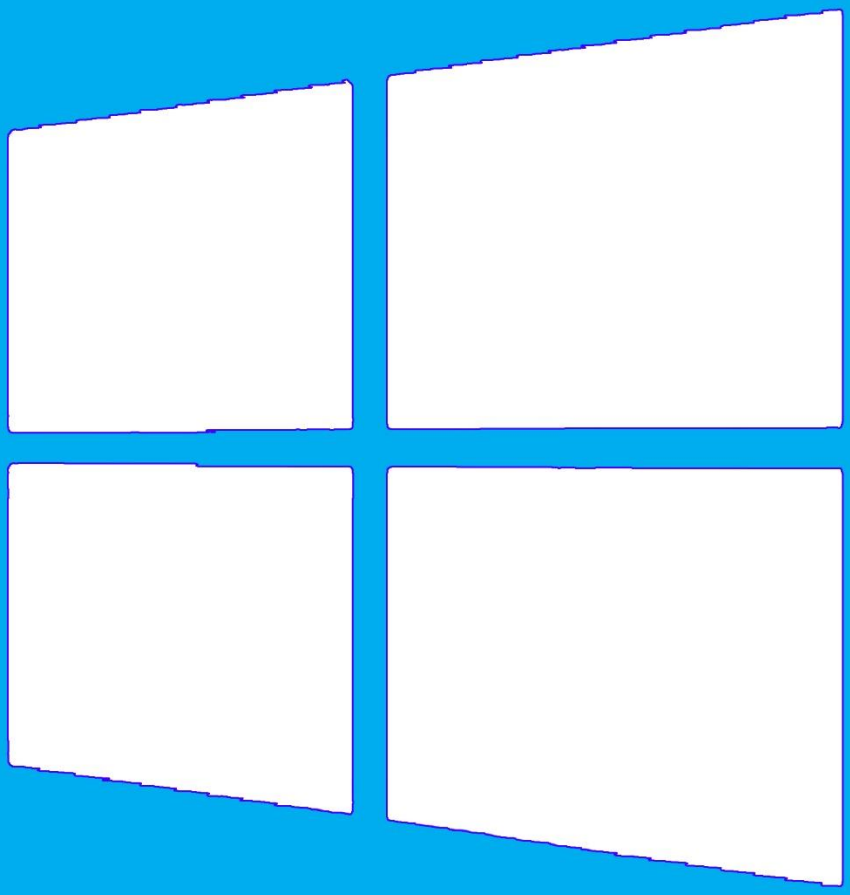
کتاب آموزشی

MCSE 2012

نویسنده: فرشید باباجانی



Windows Server 2012

عنوان

صفحه

مقدمه

این کتاب، دربرگیرنده‌ی موضوعات مربوط به ویندوز سرور 2012 است که با گذراندن 8 ماه تلاش به نگارش درآمده است، هرچند کار بسیار طاقت‌فرسایی بوده، اما اگر نتیجه‌ی کار خوب باشد، این خستگی‌ها به چشم نمی‌آید.

در سال‌های پیش، نگارنده کتاب‌های متفاوتی را در عرصه‌ی کامپیوتر و شبکه به نگارش درآورده که یکی از بهترین و پرمحتواترین کتاب‌ها، کتاب کاملاً تصویری "شیرپوینت را قورت دهید"، بود که با استقبال بی‌نظیر شما عزیزان همراه بود، در این کتاب نیز سعی شده است که مطالب به زبان بسیار ساده و پرکاربرد به همراه تصویر موردنظر بیان گردد که می‌توان گفت کتاب خوبی ازنظر این‌جانب بوده است، هرچند نظر خوانندگان کتاب مهم‌تر است.

از شما دوست عزیز خواهشمند است که انتقادات و نظرات خود را درباره‌ی کتاب، در میان بگذارید. هزینه‌ای که برای این کتاب پرداخت می‌کنید، مطمئن باشید کاملاً باارزش بوده و شمارا در پیشرفت کارتان کمک خواهد کرد و به بنده نیز این انرژی را می‌دهد تا بتوانم کتاب‌های بیشتری را به قلم آورم.

چنانچه نتوانسته‌اید مبلغی را پرداخت کنید و آن را از دوستان خویش به‌رایگان دریافت نموده‌اید، مبلغ 18000 تومان را به شماره کارت 6219 8610 0688 3549 بانک سامان به نام فرشید بابجانی زاده واریز کنید.

با تشکر- فرشید باباجانی.

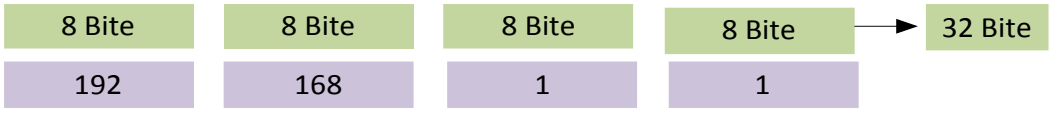
بررسی IPV4

در این بخش، گذری به دنیای زیبای IP ها داریم و نحوه‌ی آدرس‌دهی در شبکه را می‌آموزیم.

اگر با IP ها مشکل‌دارید حتماً این بخش را به‌دقت مطالعه کنید.

شروع کار:

همان‌طور که مشاهده می‌کنید IPv4 از چهار قسمت تشکیل‌شده است که هر بخش آن 8 بیت است و اگر 8 ضربدر 4 کنیم، می‌شود 32 بیت، به همین راحتی.



به هر یک از این قسمت‌ها یک هشت‌تایی یا همان octet می‌گویند. مثلاً 192.168.1.1 که به هر قسمت برفرض 192 یک octet می‌گویند.

IP ها به 5 کلاس تقسیم می‌شوند که هرکدام را باهم مرور می‌کنیم.

Class A:	**1 – 127**
Class B:	**128-191**
Class C:	**192- 223**
Class D:	**224 – 239**
Class E:	**240 – 255**

مثال:

192.168.1.1 که IP اول عدد آن 192 هست این IP، در رنج کلاس c قرار دارد. به همین صورت اگر IP قسمت octed اول دریکی از رنج‌های مشخص‌شده‌ی بالا قرار داشته باشد، میگوییم که در این کلاس قرار دارد. مثلاً 10.10.10.1 یک IP در کلاس A است، چون 10 بین شماره 1-127 قرار دارد.

- تذکر: رنج IP کلاس A از 126 - 1 است و شماره 127 برای تست کارت شبکه می‌باشد که همان IP 127.0.0.1 است و به loopback معروف است. پس برای استفاده از کلاس A می‌توان از شماره 126 – 1 را استفاده کرد.

توجه داشته باشید که کلاس D برای multicasting به کار می‌رود که این بحث را در درس‌های بعدی باهم مرور می‌کنیم، این IP ها روی‌هاست یا همان سیستم تنظیم نمی‌شوند و IP های کلاس E برای تحقیقات به کار می‌رود و قابل‌استفاده نیست. پس، فقط ما از IP های کلاس‌های A,B,C برای شبکه خود استفاده می‌کنیم.

IP ها بر دو نوع می‌باشند:

1- Private address: این دسته از IP، فقط و فقط در شبکه‌های داخلی بکار می‌روند و در دنیای اینترنت اعتباری ندارند. این نوع از IP ها در هر کلاس وجود دارند که به ترتیب زیر است:

Class A:	**10.0.0.0**
Class B:	**172.16.0.0 - 172.31.255.255**
Class C:	**192.168.0.0**

IP هایی که با این اعداد شروع می‌شوند، مربوط به شبکه داخلی می‌باشند و اعتباری در اینترنت ندارند.

2- Public Address: این دسته از IP ها توسط سازمانی به نام IANA ریجیستر می‌شوند و بعدازاین کار در اینترنت، اعتباردارند این دسته شامل تمام IP های کلاس‌های A,B,C است به غیر از آدرس‌های Private Address که در قسمت قبل باهم بررسی کردیم.

یک IP از دو بخش تشکیل‌شده است:

- Network address
- Host address

Network Address، به تعداد شبکه‌های موجود و Host address، به تعداد میزبان موجود اشاره دارد.

برای اینکه بتوانیم این دو موضوع را درک کنیم باید subnet mask را بررسی کنیم:

Subnet Mask:

این آدرس، نشان‌دهنده‌ی این است که چه مقدار بیت متعلق به آدرس شبکه و چه مقدار آن، متعلق به میزبان شبکه است.

Class	IP	Subnet Mask
A	**11.1.5.1**	255.0.0.0
B	**175.1.1.1**	255.255.0.0
C	**192.168.1.1**	255.255.255.0

همان‌طور که مشاهده می‌کنید برای هر IP در کلاس مشخص یک subnet mask تعریف‌شده است که نشان‌دهنده‌ی تعداد شبکه و هاست است.

در قسمت Subnet Mask اعداد 255 مربوط به قسمت Network Address و اعداد 0 مربوط به Host address می‌باشند.

مثلاً اگر IP به شماره 195.1.1.1 به شما بدهند و بگویند subnet Mask آن را مشخص کنید، سریع با نگاه کردن به کلاس‌های IP متوجه می‌شوید که عدد اول این IP در رنج کلاس c قرار دارد و Subnet Mask آن به‌صورت 255.255.255.0 است.

همیشه روال به این صورت نیست که IP ها به همین صورت، استاندارد در شبکه‌ها نشان داده شوند به این کلاس‌بندی‌ها اصولاً یک الگوی استاندارد می‌گویند، امّا همیشه این‌چنین نیست و الگوی غیراستاندارد هم وجود دارد.

الگوی غیراستاندارد:

ببینید دوستان هر قسمت IP (octet) از هشت عدد تشکیل‌شده است که می‌تواند صفر یا یک باشد.

11110111 . 11111110 . 11101011 . 11000111

هرکدام از این شماره‌ها در هر بخش دارای یک شماره اختصاصی می‌باشند که به‌صورت زیر است.

1 2 4 8 16 32 64 128 این شماره‌ها، روی هرکدام از چهار بخش بالا به‌صورت جداگانه قرار می‌گیرند.

اولین قسمت از سمت چپ را در زیر مشاهده می‌کنید، به نحوه‌ی قرار گرفتن اعداد توجه کنید.

128	64	32	16	8	4	2	1
1	**1**	**1**	**1**	**0**	**1**	**1**	**1**

برای درک بهتر موضوع، یک مثال را باهم بررسی می‌کنیم:

192.168.1.1، برای به دست آوردن Binary این IP، طبق شماره‌هایی که در هر قسمت به شما گفتیم، عمل کنید.

مثلاً اگر بخواهیم شماره‌ی 192 را از بین شماره‌های 1 2 4 8 16 32 64 128 به دست بیاوریم، همیشه از سمت چپ شروع می‌کنیم، میگوییم 128 از 192 کوچک‌تر است، پس زیر 128 را 1 قرار می‌دهیم، در ادامه 128 را که تا اینجا به دست آوردیم، پس عدد بعدی ما چند است؟ خوب اگر 64 را با 128 که قبلاً به دست آوردیم جمع کنیم می‌شود 192!!! چه جالب 192 شد پس زیر 64 هم 1 قرار می‌دهیم، با این حساب، توانستیم شماره‌ی 192 را پیدا کنیم، وقتی به شماره‌ی موردنظر رسیدیم، زیر بقیه‌ی شماره‌ها، صفر قرار می‌دهیم. طبق جدول:

128	64	32	16	8	4	2	1
1	**1**	**0**	**0**	**0**	**0**	**0**	**0**

پس شماره‌ی باینری به‌دست‌آمده، 11000000 است. بقیه‌ی اعداد هم به‌صورت زیر است.

192	168	1	1
11000000	**10101000**	**00000001**	**00000001**

در یک رنج IP، دو نوع IP قابل‌استفاده نیستند، به مثال زیر توجه کنید (مهم):

IP: 192.168.1.1

Sbnet Mask:255.255.255.0

همان‌طور که آموختیم، 255 به این نکته اشاره می‌کند که IP های 192.168.1 ثابت است و فقط octet آخر قابل‌تغییر از 0 تا 255 است. ببینید دوستان هر یک از قسمت‌های IP از 0 تا 255 قابل‌تغییر است.

خوب این IP، فقط در قسمت آخر قابل‌تغییر است، بین 0 تا 255، همان‌طور که گفتیم دو IP در هر رنج مانند این IP قابل‌استفاده نیستند. به جدول زیر توجه کنید:

192.168.1.0	**Network address**
192.168.1.1	**IP قابل‌استفاده**
192.168.1.2	**IP قابل‌استفاده**
192.168.1.3	**IP قابل‌استفاده**
⋮	
192.168.1.255	**Broadcast**

اولین IP به‌عنوان Network address و آخرین IP به‌عنوان Broadcast IP انتخاب می‌شود و نمی‌توانیم در شبکه از آن‌ها استفاده کنیم.

تذکر: نام دیگر Network address، Net ID است.

مثالی دیگر: در IP زیر، Net ID و Broadcast ID را به دست می‌آوریم:

172.16.1.1

255.255.0.0

در این مثال،IP از رنج B است. همان‌طور که مشاهده می‌کنید، subnet mask از دو تا255 تشکیل‌شده است پس 2 قسمت اول IP، ثابت (172.16) و دو قسمت بعد قابل‌تغییرند، به این صورت نتیجه می‌دهد که:

Net ID: 172.16.0.0

Broadcast ID: 172.16.255.255

اختصاص دادن رنج IP به شبکه:

زمانی پیش می‌آید که شما مدیر شبکه‌ی یک شرکت یا یک کارخانه می‌شوید، رئیس شما یک رنج IP خاصی را به شما می‌دهند و می‌گویند که این رنج IP را به اتاق‌های مختلف این شرکت بدهید، به‌طوری‌که IP ها هدر نرود و کم نیاید.

خوب برای این کار یک مثال می‌زنیم و باهم حل می‌کنیم:

شما در یک شرکت کار می‌کنید که از 3 اتاق حسابداری، کامپیوتر و طراحی تشکیل‌شده است؛ در این اتاق‌ها، چندین کامپیوتر به‌قرار زیر وجود دارد.

اتاق حسابداری 50 کامپیوتر،

اتاق کامپیوتر 60 کامپیوتر،

اتاق طراحی 14 کامپیوتر.

رئیس شرکت به شما یک IP در رنج زیر می‌دهد.

192.168.1.0

255.255.255.0

خوب سریع این IP را در ذهن خود تحلیل کنید، حداکثر IP قابل‌استفاده، 255 تا عدد است. امیدوارم بحث‌های قبلی را خوب خوانده باشید، اگر متوجه شده باشید که حتماً همین‌طور است، Subnet mask از سه قسمت ثابت تشکیل‌شده است که فقط، گزینه‌ی آخر قابل‌تغییر از 0 تا 255 است.

برای اختصاص دادن IP به این اتاق‌ها، اول‌ازهمه، اتاقی را انتخاب کنید که بیشترین کامپیوتر را دارد که در این مثال، اتاق کامپیوتر از 60 کلاینت برخوردار است.

همان‌طور که قبلاً گفتیم در هر قسمت از IP، اعدادی استاندارد و ثابتی وجود دارد.

128 64 32 16 8 4 2 1

همیشه این اعداد را در ذهن خود نگه‌داشته باشید، کل IP به همین اعداد خلاصه می‌شود و در ادامه، خیلی به آن نیاز داریم.

خوب شما اول باید ببینید 60 بین کدام‌یک از اعداد بالا قرار دارد. باکمی دقت متوجه می‌شوید که بین 32 و 64 قرار دارد، چون ما احتیاج به 60 تا IP داریم، پس عدد 64 انتخاب می‌شود.

IP ما می‌شود 192.168.1.0~63 در این IP، از علامت ~ استفاده کردیم که نشان‌دهنده‌ی تعداد IP است. همان‌طور که گفتیم دو آدرس از این رنج برای Net ID و Broadcast ID است؛ یعنی رنج زیر:

Net ID: 192.168.1.0

Broadcast ID: 192.168.1.63

پس با کسر این دو IP، 62 آدرس برای ما می‌ماند که 60، IP آن به کامپیوترها تخصیص داده می‌شود و 2، IP هم برای زمانی که اگر خواستیم کامپیوتر جدید در اتاق اضافه کنیم، به کار می‌رود.

رنج IP را به دست آوردیم؛ ولی subnet mask مربوط به این IP را به دست نیاوردیم؛ برای این کار همان عدد 64 را که درون شماره‌ها به دست آوردیم را منهای 256 می‌کنیم (256 عددی است که از اعداد 0 تا 255 به دست می‌آید).

256 - 64 = 192

پس subnet mask برای این IP می‌شود: 255.255.255.192 که 192 نشان‌دهنده‌ی 64، IP برای این شبکه است.

اتاق بعدی‌ای که انتخاب می‌شود اتاق حسابداری است که شامل 50 کامپیوتر است، برای به دست آوردن رنج IP برای این اتاق، از IP هایی که استفاده‌نشده است، استفاده می‌کنیم.

IP هایی که در اختیارداریم به‌صورت زیر است:

192.168.1.64

به این خاطر، از عدد 64 در آخر این IP استفاده کردم که 64 تا آدرس به اتاق قبلی داده‌شده است و قابل‌استفاده نیست.

مانند اتاق قبلی، شما به 64، IP نیاز دارید؛ چون 50 بین 32 و 64 قرار دارد، پس 64 انتخاب می‌شود.

IP و subnet mask برای این اتاق، به‌صورت زیر است:

192.168.1.64~128

255.255.255.192

برای اتاق سوم (طراحی)، احتیاج به 14،IP داریم، باید از بین 8 و 16 عدد 16 را انتخاب کنیم، پس IP و subnet mask به‌صورت زیر می‌شود:

192.168.1.129~145

255.255.255.240

باید متوجه شده باشید که ما احتیاج به 16، IP داریم؛ پس، برای به دست آوردن subnet mask باید 16 را از 256 کم کنیم تا عدد آخر که 240 است به دست بیاید.

با این حساب، جدول نهایی IP ها به‌صورت زیر است:

طراحی	حسابداری	کامپیوتر
192.168.1.129~145	**192.168.1.64~128**	**192.168.1.0~63**
255.255.255.240	**255.255.255.192**	**255.255.255.192**
16	**64**	**64**

در این رنج‌ها، حداقل هدر رفتIP را داشتیم.

در این قسمت اگر مشکلی داشتید، می‌توانید از طریق ایمیل با من در تماس باشید.

IP ها به دو نوع Class Full و Class Less تقسیم می‌شوند که کلاس‌های A,B,C از نوع Class Full می‌باشند، به این دلیل به آن‌ها Class Full می‌گویند که subnet mask آن‌ها ثابت می‌باشد و تغییری نمی‌کند؛ مثلاً 255.255.0.0 که این subnet مربوط به Class b می‌باشد.

CIDR (Class Less Inter-Domain Routing)

این قسمت را باکمال دقت بخوانید.

این دسته از IP ها، برای شرکت‌هایی که ISP هستند و ارائه‌دهنده‌ی خدمات اینترنتی می‌باشند، به کار می‌رود. برای این شبکه‌ها، مهم است که چه مقدار IP را به چه کسی می‌دهند.

IP هایی که به‌عنوان Class Less شناخته می‌شوند، به‌صورت زیر می‌باشند:

172.16.1.1/16

یک‌چیز جدید در این IP مشاهده می‌کنید و آن‌هم، یک slash به همراه یک IP است که نشان‌دهنده‌ی تعداد شبکه یا همان Net ID است که در این رابطه باهم به‌صورت کامل بحث می‌کنیم.

بعد از Slash، عددی بین 1 تا 32 قرار می‌گیرد؛ این همان عددی است که در ابتدای کار اشاره کردم؛ یعنی هر IP از چهار قسمت هشت‌تایی تشکیل‌شده که می‌شود 32 تا، توجه داشته باشید که حداکثر عددی که پشت slash قرار گیرد 30 است، چون 2 بیت برای host Bite است.

مثال: تعداد Host و subnet mask رنج IP زیر را به دست می‌آوریم:

192.168.1.1/24

سریع‌ترین روش برای به دست آوردن جواب به‌صورت زیر است:

ببینید دوستان، هر قسمت از IP از هشت بیت تشکیل‌شده است که به‌صورت زیر می‌باشد:

1	2	3	4	5	6	7	8		9	10	11	12	13	14	15	16		17	18	19	20	21	22	23	24		25	26	27	28	29	30	31	32
1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1

در مثالی که زدیم، 24/ است که اگر به شکل نگاه کنید 3 تا octet اول را با هم جمع کنیم 24 می‌شود پس، می‌توان IP و Subnet mask را به این صورت نوشت:

192.168.1.0

255.255.255.0

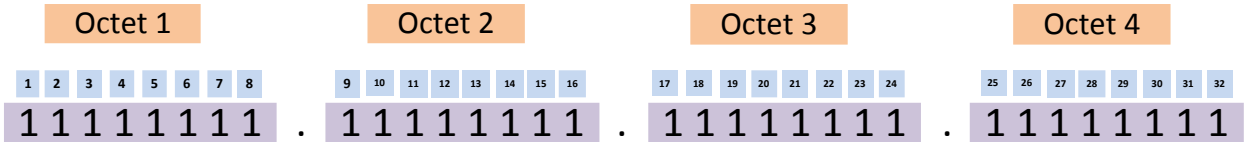
24/ می‌گوید که 3 تا octet اول ثابت باشد و octet آخر تغییر کند.

مثال بعدی:

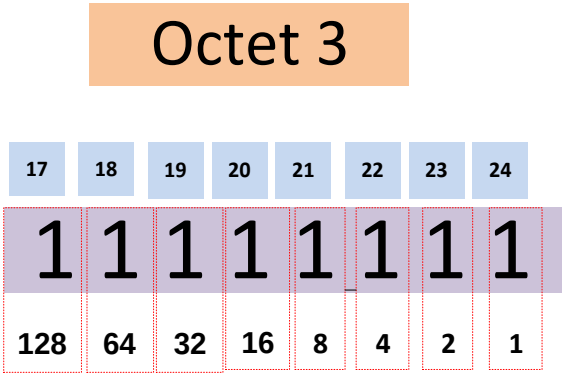
172.16.1.1/17

اگر به شکل زیر درست نگاه کنید 16 عدد اول را داریم، پس 2 تا عدد اول IP ثابت است که در یک‌گوشه می‌نویسیم 172.16 بعد نگاه می‌کنیم که عدد 17 در octet سوم قرار دارد؛ پس، فقط با octet سوم کار می‌کنیم.

سریع اعداد 1 2 4 8 16 32 64 128 یادداشت می‌کنیم و بعدازآن، این اعداد را، بالای عدد 17 تا 24 از سمت چپ به راست قرار می‌دهیم تا عدد 17 را پیدا کنیم. به شکل زیر توجه کنید:



در این شکل، به‌راحتی می‌توانید درک کنید که 17/ یعنی چه، ببینید سؤال از ما 17/ را می‌خواهد؛ پس طبق شکل، ما با octed3 کارداریم و دو octet اول را به‌صورت ثابت می‌نویسیم؛ چون تمام اعداد آن 1 است. پس برای به دست آوردن عدد 17، باید اعداد 1 2 4 8 16 32 64 128 را یادداشت کرده و از سمت چپ، اعداد 17 تا 24 را به آن‌ها اختصاص دهیم؛ یعنی عدد اولی که 128 باشد، به‌عنوان عدد 17 است و عدد دوم که عدد 64 باشد، به‌عنوان عدد 18 است. به شکل زیر توجه کنید:



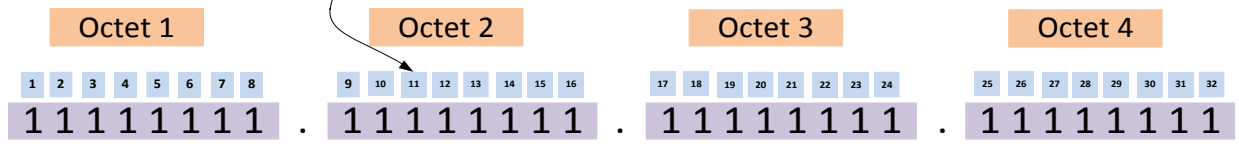
پس 17 همان عدد 128 است. این عدد را از 256 کم می‌کنیم و subnet mask ما به دست می‌آید.

172.16.0~127.0

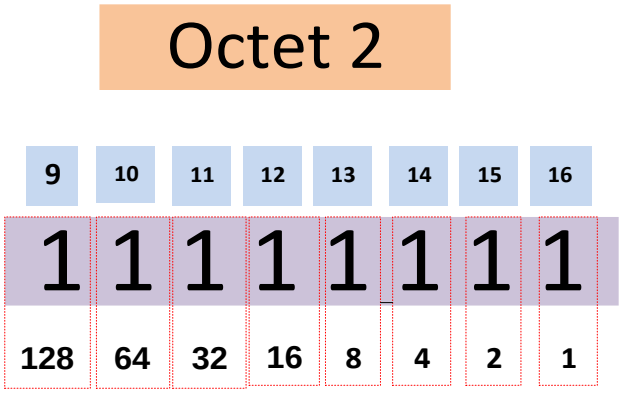
255.255.128.0

مثال پایانی این بحث:

10.10.10.1/11



همان‌طور که مشاهده می‌کنید 11/ از octed اول رد شده است؛ پس با octed دوم کارداریم این قسمت از عدد 9 شروع‌شده و به 16 ختم می‌شود، عددی که در مثال گفته 11/ است؛ پس، از 9 و 10 باید بگذریم تا به عدد 11 برسیم، برای این منظور اعداد 1 2 4 8 16 32 64 128 و از سمت چپ اعداد را با شماره 9 و بعد 10 و بعد 11 شماره‌گذاری می‌کنیم؛ مانند شکل بالا عدد زیر 11 که عدد 32 است را از 256 کم می‌کنیم که 224 به دست می‌آید.

