مدرس : مهندس جعفر عقربی

WWW.NETRES.IR

JAAFAR_AGHRABI@YAHOO.COM

# MCITP

تهیه‌کننده : فرشید عجب‌نوش

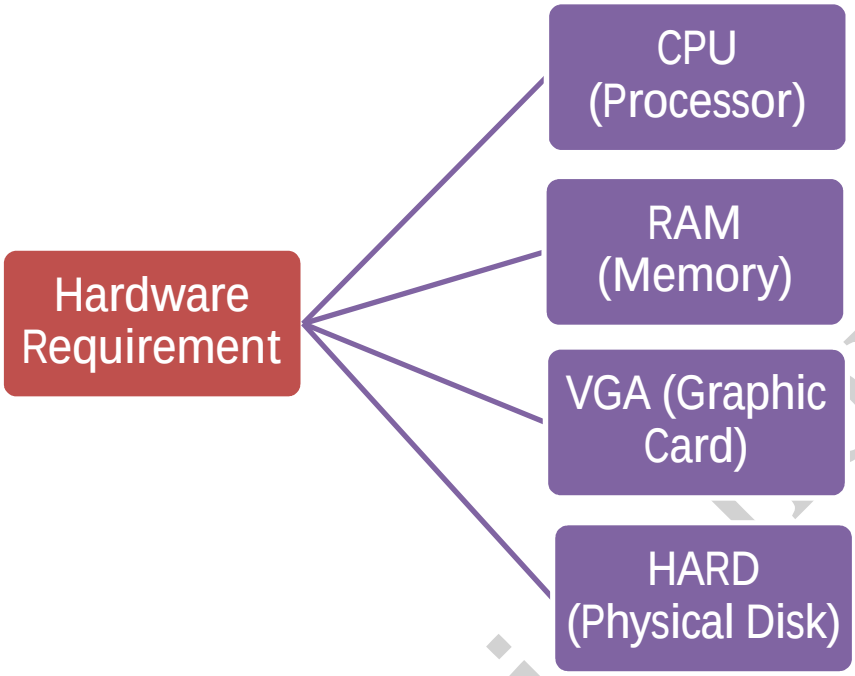
FARSHIDAJABNOUSH@GMAIL.COM

**با سپاس بیکران از خداوند منان که توفیق نگارش این جزوه را عطا فرمود و تشکر و قدردانی از زحمات بی شائبه استاد گرامی و بزرگوار *جناب آقای مهندس جعفر عقربی* که در طول انجام این امر بنده حقیر را از راهنمایی ها و هدایت های بی دریغ خویش برخوردار نموده اند، از خداوند بزرگ طول عمر و عزت ایشان را خواهانم و امیدوارم که این کار کوچک و پر از کاستی مورد قبول واقع گردد.**

**فرشید عجب‌نوش**

FarshidAjabnoush

نصب و پیکر بندی یک Client داخل شبکه :

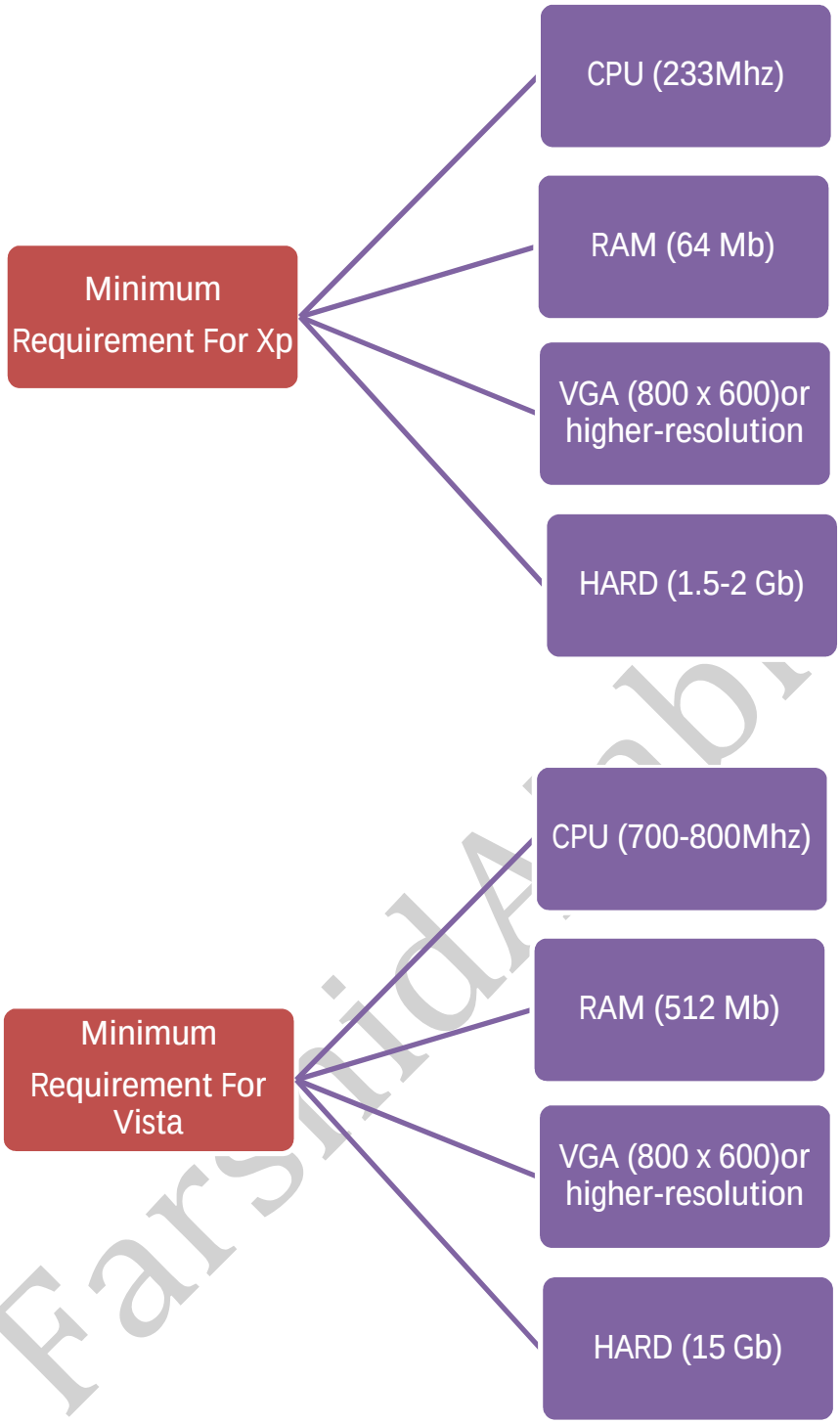



تفاوت بین 64 بیت و 32 بیت :

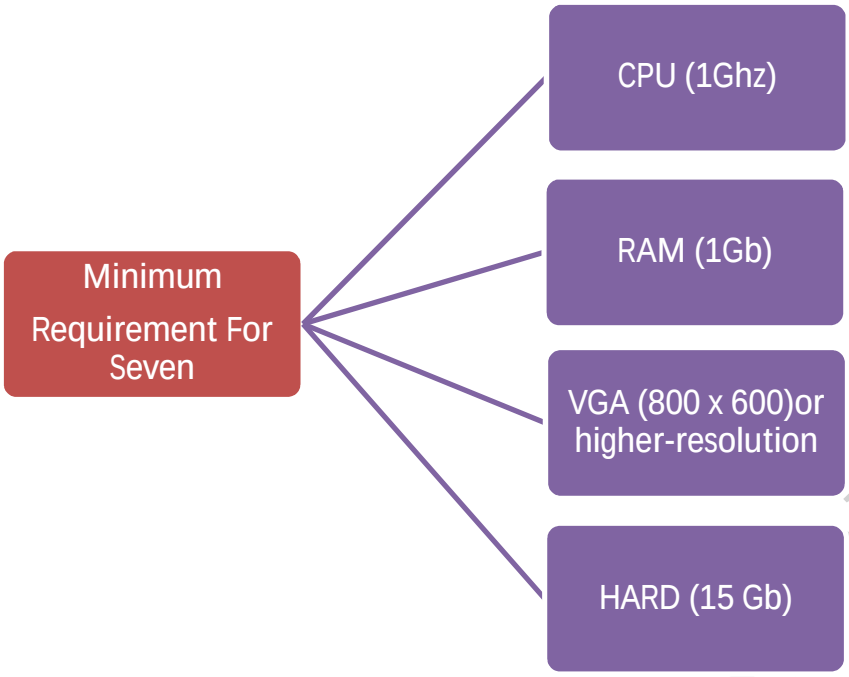
در سیستم عامل های 32 بیتی پردازشگر داده ها را بصورت 32 بیت 32 بیت از روی رم برمیدارد،به این معنی که برای هر32بیت یکبار به سراغ رم می آید،این یعنی درگیر شدن بیهوده پردازشگر، نتیجه افت سرعت در پردازشگر در حالی که در سیستم عامل های 64 بیتی پردازشگر داده ها را بصورت 64 بیت 64بیت از روی رم برمیدارد،به این معنی که برای برداشتن داده ها یکبار به سراغ رم میرود واین باعث بالا رفتن سرعت پردازشگر می شود،مزیت دومی که باعث برتری سیتم عامل64 بیتی نسبت به سیتم عامل32 می شود این است که سیستم عامل64 بیتی قادر به پشتیبانی تا 128گیگا بایت حافظه رم و حتی بالاترمی باشد ولی سیستم عامل 32 بیتی تا 4 گیگا بایت حافظه رم را بیشتر پشتیبانی نمی کند.

- در زمان استفاده از سیستم عامل64 بیتی باید به این نکته توجه داشته باشیم که سخت افزارهای ما قابلیت پشتیبانی از سیتم عامل 64 بیتی را دارا باشند درغیر اینصورت از مزیت های گفته شده درباره سیستم عامل64 بیتی بی بهره میمانیم.(درایورهای 64 بیتی)
- در کامپیوترهای سرور به دلیل اهمیت سرعت، بیشتر از سخت افزار و سیستم عامل64 بیتی استفاده می‌شود.

FarshidAjamoush

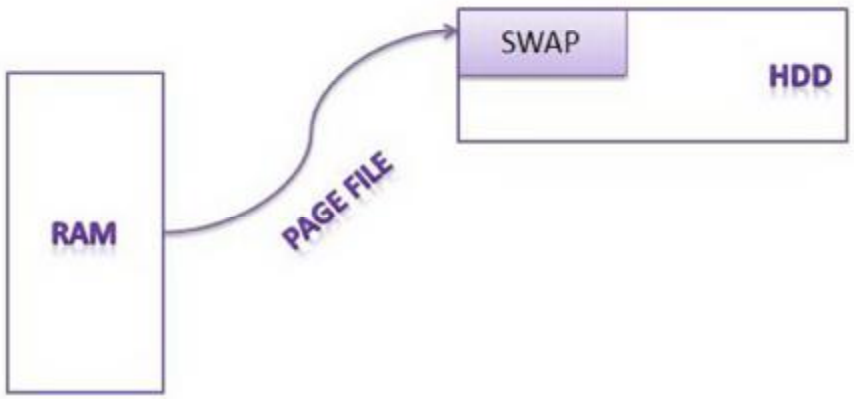



FarshidAbbasi




Virtual Memory (swap):

**زمانی که رم فضای کافی برای باز کردن فایلها بر روی خود را نداشته باشد به همان مقدار مورد نیاز از ظرفیت هارد استفاده می کند.**




FarshidAjabshoush

اصطلاح انواع سیستم عامل ها :

Windows 98: Down Level

Windows Xp,2003: Legacy

Windows Xp,2003: High Level

Windows Vista,7,2008: Next Generation

ACPI(Advance Confuragation Power Interface):

یکی از ویژگی های مادربرد است که مکمل ویژگیPNP می باشد،در واقع کار اصلی ACPI این است که زمانی که ویندوز درایور سخت افزاری را پیدا نکند آن سخت افزار را بصورت استاندارد بالا می آورد.

- ACPI را می توان از Bios سیستم فعال یا غیر فعال کرد.
- در هنگام نصب ویندوز اگر با صفحه آبی (Blue Page ) برخورد کردیم یکی از راه حل ها، غیر فعال کردن ACPI است.

انواع نسخه های سیستم عامل های NG :

- STARTER
- HOME BASIC
- HOME PREMIURE
- BUSINES
- INTERPRISE
- ULTIMATE

تفاوت بین Work Group وDomain در مدیریت متمرکز (Centralized Management ) است.

FarshidAjabnoush

- سرویسی که مشخص می کند شبکه Work Group است یا Domain سرویس Active Directory است.

Member Server :

به سرورهایی که داخل شبکه Domain هستند ولی سرویس Active Directory ندارند را Member Server گویند،مانندPrint Server, File Server و..

Stand Alone :

به سرورهایی که داخل شبکه Work Group هستند گویند.

- Domain Controller) DC )
- Product Key : پسوردی برای نصب نرم افزار است
- License Key: پسوردی برای اجازه آپدیت کردن نرم افزار است

IP(Internet Protocol):

هردستگاهی (Host )که بخواهد با شبکه ارتباط بر قرار کند احتیاج به یک عدد 32 بیتی منحصر به فرد(Unique ) به نام Ip دارد.

- یک Host در درون شبکه با Ip یا Mac Address شناسایی می شود.

Mac Address :

یک عدد 48 بیتی منحصر به فرد(Unique ) برای کارتهای شبکه(NIC ) است.

- اساس کار روتر(Router ) بر اساس Ip است و اساس کار سوئیچ(Switch )بر اساس Mac است.

پروتکلARP (Address Resolution Protocol ):

این پروتکل وظیفه تبدیل Ip به Mac را بر عهده دارد.

FarshidAjabnoush

Arp Cash :

روی تمامی سیستم های شبکه حافظه ای وجود دارد که کار آن نگهداری تمامی Mac Address دستگاهها است، وجود این حافظه باعث بالا رفتن سرعت ارتباط بین کامپیوترهای درون شبکه می شود.

برای دیدن این حافظه از دستور Arp –a استفاده می کنیم:

برای پاک کردن این حافظه از دستور Arp –d استفاده می کنیم:

FarshidAghajoush

برای اضافه کردن دستی به این حافظه از دستور Arp –s ip:... Mac:... استفاده می کنیم:

```
C:\Documents and Settings\Farshid>arp -s 192.168.1.105 00-0c-29-84-bb-1d
```

برای دیدن ip وMac هر دستگاه از دستورIpconfig /all استفاده می کنیم:

```
C:\Documents and Settings\Farshid>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : farshidpc
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter

        Physical Address. . . . . . . . . : 00-0C-29-84-BB-1D
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.105
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
```

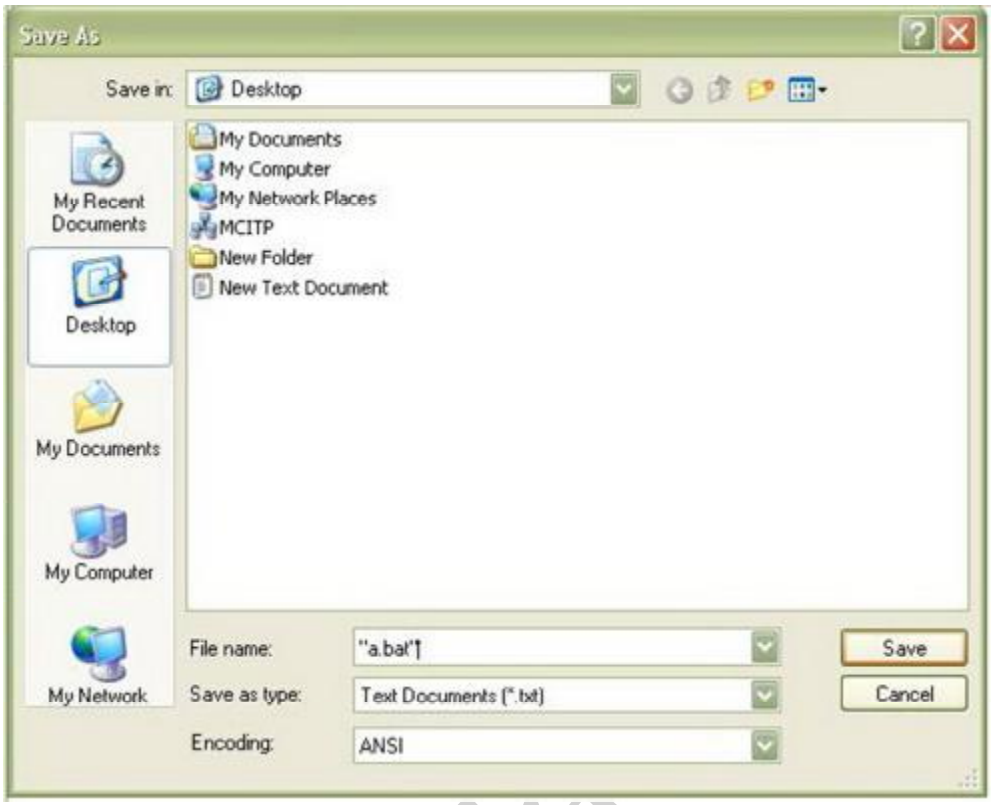
در اینجا منظور از Physical Address همانMac Address است.

Farshidnoush

طرز ساخت فایلهای دسته ای(Batch File ):

- در ابتدا یک فایل Note pad را باز کرده و بصورت زیر شروع به نوشتن می کنیم:

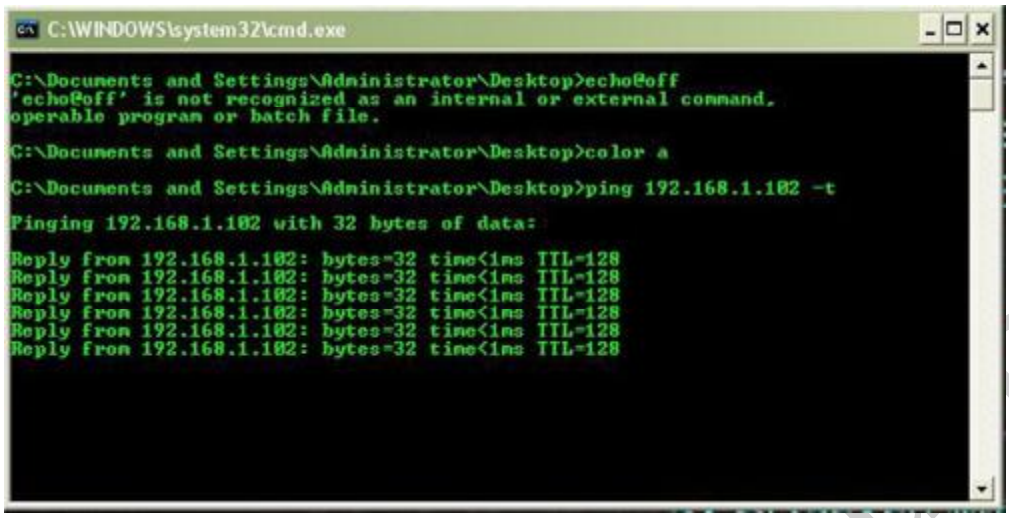
Farshidr...sh




برای ذخیره کردن فایل، اسم وپسوند فایل را داخل دابل کوتیشن قرار می دهیم،این کار به این دلیل انجام می شود که فایل مورد نظر با پسوند که گفته می شود ذخیره شود،سپس فایل مورد نظر به صورت زیر نمایان می شود:

پس از اجرا کردن Batch File (آیکونa) صفحه Ping به صورت زیر نمایان می شود

FarshidAja




- به خاطر داشته باشیم که هنگام ذخیره سازی فایل آن را با پسوندBat. ذخیره کنیم.

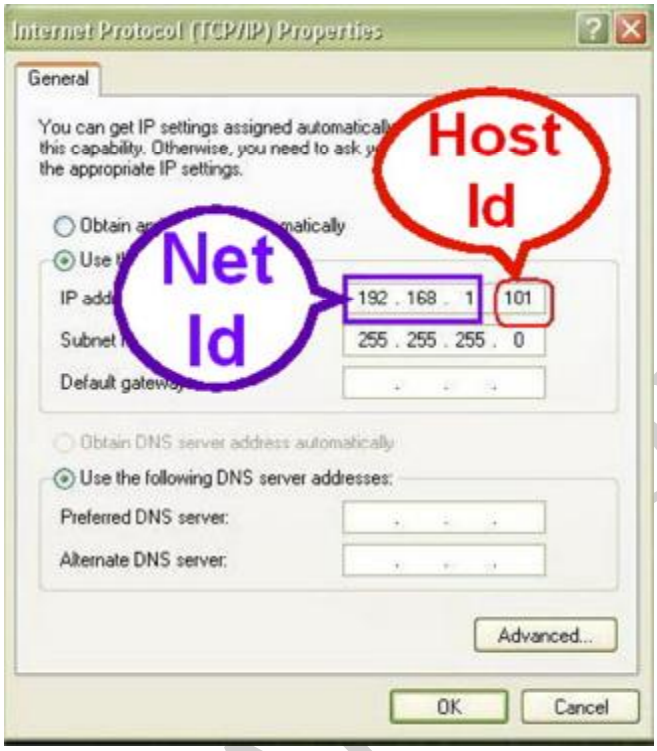
Net Id :

به قسمتی از Ip که در تمامی دستگاه های یک شبکه ثابت هستند گویند.

Host Id :

به قسمتی ازIp که برای هر دستگاه منحصر به فرد می باشد،این قسمت از Ip قابل تغییر می باشد.

FarshidAjabnoon




FarshidAjoush

کلاس IP :

Ip ها به 5 کلاس تقسیم بندی می شوند:

A. از 1 تا 126 (127 Loop Back = )
B. از 128 تا 191
C. از 192 تا 223
D. از 224 تا 238
E. از 239 تا 254

از کلاس D در Multi Cast(ارسال اطلاعات به چندین نقطه مانند ویدئو کنفرانس) استفاده می شود.

Subnet Mask (Net Mask ):

کار این قسمت جداسازی Net Id از Host Id است.

a) 255.0.0.0

b) 255.255.0.0

c) 255.255.255.0

به ازای هر 255 در Subnet یک قسمت از Ip ثابت است،به این صورت که اگر Subnet برابر 255.255.255.0 باشدو Ip به این صورت باشد 192.168.1.100 Host Id که قابل تغییر است میشود100 وNet Id که غیر قابل تغییر است می شود192.168.1

Ip ها به دو ورژن تقسیم می شوند :

1) Ip های ورژن4

2) Ip های ورژن6

Ip ورژن6:

Ip هایی که در آینده نزدیک از آنها استفاده خواهیم کرد از این رنج هستند،این رنج از Ip در ویندوز7 وجود دارد.

Ip ورژن4 :

Ip هایی که در حال حاظر از آنها استفاده می کنیم از این رنج هستند و به دو دسته:

Public (Valid-Register )

Private ( In valid-Un register )

تقسیم می شوند.

FarshidAjabnoush

Public (عمومی):

Ip های موجود بر روی شبکه اینترنت از این دسته هستند.

Private ( خصوصی):

Ip های موجود بر روی شبکه های خصوصی از این دسته هستند،این دسته از Ip ها قابل مشاهده بر روی اینترنت نیستند.

رنج Ip های Private:

a) ۱۰.۰.۰.۰ c) ۱۷۲.۱۶.۰.۰ e) ۱۹۲.۱۶۸.۰.۰
b) ۱۰.۲۵۵.۲۵۵.۲۵۵ d) ۱۷۲.۳۹.۲۵۵.۲۵۵ f)۱۹۲.۱۶۸.۲۵۵.۲۵۵

- Ip هایی که در یک رنج هستند توسط سوئیچ به هم وصل می شوند و Ip هایی که در رنج های متفاوتی هستند توسط روتر به هم وصل می شوند.

Ip های Private توسط Admin شبکه تنظیم می شود ولی Ip های Public را باید از ISP خریداری کرد،خودISP از مخابرات تهیه می کند و مخابرات هم از سازمان IANA خریداری می کند.

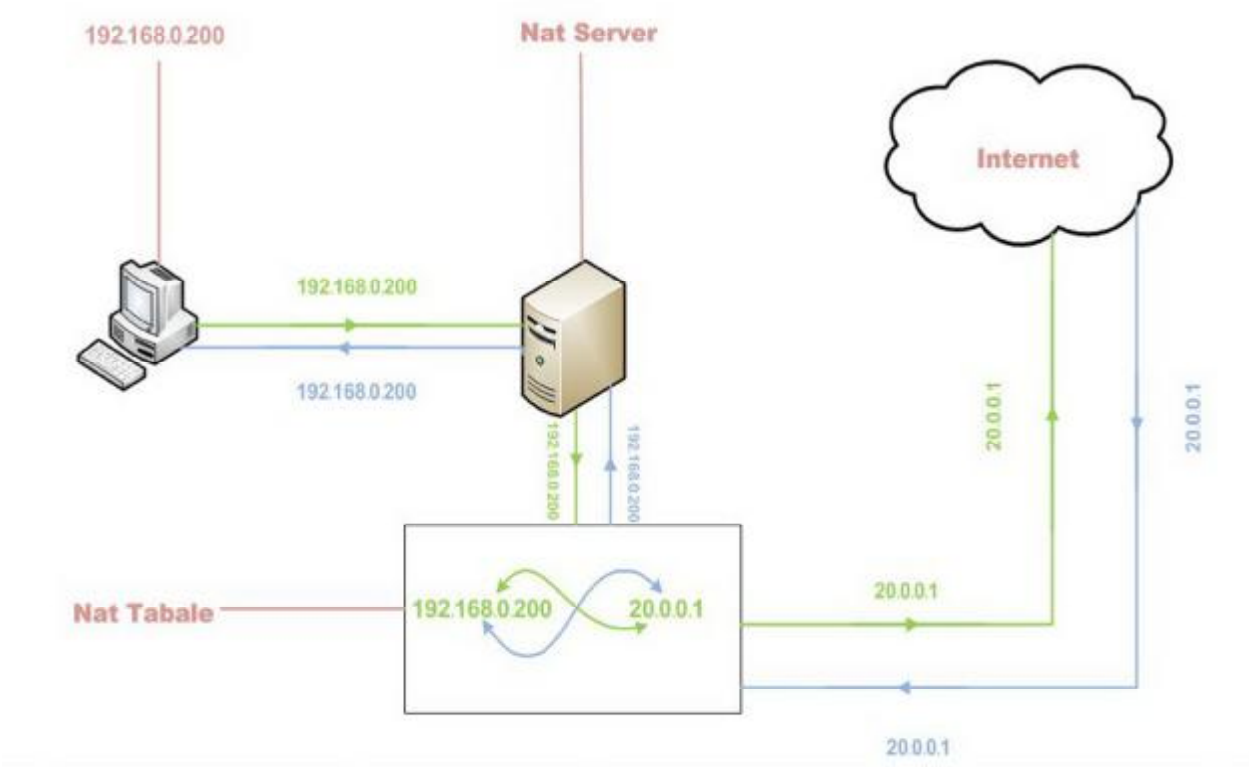
- IANA : سازمان جهانی نظارت بر IP
- I CAN : سازمان جهانی نظارت بر اسامی سایت ها
- ARPANET : سازمانی در آمریکا که کل اینترنت دنیا در دست این سازمان است

Nat (Network Address Translate )

یکی از راههای بردن Ip Private بر روی اینترنت استفاده از سرور Nat است.

طرز کار این سرور به این شکل است که هنگام اتصال شما به اینترنت،Ip شما را گرفته و یک Ip دیگر به شما می دهد وشما به روی اینترنت می روید این Ip ها در جدولی به نام Nat Table ذخیره می شود به این معنی که در زمان برگشت Ip که سروربه شما داده بود را پس گرفته وIp خودتان را به شما بر می گرداند.

FarshidAjabnoush




- در این روش فیلترینگ وجود ندارد.

انواع Nat :

1. Static Nat
2. Dynamic Nat
3. Pat(Port Address Translations)

FarshidAj

Static Nat :

به این صورت است که به ازای هر کامپیوتری که پشت Nat سرورمنتظر است یک Ip در طرف دیگر سرور رزرو شده است.

Dynamic Nat :

در این روش ما تعدادی محدودی Ip داریم(فرض بر اینکه ما 10 Ip داریم) به ازای هر کامپیوتر که درخواست Ip می کند یک Ip بصورت Random در اختیارش گذاشته می شود زمانی که کامپیوتر 11 بیاید باید صبر کند تا یکی از آن 10 کامپیوتر برگردد در نتیجه یک Ip خالی می شود و کامپیوتر 11 می تواند از آن Ip استفاده کند.

Pat:

این روش همانند روش Dynamic است ولی با این تفاوت که اگر کامپیوتر11 وارد شود وIp خالی نداشته باشیم دیگر احتیاج به صبر کردن برای خالی شدن Ip را نداریم،به این صورت که هر Ip که دانلود آن کمتر از بقیه باشد کامپیوتر 11 را روی آنIp قرار می گیرد یعنی به صورت مشترک از یک Ip استفاده می شود.

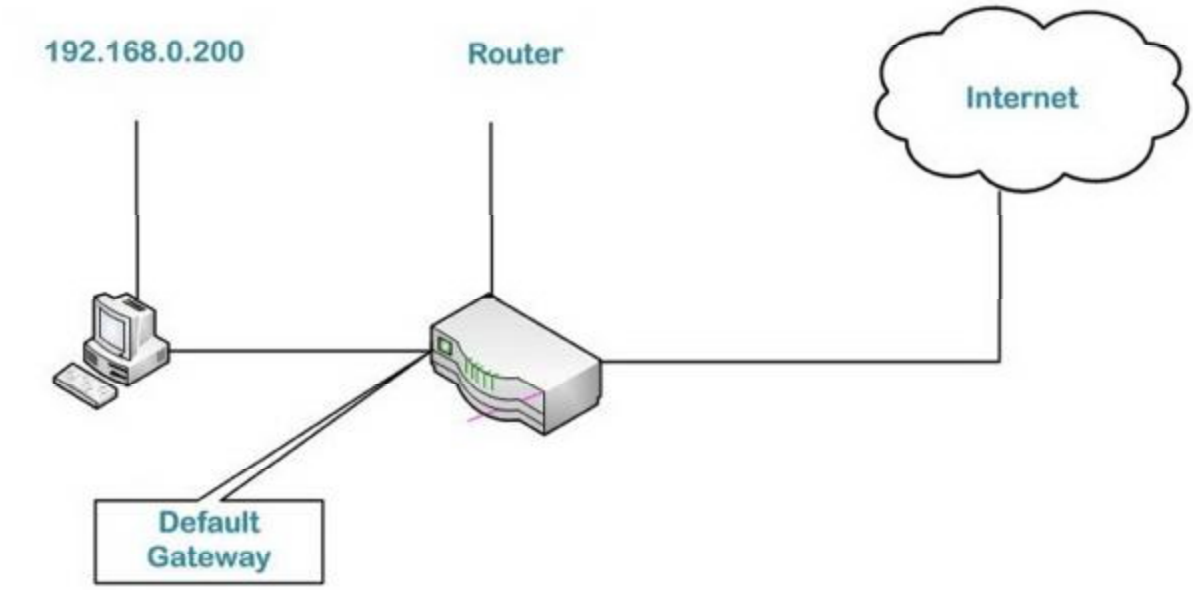
Proxy Server:

در پروکسی سرور ما هیچ وقت روی اینترنت نمی رویم به این معنی که وقتی ما آدرس سایتی را وارد می کنیم پروکسی سرور آدرس را از ما گرفته و ما را پشت سرور نگاه می دارد و خودش آن آدرس را چک کرده واگر مجاز باشد آن را برای ما می آورد و اگر مجاز نباشد صفحه معروفی را به ما نشان می دهد که در آن نوشته شده: دسترسی به تارنمای خوانده شده مجاز نمی باشد،در این روش فیلترینگ داریم.

FarshidAjabnoush

Default Gateway:

**به ورودی رتور از سمت ما** Default Gateway **گویند.**



DNS (Domain Name Server ):

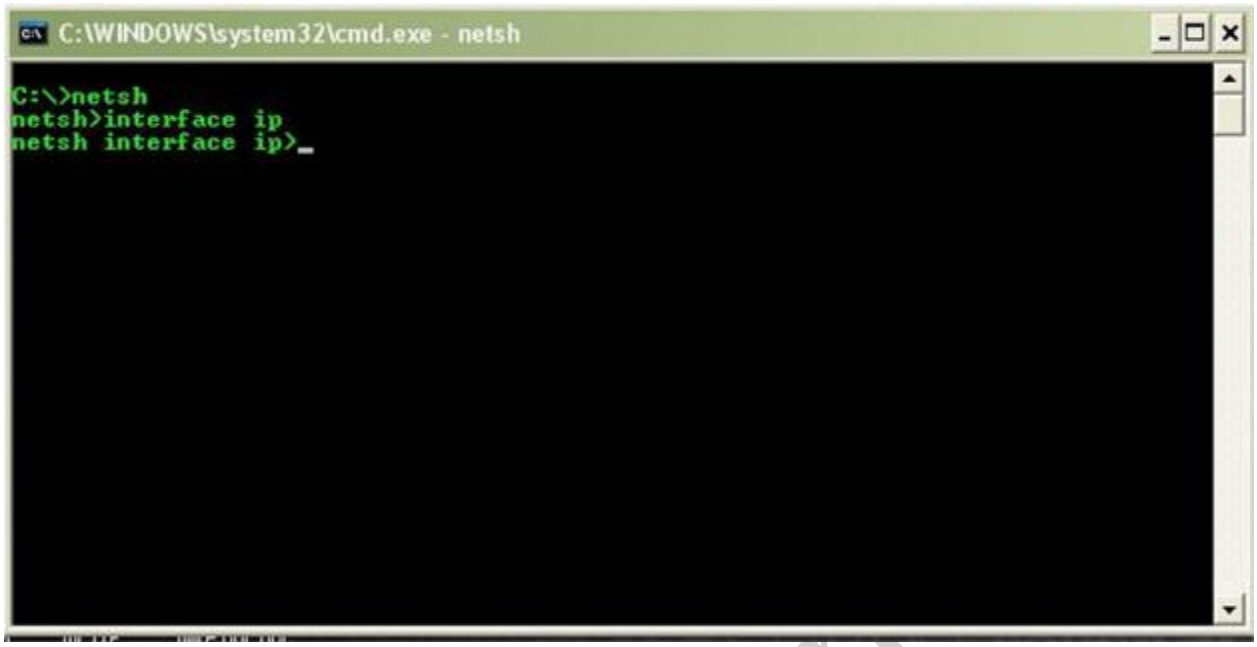
وظیفه تبدیل اسم به آی پی و آی پی به اسم را دارد.

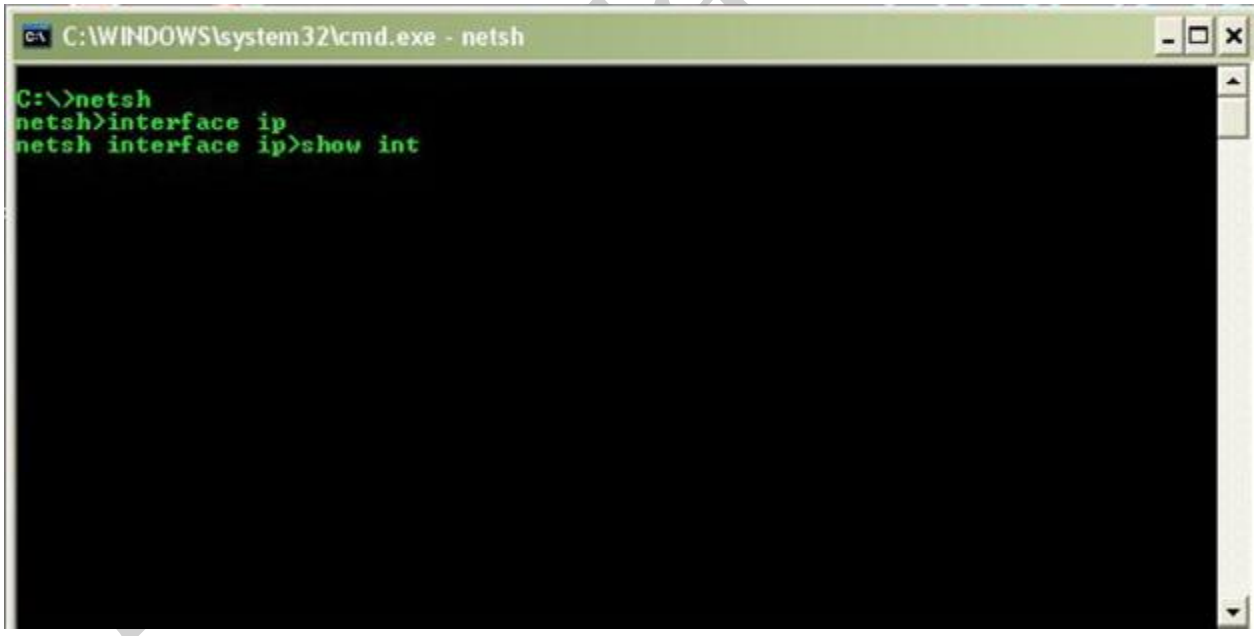
DNS های بین المللی:

4.2.2.4 8.8.8.8 85.15.1.10 85.15.1.12

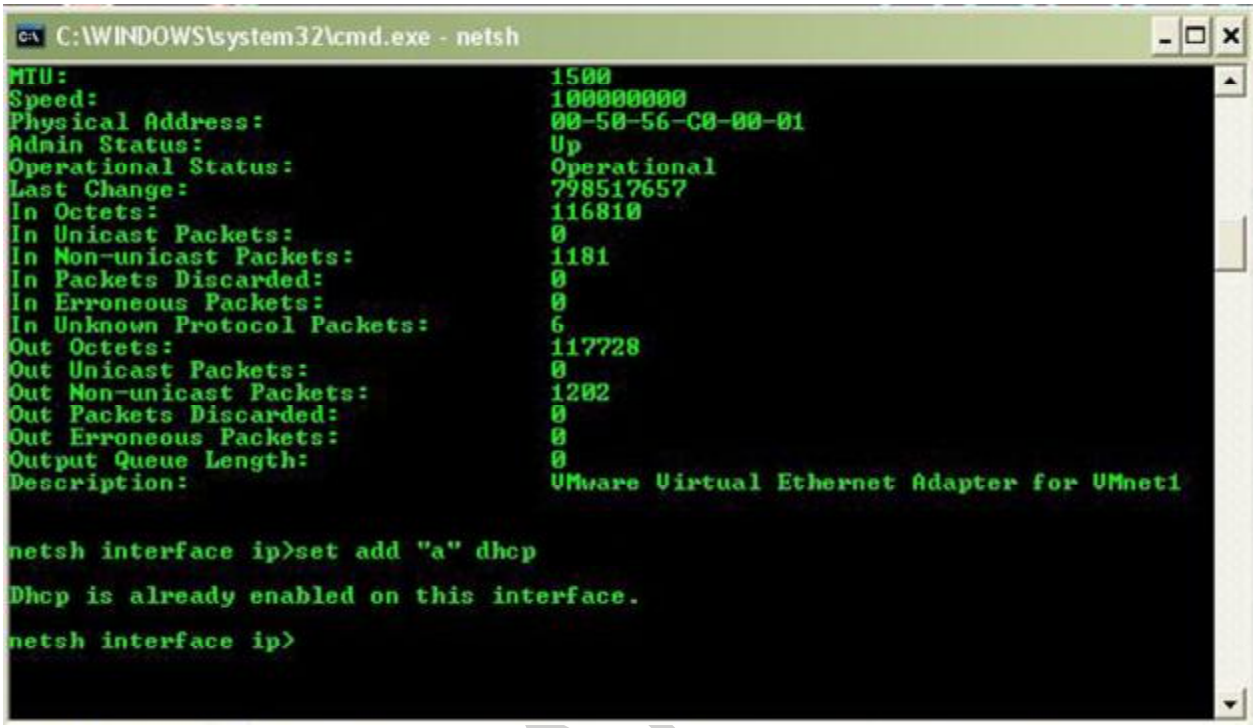
انجام تنظیمات TCP/IP با Command:

بعد از باز کردن Command اول دستور Netsh را تایپ می کنیم سپس Interface ip وShow int


C:\WINDOWS\system32\cmd.exe - netsh
C:\>netsh
netsh>interface ip
netsh interface ip>


C:\WINDOWS\system32\cmd.exe - netsh
C:\>netsh
netsh>interface ip
netsh interface ip>show int

در این مرحله برای خالی کردن Ip های کارت شبکه از دستورSet add "a" dhcpاستفاده می کنیم ، بخاطر داشته باشید که باید داخل دابل کوتیشن اسم کانکشن شبکه را بنویسیم ما آن را به A تغییر دادیم.




سپس برای تنظیم کردن Ip از دستورset add "a" static

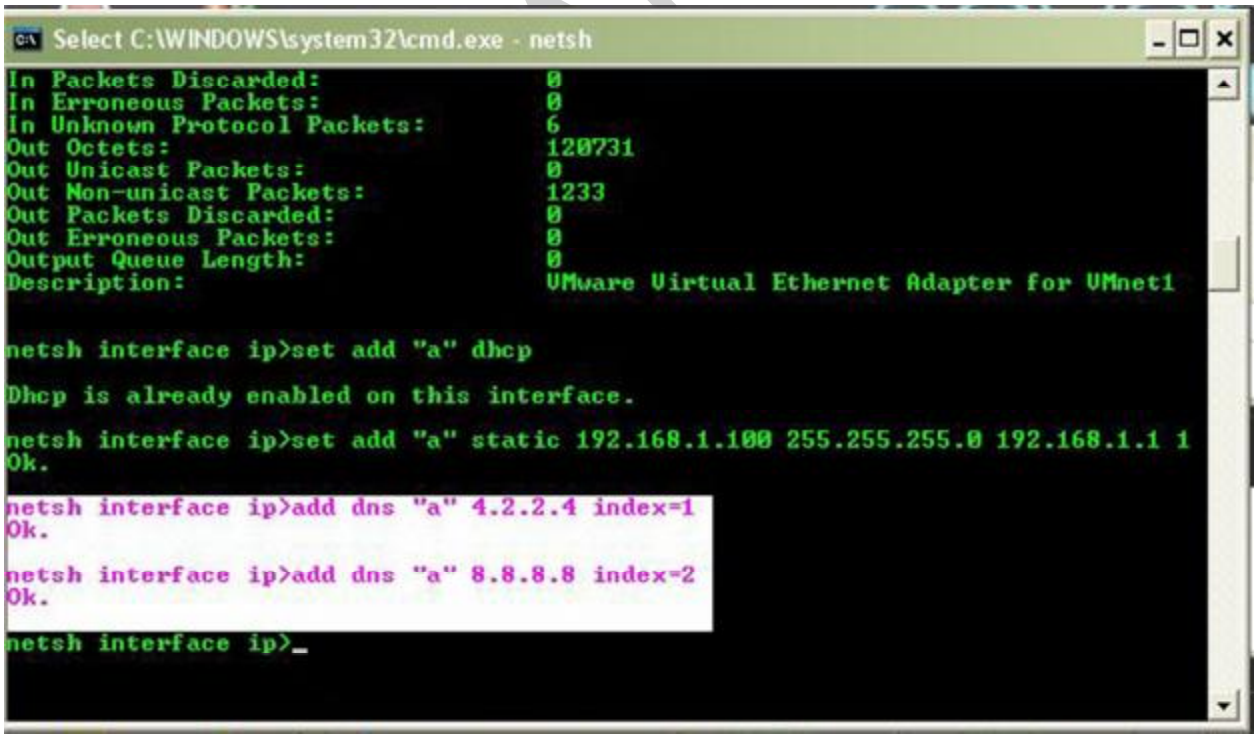
همانطور که در شکل میبینید ادامه دستور به ترتیب اول Ip بعد Subnet و در آخرهم Gateway را وارد می کنیم،در آخر هم اولویت کارت شبکه را وارد می کنیم که 1 است.

بعد از تنظیمات Ip وSubnet و Gateway نوبت به DNS می رسد.

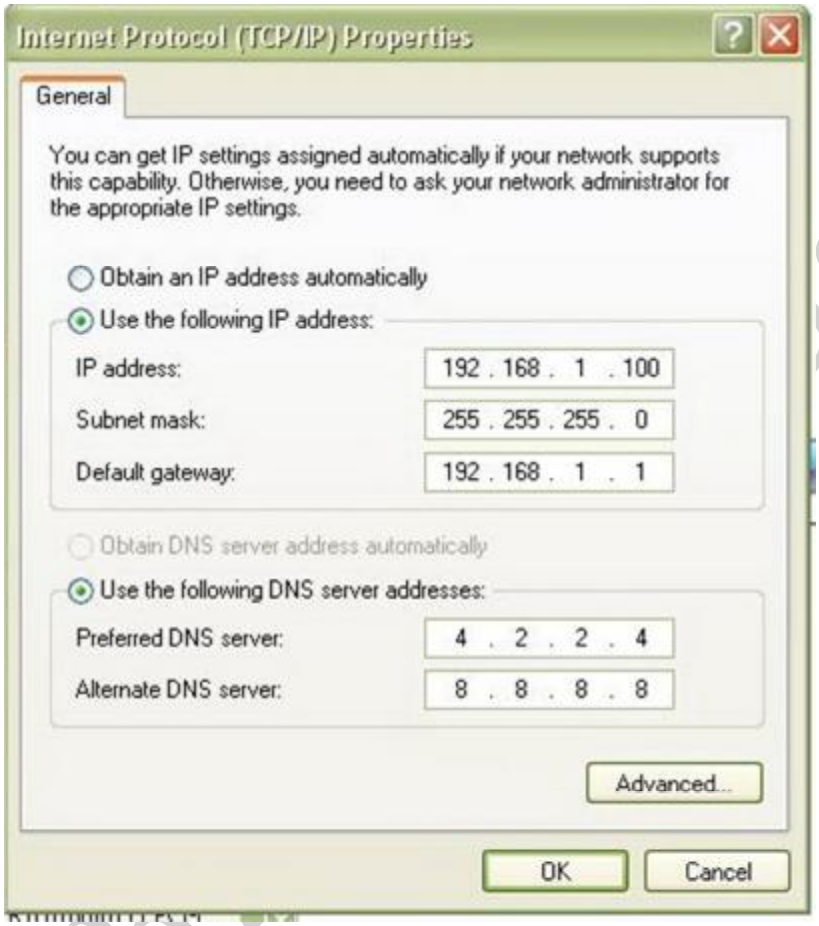
برای تنظیم DNS در ویندوزهای Legacyاز دستور add dns "a" index=1

add dns "a" index=2

در جای خالی بین دستورها Dns را وارد می کنیم Index هم برای این است که Index=1برای فیلد اول Dns وIndex=2 برای فیلد دوم است.



و در آخر تنظیمات به صورت زیر می شود:



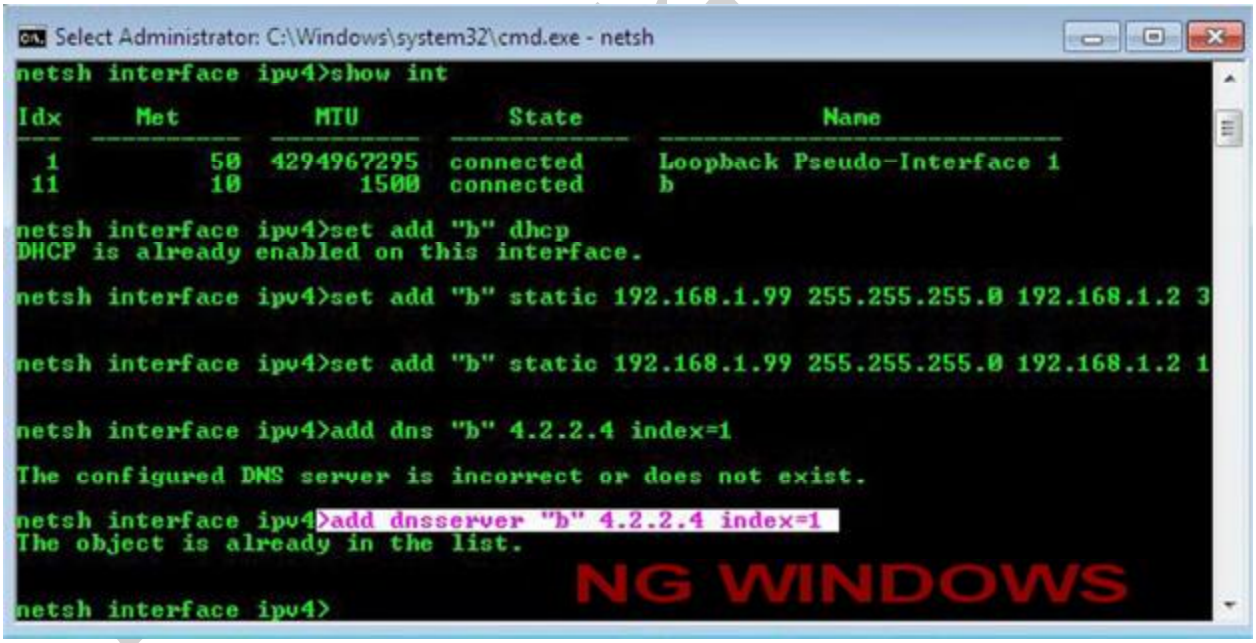

در ویندوزهای NG تمامی دستورات همانند دستورات در ویندوز Legacy است فقط دستور DNS تفاوت دارد که آن هم بصورت زیر است:

Add dnsserver "a" index=1

Add dnsserver "a" index=2

Farshash

Administrator: C:\Windows\system32\cmd.exe - netsh
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Farshid7.Farshid7-PC>color b
C:\Users\Farshid7.Farshid7-PC>color a
C:\Users\Farshid7.Farshid7-PC>netsh
netsh>interface ip
netsh interface ipv4>show int
Idx Met MTU State Name
1 50 4294967295 connected Loopback Pseudo-Interface 1
11 10 1500 connected b
netsh interface ipv4>set add "b" dhcp
DHCP is already enabled on this interface.
netsh interface ipv4>
NG WINDOWS


Select Administrator: C:\Windows\system32\cmd.exe - netsh
netsh interface ipv4>show int
Idx Met MTU State Name
1 50 4294967295 connected Loopback Pseudo-Interface 1
11 10 1500 connected b
netsh interface ipv4>set add "b" dhcp
DHCP is already enabled on this interface.
netsh interface ipv4>set add "b" static 192.168.1.99 255.255.255.0 192.168.1.2 3
netsh interface ipv4>set add "b" static 192.168.1.99 255.255.255.0 192.168.1.2 1
netsh interface ipv4>add dns "b" 4.2.2.4 index=1
The configured DNS server is incorrect or does not exist.
netsh interface ipv4>add dnsserver "b" 4.2.2.4 index=1
The object is already in the list.
netsh interface ipv4>
NG WINDOWS

آشنایی با System Properties در ویندوز7:

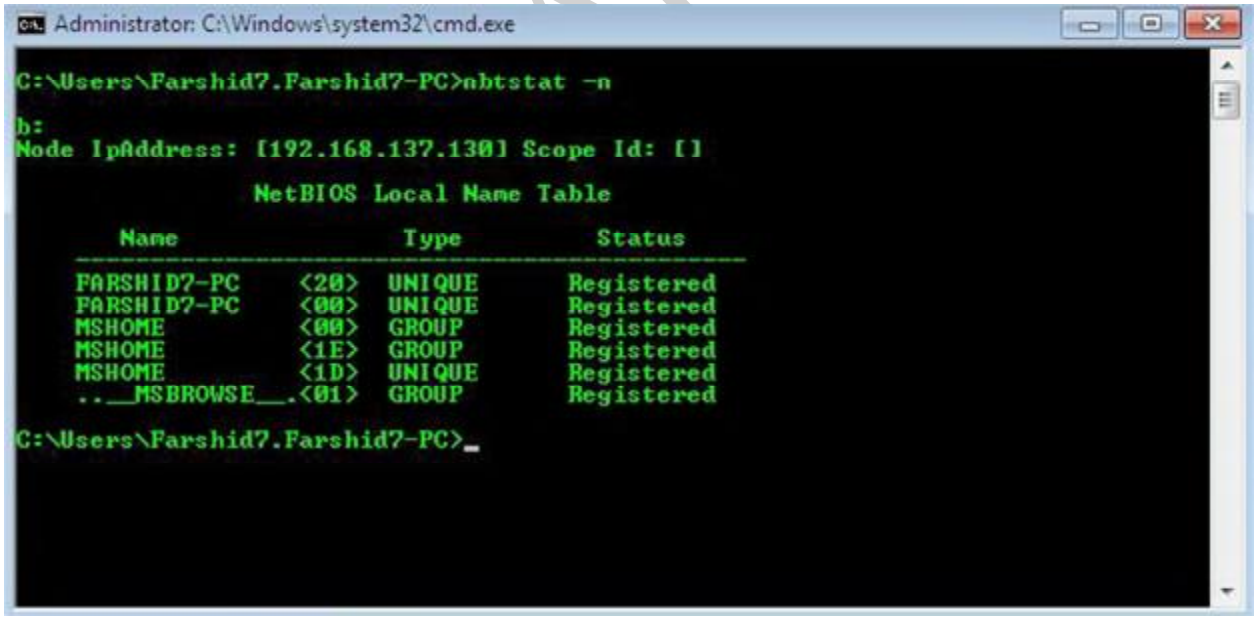
ابتدا بر روی Computer کلیک راست می کنیم سپس گزینه Properties را انتخاب می کنیم و در پنجره باز شده System Properties را باز کرده و از تب Computer Name گزینه Change را می زنیم تا بتوانیم اسم کامپیوتر را عوض کنیم.

سه نوع اسم برای کامپیوتر داریم: 1)Net Bios Name 2)Host Name 3)Domain Name

Net Bios Name:

این نوع اسم 15 کاراکتری است و در ویندوزهای Down Level 98 و سیستم عامل لینوکس کاربرد دارد.

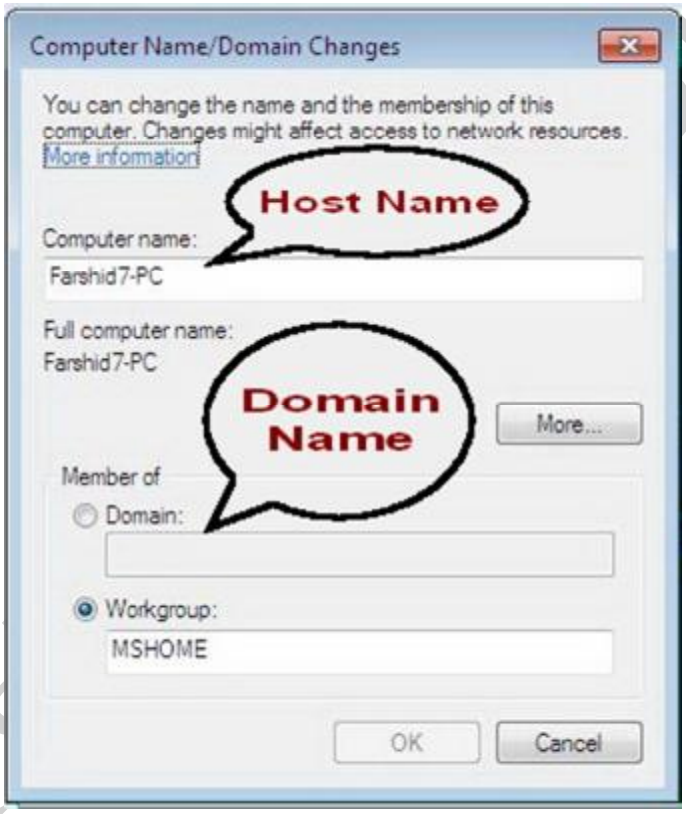
- اسمی که هنگام نصب ویندوز از ما سوال می شود از این دسته هستند
- برای دیدن این نوع اسم از دستور nbtstat –n استفاده می کنیم




Aiabnoush

: Host Name

**همان اسم کامپیوتر است که می توان از داخل ویندوز عوض کرد و در ویندوزهای High Level کاربرد دارد.**

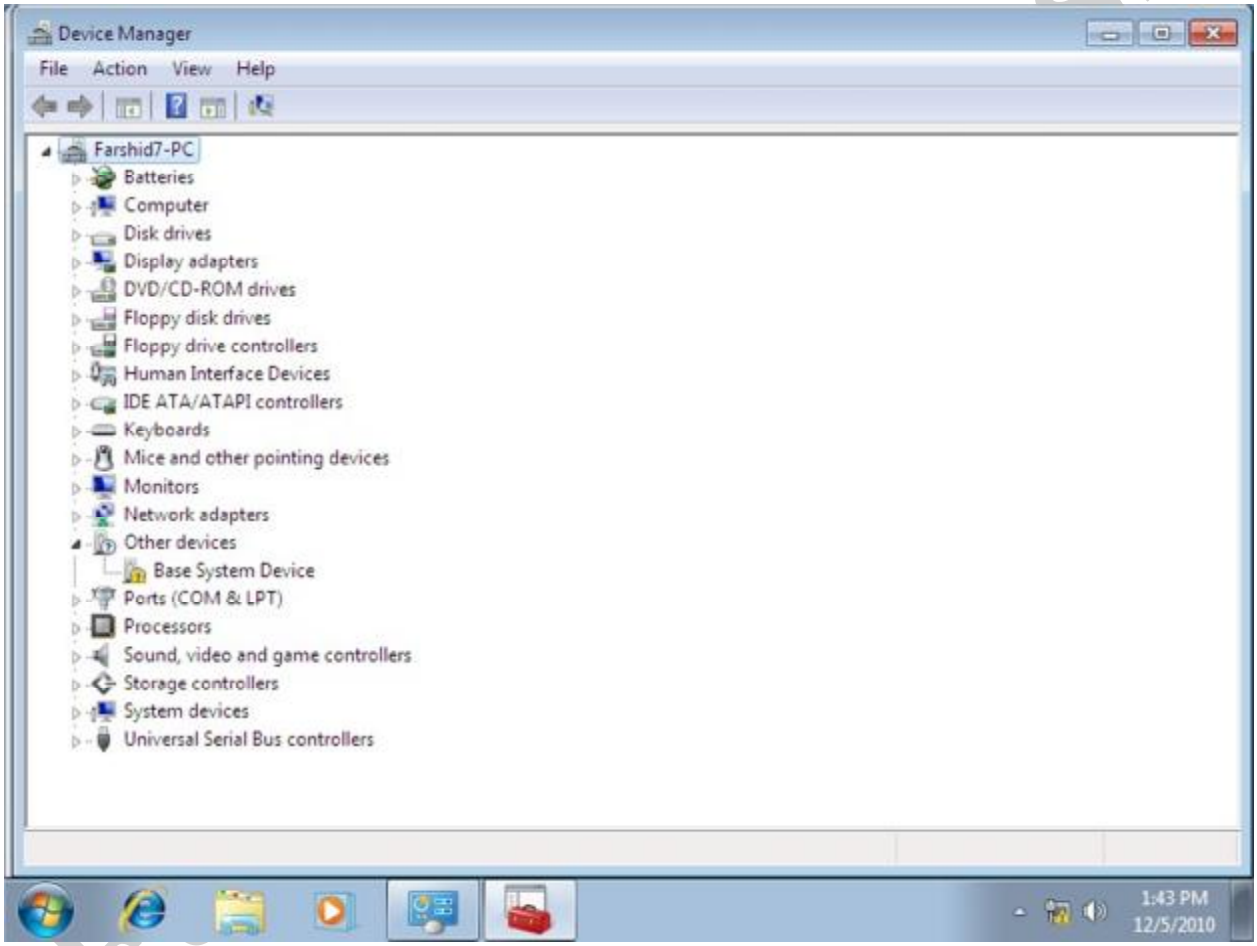


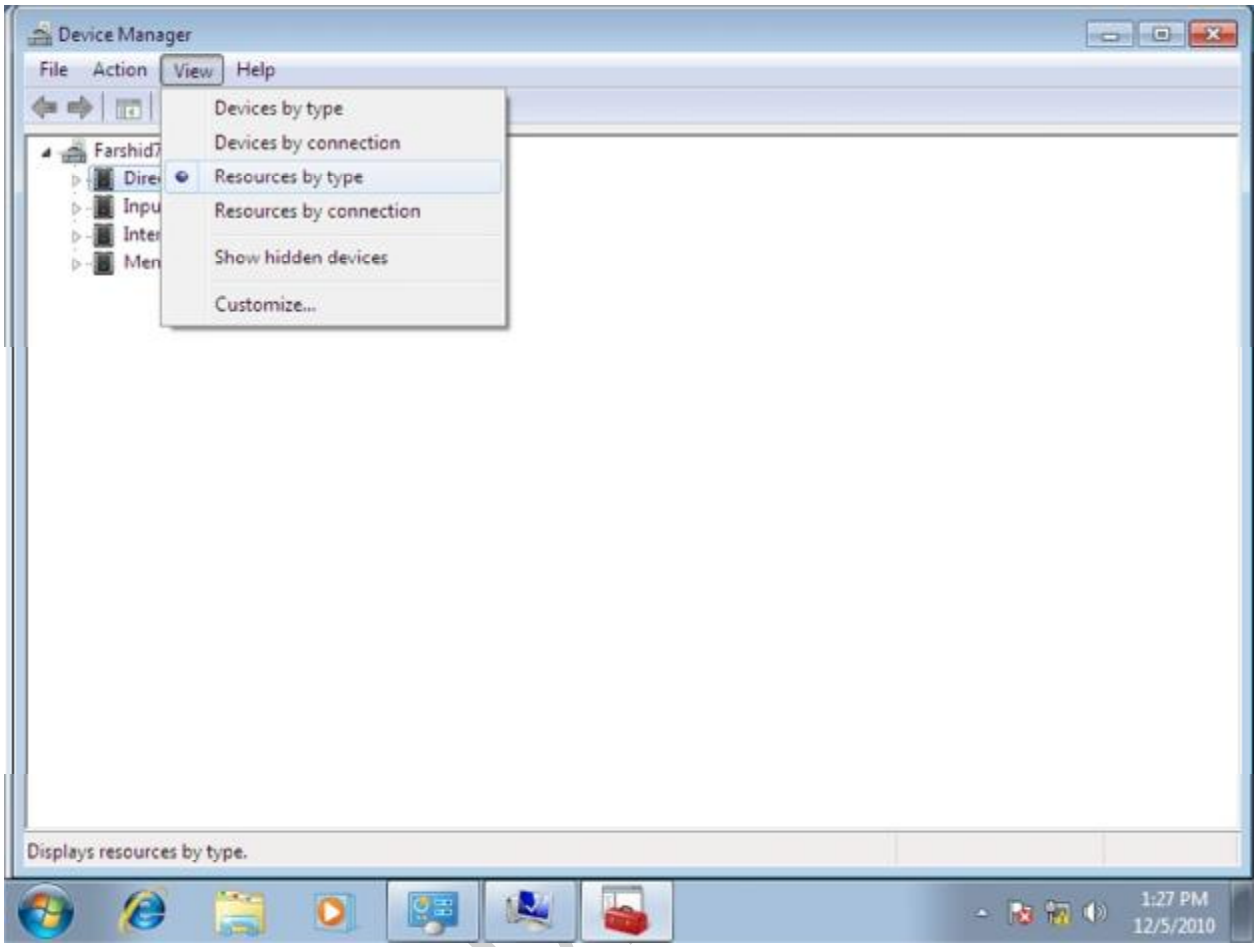

- **دستور NETSTAT -S پکت های ارسال شده و دریافت شده را در هر سیستم نشان می دهد**

Farshid Ghoush

**آشنایی با منابع سخت افزاری سیستم(Device Manager):**

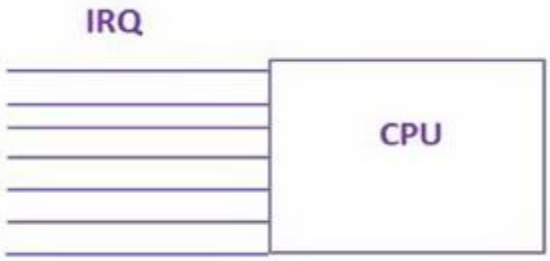
**اگر در Device Manager علامت بنفش رنگی را مشاهده کردیم آن برای Conflict IRQ است.**






(Interapt Request) IRQ:

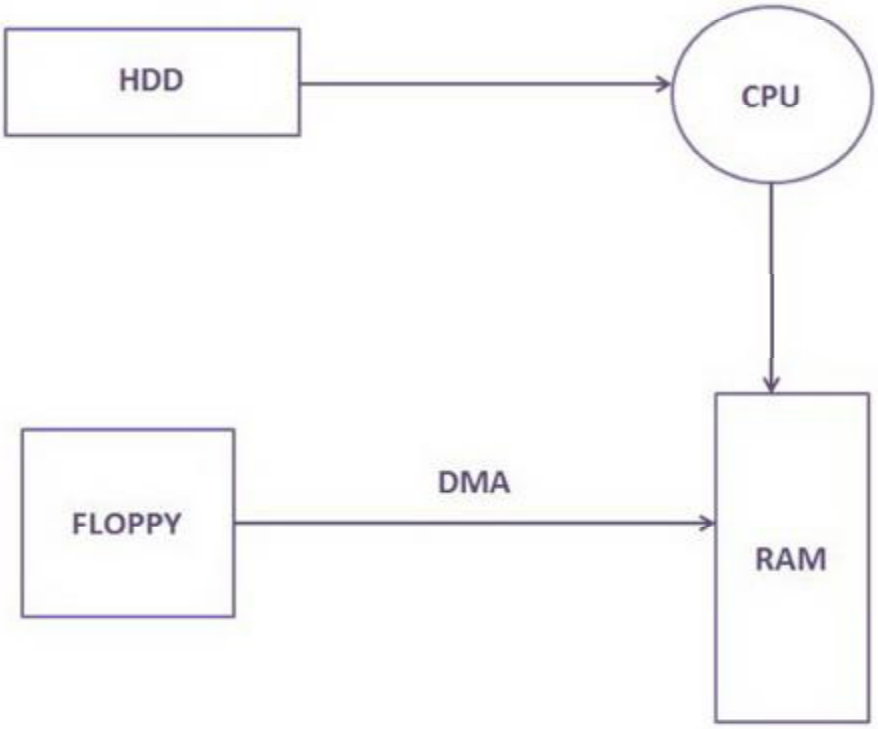
هر سخت افزار برای ارتباط با Cpu احتیج به یک مسیر دارد،به این شکل است که اگر کی برد با Cpu کار داشته باشد باید نخ شماره 1 تکان دهد تا Cpu متوجه شود،به این نخ ها IRQ گویند.از irq16 تاirq255 مربوط به نرم افزارها است. Irq0 برای خود cpu است.




Farshid

DMA (Direct Memory Access):

**هر سخت افزاری برای ارتباط بر قرار کردن با رم باید از CPU اجازه بگیرد در سخت افزار هایی که سرعت آنها پایین است مانند فلاپی دیگر نیاز به اجازه گرفتن نمی باشد و مستقیم می توانند با رم ارتباط برقرار کنند به این ارتباط مستقیم DMA گویند.**



درایورهای هر سخت افزار 2 کار را انجام می دهند: 1) زبان سخت افزار مورد نظر را به بقیه سخت افزار ها می فهماند.

2)قسمتی از رم را برای کارهای آینده آن سخت افزار رزرو می کند(Buffer )

درایورها را با زبان اسمبلی می نویسند،پسوند تمامی درایورها SYS. است.

Buffer Over Flow:

یک نوع ویروس است،طرز کار آن به این صورت است که فضای خالی رم را پر می کند و در نهایت با این پیغام مواجه می شویم برای رهایی از این ویروس باید رم را توسط نرم افزارMEM TEST 86 فرمت کنیم ، اگر این کار هم جواب نداد باید ویندوز را عوض کنیم.

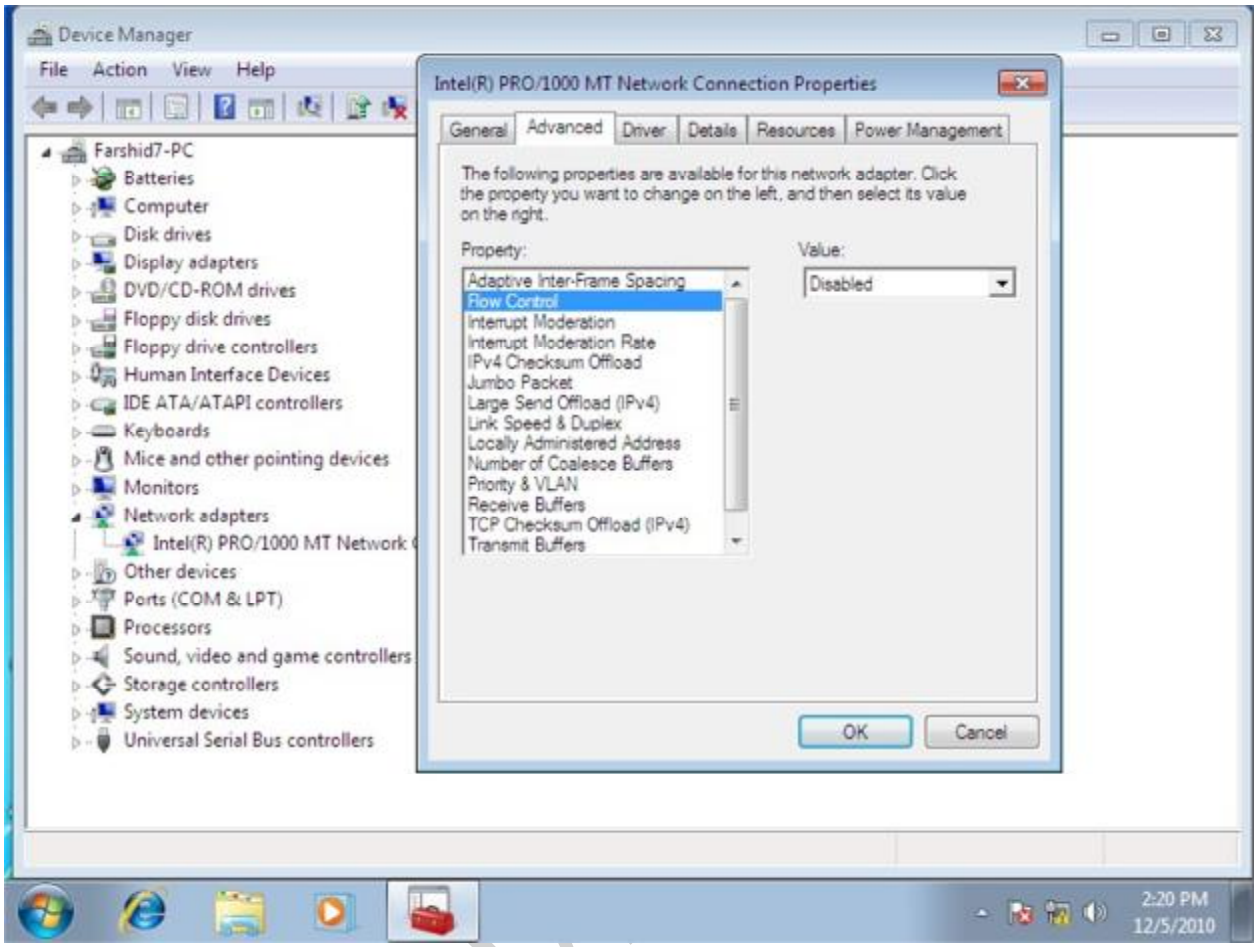
Heap:

مجموعه ای از مکانهای ذخیره بر روی رم که توسط یک برنامه می تواند جهت محاسبه به طور موقت گرفته شود و سپس برگرداند راHEAP گویند.:

- بهترین نرم افزار مانیتورینگ شبکه Solar Winds است.
- مشخصات دقیق سخت افزاری یک سیستم توسط نرم افزار Network Inventory مشخص می شود.

در لیست سخت افزاری روی کارت شبکه راست کلیک کرده و Properties گرفته وتبAdvance را انتخاب می کنیم

FarshidAjabnoush

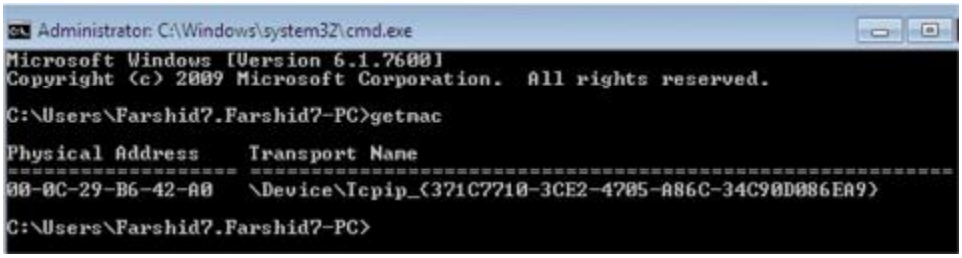



در قسمت آبی رنگ گزینه هایی داریم.

Flow Control: کنترل سرعت دریافت و ارسال اطلاعات آن سخت افزار.

Locally Administered Address: تغییر دادن شناسه Mac Address.

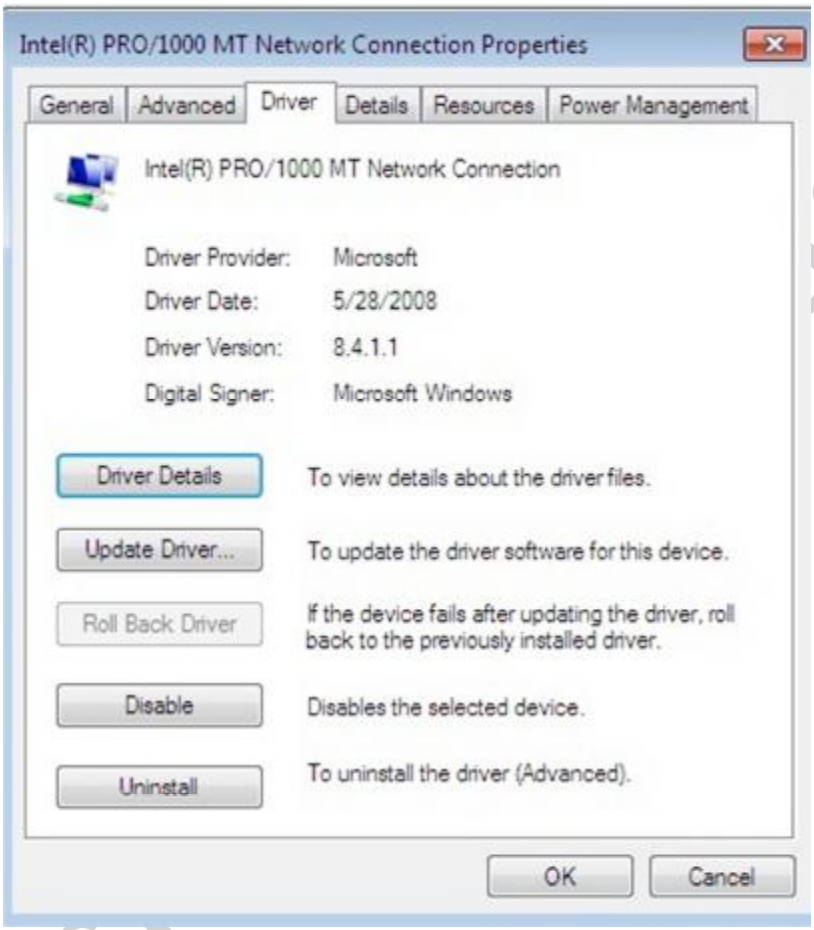
برای دیدن Mac Address از دستور GetMac استفاده می کنیم




برای جعل کردن Mac Address از نرم افزار Smac وبرای جعل کردنIp از نرم افزار N map استفاده می کنیم.

: Roll Back Driver

**اگر درایور سخت افزاری را بروز کردیم و به هر دلیل سیستم بهم ریخت از این گزینه که استفاده کنیم درایور را به زمان قبل از بروز رسانی بر می گرداند.**



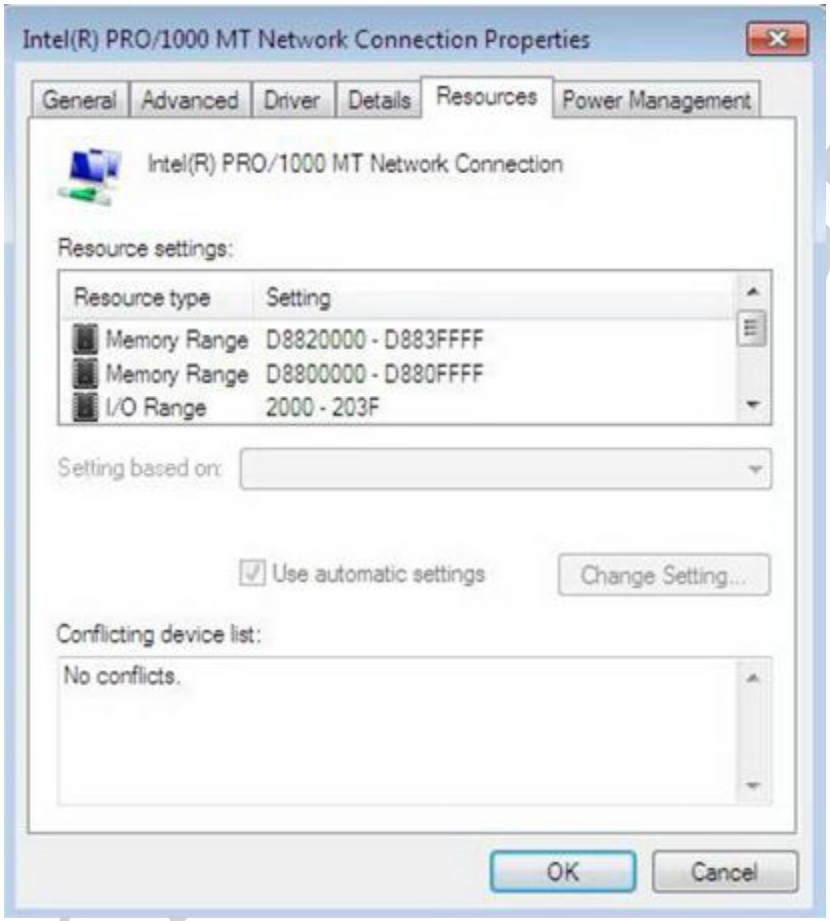

**درایورها به دودسته: 1)Singn که مورد تایید مایکروسافت می باشد 2) Unsingnکه مورد تایید نمی باشد تقسیم می شوند.**

**برای دیدن Unsingn از دستور Sigverif در گزینه Run استفاده می کنیم.**

Farsh

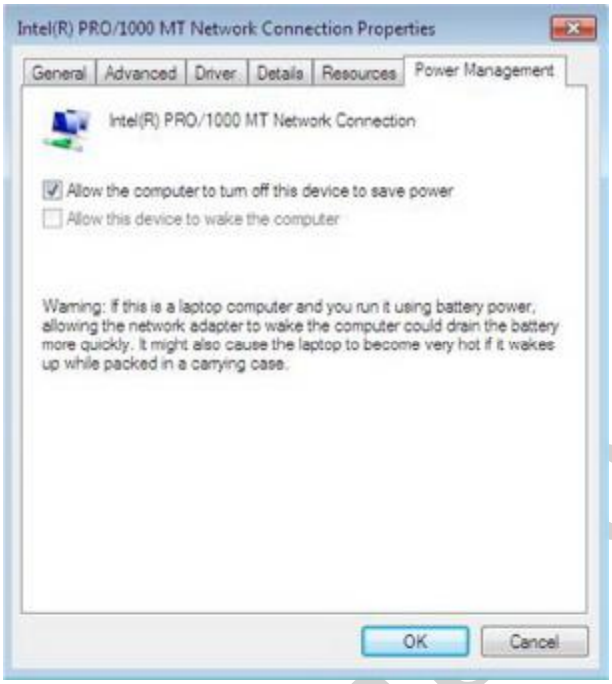
تب Resources :

**در این تب می توانیم ببینیم که سخت افزار مورد نظر با Irq تداخل(Conflict ) دارد یا نه**




Fars

در لپ تاپ ها برای استفاده بهینه از باتری گزینه زیر را فعال می کنیم:




برای روشن کردن یک کامپیوتر از راه دور توسط تکنولوژی Wake On Lan (WOL) از نرم افزار Solar Winds Wake On Lan استفاده می کنیم که توسط چند فرکانس که نام یکی از این فرکانس ها Sig-Wio می باشد استفاده می کند.

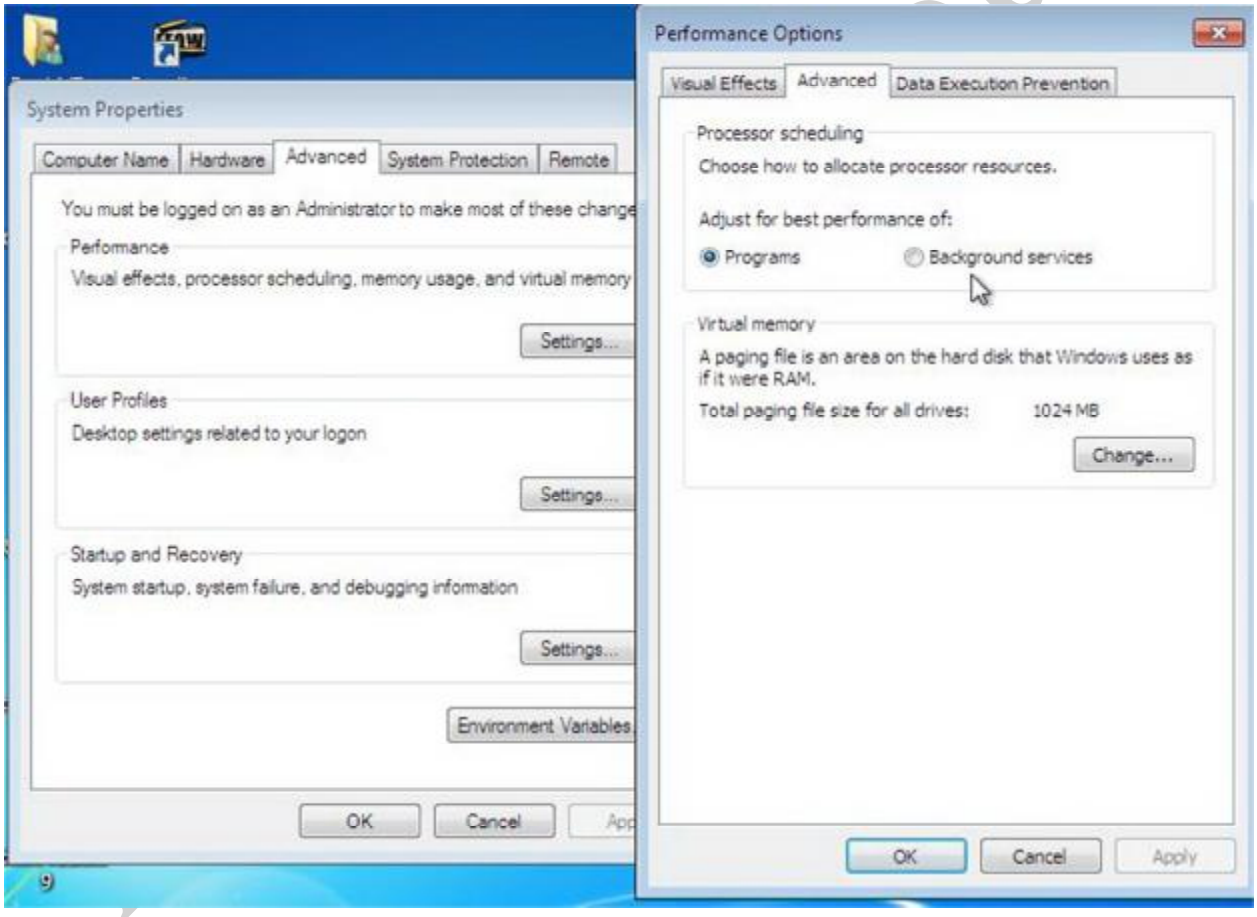
Rout Kit :

نرم افزاری برای مخفی نگاه داشتن ویروس از دید آنتی ویروس است

FarshidAjamoush

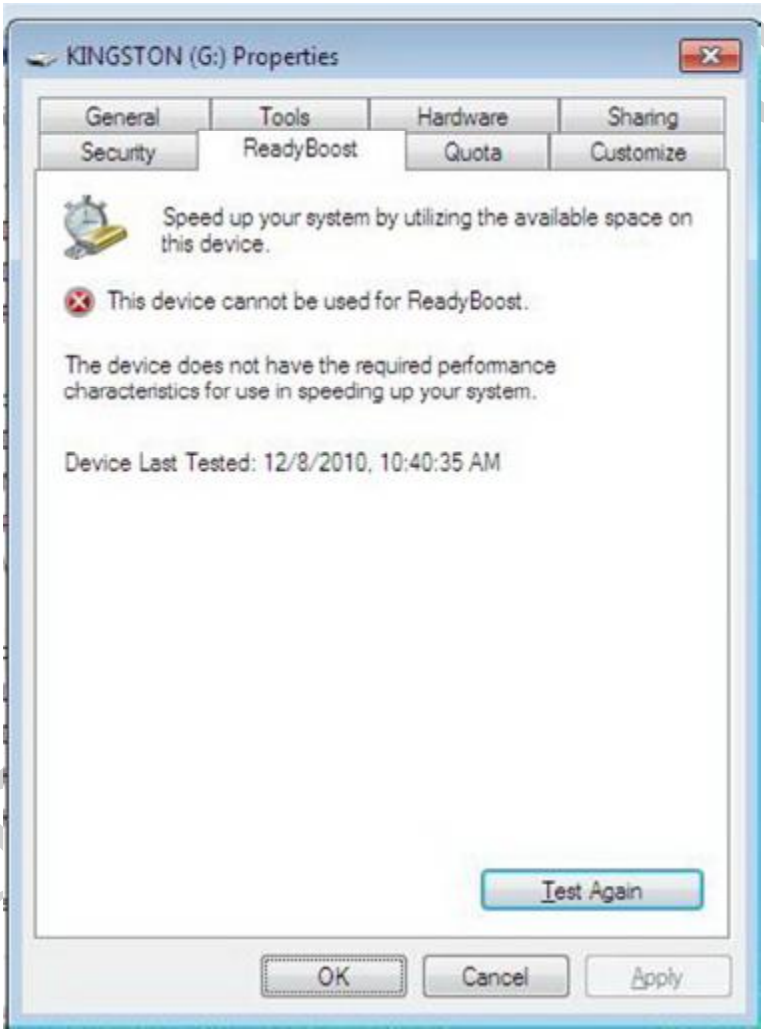
System Properties –Performance-Settings-Advance

**از مسیر بالا می توان سهم Cpu ( Threads) تغییر دهیم با انتخاب گزینهPrograms سهم بیشتر Cpu در اجرای برنامه هایی که کاربر اجرا می کند قرار می گیرد و با انتخاب گزینه ...Background سهم بیشتر Cpu در اجرای برنامه هایی که پشت پرده هستند صرف می شود.**



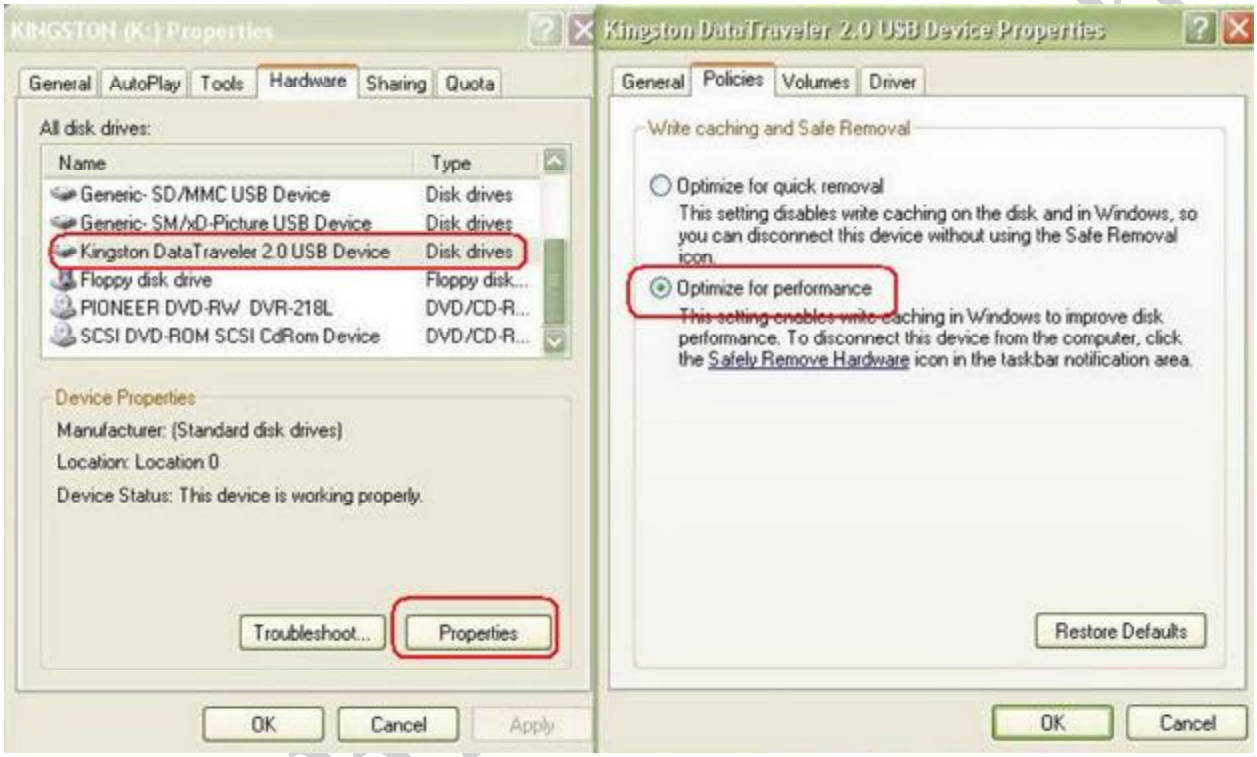
Ready Boost:

**در ویندوز7 قابلیتی  وجود دارد که توسط آن می توان یک فلش را به حافظه رم اضافه کرد.**

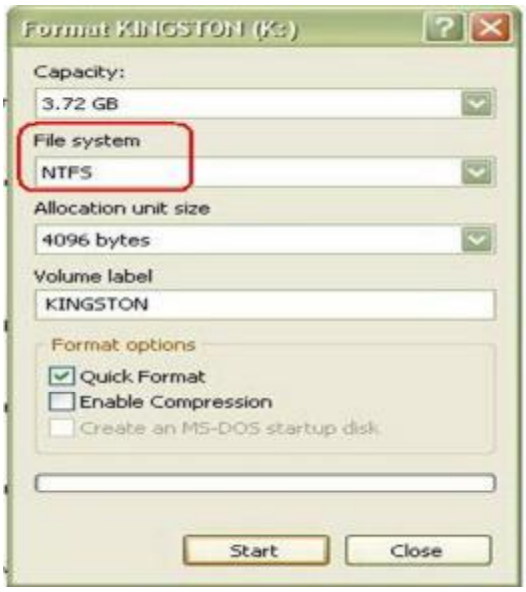



Farsh

فرمت کردن فلش با فایل سیستم NTFS در ویندوزXp :




Farsh



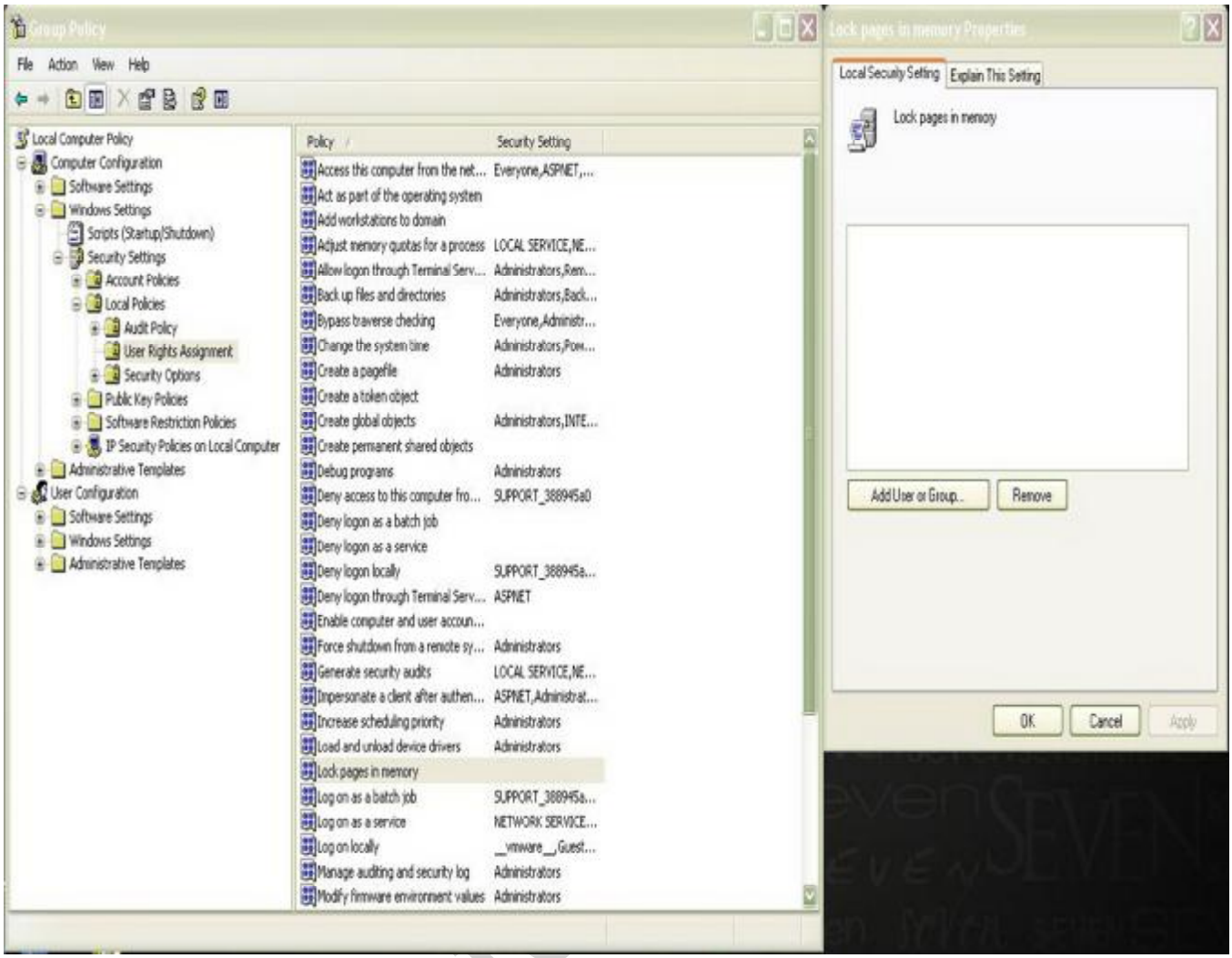

قفل کردن محتویات Pages File :

Run-gpedit.msc

Computer configuration-Windows setting-Security setting-Local policy-User rights assignment

-look page in memory

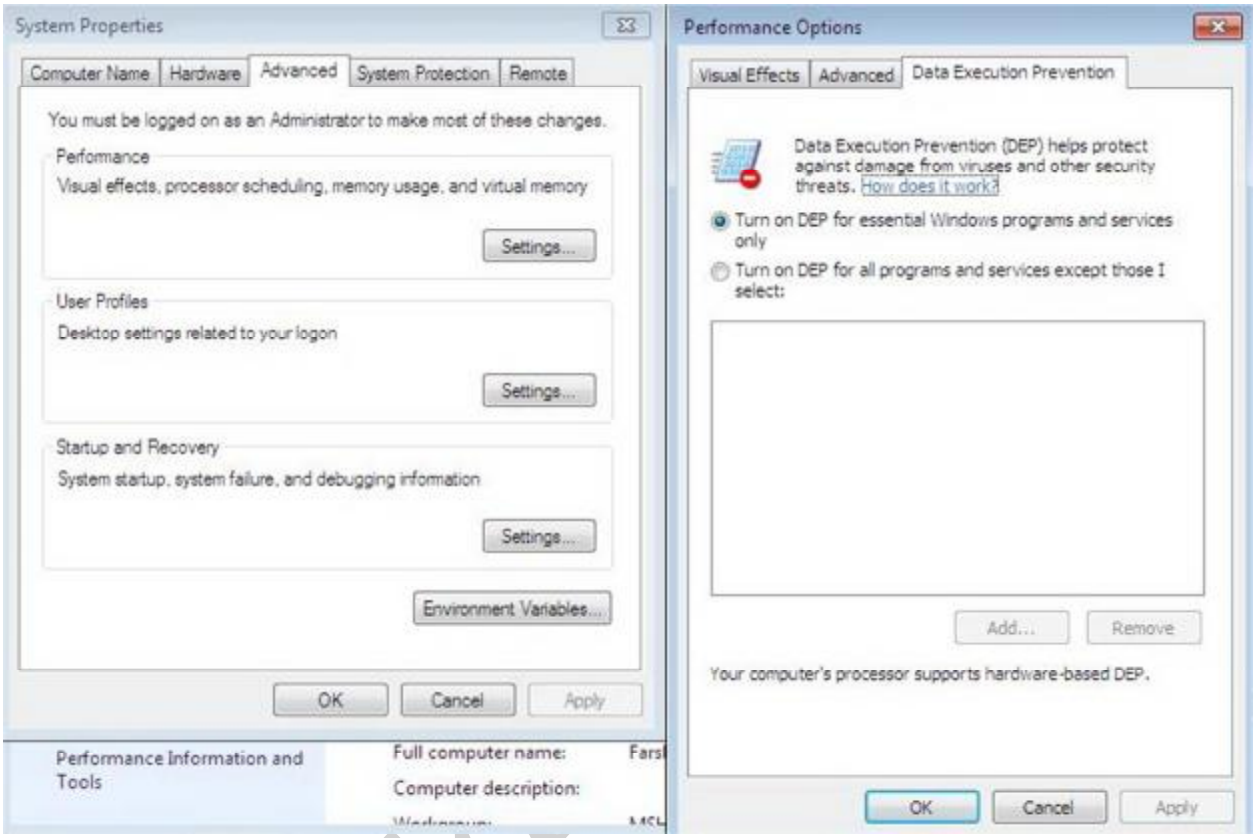
FarshidAjabnoush


Group Policy
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Public Key Policies
Software Restriction Policies
IP Security Policies on Local Computer
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Policy
Security Setting
Access this computer from the net... Everyone,ASPNET,...
Act as part of the operating system
Add workstations to domain
Adjust memory quotas for a process LOCAL SERVICE,NE...
Allow logon through Terminal Serv... Administrators,Rem...
Back up files and directories Administrators,Back...
Bypass traverse checking Everyone,Administr...
Change the system time Administrators,Pow...
Create a pagefile Administrators
Create a token object
Create global objects Administrators,INTE...
Create permanent shared objects
Debug programs Administrators
Deny access to this computer fro... SUPPORT_388945a0
Deny logon as a batch job
Deny logon as a service
Deny logon locally SUPPORT_388945a...
Deny logon through Terminal Serv... ASPNET
Enable computer and user accoun...
Force shutdown from a remote sy... Administrators
Generate security audits LOCAL SERVICE,NE...
Impersonate a client after authen... ASPNET,Administrat...
Increase scheduling priority Administrators
Load and unload device drivers Administrators
Lock pages in memory
Log on as a batch job SUPPORT_388945a...
Log on as a service NETWORK SERVICE...
Log on locally __vmware__,Guest...
Manage auditing and security log Administrators
Modify firmware environment values Administrators
Lock pages in memory Properties
Local Security Setting
Explain This Setting
Lock pages in memory
Add User or Group...
Remove
OK
Cancel
Apply

Farshi

: DEP

ویژگی است که باعث می شود Theard Cpu بیشتر از سهم نشود.




:Stegano

این روش برای مخفی کردن اطلاعاتی که بصورتTXT هستندبه کاربرد می رود،ابتدا یک Note pad در یکی از درایو ها (E ) به نام مثلا A می سازیم و در cmd این دستور را E:notepad a.txt:b.txt را انجام داده ، از ما سوال می کند B وجود ندارد ایجاد کنم؟ بله ایجاد کن و در فایل B هر چقدر که می خواهید بنویسید سپس Save را زده در ظاهر B را نمیبینید ولی دوباره اگر دستور بالا را اجرا کنید میبینید در صورتی که حجم A صفر است و میتوانید فایلA را هر جا که می خواهیدکپی کنید مثل فلش و با انجام دستور بالا B که روی A مخفی شده باز می شود.

Farshid

بهترین نرم افزار قفل گذاری بر روی سی دی Z copy

بهترین نرم افزار قفل شکن سی دی Protect Detect

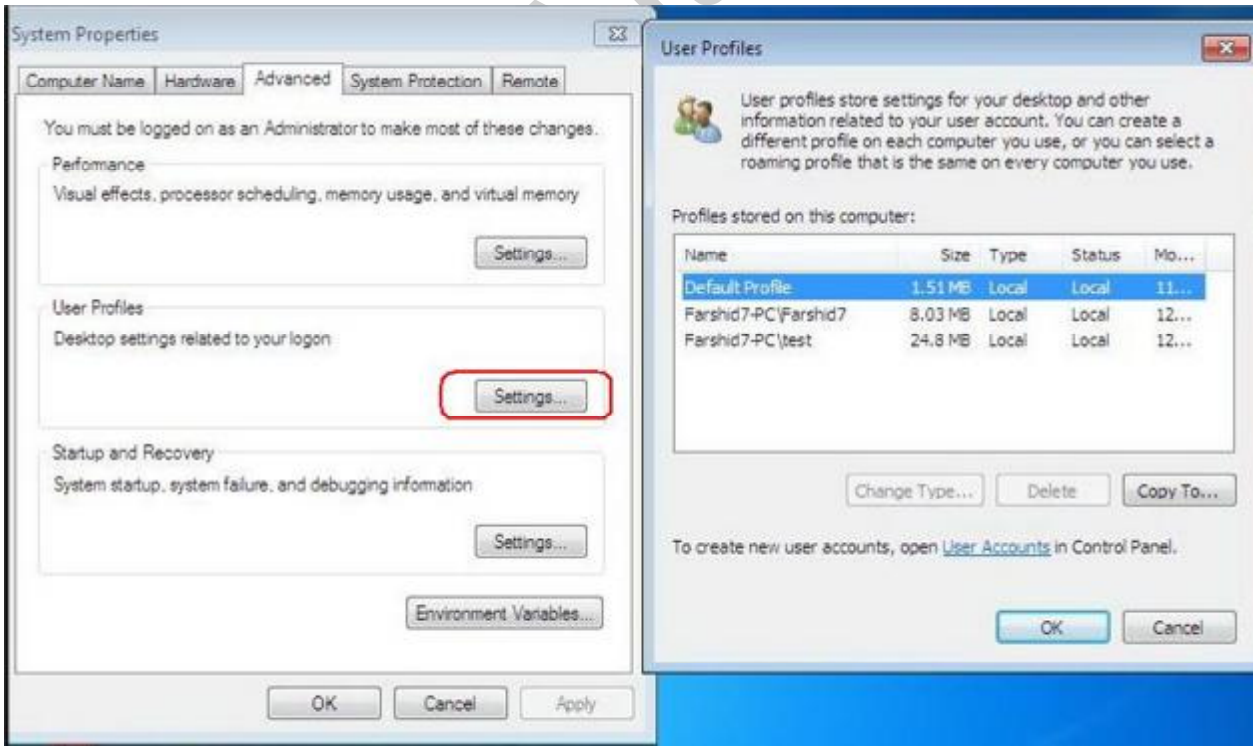
بهترین نرم افزار رهگیری هک سیستم Helix

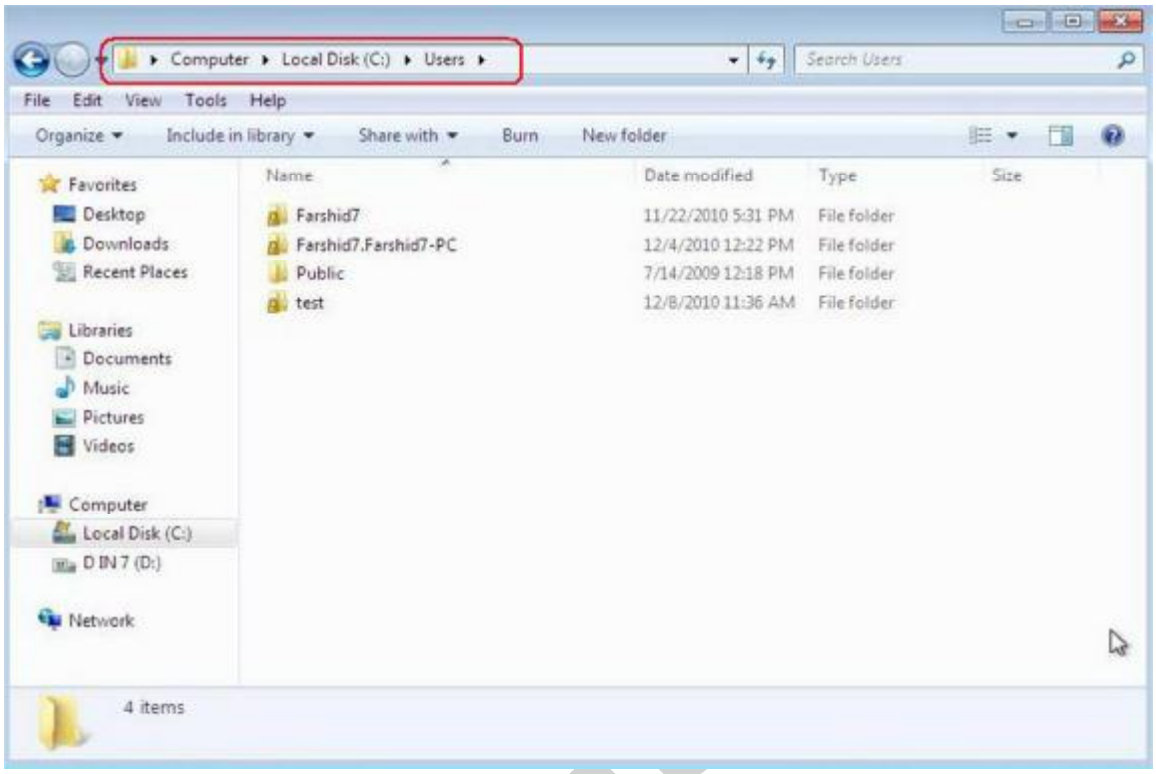
برای بدست آوردن پسوردهای یک کاربر فایل NTUSER.DAT را از پروفایل هر کاربر می توان برداشت.

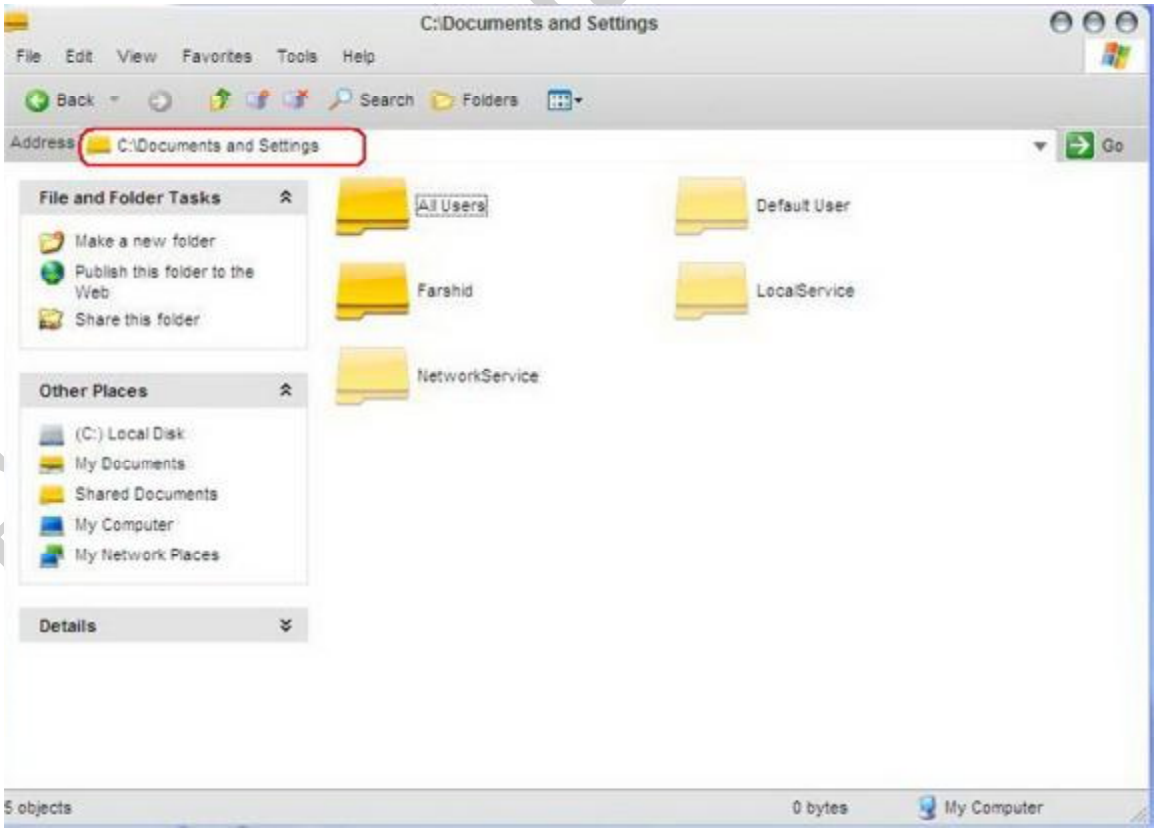
توسط نرم افزارReg scanner می توان پسورد های هش شده را بدست آورد و توسط سایت Passcraking.com آنها رادید.

User Profile:

مجموعه اطلاعات شخصی وتنظیمات نرم افزاری هر کاربر داخل پوشه ای به نام همان کاربر ذخیره می شود که به آن پروفایل گویند.




Computer ▸ Local Disk (C:) ▸ Users ▸
Search Users
File Edit View Tools Help
Organize
Include in library
Share with
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
D IN 7 (D:)
Network
Name
Date modified
Type
Size
Farshid7
11/22/2010 5:31 PM
File folder
Farshid7.Farshid7-PC
12/4/2010 12:22 PM
File folder
Public
7/14/2009 12:18 PM
File folder
test
12/8/2010 11:36 AM
File folder
4 items


C:\Documents and Settings
File Edit View Favorites Tools Help
Back
Search
Folders
Address
C:\Documents and Settings
Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
(C:) Local Disk
My Documents
Shared Documents
My Computer
My Network Places
Details
All Users
Default User
Farshid
LocalService
NetworkService
5 objects
0 bytes
My Computer

در شبکه های کامپیوتری 4 نوع پروفایل داریم:

1) Default user: همانطور که از نامش پیداست یک پروفایل پیش فرض است.

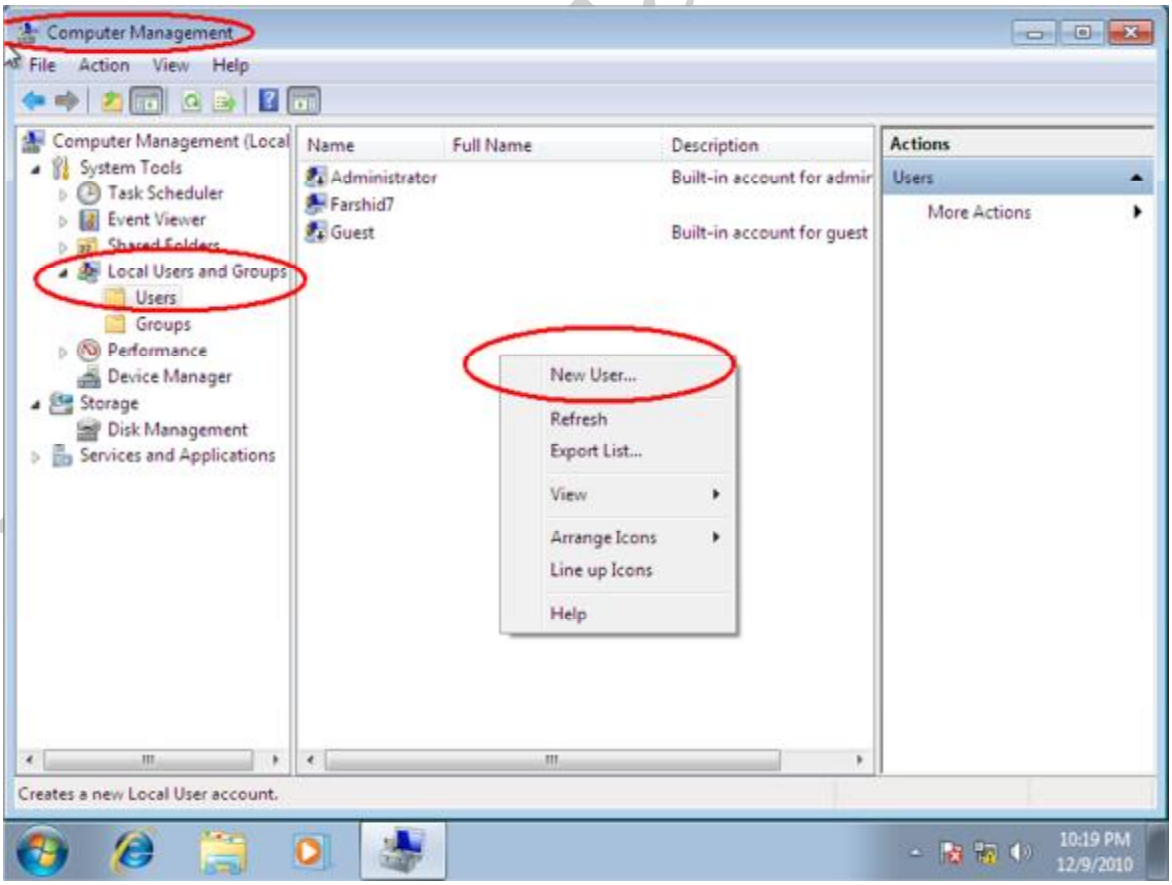
2) Local profile : به پروفایل هر کاربری لوکال پروفایل گویند.

3) Roaming profile : اگر پروفایل شما در یک شبکه، سراسری(رومینگ)باشد شما می توانید از هر دستگاهی درون آن شبکه با پروفایل خودتان Log in شوید.

4) Mandatory profile(اجباری) : تنظیمات این نوع پروفایل فریز شده است یعنی اگر پروفایل شما از این نوع باشد هر تغییری که در ویندوز دهید با یک بار ری استارت کردن سیستم به حالت اول خود باز می گردد.

یکی از روش های تبدیل پروفایل معمولی به پروفایل اجباری تغییر پسوند فایل رجیستری آن پروفایل است یعنی فایل NTUSER.DAT را NTUSER.MAN تغییر دهیم.

ساختن User :

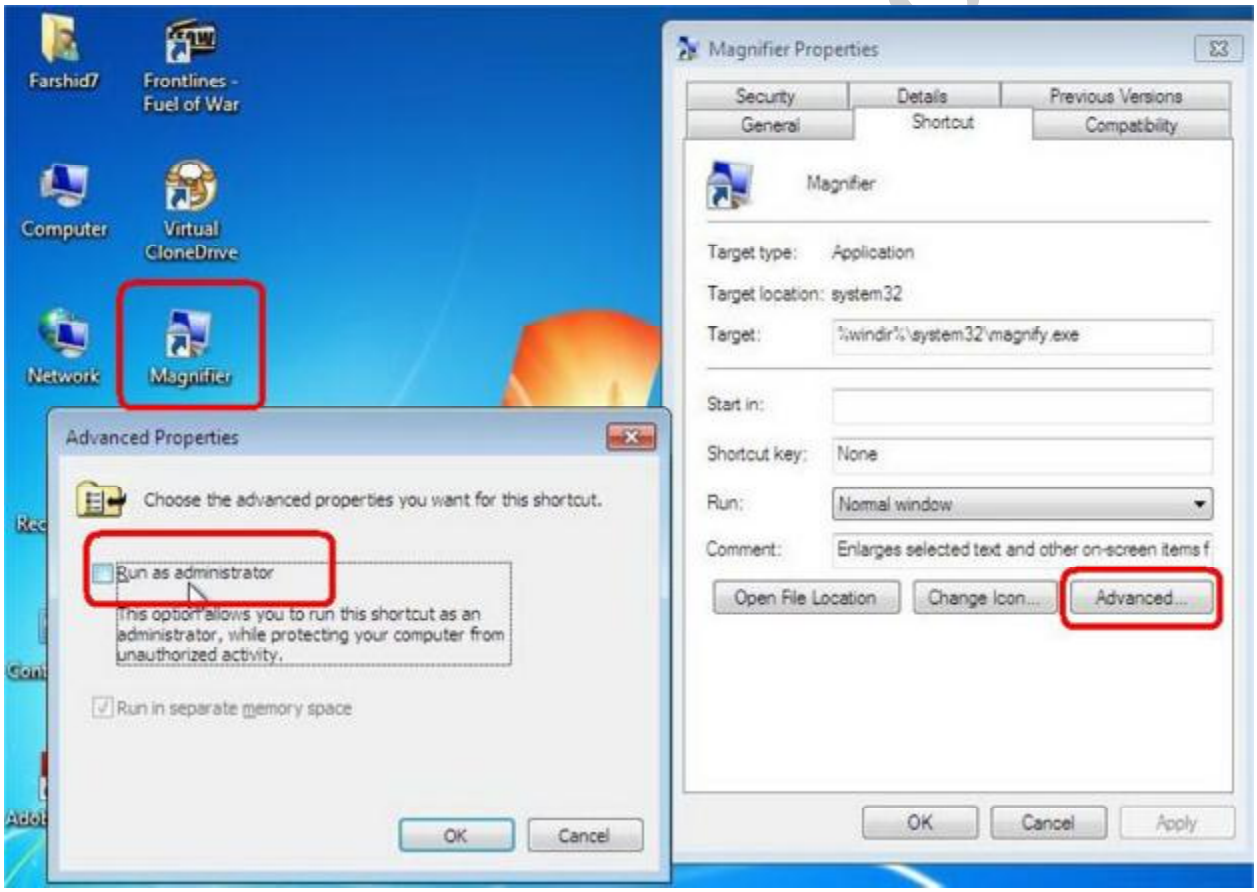


اساس کار دسترسی در شبکه های کامپیوتری مایکروسافت بر اساس TGT (Ticket Grant Ticket )

درویندوزهای NG موقع Log on کردن یوزرAdmin ،با دسترسی استاندارد Log in می شود اگر بخواهیم از دسترسی Admin استفاده کنیم باید از Run as استفاده کنیم.

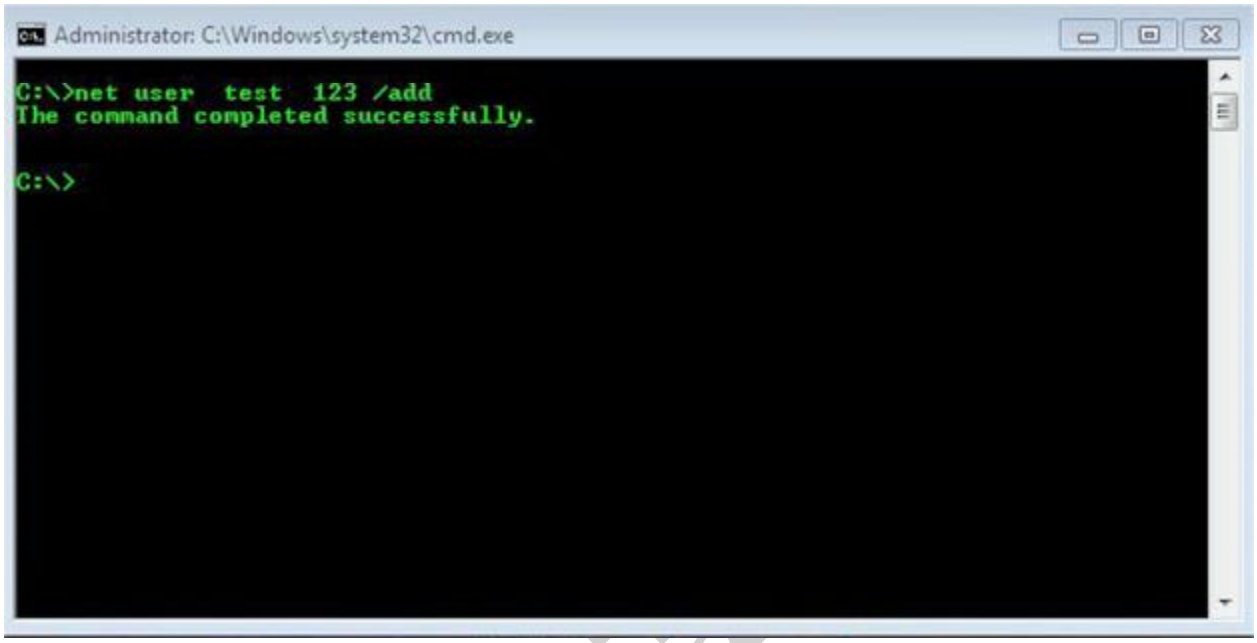
بعضی از نرم افزارها هستند که فقط با دسترسی Admin کار میکنند، نباید پسوردAdmin را به کاربرانی که با این دسته از نرم افزارها کار میکنند داد باید برای این نرم افزارها تعیین کرد که با دسترسی Admin در هر محیطی کار کنند، مثلا نرم افزار Magnifier :

Right click-properties-shortcut tab-advance choose-select Run as administrator

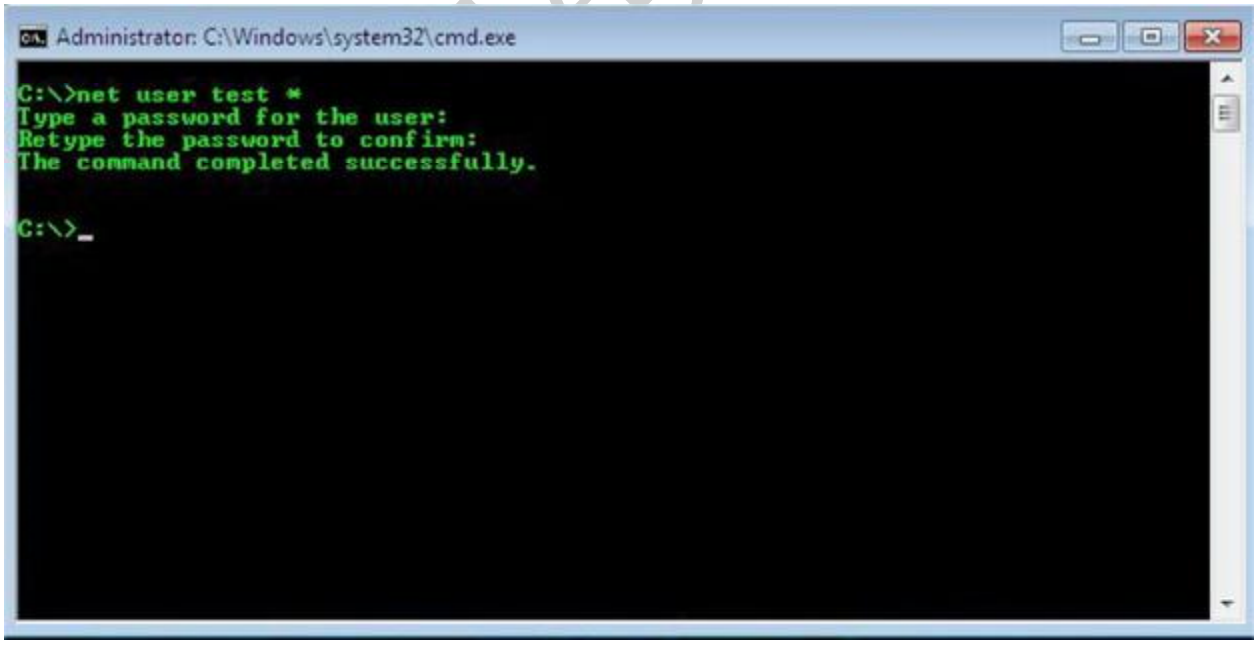


ایجاد و ویرایش User توسط Command :

برای ساختن یک User از دستور: Net user Name userpassword user /add




برای عوض کردن پسورد Userاز دستور: Net user Name user *



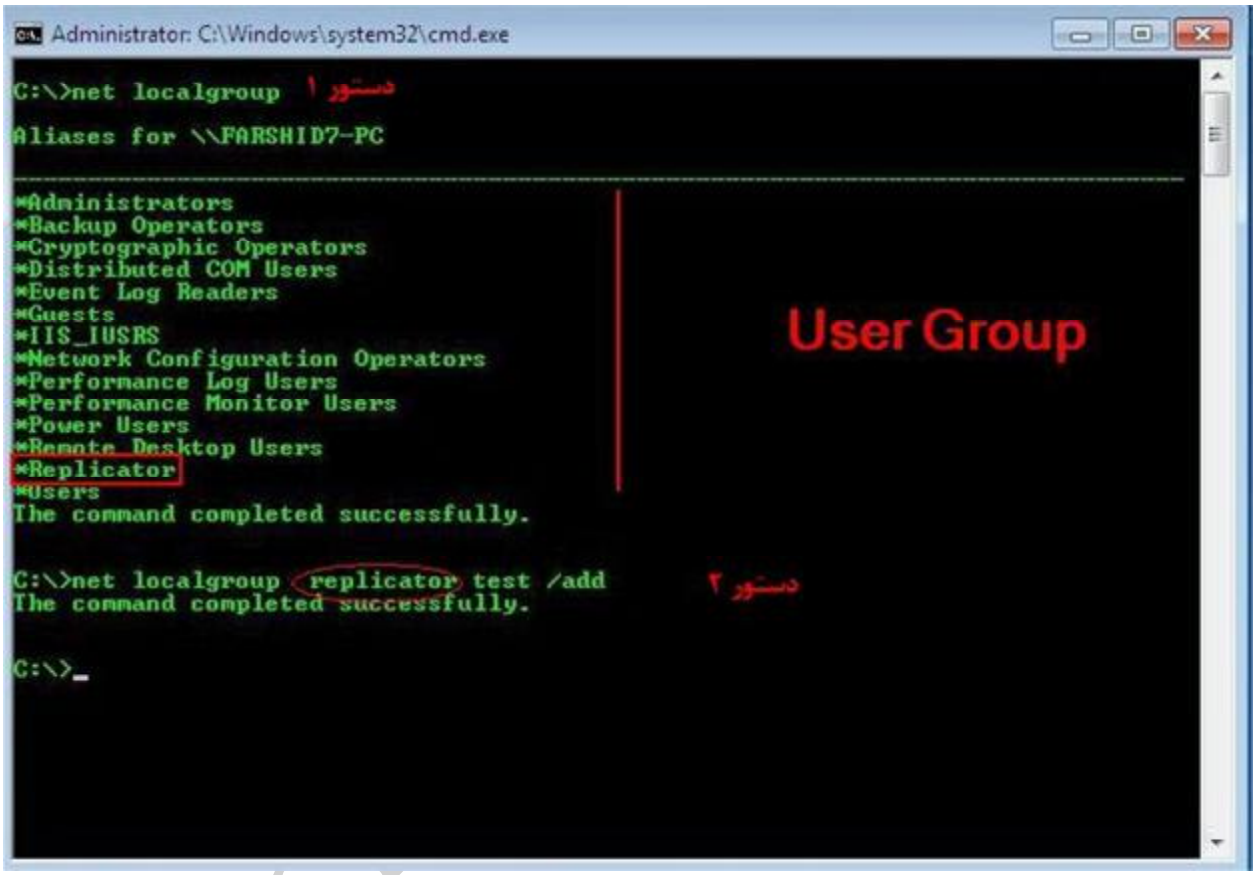

در هنگام تایپ کردن پسورد جدید ما هیچ کاراکتری را روی صفحه مشاهده نمیکنیم مانند شکل بالا ولی پسورد عوض می شود

این به دلیل امنیت است که ویندوز پسورد را به ما نشان نمیدهد.

برای اینکه بتوانیم ماهیتUserرا تغییر دهیم از دستور:

Net localgroup

Net localgroup Name groupUser name/add

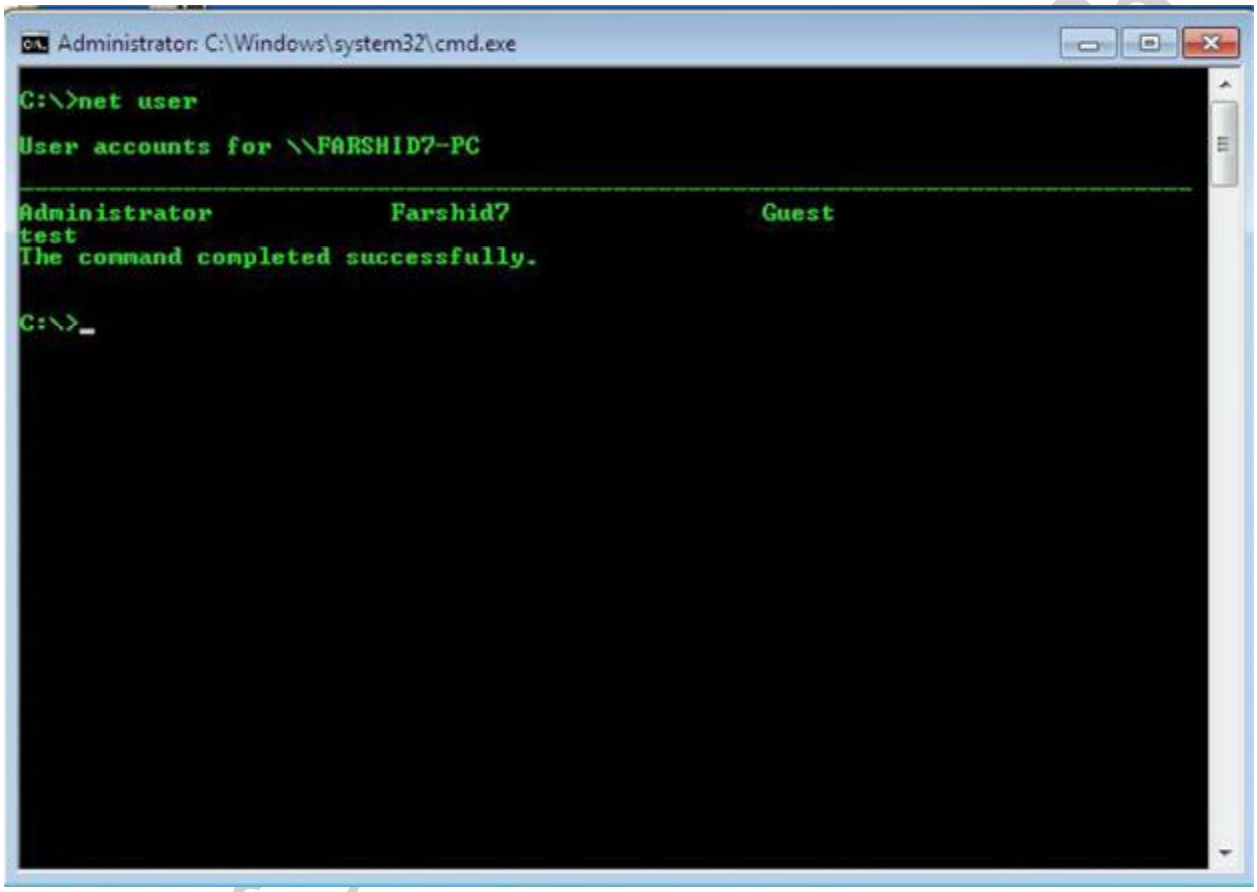



در اینجا از 2 دستور استفاده شده که دستور اول برای دیدن گروه هایی که User می تواند عضو آنها شود و دستور دوم برای اضافه کردن User در یکی از این گروه ها است.

Fars

برای اینکه بتوانیم ببینیم که تعداد User های چقدر است از دستور:

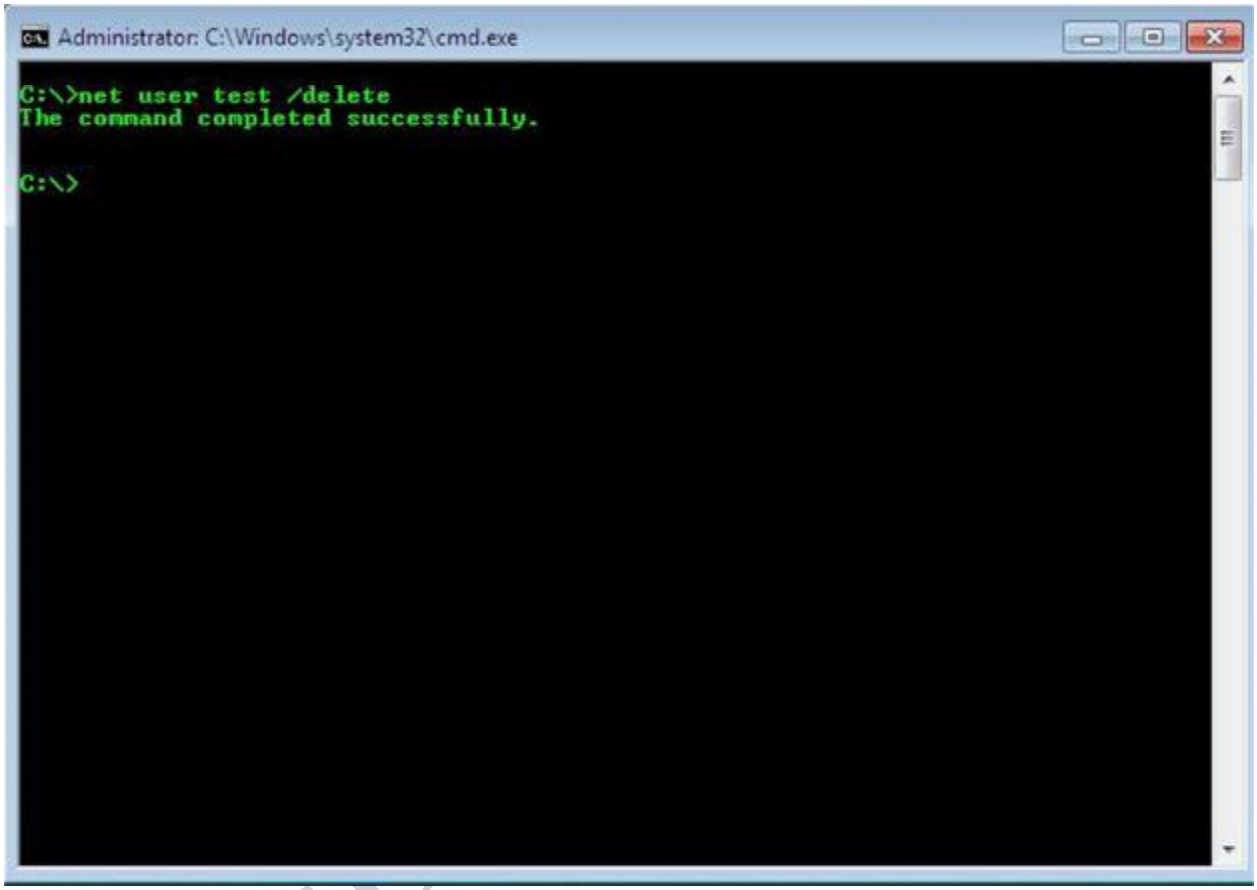
Net user




Fars

برای پاک کردن User از دستور:

Net user Username /delete




Farsi

:POLICY

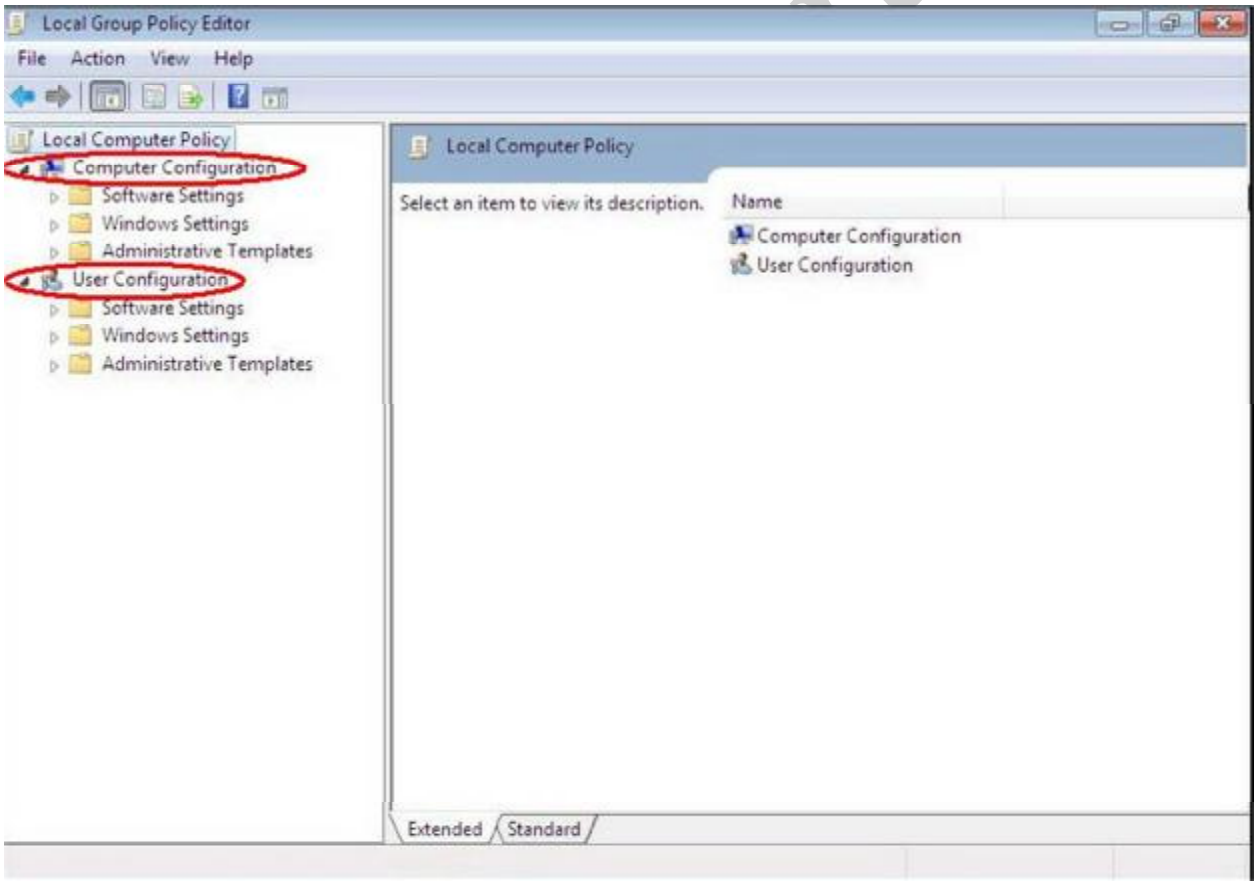
Run-gpedit.msc

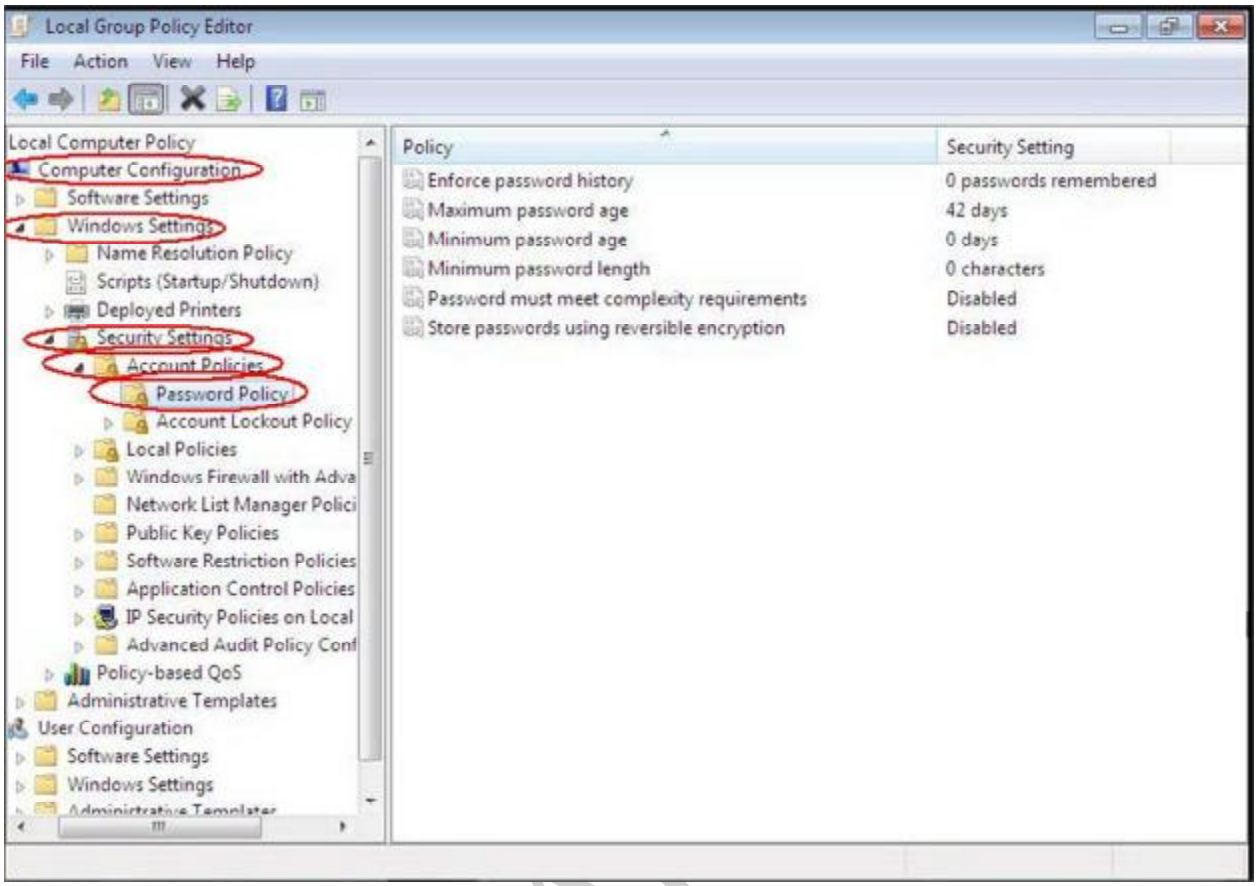
**بعد از باز شدن کنسول ما دو دسته کلی داریم:**

Computer Configuration : **اگر تنظیماتی اینجا اعمال شود، بر روی تمامی کامپیوتر ها و User ها اعمال می شود.**

User Configuration: **اگر تنظیماتی اینجا اعمال شود،فقط بر روی User که با آن داخل ویندوز هستیم**

(Current User ) **اعمال می شود.**






Enforce Password History: در اینجا میتوان تنظیم کرد که یک پسورد را داخل حافظه خود نگهداری کند که با عوض کردن پسورد نتوان همان پسوردی را که در حافظه خودش نگه داشته تا دفعات قابل تنظیم مثلا10 بار دوباره گذاشت.

Maximum Password Age:طول عمر پسورد را می توان تنظیم کرد(برای ایران7روز بهتره)

Minimum Password Age:اگر مقدار این گزینه را مثلا 1 کنیم پسوردی را که تنظیم کرده ایم باید حداقل 1 روز استفاده کنیم تا بتوانیم آن را عوض کنیم.

Minimum Password Length: طول پسورد را می توان تنظیم کرد که نباید کمتر از 8 کاراکتر و بیشتر از 14 کاراکتر باشد چون ویندوز تا 14 کاراکتر پردازش می کند.

FarshidAj

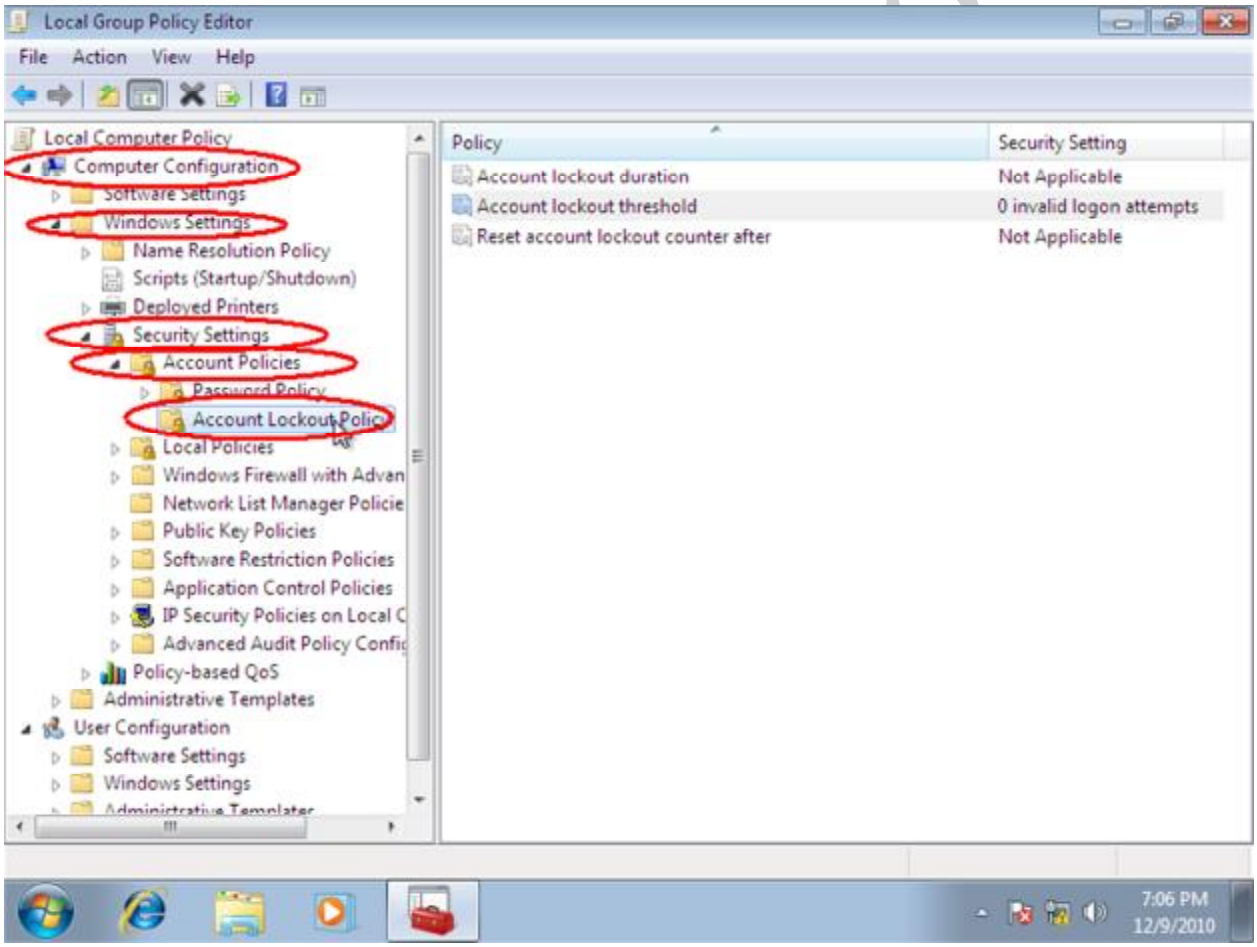
:Password Must meetComplexityRequirements

**این گزینه حتماً باید فعال باشد بدلیل امنیت بالا، با فعال بودن این گزینه پسورد های ما باید (Complexity) پیچیده باشند به پسوردهایی که ترکیبی از علامت،عدد،حروف کوچک وبزرگ باشند Complexity گویند.**

:Store Passwords Using Reversible encryption

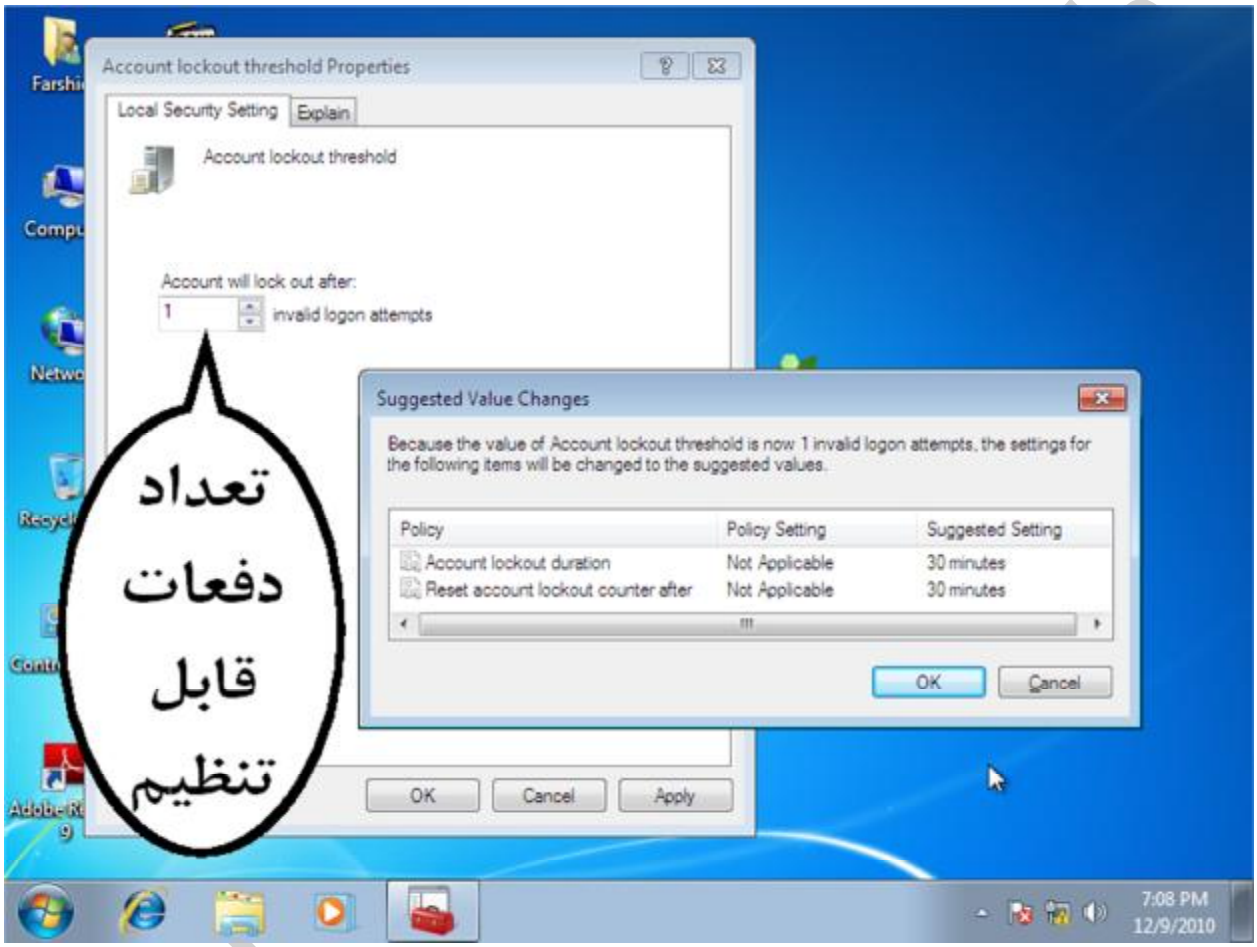
**با فعال بودن این گزینه پسوردها طوری ذخیره می شوند که قابل بازگشت باشند،این گزینه حتماً باید غیر فعال باشد.**

:Account Lockout Policy



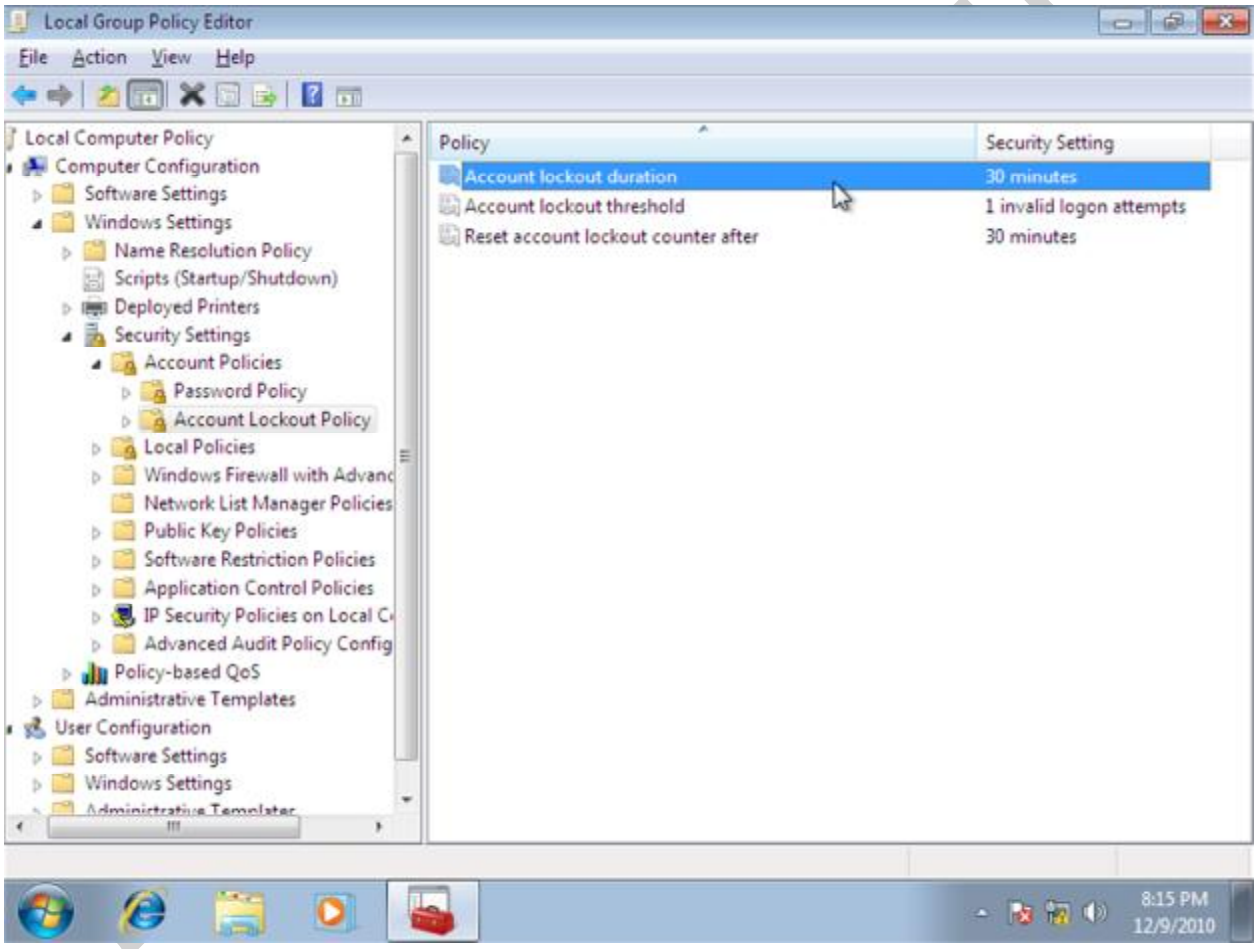
Account Lockout Threshold:

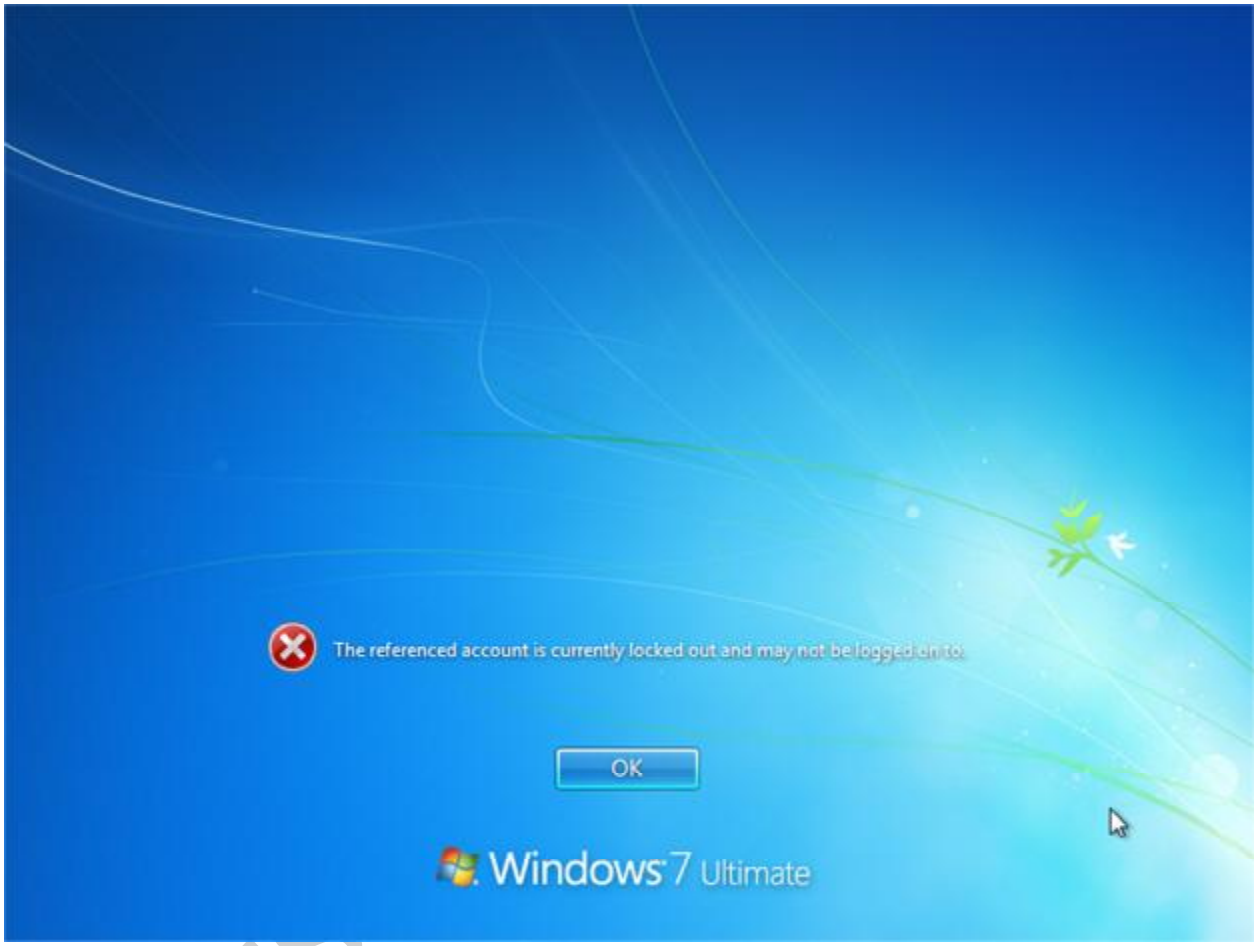
با فعال کردن این گزینه اگر کاربری پسوردش را1بار (تعداد دفعات قابل تنظیم است) اشتباه وارد کند،سیستم قفل میکند (شکلB ) اگر این گزینه را فعال کنیم دو گزینه دیگر هم اتوماتیک فعال می شوند.



Account Lockout Duration:

با فعال کردن این ویژگی اگر کاربری پسوردش را1 بارراشتباه واردکند(تعداد دفعات اشتباه از ویژگی Account Lockout Thresholdقبلاً تنظیم شده) سیستم بطور پیش فرض 30 دقیقه قفل می کند(مدت زمان قابل تغییر است) یعنی حتی اگر دفعه دوم پسورد را صحیح وارد کنیم باز قبول نمی کند(شکلB ) تا آن مدت زمان بگذرد اگر بخواهیم زودتر از 30 دقیقه از حالت قفل در بیایم بایدAdmin این کار را برایمان انجام دهد،البته باید قبل از فعال کردن این ویژگی،ویژگی Account Lockout Threshold را فعال کرد.




The referenced account is currently locked out and may not be logged on to.
OK
Windows 7 Ultimate

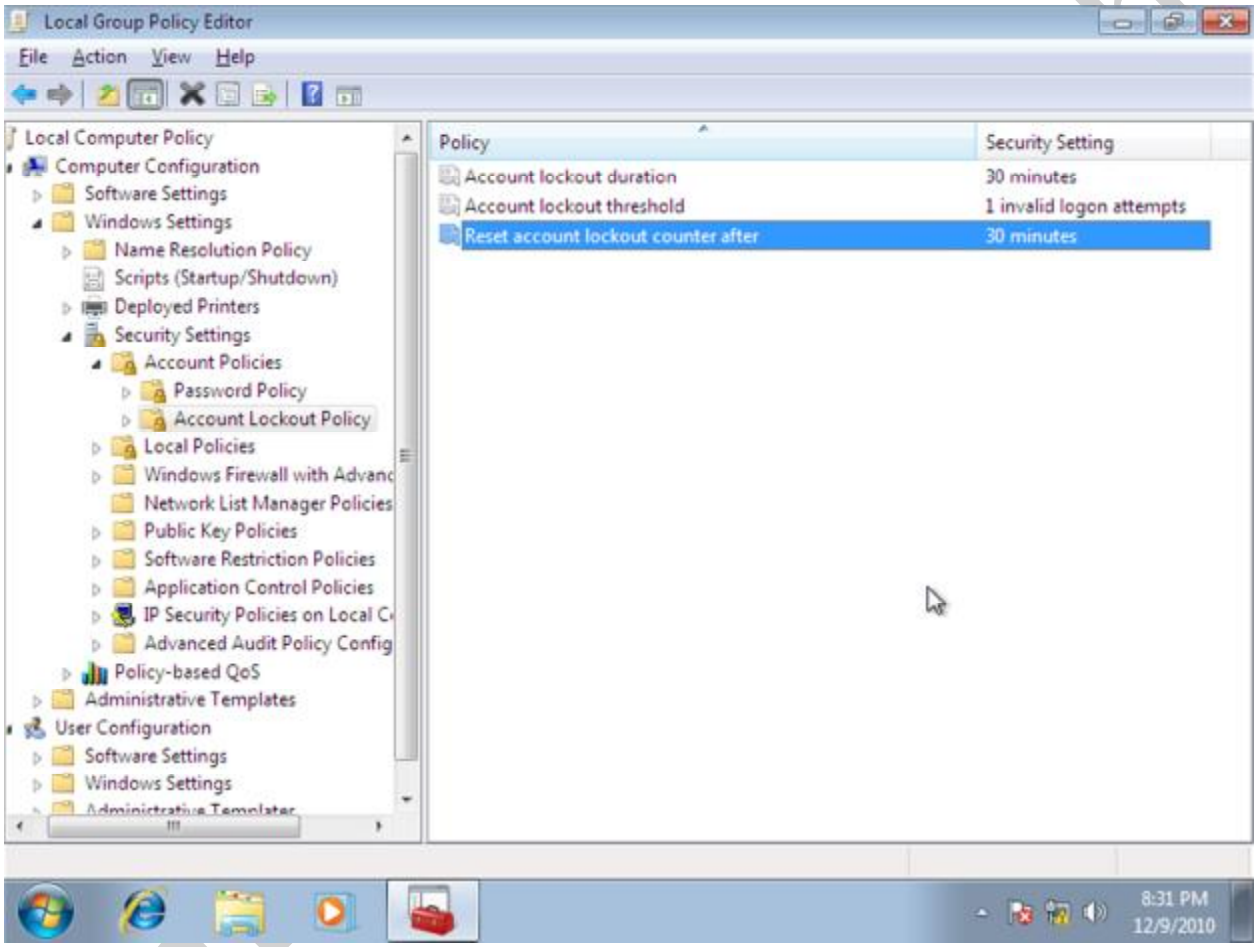
شکل B

Fars

: Reset Account Lockout Counter After

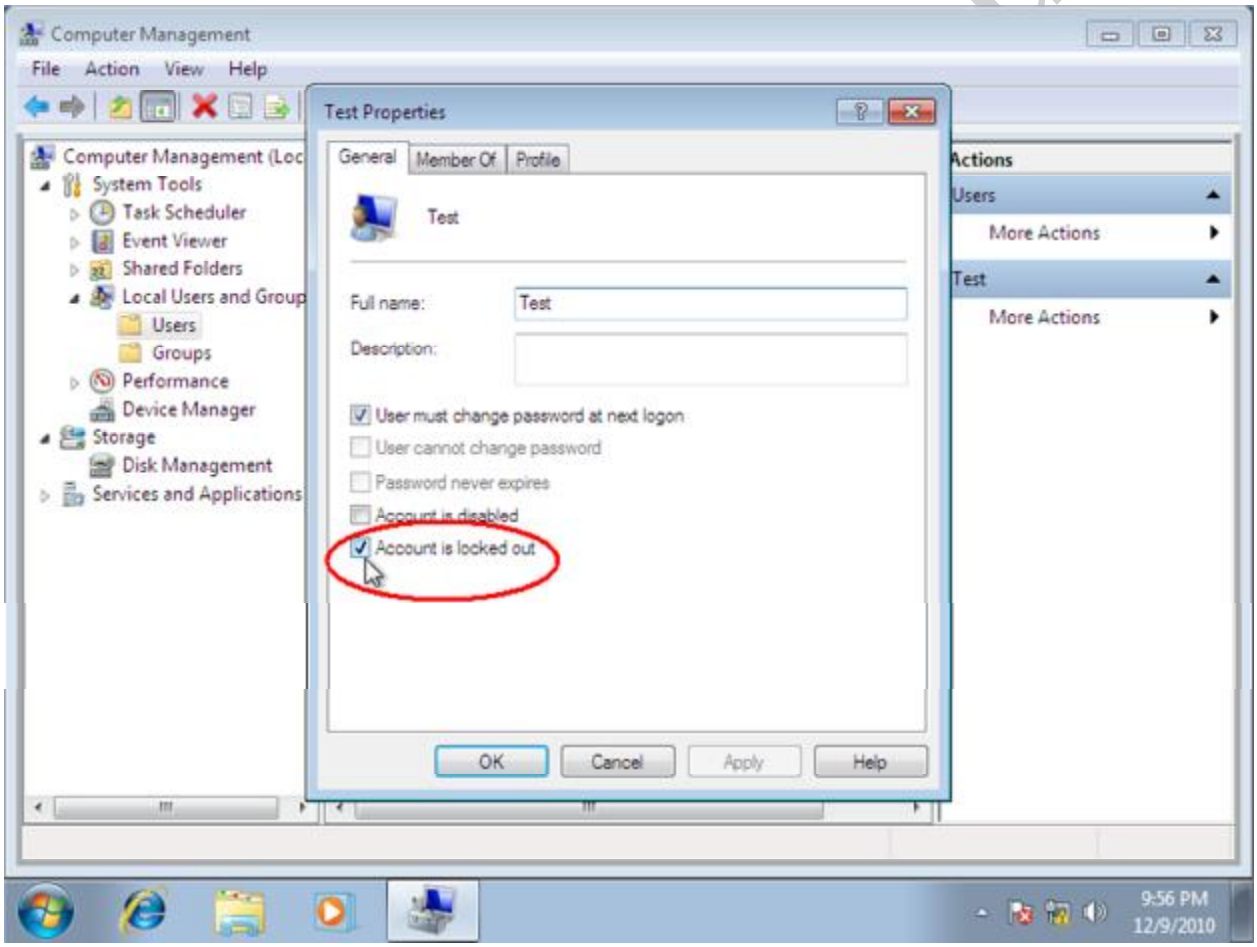
با فعال بودن این ویژگی، حافظه بعد از مدت مشخص( بطور پیش فرض 30 دقیقه) از پسوردهای اشتباه خالی می شود.

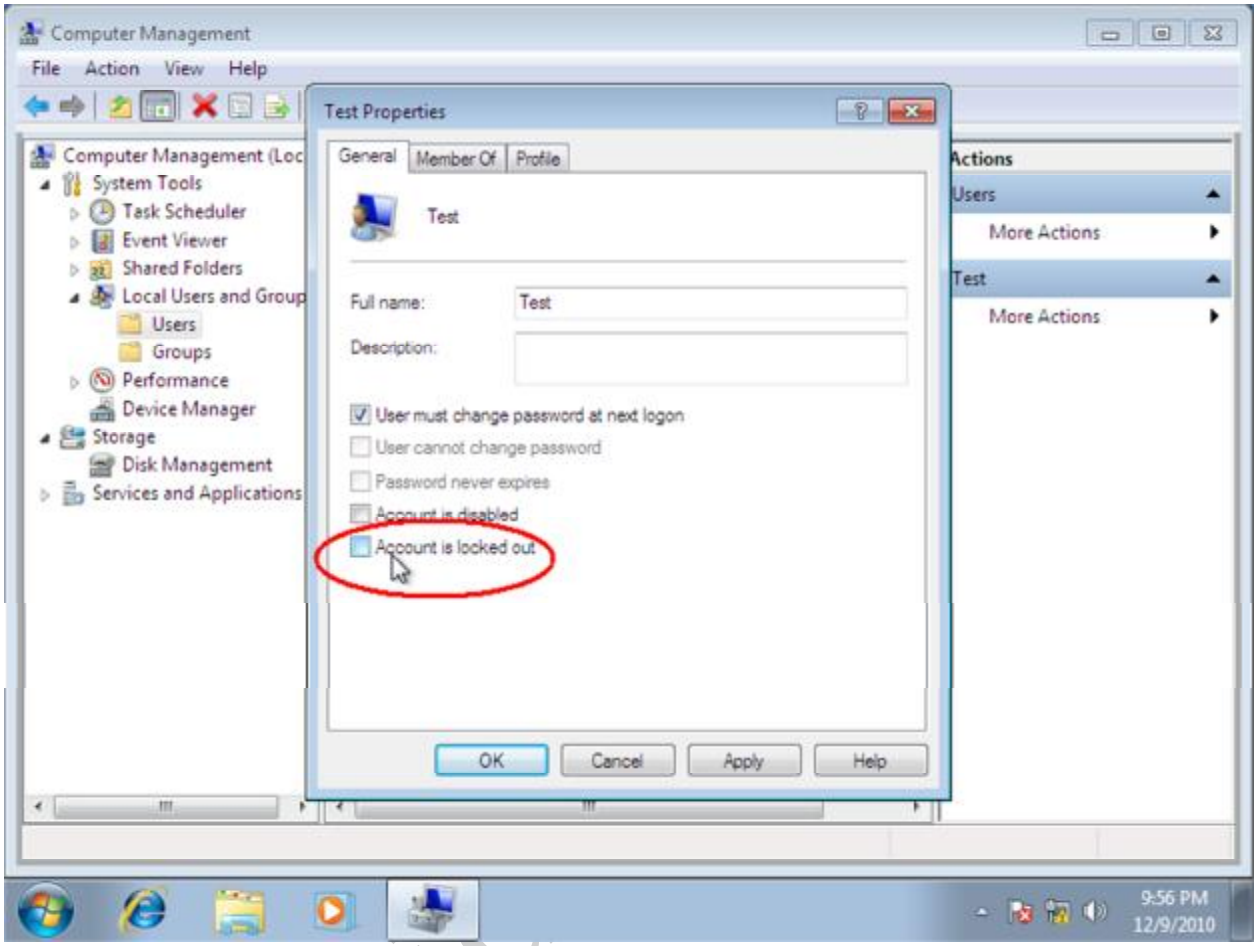
البته باید قبل از فعال کردن این ویژگی،ویژگی Account Lockout Threshold را فعال کرد.




- تمامی User ها وپسوردها در فایلی به نام Sam Account در System32 ذخیره می شود که توسط نرم افزار LC5 می توان آنرا باز کرد.

- هنگامی که بـه مشـکل شـکل B( کـه قـبلاً توضـیح داده شـده) برخـوردیم بایـد بـا User Adminوارد بشـویم سـپس از طریـق Computer Management وارد قسـمت User هـا شـویم User مـورد نظـر را انتخـاب کنـیم و Properties بگیـریم و تیـک گزینـه Account is locked out را بـرداریم سـپس می توانیم دوباره با User مورد نظر وارد ویندوز شویم .




Computer Management
File Action View Help
Computer Management (Loc
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Group
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Test Properties
General Member Of Profile
Test
Full name: Test
Description:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
Account is locked out
OK Cancel Apply Help
Actions
Users
More Actions
Test
More Actions
9:56 PM
12/9/2010

Farshid

- نرم افزاری به نام Key Loger وجود دارد که زمانی که بر روی سیتمی نصب کنیم بدون اینکه کاربر متوجه بشود هرچیزی را که توسط کی برد وارد کند ثبت می کند و برای ما ایمیل می کند.

- راه حلی که بشود Key Loger را غیر فعال کرد استفاده از ctr+alt+del در هنگام Log on شدن به ویندوز است که باعث می شود تمام برنامه هایی که درون System32 هستند Lock بشوند از جمله Key Loger.

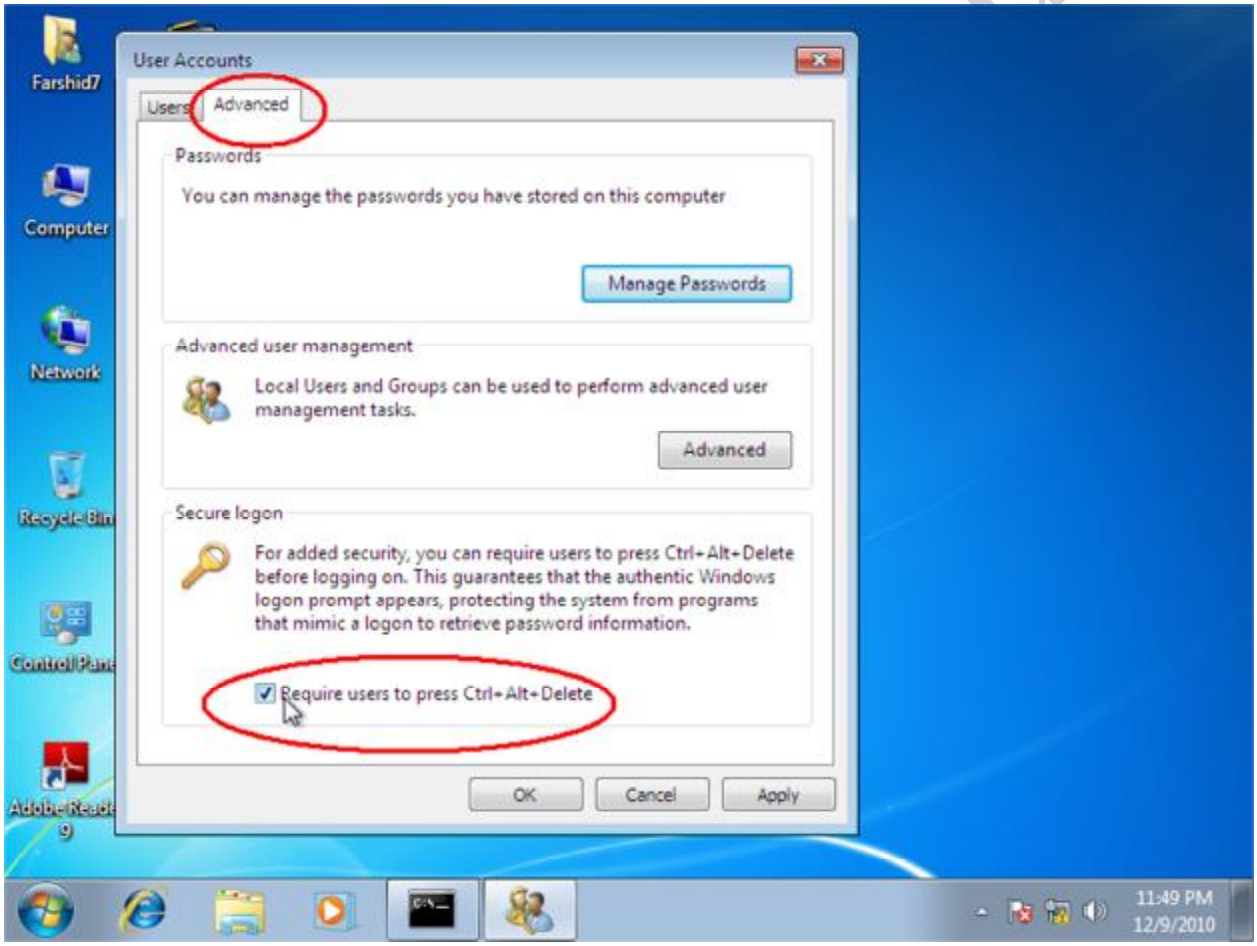
- اگر پنجره Log onفعال نبودمی توانیم توسط دستور زیر هم در ویندوزهای NG و هم در ویندوزهای Legacy آن را فعال کنیم:

Control userpasswords2

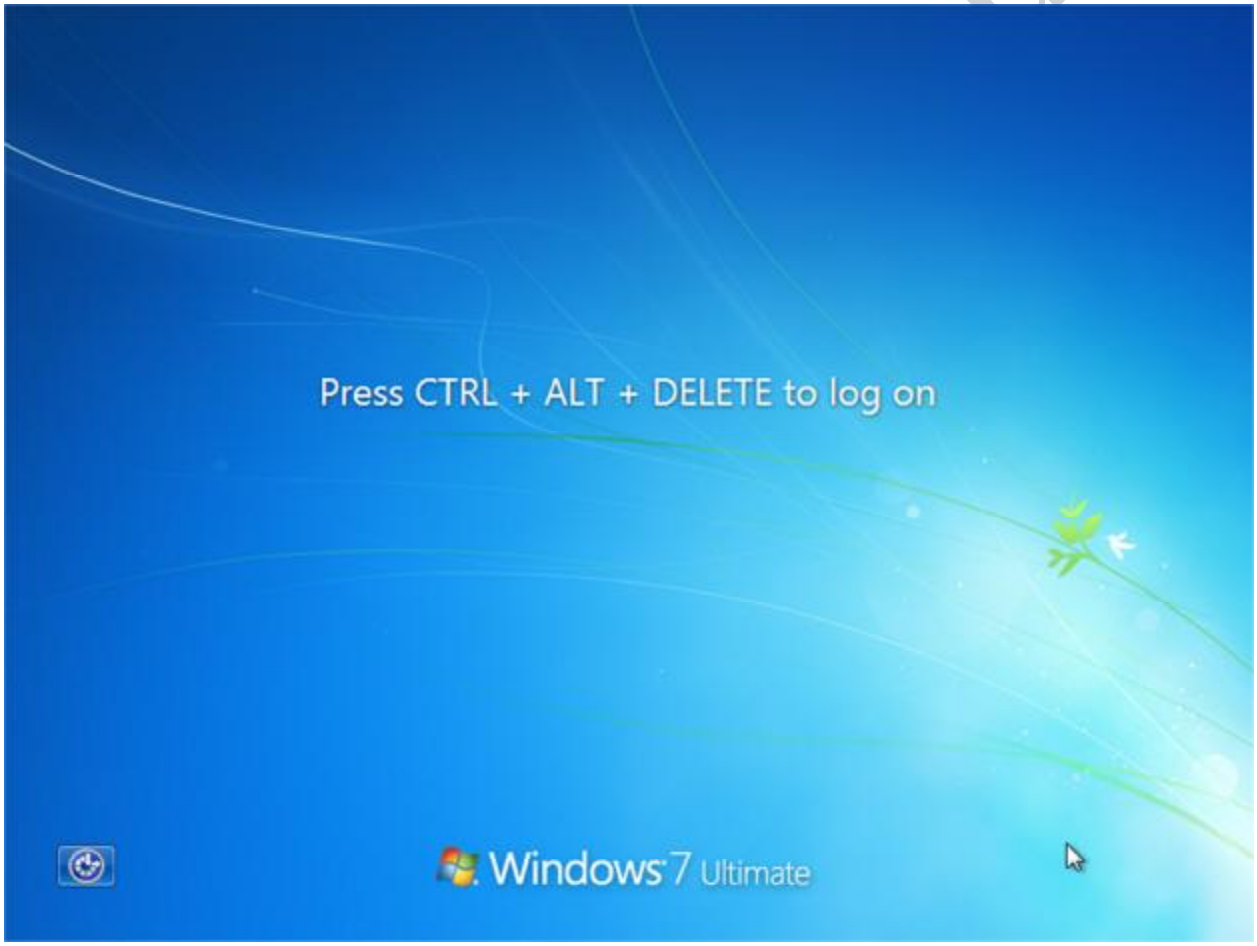
Farshid Soroush

سپس پنجره ای همانند شکل زیر باز می شود :

به تب Advance می رویم و تیک گزینه Require Users To Press Ctr+Alt+Del می زنیم.

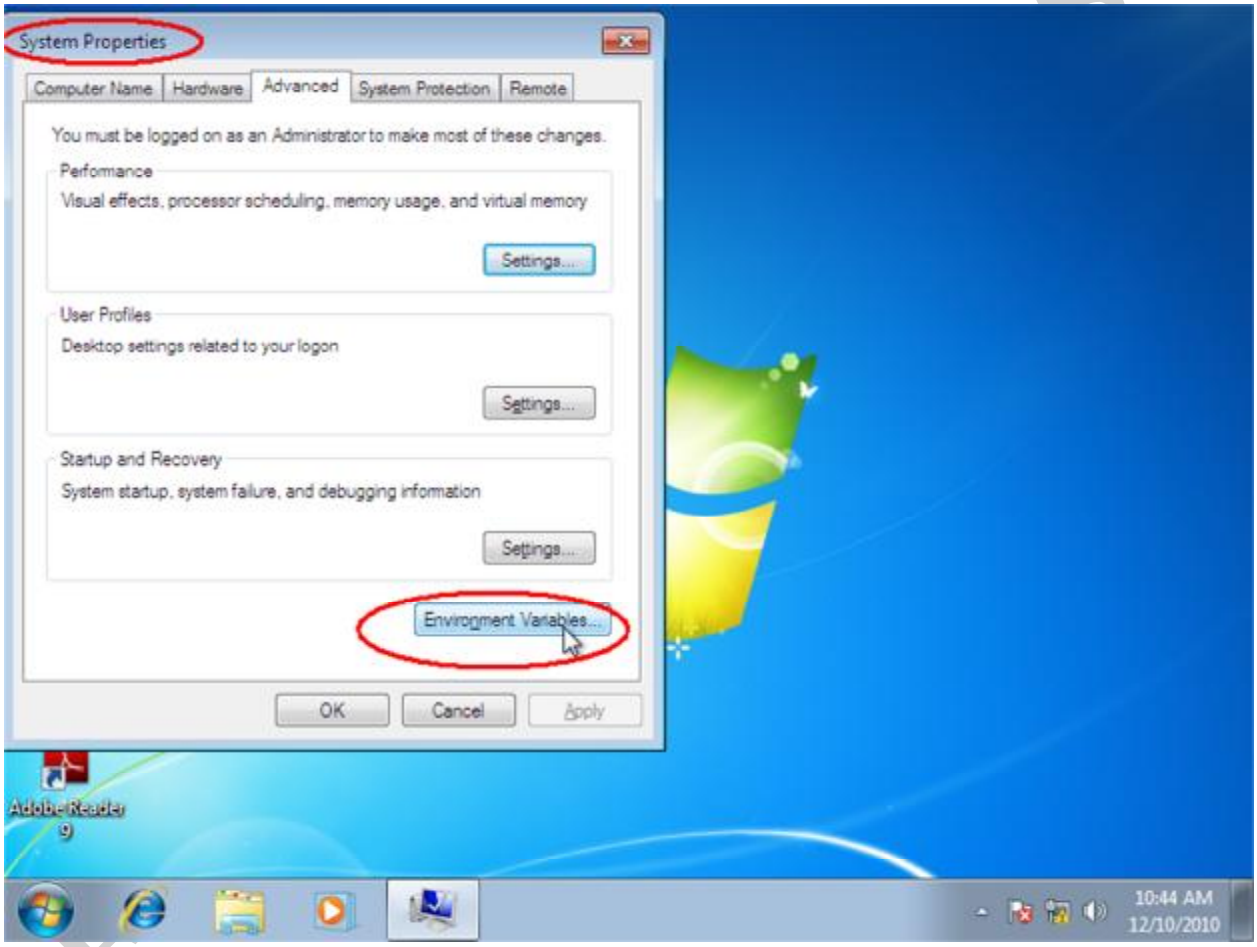


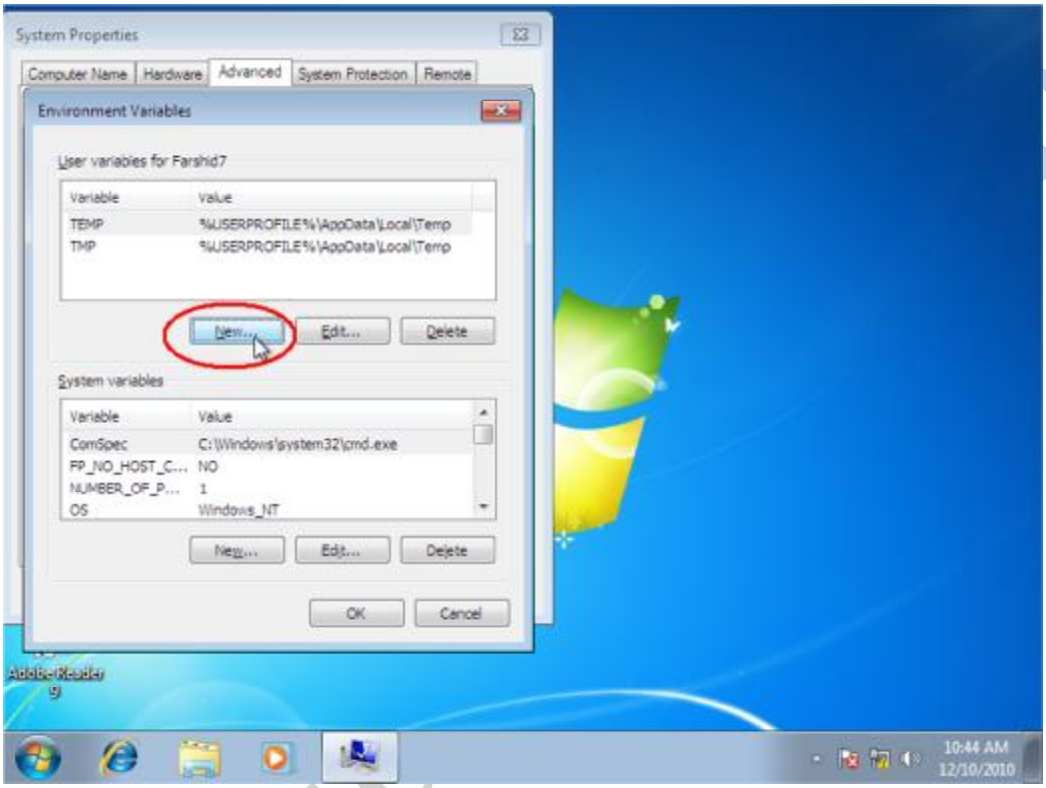
و از این به بعد وقتی که بخواهیم وارد ویندوز شویم باید Ctr+Alt+Del را بگیریم.



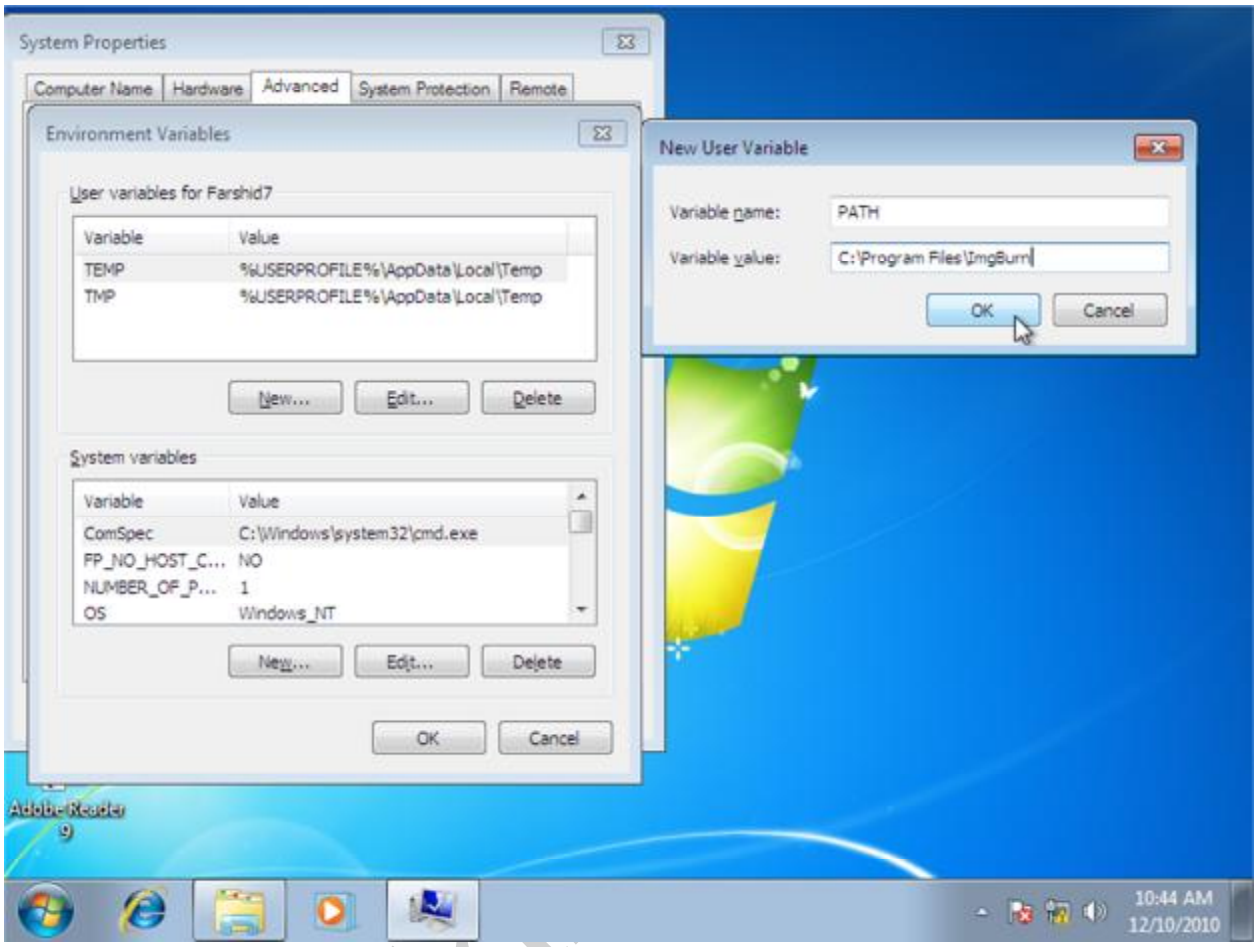
:Environment Variables

**بعضی از نرم افزارها هستند که برای اجرا کردن آنها باید مسیر نصب شدن آن ها را هر دفعه در Run وارد کرد تا اجرا شوند، حفظ کردن مسیر کمی سخت است،در ویندوز ویژگی وجود دارد که یک بار مسیر را به آن می دهیم و هر دفعه که با آن نرم افزار کار داشتیم کافی است اسم آن نرم افزار را در Run وارد کنیم سپس اجرا می شود.**

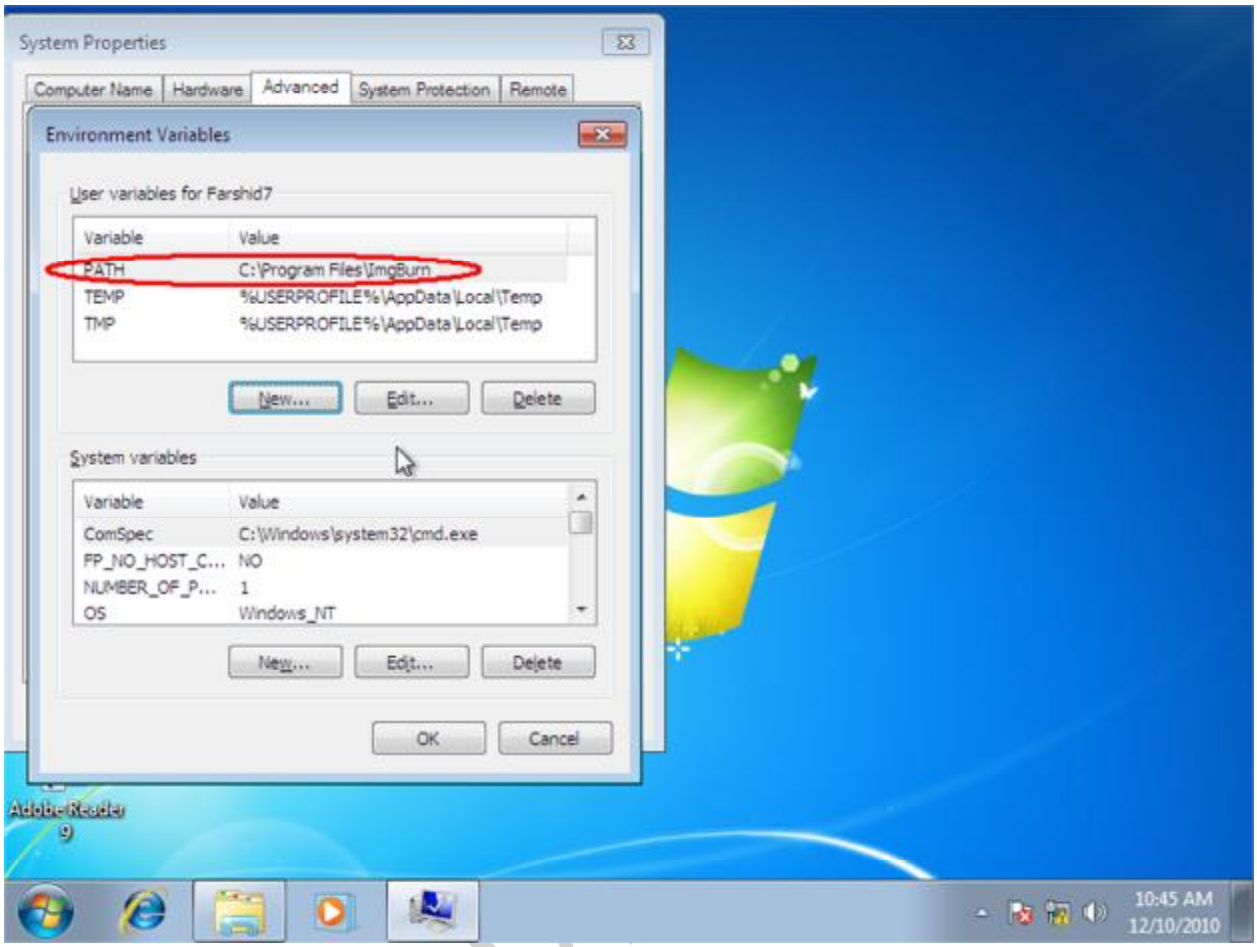



System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
Environment Variables
User variables for Farshid7
Variable
Value
TEMP
%USERPROFILE%\AppData\Local\Temp
TMP
%USERPROFILE%\AppData\Local\Temp
New...
Edit...
Delete
System variables
Variable
Value
ComSpec
C:\Windows\system32\cmd.exe
FP_NO_HOST_C...
NO
NUMBER_OF_P...
1
OS
Windows_NT
New...
Edit...
Delete
OK
Cancel
Adobe Reader 9
10:44 AM
12/10/2010

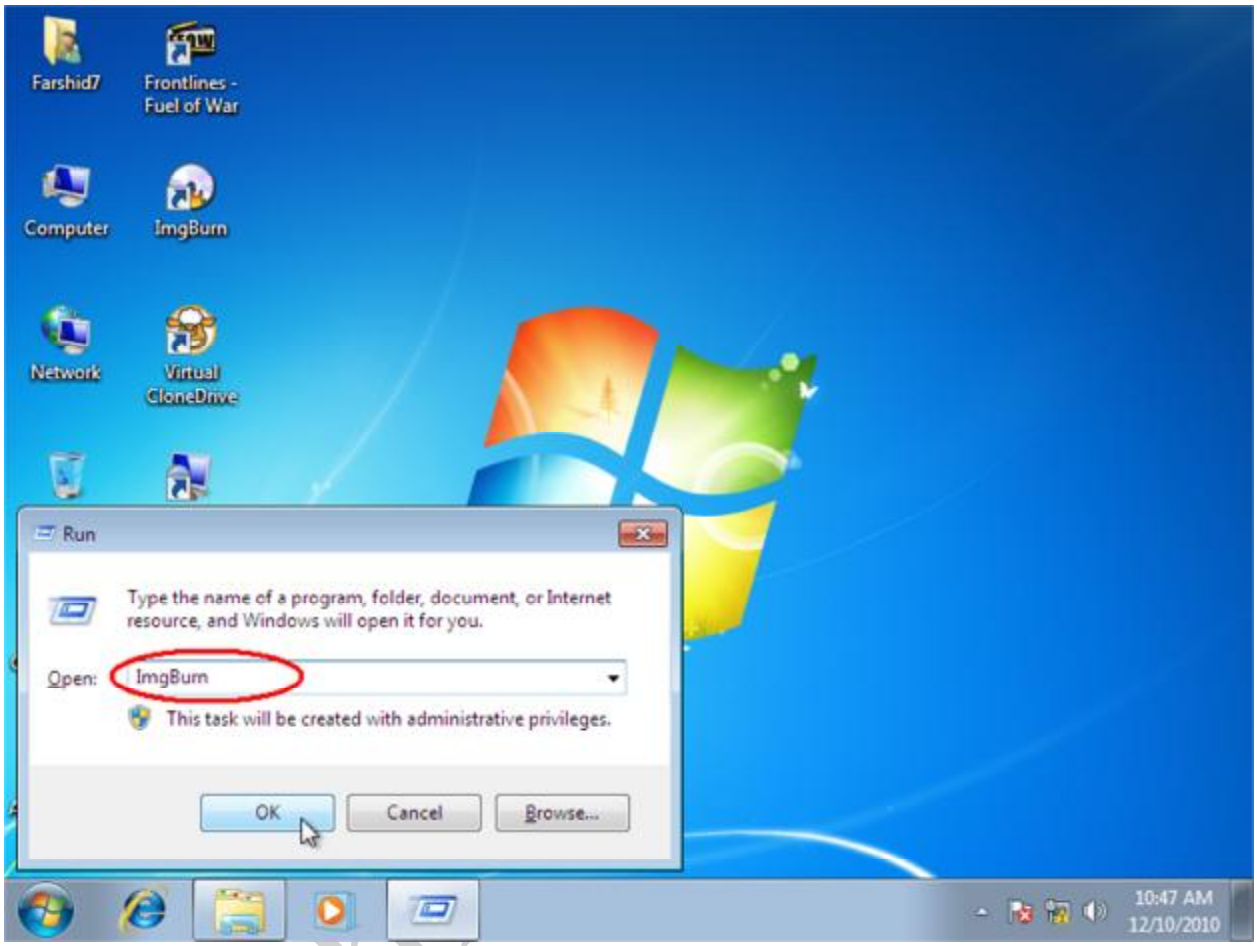
Farshid


System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
Environment Variables
User variables for Farshid7
Variable
Value
TEMP
%USERPROFILE%\AppData\Local\Temp
TMP
%USERPROFILE%\AppData\Local\Temp
New...
Edit...
Delete
System variables
Variable
Value
ComSpec
C:\Windows\system32\cmd.exe
FP_NO_HOST_C...
NO
NUMBER_OF_P...
1
OS
Windows_NT
New...
Edit...
Delete
OK
Cancel
New User Variable
Variable name:
PATH
Variable value:
C:\Program Files\ImgBurn
OK
Cancel
Adobe Reader 9
10:44 AM
12/10/2010

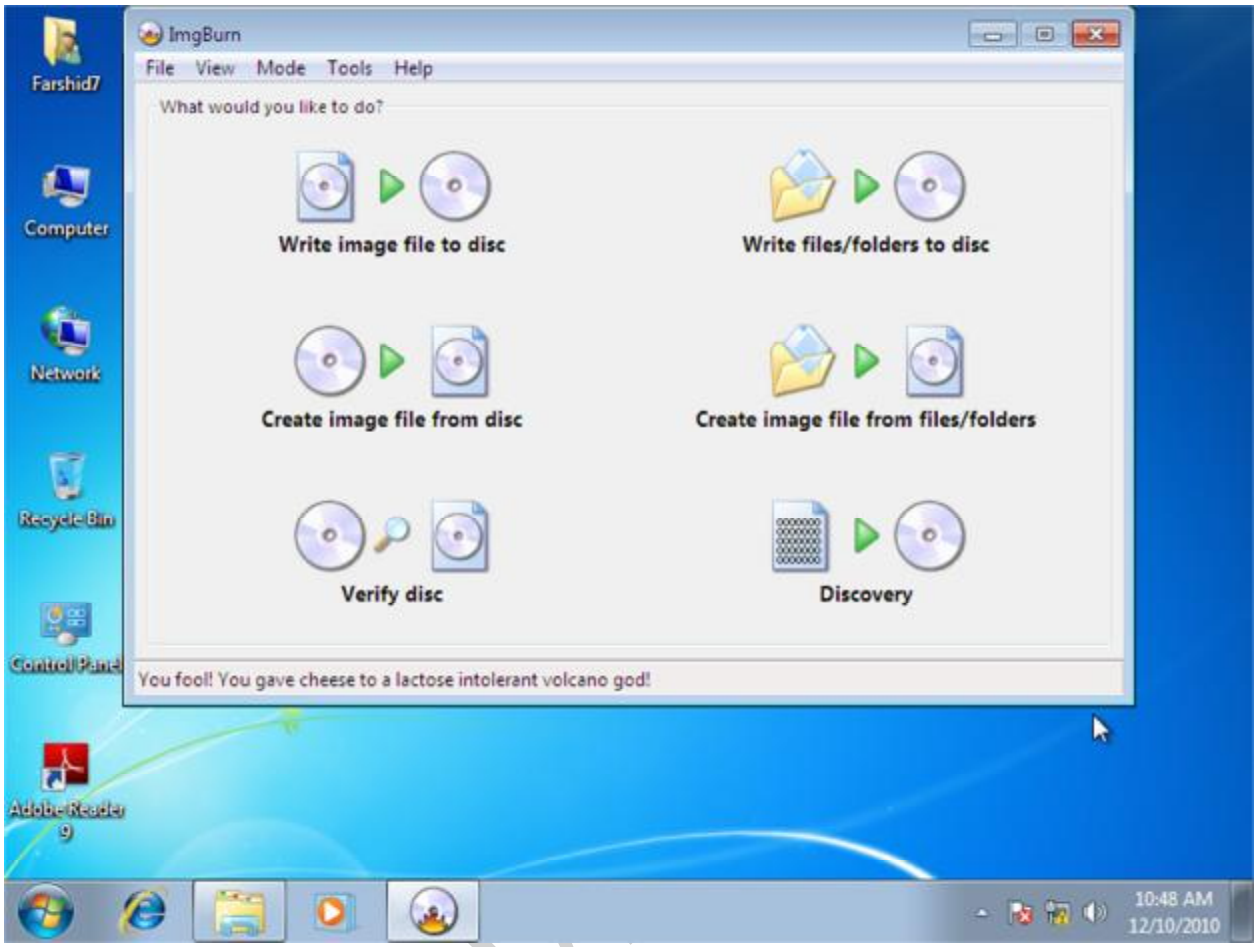
Farshid


System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
Environment Variables
User variables for Farshid7
Variable
Value
PATH
C:\Program Files\ImgBurn
TEMP
%USERPROFILE%\AppData\Local\Temp
TMP
%USERPROFILE%\AppData\Local\Temp
New...
Edit...
Delete
System variables
Variable
Value
ComSpec
C:\Windows\system32\cmd.exe
FP_NO_HOST_C...
NO
NUMBER_OF_P...
1
OS
Windows_NT
New...
Edit...
Delete
OK
Cancel
Adobe Reader 9
10:45 AM
12/10/2010

Farshid


Farshid7
Frontlines - Fuel of War
Computer
ImgBurn
Network
Virtual CloneDrive
Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
ImgBurn
This task will be created with administrative privileges.
OK
Cancel
Browse...
10:47 AM
12/10/2010

Farshi

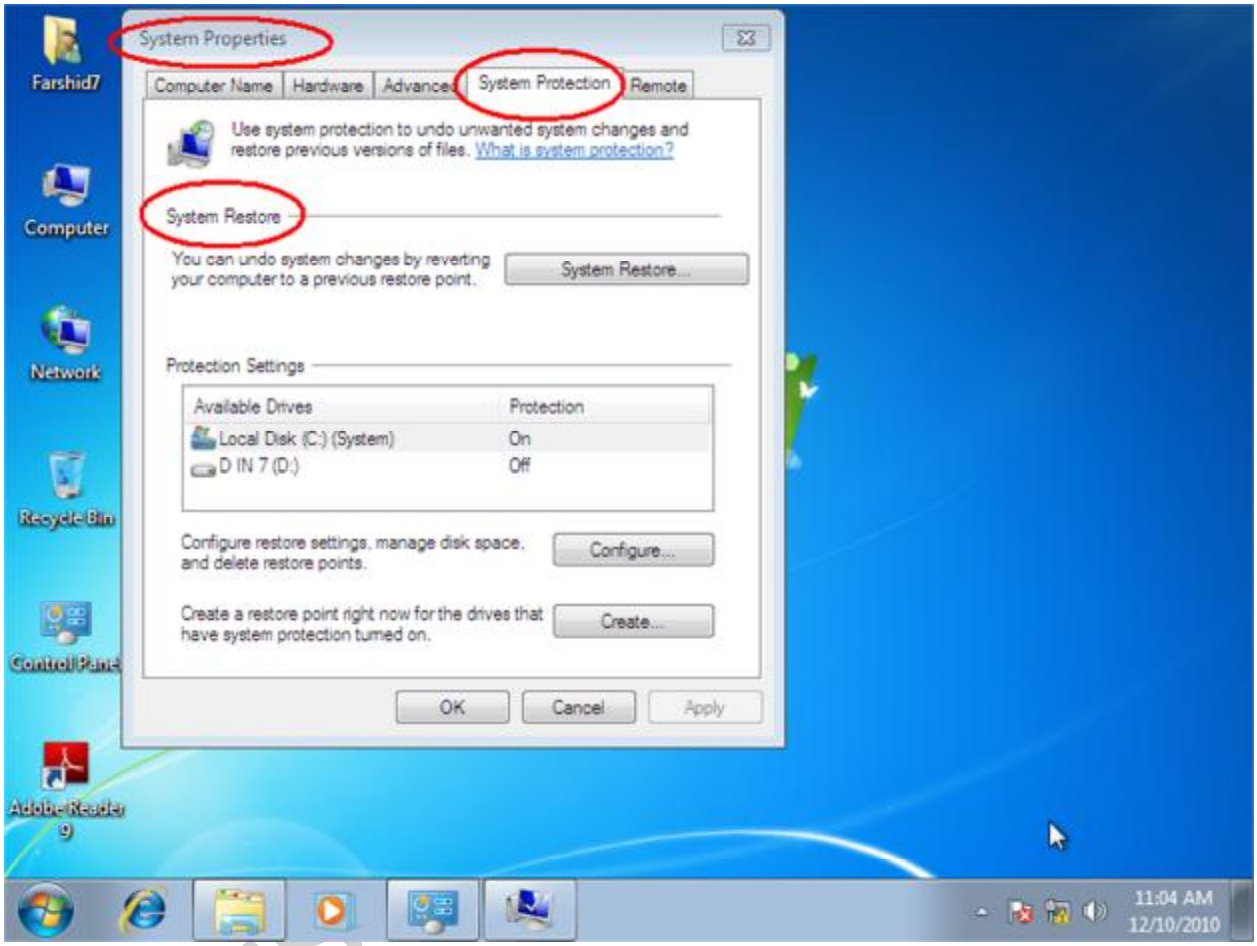



**همانطور که دیدید با تایپ کردن اسم نرم افزار نرم افزار همانند شکل با لا اجرا شد.**

Farshid

: System Restore

همه با این گزینه آشنا هستیم،فقط مسیر آن را در ویندوز 7 با هم میبینیم.




Restore Pointها در ویندوزهای NG بعد از 137 روز و در ویندوزهای Legacy بعد از 90 روز پاک می شوند،

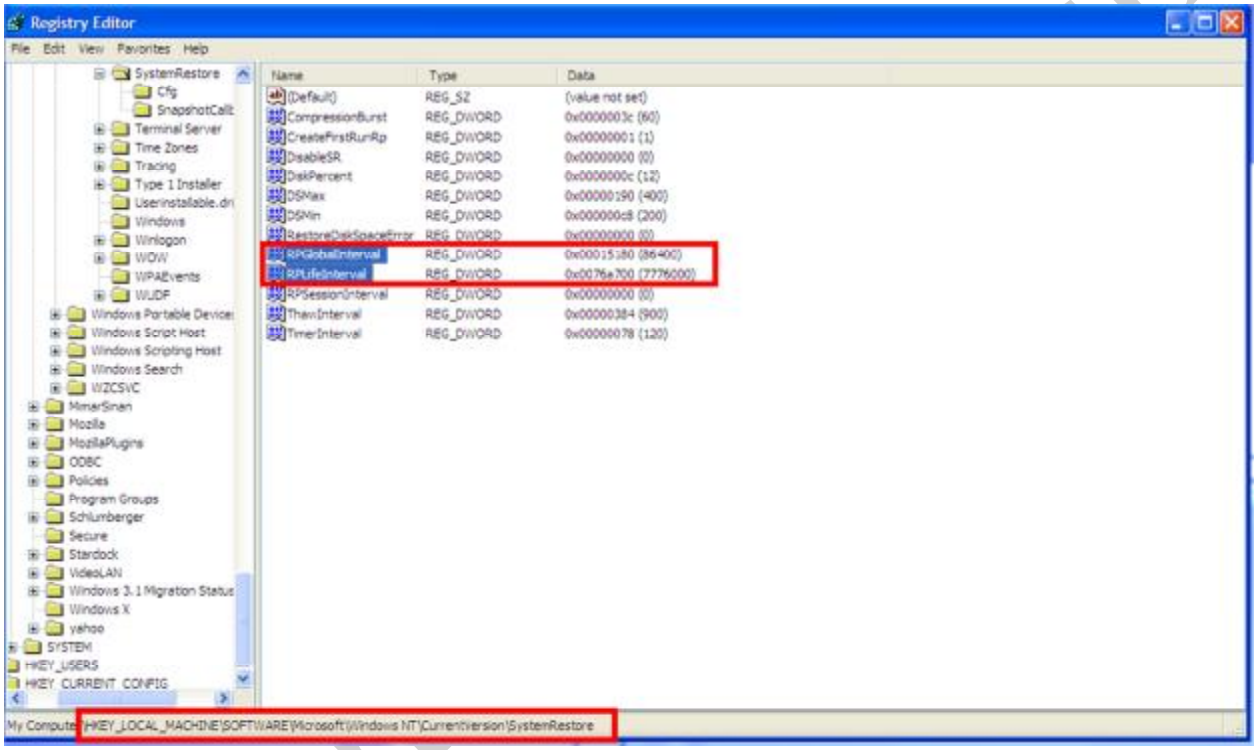
Restore Point ها در مواقع زیر ساخته می شوند:

1) هر 24 ساعت یکبار
2) هنگام بروز رسانی ویندوز
3) موقع نصب نرم افزار
4) به صورت دستی

Fars

برای اینکه بتوانیم تنظیمات System Restore را تغییر دهیم باید وارد رجیستریشویم و مسیر زیر را دنبال کنیم

