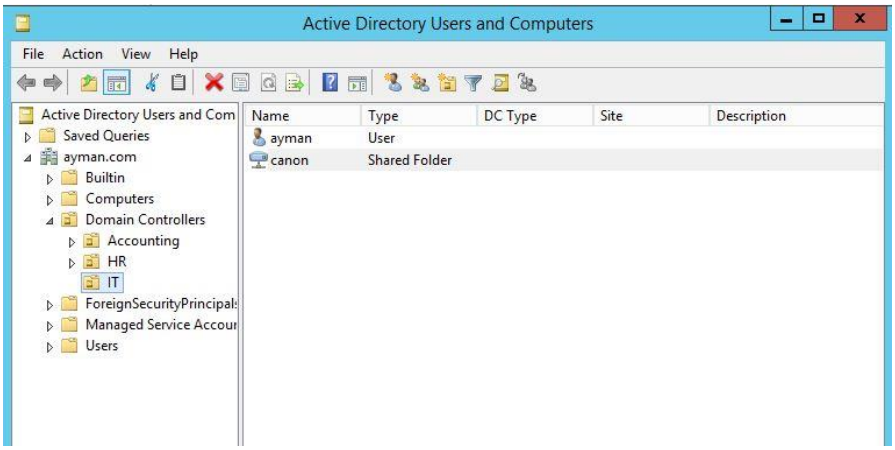
- Is for make shared folders be shared on Active directory for make users can use it easily because users usually aren't educated enough for fix IT problems.
- So publish source going to help in that case is create shared folder and publish in all users in 1 place have them tools which they're need for work " shared folder , printers , files , etc " without need path or IP or change nothing.

Steps:

"Server manager > active directory > Ou > right click > shared folder > give it path > ok ".







Notes:

*this option going to save a lot of time for not waste on users or users waste in find path or change IP or printer be offline.

* Users going to use them tools more easily and fast.

* No more pressure on the IT team for solve simple options.

Backup solutions

Problems:

1st lose or delectation in the domain... Then how can bring back same files with the SID for it work on users in OU's again.

2nd when the domain server be down.

3rd when have backup weekly and is for example Sunday but what going to happen when domain be down at Saturday that will make backup lose 6 days of work.

4th when have online folders like in banks or stoke holders and always someone using folder and can't make backup while.

Backup solutions		
System	**Data " backup strategy"**	**Online application**
• System state • Image	• Normal " full backup" • Incremental • Differential • copy	• shadow

- **System**

1- System state:-

Is take backup from system state only and it include the SAM files inside and it was could be controlled perfectly until XP O/S.

2- **Image**:-

Is take image from data.

- **Online application:**

1 - Shadow:

Is take flash backup while folders are in use and without effect on the system.

- **Data " backup strategy:**

1 - normal " full backup" :-

Backup all selected files.

Doesn't look for archiving marker.

Clear the marker.

2 – incremental :-

Backup all selected files with the archiving marker.

Clear the marker archiving.

3 – differential :-

Backup all selected files with marker.

Doesn't clear the marker.

4 - **copy:-**

Is take copy backup without effect on current backup type or scheduling.

Symantec backup exec 2012

- Add storage type " H.DD, Mas , NAS "
- Choose which need for backup "Data, system ".
- Choose the backup strategy type "full, incremental, differential ".
- Choose schedule "daily, weekly, monthly, and hourly".

Notes:

- For make perfect backup of system state must make image of windows with active directory "before it be configured "because system state must restored in the same in the same device with the same SID.
- Symantec backup exec 2012 work on only windows server 2008 and below.

User profile

1) **Local user profile:**

Windows security requires a user profile for each user account on a computer.

The system automatically creates a local user profile for each user when the user logs on the computer for the first time.

2) **Roaming user profile:**

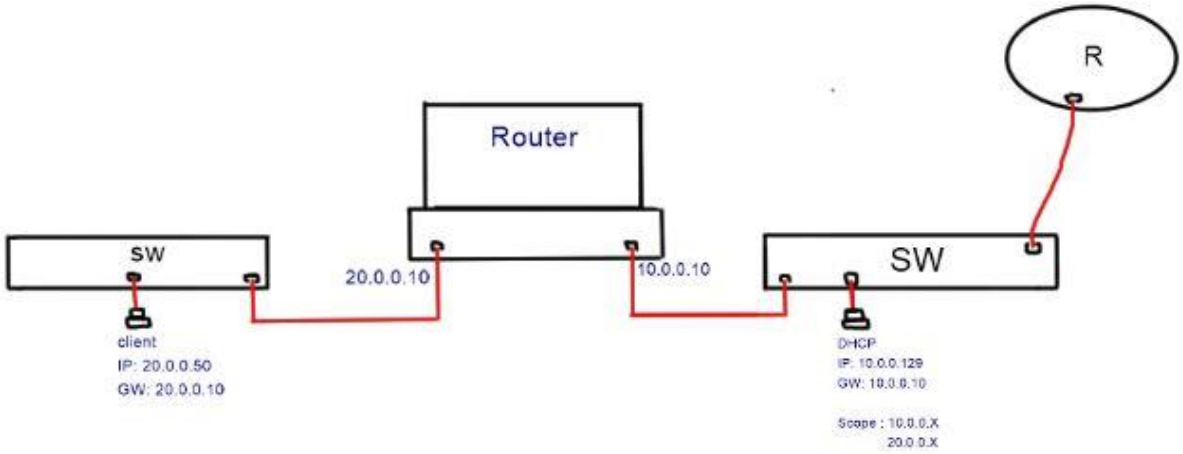
Users can store their profiles on the servers these are called roaming user profiles.

Automatic resources availability, a user's unique profile is automatically available when he or she logs on the any computer on the network, user won't need to create profile on each computer going to use.

User will find his saved data as it is in any device going to use it.

User must logoff after finish for action be updated and start work in other device.

Routing, NAT, Relay Agent



- **1st Routing:**

Is service in windows server able device for be router just need it have 2 network cards for it can made 2 networks 10.0.0.x and 20.0.0.x.

- **2nd NAT:**

Is option inside routing service be configured for make network 20.0.0.x and able for access the internet.

- **3rd relay agent:**

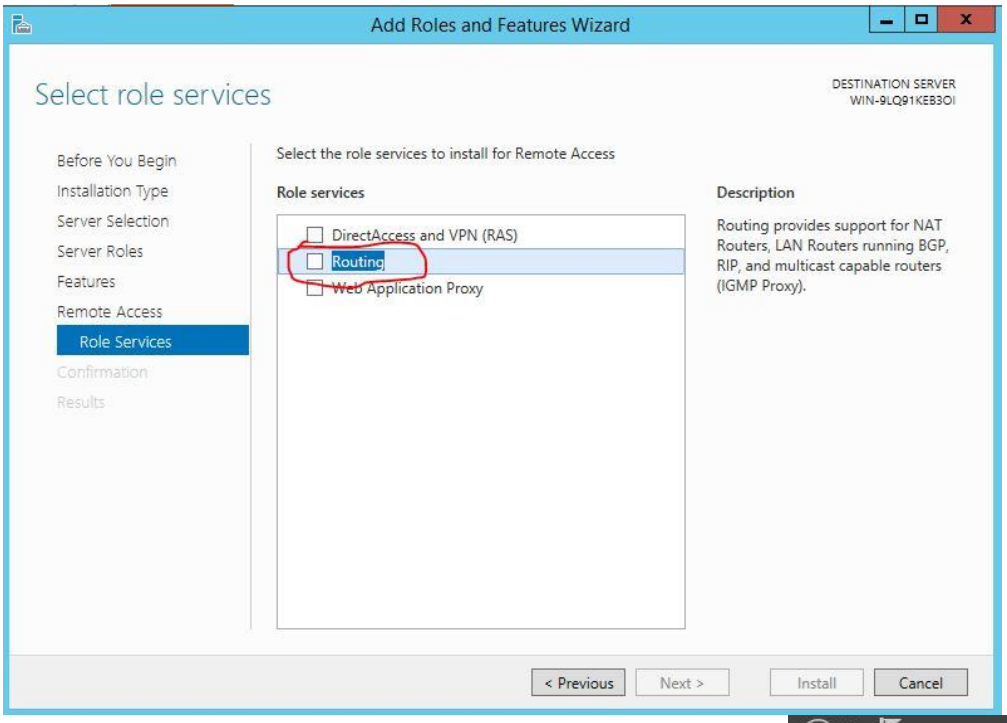
Is option inside routing service be configured for listen to network 20.0.0.x and pass the request to DHCP and back with IP.

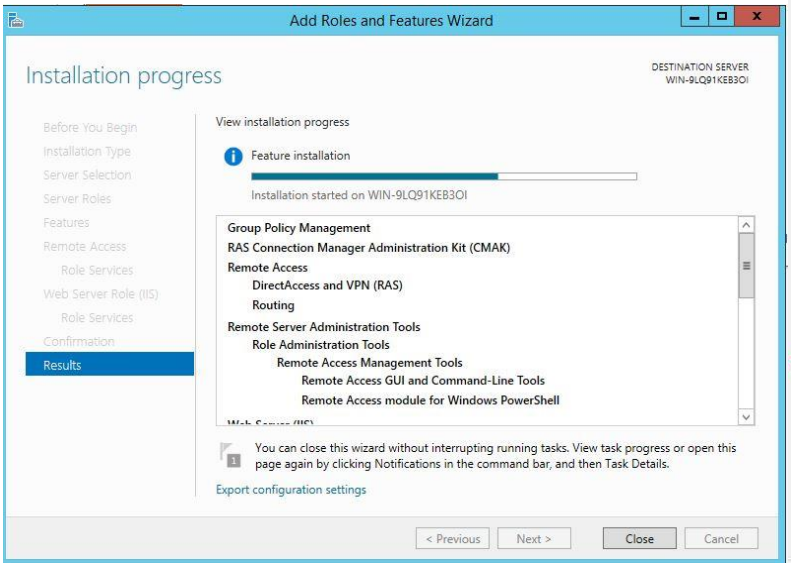
- **Routing**:-

Is service for make device be router and connect 2 networks in the same time.

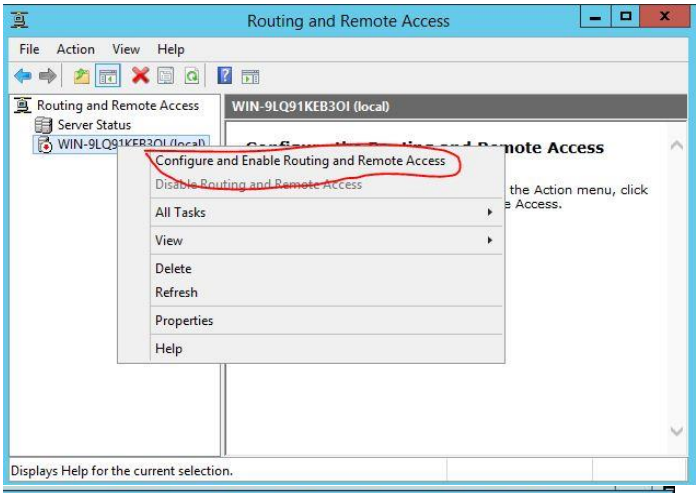
Steps:

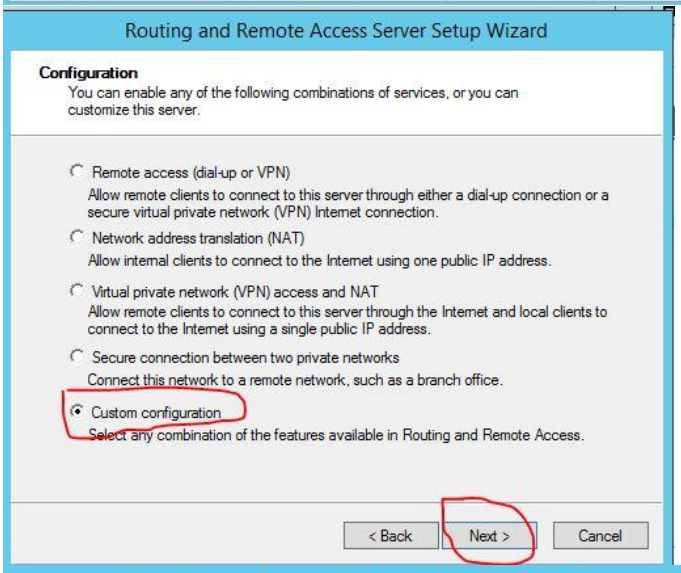
"Server manager > add role > next > remote access > next > choose routing > install > tools > routing and remote access > right click > configure and enable routing > in the wizard > in the wizard press next > customized > next > choose lan routing > next > finish "