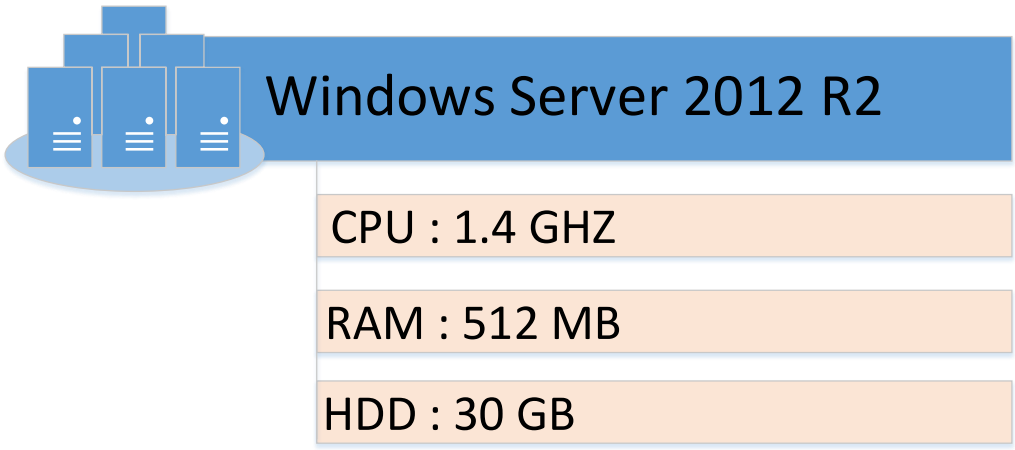


10.0~32.0.0

255.224.0.0

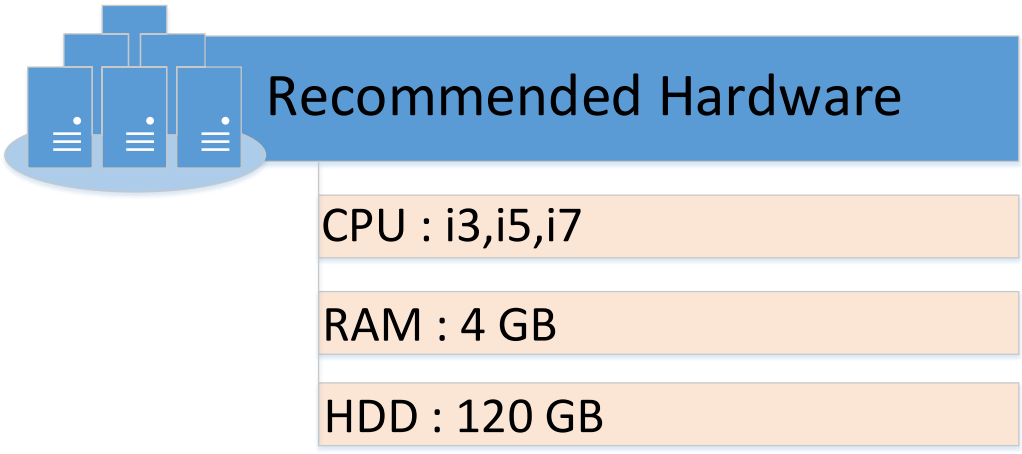
حداقل سخت‌افزار موردنیاز برای نصب ویندوز سرور 2012:

حداقل سخت‌افزار موردنیاز برای راه‌اندازی Windows Server 2012 R2 به‌صورت زیر است:



همان‌طور که مشاهده می‌کنید، حداقل سخت‌افزار موردنیاز برای این ویندوز مشخص‌شده است که مشخصاً نمی‌تواند سخت‌افزار خوبی برای اجرای ویندوز و سرویس‌های آن باشد، اما حداقل می‌تواند ویندوز سرور 2012 را اجرا کند.

سخت‌افزار مناسب برای Windows Server 2012 R2:



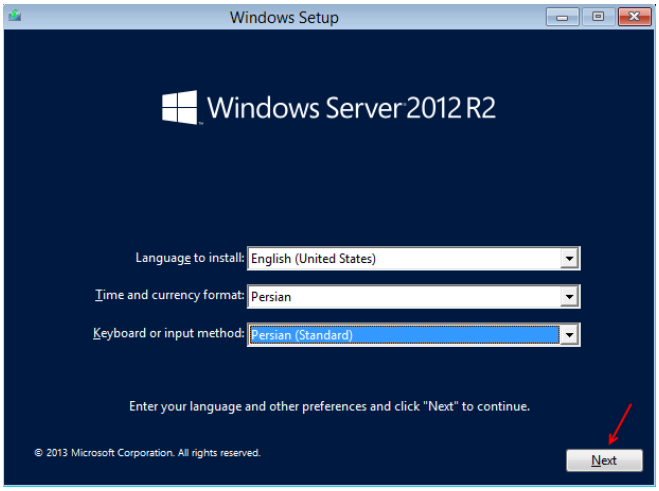
سخت‌افزاری که در شکل بالا لیست شده است، می‌تواند سخت افزار مناسبی برای اجرای ویندوز سرور باشد.

نصب و پیکربندی ویندوز سرور 2012:

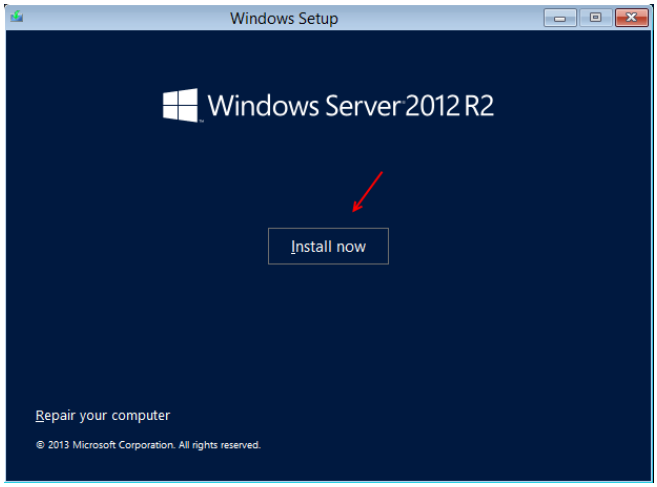
برای شروع باید ویندوز سرور را از سایت مایکروسافت دانلود کنیم و آن را طبق روش زیر نصب و پیکربندی کنیم. بعد از دانلود، فایل موردنظر با پسوند ISO است که شما می‌توانید آن را روی DVD قرار دهید و از آن در سیستم واقعی خود استفاده کنید و یا می‌توانید از آن به‌صورت یک سیستم مجازی در نرم‌افزار VMware 10 و یا سرویس Hyper-V و یا سرور مجازی ESX و ... استفاده کنید.

تمام سیستم‌ها در این کتاب، بر روی سرویس مجازی‌سازی Hyper-V اجرا می‌شوند که آموزش این سرویس را می‌توانید از این قسمت دانلود کنید.

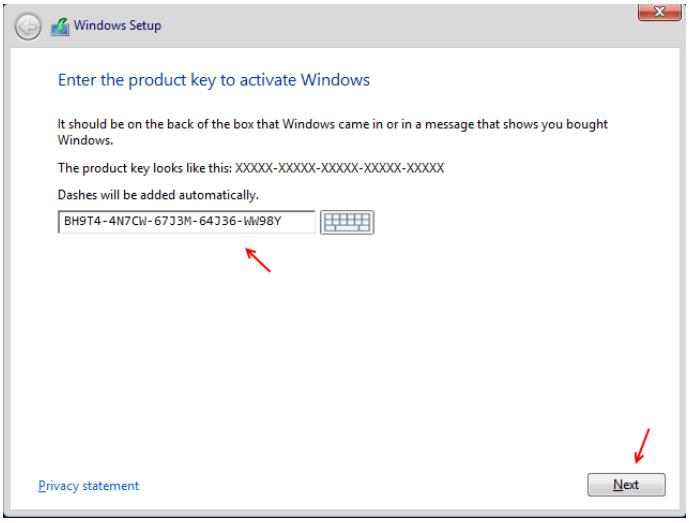
شروع نصب ویندوز سرور 2012:



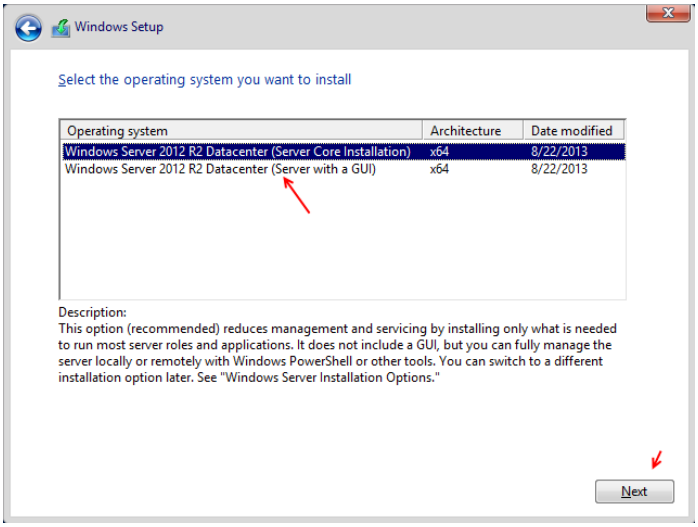
ویندوز سرور را اجرا می‌کنیم تا صفحه‌ی اول آن به‌صورت شکل روبرو ظاهر شود، در این صفحه مانند شکل، زبان موردنظر و نوع آن را مشخص کنید و بر روی Next کلیک کنید.



در این قسمت، بر روی Install now کلیک کنید تا وارد صفحه‌ی نصب شویم. در پائین همین صفحه گزینه Repair Your Computer وجود دارد که این گزینه، زمانی به کار شما می‌آید که بخواهید ویندوز قبلی خود را تعمیر کنید.



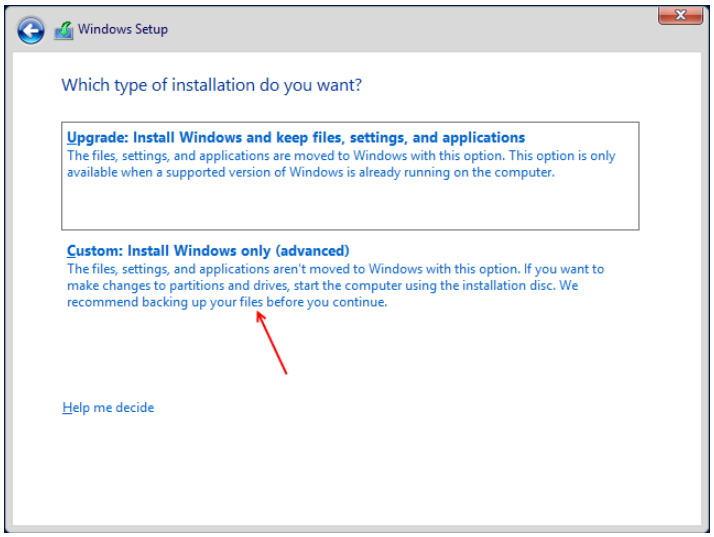
در این قسمت، سریال ویندوز سرور 2012 را وارد کنید و بر روی Next کلیک کنید. توجه داشته باشید این سریال با محدودیت زمانی است و فقط برای نصب ویندوز استفاده می‌شود.



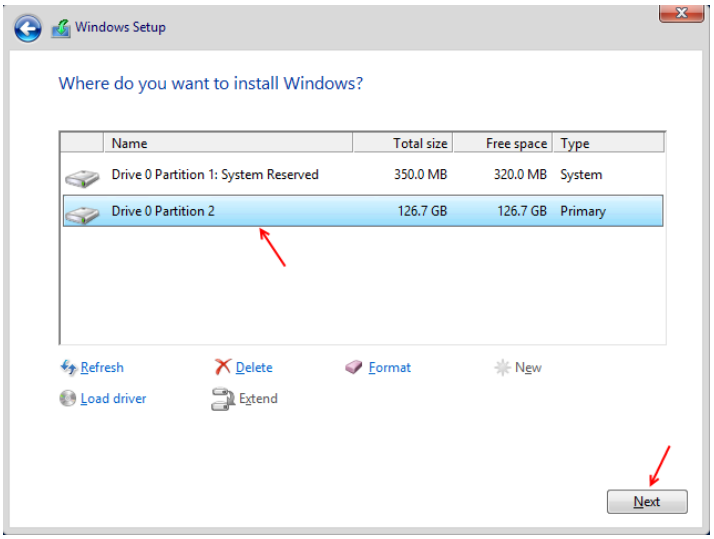
در این قسمت، دو گزینه وجود دارد که نوع سیستم‌عامل و ورژن آن را مشخص می‌کند، گزینه‌ی اول Server Core است که تمام اجزا به‌صورت دستور اجرا خواهد شد؛ یعنی برای استفاده از این قسمت باید دستورات ویندوز سرور را آموخته باشید.

در گزینه‌ی دوم که Server with a GUI است تمام اجزای ویندوز به‌صورت گرافیکی است در این قسمت، همین گزینه را انتخاب و بر روی Next کلیک کنید.

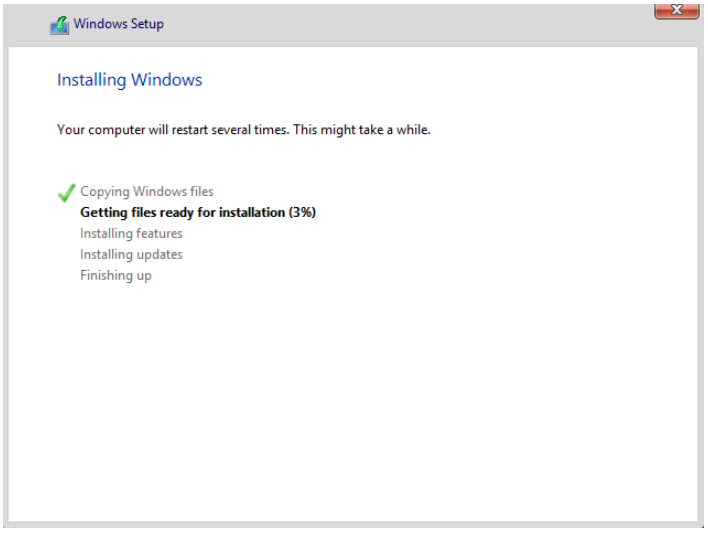
در این صفحه، قرارداد نامه‌ی مربوط به ویندوز سرور 2012 را مطالعه کنید و اگر مشکلی ندارید، تیک گزینه‌ی I accept the license terms را انتخاب و بر روی Next کلیک کنید.



در این صفحه، دو گزینه را مشاهده می‌کنید که گزینه اول، زمانی استفاده می‌شود که بخواهید ویندوز قبلی خود را که روی سرور قرار دارد به همراه نرم‌افزارهای آن حفظ کنید و فقط ویندوز قبلی آپدیت شود ولی در گزینه دوم می‌توانید ویندوز جدید خود را روی سرور نصب کنید. روی گزینه‌ی دوم کلیک کنید تا شکل بعد ظاهر شود.

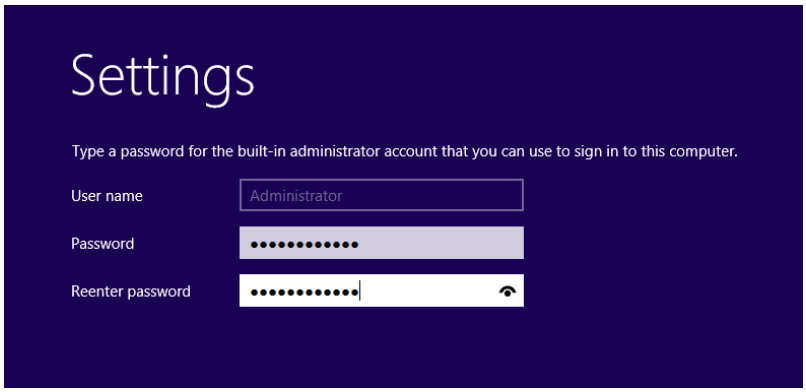


در این قسمت، درایو موردنظر خود را برای نصب ویندوز انتخاب کنید و بر روی **Next** کلیک کنید. توجه داشته باشید که گزینه‌هایی در زیر درایوها قرار دارد که برای **Format, Delete** و... استفاده می‌شود.



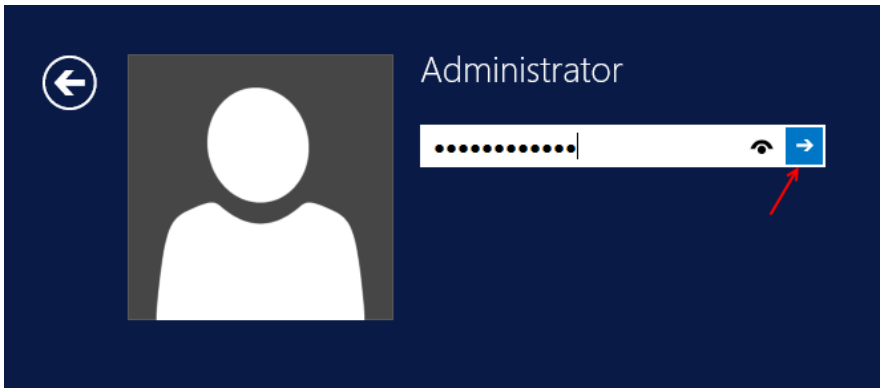
در حال نصب....

این قسمت، بسته به سیستم شما بین 10 تا 25 دقیقه به طول خواهد انجامید.



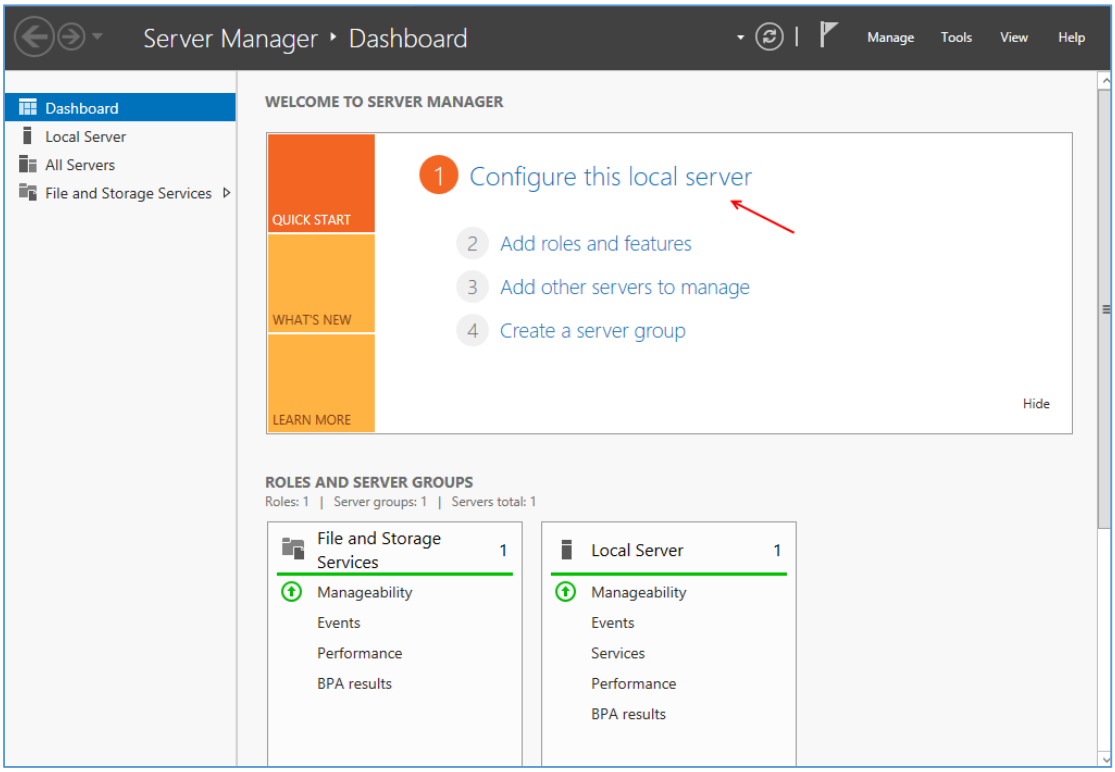
در این قسمت، رمز عبور را برای مدیریت ویندوز سرور خود وارد کنید، سعی کنید رمز عبور را به‌صورت پیچیده به‌مانند Test@12345 وارد کنید که ترکیبی از عدد، حروف و علائم است. بعد از واردکردن رمز بر روی Finish کلیک کنید.

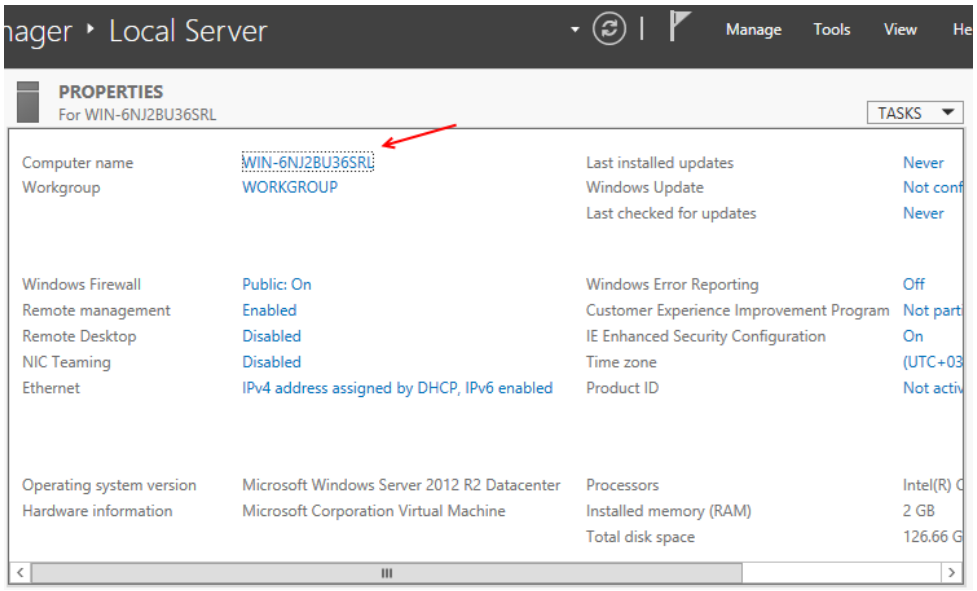
با مشاهده صفحه‌ی مقابل، کار نصب ویندوز سرور به اتمام رسیده است و حالا باید وارد ویندوز سرور شویم و تنظیمات اولیه را انجام دهیم. برای ورود به ویندوز، بر روی کلید ترکیبی Ctrl + Alt + Delete را فشار دهید تا شکل بعد ظاهر شود.



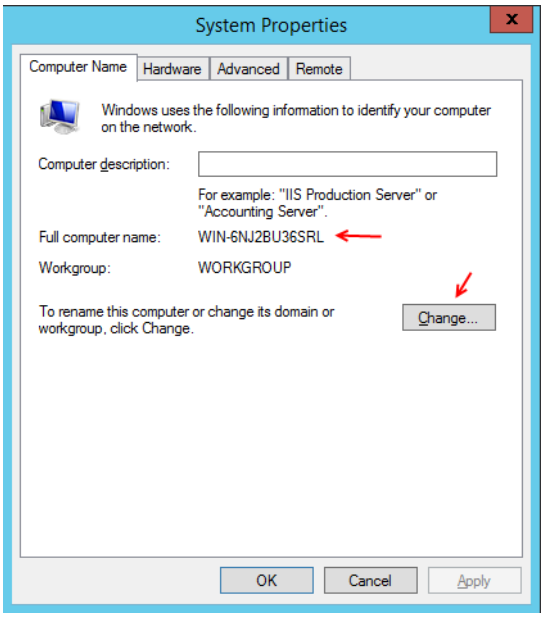
در این قسمت، رمز عبوری که در بخش قبلی وارد کردیم را اینجا وارد می‌کنیم و بر روی Enter فشار می‌دهیم تا وارد سرور 2012 شویم.

بعد از ورود به ویندوز سرور 2012، سرویس Server Manager به‌صورت خودکار در زمان ورود به ویندوز اجرا می‌شود. در این سرویس، کل اطلاعات مربوط به ویندوز سرور قرار دارد مانند Services Features, Local Servers و ... که باهم در این کتاب، تمام آن‌ها را بررسی خواهیم کرد. برای شروع تنظیمات بر روی Configure this local server به‌مانند شکل زیر کلیک می‌کنیم.