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRestore #
```

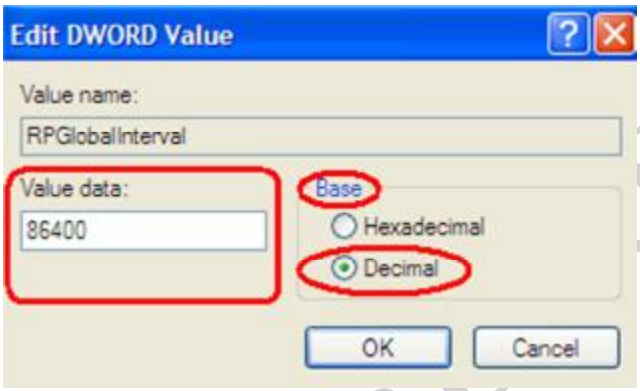



سپس دو مقدار به نا م های RPGlobalInterval و RPLifeInterval وجود دارند.

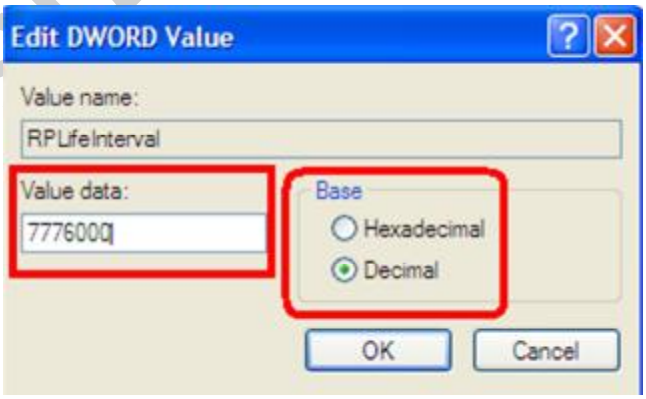
RPGlobalInterval: برای اینکه بتوانیم زمان ساخته شدن Restore Point را که به صورت پیش فرض هر 24 ساعت است را تغییر دهیم از این گزینه استفاده می کنیم.

RPLifeInterval :برای اینکه بتوانیم زمان نگهداری Restore Point را که بصورت پیش فرض 90 روز(درXp ) و137 روز(در7) است را تغییر دهیم از این گزینه استفاده می کنیم .

به خاطر داشته باشید که برای تغییر در دو متغیر بالا، زمان را باید به ثانیه وارد کنیم (هر روز 86400 ثانیه است) و برای اینکه مقدار ثانیه را وارد کنیم Base باید روی Decimal تنظیم باشد مانند شکل 1 که مدت ثانیه ما (Value Data ) برابر یک روز است و در شکل 2 که مدت ثانیه ما برابر 90 روز می شود.




شکل 1




شکل2

FarshidAjamoush

تکنولوژی ها و بسترهای لازم برای Remote :

از تکنولوژی های Remote می توان به موارد زیر اشاره کرد:

| | | | |
|---|---|---|---|
| 1) Remote Desktop | 3) Telnet | 5) IIS | 7)VPN |
| 2) Remote Assistance | 4) SSH | 6) FTP | |

به تکنولوژی های 1و2 RDP(Remote Desktop Protocol) گویند.

از بسترهای Remote می توان به موارد زیر اشاره کرد:

| | | |
|---|---|---|
| 1) PSTN ( Public Switching Telephone Network) | 3) DSL | 5)LESED LINE |
| 2) ISDN | 4) CA TV | 6) WIRELESS |

- به مرکز مخابراتی که آنالوگ باشد PSTN گویند و سرعتی برابر 56 Kbps دارند ولی سرعت واقعی آنها برابر 32 Kbps است.
- به مرکز مخابراتی که دیجیتال باشدISDN گویند و سرعتی برابر 128Kbps دارند.
- DSL به5 کلاس تقسیم می شود:1) ADSL (2 VDSL(3 BDSL (4 HDSL (5 SDSL

کابل های خطوط تلفن Cat3 است که فرکانسی برابر 1 MHz دارند، فرکانس صدای انسان برابر4 Hz است به همین دلیل است که می توان از خطود تلفن هم صدای انسان را ارسال و دریافت کرد و هم اطلاعات را ارسال و دریافت کرد.

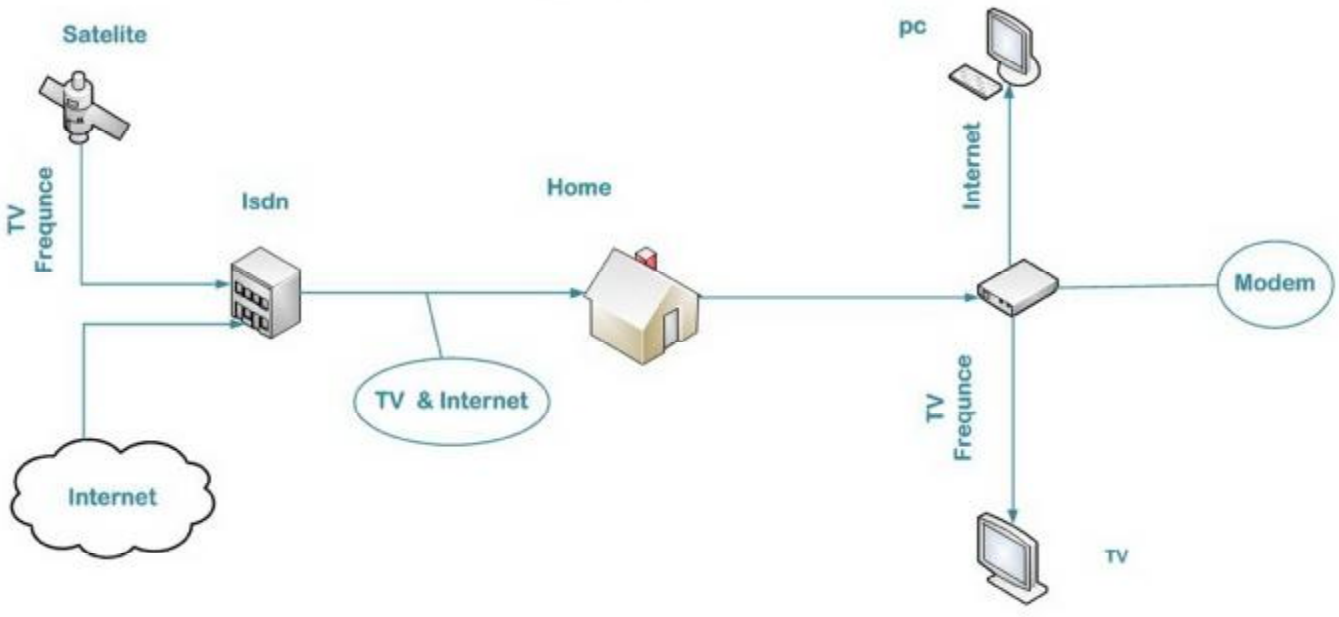
CAT 3 CABLE

FarshidAjabnoush

| نوع | حداکثر سرعت | متراژ قابل پشتیبانی |
|---|---|---|
| ADSL | 8 MG | 6 کیلومتر |
| ADSL 2 | 10 MG | 3 کیلومتر |
| ADSL 2+ | 24 MG | 2کیلومتر |

CA TV (Cable TV):

در این تکنولوژی اینترنت و شبکه تلویزیون روی یک کابل به خانه ها فرستاده می شوند به این ترتیب که تلویزیون های خصوصی یک ماهواره در مدار زمین به فضا می فرستند وشبکه ها خودشان را، روی این ماهواره ها قرار می دهند سپس در مخابرات دیش ریسیو می گذارند و امواج را دریافت می کنند، سپس مخابرات اینترنت هم در کنارش قرار می دهد و توسط کابل به محل مورد نظر میفرستد.(70% شبکه های تلویزیونی آمریکا خصوصی هستند و از این تکنولوژی استفاده می کنند)




Ajabnoush

:LESED LINE

**مانند خطوط E1 ، و بر 2 استاندار E برای اروپا و T برای آمریکا هستند.**

:WIRELESS

**اساس کار شبکه های بیسیم مبتنی بر فرکانس رادیویی RF(Radio Frequency) می باشد .**

**دو شرکت IEEE و FCC تمامی کارهای مربوط به وایرلس دنیا را انجام می دهند.**

: IEEE

**کار این شرکت تعیین استاندارد است.**

| IEEE | |
|---|---|
| **نوع استاندارد** | **کد استاندارد** |
| WLAN | 802.11 |
| WMAN (WIMAX) | 802.16 |
| WPAN(BLUETHOTH) | 802.15 |

**یک نوع دیگر از استاندارد وجود دارد به نام WWAN که توسط آن کل دنیا به وسیله ماهواره ها با هم در ارتباط هستند.**

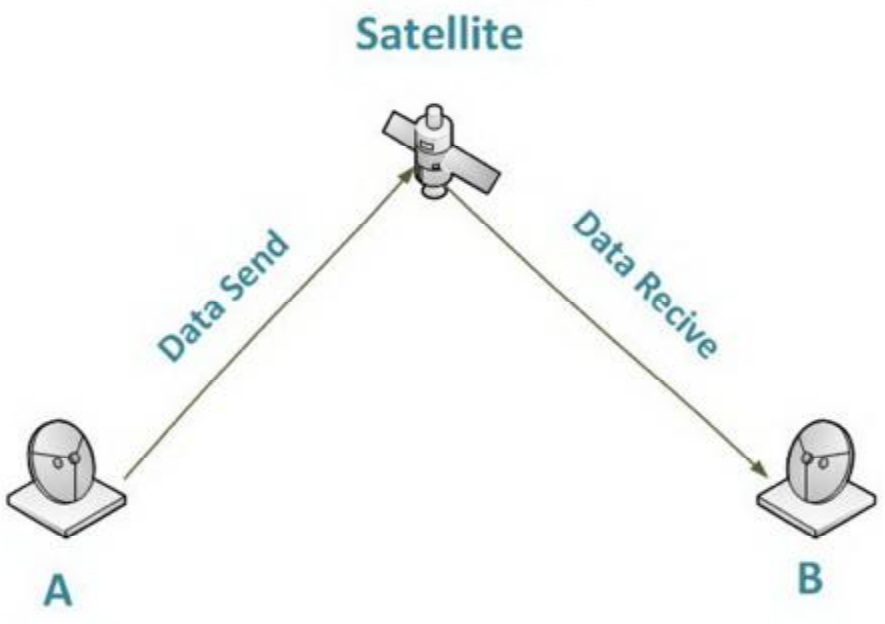
Farshidjabnoush

: WWAN

**این نوع از تکنولوژی ارتباط خود به دو دسته Satellite و V sat تقسیم می شود.**

: Satellite

**زمانی که بخواهیم از دو نقطه دور، همانند دو نقطه مختلف از دنیا با هم ارتباط برقرار کنیم از این تکنولوژی استفاده می کنیم ، فرض کنید که می خواهیم از یک نقطه از دنیا به نام A اطلاعاتی را به نقطه دیگری از دنیا به نام B ارسال کنیم،ابتدا یک ماهواره در فضا در مدار زمین قرار می دهیم سپس نقطه A باید اطلاعاتی را که برای نقطه B می خواهد ارسال کند،به این ماهواره بفرستد و نقطه B هم باید اطلاعات را از ماهواره دریافت کند.(همانند گزارش زنده جام جهانی)**



: V sat

**این نوع تکنولوژی همانند تکنولوژی Satellite است با این تفاوت که در این نوع تکنولوژی دیگر احتیاجی به ماهواره در فضا نداریم و دو نقطه به طور مستقیم ( Point To Point ) با هم ارتباط برقرار می کنند این نوع از تکنولوژی برای فواصلی که موانع بلند همانند کوه بین دونقطه نباشد  مناسب است(دیش های بانک ها)**

Farsroush

: FCC

کار این شرکت تعیین رنج فرکانسی برای شبکه های وایرلس است،شبکه های وایرلس مبنتنی بر 2 فرکانس GHz2/4 وGHz5 می باشند.

- فرکانس شنوایی انسان 20 Hz - 20 KHz می باشد.
- فرکانس صدای انسان 0 Hz - 4 KHz می باشد.
- فرکانس صدای مورچه ها بالای 20 KHz می باشد.
- فرکانس بیسیم پلیس GHz2/4 می باشد.

| سرعتاستاندارد | نوع استاندارد |
|---|---|
| 11 Mbps(مگا بیت) | 80211.B |
| 54 Mbps | 80211.A |
| 54 Mbps | 80211.G |
| 560(In book) = 300 Mbps (Real) | 80211.N |

- استاندارد N از سال 2007 طراحی شد.

با پروتکل هایWEP- WPA – WPA2 می توان بر روی شبکه های وایرلس ایجاد امنیت کرد.

:WEP

با نرم افزار WEP CRACKمی تواناین پروتکل را هک کرد.

:WPA

با نرم افزار AIR CRACK می توان این پروتکل را هک کرد.

:WPA2

تا کنون کسی موفق به هک این پروتکل نشده است،به این دلیل که 90% از تجهیزات این پروتکل را پشتیبانی نمیکنند.

- برترین نرم افزار هک وایرلس Back Track 4می باشد که خود یک OS محسوب می شود.

FarshidAjamoush

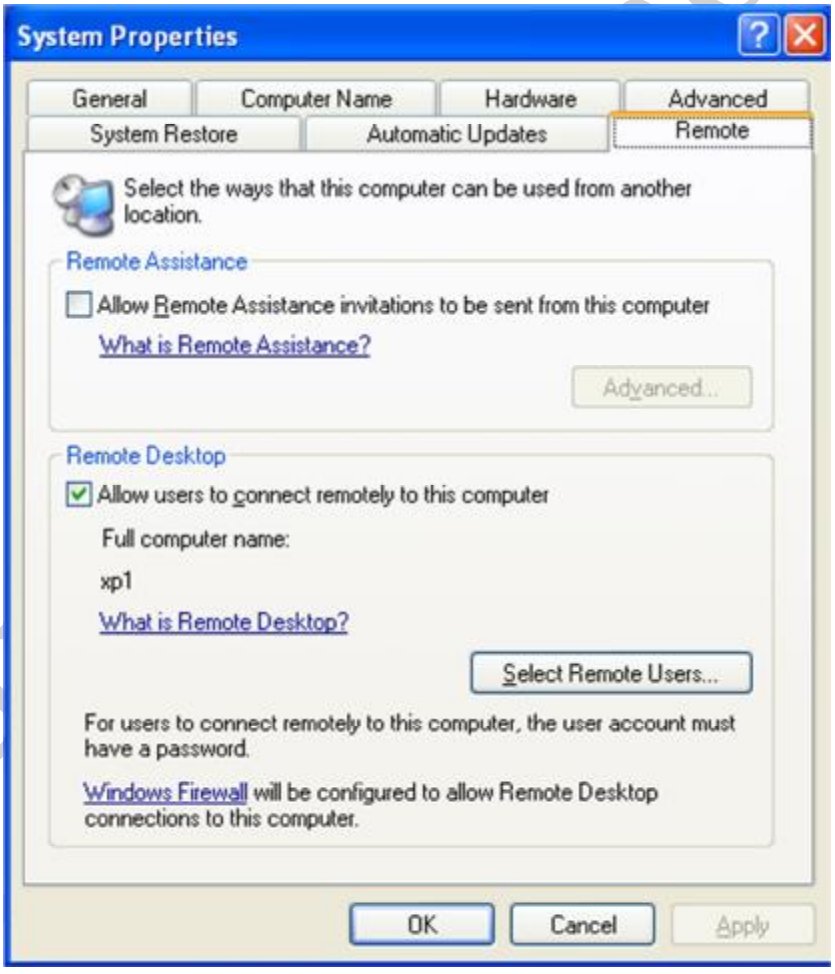
MPLS :

**یک نوع تکنولوژی ارتباط است،برای اتصال چند شبکه به یکدیگر مانند اتصال شعبه های یک فروشگاه به یکدیگر عیب این تکنولوژی گران بودن آن است.**

**پروتکل RDP :**

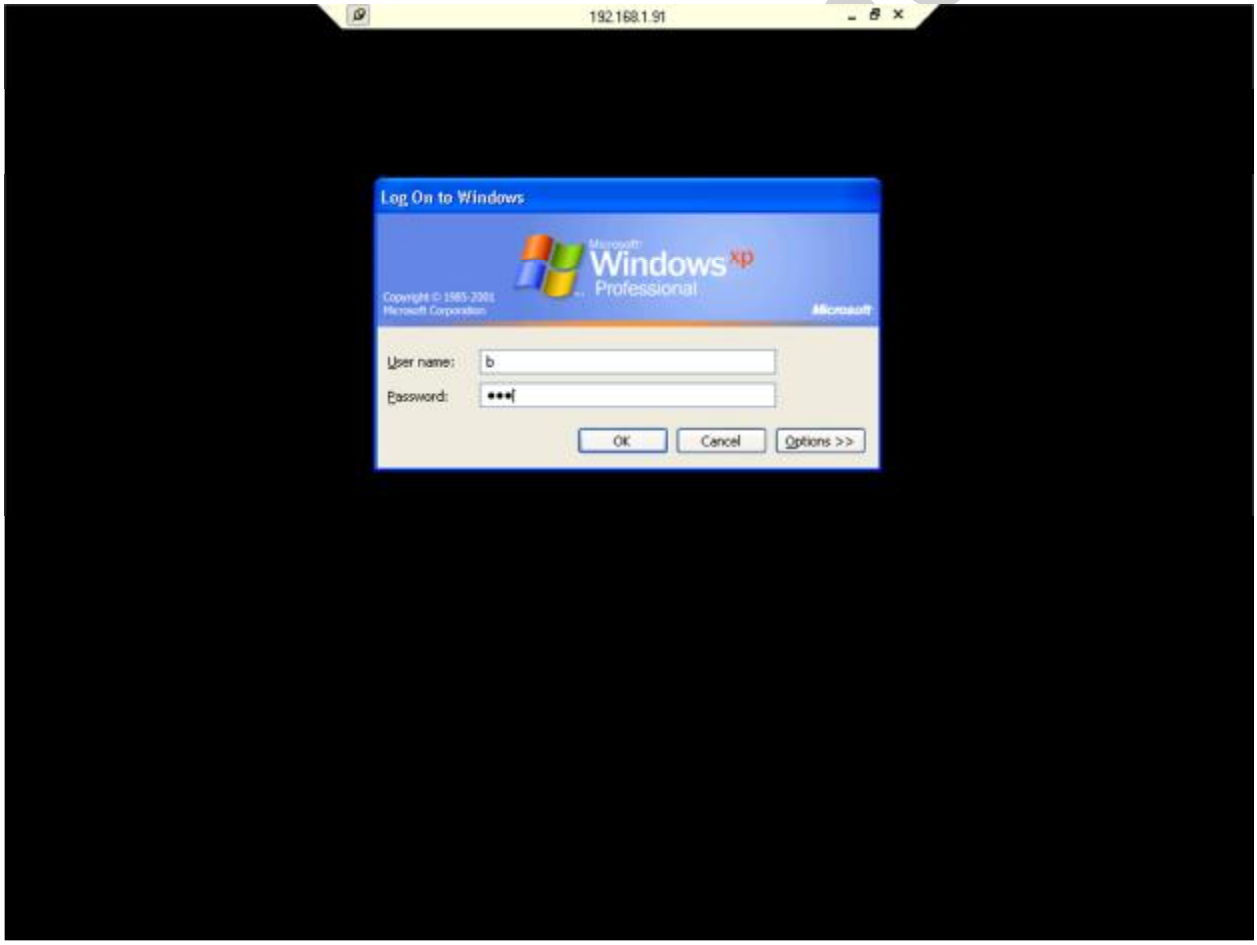
**از این پروتکل برای ریموت کردن استفاده می شود،برای ریموت کردن ابتدا باید در کامپیوتر مقصد تیک گزینه ریموت فعال باشد**

- **استفاده از پروتکل RDP در ویندوزهای NG وLAGACY کاملاً متفاوت است.**



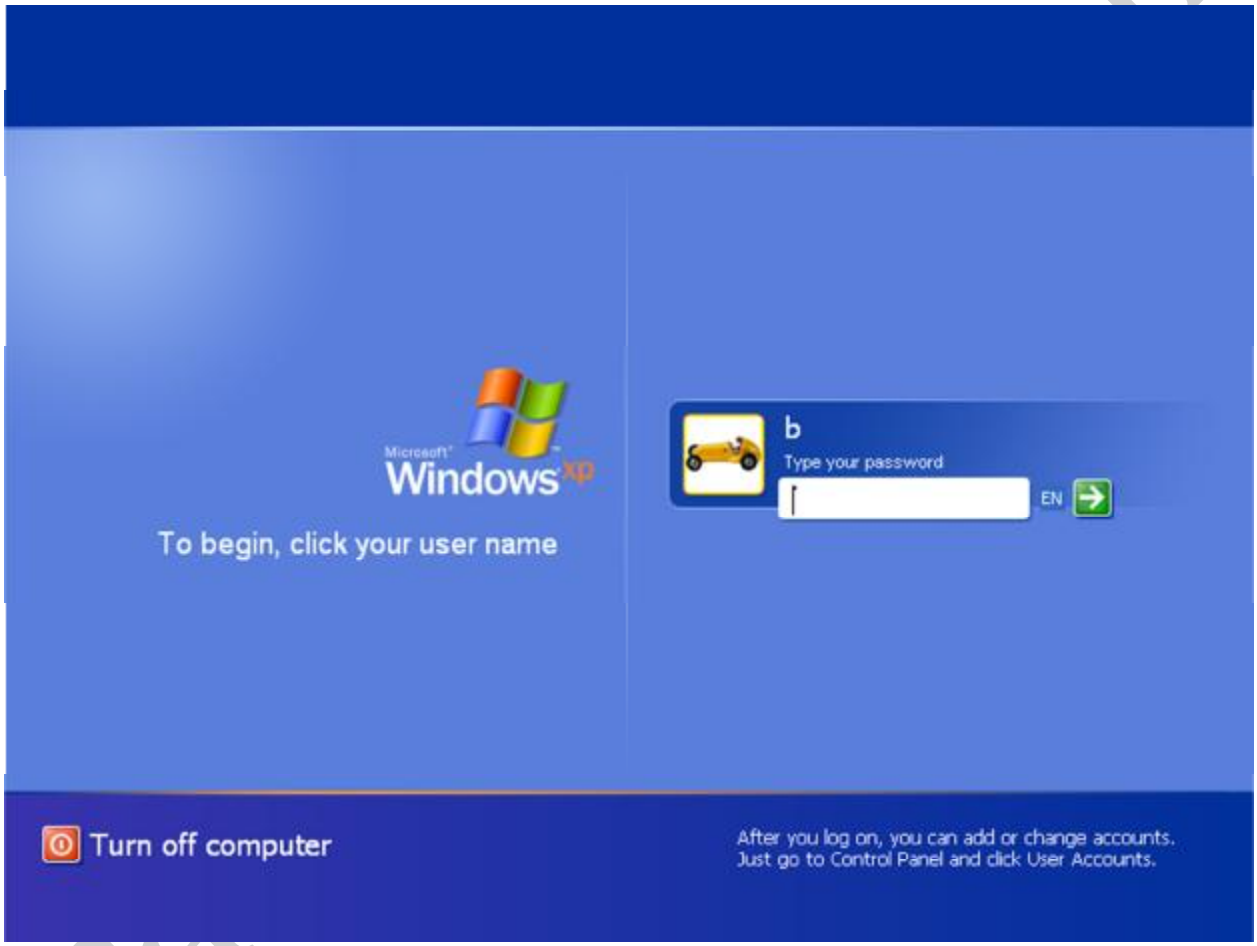

**سپس از کامپیوتر مبدا باید دستور MSTSC را وار کنیم،در کادر باز شده Ip سیستم مقصد را وارد می کنیم**

**بعد از وصل شدن به کامپیوتر مقصد باید نام کاربری و پسورد را وارد کنیم**



بزرگترین مشکل در ریموت کردن این است که فقط یک نفر می تواند به کامپیوتری که ریموت شده وصل باشد آن هم کامپیوتر ریموت کننده است،زمانی که کامپیوتری را ریموت می کنیم آن کامپیوتر به حالت Log off در می آید مانند شکل زیر :

البته این مشکل در نسخه های سروری ویندوز وجود ندارد




از این روش ریموتینگ بیشتر در شبکه های LAN استفاده می شود مانند اینکه در داخل یک ساختمان شبکه ای داشته باشیم و بخواهیم از یک کامپیوتر در طبقه اول به کامپیوتر دیگری در طبقه هفتم وصل بشویم از این روش استفاده می کنیم ولی اگر بخواهیم از بیرون این شبکه به آن متصل شویم پیشنهاد می شود از نرم افزارهای مخصوص ریموتینگ استفاده کنید( به دلیل سرعت بالاتر).

**تعدادی از نرم افزارهای برتر ریموتینگ:**

Log mein–Radmin–Team Viewer-Skype-Sert Party

**برای استفاده از این نرم افزار ها جهت ریموت کردن احتیاجی به**ValidIp**نداریم.**

**نرم افزار** Radmin **کنترل نامحسوس دارد یعنی اینکه طرف مقابل متوجه ریموت کردن ما نمی شود تنها مشکل این نرم افزار این است که** Agent **دارد یعنی یک نسخه از نرم افزار هم باید روی کامپیوتر مقصد نصب باشد.**

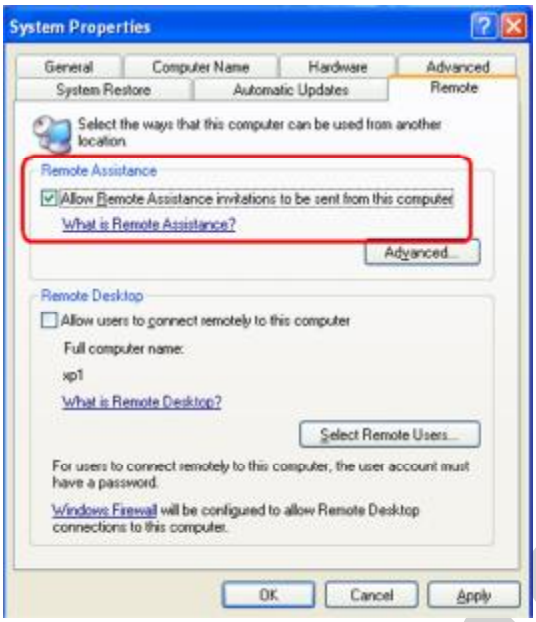
**نرم افزار** IDEAL ADMINISTRATOR **می تواند بدون** Agent **فقط با دانستن** Ip **کامپیوتر مقصد به آن وصل شود.**

**برای اینکه بتوانیم نرم افزار های مورد نیازمان را** Portable **(قابل حمل-بدون احتیاج به نصب) کنیم می توانیم از نرم افزار** VM WARE THIN APP **استفاده کنیم.**

Remote Assistant :

**این سرویس هم همانند** Remote Desktop **می باشد با این تفاوت که برای استفاده از این سرویس باید در** Hot Mail **عضو باشید و** Account **داشته باشید تا از این سرویس بتوانید استفاده کنید، طرز استفاده این سرویس همانند استفاده وب کم در یاهو می باشد با این تفاوت که شما به دسکتاپ کامپیوتر مقابل دسترسی دارید(استفاده از این سرویس منسوخ شده است)**

FarshidAjabnoush




همانطور که گفتیم ریموت کردن در ویندوزهای NG با ویندوزهای Legacy متفاوت است.

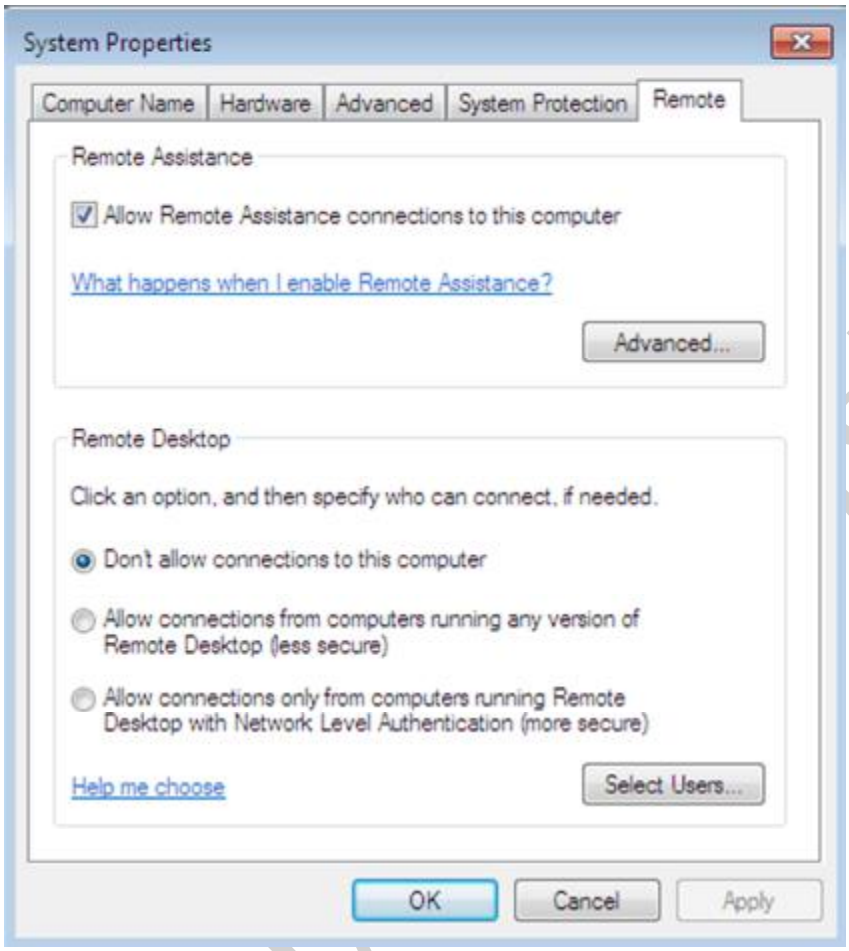
در صفحه ای که باید تیک گزینه ریموت را بزنیم گزینه هایی به شرح زیر دارد:

1) همانطور که مشخص است اجازه ریموت شدن را به هیچ کامپیوتری نمی دهد.
2) به هر کامپیوتری اجازه وصل شدن را می دهد، حتی سیستم هایی که NLA را ساپورت نمی کنند( XP )
3) به کامپیوتری اجازه وصل شدن می دهد که NLA را ساپورت کند.

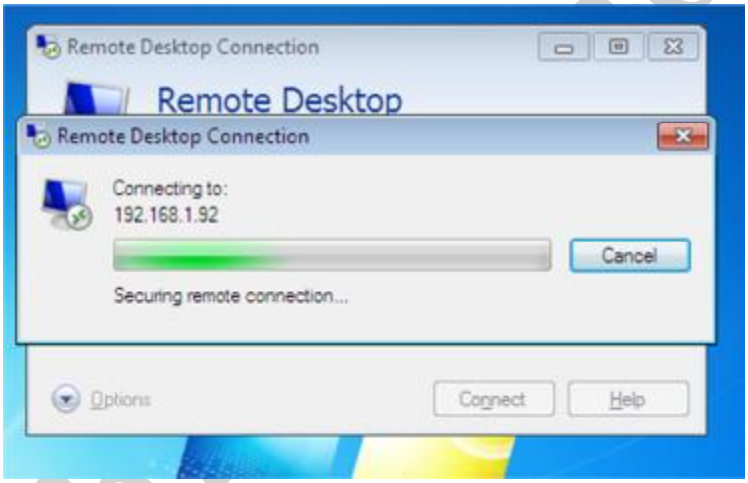
NLA ( Network Level Authentication ):

این خصوصیت در ویندوزهای NG می باشد،که باعث می شود زمانی که ما Ip کامپیوتر مقصد را وارد می کنیم بلافاصله از ما نام کاربری و رمز عبور را می خواهد بعد به سیستم وصل می شود ولی در Legacy به سیستم مقصد وصل شده وسپس نام کاربری و رمز عبور را می خواهد.

FarshidAjaboush



Farzad Nozarash




پورت پروتکل RDP 3389 است.

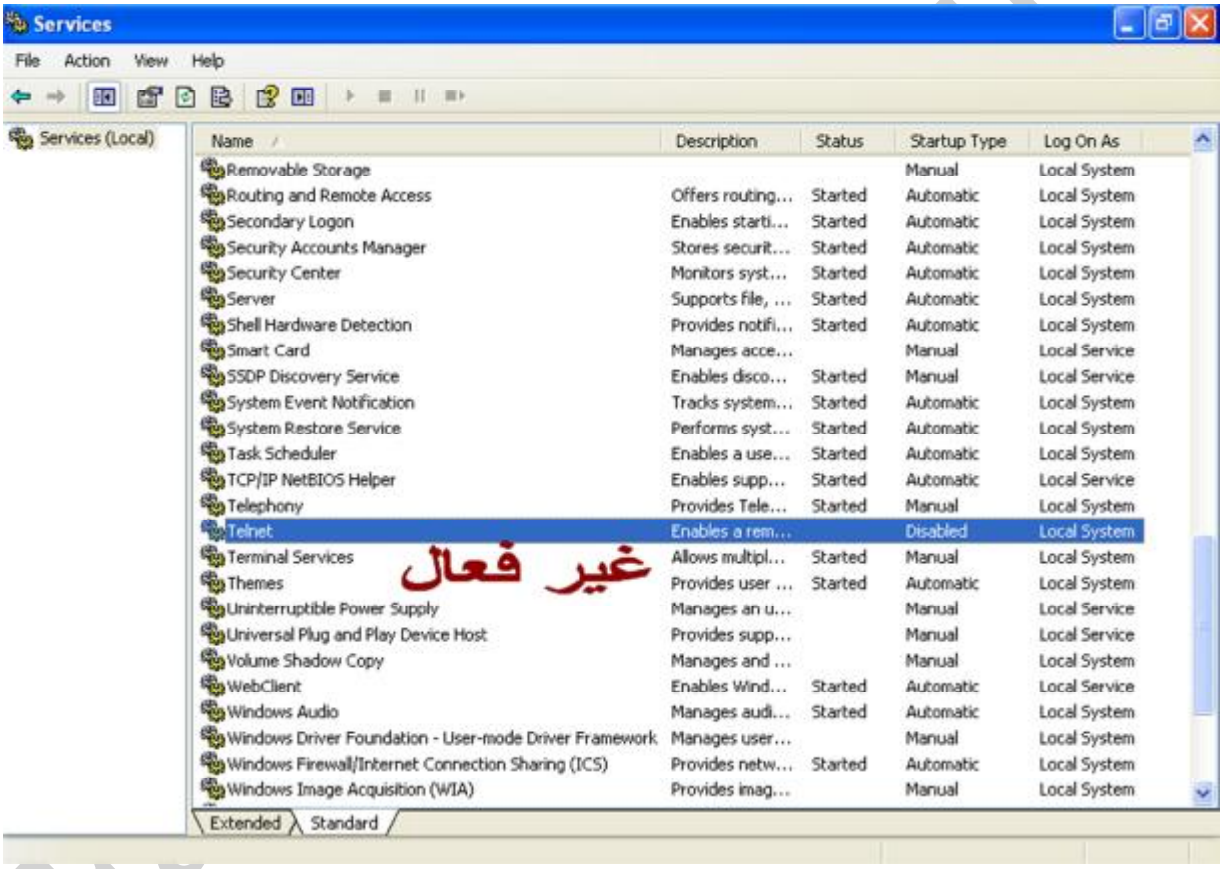
پروتکل Tel Net :

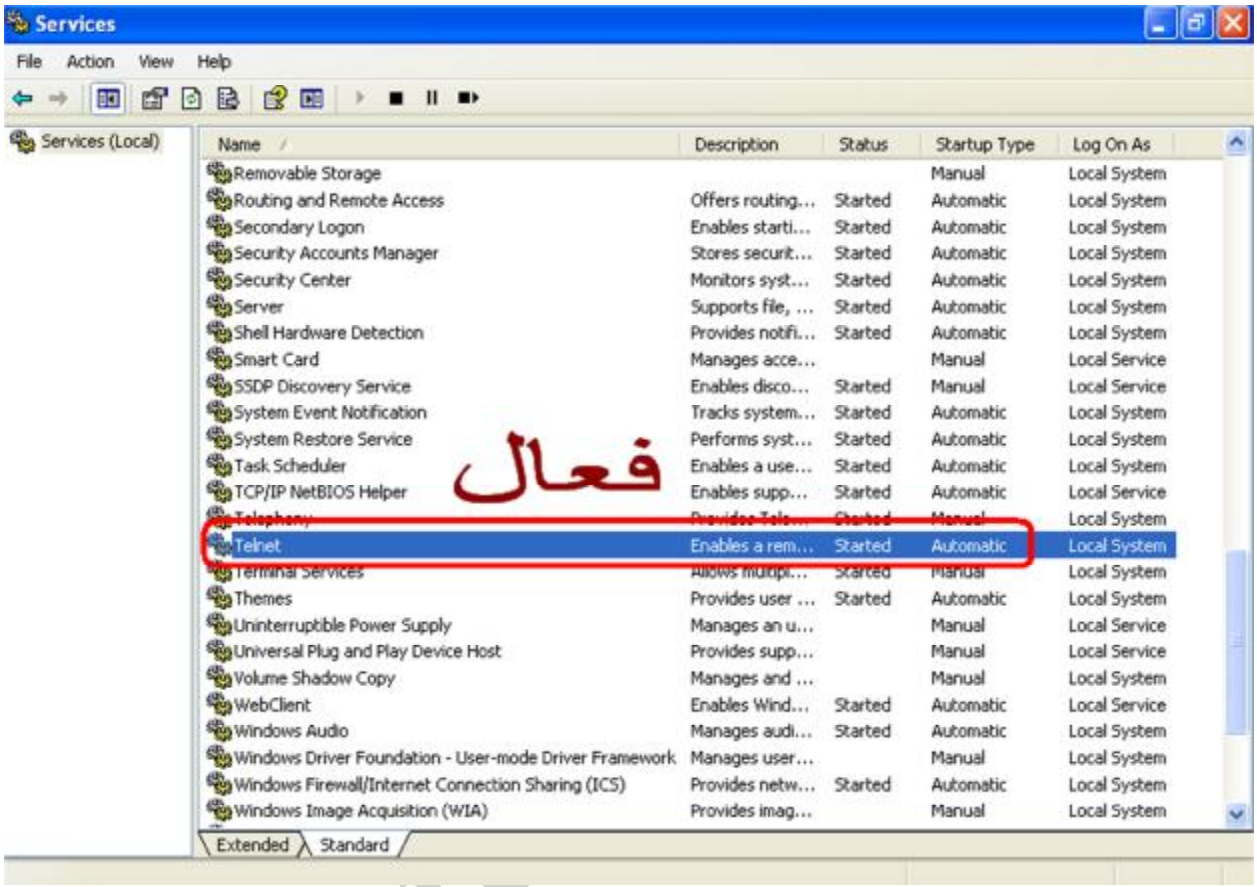
پروتکلی است برای مدیریت از راه دور سیستم ها بصورت کاملاً CLI ( Command Line Interface ) این پروتکل در ویندوزهای Legacy وجود دارد ولی باید فعال شوند اما در سیستم های NGبه صورت پیش فرضوجود ندارد.

Farshid Soroush

**فعال کردن Telnet در Legacy :**

**با وارد کردن دستور Services.msc در Run پنجره سرویس های ویندوز باز می شود سپس به سراغ سرویس Telnet رفته و آن را فعال می کنیم.**



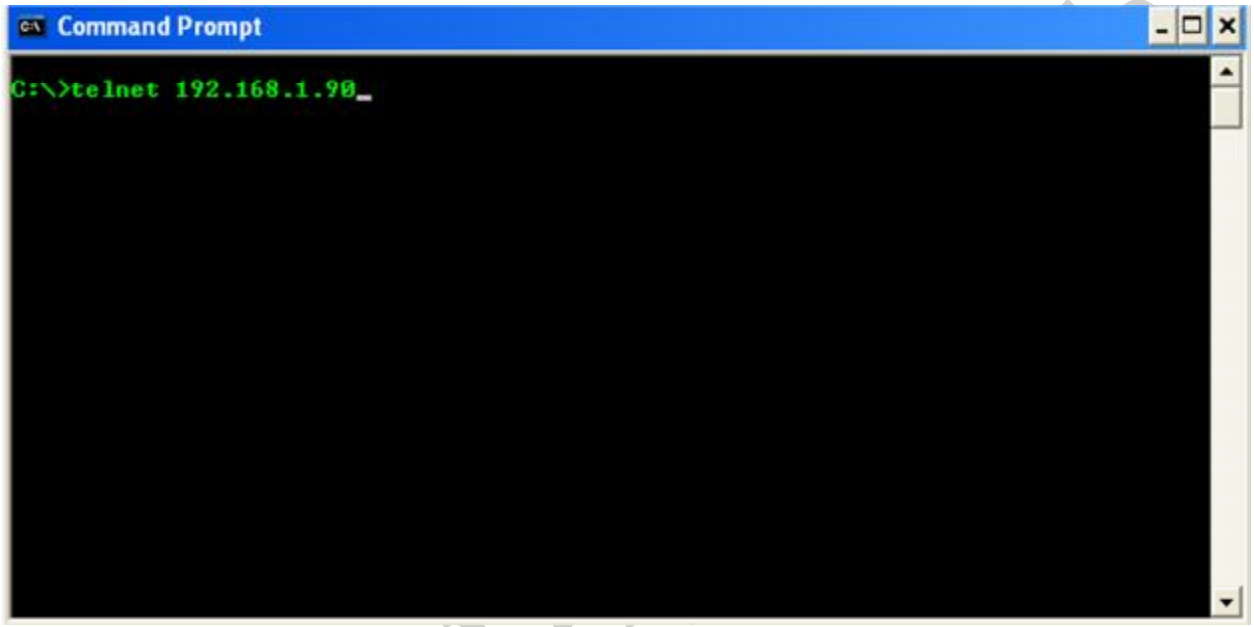

Services
File Action View Help
Services (Local)
Name
Description
Status
Startup Type
Log On As
Removable Storage
Manual
Local System
Routing and Remote Access
Offers routing...
Started
Automatic
Local System
Secondary Logon
Enables starti...
Started
Automatic
Local System
Security Accounts Manager
Stores securit...
Started
Automatic
Local System
Security Center
Monitors syst...
Started
Automatic
Local System
Server
Supports file, ...
Started
Automatic
Local System
Shell Hardware Detection
Provides notifi...
Started
Automatic
Local System
Smart Card
Manages acce...
Manual
Local Service
SSDP Discovery Service
Enables disco...
Started
Manual
Local Service
System Event Notification
Tracks system...
Started
Automatic
Local System
System Restore Service
Performs syst...
Started
Automatic
Local System
Task Scheduler
Enables a use...
Started
Automatic
Local System
TCP/IP NetBIOS Helper
Enables supp...
Started
Automatic
Local Service
Telephony
Manual
Local System
Telnet
Enables a rem...
Started
Automatic
Local System
Terminal Services
Started
Manual
Local System
Themes
Provides user ...
Started
Automatic
Local System
Uninterruptible Power Supply
Manages an u...
Manual
Local Service
Universal Plug and Play Device Host
Provides supp...
Manual
Local Service
Volume Shadow Copy
Manages and ...
Manual
Local System
WebClient
Enables Wind...
Started
Automatic
Local Service
Windows Audio
Manages audi...
Started
Automatic
Local System
Windows Driver Foundation - User-mode Driver Framework
Manages user...
Manual
Local System
Windows Firewall/Internet Connection Sharing (ICS)
Provides netw...
Started
Automatic
Local System
Windows Image Acquisition (WIA)
Provides imag...
Manual
Local System
Extended
Standard
فعال

Farshi

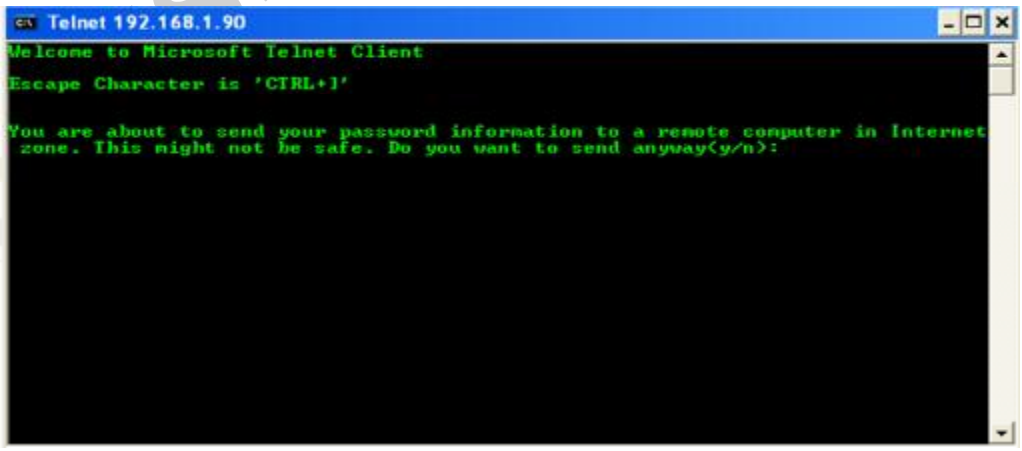
**استفاده از Telnet:**

**ابتدا وارد محیط CMD می شویم سپس دستور Telnet lp computer را وارد می کنیم**

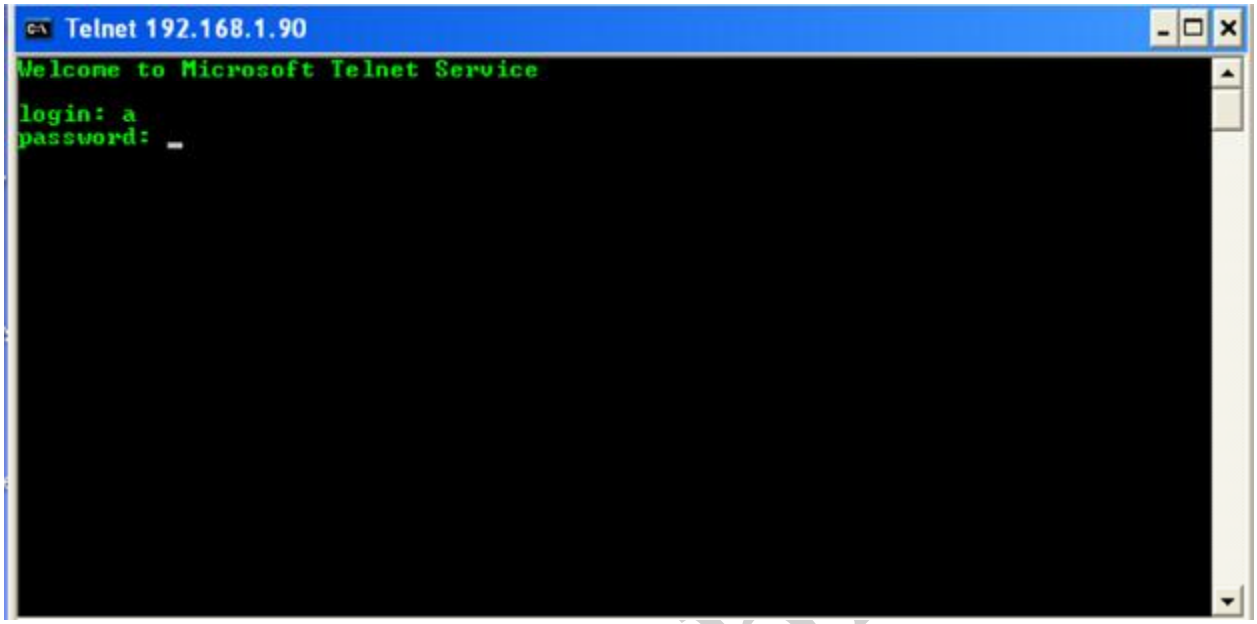
- **lp computer،lp سیستم مقصد می باشد.**



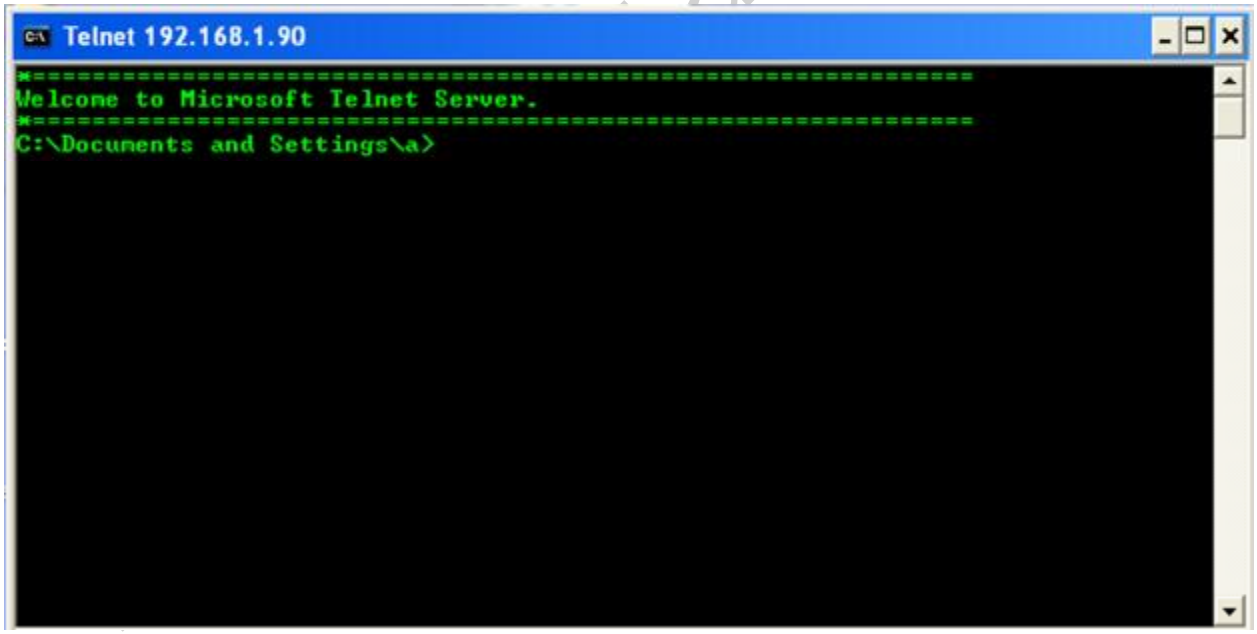

**سپس با هشداری روبرو می شوید که می گوید نام کاربری و کلمه عبوری را که وارد میکنی احتمال دارد کسی متوجه آن شود**



در مرحله بعد نام کاربری و کلمه عبور سیستم مقصد را می خواهد




و در نهایت وارد می شویم

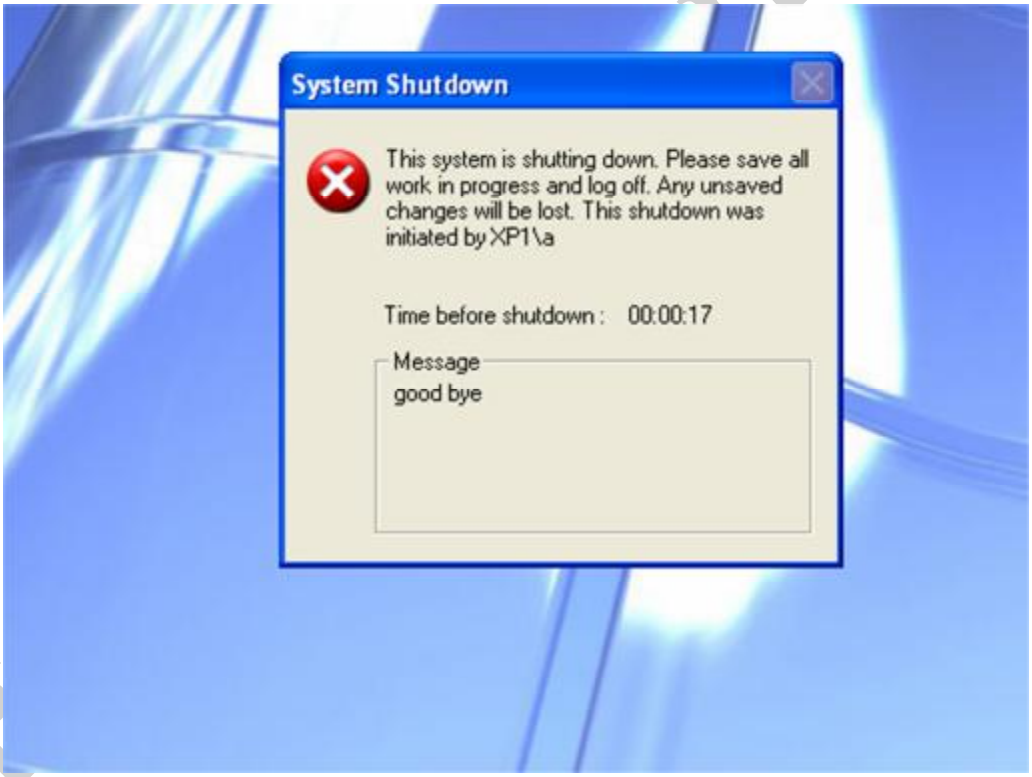


چند دستور کوچک برای کنترل سیستم مقصد:

خاموش کردن سیستم مقصد بعد از 20 ثانیه Shutdown -s -t 20

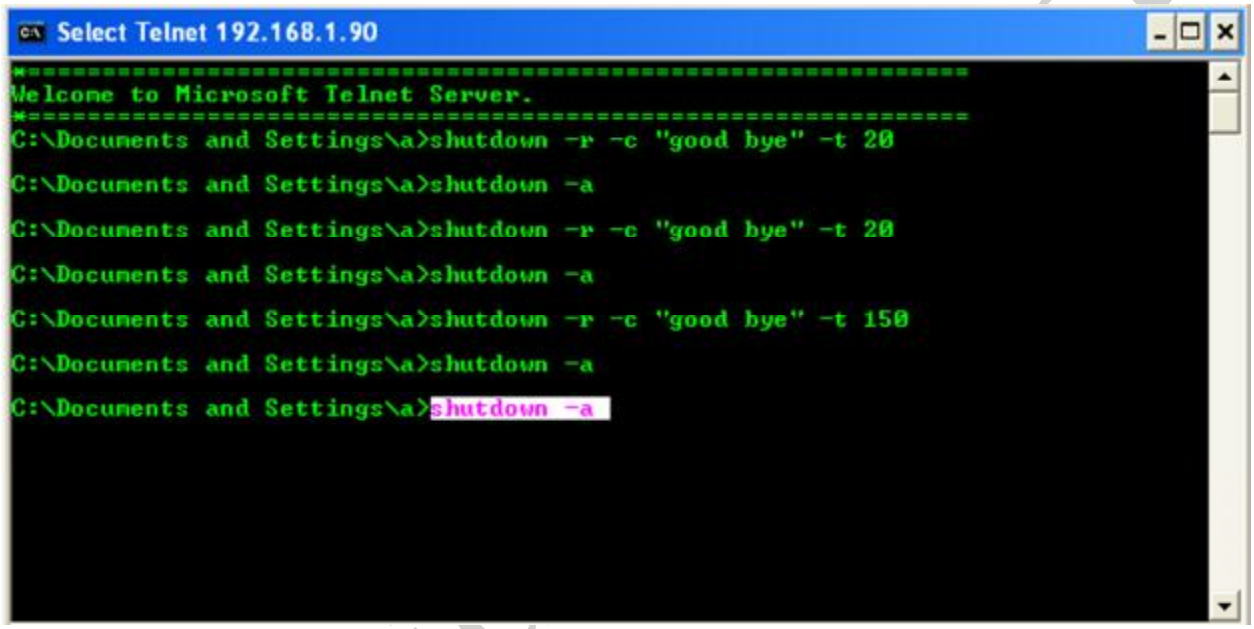
ریستارت کردن سیستم مقصد بعد از 15 ثانیه Shutdown -r -t 15

ریستارت کردن سیستم مقصد بعد از 17 ثانیه به همراه پیغامی برای کاربر Shutdown -r -c "Good Bye" -t 17




Farnoush

قبل از به اتمام رسیدن زمان اگر از دستورمان پشیمان شدیم با دستور Shutdown -a می توانیم دستورمان را غیر فعال کنیم.

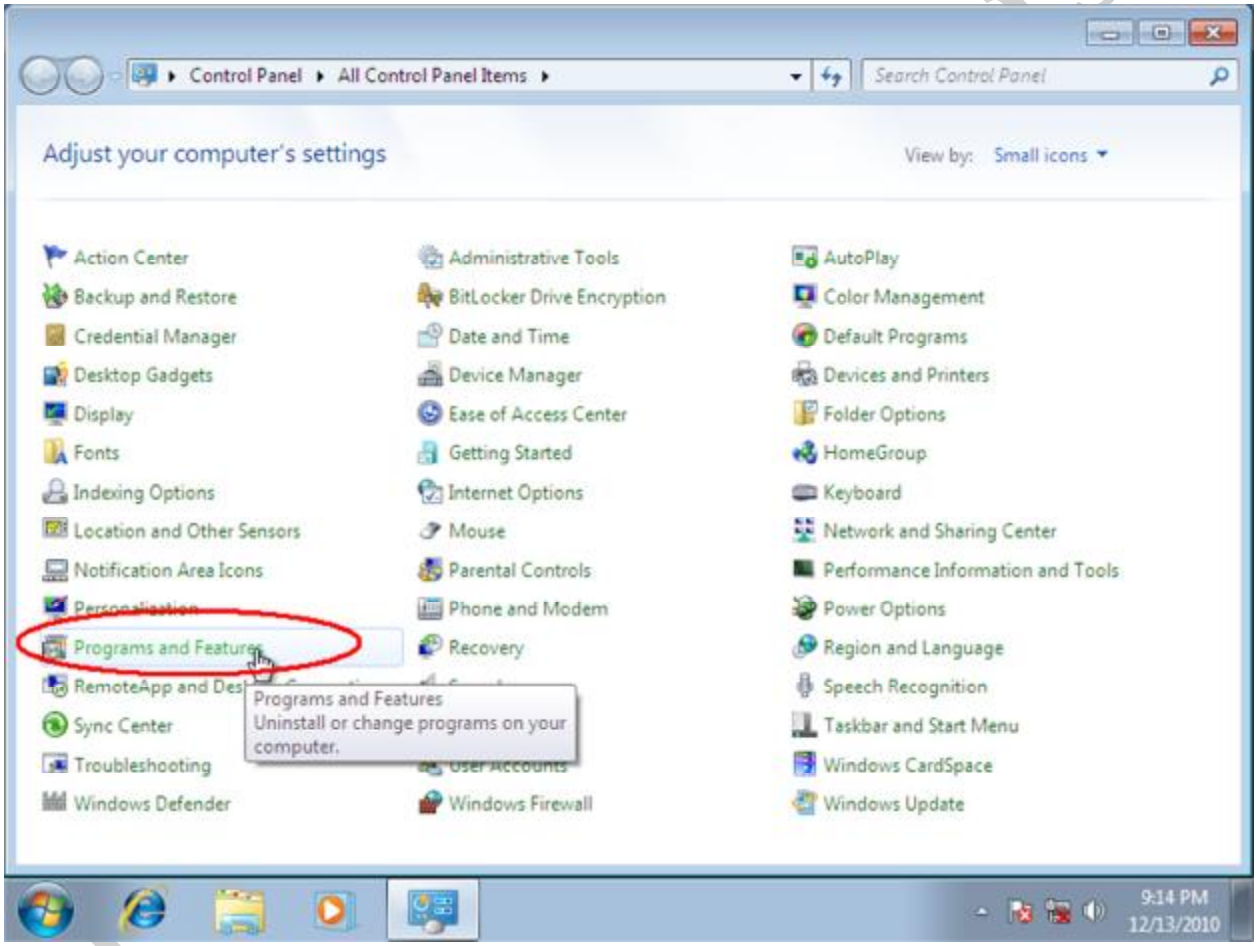


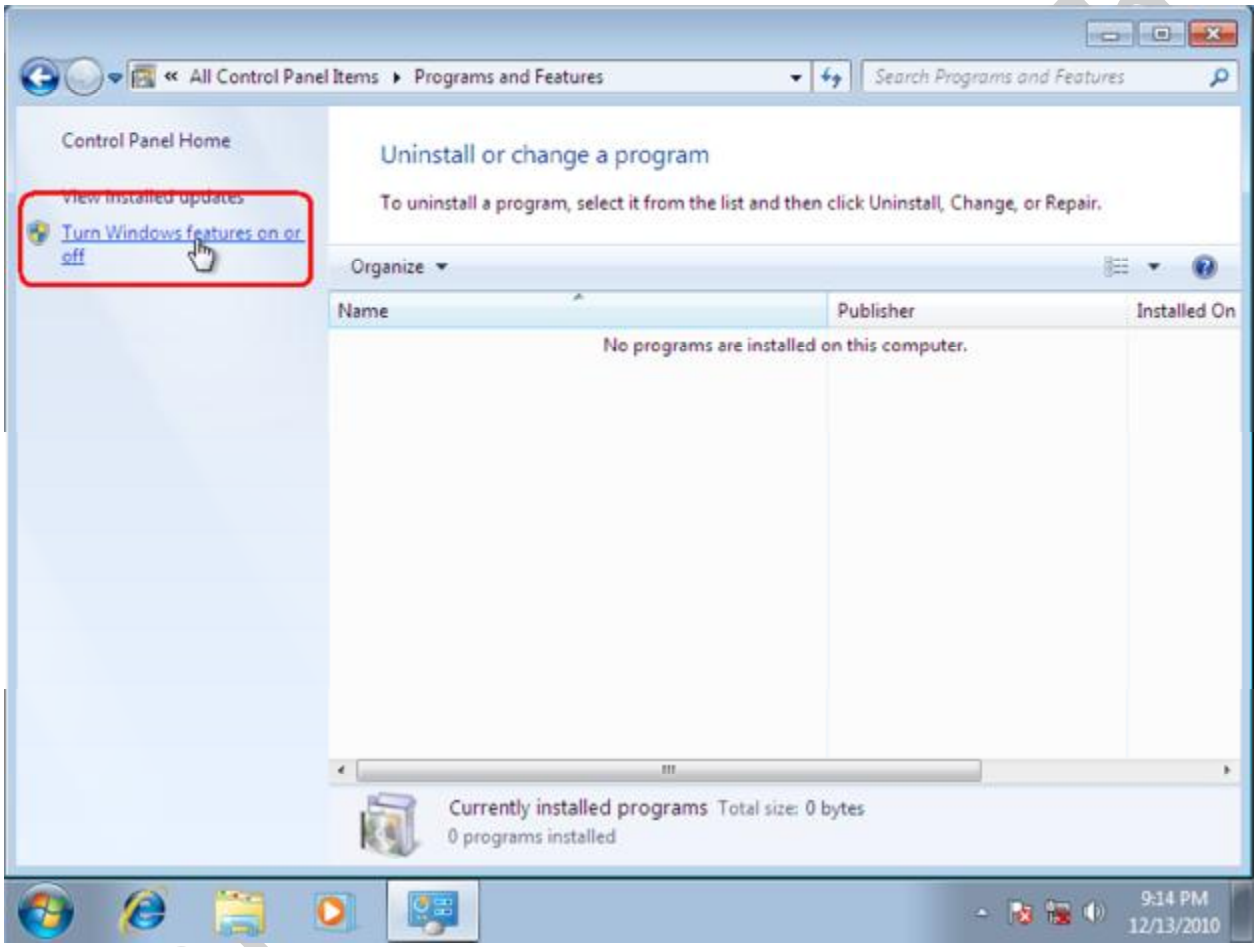

پروتکل Telnet اطلاعات را به صورت Clear Text (عبارات رمز نشده) ارسال ودریافت می کند به همین دلیل است که در ویندوزهای NG به صورت پیش فرض وجود ندارد.

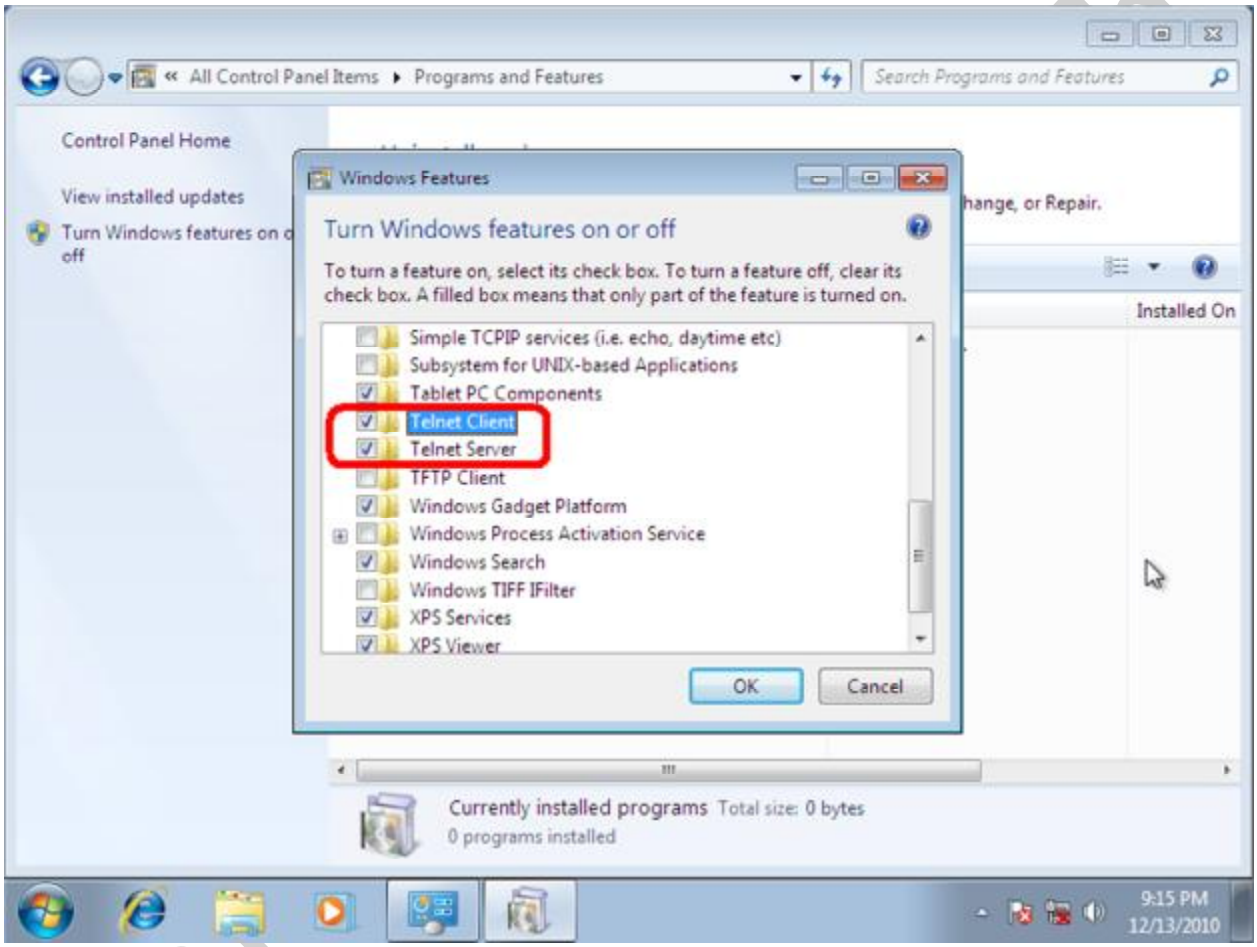
Farshid

فعال کردنTelnetدر ویندوز NG:

برای این کار ابتدا به کنترل پنل می رویم سپس گزینه Program & Features را باز می کنیم و از سمت چپ گزینه ای به نام Turn Windows Features on or off را باز می کنیم سپس از کادر باز شده گزینه های Telnet Server وTelnet Client را انتخاب می کنیم بعد از انجام این مراحل نوبت به فعال سازی سرویس Telnet از کنسول سرویس های مایکروسافت می باشد( Services.msc ) بقیه مراحل هم مانند ویندوزهای Legacy می باشد.




« All Control Panel Items ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Uninstall or change a program
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.
Organize
Name
Publisher
Installed On
No programs are installed on this computer.
Currently installed programs Total size: 0 bytes
0 programs installed
9:14 PM
12/13/2010


« All Control Panel Items ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
Simple TCPIP services (i.e. echo, daytime etc)
Subsystem for UNIX-based Applications
Tablet PC Components
Telnet Client
Telnet Server
TFTP Client
Windows Gadget Platform
Windows Process Activation Service
Windows Search
Windows TIFF IFilter
XPS Services
XPS Viewer
OK
Cancel
Installed On
Currently installed programs Total size: 0 bytes
0 programs installed
9:15 PM
12/13/2010

Fa

پروتکل SSH( Secure Shell ) :

این پروتکل دقیقاً همانند Telnet می باشد فقط با این تفاوت که در این پروتکل برخلاف Telnetاطلاعات بصورت Cipher(رمز گذاری شده)ارسال ودریافت می گردد.

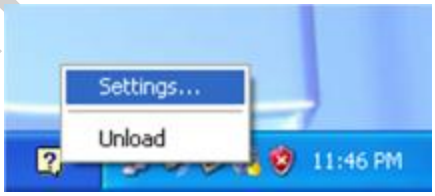
- برای استفاده از پروتکل SSH باید از نرم افزار استفاده کنیم.

باید روی کامپیوتر مبدا نرم افزار PUTTY و روی کامپیوتر مقصد نرم افزار FREE SSHD نصب باشد.

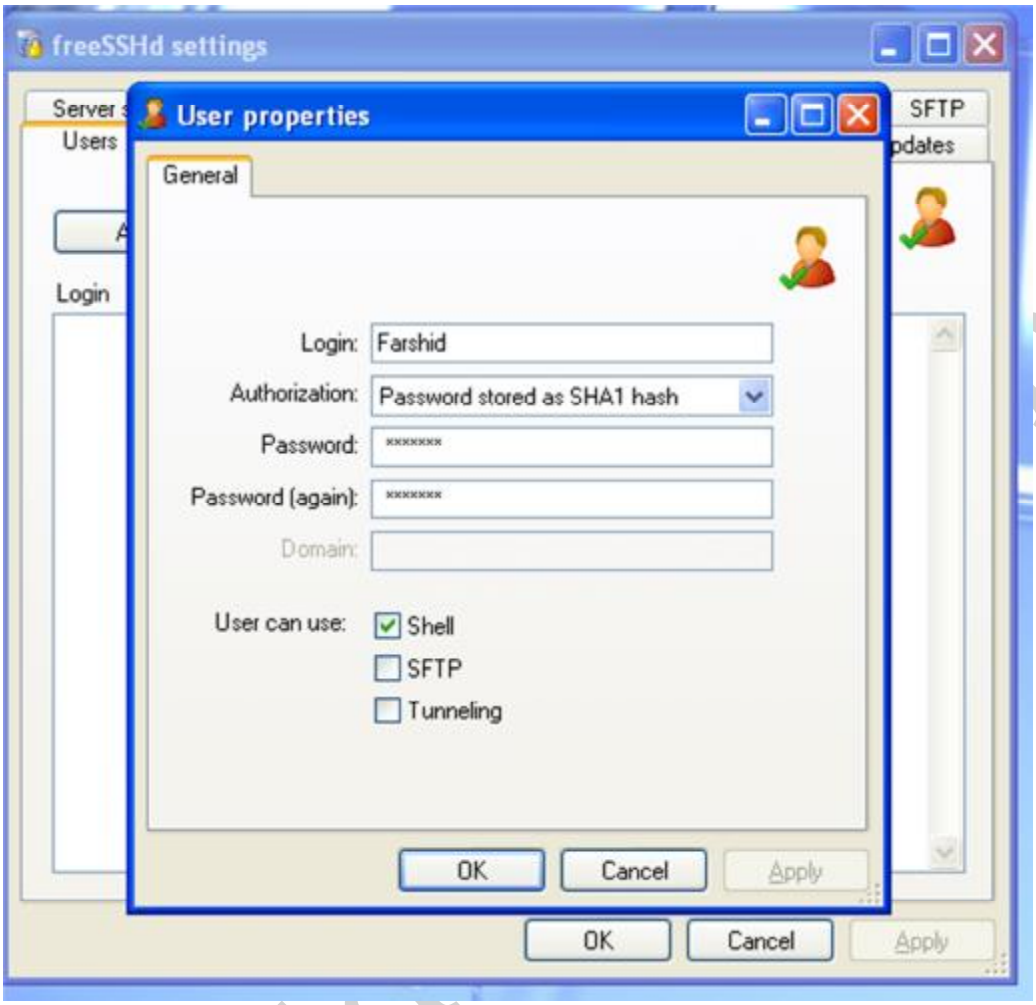
- ابتدا باید کامپیوتر مقصد را تنظیم کنیم.

کامپیوتر مقصد:

بعد از نصب نرم افزار FREE SSHD به سراغ تنظیم کردن نرم افزار می رویم،روی تنظیمات نرم افزار کلیک می کنیم وارد تب User می شویم و آنجا یک نام کاربری می سازیم




FarshidAjabnoush

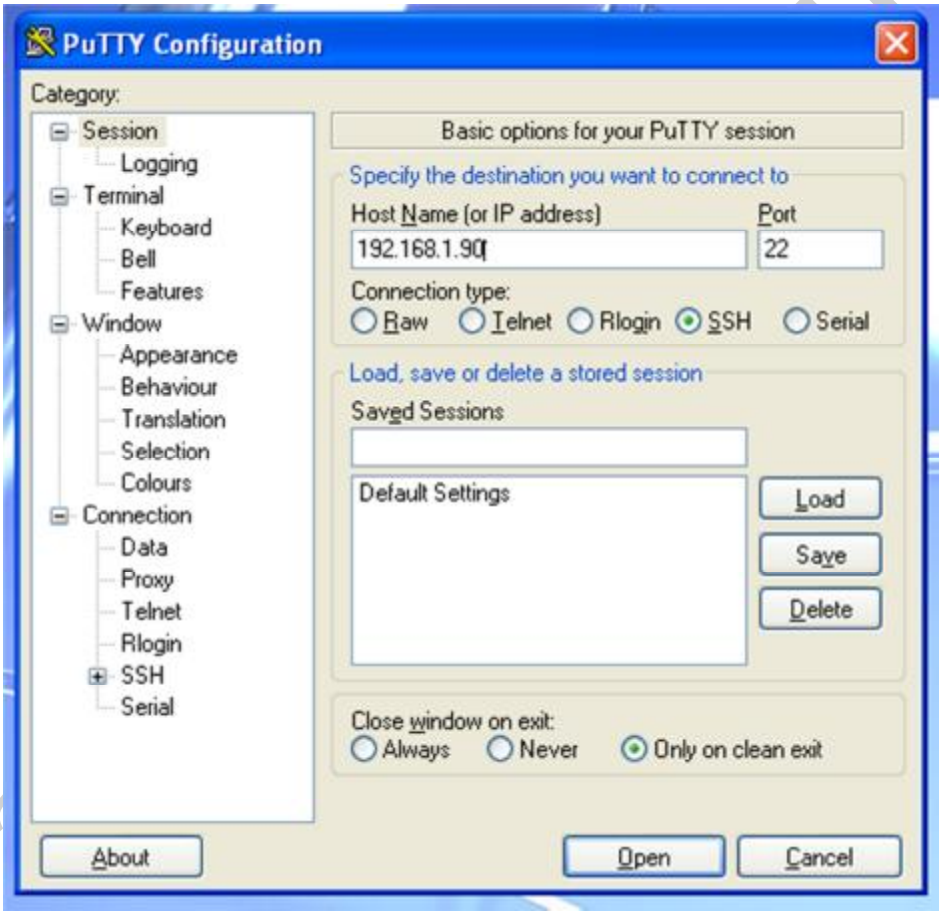


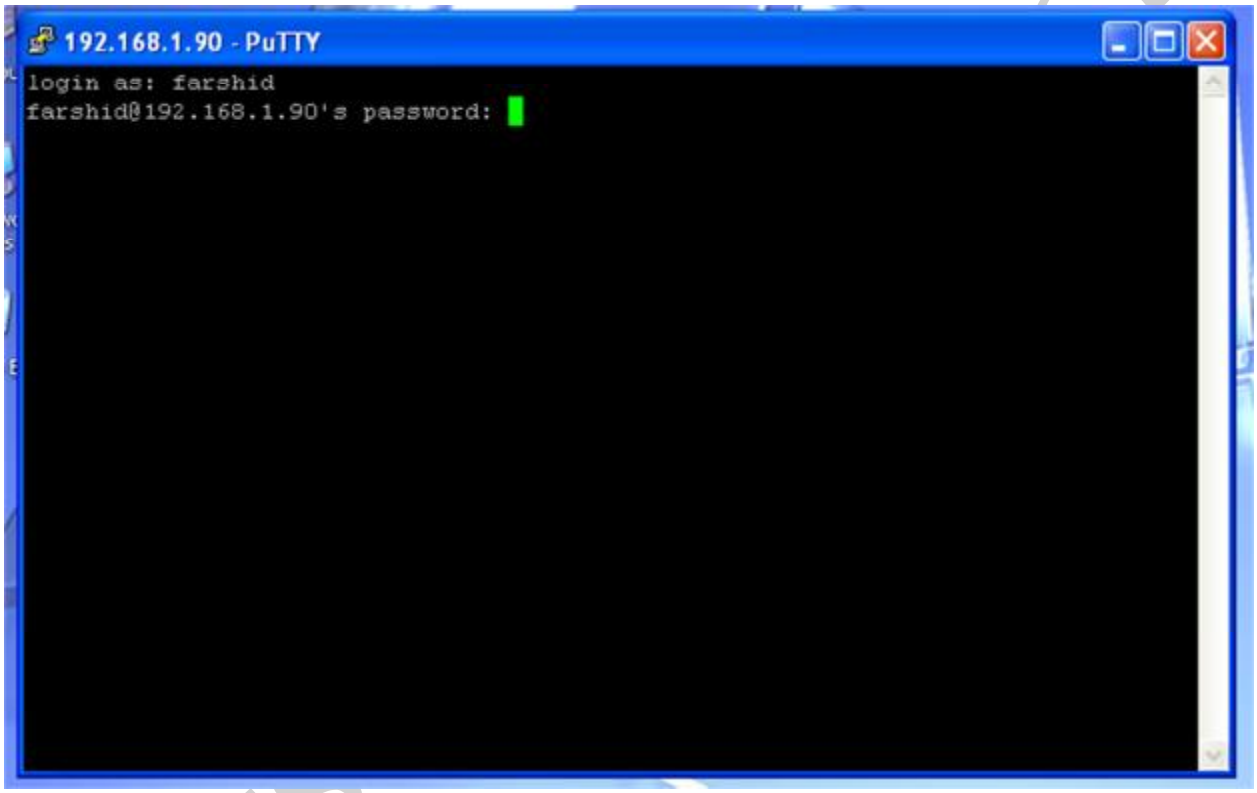

**در هنگام ساختن نام کاربری، گزینه Authorization را همانند شکل تنظیم کنید چون باعث می شود نام کاربری که ساخته می شود فقط در این نرم افزار بکار می رود و در سیستم شما ایجاد نشود.**

Farshid

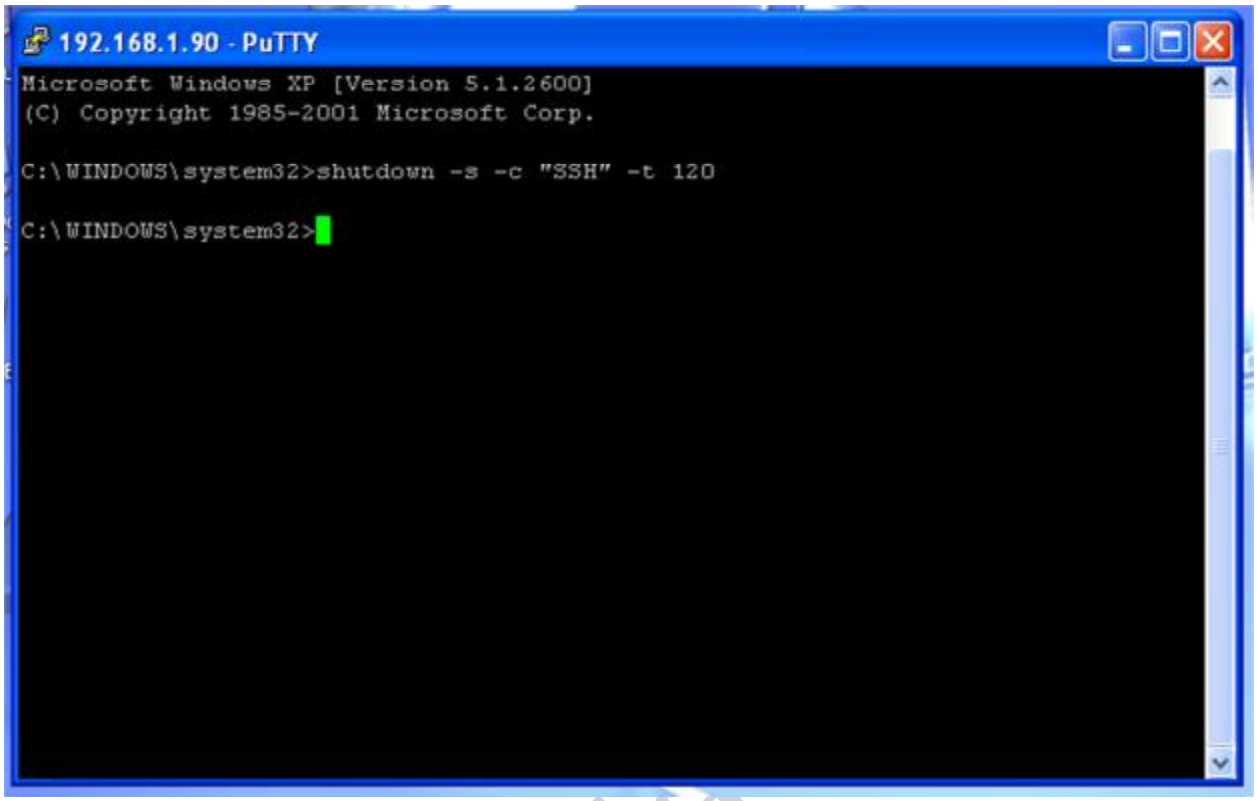
سیتم مبداً:

بعد از نصب نرم افـزار PUTTY بـه سـراغ تنظـیم کـردن نـرم افـزار مـی رویـم،در قسـمت Ip Address بایـد Ip سیسـتم مقصـد را وارد کنـیم سـپس پنجـره ای در محـیط Command بـاز مـی شـود کـه بایـد در آنجـا نـام کـاربری و رمـز عبـوری را کـه در نـرم افـزار FREE SSHD بـر روی کـامپیوتر مقصـد سـاخته بـودیم وارد کنـیم سپس به کامپیوتر مقصد وصل می شویم و بقیه مراحل همانند Telnet اجرا می شود.




192.168.1.90 - PuTTY
login as: farshid
farshid@192.168.1.90's password:

Farshid


192.168.1.90 - PuTTY
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>shutdown -s -c "SSH" -t 120
C:\WINDOWS\system32>

System Shutdown
This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM
Time before shutdown : 00:01:54
Message
SSH

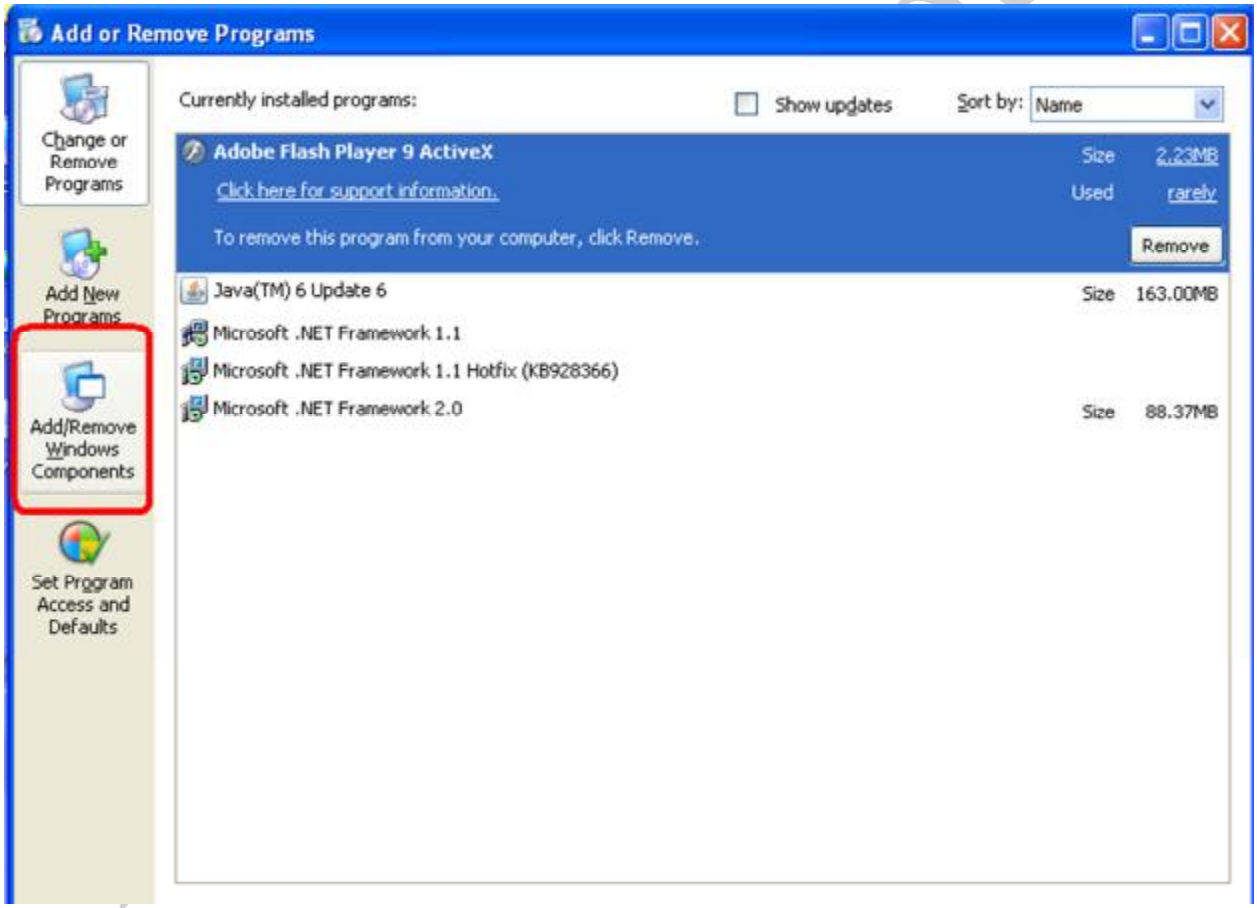
FarhidAja

پروتکل IIS ( Internet Information Service):

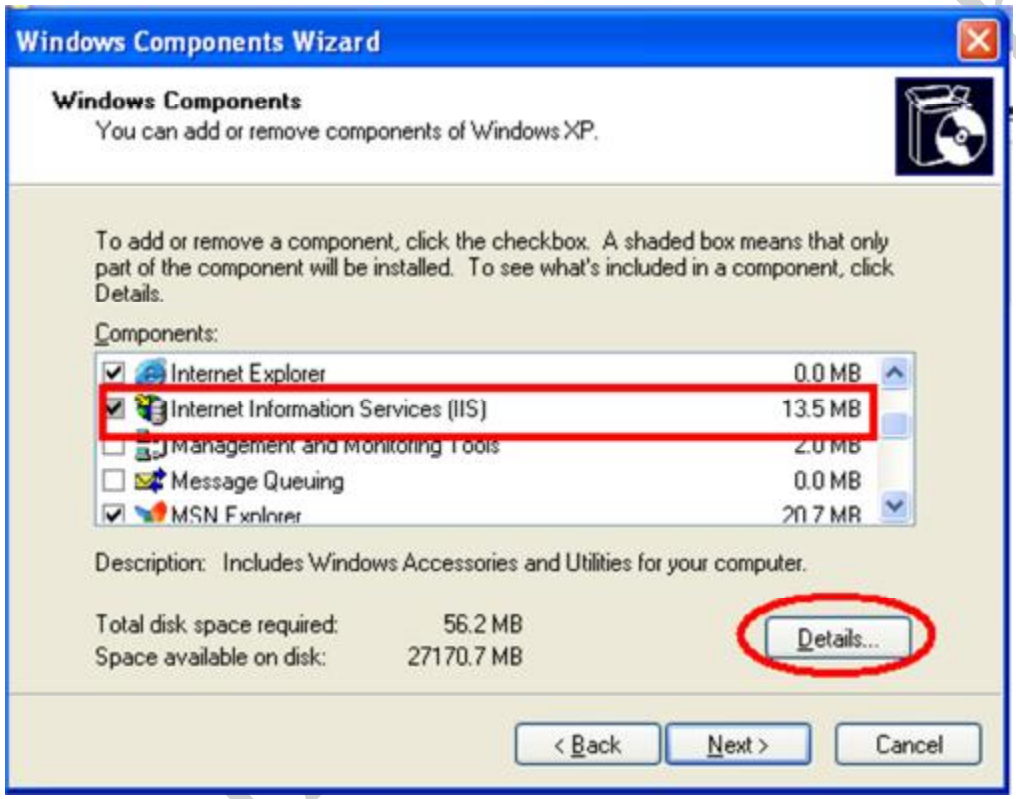
این سرویس توسط پروتکل HTTP ( HiperTextTransfareProtocol ) می تواند به یک کامپیوتر به صورت ریموت وصل شود.

فعال سازی سرویس IIS :

برای فعال سازی این سرویس ابتدا وارد Components ویندوز می شویم



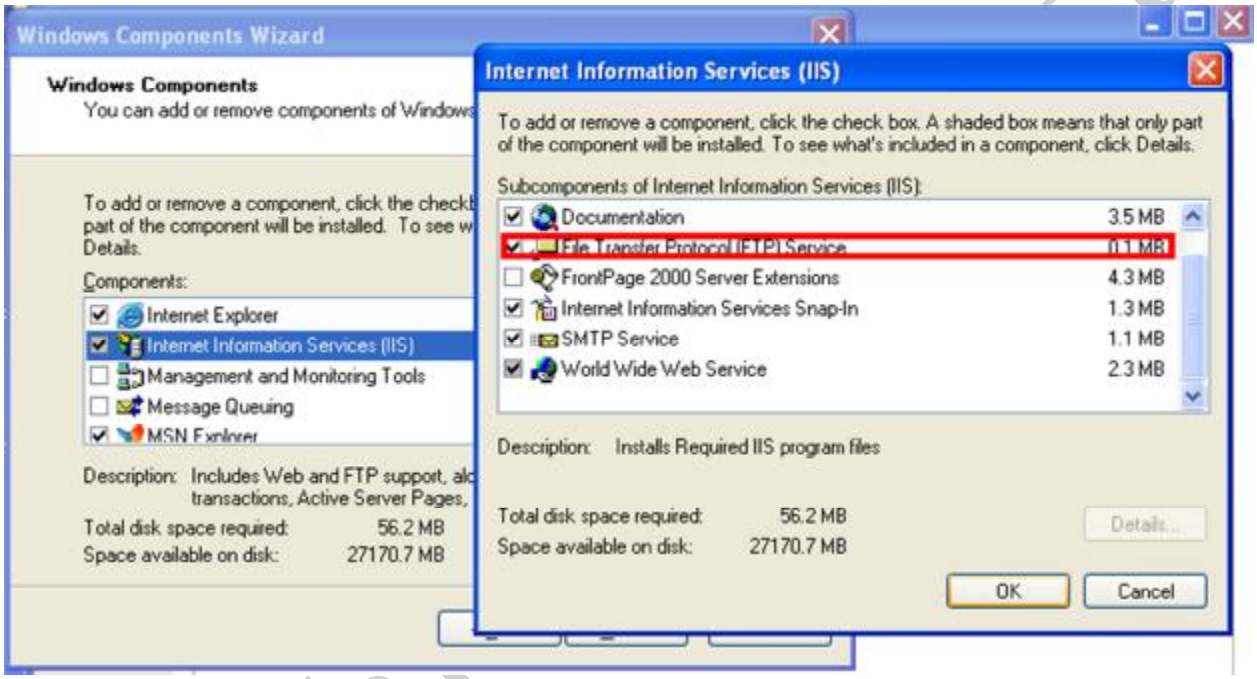
سپس گزینه IIS را فعال می کنیم،برای فعال سازی باید CD ویندوز داخل کامپیوتر باشد




- پورت FTP 21 است
- پورتHTTP 80 است

Farsi

**بعد از فعال کردن IIS باید سرویس FTP را هم فعال کنیم، برای این کار گزینه DETAILS را انتخاب کرده و از منوی باز شده FTP را فعال می کنیم.**




VPN :

**نوعی از تکنولوژی است که توسط آن می توان دو یا چند کامپیوتر یا شبکه خصوصی را بصورت امن تحت یک بستر عمومی مثل اینترنت به هم وصل کرد.**

Farshid

Managing Storage Device In Microsoft Network (منابع ذخیره سازی سخت افزاری و نرم افزاری):

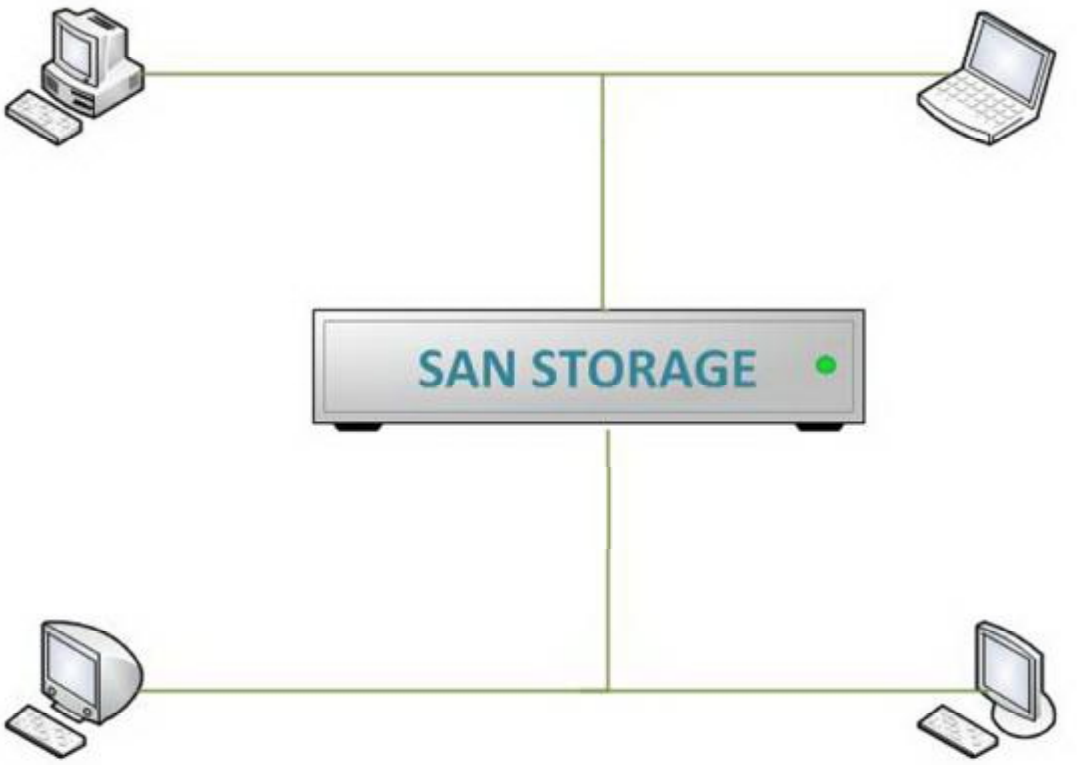
منابع ذخیره سازی (Storage Device) به 3 دسته تقسیم می شوند:

DAS (Direct Attach Storage):

به کامپیوترهایی که منابع ذخیره سازی (هارد) آنها به صورت اینترنال یا اکسترنال اتصال دارند را DAS گویند.

SAN (Storage Area Network ):

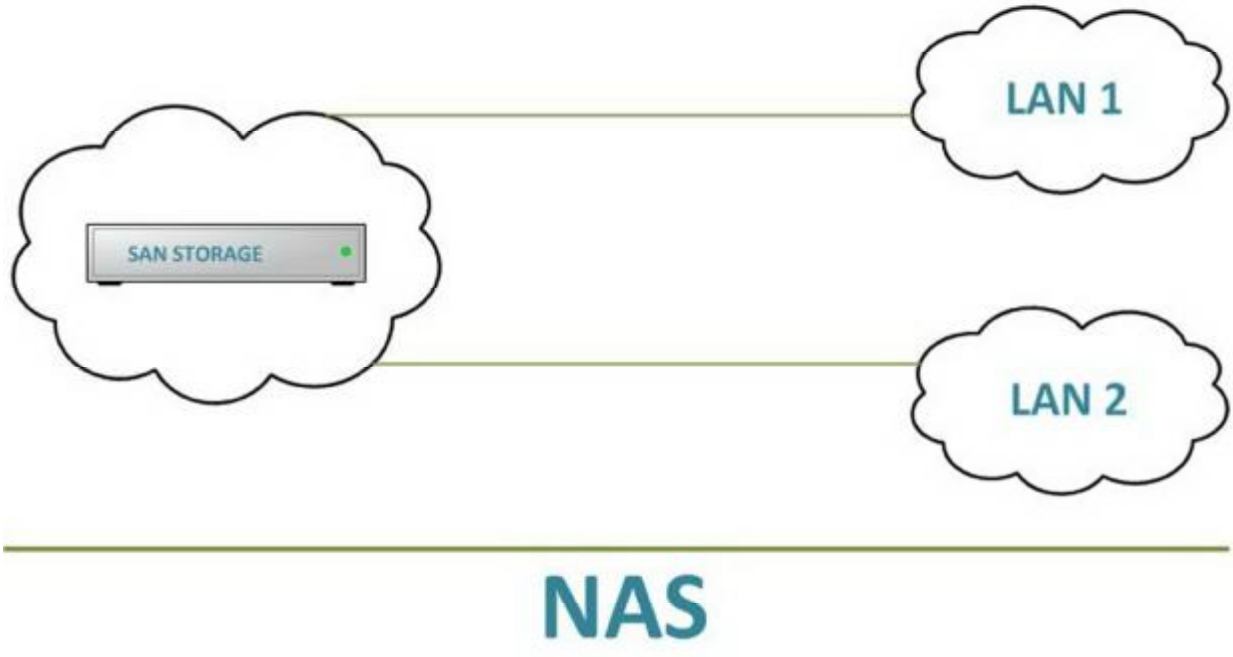
در این تکنولوژی تمامی کامپیوترهای سرور با اینکه خودشون هارد دارند ولی اطلاعات را بر روی دستگاهی به نام San Storage ذخیره می کنند،San Storage ها کیس هایی پر از هارد هستند.(از این تکنولوژی در مراکز Data Center استفاده می شود)




hnoush

NAS (Network Area Storage ):

**هنگامی که چند شبکه اطلاعاتشان را روی شبکه ای دیگر که داخل آن SanStorage است ذخیره می کنند به آن NAS گویند.**




- **از NAS فقط برای Backup گرفتن استفاده می شود.**

**آشنایی با منابع ذخیره سازی**

**هاردها به2دسته تقسیم می شوند: 1)سخت افزاری 2)نرم افزاری**

**نرم افزاری: خود به2 دسته به نام های 1)Dynamic 2)Basic تقسیم می شوند**

**سخت افزاری:**

1) IDE 2)SCSI

1-1) IDE: ATA - SATA

1-1-2) SATA: ESATA -SATA2 –SATA3

Basic:

**تمامی هاردهایی که استفاده می کنیم بصورت پیش فرض Basic هستند،در این نوع از هاردها می توانیم 2 نوع پارتیشن داشته باشیم: 1) Primary 2)Extended**

**تفاوت بین پارتیشن های Primary و Extended در این است که پارتیشن Primary قابلیت Boot شدن را دارد و پارتیشن Extended قابلیت ذخیره سازی اطلاعات را دارد.**

**بر روی یک هارد دیسک می توانیم 4 پارتیشن Primary بدون پارتیشن Extended داشته باشیم یا 3پارتیشن Primary با 1 پارتیشن Extended داشته باشیم.**

**تفاوت بین Partition و Volume :**

**به پارتیشنی که روی آن Letter(حروف انگلیسی) زده شود Volume گویند همانند:D،E،F**

FarshidAjabnoush

File System

**به نوع ذخیره سازی اطلاعات بر روی هارد فایل سیستم گویند،فایل سیستم ها بر دو نوع هستند:**

FAT (File Allocate Table)  NTFS (New Technology File System)

**تفاوت بین FAT و NTFS :**

**در ماکزیمم**
- **FAT 16 : 2 گیگا بایت**
- **FAT 32 : 32 گیگابایت**

**سایز درایوها** - **NTFS : در ویندوزهای 2Legacy TR و در ویندوزهای 16NGTR**

**مینیموم**
- FAT 16 : 64K
- FAT 32 : 16 K

**سایز** - NTFS : 4K

SECTOR

**به فضای از بین رفته در کلاسترها SLACK گویند،سیستم عامل از فضاهای SLACK برای ریکاوری کردن استفاده می کند.**

**MFT نام الگوریتمی است که فایل سیستم FAT از آن برای ریکاوری کردن استفاده می کند.**

- **بهترین نرم افزار ریکاوری ENCASE می باشد.**

FarshidAjabnoush

Permission: اجازه دسترسی به قسمت های مختلف هارد

Quota : سهمیه بندی فضای دسترسی روی هارد(بیشتر بر روی Mail Server اجرا می شود)

Encryption: رمز نگاری اطلاعات

Compress: فشرده سازی اطلاعات

اطلاعات Encryption شده را می توان توسط نرم افزار EFS RECOVERY بازگردانی کرد.

بهترین نرم افزار فشرده سازی ACE نام دارد.

فایل سیستم های سیتم عامل لینوکس عبارتند از:

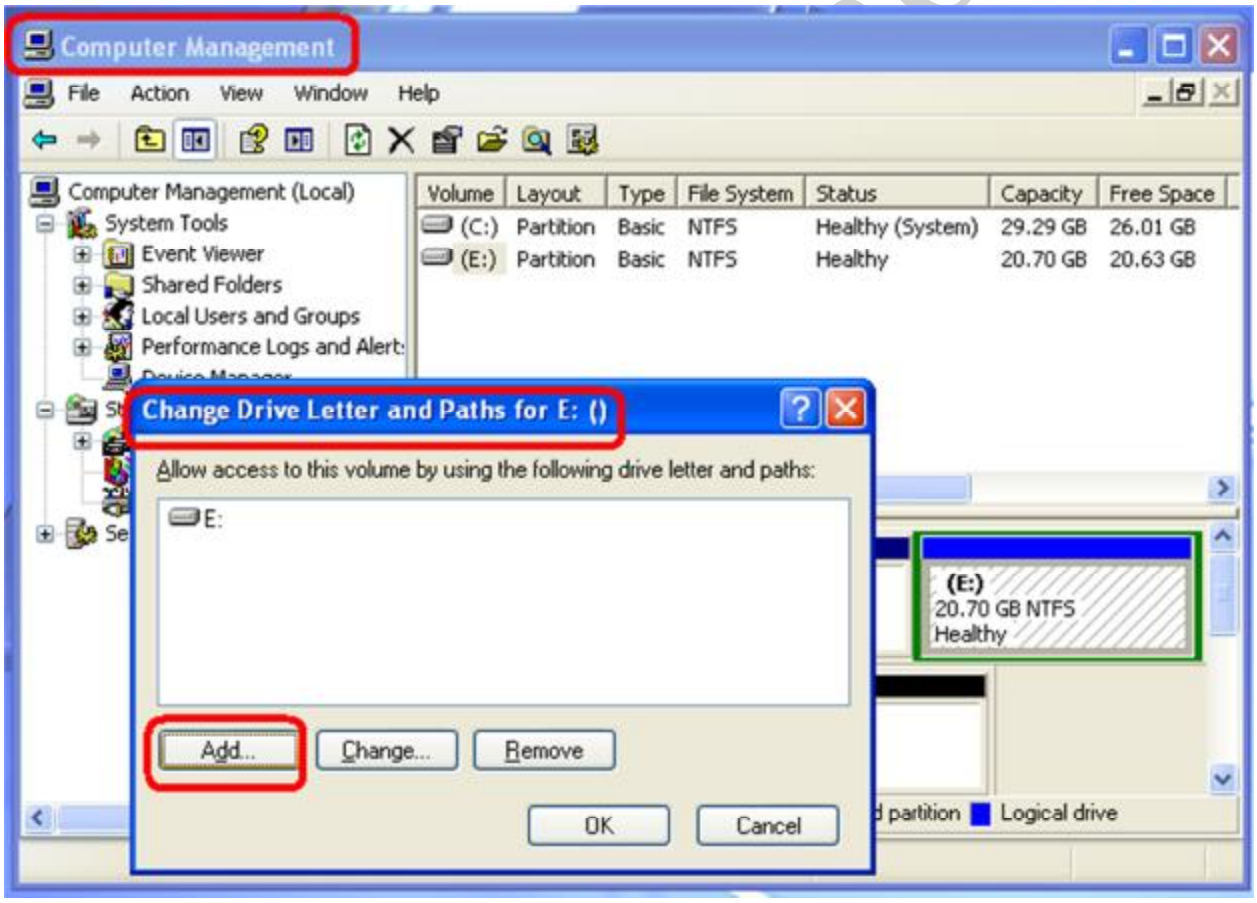
1) Ext2 2) Ext3 3) Ext4 4) Reiser

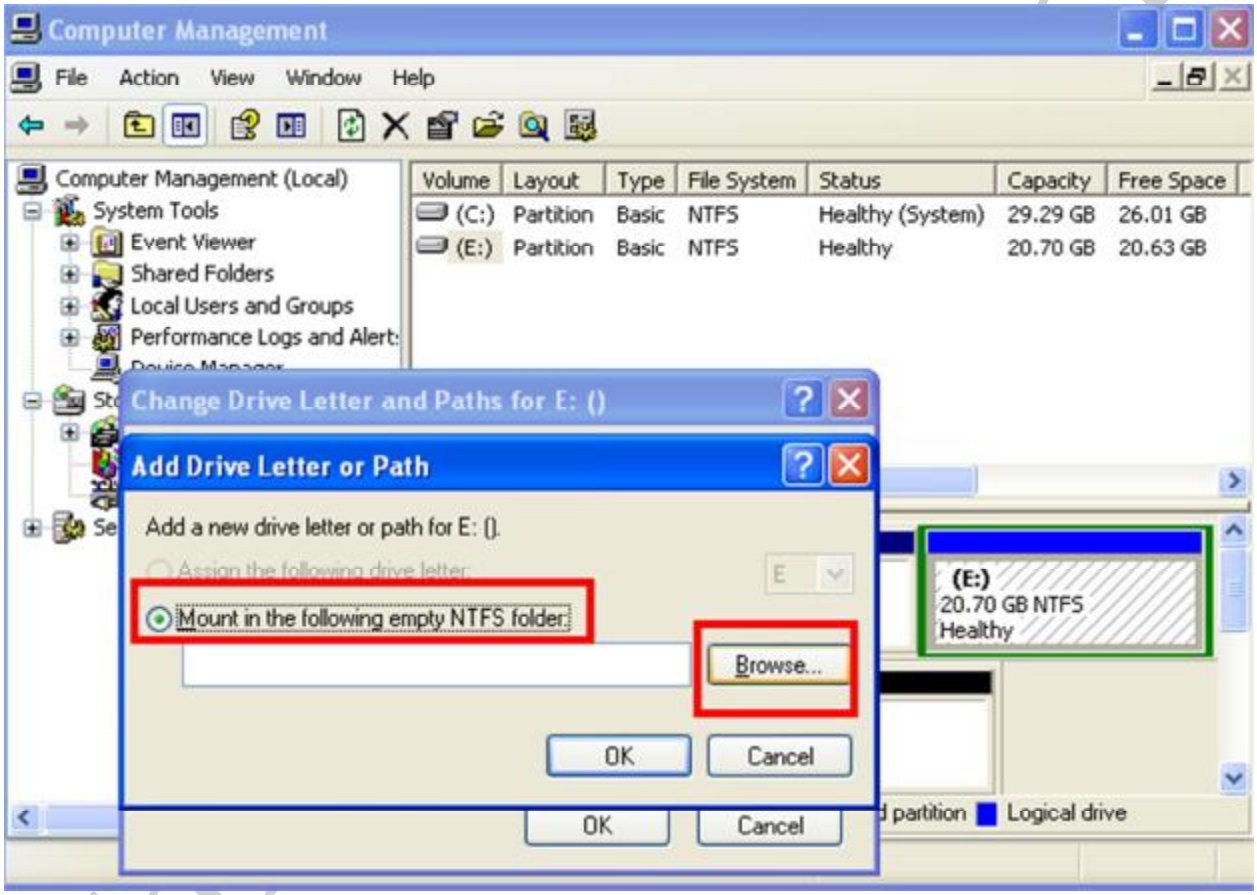
FarshidAjabnoush

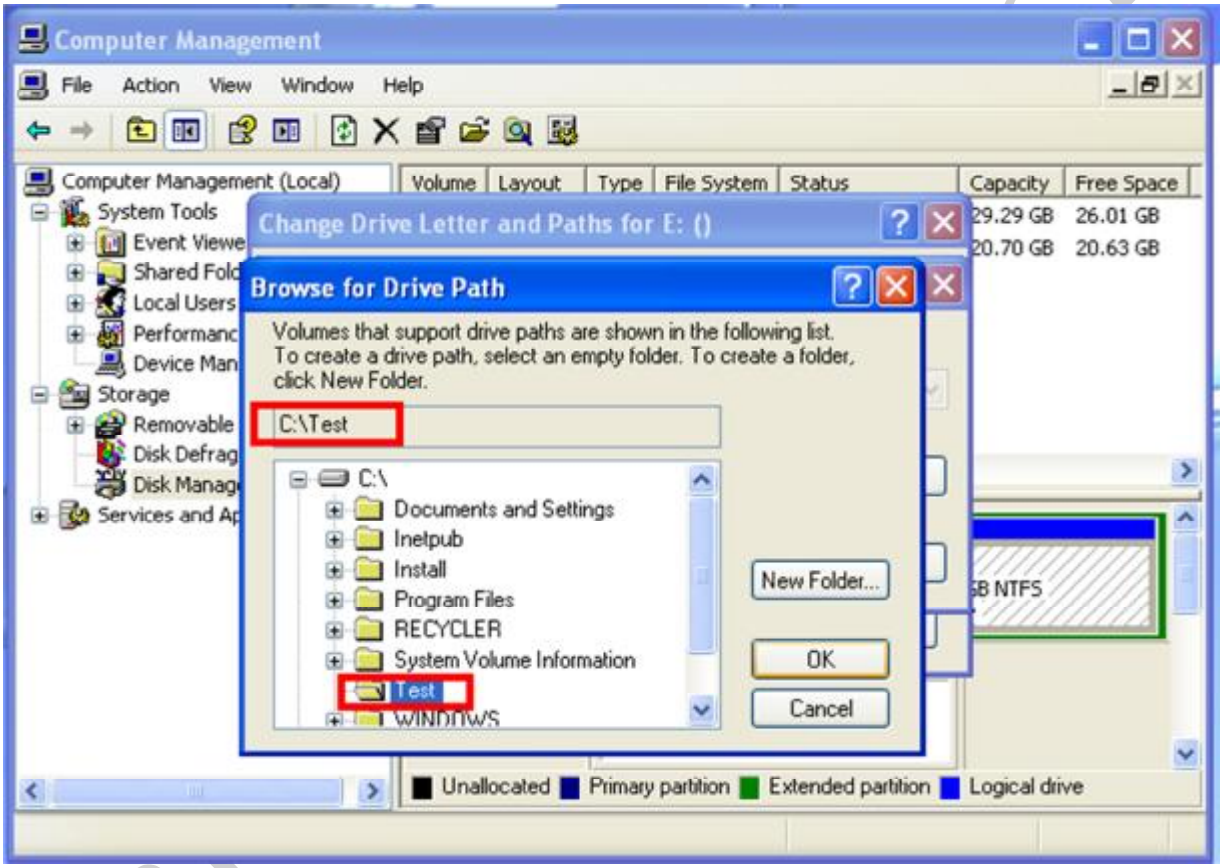
MOUNT (اتصال):

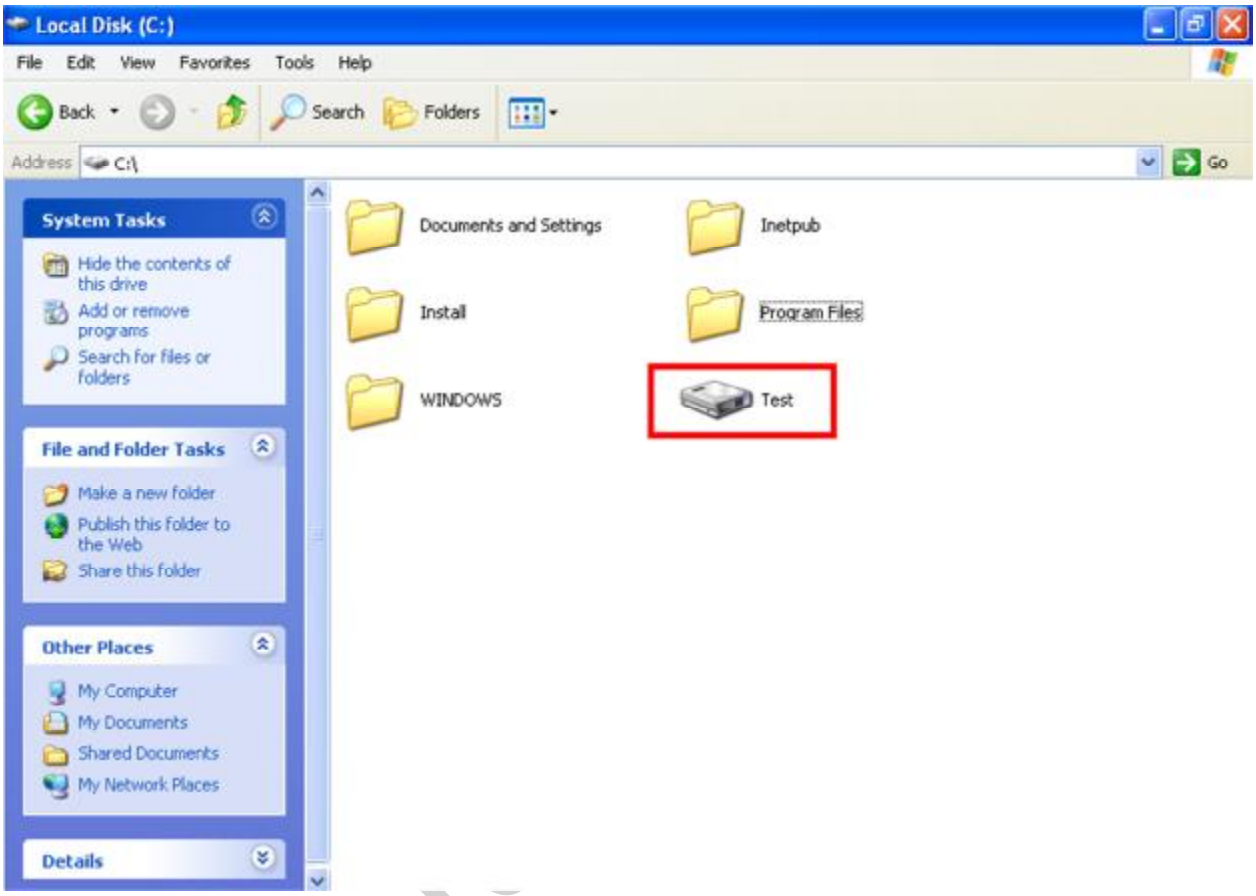
**به طور مثال ما پوشه ای در داخل درایو C داریم و درایو C فضای کافی برای ادامه کار با پوشه ما را ندارد و ما هم نمی توانیم پوشه مورد نظر را CUT کنیم در اینجا باید از عمل اتصال استفاده کرد این عمل باعث می شود پوشه در درایو مورد نظر باقی مانده و از فضای درایو دیگری مانندE استفاده کند زمانی که عمل اتصال انجام شد هر اطلاعاتی که در داخل پوشه ریخته شود در درایو E ذخیره می شود در صورتی که پوشه سر جای خودش است(C) و از داخل پوشه، اطلاعات درایو E را می توان دید، برای عمل اتصال باید از مقصد شروع کنیم.**

- **زمانی که عمل اتصال انجام شد آیکون پوشه مورد نظر به صورت شکل4 تغییر پیدا می کند**



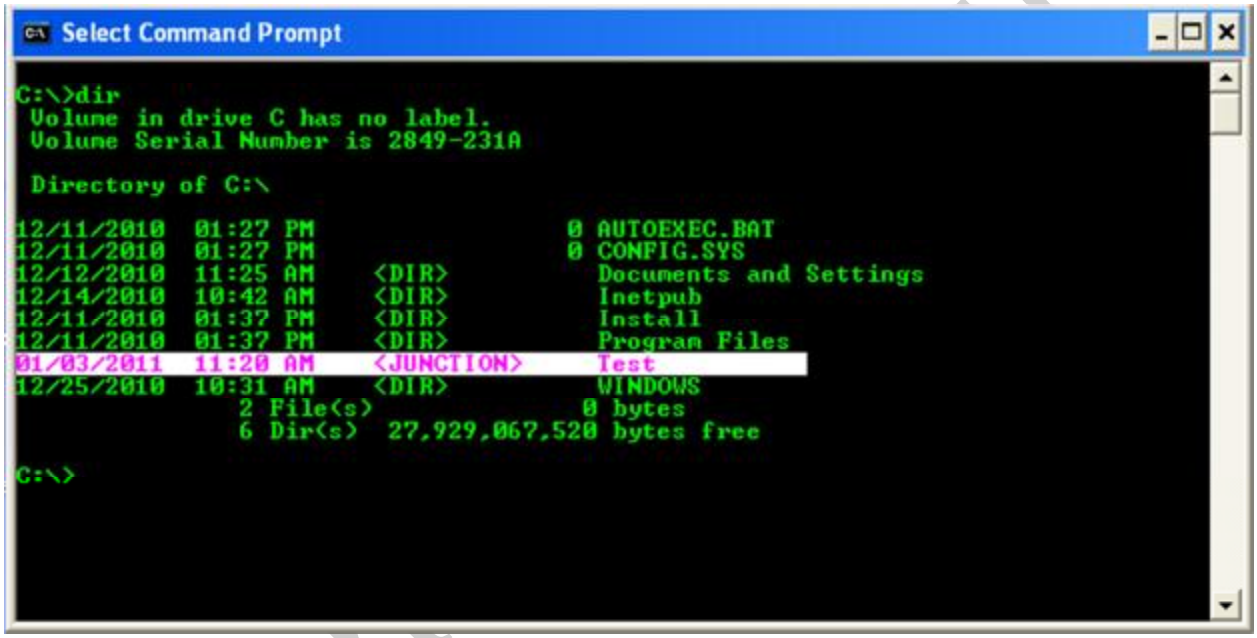

Computer Management
File Action View Window Help
Computer Management (Local)
System Tools
Event Viewer
Shared Folders
Local Users and Groups
Performance Logs and Alert
Volume Layout Type File System Status Capacity Free Space
(C:) Partition Basic NTFS Healthy (System) 29.29 GB 26.01 GB
(E:) Partition Basic NTFS Healthy 20.70 GB 20.63 GB
Change Drive Letter and Paths for E: ()
Add Drive Letter or Path
Add a new drive letter or path for E: ().
Assign the following drive letter:
Mount in the following empty NTFS folder:
Browse...
OK
Cancel
OK
Cancel
(E:)
20.70 GB NTFS
Healthy
partition
Logical drive


Computer Management
File Action View Window Help
Computer Management (Local)
System Tools
Storage
Volume Layout Type File System Status Capacity Free Space
29.29 GB 26.01 GB
20.70 GB 20.63 GB
Change Drive Letter and Paths for E: ()
Browse for Drive Path
Volumes that support drive paths are shown in the following list.
To create a drive path, select an empty folder. To create a folder, click New Folder.
C:\Test
C:\
Documents and Settings
Inetpub
Install
Program Files
RECYCLER
System Volume Information
Test
New Folder...
OK
Cancel
Unallocated
Primary partition
Extended partition
Logical drive


Local Disk (C:)
File Edit View Favorites Tools Help
Back Search Folders
Address C:\
Go
System Tasks
Hide the contents of this drive
Add or remove programs
Search for files or folders
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
My Computer
My Documents
Shared Documents
My Network Places
Details
Documents and Settings
Inetpub
Install
Program Files
WINDOWS
Test

Farshi

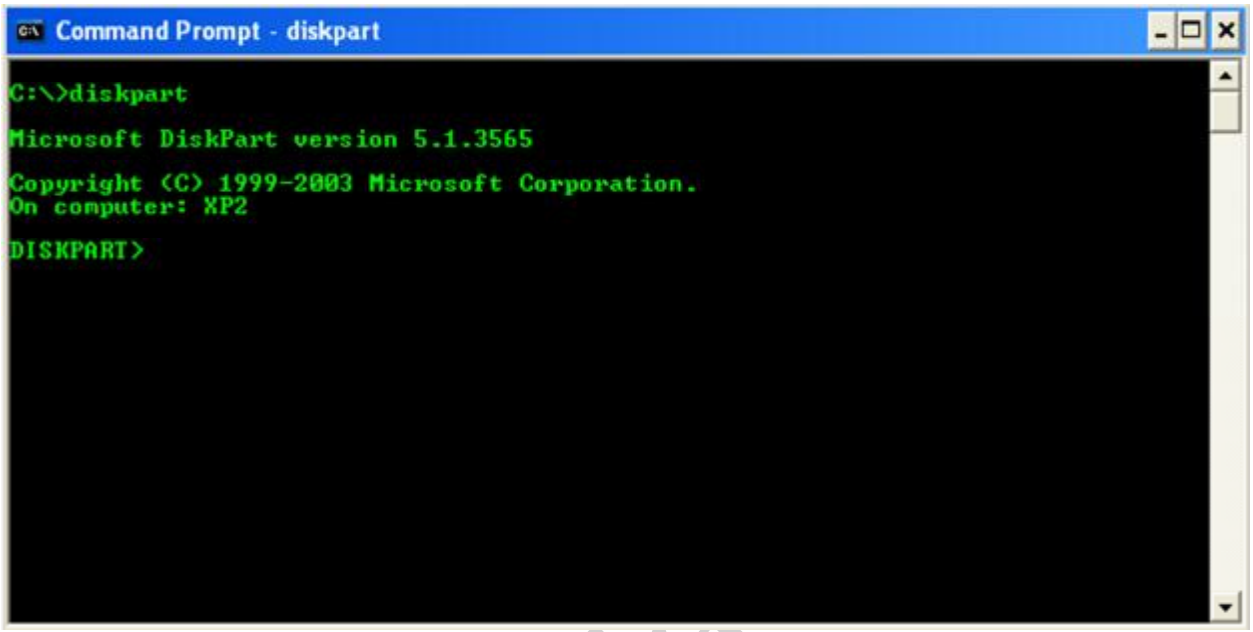
- در محیط Command پوشه ای را که Mount شده باشد را با لیبل JUNCTION نمایش می دهد.



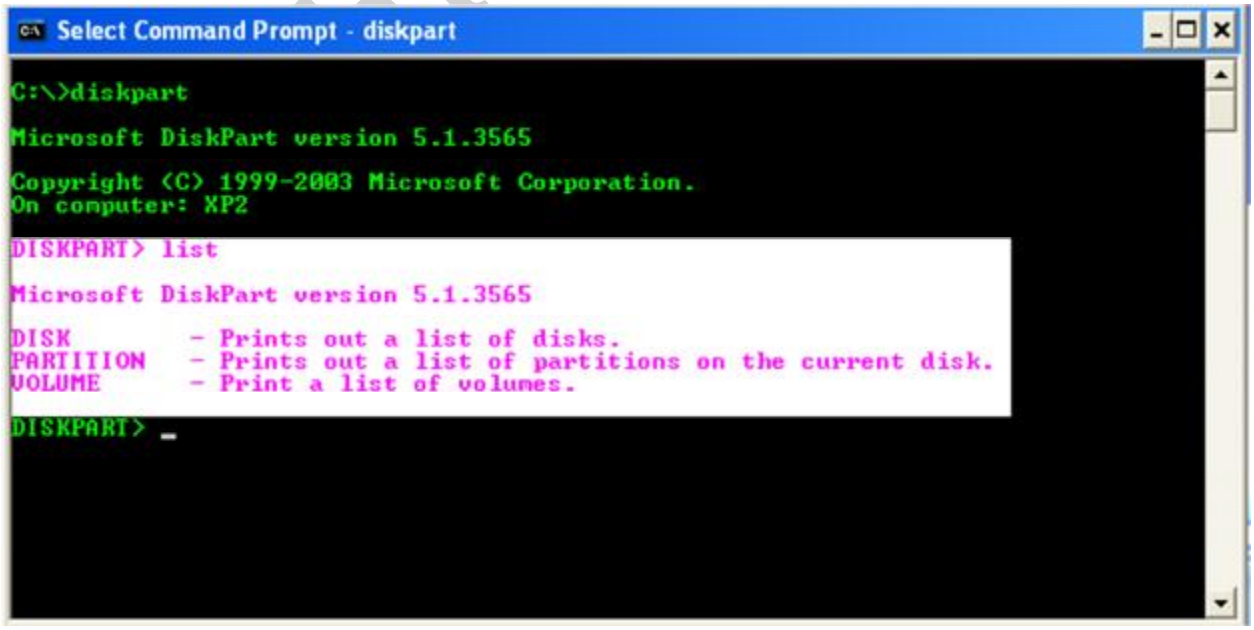

Farsi English

مدیریت هارد توسط Command :

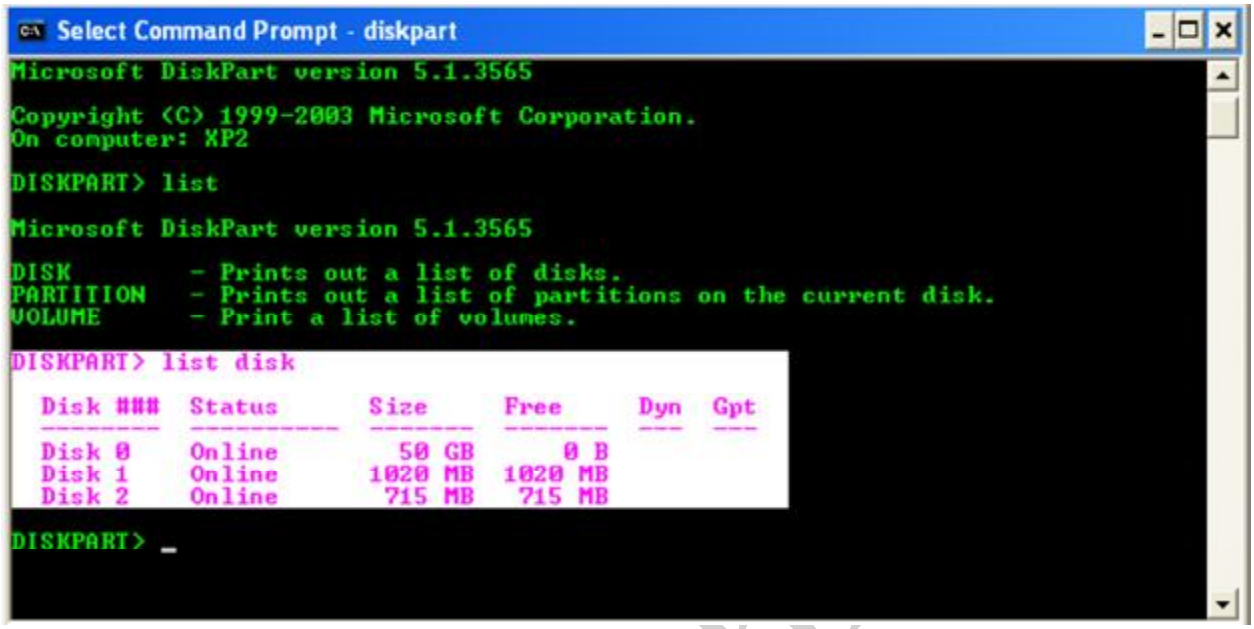
برای وارد شدن به این محیط از دستور Diskpart استفاده می کنیم




سپس از دستورList برای لیست کردن 1)دیسک 2)پارتیشن 3) والیوم استفاده می کنیم

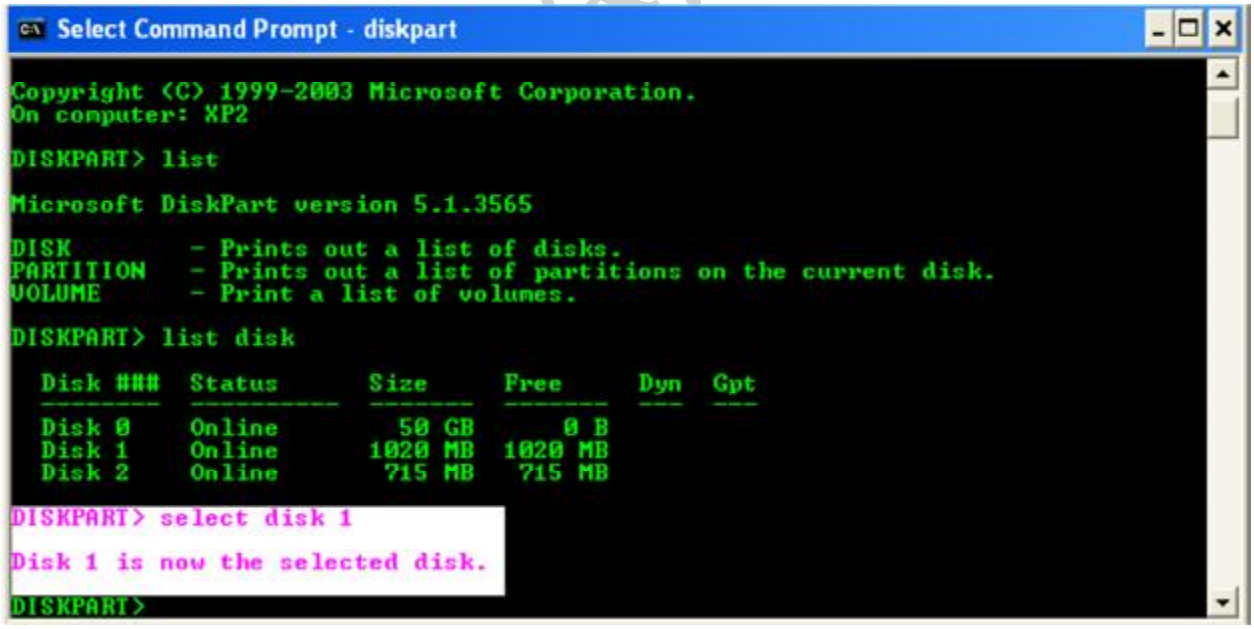


از دستور List Disk برای نشان دادن تعداد دیسک ها استفاده می کنیم



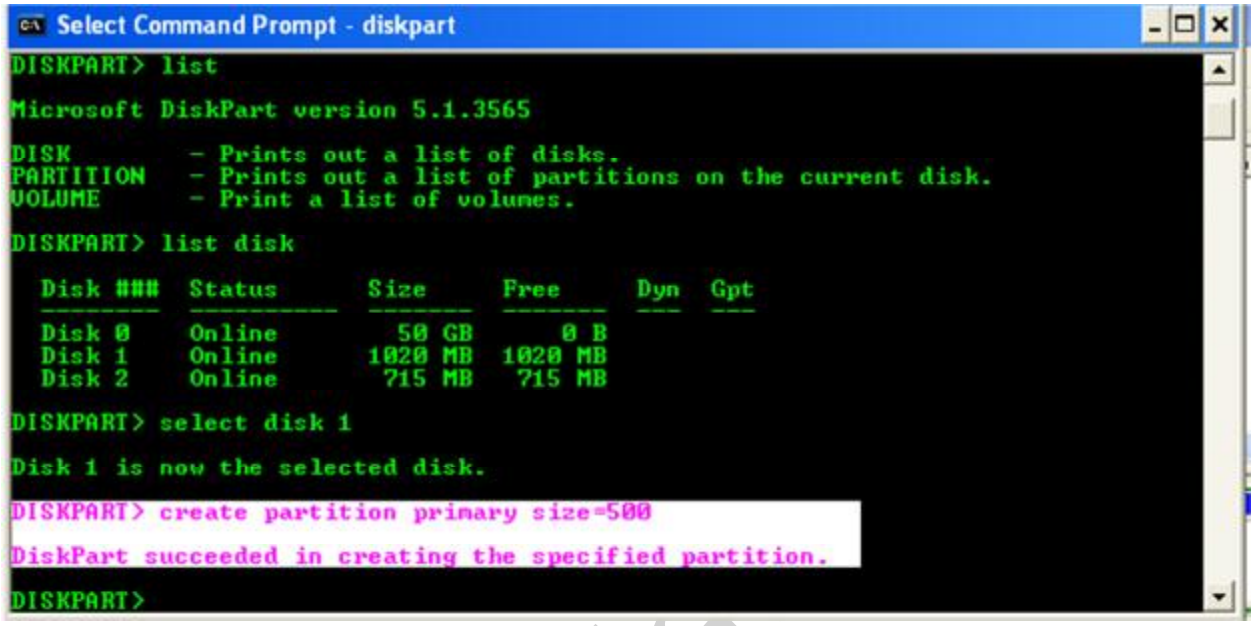

به خاطر داشته باشید که همیشه دیسک صفر همان دیسک اصلی سیستم می باشد.

برای انتخاب دیسک از دستور Select Disk+شماره دیسک مورد نظر استفاده می کنیم

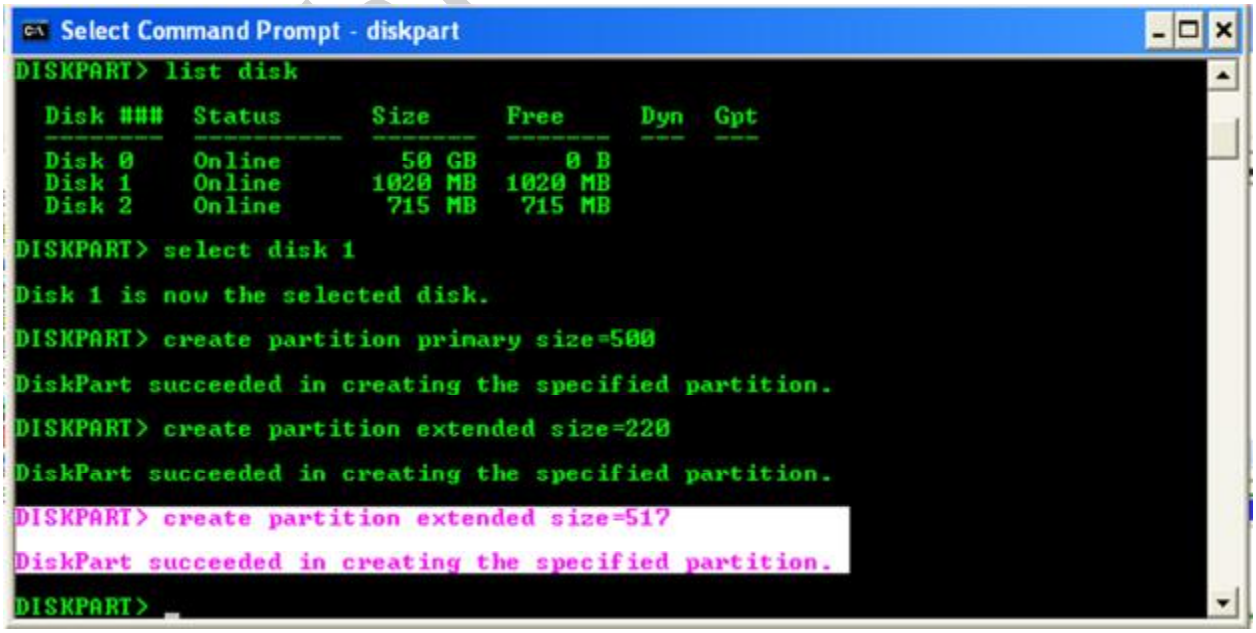


بعد از انتخاب دیسک نوبت ساختن پارتیشن می باشد،برای ساختن پارتیشن Primary از دستور :

Create partition primary size=.....(سایز بر حسب MB محاسبه می شود)

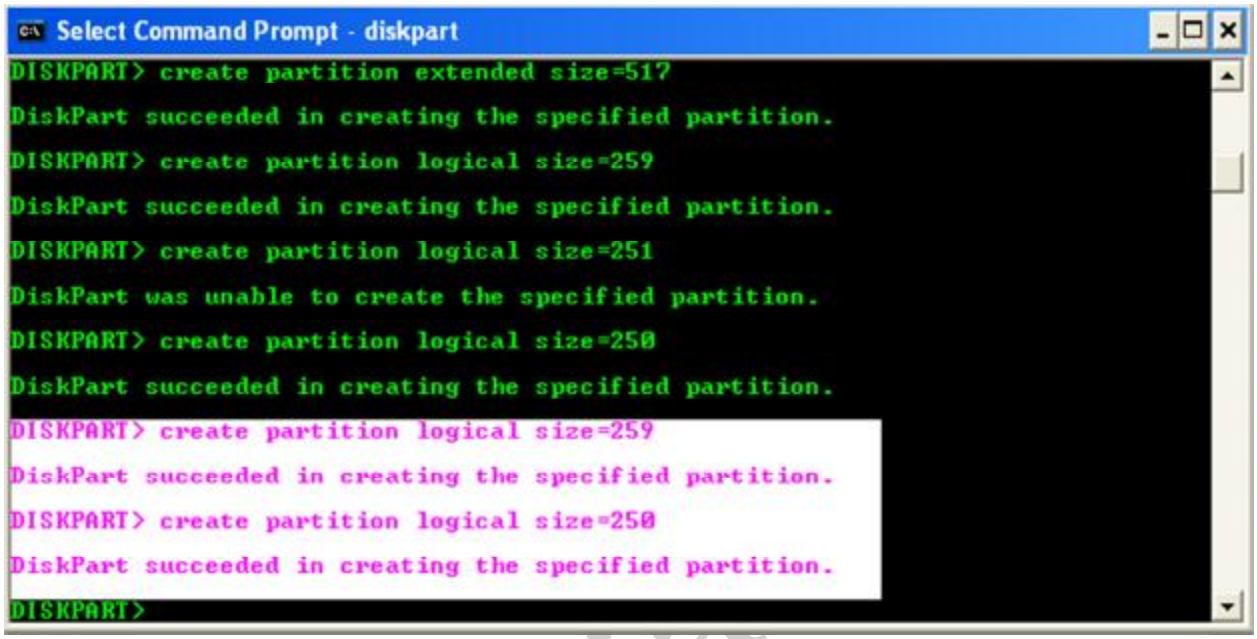



و برای ساختن پارتیشن Extended از دستور: Create Partition Extended Size=..... استفاده می کنیم.

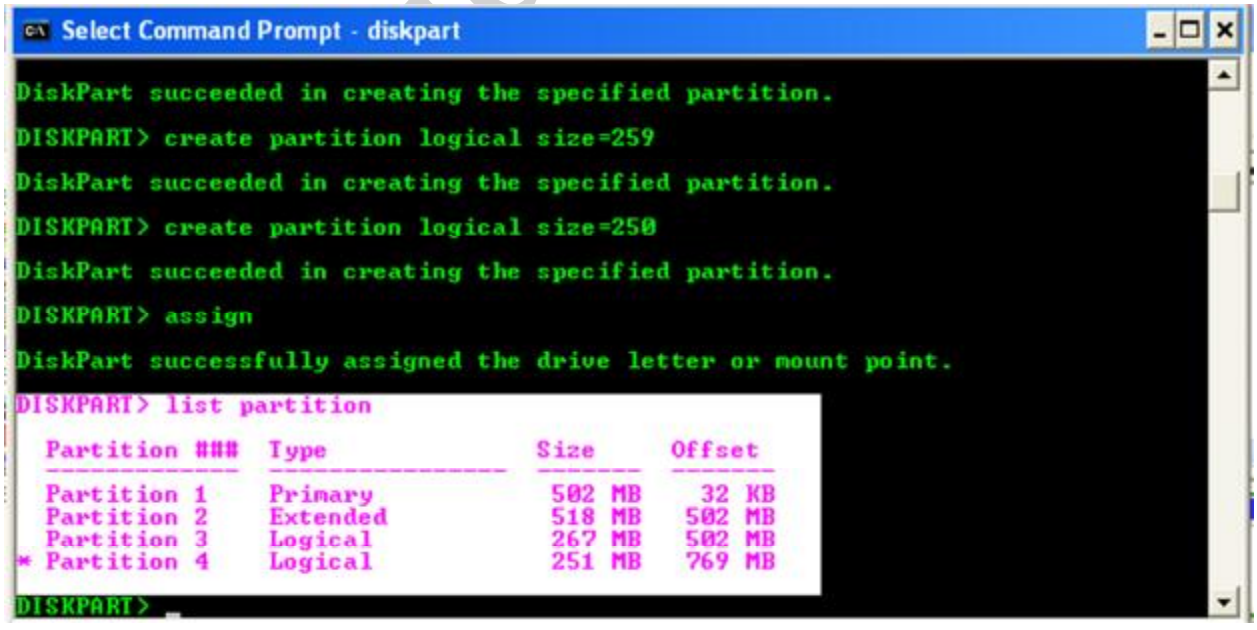


بعد از ساختن پارتیشن Extended نوبت به ساختن پارتیشن Logical می رسد برای این کار از دستور :

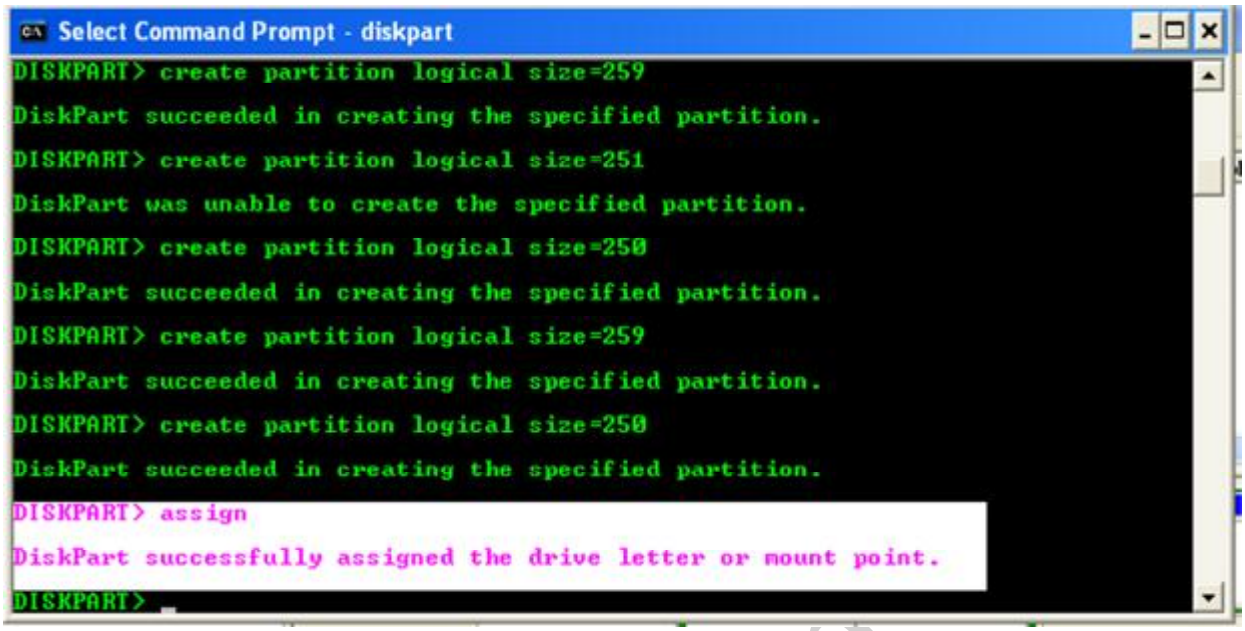
Create Partition Logical Size=..... استفاده می کنیم.




حالا نوبت به Letter زدن به پارتیشن های ساخته شده می باشد برای این کار ابتدا باید از دستور List Partitionبرای دیدن پارتیشن ها و از دستور Select Partitionبرای انتخاب پارتیشن استفاده کرد،پارتیشنی که علامت ستاره در کنارش آمده انتخاب شده است.

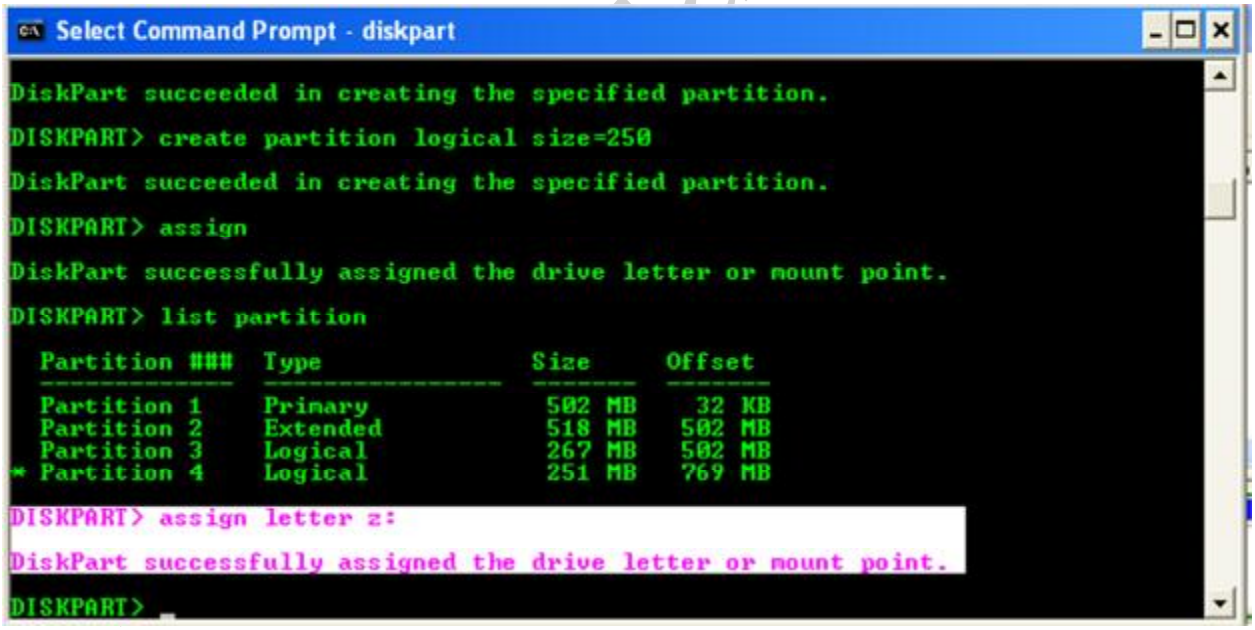



بعد از انتخاب پارتیشن برای Letter زدن ابتدا باید یکبار دستور Assign را به تنهایی وارد کنیم



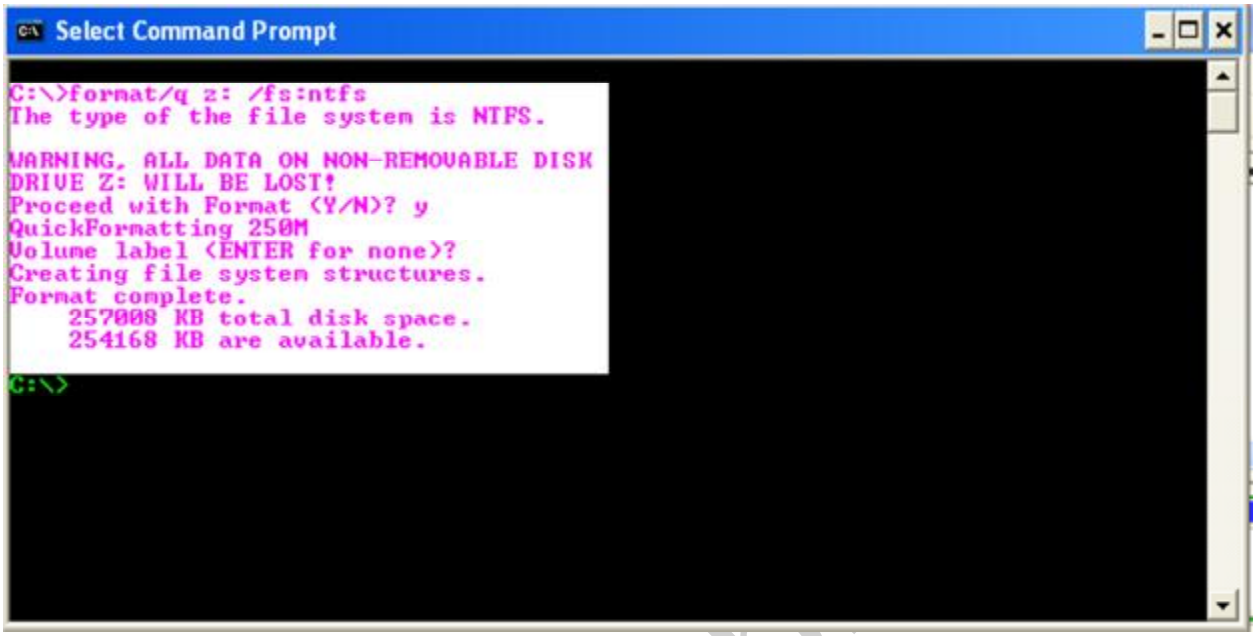

زمانی که دستور تأیید شد برای اضافه کردن نام درایو که در اینجا Z در نظر گرفته شده است از دستور:

Assign Letter Z:استفاده می کنیم.

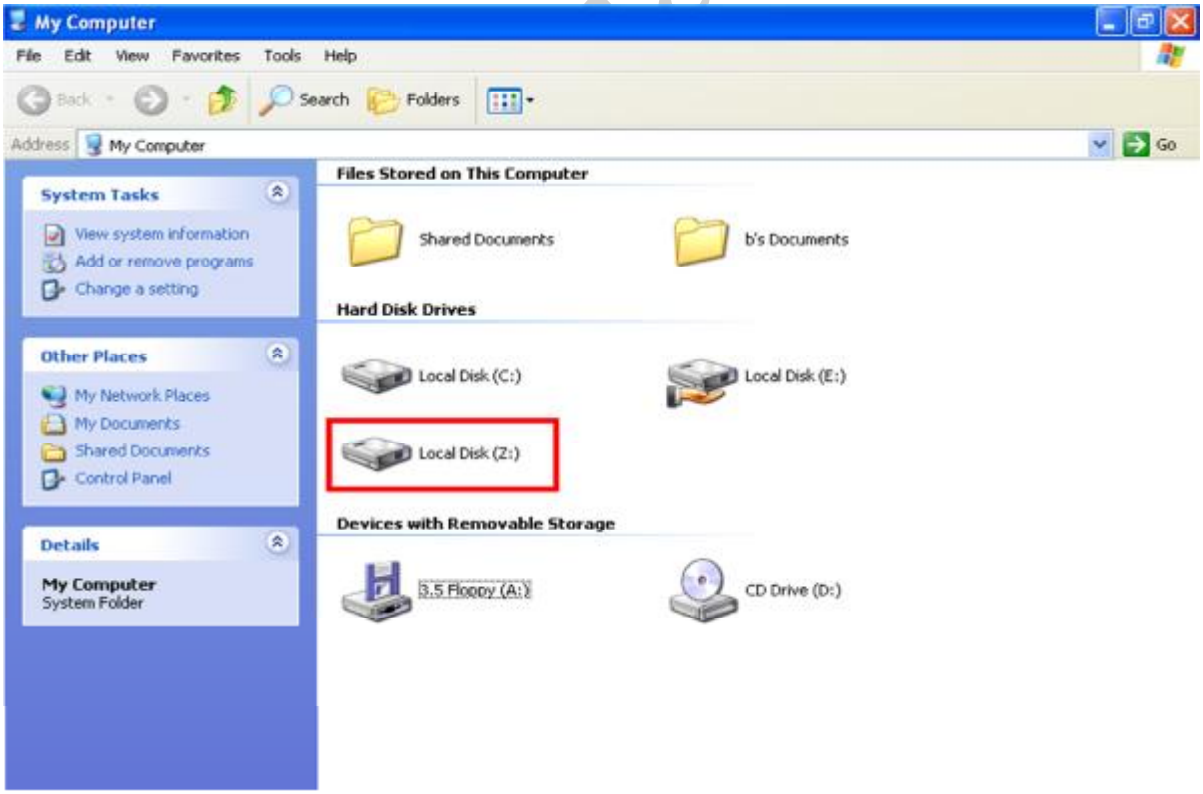



بعد از Letter زدن نوبت به Format کردن پارتیشن مورد نظر می رسد که از دستور:Format/q z: /fs:NTFS

استفاده می کنیم،در اینجا /Q بیانگر فرمت سریع می باشد.




و در نهایت پارتیشن Z آماده استفاده می باشد.



: Dynamic

**اگر هاردی را از حالت Basic به Dynamic تبدیل کنیم پارتیشن های زیر بر روی آن هارد ایجاد می شود.**

**1) Simple : مانند پارتیشن های Extended فقط برای ذخیره سازی اطلاعات استفاده می شود.**

**2) Spand(گسترش دادن) : اگر چندین هارد داشته باشیم تمامی ظرفیت های باقی مانده هاردها را با هم یکی کرده و بر روی آنها می نویسد.**

**3) Striped(رشته رشته کردن) : اطلاعات بر روی 2 هارد نوشته می شود یعنی اطلاعات نصف می شود،نصف روی هارد1 و نصف روی هارد2**

RAID

(Raid 1) Mirror:

**در این Raid از2 هارد استفاده می شود،هنگامی که اطلاعات را بر روی هارد1 می نویسیم روی هارد2 هم نوشته می شود( Auto Backup )**

**( Raid 5) Parity:**

**در این Raid از3هارد استفاده می شود،وقتی روی هارد1 اطلاعات نوشته می شود بر روی هاردهای 2و3 اطلاعات به صورت Parity نوشته می شود.**

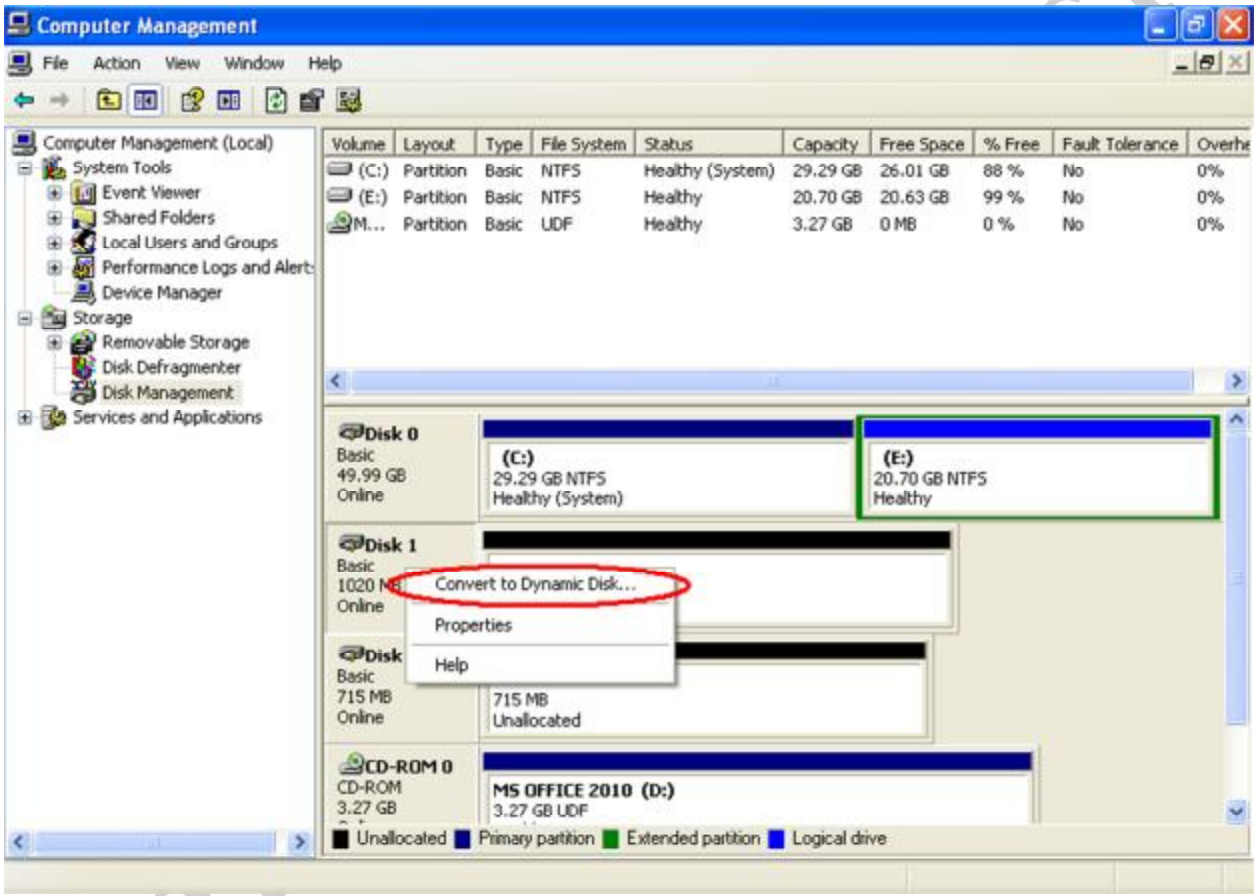
- **هنگامی که می خواهیم هاردهای Raid را از لحاظ سخت افزاری جابجا کنیم باید از اطلاعات نسخه پشتیبان تهیه کنیم**
- **ماکزیمم تعداد هارد برای Raid کردن 32 هارد است**

FarshidAjabnoush

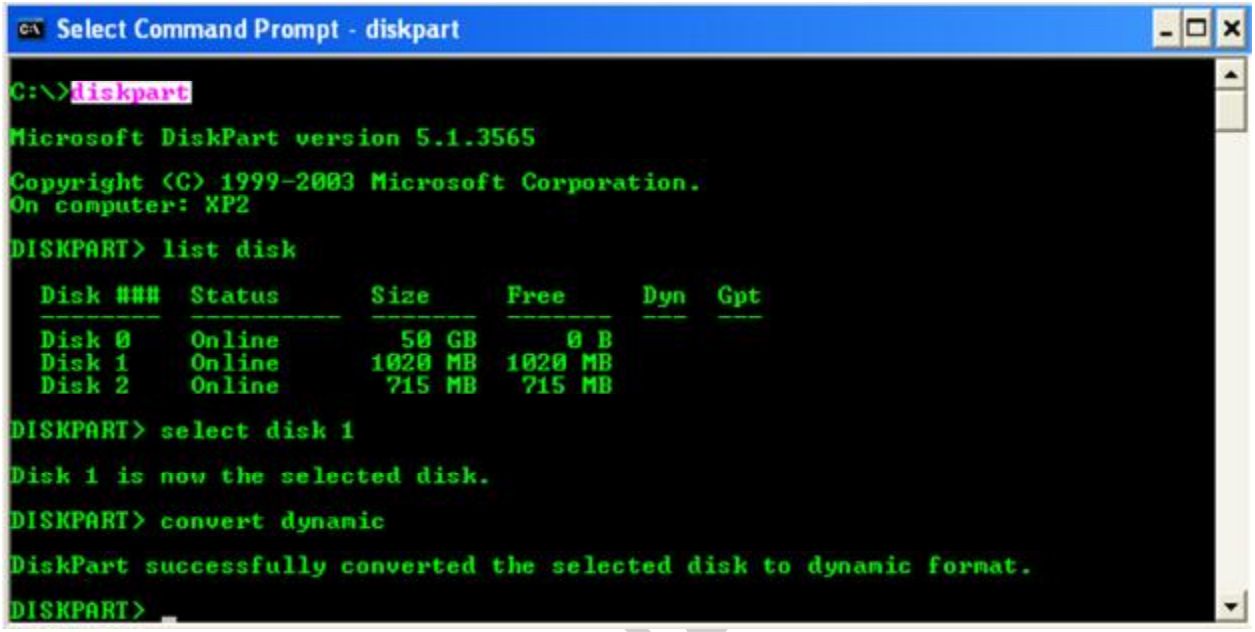
تبدیل Basic به Dynamic:

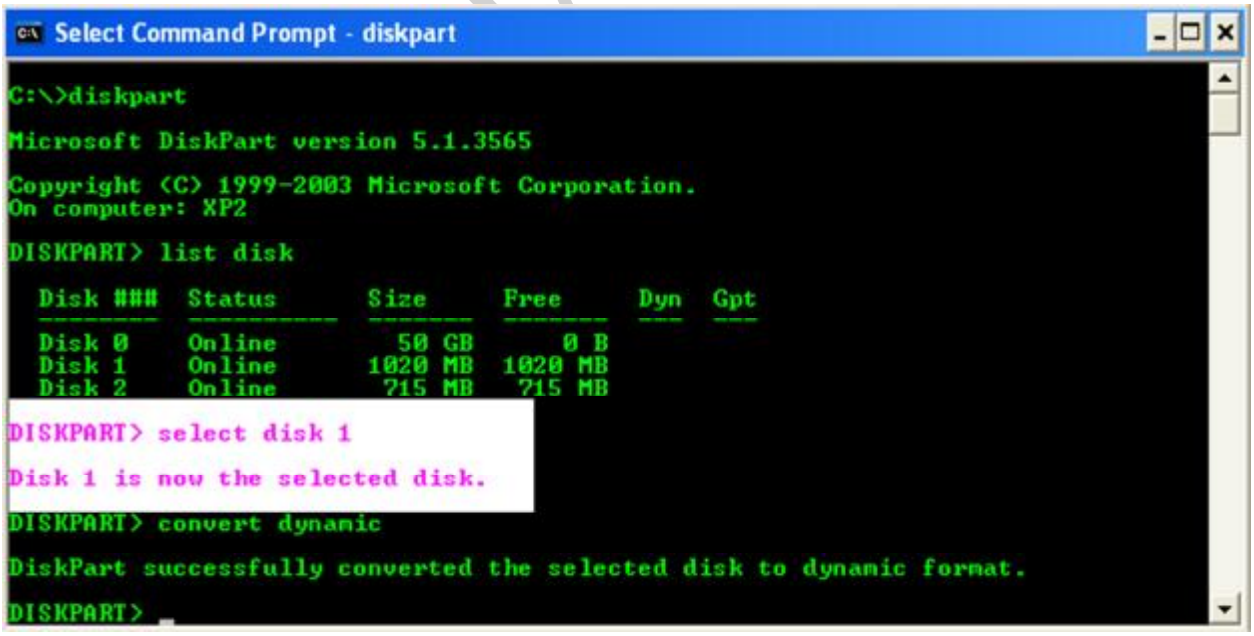
به 2 روش قابل اجرا است.

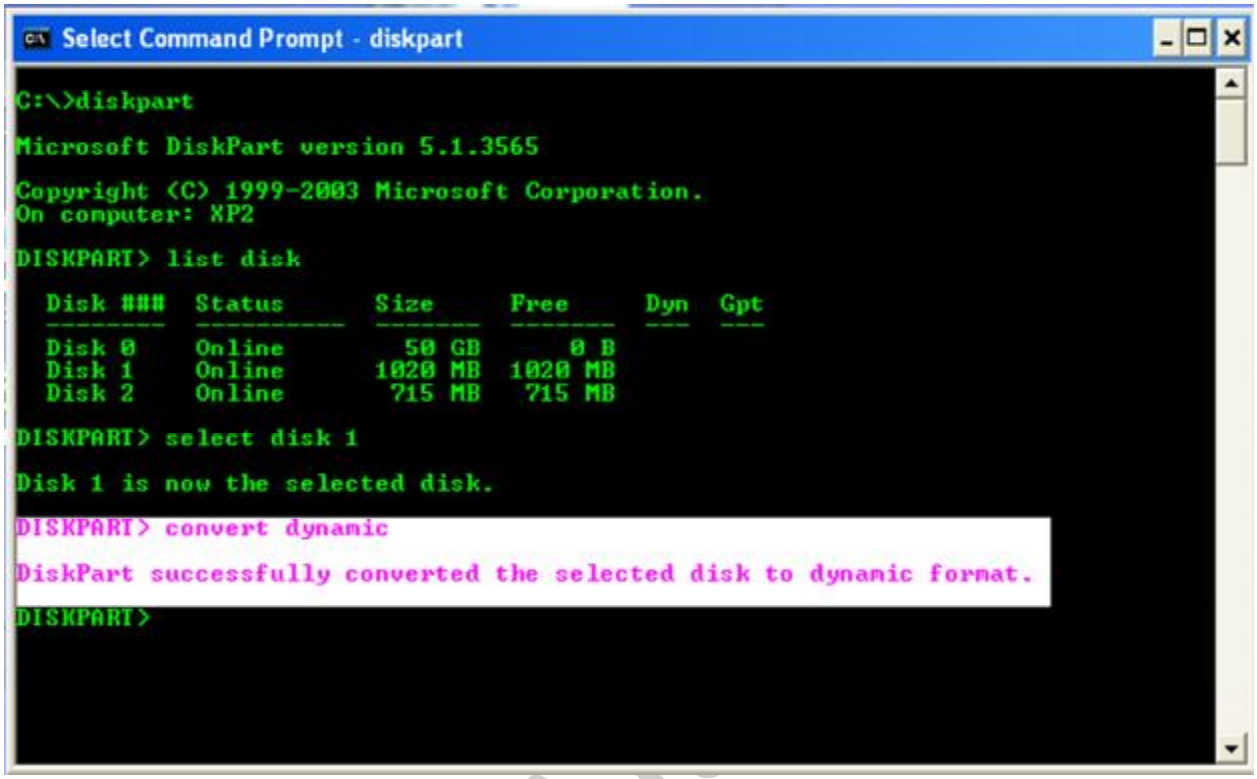
1) وارد Disk Management می شویم روی دیسک مورد نظر کلیک راست می کنیم و گزینه Convert To Dynamic Disk را می زنیم



2) وارد محیط Command می شویم، ابتدا از دستور DiskPart استفاده می کنیم سپس از List disk و Select Disk و در آخر هم از Convert dynamic استفاده می کنیم.






برای تبدیل به Basic هم تمام مراحل مانند بالا اجرا می شود با این تفاوت که در مرحله آخر از دستور

Convert Basic استفاده می شود.

FarshidAj

Security Essentials

**با رعایت 4 پارامتر زیر سیستمی امن داریم**

1) **فعال بودن فایروال**
2) **بروز بودن سیستم عامل**
3) **بروز بودن آنتی ویروس**
4) **بروز بودن آنتی مالورها(Malware )**

**تهدیدات امنیتی:**

**1)تروجان(Trojan ): برنامه هایی هستند که سیستم عامل را کنترل می کنند در کل 2 کار را انجام می دهند:1-کنترل سیستم عامل را به دست می گیرند2-پشت پرده اطلاعات سیستم را ارسال می کنند**

**2)ورم(Worm ): برنامه های مستقلی هستند که به خودی خود اجرا می شوند**

**3)ویروس(Virus): برنامه هایی هستند که برای اجرا شدن حتماً باید روی آنها کلیک شود**

- **اگر Trojan-Worm-Virus هر 3 در یکجا با هم باشند به آنها Malwareگویند.**

**از نرم افزار TCP/VIEW برای نشان دادن اطلاعاتی که پشت پرده ارسال می شود استفاده می شود**

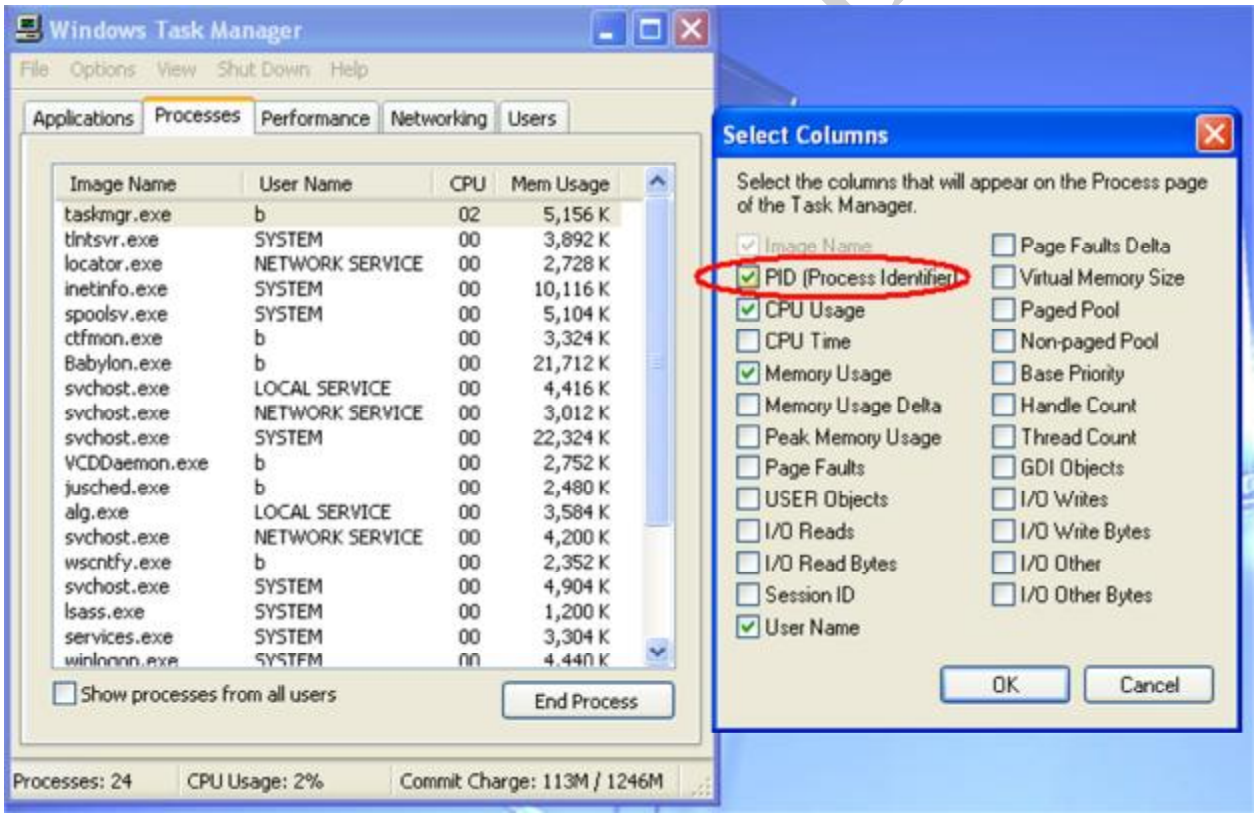
FarshidAjabnoush

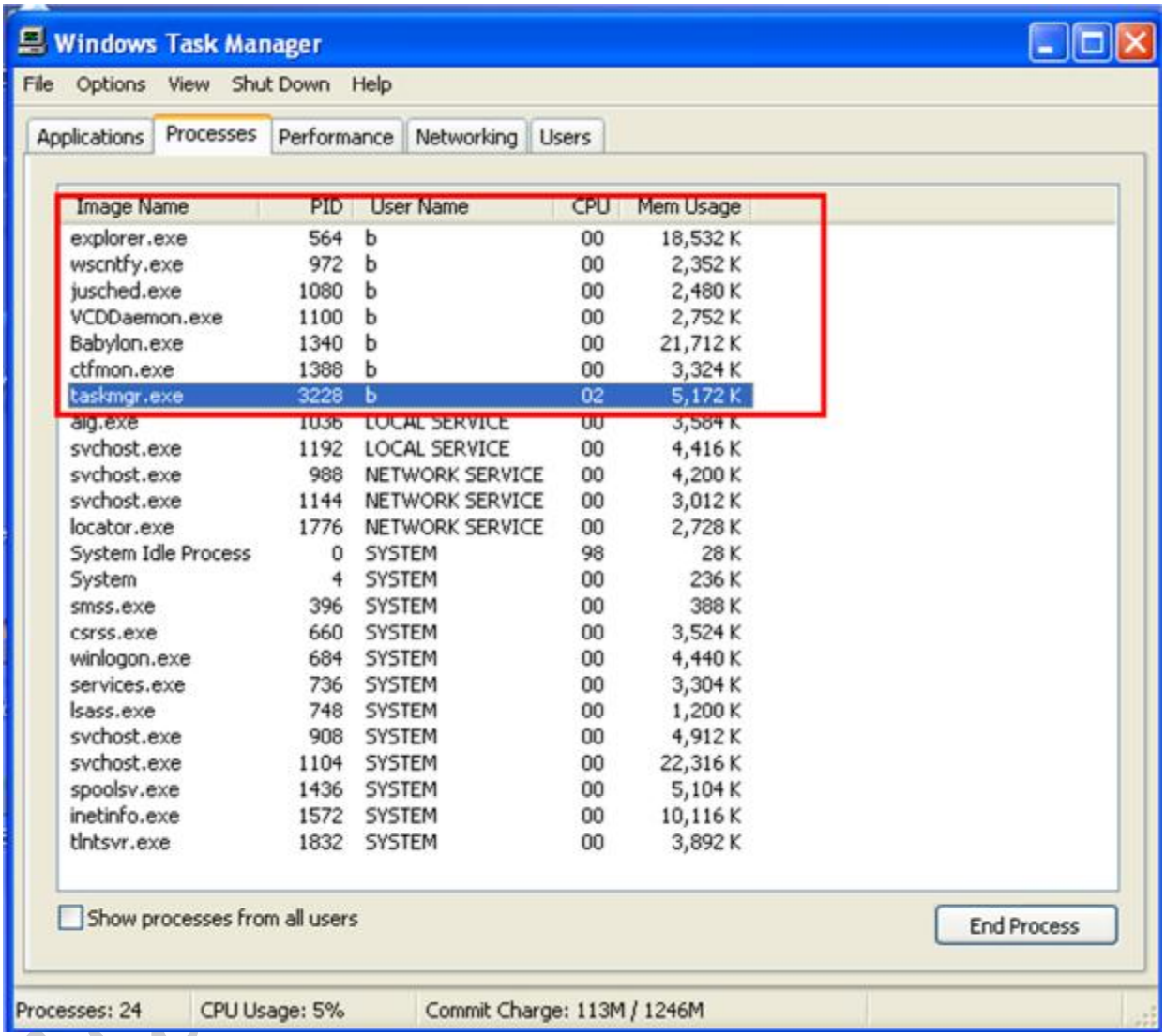
PID

اگر Pid نرم افزاری زیر 100 باشد آن نرم افزار تروجان می باشد،باید به این نکته توجه داشته باشیم که Pidحتماً باید با نام کاربری که ما برای سیستم عامل ساخته ایم فعال باشد و نرم افزارهای سیستمی مانند IE جزو تروجان ها نیستند.

دیدن Pid

ابتـدا وارد Task Manager مـی شـویم سـپس وارد تـب Processes مـی شـویم از منـوی View وارد Select Columns می شویم و تیک گزینه PID را می زنیم






بعضی از ویروس ها در Start up در Msconfig مشخص می شوند که معمولاً اسمی ندارند و تیک خورده اند.

بهترین آنتی ویروس MacAfee است

**مواردی که در داخل ویندوزهایNG برای ایجاد امنیت ارائه شده اند:**

1) UAC 2) Parental Controls 3) Bit Locker 4) Restriction on Removable Device
5) Application Locker 6) Two-Way Fire Wall 7) Windows Defender
8) Enhancement IE 9) Buffer Overrun Flow 10) Path Gourd 11) NLA

Restriction on Removable Device:

Gpedit.msc ← Local Computer Policy ← Computer Configuration ←
Administrative Template ← System ← Removable Storage Access

**از این مسیر می توانیم فلش،رایت کردن،خواندن CD و... را فعال یا غیر فعال کرد.**

Application Locker :

**از طریق این گزینه می توان پوشه ای را انتخاب کرد که هیچ گاه اطلاعات داخل آن کپی نشود.**

Gpedit.msc ← Local Computer Policy ← Computer Configuration ←
Windows Settings ← Security Settings ← Application Control Policies ←
Executable Rules

Two-Way Fire Wall:

**فایر وال موجود در Xp فقط می تواند جلوی ترافیک ورودی به سیستم(In Bond ) را بگیرد ولی در 7فایروال می تواند جلوی ترافیک ورودی و خروجی(Out Band ) سیستم را بگیرد**

Windows Defender :

آنتی Malware پیش فرض 7 است

Path Gourd:

**با فعال بودن این ویژگی ما اجازه نصب درایورهای Unsinghرا نداریم البته این ویژگی فقط در ویندوزهای NG می باشد**

FarshidAjabnoush

Enhancement IE:

**مرورگر صفحات وب نسخه7 ویندوز این ویژگی را دارد که باعث می شود فریب هکرها را نخورد،هکرها برای اینکه بتوانند به سیستم شما بدون اینکه متوجه بشوید دسترسی داشته باشندآدرسی را که شما وارد می کنید بدون اینکه متوجه بشوید به سرور دیگری انتقال می دهند ویژگیEnhancement IEبه راحتی اینگونه فریب ها راتشخیص می دهد.**

**اگر درurl ،@ بیاید آدرس قبل از@ پردازش نمی شود،کد اسکی@ معادل40% می شود،بعد از40%یا@درurl آدرس Ip را می زنند که به آن فرمول10 می گویند این دقیقاً همان کلک هکرها است.**

Fire Wall :

**نرم افزار یا سخت افزاری است که می تواند بر اساس ترافیک هایی که ما مشخص می کنیم (Access Rule )به برخی از ترافیک ها اجازه عبور دهد یا جلوی آنها را بگیرد**

**تمامی فایروال ها وقتی به ترافیکی برخورد می کنند یکی از این 3 عمل را انجام می دهند**

ACCEPT

DROP

DENY

Farid Ajabnoush

اگر ترافیکی DROP بشه یعنی اینکه فایروال اجازه عبور به آن ترافیک را نداده است و شما متوجه می شویدکه فایروال جلوی آن را گرفته است.

اگر ترافیکی DNEY بشه یعنی اینکه فایروال اجازه عبور به آن ترافیک را نداده است و شما متوجهنمی شویدکه فایروال جلوی آن را گرفته است.

تمامی فایروال ها در یکی از 3 لایه زیر کار می کنند:

1)DATA LINK

2)NETWORK LINK

3)APPLICATION LINK

DATA LINK:

در این لایه فایروال بر اساس Mac Address کار می کند.

NETWORK LINK:

در این لایه فایروال بر اساس IP کار می کند.

1) Source Ip
2) Destination Ip
3) Spork
4) Dport
5) Protocol Type

به 5 روش بالا که برای فیلترینگ به کار می رود Packet Filter گویند.

فایر وال ویندوزها در لایه NETWORKکار می کنند.

FarshidAjabnoush

APPLICATION LINK:

در این لایه فایر وال ها بر اساس Content (لغت) عمل فیلترینگ را انجام می دهند.

به فایروال هایی که در این لایه کار می کنند و عمل فیلترینگ را انجام می دهند پروکسی گویند.

- فایر وال ها به تنهایی امن نیستند،برای امنیت بیشتر احتیاج به مکمل هایی به نامIDS و یاIPS دارند.

IDS (Intrusion DetectionSystem ):

فقط تشخیص می دهد که باید جلوی این ترافیک را بگیرد.

IPS (Intrusion PreventionsSystem):

می تواند هم تشخیص دهد و هم جلوی ترافیک را بگیرد.

تمامی Admin ها از IDPS استفاده می کنند به نام SNORT

ابتدا باید فایروال نصب شود سپس IDS یا IPS

در ویندوزها 2نوع فایر وال داریم:

1) ICF (Internet Connection Firewall)

این نوع از فایر وال هم در ویندوزهای NG و هم در ویندوزهایLEGASY وجود دارد، همان ویندوز فایر وال است

2) Windows Firewall With Advanced Security

این نوع فایر وال فقط در ویندوزهای NG است.

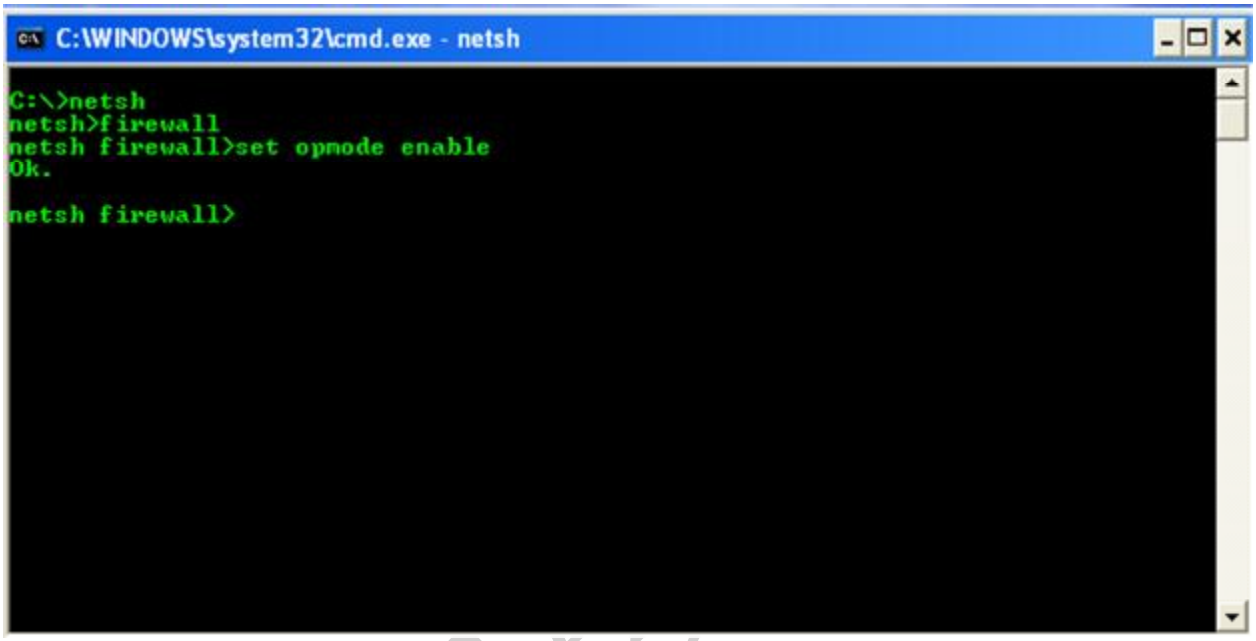
FarshidAjabnoush

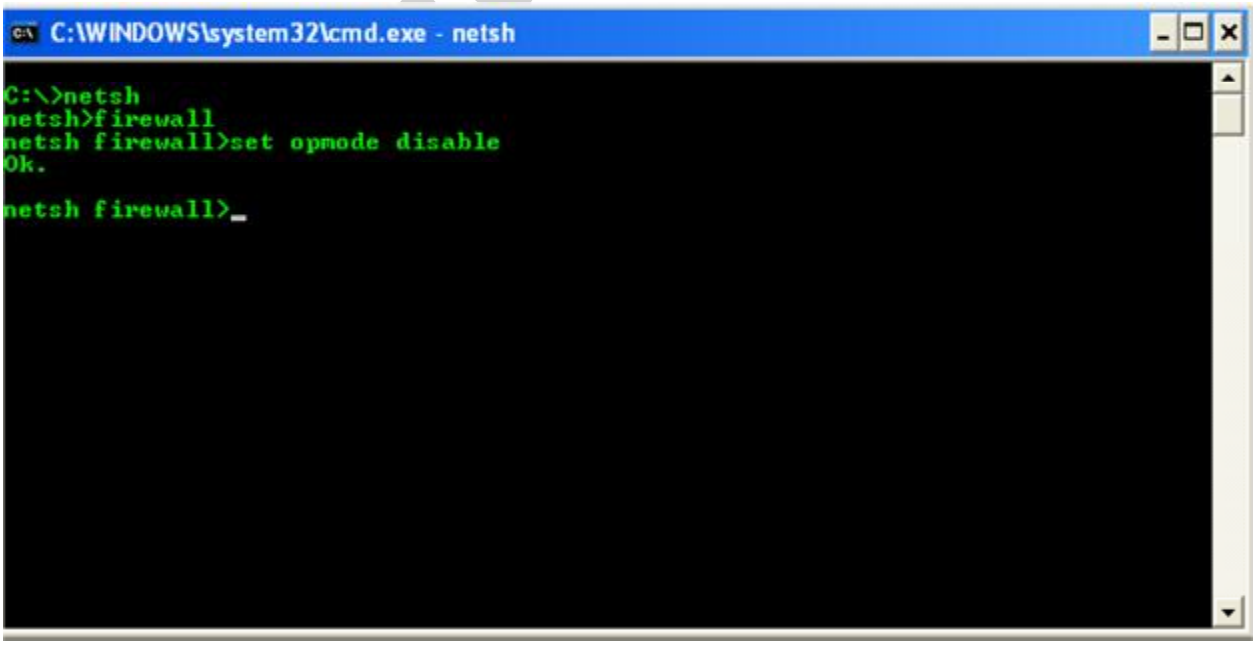
: Command Firewall

**فعال و غیر فعال کردن فایر وال:**

Netshfirewall Set opmode enable

Disable

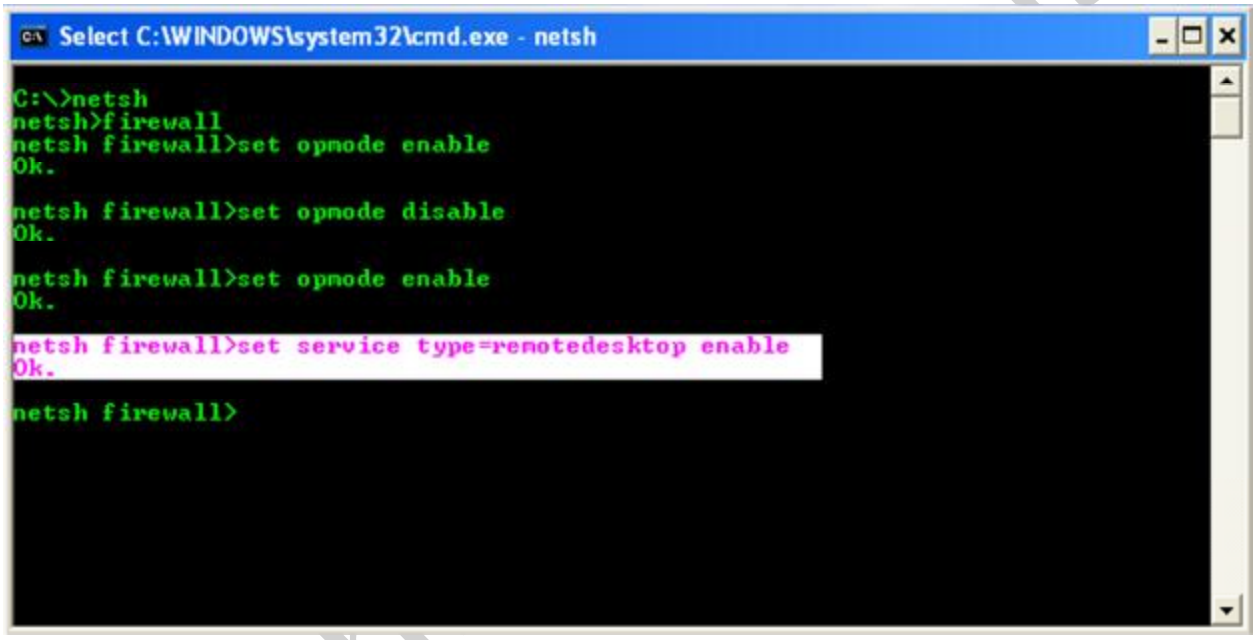


**با فعال بودن یا غیر فعال بودن فایروال می توان یک سری از سرویس ها را فعال یا غیر فعال کرد**

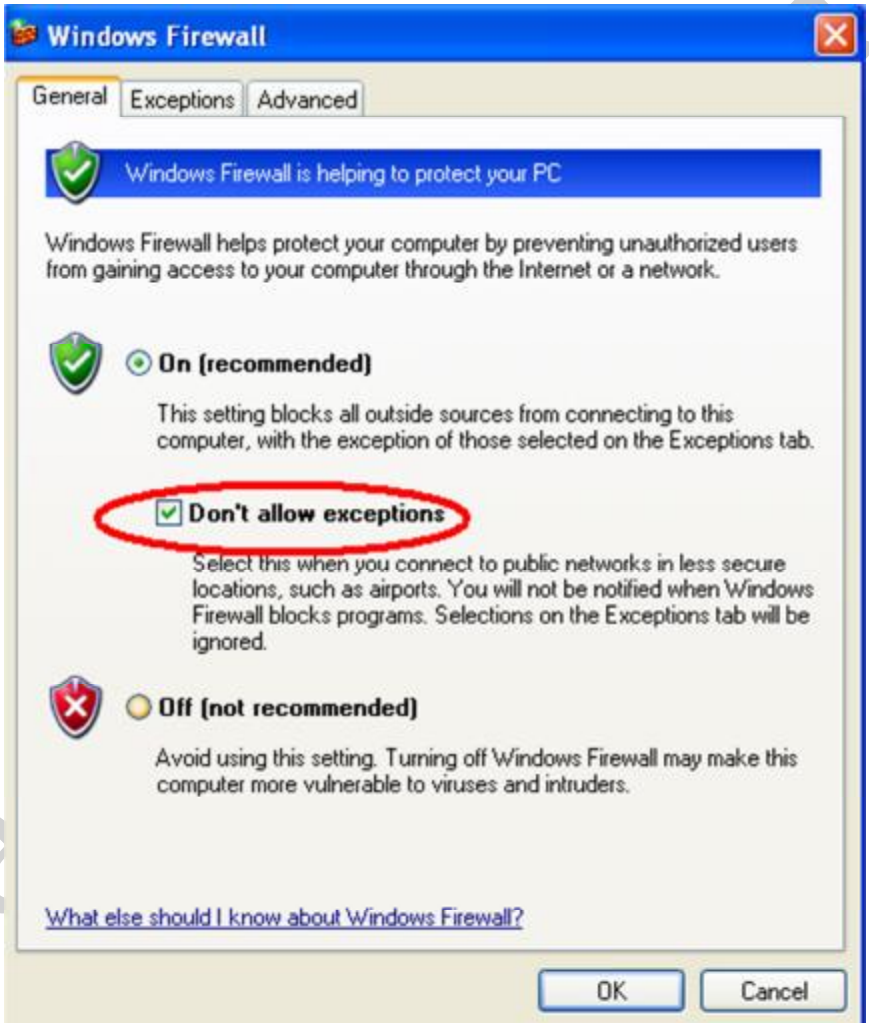
Remote Desktop,File Sharing و.....

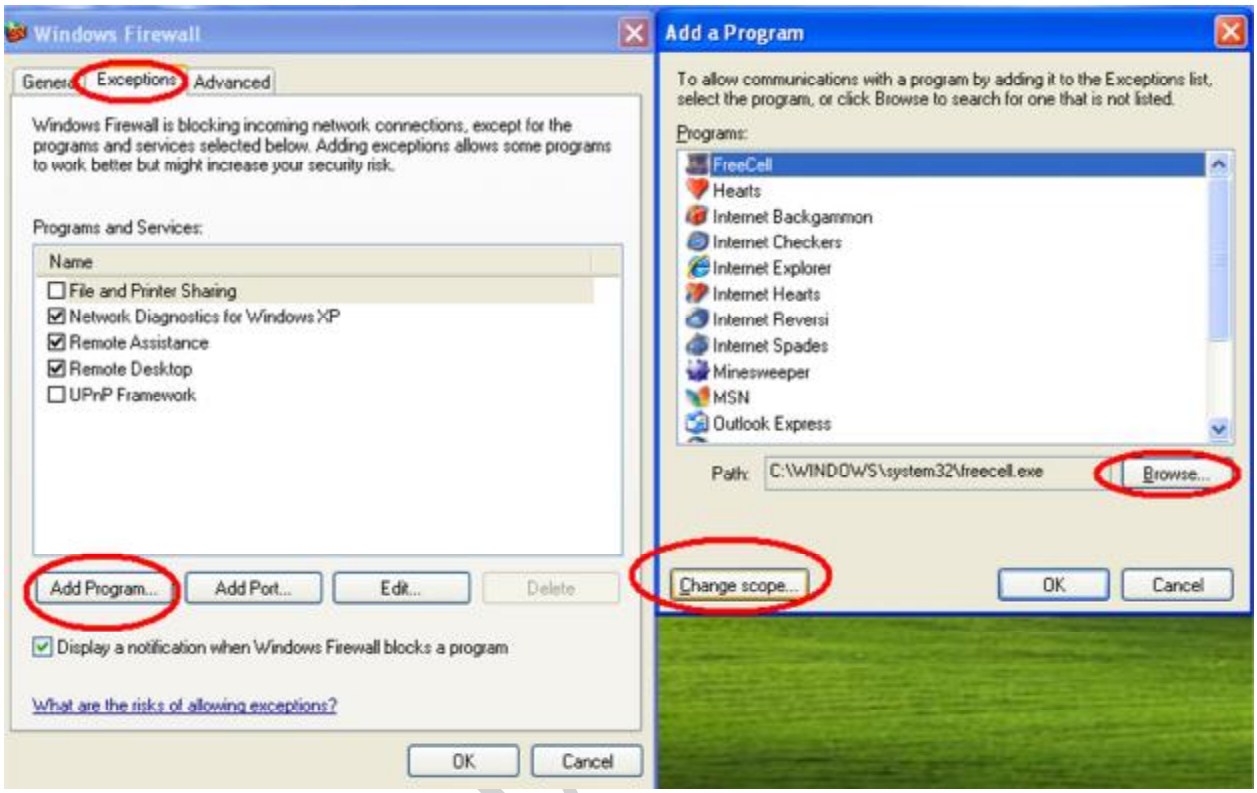
NetshfirewallSet service type=remotedesktop enable




Farsh

در ویندوزهای Legacy وقتی فایروال را فعال می کنیم اگر تیک گزینه Don't Allow Exceptions را بزنیم دیگر هیچ کس نمی تواند وارد شود و اگر تیک را نزنیم از یک سری پورت ها و نرم افزارها که در تبExceptionsهستند می توان وارد شد(Exceptions= استثناء)

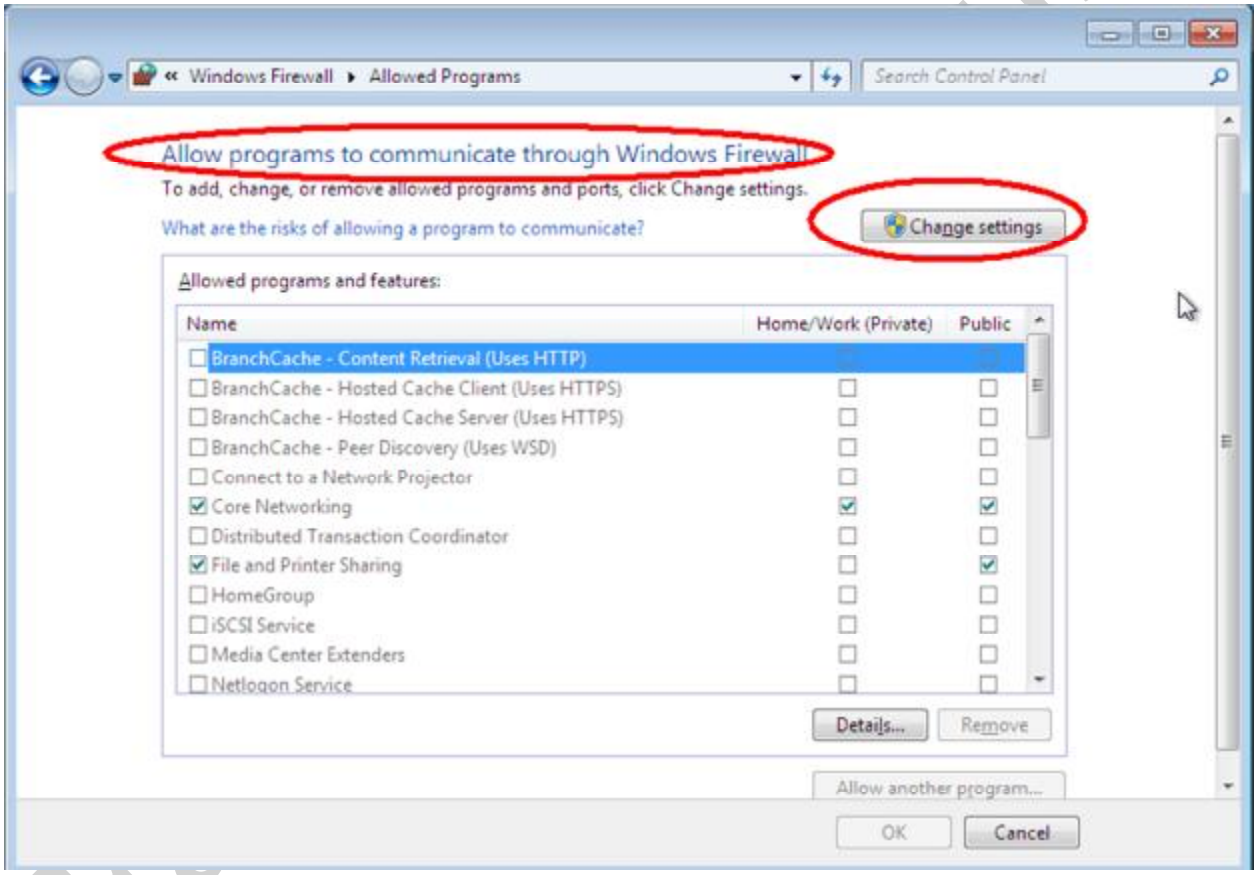





در اینجا می توان برنامه و یا پورتی را هم اضافه کرد تا در هنگام فعال بودن فایروال بتوان از آنها استفاده کرد البته در صورتی که گزینه Don't Allow Exceptions فعال نباشد، با زدن Change Scope می توان تنظیم کرد که کدام آی پی ها می توانند به این نرم افزارها دسترسی داشته باشند.

Farshid

معادل Exceptions در ویندوزهای NG گزینه Allow Program To Communicate Through Windows Firewall است



پورت های مهم:

| | | | | | |
|---|---|---|---|---|---|
| PING | 7 | SSH | 22 | DHCP | 67 |
| FTP | 21 | SMTP | 25 | HTTP | 80 |
| TELNET | 23 | DNS | 53 | POP3 | 110 |
| IMAP | 143 | SHARING | 445 | HTTPS | 443 |

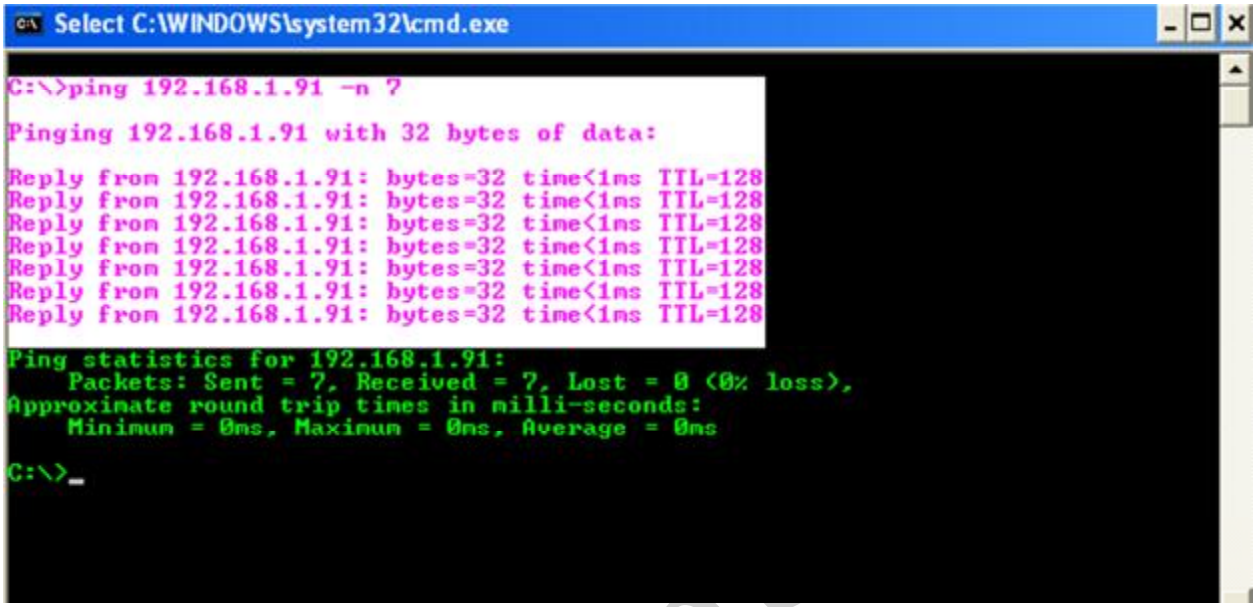
IMAP و POP3 پورت های دریافت ایمیل می باشند تفاوت این دو در این است که IMAP فقط موضوع ایمیل را نشان می دهد و برای دیدن کل ایمیل باید روی آن کلیک کرد ولی POP3 کل ایمیل را نشان می دهد،سرعت IMAP از POP3 بیشتر است.

SMTP پروتکل ارسال ایمیل است.

- هنگامی که می خواهیم وارد ایمیل خودمان بشویم در صفحه ای که یوزر و پسورد را وارد می کنیم داریم از پورت POP3 استفاده می کنیم.

FarshidAjabnous

با دستور n– می توان تعداد دفعات پینگ کردن را تغییر داد




در اینجا ما تعداد دفعات را به7 تغییر دادیم یعنی n7–

TTL نشان دهنده تعداد روترهای موجود در مسیر است،حجم پکت ها را می توان با L– تا ماکزیمم سایز 65500 بایت تغییر داد.

ICMP پیک شبکه است.

در پروتکل TCP سرعت پایین ولی امنیت بالا است،در پروتکلUDP سرعت بالا ولی امنیت پایین است.

در ویدئو کنفرانس و VOIP از UDP استفاده می شود.

FarshidAja

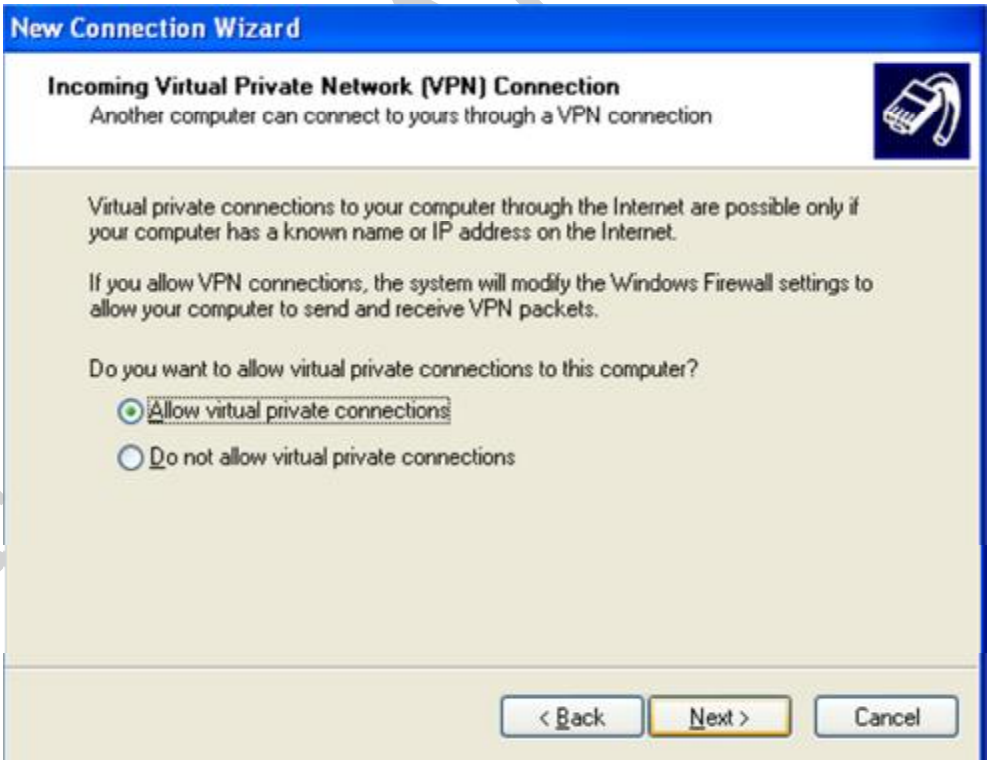
ساختن VPN بین 2 XP :

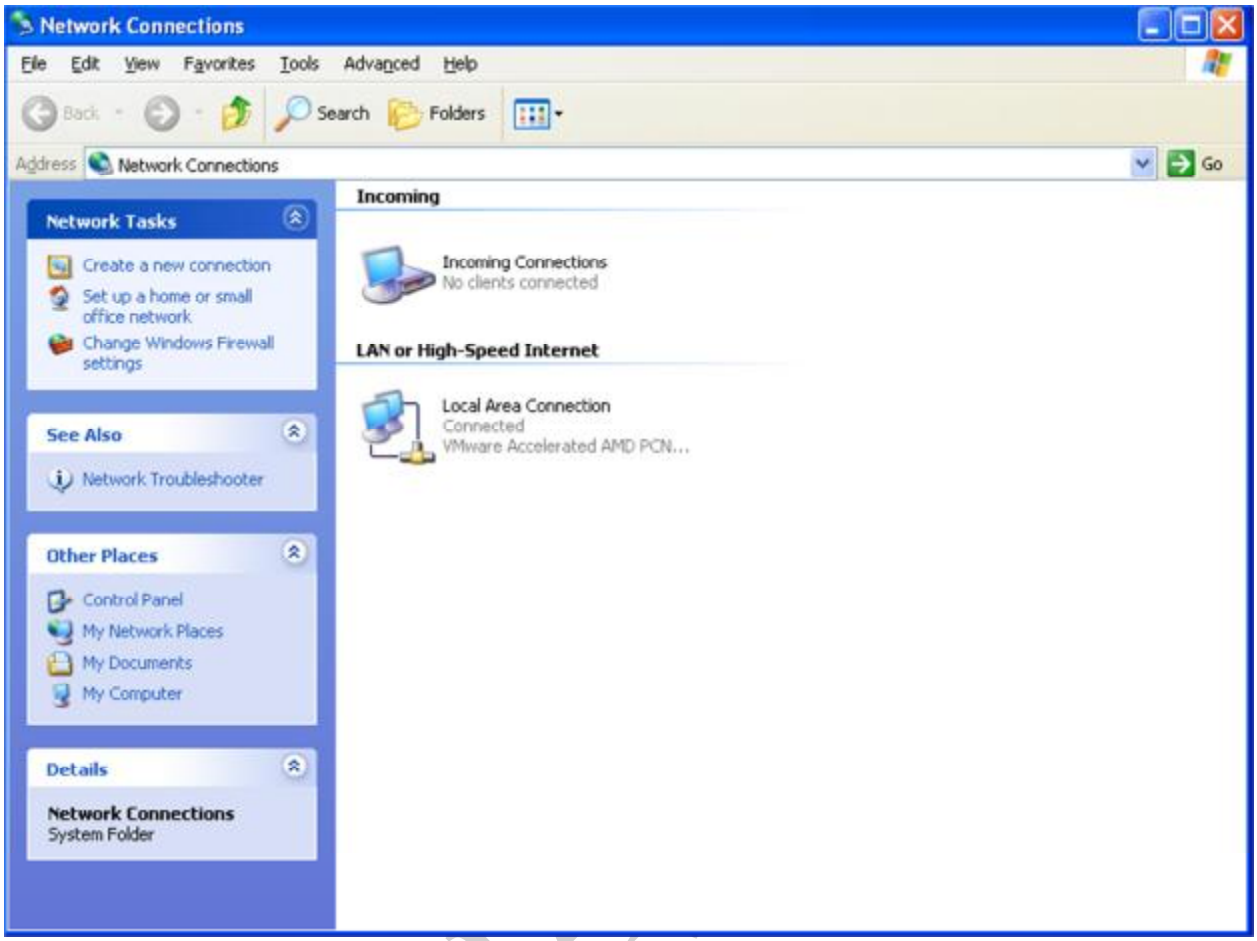
**ابتدا باید از سیستم مقصد شروع کنیم**

**برای شروع باید یک کانکشن VPN بصورت زیر در سیستم مقصد بسازیم**

Farsi

New Connection Wizard
Advanced Connection Options
Which type of connection do you want to set up?
Select the connection type you want:
Accept incoming connections
Allow other computers to connect to this computer through the Internet, a phone line, or a direct cable connection.
Connect directly to another computer
Connect to another computer using your serial, parallel, or infrared port.
< Back
Next >
Cancel


New Connection Wizard
Incoming Virtual Private Network (VPN) Connection
Another computer can connect to yours through a VPN connection
Virtual private connections to your computer through the Internet are possible only if your computer has a known name or IP address on the Internet.
If you allow VPN connections, the system will modify the Windows Firewall settings to allow your computer to send and receive VPN packets.
Do you want to allow virtual private connections to this computer?
Allow virtual private connections
Do not allow virtual private connections
< Back
Next >
Cancel




**همانطور که در شکل بالا میبینیم با اتمام مراحل ساخت کانکشن،کانکشنی به نام Incoming Connections در سیستم مقصد ساخته می شود**

Farshidan

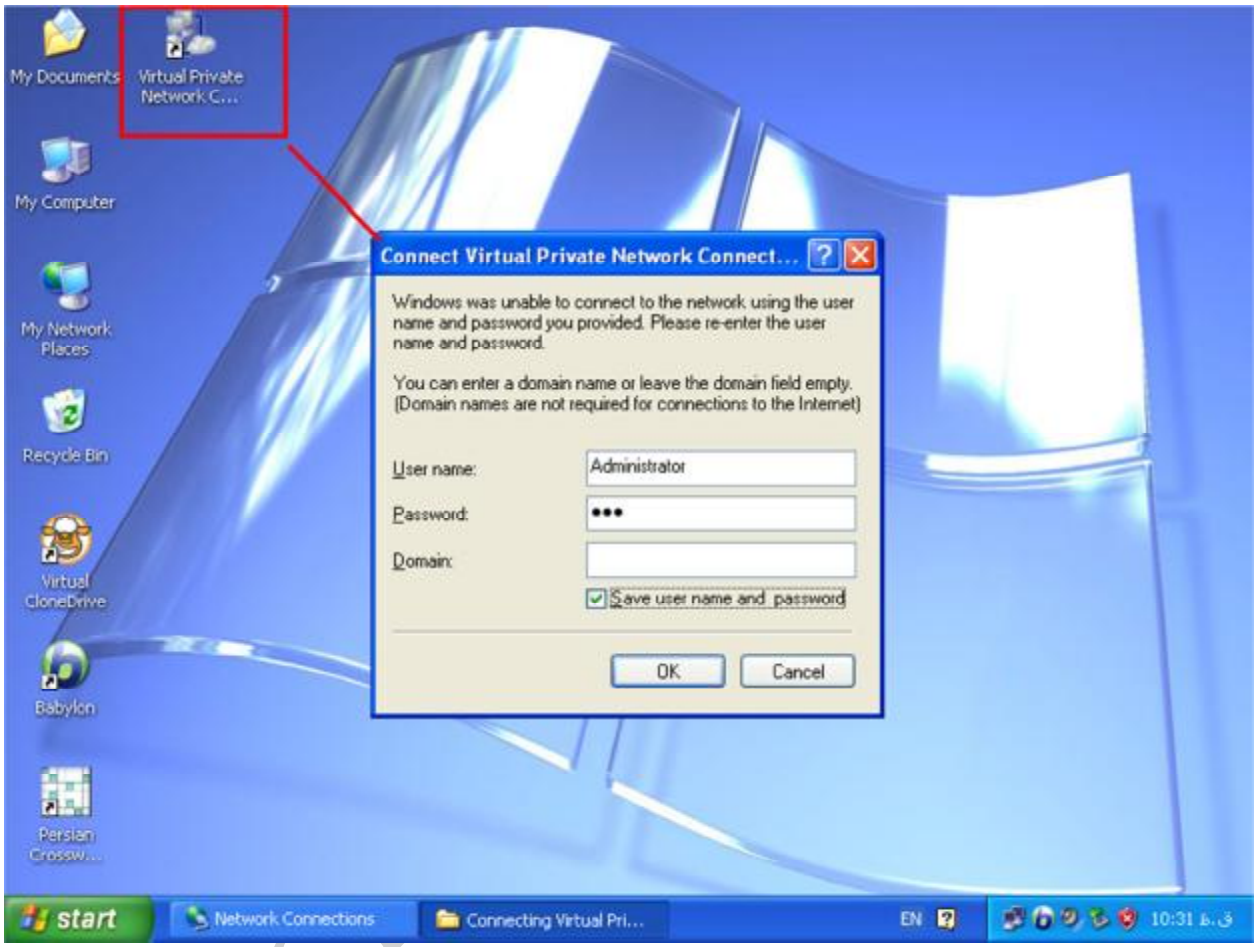
**حالا نوبت به سیستم مبدأ می رسد**

**در اینجا هم باید کانکشن به صورت زیر بسازیم**

**در مرحله3 باید آی پی سیستم مقصد را وارد کنیم(شکل بالا)**

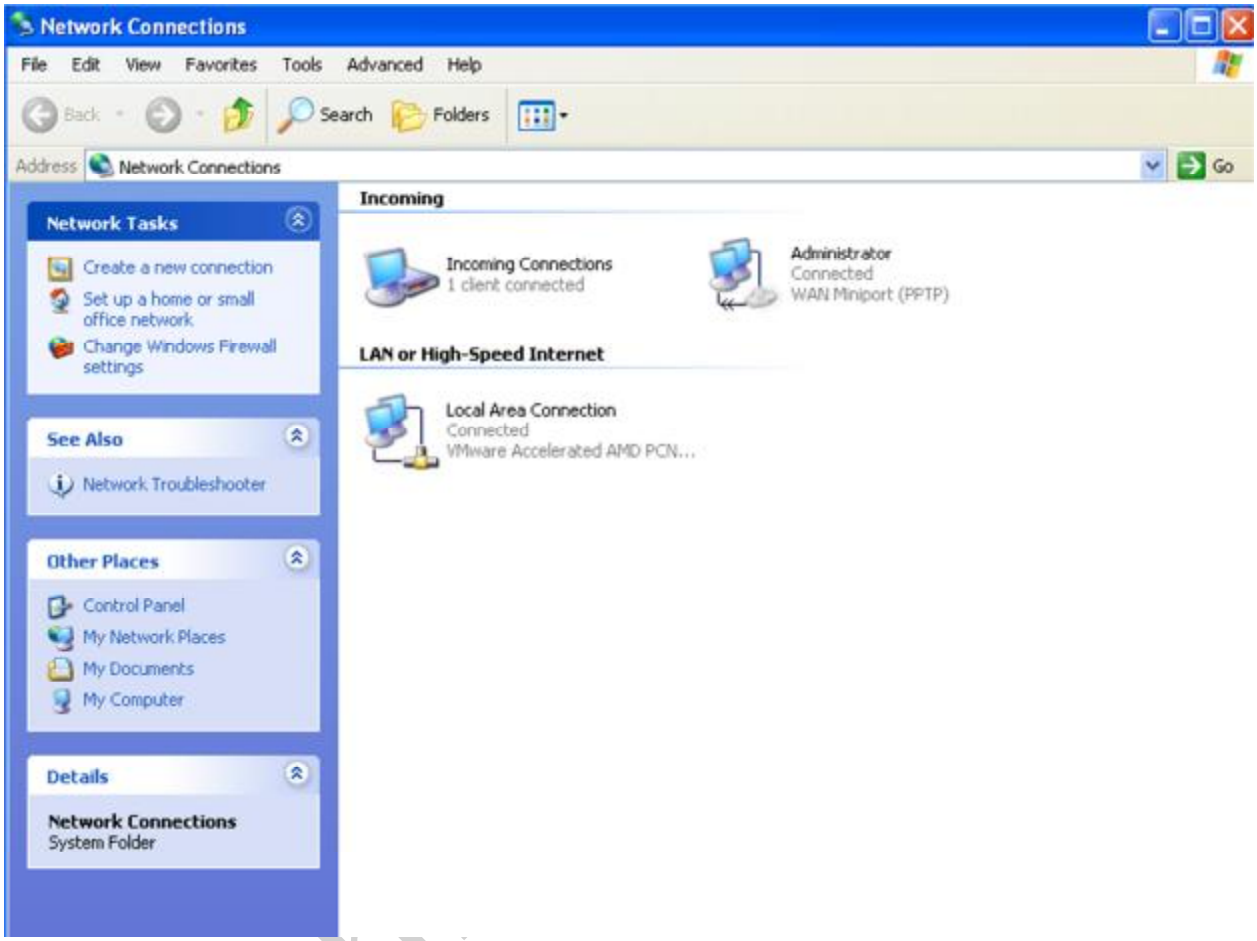
Farshid

بعد از اتمام مراحل نوبت به اتصال می رسد،برای اولین اتصال از سیستم مبدأ به مقصد با پنجره زیر مواجه می شویم که باید نام کاربری و رمز عبور سیستم مقصد را وارد کنیم.




Fars

و در نهایت موقع وصل شدن به سیستم مقصد کانکشن ها در سیستم مقصد به شکل زیر نمایان می شود




VPN زدن باعث می شود تا اطلاعات از یک کانال امن بین سیستم های در حال ارتباط با هم ردوبدل شود.

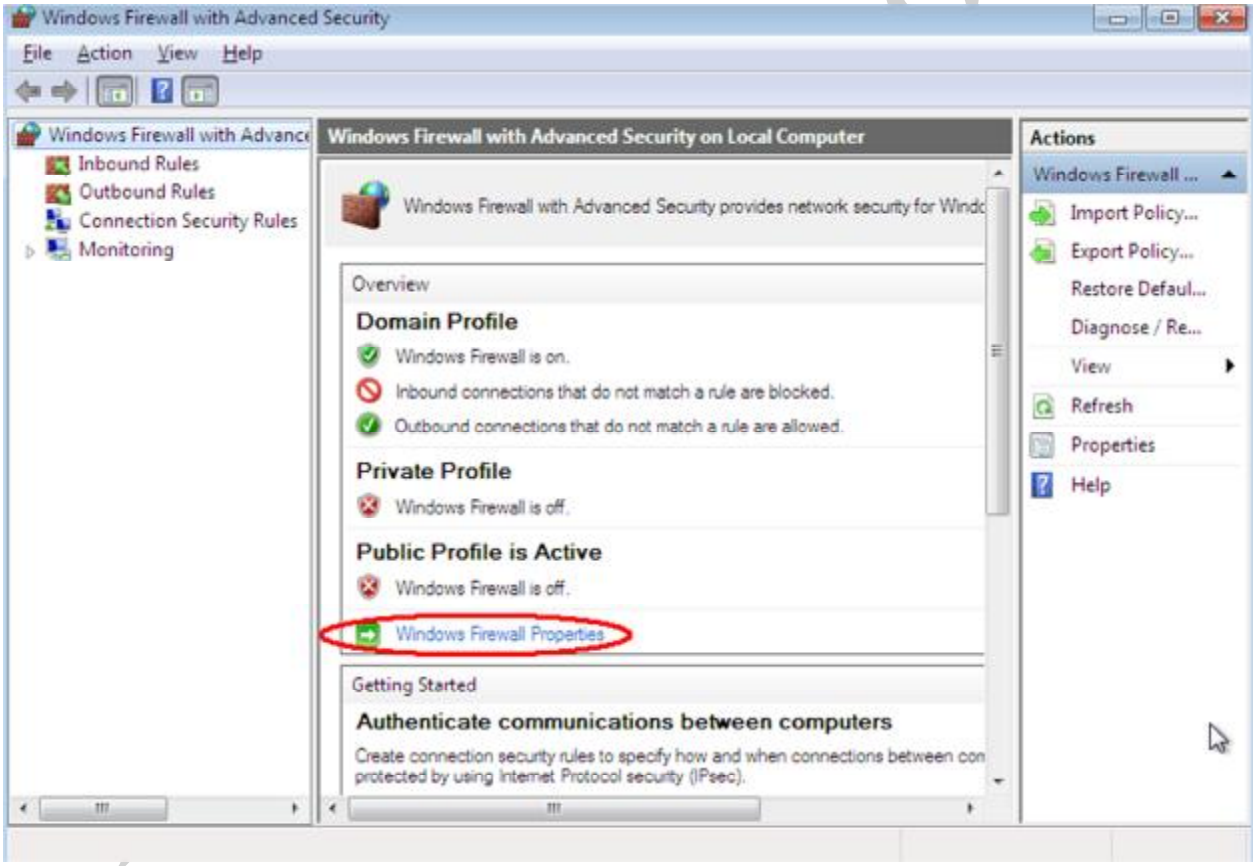
Farsi

Windows Firewall With Advanced Security

**این گزینه همان فایروال در ویندوز7 می باشد که از 2 مسیر قابل دسترسی می باشند:**

Run Gpedit.mscComputer ConfigurationWindows SettingSecurity SettingWindows Firewall(1

Cotrol PanelAdministrativeToolsWindows Firewall(2



این فایروال شامل 3 پروفایل می باشد:

Domain: برای کامپیوترهایی استفاده می شود که عضو شبکه دامینی باشند.

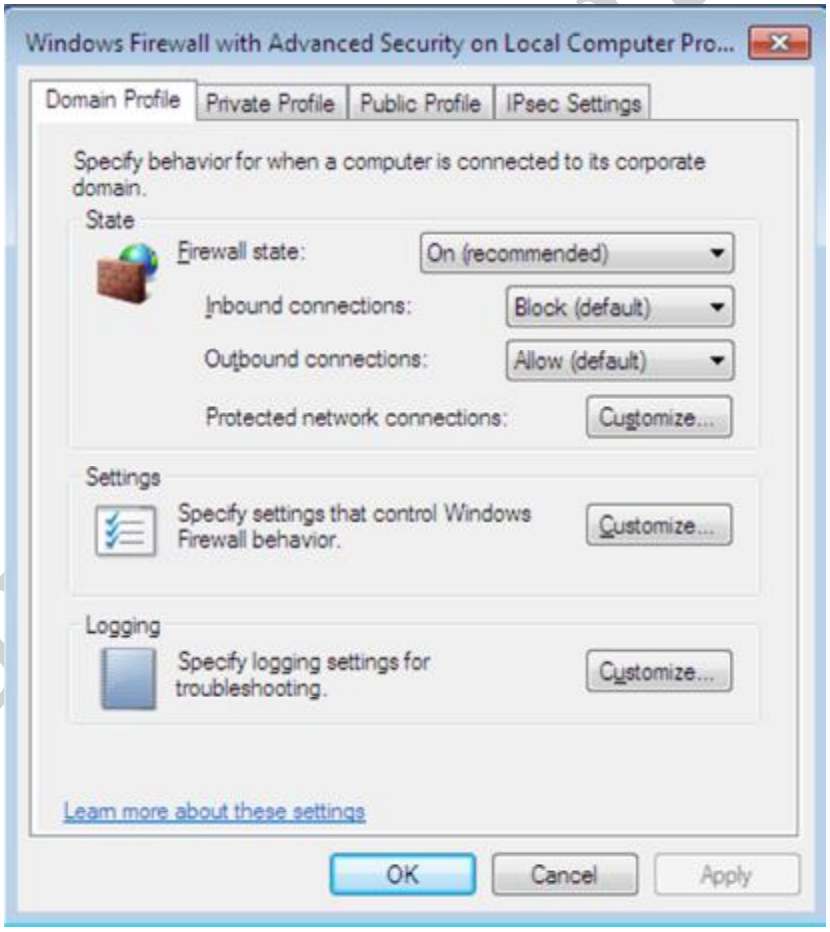
Private : برای کامپیوترهای خانگی یا شبکه های Workgroup استفاده می شود.

Public :زمانی که به اینترنت متصل می شویم به روی این پروفایل می رویم.

- امنیت در پروفایل Public از بقیه پروفایل ها بالاتر است

برای ایجاد تغییر در تنظیمات این پروفایل ها از گزینه Windows Firewall Properties استفاده می کنیم.

وقتی که وارد گزینه گفته شده می شویم با منوی زیر مواجه می شویم که در آن همه تنظیمات 3 پروفایل مانند یکدیگر است.



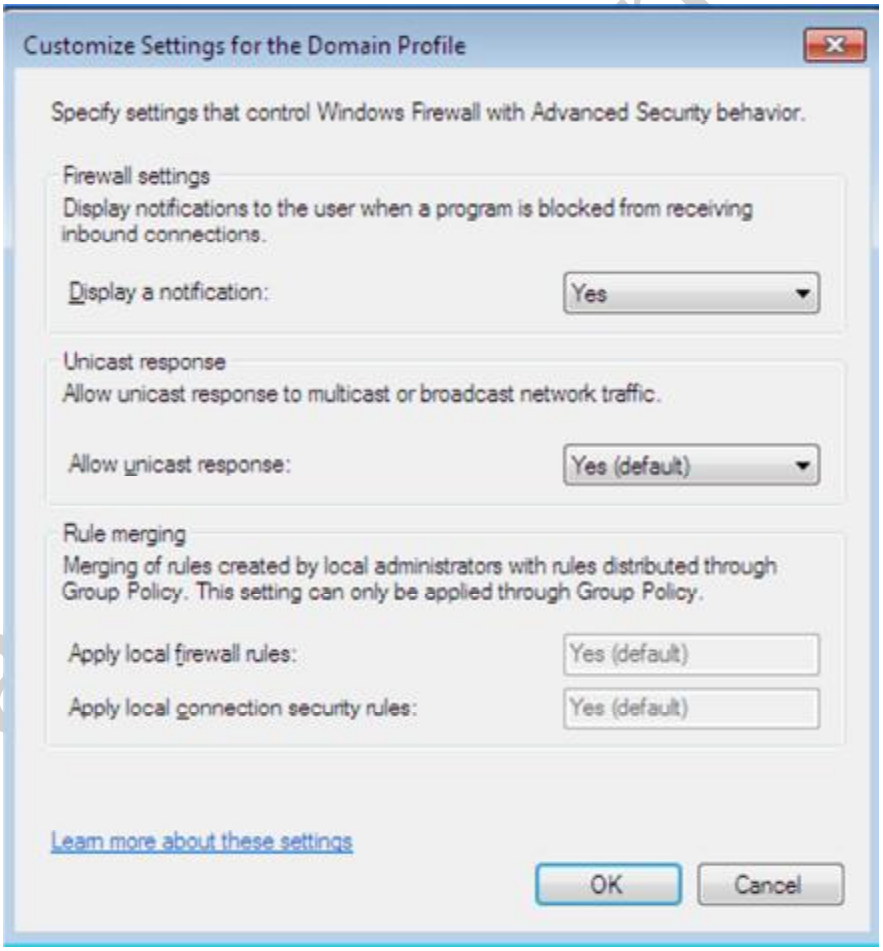
Inbound Connection :

**این گزینه به صورت پیش فرض بر روی Block تنظیم می باشد که باعث می شود فایروال جلوی ترافیک های ورودی به سیستم را بگیرد.**

Outbound Connection:

**این گزینه به صورت پیش فرض بر روی Allow تنظیم می باشد که اجازه عبور به ترافیک های Exceptions را می دهد،با تغییر این گزینه به Block حتی دیگر Exceptions هم اجازه عبور ندارد.**

**با زدن گزینه Customize در Setting با منوی زیر مواجه می شویم**



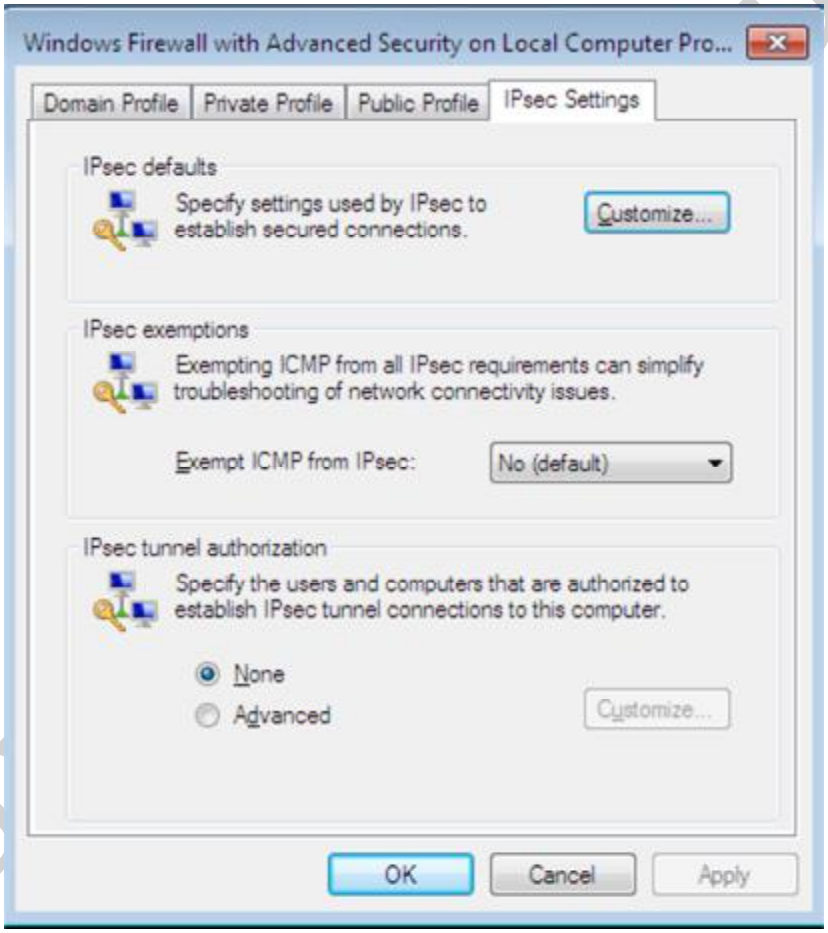
: Unicast Response

وقتی در شبکه Unicast,Multicast,Broadcast انجام می شود تا3 ثانیه شما اجازه جواب دادن را دارید اگرجواب دادن شما بیشتر از این زمان طول بکشد فایروال جلوی جواب دادن شما را می گیرد.

: Rule Merging

با فعال بودن این گزینه اگر در شبکه بر روی سیستم Client فایروال تنظیم باشد و بر روی سرور هم فایروال تنظیم باشدتنظیماتهر2 فایروال را اجرا می کند.

تبIpsec Setting( Internet Protocol Security) :



توسط سه پروتکل IpSec–VPN–SSL می توان بر روی انتقال داده ها ایجاد امنیت کرد.

بیشترین کاربرد پروتکل IpSec در شبکه های LAN می باشد،از پروتکل VPN هم در شبکه های LAN وهم در شبکه های WAN (اینترنت) می توان استفاده کرد،پروتکل SSL را هم در شبکه های WAN استفاده می کنند.

نمونه ای از پروتکل HTTPS،SSL می باشد.

با استفاده از IPSEC می توان برای اینکه فایروال به کسی اجازه عبور دهد شرط گذاشت،مثلاً به شرطی اجازه عبور به کاربرA را بدهد که تمامی پکت های کاربر مورد نظر توسط Ipsec رمز گذاری شده باشد.

زمانی که 2 کامپیوتر بخواهند از طریق Ipsec اطلاعات را ردوبدل کنند ،2کامپیوتر باید از قبل مشخص باشند (همدیگر را بشناسندAuthenticate )

Ipsec برای شناسایی از سه پروتکل "CA" Kerberos,Pre Shared Key,Certificate استفاده می کند.

Kerberos :

برای استفاده از این پروتکل همه کامپیوترها باید عضو یک شبکهدامینی باشند.

Pre-Shared Key :

قبل از ارسال اطلاعات سیستم ها باید به هم وصل شوند به این ترتیب که 2 سیستمی که می خواهند با هم ارتباط برقرارکنند باید هردو یک پسورد را وارد کنند وسپس به هم وصل می شوند و در آخر اطلاعات را با هم ردوبدل می کنند( مانند بعضی از بلوتوث های موبایل )

Certificate(CA) :

به سروری که SSL را تولید می کند CA گویند.

CA دنیا تحت اختیار 2 شرکت به نام های Verisign وGeotrust می باشد،CA ایران تحت اختیار وزارت بازرگانی می باشد.

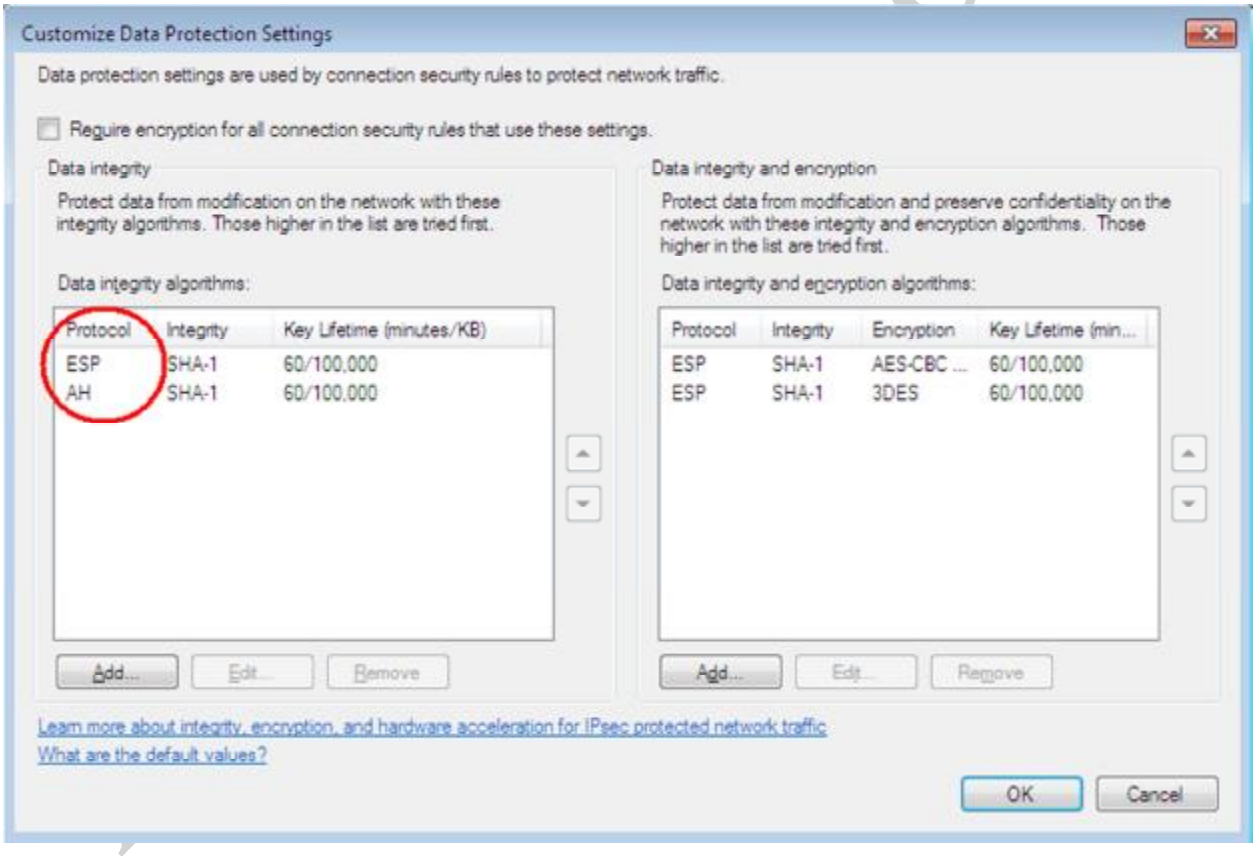
FarshidAjabnoush

از پروتکل IKE(Internet Key Exchange) برای معاوضه کلیدها بین سیستم ها استفاده می شود.

Protocol (Encryption =Aes-Des-3ps)

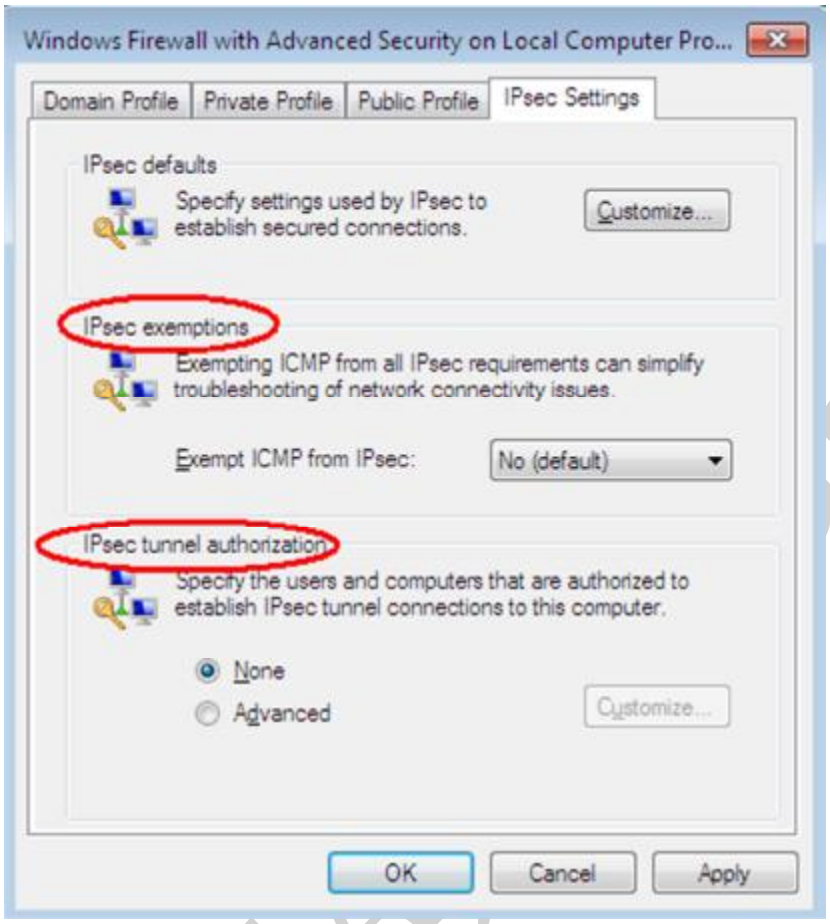
رمز گذاری

Protocol(Hashing-Md5-Sha)Integrity=




ESP=Encapsulate Security Payload

AH=Authentication Header

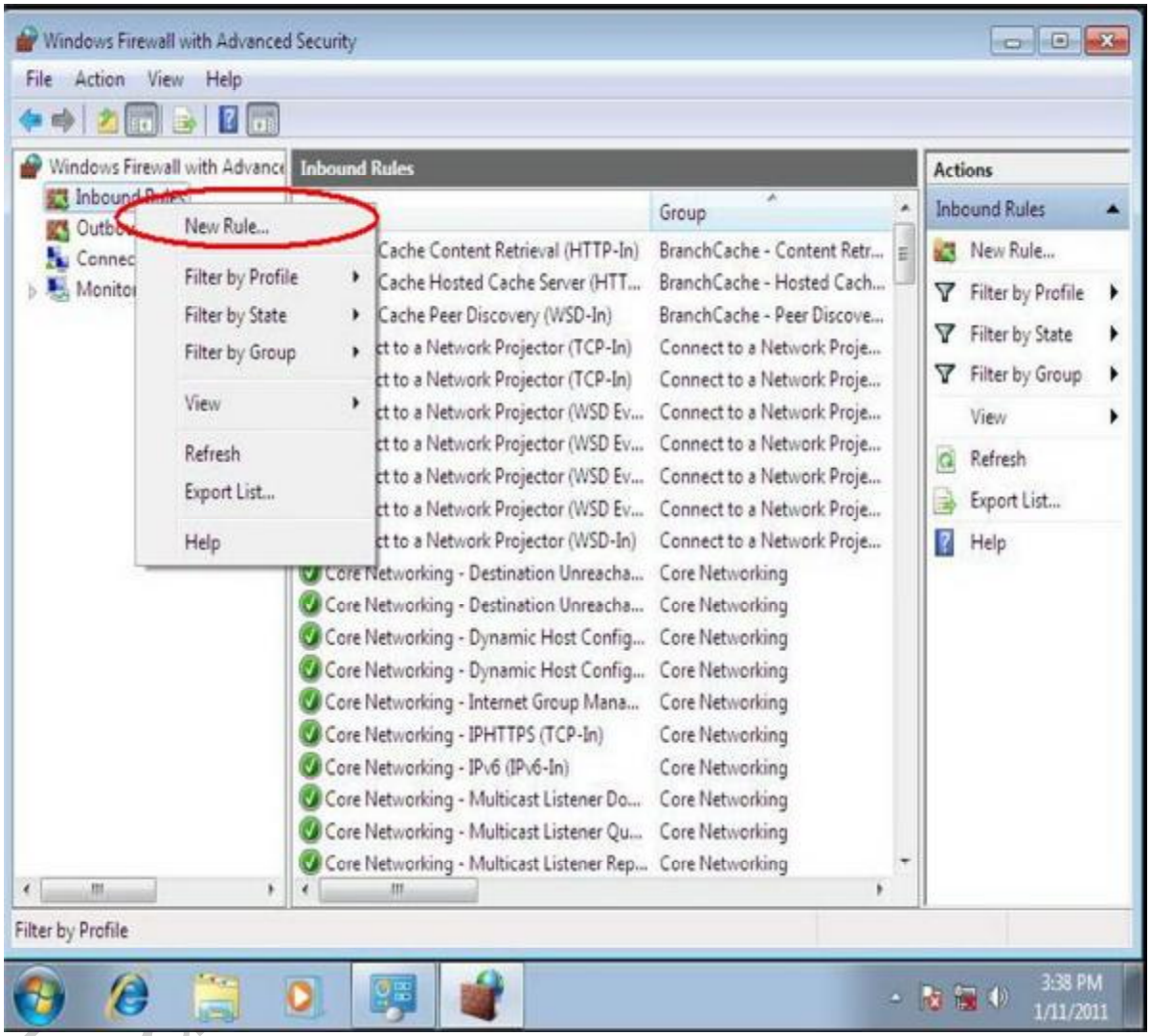


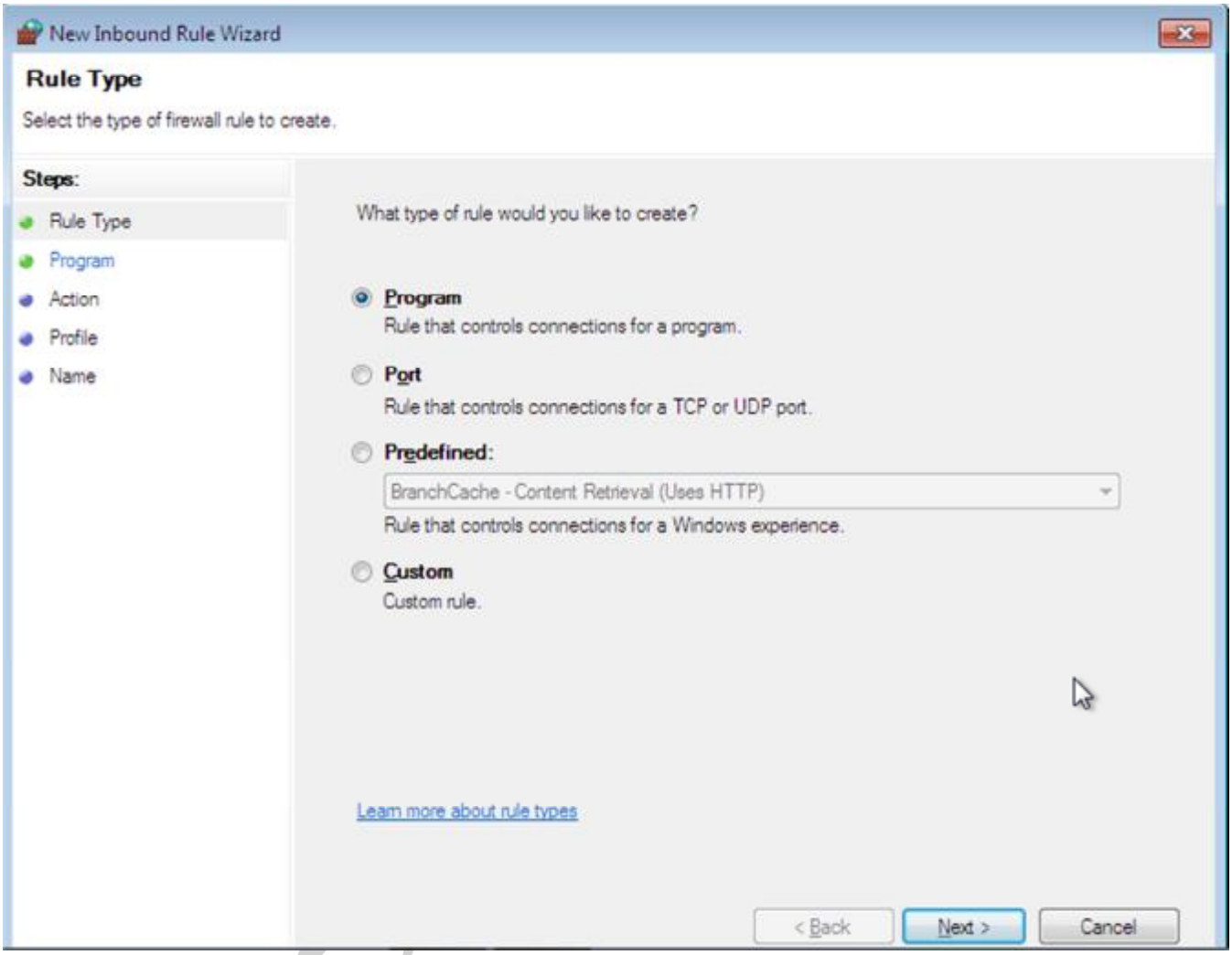

در قسمت Ipsec exemption از ما سؤال می کنه که می خواهید پکت های پینگ(Ping ) هم رمز بشن؟

در قسمتIpsec tunnel authorization از ما سؤال می کنه که می خواهید اطلاعاتی را هم که از طریق تونلی مثل VPN عبور میکند رمزگذاری کند؟

FarshidAsh

برای اضافه کردن Rule به فایروال مراحل زیر را طی می کنیم:




New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.
Custom
Custom rule.
Learn more about rule types
< Back
Next >
Cancel

Fars

1) پردازنده کد موجود در رام بایوس را که نشان دهنده ویژگی به نام پست( Post ) را اجرا می کند.
2) کد موجود در بایوس به512 بایت اول هارد اشاره می کند که بیانگر جدولی به نام MBR می باشد.
- به اولین سکتور داخل درایوی که قابلیت بوت را دارد بوت سکتور گویند.
3) زمانی که بوت سکتور اجرا می شود همزمان با اجرا شدن خود برنامه ای به نام Boot Mgr را هم اجرا می کند در ویندوز ,XpBoot Mgr به نام NTLDR می باشد.(Windows Boot Managing )
4) هنگامی که Boot Mgr اجرا شد از حالت Protected Mode به حالت Real Mode تغییر پیدا می کند.
- حالت Protected Modeحالتی از پردازنده است که در آن فقط یک برنامه به حجم 640 کیلو بایت از رم را می تواند اجرا کند.
- حالت Real Mode حالتی از پردازنده است که در آن می تواند چندین برنامه به حجم کل رم را اجرا کند.
5) Boot Mgr محتویات فایل BCD (Boot Configuration Data ) را خوانده ولیست ویندوزها را برایمان می آورد،معادل فایل BCD در Xp فایلBoot.ini می باشد.
6) با انتخاب یکی از سیستم عامل ها لود کرنل آن و مقدار دهی آن انجام می شود، مسیر آن در System32\ntoskrnl.exe می باشد، و می توان این فایل را با نرم افزار Res Hack باز کرد.
7) سخت افزارها و Config آنها در قسمت HK LOCAL MECHINE\HARDWARE در رجیستری ویندوز می باشد.
8) مرحله ورود به ویندوز با اجرای فایل WinLogOn.exe شروع می شود.

FarshidAjabnoush

فایل های مهم در مرحله بارگذاری سیتم عاملLegacy به شرح زیر می باشد:

1)NTLDR( فایل های مهم برای لود سیستم عامل)

2)NTDETECT (شناسایی سخت افزار)

3)NTOSKRNL.EXE (هسته اصلی سیستم عامل)

4) HAL

- زمانی که کاربر بخواهد با هسته اصلی(Kernel ) ارتباط برقرار کند باید توسط لایه SHELL یا همانCMD

این کار را انجام دهد، اگر هسته اصلی بخواهد با سخت افزار ارتباط برقرار کند باید توسط HAL این کار را انجام دهد.

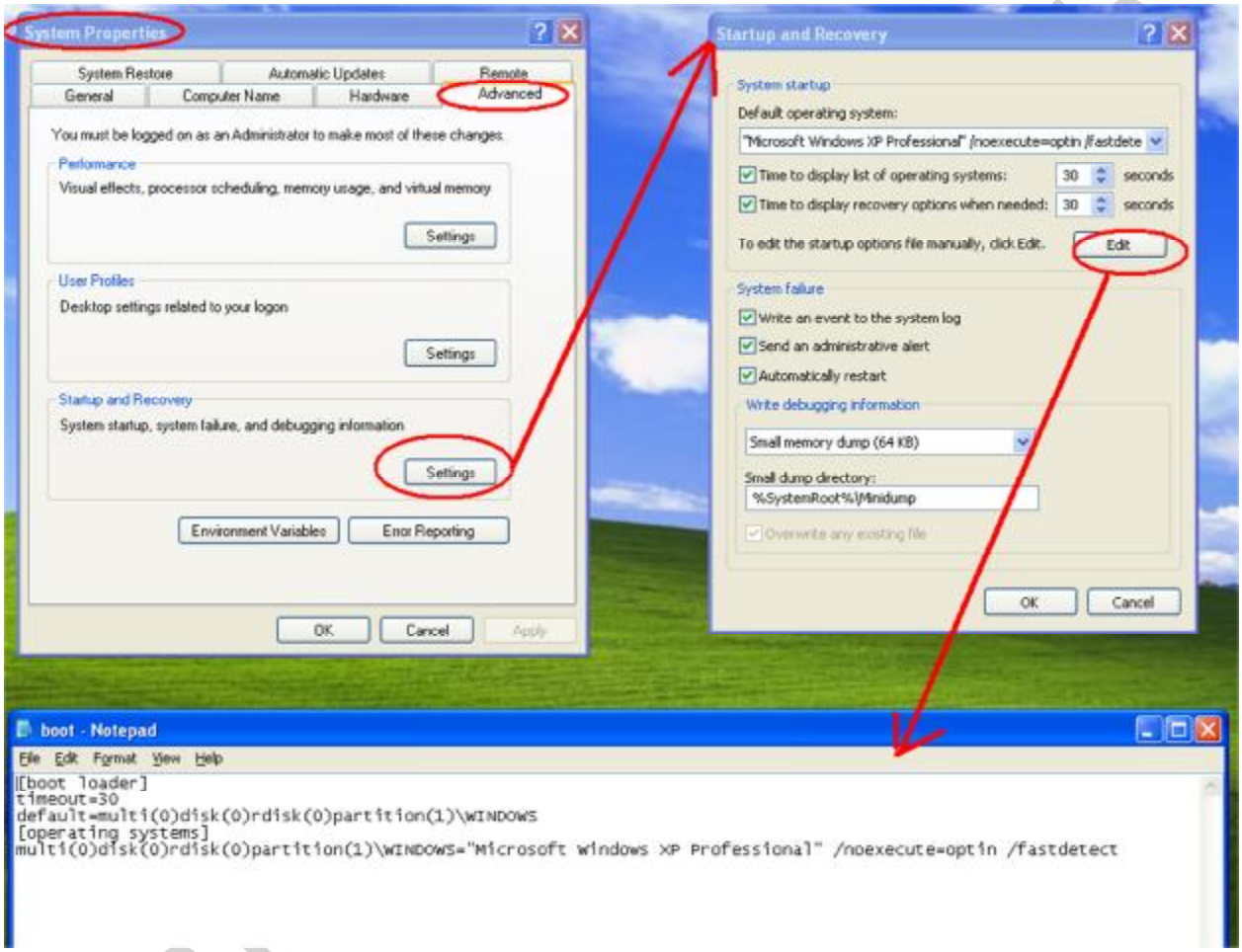
- بهترین نرم افزار برای بازگردانی سیستم عامل(Windows&Linux )Super Grub می باشد.

- فایل BCD که در ویندوزهای NG می باشد را می توان توسط نرم افزار EASY BCD ویرایش کرد.

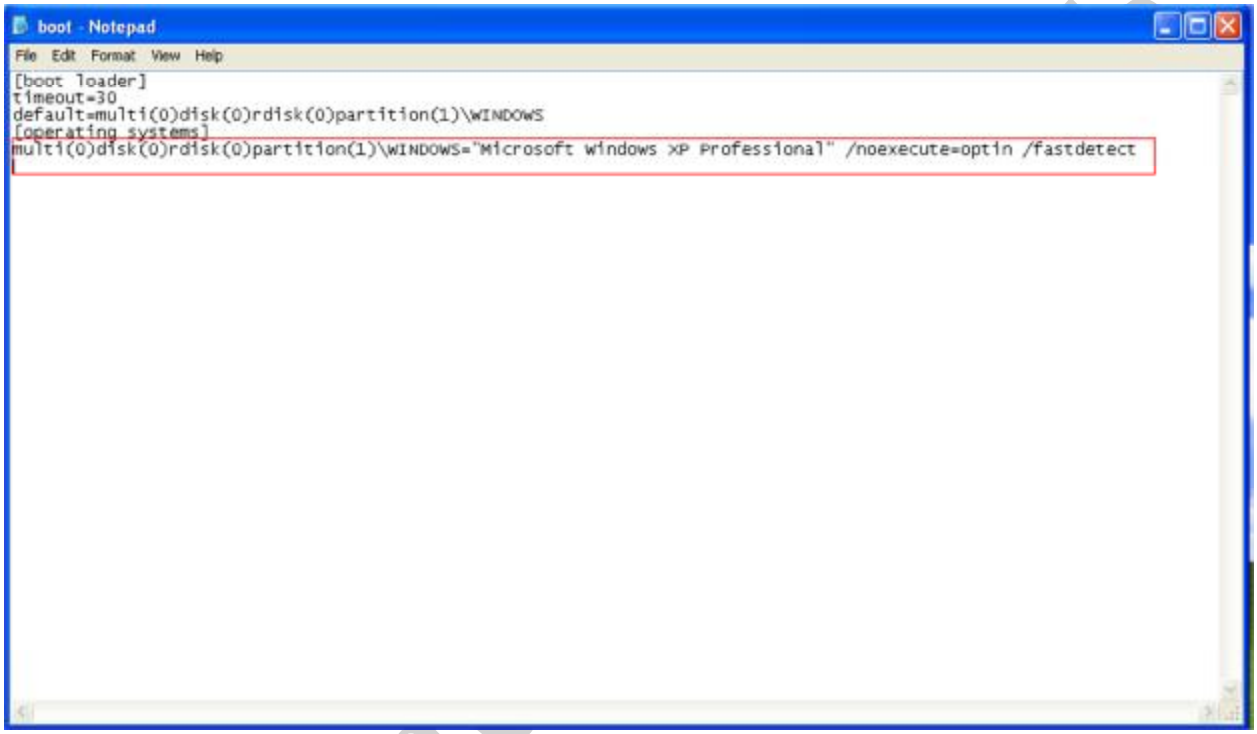
FarshidAjabnoush

:BOOT.INI

**این فایل در ویندوزهای Legacy(Xp ) موجود می باشد،برای دسترسی به این فایل مسیر زیر را طی می کنیم:**



در فایل متنی باز شده یکسری دستورات داریم که به آنها ARC PATH گویند که اطلاعاتی ازلحاظ سخت افزاری و نرم افزاری به ما می دهند.




Multi(0) : به ما نشان می دهد که ما هارد دیسک اسکازی داریم یا نه.

DISK(0) : در صورت داشتن هارددیسک اسکازی تعدادشان را نشان می دهد.

RDISK: نشان دهنده هارد دیسک IDEامی باشد.

PARTION(1): نشان دهنده پارتیشن بوت می باشد که=C1 یعنی پارتیشنC می باشد.

FASTDETECT : باعث می شود که سخت افزارهای اضافی موقع بوت شدن شناسایی نشوند.

Farshid

: Recovery

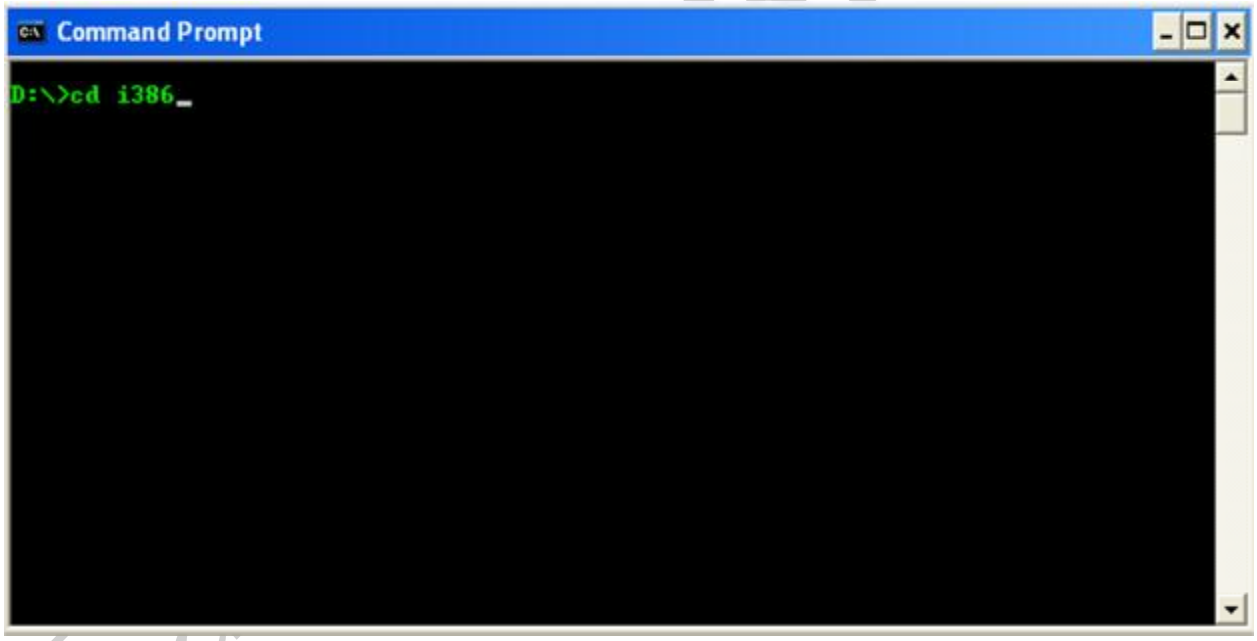
برای ریکاوری کردن ویندوز،در ویندوزهای NG از گزینهRecovery Option و در ویندوزهای Legacy از گزینه Recovery Console استفاده می کنیم.

:( Xp)Recovery

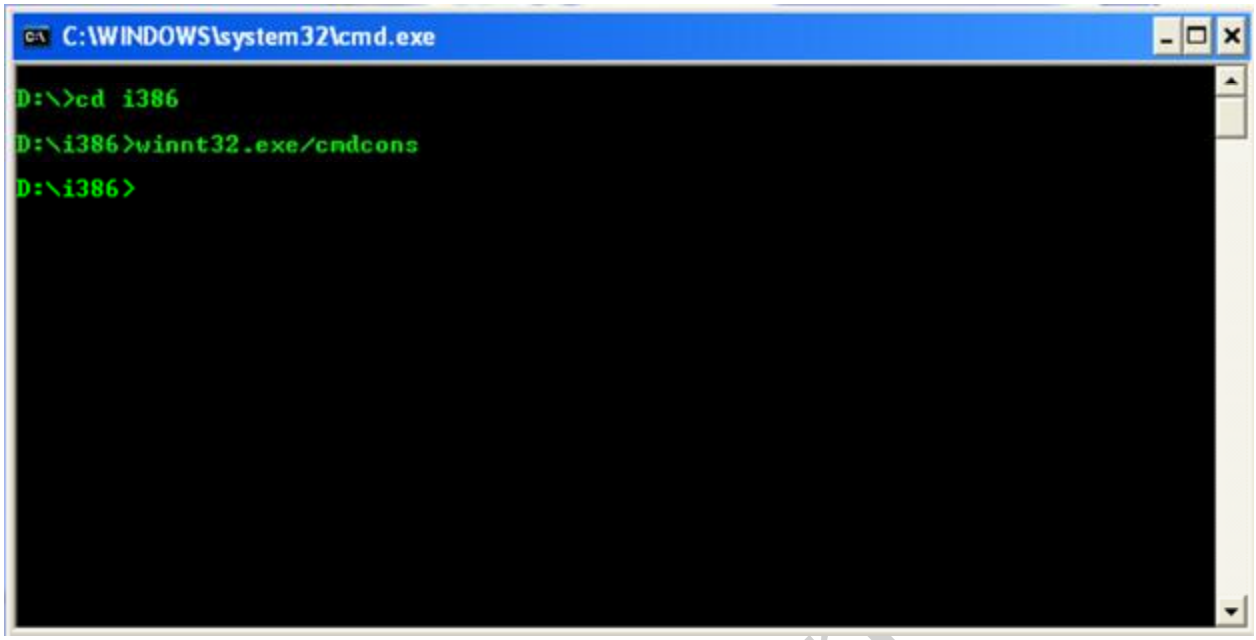
برای ریکاوری کردن در ویندوز 2 روش وجود دارد روش اول نصب کنسول ریکاوری در زمان سالم بودن ویندوز از داخل خود ویندوز می باشد روش دوم ریکاوری کردن ویندوز بعد از خراب شدن ویندوز می باشد.

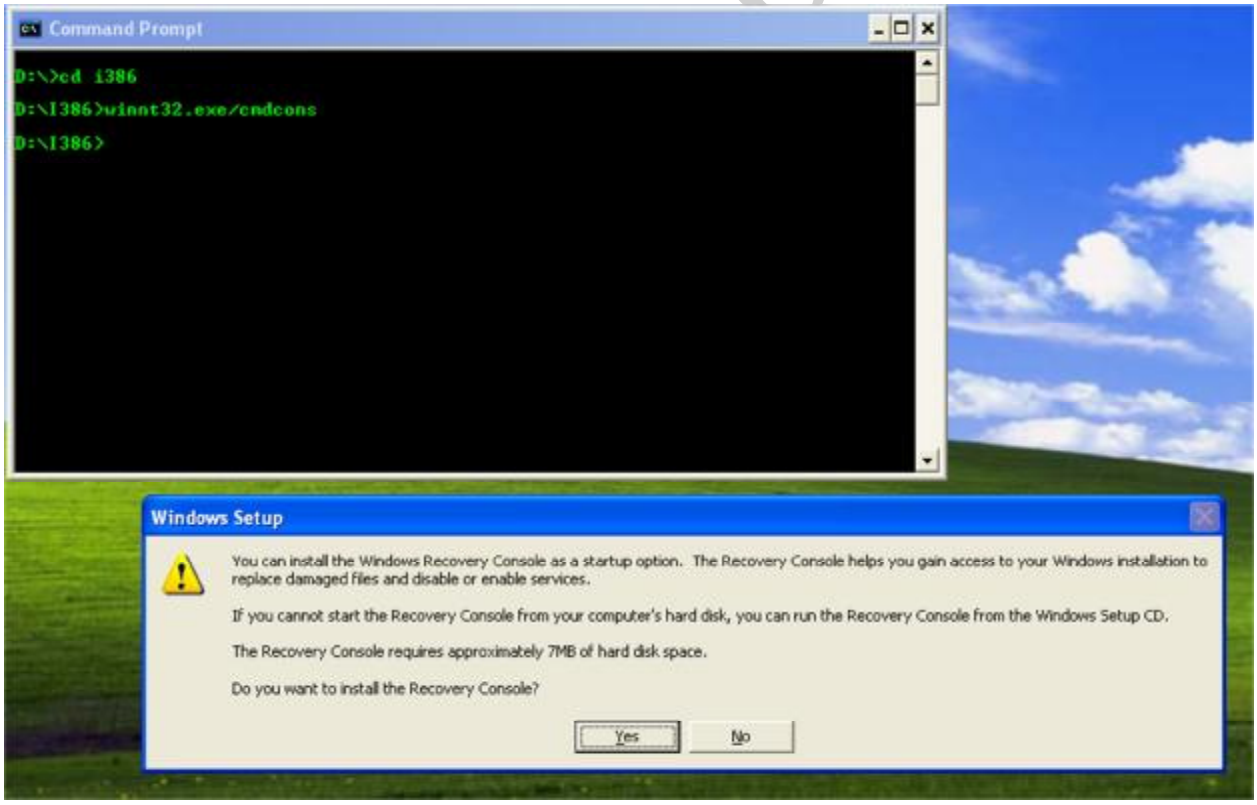
روش اول:

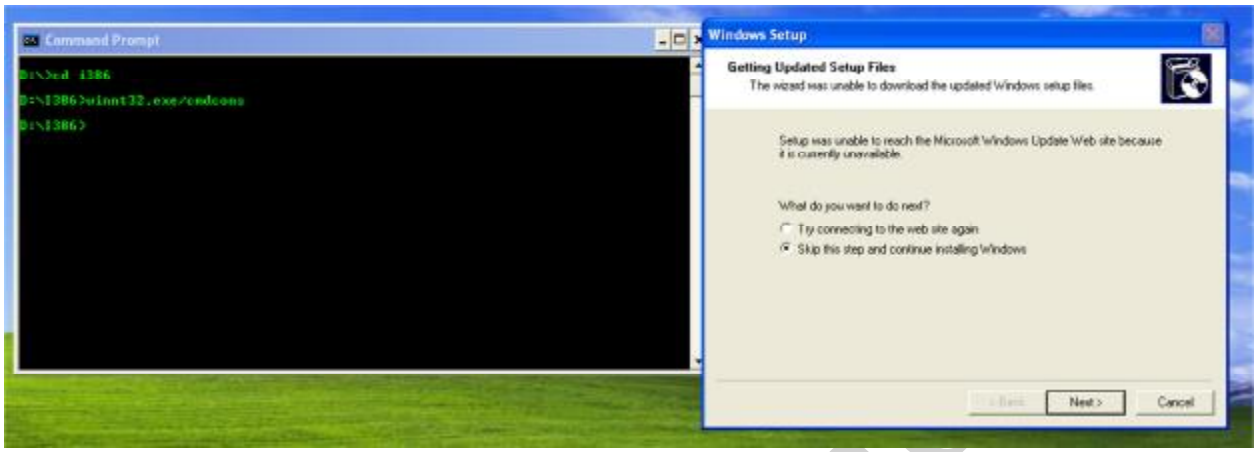
از محیط کامند وارد سی دی رام می شویم سپس دستور نصب ریکاوری کنسول را بصورت زیر وارد می کنیم،وارد i386 می شویم و دستور winnt32.exe/cmdcons را وارد کرده و کنسول شروع به نصب می شود.

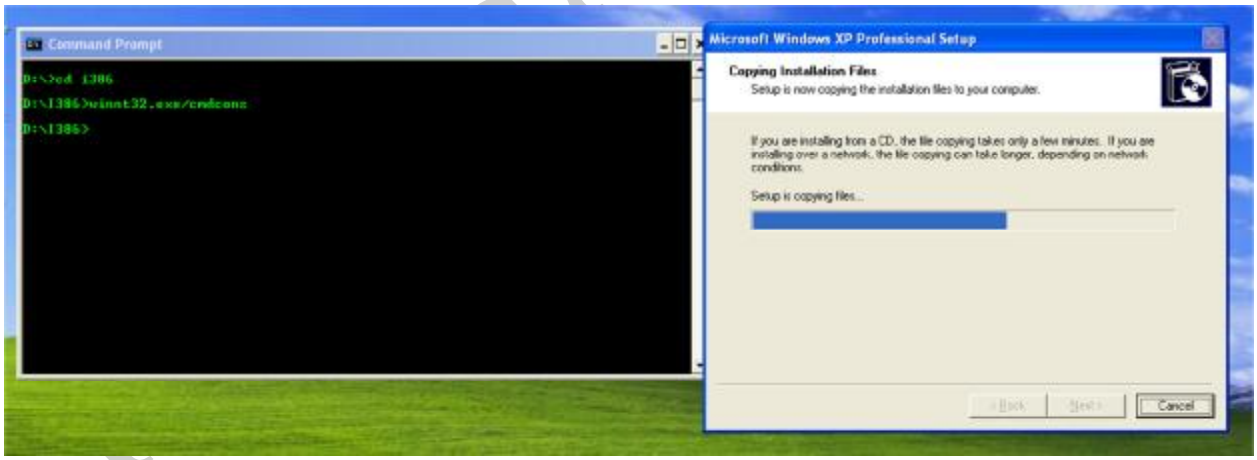



Fa noush

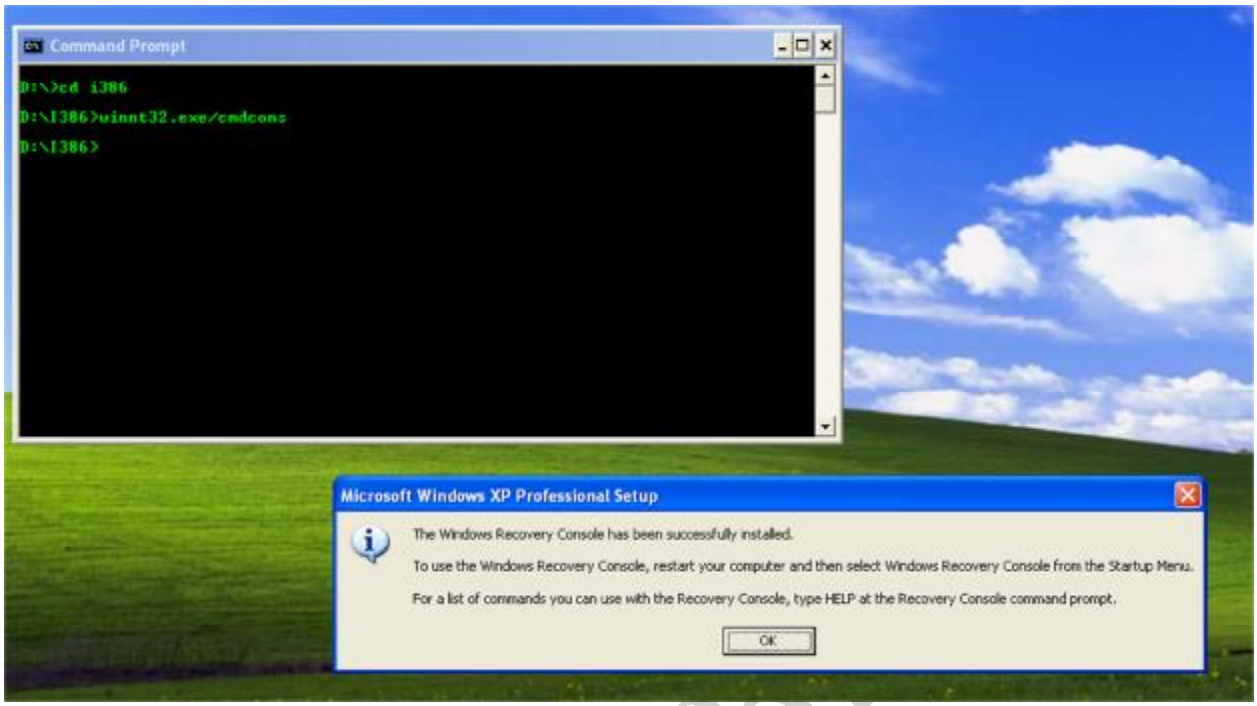

C:\WINDOWS\system32\cmd.exe
D:\>cd i386
D:\i386>winnt32.exe/cmdcons
D:\i386>


Command Prompt
D:\>cd i386
D:\I386>winnt32.exe/cmdcons
D:\I386>
Windows Setup
You can install the Windows Recovery Console as a startup option. The Recovery Console helps you gain access to your Windows installation to replace damaged files and disable or enable services.
If you cannot start the Recovery Console from your computer's hard disk, you can run the Recovery Console from the Windows Setup CD.
The Recovery Console requires approximately 7MB of hard disk space.
Do you want to install the Recovery Console?
Yes
No

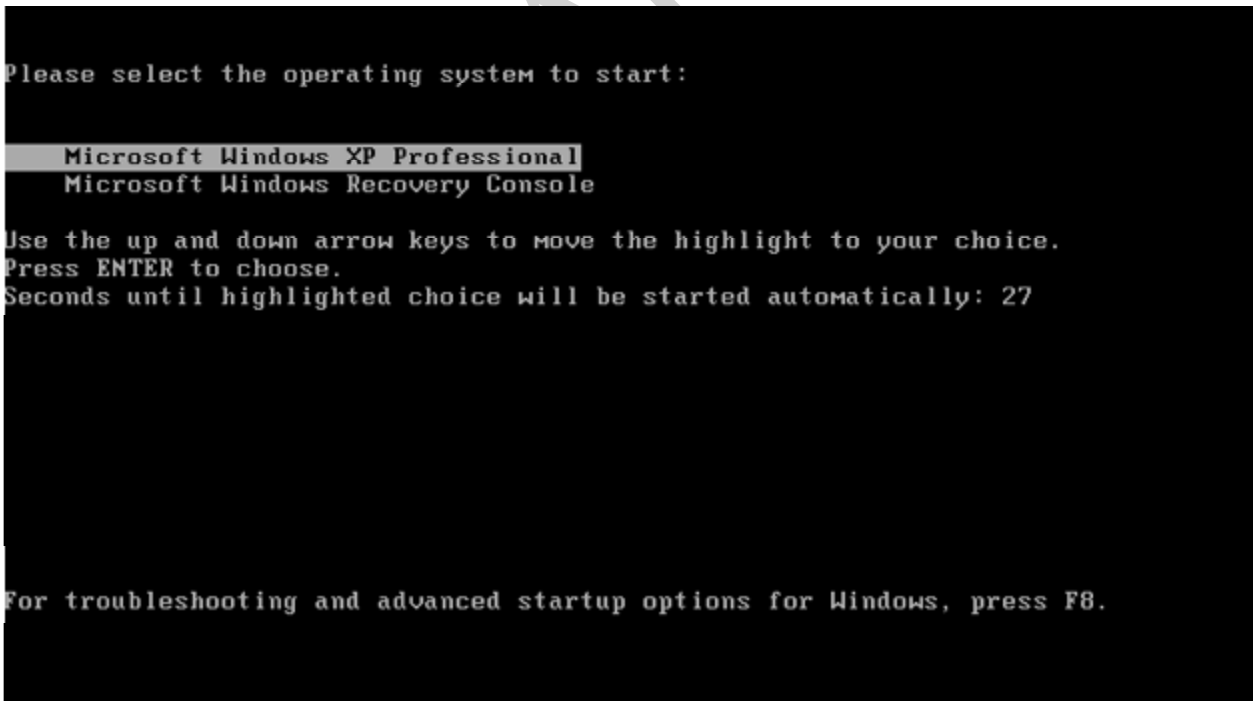

Command Prompt
D:\>cd i386
D:\I386>winnt32.exe/cmdcons
D:\I386>
Windows Setup
Getting Updated Setup Files
The wizard was unable to download the updated Windows setup files.
Setup was unable to reach the Microsoft Windows Update Web site because it is currently unavailable.
What do you want to do next?
Try connecting to the web site again
Skip this step and continue installing Windows
< Back
Next >
Cancel


Command Prompt
D:\>cd i386
D:\I386>winnt32.exe/cmdcons
D:\I386>
Microsoft Windows XP Professional Setup
Copying Installation Files
Setup is now copying the installation files to your computer.
If you are installing from a CD, the file copying takes only a few minutes. If you are installing over a network, the file copying can take longer, depending on network conditions.
Setup is copying files...
< Back
Next >
Cancel

Ajabnet




**بعد از اتمام نصب سیستم را که ریستارت کنیم گزینه ریکاوری کنسول به آن اضافه شده و هر وقت که ویندوز خراب شود وارد آن شده وبا تایپ دستورات فایل های خراب را ریکاور می کنیم.**



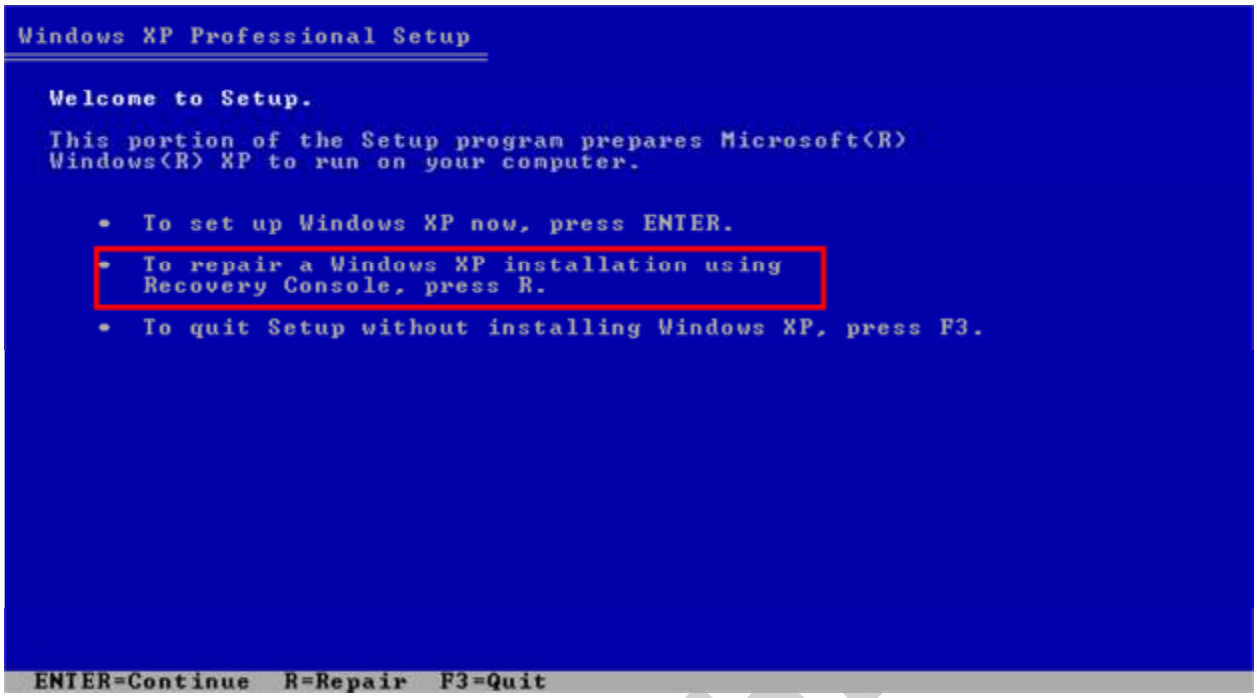
**روش دوم:**

**زمانی که ریکاوری کنسول نصب نباشد و ویندوز دچار مشکل شود از این روش استفاده میکنیم**

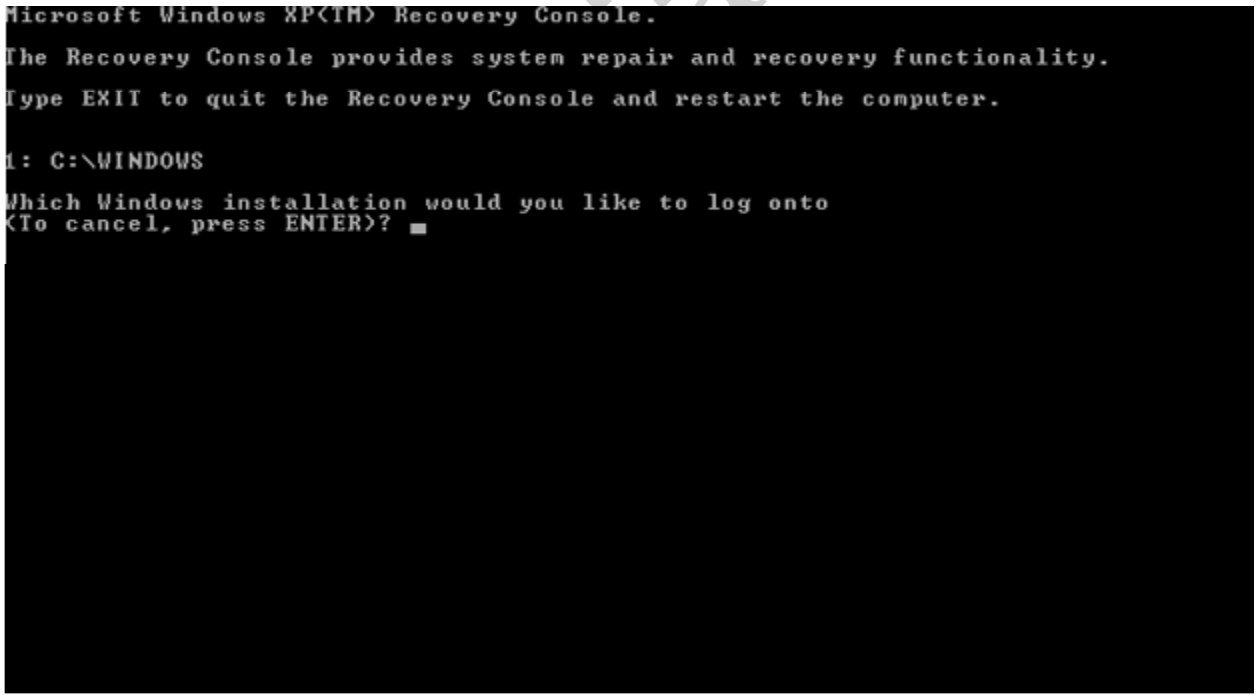
**در ابتدا باید توجه کنیم که ویندوز کدام یک از فایل های سیستمی را نمی تواند پیدا کند سپس به نصب مجدد آن بپردازیم.**

**در اینجا فایل NTDETECT.COM در ویندوز پاک شده است برای بازگردانی این فایل سی دی ویندوز را داخل سی دی رام قرار داده و سیستم را با سی دی بوت می کنیم سپس در صفحه نمایش داده شده برای ریکاوری ویندوز کلیدR را فشار می دهیم و بقیه مراحل به صورت زیر انجام می شود.**

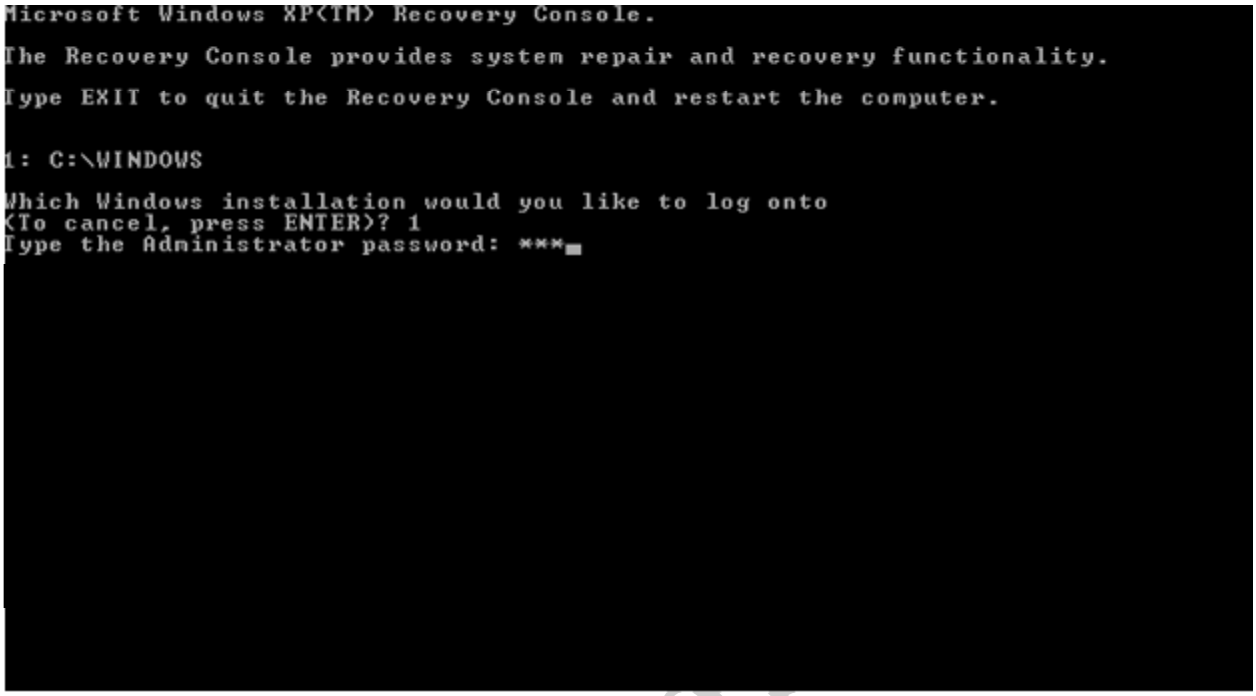
Farshid




در مرحله بعدی ویندوزهای موجود در سیستم را نمایش می دهد وباید ویندوز مورد نظر را باعدد انتخاب کنیم



در مرحله بعد پسورد Admin ویندوز را می پرسد



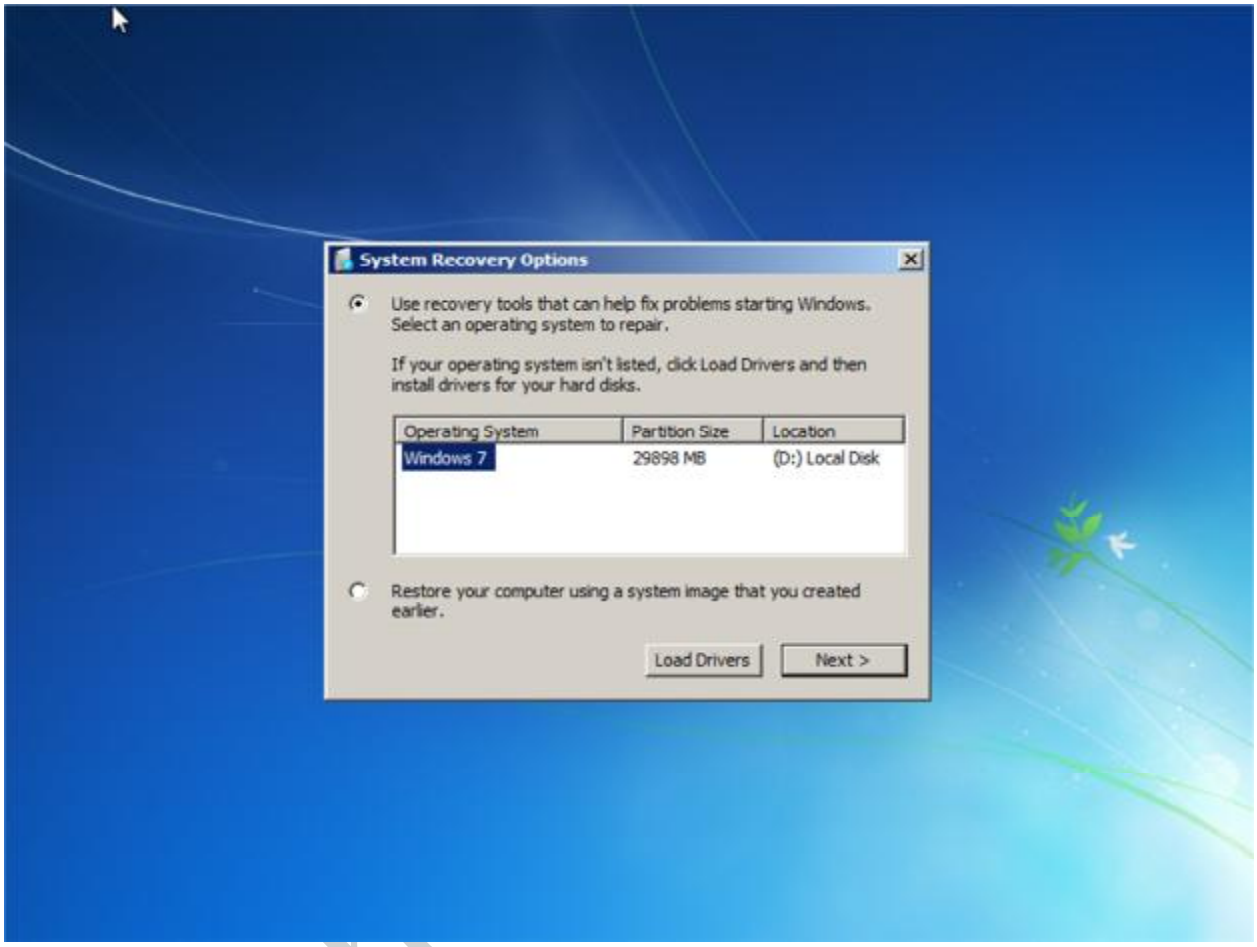

در مرحله آخر باید وارد درایو سی دی رام شویم و دستور کپی کردن فایل مورد نظر را وارد کنیم

وارد i386 می شویم و دستور را تایپ می کنیم i386>copy ntdetect.com c:\ با این دستور فایل مورد نظر از داخل سی دی در درایو C کپی می شود.

**ریکاوری در ویندوزهای NG :**

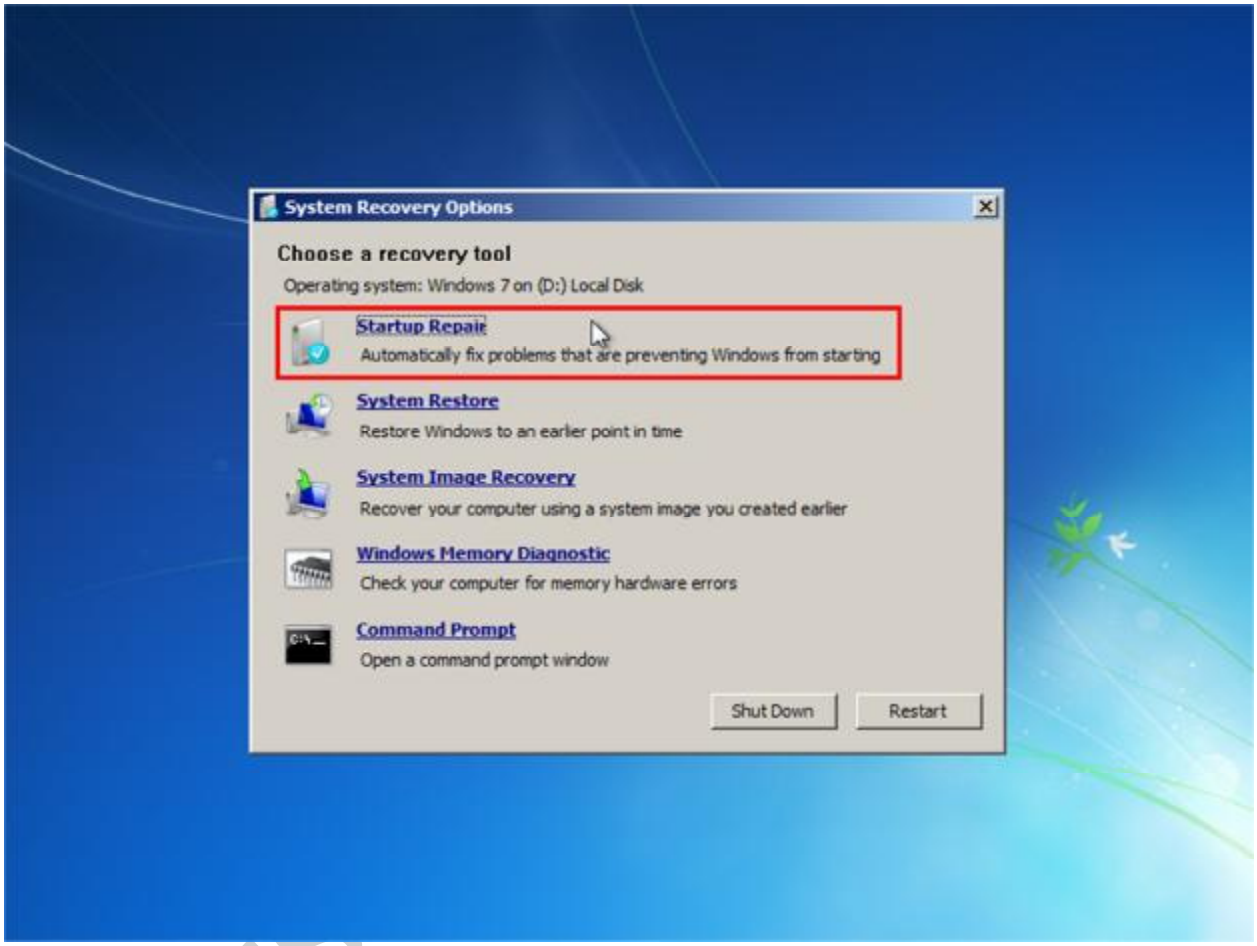
**در ابتدا با سی دی بوت می شویم، گزینه Repair Your Computer را انتخاب می کنیم**

در این مرحله ویندوزها را شناسایی می کند




Farsi

و در مرحله آخر StartUp Repair را می زنیم




Fars

سرور 2008 (70-647 )

تمامی نسخه های ویندوز سرور 2008 در 32 بیت و 64 بیت طراحی شده اند.

تفاوت بین 32 بیت و 64 بیت ویندوز سرور 2008 در ویژگی Hyper-V می باشد،که این ویژگی در 64 بیت می باشد.

Hyper-v : سرویسی برای مجازی سازی می باشد،مجازی سازی یعنی استفاده بهینه از سخت افزار های موجود.

نرم افزارهای مجازی سازی:

1) VMware esx (vsphere)
2) Hyper-v
3) Citrix
4) VMware

4-1 ) Workstation

4-2) Virtual pc

4-3)Virtual box

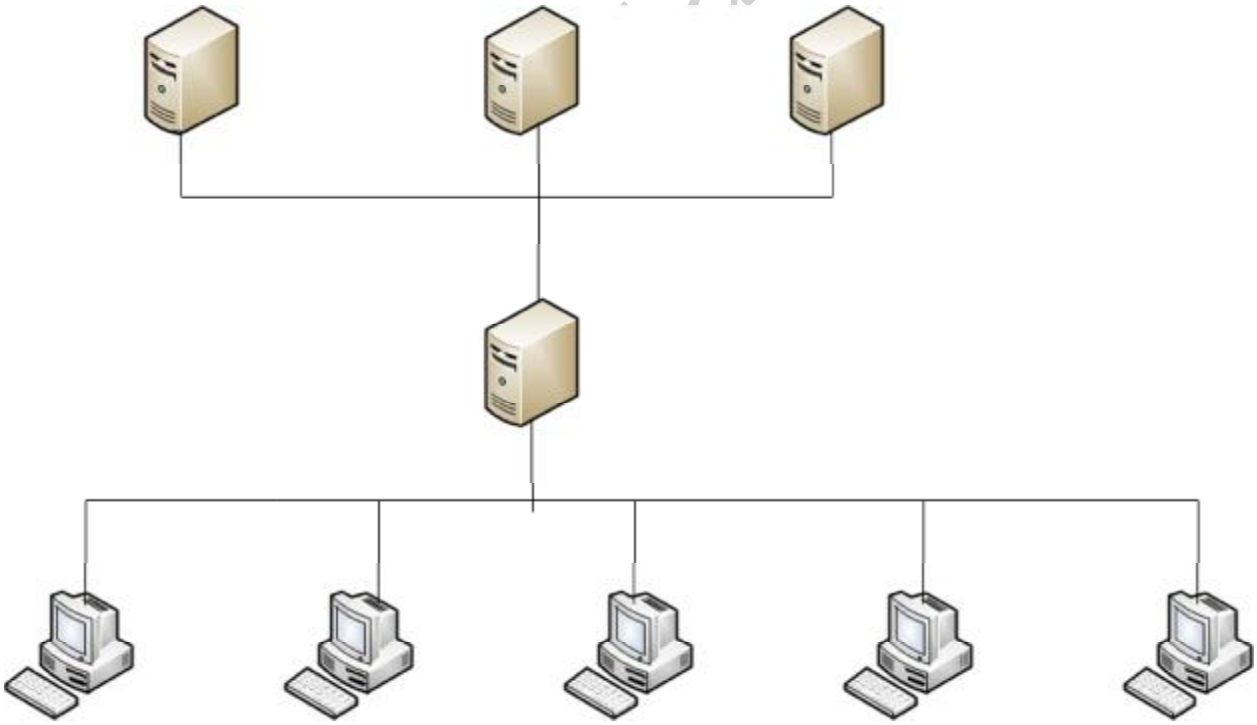
نرم افزار های مجازی سازی 3-1 Enterprise می باشند.

FarshidAjabnoush

نسخه های سرور2008

1) اولین نسخه سرور 2008 نسخهStandard می باشد این نسخه برای شبکه های کوچک و متوسط طراحی شده است و قابلیت راه اندازی یک Virtualizations را دارد.
2) دومین نسخه سرور 2008 نسخه Enterprise می باشد که برای شبکه های کاملاً بزرگ طراحی شده است این نسخه 2 مزیت مهم دارد،مزیت اول قابلیت پشتیبانی از4 Virtualizations را دارد و مزیت دوم قابلیت پشتیبانی از ویژگی Clustering را هم دارد.( Hot Add Memory )

- Clustering: فرض کنید 100000 نفر می خواهند به یک سرور وصل شوند این سرور قابلیت پشتیبانی از 100000 نفر را ندارد برای تقویت این سرور تعدادی سرور دیگر را به این سرور متصل می کنند تا توانایی پشتیبانی از10000 نفر را پیدا کند ولی آن 100000 نفر فقط به سرور اصلی اتصال پیدا می کنند وسرورهای کمکی را نمی بینند.



abroush

3) سومین نسخه سرور 2008 نسخه Data Center Editionمی باشد تمام ویژگی های نسخهEnterpriseرا دارا می باشد و خود دارای ویژگی هایی مانند Hot Add Processor ، پشتیبانی از نرم فزارهای بروز مانند SQL2010، EXCHANGE ، FOR FRONT به این ویژگی High End App Support گویند، ویژگی دیگر این نسخه Large Scale می باشد یعنی محدودیتی برای Virtualizations ندارد.

4) چهارمین نسخه سرور 2008 نسخه WEB EDITION می باشد این نسخه در مکانهایی استفاده می شود که از IIS7، NET FRAME WORK. و ASP.NET استفاده می کنند در کل این نسخه برای کار کردن تخصصی برنامه نویسی می باشد.

5) پنجمین نسخه سرور 2008 نسخه ITANIUM EDITION می باشد این نسخه مخصوص CPUهای ITANIUM طراحی شده توسط شرکت INTEL که 64 بیتی هستند می باشد،از این نوع CPU ها در جاهایی که احتیاج به پردازش بالا دارند استفاده می شود.

- بهترین نسخه ویندوز سرور2008 نسخه ENTERPRISE می باشد.
- تفاوت بین نسخه ENTERPRISE و STANDARD در ترمینال سرور ( CCU ) می باشد،در نسخه استاندارد ترمینال سرور برابر با 250 کامپیوتر می باشد ولی در نسخهENTERPRISE ترمینال سرور نا محدود می باشد.
- CUN CURRENT CONNECTION UNIT (CCU ): به تعداد کامپیوتری که سرور می تواند به آنها سرویس دهد را گویند.
- نسخ 5و4 را نمی توان در شبکه استفاده کرد (سرویس دهی خوبی ندارند)
- اگر CPU دارای ویژگی DEP باشد می توان روی آن سیستم نرم افزار شبیه ساز VMware را نصب کرد ولی اگر ویژگی VT را نداشته باشد نمی توان داخل VMware سیستم عامل 64 بیتی نصب کرد.

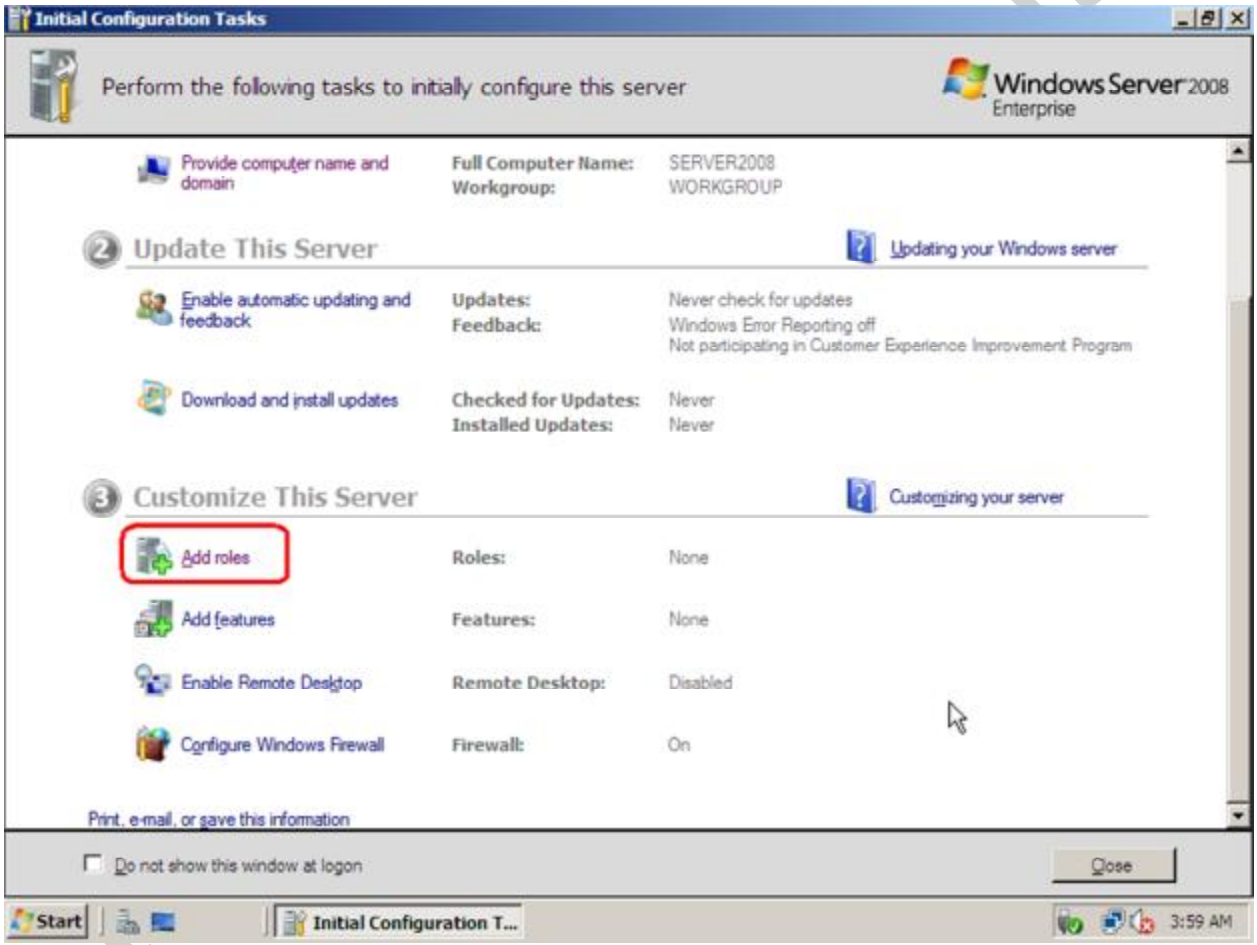
FarshidAjabnoush

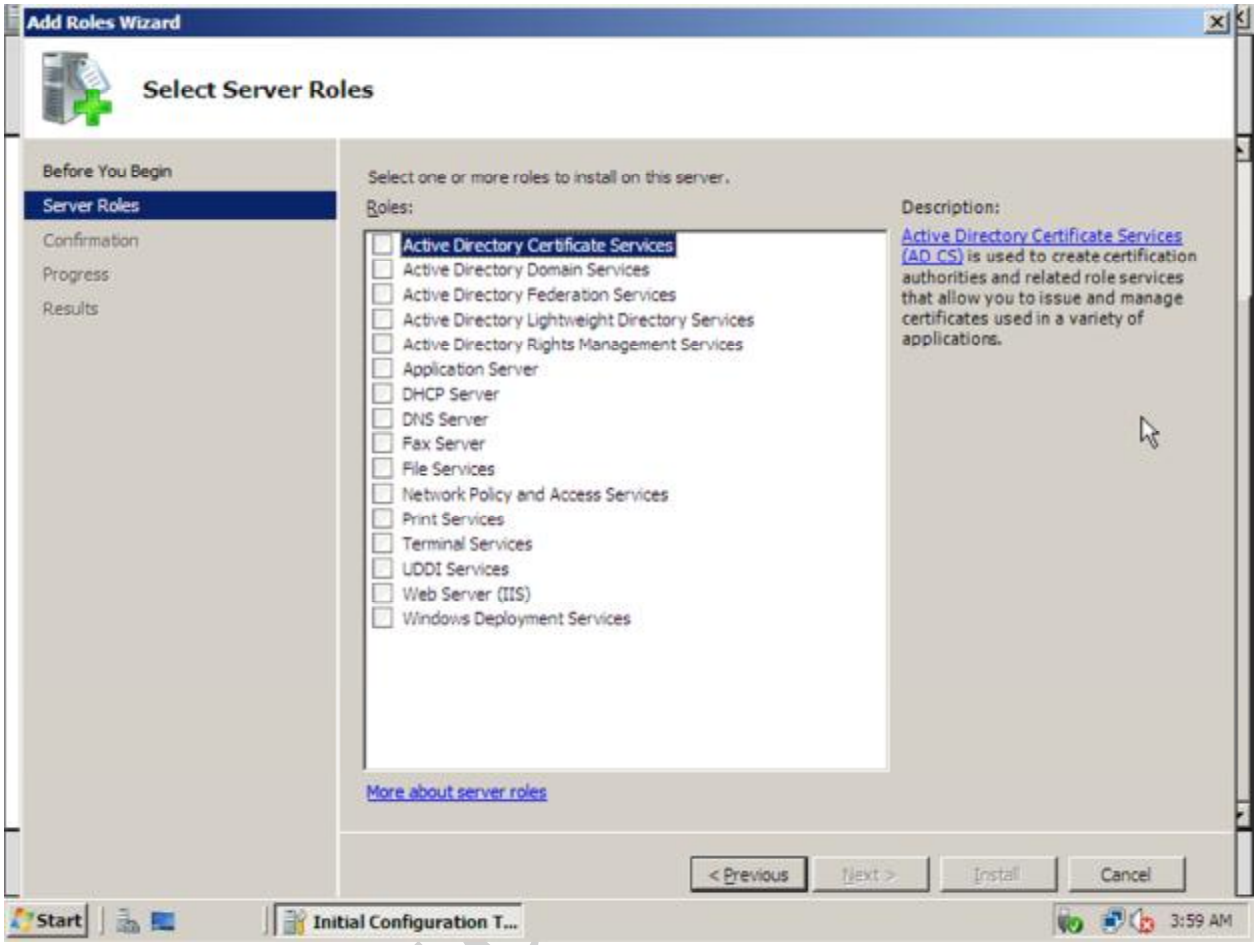
ویژگی که منابع شبکه را برای مدیریت متمرکز یکجا جمع می کند (DIRECTORY SERVICE (DS می باشد.

دایرکتوری سرویس مایکروسافت (ACTIVE DIRECTORY (AD می باشد،دایرکتوری سرویس لینوکس NIS,LDAP می باشد،دایرکتوری سرویس ناول NDS می باشد، بهترین و کاملترین دایرکتوری سرویس،AD می باشد.

- به سیستمی که روی آن AD باشد، DC ( Domain Controller) گویند.
- در سرور 2008 می توان یکی از 5رول اکتیو دایرکتوری را نصب کرد.

مسیر این رول ها را با هم می بینیم




Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
Confirmation
Progress
Results
Select one or more roles to install on this 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 Services
Network Policy and Access Services
Print Services
Terminal Services
UDDI Services
Web Server (IIS)
Windows Deployment Services
Description:
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
More about server roles
< Previous
Next >
Install
Cancel
Start
Initial Configuration T...
3:59 AM

Farshi

1) Active Directory Domain Services اگر روی سروری نصب باشد آن سرور DC می شود،برای نصب AD از دستور DCPROMO استفاده می کنیم.(2003-2008)

2) Active Directory Certificate Services اگر روی سیستمی نصب شود آن سیستم CA سرور می شود.(2003-2008)

- CA (Certificate Authority ) کار CA رمز کردن اطلاعات می باشد،تبدیل HTTP بهHTTPS.

3) Active Directory Light Weight Directory Services برای برنامه هایی استفاده می شوند که وب بیس (Web Base )مانند Exchange, Isa enterprise, Fore front اگر این سرویس نباشد Exchange فعال نمی شود. (2008 )

- در ویندوز2003 اگر خواستیم Exchange نصب کنیم باید AD یا ADAM قبل از آن نصب کنیم.