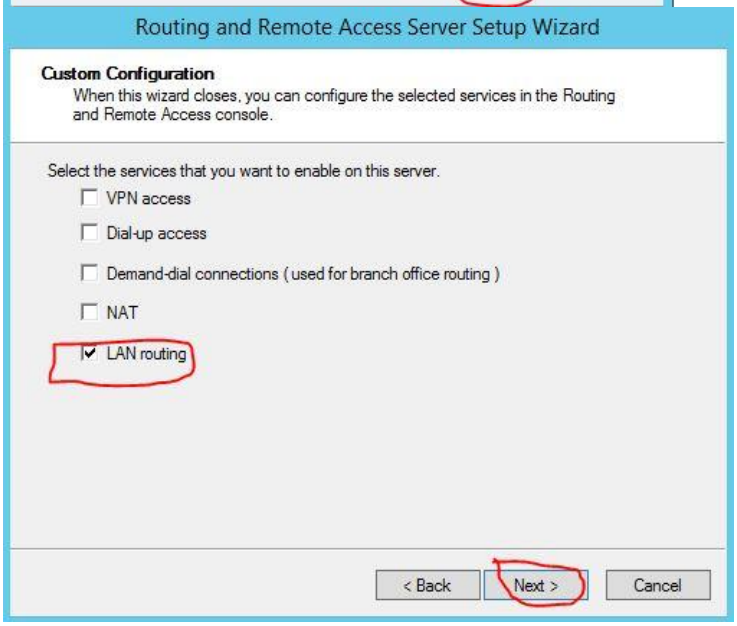

Add Roles and Features Wizard
Select role services
DESTINATION SERVER
WIN-9LQ91KEB3OI
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results
Select the role services to install for Remote Access
Role services
DirectAccess and VPN (RAS)
Routing
Web Application Proxy
Description
Routing provides support for NAT Routers, LAN Routers running BGP, RIP, and multicast capable routers (IGMP Proxy).
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN-9LQ91KEB3OI
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Installation started on WIN-9LQ91KEB3OI
Group Policy Management
RAS Connection Manager Administration Kit (CMAK)
Remote Access
DirectAccess and VPN (RAS)
Routing
Remote Server Administration Tools
Role Administration Tools
Remote Access Management Tools
Remote Access GUI and Command-Line Tools
Remote Access module for Windows PowerShell
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


Manage
Tools
View
Help
Active Directory Module for Windows PowerShell
Component Services
Computer Management
Connection Manager Administration Kit
Defragment and Optimize Drives
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Network Policy Server
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Remote Access Management
Resource Monitor
Routing and Remote Access
Security Configuration Wizard
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic


Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
WIN-9LQ91KEB3OI (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help
Displays Help for the current selection.


Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access.
< Back
Next >
Cancel


Routing and Remote Access Server Setup Wizard
Custom Configuration
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.
Select the services that you want to enable on this server.
VPN access
Dial-up access
Demand-dial connections (used for branch office routing)
NAT
LAN routing
< Back
Next >
Cancel

- **NAT**:-

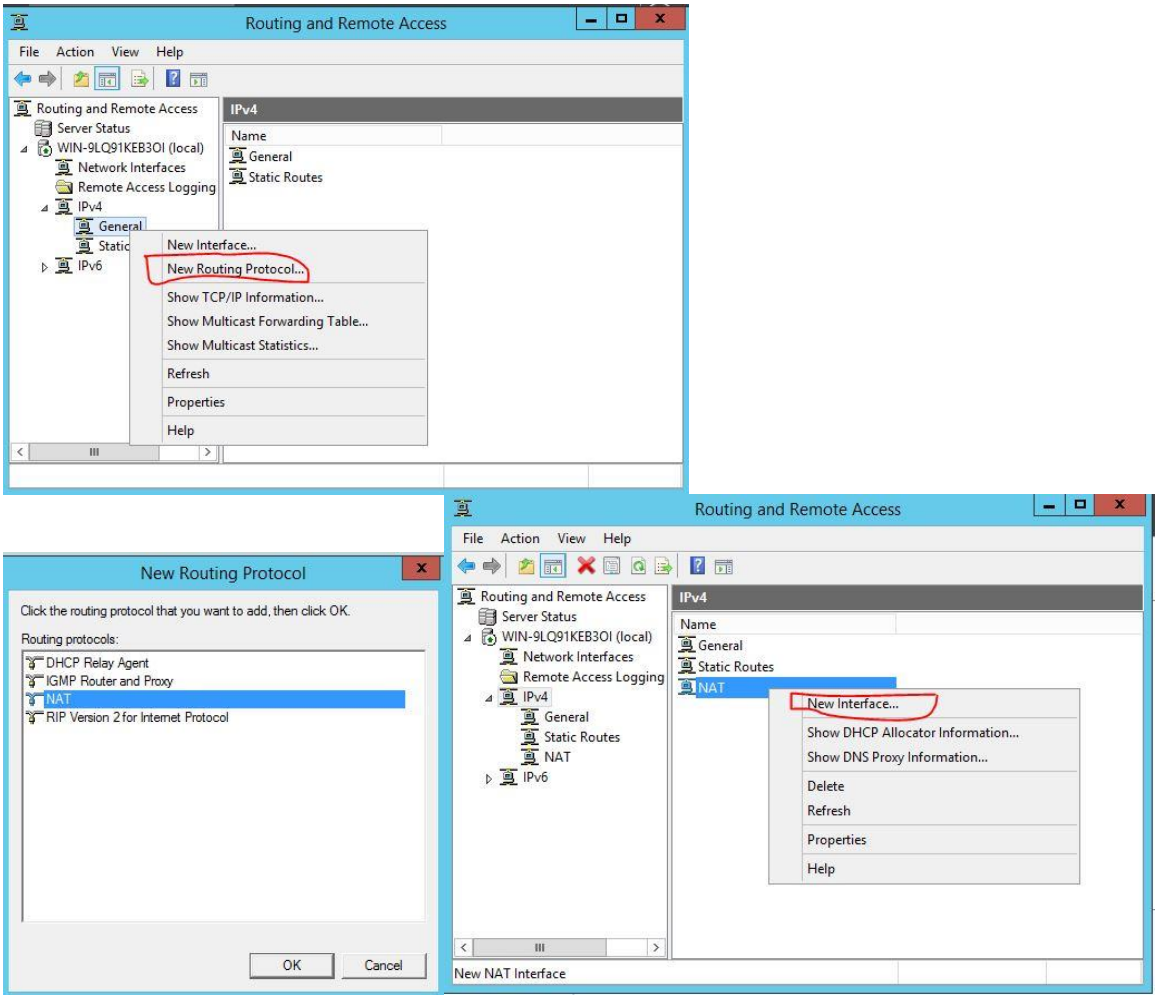
Is option responsible for change network IP to other ip for access internet, example cange virtual IP inside network to Real ip while accessing the internet.

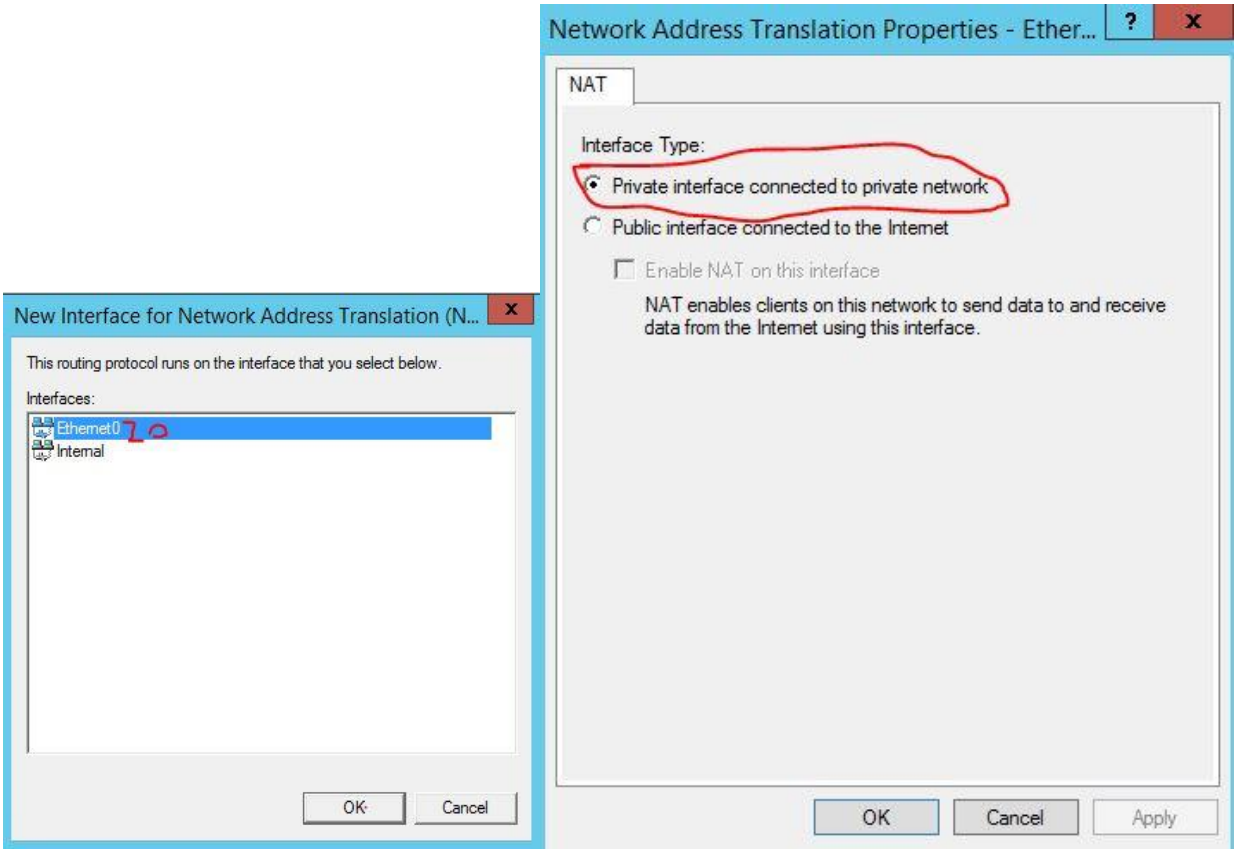
In our scenario it going to change the G, W for 10.0.0.x to can access.

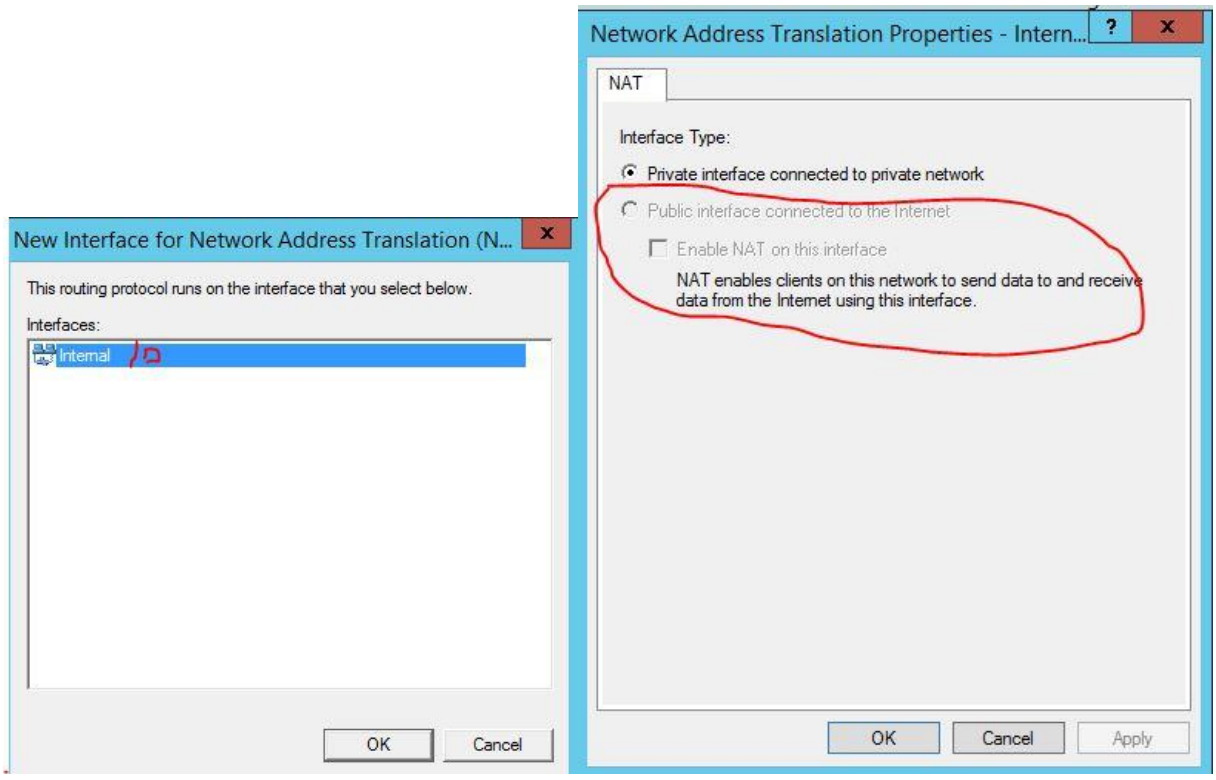
Steps:

"Server manager > tools >routing and remote access > ipv4 > general > right click > new routing protocol > ok > choose NAT > right click > new interface > choose 20 > ok > choose (private).