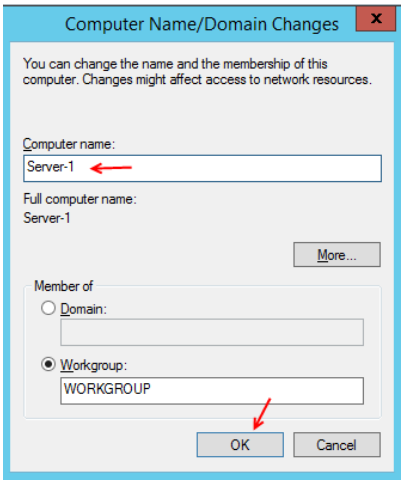




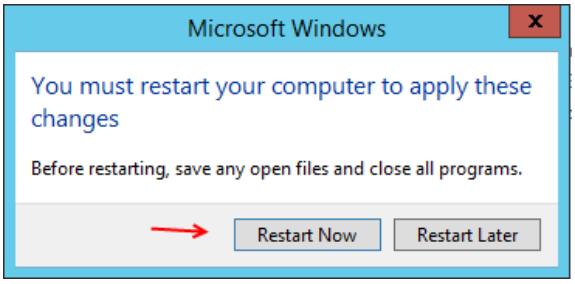
در این قسمت، می‌خواهیم تنظیمات اولیه‌ی سرور را انجام دهیم. اولین کاری که در این قسمت انجام می‌دهیم، تغییر نام سرور است که مانند شکل بر روی نام سرور خود کلیک می‌کنیم تا شکل بعد ظاهر شود.



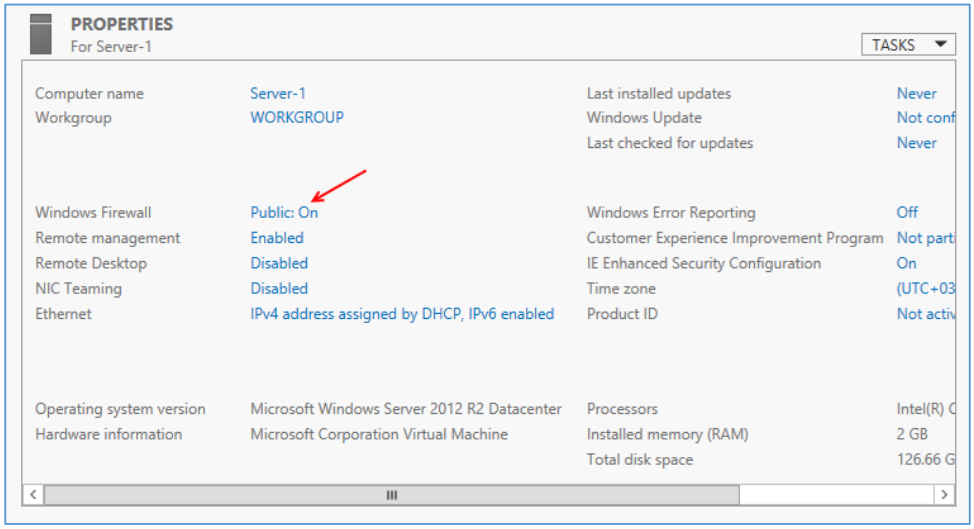
در این شکل، برای تغییر نام سرور بر روی Change کلیک می‌کنیم تا شکل زیر ظاهر شود.



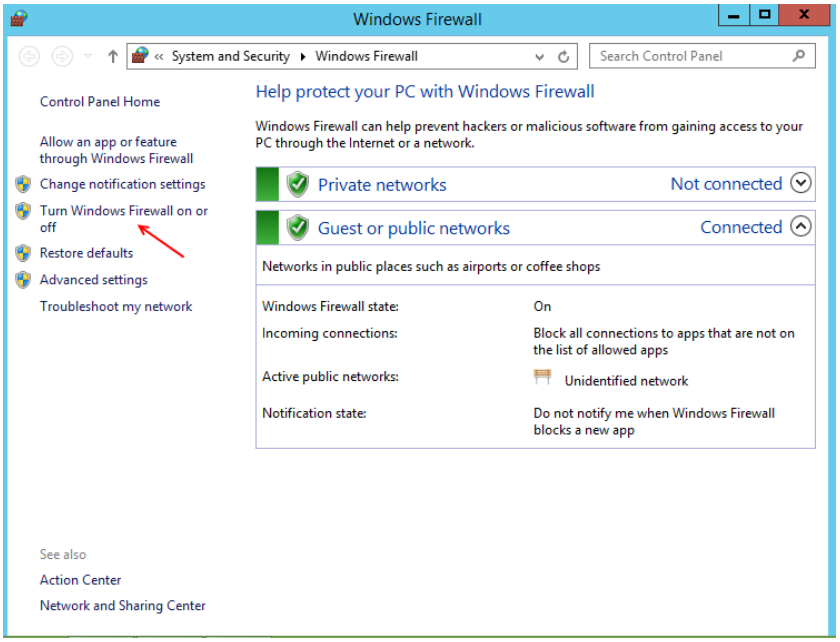
در این شکل و در قسمت Computer name نام سرور خود را وارد و بر روی ok کلیک کنید. قسمت Workgroup و Domain را بعداً بررسی خواهیم کرد.



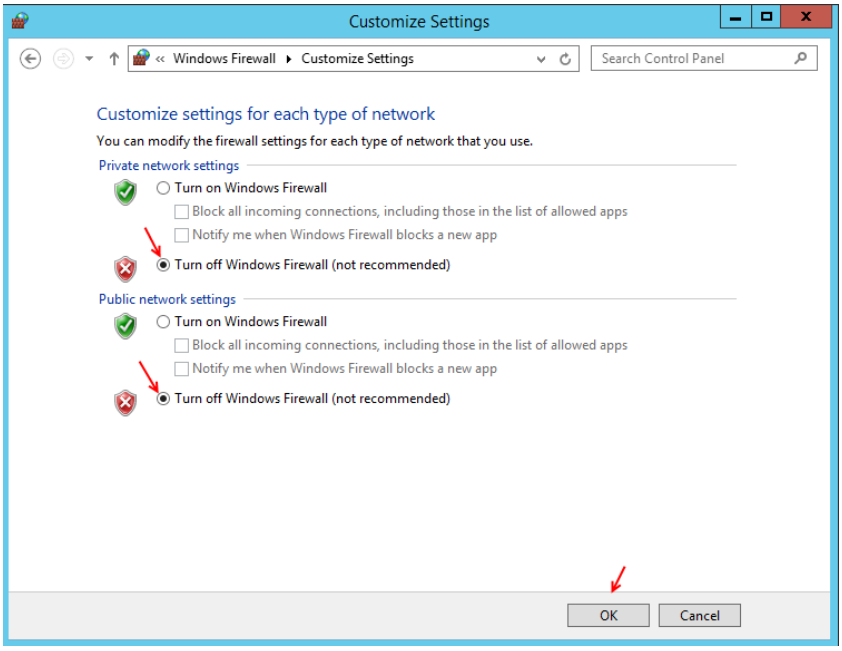
بعد از کلیک بر روی ok شکل مقابل ظاهر می‌شود که باید بر روی Restart Now کلیک کنید تا سیستم Restart شود و تنظیمات اعمال شود.



بعد از ورود به ویندوز، دوباره وارد Server Manager می‌شویم و بر روی Configure this local server کلیک می‌کنیم تا شکل مقابل ظاهر شود، همان‌طور که در این شکل مشاهده می‌کنید، نام سرور تغییر کرده است. مرحله‌ی بعد خاموش کردن Firewall سرور است که برای این کار روی Public: on کلیک کنید.



در این صفحه، برای اینکه Firewall را خاموش‌کنیم، بر روی Turn Windows Firewall on or off در سمت چپ صفحه کلیک کنید.

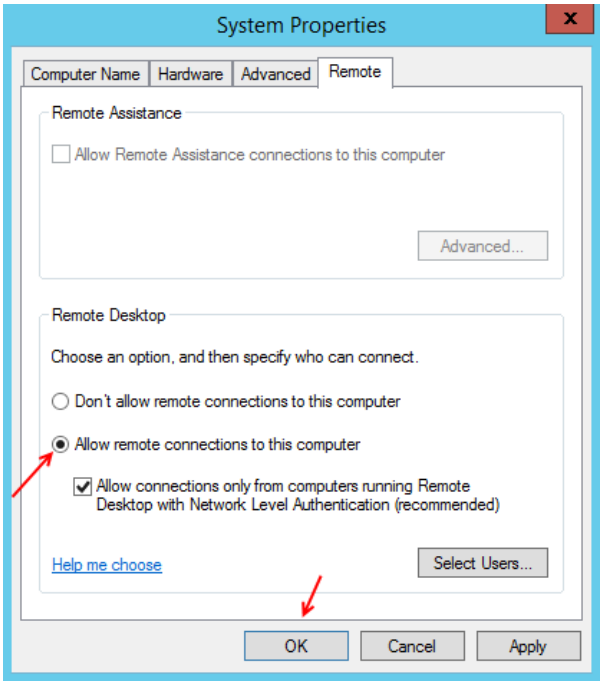


در این قسمت، به‌مانند شکل Turn Off Windows Firewall را انتخاب کنید و بر روی ok کلیک کنید.

بعدازاین کار Firewall خاموش خواهد شد که این کار ازنظر امنیتی جالب نخواهد بود. در ادامه، نحوه‌ی کار با آن را بررسی خواهیم کرد.

همان‌طور که مشاهده می‌کنید، Firewall خاموش شده است. البته باید صفحه را Refresh کنید تا تغییرات

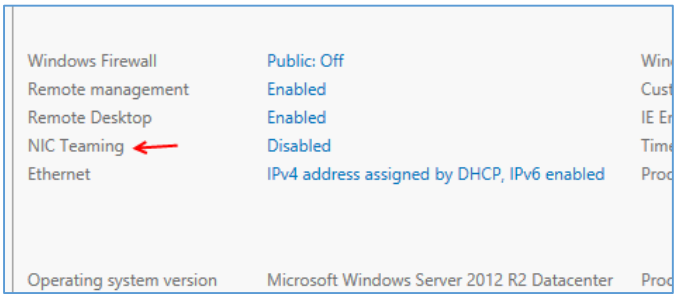
اعمال شود، بعدازاین کار نوبت به فعال‌سازی Remote Desktop است تا بتوانیم از راه دور به سیستم متصل شویم، بر روی Disabled کلیک کنید تا شکل بعد ظاهر شود.



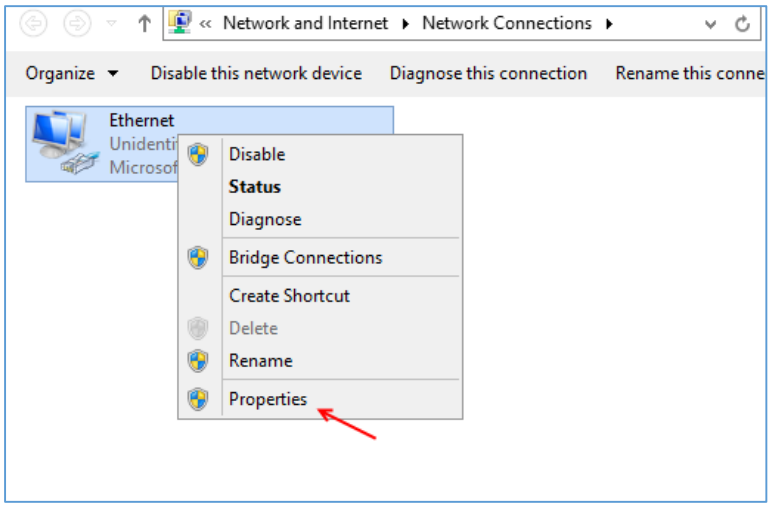
در این قسمت بر روی Allow remote connections.. کلیک کنید تا دسترسی از راه دور، توسط سرویس Remote Desktop فعال شود. توجه داشته باشید با کلیک بر روی Select Users می‌توانید کاربر موردنظر خود را به لیست کاربران دارای مجوز ورود از راه دور اضافه کنید.

بر روی ok کلیک کنید تا به صفحه‌ی Service Manager برگردیم.

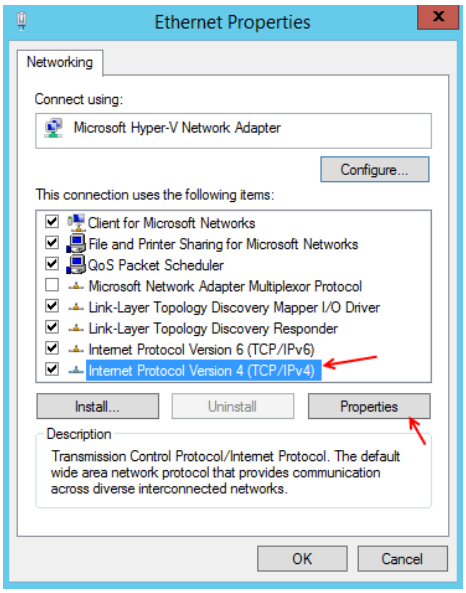
گزینه‌ی بعدی، یعنی NIC Teaming که برای استفاده از چند کارت شبکه برای تقسیم بار شبکه بر روی چند خط است که فعلاً با این موضوع کاری نداریم.



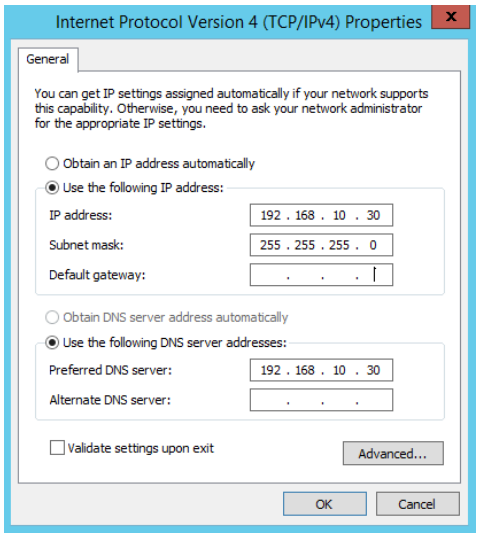
گزینه‌ی بعدی که وجود دارد تنظیم IP Address کارت شبکه موردنظر است که برای این کاربر روی IPv4 address assigned... کلیک می‌کنیم تا شکل روبرو ظاهر شود.



همان‌طور که در شکل روبرو مشاهده می‌کنید باید بر روی کارت شبکه موردنظر خود کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید تا شکل بعد ظاهر شود.

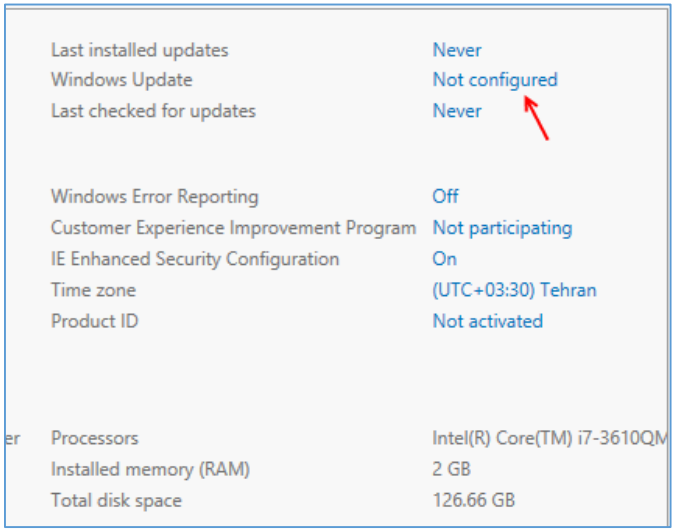


در این قسمت از لیست موجود، در ابتدا تیک گزینه‌ی Internet Protocol Version 6 را بردارید و بعد بر روی Internet Protocol Version 4 کلیک کنید و بر روی Properties کلیک کنید تا شکل بعد ظاهر شود.

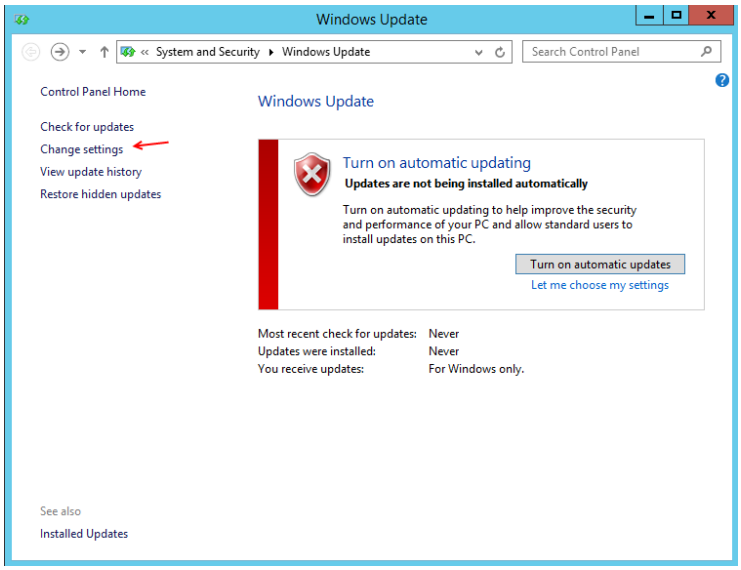


در این صفحه و در قسمت IP Address می‌توانید IP به شماره‌ی 192.168.10.30 را وارد کنید و در قسمت Subnet Mask باید 255.255.255.0 را وارد کنید و در قسمت DNS که درباره‌ی این سرویس در بخش‌های بعدی کتاب بحث خواهیم کرد شماره‌ی 192.168.10.30 را وارد می‌کنیم.

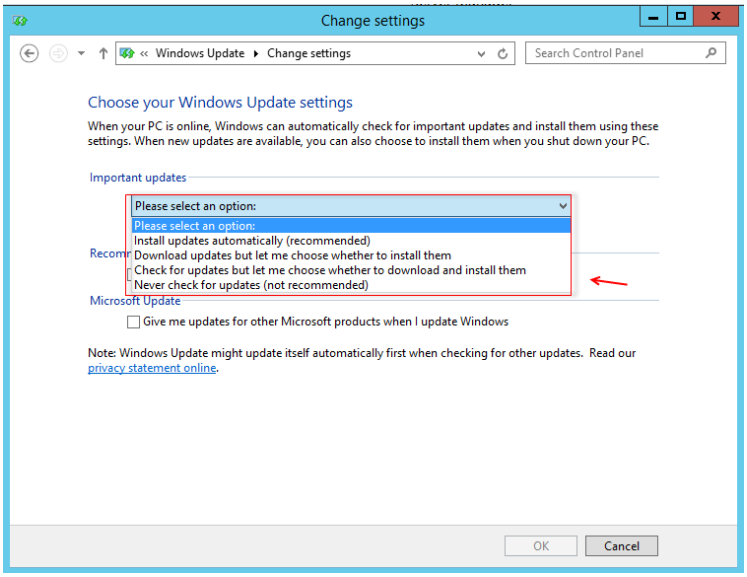
بر روی ok کلیک کنید تا تنظیمات اعمال شود.



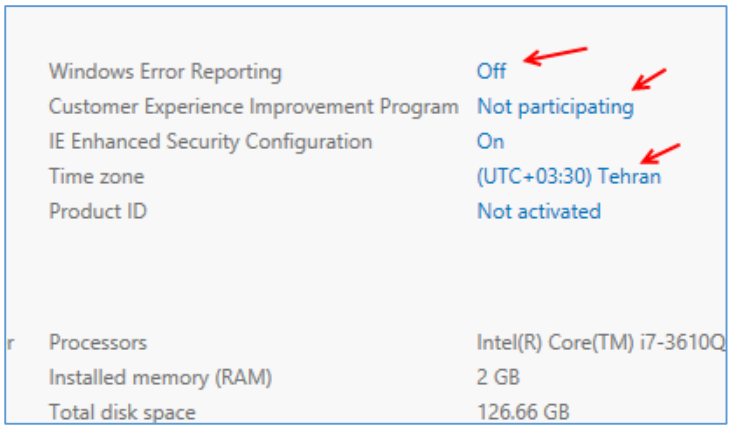
بعد از تنظیم کردن IP Address به قسمت Update مراجعه می‌کنیم که برای تنظیم قسمت Update باید بر روی Not Configured کلیک کنید تا شکل بعد ظاهر شود.



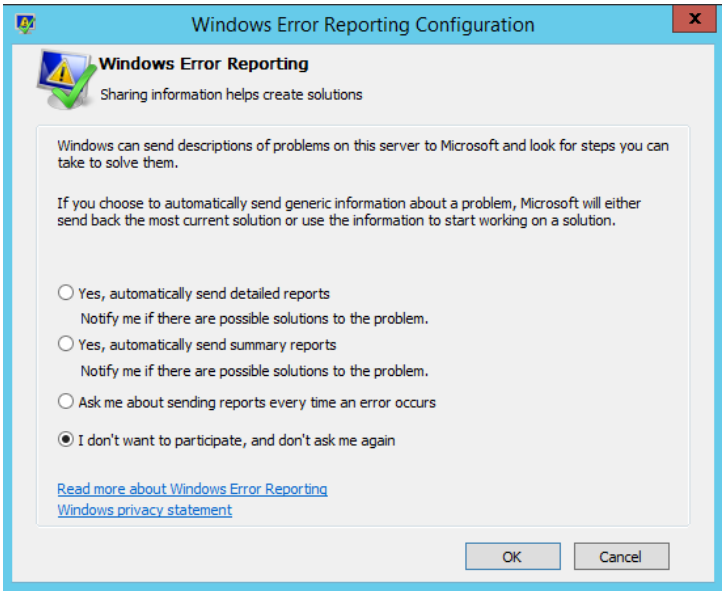
در این صفحه از سمت چپ، بر روی Change Settings کلیک کنید.



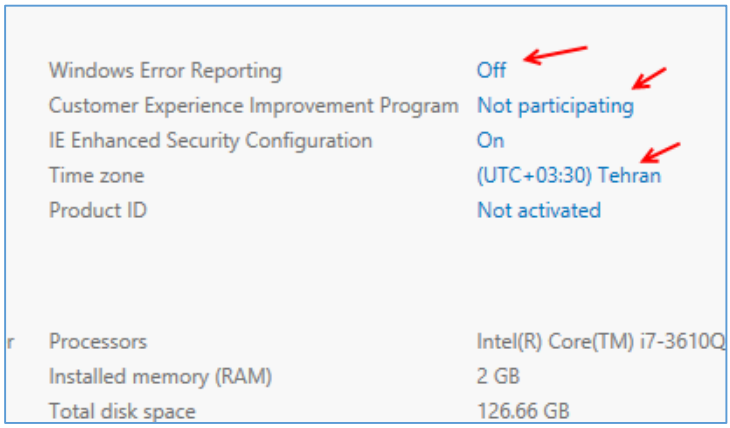
در این قسمت، گزینه‌های مختلفی را مشاهده می-کنید، اگر می‌خواهید آپدیت به‌صورت خودکار در زمان متصل شدن به اینترنت، دانلود و نصب شود، گزینه‌ی اول را انتخاب کنید و یا اگر می‌خواهید به‌صورت دستی، آپدیت موردنظر خود را انتخاب کنید، گزینه‌ی دوم و سوم را انتخاب کنید و اگر نمی-خواهید آپدیتی صورت گیرد بر روی Never Check for .... کلیک کنید و بعد بر روی ok کلیک کنید تا تنظیمات موردنظر اعمال شود.



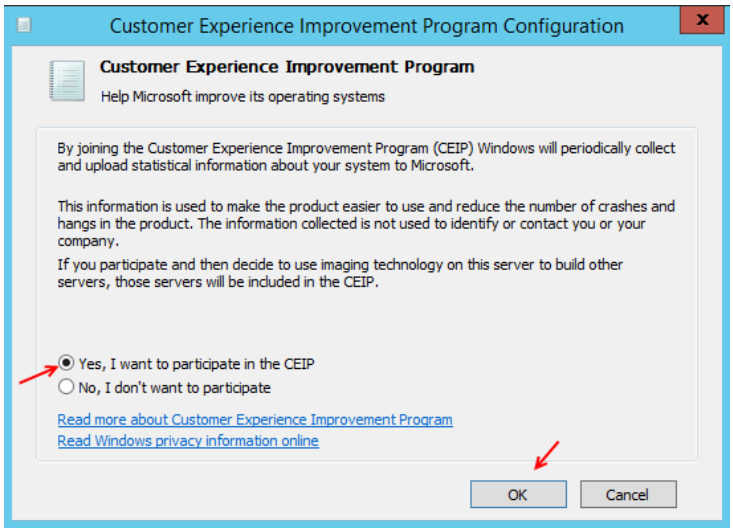
در قسمت بعد، گزینه‌ای با عنوان Windows Error Reporting وجود دارد که این گزینه، برای ارسال اطلاعات و مشکلات ویندوز سرور شما به سایت مایکروسافت است که برای فعال کردن آن بر روی off کلیک کنید تا شکل بعد ظاهر شود.



در این صفحه، چهار گزینه وجود دارد که گزینه‌ی اول، برای ارسال اطلاعات با جزئیات به سایت مایکروسافت است. گزینه‌ی دوم، برای ارسال اطلاعات بدون جزئیات و با جمع‌بندی کامل است. گزینه‌ی سوم، در هنگام ارسال از شما سؤال خواهد کرد و گزینه‌ی آخر، برای غیرفعال کردن آن به کار خواهد رفت. بر روی ok کلیک کنید.