- سرویس های AD به 2 دسته تقسیم می شوند،دسته اول پروتکل Search (LDAP ) هستند و دسته دوم پروتکل احراز هویت Authentication (KERBEROS )

4) Active Directory Rights Management Services کار این سرویس کنترل اعمال صحیح Policy ها به شبکه است.(RMS ) (2008)

5) Active Directory Federation Services با نصب این سرویس می توان سرویس SSO را بر روی برنامه های تحت وب فعال کرد.(2008)

- SSO (Single-Sign-On ) با بیان یک مثال توضیح می دهیم وقتی داخل ایمیلمان هستیم به هر کجا از ایمیل که بخواهیم می رویم بدون اینکه هر دفعه از ما پسورد را بپرسد چون یکبار در هنگام وارد شدن پسورد را از ما پرسیده است و در خودش ذخیره کرده است ولی اگر از ایمیل بیرون برویم و دوباره بخواهیم وارد شویم از ما پسورد را می خواهد،یعنی تا زمانی که داخل ایمیل هستی پسورد اعتبار دارد وقتی از آن بیرون بیاییم دیگر اعتبار ندارد.

- سخت افزاری به نام NAC (Network Accesses Control ) کار RMS را انجام می دهد.

FarshidAjabnoush

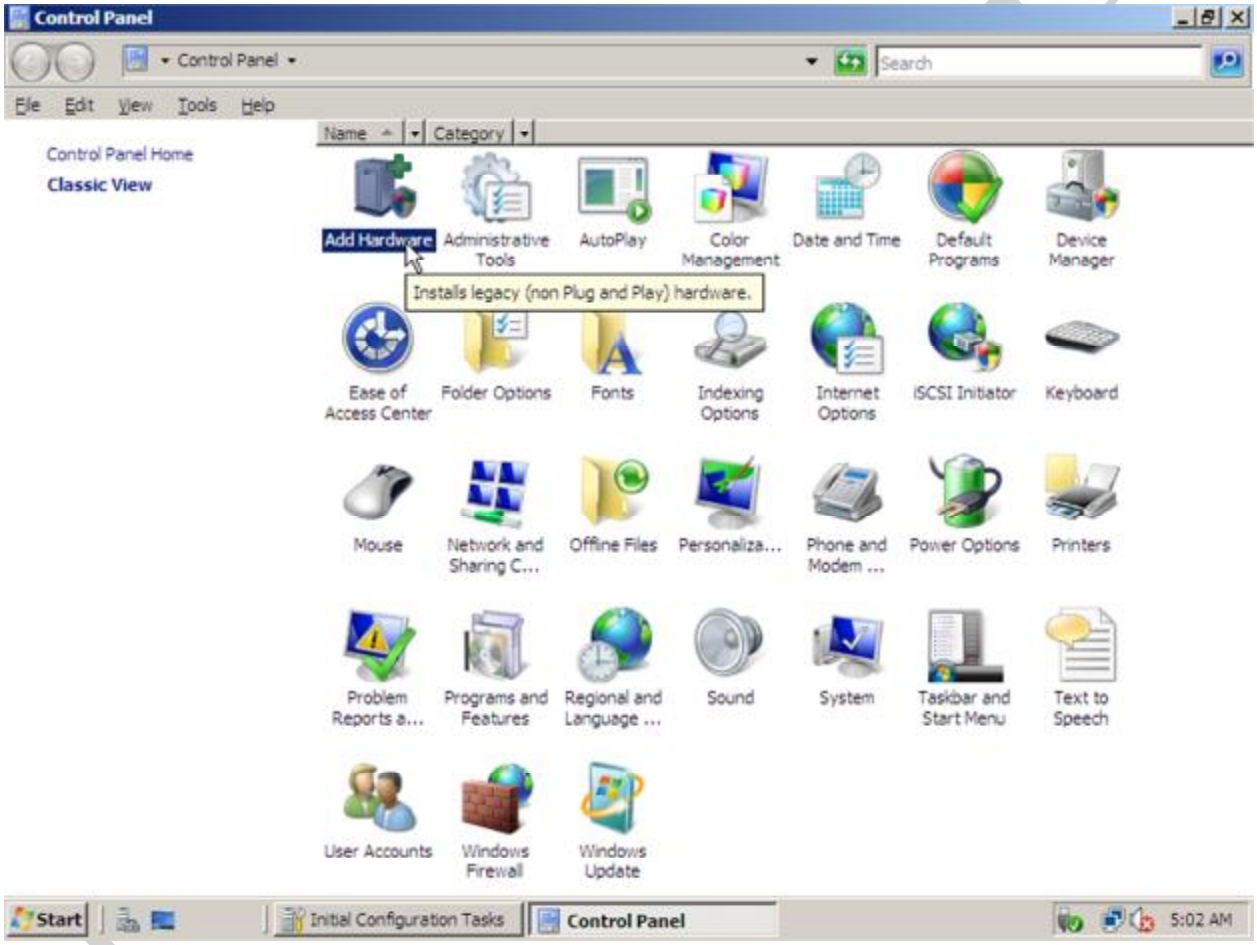
نصب Active Directory در ویندوز سرور2008

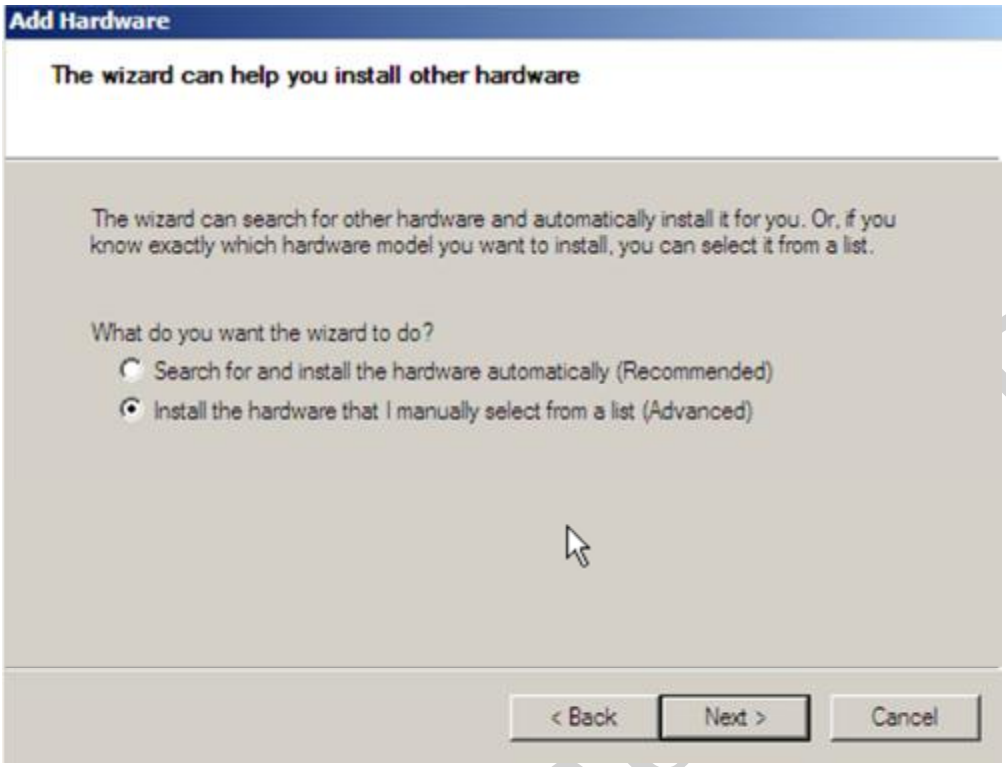
در ابتدا احتیاج به پیشنیاز های نصب داریم:

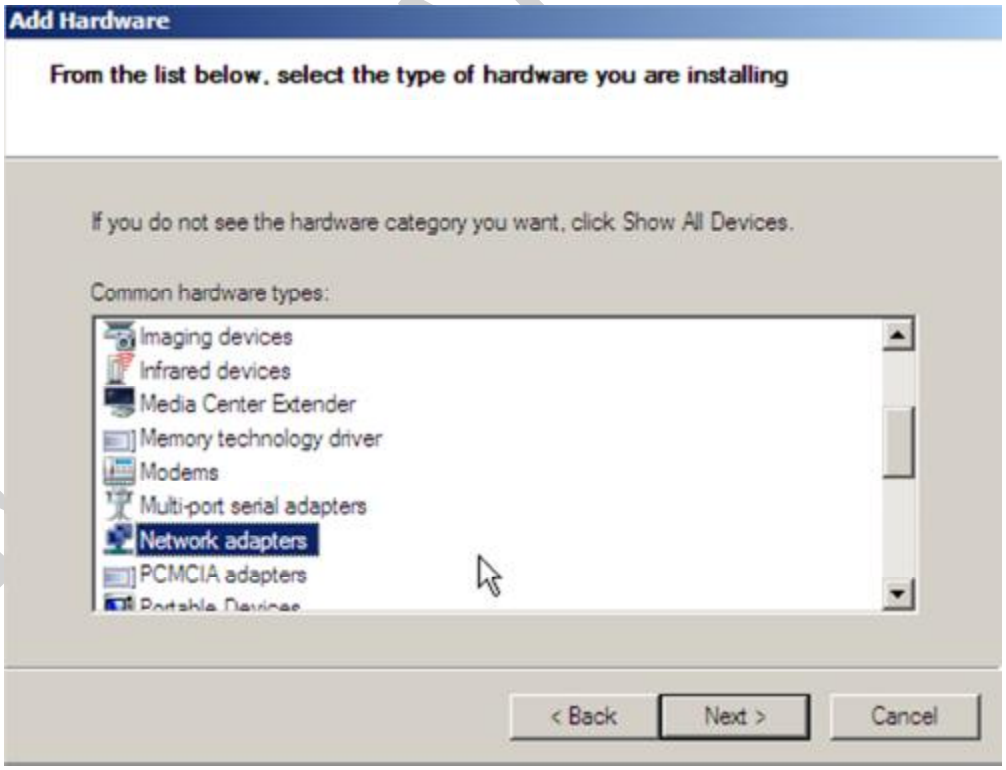
1) کارت شبکه : روی کامپیوتری که کارت شبکه نباشد AD نصب نمی شود برای جاهایی که بخواهیم کار تست پینگ انجام دهیم باید کارت شبکه Loop Back اضافه کنیم.

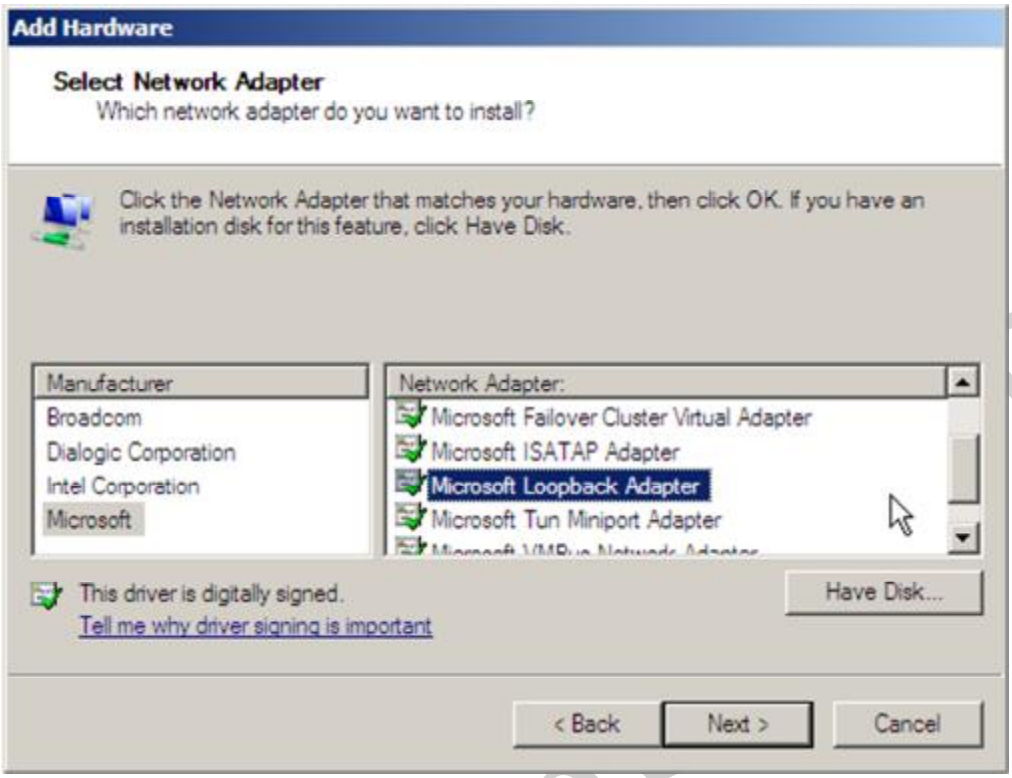
- برای ساختن کارت شبکه Loop Back مسیر زیر را طی می کنیم

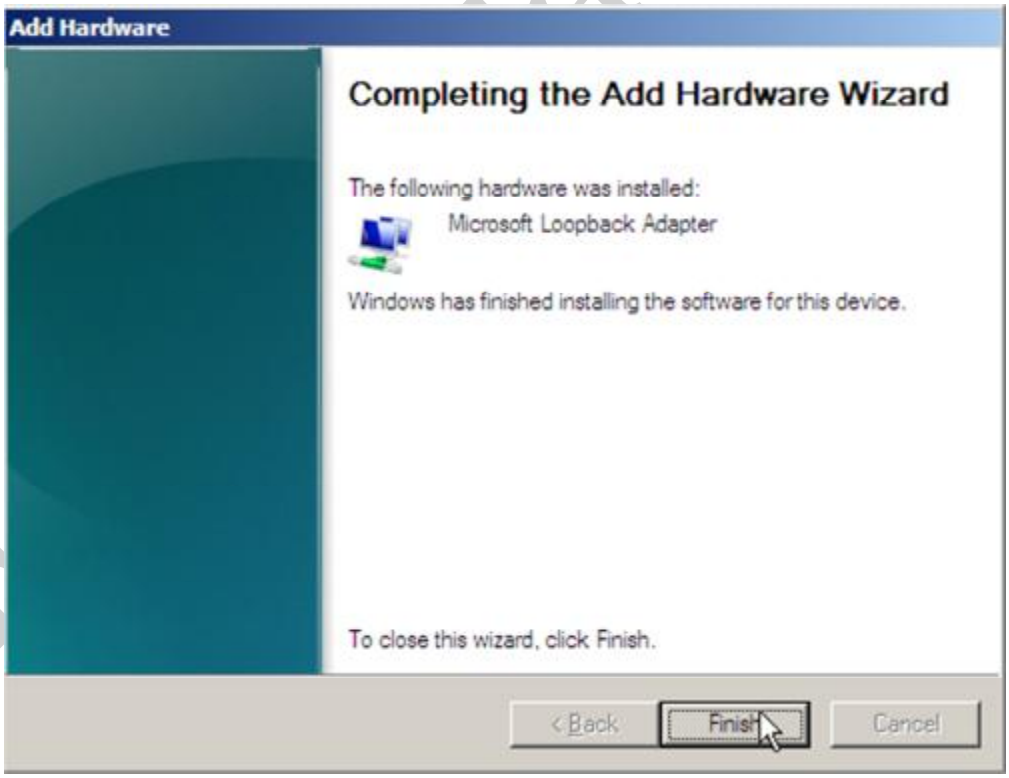
ابتدا به کنترل پنل رفته و وارد گزینه Add Hardware می شویم




Add Hardware
The wizard can help you install other hardware
The wizard can search for other hardware and automatically install it for you. Or, if you know exactly which hardware model you want to install, you can select it from a list.
What do you want the wizard to do?
Search for and install the hardware automatically (Recommended)
Install the hardware that I manually select from a list (Advanced)
< Back
Next >
Cancel

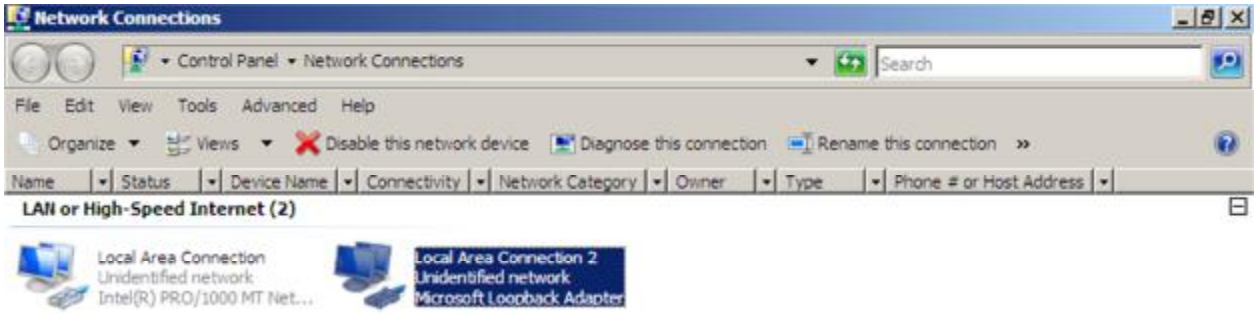

Add Hardware
From the list below, select the type of hardware you are installing
If you do not see the hardware category you want, click Show All Devices.
Common hardware types:
Imaging devices
Infrared devices
Media Center Extender
Memory technology driver
Modems
Multi-port serial adapters
Network adapters
PCMCIA adapters
< Back
Next >
Cancel






**همانطور که در شکل زیر میبینید کارت شبکه مورد نظر ساخته شد**



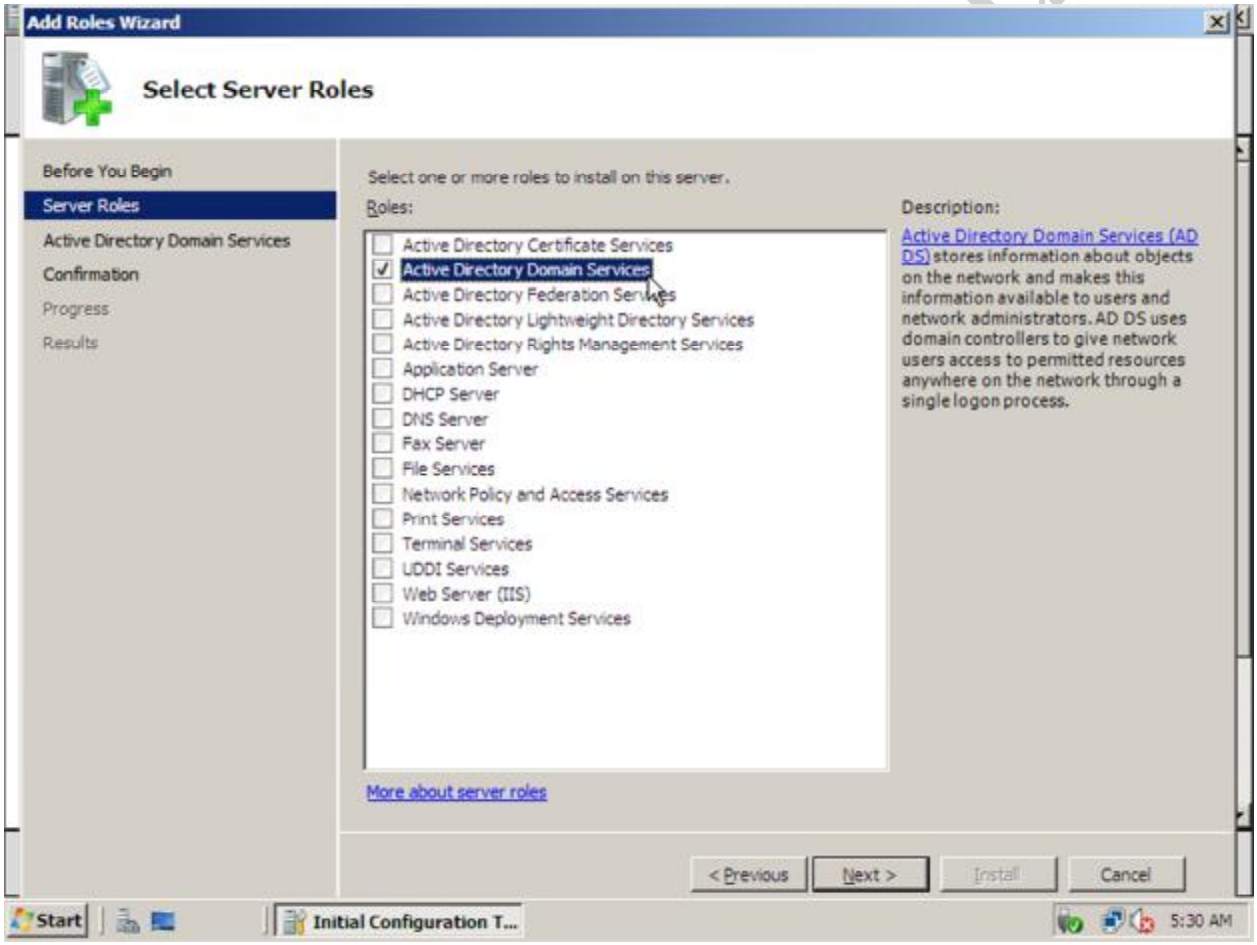
2) روی کارت شبکه باید IP تنظیم شده باشد.

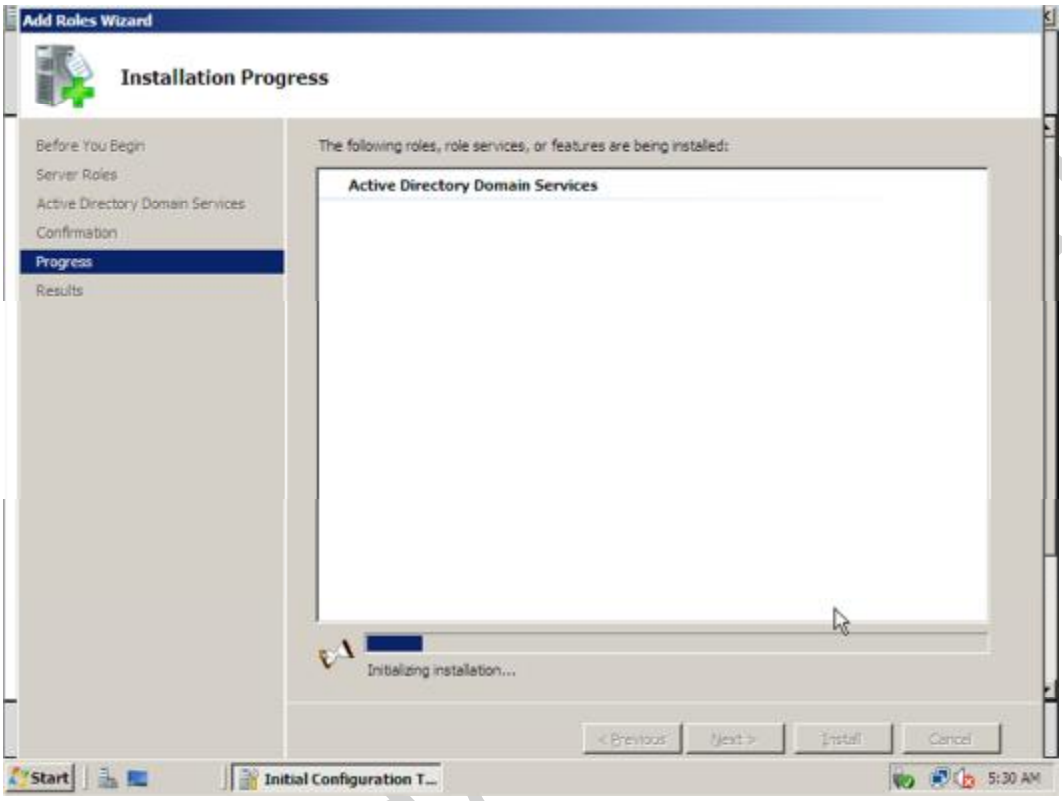
3) موقع نصب AD روی کارت شبکه نباید DNS تنظیم شده باشد،اگر DNS تنظیم باشد باید آن را برداشت و سپس حتماً باید پوشهDNS را از داخل System32 بصورت دستی پاک کنیم.

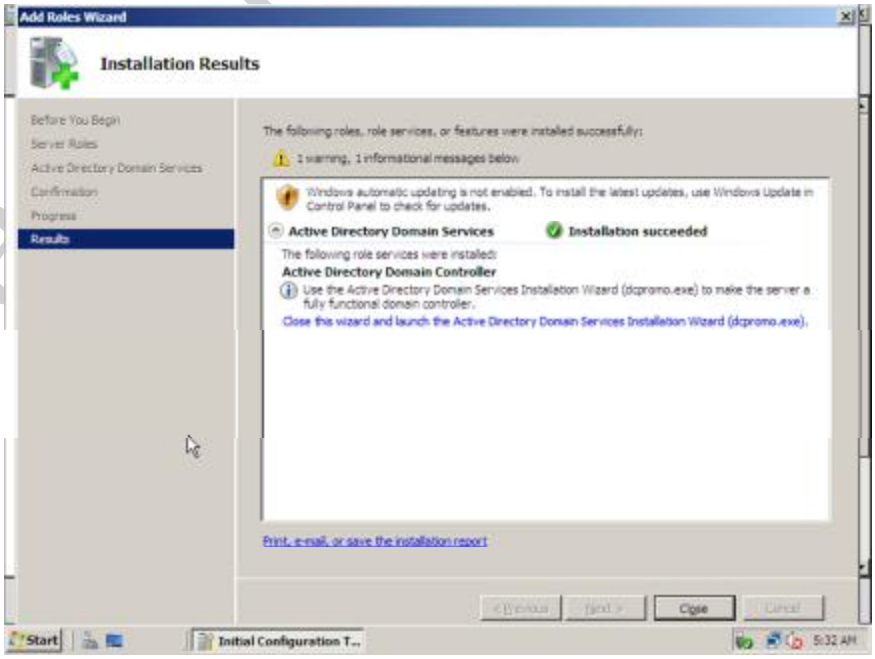
- روی سیستمی که سرویس DNS فعال است اکتیو نصب کنیم آن سیستم مکرراً Rejoin می شود.
- سرویس DNSهم نباید برروی سیتم باشد اگر بود باید Uninstall شود وپوشه DNS از System32 پاک شود.
- اگر بخواهیم لینوکس را به اکتیو Join کنیم باید بر روی آن پروتکل Samba نصب کنیم.
- Gateway زمانی تنظیم می شود که بخواهیم به یک رنج Ip متفاوت وصل شویم مثل اینترنت.

Farshid

نصب Active Directory




Add Roles Wizard
Installation Progress
Before You Begin
Server Roles
Active Directory Domain Services
Confirmation
Progress
Results
The following roles, role services, or features are being installed:
Active Directory Domain Services
Initializing installation...
< Previous
Next >
Install
Cancel
Start
Initial Configuration T...
5:30 AM


Add Roles Wizard
Installation Results
Before You Begin
Server Roles
Active Directory Domain Services
Confirmation
Progress
Results
The following roles, role services, or features were installed successfully:
1 warning, 1 informational messages below
Windows automatic updating is not enabled. To install the latest updates, use Windows Update in Control Panel to check for updates.
Active Directory Domain Services
Installation succeeded
The following role services were installed:
Active Directory Domain Controller
Use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.
Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).
Print, e-mail, or save the installation report
< Previous
Next >
Close
Cancel
Start
Initial Configuration T...
5:32 AM

Fa

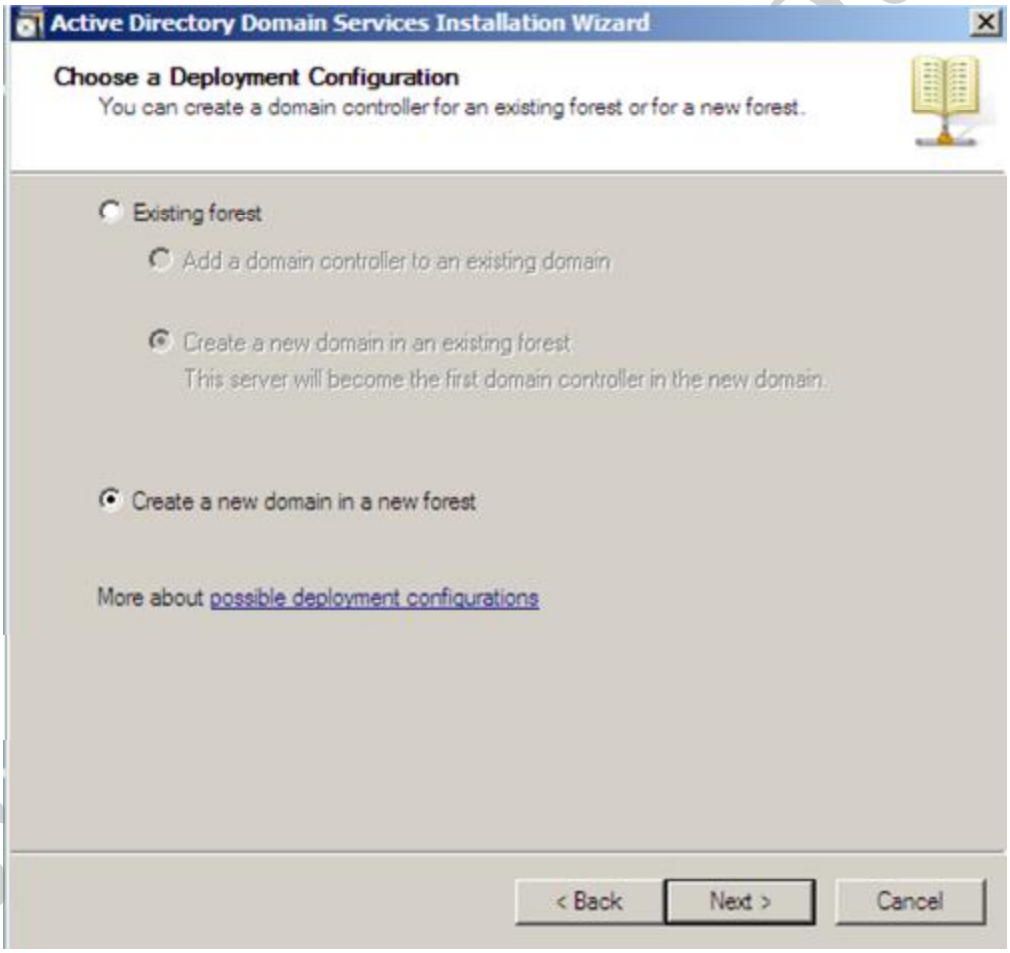
**بعد از انجام آخرین مرحله(شکل بالا) دستور DCPROMO را در RUN وارد می کنیم وپنجره زیر ظاهر می شود**

Farsi

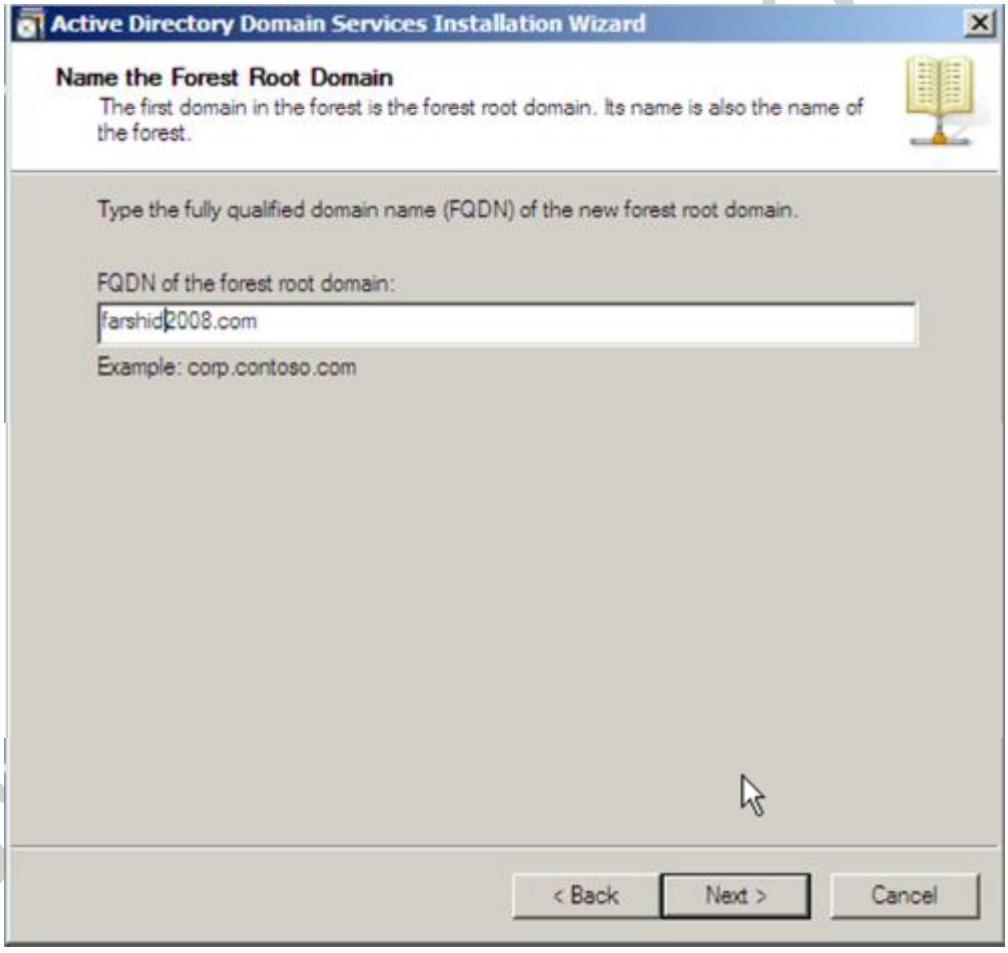
Add a domain controller to an existing domain: برای نصب اکتیو دایرکتوری بر روی سرور دوم مانندBDC می باشد.

Create a new domain in an existing forest : برای نصب اکتیو دایرکتوری بر روی Sub Domain می باشد.

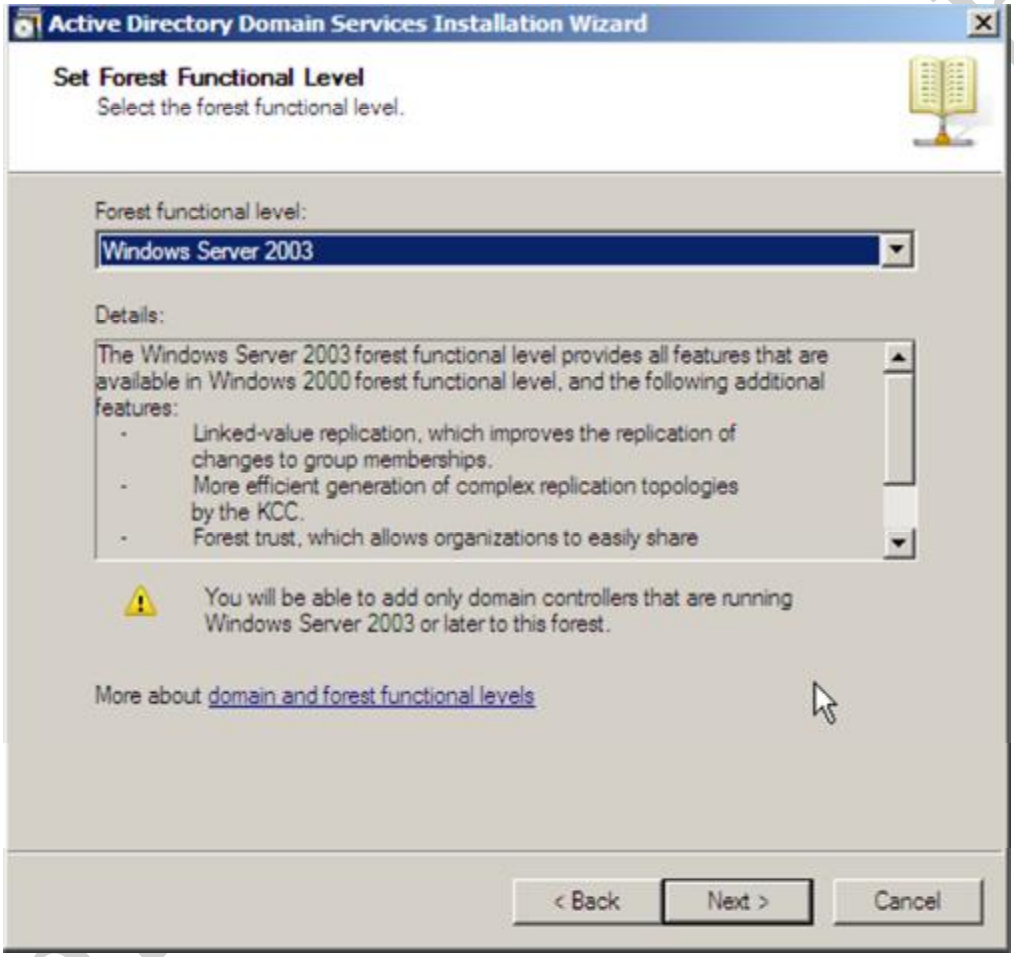
Create a new domain in a new forest : برای نصب اکتیو دایرکتوری بر روی اولین دامینمان می باشد.



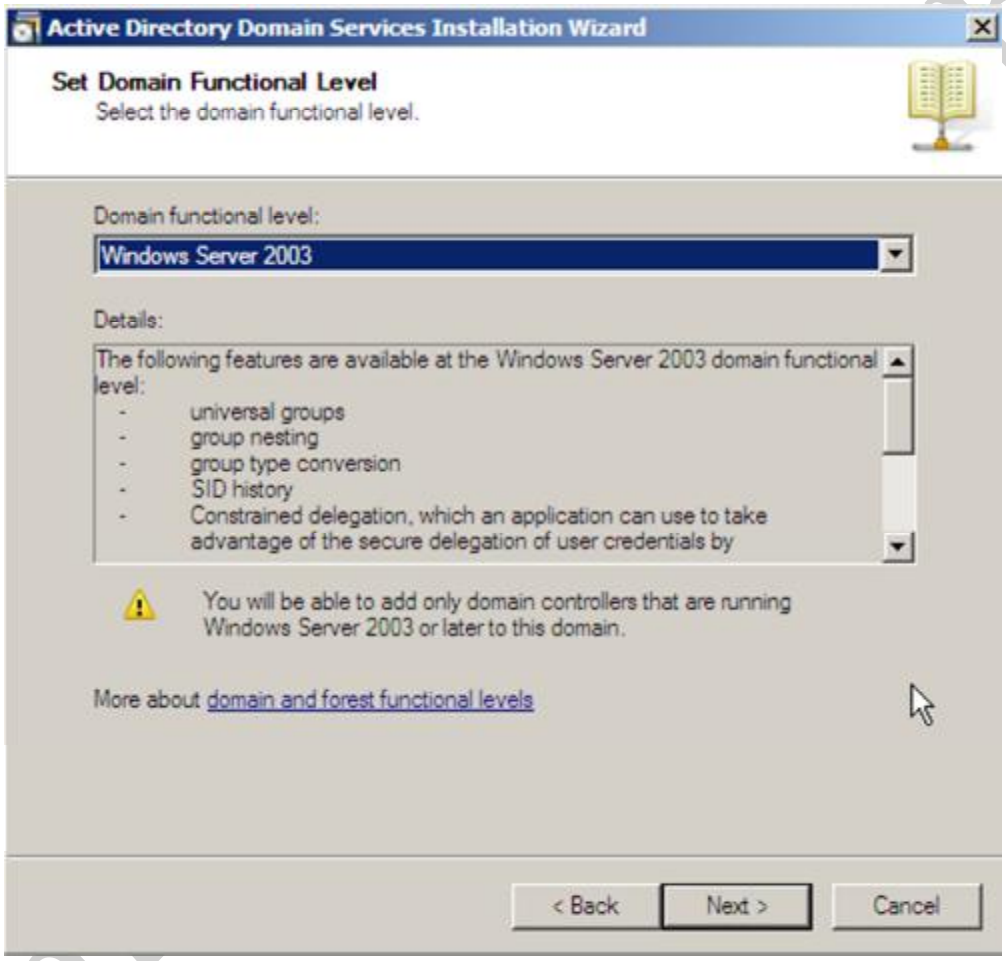
در اینجا اسم دامین را وارد می کنیم

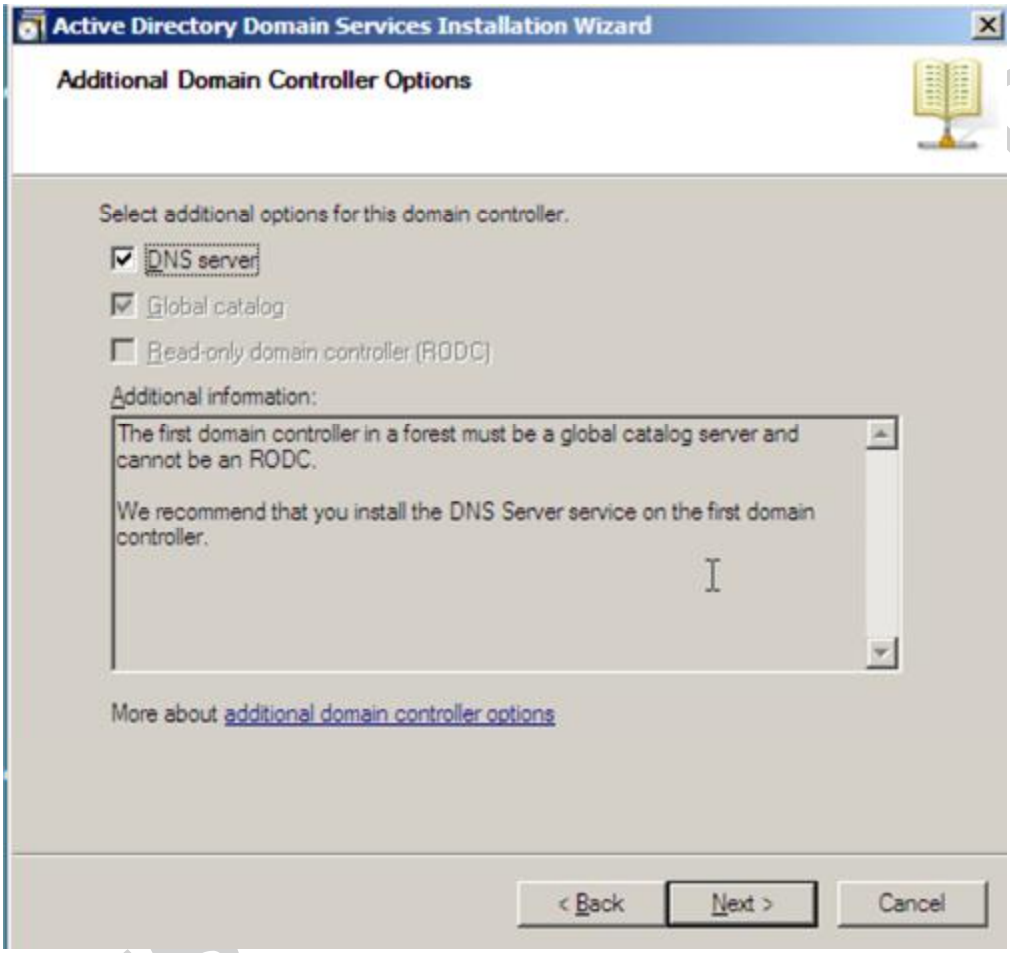


FFL را بر روی ویندوز2003 تنظیم می کنیم

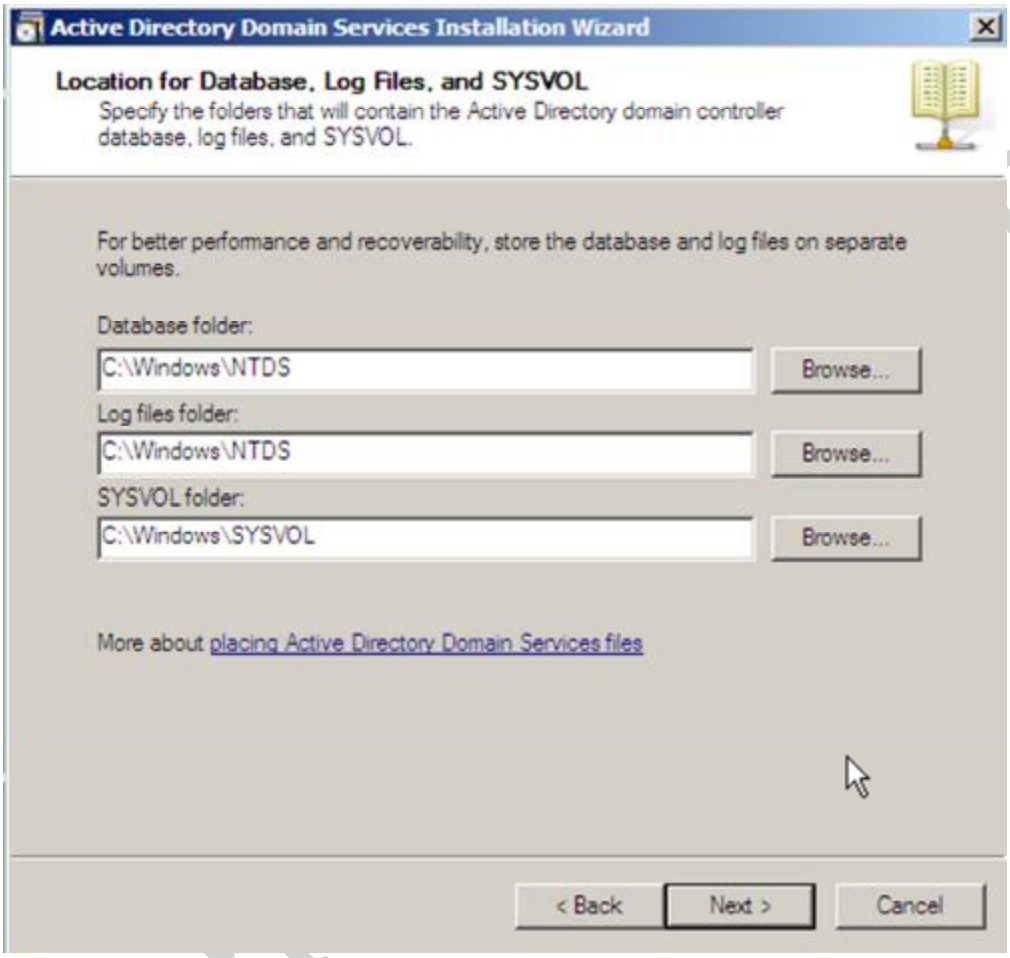


DFL را هم بر روی ویندوز2003 تنظیم می کنیم



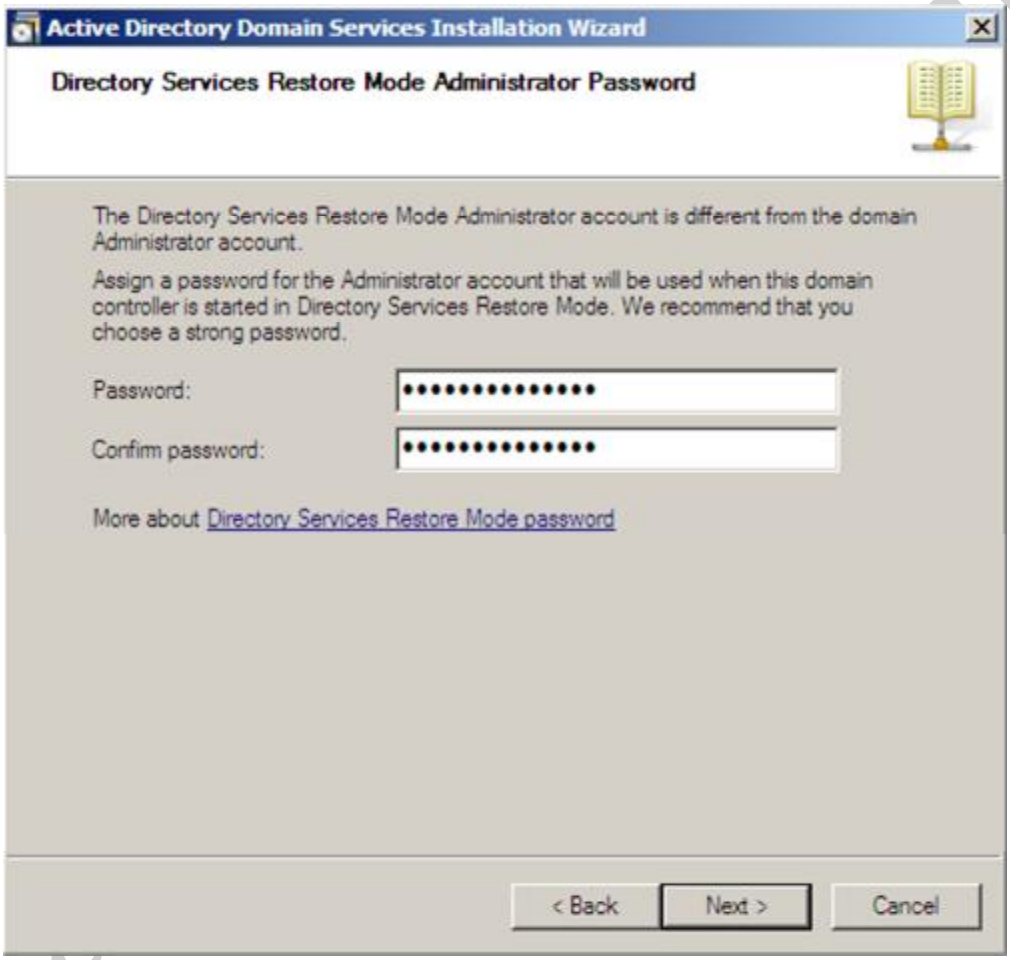

Active Directory Domain Services Installation Wizard
Additional Domain Controller Options
Select additional options for this domain controller.
DNS server
Global catalog
Read-only domain controller (RODC)
Additional information:
The first domain controller in a forest must be a global catalog server and cannot be an RODC.
We recommend that you install the DNS Server service on the first domain controller.
More about additional domain controller options
< Back
Next >
Cancel

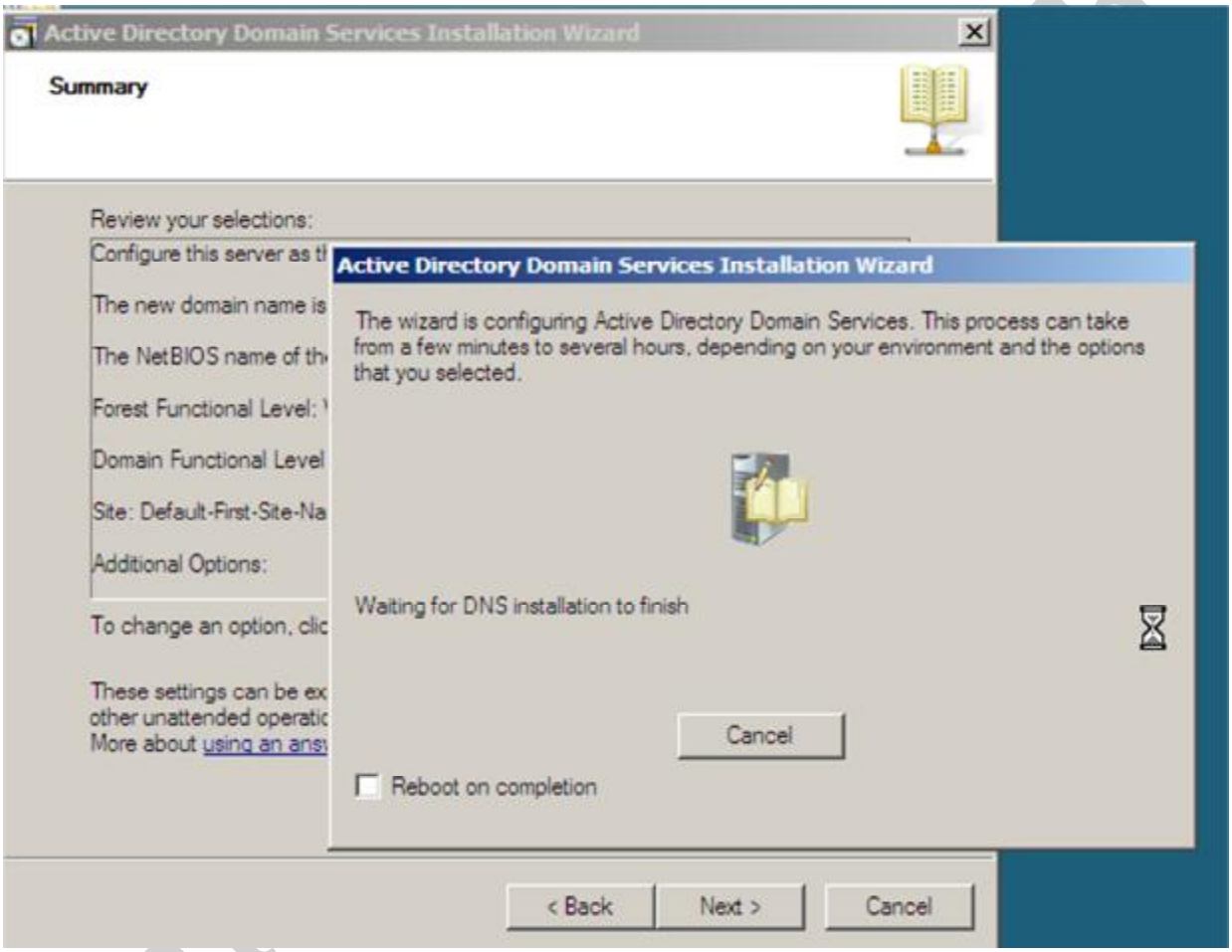
Fars


Active Directory Domain Services Installation Wizard
Location for Database, Log Files, and SYSVOL
Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.
For better performance and recoverability, store the database and log files on separate volumes.
Database folder:
C:\Windows\NTDS
Browse...
Log files folder:
C:\Windows\NTDS
Browse...
SYSVOL folder:
C:\Windows\SYSVOL
Browse...
More about placing Active Directory Domain Services files
< Back
Next >
Cancel

Farsi

در اینجا پسوردی از ما پرسیده می شود که پسورد ریکاوری اکتیو دایرکتوری می باشد در صورت خراب شدن اکتیو دایرکتوری با داشتن این پسورد می توانیم اکتیو را ریکاوری کنیم این پسورد با پسورد Admin تفاوت دارد.




Active Directory Domain Services Installation Wizard
Summary
Review your selections:
Configure this server as t
The new domain name is
The NetBIOS name of th
Forest Functional Level:
Domain Functional Level
Site: Default-First-Site-Na
Additional Options:
To change an option, clic
These settings can be ex
other unattended operatic
More about using an ans
Active Directory Domain Services Installation Wizard
The wizard is configuring Active Directory Domain Services. This process can take from a few minutes to several hours, depending on your environment and the options that you selected.
Waiting for DNS installation to finish
Cancel
Reboot on completion
< Back
Next >
Cancel

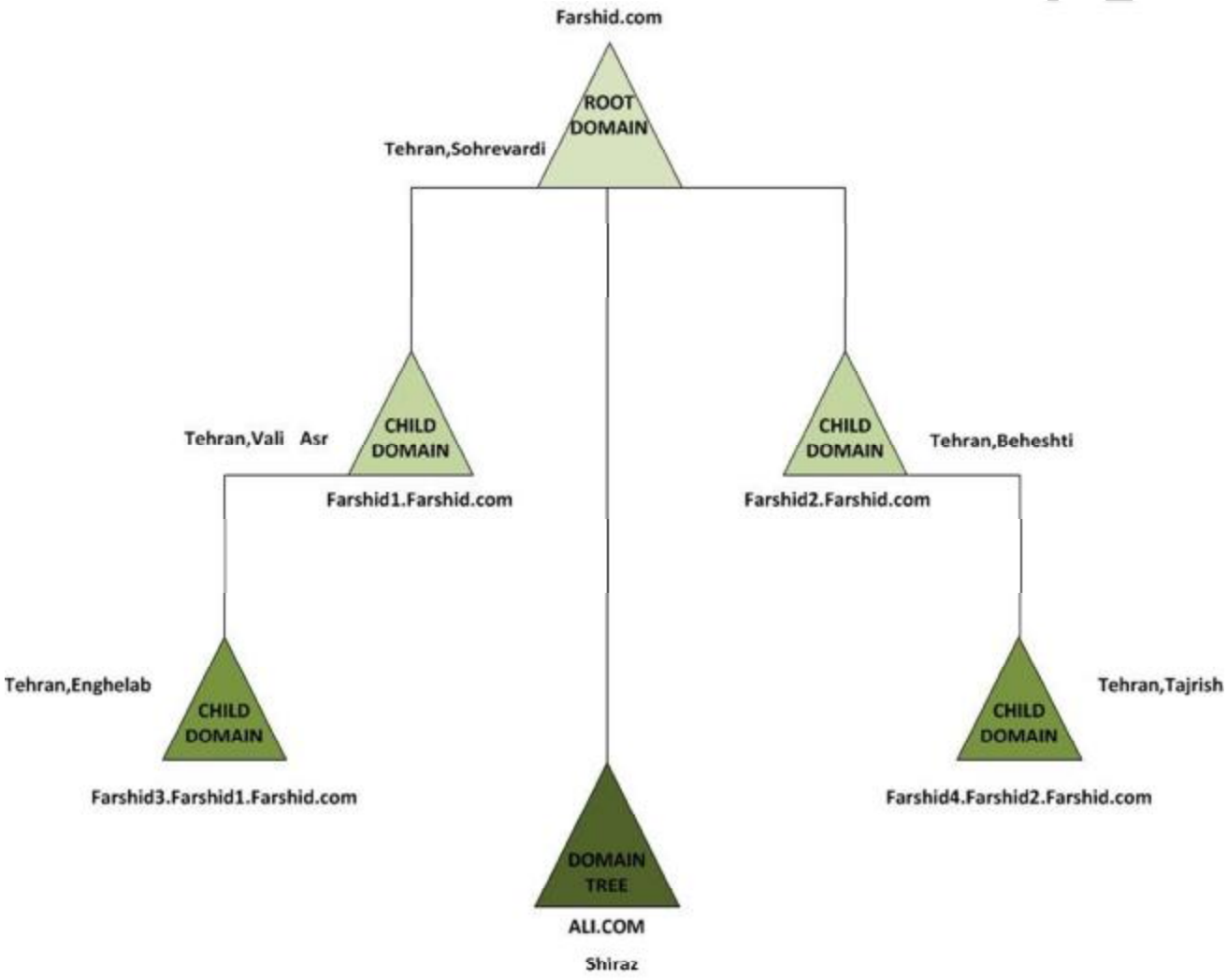
Active Directory Domain Services Installation Wizard
Completing the Active Directory Domain Services Installation Wizard
Active Directory Domain Services is now installed on this computer for the domain farshid2008.com.
This Active Directory domain controller is assigned to the site Default-First-Site-Name. You can manage sites with the Active Directory Sites and Services administrative tool.
To close this wizard, click Finish.
< Back
Finish
Cancel

Farshid

به اولین دامینی که داخل شبکه ای درست می کنیم ROOT DOMAIN می گوییم.

به دامینی که زیر مجموعه دامین اصلی می شود CHILD DOMAIN یا SUB DOMAIN گویند.

به دامینی که با دامین اصلی(Root Domain ) فاصله جغرافیایی (بین شهری) داشته باشد DOMAIN TREE گویند نام این دامین می تواند کاملاً مجزا از دامین اصلی باشد.




# FOREST

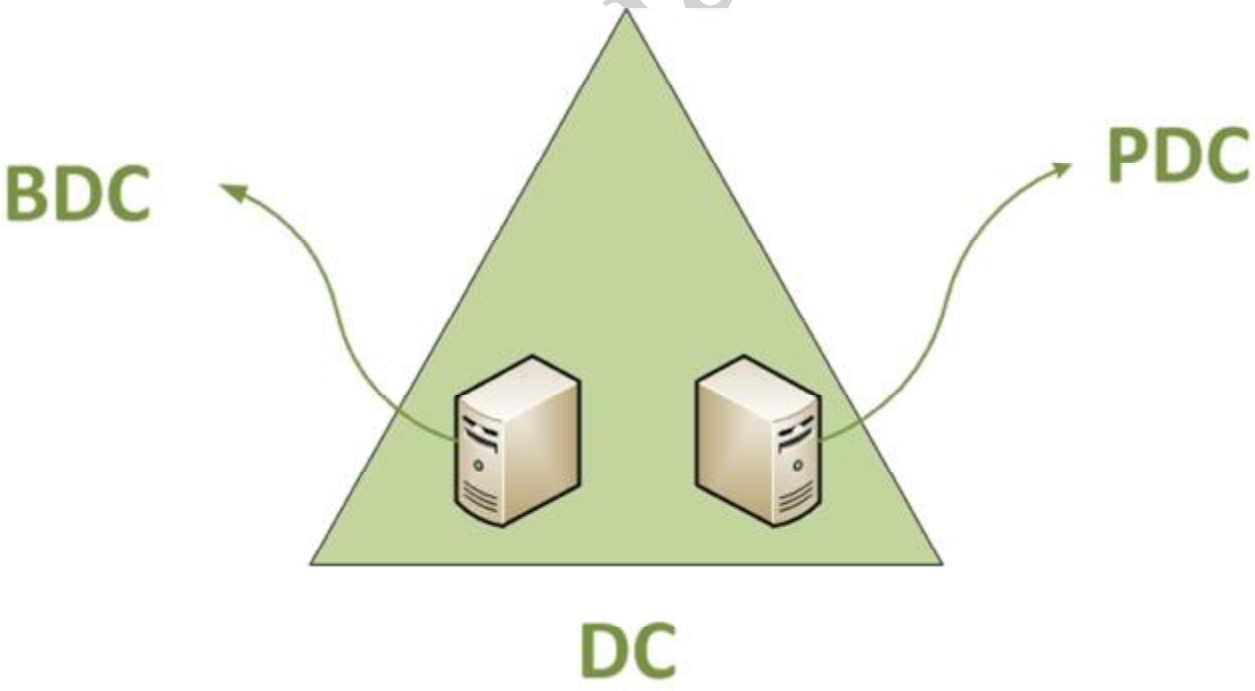
به کل این مجموعه Forest گویند هر فارست باید اسمی داشته باشد وآن اسم باید اسم Root Domain باشد.

آشنایی با اصطلاحات مهم:

1) Global Catalog (GC): آدرس تمامی یوزرهای شبکه داخلش هست, Rootdomain بصورت پیش فرض GC شبکه می باشد.
2) PDC,BDC

PDC (Primary Domain Controller ): به سروری که روی آن Active Directory نصب می شود PDC گویند.

BDC (Backup Domain Controller ):به سرور پشتیبان BDC، PDC گویند در یک دامین باید BDC باشد تا اگر PDC از کار افتاد BDC فعال شود. BDC=ADDITIONAL



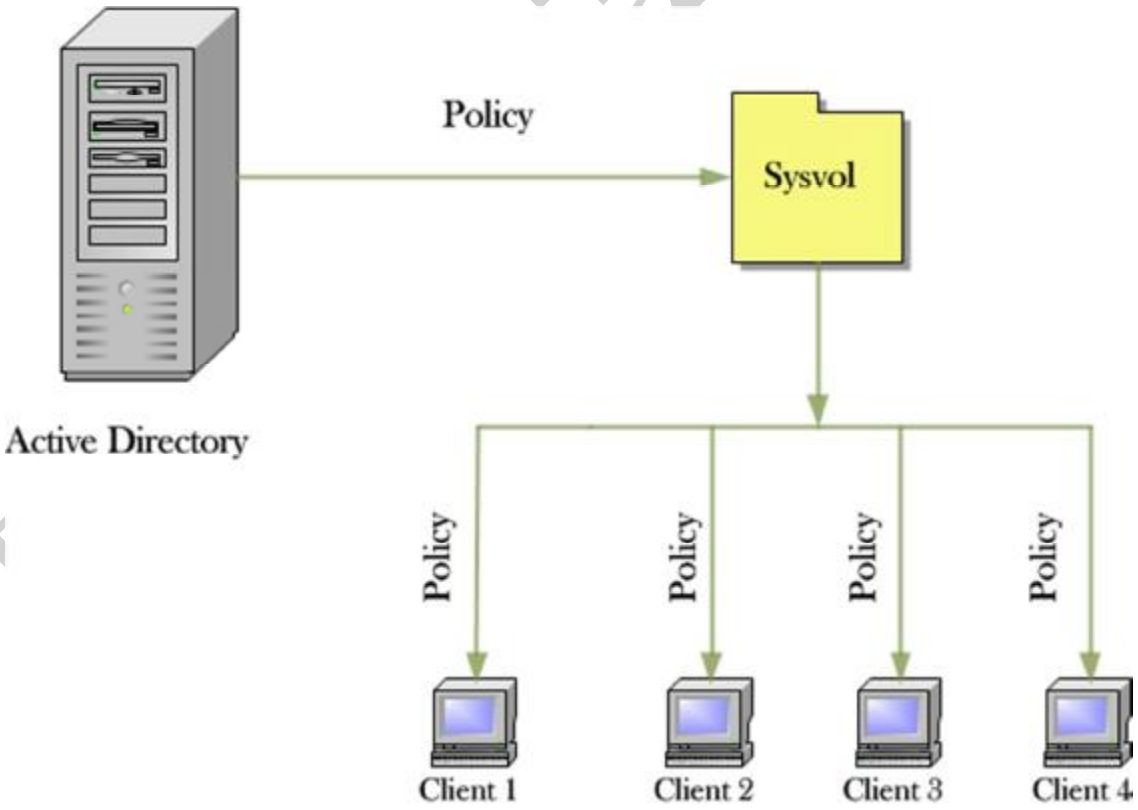

jabnoush

3) FFL (Forest Functional Level ) : مشخص می کند دامینی که بخواهد به عنوان Subدامینش باشد باید چه ویندوزی داشته باشد،اگرFFL 2003 باشد ویندوز Child دامینش باید 2003 یا بالاتر باشد.

4) DFL ( Domain Functional Level ): مشخص می کند سروری که بخواهد به عنوان BDC باشد چه نوع ویندوزی داشته باشد،اگرDFL 2003 باشد باید BDC هم2003 باشد.

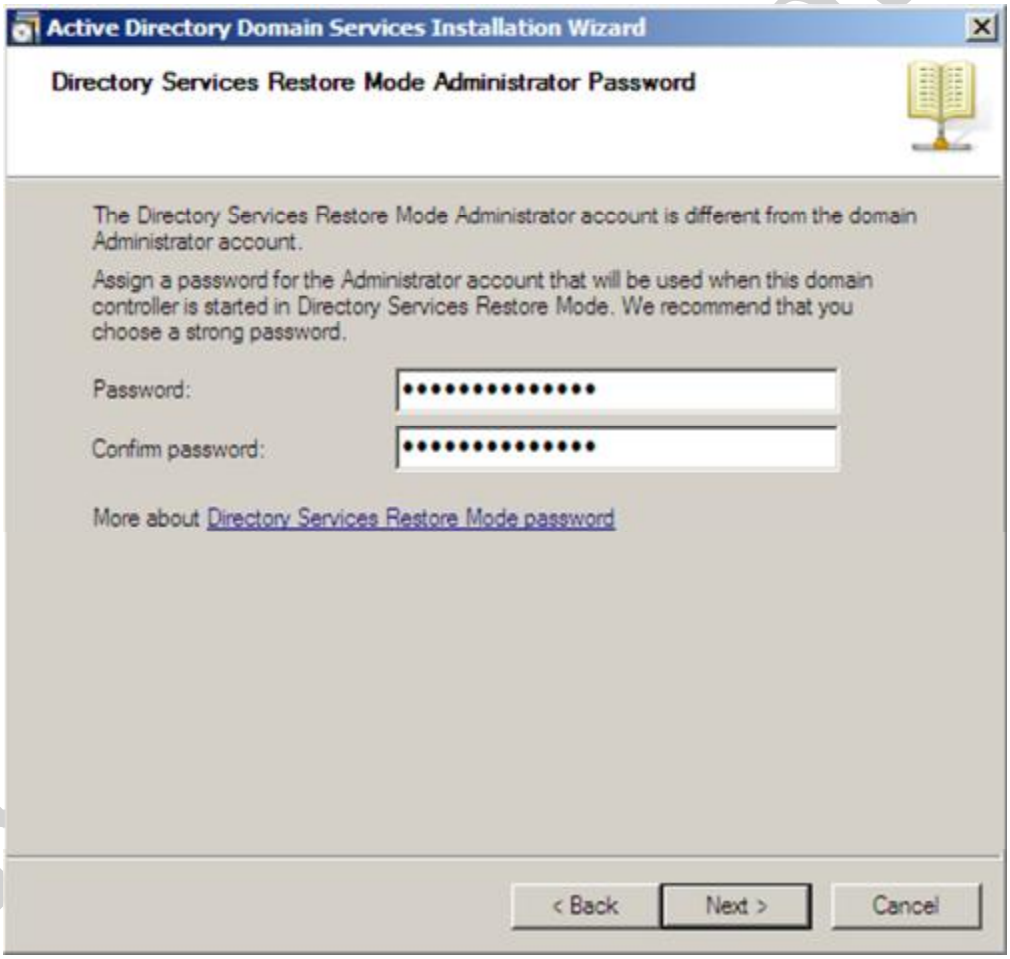
5) RODC (Read Only Domain Controller ): در ویندوز 2003 به این صورت بود که اگر یوزری(هر تغییر دیگری) را در PDC می ساختیم در BDC هم ساخته می شد و بر عکس ولی در ویندوز 2008 قابلیتی به نام RODC را بر روی BDC گذاشته اند که این قالبیت باعث می شود مستقیماً نتوانیم تغییری بر روی BDC انجام دهیم، هر تغییری که میخواهیم اعمال کنیم باید بر روی PDC انجام شود تا بر روی BDC هم انجام شود .(در اصل BDC فقط خواندنی شده استRead Only )

6) پوشه SYSVOL : تمام Policy هایی که در شبکه اعمال می شوند در این پوشه ذخیره می شوند،Client ها زمانی که بخواهند به شبکه متصل شوند باید ابتدا به سراغ این پوشه بروند تا دستورات جدید را دریافت و اعمال کنند.

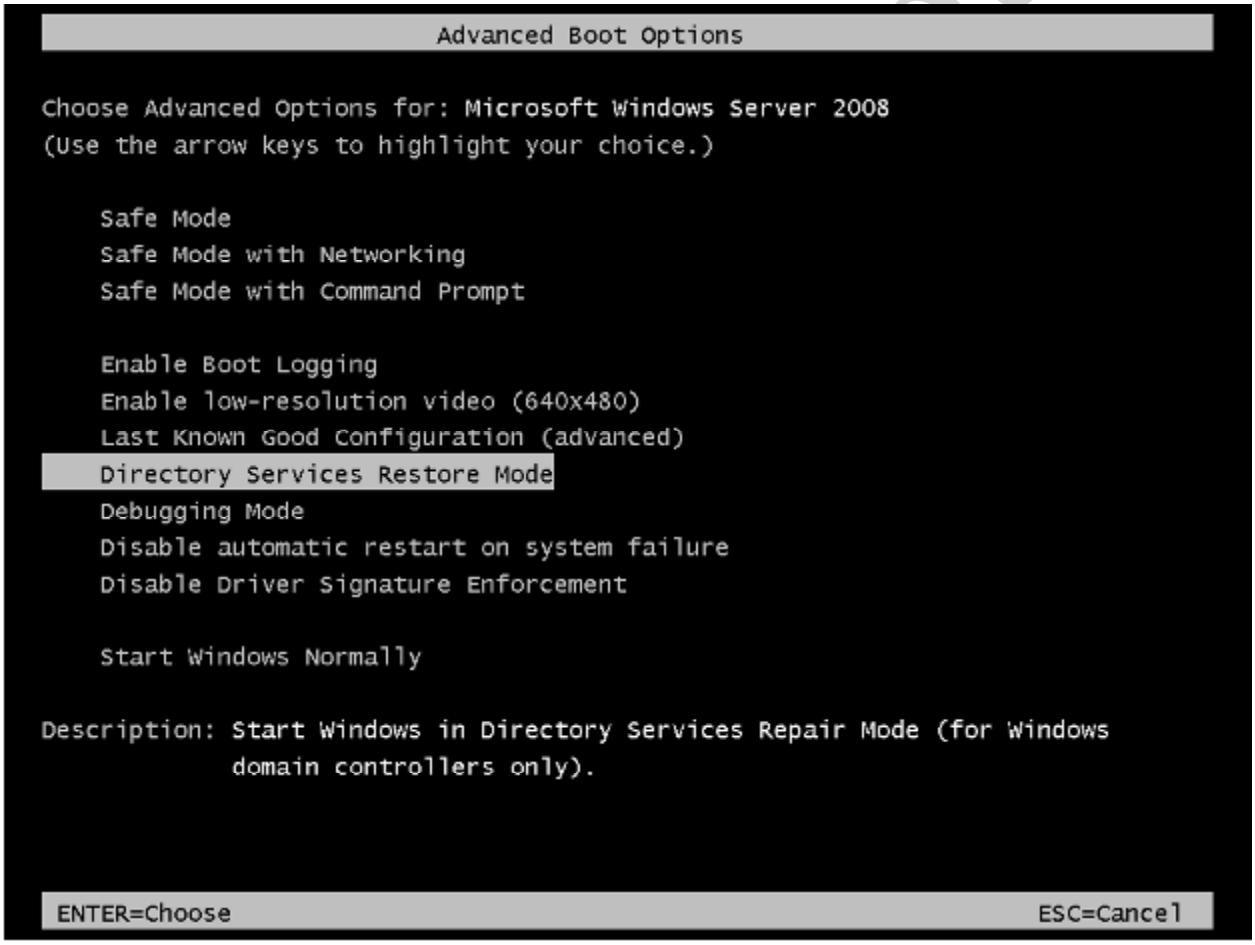


Directory Services Restore Mode:

**گفتیم با دادن پسورد به اکتیو دایرکتوری می توان در صورت خراب شدن آن، با این پسورد اکتیو دایرکتوری را ریکاور کرد. در شکل زیردرهنگام نصب اکتیو دایرکتوری از ما پسورد را می پرسد**

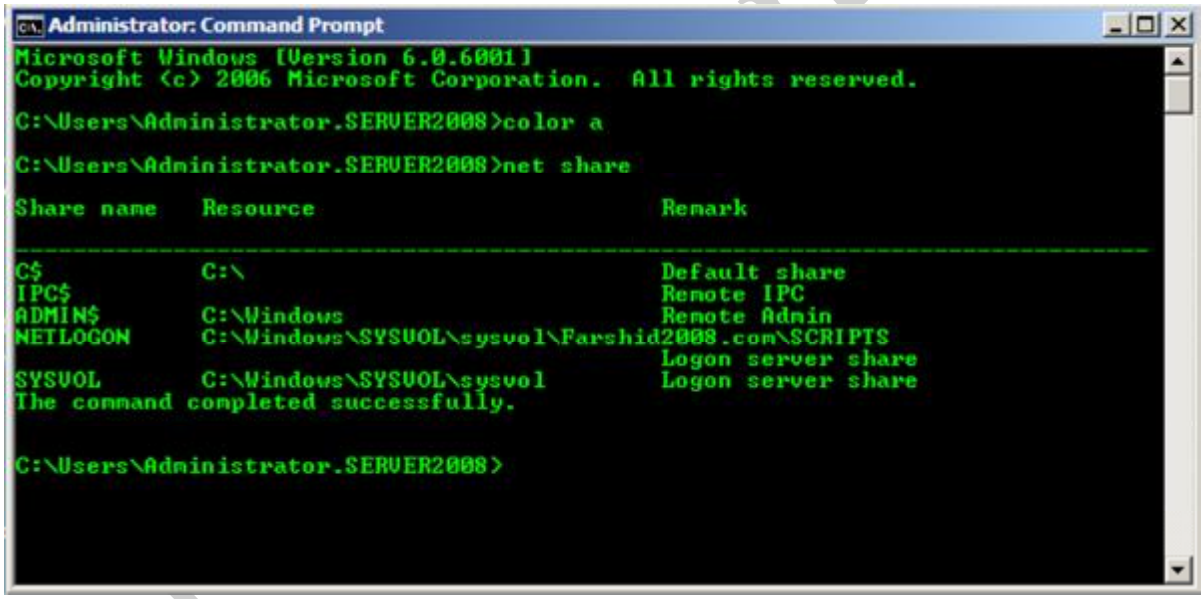


بعد از دادن پسورد اگر اکتیو دایرکتوری ما خراب شد، در هنگام بالا آمدن ویندوز دکمه F8 را می زنیم و از صفحه باز شده(Advanced Boot Options ) گزینه Directory Services Restore Mode را انتخاب می کنیم و سپس پسورد ریکاوری را وارد کرده وریکاوری انجام می شود.



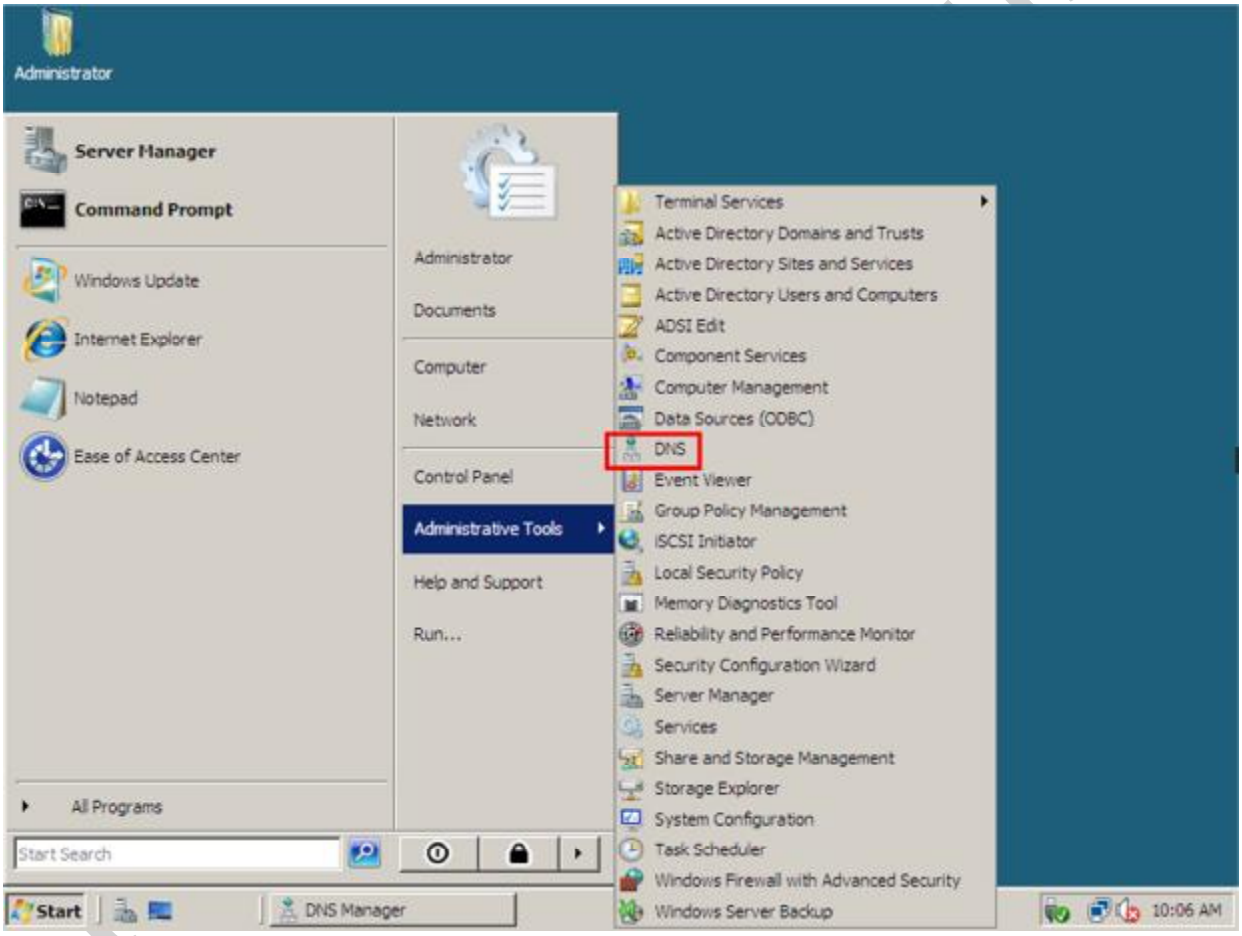
حالا نوبت به تست ADمی رسه که باید دستور NET SHARE را وارد کنیم وقتی که این دستور را وارد می کنیم دو پوشه NET LOG ON و SYSVOL باید SHARE باشد.

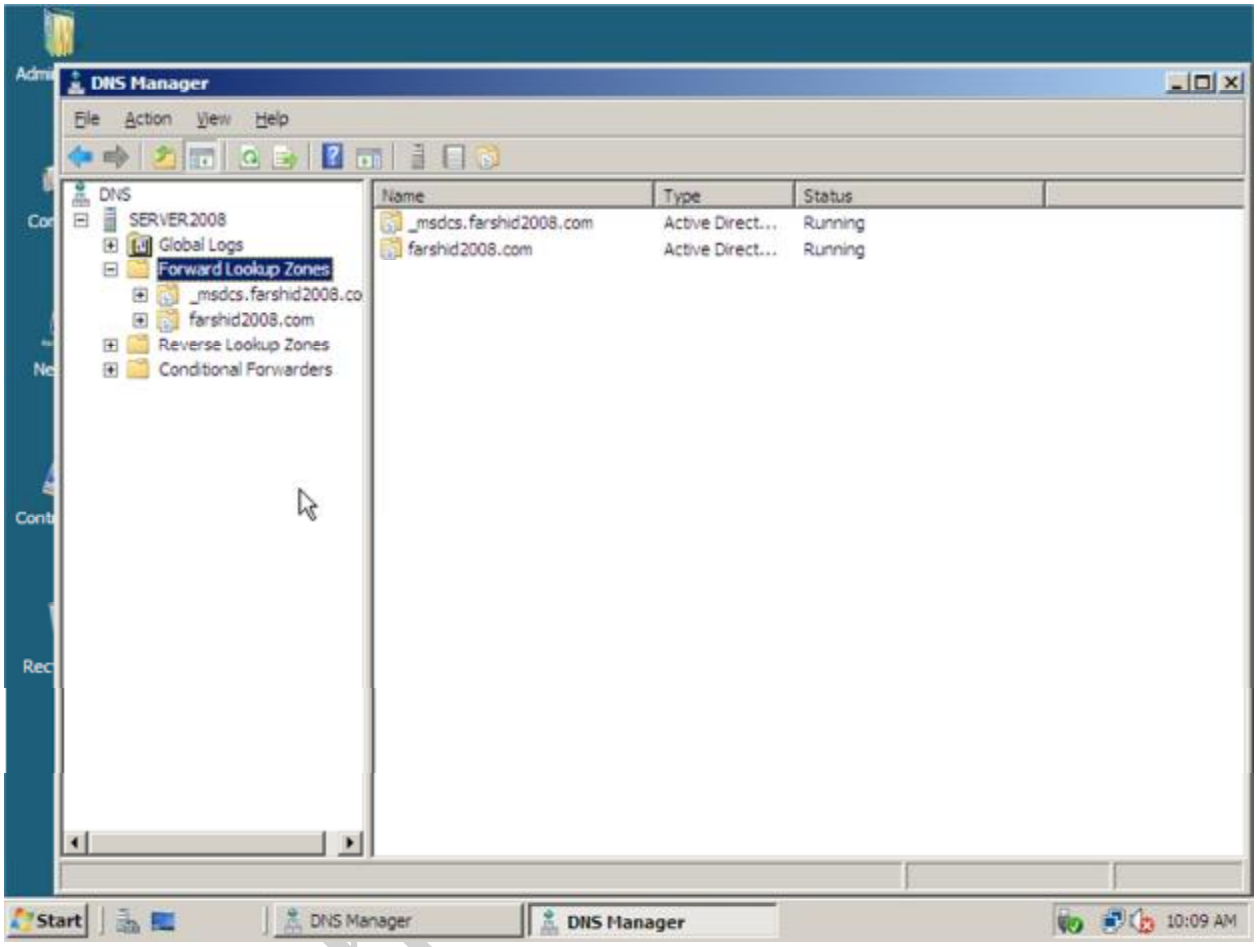
پوشه NET LOG ON شامل یک سری Script های لازم برای ورود به دامین می باشد.




Farshidnoush

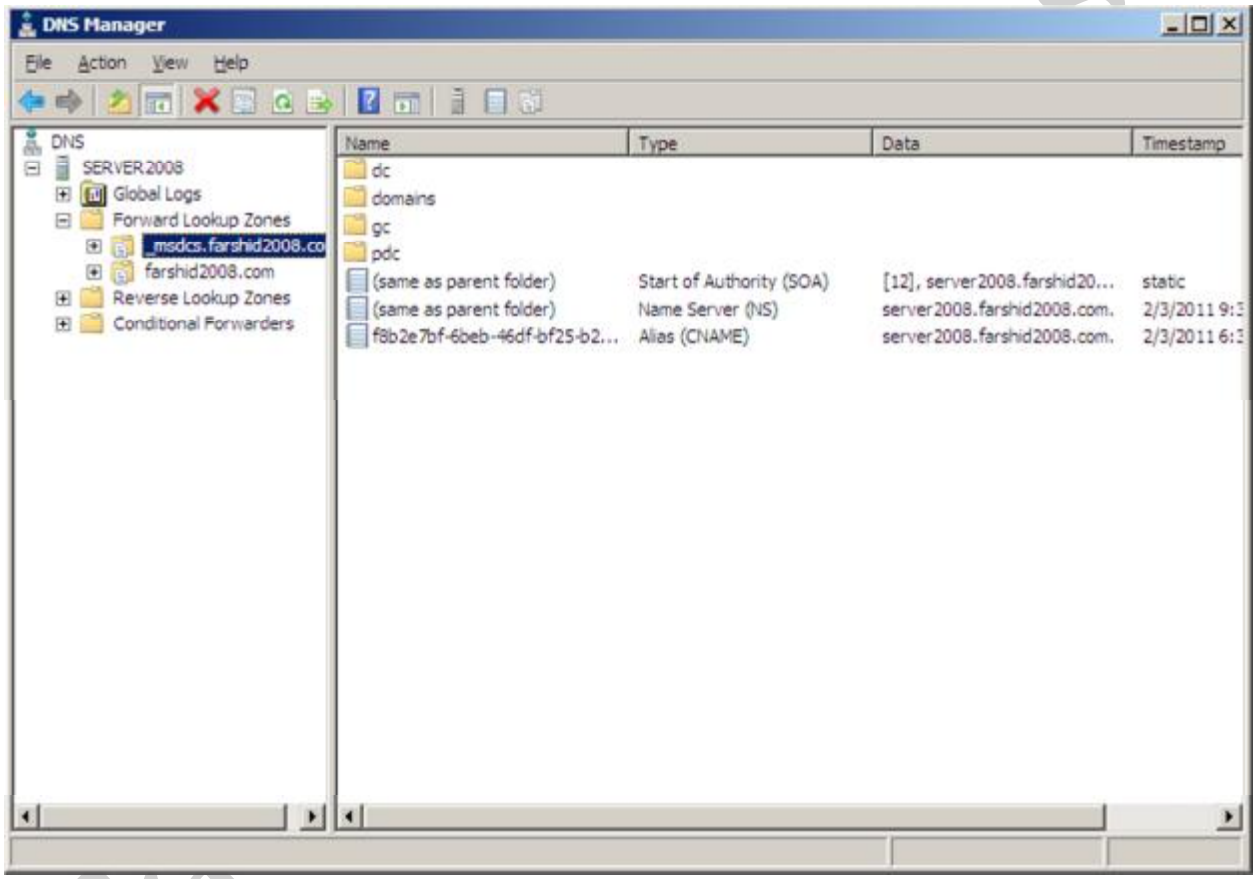
نوبت به تست دوم می رسد وارد Administrative Tools می شویم سپس وارد منوی DNSو شاخه Forward Lookup Zones را باز می کنیم و زیرشاخه های آن باید به صورت زیر باشد



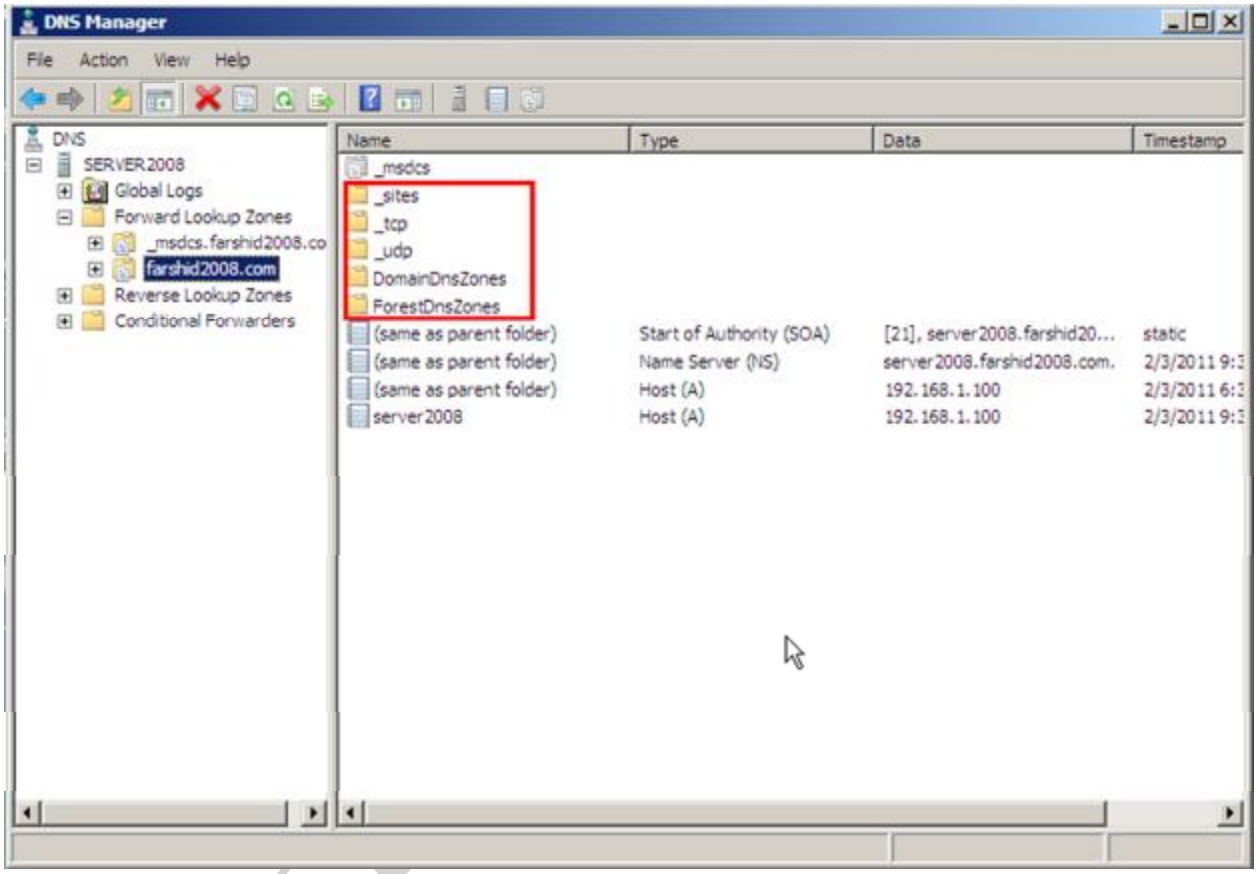

DNS Manager
File Action View Help
DNS
SERVER2008
Global Logs
Forward Lookup Zones
_msdcs.farshid2008.co
farshid2008.com
Reverse Lookup Zones
Conditional Forwarders
Name
Type
Status
_msdcs.farshid2008.com
Active Direct...
Running
farshid2008.com
Active Direct...
Running
Start
DNS Manager
DNS Manager
10:09 AM

Farsh

زیر شاخه های پوشه Forward Lookup Zones (1 _msdcs.farshid2008.com که farshid2008.com. اسم دامینمان هست که در بقیه دامین ها تفاوت دارد ولی msdcs_ همیشه ثابت است،اطلاعاتی که در این پوشه است برای برقراری ارتباط شعبات دیگر با شعبه ما می باشد.

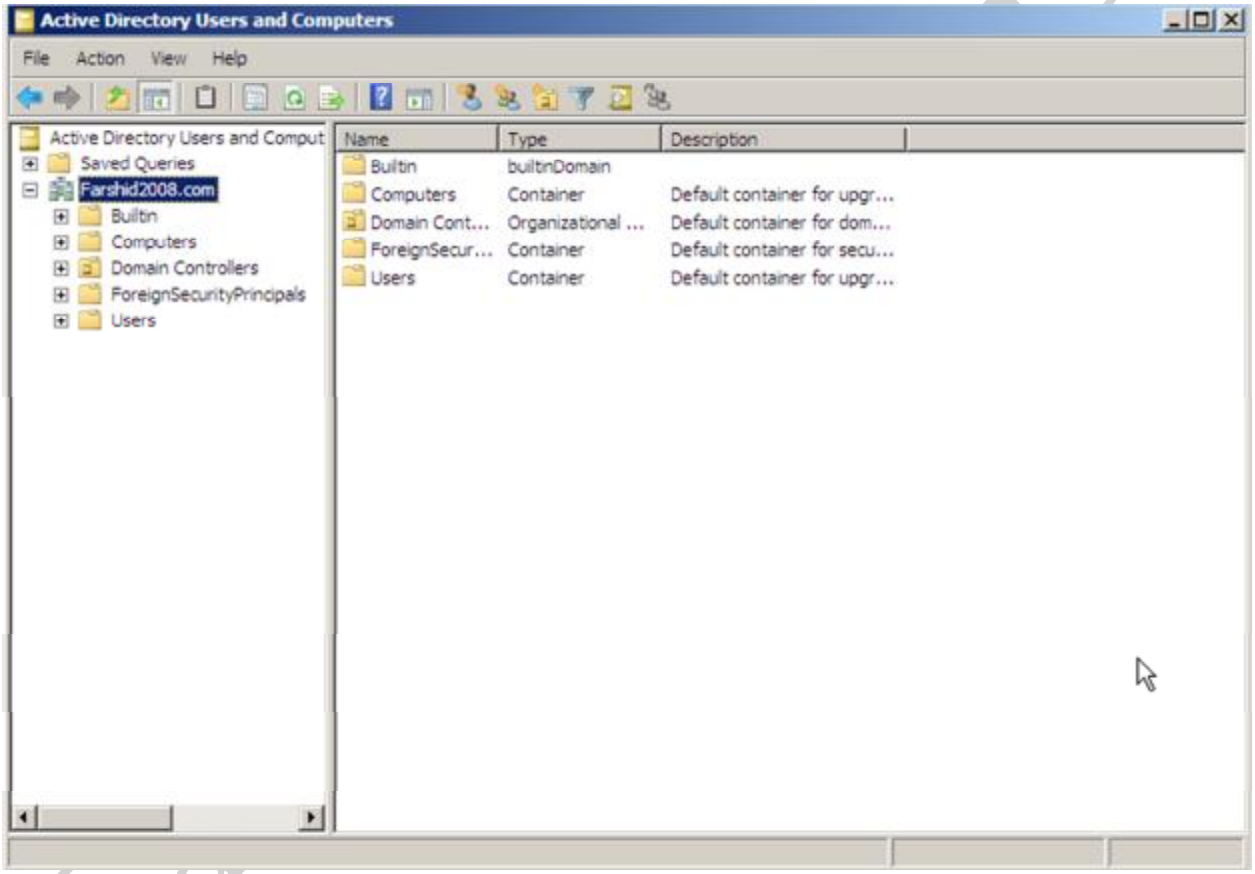


محتویات پوشه ای که به اسم دامینمان است برای برقراری ارتباط Client های شبکه با دامینمان می باشد،در این پوشه یعنی پوشه ای که به اسم دامینمان است باید حتماً 5 پوشه دیگر موجود باشد نه بیشتر نه کمتر.

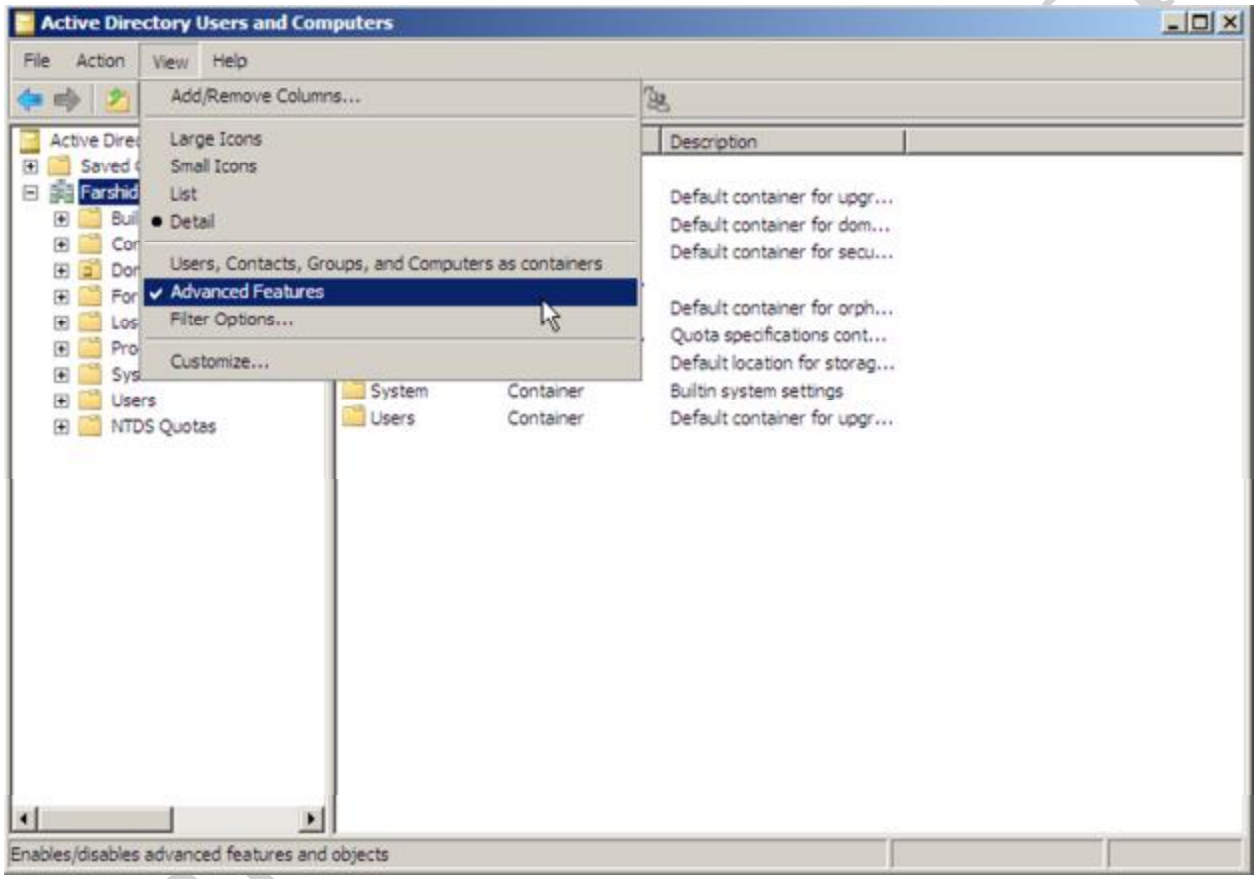


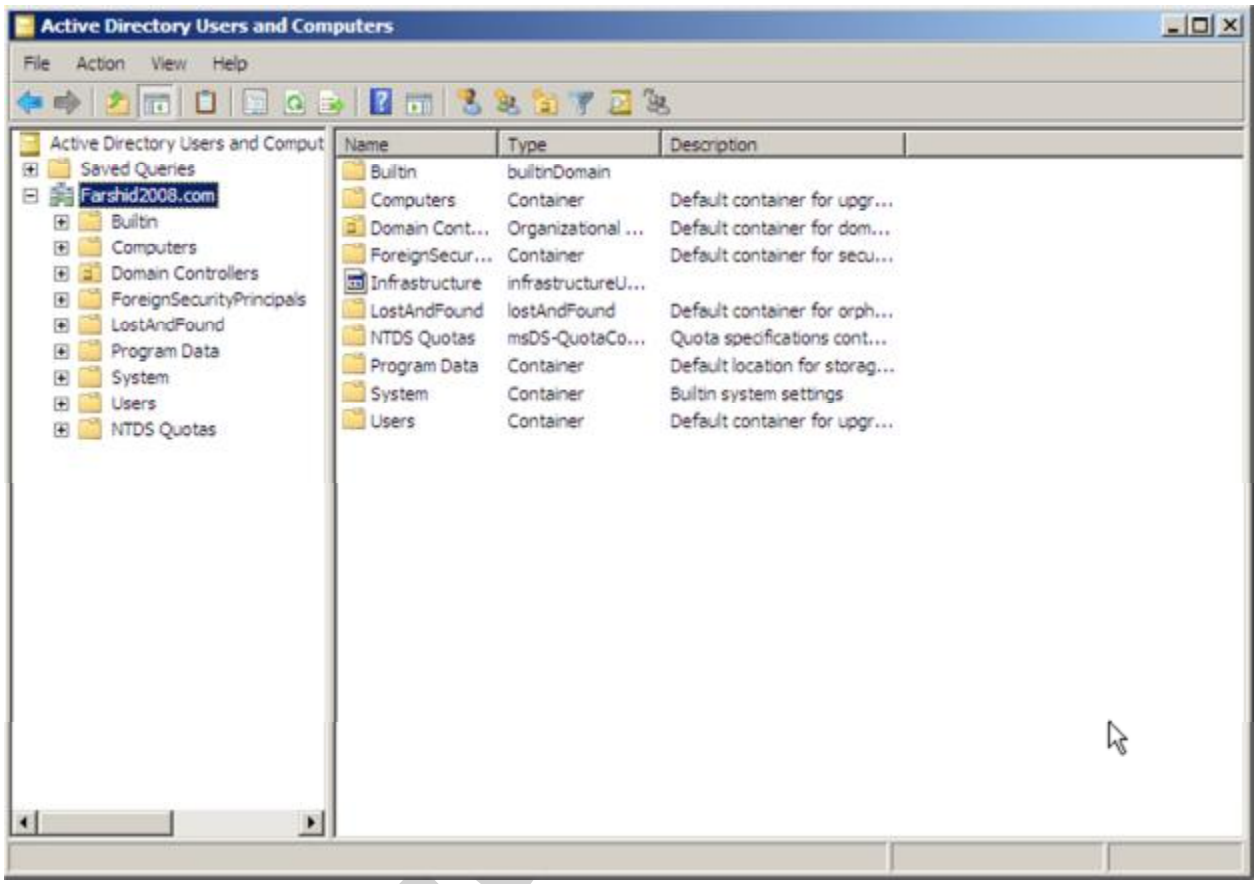

Farsi

نوبت به تست سوم می رسد وارد Administrative Tools می شویم بعد وارد Active Directory Users and Computer(ADUC) می شویم سپس وارد اسم دامینمان می شویم در زیر شاخه آن بایدحداقل 9فولدر موجود باشد کمتر از9 فولدر نباید باشد اگر بیشتر بود مشکلی ندارد.



همانطور که در شکل بالا می بینید 5 فولدر را به صورت پیش فرض به ما نشان می دهد برای اینکه 9 فولدر را کامل ببینیم وارد تب View می شویم وگزینه Advanced Features را انتخاب می کنیم.



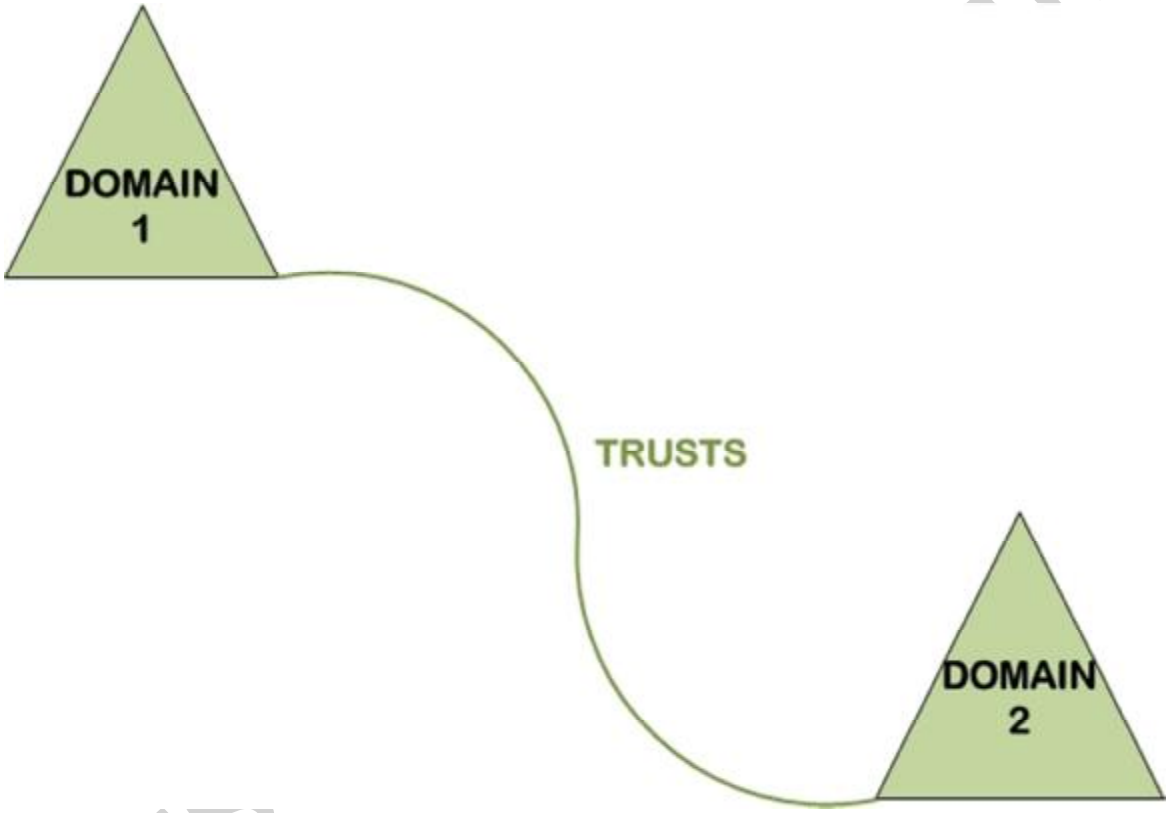



**در اینجا مطمئن می شویم که AD ما درست نصب شده است، اگر فقط یکی از این 3 مرحله درست نبود باید اکتیو را دوباره نصب کنیم.**

Farshid

همزمان با نصب اکتیو روی سرور ما 4 کنسول اضافه می شود:

1) Active Directory Users and Computers (ADUC ): کنسول مدیریت اکتیو دایرکتوری AD
2) Active Directory Domains and Trusts(ADDT): برای وصل کردن شعبات به یکدیگر




Fars

3) Active Directory Sites and Services (ADSS ): کنسولی برای مدیریت ترافیک بین شعبات می باشد.

4) Active Directory Services Interface (ADSI EDIT) : کنسولی برای ارتباط برقرار کردن با اکتیو به زبان خود اکتیو دایرکتوری.همان کنسول اکتیو دایرکتوری است ولی به زبان Distinguished Name(DN) زبان

کاربرد دوم این کنسول برقراری ارتباط بین دایرکتوری سرویس لینوکس(LDAP ) ودایرکتوری سرویس مایکروسافت می باشد یعنی اطلاعات به این کنسول فرستاده و از این کنسول دریافت می شود.

CN=Jaafar,CN=Users,DC=Hani,DC=Com زبان DN

مدیریت شبکه های دامینی:

برای مدیریت دامین اولین کار ایجاد Object ها داخل اکتیو دایرکتوری است

به پارامترهایی که ما میسازیم تا شبکه های دامینی را با آن مدیریت کنیم Object گویند.

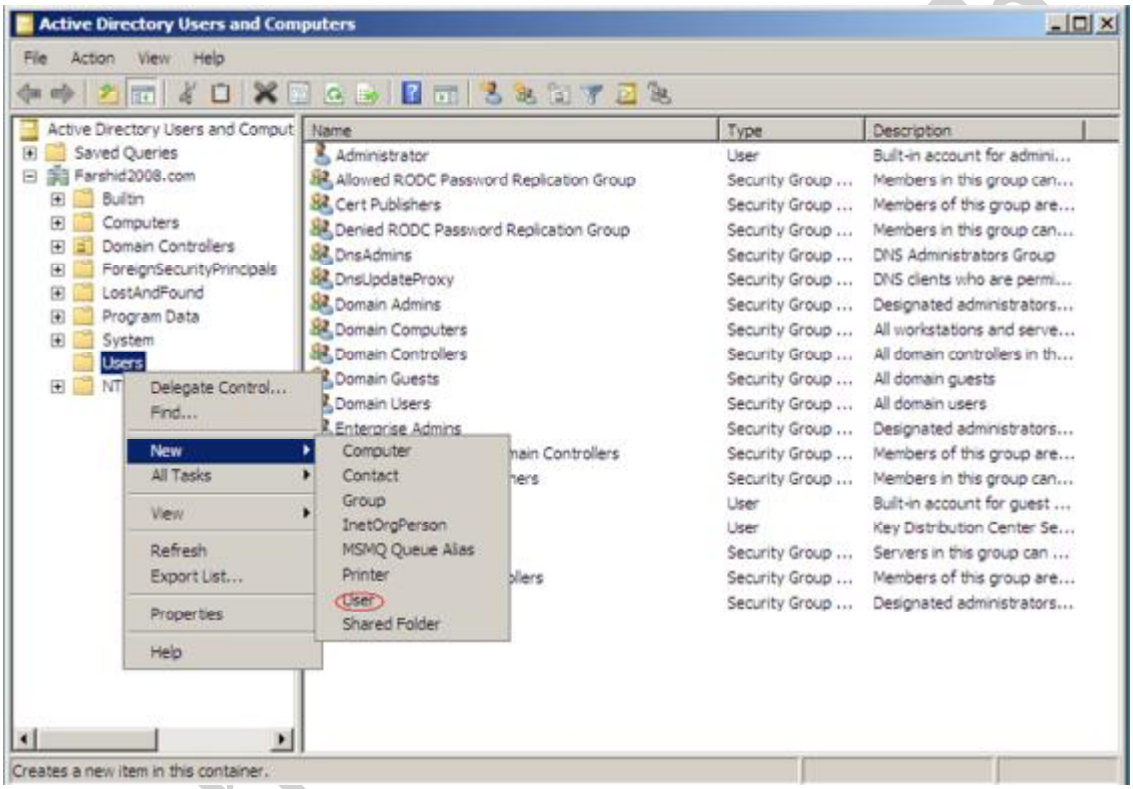
4مورد از Object های مهم: 1) Users 2) Group 3) Computers 4) UnitOrganizaitional (OU )

- هر object که در شبکه های دامینی ساخته می شود از پارتیشنی به نام Schema نشعت می گیرد.
- در داخل پارتیشن Schema هم object ساخته می شوند و هم گزینه های موجود در Properties آنها.

FarshidAjabnoush

اولین Object ، Users:

ساختن Users در اکتیو دایرکتوری:

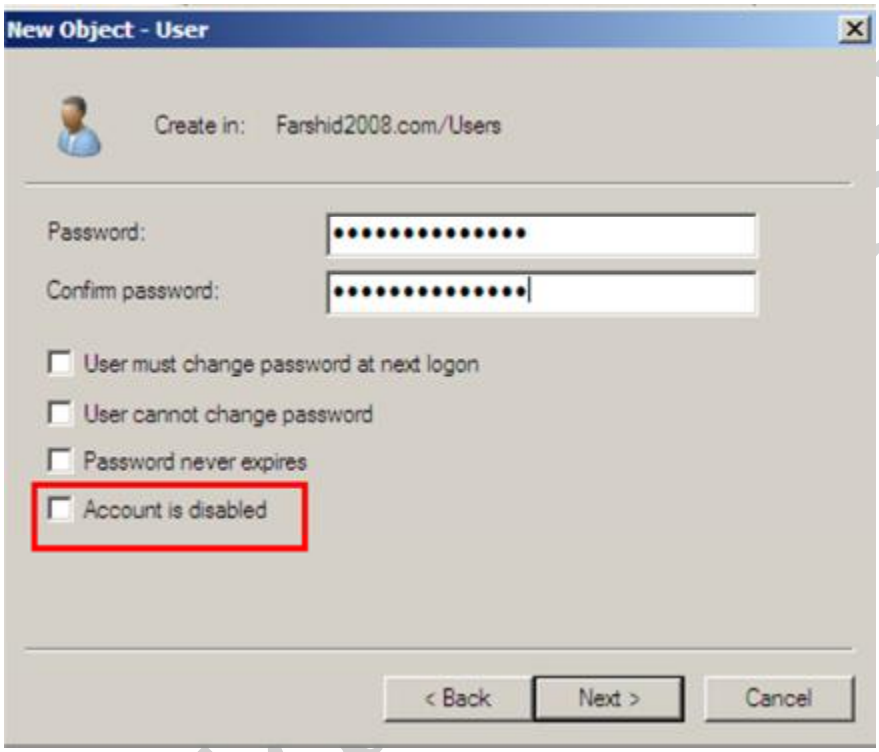



برای اینکه یوزرها پراکنده نباشد همه را داخل یک پوشه به نام Users می سازیم.

Farshid

New Object - User
Create in: Farshid2008.com/Users
First name:
Farshid
Initials:
Last name:
Ajabnoush
Full name:
Farshid Ajabnoush
User logon name:
Farshid_Ajabnoush
@Farshid2008.com
User logon name (pre-Windows 2000):
FARSHID2008\
Farshid_Ajabnoush
< Back
Next >
Cancel

Farshid




مراحل ساختن یک یوزر را در شکل های بالا دیدیم، نوبت به توضیحی در باره پسورد یوزرها می رسد: 1- پسورد یوزرها باید Complexity باشد یعنی ترکیبی از حروف،اعداد و علامت باشد مانند: ADF@$256

2- Accont is disabled : اگر این گزینه فعال باشد،یوزر با این نام کاربری نمی تواند به شبکه Log in کند ولی می تواند در Run as از این یوزر استفاده کند.

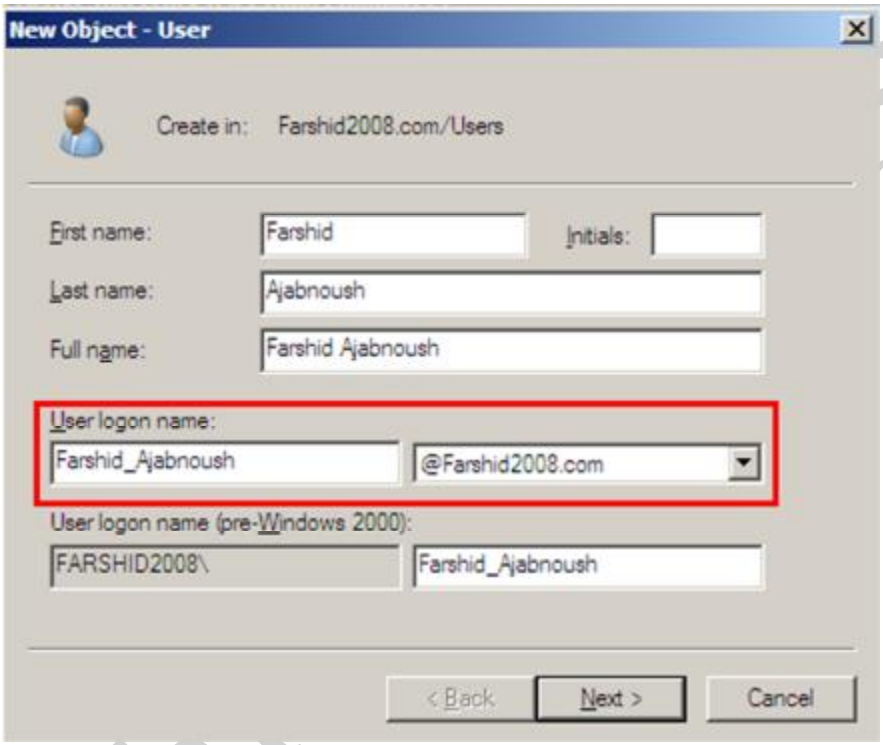
همزمان با ایجاد یک یوزر در اکتیو دایرکتوری نا خواسته 3 اکانت برایش ایجاد می شود.

نام اولین اکانت User Log on Name می باشد که یوزر با این اسم می تواند وارد شبکه بشود.

Farshid Ajabnoush

نام دومین اکانت User Principal Name (UPN ACCONT ):

به ترکیب اسم User Log on Name و اسم دامین UPN ACCONT گویند.



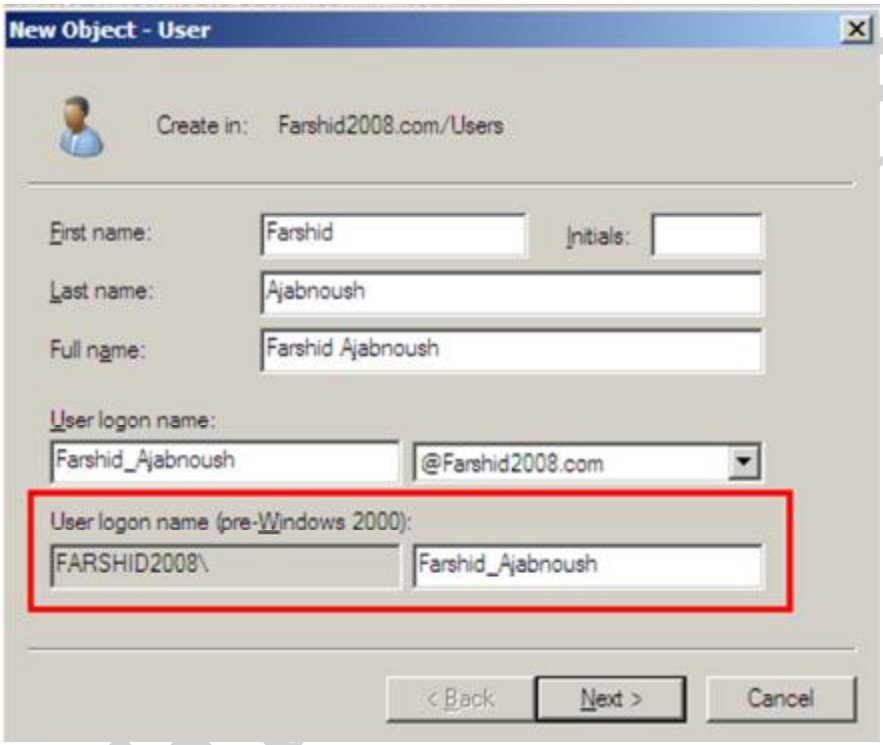

UPN ACCONT:Farshid_Ajabnoush@Farshid2008.Com

**این اکانت یک اکانت ایمیلی میباشد یعنی با ساختن یک یوزر در مجموعه یک ایمیل هم در مجموعه برایمان ساخته می شود.**

Farshid Ajabnoush

نام سومین اکانت UserLogon Name (Pre-Windows2000):

به ترکیب اسم دامین و User Logon Name گویند




در ویندوزهای NG وقتی بخواهیم وارد شبکه بشویم باید به این فرم وارد شویم.

Farshid2008\ Farshid_Ajabnoush یعنی در صفحه Log On از این اسم استفاده می کنیم.

Farshid Ajabnoush

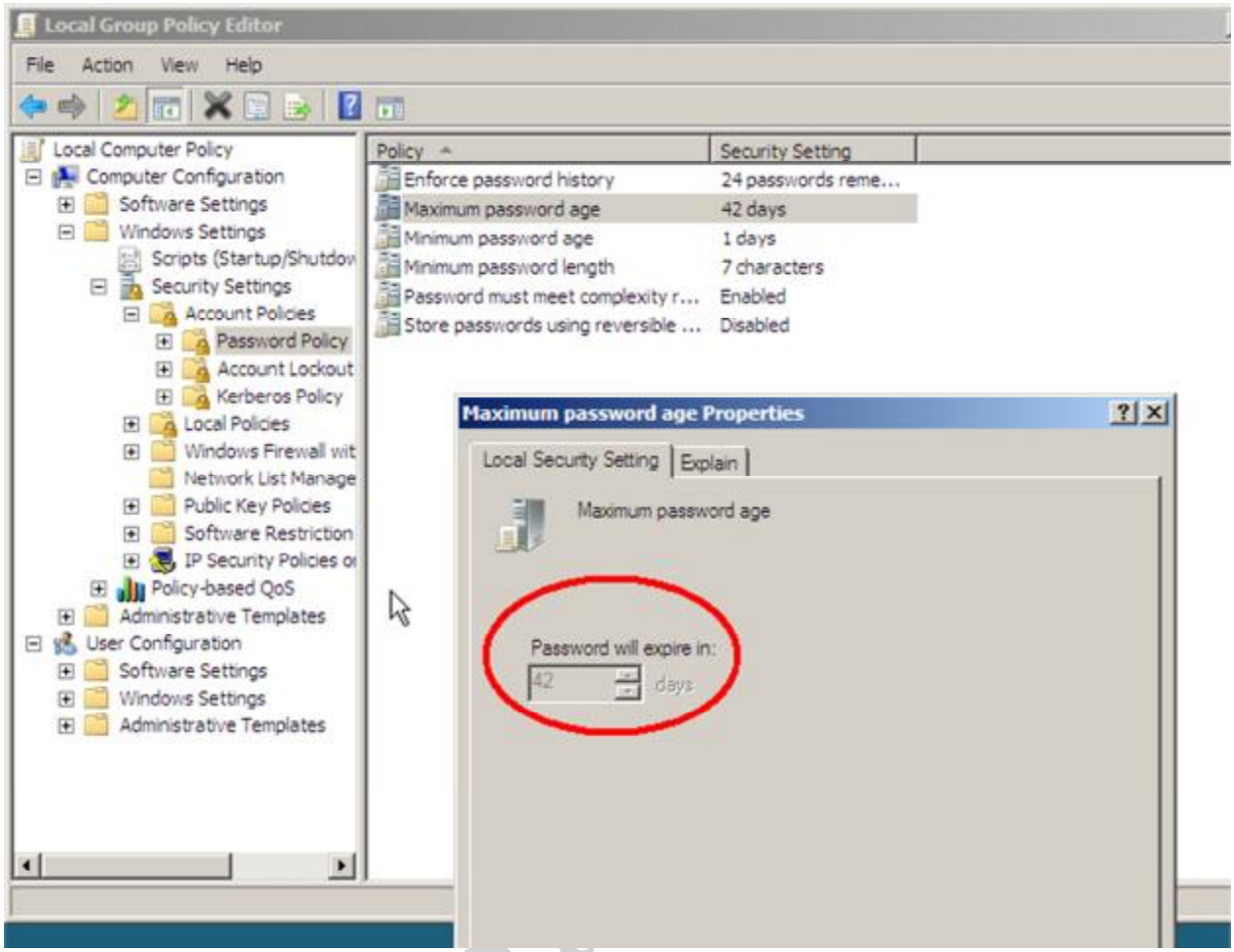
پشت کامپیوتری که AD نصب شده باشد نمی توان بصورت Local (WorkGroup ) وارد شد حتماً باید بصورت دامینی وارد شد به این دلیل که در شبکه های Work Group یوزر نیم و پسورد ما در فایلی به نام SAM ACCOUNT ذخیره می شود وقتی به دامین وصل می شویم فایل SAMوارد فایل NTDS.DIT می شود.

- اسم دیتا بیس اکتیو دایرکتوری NTDS.DIT می باشد.
- روی سروری که AD نصب شده است 2 نوع پالیسی داریم 1)Local Group Policy 2) Default Domain Policy

- Local Group Policy: پالیسی هایی که اینجا اعمال بشوند فقط به همان کامپیوتر اعمال می شوند.
- Default Domain Policy : : پالیسی هایی که اینجا اعمال بشوند به کل شبکه اعمال می شوند.

اگر گروپ پالیسی را از Run باز کنیم به این صورت: Run سپس تایپ کنیم gpedit.msc به مشکل زیر بر می خوریم

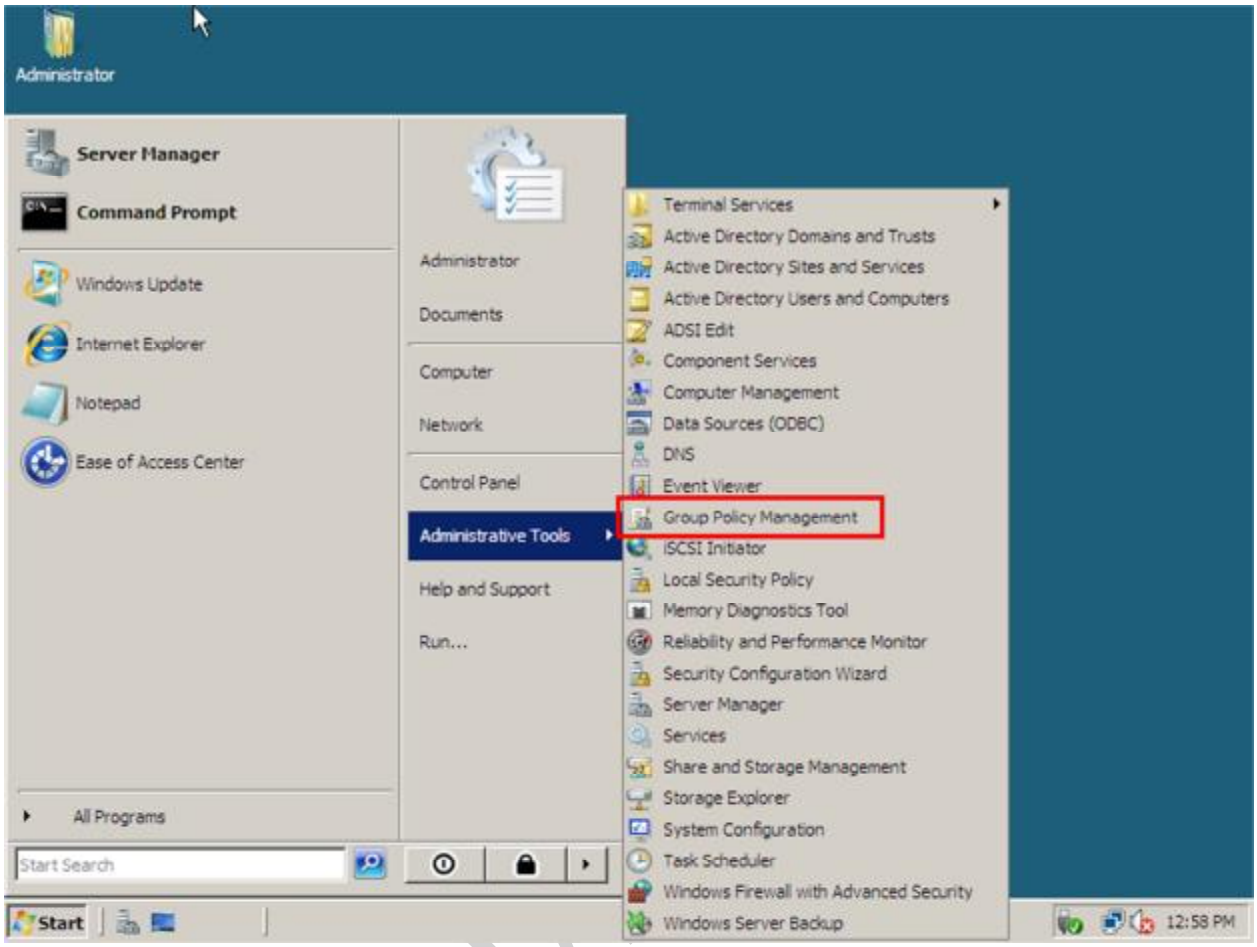
FarshidAjabnoush




**که هیچ تغییری نمی توانیم ایجاد کنیم .**

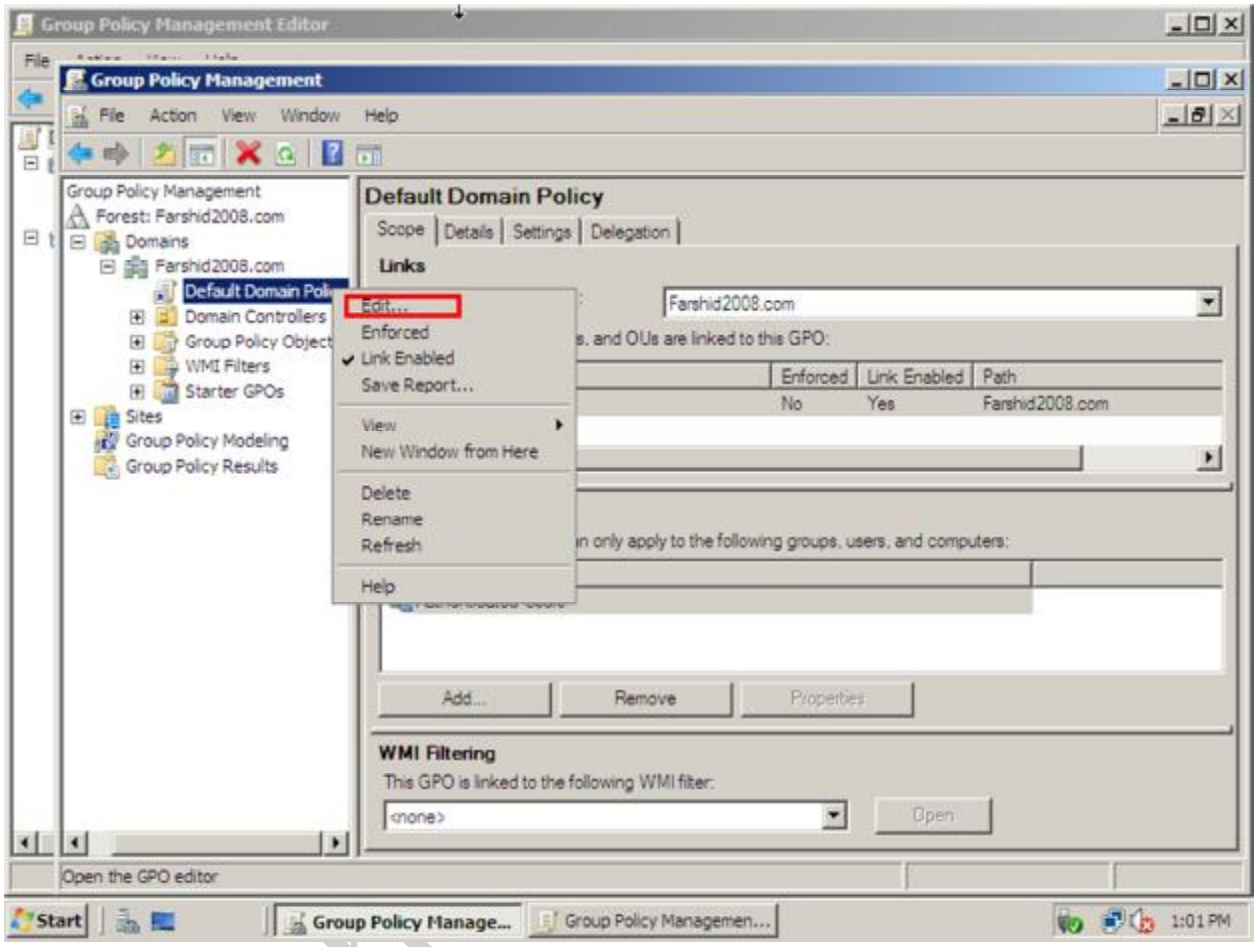
**برای باز کردن گروپ پالیسی در سیستمی که روی آن اکتیو دایرکتوری (AD ) نصب است باید وارد Administrative Tools بشویم وسپس Group Policy Management را باز می کنیم.**

Farshid

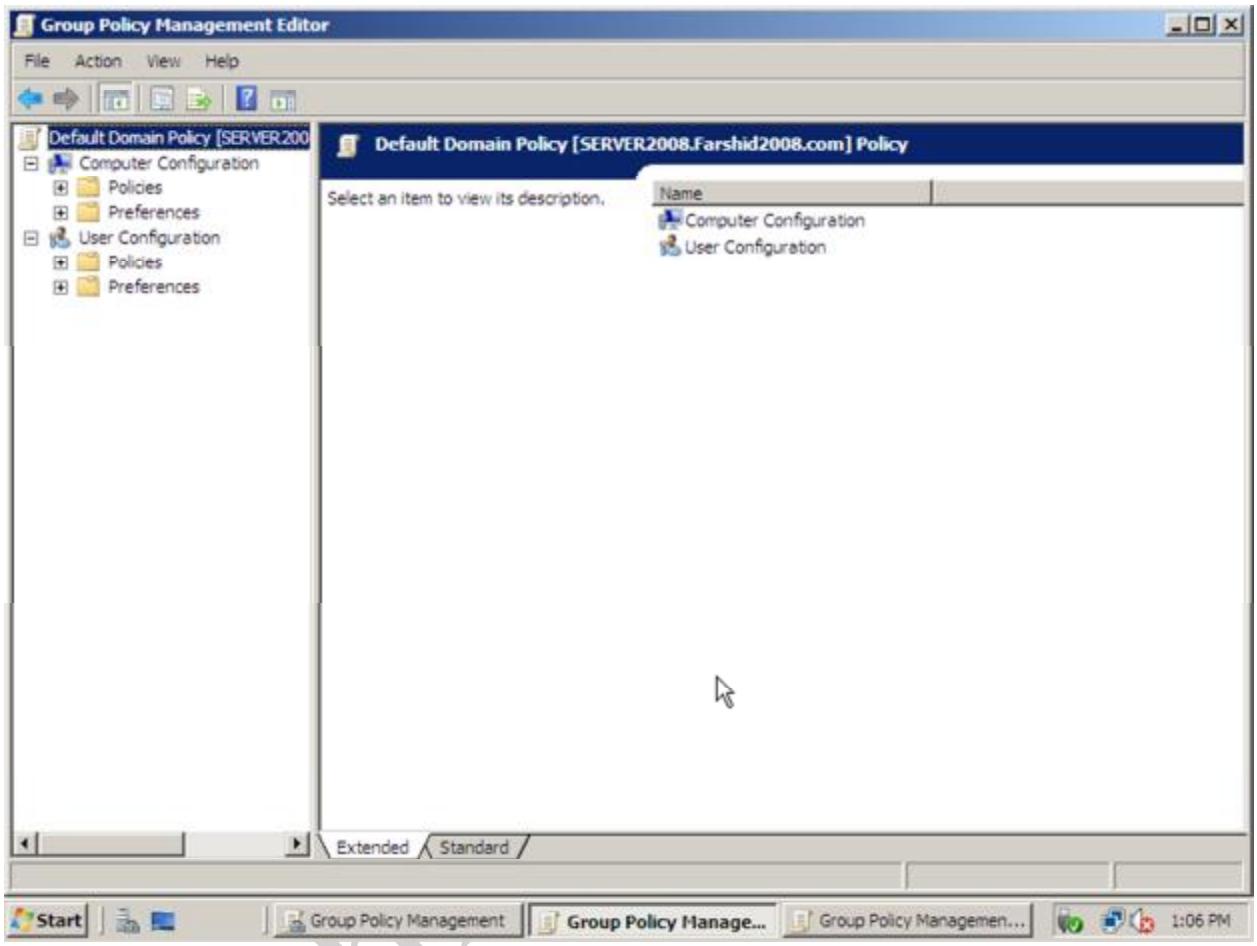



Farshida

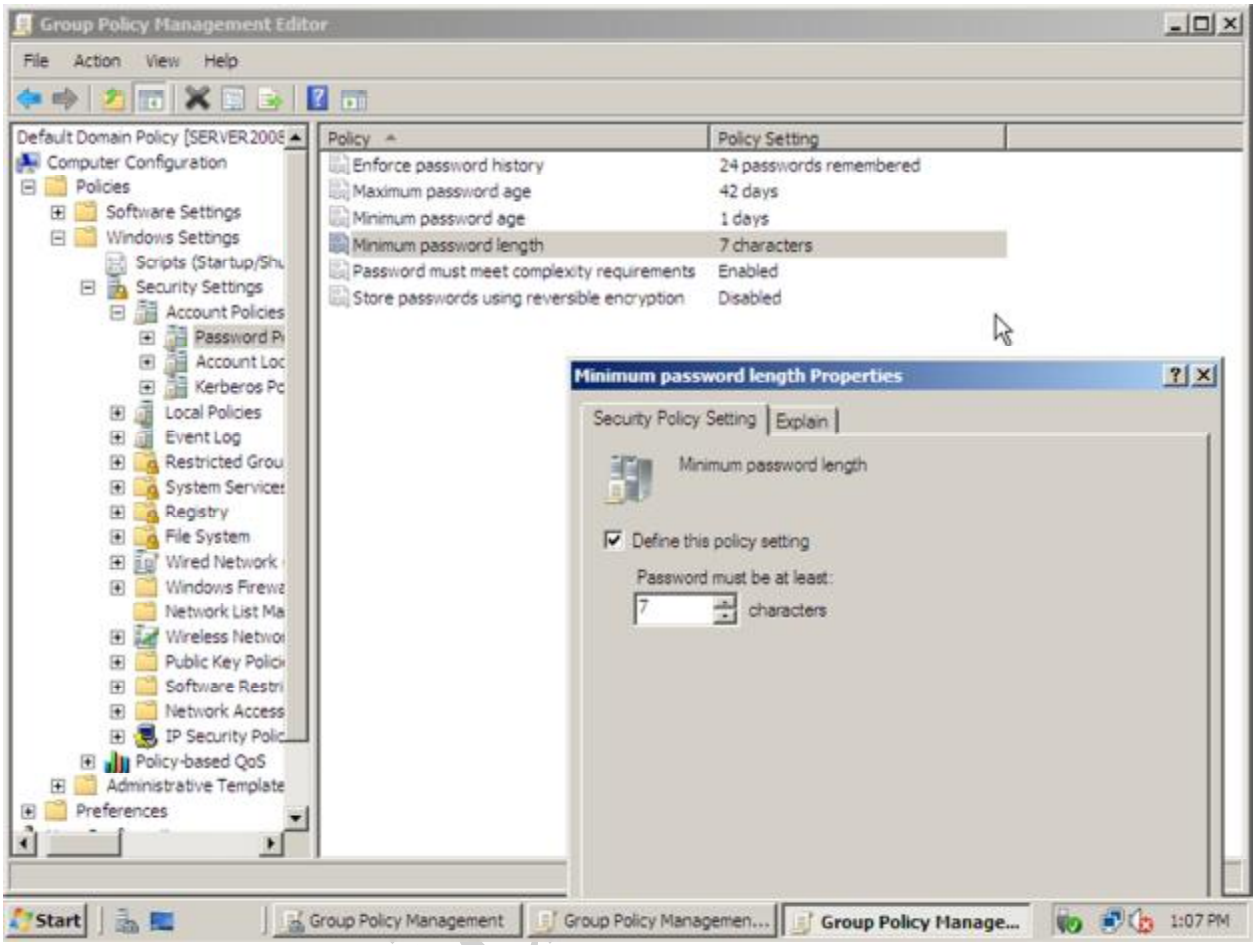
وقتی که باز شد ابتدا وارد Forestشده سپس وارد Domains و وارد اسم دامین می شویم و روی Default Domain Policy راست کلیک کرده وگزینه Edit را می زنیم .


Group Policy Management Editor
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: Farshid2008.com
Domains
Farshid2008.com
Default Domain Polic
Domain Controllers
Group Policy Object
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Default Domain Policy
Scope Details Settings Delegation
Links
Farshid2008.com
Edit...
Enforced
Link Enabled
Save Report...
View
New Window from Here
Delete
Rename
Refresh
Help
Enforced Link Enabled Path
No Yes Farshid2008.com
Add... Remove Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
Open the GPO editor
Start
Group Policy Manage...
Group Policy Managemen...
1:01 PM

Farsh


Group Policy Management Editor
File Action View Help
Default Domain Policy [SERVER200
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Default Domain Policy [SERVER2008.Farshid2008.com] Policy
Select an item to view its description.
Name
Computer Configuration
User Configuration
Extended Standard
Start
Group Policy Management
Group Policy Manage...
Group Policy Managemen...
1:06 PM

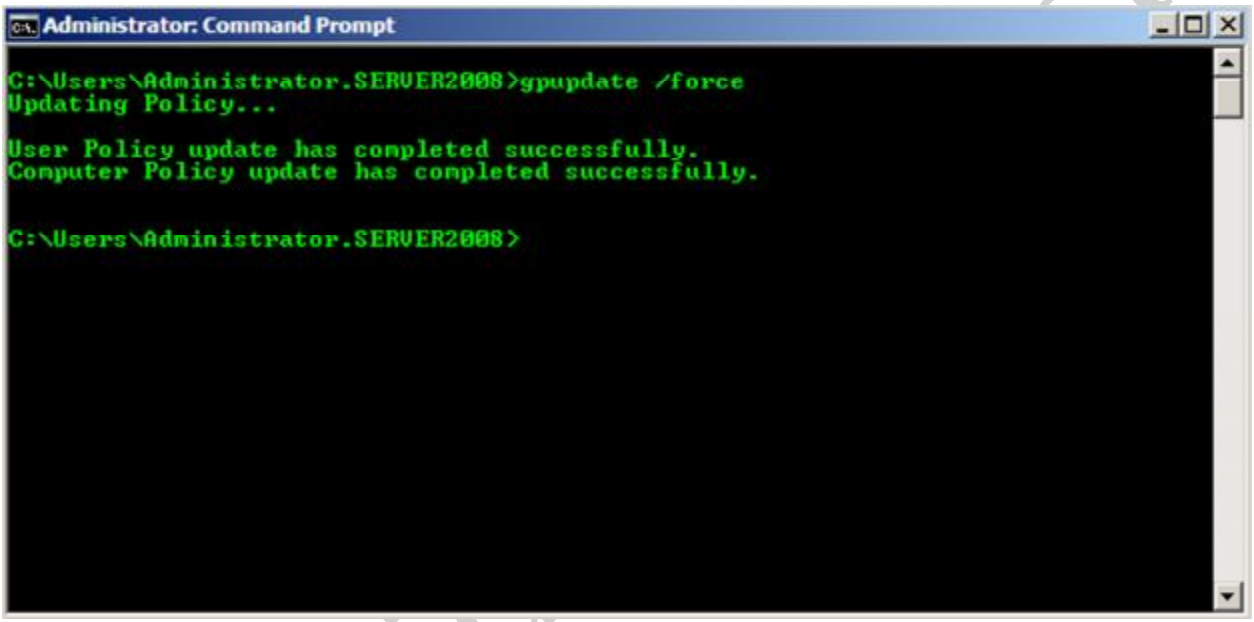
Farshid




**همانطور که میبینید تمامی منوها باز و فعال می باشند**

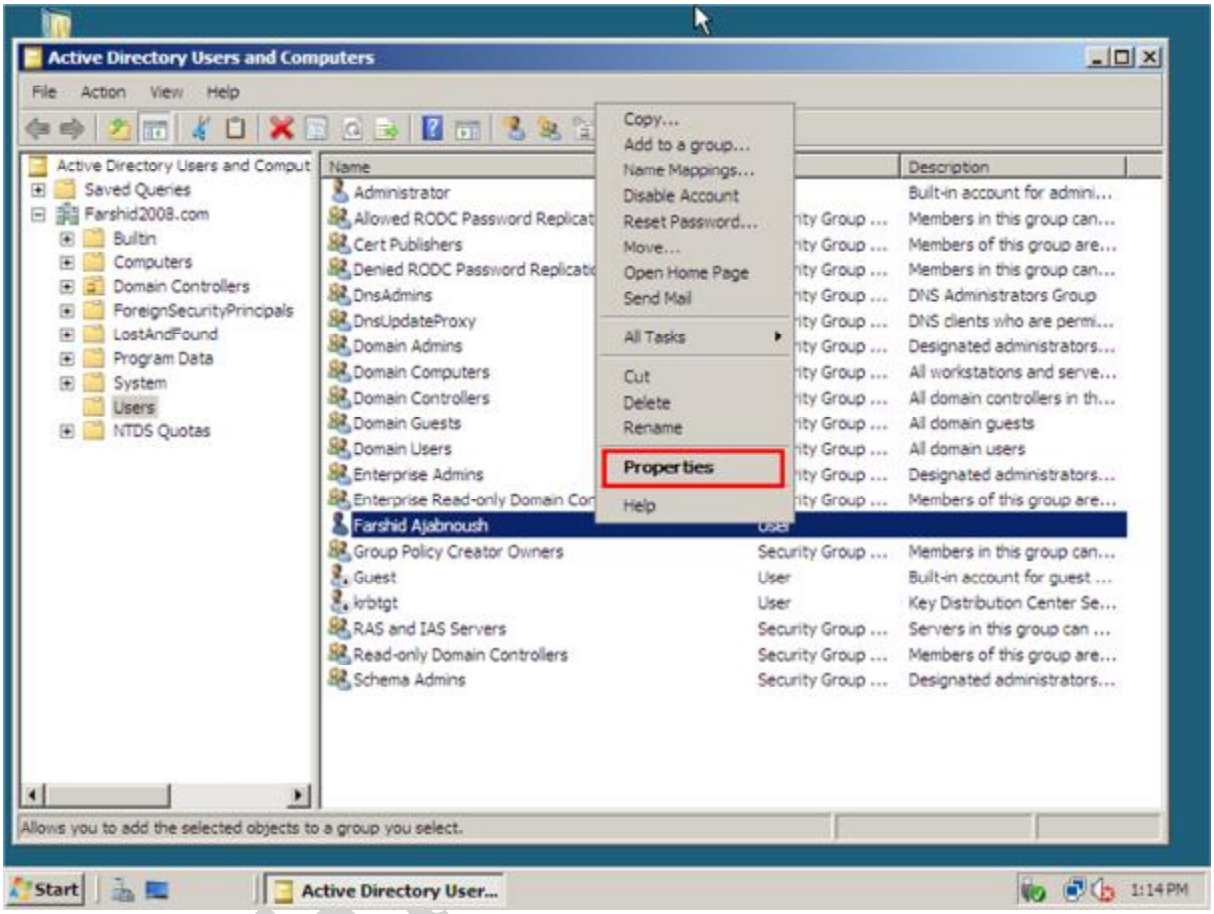
Farshid

- به خاطر داشته باشید که بعد از تغییر در گروپ پالیسی برای اعمال پالیسی باید در محیط کامند دستور Gpupdate /force را وارد کنیم تا پالیسی اعمال شود.

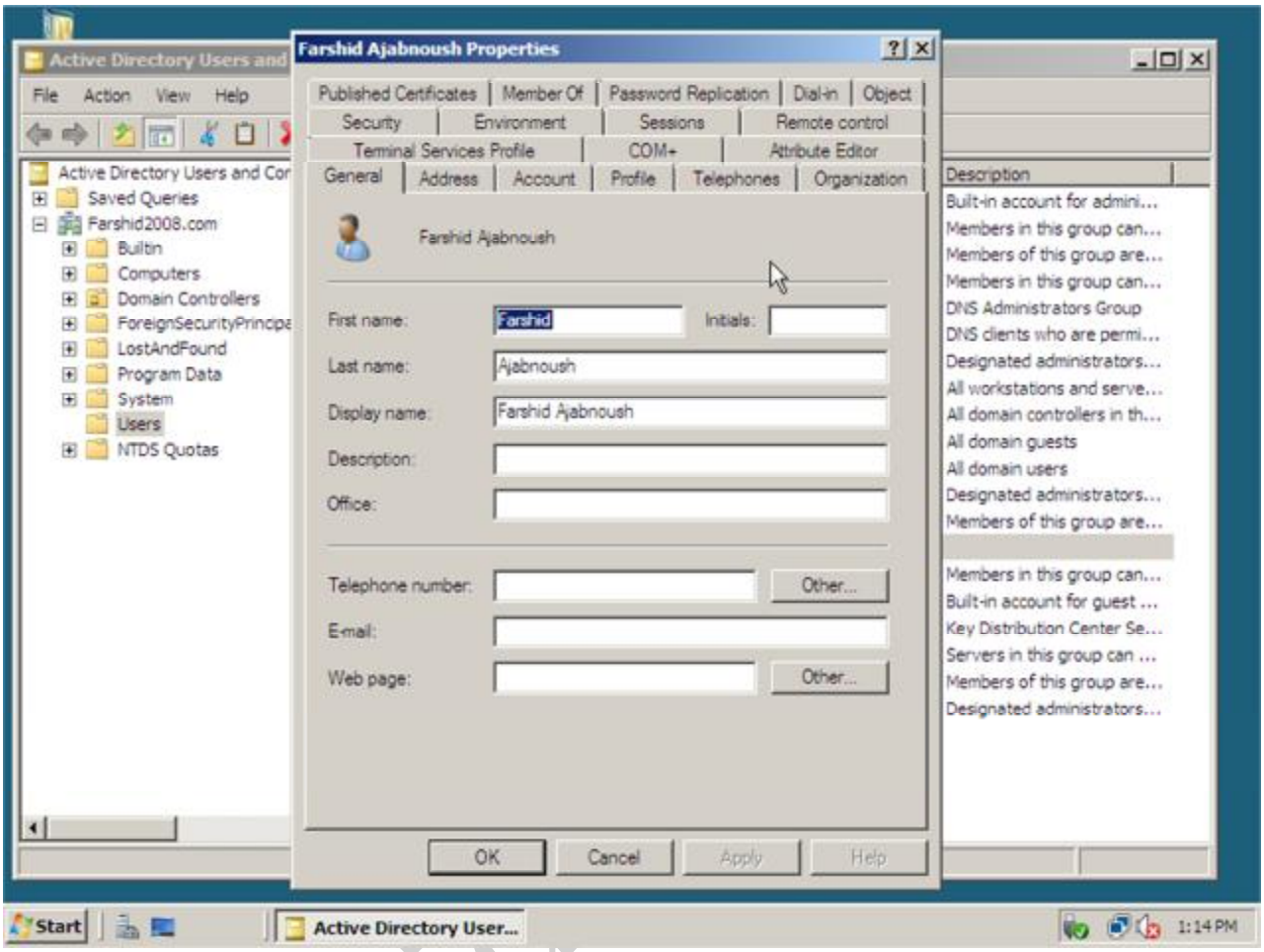



Farshid

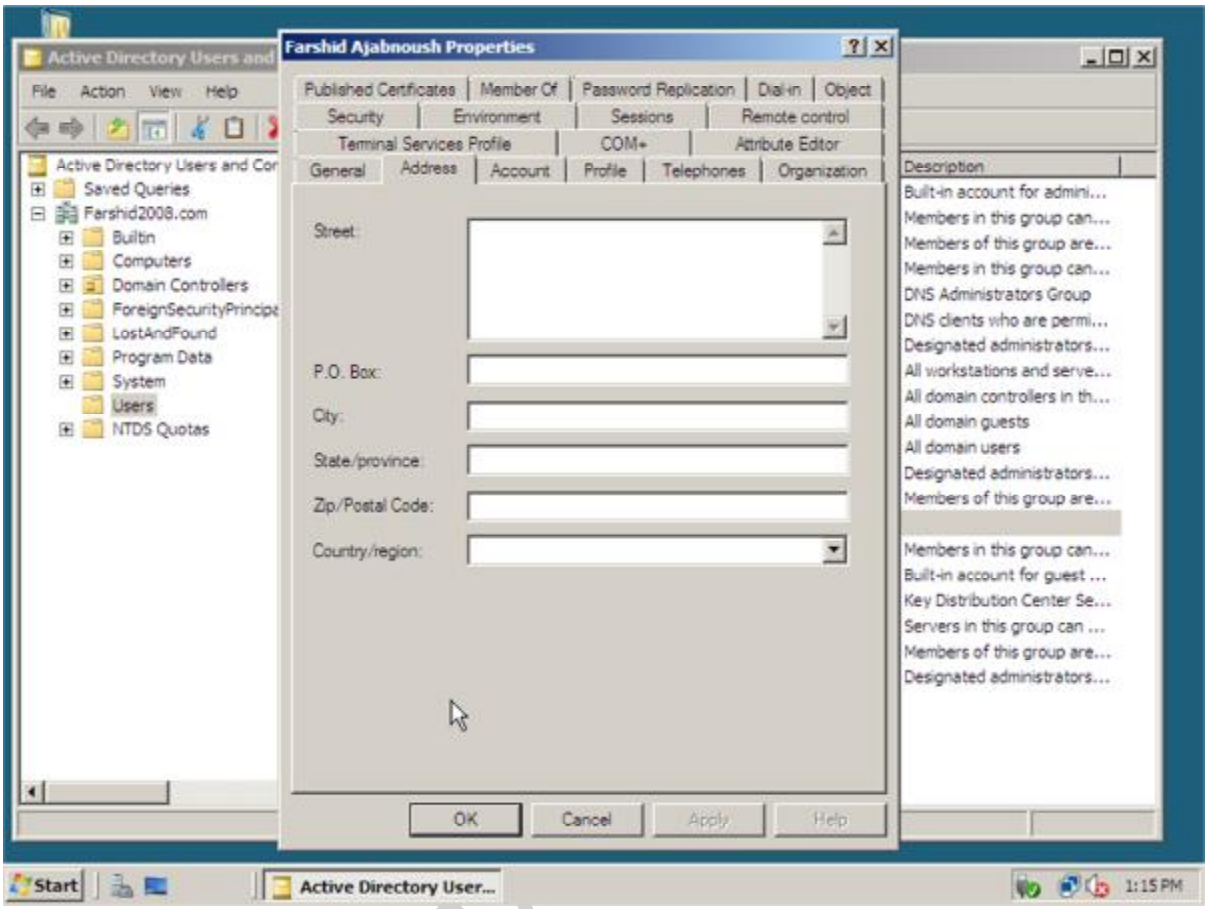
**اولین کار بعد از ساختن یوزر پر کردن اطلاعات پروفایل آن یوزر است**




Farsh


Active Directory Users and
File Action View Help
Active Directory Users and Cor
Saved Queries
Farshid2008.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipa
LostAndFound
Program Data
System
Users
NTDS Quotas
Farshid Ajabnoush Properties
Published Certificates | Member Of | Password Replication | Dial-in | Object
Security | Environment | Sessions | Remote control
Terminal Services Profile | COM+ | Attribute Editor
General | Address | Account | Profile | Telephones | Organization
Farshid Ajabnoush
First name: Farshid
Initials:
Last name: Ajabnoush
Display name: Farshid Ajabnoush
Description:
Office:
Telephone number:
Other...
E-mail:
Web page:
Other...
OK
Cancel
Apply
Help
Description
Built-in account for admini...
Members in this group can...
Members of this group are...
Members in this group can...
DNS Administrators Group
DNS clients who are permi...
Designated administrators...
All workstations and serve...
All domain controllers in th...
All domain guests
All domain users
Designated administrators...
Members of this group are...
Members in this group can...
Built-in account for guest ...
Key Distribution Center Se...
Servers in this group can ...
Members of this group are...
Designated administrators...
Start
Active Directory User...
1:14 PM

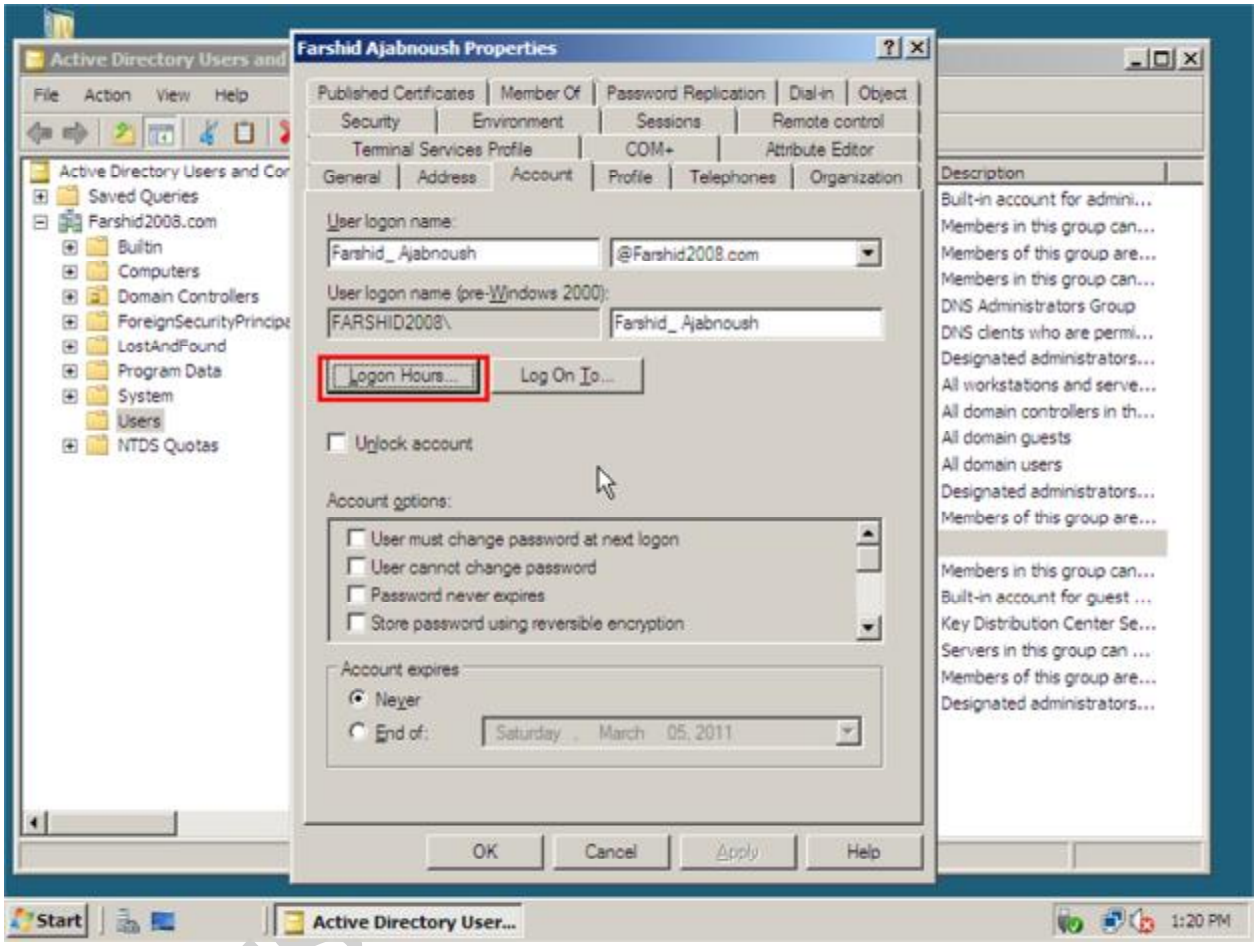
Farshid



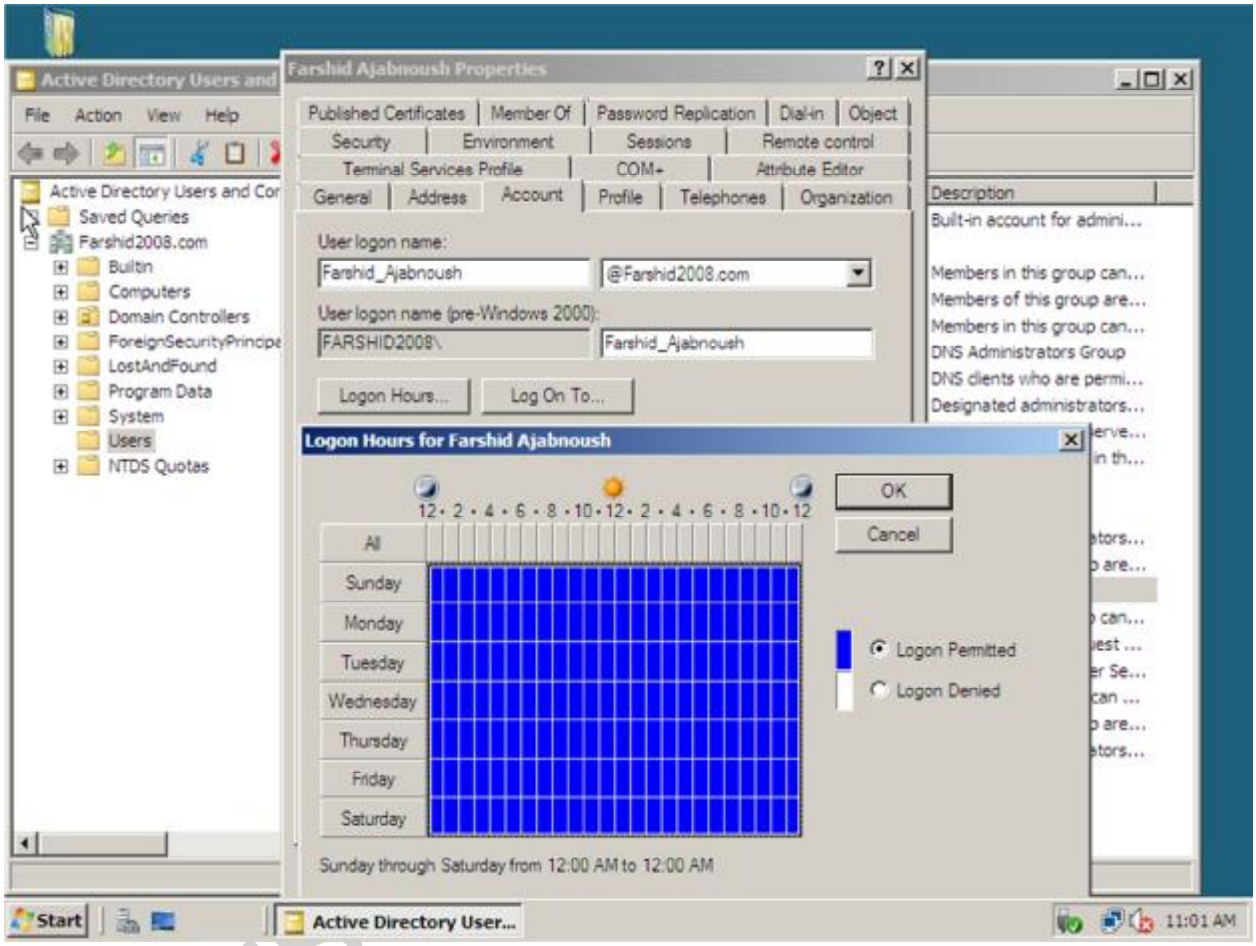

**پر کردن تمام این فیلدها باعث راحتی کار خودمان در آینده می شود مثلاً برای پیدا کردن کارمندهایی که در یک محدوده زندگی می کنند.**

Farshid

از تب Account وارد گزینه Log on Hours می شویم و ساعت ورود وخروج هر یوزر به شبکه را تنظیم می کنیم .

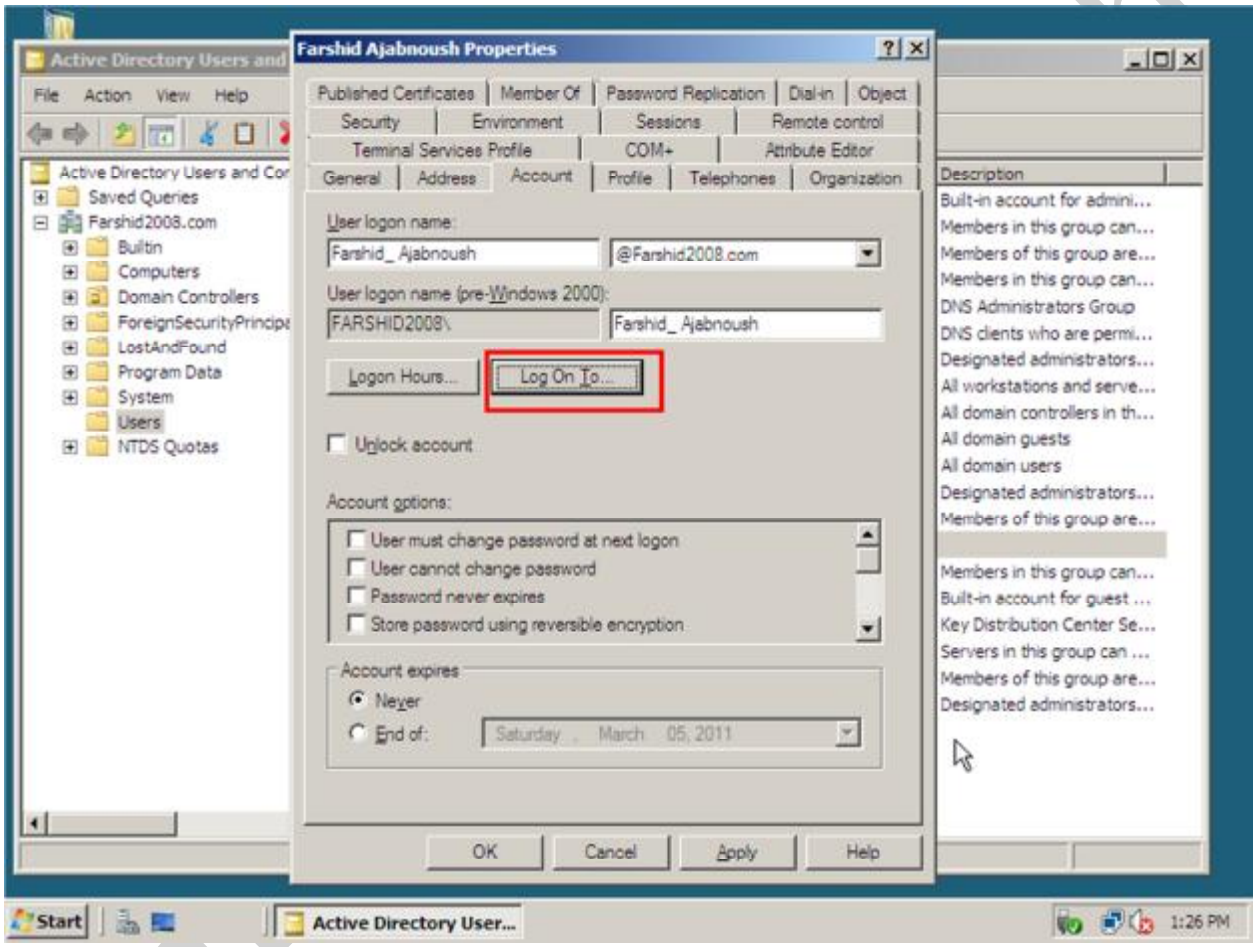



Fars

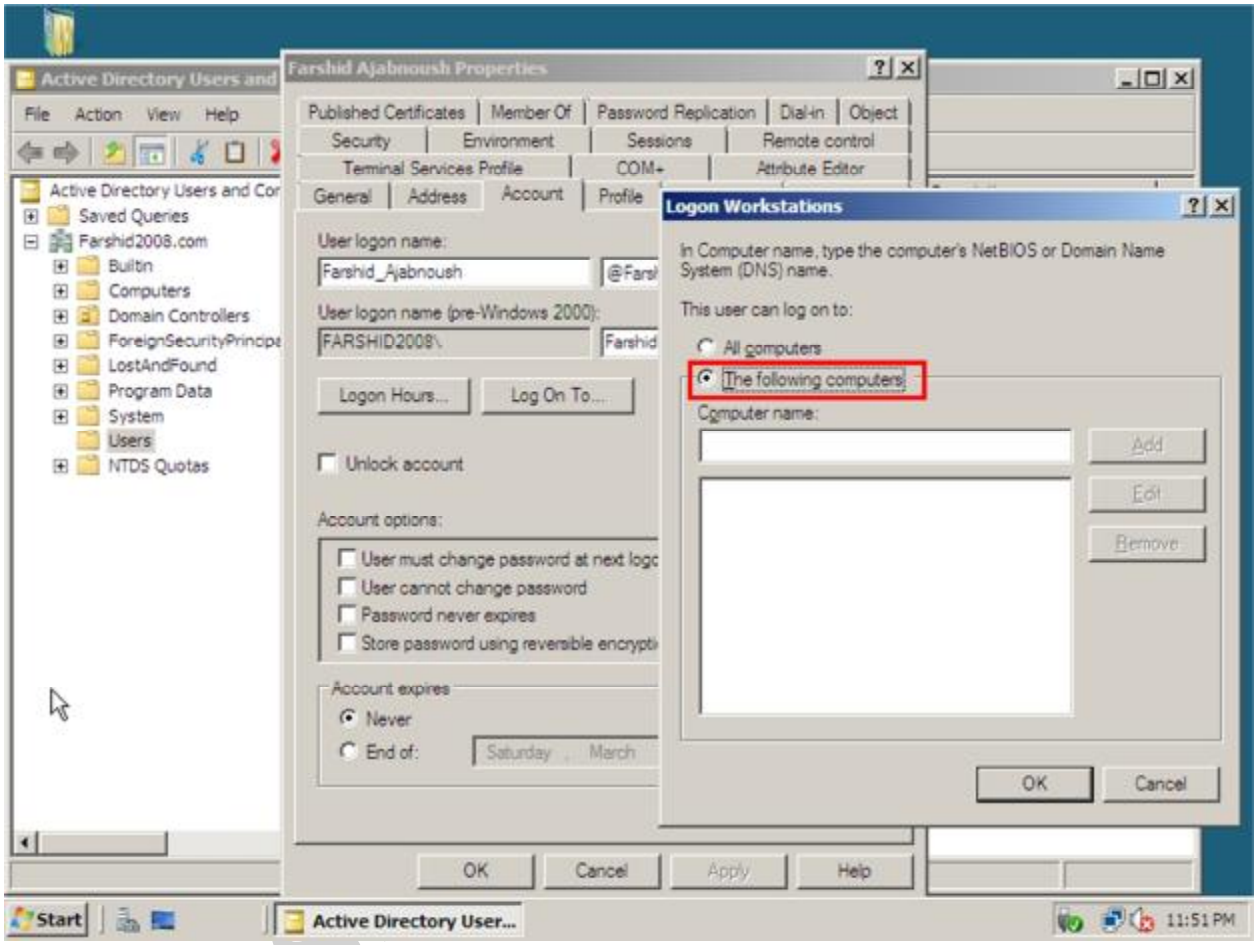

Active Directory Users and
File Action View Help
Active Directory Users and Cor
Saved Queries
Farshid2008.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipa
LostAndFound
Program Data
System
Users
NTDS Quotas
Farshid Ajabnoush Properties
Published Certificates | Member Of | Password Replication | Dial-in | Object
Security | Environment | Sessions | Remote control
Terminal Services Profile | COM+ | Attribute Editor
General | Address | Account | Profile | Telephones | Organization
User logon name:
Farshid_Ajabnoush
@Farshid2008.com
User logon name (pre-Windows 2000):
FARSHID2008\
Farshid_Ajabnoush
Logon Hours...
Log On To...
Logon Hours for Farshid Ajabnoush
12 2 4 6 8 10 12 2 4 6 8 10 12
All
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
OK
Cancel
Logon Permitted
Logon Denied
Sunday through Saturday from 12:00 AM to 12:00 AM
Description
Built-in account for admini...
Members in this group can...
Members of this group are...
Members in this group can...
DNS Administrators Group
DNS clients who are permi...
Designated administrators...
Start
Active Directory User...
11:01 AM

Fars

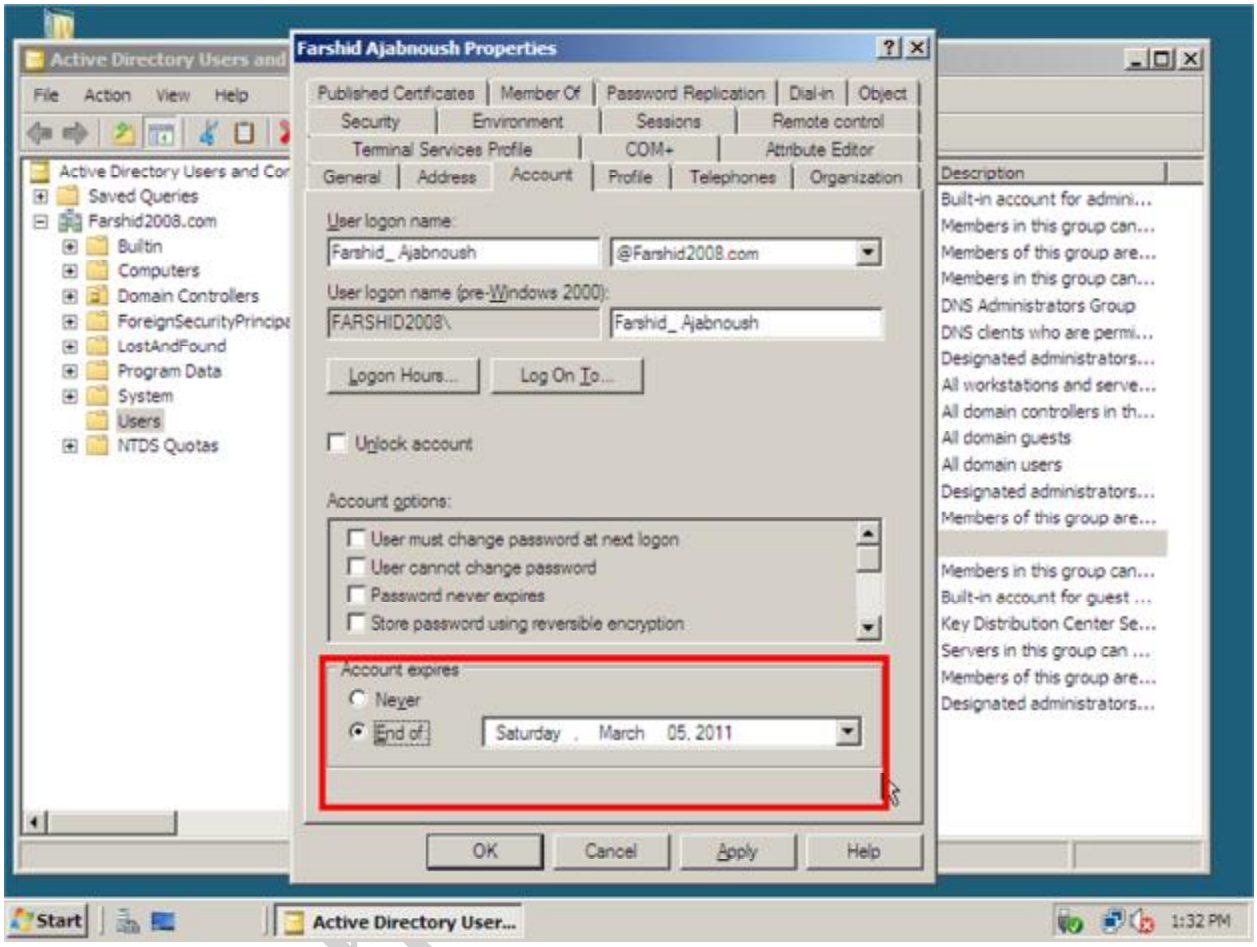
با گزینه LogonTo می توانیم بگوییم هر کاربر از کدام کامپیوتر ها یا کامپیوتر بتواند وارد شود.



سپس در قسمت Computer name اسم کامپیوتر یا کامپیوتر ها را می نویسیم و Add را می زنیم.




Fars




**گزینه Account Expires اگر فعال کنیم می توانیم بگوییم که این یوزر در 1 سال بعدیا 2 سال بعد که قراردادش تمام می شود یوزرش هم Expireشود.**

Farsh

ساختن User با کامند:

یکی از مواقعی که باید یوزر را توسط کامند ساخت زمانی است که Admin شبکه دسترسی مستقیم به سرور نداشته باشد و از سیستم دیگری به سرور وصل شود،وقتی به سرور وصل شدیم برای ساختن یوزر از دستور زیر استفاده می کنیم

Dsadd user cn=reza,cn=users,dc=farshid2008,dc=com -pwd @$df2262343 -disabled no -u Administrator -p .....

Dsadduser: برای اضافه کردن یوزر است می توانیم برای اضافه کردن گروپ از دستور Dsadd group استفاده کنیم.

cn=reza : اسم یوزرمان است.

cn=users: اسم پوشه ای که یوزر reza در آن ساخته می شود است.

dc=farshid2008,dc=com: اسم دامینمان می باشد.

-pwd @$df2262343: پسورد یوزر reza می باشد.

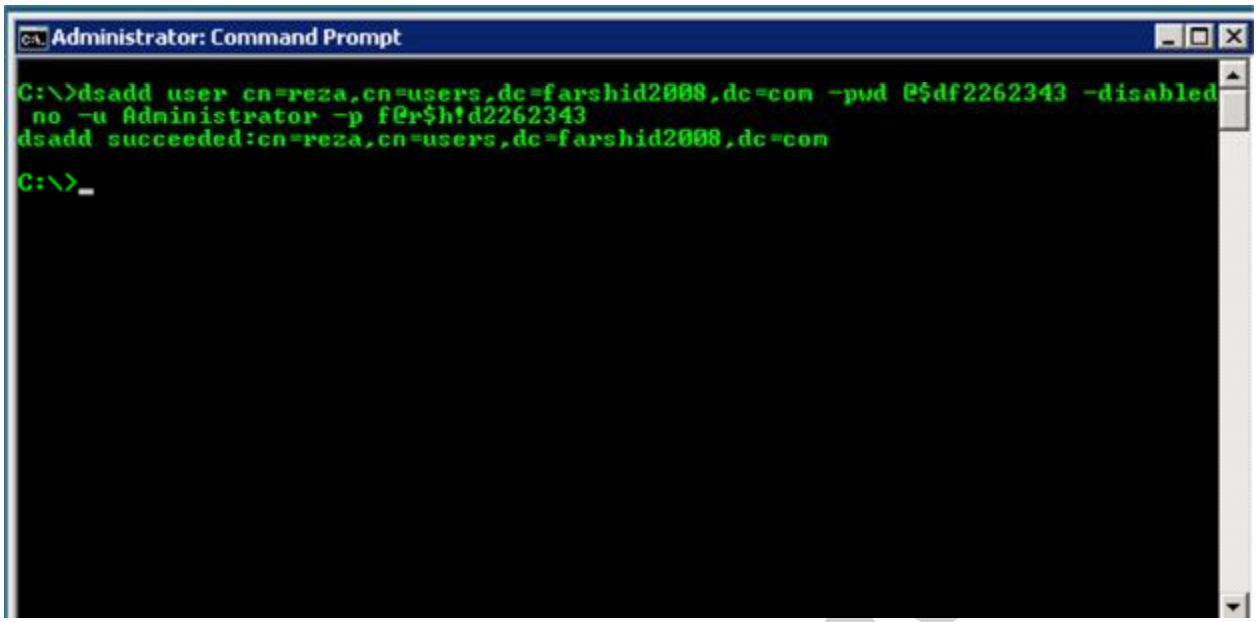
-disabled no: یعنی بتواند با یوزر reza وارد شبکه شود، اگر Yes باشد فقط می تواند ازقابلیت Runas این یوزر استفاده کند.

-u Administrator: اسم یوزر ادمین شبکه می باشد.

-p: پسورد ادمین شبکه را باید جلویش بنویسیم.

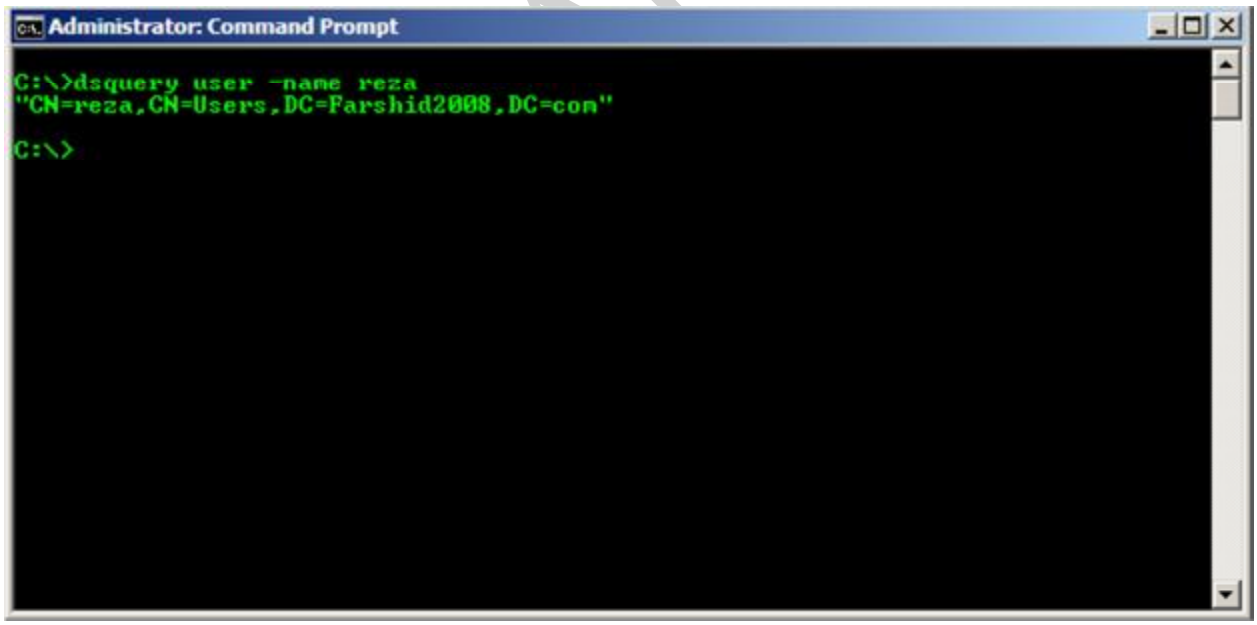
- اگر از روی خود سرور یوزر را ساختیم احتیاجی به یوزر نیم و پسورد ادمین نداریم (2 موضوع آخر)

FarshidAjabnoush




و طبق شکل یوزر با موفقیت اضافه شد.

حالا برای اینکه مطمئن شویم یوزری را که ساختیم اضافه شده است از دستور dsquery user -name reza استفاده می کنیم



یک سری از کامندهای مهم:

Dsadd : برای اضافه کردن

Dsrm : برای پاک کردن

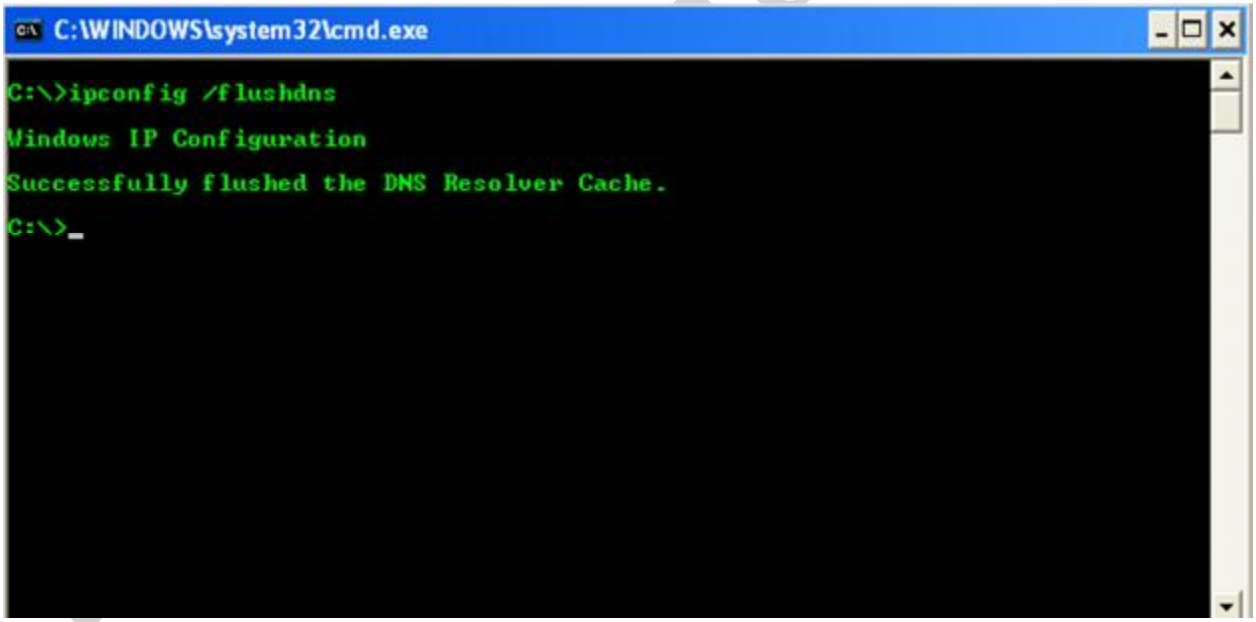
Dsmove : برای انتقال دادن

Dsquery : برای جستجو کردن

Dsmod : برای تغییر دادن

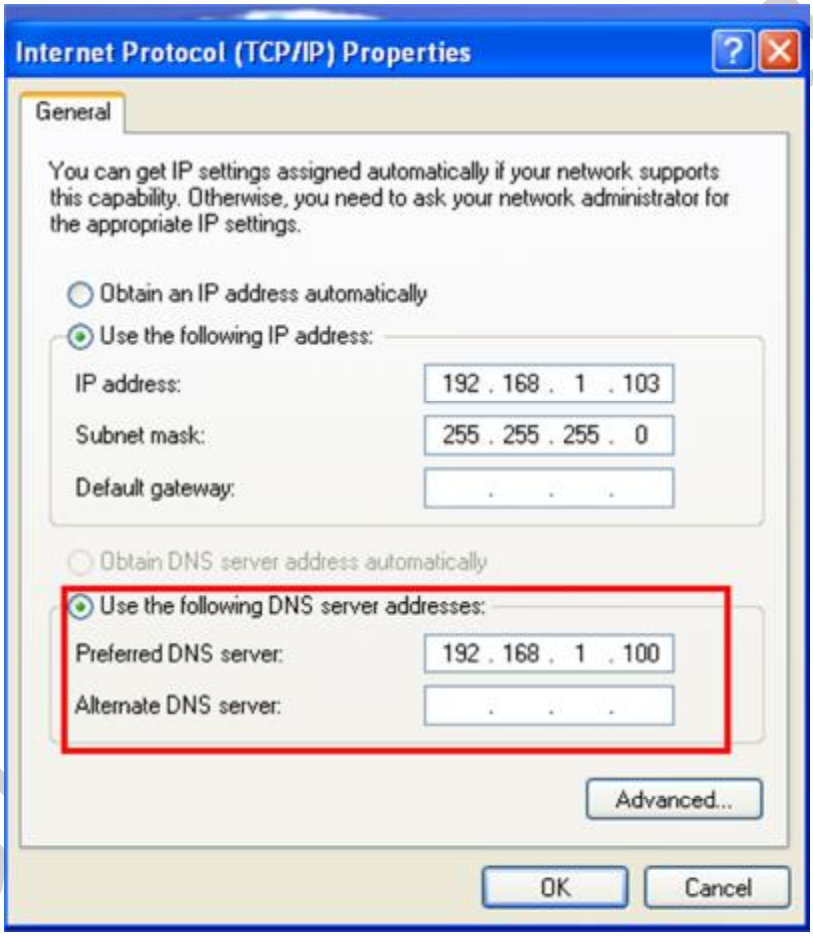
Dsget : برای نشان دادن مشخصات

- برای پاک کردن Cach DNS از دستور ipconfig /flushdns استفاده می کنیم



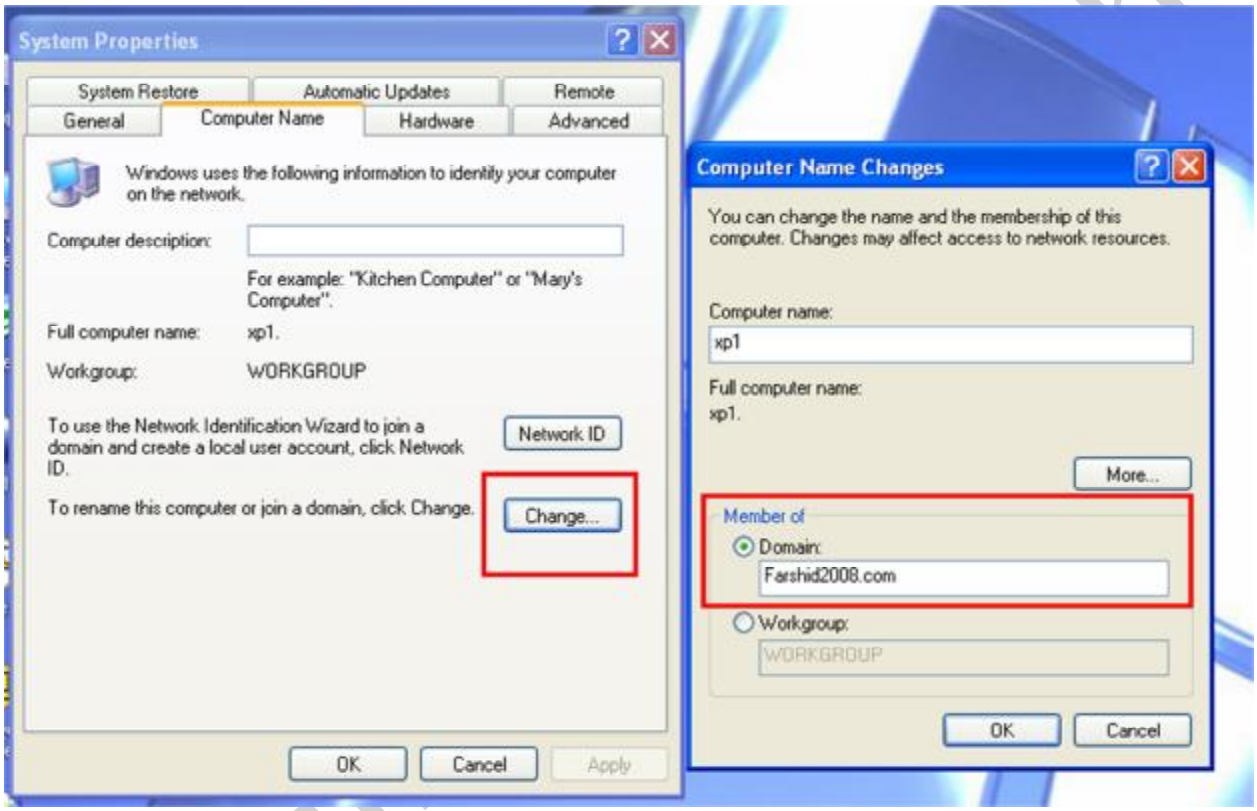
: Join

زمانی که بخواهیم کامپیوتری را به دامین اتصال(Join ) دهیم اولین کاری که انجام می دهیم این است که حتماً باید ipسرور را به عنوان DNS آن کامپیوتر قرار دهیم ( در اینجا ip دامین ما 192.168.1.100 می باشد)و بر روی کارت شبکه Ip تنظیم شود.



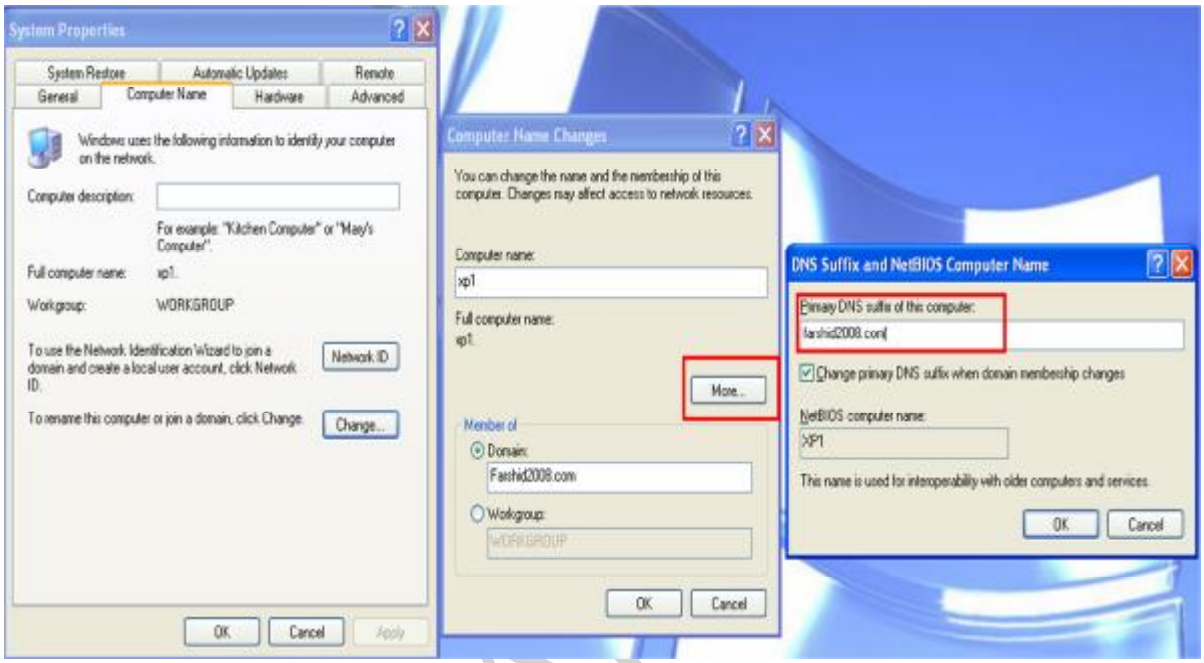

Fa ush

**دومین کاری که باید انجام بدهیم وارد کردن اسم دامینمان است**




Farsh

سومین کار زدن دکمه More و وارد کردن دوباره اسم دامین، با انجام این کار ما می گوییم برو بصورت اتو ماتیک اسم خودت را در DNS ثبت کن تا از این به بعد با اسم در تماس باشیم .




وقتی که ok کنیم پنجره زیر باز می شود که از ما یوزر و پسورد می خواهد بهتر است با یوزر وپسورد ادمین Join نشویم، به این دلیل که دیگر ممکن است پالیسی بر روی آن کامپیوتر اعمال نشود چون با Admin اتصال پیدا کرده با یوزر و پسوردی که برای این کامپیوتر قبلاً ساخته ایم Join شویم،حتی می توانیم با User خود کاربر این کار را انجام دهیم.

FarshidAj

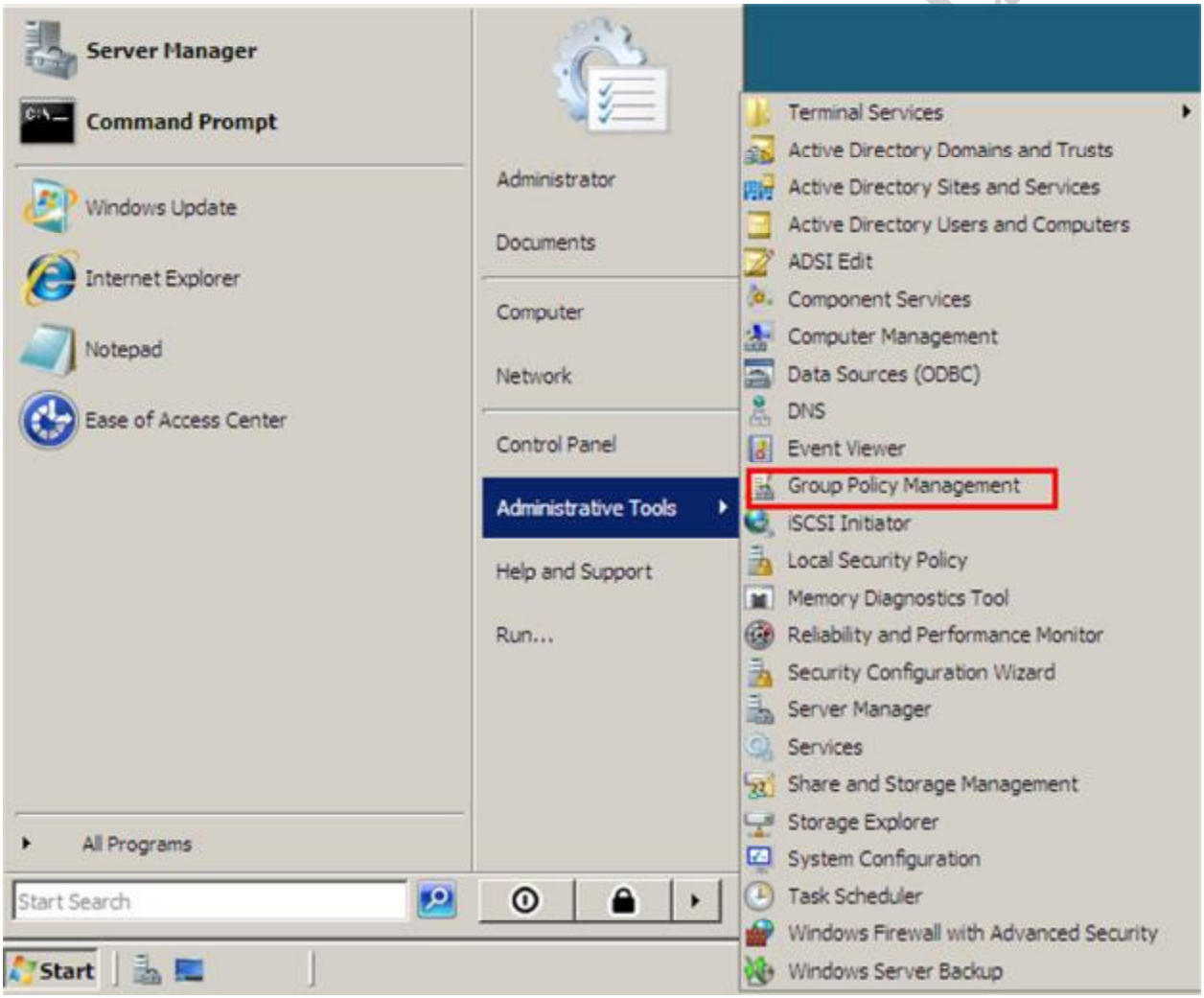
و در آخر به ما خوش آمد می گوید و حتماً باید سیستم ریستارت شود.

- هر یوزری می تواند 10 کامپیوتر یا 10 بار 1 کامپیوتر را به دامین Join کند.
- اگر کامپیوتری با ادمین Join شد و پالیسی بر روی آن اعمال نشد بهتر است یک OU ساخته و اسم کامپیوتر را به همراه User مورد نظر داخل OU قراردهیم و به آن OU پالیسی اعمال کنیم.

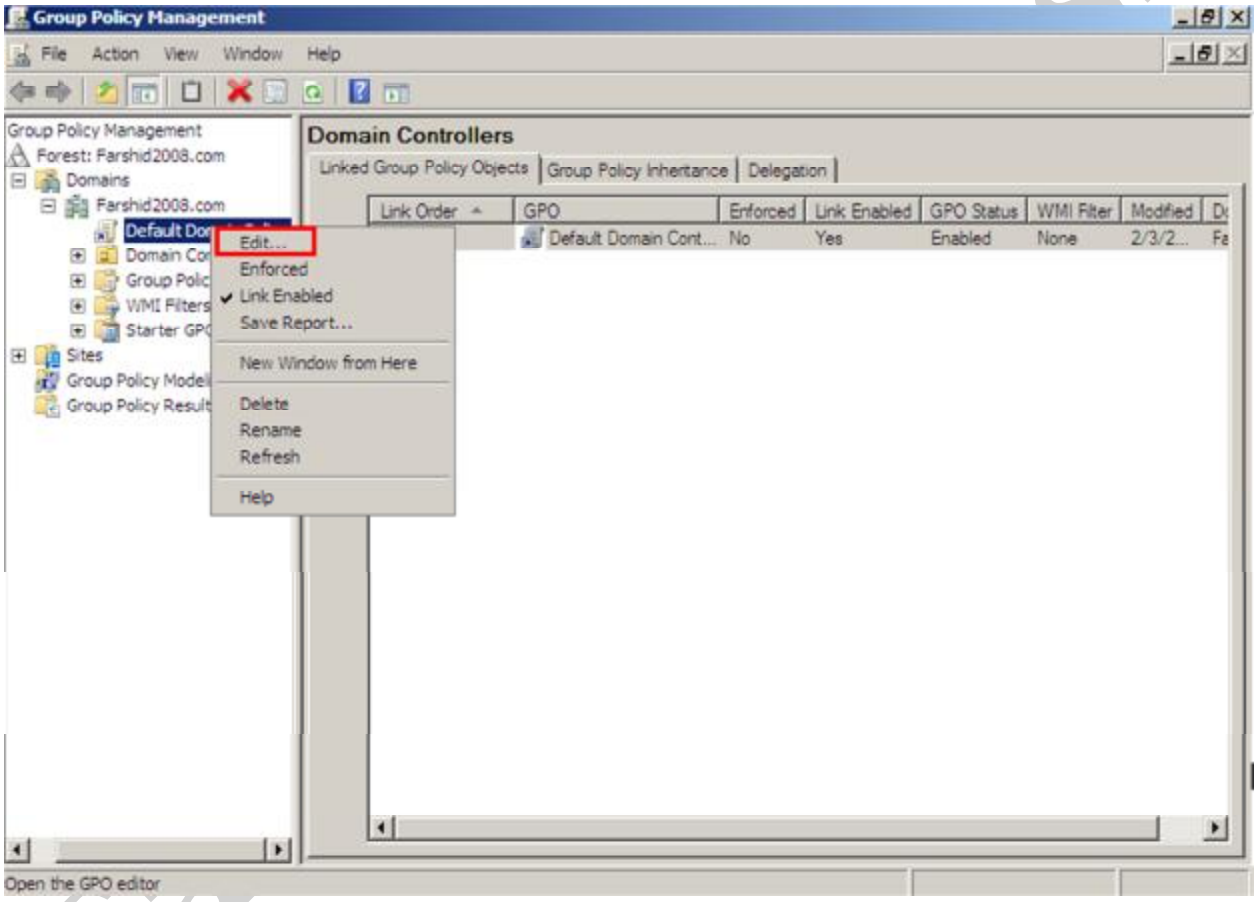
FarshidAjaboush

**تنظیم کردن یک عکس به عنوان Background برای تمامی سیستم های داخل یک شبکه**

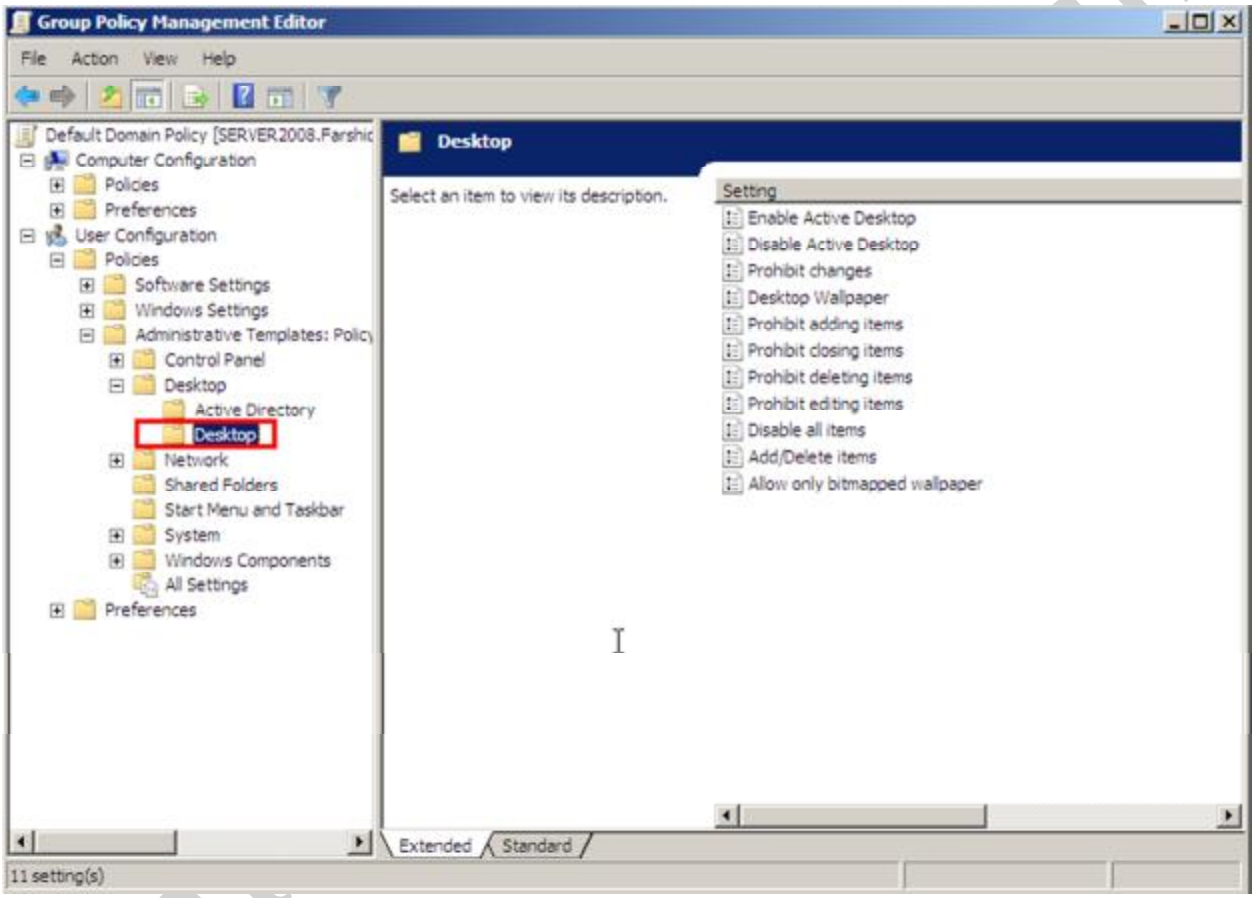
1) ابتدا از Administrative Tools وارد Group Policy می شویم



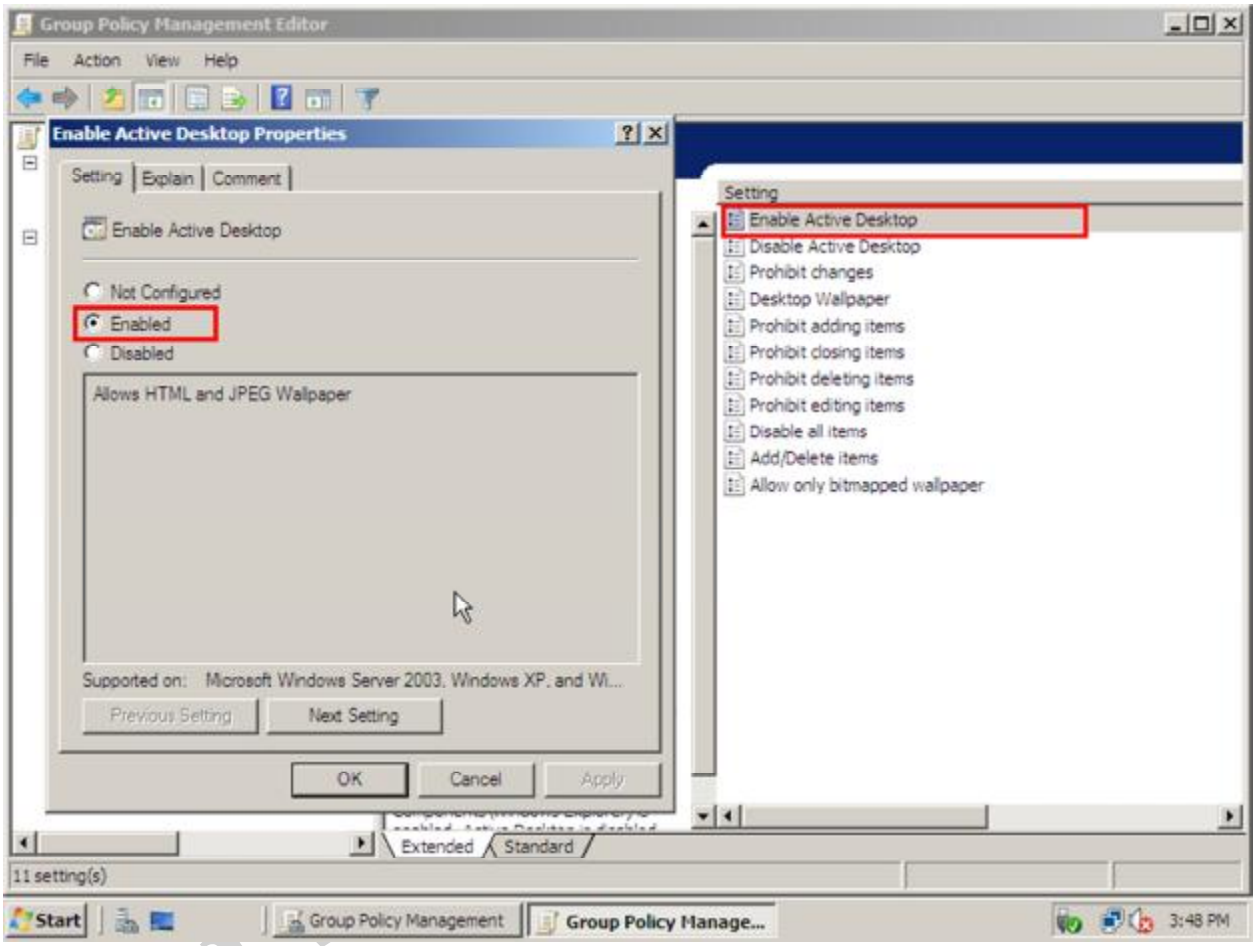
2) کلیک راست وانتخاب Edit



3) از مسیر Desktop User Configuration – Policies - Administrative Templates - وارد پوشه Desktop می شویم.

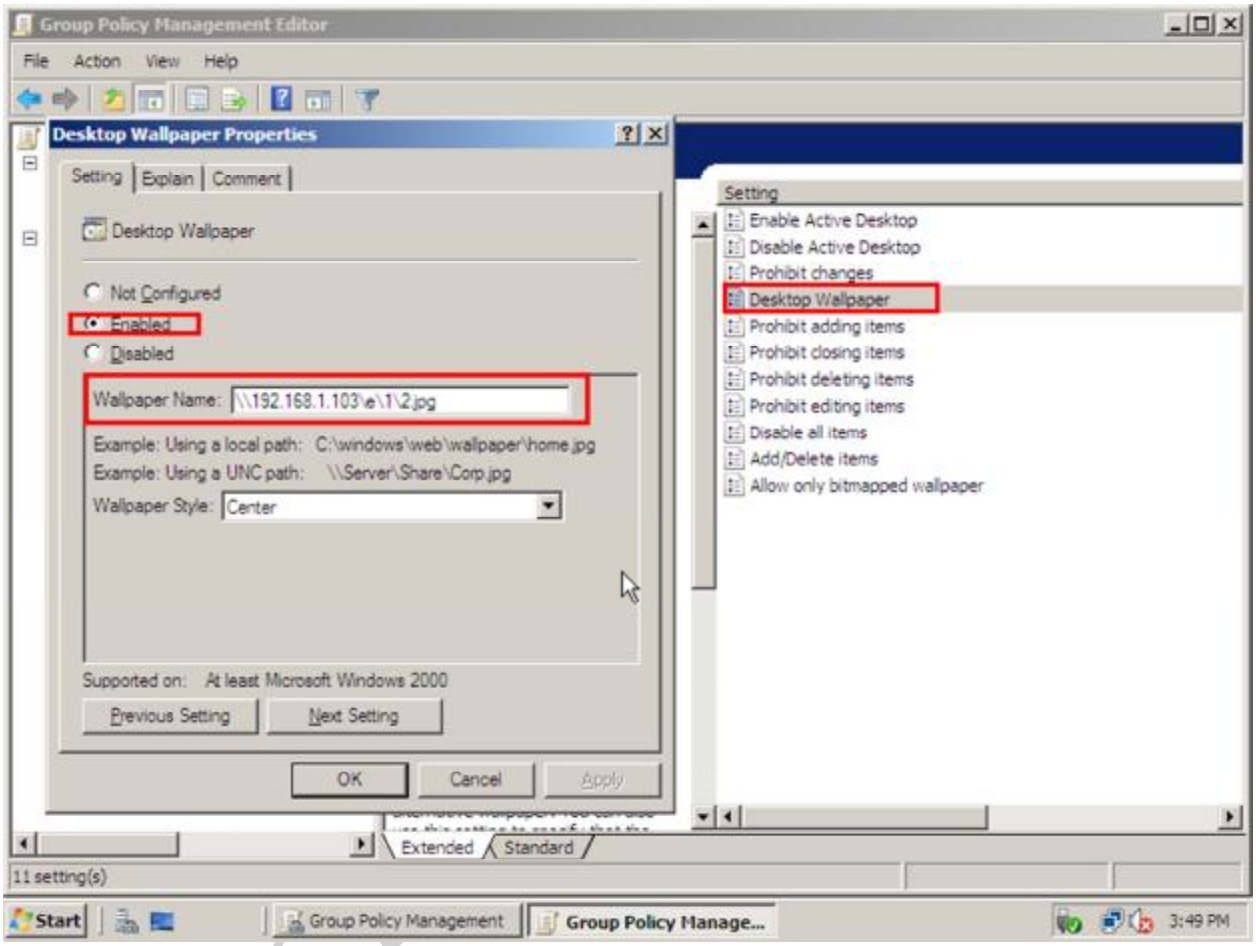


4) در صفحه سمت راست بر روی عبارت Enable Active Desktop کلیک کرده و در صفحه باز شده گزینه Enable را انتخاب می کنیم و بر روی Ok کلیک می کنیم.




Fa

5) دوباره از صفحه سمت راست بر روی عبارت Desktop Wallpaper کلیک کرده و از صفحه باز شده گزینه Enable را انتخاب می کنیم و در قسمت Wallpaper Name مسیر عکس مورد نظرمان را وارد می کنیم.




در آخر هم برای اعمال Policy داده شده دستور Gpupdate /Force را هم در CMD اجرا می کنیم و یک بار سیستم ها را ریستارت می کنیم.

Farsi

دومین Object،Group :

گروه ها در اکتیو دایرکتوری به دو نوع تقسیم می شوند: 1- Type (از لحاظ نوعشون) 2- Scope ( ناحیه،منطقه پوشش دهیشون)

Type

به دو گروه Security وDestribution تقسیم می شوند.

گروه هایی که از نوع Security هستند فقط بدرد Permision (اجازه دسترسی) دادن می خورند.

گروه هایی که از نوع Destribution فقط بدرد ارسال دسته جمعی ایمیل می خورند.

- 99% گروه هایی که ما خواهیم ساخت از نوعSecurityمی باشند.
- کاربرد Destribution در شبکه هایی می باشد که در آنجا ایمیل سرورExchange) ( داشته باشند.
- تمامی شماره مو بایل های ما در سرور مخابرات عضو گروه Destribution است که ما می توانیم sms تبلیغاتی در یافت کنیم.

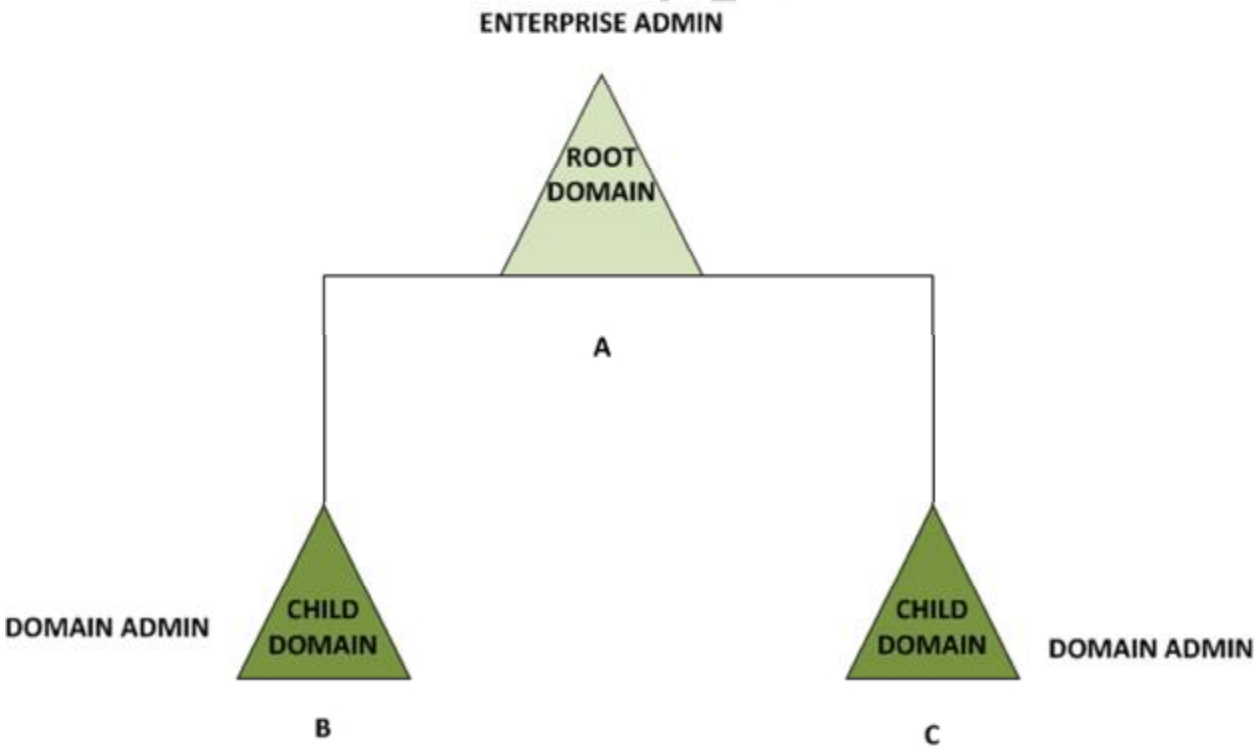
Scope

به سه نوع تقسیم می شوند:1-Universal 2-Domail Local 3- Global

FarshidAjabnoush

در دامین A که Root Domain ما می باشد گروهی از نوع Universal می سازیم،این گروه علاوه بر دامین A می تواند از دامین های B وC عضو بگیرد و هم می تواند به کامپیوتر های این دامین ها Permision (اجازه دسترسی) بدهد. (این گروه هم در دامین خودش اعتبار دارد و هم در بقیه دامین ها، هم از دامین خودش می تواند عضو بگیرد و هم از بقیه دامین ها )

- فقط Admin Enterpriseباید عضو این گروه باشد(این گروه را بسازد).
- به Admin ،Admin Enterprise, Root Domainگویند.
- به Admin، بقیه دامین ها Domain Admin گویند.



Domain Local

**این گروه را می توان در هر دامینی ایجاد کرد، به عنوان مثال ما این گروه را در دامین C ایجاد می کنیم ، این گروه فقط می تواند به کامپیوتر های دامین خودش( C ) Permisionبدهد ولی می تواند از بقیه دامین ها عضو بگیرد.**

**این گروه فقط در دامین خودش اعتبار دارد ولی از بقیه دامین ها هم می تواند عضو بگیرد.**

Global

**این گروه فقط می تواند از دامین خودش عضو بگیرد و به کامپیوتر های دامین خودش Permision بدهد.**

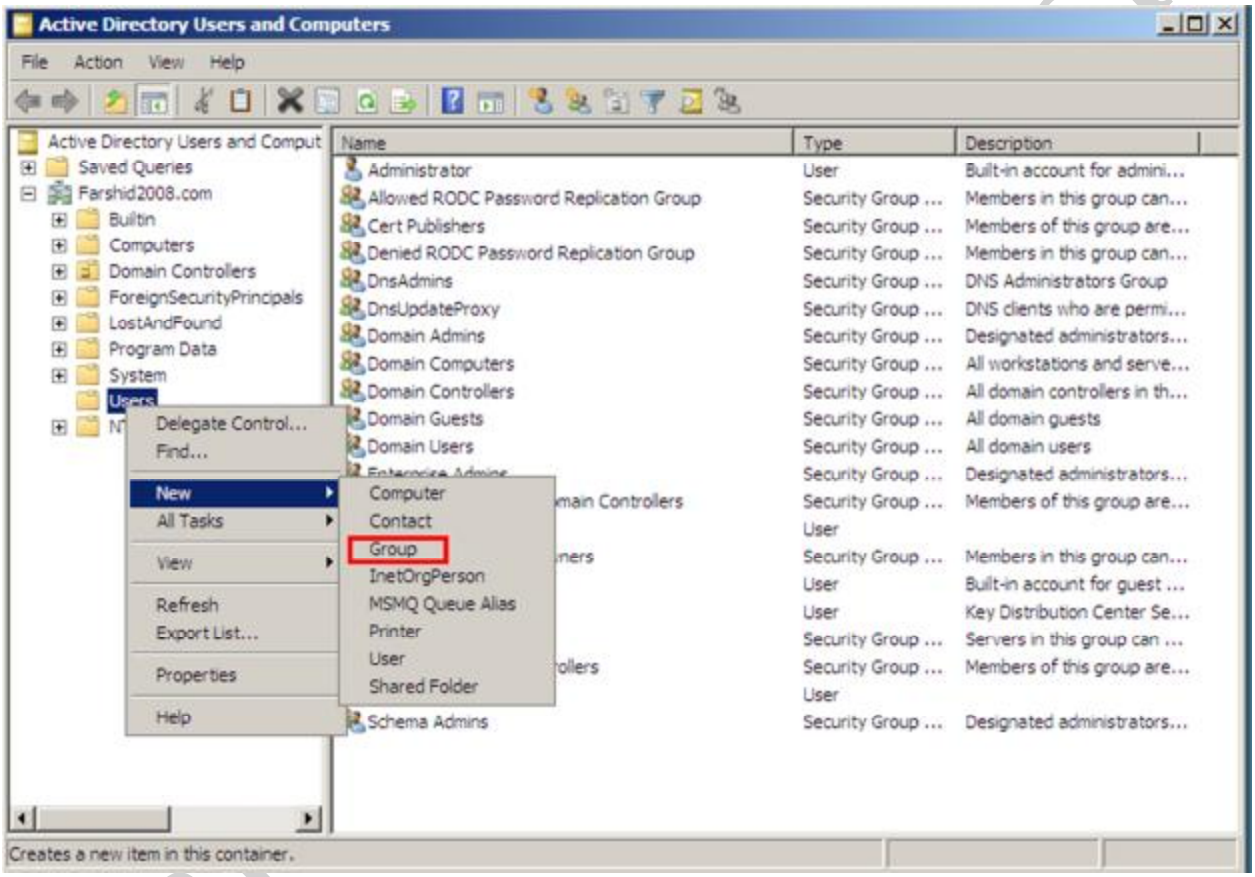
**این گروه فقط در دامین خودش اعتبار دارد .**

- Scope Global فقط در مکان هایی کاربرد دارد که 1 دامین دارند.
- در مکان هایی که دارای یک دامین می باشند زمانی که گروهی را می سازیم به طور پیش فرض Type آن از نوع Security و Scope آن از نوع Global می باشد.

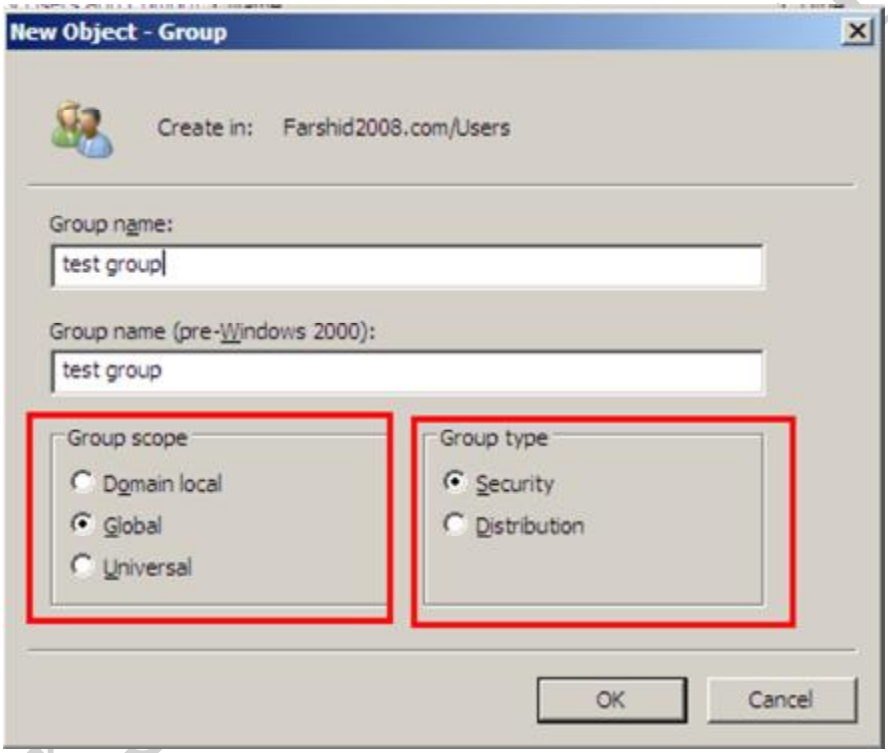
FarshidAjabnoush

## ساختن Group

برای ساختن یک گروه ابتدا وارد کنسول اکتیو دایرکتوری می شویم سپس در پوشه Users (این پوشه انتخابی است) کلیک راست کرده و گزینه New Group را انتخاب می کنیم.

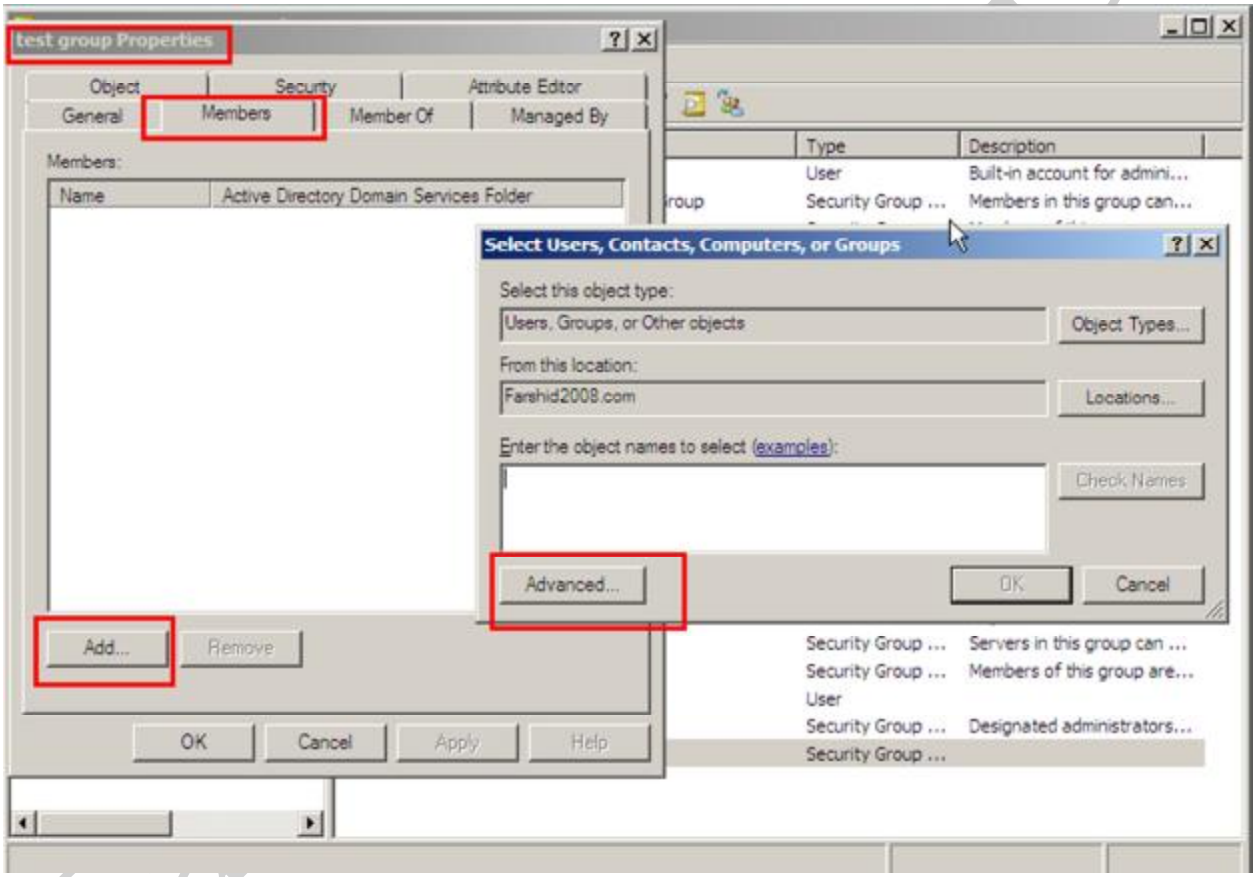


سپس در پنجره باز شده اسم گروه را وارد می کنیم ، همانطور که گفتیم به صورت پیش فرض Scope وType به صورت زیر تنظیم می باشد.

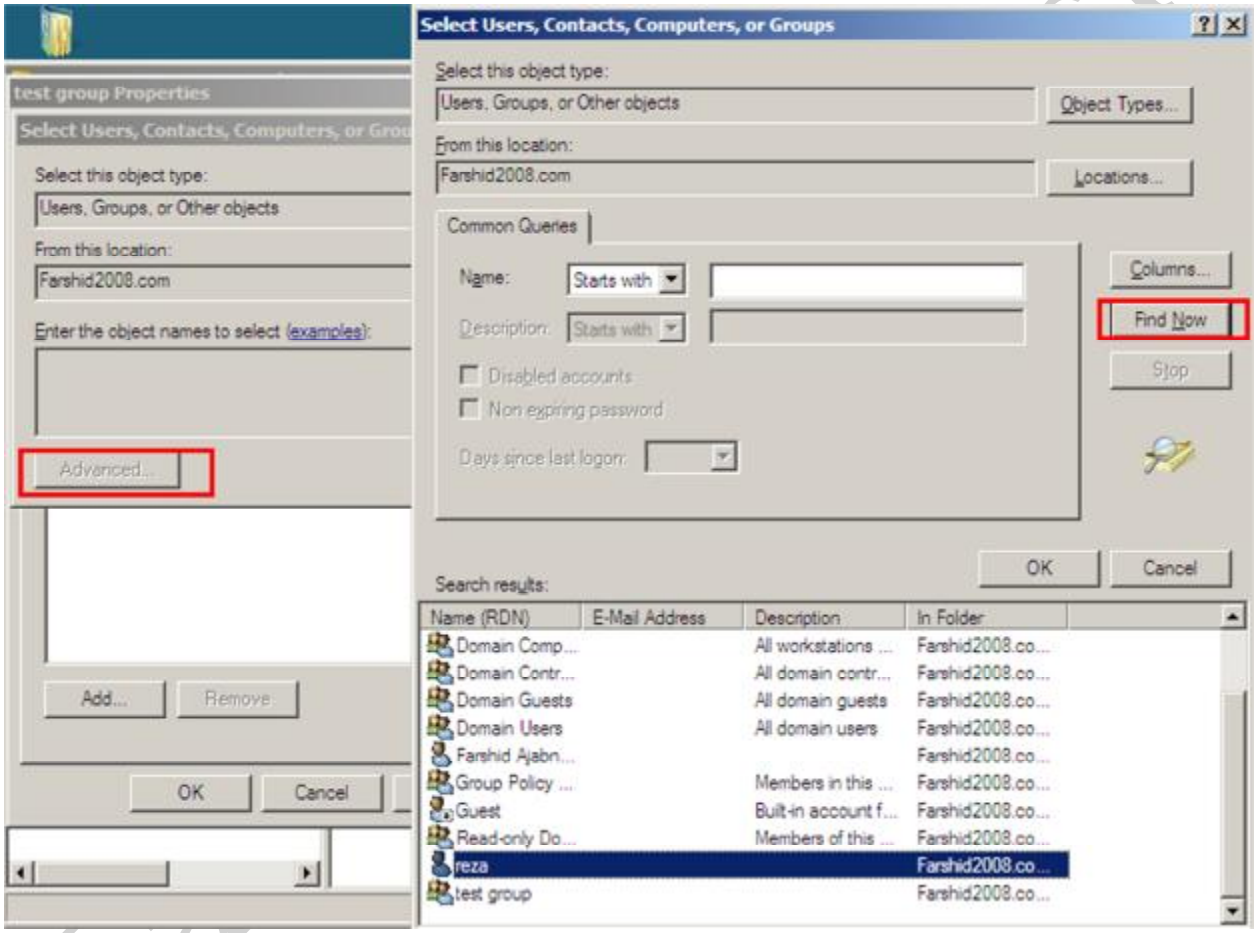



Farshid

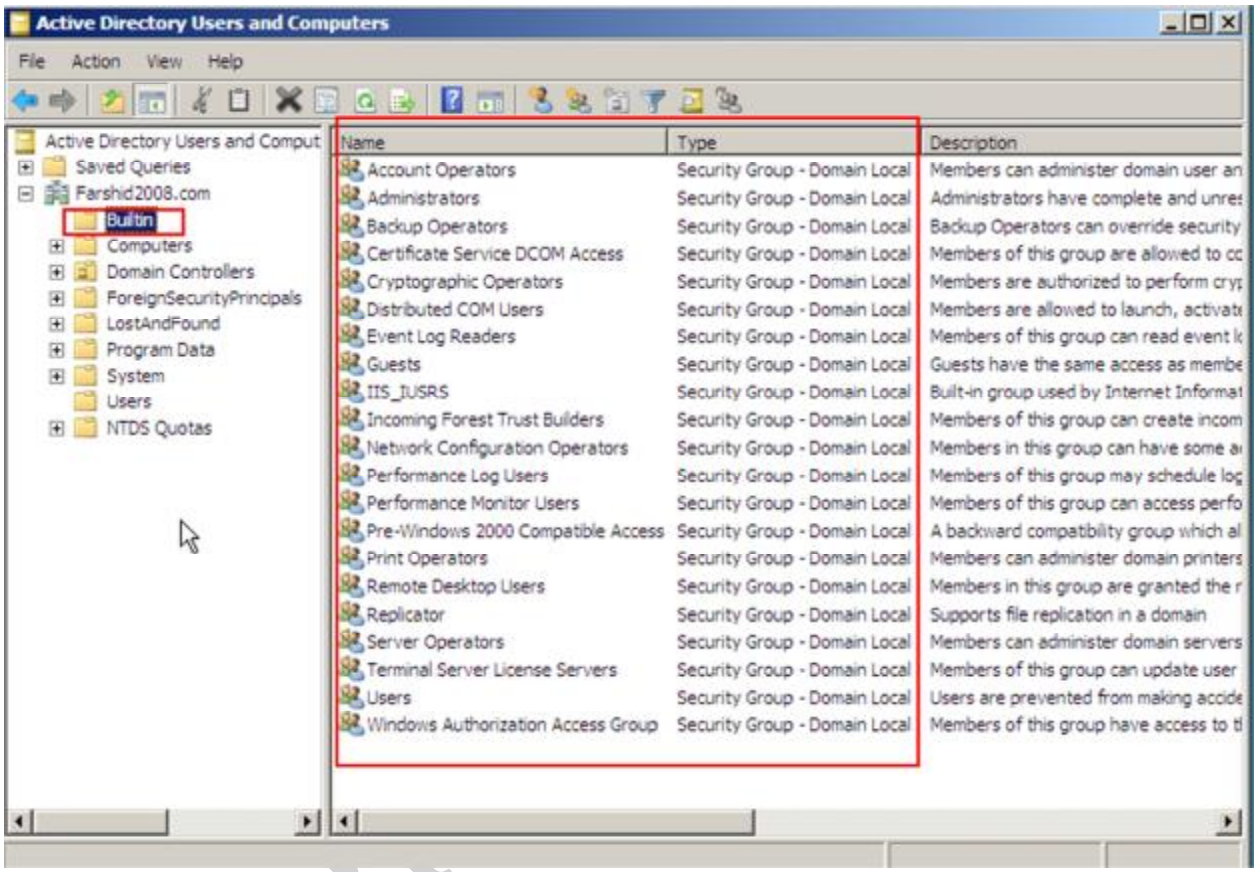
زمانی که گروه ساخته شد، برای اینکه بتوانیم یوزری را به این گروه اضافه کنیم روی گروه کلیک راست کرده و گزینه Properties را می زنیم و از پنجره باز شده به تب Members می رویم دکمه Add را می زنیم و از پنجره باز شده دکمه Advanced را هم می زنیم



بعد از زدن دکمه Advanced از پنجره باز شده دکمه Find Now را می زنیم و از لیست باز شده یوزر مورد نظر را انتخاب می کنیم.



در اکتیو دایرکتوری یک سری گروه های از پیش تعریف شده (Bulting ) وجود دارد.

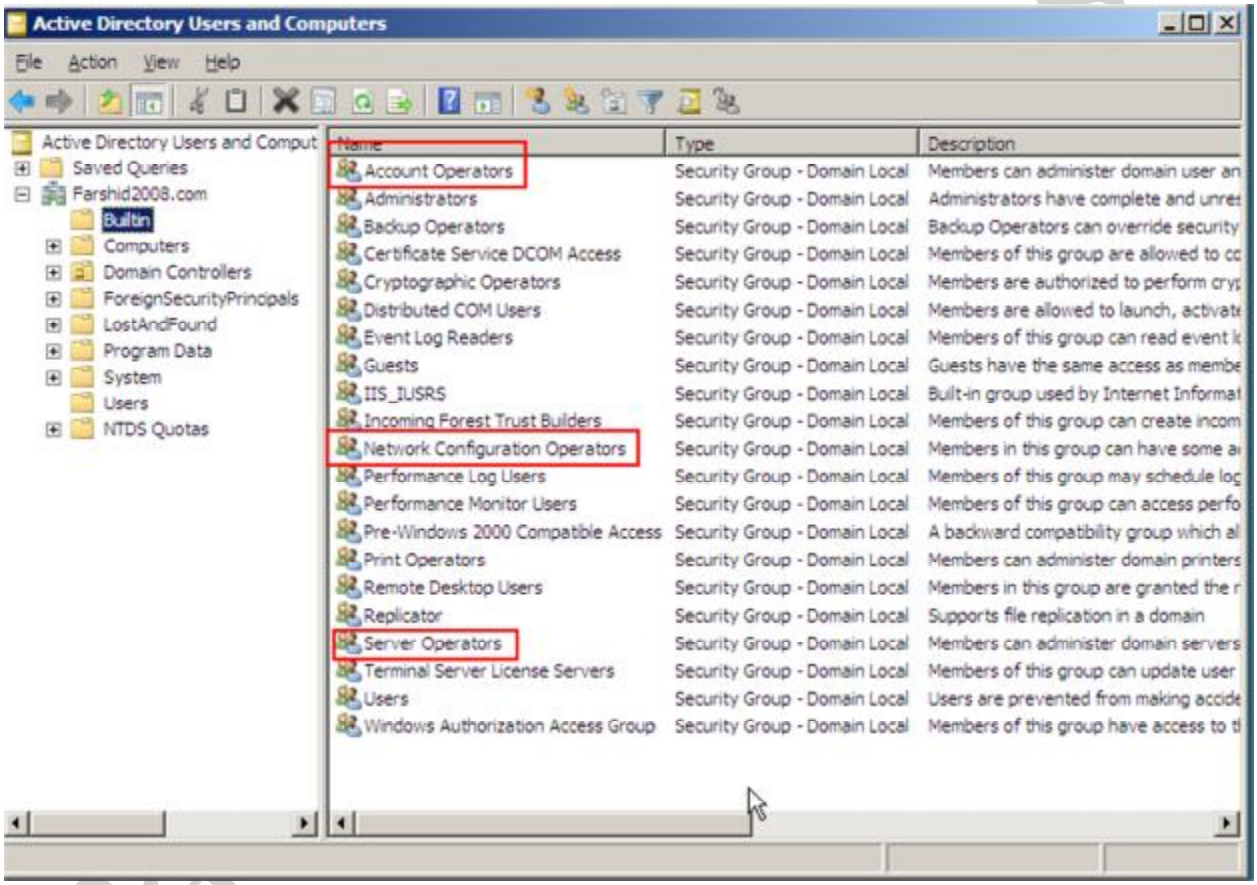



Farsh

Account Operators : اگر یوزری عضو این گروه باشد می تواند تمامی اکانت های موجود در اکتیو دایرکتوری را مدیریت کند.( ساختن، پاک کردن و.....)

Netwok Configuration Operators : اگر یوزری عضو این گروه باشد می تواند تنظیمات شبکه ای یوزرش را تغییر دهد. (عوض کردن ip و ..... )

Server Operators : یوزری که عضو این گروه باشد یک پله پایین تر از Admin می باشد. ( می تواند نرم افزار نصب کند و .....)



ساختن گروه با استفاده از کامند

دستور زیر را در محیط CMD تایپ می کنیم

Dsadd group cn=test,cn=users,dc=farshid2008,dc=com –secgrp yes -scope u

Dsadd group : دستور اضافه کردن گروه

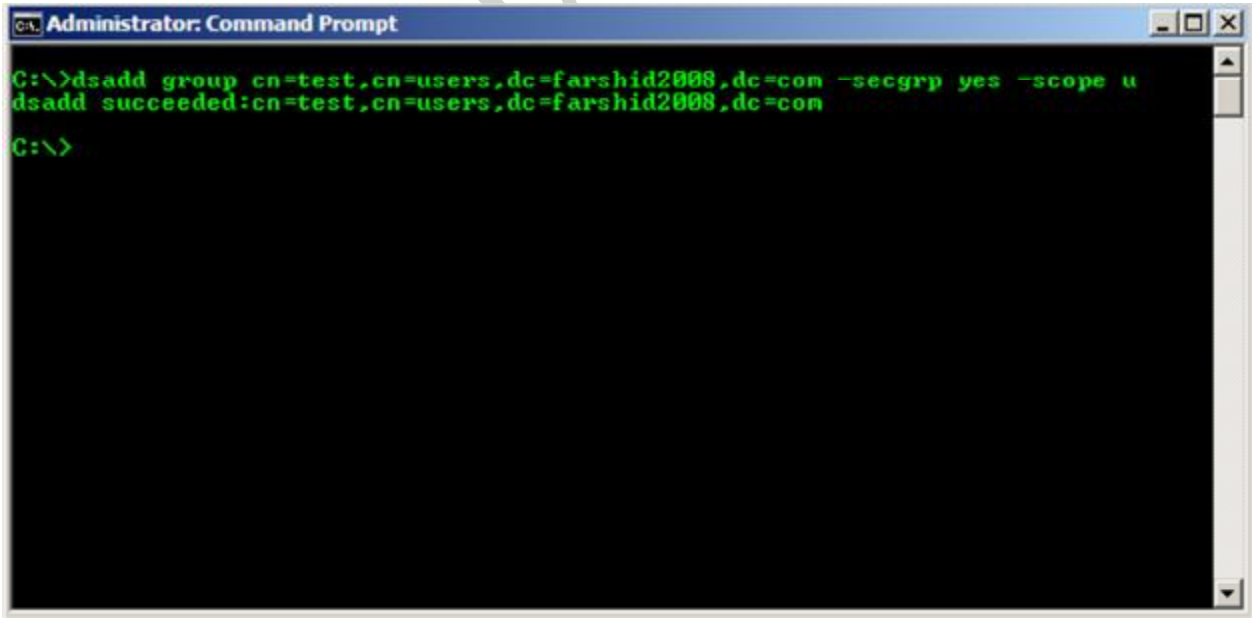
cn=test: اسم گروه Test

cn=users: محل ساخته شدن گروه، در اینجا در پوشه Users می باشد

dc=farshid2008,dc=com : اسم دامین

–secgrp yes: بدین معنی است که Type گروه از نوع Security باشد، اگر No تایپ می کردیم Type گروه از نوع Destribution می شد.

-scope u : نوع Scope گروه را Universal انتخاب کر ده ایم ، برای تغییر می توانیم بجای Uاز DL که مخفف Domain Local و G که مخفف Global می باشد استفاده کنیم .

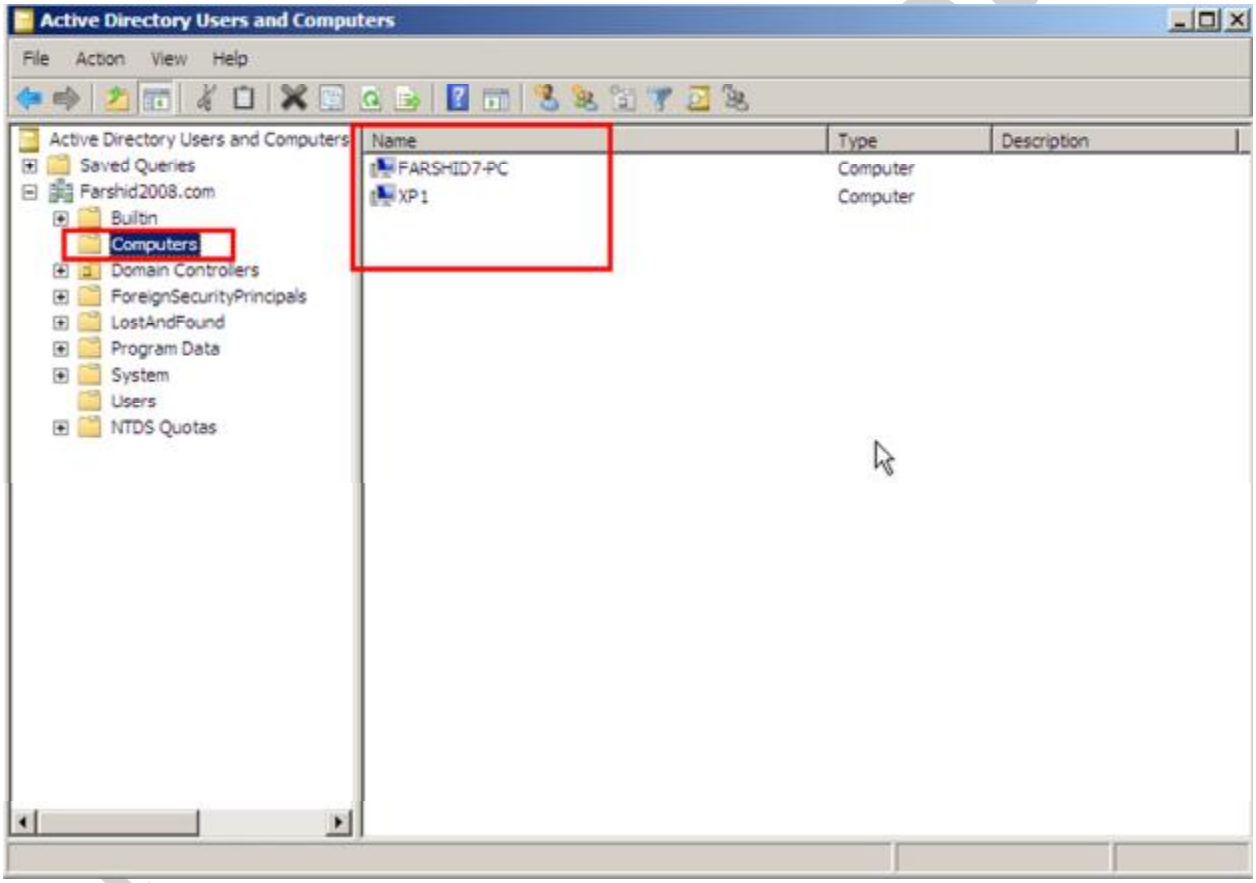



Ajabnoush

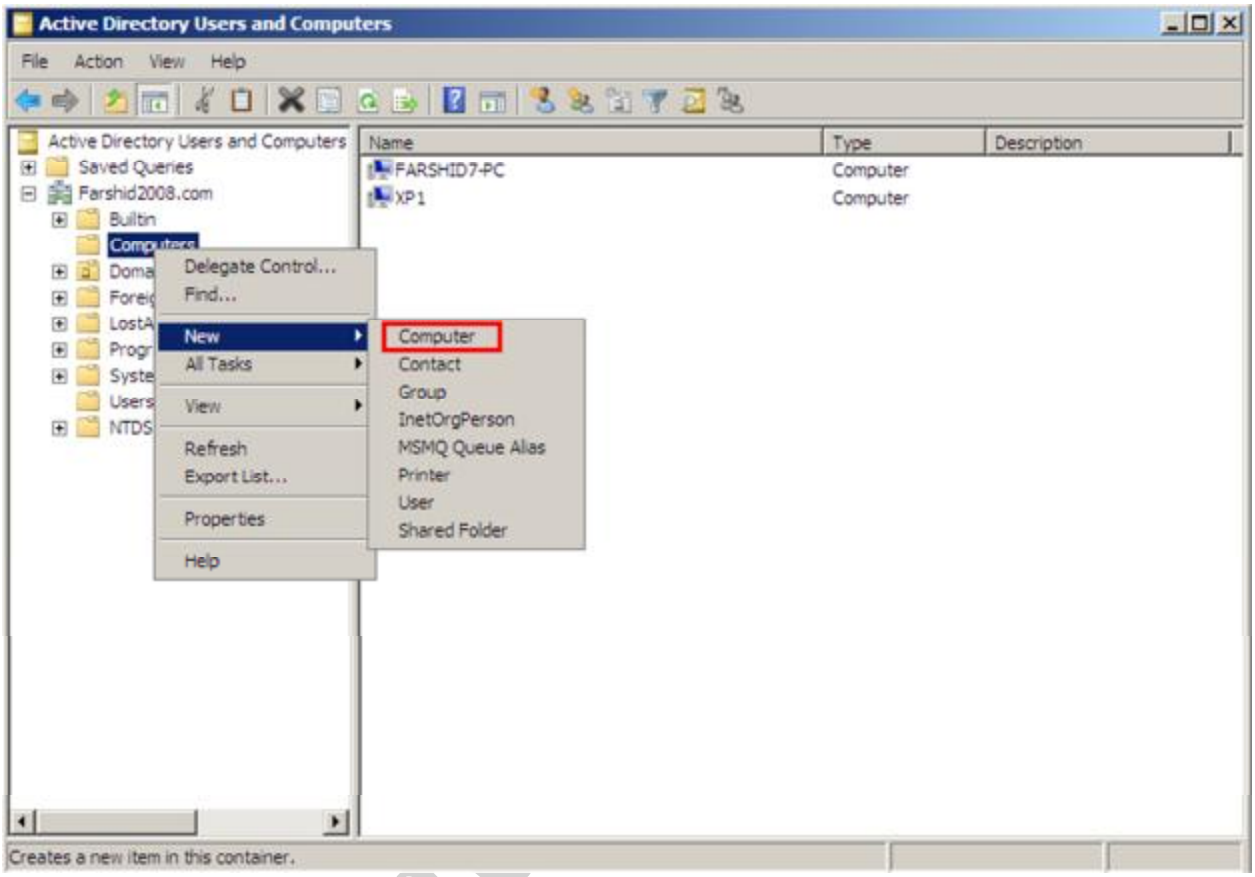
سومین Computer، Object :

تمامی Objectهای کامپیوتر ها در موقع Join به دامین به صورت اتوماتیک درون پوشه ای به نام Computers ایجاد می شوند.(مانند اسم کامپیوتر)

در شکل زیر از پوشه Computers اسامی تمامی کامپیوترهایی که به دامین ما Join شده اند را می بینیم.

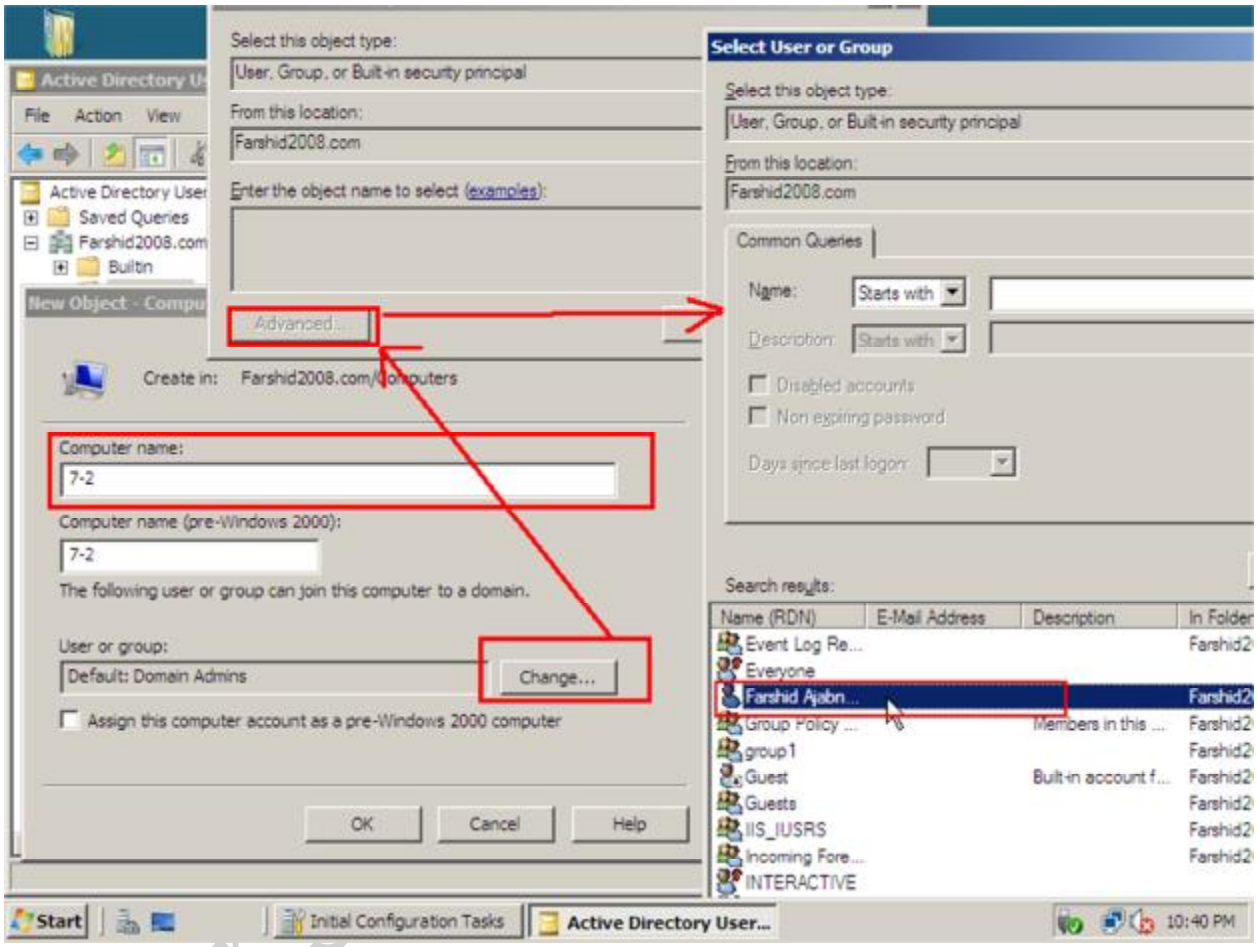


**بصورت دستی هم می توانیم کامپیوتری را اضافه کنیم.**



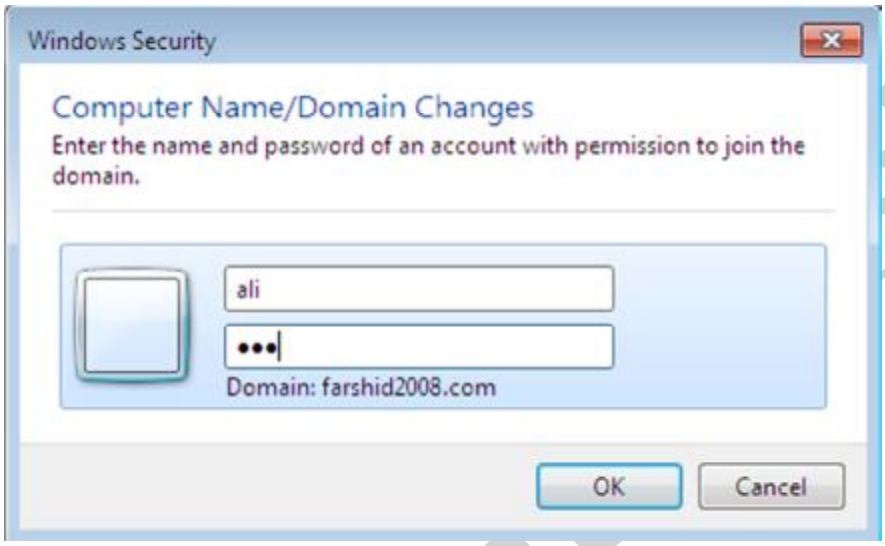

Farshid

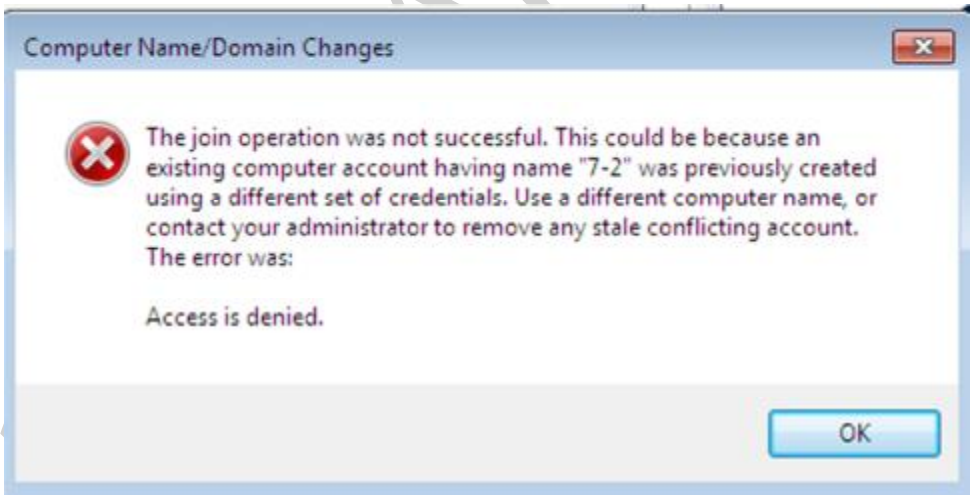
در صفحه باز شده اسم کامپیوتری را که می خواهیم به دامین اتصال دهیم را وارد می کنیم با زدن دکمه Change می توانیم بگوییم که این کامپیوتر با کدام یوزر بتواند Join شود اگر یوزری را انتخاب کنیم ،با یوزر دیگری نمی توانیم کامپیوتر را Join کنیم فقط با همان یوزر امکان پذیر است.




در اینجا ما یوزر Farshid_Ajabnoush را انتخاب کرده ایم.

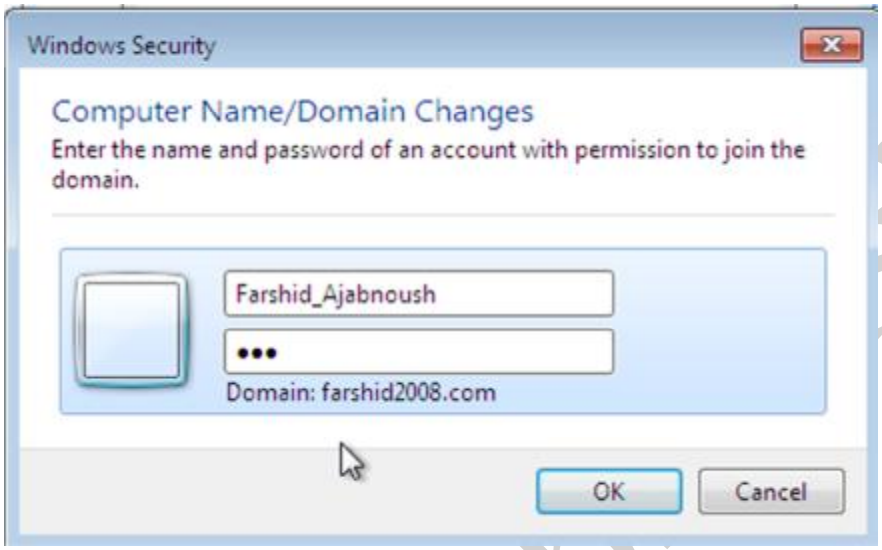
حالا می خواهیم کامپیوتر 7-2 را Join کنیم برای Join کردن یک بار از یوزر Ali استفاده می کنیم تا ببینیم می توانیم با این یوزر Join کنیم؟




همانطور که دیدید کامپیوتر با یوزر Ali به شبکه Join نشد!!

حالا با یوزرFarshid_Ajabnoushامتحان می کنیم.



کامپیوتر Join شد.

Farshid Ajabnoush

چهارمین Object ،OU(Organizatial Unit) :

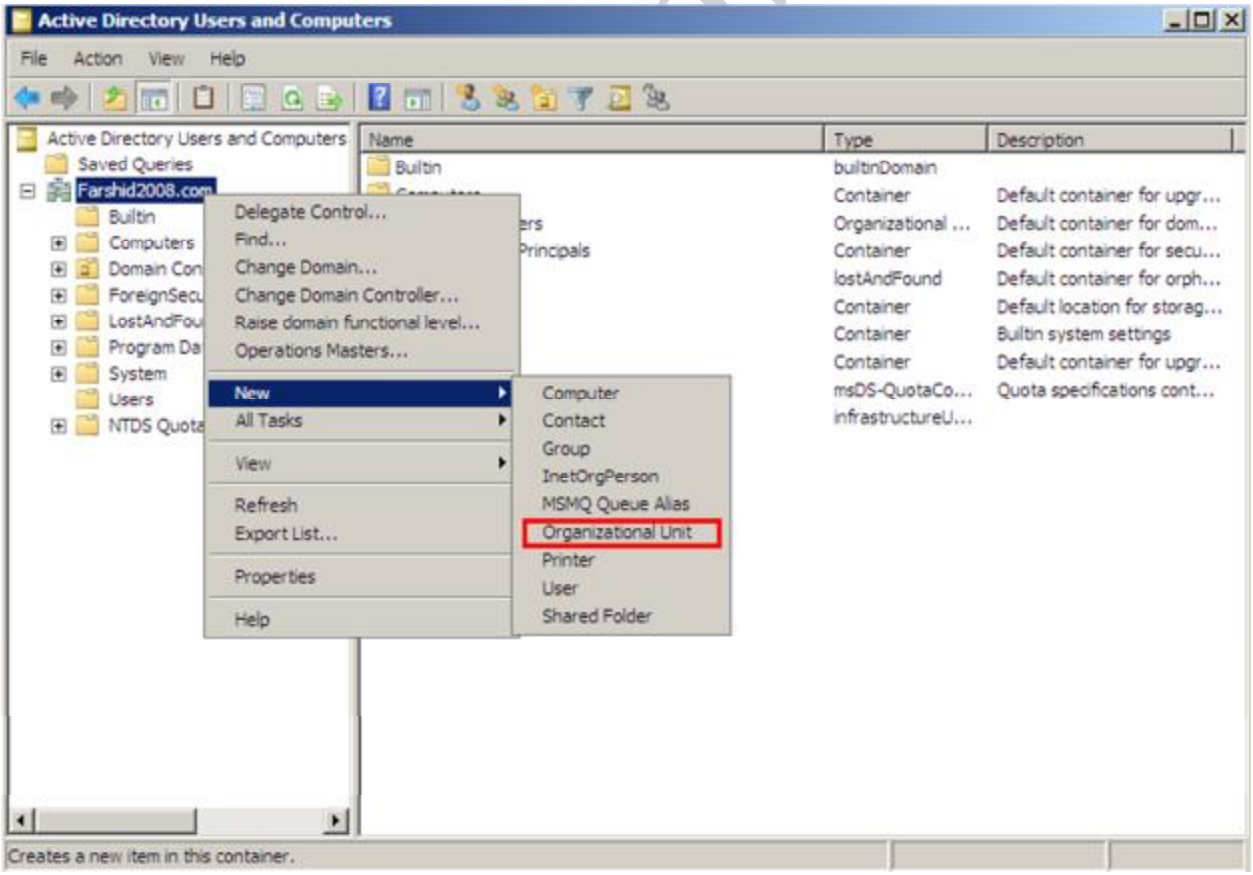
1) OU فقط می تواند در زیرشاخه اسم دامین ساخته شود.
2) OU چیزی شبیه به گروه است برای مدیریتObject ها بکار می رود ولی از گروه فراتر می باشد.

## تعریف OU

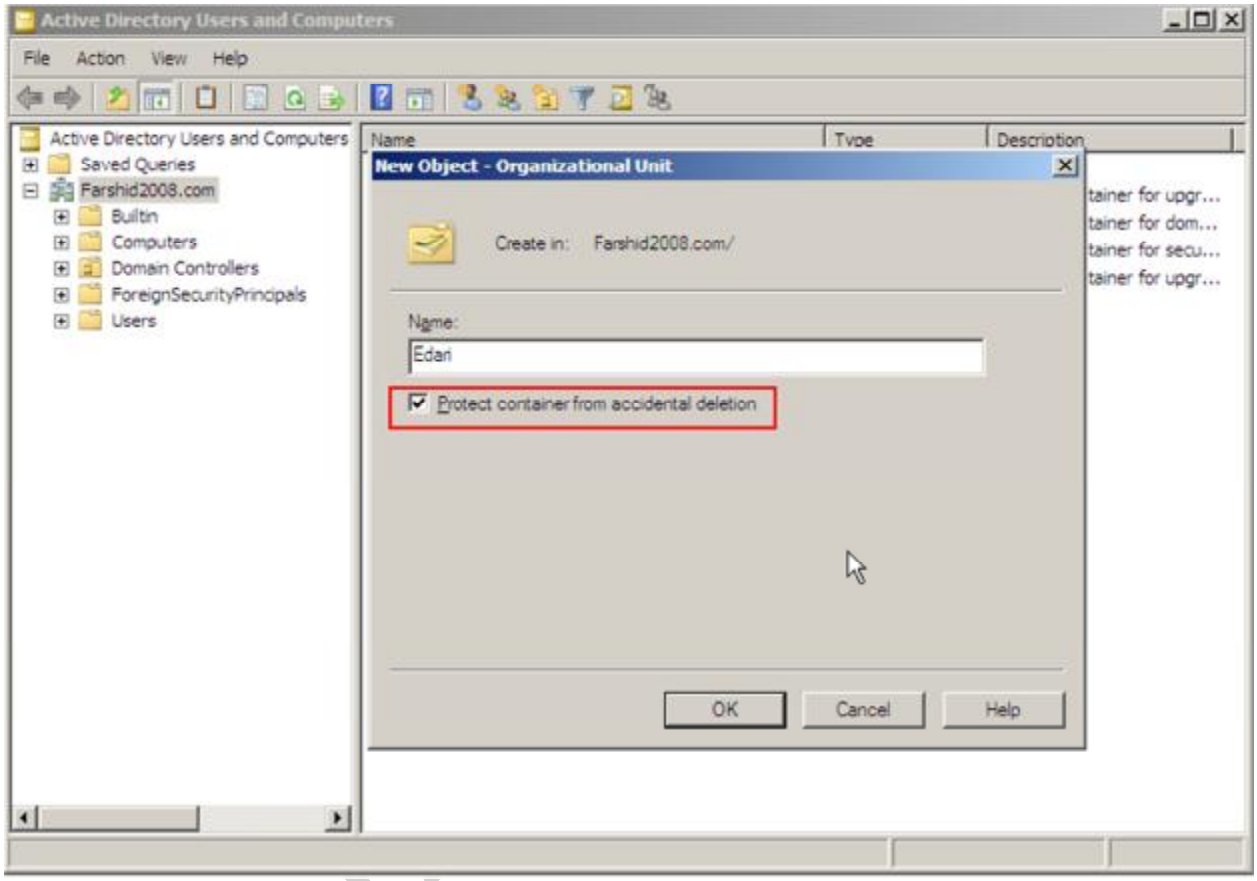
با یک مثال تعریف می کنیم یک ساختمان5 طبقه را در نظر بگیرید در هر طبقه از این ساختمان 10 اتاق داریم، ما کل ساختمان را یک دامین می کنیم و هر اتاق که چندین کاربر دارد را یک گروه و هر طبقه را یک OU می کنیم.

## ساختن OU

بر روی اسم دامین کلیک راست می کنیم و از آنجا این کار را انجام می دهیم



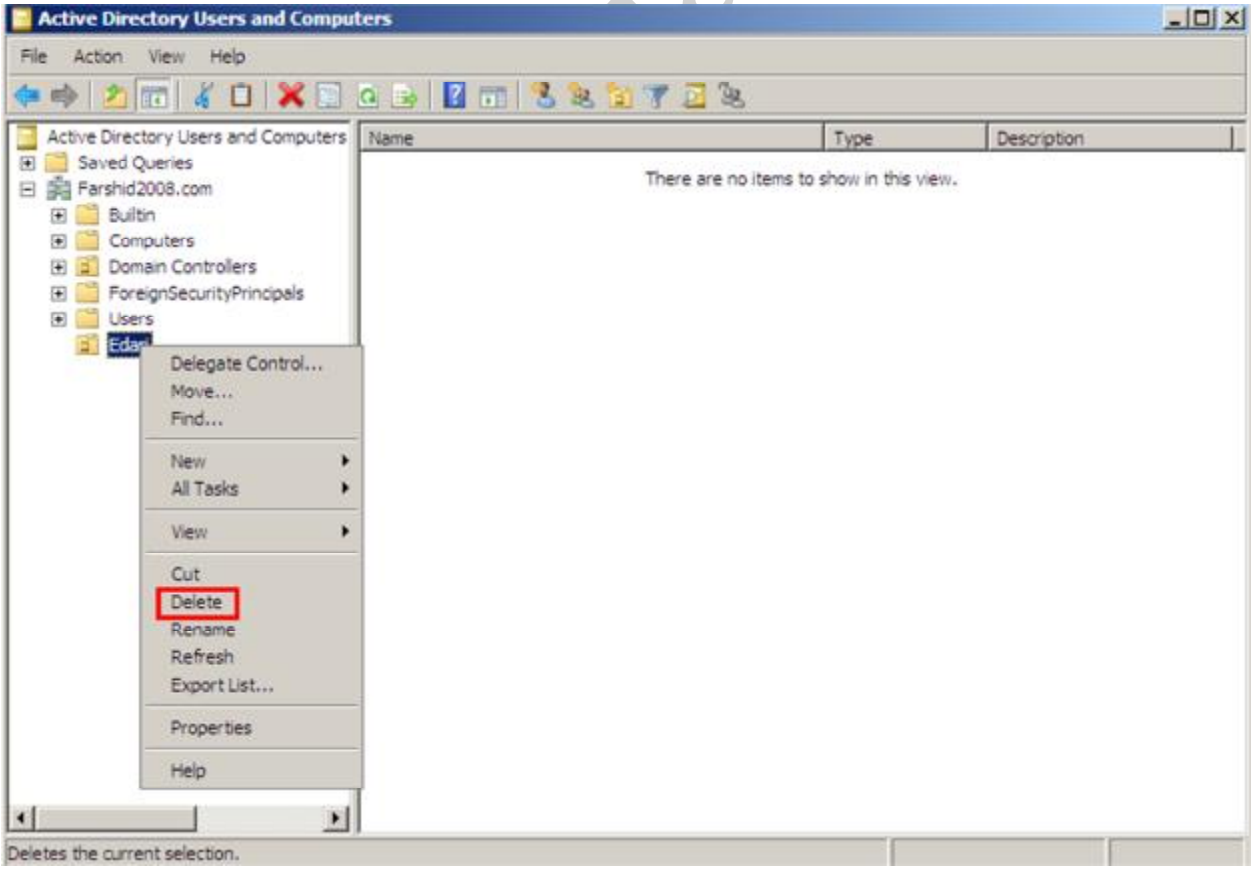
در صفحه بعدی نام OU را مشخص می کنیم، با انتخاب گزینه زیر اجازه نمی دهیم کسی این OU را پاک کند

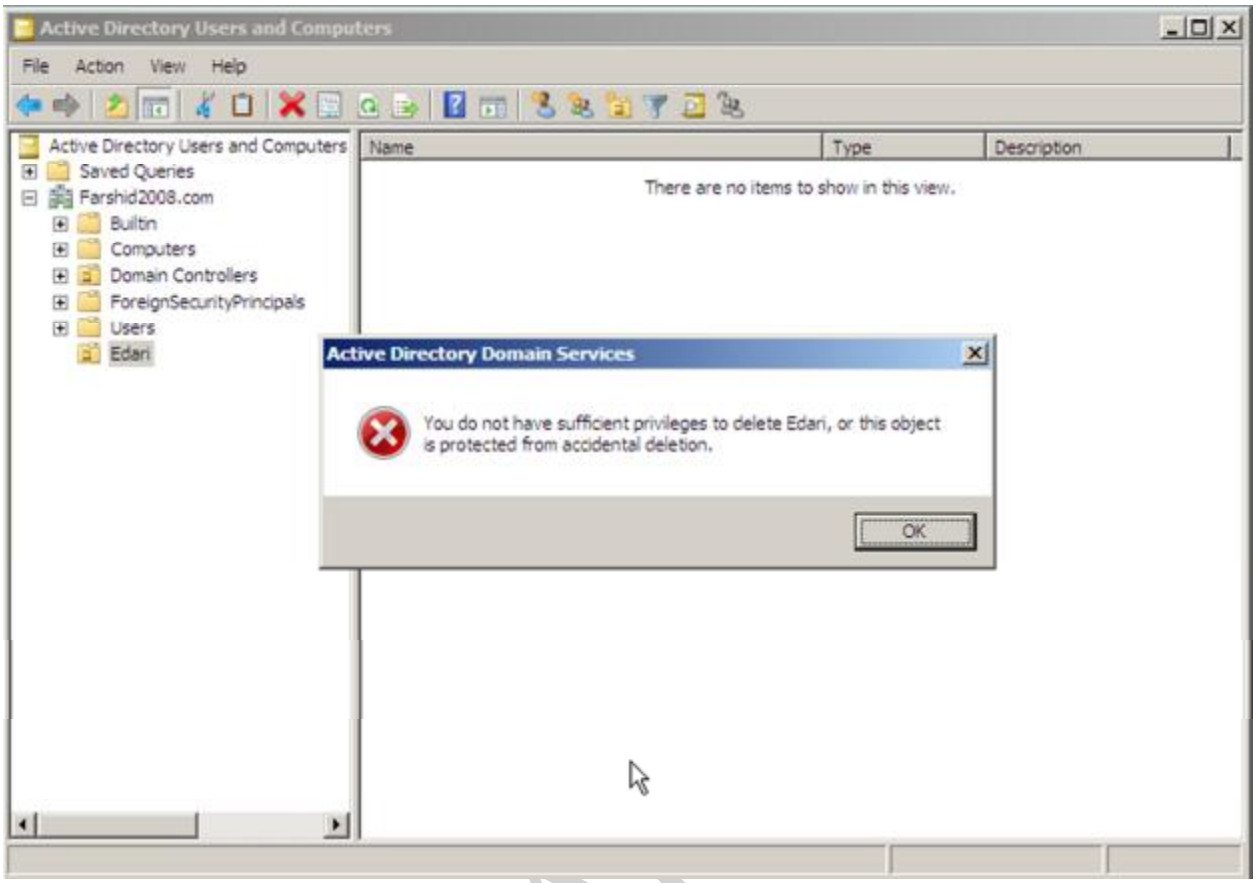



Farsi

**همانطور که می بینید اضافه شد**

**حالا می خواهیم این OU را پاک کنیم**

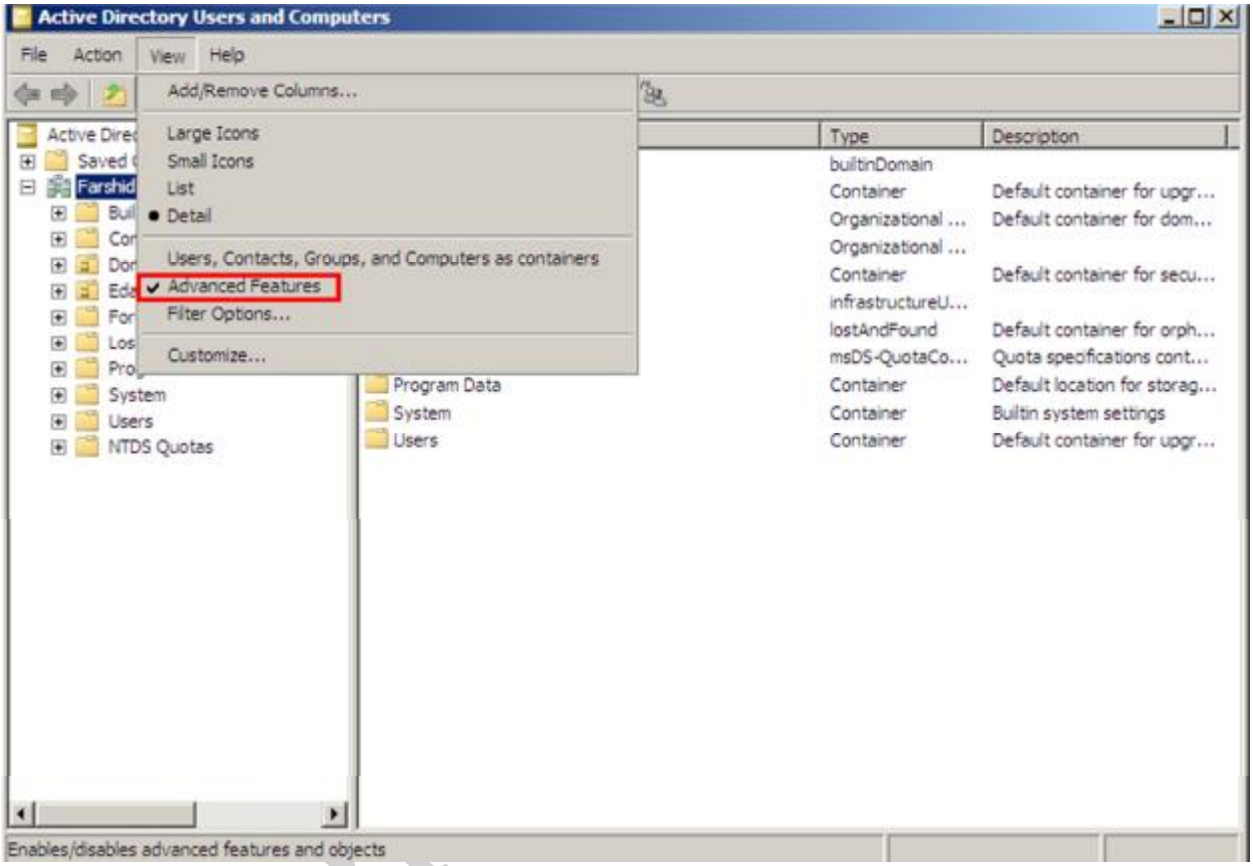



Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers
Saved Queries
Farshid2008.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Edari
Name
Type
Description
There are no items to show in this view.
Active Directory Domain Services
You do not have sufficient privileges to delete Edari, or this object is protected from accidental deletion.
OK

FarshidAj

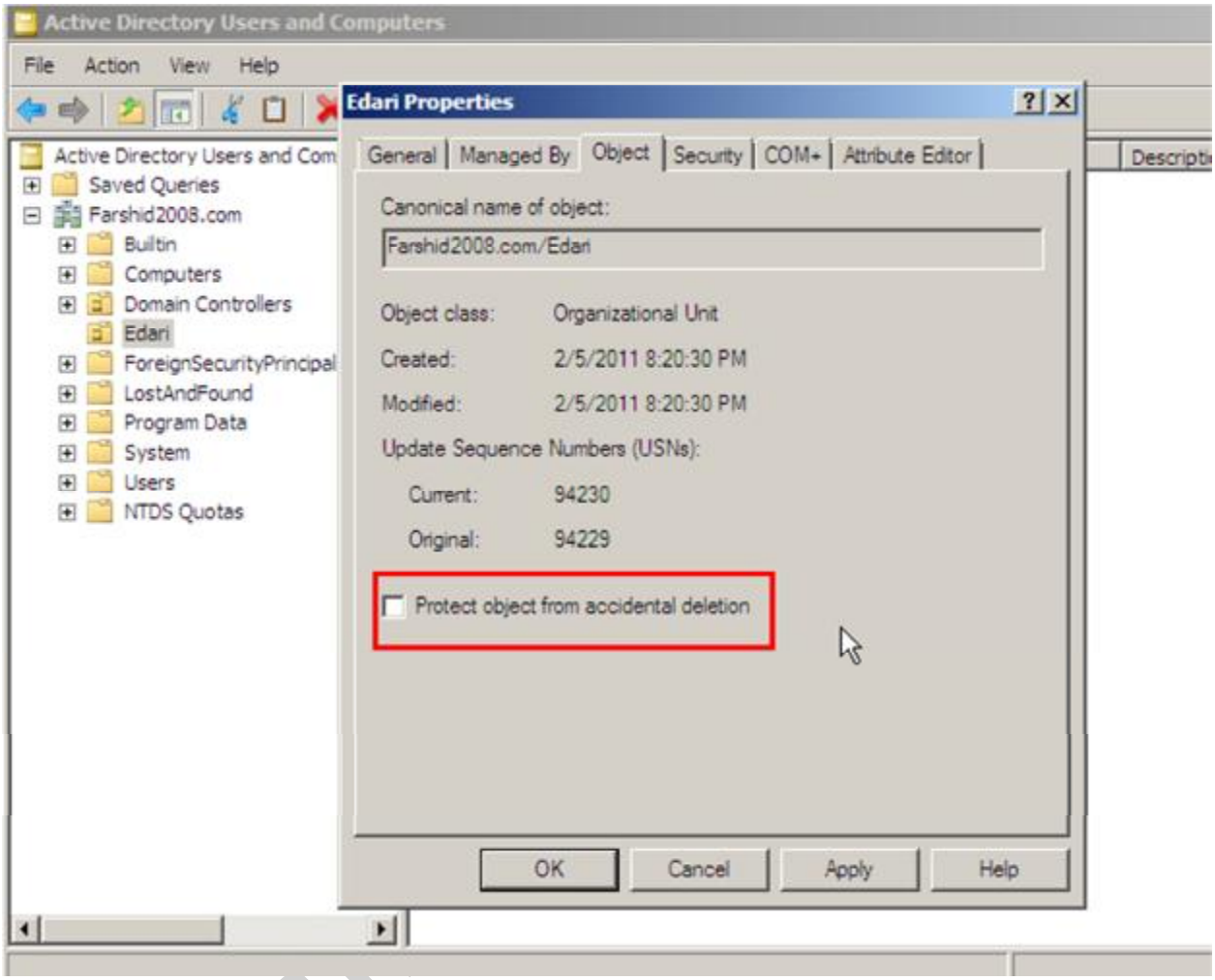
برای اینکه بتوانیم پاک کنیم مسیر زیر را می رویم

تیک .....Advanced را می زنیم




Farsi

سپس روی OU پراپرتیز می گیریم و از تب Object تیک گزینه .... Protect را بر می داریم

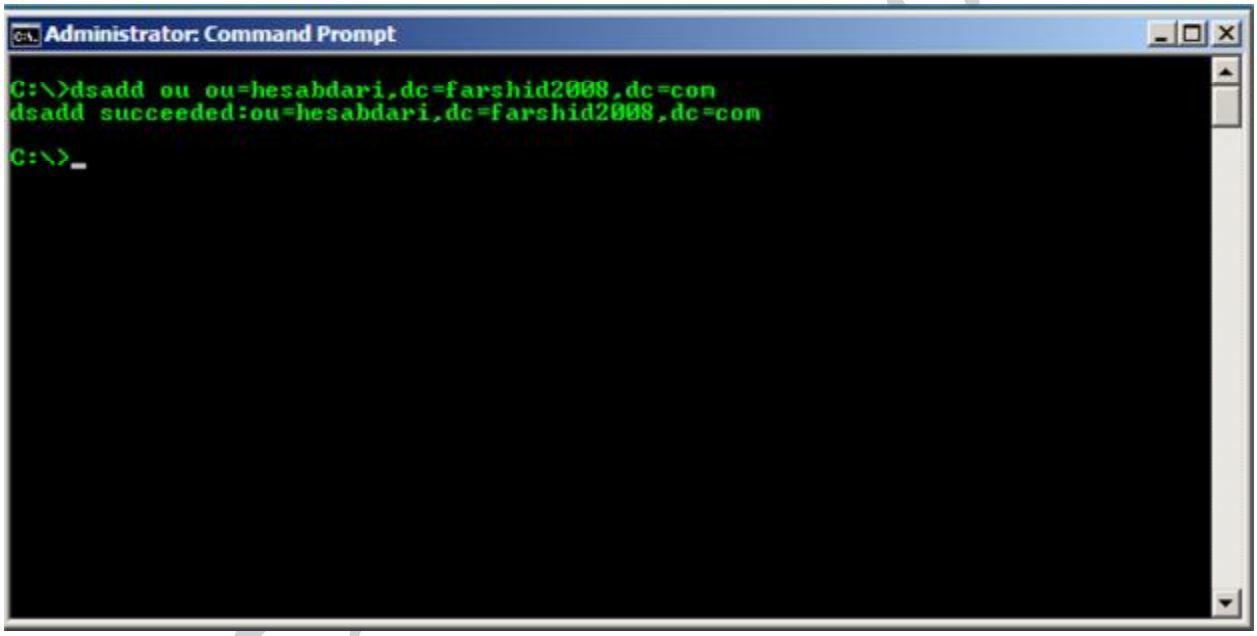



Farsi

اضافه کردن OU با کامند:

Dsadd ou ou=hesabdari,dc=farshid2008,dc=com

ou=hesabdari:اسم OU



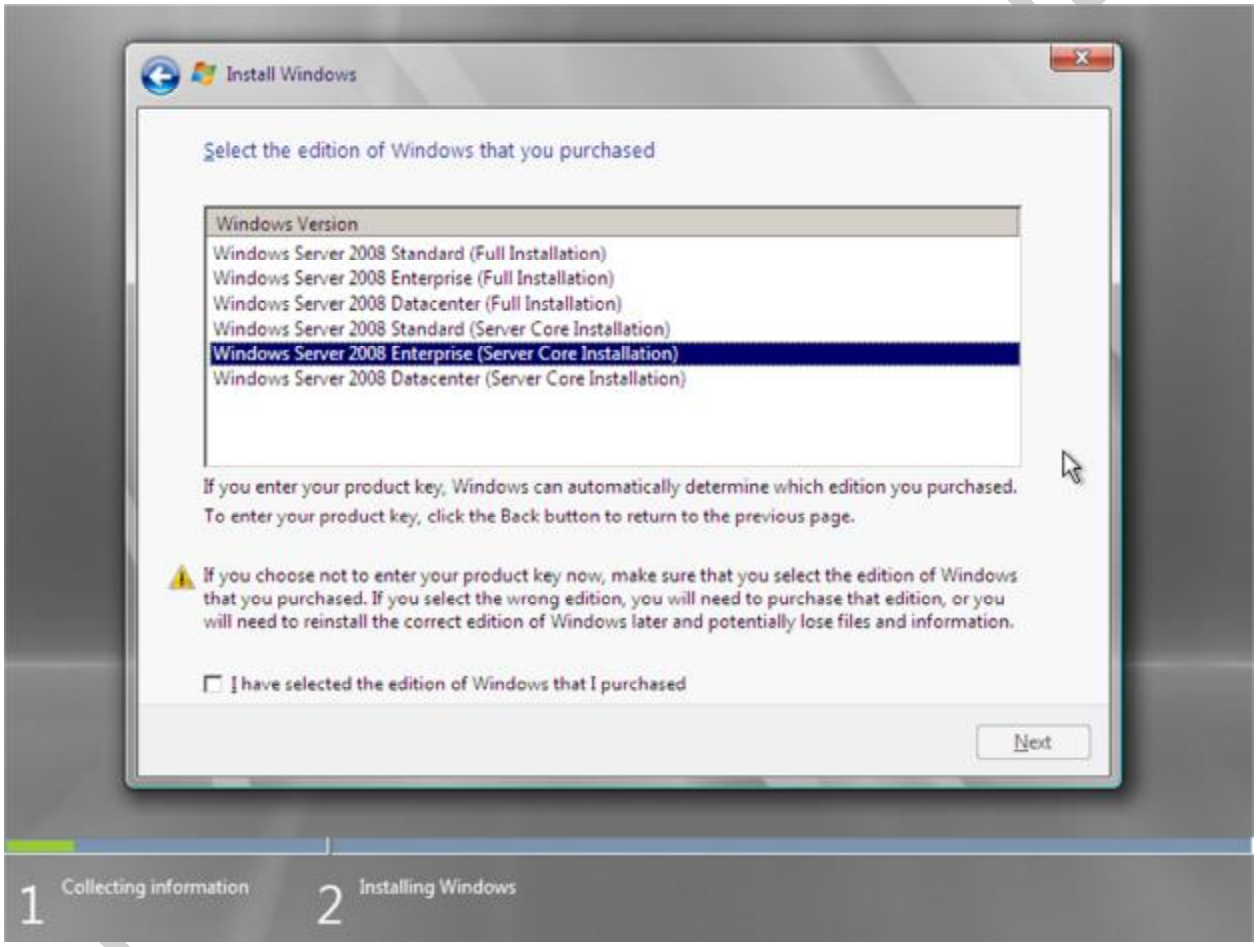

Farshidoush

## Windows Server Core

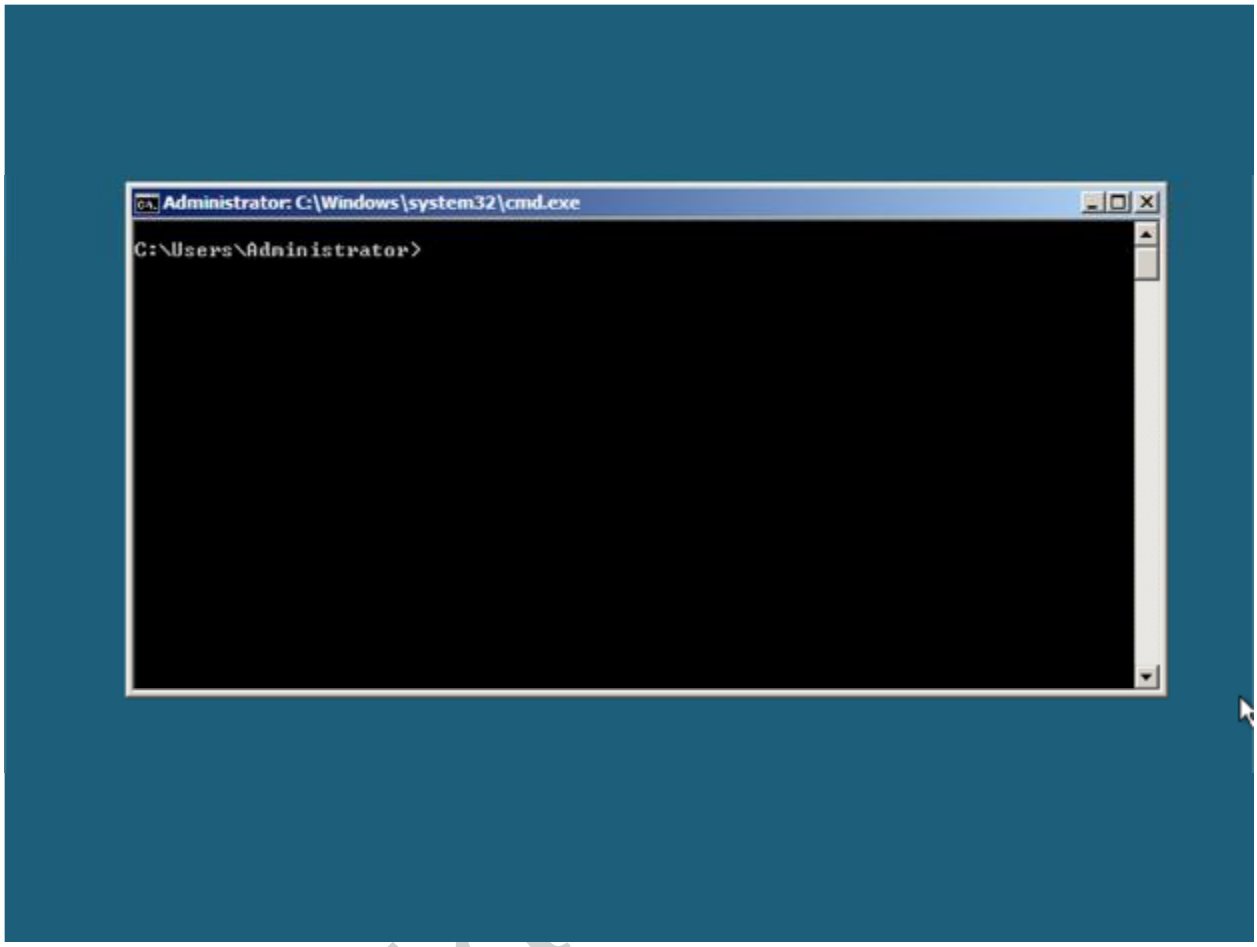
همان ویندوز سرور2008 می باشد با این تفاوت که این سیستم عامل به صورت CLI (Command Line Interface ) می باشد و به همین دلیل امن تر از نسخه GUI (Graphic User Interface ) .

نصب :

همان DVD ویندوز سرور را گذاشته و موقع نصب Server Core Installation را انتخاب می کنیم.



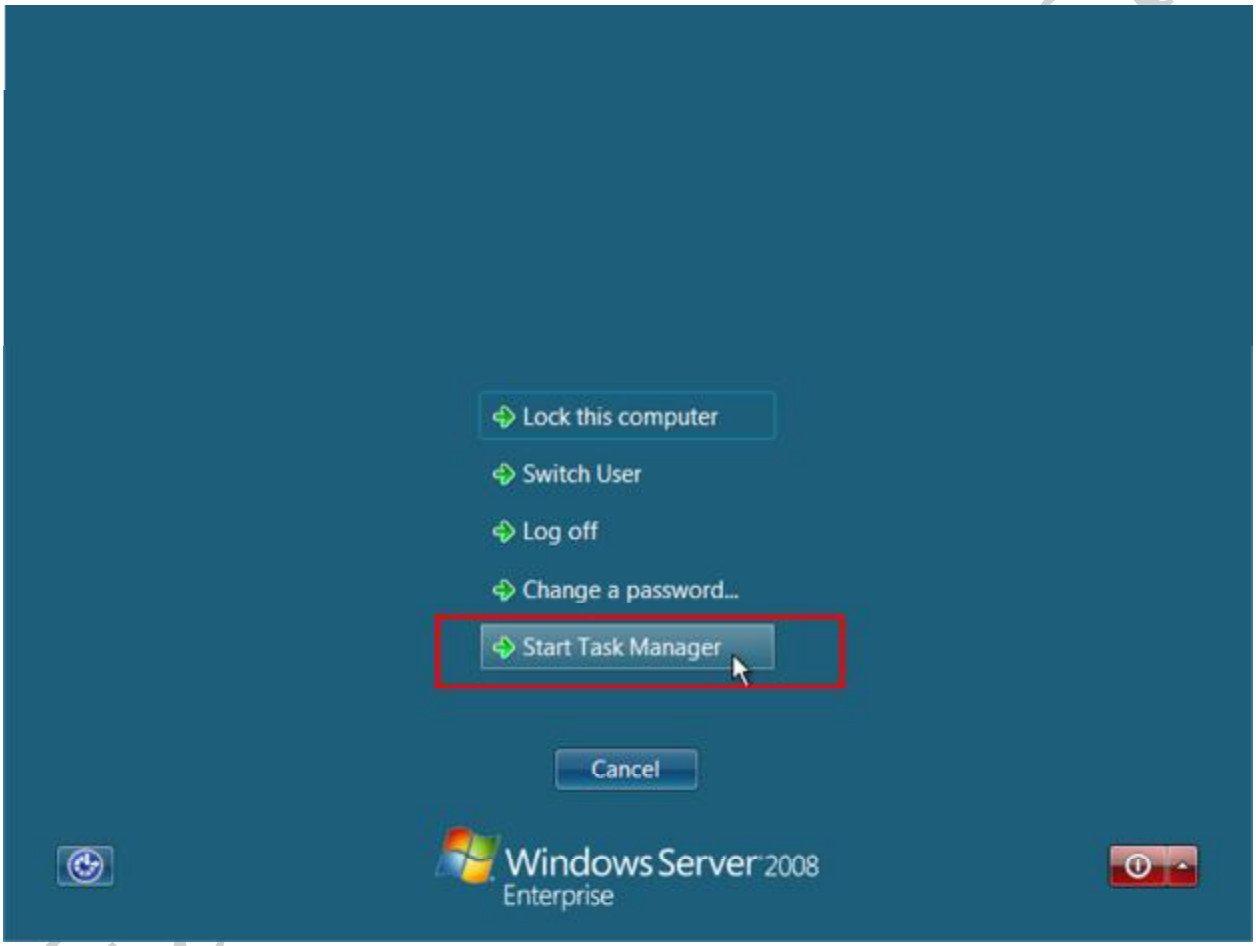
**بعد از اتمام نصب فقط یک محیط کامند داریم**



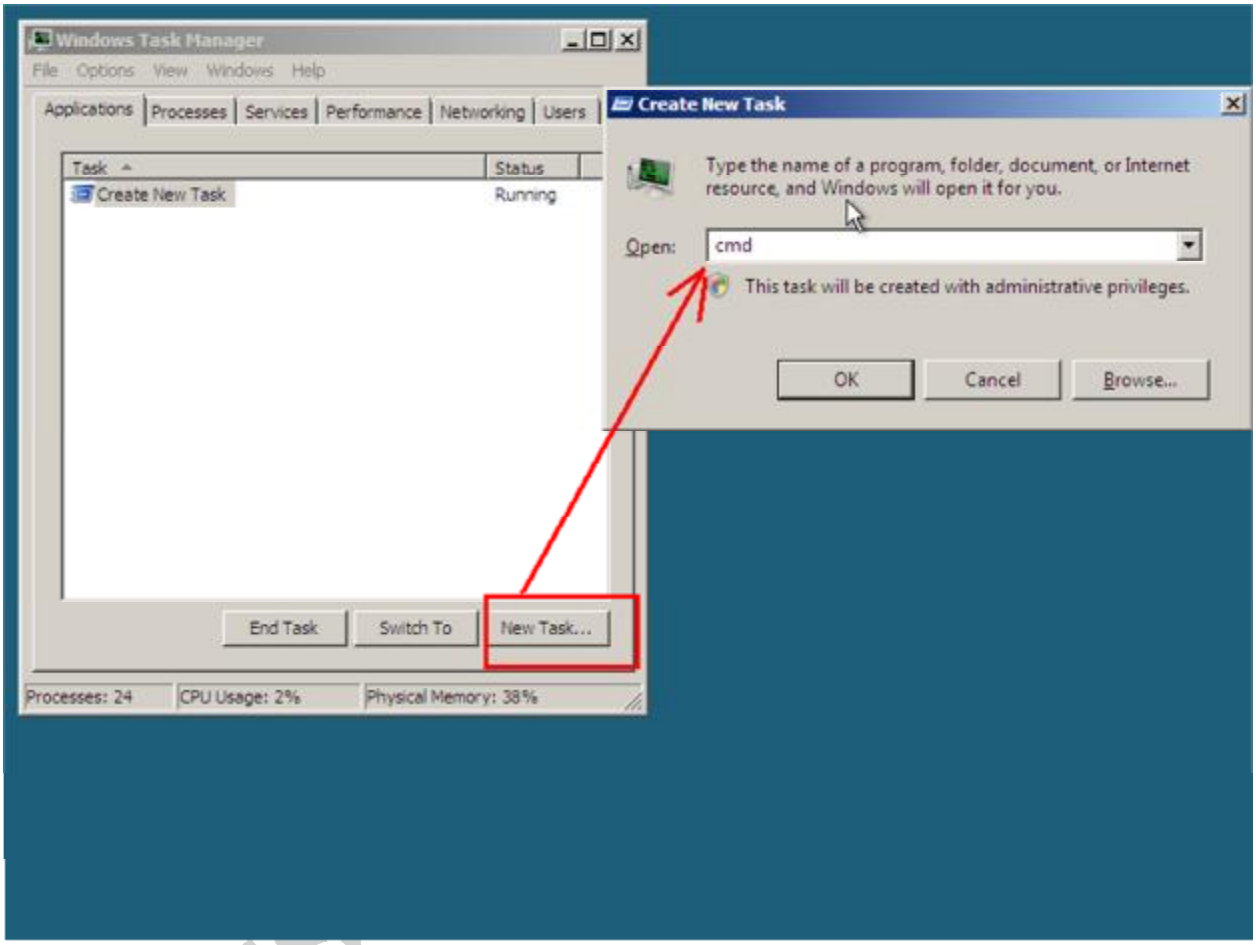

**همانطور که می بینید هیچ آیکونی نداریم،این محیط را می بندیم و دوباره باز می کنیم**

Farshid

برای باز کردن دوباره این پنجره کلیدهای Ctr+Alt+Delete را گرفته و از پنجره باز شده گزینه Start Task Manager را انتخاب می کنیم

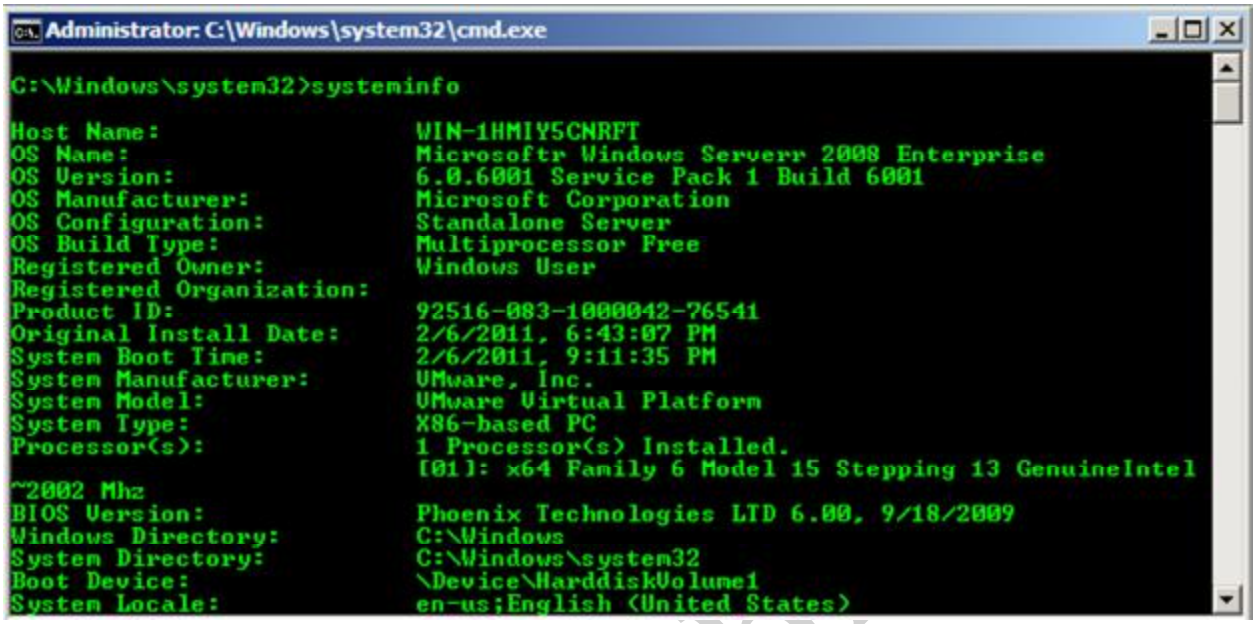


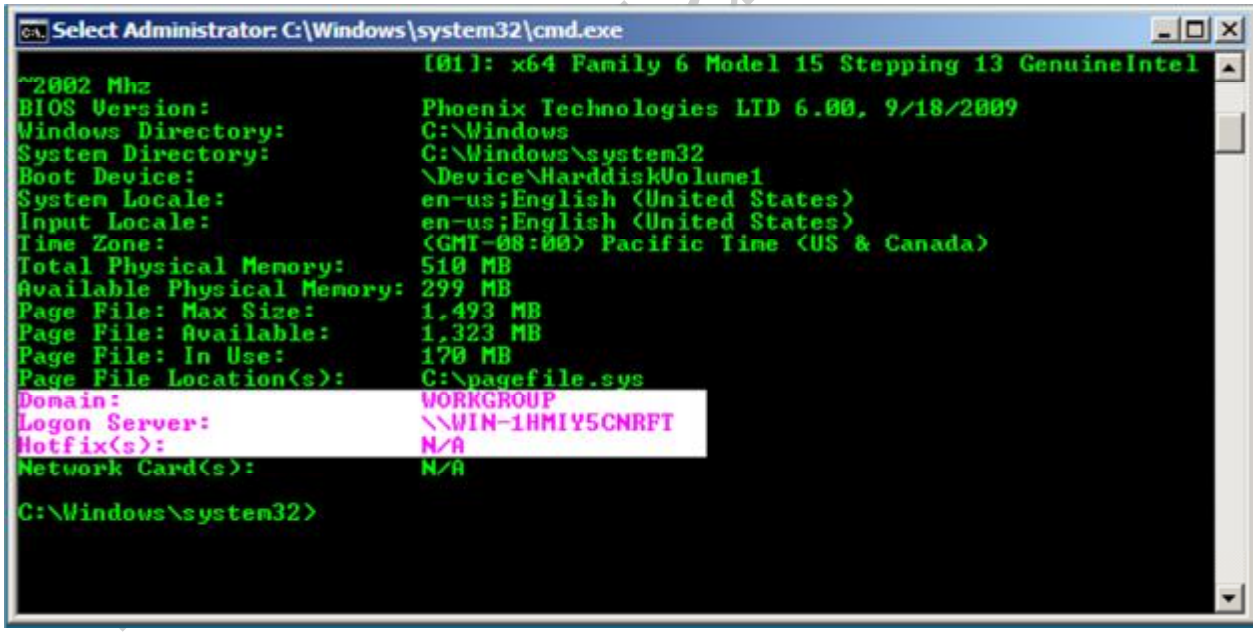
در پنجره بعدی بر روی New Task کلیک می کنیم و تایپ می کنیم CMD و دوباره محیط کامن باز می شود.




Fars

اولین دستوری را که اجرا می کنیم SystemInfo برای دیدن اطلاعات سیستم می باشد



مهمترین مسئله که باید درباره سیستم عامل بدانیم این است که عضو دامین است یا ورک گروپ که در اینجا ورک گروپ می باشد.

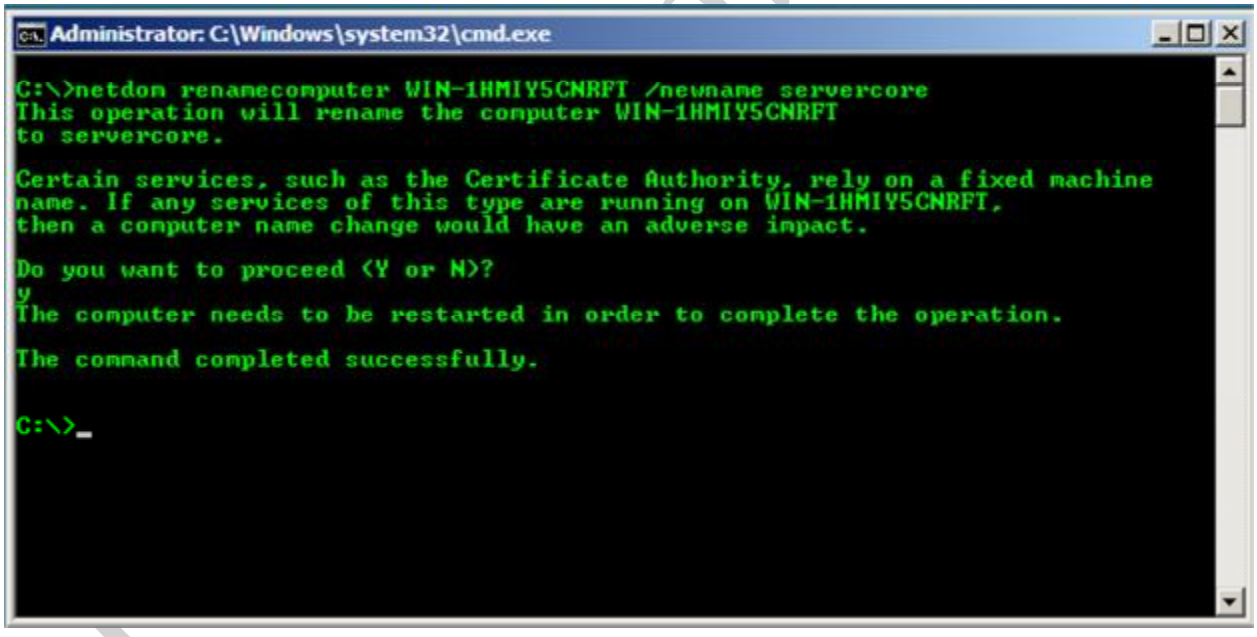
HotFix : به فایل های مهم (آپدیت)که بر روی سرورها نصب می شود تا ورژن آنها را بالا ببرد گویند،این فایل ها در درایو C می باشند که اول آنها با $ (دالر) شروع می شود.

حالا نوبت به عوض کردن اسم کامپیوتر با دستور

netdom renamecomputer win-8z../newname servercore

win-8z..: اسم قدیمی کامپیوتر

Servercore: اسم جدید کامپیوتر

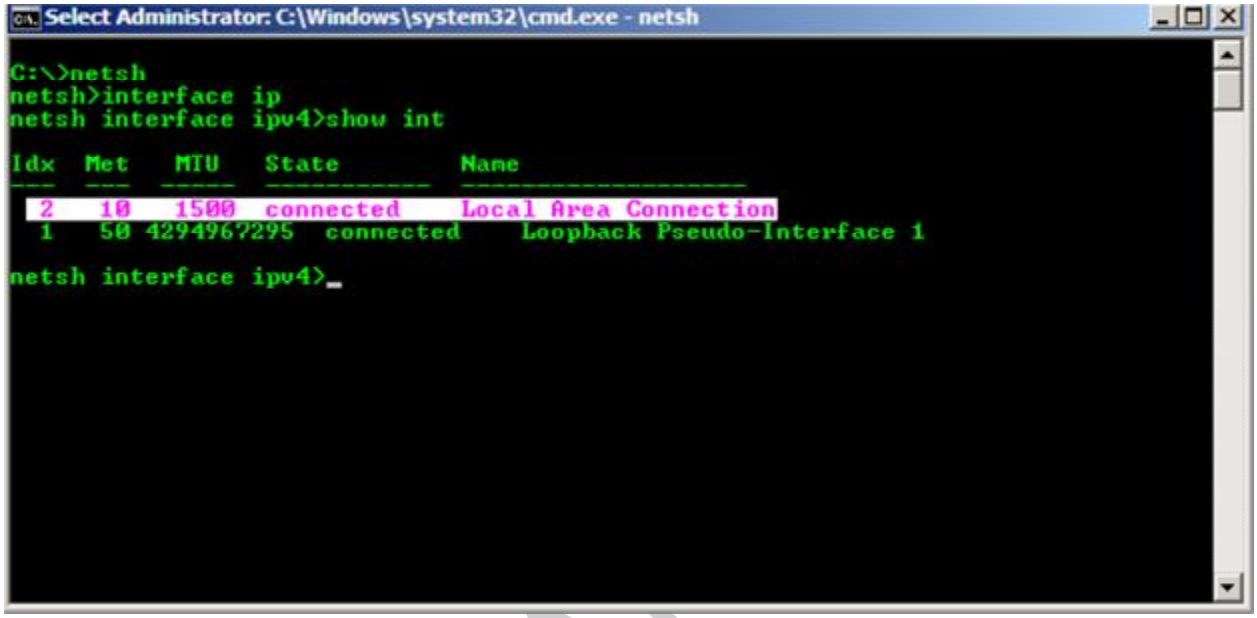



بعد از انجام این کار سیستم باید ریستارت شود، دستور Shutdown -r -t 1، منظور از 1 -t ریستارت شدن بعد از 1 ثانیه است.

حالا نوبت به دادن ip می باشد برای این کار از دستورات زیر استفاده می کنیم:

netsh (1 interface ip(2 show int(3

بعد از تایپ این دستور لیستی از کارت شبکه ها ی موجود را نمایش می دهد کهIDX اولیت کارت شبکه می باشد



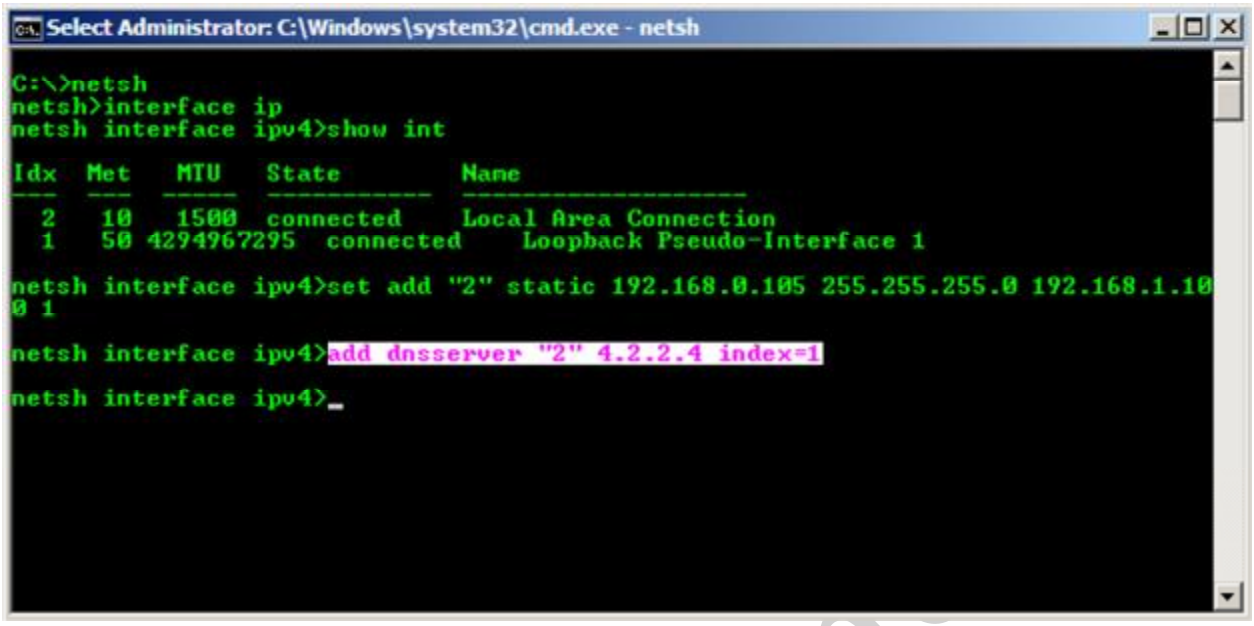

مرحله بعد تنظیم ip با دستورset add 1 192.168.1.100 255.255.255.0 static "2"

"2": اسم کارت شبکه ، 1 اولویت استفاده کارت شبکه

نوبت به تنظیم DNS می باشد. دستور add dnsserver "2" 4.2.2.4 index=1

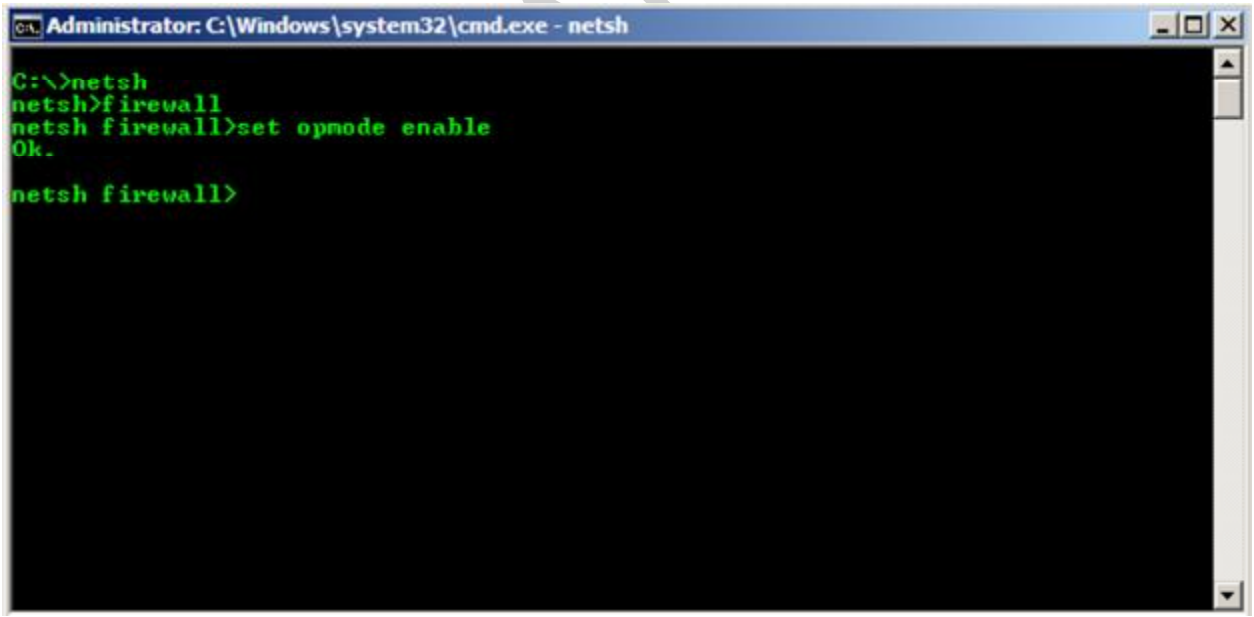
index=1 اولین DNS ، index=2 دومینDNS

FarshidAj



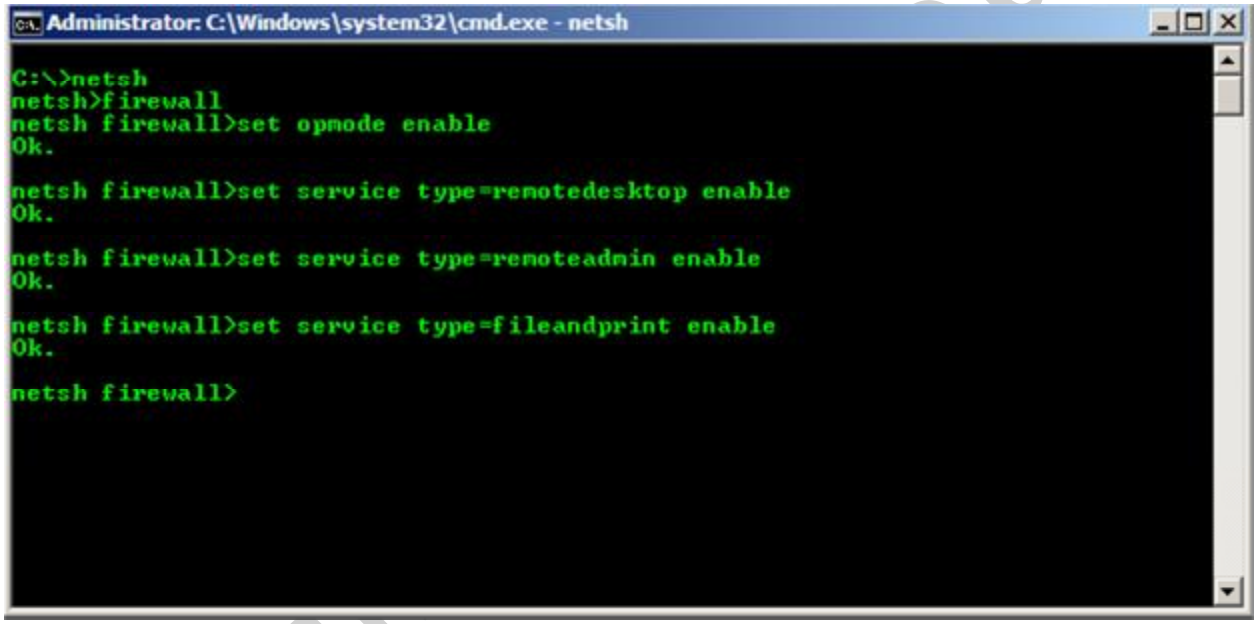

تنظیم فایروال:

برای این کا ر از دستور 1)netsh 2) firewall 3)Set opmode enable ( or disable)



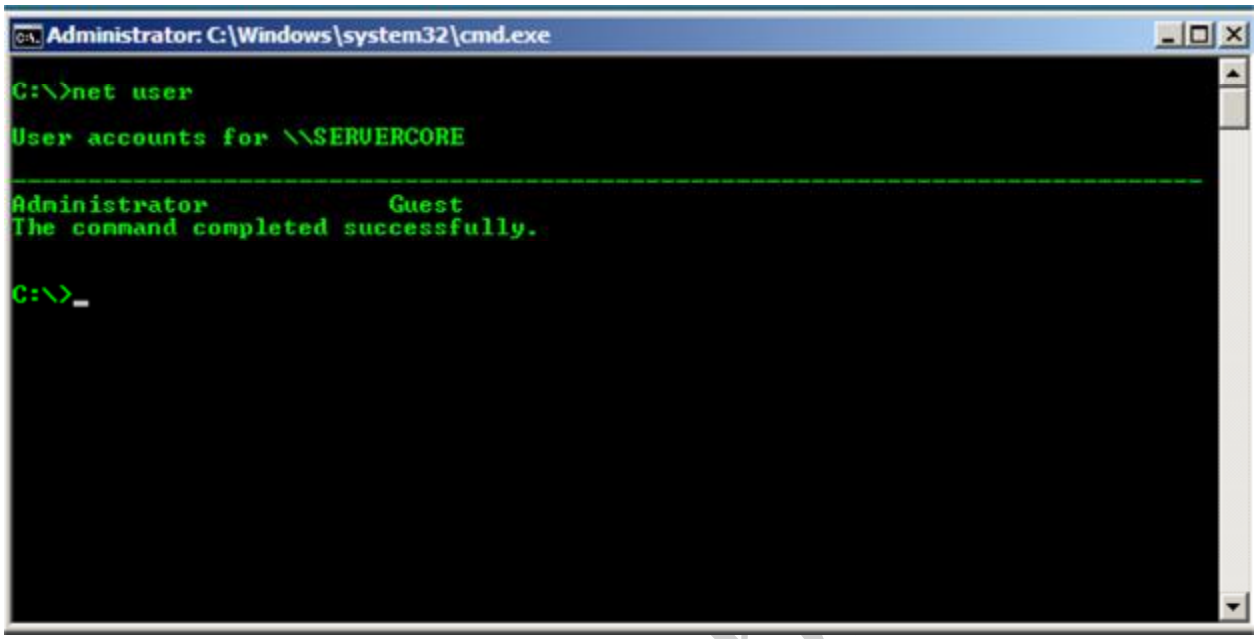
نوبت به فعال کردن سرویس ها می رسد

1) Set service type=remotedesktop enable
2) Set service type=remotadmin enable= اجازه مدیریت از بیرون
3) Set service type=fileandprint enable= اجازه دسترسی به فایلهای Share و Ping کردن



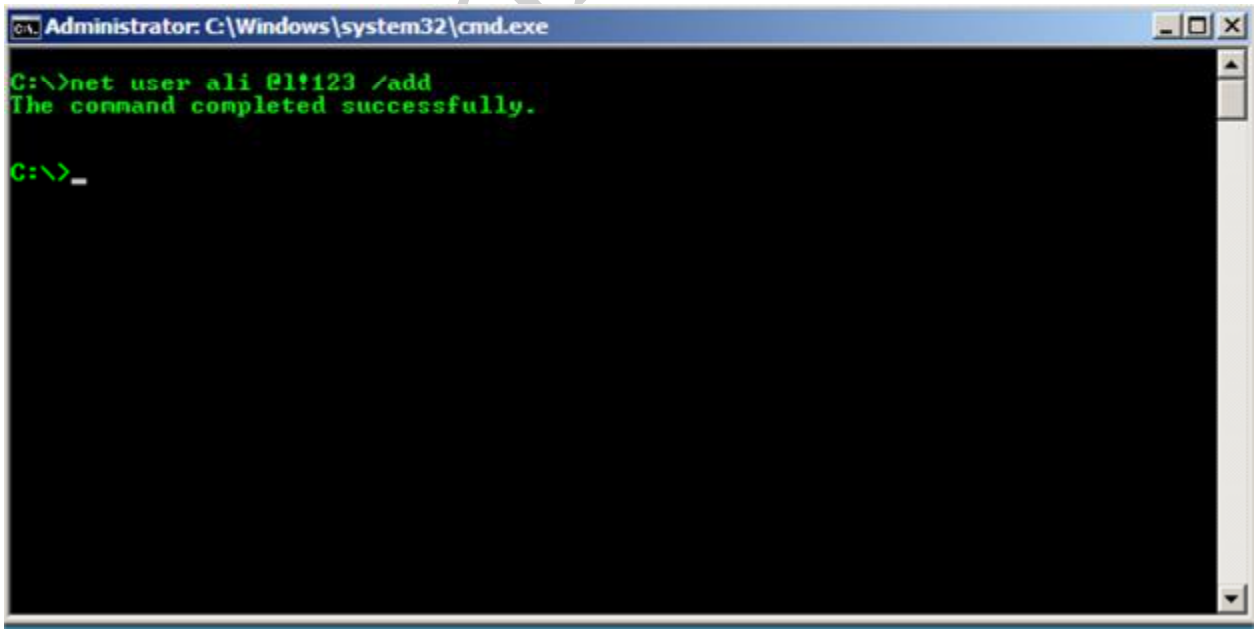

Farsroush

تمامی یوزرهای سیستم را نشان می دهد Net user

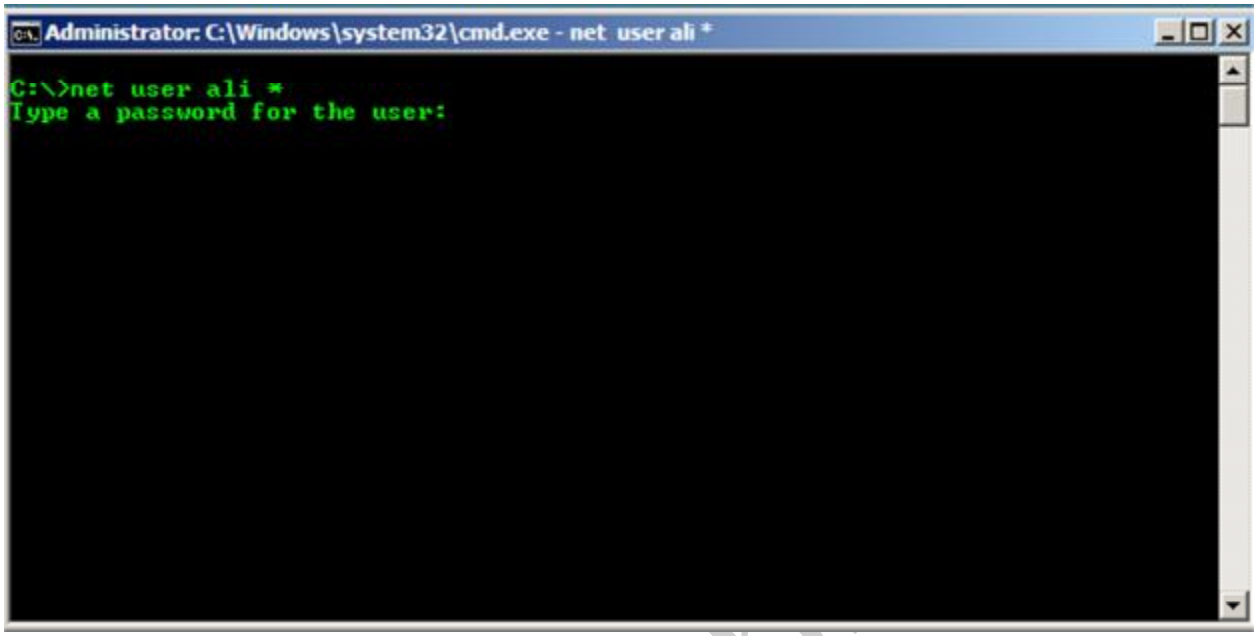



ساختن یوزر net user ali @l!123 /add

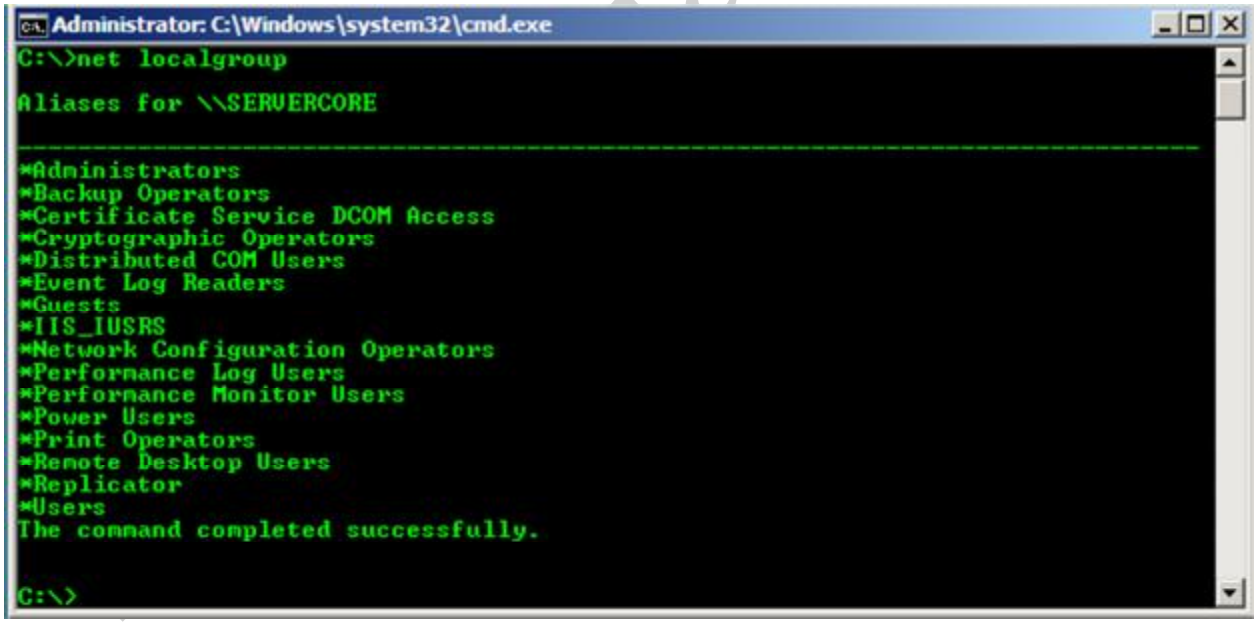
@l!123: پسورد، ali : اسم یوزر



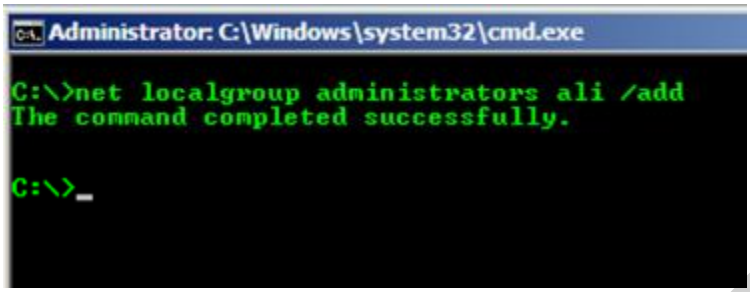
تعویض پسورد * Ali=net user ali



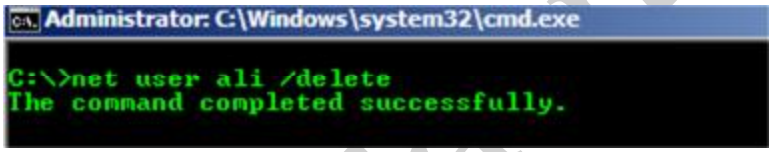

دیدن گروه ها: net localgroup



اضافه کردن ali به گروه Admin : net localgroup administrators ali /add

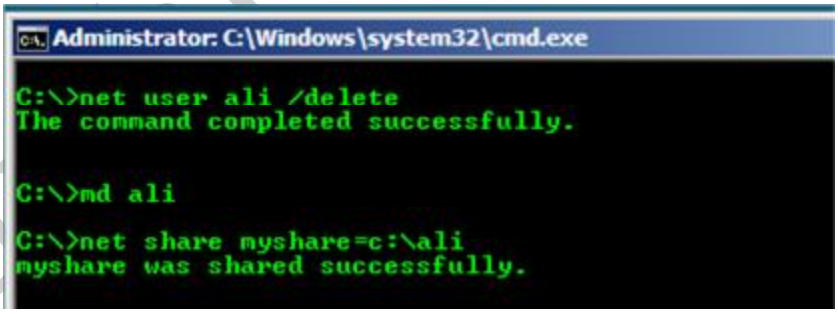



پاک کردن Ali: net user ali /delete




Share

ساختن پوشه علی md ali

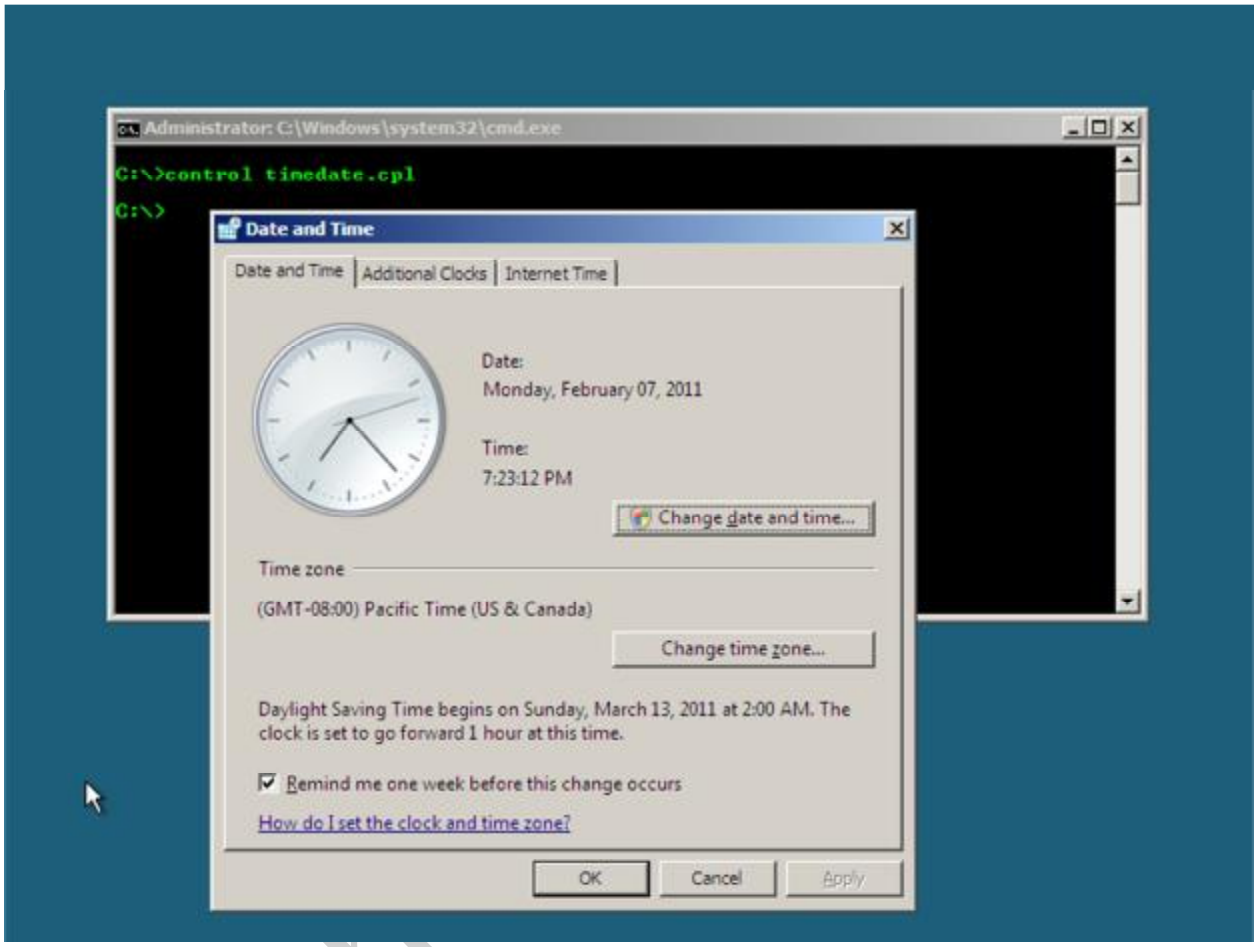



سپس با دستور Share Net share myshare=c:\aliمی کنیم.

Myshare اسم شیر نیممان است، در کامپسوتر دیگر Ip سیستم را که بزنیم Share ها باز می شود.

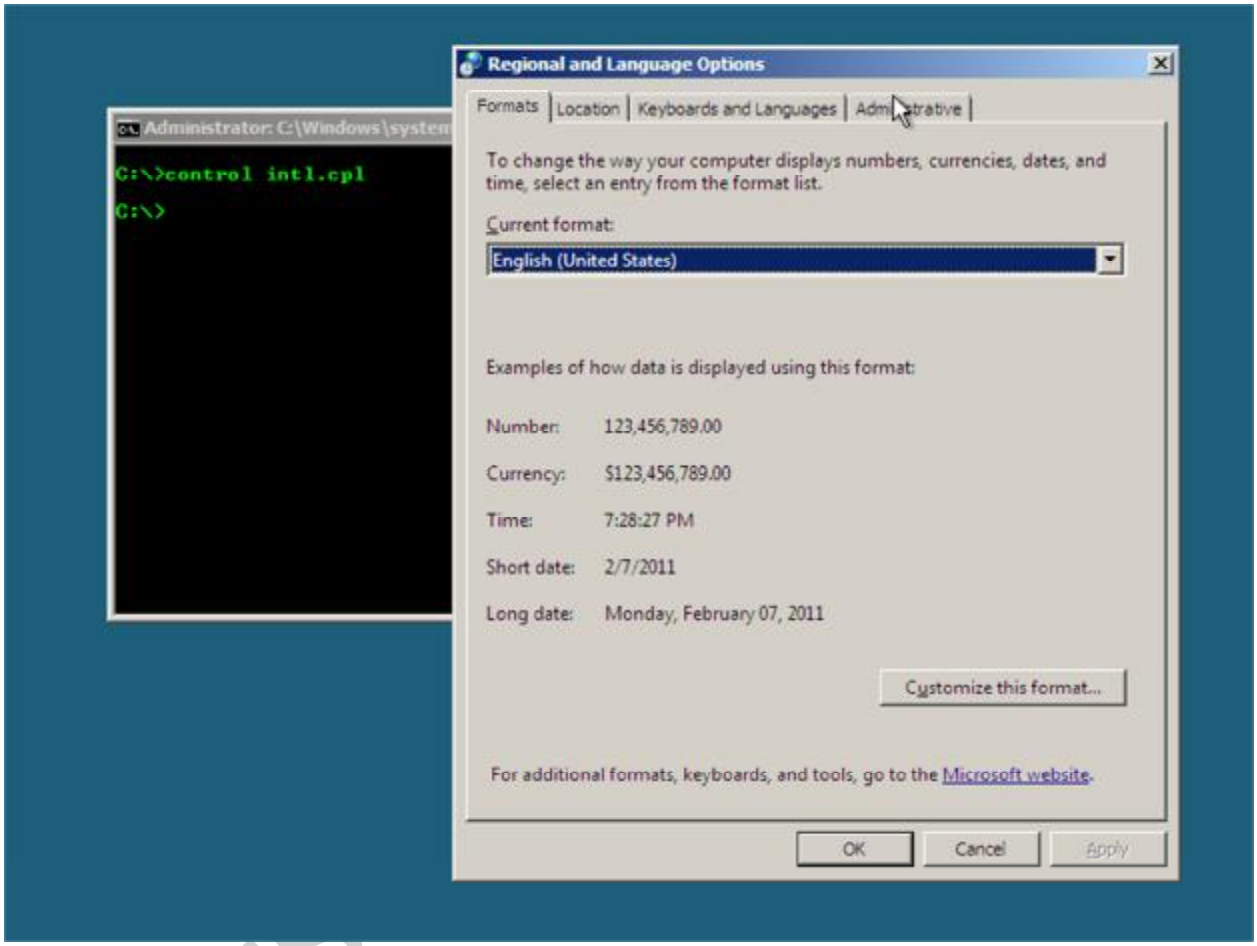
FaridAjamoush

برای تنظیم کردن ساعت سرور از دستور control timedate .cpl




Farsi

برای تنظیم Regional and Languge از دستور control intl.cpL

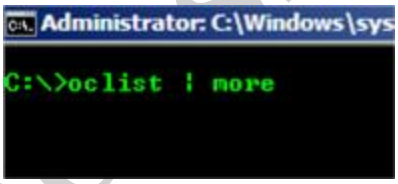



Fars

اگر بخواهیم پشت این سرور سرویسی نصب کنیم از دستور oc setup برای هر سرویسی به غیر از اکتیو دایرکتوری

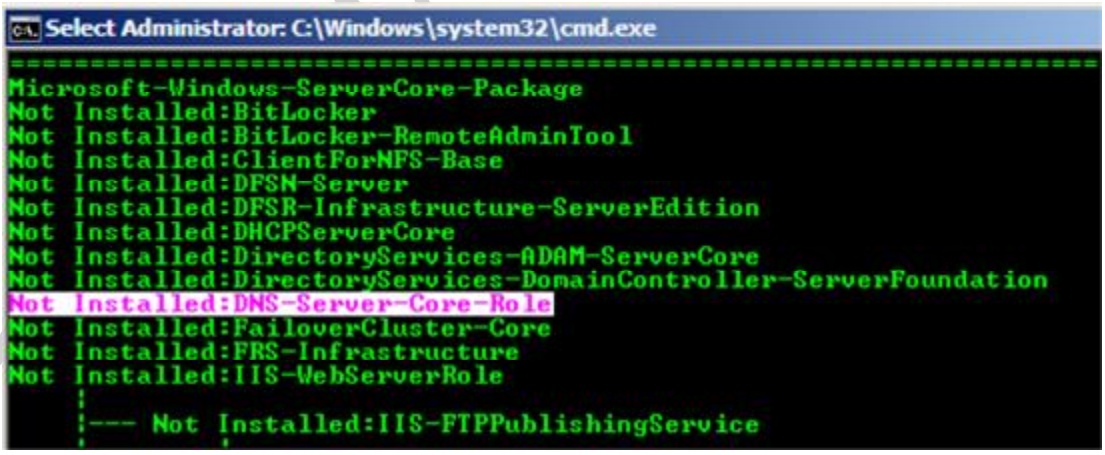
Dcpromo برای نصب اکتیو دایرکتوری

دستور oc list | more برای نمایش دادن صفحه به صفحه سرویس ها می باشد



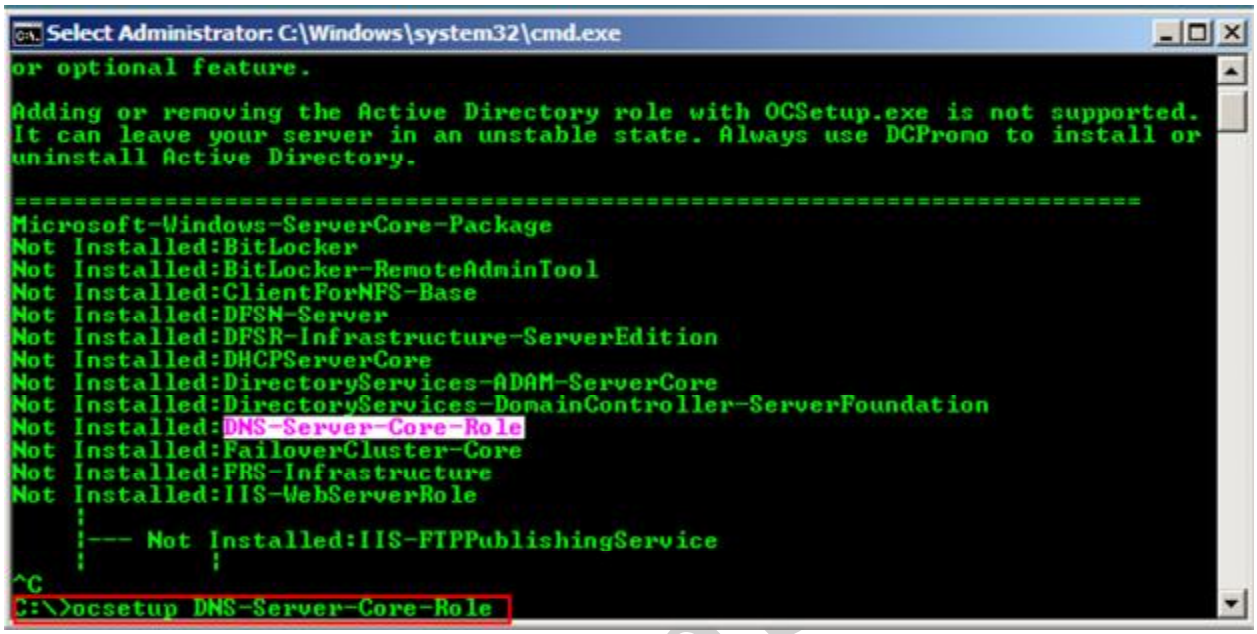

|=shift+\

در اینجا می بینیمDNS سرورنصب نمی باشد

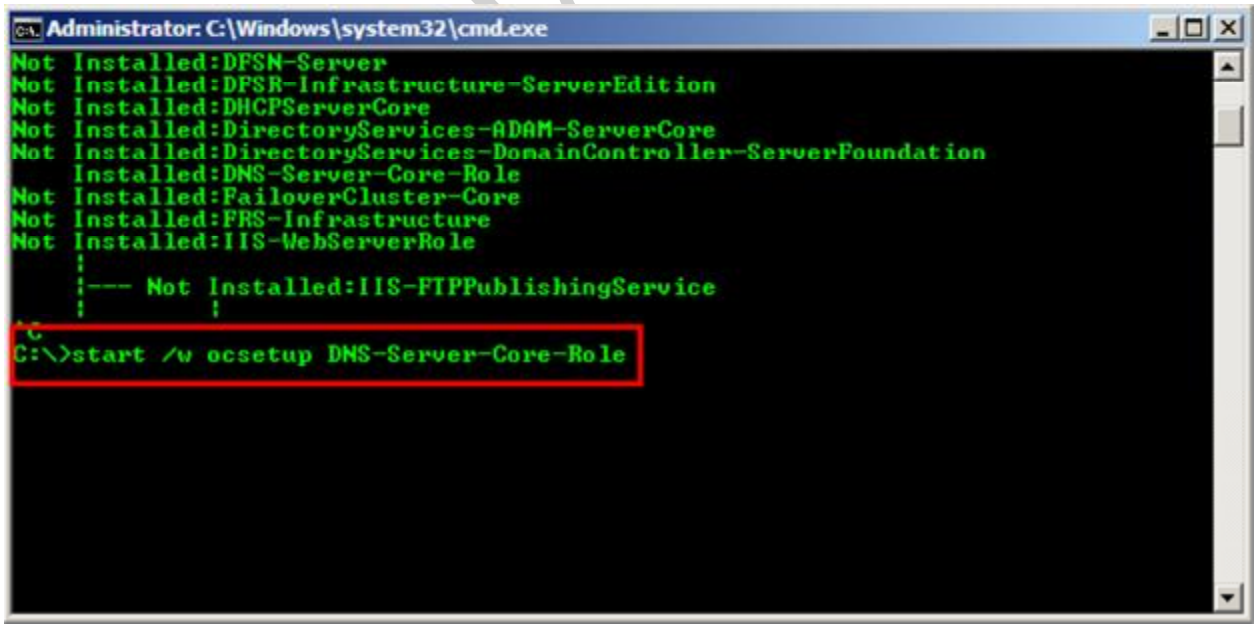



Fa Ajabnesh

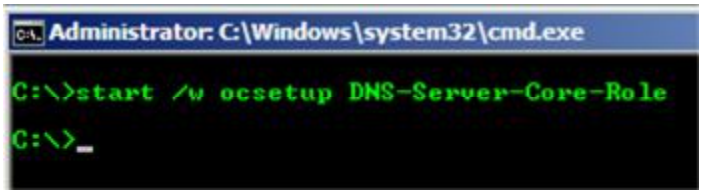
برای نصب DNS از دستور ocsetup DNS-Server-Core-Role استفاده می کنیم این دستور به اندازه حروف حساس می باشد DNS-Server-Core-Role را می توانیم کپی کنیم.



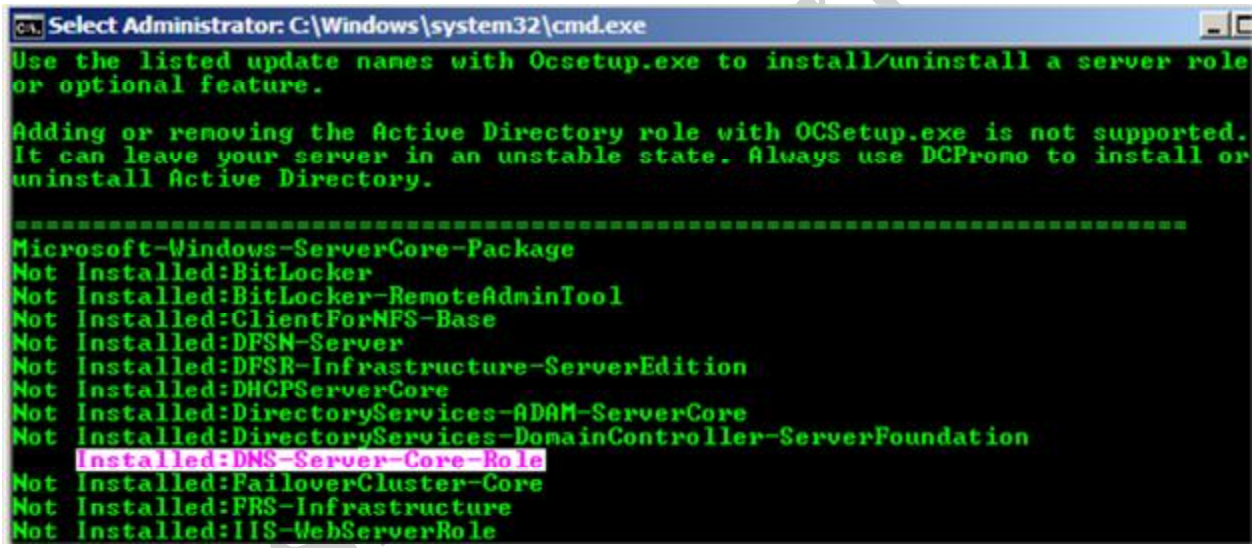

اگر از دستور بالا استفاده کنید خط به خط نصب را نشان می دهد برای غیر فعال کردن این نمایش به اول دستور start /w را اضافه می کنیم



در اینجا می بینیم که نصب شد

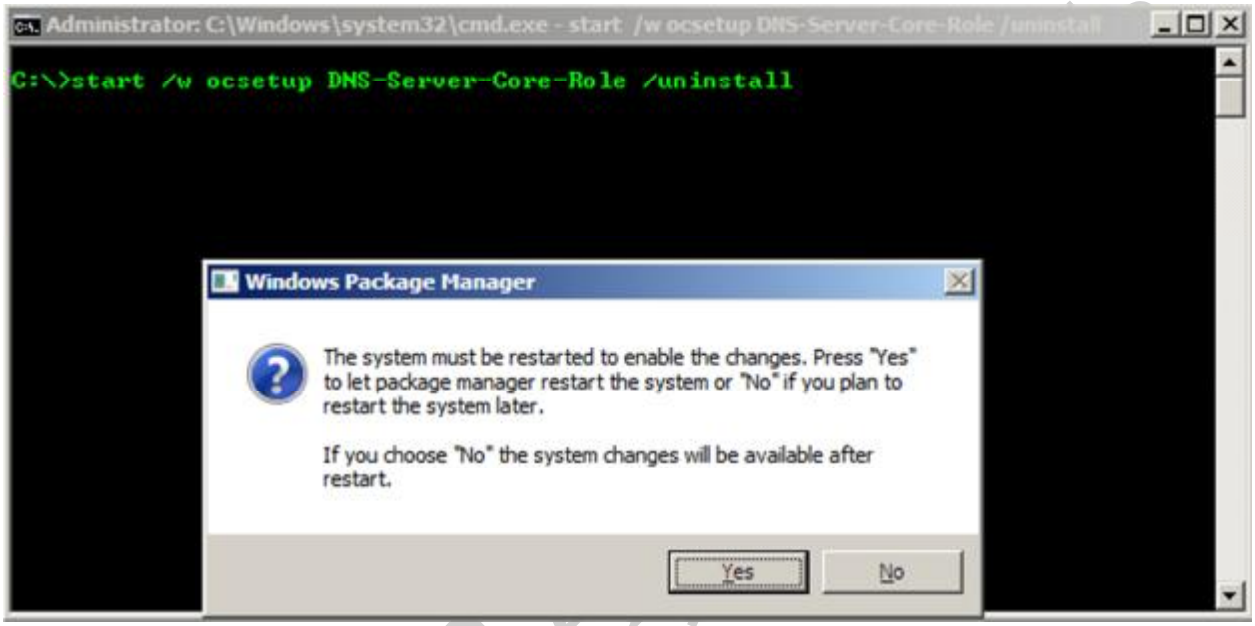



برای اطمینان از نصب از دستور oclist | more استفاده می کنیم




Fars

برای Uninstall کردنDNS از دستور start /w ocsetupDNS-Server-Core-Role /uninstall استفاده می کنیم.



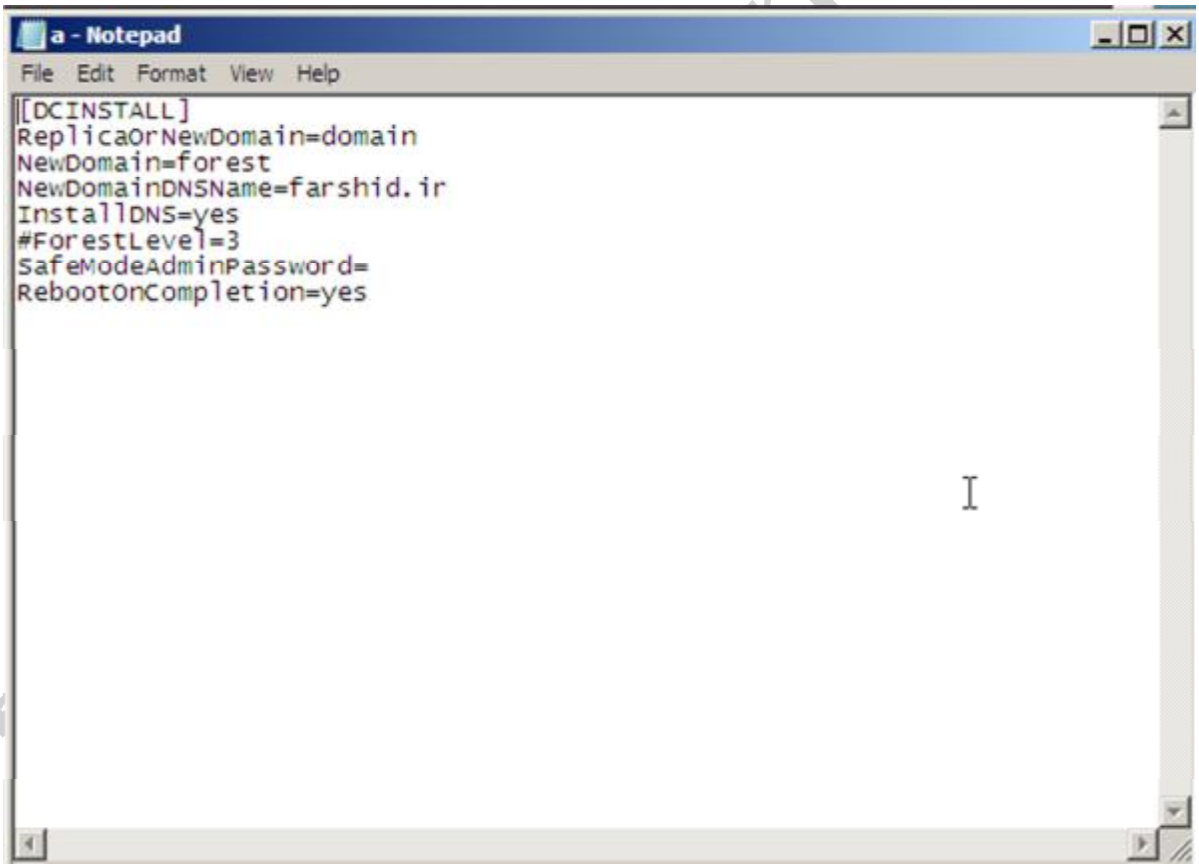

Farshida

نصب اکتیو دایرکتوری

برای این کار باید در ابتدا یک فایل نوت پد باز کنیم و دستورات را تایپ کنیم و سپس آن را ذخیره کنیم و در هنگام نصب آن را فرا بخوانیم.

با دستور notepad a.txt نوت پد A را باز می کنیم.

سپس دستورات را تایپ می کنیم ،دقت به حروف کوچک وبزرگ کنید




- بعداز مساوی حروف کوچک وبزرگ مهم نیست.

در سطر دوم domain= : اگر اولین دامین باشد(Root Domain ) این را می نویسیم اگر دامین هایی غیر اولین دامین باشد (مانندChild,DomainTree,Bdc )عبارت Replicaرا بعد از مساوی می نویسیم.

در سطر سوم forest=زمانی که می نویسیم فارست یعنی این دامین(Rootdomain) اولین دامین است،اگر Child یاDomainTree باشد عبارات (Child,DomainTree ) را بعداز = قرار می دهیم.

سطر چهارم اسم دامین را می نویسیم

سطر پنجم یعنی خود اکتیو،DNS راهم نصب کند

سطر ششم این خط به صورت انتخابی است، این همان FFL است ، بعد از = می توانیم اعداد 0 که بیانگر ویندوز 2000و 1 برابر 2003و 3 برابر 2008 است بخاطر اینکه این دستور انتخابی است در ابتدای دستور یک ( )# =Sharp قرار می دهیم یعنی انتخابی

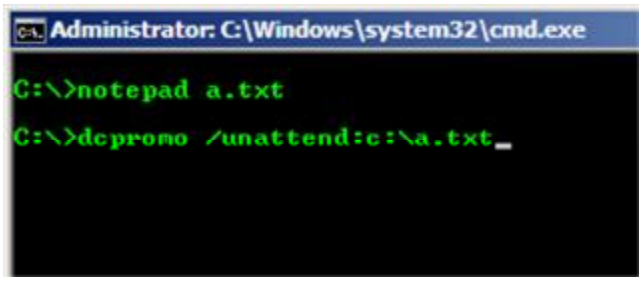
سطر هفتم پسورد بازیابی اکتیو دایرکتوری است

سطر هشتم یعنی زمانی که نصب تمام شد بطور اتوماتیک ریستارت کن

در آخر هم ذخیره می کنیم

حالا نوبت به نصب می رسد dcpromo /unattend:c:\a.txt

c:\a.txt مسیر ذخیره شده نوت پد می باشد




FarshidAjabnoush

## Emplementing DNS Server In Microsoft Network

در شبکه 2 نوع اسم برای کامپیوتر ها داریم 1) NetBios Name 2) Host Name

Host Name: اسامی هستند که در سیستم عامل های High Level بکار می روند مانند: Xp,Vista,Seven,2003

NetBios Name: اسامی هستند که در سیستم عامل های Down Level بکار می روند مانند: 98

- Host Name ماکزیمم 255 کاراکتری هستند و NetBios Nameماکزیمم 15 کاراکتری هستند.
- تمامی سیستم عامل هایی که استفاده می کنیم دارای NetBios Name هستند برای دیدن NetBios Name از دستور NBTSTAT -N است در هنگام نصب ویندوز اسمی را که از ما می پرسد از این نوع می باشد.
- زمانی که My Network Place را باز می کنیم اسامی کامپیوتر هایی را که نوشته بر اساس NetBios Name است،برای اینکه شبکه های لینوکسی بتوانند با شبکه های مایکروسافتی از طریق اسم ارتباط برقرار کنند، از این نوع اسم با مایکروسافت ارتباط برقرار می کنند.

در شبکه ها برای تبدیل اسم به Ip وبرعکس از دو روش استفاده می کنیم

1) Static(یعنی بصورت دستی این کار را بکنیم) 2)Dynamic(سرویسی این کار را انجام می دهد)

روش Dynamic به 2 دسته تقسیم می شود 1) DNS 2)WINS (Windows Internet Name Service )

FarshidAjabnoush

- سرویسی که Host Name را به Ip تبدیل کند DNS گویند، در شبکه های High Level برای تبدیل Ipبه اسم از DNS استفاده می کنند.
- سرویسی که NetBios Name را به Ip تبدیل کند WINS گویند.در شبکه های Down Level برای تبدیل Ipبه اسم از WINSاستفاده می کردند.
- WINS کاملاً در شبکه های ماکروسافتی منسوخ شده است.
- به کار DNS,WINSName Resolution گویند.

نحوه انجام Name Resolution توسط DNS :

http:// www.yahoo.com.

وقتی که اسم سایتی را در مرورگر تایپ می کنیم در پایین مرورگر اسم سایت به صورت بالا نمایان می شود که گاهی بجای دات آخر آدرس / می آید.

به کل آدرس بالا Uniform Resource Locator گویند.

به www.yahoo.com، Fully Qualified Domain Name گویند.

به com. Top Level Domain گویند.

به دات ( نقطه) بعد از COM، Root Hints گویند.

عمل Name Resolution کل دنیا را 13 سرور DNSانجام می دهند که به آنها Root Hints گویند.

FarshidAjabnoush

- تبدیل اسم به Ip از سمت راست به چپ صورت می گیرد.
- زمانی که DNS نصب می کنیم به صورت اتوماتیک آدرس 13 سرور DNS بر روی DNS سرور ما کپی می شود.
- اساس کار تمامی DNS ها بر حسب ZONE است،در DNS 2نوع Zone می توانیم بسازیم:
- 1)Forward Lookup Zone : اگر زونی از این نوع باشد کارش تبدیل اسم به Ip می باشد.
- 2)Reverse Lookup Zone :اگر زونی از این نوع باشد کارش تبدیلIp به اسم می باشد.
- 99% زونهایی که می سازیم از نوع Forward Lookup Zone خواهند بود.
- کاربرد Reverse Lookup Zone در 2 جا می باشد 1)Clustering 2)Emailserver

وقتی شروع به ساختن زونی می کنیم (فرقی بین Reverse وForwardنیست) تبدیل به 3دسته خواهد شد:

Primary-Secondary-Stub

زمانی که برای اولین بار در داخل DNS زونی می سازیم باید از نوع Primary باشد.

تمامی زونها باید اسم داشته باشد مانند Ali.com یا Ali.Ali یعنی باید بر اساس اسم.اسم باشد.

- Secondary : DNS سرور Backup می باشد ،زمانی که ما یک DNS سرور داریم(Primary ) باید یک سرور دیگر هم به عنوان Backup این سرور داشته باشیم که به آن Secondary گویند.
- اگر در شبکه ایDNSآن به نام Ali.com بود(ازنوعPrimaryمی باشد)Backup DNS آن هم باید Ali.com ولی از نوع Secondary باشد.
- تمامی اسامی که در زون Primary باشد در زون پشتیبانش Secondary هم خواهد آمد.
- زون Secondary فقط Read Only می باشد .
- در زون Primary هرچی بسازیم در زونSecondaryهم ساخته خواهد شد به این حرکت در اصطلاح Zone Transferring گویند.
- Stub هم یک سرور پشتیبان دیگر DNS می باشد که اطلاعات از روی زون Primary بر روی آن کپی می شود تفاوت این زون با زون Secondary در این است که در زون Stub فقط اسامی سرورها ذخیره می شوند ولی در زون Secondary علاوه بر اسامی سرورها اسامی بقیه کامپیوتر ها هم ذخیره می شود.

FarshidAjabnoush

زون ها از لحاظ دیگر به 2 دسته تقسیم می شوند

1) Active Directory Integrated Zone
2) Standard Zone

اگر شبکه ما دارای اکتیو دایرکتوری بود زون های ما باید از نوع اول باشد و اگر اکتیو دایرکتوری نداشتیم(WorkGroup بود) باید از نوع دوم باشد.

- اگر زون از نوع اول باشد اطلاعات زون در دیتا بیس اکتیو دایرکتوری که اسم آن NTDS.DIT می باشد ذخیره می شود.
- اگر زون از نوع دوم باشد اطلاعات زون در پوشه ای به نام DNS در System 32 ذخیره می شود.
- به اطلاعاتی که در داخل زون ها نوشته می شود Record گویند.

مهمترین Record ها:

1) A record=Host A : کار این رکورد تبدیل اسم به Ipاست.
- Dynamic Update (DDNS=Dynamic Dns ): برای اینکه دستی A record تنظیم نکنیم از این روش استفاده می کنیم که بصورت اتوماتیک این کار را انجام می دهد،به شرط اینکه Dynamic Update فعال باشد.
2) PTR record (Pointer ) : کار این رکورد تبدیل IP به اسم است.
3) MX record (Mail Exchanger ): نشان دهنده ایمیل سرور همان شبکه.
4) NS record ( Name Server ) : نشان دهنده DNS شبکه .
5) SRV record (Service ) : کدام کامپیوتر کدام سرویس را به شبکه ارائه می دهد.
6) C NAME record : برای اینکه اسامی کامپیوتر ها در اینترنت با هم تداخل نداشته باشد باید یک اسم مستعار برای آنها در نظر بگیرند،که در اینترنت این اسم WWW است، به اسم مستعار C NAME record گویند.

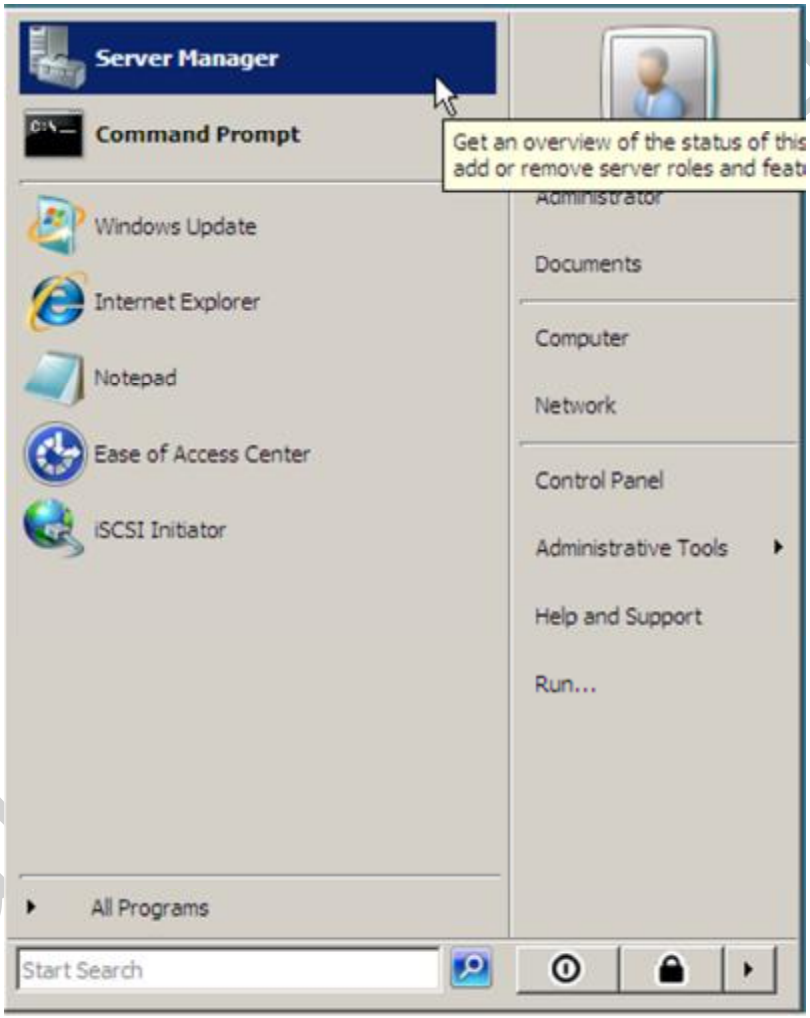
- اسم مستعار تمامی سرورهای وب دنیا WWW می باشد.

FarshidArabnoush

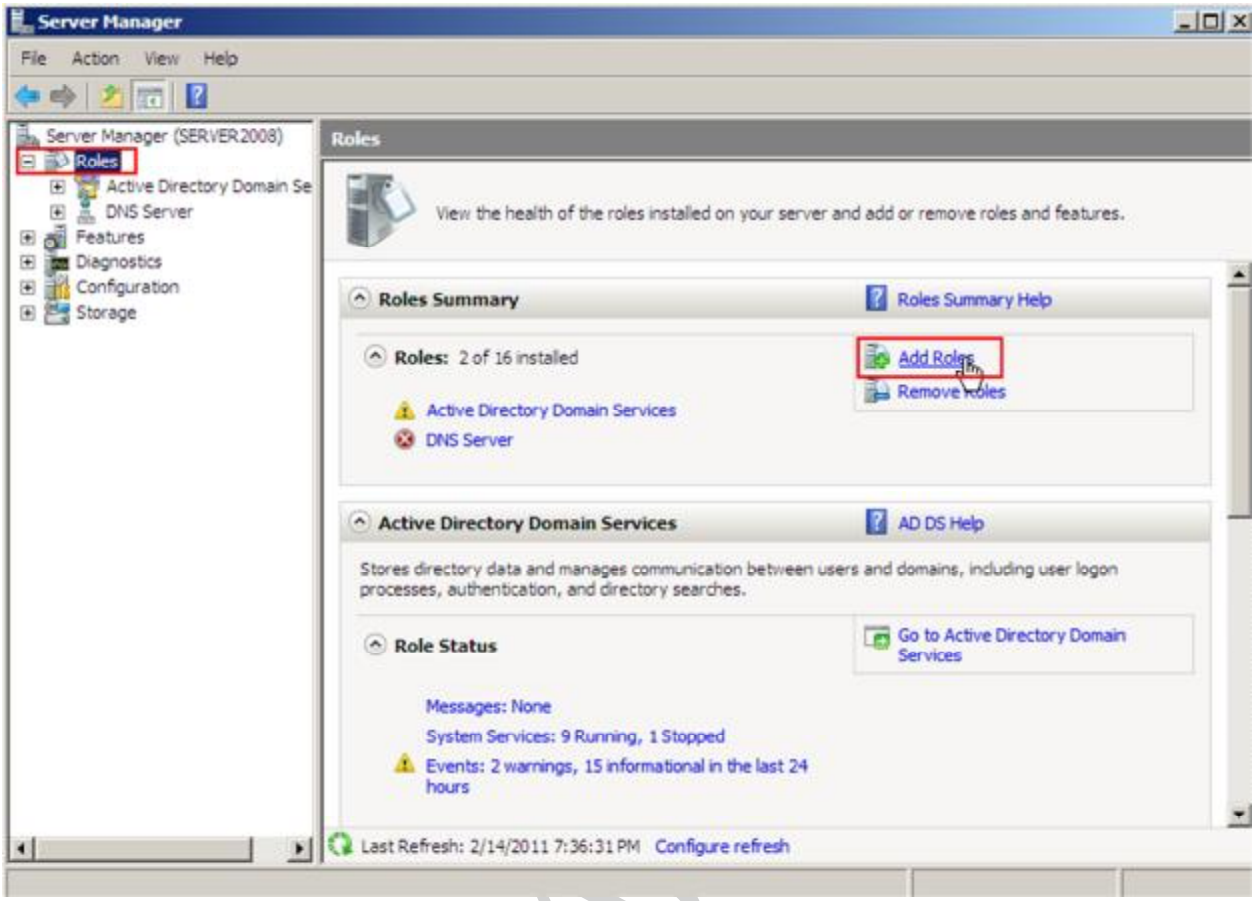
7) SOA record: وقتی سرور DNS نصب می کنیم یک دیتابیس کلی برای خودش میسازه ,SOA محل قرارگیری(از ابتدا تا انتها) هر زون را داخل دیتا بیس مشخص می کند.

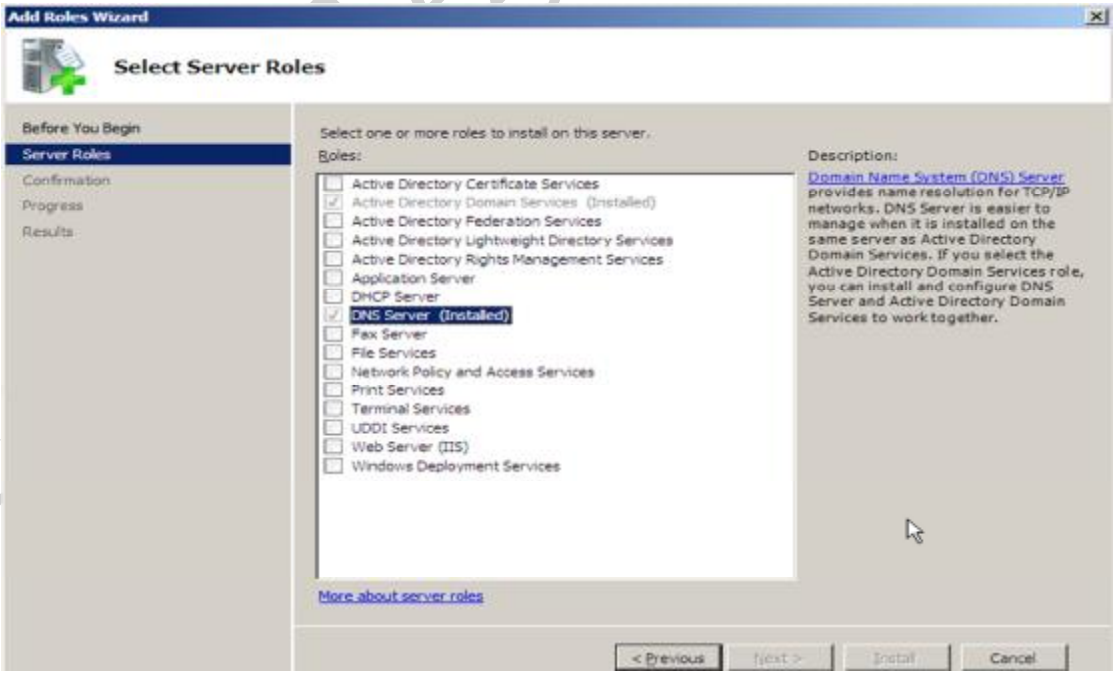
- هر وقت داخل DNS زونی ساخته می شود به صورت اتوماتیک یک SOA record و یکNS recordداخل آن زون اضافه می شود.

نصب DNS :




Fa sh

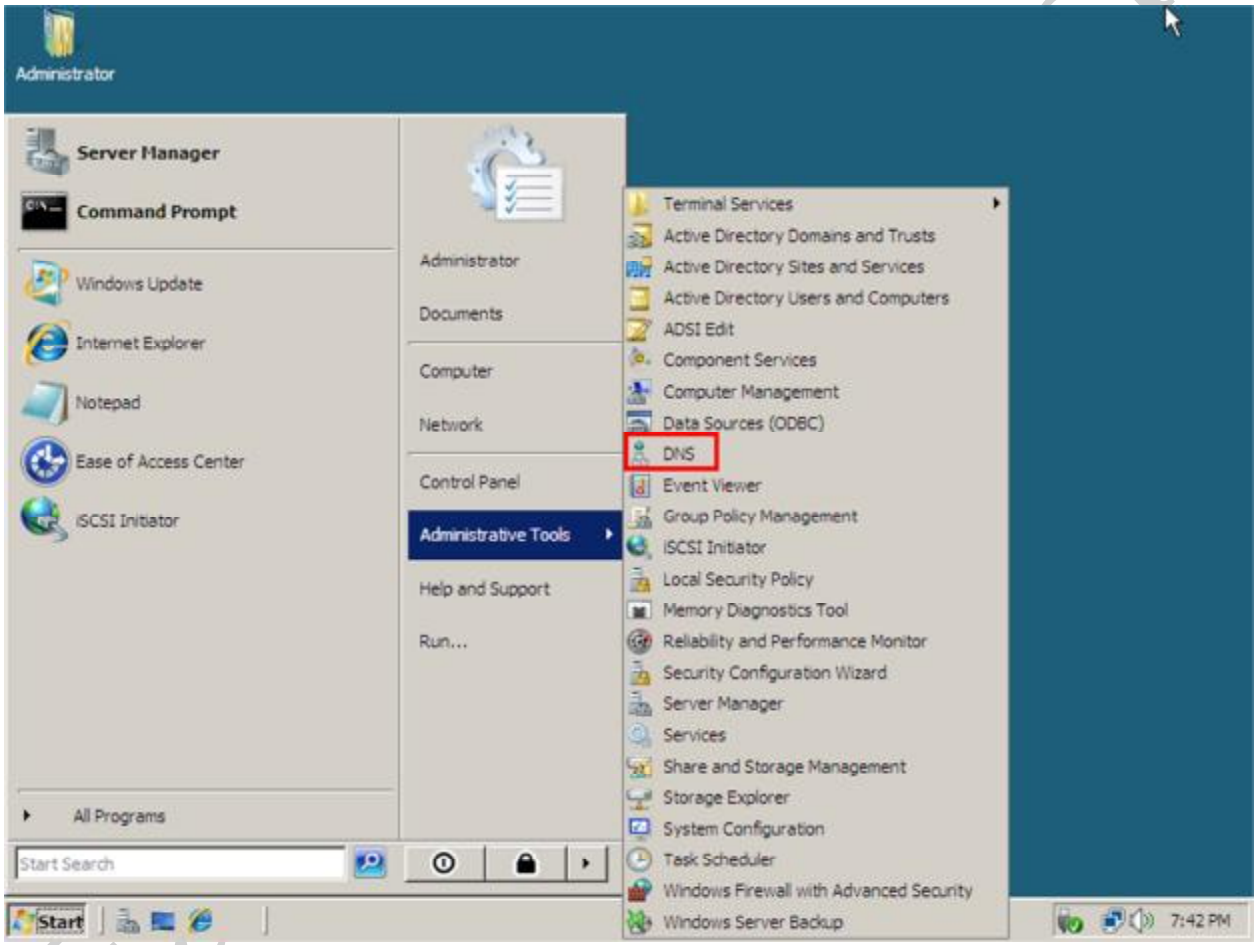

Server Manager
File Action View Help
Server Manager (SERVER2008)
Roles
Active Directory Domain Se
DNS Server
Features
Diagnostics
Configuration
Storage
Roles
View the health of the roles installed on your server and add or remove roles and features.
Roles Summary
Roles Summary Help
Roles: 2 of 16 installed
Add Roles
Remove Roles
Active Directory Domain Services
DNS Server
Active Directory Domain Services
AD DS Help
Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.
Role Status
Go to Active Directory Domain Services
Messages: None
System Services: 9 Running, 1 Stopped
Events: 2 warnings, 15 informational in the last 24 hours
Last Refresh: 2/14/2011 7:36:31 PM Configure refresh


Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
Confirmation
Progress
Results
Select one or more roles to install on this 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 Services
Network Policy and Access Services
Print Services
Terminal Services
UDDI Services
Web Server (IIS)
Windows Deployment Services
Description:
Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.
More about server roles
< Previous
Next >
Install
Cancel

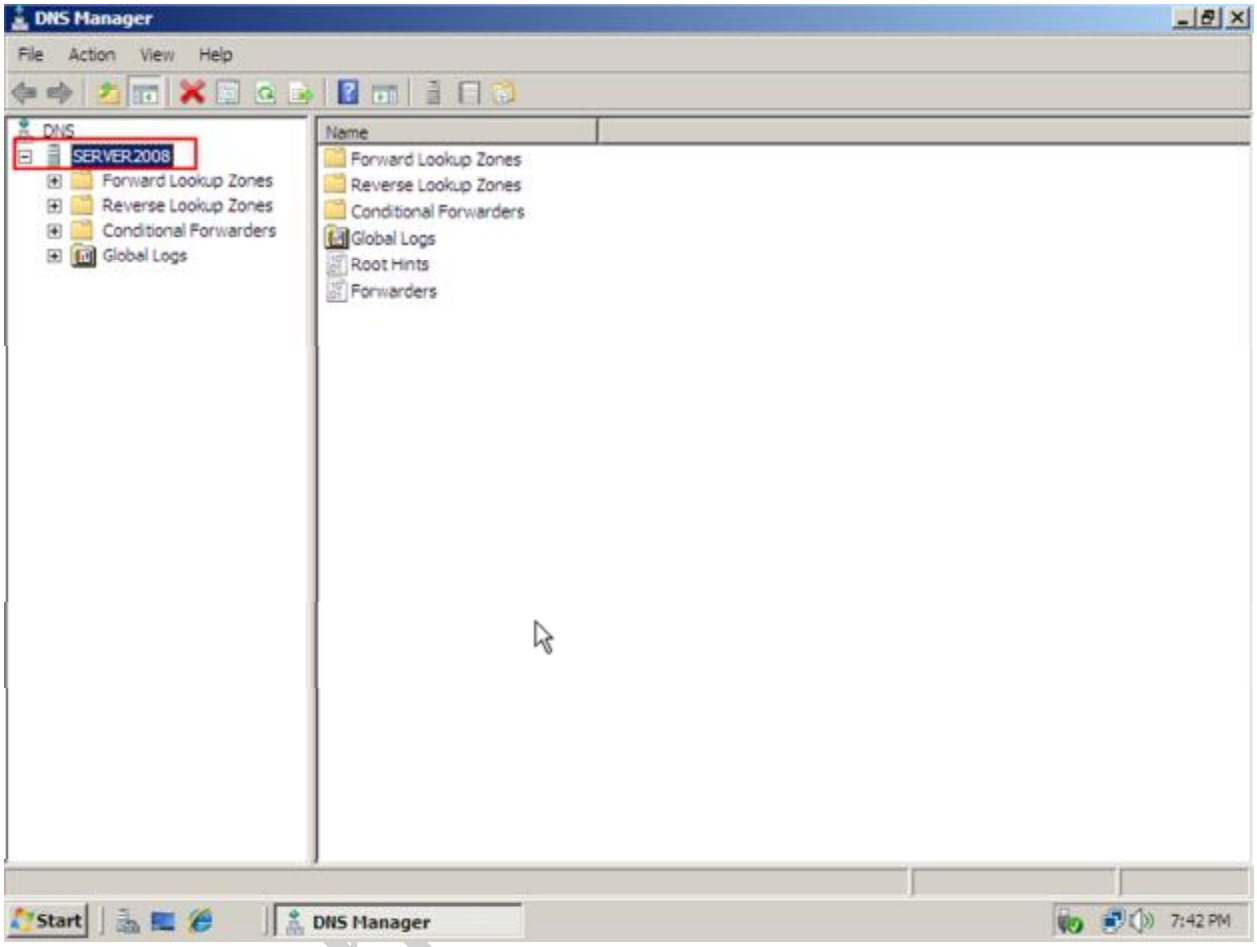
- اگر اکتیو دایرکتوری را نصب کرده باشیم دیگر احتیاجی به نصب دستی DNS نداریم چون بصورت اتومات توسط اکتیو نصب شده است(شکل3-بالا)

بعد از نصب DNS اولین کار ساختن زون است و دومین کار ساختن Record

ساختن زون:

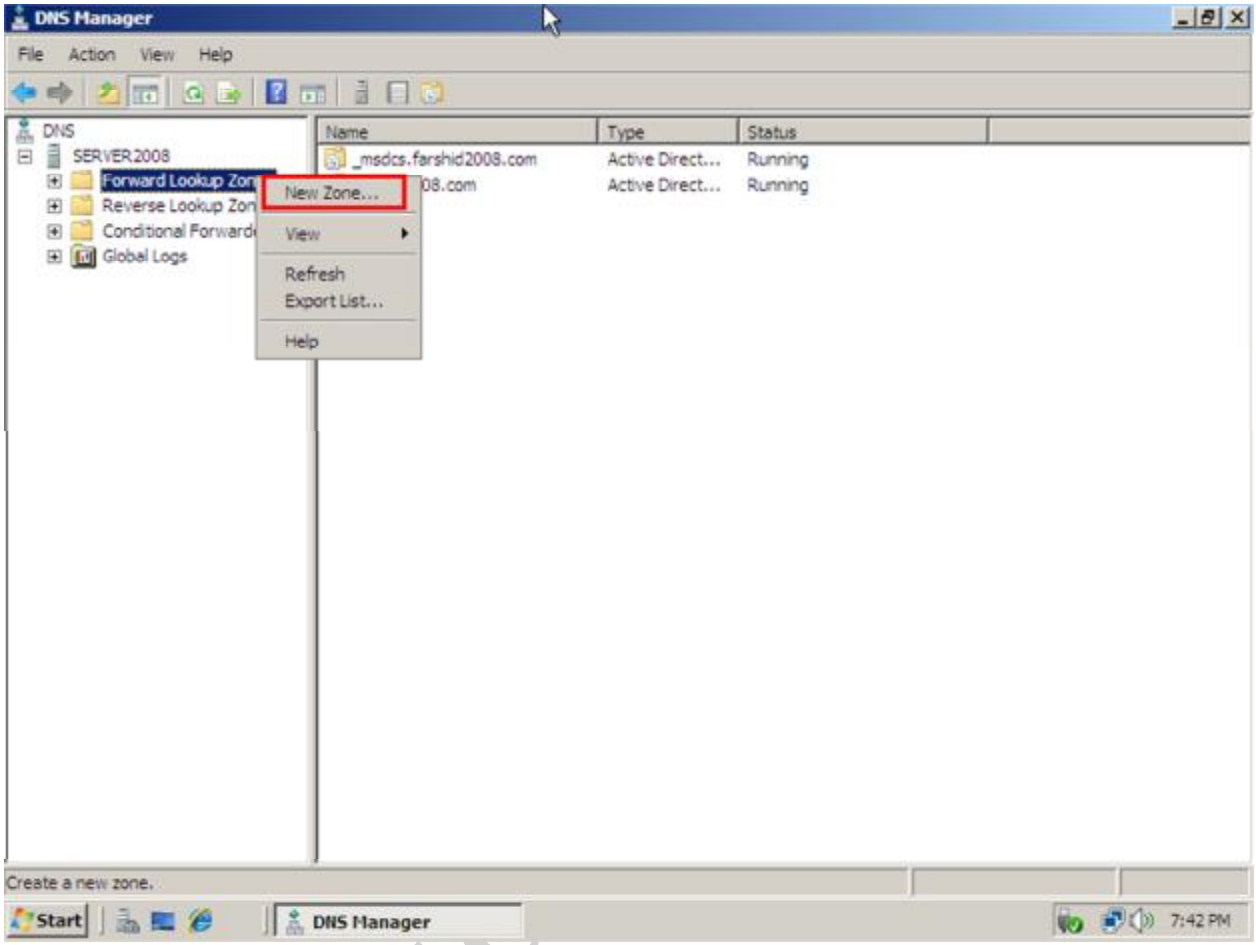


بر روی اسم کامپیوترمان کلیک می کنیم




Farsi

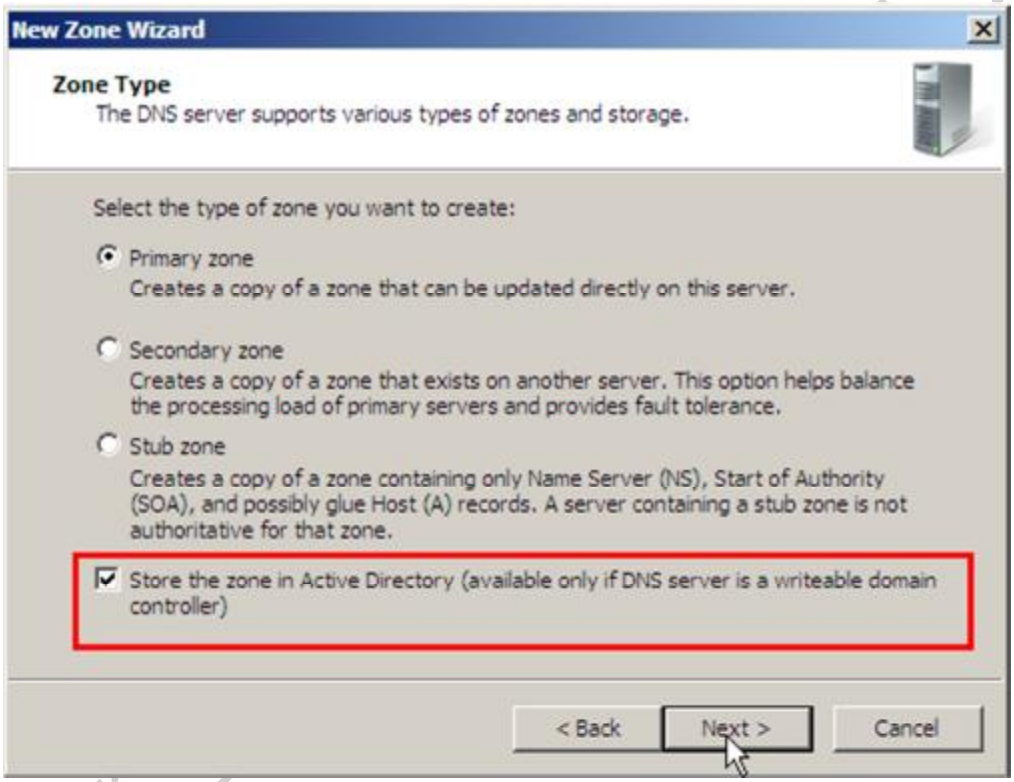
کلیک راست بر روی Forward Lookup Zone




Farshid

1) اگر اولین زونی است که داخل یک شبکه می سازیم(مانند Ali.com ) باید از نوع Primary باشد،اگر اکتیو دایرکتوری داشته باشیم گزینه آخر برایمان فعال می شود که اگر آن را انتخاب کنیم زون ما از نوع Active Directory Integrated Zone

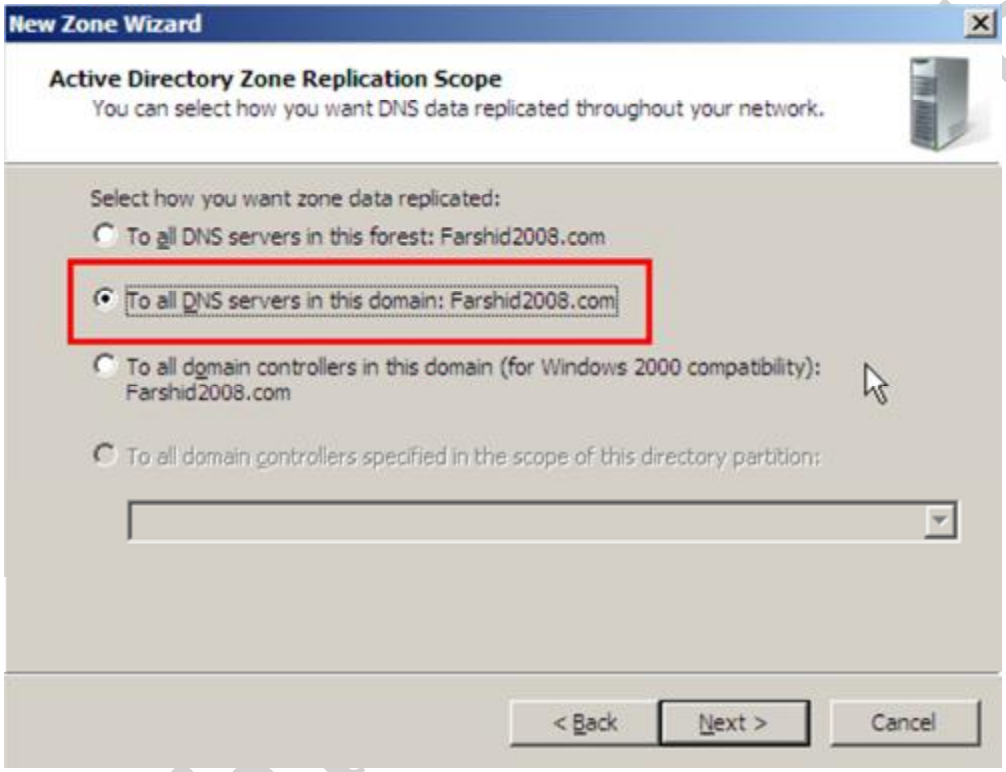
می شود واگر تیک این گزینه را برداریم زون ما از نوع Standard می شود.




Farsh

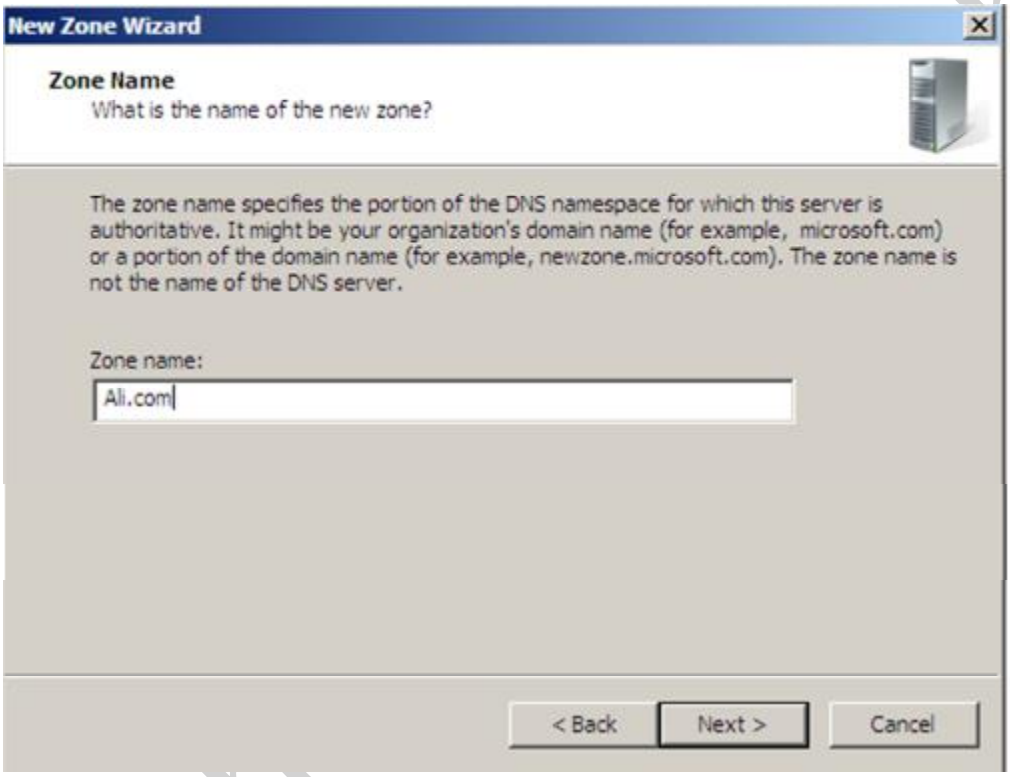
**در اینجا سؤالی پرسیده می شود که می گوید اجازه دارم که اطلاعات این زون را به بقیه DNS سرورها بدهم؟**

**در جواب باید گزینه وسط را انتخاب کنیم بدین معنی که اطلاعات این زون به DNS سرورها یی داده شود که فقط در این شعبه وجود دارند .**



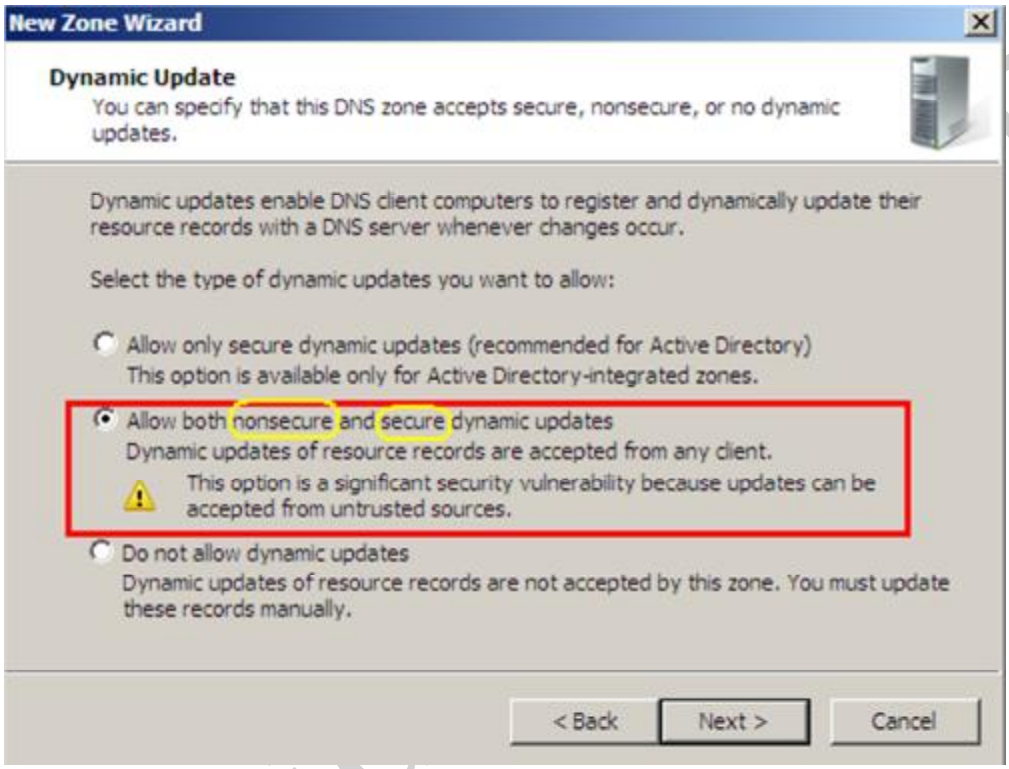

Farshid

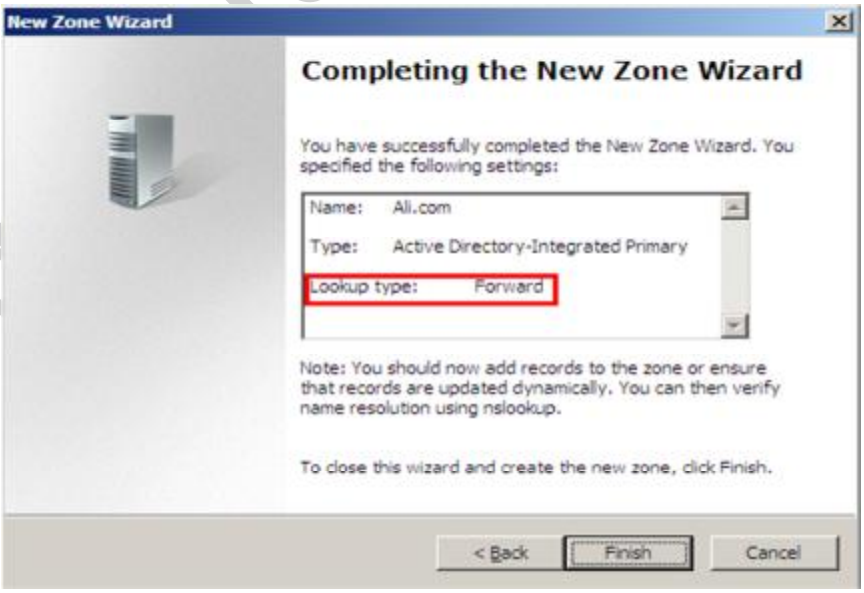
سپس اسم زون را می نویسیم



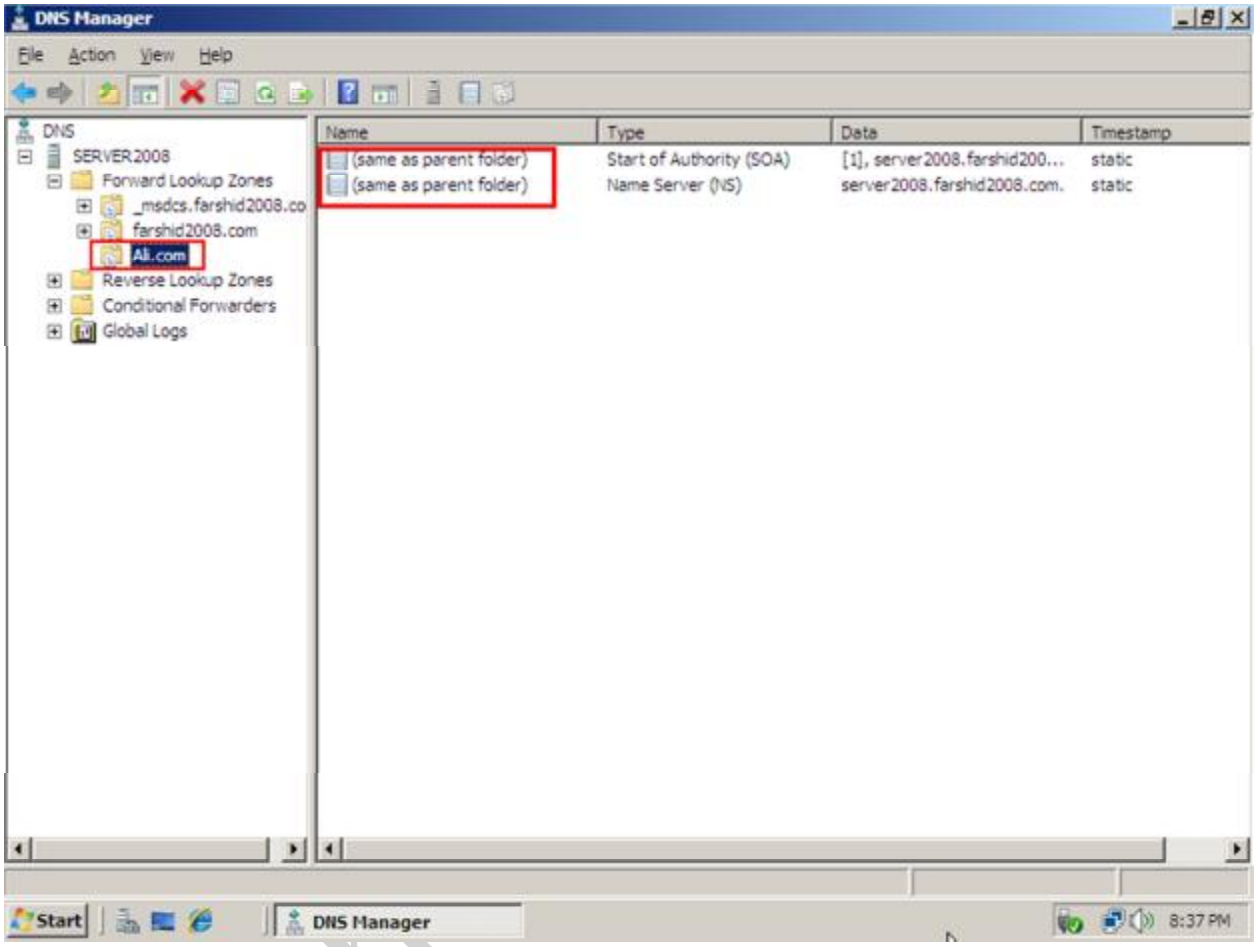

Farsi

در صفحه Dynamic Update کاری می کنیم که کلاینت ها بصورت اتوماتیک اسم خودشون را اضافه کنند،بهترین حالت در این صفحه عبارت وسط می باشد که می گوید تمام کسانی که عضو این دامین هستند (Secure ) و کسانی که عضو این دامین نیستند(None Secure ) مانند Workgroup ها بتوانند عضو این زون بشوند. ( امنیت بالایی دارد )



وارد زونی که ساختیم می شویم(Ali.com ) به صورت پیش فرض 2 رکورد ساخته شده اند



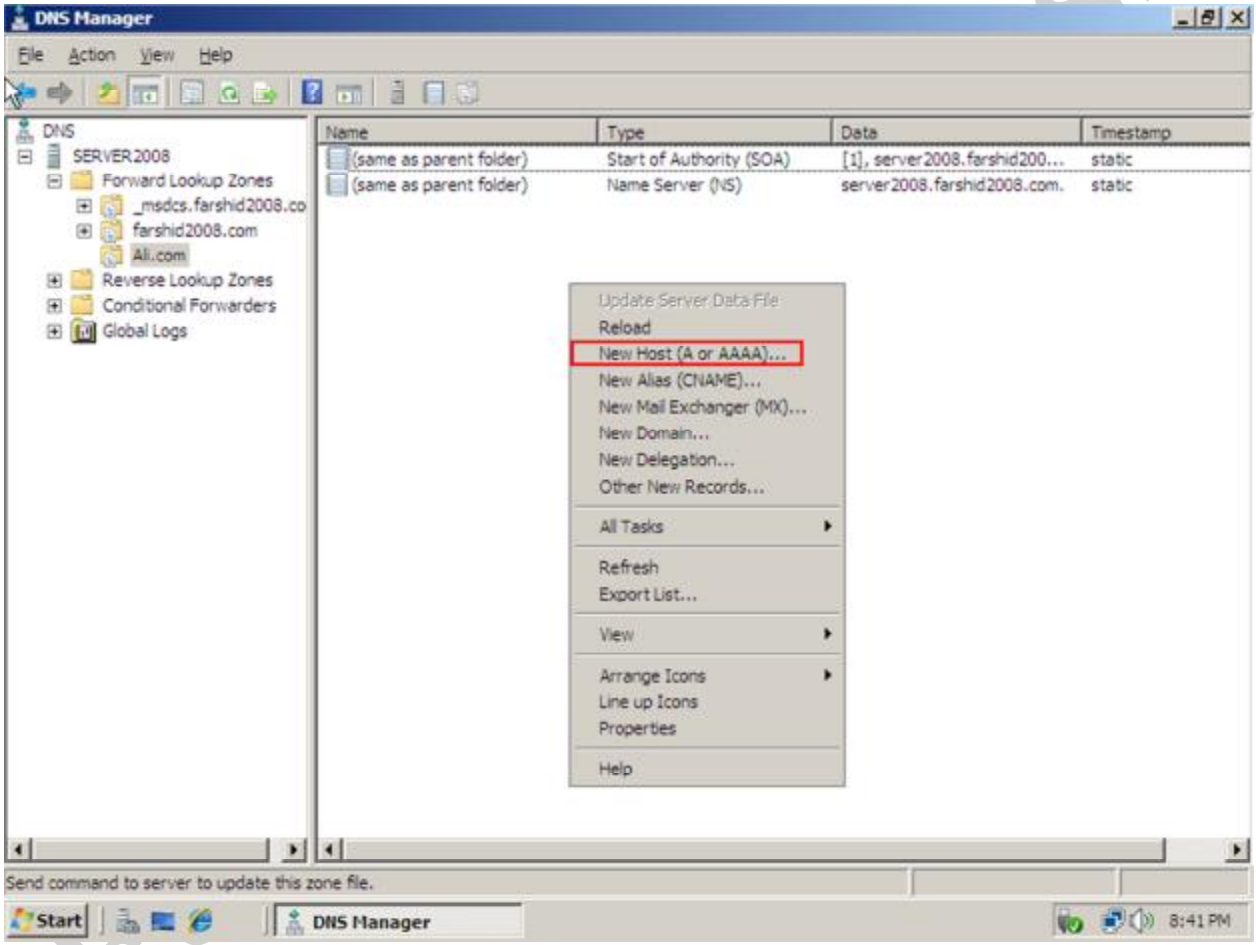

Farsh

همیشه باید 2 رکورد هم به صورت دستی بسازیم 1- A record 2- CNAME record

بر روی جای خالی کلیک راست می کنیم و گزینه( New Host ( A or AAAA را می زنیم

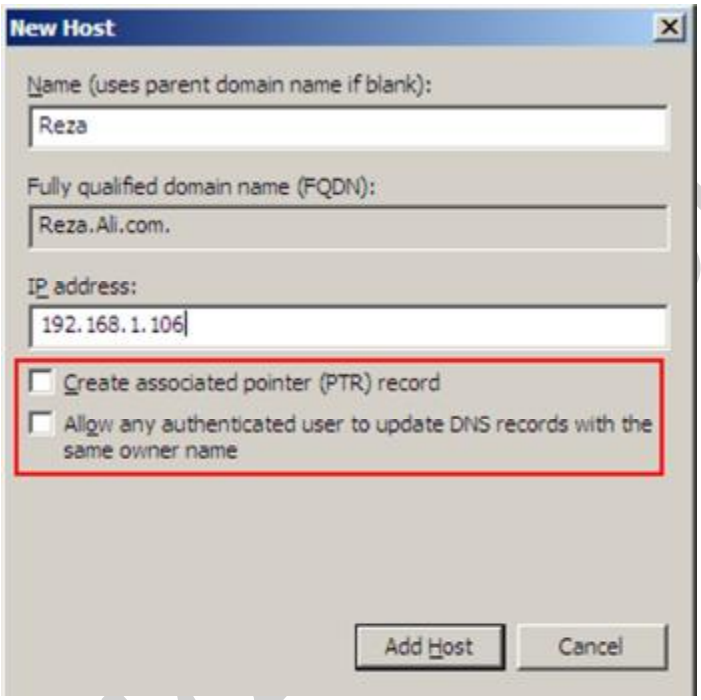
A: یعنی Ip ورژن4AAAA: یعنی Ip ورژن 6

یعنی اسم تبدیل می شود به Ip ورژن4 یا6



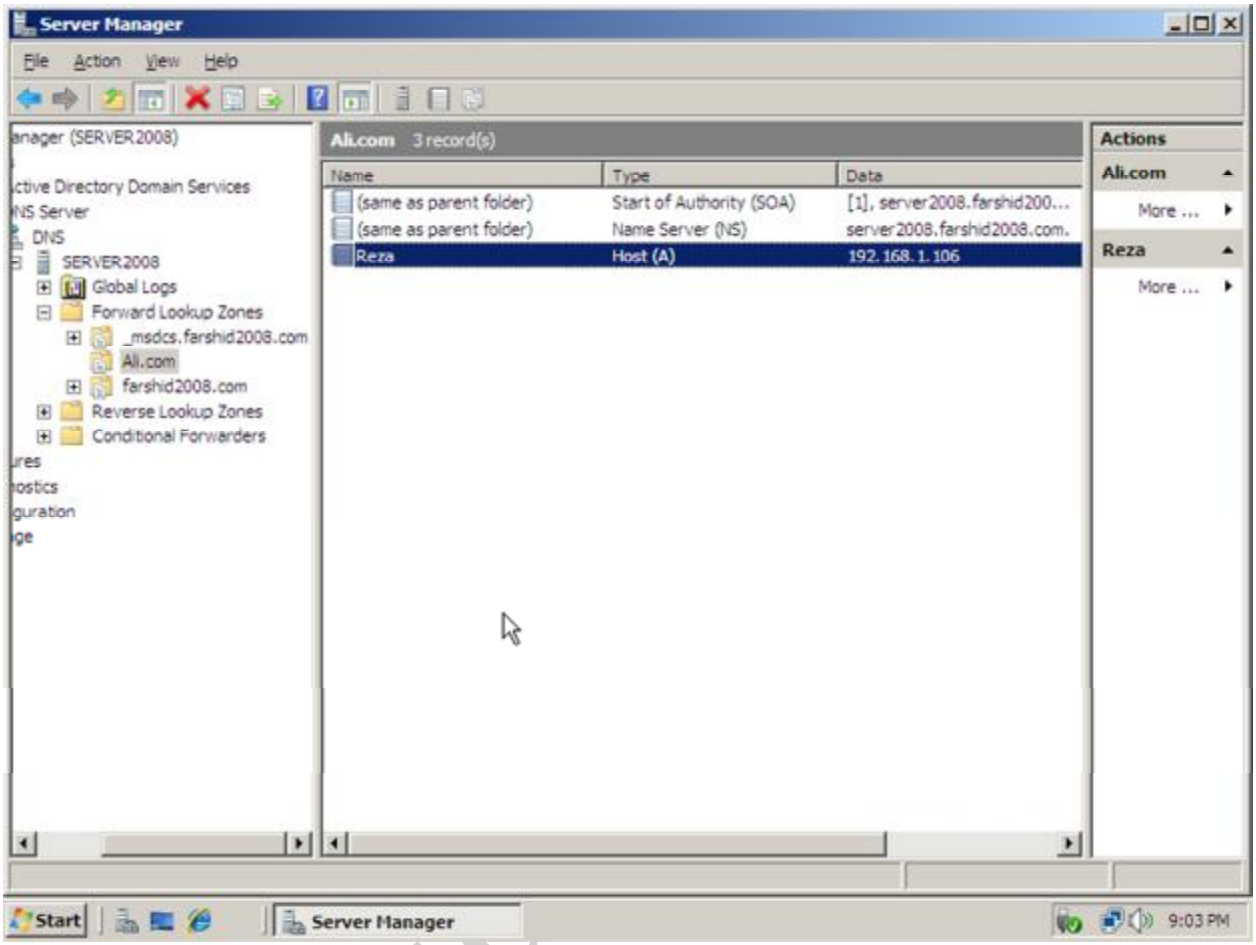
در اینجا باید اسم کامپیوتری را که می خواهیم به آن وصل شویم را به همراه Ip آن وارد کنیم.

هیچ کدام از گزینه ها را تیک نمی زنیم،گزینه اول می گوید می خواهی برایش PTR بسازم ، انتخاب نمی کنیم چون PTR ساختن احتیاج به یک زون از نوع Revers دارد، گزینه دوم می گوید هر کسی بتواند این رکورد را تغییر دهد.

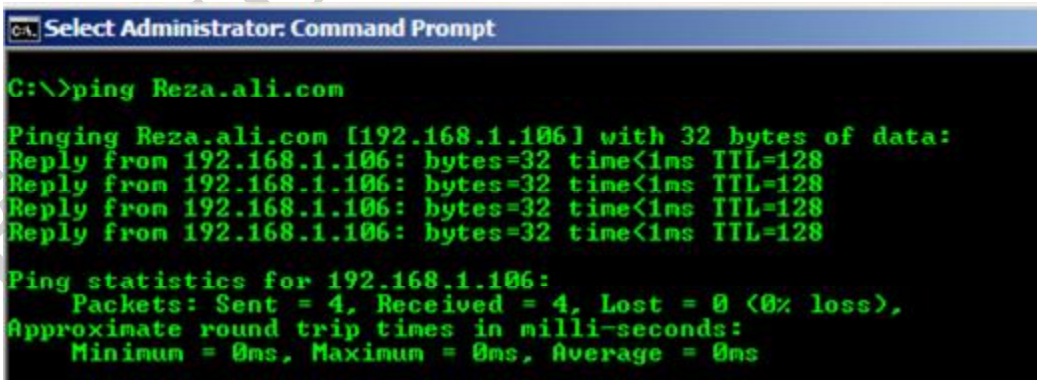


Farshid Roush

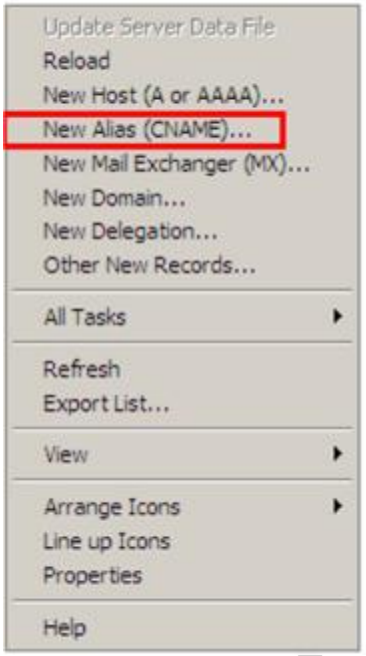
در اینجا می بینیم که اضافه شد




حالا پینگ رضا را به این صورت می گیریم Ping Reza.ali.com

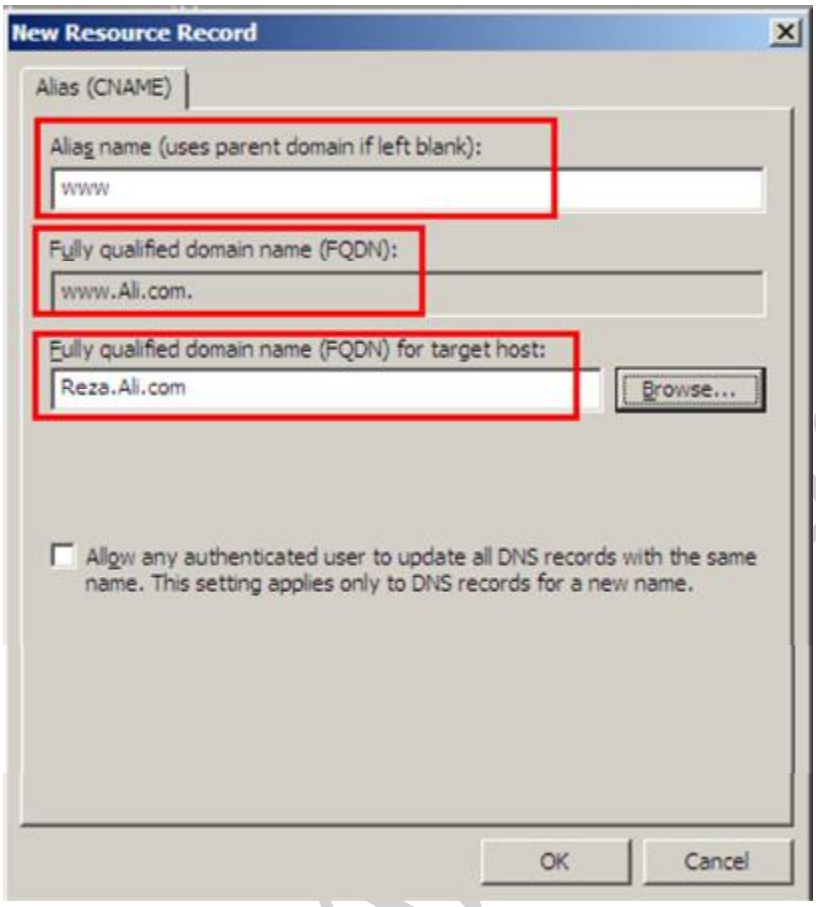


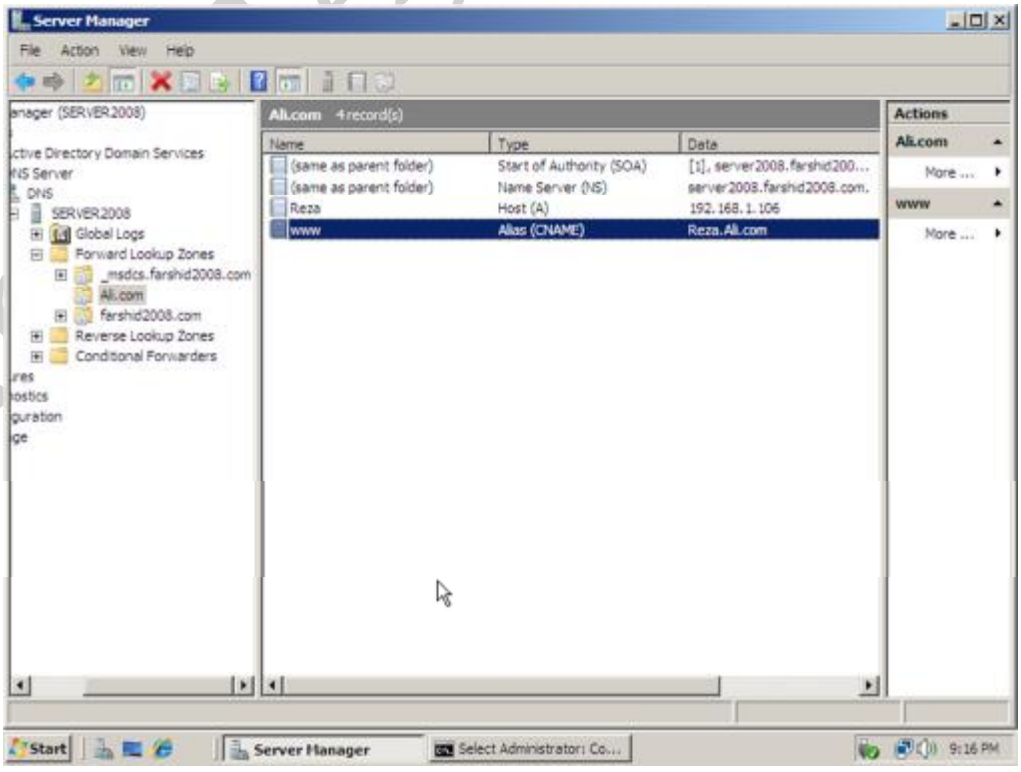
ساختن رکورد CNAME




در کادر اول از ما اسم مجازی را می پرسد که در اینجا ما WWW را وارد می کنیم،در کادر دوم تبدیل به اسم زونمان که Ali.com است می شود،در کادر سوم از ما می پرسد این اسم مجازی برای کدام اسم واقعی است که Browse را می زنیم و Reza را انتخاب می کنیم.

FarshidAjaghoush


New Resource Record
Alias (CNAME)
Alias name (uses parent domain if left blank):
www
Fully qualified domain name (FQDN):
www.Ali.com.
Fully qualified domain name (FQDN) for target host:
Reza.Ali.com
Browse...
Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.
OK
Cancel


Server Manager
File Action View Help
Ali.com 4 record(s)
Name
Type
Data
(same as parent folder)
Start of Authority (SOA)
(same as parent folder)
Name Server (NS)
Reza
Host (A)
192.168.1.106
www
Alias (CNAME)
Reza.Ali.com
Actions
Ali.com
More ...
www
More ...
DNS
SERVER2008
Global Logs
Forward Lookup Zones
_msdcs.farshid2008.com
Ali.com
farshid2008.com
Reverse Lookup Zones
Conditional Forwarders
Start
Server Manager
Select Administrator: Co...
9:16 PM

Farshid

قبل از CNAME ساختن حتماً باید A record را ساخته باشیم.

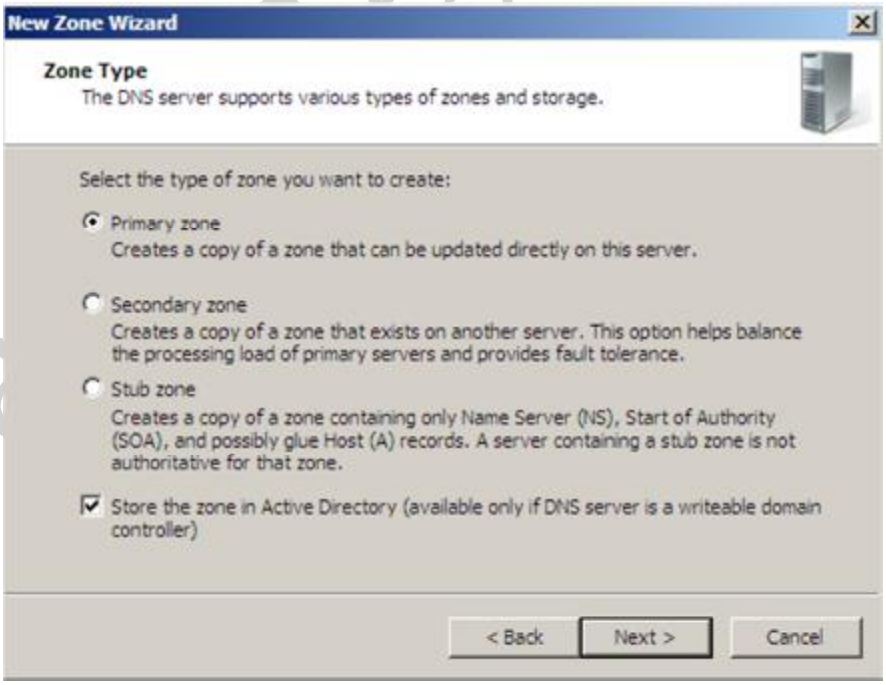
نوبت به پینگ با اسم مجازی می رسد Ping WWW.Ali.com که خودش بصورت اتوماتیک اسم مجازی را تبدیل به اسم واقعی می کند یعنی Reza.Ali.com [192.168.1.106 ]