The same steps again but choose 10 > (public) > check mark (enable NAT on interface".




Network Address Translation Properties - Ether...
NAT
Interface Type:
Private interface connected to private network
Public interface connected to the Internet
Enable NAT on this interface
NAT enables clients on this network to send data to and receive data from the Internet using this interface.
OK
Cancel
Apply
New Interface for Network Address Translation (N...
This routing protocol runs on the interface that you select below.
Interfaces:
Ethernet0
Internal
OK
Cancel

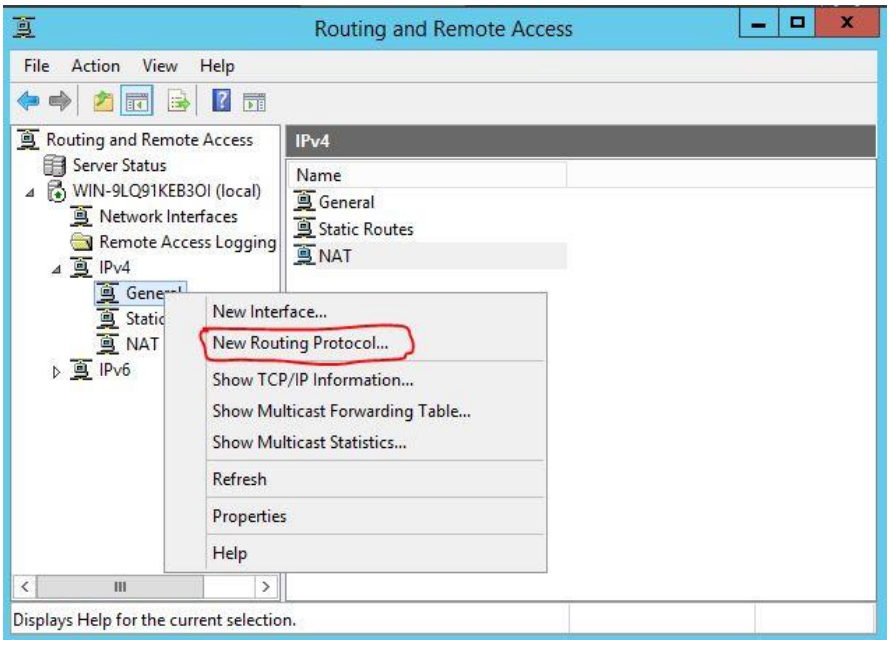

Network Address Translation Properties - Intern...
NAT
Interface Type:
Private interface connected to private network
Public interface connected to the Internet
Enable NAT on this interface
NAT enables clients on this network to send data to and receive data from the Internet using this interface.
OK
Cancel
Apply
New Interface for Network Address Translation (N...
This routing protocol runs on the interface that you select below.
Interfaces:
Internal
OK
Cancel

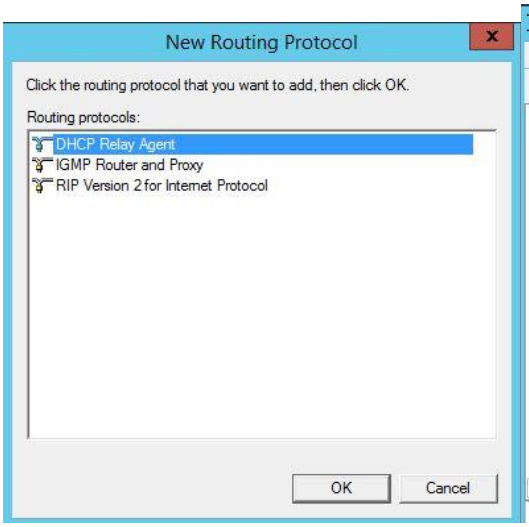
- **Relay Agent:-**

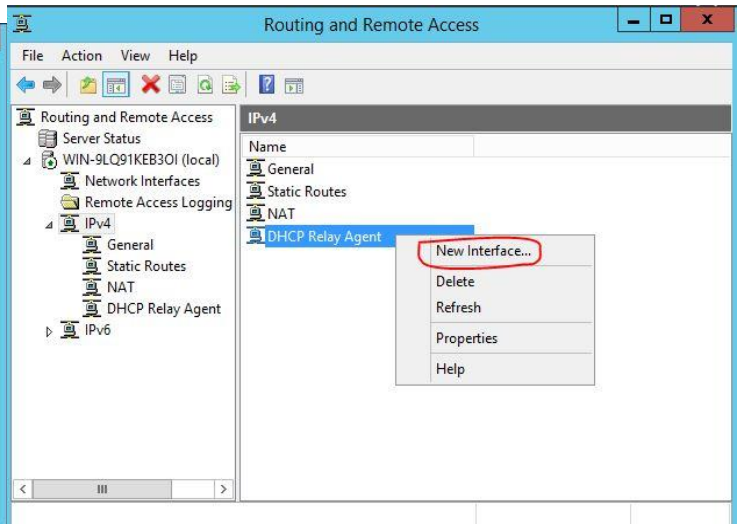
Is option responsible for to network broadcast and then deliver it for DHCP as broadcast will can't pass cause router will stop it so relay agent will change broadcast to unicast and be middleman to send it to DHCP and back with IP.

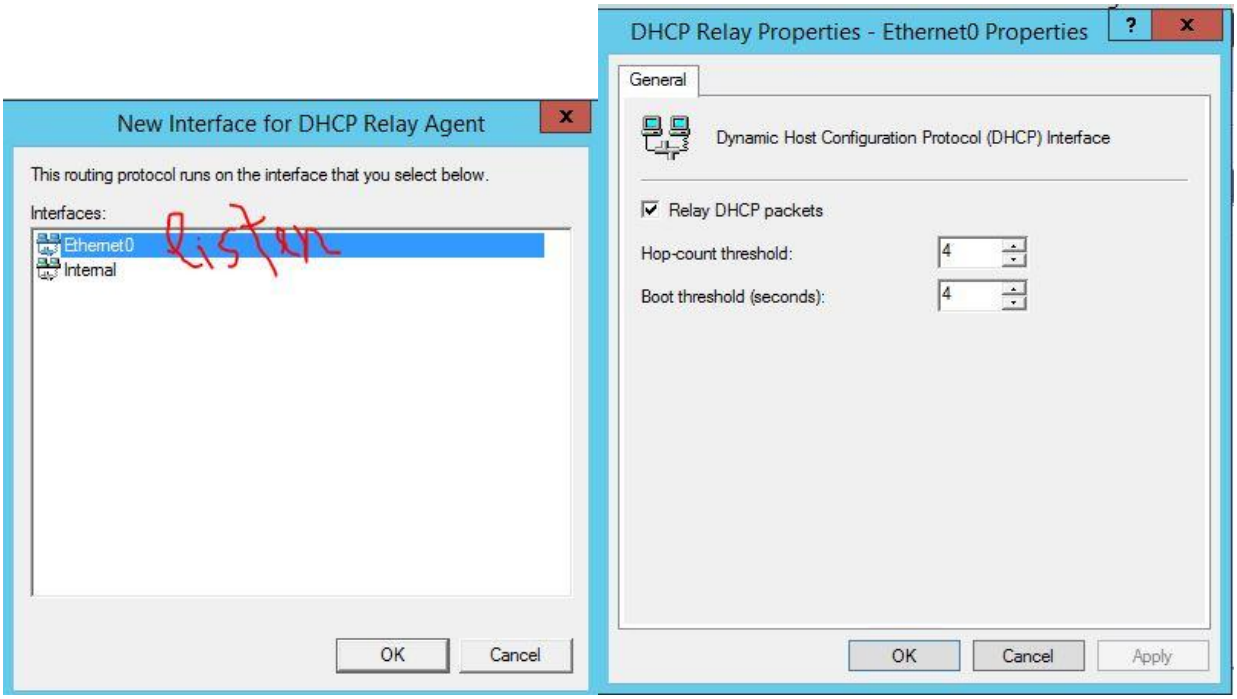
Steps:

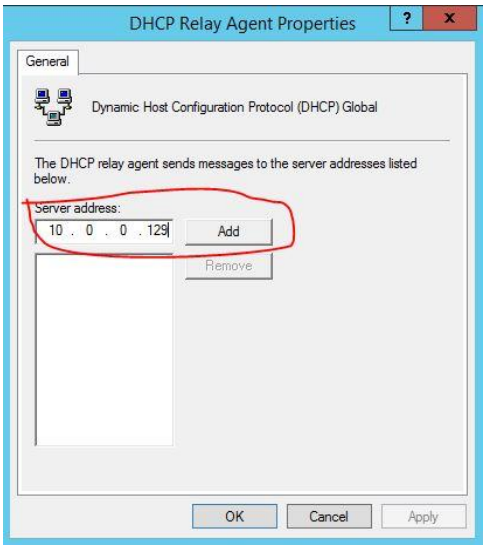
"server manager > tools > routing and remote access > ipv4 > general > right click > new routing protocol > DHCP (right click) > new interface > first choose listen network > right click on relay > properties > put IP of DHCP > ok ".





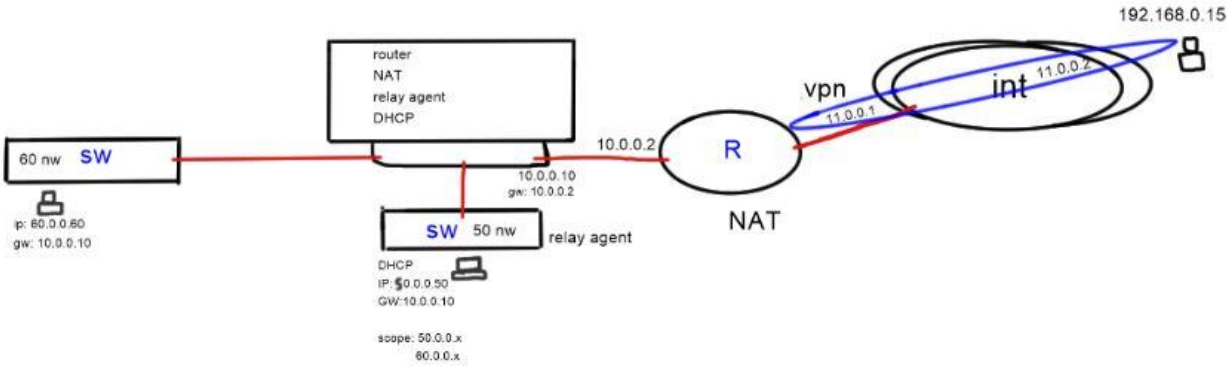



New Interface for DHCP Relay Agent
This routing protocol runs on the interface that you select below.
Interfaces:
Ethernet0
Internal
OK
Cancel
DHCP Relay Properties - Ethernet0 Properties
General
Dynamic Host Configuration Protocol (DHCP) Interface
Relay DHCP packets
Hop-count threshold:
4
Boot threshold (seconds):
4
OK
Cancel
Apply


DHCP Relay Agent Properties
General
Dynamic Host Configuration Protocol (DHCP) Global
The DHCP relay agent sends messages to the server addresses listed below.
Server address:
10 . 0 . 0 . 129
Add
Remove
OK
Cancel
Apply

RAS

Remote Access server



- 1st two networks 50.0.0.X and 60.0.0.X need Routing service for they can connect to each other.
- 2nd DHCP server is at network 50.0.0.X so it will can't listen to network 60.0.0.X and took the IP to them.
- 3rd need use NAT for devices can access to internet because they will have other gateway.
- 4th remote access from outside network and its not secured as it's in public worldwide network and here need use VPN.

VPN (Virtual private Network):

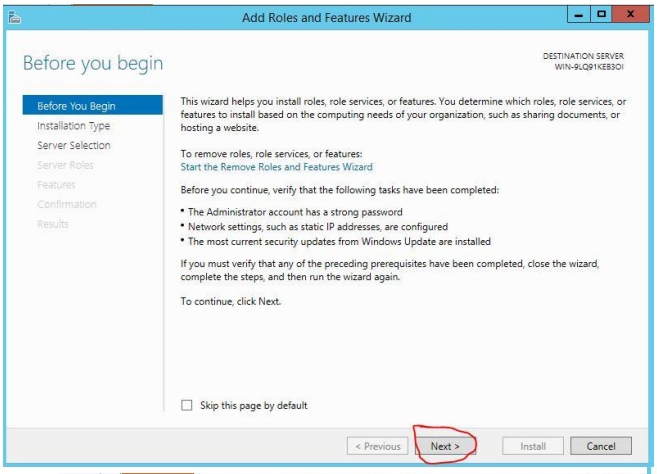
- Is creating virtual tunnel from remote user to host router and it be secured with virtual ip address away from hackers.