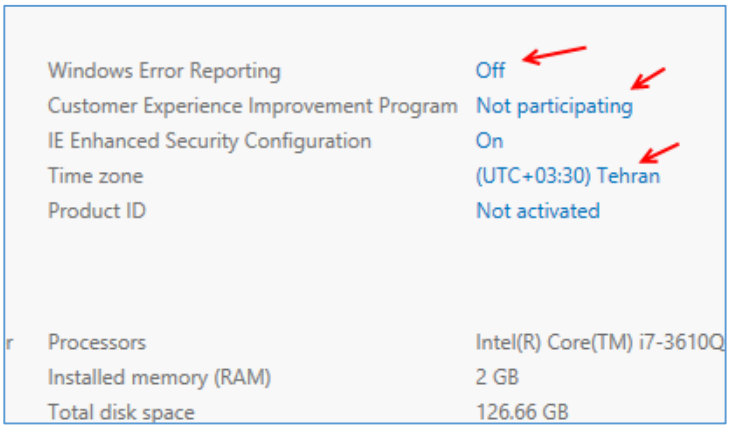


قسمت بعدی که باید باهم بررسی کنیم گزینه‌ی Customer Experience improvement Program است که به‌مانند قسمت قبلی اطلاعات کاملی از سیستم شمارا تهیه و در یک فایل بسته‌بندی می‌کند و به سایت مایکروسافت ارسال خواهد کرد که برای فعال کردن آن بر روی Not particIPating کلیک کنید.



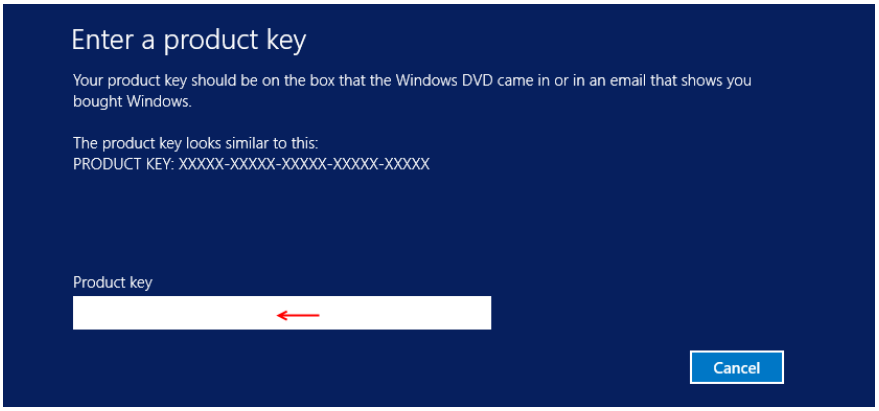
در این شکل برای فعال کردن CEIP بر روی Yes, I want to particIPate in the CEIP کلیک کنید و بعد بر روی ok کلیک کنید.

در کل سعی کنید این قسمت و قسمت قبلی را در صورت کرک بودن ویندوز خود فعال نکنید.



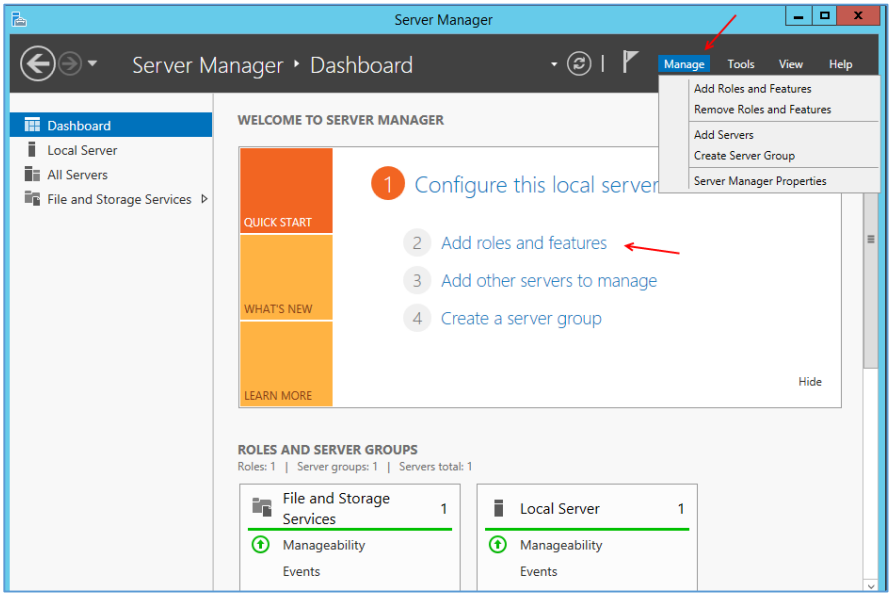
قسمت بعدی که در این شکل وجود دارد، گزینه‌ی Time Zone است که این قسمت را در هنگام نصب باهم تنظیم کردیم. اگر تنظیمات شما با مشکل مواجه شده است، باید بر روی منطقه‌ی موردنظر خود کلیک کنید و در شکل بازشده، منطقه‌ی خود را انتخاب کنید.

در قسمت Product ID، گزینه‌ی Not activated قرار دارد که نشان می‌دهد این ویندوز فعال نشده است، برای فعال کردن ویندوز، بر روی Not activated کلیک کنید تا شکل زیر ظاهر شود.



در این قسمت باید سریال اصلی ویندوز سرور 2012 را وارد کنید تا ویندوز به‌صورت کامل فعال شود.

بعد از اتمام کار یک‌بار سیستم را Restart کنید تا تنظیمات به‌درستی اعمال شود.

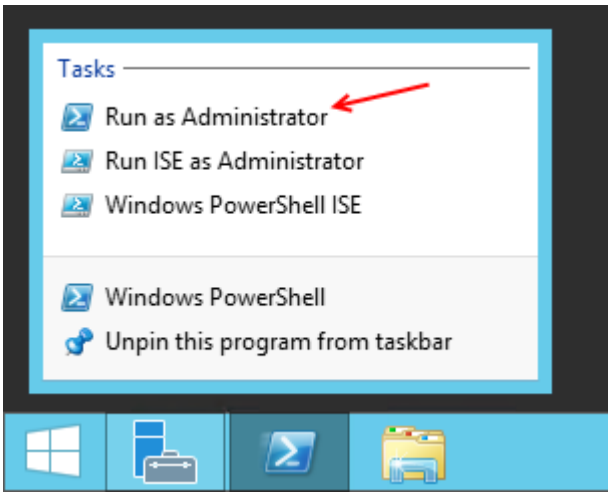


بعد از اعمال تغییرات بالا از سمت چپ به‌مانند شکل روبرو، بر روی Dashboard کلیک می‌کنیم که در این قسمت، گزینه‌های مختلفی مانند Add Roles and Features وجود دارد که برای نصب Feature ها مورداستفاده قرار می‌گیرد، در ادامه با قسمت‌های مختلف آن آشنا خواهیم شد.

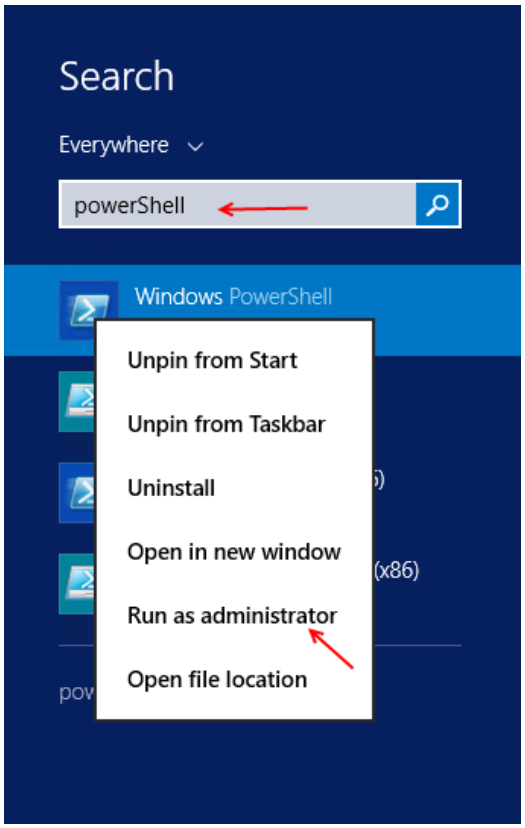
کار با PowerShell:

این سرویس که قلب ویندوز سرور است، نوع جدیدی از سرویس CMD می‌باشد که در آن، تمام‌کارهایی را که شما در ویندوز سرور به‌صورت گرافیکی انجام می‌دهید، می‌توانید به‌صورت دستور اجرا کنید.

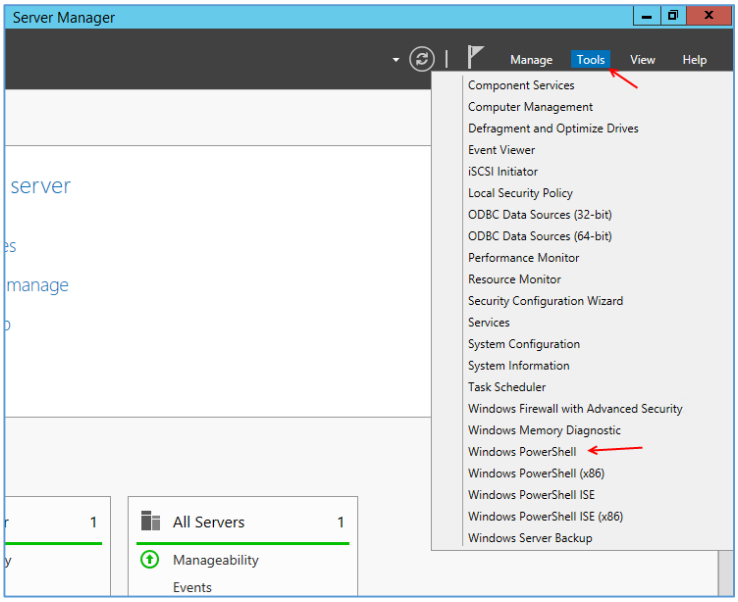
برای اجرای PowerShell، روش‌های مختلفی وجود دارد که آن‌ها را باهم بررسی می‌کنیم:



آسان‌ترین راه اجرای PowerShell، این است که در نوار Taskbar روی آیکون PowerShell که در شکل روبرو هم مشاهده می‌کنید کلیک راست کنید و گزینه‌ی Run as Administrator را انتخاب کنید، همیشه سعی کنید که این از روی کاربر Administrator، این سرویس را اجرا کنید تا به‌خوبی دستورات اجرا شوند.

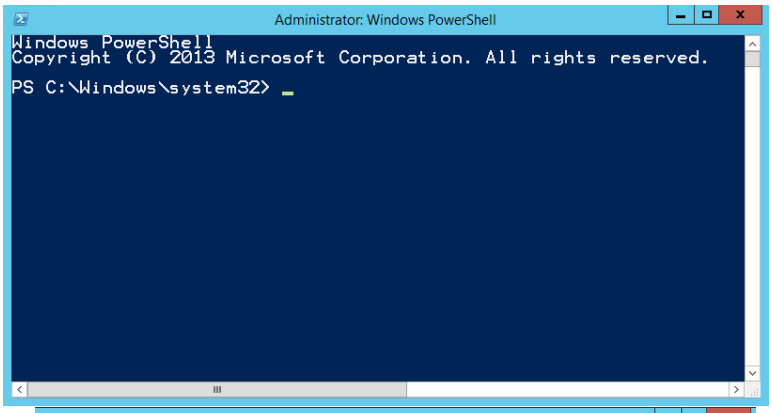


روش دوم اجرای PowerShell به این صورت است که وارد Search ویندوز خود شویم و کلمه‌ی PowerShell را وارد کنیم و درنتیجه جستجو بر روی Windows PowerShell کلیک راست کنید و گزینه‌ی Run as administrator را انتخاب کنید تا مانند قبل، از روی کاربر Administrator اجرا شود.

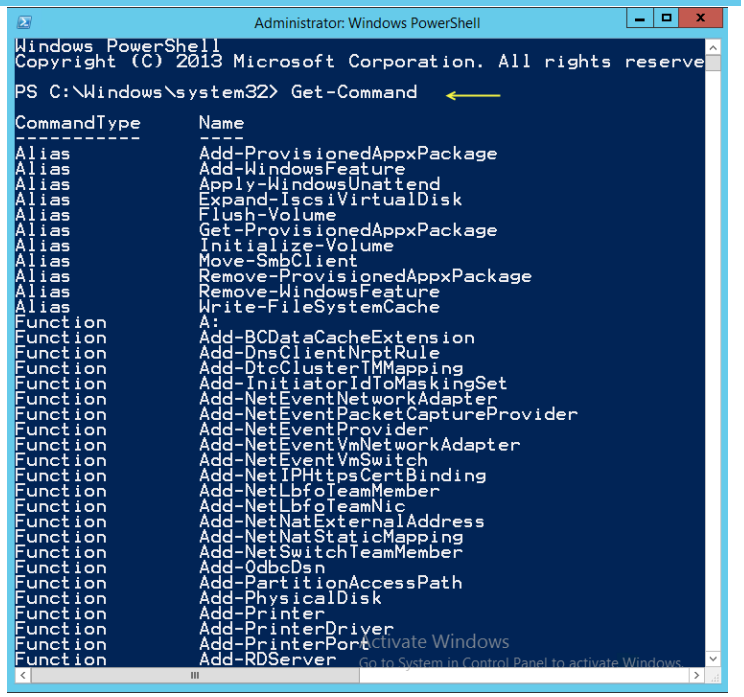


روش سوم به این صورت است که وارد Server Manager شویم و از منوی Tools گزینه‌ی Windows PowerShell را انتخاب کنیم.

توجه داشته باشید با این کار، سرویس PowerShell روی کاربری که وارد ویندوز شده است، اجرا می‌شود و نمی‌توانید روی کاربر Administrator اجرا کنید، مگر اینکه با کاربر Administrator وارد شوید.



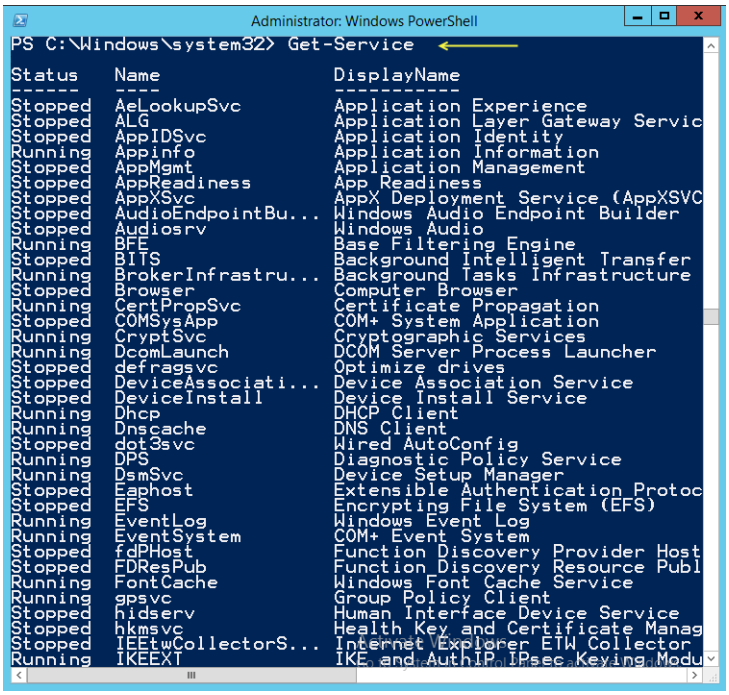
بعد از اجرای PowerShell با کاربر Administrator شکل مقابل را مشاهده خواهید کرد که کاملاً شبیه به CMD ویندوز است و رنگ پیش‌فرض آن آبی است.



نکته: دستوراتی که در PowerShell اجرا می‌شود به‌عنوان cmdlets شناخته می‌شوند.

در PowerShell ویندوز سرور 2012 چندین دستور cmdlets قرار دارد که برای مشخص کردن آن می‌توانید از دستور Get-Command استفاده کنید که این کار در شکل مقابل انجام‌شده است و تمام دستورات این بخش را نمایش داده است.

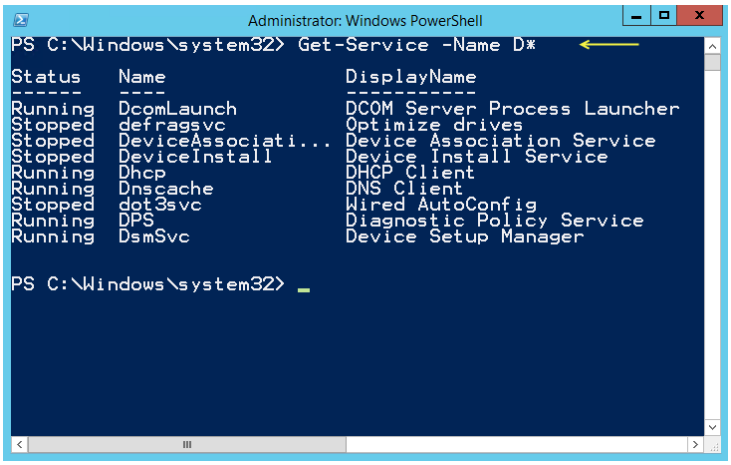
در ادامه کار با دستورات مختلف این بخش کارخواهیم کرد.



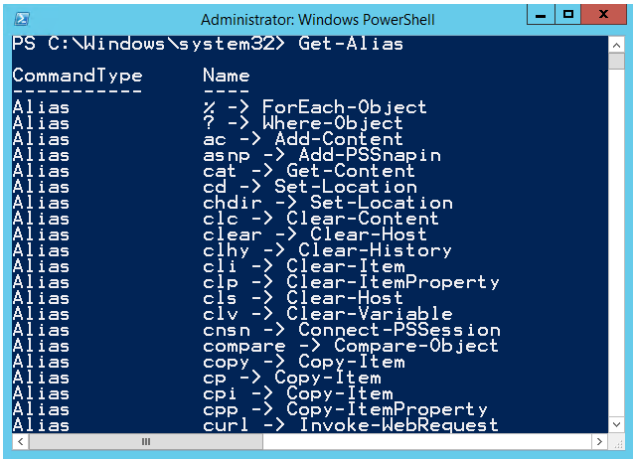
برای اینکه در PowerShell متوجه شویم که چه سرویس‌هایی در حال کار می‌باشند می‌توانیم از دستور Get-Service استفاده کنیم که این عمل را در شکل مقابل مشاهده می‌کنید.

شاید در این بخش بخواهید سرویس‌هایی بانام D را از بقیه‌ی سرویس‌ها جدا کنید؛ برای این کار از دستور زیر استفاده می‌کنیم.

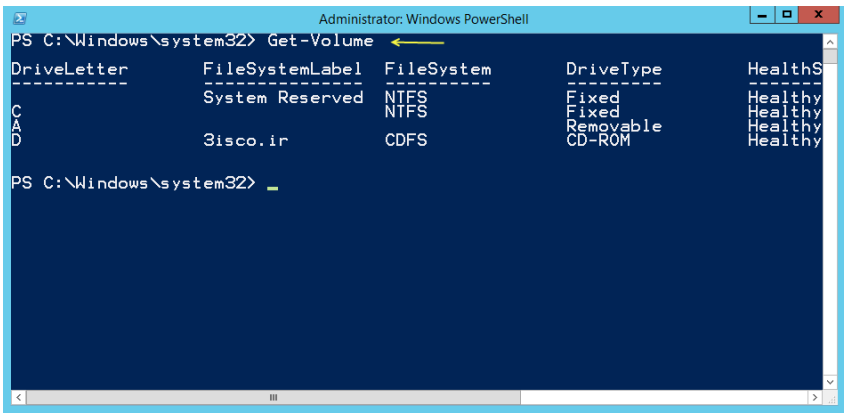
```
Get-Service -Name D*
```



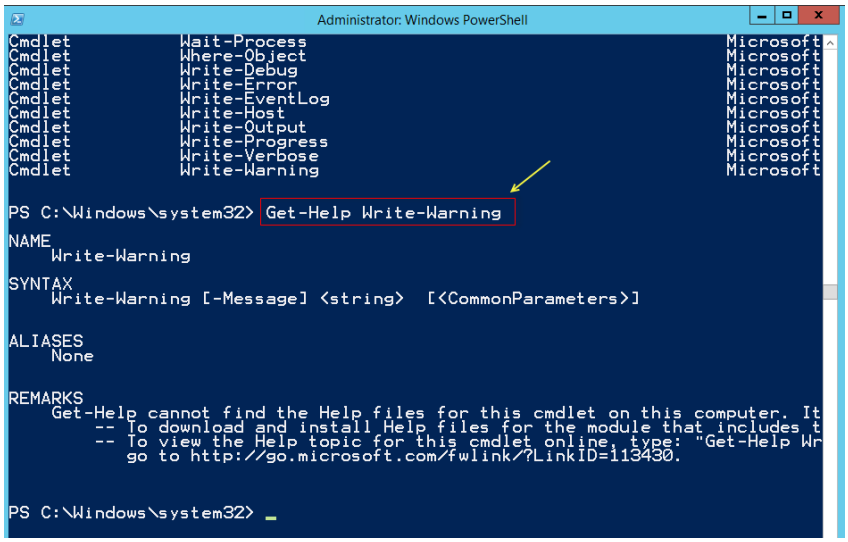
همان‌طور که در شکل مقابل مشاهده می‌کنید با واردکردن دستور Get-Service -Name D* لیست سرویس‌هایی که با حرف D در حال کار می‌باشند را برای ما لیست کرده است.



دستوری بانام Alias وجود دارد که با واردکردن Get-Alias می‌توانید لیست دستورات مخفف و کوتاه شده را مشاهده کنید، مثلاً به‌جای اینکه دستور Add-Content را وارد کنیم، از دستور کوتاه شده‌ی ac استفاده می‌کنیم.



با دستور Get-Volume می‌توانید لیست درایوهای خود را به‌مانند شکل مقابل مشاهده کنید.

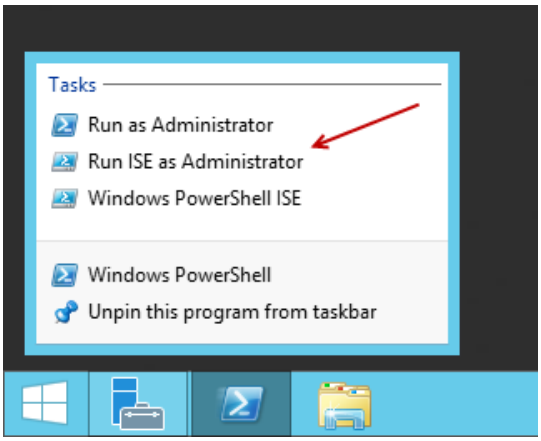


با استفاده از دستور Get-Help می‌توانیم متوجه شویم که چگونه از یک دستور داخل PowerShell استفاده کنیم، مثلاً با اجرای دستور Get-Command لیست دستورات مشخص می‌شود و بعدازآن می‌توانیم دستور موردنظر را به‌مانند شکل جلوی Get-Help وارد کنیم تا اطلاعات درباره‌ی آن مشخص شود و برای اینکه مثالی از دستور موردنظر را مشاهده کنید، در ادامه‌ی دستور بالا، دستور Examples– را اضافه کنید؛ یعنی به‌صورت زیر وارد کنید. Get-Help Write-Warning –Examples

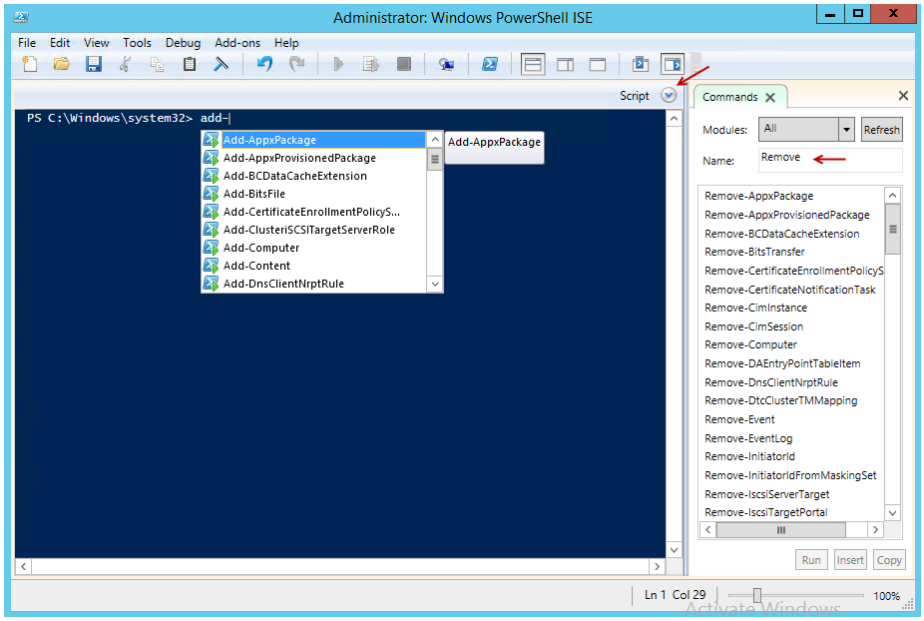
همان‌طور که گفتیم، دستور Write-Warning یکی از هزاران دستور Get-Command است که شما می‌توانید به‌جای آن، دستور دیگر را جایگزین کنید.

تذکر: زمانی که دستوری را در حال تایپ کردن هستید، می‌توانید با کلیک بر روی دکمه‌ی TAB دستور کامل آن را به‌صورت خودکار مشاهده کنید؛ مثلاً با واردکردن دستور Get-c و بعد فشردن کلید TAB می‌توانید دستور کامل آن، یعنی GET-Command را مشاهده کنید، یا با واردکردن دستور GET- و فشردن کلید TAB به‌دفعات متعدد می‌توانید، تمام دستورات بعد GET- را مشاهده کنید.