```
C:\>ping www.ali.com

Pinging reza.ali.com [192.168.1.106] with 32 bytes of data:
Reply from 192.168.1.106: bytes=32 time=14ms TTL=128
Reply from 192.168.1.106: bytes=32 time<1ms TTL=128
Reply from 192.168.1.106: bytes=32 time=6ms TTL=128
Reply from 192.168.1.106: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.106:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 5ms
```

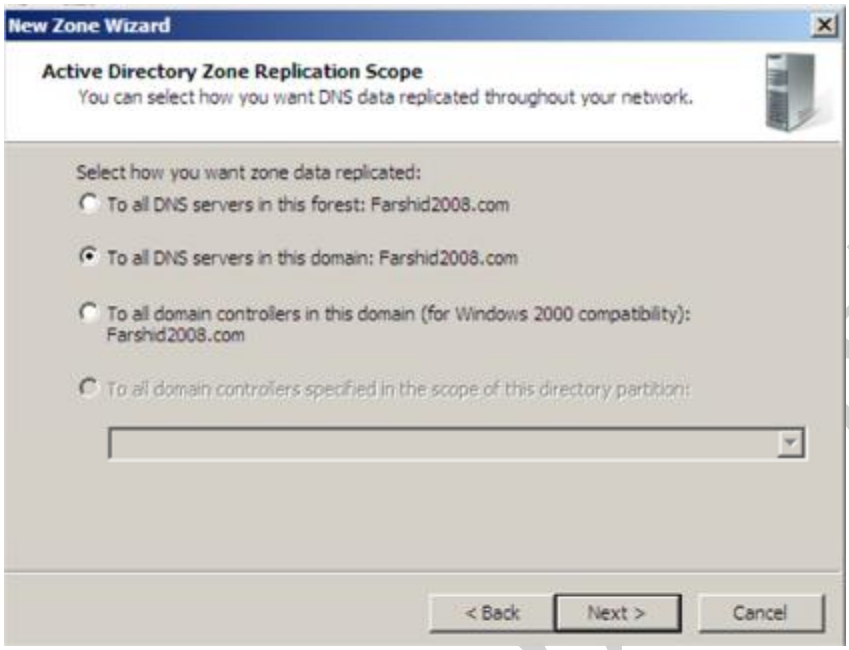
ساختن Reverse Lookup Zone :

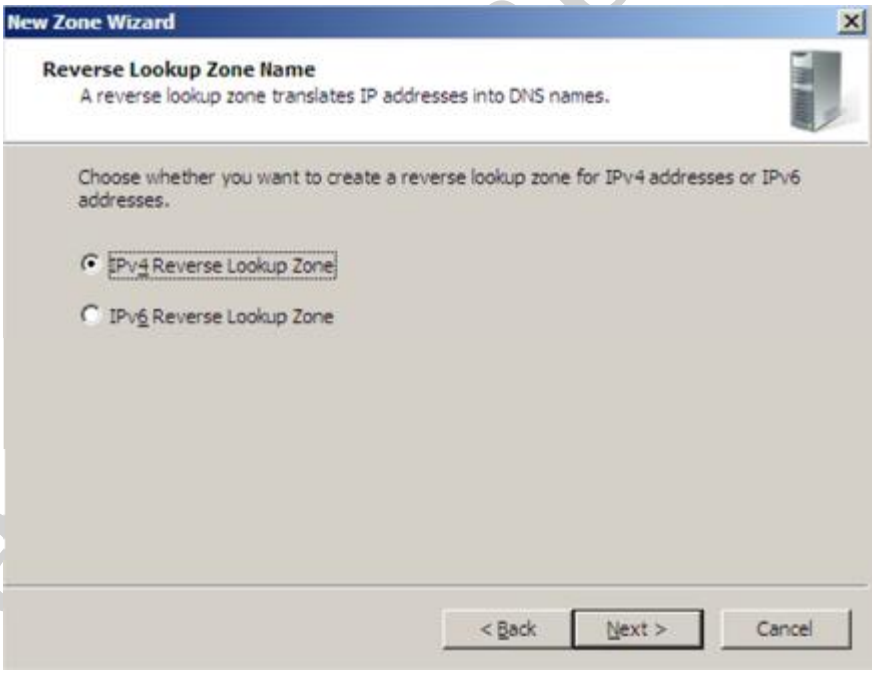
روی Reverse Lookup Zone کلیک راست و New Zone

در مرحله بعد باید Primary را انتخاب کنیم چون اولین باری است که Reverse Lookup Zone می سازیم.



تمامی مراحل مانند ساختن زون Forward است

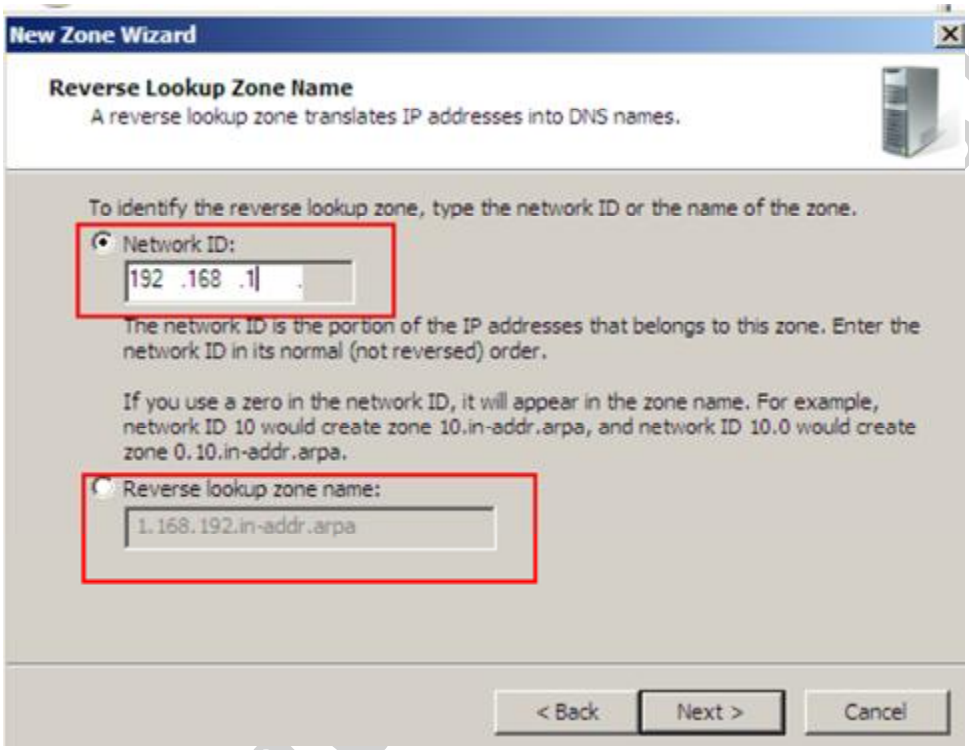


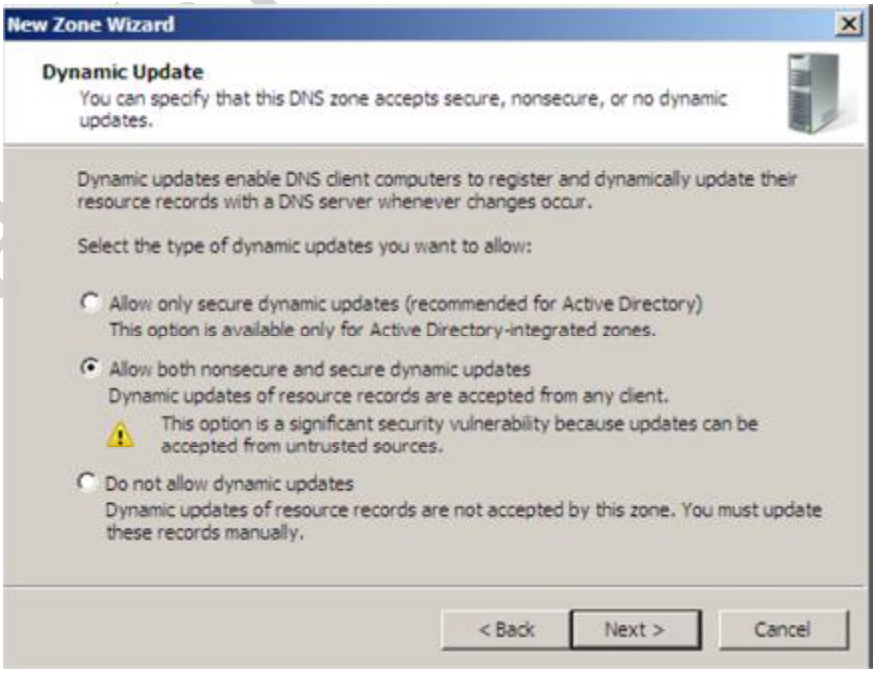




در مرحله سوم از ما سؤال می پرسد که این زون مربوط به چه ورژنی از Ip می باشد ( در اینجا ورژن 4)

در این مرحله از ما Net Id را می پرسد که در اینجا می شود 192.168.1 ، در پایین صفحه اسم Reverse Zone به این صورت ساخته می شود 1.168.192.in-add.arpa (مهم)

Internet Address Arpanet :in-add.arpa

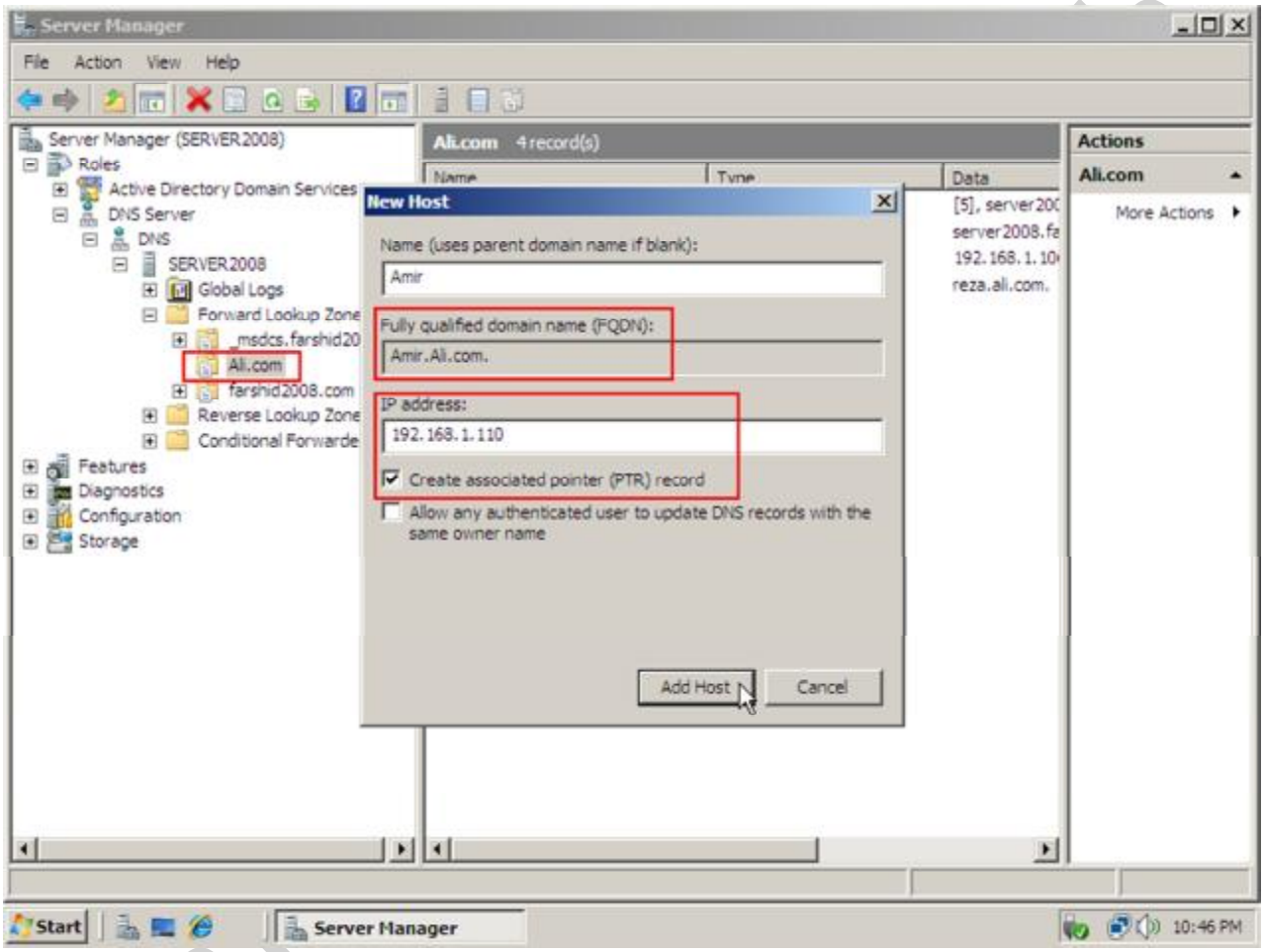


در شکل بالا Dynamic Update را می پرسد که قبلاً توضیح دادیم.

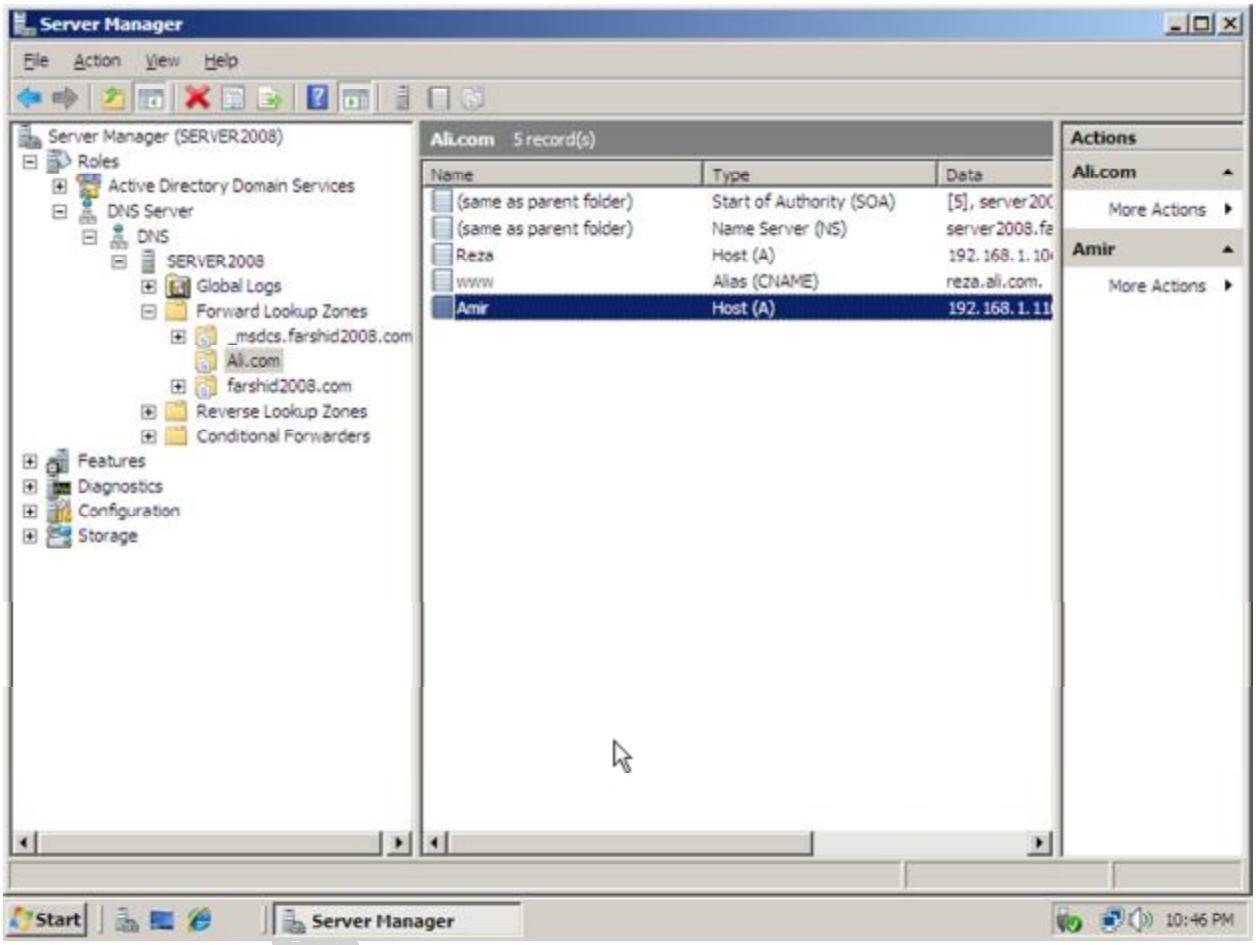
Farshid

وارد Ali.com می شویم یک A record اضافه می کنیم تا PTR هم بسازیم، اسم این A record را Amir می گذاریم و Ip آن 192.168.1.110 است و تیک PTR هم می زنیم



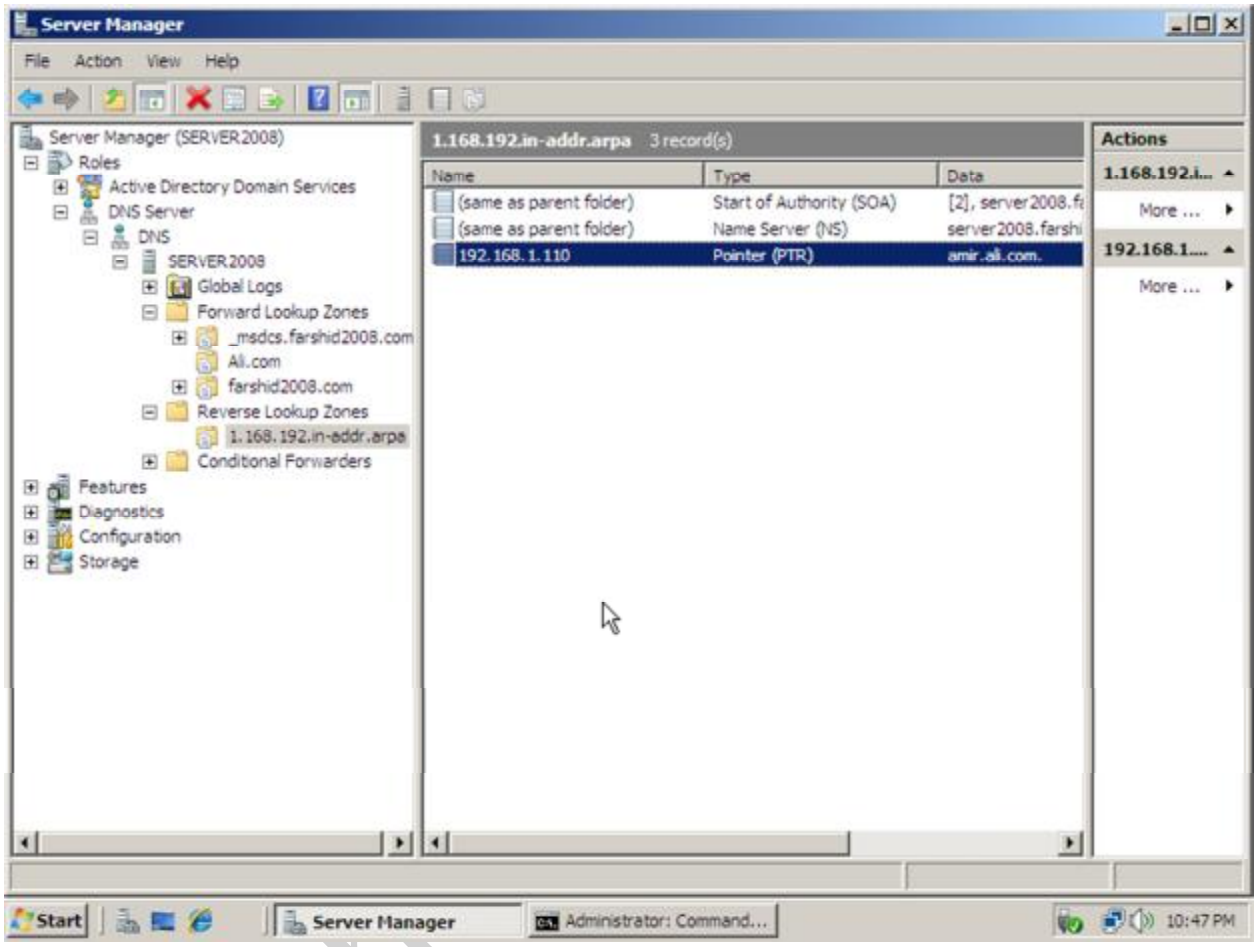

Far

**در اینجا می بینید که ساخت**




Fars

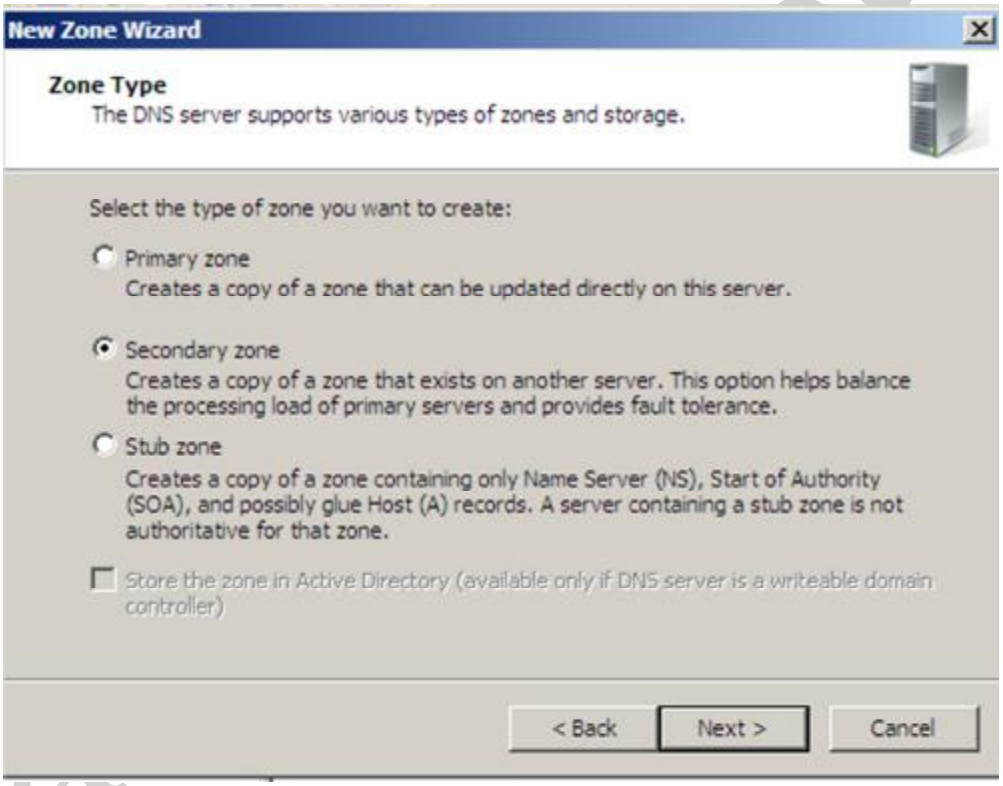
حالا در Reverse Zone هم چک می کنیم



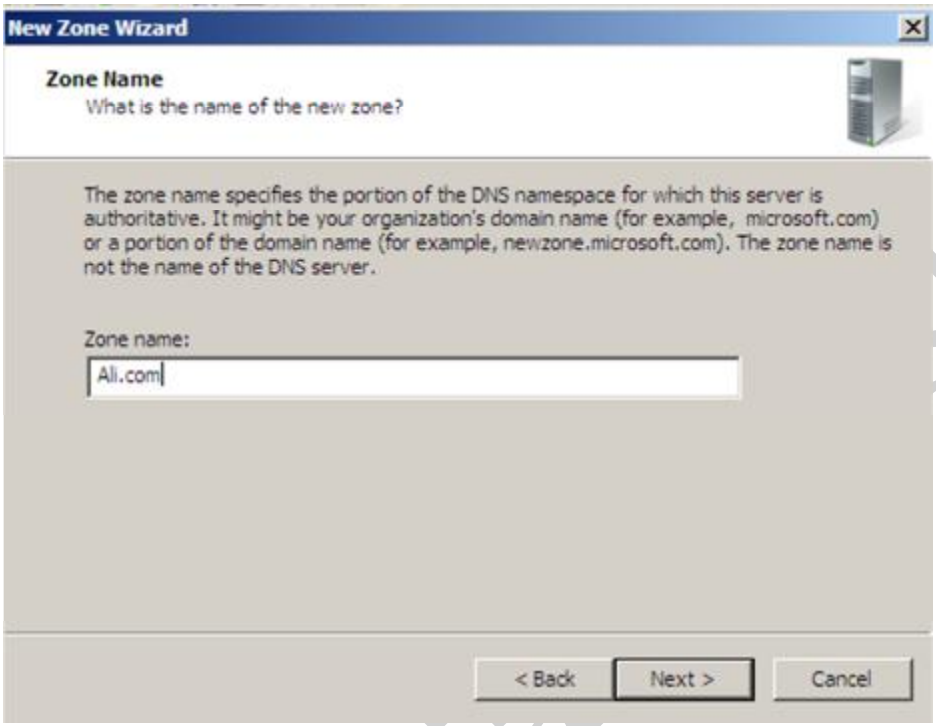

Farsh

- هنگام ساختن این زون در واقع داریم از DNS نسخه پشتیبان تهیه می کنیم (Backup ).
- Secondary Zones را حتماً باید پشت یک سرور دیگر(به غیر از سرور Primary ) ساخت.
- برای ساختن Secondary Zones یک سرور DNS دیگر بالا می آوریم علاوه بر Primary .

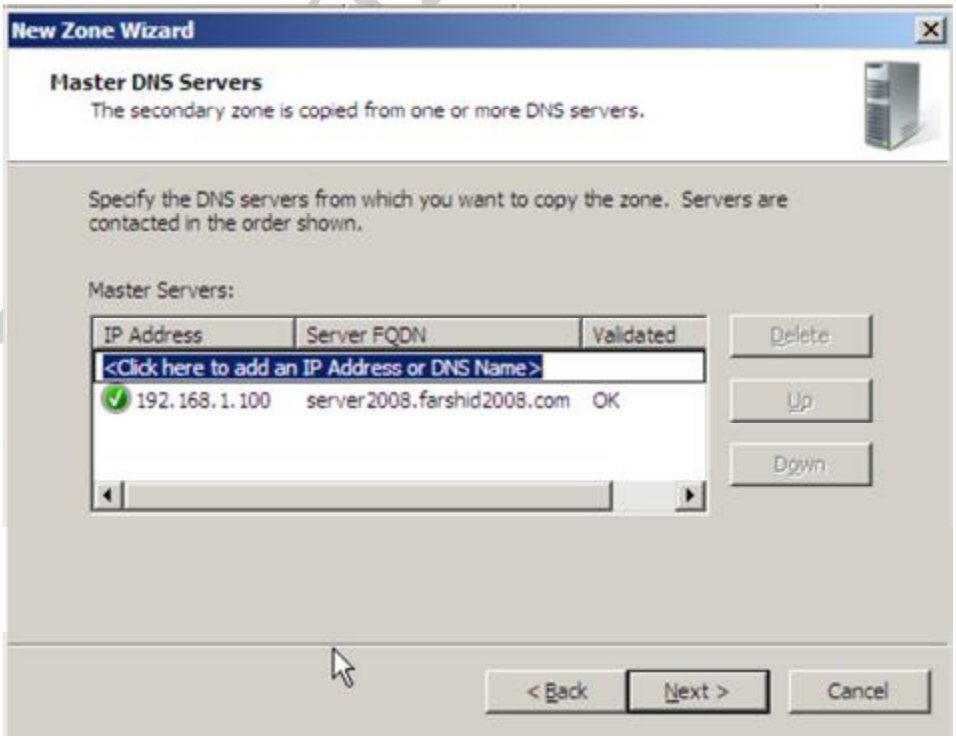
3) در سرور DNS دوم شروع به ساختن Secondary Zones می کنیم,همانطور که در شکل می بینید گزینه Active Directory Integrated Zone غیر فعال است بدین معنی که Secondary Zones ها همیشه از نوع استاندارد زون هستند,دیتا بیس آنها در پوشه DNS در Sytem32 ذخیره می شوند.



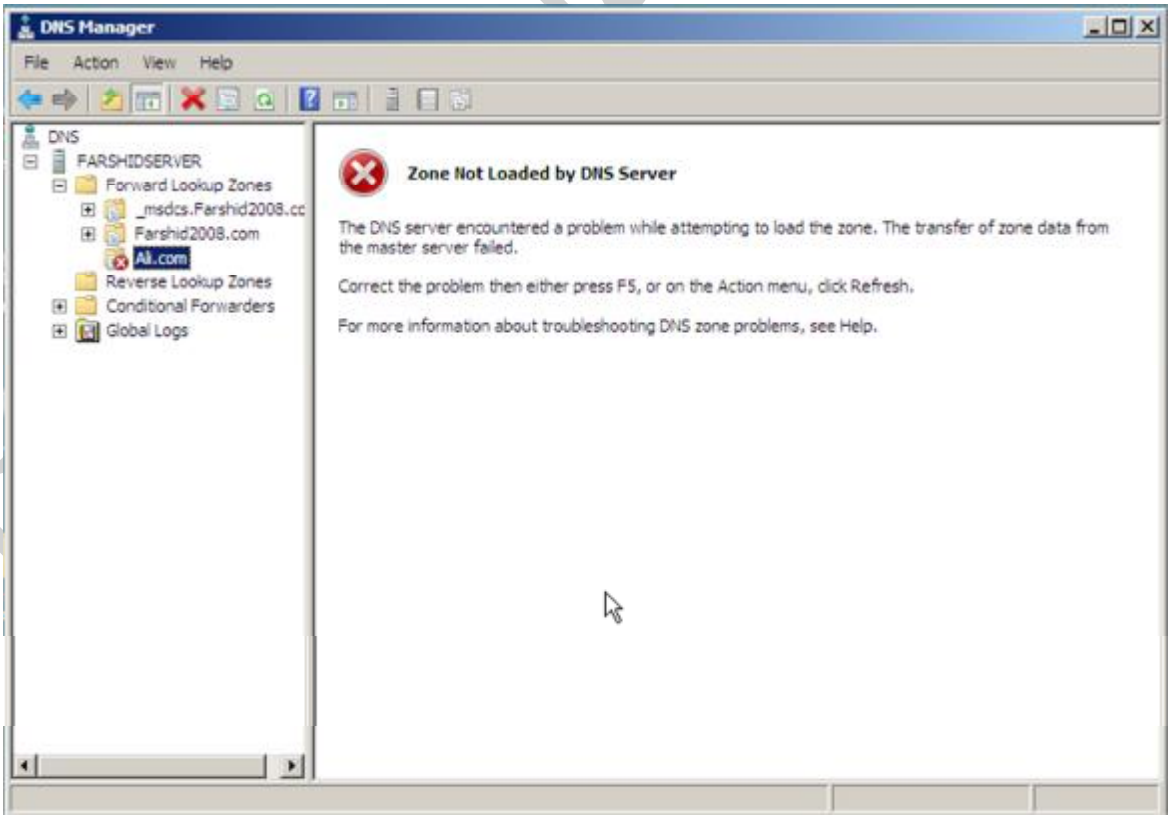
اسم Secondary Zones باید همان اسم Primary Zones باشد.




در این صفحه اسم زون اصلی (Primary Zones یا همان Master ) را از ما می خواهد که Ip, Primary Zones را وارد می کنیم.



و در آخر این زون ساخته شد اگر بر روی این زون کلیک کنیم Error می دهد چون باید در سرور اصلی(Primary )اجازه انتقال اطلاعات (Zone Transfare ) به Secondary داده شود.

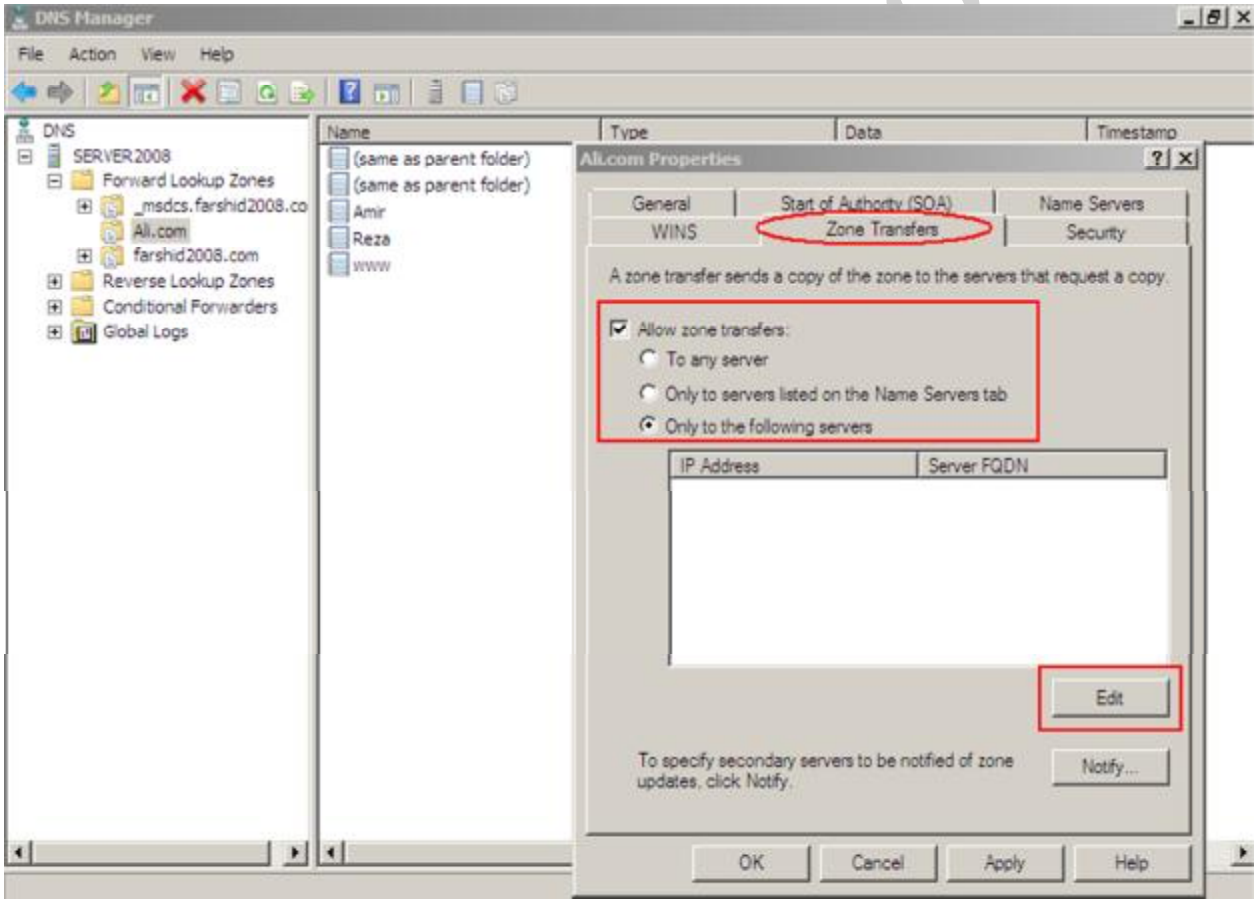


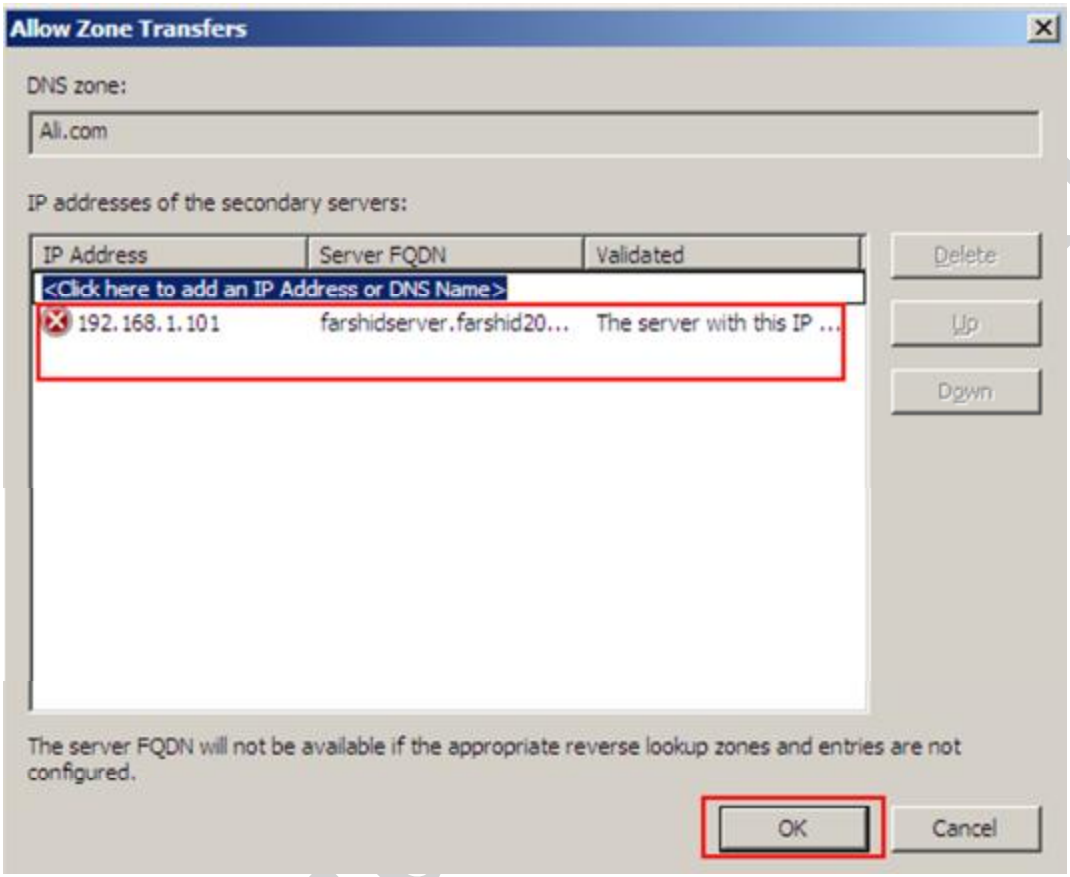
برای صدور اجازه انتقال , بر روی اسم زونمان در Primary Server کلیک راست و گزینه Properties سپس وارد تب Zone Transfers می شویم وگزینه Allow Zone Transfres را فعال می کنیم بعد از فعال سازی این گزینه باید یکی دیگر از این گزینه ها را انتخاب کنیم .

گزینه اول می گوید اطلاعات این زون را به هر سرور دیگری که می خواهد بدهد.(گزینه مناسبی نیست)

گزینه دوم می گوید اطلاعات این زون را فقط به سرورهایی بدهید که اسامی این سرورها در تب Name Serverموجود می باشد, در این تب اسم تمامی DNS سرورهایی که به دامین ما Join شده اند موجود می باشد.

گزینه سوم می گوید اطلاعات این زون را فقط به سرورهایی بدهید که من در اینجا اسامی آنها را وارد می کنم, Edit را می زنیم وIp , Secondry Zones را وارد می کنیم.

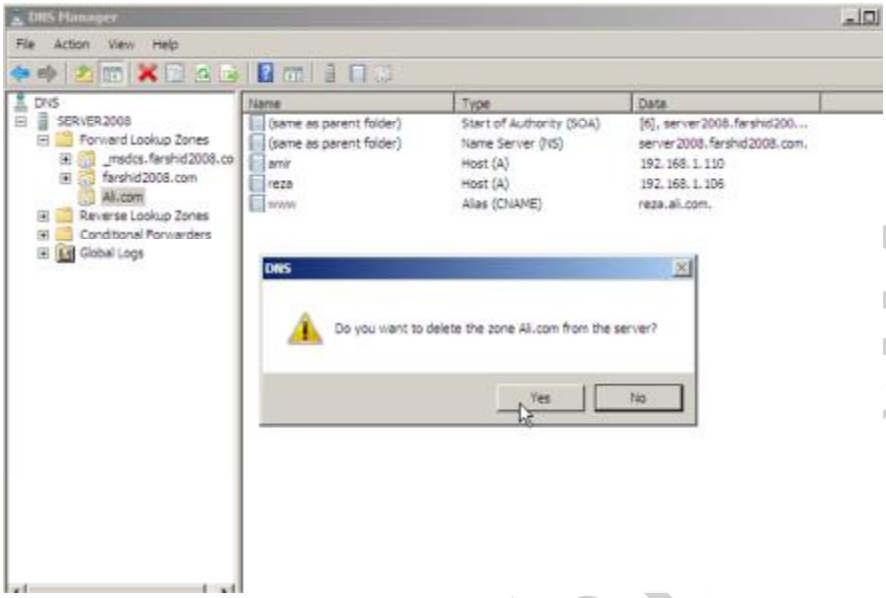




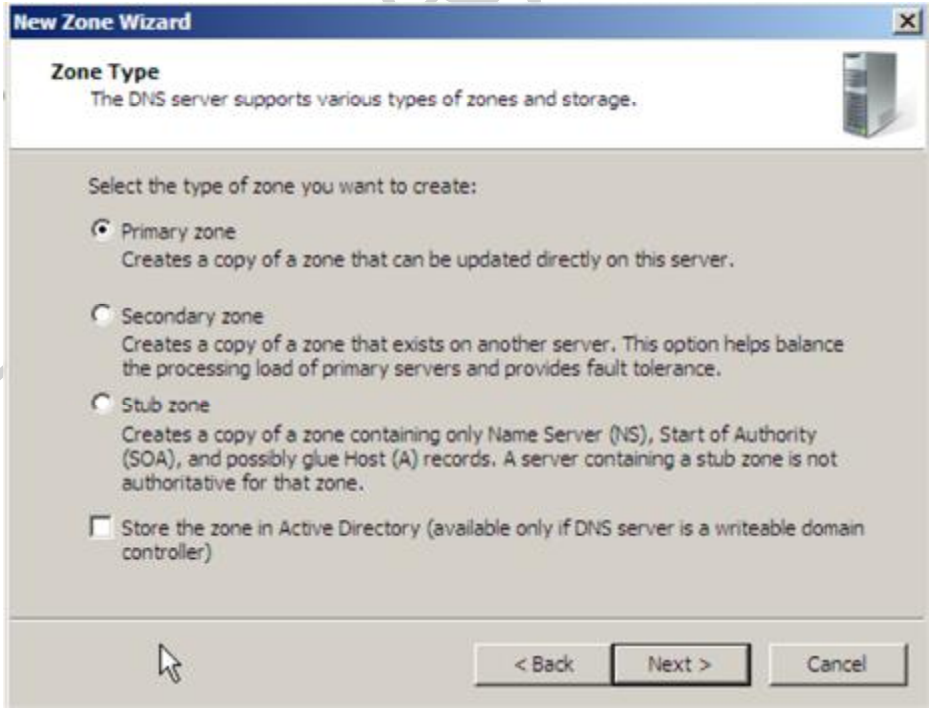

این گزینه (یعنی گزینه3) امنیت پایینی دارد چون هکرها بعد از اسکن سرور Ip را که در اینجا تنظیم کردیم را پیدا می کنند و بر روی کارت شبکه خودشان تنظیم می کنند و به راحتی اطلاعات DNS را کپی می کنند.

بهترین گزینه,گزینه2 می باشد چون در این گزینه گفته می شود اطلاعات بر روی سروری کپی شود که Join به دامین می باشد.

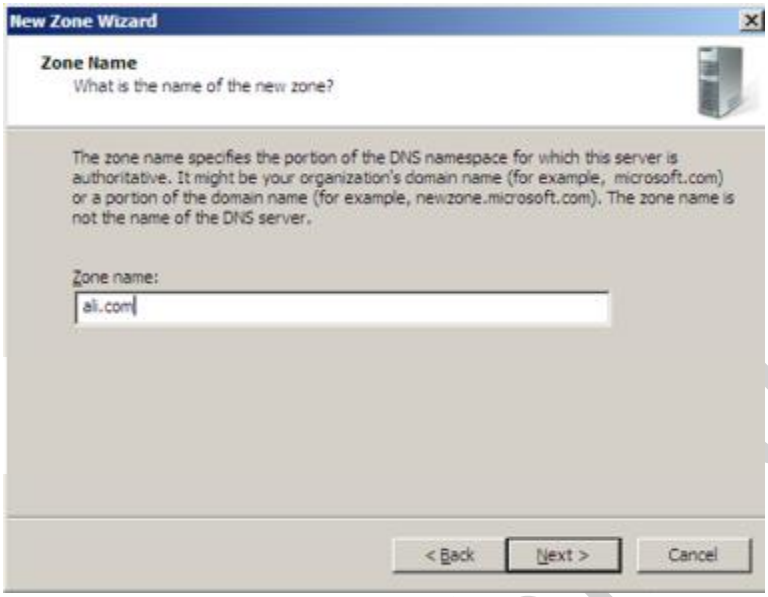
در سرور اصلی ما زونمان را پاک می کنیم و دوباره از زون پشتیبانمان فایلها را بر می گردانیم

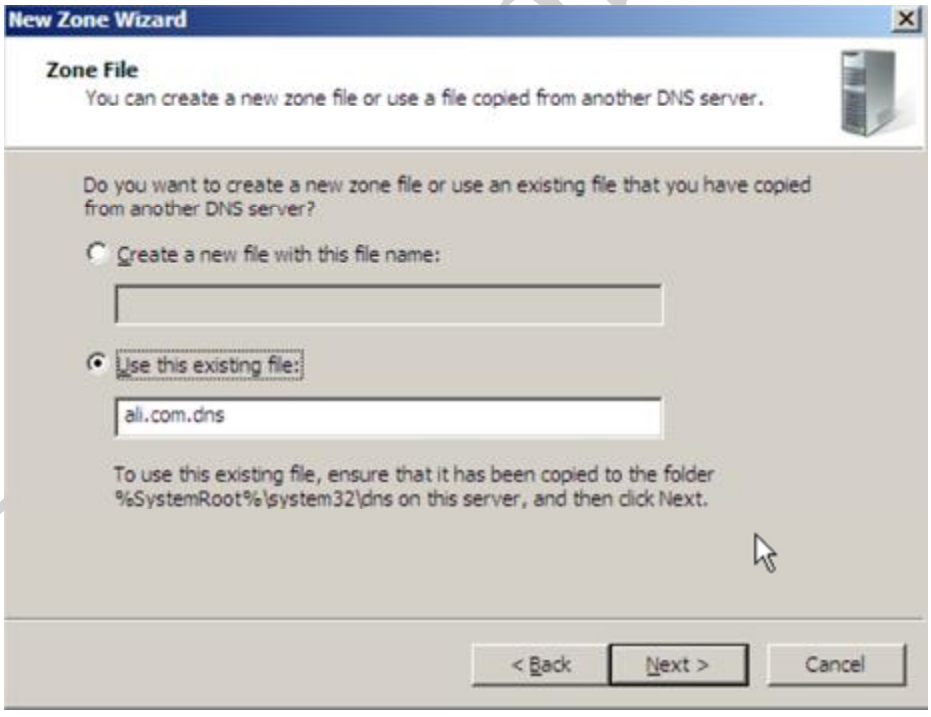


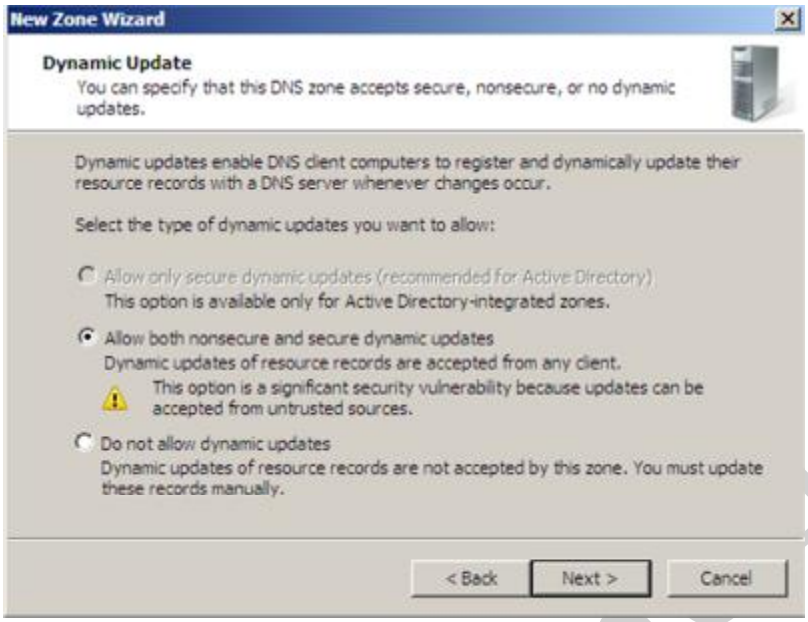

برای بازگردانی زون ابتدا وارد زون پشتیبان می شویم وارد System32 \ dns می شویم و پوشه DNS را کپی می کنیم سپس در سرور اصلی در همان مسیر بالا Paste می کنیم برای بازگردانی،در سرور اصلی دوباره Primary Zones می سازیم به صورت زیر

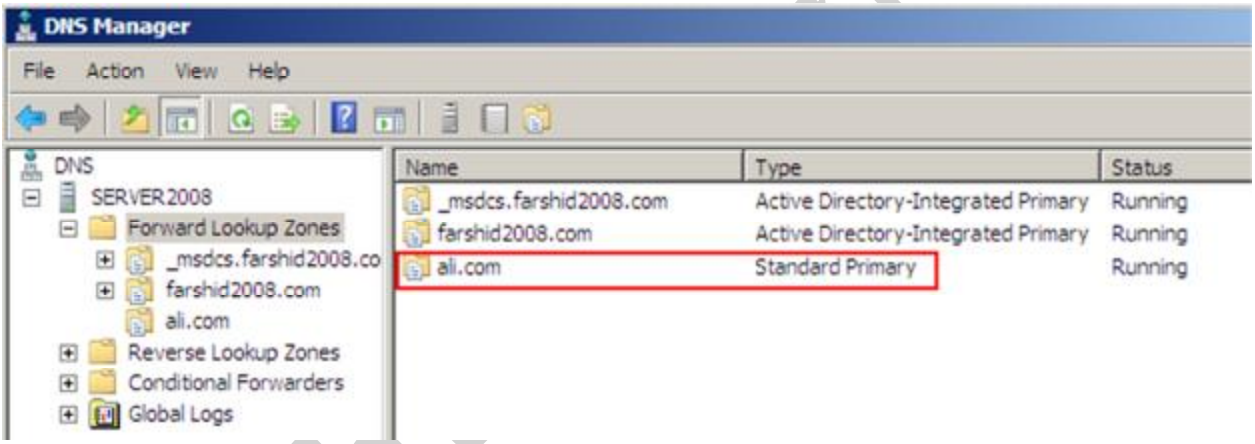


در اینجا اسم زونمان را می نویسیم(پاک شده Ali.com)





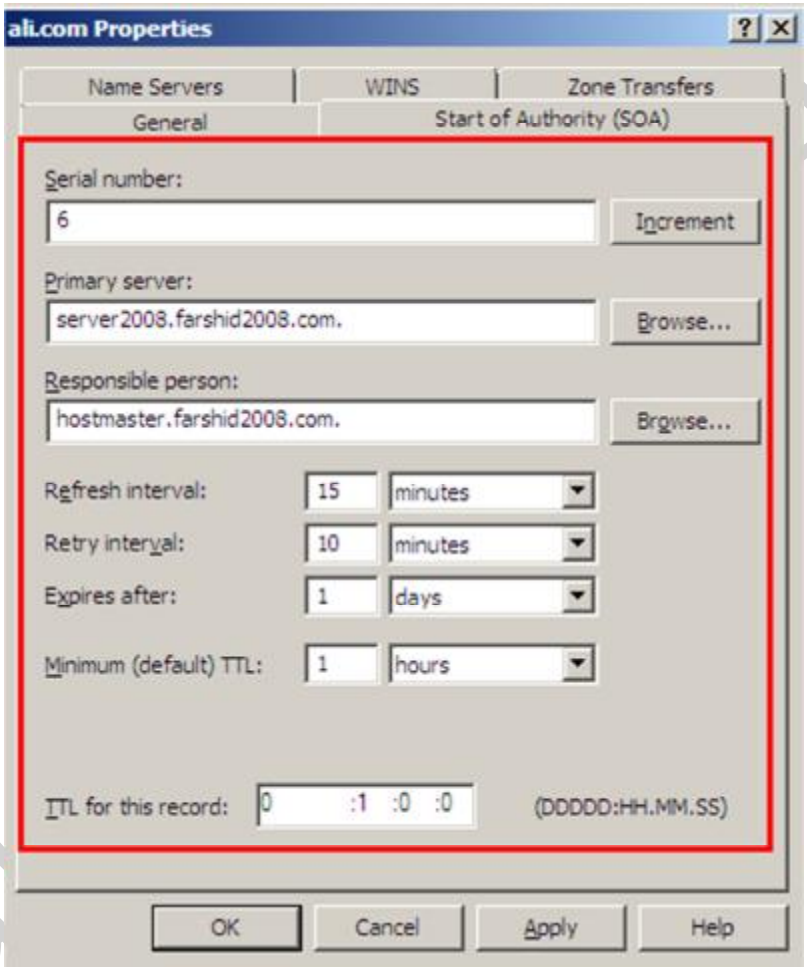




**ودر آخر ساخته شد.**

Farshid Nasiri

- Zone Secondary با استفاده از تنظیمات زیر از تغییرات Primary با خبر شده و اطلاعات را به روی خود انتقال می دهد.

روی زون Primary کلیک راست می کنیم و وارد تب SOA می شویم




Farshid

Serial Number : زمانی که تغییری در زون اصلی بوجود می آید این عدد یک واحد افزایش پیدا می کند و زون پشتیبان متوجه این تغییر می شود.

Refresh interval : در اینجا زون پشتیبان هر15 دقیقه به اصلی سر می زند تا تغییرات اعمال شده را کپی کند.

Retry interval : اگر در هر 15 دقیقه نتوانستیم به اصلی وصل شویم این گزینه می گوید از این به بعد هر10 دقیقه بیاییم.

Expire after : اگر در آن 10 دقیقه ها هم نبتوانستیم وصل بشویم به مدت 1 روز باید هر دقیقه 10 دوباره سعی کنیم،بعد از 1 روز دیگر نمی توانیم کاری کنیم.

Minimum TTL : به مدت زمان نگهداری رکوردها در کش DNS می باشد( مانند نگه داشتن آدرس Yahoo در کش DNS ) با دستور Ipconfig /displaydns تمامی سایتهایی را دیده ایم را نشان می دهد.

آشنایی با مباحث Forwardes در DNS ها

- به سؤالاتی که کلاینت ها از DNS می پرسند Queryگویند،اگر DNS جواب را بداند به کلاینت می دهد و اگر نداند آن سؤال را بصورت تصادفی از یکی از 13 DNS می پرسد.
- Query 2 نوع می باشد،به سؤال کلاینت از DNS ، Recurisive گویند وبه سوال DNS از13 DNS دیگر Iteractive گویند.

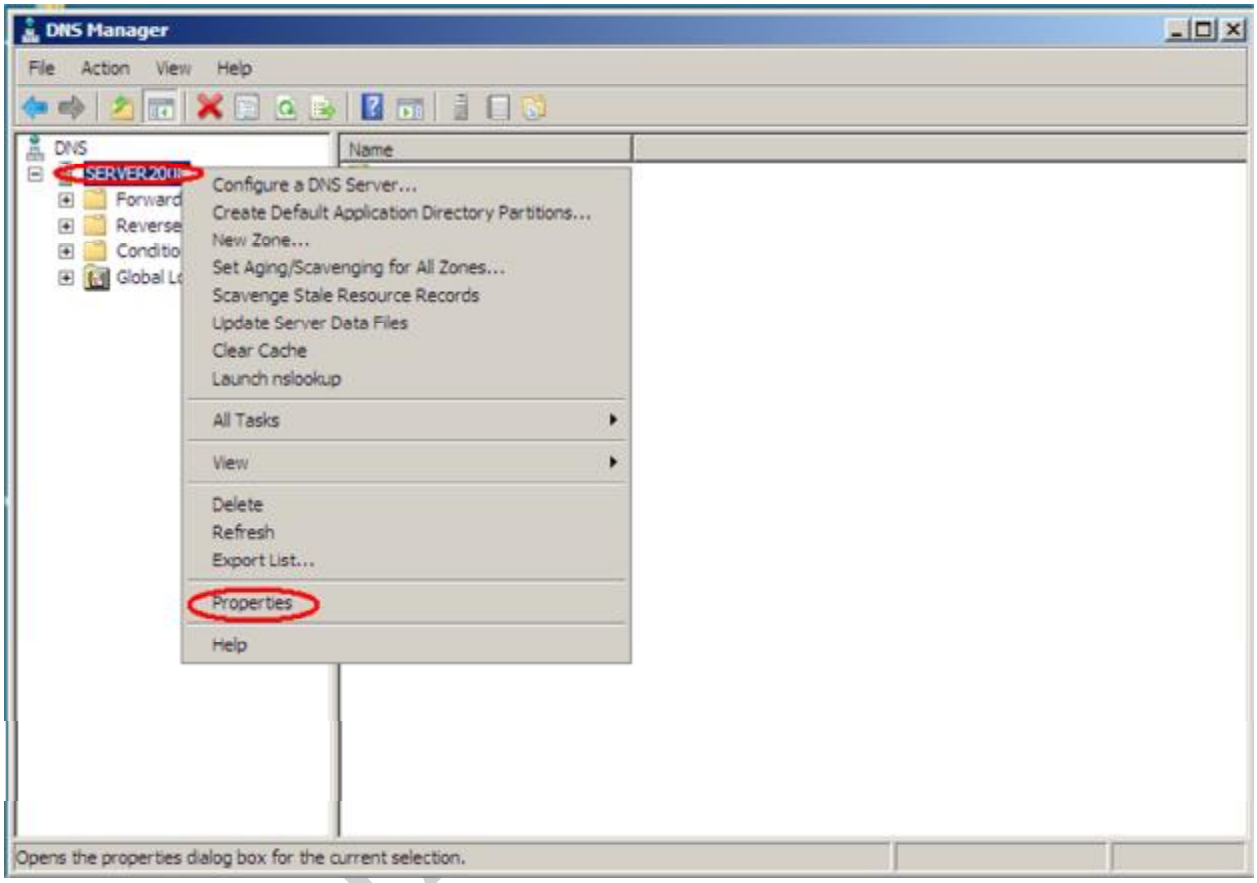
- سؤالات Iteractive به خاطر اینکه بصورت تصادفی از 13 سرور پرسیده می شود مقداری تاخیر دارد.

- برای اینکه زمان تاخیر را کاهش دهیم باید برای DNS شبکه خودمان آدرس یکی از 13 DNS را بدهیم که هر دفعه به همان مراجعه کند به این عمل Forwardes گویند.

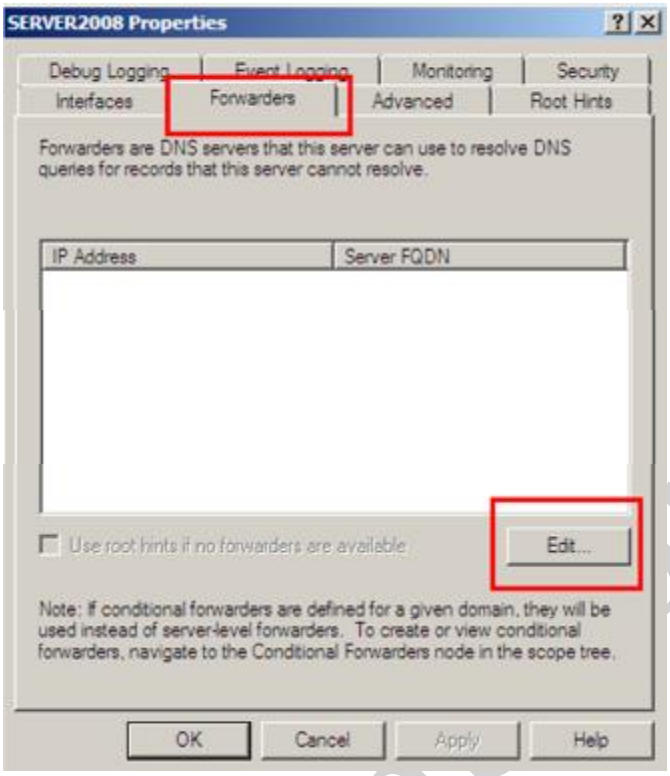
FarshidAjabnoush

نحوه انجام Forwardes

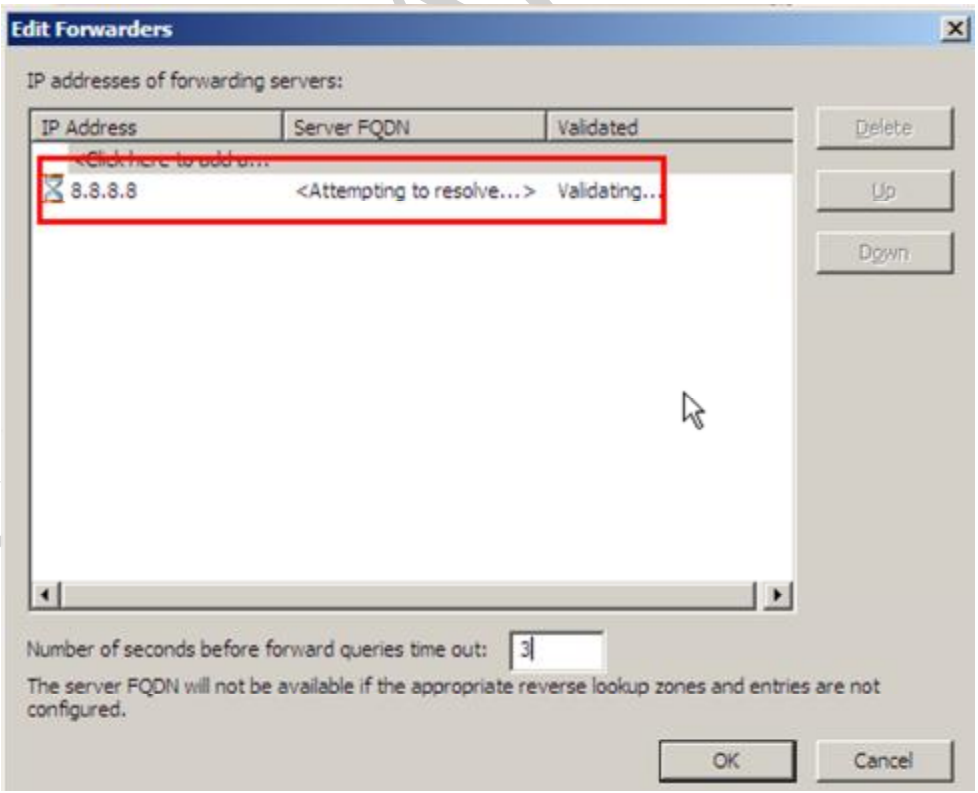
وارد DNS می شویم بر روی اسم سرور کلیک راست،سپس وارد تب Forwardes می شویم




Farsi



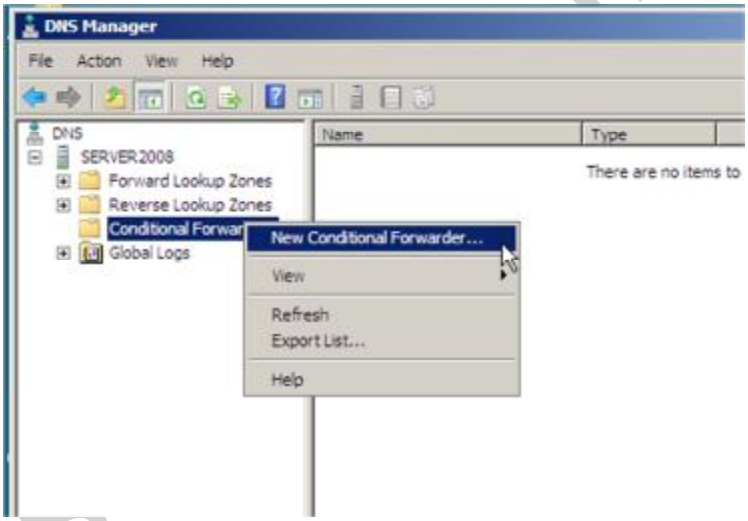

در اینجا Ip ،DNS مقصد را وارد می کنیم



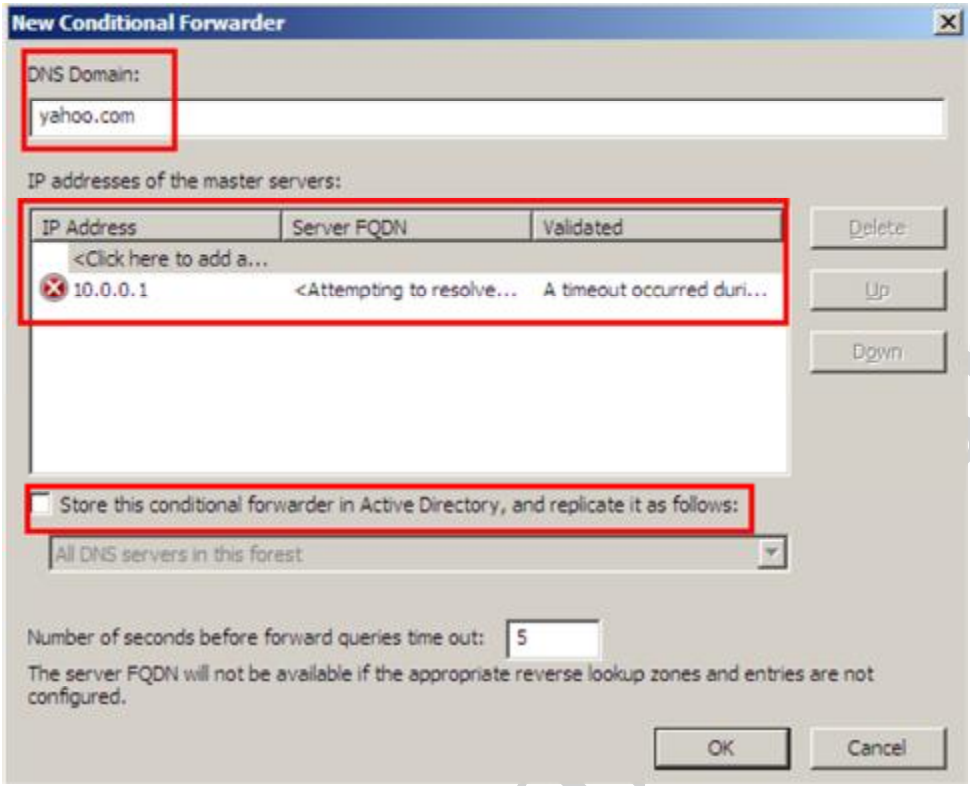
این عمل را زمانی انجام می دهیم که به عنوان مثال سه شعبه داریم و اینترنت را هم از شعبه 1 می گیریم اگر DNS شعبه 2 سؤالی را نداند از DNS شعبه1 می پرسد(Forwardes ) و اگر DNS شعبه 1 هم جواب را نداند از یکی از 13 سرور می پرسد.

Conditional Forwardes

این گزینه Forwardes های مارا هوشمند می کند،یعنی اگر در شعبه2 سؤالی را بخواهیم باید از DNS شعبه1 بپرسیم این عمل بعضی وقتها خوب نیست،این گزینه عمل Forwardesرا هوشمند می کند به این صورت که اگر دنبال Yahoo هستیم آدرس DNS ، Yahoo را به ما می دهد(یعنی اگر دنبال Yahoo هستیم کل اینترنت را دور نمی زنیم، مستقیم به Yahoo وصل می شویم و Ip آن را می پرسیم) و به همین ترتیب.




Fars noush




**در قسمت اول می گوییم اگر آدرسی به Yahoo.com ختم شد باید به Ip که در قسمت دوم وارد شده مراجعه کنی ، تیک گزینه آخر نباید فعال باشد چون اگر فعال باشد اطلاعاتی را که از Ip آدرس وارد شده پیدا کرده است را به اشتراک می گذارد.**

FarshidAjami.com

Cashing Only Dns Server

در 2 حالت در شبکه از Cashing Only Dns Server استفاده می کنیم

حالت1: در ISP ها وقتی اولین مشتری به سایت Yahoo وارد می شود این آدرس را DNS نگه می دارد، اگر نفر بعدی آمد و سایتYahoo را خواست آدرسش را از Cash،DNS بر می دارد (این عمل باعث بالا رفتن سرعت می شود)

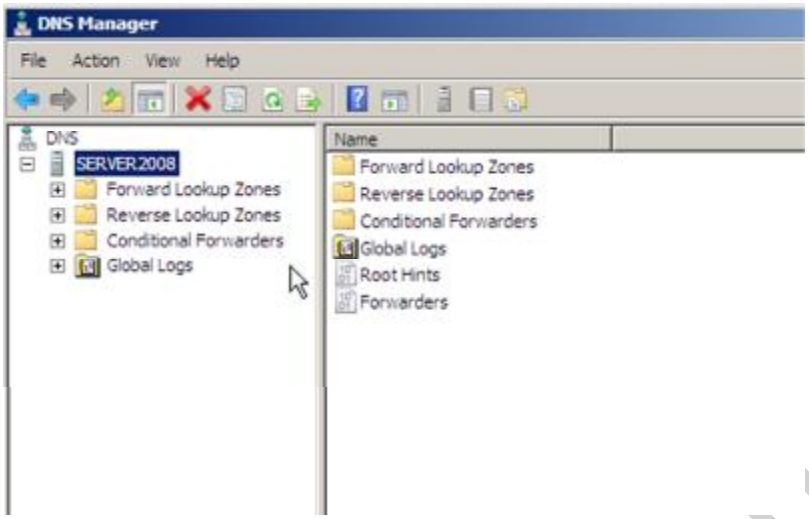
حالت2:در مکانهایی به کار می رود که شعبات مختلفی دارند و همه شعبات برای عمل Name Resolution از یک DNS استفاده می کنند، به این صورت که باید در هر شعبه یک Secondary بسازیم و هر شعبه سؤالاتش را از Secondary خودش بپرسد.

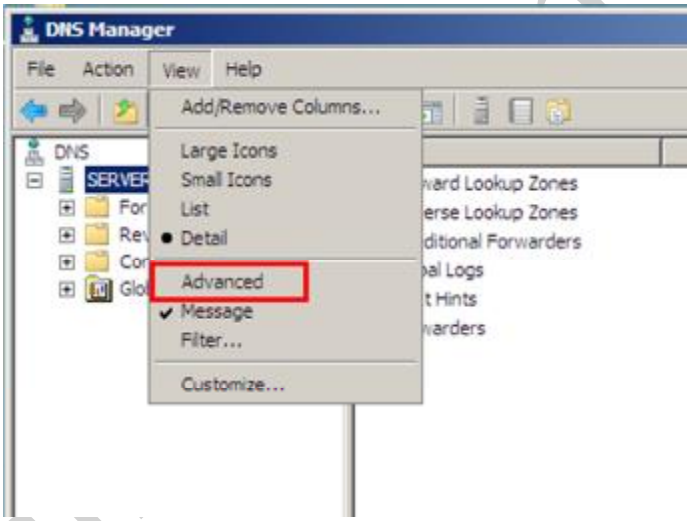
در حالت دوم باید سرعت انتقال اطلاعات بین شعبه اصلی و دیگرشعبات بالاتر از 512 K باشد اگر سرعت پایین تر از این حد باشد در شعبات دیگر بایدCashing Only Server فعال کنیم.

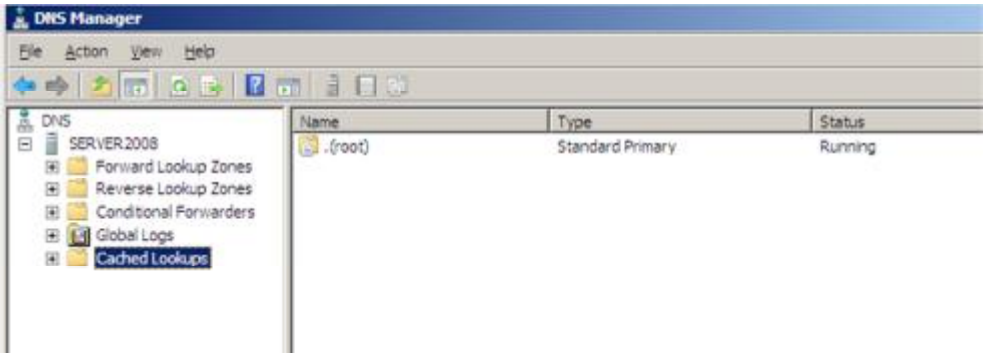
- به سرعت های پایین تر از 512 K ، Wan Link گویند.
- تمامی DNS های دنیا به صورت پیش فرض در حالت Cashing Only Server هستند.

برای دیدن Cashing Only Server مسیر زیر را دنبال می کنیم

FarshidAjabnoush


DNS Manager
File Action View Help
DNS
SERVER2008
Forward Lookup Zones
Reverse Lookup Zones
Conditional Forwarders
Global Logs
Name
Forward Lookup Zones
Reverse Lookup Zones
Conditional Forwarders
Global Logs
Root Hints
Forwarders


DNS Manager
File Action View Help
Add/Remove Columns...
Large Icons
Small Icons
List
Detail
Advanced
Message
Filter...
Customize...


DNS Manager
File Action View Help
DNS
SERVER2008
Forward Lookup Zones
Reverse Lookup Zones
Conditional Forwarders
Global Logs
Cached Lookups
Name
Type
Status
(root)
Standard Primary
Running

Farsh Noush

زمانی که Cashing Only Server راه اندازی کردیم روی آن سرور هیچ وقت زون نمی سازیم، زمانی که در جایی Cashing Only Serve راه اندازی کردیم باید Forward کنیم به یک DNS اصلی و کلاینت ها باید DNS ها را بر روی Cashing Only Serve تنظیم کنند.

ایجاد Load Blancing بر روی DNS Server

وقتی که در شبکه 100 کاربر داریم باید یک DNS ، Primary و یک DNS ، Secondary در شبکه راه اندازی کنیم برای 50 کاربر اول آدرس DNS ، Primary را به عنوان DNS اولشان (Preferred ) و آدرس DNS ، Secondary را به عنوان DNS دومشان (Alternate) تنظیم می کنیم . برای 50 کاربر دوم آدرس DNS های PreferredوAlternate را جابجا می کنیم.

آشنایی با D DNS( Dynamic DNS) و پیاده سازی آن

برای پیاده سازی ،علاوه بر DNS به DHCP سرور هم نیاز داریم، زمانی که DHCP به کلاینت ها Ip داد،واردDNS می شود و در زون مربوطه اسم کامپیوتر ها و Ip آنها را ثبت می کند اگرIp هر کامپیوتری عوض شد خود DHCP وارد زون مربوطه می شود وIp آن کامپیوتر را تغییر می دهد.

- Ip هر کامپیوتر به صورت اتوماتیک و پیش فرض هر 8 روز تعویض می شود.

FarshidAjabnoush

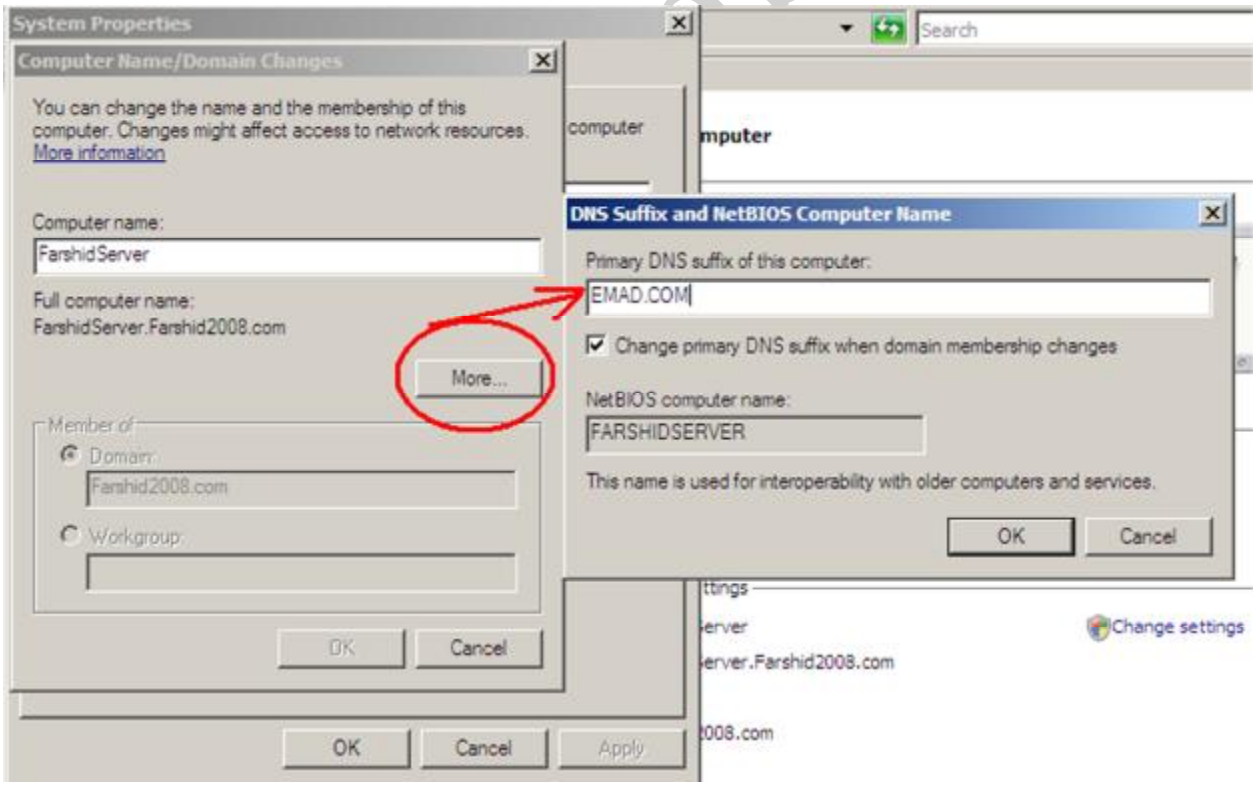
Dynamic Update

در اینجا فقط به DNS سرور احتیاج داریم، داخل DNS زون می سازیم سپس زمانی که کلاینت ها Login کردن خود کلاینت ها به صورت اتوماتیک اسم وIp شان را داخل زون ساخته شده ثبت می کنند.

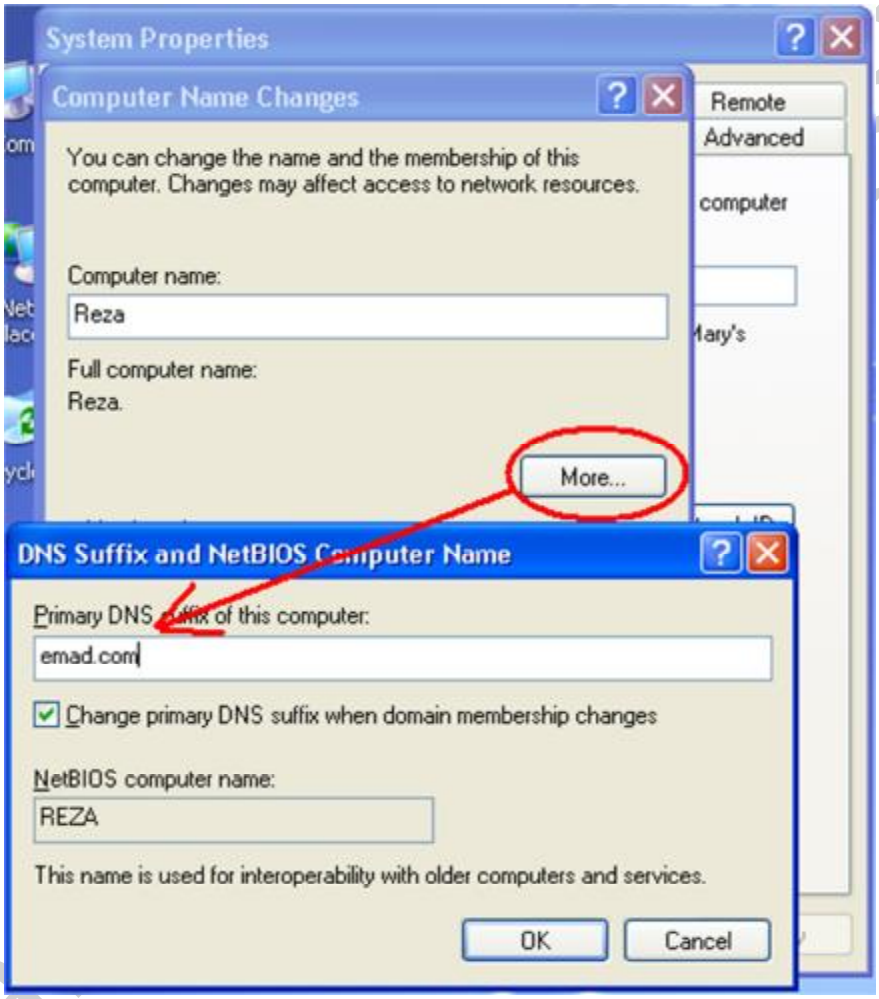
- در شبکه های دامینی (Active Directory دارند) زمان Join شدن کلاینت ها به شبکه ،به صورت اتوماتیک Dynamic Update انجام می شود.

در شبکه های WorkGroup برایDynamic Update باید به صورت زیر عمل کنیم.

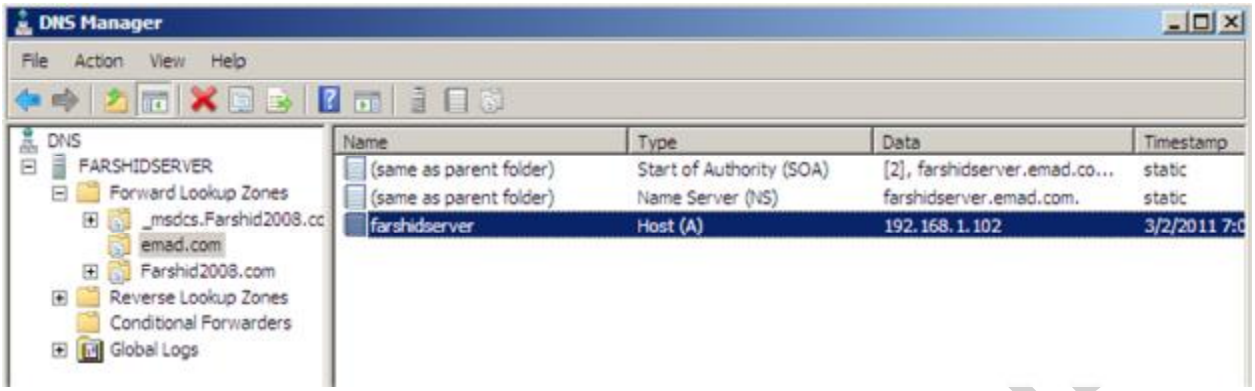
ابتدا وارد DNS سرور می شویم سپس به قسمت اسم دامین می رویم بر روی More کلیک می کنیم سپس اسم زونمان را آنجا می نویسیم (Emad.com ) و سیتم را ریستارت می کنیم.



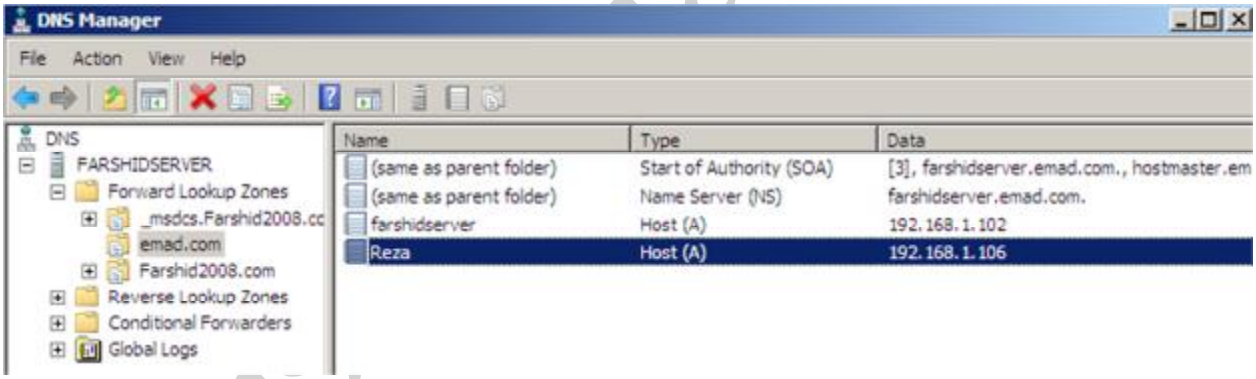
بعد از ریستارت کردن زونمان را به همان اسم می سازیم،به روی کلاینت بر می گردیم و در قسمت More مانند شکل زیر عمل می کنیم و در قسمت Preferred DNS ،Ip سرور را وارد می کنیم و سیستم را ریستارت می کنیم.



- در زونِ ساخته شده حتماً باید اسم خود سرور و Ip آن اضافه شده باشد.



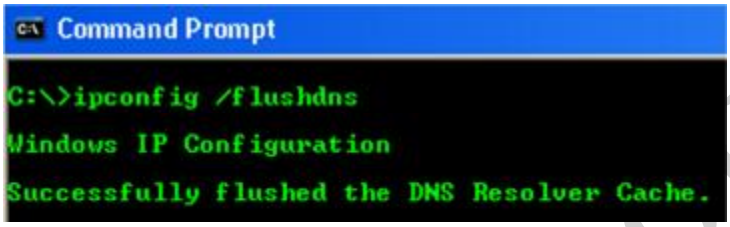

- در زونِ ساخته شده علاوه بر اسم سرور باید اسم کلاینت و Ip آن هم اضافه شده باشد.



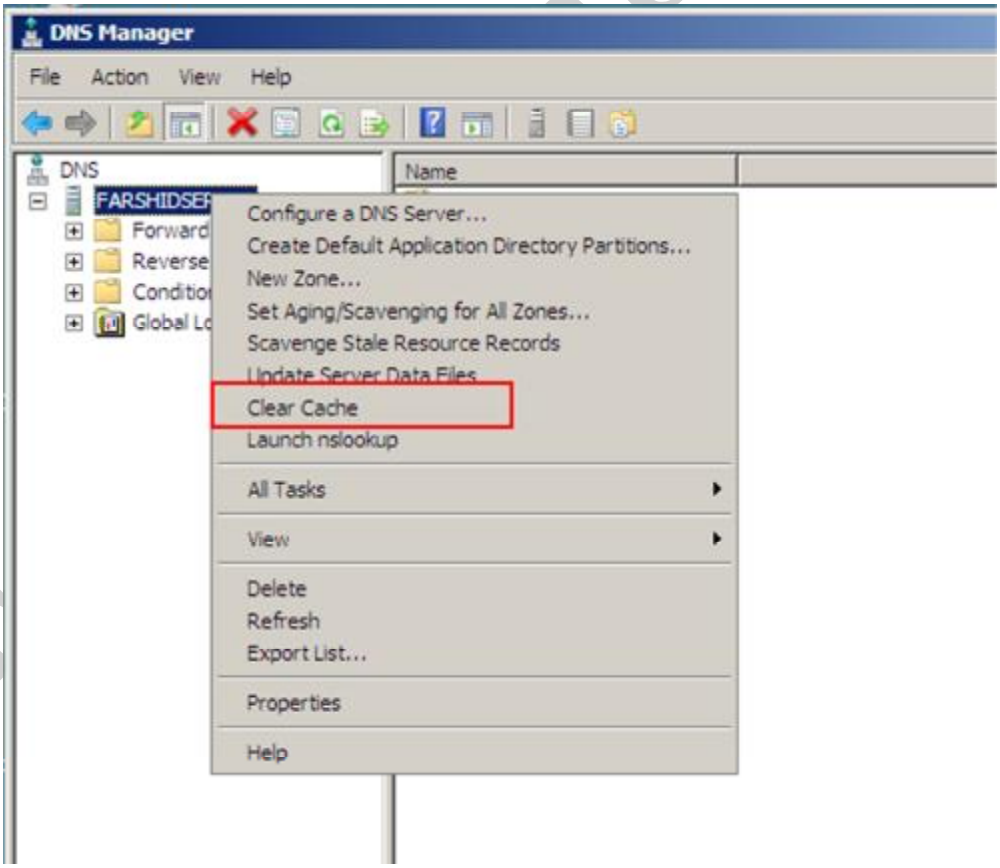

Farshidabnou

- روش اول پاک کردن کش DNS هم در کلاینت و هم در سرور،در کلاینت با دستور Ipconfig /Flushdns و در سرور وارد کنسول DNS می شویم بر روی اسم سرور کلیک راست می کنیم سپس بر روی Clear Cash کلیک می کنیم.

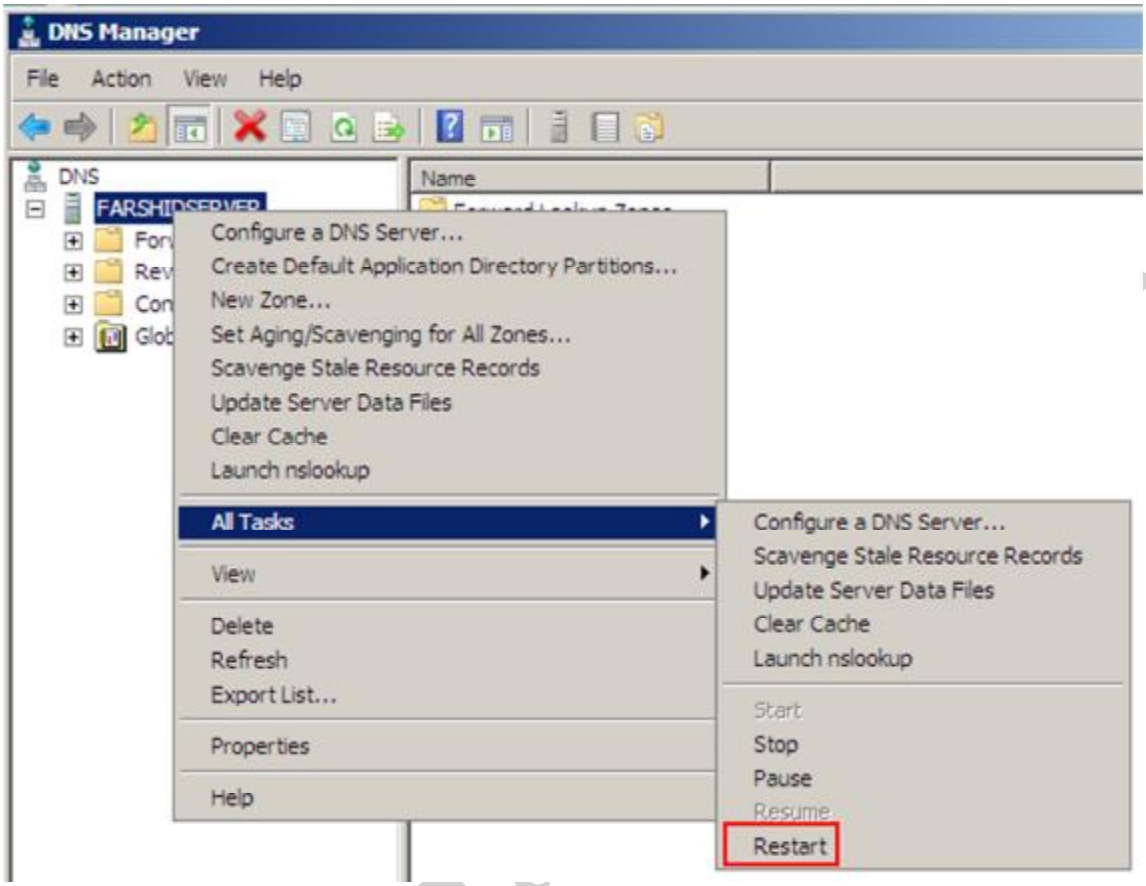
Client




Server



- روش دوم ریستارت کردن سرویس DNS



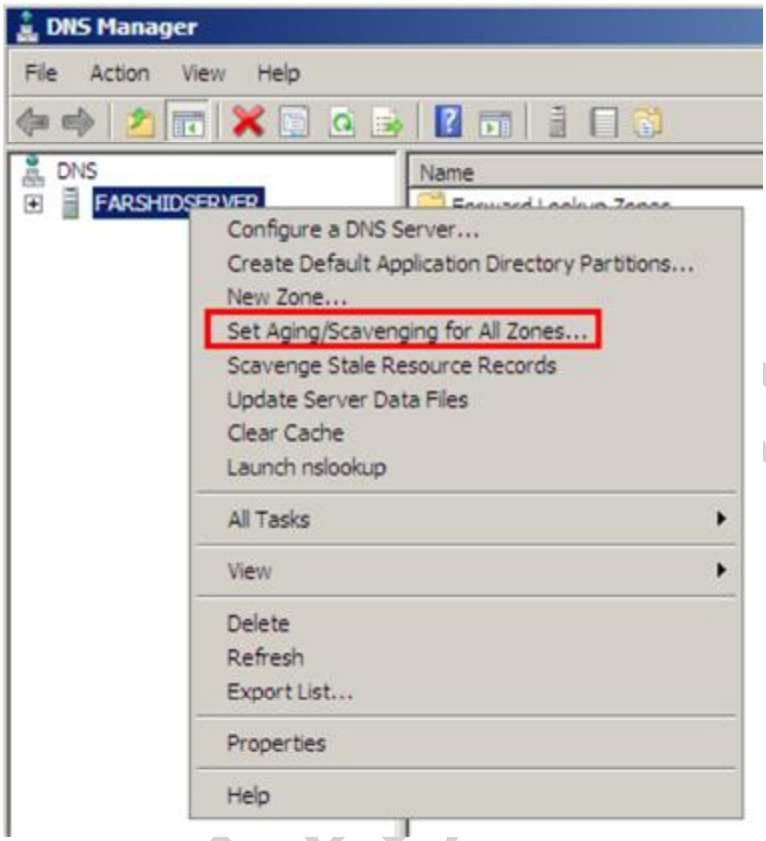

- روش سوم رکوردهایی را دیگر استفاده نمی شوند از داخل کش DNS پاک کنیم این کار را به صورت دستی نمی توان انجام داد باید DNS را طوری تنظیم کنیم که این کار را به صورت اتوماتیک انجام دهد، به این حالت اتوماتیک Aging& Scavenging گویند. Aging یعنی شناسایی رکوردهای فرسوده و Scavenging یعنی پاک کردن رکوردهای فرسوده.

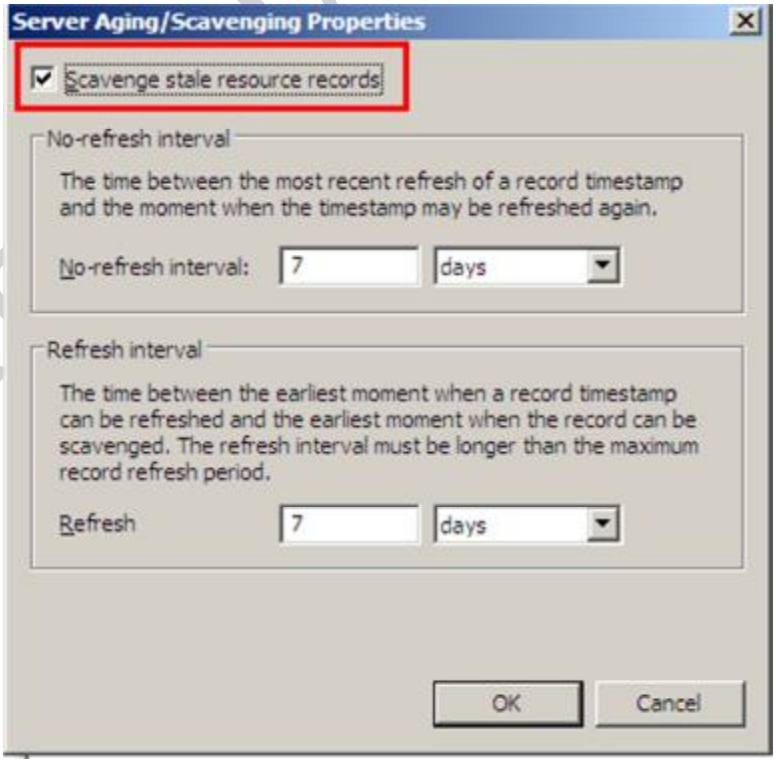
این حالت به صورت پیش فرض غیر فعال می باشد برای فعال سازی باید مراحل زیر را طی کنیم.

ابتدا بر روی اسم DNS کلیک راست می کنیم و گزینه ....Aging را انتخاب و تیک گزینه مر بوطه را می زنیم

- اگر بخواهیم ....Aging را برای زون خاصی فعال کنیم روی آن زون کلیک راست می کنیم,Propertiesسپس ....Aging را فعال می کنیم.

Farshid


DNS Manager
File Action View Help
DNS
FARSHIDSERVER
Name
Configure a DNS Server...
Create Default Application Directory Partitions...
New Zone...
Set Aging/Scavenging for All Zones...
Scavenge Stale Resource Records
Update Server Data Files
Clear Cache
Launch nslookup
All Tasks
View
Delete
Refresh
Export List...
Properties
Help


Server Aging/Scavenging Properties
Scavenge stale resource records
No-refresh interval
The time between the most recent refresh of a record timestamp and the moment when the timestamp may be refreshed again.
No-refresh interval:
7
days
Refresh interval
The time between the earliest moment when a record timestamp can be refreshed and the earliest moment when the record can be scavenged. The refresh interval must be longer than the maximum record refresh period.
Refresh
7
days
OK
Cancel

Farshidush

DNS Server از فرمول زیر متوجهه می شود که تاریخ مصرف یک رکورد گذشته است.

If{TimeStap+2(87.5% Lease Duration)>Today}=else remove

TimeStap تاریخ ساخته شدن رکورد.

Lease Duration عدد ثابت DHCP که 8 می باشد است.

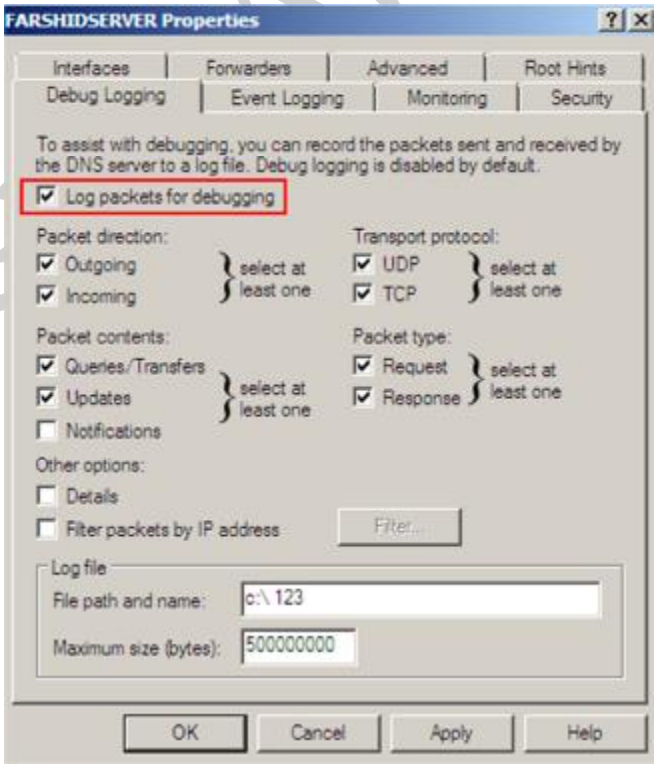
87.5% عدد 8 مساوی 7 می باشد.

Today تاریخ امروز

این فرمول به این صورت است که می گوید تاریخ ساخته شدن رکورد + 2برابر87.5% اگر بزرگتر از تاریخ امروز بود این رکورد تاریخ مصرف دارد ولی اگر کوچکتر بود تاریخ مصرف ندارد.

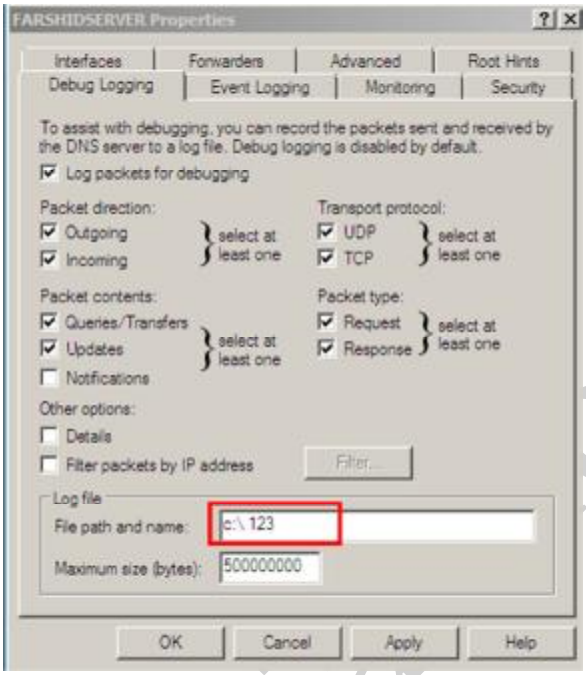
روش چهارم (بهترین روش) در این روش LogFile ها را فعال می کنیم،به صورت پیش فرض غیرفعال است

بر روی اسم سرورDNSProperties, می گیریم وارد تب Debug Logging می شویم وتیک مربوطه را می زنیم.

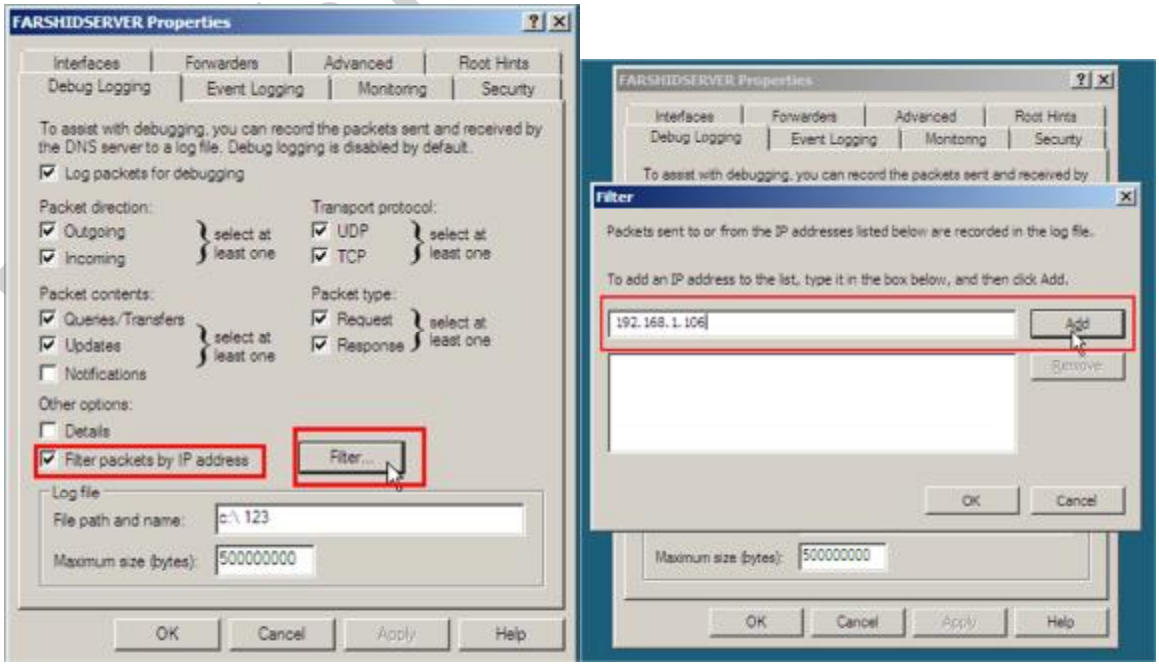



Farshid Nabroush

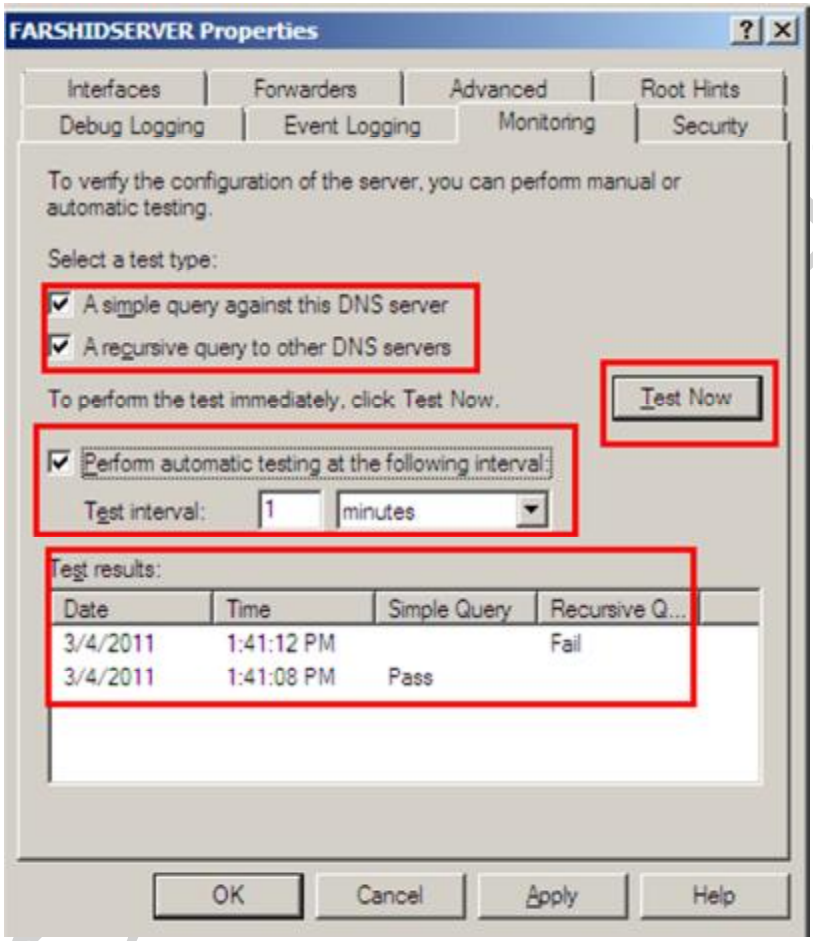
در قسمت Log File مسیر ذخیره شدن Log ها را می دهیم. Logfileبه این دلیل غیر فعال است که اگر کوچکترین اتفاقی بیفتد در Log ثبت می شود.




بهترین روش برای Log گیری از سیستمی که مشکل دارد این است که Ip آن را وارد کنیم تا فقط Log همان سیستم را برای ما ذخیره کند.



- روش پنجم استفاده از تب Monitoring می باشد، در این تب دوگزینه Simple Query و Query Recursive وجود دارد ، گزینه اول برای تست کردن تنظیمات داخلی DNS می باشد وگزینه دوم برای تست گرفتن این DNS با RootHints ها می باشد که اگر به اینترنت متصل نباشیم Fail می دهد (مانند شکل).



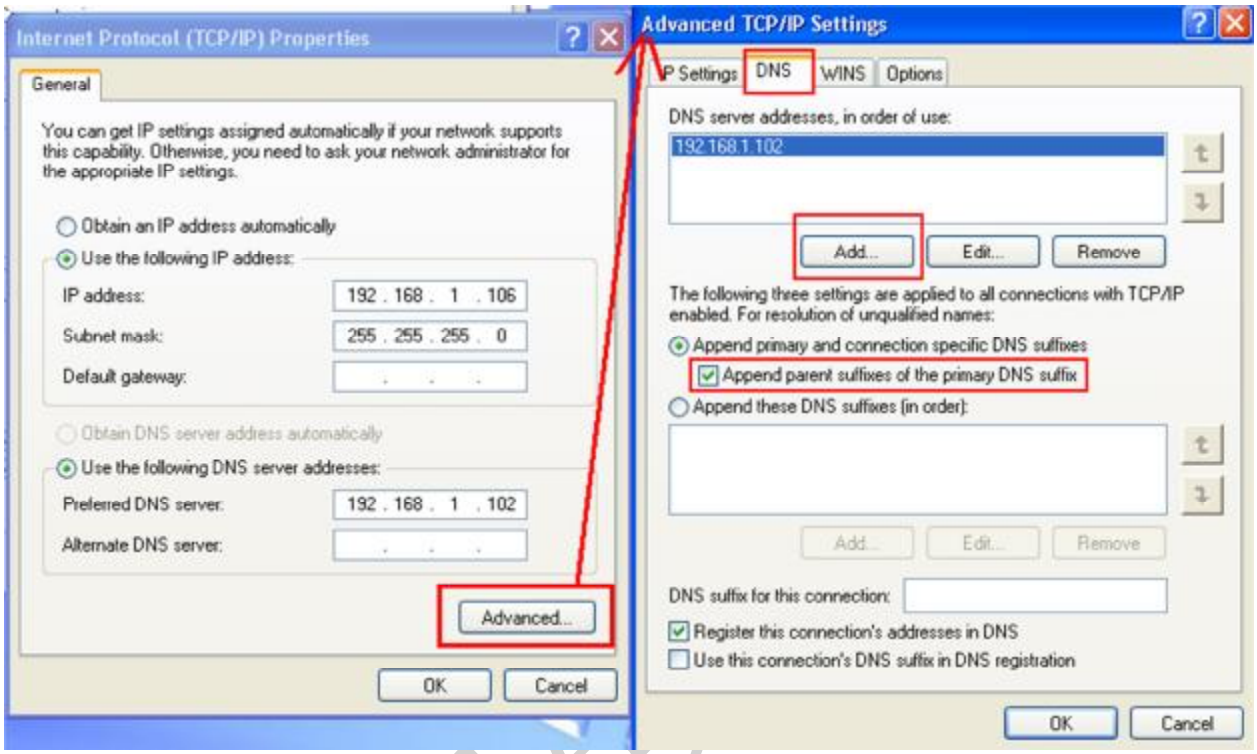

اگر گزینه ....Performe automatic فعال باشد به صورت پیش فرض هر 1 دقیقه تست را به صورت اتوماتیک انجام می دهد طرز کار این گزینه به این صورت است که هر 1 دقیقه یک Flag یا خونه ارسال می کند اگر طرف مقابل باشد آن خونه را پر می کند (Ping )

- از همه این روشها بهتر، ریستارت کردن DNS می باشد.

تنظیمات DNS Client

به کسی که می خواهد از DNS Server سرویس بگیرد DNS Client گویند (حتی می تواند یک سرور دیگر باشد)

برای تنظیمات به مسیر زیر می رویم

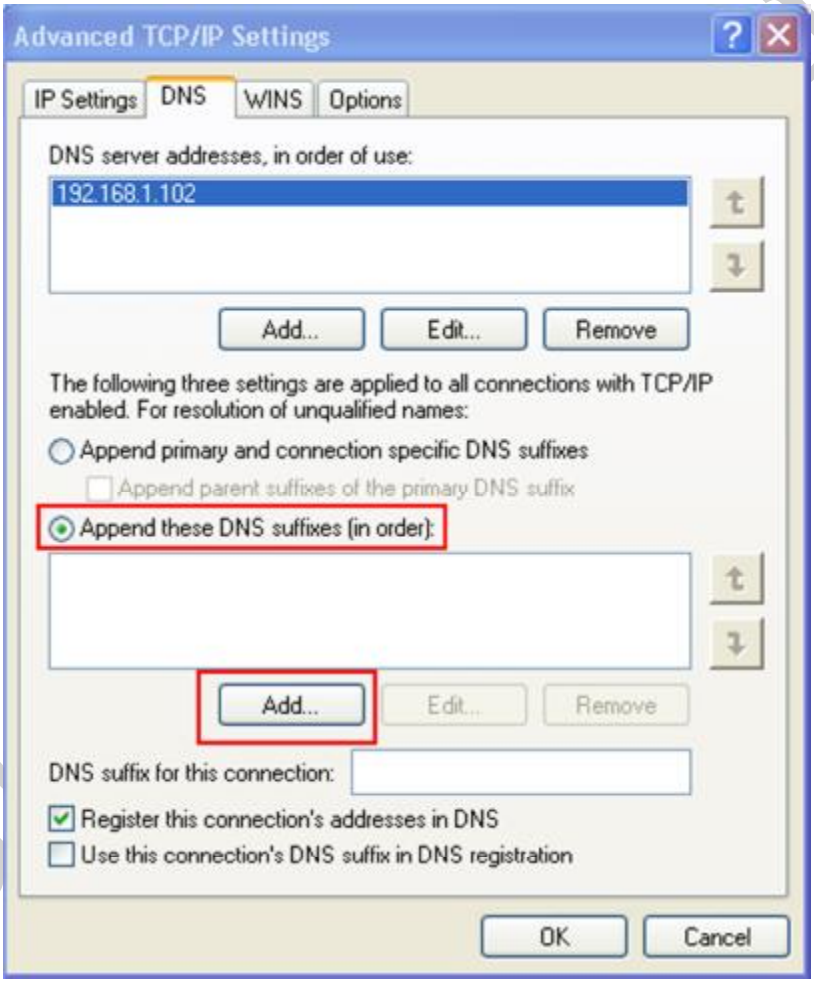



به صورت پیش فرض می توانیم DNS2 داشته باشیم برای اینکه بیشتر DNS داشته باشیم می توانیم بر روی Add کلیک کنیم وDNS اضافه کنیم.

اگر گزینه Append parent suffixes فعال باشد،زمانی که کامپیوتر مورد نظر را با اسم Ping کنیم به ما جواب می دهد.(اسمی را که در قسمت More است را جلوی اسم Ping ما می نویسد و انجام می دهد)

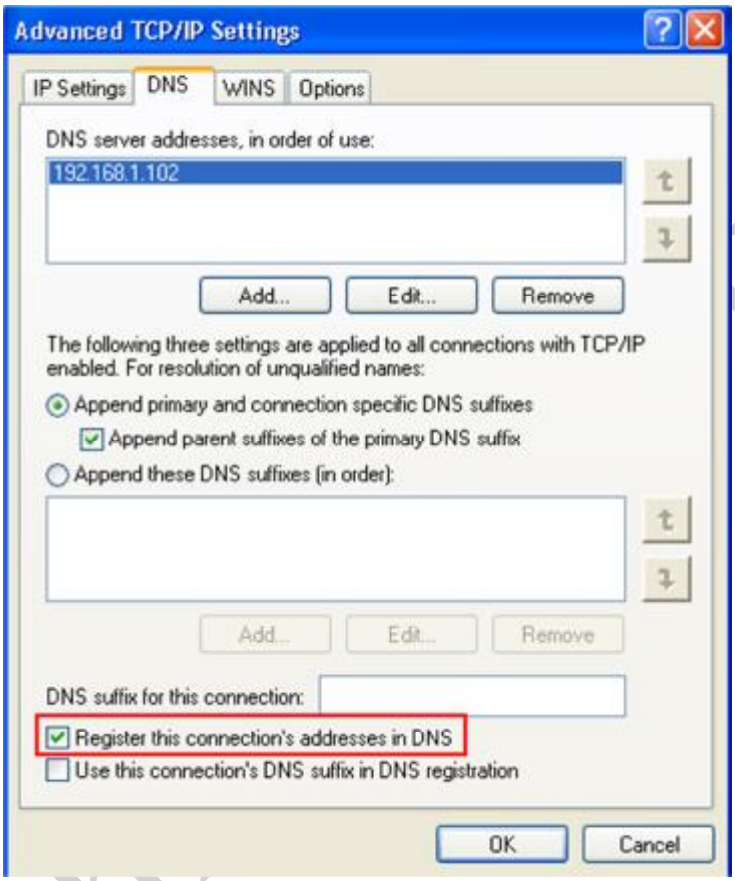
FarshidA

اگر ما 2 زون داشته باشیم به نام های Ali.com و Hani.com و داخل زون Hani کامپیوتری به نام Pc2 داشته باشیم ودر قسمت More سیستم زون Ali.com تعریف شده باشد،وقتی از Pc2، Ping بگیریم به ما جواب نمی دهد به این دلیل که Ali.com را در جلوی اسم Pc2 قرار می دهد و می بیند در این زون چنین اسمی (Pc2 ) وجود ندارد 2روش برای حل این مشکل وجود دارد 1- در قسمت More زون Hani را وارد کنیم 2- از تنظیمات DNS بگوییم اگر اسمی در زونی که در قسمت More وارد شده وجود نداشت، در زون هایی که اسامی آنها در این قسمت اضافه شده را جستجو کن.




Fa

زمانی که گزینه زیر فعال باشد سیستم به صورت اتوماتیک می تواند اسم خودش را در زونی که اسم آن در قسمت More آمده اضافه کند( Dynamic Update )

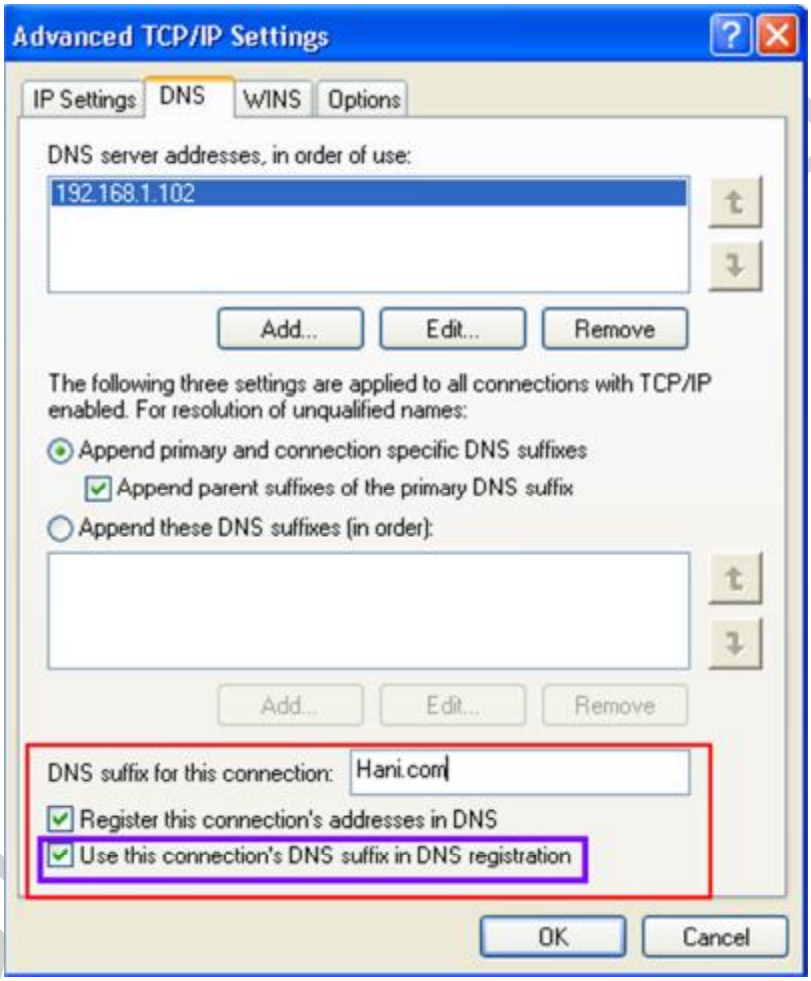



- به کامپیوتری که بیش از یک کارت شبکه داشته باشد Multi Homed گویند.
- در شبکه های دامینی عملیات DynamicUpdate موقع Join به صورت اتوماتیک انجام می شود به این دلیل که گزینه .... Register this (شکل با لا) فعال می باشد.

Farsh

اگر کامپیوتری 2 کارت شبکه داشته باشد اسم خودش را 2 بار در زونی که در قسمت More آمده ثبت می کند حال اگر بخواهیم کارت شبکه دوم اسم خودش را در زون دیگری ثبت کند باید گزینه ...Use This را انتخاب کنیم و در کادر مربوطه اسم زونمان را وارد کنیم.

- هر دو گزینه باید انتخاب شوند.




- برای پاک کردن کش DNS بر روی سرور از گزینه Clear Cache و بر روی کلاینت از دستور Ipconfig /flushdns استفاده می کنیم.
- TTL های DNS 1 ساعت هستند.

WEBSERVER

به سروری کهسرویس های (IIS,FTP,APPSERVER )را تحت وب توسط پروتکل هایی مانند HTTP,SNTP,FTPارائه می کند راوب سرور گویند.

ورژن های IIS ( Internet Information Service )

5Win2000 ( بسیار نا امن)

6 Win2003 (باز هم نا امن)

7Win2008 (به دلیل ماژولار بودن، امنیت بالایی داشت)

7.5Winserver2008 R2

- از بهترین Web Server ها می توان به IIS و (Apache(linux اشاره کرد،از زمانی که IIS7 وارد بازار شد همه از Apache به سوی IIS آمدند چون در Apache محیط فقط کامندی بود،امنیت Apache از IIS 6 بالاتر بود.

- برای راه اندازی Web Server باید IIS و Application Server با هم اجرا شوند، و این 2 حتماً باید با FTP، هر سه با هم اجرا شوند.

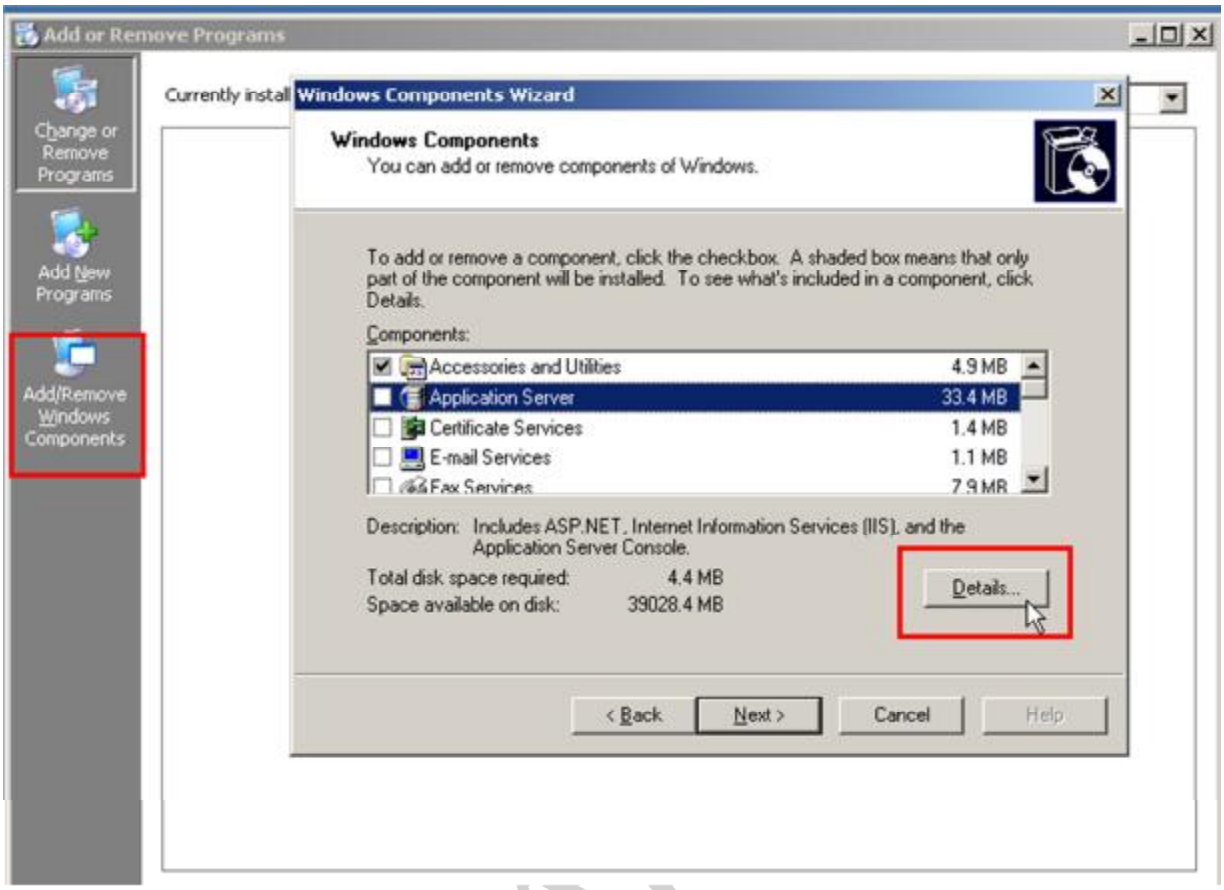
- برای بالا آوردن یک سایت از IIS استفاده می شود، برای انتقال و مدیریت بر فایل ها در یک فضای اینترنتی از FTP استفاده می شود، از Application Server می توان به SharePoint(اتوماسیون اداری) اشاره کرد.
- برای یادگیری IIS7 باید کاملاً به IIS6 مسلط بود.
- IIS بر روی پورت80 همان پورت HTTP کار می کند,HTTPS هم بر روی پورت 443 کار می کند.
- FTP روی پورت 20 Transfare می کند و بر روی 21 شناسایی می کند(ابتدا شناسایی بعد انتقال)
- برای بالا آوردن چند سایت بر روی یک کارت شبکه باید به ازای هر سایت یک IP روی کارت شبکه تنظیم کنیم.

FarshidAjabnoush

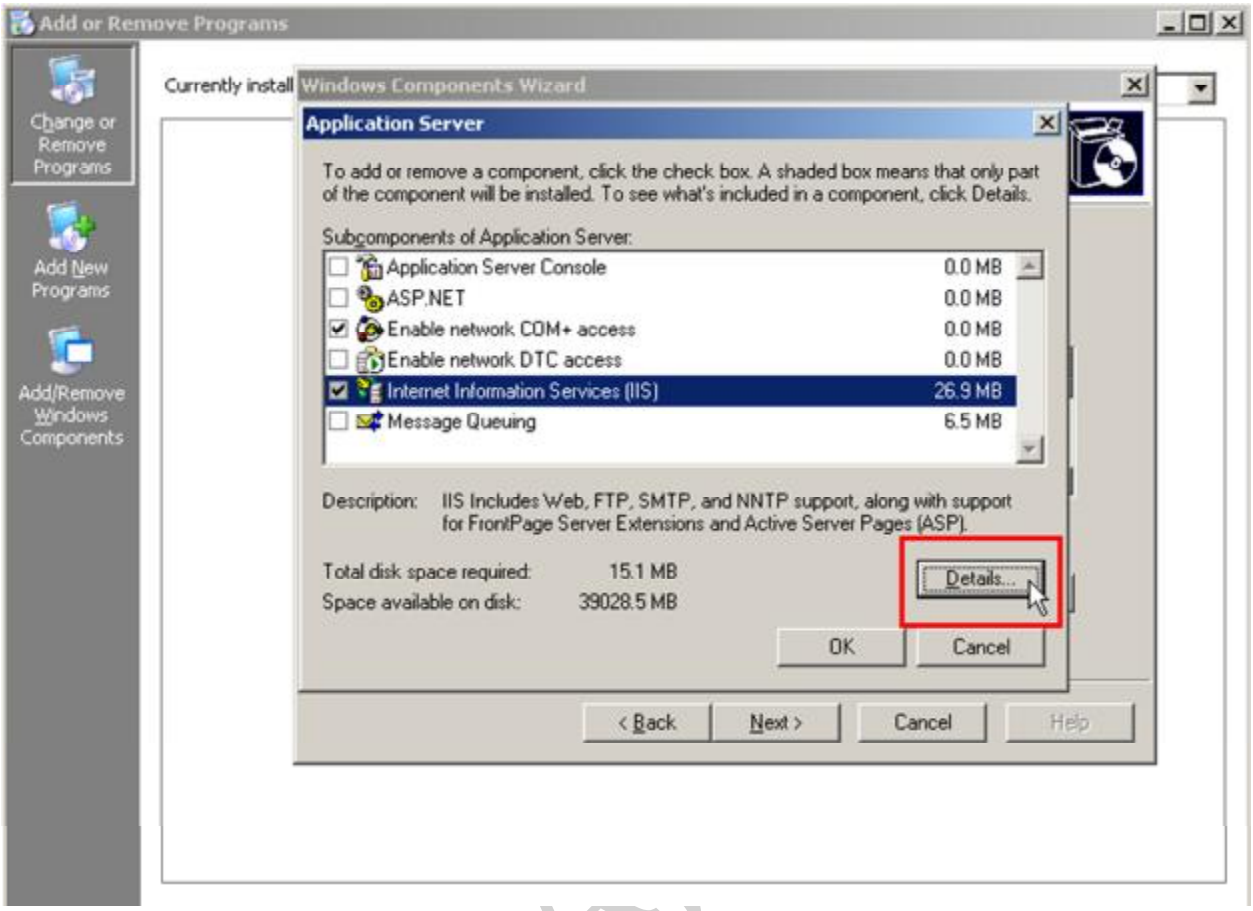
طریقه نصب IIS 6

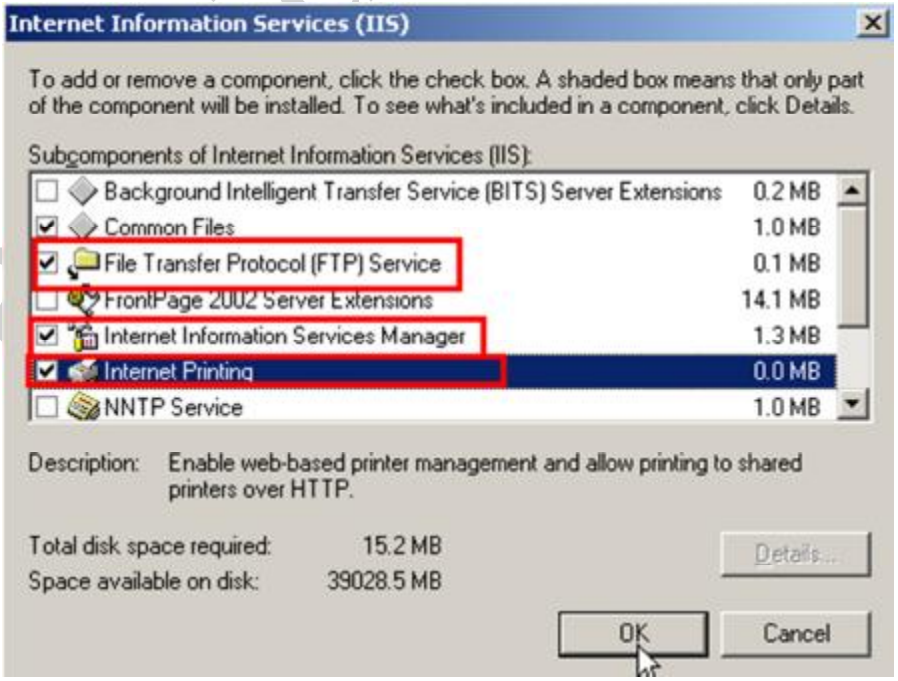
ابتدا باید Server 2003 داشته باشیم.

FarshidAja


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently install
Windows Components Wizard
Windows Components
You can add or remove components of Windows.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Accessories and Utilities 4.9 MB
Application Server 33.4 MB
Certificate Services 1.4 MB
E-mail Services 1.1 MB
Fax Services 7.9 MB
Description: Includes ASP.NET, Internet Information Services (IIS), and the Application Server Console.
Total disk space required: 4.4 MB
Space available on disk: 39028.4 MB
Details...
< Back
Next >
Cancel
Help

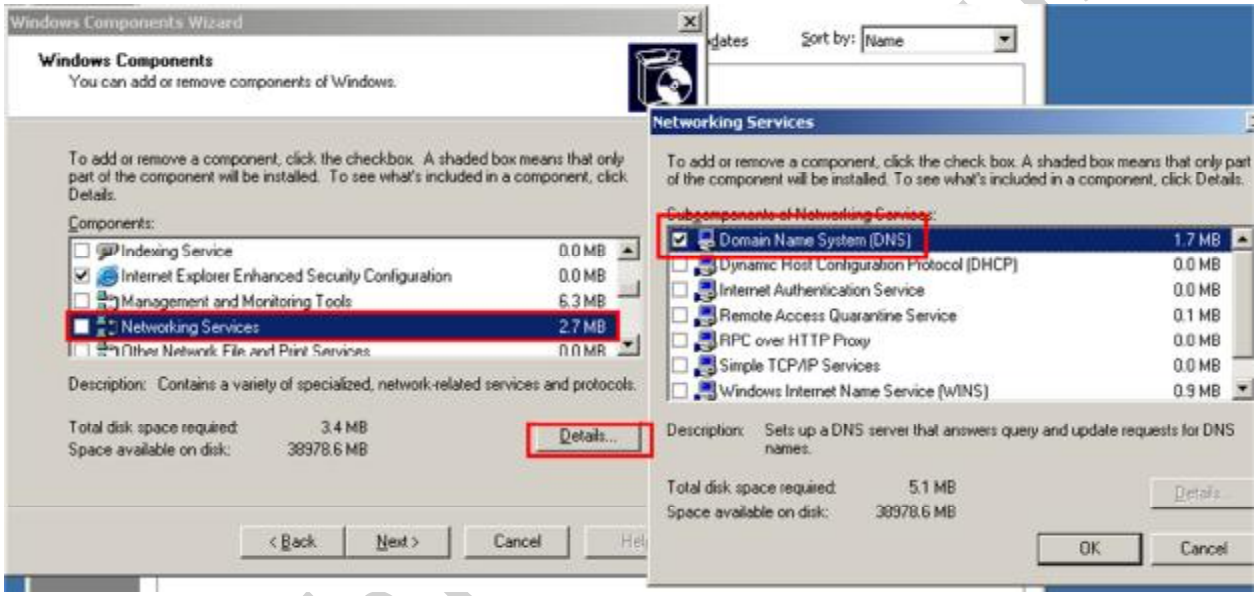
FarshidA,


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently install
Windows Components Wizard
Application Server
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Application Server:
Application Server Console 0.0 MB
ASP.NET 0.0 MB
Enable network COM+ access 0.0 MB
Enable network DTC access 0.0 MB
Internet Information Services (IIS) 26.9 MB
Message Queuing 6.5 MB
Description: IIS Includes Web, FTP, SMTP, and NNTP support, along with support for FrontPage Server Extensions and Active Server Pages (ASP).
Total disk space required: 15.1 MB
Space available on disk: 39028.5 MB
Details...
OK
Cancel
< Back
Next >
Cancel
Help


Internet Information Services (IIS)
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Internet Information Services (IIS):
Background Intelligent Transfer Service (BITS) Server Extensions 0.2 MB
Common Files 1.0 MB
File Transfer Protocol (FTP) Service 0.1 MB
FrontPage 2002 Server Extensions 14.1 MB
Internet Information Services Manager 1.3 MB
Internet Printing 0.0 MB
NNTP Service 1.0 MB
Description: Enable web-based printer management and allow printing to shared printers over HTTP.
Total disk space required: 15.2 MB
Space available on disk: 39028.5 MB
Details...
OK
Cancel

- با فعال کردن Internet Printing اجازه می دهیم اگر کسی از مطالب روی سایت خواست پرینت بگیرد و دسترسی به پرینتر نداشت، از پرینتری که ما برای سایت تعریف کرده ایم استفاده کند(به نوعی Share )

- در آخر هم باید سرویس DNS را نصب کنیم،هرجا که از IIS استفاده می کنیم طرف دیگر آن DNS می باشد.

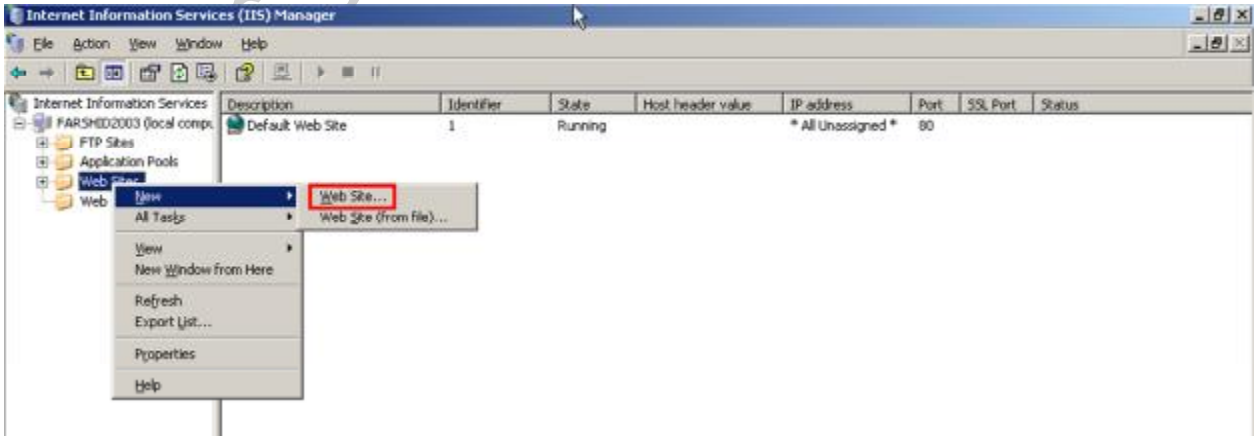



- به ازای هر سایتی که در Web Server بالا می آوریم باید داخل DNS زونی به نام همان سایت داشته باشیم،داخل هر زون هم باید Arecord و C name داشته باشیم.(در اینجا اسم زونمان Reza.ir است)

Farshad

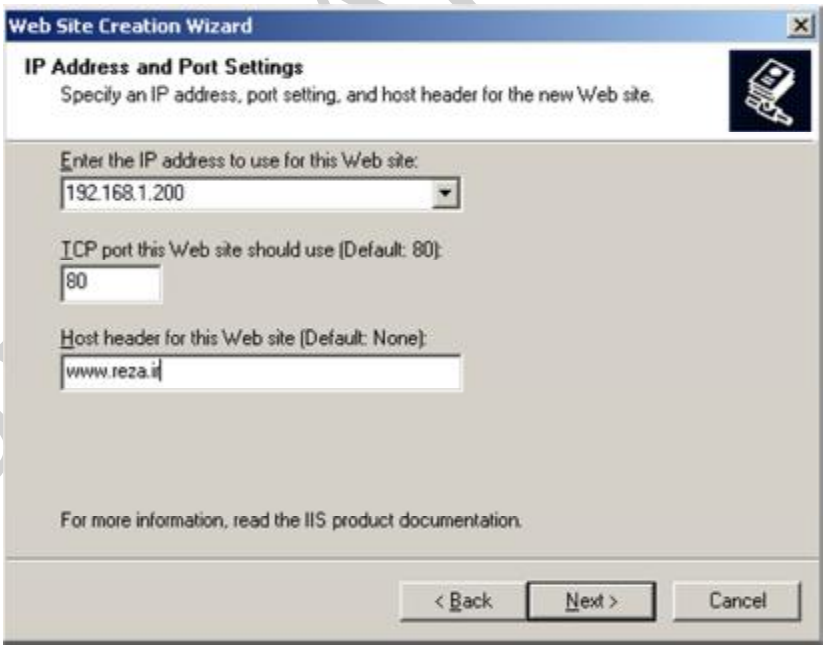
ابتدا وارد IIS می شویم

سپس باید New Website را بزنیم



در اینجا باید اسم سایت مورد نظرمان را وارد کنیم،باید قبلاً زونی به همین اسم و Arecord و C name را ساخته باشیم.

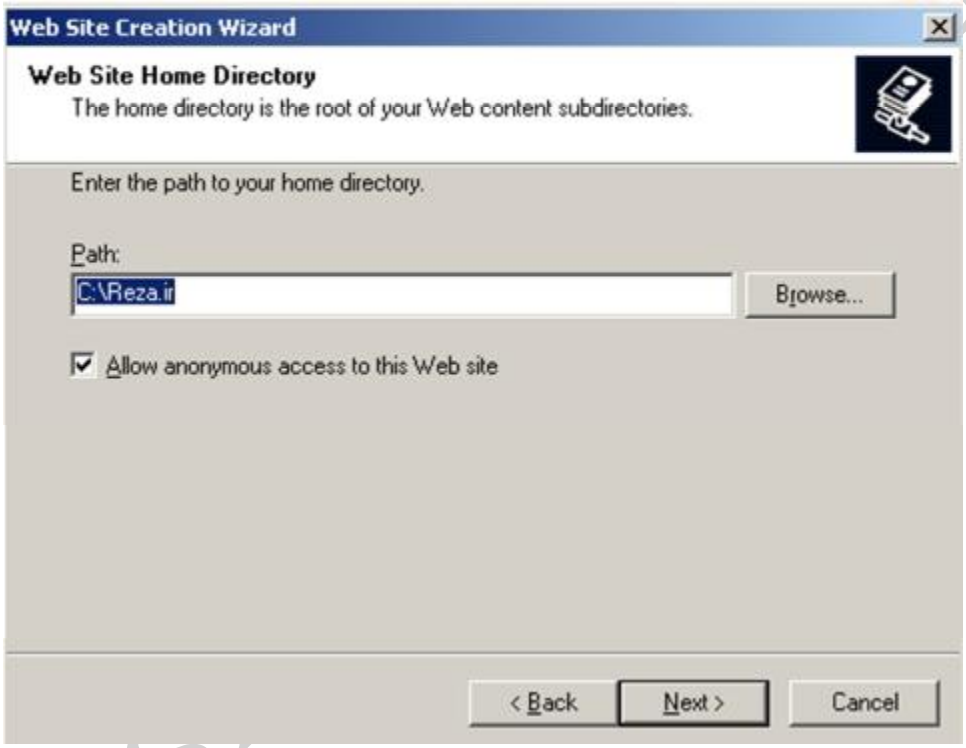
در اینجا باید Web Server ،Ip را وارد کنیم




در اینجا می توانیم پورت را از 80 به9000 تغییر دهیم و آدرس سایت را در Browser به این صورت وارد کنیم:

www.reza.ir:9000

در اینجا از ما مسیر صفحات سایت را می خواهد که ما در درایو C در پوشه ای به نام خود سایت صفحه ای به نام Index.htm ساخته ایم.(حتماً باید به این اسم باشد)، اگر تیک گزینه زیر فعال باشد هرکسی که بخواهد سایت را ببیند احتیاج به وارد کردن یوزر و پسورد ندارد ولی اگر تیک این گزینه فعال نباشد باید برای دیدن سایت یوزر و پسورد را وارد کنیم.




Fars

در این مرحله میزان دسترسی کاربر را تنظیم می کنیم.

Read : فقط می تواند سایت را ببیند.

Run Scripts : می تواند داخل سایت اسکریپت اجرا کند.

Execute : می تواند داخل سایت و سرور از طریق URL کامند Dos اجرا کند.

Write : اجازه نوشتن داخل سایت را دارد.

Browse : از طریق URL می تواند به قسمتی از هارد دسترسی پیدا کرد.

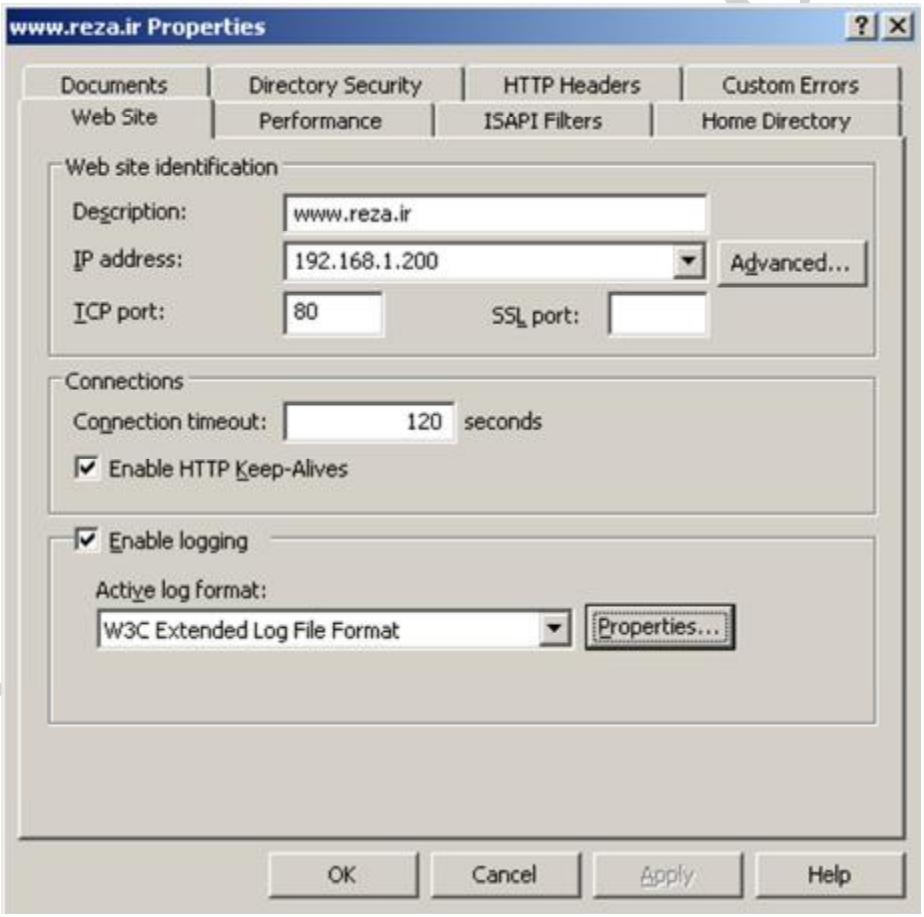
در آخر هم آدرس سایت را وارد Browser می کنیم و سایت را نشان می دهد.

FarshidAja...n

- در دنیای شبکه سایت ها بر 2 نوع می باشند Ip Base ، Name Base
- Ip Base: به ازای هر سایت احتیاج به Ip مجزا داریم.
- Name Base : روی یک Ip و یک Port می توان بی نهایت سایت بالا آورد، 2 مشکل در این حالت وجود دارد 1- نمی توان صفحات را https بالا آورد. 2- نمی توان پهنای باند را کنترل کرد.

**تنظیمات اضافی روی یک سایت**

ابتدا وارد IIS می شویم سپس بر روی اسم سایت Properties می گیریم و وارد تب Website می شویم.



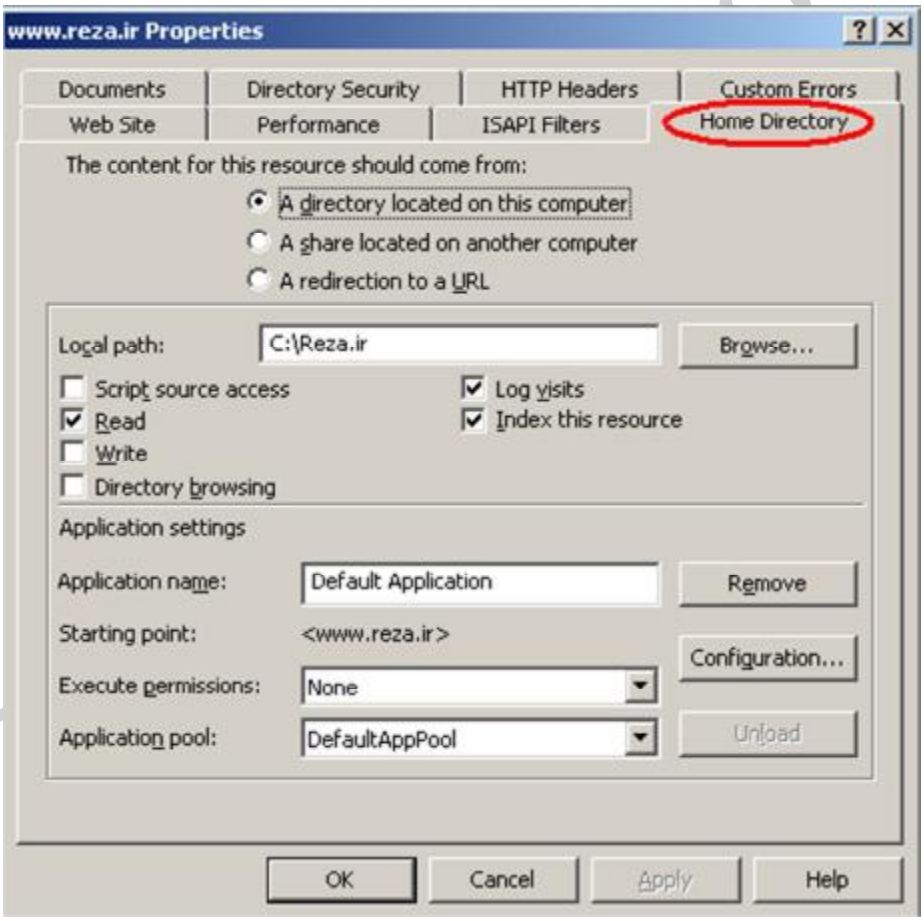
Sslport : همان پورت https است(443).

Connection timeout : مدت زمان انتظار برای Load سایت برای بازدید کننده .

Enable logging : با فعال بودن این گزینه هر کسی که از سایت بازدید کند اطلاعاتش مانند Ip, Server name و... ذخیره می شود.

W3C یعنی به فرمت TXT ذخیره می شود.

تب Home Directory




اولین گزینه محل قرارگیری صفحات سایت را از می پرسد که گزینه اول محل قرارگیری صفحات را در این کامپیوتر نشان می دهد،گزینه دوم از به اشتراک گذاشته شدن صفحات بر روی کامپیوتر دیگر اطلاع می دهد،گزینه سوم،با انتخاب این گزینه باید آدرس سایت را به آدرس دیگری Redirect کنیم مثلاً زمانی که وارد می کنیم Ali.com سایت Hani.com باز می شود.

در مرحله بعد نوع Permissions ها نمایان می شود.

Application name

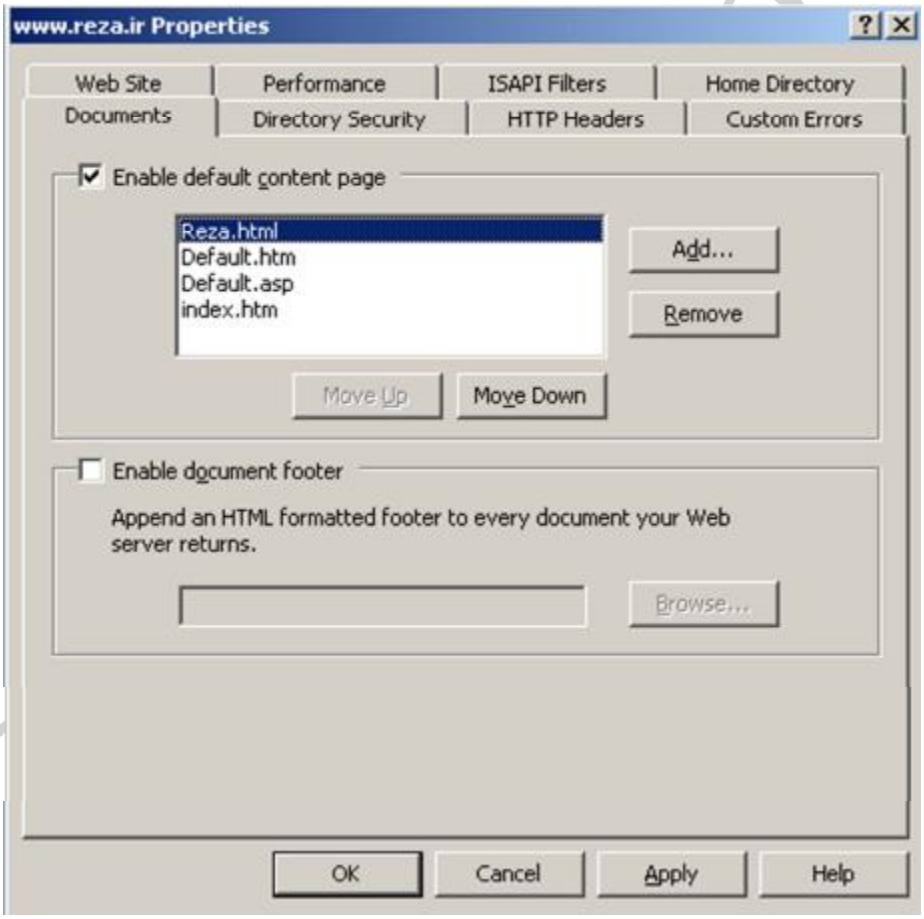
زمانی که بخواهیم سایتی را با IIS بالا بیاوریم احتیاج به نرم افزارهایی مانند .NET و... داریم که همه در Default Application وجود دارد.

Execute Permissions

اگر سایت را با Active Server Page که یک زبان طراحی سایت به صورت دینامیک می باشد،طراحی کردید و می خواهید IIS آن را Load کند باید Execute Permissions برروی

تنظیم شود.

تب Documents

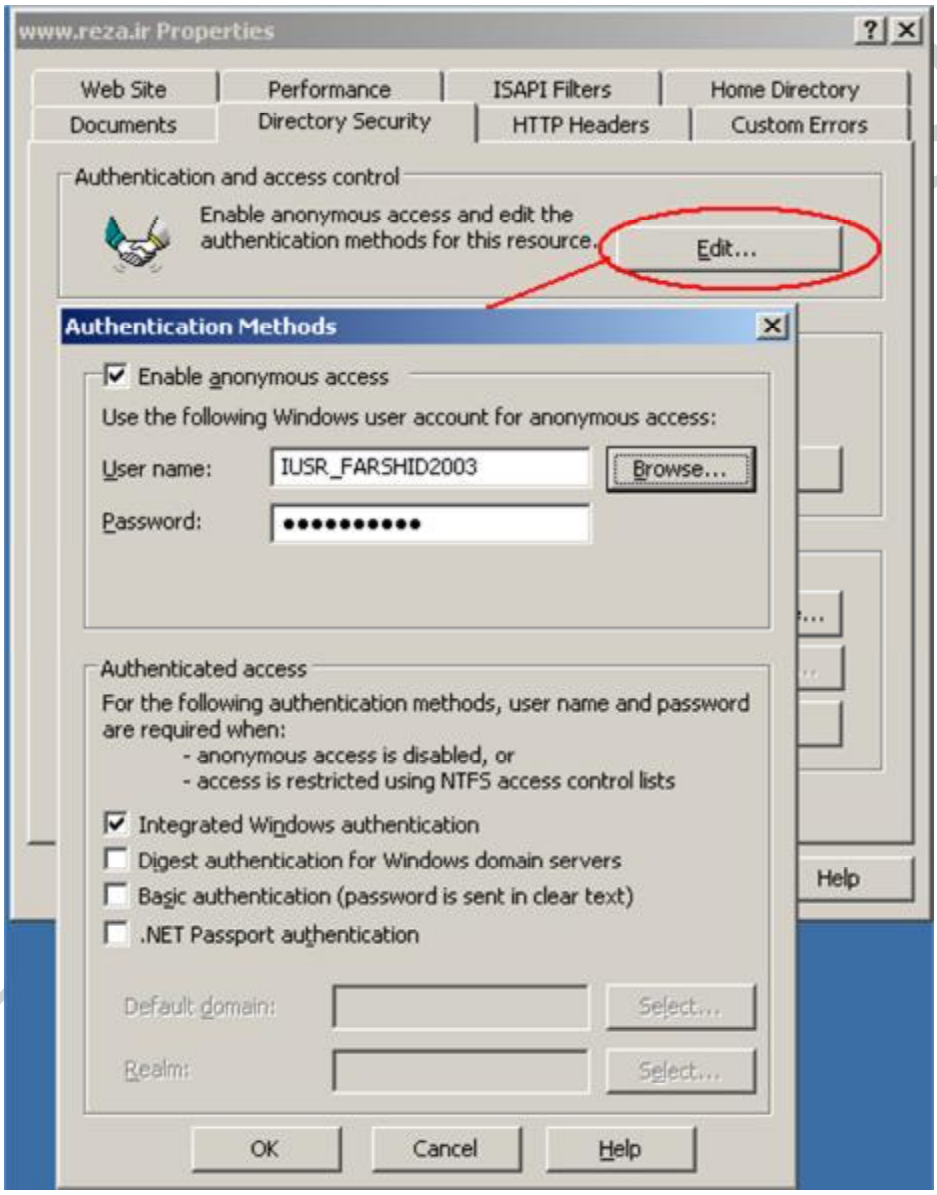



در قسمت اول می توان با زدن دکمه Add و با تایپ کردن اسم اولین صفحه سایت Reza.html (که بصورت پیش فرض index.htm است)اسم اولین صفحه سایت را تغییر دهیم (به دلیل امنیت)

در قسمت Footer می توان در قسمت پایین صفحه با HTML چیزی بنویسیم که هر کسی سایت را بازدید کرد برایش نمایش داده شود.

تب Directory Security

با زدن اولین Edite در این صفحه وارد صفحه دیگری می شویم که در این صفحه اگر گزینه ...Enable را غیر فعال کنیم زمانی که بخواهیم وارد سایت شویم از ما یوزر و پسورد می خواهد.




در قسمت دوم این صفحه 4 گزینه به صورت زیر وجود دارد.

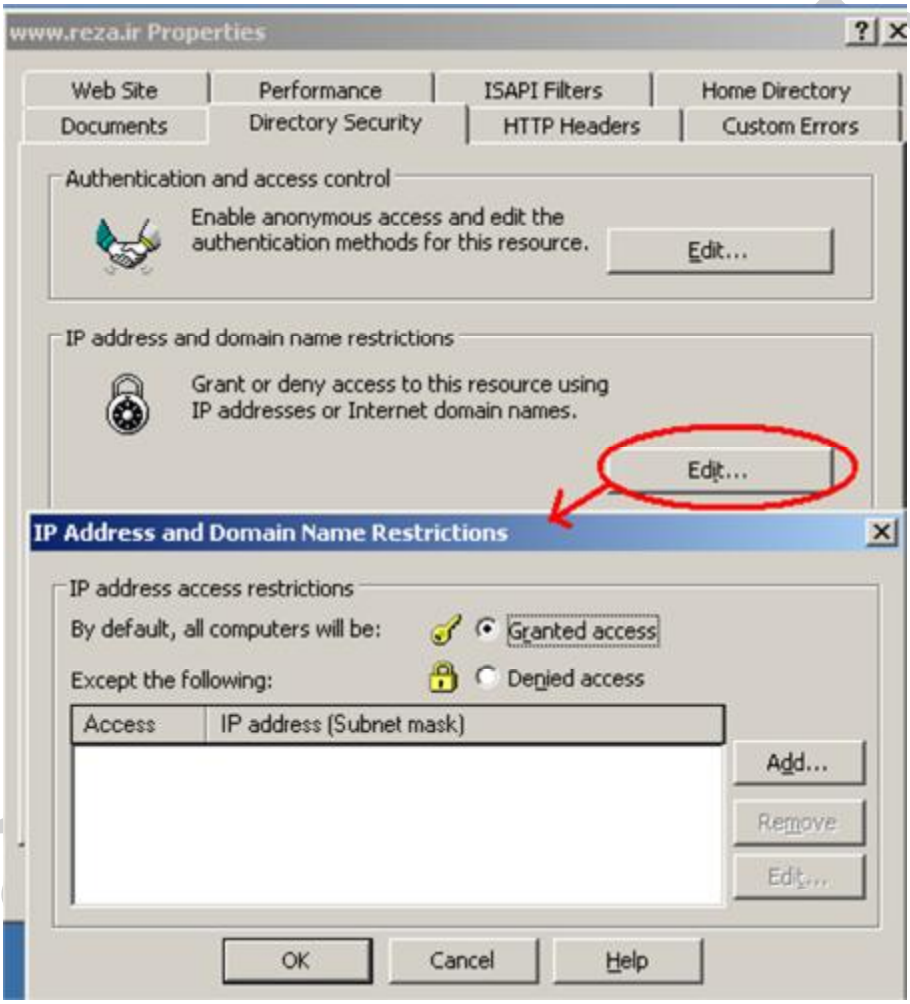
1- با فعال بودن این گزینه کلاینت ها باید یوزر پسوردهایی را وارد کنند که در این کامپیوتر(سرور) وجود داشته باشد،این گزینه با IEسازگار می باشد.

2- تمامی یوزر و پسوردها در دامین می باشند و کاملاً رمز گذاری شده هستند.

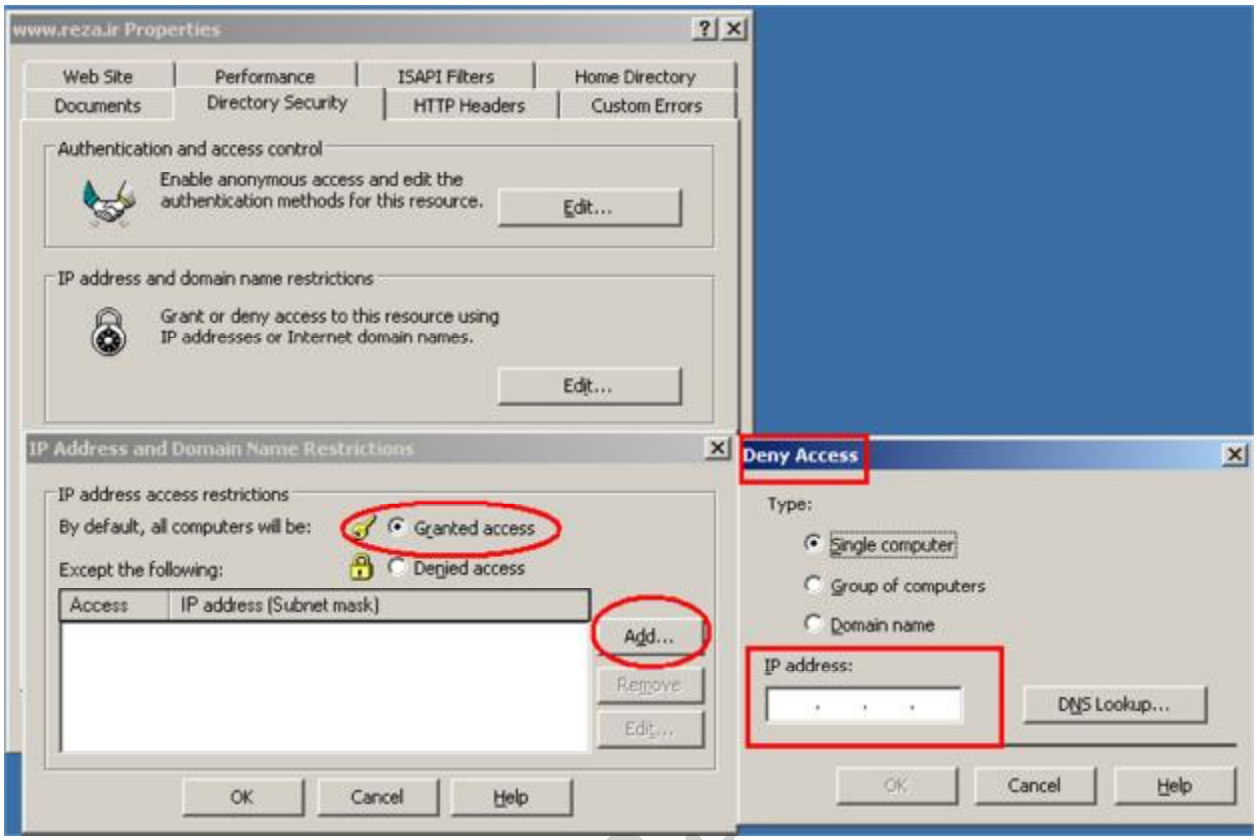
3- دقیقاً مانند گزینه1 می باشد با این تفاوت که با تمامی مرورگرهای اینترنتی سازگار می باشد.

4- این گزینه در حقیقت پروژه ای برای ماکروسافت بود،به این صورت که قراربود به ازای هر نفر که به اینترنت متصل می شود یک اکانت Hotmail( Windows Live) برایش ساخته شود در حقیقت این اکانت شناسه هر کاربر در اینترنت بود.(پروژه با شکست مواجه شد! )

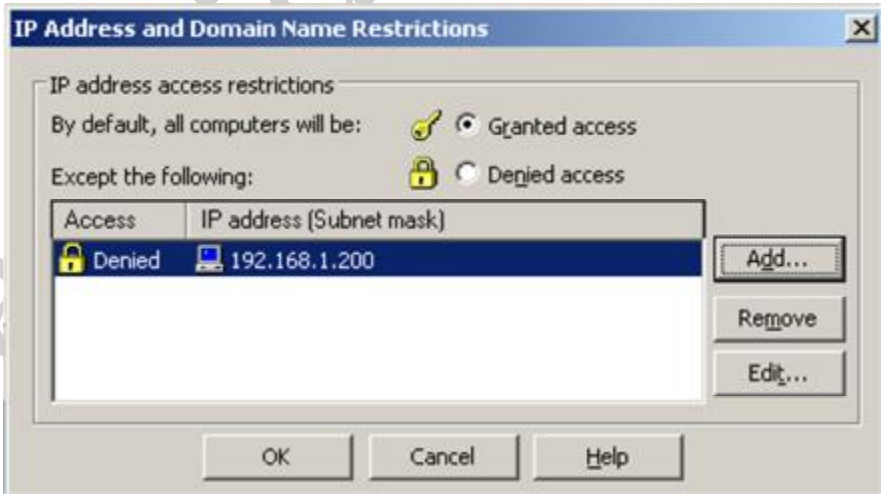
دراین قسمت می توان بگوییم که چه کسانی بتوانند به سایت ما دسترسی داشته باشند و چه کسانی دسترسی نداشته باشند.



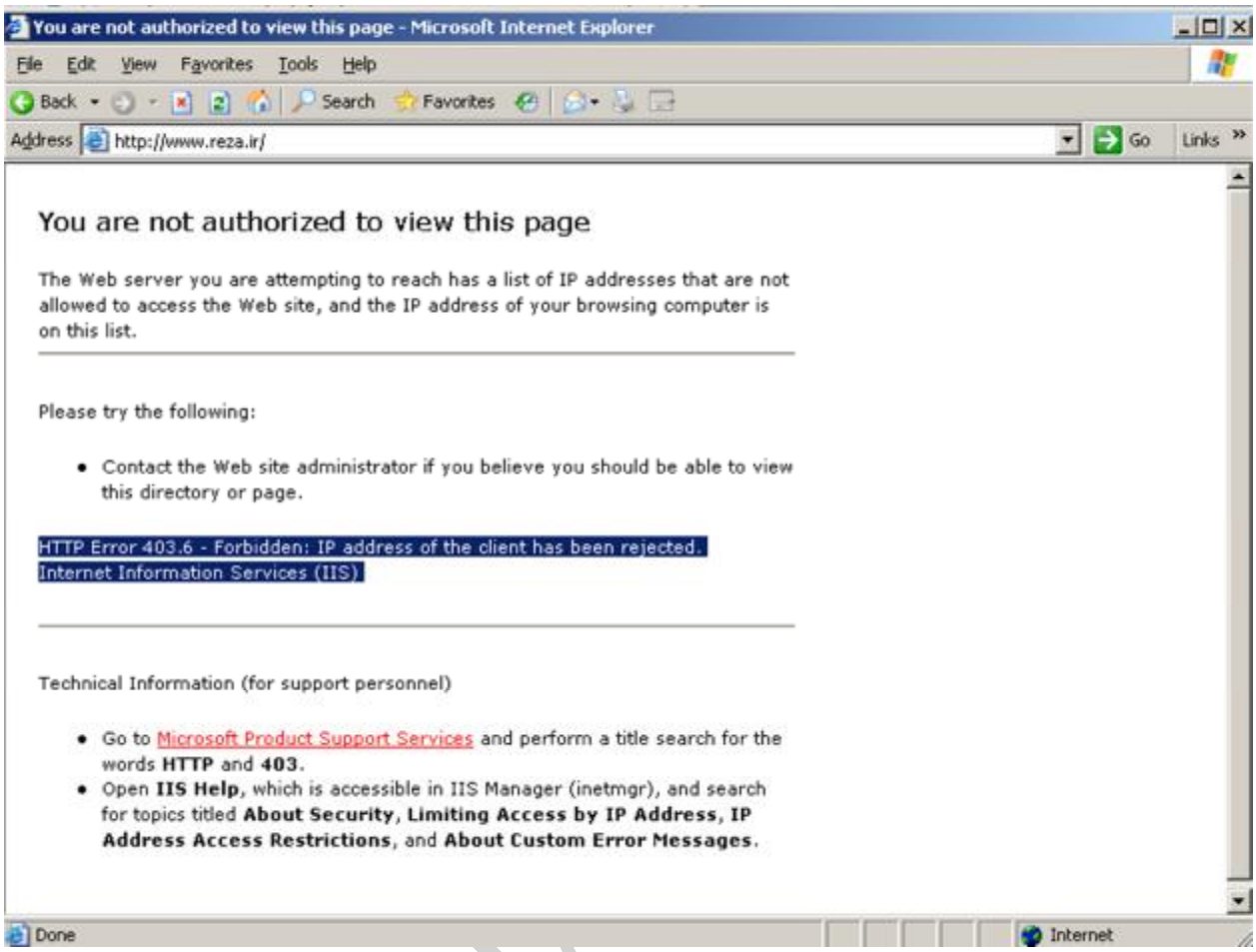

با انتخاب این گزینه می توانیم یک کامپیوتر یا گروهی از کامپیوتر ها (با وارد کردن رنج Ip )یا با وارد کردن اسم دامینی دسترسی آنها را به سایت خود ببندیم.




در اینجا با وارد کردن 192.168.1.200 Ip دسترسی این کامپیوتر به سایتمان را می بندیم(Denied ).




زمانی که از کامپیوتر 192.168.1.200 می خواهیم به سایت مورد نظر برویم با Error زیر مواجه می شویم.

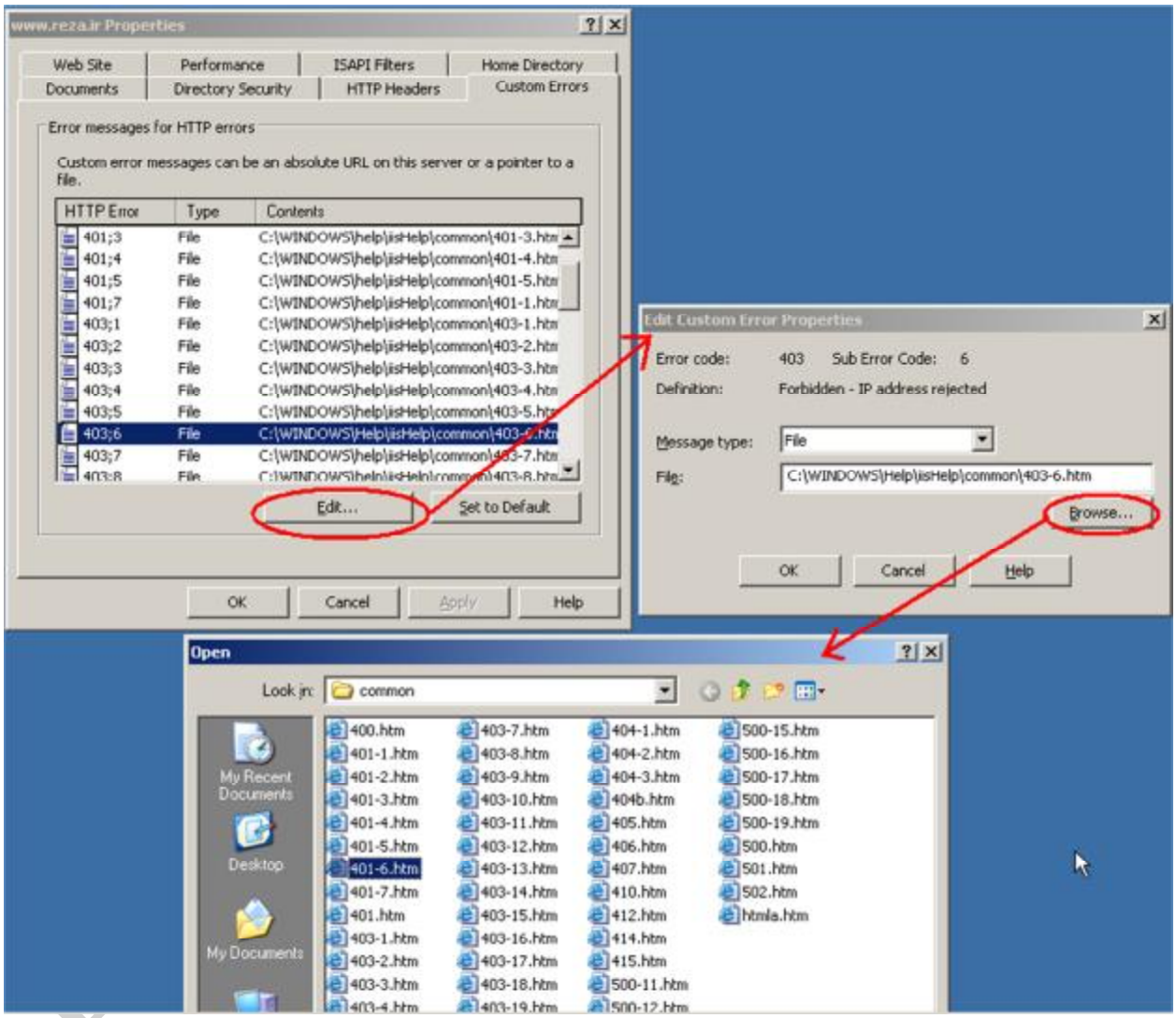



این Error به این معنی است که اجازه دسترسی این کامپیوتر به سایت مورد نظر توسط IIS گرفته شده است.

Farshid

تب Custom Errors

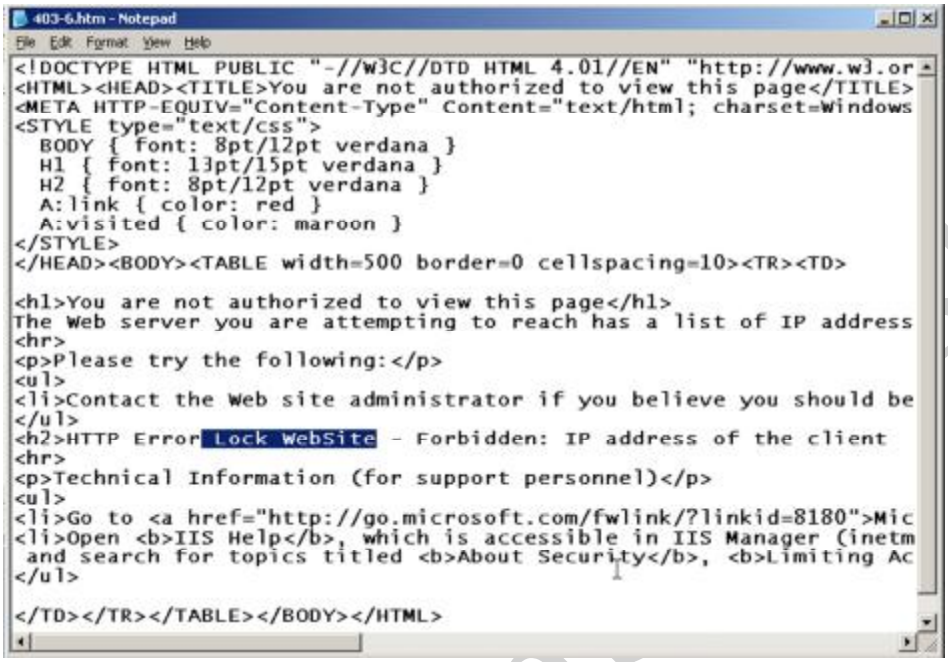
در این تب می توان Error های IIS را به دلخواه ویرایش کنیم، به این ترتیب که Error مورد نظر را انتخاب می کنیم سپس Edit را می زنیم ودر صفحه باز شده مسیر ذخیره آن را نشان می دهد که با زدن Brows پنجرهدیگری باز می شود.

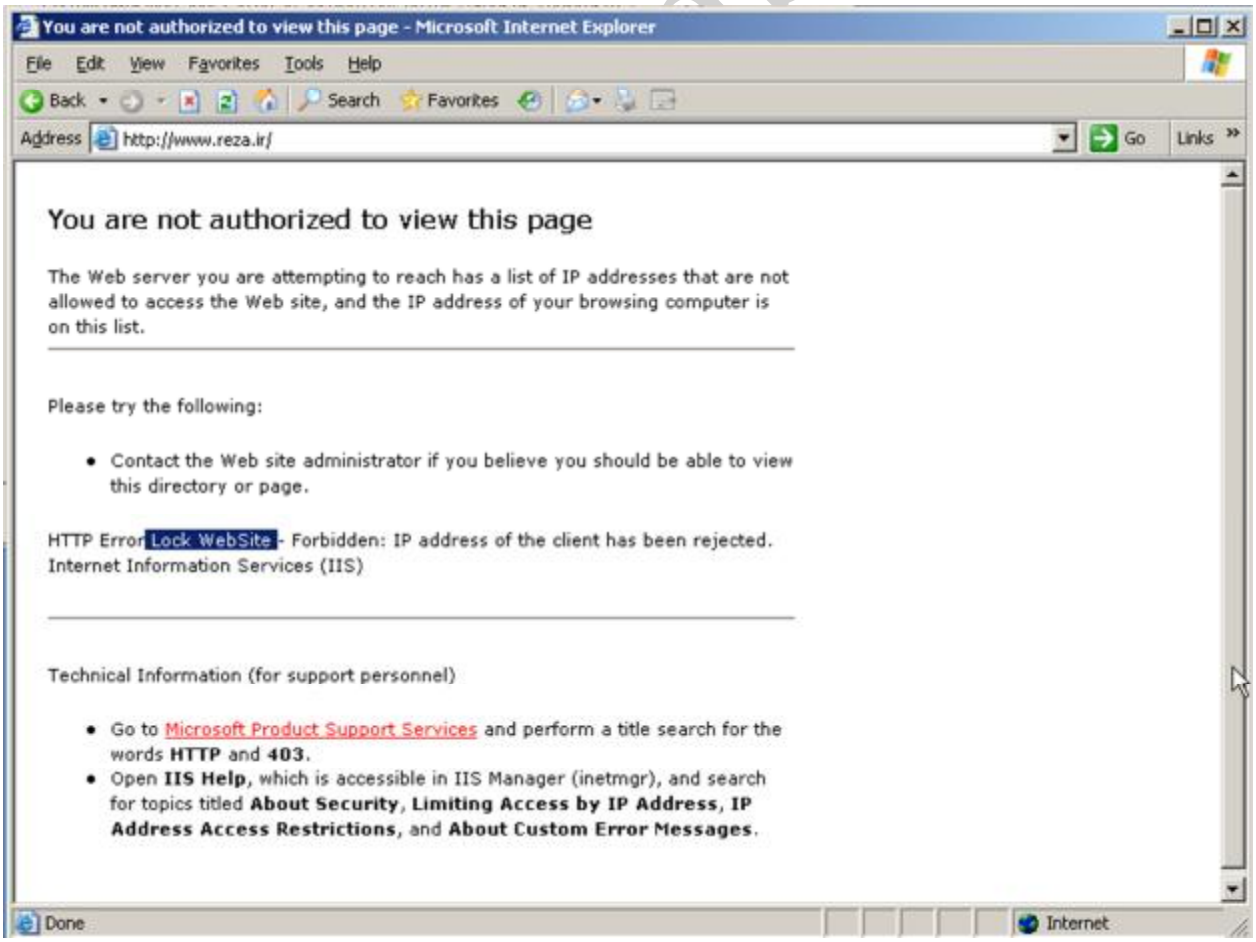



در این پنجره بر روی Error مورد نظر کلیک راست و Edit را می زنیم.

در صفحه باز شده می توانیم بر روی کد Error مورد نظر هر متنی را که بخواهیم جایگزین کنیم.

در این صفحه به جای کد عبارت Lock Website را وارد کرده ایم.



تبدیل سایت HTTP به HTTPS

برای این کار از پروتکلی به نامSSL( Secure Socket Layer ) استفاده می شود،سایت های HTTPS برای رمز نگاری اطلاعات از این پروتکل استفاده می کنند،پورت SSL 443 می باشد،به سروری که امکان استفاده از این پروتکل(SSL ) را برای ما فراهم می کند CA سرور گویند.

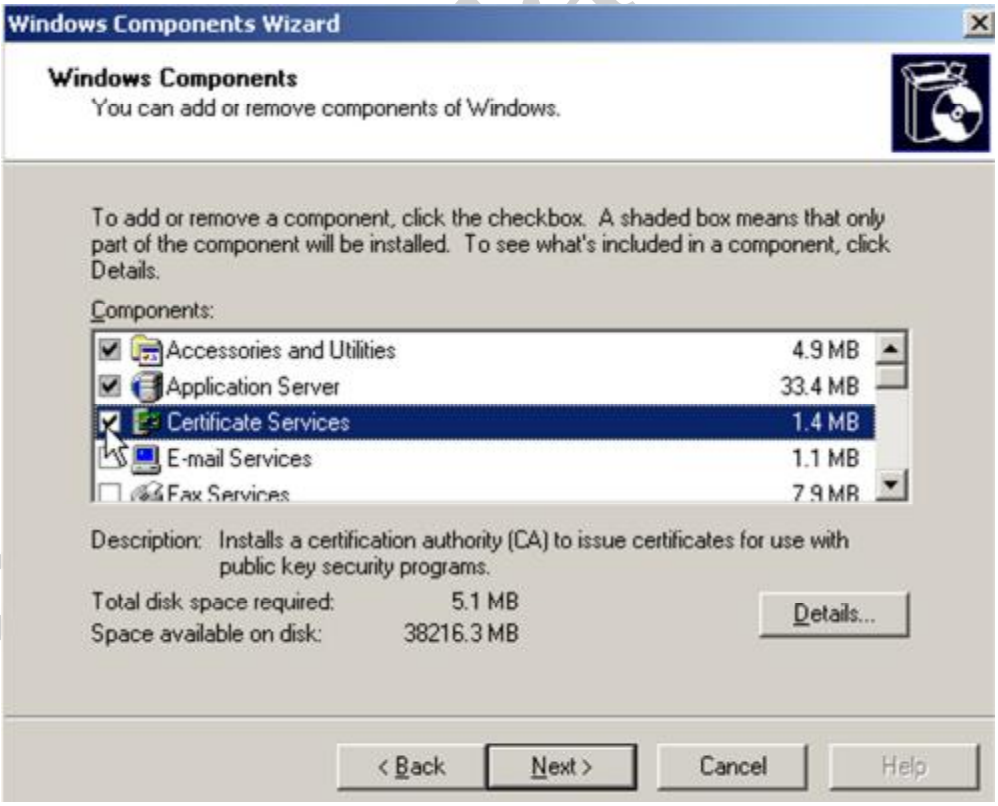
زمانی که می خواهیم به یک سایت HTTPS وصل شویم یک CA سرور هم وجود دارد که در زمان اتصال به سایت 2 کلید به نام های Public Key و Private Key تولید می کند،زمانی که سایت HTTPS را باز می کنیم یک پیغام مبنی بر اینکه CA سرور می خواهد یک کلید بر روی کامپیوتر ما بسازد نمایان می شود که حتماً باید آن را قبول کنیم این کلید از نوع Public می باشد. بعد از ساخته شدن این کلید بر روی سیتم در هنگام ارتباط ما با سایت اطلاعات را ما با Public رمز گذاری می کنیم و سرور هم آنها را با Private باز می کند.

- برای استفاده از HTTPS باید CA سرور داشته باشیم.

طریقه نصب CA سرور در 2003

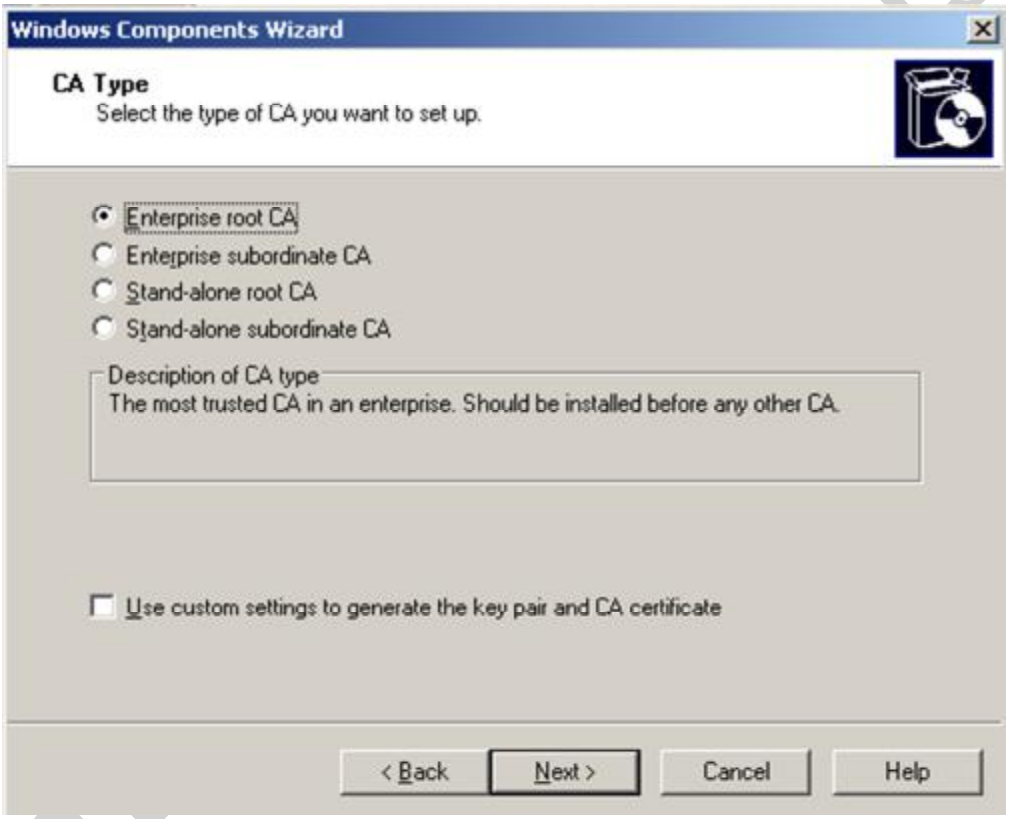
پیشنیاز CA نصب اکتیو دایرکتوری می باشد،

وارد Windows Components می شویم سپس گزینه Certificates Services را انتخاب می کنیم

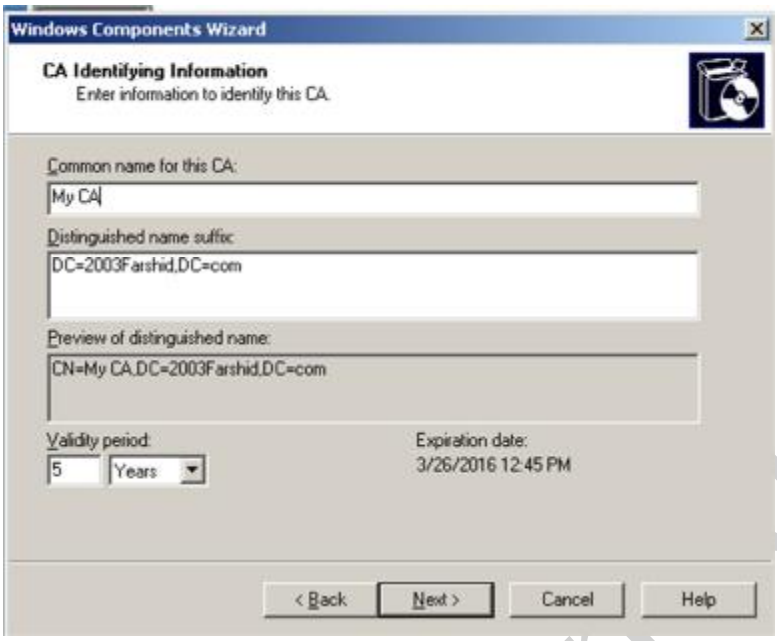


در این مرحله4 گزینه وجود دارد،زمانی که اکتیو دایرکتوری و CA سرور بر روی یک کامپیوتر نصب باشد از Enterprise استفاده می کنیم،زمانی که اکتیو دایرکتوری و CA سرور هر کدام بر روی یک کامپیوتر نصب باشند از Stand-alone استفاده می کنیم.

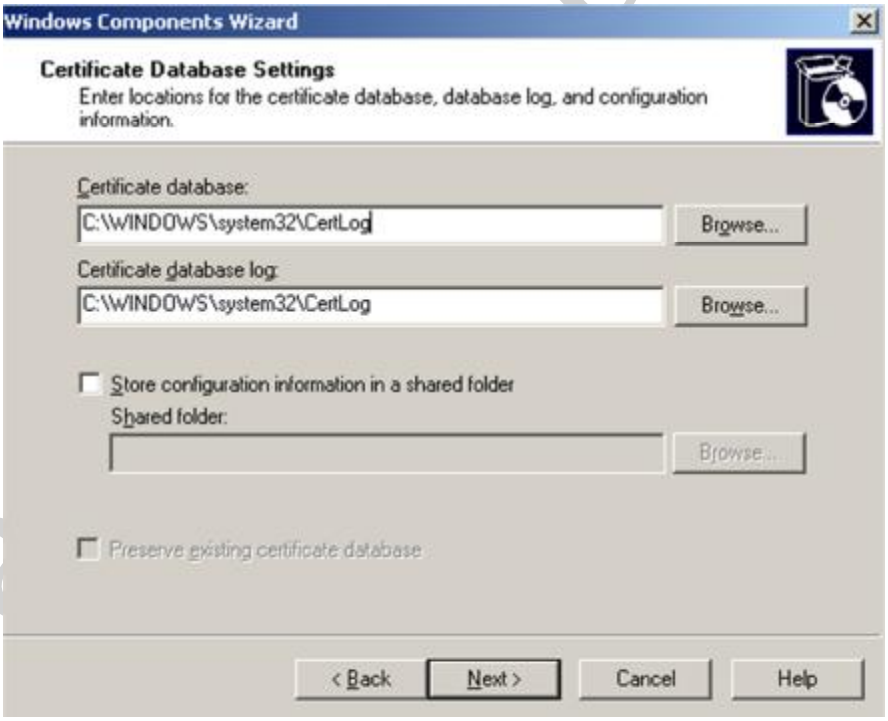
زمانی که خود CA تولید کننده گواهینامه باشد از Root Ca و زمانی که CA گواهینامه را از جایی دیگر مانند Verisign می گیرد از Subordinate استفاده می کنیم که این گزینه(Subordinate )در شبکه های اینترنتی کاربرد دارد.




در مرحله بعد باید یک اسم برای CA سرور وارد کنیم (My Ca )

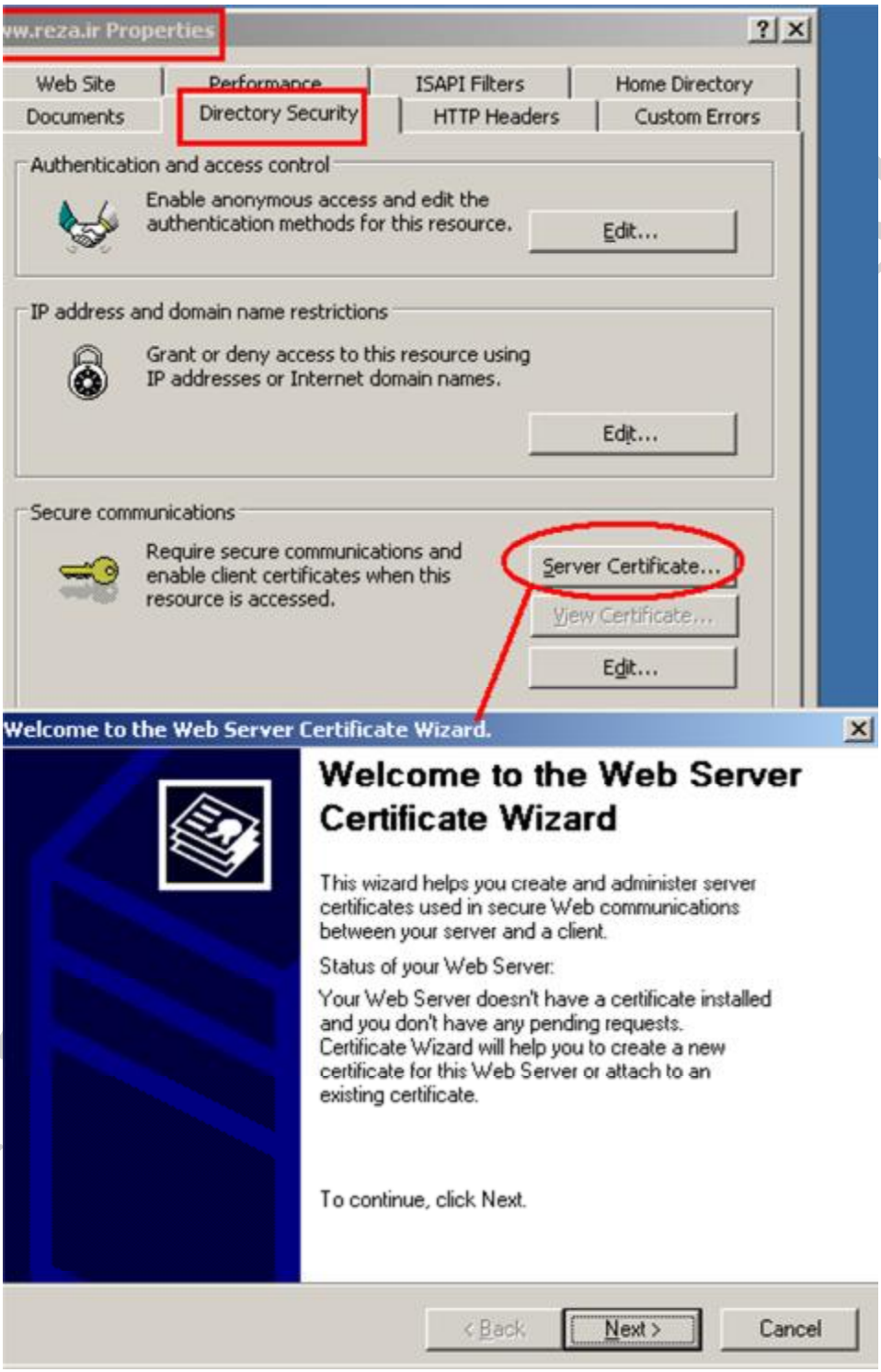



**در مرحله بعد محل ذخیره شدن کلید ها را نمایش می دهد.**

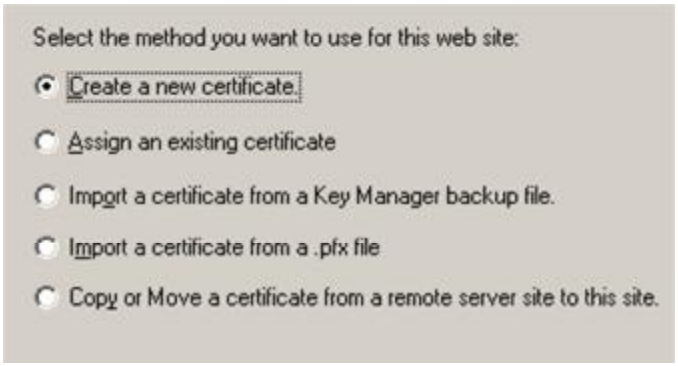



Farshid

در مرحله بعد وارد IIS می شویم بر روی اسم سایت Properties و وارد تب Directory Security می شویم در این مرحله یک گواهینامه از CA برای IIS می گیریم.

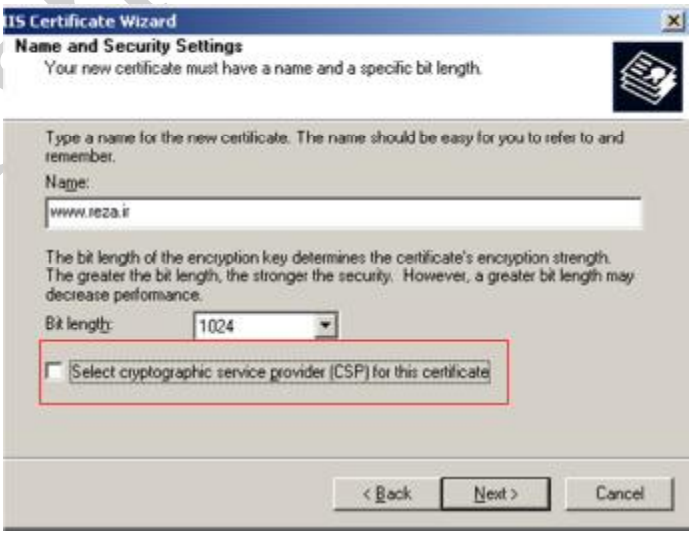


در اینجا چون ما گواهینامه را نداریم برای ایجاد آن گزینه اول را انتخاب می کنیم



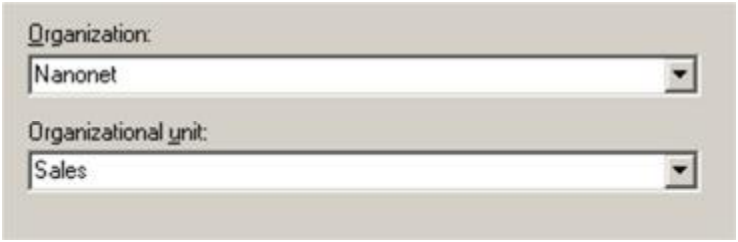

در اینجا باید عبارت دوم را انتخاب کنیم، با انتخاب این گزینه مراحل ساخت و جا سازی کلید های Public و Private به صورت اتوماتیک انجام می شود اگر گزینه اول را انتخاب کنیم هر کس که بخواهد از سایت ما بازدید کند ما باید به صورت دستی هر بازدید کننده را تایید کنیم.

در این مرحله از ما می خواهد که CSP را برایش مشخص کنیم،به شرکتی که کایدهای رمز نگار را تولید می کند CSP گویند،نام این شرکت RSA است.



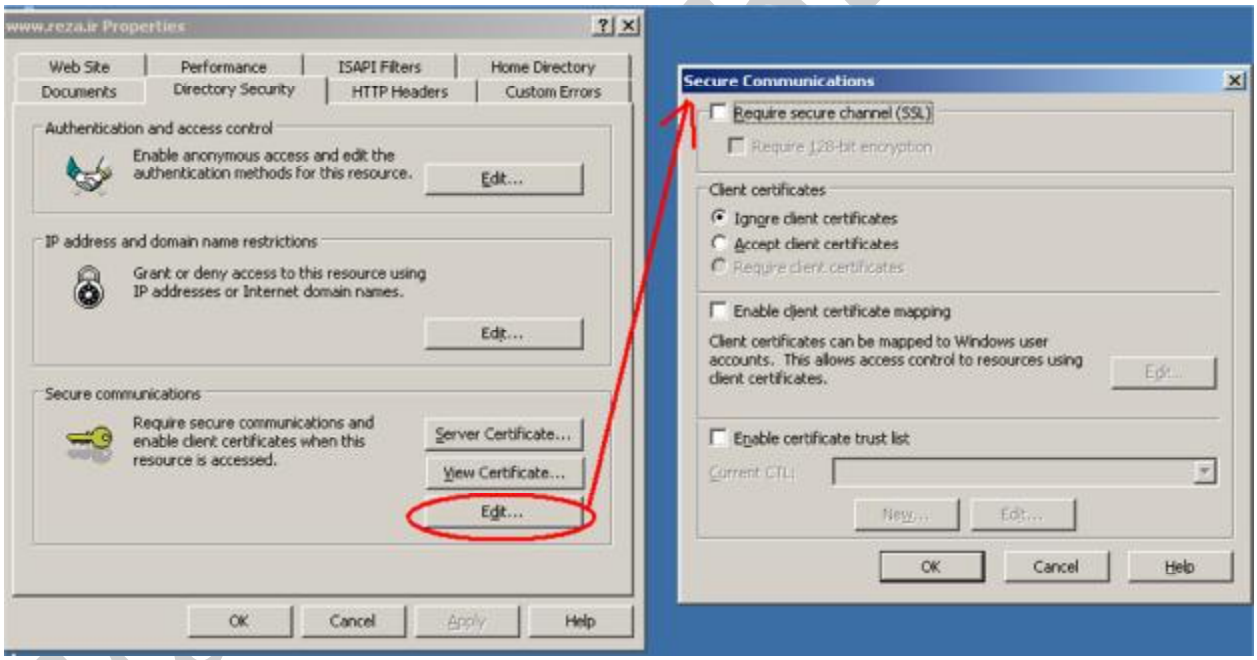

Farhiz Ghanbroush

در این مرحله از ما محل کار و واحد کاری را می پرسد

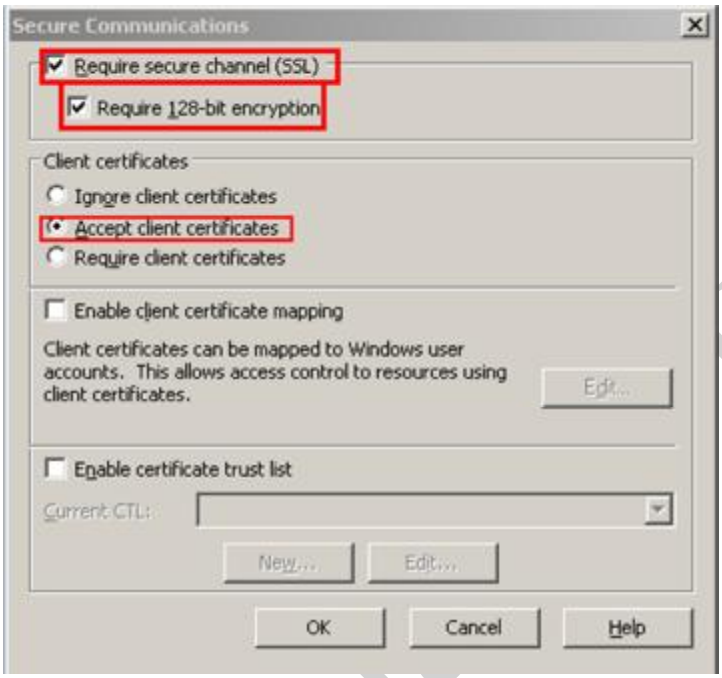



در اینجا می توانیم پورت را تغییر دهیم، در صورت تغییر باید آخر آدرس از : و در ادامه شماره پورت را وارد کنیم بهتر است این گزینه را تغییر ندهیم

بعد از پایان این مرحله،Edit را می زنیم

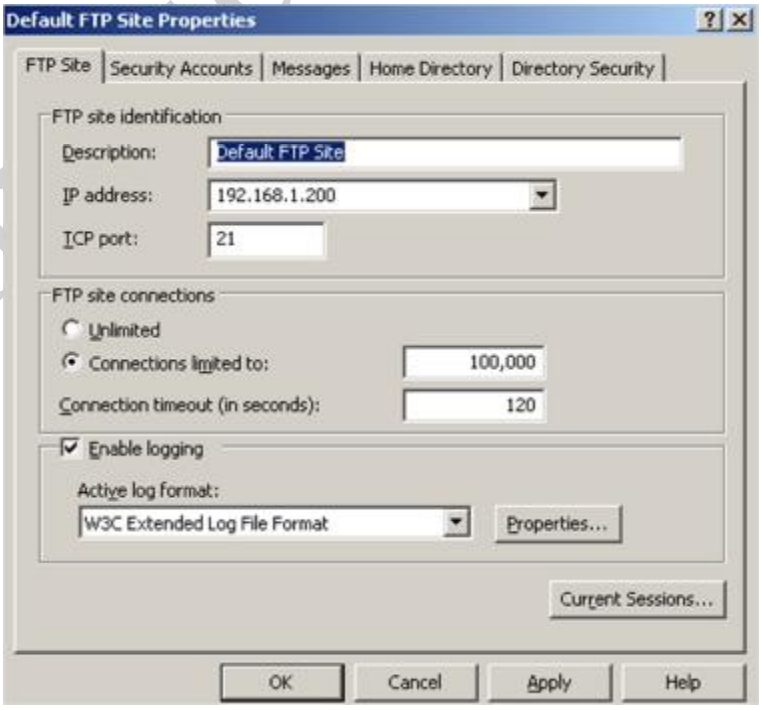


در اینجا باید  سه گزینه زیر را انتخاب کنیم،گزینه اول می گوید حتماً باید وب سایت با HTTPS باز شود، گزینه دوم می گوید طول رمز نگاری از 128 کمتر نباشد،گزینه سوم می گوید زمانی که کلاینت اطلاعات را رمز می کند و آن را ارسال می کند قبول کن .




FTP دار کردن سایت ها

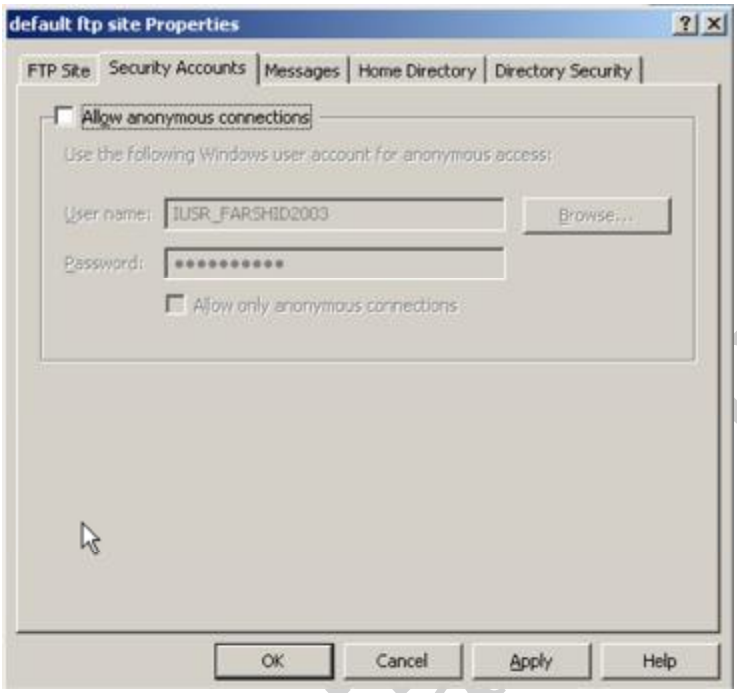
بر روی Default Ftp Site کلیک راست کرده و Properties می گیریم در صفحه باز شده ابتدا Ip را وارد کرده



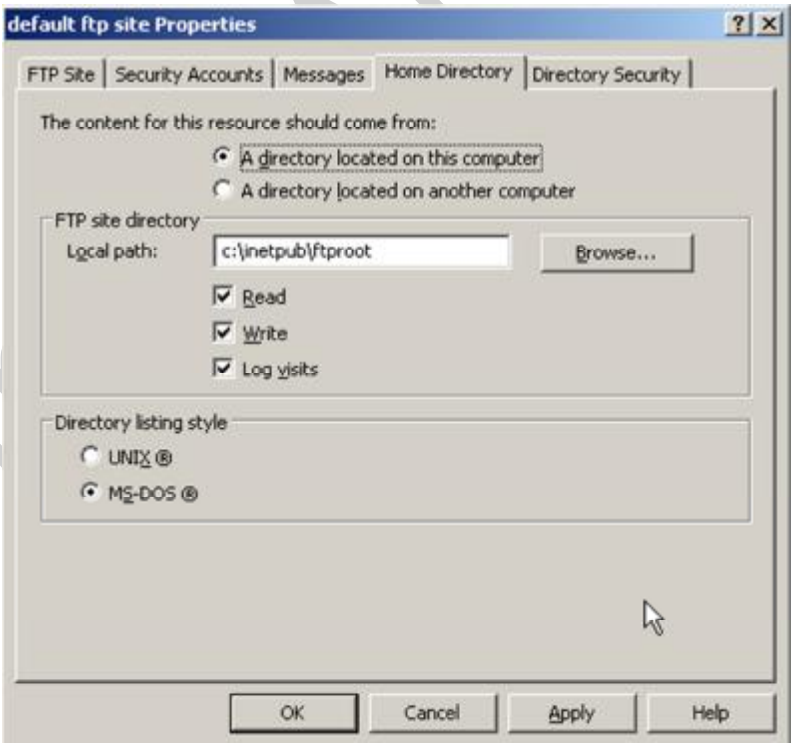

FarhadAjamush

در قسمت پایین صفحه اگر بر روی Current Sessions کلیک کنیم نشان می دهد چه کسانی متصل هستند.

در این تب باید گزینه .... Allow غیر فعال باشد تا فقط کسانی بتوانند FTP کنند که یوزر و پسورد را داشته باشند.



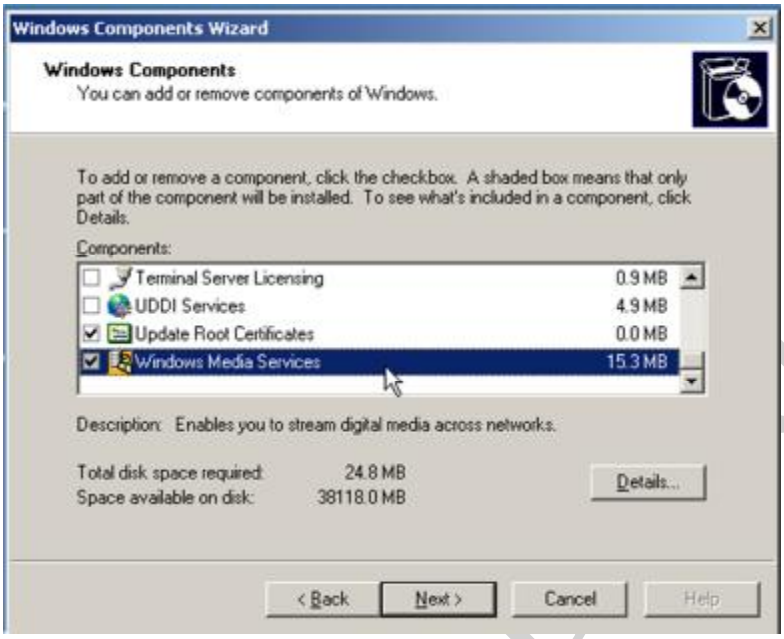

در این تب باید دسترسی Write را هم بدهیم تا بتوانند تغییرات را اعمال کنند.




بعد از اتمام تنظیمات داخل مرورگر FTP.Reza.ir را وارد می کنیم تا بتوانیم روی سایت Reza عمل FTP را انجام دهیم.

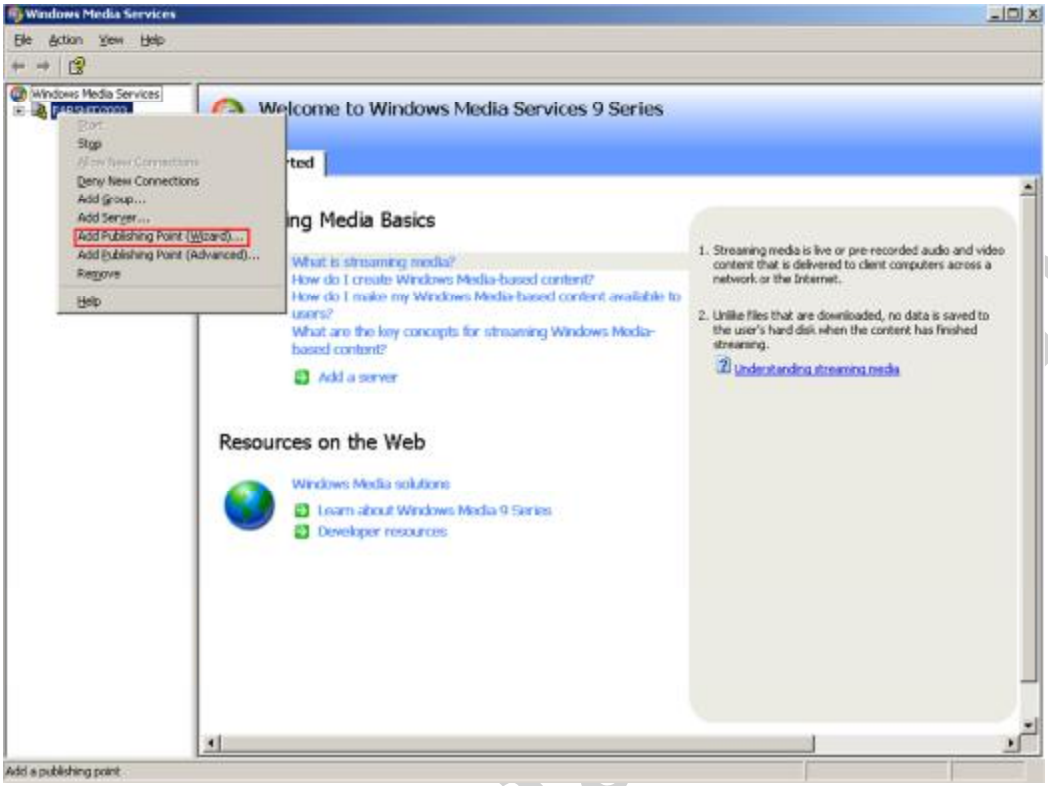
## پخش کردن فیلم تحت شبکه ( Media Server ) در 2003

**ابتدا وارد Component ها می شویم و سرویس Windows Media را نصب می کنیم.**

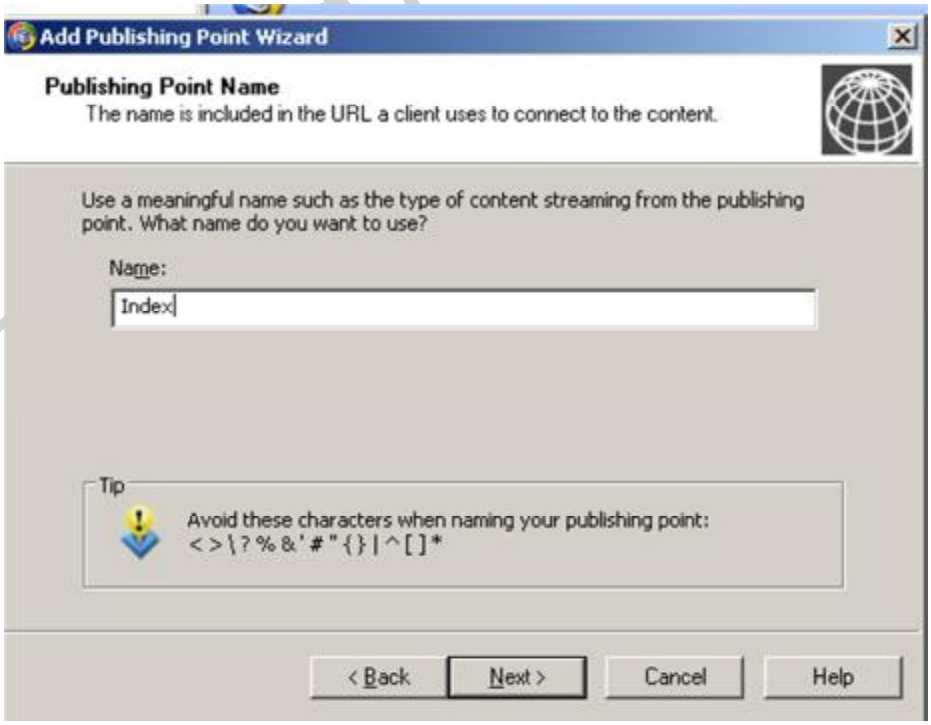



**بعد از نصب آن را از مسیر زیر باز می کنیم**

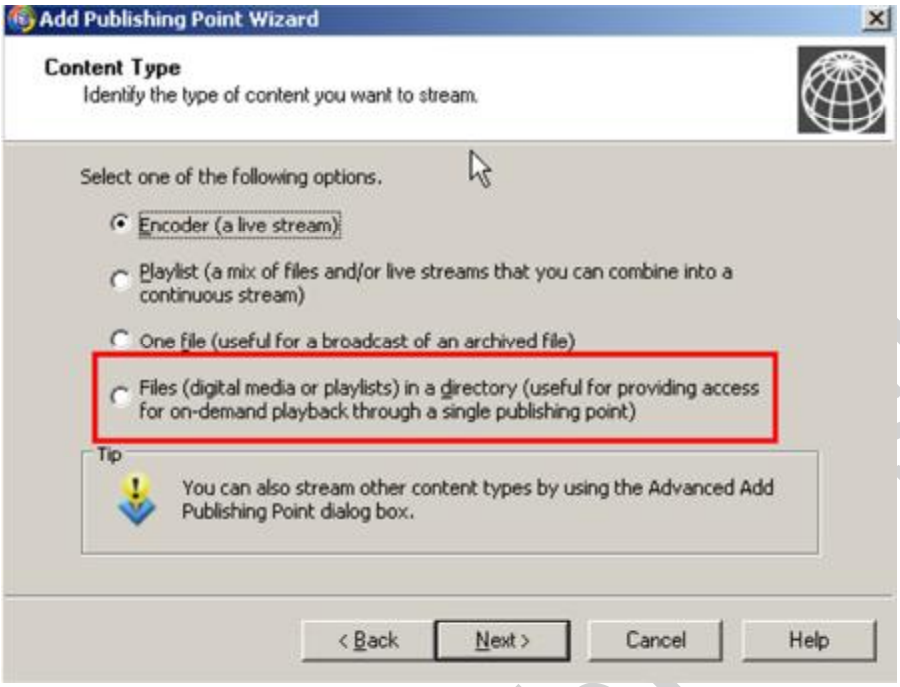
به فیلم هایی که برای کلاینت ها به نمایش (Stream ) می گذاریم Publishing Point گویند.



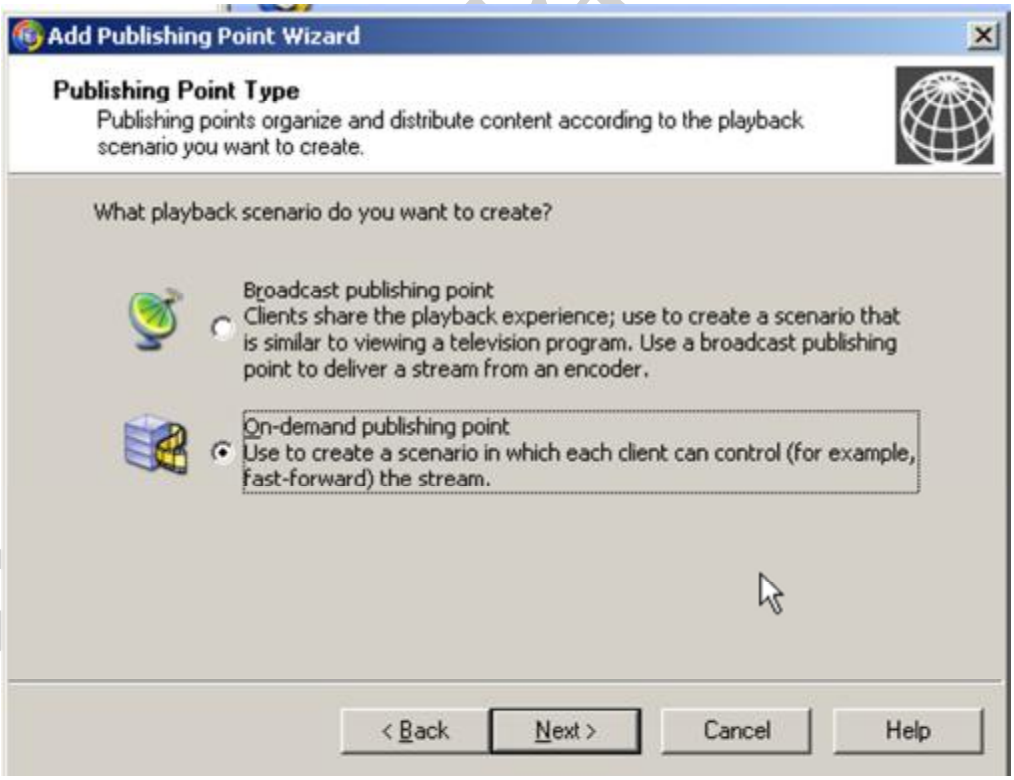

حالا باید یک اسم برای فیلم تعریف کنیم



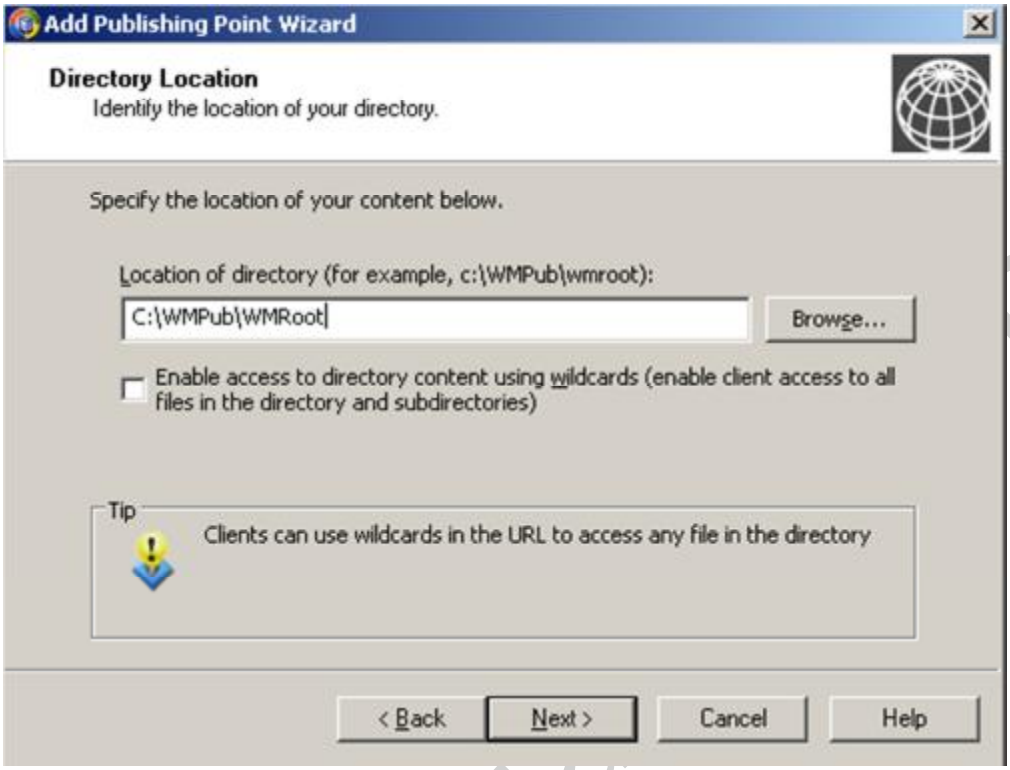

در اینجا عبارت 4 را انتخاب می کنیم چون فیلم در هارد کامپیوتر ذخیره می باشد



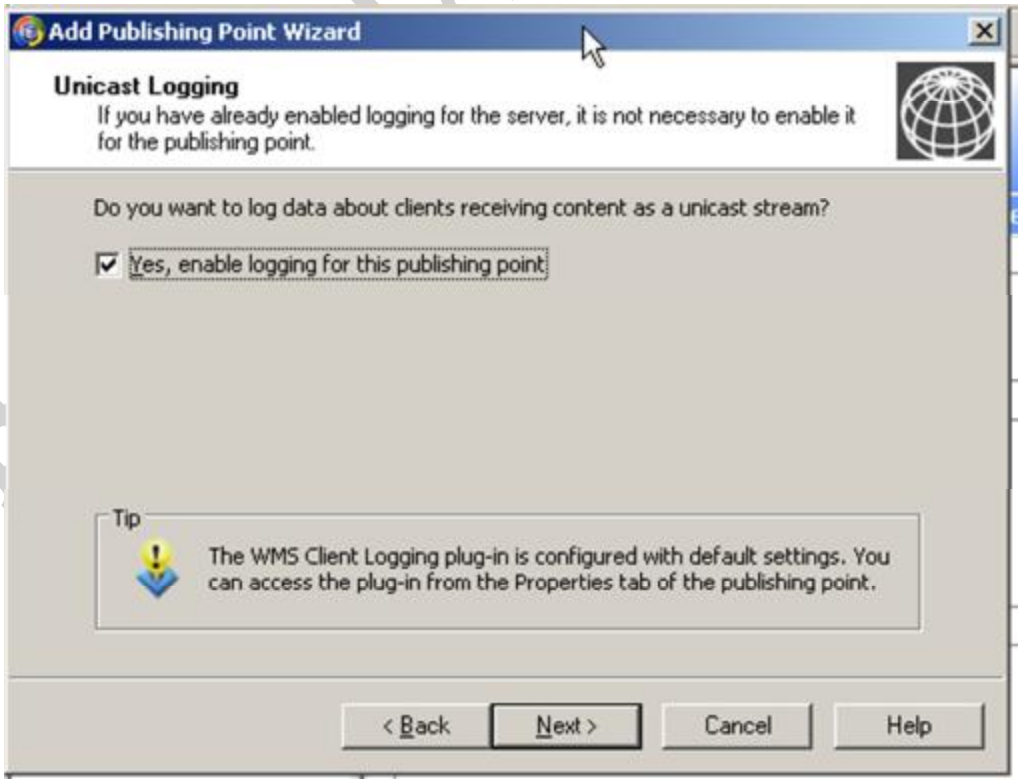

در این قسمت 2 گزینه موجود می باشد 1)BroadCast که در اینجا یعنی به صورت زنده فیلم را از دیش می گیریم 2)On-demand یعنی فیلم بر روی هارد ذخیره می باشد.



در اینجا محل ذخیره سازی فیلم ها را نشان می دهد.



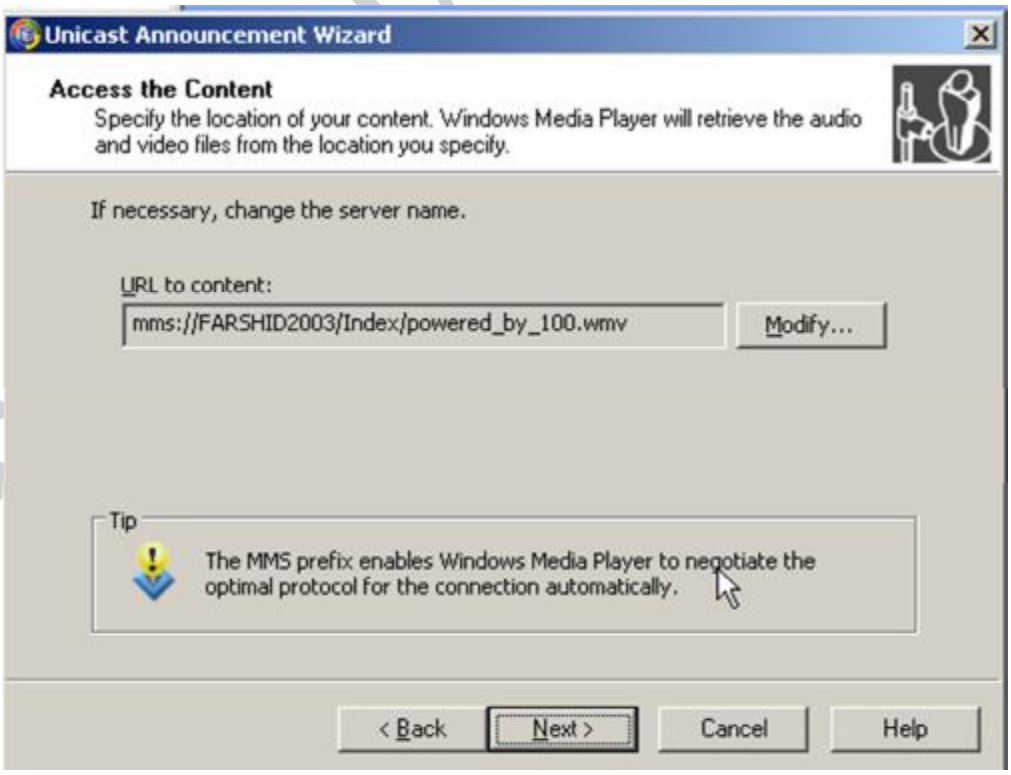

باید گزینه Enable Login فعال باشد تا Log فیلم ها را بندازد.



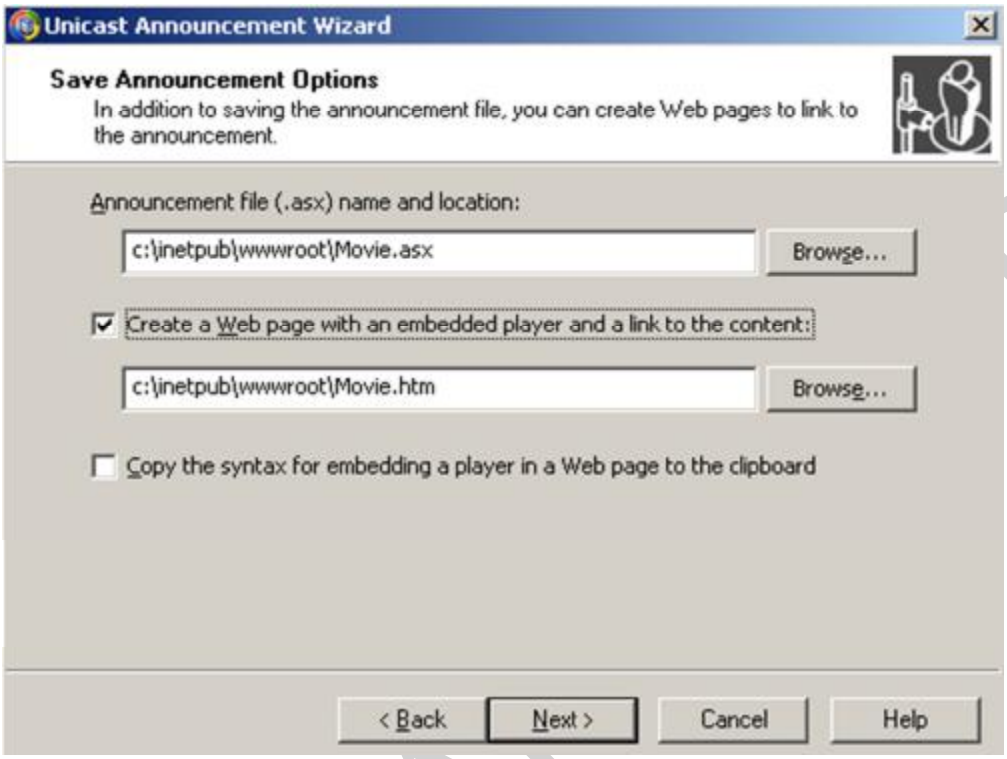
در این مرحله باید گزینه اول انتخاب شود تا فیلم به صورت اتوماتیک برای همه پخش شود.

بعد از Finish یک صفحه Wizard دیگر باز می شود.

در اینجا باید این آدرس را مرورگر کلاینت ها کپی می کنیم.



در اینجا گزینه ....Create را انتخاب می کنیم تا فیلم در وسط صفحه نمایش داده شود.




و در آخر هم Finish می کنیم.

حالا در URL آدرس ...mms:// را تایپ می کنیم و فیلم نمایش داده می شود.می توانیم در URLhttp:// ipserver را هم بنویسیم.

- در2008 Media Server به عنوان یک سرویس موجود نمی باشد باید حتماً از مایکروسافت دانلود شود,چون این سرویس به عنوان Additional Role می باشد.
- برای دیدن فیلم به صورت HD باید به دنبال Cache Proxy Management باشیم.

FarshidAjorloo

## IP V6

این Ip 128 بیتی می باشد،به نوع نوشتن این Ip ,Colon Hexa decimal گویند.

2001:1234:0000:0000:AB01:0000:0001:0002

فرمول ساده کردن Ip v6

- اگر در طول Ip, 4 صفر پشت سر هم بیایند می توان آنها را با یک صفر جایگزین کرد ( 0=0000 ).
- در طولIpامی توان صفرهای پشت سر اعداد را حذف کرد(2=0002 ).
- اگر در طول Ip, 2تا صفر خلاصه شده یا بیشتر پشت سرهم بیایند را می توان با 2 کالون( : : ) نمایش داد (:: = 0000:0000 ).
- در طول Ip فقط یکبار مجاز به استفاده از 2 کالون( : : ) می باشیم.

خلاصه شده Ip بالا برابر با 2001:1234::AB01:0:1:2 می شود.

- در Ip6 چیزی به نام NetMask نداریم جایگزین NetMask,Prefix می باشد(جداسازی Host id از Net id )

2001:1234:0000:0000:AB01:0000:0001:0002/64 در اینجا 64/ یعنی باید از سمت چپ 64 بیت به جلو برویم بعد از 64/ ,Host Id می شود و قبل از آن Net Id . ( هر عدد در اینجا معادل 4 بیت می باشد).

- در IP V4 , Unicast – Multicast – Broadcast داشتیم در IP V6 بجای Broadcast – , Anycast داریم.
- Unicast : ازیک کامپیوتر به یک کامپیوتر مشخص.
- Multicast : ازیک کامپیوتر به چند کامپیوتر مشخص.(ویدئو کنفرانس)
- Broadcast: ازیک کامپیوتر به چند کامپیوترنا مشخص.

FarshidAlabnoush

- Anycast : همانند Broadcast با این تفاوت که در Broadcast هر کامپیوتری باید جواب بدهد که این بسته برای آن هست یا نه,ولی درAnycastفقط کامپیوتری که بسته برای آن هست پاسخ می دهد.
- Anycast را در حال حاضر فقط بر روی روترها تنظیم می کنند.

Unicast به 4 دسته تقسیم می شود

1- Global Unicast: معادل Ip های Public در ورژن4 می باشند(برای رفتن بر روی اینترنت با Ip v6 باشد Global Unicast تنظیم کنیم)

فرم کلی Global Unicast

| FP | TLA-ID | RES | NLA-ID | SLA-ID | INTERFACE-ID |
|---|---|---|---|---|---|

FP3بیت , TLA-ID13 بیت,RES 8 بیت,NLA-ID 16 بیت, SLA-ID24بیت,INTERFACE-ID 64بیت

FP: نشان دهنده نوع Ip ورژن 6 می باشد (Format Prefix )Ip های Public ورژن6 در حالت باینری با 001 شروع می شوند.

TLA-ID (TopLevel Aggregator Identifire ) :دسته بندی Ip هایی هستند که به جاهای بزرگ مانند قاره ها اختصاص پیدا می کنند.

RESیعنی رزرو شده است.

NLA-ID ( Next Aggregator Identifire) : Ipهای منحصر به فردی هستند که به جاهای بزرگ مانند کشورها اختصاص پیدا می کنند.

SLA-ID (Site Level ): Ipهای منحصر به فردیهستند که به جاهای بزرگ مانند شهرها و سازمانهای بزرگ اختصاص پیدا می کنند(ایران خودرو).

Interface : Ipهای منحصر به فردی هستند که به هر NOD که بر روی اینترنت هستند اختصاص پیدا می کنند.

FarshidAjabnoush

استاندارد EUI64 :

همانطور که میدانیم MAC هر کارت شبکه منحصر به فرد می باشد وطول آن 48بیت می باشد.

00-50-8d-12-34-56

اعداد بالا را یک MAC در نظر بگیرید,3قسمت اول هر MAC (00-50-8d )نشان دهنده Company Id و3قسمت آخر آن (12-34-56 ) نشان دهنده Board Id می باشد.

همانطور که گفتیم MAC 48بیت می باشد,طبق استاندارد EUI64 , باید 64 بیت داشته باشیم برای همین باید بین Company Id وBoard Id عدد ثابت FFFE را اضافه کنیم 00-50-8d-FFFE-12-34-56

و 2عدد اول(00 ) را به صورت باینری بنویس 00=00000000واگر عدد هفتم صفر بود یعنی توسط IEEE رزرو می باشد,و ما باید آن را به1 تغییر دهیم, ولی اگر واگر عدد هفتم یک بود یعنی آدرس Local می باشد و توسط آن نمی توانیم به روی اینترنت برویم و باید تبدیل به 0 شود تا بتوانیم به اینترنت برویم.

بعد از اتمام این مراحل این اعداد باید بر روی Interface Id تنظیم شود.

SteLocalUnicast

معادل آدرسهای Private در ورژن4 هستند و فقط بدرد استفاده داخل شبکه می خورند,Ip های ورژن6 که با FEC0 شروع شوند Private هستند.

LinkLocalUnicast

معادل آدرس های APIPA در ورژن4 هستند,APIPA در ورژن6 با FE80 شروع می شود.

- زمانی که کلاینتی نتواند از Ip, DHCP بگیرد از ویندوز Ip را می گیرد که در رنج 169.254.0.0 است, به این APIPA گویند.

Special Unicast

در ورژن4 دونوع Special داریم,127.0.0.1 (خودم) 0.0.0.0 (همه),معادل 127.0.0.1 در ورژن6 1:: و معادل 0.0.0.0 در ورژن6 :: می باشد.

FarshidAjabnoush

MultiCast

در ورژن4 Ip های MultiCast با224.0.0.0 و در ورژن6 با FF شروع می شوند.

AnyCast

اگر بر روی رتور ip ورژن 6 تنظیم شده باشد که Host Id آنها همه صفر باشد,هر پکت AnyCast از سمت آن شبکه را از خود دیگر عبور نخواهد داد.

- رتورها BroadCast را ازخود عبور نمی دهند(داخل همان شبکه می ماند)

در حال حاضر اینترنت بر روی ورژن4 است,اگر بخواهیم شبکه ای با ورژن6 را به اینترنت متصل کنیم باید از یکی از روش های زیر اقدام کنیم

DualStack

در این روش باید هم ورژن4 و هم ورژن6 بر روی کامپیوتر داشته باشیم در هر زمان که خواستیم از آنها استفاده کنیم.(روش مناسبی نیست)

Tunneling

به این ترتیب است که در اینترنت تونلی می زنند از یک سر تونل ورژن6 را می ریزند واز سر دیگر آن,6 را بر می دارند.( VPN یکی از پروتکل هایTunnelingمی باشد)

6 To 4

هر پکتی که از شبکه می گذرد بر روی آن (بسته بندی)Encapsulation اتفاق می افتد,این روش می گوید پکت هایی که ورژن6 هستند را با ورژن4 بسته بندی کن.

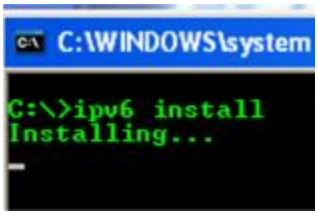
Mapping

از روی ورژن4, ورژن6 را بدست می آورند ( و بر عکس)

FarshidAjabnoush

نصب Ip ورژن6 بر روی XP

وارد CMD می شویم و دستور ipv6 install را وارد می کنیم , بقیه مراحل هم مانند شکل انجام می دهیم.




```
C:\>netsh
netsh>int ipv6
netsh interface ipv6>show int
Querying active state...

Idx  Met   MTU    State         Name
---  ----  -----  ------------  -----
  5    2   1280  Disconnected  Teredo Tunneling Pseudo-Interface
  4    0   1500  Connected     b
  3    1   1280  Connected     6to4 Pseudo-Interface
  2    1   1280  Connected     Automatic Tunneling Pseudo-Interface
  1    0   1500  Connected     Loopback Pseudo-Interface

netsh interface ipv6>set add "b" 2001::1
Ok.

netsh interface ipv6>
```

Farhad Gabnoush

DHCP (DynamicHostConfigurationProtocol)

وظیفه DHCP دادن تنظیمات TCP/IP به صورت اتوماتیک به کلاینت ها می باشد برای این کار از پورت 67 و68 استفاده می کند,روی پورت 67 درخواست کلاینت برای DHCP ارسال می شود و روی پورت68 IP, DHCP را به کلاینت می دهد.

- کلاینتی که گزینه Obtain آن فعال باشد می تواند از Ip, DHCP بگیرد.

کامپیوتری که گزینهObtain آن فعال باشد طی 4 مرحله زیر از DHCP , Ip می گیرد.

- با دستور Dhcp "2" Set Add می توانیم Ip های کارت شبکه را برداشته وگزینه Obtainفعال می شود.

زمانی که گزینه Obtainفعال شود طی 4 مرحله Client از Ip, DHCP می گیرد.

1) زمانی که کلاینت بالا می آید ( Obtainفعال است) یک پکت به نام DHCP DISCOVERY از نوع BroadCast در شبکه ارسال می کند مبنی بر این که Obtain من فعال است آیا کسی هست که به من Ip بدهد؟
2) اولین سرور DHCP که پکت بالا را دریافت کند پکتی به نام DHCP OFFER از نوع UniCast به کلاینت می فرستد مبنی بر اینکه من DHCP شبکه هستم می خواهی Ip بدم؟
3) در این مرحله, کلاینت پکتی به نام DHCP REQUEST از نوع UniCast به سرور DHCP ارسال می کند مبنی بر اینکه متوجه شدم شما DHCP هستید, لطفاً به من Ip بدهید.
4) در این مرحله, Ip, DHCP را بر روی پکتی به نام DHCP ACK از نوع UniCast برای کلاینت ارسال می کند.

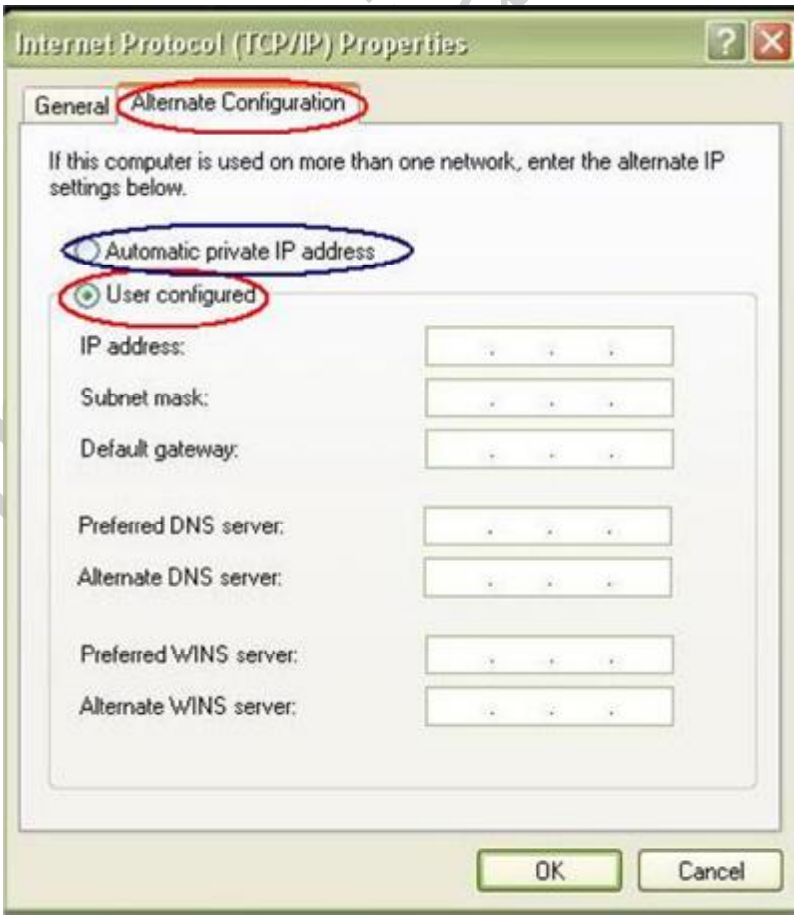
- به این 4 مرحله در اصطلاح DORA STAGEگویند.
- تمام مراحل DORA بر روی MAC انجام می شود.
- زمانی 2 کلاینت همزمان در خواستIp کنند (تا مرحله3 پیش روند) وDHCP فقط یک Ip داشته باشد, به کلاینتی که زودتر درخواست کرده باشد آن را می دهد و کلاینت دوم در مرحله4 پکت NAC (NO ACK ) دریافت می کند.
- سرورDHCPکه پکت NAC زیاد داشته باشد, سرور خوبی نیست.
- Ip که DHCP به کلاینت می دهد تاریخ مصرف داردیامدت اجاره (Lease Duration ) این مدت به صورت پیش فرض در ویندوز8 روز,لینوکس4 روز,سیسکو1 روز می باشد.

در اینجا فرض می کنیم از ویندوز استفاده می کنیم و به صورت پیش فرض 8 روز یک Ip را از DHCP می گیریم زمانی که به 50% زمان اجاره(4 روز) که به آن T1 گویند رسیدیم کلاینت به DHCP می گوید مدت زمان اجاره این Ip را تمدید کن و DHCP هم زمان آن را صفر کرده و از آن روز دوباره 8 روز دیگر Ip را به کلاینت اجاره می دهد, این در

FarshidAlabnoush

صورتی است که DHCP در شبکه باقی مانده باشد اگر DHCP در شبکه نباشد کلاینت هر 30 ثانیه به DHCP سر می زند که ببیند آمده یا نه اگر تا 87.5% زمان اجاره (روز 7) که به آن زمان T2 گویند DHCP آمده باشد ,IP تمدید می شود و اگر نیامده باشد روز 7, IP را که کلاینت دارد از دست می دهد و به جای آن 0.0.0.0 می گیرد و دوباره مراحل DORA تکرا می شود و اگر DHCP باشد Ip را می دهد و اگر نباشد همان کلاینت می شود Mini DHCP و Ip میدهد از رنج APIPA (169.254.0.0 تا 169.254.255.255 )هر Mini DHCP که می خواهد Ip را بردارد در شبکه Broad Cast می کند که من این Ip را برداشتم مال کس دیگری نیست؟ بعد آن Ip را تنظیم می کند (Ip, Mini DHCP را به صورت تصادفی انتخاب می کند)

- بزرگترین عیب APIPA بالا رفتن ترافیک شبکه است.(به دلیل BroadCast هر کلاینت)
- بزرگترین عیب دیگر APIPA این است که شبکه ای که APIPA داشته باشد اینترنت ندارد چون APIPA فقط Ip تنظیم می کند, Gateway ندارد.
- زمانی که DHCP نباشد و کلاینت هم نمی خواهد از APIPA , IP بگیرد باید ازقبل Ip و.. را برای آن تعیین کنیم برای این کار وارد کارت شبکه می شویم (Obtain باید فعال باشد) بر روی تب2 می رویم گزینه اول می گوید در صورت نبودن DHCP ازIp, APIPA بگیر وگزینه دوم می گوید در صورت نبودن DHCP تنظیمات زیر را اعمال کن.




Farzaneh Abroush

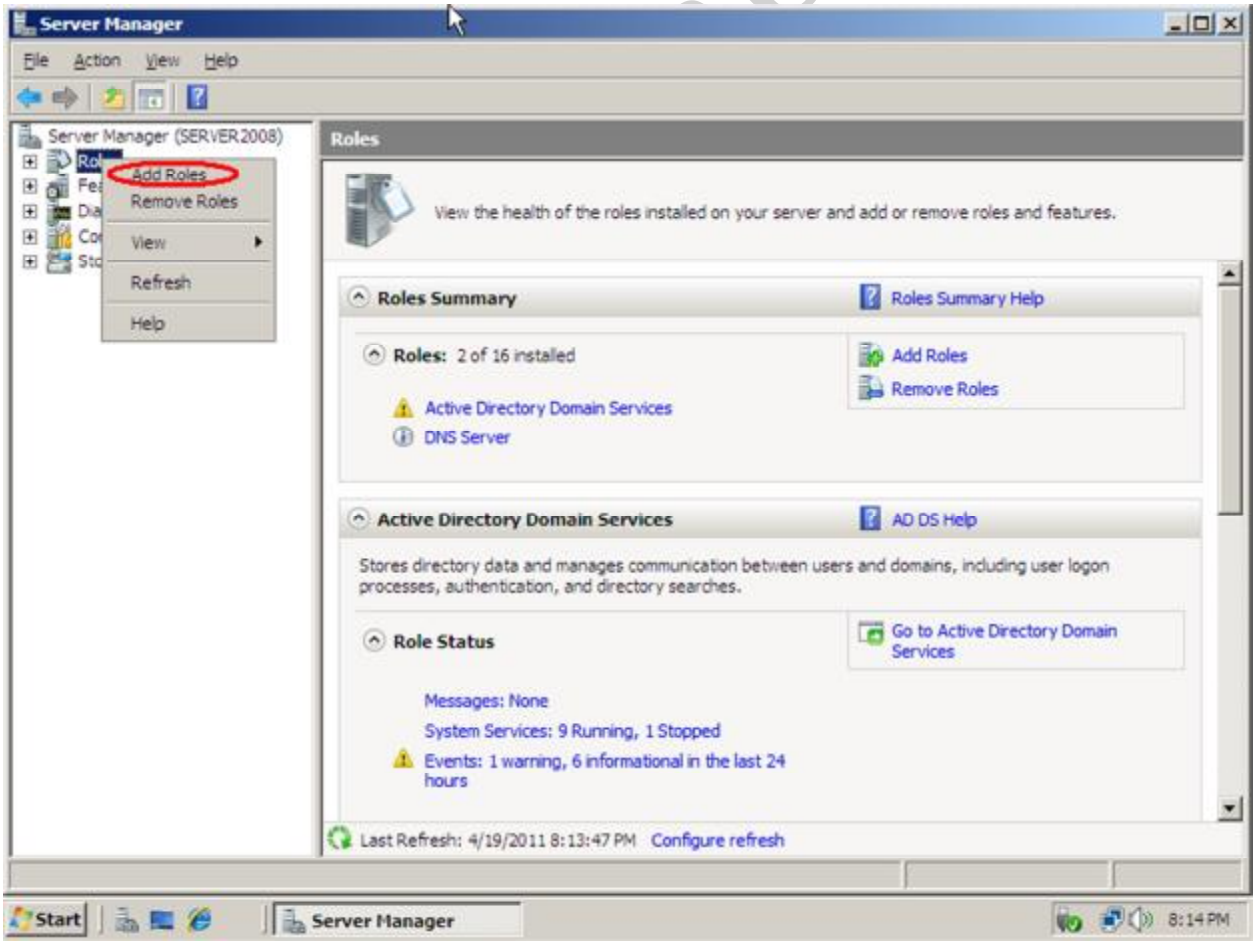
با انتخاب گزینه APIPA 2 غیر فعال می شود.

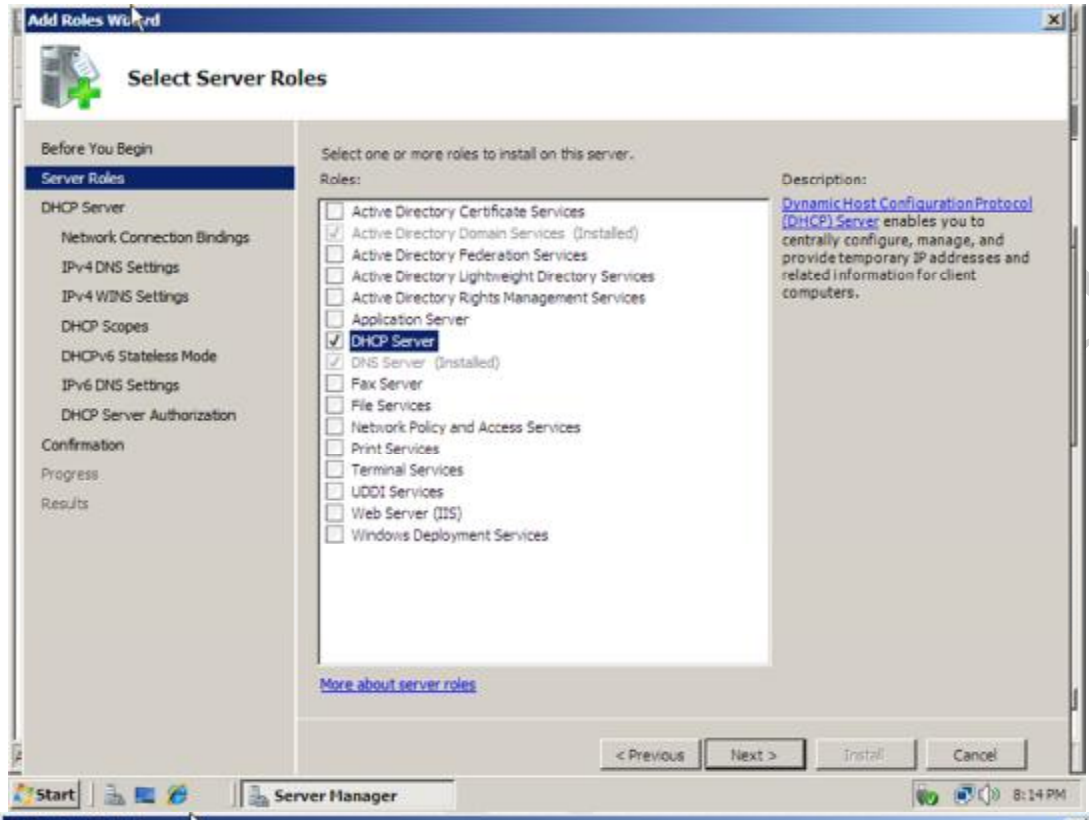
- ترمینال سرور یا همان App Server باید یک سرور جدا باشد, Exchange و IsaServer هم هر کدام باید یک سرورجداگانه باشند,اکتیو DHCP وDNS می توانند هر3 بر روی یک سرور باشند,SQL هم باید جدا باشد,در شبکه هایی که خدمات به مشتریانشان می دهند باید یک DNS سرور جداگانه برای مشتری ها بگذاریم(علاوه بر DNS که بر روی اکتیو است),Print Server را می توان بر روی تمامی این سرورها گذاشت, سرور آنتی ویروس باید حتماً مجزا باشد.
- اساس کار DHCP بر حسب Scope (Ip Pool ) می باشد.
- Ip Pool را یک ظرف پر از Ip در نظر بگیریداگر این ظرف در سرور مایکروسافت باشد Ip ها به ترتیب از 0 تا آخرین رنج می رود ولی اگر در لینوکس باشد از آخر به اول می آید.

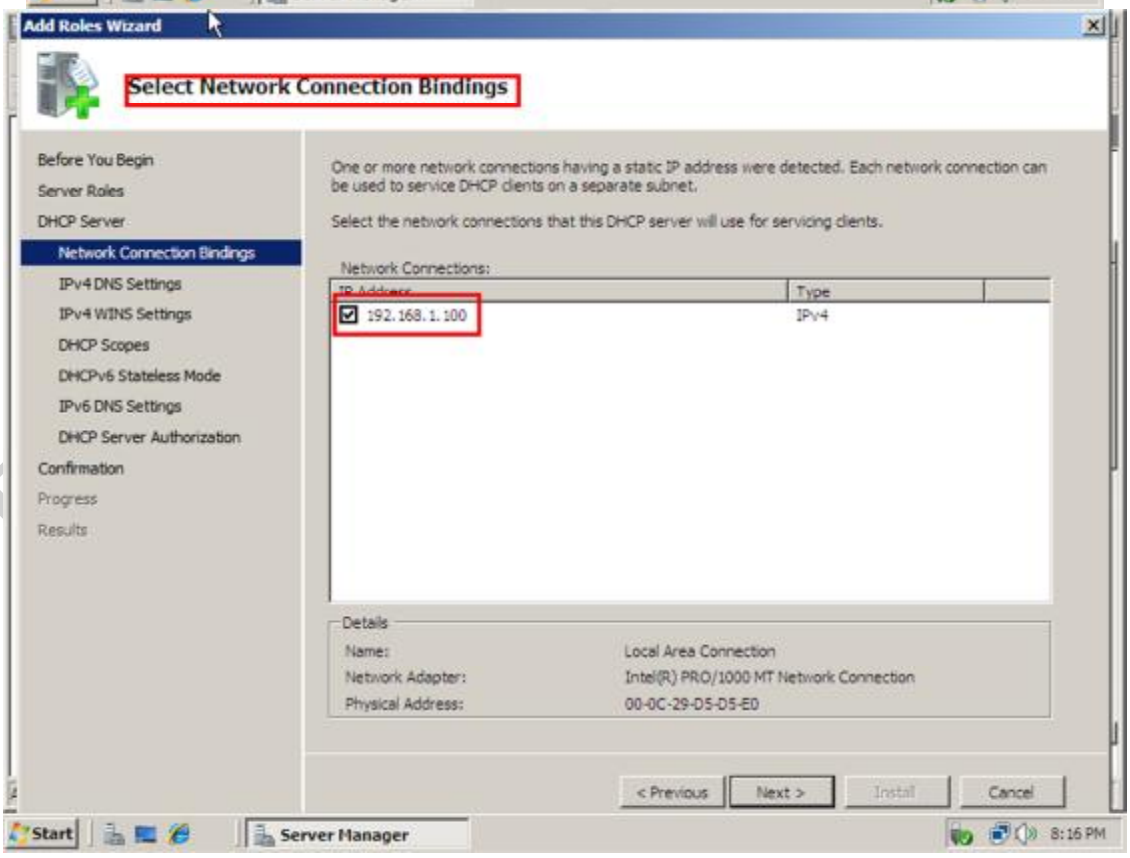
مایکروسافت: 192.168.1.1 .... 192.168.1.200 لینوکس: 192.168.1.200.... 192.168.1.1 .

- خود سرور DHCP نباید گزینه Obtain آن فعال باشد.

نصب DHCP 2008



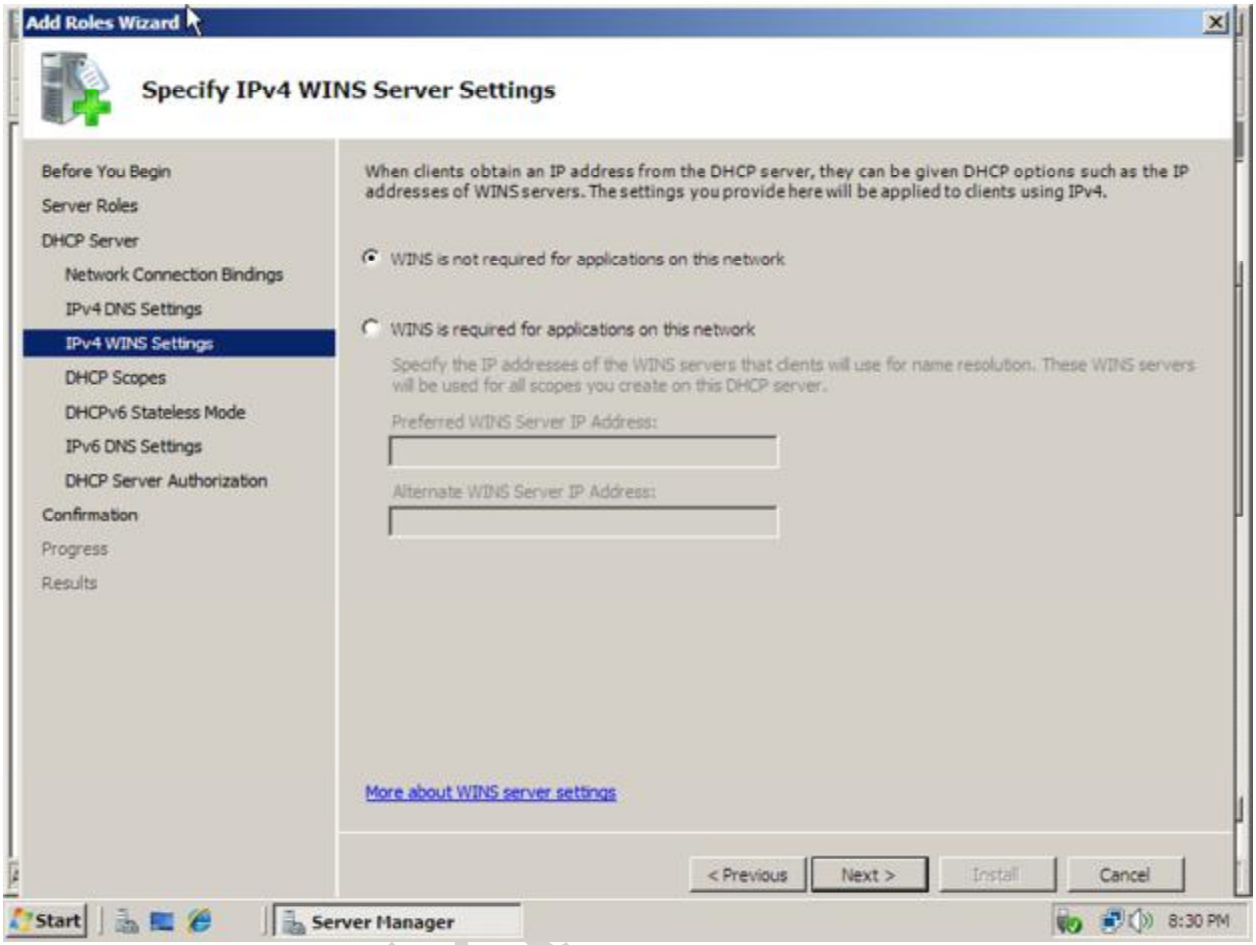

Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
DHCP Server
Network Connection Bindings
IPv4 DNS Settings
IPv4 WINS Settings
DHCP Scopes
DHCPv6 Stateless Mode
IPv6 DNS Settings
DHCP Server Authorization
Confirmation
Progress
Results
Select one or more roles to install on this server.
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 Services
Network Policy and Access Services
Print Services
Terminal Services
UDDI Services
Web Server (IIS)
Windows Deployment Services
Description:
Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.
More about server roles
< Previous
Next >
Install
Cancel
Start
Server Manager
8:14 PM


Add Roles Wizard
Select Network Connection Bindings
Before You Begin
Server Roles
DHCP Server
Network Connection Bindings
IPv4 DNS Settings
IPv4 WINS Settings
DHCP Scopes
DHCPv6 Stateless Mode
IPv6 DNS Settings
DHCP Server Authorization
Confirmation
Progress
Results
One or more network connections having a static IP address were detected. Each network connection can be used to service DHCP clients on a separate subnet.
Select the network connections that this DHCP server will use for servicing clients.
Network Connections:
IP Address
Type
192.168.1.100
IPv4
Details
Name:
Local Area Connection
Network Adapter:
Intel(R) PRO/1000 MT Network Connection
Physical Address:
00-0C-29-D5-D5-E0
< Previous
Next >
Install
Cancel
Start
Server Manager
8:16 PM

به کارت شبکه ای که به دادهای کلاینت ها گوش می کند و آنها را به سرور انتقال می دهد Binding گویند, در شکل3 Ip کارت شبکه Binding نوشته شده است ( تمامی Scop هایی که می سازیم باید در رنج کارت شبکه Binding باشد) در اینجا هرچندتا کارت شبکه داشتیم فقط باید یکی از آنها را انتخاب کنیم چون با انتخاب هر کدام CPU برای آنها سهم قائل می شود.

در مرحله بعدی اسم دامین و Ip را تشخیص می دهد.

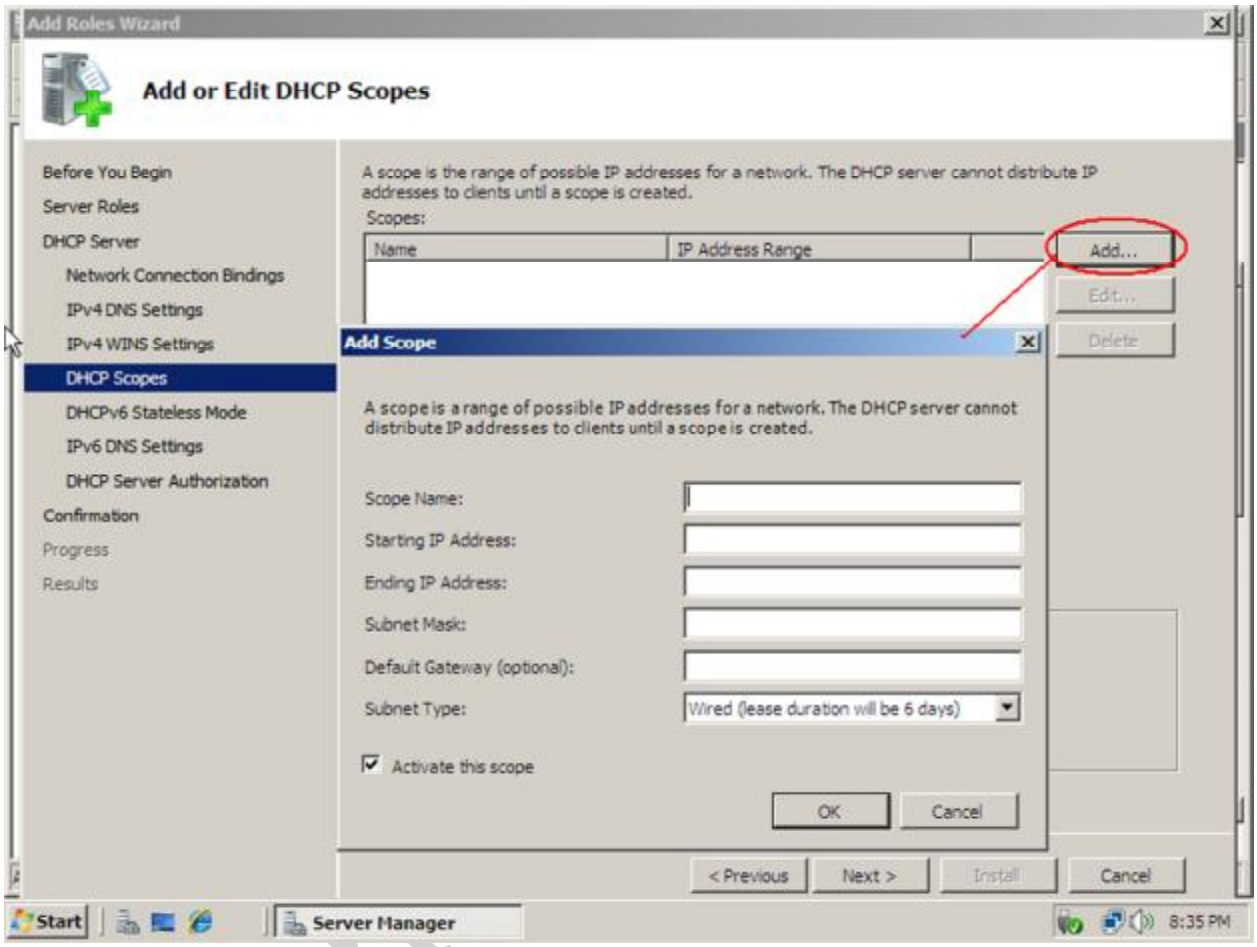
در مرحله بعد از ما  می پرسد که در این شبکه Wins استفاده می شود.




Wins هنوز در شبکه ها استفاده می شود,My Network Plase

Farshid

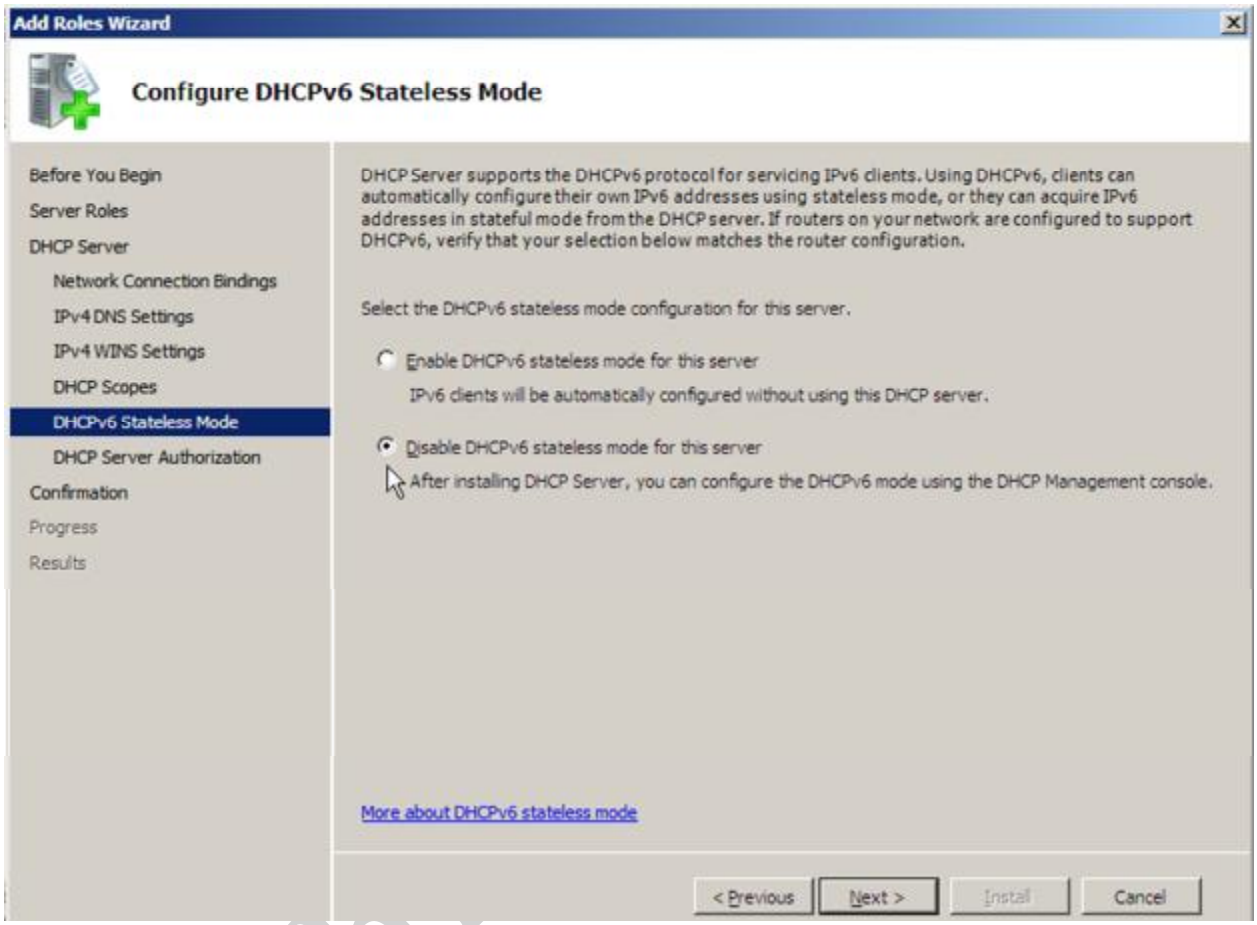
در اینجا می توانیم Scope تعریف کنیم بهتر است این کار را نکنیم چون در اینجا نمی توانیم DNS تعریف کنیم و همینطور نمی توانیم Ip خود سرور را رزرو کنیم.




به دلیل ضعیف بودن مباحث مدیریتی در اینجا Scope تعریف نمی کنیم.

Farsi

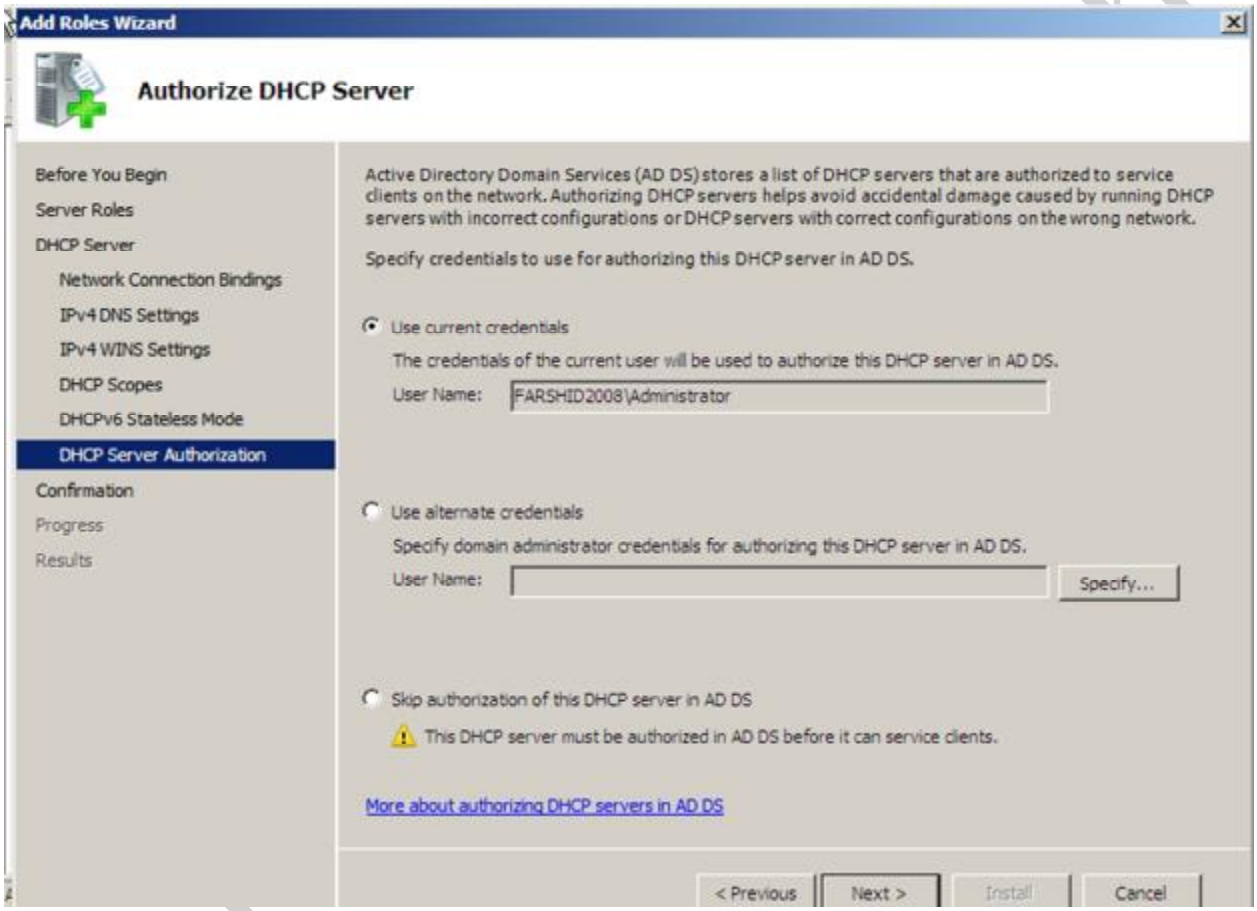
برای اینکه DHCP بتواند علاوه بر Ip 6, IP 4 هم به کلاینت ها بدهد باید گزینه2 را انتخاب کنیم(EUI64 )




Farsh

در مر حله بعد باید DHCP را Authorize کنیم ,اگر این کار را نکیم هکر خودش را به عنوان DHCP معرفی می کند و کلاینت ها نصف از هکر و نصف از سرور ما Ip می گیرند به این ترتیب اختلاف بین کلاینت ها بوجود می آید. اگر Admin نباشیم باید گزینه2 را انتخاب کنیم تا با یک یوزر و پسورد دیگر که باید Admin باشد این کار را انجام دهیم, گزینه بعدی می گوید نیازی به Authorize کردن نیست.

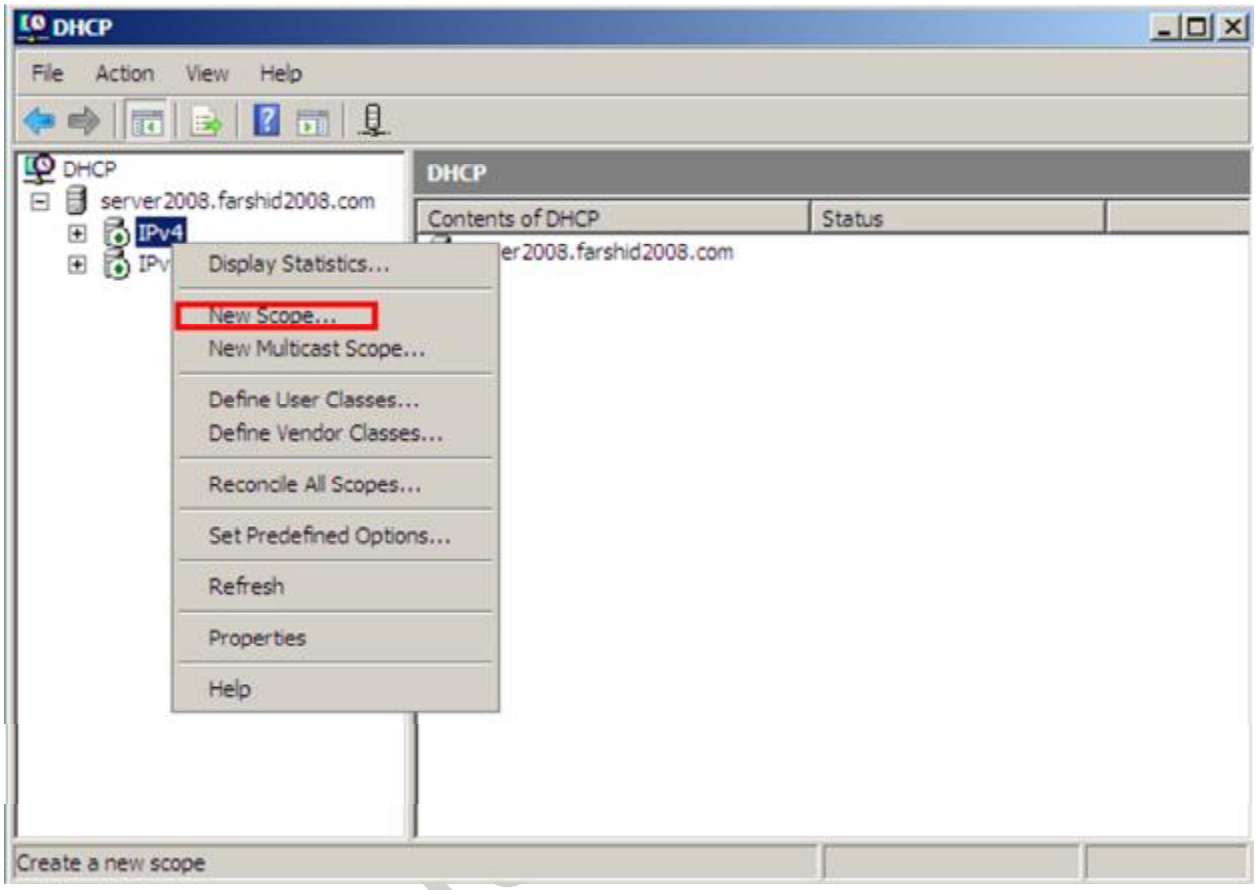
این مرحله فقط در شبکه های دامینی کار می کند.




Authorize از 2 طریق نرم افزاری وسخت افزاری امکان پذیر می باشد, راهکار نرم افزاری DHCP, Authorize داخل اکتیو می باشد و راهکار سخت افزاری DHCP Snooping می باشد که بر روی سوئیچ شبکه انجام می شود.

Rouge DHCP=DHCP تقلبی

بعداز نصب DHCP وارد کنسول آن می شویم,سپس باید Scope بسازیم, در اینجا هم Ip4 وهم Ip6 را داریم.



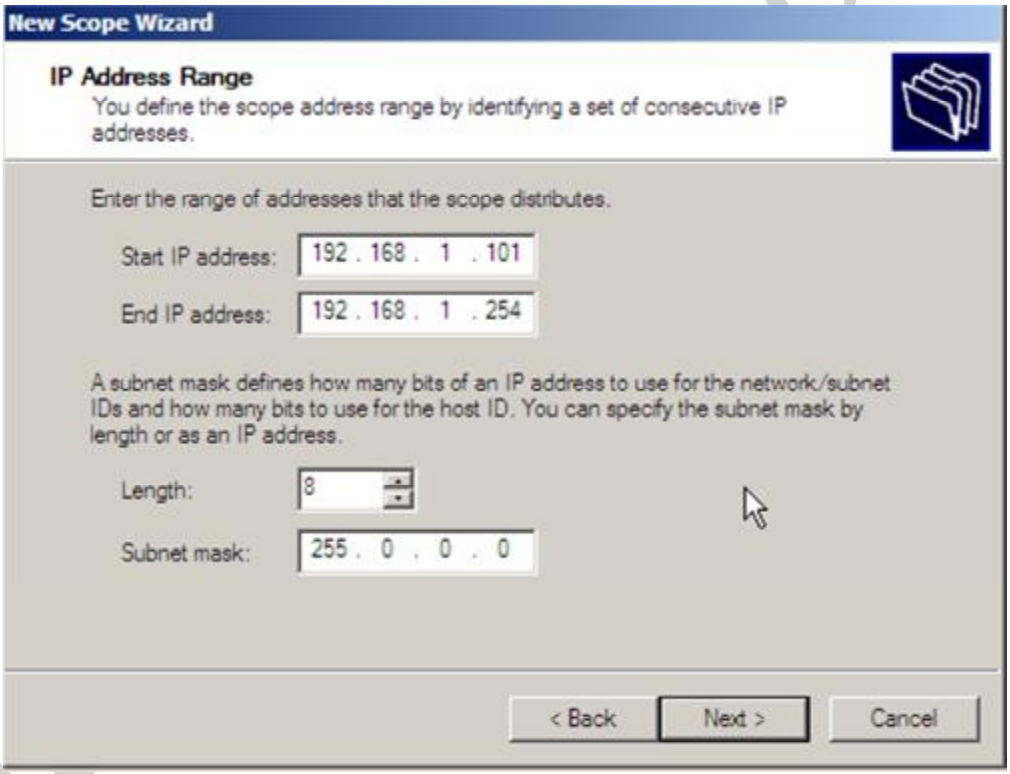

در مرحله بعد اسم اِسکوپ را وارد می کنیم.

- بعد از نصب DHCP اولین کار ساختن اِسکوپ می باشد.

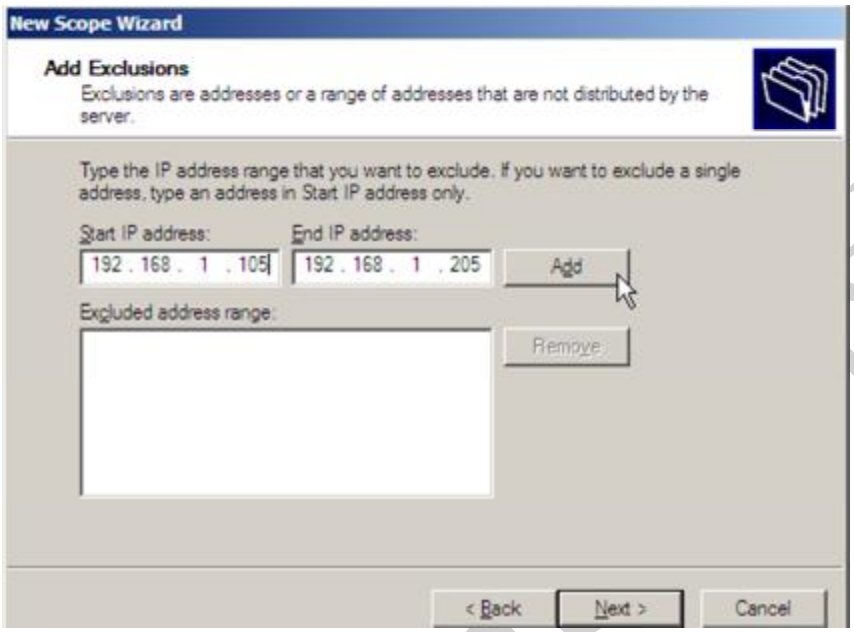
Farshid

در مرحله بعد باید داخل ظرف Ip ,Ip بریزیم, در اینجا باید Ip هایی را که وارد می کنیم در رنج Ip سرور باشد ( در اول نصب DHCP مشخص شد) خود Ip سرور نباید اینجا باشد یعنی در اینجا از 101 شروع می کنیم,در2003 Ip سرور هم بایداینجا باشد.

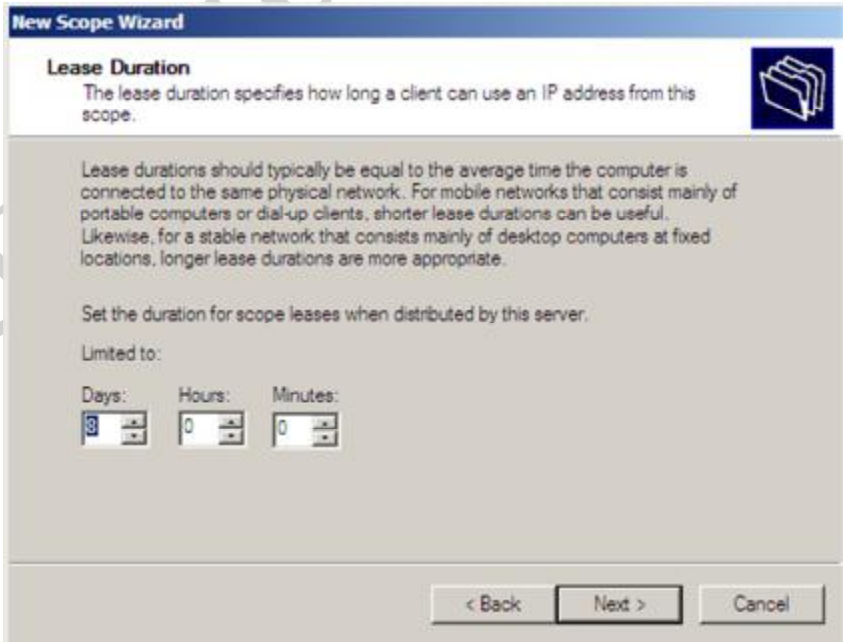
- تعداد Ip ها در این مرحله باید همیشه حداقل 20% بیشتر از تعداد کلاینت های موجود در شبکه باشد, به این دلیل که ممکن است در آینده کلاینت به شبکه اضافه شود.



در اینجا می توانیم Ip هایی را که می خواهیم رزرو کنیم,Ip های سرورها باید رزرو شوند,در2003 باید Ip خود سرور را هم در لیست رزرو ها بگذاریم.



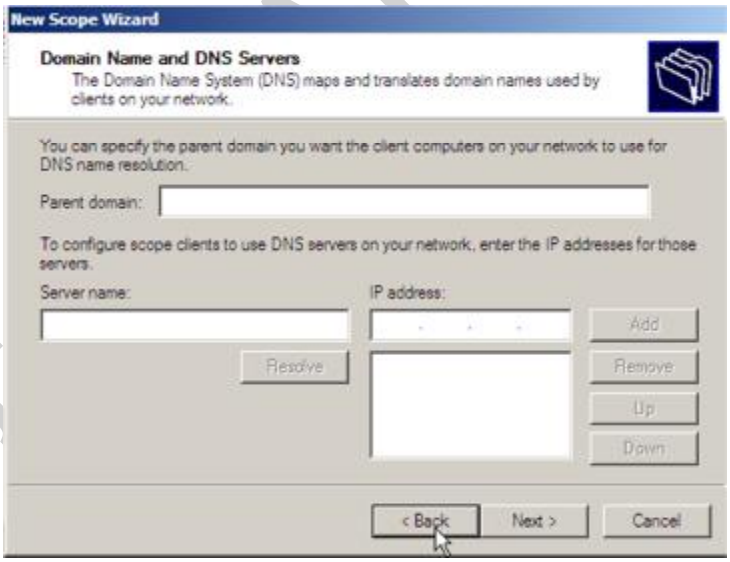

در اینجا می توانیم زمان اجاره را تغییر دهیم,بهتر است این کار را انجام ندهیم چون اگر این زمان را کم کنیم ترافیک شبکه زیاد می شود و اگر این زمان را زیاد کنیم امنیت شبکه پایین می آید.



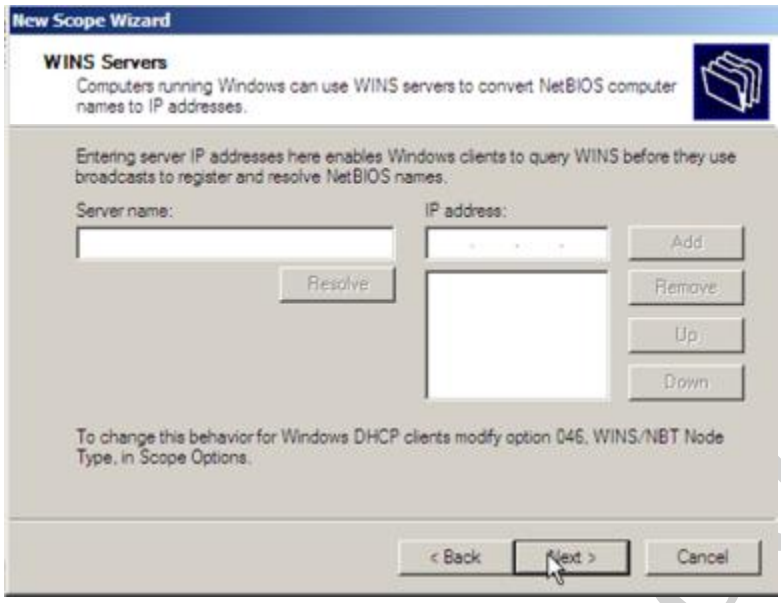

FarhadAjamesh

به تنظیمات اضافه تری که DHCP می تواند اعمال کند ( به غیر از Ip ) DHCP Option گویند مانند دادن Gateway DNS و... , درکنسول DHCP Option 3 نوع Option داریم Scope option-Server Option-Reservation Option

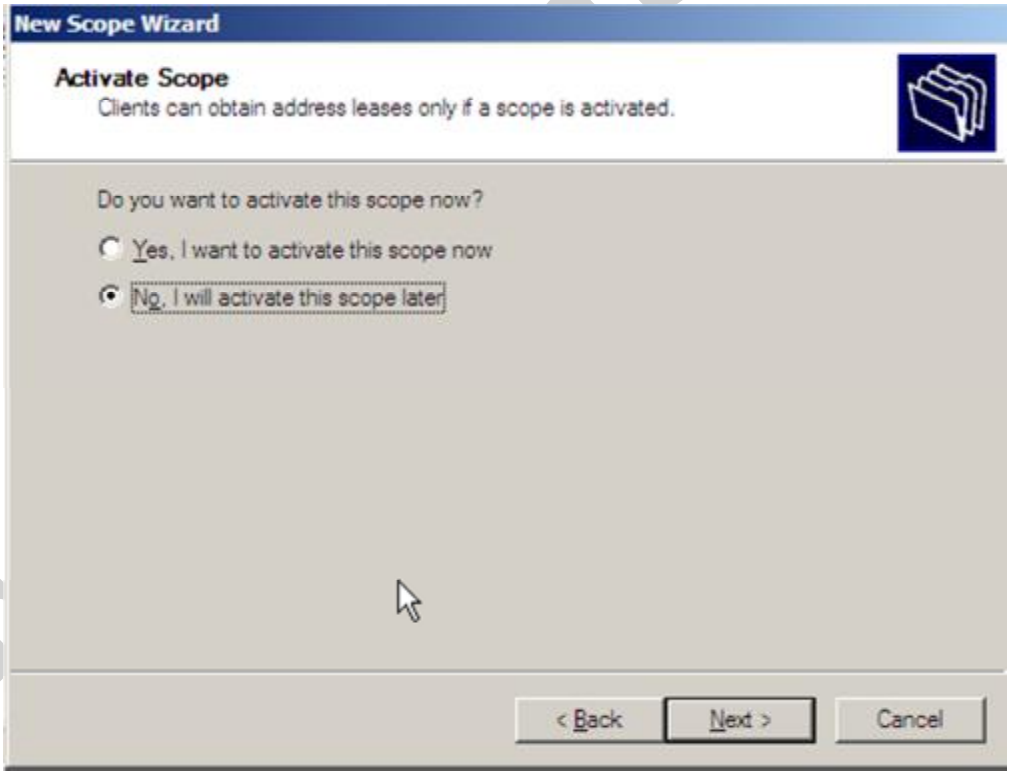
در مراحل بعدی می پرسد که می خواهی به ترتیب Gateway وDNS وWINS را هم اعمال کنم



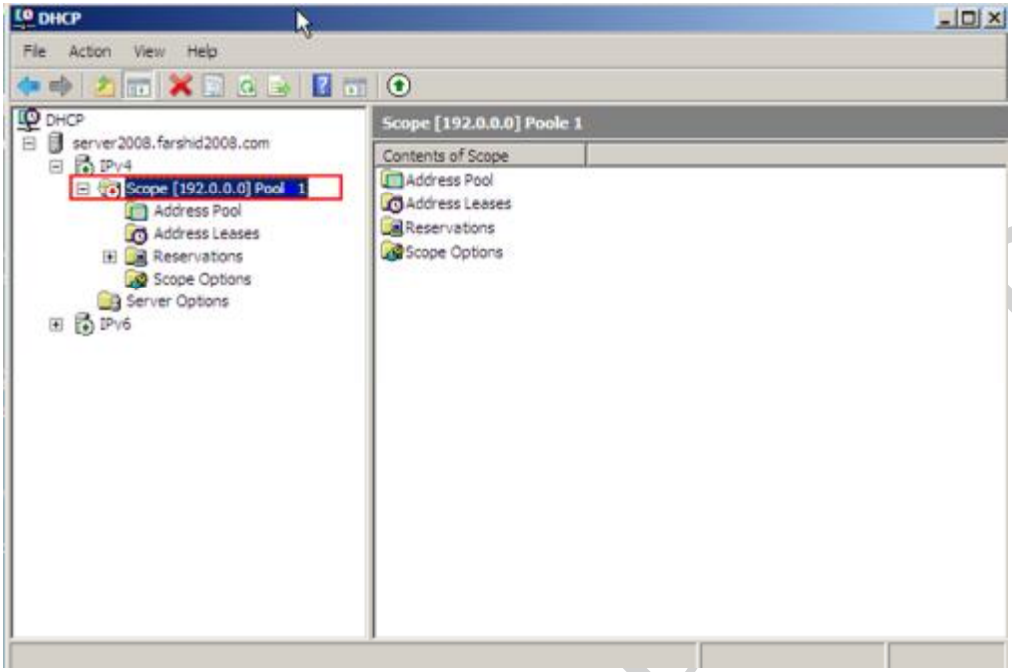

Far... ush




**در آخرین مرحله هم از ما می پرسد می خواهیدSCOPE را بعد از اتمام فعال کنم؟ که باید بله باشد ولی در اینجا گزینه 2 را می زنیم تا با پیغام بعدی مواجه شویم.**

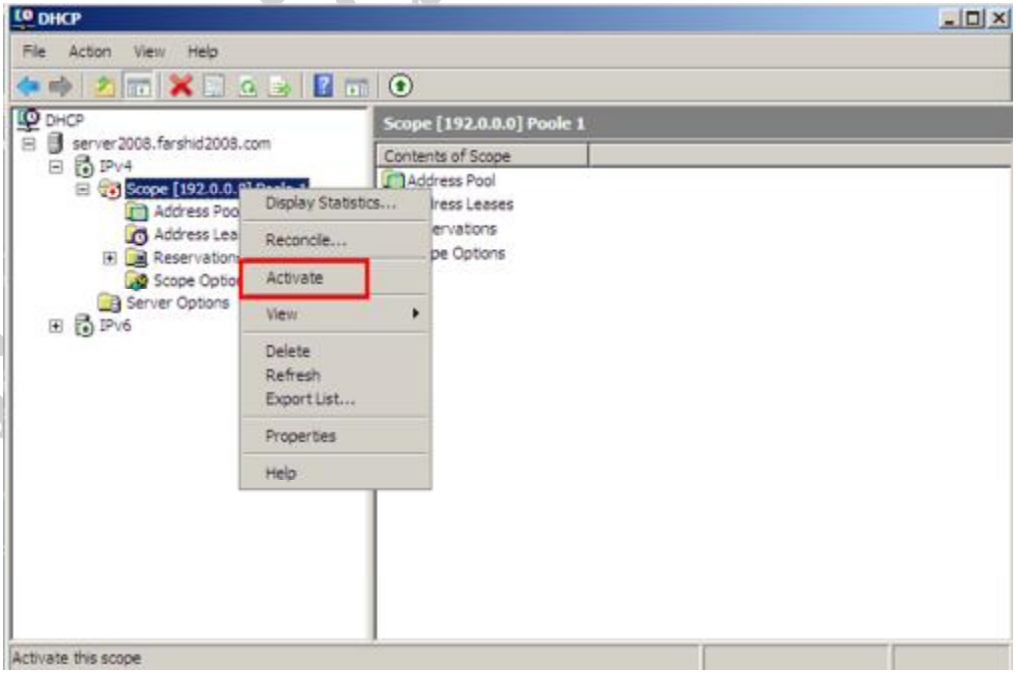


در اینجا می بینیم که Scope غیر فعال می باشد( فلش قرمز روبه پایینStop= )(فلش سبز روبه بالاStart= )

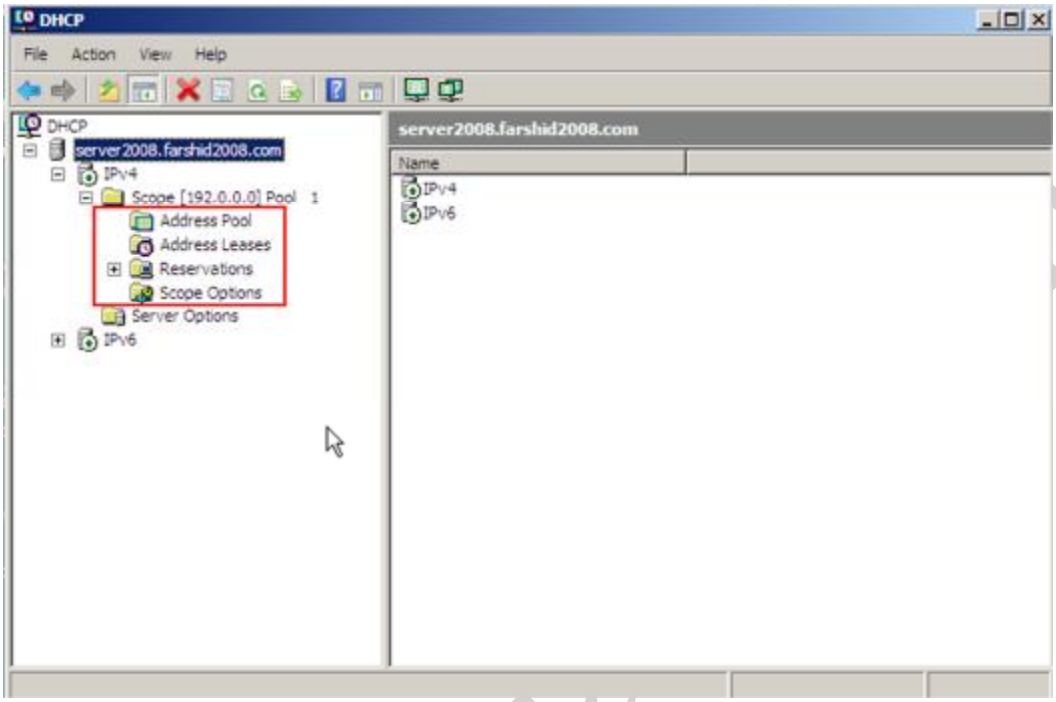



اگر روزی دیدیم که سرور ما Stop شده باید متوجه شویم که رنج ipظرف ما تمام شده است ( ظرف Ip )

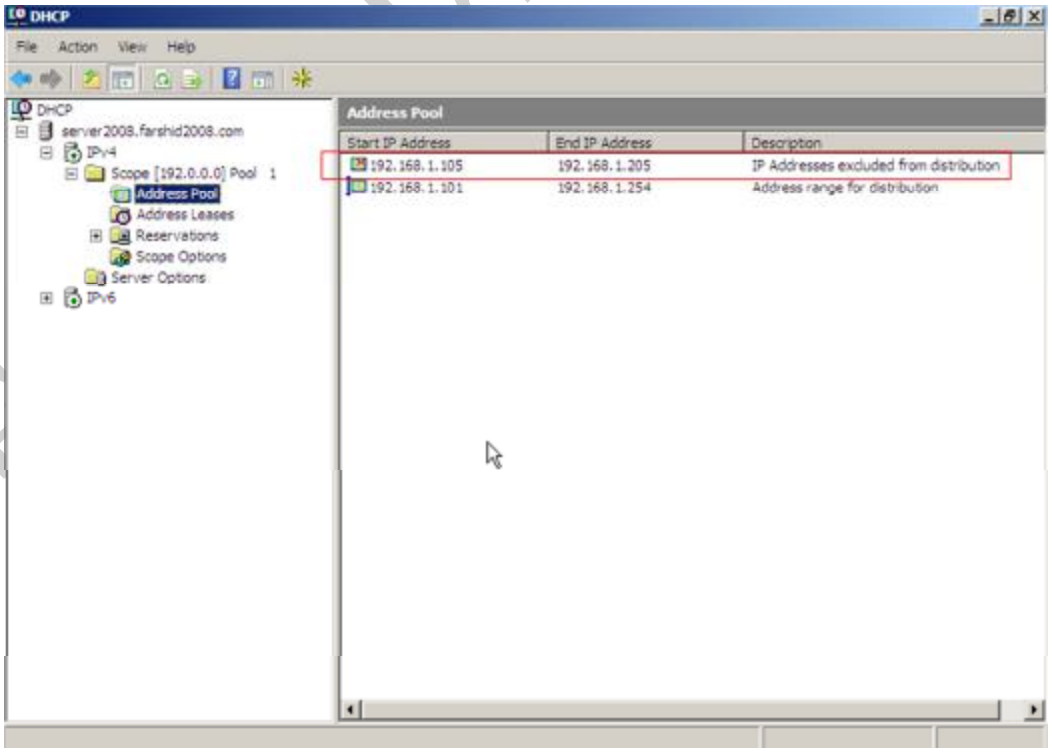
اگر Ip های ما در ظرف 20 بود باید بیاییم تعداد آنها را افزایش دهیم مثلاً50 , اگر Ip 254 بود باید یک Scope دیگر تعریف کنیم, سپس باید Scope را مانند زیر فعال کنیم



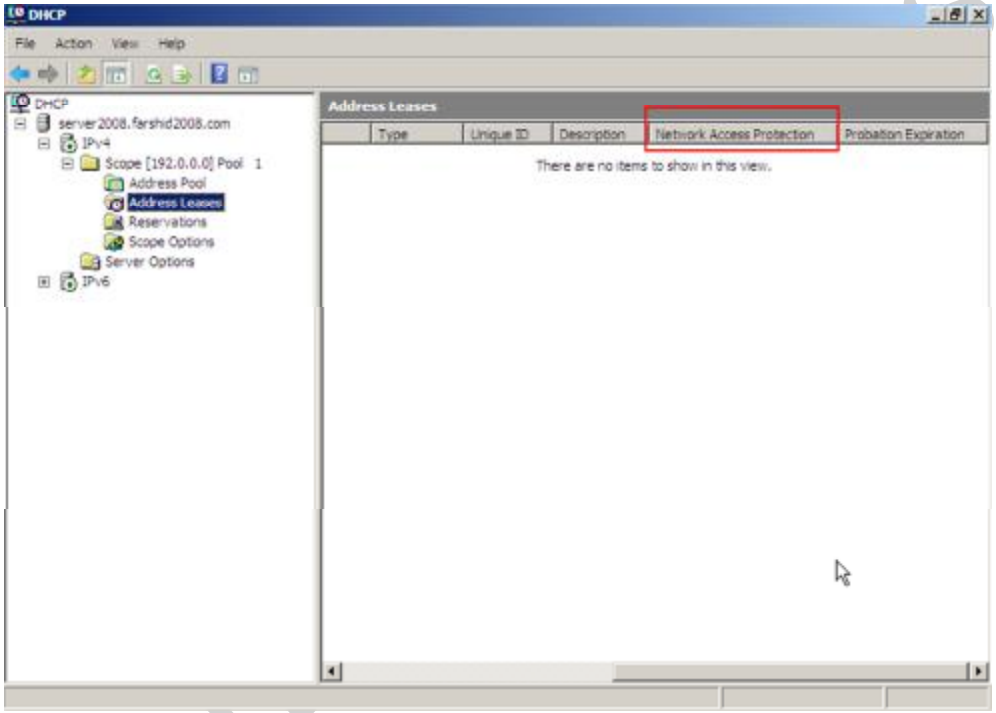
بعد از تعریف کردن Scope ( همان ظرف) باید زیر مجموعه های آن هم به این ترتیب باشند-Address Pool Address Leases-Reservations-Scope Options




در اولین پوشه محتویات ظرف را نشان می دهد, آن دسته از ip هایی که قرمز هستند رزرو شده اند

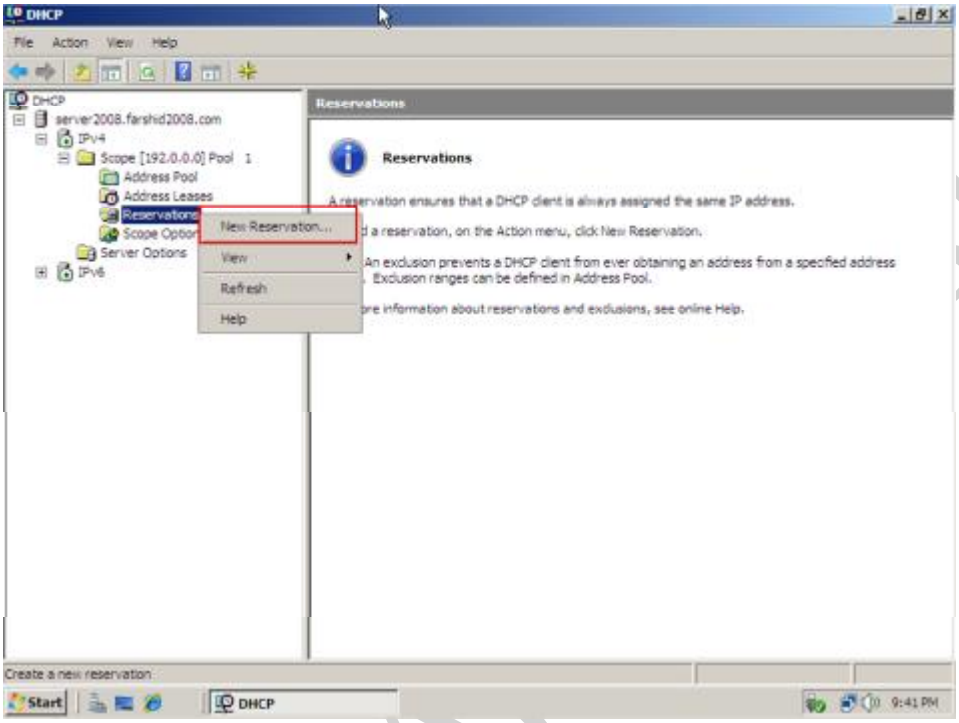


در دومین پوشه مشخصات  هر Ip و هر کلاینت را می نویسد,در زیر NAP را مشاهده می کنیم این سرویس سالم بودن هر کلاینت را چک می کند یعنی هر کلاینتی که می خواهد Ip بگیرد باید سالم باشد سالم بودن یعنی داشتن 4 شرط. 1- فایروال کلاینت روشن باشد2- آنتی ویروس داشته باشد و آپدیت باشد 3- آنتی Spyware داشته باشد+ آپدیت 4- ویندوزش آپدیت باشد.




Farsh

در این مرحله از Ip هایی که قبلاً رزرو کردیم باید برای سرورها استفاده کنیم



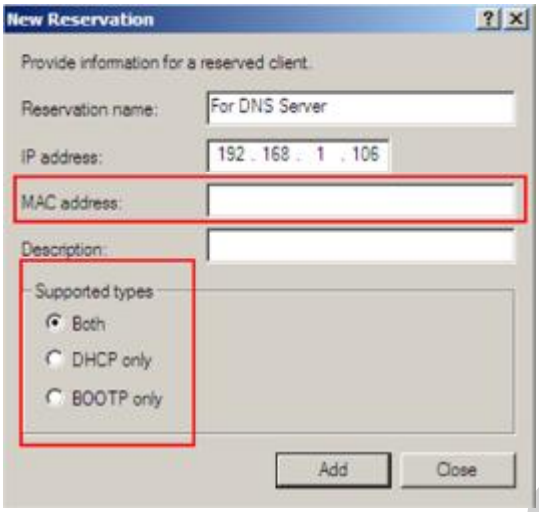

در اینجا اسم سرور را وارد می کنیم ip را هم که می خواهیم به آن اختصاص دهیم را می نویسیم و در قسمت MAC باید MACکامپیوتر مورد نظر را وارد کنیم تا DHCP بتواند آن را از روی MAC بشناسد و Ip مورد نظر را به آن بدهد.

در قسمت دوم از ما می پرسد چه پروتکلی را استفاده کنم بهتر است گزینه Both انتخاب کنیم

DHCP Only برای کامپیوتر هایی که داخل شبکه ما هستند استفاده می شود.

FarshidAsgari.ir

BOOTP Only برای کامپیوتر هایی که خارج از شبکه ما هستند استفاده می شود.

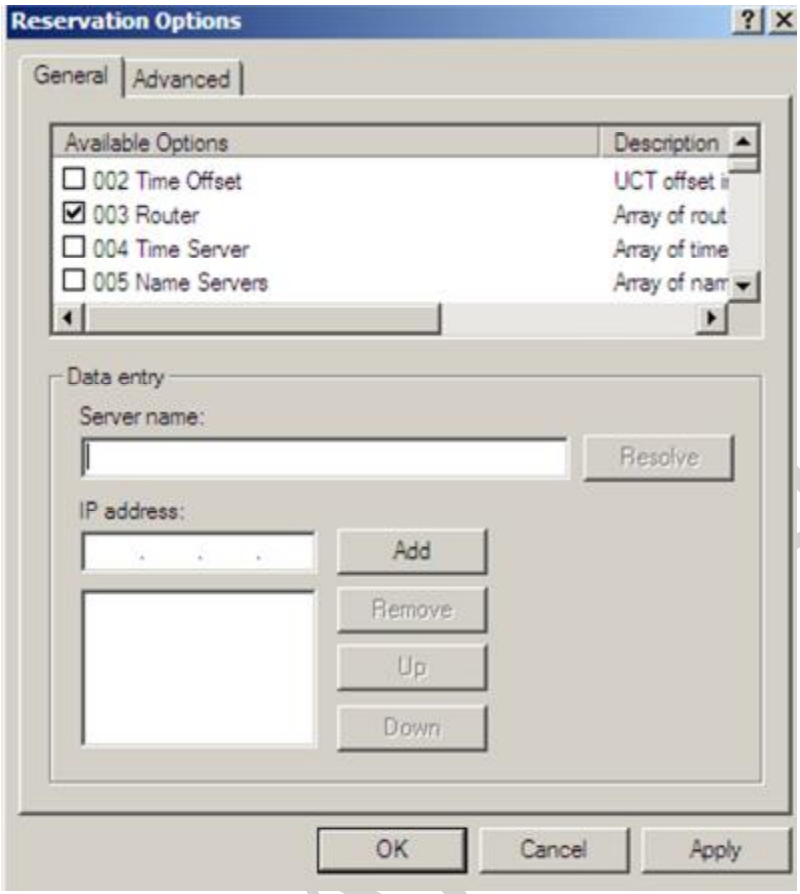



- برای بدست آورد MAC کامپیوتر ابتدا باید آن را از روی کامپیوتر خودمان Ping کنیم سپس با دستور Arp –a می توانیم MAC را ببنیم.

در Scope Option اگر تنظیمی انجام دهیم به همان Scope اعمال می شود,در Server Option تنظیمی انجام دهیم به تمامیScopeهای آن سرور اعمال می شود,Reservation Option در اینجا تنظیم اضافه تر به همان Reserve اعمال می شود.

در اینجا می خواهیم تغییراتی بر روی Reservation Option بوجود آوریم, بر روی Reservation Option کلیک راست می کنیم و گزینه Configure Options را انتخاب می کنیم سپس از صفحه باز شده ( شکل زیر) تغییرات مورد نظر را اعمال می کنیم.

FarshidAjabnoush




در اینجا Router همان Gateway است که باید در رنج Ip شبکه باشد, 015=DNS Domain Name دقیقاً مانند قسمت More می باشد, 042=NTP Server سروری است که کلاینت ها ساعتشان را با آن چک می کنند, 006=DNS

پیاده سازی DHCP در ServerCore

در ابتدا باید بر روی سرور Ip تنظیم کنیم بعد از این مرحله باید کنسول DHCP را با دستور زیر نصب کنیم

```
Start /w ocsetup DHCPServerCore
```

بعد از نصب باید با دستور زیر مشخص کنیم هر بار که سرور روشن شد DHCP اتوماتیک فعال شود

```
Sc config dhcpserver start= auto
```

بعد از اجرای این دستور حتماً باید سرور ریستارت شود در غیر این صورت با پیغام زیر مواجه می شویم.

```
Unable to determine the DHCP Server version for the Server 192.168.1.101.
Server may not function properly.
```

FarshidAsh

برای ساختن اِسکوپ مانند زیر عمل می کنیم

```
C:\>netsh
netsh>dhcp
netsh dhcp>server
netsh dhcp server>add scope 192.168.1.0 255.255.255.0 scope1 "test"

Command completed successfully.
```

مشخص کردن رنج Ip(ابتدا و انتهای Ip )

```
netsh dhcp server>scope 192.168.1.0 add iprange 192.168.1.1 192.168.1.254
```

مشخص کردن رنج Exclude

```
netsh dhcp server>scope 192.168.1.0 add excluderange 192.168.1.115 192.168.1.220
```

اگر یک Ip را بخواهیم Exclude کنیم باید 2 بار بنویسیم (192.168.1.115 192.168.1.115 بعداز Exclude می نویسیم )

تنظیم کردن Gateway که کد آن 003 است

```
netsh dhcp server>scope 192.168.1.0 set optionvalue 003 ipaddress 192.168.1.117
```

غیر فعال کردن Scope

```
netsh dhcp server>scope 192.168.1.0 set stat 0
```

فعال کردن Scope

```
netsh dhcp server>scope 192.168.1.0 set stat 1
```

دیدن دستورات مدیریت پایه ای

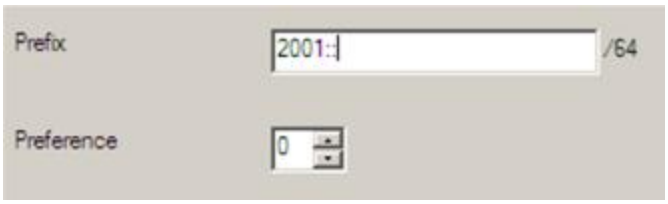
```
netsh dhcp server>show mibinfo