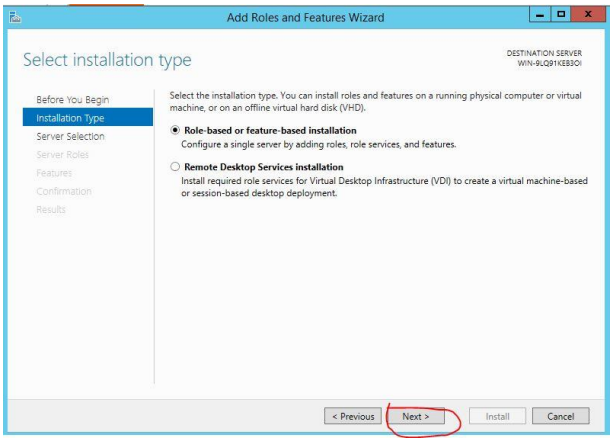
RAS (remote access server):

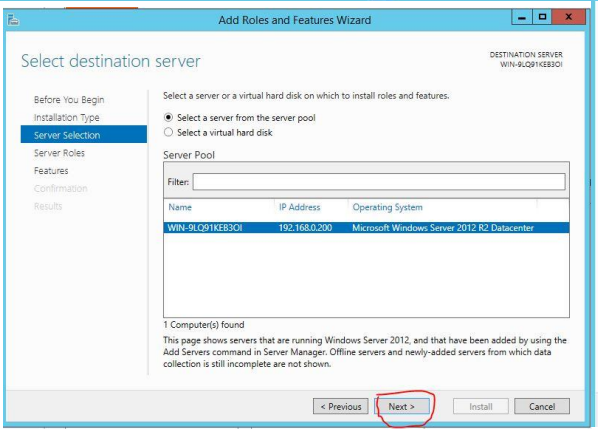
- Is for networks router accept the VPN session or dial up.
- Installing the RAS service is going to install routing automatically.

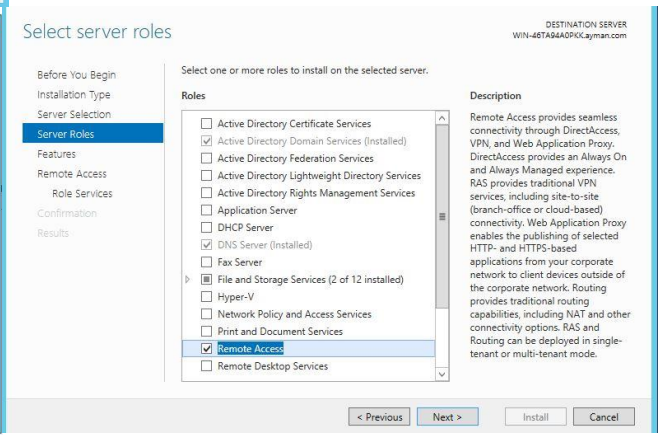
Steps:

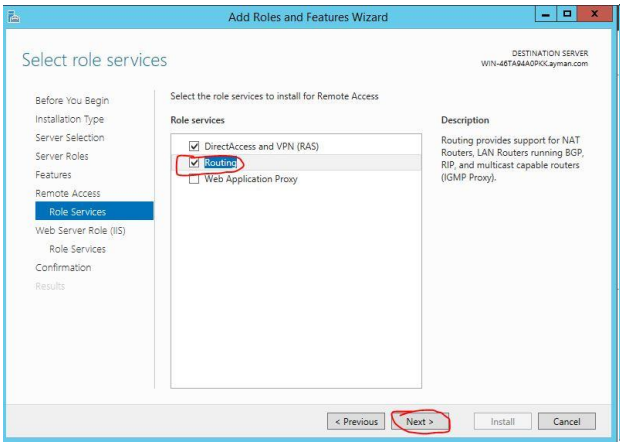
"Server manager > add role > routing and remote access > next > choose (routing) > install > tools > routing > and remote access > configure > choose VPN properties > set amount of ports".

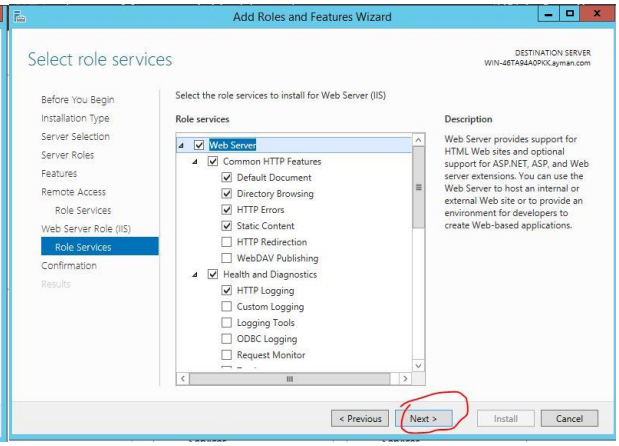

Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
WIN-9LQ91KEB3OI
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install 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

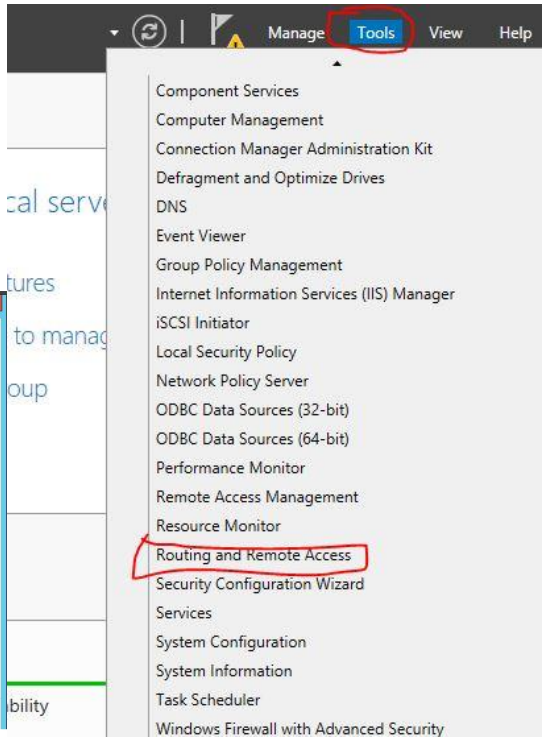

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
WIN-9LQ91KEB3OI
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, 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

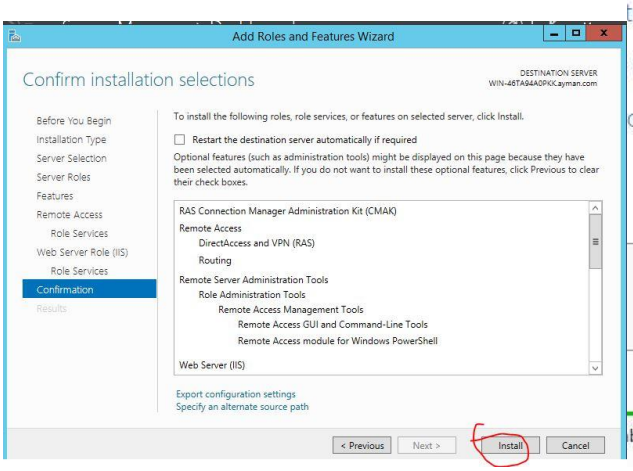

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
WIN-9LQ91KEB3OI
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
WIN-9LQ91KEB3OI
192.168.0.200
Microsoft Windows Server 2012 R2 Datacenter
1 Computer(s) found
This page shows servers that are running Windows Server 2012, 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

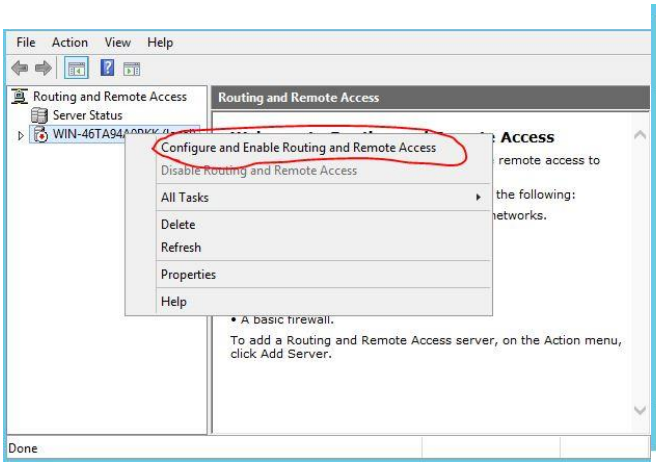

Select server roles
DESTINATION SERVER
WIN-46TA94A0PKK.ayman.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services (Installed)
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server (Installed)
Fax Server
File and Storage Services (2 of 12 installed)
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Description
Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.
< Previous
Next >
Install
Cancel

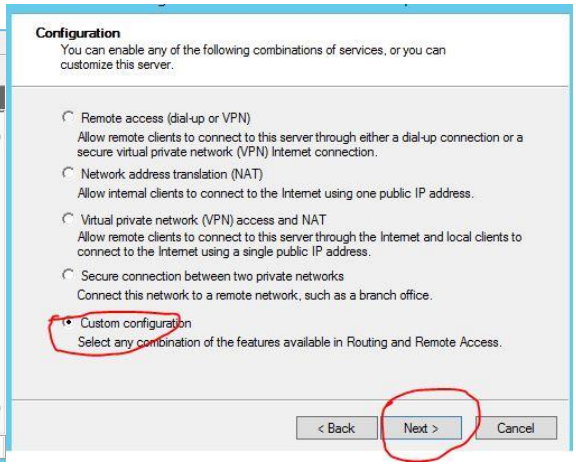

Add Roles and Features Wizard
Select role services
DESTINATION SERVER
WIN-46TA94A0PKK.ayman.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Remote Access
Role services
DirectAccess and VPN (RAS)
Routing
Web Application Proxy
Description
Routing provides support for NAT, Routers, LAN Routers running BGP, RIP, and multicast capable routers (IGMP Proxy).
< Previous
Next >
Install
Cancel

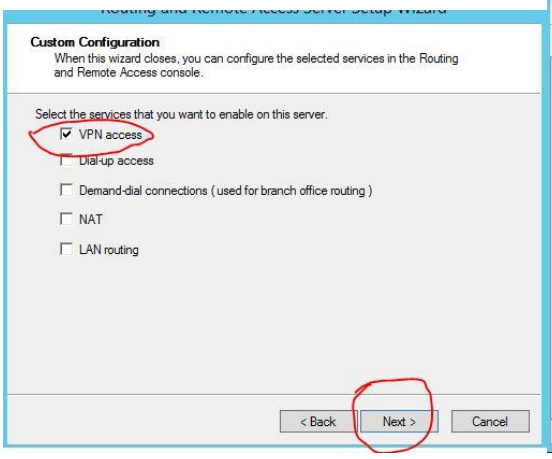

Add Roles and Features Wizard
Select role services
DESTINATION SERVER
WIN-46TA94A0PKK.ayman.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Web Server (IIS)
Role services
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
HTTP Redirection
WebDAV Publishing
Health and Diagnostics
HTTP Logging
Custom Logging
Logging Tools
ODBC Logging
Request Monitor
Description
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
< Previous
Next >
Install
Cancel

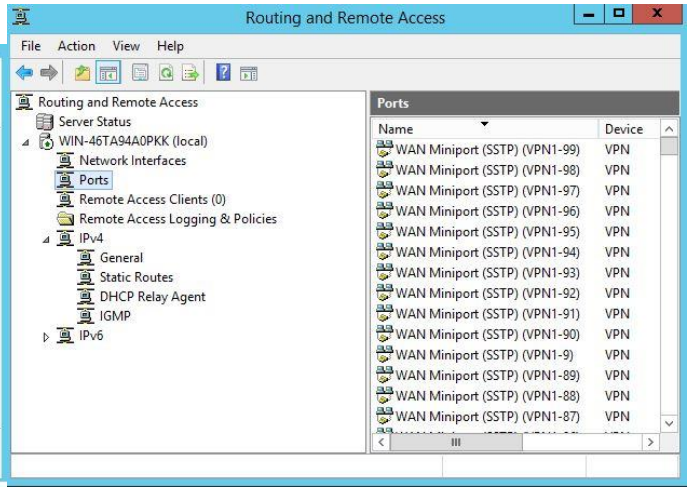

Manage
Tools
View
Help
Component Services
Computer Management
Connection Manager Administration Kit
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Network Policy Server
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Remote Access Management
Resource Monitor
Routing and Remote Access
Security Configuration Wizard
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security


Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
WIN-46TA94A0PKK.ayman.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
RAS Connection Manager Administration Kit (CMAK)
Remote Access
DirectAccess and VPN (RAS)
Routing
Remote Server Administration Tools
Role Administration Tools
Remote Access Management Tools
Remote Access GUI and Command-Line Tools
Remote Access module for Windows PowerShell
Web Server (IIS)
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel


File
Action
View
Help
Routing and Remote Access
Server Status
Routing and Remote Access
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
Delete
Refresh
Properties
Help
• A basic firewall.
To add a Routing and Remote Access server, on the Action menu, click Add Server.
Done


Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access.
< Back
Next >
Cancel


Custom Configuration
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.
Select the services that you want to enable on this server.
VPN access
Dial-up access
Demand-dial connections (used for branch office routing)
NAT
LAN routing
< Back
Next >
Cancel


Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
WIN-46TA94A0PKK (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging & Policies
IPv4
General
Static Routes
DHCP Relay Agent
IGMP
IPv6
Ports
Name
Device
WAN Miniport (SSTP) (VPN1-99) VPN
WAN Miniport (SSTP) (VPN1-98) VPN
WAN Miniport (SSTP) (VPN1-97) VPN
WAN Miniport (SSTP) (VPN1-96) VPN
WAN Miniport (SSTP) (VPN1-95) VPN
WAN Miniport (SSTP) (VPN1-94) VPN
WAN Miniport (SSTP) (VPN1-93) VPN
WAN Miniport (SSTP) (VPN1-92) VPN
WAN Miniport (SSTP) (VPN1-91) VPN
WAN Miniport (SSTP) (VPN1-90) VPN
WAN Miniport (SSTP) (VPN1-9) VPN
WAN Miniport (SSTP) (VPN1-89) VPN
WAN Miniport (SSTP) (VPN1-88) VPN
WAN Miniport (SSTP) (VPN1-87) VPN

User properties “Tabs”:

- Dial up:-

- **Network access permission:**

Totally allow all remote access.

Totally deny all remote access.

Configure it as it needs.

Notes:

- **At remote access the RAS will have 3 terms**

1- Authority
2- Authorization
3- Accounting

- When client try access RAS will check the AAA in the local device or the AAA/ ISE / radius “which they have records data of users.
- It will check first if username and password are available and then check user roles and what they can do when start session m then it going to make log file of session.

- **Verify caller ID:**

Is option for make users can access from specific place and specific device outside the network.

- **Call back option:**

is belong to Dial up connections which its high cost and it make when user try access it will hang up then call him back for save the expenses. .

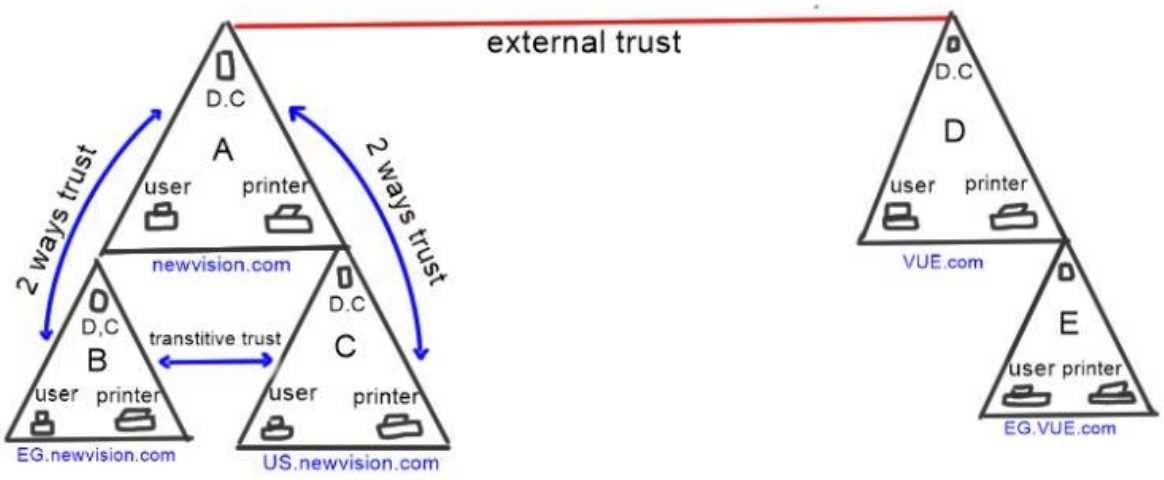
- **assign static ip:**

Is give user fixed static ip.

- **Apply static routes.**

Is give specific path and hops for users incase network has many routers.

Trust



- In domain "A" user can use printer inside the domain with its G.P.O.
- But user of domain "B" can also use the printer of domain "A", just as domain "A" user "B" trust each other.
- When domain "A" trust domain "B" it will be two ways trust and is going to allow both users use each other printers and data and sure every user will use with his own G.P.O.
- As long as domain "A" parent trust domain "B" child and domain "C" child domain "B" and "C" going to transitive trust and that will happen automatically.
- But when want trust domain from outside forest "D" must make external trust but it won't have transitive trust.

EX:

When new vision company buy VUE Company it will can't delete all database and build newer with policies of VUE so going to use external trust for connect both companies without rebuild over new

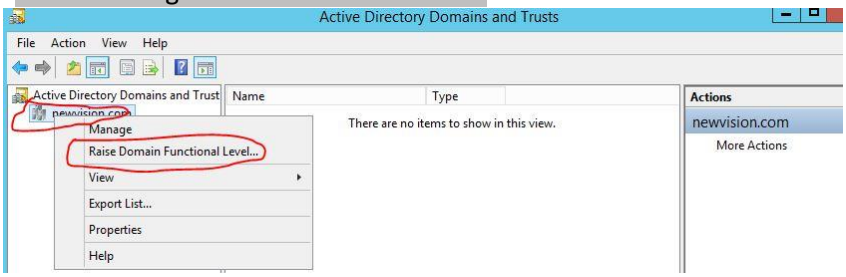
Function level

Their 2 levels domain and forest.

- Is option while installing domain controller in first domain in the first domain are doing the function level option will be shown and it has “2003-2008-2012” but can’t downgrade if once raise to other level.
- When DC be 2003 then can be 2008 or 2012 and users can be any OS.

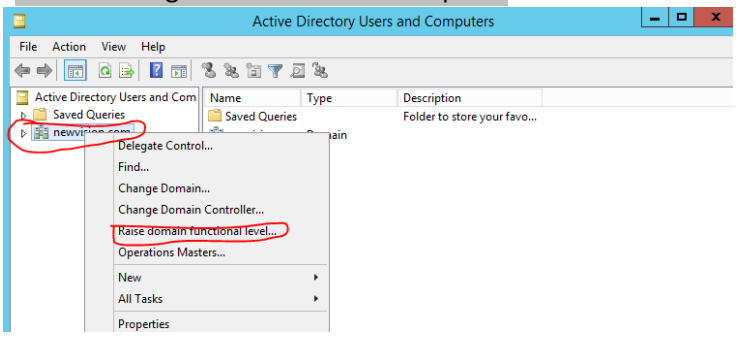
Steps for forest raise:

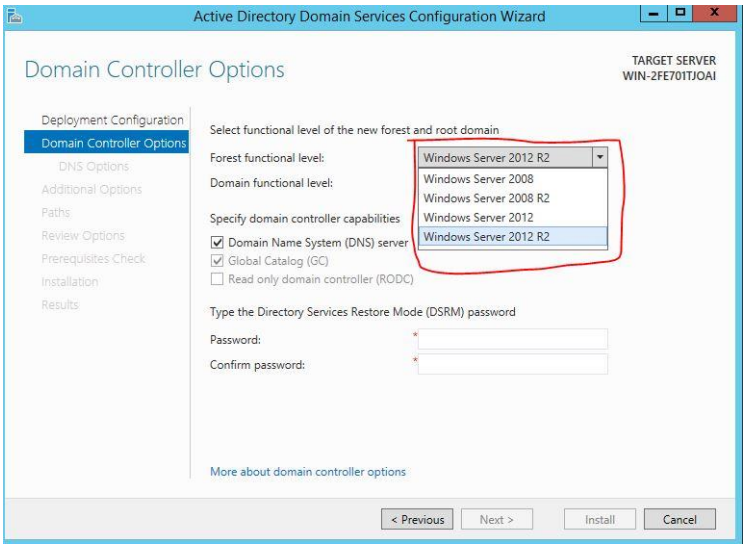
“Server manager > A.D domain and trust “



Steps for domain raise:

“Server manager > A.D user and computer”

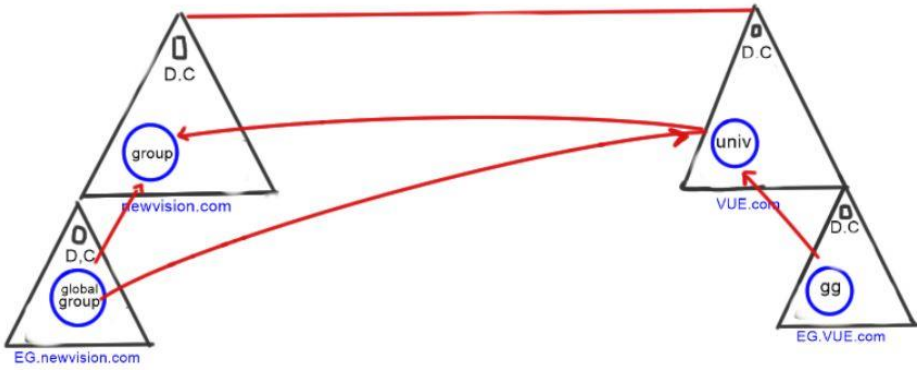




Notes:

- RODC work 2008 and 2012 but can't work 2003.
- When forest function level is 2003 the domains can be 2003, 2008, 2012 and if 2008 then domain will be 2008, 2012.

Domain Group



1) Distribution:

Is for mail exchange.

2) Security:

Is for apply permissions on groups.

- **Groups scope**:

1) Domain local group:

Members: the same domain /forest.

Permission: the same domain.

2) Global group:

Members: the same domain.

Permission: any domain in forest.

3) Universal:

Members: any domain.

Permissions: any domain.

Site

- **Site definition:**

Is ever high speed connection between sites.

- As create domain a site will be automatically created by default.
- In figure 1 domain has 2 companies branch in EG and US and both has 4 domain controllers.

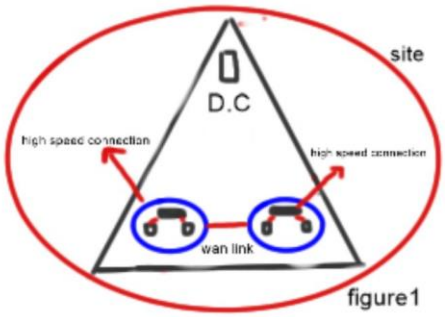


figure1

- Domain controller are replicating data every 15 sec and can't be managed or make specific hourly for it and that loading on the wan link cause beside replicating D.C data its replicating DHCP and DNS data and requests that beside normal users data transferring.