اگر با Visual Studio کارکرده باشید در زمان واردکردن دستورات لیست، دستورات به‌صورت منو برای شما باز می‌شود و کاربر به‌راحتی می‌تواند به‌جای نوشتن دستور کامل، دستور موردنظر را از منوی موردنظر انتخاب کند، در ویندوز سرور هم با ارائه‌ی سرویس Windows PowerShell ISE امکان‌پذیر شده است.



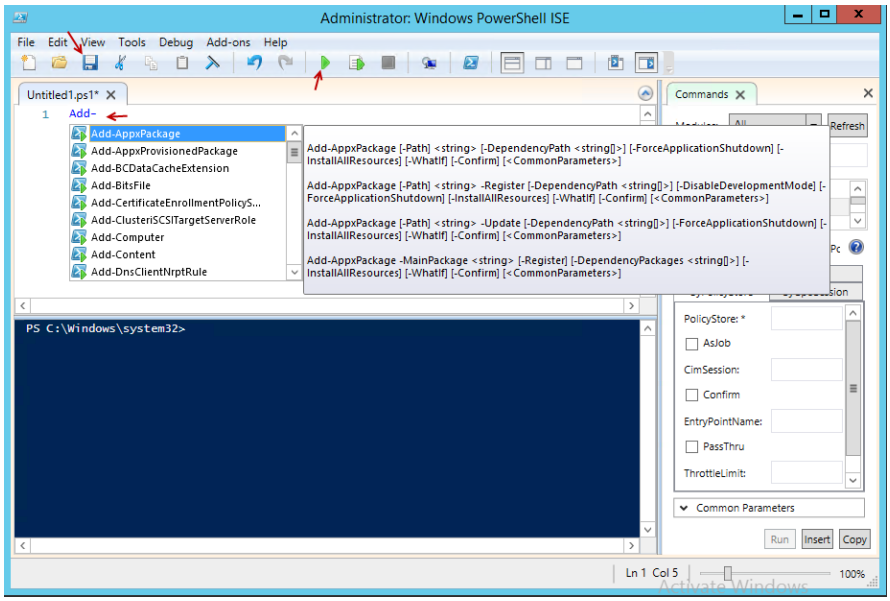
برای اجرای این سرویس بر روی Taskbar روی آیکون PowerShell کلیک راست کنید و گزینه‌ی Run ISE as Administrator را انتخاب کنید تا شکل بعد ظاهر شود.



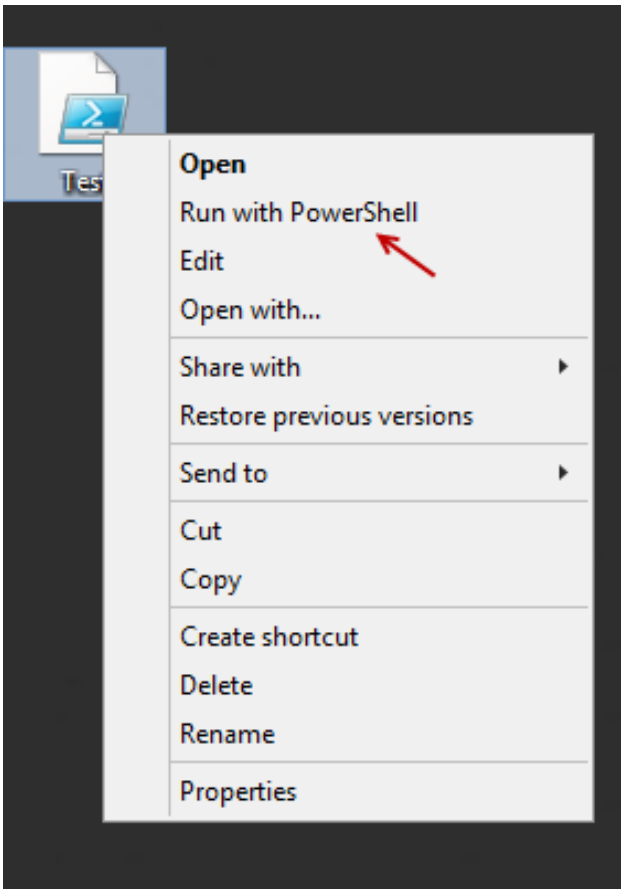
همان‌طور که در شکل مقابل مشاهده می‌کنید با واردکردن کلمه‌ی Add- تمام دستورات بعدازآن را به ما نمایش داده است که شما می‌توانید یکی از دستورات را انتخاب کنید.

در سمت راست و در قسمت Commands شما می‌توانید نام دستور موردنظر خود را در قسمت Name وارد کنید تا لیست دستورات موردنظر را مشاهده کنید. در این مثال، کلمه‌ی Remove واردشده است که لیست تمام دستوراتی که با Remove آغازشده است را مشخص کرده است. برای اینکه دستورات موردنظر را وارد خط فرمان کنید، روی دستور موردنظر درون لیست کلیک کنید و بعد از پائین صفحه و زیر دستور موردنظر، بر روی Insert کلیک کنید تا دستور موردنظر وارد صفحه شود.

یکی دیگر از راه‌های استفاده از دستورات PowerShell، این است که از Script استفاده کنیم؛ یعنی اینکه دستورات را داخل یک فایل قرار دهیم و از آن در موقع نیاز استفاده کنیم، برای این کار در شکل قبلی، بر روی آیکون Script که با فلش هم مشخص‌شده کلیک کنید تا شکل زیر ظاهر شود.



در این صفحه، قسمت Script فعال‌شده است و برای اینکه از این قسمت استفاده کنیم باید دستورات موردنظر را در قسمت مشخص‌شده وارد کنیم و برای اینکه از دستورات، خروجی تهیه کنیم باید بر روی آیکون Start کلیک کنیم و برای ایجاد فایل Script باید بر روی آیکون Save کلیک کنیم و فایل موردنظر را بانام مشخص، در جای مشخص ذخیره کنیم. همان‌طور که در شکل مقابل مشاهده می‌کنید، Script موردنظر بانام Test در جای مناسب ذخیره‌شده است و برای اجرای آن باید روی آن کلیک راست کنیم و گزینه‌ی Run with PowerShell را انتخاب کنیم تا فایل موردنظر اجرا شود.

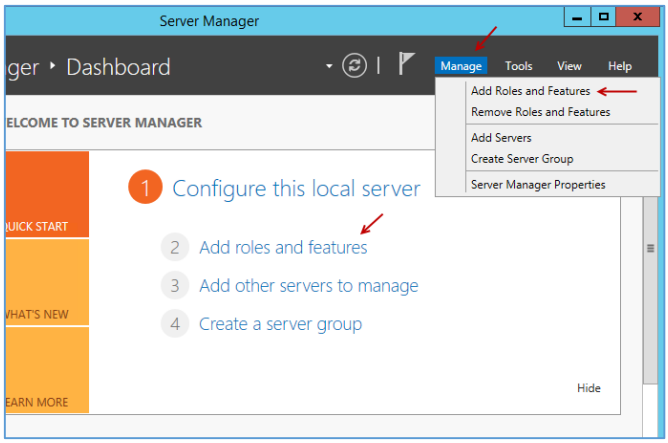


تذکر: این آموزش‌هایی را که باهم بررسی کردیم، فقط در حد معرفی سرویس‌ها است و برای استفاده از دستورات و Script های پیشرفته، در ادامه‌ی کتاب بر روی آن‌ها کارخواهیم کرد.

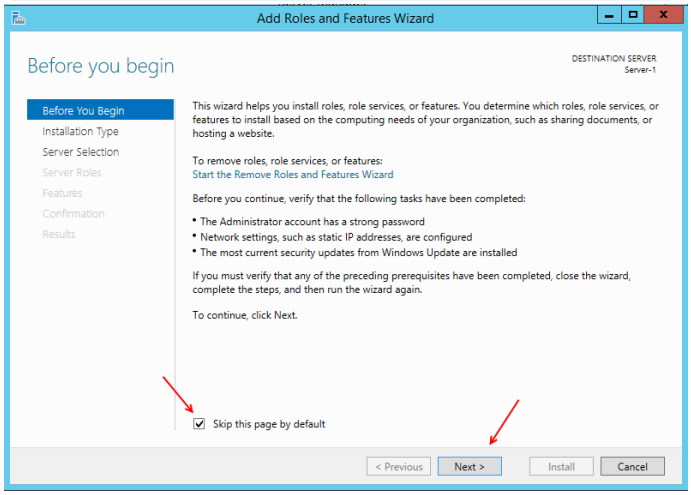
نصب و راه‌اندازی Active Directory 2012:

Active Directory، یک دایرکتوری فعال در ویندوز سرور شرکت مایکروسافت است که برای جمع‌آوری اطلاعات کاربران و گروه‌ها به کار می‌رود؛ اگر در یک سازمان از سرویس Active Directory استفاده نکنیم، مدیریت بر روی منابع کار بسیار سختی خواهد شد؛ مثلاً اگر 100 کاربر در سازمان خود داشته باشید باید این 100 کاربر را در تک‌تک دستگاه‌های موجود سازمان تعریف کنید تا کاربر موردنظر بتواند وارد سیستم شود ولی اگر از Active Directory استفاده کنیم، می‌توانیم این 100 کاربر را در سیستم Active وارد کنیم و بقیه‌ی کاربران از طریق آن به‌راحتی می‌توانند وارد سیستم شوند.

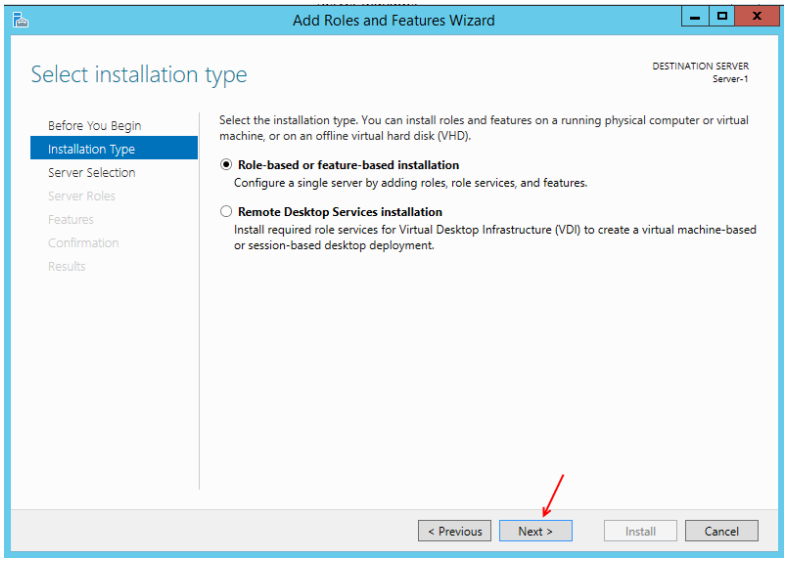
برای نصب Active Directory، نیاز به این داریم که IP Address را به‌صورت دستی و یا همان Static تعریف کنیم که این کار را در مراحل معرفی Server Manager انجام دادیم و IP با شماره‌ی 192.168.10.30 را به سرور معرفی کردیم. توجه داشته باشید که اگر از سرویس DHCP که در ادامه‌ی کتاب بر روی آن کارخواهیم کرد، روی سرور شما فعال است، باید IP را وارد کنید که در رنج، همان DHCP باشد.



برای شروع کار باید Server Manager را اجرا کنیم، به‌مانند شکل مقابل برای شروع کار باید بر روی Add roles and features کلیک کنیم که برای این کار می‌توانید از دو طریق اقدام کنیم.



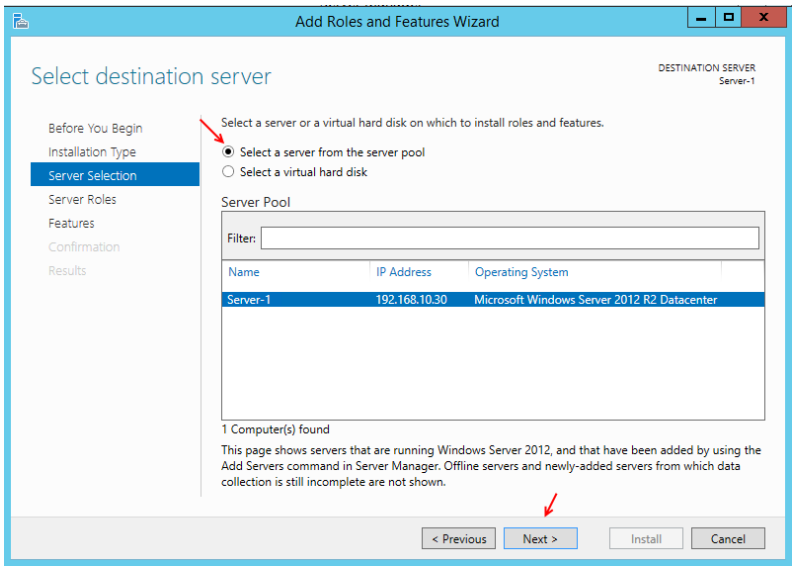
صفحه‌ی روبرو، مربوط به صفحه‌ی آغازین نصب Features است که برای شروع، گزینه Skip this پی‌جویی کردن by default را انتخاب کنید تا صفحه‌ی موردنظر در ورود بعدی اجرا نشود و به صفحه بعدی برود.



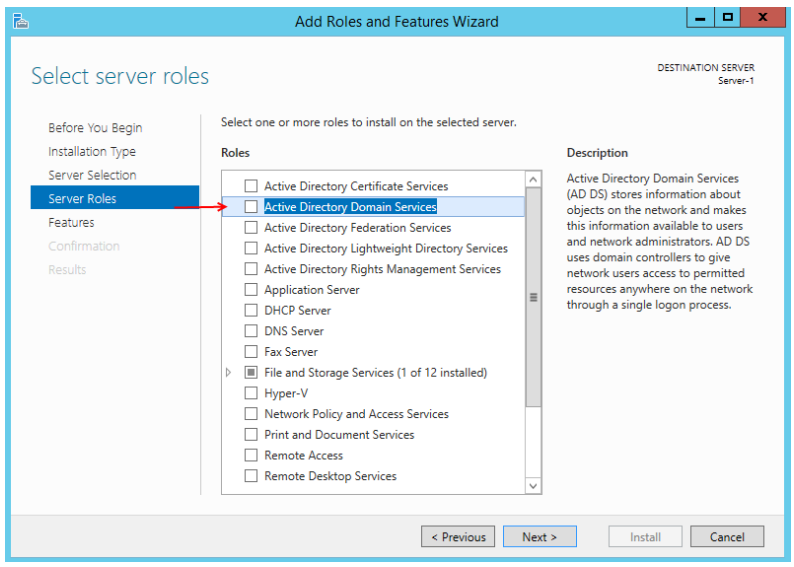
بر روی Next کلیک کنید.

در این صفحه، گزینه‌ی ....Role-based را انتخاب و بر روی Next کلیک کنید.

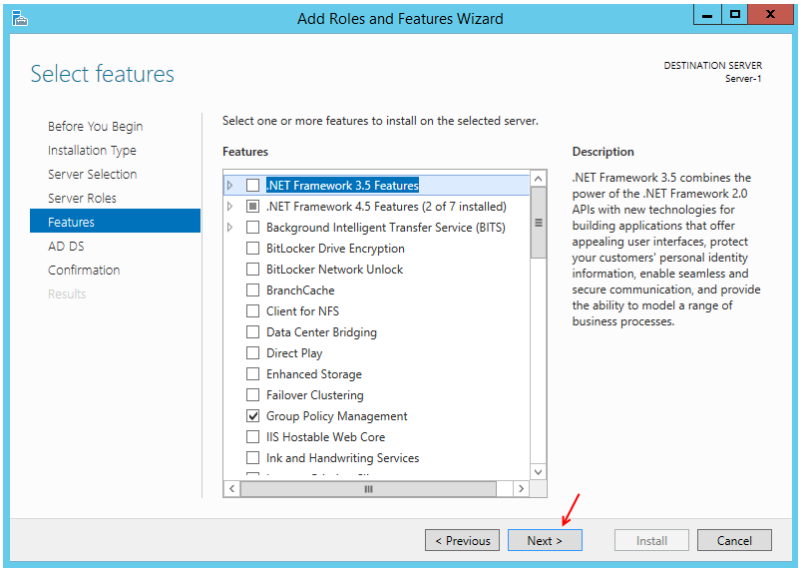
گزینه‌ی دوم برای ارتباط از راه دور به یک سرور دیگر است که در ادامه، روی آن بحث خواهیم کرد.



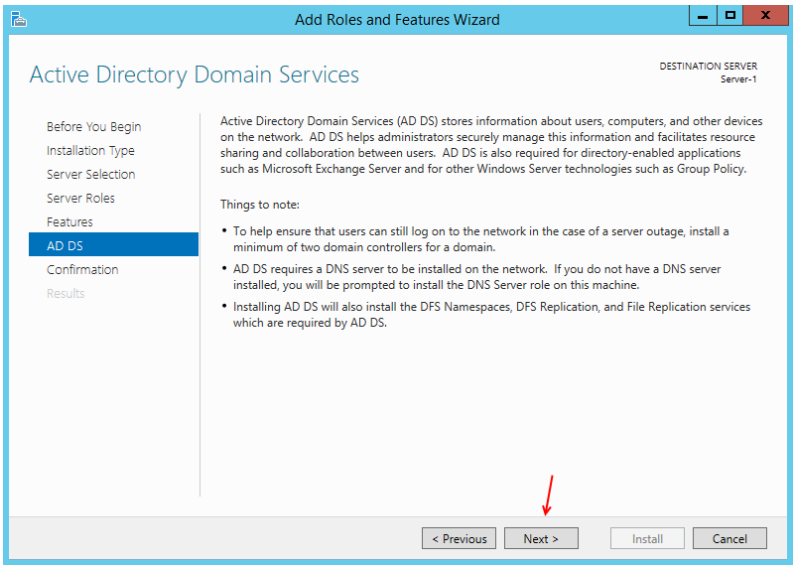
در این قسمت، برای اینکه Features و Role نصب شود، باید یک سرور و یا یک هارددیسک مجازی را انتخاب کنید که در این بخش گزینه‌ی Select a Server From the server pool را انتخاب می‌کنیم و بر روی Next کلیک کنید.



در این قسمت از لیست Roles گزینه‌ی Active Directory Domain Services را انتخاب کنید و در شکل ظاهرشده، بر روی Add Features کلیک کنید و بعد بر Next کلیک کنید.

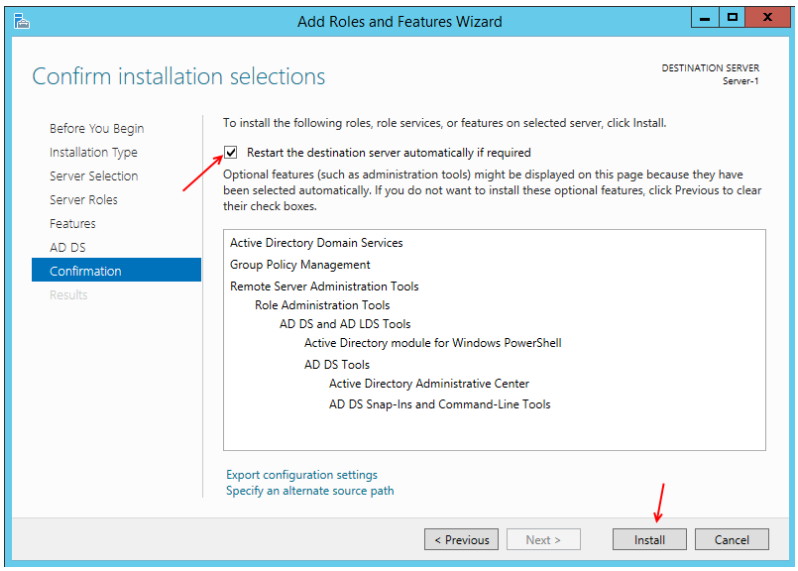


این قسمت مربوط به Features است، نباید به گزینه‌ای دست بزنید و تنها بر روی Next کلیک کنید.

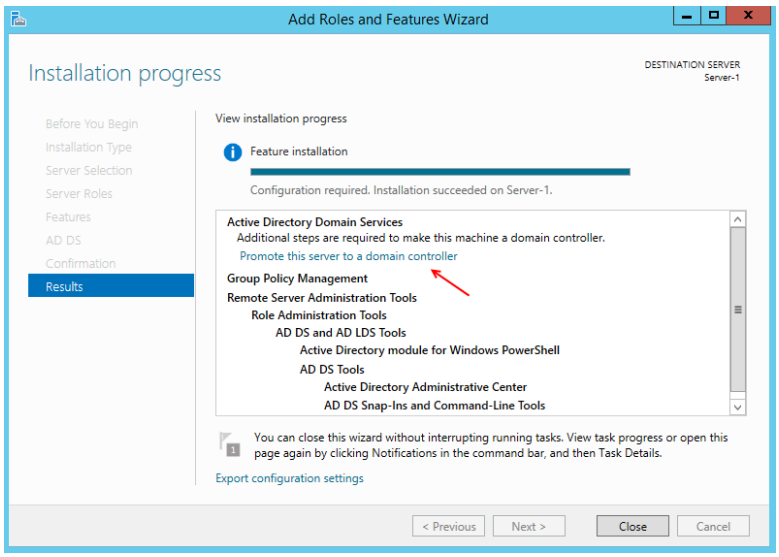


این صفحه در مورد راه‌اندازی Domain Controllers بحث می‌کند که در ادامه‌ی کار به آن خواهیم پرداخت.

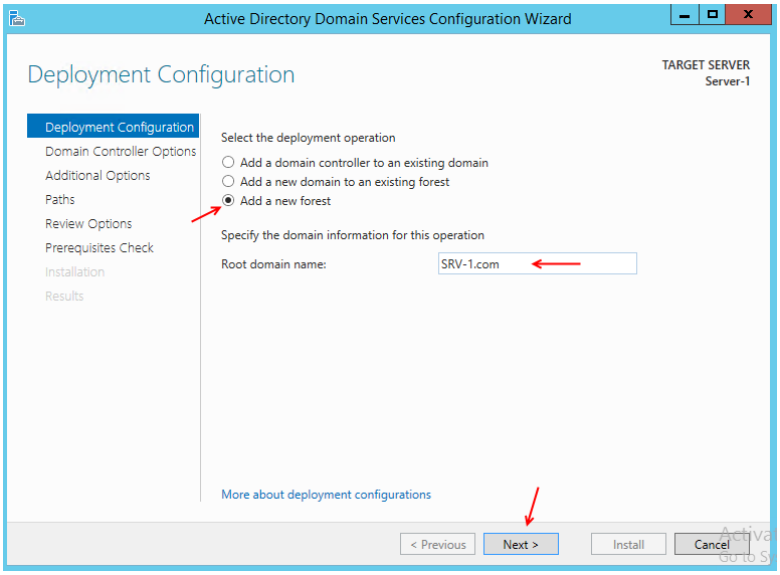
بر روی Next کلیک کنید.



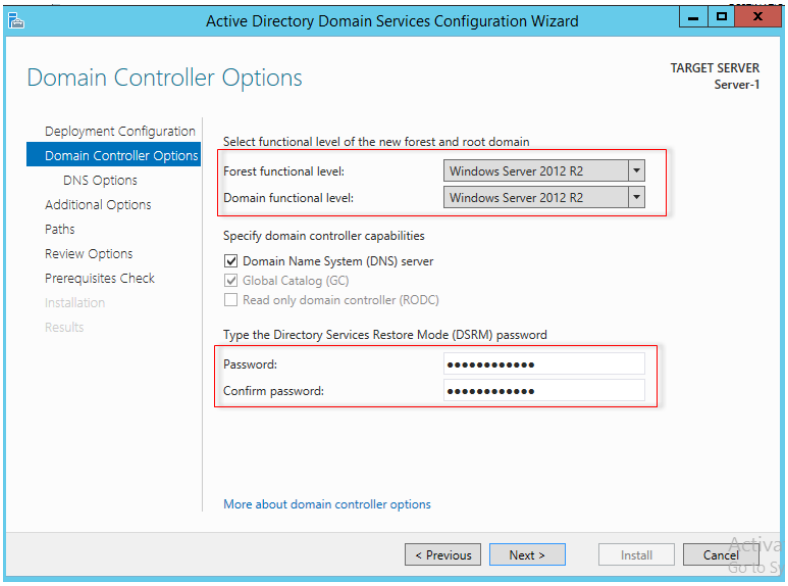
در این قسمت، گزینه‌ی .... Restart the را انتخاب کنید و در شکل ظاهرشده بر روی Yes کلیک کنید و بعد بر روی Install کلیک کنید.



در این صفحه، سرویس Active Directory به‌صورت کامل نصب‌شده است و بعدازآن اعلام می‌دارد که Domain Controllers هم باید بعد از تعریف Active Directory فعال شود؛ برای همین باید بر روی Promote this server to a domain واپایشگر کلیک کنید تا شکل بعد ظاهر شود.