MIBCounts:
        Discovers = 0.
        Offers = 0.
        Requests = 0.
        Acks = 0.
        Naks = 0.
        Declines = 0.
        Releases = 0.
        ServerStartTime = Thursday, April 21, 2011 10:20:18 PM
        Scopes = 1.
        Subnet = 192.168.1.0.
                No. of Addresses in use = 0.
                No. of free Addresses = 148.
                No. of pending offers = 0.
```

PershidAjabnoush

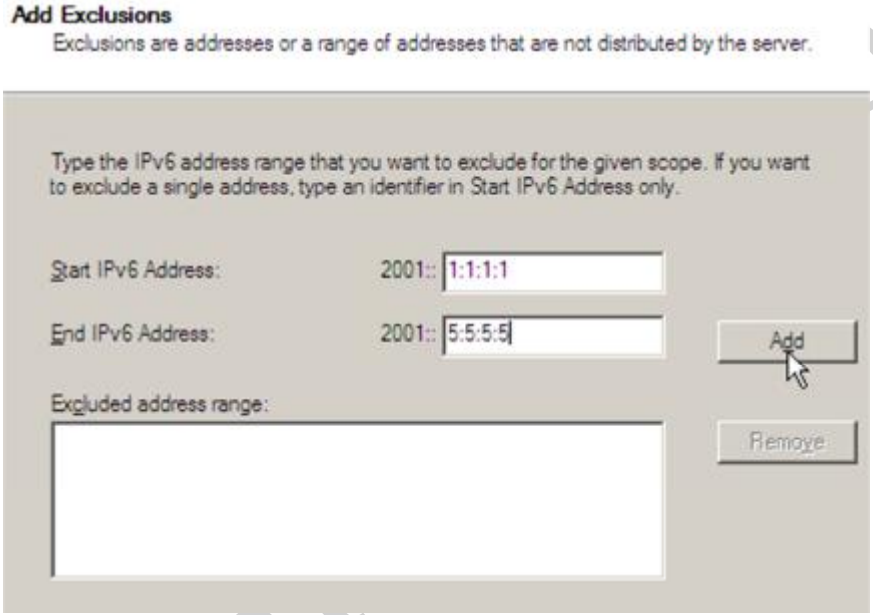
ساختن Scope v6 در DHCP

وارد کنسول DHCP می شویم بر روی Ip V6 کلیک راست می کنیم,عبارت New Scope سپس اسم اِسکوپ را می نویسیم در صفحه بعد باید Net Id را وارد کنیم(HostId را نمی نویسیم)::2001

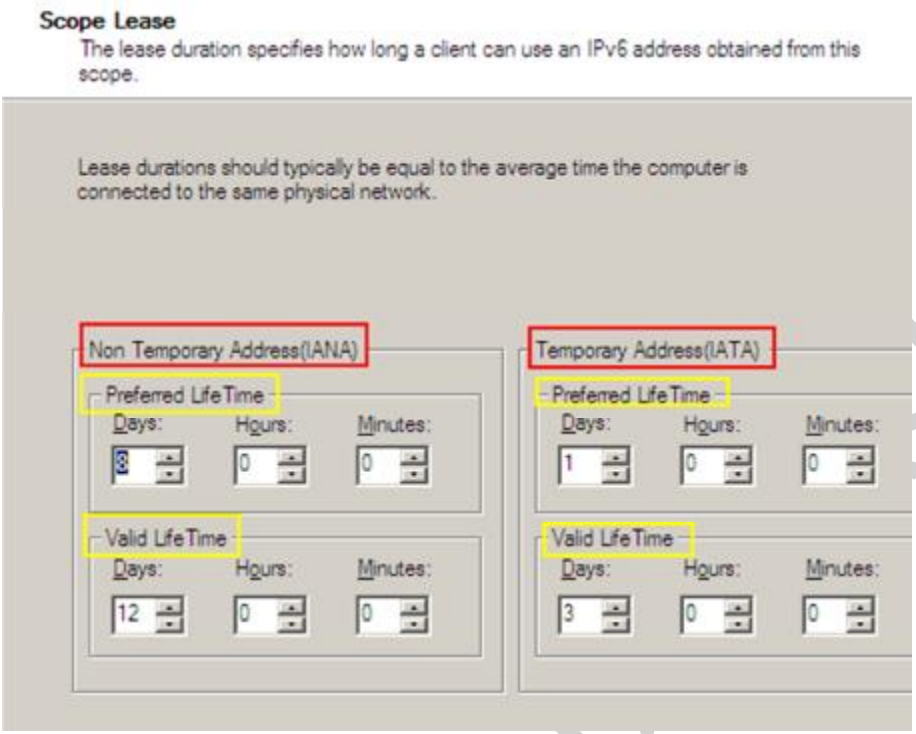
- در ورژن6 می توانیم چند Ip را بر روی یک کارت شبکه داشته باشیم(برای هرکدام باید اِسکوپ بسازیم) برای اولویت دادن به استفاده از آنها,در قسمت Preference عدد می دهیم ,اولویت با Scopeاست که عدد وارد شده اش در Preference بزرگتر باشد.



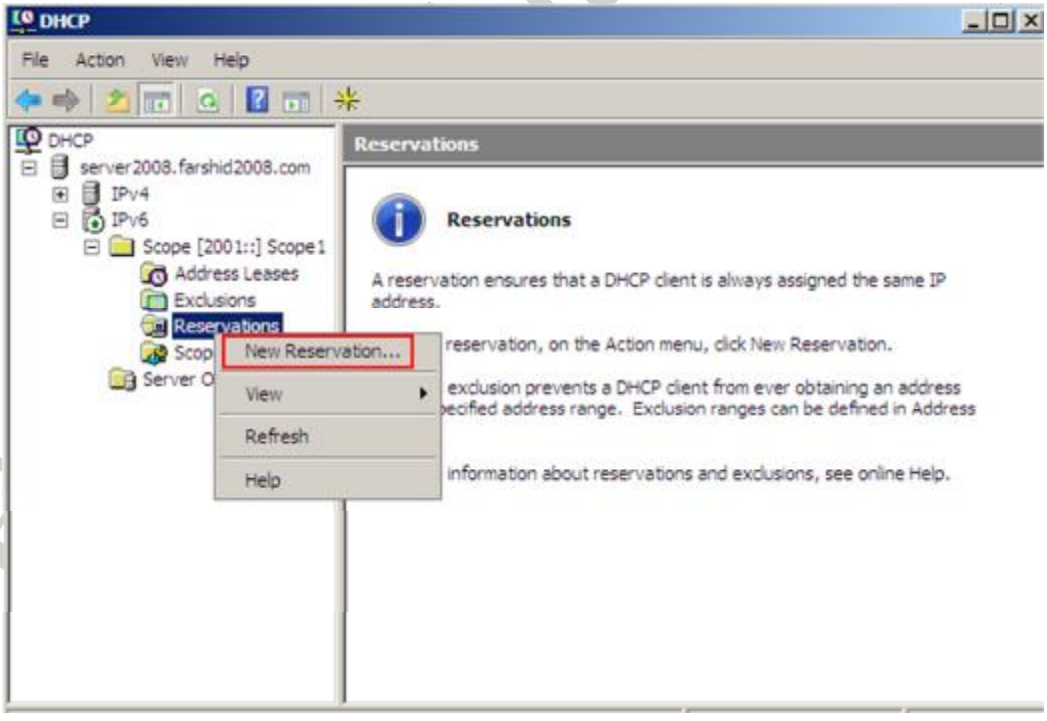

در اینجا می توانیم Exclude کنیم



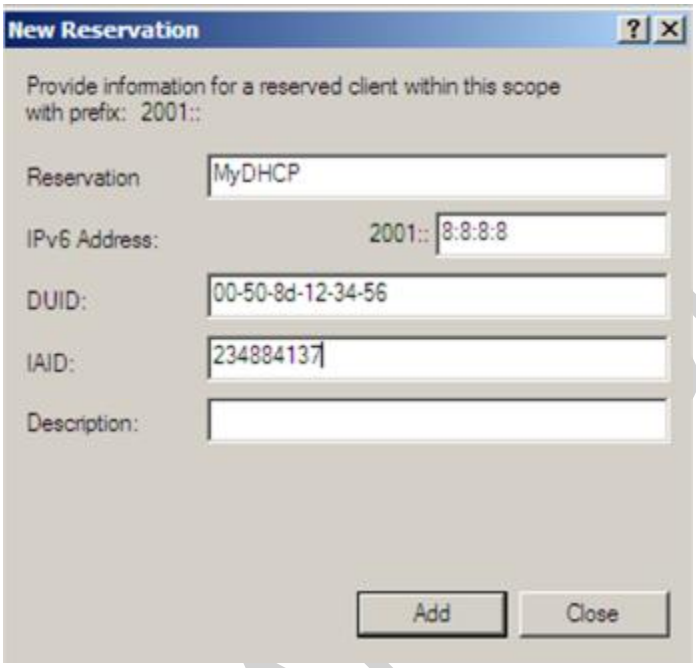

در مرحله بعد می توانیم مدت زمان اجاره را مشخص کنیم,که به2 بخش IANA برای PC و IATA برای قابل حمل ها( LapTop ) به کار می روند, حداقل زمان 8 روز و حداکثر12 روز می باشد.




**نحوه رزرو کردن در اِسکوپ6**

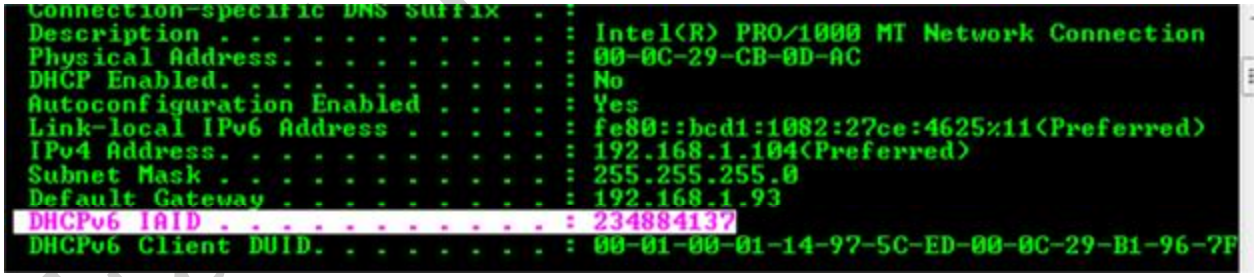


در صفحه باز شده اسم موردنظر را همراه با Ip خواسته شده وارد می کنیم در قسمت MAC, DUID سیتم مورد نظر را وارد می کنیم (Mydns ),IAID یک عدد9 رقمی موجود در ویندوزهای7 و ویستا می باشد که باید در اینجا وارد کنیم.




بدست آوردن IAID

ابتدا وارد ویندوز سیستم مورد نظر می شویم (7 یا ویستا باید باشد)سپس دستور Ipconfig /all را وارد می کنیم



تنظیمات Advance در DHCP

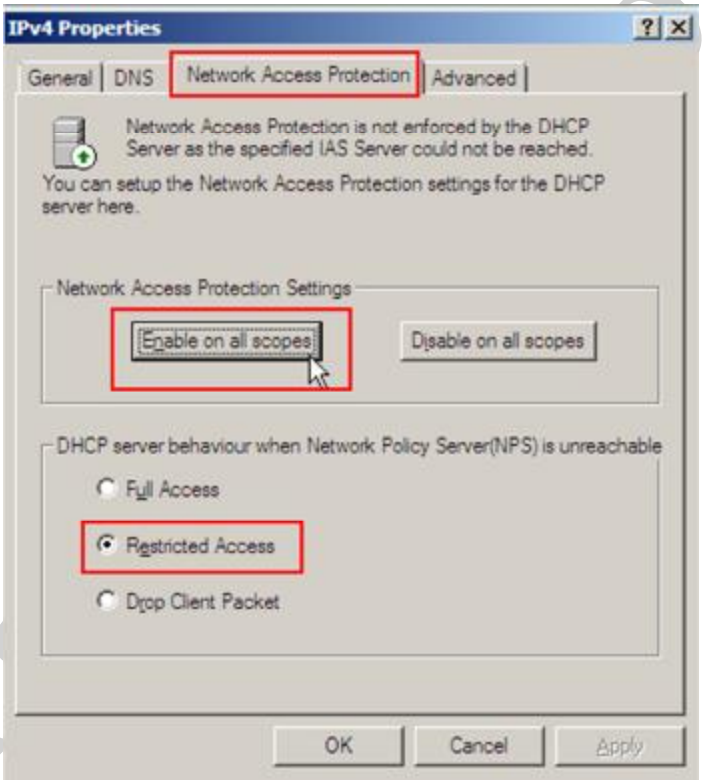
1) NAP (Network Access Protection)

کارش چک کردن سلامتی کلاینت ها است( شامل 4 مرحله می باشد که توضیح داده شده است)

- DHCP جزو آن دسته از سرورهایی است که NAP باید کلاینت مورد نظر را تایید کند تا بتواند به آن Ip دهد.
- بر روی VPN,DHCP,IPSEC,WIRELESS می توان از NAP استفاده کرد.

فعال سازی NAP

بر روی Ip v4 کلیک راست, پراپرتیز

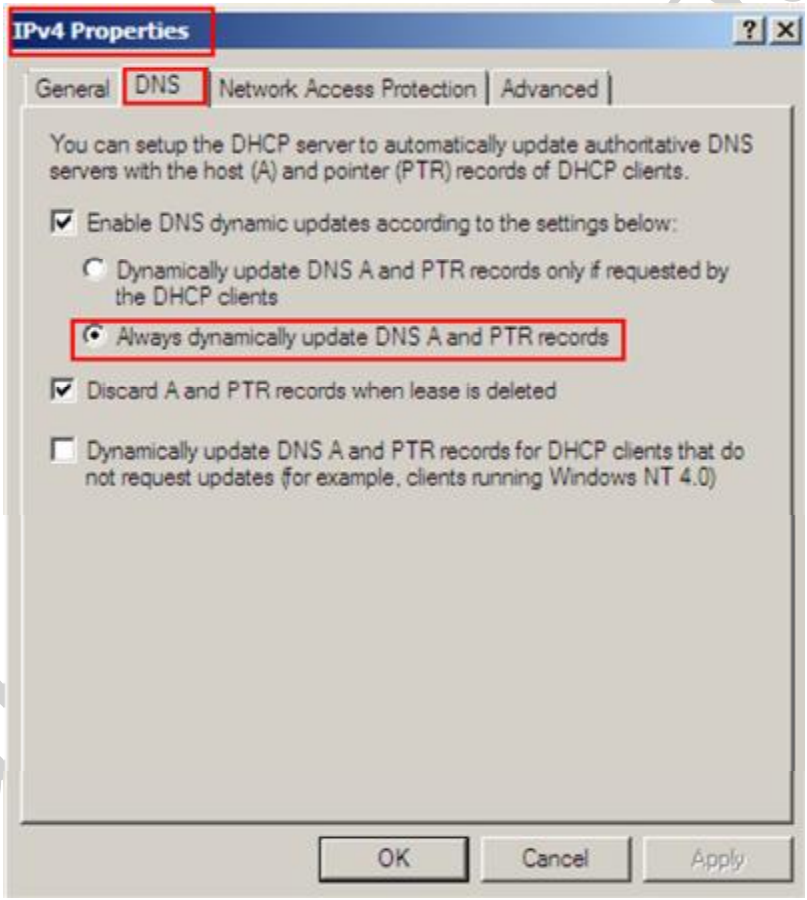



بعد از فعال سازی, در قسمت دوم می پرسد اگر سروری که سلامتی راچک می کند خراب بود و کسی از من Ip خواست چه کار کنم؟ گزینه2 را انتخاب می کنیم یعنی Ip بده ولی دسترسی آن را محدود کن.

- اگر بخواهیم NAP را بر روی یک اسکوپ فعال کنیم باید مراحل بالا را بر روی آن اسکوپ انجام دهیم.

2) DDNS (Dynamic DNS)

با یک مثال توضیح می دهیم,در اینجا ما یک DNS , DHCP و یک کلاینت و یک کاربر داریم, کلاینت اسم خودش را همراه با Ip192.168.6.200 در DNS ثبت کرده و کاربر هم با اسم کلاینت را Ping می کند حالاDHCP, Ip جدید 6.100 را به کلاینت داده است ولی در DNS اسم کلاینت با Ip قبلی ثبت شده است و الان کاربر با مشکل مواجه می شود اگر DDNS در DHCP فعال باشد هر بار که Ip تغییر کند به صورت اتوماتیک در DNS هم این تغییر را اعمال می کند.

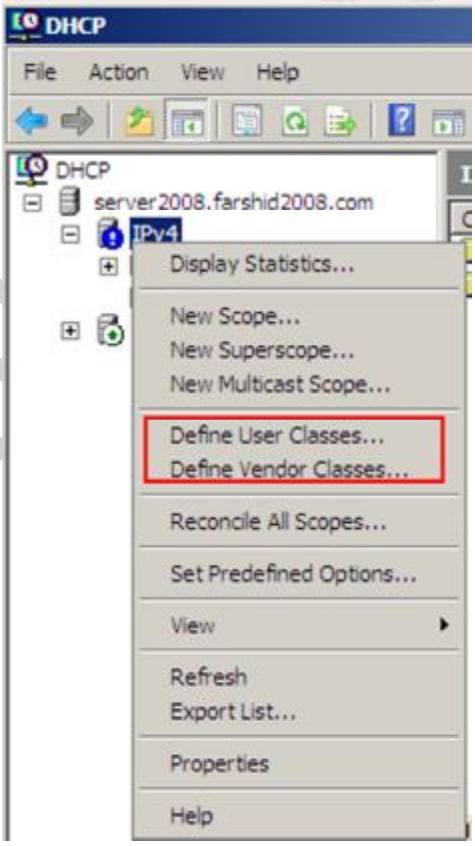



این ویژگی به صورت پیش فرض فعال می باشد.

3) مفهوم کلاسها در DHCP

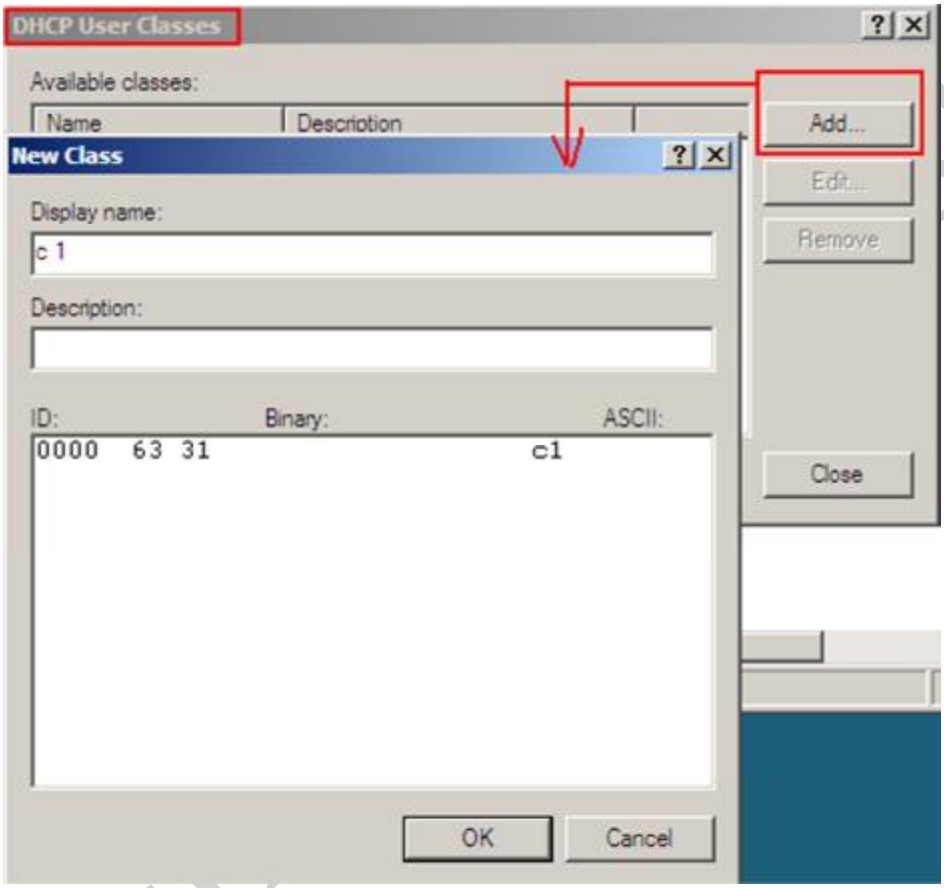
فرض کنیم 500 کلاینت داریم که می خواهیم به250 از آنها Gateway 6.100 بدهیم به 250 دیگر Gateway 6.200 بدهیم, 2 راه حل وجود دارد 1- به صورت دستی به تک تک آنها Gateway بدهیم 2- 2 کلاس بسازیم و کلاینت ها را عضو کلاسها کنیم و تغییرات را به کلاسها اعمال کنیم.

کلاسها به 2دسته User classes وVendor classesتقسیم می شوند در دسته اول می توانیم هر تغییری را اعمال کنیم دسته2 کلاینت ها را براساس سیستم عامل آنها تقسیم بندی می کند به طور مثال می توانیم تعریف کنیم که کلاینت هایی که 98 هستند Wins اعمال کن و به کلاینت هایی که 7 هستند DNS اعمال کن.



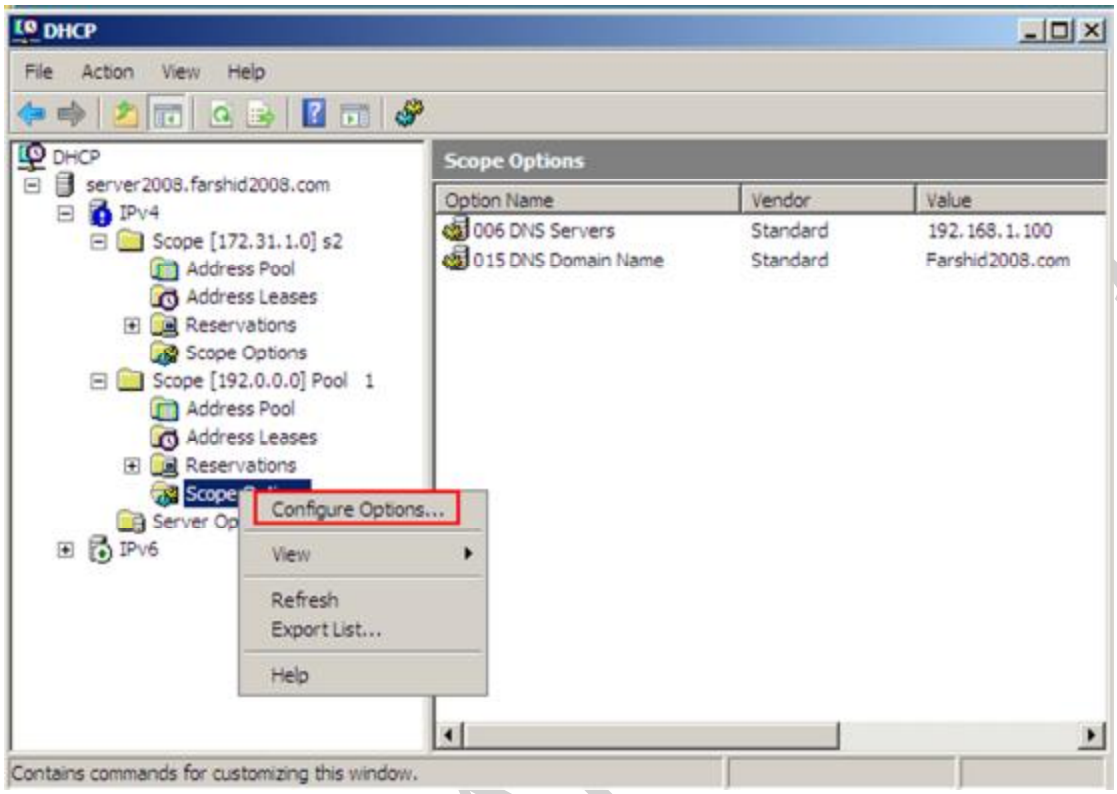

Farshidnoush

برای ساختن کلاس به صورت زیر عمل می کنیم

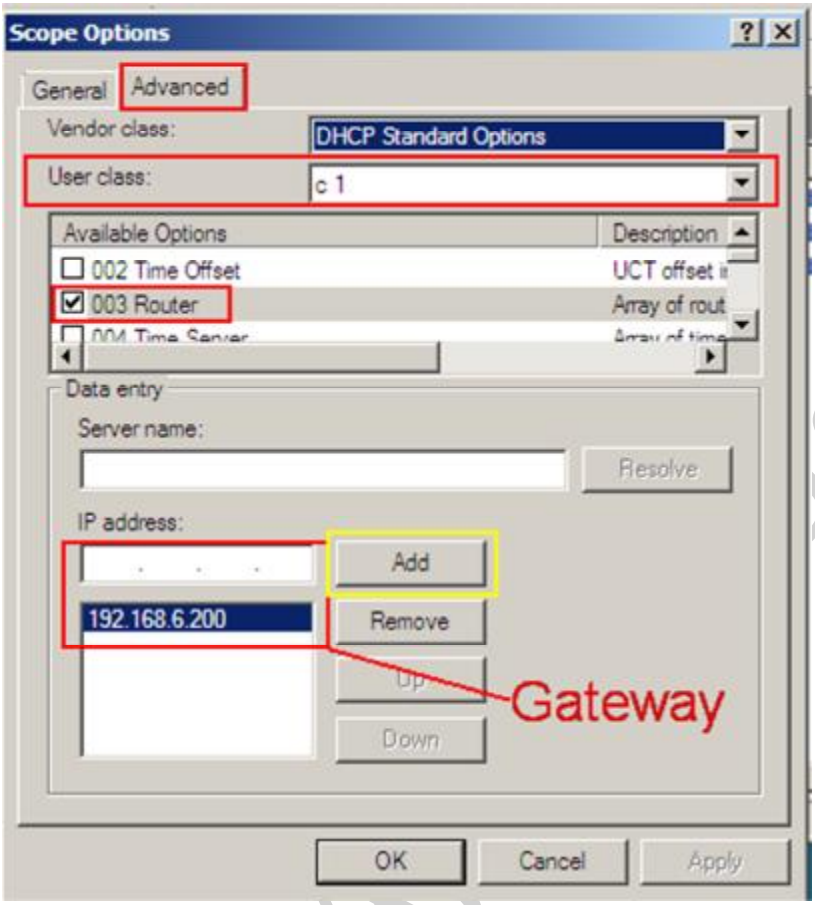



بعد از اینکه اسم کلاس را وارد کردیم باید در قسمت ASCII هم دوباره اسم کلاس را وارد کنیم.

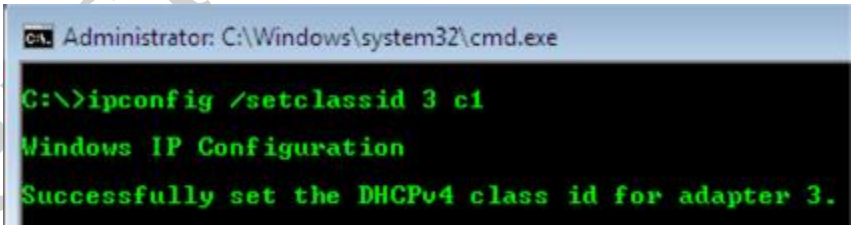
در مرحله بعد باید وارد اِسکوپ مورد نظر بشویم و آن را وارد کلاس C1 کنیم و برای Gateway, C1 مورد نظر را تعریف کنیم


DHCP
File Action View Help
DHCP
server2008.farshid2008.com
IPv4
Scope [172.31.1.0] s2
Address Pool
Address Leases
Reservations
Scope Options
Scope [192.0.0.0] Pool 1
Address Pool
Address Leases
Reservations
Server Op
IPv6
Scope Options
Option Name
Vendor
Value
006 DNS Servers
Standard
192.168.1.100
015 DNS Domain Name
Standard
Farshid2008.com
Configure Options...
View
Refresh
Export List...
Help
Contains commands for customizing this window.

FarshidAj

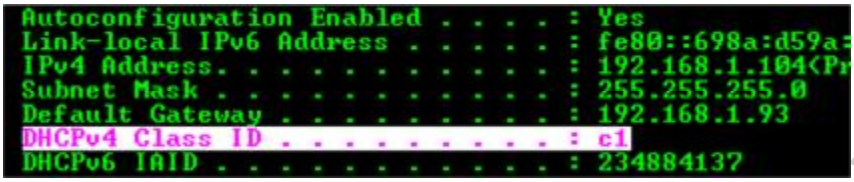



برای اینکه کلاینت ها را عضو کلاس بکنیم باید پشت هر کلاینت برویم و دستور ipconfig /setclassid 3 c1را وارد کنیم. 3= اسم کانکشن , c1 اسم کلاس




Farshid Ayash

برای اینکه ببینیم تغییرات اعمال شده دوباره دستور ipconfig را وارد می کنیم




- در اینجا 2 شبکه را در نظر بگیرید در شبکه اول تعدادی کلاینت داریم و در شبکه دوم یک سرور DHCP داریم این 2 شبکه توسط یک روتر به هم متصل شده اند و ما می خواهیم کلاینت ها یی که در شبکه اول هستند از شبکه دوم که سرور DHCP است Ip بگیرند, پس لازم است که کلاینت ها درخواست Ip کنند (DHCP DISCOVERY ) ولی یک مشکل وجود دارد,پکت DHCP DISCOVERY از نوع BroadCast می باشد و روترها پکت های BroadCast را از خود عبور نمی دهند.

برای حل این مشکل 3 راه حل وجود دارد 1) RFC1542 2) Ip Helper 3) DHCP RelayAgent

1)RFC1542این ویژگی در بعضی از روترها وجود دارد به این ترتیب که پکت DHCP DISCOVERY را از خود عبور می دهند اما روتری که این ویژگی را ساپورت کند گران است به همین دلیل کسی از این راهکار استفاده نمی کند.

2)IpHelper این یک دستور می باشد, باید به کنسول Device مورد نظر وصل شویم و این دستور را اجرا کنیم طرز کار آن به این صورت است که پکت BroadCast را به UniCast تبدیل می کند در واقع اینجا روتر در نقش یک مبدل عمل می کند.

- روترها می توانند Ip ها را با رنج متفاوت به هم وصل کنند.

4) DHCP Relay Agent

برای توضیح این روش سناریو 2 شبکه را به یاد بیاورید,در این روش در شبکه اول یک سرور 2008یا2003 نصب می کنیم کار این سرور این است که پکت های DHCP DISCOVERY که از نوع BroadCast می باشند را از کلاینت ها گرفته و به پکت های UniCast تبدیل می کند و از رتور عبور می دهد وبه سرور DHCP در شبکه دوم می رساند.

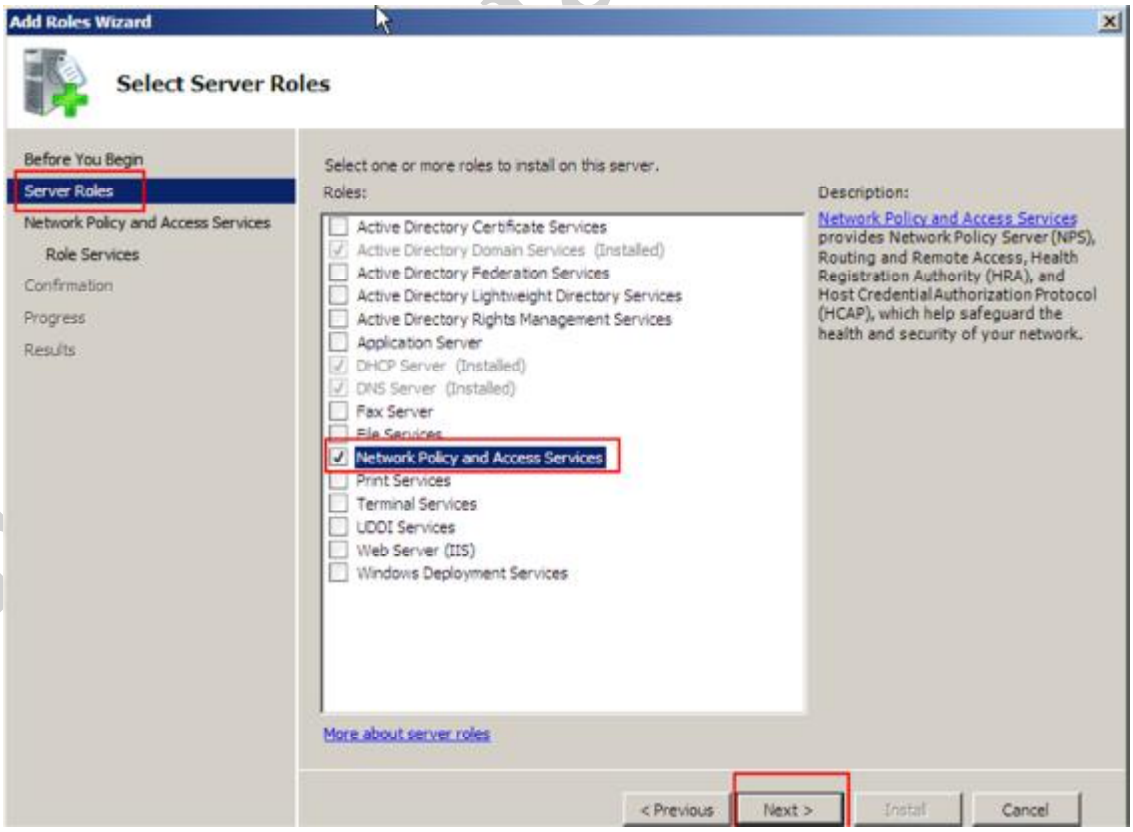
- خود DHCP Relay Agent باید Ip Static داشته باشد و Gatewaye آن باید Ip روتر باشد.
- DHCP Server احتیاج به RAM بالایی دارد چون IP اسکوپ ها روی RAM باز می شوند.

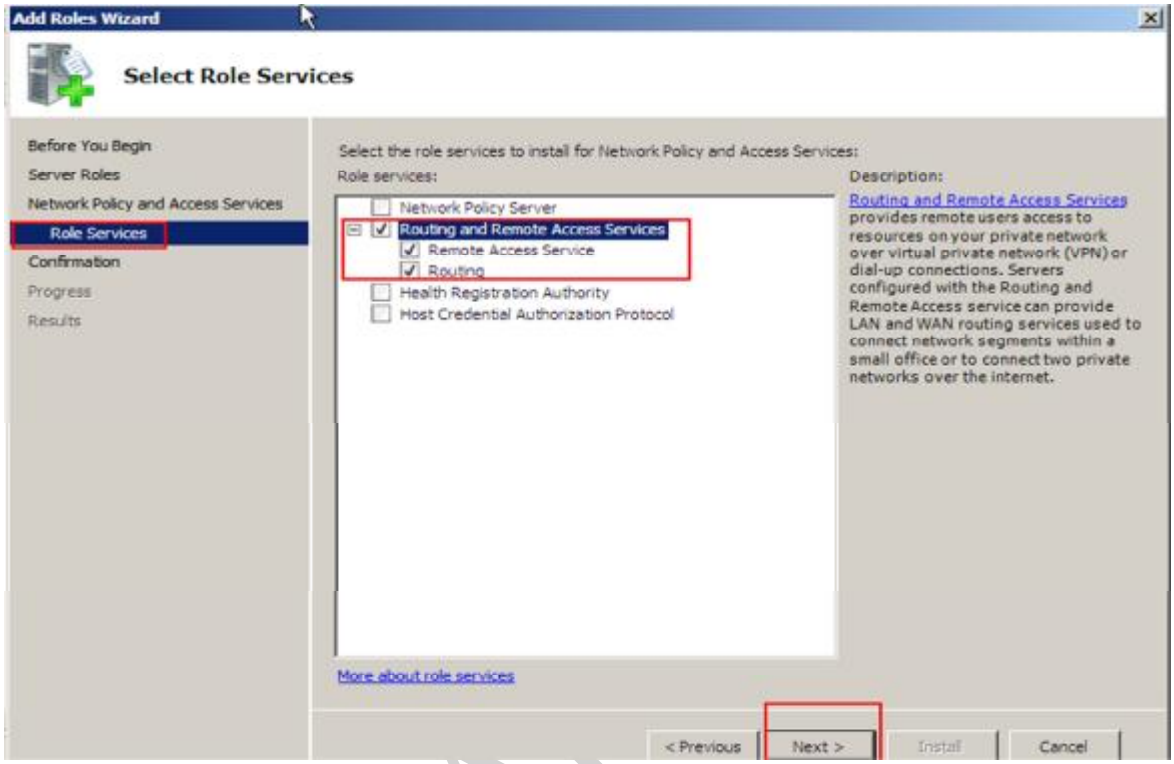
FarshidAjabnoush

بنا به 2 دلیل از این روش استفاده می کنیم در صورتی که می توانیم در همان شبکه اول یک سرور DHCP بگذاریم

1. در شبکه های که به صورت HUB & SPOKE طراحی می شوند برای اینکه بتوانند از شعبه اصلی(Hub ) به شعبات دیگر(Spoke ) Ip بدهند از روش DHCP Relay Agent استفاده می کنند به این دلیل که شعبات توسط روتر به هم متصل شده اند(اگر از این روش استفاده نکنند باید در هر شعبه یک DHCP بگذارند که روش مناسبی نمی باشد)
2. یک شبکه را درنظر بگیرید که فقط2 شعبه دارد ودر هر 2 شعبه سرور DHCP دارند اگر در شعبه2 سرور DHCP از کار بیفتد باید در همان شعبه2 یک کامپیوتر معمولی را بانصب سرور2003 یا2008 و راه اندازی RelayAgent بالا بیاوریم بعداز این کار سرور RelayAgent از DHCP سرور شعبه 1 برای کلاینت های شعبه2 Ip می گیرد به این نکته توجه داشته باشید که اولویت اول برای Ip دادن در شعبه 2 با DHCP سرور همان شعبه می باشد RelayAgent در زمان نبودن DHCP سرور فعال می شود, به این طراحی در اصطلاح Clustering On Server گویند.

اولین قدم برای راه اندازی DHCP RelayAgent نصب کنسول R Ras می باشد که به صورت زیر نصب می کنیم

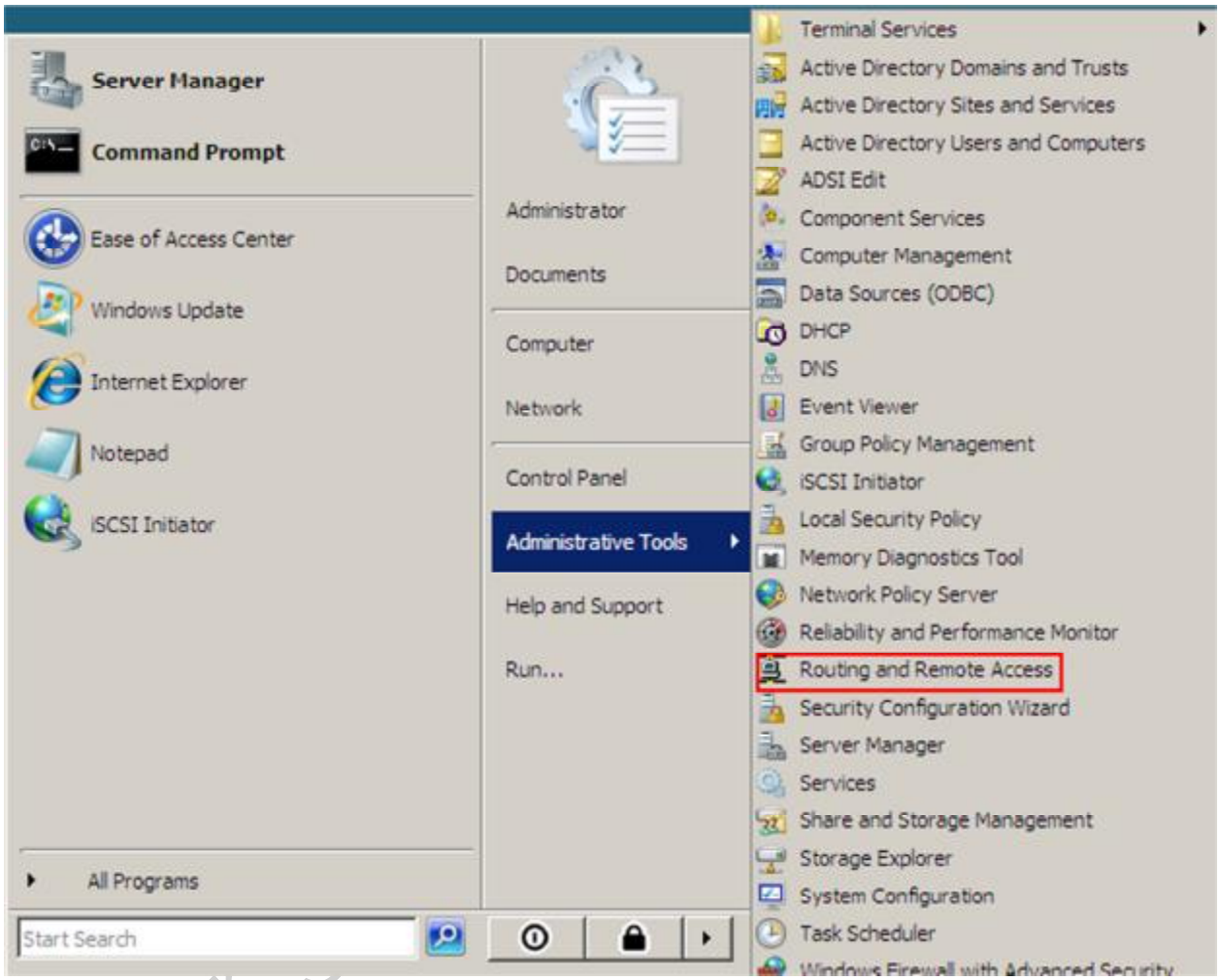





- در 2003 به صورت پیش فرض R Ras ( Routing and Remote AccessServices )نصب می باشد.

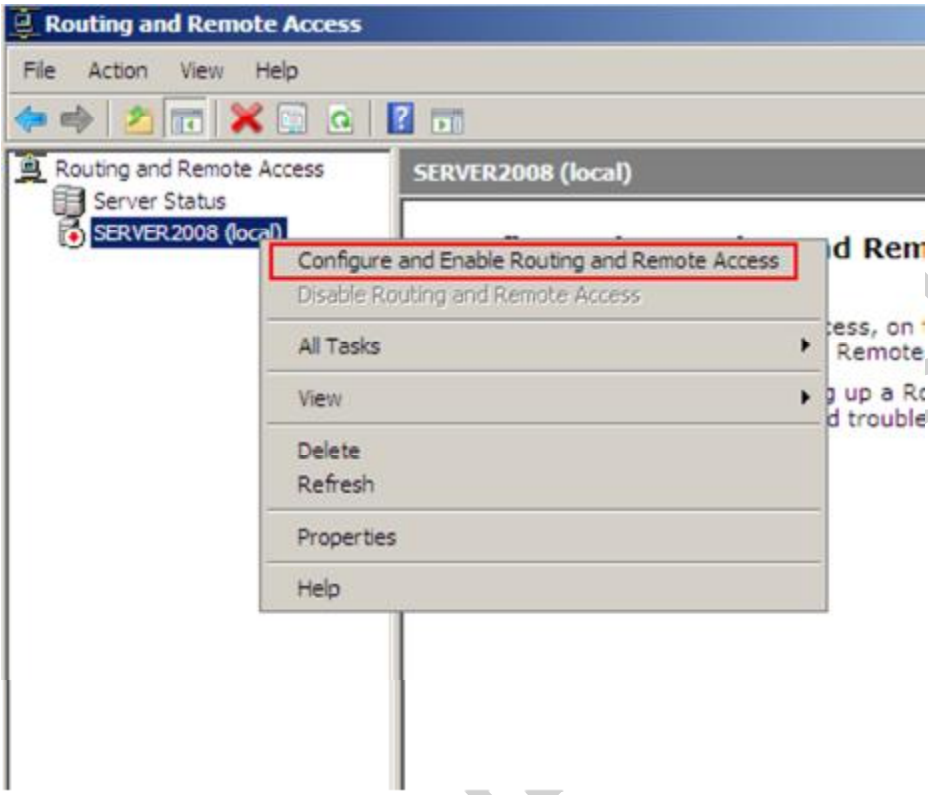
FarshidAj

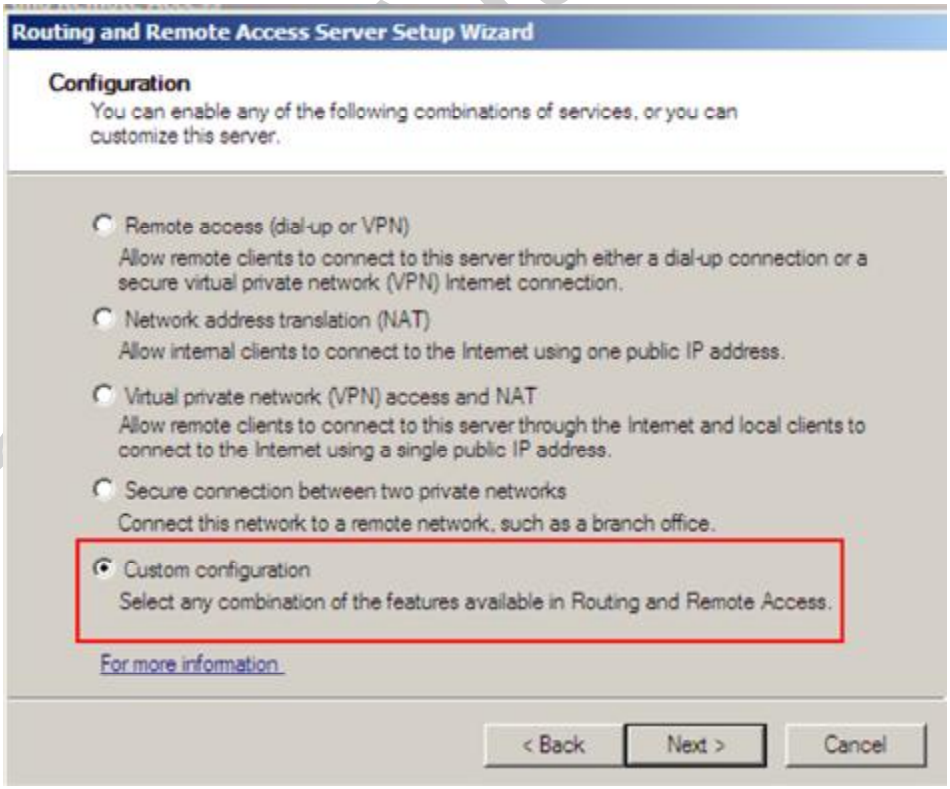
**بعد از نصب وارد کنسول می شویم**

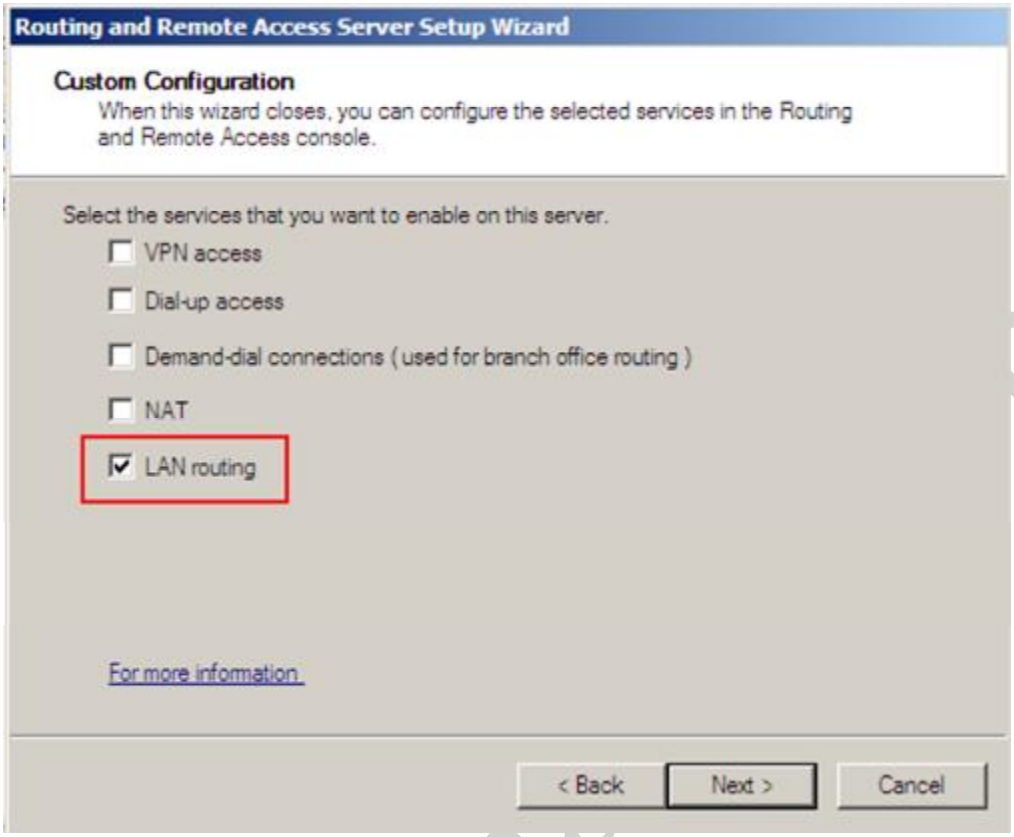



Far

سپس برای تنظیم کنسول مانند زیر عمل می کنیم

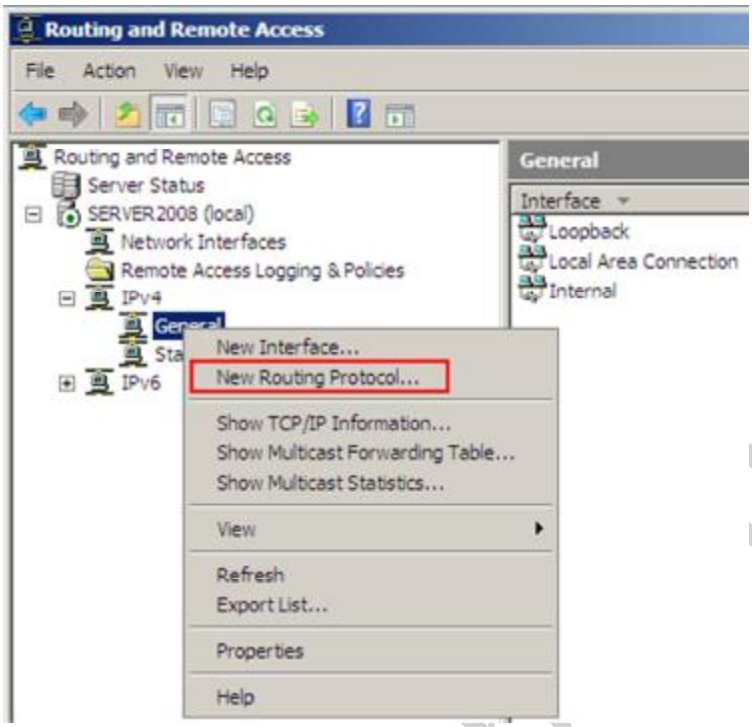


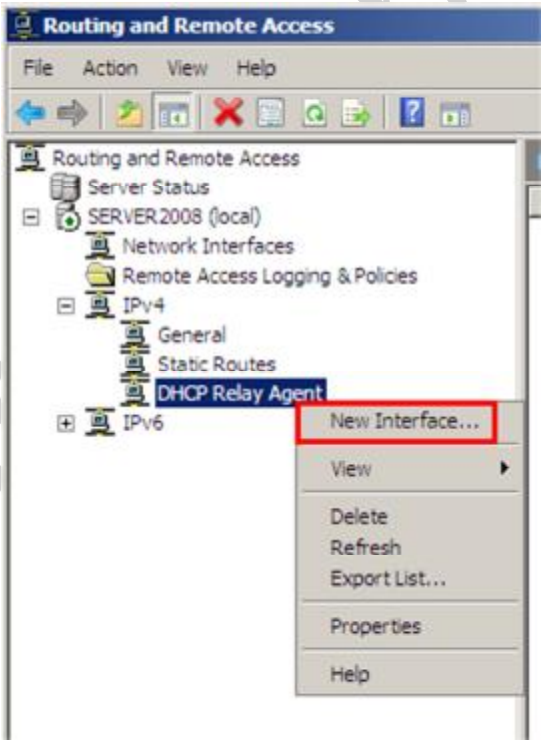





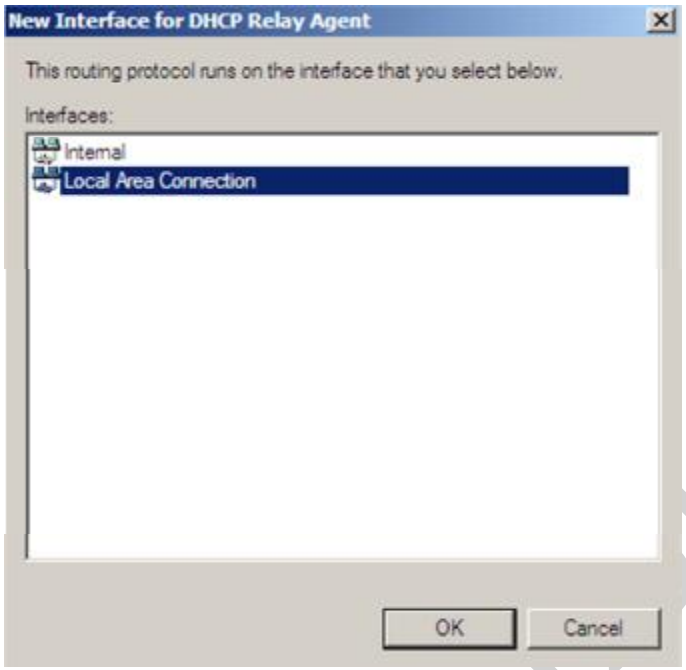

بعداز اتمام تنظیمات سرویس باید اجرا شود بعد از اجرا شدن سرویس بر روی General در Ip v4 کلیک راست و گزینه New Routing Protocol را انتخاب می کنیم

FarshidAj...n

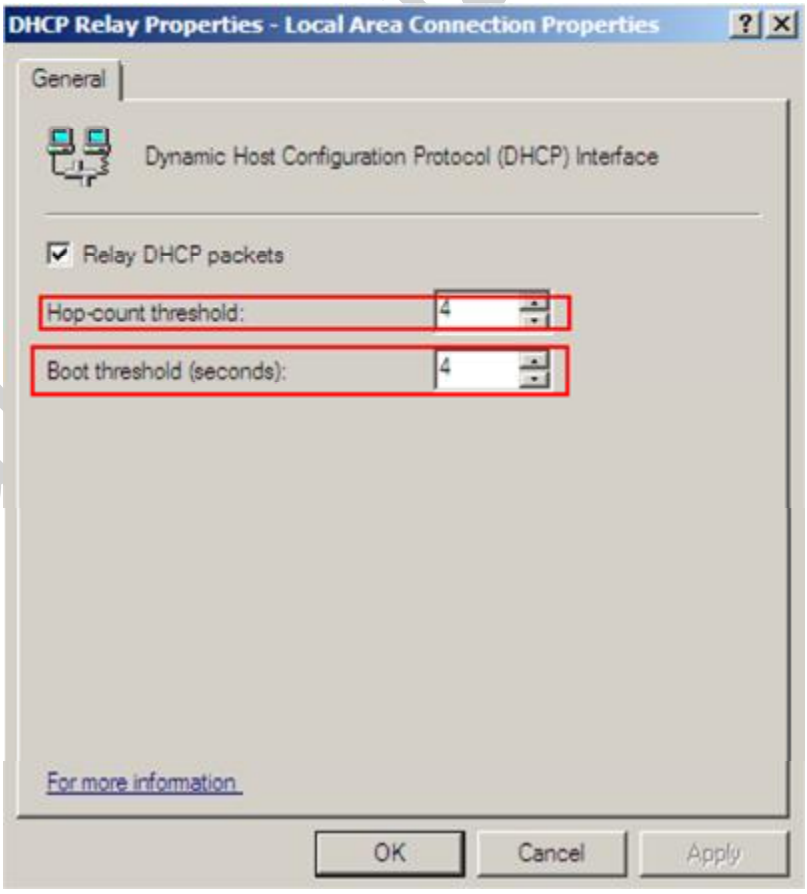



**در مرحله بعد باید کارت شبکه ای را انتخاب کنیم که عمل Binding ( کارتی که به طرف کلاینت ها است) را انجام می دهد**



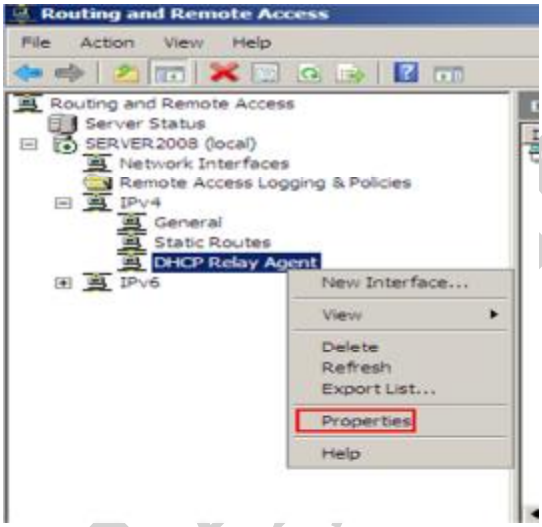

سپس به این صفحه منتقل می شویم

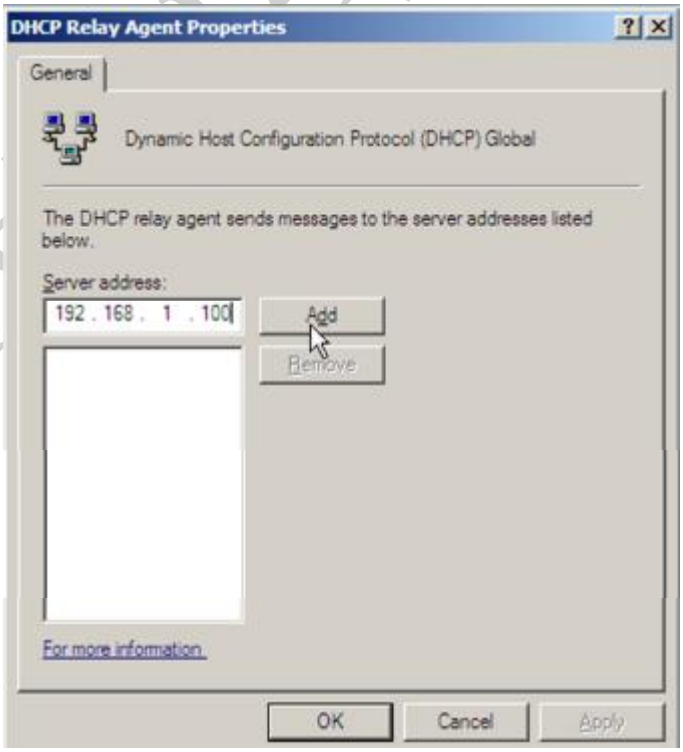


Hop-Count یعنی باید ازچند مسیر روتر عبور کند تا به DHCP برسد,منظور مسیر عبوری از یک روتر به روتر دیگر می باشد در اینجا 5 روتر داریم با 4 مسیر عبور به هر کدام از این مسیرها Hop-Count گویند.

Bootthresholdمنظور این گزینه اینست که بعد ازگذشت 4 ثانیه ازدرخواست کلاینت (DHCP Discovery ) اگر جوابی از سمت DHCP نیامد اتوماتیک درخواست را به RelayAgent منتقل کند.

در اینجا باید سرور DHCP را برایش تعریف کنیم, سناریو 2 شبکه را به یاد بیاورید در اینجا باید Ip سرور DHCP موجود درشبکه2 را به عنوان DHCP اصلی وارد کنیم.




Farzaneh Akbarpour

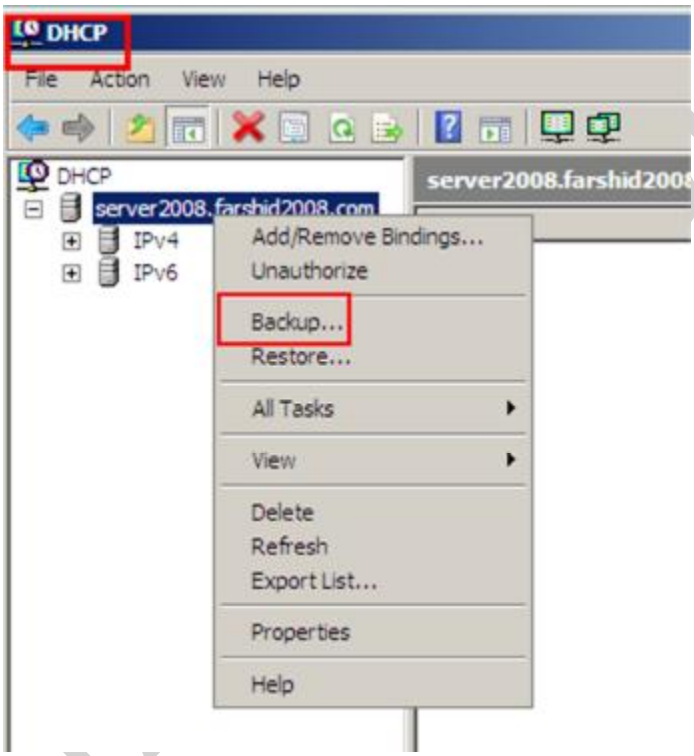
5) TroubleShooting DHCP

a) تمام شدن Ip در اِسکوپ  راه حل: از قبل باید 20% بیشتر از تعداد کلاینت ها اِسکوپ را درنظر بگیریم.

b) مناسب نبودن شرایط سرور برای DHCP سرور شدن  راه حل: بالا بودن Ram سرور (حداقل رم 1GB)

c) همیشه باید از اِسکوپ Backup داشته باشیم .

طریقه Backup گرفتن از اِسکوپ




Backup ها در مسیر C:\Windows\System32\dhcp ذخیره می شوند (دیتا بیس DHCPبا پسوند mdb)

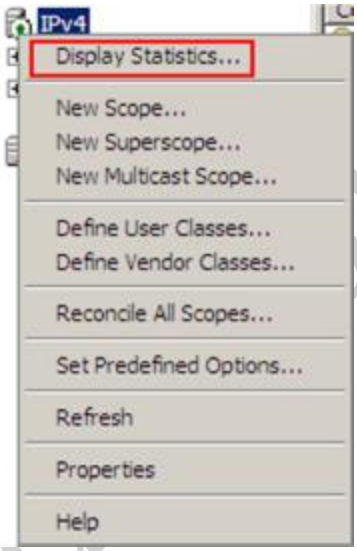
- DHCP اتوماتیک هر1 ساعت ازخودش Backup می گیرد.

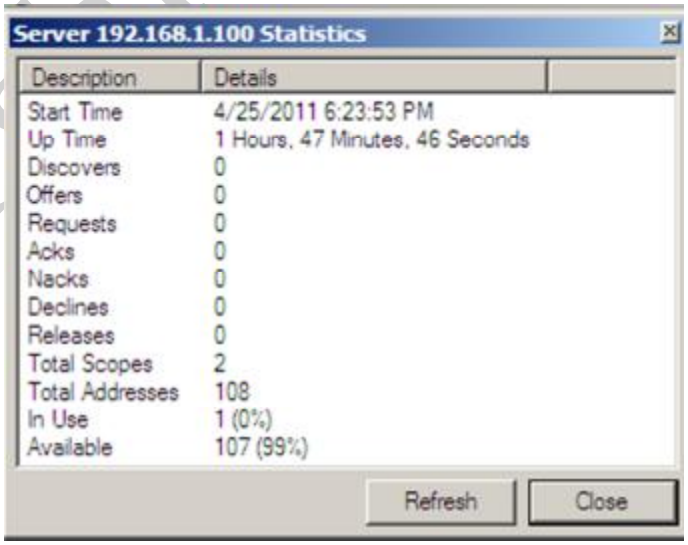
- زمانی پوشه Backup را باز می کنیم 2 فایل با پسوند JRS می بینیم این ها فایل های رزور شده توسط خود DHCP می باشند,این فابل ها خالی می باشند و برای زمان های خاص در نظر گرفته شدند هر کدام 1024 KB فضادارند.

Farshid Yousefi

- فایل های J50 , TransAction Log هستند یعنی اگربخواهیم تغییری در دیتابیس بوجود آوریم ابتدا بر روی این فایل ایجاد می شود وسپس بر روی دیتابیس.
- زمانی پوشه Backup را باز می کنیم فایلی با پسوند chk می بینیم,هر چیزی که داخل دیتا بیس DHCP ریخته می شود لاگشون داخل chk ذخیره می شود( برای ریکاوری).
- یک سری از فایل های دیگر هستند که انتهاشون به روزهای هفته ختم می شوند این فایل ها, لاگ فایل های هر روز هستند به این لاگ ها Auditing (بازرسی)گویند هر کدام از این فایل ها بعداز 7 روز پاک می شوند.
- تمامی Ip در رم لود می شوند.

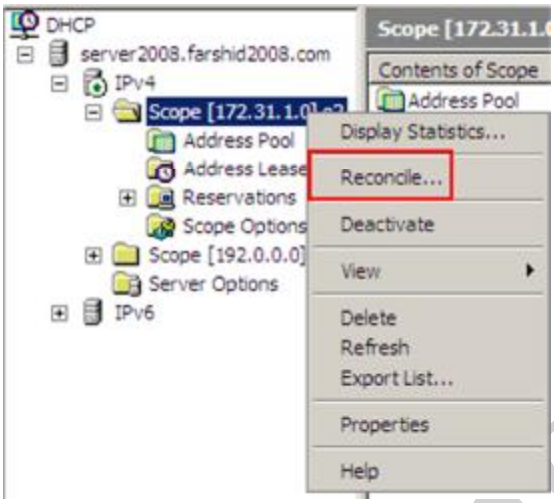
D ) برای دیدن آمار DHCP مانند زیر عمل می کنیم




Farshid Ghoush

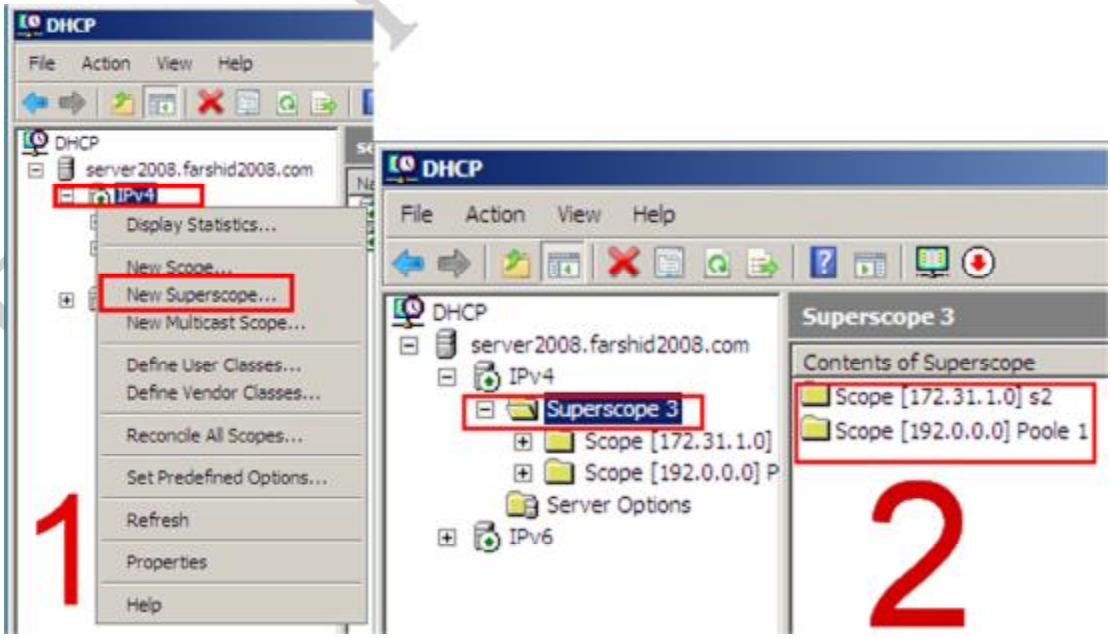
E ) اگر تنظیمی را در DHCP انجام دادیم و به کلاینت ها اعمال نشد برای این است که کنسول و رجیستری سرور با هم یکی نیستند برای برطرف کردن این مشکن مانند زیر عمل می کنیم




Super Scope

دلیل استفاده از این گزینه راحت تر کردن کارهای مدیریتی می باشد,با استفاده از گزینه تمام Scope ها با هم یکی می شوند یعنی اگر از Super Scope دستور غیرفعال کردن را بدهیم تمامی Scope ها غیر فعال می شوند.

- در DHCP فقط یکSuper Scope می توانیم بسازیم آن هم فقط در Ip v4 , در Ip v6Super Scope نداریم.




FarshidAjabnoush

## Terminal Server

**کار این سرور به اشتراک گذاری برنامه ها و فول دسکتاپ سرور تحت شبکه می باشد.**

- **این سرور احتیاج به کارت شبکه مناسب (Intel Pro 1000 ) RAM وCPU بالا احتیاج دارد علاوه بر این احتیاج به هاردی با سرعت Read/Write بالا دارد.**

**طرز کار ترمینال سرور**

**هر نرم افزاری که پشت ترمینال سرور نصب می شود به ازای هر کلاینت که به سرور وصل می شود مجزا اجرا می شود به این دلیل است که ترمینال سرور احتیاج به رم بالایی دارد به خاصیتی (مجزا اجرا شدن )که ترمینال سرور برای نرم افزارها بوجود می آورد Multiple User Enviroment گویند.**

- **لایسنس ترمینال سرور از لایسنس سیستم عامل مجزا می باشد اگر TS بدون لایسنس باشد 120 روز کارمی کند و بعد از 120روز بر روی سرور پیغامی مشاهده نمی کنیم زمانی که کلاینت ها می خواهند به TS وصل شوند به آنها پیغام لایسنس می دهد.**
- **لایسنس ترمینال سرور را باید بر روی کلاینت ها نصب کنیم.**
- **پورت TS 3389 می باشد.**

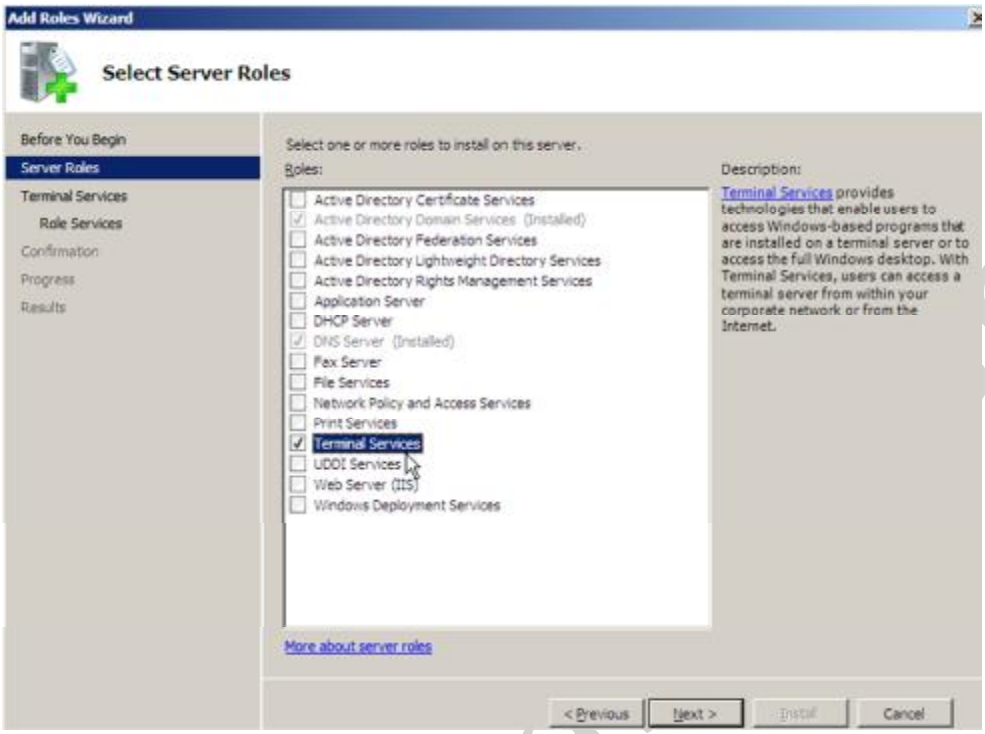
**تفاوت TS در 2003 و2008**

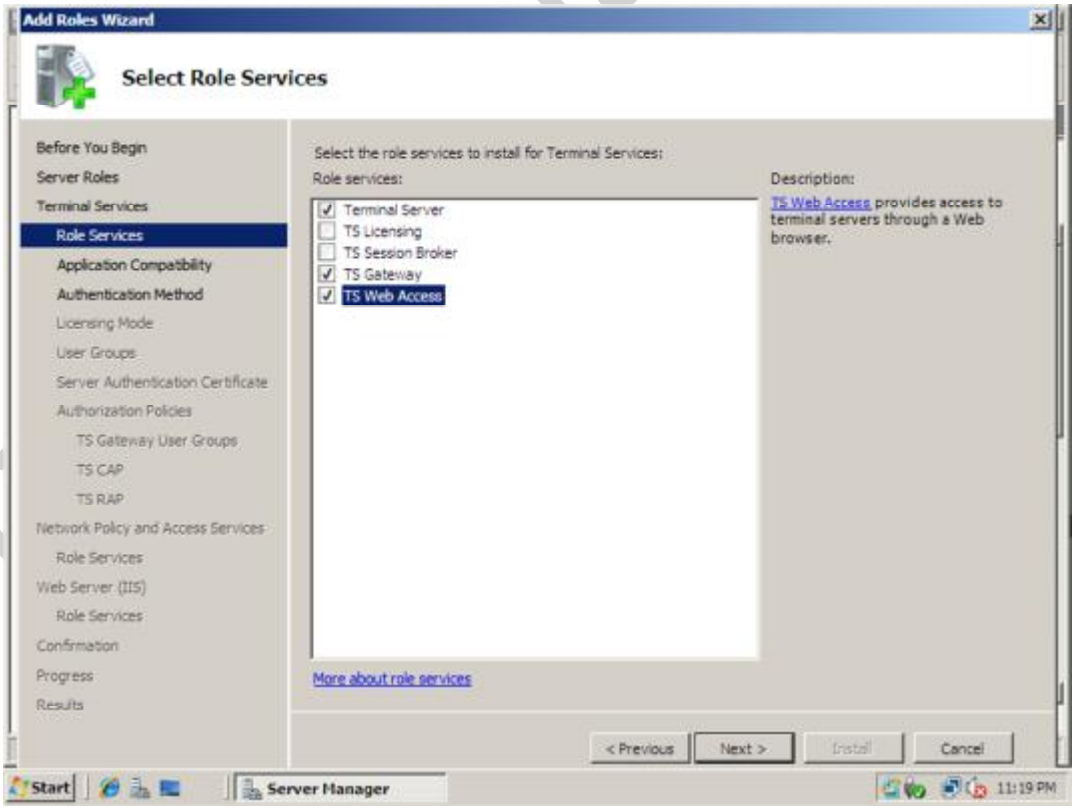
1) **TS 2003 Single Program می باشد یعنی در زمان استفاده از TS2003 فقط می توانیم یک نرم افزار را Load کنیم ولی 2008 Multi Program می باشد یعنی محدودیتی برای Load نرم افزار از TS ندارد.**
2) **در 2003 برای وصل شدن به TS باید به صورت RDP (ریموت دسکتاپ) وصل شویم ولی در 2008 علاوه بر RDP می توانیم (Web Base ) HTTP وصل شویم.**

**TS WEB**

**یک سری کلاینت را درنظر بگیرید,جلوی این کلاینت ها یک TS WEB بالا می آوریم و به آن IP Public می دهیم و به روی اینترنت قرار می گیرد سپس از بیرون و بر روی اینترنت TS WEB, IP Publicرا وارد می کنیم وبه آن وصل می شویم,زمانی که به آن وصل می شویم تمامی Ip های کلاینت ها را هم می بینیم و با انتخاب هر کدام از آنها دسکتاپ آن را در وسط IE خودمان مشاهده می کنیم یعنی به صورت Web Base ریموت دسکتاپ کرده ایم.**

FarshidAjabnoush


Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
Terminal Services
Role Services
Confirmation
Progress
Results
Select one or more roles to install on this 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 Services
Network Policy and Access Services
Print Services
Terminal Services
UDDI Services
Web Server (IIS)
Windows Deployment Services
Description:
Terminal Services provides technologies that enable users to access Windows-based programs that are installed on a terminal server or to access the full Windows desktop. With Terminal Services, users can access a terminal server from within your corporate network or from the Internet.
More about server roles
< Previous
Next >
Install
Cancel


Add Roles Wizard
Select Role Services
Before You Begin
Server Roles
Terminal Services
Role Services
Application Compatibility
Authentication Method
Licensing Mode
User Groups
Server Authentication Certificate
Authorization Policies
TS Gateway User Groups
TS CAP
TS RAP
Network Policy and Access Services
Role Services
Web Server (IIS)
Role Services
Confirmation
Progress
Results
Select the role services to install for Terminal Services:
Role services:
Terminal Server
TS Licensing
TS Session Broker
TS Gateway
TS Web Access
Description:
TS Web Access provides access to terminal servers through a Web browser.
More about role services
< Previous
Next >
Install
Cancel
Start
Server Manager
11:19 PM

در مرحله 2 باید 3گزینه موجود در شکل بالا را انتخاب کنیم.

گزینه اول,این گزینه باید فعال شود در غیر این صورت سیستم ما تبدیل به ترمینال سرور نمی شود.

گزینه دوم,این گزینه را ما ایرانی ها فعال نمی کنیم چون کنسولی است برای مدیریت لایسنس ها,به لایسنس های روی ترمینال سرور Ts Cals گویند.

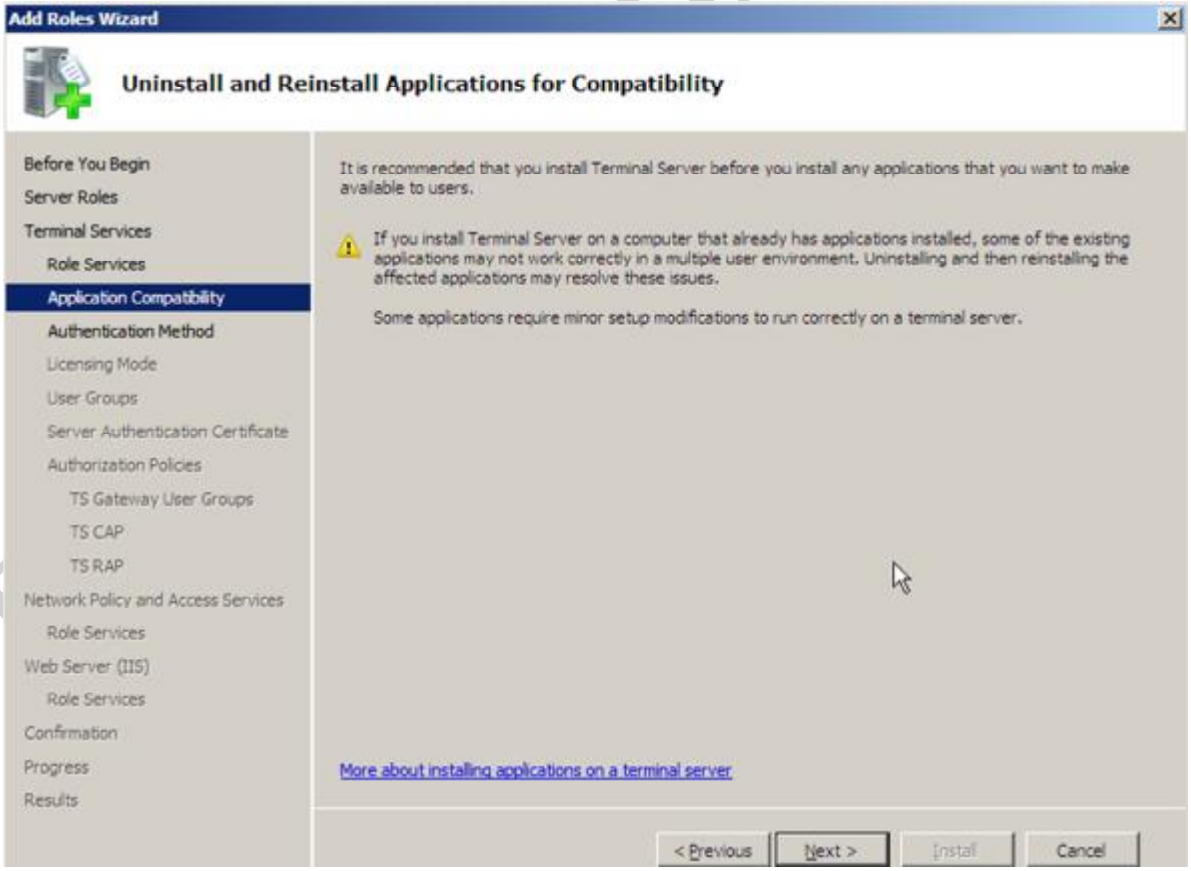
- لایسنس ها بر دو دسته هستند 1) Per Device به ازای هر کامپیوتر 2) Per User به ازای هر کاربر
- کرک های موجود برای TS , Per User می باشند.

گزینه سوم,یک شبکه را درنظر بگیرید در این شبکه 5 ترمینال سرور وجود دارد کلاینتی به TSسوم وصل می شود و شروع به استفاده از منابع TS می کند,بنا به دلایلی کلاینت DC می شود زمانی که دوباره کلاینت به شبکه وصل می شود و به سراغ همان TS می رود یعنی به همان TS قبلی که TSسوم بود وصل می شود.

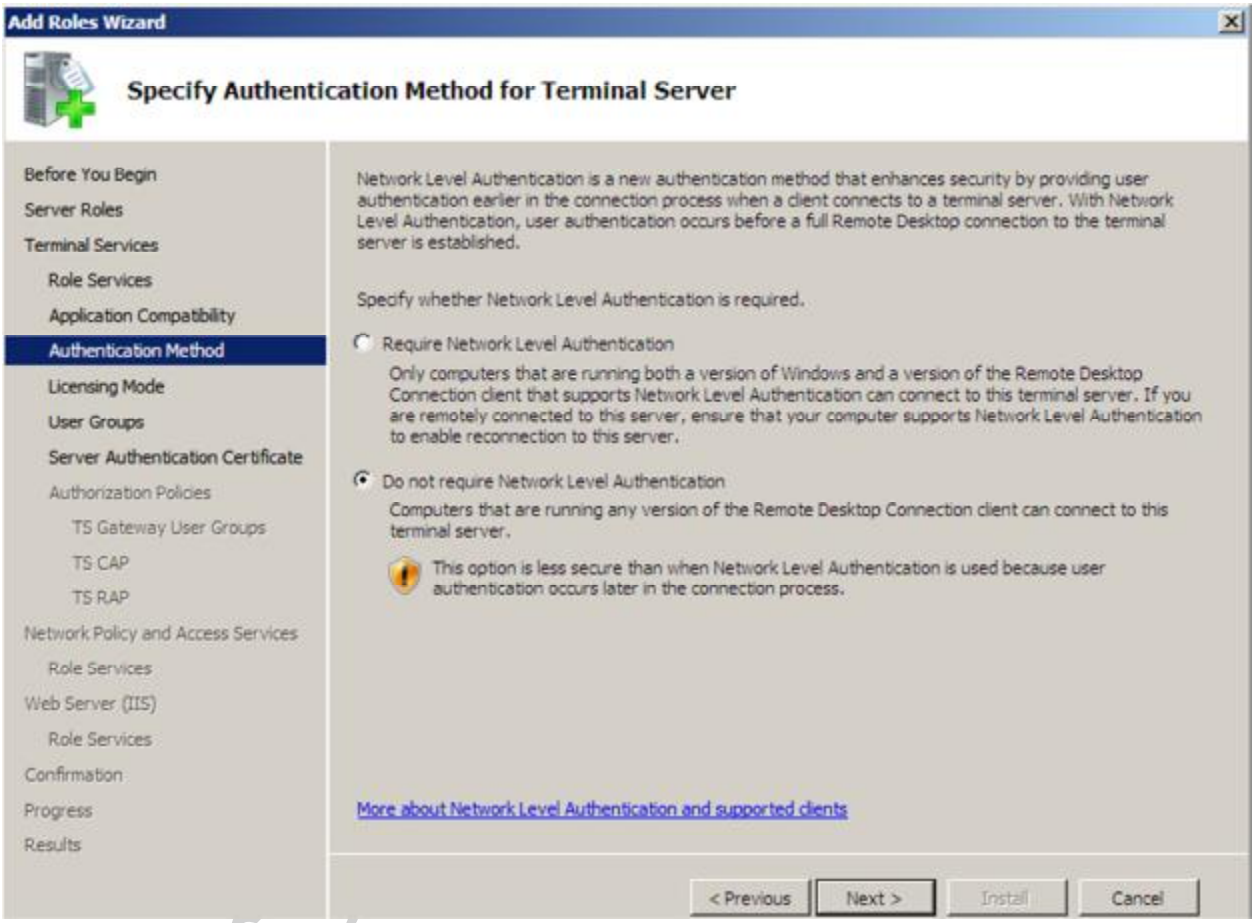
- با فعال بودن گزینه 3 ,ویژگی کلاسترینگ بر روی TS فعال می شود, برای استفاده از گزینه3 احتیاج به AD داریم یعنی فقط در شبکه های دامینی کار می کند.

گزینه چهارم,این گزینه حتماً باید فعال باشد با فعال بودن این گزینه TS ما از روی اینترنت هم قابل دسترس می باشد.

گزینه پنجم,باید فعال باشد.

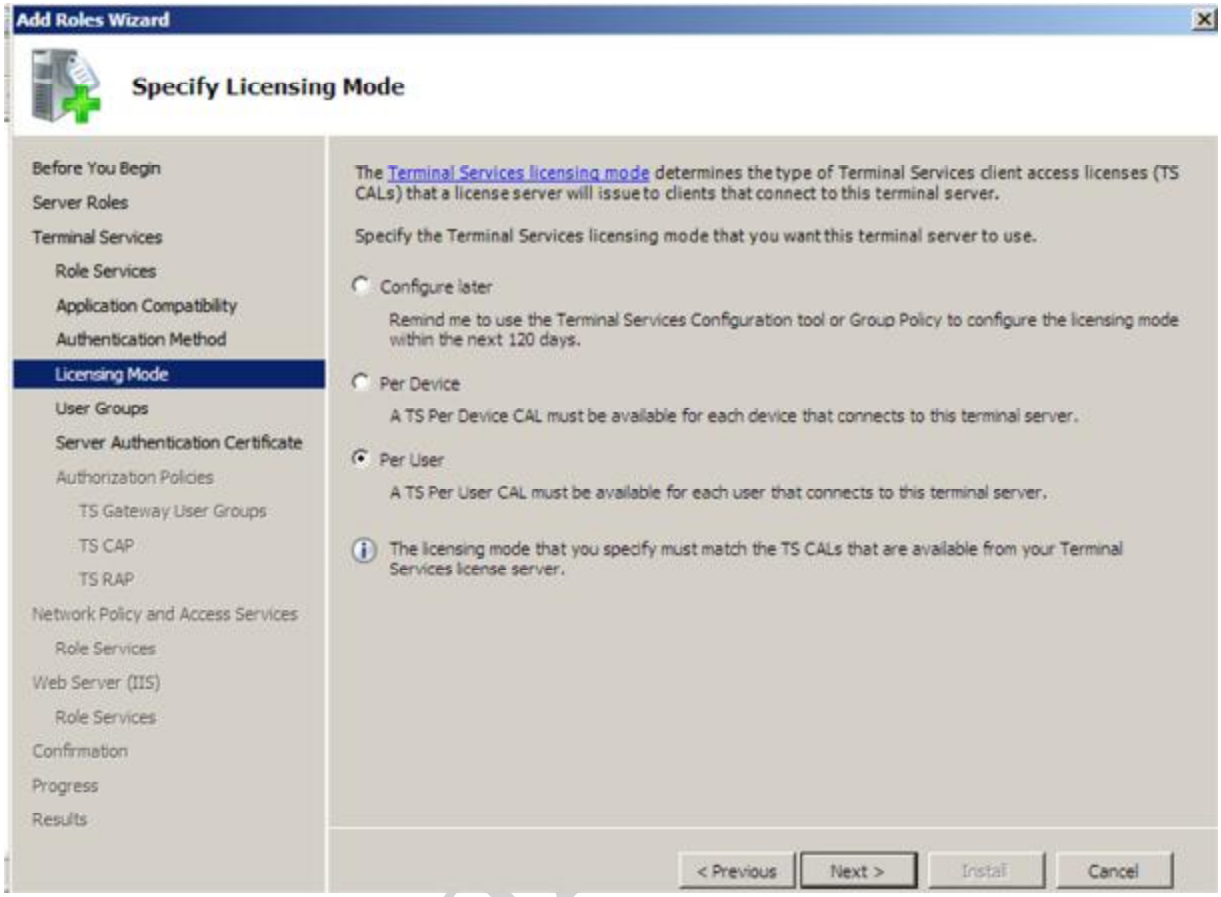


در صفحه بعد ( شکل بالا) توصیه می کند برای اینکه نرم افزارهای موجود در TS خاصیت Multiple UserEnviromentپیدا کنند بهتر است بعداز راه اندازی TS آنها را نصب کنیم چون ممکن است نرم افزاری که قبل از TS نصب شده باشد نتواند ویژگی Multiple User Enviromentپشتیبانی کند.



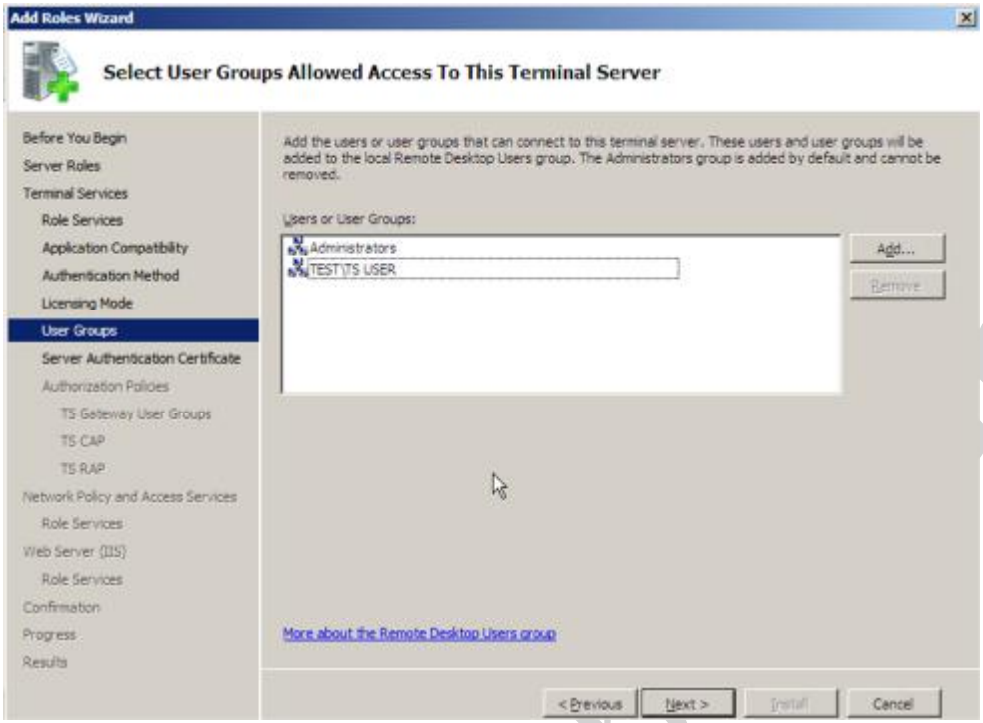

در صفحه بالا از ما می پرسد کسانی که با RDP وصل می شوند NLA آنها را چک کند؟ اگر فعال باشد XP نمی تواند وصل شود در این صورت باید RDP 6.1 را بر روی XP نصب کنیم تا NLA را ساپورت کند.

در این مرحله از ما تکلیف لایسنس را می پرسد که بر روی Per User می گذاریم تا بعداً آن را کرک کنیم !! :)



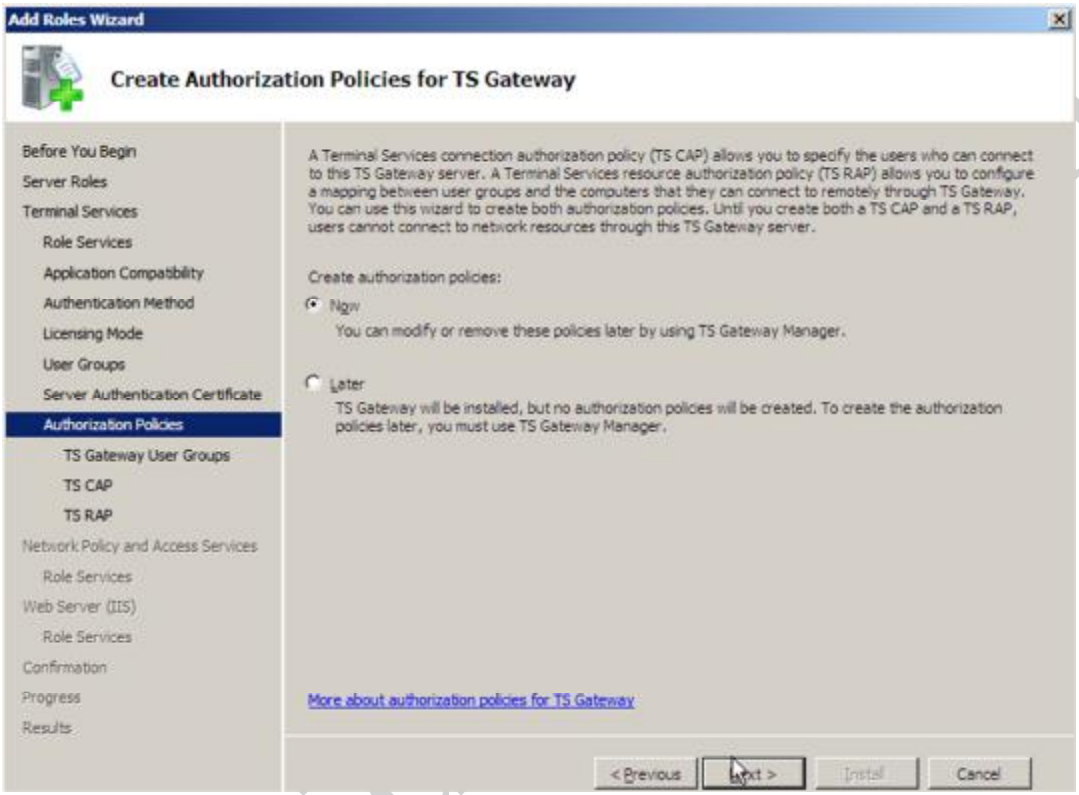

**در مرحله بعد از ما سوال می کند که چه کسانی می توانند از داخل شبکه به TS وصل بشوند و از آن استفاده کنند گروه Administrators به صورت پیش فرض در اینجا موجود می باشد,بهتر است گروهی بسازیم و کاربرهای مورد نظر را به آن گروه اضافه کنیم و آن گروه را هم در اینجا اضافه کنیم (مانند شکل).گروه Administrators را نمی توان از اینجا پاک کرد.**

Farshid




**در مرحله بعد می گوید کسانی که از بیرون می خواهند وصل شوند باید با HTTPS وصل شوند و برای این کار احتیاج به CA سرور داریم اگر CA داریم گزینه1 و باید مسیر آن مشخص شود اگر هم نداریم گزینه 2 را انتخاب می کنیم که می گوید خودت آن را بساز**

در اینجا می گوید برای کسانی که می خواهند از بیرون وصل شوند باید پالیسی تعریف شود, الان پالیسی را تعریف می کنی یا بعداً ؟



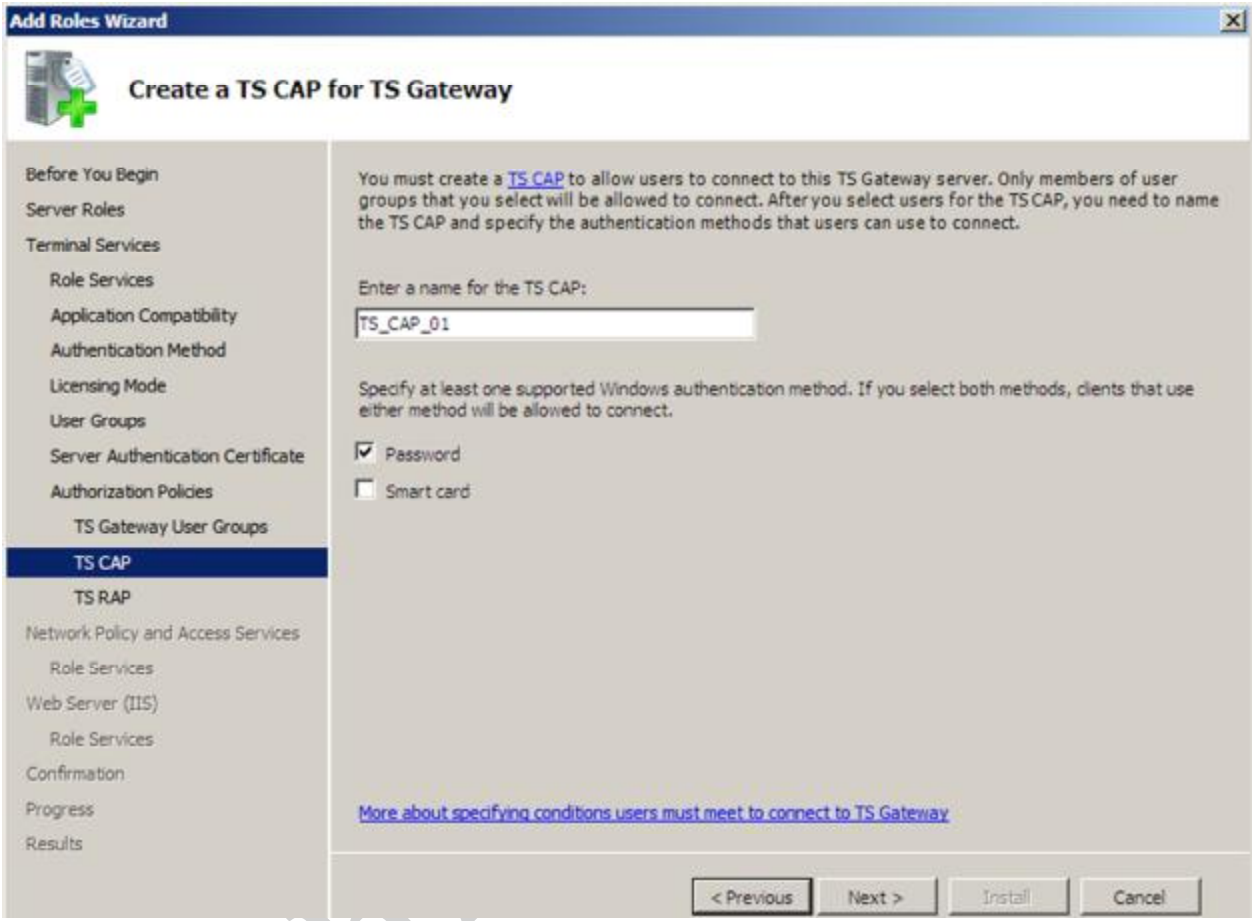

ما 2 نوع پالیسی داریم

1) Terminal Services Connection Authorization Policies ( TS CAP)

2) Terminal Services ResourceAuthorization Policies ( TS ARP )

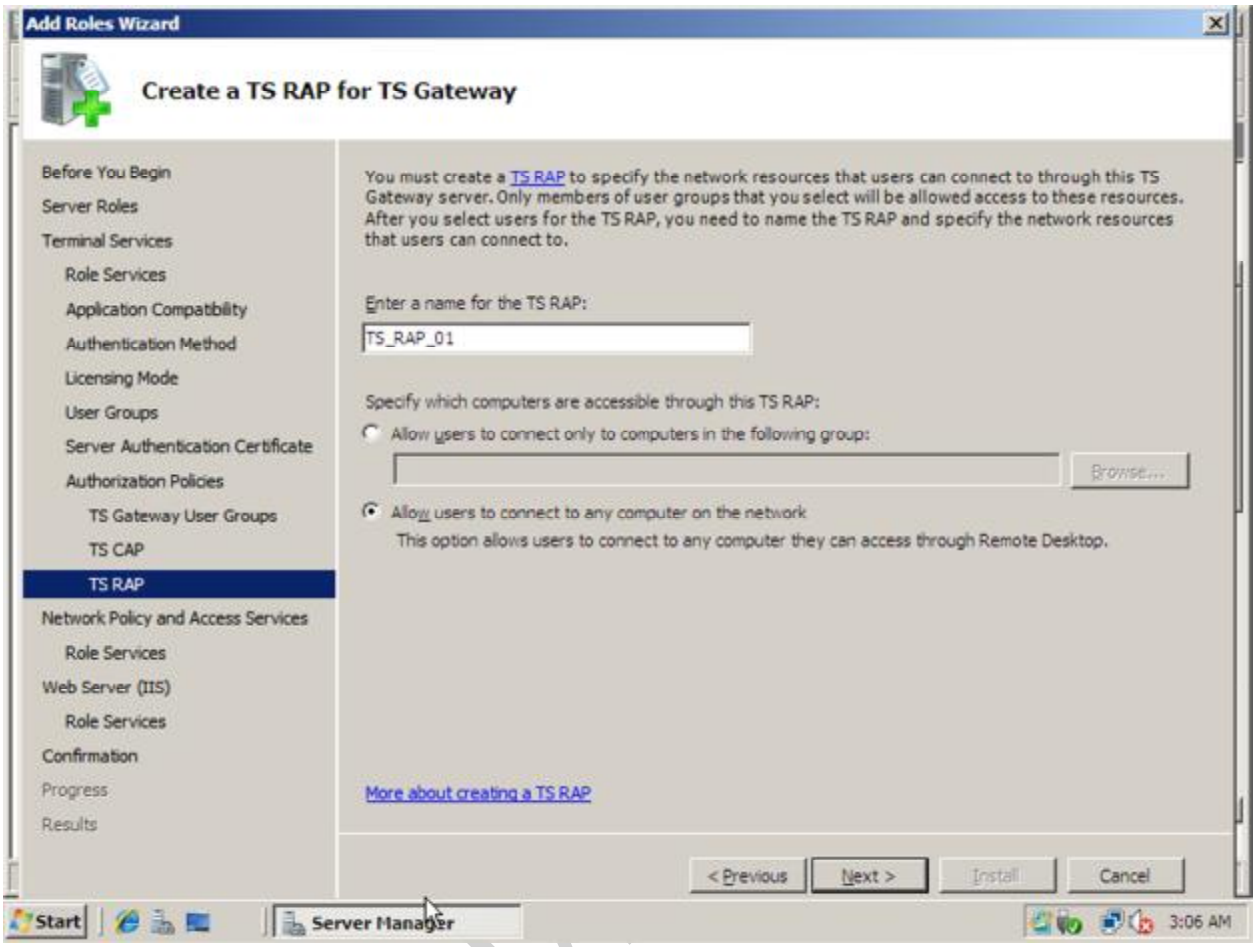
Farshid

در اینجا سوال می پرسد زمانی که وصل شدند برای لایسنس از آنها پسورد بخواهم یا کارت هوشمند؟ ( پسورد)




Farsh

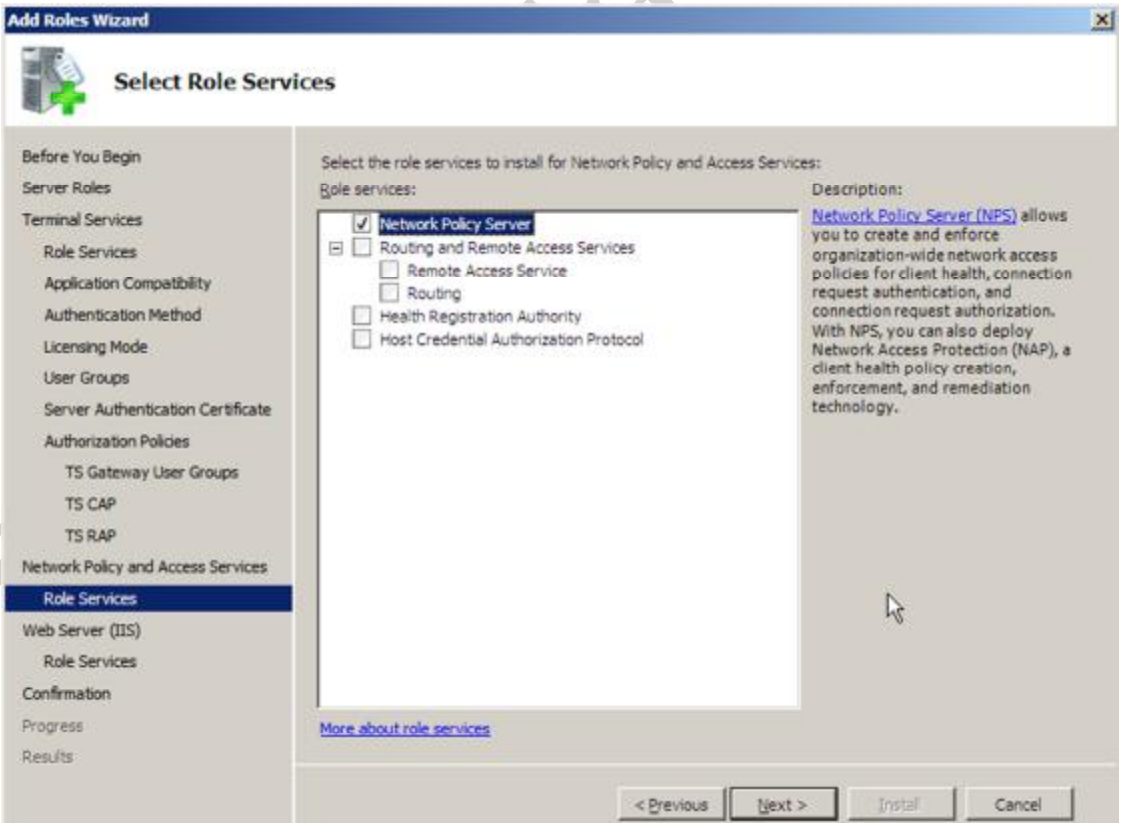
در مرحله بعد از ما سوال می کند اگر کسی از بیرون وصل شد به کدام کامپیوترها دسترسی داشته باشد؟ با انتخاب گزینه اول می توانیم اسامی کامپیوترهایی را که می خواهیم بتوانیم از بیرون بر روی آنها RDP کنیم را می توانیم اضافه کنیم گزینه دوم می گوید به تمامی کا مپیوترها .



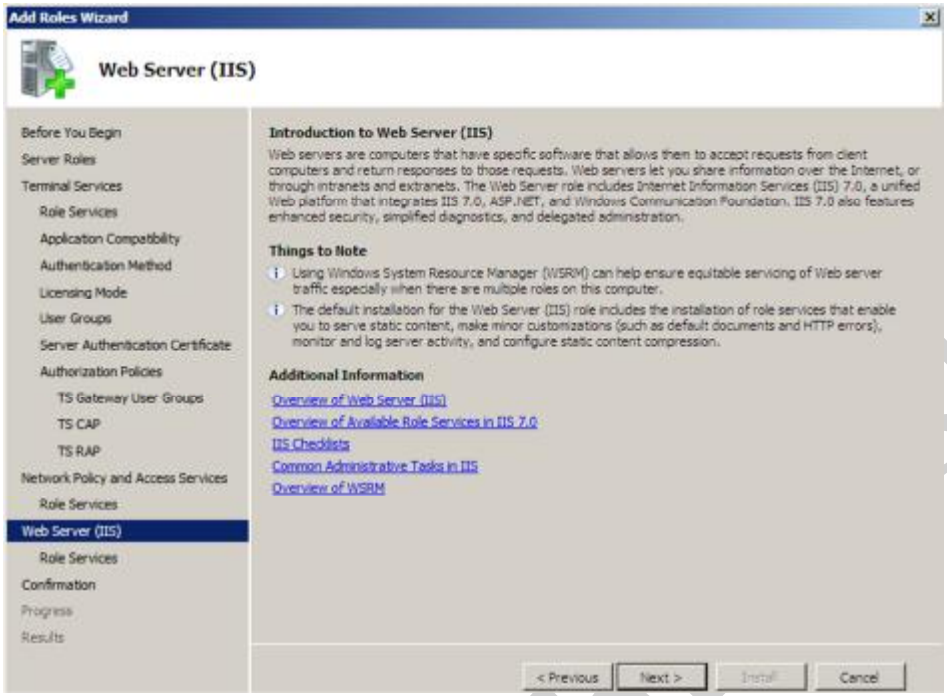

- گزینه اول امنیت بالاتری دارد.
- این صفحه  برای TS WEB می باشد.

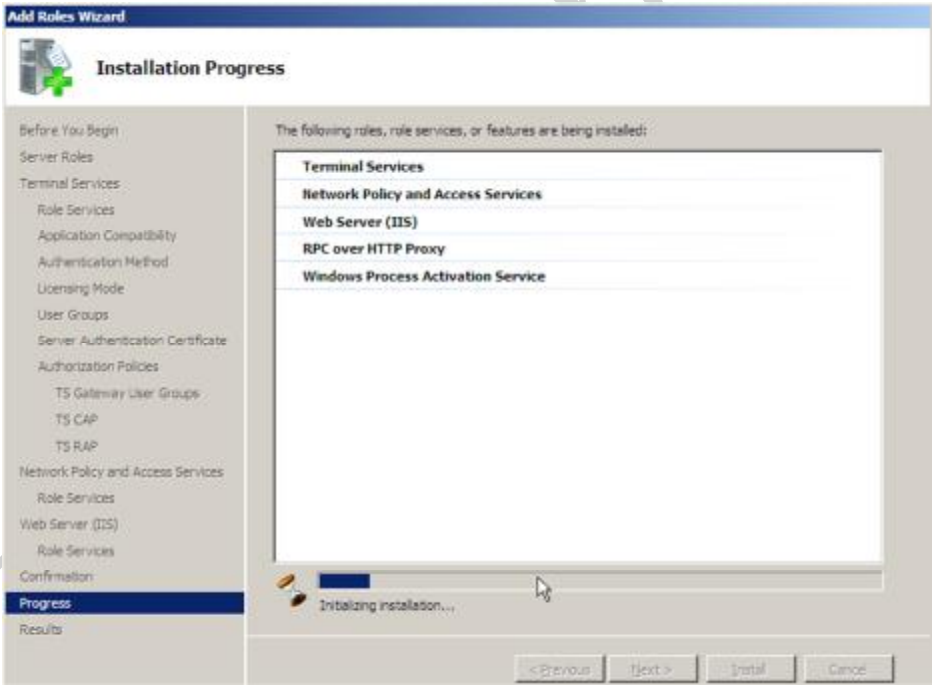
اسم سروری که پالیسی ها را در اینجا کنترل می کند Network Policy Server می باشد( NPS)

Farshidan




چون باید به اینترنت وصل شود احتیاج IIS دارد

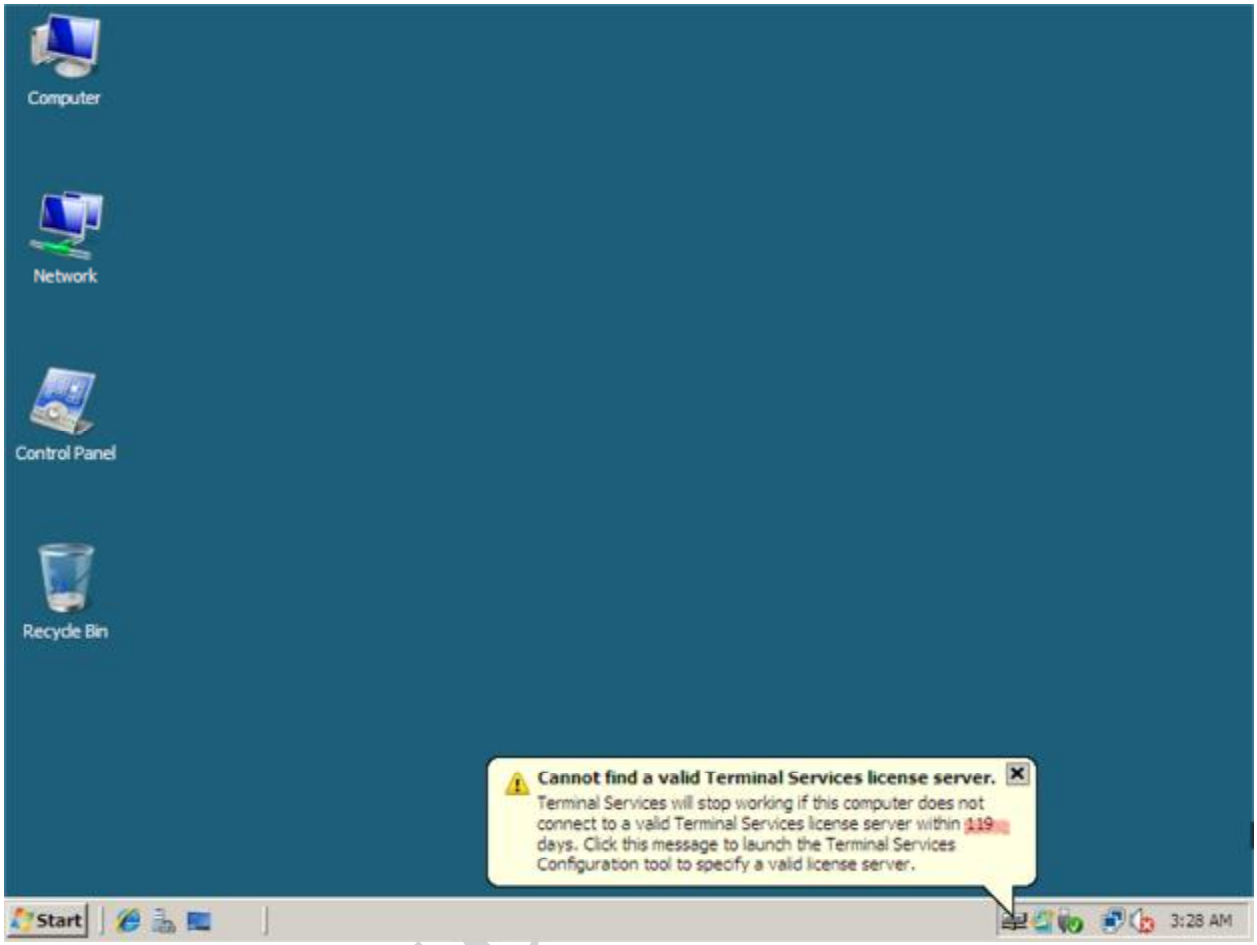



**و در آخر هم باید حتماً ریستارت شود.**

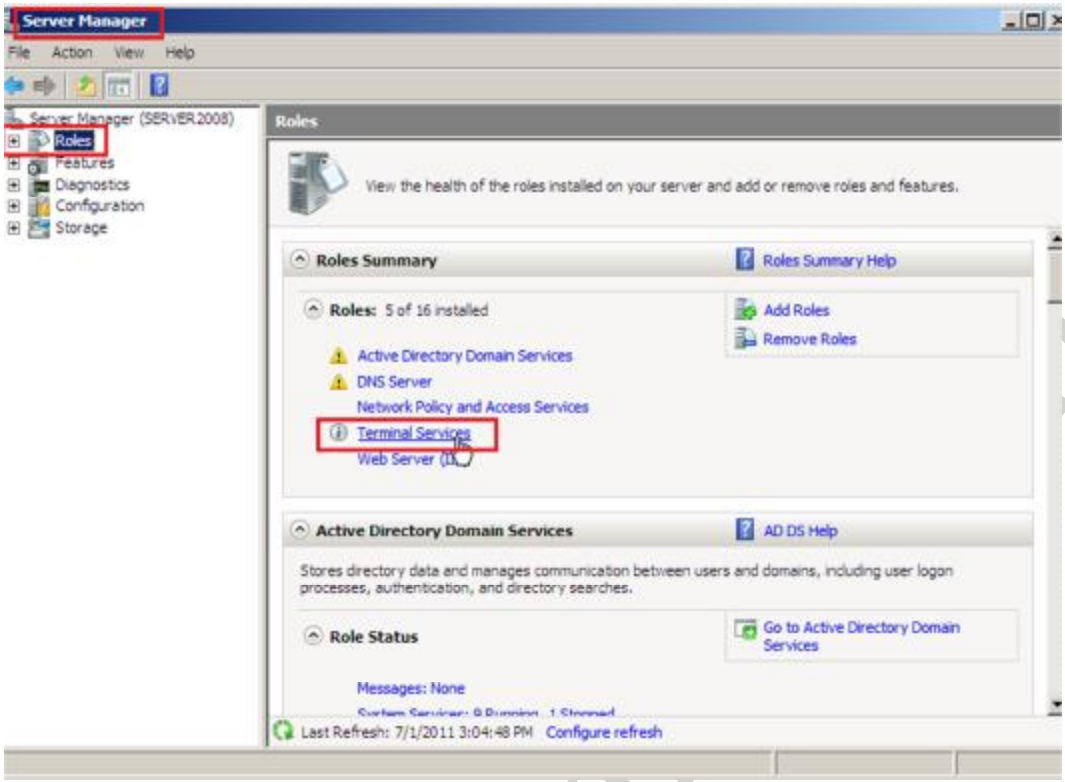
- **با کنسول WSRM می توان مقدار منابع سخت افزاری لازم برای هرکلاینت های TS را تعیین کرد این کنسول هم در2008 و هم در 2008 R2 موجود می باشد که در R2 بهتر عمل می کند.**

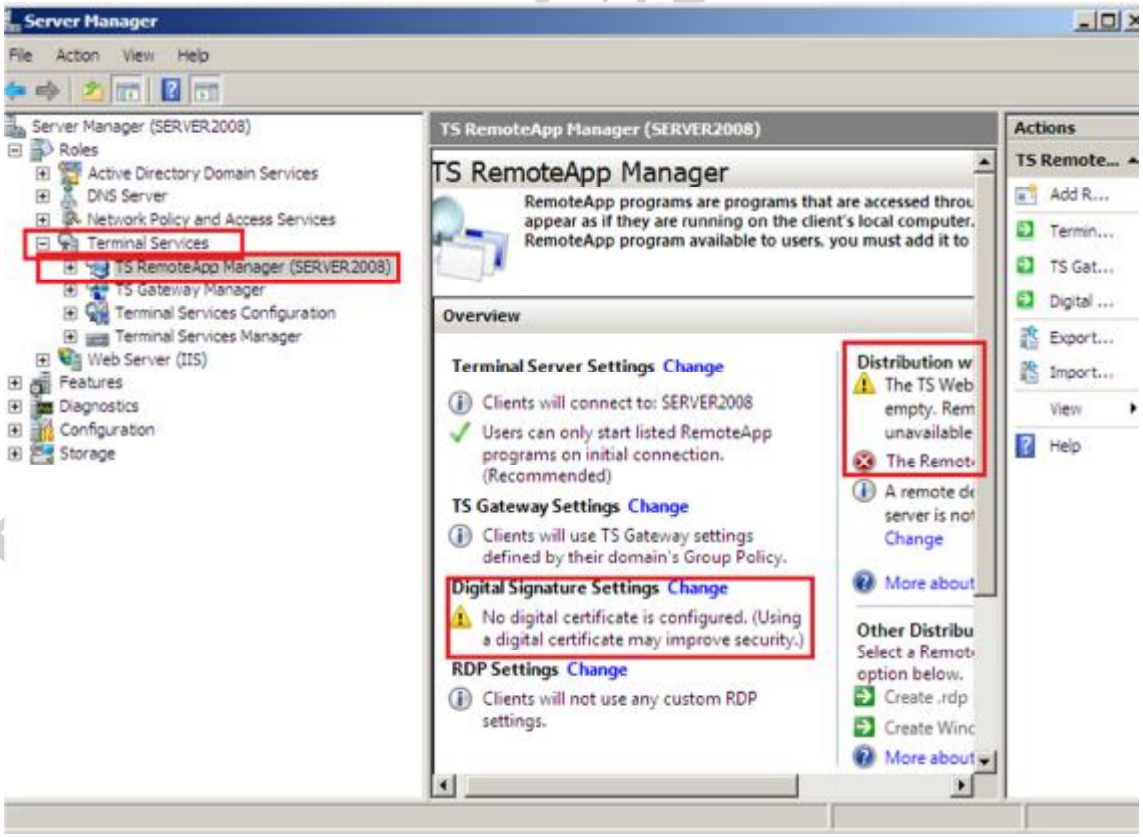
**بعد از نصب و ریستارت شدن وقتی سرور بالا می آید با پیغام زیر مواجه می شویم**




**در این پیغام می گوید از 120 روز لایسنس شما 119 روز باقی مانده است.**

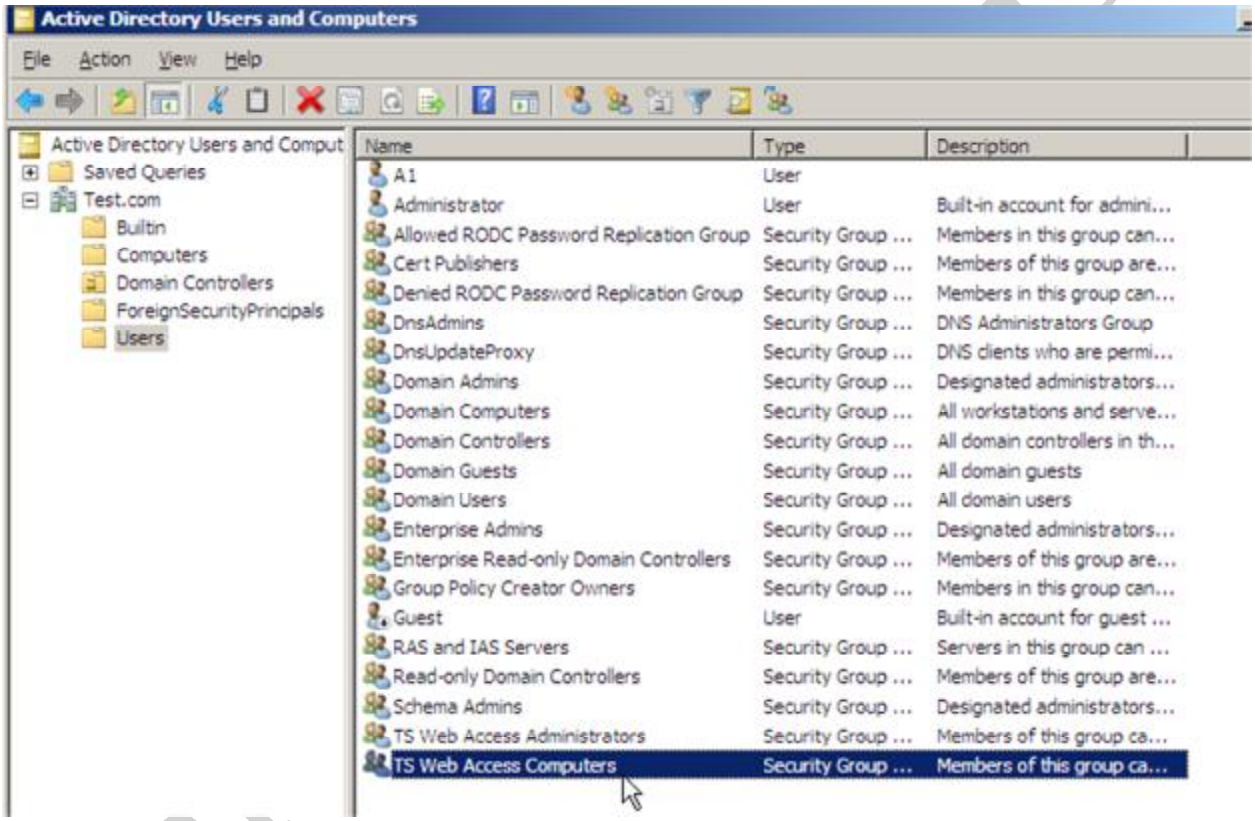
Farshid

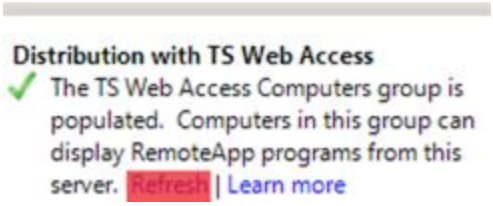

Server Manager
File Action View Help
Server Manager (SERVER2008)
Roles
Features
Diagnostics
Configuration
Storage
Roles
View the health of the roles installed on your server and add or remove roles and features.
Roles Summary
Roles Summary Help
Roles: 5 of 16 installed
Add Roles
Remove Roles
Active Directory Domain Services
DNS Server
Network Policy and Access Services
Terminal Services
Web Server (IIS)
Active Directory Domain Services
AD DS Help
Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.
Role Status
Go to Active Directory Domain Services
Messages: None
Last Refresh: 7/1/2011 3:04:48 PM Configure refresh


Server Manager
File Action View Help
Server Manager (SERVER2008)
Roles
Active Directory Domain Services
DNS Server
Network Policy and Access Services
Terminal Services
TS RemoteApp Manager (SERVER2008)
TS Gateway Manager
Terminal Services Configuration
Terminal Services Manager
Web Server (IIS)
Features
Diagnostics
Configuration
Storage
TS RemoteApp Manager (SERVER2008)
TS RemoteApp Manager
RemoteApp programs are programs that are accessed throu
appear as if they are running on the client's local computer.
RemoteApp program available to users, you must add it to
Overview
Terminal Server Settings Change
Clients will connect to: SERVER2008
Users can only start listed RemoteApp programs on initial connection. (Recommended)
TS Gateway Settings Change
Clients will use TS Gateway settings defined by their domain's Group Policy.
Digital Signature Settings Change
No digital certificate is configured. (Using a digital certificate may improve security.)
RDP Settings Change
Clients will not use any custom RDP settings.
Distribution w
The TS Web
empty. Rem
unavailable
The Remot
A remote de
server is not
Change
More about
Other Distribu
Select a Remot
option below.
Create .rdp
Create Winc
More about
Actions
TS Remote...
Add R...
Termin...
TS Gat...
Digital ...
Export...
Import...
View
Help

در شکل بالا 2 Warning می بینیم و 1 Error, اولین Warning می گوید لایسنس را من نصب کردم باید برای بهبود امنیت لایسنس خودت را وارد کنی,دومینWarning

می گوید گروهی به عنوان TS Web Access Computer وجود دارد که اگر کسی عضو این گروه بشود می تواند ازتمامی برنامه های روی ترمینال سرور را استفاده کند, کسی عضو این گروه نیست برای اینکه کسی را عضو این گروه کنیم مانند شکل زیر وارد آن گروه می شویم و کاربری را به آن اضافه می کنیم و دوباره به کنسول قبلی باز گشته وبا زدن Refresh دومینWarningهم از بین می رود.



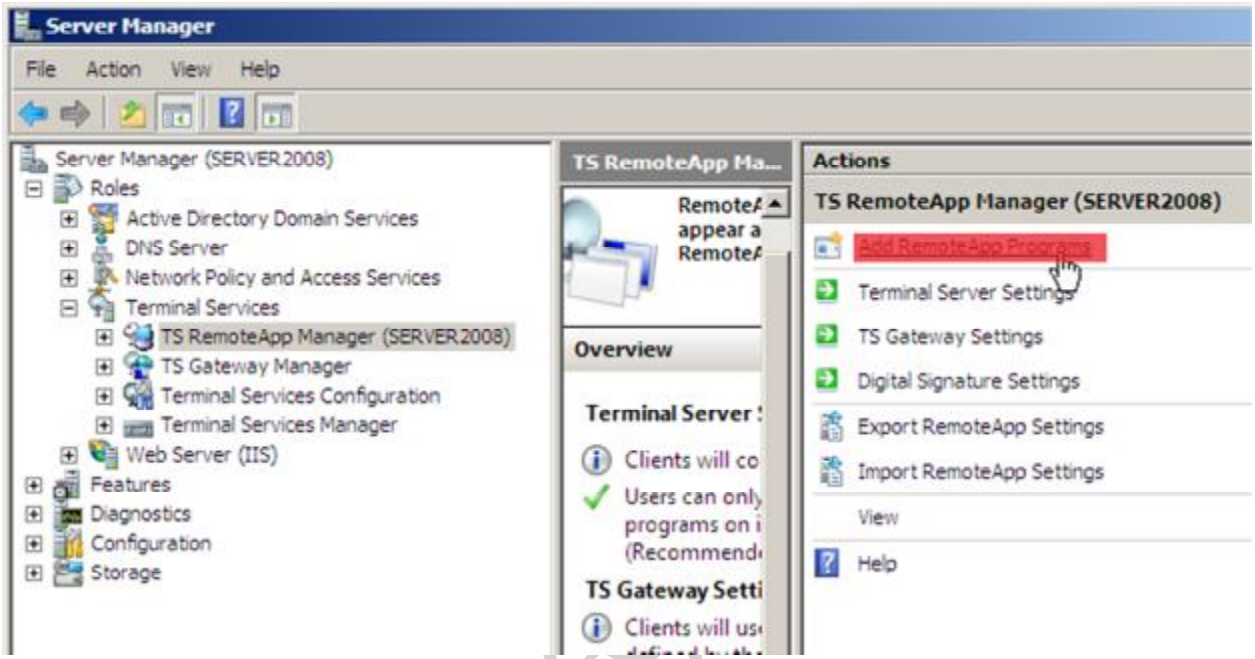
The RemoteApp Programs list is empty.

A remote desktop connection for this server is not visible in TS Web Access.
Change

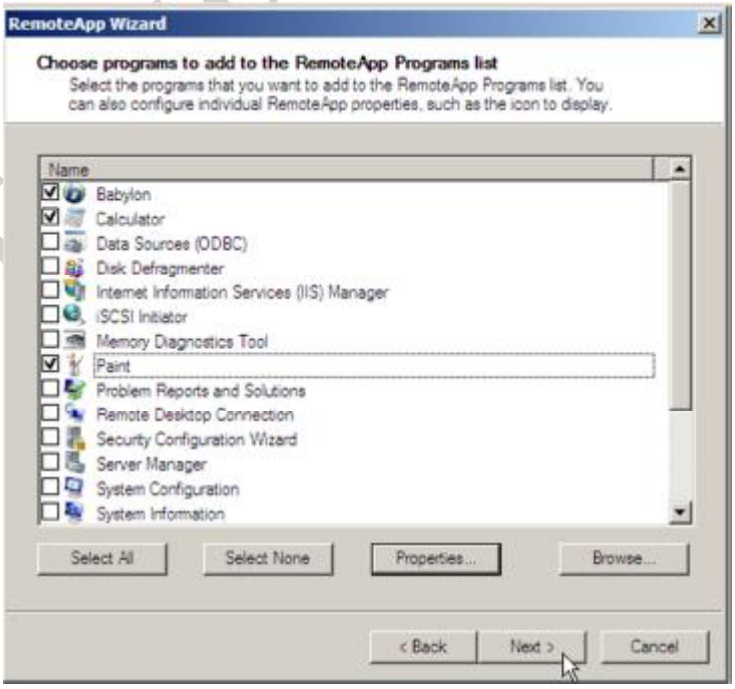
Error هم به ما می گوید هیچ نرم افزاری پشت ترمینال سرور موجود نیست

برای رفع این مشکل وارد پنل سمت راست می شویم و گزینه مورد نظر را انتخاب می کنیم

(Add Remove App Programs)

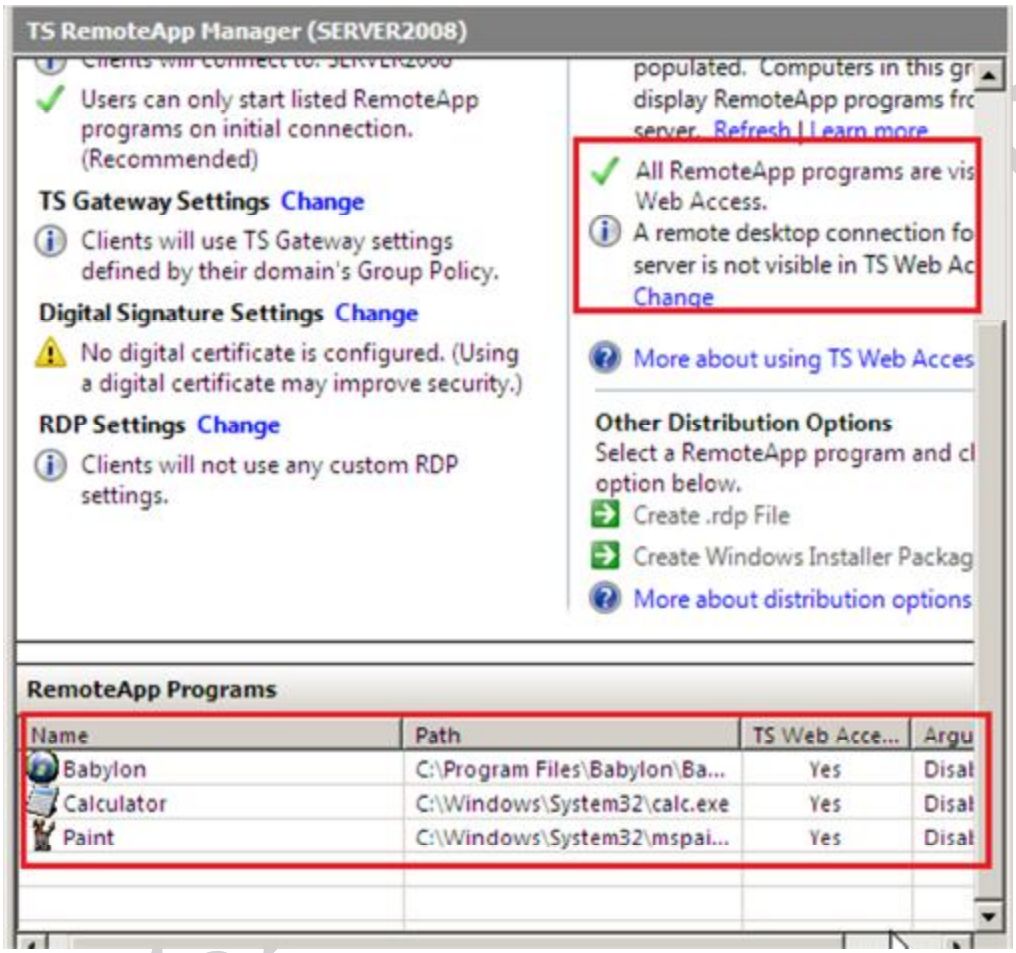



در پنجره باز شده لیستی از نرم افزارهای نصب شده بر روی سرور را نمایش می دهد




Farid

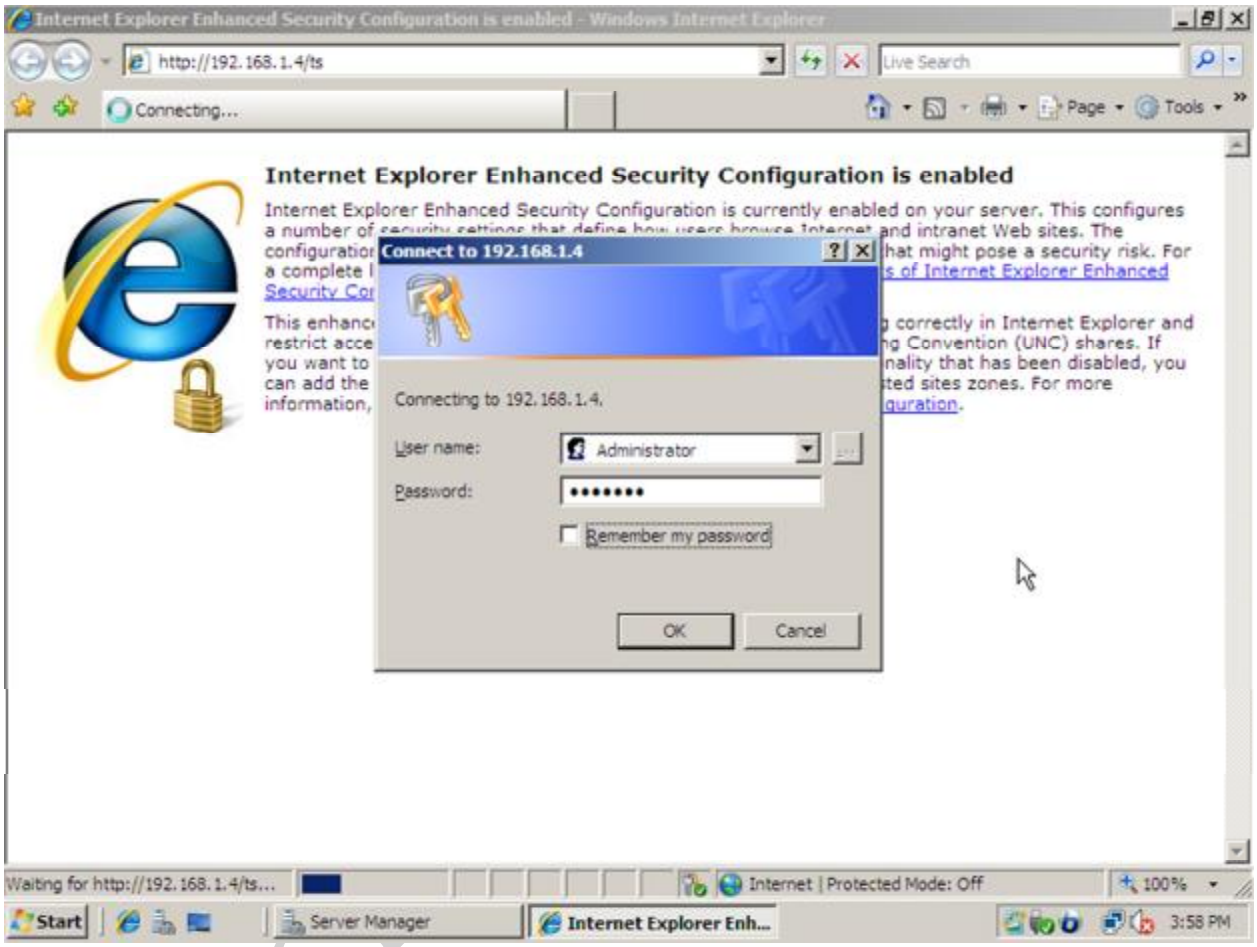
با انتخاب نرم افزارهایی که می خواهیم به اشتراک بذاریم Error هم ازبین خواهد رفت در آخر هم لیستی از نرم افزارهای انتخابی را به ما نشان می دهد.




برای اینکه بتوانیم از شبکه داخلی به TS دسترسی داشته باشیم Browser را باز می کنیم و درآن http:// 192.168.1.4/ts را تایپ می کنیم اگر از بیرون بخواهیم وصل شویم باید https:// و آی پی پابلیک را وارد کنیم.

- Ip Server, 192.168.1.4

در هنگام وصل شدن از ما یوزر و پسورد می خواهد که می توانیم از یوزرهای اضافه شده در گروه مورد نظرمان استفاده کنیم.

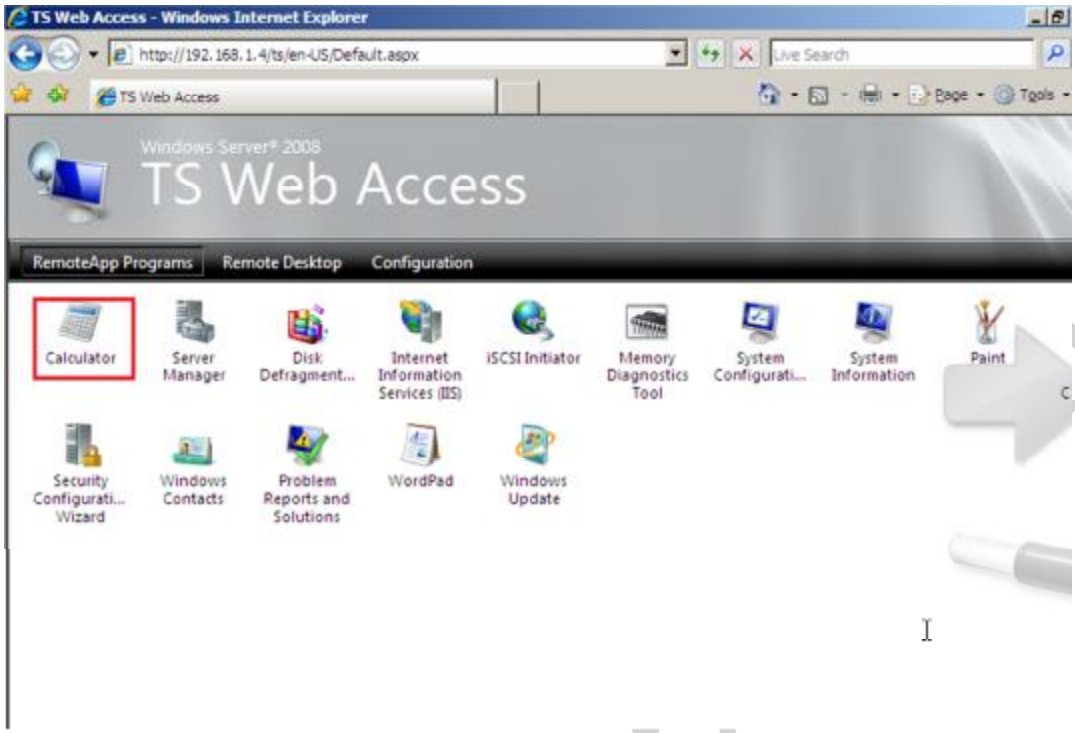


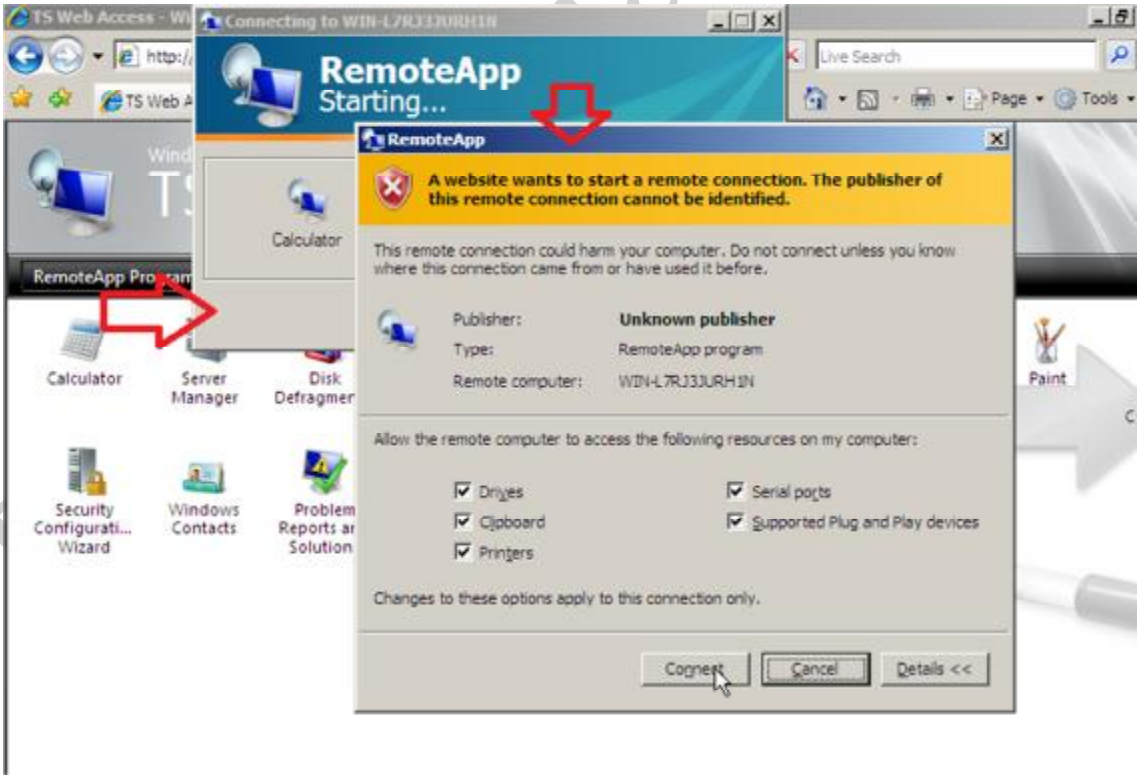

و سپس TS باز می شود.

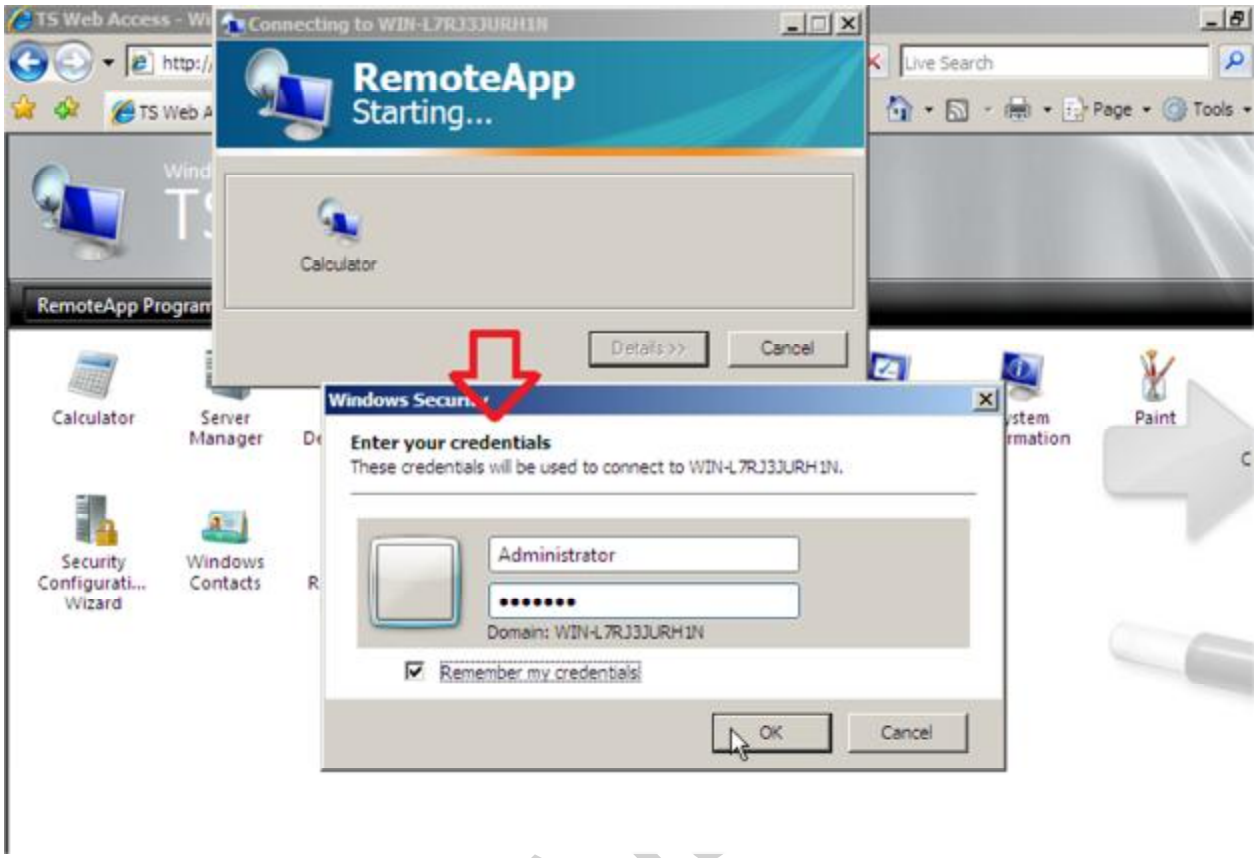
در اینجا می خواهیم ماشین حساب را اجرا کنیم.

در شکل2 از ما سوال می کند که می خواهی Driver,Clipboard و... بین شما و TS یکی شود؟

Fars

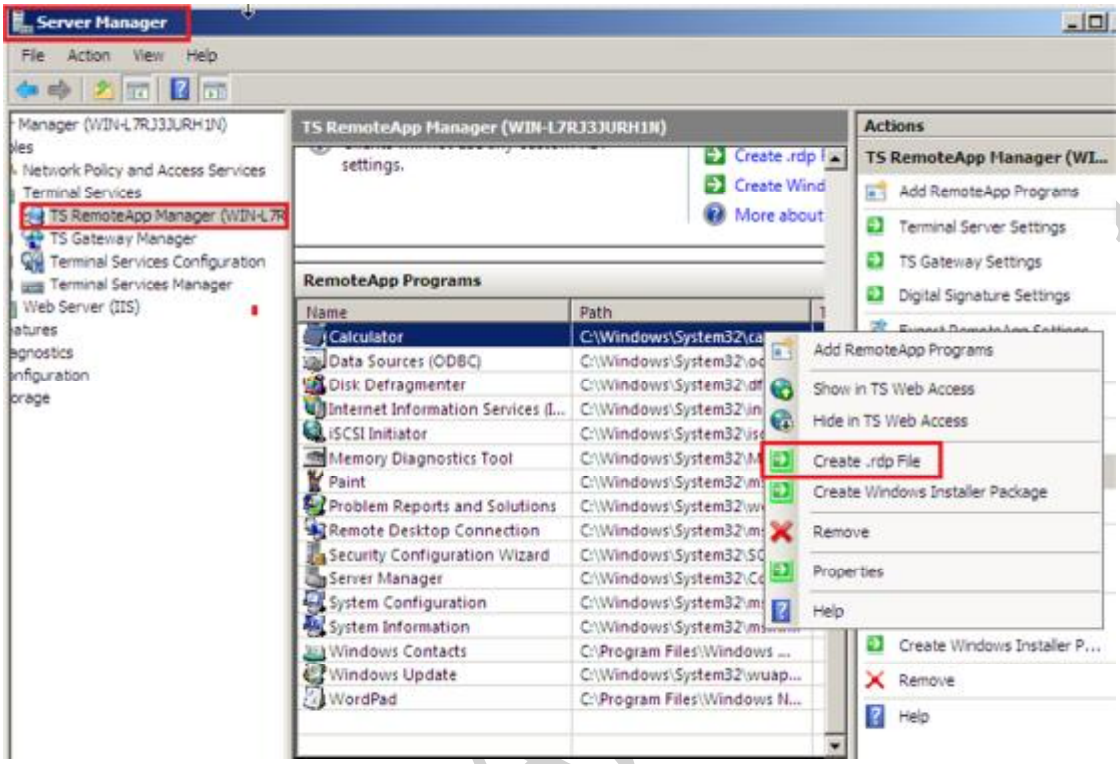

TS Web Access - Windows Internet Explorer
http://192.168.1.4/ts/en-US/Default.aspx
TS Web Access
Windows Server® 2008
TS Web Access
RemoteApp Programs
Remote Desktop
Configuration
Calculator
Server Manager
Disk Defragment...
Internet Information Services (IIS)
iSCSI Initiator
Memory Diagnostics Tool
System Configurati...
System Information
Paint
Security Configurati... Wizard
Windows Contacts
Problem Reports and Solutions
WordPad
Windows Update

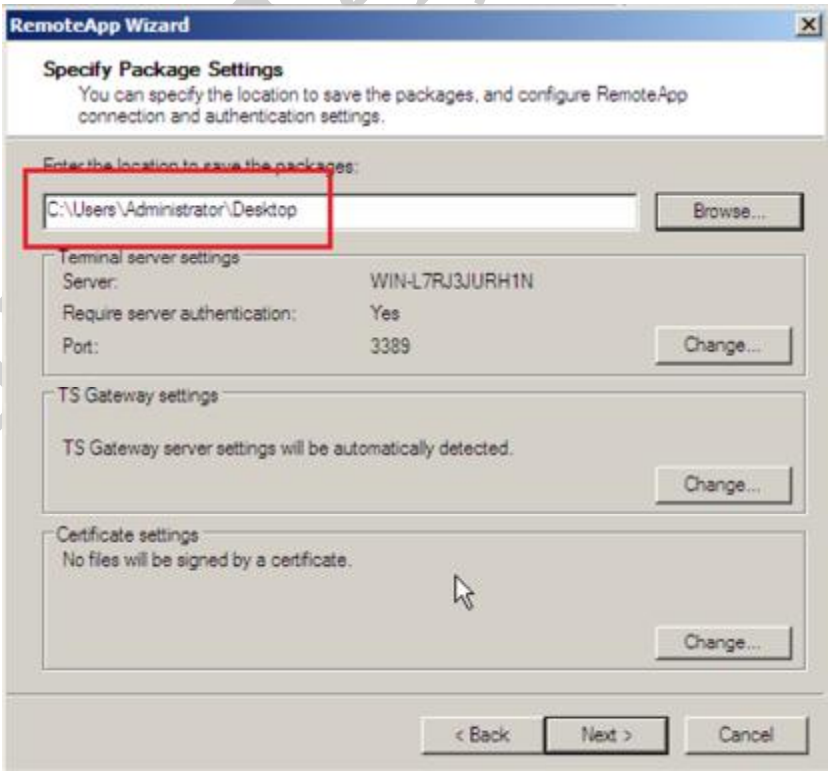

Connecting to WIN-L7RJ3JURH1N
RemoteApp
Starting...
RemoteApp
A website wants to start a remote connection. The publisher of this remote connection cannot be identified.
This remote connection could harm your computer. Do not connect unless you know where this connection came from or have used it before.
Publisher: Unknown publisher
Type: RemoteApp program
Remote computer: WIN-L7RJ3JURH1N
Allow the remote computer to access the following resources on my computer:
Drives
Clipboard
Printers
Serial ports
Supported Plug and Play devices
Changes to these options apply to this connection only.
Connect
Cancel
Details <<
Calculator
Server Manager
Disk Defragmer
Security Configurati... Wizard
Windows Contacts
Problem Reports ar Solution
Paint



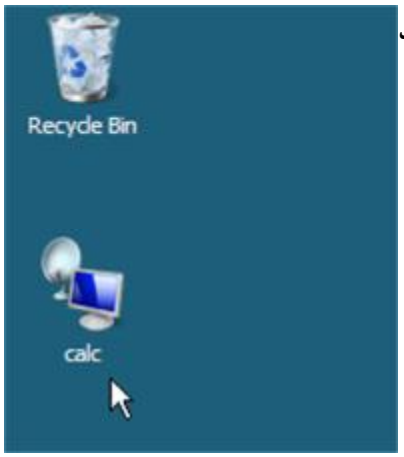
**برای اولین بار طول می کشد تا نرم افزار اجرا شود.**

برای اینکه کاربران بتوانند راحت تر با نرم افزار های TS کار کنند می توانیم از آنها یک RDP فایل ( ShortCut ) برای هر نرم افزار بسازیم و در اختیار کاربران قرار دهیم.

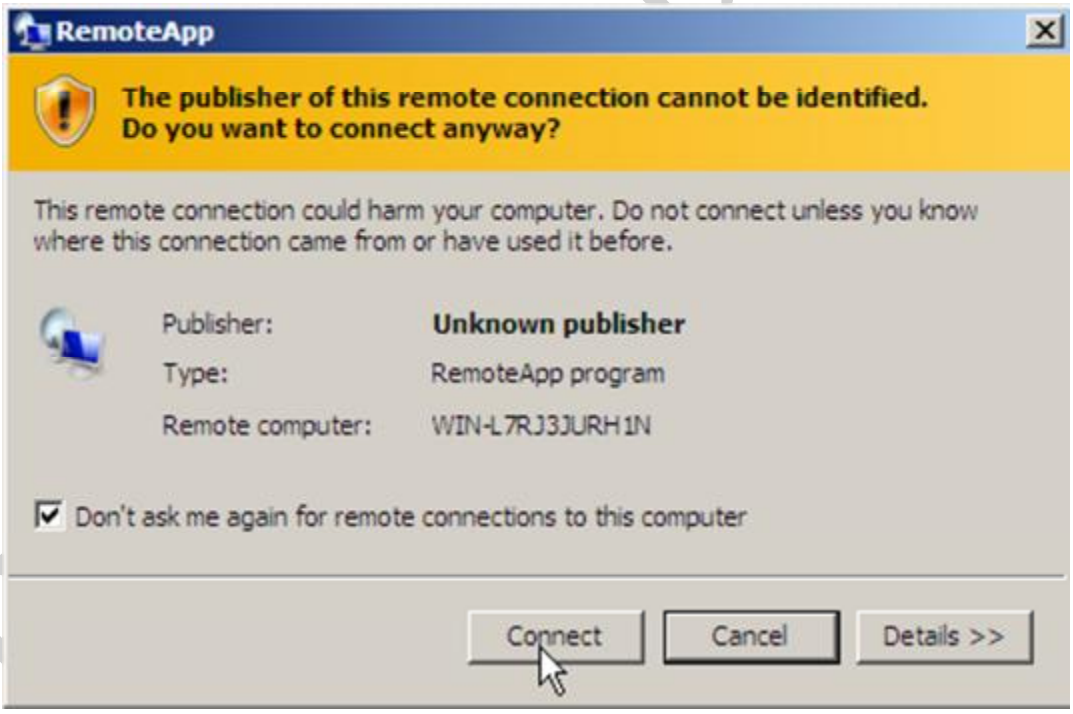


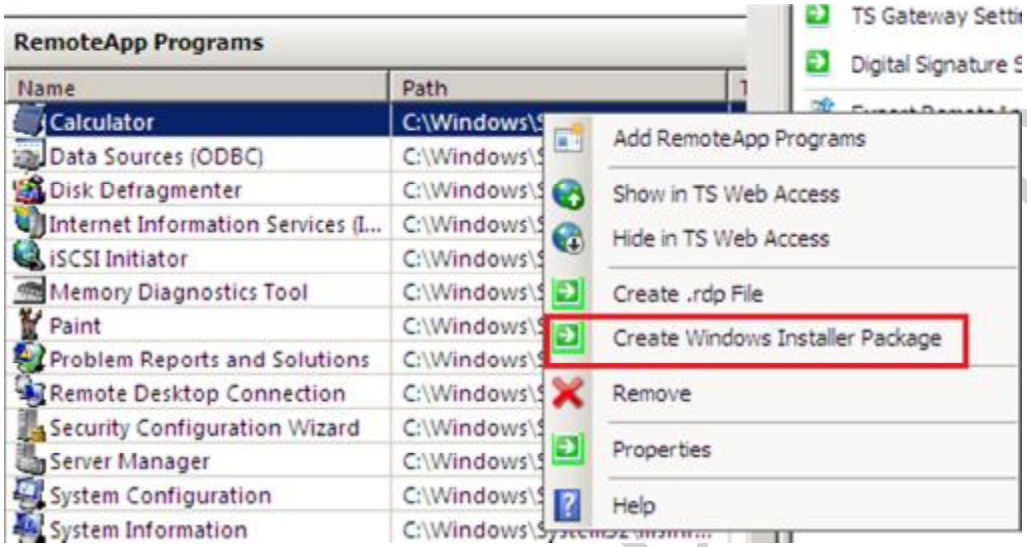
همانطور که می بینید آیکون ماشین حساب در مسیر مورد نظر ساخته شد

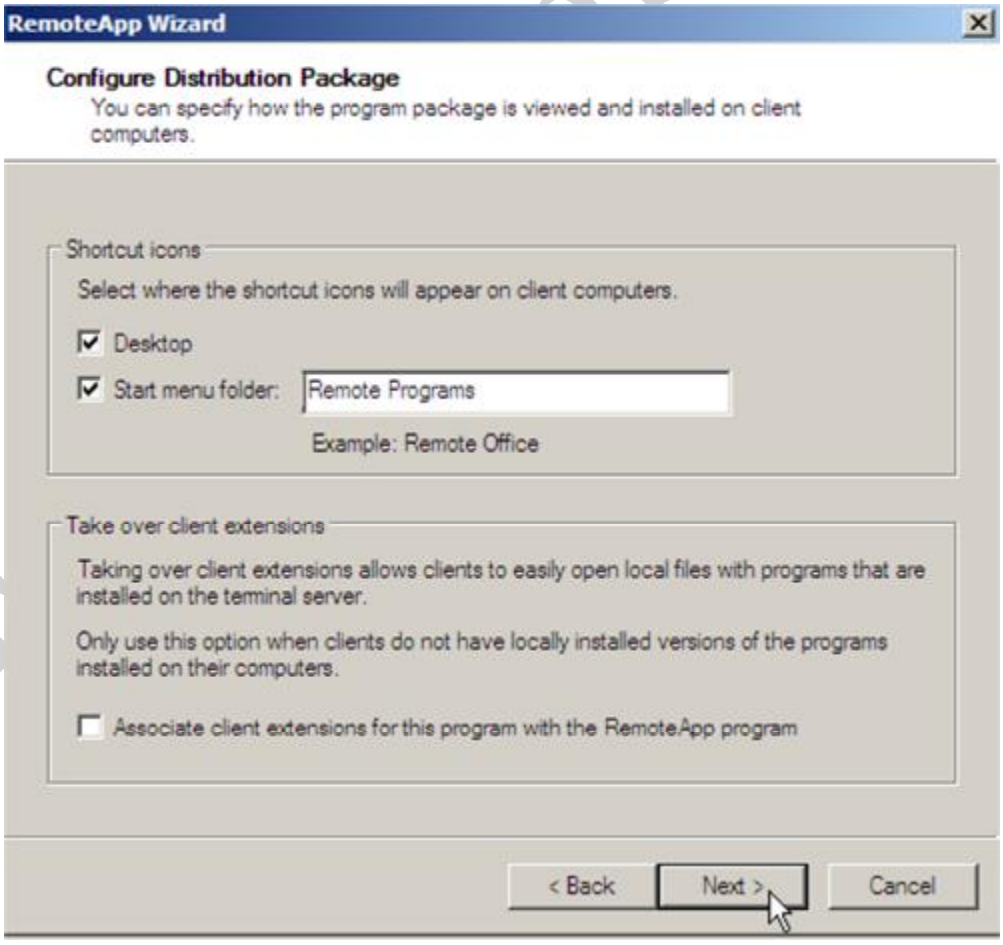



وقتی برای اولین بار آن را باز می کنیم با پیغام زیر مواجه می شویم



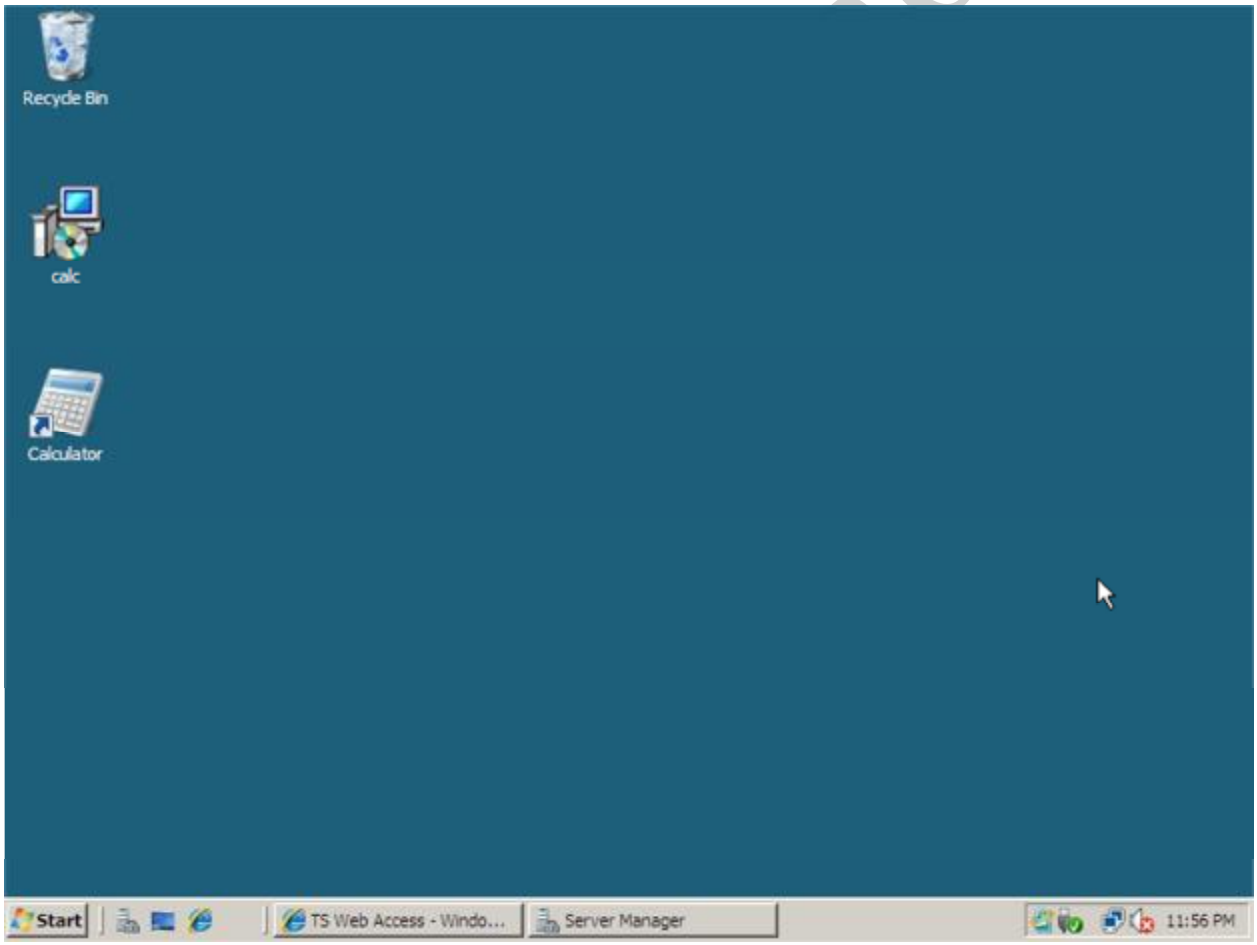
حتی می توانیم از روی نرم افزارهای TS فایل نصبی برای کاربرانمان تهیه کنیم و آنها بعد از نصب از آن نرم افزار ها استفاده کنند درحقیقت نرم افزار باز از روی TS خوانده می شود و فقط کاربران دیگر مراحل قبلی را برای استفاده نروم افزار TS طی نمی کند.



در شکل دوم(بالا)گزینه Desktop را هم انتخاب می کنیم تا بعد از نصب ShortCut را هم در دسکتاپ ببینیم.

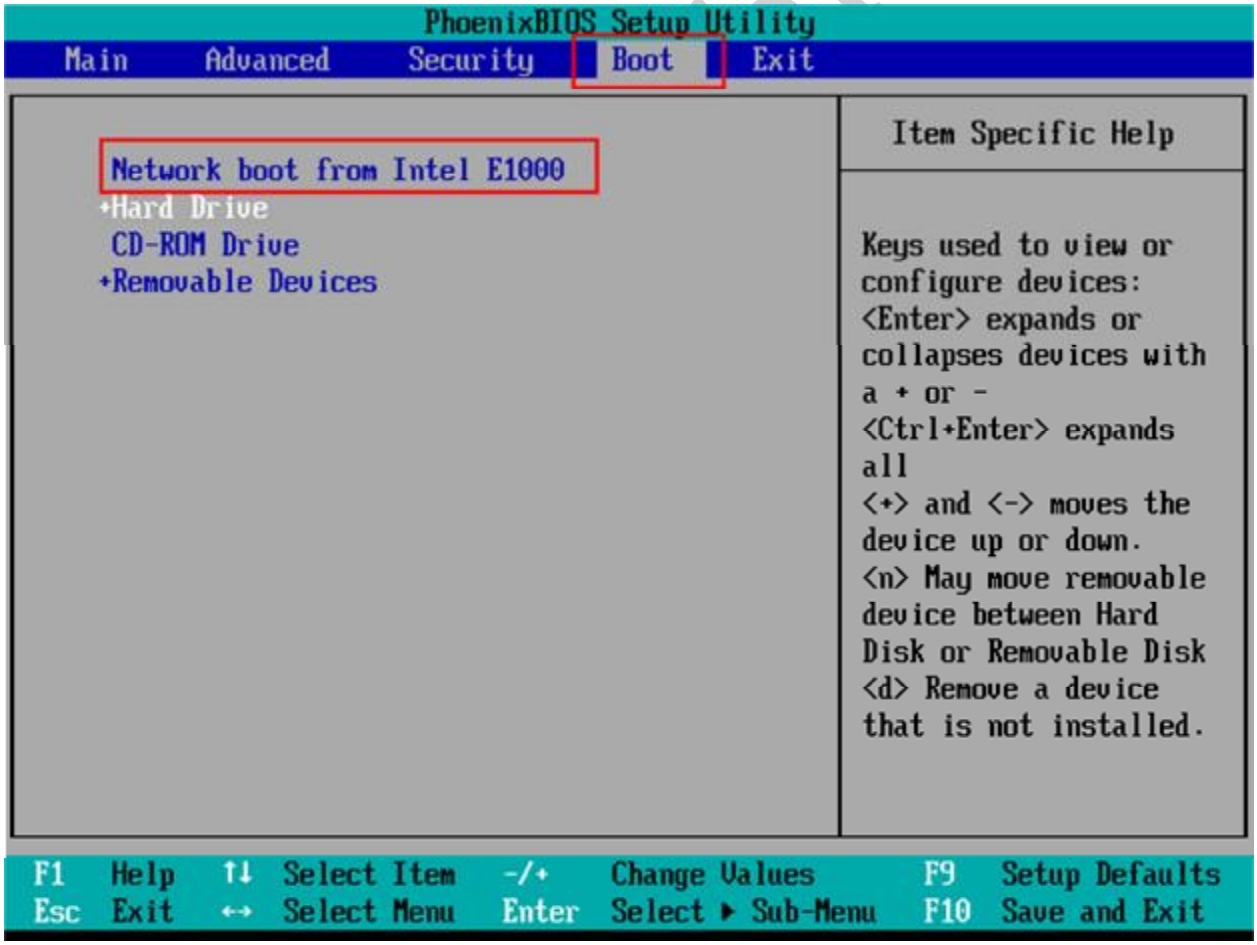
در شکل پایین فایل نصبی هم بر روی دسکتاپ ساخته شد بعد از نصب مانند شکل چهارم می توانیم از ماشین حساب استفاده کنیم



## WDS ( Windows Deployment Server )

کار این سرور راحت تر کردن نصب مکرر سیستم عامل ها بر روی بستر شبکه است,ویندوزهای Vista, 7, Xp , 2008, 2003 را می توان توسط WDS در شبکه نصب کرد.

- برای راه اندازی سرور WDS احتیاج به پیش نصب هایی از قبیل DHCP–DNS–Active Directory
- تمامی کارت شبکه های کلاینت ها باید PXE SUPPORT باشند.
- به کارت شبکه هایی که دارای ROM بوده و توانایی Boot شدن از طریق شبکه را دارند PXE SUPPORT گویند.
- برای اینکه متوجه شویم کارت شبکه ما دارای قابلیت PXE SUPPORT می باشد یا نه وارد قسمت Boot سیستم می شویم و اگر کارت شبکه ما در آن قسمت وجود داشت این قابلیت را ساپورت می کند.
- برای نصب ویندوز از طریق شبکه باید از Image ویندوز استفاده کرد.



کاربردهای DHCP–DNS–Active Directory در WDS

1) کلاینتی که ویندوز ندارد زمانی که روشن می شود کارت شبکه آن به دنبال Ip گرفتن از DHCP می باشد.
2) بعد از گرفتن Ip, از DNS شبکه می پرسد WDS شبکه کیست و DNS هم WDS شبکه را به آن معرفی می کند.
3) سرور WDS برای اینکه متوجه شود باید به چه کامپیوتری ویندوز بدهد از اکتیو دایرکتوری سوال می کند.

انواع Image قابل استفاده در WDS

1) Boot Image:Image که قابلیت اتصال به شبکه ودیدن Image های پشت WDS را به کلاینت ها می دهد(بودن این Image اجباری می باشد)
2) Capture Image : به Image که خود کلاینت از خودش به همراه تمامی نرم افزارهایش می گیرد و پشت WDS می گذارد را Capture Image گویند, برای استفاده از این Image بر روی دیگر کامپیوتر ها بایدتمامی سخت افزارهای کلاینت ها یکی باشداگر نبود می توان از نرم افزاری به نام New sid یا ازفرمان Syspre استفاده کرد.

- هر کلاینت در شبکه دارای یک شماره منحصر به فردی به نام SID می باشد,هنگامی که از یک کلاینت Image می گیریم با همان SID خودش Image گرفته ایم زمانی که بر روی دیگر کلاینت ها نصب می کنیم با همان SID قبلی نصب می شود برای تغییر SID باید از نرم افزار یا دستور گفته شده استفاده کنیم.

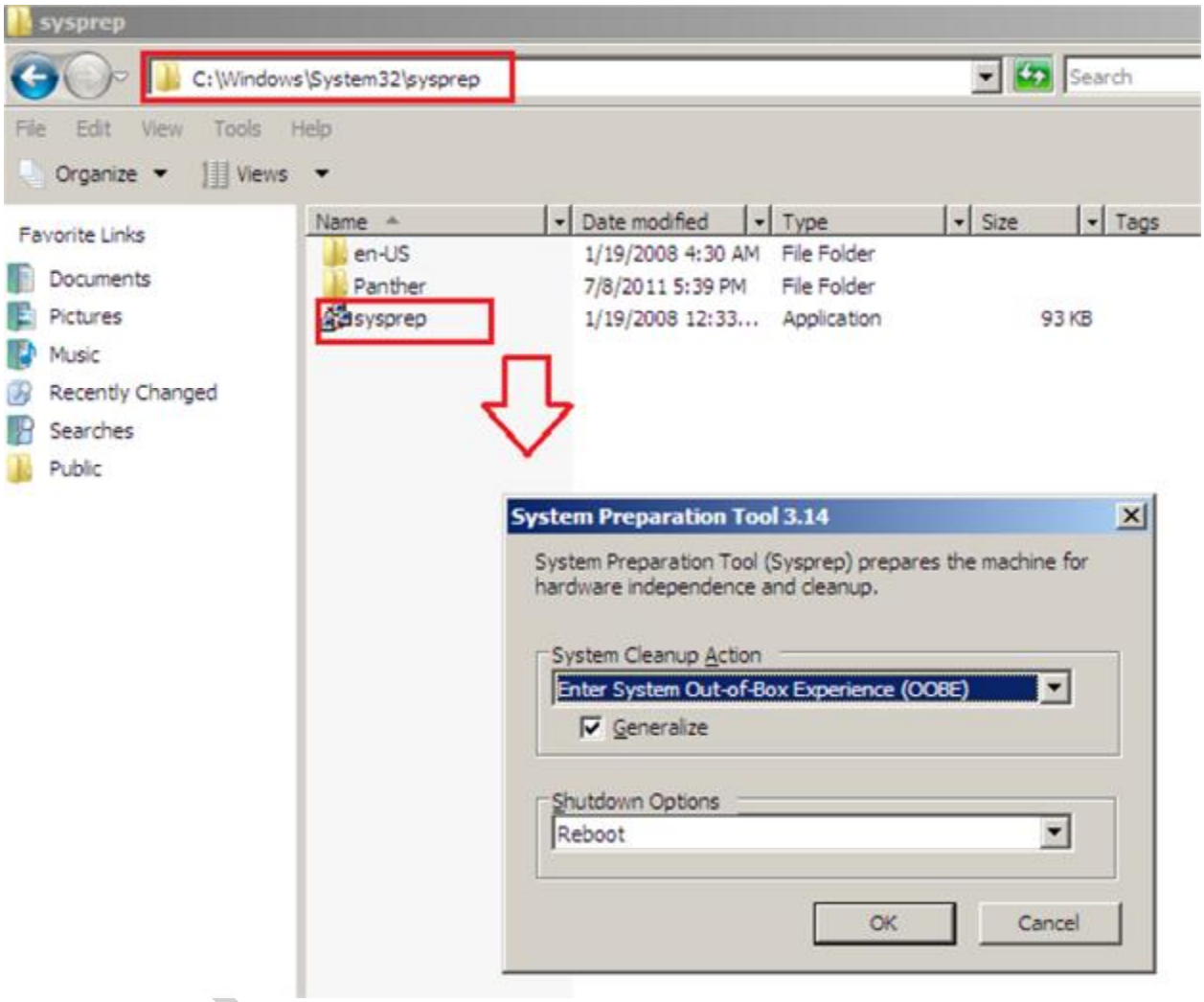
3) Custom Image : بعد از نصب ویندوز نرم افزارهای مورد نیاز را بر روی آن نصب می کنیم اگر از این ویندوز Image بگیریم به این image ویندوز,Custom Image گویند مانند ویندوزهای MRT
4) Install Image : همان CD,DVD سیستم عامل که قابلیت نصب را دارد.

- پسوند Install Image ویندوزهای Next Generation , wim می باشدوپسوند ویندوزهای Legacy ,exe وiso می باشد.
- در سرور 2008 فقط می توان ویندوزهای NG را به صورت WDS اجرا کرد برای اینکه بتوانیم از ویندوزهای Lagecy هم در 2008 استفاده کنیم باید با نرم افزار AIK(WAIK) , Image آنها(Lagecy)را به wim تبدیل کنیم .
- معادل WDS در 2003(RIS(Remote Installation Service می باشد, در 2003 بدون استفاده از AIK می توان Xp نصب کرد.

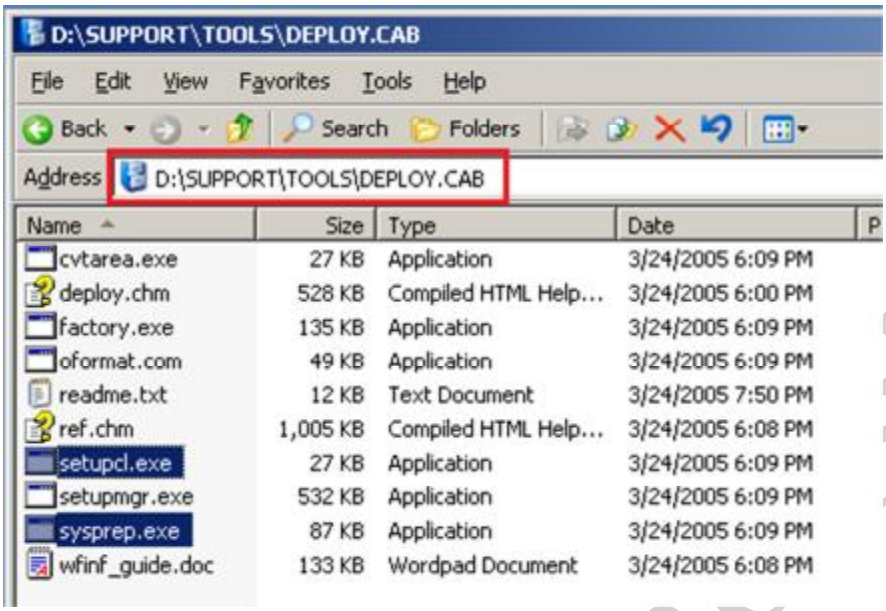
5) Discover Image : زمانی که کامپیوتری قابلیت pxe را پشتیبانی نکند از این Image استفاده می کنند طرز کار به این صورت می باشد که باید image گرفته شده(ویندوز) را از روی سرور رایت کنیم و مستقیم بر روی کلاینت مورد نظر از طریق DVD ROM آن کلاینت نصب کنیم.

FarshidAjabnoush

- اگر بخواهیم از SysPrep استفاده کنیم باید قبل از Image گرفتن از ویندوز مرجع یک بار SysPrep را اجرا کنیم و سپس از آن Image بگیریم برای این کار در ویندوزهای NG مانند شکل زیر عمل می کنیم




برای استفاده از این دستور در ویندوزهای Legacy مانند زیر عمل می کنیم




2 فایل انتخاب شده فشرده هستند باید آنها را از این حالت درآورده و سپس از آنها استفاده کنیم

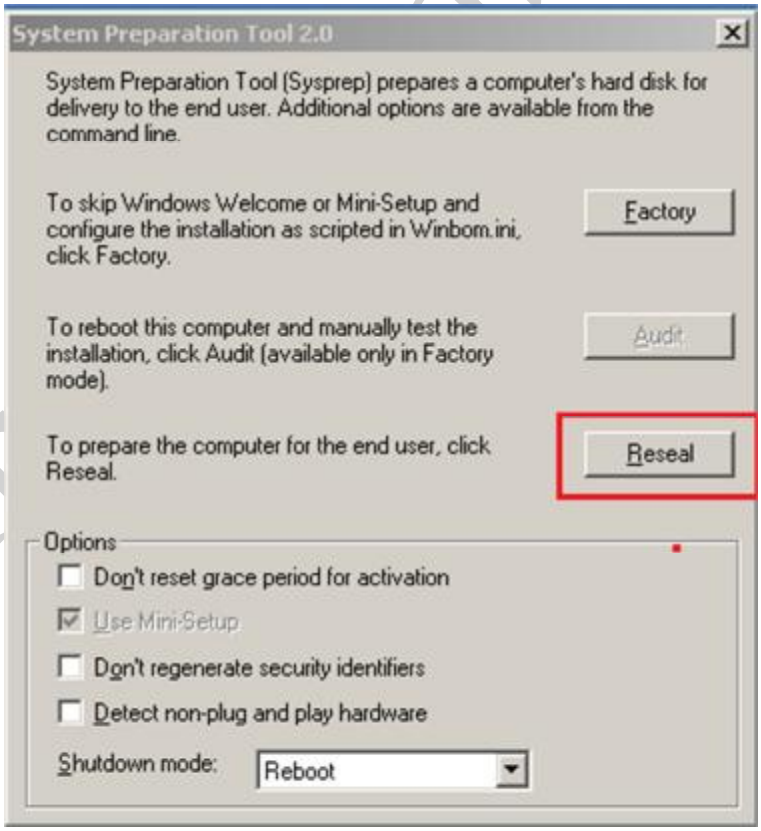


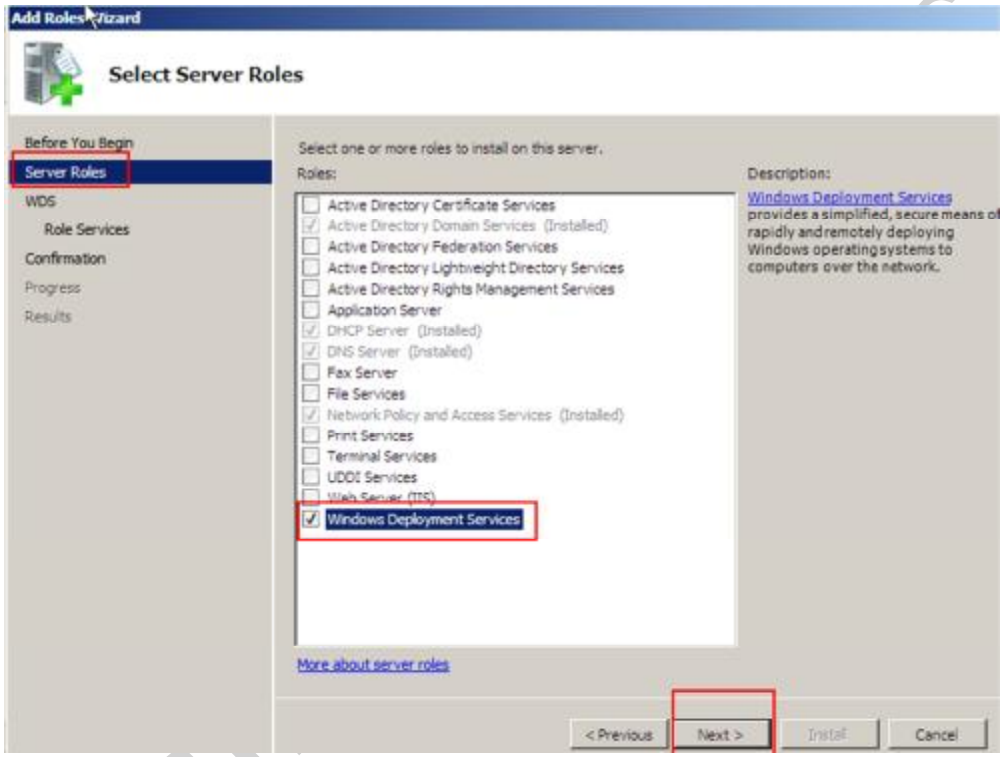

Image هایی که به این طریق گرفته می شوند زیاد خوب کار نمی کنند.

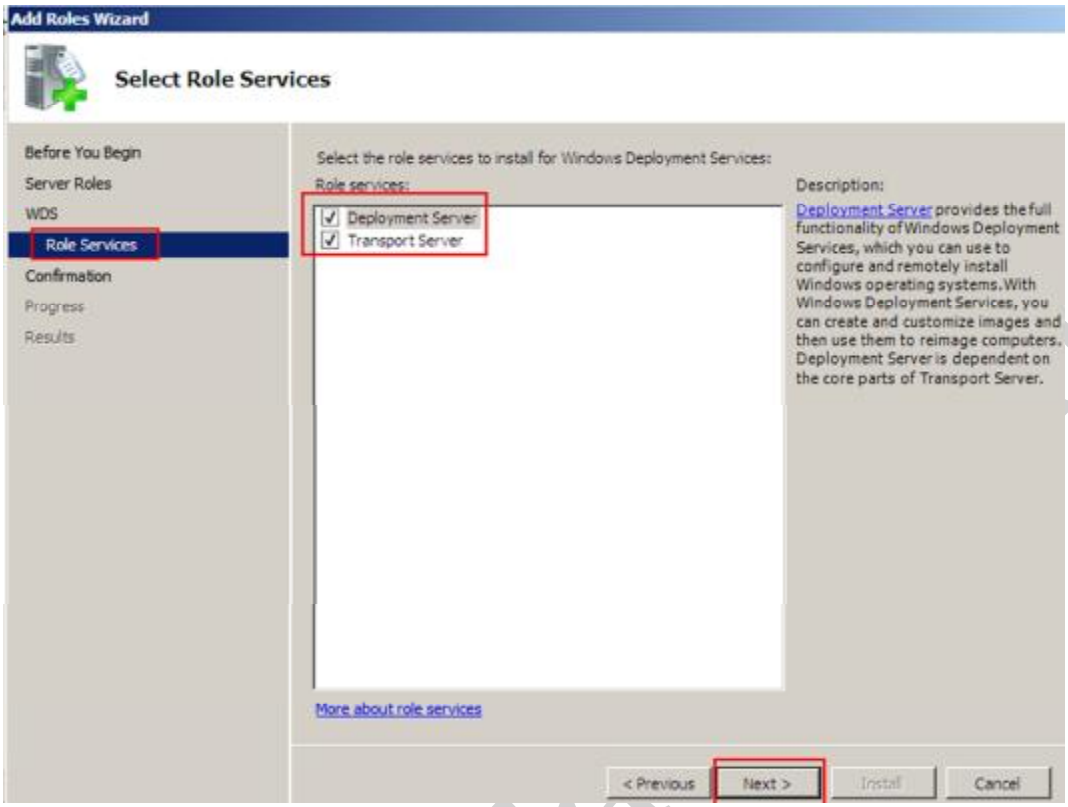
- برای استفاده از نرم افزار Newsid باید ابتدا Image گرفته شده را بر روی سیستم مورد نظر برگردانیم وسپس نرم افزار را بر روی آن سیستم اجرا می کنیم.

مراحل پیاده سازی WDS

1) نصب Active Directory و 2 DNS) نصب DHCP

بعد از انجام مراحل بالا نوبت به نصب WDS می رسدکه مانند زیر عمل می کنیم

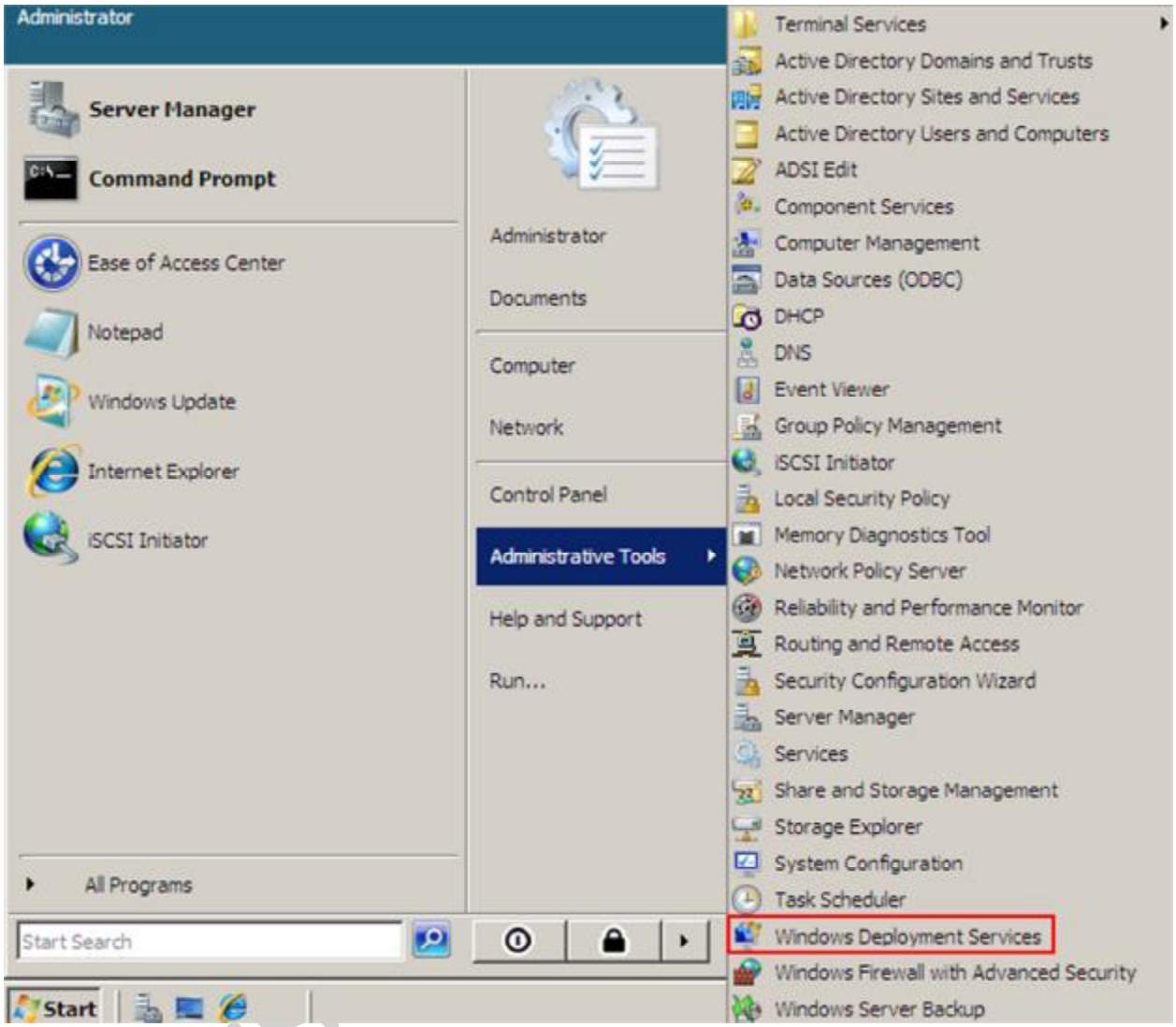





2 گزینه Deployment Server و Transport Server باید فعال باشند, Deployment باعث می شود Image ها از پشت سرور(WDS ) به پشت کلاینت ها انتقال پیدا کنند و Transport باعث می شود Image ها از پشت کلاینت ها به پشت سرور انتقال پیدا کنند.

FarshidAja

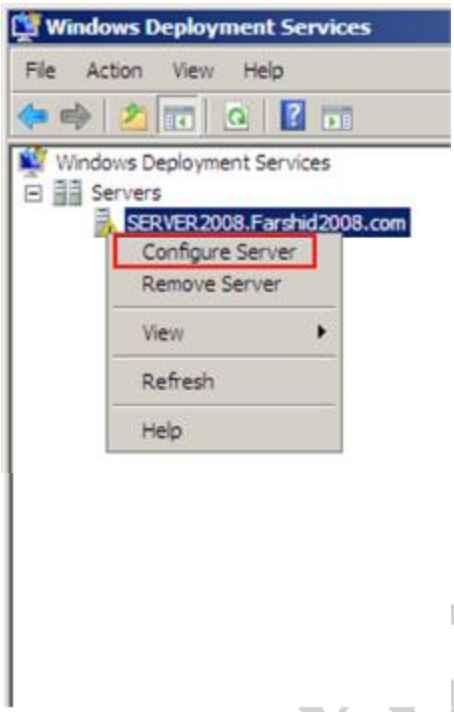
**بعد از نصب باید وارد کنسول آن بشویم**



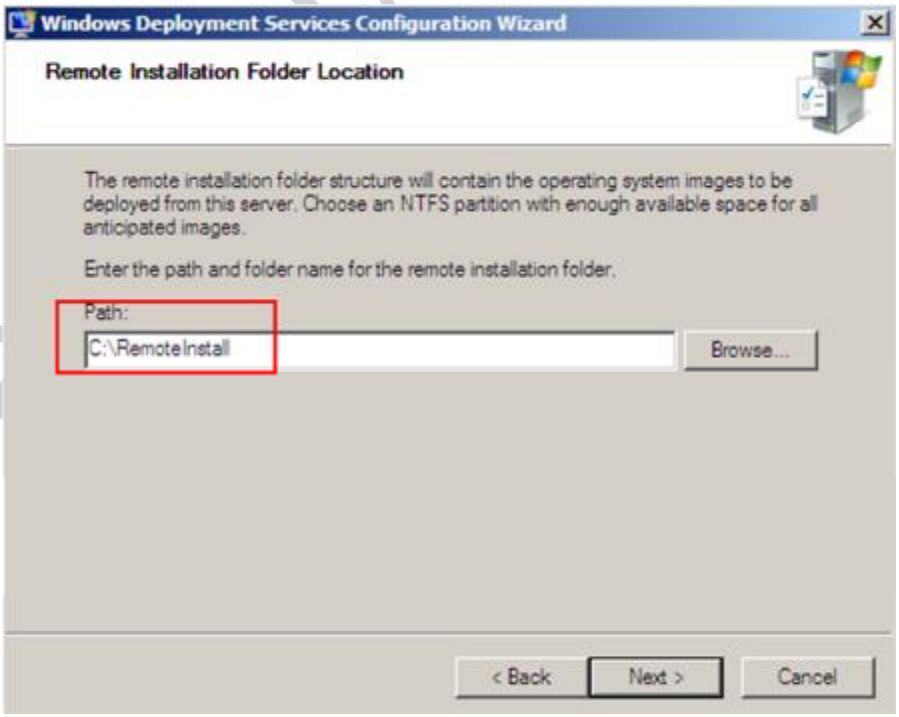

**قبل از تنظیمات باید یک اسکوپ در DHCP در رنج شبکه داشته باشیم سپس باید WDS را تنظیم کنیم**

**علامت زرد رنگ در شکل زیر به این دلیل است که هنوز WDS تنظیم نشده است.**

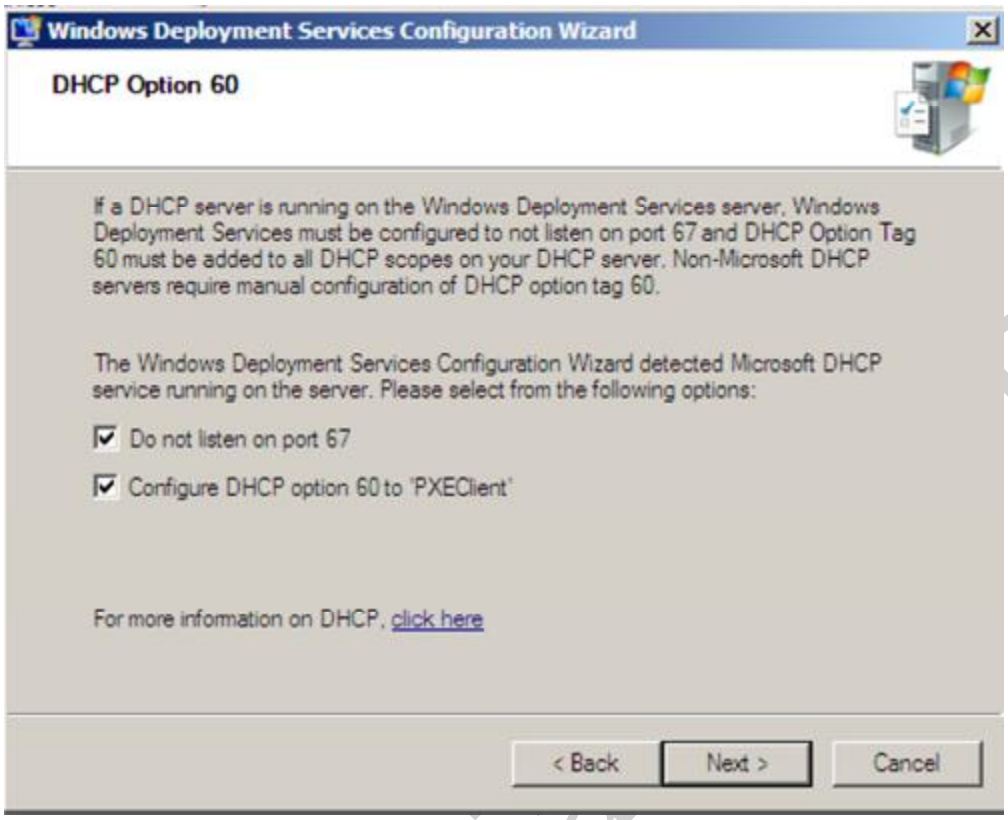
Fars




در مرحله بعد محل ذخیره سازی Image ها را از ما می پرسد,بصورت پیش فرض در C می باشد که باید محل آن را عوض کنیم.




Farshid Ajabroush

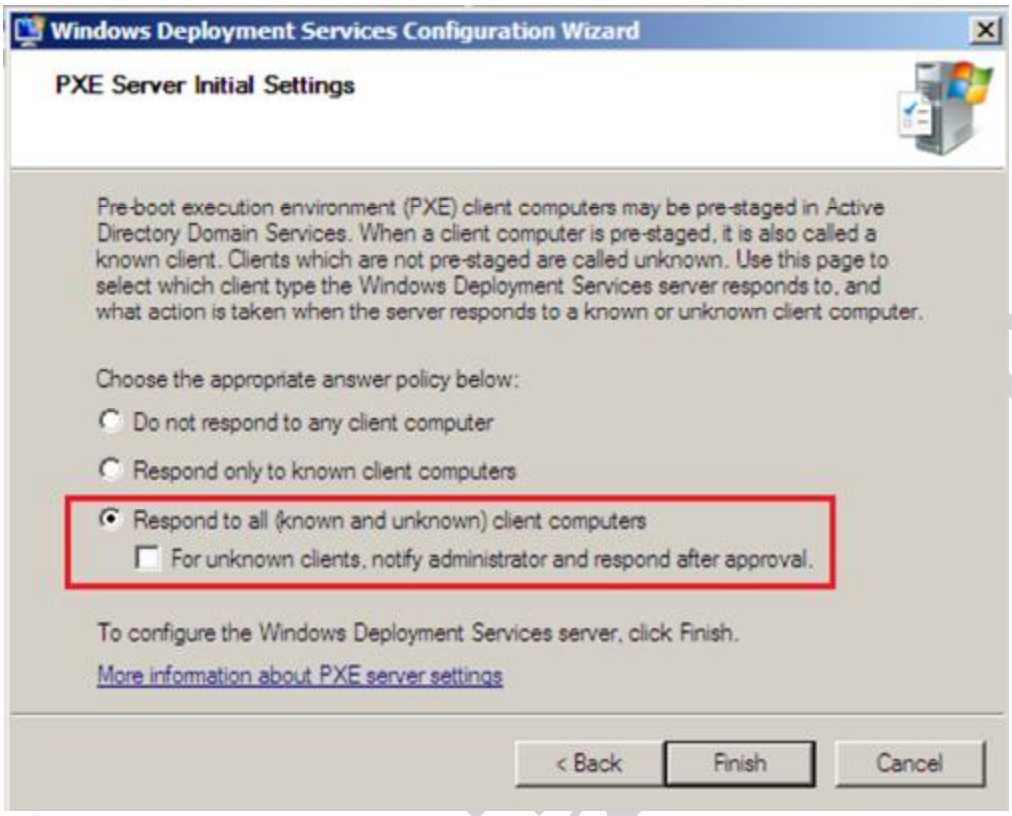



DHCP وWDS هر 2 بر روی یک پورت(67) کار می کنند,در شبکه2 سرویس نمی توانند بر روی یک پورت باشند اگر DHCP وWDS بر روی یک سرور باشند باید 2 گزینه بالا فعال باشند,گزینه اول می گوید WDS بر روی پورت67 کار نکند و گزینه2 می گوید DHCP بر روی پورت 67 کار کند.

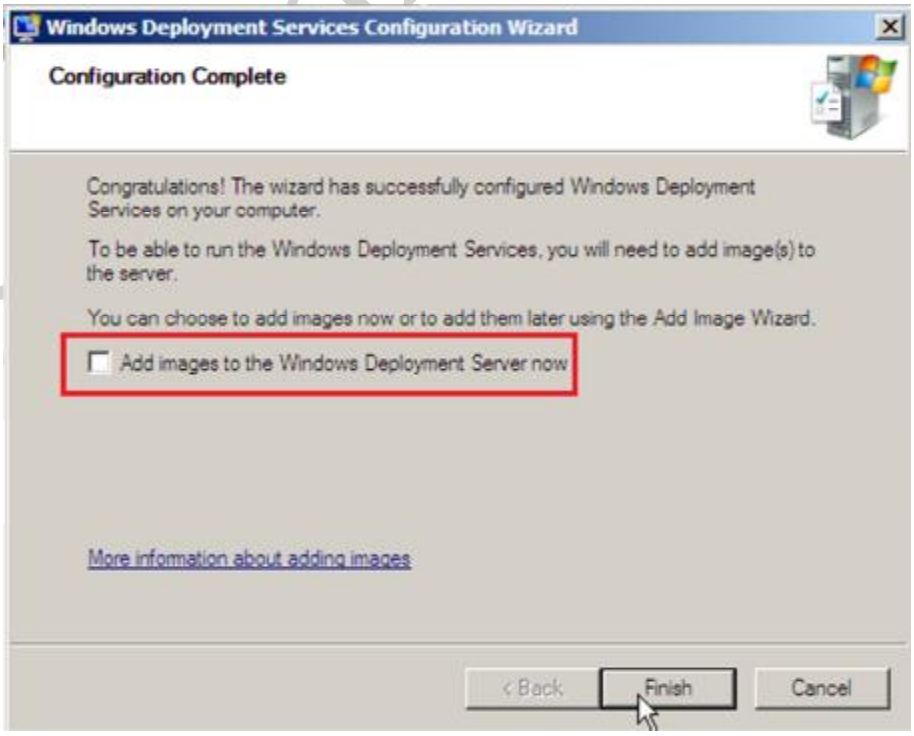
- زمانی 2 گزینه بالا را فعال می کنیم که DHCP وWDS هر2 بر روی یک سرور باشند.

در مرحله بعد از می پرسد به چه کسانی اجازه نصب ویندوز را از روی این سرور بدهم(Known سیستم هایی که Join هستند, Unknown سیستم هایی که Join نیستند) گزینه3 مناسب ترین گزینه است چون وقتی سیستم جدیدی را خریداری می کنیم قبلاً به شبکه ما Join نبوده ,پس Unknown می باشد گزینه آخر هم می گوید برای Unknown ها به من اطلاع بده.

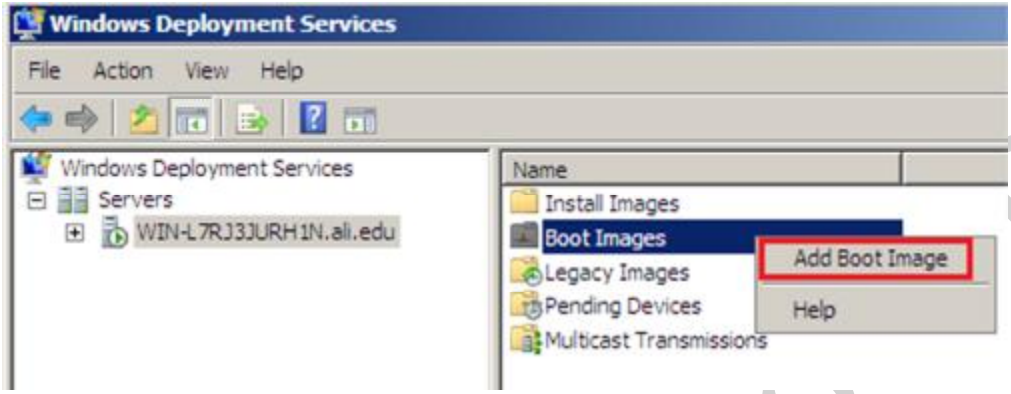
FarshidAjam



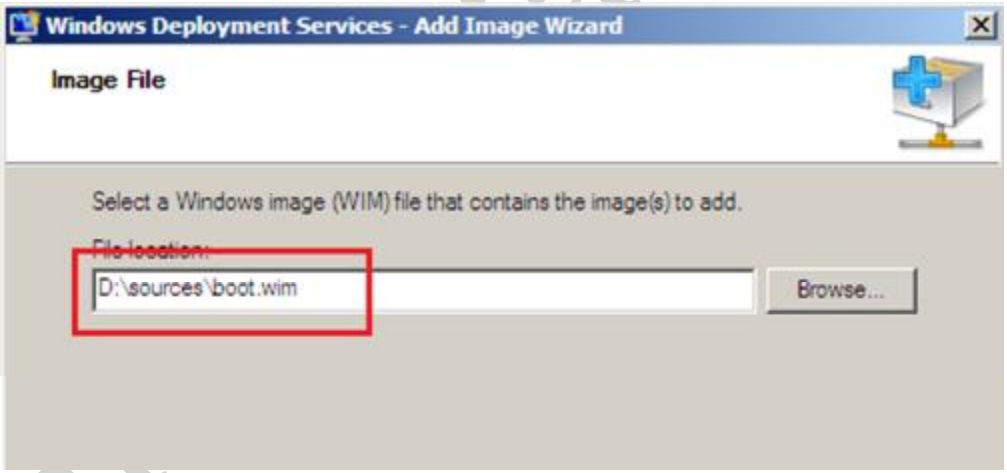

**در مرحله بعد اگر این گزینه فعال باشد با زدن3 Next تمامی Image ها اضافه می شود ولی در اینجا ما این گزینه را فعال نمی کنیم چون باید مرحله به مرحله آموزش دهیم.**



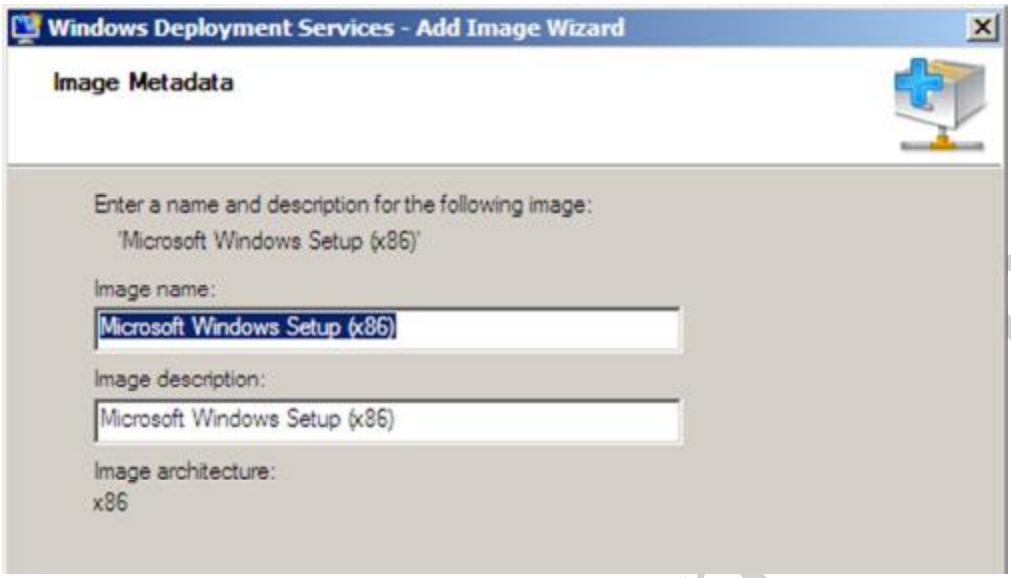
اولین کار اضافه کردن BootImage می باشد برای این کار DVD 7 را می گذاریم



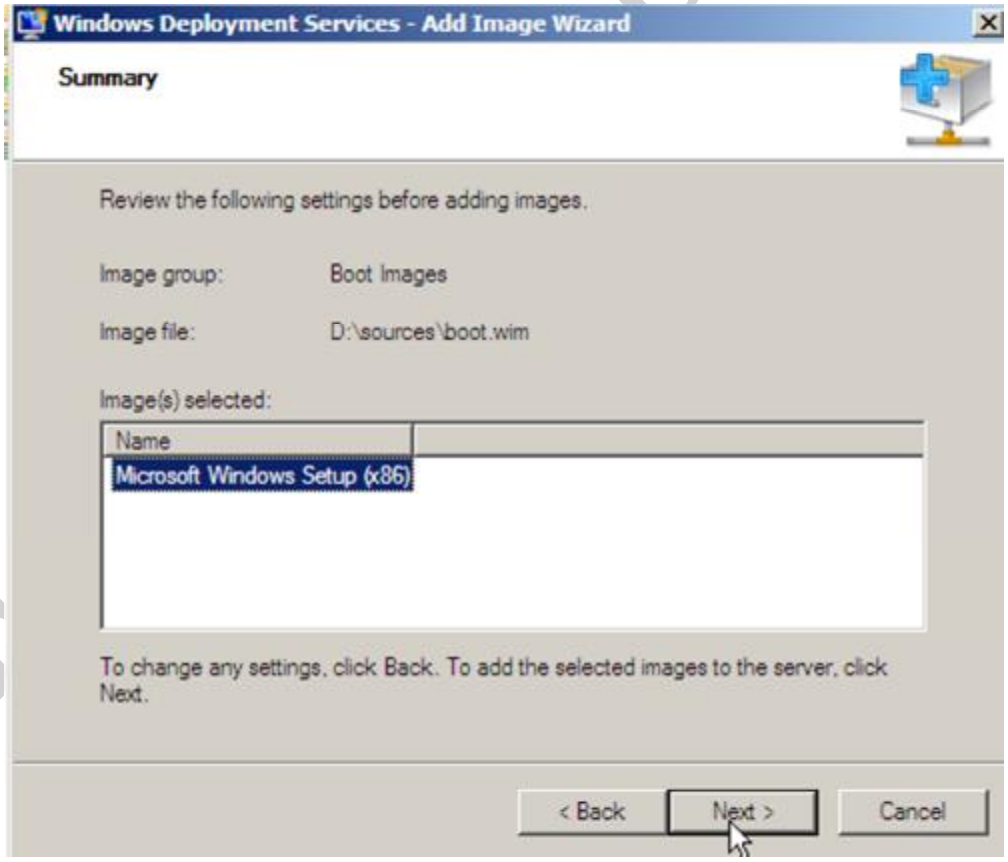

در اینجا از ما منبع ویندوز را می خواهد



اسم Image را وارد می کنیم



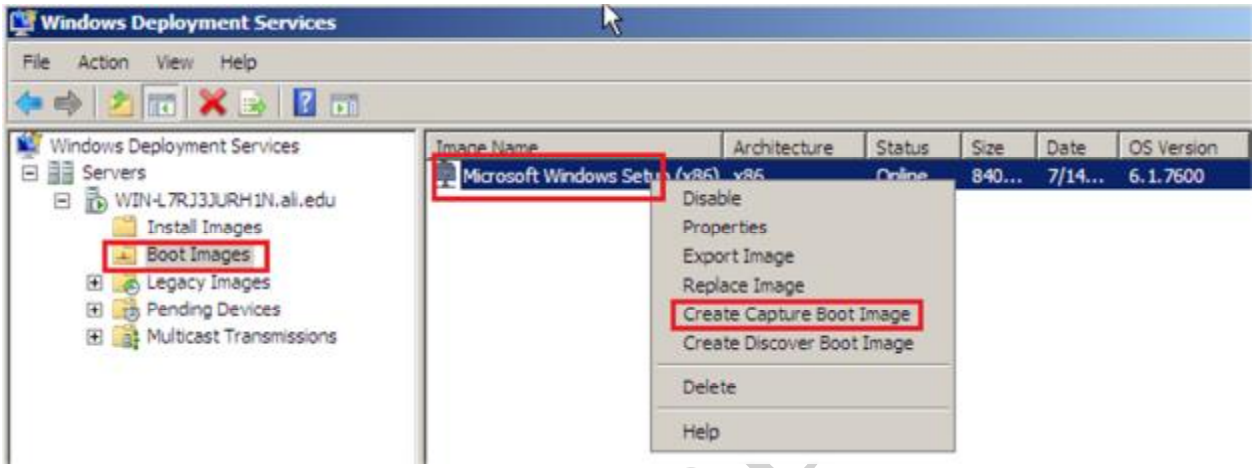

مراحل نصب طی می شود



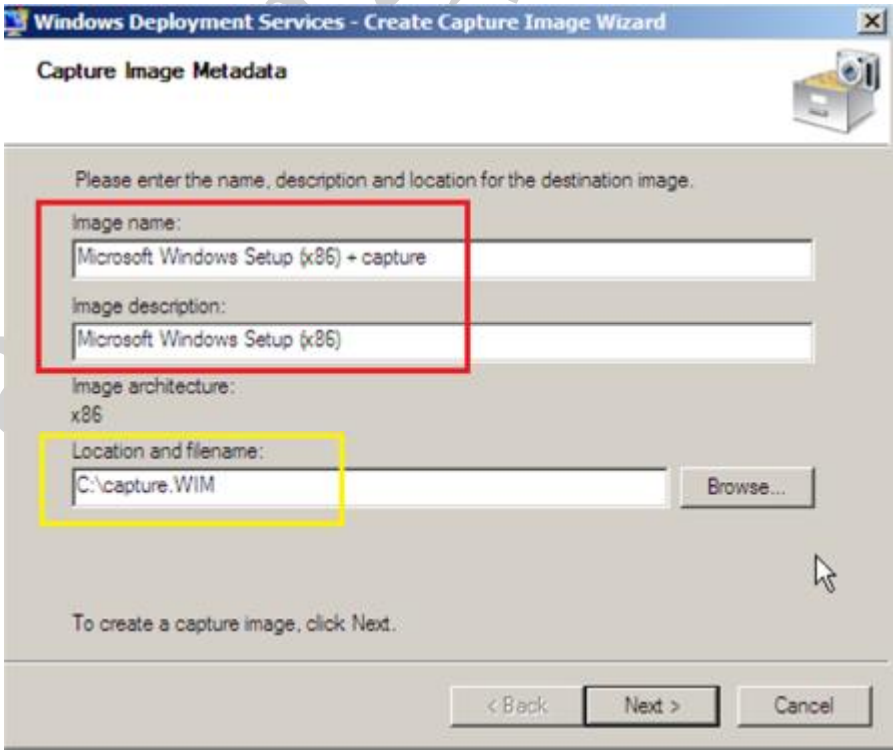
- اگر بخواهیم از XP استفاده کنیم ابتدا باید از XP فایل ISO تهیه کنیم سپس با استفاده از نرم افزار AIK آن را تبدیل به WIM. کنیم سپس بقیه مراحل.

ساختن Capture Image

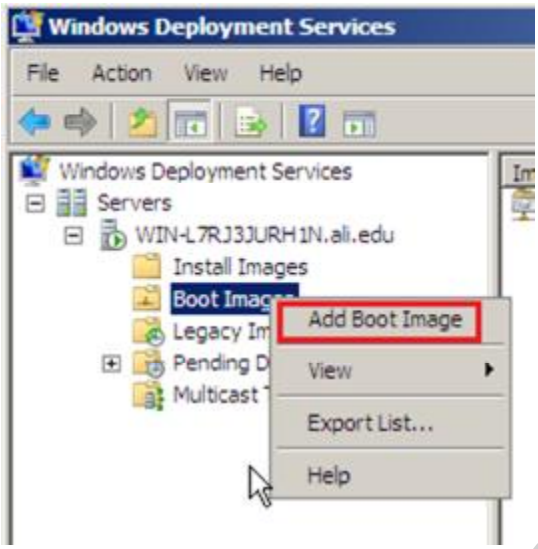
ابتدا وارد Image که ساخته ایم می شویم وسپس گزینه Capture Image



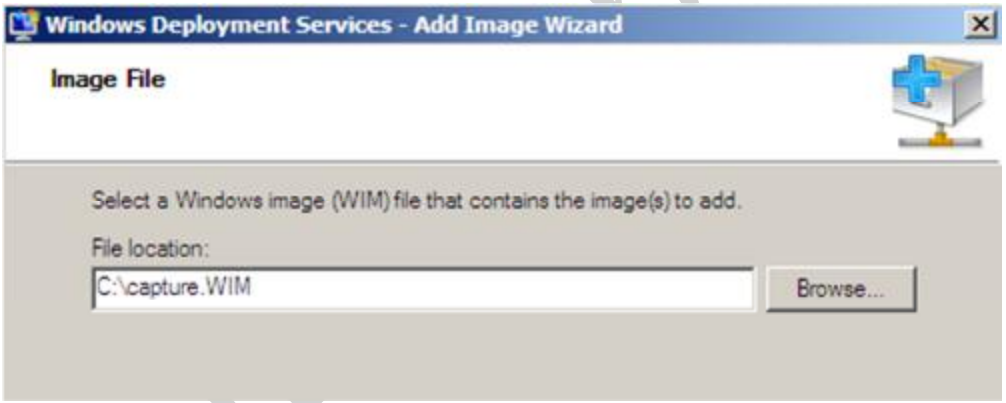

در اینجا باید اسم و محل ذخیره سازی را مشخص و در آخر هم ساخته می شود




اضافه کردن Capture Image ساخته شده به WDS




سپس وارد محل ذخیره سازی Image می شویم

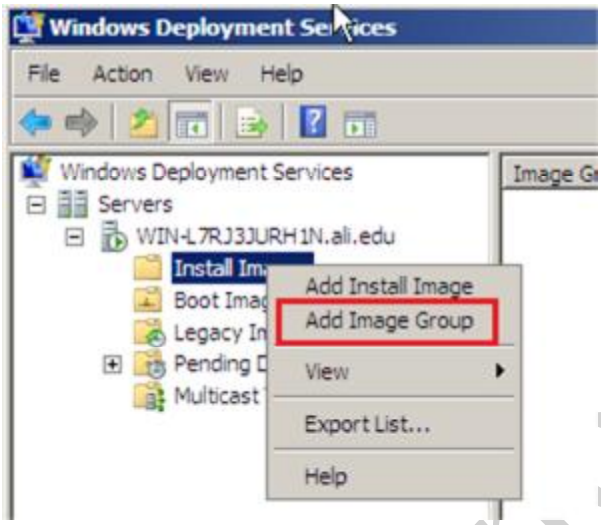



و Image اضافه می شود.

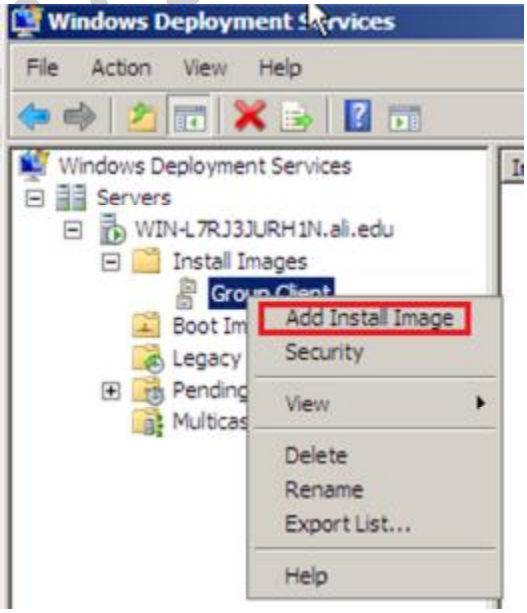
Farsiboush

اضافه کردن Install Image

برای این کار ابتدا باید گروه بسازیم



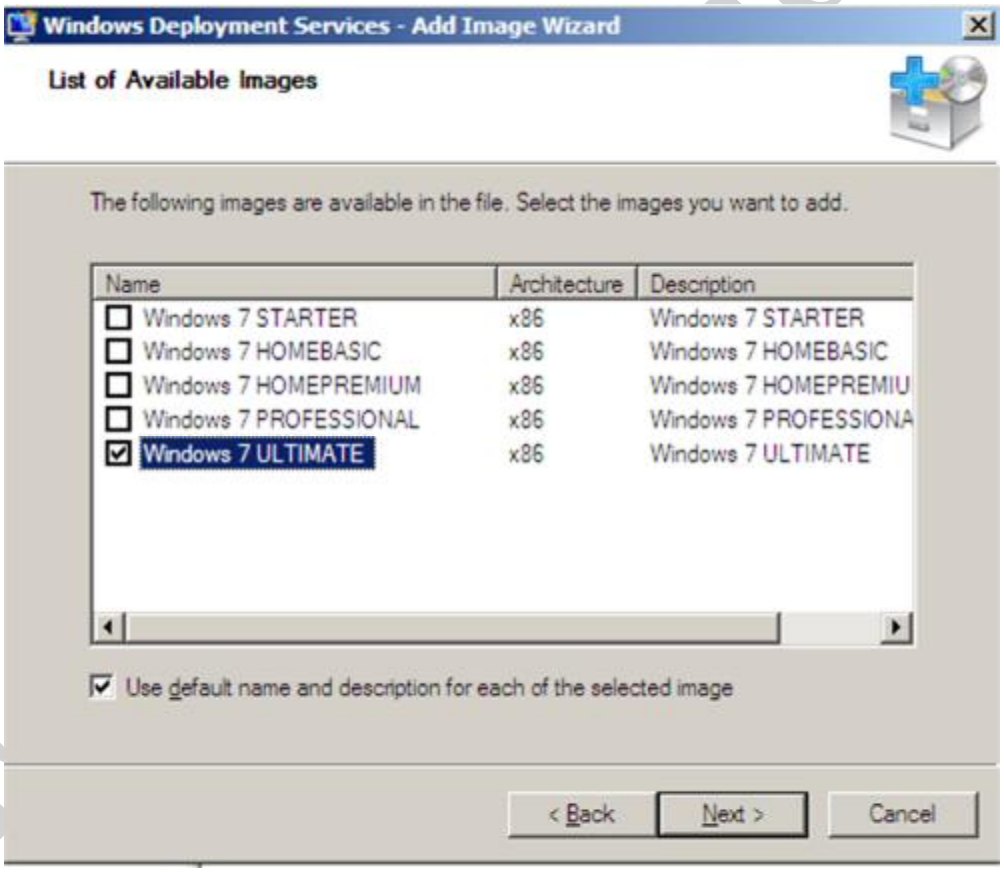
سپس




Farshad Jamshidi Boroush

سپس از داخل DVD 7 فایل Install.wim را انتخاب می کنیم

در اینجا نسخه مورد نظررا انتخاب می کنیم




و نصب تمام می شود.

برای نصب ویندوز از روی WDS بر روی کلاینت باید بوت آن را بر روی کارت شبکه تنظیم کنیم بعد از بوت شدن از روی شبکه بقیه مراحل مانند نصب ویندوز معمولی می باشد,برای اینکه کلاینت بتواند از ویندوزش بر روی سرور Image بگیرد تمامی مراحل بالا را طی می کنیم و بعد از بوت گزینه Capture Image را انتخاب می کنیم.

File And Print Server

برای به اشتراک گذاری منابع در شبکه از File And Print Server استفاده می کنیم

تفاوت های فایل سرور 2008 و2003

1. فایل سرور 2008 دارای کنسولی به نام FileServerResourceManager می باشد( FSRM ).

1-1. Quota Per Folder : در 2003 سهمیه بندی هارد برای کاربرهابر روی درایو ها بود ولی در 2008 سهمیه بندی بر روی فولدرها می باشد .

1-2. File Screen : با استفاده از این قابلیت می توانیم بر روی فولدر هایی که به اشتراک گذاشته ایم محدودیت ایجاد کنیم به طور مثال اجازه نمی دهیم فایل هایی با پسوند ....avi,mpeg,jpg,tif,gif داخل فولدر مورد نظر کپی شود حتی می توانیم فایل را با اسم محدود کنیم.

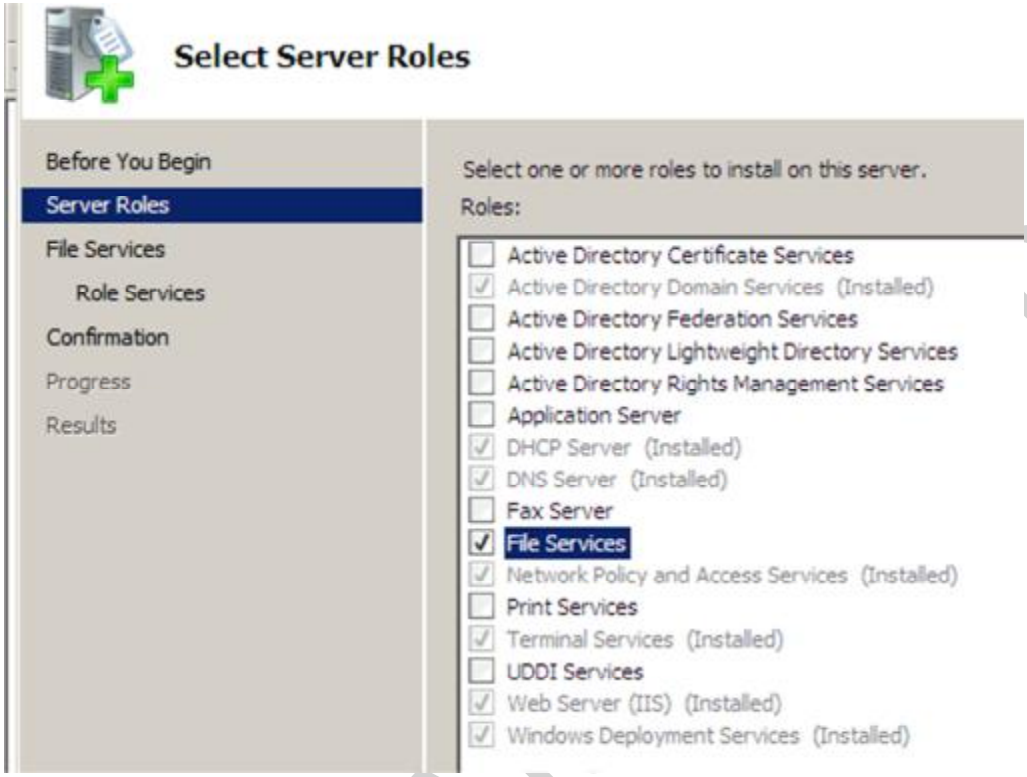
1-3. Report On Share : با فعال بودن این گزینه هر اتفاقی بر روی فایل ها و فولدرهای ما در شبکه بیفتد را به ما اطلاع می دهد,از طریق mail و..

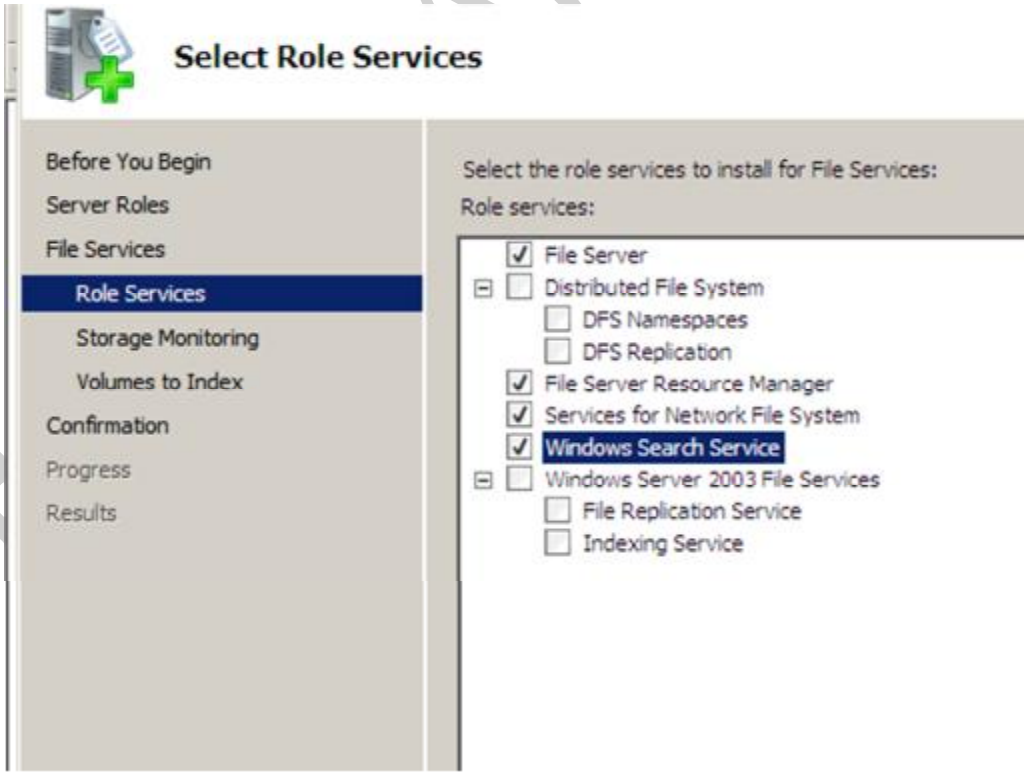
2- Enhancement distributedFile System Server :فرض کنید تعدادی شعب در نقاط مختلف داریم در هر کدام از این شعب هم یکسری فایل های Share شده داریم برای دسترسی به هر کدام از این فایل ها باید Ip سرورها را بدانیم به خاطر سپردن این Ip ها کار ساده ای نیست,برای اینکه تمامی فایل ها ی به اشتراک گذاشته را از روی سرورها بر روی یک سرور دیگر متمرکز کنیم ( Shortcut بسازیم ) از DFSسرور استفاده می کنیم و فقط IP DFS را به خاطر می سپاریم با وصل شدن به DFS به تمامی Share ها از نقاط مختلف دنیا دسترسی داریم به اسم DFS سرور که در Run تایپ می کنیم DFS Name Space گویند.

3- DFS Replication : فرض کنید در ایران یک DFS سرور داریم در کانادا هم یک DFS سرور دیگر با همان اطلاعات سرور اول راه اندازی می کنیم (Backup server 1 ) هر تغییری در DFS ایران ایجاد شود بر روی DFS کانادا هم ایجاد می شود,در صورت خرابی سرور ایران می توان از سرور کانادا استفاده کرد. در اصطلاح به این عمل Tolerance Fault گویند.

- \\192.168.1.1\share به این طرز دسترسی به فایل ها در شبکه که درRun می نویسیم ,UNC گویند.

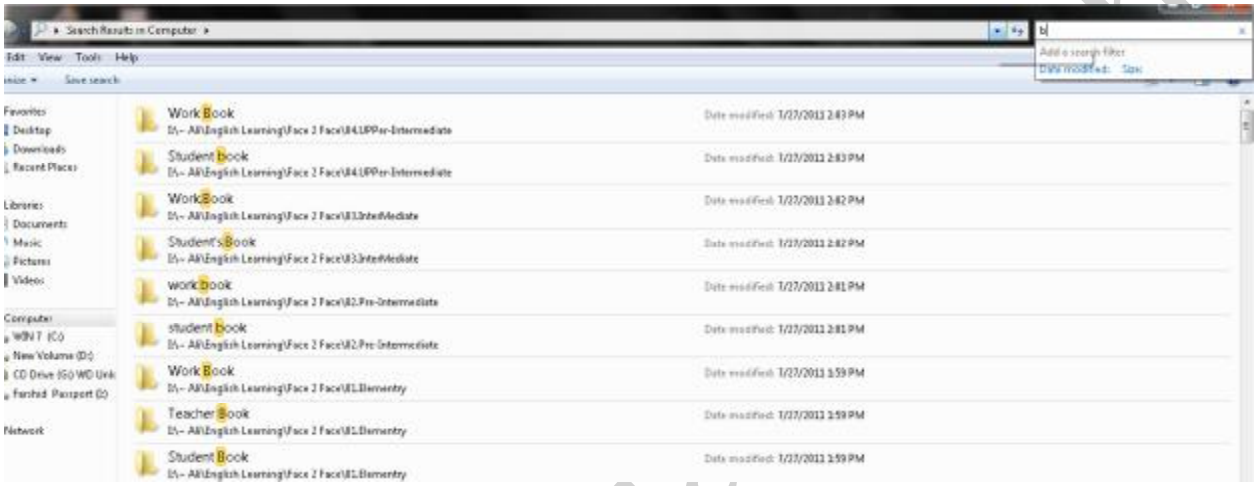
FarshidAjamnoush


Select Server Roles
Before You Begin
Server Roles
File Services
Role Services
Confirmation
Progress
Results
Select one or more roles to install on this 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 (Installed)
DNS Server (Installed)
Fax Server
File Services
Network Policy and Access Services (Installed)
Print Services
Terminal Services (Installed)
UDDI Services
Web Server (IIS) (Installed)
Windows Deployment Services (Installed)


Select Role Services
Before You Begin
Server Roles
File Services
Role Services
Storage Monitoring
Volumes to Index
Confirmation
Progress
Results
Select the role services to install for File Services:
Role services:
File Server
Distributed File System
DFS Namespaces
DFS Replication
File Server Resource Manager
Services for Network File System
Windows Search Service
Windows Server 2003 File Services
File Replication Service
Indexing Service

- پروتکل های Sharing 2 نوع می باشند 1- Samba=SMB و Network File System=NFS ,پروتکل 1 برای ویندوز و 2 برای لینوکس می باشد,در اینجا برای اینکه ویندوز بتواند با فایل سرور لینوکس ارتباط برقرار کند باید گزینه Services for Network File System فعال باشد.

Windows Search Service : ویندوزهای NG برای جستجو کردن از این پروتکل استفاده می کند این پروتکل به صورت Live جستجو می کند



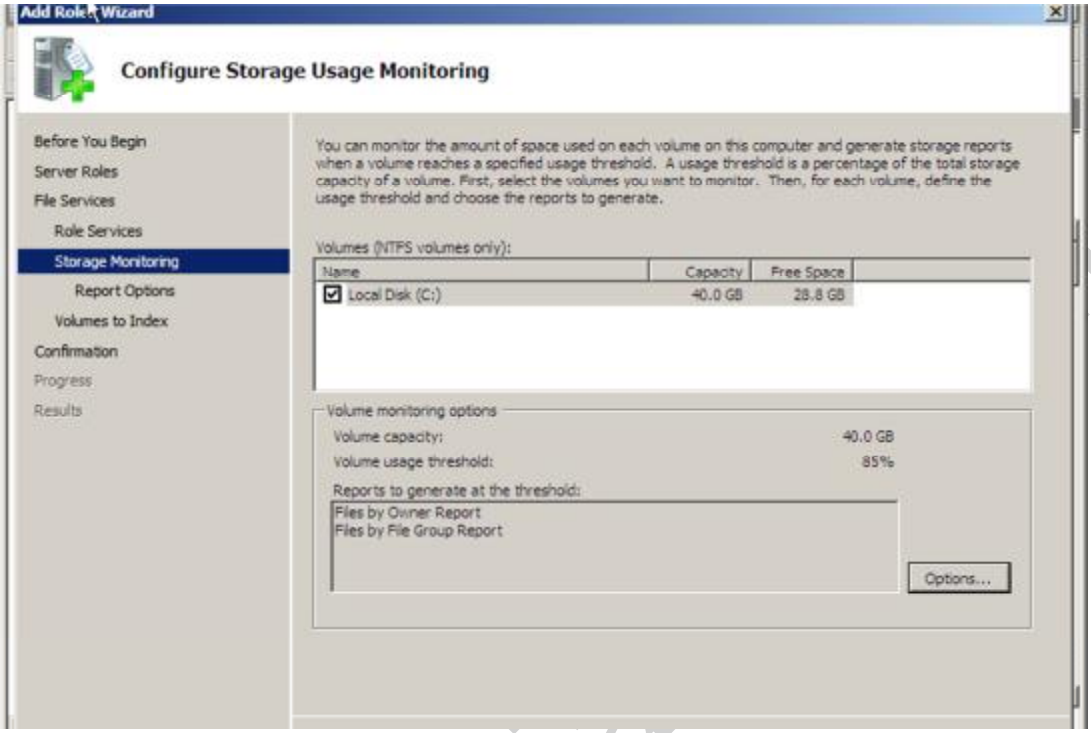

Indexing Service : ویندوزXp از این پروتکل برای جستجو استفاده می کند.

- به طور همزمان نمی توان Windows Search Service وIndexing Service را فعال کرد.

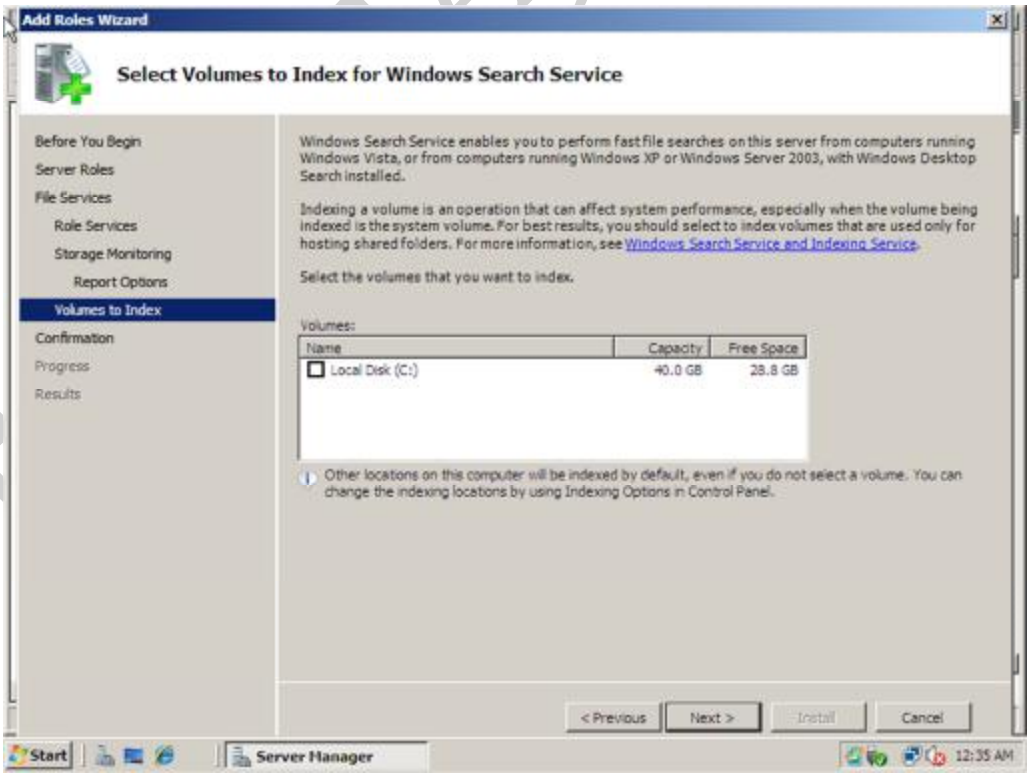
Windows Server2003 File Services : اگر درشبکه فایل سرور2003 داشته باشیم با فعال سازی این گزینه بر روی2008 فایل سرور ما با 2003 به زبان همان 2003 با آن ارتباط برقرار می کند.

FarshidAj...

در مرحله بعد تمامی هارد ها ودرایو ها را لیست میکند و می گوید از کدام می خواهی Report تهیه شود.

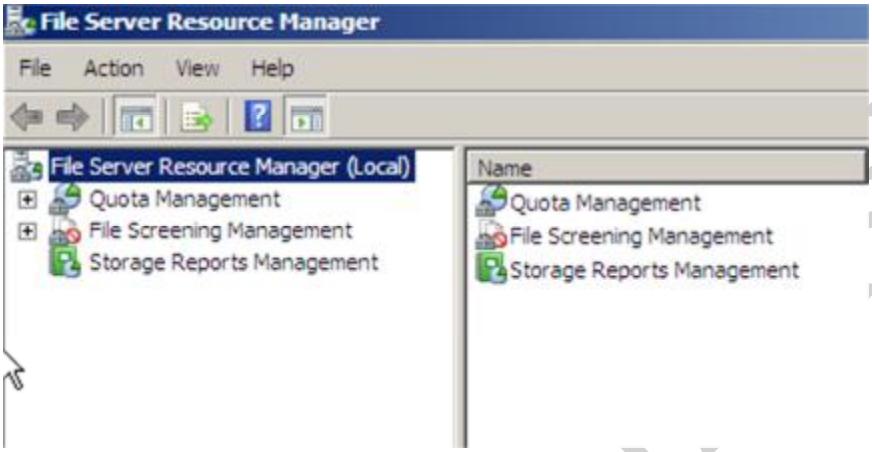



در اینجا از ما می پرسد می خواهی جستجو را بر اساس Index بگذارم؟



- نرم افزار smb crack نرم افزاریست برای بدست آوردن یوزر و پسورد در هنگام وصل شدن به Share یک سیستم.

FSRM

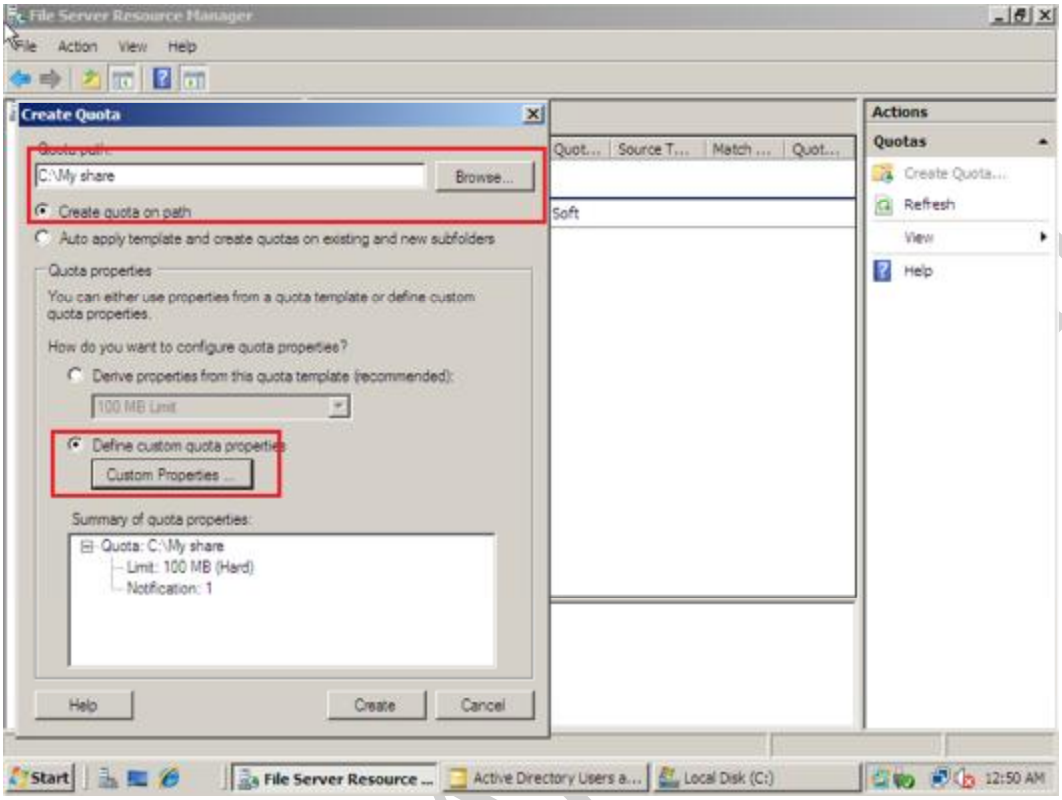


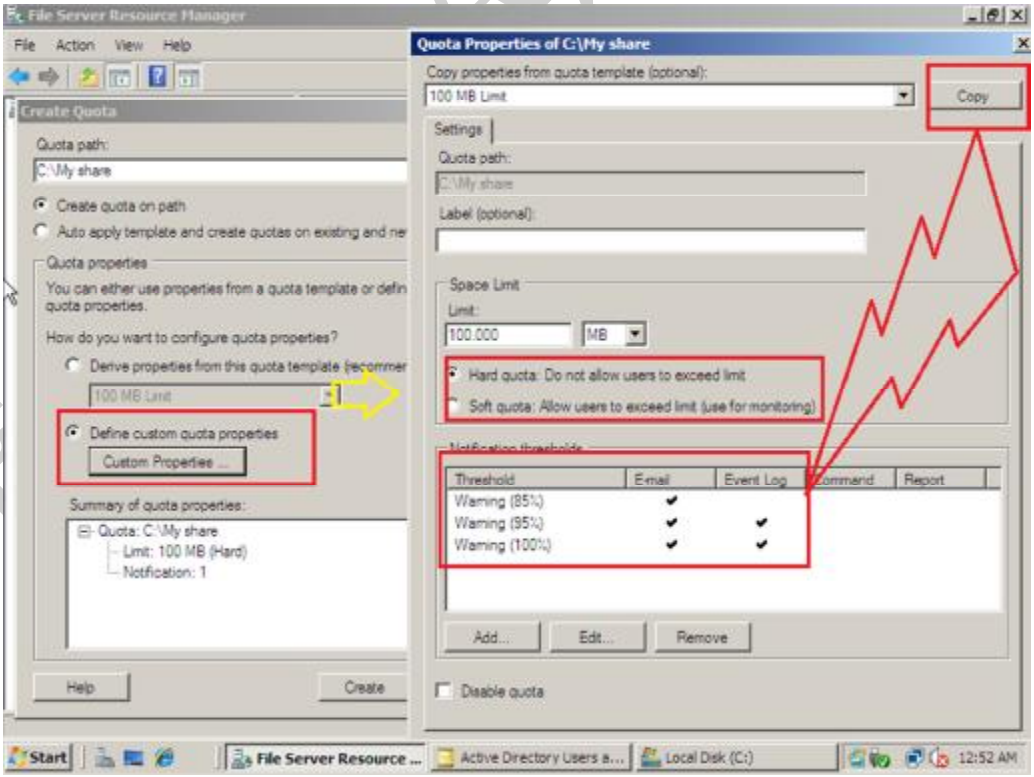

برای نوشتن Template در Quota مانند زیر عمل می کنیم

- Quota که در اینجا تعیین می کنیم بر روی فولدر ها می باشد.
- وارد کنسول FSRM می شویم.

Farshidnabizadeh

سپس پوشه ای را که می خواهیم روی آن سهمیه بندی ایجاد کنیم را انتخاب می کنیم

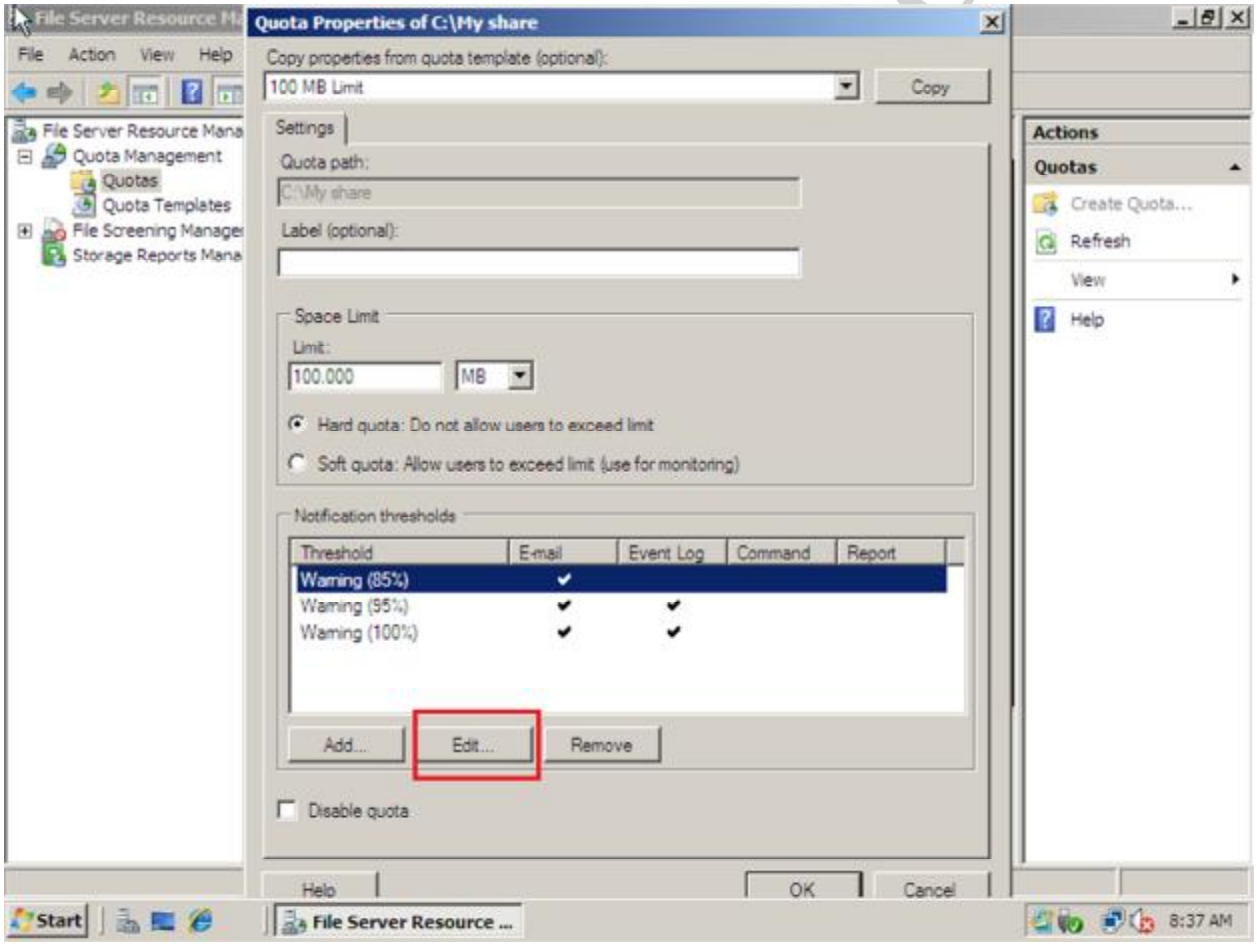


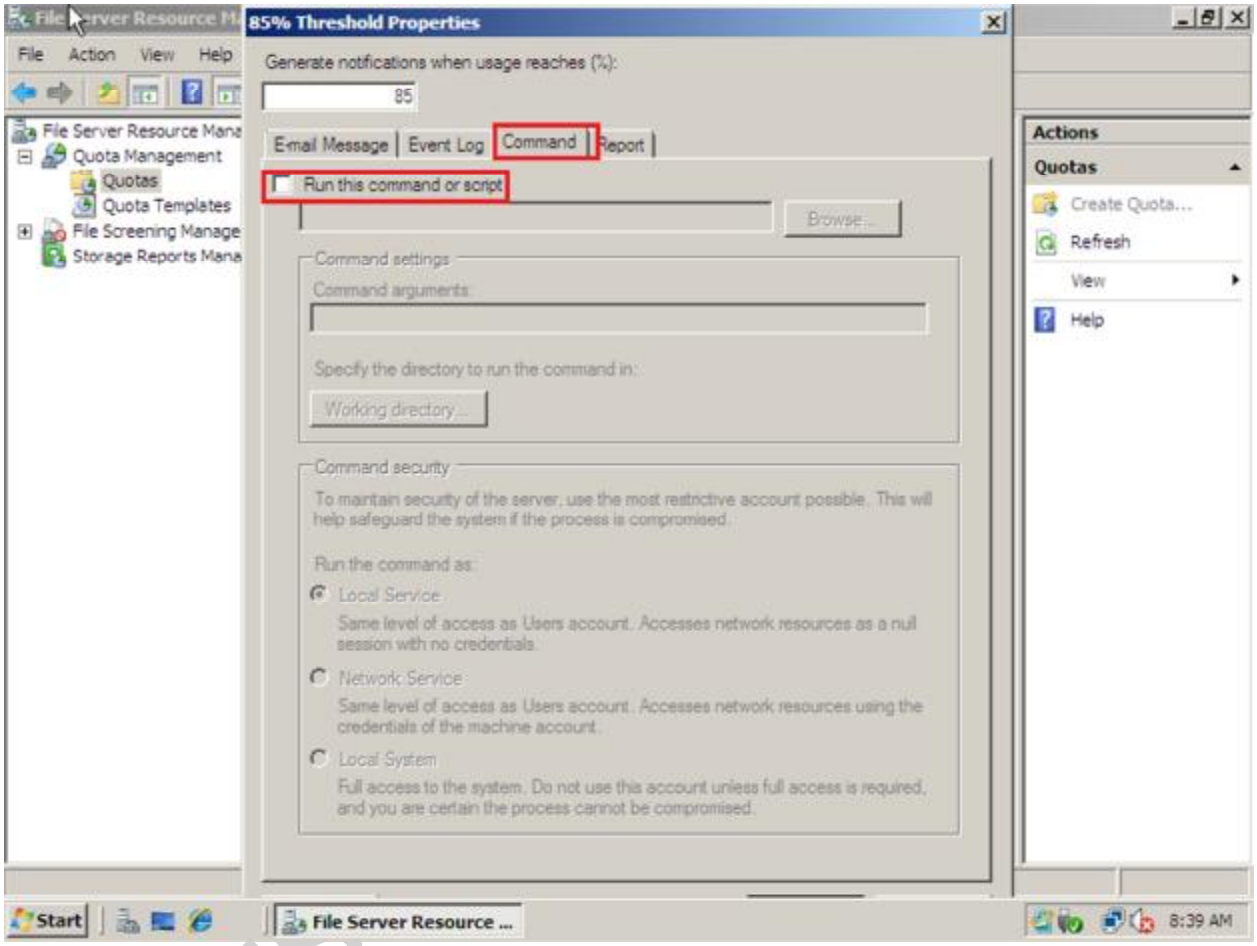
Hard Quota=Hard Limit :اگر این گزینه را انتخاب کنیم,زمانی که مقدار حجم مجاز هر کاربر بر روی فولدرش پر شده باشد به کاربر پیغام داده ودیگر اجازه ریختن اطلاعات را به آن نمی دهد.

Soft Quota=Soft Limit : اگر این گزینه را انتخاب کنیم,زمانی که مقدار حجم مجاز هر کاربر بر روی فولدرش پر شده باشد به کاربر پیغام داده و اجازه می دهد کاربر به ریختن فایل ادامه دهد.

با ویرایش کردن پیغامهای زیر می توانیم بگوییم که اگر به 85%فضای اختصاص داده شده رسید چه عملی را انجام دهد مثلاً اسکریپتی اجرا شود که فایلهای 2 روز گذشته را پاک کند.

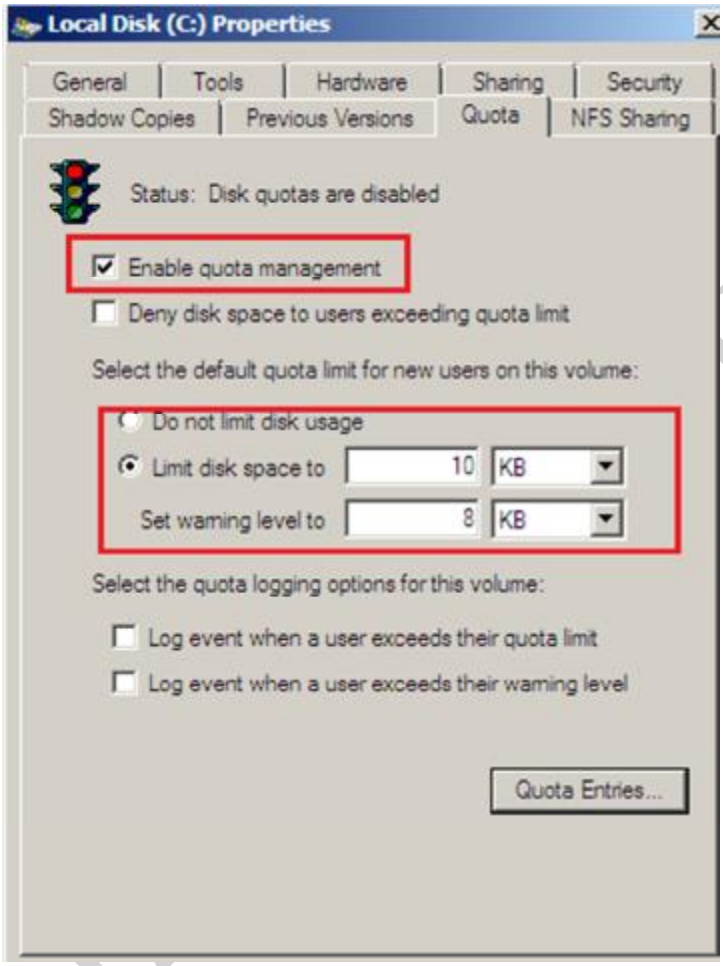


- زبان اسکریپت نویسی VBS می باشد.




Fars

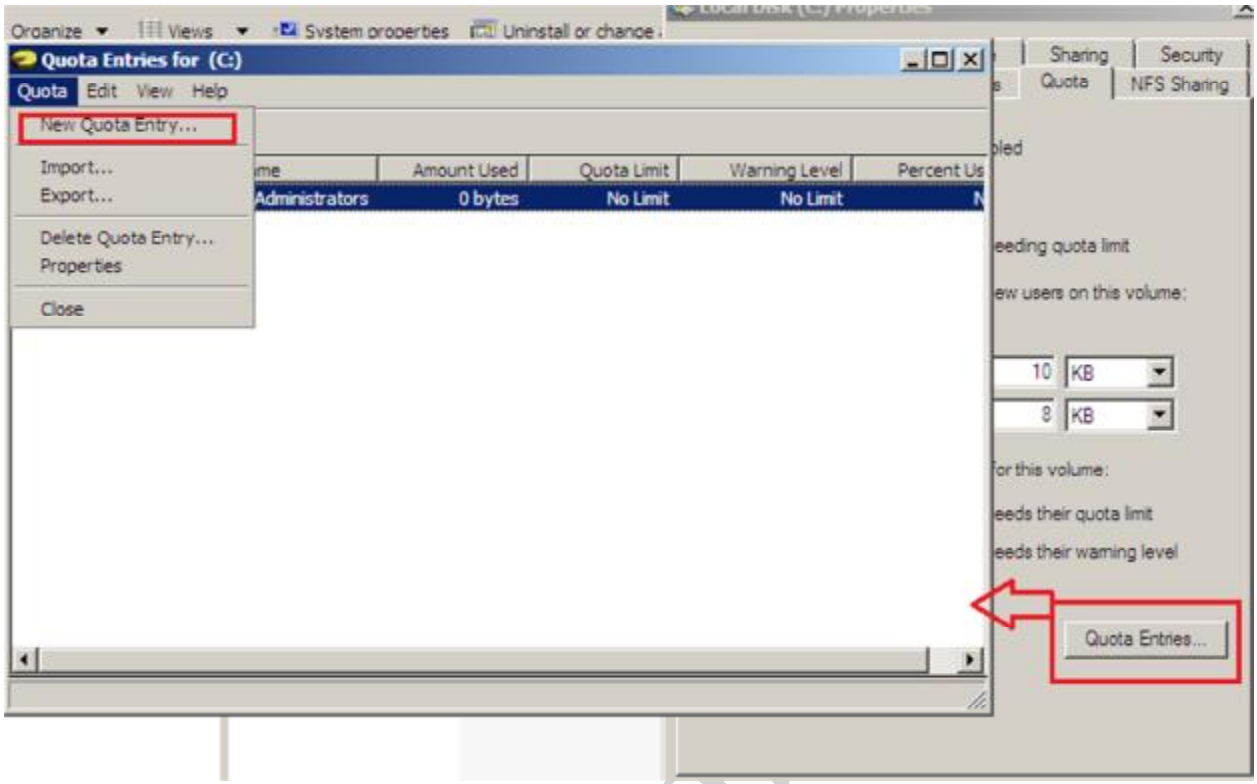
Quota بر روی Drive



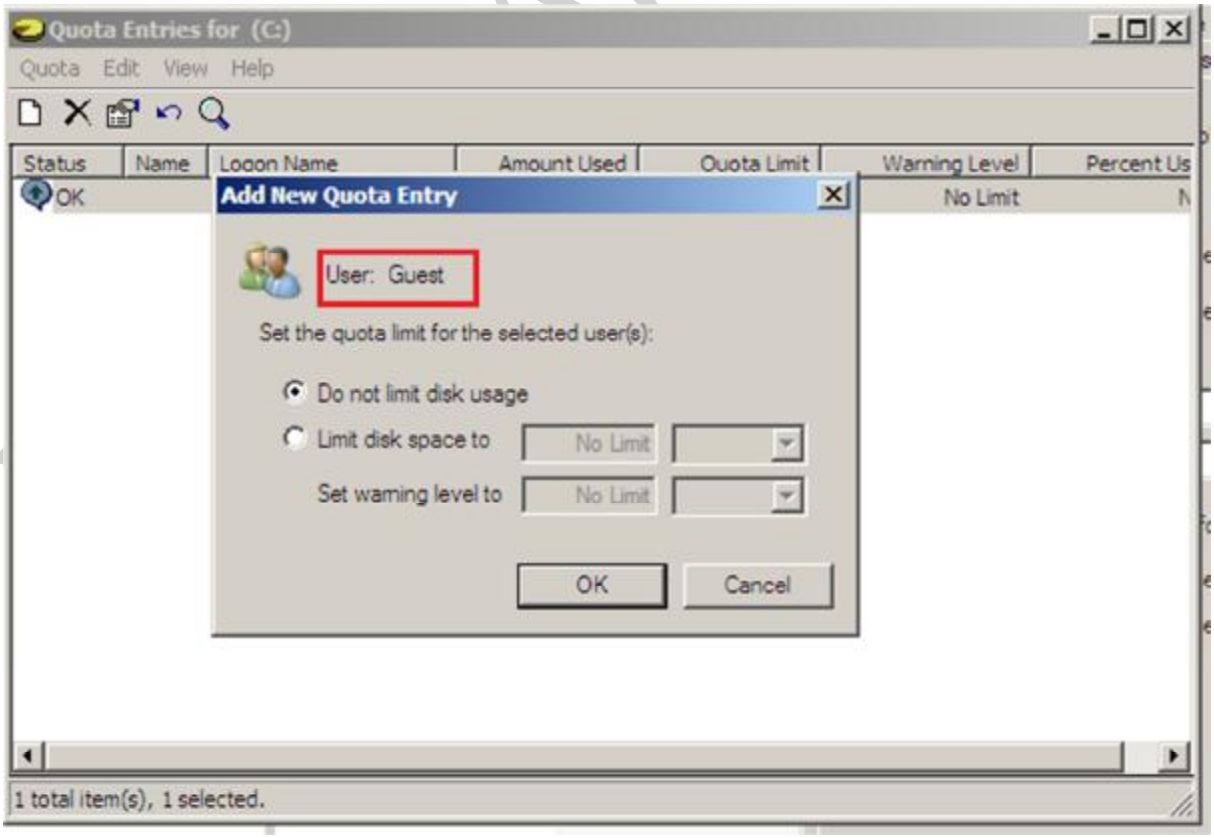

**با فعال بودن گزینه اول مدیریت بر Quota فعال می باشد زمانی که گزینه Limit فعال می شود محدودیت برای Every one فعال می باشد , 10k معادل Hard Limit و 8k معادل Soft Limit می باشد.**

**برای اینکه بتوانیم برای کاربر مشخصی محدودیت ایجاد کنیم باید مانند زیر عمل کنیم**

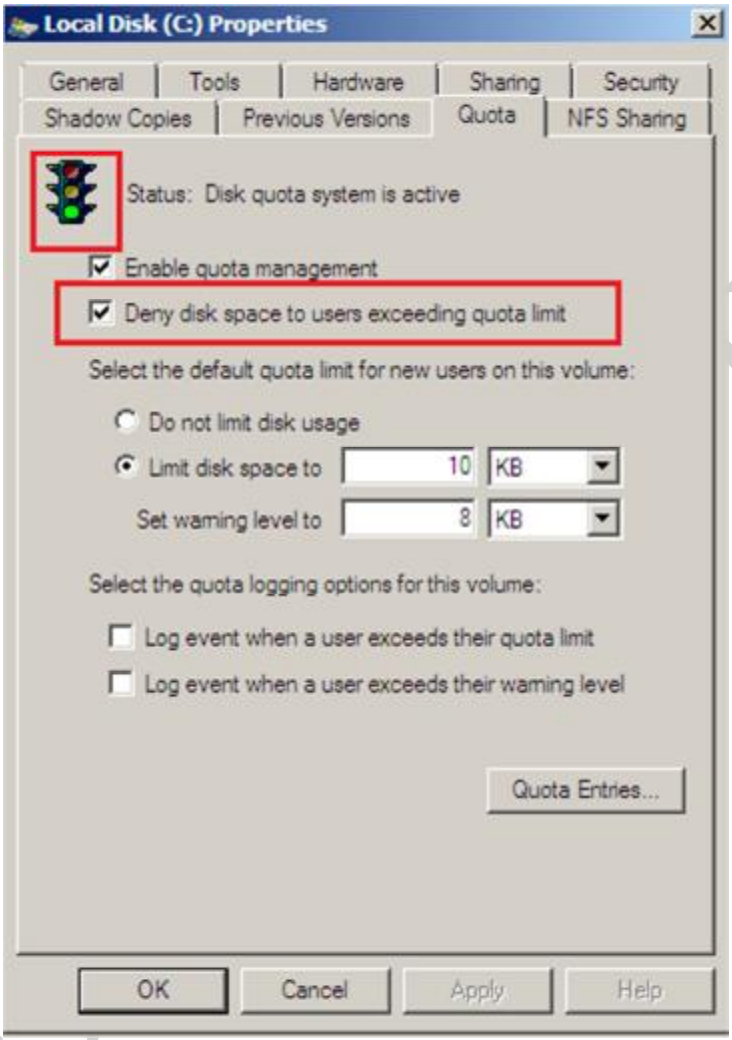
Farsi Kush



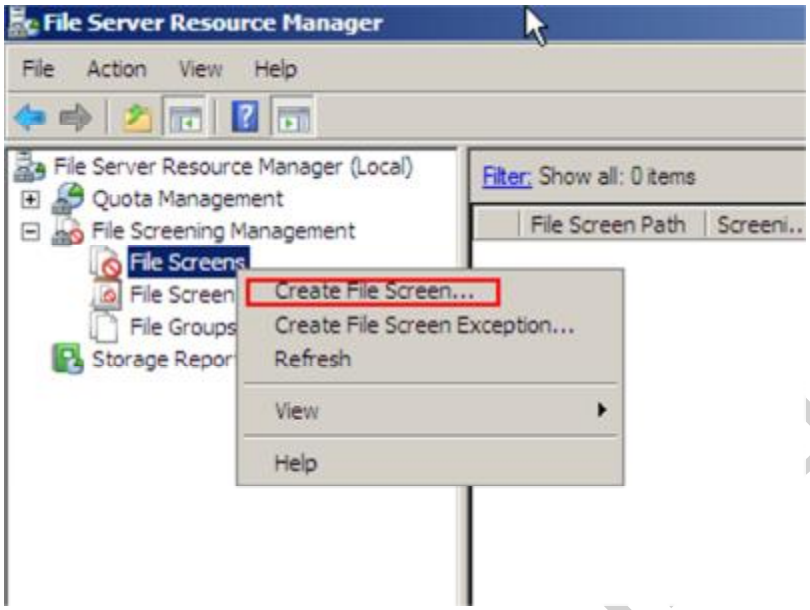

**کاربر مورد نظر را انتخاب می کنیم**

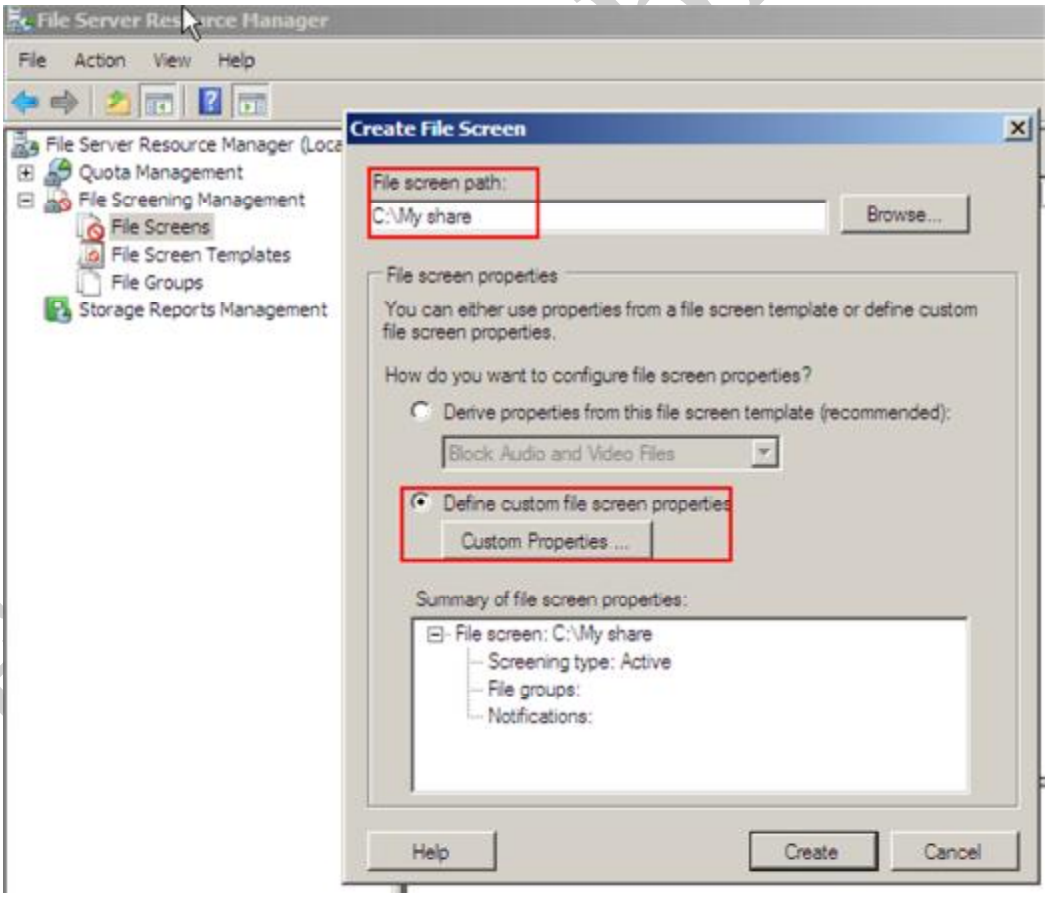


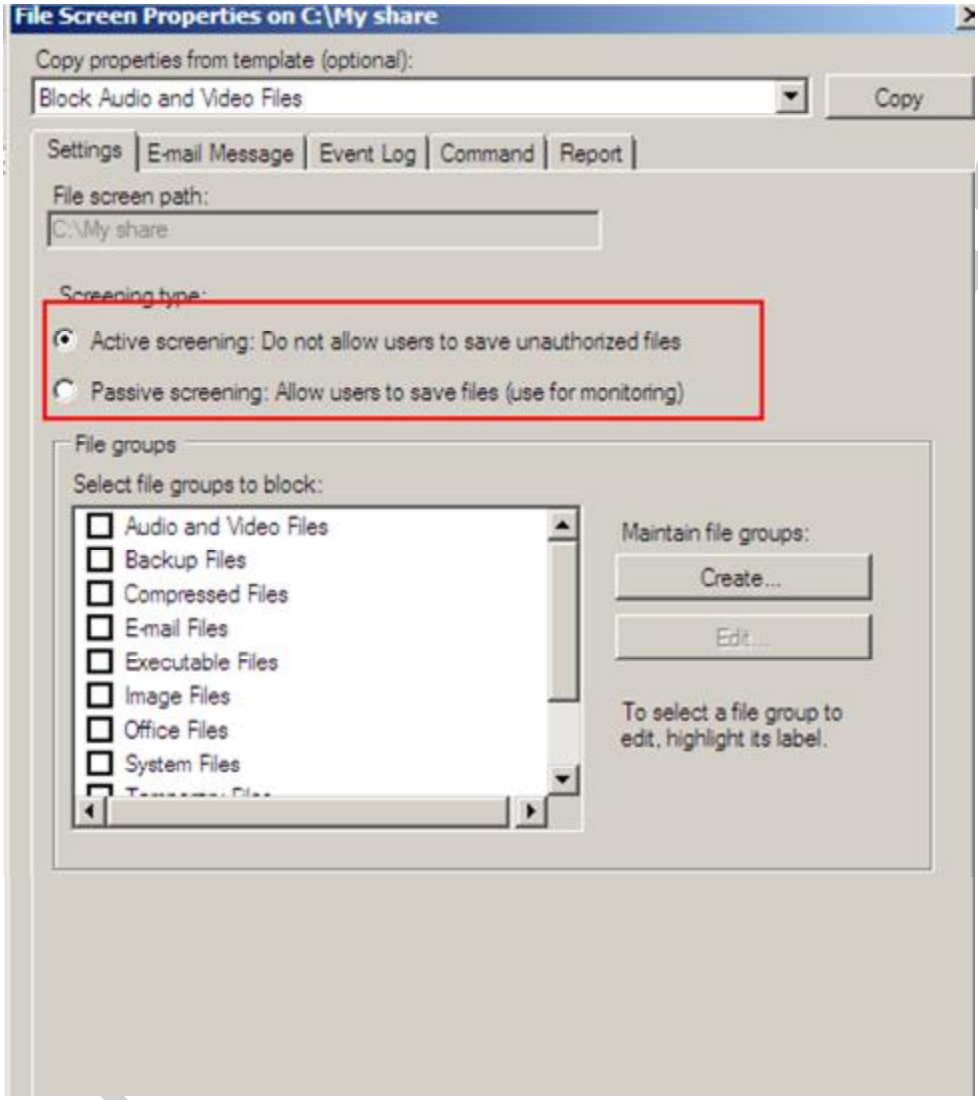
در آخر هم برای اینکه محدودیت اعمال شود گزینه ...Deny را فعال می کنیم.




- می توانیم زمانی که محدودیت برای یک درایو ایجاد کردیم از همان محدودیت ها با همان کاربرها بر روی درایو دیگر هم استفاده کنیم فقط باید Import & Export کنیم.

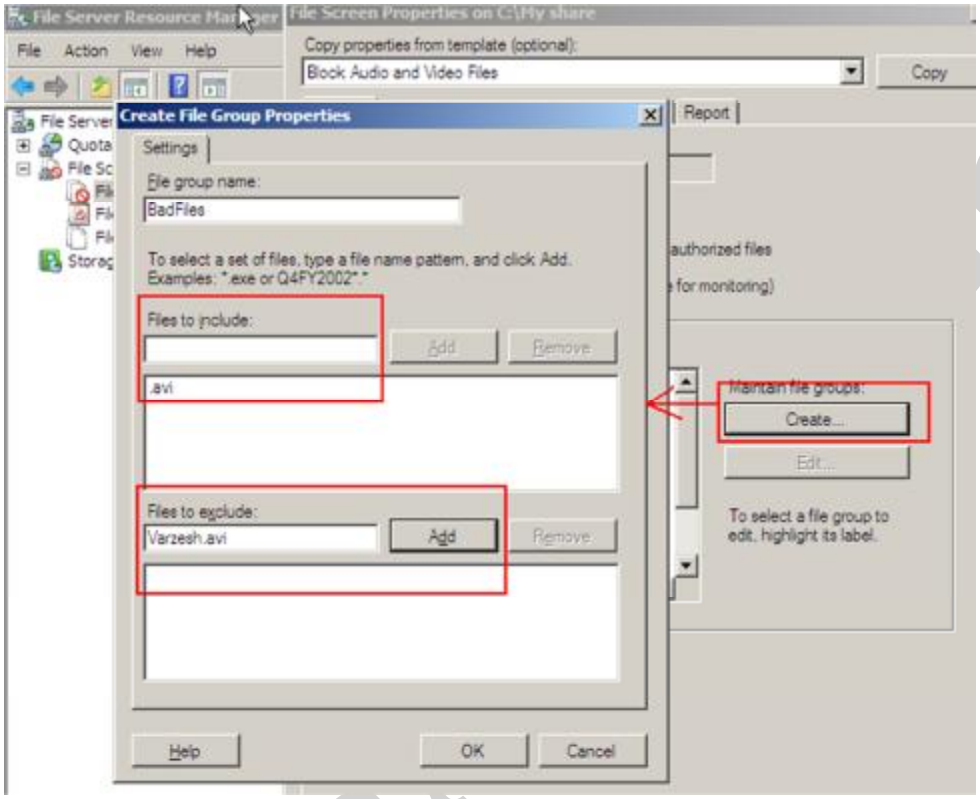

File Server Resource Manager
File Action View Help
File Server Resource Manager (Local)
Quota Management
File Screening Management
File Screens
File Screen
File Groups
Storage Repor
Filter: Show all: 0 items
File Screen Path
Screeni..
Create File Screen...
Create File Screen Exception...
Refresh
View
Help


File Server Resource Manager
File Action View Help
File Server Resource Manager (Loca
Quota Management
File Screening Management
File Screens
File Screen Templates
File Groups
Storage Reports Management
Create File Screen
File screen path:
C:\My share
Browse...
File screen properties
You can either use properties from a file screen template or define custom file screen properties.
How do you want to configure file screen properties?
Derive properties from this file screen template (recommended):
Block Audio and Video Files
Define custom file screen properties
Custom Properties ...
Summary of file screen properties:
File screen: C:\My share
Screening type: Active
File groups:
Notifications:
Help
Create
Cancel




- Active & Passive مانند Soft & Hard Limit می باشد.

در قسمت Include هر اسم,پسوند را وارد کنیم اجازه ریختن آن در پوشه به اشتراک گذاشته مورد نظر را نمی دهد.




در قسمت Exclude هر اسم,پسوند را وارد کنیم اجازه ریختن آن در پوشه به اشتراک گذاشته مورد نظر را می دهد.

تمامی منوها هم مانند Quota می باشد.

- پاک کردن Log ویندوز با نرم افزار elsave از راه دور
- بهترین سایت برای Admin ها Manageengine.com

سه نوع Share داخل سیستم های کامپیوتری موجود داریم : 1) Admin Share 2) Hidden Share

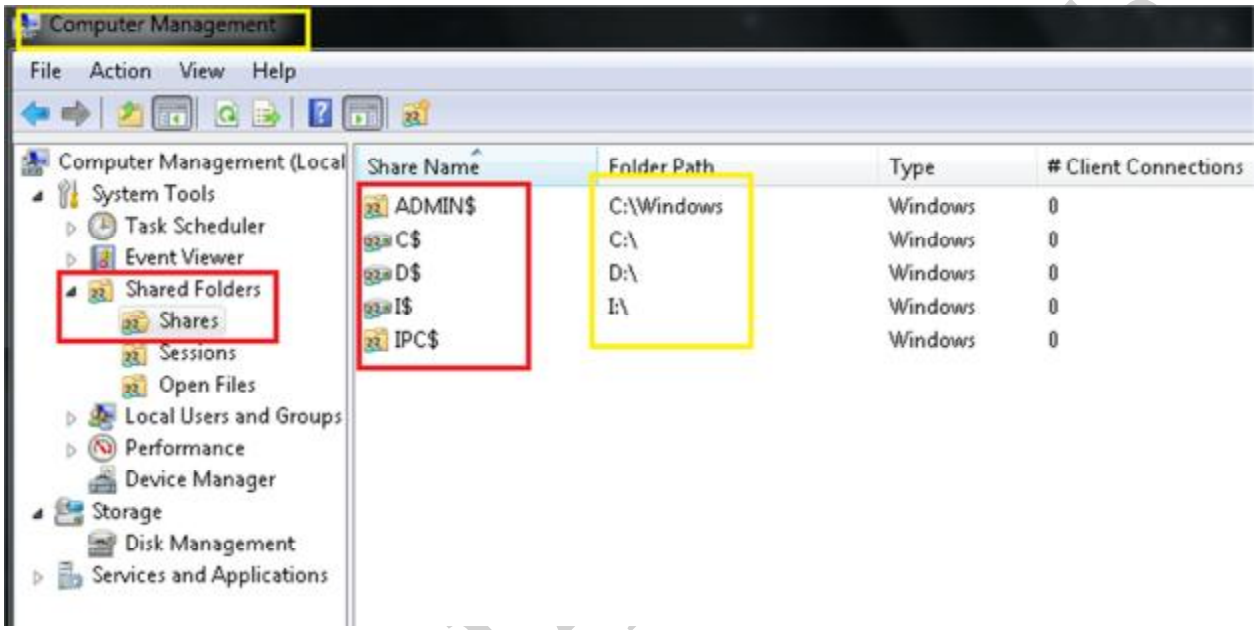
3) Provision Share

Farshidan

Admin Share : به مجموع Share های خود ویندوز که به صورت اتوماتیک Share می باشند ( Admin c$-Ip c$- Drive $ ) گویند.

Ip c$ اگر غیر فعال کنیم دیگر کسی نمی تواند از بیرون به سیستم ما وصل شود.

Admin $ معادل c:\Windows می باشد.




برای غیر فعال کردن آنها بر رویشان راست کلیک وStop , تا زمانی که ریستارت نکرده ایم Stop می باشد, برای Stop کردن دائم باید از رجیستری آنها را غیر فعال کنیم.

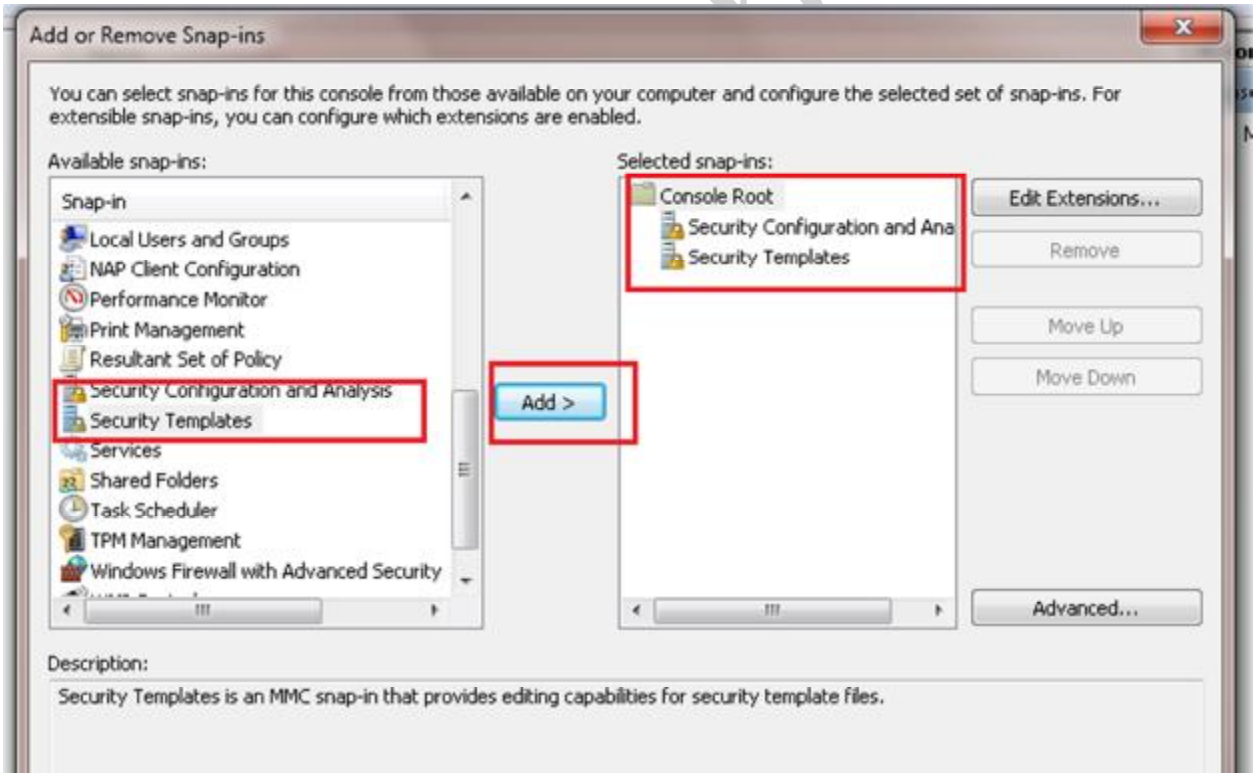
- کاربرانی که عضوء گروه Admin باشند می توانند ازبیرون به Admin Shareدسترسی داشته باشند.

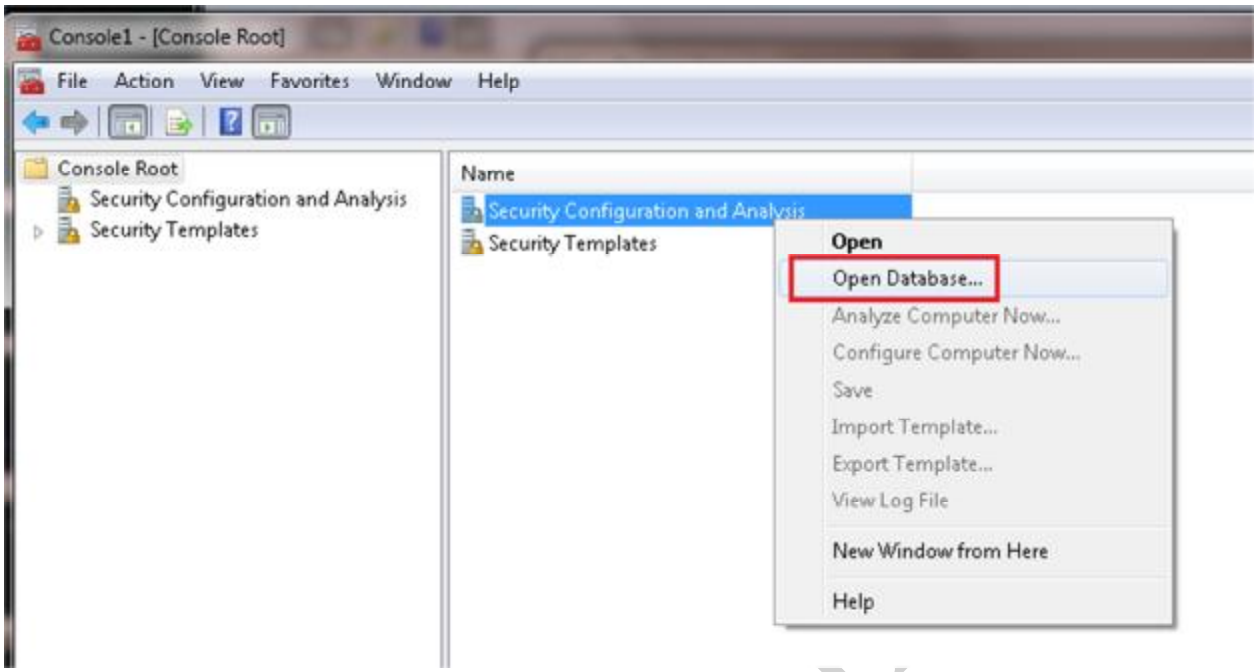
برای بستن راه دیگری هم وجود دارد

وارد mmc می شویم

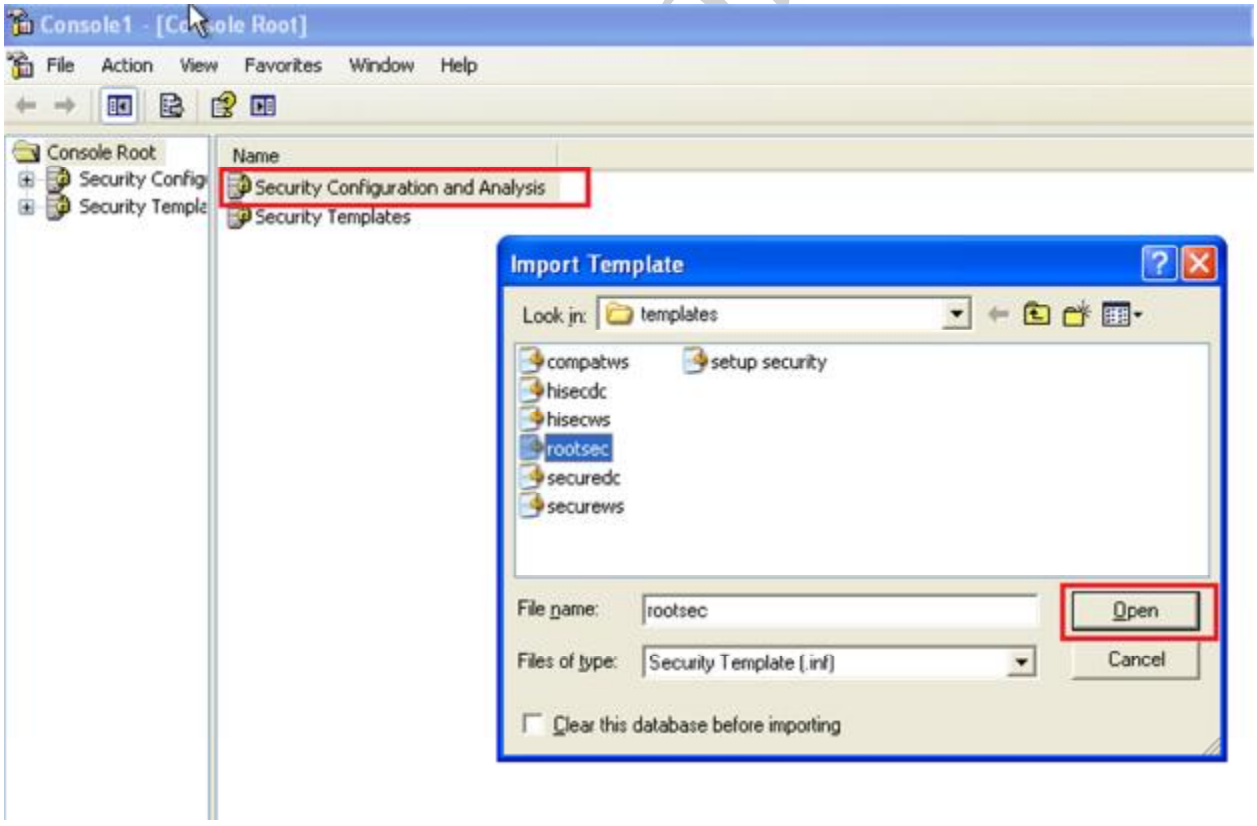
Farshid

Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\system32\compmgmt
2 C:\Windows\system32\devmgmt
3 C:\Windows\system32\wf
4 C:\Windows\System32\services
Exit


Add or Remove Snap-ins
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.
Available snap-ins:
Snap-in
Local Users and Groups
NAP Client Configuration
Performance Monitor
Print Management
Resultant Set of Policy
Security Configuration and Analysis
Security Templates
Services
Shared Folders
Task Scheduler
TPM Management
Windows Firewall with Advanced Security
Add >
Selected snap-ins:
Console Root
Security Configuration and Ana
Security Templates
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
Description:
Security Templates is an MMC snap-in that provides editing capabilities for security template files.

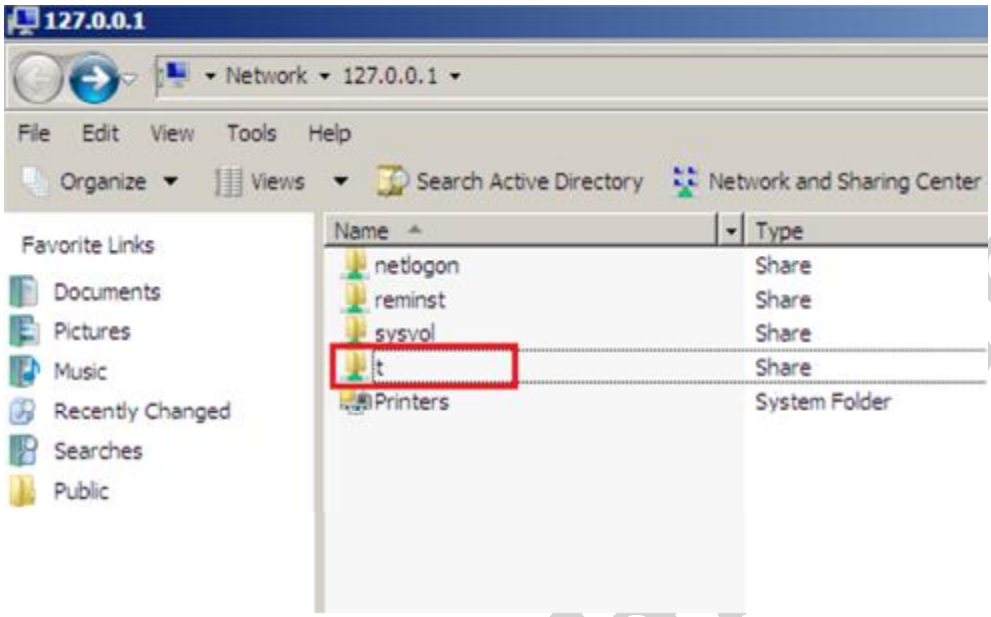


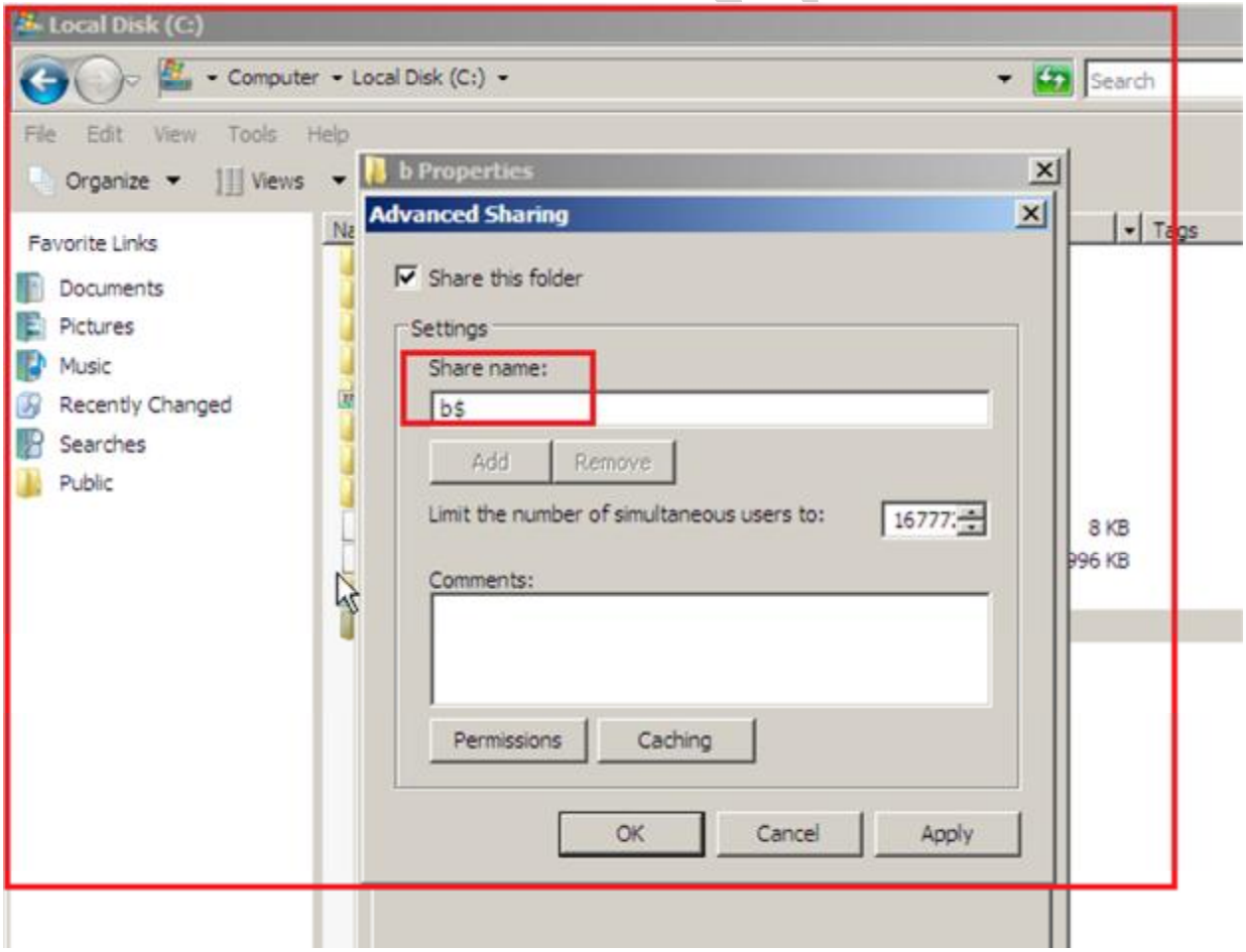

**حالا یک اسمی وارد می کنیم از نمونه ای باز شده باید نمونه زیر را انتخاب کنیم.**



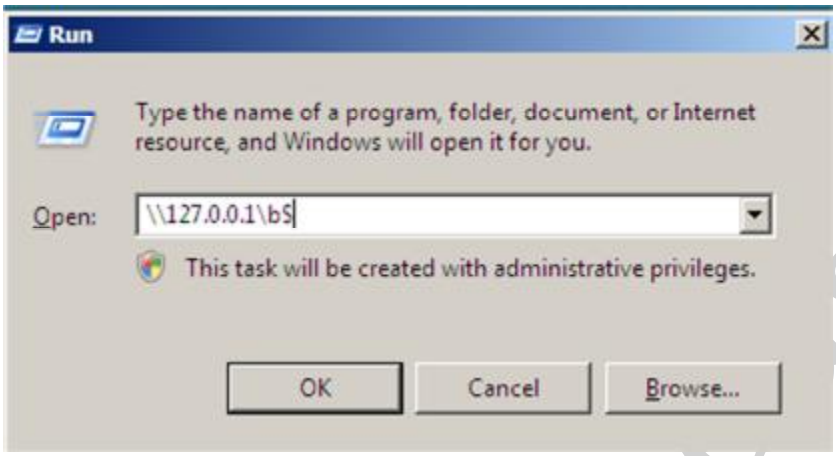

**حتما باید این نمونه ها را کامل یاد بگیریم در 2008 این نمونه موجود نیست باید از Xp کپی کنیم.**

Hidden Share : 2 فایل را Share می کنیم T وB

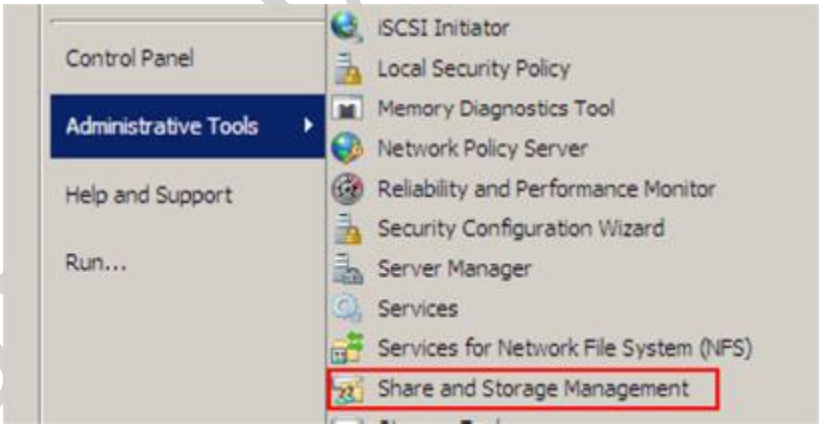


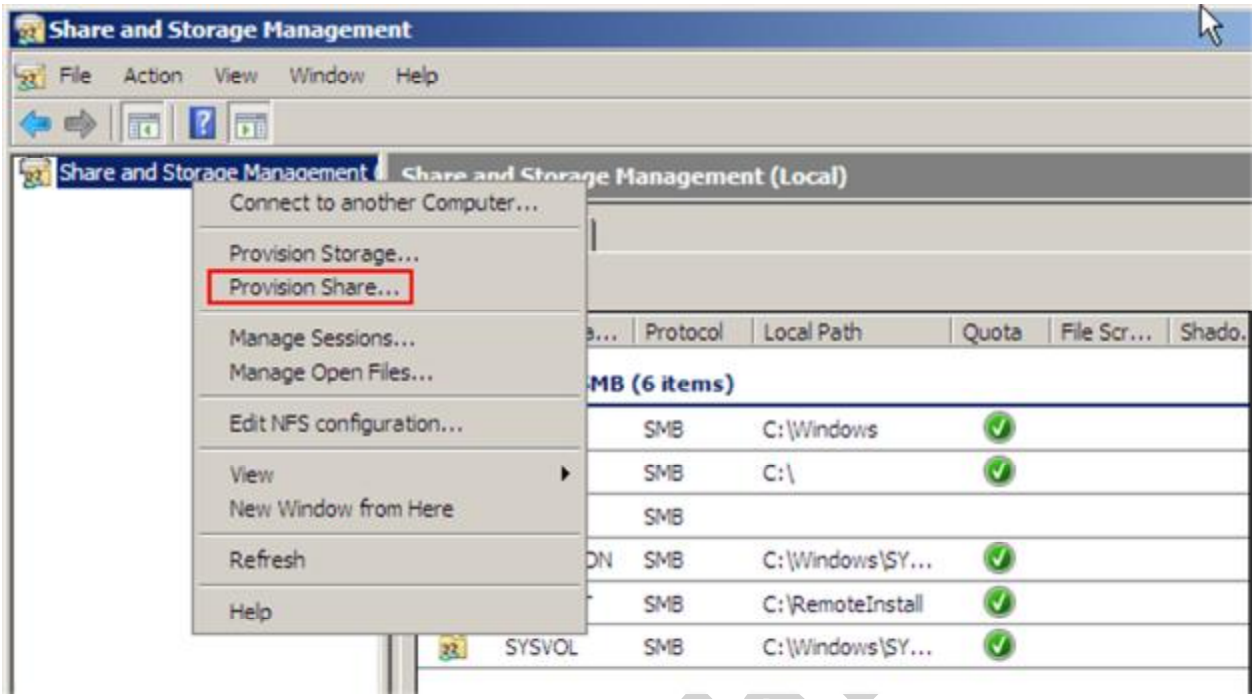
انتهای B علامت $ را اضافه می کنیم و دیگر پوشه B در فایل های Share قابل دیدن نمی باشد,برای دیدن این پوشه باید بصورت زیر عمل می کنیم(چون فایل پنهان شده).

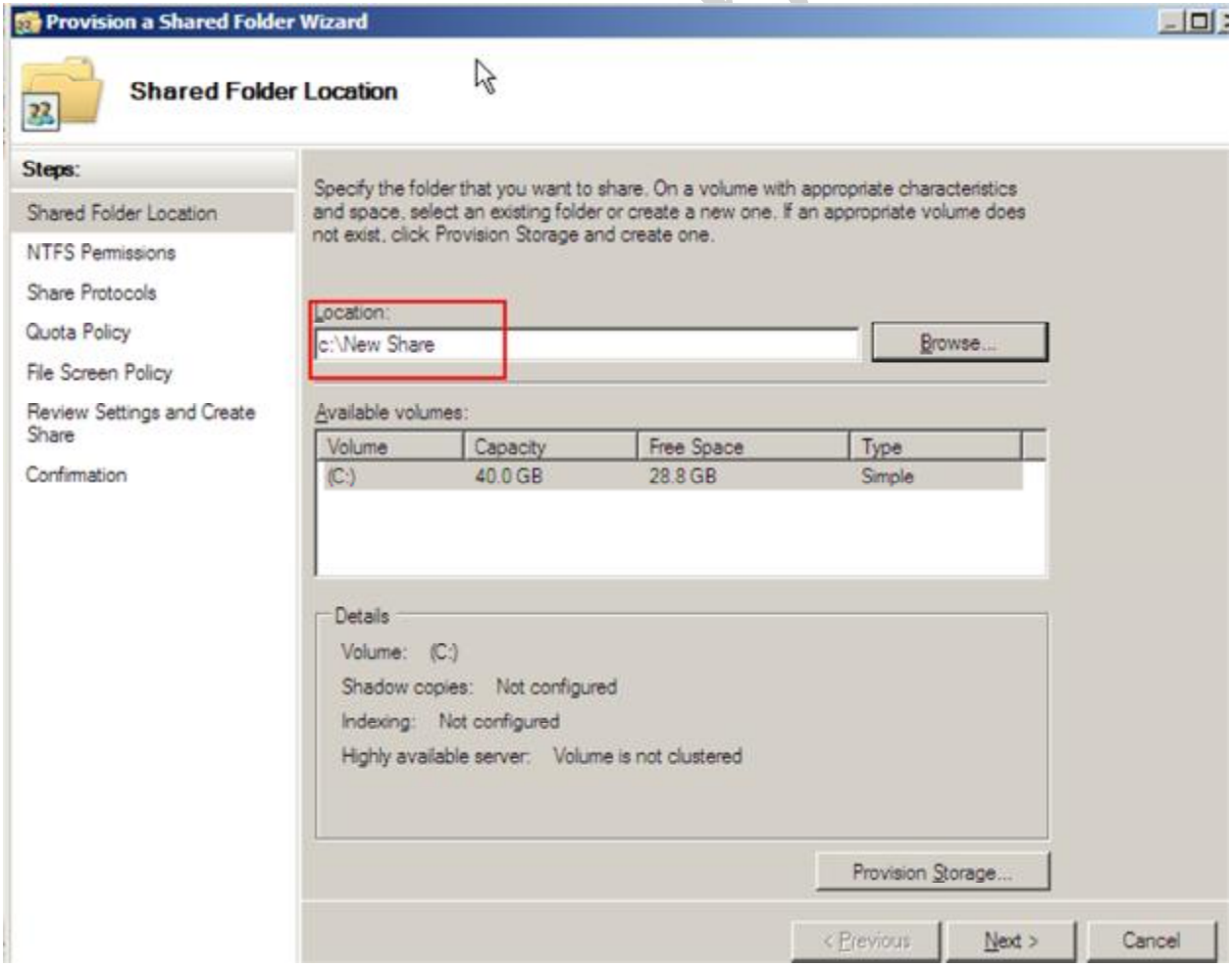



Provision Share :

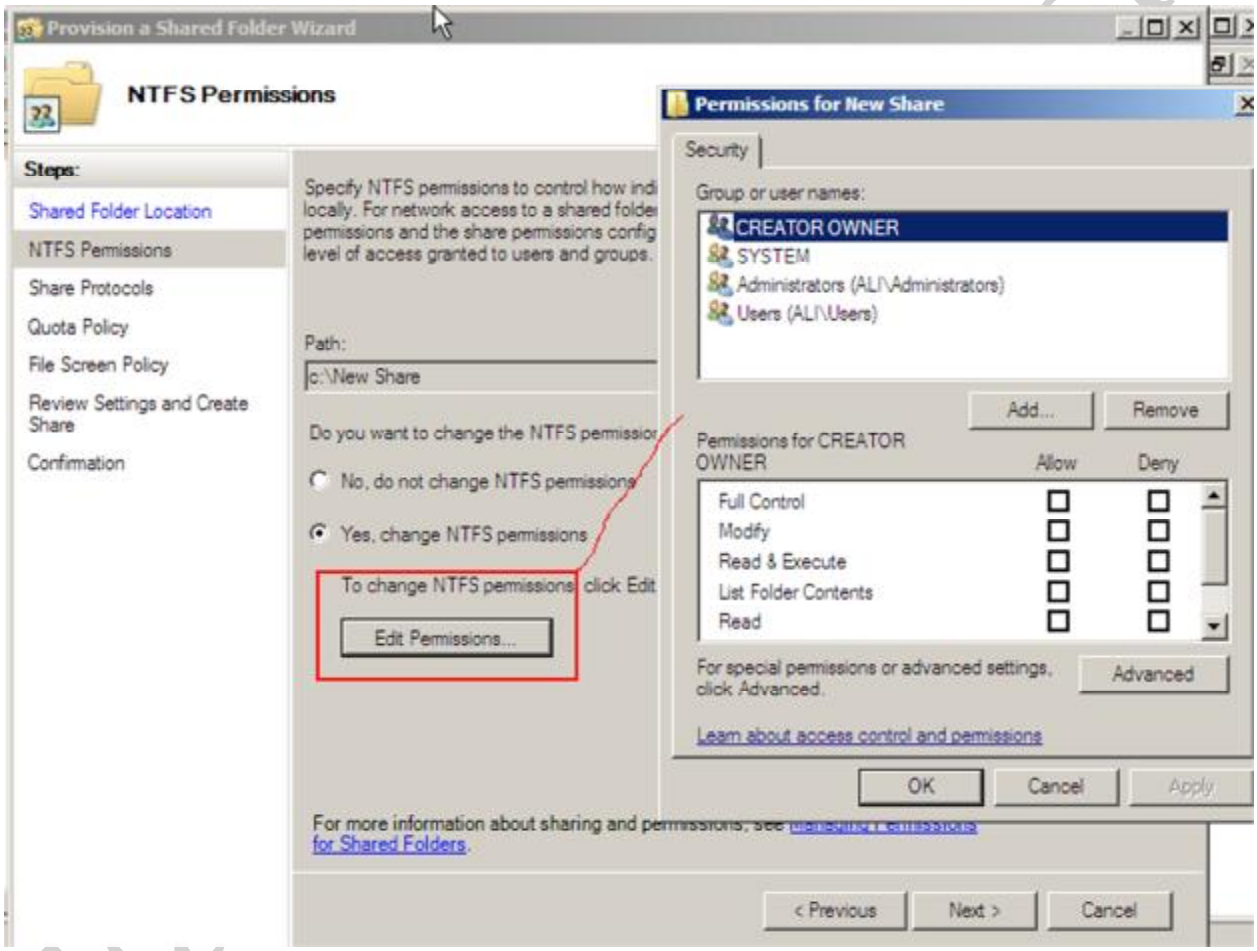



Fa Ajabnesh

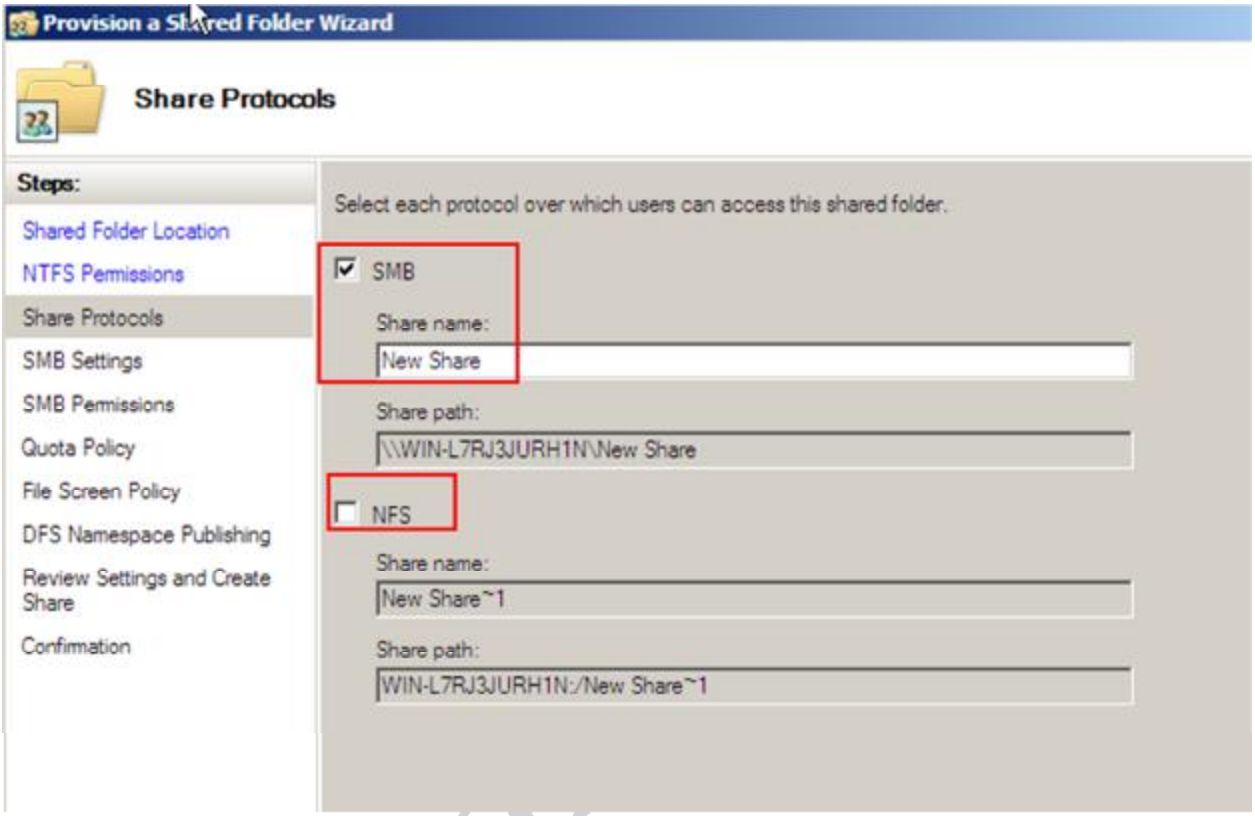

Share and Storage Management
File Action View Window Help
Share and Storage Management
Share and Storage Management (Local)
Connect to another Computer...
Provision Storage...
Provision Share...
Manage Sessions...
Manage Open Files...
Edit NFS configuration...
View
New Window from Here
Refresh
Help
Protocol
Local Path
Quota
File Scr...
Shado.
MB (6 items)
SMB C:\Windows
SMB C:\
SMB
SMB C:\Windows\SY...
SMB C:\RemoteInstall
SYSVOL SMB C:\Windows\SY...


Provision a Shared Folder Wizard
Shared Folder Location
Steps:
Shared Folder Location
NTFS Permissions
Share Protocols
Quota Policy
File Screen Policy
Review Settings and Create Share
Confirmation
Specify the folder that you want to share. On a volume with appropriate characteristics and space, select an existing folder or create a new one. If an appropriate volume does not exist, click Provision Storage and create one.
Location:
c:\New Share
Browse...
Available volumes:
Volume
Capacity
Free Space
Type
(C:)
40.0 GB
28.8 GB
Simple
Details
Volume: (C:)
Shadow copies: Not configured
Indexing: Not configured
Highly available server: Volume is not clustered
Provision Storage...
< Previous
Next >
Cancel

در این مرحله از ما می پرسد که می خواهی NTFS Permission انجام بدهی؟ اگر Yes کنیم تب Security باز می شود.

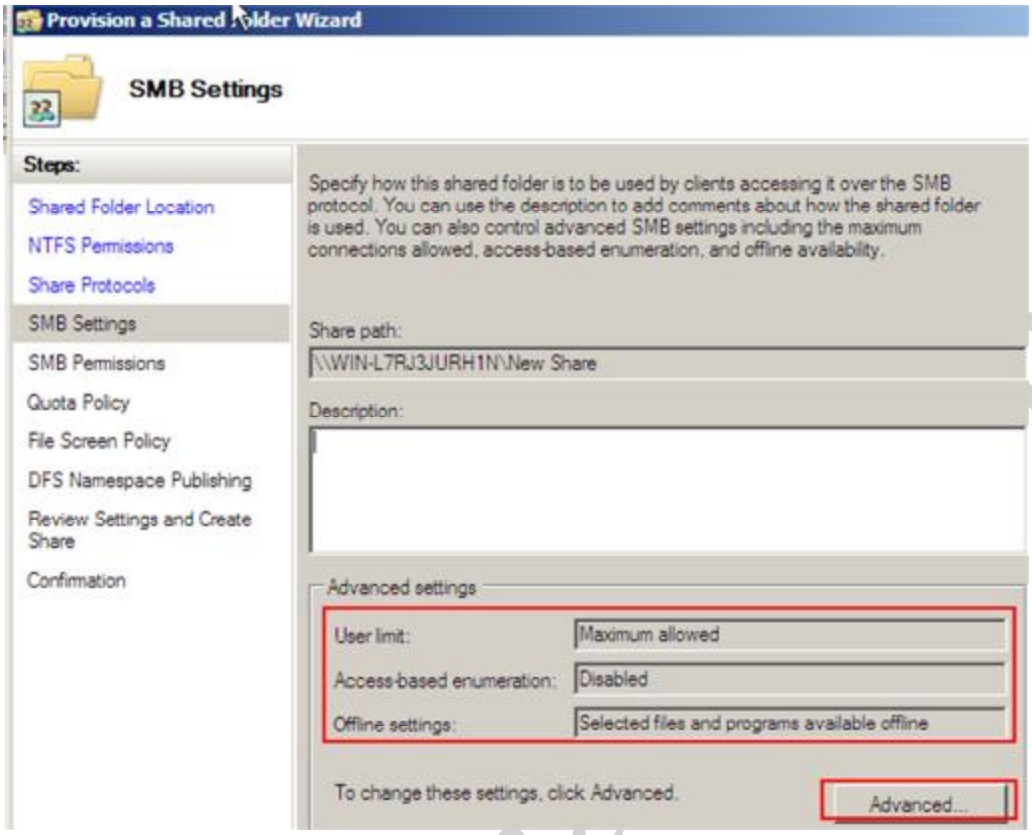


در اینجا نوع پروتکلShare را می پرسد (لینوکسی یا ویندوزی)

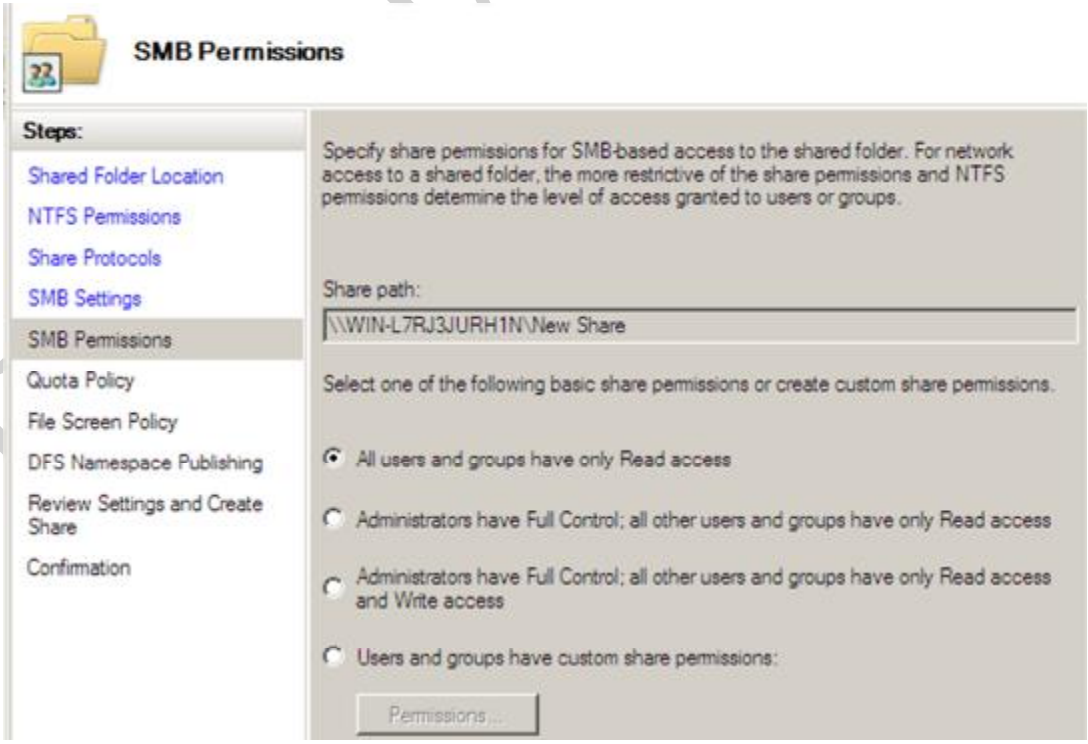



در مرحله بعد می توانیم تعداد دسترسی های کاربران را مشخص کنیم, Hidden Share را فعال کنیم (Access-Based... ) آفلاین را فعال کنیم,منظور از آفلاین استفاده از حالت Sync می باشد.

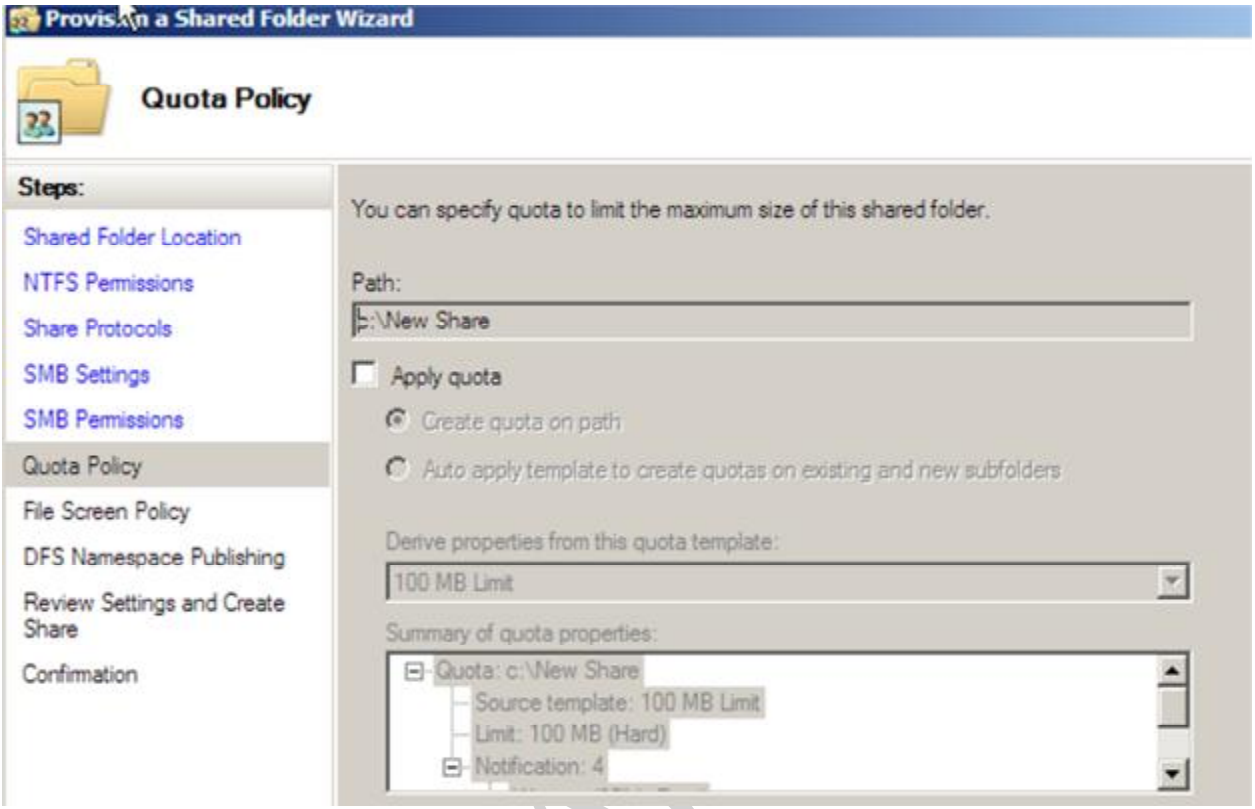
Farshid

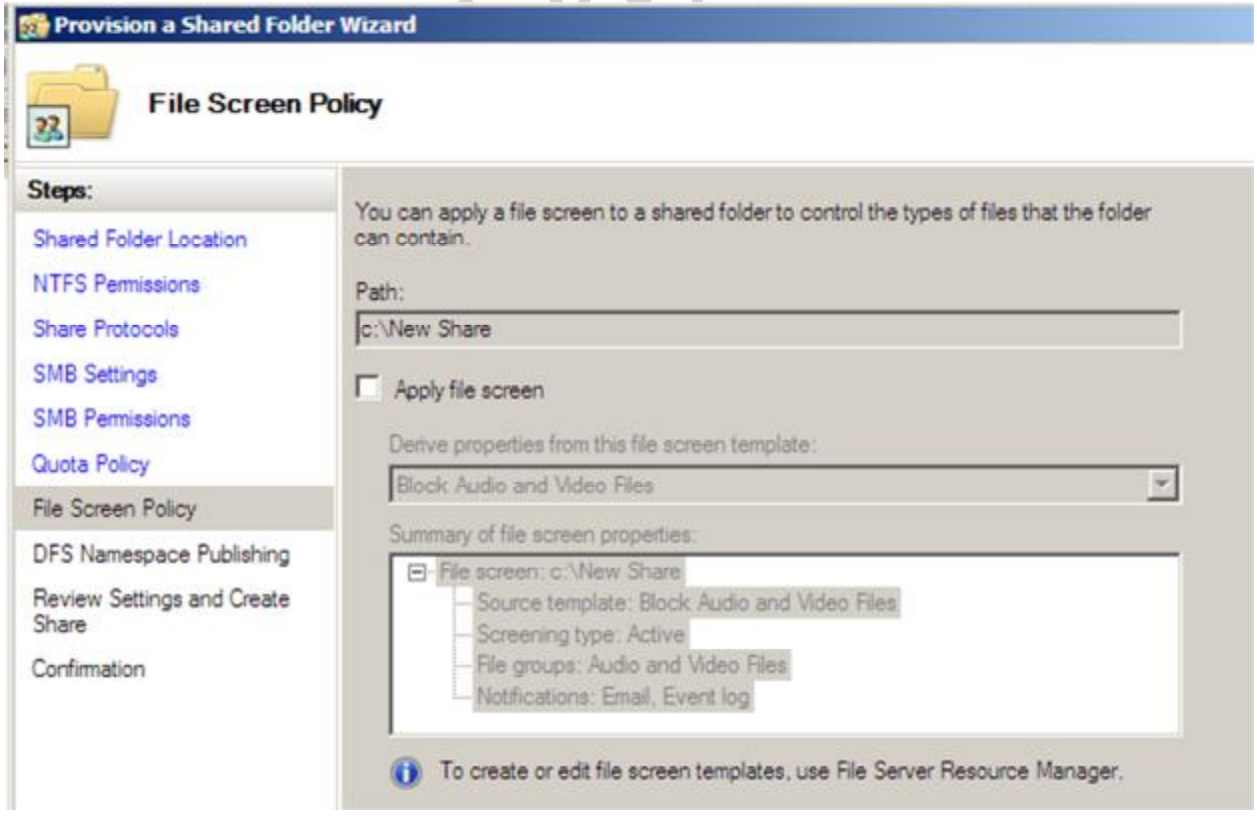


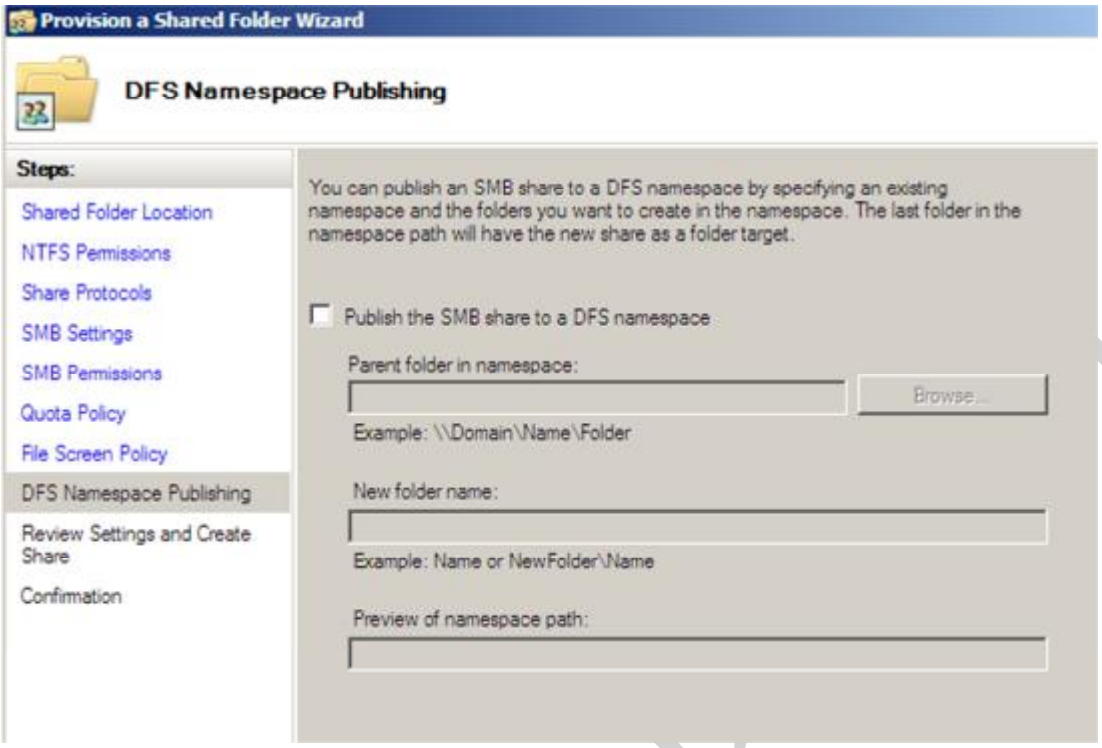

در اینجا می توانیم به SMB Permission دهیم.

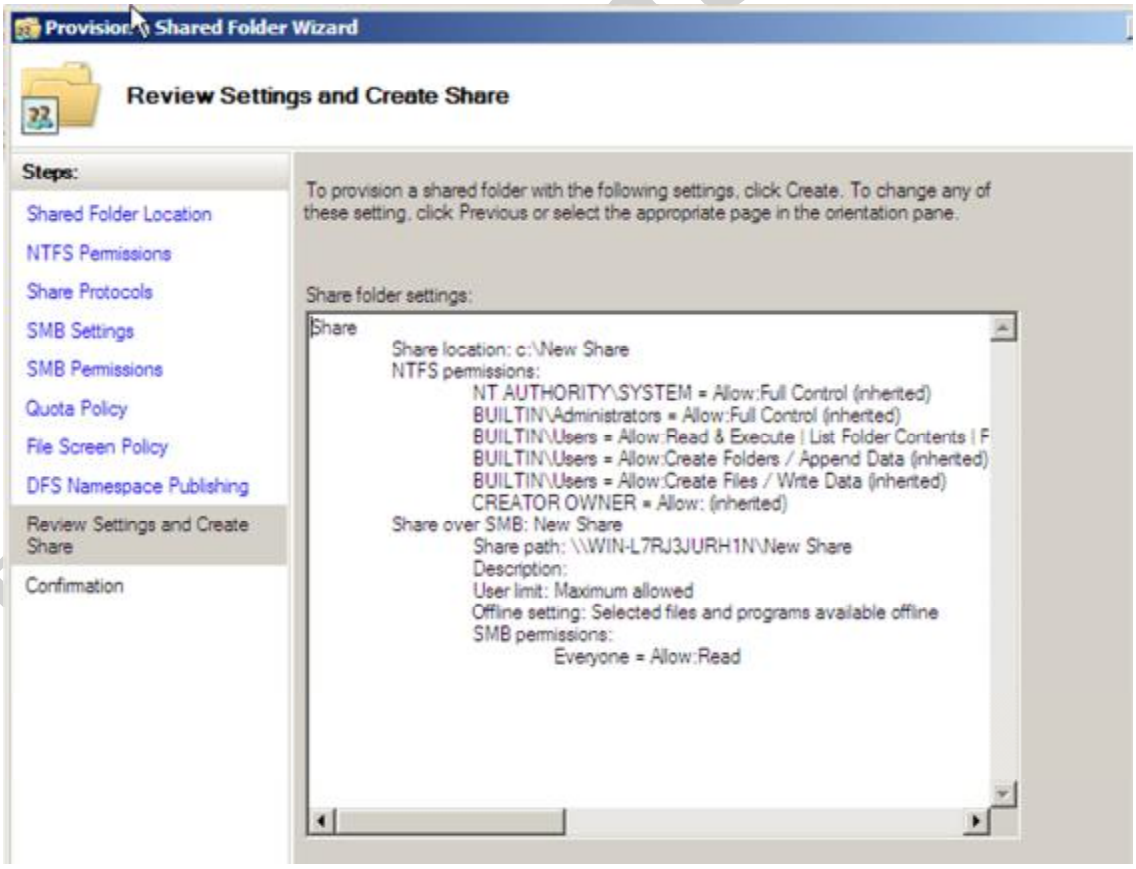


همینطور می توانیم Quota بدهیم






**طی یک Wizzard می توان تمام پارامتر ها را به یک پوشه اعمال کرد.**

Permissions

به اجازه دسترسی به فایلها و فولدرها Permissions گویند و به 3 دسته تقسیم می شوند 1- MAC (Mandatory Access Controle) 2- DAC (Discretionary Access Controle) 3- RBACK (Role Base Access Controle)

MAC : در شبکه هر چیزی( کاربر,کامپیوتر و ....) دارای یک لیبل می باشند,در این لیبل بندی هر کسی دارای لیبل بالا تری باشد به لیبل های پایین تر از خودش دسترسی دارد ولی به لیبل های بالاتر از خودش دسترسی ندارد.

- تنها راه پیاده سازی MAC در شبکه استفاده از برنامه نویسی می باشد.

DAC : هر فولدر دارای قسمتی به نام ACL می باشد که سطح دسترسی هر یوزر به آن فولدر مشخص شده است (همان Tab Security می باشد)

RBACK : به ازای نقشی که یوزر دارد به یک سری از منابع دسترسی دارد ( همان OU می باشد )

- در ویندوز از RBACK,DAC استفاده می شود.

قوانین Permision ها:

1) Permision is Inherited : اگر کاربری به پوشه A دسترسی Full داشته باشد و داخل A هم پوشه B باشد پوشه B از A دسترسی ها را به ارث می برد یعنی به B هم دسترسی Full داریم.
2) Permision on Camulative (ترکیب شونده): وقتی یک یوزر عضو یک گروه باشد که در آنجا دسترسی Write داشته باشد و در گروهی دیگر دسترسی Read این دو با هم ترکیب می شوند.
3) Deny is Precedence : وقتی یک یوزر عضو یک گروه باشد که در آنجا دسترسی Write داشته باشد و در گروهی دیگر دسترسیDenyداشته باشد همیشه دسترسی Deny می شود یعنی دسترسی نداریم.

- 2نوع Permision داریم 1)NTFS 2)SHARE

NTFS: فقط به درایوهایی که به صورت NTFS فرمت شدند می توان اعمال کرد با استفاده از Tab Securityودر حالت Local به کار می رود,که شامل Modify, Write, Read, Full Controleو...

SHARE : فقط برای کسانی به کار می رود که به صورت UNC به Share ها وصل می شوند و شامل دسترسی های Read, Change, Full Controle می باشد.

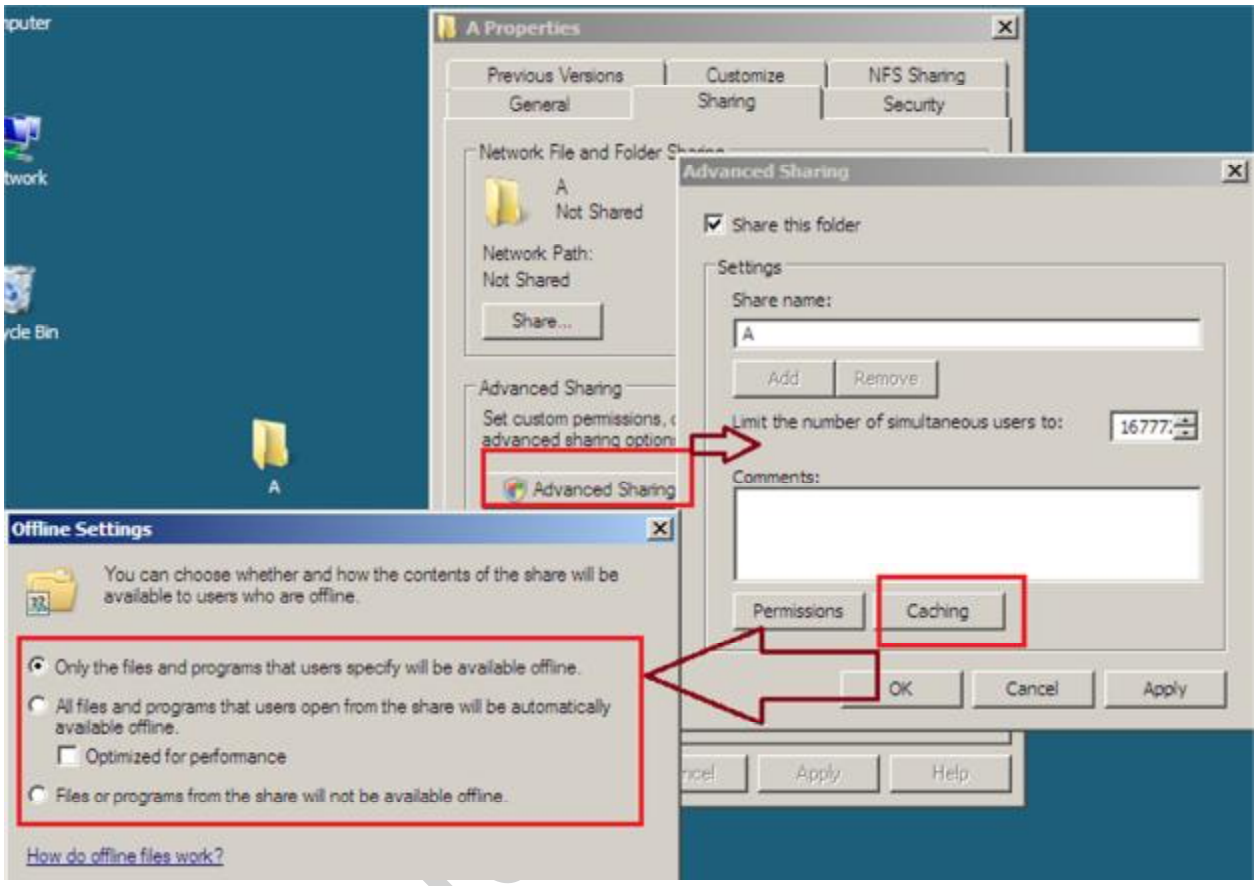
- اگر بر روی یک پوشه هم NTFS و هم SHARE اعمال شود آن Permision که محدودتر باشد بر روی آن اجرا می شود.

FarshidAjabnoush

Offline Share :

**تنظیمات سرویس دهنده**

**ابتدا پشت سیستمی که می خواهیم فولدرش را Shareکنیم می نشینیم و مانند زیر عمل می کنیم**




**اگر گزینه اول فعال باشد Share هایی را که کلاینت مشخص می کند به صورت Offline فعال خواهد شد.**

**اگر گزینه دوم فعال باشد هرفایل Share از سیستم باز شود به صورت اتوماتیک Offline خواهد شد.**

**با فعال بودن Optimizedهیچ فایل اجرایی (exe) از سمت کلاینت به سمت سرور Sync نخواهد شد چون اولین جایی که ویروس ها می نشیند فایل های اجرایی می باشند.**

**اگر گزینه سوم فعال باشد Offline غیر فعال می شود (مانند نرم افزارهای همکاران سیستم)**

- **Offline Share را می توان بین 2 xpیا7 فعال کرد.**
- **بهترین حالت گزینه اول می باشد.**

Farshid

**تنظیمات سرویس گیرنده**

**بین XP و7 تفاوت دارد**

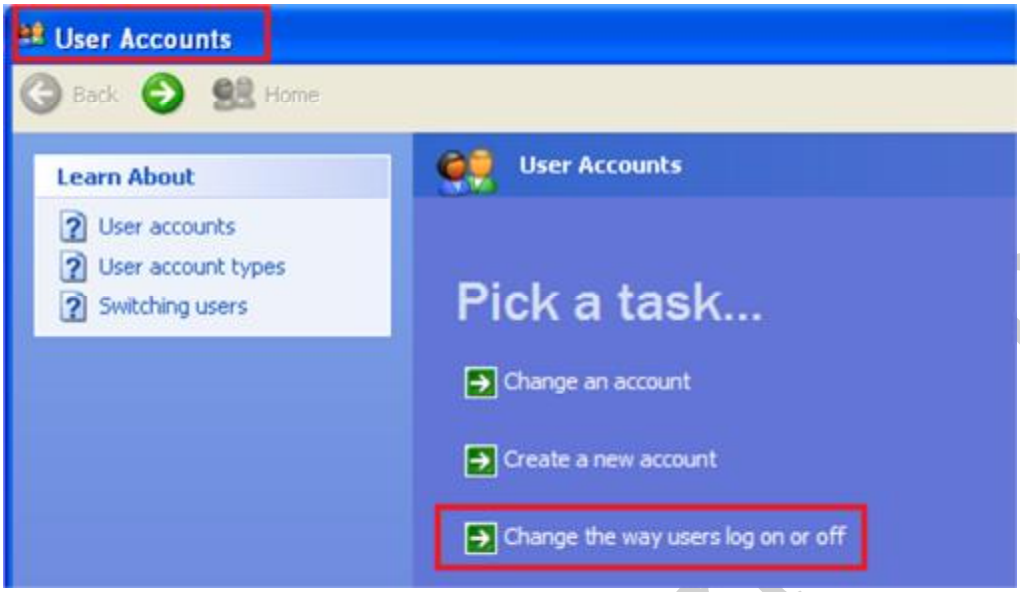
XP

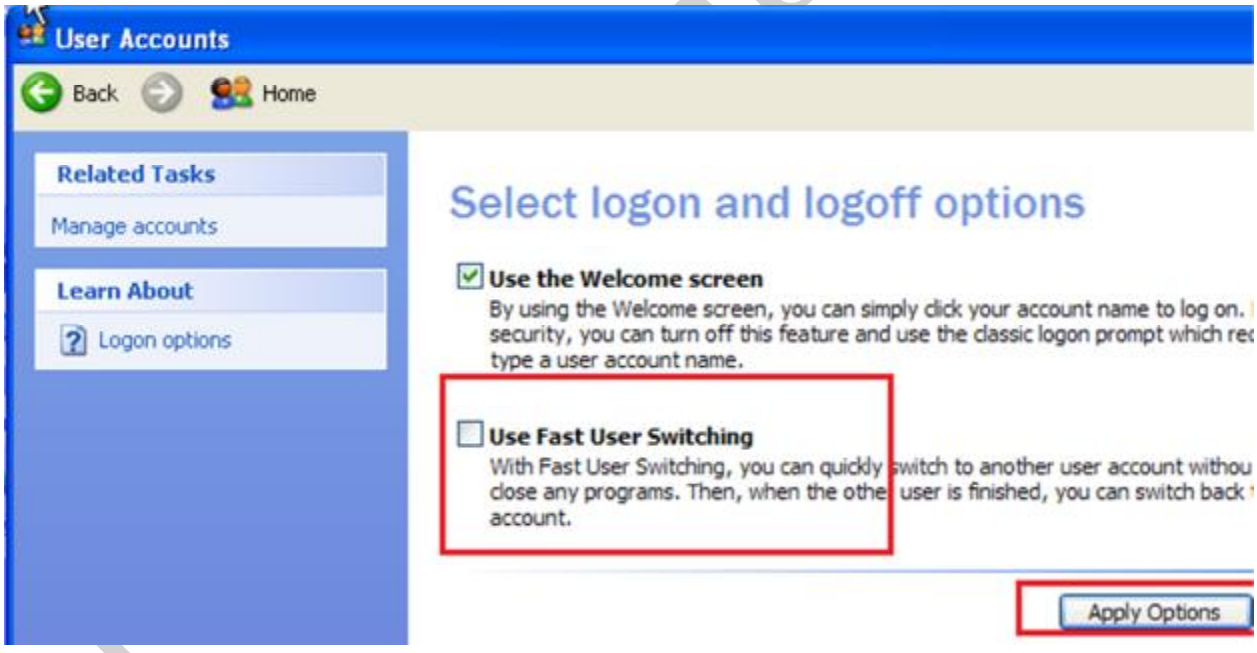
**برای فعال سازی Offline Share مانند زیر عمل می کنیم**

**ابتدا از منوی Tools وارد Folder Options می شویم.**

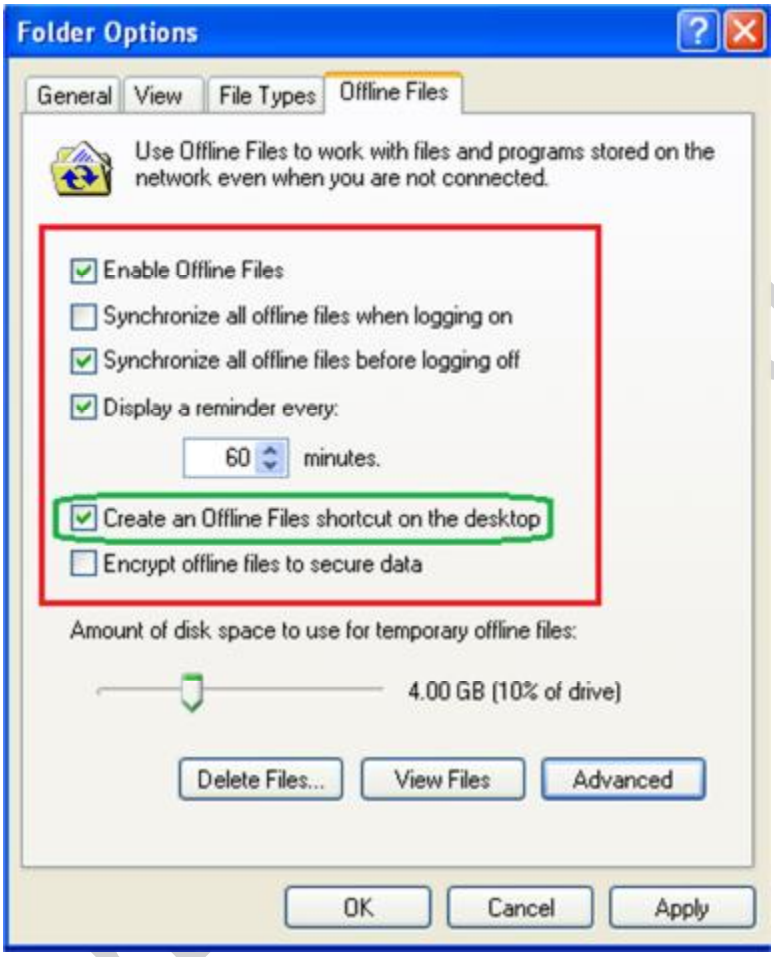
**برای فعال شدن Offline Share باید گزینه Fast User Switchingغیرفعال باشد برای این کار مانند زیر عمل می کنیم.**

Farsh


User Accounts
Back
Home
Learn About
User accounts
User account types
Switching users
User Accounts
Pick a task...
Change an account
Create a new account
Change the way users log on or off


User Accounts
Back
Home
Related Tasks
Manage accounts
Learn About
Logon options
Select logon and logoff options
Use the Welcome screen
By using the Welcome screen, you can simply click your account name to log on.
security, you can turn off this feature and use the classic logon prompt which re
type a user account name.
Use Fast User Switching
With Fast User Switching, you can quickly switch to another user account withou
close any programs. Then, when the othe user is finished, you can switch back
account.
Apply Options

با غیر فعال شدن گزینه بالا می توان از Offline Share استفاده کرد

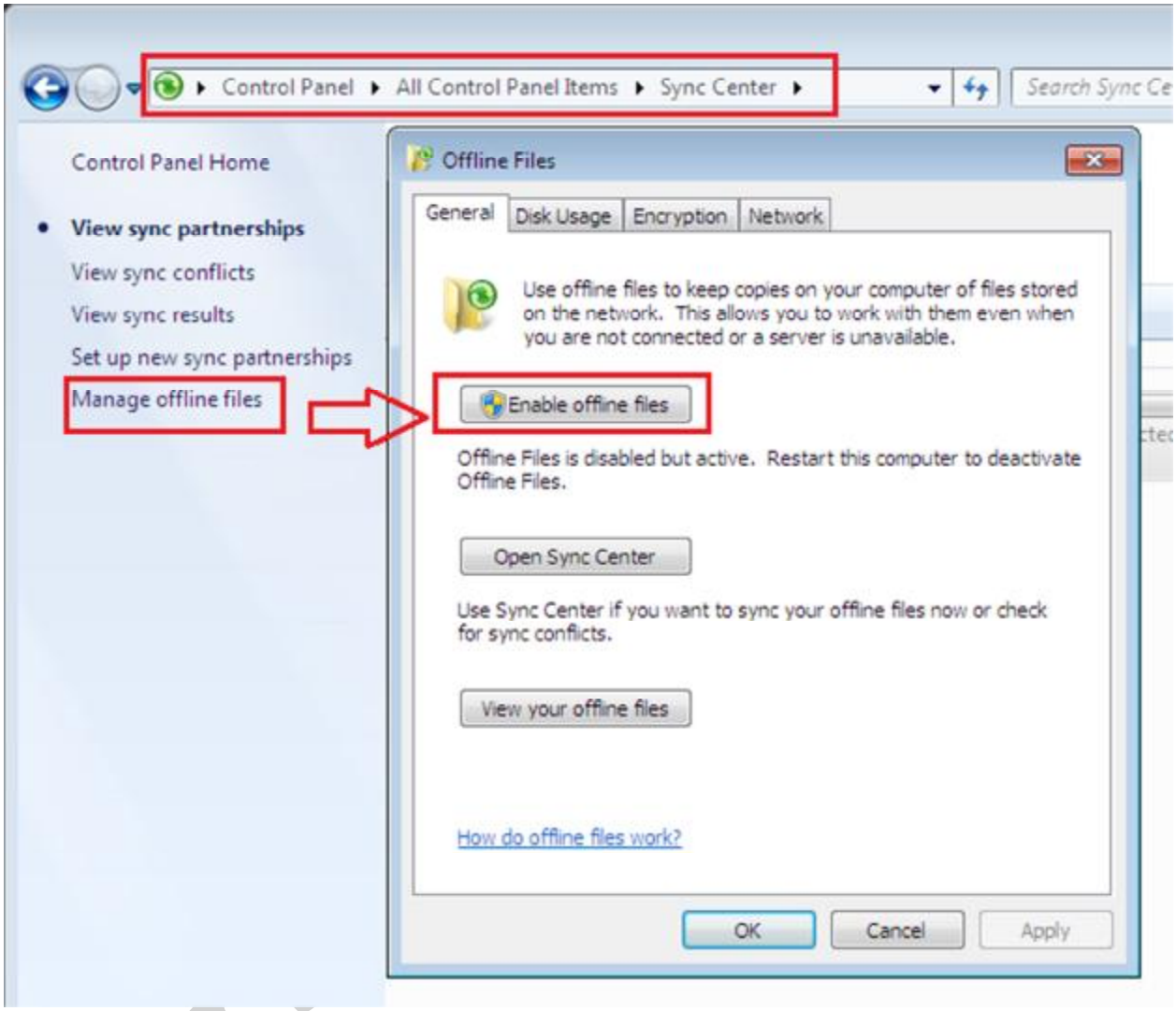



تمامی گزینه مشخص است واحتیاج به توضیح ندارد,فقط گزینه سبز رنگ می گوید از Offline Share یک میانبر بر روی دسکتاپ ایجاد می کند

Farsi Kush

7

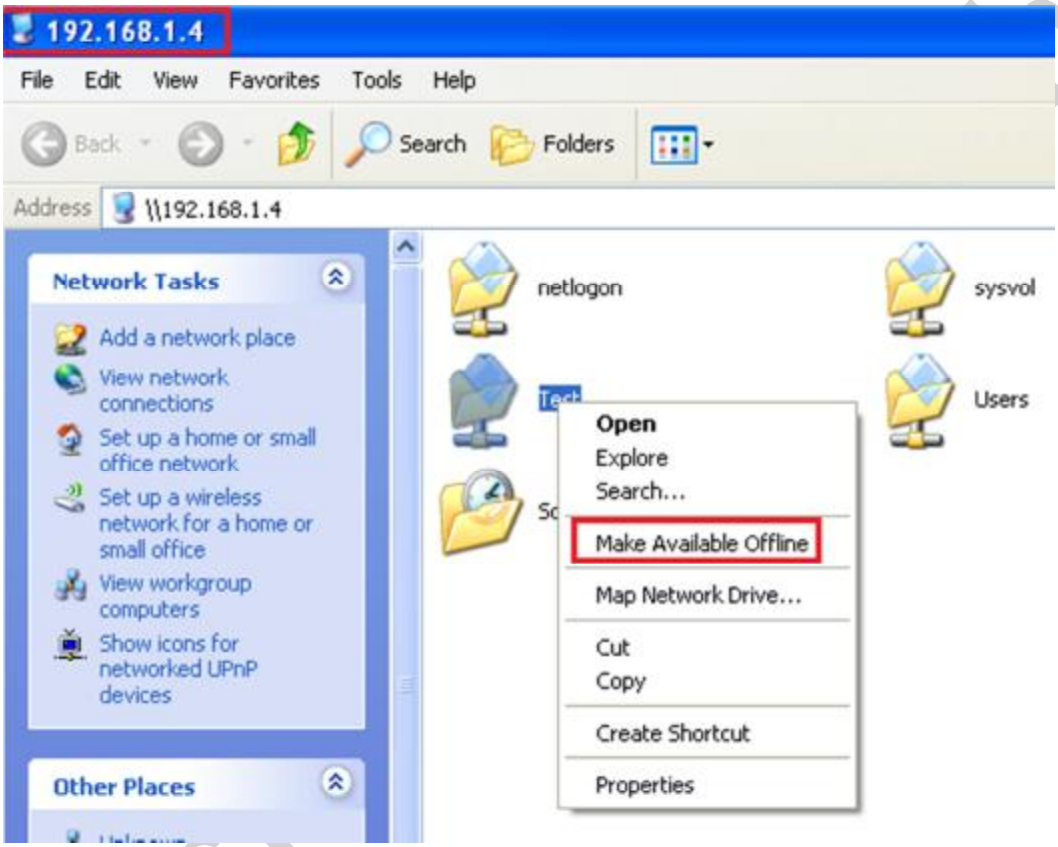
برای فعال سازی Offline Share مانند زیر عمل می کنیم




بعد از فعال کردن Offline Share حتماً سیستم باید Restart شود.

Fa

برای استفاده از فایل هایی که بصورت Offline Share هستند باید ابتدا از یک سیستم دیگر به آنها وصل شویم و بر روی فولدر مورد نظر گزینه ...Make را فعال کنیم.

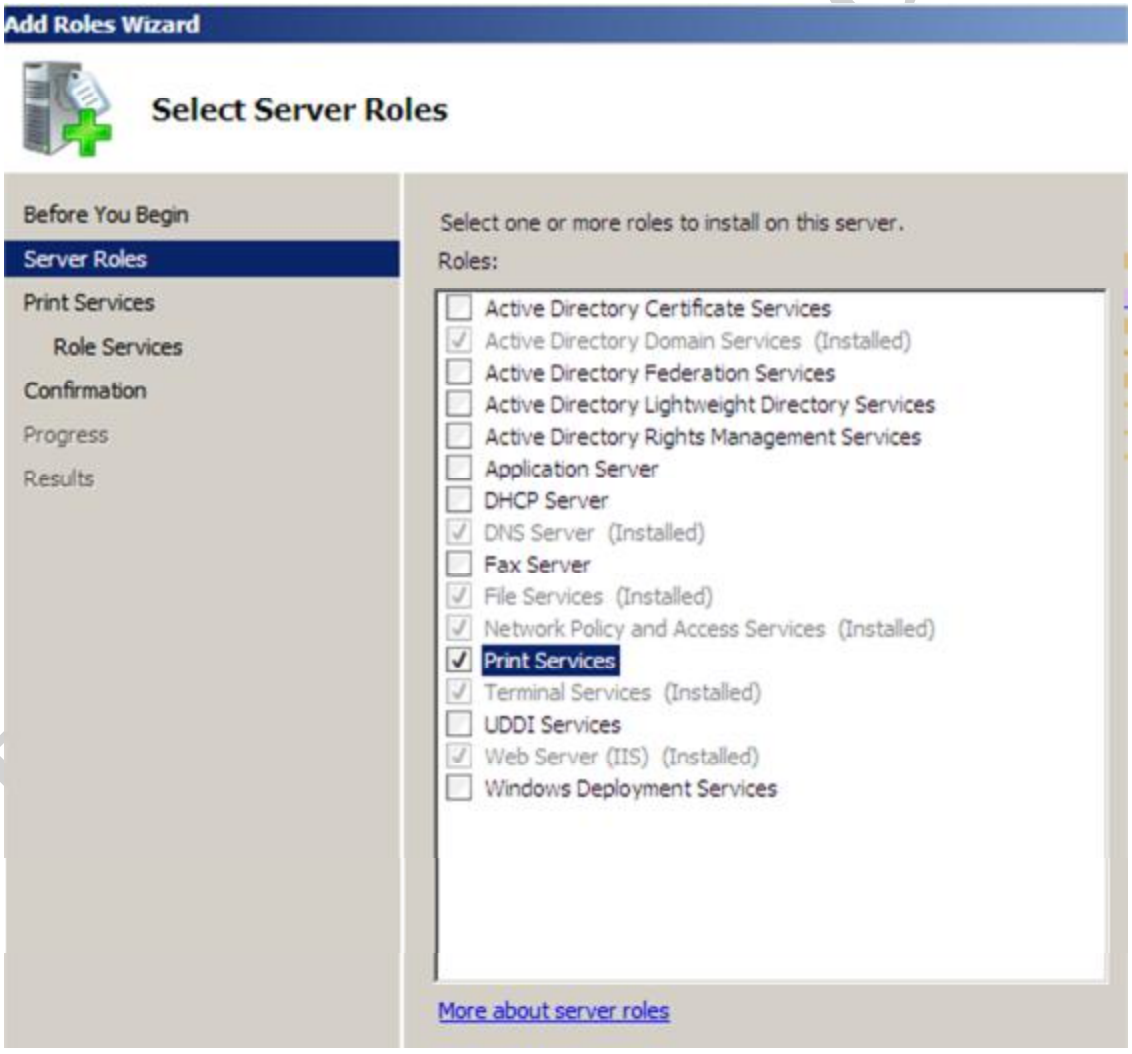


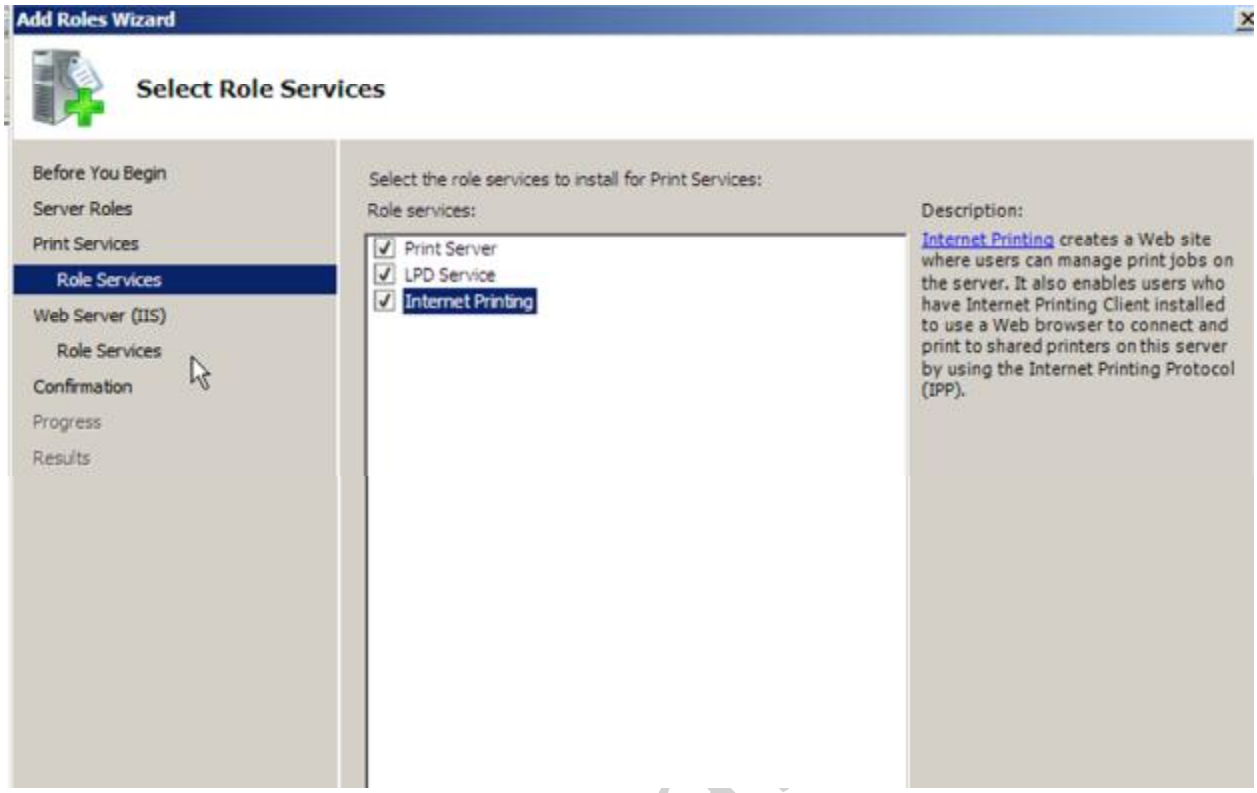

Farsi

1) هر کلاینتی که درایور پرینتر بر روی آن نصب باشد می تواند پرینت ارسال کند.
2) داخل سرور, داخل پوشه Spooler پرینت ها داخل آن Spool می شوند.
3) اگر نوبت به پرینت مربوط به کلاینت برسد از داخل پوشه Spooler به داخل Ram سرور Load شده وبه پرینتر ارسال می شود.

- اگر پرینتر عکس یا متنی را نصفه چاپ می کند یکبار سیستم را ریستارت کنید چون رم سیستم پر شده است.
- اگر سرعت پرینت گرفتن کم شده است درایو C را دیفرگ کنید.

برای نصب پرینت سرور مانند زیر عمل می کنیم