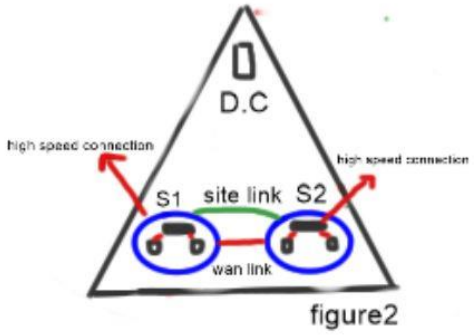
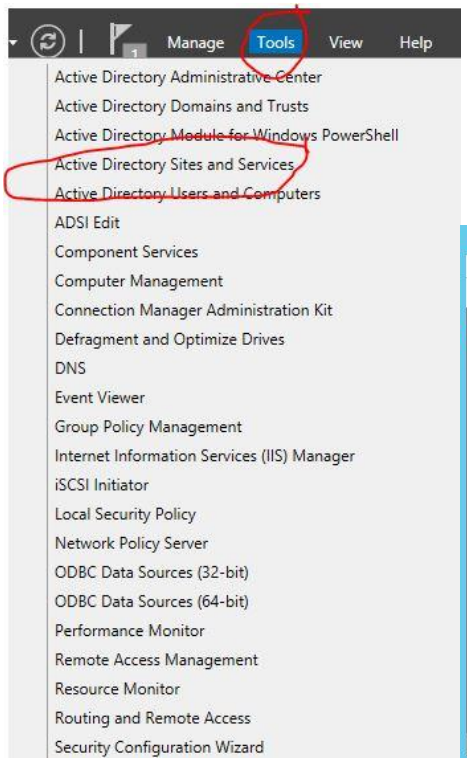


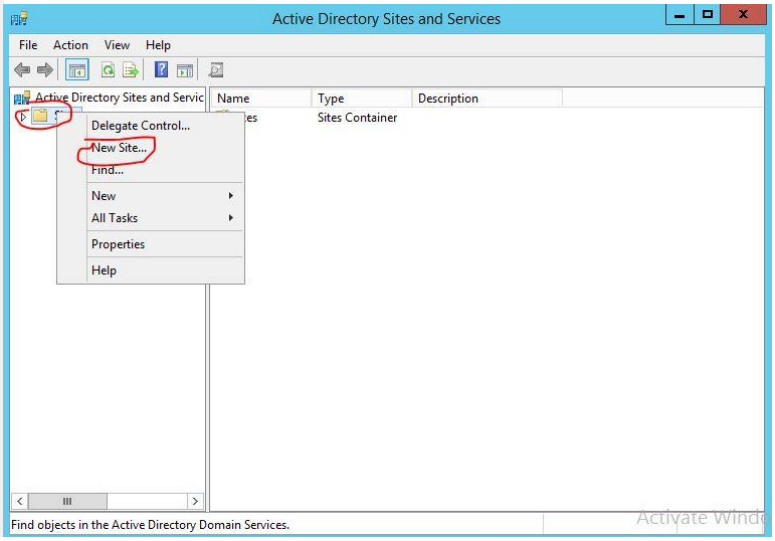
figure2

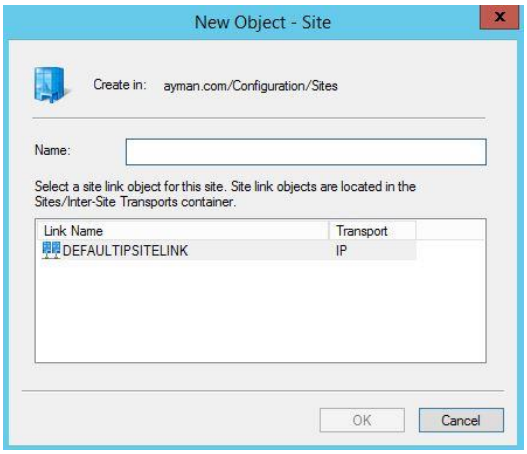
- Using site to divide main default site for 2 sites 1 is the default other be created like in figure 2
- Create site link for less the load on wan link and for be controlled with specific hourly.
- When servers start replicate it repeat itself many times for example in figure 2 the EG site servers add it replicate its data with the sites 2 servers then with its D.C then D.C replicate its data + add data and its mean replicate repeat the same many times, then we make 1 server in each site are responsible for replicating.

Steps:

"Server manager > tools > active directory sites and services > right click on site > new site > rename the default site > right click on subnet > put range".

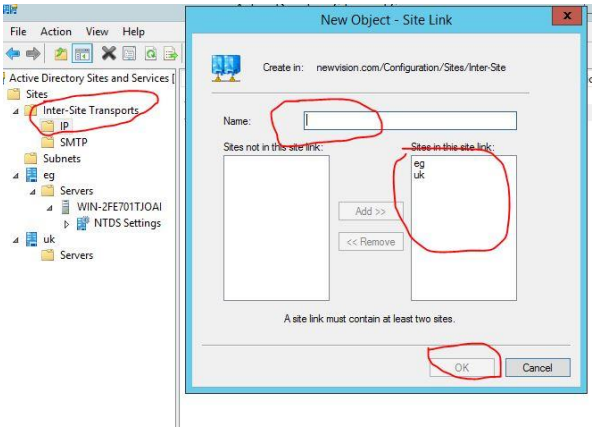






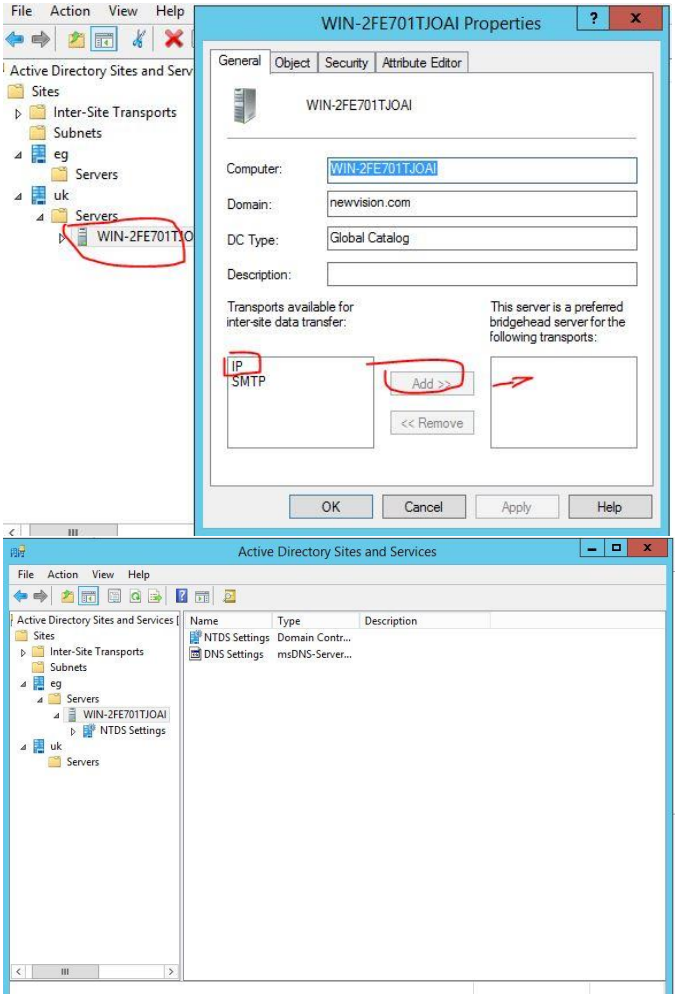
- **Site link:**

In inter-site transport > right click on site > add replication > after finish put sites inside server folder.

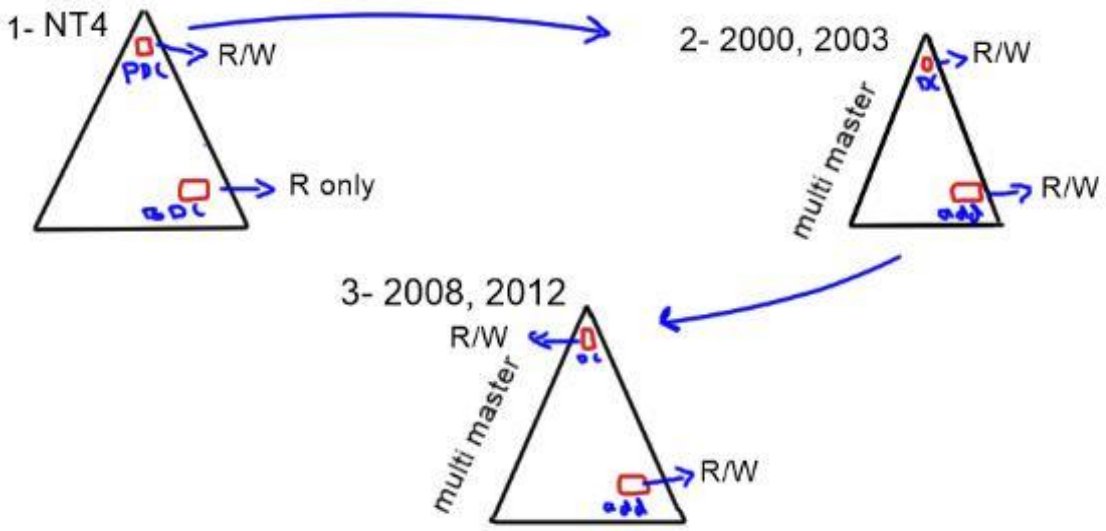


- **For make 1 server responsible for replicating :**

Server (name) > properties > general tab > add "IP" option to this server is preferred bridge head.



Operation Masters



- When Master "first DC "be down the additional be automatically read only.
- Any task DC had add it or made it will need 5 operation masters for be done.

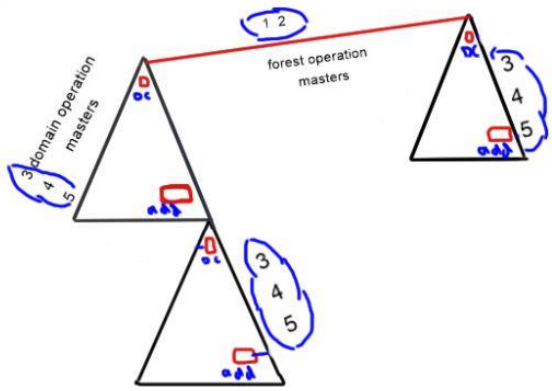
- **5 operation masters:-**

Per forest:-

1- Schema master.
2- Domain name master.

Per domain:-

3- PDC emulator.
4- RID "Relative identifier".
5 Infra-structure.



- **Notes:**

- **Schema master:**

Its table have all attribute of forest.

- **Domain naming master:**

FSMO role owner is the DC responsible for making changes to the forest wide domain name space of the directory in the partition container.

- Domain / forest prep:

Is responsible for match database.

- **PDC:**

1- Is responsible for group policy management.
2- Is responsible for password changes.
3- Is responsible for organizing the time for the whole domain.

- **RID**:

is responsible for give users tag if there the same SID in the domain, for can identify the difference.

- **Infrastructure:**

Responsible for follow objects which have updates and transfer the update notes to D.C.

- **Steps for transfer operation masters: "domain".**

Server manager > tools > active directory domain and trusts > right click on AD domain and trust > operating master > change.

- **Steps for transfer operating masters " user"**

Server manager > tools > active directory users and computers > right click on server > operating masters > RID "change" > PDC "change" > infrastructure "change".

- **Steps for transfer operating masters: "System"**

Start > run > type "regsvr32 schmmgmt.dll ".

Run > mmc > file > add/remove snap in > add "active directory schema" > change active server > choose current device > right click > operation master > change.

Global catalog

Is small copy of schema master but has the most common attribute in every domain.

EX: have domain has inside it 3 sites users complaints that authentication are slow that because user must move to main D.C because it has global catalog,

So must create additional D.C and put inside it copy of global catalog.

- **Steps for transfer G.C:**

Server manager > tools > active directory users and computers > default first site name > server name > right click properties > check mark on global catalog.

Notes:

NTDS: is name of A.D database.

Migration and time sync

- **Migration:**

Company with domain and it work with windows server 2008 and want to migrate it to 2012 windows server,

Without losing the data or group policy, and without down the server.

- **Steps**:

1st create additional work with windows server 2012.

2nd transfer all operating masters from D.C 2008 to the add 2012.

3rd demote/ remove / reinstall the D.C 2008.

4th make additional 2012 server.

- **Time sync:**

Is when site in USA and other in Egypt have.

Must both time be accrued.

If both site have same time zone system will fall.

Time zone of the site country if in USA 1pm then be in Egypt time zone 7pm.

Domain time it be the same.

G.P.O deploy software

Computer	User
- .msi - Assign	- . msi , .zap - Assign , publish

- **Steps**:

First must put software in shared folders and make sure it have at least read permission and also in security, and while search, search with same ip of domain.

Server manager > tools > group policy management > software installation > new > package > choose software > assign > publish

Start > run > gpupdate /force > logoff user.

Steps for remove:

Server manager > tools > group policy management > computer/users > d.c > software installiation > right click on S.W > remove

Start > run > gpupdate /force.

- **Notes**:

Assign:

Is make the deployed software appear in start menu and control panel.

Publish:

Is appear in file invocation and control panel and can hide it.

Software installation tabs:

1) **General**:-

- Default package location:

It has the shared file location, for any D.C user can find the shared s.w folder.

- When adding new package to user settings:

Is for display the deployment, assign, publish.

2) **Advanced**:-

If it has check mark it will remove the S.W when user change the Ou, because every OU has its policy.

But if unchecked then user can have his S.W in other Ou, but its risk because it may cause a conflicts.

3) **File extension:-**

When program have 2 version one is old and other is newer, in this tab can choose which of versions is going to install when user open the icon.

4) **Categories:-**

Is for make category for each user which want give the specific S, W without see all S.W.

5) **Modification**:-

When have multinational company it have branches in all over the world and more than 1 branch in each country , and for example have Microsoft office for deploy and with it languages packs this language file must be work as ” .mst” Extend for it work.

When do it each Ou will have language as admin specific for the country language.

NLB

Network load balancing protocol

1) **Round robins :**

Is feature in DNS responsible for rotate requests for services hosts, web servers, FTP servers, by managing the domain name system "DNS" responses to address requests from client computers according to an appropriate statically.

EX:

When devices request enter www.yahoo.com,

Round robin will be responsible for which server going to response,

For less the traffic on first server.