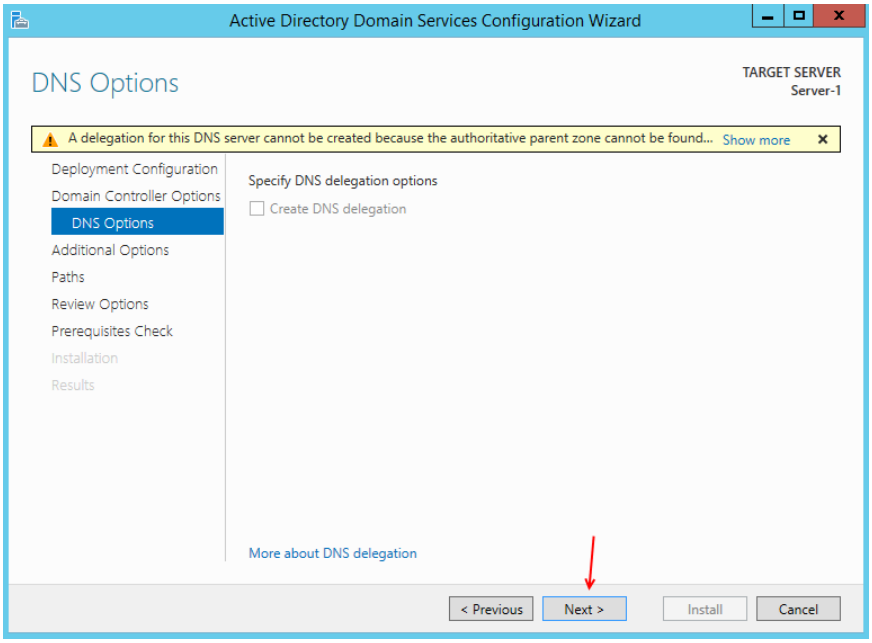


در این قسمت، گزینه‌های مختلفی وجود دارد که هرکدام از آن‌ها را در وقت خویش بررسی خواهیم کرد، فعلاً برای اینکه یک Domain Controller جدید ایجاد کنیم گزینه‌ی Add a New Forest را انتخاب می‌کنیم و در قسمت Root Domain Name نام دومین خود را که در اینجا Srv-1.com است را وارد می‌کنیم و بر روی Next کلیک می‌کنیم.

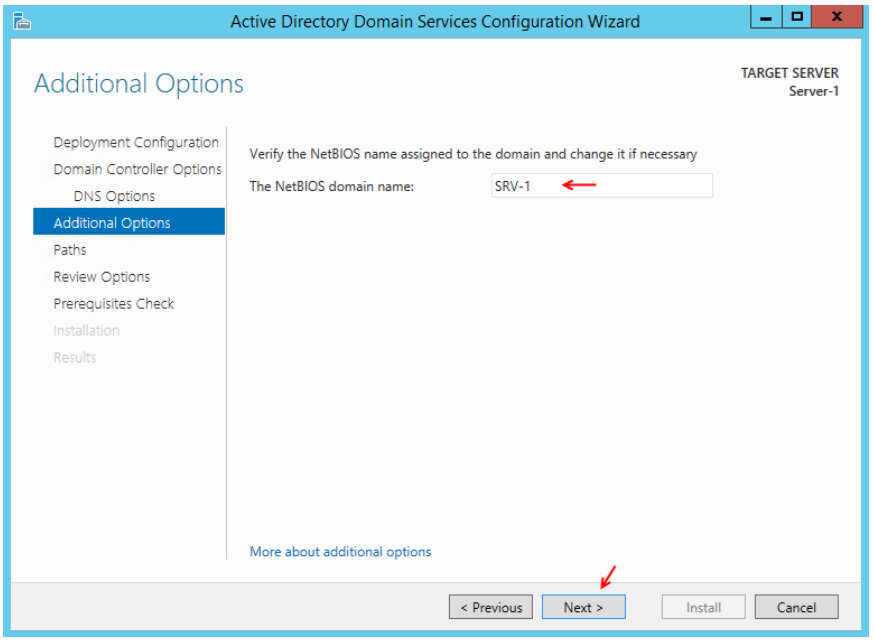


در این صفحه، در قسمت اول باید ویندوز سرورهایی را انتخاب کنیم که می‌خواهیم به سرور اصلی ما Join شوند که در این کتاب تمام سرورهایی که می‌خواهیم به این سرور متصل شوند از نوع ویندوز سرور 2012 است. در قسمت دوم باید رمز عبور را برای DSRM وارد کنیم، این رمز عبور زمانی به کار می‌رود که بخواهیم Domain Controller خود را

Recovery کنیم که این قسمت را در همین کتاب بررسی خواهیم کرد، فقط رمز عبوری را که برای این قسمت در نظر می‌گیریم، باید به‌صورت پیچیده وارد کنیم، مانند Test@123456789. بعد از انجام کارهای بالا بر روی Next کلیک کنید.

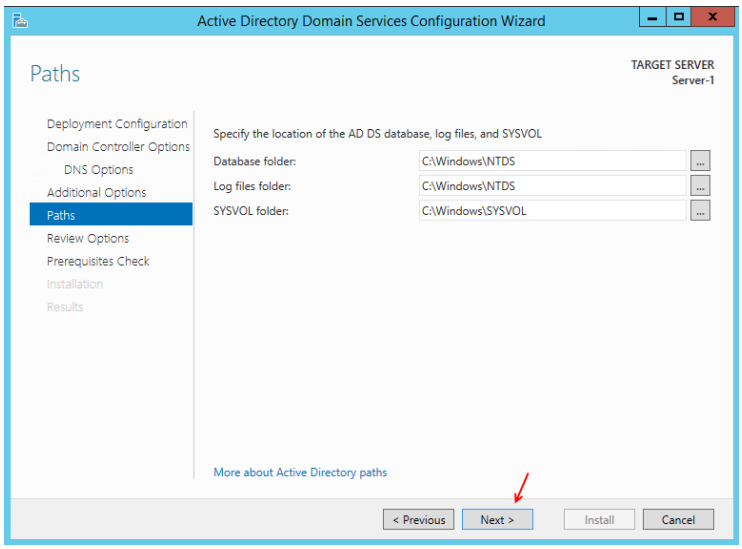


در این قسمت، به ما اعلام می‌کند که برای راه‌اندازی Domain Controller احتیاج به سرویس DNS است که این سرویس به‌صورت خودکار بعد از نصب Domain Controller نصب خواهد شد. بر روی Next کلیک کنید.



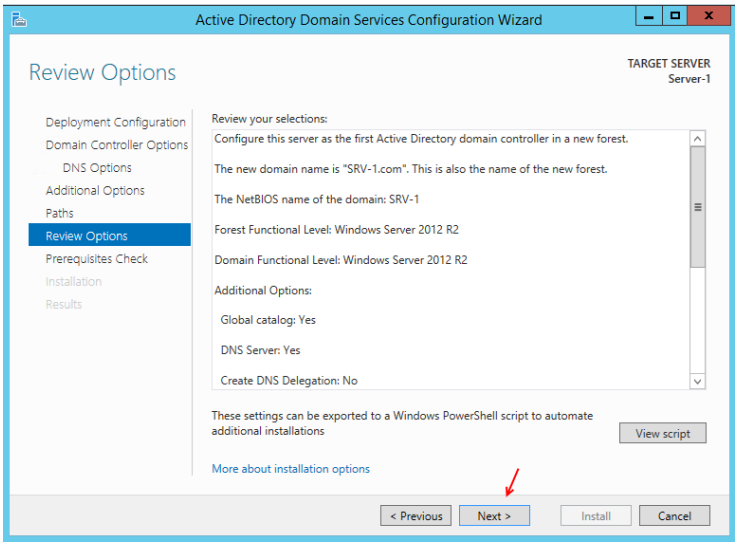
در این قسمت، نام Domain شما جستجو می‌شود که اگر این نام از قبل وجود داشته باشد به شما Error خواهد داد و یا نام موردنظر شمارا به‌صورت خودکار تغییر می‌دهد، توجه داشته باشید اگر دومینی مانند cisco.com تعریف کنید و به اینترنت متصل باشید، به‌هیچ‌وجه نمی‌توانید از آن استفاده کنید.

در این قسمت، نام دومین SRV-1.com جستجو شده و بدون هیچ مشکلی تأییدشده است. برای ادامه کار بر روی Next کلیک کنید.

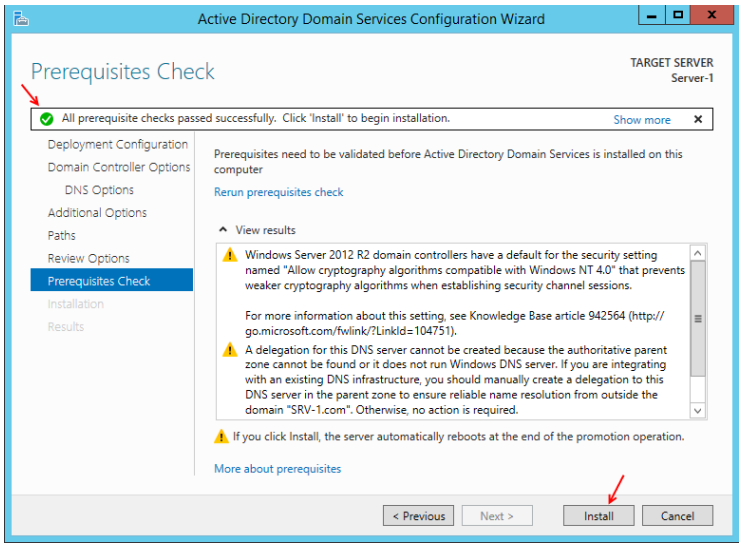


این صفحه، مربوط به آدرس ذخیره سازی فایل‌های مربوط به Domain می‌باشد که باید آدرس پوشه-های Database, Log, SYSVOL را مشخص کنید.

بر روی پیش فرض قرار دهید و بر روی Next کلیک کنید.



در این قسمت، اطلاعات کامل از مراحل کار به شما نشان داده می‌شود که اگر با اطلاعات وارد شده، مشکلی ندارید بر روی Next کلیک کنید.

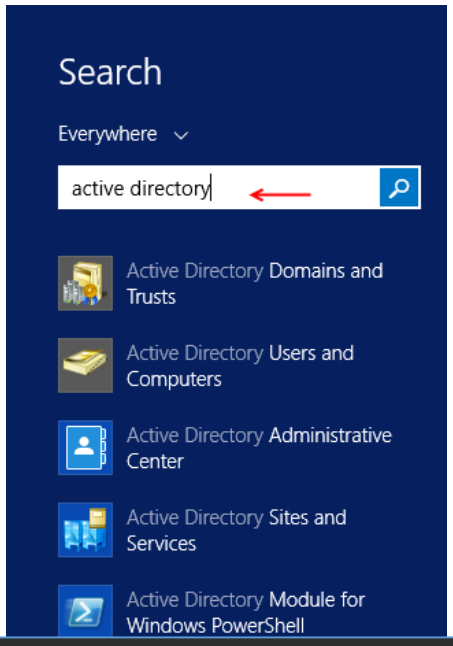


در این صفحه، پیش‌نیاز های نصب بررسی می‌شود و اگر مشکلی نداشت به شما اجازه کار را می‌دهد.

توجه داشته باشید که اگر IP را به صورت Static وارد نکنید به شما خطا خواهد داد.

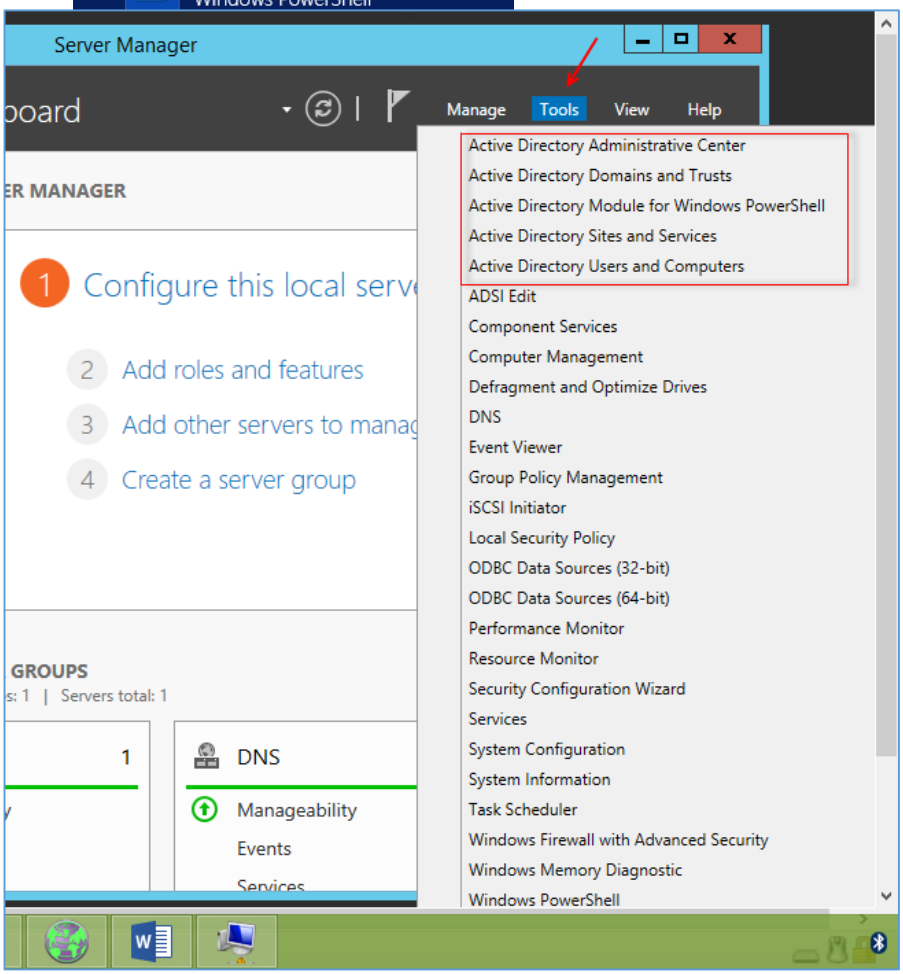
بر روی Install کلیک کنید تا نصب Domain Controller آغاز شود.

بعد از نصب کامل Active Directory به همراه Domain Controller، روش‌های متفاوتی برای دسترسی به اجرای آن وجود دارد که با هم آن‌ها را بررسی می‌کنیم.



سریع‌ترین روش برای دسترسی به اجزای Active Directory، مراجعه به منوی Start می‌باشد. زمانی که وارد منوی Start شدید، می‌توانید با وارد کردن Active Directory به تمام اجزای Active Directory دسترسی داشته باشید، البته کلمات کوتاه تر هم جواب خواهد داد.

همان‌طور که در شکل مقابل مشاهده می‌کنید، اجزای کامل Active Directory مشخص‌شده است که در خلال این کتاب همه آن‌ها را بررسی خواهیم کرد.



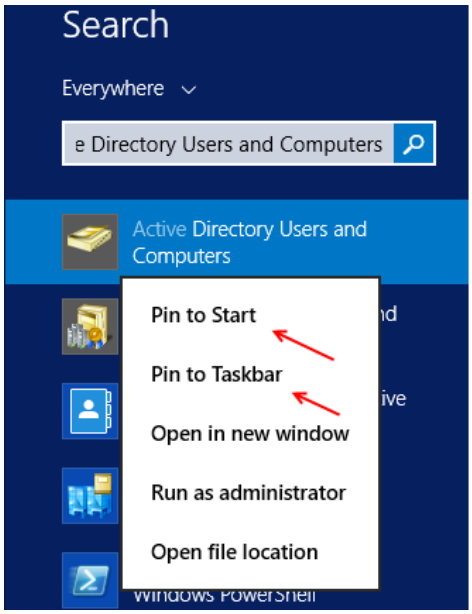
روش دوم، دسترسی به اجزای Active Directory، مراجعه به Server Manager می‌باشد. شکل مقابل مربوط به Server Manager است که با مراجعه به منوی Tools می‌توانید همه ی اجزای Active Directory را مشاهده کنید.

روش های دیگری برای اجرا وجود دارد که زیاد به آن‌ها نیاز نیست.

ادامه کار را با هم بررسی می‌کنیم.

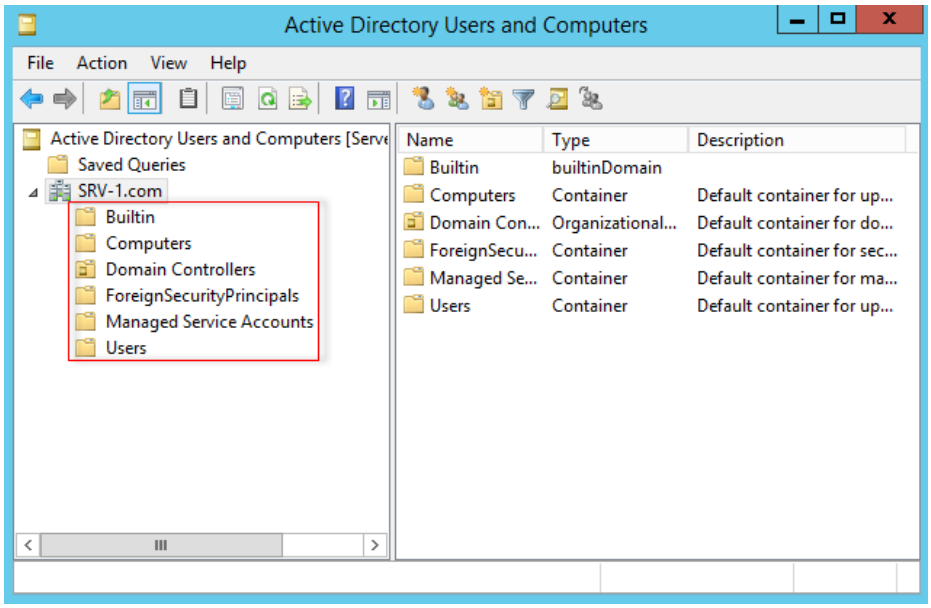
کار با سرویس Active Directory Users And Computers:

این سرویس، یکی از پرکاربردترین سرویس مجموعه ی Active Directory است که برای ایجاد و مدیریت گروه ها، کاربران، مجموعه ی سازمانی و ..... به کار می‌رود که در این قسمت این سرویس را به صورت کامل بررسی خواهیم کرد.

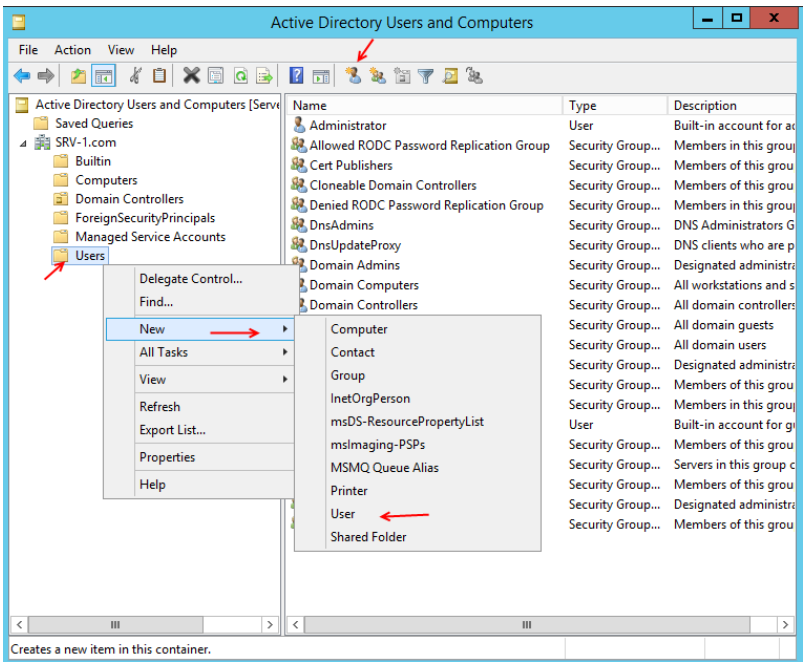


برای اجرای این سرویس، وارد Start می‌شویم و در Search کلمه ی Active ویا Active Directory را وارد می‌کنیم و در لیست موردنظر بر روی Active Directory Users and Computers کلیک راست می‌کنیم تا منوی مقابل باز شود. برای اینکه این سرویس را در Start خود داشته باشید بر روی Pin to start کلیک کنید و اگر می‌خواهید در Taskbar خود داشته باشید، بر روی Pin to Taskbar کلیک کنید.

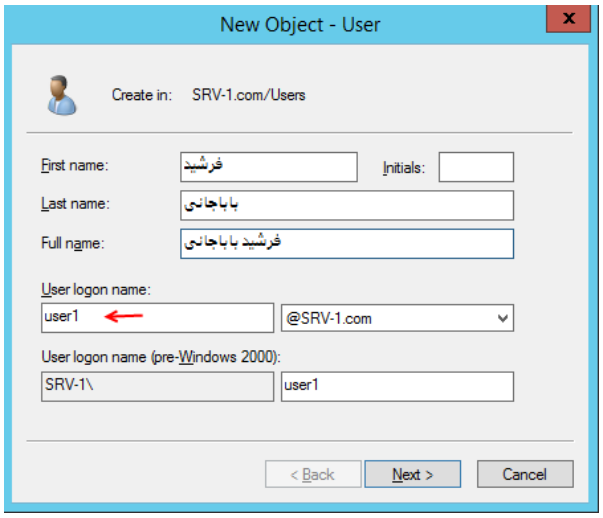
بعد از انجام کارهای بالا، سرویس موردنظر را اجرا می‌کنیم.



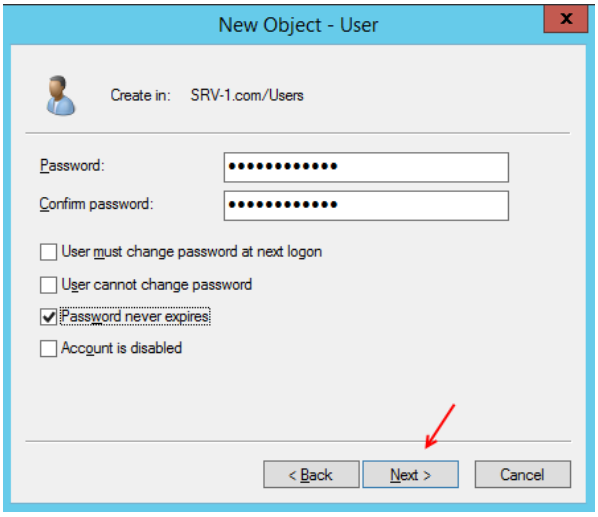
همان‌طور که در شکل مقابل مشاهده می‌کنید، سرویس موردنظر اجرا شده است. از سمت چپ، بر روی فلش کنار نام سرور خود کلیک کنید تا اطلاعات موردنظر را مشاهده کنید. همه ی این گزینه‌ها را در ادامه بررسی خواهیم کرد؛ در حال حاضر بر روی Users کلیک کنید تا شکل بعد را مشاهده کنید.



در این قسمت، می‌توانیم کاربران، گروه‌های سازمانی و داخلی ایجاد کنیم که برای شروع، یک کاربر را با هم ایجاد می‌کنیم و تنظیمات مربوط به آن را مورد بررسی قرار می‌دهیم، برای این کار به مانند شکل، از سمت چپ بر روی Users کلیک راست می‌کنیم و از قسمت New گزینه ی User را انتخاب می‌کنیم و یا می‌توانیم، از نوار ابزار بالا بر روی آیکون New User کلیک کنید تا شکل بعد ظاهر شود.



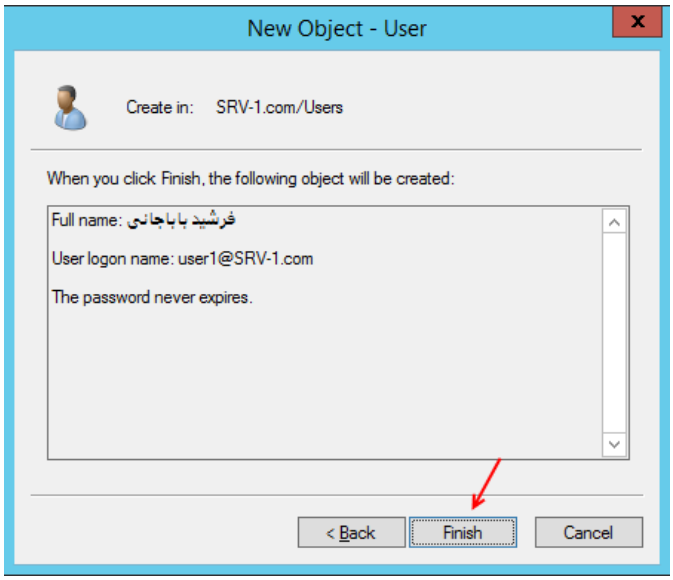
در این صفحه، در قسمت First Name نام کاربر خود را وارد کنید. در قسمت Last name نام فامیل و یا نام دوم را وارد کنید؛ توجه داشته باشید که می‌توانید هم به زبان فارسی و هم به انگلیسی بنویسید. در قسمت User logon name که مهم‌ترین بخش می‌باشد، باید نام کاربری را که برای ورود، مورد احتیاج می‌باشد را وارد کنید که در این قسمت user1 وارد کردیم؛ به کوچکی و بزرگی حروف توجه کنید. بر روی Next کلیک کنید.