FarshidAja

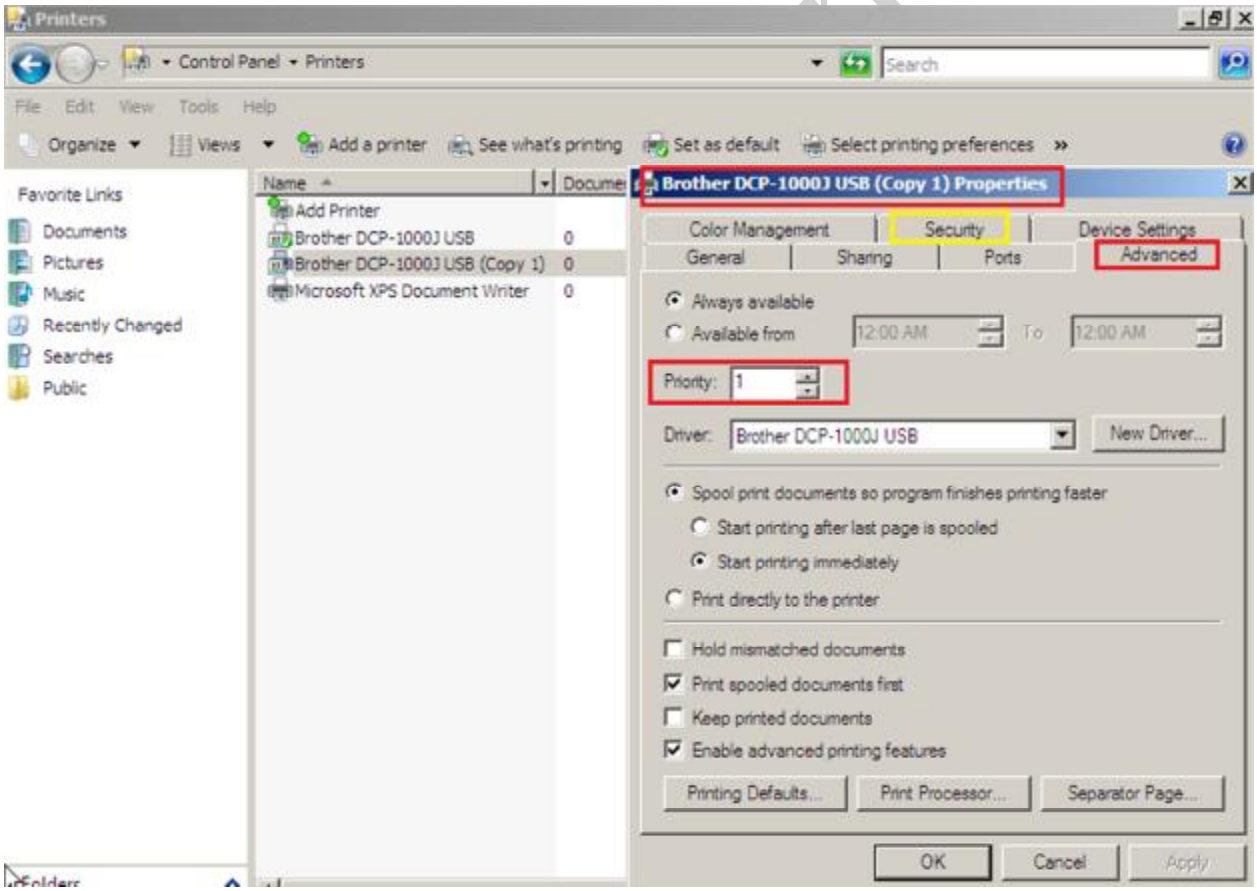
LPD پروتکل پرینت سرور لینوکس می باشد که آن را هم نصب می کنیم که اگر در شبکه, لینوکس وجود داشت بتواند از پرینت سرور استفاده کند,گزینه آخر IPP (Internet Printing Protocol )
هم برای پرینت گرفتن به صورت Webbase می باشد.

- در حال حاضر پروتکل پرینت سرور لینوکس CUPS (Comon unix print server ) می باشد.

**اولویت بندی کلاینت ها**

**ابتدا باید به تعداد اولویت هایمان آیکون پرینتر اضافه کنیم برای این کار همان پرینترمان را یکبار دیگر از داخل کنترل پنل نصب می کنیم .**

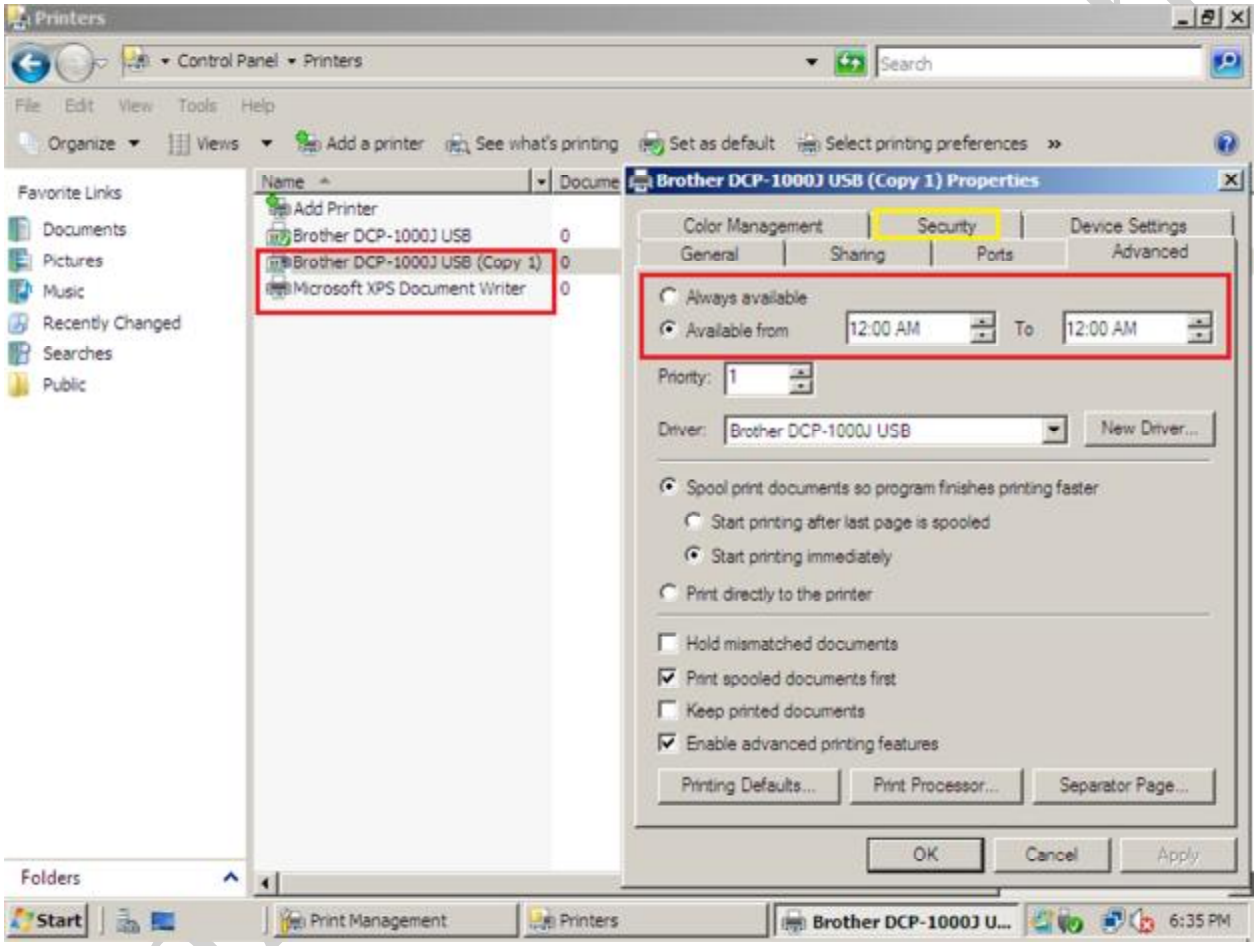
**در این سناریو ما یک مدیر و یک کارمند داریم و می خواهیم مدیر از کارمند زودتر پرینت بگیرد برای این کار روی یکی از آیکون پرینترهایمان پراپرتیز می گیریم وارد ...Adv می شویم و اولویت (Priority ) را تعیین می کنیم هرچه این عدد کمتر باشد اولویت بالاتر می باشد یعنی برای مدیر 1 و برای کارمند2 باید باشد,سپس واردتب Security می شویم و کاربر Every one را پاک می کنیم و کاربر مدیر را اضافه می کنیم حالا پرینت های مدیر به پرینت های کارمند ارجعیت دارد برای کارمند هم باید روی آیکون دیگری پرینتر این کارها را انجام دهیم.**



**زمان بندی پرینت گرفتن**

**برای این کار دوباره باید آیکون پرینتر اضافه کنیم مانند سناریو بالا (کارمند و مدیر) باید بر روی هر آیکون مانند بالا عمل کنیم,در اینجا کارمند از صبح تا بعدازظهر و مدیر تمامی ساعات می تواند پرینت بگیرد.**

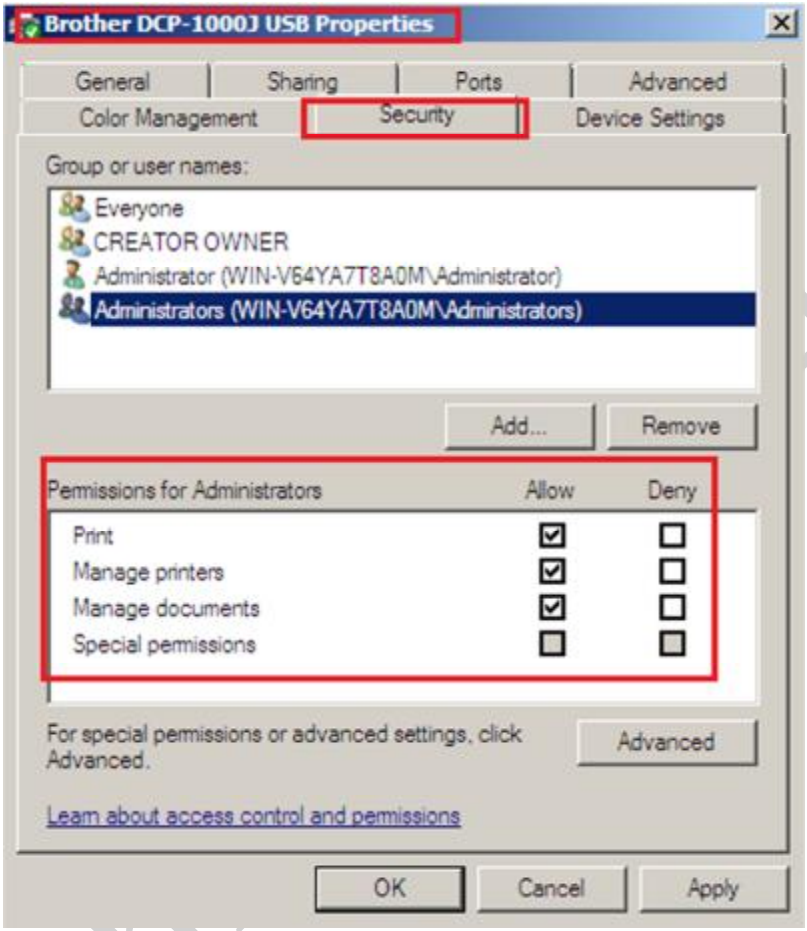
**برای این اولویت دادن یک آیکون برای مدیر و یک آیکون برای کارمند و در تب Security هم یوزر مدیر را مشخص می کنیم.**




**اگر کارمندی در خارج از ساعت تعیین شده پرینت بفرستد داخل پوشه Spooler پرینت آن ذخیره شده و در ساعت مجازش پرینت آن گرفته می شود.**

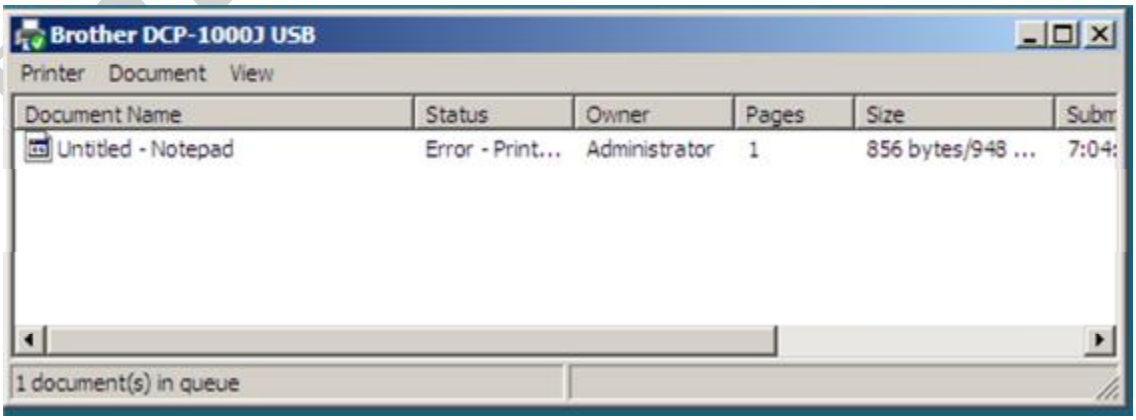
Permission دادن بر روی پرینتر

برای این کار باید وارد Security پرینتر مورد نظر شویم



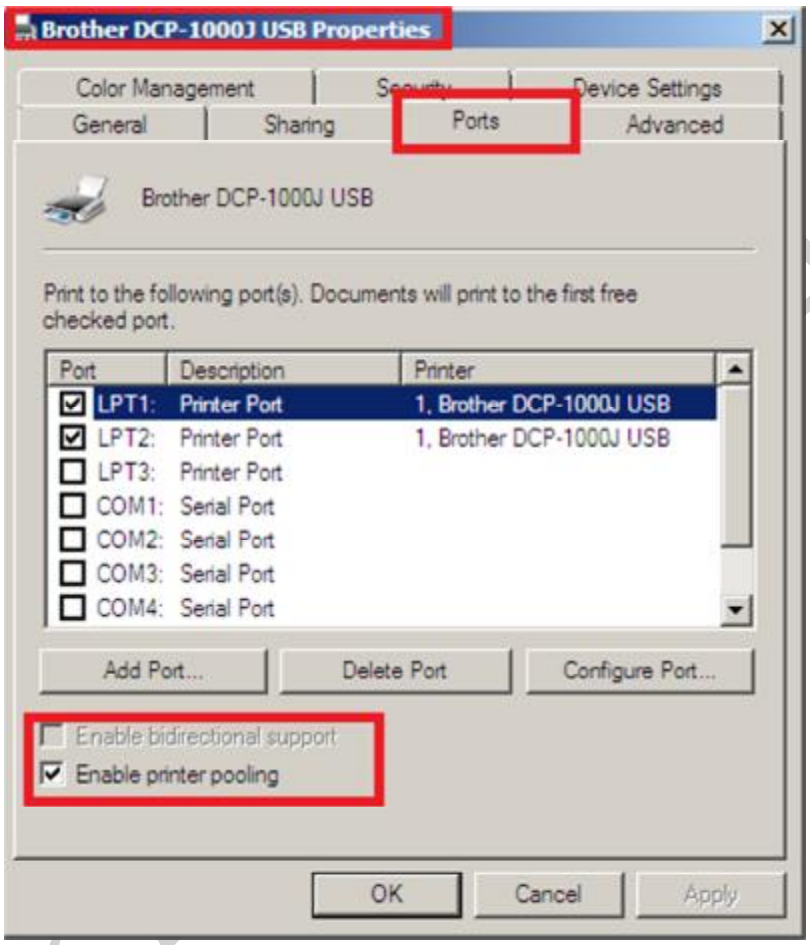

با داشتن دسترسی Manage Printers , می تواند همان پرینتر را در کنسول Print Management مدیریت کند.

با داشتن دسترسی Manage Documents , می توان صفحه زیر را مدیریت کرد.

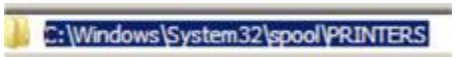


Clustring در پرینتر

برای تقسیم کار در پرینترها باید این کار را انجام دهیم برای این کار هم بهتر است پرینترهایمان یکسان باشد برای این کار باید مانند زیر عمل کنیم .




این کار باید بر روی هر 2 پرینتر انجام شود.

- برای قفل کردن IP از نرم افزار Kerio استفاده می کنیم,قابل دانلود از سایت Manage engine.com
- مسیر پوشه Spool داخل 

می باشد,بهتر است این مسیر را تغییر دهیم.
- هرگاه مشکلات پرینتر زیاد شد یکبار سرویس Spoolsv.exe را دوباره اجرا می کنیم از Taskmanager

( Internet Protocol Security) Ipsec

پروتکل امنیتی است که می تواند اطلاعات را هنگام عبور از شبکه امن کرده و جلوی Sniff غیر مجاز آنها را بگیرد.

برای ایجاد امنیت بر روی اطلاعات در شبکه از 3 روش استفاده می شود

- IPSEC : از این روش بیشتر در شبکه های LAN استفاده می شود به این دلیل که Header که به اطلاعات ما می خورد حجمش بالا بوده از این رو احتیاج به شبکه با سرعت با لا داریم.
- VPN : بیشتر در شبکه های LAN,WAN استفاده می شود.
- SSL)CERTIFICATE ( : بیشتر در شبکه هاWAN استفاده می شود.

IPSEC

تشکیل شده است از ISA KMP-AH- ESP که خود ISA KMP از Phase1,2 تشکیل شده است.

- هر پکت داخل شبکه از 4 قسمت تشکیل شده است 1- ( Check Sum) CRC 2- DATA (PayLoad) 3- FRAME TYPE 4- Ip HEADER
- در FRAME TYPE اطلاعات لایه2 قرار می گیرد (مک آدرس)
- Ip HEADER لایه3
- IPSEC اطلاعات را با (Encapsolution Security Payload ) ESP رمزنگاری می کند.
- Ip HEADER و FRAME TYPE را هم با (Authentication Header ) AH رمز می کند.
- زمانی که Ipsec با Esp اطلاعات را رمز کند به آن نوع از Ipsec , Transparent گویند.
- زمانی که Ipsec با EspوAh اطلاعات را رمز کند به آن نوع از Ipsec ,Tunnel Mode گویند.
- در شبکه های ما یکروسافت از Transparent استفاده می شود.
- در اینترنت از AH به دلیل امنیت بالا استفاده می شود و در شبکه ها از ESP به دلیل سرعت بالا استفاده می شود.
- Ipsec از پورت 50,51 استفاده می کند.
- برای اینکه بتوانیم ایمیلی بدون بجا گذاشتن ردپا بزنیم باید از نرم افزار PGP استفاده کنیم,باید بر روی هر2 کامپیوتر نصب باشد.

ISAKMP

یک فرآیندی می باشد که طی آن طرفین همدیگر را شناسایی می کنند(فاز1)و بعد از شناسایی تصمیم می گیرند که با کدام پروتکل اطلاعات را رمز نگاری و Hash کنند.

FarshidAjabnoush

- در رمز نگاری به این صورت عمل می شودکه مثلاً حرف A توسط یک سری کلیدهای رمز نگاری تبدیل به 123 در مبداء می شود و در مقصد هم دو باره توسط کلیدهای رمز نگاری به همان A تبدیل می شود.
- Encryption به معنای رمزنگاری می باشد.
- Hash در این روش توسط نرم افزاری به نامMD5-SUM , Hash یک فایل مانند a.exe حساب می شود اگر این فایل را در هر جایی ببریم Hash آن ثابت است ولی اگر داخل فایل a چیزی اضافه یا کم شود Hash آن هم تغییر خواهد کرداستفاده از این روش برای دانلود فایل از اینترنت مناسب است چون اگر Hash را که سایت برای فایل موردنظرش معرفی کرده با Hash که خودمان بعداز دانلود بدست آوردیم برابر نباشد بدین معنی است که کسی در حین دانلود ما چیزی به این فایل اضافه یا کم کرده است.
- در Hash از پروتکل های MD5,SHA استفاده می شود.

3 روش شناسایی در فاز1 IPSEC وجود دارد

1- Kerberos: پروتکل احراز هویت در شبکه های دامینی می باشند(یعنی تشخیص می دهد که 2 سیستم عضو یک دامین هستند)
2- Certificate: یکCAسرور در شبکه قرار می گیرد که به همه Certificate می دهد.
3- Pre-sharedKey: باید در 2 طرف یک رمز تنظیم شود و آن رمز را هم زمان ارسال فایل از 2 طرف می خواهد (مانند بلوتوث),به مکانیزم مبادله کلیدها IKE(Internet Key Exchange) گویند و به پروتکل مورد استفاده DH (DeffyHelman) گویند.

اساس کار Ipsec بر حسب پالیسی می باشد با استفاده از این پالیسی ها تعیین می کنیم چه نرافیکی به چه نحوی امن شود در ویندوزهای xp,98 سه پالیسی برای این کار وجود دارد ولی در 7 این پالیسی ها وجود ندارد و باید این پالیسی ها نوشته شود.

3پالیسی عبارتند از 1-Client (Respond only) 2-Server ( Request Security) 3- Secure Server (Require Security)

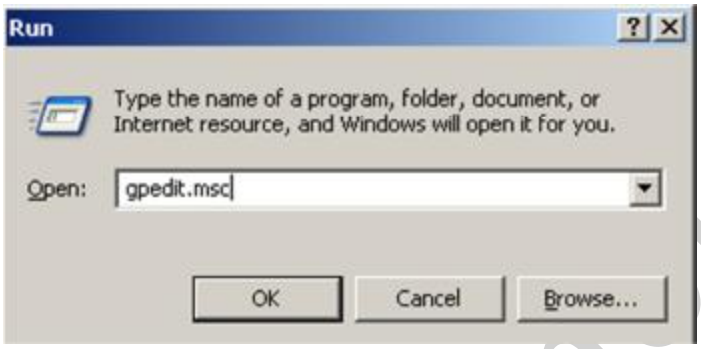
فعال سازی IPsec یعنی اعمال یکی از این پالیسی ها

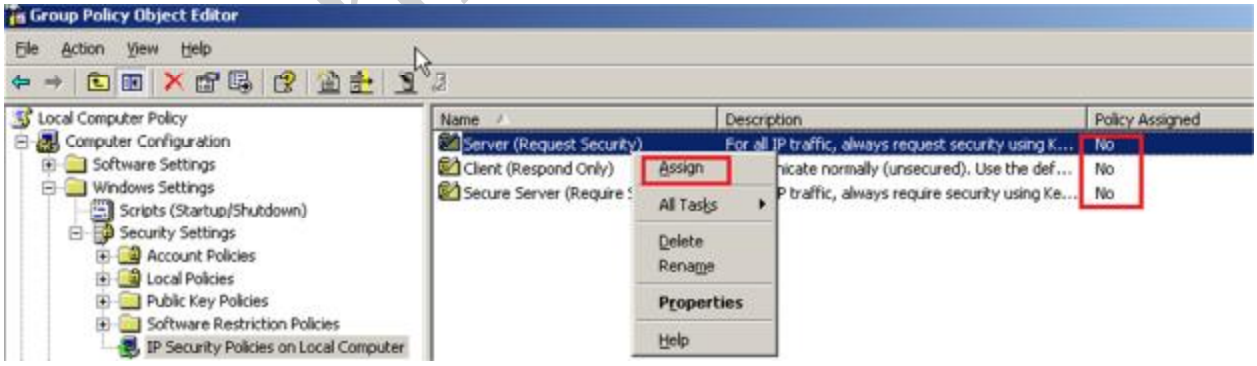
- اگر بر روی کلاینتی پالیسی نوع 1 فعال باشد می تواند به درخواستهای Ipsec جواب دهد ولی خودش نمی تواند از کسی درخواست برقراری ارتباط با Ipsec را داشته باشد.
- با فعال بودن نوع2 از پالیسی, آن سیستم می تواند به درخواست های ارتباط با Ipsec پاسخ دهد و خود می تواند از سیستم دیگری درخواست ارتباط با Ipsec داشته باشد اگر سیستم مقابل Ipsec ساپورت کند با آن ارتباط برقرار می کند و اگر ساپورت نکند به صورت ساده ارتباط برقرار می کند.

FarshidAjabnoush

- با فعال بودن نوع3 از پالیسی, آن سیستم می تواند به درخواست های ارتباط با Ipsec پاسخ دهد و خود می تواند از سیستم دیگری درخواست ارتباط با Ipsec داشته باشد اگر سیستم مقابل Ipsec ساپورت کند با آن توسط Ipsecارتباط برقرار می کند و اگر ساپورت نکند ارتباط برقرار نمی کند.

Ipsec در ویندوزهای Legacy

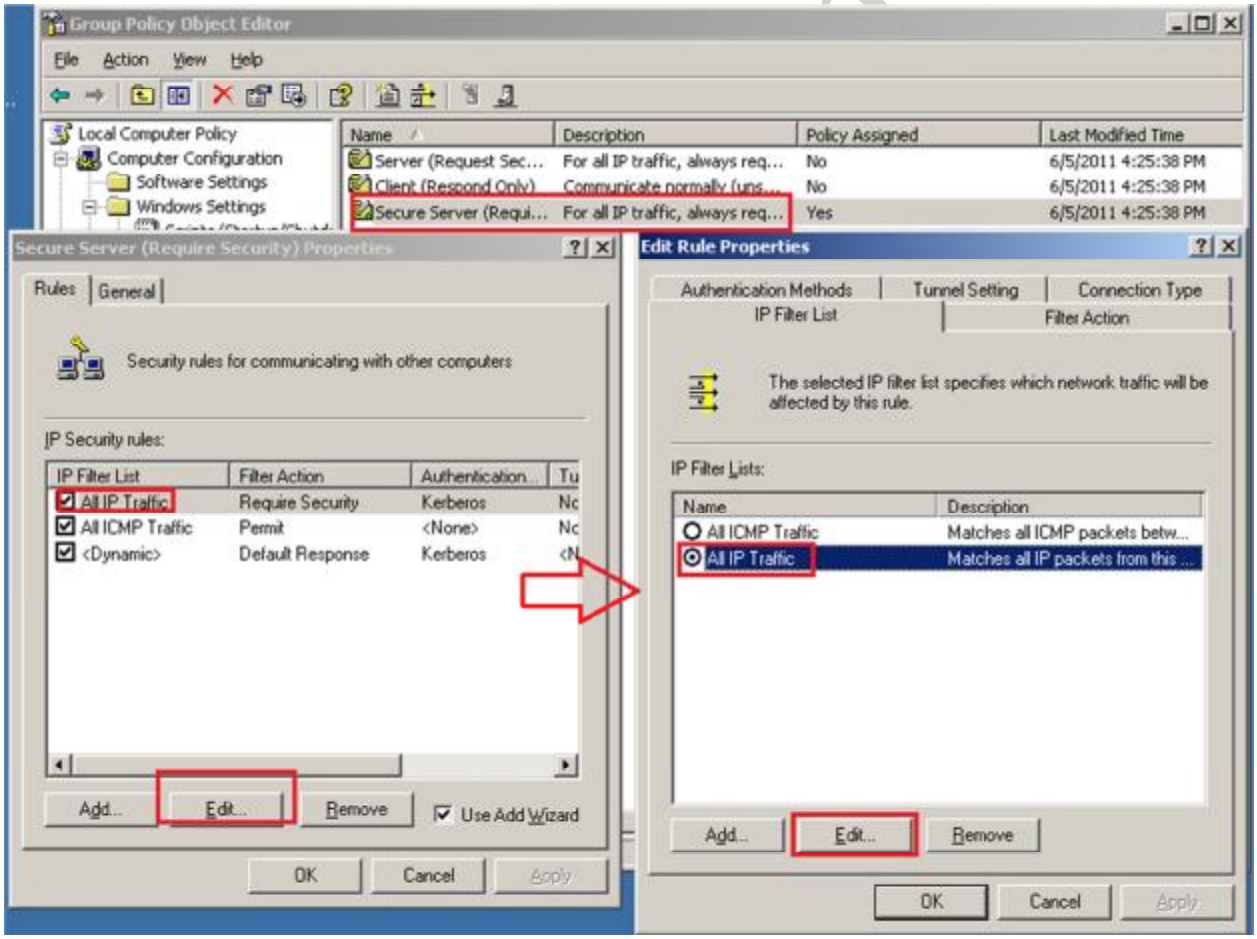


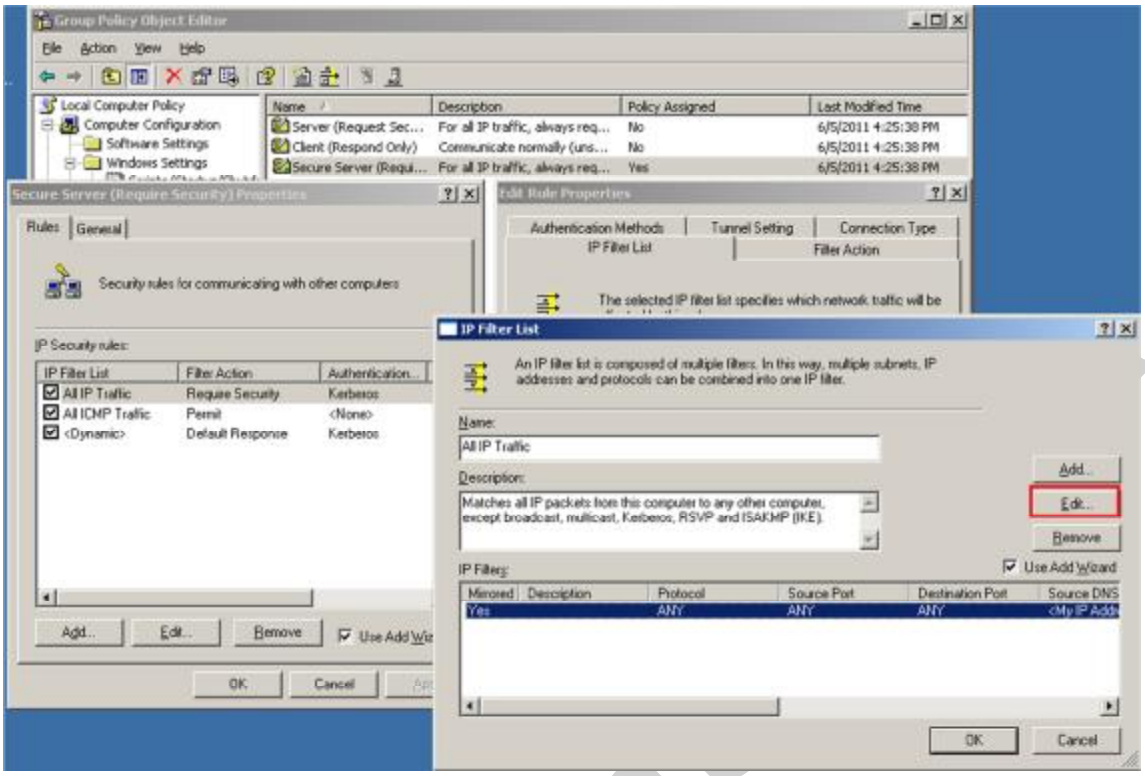


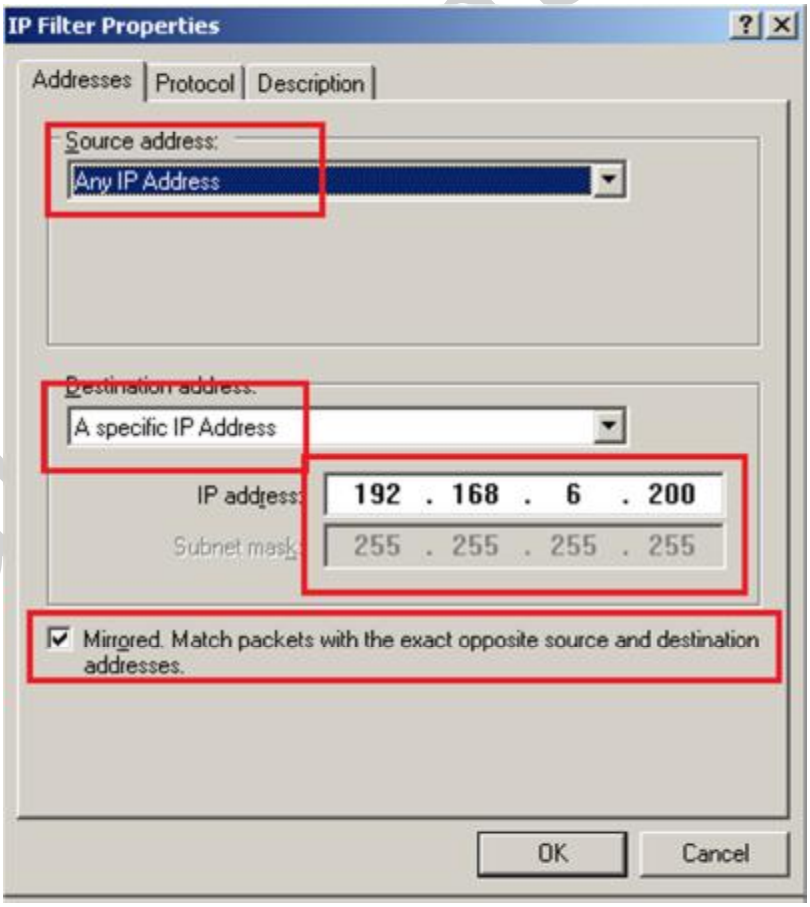

- برای فعال سازی باید بر روی یکی Assign کنیم.
- فقط یکی از 3 پالیسی را می توان فعال کرد.
- نوع فعال سازی در ویندوزهای Legacy تفاوتی با هم ندارند,فقط باید در هر دو طرف فعال باشد اگر از نوع 3 استفاده کنیم.

- بهتر است Ipsec را بر روی ترافیک های مهم فعال کنیم,به ترافیک هایی که در هنگام وصل شدن از ما یوزر پسورد می خواهد ترافیک های مهم گویند,به این دلیل این کار انجام می شود که ترافیک شبکه بیخودی بالا نرود.
- Ipsec به صورت پیش فرض بر روی همه ترافیک ها فعال می باشد.
- ترافیک های مهم 2 نوع می باشند 1- All Ip Traffic 2- All Icmp Traffic
- ترافیک های مربوط به پروتکل Icmp مانند دستور پینگ مربوط به All Icmp Traffic می باشند.
- هر ترافیکی که به All Icmp Traffic مربوط نباشند جزو All Ip Traffic می باشند(مانند http,RDP )
- بیشترین ترافیک ها مربوط به All Ip Traffic می باشند.
- ازIpsec در شبکه های داخلی استفاده می شود,بر روی اینترنت از VPN استفاده می شود.

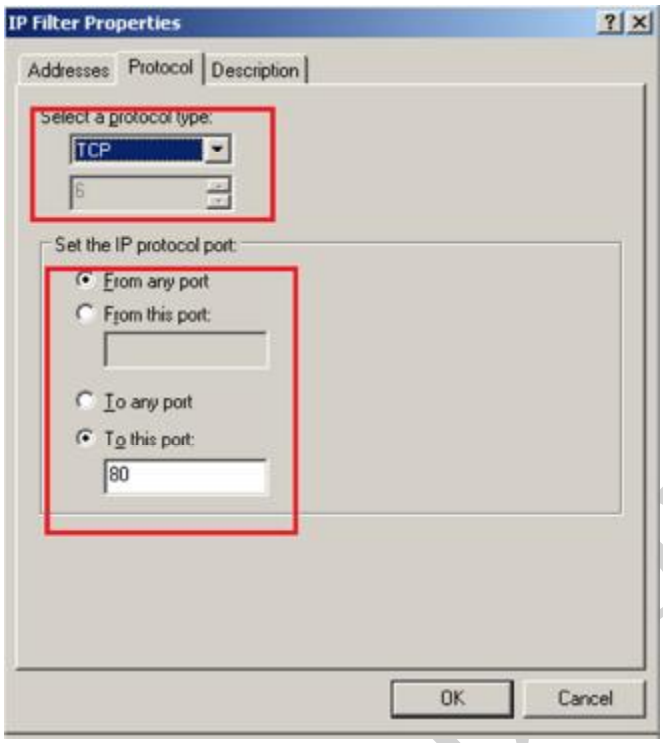
برای فعال سازی Ipsec مانند زیر عمل می کنیم



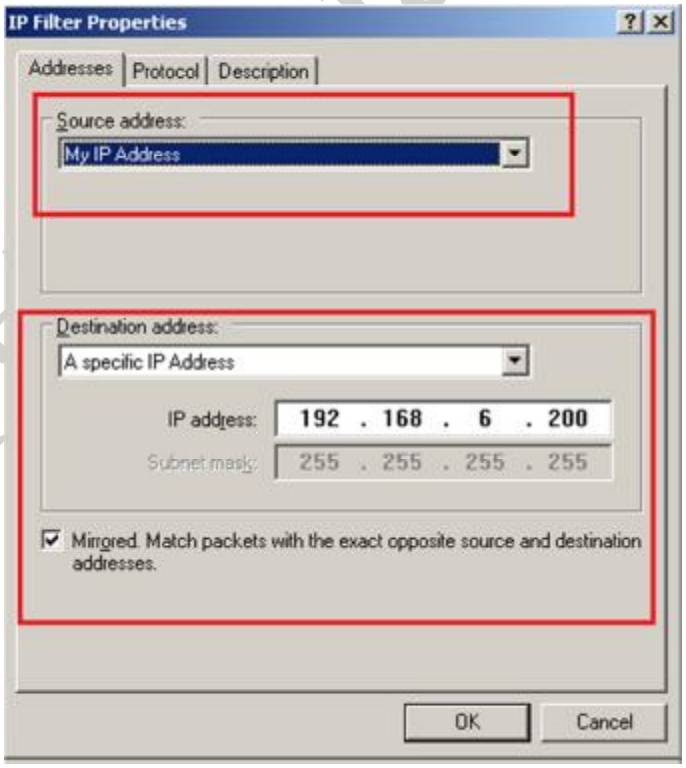


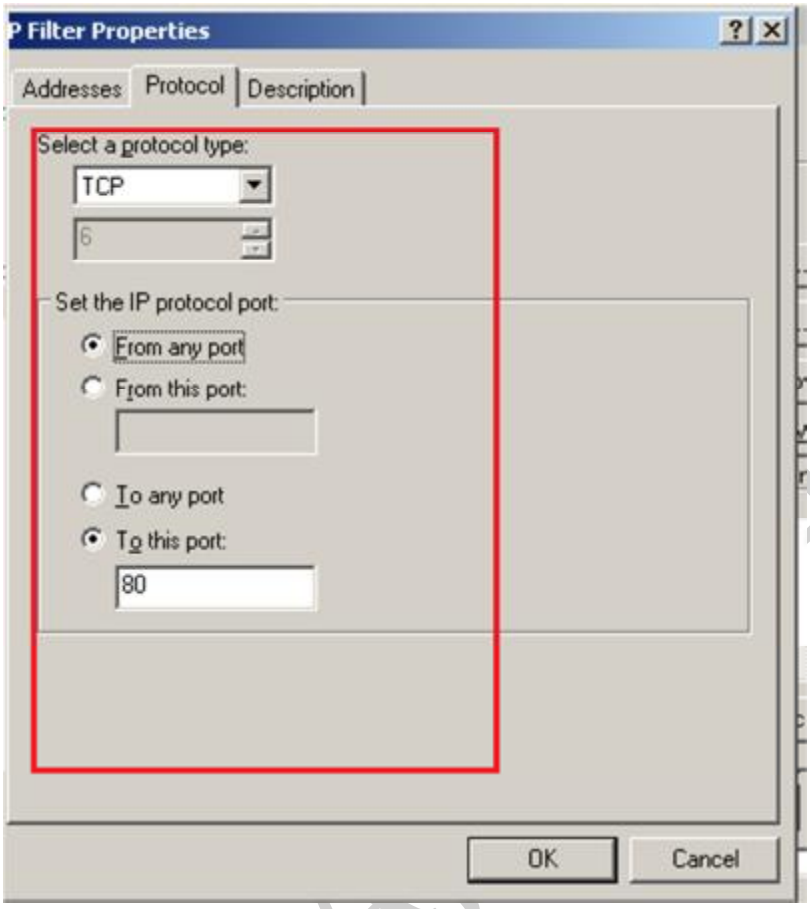

**گزینه آخر باید فعال باشد که ترافیک های ردوبدل شده میان سرور و کلاینت رمز باشند.**




نوبت به تنظیمات پشت کلاینت می رسد:



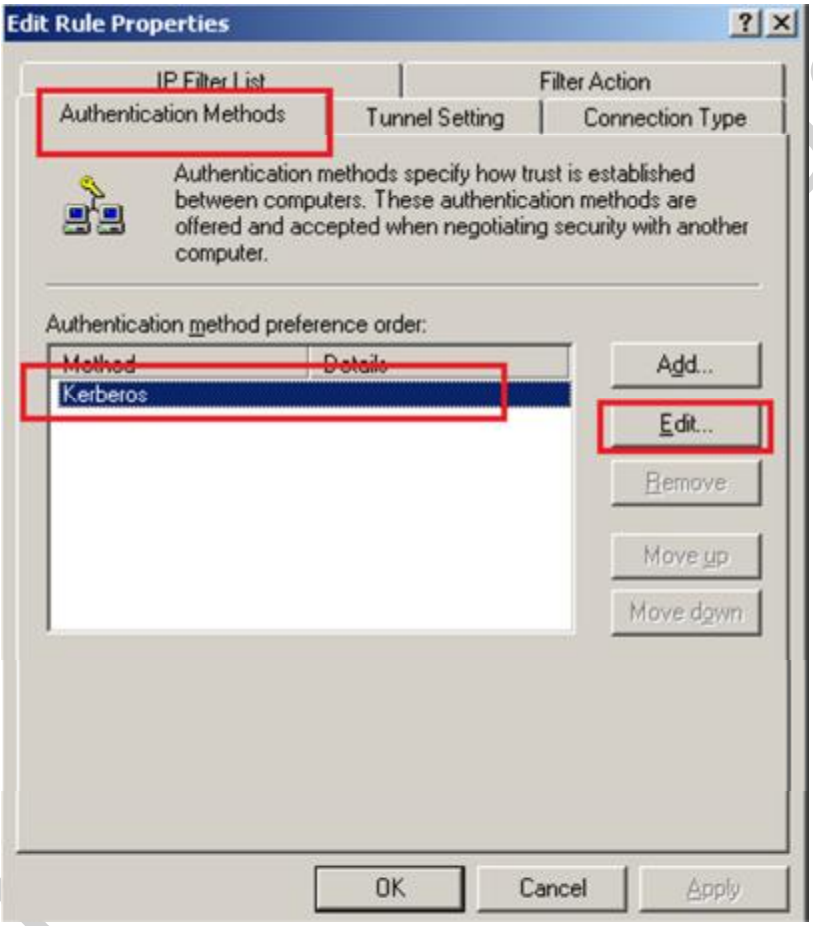

Farsiabzush




- در شبکه های دامینی تنظیمات فقط پشت سرور اعمال می شود ولی در شبکه های WorkGroup باید پشت کلاینت هم اعمال شود.

FarshidAsh

- برای اینکه کلاینت و سرور بتوانند ارتباط برقرار کنند باید توسط یک پروتکل همدیگر راشناسایی کنند که این پروتکل باید در 2 طرف یکسان باشد در شبکه های دامینی پروتکل استفاده شده Kerberos و در شبکه های WorkGroup پروتکل استفاده شده Pre-SharedKey می باشد.




Farsh

نحوه نوشتن Ipsec Policy در NextGeneration

هر Ipsec Policy از 5 قسمت تشکیل شده است

1- Ip Filter List : در این قسمت مشخص خواهیم کرد که چه ترافیکی را می خواهیم امن کنیم(ICMP-ALL IP)

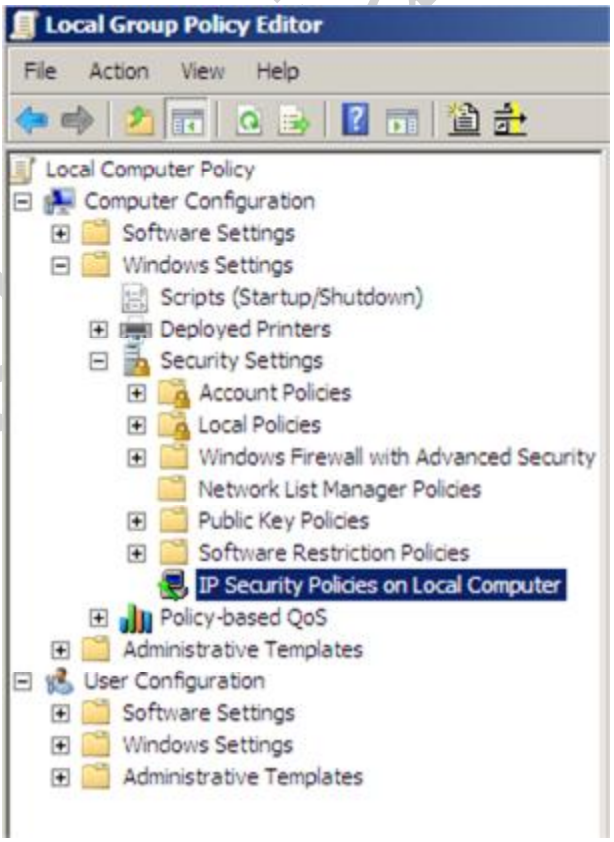
2- Filter Action : مشخص خواهیم کرد در مواجهه با ترافیک مشخص شده چه واکنشی باید نشان دهد(Permit-Reguest Security-Require Security )

3- Authentication Methods : مشخص خواهیم کرد که طرفین چگونه همدیگر را شناسایی کنند(Kerberos-Certificate-pre-shared key )

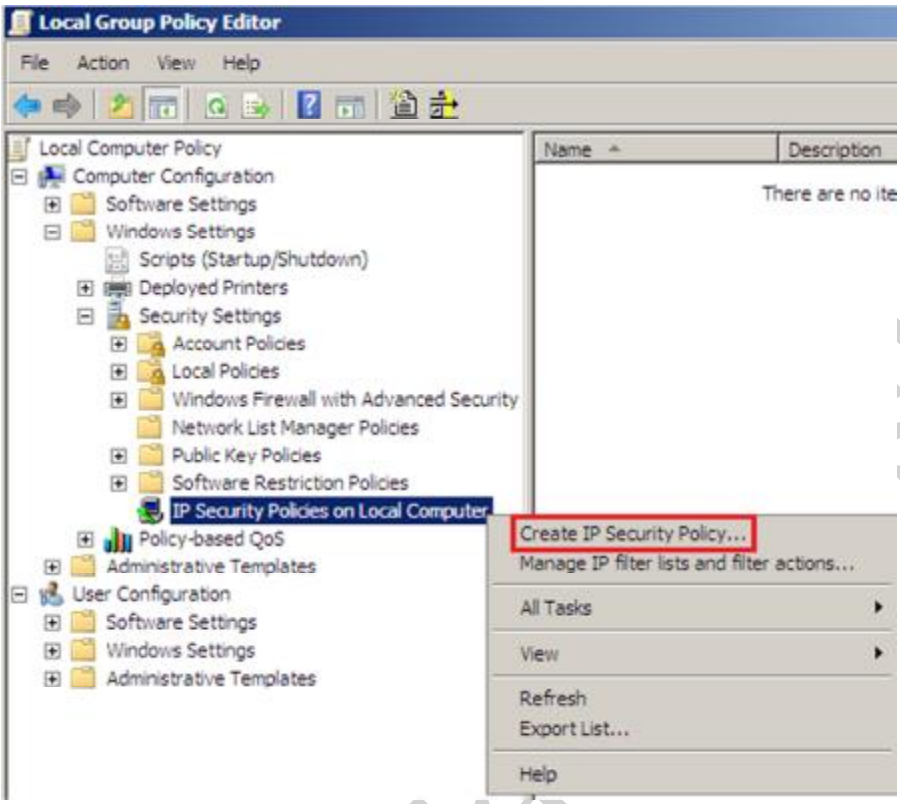
4- Tunnel Setting : مشخص خواهیم کرد برای ارتباط Ipsec نقطه انتهایی (Endpoint ) وجود دارد؟ مانند : ما 3 شعبه تهران قزوین تبریز داریم ارتباط از تهران تا قزوین به صورت Ipsec می باشد و از قزوین تا تبریز بدلیل پایین بودن پهنای باند ارتباط به صورت ساده می باشد, در اینجا سرور قزوین Endpoint ما می شود.

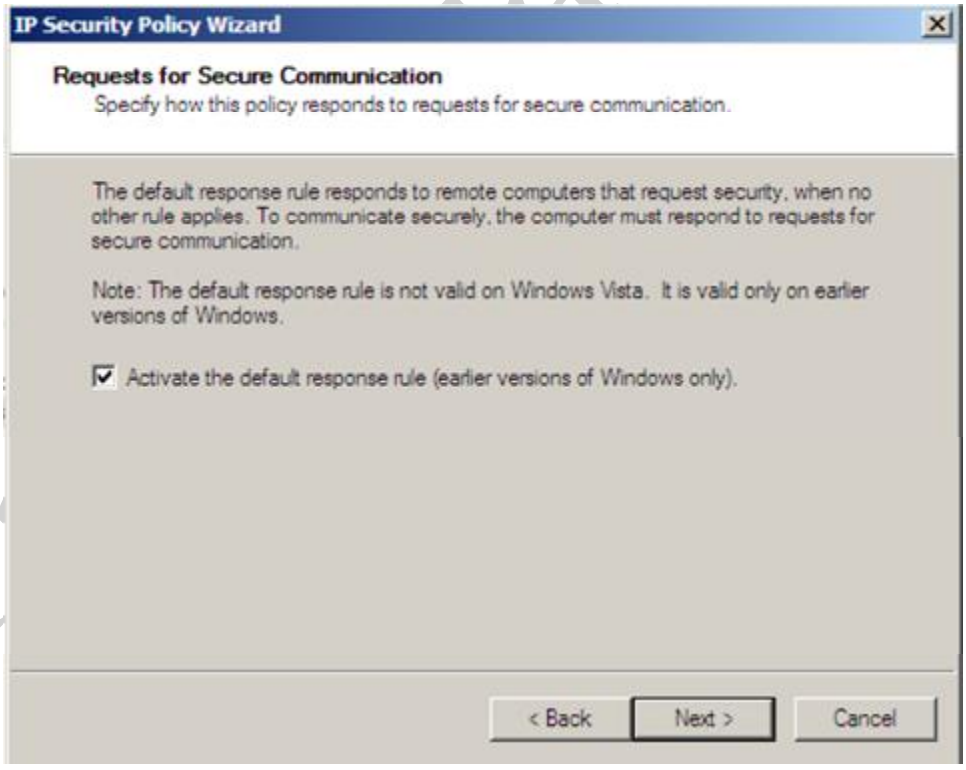
5- Connection Type : مشخص خواهیم کرد که اگر اطلاعات ما که داخل شبکه به صورت Ipsec با هم ارتباط دارند به شبکه WAN رفت Ipsec در آنجا (WAN ) هم فعال باشد یا نه؟

- ابتدا وارد گروپ پالیسی می شویم

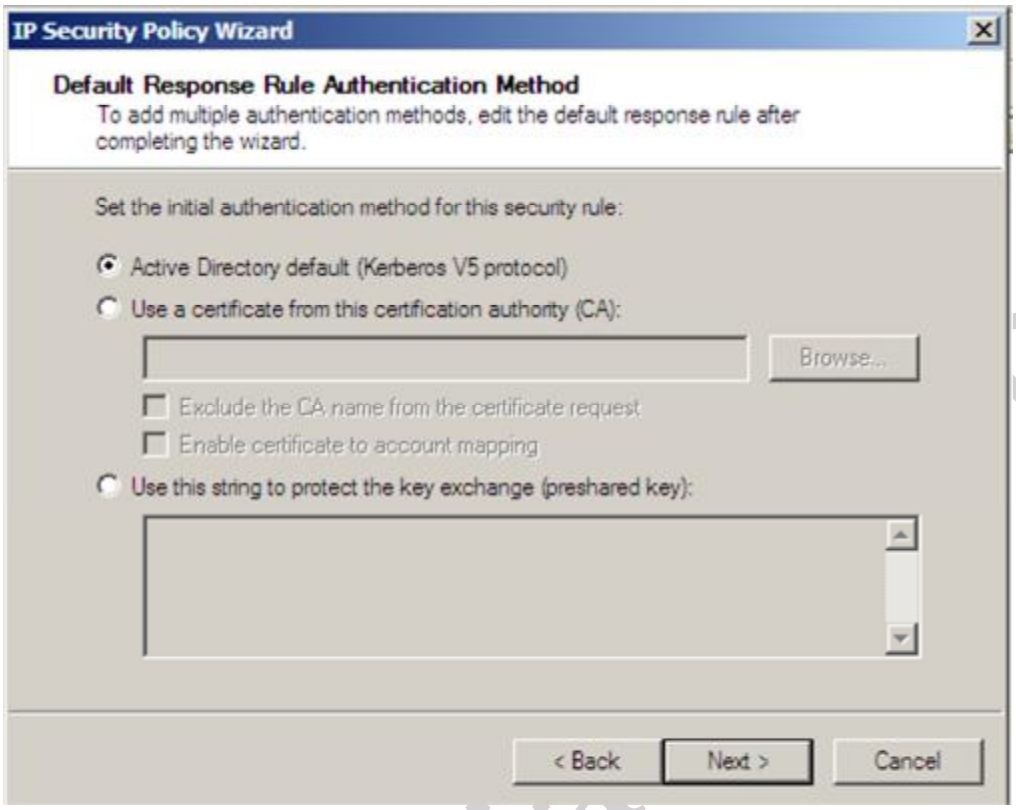



Farshad Jabnoush

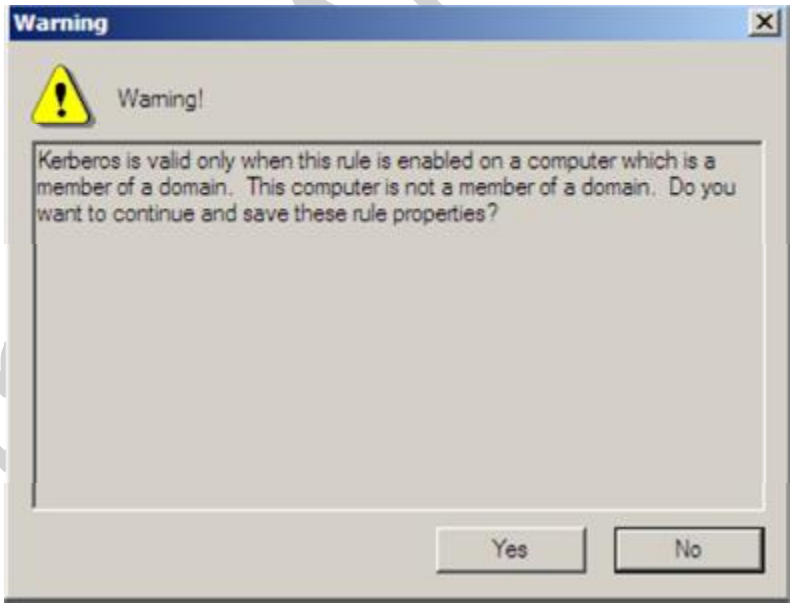



**با فعال بودن گزینه بالا اگر در شبکه Xp داشته باشیم به درخواست های آن هم پاسخ می دهد.**



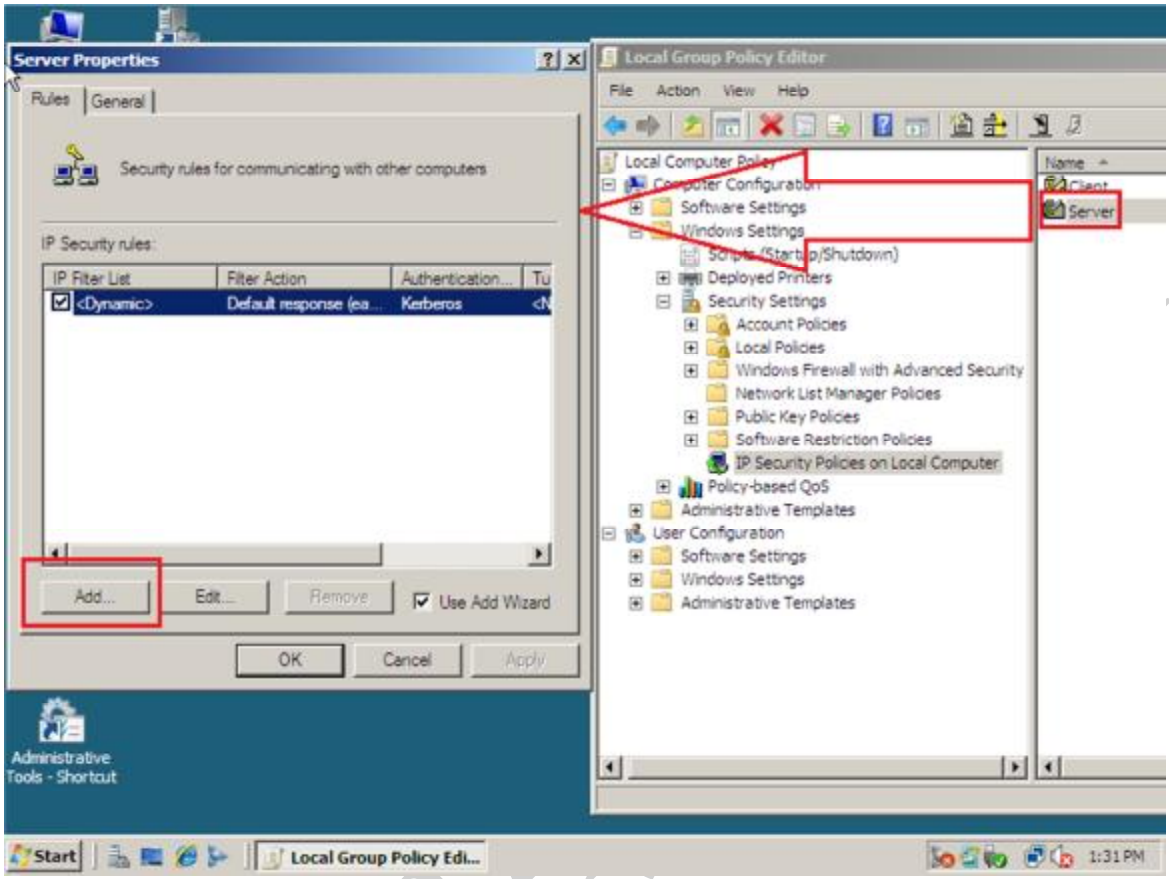

در شکل بالا می گوید Authentication بر اساس Kerberos انجام می شود.

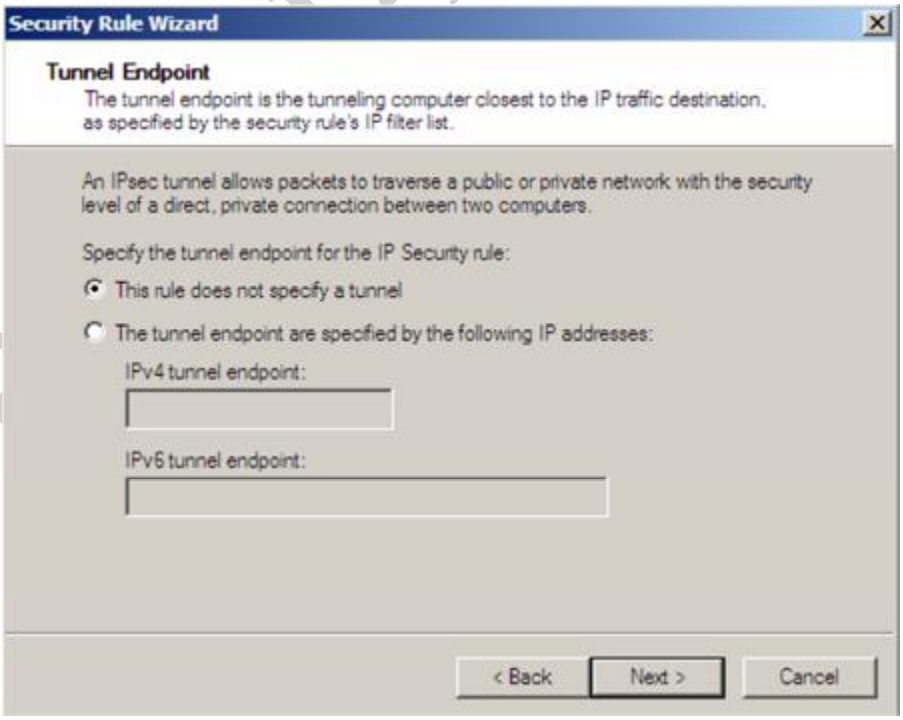



در شکل بالا می گوید Kerberos برای شبکه های دامینی می باشد,شبکه شما Workgroup می باشد.

- در پالیسی کلاینت (بالا) 5 مورد Ipsec Policy را لازم ندارد ولی در پالیسی سرور لازم است.

در اینجا(پالیسی سرور)5 مورد Ipsec Policy را لازم دارد برای ایجاد آن ها مانند زیر عمل می کنیم

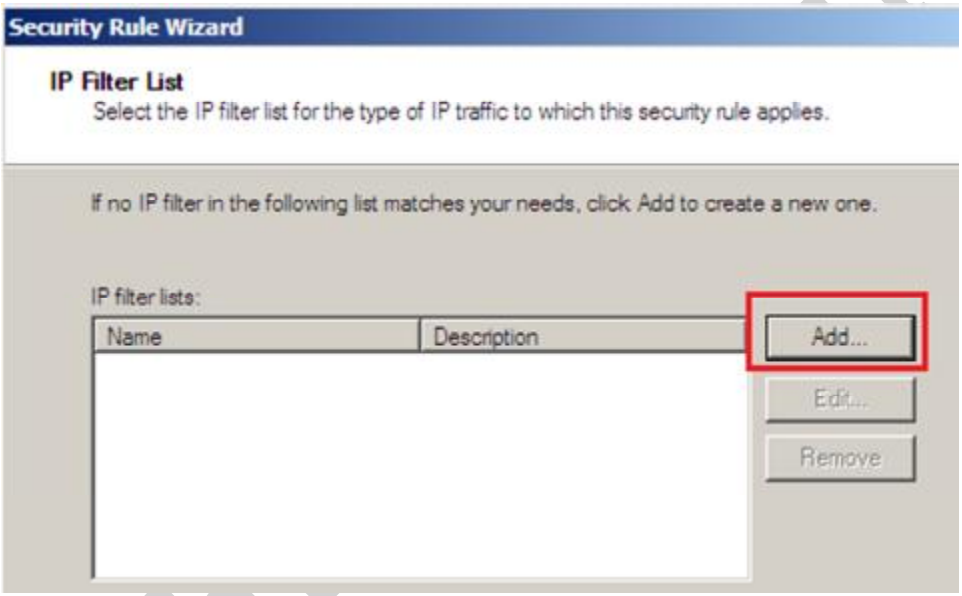


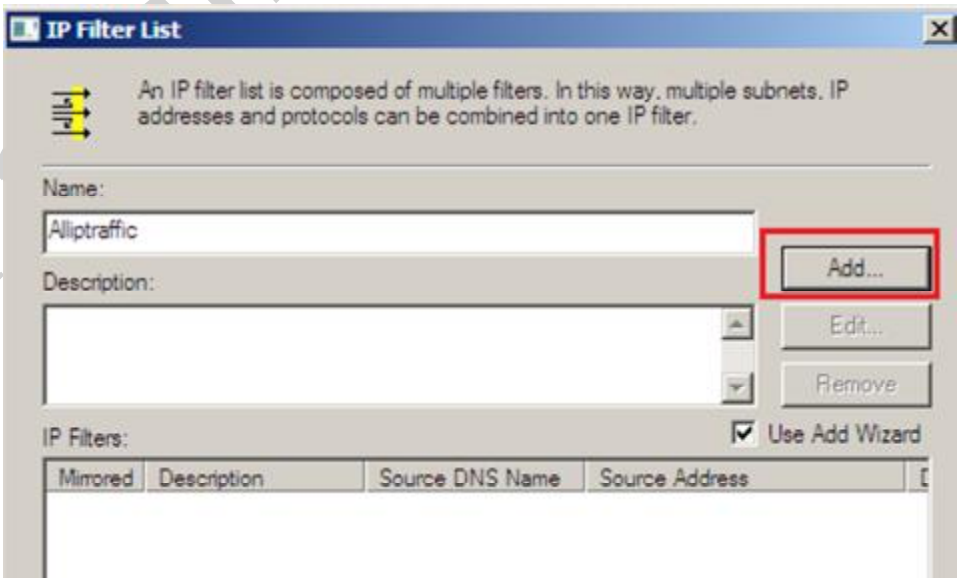

در شکل بالا از ما Endpoint می خواهد که ما آن را نداریم,پس گزینه اول را انتخاب می کنیم.

در اینجا می گوید هم در داخل شبکه و هم بیرون از شبکه با Ipsec کار کند.

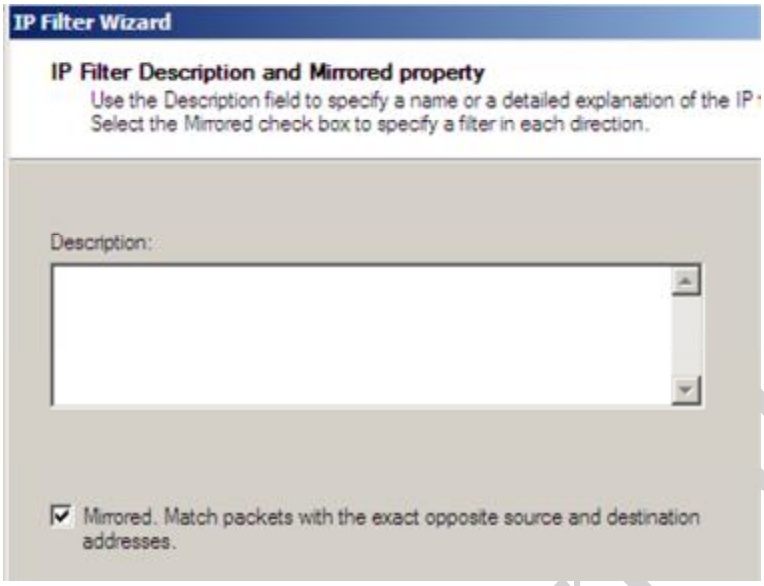
در اینجا باید Ipfilterlist را مشخص کنیم




بعداز زدن Add صفحه زیر باز می شود



در شکل بالا باید Ipfilterlist را مشخص کنیم , بازدن Add وارد شکل زیر می شویم

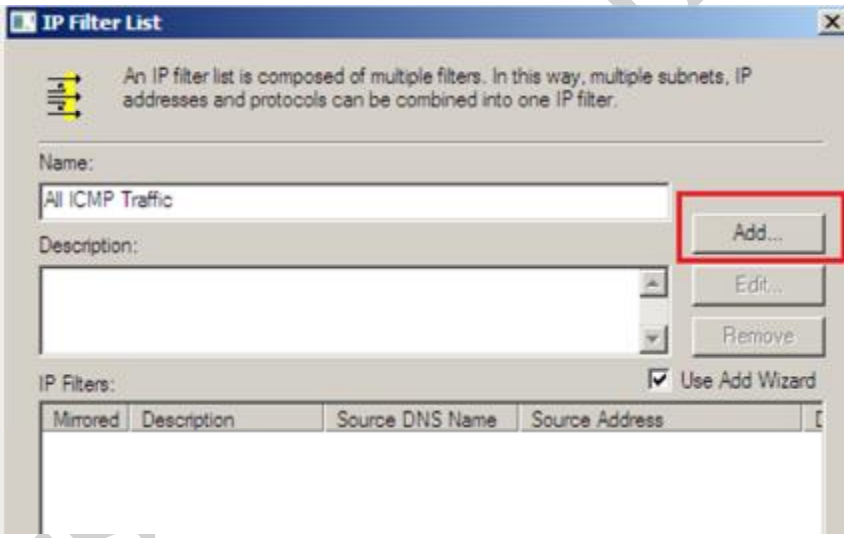


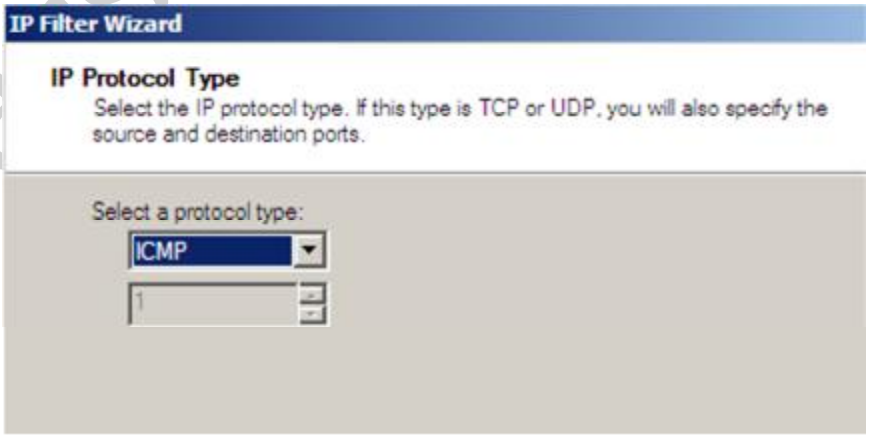

گزینه Mirrored باید فعال باشد به این دلیل که اگر ترافیکی که به سمت سرور می آید به صورت رمز است جواب آن از سمت سرور هم به صورت رمز ارسال شود.

در این مرحله می توانیم مبدا و مقصد و پروتکلی که باید با رمز با هم حرف بزنند را مشخص کنیم

Farabi Abrash

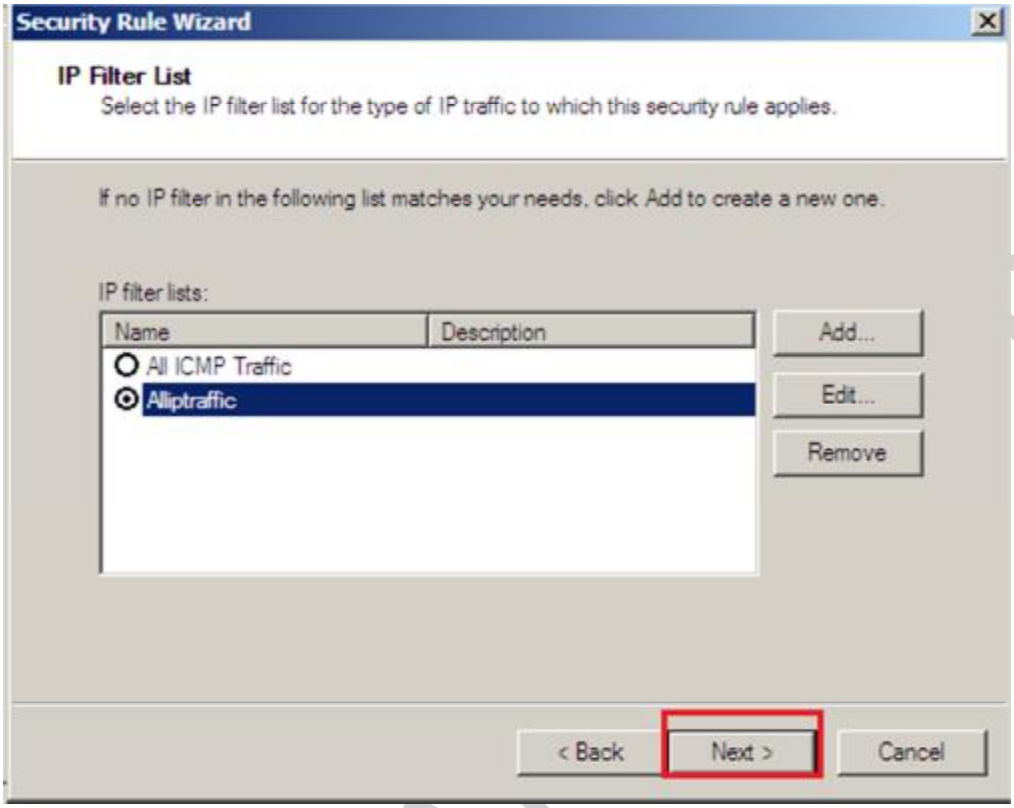
بعد از به پایان رسیدن مرحله بالا,کار ساختن Alliptraffic به پایان رسیده است,حالا نوبت اضافه کردن Allicmp می باشد,تنها تفاوت در اینجا (ICMP ) در پروتکل می باشد.



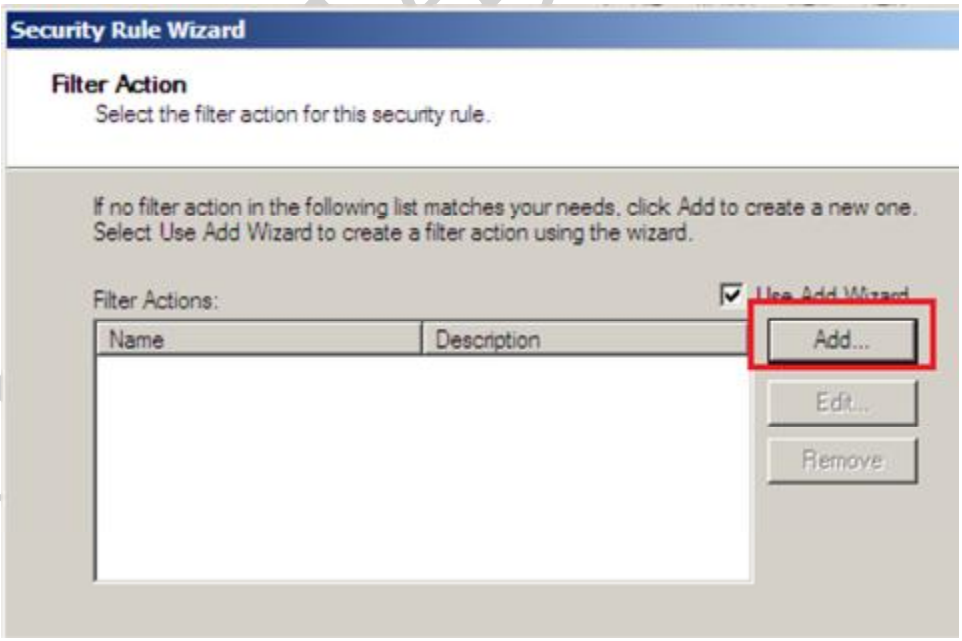




Fa...sh

در این مرحله Ip را انتخاب می کنیم

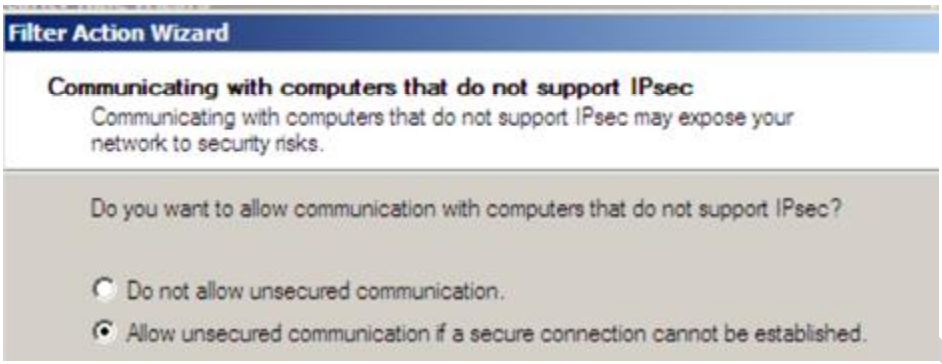



در این مرحله باید Filter Action تعریف کنیم,3نوعFilter Actionداریم.



نوبت به دومین Filter Action می رسد

Farsiabroush




**حالا نوبت به انتخاب نوع رمزنگاری می رسد**

**گزینه اول می گوید هم از رمزنگاری و هم ازصحت داده (Hash) استفاده می کند.**

- **پروتکل های Encryption عبارتند از DES,3DES,AES و پروتکل های Integrity(hash) عبارتند از SHA,MD5**
- **Hash را می توان توسط سایت .www Passcracking.comبدست آورد.**

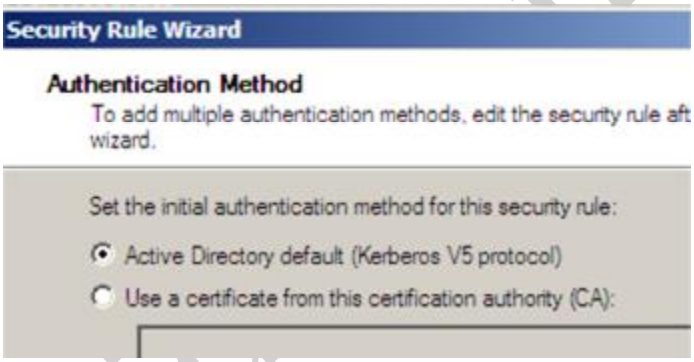
**نوبت به سومینFilter Action می رسد**

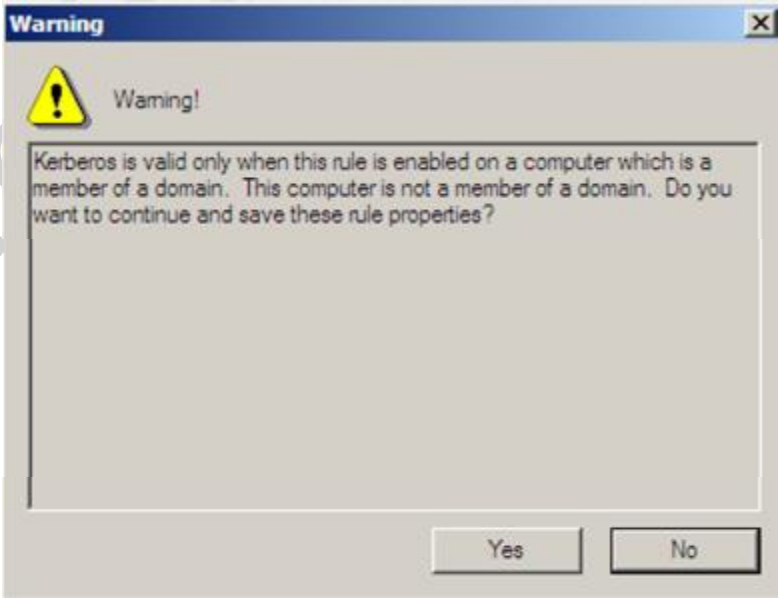
Farshid Nash

**در مرحله بالا می گوییم اگر به صورت امن ارتباط برقرار نشد آن را قطع کن**

**حالا نوبت به فعال سازی می باشد,چون ما بر روی سرور کار می کنیم باید Request را فعال کنیم مانند زیر**

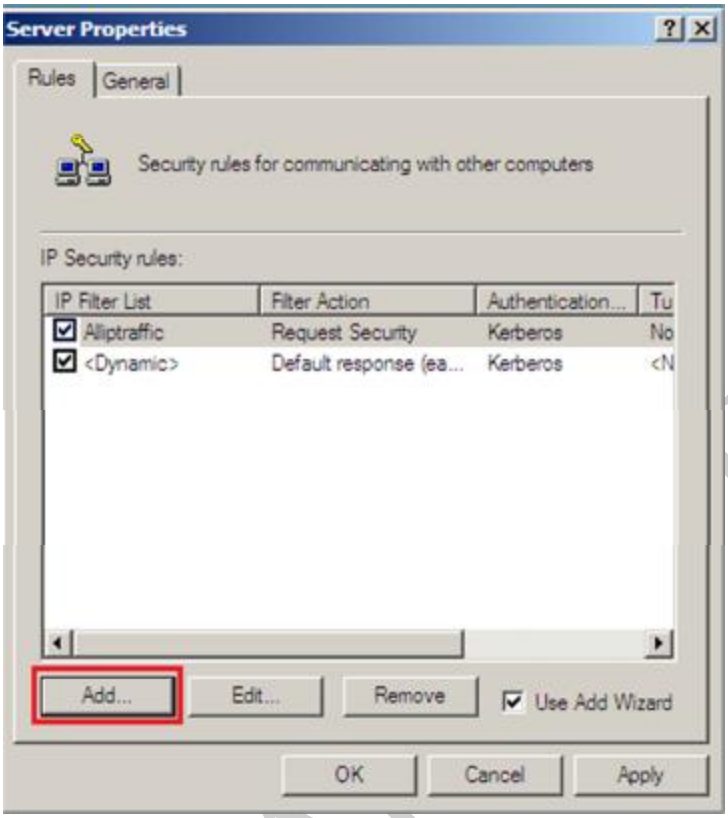
Farnia

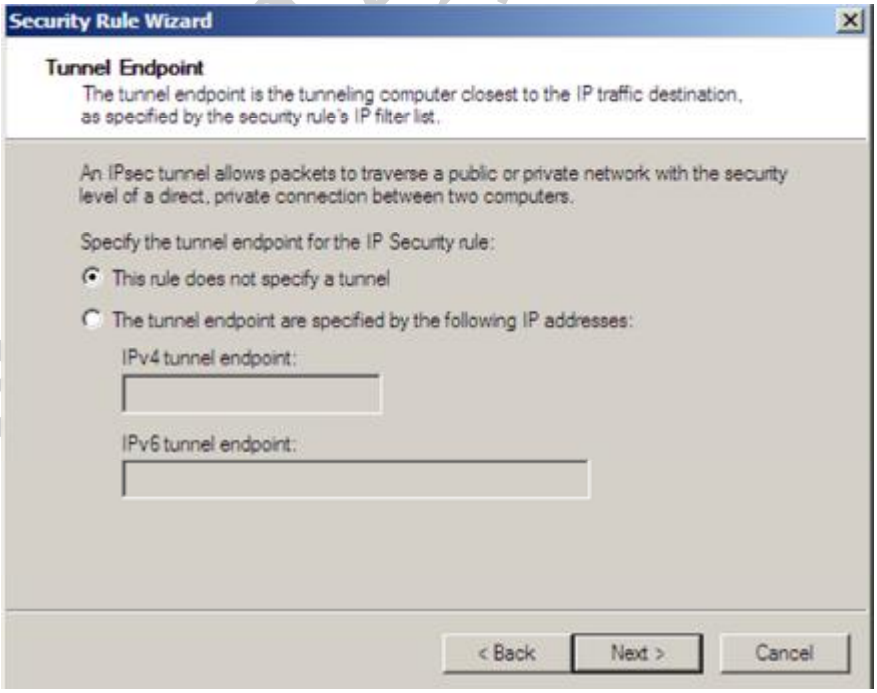



**بعد از اتمام مراحل بالا به مرحله زیر می رسیم**

پیاده سازی All ICMP

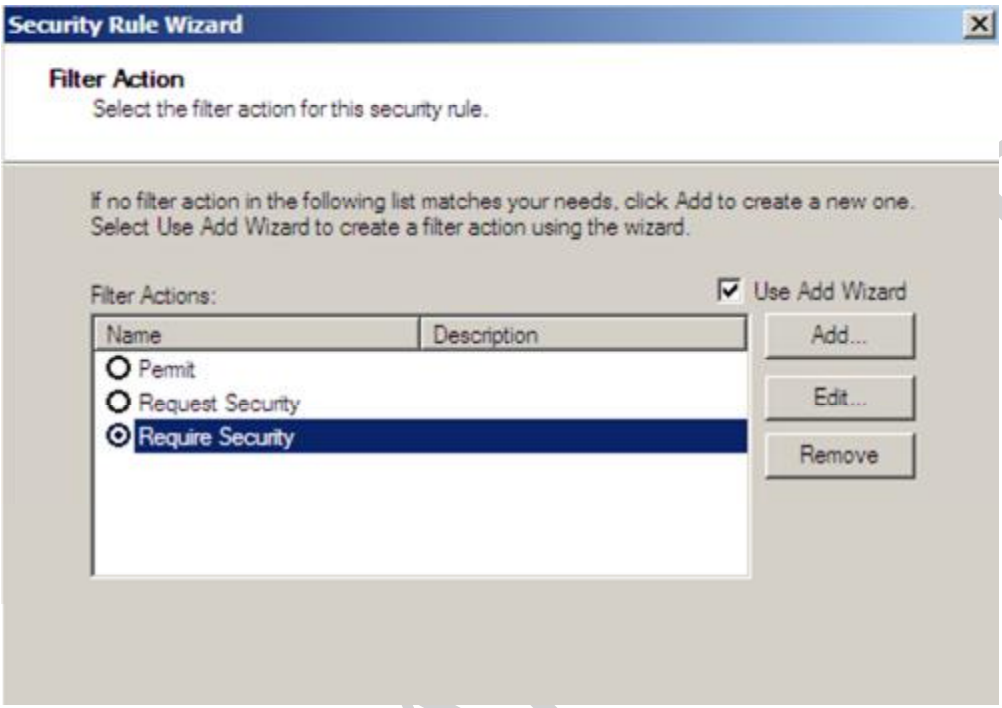



Fa Ajush

- All ICMP همیشه باید Permit باشد به این دلیل که احتیاجی نیست ترافیک های ICMP به صورت رمز از IPSEC گذر کنند.

برای Secure Server تمامی مراحل ICMP را تکرار می کنیم به جز قسمتی که در شکل زیر نشان داده می شود.

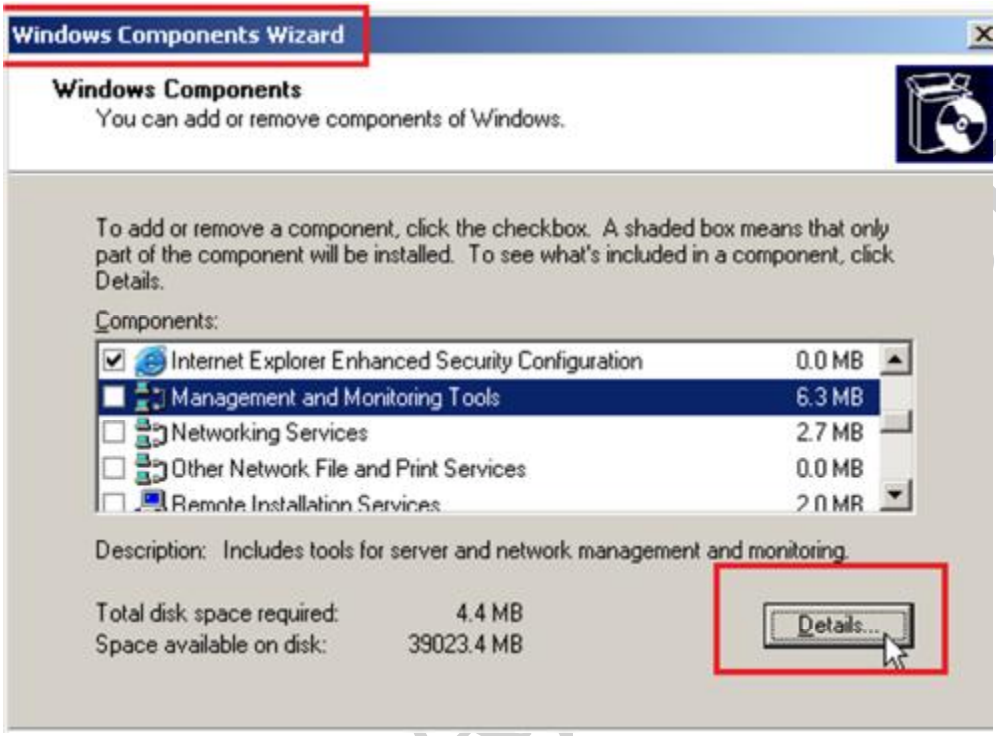


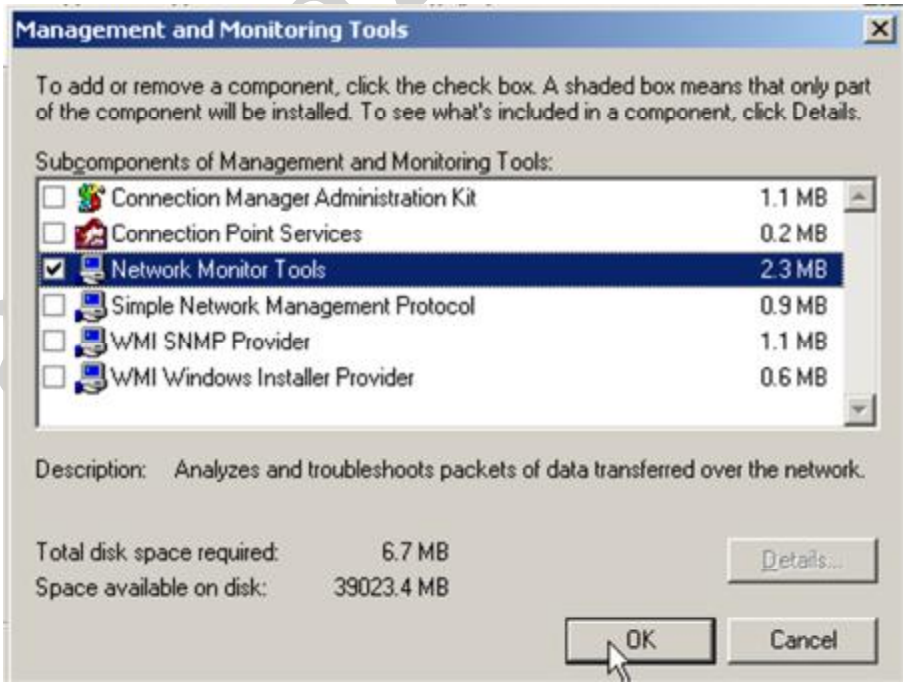

- در سرورها کنسولی به نام Net Mon موجود می باشد که توسط آن می توان ترافیک ههی ورودی و خروجی سرور را مشاهده کرد,این کنسول به صورت پیش فرض در2003 موجود می باشد ولی در 2008 باید دانلود و نصب گردد.

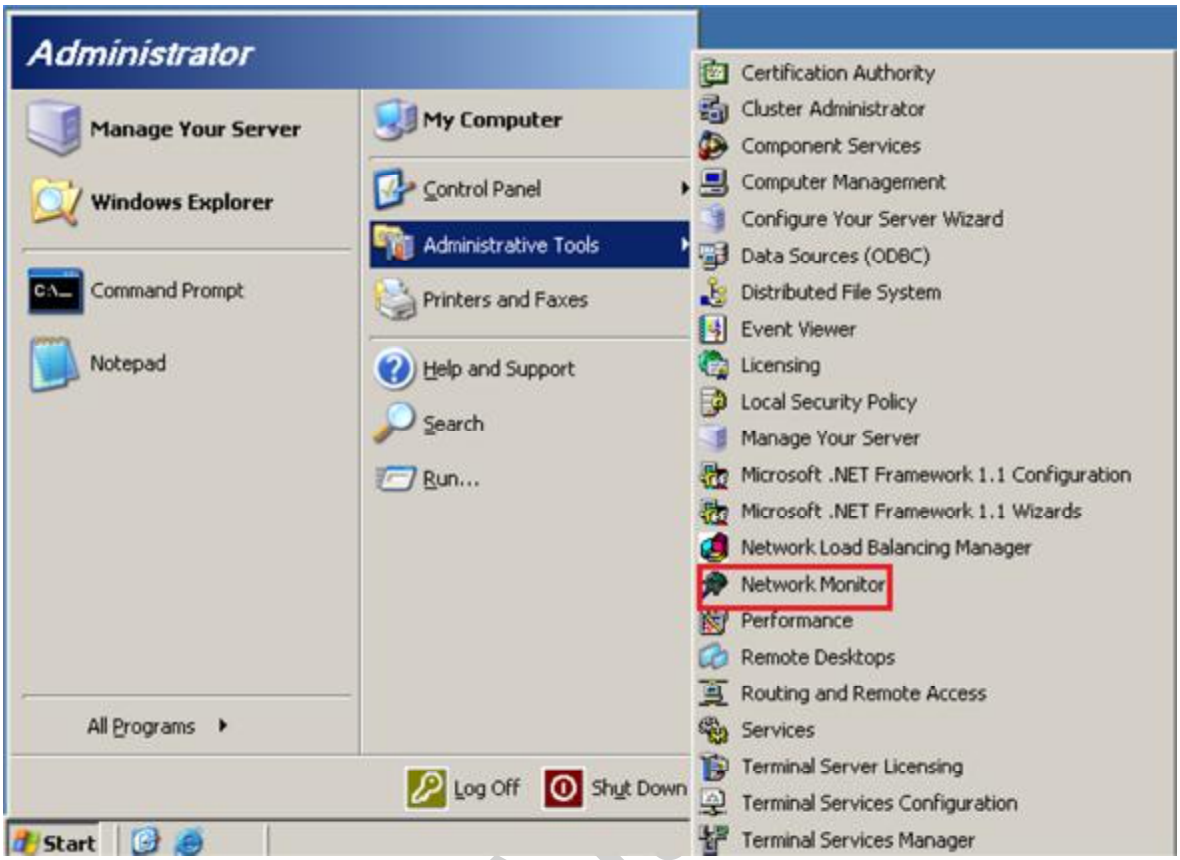
FarshidAj.ir

راه اندازی NetMon در 2003

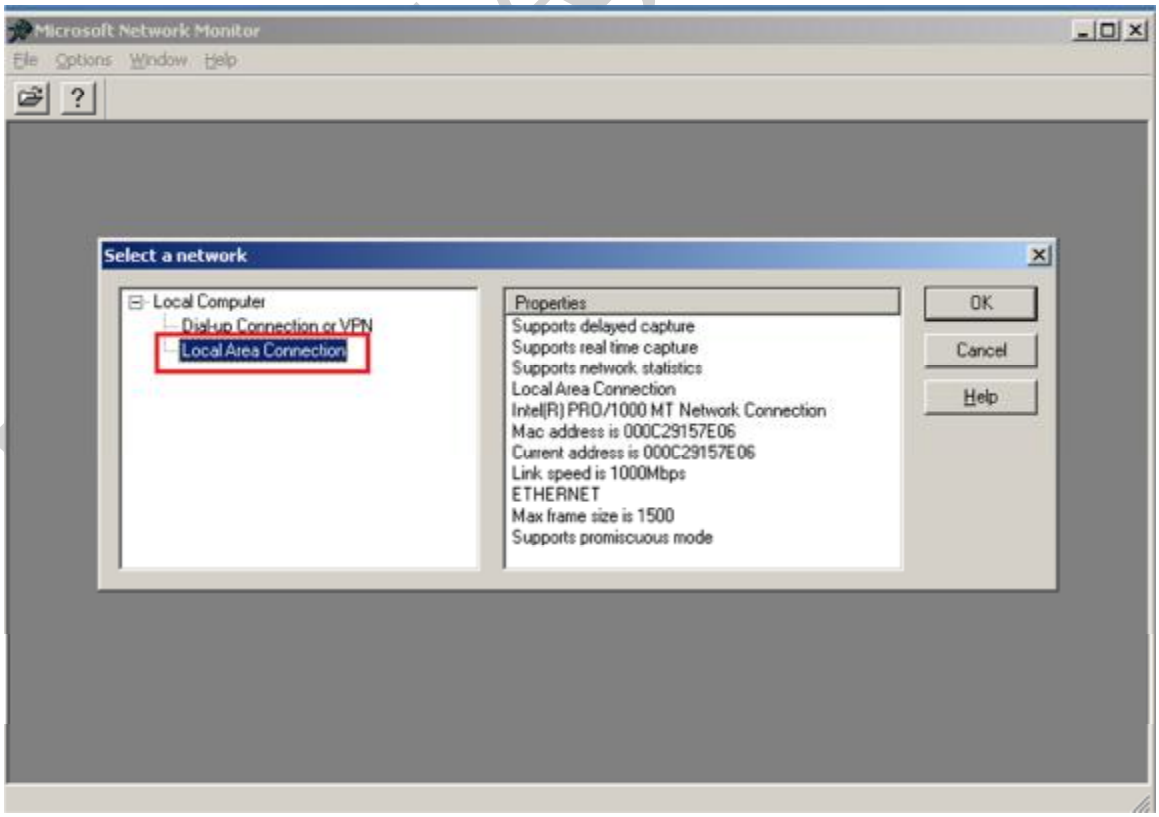
ابتدا باید CD 2003 را داخل دستگاه بگذاریم سپس باید مانند زیر عمل کنیم



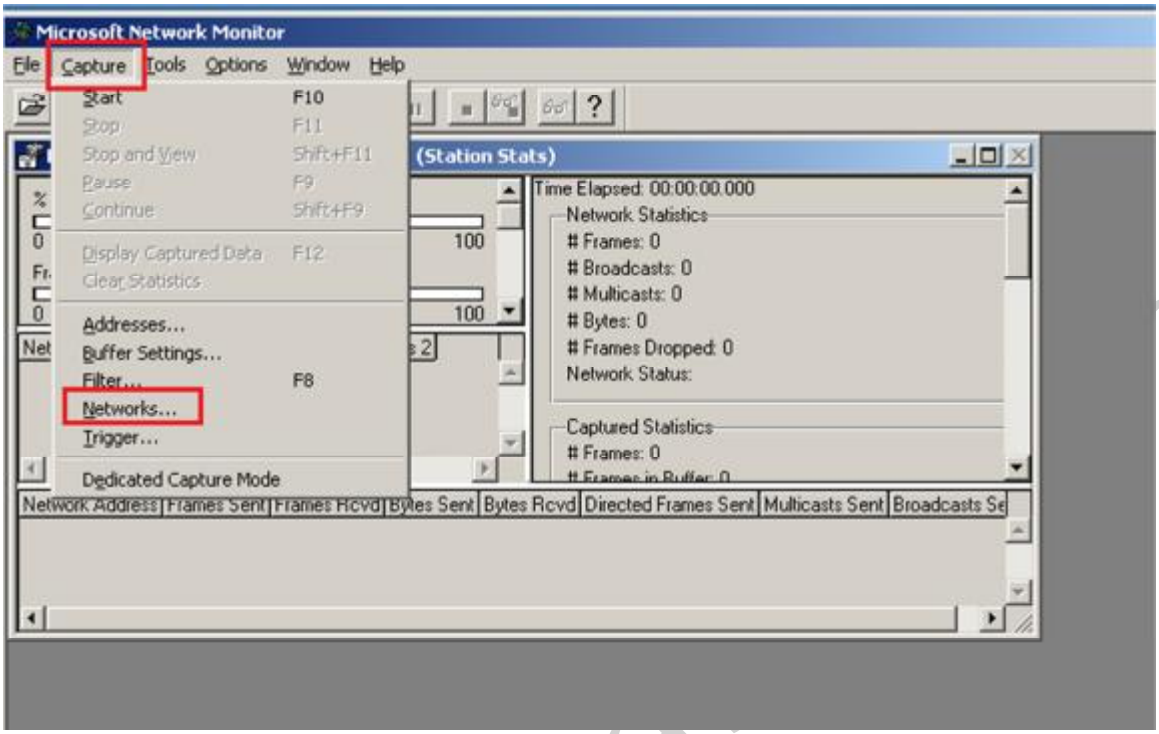





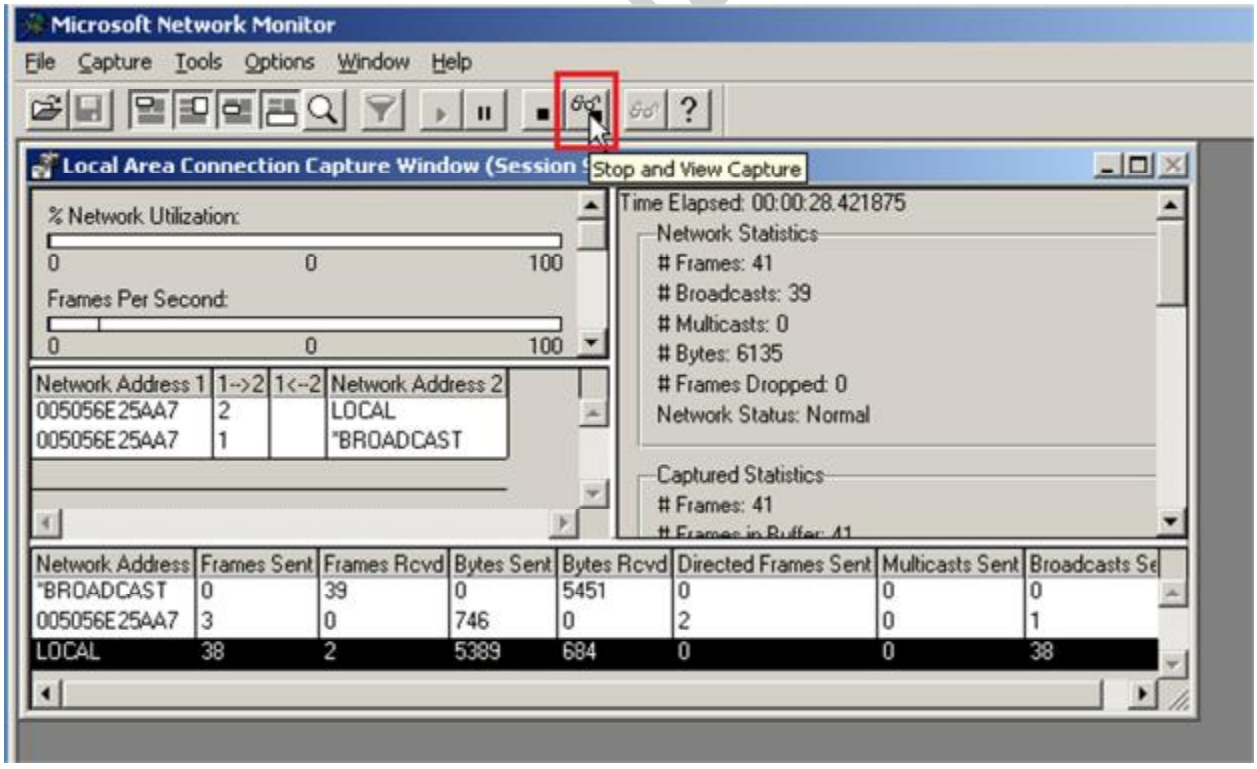

در کنسول باز شده باید کارت شبکه ای را که می خواهیم اطلاعاتش را Capture کنیم انتخاب کنیم(شکل زیر)



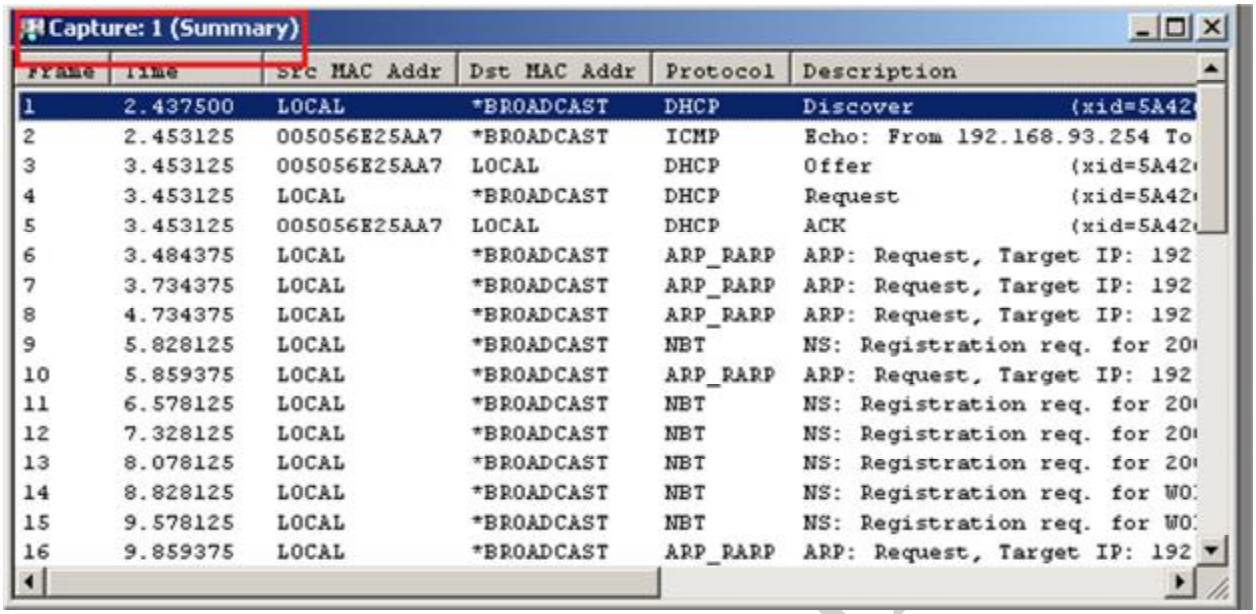
اگر بخواهیم کارت شبکه را عوض کنیم مانند زیر عمل می کنیم




برای دیدن Capture مانند زیر عمل می کنیم



Capture های ضبط شده




- بهترین نرم افزار مانیتورینگ شبکه Wire Shark می باشد.

Remote Access

توسط این سرویس کاربر داخل شبکه می تواند از خارج از شبکه به شبکه متصل شود.

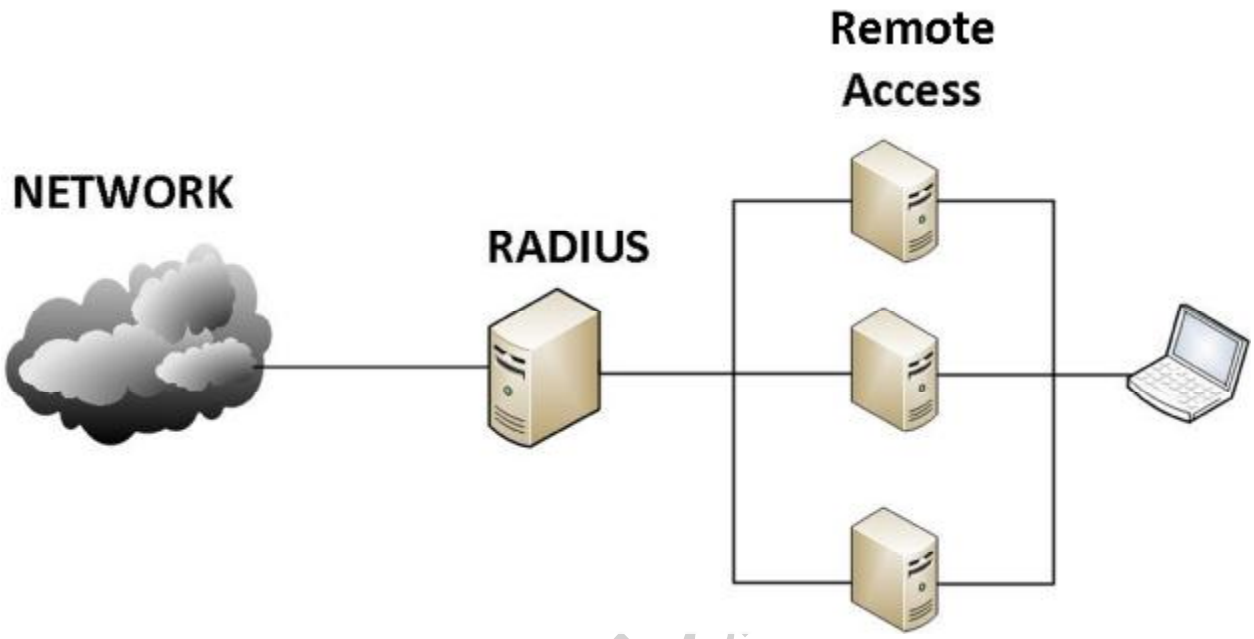
راه اندازی Remote Access احتیاج به یک سری پیش راه انداز دارد:

1) Remote Access Server : به سروری که اجازه وصل شدن بیرون از شبکه را به افراد می دهند گویند این سرور را توسط RRAS پیاده سازی می کنند.
   - سخت افزاری به نام Access Server کار RAS را انجام می دهد.
2) Remote Access Client : به کسی که اجازه وصل شدن به شبکه را از خارج از شبکه دارد گویند که بر 2 نوع هستند الف) Interanet : به شبکه هایی که فقط کاربرانش اجازه وصل شدن از بیرون را به آنها دارند ب) Exteranet : به شبکه هایی که محدودیتی برای وصل شدن کاربران به آنها وجود ندارد را گویند مانند اینترنت.
3) Remote Access Authenticator : به سروری که جلوی شبکه ما قرار می گیرد و کسانی را که از بیرون از شبکه وصل می شوند شناسایی کرده وسطح دسترسی آنها را مشخص می کند گویند که به 3 دسته تقسیم می شوند 1- Local 2- Radius 3- Tacacs+

1-3) Local : تمامی اکانت ها, پشت سرور Remote Access که کاربران از بیرون به آن وصل می شوند ذخیره شده است یعنی تمامی مراحل شناسایی و...پشت همین سرور اجرا می شود.

FarshidAjabi

3-2) Radius : در این سناریو یک سرور به نام Radius قرار دارد که تمامی اکانت ها در این سرور ذخیره هستند و سرور Remote Access باید کاربرانی را که از بیرون وصل می شوند را از روی این سرور چک کند.




3-3) این روش یک روش سخت افزاری می باشد.(cisco )

- روش 3-1 ,روش مناسبی نمی باشد چون اگر مانند شکل بالا 3 سرور داشته باشیم تمامی اکانت ها پشت هر 3 ذخیره می شوند و این ذخیره سازی امنیت را پایین می آورد.
- برای پیاده سازی روش3-3 بر روی ویندوز از نرم افزارهای +NtTac و Secure Acs استفاده می شود.

4) Active Directory : اگر این کامپوننت فعال باشد عمل احراز هویت توسط پروتکل Kerberos انجام می شود .

FarshidAj

مزیت های کنسول RRAS

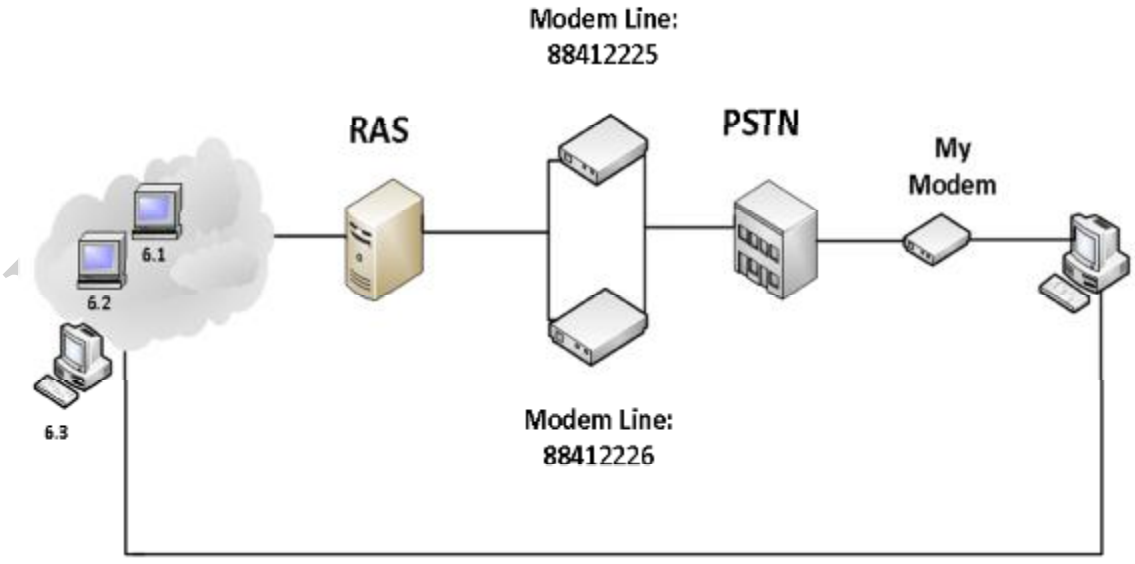
- توسط این کنسول می توان سرور را روتر کرد.
- روتر Device می باشد که می تواند چندین رنج متفاوت از Ip هارا به هم وصل کند.
- می توان فایروال فعال کرد تا بتوانیم Packet Filter کنیم.
- می توان VPN Server که خود 2 نوع Remote Access VPN وVPN Site-to-Site می باشد اجرا کرد.
- می توان Nat Server فعال کرد.
- می توان Dialup Server فعال کرد.
- می توان Wireless Server فعال کرد.

یک کلاینت توسط یکی از 3 روش زیر می تواند با RRAS ارتباط برقرار کند

1) VPN (2Dialup(ADSL+ PSTN) 3) Wireless

Dialup(ADSL+ PSTN)

یک شبکه را در نظر بگیرید داخل این شبکه 2 کلاینت به Ip های 6.1 و 6.2 وجود دارد, جلوی شبکه یک RAS سرور می باشد بعد از آن 2 مودم توسط خط تلفن به مخابرات وصل شده است بعد از مخابرات ,مودم کامپیوتر خانگی ما قرار دارد, در اینجا توسط کامپیوتر خانگی می خواهیم به شبکه مورد نظر وصل شویم برای این کار باید داخل کامپیوتر خانگی توسط Dialup Connection وصل شویم, داخل کادر User باید User را وارد کنیم که پشت Ras سرورمان وجود دارد همین طور پسورد,در قسمت Dial شماره تلفن یکی از مودم های بعد از Ras سرور را وارد می کنیم 88412225, سپس کامپیوتر خانگی ما داخل شبکه قرار می گیرد(مانند شکل) در اینجا احتیاج به Ip دارد که Ras سرور تبدیل به Mini DHCP می شود و به آن Ip 6.3 را می دهد.



این روش دارای معایبی می باشد مانند : برقراری ارتباط با سرعت K64 ,هزینه بالا برای برقراری ارتباط بین شهری ,به ازای هر مودم یک نفر می تواند به شبکه وصل شود(برای از بین بردن این مشکل از خطوط1E استفاده می کنند) مزیت این روش اختصاصی بودن هر خط تلفن می باشد,پس امنیت بالایی دارد.

VPN (Tunneling )

- VPN یک تکنولوژی می باشد که توسط آن ما می توانیم دوشبکه(یا دو کامپیوتر) را به صورت کا ملا امن تحت یک بستر عمومی(اینترنت) به هم وصل کنیم.

در این روش جلوی شبکه, یک سرور RAS در حالت VPN بالا می آوریم این سرور باید 2 کارت شبکه داشته باشد کارت شبکه اول به شبکه وصل می باشد و کارت شبکه دوم باید IP Publicداشته باشد و به اینترنت متصل باشد سپس کامپیوتری که بیرون از شبکه ما قرار دارد و می خواهد داخل شبکه ما بشود باید یک کانکشن VPN بسازد و درون کانکشن یوزر و پسوردی را وارد کند که در RAS سرور موجود باشد و در قسمت IP Public, IP را وارد می کند و سپس در شبکه ما قرار می گیرد و از طریق Mini DHCP (RAS ) IP می گیرد.

VPN-Remote Access

در این روش فرض کنید یک سرور VPN در کانادا داریم و بر روی آن اینترنت داریم برای اینکه یک کلاینت بتواند از اینترنت آن استفاده کند باید به آن سرور از طریق کانکشن VPN وصل شود تا بتواند از اینترنت استفاده کند.

VPN-Site-To-Site

از این روش برای اتصال شعبات به یکدیگر توسط VPN استفاده می شود,فرض کنید دو شعبه یکی در تهران و دیگری در تبریز داریم در جلوی هر کدام از این شعبات یک سرور داریم که این دو توسط VPN به یکدیگر متصل شده اند,اگر کلاینتی از تهران بخواهد به تبریز وصل شود باید از طریق سرور تهران به سرور تبریز وصل شود در نتیجه ارتباط کلاینت با تبریز از طریق VPN انجام می شود و بالعکس.

VPN ها به 3 دسته زیر تقسیم می شوند:

1) PPTP (Point To Point Tunneling Protocol ):در این روش برای رمز نگاری اطلاعات از MPPE (MicrosoftPoint To Point Encryption ) استفاده می کند,Level رمز نگاری در این روش 40 -56- 128 بیت می باشد,پورت استفاده شده در این روش 17223 می باشد.
2) L2TP (Layer2Tunneling Protocol ): در این روش برای رمز نگاری از Ipsec استفاده می شود, Level رمز نگاری در این روش 56 -168 بیت می باشد,پورت استفاده شده در این روش 50و51 می باشد.

FarshidAjabnoush

3) SSTP (Secure Socket Tunneling Protocol ) : در این روش برای رمز نگاری از SSL استفاده می شود, Level رمز نگاری در این روش 256 بیت و256 به بالا می باشد,پورت استفاده شده در این روش 443 می باشد.

- روش SSTP از دو روش دیگر امن تر می باشد,نام دیگر SSTP , Web VPN و SSL VPN می باشد.

Wireless

اساس کار شبکه های وایرلس بر حسب Radio Frequency,تمامی قوانینی که در مورد AM وFM وجود دارد در شبکه های وایرلس هم صدق می کند,2سازمان بزرگ به نام های FCC وIEEE تمامی قوانین و مقررات وایرلس را تنظیم می کنند.

FCC : این سازمان رنج فرکانس های مورد استفاده در شبکه های وایرلس را تعیین می کند,2 رنج فرکانسی در شبکه های وایرلس داریم 2.4 GHZ = 2.4 ISM Band و 5GHZ = 5 GHZ UNII Band

IEEE : این سازمان بر روی تکنولوژی های شبکه استاندارد گذاری می کند,مانند:

Ethernet : 802.3 TokenRing : 802.5 Wireless : 802.11 Wimax : 802.16 Bluetooth : 802.15

| Standard | Speed | Frequency range |
|---|---|---|
| 802.11 | 1 or 2 Mbps | 2.4 |
| 802.11 B | 11 Mbps | 2.4 |
| 802.11 A | Up To 54 Mbps | 5 Ghz |
| 802.11 G | Up To 54 Mbps | 2.4 |
| 802.11 N | Up To 380 Mbps | 2.4 |

تمامی سرعت هایی که در جدول بالا آورده شده است سرعت های پایه می باشند,این سرعت ها می توانند در محصولات مختلف از سمت سازنده تغییر داده شوند.

- شرکت D-LINK از تکنولوژی به نام Speed Booster در محصولاتش استفاده می کند که باعث بالا رفتن سرعت می شود,شرکت Cisco هم از تکنولوژی به نام Mime استفاده می کند.
- برای را ه اندازی شبکه وایرلس باید به 2 نکته interoperability و Compatibility توجه کرد.

Wimax

از 2 استاندارد 802.16 و 802.16a استفاده می کند سرعت آن 70Mbps می باشد و امواج آن از نوع مایکروویو می باشد ,رنج فرکانس بین 2 دکل وایرلس برابر با 10-66 Ghz می باشد و رنج فرکانس بین دکل و مودم مصرف کننده برابر با 2-11 Ghz می باشد.

Farshid Aabnoush

Bluetooth

در رنج فرکانسی 2.4Ghz با سرعتی برابر با 2Mbps و با شعاعی برابر با 10 متر کار می کند.

- وایرلس و بلوتوث با هم تداخل دارند به این دلیل که در یک رنج فرکانسی هستند.
- وایرلس ها در فضای باز تا 600 متر پشتیبانی می کنند و در فضای بسته تا 150 متر,برای استفاده در فواصل بیشتر باید از Access Point استفاده کرد.
- با پروتکل های WPA2-WPA-WEP می توان روی شبکه های وایرلس ایجاد امنیت کرد.
- فرکانس ها از 2.400 شروع و به 2.499 ختم می شوند ما بین این رنج را کانال بندی کرده اند(11 کانال موجود می باشد)
- اگر بخواهیم دو یا چند کامپیوتر را که دارای رنج IP یکسان هستند را به هم وصل کنیم از Switch استفاده می کنیم ولی اگر رنج IP ها متفاوت بود باید از Router استفاده کنیم.
- Switch لایه 3 به صورت پیش فرض Switch می باشد ولی می تواند به Router هم تبدیل شود,تفاوت Switch لایه 3 با Router در این است که این سوئیچ ها دارای ویژگی به نام Caching می باشد که باعث بالاتر رفتن سرعتشان نسبت به روتر می شود.

برای پیاده سازی شبکه های وایرلس از 2 روش استفاده می کنیم 1- Adhoc 2- Infrastructure

Adhoc : شبکه هایی هستند که کامپیوترها در آن از طریق کارت شبکه های وایرلسشان به یکدیگر وصل می شوند.

Infrastructure : شبکه هایی هستند که کامپیوترها در آن از طریق Access Point به یکدیگر وصل می شوند.

پیاده سازی ویژگی Router با RRAS

می توانیم با استفاده از کنسول RRAS سرورمان را تبدیل به Router کنیم.

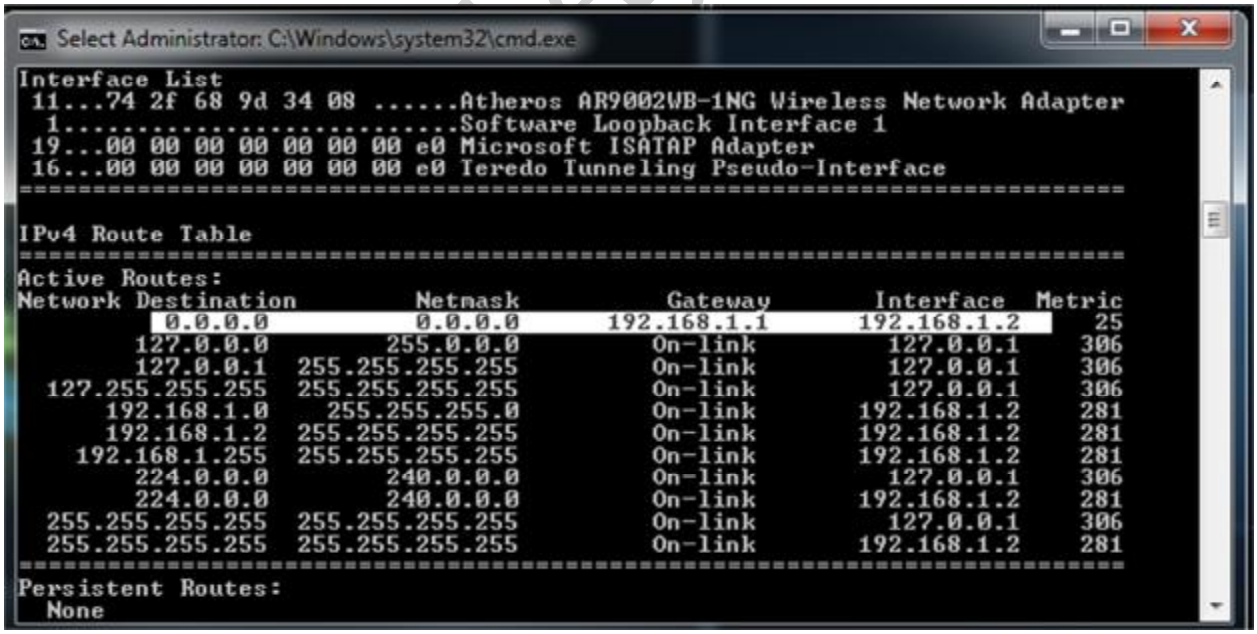
- برای روتر کردن سرورمان احتیاج به 2 کارت شبکه داریم, این ویژگی را زمانی استفاده می کنیم که می خواهیم شبکه هایی را که در نزدیکی یکدیگر هستند را به هم وصل کنیم مانند طبقه1و2 ولی در فاصله های بیشتر باید به صورت سخت افزاری این کار را انجام دهیم.

برای روتر شدن باید 3 ویژگی زیر را دارا باشد:

1- Routing Interface: به ازای هر شبکه (رنج Ip ) باید 1 کارت شبکه داشته باشد.
2- Routing Protocol: به پروتکل هایی که این امکان را به روتر ما می دهند تا شبکه هایی را که می تواند با آنها در ارتباط باشد را شناسایی کند.
3- Routing Table:اسامی شبکه هایی که توسط Routing Protocol شناسایی شده اند در این جدول ذخیره می شود.

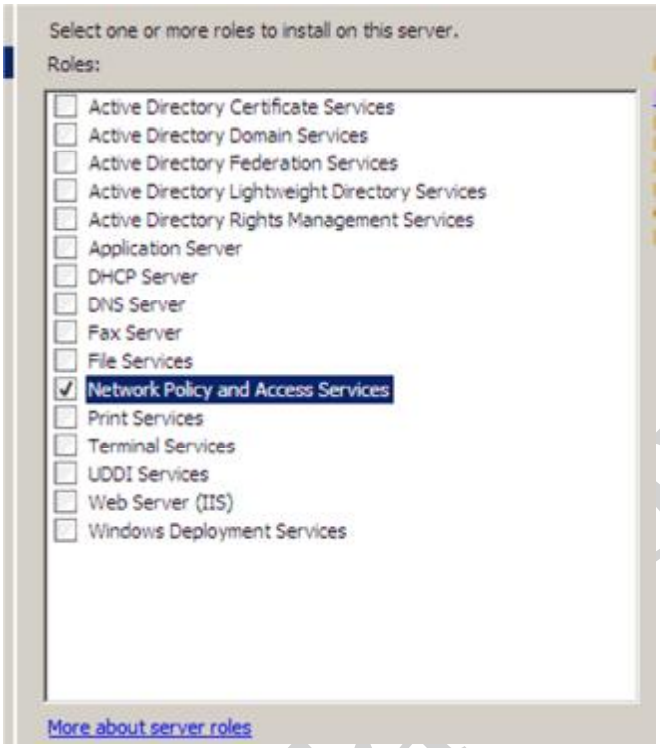
FarshidAjabnoush

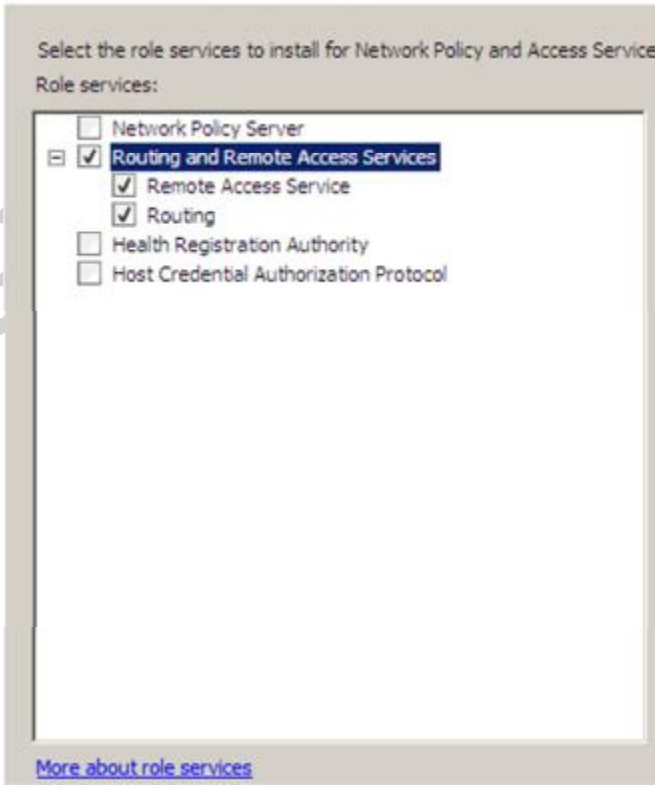
- اسامی Rip : Routing Protocol (در شبکه های کوچک استفاده می شود), EigRp-Ospf (این 2 در شبکه های بزرگ استفاده می شوند),Isis ( در شبکه های خیلی بزرگ استفاده می شود),BGP (در اینترنت استفاده می شود)
- سرور 2003 پروتکل RIP,OSPF را پشتیبانی می کند و 2008 فقط RIP را پشتیبانی می کند.
- تمامی ویندوزها دارای Routing Table می باشند, با دستور Routeprint می توانیم جدول را ببینیم.
- در جدول زیر شبکه هایی را می بینیم که می توانیم با آنها در ارتباط باشیم(ستون Network Destination ) .اگر آدرس موردنظر در جدول نباشد آن آدرس را بجای صفرهای جدول جایگزین می کند و وصل می شود.
- ستون Netmask برای تشخیص شبکه ای به کار می رود که شبکه ما در آن قرار دارد(240 Multicast ) می باشد.
- ستون Gateway مشخص می کند برای رسیدن به شبکه مورد نظر پکت ها باید به کدام Gateway تحویل داده شود.
- ستون Interface مشخص می کند برای رسیدن به Gateway موردنظر پکت ها باید به کدام کارت شبکه تحویل داده شود.
- ستون Metric اولویت خط ها را نشان می دهد هر چه این عدد پایین تر باشد اولویت آن خط بالاتر می باشد.




با دستور Route add خطی را اضافه,Route delete خطی را پاک,Route change خطی را تغییر می دهد.

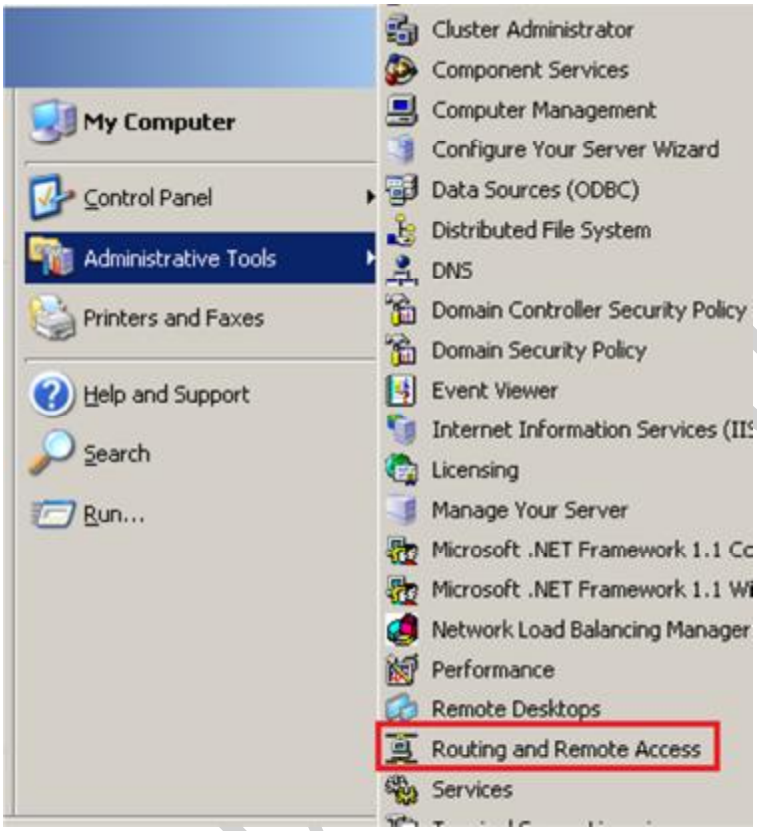
برای را ه اندازی کنسول RRAS در 2008 باید Role زیر را نصب کنیم

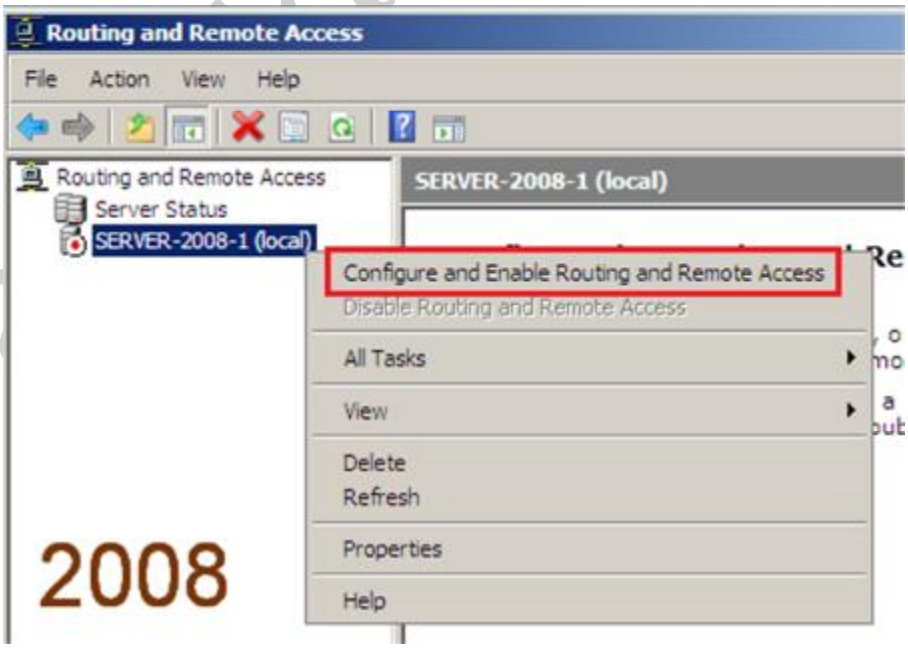


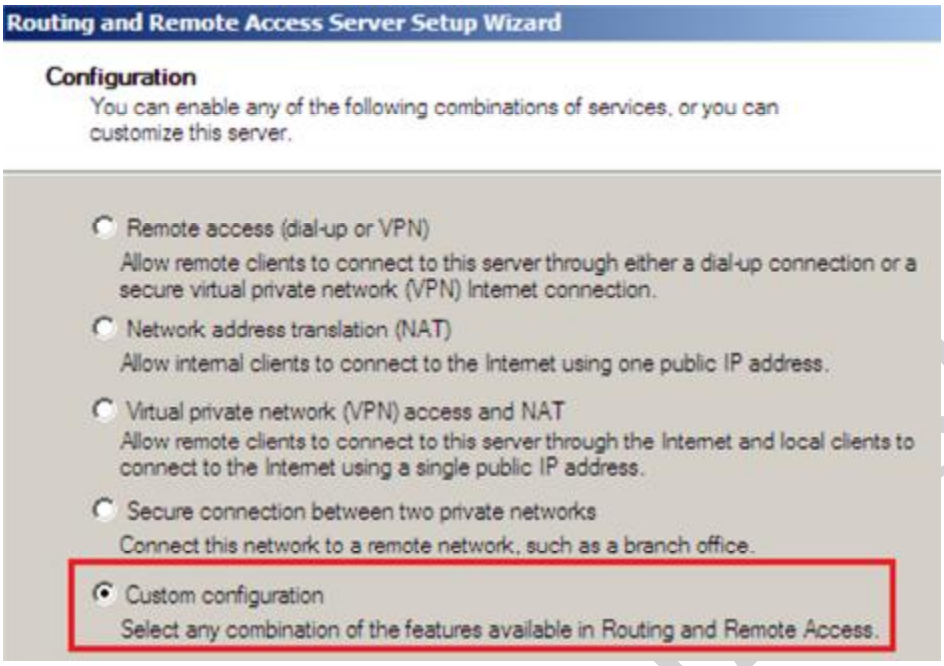



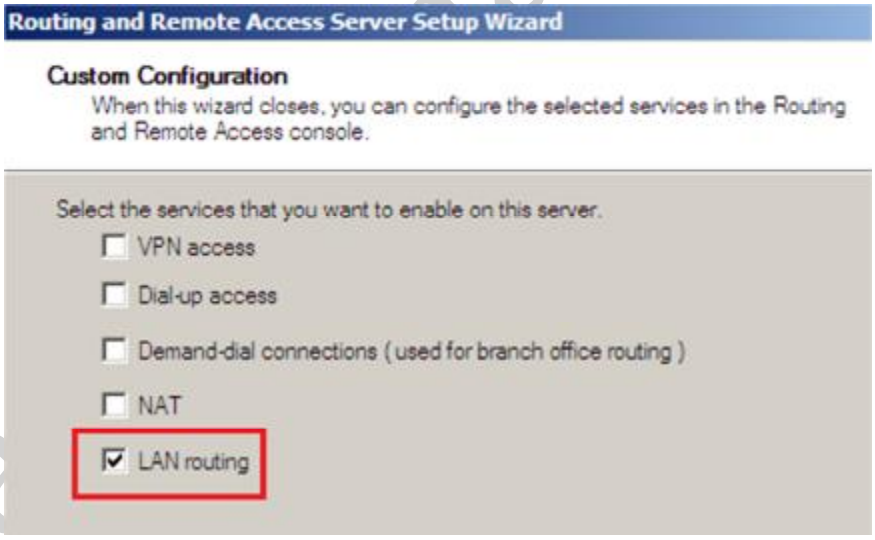

Farsi Visual Basic

- در 2003 احتیاج به نصب این کنسول نیست چون به صورت پیش فرض نصب می باشد،برای دیدن این کنسول در 2003 مانند زیر عمل می کنیم .



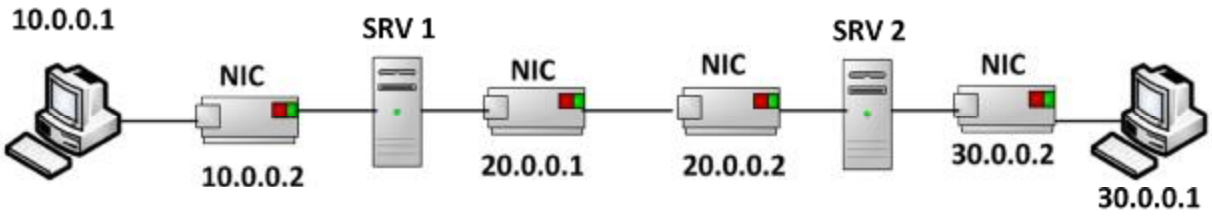



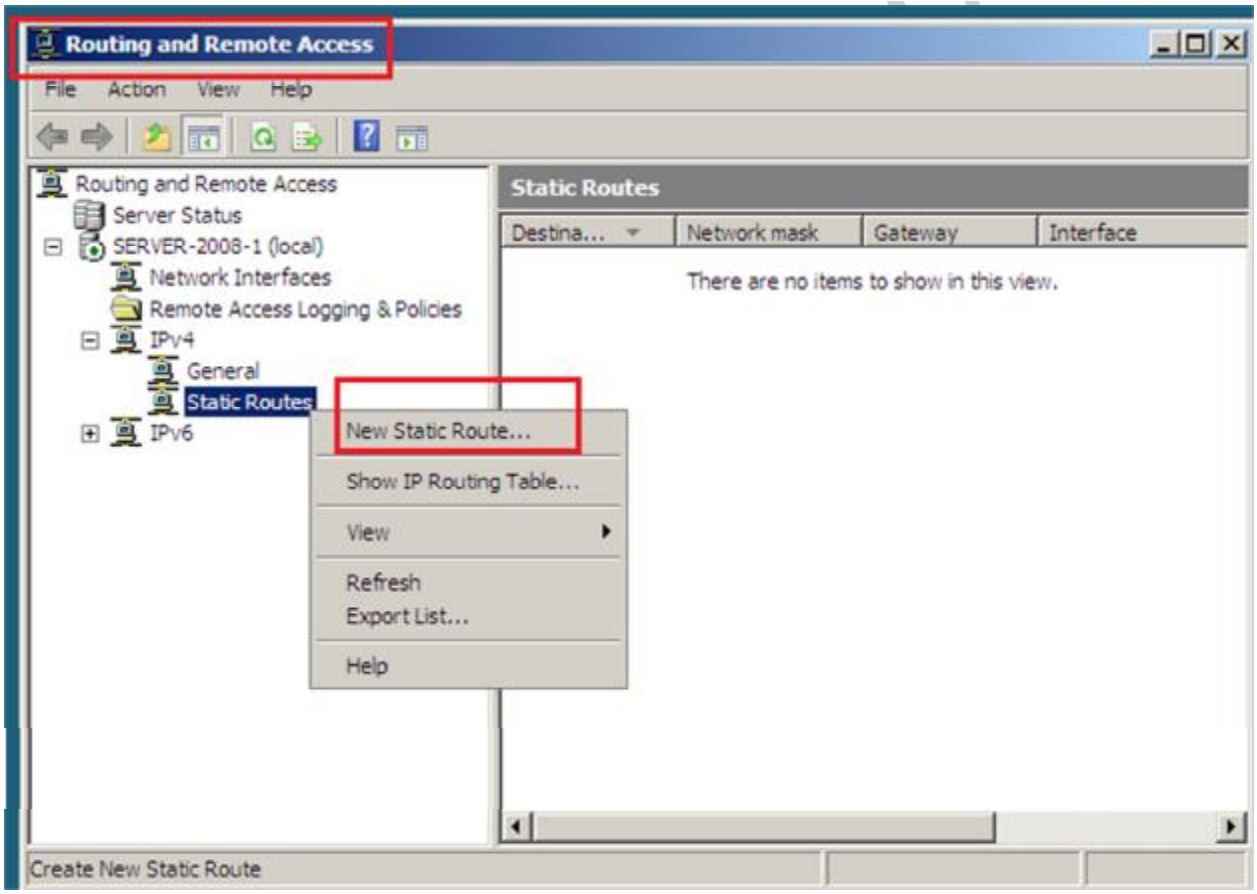

Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (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.

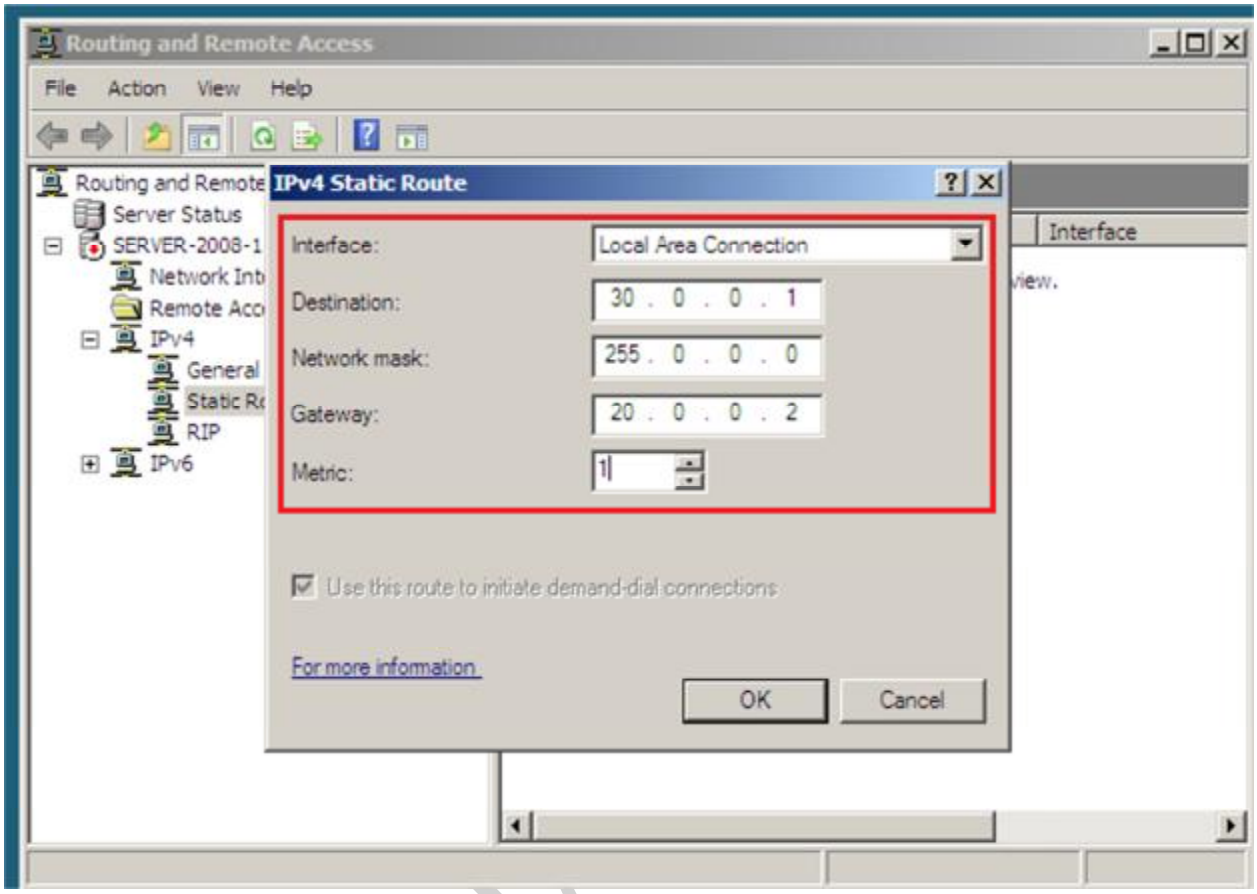

Routing and Remote Access Server Setup Wizard
Custom Configuration
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.
Select the services that you want to enable on this server.
VPN access
Dial-up access
Demand-dial connections (used for branch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

Fa

- همیشه AddRoute را بر روی کارت شبکه ای تنظیم می کنیم که ما را به بیرون وصل می کند,در این سناریو بر روی کارت شبکه های 20.1 و 20.2 تنظیم می شود.



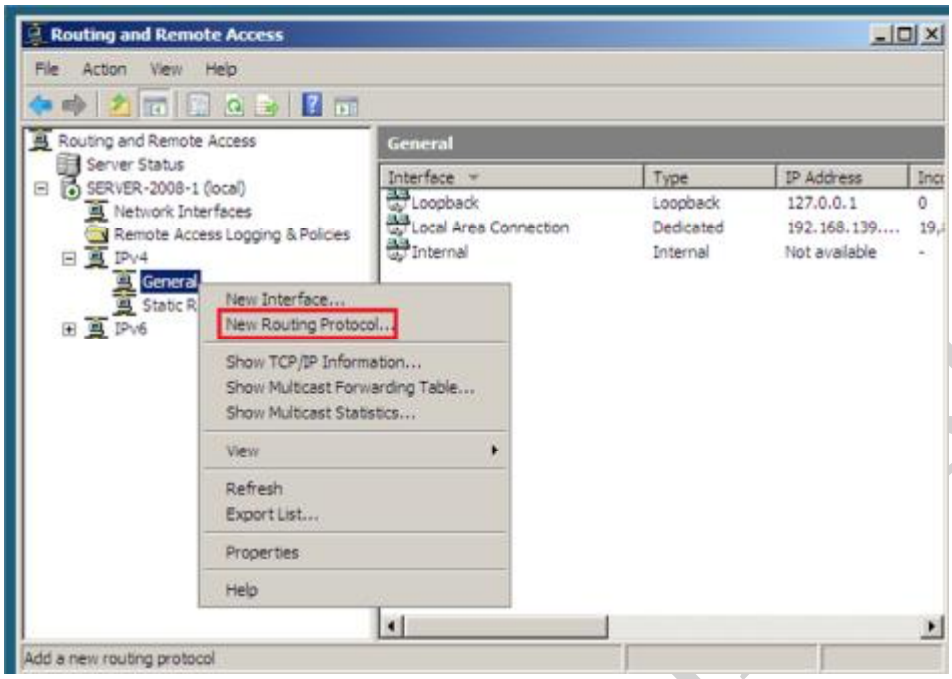


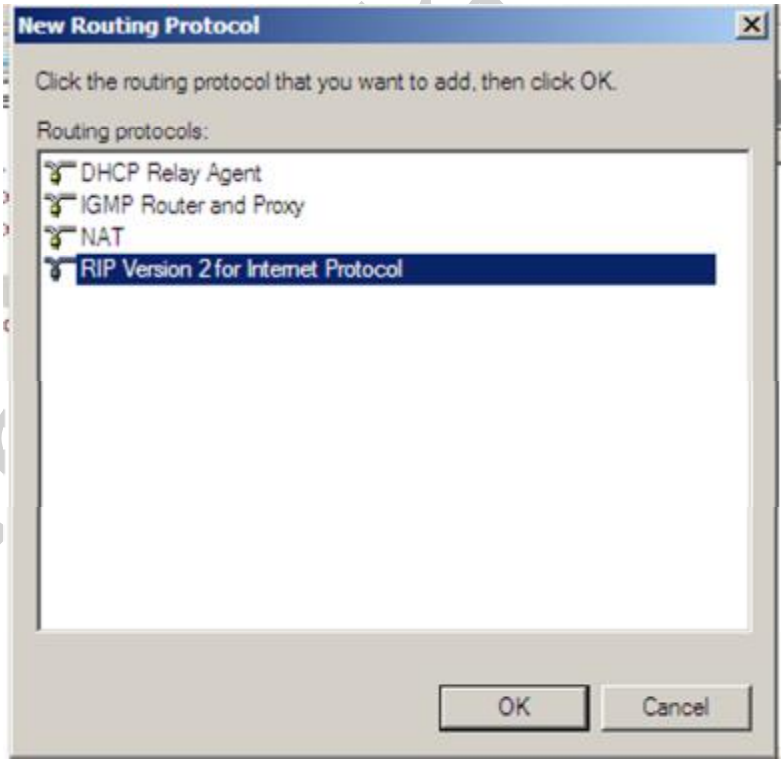

ابتدا پشت سرور1 تنظیمات بالا را انجام می دهیم در قسمت Interface کارت شبکه ای را انتخاب می کنیم که Ip20.0.0.1 روی آن تنظیم شده است در قسمت Ip–Destination مقصد را تنظیم می کنیم پشت سرور2 هم مانند بالا تنظیمات را انجام می دهیم.

احتیاج به این همه تنظیمات نمی باشد, راه آسان تر استفاده از تنظیمات زیر می باشد(اجرا کردن Routing Protocol )

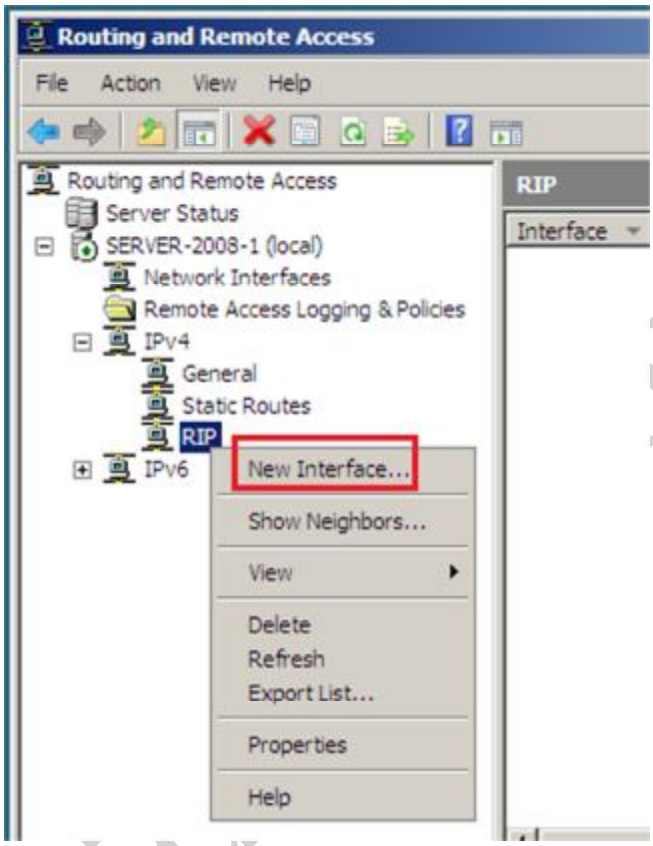
- در 2008 Routing Protocol که استفاده می شود RIP می باشد.

Farshid


Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
SERVER-2008-1 (local)
Network Interfaces
Remote Access Logging & Policies
IPv4
General
Static R
IPv6
General
Interface
Type
IP Address
Loopback
Loopback
127.0.0.1
Local Area Connection
Dedicated
192.168.139....
Internal
Internal
Not available
New Interface...
New Routing Protocol...
Show TCP/IP Information...
Show Multicast Forwarding Table...
Show Multicast Statistics...
View
Refresh
Export List...
Properties
Help
Add a new routing protocol


New Routing Protocol
Click the routing protocol that you want to add, then click OK.
Routing protocols:
DHCP Relay Agent
IGMP Router and Proxy
NAT
RIP Version 2 for Internet Protocol
OK
Cancel

**در آخر هم برای اینکه بتوانند همدیگر را ببینند باید کارت شبکه ها را به صورت زیر اضافه کنیم.**

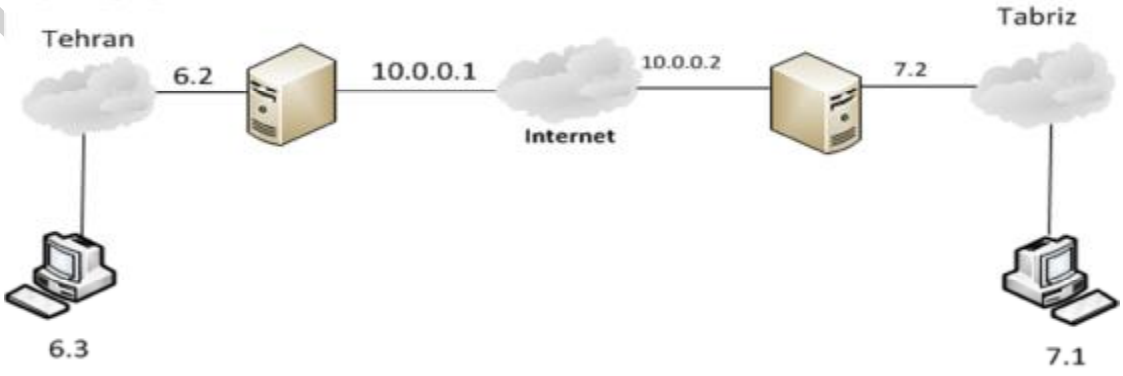



پیاده سازی VPN با RRAS

1) Site To Site VPN

**برای وصل کردن شعبات یک سازمان یا یک شرکت از این نوع VPN استفاده می کنیم.**

- **این نوع VPN با ISA,SERVER,ROUTER قابل پیاده سازی می باشد.**

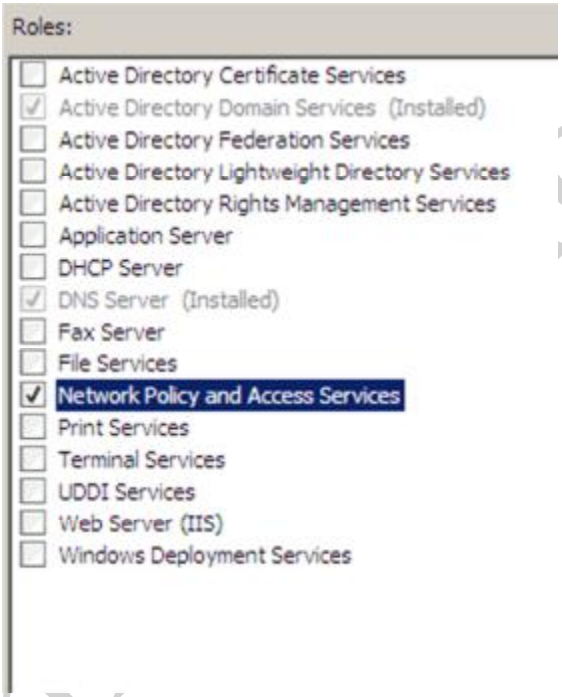


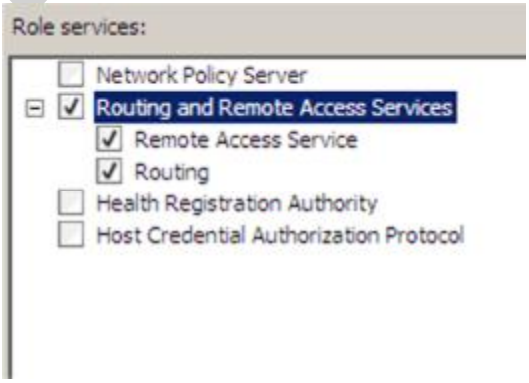
در شکل بالا بجای اینترنت می تواند هر بستر ارتباطی دیگری هم باشد.

- با توجه به شکل بالا هرکدام از سرورها باید 2 کارت شبکه داشته باشند که بر روی یکی IP Puplic و بر روی دیگری IP شبکه داخلی تنظیم شده باشد.
- در سرور 2008 سرویس RRAS نصب نیست وباید نصب شود ولی در 2003 این سرویس نصب می باشد.

برای نصب در 2008 ابتدا وارد AddRoles می شویم وسپس مانند زیر عمل می کنیم

سرور تهران:

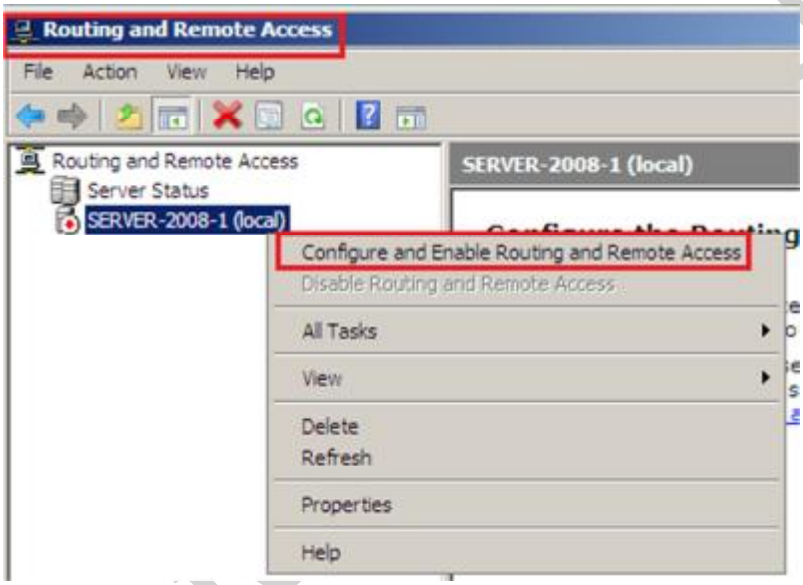


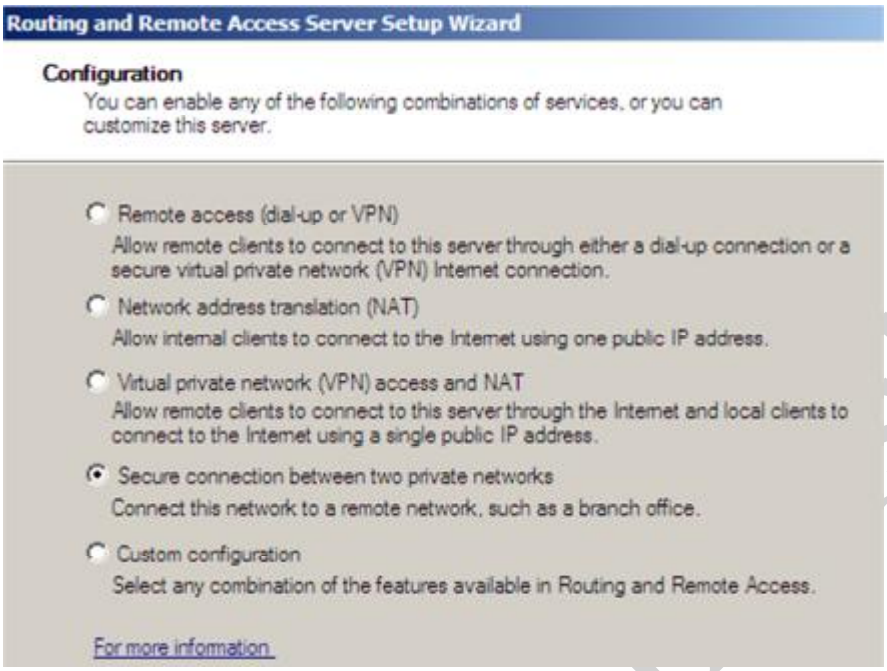

Farsh Soush

**بعد از اتمام نصب در سرور تهران باید تنظیمات زیر را انجام دهیم :**

**ابتدا وارد کنسول RRAS می شویم (Routing and Remote Access ) سپس باید روی اسم سرور کلیک راست کنیم وRRAS را فعال کنیم**

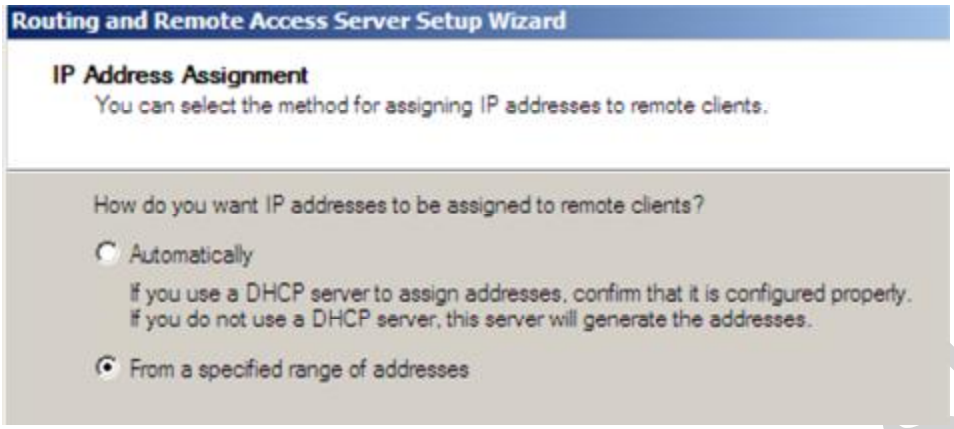



Farshid Yousefi



- **با فعال بودن Demand-Dial زمانی که کامپیوتری از تهران بخواهد به کامپیوتر دیگری در تبریز وصل شود ابتدا سرور تهران ارتباط را با سرور تبریز برقرار می کند(Connect) سپس کامپیوترها به هم وصل می شوند و پس از اتمام کار هم ارتباط بین سرورها را قطع می کند(Disconnect ).**

**در مرحله بعد از ما می پرسد در صورت وصل شدن از تبریز به تهران(خودمان) سیستم ها IP شان را از کجا بگیرند؟ از سرور DHCP داخل شبکه تهران یا از یک رنج مشخص,که باید گزینه دوم را انتخاب کنیم ویک رنج کاملا نامشخص (الکی J ) انتخاب کنیم.**

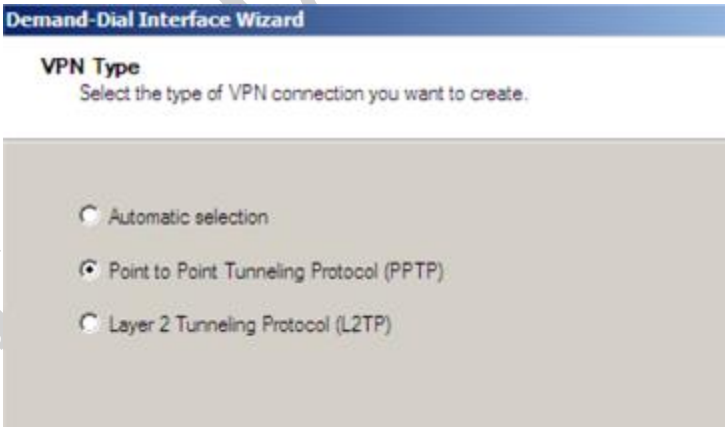


و در آخر هم Finish,بعد از Finish کردن بلافاصله Setup مربوط به Demand-Dial باز می شود,ازما سوال میکند که اسم کانکشن را مشخص کن بهتر است اسم شعبه مقابل(تبریز)را وارد کنیم.

Farshid Rush

در مرحله بعد از ما سوال می کند که با چه کانکشنی می خواهید وصل شوید,گزینه اول ISDN برای وصل شدن با خطوط E1و... می باشد به این دلیل غیر فعال می باشد که بر روی سیستم Modem Dial-up نداریم,گزینه سوم با کانکشن های DSL ,گزینه دوم با کانکشن VPN

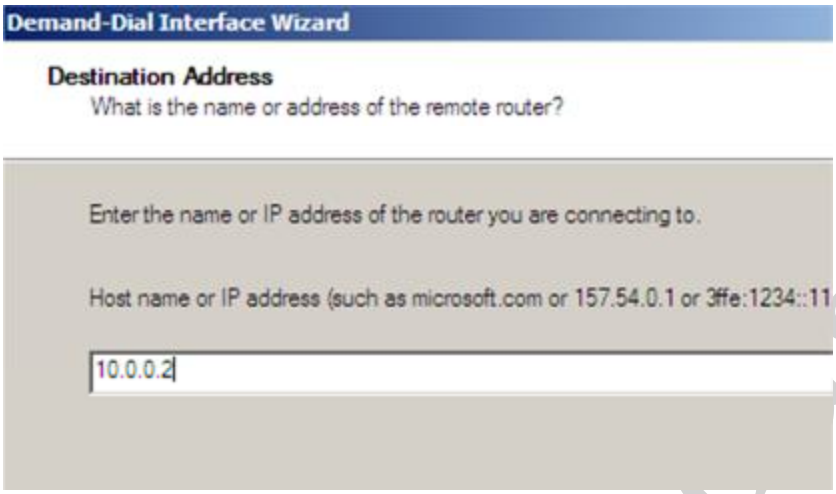
در مرحله بعد از ما نوع VPN را می پرسد




در اینجا PPTP را انتخاب می کنیم البته تفاوتی با L2TP ندارد تنها تفاوتش این است که در L2TP در هنگام وصل شدن در هر دوطرف از ما پسورد می پرسد که باید پسورد یکسان باشد.

- بین 2 شعبه نمی توان به صورت SSTP VPN (SSL) زد,البته با نرم افزار OpenVPN می توان این کار را انجام داد.

در مرحله بعد از ما IP Public تبریز را می پرسد

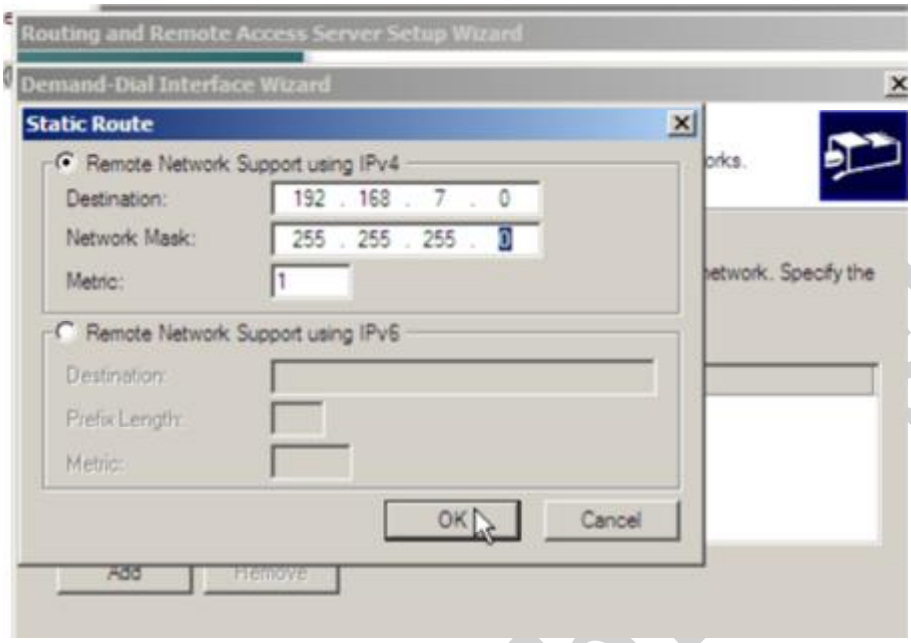



- هر وقت صحبت از VPN می شود باید IP Public در هر2 طرف وجود داشته باشد.

در مرحله بعد باید هر2 گزینه را انتخاب کنیم ,گزینه اول به ما می گوید تمامی روت ها بر روی کانکشن ساخته شده از قبل انجام می گیرد و با فعال بودن گزینه2 یوزروپسورد می سازیم که از شعبه مقابل با این یوزروپسورد بتوانند به ما وصل شوند.

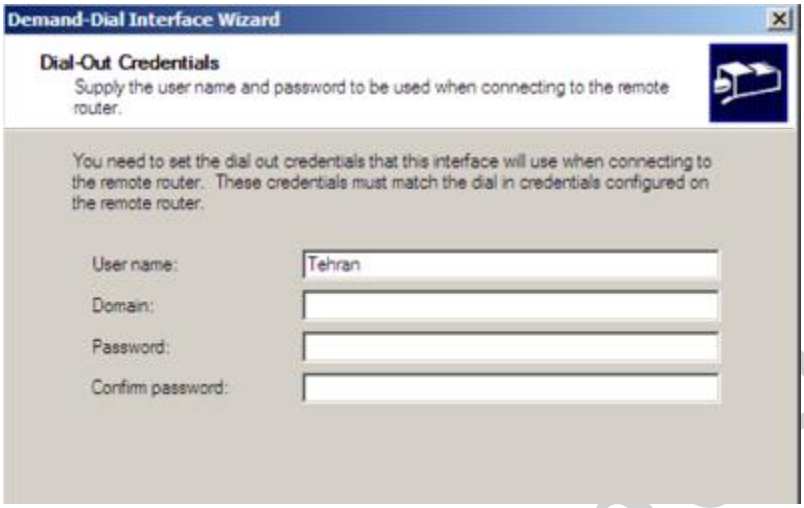
Fa Nabnesh

در مرحله بعد باید رنج IP داخلی شبکه  تبریز را وارد کنیم



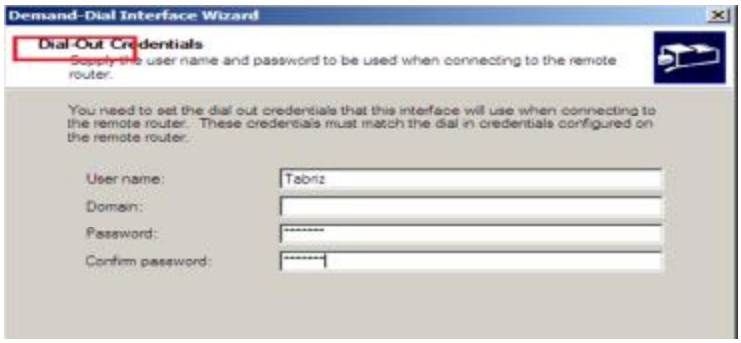

در اینجا باید برای وصل شدن از سرور تبریز به سرور تهران یک یوزر و پسورد تعریف شود,همانطور که می بینید یوزر ما برابر است با اسم Interface که در ابتدا وارد کردیم,بعد از اتمام این مرحله باید یوزر و پسورد موجود در این صفحه را به تبریز بدهیم تا بتوانند به ما وصل شوند.

در مرحله بعد از ما (تهران) سوال میکند که برای وصل شدن به تبریز چه یوزر و پسوردی دارید؟(این یوزر وپسورد را باید از تبریز بگیریم و در اینجا تنظیم کنیم)

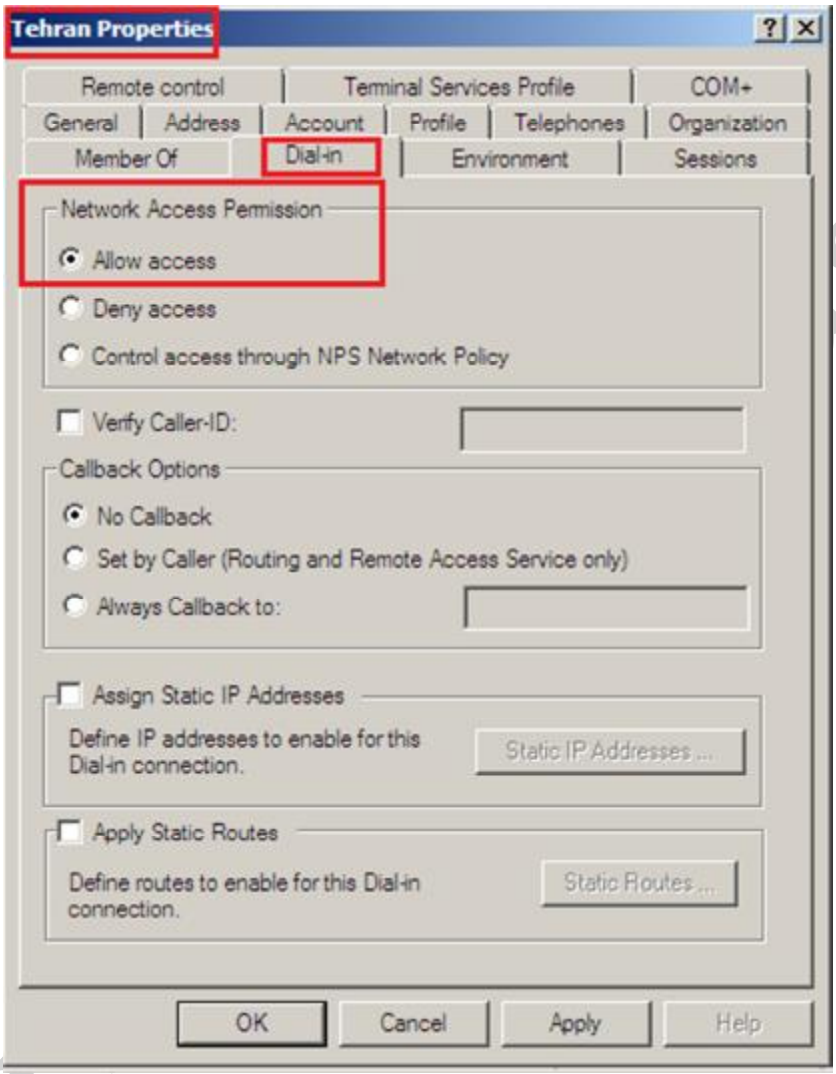



کار در پشت سرور تهران تمام شد حالا باید تنظیمات را در سرور تبریز هم اعمال کنیم،برای این کار باید پشت سرور تبریز بنشینیم و تمامی تنظیمات را مانند بالا انجام دهیم فقط یک کار را انجام نمی دهیم آن هم این است که گزینه دوم در شکل زیر را انتخاب نمیکنیم به این دلیل که یادبگیریم به صورت دستی این گزینه را فعال کنیم.

بعداز این مرحله مانند زیر عمل می کنیم،به این صفحه که رسیدیم یوزر پسورد تبریز را که در سرور تهران وارد کردیم دوباره در اینجا (تبریز) وارد می کنیم.

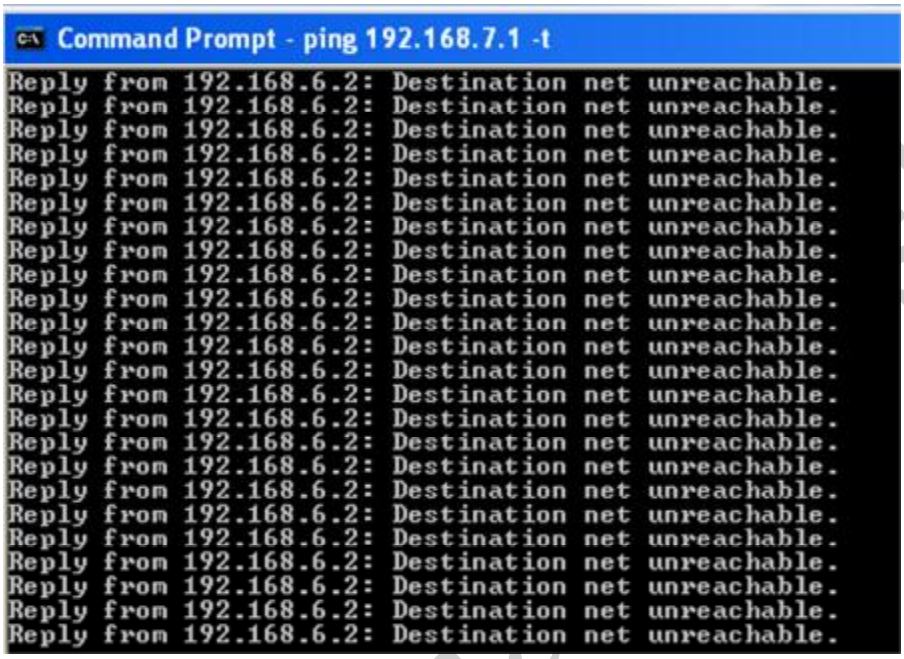


در اینجا (تبریز) باید یوزرتهران را به صورت دستی وارد کنیم,برای این کار ابتدا یک یوزر می سازیم به نام تهران و مانند زیر عمل می کنیم



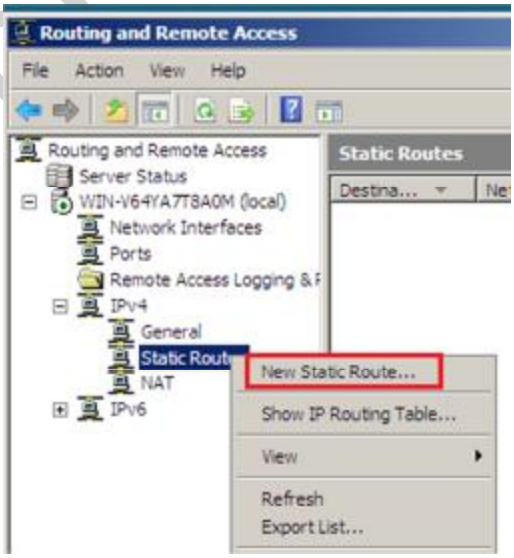

سپس وارد تب Dial-in می شویم و Allowaccess را فعال می کنیم.

برای وصل شدن از کلاینت تهران(192.168.6.1) به کلاینت تبریز(192.168.7.1) و با لعکس باید ابتدا در هر دو کلاینت GW هایشان را IP های سرور خودشان بگذاریم یعنی GW تهران 192.168.6.2 وتبریز192.168.7.2 می باشد, حال برای برقراری ارتباط از کلاینت تهران به کلاینت تبریز ابتدا تبریز را Ping می کنیم که با مشکل زیر مواجه می شویم

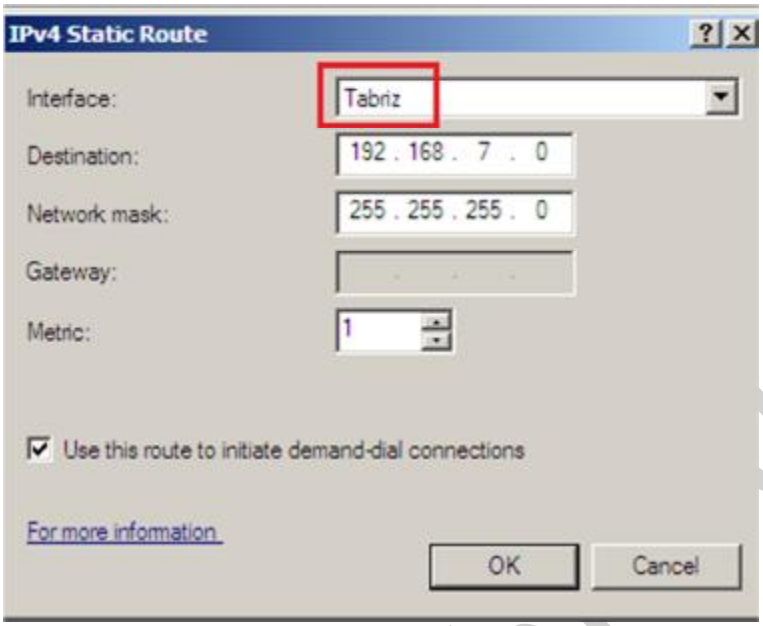



این مشکل به این دلیل به وجود آمده است که StaticRoute که در Site to Site VPNتعریف کرده بودیم(در سرور)از بین رفته است این مشکل سرور2008 می باشد در نسخه R2 این مشکل برطرف شده است,برای رفع مشکل در اینجا مانند زیر عمل می کنیم

پشت هر 2 سرور این کار باید انجام گیرد ابتدا پشت سرور تهران

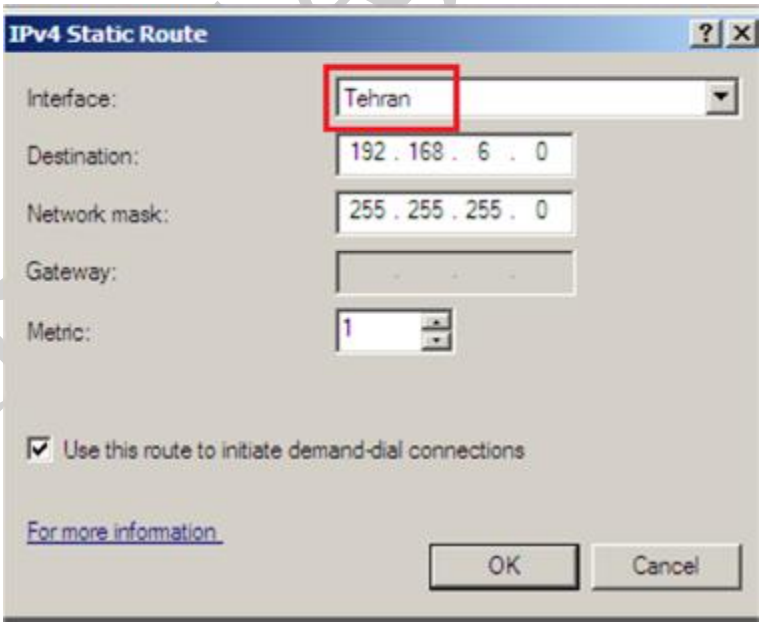



FarshidAsgh



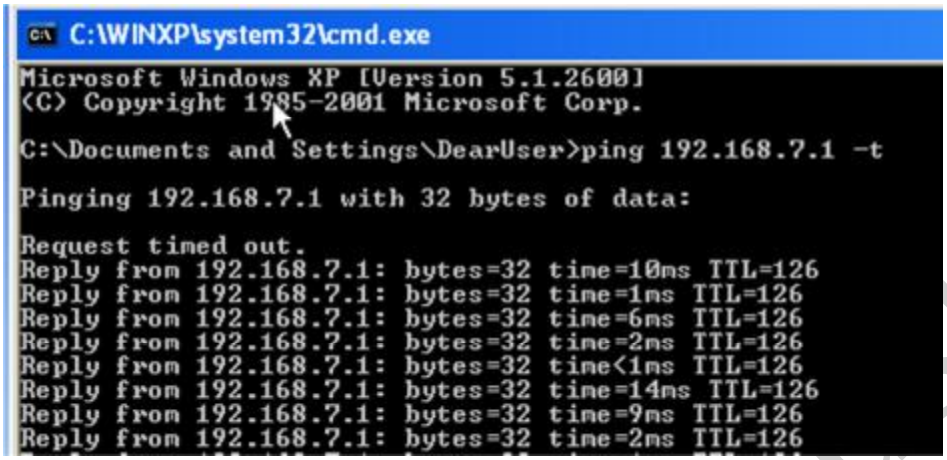

در سرور تهران, Interface را Tabriz انتخاب می کنیم و رنج داخلی شبکه تبریز را وارد می کنیم(شکل بالا)

در سرور تبریز,Interface را Tehran انتخاب می کنیم و رنج داخلی شبکه تهران را وارد می کنیم (شکل پایین)

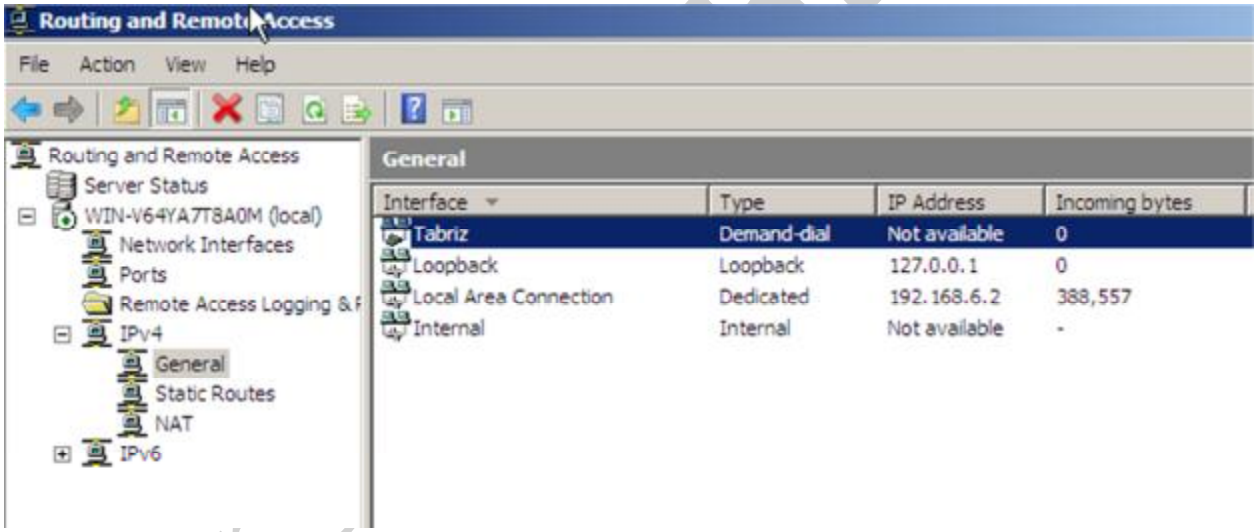



Fa Ajabi ush

و در آخر هم از کلاینت تهران Ping کلاینت تبریز را می گیریم.




سرور تهران




در اینجا می توان زمان وصل شدن کلاینت ها و... را به یکدیگر مشخص کرد.

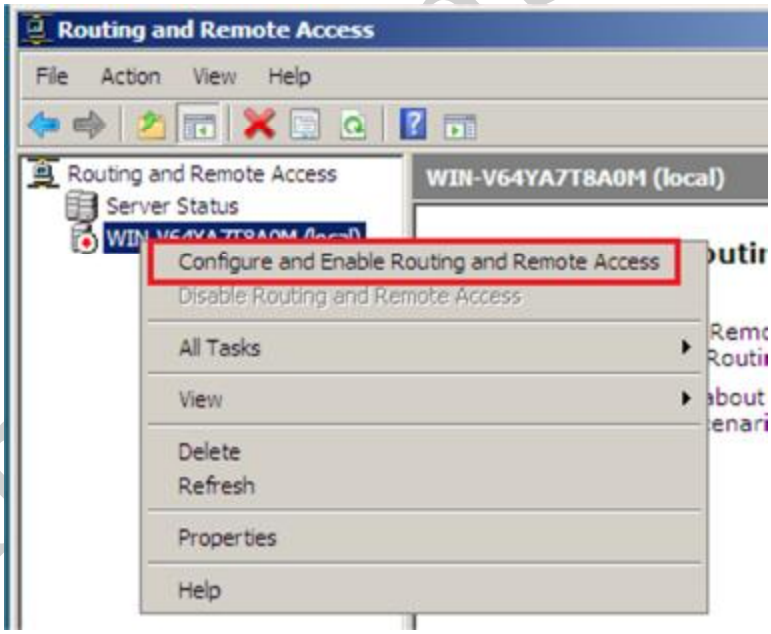
Farahnoush

Remote Access

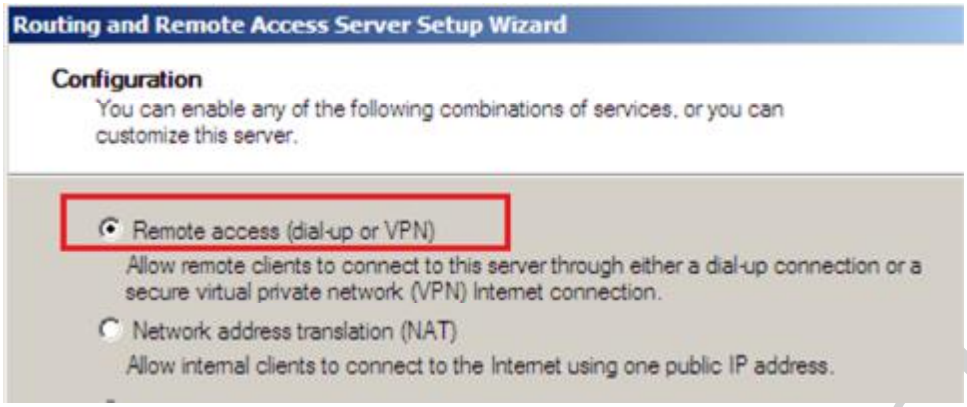
**هنگامی که سروری دریک کشور دیگر (کانادا) داریم وکلاینت ها از سراسر دنیا به آن وصل می شوند و از اینترنت آن استفاده می کنند به این نوع Remote Access, VPN گویند(VPN های مورد استفاده در حال حاضر از این نوع می باشند)**

- **به سرور VPN که در یک کشور دیگر قرار گرفته است VPS گویند.**
- **VPN تکنولوژی است که حداقل 2 شبکه Private را تحت بستر عمومی (مثل اینترنت )به هم وصل می کند.**
- **برای راه اندازی VPS حداقل باید 2 کارت شبکه بر روی سرور وجود داشته باشد.**
- **راه اندازی VPS در 2008 و2003 تفاوتی ندارد.**

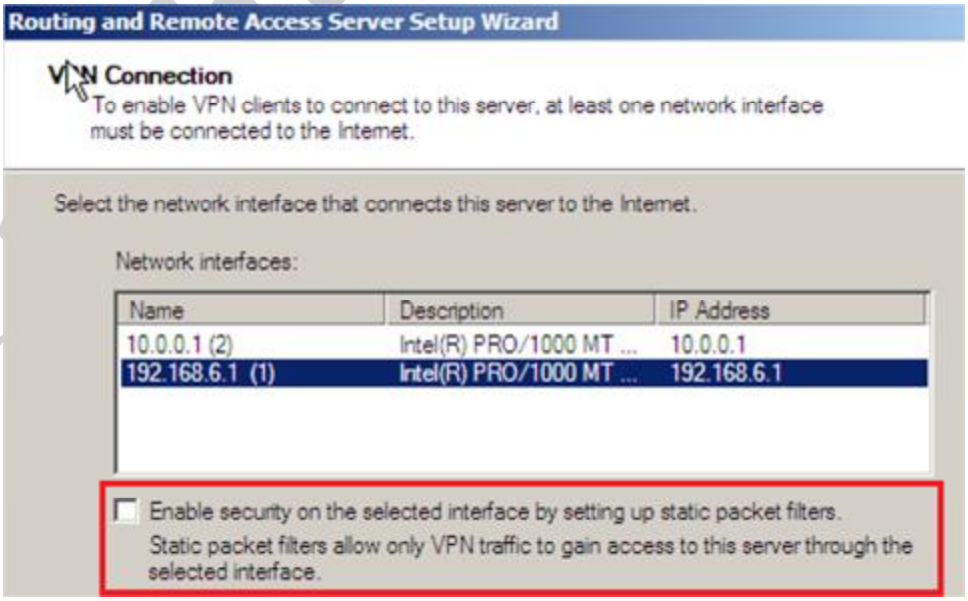
**برای راه اندازی Remote Access مانند زیر عمل می کنیم**




Farnoush

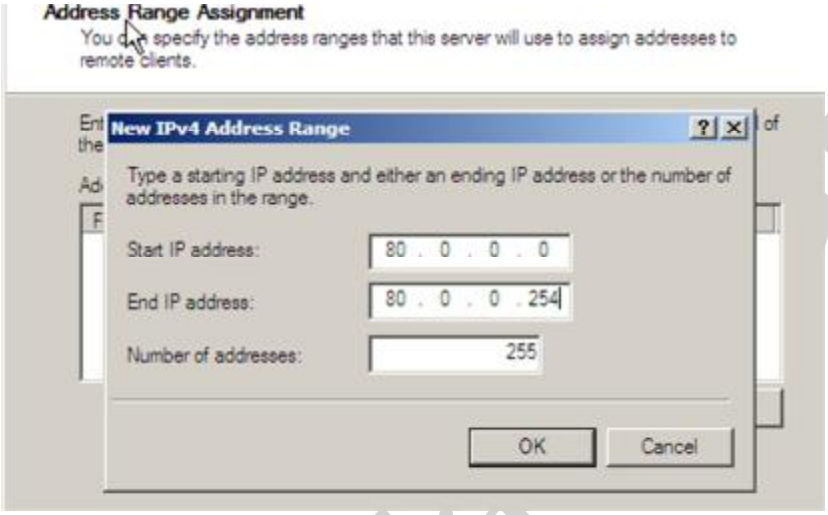


به سرور VPN Gateway, VPN هم گویند.

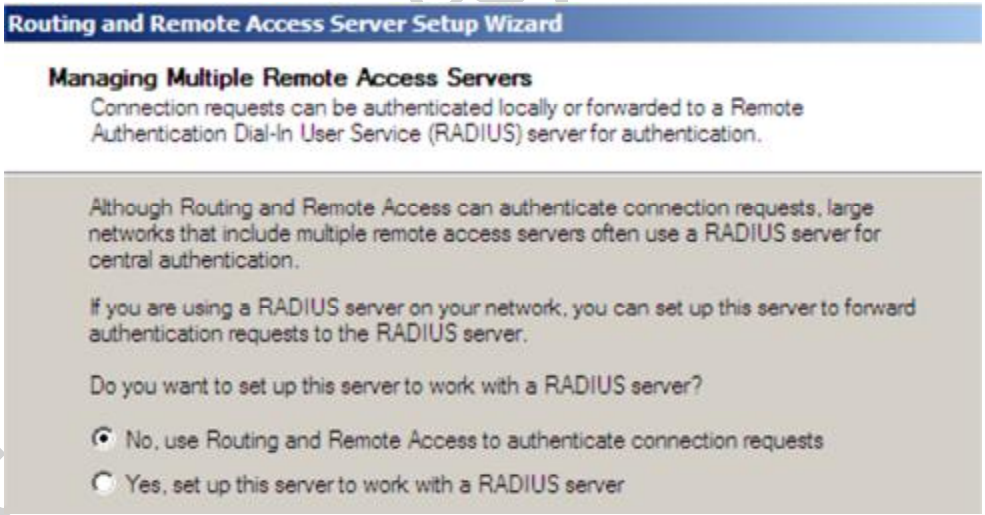


درمرحله قبل باید گزینه مورد نظر غیرفعال باشد,اگر این گزینه فعال باشد فایروال بر روی VPN فعال می شود و یک سری از ترافیک ها را فیلتر می کند که باید در فایروال به صورت دستی آن ترافیک ها را باز کنیم,در مورد IP ها باید IP را انتخاب کنیم که از طریق آن به ما VPN می زنند (Public–IP External ) در اینجا کارت شبکه 1 می باشد.

یک رنج نا مشخص وارد می کنیم




در اینجا از ما سوال می پرسد که RADIUS در شبکه داریم,کار RADIUS احراز هویت در شبکه بود.



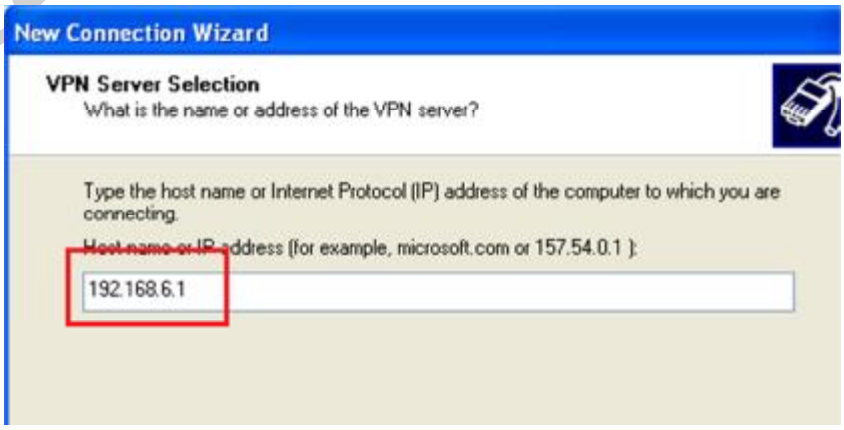

و در آخر هم Finish .

حالا نوبت به ساخت کانکشن VPN بر روی کلاینت می باشد برای این کار مانند زیر عمل می کنیم

New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

New Connection Wizard
Network Connection
How do you want to connect to the network at your workplace?
Create the following connection:
Dial-up connection
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
Virtual Private Network connection
Connect to the network using a virtual private network (VPN) connection over the Internet.

New Connection Wizard
Connection Name
Specify a name for this connection to your workplace.
Type a name for this connection in the following box.
Company Name
Testh
For example, you could type the name of your workplace or the name of a server you will connect to.

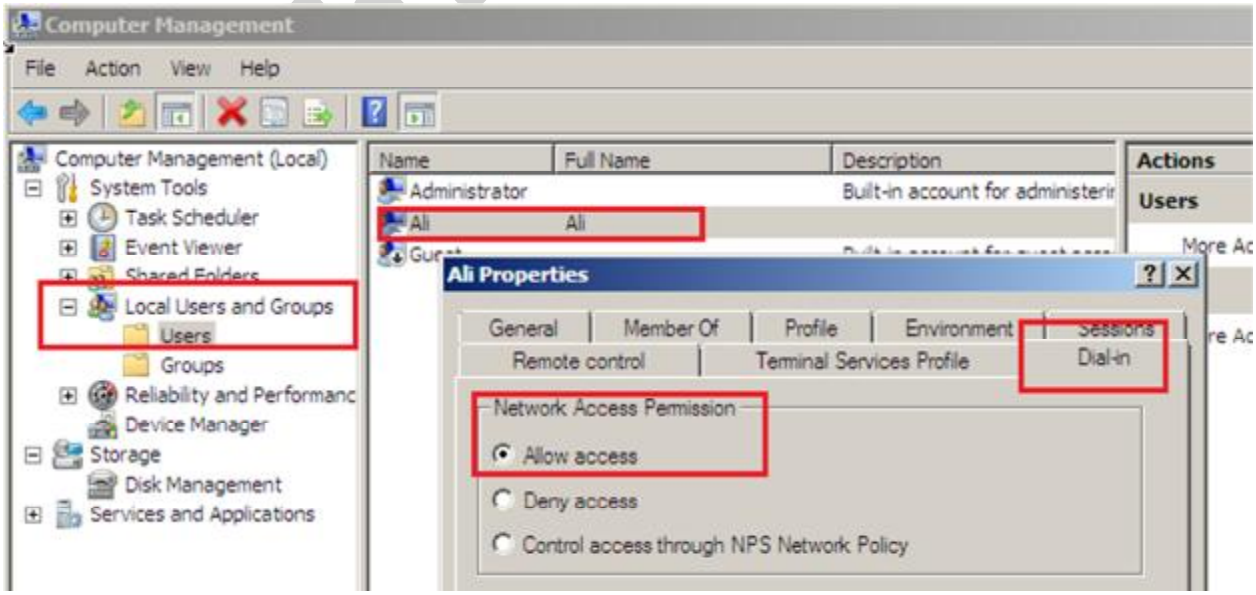

New Connection Wizard
VPN Server Selection
What is the name or address of the VPN server?
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.
Host name or IP address (for example, microsoft.com or 157.54.0.1 ):
192.168.6.1

Fa... ...ash

در مرحله قبل (شکل بالا باید IP را که در سرور انتخاب کرده ایم را وارد کنیم)

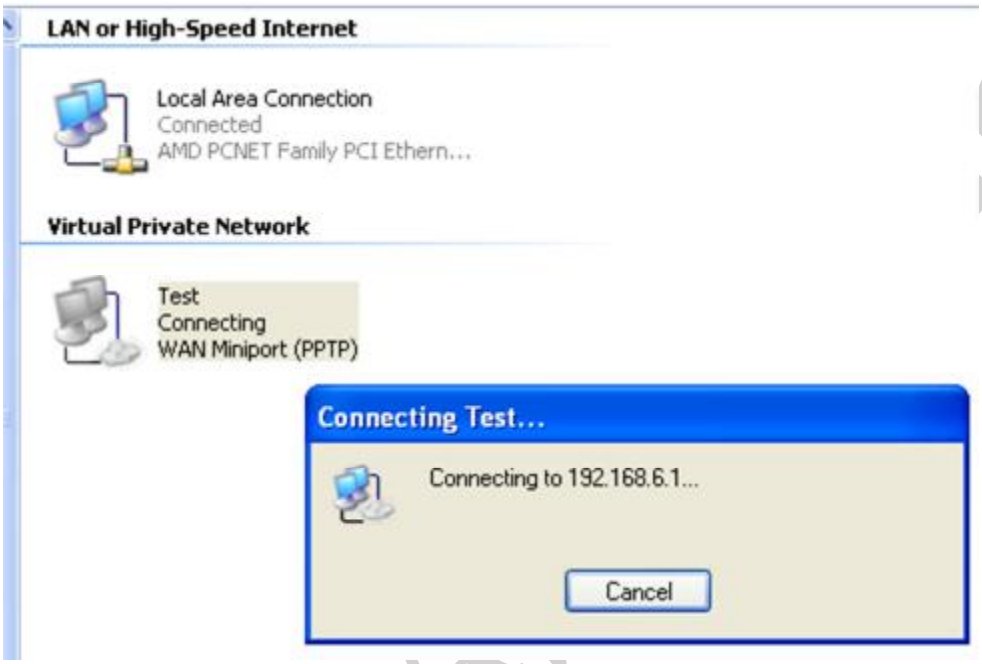
با تمام شدن مرحله ساختن با صفحه زیر برخورد می کنیم.

در اینجا احتیاج به یوزر و پسورد داریم اگر RADIUS داشتیم باید در آن یوزر را می ساختیم ولی حالا که نداریم پشت خود ویندوز سرور می سازیم (در سرور اکتیو دایرکتوری نداریم و بصورت Local می سازیم).



بعد از ساختن یوزر حتما باید گزینه Allow access فعال کنیم با این کار اجازه ریموت شدت به سرور (VPN زدن ) را به این یوزر  می دهیم.

این نوع VPN از نوع PPTP می باشد.

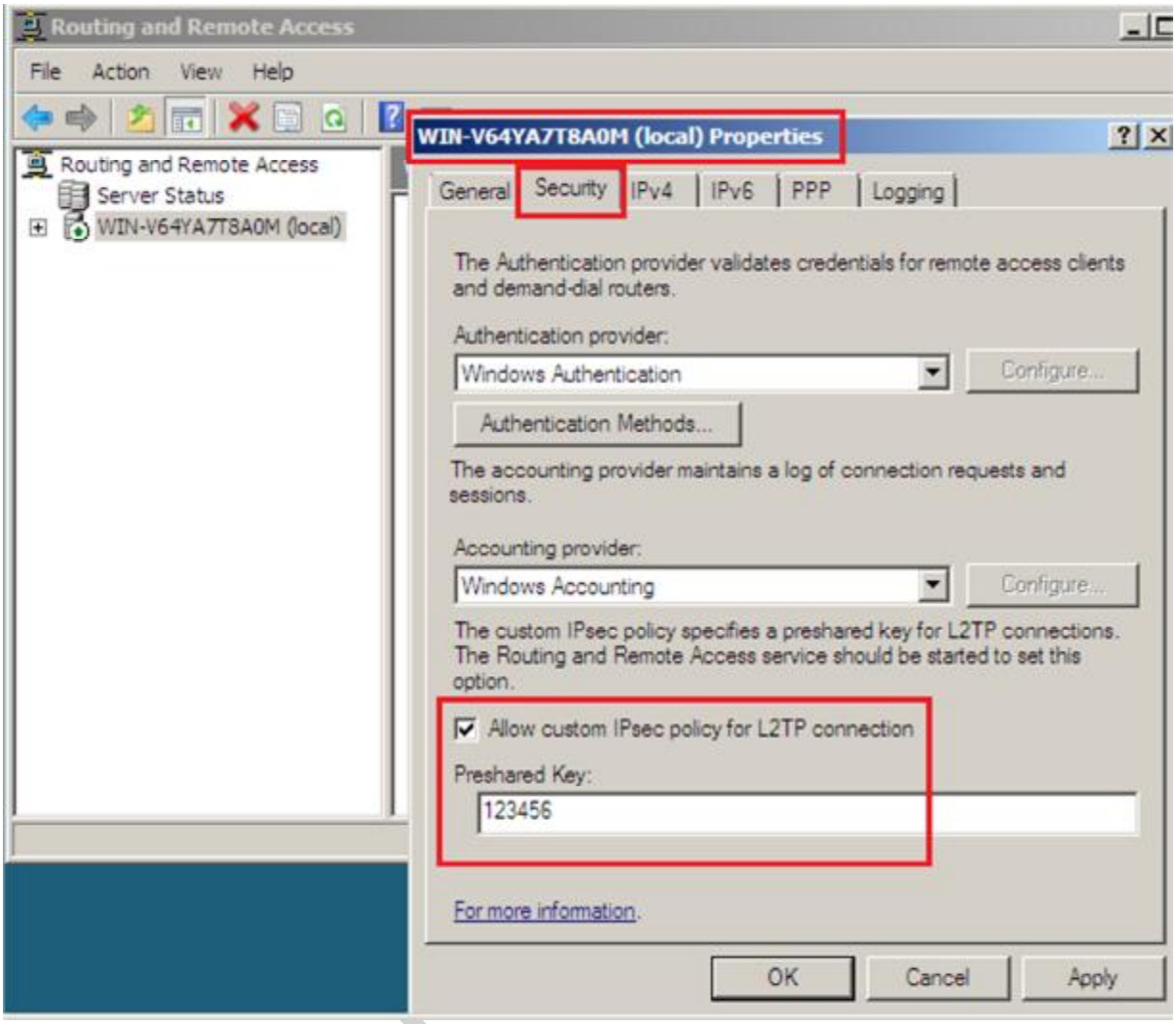



برای خرید سرور VPN در ایران Mihanserver.com

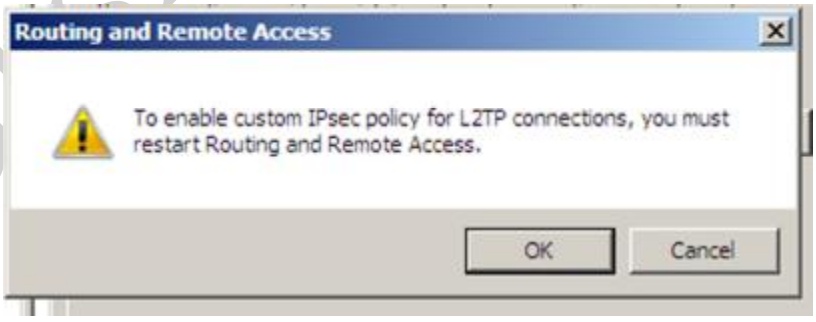
L2TP VPN

امنیت  L2TP از PPTP بیشتر است, برای راه اندازی  L2TP مانند زیر عمل می کنیم

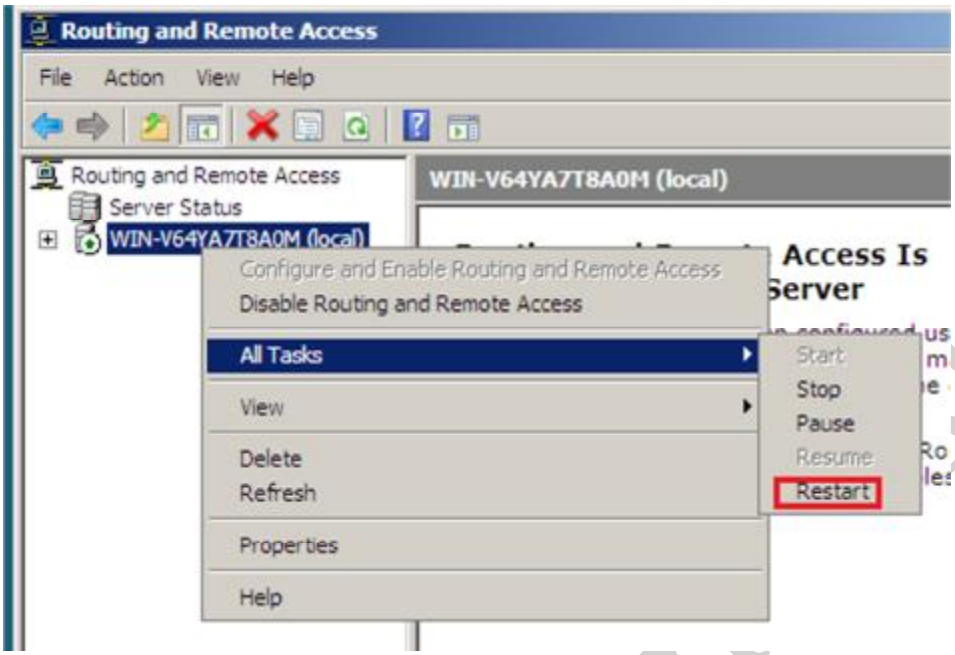
Farshid



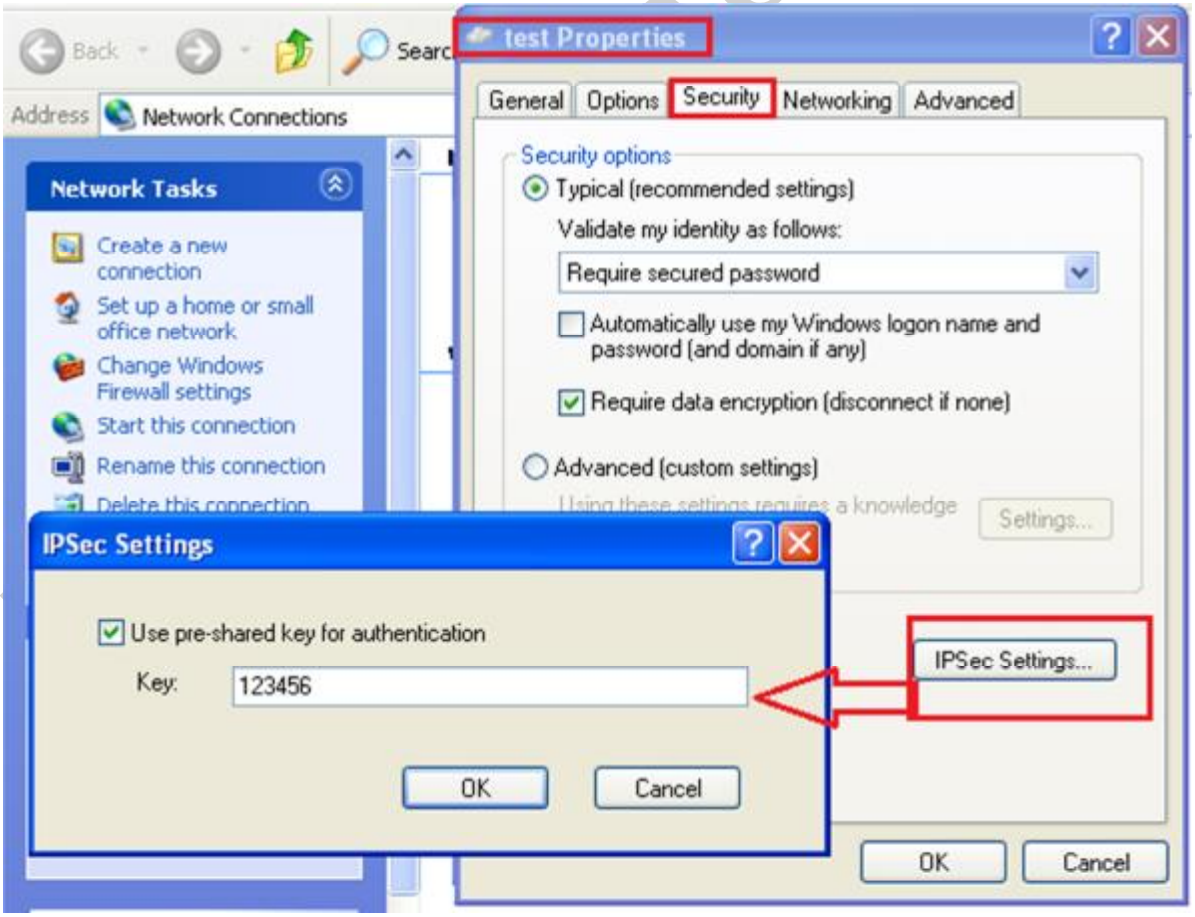

**بعد از اتمام با پیغام زیر مواجه می شویم که کنسول RRAS را باید یکبار ریستارت کنیم**

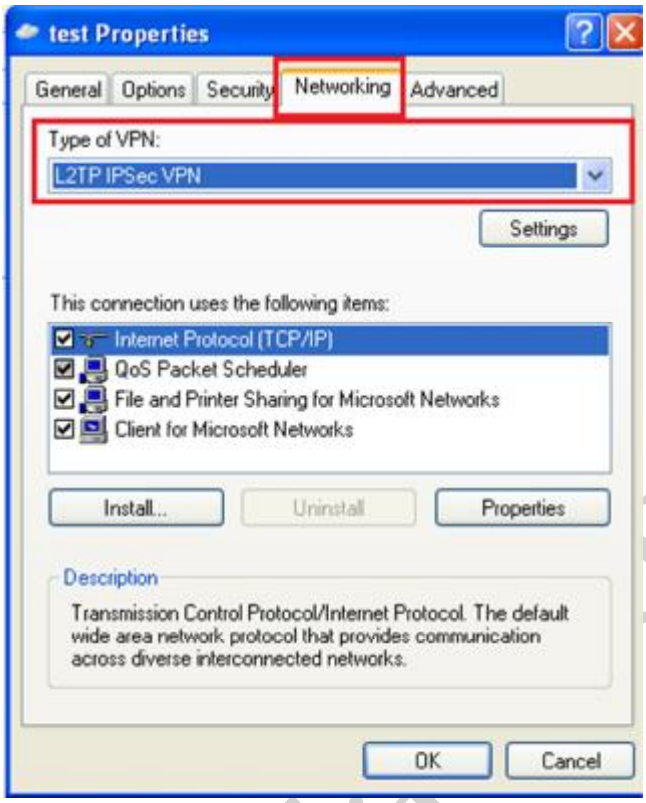


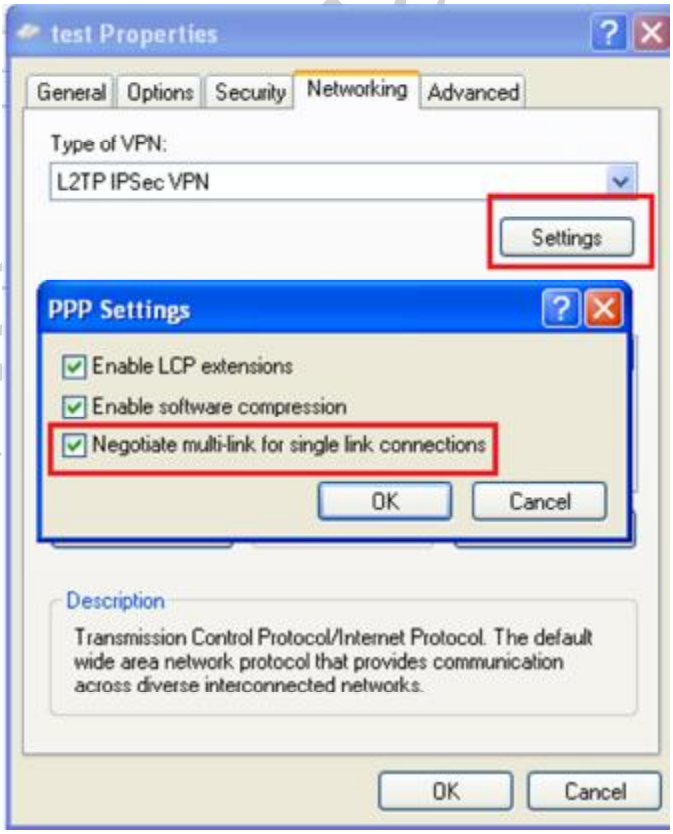

Farshad




**حالا نوبت به تنظیم در کلاینت می باشد**



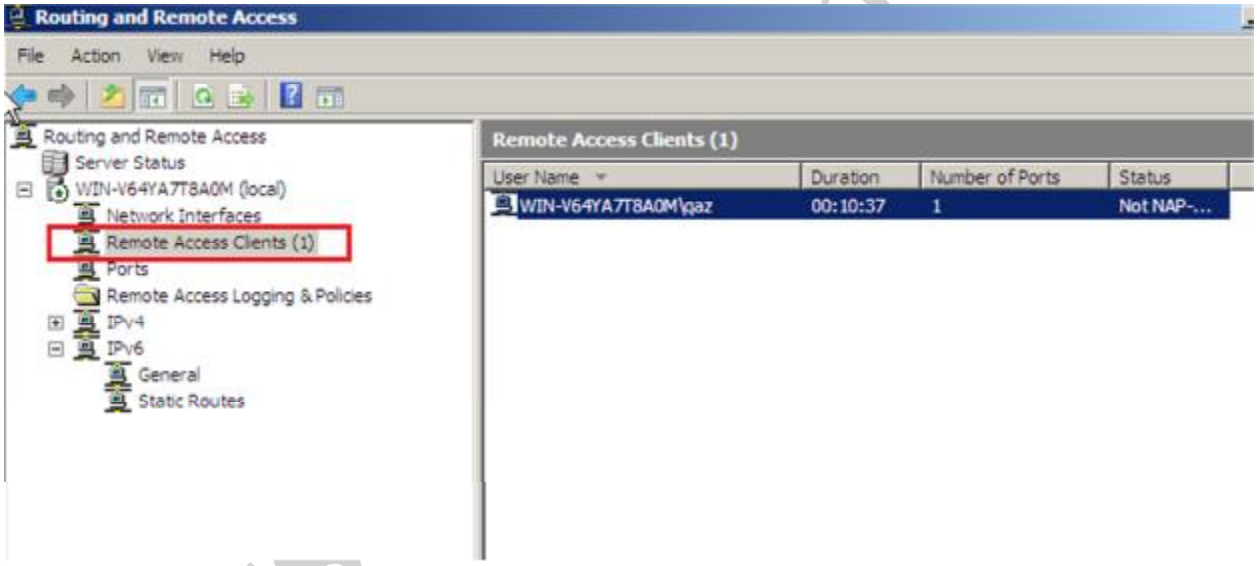


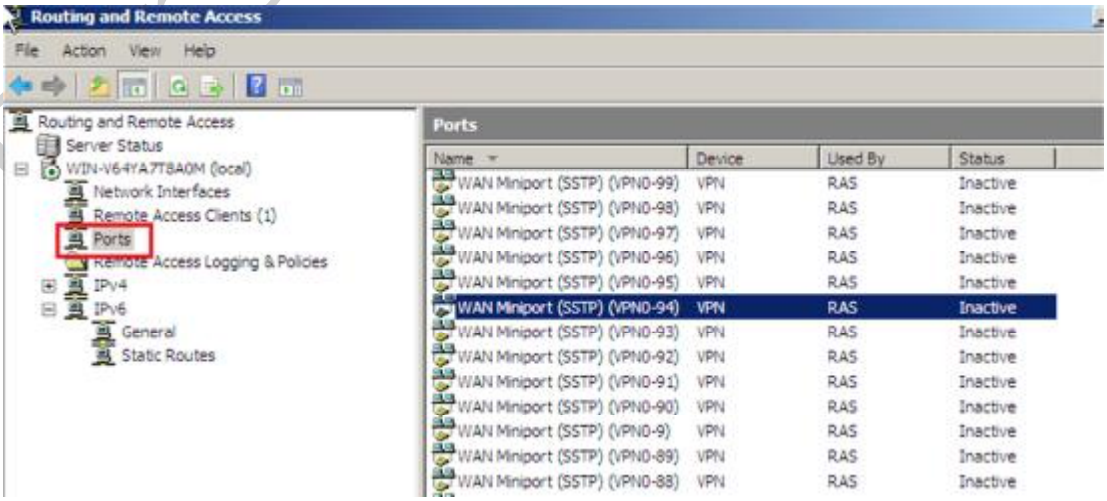




Farnaz Kiaroush

با فعال سازی این گزینه(شکل بالا) اگر بیش از یکی کانکشن VPN داشته باشیم و سرعت های آنها هم متفاوت باشد سرعت کانکشن ها را در هنگام برقراری ارتباط,با هم یکی می کند 100 k+200k=300k

با وارد شدن به کنسول زیرمی توانیم متوجه شویم که چند نفر و با چه یوزرهایی به سرور ما VPN زده اند



در قسمت پورت به ازای هر PPTP, L2TP, SSTP, 128 کانکشن وجود دارد یعنی 3*128 کانکشن که می توانیم آن را کم یا زیاد کنیم.

- پورت PPTP 1723 می باشد, L2TP 50و51 ,SSTP 443 می باشد.
- بهترین مکان برای تعویض کردن پورت ها رجیستری می باشد.

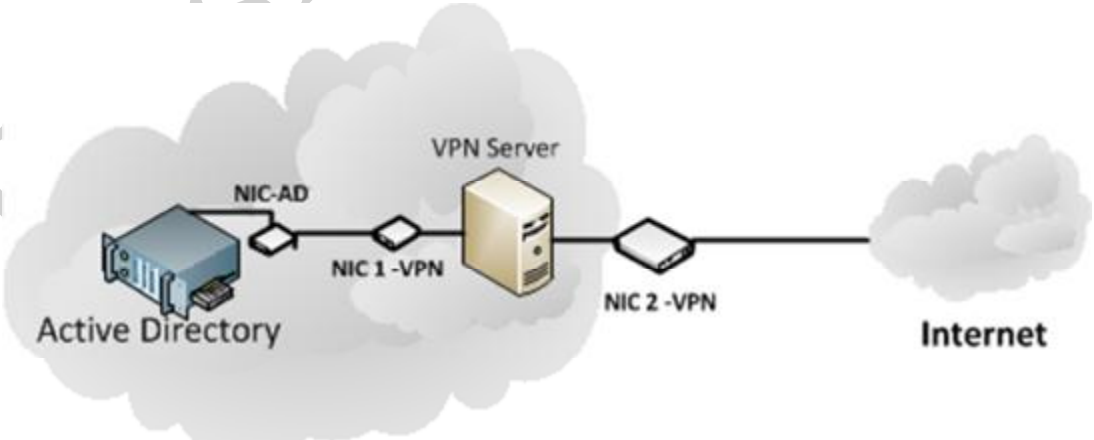
SSTP VPN on 2008

در 2003 نمی توان SSTP پیاده سازی کرد ولی با استفاده از نرم افزار OpenVPN می توان این کار را انجام داد(openvpn.se ) .

- SSTP VPN احتیاج به Domain دارد پس باید AD نصب کنیم.
- SSTP را نمی توان فیلتر نکرد.

قبل از راه اندازی SSTP باید مرا حل زیرانجام شود:

1. Install Active Directory
2. Join RRAS to Domain
3. Install Certificate Authentication Server
4. Get Certificat
5. Install Certificate for Computer Account
6. Install RRAS and Configur VPN
7. Change Host File
8. Get Certificate
9. Install Certificate for Computer Account
10. SSTP VPN to Server




SSTP Modeling

RashidAjabnoush

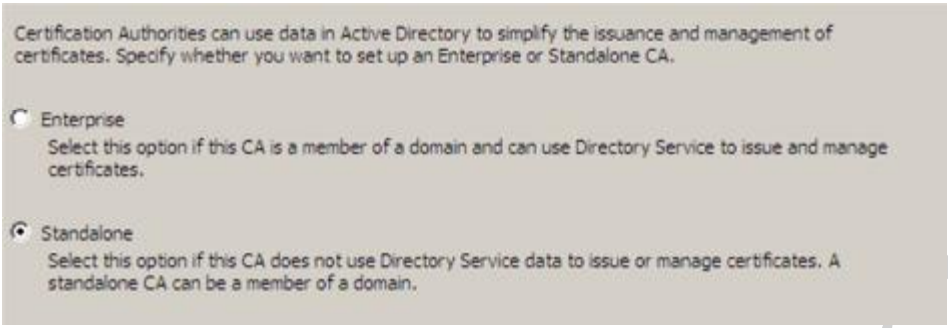
- برای پیاده سازی سناریو فوق بهتر است سرورAD وVPN از هم جدا باشند چون یک دست VPN روی اینترنت می باشد,اگرهر2 پشت یک سرور باشند امنیت اکتیو پایین می آید(به دلیل اینترنت VPN )
- در این سناریو کارت شبکه 6.200 سمت اکتیو دایرکتوری می باشد و 7.200 کارت شبکه External (خروجی VPN– می باشد)
- قبل از ساختن CA باید ساعت و تاریخ در سرور و کلاینت تنظیم باشد در غیر اینصورت کار نمی کند.

در ابتدا باید اکتیو دایرکتوری نصب کنیم سپس پشت سرور اکتیو, CA Server نصب کنیم

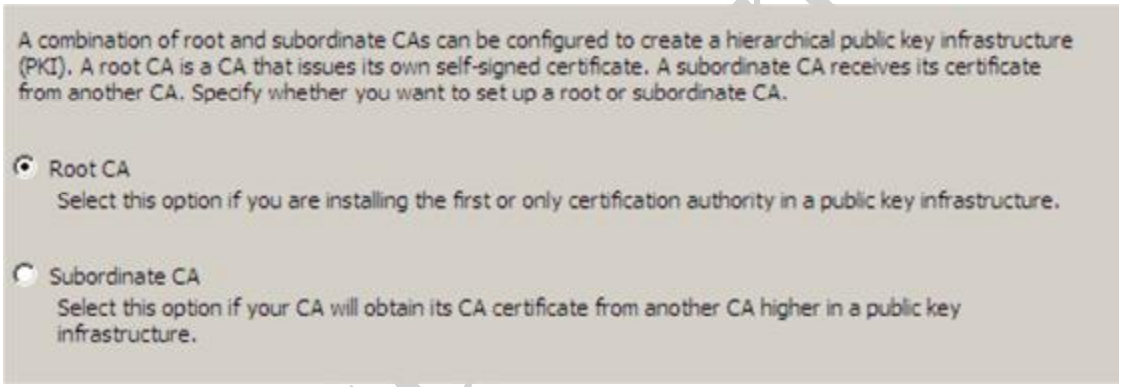
با انتخاب گزینه 2 در مرحله بعد,تمامی کلاینت های ما می توانند از طریق Certificate, Browser دریافت کنند.

در مرحله بعد اگر اکتیو و CA پشت یک سرور بود گزینه1 و اگر هر کدام مجزا نصب شده بودند گزینه2 را انتخاب می کنیم.

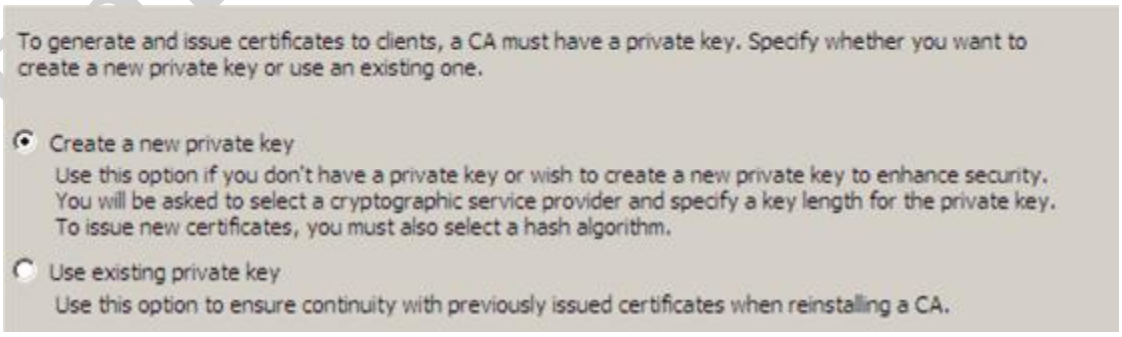
- در SSL VPN حتی اگر AD و CAپشت یک سرور باشند باز باید گزینه2 را انتخاب کنیم.




**اگر شما وابسته به CA سروری هستید (در ایران وزارت بازرگانی ) باید گزینه 2 را انتخاب کنیم ( در واقعیت باید این گزینه را انتخاب کنیم) اگر خودتان مستقل هستید یعنی یک CA مجزا دارید باید گزینه 1 را انتخاب کنید( در این سناریو گزینه1)**

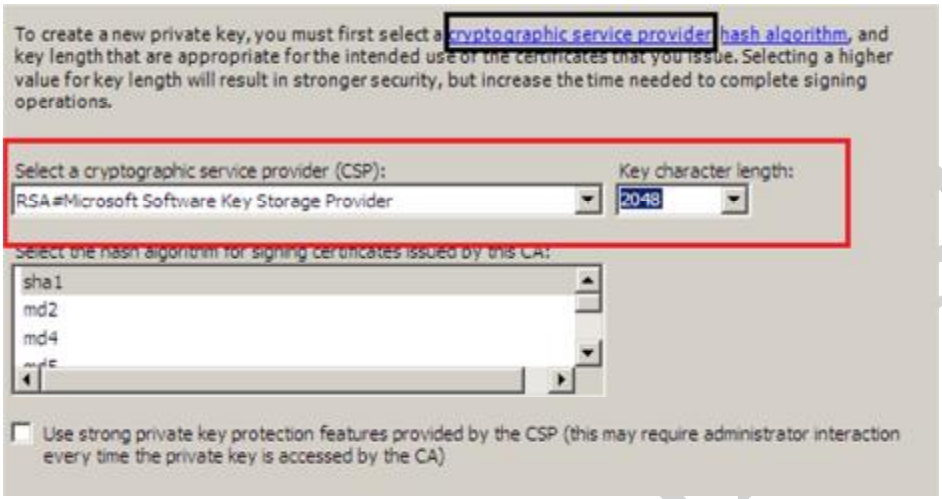



**در مرحله بعد از ما سوال می کند که Private Key داریم یا بسازم اگر داشته باشیم گزینه2 (در ایران اگر از وزارت بازرگانی فلش گرفته باشیم از این گزینه استفاده می کنیم) و اگر نداشته باشیم گزینه 1**

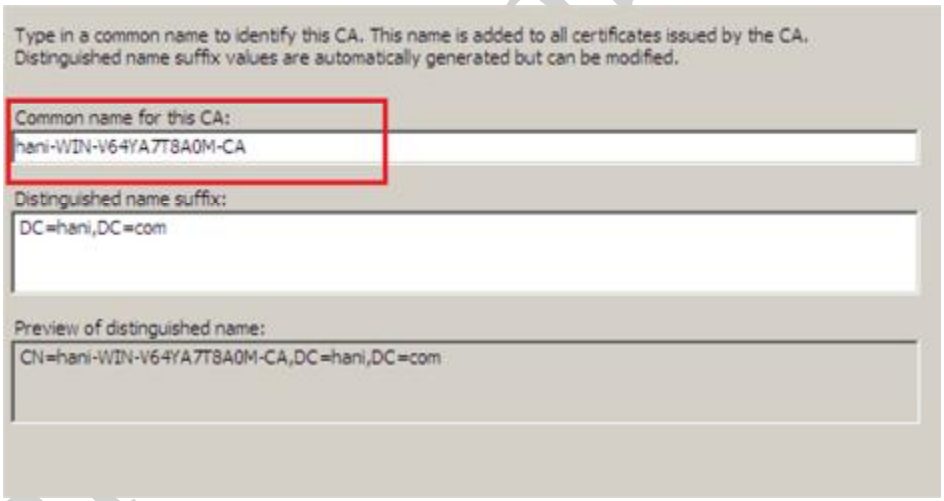


در این مرحله نوبت به مشخص کردن الگوریتم و طول کلیدهایمان می باشد که در اینجا فقط Next می کنیم

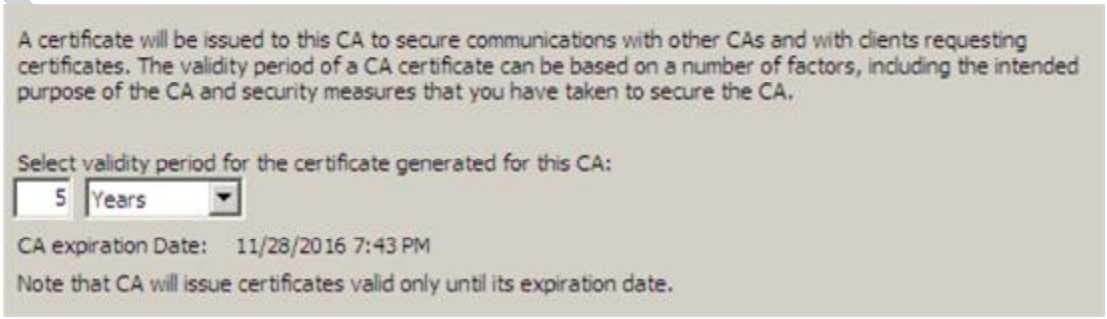
- به علم رمز نگاری CryptoGraphic گویند.



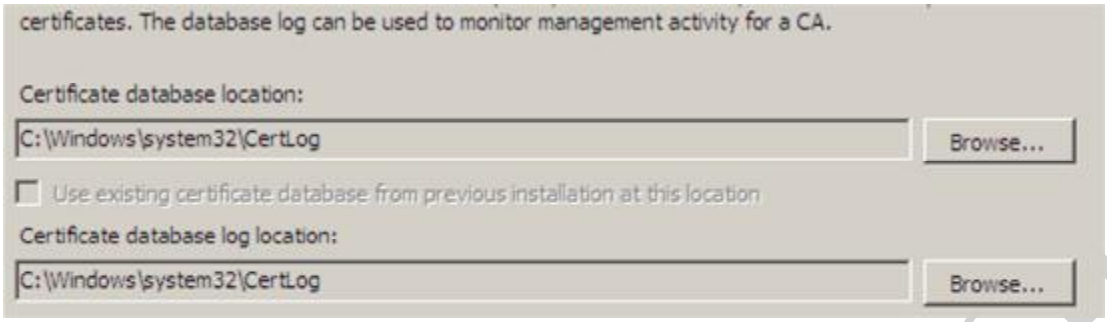

در این مرحله اطلاعاتی از قبیل اسم دامین,کامپیوتر نیم, کار سرور به ما نشان می دهد




در اینجا مدت زمان کارکرد این سرور ( اعتبار Certificate ) ها را سوال می کند

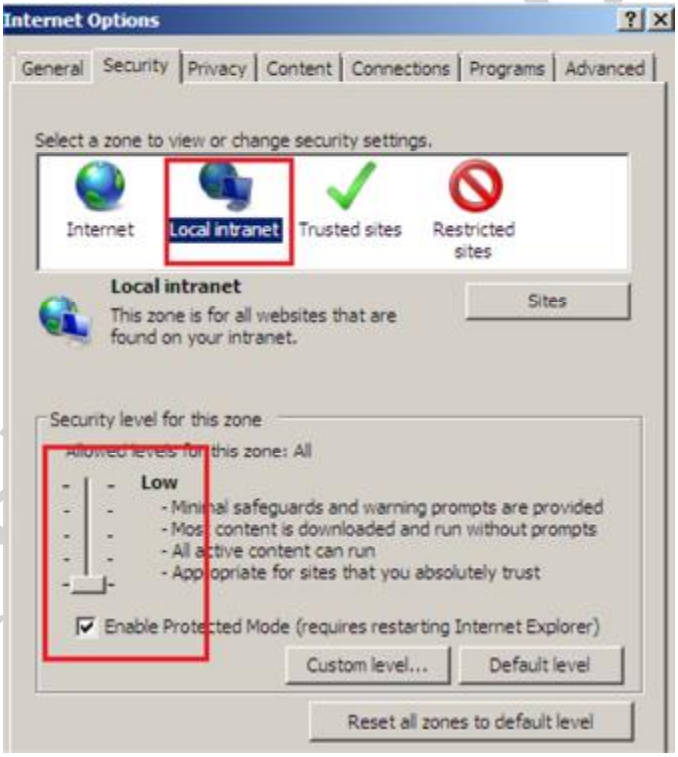


تمامی Certificate ها درمسیر زیر ذخیره می شود



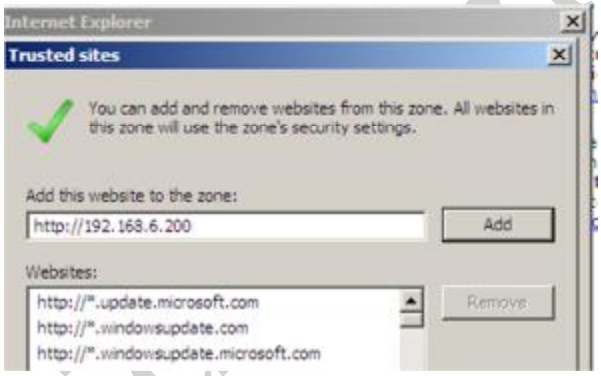

درمرحله آخر به دلیل ویژگی Web Enrollment احتیاج به نصب IIS دارد.

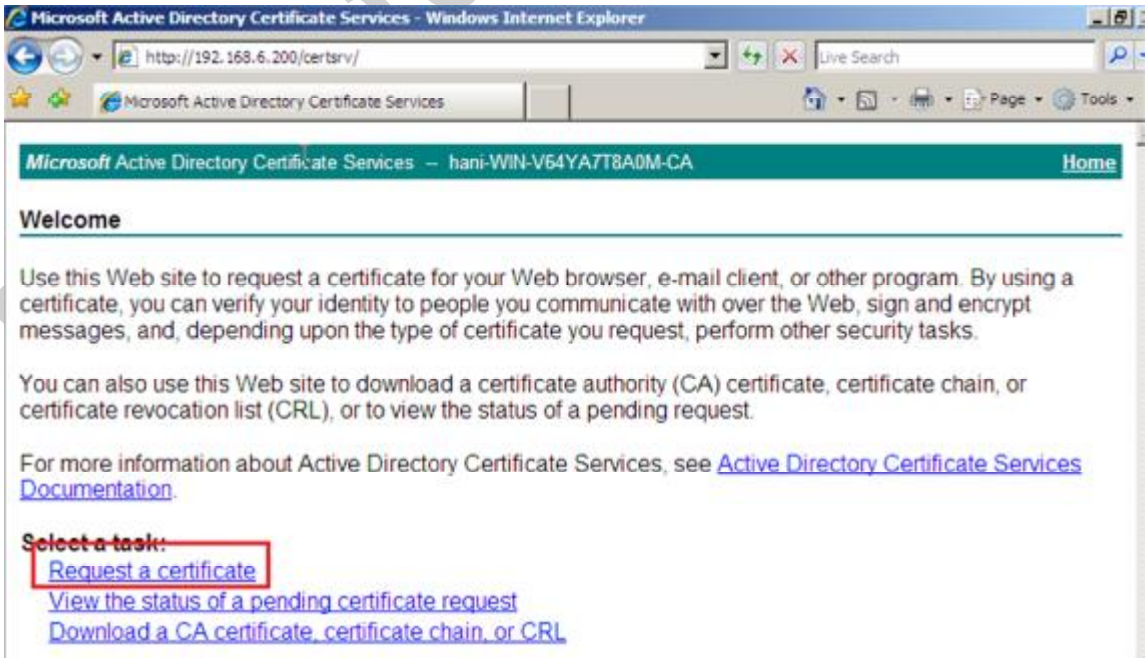
در این مرحله باید برای VPN باید یک Certificate بگیریم که تبدیل به SSL VPN (SSTP )شود, برای این کار مانند زیر عمل می کنیم



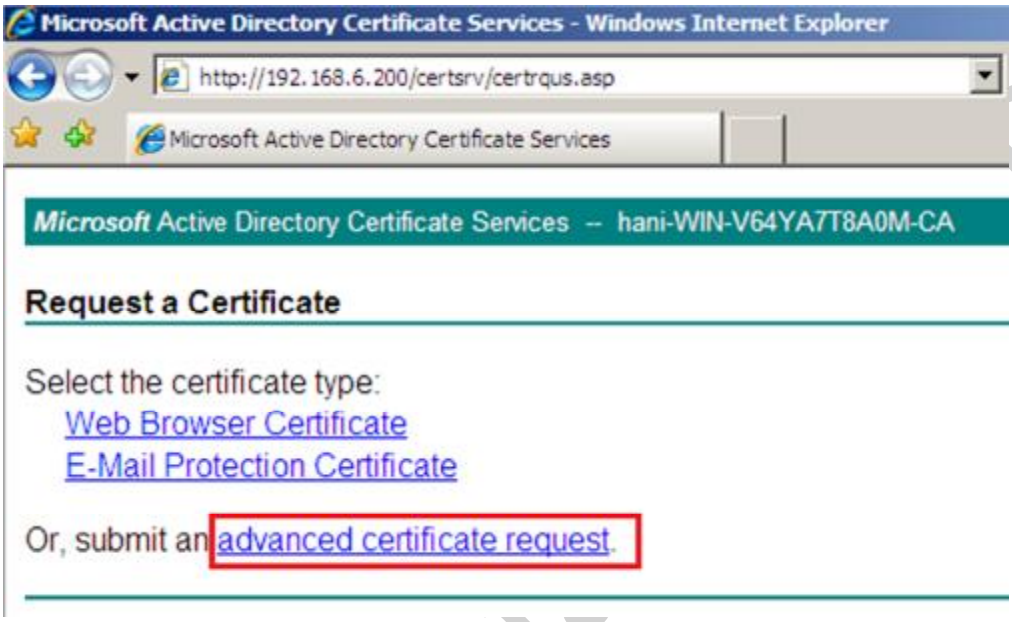

- این کار را برای این انجام می دهیم که پنجره های Pop up باز نشوند.
- تنظیم ساعت و تاریخ فراموش نشود.

http:\ \192.168.6.200/certsrv

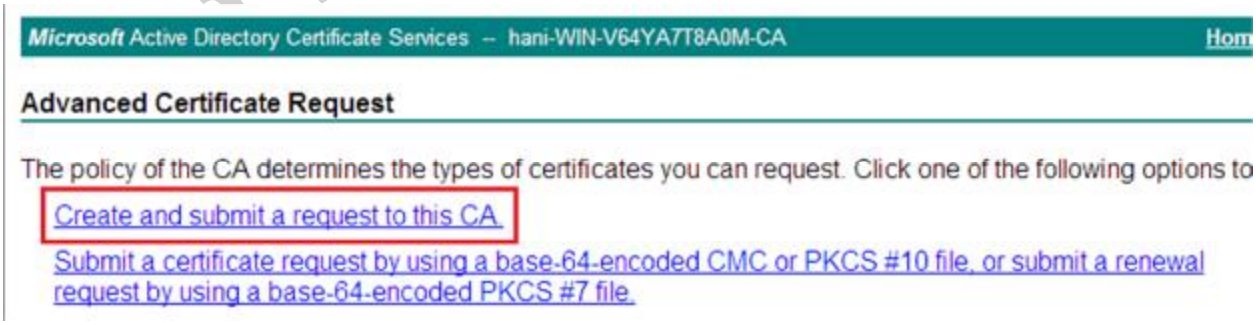


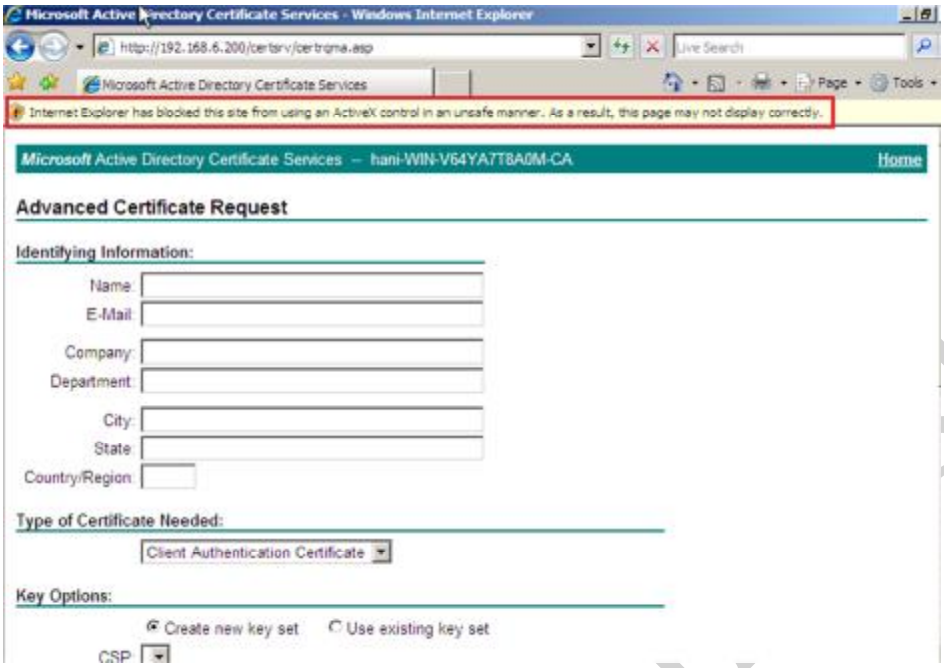
در این مرحله از ما می پرسد چه نوع Certificate می خواهید؟ 1 برای وب سایت 2 برای ایمیل 3 برای دیگر موارد ,در اینجا ما برای VPN می خواهیم پس گزینه3



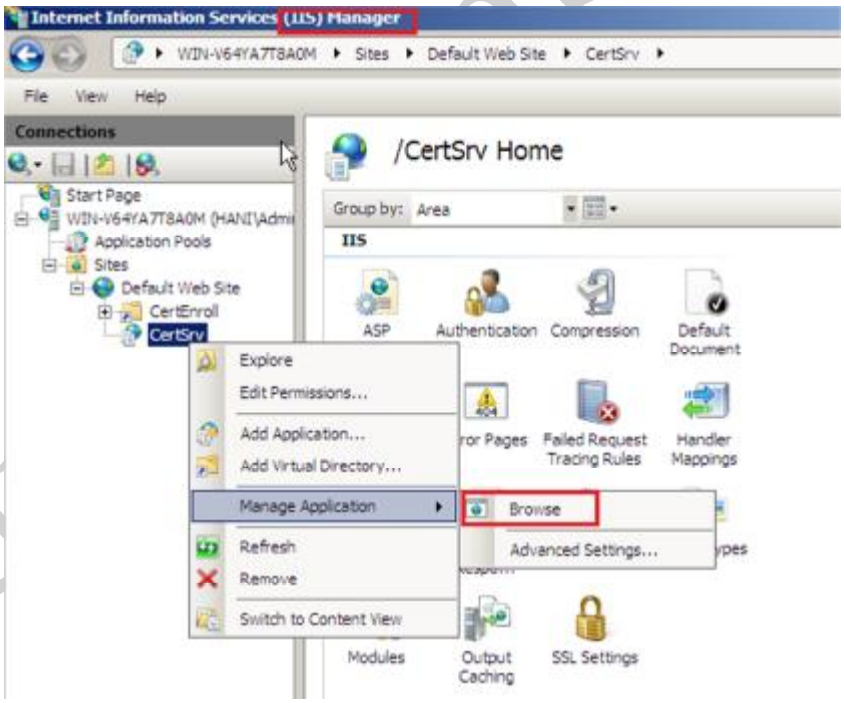

در اینجا می پرسد Certificate را از چه نوع می خواهی 1- معمولی 2- در حالت بیس64 ,این روش یکی از روشهای برنامه نویسی Visual Basic می باشد کار این روش این است که می تواند یک نرم افزار را برای اینکه از دید آنتی ویروس مخفی بماند را کد کند و پس از عبور از آنتی ویروس دوباره به حالت اول برگرداند



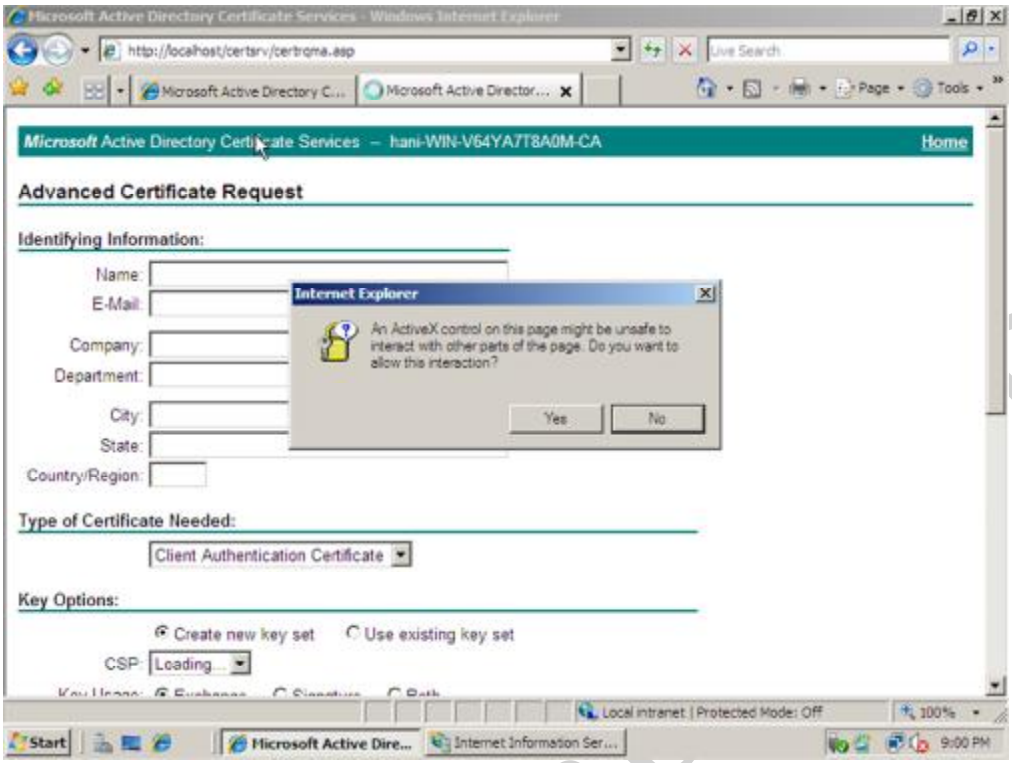

سپس در صفحه بعد با مشکل زیر مواجه می شویم

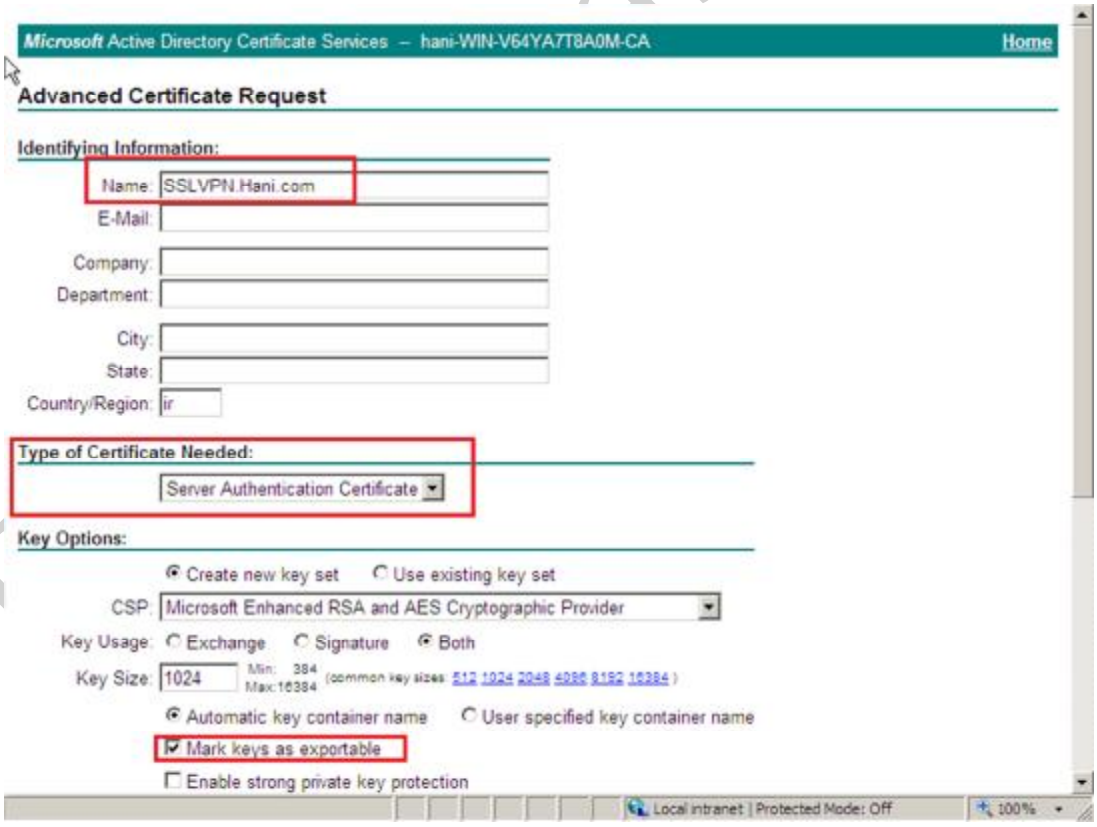



**برای حل آن مانند زیر عمل می کنیم**




**سپس با پنجره زیر مواجه می شویم که باید Yes را بزنیم.**

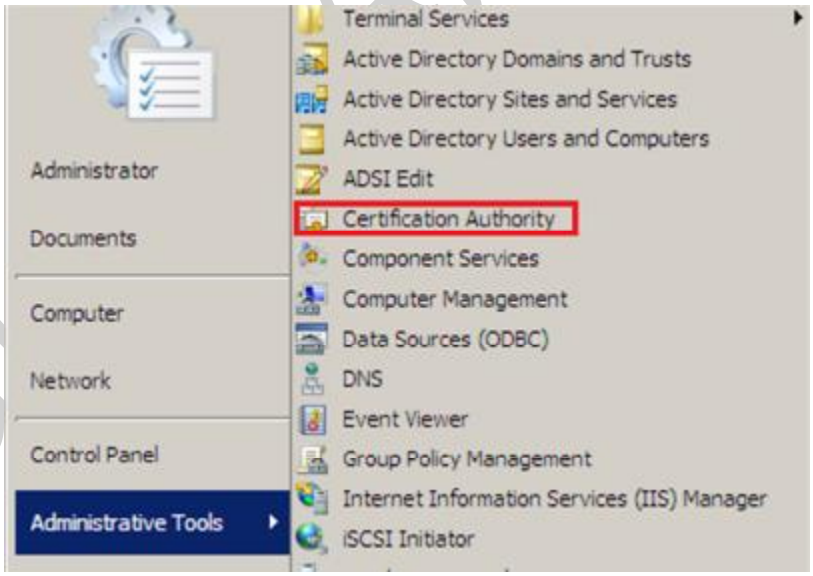


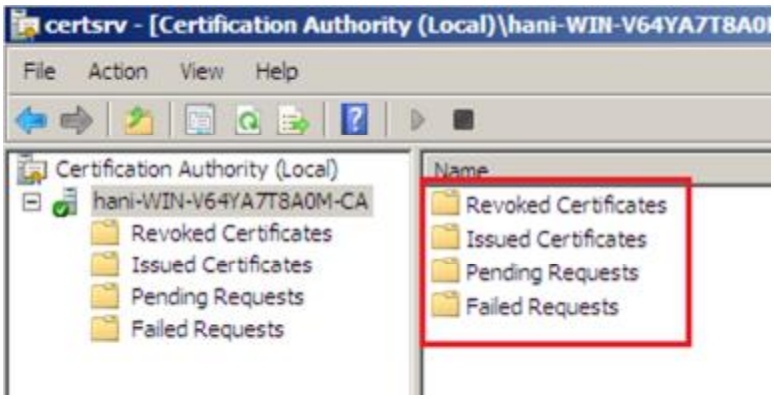

در قسمت Name اسمی را که وارد می کنیم کلاینت ها با این اسم به ما وصل می شوند یعنی داخل VPN Connection بجای Ip این اسم را وارد می کنند درقسمت 2 نوع Certificate را مشخص می کنیم در قسمت 3 با

انتخاب گزینه.. Mark می توانیم Certificate تولید شده را جابجا کنیم (داخل فلش و....) بعد از این مرحله با صفحه زیر مواجه می شویم که می گوید این Certificate معلق می باشد.

برای اینکه Certificate را تایید کنیم مانند زیر عمل می کنیم

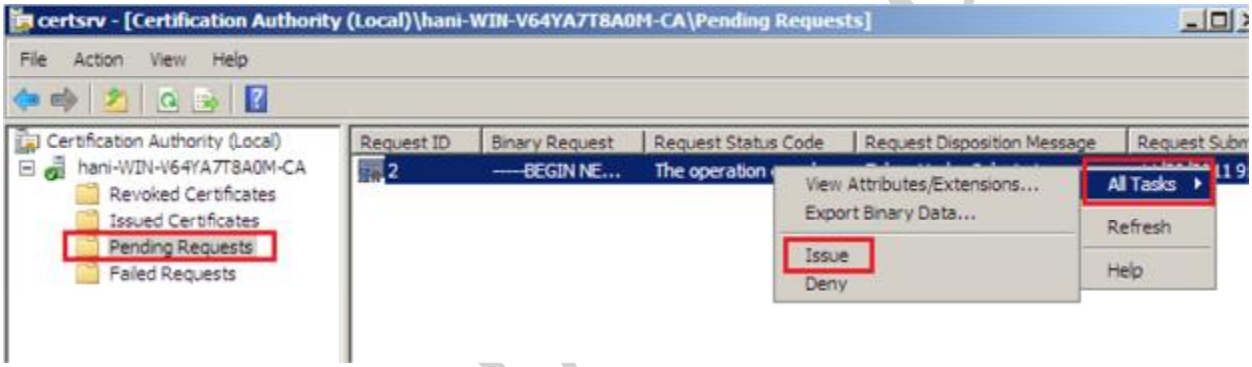



در کنسول باز شده با گزینه های زیر برخورد می کنیم

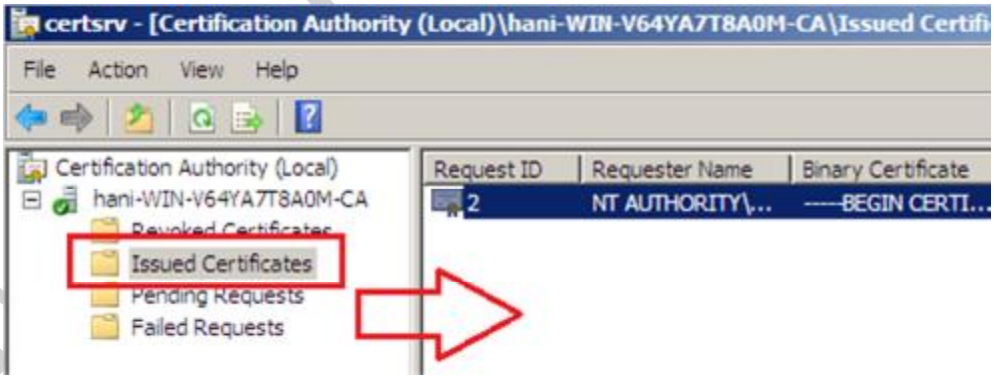



**به ترتیب : گواهینامه های باطل شده,قابل استفاده,معلق,تایید نشده را داریم.**

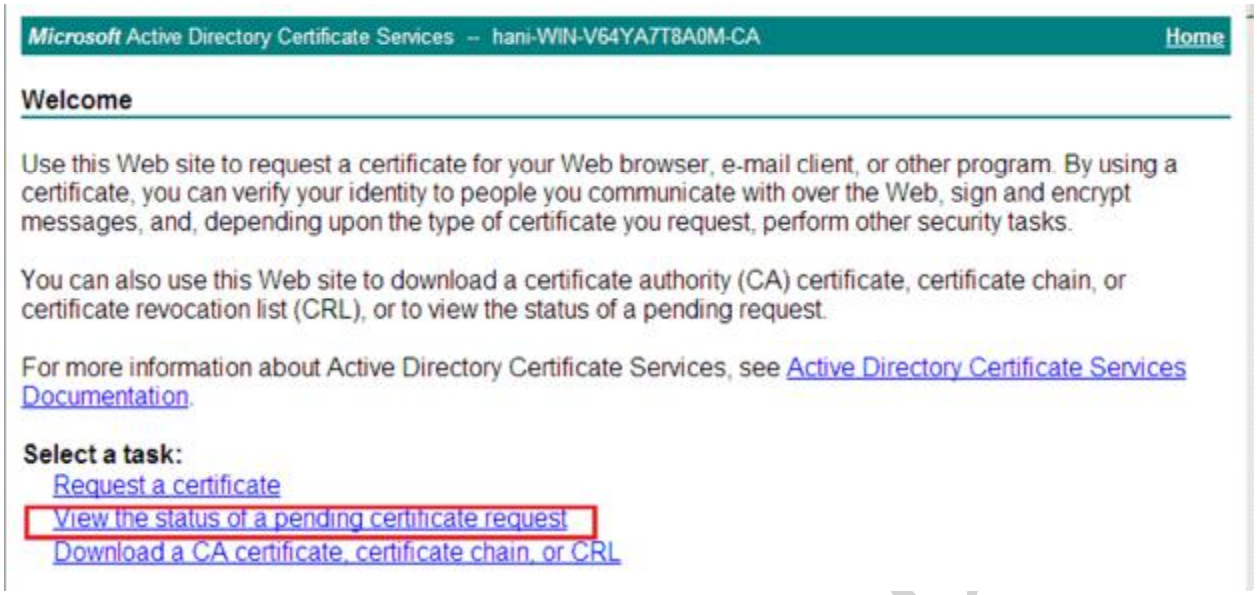
**برای اینکه Certificate را از حالت Pending دربیاوریم مانند زیر عمل می کنیم**

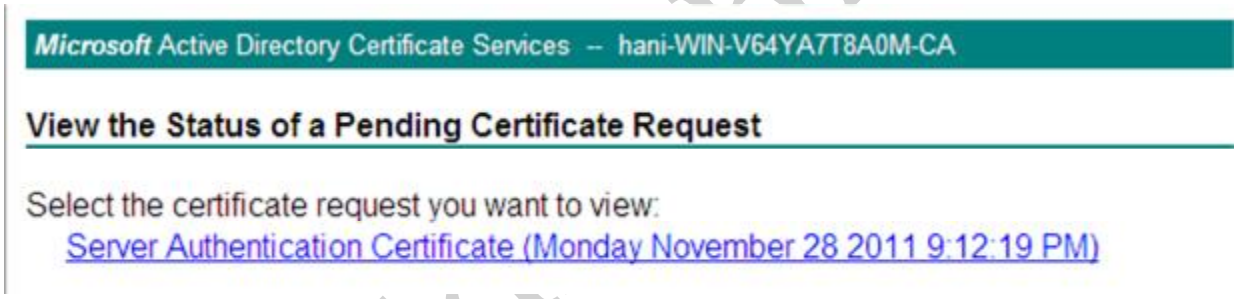


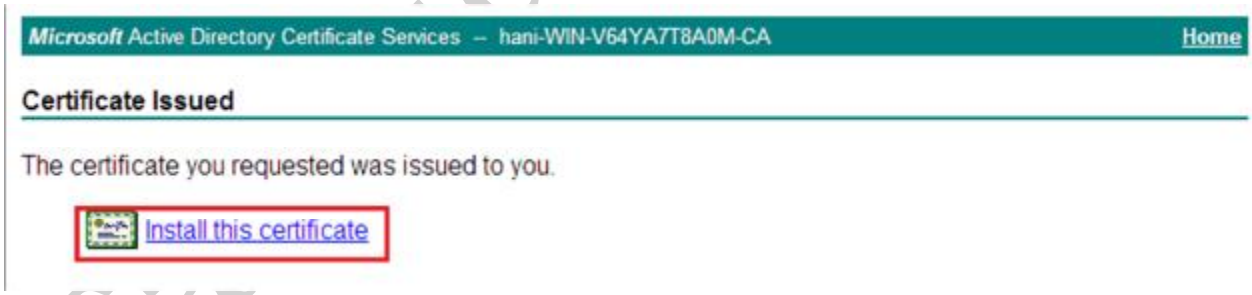

**حا لا قابل استفاده شد**




**برای اینکه بفهیم Certificate که Pending بود در چه وضعیتی قرار دارد**



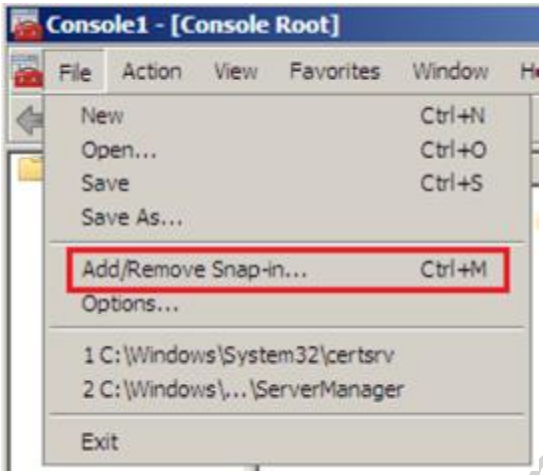



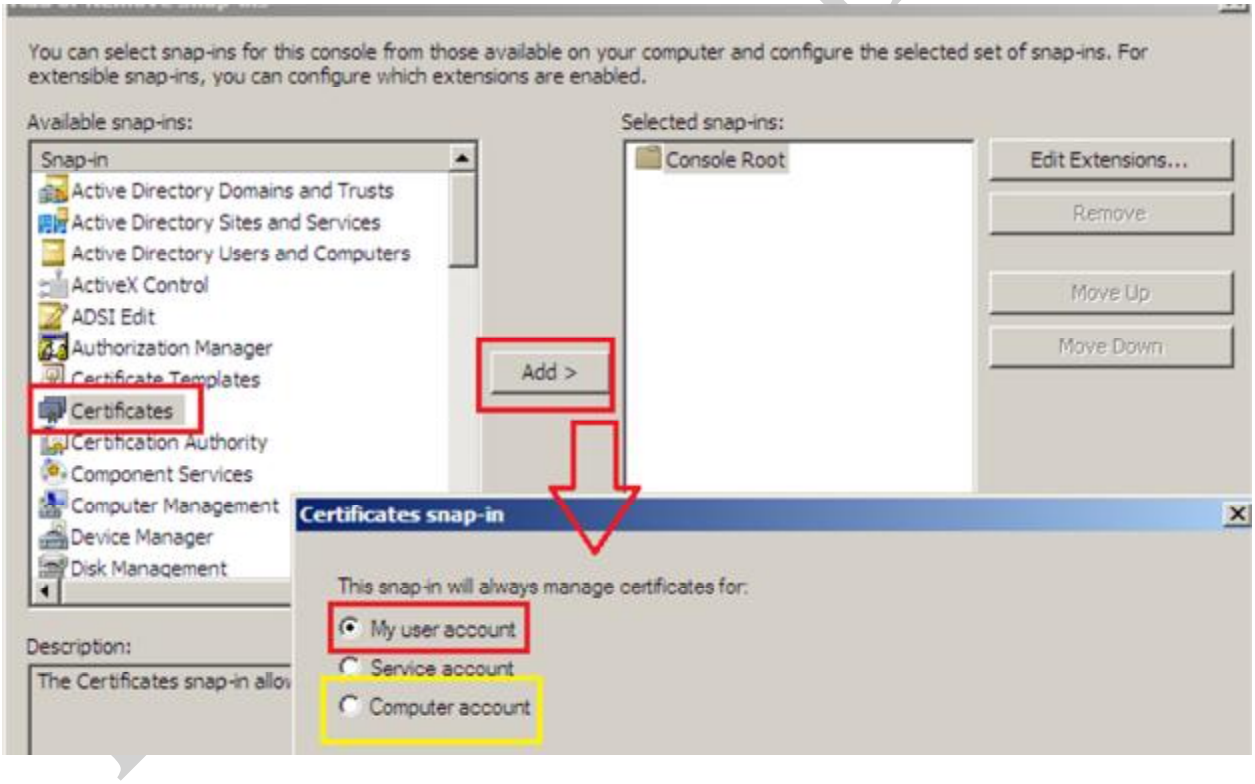

تا اینجا Certificate بصورت کامل نصب شده است.

- این Certificate نصب شده برای Current User می باشد یعنی با User که الان لاگین هستیم کار می کند
- در VPN (Tunneling ) کامپیوتر به کامپیوتر به هم وصل می شوند برای اینکه Certificate نصب شده در بالا از User به کامپیوتر انتقال پیدا کند مانند زیر عمل می کنیم.

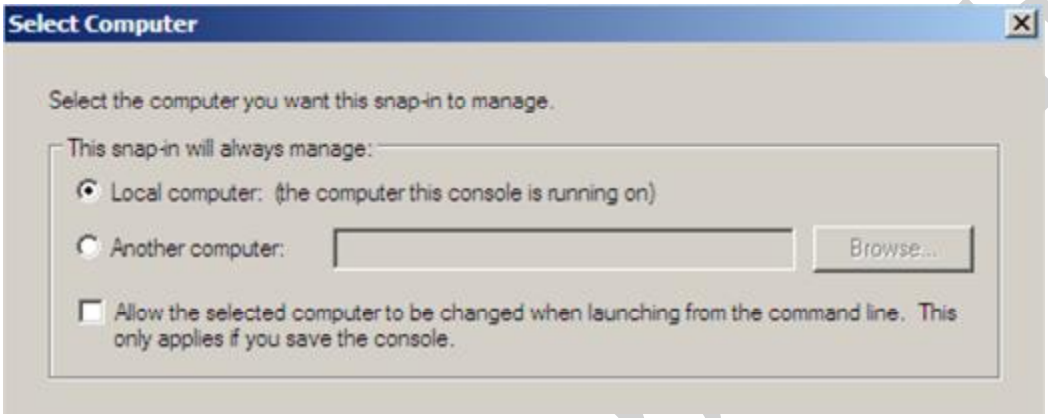
ابتدا وارد کنسول مایکروسافت می شویم



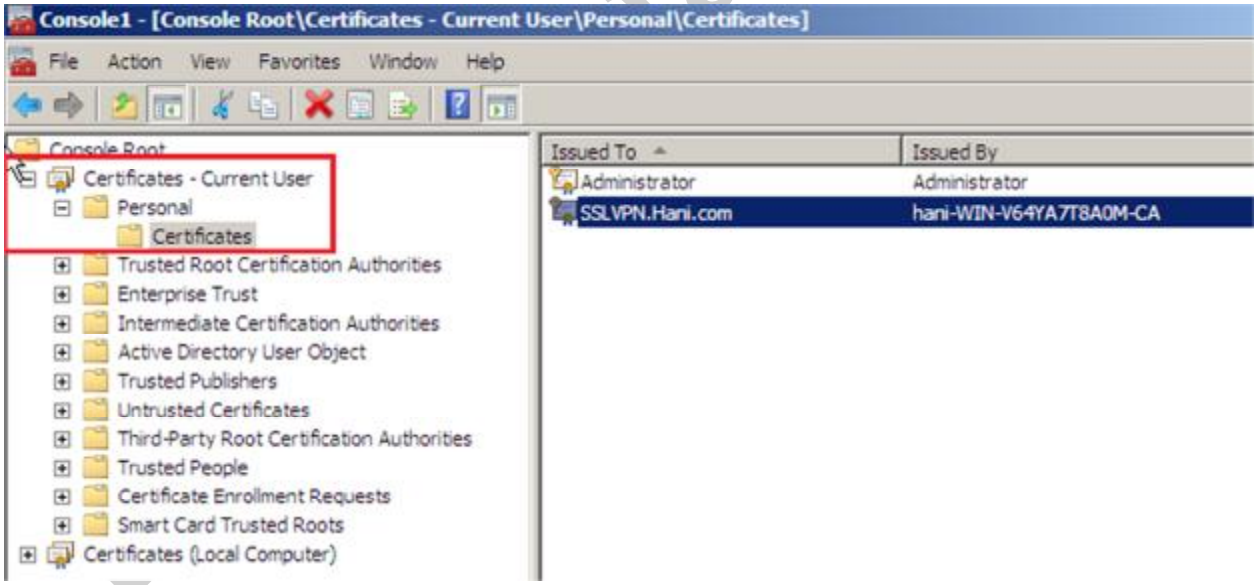

**در این مرحله دوبار باید کنسول را مانند زیر اضافه کنیم**



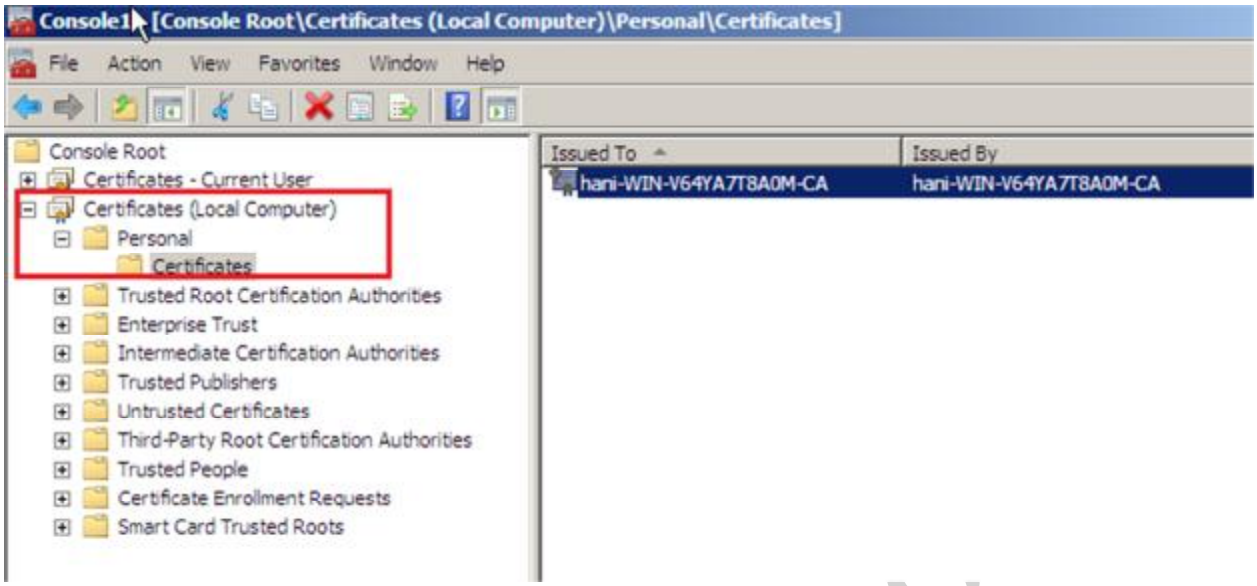

noush



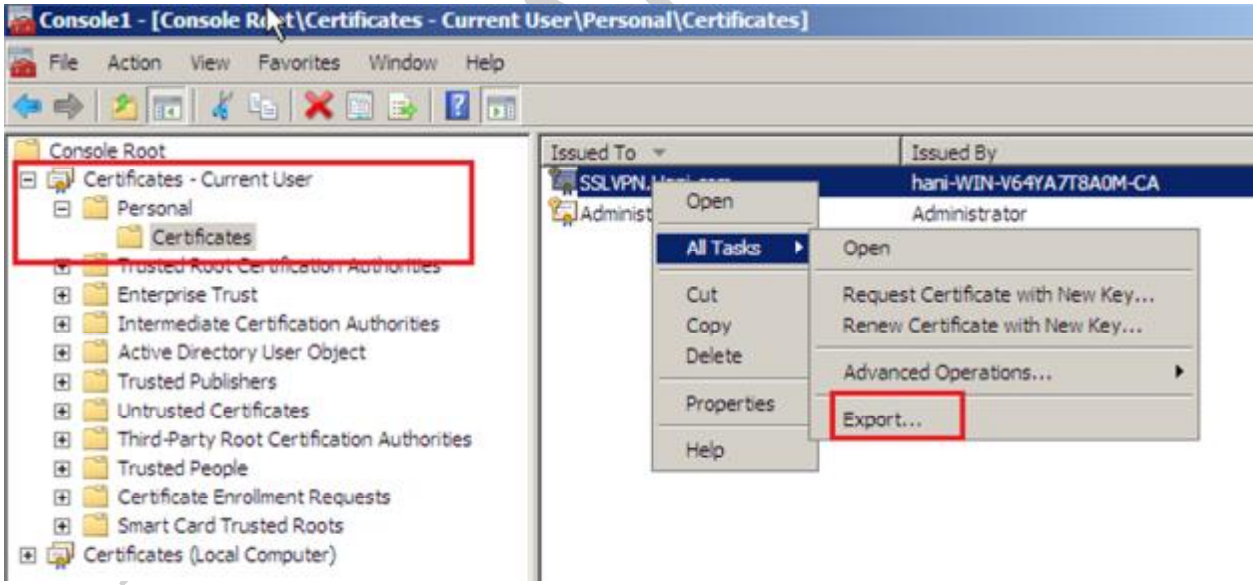

**بعد از اضافه شدن کنسول باید از مسیر زیر Certificate را بر داریم و در مسیر دیگری کپی کنیم**




**برای جلوگیری از مشکلات که ممکن است در آینده پیش بیاید بهتر است هر چیزی که در مسیر زیر قرار دارد را پاک کنیم سپس Certificate را در آنجا کپی کنیم**



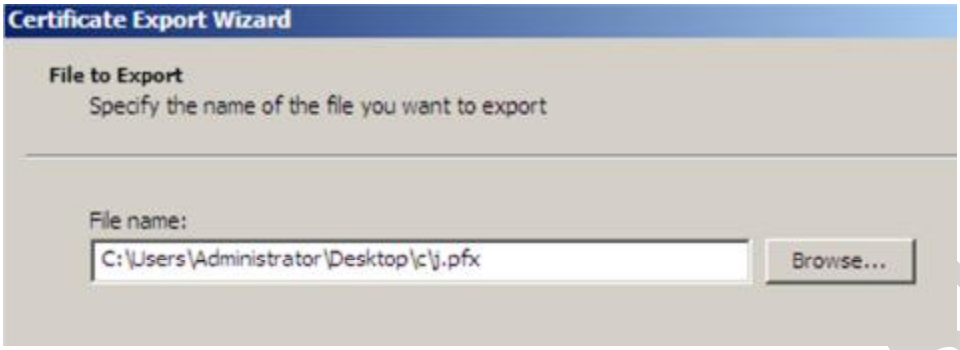

حالا نوبت به Export کردن Certificat می باشد



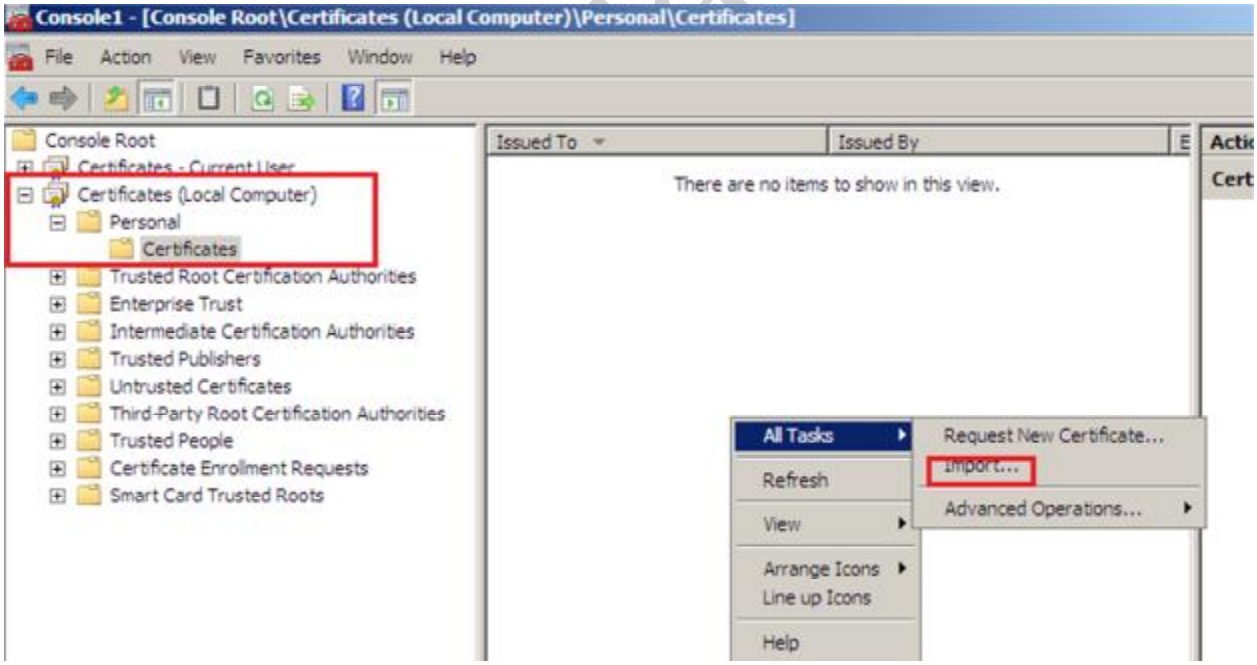
در این مرحله از ما می پرسد آیا می خواهی Private Key را هم Export کنی؟

در این مرحله یک پسورد تنظیم می کنیم که کسی نتواند بدون داشتن رمز از آن استفاده کند.

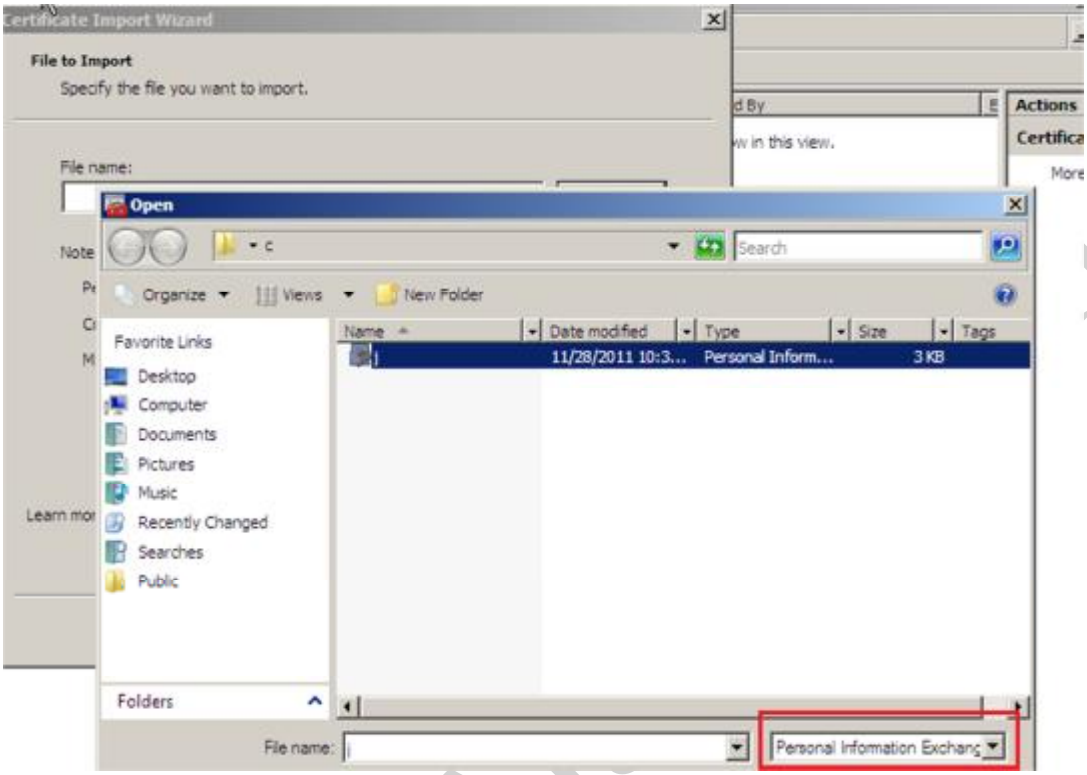
در اینجا محل ذخیره Export را از ما می پرسد و در نهایت Finish




برای Import کردن مانند زیر عمل می کنیم



در این مرحله نوع پسوند باید مانند زیر باشد

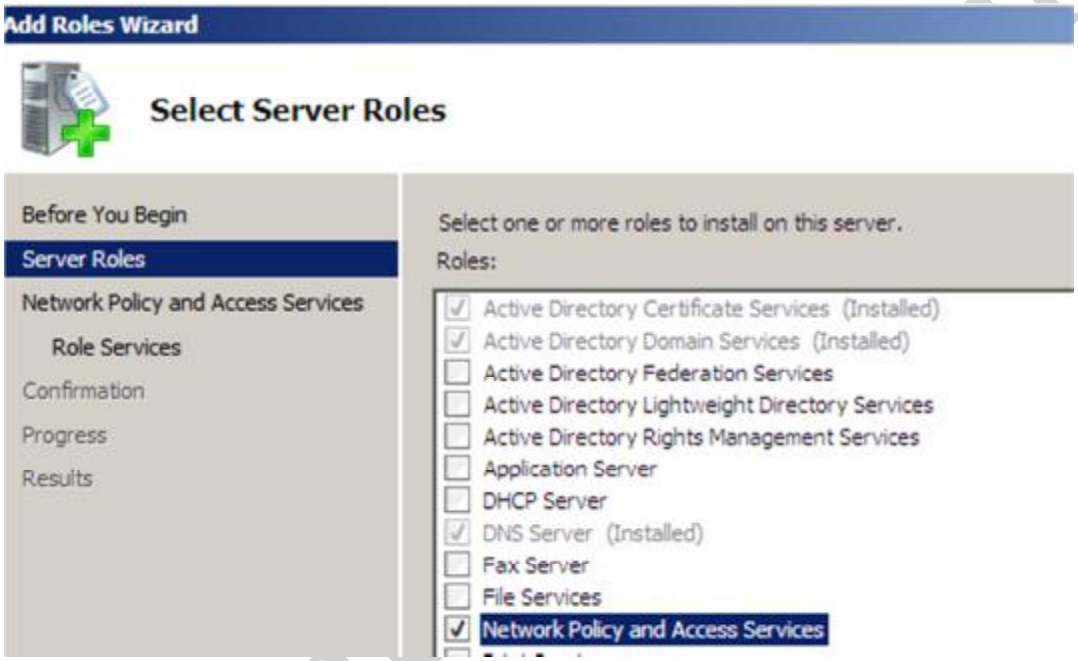


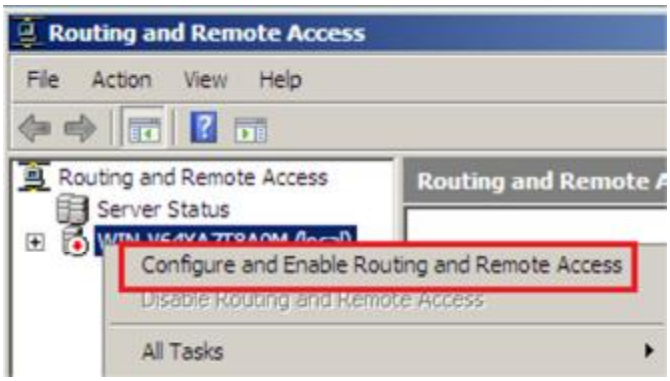

در اینجا باید پسورد تنظیم شده را وارد کنیم و در نهایت Finish

در مرحله بعد باید RRAS را در حالت VPN اجرا کنیم,برای این کار مانند زیر عمل می کنیم

- حتما RRAS باید بعد از Import کردن نصب شود اگر قبل از Import این عمل انجام شود SSL VPN کار نخواهد کرد.

برای نصب RRAS مانند زیر عمل می کنیم



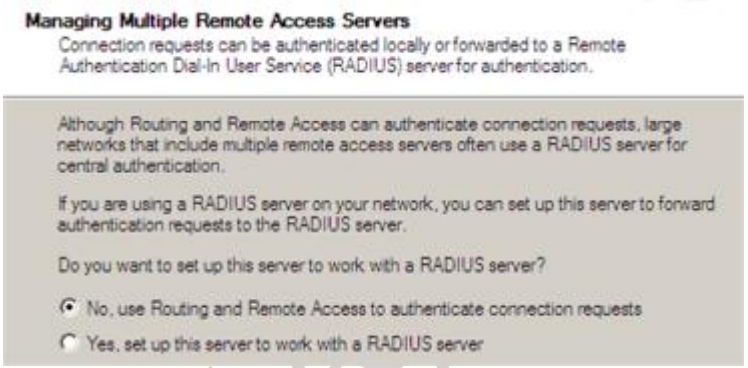


**در این مرحله باید کارت شبکه خروجی را مشخص کنیم , گزینه پایین نباید فعال باشد**

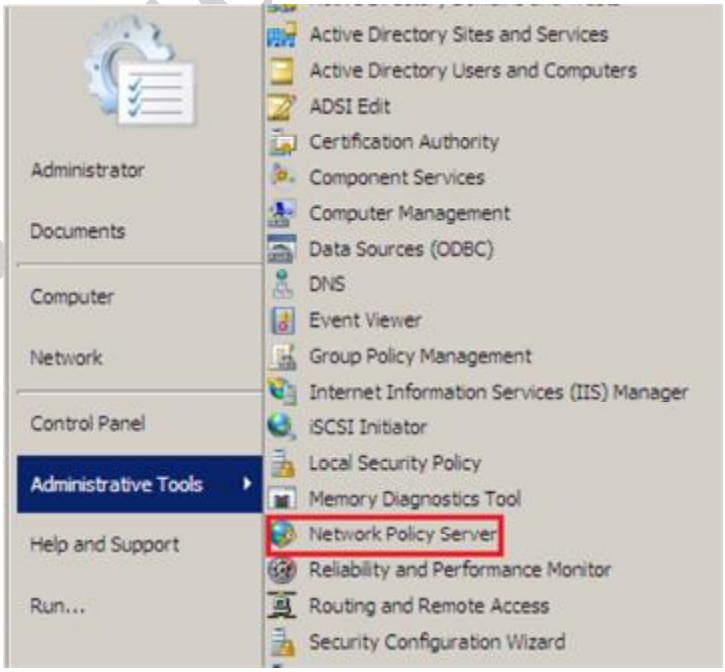
Far-hang-Bash

خود RRAS را Mini DHCP می کنیم

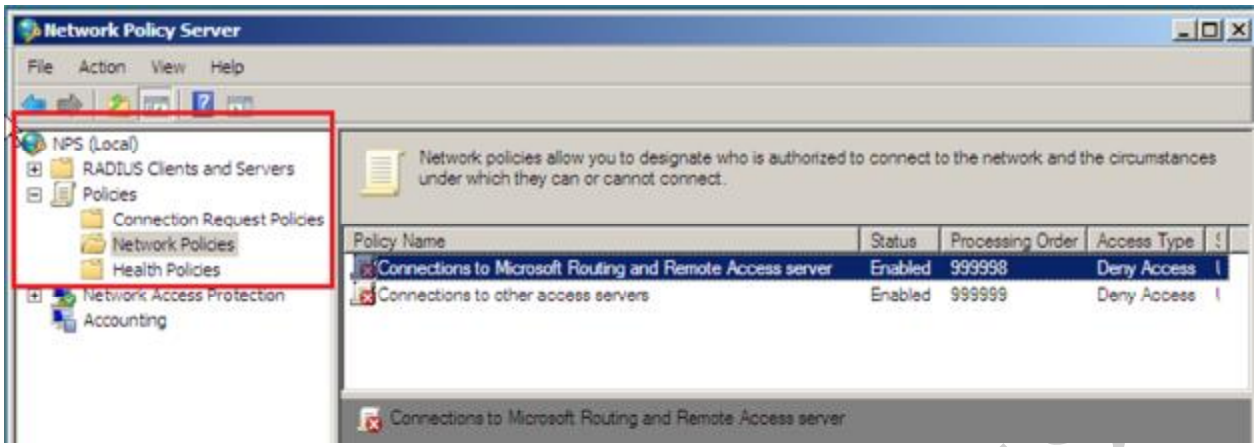
سرور RADIUS هم در شبکه نداریم



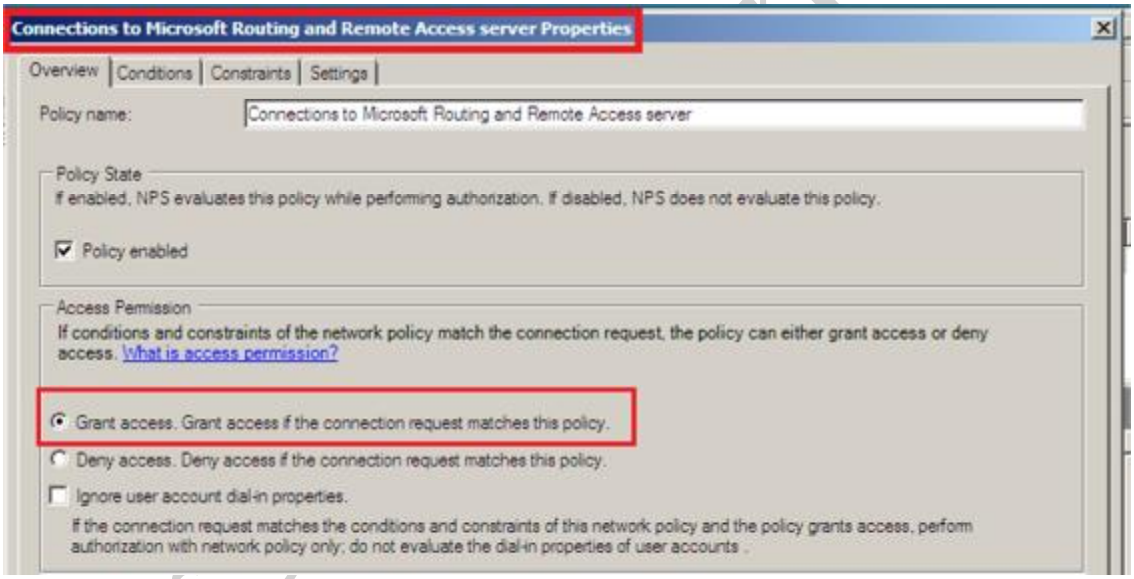

در نهایت برای فعال سازی SSL VPN وارد کنسول زیر می شویم(RADIUS 2008=.....Network Policy )



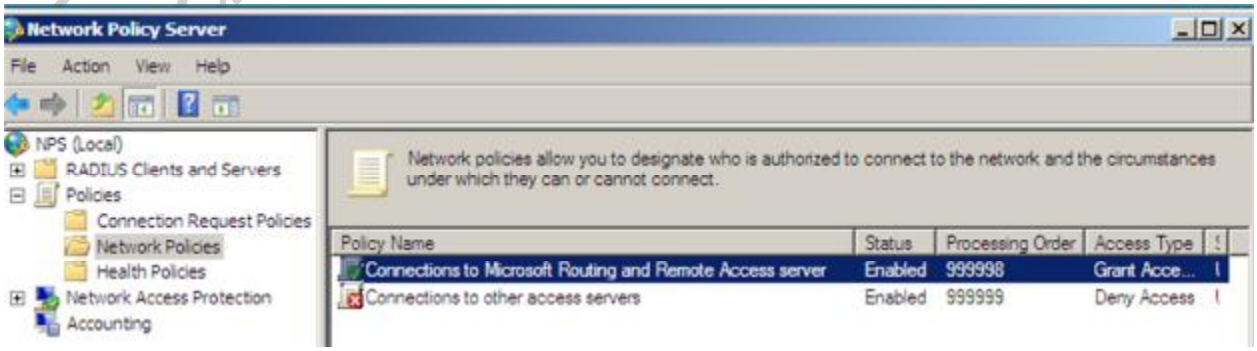

Farideh Roush




از قسمت آبی رنگ Properties می گیریم,درپنجره باز شده گزینه ...Grant را فعال می کنیم



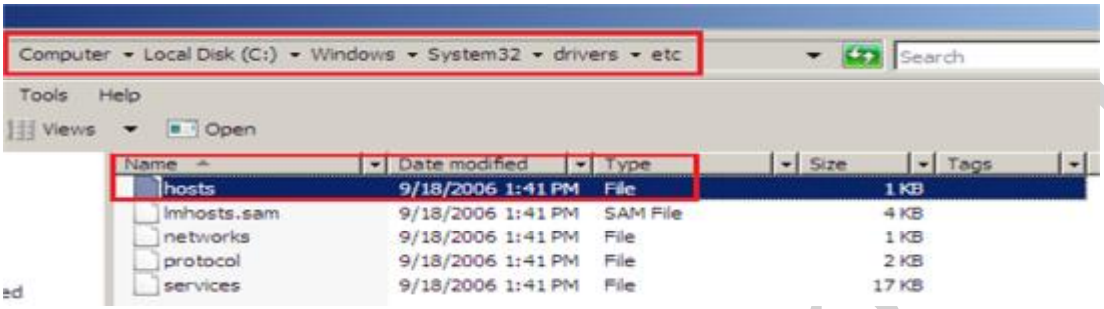

باید گزینه بالا فعال شود تا بتوانند به این سرور VPN بزنند و در نهایت مانند زیر گزینه سبز می شود.



حالا نوبت به استفاده از VPN می باشد برای این کار باید یک کامپیوتر با یکی از سیستم عامل های زیر بالا بیاوریم

Vista Sp1,Xp Sp3,Server2008 ,سپس یک Ip دررنج کارت شبکه خروجی سرور VPN به آن می دهیم (7.200)

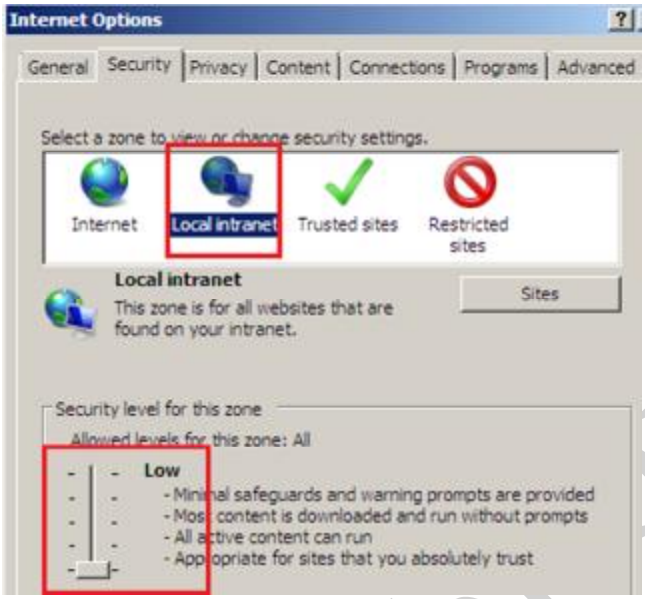
در این سناریو IP کلاینت 7.201 می باشد و وارد فایل HOST کلاینت می شویم.



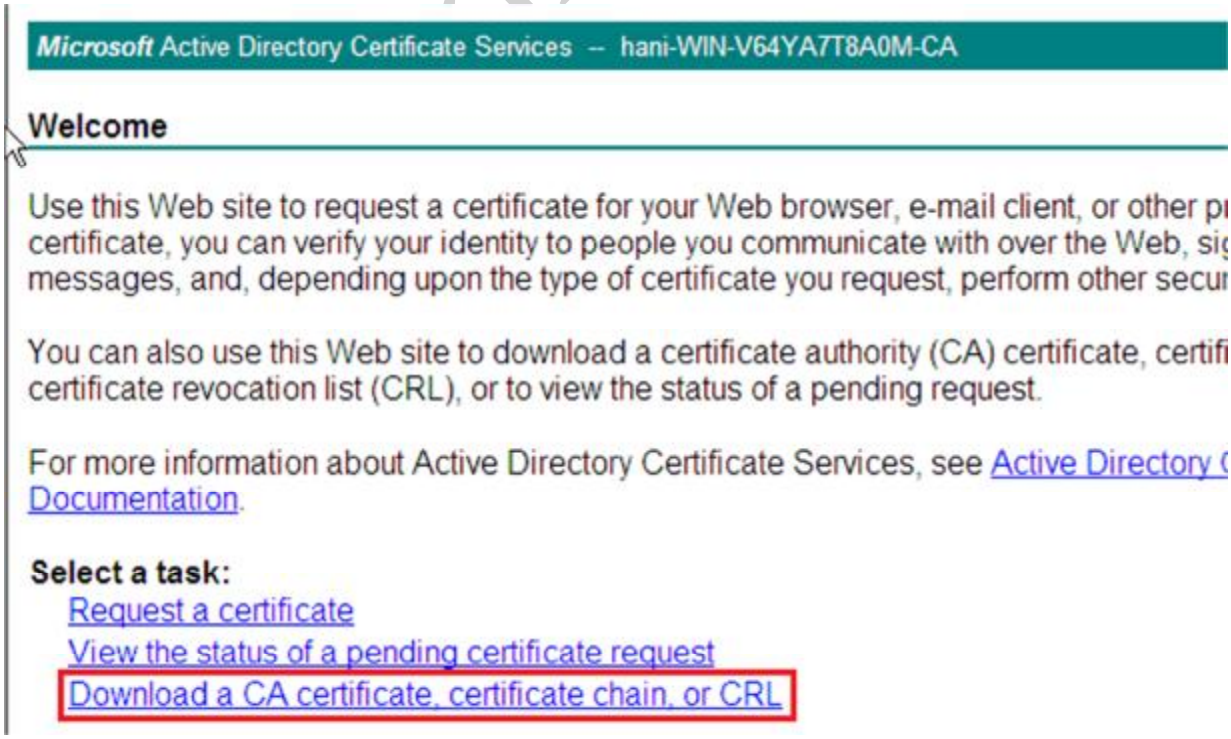

سپس با Notepad آن را باز می کنیم و Ip زیر را در آن وارد می کنیم

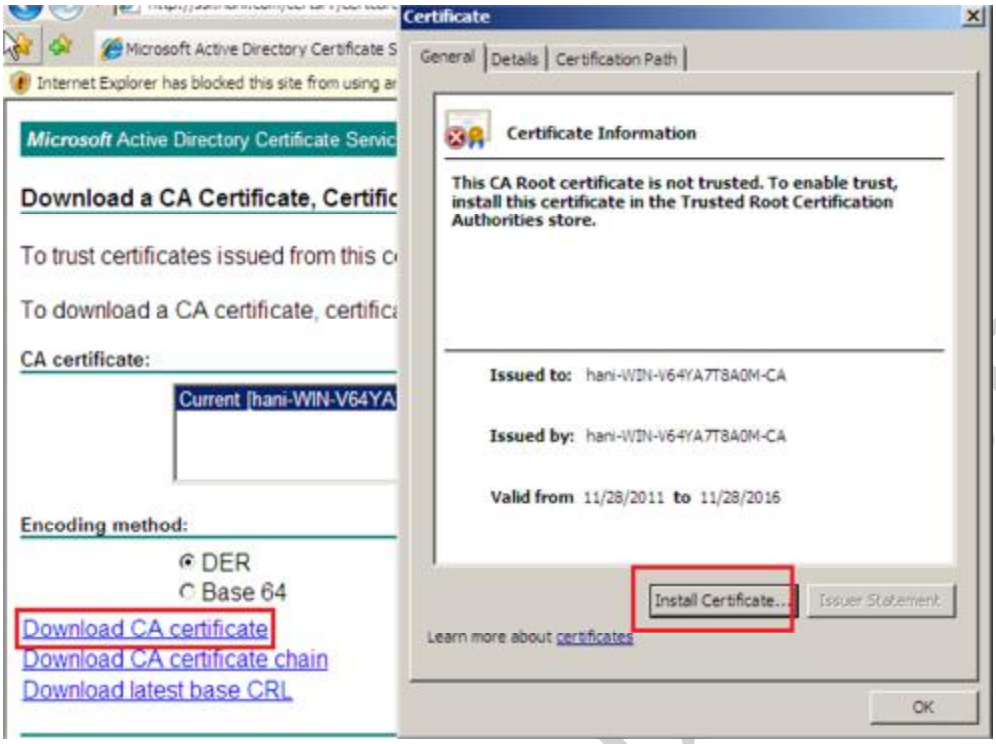
- این فایل دقیقا کار DNS را انجام می دهد به دلیل اینکه به اینترنت متصل نیستیم به صورت دستی Ip سرور را وارد می کنیم.
- کانکشن های آماده VPN دقیقا تمامی این تنظیمات را انجام می دهد.
- تنظیم ساعت و تاریخ فراموش نشود.

سپس IE را باز کرده و مانند زیر عمل می کنیم

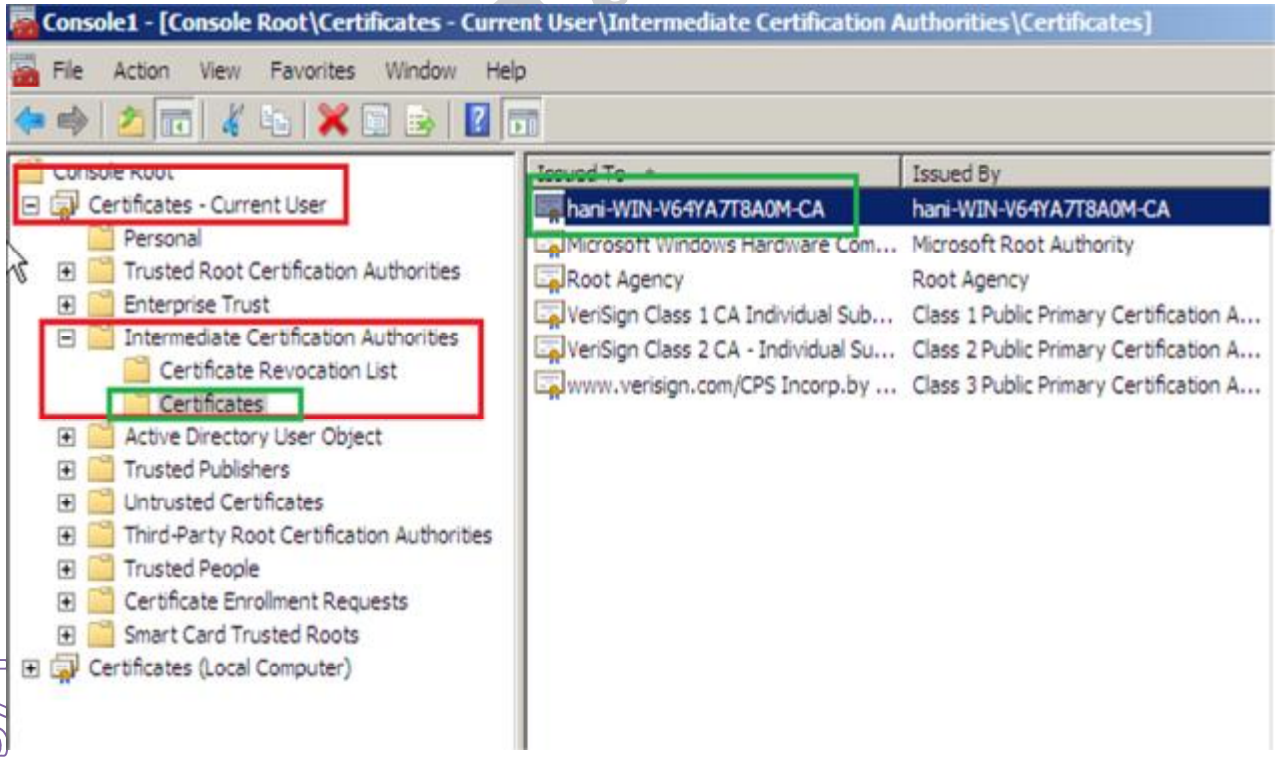


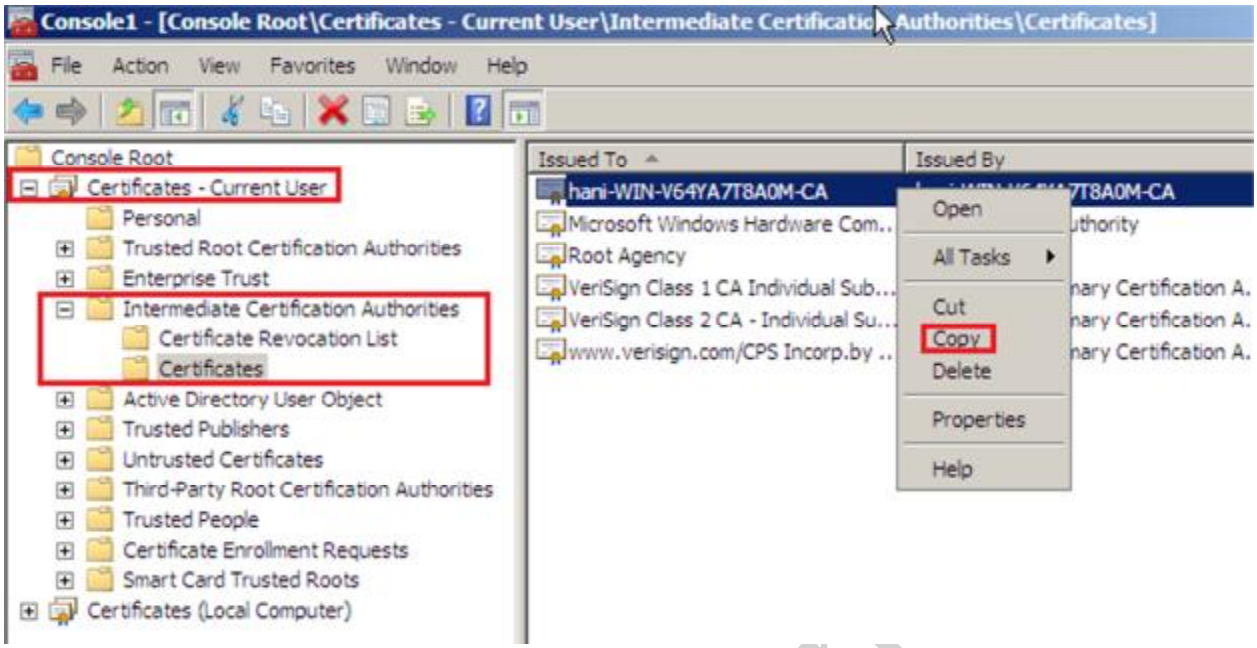
بعد از وارد کردن آدرس بالا باید از ما پسورد بپرسد،به این دلیل که ما در رنج Ip سرور هستیم از ما پسورد نمی خواهد.



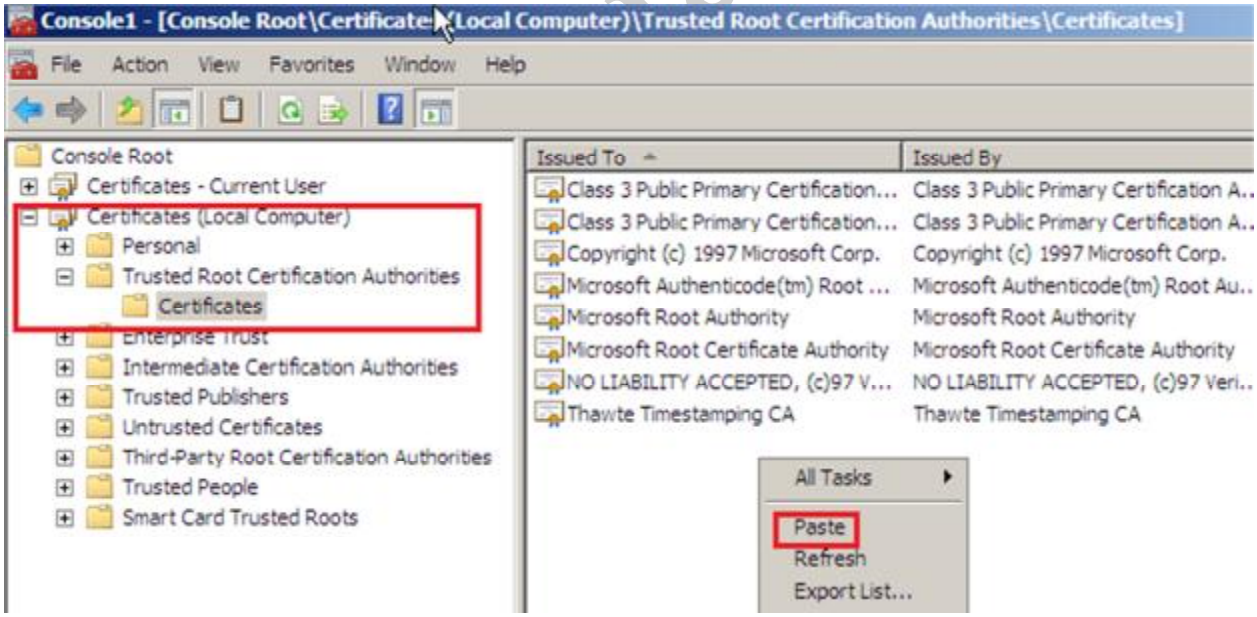



در اینجا Certificate بر روی User فعال شده است برای اینکه Certificate را به کامپیوتر انتقال دهیم ابتدا مانند سرور اصلی وارد کنسول MMC می شویم سپس تمامی کارها مانند مرحله سرور اصلی انجام می شود با این تفاوت که هنگام Export کردن Certificate مانند زیر عمل می کنیم

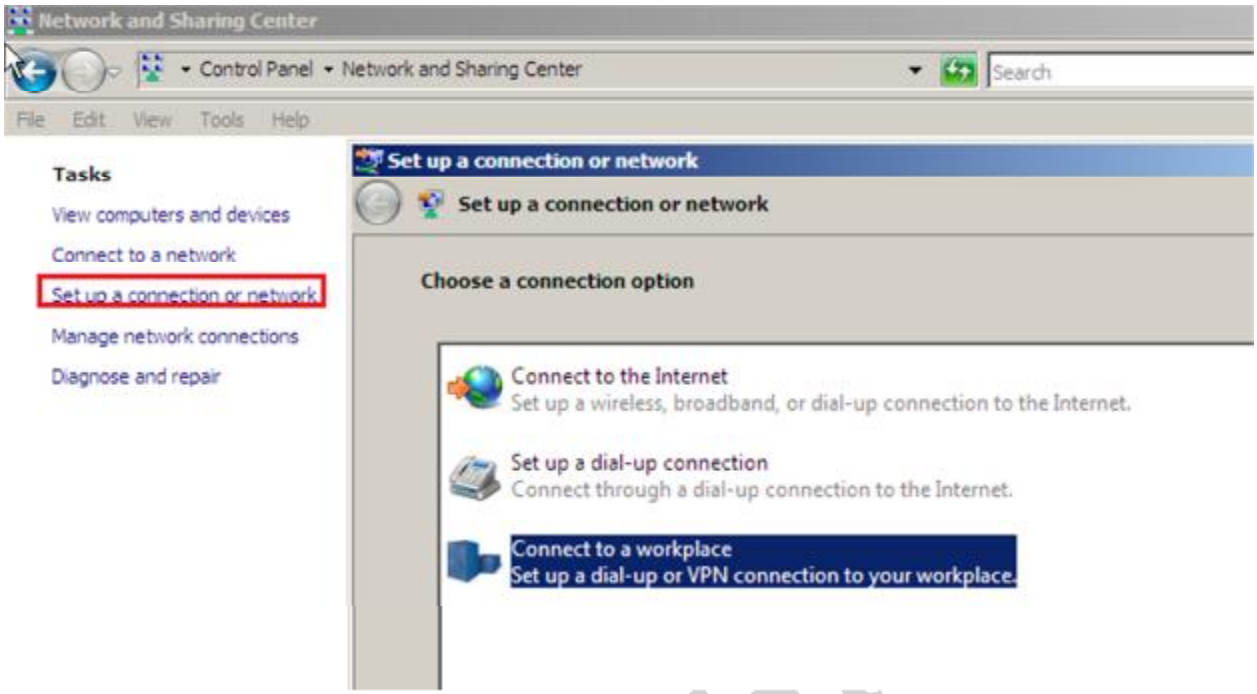


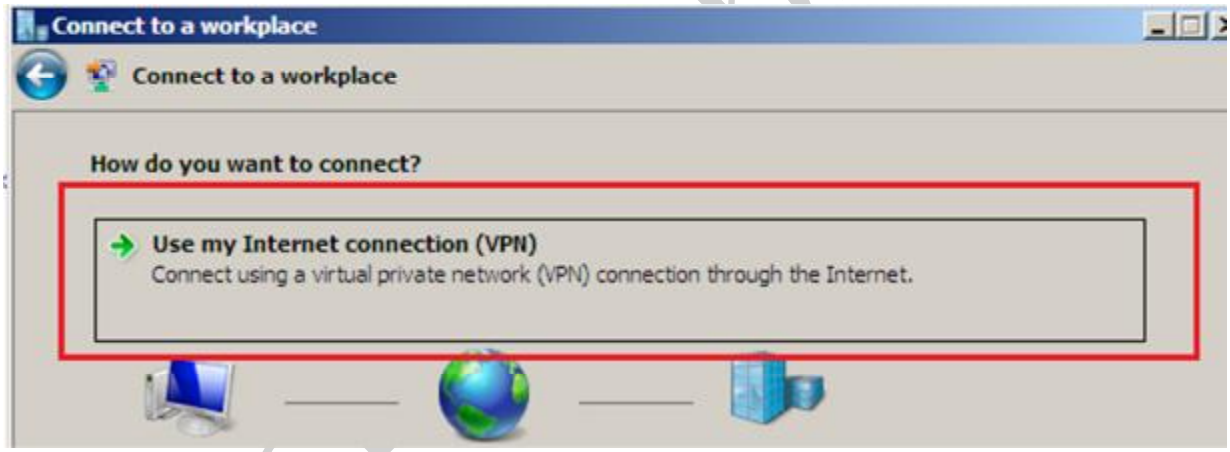


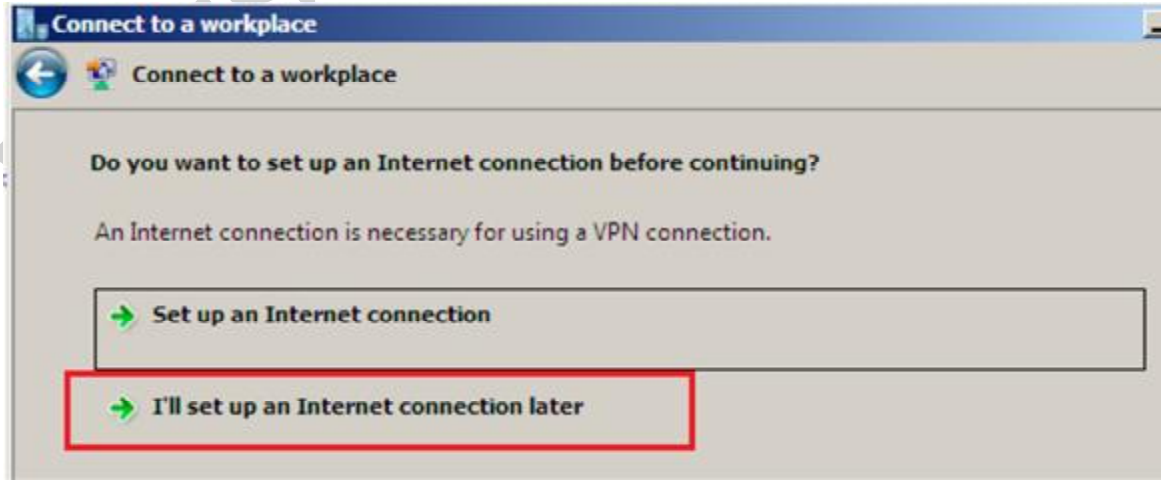

سپس در Local Computer آن را Paste می کنیم



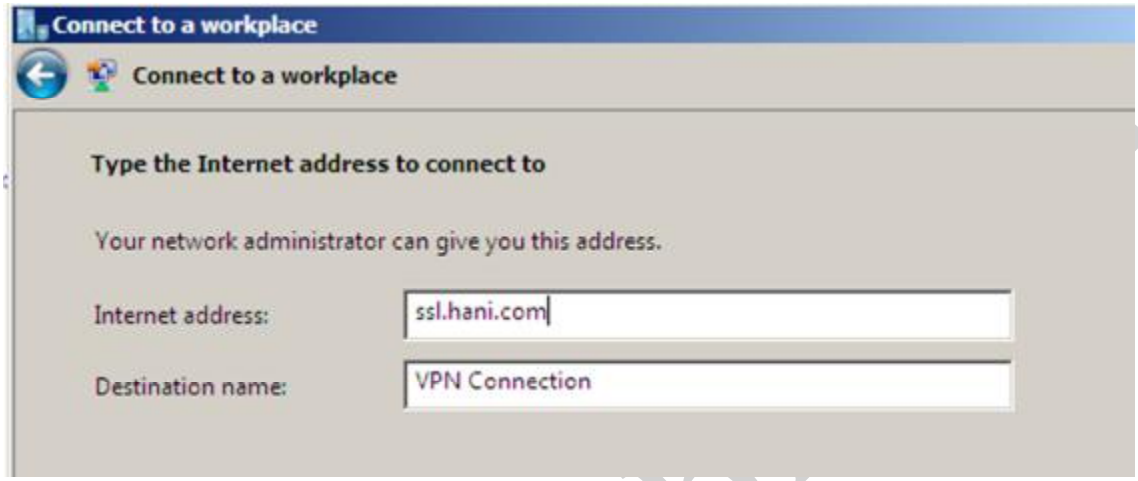

سپس نوبت به ساختن کانکشن VPN می رسد که مانند زیر عمل می کنیم


Network and Sharing Center
Control Panel ▸ Network and Sharing Center
Search
File Edit View Tools Help
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
Set up a connection or network
Set up a connection or network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.
Set up a dial-up connection
Connect through a dial-up connection to the Internet.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.


Connect to a workplace
Connect to a workplace
How do you want to connect?
Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

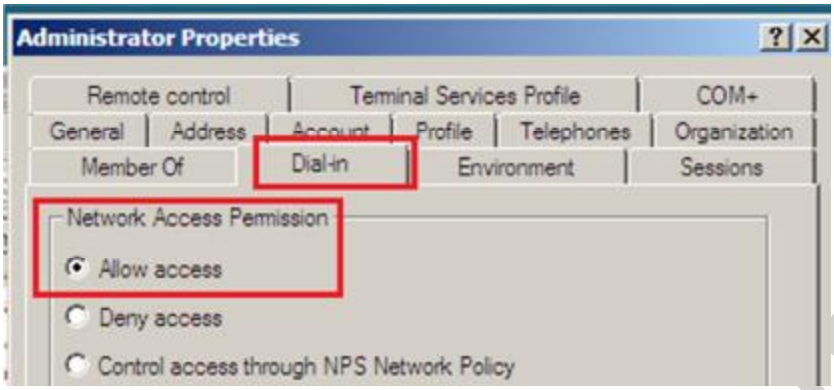

Connect to a workplace
Connect to a workplace
Do you want to set up an Internet connection before continuing?
An Internet connection is necessary for using a VPN connection.
Set up an Internet connection
I'll set up an Internet connection later

در مرحله 3 (عکس بالا)در سناریو واقعی باید گزینه 1 را انتخاب کنیم چون ابتدا باید اینترنت داشته باشیم تا بتوانیم از VPN استفاده کنیم در اینجا چون به شبکه داخلی VPN می زنیم گزینه 2 را انتخاب کرده ایم.

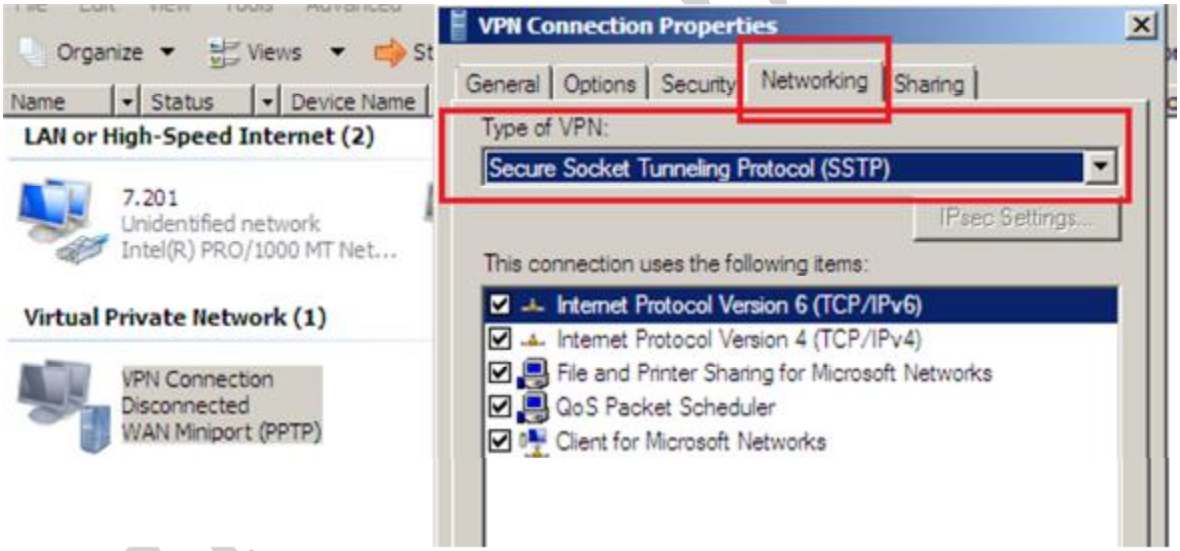



در اینجا باید یوزر و پسورد موجود در سرور را وارد کنیم

برای استفاده از یوزر وارد شده در بالا باید گزینه زیر را بر روی یوزر در سرور اصلی فعال کنیم




سپس به کلاینت بر می گردیم,حالا نوبت به تست می رسد قبل از تست باید کانکشن را بر روی SSTP مانند زیر تنظیم کنیم.

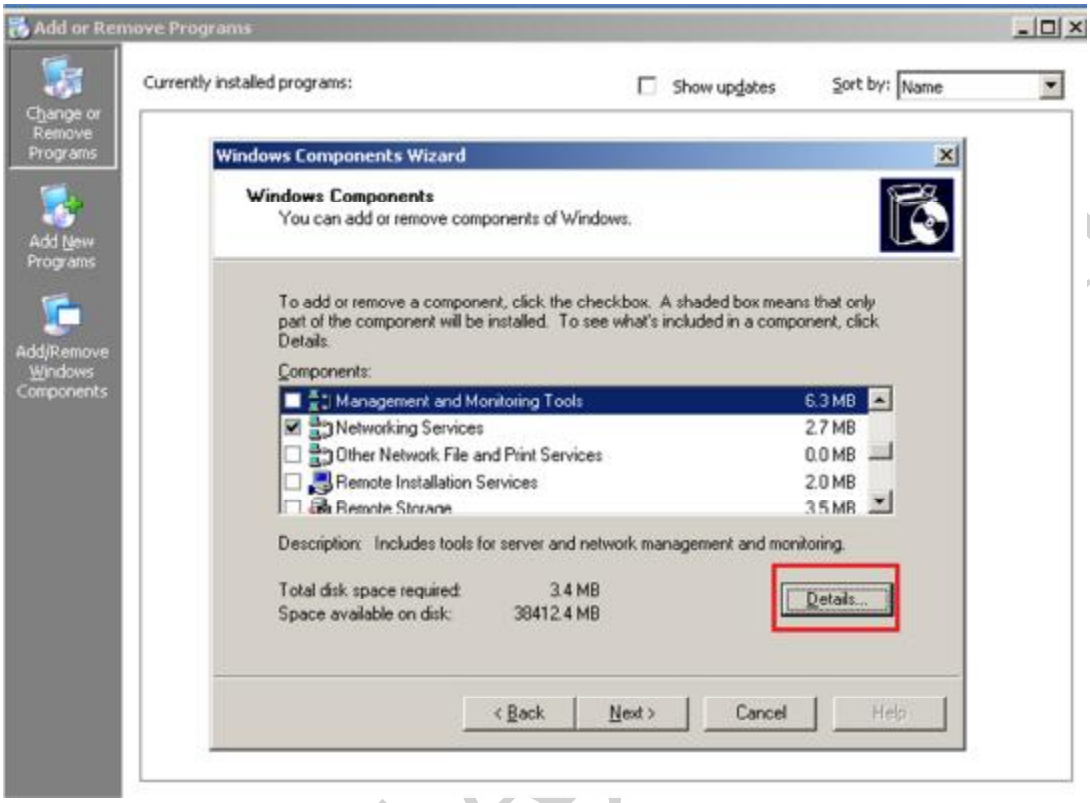


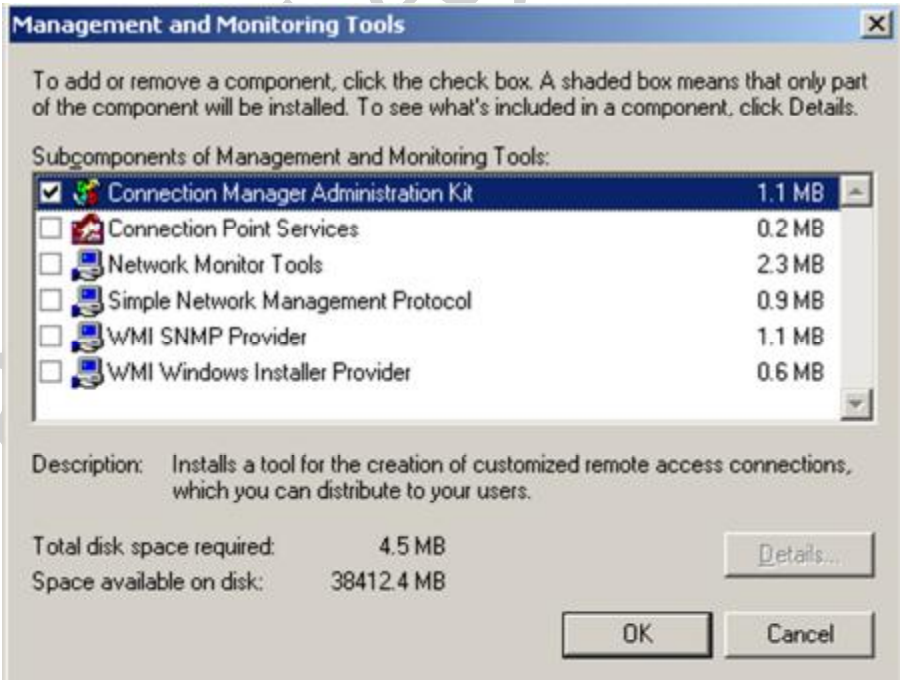

- Open VPN بهترین نرم افزار برای انواع VPN ها است.

Fa bnoush

نحوه ساختن کانکشن آماده VPN

برای این کار در2008 باید کنسول آن را دانلود کنیم ولی در 2003 موجود می باشد




و در نهایت نصب می شود برای استفاده وارد کنسول می شویم و توسط Wizard باز شده کانکشن را می سازیم.

- کلاینتی که می خواهد به سرور ما SSTP VPN وصل شود باید یکی از سیستم عامل های زیر را داشته باشد: Vista SP2 or up ,Xp SP3 ,7 ,1اگر Open VPN داشته باشیم(بر روی سرور) می توانیم با سیستم عامل های دیگر هم وصل شویم.
- برای وصل شدن به صورت SSTP می توان از کانکشن های آماده استفاده کرد.

پیاده سازی NAT(Network Address Translation ) با RRAS

دلیل استفاده از NAT در شبکه 1 – تبدیل IP Private به Public 2- تنظیمات و پیکربندی شبکه ما را مخفی می کند ( Hide Configuration ) 2 شبکه را در نظر بگیرید شبکه 1 به شبکه2 NAT شده است زمانی که شبکه 1 به هر کجا وصل شود با IP شبکه2 وصل می شود.

- اسم دیگر پروتکل NAT , Mapping می باشد,دو نوع NAT داریم 1- Static=Reservation 2- Dynamic=Pat .

STATIC NAT

به تعداد سیستم هایی که Ip Private دارند در سرور NAT , Ip Public داریم,مشکل این روش این باشد که به تعداد Ip ها احتیاج به Ip Public داریم و اگر یک کلاینت در شبکه نباشد ازIp Public آن نمی توان استفاده کرد ,مزیت آن سرعت بالا می باشد, از این روش زمانی استفاده می کنیم که بخواهیم سروری را بر روی اینترنت ببریم چون باید Ip سرور ما ثابت باشد برای این کار از روشی به نام Publishing استفاده می کنیم,این روش به این صورت عمل می کند که زمانی که اطلاعاتی را از سروری درخواست می کنیم با وارد کردن Ip آن به پشت سرور منتقل می شویم و درخواست ما از سرور عبور کرده و صفحه مورد نظرمان را برایمان می آورد ( ما پشت سرور می مانیم)با این روش کسی نمی تواند مستقیم بر روی سرور برود,Publishing را با ISA می توان انجام داد البته بدون ISA هم با استفاده از نرم افزار های خاص می توان انجام داد.

DYNAMIC NAT

در این روش مجموعه ای ازPublicIP داریم که هر زمان سیستمی بخواهد روی اینترنت برود Ip خودش را با یک IpPublic تعویض می کند و به روی اینترنت می رود زمانی هم که برگشت همان Ip خودش را دریافت می کند و IpPublic را هم تحویل می دهد در این روش اگر به سیستمیIp Public نرسد باید منتظر باشد تا یک Ip Public خالی شود و به آن اختصاص پیدا کند,برتری این روش نسبت به روش قبل این است که از Ip ها بهینه استفاده می شود,عیب این روش هم این است که به ازای هر کلاینت احتیاج به یک Ip داریم.