2) **NLB " Net load balancing " :**

Is feature distribute traffic across several servers ,by combining 2 or more computers that are running application into a single virtual cluster.

The hosts inside cluster can be configured the load that is to be handled by each host; you can also add hosts dynamically to the cluster to handled increase load.

NLB support up to 32 computers in a single cluster.

Add hosts to the NLB cluster as long as load increases.

Remove hosts from the NLB cluster as the load decreases.

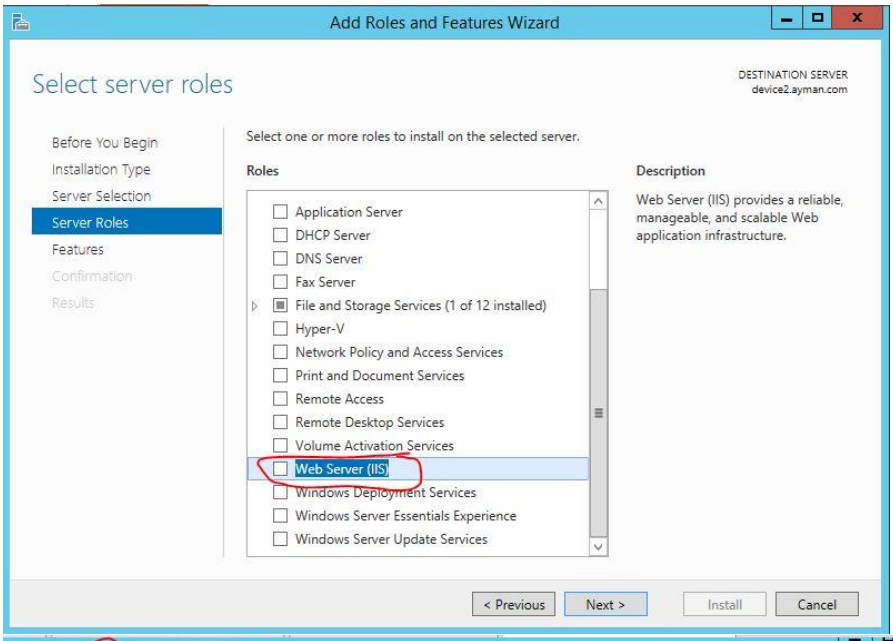
- **Manageability**:

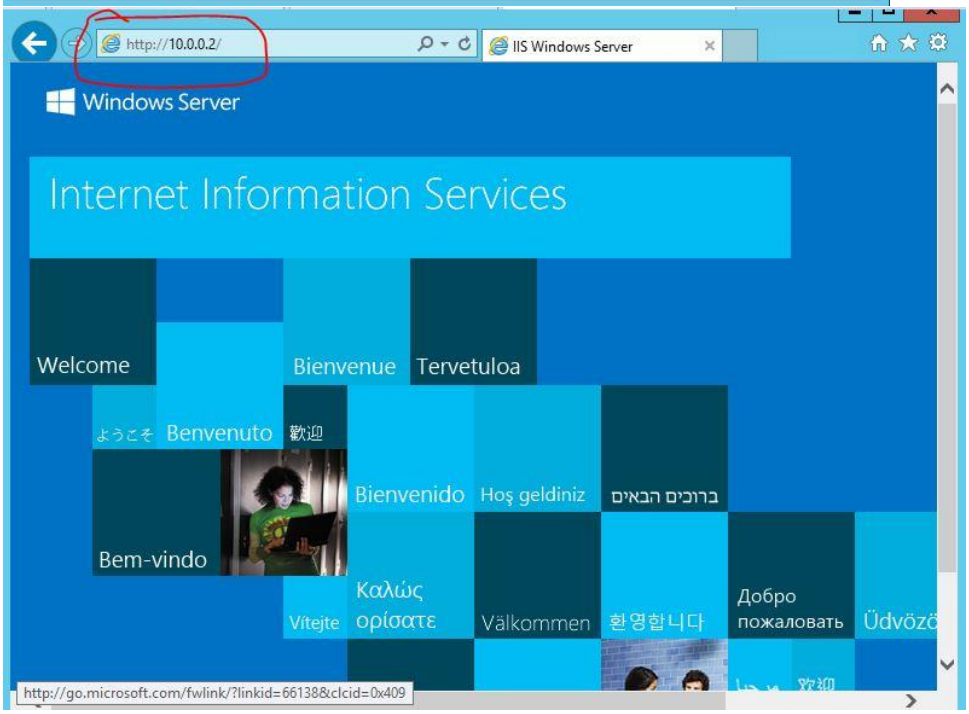
1) Specify the load balancing behavior for single ip port by using port management.
2) Define different port rules for each website.
3) Direct all clients' requests to a single host by using option "single host rule".
4) Block undesired network access to certain ip ports.
5) Enable "IGMP" internet group management protocol" support on cluster hosts to control switch port flooding "when incoming network packets are sent to all ports on switch".
6) Start, stop and control the NLB actions from its properties.
7) Drain stop is stop getting incoming requests till finish the current requests then it will stop, for not down the server.

Installation Steps:

- 1st in the devices which will join the virtual cluster install the IIS role for devices be webservers.
- Make sure firewall is disabled for webservers be able to communicate.

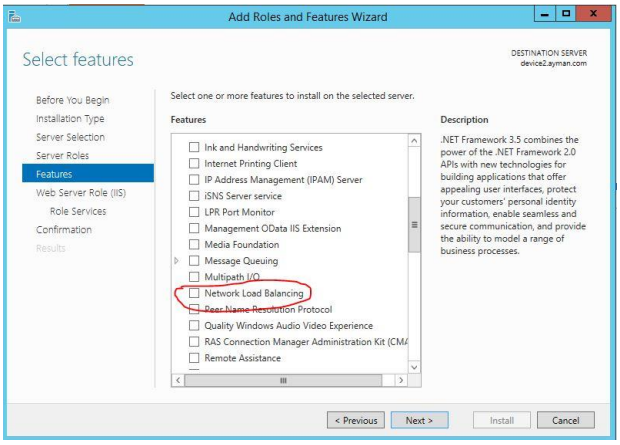
"Server manager > tools > add role > IIS > next > install".





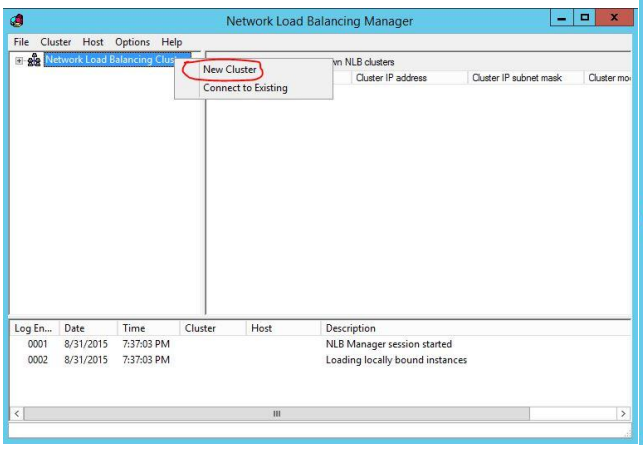
- 2nd install net load balance on devices.

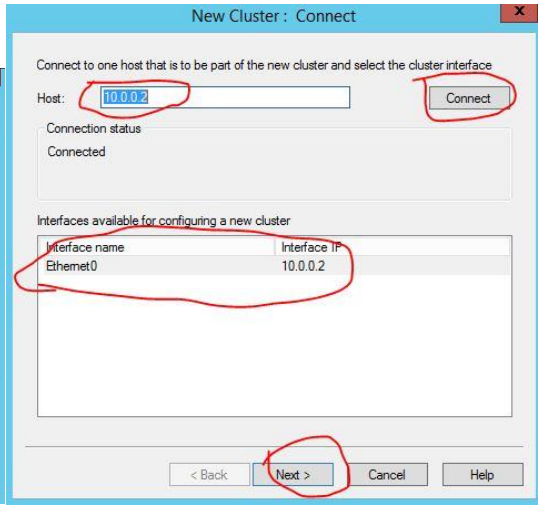
"Sever manager > tools > add features > net load balance > next > install".

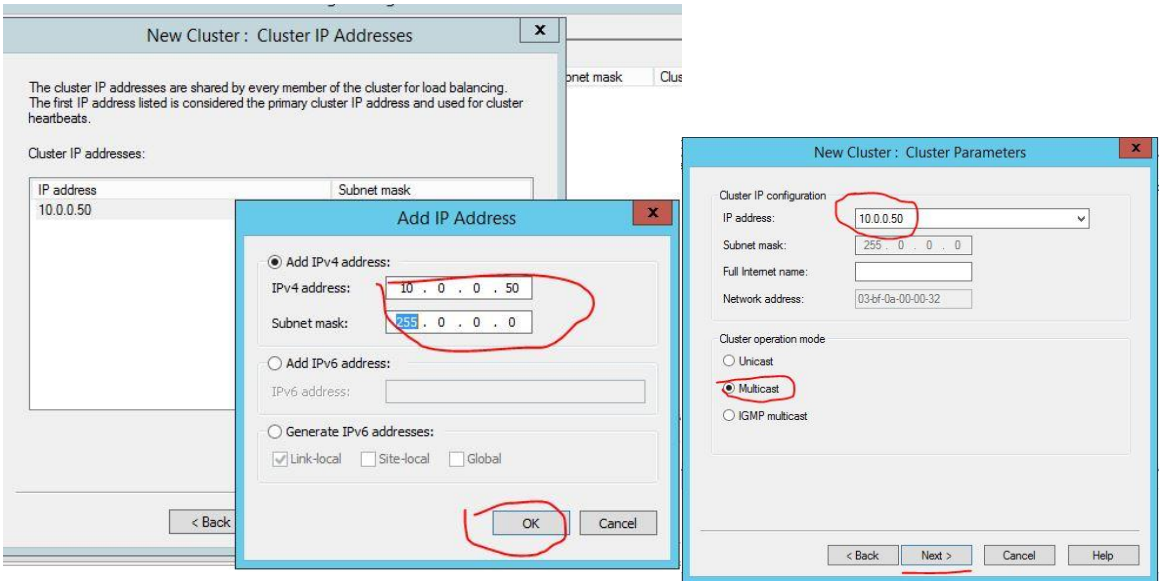


- 3rd connect devices ip with NLB.

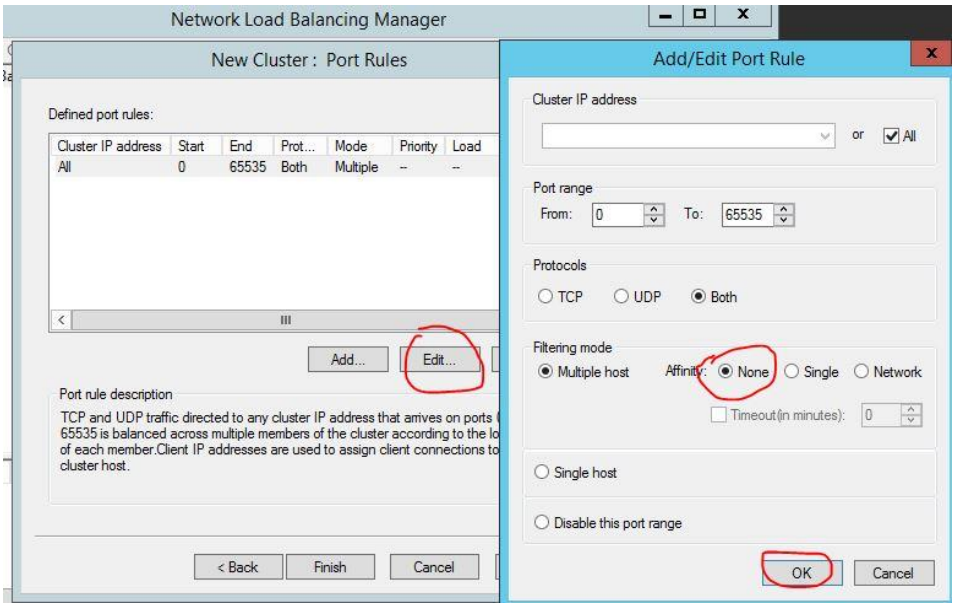
"Net load balance > add new cluster > add devices > add ip > full server name > choose mode".