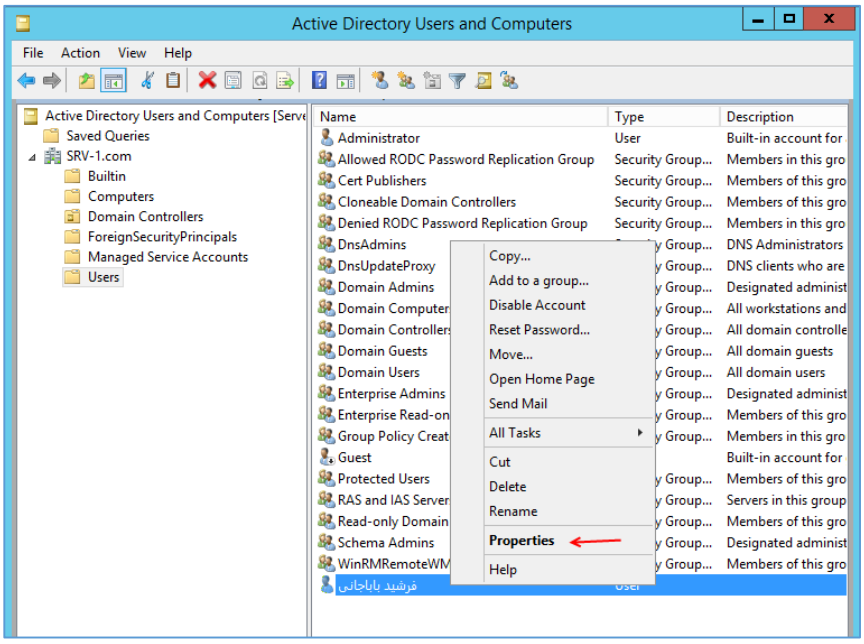
در این قسمت، باید رمز عبور برای کاربر خود در نظر بگیرید؛ توجه کنید که این رمز، باید به صورت پیچیده وارد شود؛ یعنی ترکیبی از حروف، اعداد و علائم مانند Test@123456 باشد. 4 گزینه در زیر آن مشاهده می‌کنید که گزینه ی اول، برای این منظور به کار می‌رود که کاربر موردنظر بعد از ورود به ویندوز، باید رمز عبور را تغییر دهد. گزینه ی دوم، این توانایی را به مدیر شبکه می‌دهد تا از تغییر رمز عبور توسط کاربر جلوگیری کند.

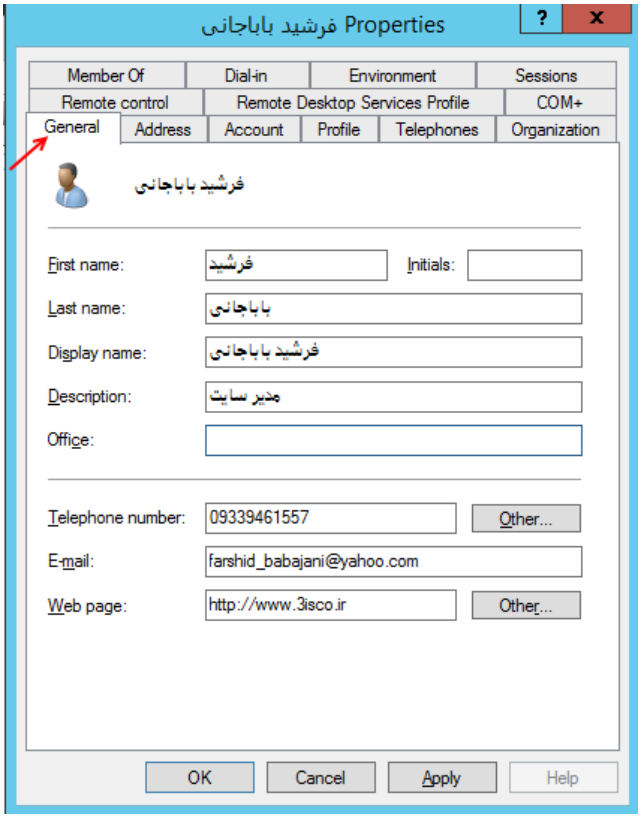
گزینه ی سوم را اگر انتخاب کنید، این رمز عبور به هیچ عنوان انقضاء نمی‌شود، درباره ی این موضوعات، در قسمت Group Policy بحث خواهیم کرد. اگر گزینه ی Account is disabled فعال باشد کاربر موردنظر غیرفعال خواهد شد و امکان ورود به ویندوز را نخواهد داشت. در حال حاضر گزینه ی Password Never Expires را انتخاب و برروی Next کلیک کنید.

در این قسمت، اطلاعات وارد شده را مشاهده می‌کنید که برای ایجاد کاربر موردنظر، باید بر روی Finish کلیک کنید.



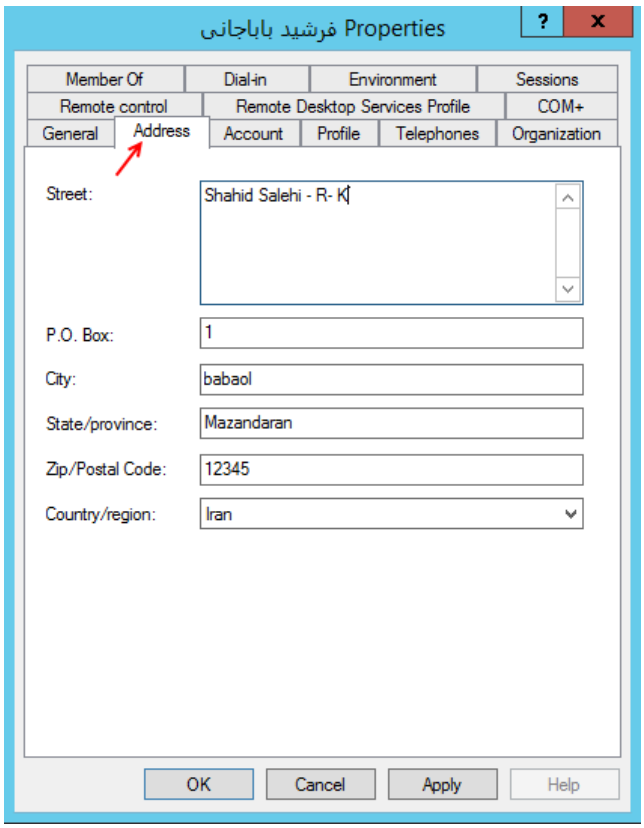
بعد از ایجاد کاربر به مانند شکل مقابل، بر روی آن کلیک راست کنید و گزینه ی Properties را انتخاب کنید تا شکل صفحه ی بعد ظاهر شود.





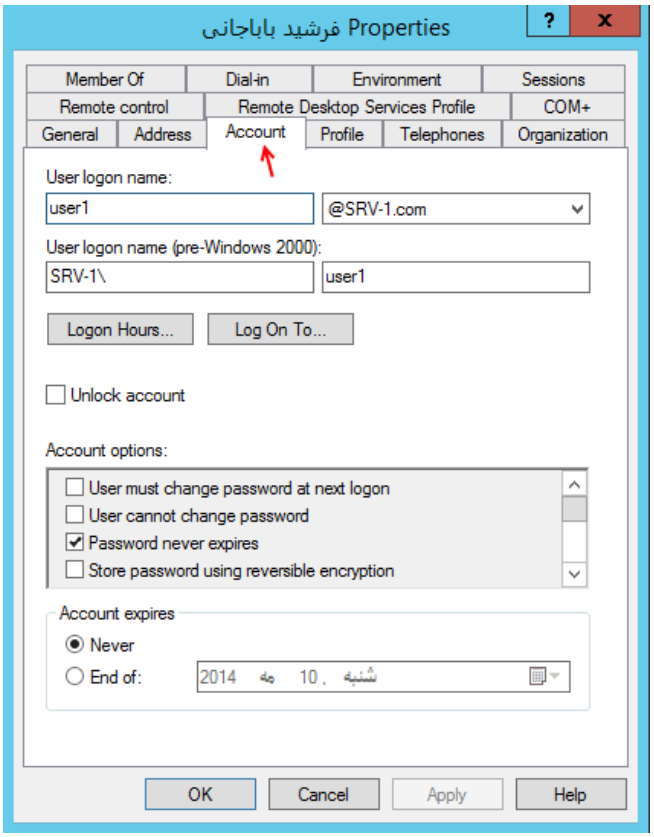
در این صفحه و در تب General، اطلاعاتی را در مورد کاربر موردنظر مانند آدرس ایمیل، سایت و شماره ی تلفن و توضیحات مربوط به آن را مشاهده کنید و یا تکمیل کنید.

بر روی تب Address کلیک کنید و به صفحه ی بعد توجه کنید.

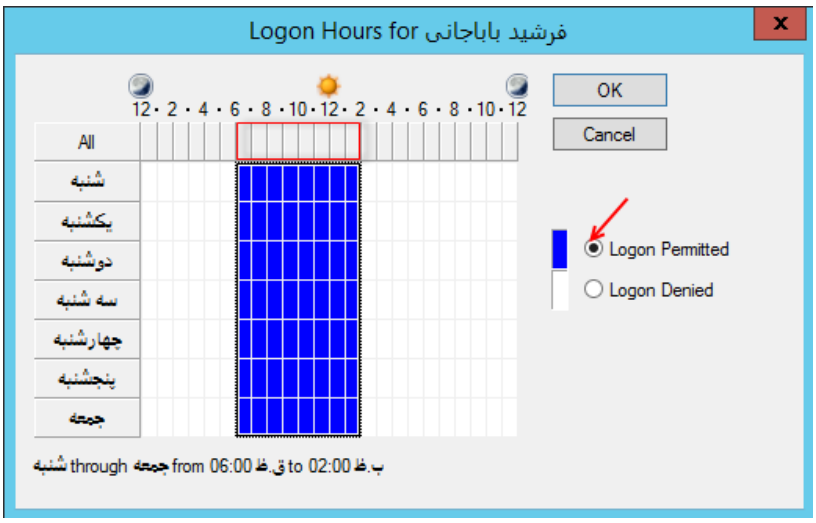


در تب Address، می‌توانید مشخصات محل سکونت را به صورت کامل، به مانند شکل روبرو وارد کنید.

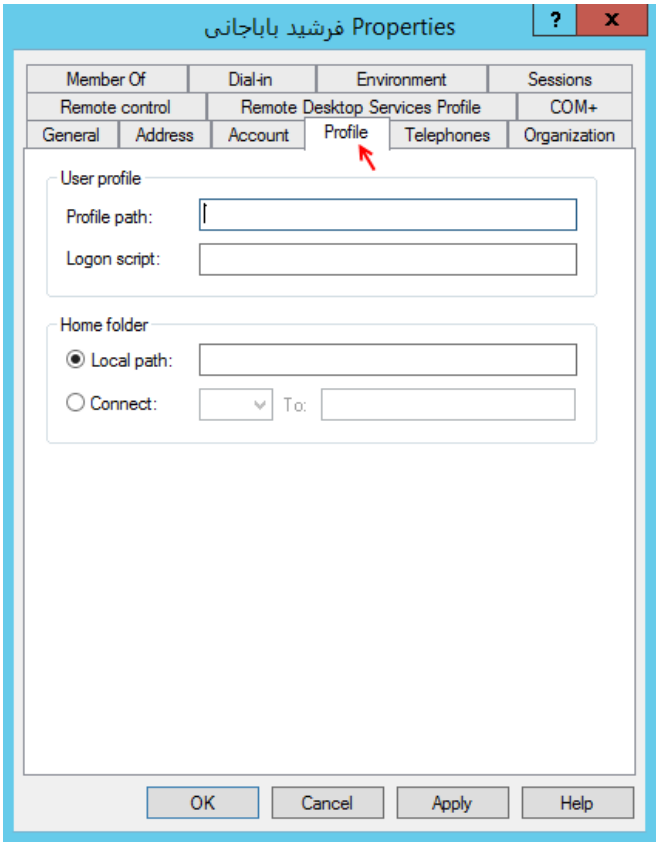
بر روی تب Account کلیک کنید و به شکل بعد توجه کنید.



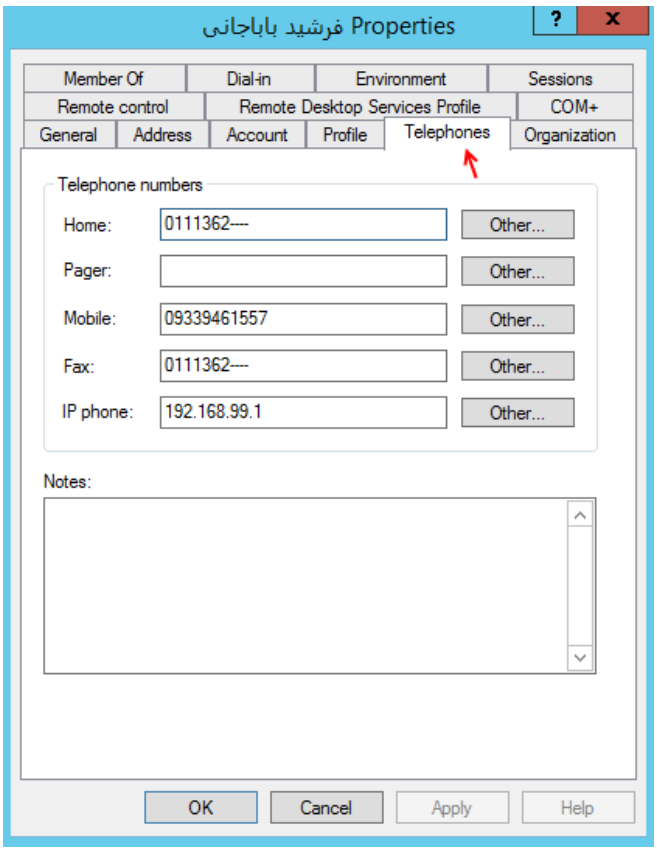
در تب Account، می‌توانید نام کاربری و تنظیمات آن را تغییر دهید؛ برای این کار در قسمت User logon name می‌توانید نام کاربری را تغییر دهید. همان‌طور که گفتیم این نام برای ورود به ویندوز است. در قسمت Account Options گزینه هایی را که قبلاً در قسمت *ایجاد کاربر*، آن‌ها را بررسی کردیم، در این قسمت هم مشاهده می‌کنید. البته گزینه های جدیدتر هم در این قسمت وجود دارد که برای رمز نگاری و امنیت می‌باشد که در وقت مناسب به آن خواهیم پرداخت. شما می‌توانید برای کاربران خود زمان ورود به ویندوز را مشخص کنید؛ برای این کار بر روی Logon Hours کلیک کنید تا شکل زیر ظاهر شود.



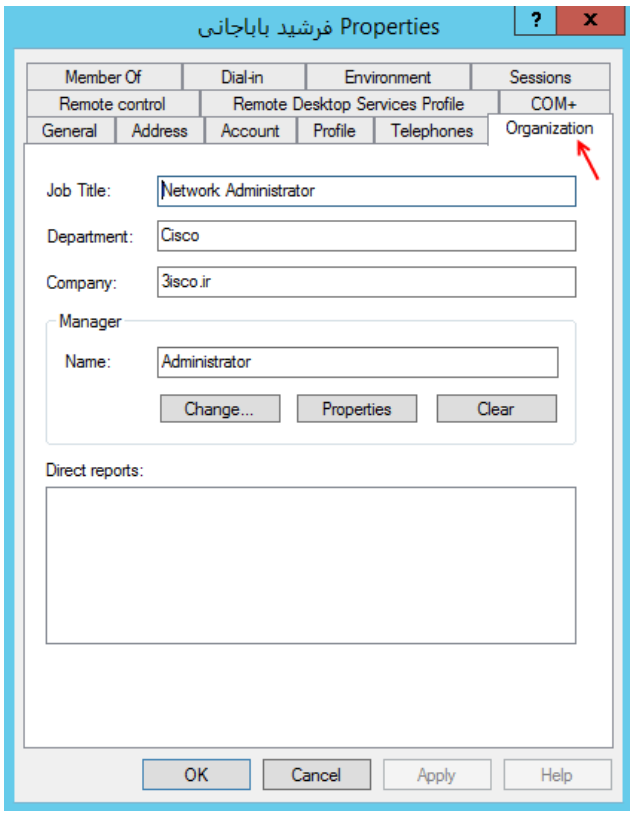
در این صفحه، می‌توانید به کاربر موردنظر اجازه ی ورود در ساعت مشخص‌شده را بدهید؛ برای این کار، ابتدا کل روزهای هفته را انتخاب و بر روی Logon Denied کلیک کنید تا رنگ آن به سفید تغییر کند؛ این گزینه یعنی اینکه کاربر موردنظر نمی‌تواند وارد ویندوز شود. بعد از آن، برای اینکه به کاربر موردنظر خود اجازه ی ورود دهید، ساعت مشخص‌شده را به مانند شکل، انتخاب و بر روی Logon Permitted کلیک کنید؛ توجه داشته باشید که به کاربر خود، می‌توانید اجازه ی ورود در روز و زمان مشخص هم بدهید، اگر به پائین شکل توجه کنید، مشخص‌شده است که به کاربر موردنظر از روزهای شنبه تا جمعه و از ساعت 0600 تا 0200 اجازه ی ورود به ویندوز داده شده است. بر روی ok کلیک کنید. گزینه ای دیگر با نام Log On To وجود دارد که می‌توانید مشخص کنید که کاربر موردنظر از طریق چه سیستمی، توانایی ورود داشته باشد.



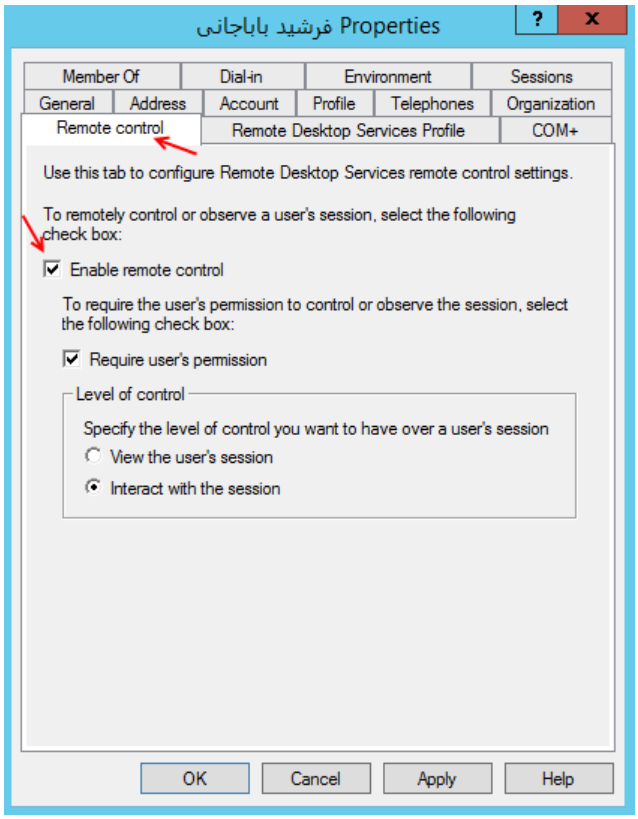
برای ادامه کار بر روی تبProfile کلیک کنید تا شکل روبرو ظاهر شود. تب Profile یکی از سودمندترین و پرکاربردترین تب‌ها می‌باشد. در این تب، شما می‌توانید برای تمام کاربران خود در قسمت User Profile یک محل مناسب برای Profile آن‌ها ایجاد کنید؛ یعنی Profile تمام کاربران در آدرسی درون سرور اصلی ایجاد شود و در قسمت Home Folder هم می‌توانید برای کاربران خود یک درایو مجازی ایجاد کنید که تمام اطلاعات خود را درون همان درایو قرار دهند؛ این درایو، پوشه‌ای درون سرور اصلی می‌باشد که برای بقیه ی کاربران Share شده است. توجه داشته باشید در درس‌های بعد کاملاً به این موضوع خواهیم پرداخت.



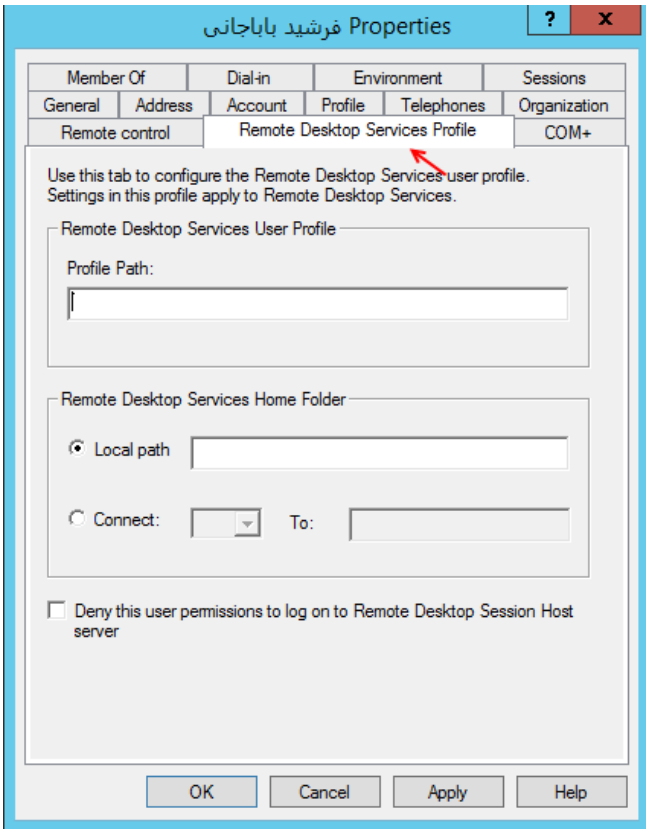
در تب Telephones، اطلاعات تماس کاربر موردنظر را می‌توانید وارد یا مشاهده کنید.



در تب Organization یا واحد سازمانی، می‌توانید نوع کار، واحد کاری، نام شرکت و مدیر کاربر موردنظر را مشخص کنید.

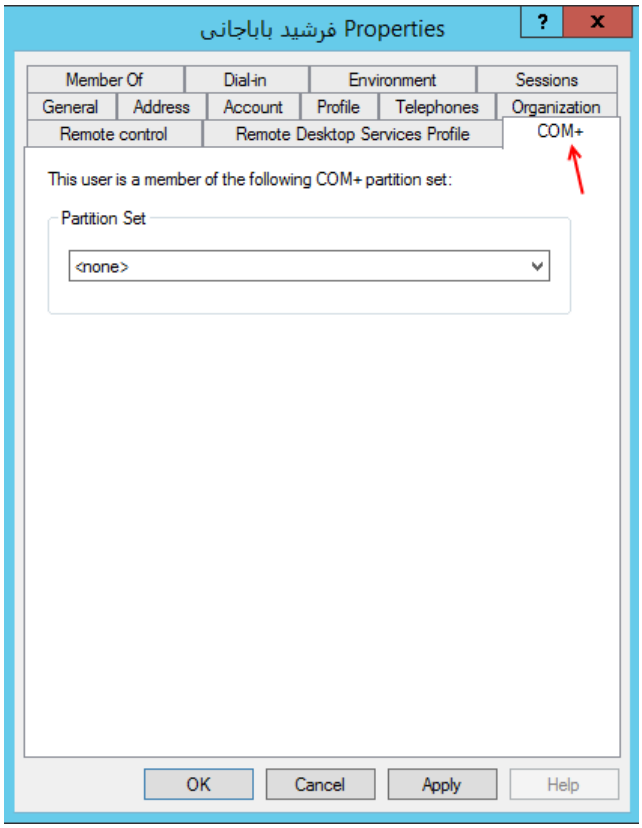


در تب Remote Control، می‌توانیم به کاربر موردنظر این اجازه را بدهیم که در شبکه ی موردنظر توانایی Remote یا ارتباط از راه دور به سیستم دیگر را داشته باشد. این موضوعات در ادامه ی کتاب به صورت کامل بررسی خواهد شد.

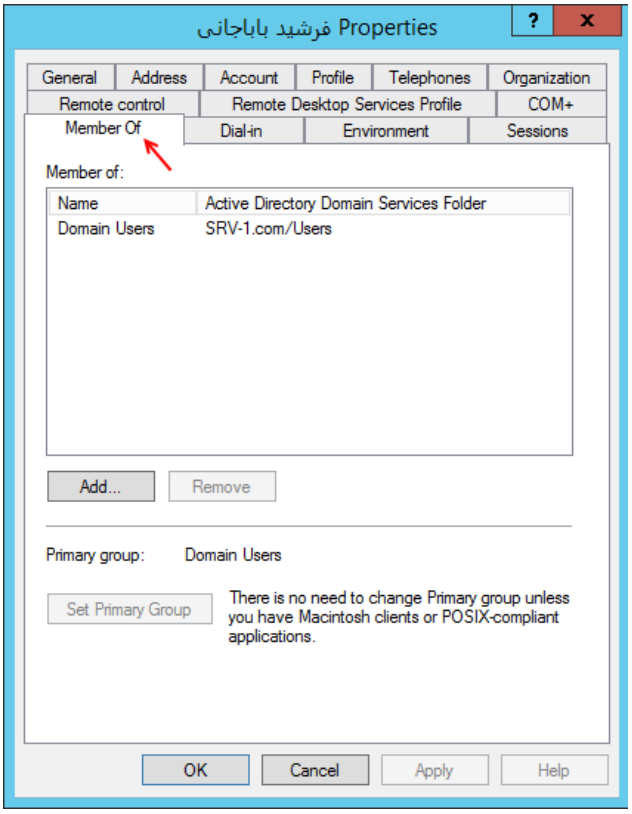


در تب Remote Desktop Service Profile، به مانند تب Profile، شما می‌توانید برای کاربران خود که به صورت Remote، وارد سیستم دیگری می‌شوند، Profile مشخص و هارد دیسک مجازی روی سرور اصلی ایجاد کنید تا تمام اطلاعات آن‌ها ثبت و در دسترس باشد.