FarshidAjabnoush

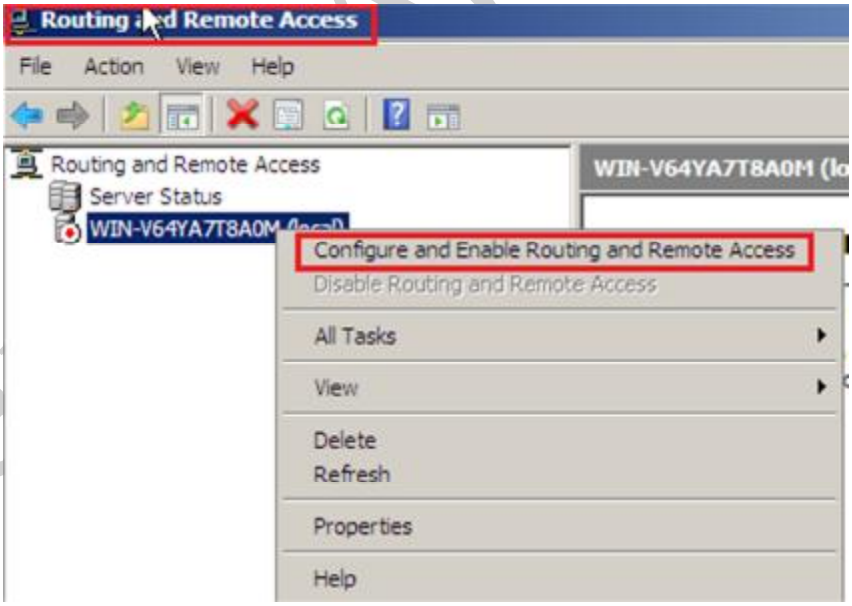
Port Address Translation

مانند روش قبل می ماند با این تفاوت که اگر Ip Public تمام شود کلاینت ,دیگر احتیاج به صبر کردن ندارد کلاینت را بر روی Ip در حال استفاده ای قرار می دهند که Download کمتری دارد به این روش OverLap گویند,مشکل این روش این است که سرعت اینترنت بخاطر استفاده چند کلاینت از یک Ip بسیار کم می شود.

- زمان استفاده چند کلاینت از یک Ipترافیکشان را با پورت از هم جدا می کنند به این معنی که کلاینت اول از یک پورت متفاوت با همان Ip مشترک استفاده می کند, تعداد پورتها 65535 می باشد.
- تمامی ISP ها از روش PAT استفاده می کنند.
- برای استفاده از اینترنت از 2 روش استفاده می کنیم NAT -1 PROXY-2

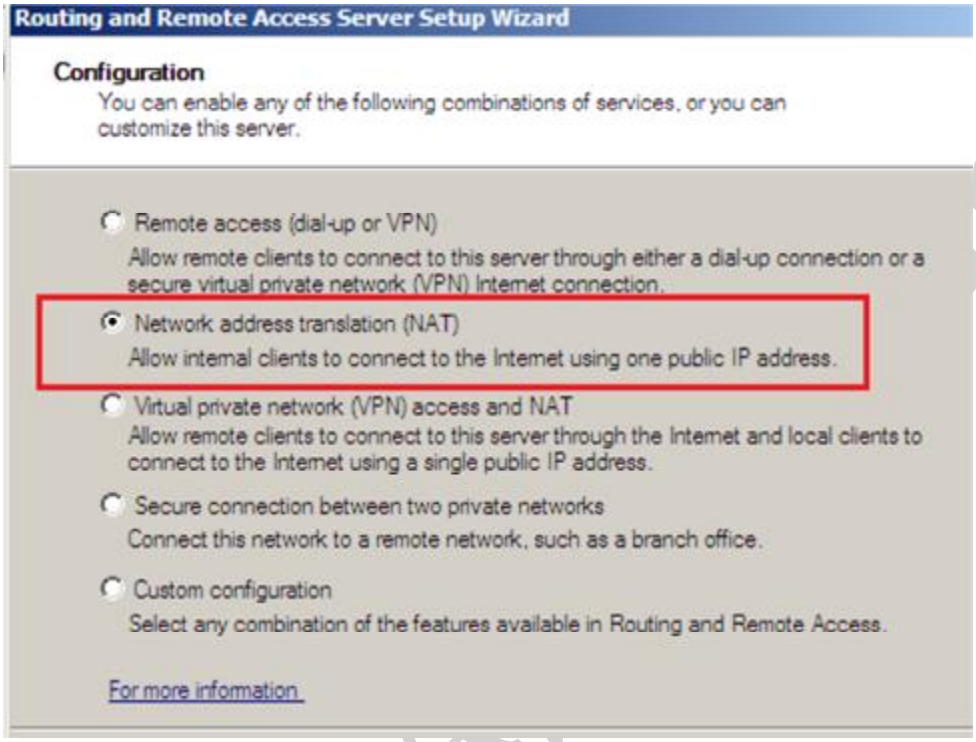
پیاده سازی NAT در SERVER 2008

ابتدا باید وارد کنسول RRAS شویم که نصب کرده ایم




Fa Niabnoush

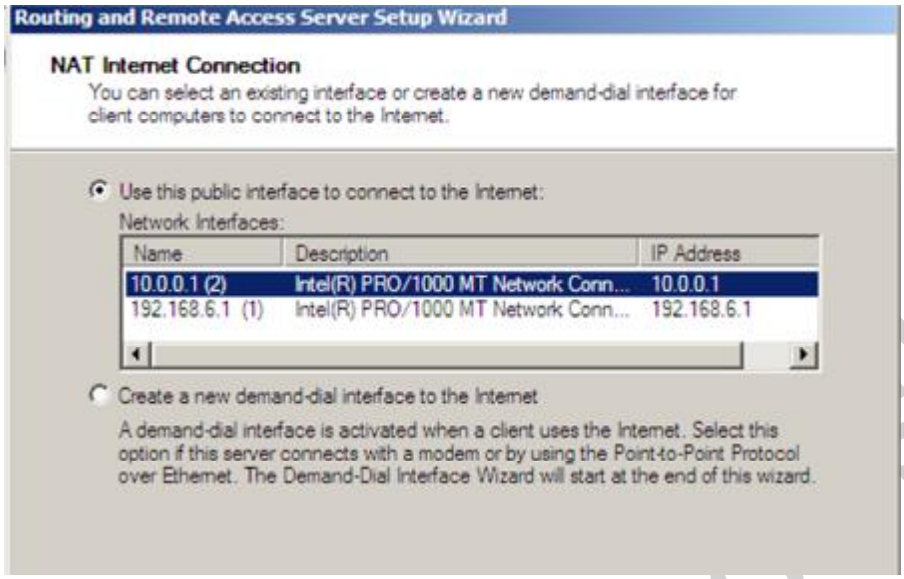
به صورت پیش فرض NAT ما از نوع PAT می باشد.




روش سوم VPN NAT می باشد که کلاینت ها باید ابتدا به سرور ما VPN بزنند سپس به اینترنت وصل شوند, با استفاده از نرم افزار NTTAC + می توان پیاده سازی کرد.

در اینجا باید کارت شبکه ای را انتخاب کنیم که بر روی آن Ip Public تنظیم شده باشد,اگر گزینه 2 را انتخاب کنیم می توانیم مودم ADSL را که بر روی آن IpPublic تعریف شده را انتخاب کنیم.

Farshidasp.ir



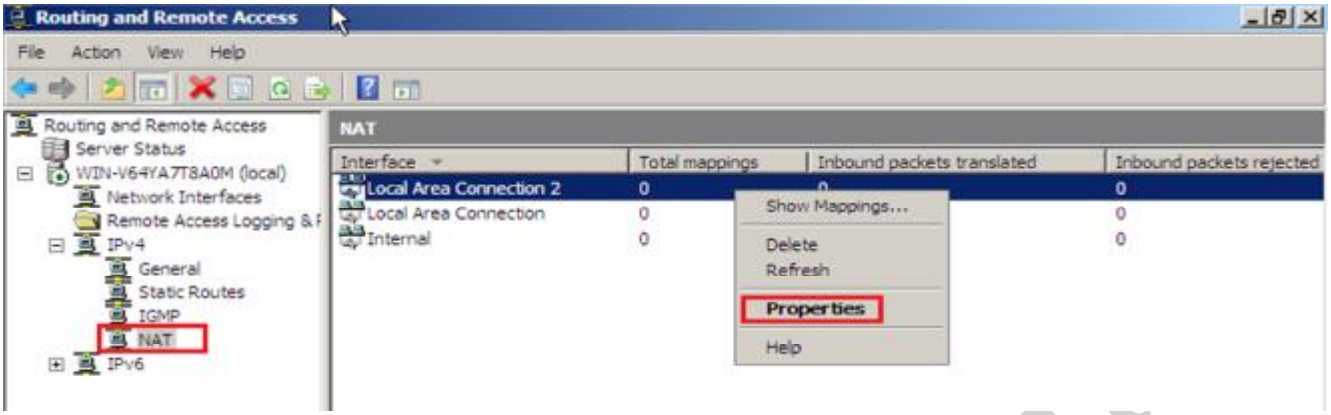

**در مرحله بعد از ما می پرسد مباحث DNSرا گی باید انجام دهد که در اینجا بر عهدهDNS تنظیم شده بر روی کارت شبکه خروجی می باشد.**

**اگر بر روی اینترنت می رویم گزینه 1 وگرنه گزینه2**

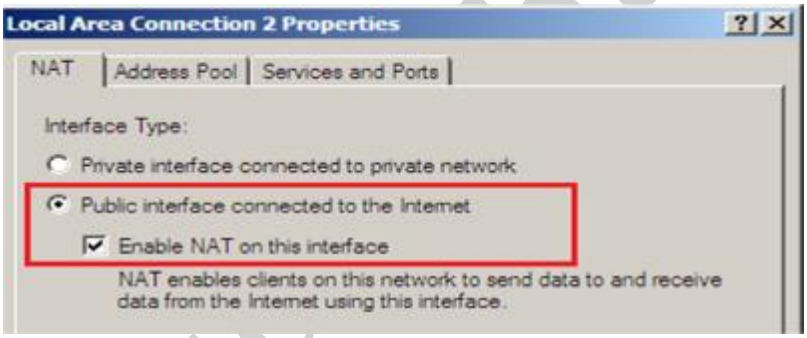
سپس Finish .

Farnia Tabnegash

پیاده سازی Static & Dynamic NAT



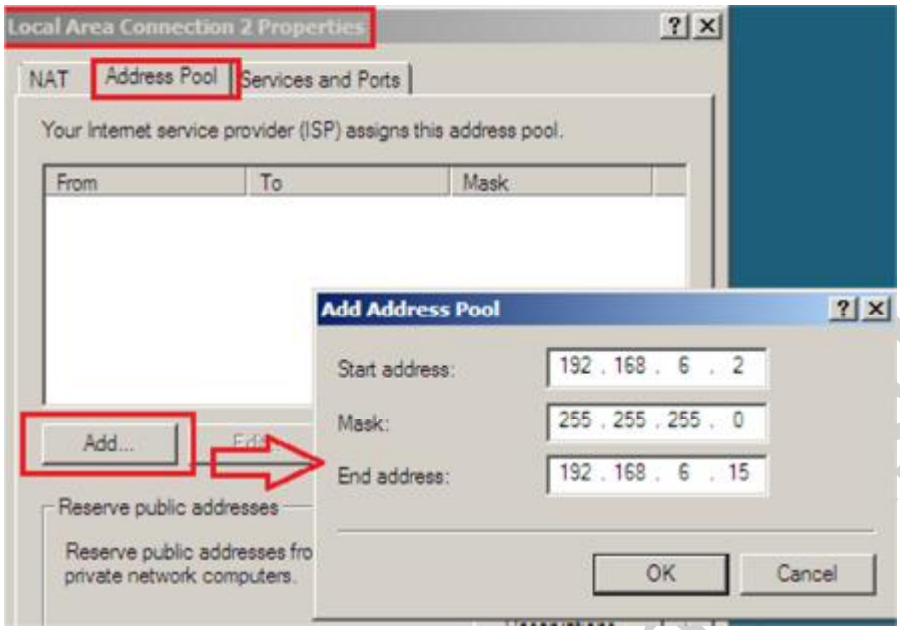

در اینجا نوع NAT ما مشخص می باشد



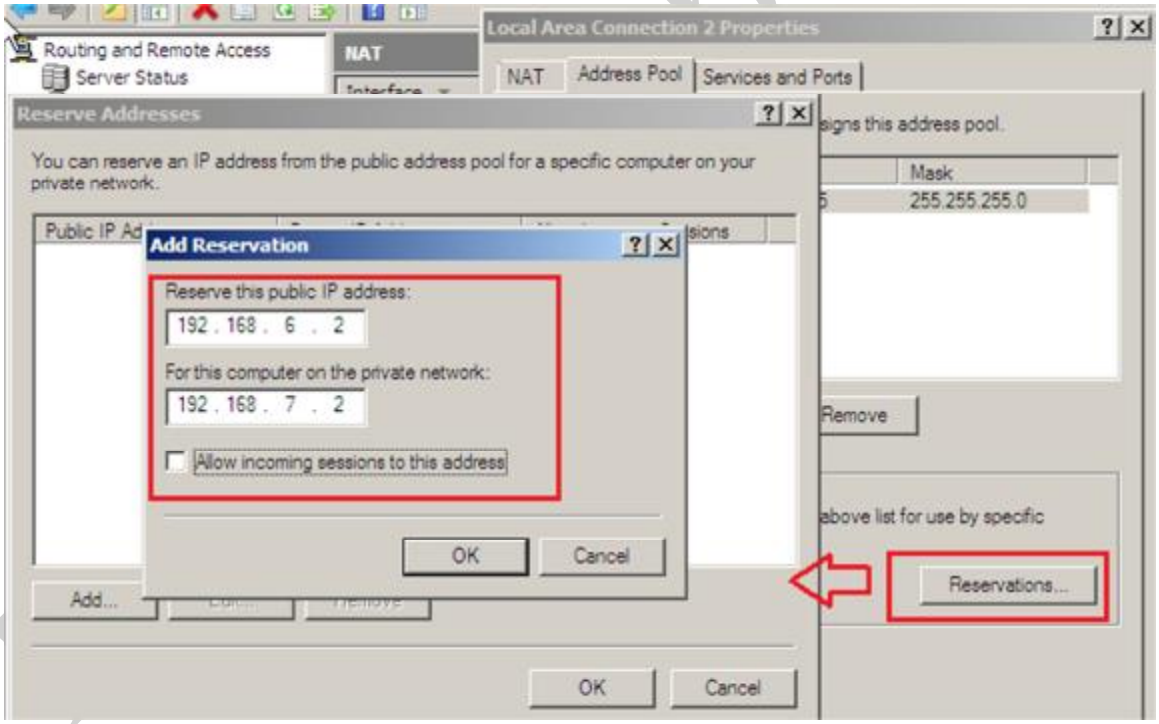

Dynamic NAT

در اینجا 6.1Ip را بر روی کارت شبکه External تنظیم کرده ایم,اینجا رنج Ip Public خریداری شده را وارد می کنیم,هیچ گاه نباید در Subnet صفر بکار ببریم چون رنج Ip را برهم می زند.

Farshid Mohammadi

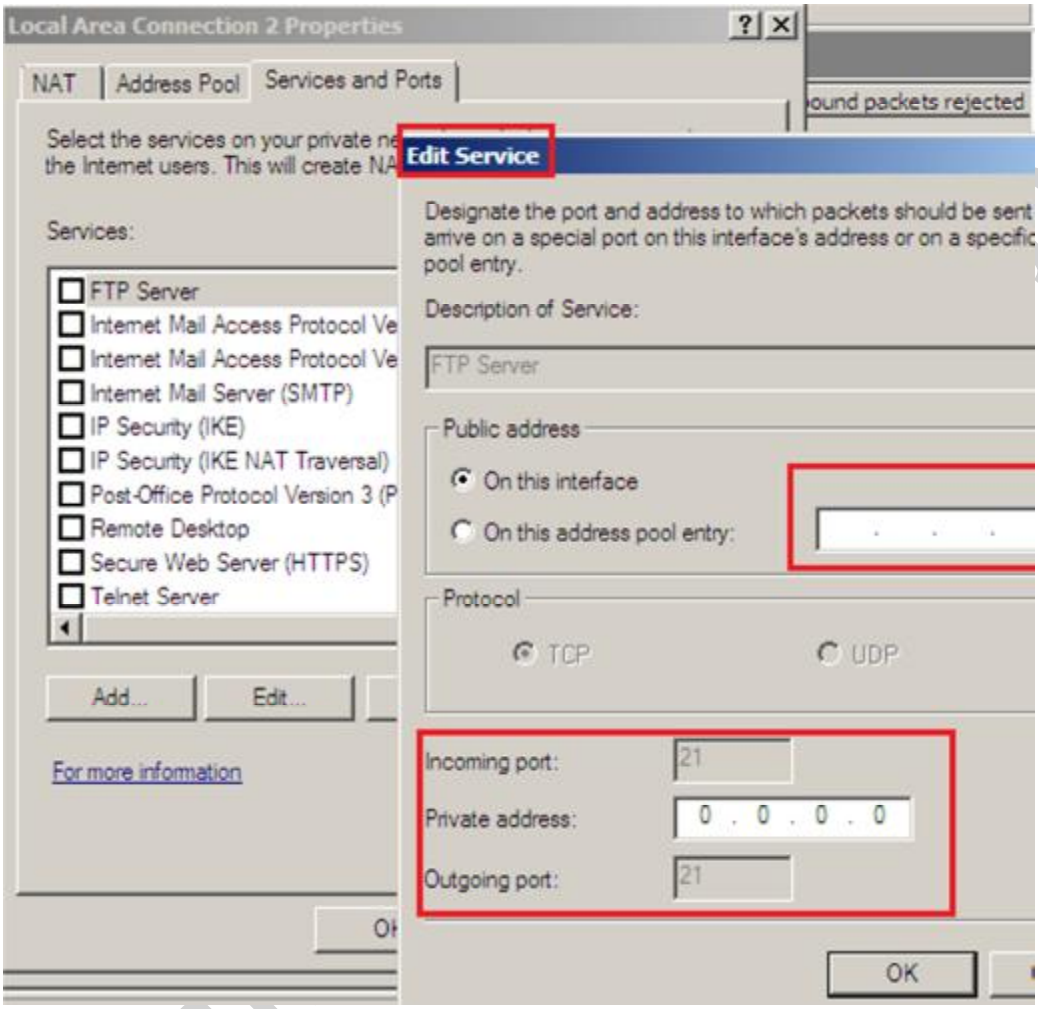



Static NAT

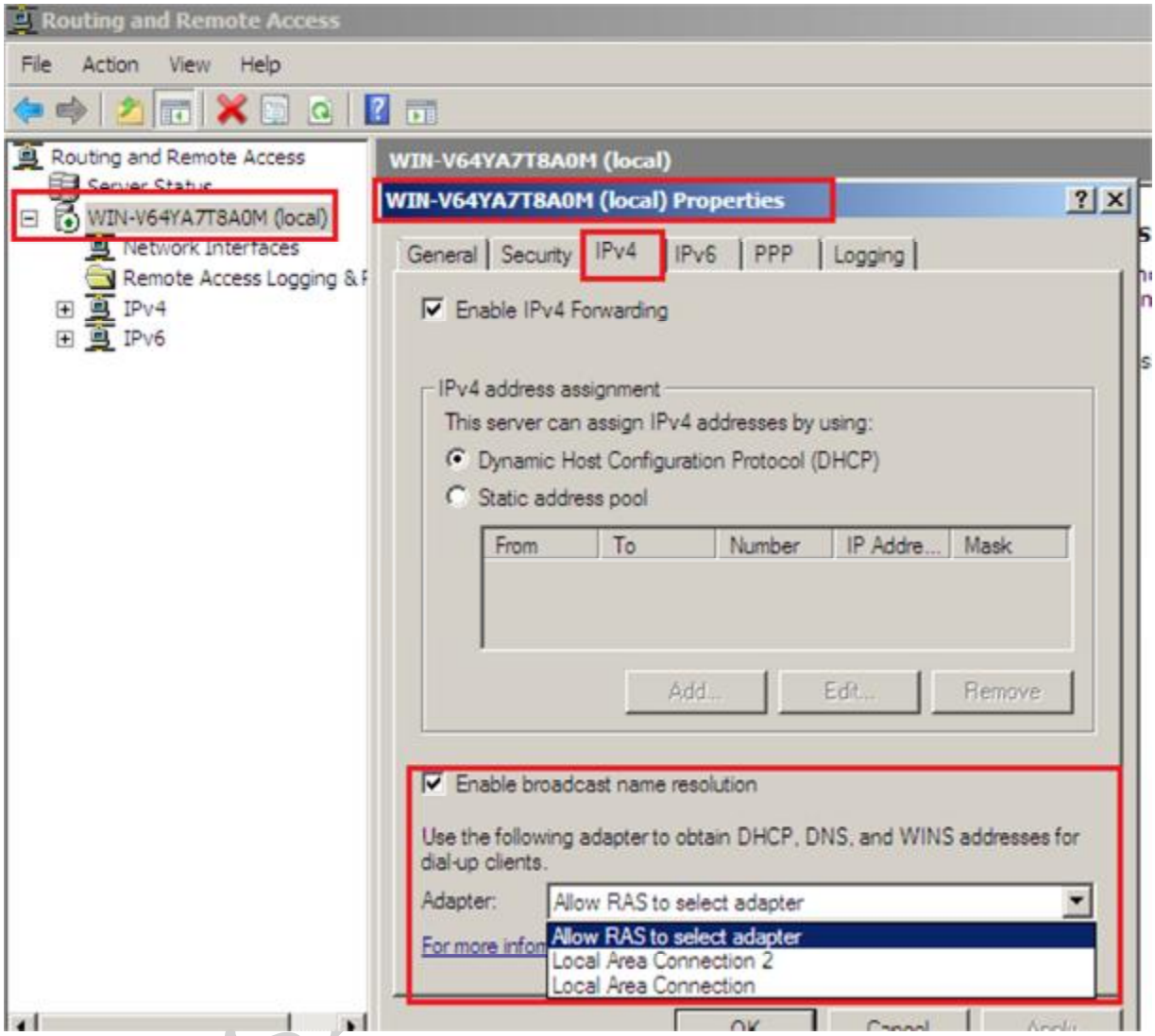



در شکل بالا مشخص می کنیم که IpPublic وارد شده(6.2) مربوط به کدام Ip Private(7.2) می باشد با فعال بودن گزینه Allow اجازه می دهیم از بیرون کسی به 6.2 وصل شود مانند این است که به 7.2 وصل شده است این کار خطرناک می باشد بهتر است Publishing کنیم.

در صفحه پایین می توان Redirection Port انجام داد که توسط آن می توانیم تعریف کنیم که اگر Ip از بیرون از شبکه بر روی پورتی مشخص به ما وصل شد به کدام Ip با کدام پورت وصل شود (دوربین های تحت Web )




Incoming Port پورتی می شود که به ما با آن وصل می شوند, Outgoing Port پورتی می شود که با آن به Ip مورد نظر در شبکه وصل می شویم.




**در شکل بالا می توانیم DNS را که تنظیم نموده بودیم را تغییر دهیم ,اگر در VPN NAT مشکل داشتیم از اینجا می توان برطرف کرد.**

Fars

A(Authentication)A(Authorization)A(Accounting) In Microsoft Network :

A(Authentication) شما را در شبکه شناسایی می کند,A(Authorization) شما شناسایی شده اید,مشخص می کند هر کسی در شبکه به چه منابعی دسترسی دارد,A(Accounting)کنترل دسترسی هاوثبت آنها.

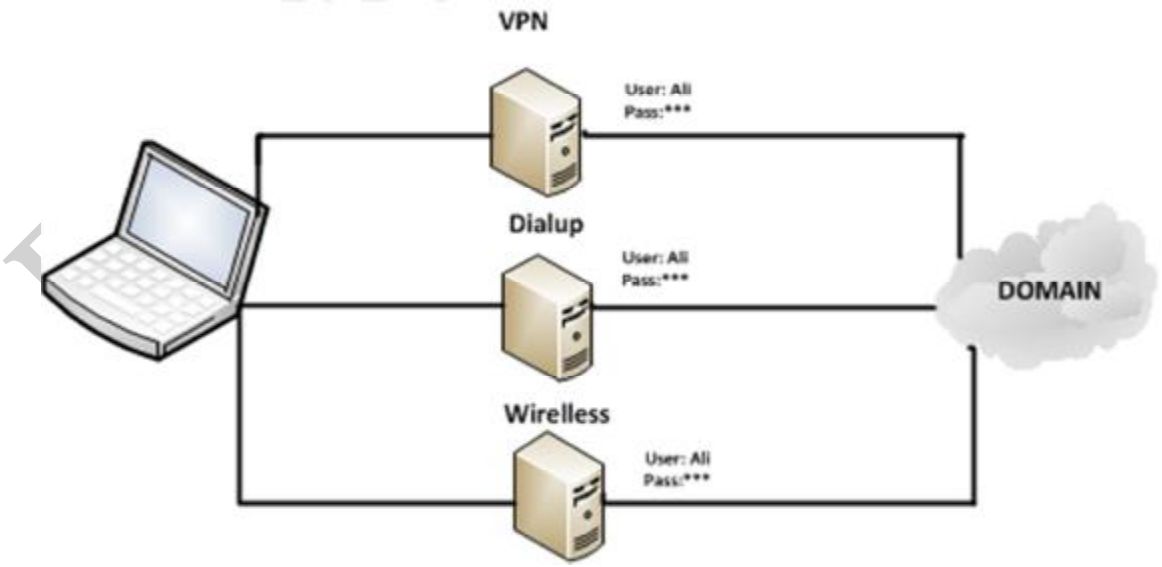
- به شبکه هایی که این سه ویژگی را بر روی یک سرور دارند Secure Host گویند و به آن سرور Radius گویند.
- برای پیاده سازی این سه ویژگی(Radius ) در ویندوز 2003 احتیاج به نصب IAS (Internet Authentication Service) و در 2008 احتیاج به نصب NPS (Network Policy Service) داریم.

دلیل استفاده از Radius

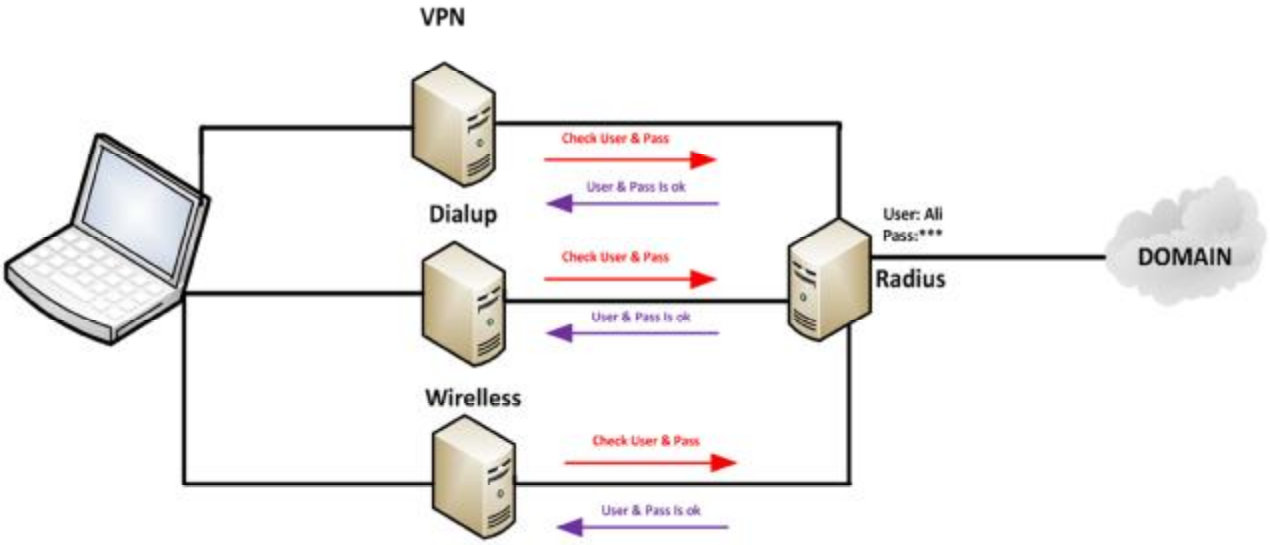
وظیفه این سرور Authentication می باشد

فرض کنید می خواهیم به شبکه خودمان وصل شویم برای این کار 3 روش (به طور مثال) در نظر می گیریم -VPN Dialup-Wireless هر بار به یک روش وصل می شویم به همین دلیل باید پشت هر کدام از این سرورها یوزر و پسورد ما موجود باشد,هر بار که به هر کدام از این سرورها وصل می شویم از ما یوزر و پسورد را می پرسد و با یوزر و پسورد موجود در خودش چک می کند, این روش باعث پایین آمدن امنیت شبکه می شود به این دلیل که یوزر و پسورد ما 3 جا در شبکه موجود است,این روش باعث بالا رفتن هزینه امنیت سرورها هم می شود چون 3 بار باید ایجاد امنیت کنیم.

روش دیگر و امن تر این است که یوزر و پسورد ما بر روی یک سرور(Radius) ذخیره شده باشد و هر بار که ما خواستیم به شبکه وصل شویم (با هر کدام از این روش ها) سرورهای موجود یوزر ما را از سرور موردنظر بپرسند.



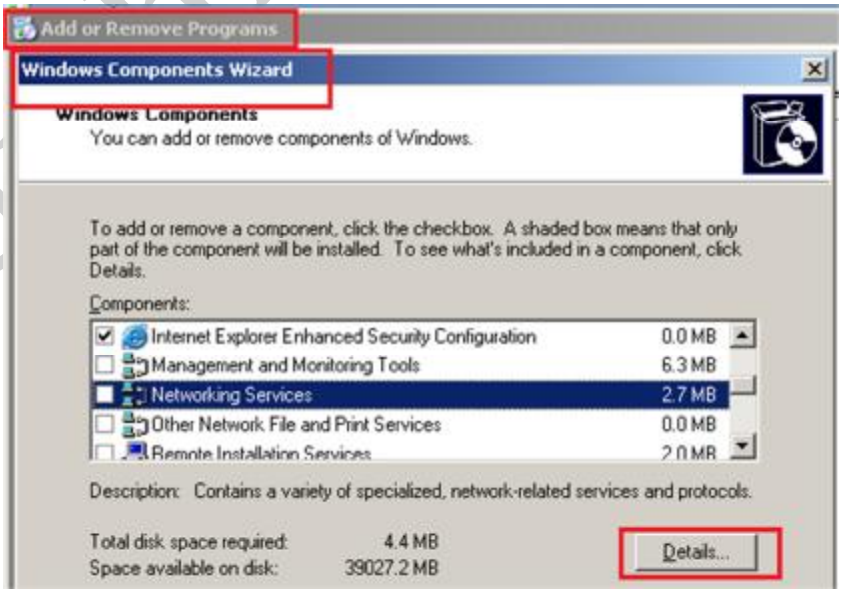

روش اول



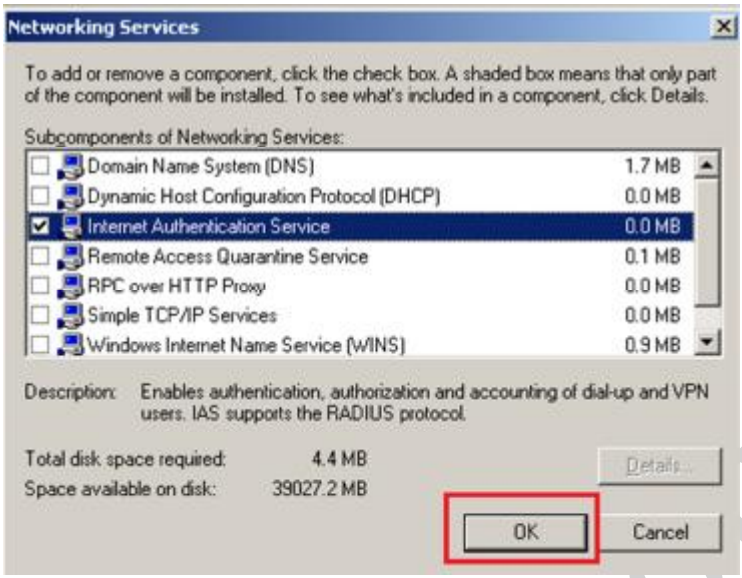

روش دوم

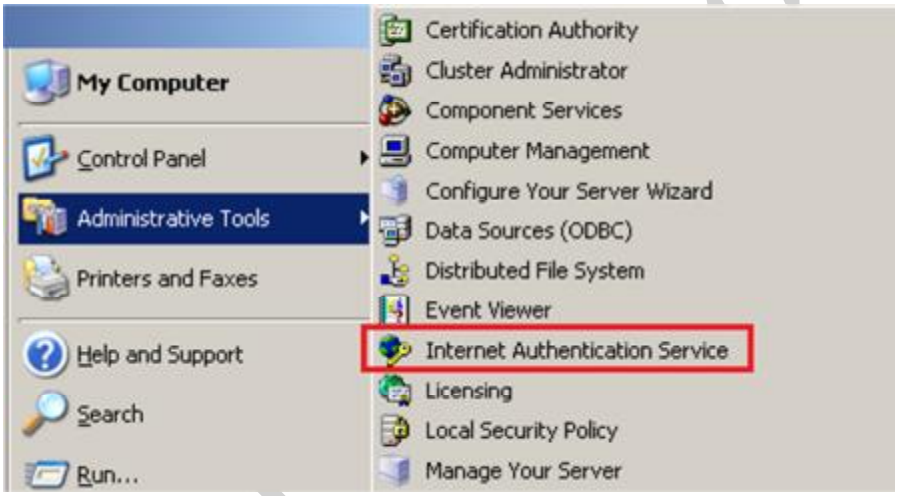
- در سناریو دوم به آن سه سرور Radius Client گویند.
- Radius یک مشکل دارد که در آن نمی توان یوزر های FlowTin (شناور)ایجاد کرد منظور از شناور این است که ما می خواهیم به یک یوزر در طول روز 2 ساعت اجازه استفاده بد هیم برای این کار باید حتما بازه زمانی تعریف کنیم (مثلا 8 تا 10 صبح) نمی توانیم بگوییم در کل روز جمعاً 2 ساعت استفاده کند برای رفع این مشکل از نرم افزار NT Tac + می توان استفاده کرد.

پیاده سازی Radius در 2003



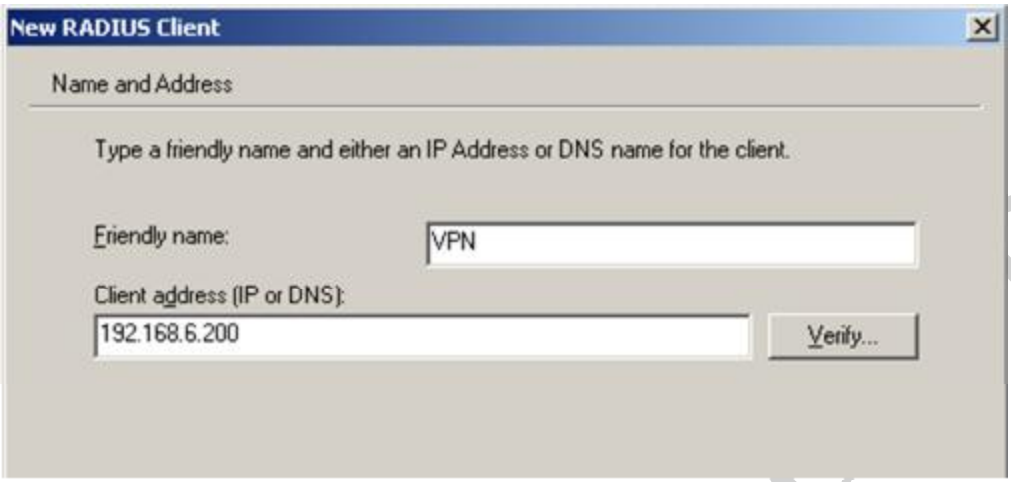

FarhidAfaghi



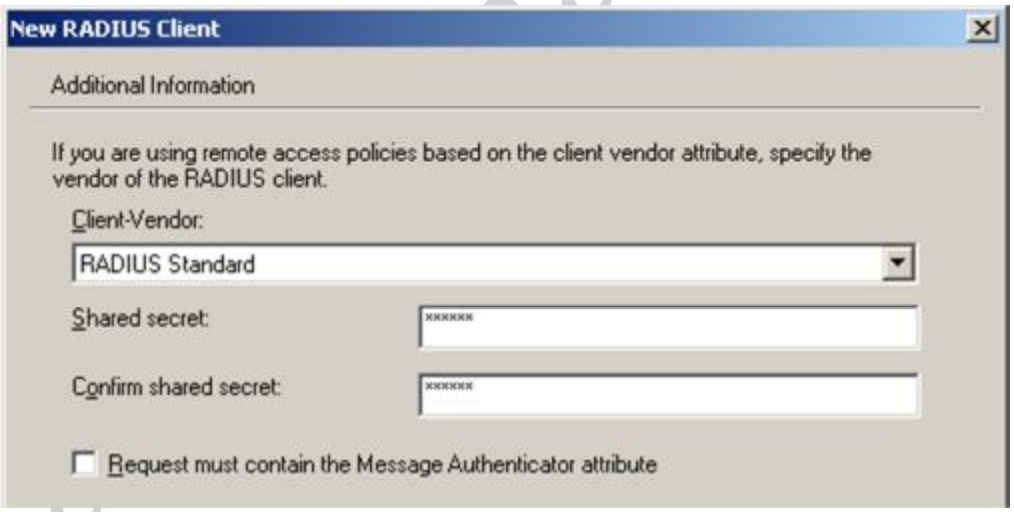



در مرحله4 باید RadiusClient تعریف کنیم(همان سه سرور)

در اینجا اسم سرور و IP را وارد می کنیم

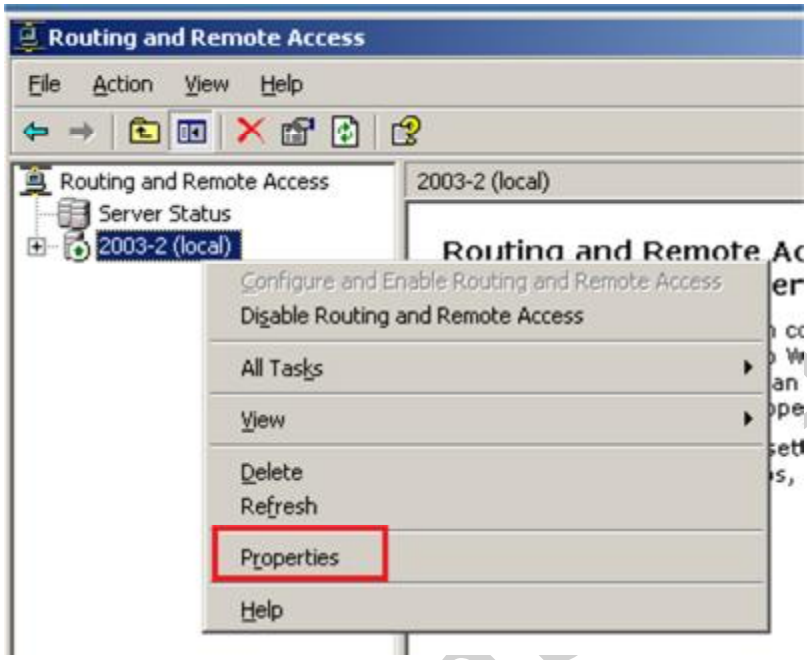


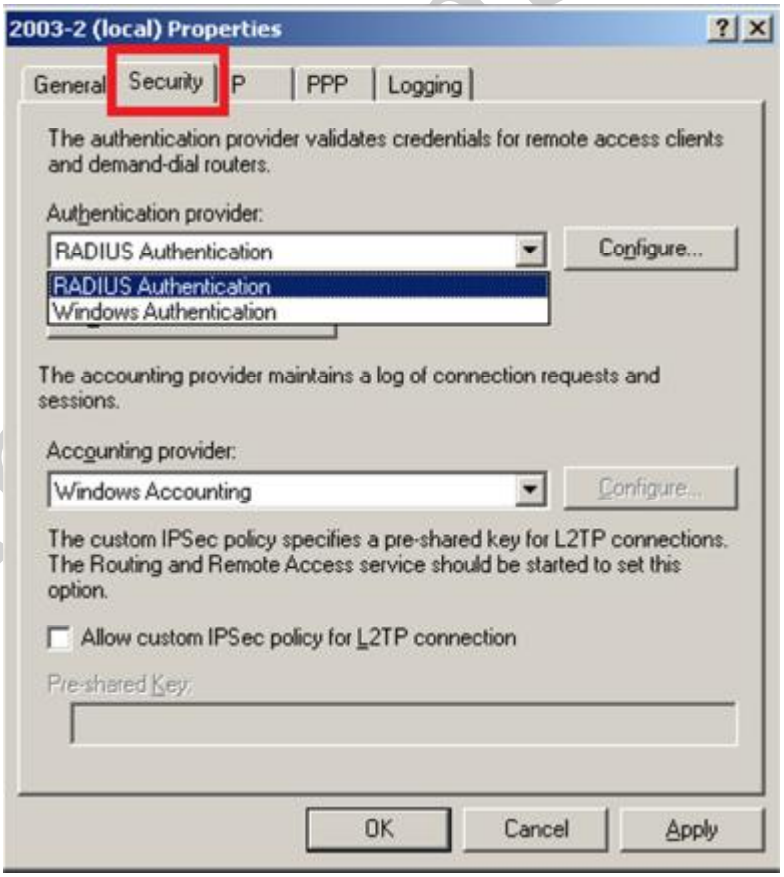

در اینجا باید برای شناسایی سرور معرفی شده به Radius یک پسورد تنظیم کنیم که Radius سرور مورد نظر را با این پسورد شناسایی می کند,گزینه ..Request می گویدعمل شناسایی رمز شود ؟




- VPN و Radius نباید پشت یک سرور باشند.

حالا نوبت به معرفی Radius بر روی VPN می باشد برای این کار وارد سرور VPN می شویم و مانند زیر عمل می کنیم

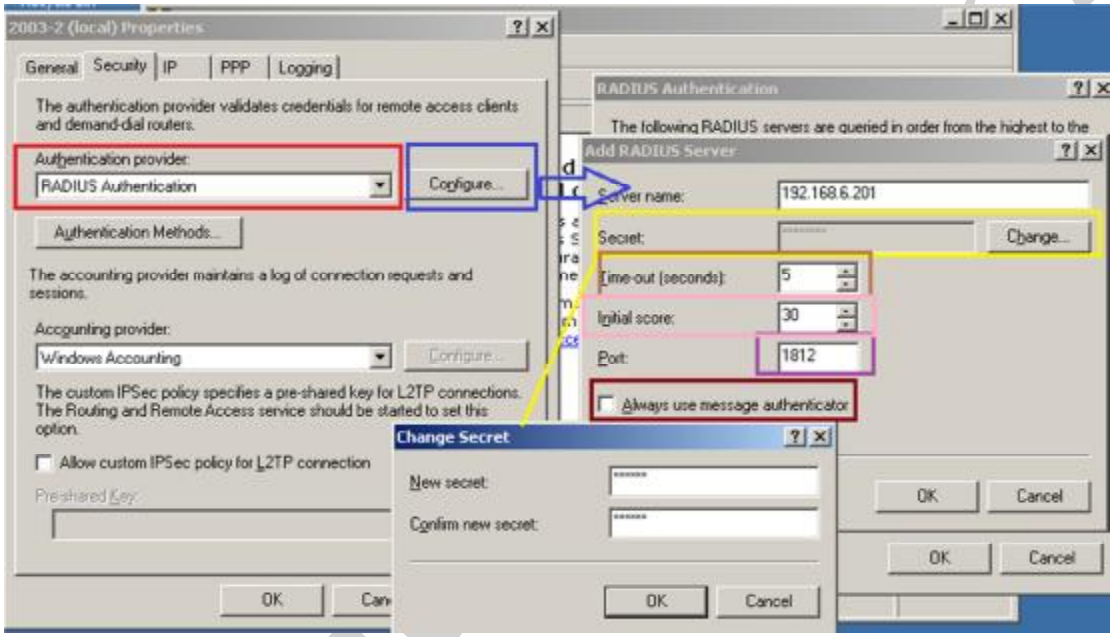


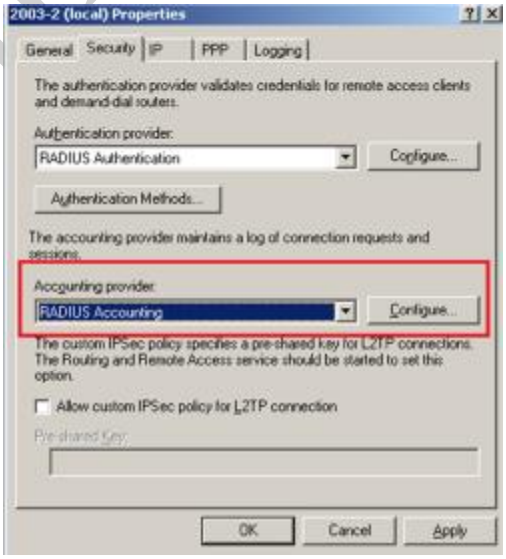
در صفحه باز شده باید بگوییم عمل شناسایی را بر عهده Radius بگذار سپس Ip , Radius را وارد می کنیم,در قسمت پسورد باید پسورد وارد شده در RadiusClient را که تنظیم کرده ایم وارد کنیم اگر در RadiusClientگزینه رمز نگاری را فعال کرده ایم در اینجا هم باید آن را فعال کنیم,پورت شناسایی در Radius,1812 می باشد,یعنی پشت سرور Radius اگر Firewall داریم باید پورت 1812 باز شود.

در قسمت Time مدت زمانی که RadiusClient باید منتظر جواب گرفتن از Radius باشد را نشان می دهد.

قسمت Intial,اگر درشبکه چندین Radius داشته باشیم با این اعداد آن ها را از هم جدا می کنیم,هرچه این عدد بزرگتر باشد ارجعیت آن Radius هم بالا تر است.




- پورت Accounting(Log ) هم 1813 می باشد.




- پورت ,+Tacas 1646 و1647 می باشد.

Farshid

سپس باید یک بار سرویس RRAS را Restart کنیم.

Remote Access Policy

به کسانی که از بیرون به سرور RRAS ما وصل می شوند می توان یک سری پالیسی اعمال نمود که شرایطی همچون زمان ورود,نوع پروتکل های مورد استفاده را چک کند به این نوع پالیسی Remote Access Policy می گویند مانند یوزر و پسورد اینترنت های شبانه و روزانه.

Remote Access Policy از 3 قسمت تشکیل شده اند :

1- Condition: یک سری شرط می باشد که موقع وصل شدن چک می شوند مانند:

Time,Group,Authentication

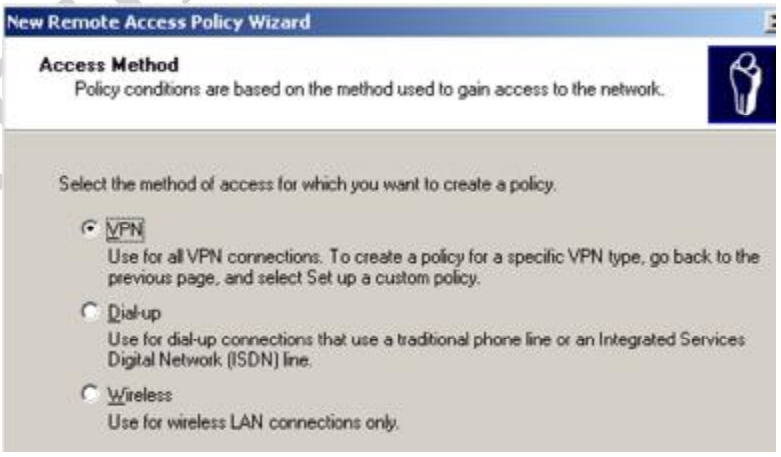
2-Profile: شروطی می باشد که بعد از وصل شدن چک می شود حتی می توان بعضی شروط را اعمال کرد مانند: Session Timeout و Idle Timeout

3-Permission : در اینجا می توان تنظیم کرد که اگر شروط لازم را داشت اجازه وصل شدن را بدهد و اگر نداشت اجازه وصل شدن را ندهد.

Farzad Ajabnoush

برای نوشتن پالیسی فرقی نمی کند که پشت VPN می نویسیم یا پشت Radius,در اینجا پشت Radius می نویسیم

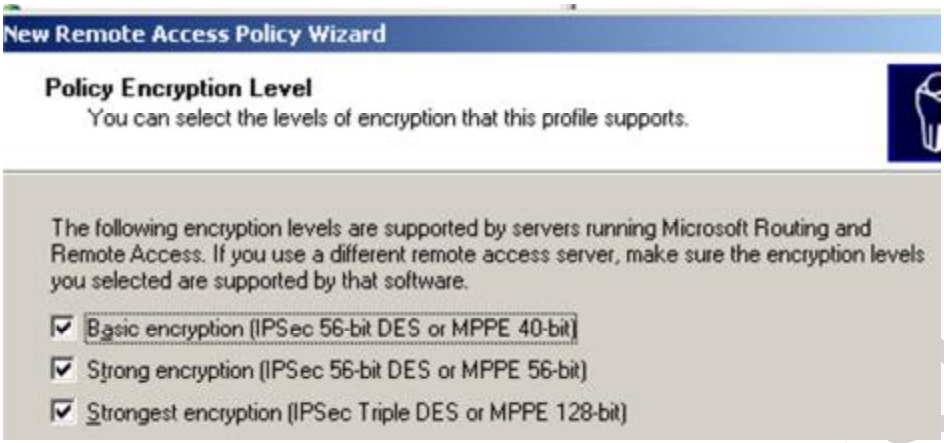
یک اسم برای پالیسی مشخص می کنیم



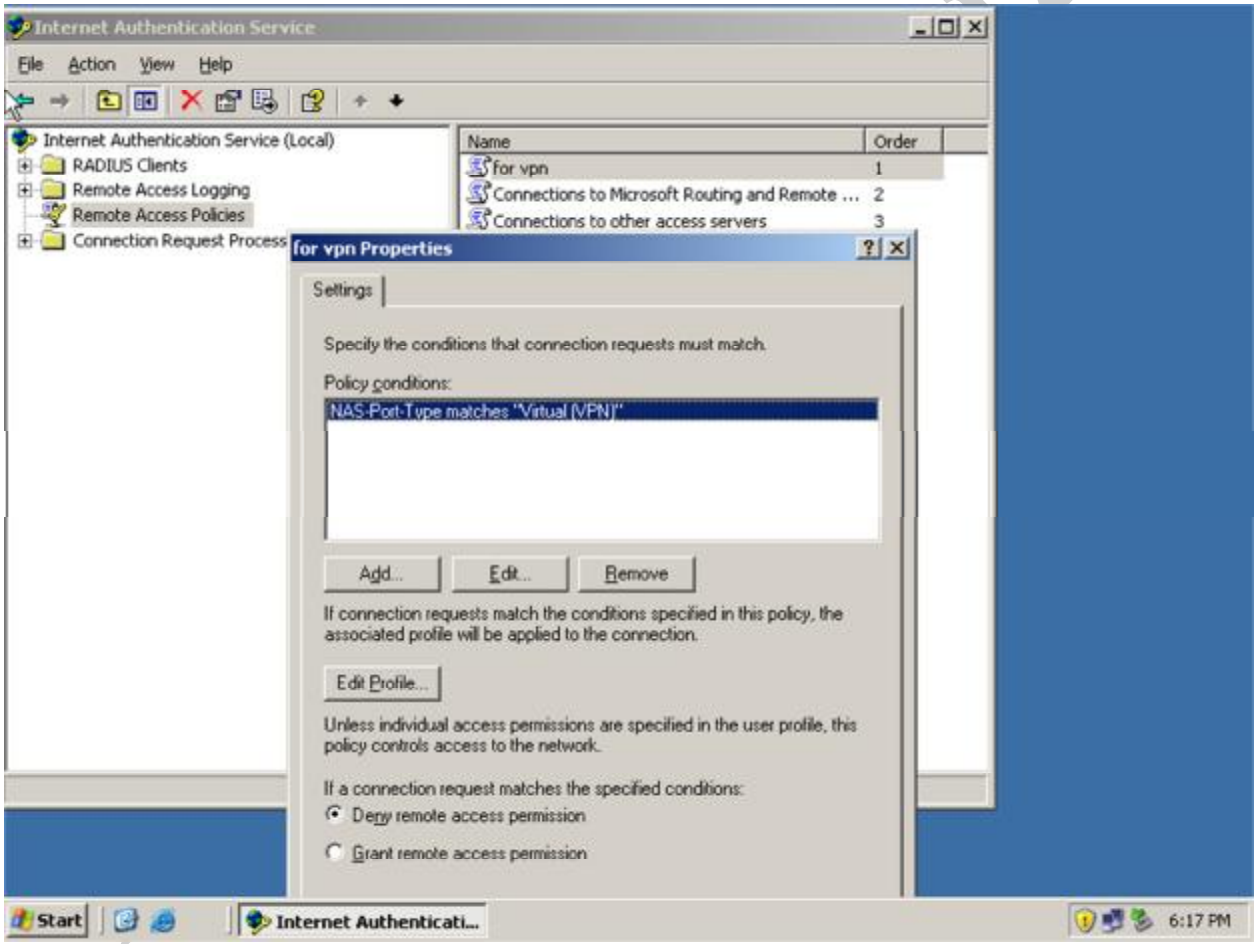

Farhad Soroush

اگر بخواهیم پالیسی به همه اعمال شود User را انتخاب می کنیم و اگر بخواهیم به یوزری مشخص اعمال شود Group را انتخاب می کنیم(باید یک گروه بسازیم و یوزر را درون آن قرار دهیم)

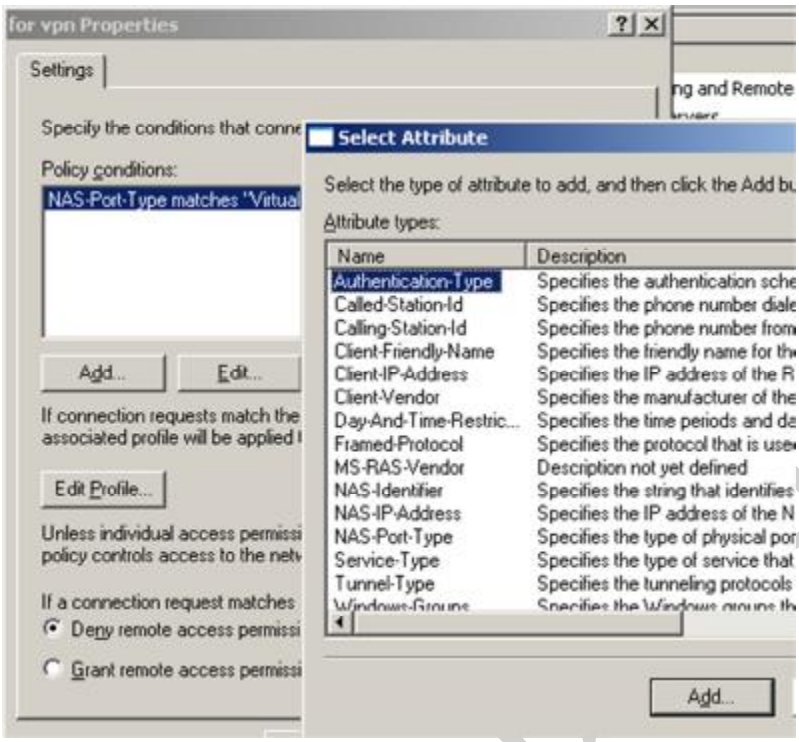
- پروتکل های Authentication برای کانکشن های Point To Point (VPN )
- PAP(PasswordAuthentication Protocol) :یوزر و پسوردها را به صورت ClearTXT ردوبدل می کند.
- SPAP(Shiva PAP) :شیوا اسم یک شرکت امریکایی است که سرورهای بانک را تولید می کند.
- CHAP(Chalenge Authentication Protocol) : یوزر وپسورد ها را Hash ردوبدل می کند.
- Ms Chap : پروتکل Chap مخصوص مایکروسافت و 2 ورژن است,1 برای ویندوزهای 98, 2برای 98 به بالا
- EAP(Extensible Authentication Protocol) : به صورت توافقی عمل می کند.



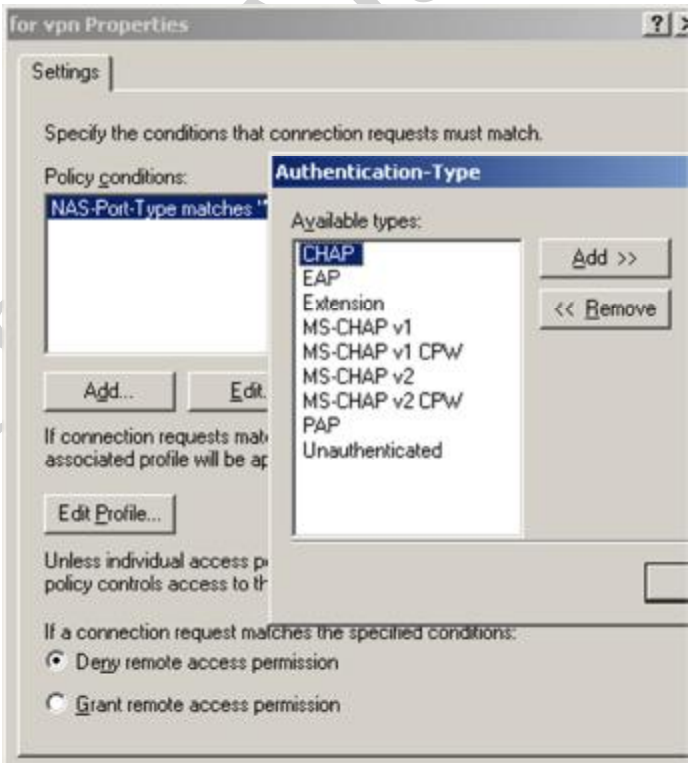

در آخر Finish




سپس روی پالیسی نوشته شده Properties می گیریم وAdd را می زنیم و در اینجا می توان شرط تعیین کرد.

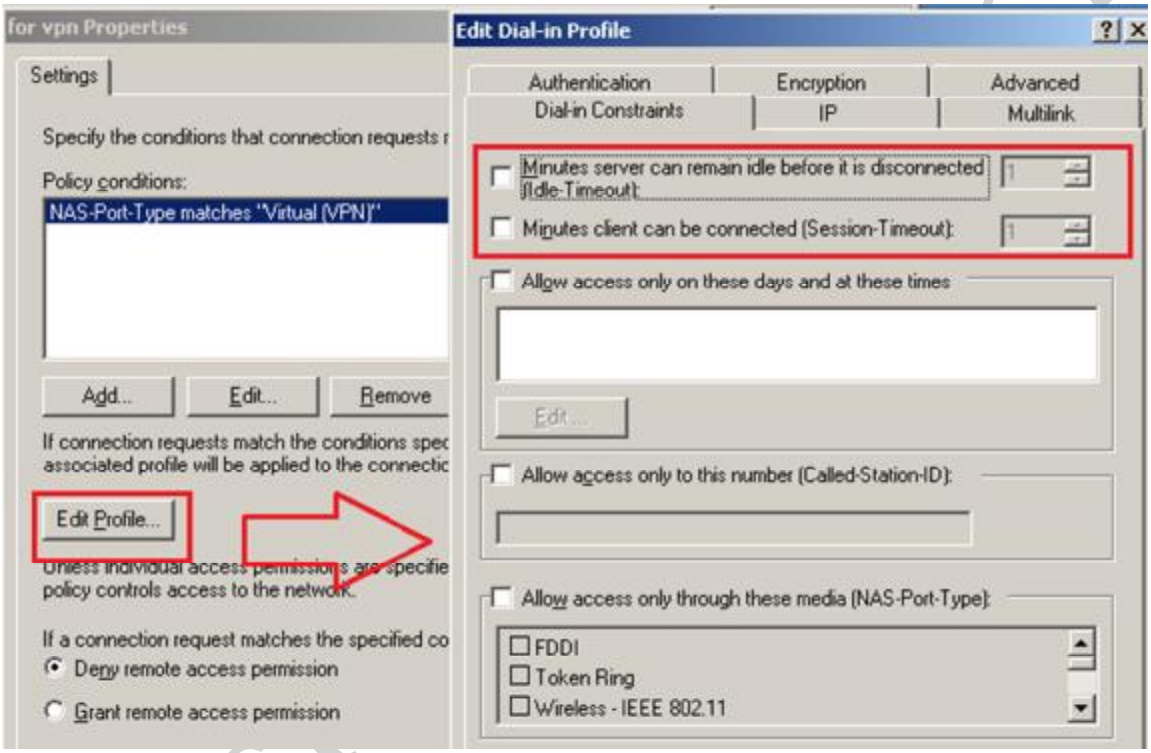



Edit را می زنیم و در اینجا می توان پروتکل شناسایی را تعیین کنیم




بعد از تعیین شروط می توانیم بگوییم اگر این شروط را دارد وصل شود (...Grant Remote) و یا اجازه وصل شدن را ندهد (...Deny Remote ).

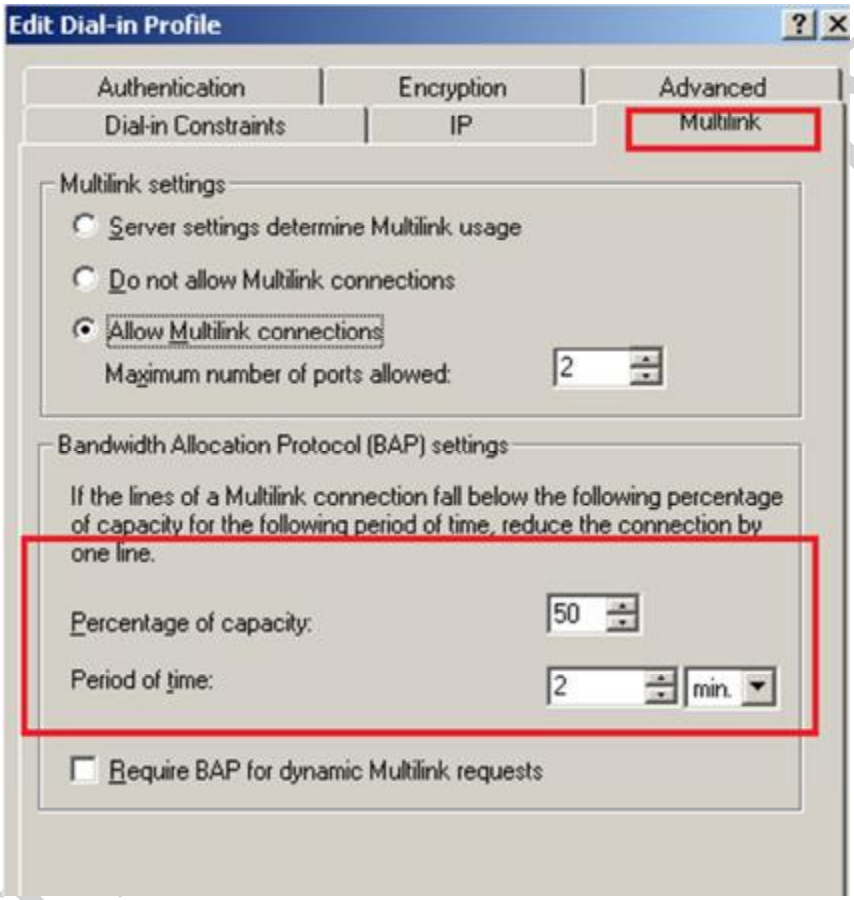
در مرحله بعد مانند زیر عمل می کنیم,گزینه اول Idle یعنی اگر 1 دقیقه غیر فعال (بیکار) بود کانکشن آن را قطع کن,Session یعنی چه فعال بود و چه نبود بعداز زمان مشخص شده آن را قطع کن.




Farsi

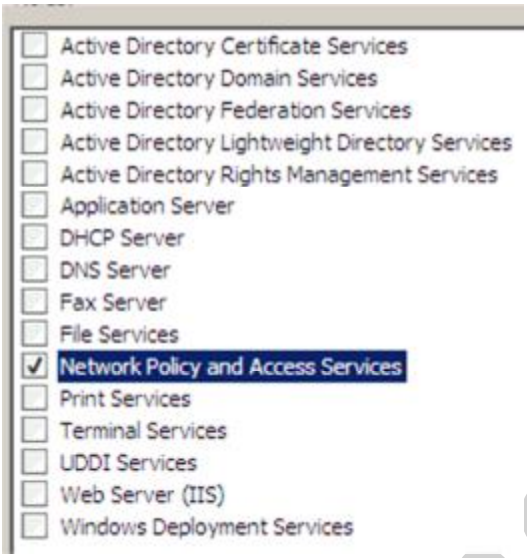
با فعال بودن MultiLink می توان با یک یوزر و پسورد, 2 یا بیشتر کانکشن زد مانند VPN های 2کاربره.

در قسمت دوم می گوید اگر یکی از کانکشن ها به مدت 2 دقیقه نتوانست بیش از 50% کانکشن را استفاده کند آن را قطع کن,با فعال بودن گزینه آخر(...Dynamic ) سرور تشخیص می دهد که حجم کانکشن اول کاملا پر شده است و کانکشن دوم را به صورت اتوماتیک ایجاد می کند.



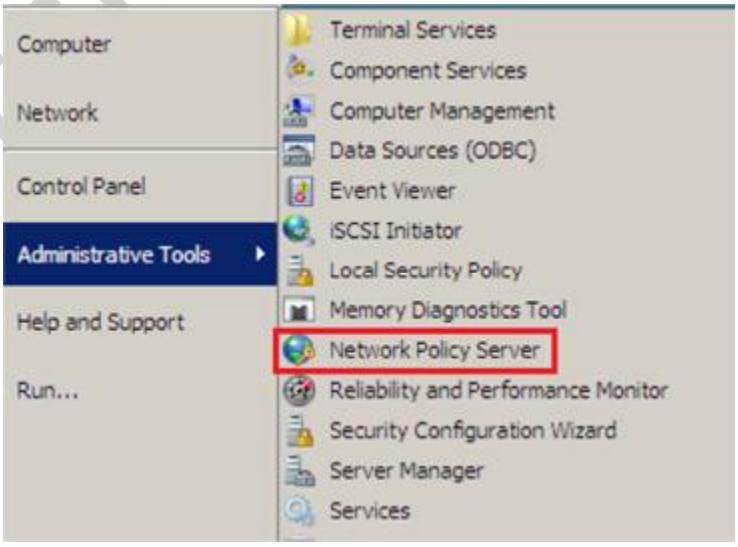

Farsh

پیاده سازی Radius در سرور 2008



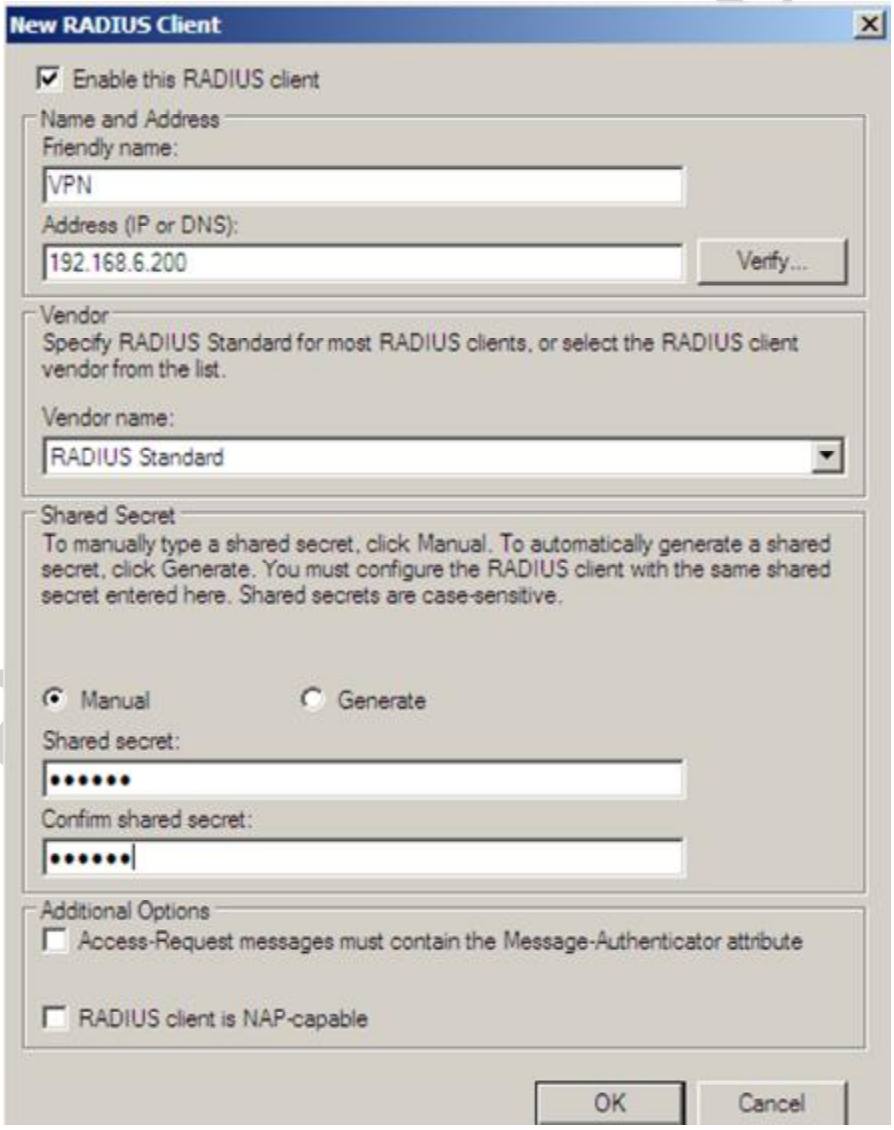
سپس Install.

سپس وارد کنسول آن می شویم

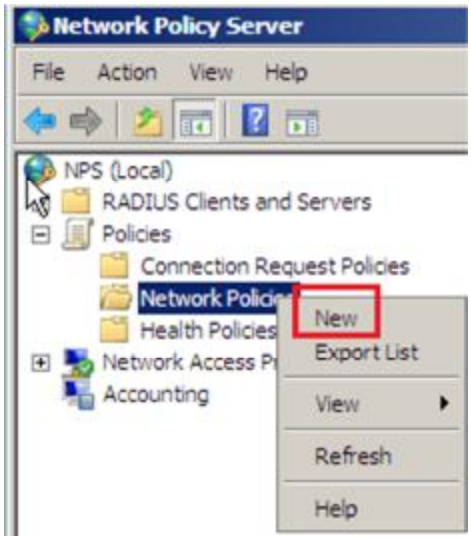



Farhidnoush

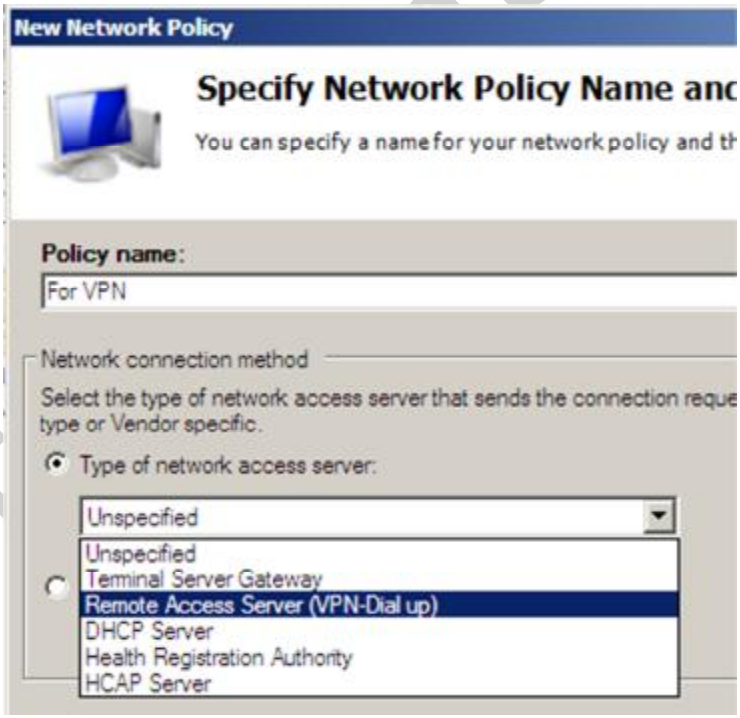
در مرحله بعد(شکل زیر) تمامی مراحل را یکجا می بینیم,NAP سرویسی است که سلامتی کلاینت ها را چک می کند.



برای نوشتن پالیسی مانند زیر عمل می کنیم

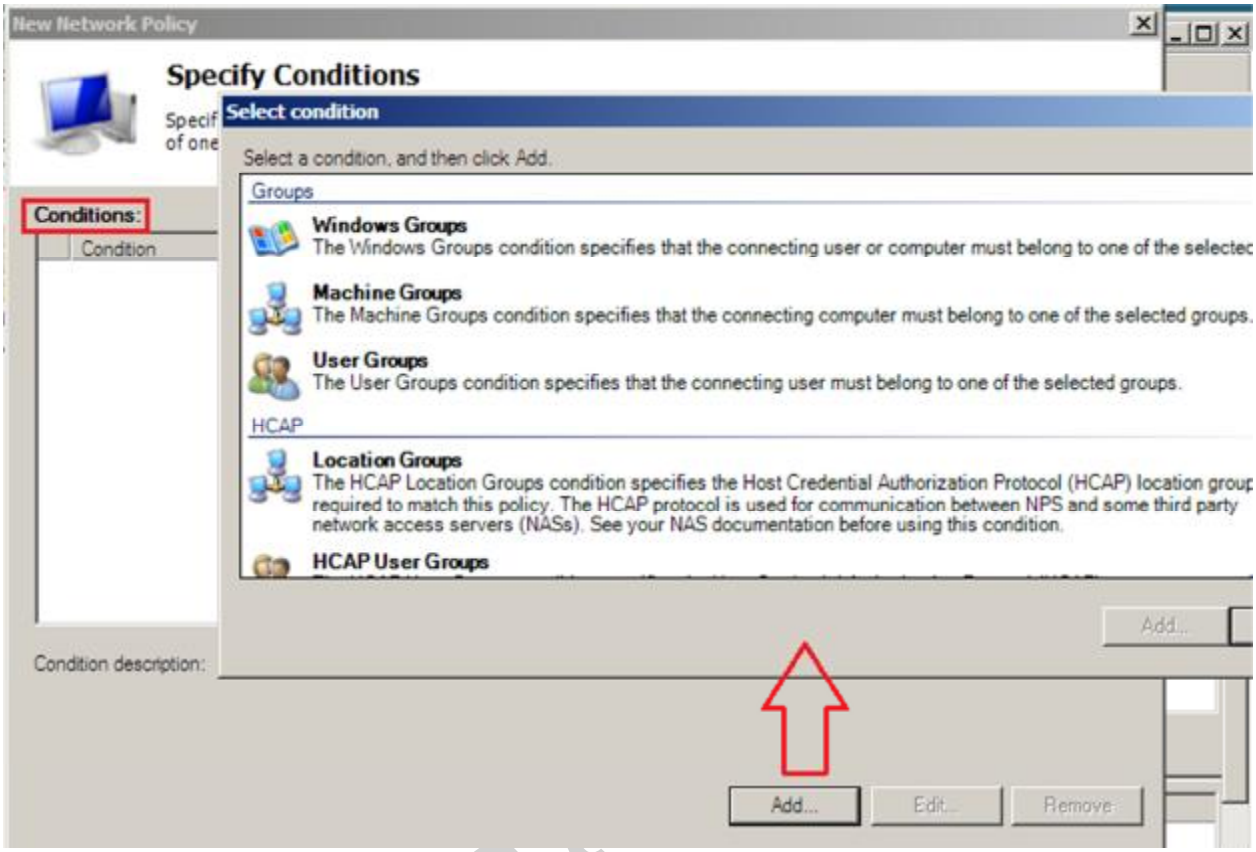



در مرحله بعد اسم می دهیم و سرویس مورد نظر را انتخاب می کنیم

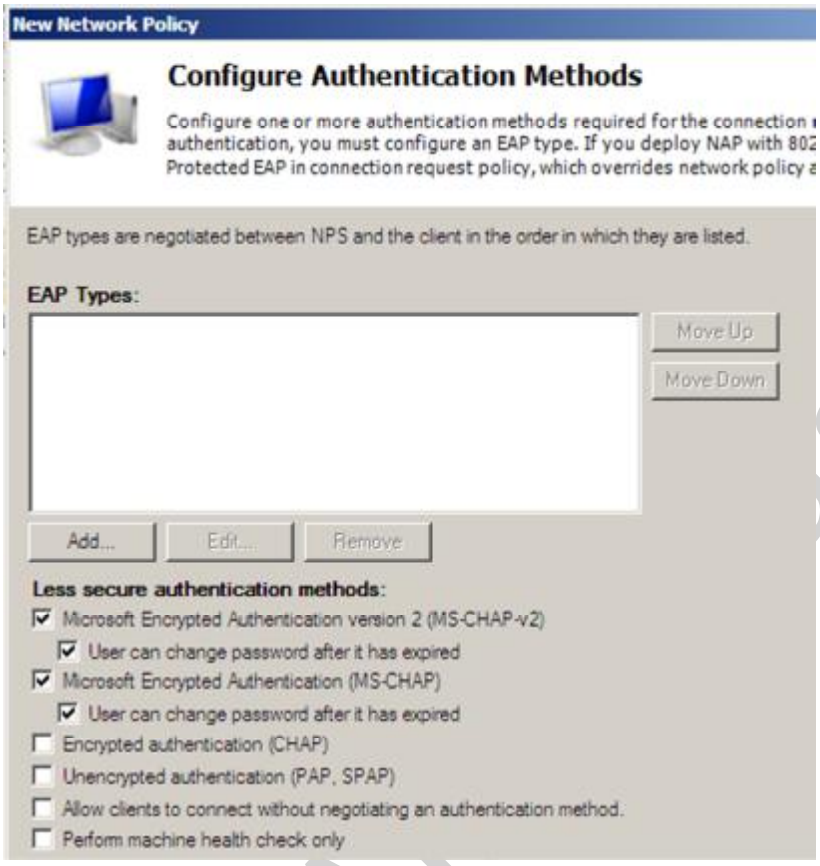


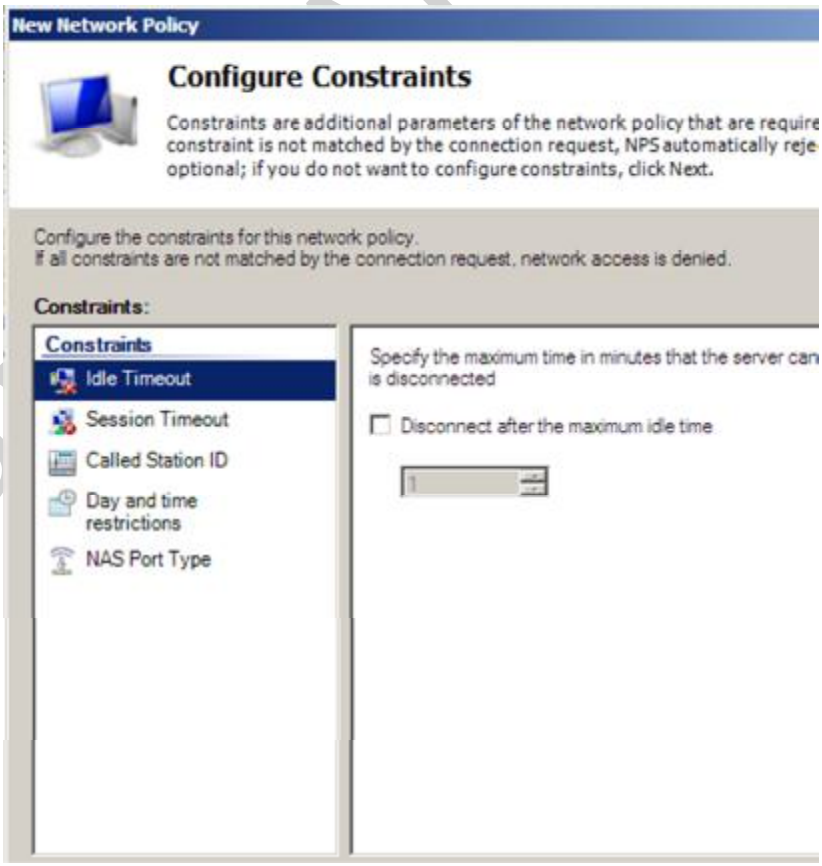

Farboush

سپس نوبت به انتخاب شروط می رسد

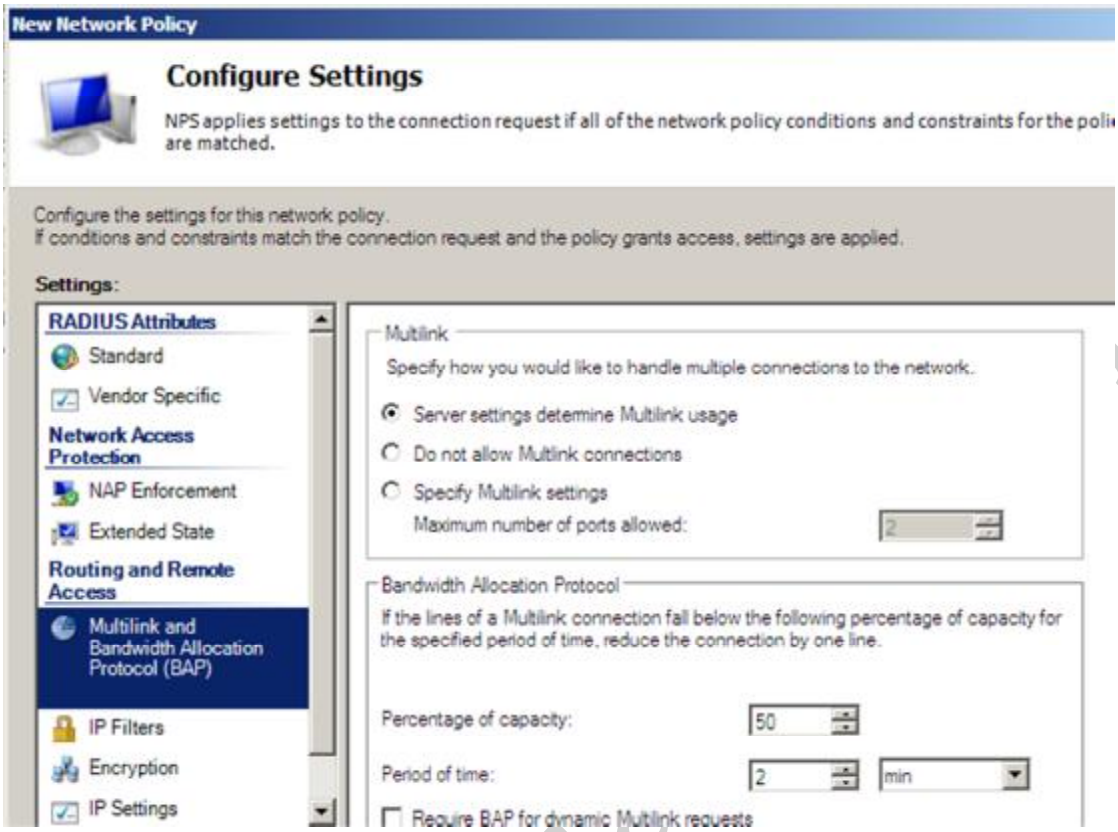



تمامی مراحل مانند 2003 می ماند ولی زیباتر


New Network Policy
Configure Authentication Methods
Configure one or more authentication methods required for the connection
authentication, you must configure an EAP type. If you deploy NAP with 802
Protected EAP in connection request policy, which overrides network policy
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method.
Perform machine health check only


New Network Policy
Configure Constraints
Constraints are additional parameters of the network policy that are require
constraint is not matched by the connection request, NPS automatically reje
optional; if you do not want to configure constraints, click Next.
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Specify the maximum time in minutes that the server can
is disconnected
Disconnect after the maximum idle time
1

Fa sh




و سپس در آخر Finish.

**پیاده سازی Clustring در شبکه های مایکروسافتی**

**به سرورهای مستقل از هم که در کنار هم فعالیت می کنند تا بتوانند یک سرویسی را ارائه دهند کلاستر گویند.**

**در سرور 2008 برای سه هدف 1-Loadbalancing 2- Scalabitity 3- HighAvaiabilityسرورهایمان را کلاستر می کنیم.**

**سه روش برای کلاستر کردن وجود دارد 1- DNS RoundRabin 2- NLB Cluster 3- Failover Cluster**

- **ساده ترین روش Loadbalancing , Loadbalancing DNS می باشد.**
- **Scalabitity : زمانی که یک شبکه را طراحی می کنیم باید امکان رشد کلاینتها را در نظر داشته باشیم,یعنی اگر در حال حاضر شبکه ما 100 کلاینت دارد امکان دارد در آینده به 1000 کلاینت برسد باید ما بستر شبکه را برای 1000 کلاینت درنظر بگیریم,شبکه ای که این قابلیت را دارد در اصطلاح می گویند این شبکه Scalabitity دارد.**

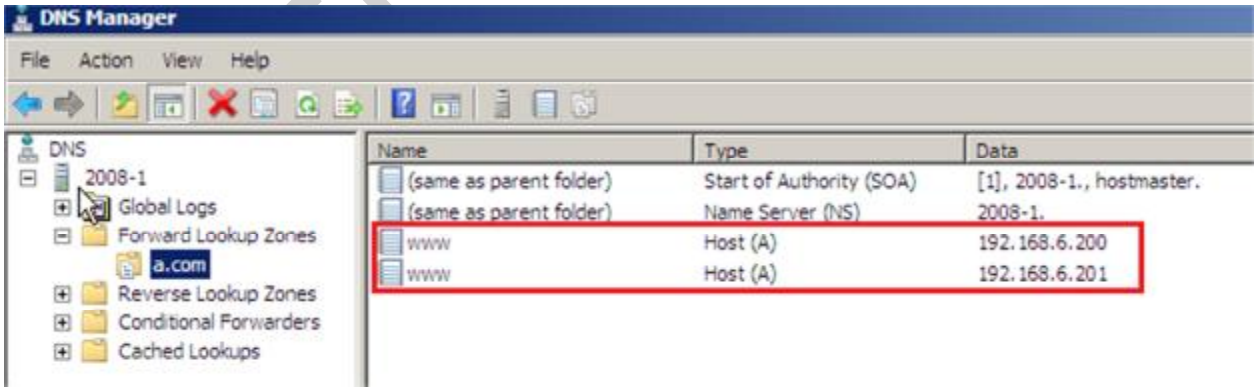
FarshidAja

- HighAvaiability ( دسترسی در شرایط سخت): زمانی که در شبکه ای سرویس دادن به مشتریان بسیار مهم است از چندین سرور استفاده می شود که اگر سروری نتوانست سرویس دهد بقیه سرورها سرویس بدهند به شبکه ای که این قابلیت را دارد, می گویند این شبکه HighAvaiability دارد.

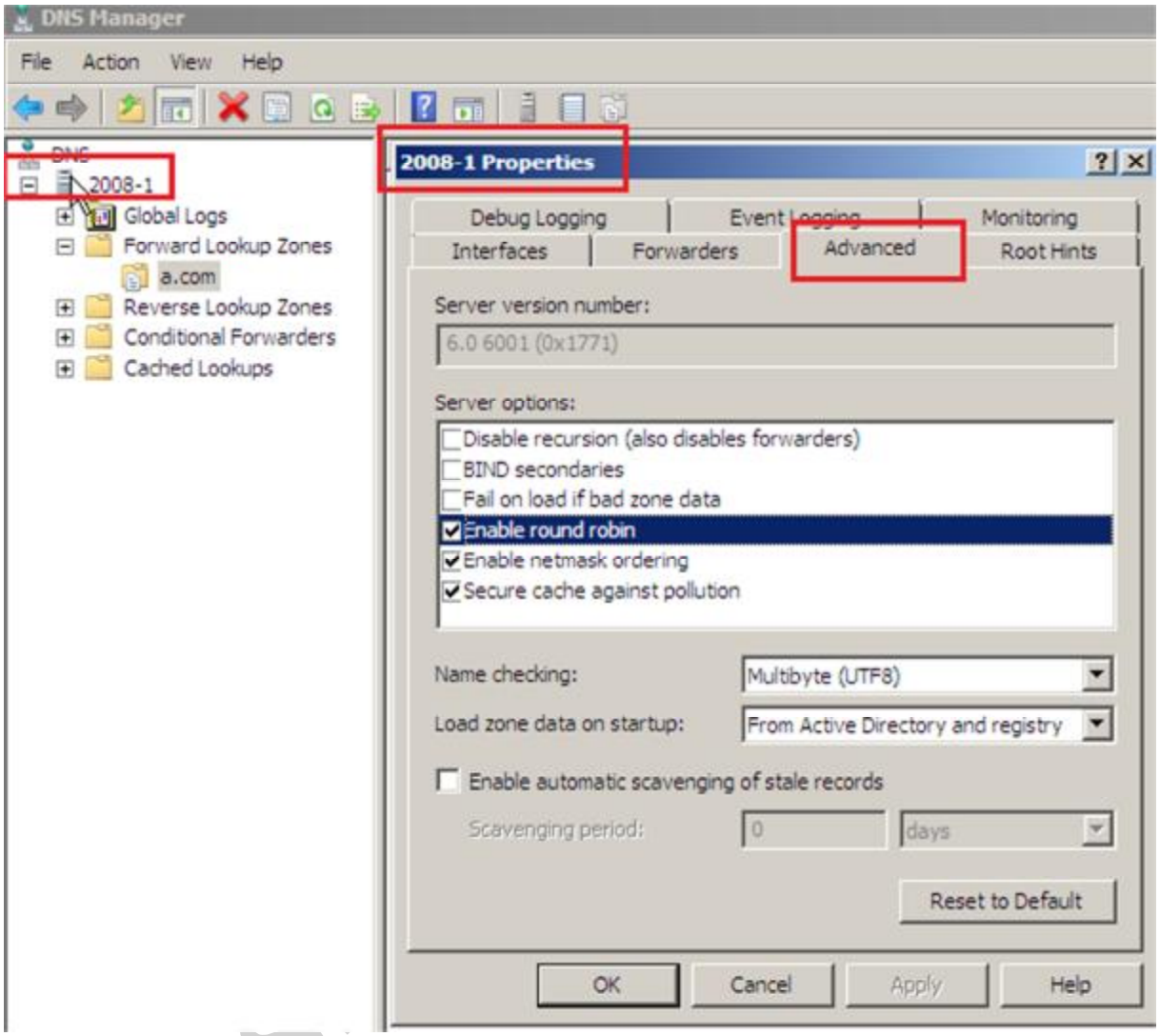
DNS RoundRabin

برای توضیح این ویژگی دو سرور را در نظر بگیرید بر روی هر دو سرور یک سایت با نام یکسان ولی با Ip های متفاوت بوجود می آوریم و یک DNS را در شبکه می آوریم و در زون آن اسامی سایت ها (a.com )و Ip های دو سرور را وارد می کنیم این کار باعث می شود که هر گاه کلاینتی اسم سایت موردنظر را وارد کرد به صورت چرخشی به یکی از دو سرور ما وصل شود, این کار( DNS RoundRabin ) باعث ایجاد Loadbalancing در شبکه می شود این یک ویژگی در DNS می باشد,یکی از معایب این روش این است که توانایی تشخیص خرابی سرورها را ندارد یعنی درخواست کلاینتها را باز به سمت سرور معیوب ارسال می کند,دیگر عیب این روش این است که نمی تواند Weight را تشخیص دهد منظور از Weight در اینجا این می باشد که فرض کنید یک سرور با قدرت بازدهی بالا و یک سرور با قدرت بازدهی کمتر داریم,RoundRabin نمی تواندتفاوت بین قدرت این دو سرور را تشخیص دهد و به یک میزان ترافیک به سمت آنها ارسال می کند,زمانی که کلاینتی به یکی از سرورها وصل می شود تا مدت یک ساعت جواب درخواستی را که از سرور کرده در خود نگه می دارد( Cache ) و در این یک ساعت اگر همان سوال را بپرسد به همان سرور وصل می شود این ویژگی با Loadbalancing مغایرت دارد.

برای پیاده سازی مانند زیر عمل می کنیم ابتدا یک زون به نام a.com می سازیم سپس 2 ,A RECORD با یک نام(www) و با Ip های متغیر می سازیم.



سپس می بینید که این ویژگی به صورت اتوماتیک در DNS فعال می باشد.




ویژگی Netmask ordering ؛ این ویژگی این امکان را می دهد که در DNS یک زون با 2 یا چند Ip متفاوت بسازیم و زمانی که کلاینت آن زون(سایت) را فرا می خواند,Ip, DNS آن کلاینت را تشخیص داده و نزدیکترین زون از نظر رنج Ip را به آن نشان می دهد,زمانی که ما به سایت مایکروسافت وصل می شویم,مستقیم به خود سایت در آمریکا وصل نمی شویم بلکه به سایت آن در آسیا وصل می شویم.

Iars

## NLB Cluster(Network Load Balancing )

**در این حالت درخواست کلاینت ها به سمت یک سرور مجازی که دارای VIP (Virtual IP) ارسال می گردد یعنی از نظر کلاینت ها تمامی سرورهای ما با یک Ip قابل دسترسی می باشند,یعنی پشت یک سرور مجازی چندین سرور واقعی فعالند.**

- **این سرور هم IP و هم MAC مجازی دارد.**

### پیاده سازی NLB Cluster

**برای پیاده سازی این سرور حداقل نیاز به 2 کارت شبکه داریم,از این 2 کارت شبکه یکی برای ارسال درخواست کلاینت ها به سمت سرور است و دیگری برای اینکه سرورها بتوانند از وضعیت هم مطلع باشند.**

- **برای اینکه به سرورهایمان فشار اضافی وارد نشود باید با یک Hub کارت شبکه هایمان را وصل کنیم چون زمانی که سروری پیغامی را به بقیه سرورها می خواهد برساند باید چندین بار تکرار کند,با وجود Hub یکبار به آن می گوید و Hub به بقیه سرورها انتقال می دهد.**
- **برای اینکه سرورها بتوانند با اسم یکدیگر را Ping کنند بهتر است وارد فایل Host آنها شویم و Ip بقیه سروها را در آن ها وارد کنیم مانند: 192.168.6.1 srv1 srv1.hani .com(حتی با داشتن DNS )**
- **برای راه اندازی NLB احتیاج به شبکه دامینی نداریم.(Optional )**
- **به سرورهایی که در NLB با هم تشکیل سرور مجازی را می دهند,در اصطلاح به آنها HOST می گویند.**
- **قبل از نصب NLB باید سرویس مورد نظر روی سرورها نصب شده باشد سپس آنها را کلاستر کنیم (مانند VPN )**
- **ماکزیمم می توان 32 سرور را با هم کلاستر کرد.**

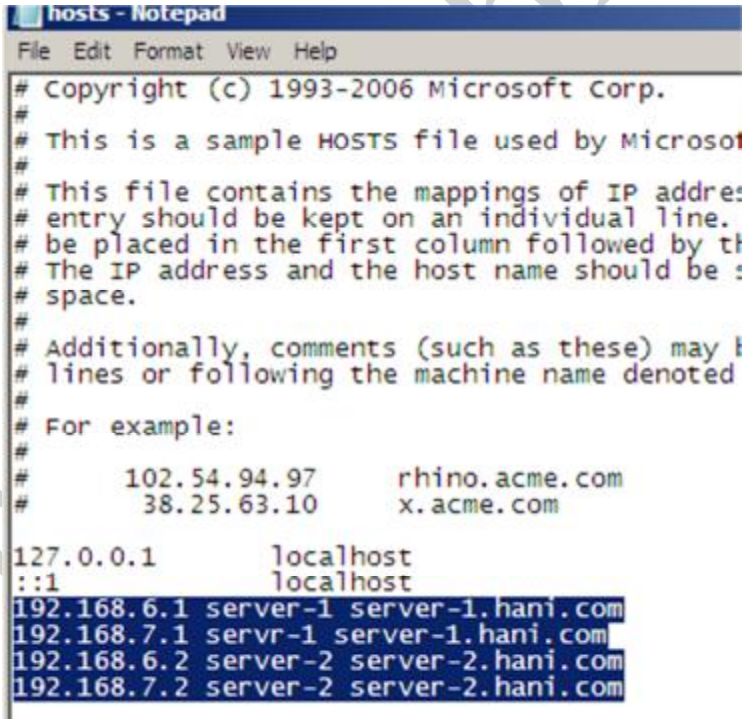
**برای راه اندازی NLB ابتدا 2 Host را مانند شکل زیر طراحی می کنیم**

Server-1

FarshidAjabnoush

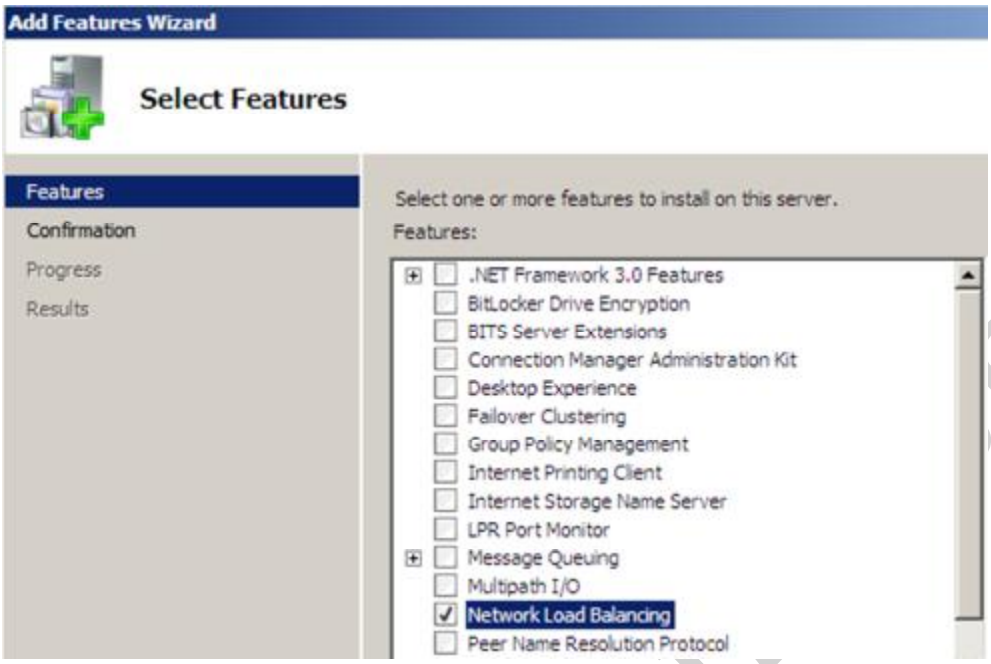
Server-2

سپس باید در فایل Host هر Host 2 مانند زیر عمل کنیم

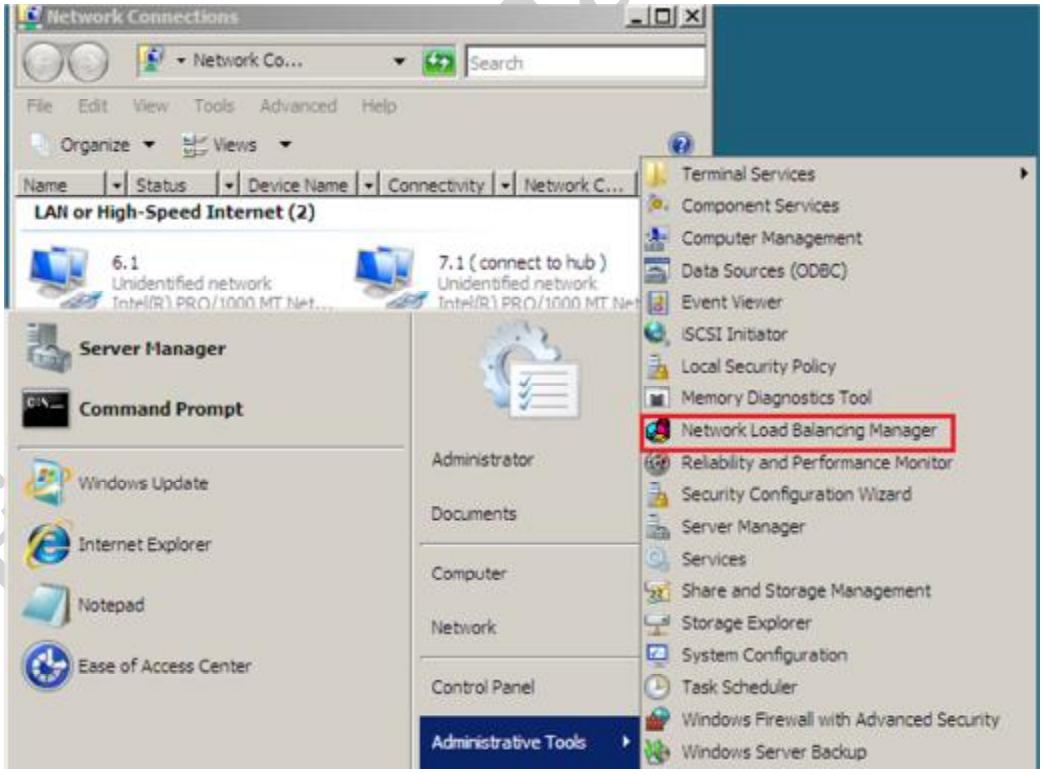


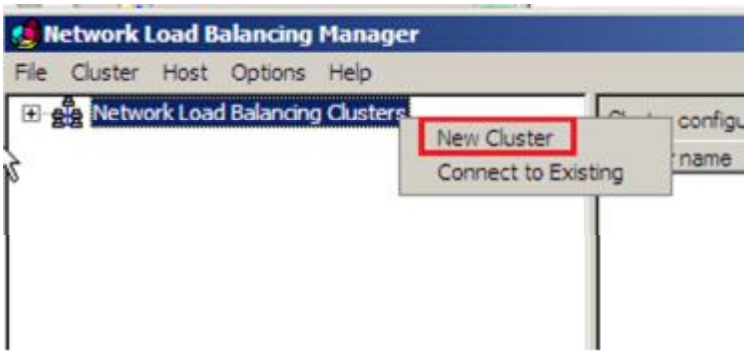

سپس باید بر روی هر Host 2 سرویس Network Load Balancing را نصب کنیم.

- در 2003 این سرویس نصب می باشد.

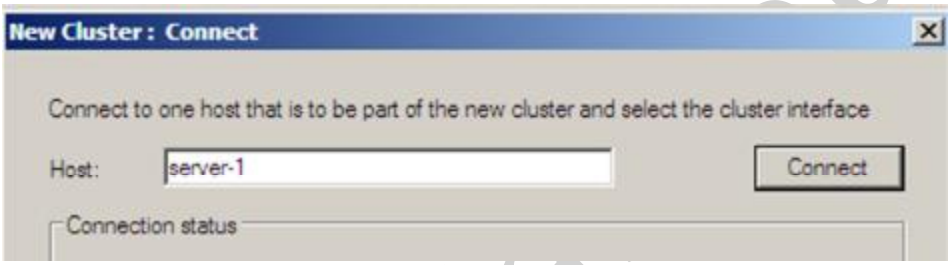



سپس باید وارد کنسول Netwok Load Balancing یکی از Host ها بشویم

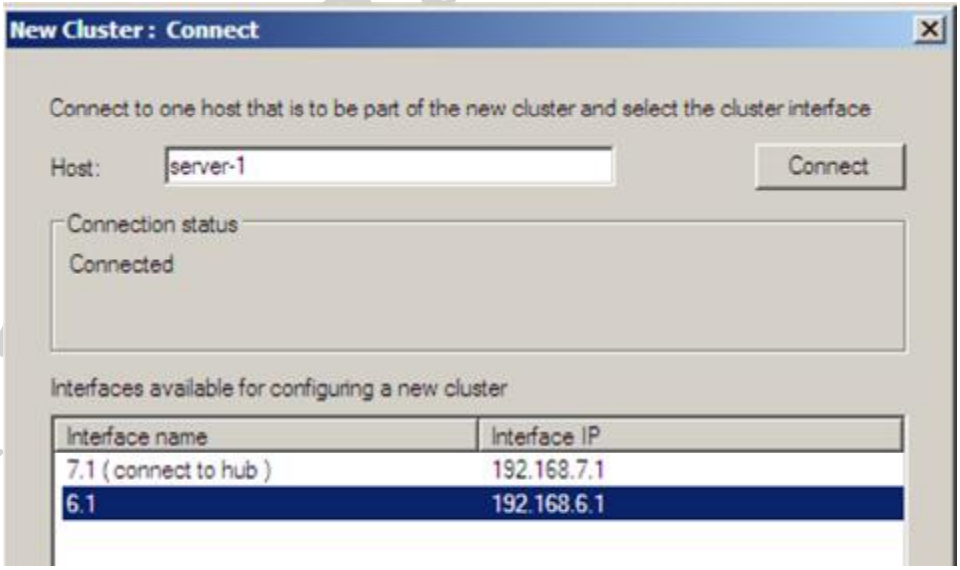




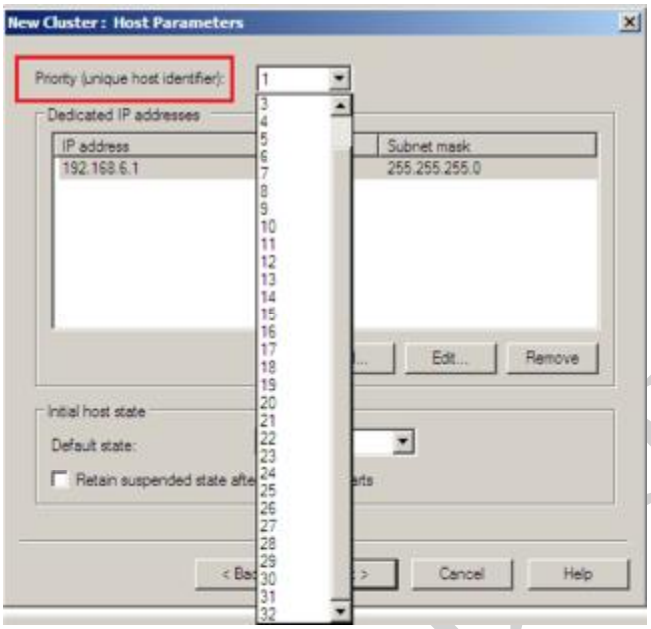

سپس باید یکبار باید اسم خودمان (Server-1) و اسم Host دوم را اضافه کنیم

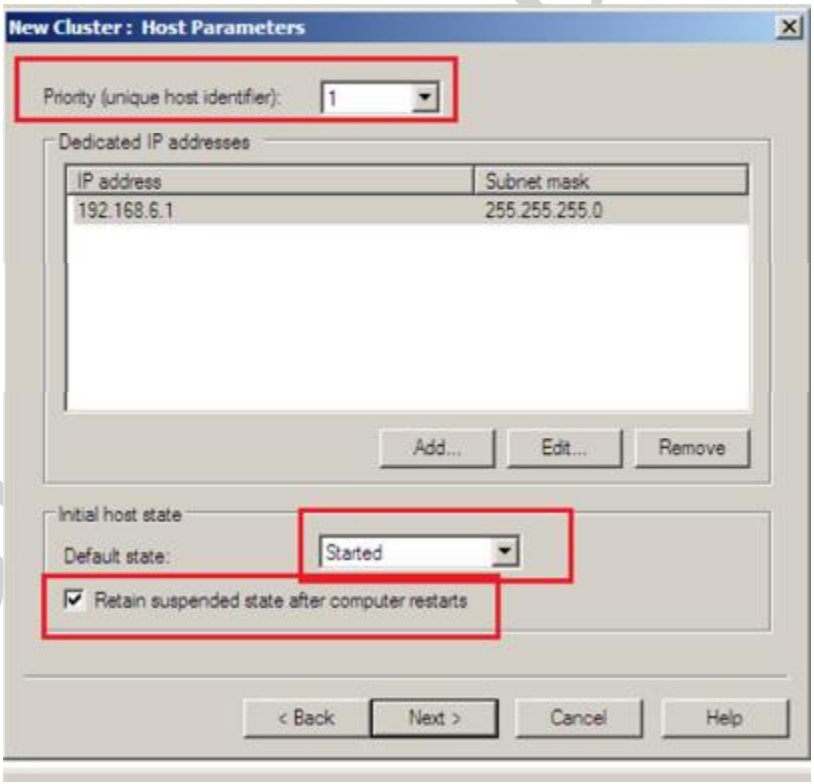



در اینجا باید کارت شبکه ای را که با آن به کلاینت ها وصل می شویم را مشخص کنیم (6.1)



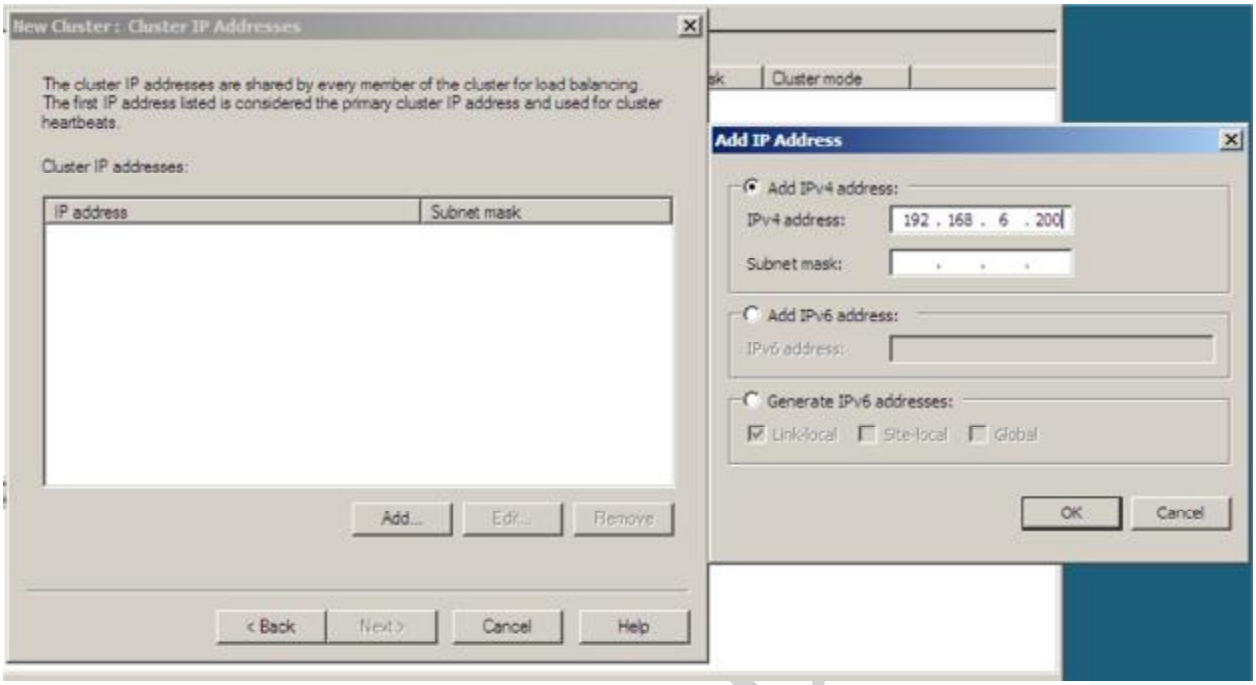
در مرحله بعد Identifire آن سرور را تعیین می کنیم,بیشتر از 32 نمی توانیم,هرچه این مقدار پایین تر باشد اولویت آن Host بالاتر می باشد.



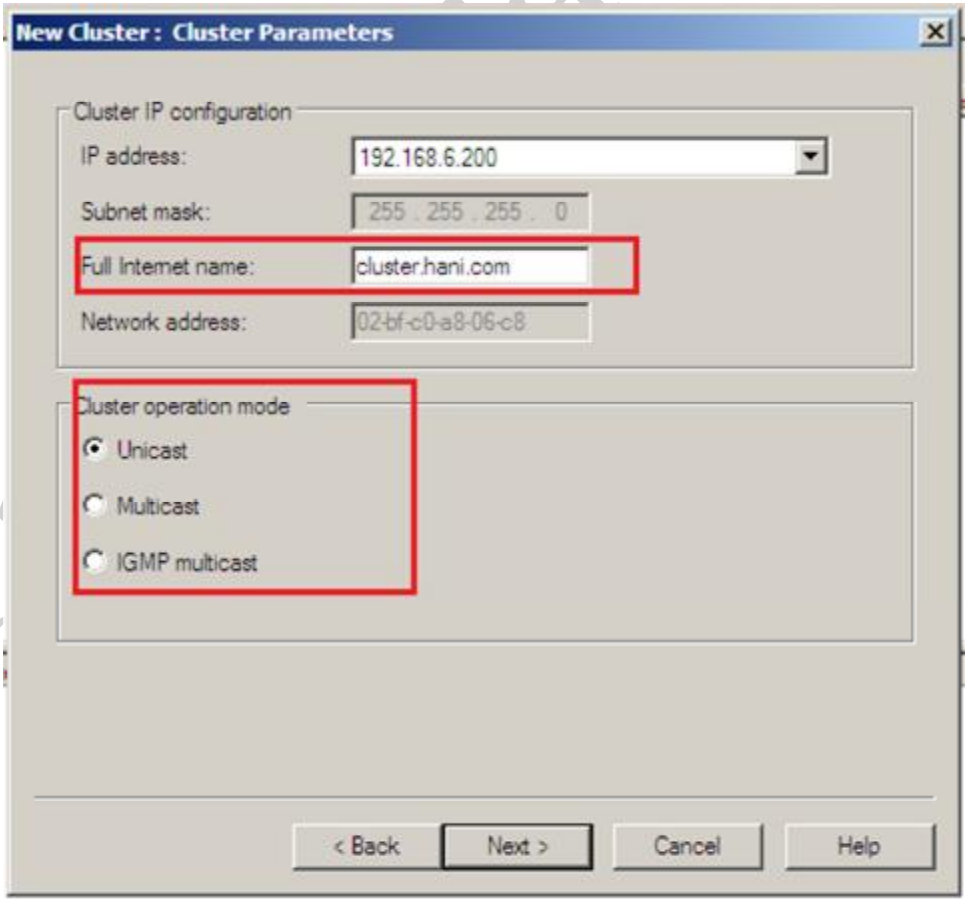




با فعال بودن گزینه ...Retain اگر سرور به طور ناگهانی ریستارت شود پس از بالا آمدن ویندوز ادامه کار سیستم میسر نیست,این گزینه باید فعال باشد تا ما متوجه مشکل سرور بشویم و آن را برطرف کنیم.

در اینجا نوبت به تنظیم کردن ip مجازی می رسد



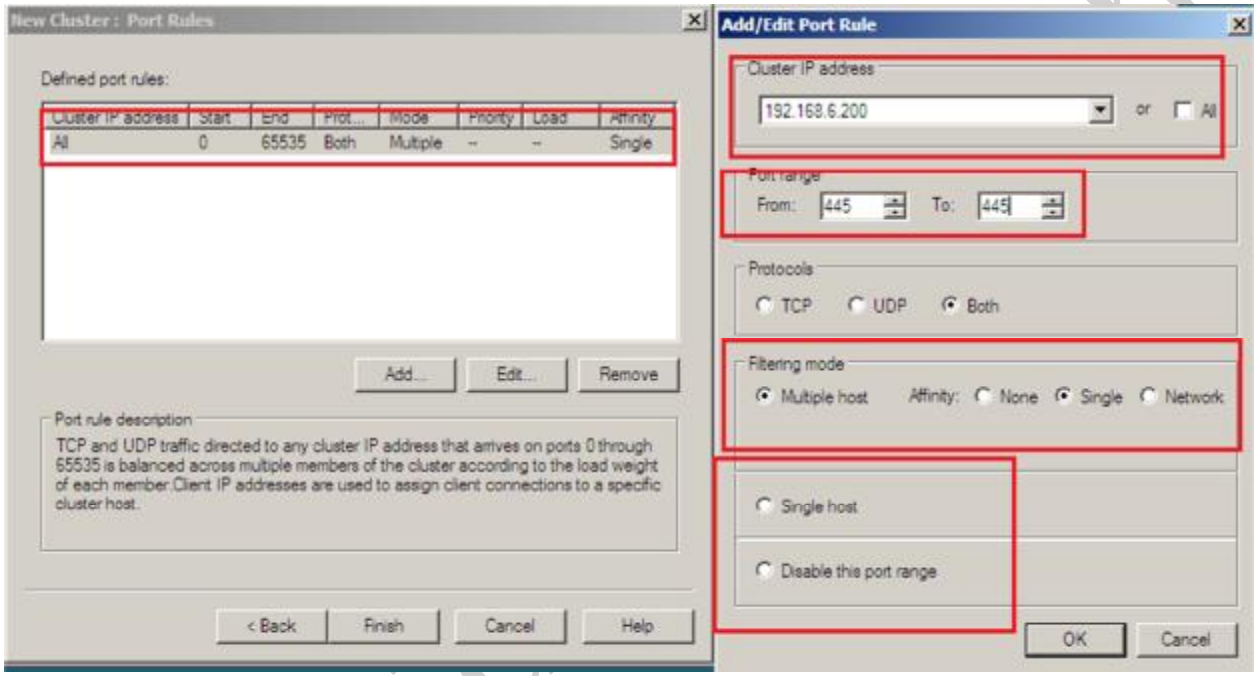

در اینجا نوبت به دادن اسم برای سرور مجازی می باشد



در قسمت دوم اگر بر روی Unicast باشد Network address وIp این سرور مجازی را برای سرور اصلی تنظیم می کند و اگر Multicast فعال باشد در کنار Ip وMac اصلی خود سرور این Ip و Mac مجازی را هم تنظیم می کند,بهترین گزینه Unicast می باشد (به دلیل امنیت).

- در این سناریو ما Multicast را انتخاب می کنیم.

در مرحله بعد مشخص می کنیم که چه ترافیکی (از چه پورتی) به سمت این سرور مجازی می آید بین سرورهای اصلی پخش شود.




به صورت پیش فرض تمامی ترافیک ها و تمامی پورتها (65535 عدد پورت) فعال می باشد برای اینکه ترافیک ها و پورت ها را کنترل کنیم Edit را می زنیم در قسمت Filtering mode ,دو حالت Multiple Host=ActiveActive و Single host=Active standby وجود دارد.

Multiple Host: دو سرور با هم فعال هستند و به محض اینکه یکی از آنها از کار بیفتد دیگری کار آن را هم به عهده می گیرد.

Single host: در این حالت فقط یک سرور فعال است و به محض اینکه مشکلی پیش آید سرور بعدی فعال می شود و کار آن سرور را انجام می دهد.

- اگر سرورهایمان قوی هستند بهترین حالت,حالت اول می باشد ولی اگر سرورهایمان قوی نیست حالت دوم را انتخاب می کنیم.
- در این سناریو ترافیک Share (445) را باز می کنیم.

در قسمت Affinity سه حالت داریم

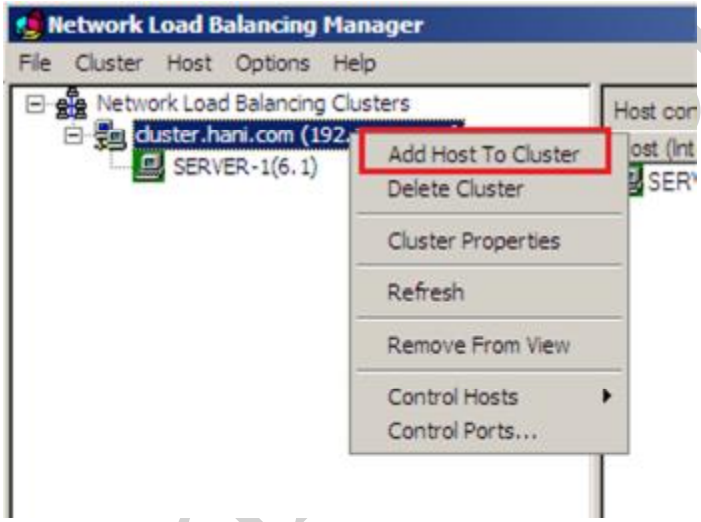
None :در این حالت زمانی که یک ترافیک به سمت سرورهایمان می آید بین آنها پخش می شود ( مانند سلام که سل به یک سرور و ام به سرور دیگر می رسد)این حالت گزینه مناسبی نیست.

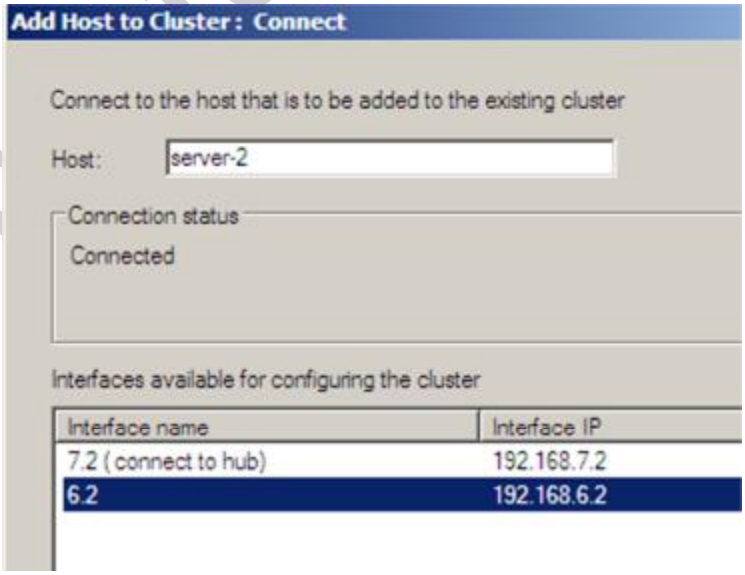
Single : در این حالت تا زمانی که کامپیوتری با ما Session دارد تمامی ترافیک های آن به سمت یک سرور می رود.

Network : در این حالت تا زمانی که شبکه ای با ما Session دارد تمامی ترافیک های آن به سمت یک سرور می رود.

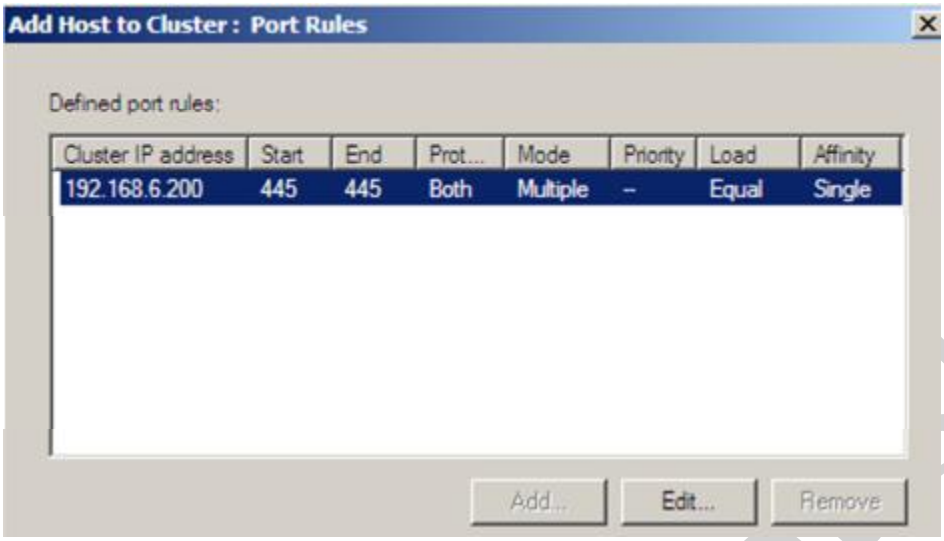
- سپس Ping ,6.200 را می گیریم.

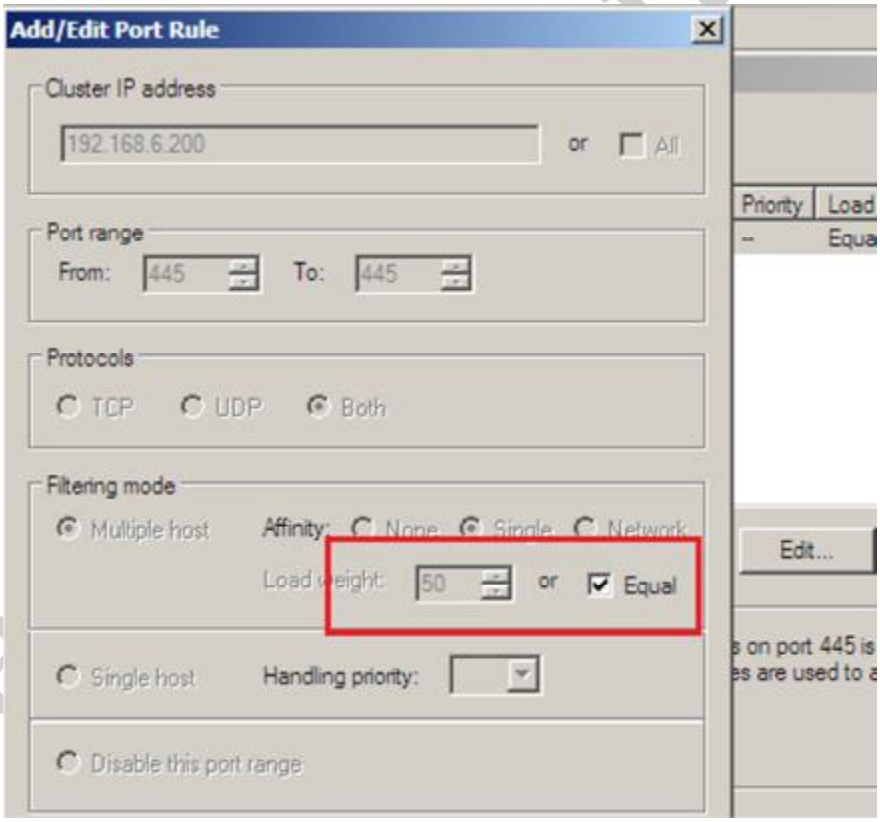
حالا نوبت اضافه کردن Host به Cluster می باشد




Farnia Rush

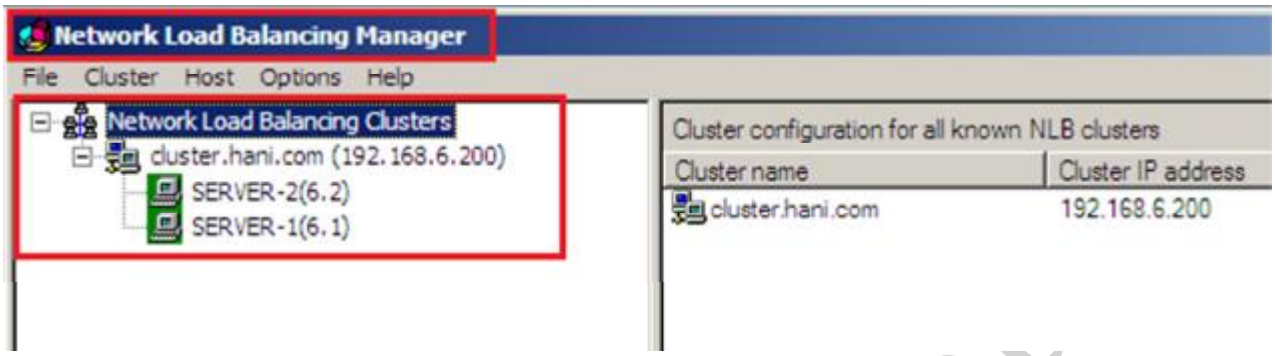



- با فعال بودن Equal ترافیک بین سرورها پخش می شود.

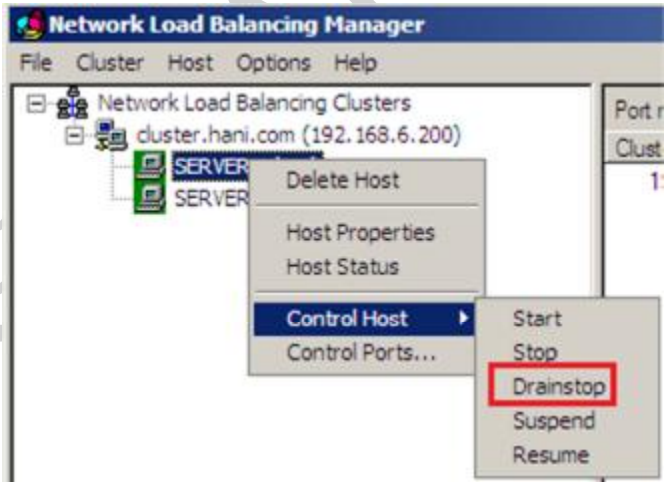
و درنهایت Finish .

برای کلاستر کردن فقط کافی است بر روی یک سرور تنظیمات (تنظیمات بالا) را انجام دهیم و در بقیه سرورها با باز کردن کنسول مربوطه تنظیمات به صورت اتوماتیک اعمال می گردد.




کنسول سرور2

- Drain Stop یعنی به شرط Start بودن,آن را Stop کن.




- NLB Cluster برای شبکه های کوچک استفاده می شود,در شبکه های بزرگ از Fail Over Cluster استفاده می شود.

تفاوت میان Fail Over Cluster وNLB Cluster

در این دو روش از تعدادی سرور حقیقی که تشکیل یک سرور مجازی را داده اند استفاده می شود با این تفاوت که در NLB Cluster زمانی که کلاینتی به سرور مجازی وصل می شود و اطلاعاتی را در آن ذخیره می کند,آن اطلاعات بر روی هارد یکی از سرورهای حقیقی ذخیره می شود در صورت ازکار افتادن آن سرور حقیقی, دیگر دسترسی به آن اطلاعات میسر نمی باشد ولی در Fail Over Cluster سروهای حقیقی اطلاعات را بر روی منابع ذخیره سازی مجزایی مانند SAN Storage ها ذخیره می کنند,این کار باعث می شود که همیشه اطلاعات در دسترس باشد حتی با از کار افتادن سرور حقیقی.

Failover Cluster

همان NLB می باشد با این تفاوت که 1) در NLB اطلاعات کلاینت ها در هارد سرورها ذخیره می شود ولی در Failover اطلاعات کلاینت ها بر روی منابع ذخیره سازی ( SAN ) ذخیره می شوند. 2) Failover فقط در شبکه های دامینی قابل پیاده سازی است,NLB را می توان در شبکه های Workgroupهم پیاده سازی کرد.

آشنایی و پیاده سازی شبکه های SAN

به Component های تشکیل دهنده شبکه های SAN , SAN FABRIC گویند که بر 2 نوع هستند: ISCSI و FC این دو کامپوننت هم پروتکل هستند و هم قطعه سخت افزاری.

FIBER CHANNEL =FC ,Internet Small Computer System Interface=ISCSI

منابع ذخیره سازی اطلاعات (SAN), تشکیل شده است از تعدادی از هاردهای SCSIیاSAS ,در این نوع از هاردها اطلاعات به صورت بلوک به بلوک (Block ) ذخیره می شود,زمانی که اطلاعات از طریق کابل شبکه برای SAN ارسال می شود این اطلاعات به صورت بیت به بیت می باشد وبرای ذخیره شدن بر روی SAN باید به بلوک تبدیل شوند, این کار باید قبل از وارد شدن به SAN انجام شود,در نتیجه در ورودی SAN ها,Device به نام ISCSI HBA و یا FC HBA وجود دارد که این تبدیل را انجام می دهد(Hub Bus Adapter ).

- 35 bit تقریبا برابر است با 1 Block

تفاوت بین ISCSI و FC

1) ISCSI ,بدون تغییر در ساختار شبکه داخلی قابل پیاده سازی می باشد ولی برای استفاده از FCشبکه حتما باید فیبر نوری باشد(ISCSI مقرون به صرفه می باشد)
2) سرعت ISCSI به دلیل استفاده از تجهیزات شبکه های داخلی (LAN) از FC که با فیبر کار می کند پایین تر می باشد.

FC= 4 GB minimum, ISCSI=100 MB

- البته برای برطرف کردن مشکل ISCSI می توان از Giga Ethernet switch استفاده کرد که حداقل سرعت آن 1 GB می باشد.



FarshidAjabnoush

3) زمانی که از ISCSI استفاده می کنیم می توانیم از پروتکل های Chap و Ipsec برای ایجاد امنیت بر روی ترافیک شبکه استفاده کنیم,تنها روش ایجاد امنیت در زمان استفاده از FC بکار بردن Restriction On Physical Access می باشد.

- برای شبکه های معمولی ISCSI مناسب می باشد و برای شبکه های FC,Enterprise .
- به علت گران بودن سخت افزارهای SAN , در شبکه های معمولی SAN را Emulate می کنند.
- Emulate را با یک مثال توضیح می دهیم, زمانی که از Vmware استفاده می کنیم و در آن یک ویندوز نصب می کنیم در حقیقت Emulate کرده ایم, ویندوز را در جایی دیگر,به غیر از کامپیوتر خودمان نصب کرده ایم.
- نرم افزاری که برای Emulate کردن شبکه های SAN بکار می رود Star Wind می باشد(Microsoft)
- نرم افزاری که برای Emulate کردن شبکه های SANدر ESXبکار می رود, OpenFiler می باشد( Open Source Storage Management Appliance).
- OpenFiler در حقیقت یک سیستم عامل می باشد ولی Star Wind یک نرم افزار است.

آشنایی با برخی از اصطلاحات قبل از Emulate کردنSAN

TARGET : به هرکدام از هاردهای موجود در شبکه های Target,SAN گویند.

LUN : به هر کدام از پارتیشن های ساخته شده در Taget هاLUN, (Logical Unit Number ) گویند.

INITIATOR : به هر کدام از سرورهای کلاستر شده که اطلاعات را داخل Target ها می ریزند,Initiator گویند.

VDS: یک API ویندوز می باشد که Target های داخل SAN را طوری بر روی INITIATOR ها نشان می دهد که به نظر می رسد Target ها به صورت فیزیکی پشت سرور قرار دارند,یعنی فاصله فیزیکی که بین Target ها و Initiator ها وجود دارد حس نمی شود, (Virtual Disk Service).

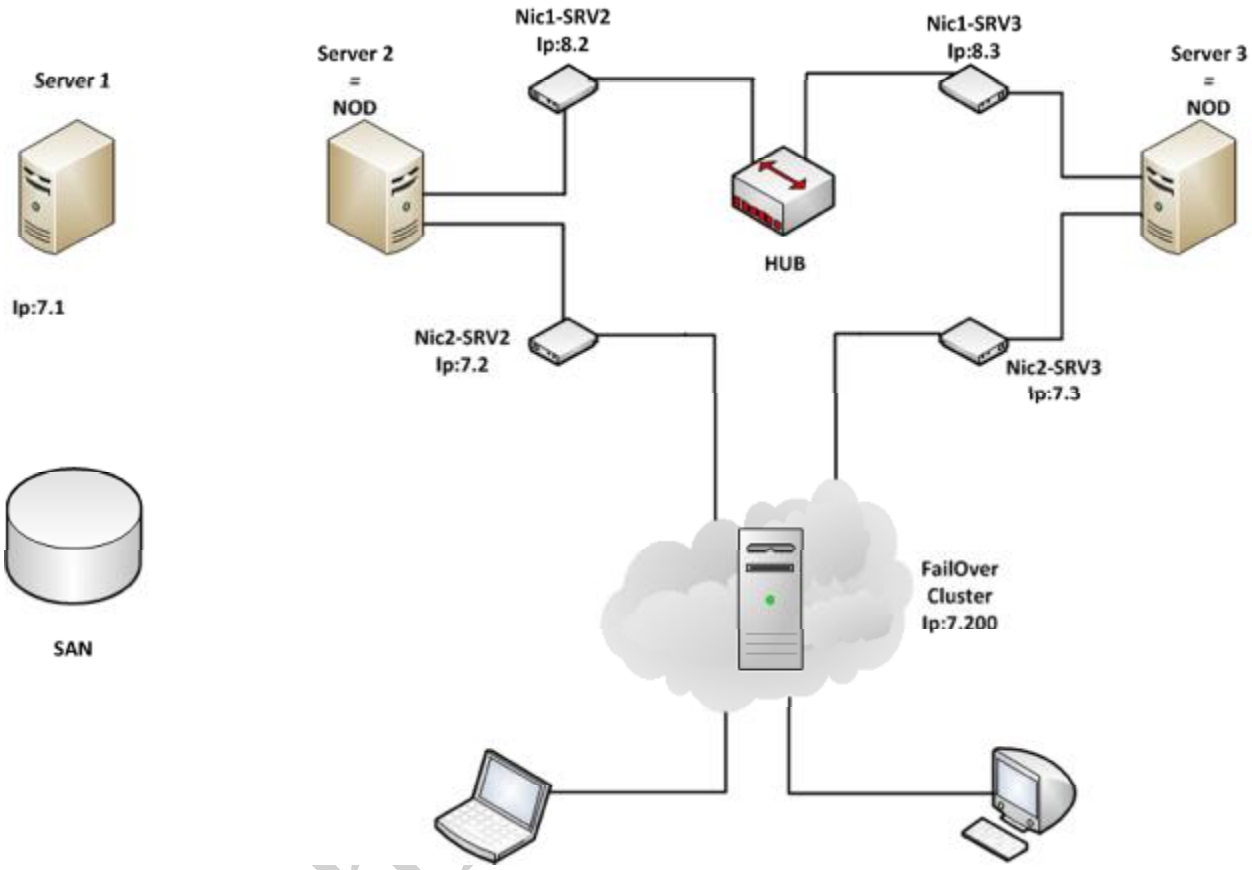
- API ( Application programming interface ): زمانی که کاربر می خواهد با سخت افزار ارتباط برقرار کند ابتدا دستوراتش به Shell و از Shell به Kernel می رسد و Kernel هم برای برقراری ارتباط با سخت افزار از یک سری توابع استفاده می کند,به یک سری از توابع خاص Kernel که کاربر برای استفاده و تغییر به آنها دسترسی دارد را API گویند.

MPIO : یک رابطبین INITIATOR ها وTaget ها هستند,کار اصلی آن برقراری چندین مسیر ارتباطی بین INITIATOR ها وTaget ها است که در صورت قطع شدن یک مسیر ارتباطی,از مسیر دیگری استفاده شود( Multipath Input/Output ).

ISNS : سرویسی می باشد که Target های داخل SAN را برای INITIATOR ها Discover می کند(تعداد هاردهای موجود درSANرا به INITIATOR ها نشان می دهد),( Internet Storage Name Service).

FarshidAjabnoush

پیاده سازی FailOver Cluster




در این سناریو بر روی سرور1 Active Directory نصب می باشد,برروی هرکدام ازسرور 2 و3 ,2عدد کارت شبکه داریم,کارت شبکه هایی که 8.2 و 8.3 هستند با Hub به هم وصل شده اند (برای اینکه از وضعیت یکدیگر با خبر باشند با Hub وصل شده اند)سرورهای 2و3,(Server1)Join To Domain می باشند سپس کارت شبکه هایی که Ip7.2 و7.3 دارند را به سرور مجازی ( 7.200 ) اتصال می دهیم,کلاینت ها برای سرویس گرفتن به 7.200 وصل می شوند.

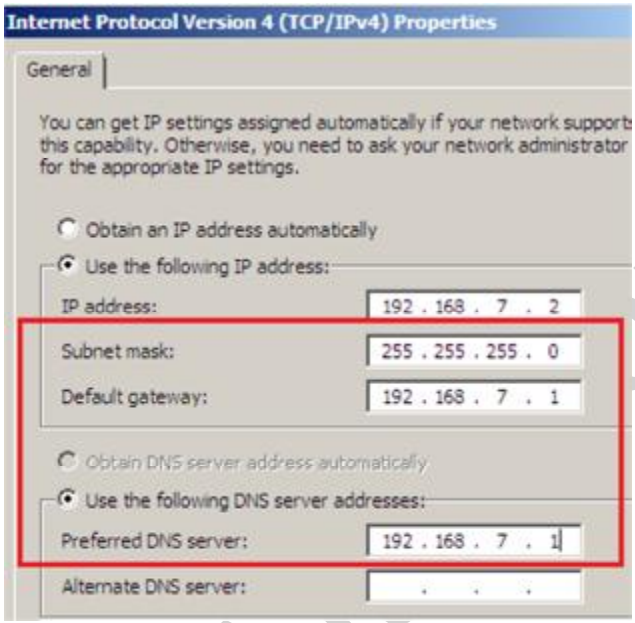
تا این مرحله NLB Cluster بود.

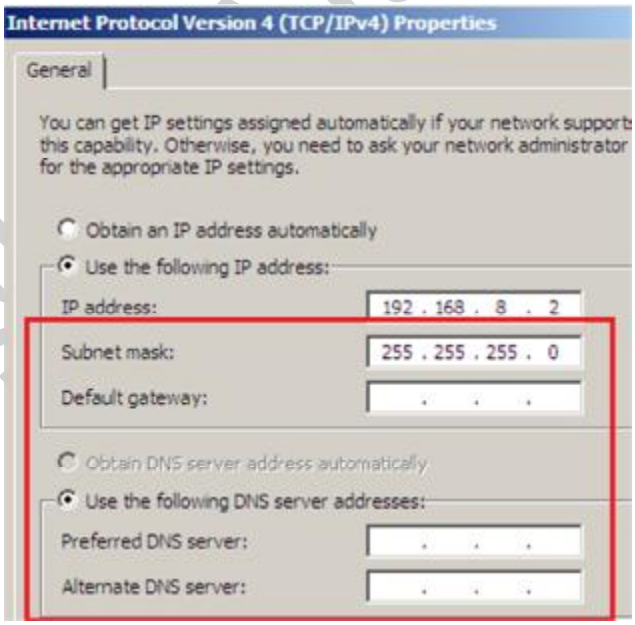
برای پیاده سازی SAN ,به دلیل کمبود امکانات بعد از اینکه کار با سرور 1 تمام شد SAN را بر روی آن سرور با همان IP تنظیم می کنیم و سرورهای 2و3 را به آن وصل می کنیم.

- در NLB به سرورهایی(2و3) که با هم تشکیل کلاستر را می دهند HOST گویند.
- در FailOver به سرورهایی(2و3) که با هم تشکیل کلاستر را می دهند NOD گویند.

- بر روی کارت شبکه هایی که به سرور مجازی متصل هستند (7.2 و7.3 ) بایدDefault Gateway و DNS تنظیم شود,در این سناریو به دلیل نداشتن اینترنت, 7.1 را تنظیم می کنیم.
- به سرور1 چند هارد باید اضافه کنیم (برای اینکه می خواهد نقش SAN را اجرا کند)

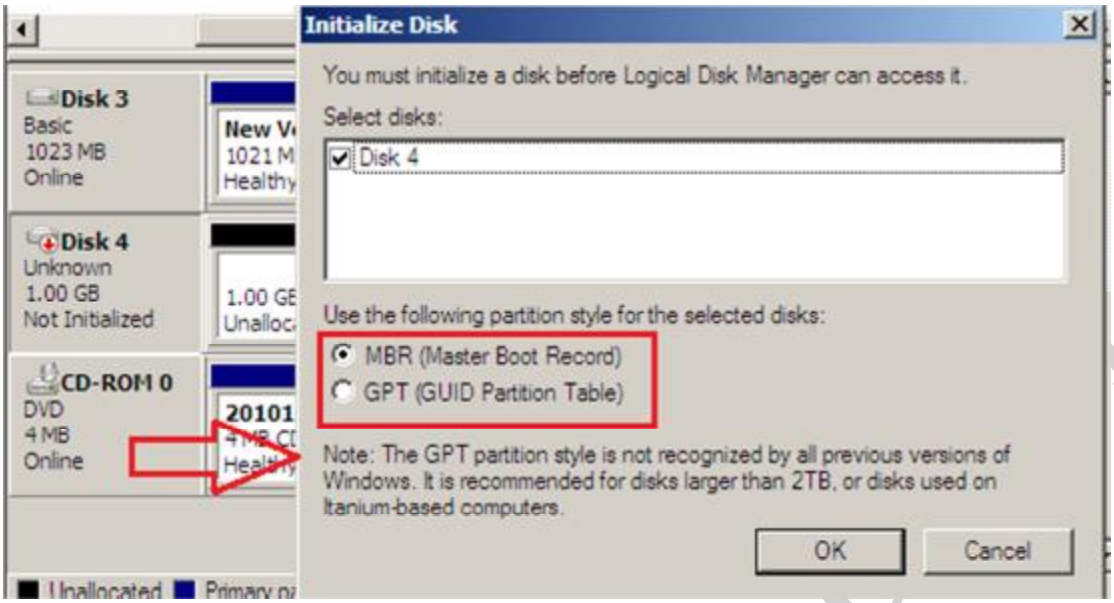
سپس IP کارت شبکه های سرورهای 2و3 را مانند زیر تنظیم می کنیم.



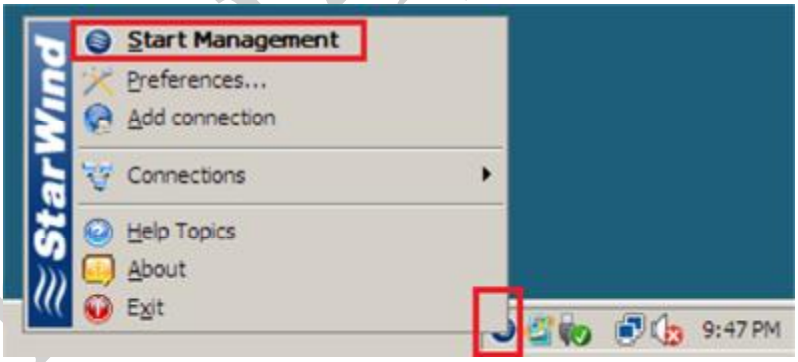

بعد از Join کردن سرورهای 2و3 نوبت به نصب Starwind بر روی سرور 1 می باشد.

- فرق بین MBR و GPT در مقدار سایز پارتیشنNTFS می باشد,با MBR حداکثر حجم یک پارتیشنTB 2 و با GPT حداکثر سایز یک پارتیشنTB 16 می باشد(Mac & Linux از GPT استفاده می کنند).

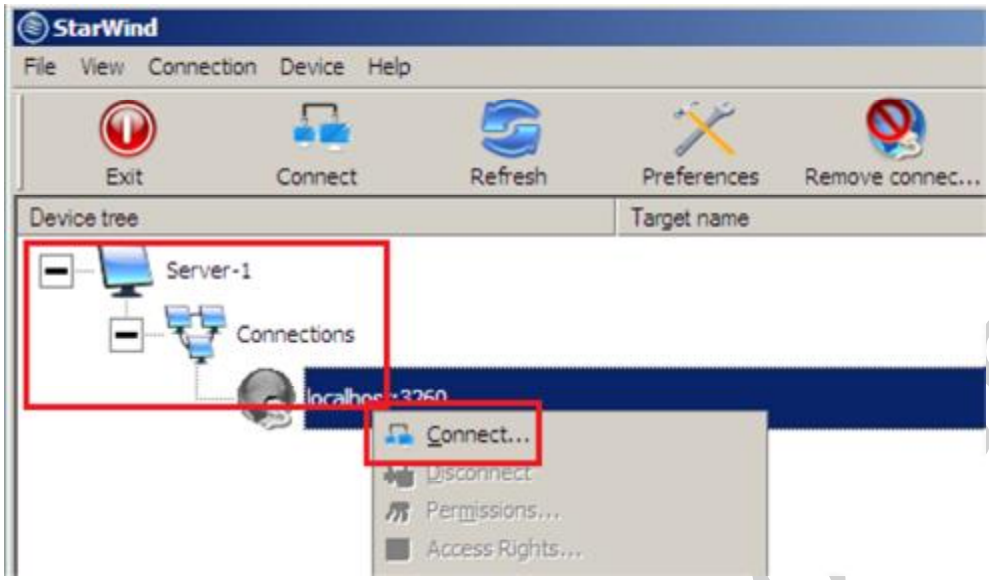



- قبل از نصب Starwind باید مطمئن شویم هاردها به سرور اضافه و فعال شده اند.
- نرم افزار شبیه ساز Starwind, SAN می باشد.

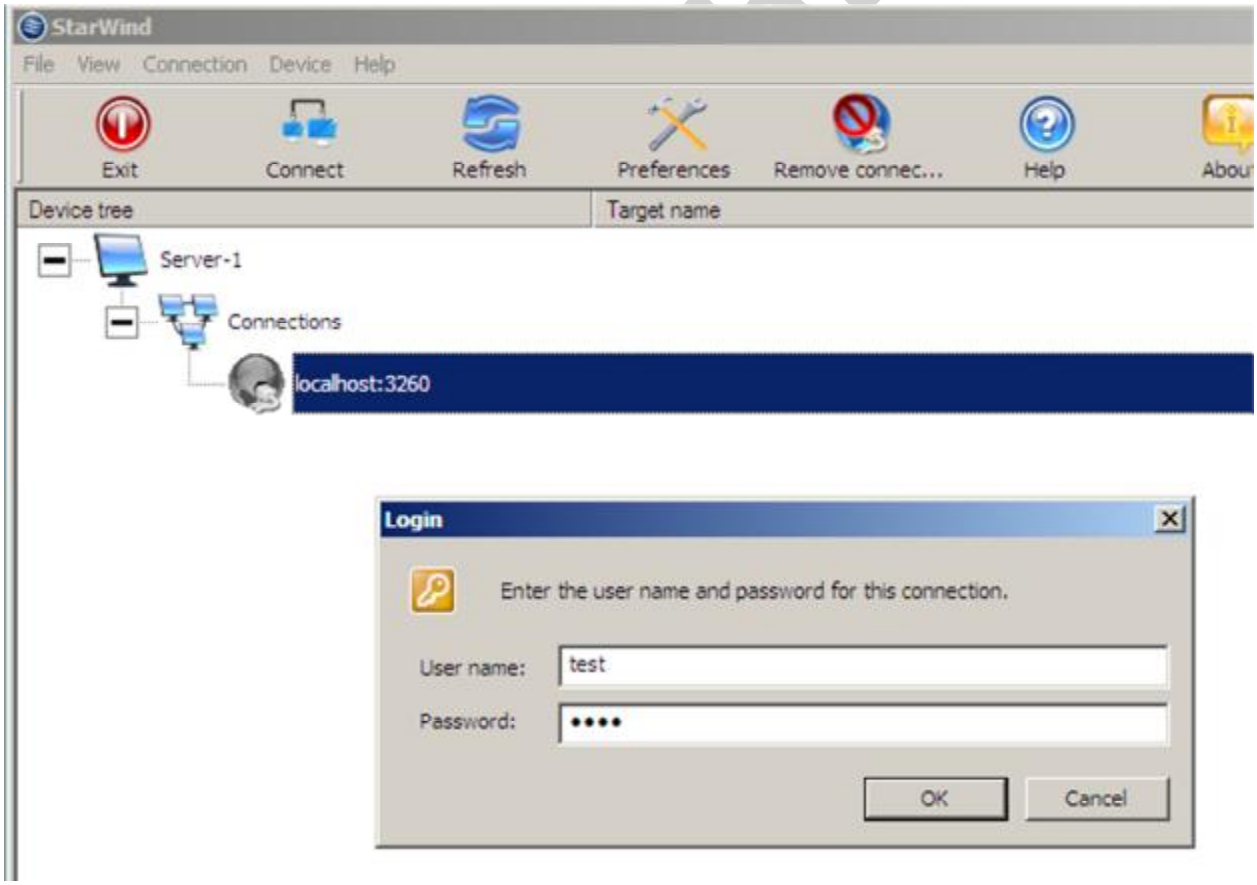
بعد از اتمام نصب مانند زیر وارد نرم افزار می شویم



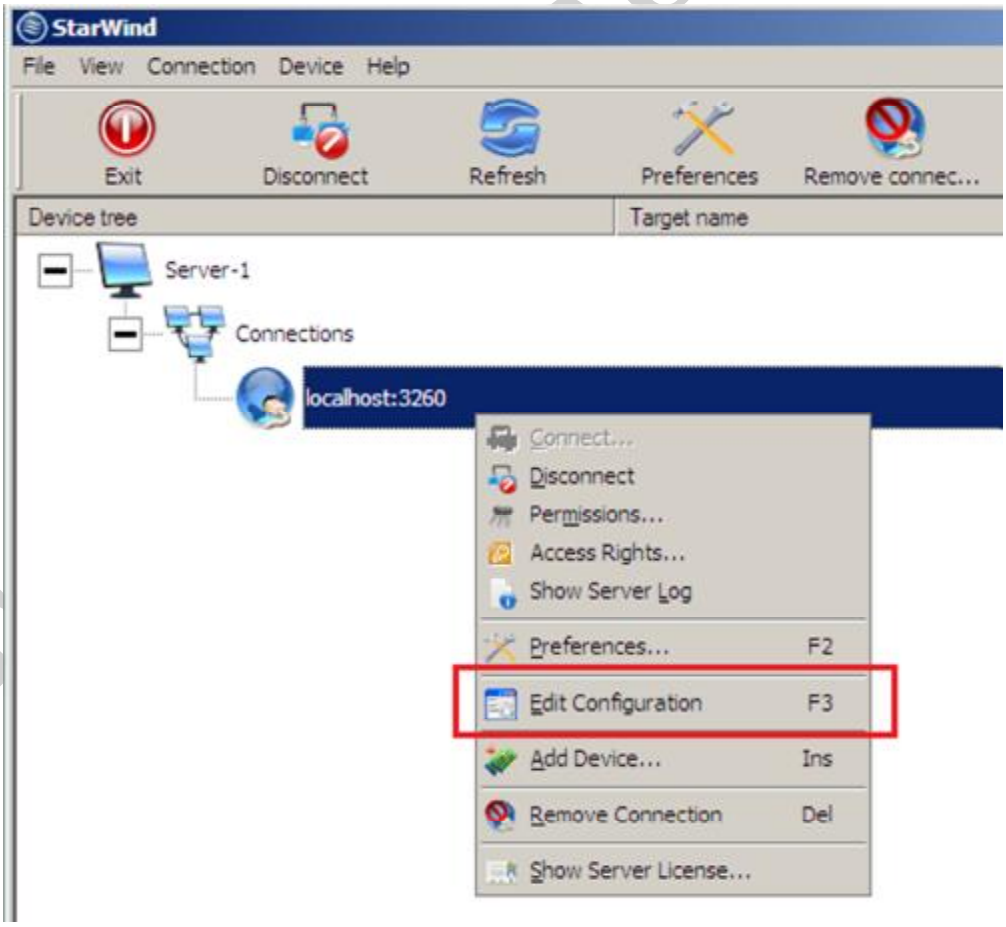

Fa Ajabn




سپس باید یوزر و پسورد پیش فرض را که test می باشد،برای وصل شدن به کنسولش وارد کنیم.

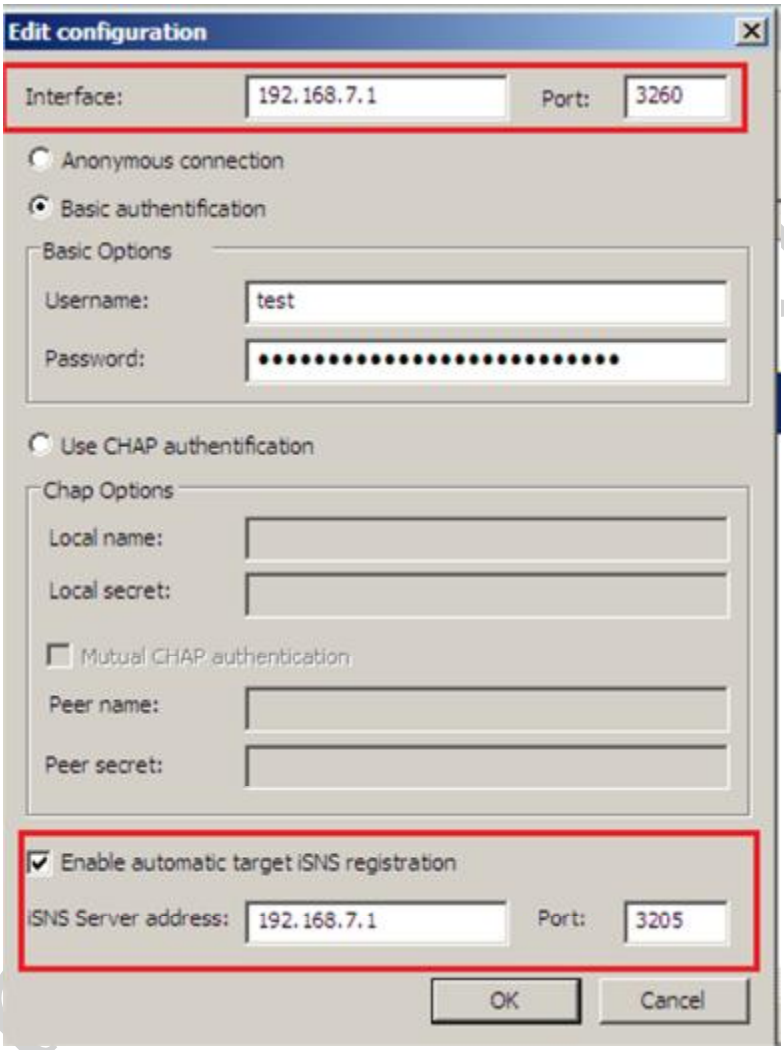


StarWind
File View Connection Device Help
Exit
Connect
Refresh
Preferences
Remove connec...
Help
About
Device tree
Type
Server-1
Service trial information
StarWind iSCSI Target v4.0 (Build 20090212, Win32)
Host address: localhost
Port: 3260
StarWind SOFTWARE
This is the trial version of the service.
Evaluation days left: 15.
More information is available at: www.starwindsoftware.com
OK
Ready


StarWind
File View Connection Device Help
Exit
Disconnect
Refresh
Preferences
Remove connec...
Device tree
Target name
Server-1
Connections
localhost:3260
Connect...
Disconnect
Permissions...
Access Rights...
Show Server Log
Preferences... F2
Edit Configuration F3
Add Device... Ins
Remove Connection Del
Show Server License...

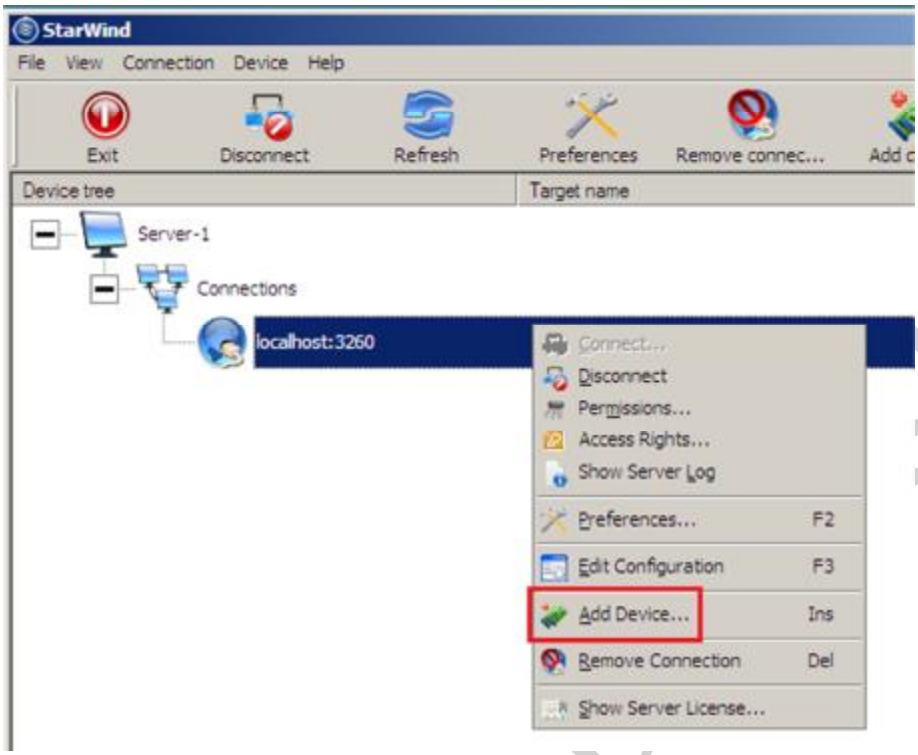
در دو قسمت مشخص شده Ip 7.1 را وارد می کنیم،در قسمت بالا به سرورها می گوییم برای برقراری ارتباط با SAN از این Ip مشخص شده استفاده کن (ورودی SAN می باشد).

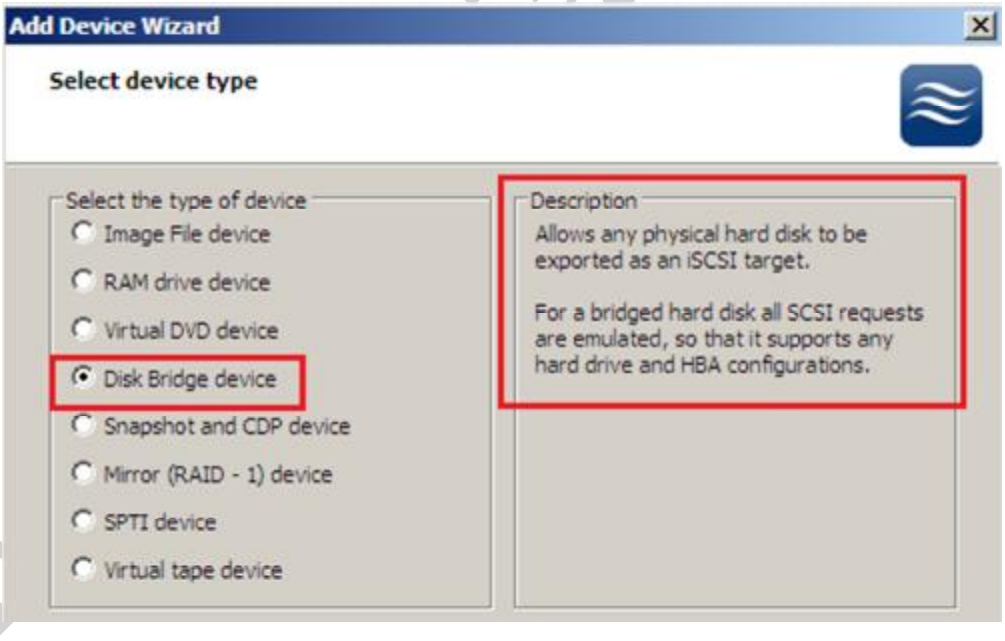
در قسمت پایین هم برای اینکه سرورها بدانند چند هارد بر روی SAN وجود دارد باز باید از این Ip که ISNS می شود بپرسند.




- بر روی سرور SAN باید وارد فایروال شویم و پورت های 3205 و 3260 را باز کنیم.

سپس نوبت به معرفی هاردها به SAN می باشد برای این کار مانند زیر عمل می کنیم

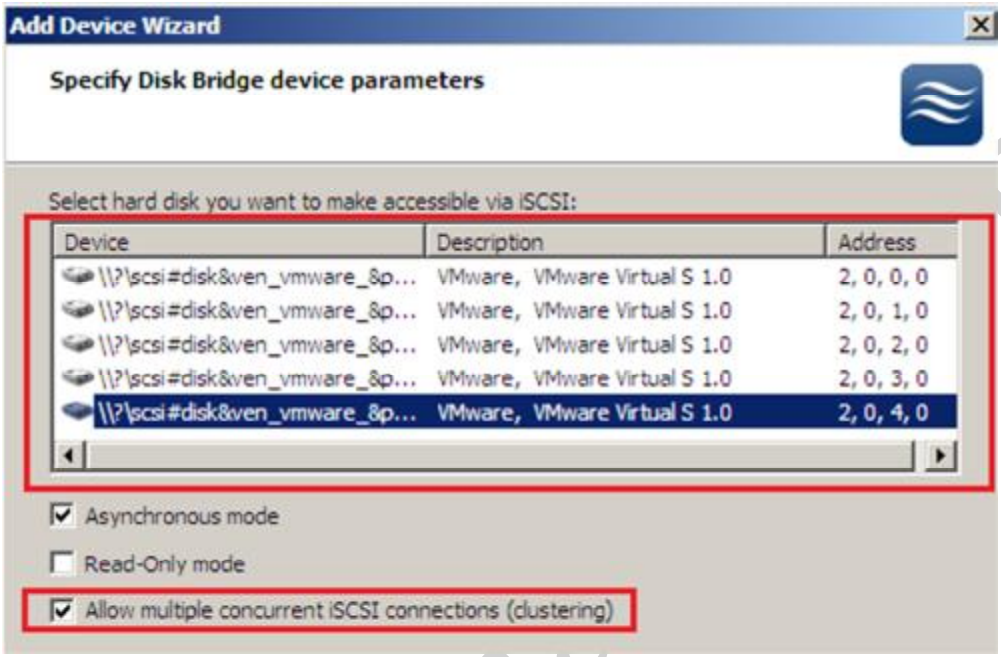



**با انتخاب گزینه بالا ..Disk , هر هارد فیزیکی که بر روی سرور داشته باشیم آن را به عنوان Iscsi Target می شناسد.**

- **هر نوع هاردی پشتیبانی می شود (SCSI, IDE,SATA و..)**

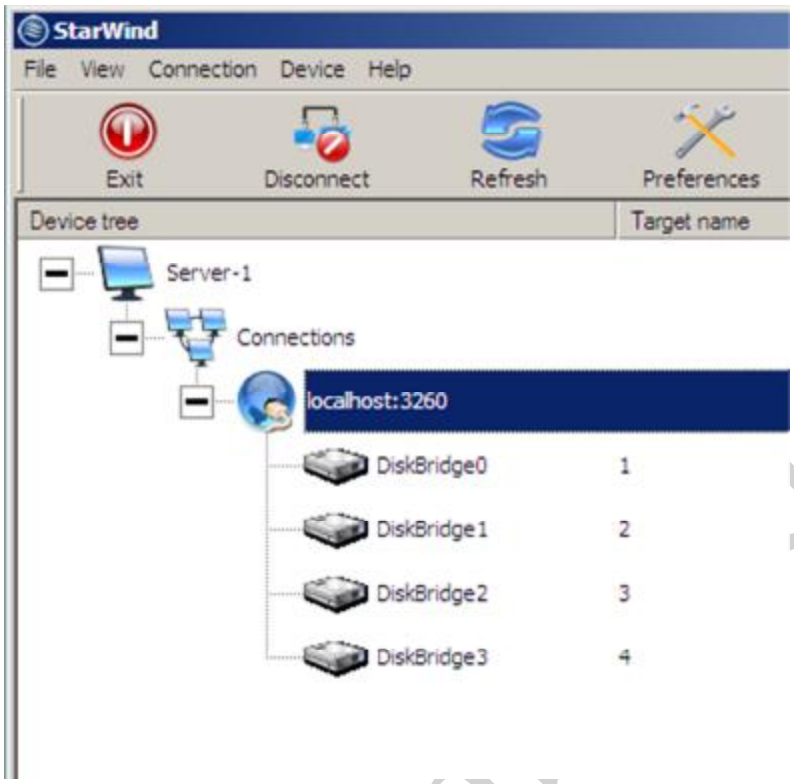
سپس نوبت به انتخاب هارد می رسد که نباید هارد اول را انتخاب کنیم چون هارد خود سیستممان می باشد در اینجا از هارد آخر شروع می کنیم,گزینه ..Allow هم باید فعال باشد چون با فعال بودن این گزینه همزمان چندین سرور می توانند از این هارد استفاده کنند.



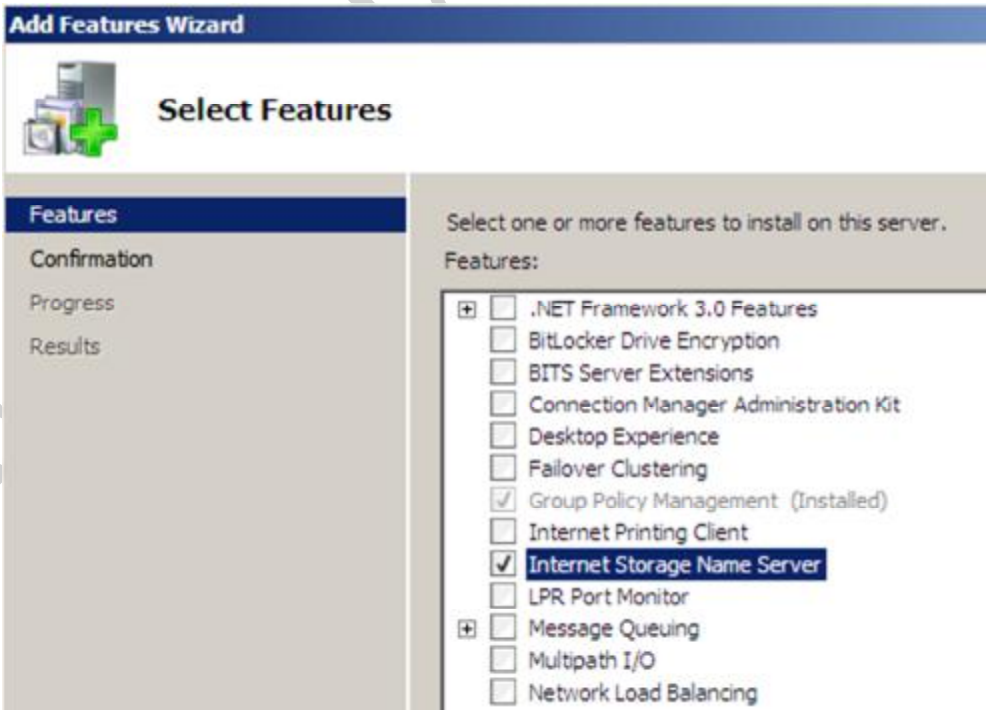

سپس اسمی برای هارد مشخص می کنیم

به ازای هر کدام از هاردهایمان بایداز مرحله Add Device دوباره شروع کنیم,در اینجا 4 هارد داریم پس 4 بار باید Add Device کنیم.

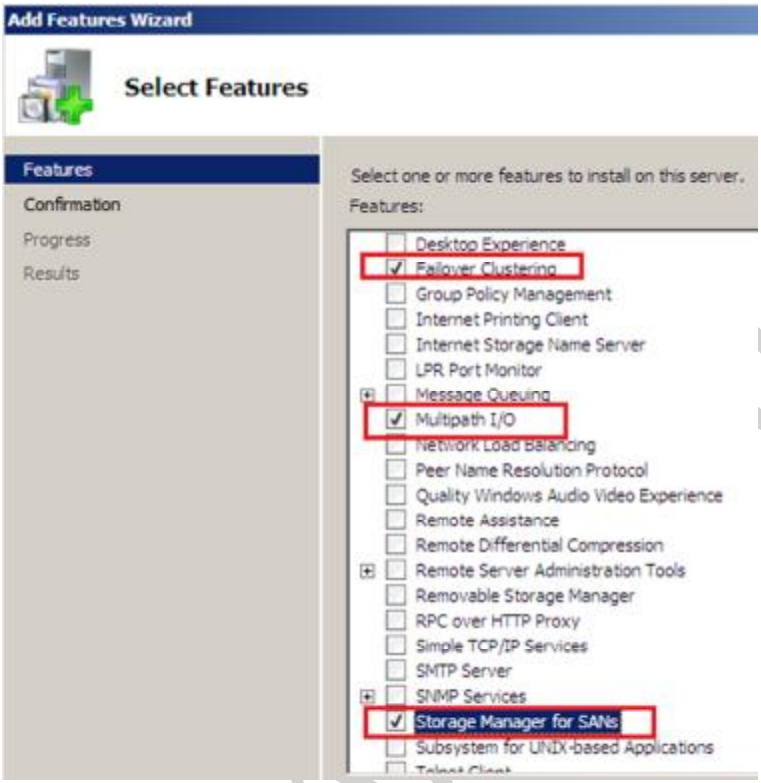
FarsiDAjan




بر روی سروری که می خواهد SAN, Emulator باشد باید Features زیر را نصب کنیم,این سرویس باعث می شود هاردهای ما قابل Discover شدن باشند.

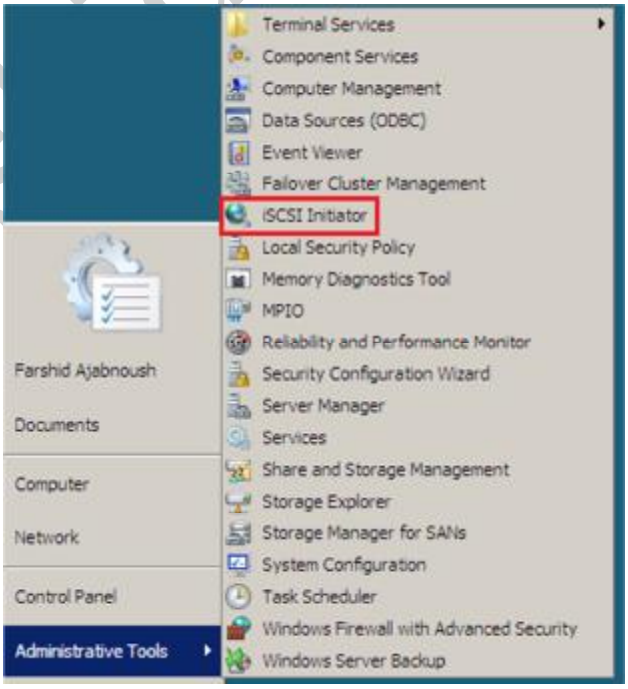


بر روی NOD ها(سرورهای 2و3) بایدFeatures های زیر نصب شود,2 Features آخر بر روی سرور2003 موجود نیست وباید Download ونصب گردد.




نوبت به معرفی SAN به NODها می باشد برای این کار مانند زیر عمل می کنیم

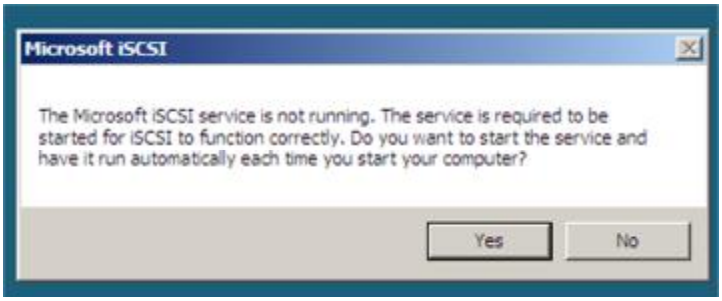
وارد NOD ها(سرور2و3) می شویم و سپس مانند زیر



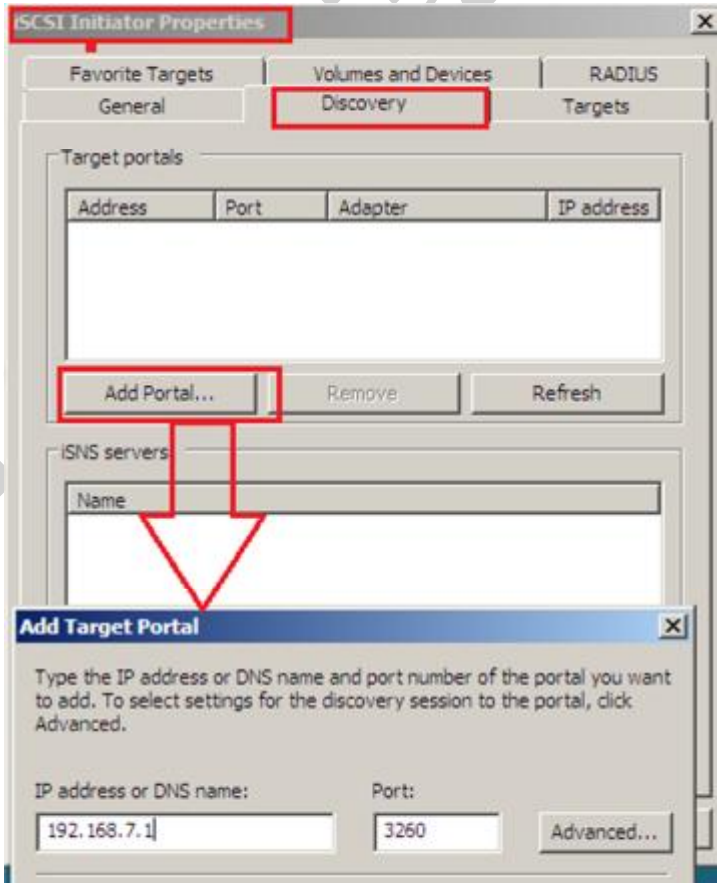

Farshid Ajabnoush

سپس با 2 سوال برخورد می کنیم

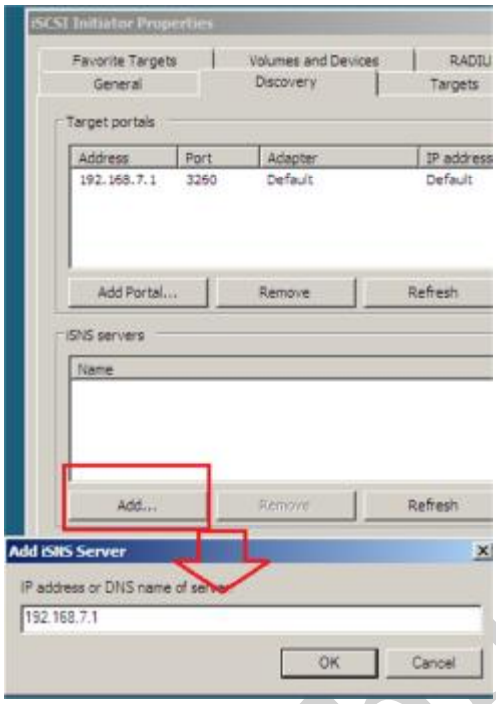
سوال1 می خواهید این سرویس را فعال کنم؟ سوال2 ISCSI از فایروال باز نشده آیا باز کنم؟

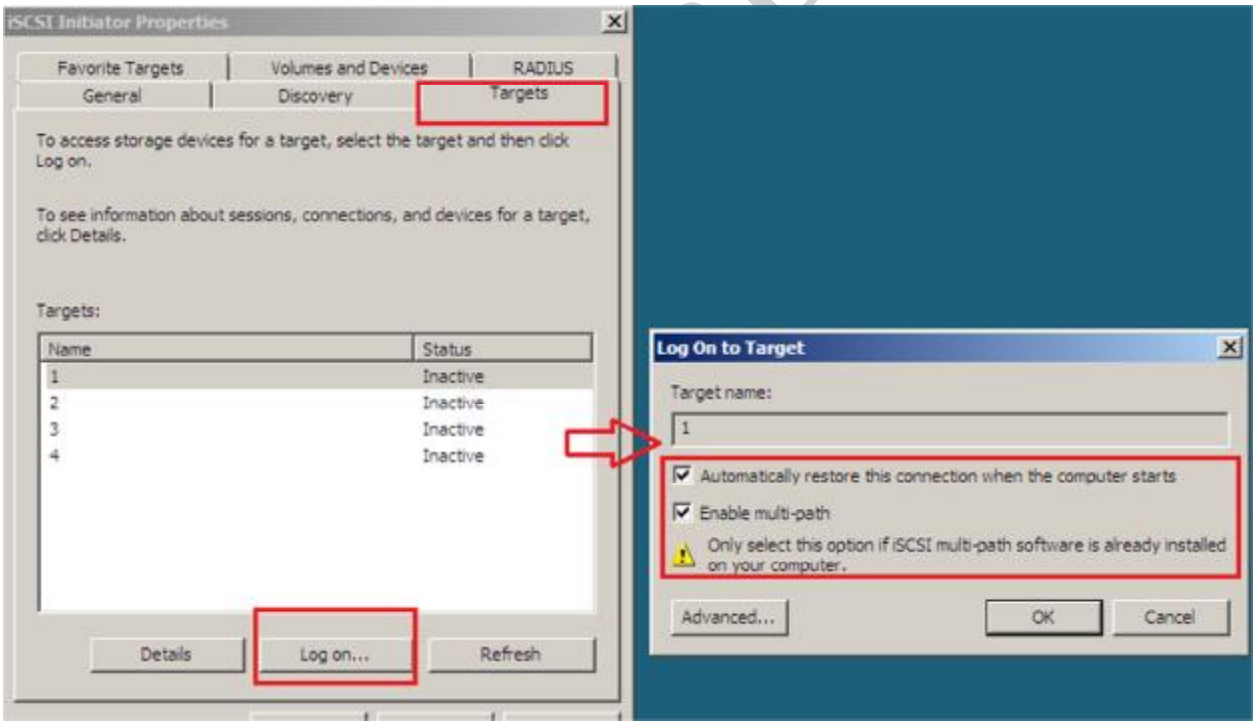


سپس کنسول باز می شود اولین کار این است که پورتال Target ها را معرفی کنیم(باید SAN را معرفی کنیم).



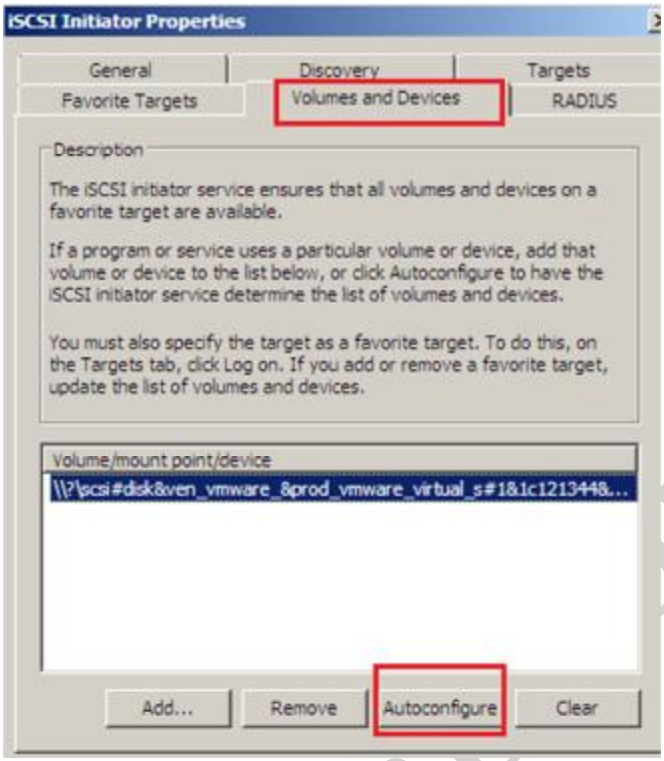

Far... Bush



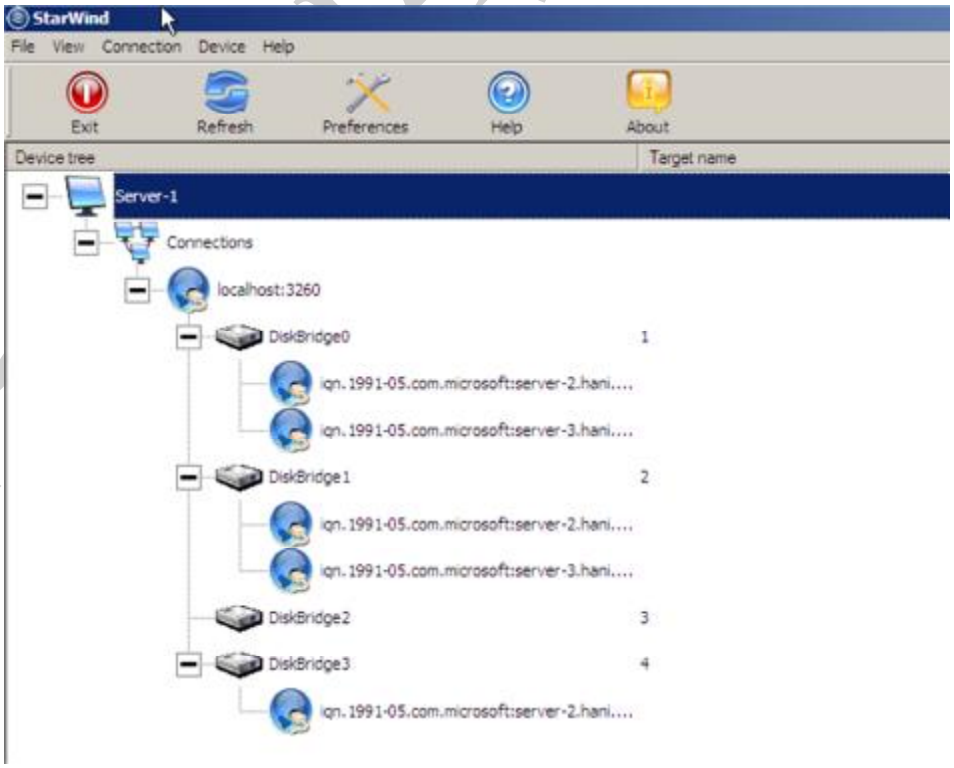

**با فعال بودن گزینه اول در صورت ریستارت شدن سیستم دوباره سعی می کند به آن هارد وصل شود،گزینه دوم برای رسیدن به این مسیر از چند مسیر استفاده کن.**

**برای هر 4 Target باید این کار انجام شود.**

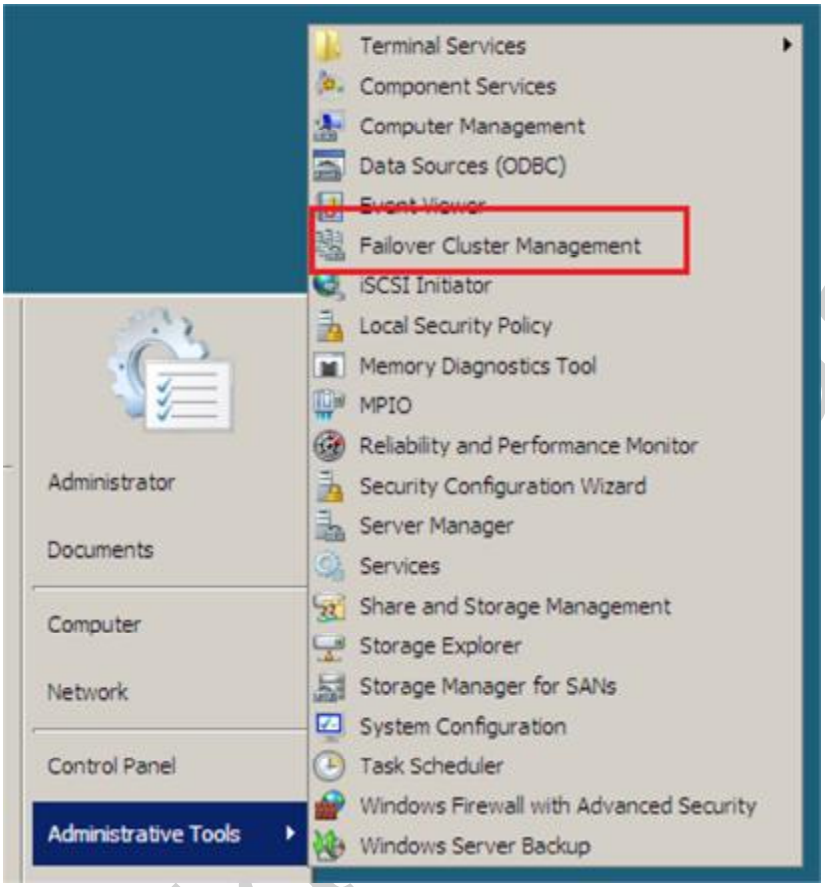



**با زدن ...Auto تمامی هاردهای داخل SAN را می شناسد (همانند هاردهای خودش). برروی هر دو سرور 2و3 باید انجام شود**

**سپس به سرور 1 بر میگردیم و تمامی سرورها شناسایی شده اند**



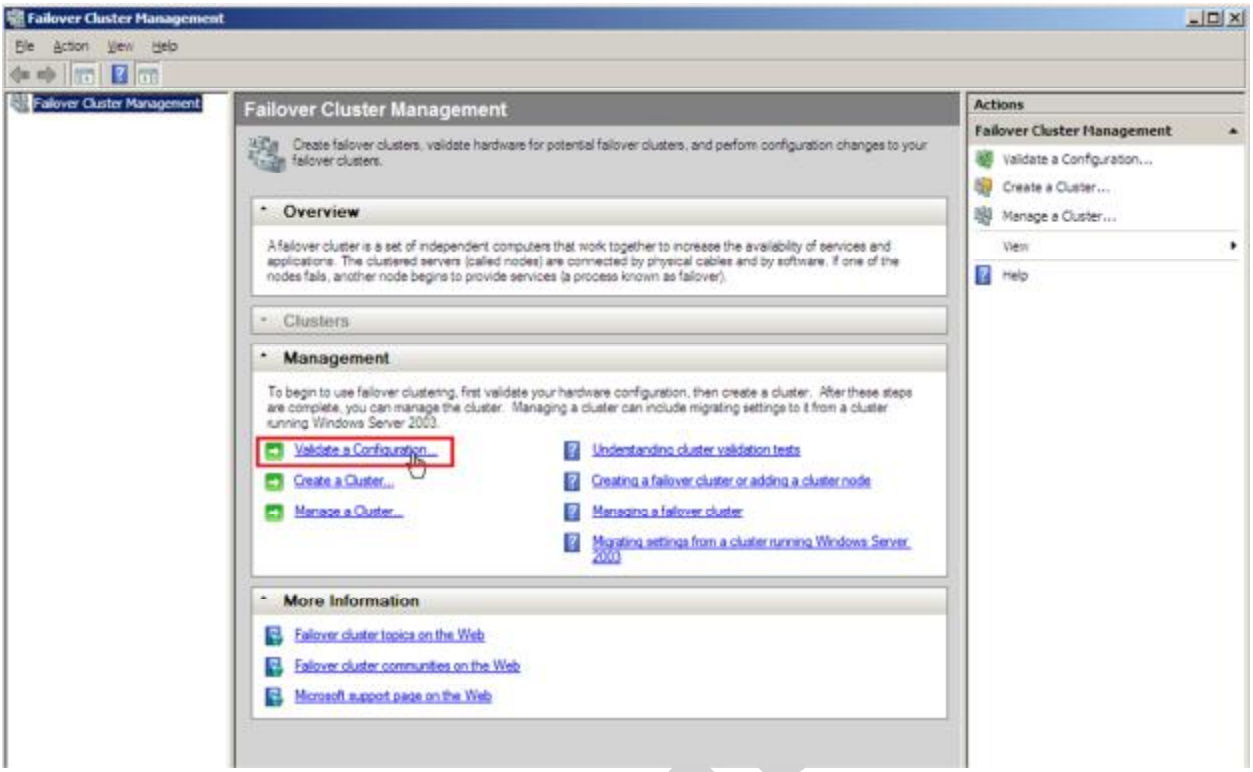

**سپس بر روی سرورهای 2و3 باید مانند زیر عمل کنیم**



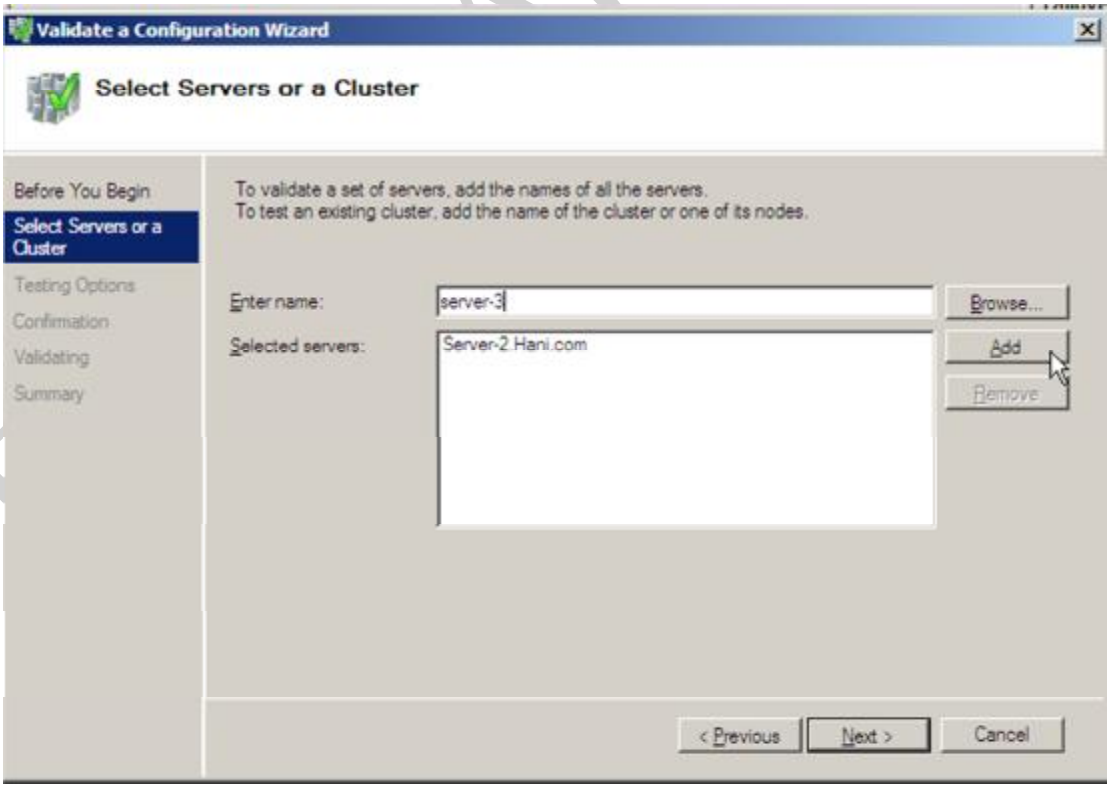

**سپس کنسول مانند زیر فعال می شود**

- **اگر لینک های آبی وسبز وسط موجود نبود به صورت Local وارد سرور شده اید.**

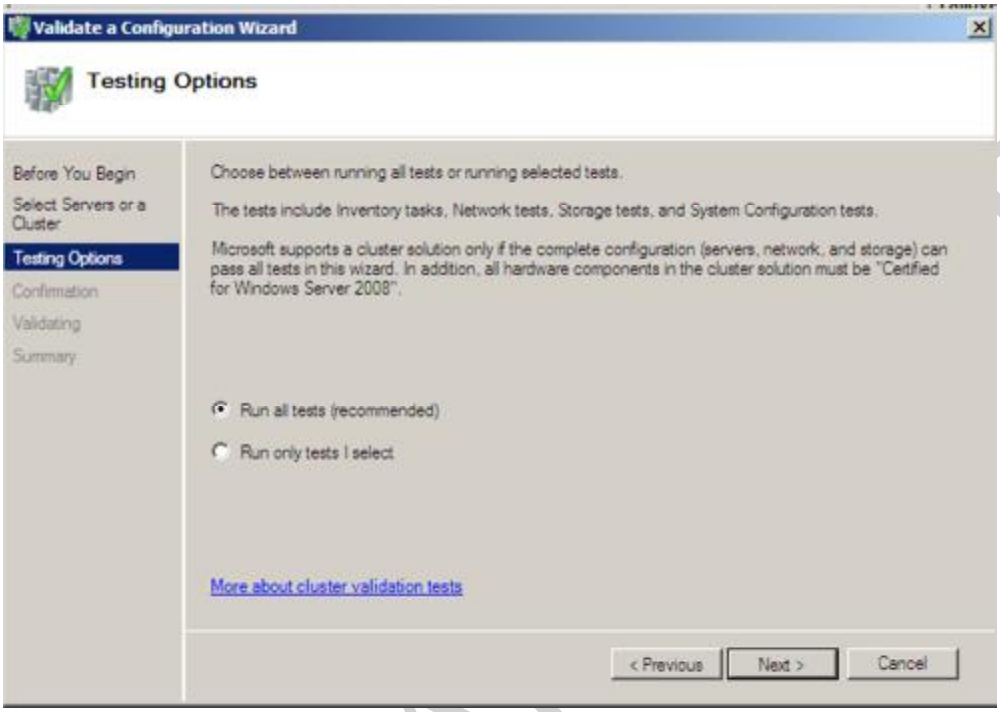
Farshid



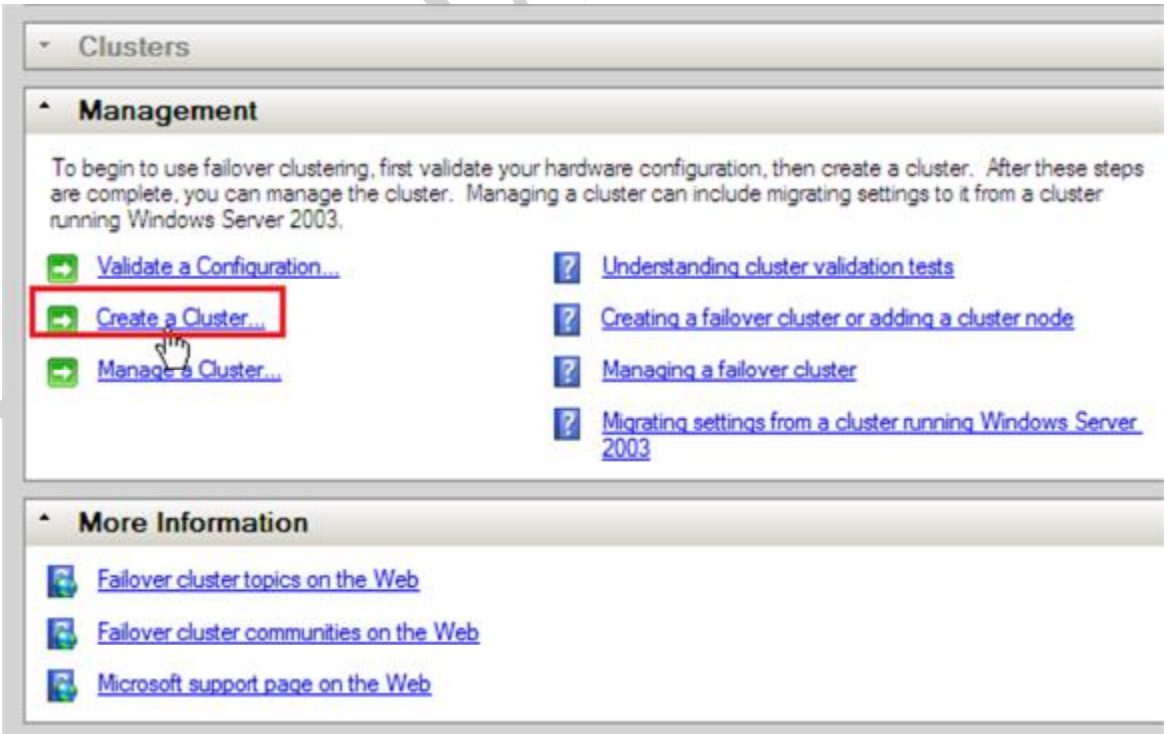

**در اینجا اسامی NOD ها را وارد می کنیم**



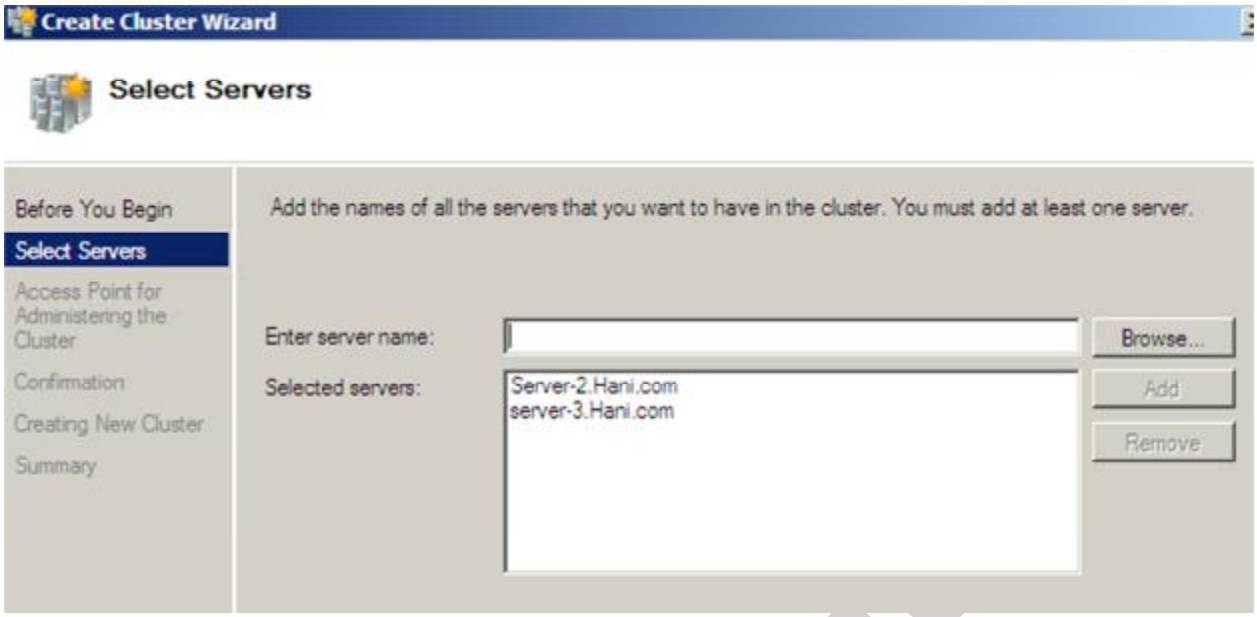
سپس نوبت به TEST می رسد که باید همه Pass شوند,2 دلیل عمده برای Pass نشدن وجو دارد 1- تنظیم نبودن DG وDNS 2- فرمت نکردن هاردهای SAN



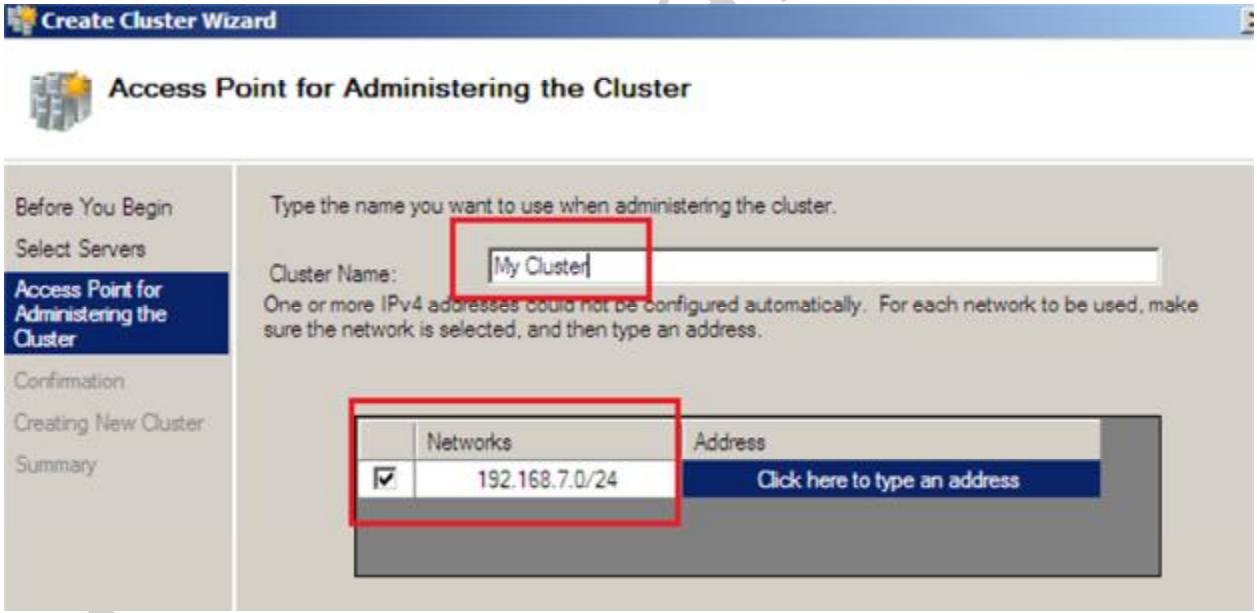

بعد از Pass شدن تمامی تست ها نوبت به ساختن کلاستر می شود.



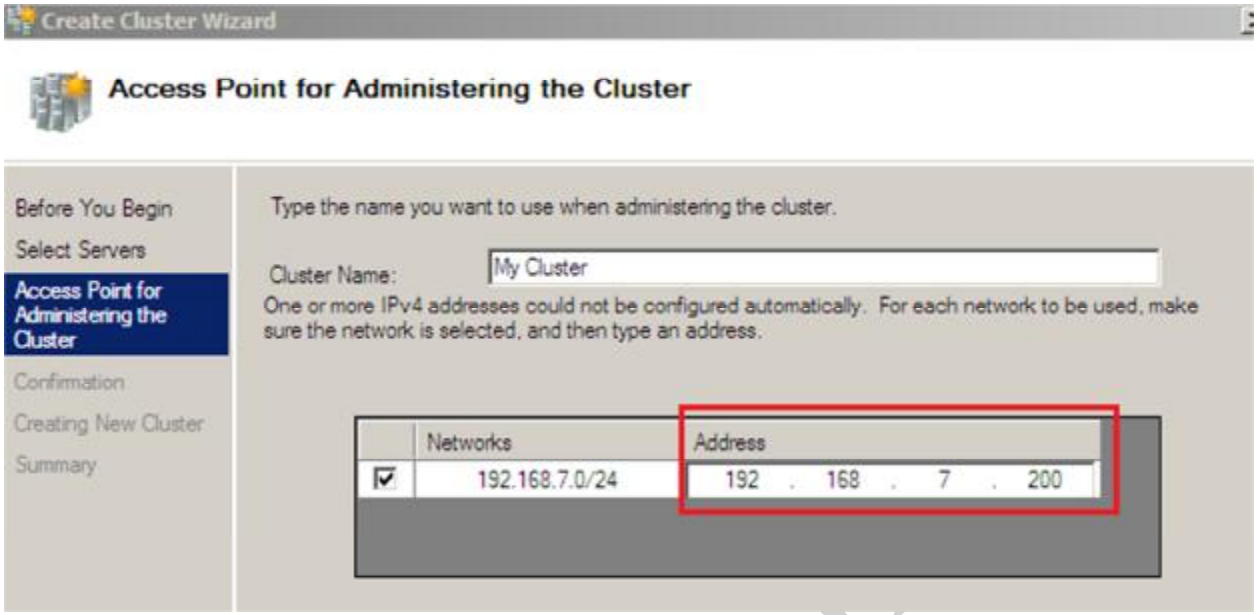

در اینجا باید اسامی سرورهایی را که می خواهیم کلاستر شوند را وارد کنیم



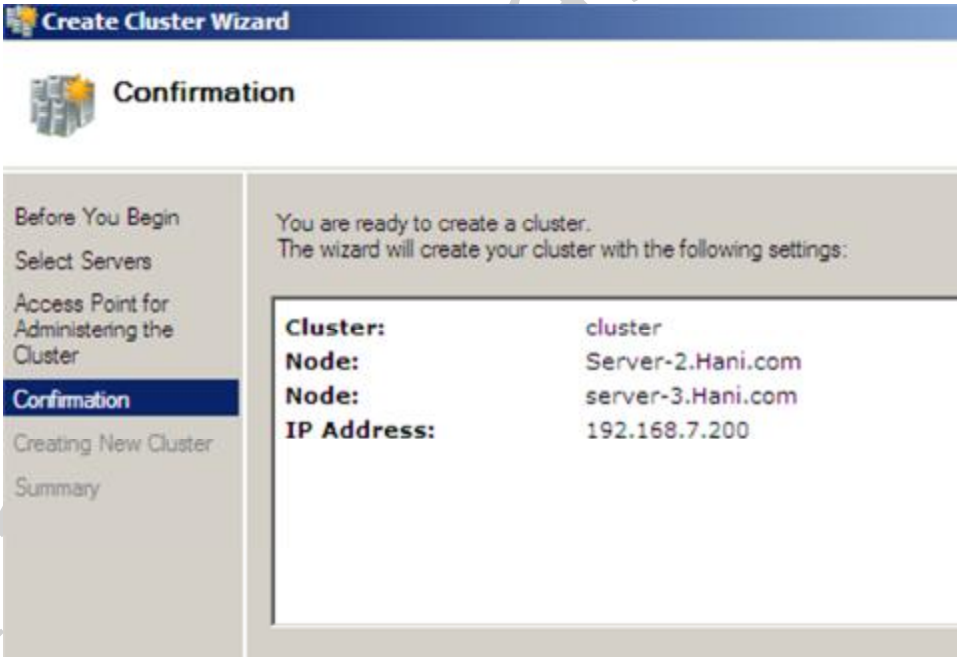

**در این مرحله یک اسم انتخاب می کنیم,رنجipها را از کارت شبکه ای که بر روی آنDG وDNS تنظیم شده بود خواند**

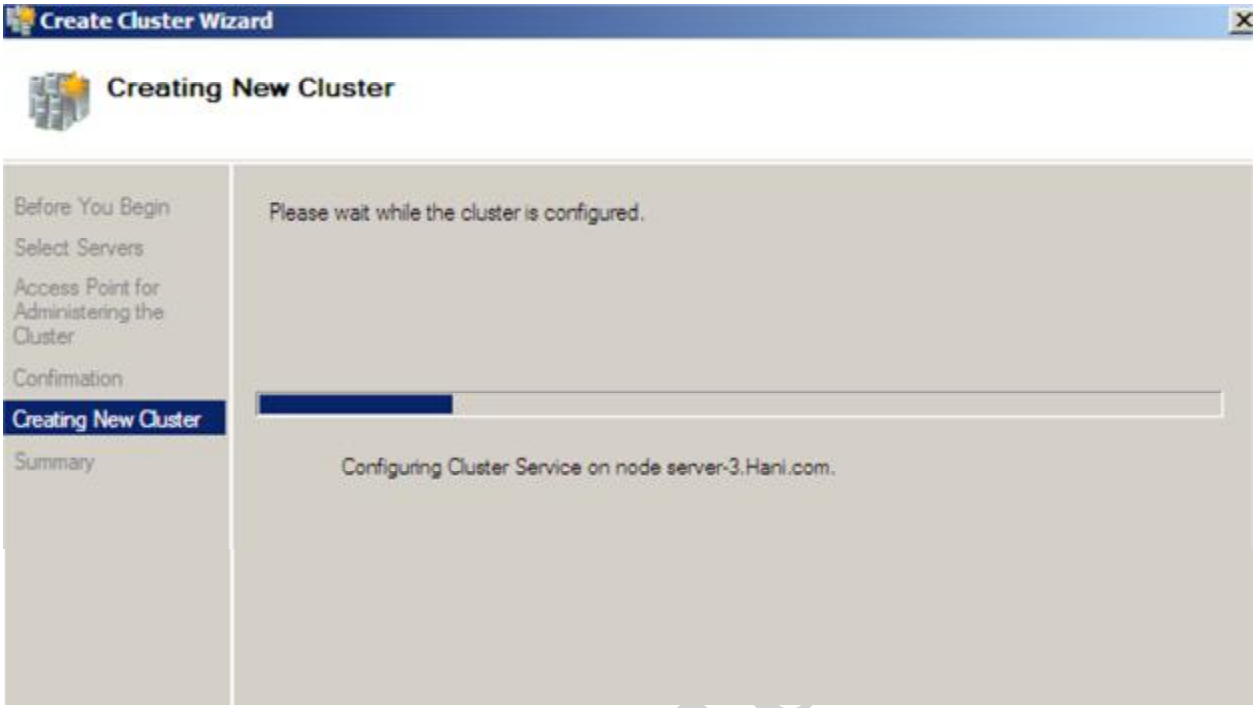


در اینجا باید برای سرور مجازی ip مشخص کنیم (در همان رنج)

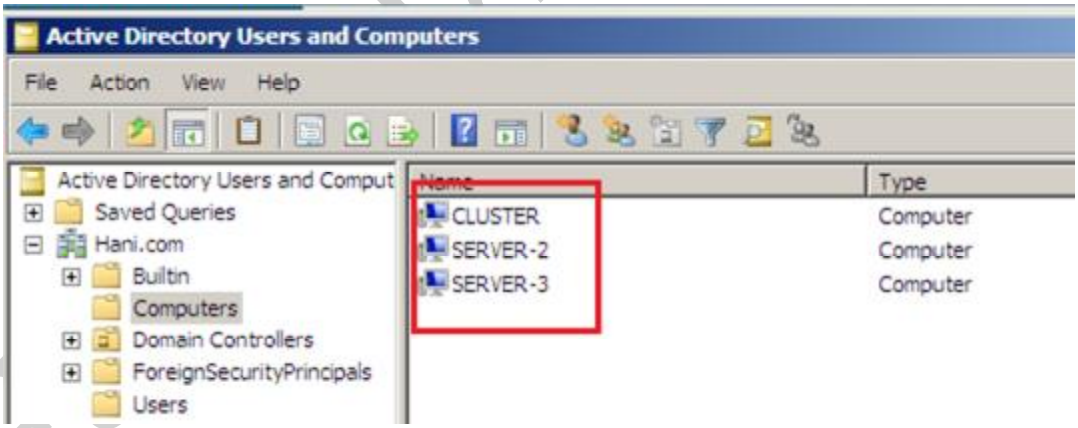



سپس نوبت به Validate کردن می رسد

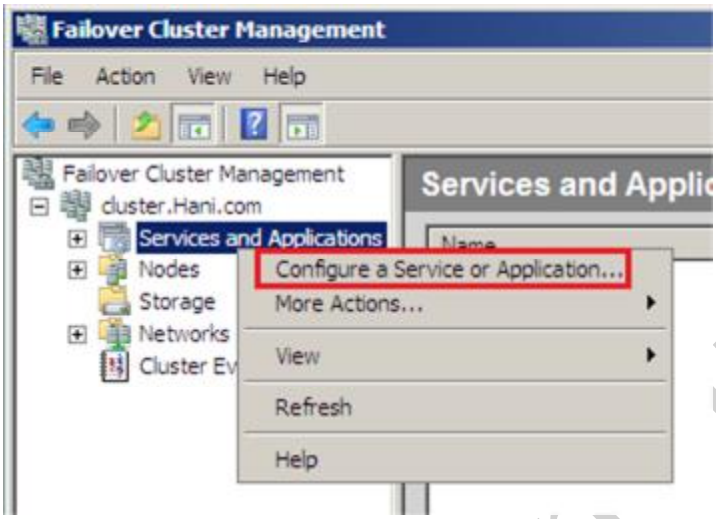




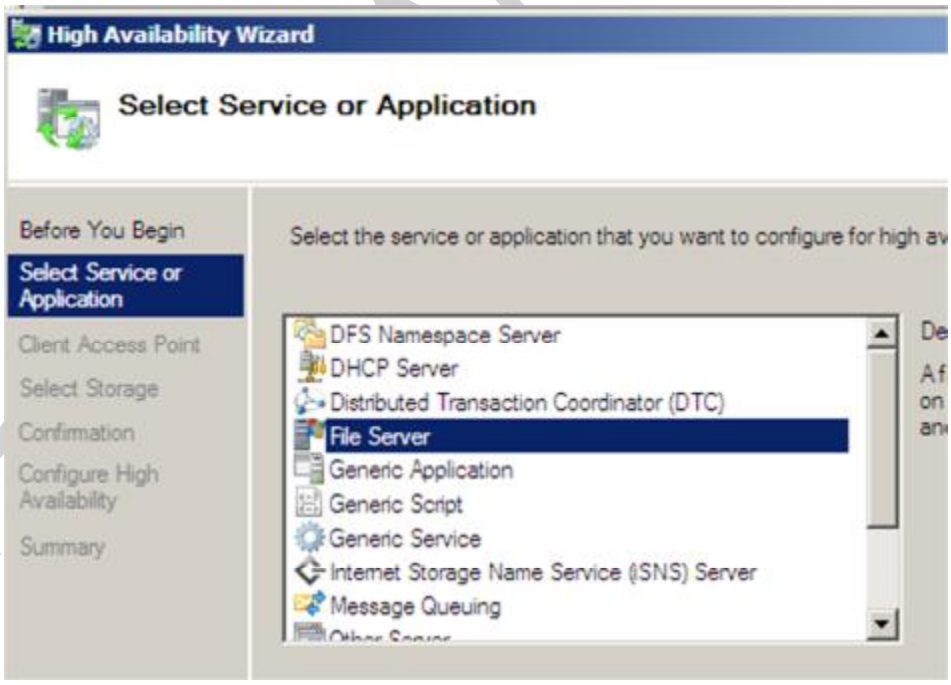

**بعد از اتمام کار وارد سرور1 می شویم و می بینیم 3 سرور اضافه شده است.**



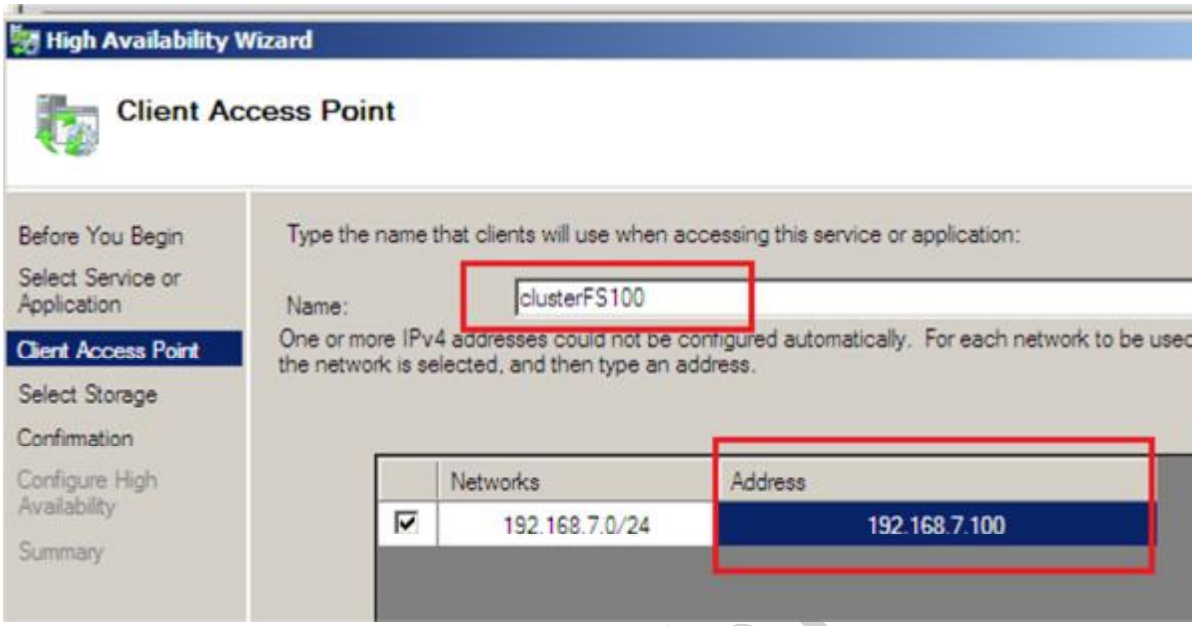
سپس نوبت به این می رسد که در کلاستر مشخص کنیم چه سرویسی را می خواهیم ارائه دهیم.



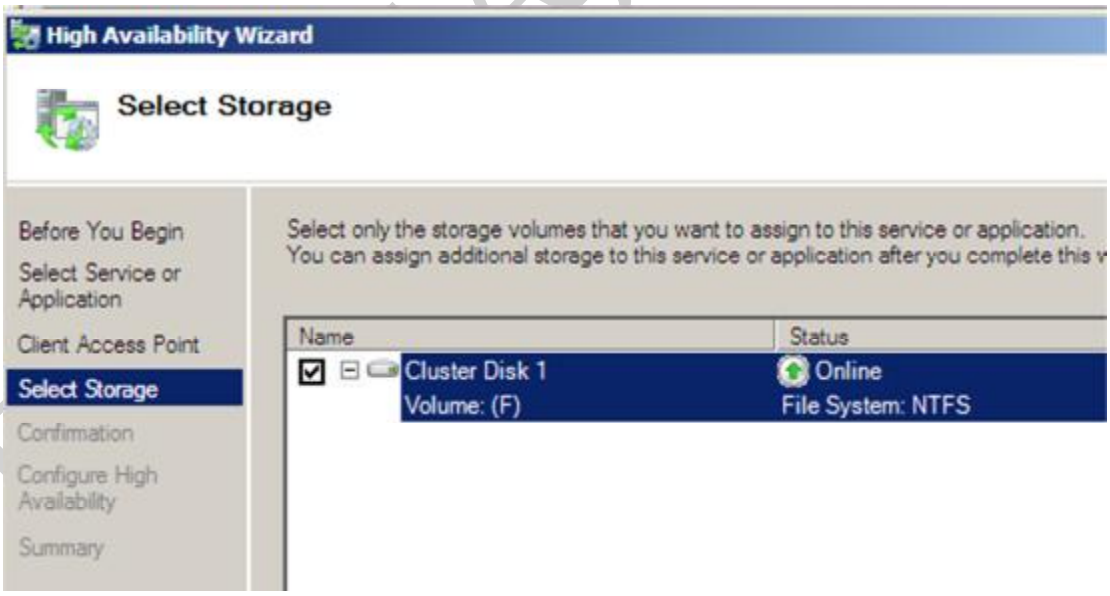

در مرحله بعد باید سرویسی را که می خواهیم ارائه دهیم را انتخاب می کنیم (در اینجا Sharing=Fileserver ) را انتخاب می کنیم.



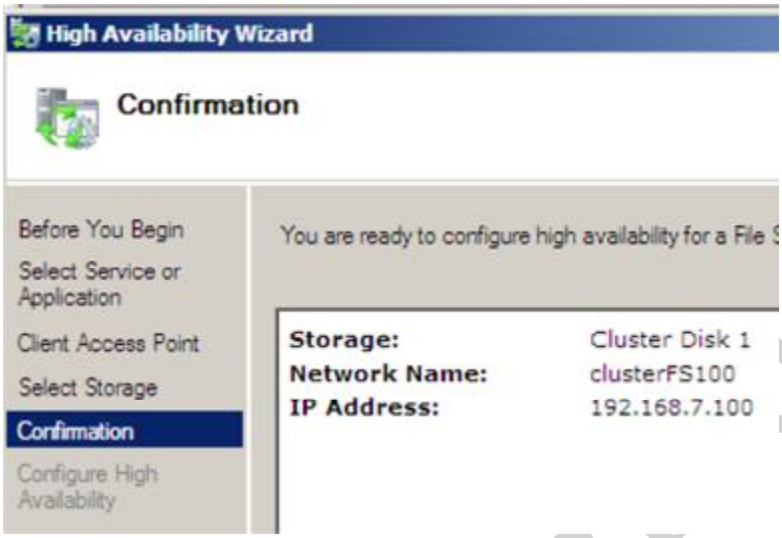
سپس باید اسم و IPتنظیم کنیم

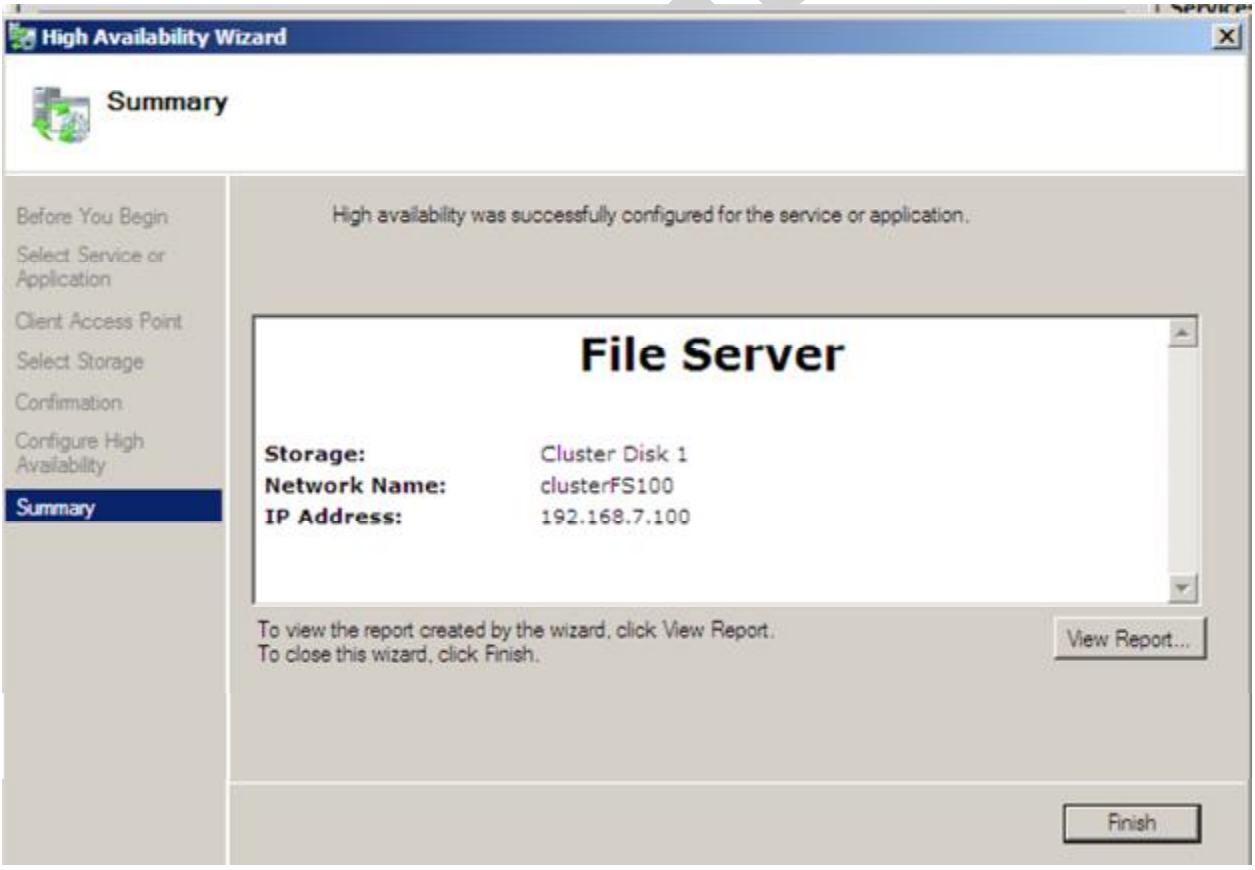



سپس باید مشخص کنیم Fileserver اطلاعاتشان را کجا ذخیره کنند(در سرور اصلی F را Share کرده بودیم)

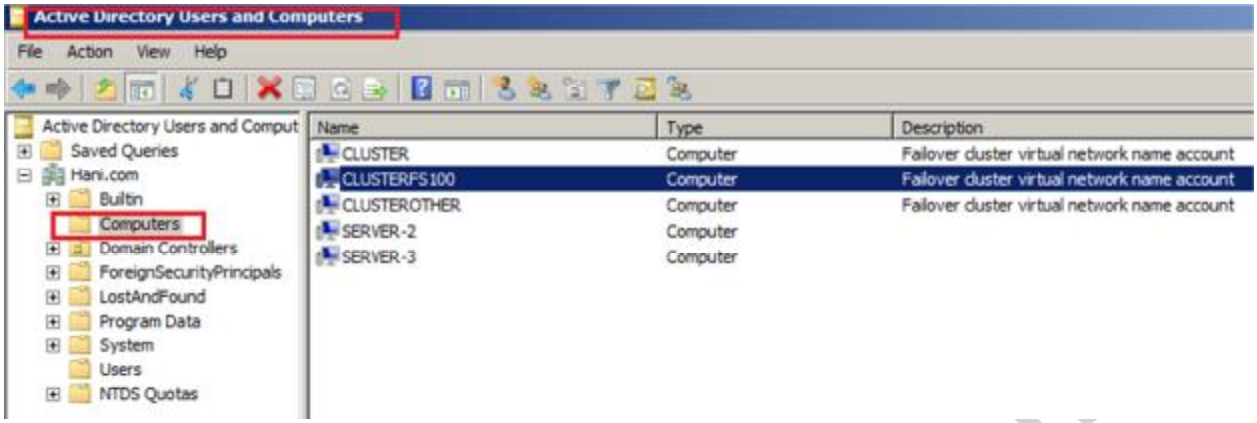


سپس یک گزارش,و در نهایت Finish

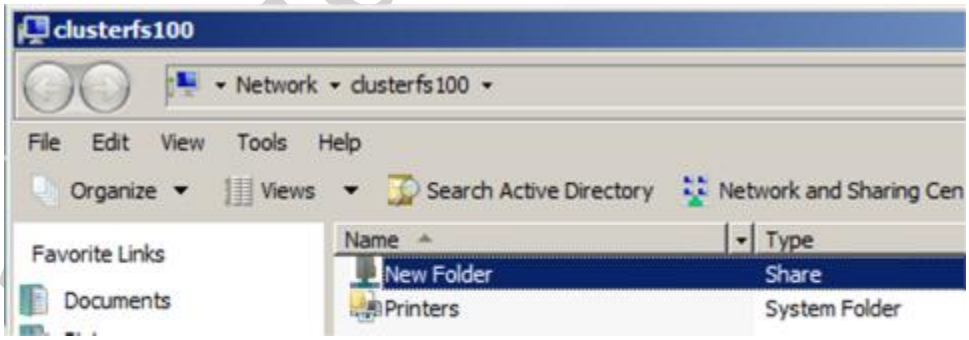



سپس وارد سرور اصلی می شویم و می بینیم که Fileserver100 اضافه شده




حالا نوبت به Test می رسد,پشت یکی از سرورها 2 یا 3 داخل درایو F (Clustered Disk ) یک Newfolder می سازیم و آن را Share می کنیم,سپس از روی یکی از کلاینت ها به192.168.7.100 وصل می شویم و آن فولدر را می بینیم.



IIS7

همیشه ISS را کنار DNS–FTP–Application Server نصب می کنند.

## ویژگی های IIS7

1- طراحی ماژولار(سرویس اضافی روی آن نصب نیست,سرویس های موردنیاز باید نصب گردد)

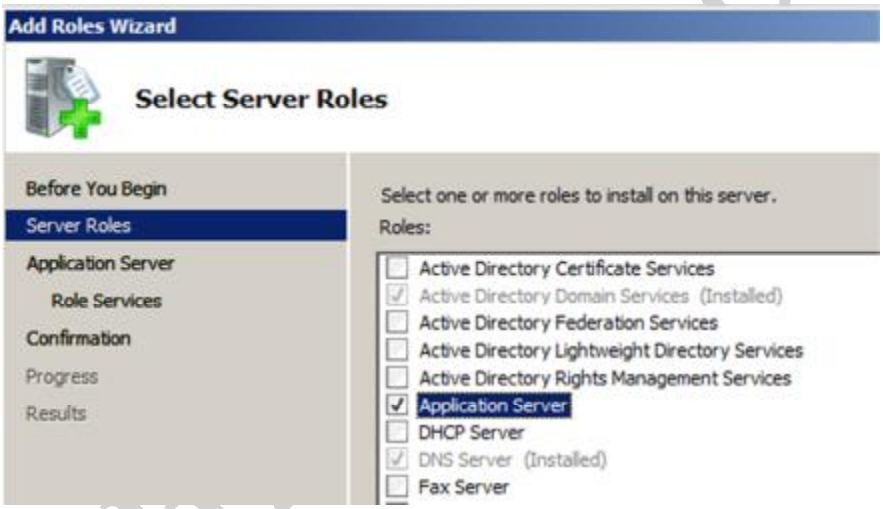
2- Delegation

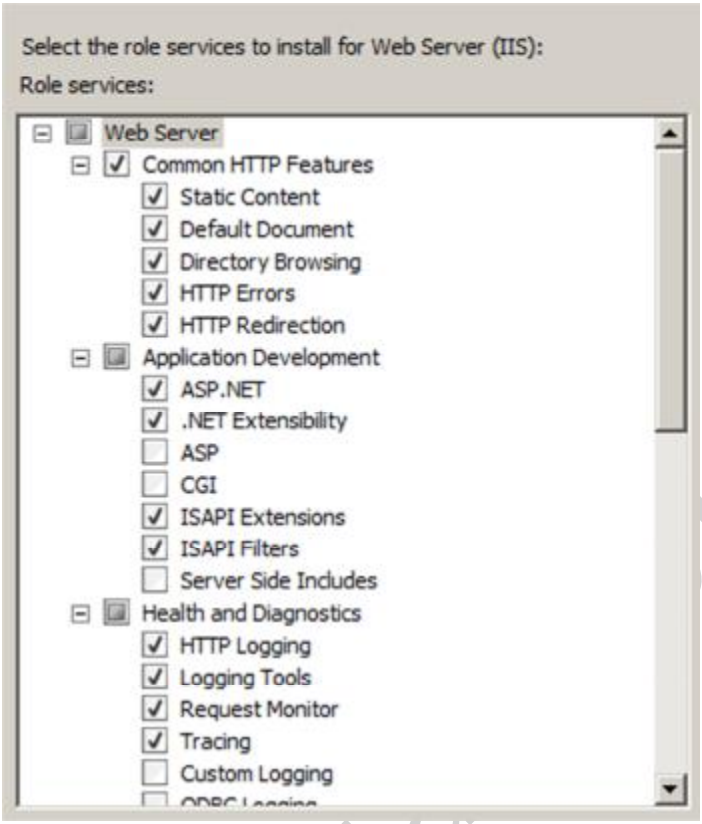
3- Backward compatibility(تمامی طراحی های روی IIS6 بر روی IIS7 قابل پیاده سازی می باشد)

4- Simple Administration

- مرجع اصلی IIS,سایت iis.net می باشد.

## نصب و پیکر بندی IIS7 در سرور2008






Static Contentهمیشه باید نصب گردد(اجباری).

Default Documentبرای زمانی است که بخواهیم اسم صفحه اول سایت را عوض کنیم (index),بهتر است فعال باشد.

Directory Browsing(Travelsal) از طریق url می توان وارد هارد سیستم شد(غیر فعال باشد بهتر است)

HTTP Errors با این گزینه می توان Error هایی را که هنگام مشاهده سایت به ما نشان می دهد را ویرایش کنیم.

HTTP Redirectionعمل Redirect را انجام می دهد

ASP.NET & ASPصفحاتی که با این زبان طراحی شده باشد را IIS نمایش می دهد.

بهترین زبان برنامه نویسی سایت php می باشد.

.Net Exte.., ISAPI Ex..., ISAPI Filبرای برنامه هایی که تحت IIS کار می کند باید این 3 گزینه فعال باشد مانندSharePoint

CGI رابط بین Browser و Webserver می باشد,اگر php, Webserver باشد رابط آن CGI ,اگر ASP.NET باشد رابط ActiveX ,اگر Java باشد رابطApplet می باشد.

Server Side Include تکنیکی در زبان برنامه نویسی ASP,سایتی که این ویژگی را دارد Header و Footer آن ثابت است و فقط محتویات وسط سایت تغییر می کند.

HHTP Logging تمامی لاگ های بازدیدکننده های سایت ما را ثبت می کند(فرمت آن هم TXT می باشد)

FarshidAjamush

Logging Tools ابزاری را در اختیار ما می گذارد که توسط آن HHTP Loggin را می توانیم بخوانیم.

Request Monitor & Tracing زمانی که ترافیک سایت زیاد می شود با استفاده از این ویژگی می توانیم مشکلات صفحات را بررسی کنیم.

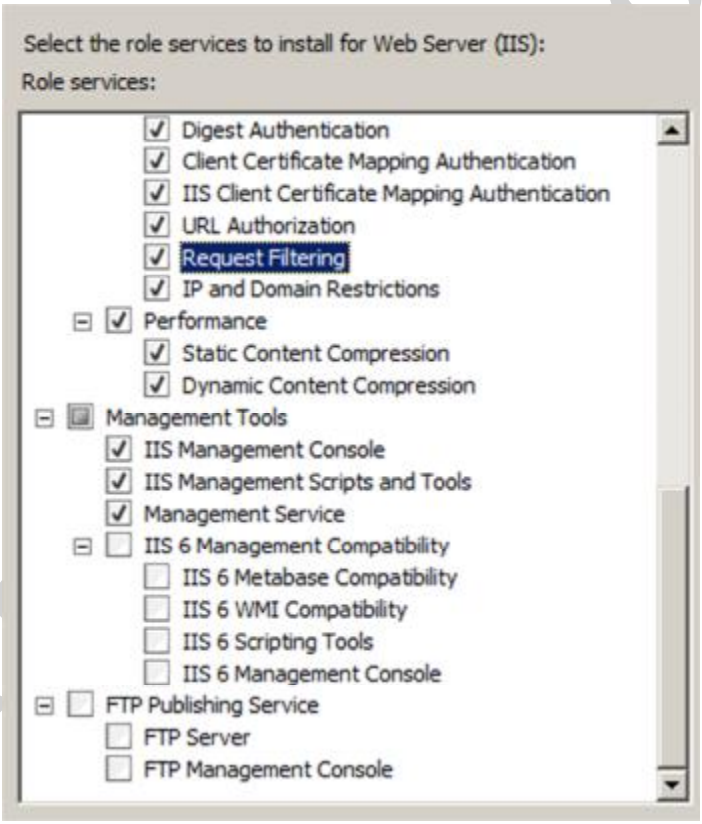
Custom Logging با فعال بودن این گزینه لاگ فایل ها با فرمت csv html ذخیره می شود.

ODBC Logging با فعال بودن این گزینه می توان لاگ ها را در Database ثبت کرد مانند: Access و SQL

Windows Authentication با فعال بودن این گزینه می توان از بازدیدکنندگان سایت قبل از ورود به سایت یوزر و پسورد بخواهیم(فقط با IE سازگار می باشد و یوزر و پسورد را به صورت clear text ردوبدل می کند)

برای برطرف کردن مشکل سازگاری گزینهAuthenticationBasicرا فعال می کنیم وبرای برطرف کردن Clear text , Digest Authentication را فعال می کنیم.

Url Authorization یوزرهارا بر اساس لینک ها باز یا بسته کنیم.

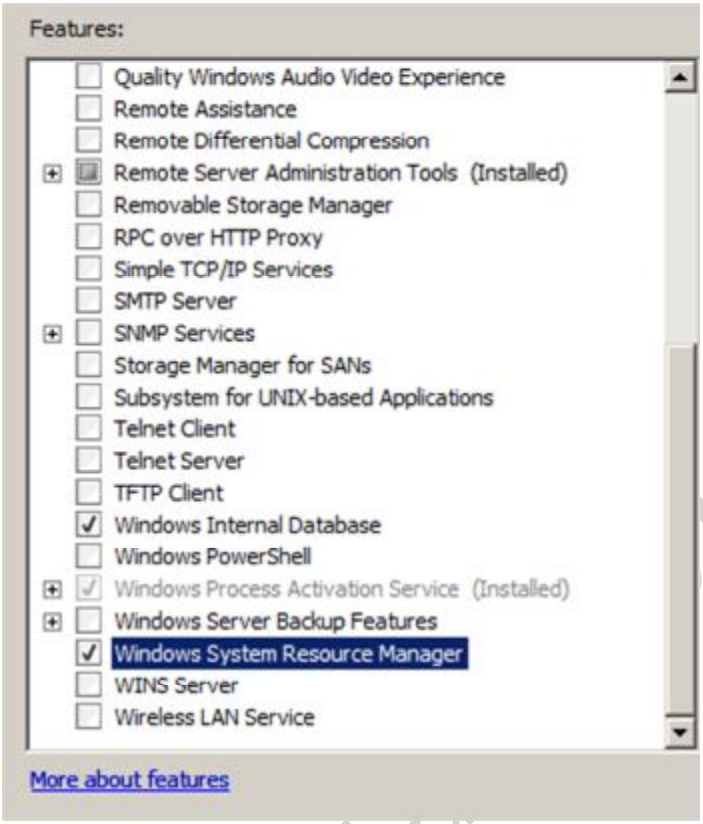



Request.....وIp... بر اساس Ip دسترسی را تنظیم می کنیم.

Performance برای نصب SharePoint و2010 Exchange باید این گزینه فعال باشد.

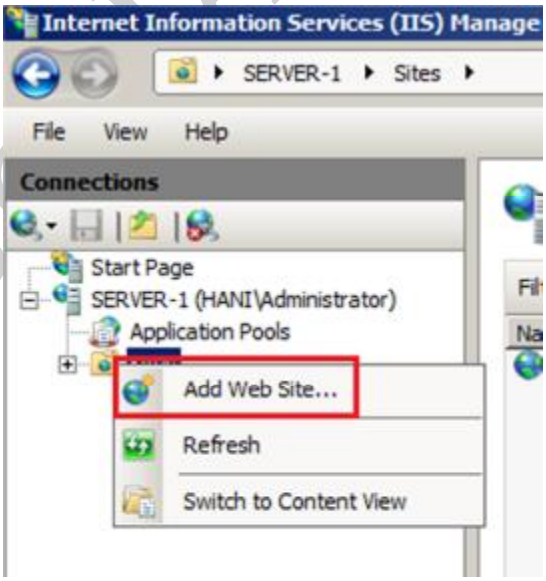
برای نصب FTP گزینه FTP را انتخاب نمی کنیم چون ورژن آن 6 است,باید7 ,و به بالا نصب شود.

بعداز نصب IIS باید کنسول زیر را هم نصب کنیم

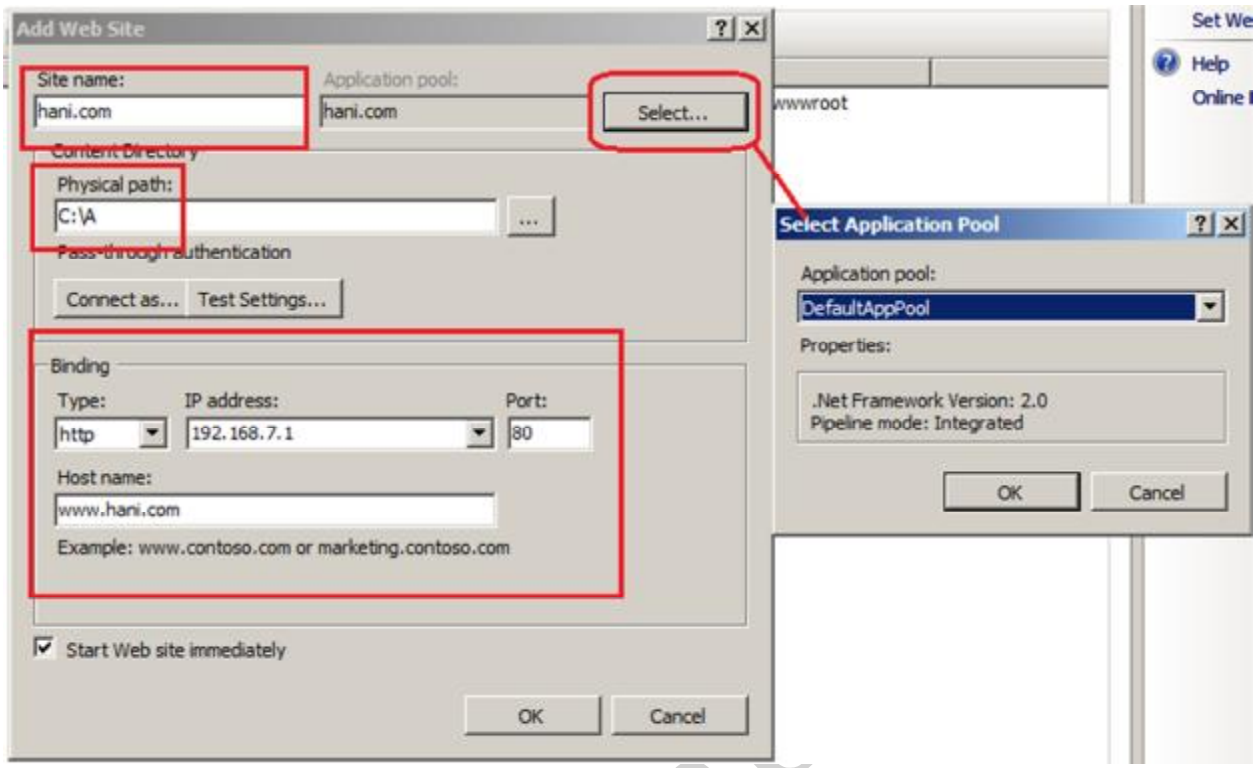



**برای مدیریت سخت افزار بر اساس کاربران می باشد(میزان Ram و... اختصاص یافته به هر کاربر)**

**برای معرفی کردن سایت داخل IIS مانند زیر عمل می کنیم(قبلا داخل DNS تنظیمات لازم را انجام داده ایم)**




Farsh Arayesh




ابتدا اسم سایت را وارد می کنیم,به ازای هر سایت یک Application Pool ساخته می شود.

Application Pool : جداسازی برنامه های سرور به ازای هر سایت,اگر سایتی را از IIS 6 به روی IIS7 آوردیم باید App Pool آن را بر روی Default App Pool تنظیم کنیم.

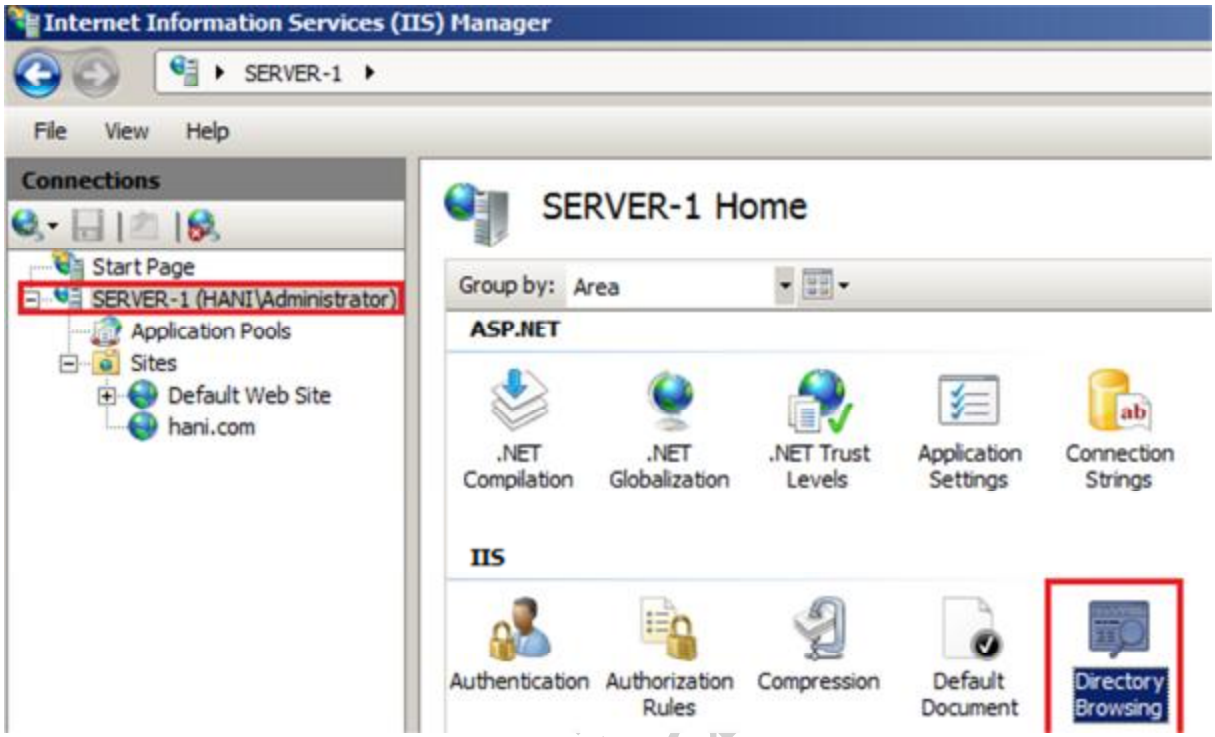
در قسمت Path آدرس پوشه سایت را می دهیم.

Hostname : در IIS6 اگر می خواستیم 2 سایت را بارگذاری کنیم 2 روش داشتیم روش اول,Ip2 بر روی کارت شبکه تنظیم می کردیم روش دوم,2 پورت را بر روی یک Ip تنظیم می کردیم,در IIS7 یک روش دیگر به نام HostNam اضافه شده است,در Hostname سایت ها با اسم از هم جدا می شوند.

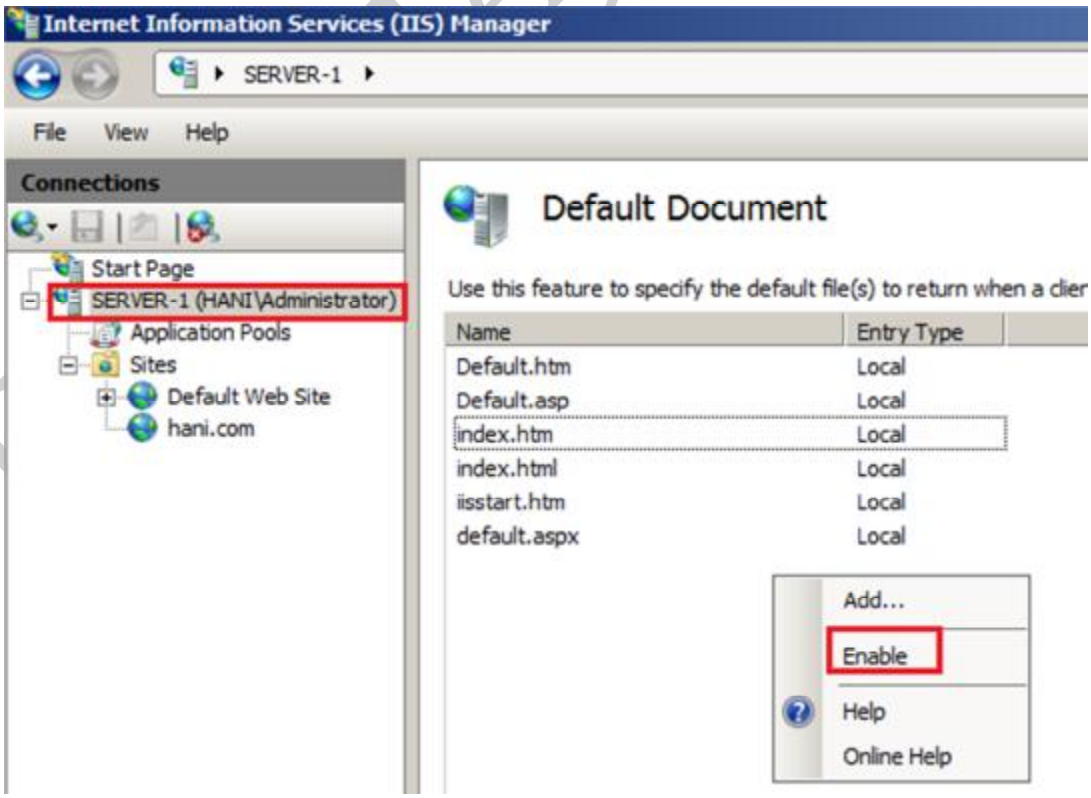
تمامی سایت ها یا Ip Base هستند یا Host Base,در Host Base نمی توان SSL و Bandwith Shapping اجرا کرد.

FarshidAjal

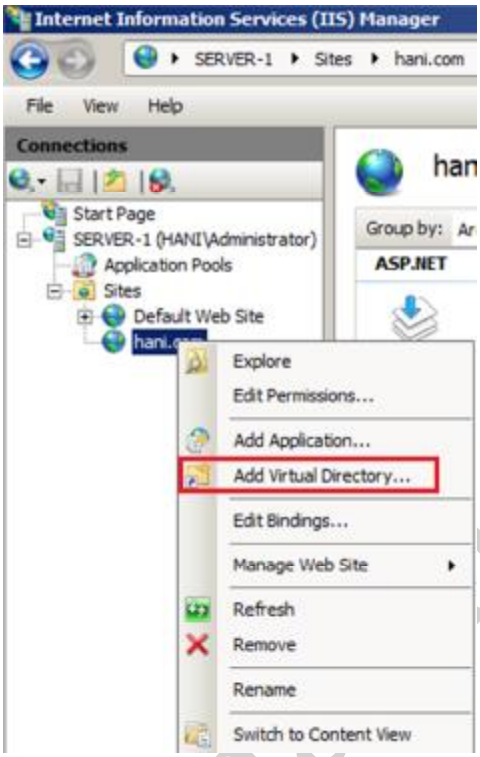
Virtual Directory بر روی سایت



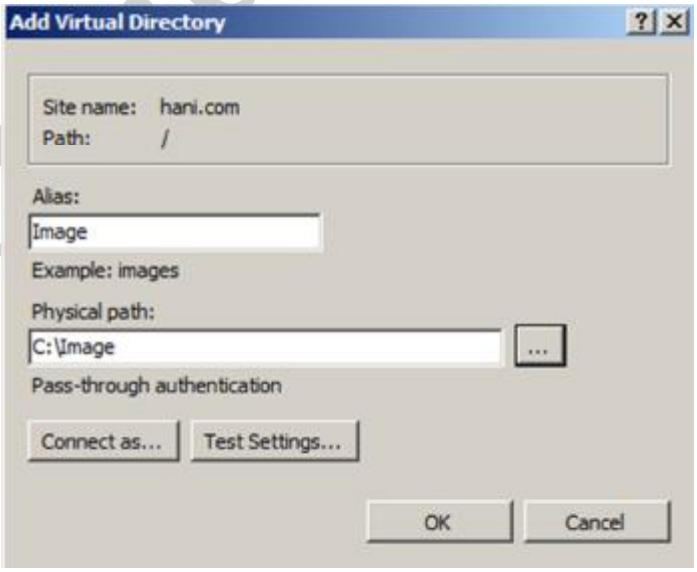

وارد Directory Browsing می شویم,کلیک راست و Enable



سپس بر روی سایت مانند زیر

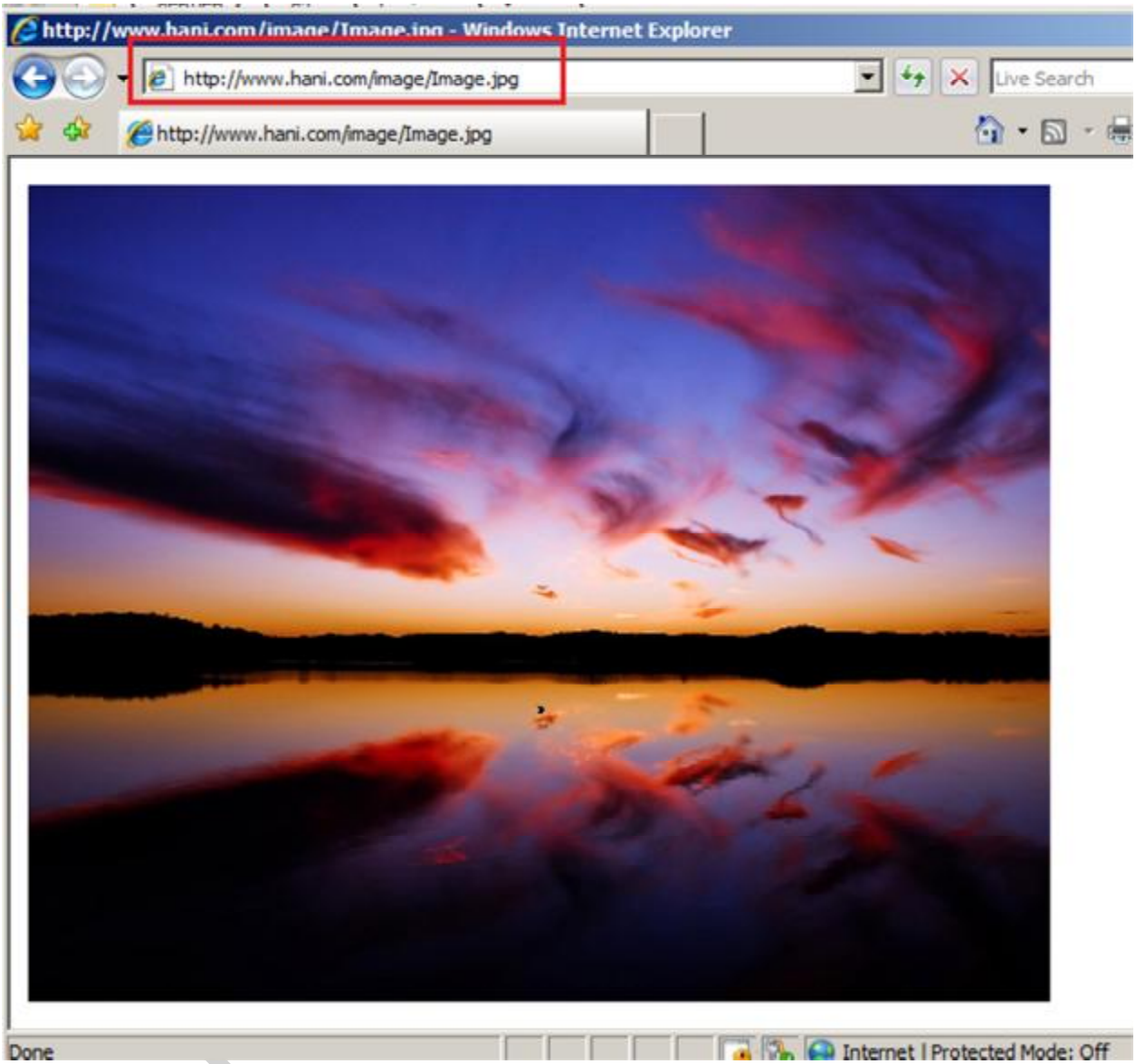



یک اسم (Image ) تعیین می کنیم,مسیر پوشه ای را هم که فایل عکسمان در آنجا هست را وارد می کنیم.



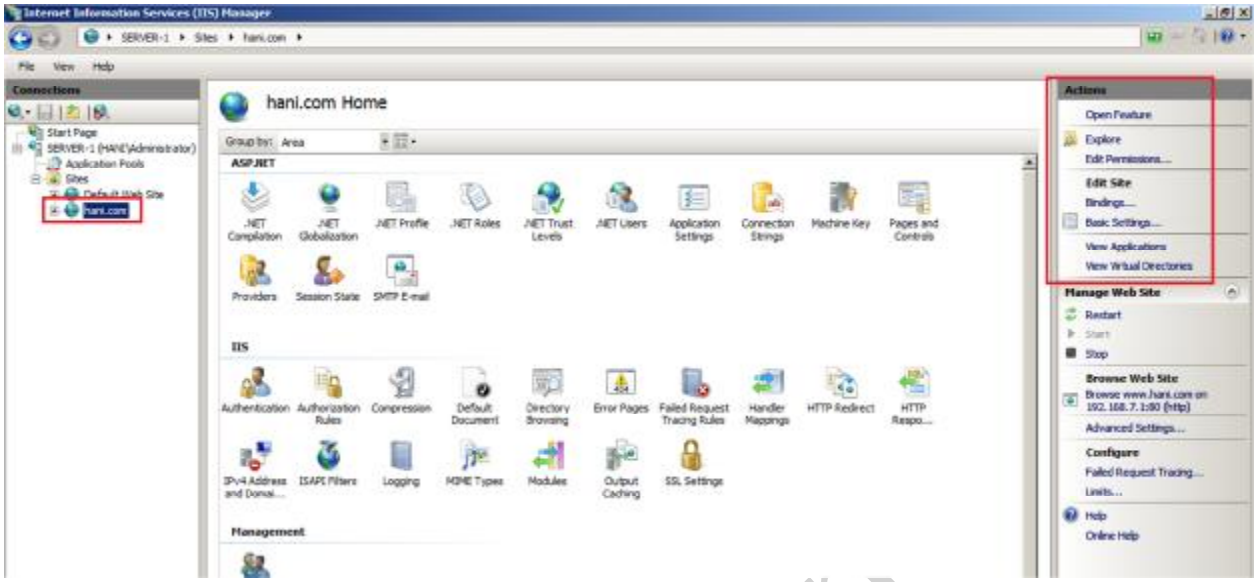

FaridAjdoush

سپس مانند زیر عمل می کنیم



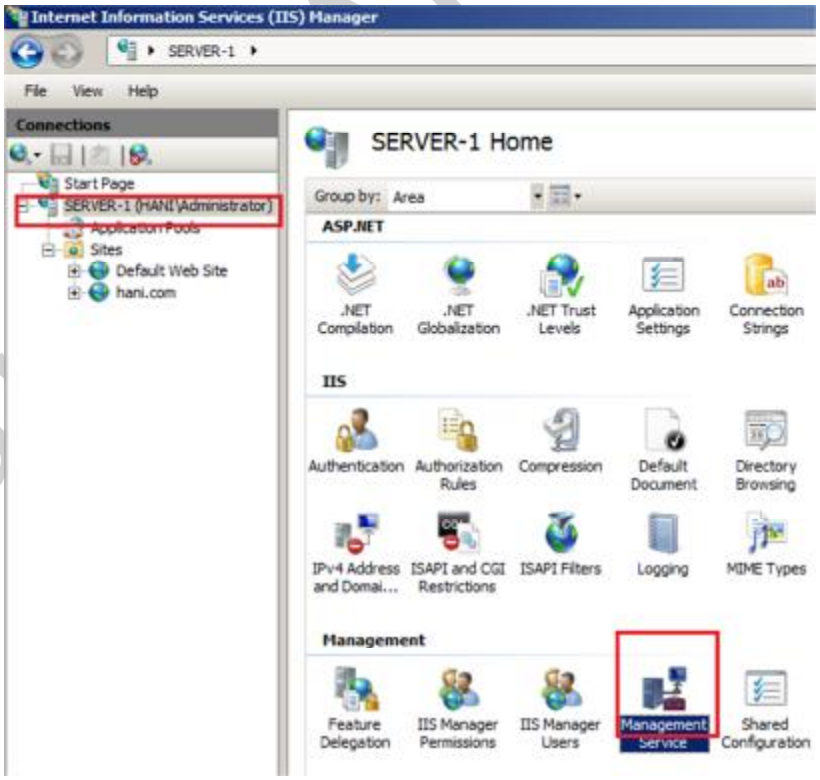

در نهایت عکس موجود در پوشه ای را که بر روی هارد ذخیره شده را می بینیم.

تنظیمات بر روی سایت

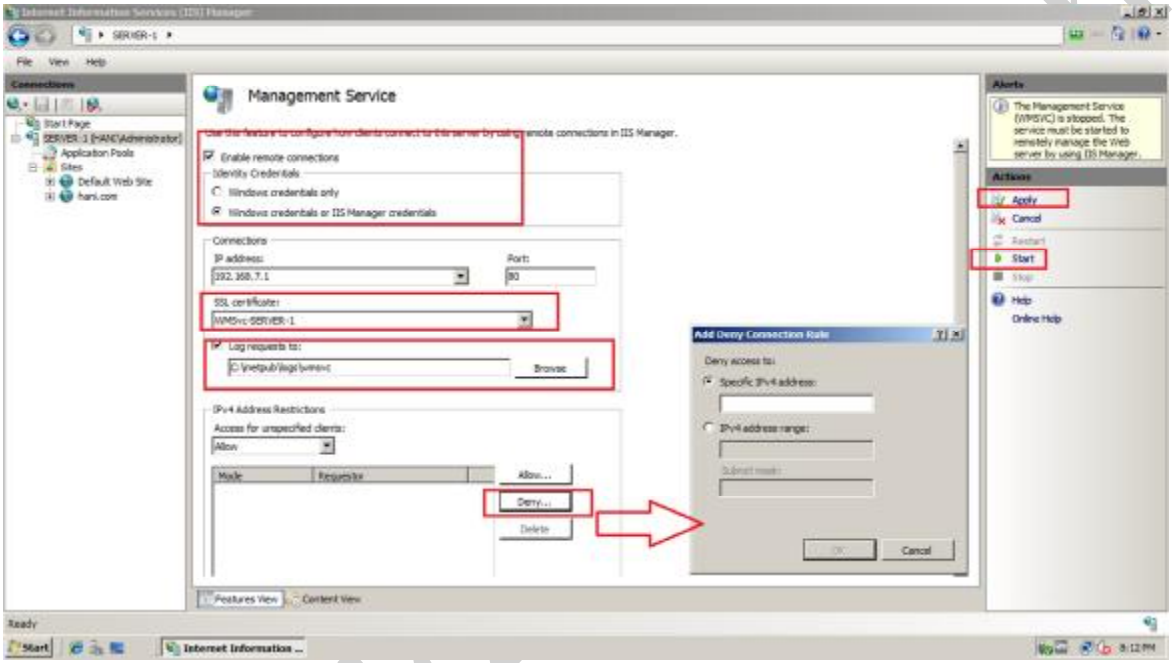



Binding تنظیمات کارت شبکه,Basic Settings مسیر صفحات و Application Pool را می توان تغییر داد.

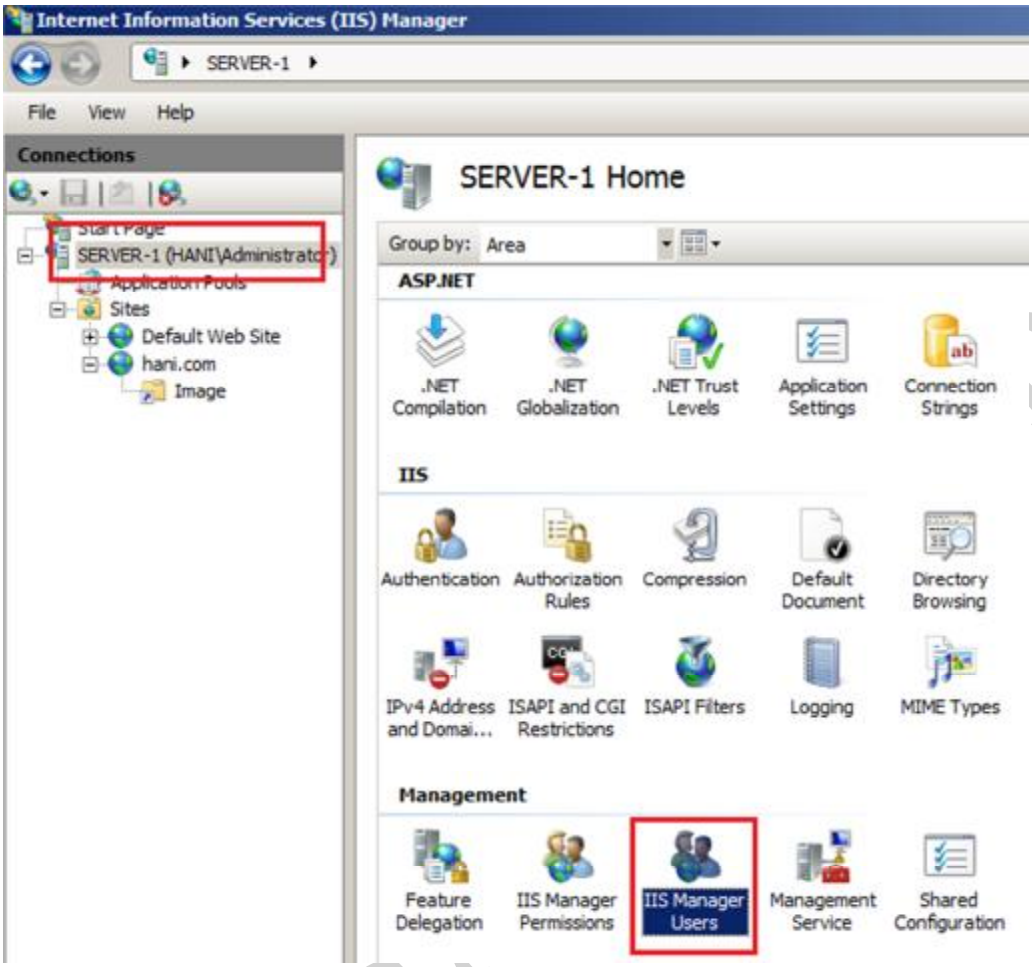
نحوه Delegate کردن یک سایت



ابتدا تیک Enable را فعال می کنیم که بتوانند از بیرون به سایت ما وصل شوند,در قسمت دوم گزینه2 را انتخاب می کنیم که می گوید هم یوزر و پس های ویندوزی و هم IIS را قبول کن,در قسمت بعدی IP و Port سپس SSl و مسیر لاگ startفایل ها را نشان می دهد,در قسمت آخر اگر بخواهیم Ip را Deny کنیم مانند زیر عمل می کنیم و درآخر هم Apply و Start .

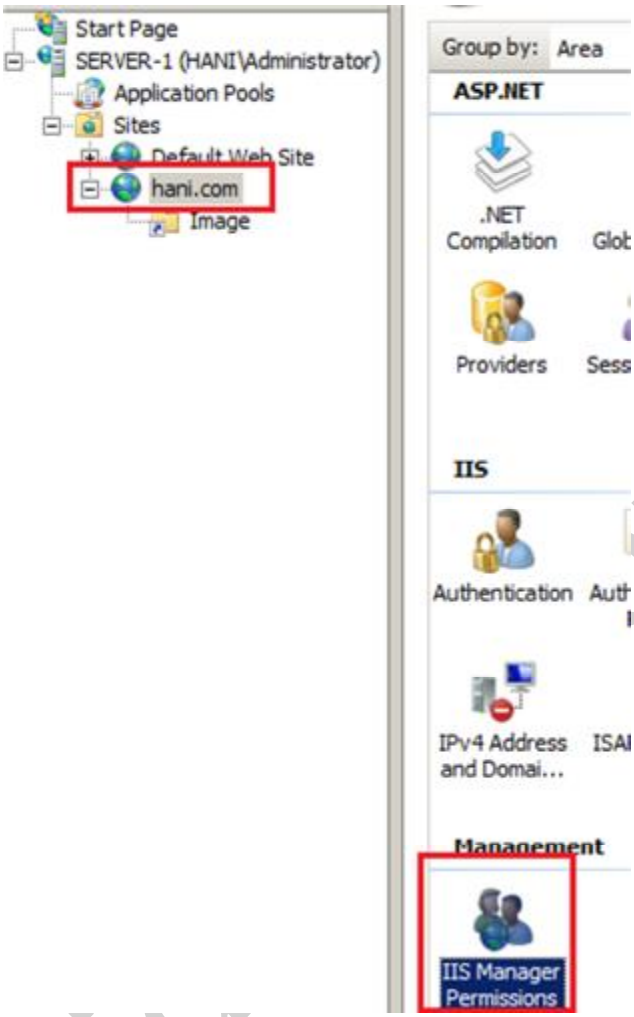



Farshid



**در اینجا می توان یوزرهایی را که از بیرون وصل می شوند تعیین کرد.**

**در این مرحله باید User که اجازه دارد از بیرون وصل شود را معرفی کنیم.**

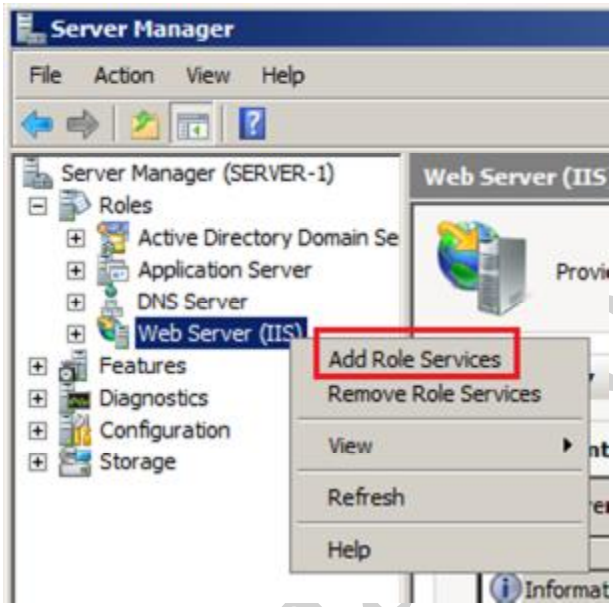


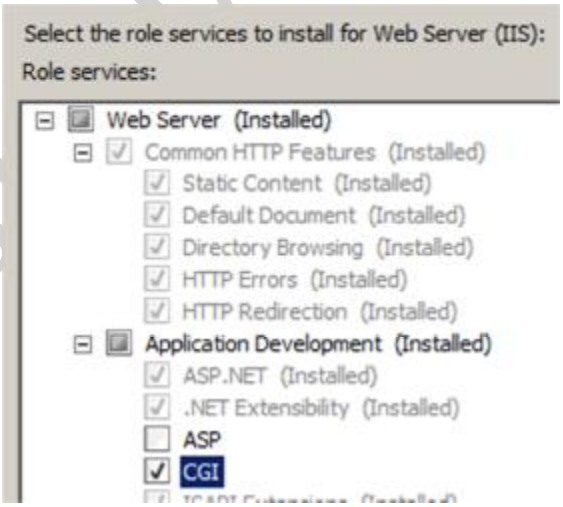

برای اینکه بتوانیم توسط User ساخته شده از روی یک کلاینت به سایت وصل شویم باید نرم افزار Inetmgr86 را از سایت IIS.net دانلود و نصب کنیم و توسط آن به سایت وصل می شویم(باید Ip سایتمان و... را وارد کنیم).

Farshid Roush

## php در IIS

**اولین کار نصب WAMP می باشد که توصیه نمی شود,بهترین کار این می باشد که آخرین ورژن php را از php.Net دانلود و نصب می کنیم,قبل از نصب نرم افزار باید CGI را فعال کنیم.**

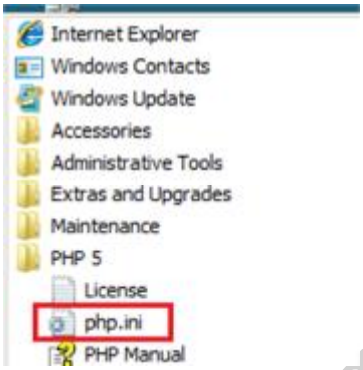


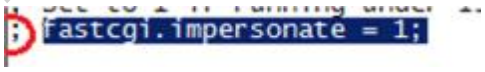

**سپس نرم افزار php را نصب می کنیم**

Farshad Ajoush

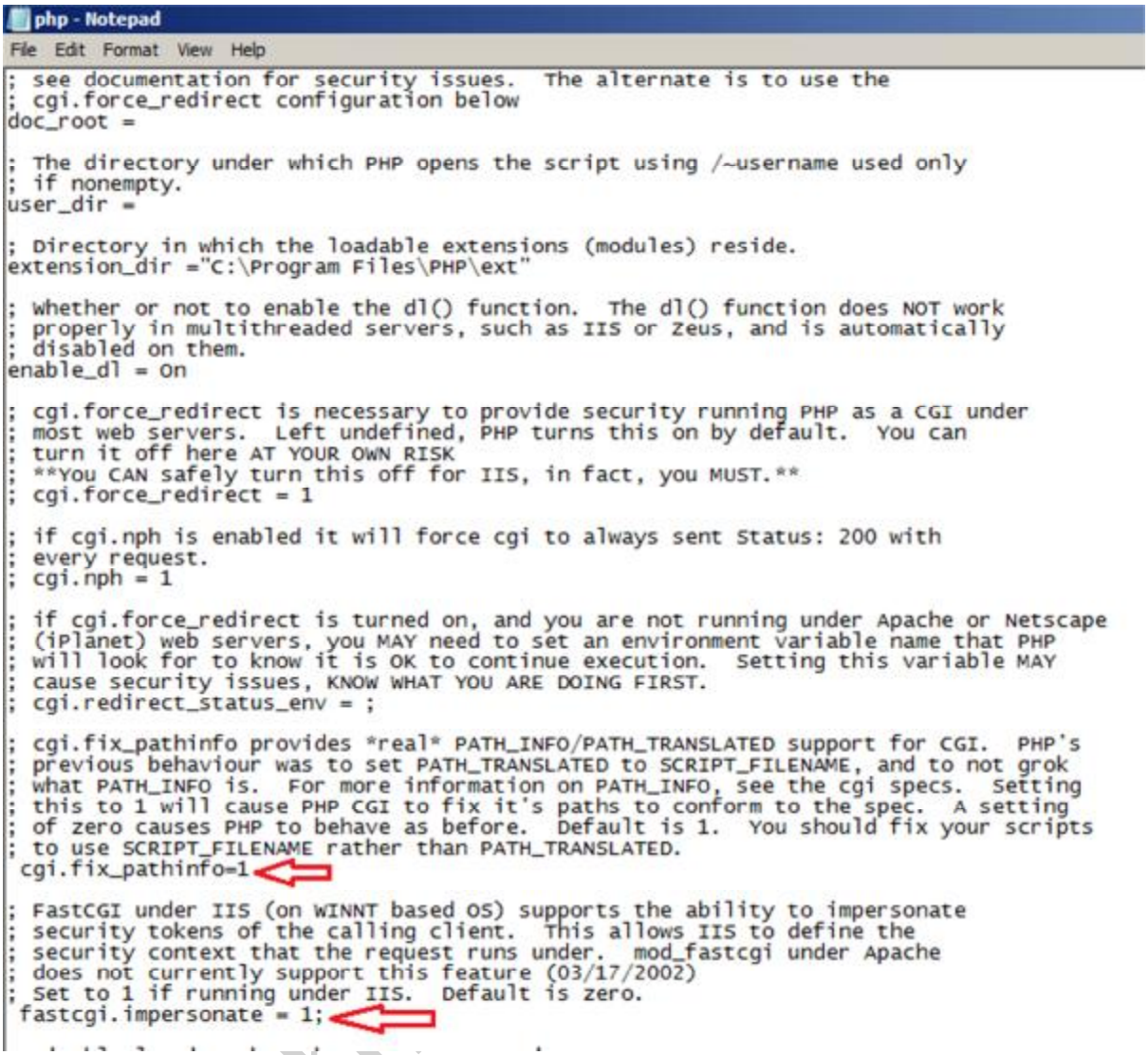
**بعد از نصب آن را اجرا می کنیم**

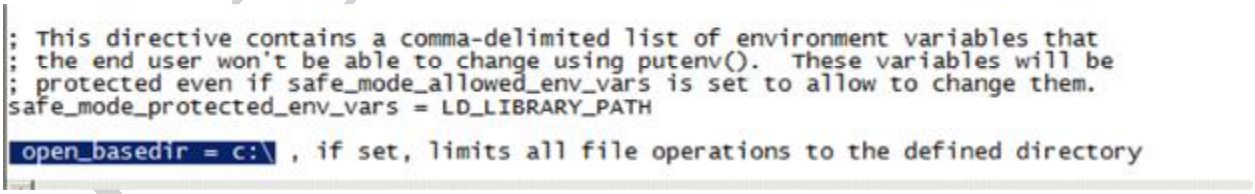



**بعد از اجرا یک Notepad باز می شود که باید3 عبارت** cgi.fix_pathinfo=1 , ;fastcgi.impersonate=1 ; , open_basedir; **رابیابیم و علامت ; را از پشت آنها حذف کنیم (با حذف ; آن دستور قابلیت اجرایی پیدا می کند) و در خط سوم باید دستوری را هم اضافه کنیم:** open_basedir= c:\

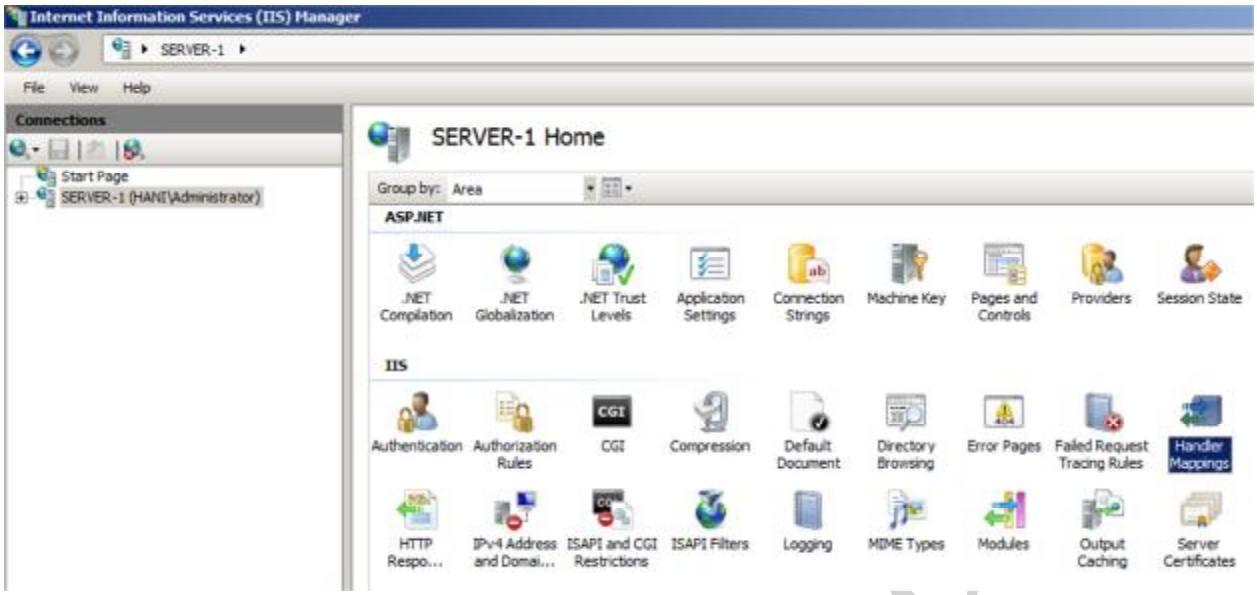


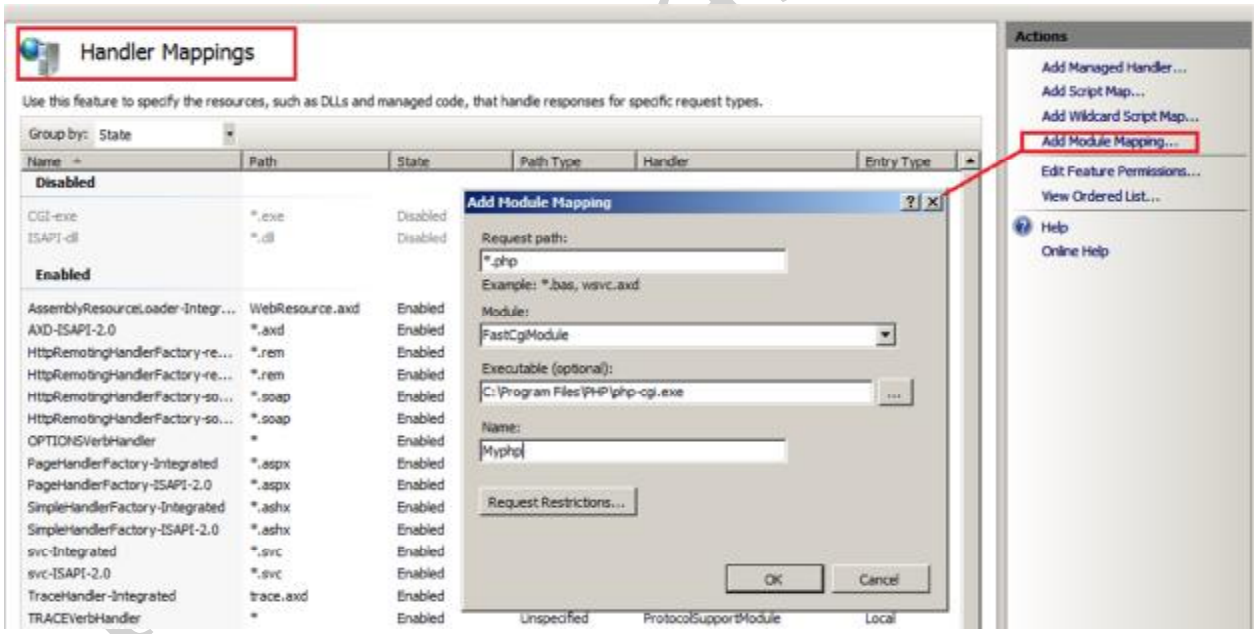
FarshidAjabnoush




برای اینکه IIS بتواند صفحات phph را پشتیبانی کند ابتدا وارد آن شده و مانند زیر عمل می کنیم




سپس یک سایت php را راه اندازی می کنیم.

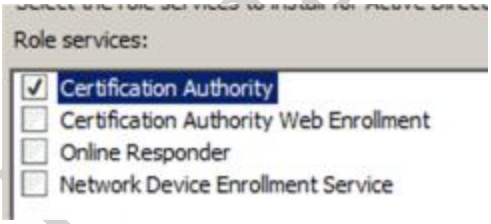
HTTPS با IIS7

زمانی که بخواهیم از https استفاده کنیم باید یک CA Server هم پشت سایتمان داشته باشیم,سناریو به این صورت می باشد که زمانی که کلاینت به یک سایت https وصل می شود آن سایت بر اساس درخواست به CA وصل می شود وCA 2کلید تولید می کند Public و Private , Public را در اختیار کلاینت می گذارد و از این پس کلاینت به صورت https به سایت وصل می شود و Private در اختیار سایت قرار می گیرد.

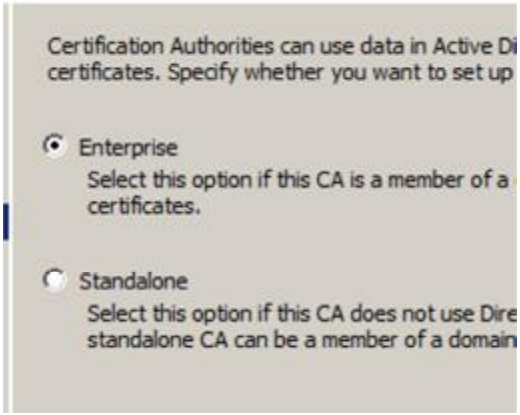
- SSL Bridge سرویسی است که می توان بین کلاینت و اینترنت فعال کرد و توسط آن ترافیک های SSL را مشاهده کرد (بر روی ISA قابل پیاده سازی می باشد-بدون متوجه شدن کلاینت ها)

پیاده سازی CA

ابتدا باید AD نصب شود,سپس IIS را نصب می کنیم و در آخر هم CA نصب می کنیم

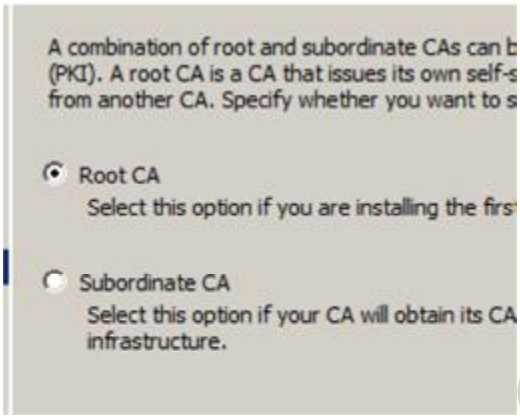


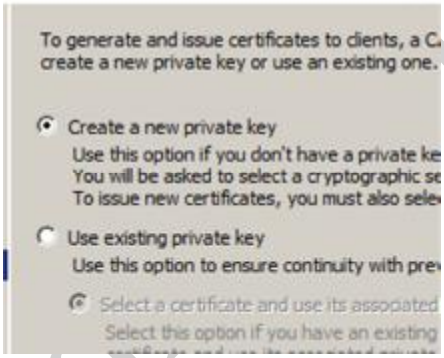

اگر CA و AD پشت یک سرور باشد گزینه اول و اگر از هم جدا باشند گزینه دوم.

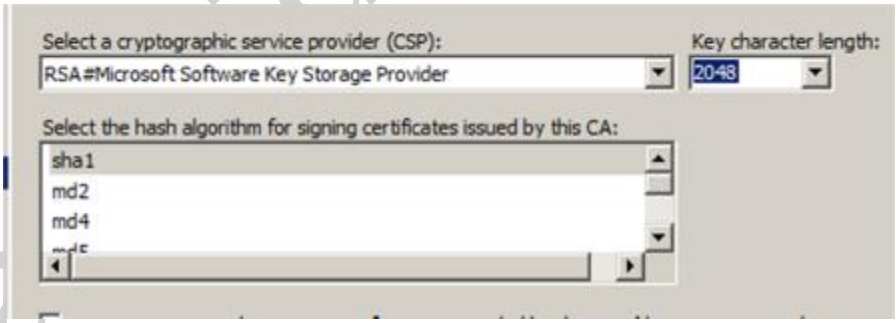


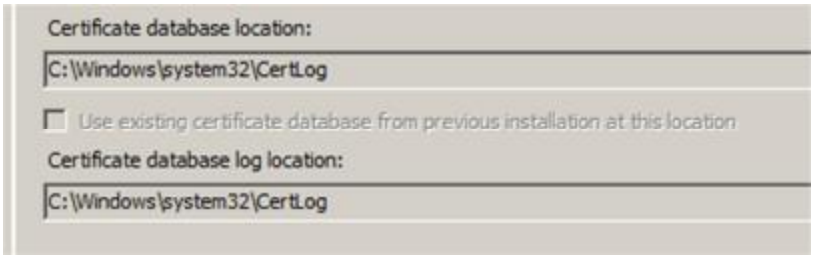

Farshidianoush

اگر CA ما اصلی (اولین) در شبکه خودمان باشد گزینه1 و اگر زیر مجموعه CA دیگری می باشد گزینه دوم



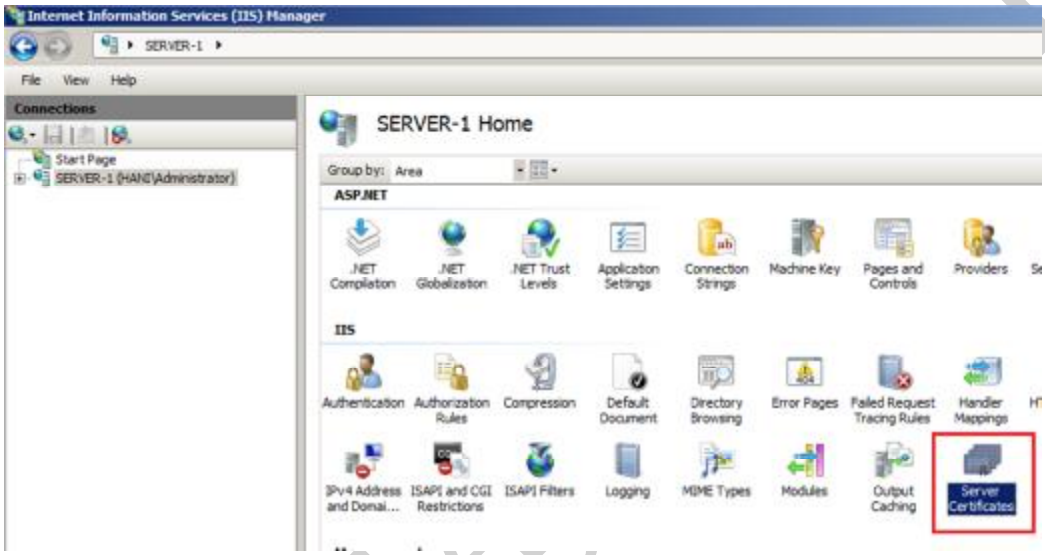

همیشه باید مسیر بالا را حفظ کنیم,برای Backup گرفتن.

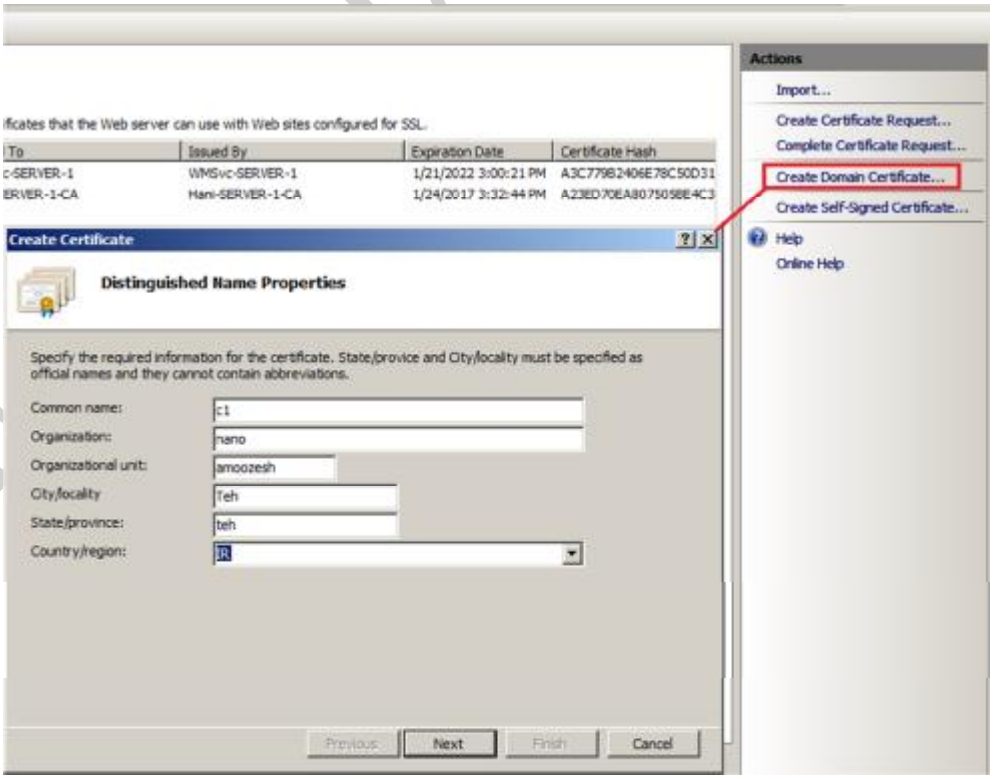
Fa...oush

- بهترین نرم افزار Backup در شبکه Symantec Backup EXEC می باشد.
- در Workgroup برای نصب CA گزینه Standalone را انتخاب می کنیم.
- بهترین نرم افزار برای دانلود کردن مطالب از سایت های پولی,Blackwidow می باشد.

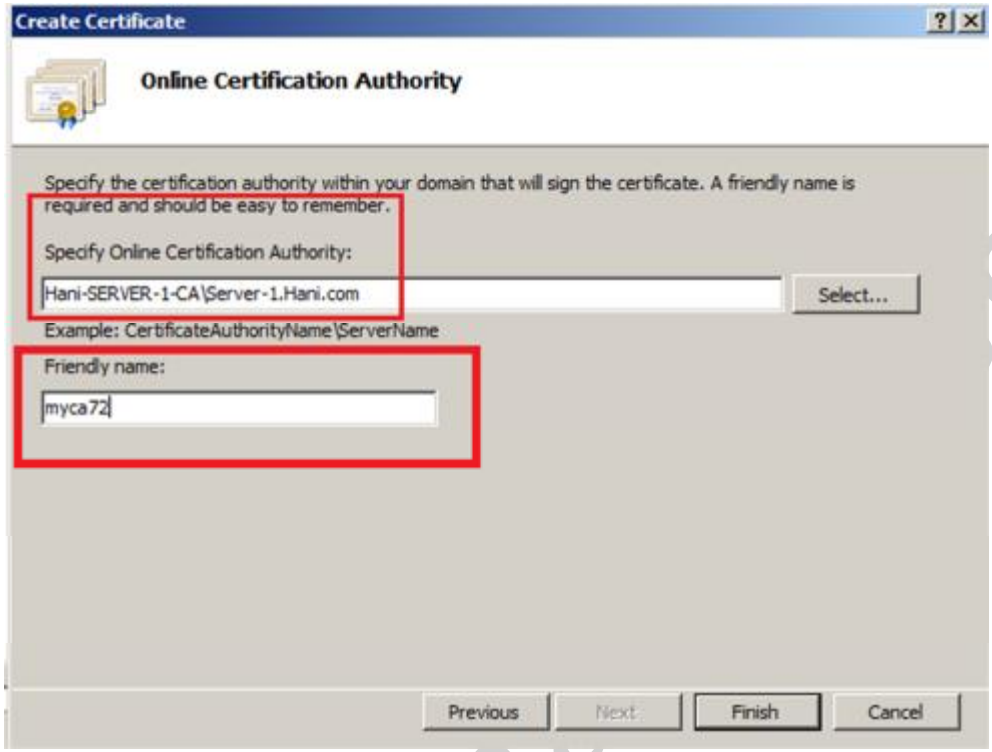
**بعد از نصب CA نوبت به معرفی CA به IIS می باشد برای این کار مانند زیر عمل می کنیم**

**وارد IIS می شویم**

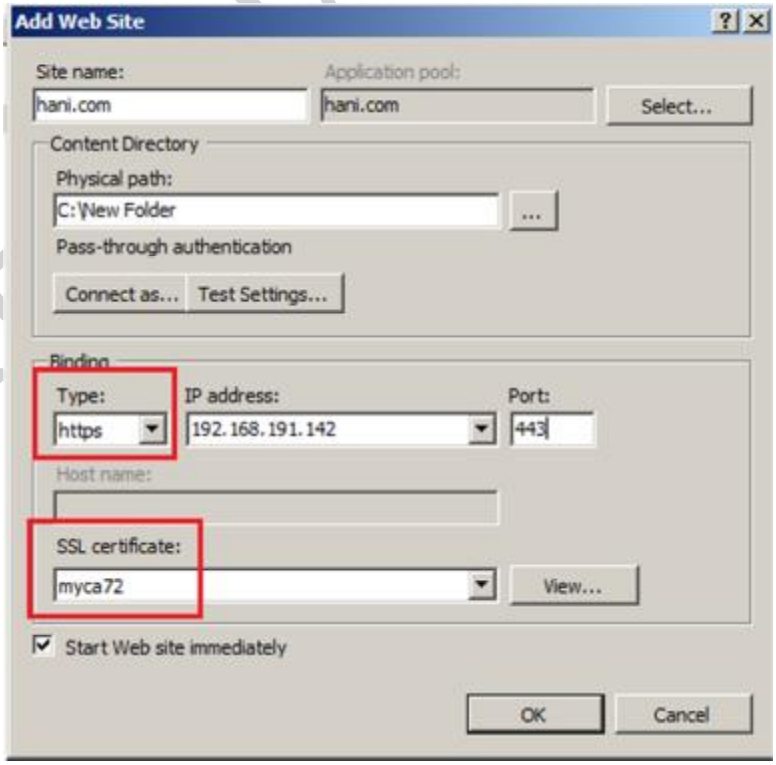


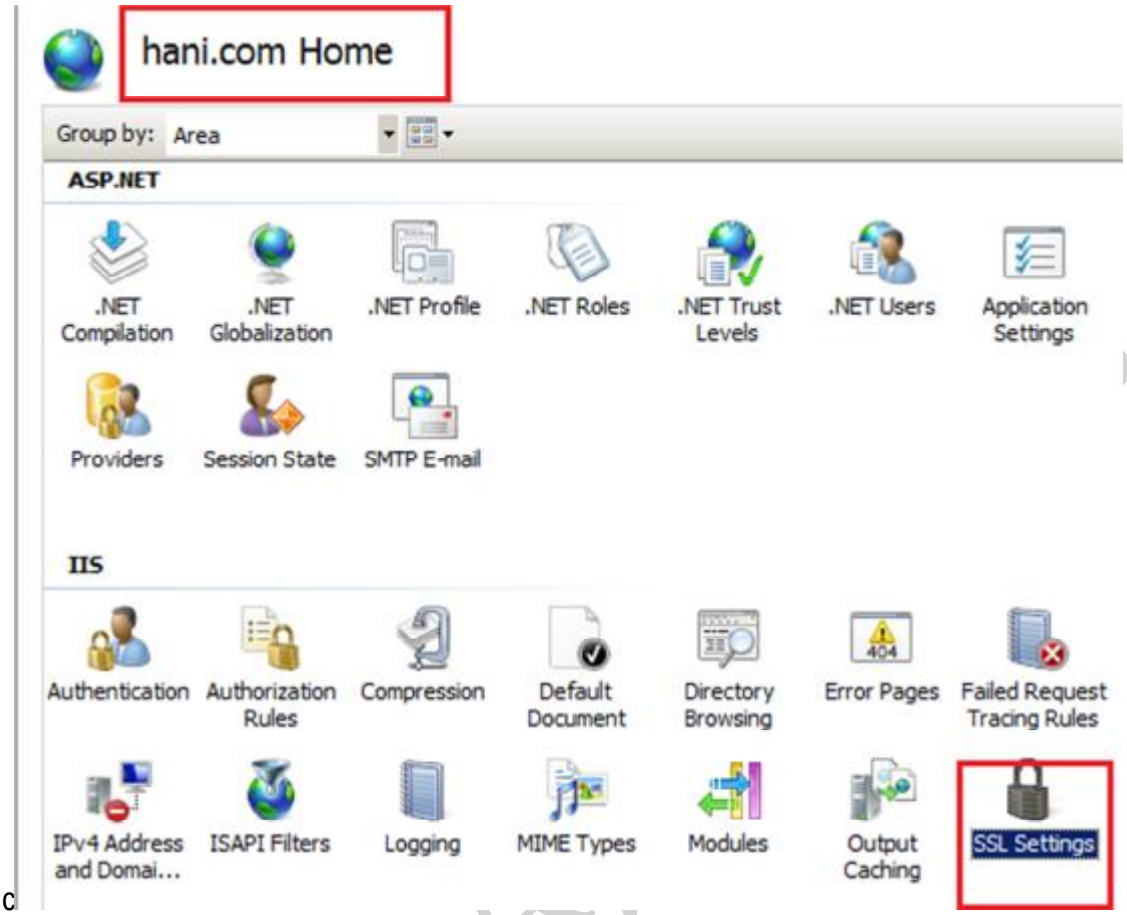
Select را می زنیم و سرور را انتخاب می کنیم,Friendly name خیلی مهم است(به خاطر بسپارید)



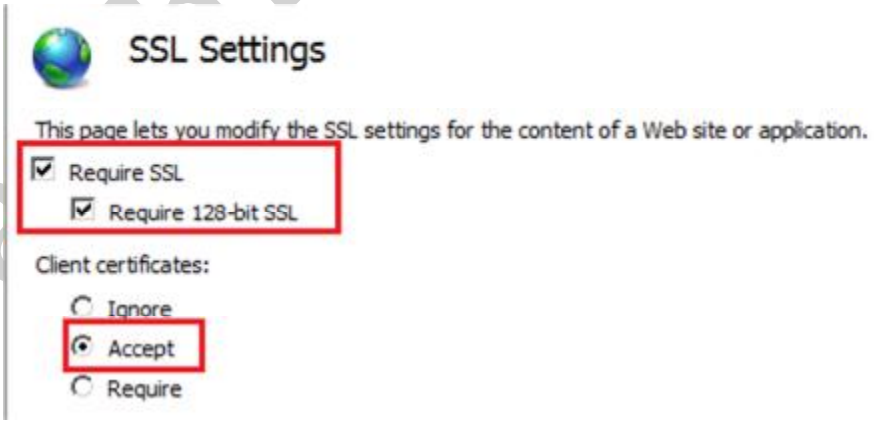

سپس وارد IIS می شویم وسایتی را که ساخته بودیم را اضافه می کنیم( ARecord,Cname)



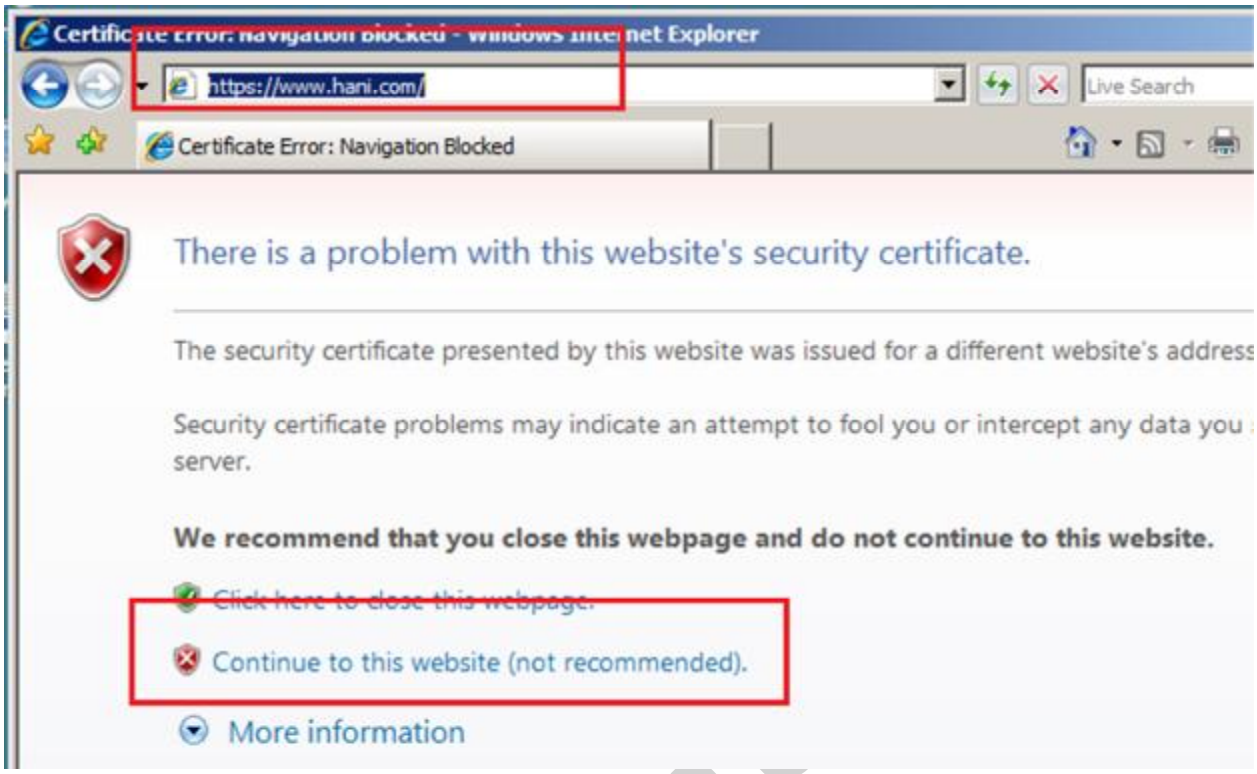

Farhad Ajdari




در اینجا تعیین می کنیم که فقط سایت را با ssl باز کن, در قسمت دوم می گوییم اگر CA از طرف ما بر روی کلاینت بود آن را هم قبول کن.




سپس وقتی وارد سایت می شویم با مشکل زیر مواجه می شویم به این دلیل می باشد که CA ما از جای معتبر تامین نمی شود.

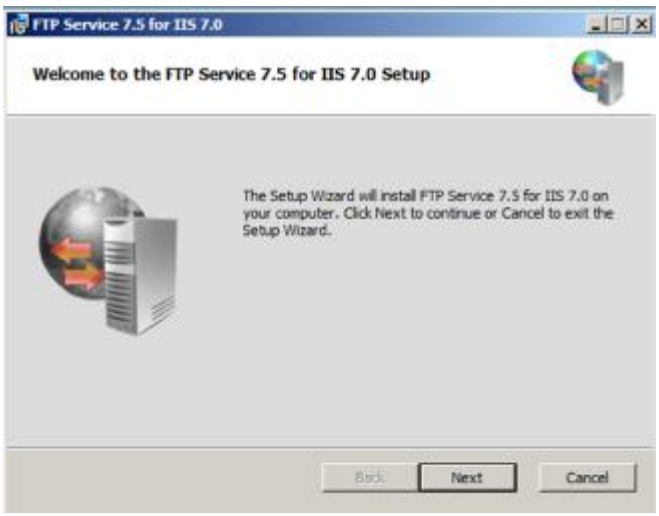



FTP در IIS

به صورت پیش فرض FTP موجود روی IIS7 , FTP 6 می باشد باید FTP 7.5 را از IIS.Net دانلود و نصب کنیم.

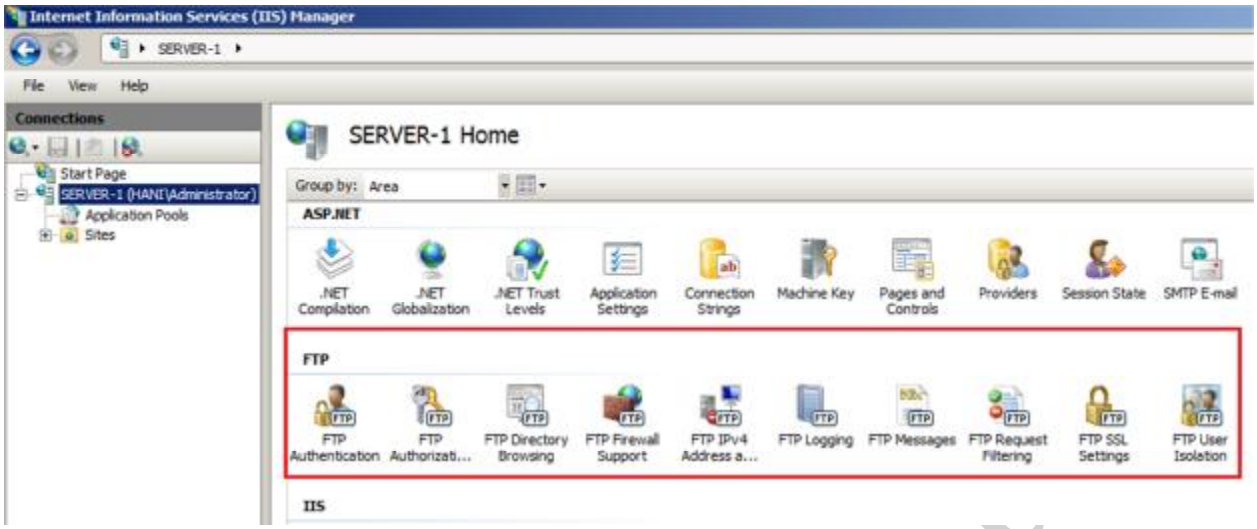
- بهترین نرم افزار FTP ,File Zilla می باشد

نصب FTP7

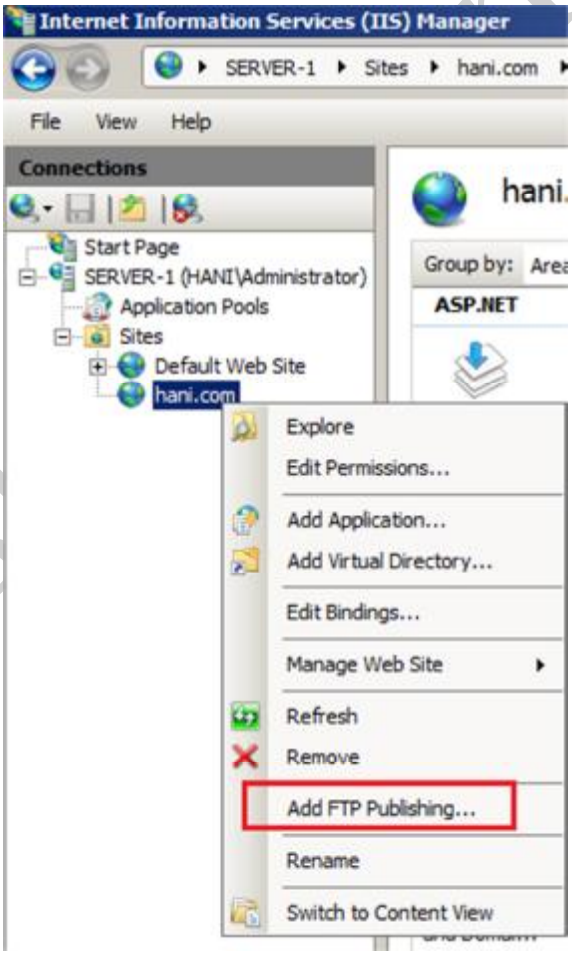



بعد از نصب واردIIS می شویم

FarshidAja




**برای اینکه ویژگی FTP را به سایتی اضافه کنیم**




Farsi

- برای بدست آوردن پسوردهای Hash شده از نرم افزارAbleCain & و سایت Passcracking.com کمک می گیریم.

Nap (Network Access Protection)

وظیفه این سرویس چک کردن سلامتی کلاینت هایی است که قصد گرفتن سرویس از شبکه مارا دارند.

سلامتی کلاینت ها از NAP یعنی دارا بودن 4 شرط: 1- Firewall is on 2- Antivirus update 3- Windows update 4- Spyware update

NAP 5 سرور را می تواند چک کند 1- DHCP 2- VPN 3- IPSEC 4- TerminalServer 5- Wireless (802.1)

به 5 سرور بالا که در صورت سالم بودن می توانند سرویس بدهند, از دیدگاه NAP , Information Point گویند.

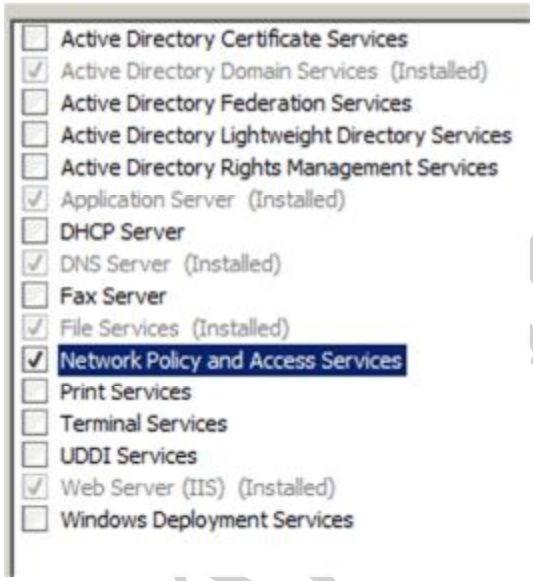
- NAP در 2003 موجود نمی باشد.

تمامی کلاینت ها سرویسی بر روی خود دارند به نام StateHealth Agent کار این سرویس این می باشد که از وضعیت سلامتی سیستم گزارشی تهیه کند به آن گزارش State Out Health گویند,این گزارش به NAP سرور

ارسال می شود و NAP با استفاده از State Health Validator ,این سرویس به سلامتی سیتم(از روی گزارش) یک Grade (رتبه) می دهد سپس سروری به نام NPS بر اساس آن Grade دسترسی لازم را برای کلاینت فعال می کند.

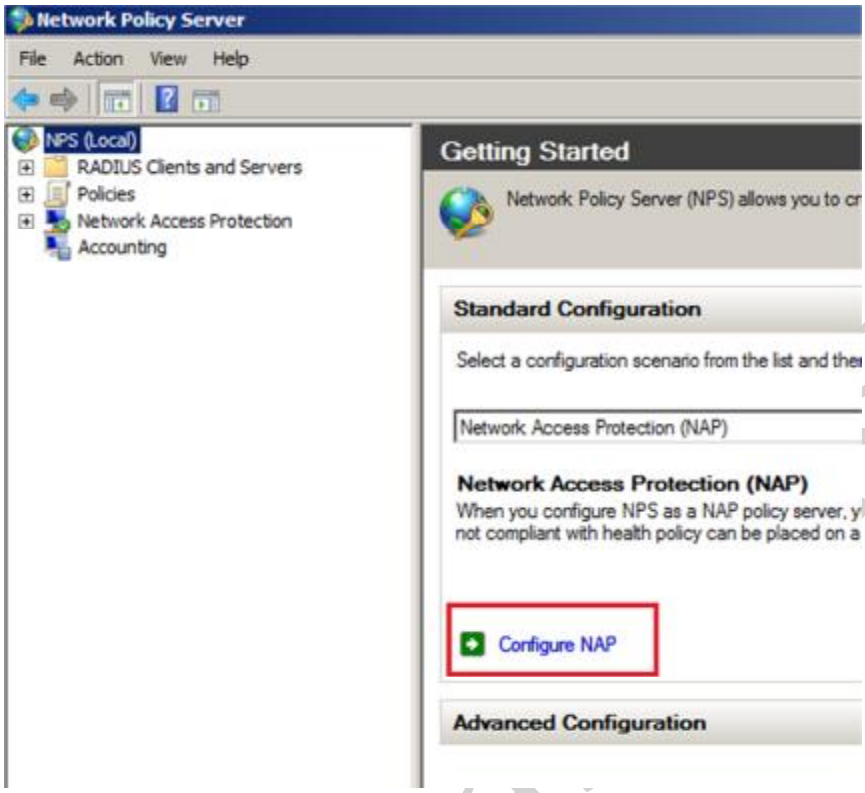
- SHA فقط بر روی xp sp3,vista sp1,7,2008 موجود می باشد.

راه اندازی NAP

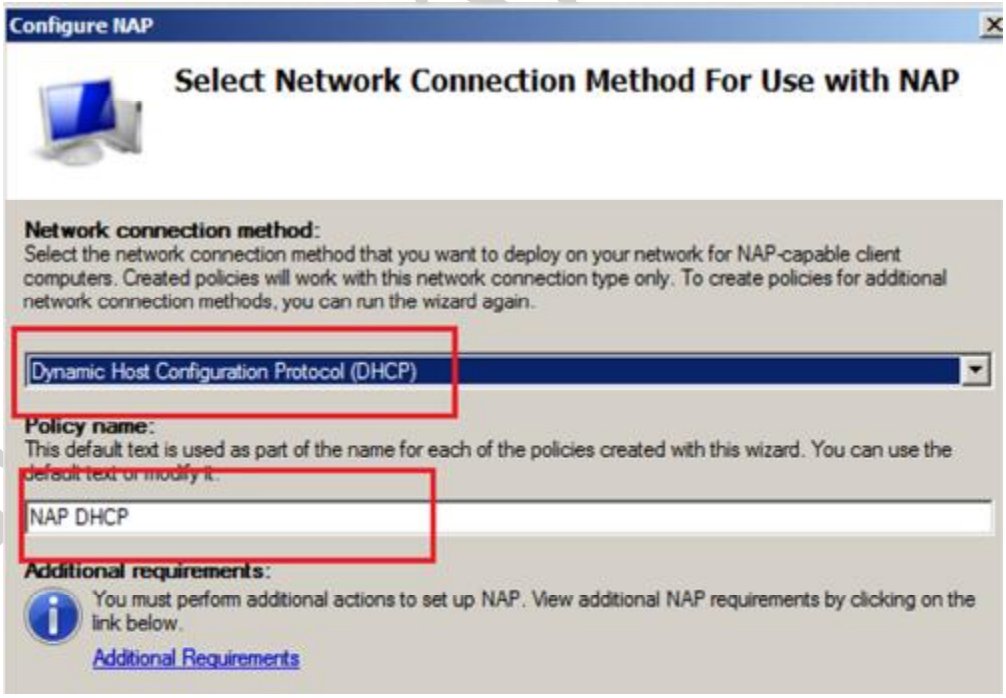


بعد از نصب مانند زیر عمل می کنیم

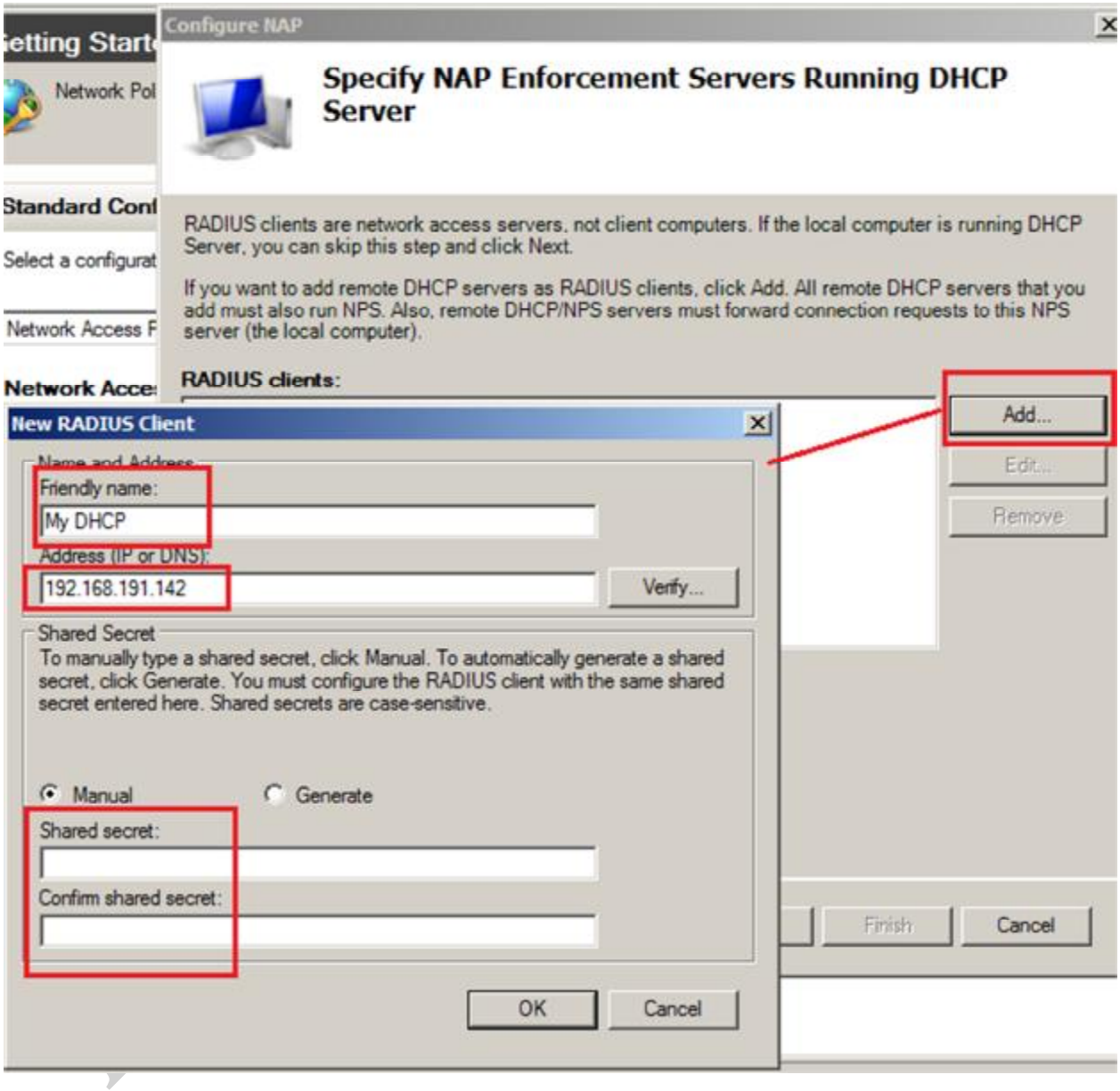
FarshidAyoush



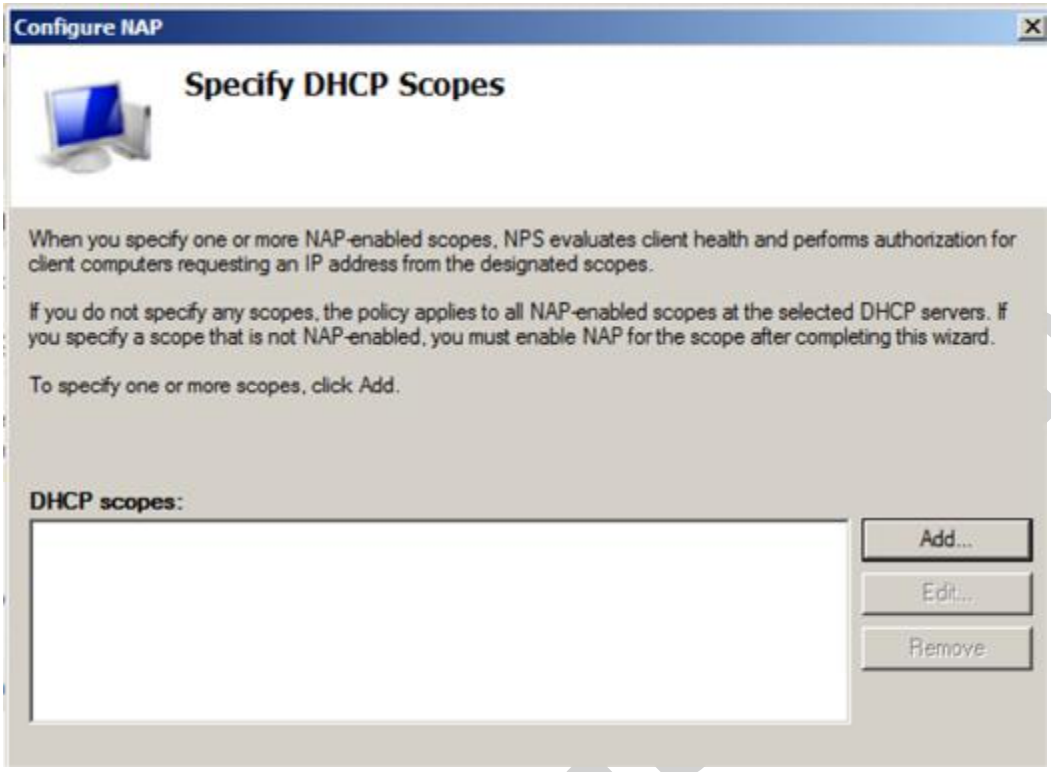

در این قسمت باید مشخص کنیم که NAP را برای کدام از5 سرور اجرا می کنیم,سپس یک اسم انتخاب می کنیم.



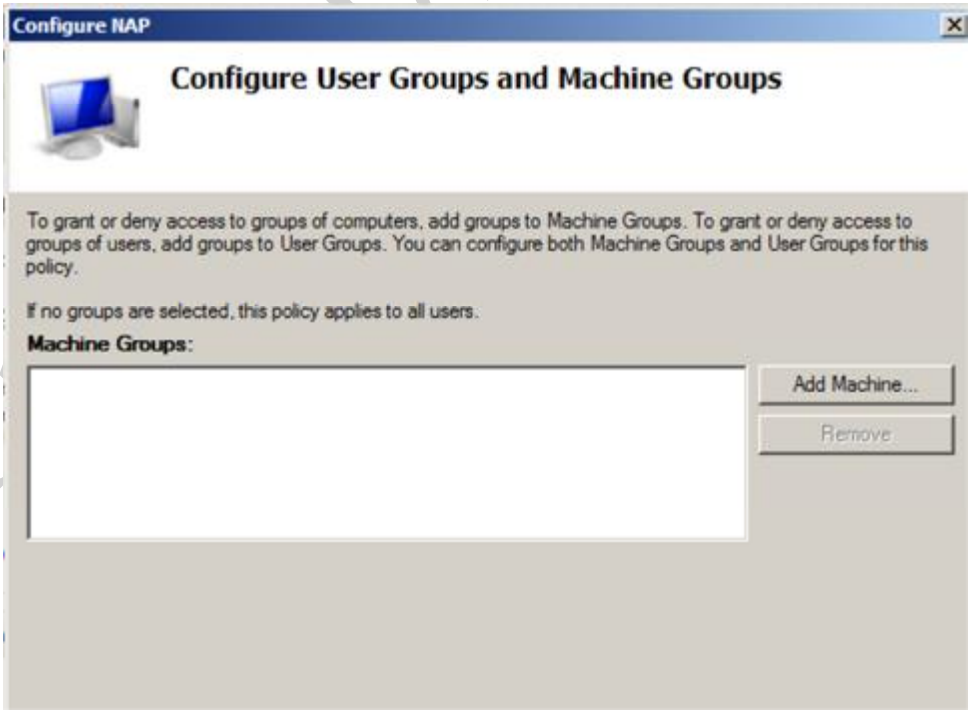
نوبت به معرفی سرور انتخابی می رسد,یک اسم انتخاب می کنیم سپس Ip آن سرور را وارد می کنیم در قسمت آخر می توانیم یک پسورد تعیین کنیم.



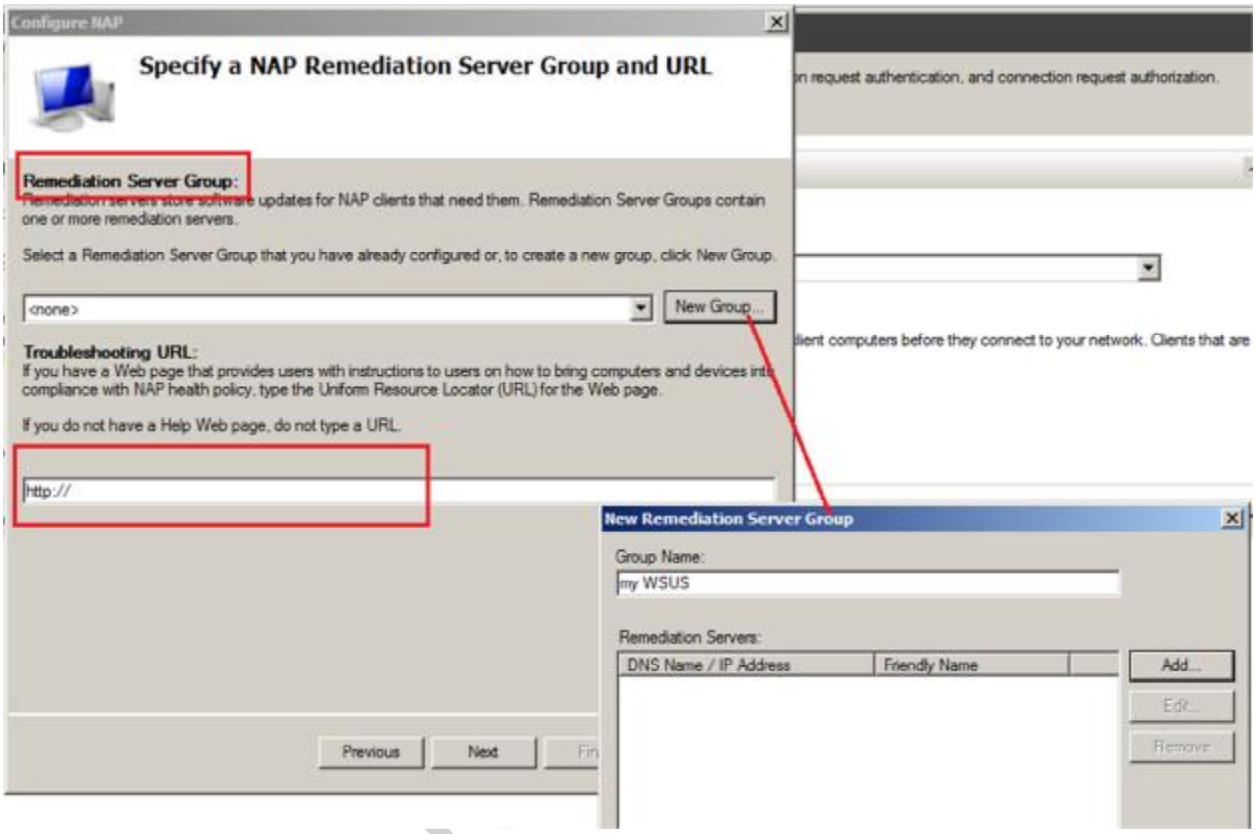

در مرحله بعد می توانیم Scope خاصی را برای سرور مشخص کنیم که آن را چک کند,اگر مشخص نکنیم منظور تمامی Scope ها می باشد.




**در مرحله بعد می توان کامپیوتر یا یوزر خاصی را معرفی کرد که سلامتی آن حتما چک شود,اگر اسمی وارد نکنیم به صورت پیش فرض تمامی سیستم ها را چک می کند.**

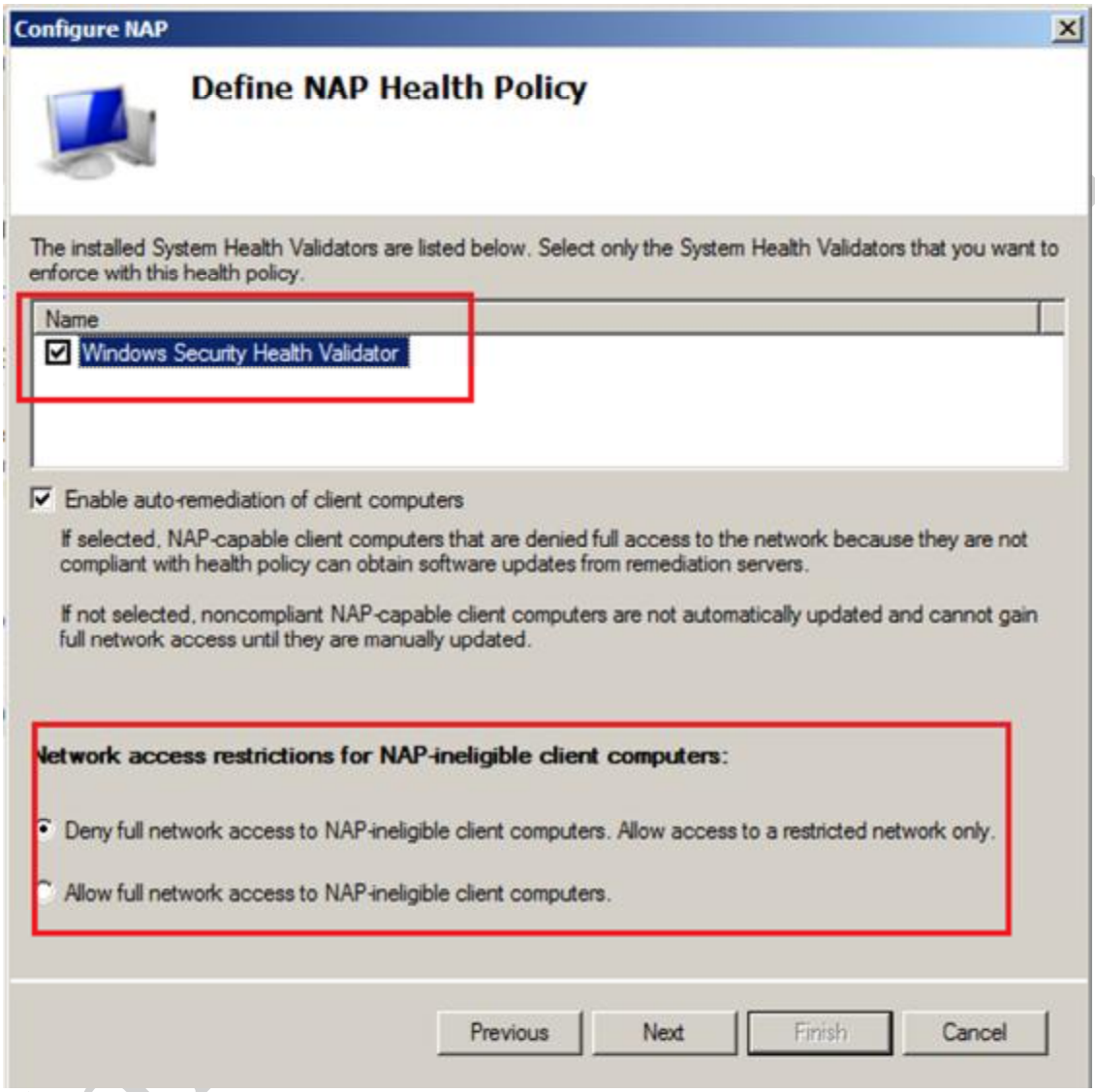


در این مرحله باید مشخص کنیم که اگر سیستمی دارای مشکل بود به سمت کدام سرور یا سایتی برود که بتواند مشکلش را برطرف کند



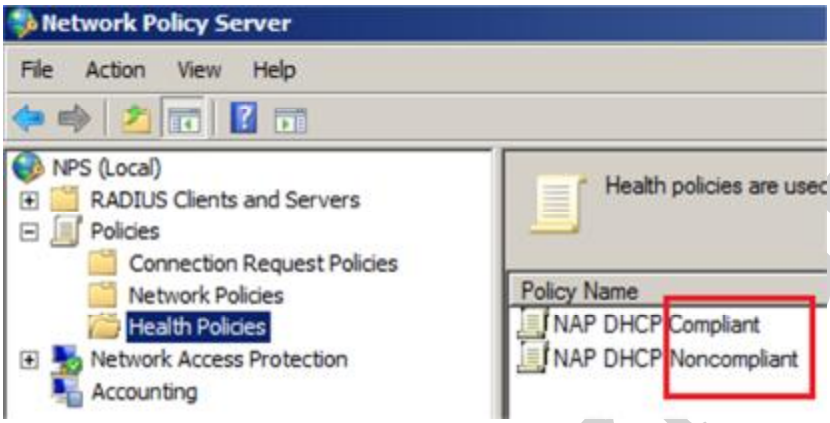

در مرحله بعد در قسمت اول سرور که رتبه می دهد را مشخص کرده و در قسمت دومش می پرسد که اگر سیستمی NAP را متوجه نمی شود چه کاری باید انجام دهم ؟ گزینه ...Deny را انتخاب می کنیم

Farshi

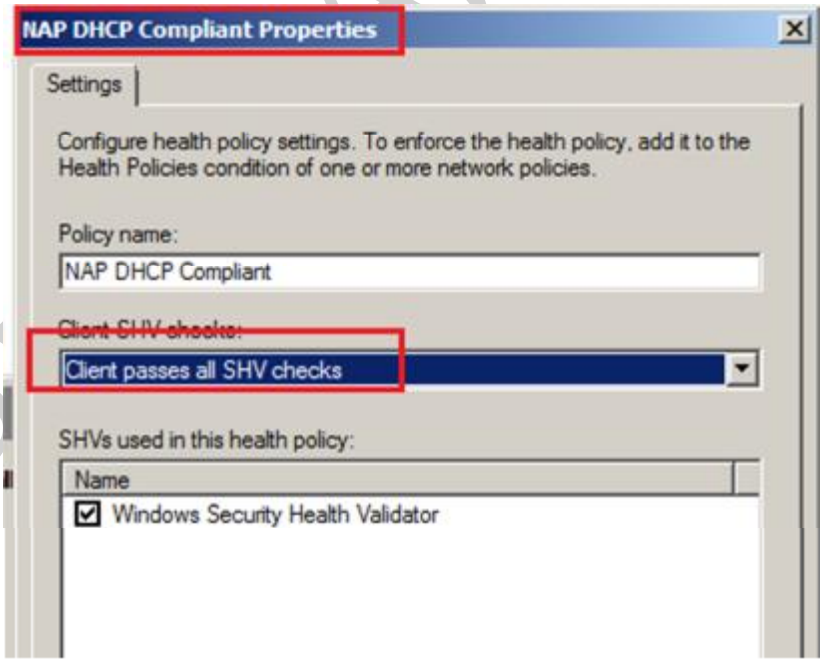

Configure NAP
Define NAP Health Policy
The installed System Health Validators are listed below. Select only the System Health Validators that you want to enforce with this health policy.
Name
Windows Security Health Validator
Enable auto-remediation of client computers
If selected, NAP-capable client computers that are denied full access to the network because they are not compliant with health policy can obtain software updates from remediation servers.
If not selected, noncompliant NAP-capable client computers are not automatically updated and cannot gain full network access until they are manually updated.
Network access restrictions for NAP-ineligible client computers:
Deny full network access to NAP-ineligible client computers. Allow access to a restricted network only.
Allow full network access to NAP-ineligible client computers.
Previous
Next
Finish
Cancel

در این مرحله باید مشخص کنیم که سیستم ها کدام شروط را پاس کنند که سالم باشند و کدام شروط می باشد که اگر پاس نشود سیستم نا سالم می باشد.

Compliant سالم, Noncompliant ناسالم




با کلیک کردن بر روی Complint صفحه زیر باز می شود که می توانیم مشخص کنیم که کدام شروط باید پاس شود تا سیستم سالم به نظر آید.

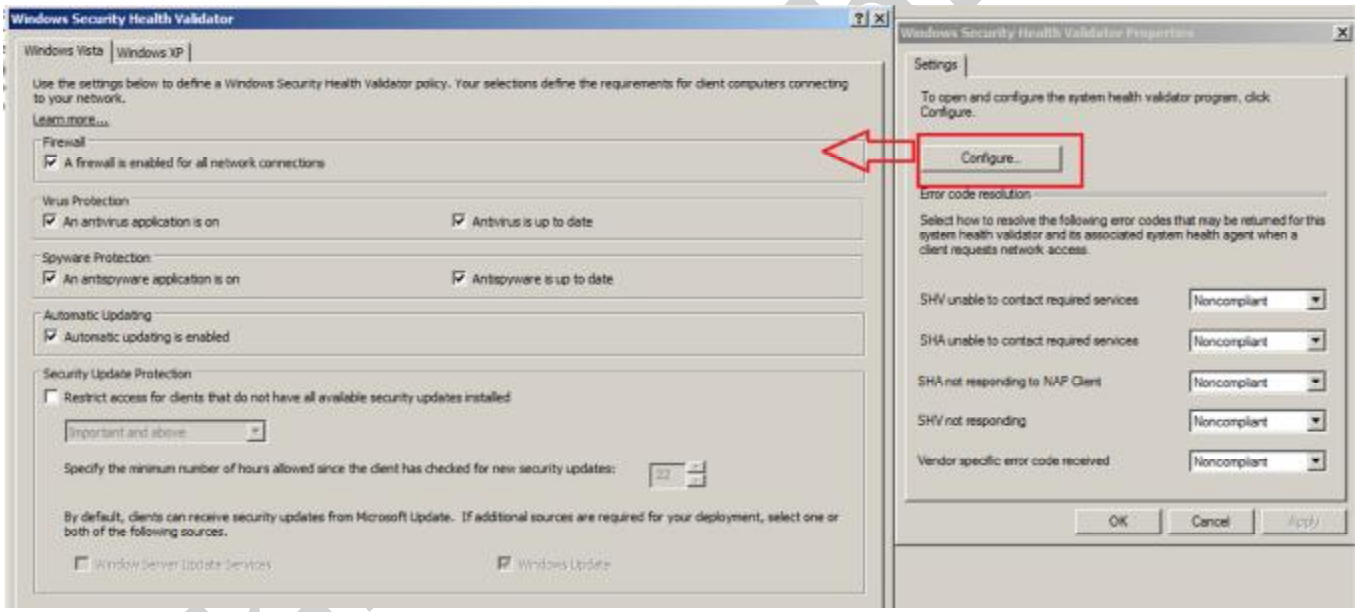



- بهتر است بر روی All SHV نباشد.

Fa Niabi sh

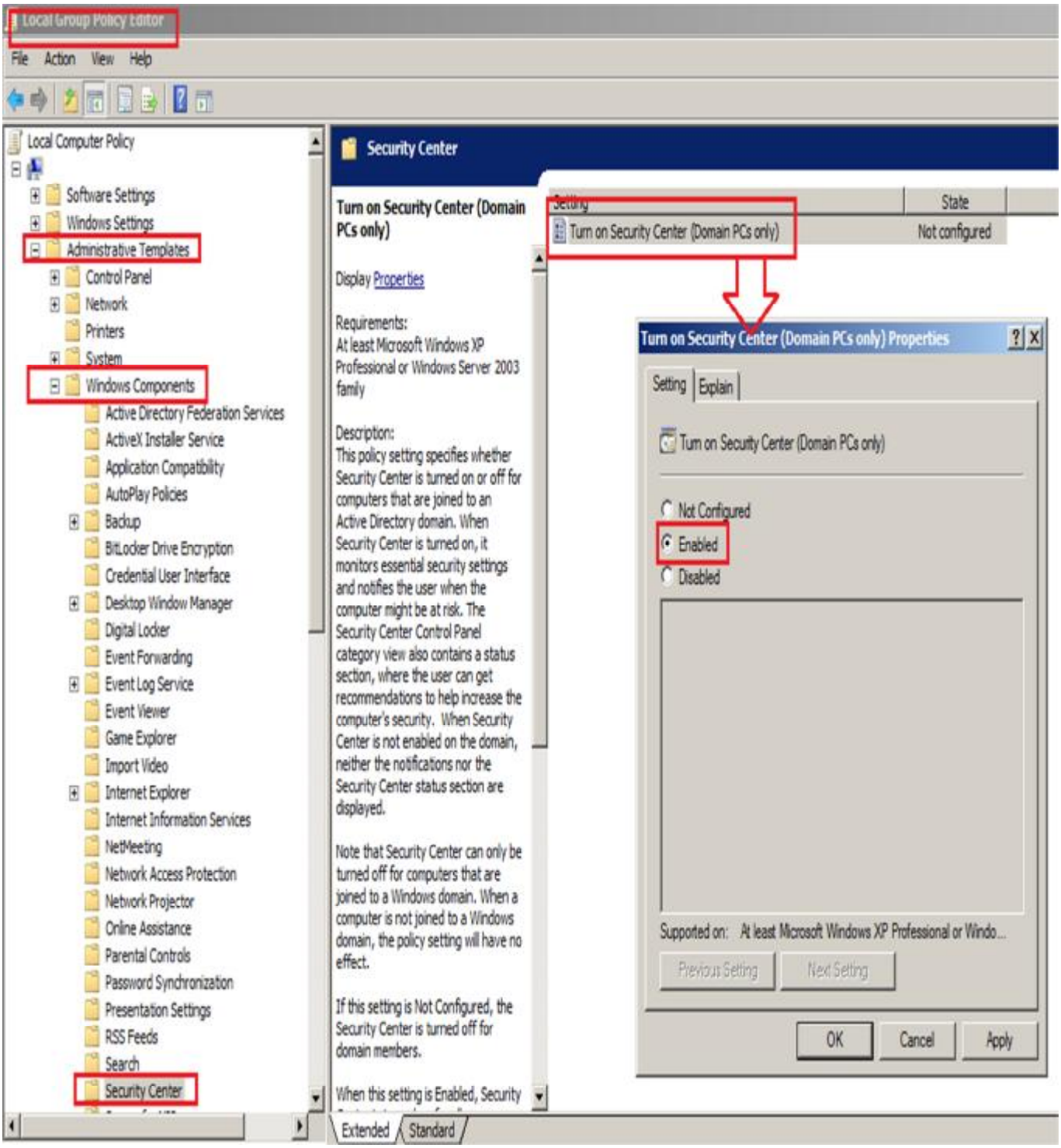
سپس وارد مرحله بعد می شویم

در اینجا می توانیم مشخص کنیم که برای ویندوزهای vista و xp چه چیزهایی باید برای سلامتی چک شود.




- سرور از Security Center ویندوز تمامی مشخصات سلامتی را چک می کند,در شبکه های دایمنی Security Center کلاینت ها غیر فعال می باشد برای فعال سازی باید مانند زیر عمل کنیم

از پشت سرور وارد گروپ پالیسی می شویم:


Local Group Policy Editor
File Action View Help
Local Computer Policy
Software Settings
Windows Settings
Administrative Templates
Control Panel
Network
Printers
System
Windows Components
Active Directory Federation Services
ActiveX Installer Service
Application Compatibility
AutoPlay Policies
Backup
BitLocker Drive Encryption
Credential User Interface
Desktop Window Manager
Digital Locker
Event Forwarding
Event Log Service
Event Viewer
Game Explorer
Import Video
Internet Explorer
Internet Information Services
NetMeeting
Network Access Protection
Network Projector
Online Assistance
Parental Controls
Password Synchronization
Presentation Settings
RSS Feeds
Search
Security Center
Security Center
Turn on Security Center (Domain PCs only)
Display Properties
Requirements:
At least Microsoft Windows XP Professional or Windows Server 2003 family
Description:
This policy setting specifies whether Security Center is turned on or off for computers that are joined to an Active Directory domain. When Security Center is turned on, it monitors essential security settings and notifies the user when the computer might be at risk. The Security Center Control Panel category view also contains a status section, where the user can get recommendations to help increase the computer's security. When Security Center is not enabled on the domain, neither the notifications nor the Security Center status section are displayed.
Note that Security Center can only be turned off for computers that are joined to a Windows domain. When a computer is not joined to a Windows domain, the policy setting will have no effect.
If this setting is Not Configured, the Security Center is turned off for domain members.
When this setting is Enabled, Security
Setting
State
Turn on Security Center (Domain PCs only)
Not configured
Turn on Security Center (Domain PCs only) Properties
Setting
Explain
Turn on Security Center (Domain PCs only)
Not Configured
Enabled
Disabled
Supported on: At least Microsoft Windows XP Professional or Windo...
Previous Setting
Next Setting
OK
Cancel
Apply
Extended
Standard

Directory Service

سرویسی است که می تواند منابع یک شبکه را برای مدیریت آسان تر در یک مکان جمع آوری کند.

دایرکتوری سرویس مایکروسافت Active Directory می باشد.

اکتیو دایرکتوری از لحاظ ساختاری از2 قسمت تشکیل شده است 1- Logical Infrastructure 2 – Physical Infrastructure

در قسمت Logical , Object –OU-Domain-Child-Domain Tree-Forest وجود دارند.

در قسمت Physical , Domain Controler (DC)-Active Directory Site وجود دارند.

Object : به هر چیزی که داخل شبکه های دامینی برای مدیریت آن شبکه ساخته می شود را Object گویند مانند Group و....

- تمامی Object ها دارای Properties و SID مخصوص به خودشان هستند,Properties تمامی Object ها داخل قسمتی به نام Schema ذخیره می شوند, Object ها به روش های ADUC,ADCommand Line Tools,VBScript,Powershell,LDIFDE,CSVDE
- به گروه نمی توان Polisy اعمال کرد ولی بهOU می توان.
- به گروه Permission می توان اعمال کرد.
- برای اینکه بخواهیم به User پالیسی اعمال کنیم ابتدا باید آن را داخل OU قرار دهیم و سپس به آن OU پالیسی را اعمال کنیم به این کار Nesting گویند.
- Global Catalog : به سروری که تمامی اطلا عات (user,group,ou,...) کل شبکه را دارد,به صورت پیش فرض Global Catalog شبکه,RootDomain می باشد.
- می توان Clobal Catalog را هم ایجاد کرد(یعنی علاوه بر rootdomain),این کار را برای شبکه های بزرگ انجام می دهیم.
- هنگام Join شدن کلاینت به شبکه,کلاینت پوشه Sysvol را بر روی خود کپی می کند.
- پروتکل احراز هویت شبکه های دامینی Kerberos می باشد,user & Passرا از Global Catalog می پرسد ( پورت Kerberos ,88 می باشد)
- Ticket Grant Ticket : نسبت به یوزر لاگین شده در شبکه های دامینی دسترسی می دهد ,می توان برای این بلیط ها طول عمر تعیین کرد,به صورت پیش فرض 10 ساعت اعتبار دارد و بعد از 7 روز هم Expire می شود,قبل از 7 روز باید یک بار Log off کند تا Expire نشود.
- PS Tools نرم افزاری می باشد که می تواند تمامی یوزرهای پشت یک سیستم را نشان دهد.
- LDAP پروتکل جست وجو داخل شبکه های دامینی می باشد(پورت آن 389 می باشد )
- پورت DNS 53 می باشد.

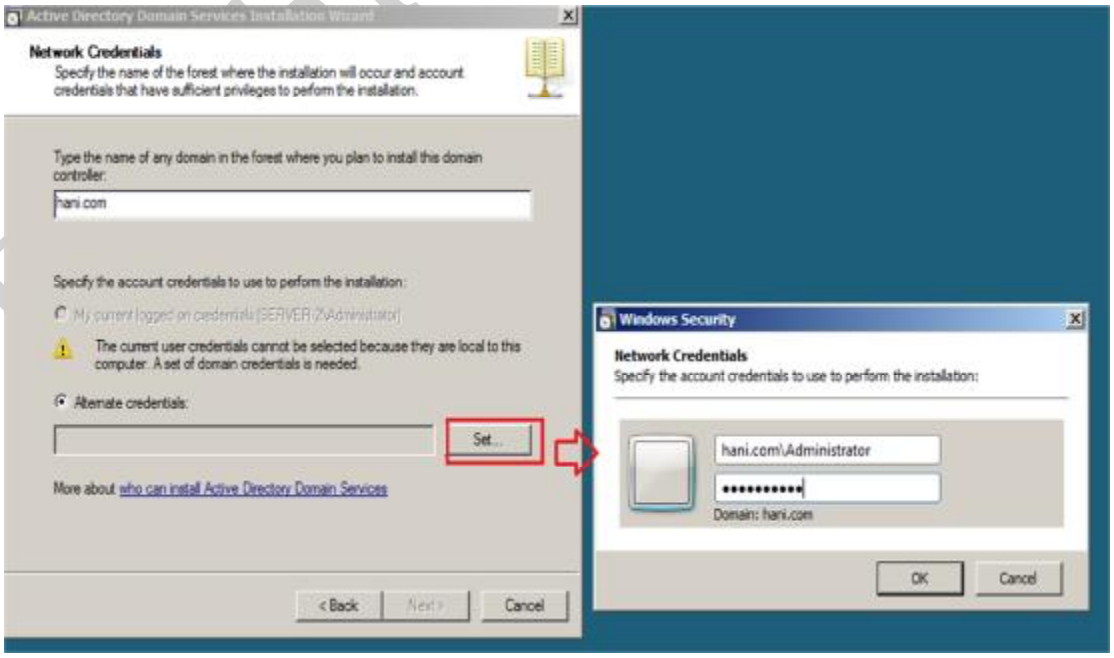
FarshidArabnoush

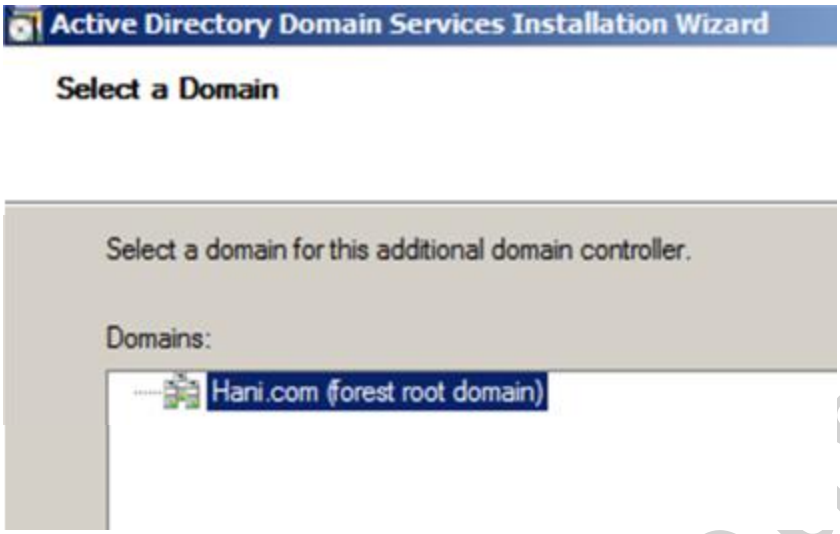
- اگر ما بین کلاینت ها و سرور اکتیو فایروال داشته باشیم برای اینکه بتوانیم کلاینت ها را Join کنیم باید 3 پورت 53-389-88 را بر روی فایروال باز کنیم.