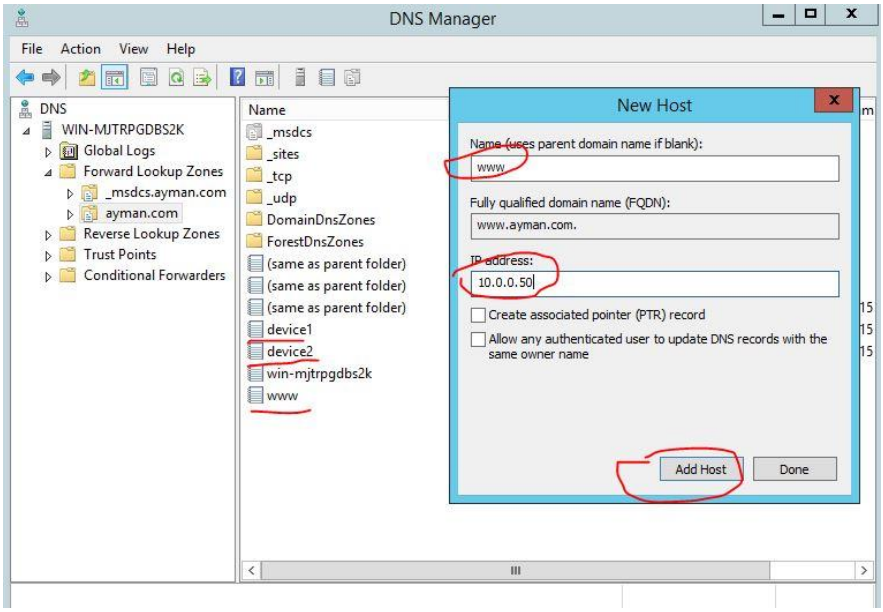


Edit port rule > choose affinity “None” > press “ok”



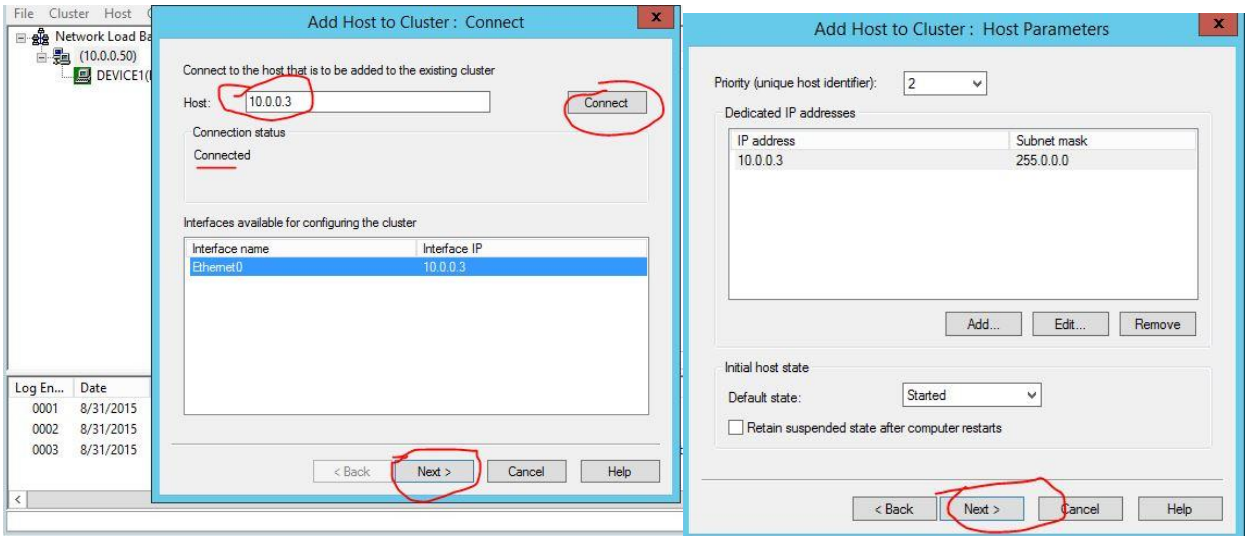
- 4th in DNS server create record with name and ip different than other devices in network “virtual cluster”.

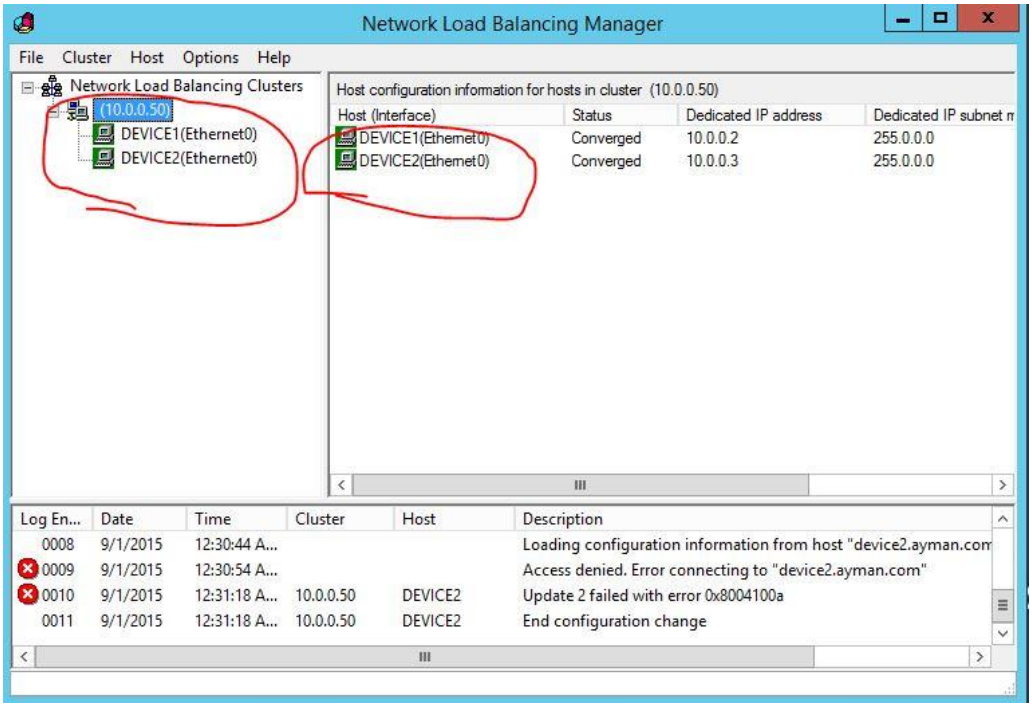
“Server manager > DNS > create “AAA” > name it “WWW” > browse > choose the webserver



- 5th in NLB

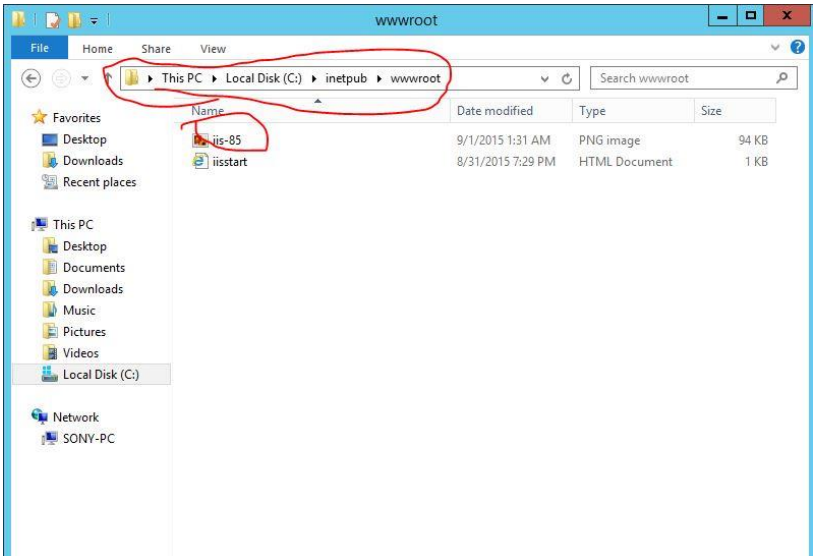
“NLB > right click on cluster > add host to cluster > type ip > connect > next“.



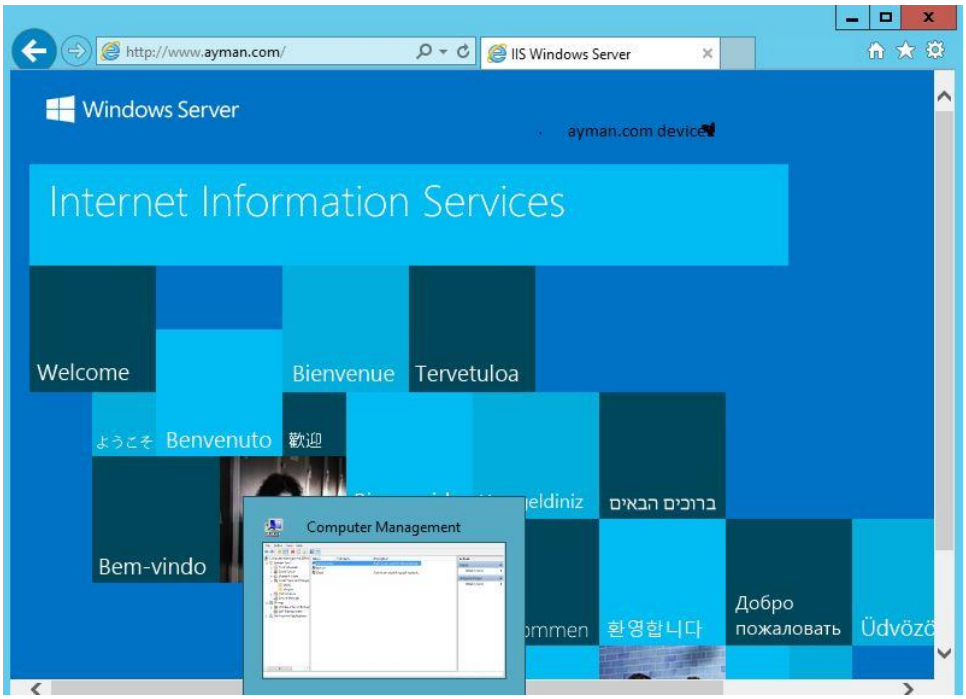


Check it from open internet explorer and type http://domainname.com if it open then it work perfectly...
Also u can disable device 1 network card then check if 2nd will can work automatically.

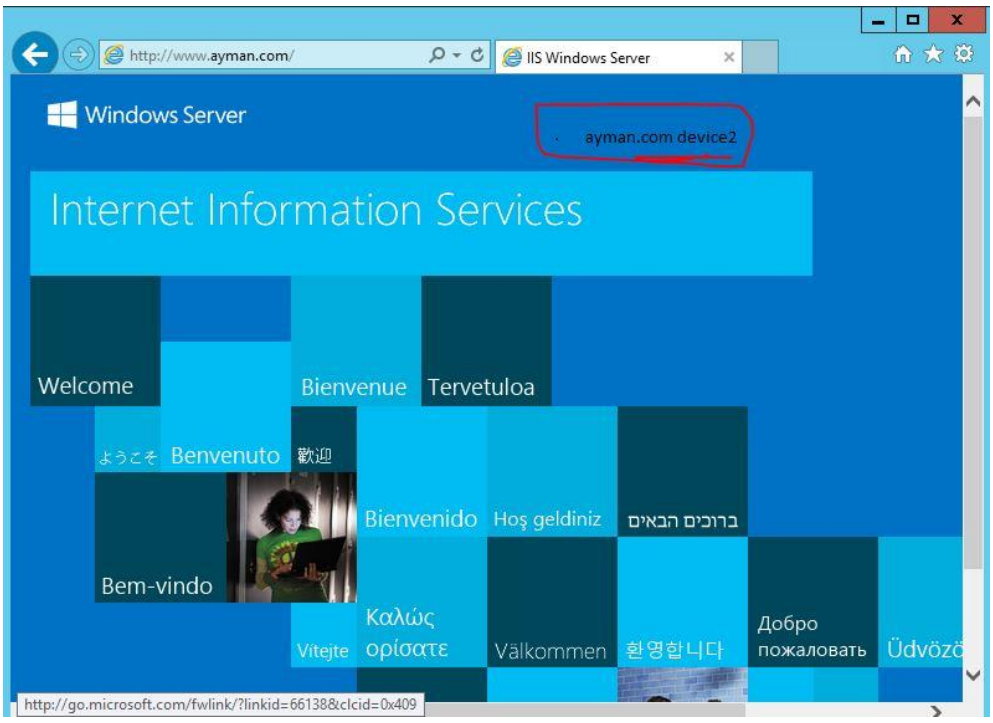
Open the iis image and edit on it >save it in same location



Open internet explorer and type http://ayman.com u will find the device 1 iis image because it have priority 1



Now disable device1 network card and try again will find the device2 iis appear



Notes:

- **Filtering mode:**

Affinity must be “none” for client when requests, devices be rotated between them and clients.

- **Unicast mode:**

It need huge firm and each device must has 2 network cards and it’s not allowed to communicate to each other.

- **Round robin:**

Cant load balance on the NLB clusters or members cause it support only 1 device.

- **IIS:**

Devices which have records must have iis service “internet info’s services”, for when devices requests web service the other can respond.