- برای نصب اکتیو باید Ip Static بر روی کارت شبکه داشته باشیم.

برای ساختن BDC مانند زیر عمل می کنیم

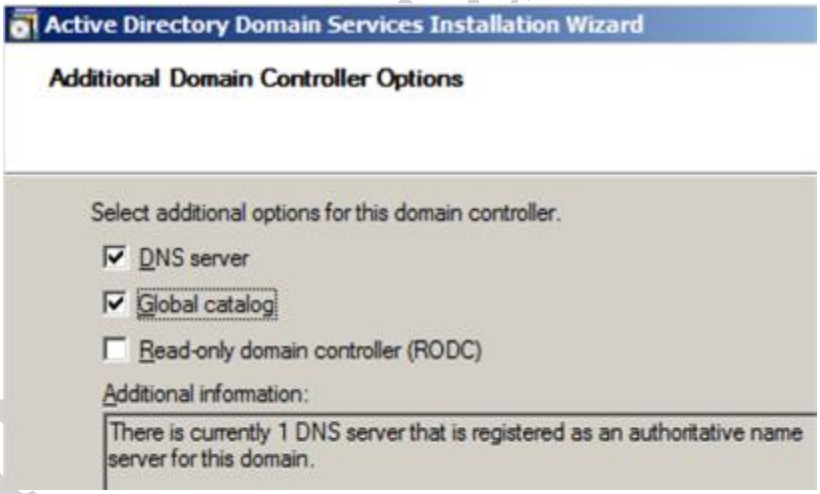
در اینجا می خواهیم یک BDC برای Root Domain ایجاد کنیم

- قبل از این کار باید Root Domain, Ip را بر روی BDC, DNS تنظیم کنیم(علاوه بر Ip Static )



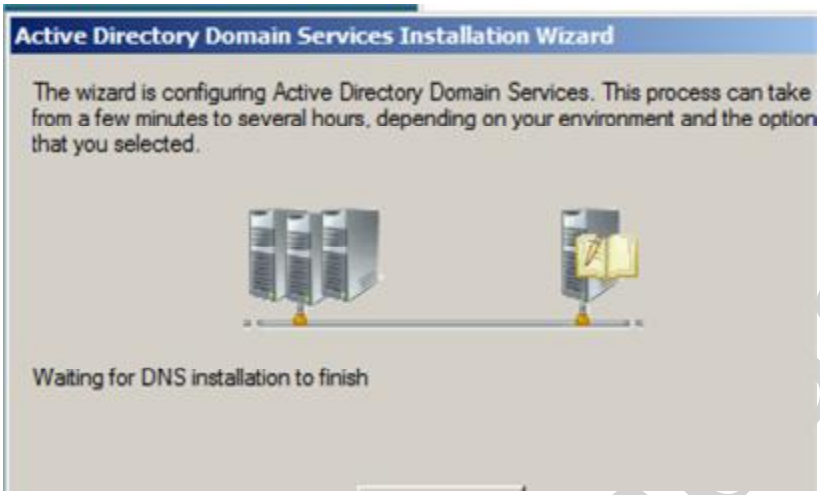



بهتر است بر روی این BDC , Global Catalog فعال باشد که اگر Root Domain, Global از کار افتاد مشکلی پیش نیاید ولی برای BDC های Child ها نباید این کار را بکنیم چون ترافیک شبکه زیاد می شود.




- زمانی که در سرور Primary تغییری اتفاق می افتد بر روی سرور BDC هم این عمل انجام می شود،به این عمل در اصطلاح Replicate گفته می شود.

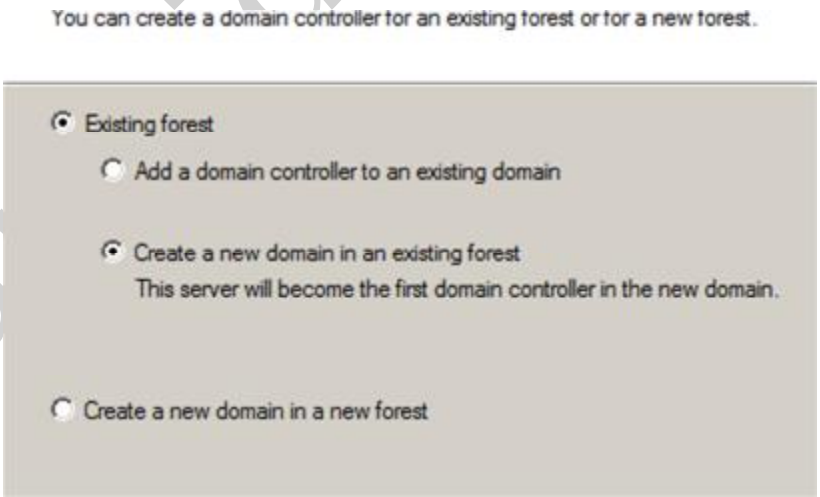
Farsiabnoosh



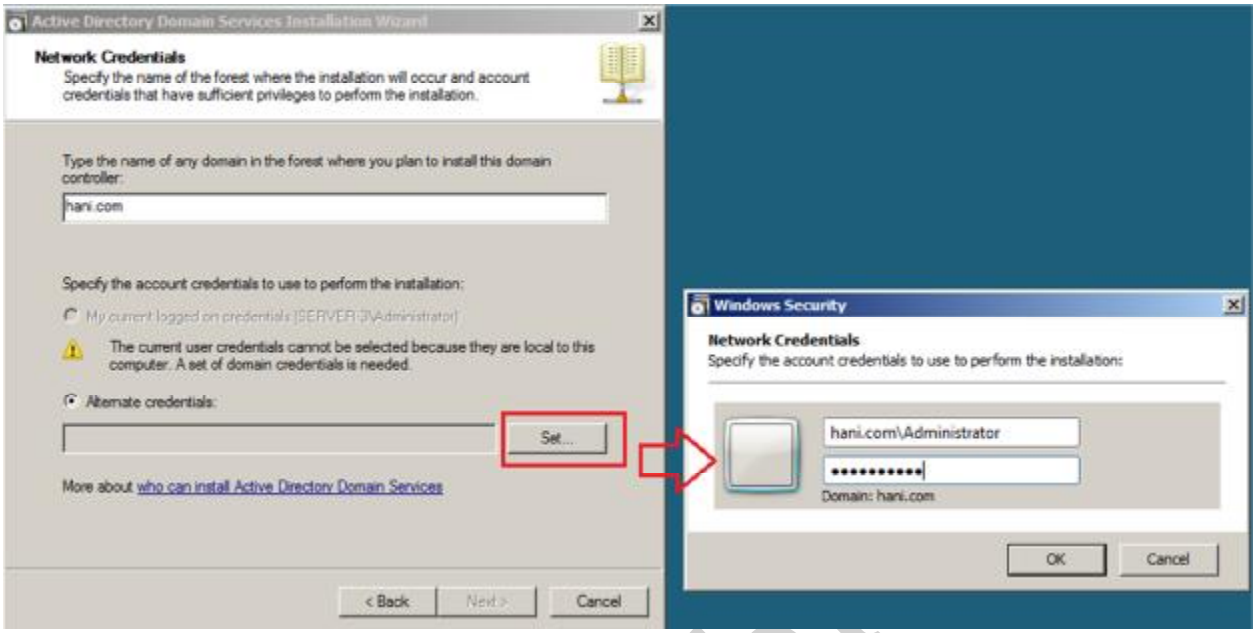

- برای Root Domain نباید به صورت DNS, Static تنظیم کنیم.

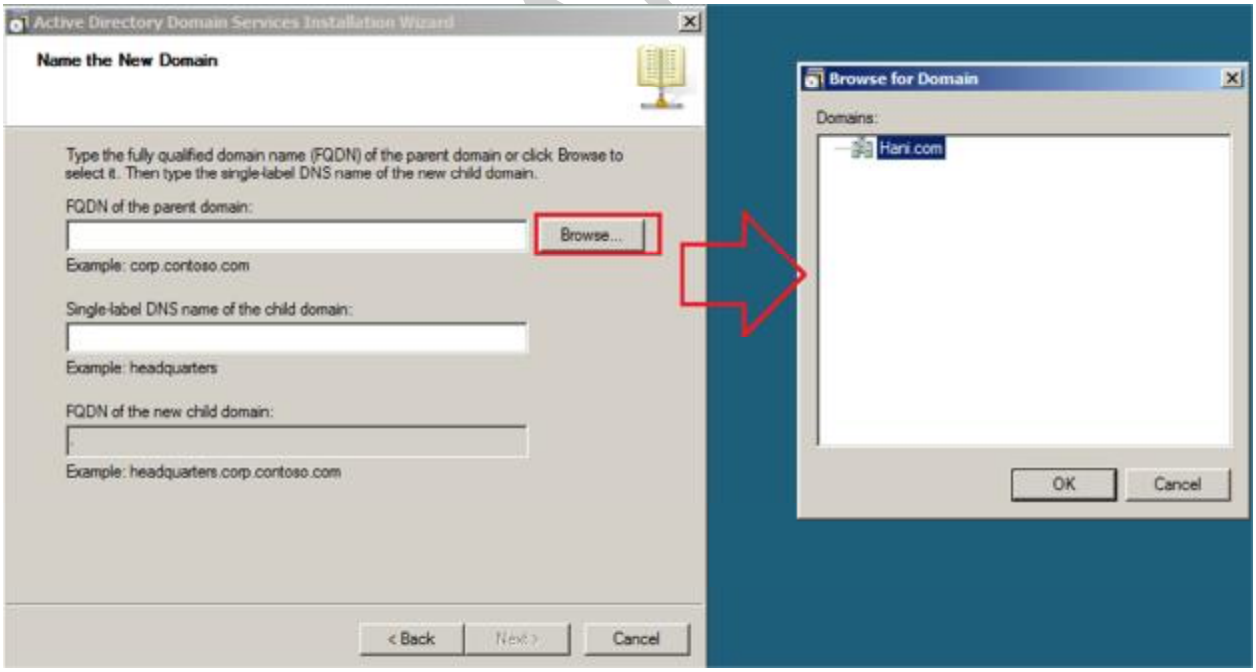
**ایجاد Child**

**برای این کار هم باید Ip بالاسر Child را به جای DNS برای Child تنظیم کنیم(علاوه بر Ip Static )**

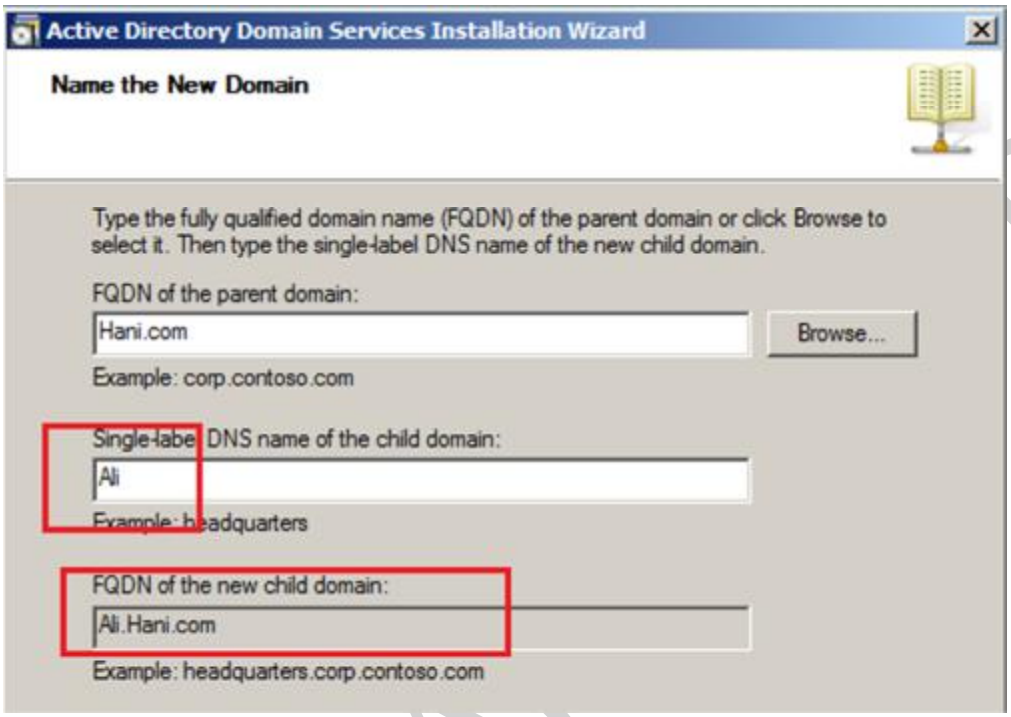



FaridAjabnoush


Active Directory Domain Services Installation Wizard
Network Credentials
Specify the name of the forest where the installation will occur and account credentials that have sufficient privileges to perform the installation.
Type the name of any domain in the forest where you plan to install this domain controller:
hani.com
Specify the account credentials to use to perform the installation:
My current logged on credentials [SERVER1\Administrator]
The current user credentials cannot be selected because they are local to this computer. A set of domain credentials is needed.
Alternate credentials:
Set...
More about who can install Active Directory Domain Services
< Back
Next >
Cancel
Windows Security
Network Credentials
Specify the account credentials to use to perform the installation:
hani.com\Administrator
Domain: hani.com
OK
Cancel

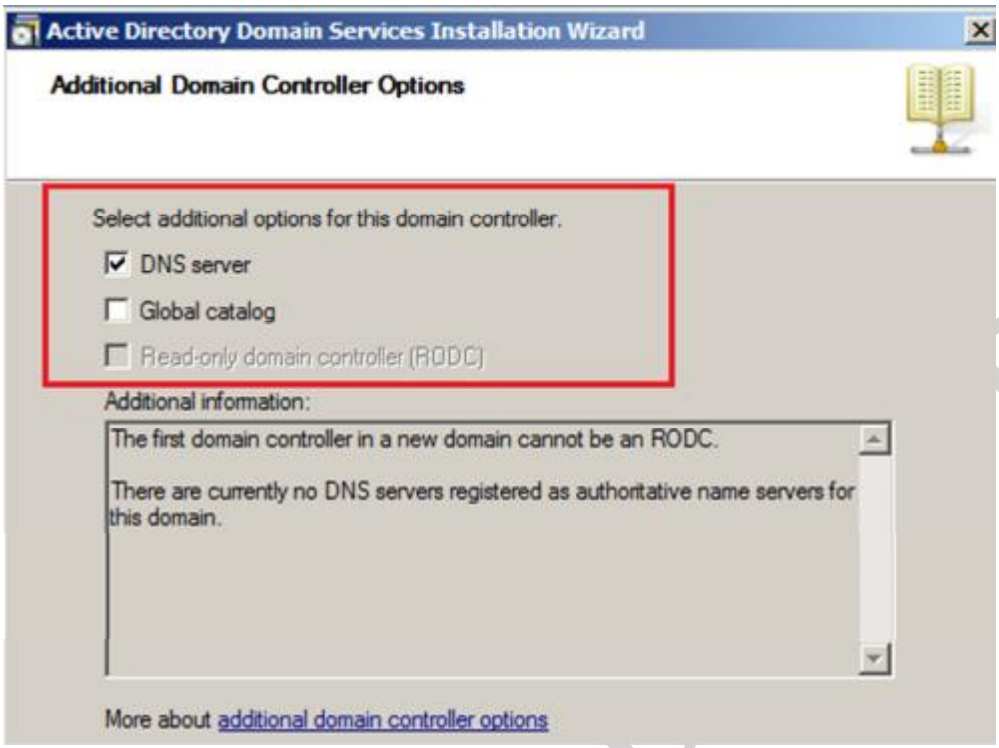

Active Directory Domain Services Installation Wizard
Name the New Domain
Type the fully qualified domain name (FQDN) of the parent domain or click Browse to select it. Then type the single-label DNS name of the new child domain.
FQDN of the parent domain:
Browse...
Example: corp.contoso.com
Single-label DNS name of the child domain:
Example: headquarters
FQDN of the new child domain:
Example: headquarters.corp.contoso.com
< Back
Next >
Cancel
Browse for Domain
Domains:
Hani.com
OK
Cancel

در اینجا باید اسم Child (Ali ) را وارد کنیم,در قسمت پایین می بینیم که یک پسوند به آن اضافه می شود

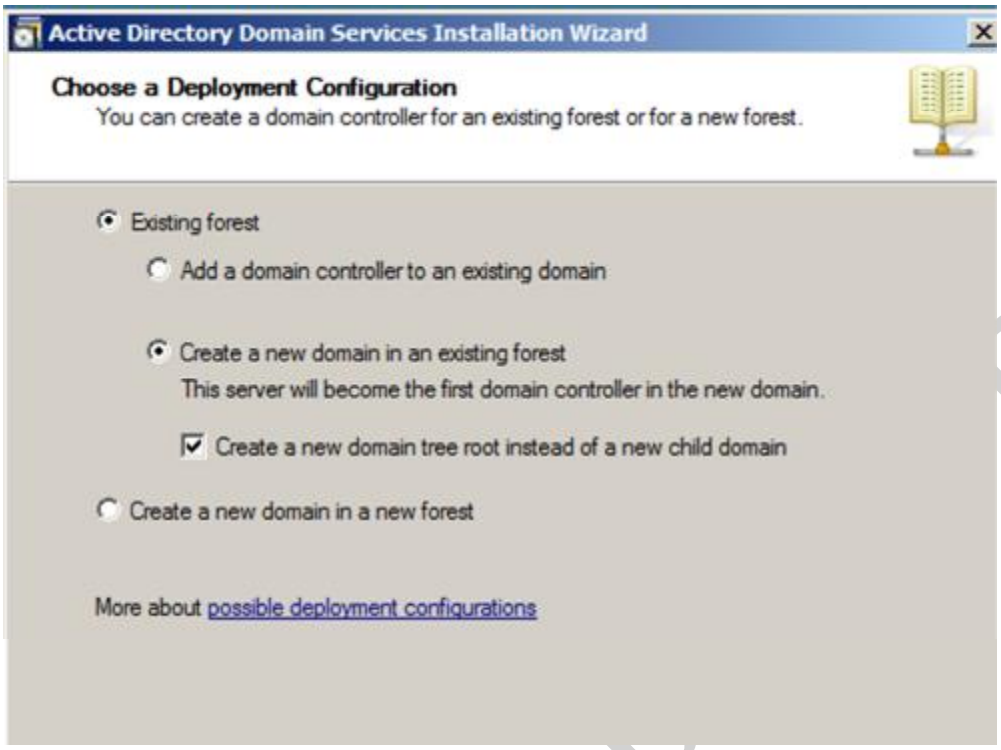


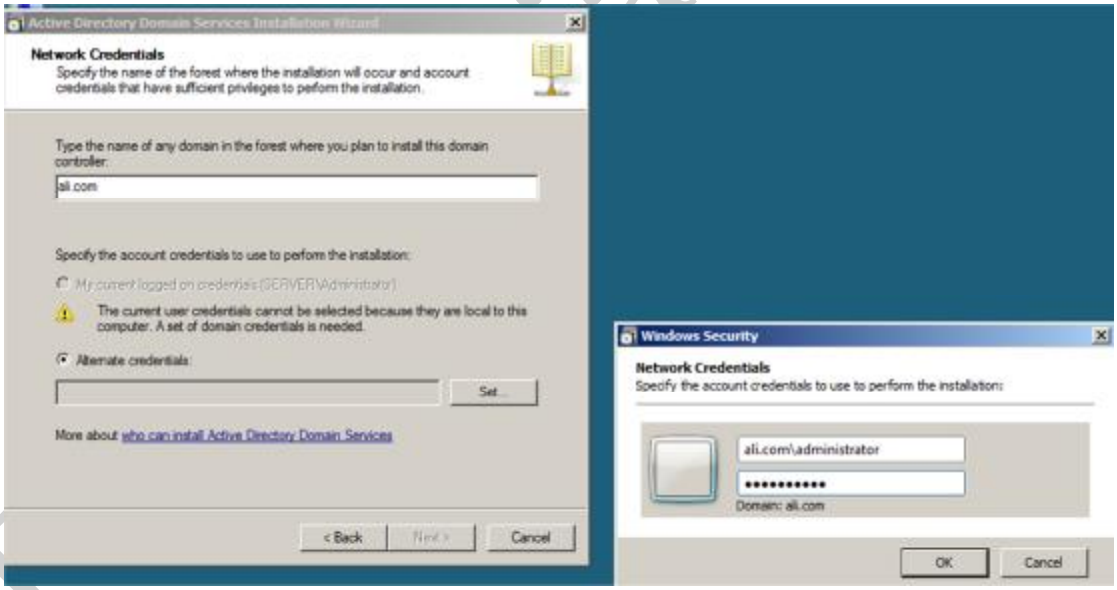

در اینجا RODC غیرفعال می باشد به این دلیل که اولین سرور در مثلث جدید می باشد و باید قابلیت نوشتن را داشته باشد.

FarshidAghaei




پیاده سازیDomain Tree


Active Directory Domain Services Installation Wizard
Choose a Deployment Configuration
You can create a domain controller for an existing forest or for a new forest.
Existing forest
Add a domain controller to an existing domain
Create a new domain in an existing forest
This server will become the first domain controller in the new domain.
Create a new domain tree root instead of a new child domain
Create a new domain in a new forest
More about possible deployment configurations


Active Directory Domain Services Installation Wizard
Network Credentials
Specify the name of the forest where the installation will occur and account credentials that have sufficient privileges to perform the installation.
Type the name of any domain in the forest where you plan to install this domain controller:
ali.com
Specify the account credentials to use to perform the installation:
My current logged on credentials (SERVER\Administrator)
The current user credentials cannot be selected because they are local to this computer. A set of domain credentials is needed.
Alternate credentials:
Set...
More about who can install Active Directory Domain Services
< Back
Next >
Cancel
Windows Security
Network Credentials
Specify the account credentials to use to perform the installation:
ali.com\administrator
Domain: ali.com
OK
Cancel

در اینجا باید یک اسم مجزا برای Tree تعریف کنیم

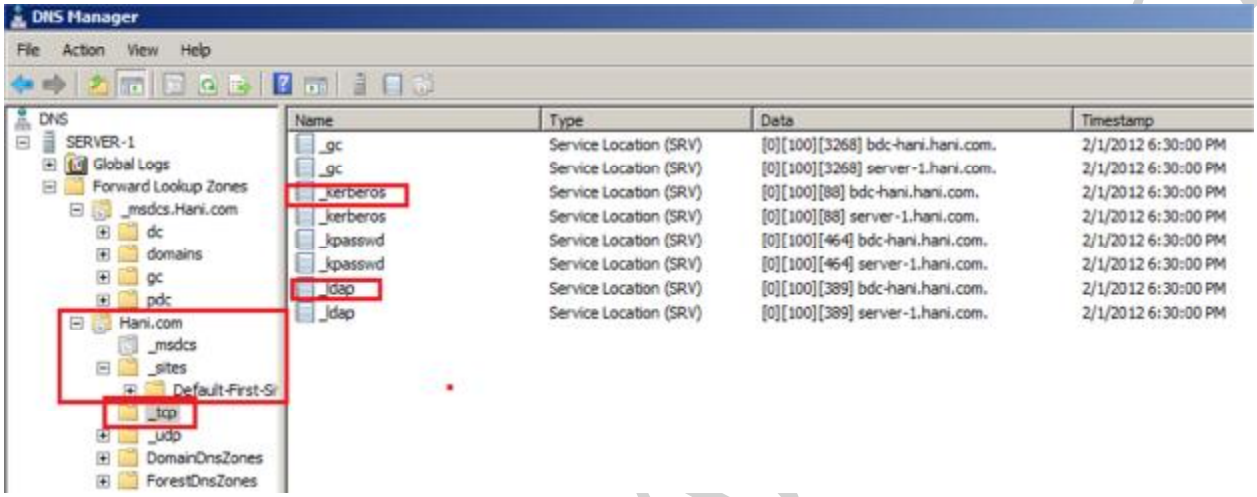
Fa Ajabi sh

ارتباط Active Directory با DNS

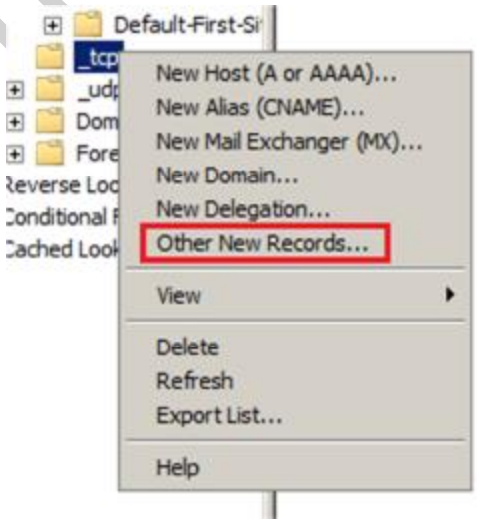
همیشه باید اجازه دهیم خود اکتیو دایرکتوری DNS را نصب کند به این دلیل که هنگامی که این کار انجام شد 2 زون در DNS به اسامی

اضافه می شود ( = hani.com اسم دامین)

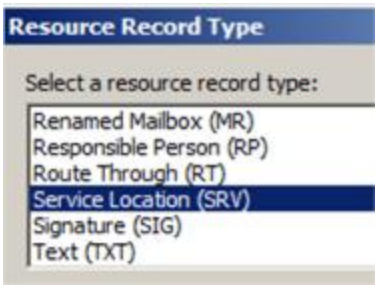
- زمانی که کلاینتی به دامین Join نمی شود مشکل از 2 Record زیر می باشد, برای برطرف کردن این مشکل باید به صورت دستی این 2 رکورد را اضافه کنیم ( در شرایط بحرانی)
- سرویس هایی که با _ شروع می شوند مخصوص اکتیو هستند .



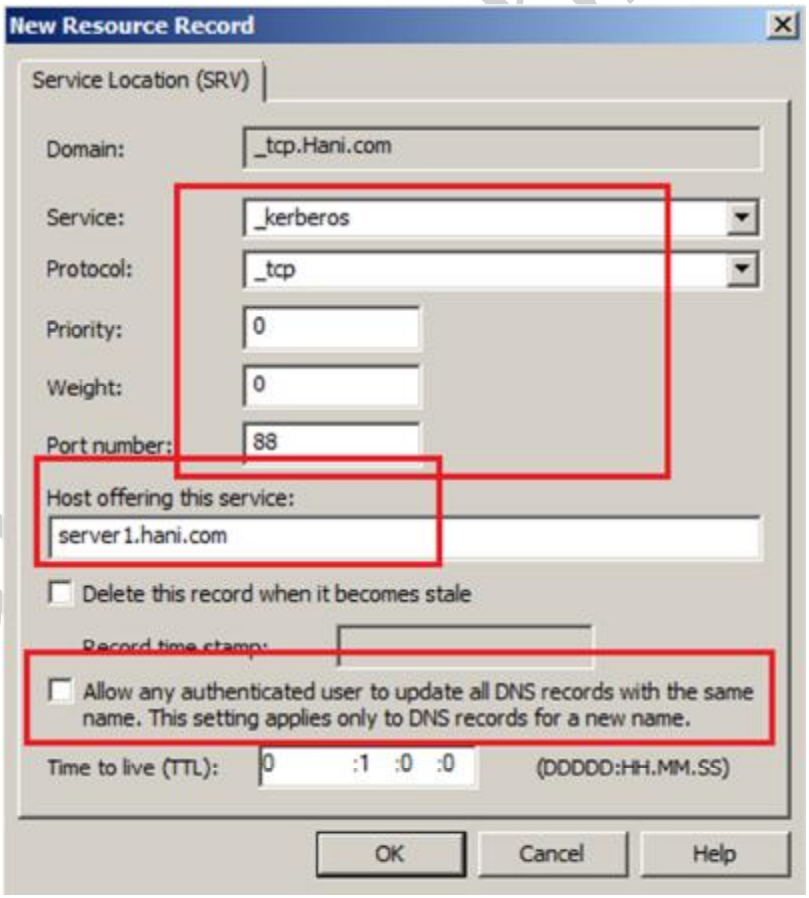

برای ساختن یک رکورد مانند زیر عمل می کنیم




FarshidA




در قسمت Service نوع سرویس را مشخص می کنیم,در Priority اولویت را مشخص می کنیم,هرچه این عدد کمتر باشد اولویت بالاتر است, Weight اگر 2 رکورد داشته باشیم که Priority آنها برابر باشد نسبت به Weight آنها اولویت مورد بررسی قرار می گیرد هرچه بالاتر باشد بهتر است,در قسمت ...Host باید اسم سرور را مانند زیر وارد می کنیم,گزینه ..Allow نباید فعال باشد چون اگر فعال باشد به هر کسی اجازه تغییر در DNS را می دهد.




Fa bnoush

Trust Releationship

به صورت پیش فرض 2 دامین با هم نمی توانند ارتباط داشته باشند مگر اینکه با هم Trust شوند.

انواع Trust

Parent child : به صورت پیش فرض هر Parent به Child , Trust می باشد.

Root Tree : به صورت پیش فرض هر Root Domain به Domain Tree خودش Trust می باشد.

Shortcut Trust : به رابطه بین 2 child یک فارست گویند,به صورت پیش فرض وجود ندارد.

Forest Trust : به رابطه بین 2 Forest 2, Root Domain متفاوت گویند.

External Trust : به رابطه بین 2 Forest 2, child متفاوت گویند.

Realm Trust : برای برقراری ارتباط بین یک دامین مایکروسافت و یک دامین غیر از مایکروسافت از این نوع Trust استفاده می کنیم.

در Trust 4 اصطلاح داریم: Twoway–Oneway–None Transitive–Transitive

Transitive

زمانی که بین 2 RootDomain رابطه Trust ایجاد می کنیم اگر این رابطه از نوع Transitive باشد,بین child های این 2 دامین هم رابطه مستقیم Trust ایجاد می شود.

None Transitive

زمانی که بین 2 RootDomain رابطه Trust ایجاد می کنیم اگر این رابطه از نوع None Transitive باشد فقط RootDomain ها با هم Trust هستند.

- Forest Trust ها از نوع Transitive می باشند وTrustExternal ها ازنوع None Transitive می باشند(Defult )

Oneway

اگر فقط دامین ما به یک دامین دیگر Trust باشد Onway Outgoing گویند و اگر فقط یک دامین به دامین ما Trustباشد به آن Oneway Incoming گویند.

Twoway

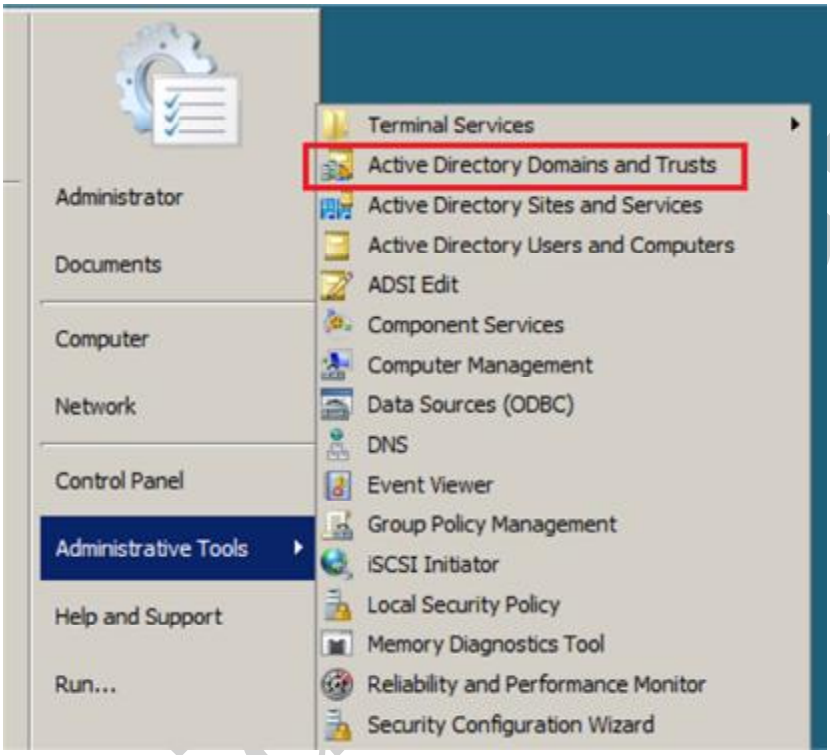
زمانی که دامین ما و یک دامین دیگر هردو به هم Trust باشد را Twoway گویند.

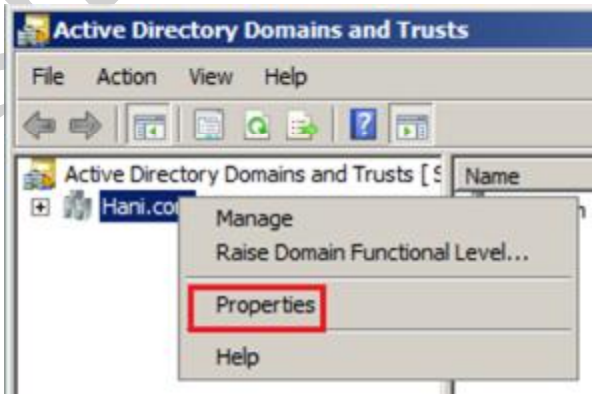
- بهترین نرم افزار برای بدست آوردن پسورد وایرلس های کاربران خانگی Kissmet می باشد.

FarshidAjabnoush

ایجاد یک رابطه Trust

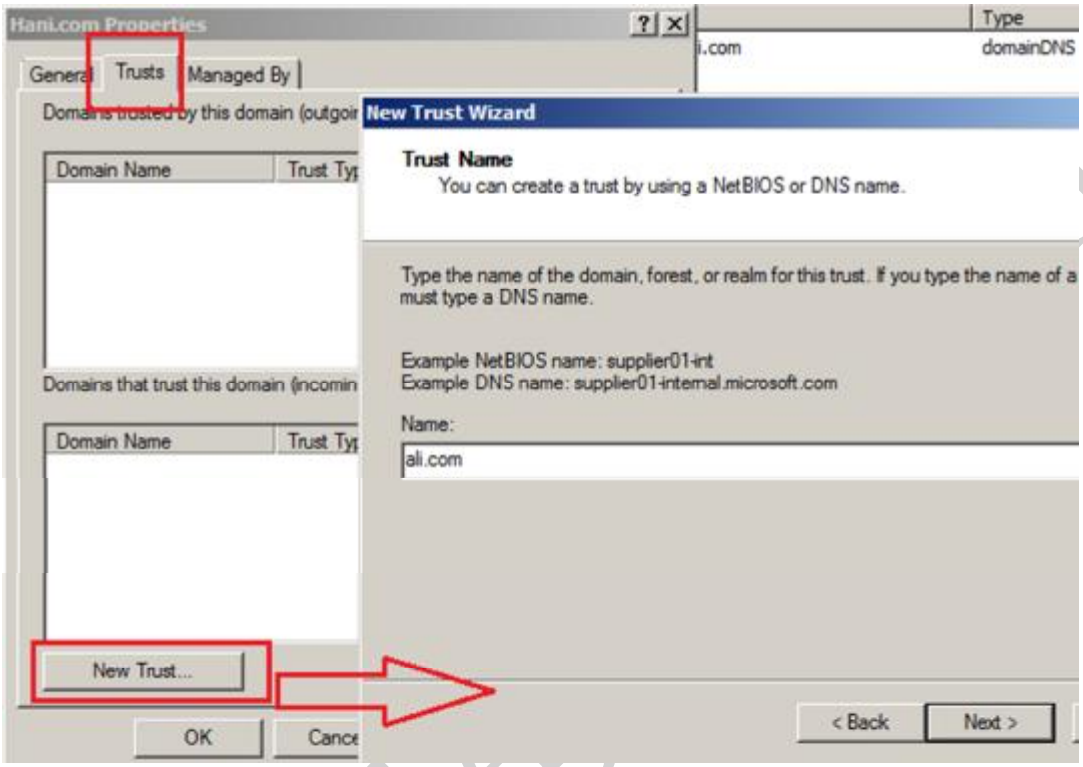
برای ایجاد رابطه Trust ابتدا باید DNS های هر دو سرور را تغییر دهیم,باید Ip سرور اول را به عنوان DNS برای سرور دوم تنظیم کنیم و Ip سرور دوم را به عنوان DNS برای سرور اول تنظیم کنیم.



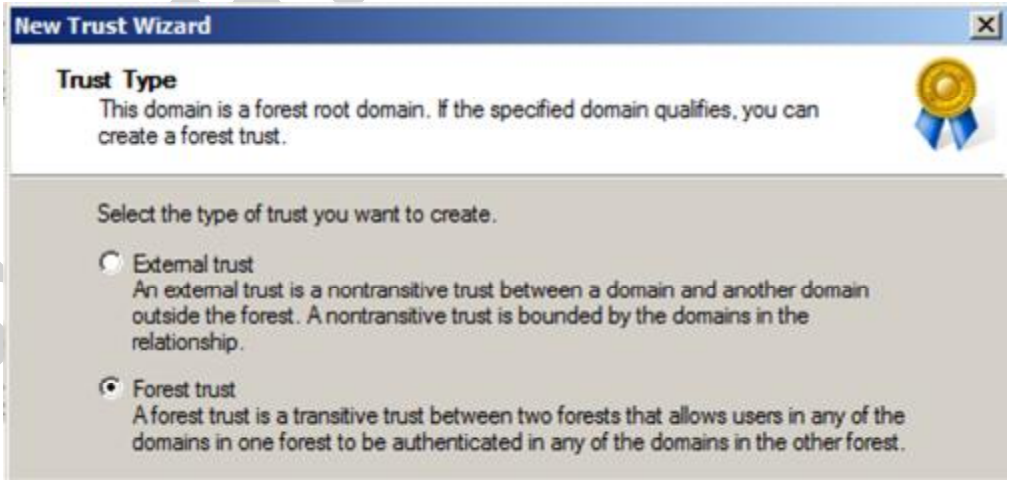



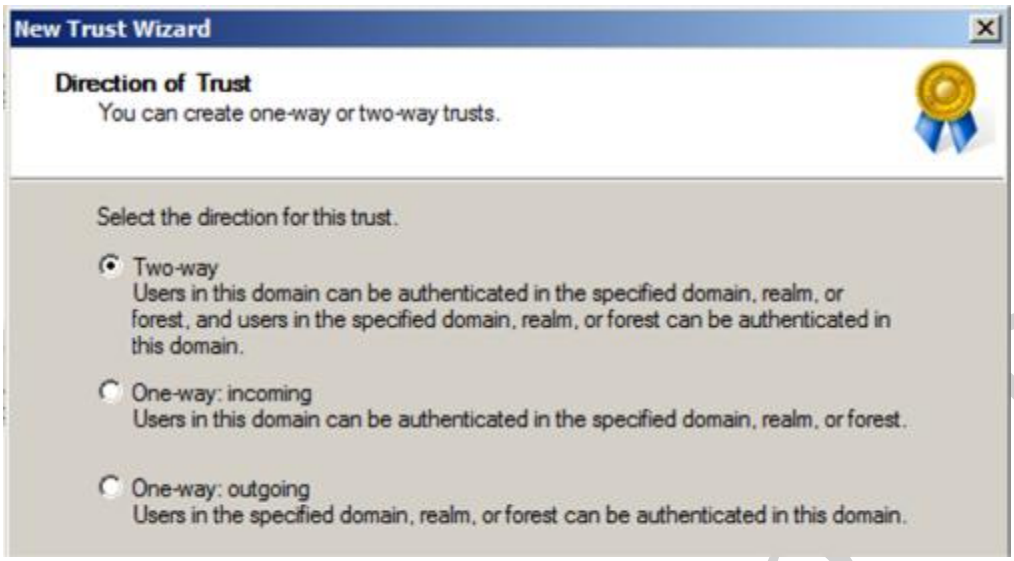

Farshid

در این مرحله باید حتما اسم شعبه مقابل را بدهیم(شعبه ای که می خواهیم به آن Trust کنیم,Ali.com ) در اینجا اسم شعبه ما Hani.com می باشد.



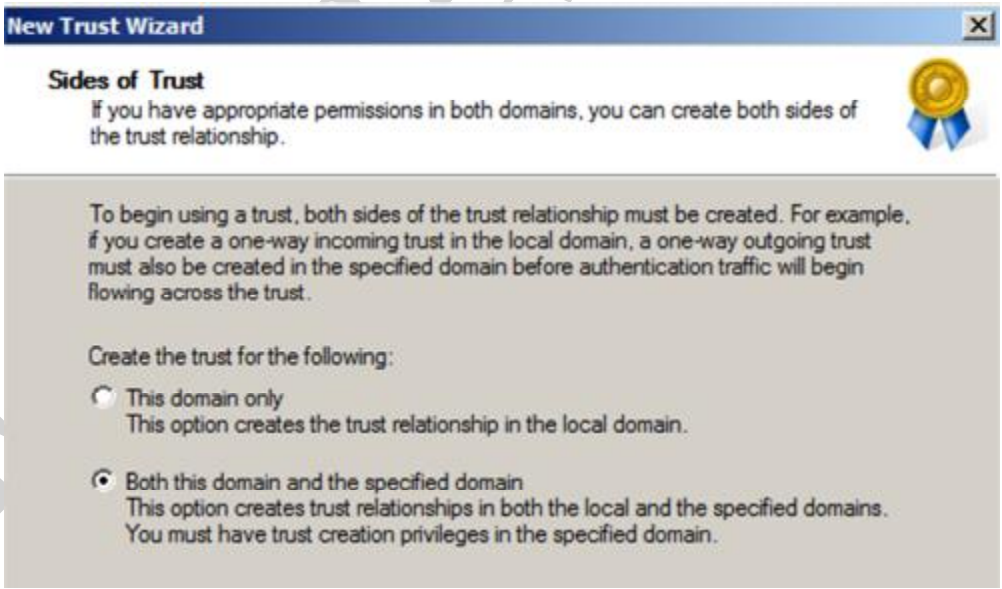

در اینجا باید Forest را انتخاب کنیم چون بین Trust, Rootdomain 2 می زنیم,اگر بین2 childبود باید External را انتخاب می کردیم.





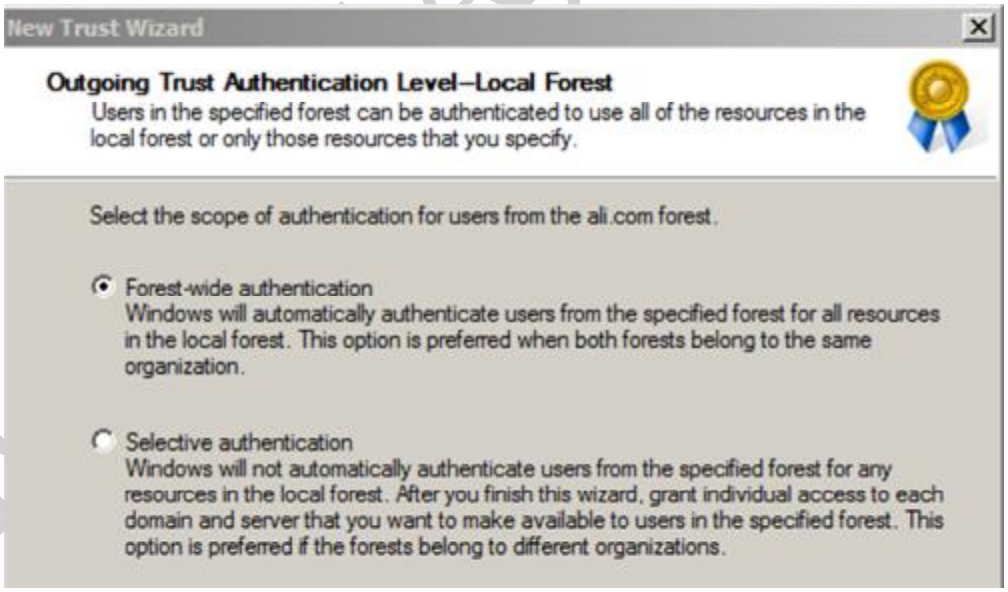

زمانی که Twoway را انتخاب می کنیم باید این تنظیمات بر روی هر دو سرور اعمال شود،برای این کار گزینه Both را انتخاب می کنیم.

- در محیط واقعی گزینه Both را انتخاب نمی کنیم چون سرور مقابل یوزر و پسورد Admin را به ما نمی دهد.

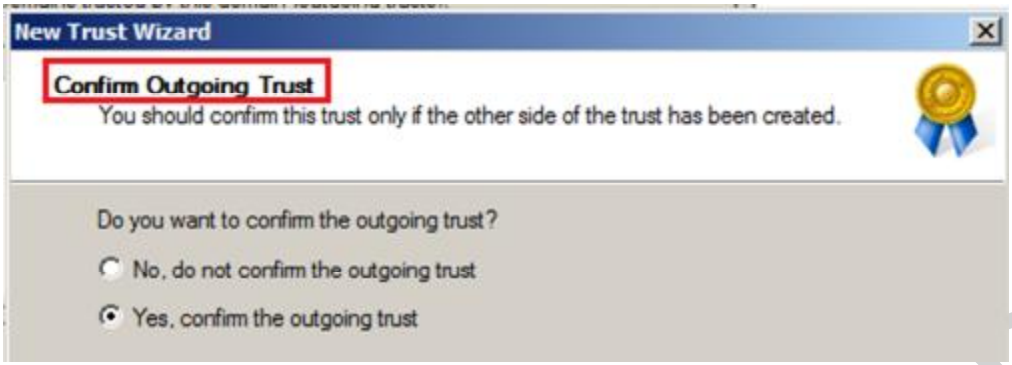


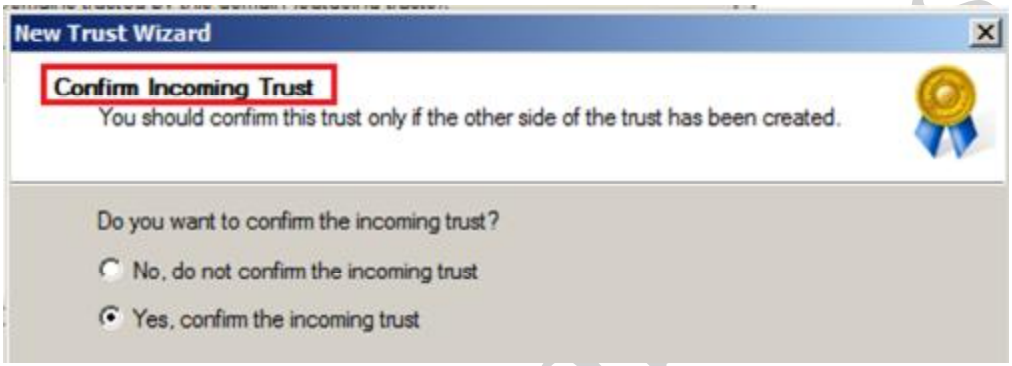
سپس باید پسورد Admin سرور دوم را وارد کنیم.

در این مرحله مشخص می کنیم که یوزری که در دامین Hani ساخته شده است در دامین Ali هم اعتبار دارد(می تواند Login کند)با انتخاب گزینه اول این اعتبار وجود دارد و با انتخاب گزینه دوم این اعتبار وجود نخواهد داشت و باید با یوزرهای موجود در دامین Ali , Login کنیم.

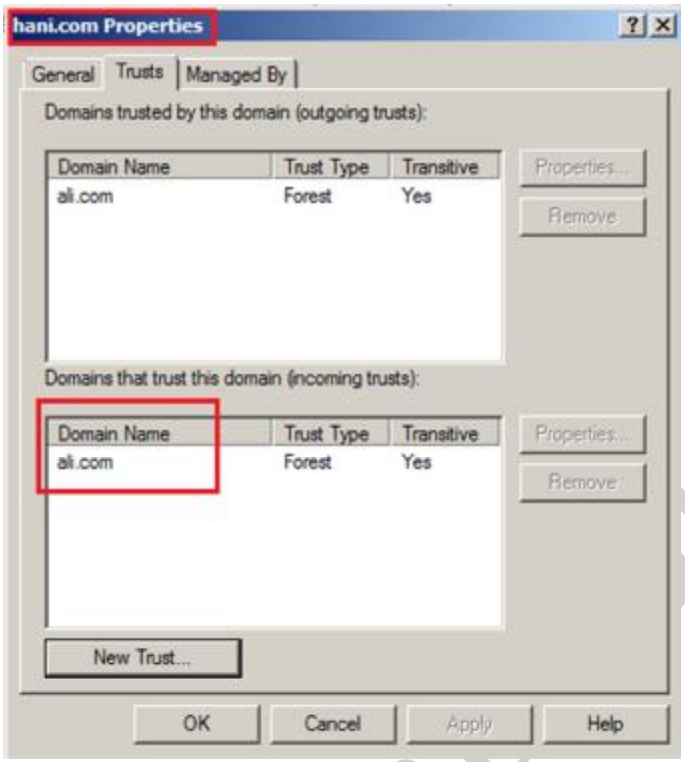



در مرحله بعد می پرسد آیا می خواهید Outgoing وIncoming راتست بگیرم

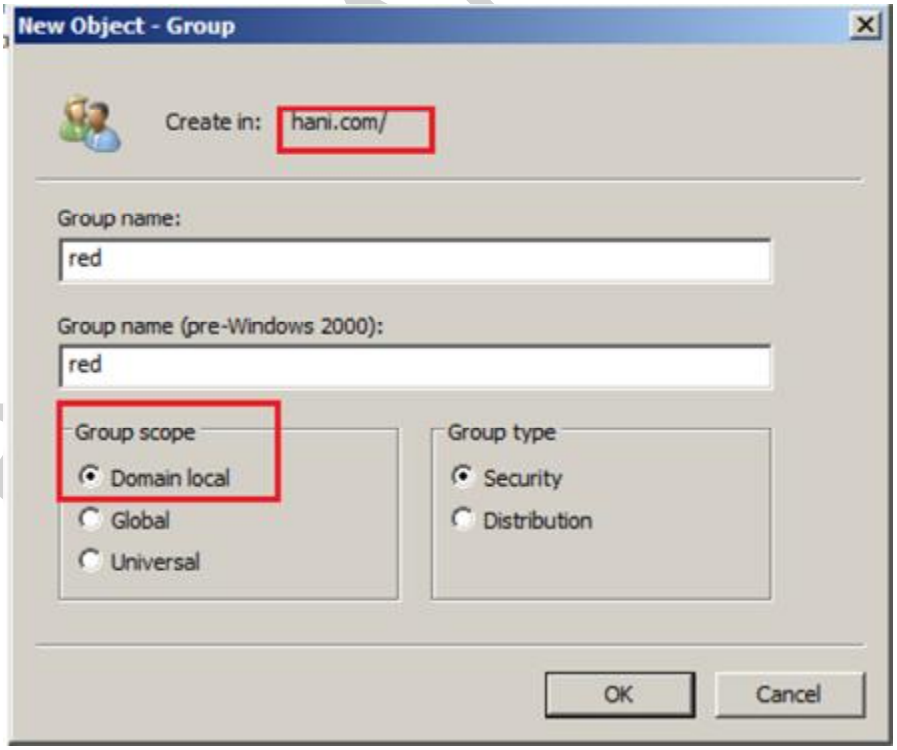

New Trust Wizard
Confirm Outgoing Trust
You should confirm this trust only if the other side of the trust has been created.
Do you want to confirm the outgoing trust?
No, do not confirm the outgoing trust
Yes, confirm the outgoing trust


New Trust Wizard
Confirm Incoming Trust
You should confirm this trust only if the other side of the trust has been created.
Do you want to confirm the incoming trust?
No, do not confirm the incoming trust
Yes, confirm the incoming trust

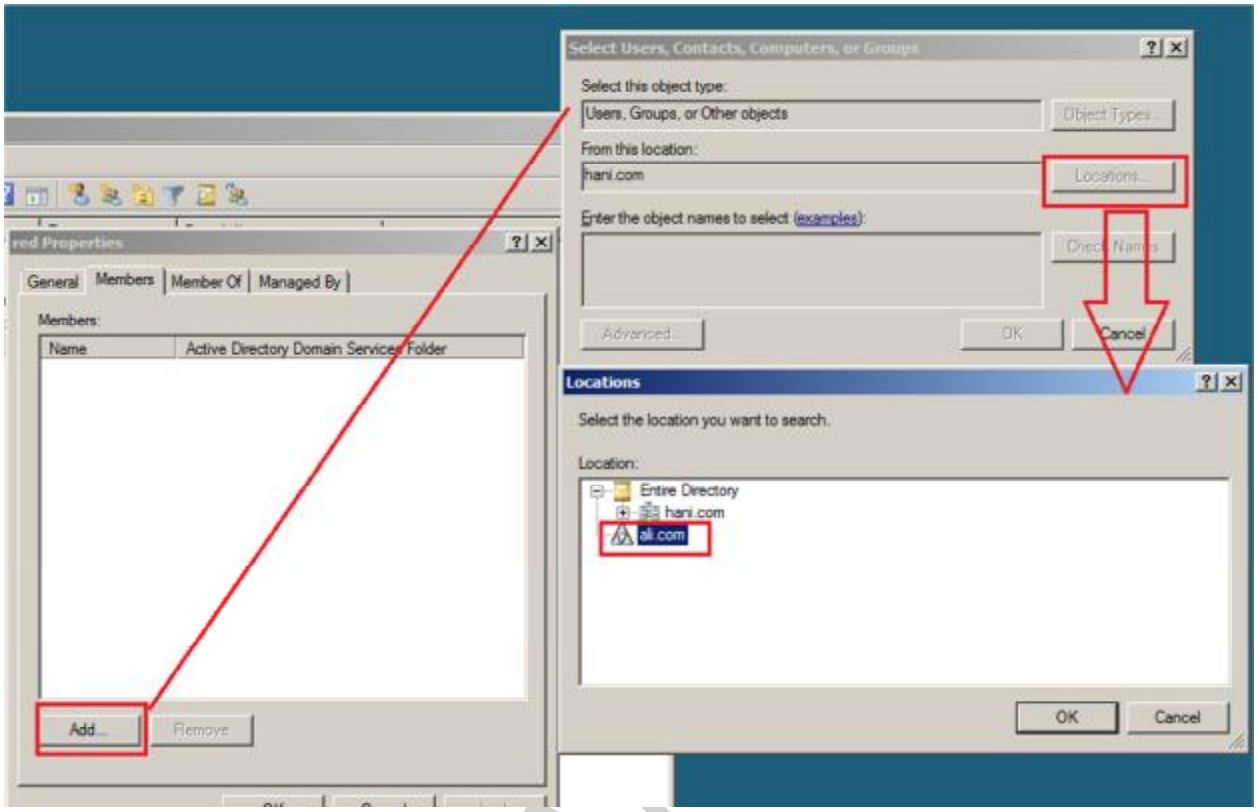
New Trust Wizard
Completing the New Trust Wizard
You have successfully completed the New Trust Wizard.
Status of changes:
The trust relationship was successfully created and confirmed.
Route these names to the specified forest:
*.ali.com
Route these names to the local forest:
*.hani.com
To close this wizard, click Finish.
< Back
Finish
Cancel

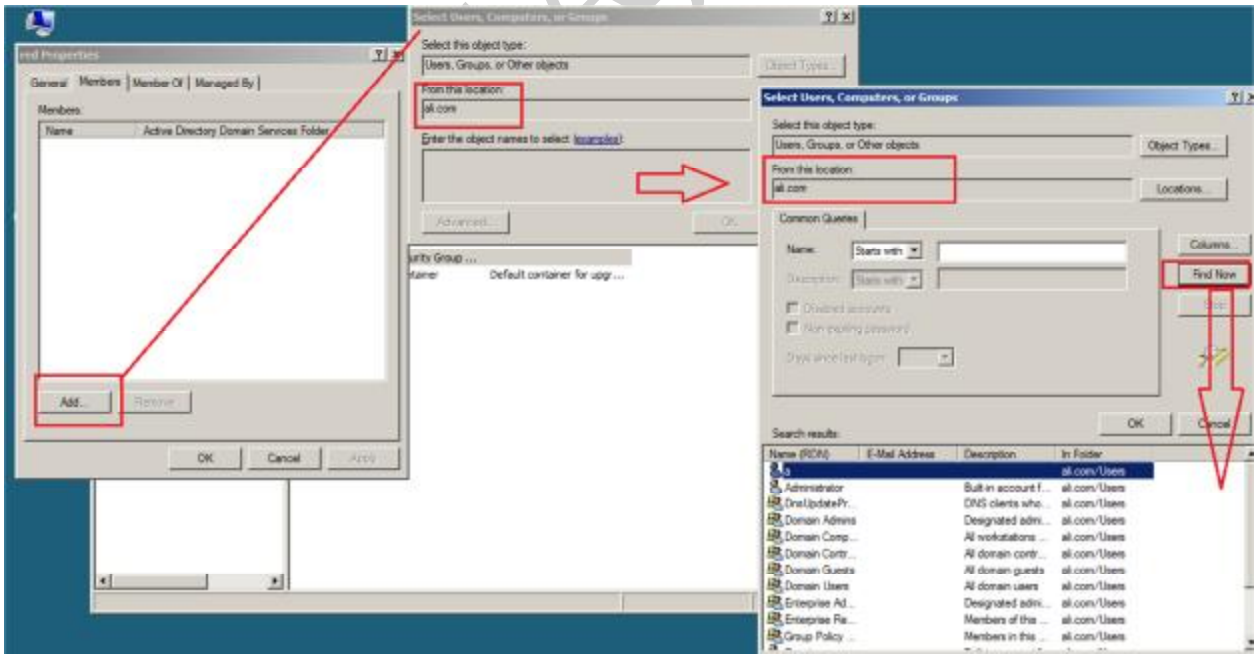



برای استفاده از Trust ابتدا در دامین Ali.com یک یوزر ایجاد می کنیم,سپس در دامین hani.com یک گروه از نوع DomainLocal ایجاد می کنیم



سپس برای گروه ایجاد شده در دامین hani از دامین ali عضو می گیریم




و در آخر هم OK .

پیاده سازی RODC داخل شبکه های دامینی

RODC یک از ویژگی های منحصر به فرد سرورBDC داخل 2008 می باشد,فقط BDC را می توان Read Only (RODC )کرد.

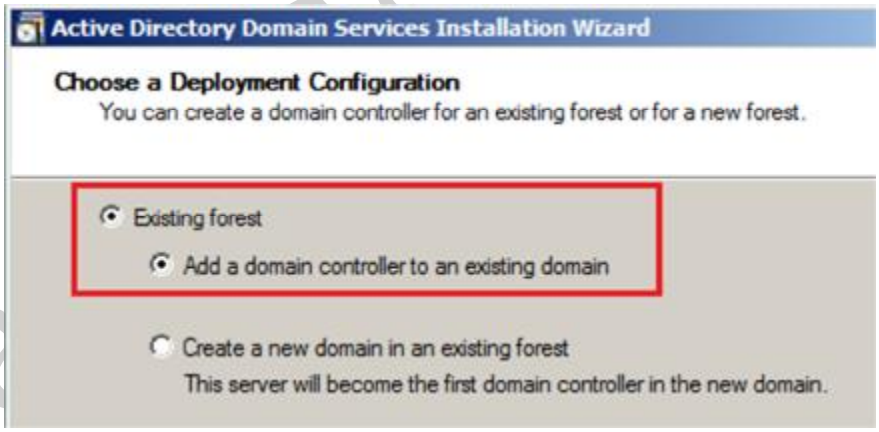
از RODC بجای Child زمانی استفاده می کنیم که در آن شعبه تعداد کاربرانمان کم باشد,لینک ارتباطی با Root سرعت کمی داشته باشد,امنیت فیزیکی پایین باشد, اگر Child داشته باشیم با Replicate, Root می کند و همین امر موجب کندی شبکه (با این سرعت پایین) می شود.

مزایای RODC

- همیشه Replication ها از شعبه اصلی به سمت RODC می باشد(به صورت یکطرفه).
- عمل احراز هویت را خودش انجام نمی دهد و از Root دامین برای این کار کمک می گیرد.
- می توانند اطلاعات را داخل خودشان Cache کنند و عمل Replication را انجام ندهند(چون اطلاعات را ذخیره می کنند از نظر امنیتی مناسب نیست,تنها اطلاعات عادی را ذخیره می کند مانند یوزر و پسوردهای معمولی).
- تنها سروری می باشد که می توان برای آن Admin Local تعریف کرد(با داشتن Active !!)

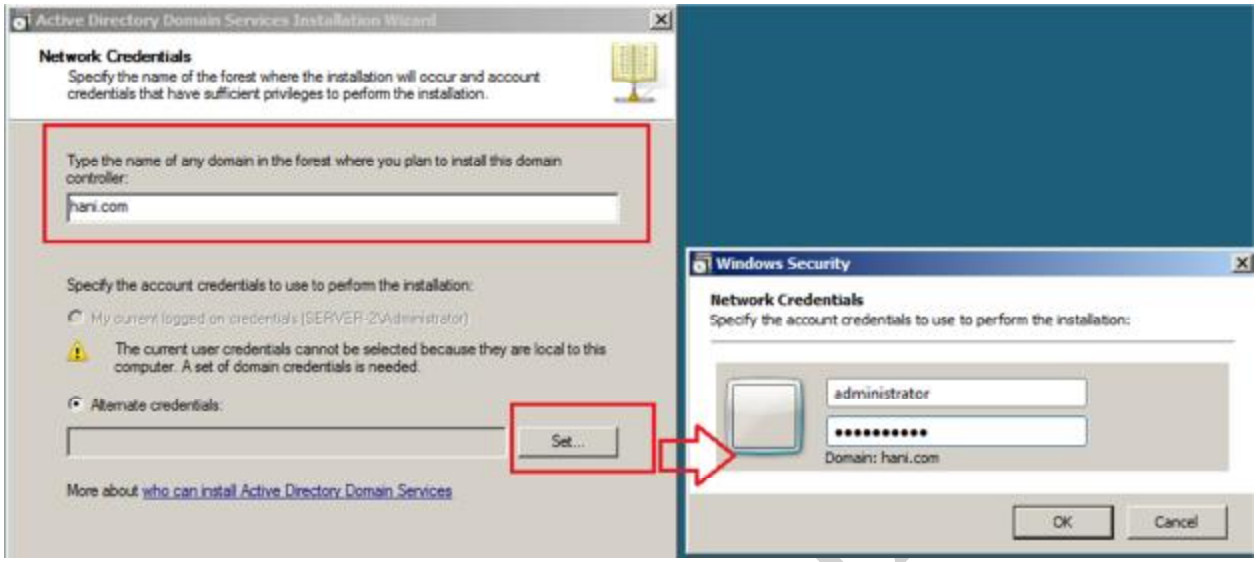
پیاده سازی RODC

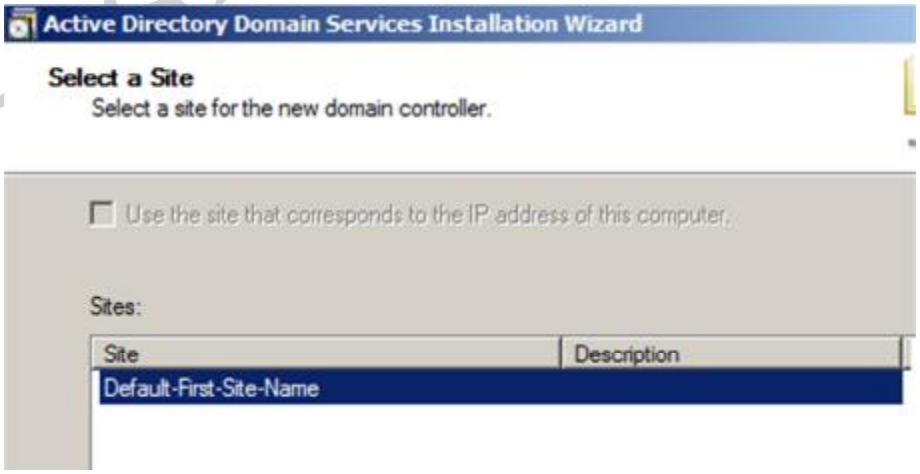
برای این کار سروری که می خواهیم RODC شود باید DNS آن سرور اصلی (Root) باشد و Ip آن Static باشد سپس نوبت به نصب اکتیو مانند زیر می رسد



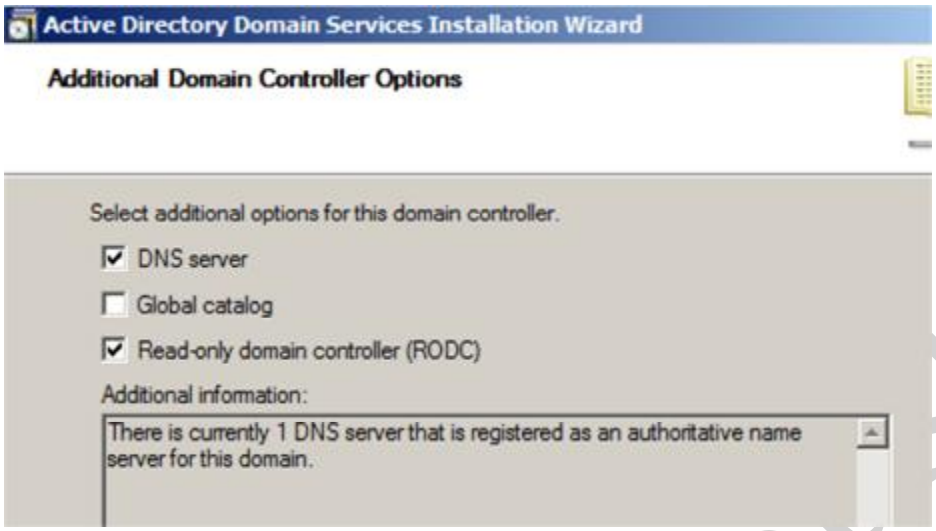

Fa Ajabnoush

در مرحله بعد باید اسم Root ویوزر پسورد آن را وارد کنیم

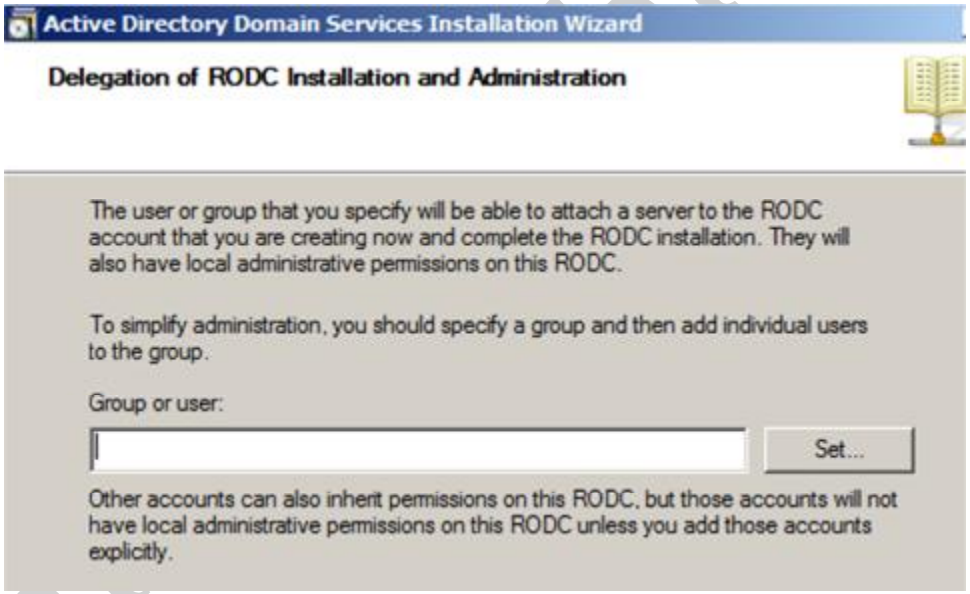





در این مرحله Global Catalog را غیر فعال می کنیم به این دلیل که از Root بپرسند




در اینجا می توانیم یوزر Admin Local را معرفی کنیم

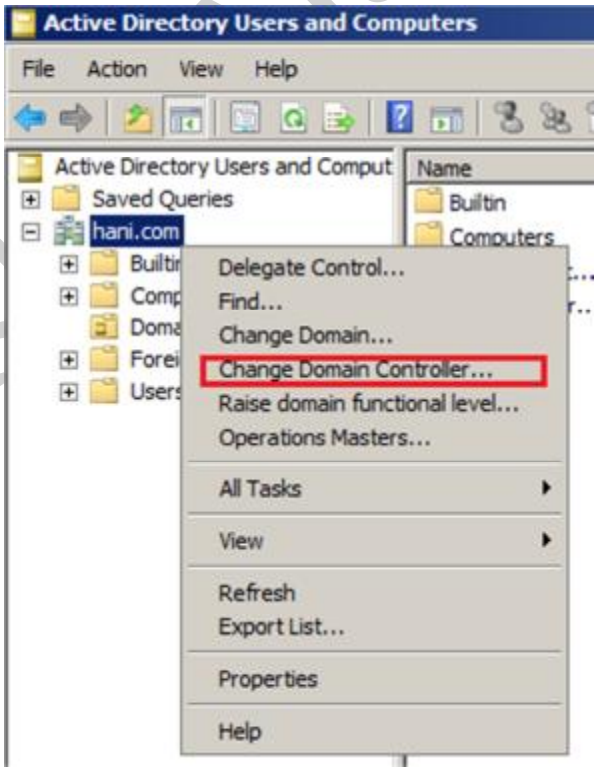



و در آخر هم Finish .

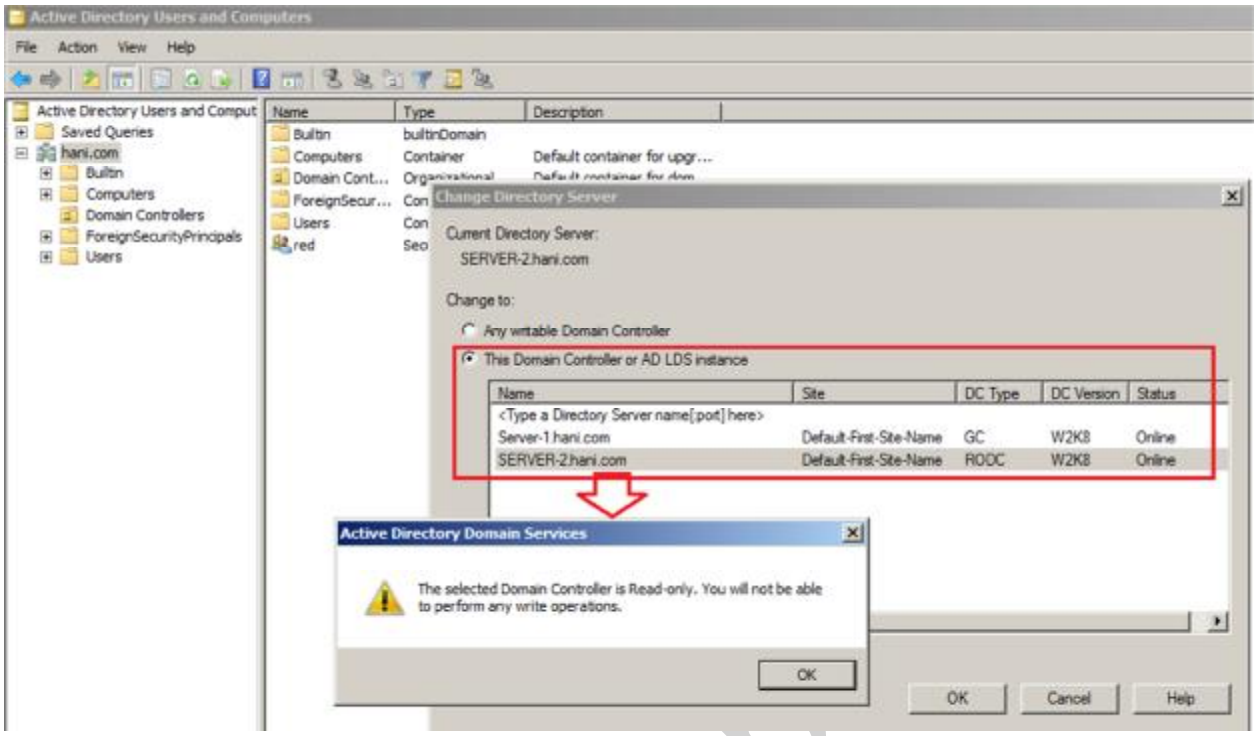
برای تست گرفتن باید سرور 1 را خاموش کنیم و سعی کنیم پشت سرور 2( RODC) لاگین کنیم,که لاگین کردن با این شرایط امکان پذیر نمی باشد.

به صورت پیش فرض Cache نمی کند،باید به صورت دستی این کار را انجام دهیم.

زمانی که بخواهیم از Root Domain به دامین کنتلرر دیگری در شبکه وصل شویم مانند زیر عمل می کنیم




در اینجا چون دامین کنتلرر ما RODC می باشد با Error زیر برخورد می کنیم




زمانی که در سرور اصلی یوزری بسازیم و بخواهیم با آن یوزر در سرور RODC لاگین کنیم با Error زیر برخورد می کنیم

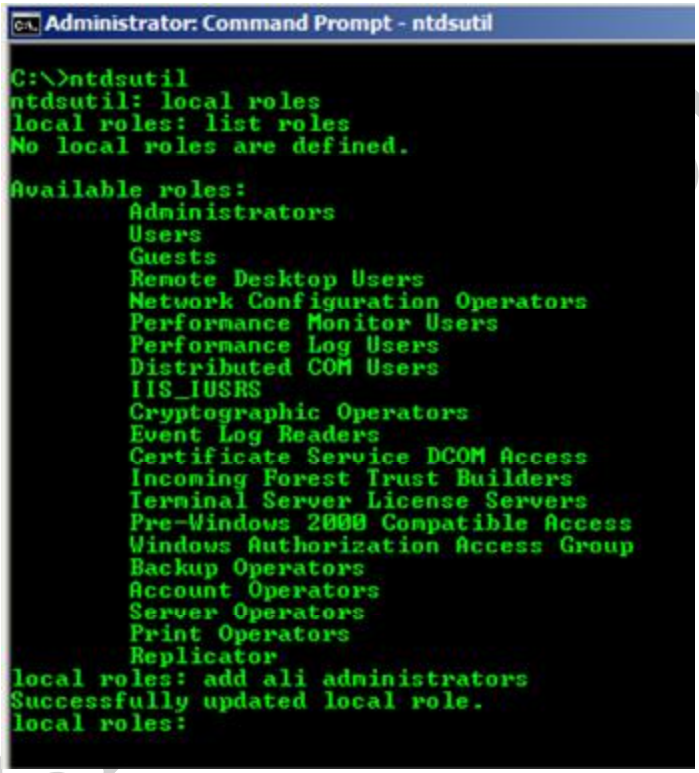
برای اینکه بتوانیم در RODC لاگین کنیم باید پشت RODC یوزری بسازیم که Admin Local باشد برای این کار مانند زیر عمل می کنیم

NTDSUTIL

LOCAL ROLES

LIST ROLES

ADD ALI ADMINISTRATORS



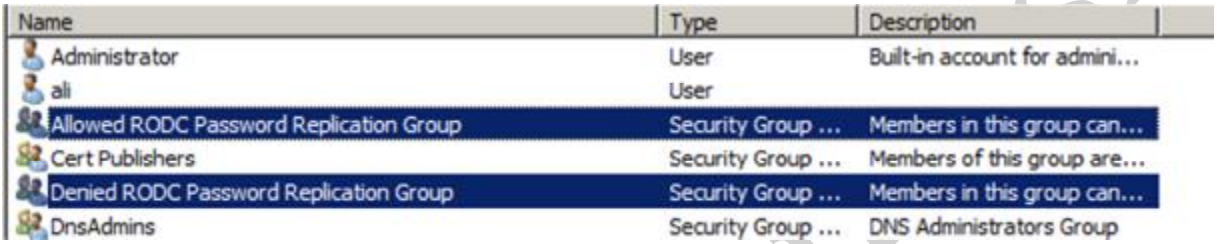

سپس می توانیم با یوزری که ساختیم (ali ) لاگین کنیم

Farsroush

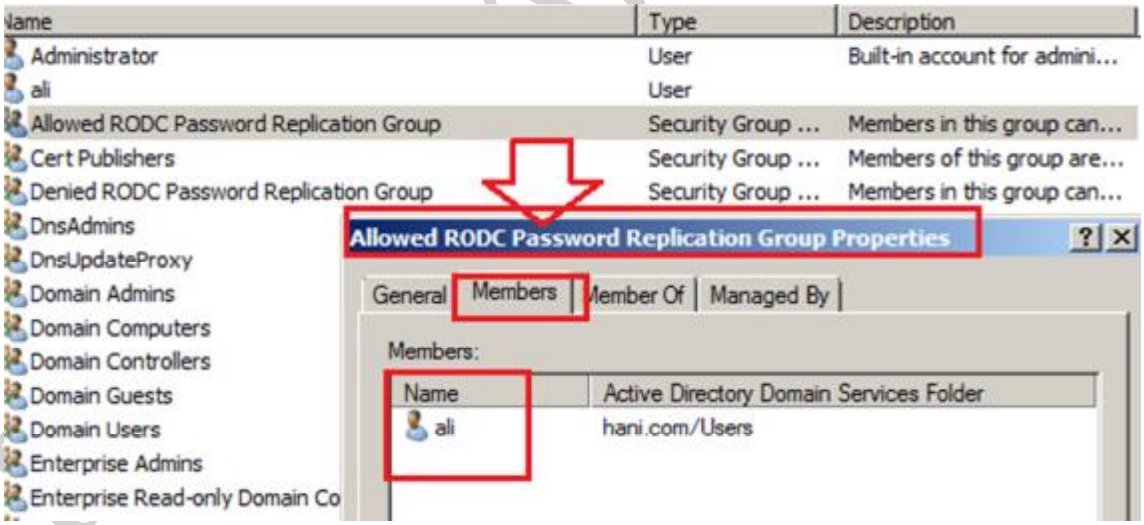
- اگر Root خاموش باشد نمی توانیم بصورت Local پشت RODC لاگین کنیم چون هنوز Cache, User Local نشده است.

Cache کردن یوزر در سرور RODC

برای این کار وارد سرور اصلی می شویم در قسمت گروه ها دو گروه مشخص شده زیر را می بینیم




در گروه Allow باید یوزرهایی را که می خواهیم پسورد آنها پشت Cache,RODC شوند را وارد کنیم و در گروه ..Denied برعکس می باشد.




- برای اولین بار,برای Cache کردن پسورد یوزر مورد نظر باید سرور اصلی فعال باشد.

# Implementing Sites For Managing Active Directory Replications

پیاده سازی سایت ها برای مدیریت Active Directory

Replication : زمانی که یک Object در سرورهای ما تغییر می کند به سرور GC گزارش داده می شود به این عمل در اصطلاح Replication گویند.

Replication بین BDC و GC هر 2 ثانیه,Child و GC هر 10 ثانیه,Tree وGC هر 30 ثانیه اتفاق می افتد.

این زمانهای کوتاه, برای زمانی که بین دو شهر می خواهد Replication اتفاق بیفتد دردسرساز می شود,برای برطرف کردن این مشکل می توان زمانها را مدیریت کرد.

- اگرDFL و FFL بر روی 2000 تنظیم شده باشد زمان Replicate شدن ,کل دیتا بیس Replicate می شود.

با استفاده از Active Directory Site می توانیم زمانهای Replication را مدیریت کنیم.

- به صورت پیش فرض کل فارست عضو سایتی به نام Default First Site Name می باشد.
- ما فقط می توانیم زمان بین سایت ها را مدیریت کنیم نه زمان داخل سایت ها را,یعنیباید Default Site را به Site های کوچکتر تقسیم می کنیم.
- طراحی سایت ترافیک را بهینه می کند,کم نمی کند.

NTDS.DIT از لحاظ طراحی به 4 پارتیشن تقسیم می شود: Schema-Configuration-Domain-Application

- زمانی که بعد از مدتی سرعت دامینمان پایین آمد برای برطرف کردن این مشکل باید پوشه NTDS را که شامل پارتیشن های بالا می باشد را Defrag کنیم فقط پوشه نه درایو C,این Defrag روش خاص خود را دارد.
- Schema:تمامی Objectهای موجود و Properties آنها در این پارتیشن قرار دارد,این پارتیشن بسیار مهم است بخصوص در Exchange چون بعد از نصب آن یکسری ویژگی در تب های یوزر اضافه می شود,زمانی که دامینمان 2003 می باشد و می خواهیم آن را به 2008 تبدیل کنیم باید ابتدا این پارتیشن را آماده کنیم.

تبدیل دامین 2003 به 2008

برای این کار از CD 2008 پوشه ای به نام ADPREP را داخل یک قسمت از هارد کپی می کنیم سپس توسط CMD وارد محل ذخیره شدن پوشه مورد نظر در هاردمان می شویم و دستور Addprep /schemaprep و سپس دستور Addprep /Adprep را اجرا می کنیم سپس بعد از 30 ثانیه اعمال می شود و سیستم را

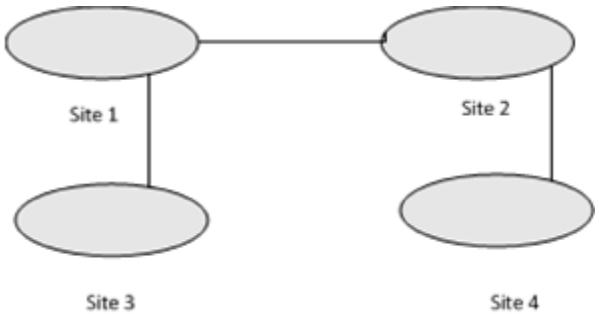
FarshidAjabnoush

ریستارت می کنیم و با 2008 سیستم را بوت می کنیم و سپس Upgrade را می زنیم,حتما قبل از Upgrade کردن باید این دو دستور را ایجاد کنیم(حتماً بررسی گردد).

- Configuration : در این پارتیشن توپولوژی (هم بندی )فارست موجود می باشد .
- Domain : محلی برای نگهداری Objectهایی هستند که داخل همان دامین ساخته می شوند.
- Application : گزارش تغییرات Object ها در این پارتیشن ذخیره می شود,به ازای هر دامین یک پارتیشن Application وجود دارد.
- در هر فارست پروسه ای به نام KCC (Knowledge Consistency Checker ) وجود دارد که هر 15 دقیقه یکبار به تمامی پارتیشن هایApplication رجوع می کند و اگر تغییری اتفاق افتاده باشد آن را به GC اعلام می کند.
- زمان KCC را می توان تغییر داد ولی حتما باید ضریبی از 15 باشد.

پیاده سازی سایت ها

- پیاده سازی سایت ها کاملا به صورت Logical بوده و از داخلnRootDomai انجام می گیرد.
- بعد از تعریف سایت ها باید بین آنها ,لینک واقعی را به عنوان SiteLink تعریف کنیم,به طور مثال 2 شعبه داریم که با ADSL به هم وصل شده اند,ما باید هر کدام از این شعب را یک سایت تعریف کنیم و سپس این سایت ها را به عنوان SiteLink به هم ارتباط دهیم(با همان بستر ارتباطی خودشان در اینجا ADSL ).
- زمانی که SiteLink ها را می سازیم چیزی به نام Cost بر روی آنها فعال می شود که اولویت استفاده از آن SiteLink را مشخص می کند هر چه این عدد کمتر باشد اولویت استفاده از آن بالاتر,به طور مثال بین 2 سایت,2 SiteLink وجود دارد که یکی ADSL و دیگری Dialup می باشد در اینجا باید ADSl,Cost پایین تر باشد تا اولویت استفاده با آن باشد.
- Cost تمامی لینک ها به صورت پیش فرض 100 می باشد.
- علاوه بر SiteLink می توانیم SiteLinkBridge هم بسازیم در این روش که مانند شکل زیر می باشد Site3 می تواند توسط مسیر ایجاد شده به Site4 وصل شود.

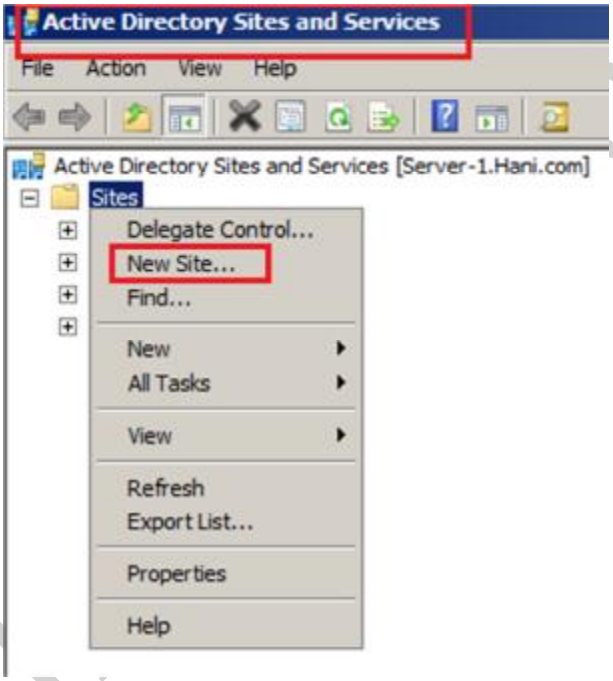



- Replication Schedule: زمان Replicate بین سایت هایمان را مشخص می کنیم.

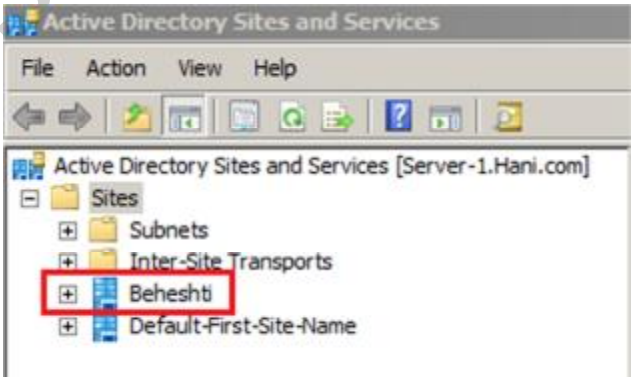
FarshidAjabnoush

- Replication Frequency : مشخص می کنیم که در زمان Replicate Schualچند بار می توانند عمل Replicate را انجام دهند.
- Replication Protocol : پروتکل مورد استفاده در Replication را مشخص می کند,برای این کار 2نوع پروتکل داریم SMTP,IP فعلا از پروتکل IP استفاده می شود به این دلیل که SMTP در فاصله های زیاد و حجم اطلاعات بالا کم می آورد.
- به سروری که داخل سایت عمل Replication را با سایت های دیگر انجام می دهد BridgeHeadServer گویند(BHS ).

برای پیاده سازی احتیاج به یک Root و یک Child داریم,بعد از راه اندازی Root,یک سایت داخل آن می سازیم




در اینجا سایت جدید به نام بهشتی می باشد,همانطور که می بینید یک سایت پیش فرض وجود دارد



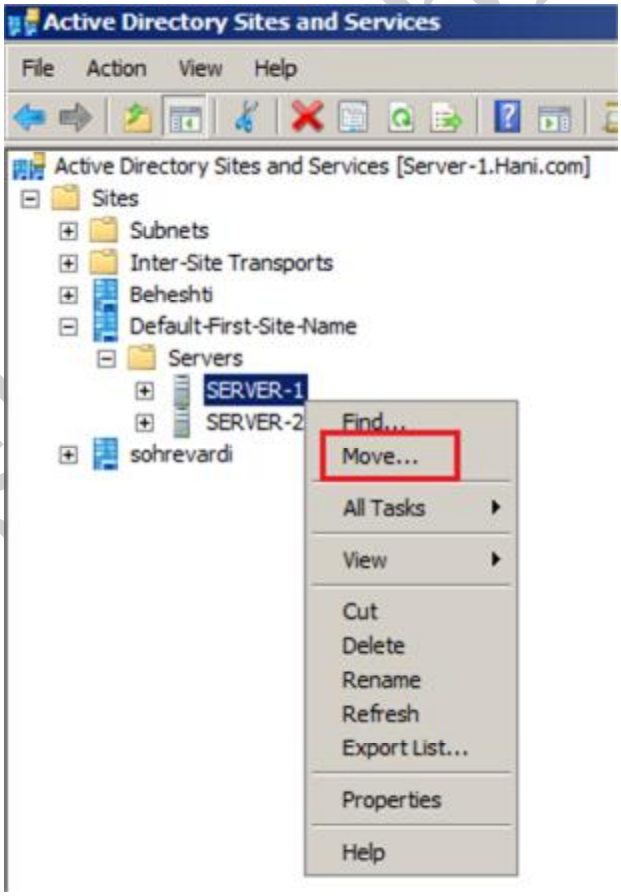

سپس نوبت به Child می باشد,برای این کار باید Child, DNS را Root تنظیم کنیم

در هنگام نصب Child به صفحه ای می رسیم که می توانیم مشخص کنیم Child ما عضو کدام سایت شود

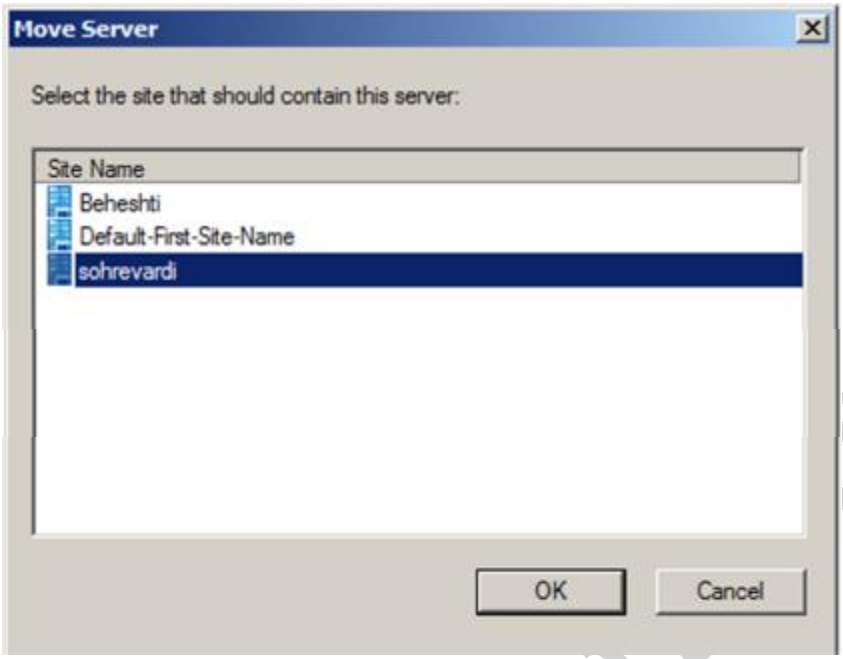
سپس وارد Root می شویم:

**می توانیم شعب را از داخل سایت ها جابجا کنیم,برای این کار مانند زیر عمل می کنیم.**

**در اینجا سرور 1 را از سایت پیش فرض به سایت سهروردی انتقال می دهیم.**




Farsi Shnoush

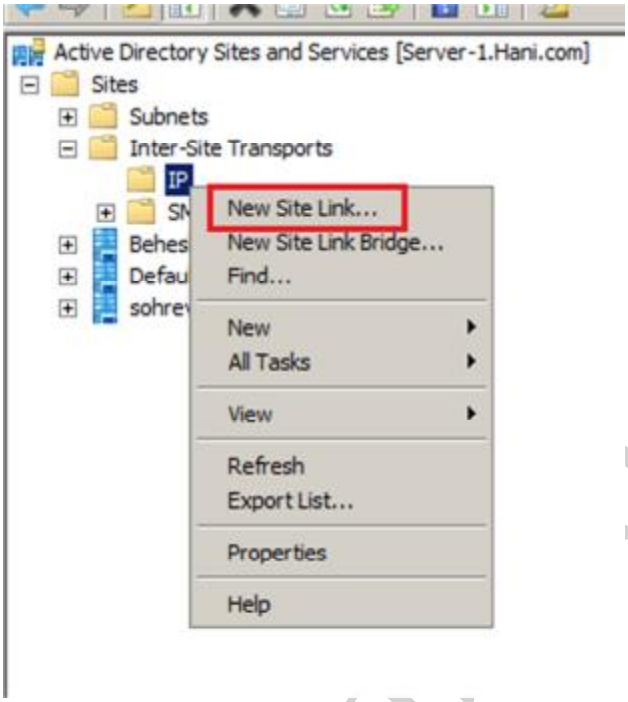



همانطور که می بینید انتقال انجام شد

- اولین سروری که داخل هر سایت اضافه می شود نقش Bridge Head Server آن سایت را دارا می باشد.
- BHS : عمل Replication را در هر سایت,BHS آن سایت انجام می دهد.
- برای Move کردن به سایت های دیگر باید سرور مورد نظر کامل Load شده باشد.

Farsiabzar.ir

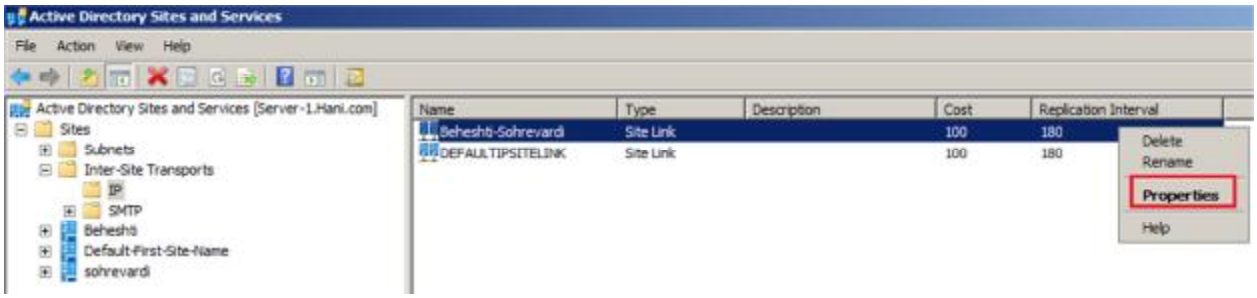
نوبت به ایجاد سایت لینک می رسد برای این کار مانند زیر عمل می کنیم



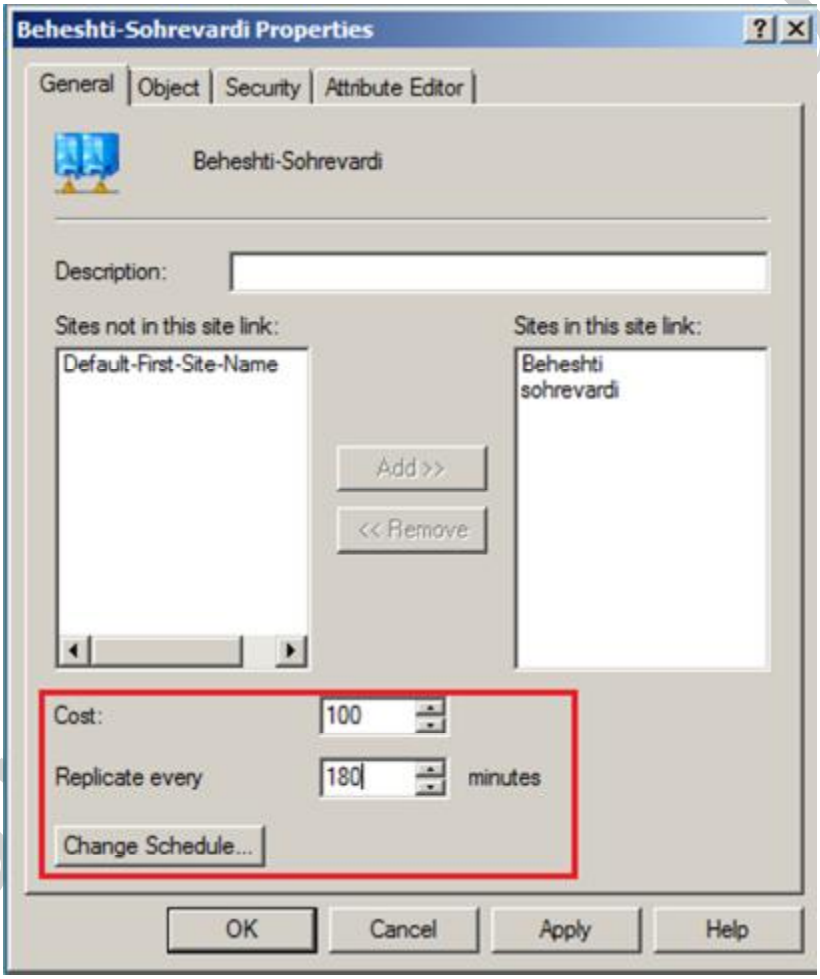

سپس سایت های مورد نظر را به سمت راست انتقال می دهیم

در آخر از روی سایت لینک ساخته شده Properties می گیریم

FarhadAjamoush



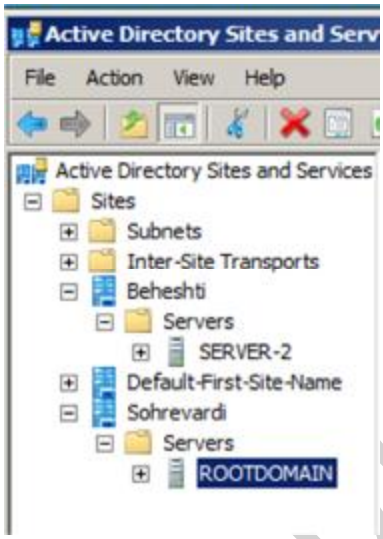

در قسمت Cost,اولویت را مشخص می کنیم,در Replicate every مشخص می کنیم هر چند دقیقه یکبار عمل Replicate انجام گیرد,در Schedule زمان Replicate را مشخص می کنیم.

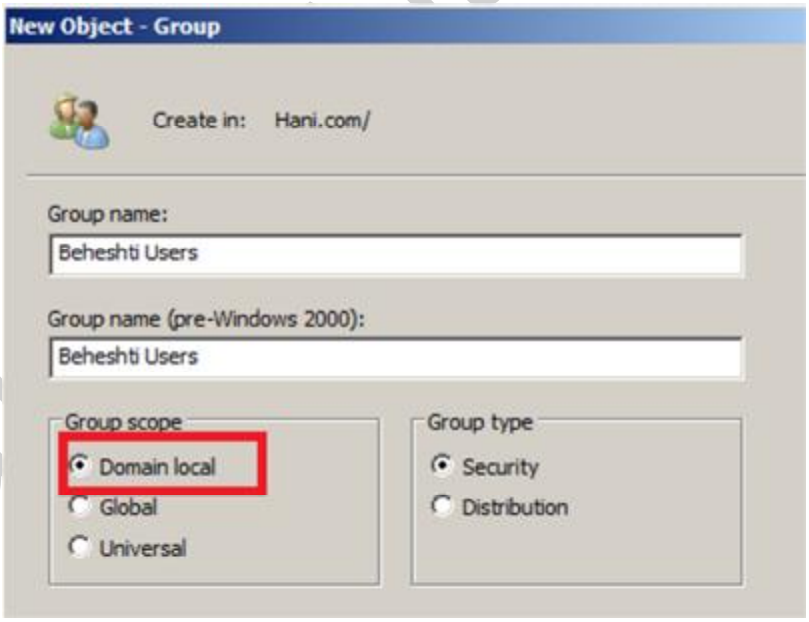



- Replicate every باید ضریبی از 15 باشد(حداقل این گزینه 15 دقیقه می باشد).

Fa

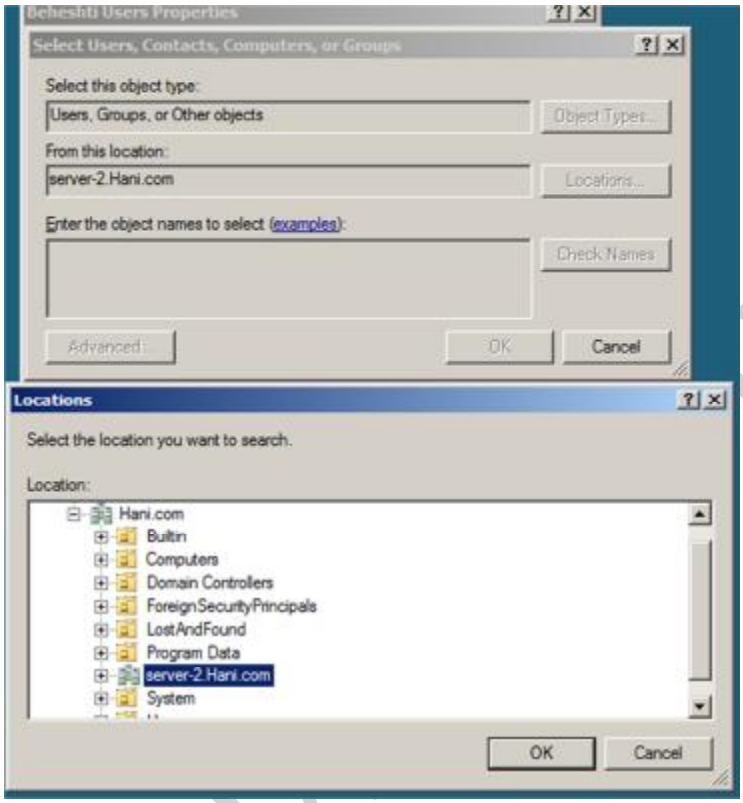
برای تست گرفتن پشت سرور 2که عضو بهشتی می باشد یک یوزر می سازیم سپس وارد سرور1 (در اینجا RootDomain نمایش داده می شود )که عضوی از سهروردی می باشد می شویم ویک گروه از نوع Domain Local می سازیم.



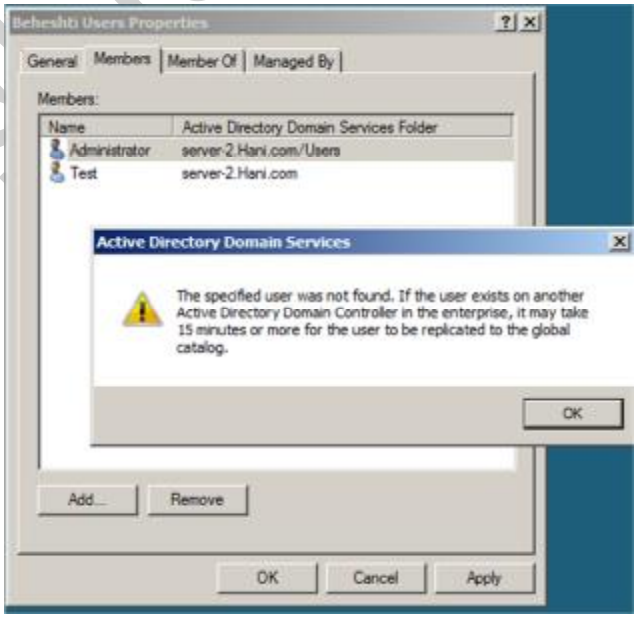




Fa iaunoush

سپس پشت RootDomain شروع به عضو گرفتن(یوزری که در سرور2 ساختیم) برای گروهمان می کنیم,وارد Member می شویم و سپس Location در آنجا Server 2 را انتخاب می کنیم.



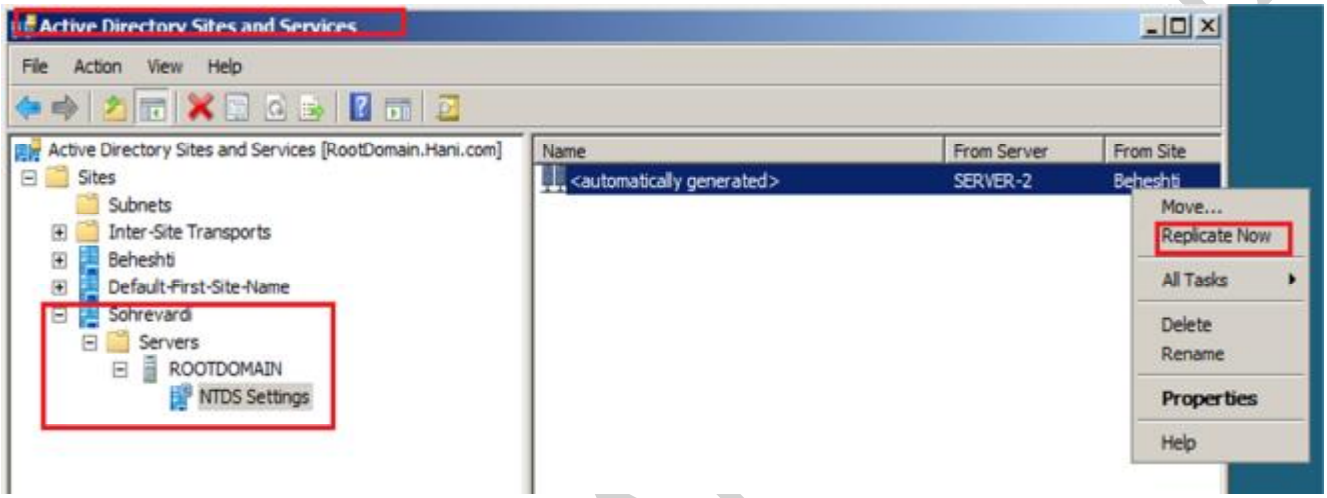

سپس بعد از انتخاب Location و انتخاب User با پیغام زیر روبرو می شویم(یوزر Test)




Farsidash

پیغام بالا به این دلیل است که هنوز عمل Replicate انجام نشده است و نمی تواند یوزر را اضافه کند,یا باید به صورت دستی این کار را بکنیم یا باید 15 دقیقه صبر کنیم تا اتوماتیک Replicate شود.

برای اینکه به صورت دستی این کار را انجام دهیم وارد سروری که GC شبکه است می شویم و روی GC شبکه Properties می گیریم و مانند زیر

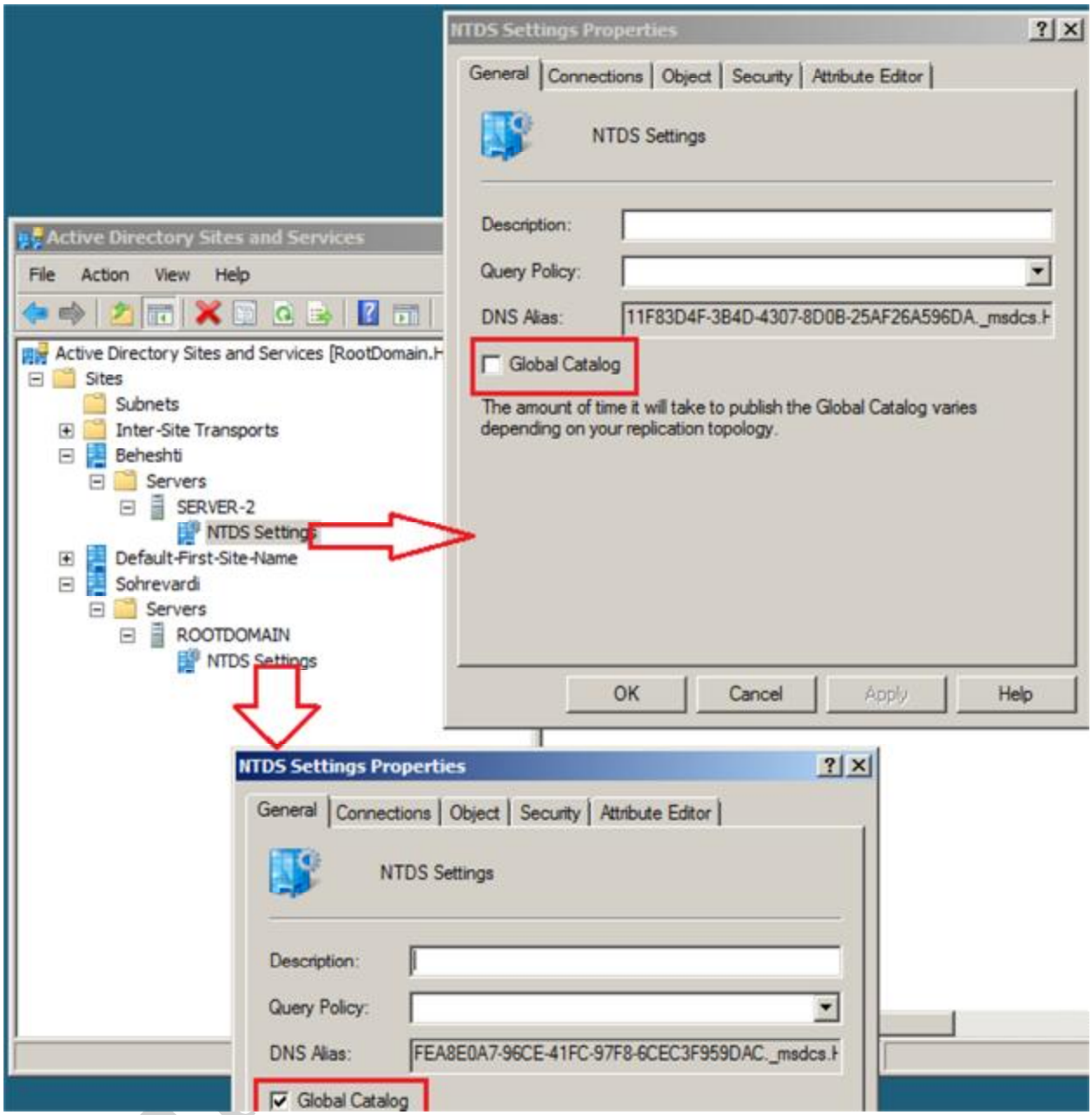



و پس از Replicate کردن, یوزر را می توان بدون هیچ پیغامی اضافه کرد.

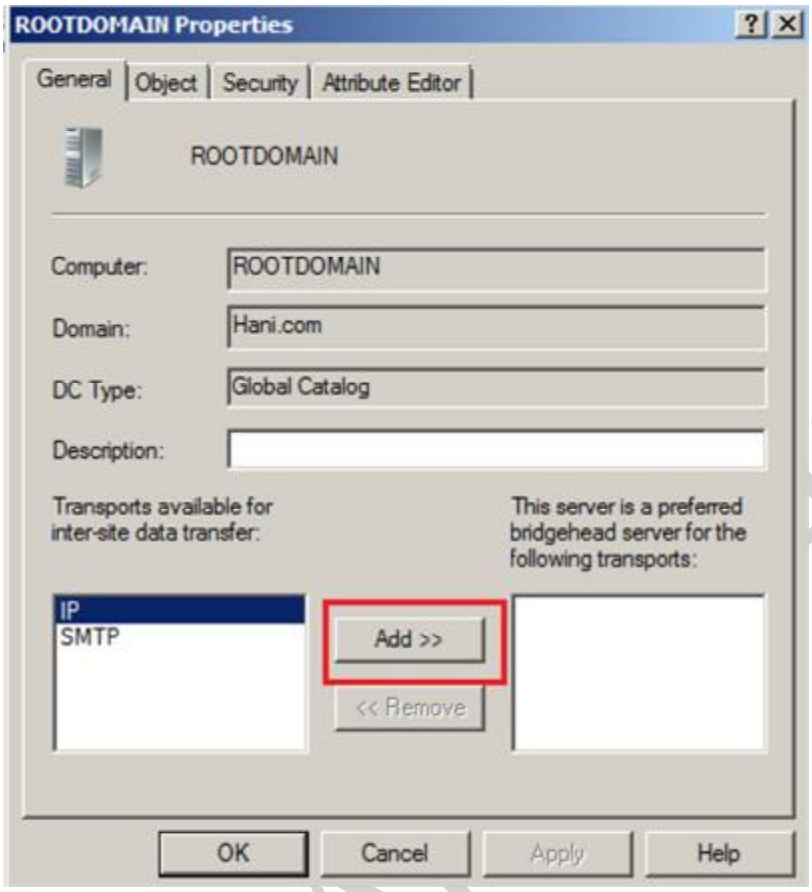
برای فهمیدن اینکه کدام سرور GC می باشد می توان بر روی NTDS هر سرور مانند زیر Properties گرفت و آن را دید حتی می توان آن را به صورت دستی هم اضافه کرد.

در اینجا می توانیم با زدن تیک گزینه مورد نظر سرور 2 را هم GC کنیم.

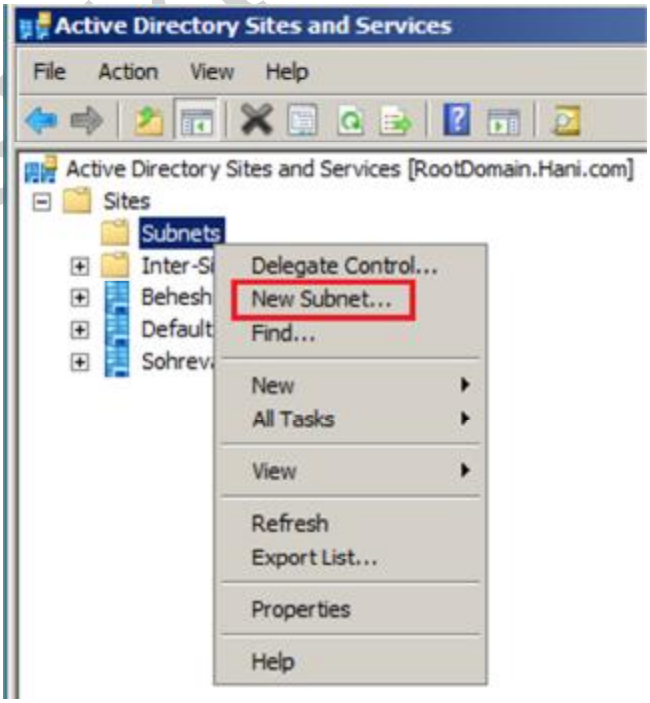
FarshidAz




زمانی که بخواهیم سروری را به صورت دستی BHS کنیم از سرور موردنظر Propertiesمی گیریم و Ip را از سمت چپ به سمت راست می بریم

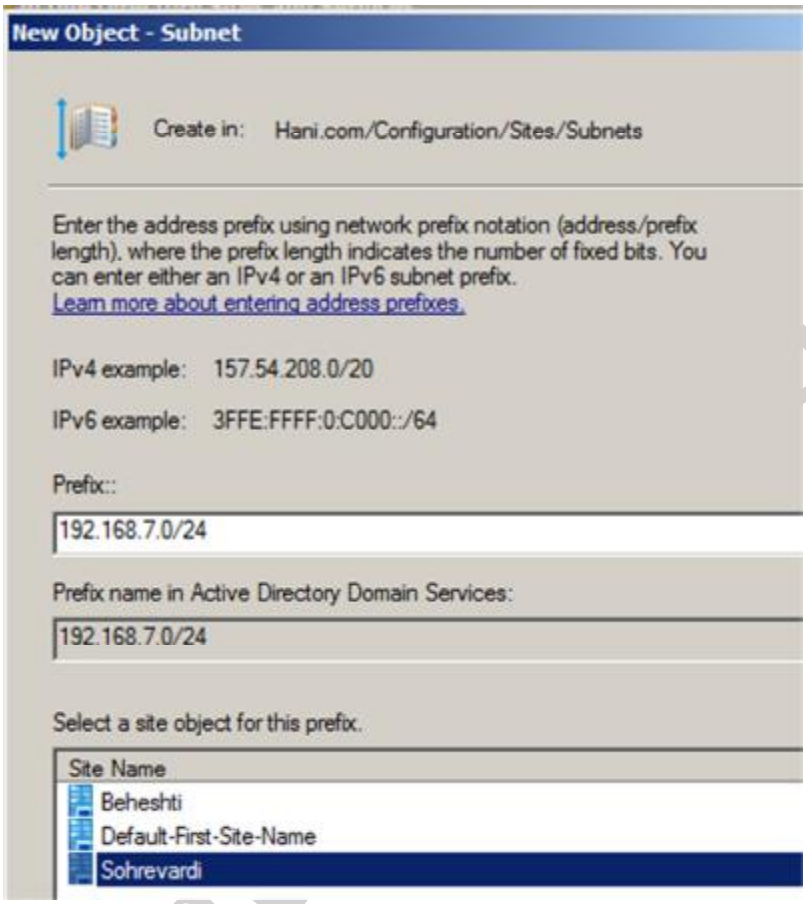


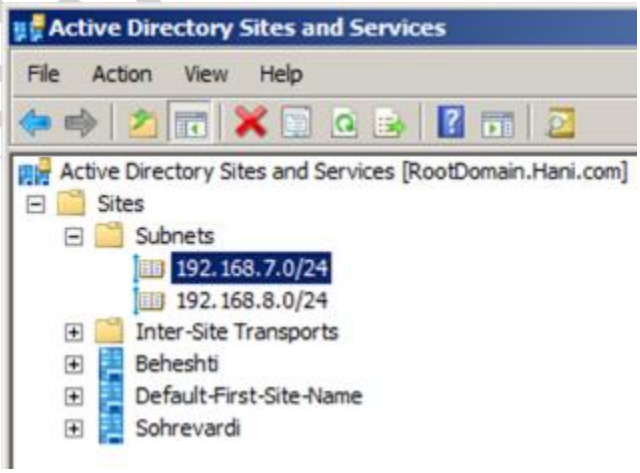

برای اینکه Subnet سایت هایمان را مشخص کنیم مانند زیر عمل می کنیم




FarsiDash

در اینجا مشخص کرده ایم که رنج 7 برای سهروردی می باشد و سرورهایی که در این رنج هستند در سهروردی احرازهویت می شوند.




رنج 8 را هم برای بهشتی در نظر می گیریم.

Farshad

## Group Policy

لینکی از رجیستری به صورت GUIمی باشد و برای Customize کردن کامپیوترها و کنترل روابط شبکه ای مورد استفاده قرار می گیرد وبر سه نوع Linked Group Policy, Default Domain Policy , Local Group Policy می باشد.

برای باز کردن Local Group Policy باید دستور gpedit.msc را در RUN وارد کنیم,در این نوع از گروپ پالیسی هر تغییری ایجاد کنیم فقط به همان سیستم اعمال می شود,از این دستور برای مدیریت در شبکه های Workgroup استفاده می شود.

### Defult Domain Policy

این نوع از پالیسی فقط در شبکه های دامینی قابل دسترس می باشد و با دستور Gpme.msc فعال می شود(این دستور فقط برای 2008 می باشد)هر تغییری در این نوع از گروپ پالیسی اعمال کنیم به کل شبکه اعمال می شود.

### Linked Group Policy

به گروپ پالیسی هایی گفته می شود که برای یک OU خاص و اعضای آن اعمال می گردد وفقط در شبکه های دامینی قابل دسترس می باشد.

- به پالیسی هایی که ما در شبکه ایجاد می کنیم Group Policy Object گویند.
- GPO ها را فقط می توان به Site,Domain,Ou اعمال کرد
- اگر بخواهیم به یک User,Group,Computer خاصی در شبکه پالیسی اعمال کنیم از روشی به نام Nesting استفاده می کنیم.
- Nesting در این روش باید ابتدا یک Ou بسازیم وUser,Group,Computer مورد نظر را در آن اضافه کنیم وسپس پالیسی از نوع Linkedرا به آن Ou اعمال کنیم.
- در پوشه SYSVOL پالیسی و اسکریپت های شبکه موجود می باشد و در هر بار که کلاینت روشن می شود ورژن این پوشه را با پوشه خودش چک می کند در صورت تغییر پوشه خودش را Update می کند.
- با نرم افزار Access Manager می توان سطح دسترسی تمامی یوزرها حتی Admin را هم تغییر داد.
- دستور Gpupdate یک دستور 2 طرفه می باشد یعنی هم باید بر روی کلاینت وارد شود و هم بر روی سرور.
- با زدن Gpupdate بر روی کلاینت,آن را مجبور می کنیم که ورژن Sysvol را با سرور چک کند و در صورت لزوم آن را بروز کند.
- در سرور AD گروپ پالیسی ها در 2 محل ذخیره می شوند Active Directory Templates ,Active Directory Container,پوشه Sysvol در Container می باشد و خود AD در Templates .
- با زدن دستور Gpupdate,پالیسی از روی AD (Templates)کپی می شود به پوشه Sysvol (Container).
- گاهی اوقات عمل کپی انجام نمی شود و ما مجبور به استفاده از دستور Gpupdate /Force می شویم.

FarshidAjabnoush

قوانین مربوط به پالیسی (Policy Rules)

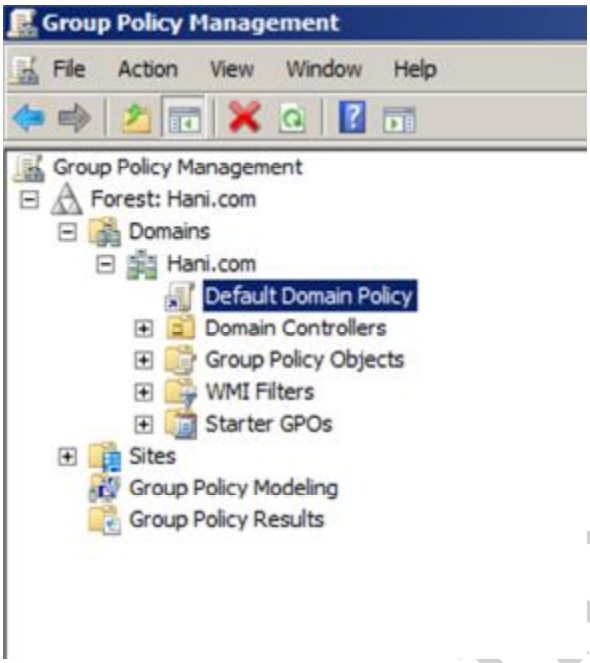
1. شبکه ای را در نظر بگیرید که در آن 2 Ou داریم و2 گروپ پالیسی از نوع GPO به آنها اعمال می شود,اگر GPO ها همدیگر را نفی نکنند به ترتیب از بالا به پایین (از1 شروع می شود) GPO ها اعمال می شوند به طور مثال در 1 GPO گفته شده است که Run وجود نداشته باشد و در 2 GPO گفته شده است Cmd وجود نداشته باشد این 2 یکدیگر را نفی نمی کنند پس به ترتیب اعمال می شوند.
2. اگر بین 2 پالیسی (GPO) تداخل یا نفی یکدیگر وجود داشته باشد,آخرین GPO اعمال می شود فرض کنید GPO1 می گوید Cmd وجود نداشته باشد ولی GPO2 می گوید Cmd وجود داشته باشد,در این نوع از تداخل GPO2 اعمال می شود.
3. اگر به یک Ou چندین پالیسی (GPO) اعمال شود قوانین 1و2 در مورد آن Ou باز هم صدقخواهد کرد.

- Admin می تواند ترتیب اعمال شدن پالیسی (GPO) را در شبکه با استفاده از Enforce,Block تغییر دهد.
- اگر بر روی یک ou گزینه Block آن فعال شود دیگر پالیسی های بالاسر به آن اعمال نمی شود فقط پالیسی های مربوط به خودش اعمال می شود,اگر Enforce فعال باشد فقط همان اعمال می شود و زیر مجموعه ها نا دیده گرفته می شوند.
- اگر هردو فعال باشد, Enforce ارجعیت به Blocked دارد.
- در 2003 برای دیدن گروپ پالیسی باید AD باز کنیم سپس تیک Advance را از تب View می زنیم روی اسم دامین Properties ,سپس یک تب به نام Group Policy اضافه شده است.

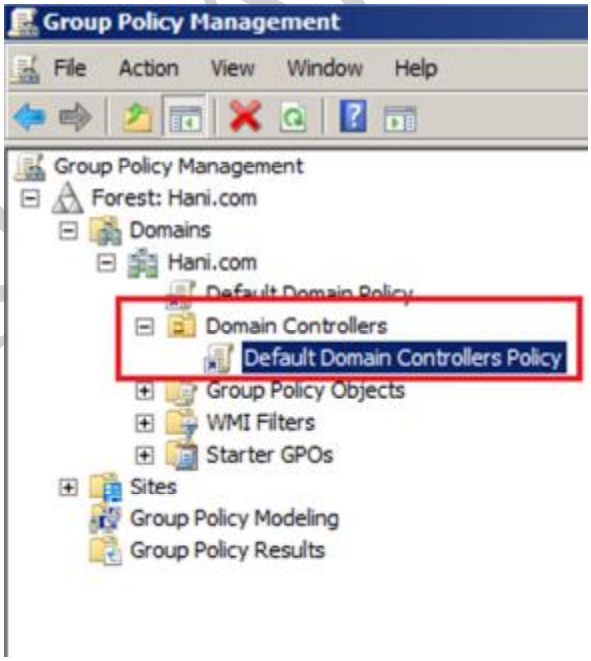
برای دسترسی به پالیسی ها در 2008 از منوی استارت مانند زیر وارد گروپ پالیسی می شویم

همانطور که در شکل زیر می بینید چون ما پشت Root هستیم می توانیم گروپ پالیسی کل فارست را مدیریت کنیم اگر مانند شکل زیر وارد ...Default شویم وEdit را بزنیم و تغییری را ایجاد کنیم آن تغییرات به کل اعضای Hani اعمال می شود.

FarshadAjabnoush

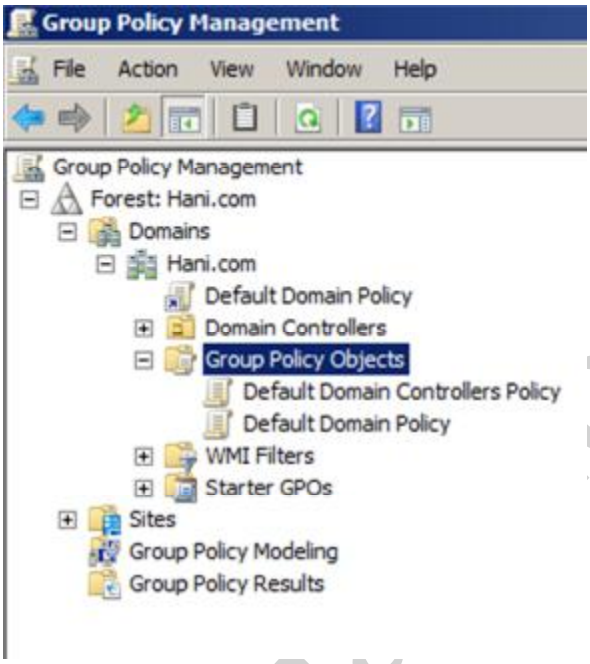



پالیسی دیگری که وجود دارد Domain Controlles می باشد که چون پشت Root هستیم آن را می بینیم اگر تغییری در اینجا اعمال کنیم به تمامی Domain Controllersاین فارست اعمال می شود,و از نوعLinked می باشد.

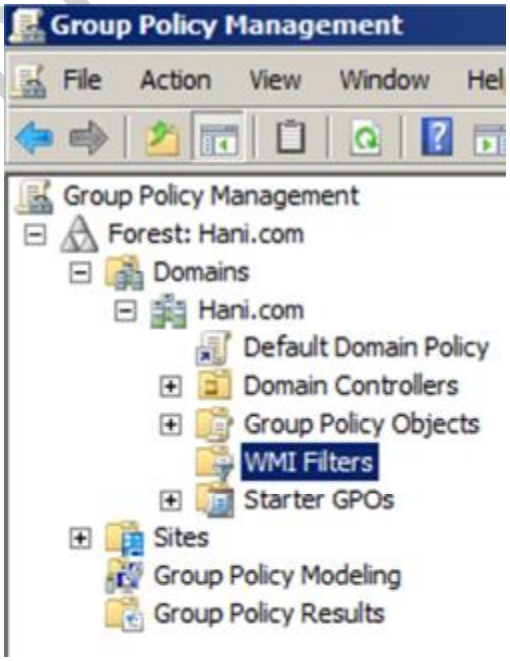



Farsi Arabi.ush

سپس نوبت به GPO می رسد




WMIیک زبان برنامه نویسی به فرمت WQLمی باشد که با آن می توان برای اعمال شدن پالیسی ها شروط سخت افزاری یا نرم افزاری تعیین کرد.

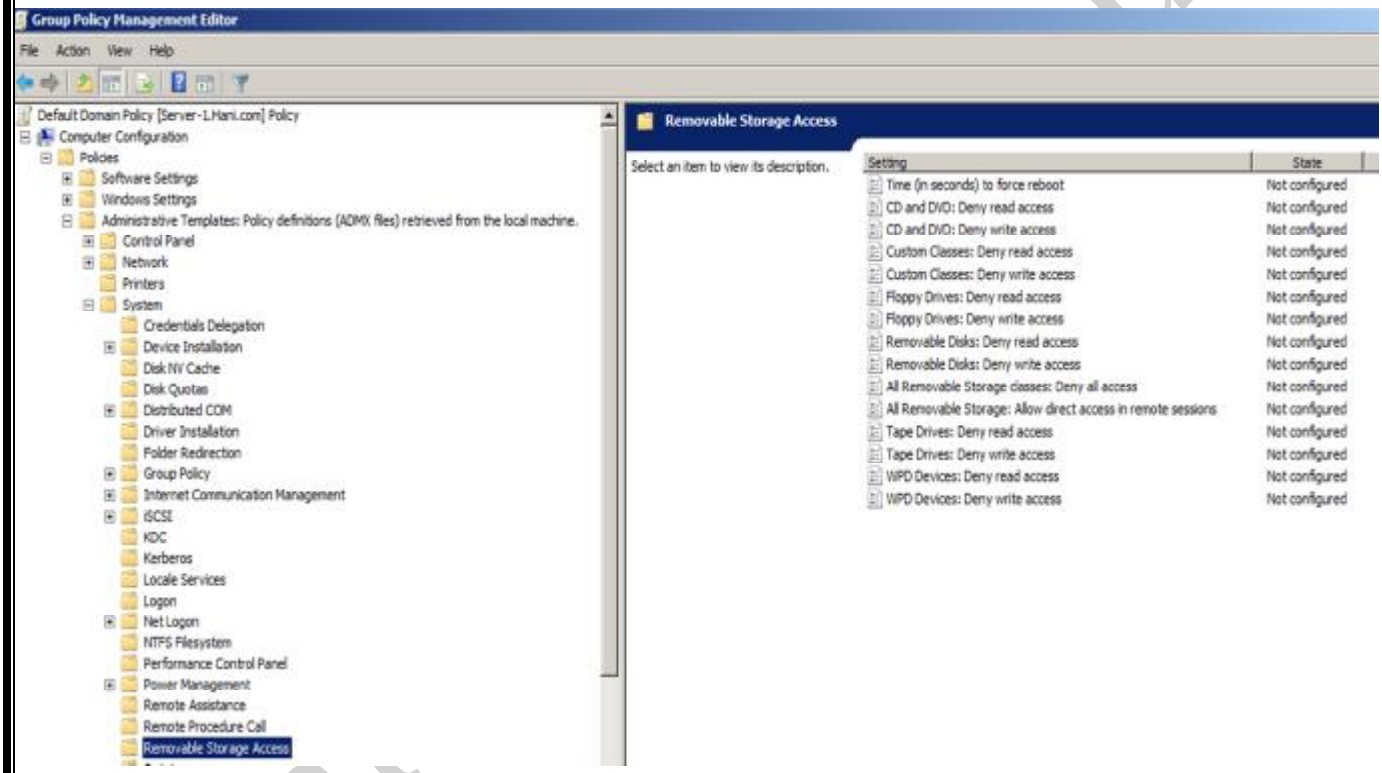



FarshidAj...oush

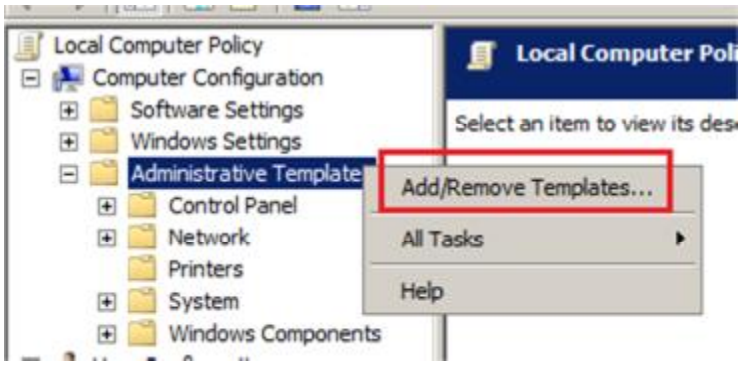
Starte GPOs : یک سری پالیسی می باشد که توسط Admin نوشته می شود و می توانند Attach بشوند به گروپ پالیسی و در 2008 با فرمت ADMX و در 2003 با فرمت ADM می باشد.

- در 2003 نمی توان توسط گروپ پالیسی USB ها را غیر فعال کرد ولی در 2008 امکان پذیر می باشد.
- بهترین نرم افزار برای کنترل USB ها در شبکه های دامینیDevice Lock می باشد.

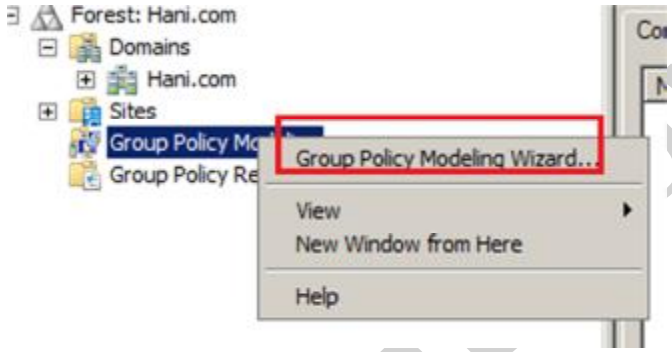
مسیر برای بستن USB



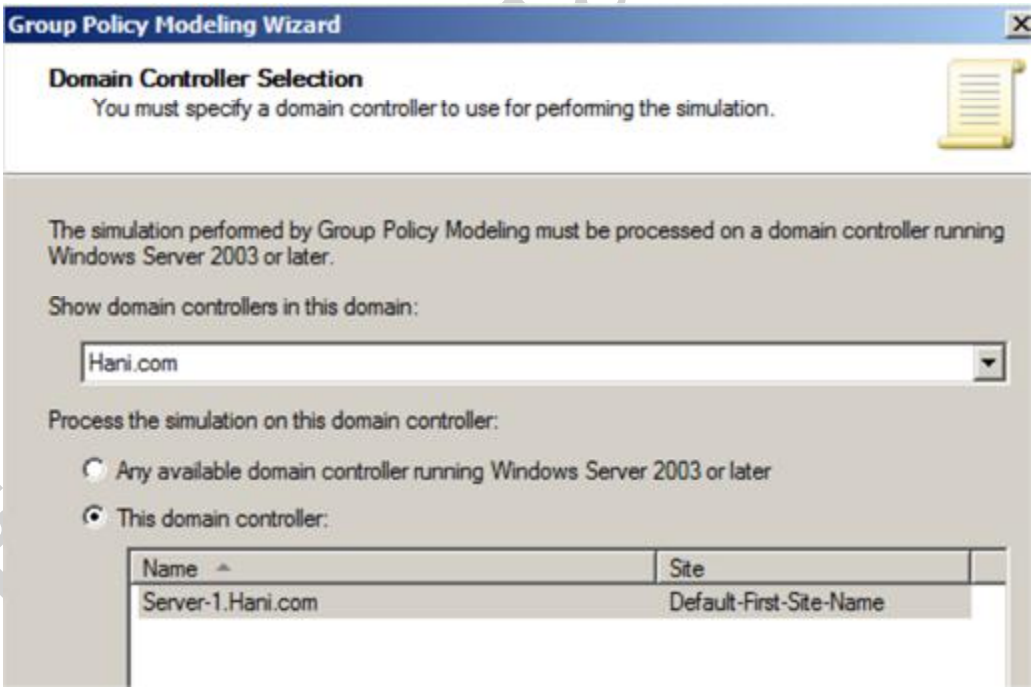

برای 2003 لازم است این پالیسی را با پسوند ADM دانلود کرده و آن را به گروپ پالیسی اضافه کرد برای اضافه کردن آن مانند زیر عمل می کنیم:



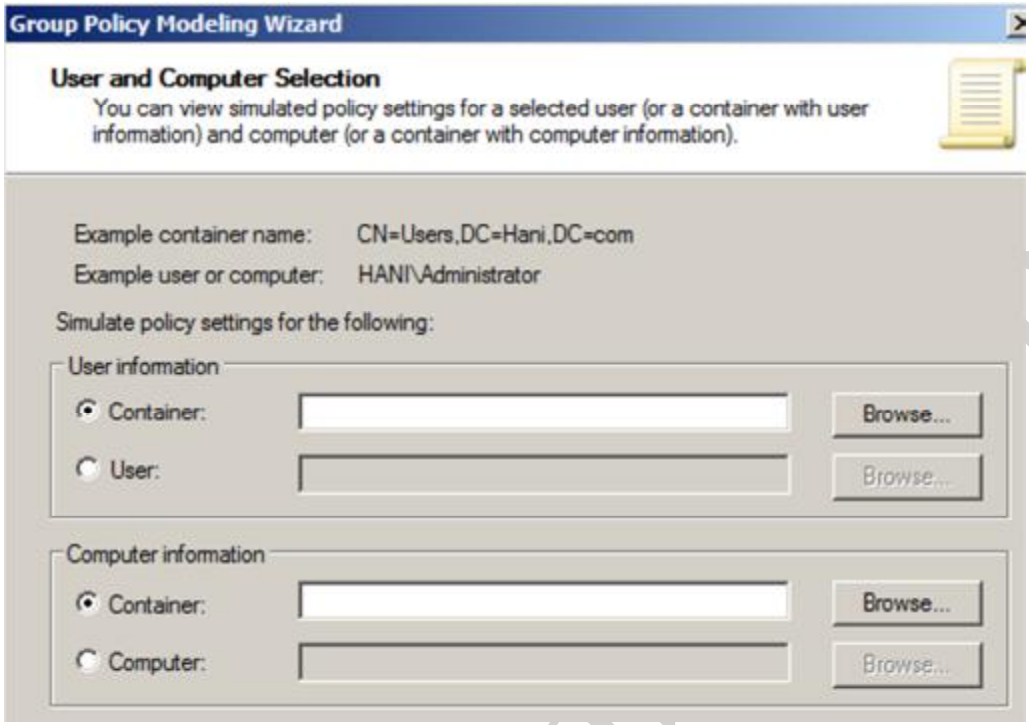

**قبل از اعمال گروپ پالیسی می توانیم آن را شبیه سازی کنیم**




**در اینجا مشخص می کنیم به کدام دامین اعمال شود(همه یا hani )**



سپس یوزر و کامپیوتر مورد نظر را انتخاب می کنیم




در آخر هم گزارش را بصورت html نشان می دهد.

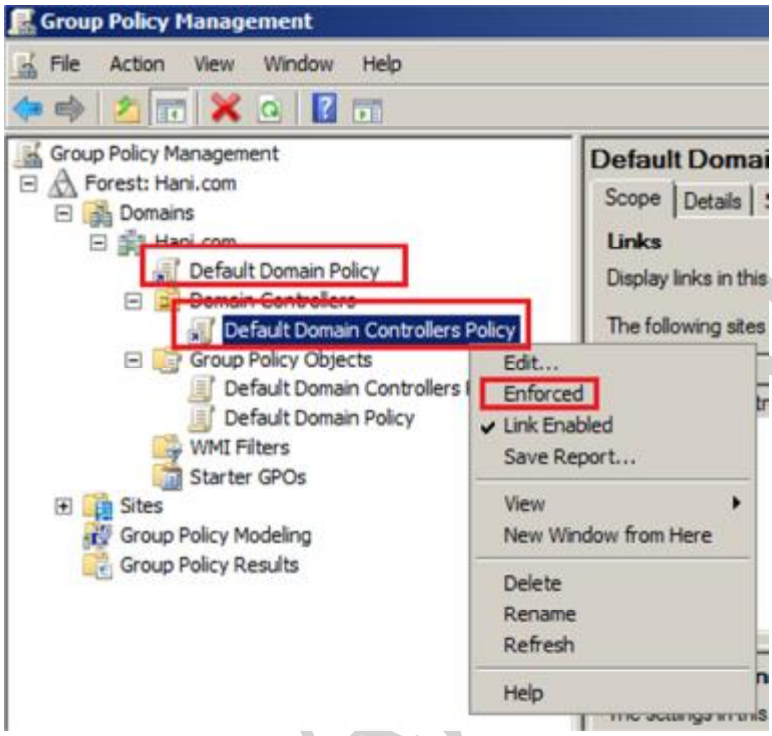
Group Policy Result

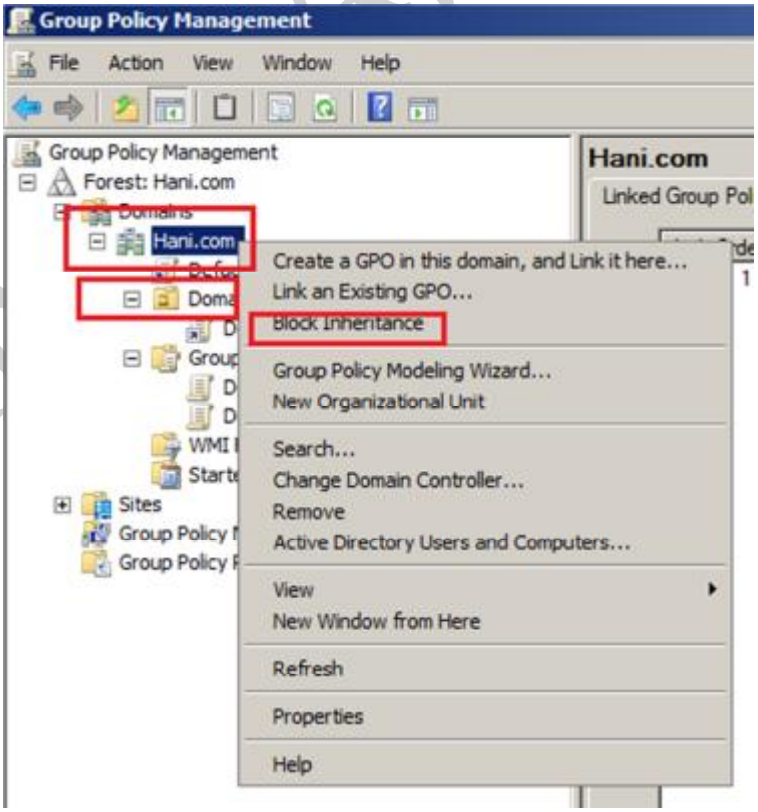
در اینجا می توانیم متوجه شویم در حال حاضر به کامپیوتر و یوزر مورد نظر چه پالیسی اعمال می شود

FarshidAjami

## تنظیمات Advance در Group Policy

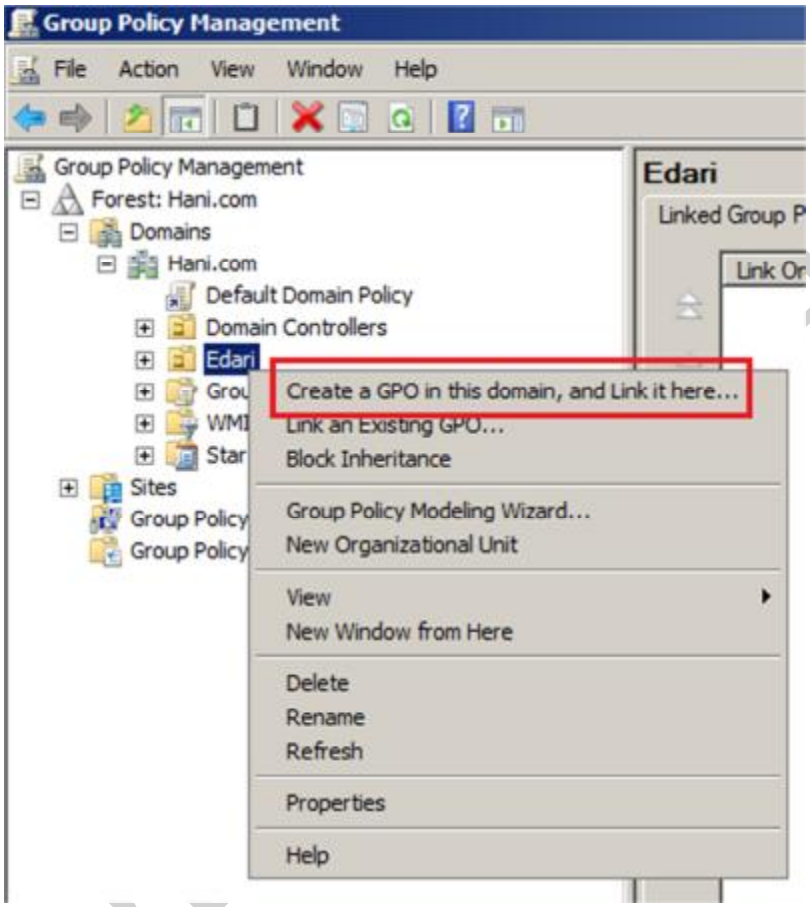
1. **تغییر دادن ترتیب اعمال پالیسی**



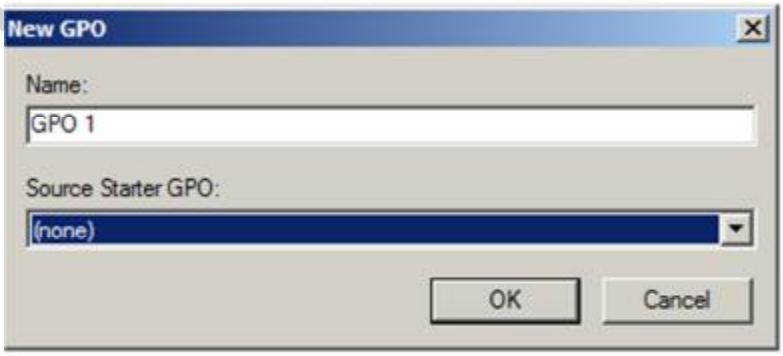




Farnoush

2. ایجاد Linked Group Policy: ابتدا یک Ou در اکتیو می سازیم (اینجا به نام Edari می باشد) سپس از گروپ پالیسی مانند زیر عمل می کنیم

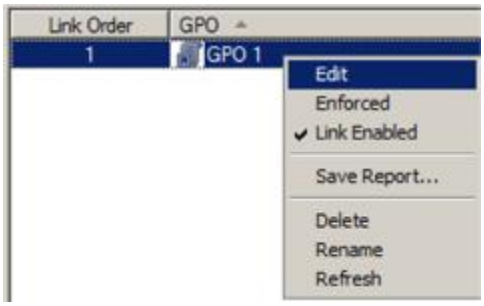



در اینجا یک اسم انتخاب می کنیم در قسمت سورس اگر پالیسی نوشته شده داشته باشیم Import می کنیم

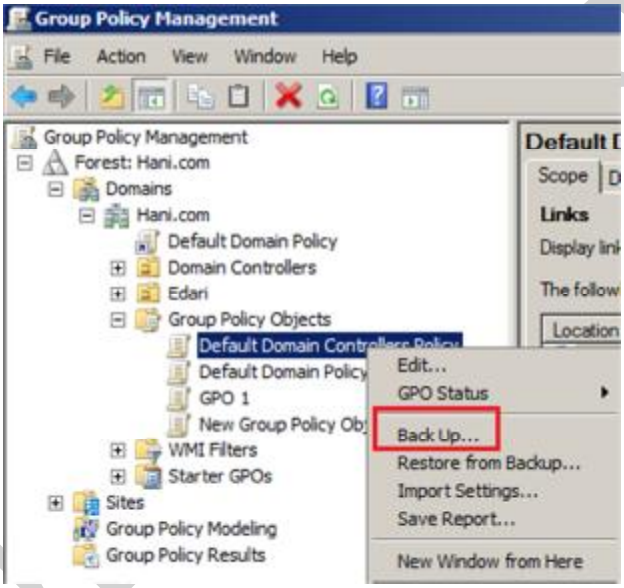



Farsi Tech

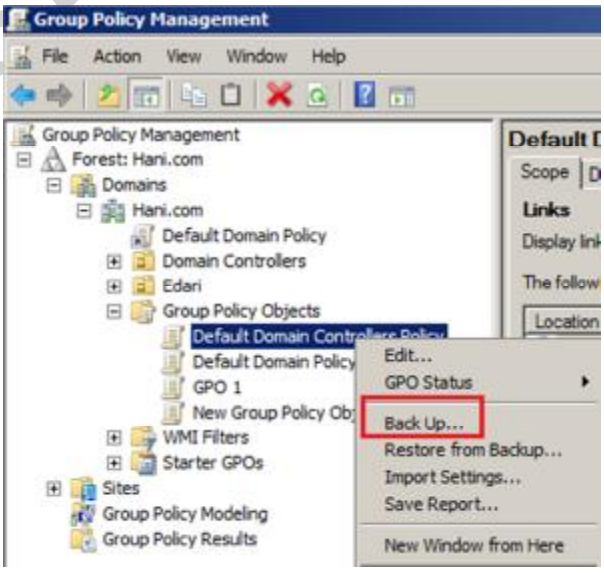
سپس با ادیت کردن این GPO هر تغییری که ایجاد کنیم به کل Ou اداری اعمال می شود.




3. Backup گرفتن از پالیسی ها



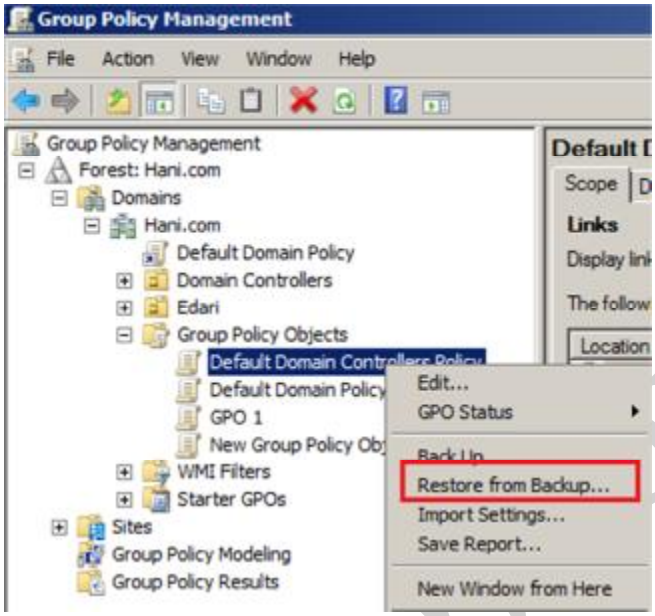

Or



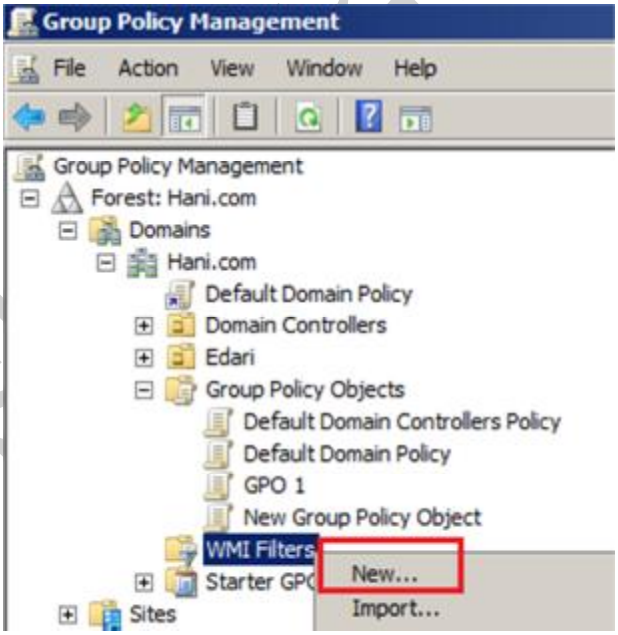

Farsi Roush

برای Restore کردن

یا از ...Restore frome و یا از Import Settings

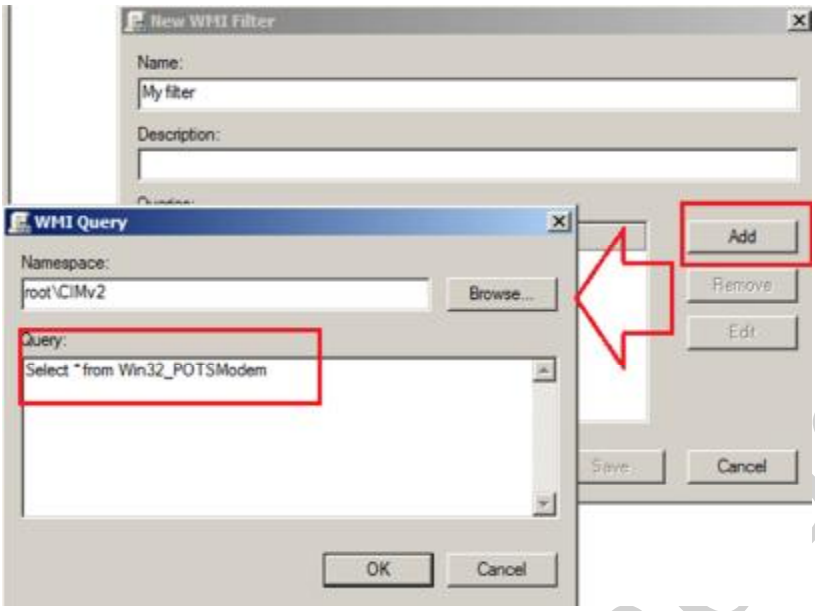



4. ایجاد یک WMI

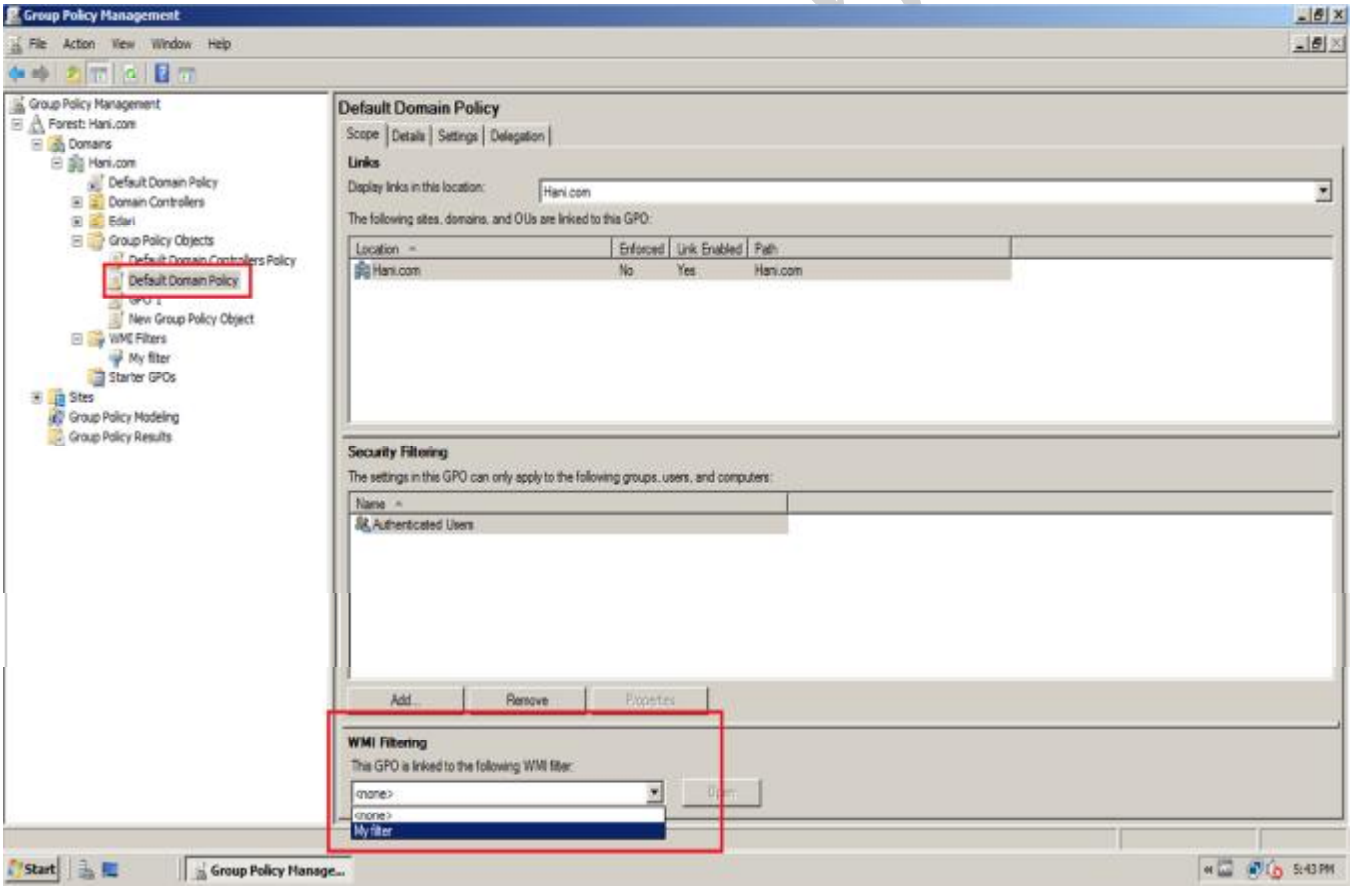



این شروط را می توان از اینترنت دانلود کرد،سپس یک اسم و Add و دستور را وارد می کنیم

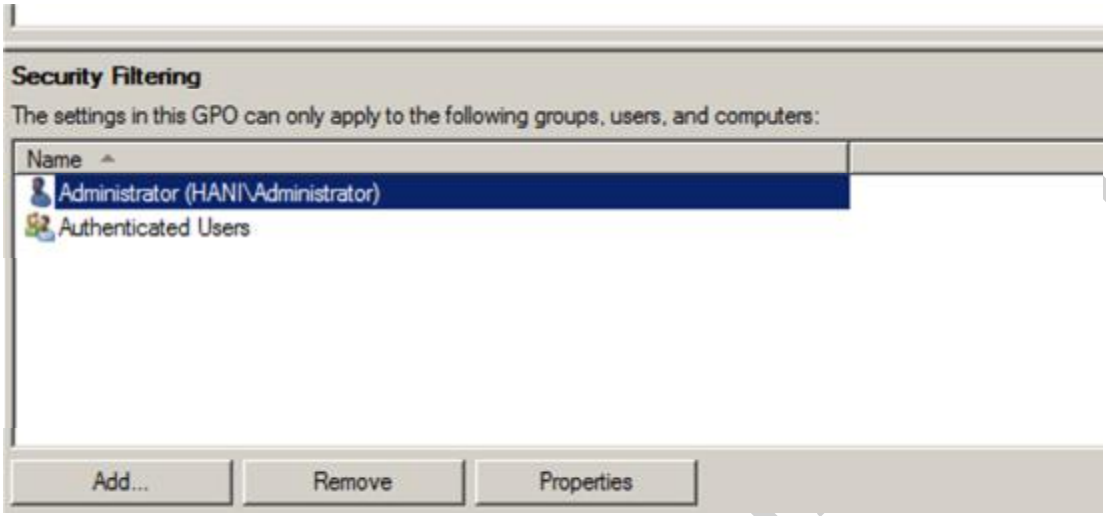
Farsroobgush



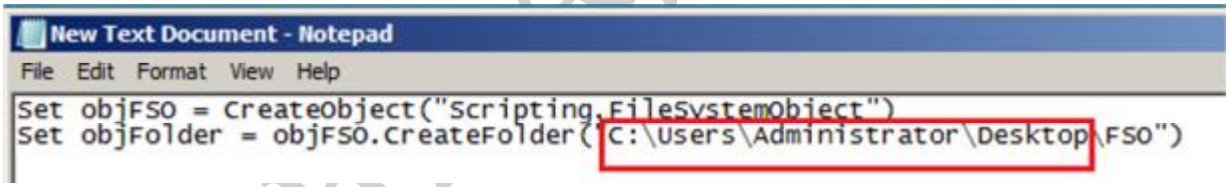

**بعد از Save کردن برای اعمال کردن این شرط روی پالیسی مورد نظر مانند زیر عمل می کنیم**



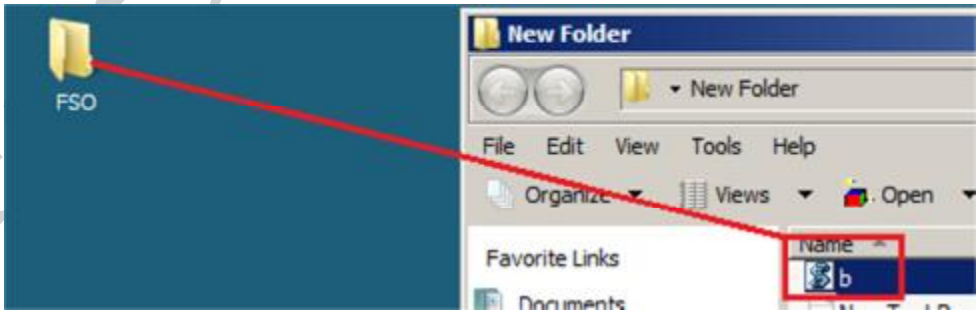
5. Security Filtering در گروپ پالیسی : گروپ پالیسی را به سایت,دامین,Ou می توان اعمال کرد,برای اینکه بتوان به یوزر پالیسی اعمال کرد ابتدا وار پالیسی مورد نظر می شویم ومانند زیر عمل می کنیم



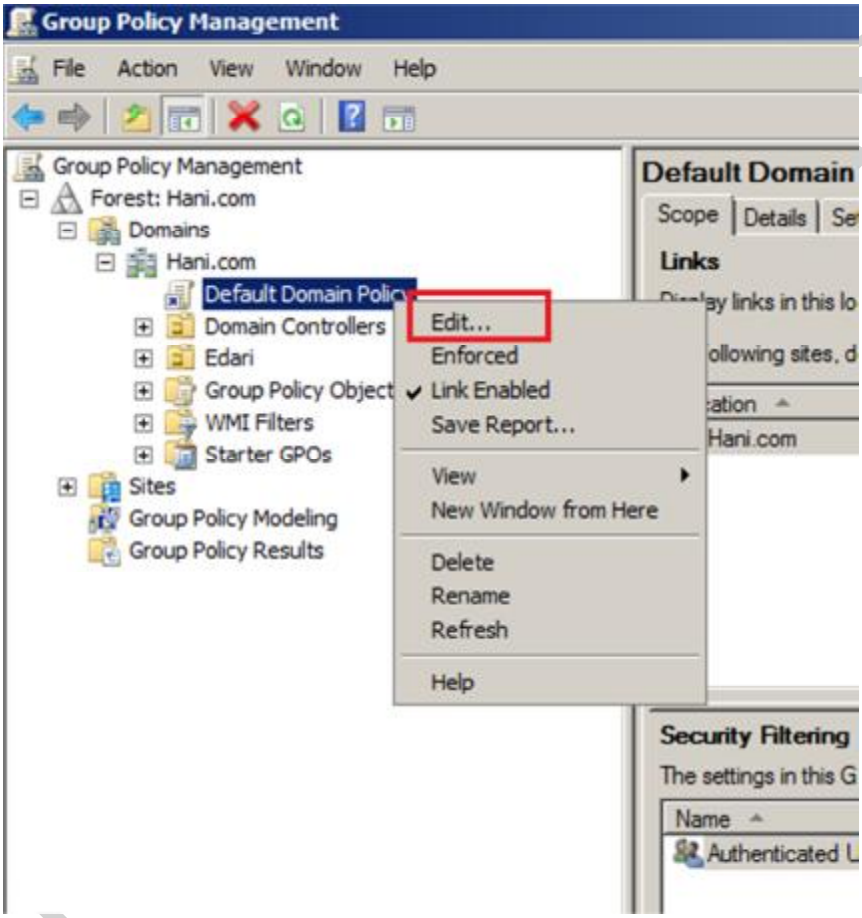

6. اعمال Script ها از گروپ پالیسی : زبان اسکریپت ها,VB Script می باشد,اسکریپت ها به صورت آماده وجود دارند برای استفاده از آنها یک Notepad باز می کنیم و متن آن را کپی می کنیم و در آخر با پسوند VBS ذخیره می کنیم,در اینجا این اسکریپت NewFolder می سازد.



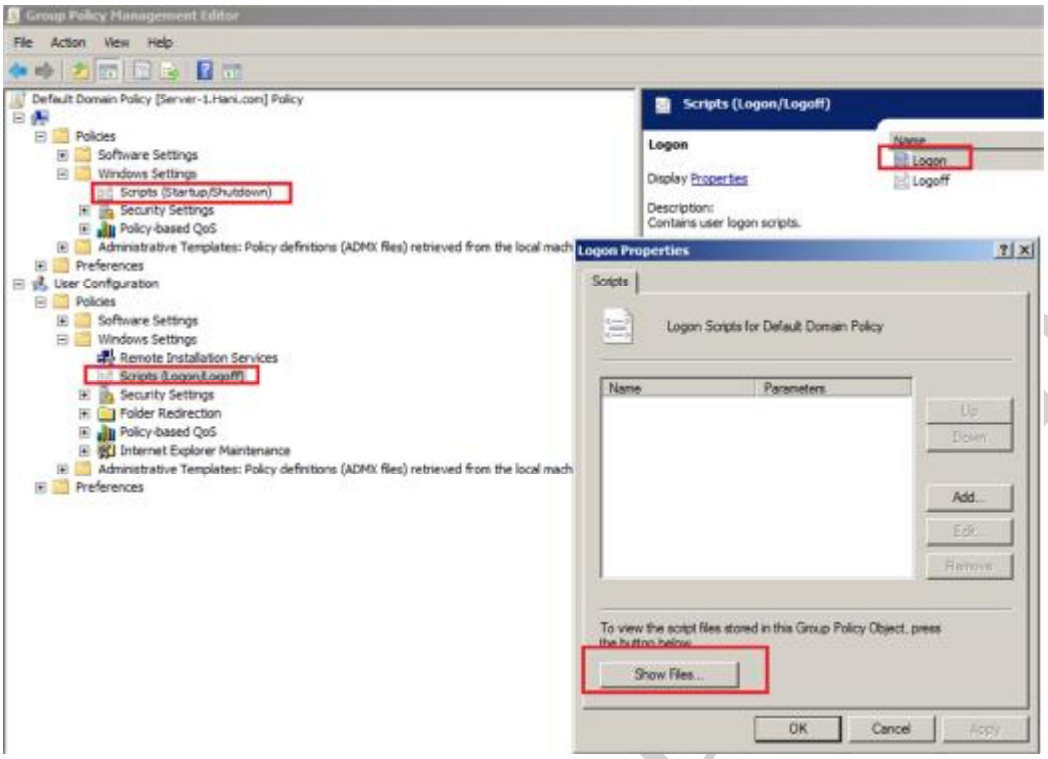

مسیر بالا را اضافه می کنیم سپس آن را "b.vbs" ذخیره می کنیم و با کلیک کردن بر روی آن فولدر ما ساخته می شود

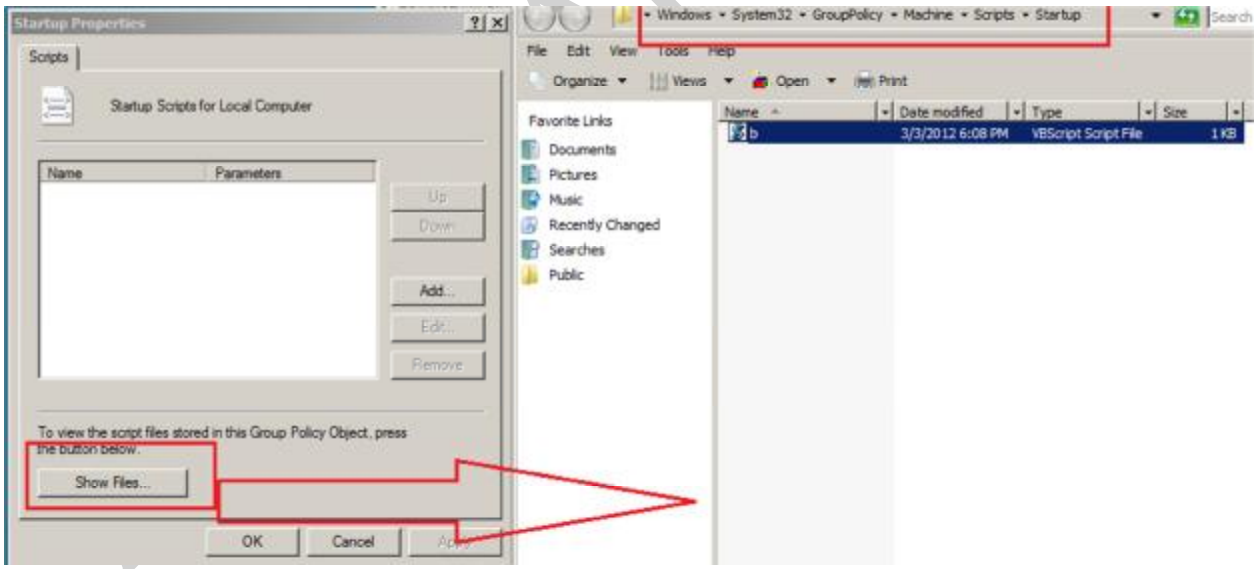


برای اینکه اسکریپت ها توسط گروپ پالیسی اعمال شوند وارد گروپ پالیسی ادیتور می شویم در 2 قسمت می توانیم آنها اضافه کنیم در قسمت اول زمان روشن و خاموش شدن سیستم اعمال می شود و در قسمت دوم هنگام Logoff وLogon کردن سیستم اعمال می شود,دراینجا روشن شدن را انتخاب می کنیم و بعد از آن حتما Show Files سپس اسکریپت مورد نظر را در صفحه باز شده توسط ..Show,کپی می کنیم

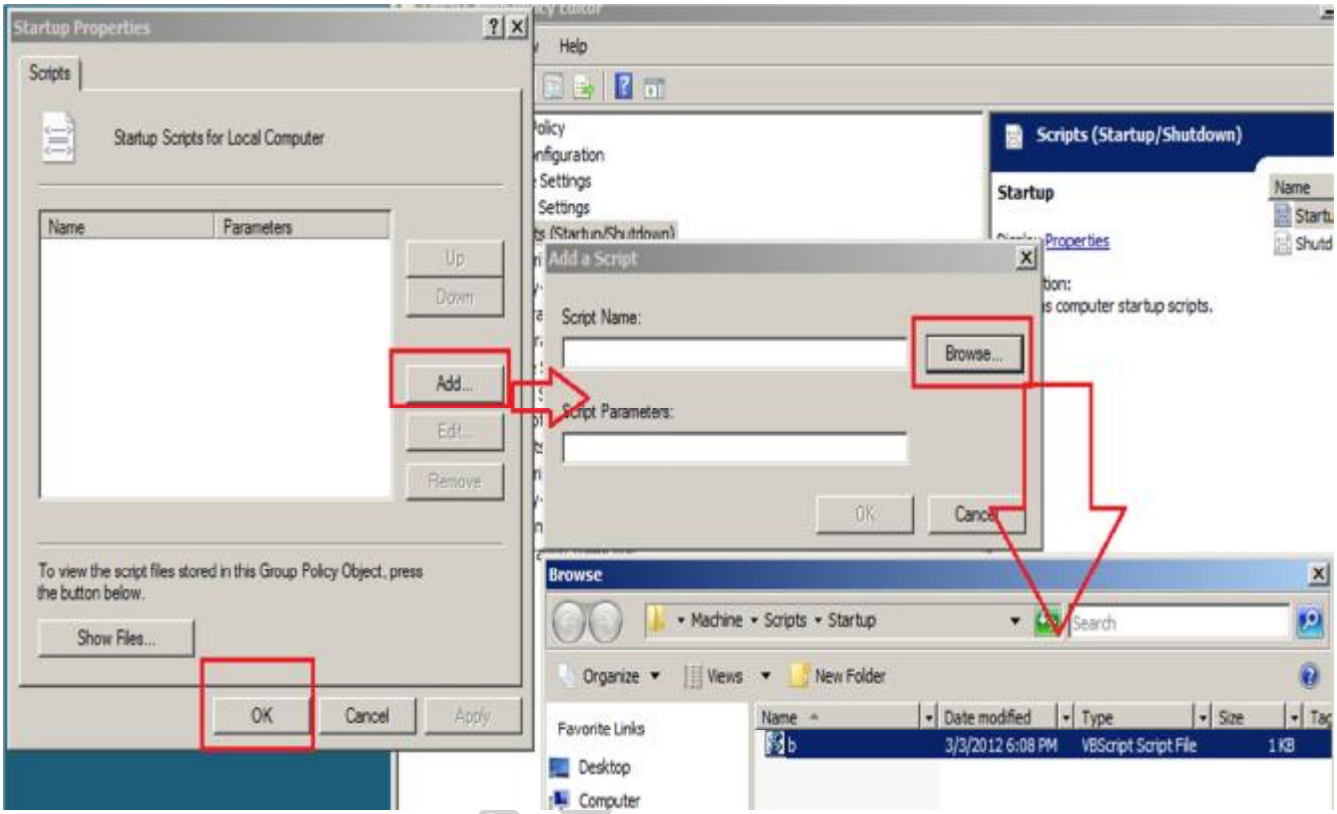



Farsh


Group Policy Management Editor
File Action View Help
Default Domain Policy [Server-1.Hani.com] Policy
Policies
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Security Settings
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) retrieved from the local mach
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Remote Installation Services
Scripts (Logon/Logoff)
Security Settings
Folder Redirection
Policy-based QoS
Internet Explorer Maintenance
Administrative Templates: Policy definitions (ADMX files) retrieved from the local mach
Preferences
Scripts (Logon/Logoff)
Logon
Display Properties
Description:
Contains user logon scripts.
Name
Logon
Logoff
Logon Properties
Scripts
Logon Scripts for Default Domain Policy
Name
Parameters
Up
Down
Add...
Edit...
Remove
To view the script files stored in this Group Policy Object, press the button below
Show Files...
OK
Cancel
Apply


Startup Properties
Scripts
Startup Scripts for Local Computer
Name
Parameters
Up
Down
Add...
Edit...
Remove
To view the script files stored in this Group Policy Object, press the button below.
Show Files...
OK
Cancel
Apply
Windows System32 GroupPolicy Machine Scripts Startup
Search
File Edit View Tools Help
Organize
Views
Open
Print
Favorite Links
Documents
Pictures
Music
Recently Changed
Searches
Public
Name
Date modified
Type
Size
b
3/3/2012 6:08 PM
VBScript Script File
1 KB

و در آخر Add را می زنیم و اسکریپت مورد نظر را از مسیر باز شده انتخاب می کنیم

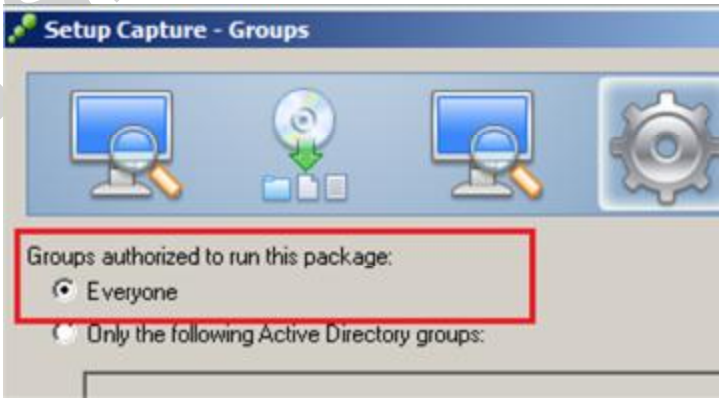



Farshid

7. نصب نرم افزار از گروپ پالیسی : برای این کار باید نرم افزار مورد نظر با پسوند msi. باشد,در اینجا exe. اجرا نمی شود,با نرم افزار Vmwarethinapplication می توان نرم افزارهارا به msi. تبدیل کرد.

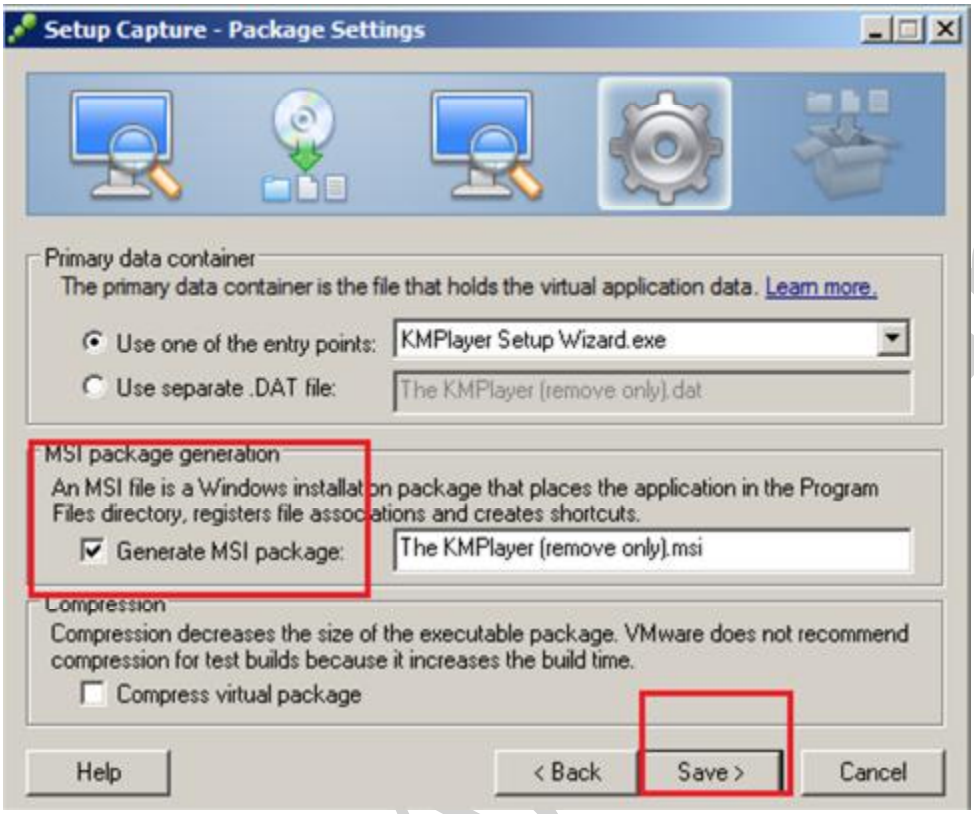
بعد از نصب و اجرای Vmwarethinapplication وقتی به مرحله زیر رسیدیم تازه نرم افزار مورد نظرمان(در اینجا KmPlayer ) نصب می کنیم

سپس می گوید چه کسانی دسترسی داشته باشند




و در آخر هم Finish

Farsh

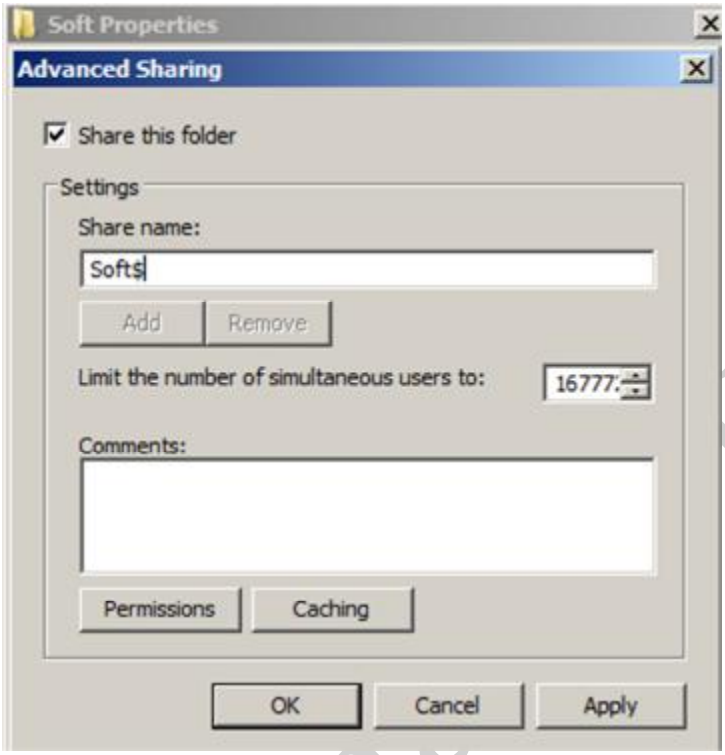



در ویندوز دستوری به نام lexpress داریم که کار تبدیل به msi را انجام می دهد.

- مزیت msi. این است که می توان سریال آنها را داخلشان گذاشت و موقع نصب می بینیم جای سریال پر شده می باشد.
- بهترین سایت آموزشی ehow.com می باشد.
- اگر نرم افزاری را بصورت Command و با دستور Setup.exe -a نصب کنیم,msi ساخته می شود,برای این کارد با دستور cd وارد پوشه مورد نظر می شویم وبجای setup.exe اسم نرم افزار را می نویسیم مانند yahoo.exe -a

از طریق گروپ پالیسی نرم افزارها را می توان Assign و Publish کرد,اگر Publish شود درقسمت Add\Remove Programs در کلاینت ها قابل مشاهده است و یک Add هم در کنار نرم افزار اضافه می شود که کلاینت با زدن آن می تواند آن نرم افزار را نصب کند(احتیاج به دسترسی نصب برای یوزر نیست,یک یوزر معمولی هم اجازه نصب این نوع نرم افزارها را دارد),ولی اگر نرم افزاری Assign شود آیکون آن در All Programs اضافه می شود و هنگامی که یوزر بخواهد آن را اجرا کند,آن نرم افزار نصب می شود.

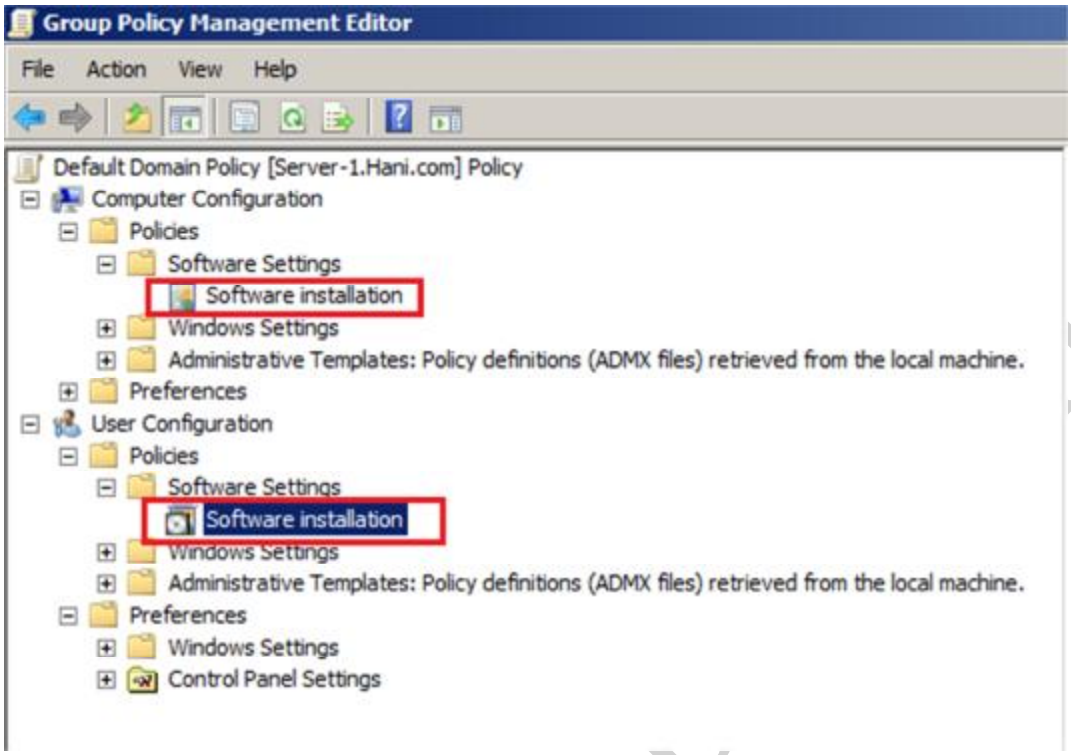
ابتدا باید نرم افزار مورد نظر را داخل پوشه ای قرار داد و آن پوشه را Share کنیم



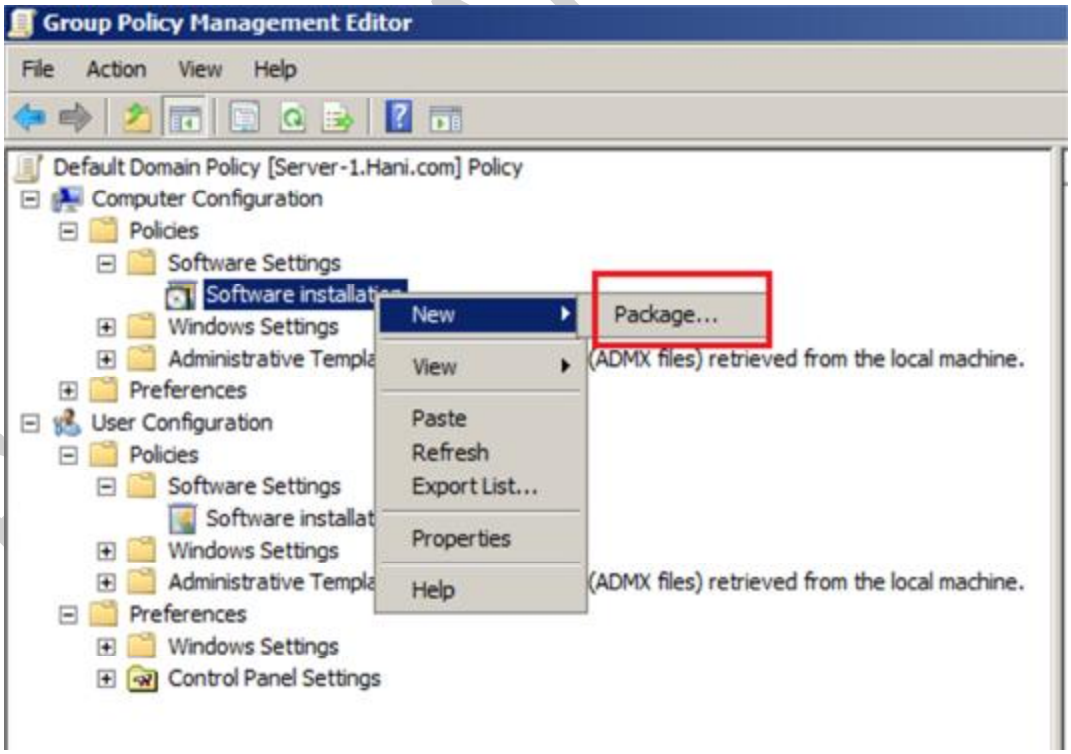

بعد از Share کردن نوبت به باز کردن گروپ پالیسی ادیتور می رسد بعد از این کار وارد Software Installation می شویم,همانطور که می بینید Soft... 2 وجود دارد که در اولی می توان نرم افزار را Assign کرد و در دومی می توان نرم افزار را هم Publish و هم Assignکرد.

- بهتر است برای Assign از اولی ( Computer ) و برای Publish از دومی (User) استفاده کنیم.

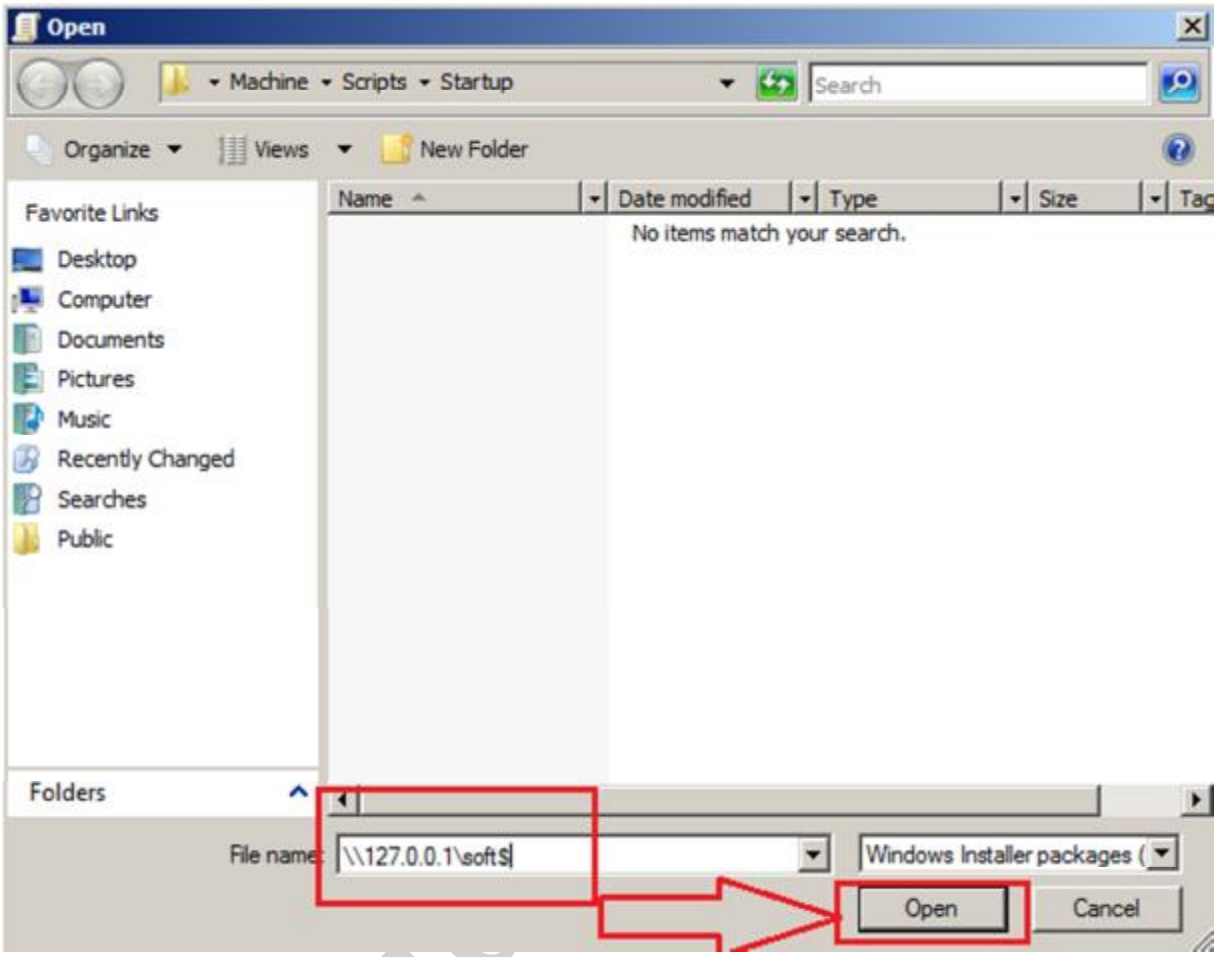
FarshidAjamush



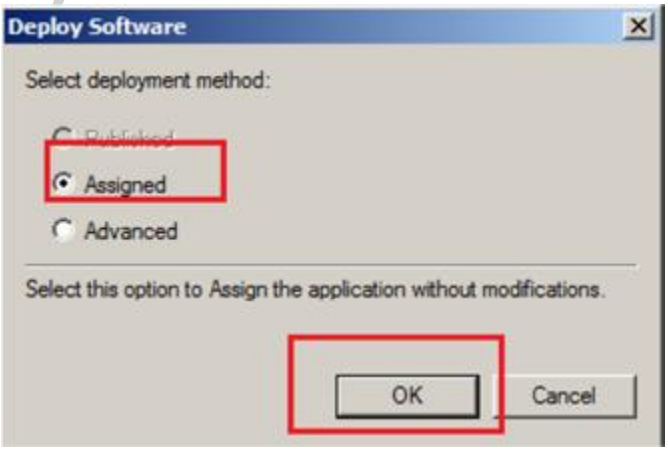

**نوبت به باز کردن فولدر مورد نظر می رسد برای این کار مانند زیر عمل می کنیم**



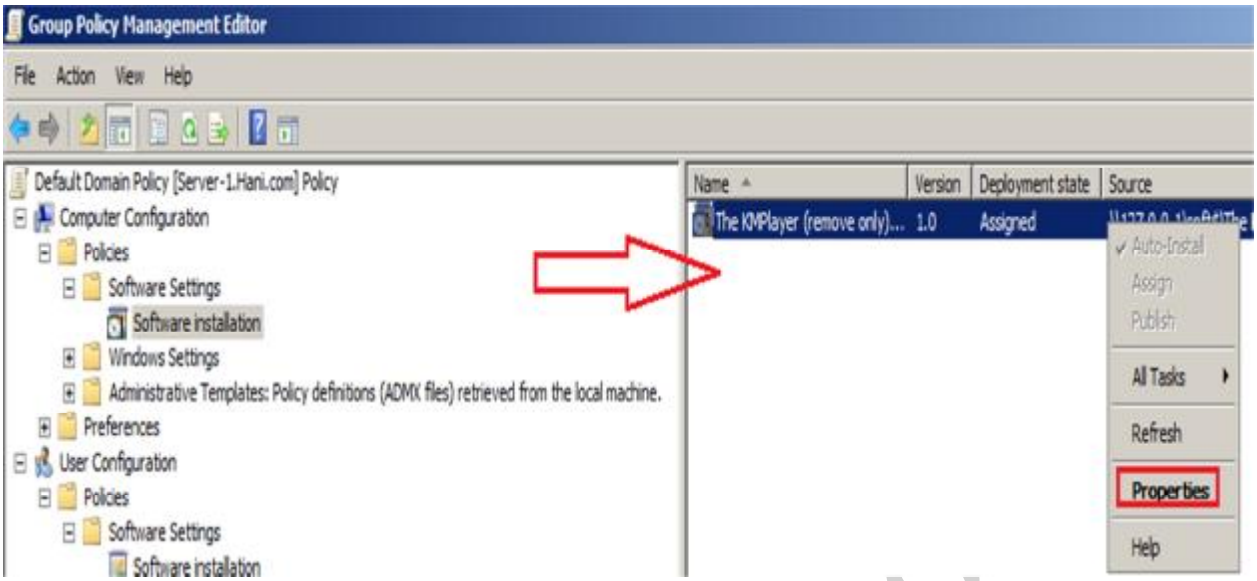
حتما باید برای باز کردن پوشه نرم افزار(soft ) به صورت UNC به سیستم خودمان وصل شویم



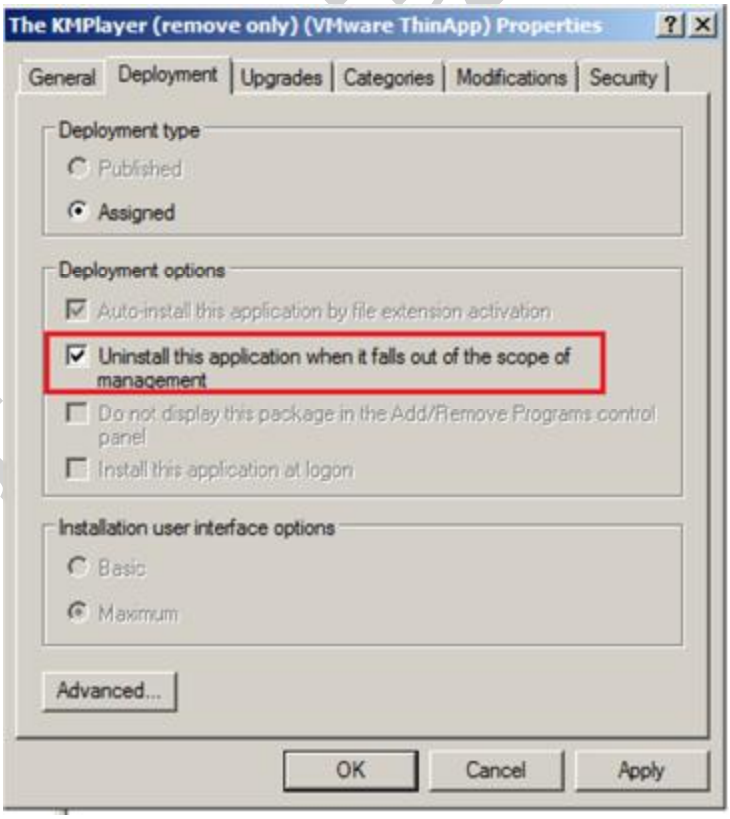

سپس نرم افزار مورد نظر که در اینجا باید با پسوند msi. ذخیره شده باشد را انتخاب می کنیم,بر روی Assign کلیک می کنیم.



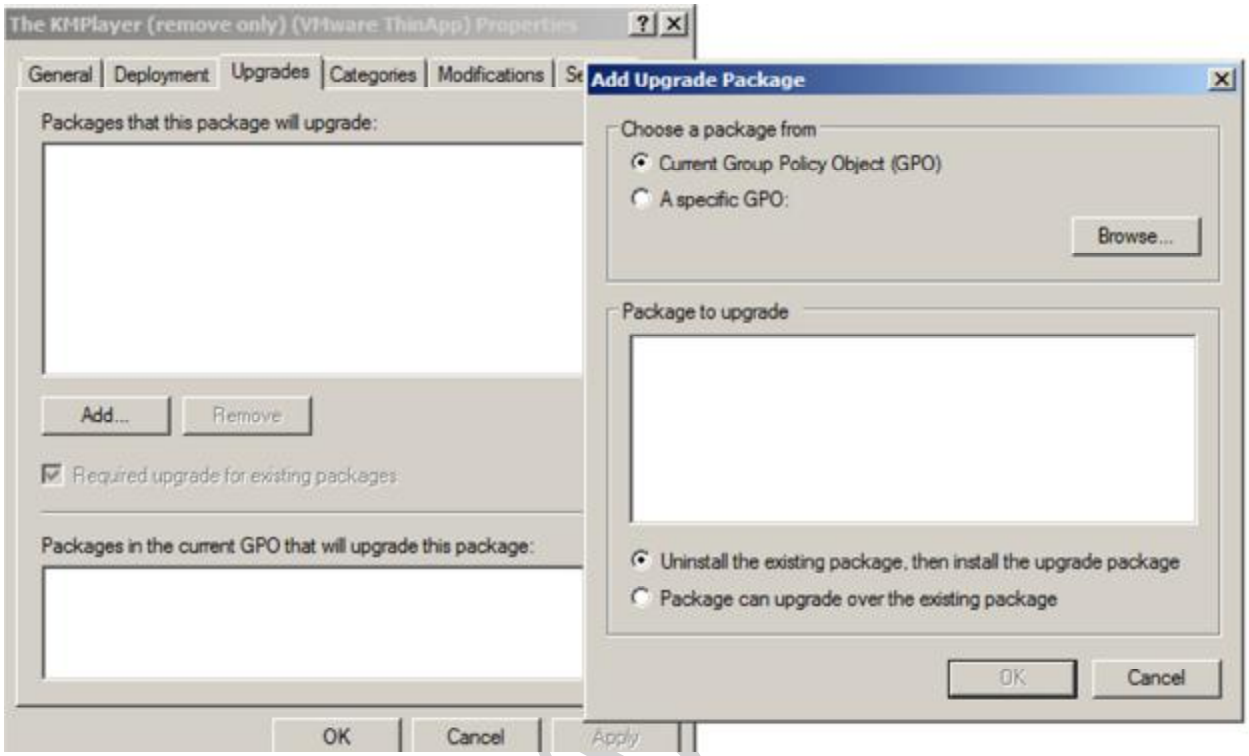

حالا نرم افزار ما اضافه شده است و باید از آن Properties بگیریم (تیک Auto-Installفعال است)



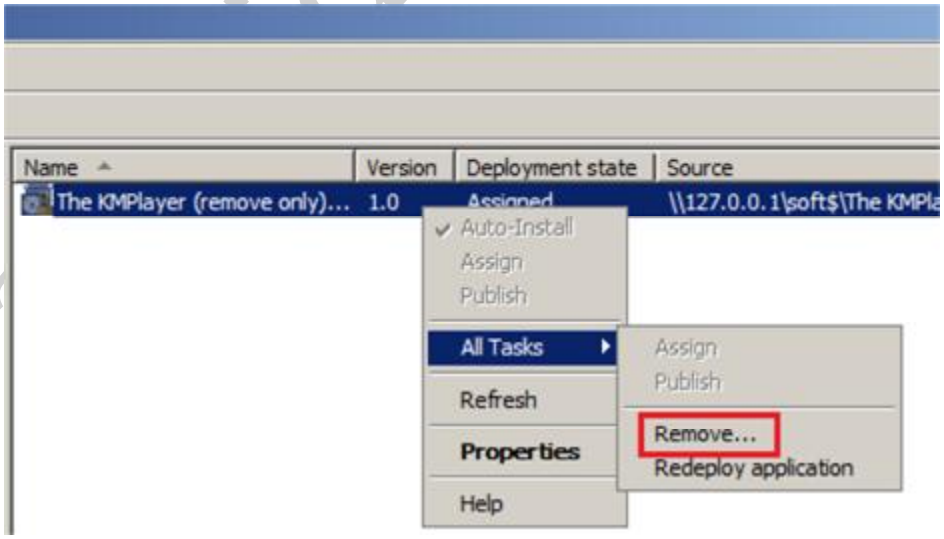

در تب دوم با فعال کردن گزینه مورد نظر زمانی که یوزری عضو Ou خاصی باشد نرم افزارهای خاص همان Ou برایش نصب می گردد(اتوماتیک) و زمانی که از آن Ou بیرون بیاید و به Ou دیگری برود آن نرم افزارهای Ou قبلی به صورت اتوماتیک پاک می شود و نرم افزارهای Ou جدید نصب می شود.



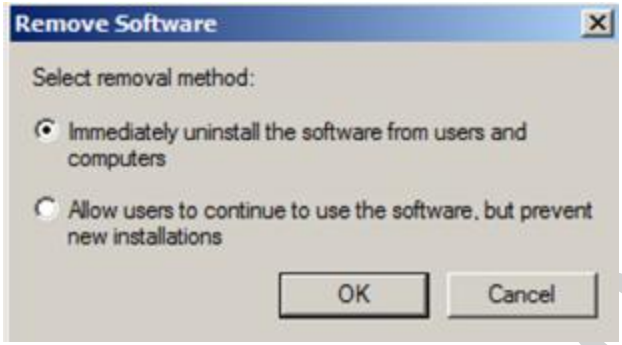
تب Upgrades: اگر نسخه جدیدتری از نرم افزارمان در شبکه موجود باشد آن را نشان می دهد حتی می تواند از گروپ پالیسی دیگر آن را بخواند




برای Remove کردن نرم افزار از روی کلاینت ها مانند زیر عمل می کنیم

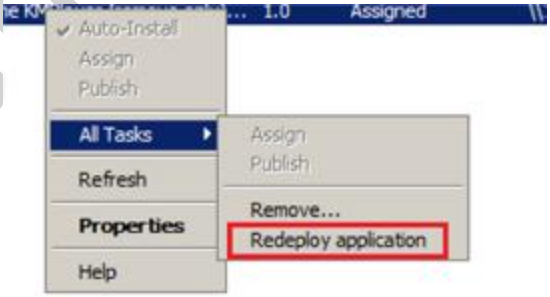


سپس با پنجره زیر مواجه می شویم



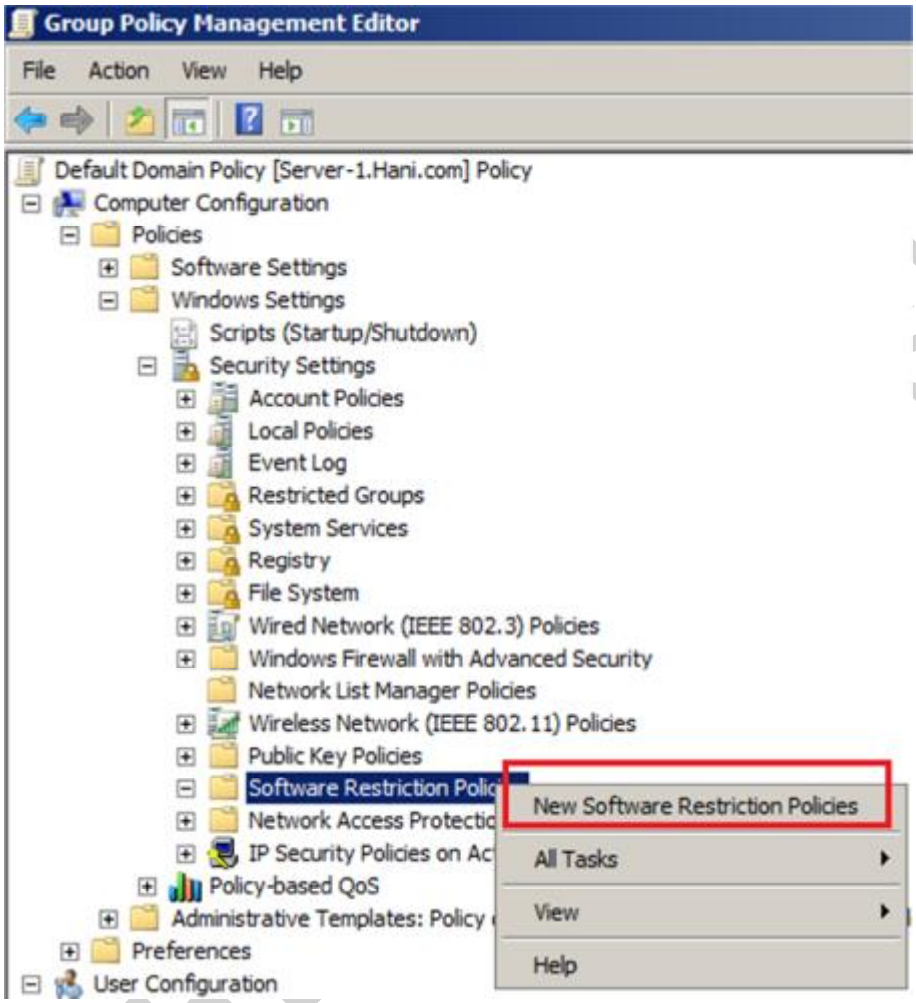

گزینه اول می گوید فورا نرم افزار را پاک کن گزینه دوم می گوید با تایید یوزر نرم افزار را پاک کن و اگر یوزر تایید نکرد نرم افزار را پاک نکن ولی دیگر توسط سرور پشتیبانی نمی شود(آپدیت نرم افزار).

اگر نرم افزار بعد از نصب مشکل داشت و باید دوباره نصب شود از گزینه زیر استفاده می کنیم



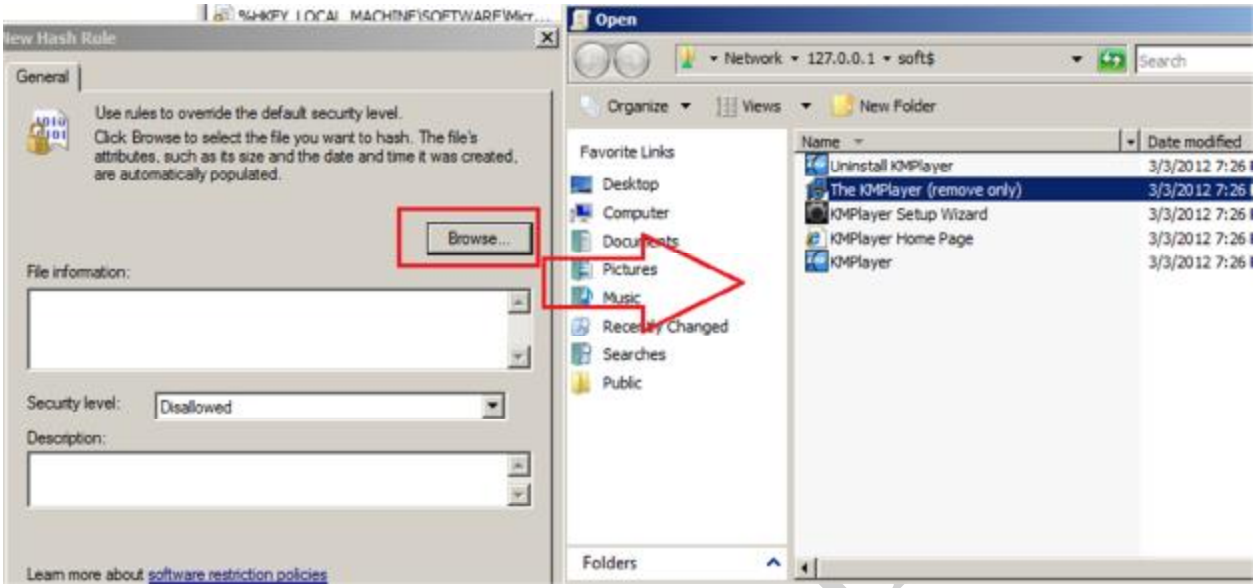

FarshidAjabnoush

برای  جلوگیری از استفاده نرم افزاری در شبکه باید Hash آن را ببندیم برای این کار مانند زیر عمل می کنیم



Farsh

سپس نرم افزار را انتخاب می کنیم




و در آخر هم ....Security آن را Dissallowed می کنیم,با این کار نرم افزار موردنظر با هیچ دسترسی حتی Admin ,در شبکه کار نمی کند(البته باید این پالیسی از نوع Default Domain Policy باشد,که در اینجا هست)

Opration Master

دامین کنتلررها ی شبکه برای کنترل و مدیریت بهتر فارست علاوه بر نقش دامین کنترلر یک سری نقش های دیگر هم بازی می کنند که در اصطلاح به این نقش ها Opration Master Roles گویند که عبارتند از :

Schema master,PDC Emulator Master,Infrastructure Master,RID Master,Domain Naming Master

- بصورت پیش فرض تمامی این نقش ها را RootDomain بر عهده دارد,به این دلیل که وجود تمامی این نقش ها در فارست الزامی می باشد.
- Schema master: زمانی که تغییری در Object ها ایجاد شود,این پارتیشن تغییرات اعمال شده را به بقیه دامین کنترلرهااعلام می کند(مثل نصب Exchange که ویژگی Send,Receive را به یوزرها اضافه می کند)
- Infrastructure Maste : تغییرات اعمال شده بر روی Group Member Ship ها اعلام می کند(عضویت یوزرها را در گروه ها بررسی می کند)
- PDC Emulator Master : این نقش 2 ویژگی دارد:1- می تواند سرور BDC برای شبکه مبتنی بر NT باشد

2-گزارش دادن تغییرات اعمال شده بر پسوردها(عوض کردن پسوردها)

FarshidAjabi

- RID Master : این ویژگی باعث می شود که در یک شبکه Object2 با RID 1 به وجود نیاید.
- زمانی که یوزری را از AD پاک می کنیم برای اینکه از History اکتیو هم پاک شود باید دستور

Netdom sid history را اجرا کرد (برای کامل و صحیح کار کردن با این دستور حتما Search انجام دهید)

- Domain Naming Master : ویژگی این نقش این می باشد که گزارش هر دامین کنترلری که به شبکه اضافه یا کم شود را به بقیه سرورها اعلام می کند.
- Opration Master ها دو ویژگی دیگر به نامهای Transferring و Seizing دارند.

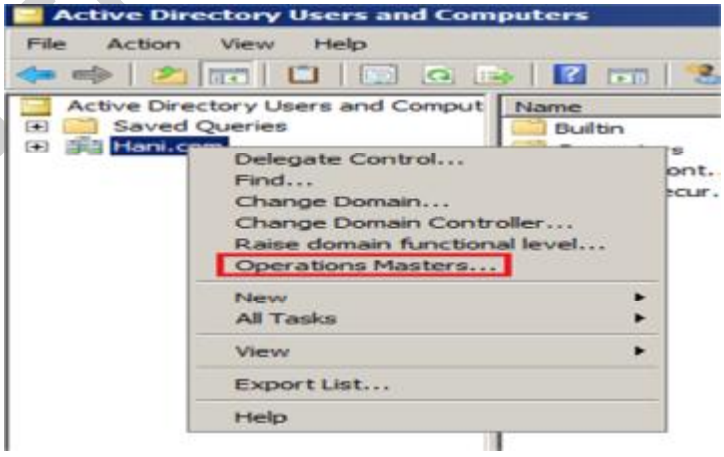
Transferr : تمامی 5 نقش گفته شده در بالا بر عهده یک سرور می باشد اگر بخواهیم تعدادی از این نقش ها را به سرور دیگری بدهیم (Load Balancing) از این روش استفاده می کنیم.

Seizing : ما در شبکه هایمان علاوه بر PDC یک سرور BDC هم داریم,زمانی که سرور اصلی ازکار افتاد سرور کمکی وارد شبکه می شود ولی 5 نقش بالا را ندارد به این دلیل که این 5 نقش به صورت پیش فرض بر روی سرور اصلی می باشد برای اینکه به این مشکل برنخوریم باید توسط یک نرم افزار از سرور اصلی که شامل 5 نقش بالا می باشد به صورت دستی Backup بگیریم.

- زمانی که سرور اصلی دچار مشکل و خواستیم سرور پشتیبان را وارد شبکه کنیم باید 2 کار را انجام دهیم اولین کار این می باشد که آن 5 نقش را از سرور اصلی بگیریم و به سرور کمکی بدهیم(Seiz ),دومین کار این می باشد که DNS را طوری تنظیم کنیم که سرور پشتیبان را به عنوان سرور اصلی شناسایی کند.

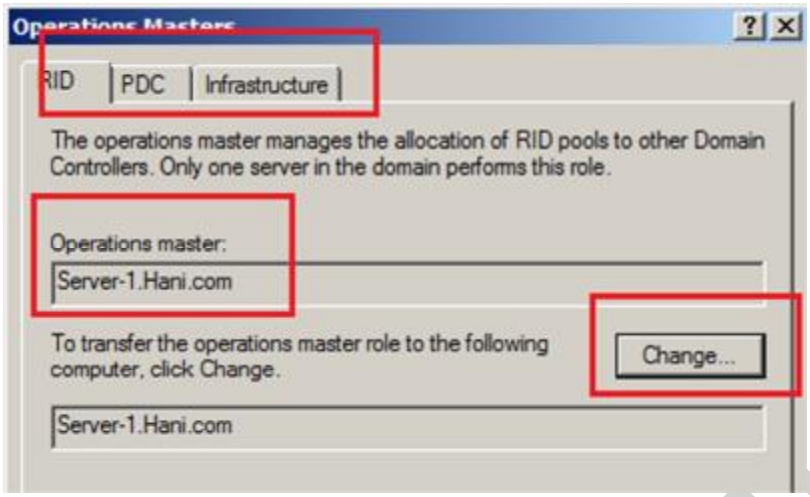
نحوه Transferr وSeiz,Opration Master ها در شبکه

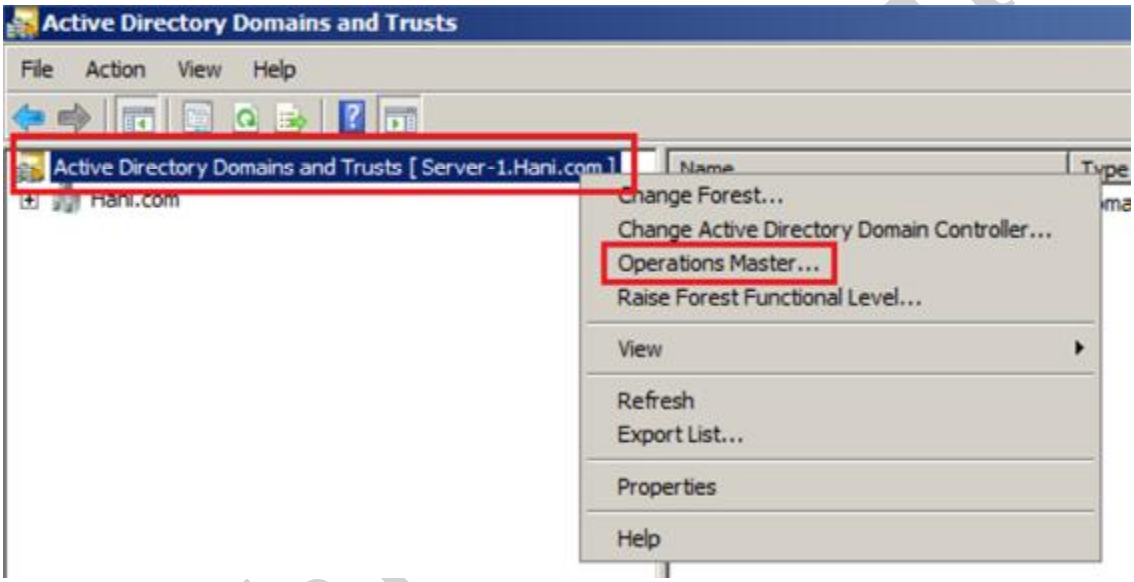
برای اینکه بفهیمOpration Masterدر کجا قرار دارد بر رویDomain Root مانند زیر عمل می کنیم

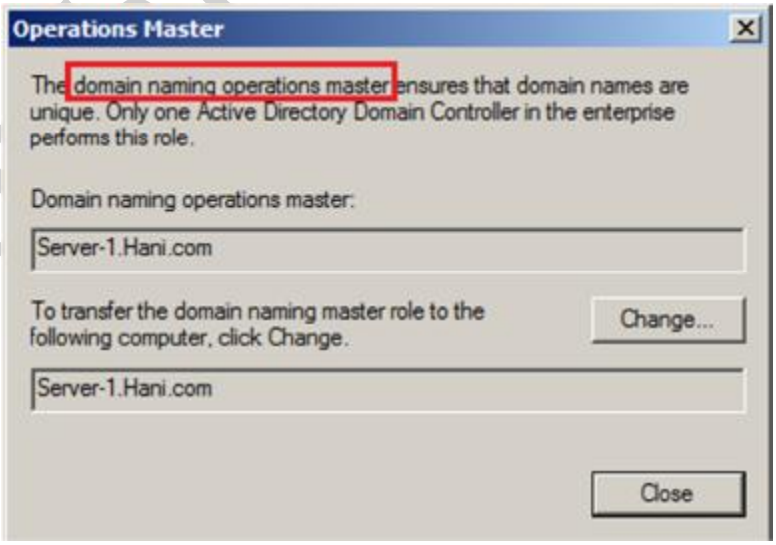



با زدن Change می توان این نقش را به سرور دیگری واگذار کرد,در اینجا نشان می دهد که سه نقش RID,PDC,Infrastructure را سرور 1 بر عهده دارد.

FarhidAjabnoush

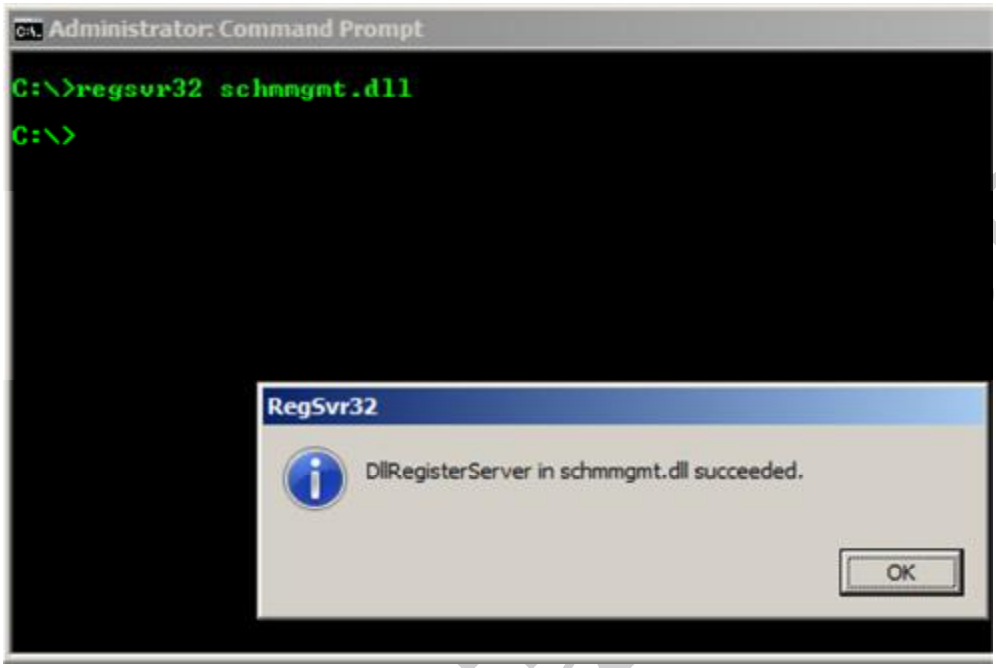

RID
PDC
Infrastructure
The operations master manages the allocation of RID pools to other Domain Controllers. Only one server in the domain performs this role.
Operations master:
Server-1.Hani.com
To transfer the operations master role to the following computer, click Change.
Change...
Server-1.Hani.com


Active Directory Domains and Trusts
File
Action
View
Help
Active Directory Domains and Trusts [ Server-1.Hani.com ]
Hani.com
Name
Type
Change Forest...
Change Active Directory Domain Controller...
Operations Master...
Raise Forest Functional Level...
View
Refresh
Export List...
Properties
Help

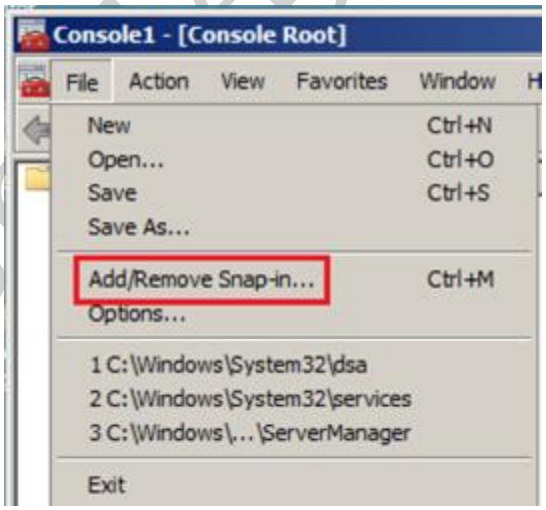

Operations Master
The domain naming operations master ensures that domain names are unique. Only one Active Directory Domain Controller in the enterprise performs this role.
Domain naming operations master:
Server-1.Hani.com
To transfer the domain naming master role to the following computer, click Change.
Change...
Server-1.Hani.com
Close

Farouk

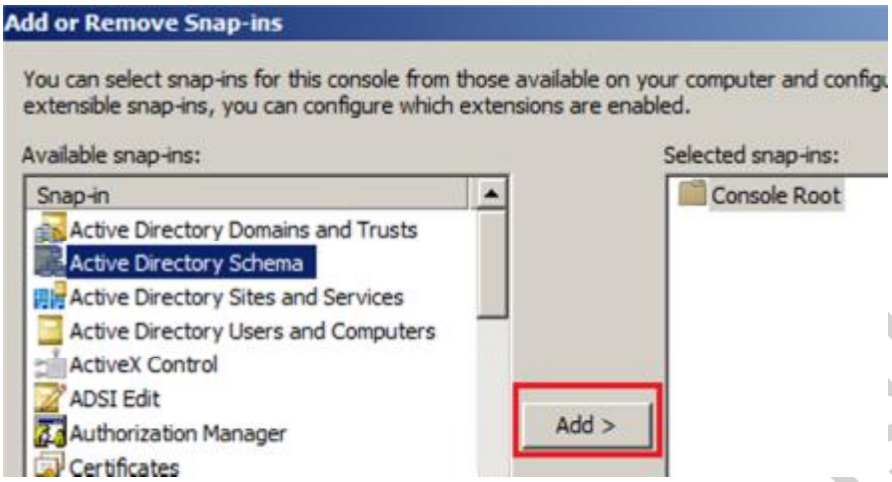
برای اینکه پارتیشن Schema را ببینیم ابتدا باید آن را به کنسول مایکروسافت اضافه کنیم قبل از اضافه کردن باید یک DLL را روی سرور از طریق دستور زیر Load کنیم.

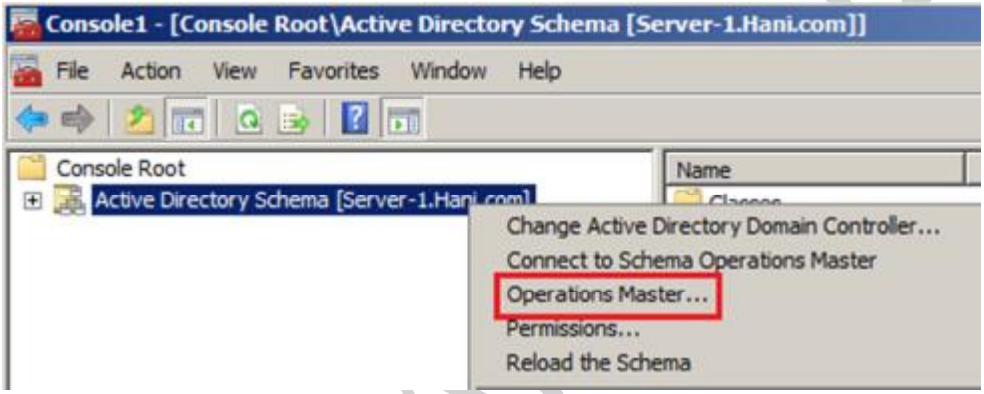



سپس وارد MMC می شویم و مانند زیر عمل می کنیم

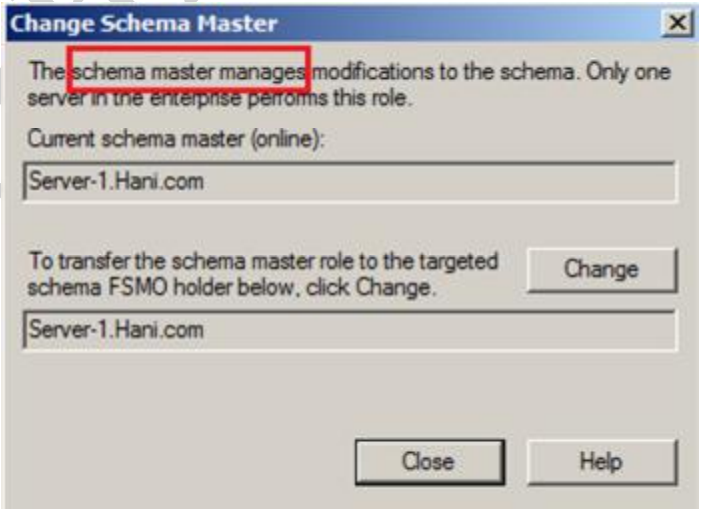



Farshad Ajami




**سپس به ما نشان می دهد که Schema دست کدام سرور می باشد**

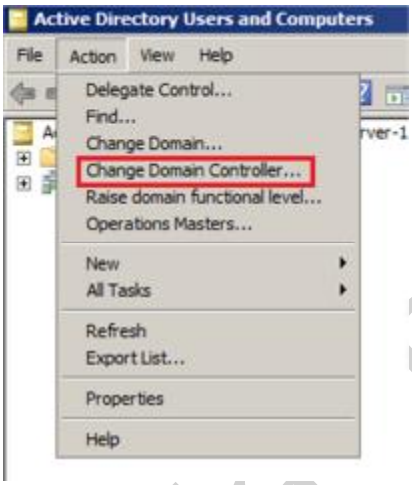



FarhidAyoush

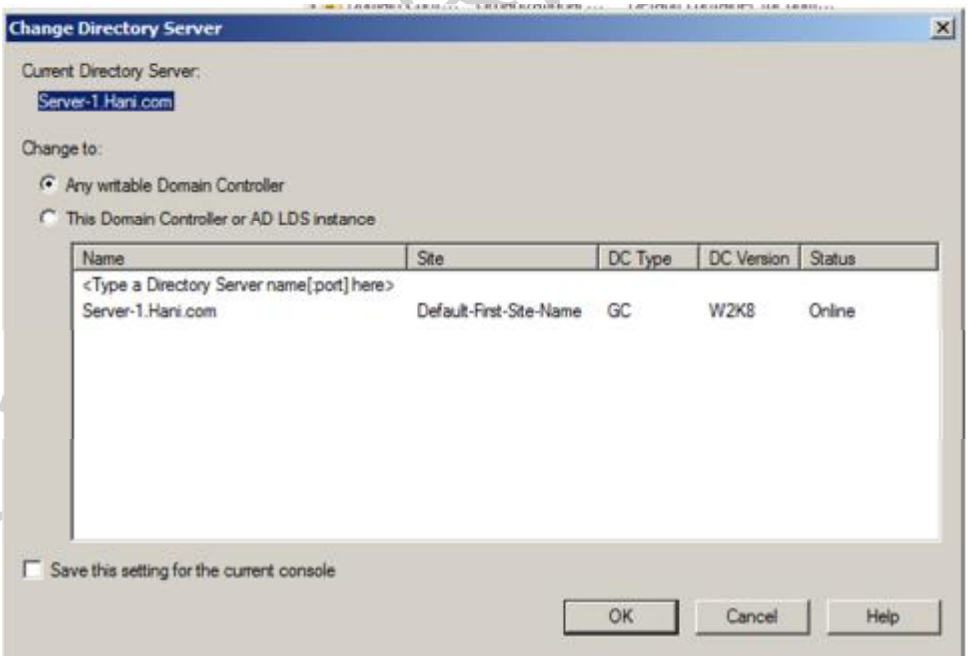
برای انتقال نقش ها (که در این سناریو پشت سرور 1 می باشد)به سرور2(گیرنده نقش ها), مانند زیر عمل می کنیم

- باید بر روی 2 سرور اکتیو نصب باشد مهم نیست که سرور Child 2 یا هر نقش دیگری داشته باشد

ابتدا انتخاب می کنیم که کدام نقش ها می خواهیم انتقال بدهیم(در اینجا وارد اکتیو دایرکتوری یوزر می شویم) سپس مانند زیر عمل می کنیم.




سپس در مرحله بعد دامین سرور 2 را انتخاب می کنیم(در اینجا وجود ندارد)

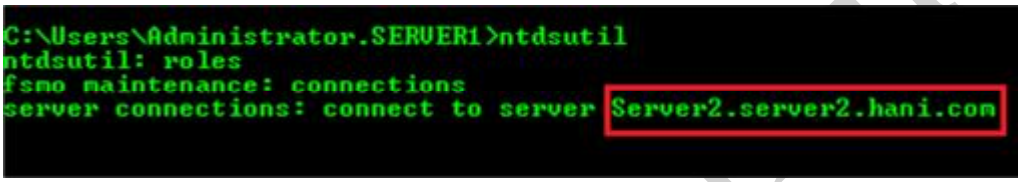



Eng. Aja noush

سپس از پشت سرور1 کنسول سرور2 برای ما باز می شود زمانی که کنسول سرور2 برای ما باز می شود همچنان سرور 1 نمایش داده می شود برای واگذار کردن نقش ها کافی است Change را بزنیم سپس نقش مورد نظر به سرور2 انتقال پیدا می کند.

پیاده سازی Seiz

Seiz زمانی استفاده می شود که سرور ما down شده باشد و باید از آن Backup داشته باشیم,باید آن Backup را داخل یک Vmware ,Loadکنیم سپس آن را ریستارت می کنیم وبا Directory Services Restore Mode (DSRM ) بالا می آوریم,سپس وقتی به صفحه لاگین رسیدیم باید Otheruser را بزنیم و با userAdmin و با پسورد Restore mode وارد می شویم ودر نهایت وارد cmd می شویم و مانند زیر عمل می کنیم




بعد از اجرای این دستور با تایپ quit یک مرحله به عقب بر می گردیم و با وارد کردن دستور seiz infrastructure یا هر دستور دیگری می توانیم نقش موردنظر را انتخاب کنیم.

- Seiz را فقط با Command می توان انجام داد.

Backup گرفتن از AD

Acronis-Norton) Image,NTDSutil,WindowsbackupAdmin,WindowsserverBackup,NTbackup

Symantec Backup Exec,ArcServ,(

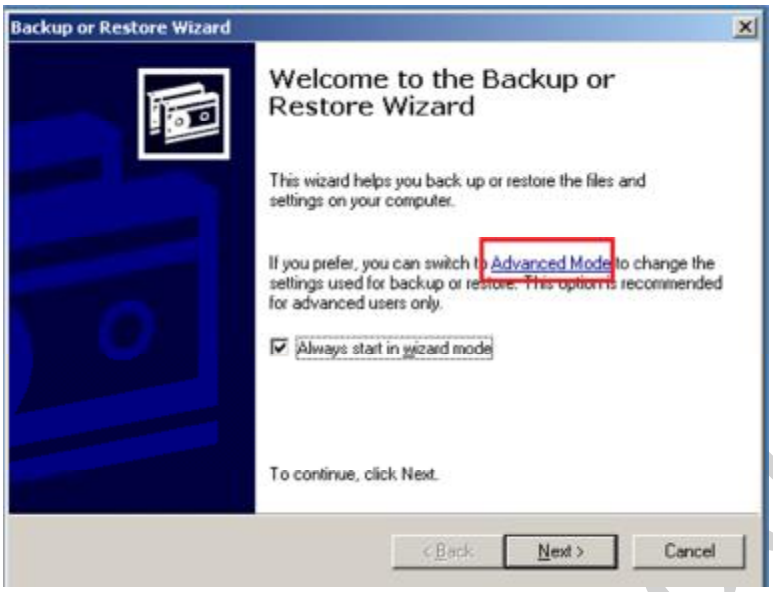
تمامی این روش ها از Backup,System Statedata می گیرد و System Stateddata شامل

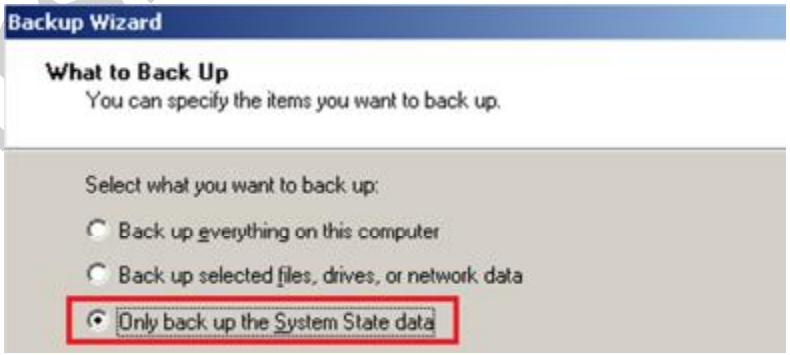
. NTDS.dit,Registery,systemfiles,bootfiles,certificates,sysvol

NTBACKUP

این روش قابل پیاده سازی برای AD 2003 می باشد,ابتدا در Run دستور ntbackup را وارد می کنیم سپس مانند زیر عمل می کنیم

FarshidAjabi.ir






سپس در آخر Finish می کنیم.

Farshad Nush

- بهتر است که Backup را در جایی بیرون از شبکه یا بر روی هارد دیگری نگهداری کنیم.
- تمامی روش های Backup به 5 صورت Backup می گیرند:

Normal,Copy,Incremental,Diffrential,Daily

- هر فایل یا فولدری که داخل سیستم می سازیمAttribute به نام Archive می سازد,اگر تغییری در آن فایل به وجود آوریم خود سیستم عامل گزینه Archive را تیک می زند.

Normal(Full)

در این روش بدون توجه به تیک ها,از تمام اطلاعات Backup می گیرد و آن فایل هایی که تیک دارند را تیکشان را بر می دارد,زمانی که برای اولین بار می خواهیم Backup بگیریم از این روش استفاده می کنیم.

Copy

در این روش بدون توجه به تیک ها,از تمام اطلاعات Backup می گیرد و تیک فایل ها را تغییر نمی دهد.

Incremental

این روش از فایل هایی Backup می گیرد که تیک آنها خورده باشد و بعد از Backup گرفتن تیک آنها را بر می دارد.

- در اینجا منظور از تیک,تیک گزینه Archive می باشد.

Diffrential

این روش از فایل هایی Backup می گیرد که تیک آنها خورده باشد و بعد از Backup گرفتن تیک آنها را برنمی دارد.

Daily

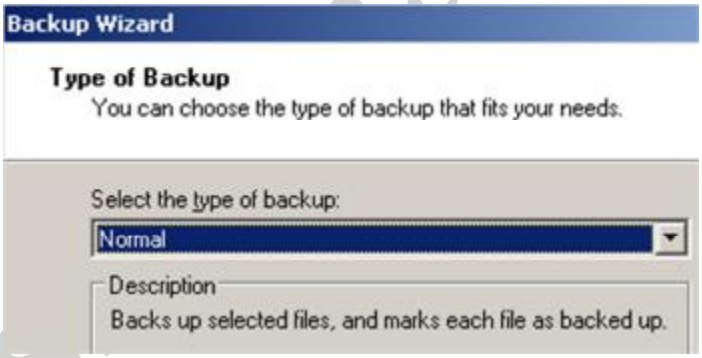
این روش توجه به تیک ندارد و نسبت به تغییرات روزانه Backup می گیرد(از روی تاریخ یعنی هرروز).

- توصیه: به دو طریق رایج می توان Backup گرفت 1- روز شنبه به صورت نرمال و بقیه روزها به صورت Incremental 2- - روز شنبه به صورت نرمال و بقیه روزها به صورت Diffrential(روش 2 بهتر است)

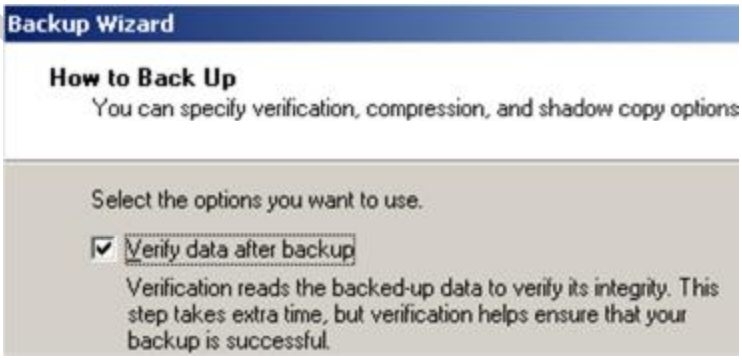
FarshidAjabroush

برای دسترسی به روش های بالا قبل از Finish کردن در آخرین مرحله ذکر شده در بالا مانند زیر عمل می کنیم

در اینجا می توانیم نوع Backup را مشخص می کنیم

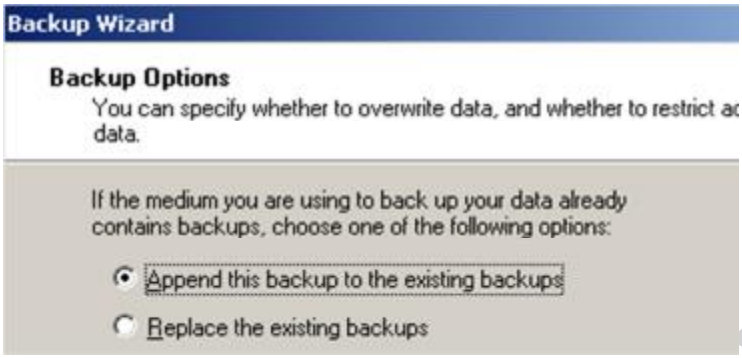



حتماً باید این گزینه فعال باشد تا پس از اتمامBackup،آن را چک کند.




Farsi Arabesh

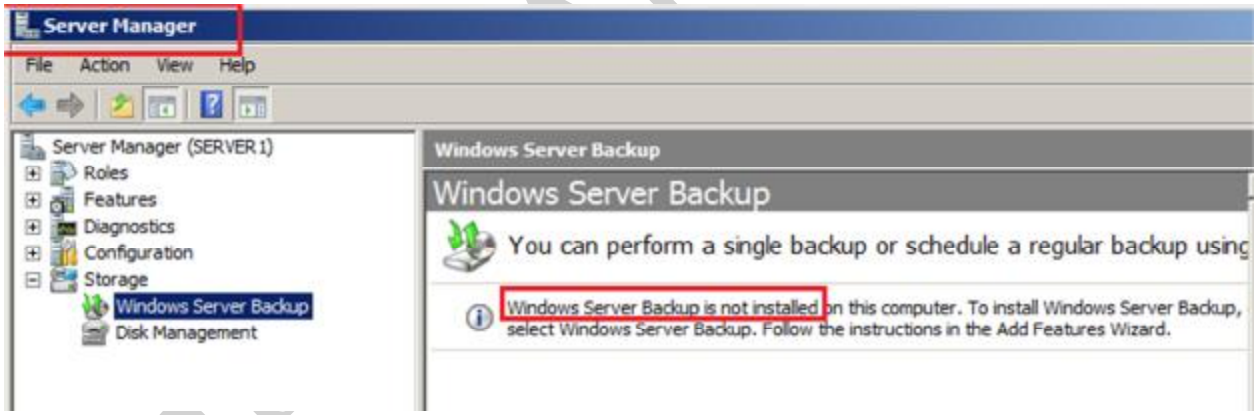
Append یعنی این Backup را به انتهای بقیه Backup ها اضافه کنیم،Replace یعنی این Backup را جایگزین کنیم.




- Backup های از نوع Diffrential را Replace می کنیم و Backup های از نوع Incremental راAppend می کنیم.

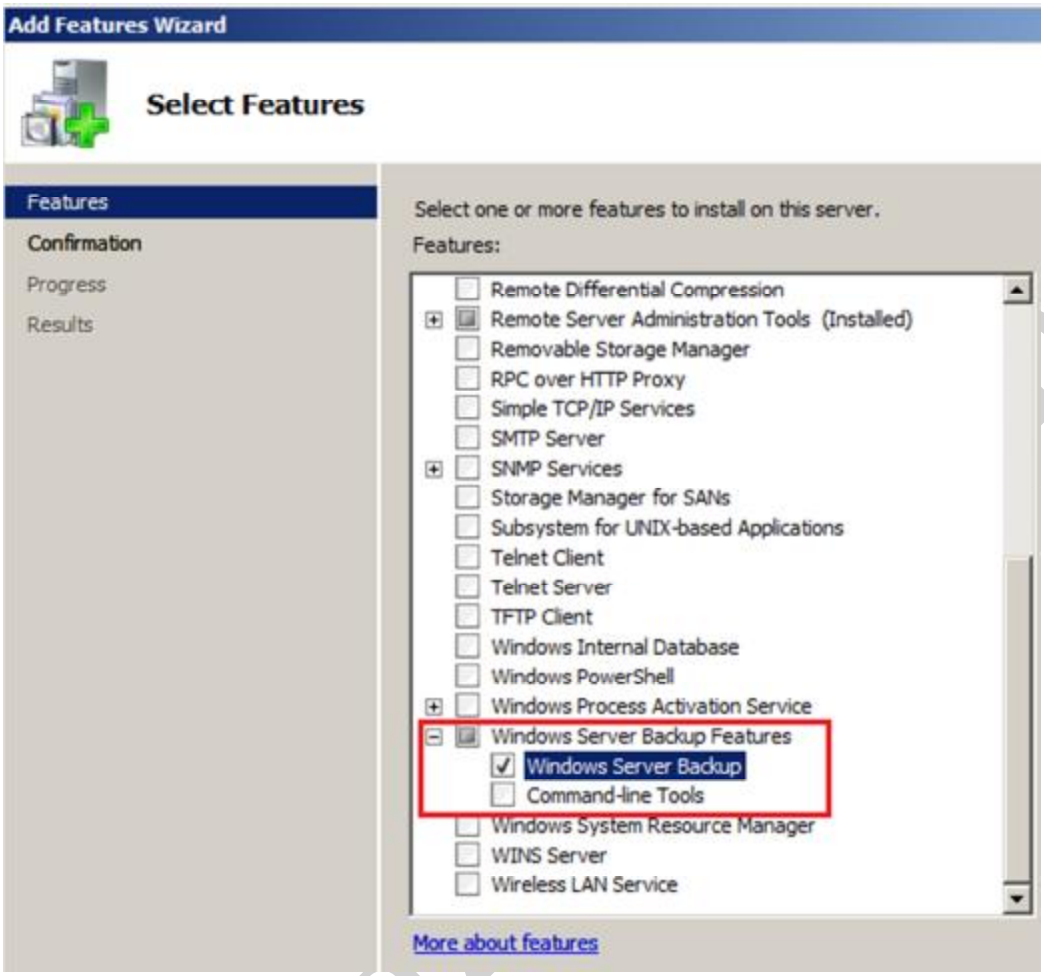
Windows Server Backup

این روش مخصوص Server2008 می باشد برای این کار مانند زیر عمل می کنیم




برای نصب وارد Features می شویم و مانند شکل زیر عمل می کنیم،گزینه Command line برای زمانی می باشد که بخواهیم توسط Command و یا Script ،Backup بگیریم

Fa Jabnoush

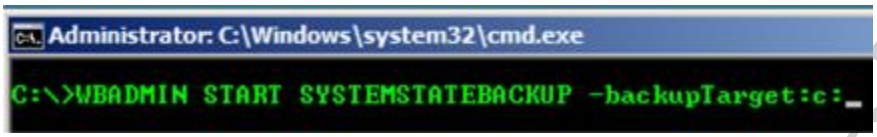



**بعد از نصب حتماً باید سرور را ریستارت کنیم.**

Farshid

Windows Backup Admin

این روش هم مخصوص 2008 می باشد و با نصب کنسول Windows Server Backup به سرور اضافه می شود،سپس با دستور زیر Backup را شروع می کنیم(در اینجا C محل ذخیره سازی Backup می باشد).

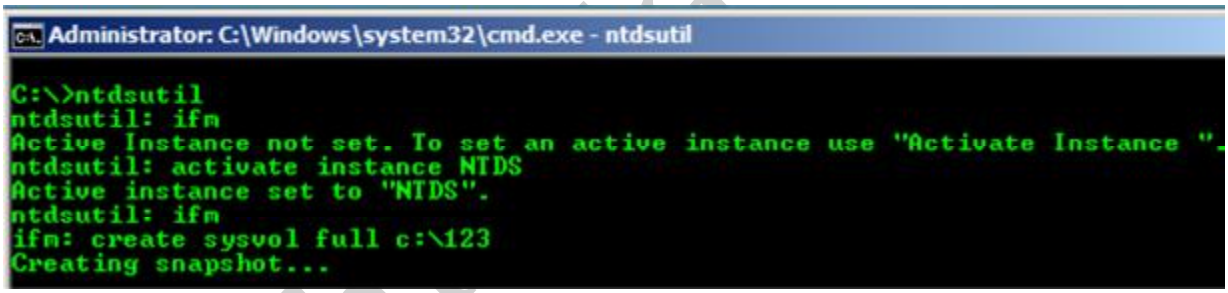



NTDSUTIL

این روش هم در 2003 و هم در2008 قابل پیاده سازی می باشد وپیاده سازی این روش با Command می باشد

- این روش می تواند به صورت Install From Media ،Backup بگیرد.
- این روش بهترین روش Command می باشد.

برای پیاده سازی مانند زیر عمل می کنیم




Ntdsutil ifm activate instance NTDS ifm create sysvol full d:\123

بعداز گرفتن Backup در پوشه 123 می توانیم آن را کپی کنیم داخل فلش و....

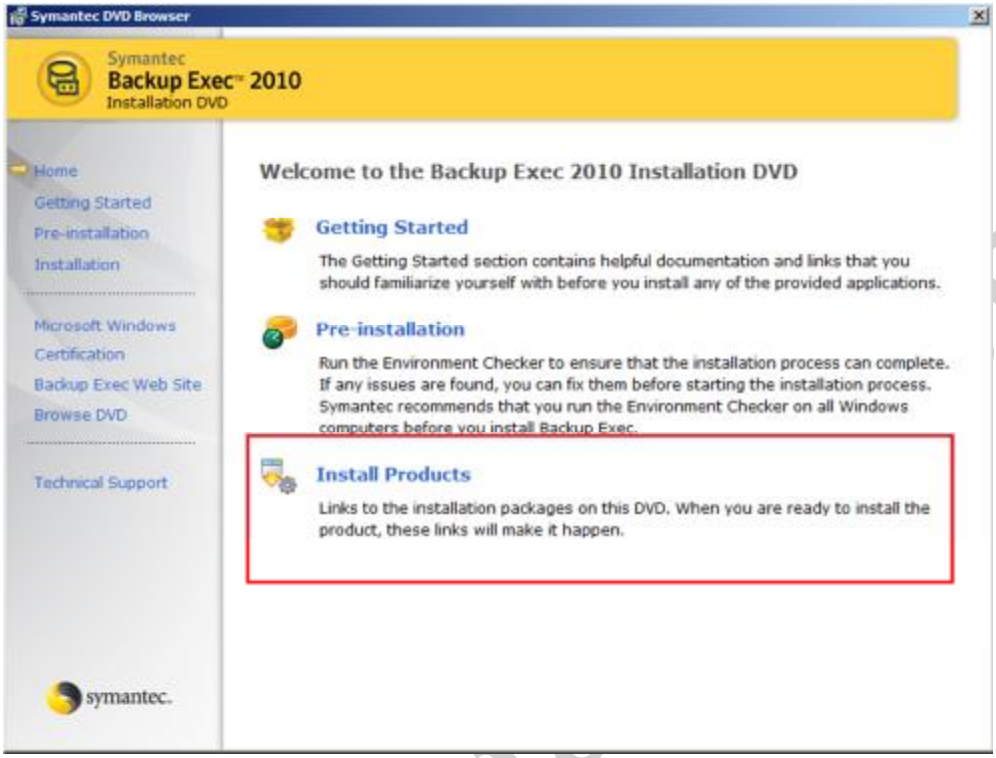
ARC Serve

این روش،یک نرم افزار مانند EXEC می باشد که قابلیت چندانی در مقابل EXEC ندارد.

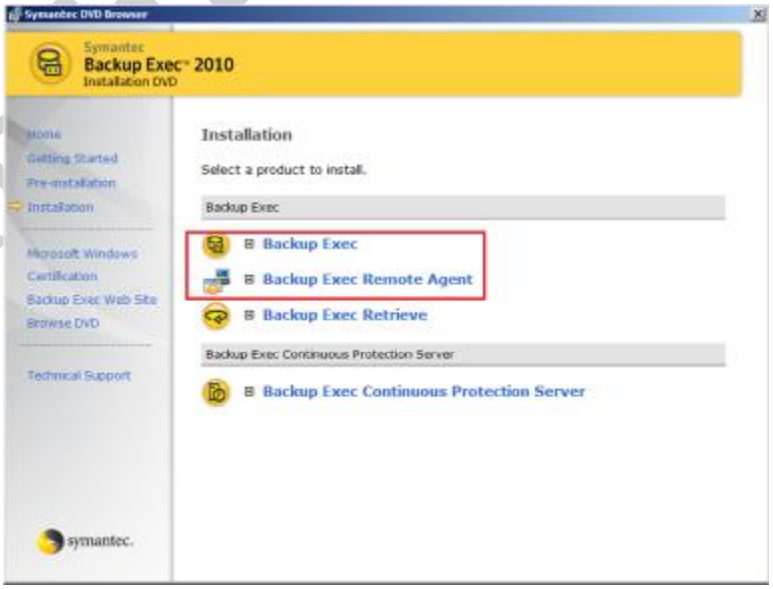
BACKUP EXEC

برای نصب این نرم افزار مانند زیر عمل می کنیم

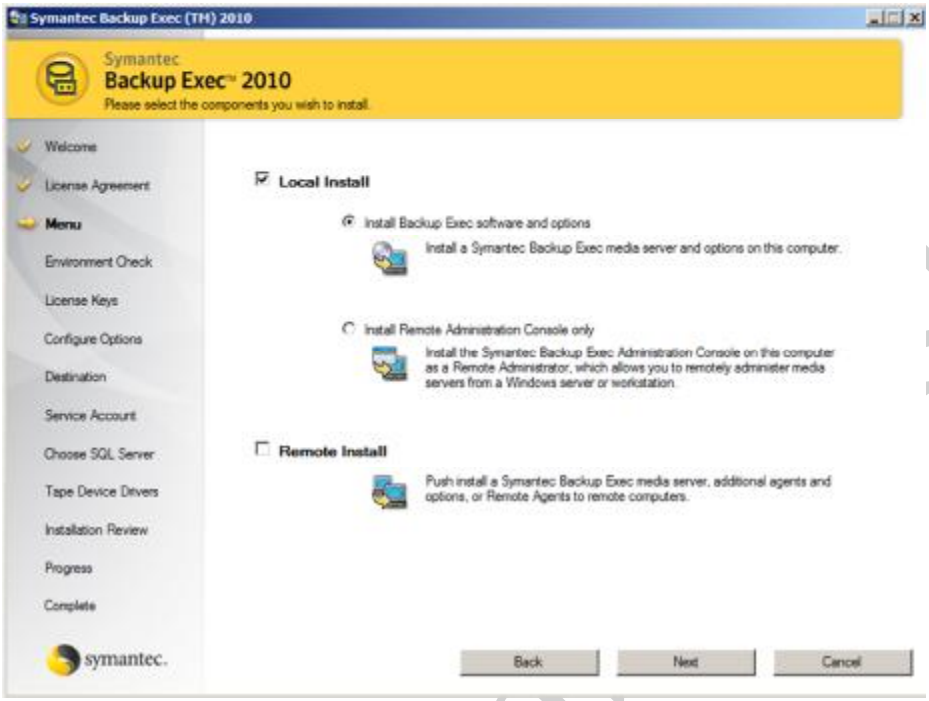
Farshad Abnoush

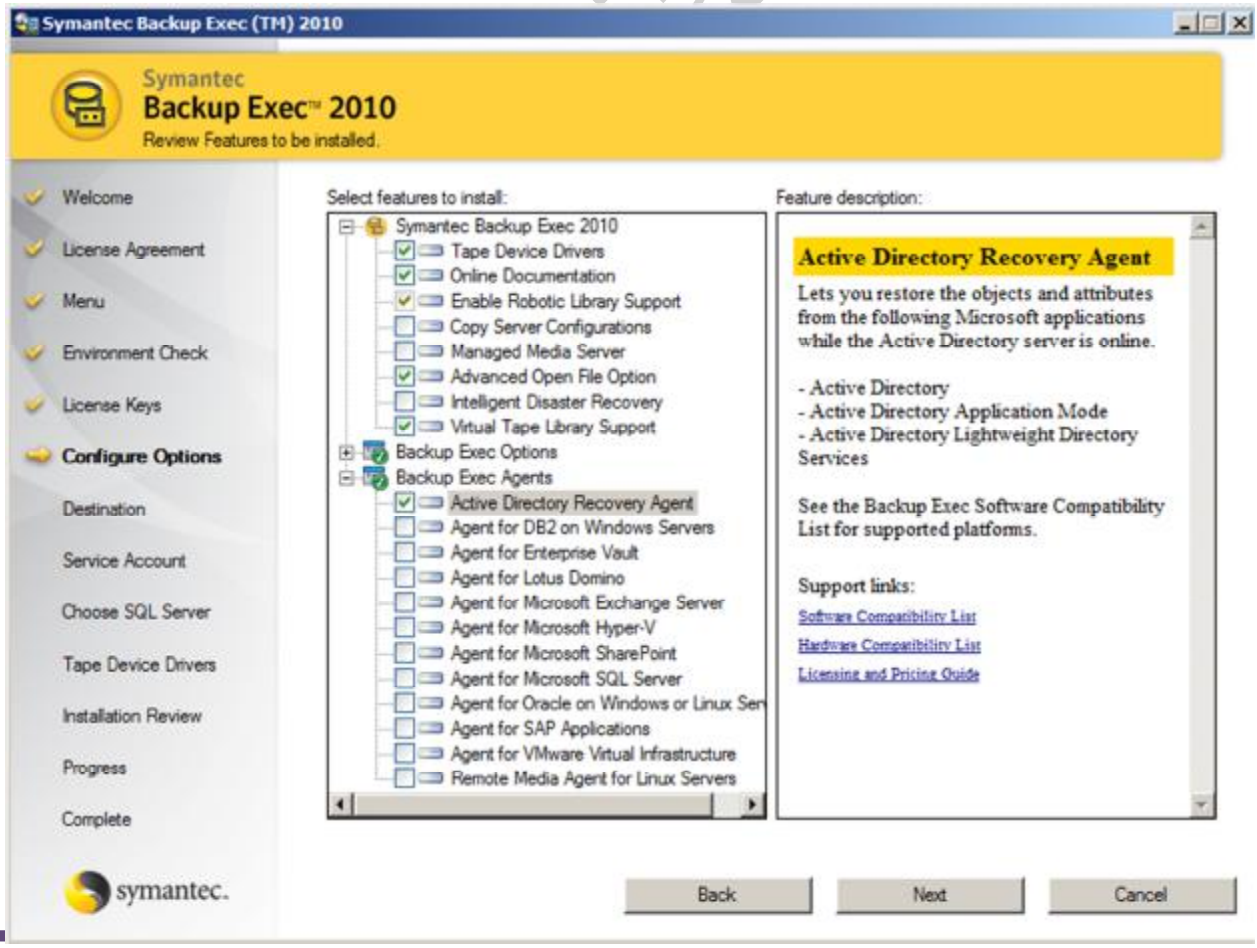



برای نصب نرم افزار بر روی سرور Backup گزینه اول و برای نصب نرم افزار بر روی کلاینت ها گزینه دوم (Agent) را نصب می کنیم که بتوانیم از کلاینت ها Backup بگیریم.

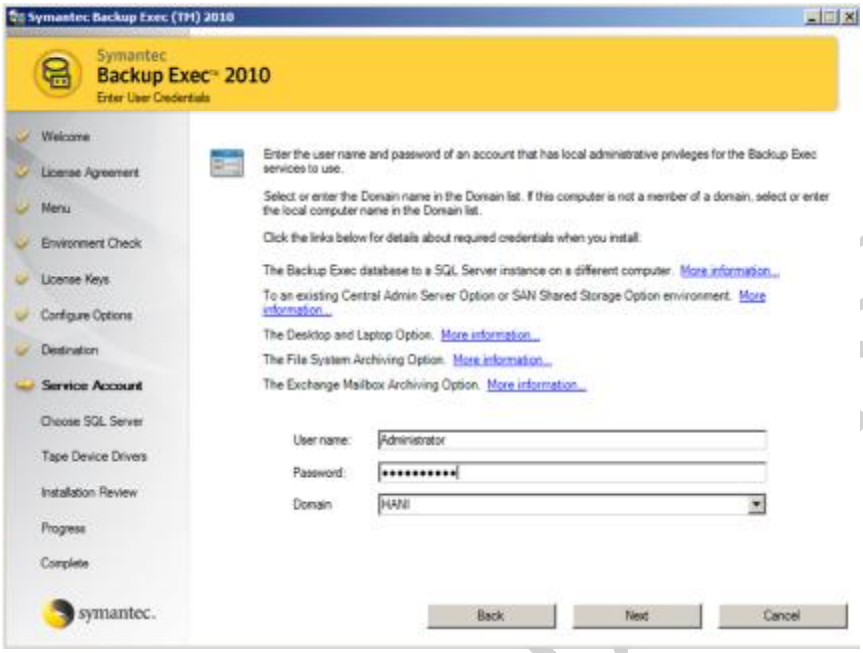


- Remote Install همان Agent می باشد.

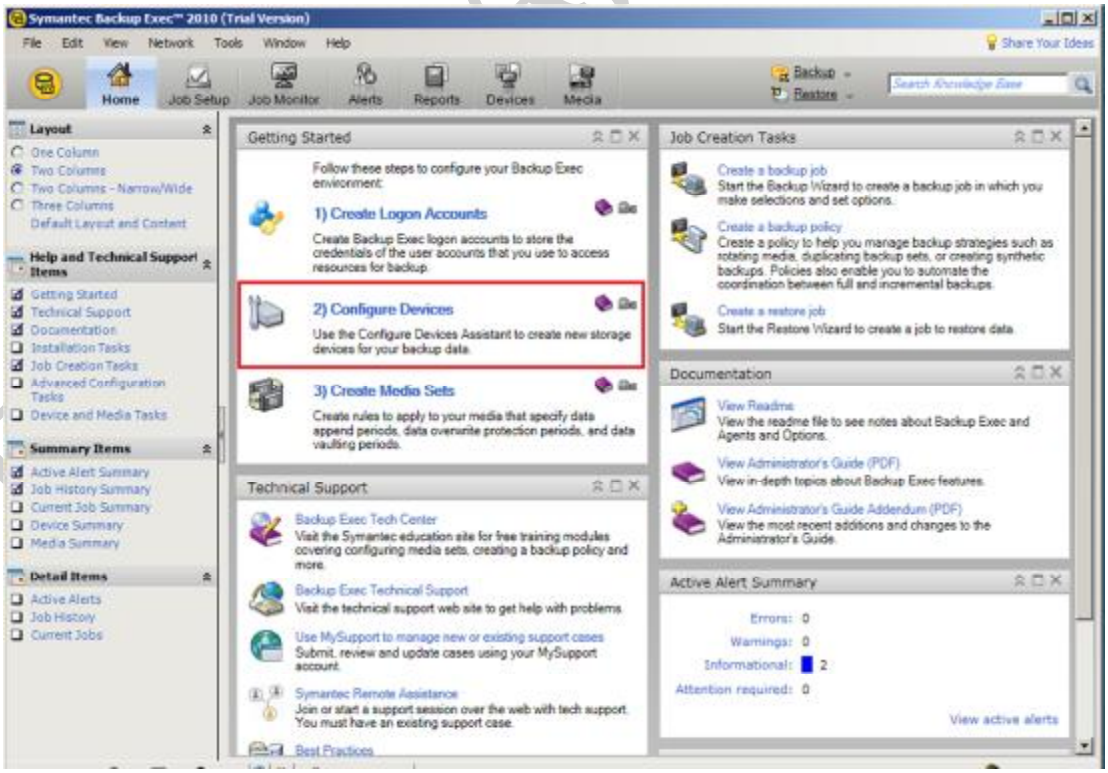


سپس یوزر و پسورد Admin را وارد می کنیم

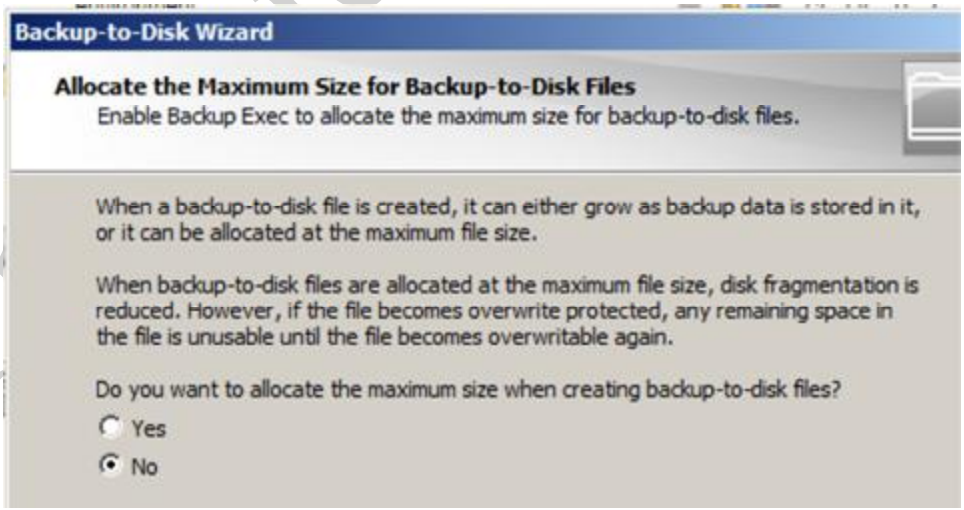



بعد از اتمام نصب اولین کار تعریف کردن محلی برای ذخیره سازی اطلاعات می باشد برای این کار مانند زیر عمل می کنیم



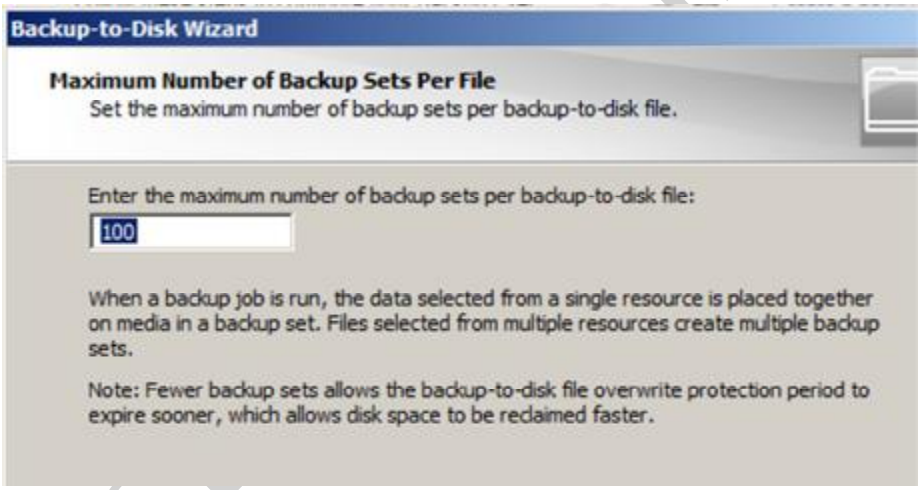
در این مرحله می توانیم مشخص کنیم که Backup را در کجا ذخیره کند،در این سناریو روی فولدری برروی هارد ذخیره می کنیم برای این کار گزینه زیر را انتخاب می کنیم.

در این مرحله می توانیم فضای خالی کل درایو را اختصاص دهیم(درایوی که پوشه در آنجا ساخته شده است)

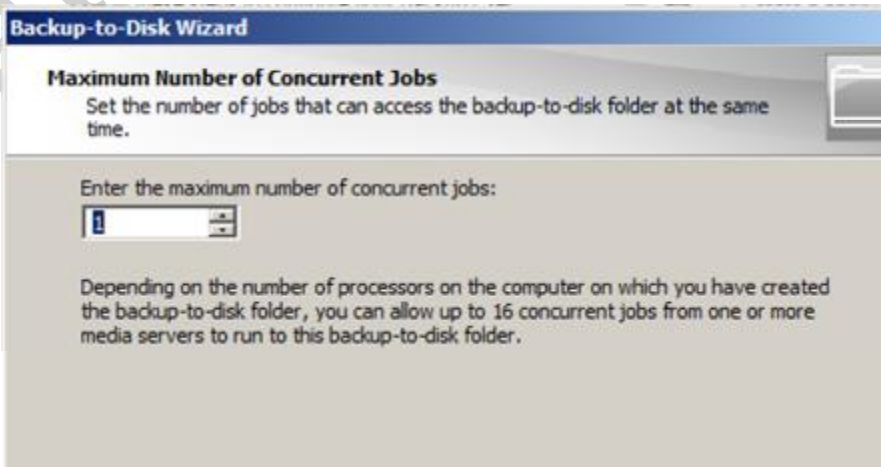


در اینجا مشخص می کنیم چه حجمی از کل درایو را به پوشه Backup اختصاص دهد.

مشخص می کنیم چندJobBackup ( کامپیوترهای مورد نظر)بتوانند اطلاعاتشان را در پوشه مورد نظر ذخیره کنند.

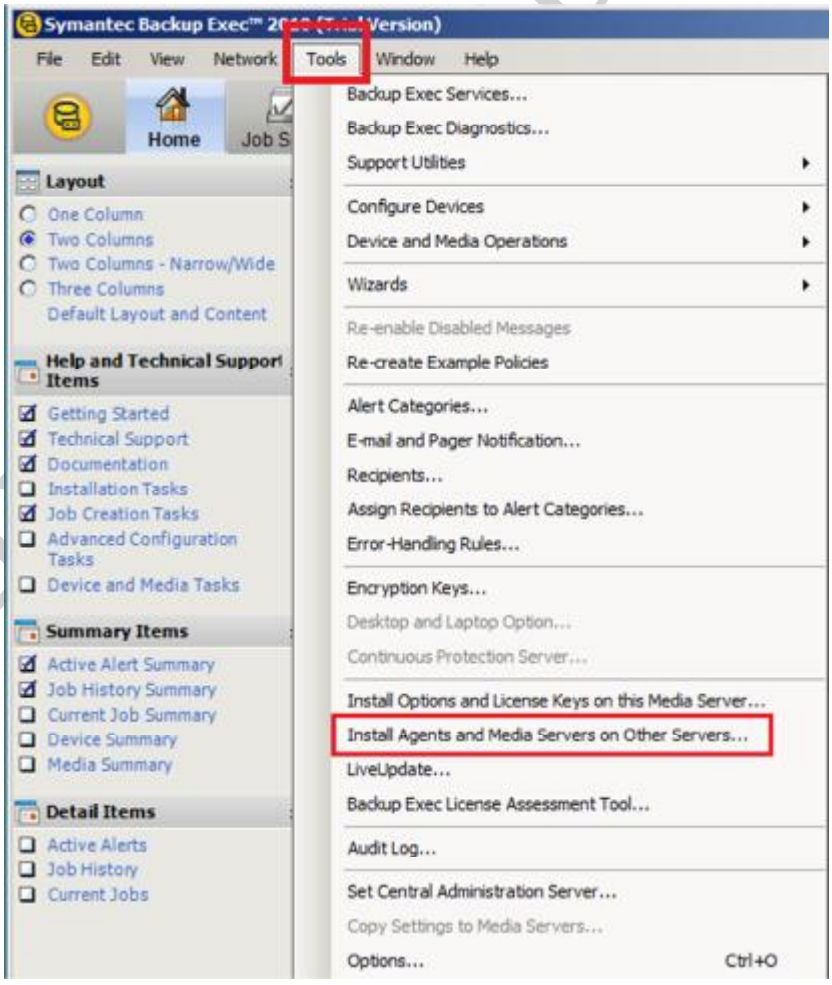



مشخص می کنیم همزمان چند سیستم می توانند اطلاعاتشان را وارد سیستم کنند

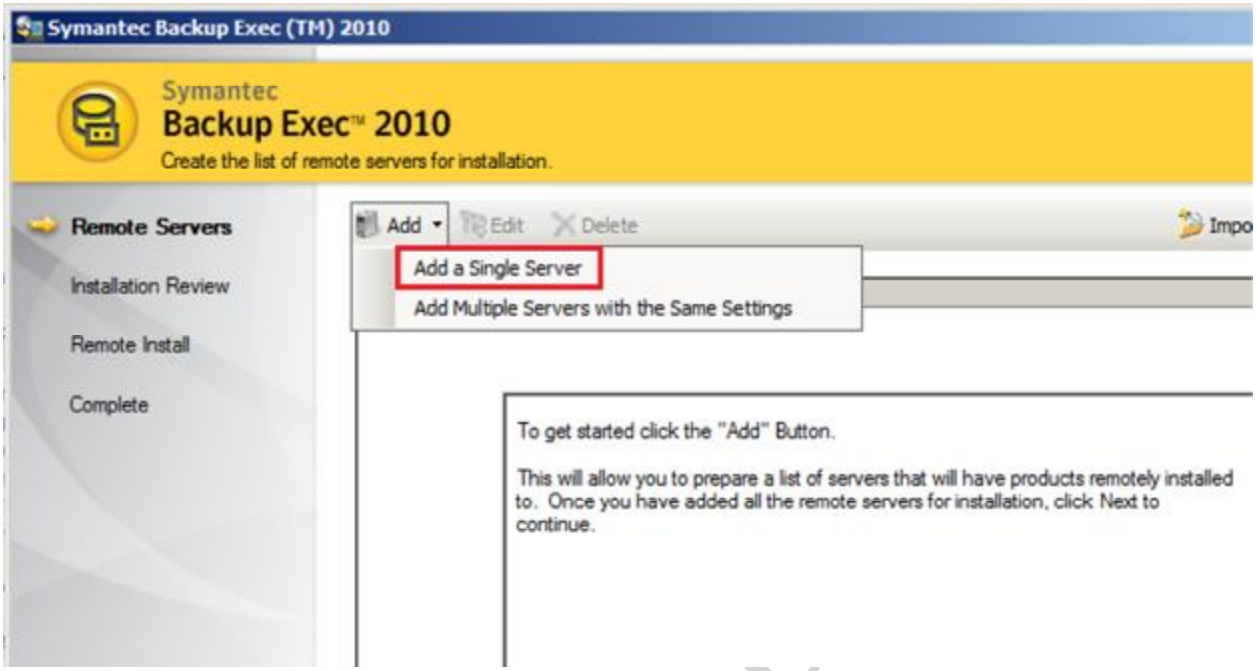


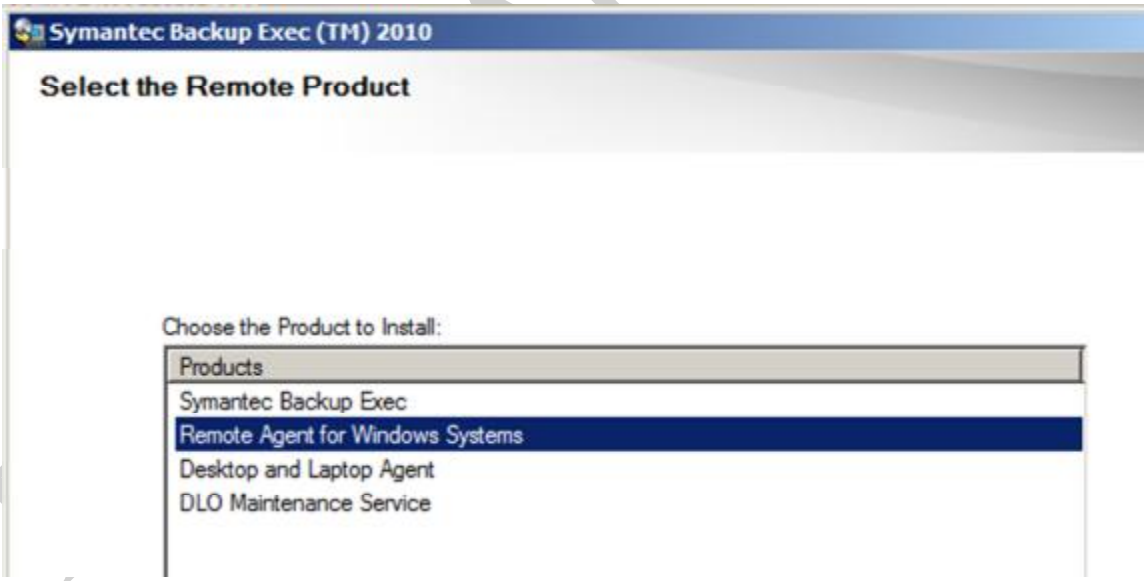
در اینجا می توانیم تعیین کنیم که زمانی که حجم پوشه در حال پرشدن بود به ما اطلاع دهد(4GB )،می توانیم یک حجم تعیین کنیم که به آن حجم رسید شروع به اطلاع دادن کند.

زمانی که بخواهیم از یک سرور دیگر Backup بگیریم باید Agent EXEC را بر روی آن نصب کنیم برای این کار مانند زیر عمل می کنیم

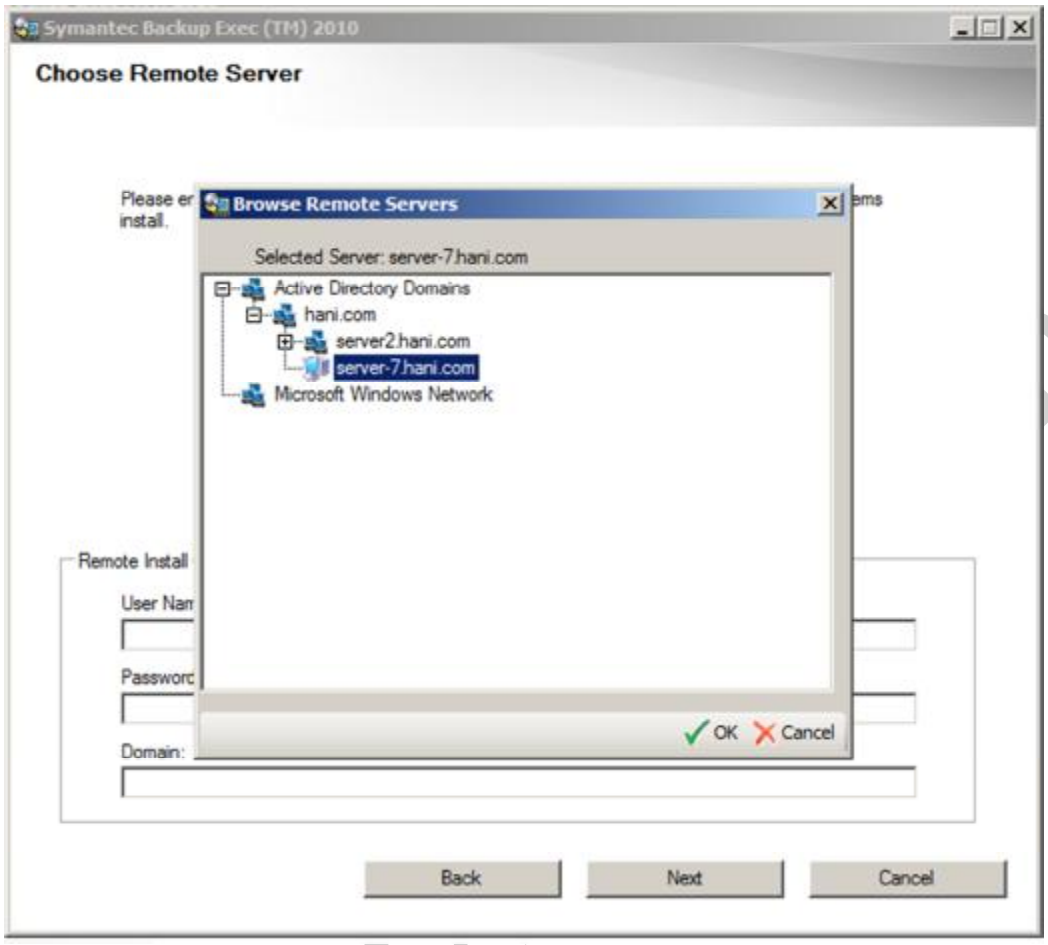


سپس باید مشخص کنیم همزمان از چند سرور می خواهیم Backup بگیریم (در این سناریو از یک سرور)



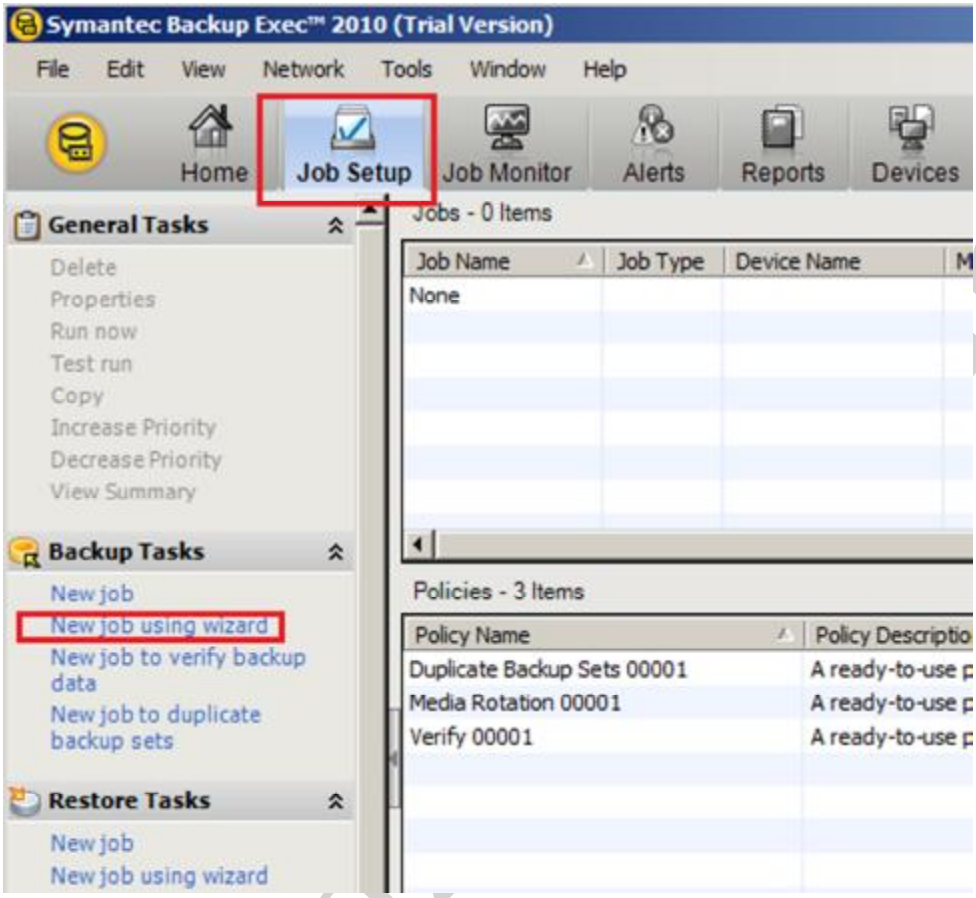



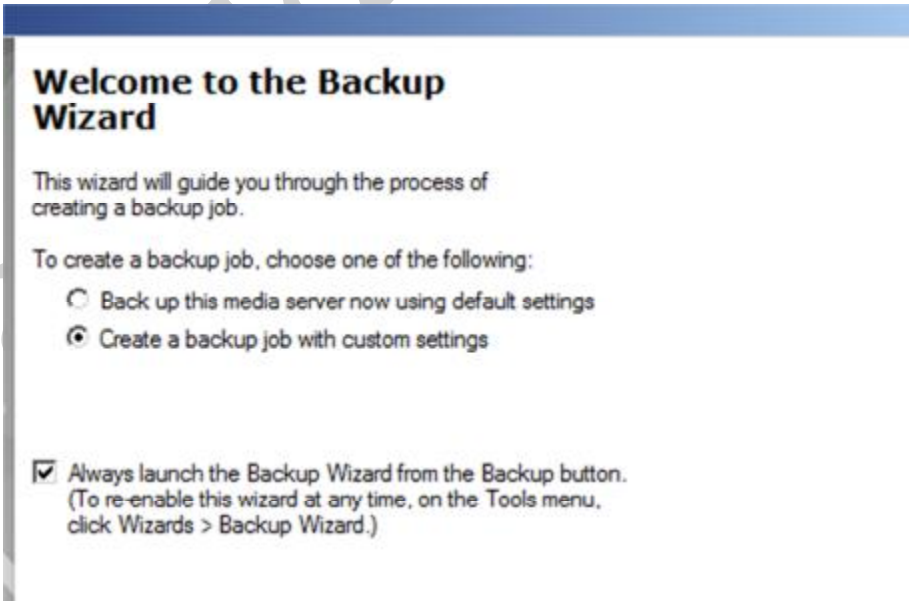

سپس باید سرور مورد نظر را انتخاب کنیم و یوزر و پسورد را وارد می کنیم



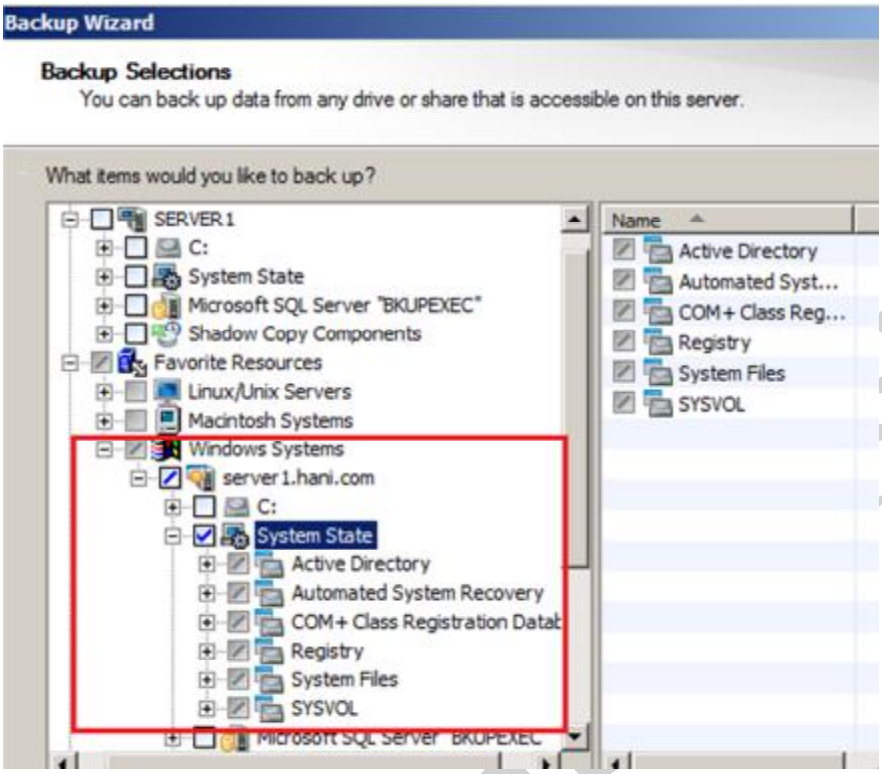
راه دیگر نصب Agent ،نصب مستقیم بر روی سرورموردنظر از طریق CD می باشد( Backup EXEC Remote Agent)

بعداز نصب وارد JobSetup می شویم(برروی سرور اصلی -سرور1)

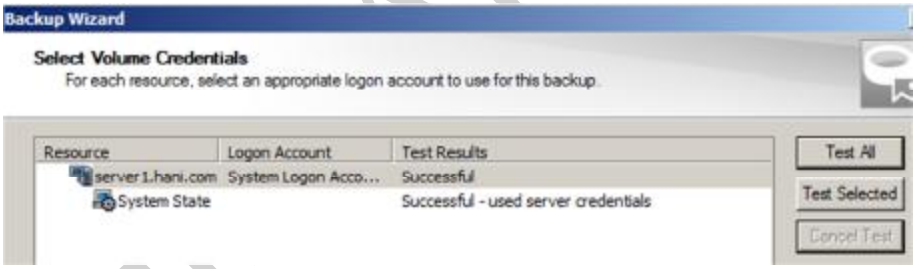


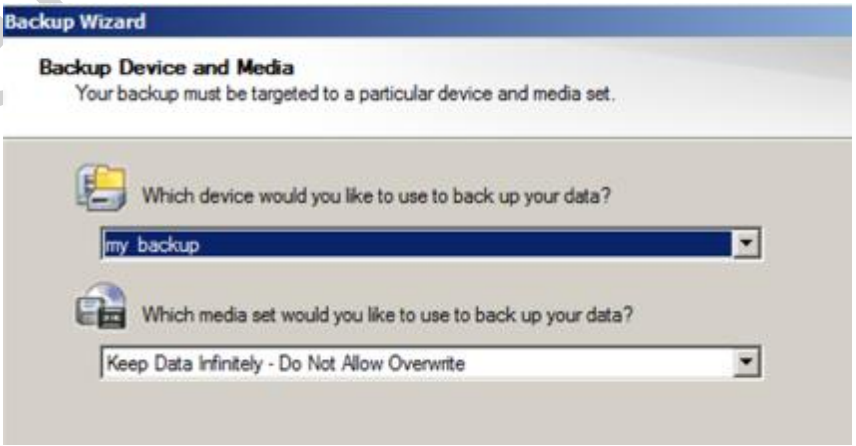

در مرحله بعد ازAD سرور1 Backup می گیریم.

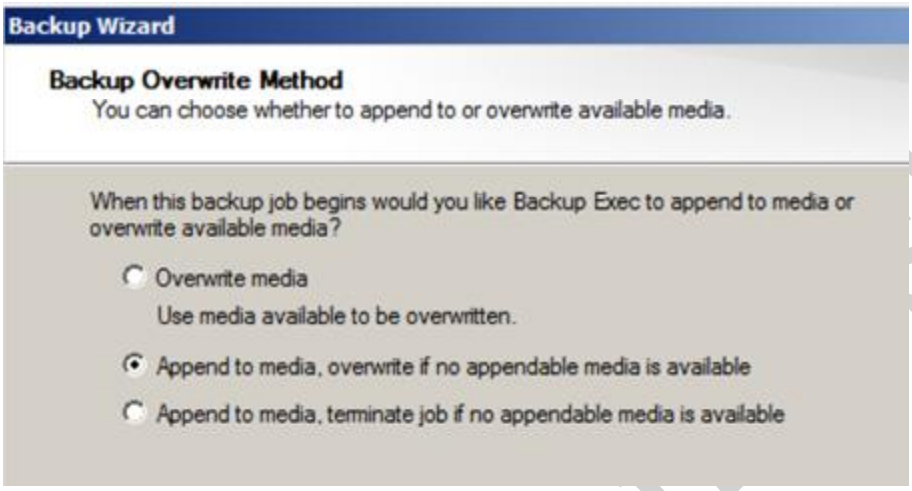



در اینجا Testall را برای تست صحیح Backup گرفتن فعال می کنیم.

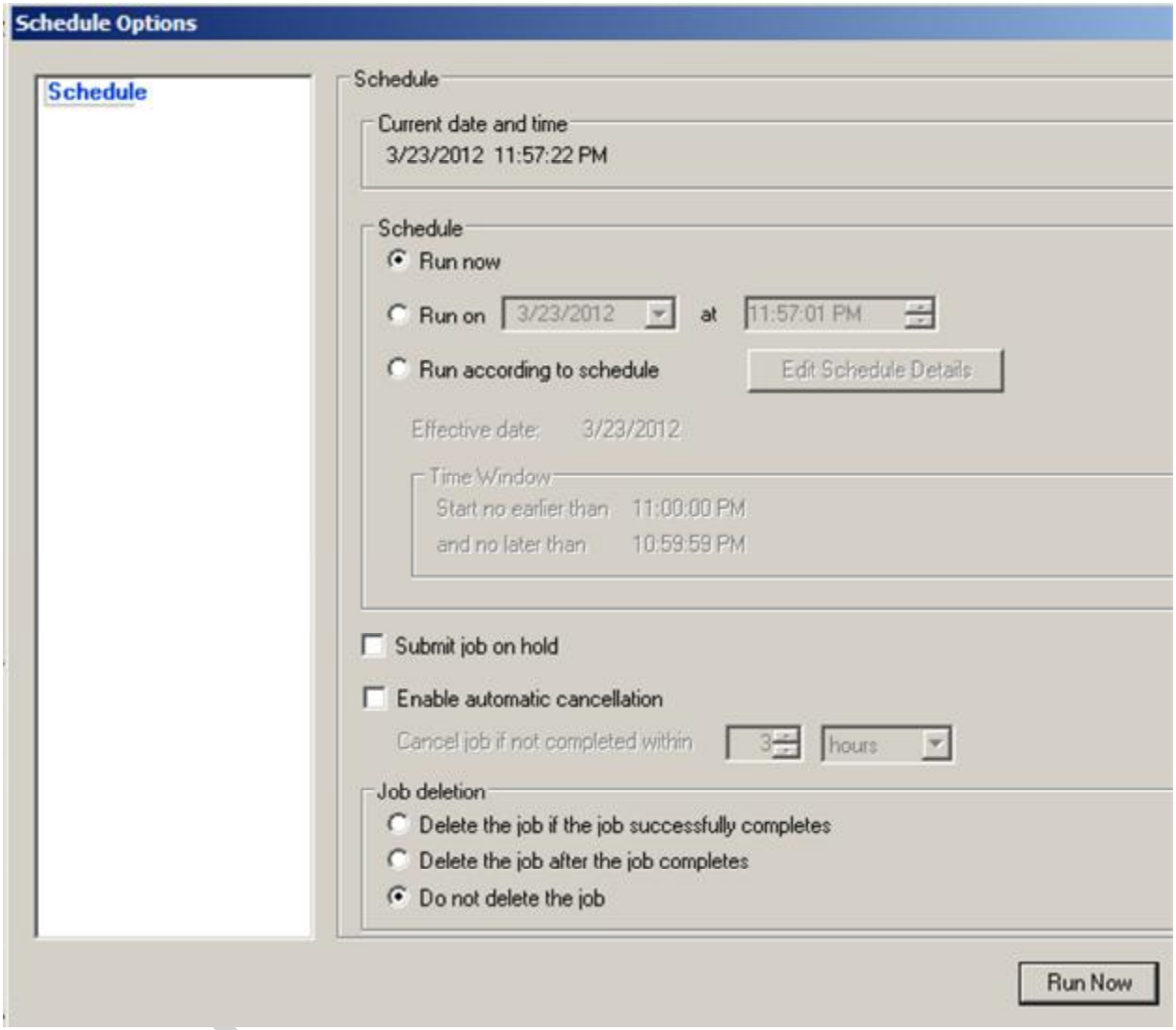



محل ذخیره سازی را مشخص می کنیم






در این مرحله می توانیم برای Backup گرفتن آن را زمان بندی کنیم




و در آخر هم برای دیدن وضعیت پشتیبان گیری وارد Job Monitor می شویم.

- یکی دیگر از روش های گرفتن Backup ، Quest می باشد .

## نحوه Restore کردن ActiveDirectory

به 2 روش انجام می گیرد: 1- Authoritative Restore  2- None Authoritative Restore

None Authoritative Restore

در این روش کل سرور اصلی از بین رفته است (کل AD)و با گذاشتن یک سرور جدید Backup که از سرور داشتیم را بر روی سرور جدید بر می گردانیم با همان Computer Name و همان Domain NAME .

- نرم افزارAcronis به روش None Authoritative کار می کند.

Authoritative Restore

در این روش یک Object از AD به صورت اتفاقی پاک شده است(مانند یک User)و با استفاده از این روش می توانیم آن Objectرا بازگردانی کنیم،در این روش ابتدا باید Backup را به صورت  None Authoritative ،Restoreکنیم و سپس آن را به Authoritative تبدیل کنیم.

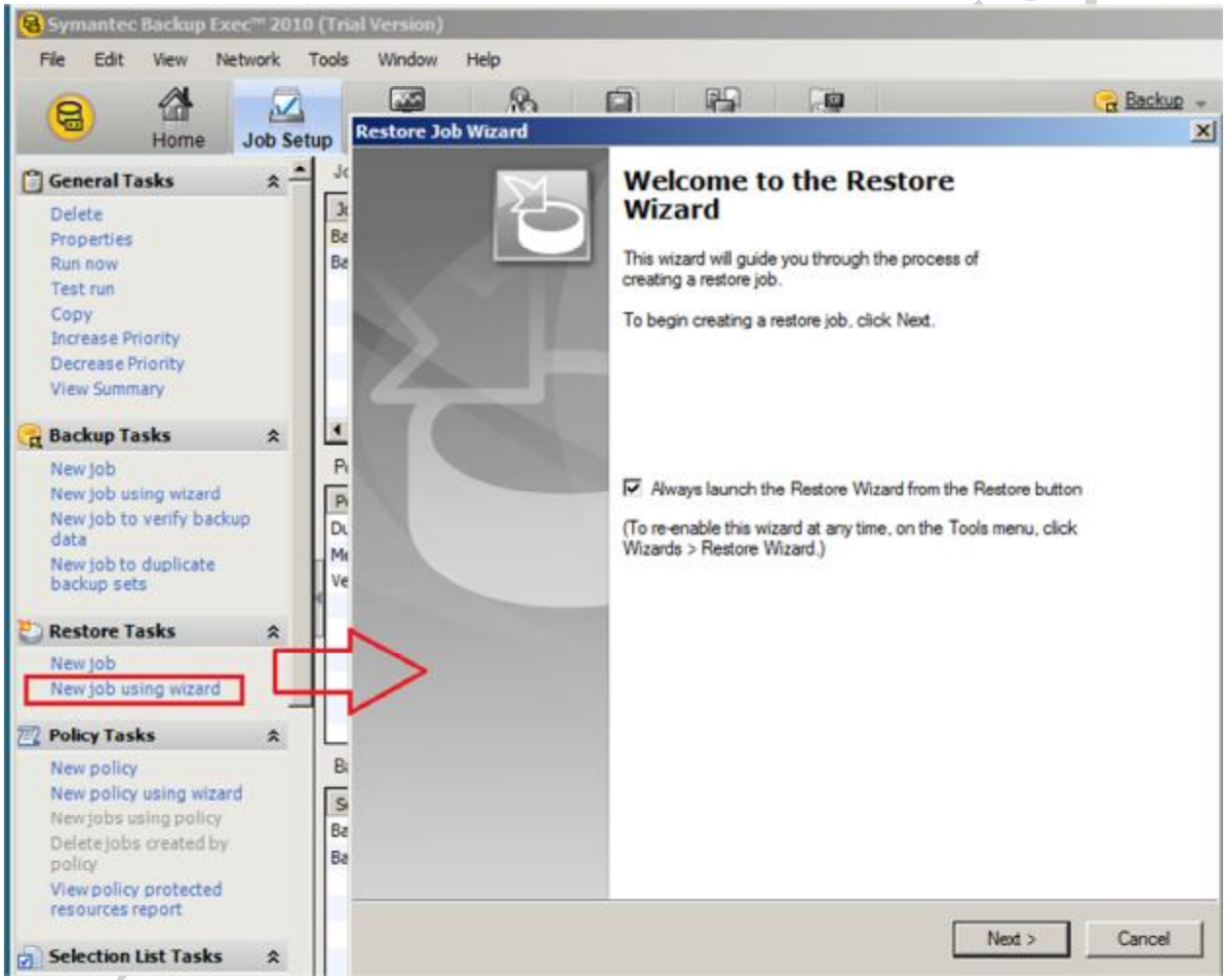
- زمانی که می خواهیم Restore کنیم باید با Directory Services Restore Mode سرور را راه اندازی کنیم.

این روش را با یک مثال توضیح می دهیم در یک شبکه دوسرور،یکی BDC و یکی PDC داریم،یکی از یوزرهایی را که در سرور PDC داشتیم به صورت اتفاقی پاک می شود و از روی BDCهم پاک می شود اگر Restoreکنیم دوباره پاک خواهد شدبرای اینکه این اتفاق رخ ندهد بایدورژن BDC را بالا ببریم برای این کار باید سرور(BDC) Unplug باشد تا از روی PDC خودش را به روز نکند که Restore را پاک کند،بعداز Restoreکردن که با  Directory ServicesRestore Mode سرور را راه اندازی کرده ایم وارد ntdsutil می شویم سپس دستور  Authoritative restore ، restore subtree ou=ou1 dc=hani dc=com اجرا می کنیم با اجرای این دستور ورژن OU را به روز کرده ایم.

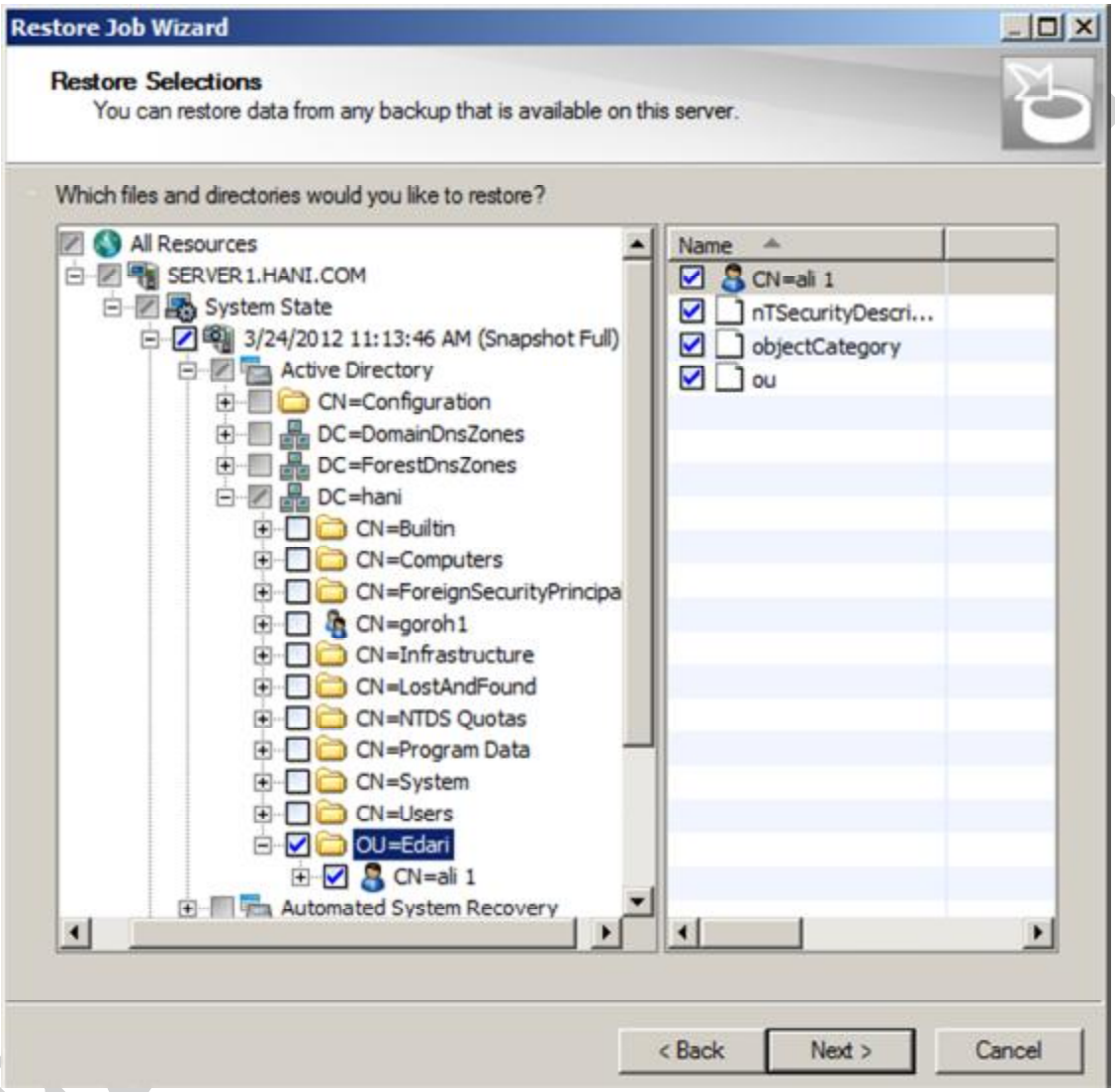
FarshidAjabnoush

بهترین روش ها برای Restore کردن

1- استفاده از EXEC : برای این کار مانند زیر عمل می کنیم

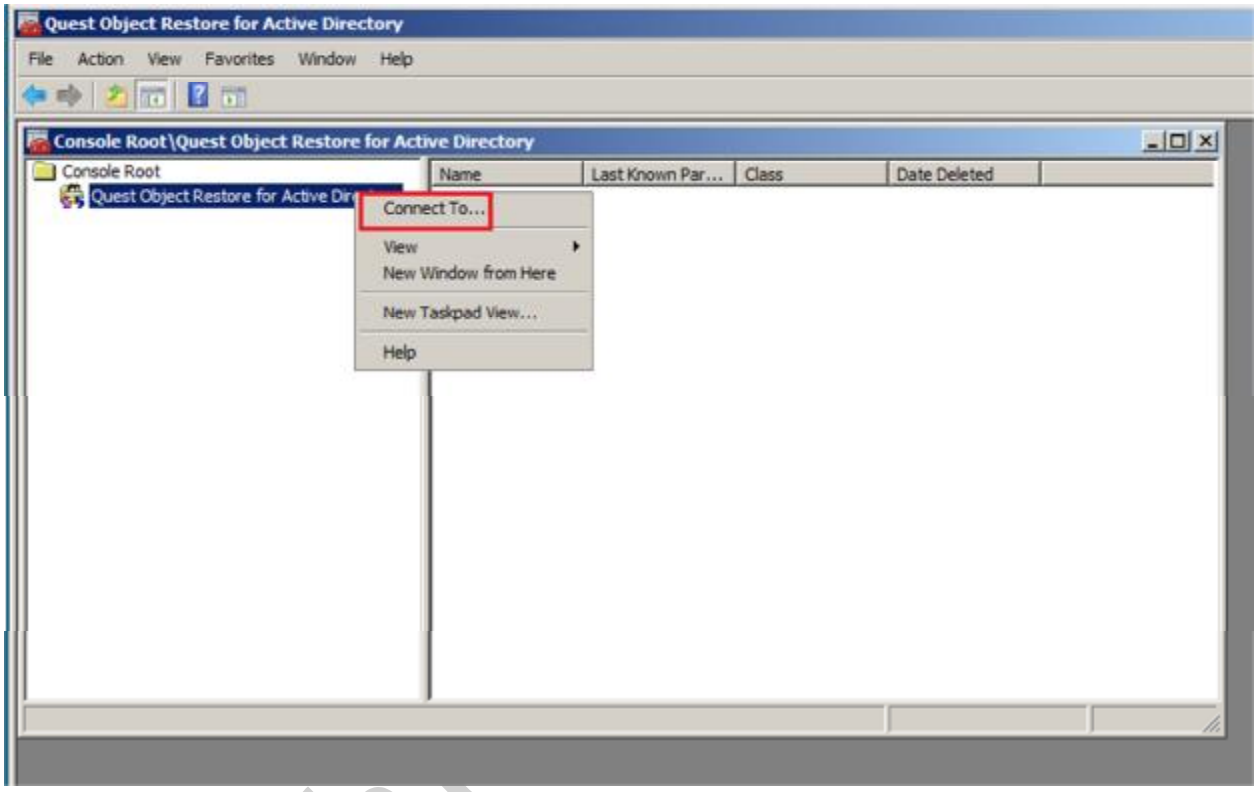



در مرحله بعد می توانیم Object مورد نظر را برگردانیم ( در اینجا OU edari می باشد)

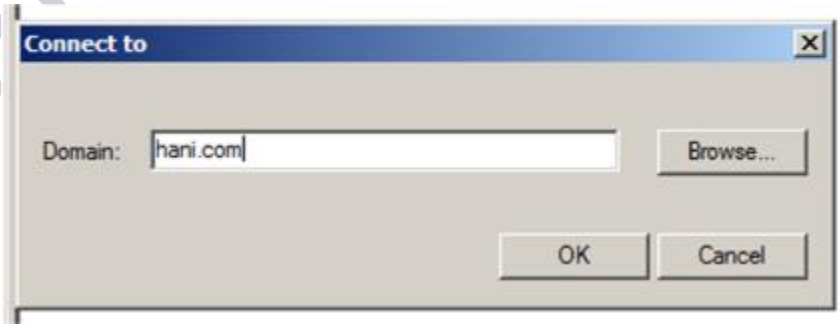



سپس Objectمورد نظر Restore (edari) می شود.

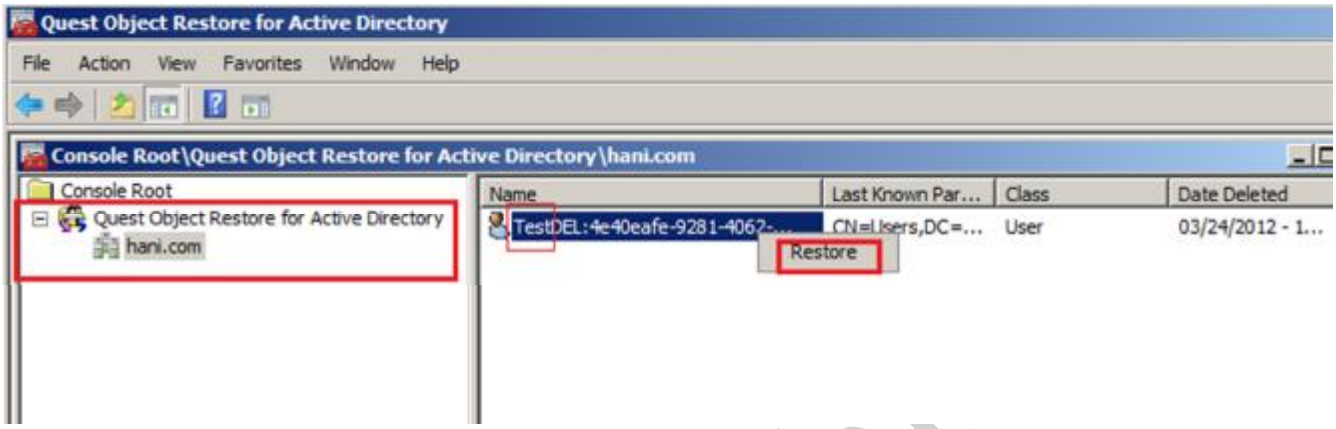
2- روش دوم برای زمانی است که Backup از ADنداریم ویک Object از AD پاک شده است و می خواهیم آن را ریکاوری می کنیم برای این کار باید بر روی سرور نرم افزارObjectRestoreforActiveDirectory نصب کنیم سپس مانند زیر یوزر Test را Restore می کنیم




در اینجا باید اسم سرور و یا دامین موردنظر را وارد کنیم



و سپس Object مورد نظر را Restore می کنیم




- این نرم افزار متعلق به شرکت Quest می باشد.
- بعد از Restore کردن یوزر،یوزر Disable می باشد که باید آن را Enableکنیم.
- این نرم افزار باید از روی سرور هر 6 ماه یکبار Remove و دوباره Install شود(Reinstall).
- نرم افزاری دیگری( Recovery Manager For Active Directory) از همین شرکت وجود دارد که توسط آن می توان کل دیتا بیس AD را Restoreکرد.
- این نرم افزار(ObjectRestoreforActiveDirectory) فقط Objectهای AD را Restore می کند.

FarshidAjabi