همان‌طور که قبلاً اشاره کردم، تمام این قسمت‌ها به صورت کامل بررسی خواهد شد.

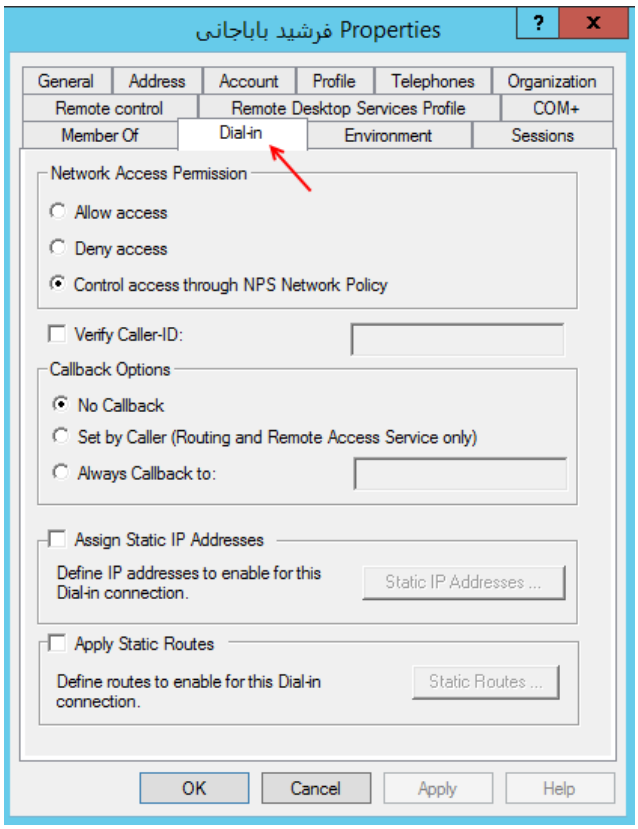


تب COM+ برای ایجاد Partition های خاص برای کاربران می‌باشد تا برنامه های COM خود را اجرا کنند. COM+ یک معماری برنامه نویسی شیء گرا است که توسط مایکروسافت ارائه شده تا بتواند با سیستم های تجزیه ی اطلاعات اوراکل و IBM رقابت کند.

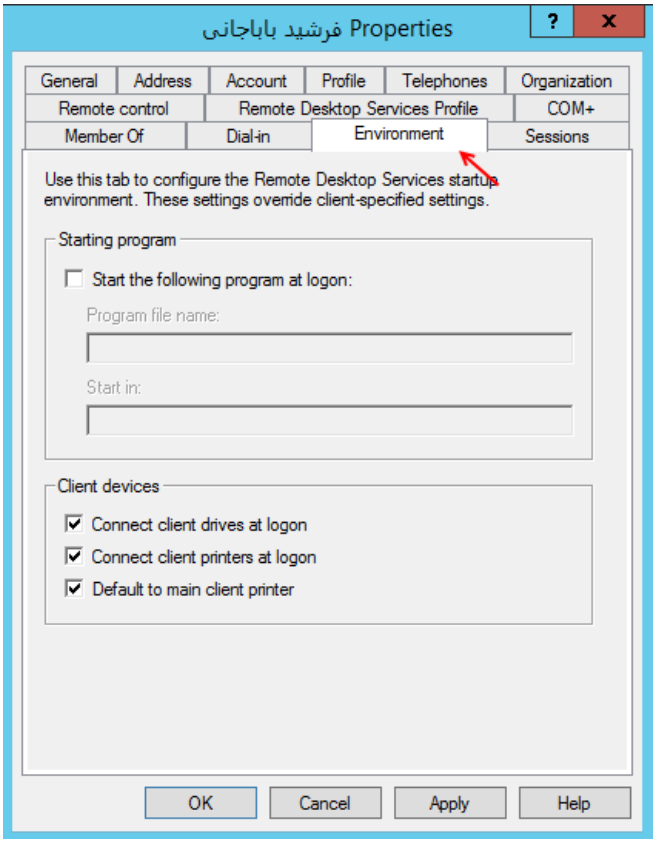


در تب Member Of، این توانایی را داریم تا کاربر موردنظر را عضو گروه خاصی کنیم که در این کتاب، بسیار بر روی این موضوع به بحث خواهیم پرداخت.

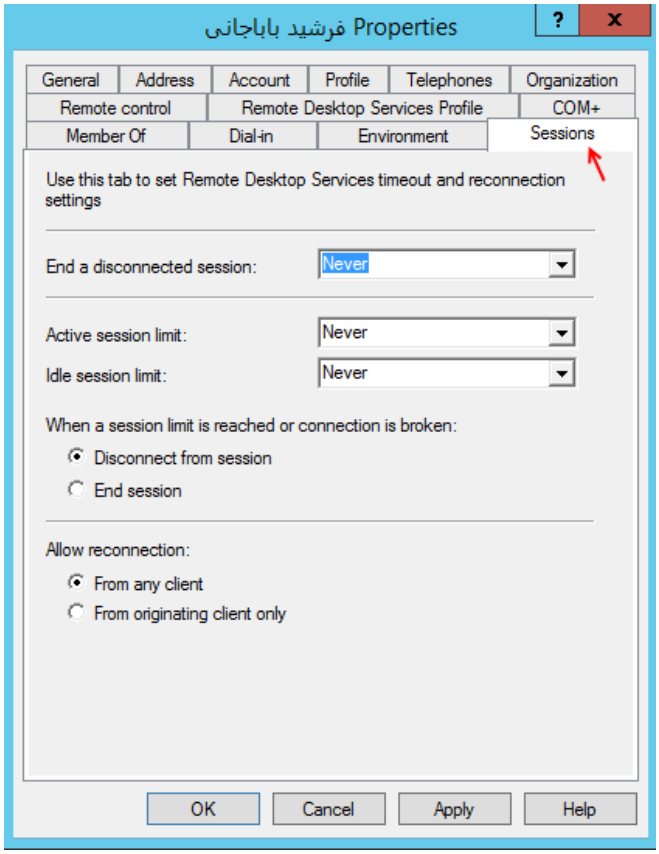
یکی از ویژگی های این تب این است که شما می‌توانید یک گروه ایجاد کنید و مجوز های خاصی را به آن بدهید و بقیه ی کاربران را عضو آن گروه کنید و دیگر لازم نیست به تک تک گروه ها مجوز دسترسی بدهید.



در تب Dial-in، این توانایی ارا به کاربر می‌دهیم تا بتواند بیرون از شبکه ی سازمانی به شبکه سازمان متصل شود، در این قسمت، می‌توانیم برای کاربر موردنظر IP Address را به صورت دستی وارد کنیم و کارهای مختلف انجام دهیم.



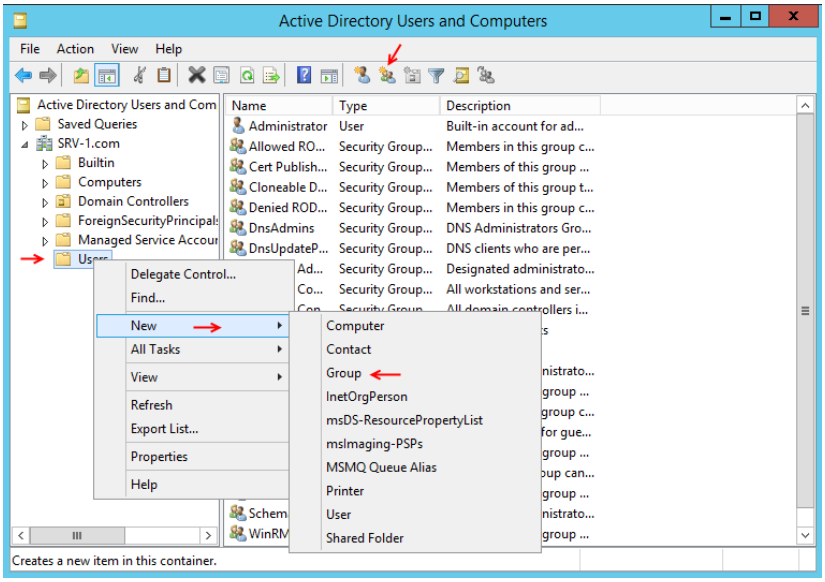
در تب Environment، می‌توانید مشخص کنید که زمانی‌که کاربر وارد سیستم می‌شود، چه نرم‌افزاری برای وی توانایی اجرا شدن داشته باشد.



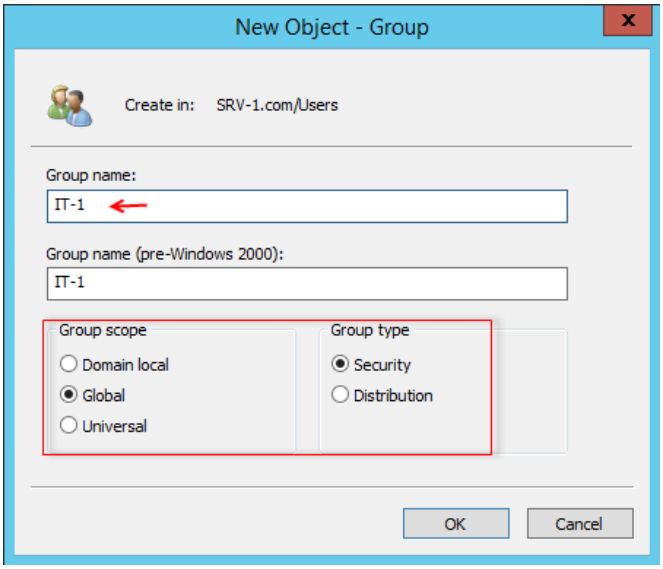
در این بخش، شما به عنوان مدیر شبکه این توانایی را دارید تا مشخص کنید که کاربر موردنظر تا چه زمانی در یک سیستم قرار داشته باشد و یا می‌توانید مشخص کنید که زمانی که کاربر بر روی سیستم قرار ندارد و سیستم بیکار است تا چه زمانی از ویندوز خارج شود.

تا این لحظه، تمام تب های مربوط به یک کاربر را با هم بررسی کردیم. در درس های بعد، روی تب های توضیح داده شده، بیشتر بحث خواهیم کرد.

ایجاد گروه در سرویس Active Directory Users and Computers:



گروه ها در Active Directory، بیش-ترین نقش را ایفا می‌کنند و در بیشتر اوقات از آن‌ها استفاده می‌کنیم. برای ایجاد گروه، وارد سرویس Active Directory Users and Computers می‌شویم و از سمت چپ به مانند شکل روبرو بر روی Users کلیک راست می‌کنیم و از قسمت New گزینه ی Group را انتخاب و یا از نوار ابزار بالایی بر روی آیکون موردنظر کلیک می‌کنیم.

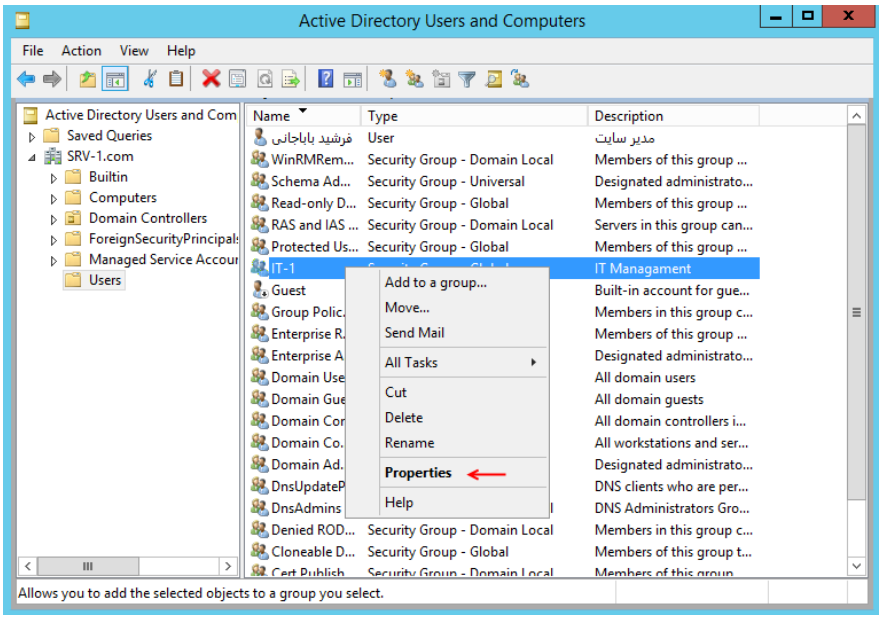


در این صفحه، در قسمت Group name نام گروه را وارد می‌کنیم. گروه ها اصولاً از تقسیمات Group Scope و Group type استفاده می‌کنند که با هم این گزینه ها را بررسی می‌کنیم.

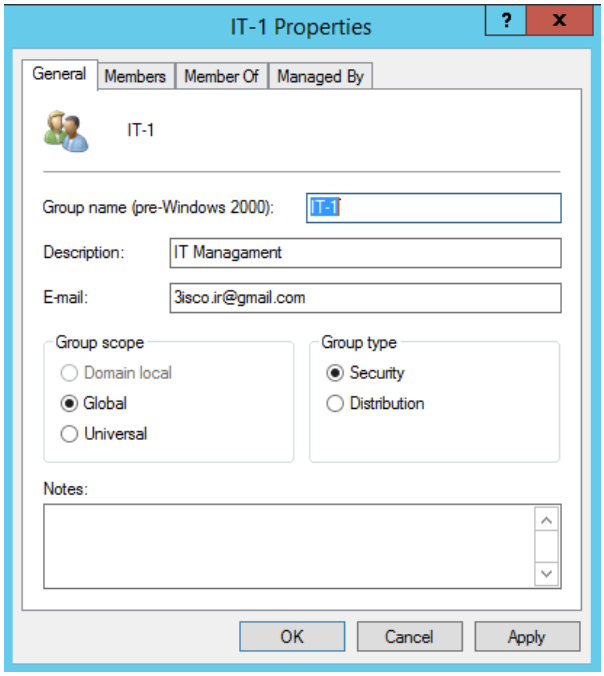
در قسمت Group Scope، سه گزینه وجود دارد؛ گزینه ی Domain Local که با انتخاب این گزینه، گروه موردنظر توانایی عضوگیری کاربران از داخل دومین خود و دومین هایی Forest که به دومین اصلی، Trust می‌باشند را دارد؛ اما گزینه ی Global که توانایی عضوگیری فقط از دومین خود و زیرمجموعه ی خود را دارد، توانایی دسترسی از تمام Forest ها و دومین ها را دارد. گزینه ی Universal، توانایی عضو گیری از هر دومین و یا Forest را دارد؛ یعنی اینکه اگر از چند دومین اصلی در شبکه خود استفاده می‌کنید، در صورت Trust بودن، می‌توانید کاربران هر دومینی را عضو این گروه کنید.

درباره ی Trust کردن دومین ها، به صورت مفصل در ادامه ی کتاب بحث خواهیم کرد. در کل، Trust کردن به این موضوع اشاره دارد که برفرض، اجزای دومین A بتواند توسط دومین B قابل دسترس باشد و یا برعکس.

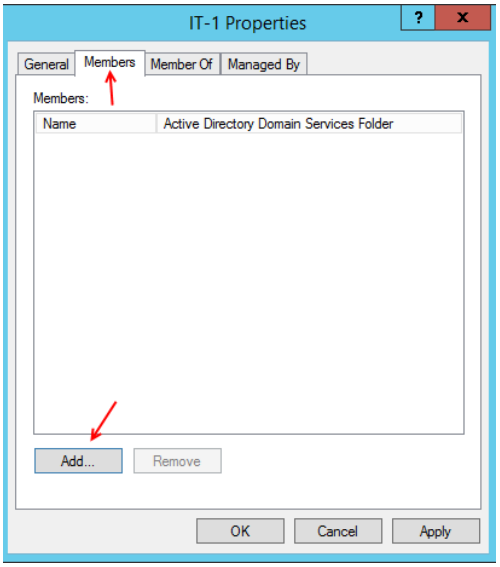
بعد از انتخاب گزینه ی Global، قسمت دیگری وجود دارد با نام Group Type که دراین دو گزینه می‌باشد؛ اگر گزینه ی Security را انتخاب کنید، این گروه مجوز یا Permission لازم را می‌توانند دریافت کنند و برای ارسال پیام گروهی در دومین استفاده می‌شود؛ ولی گزینه ی Distribution، این امکان را ندارد که Permission دریافت کند؛ اما می‌تواند به اعضای خود پیام ارسال کند. برای اتمام کار گزینه ی Global و Security را انتخاب و بر روی ok کلیک کنید.



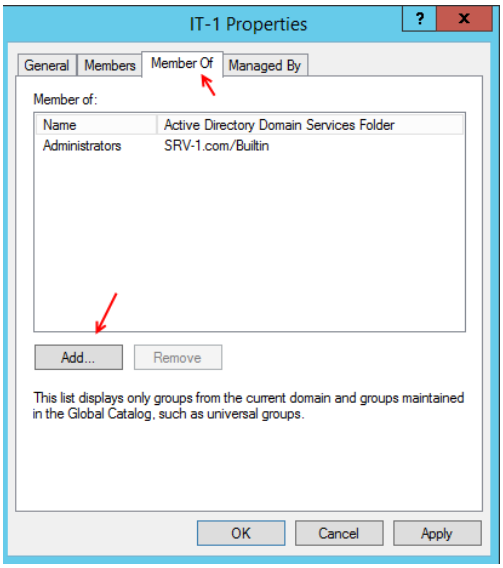
بعد از ایجاد گروه موردنظر، بر روی آن کلیک راست کنید و گزینه ی Properties را انتخاب کنید.



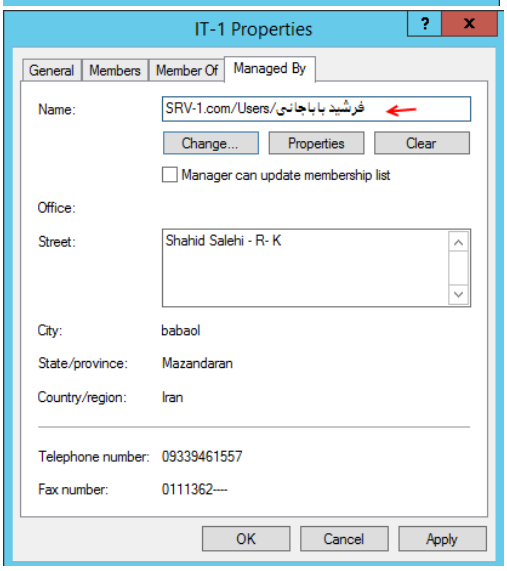
در این صفحه و در تب General، می‌توانید نوع گروه و Scope آن را مشاهده کنید و می‌توانید آن‌ها را تغییر دهید؛ به این نکته توجه کنید که اگر Scope یک گروه را Global در نظر بگیرید، نمی‌توانید آن را به Domain Local تغییر دهید و یا برعکس. توضیحات و آدرس ایمیل مربوط به این گروه را وارد کنید.



در تب **Members**، می‌توانید هر کاربری که عضو دومین باشد و یا **Forest** دیگر را زیر مجموعه ی این گروه قرار دهید؛ برای این کار، بر روی **Add** کلیک و کاربر موردنظر را جستجو کنید.

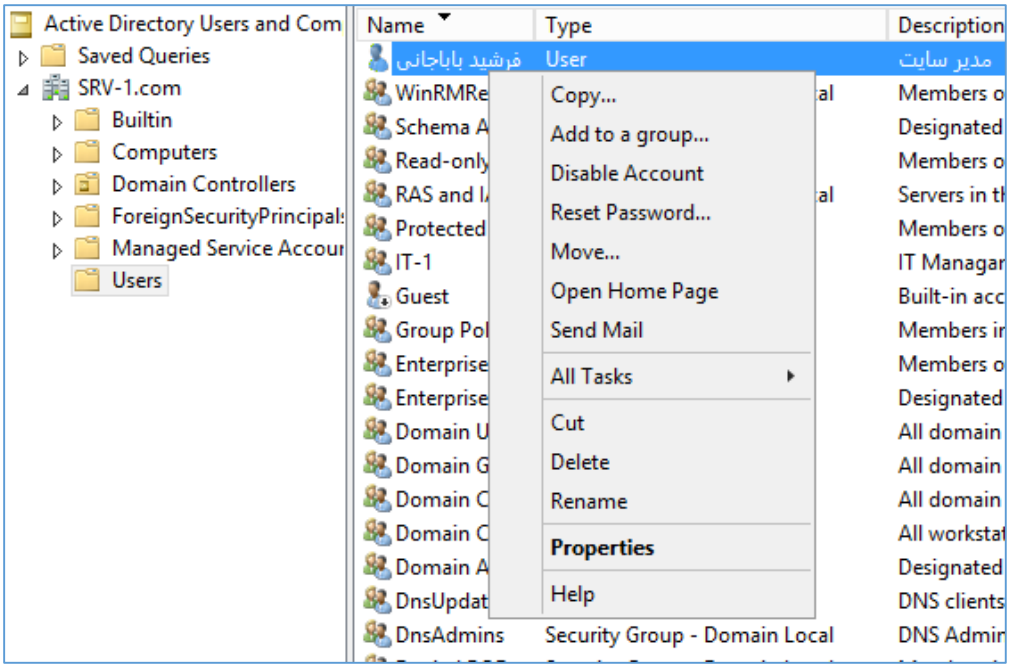


در تب **Member Of**، می‌توانید این گروه را عضو گروه دیگری کنید و از مجوزهای آن استفاده کنید؛ برای این کار، برروی **Add** کلیک کنید و گروه موردنظر را به مانند شکل روبرو به لیست اضافه کنید.



در تب **Managed By**، می‌توانید مشخص کنید که چه کاربر و گروهی، رئیس گروه موردنظر باشد؛ یعنی با انتخاب آن، فقط همان گروه یا کاربر موردنظر می‌تواند، کاربران دیگر را عضو این گروه کند.

بر روی **Ok** کلیک کنید.



اگر بر روی یک کاربر، کلیک راست کنید، گزینه های متفاوتی را به مانند شکل روبرو مشاهده می-کنید. هر کدام از این گزینه ها را با هم بررسی می‌کنیم:

Copy: اگر این گزینه را انتخاب کنید، می‌توانید یک کاربر جدید با اطلاعات کاربر قبلی که از آن کپی گرفته اید را تهیه کنید.

Add to a group: این گزینه، برای عضویت کاربر موردنظر در یک گروه خاص می‌باشد. بعد از کلیک بر روی آن، صفحه‌ای باز می‌شود که می‌توانید گروه موردنظر را برای عضویت این کاربر در آن مشخص کنید.

Disable Account: با کلیک بر روی این گزینه، کاربر موردنظر غیر فعال می‌شود و توانایی ورود به شبکه از وی گرفته می‌شود و اگر دوباره روی آن کلیک کنید، می‌توانید کاربر موردنظر را فعال کنید.

Reset Password: با کلیک بر روی این گزینه، رمز عبور کاربر را بدون دانستن رمز عبور قبلی تغییر دهید.

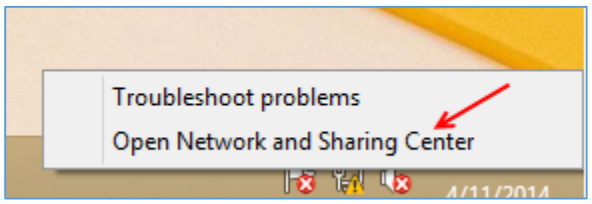
Move: با انتخاب این گزینه می‌توانید کاربر و یا گروه موردنظر را به یک قسمت دیگر که در سمت چپ عکس، مشخص‌شده انتقال داد.

Open Home Page: با کلیک بر روی این گزینه، آدرس سایت کاربر موردنظر که در قسمت General مربوط به کاربر موردنظر وارد کردیم، باز می‌شود.

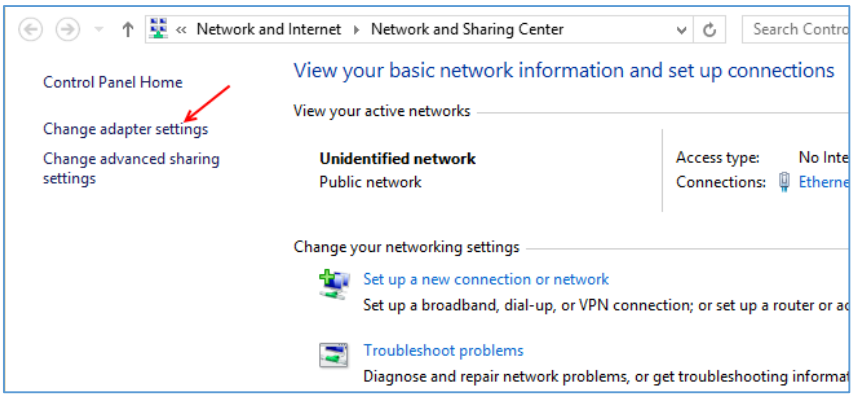
Send Mail: می‌توانید برای کاربر موردنظر در صورت نصب بودن نرم افزار Outlook، ایمیل بفرستید.

نحوه ی ارتباط ویندوز 8 با Active Directory:

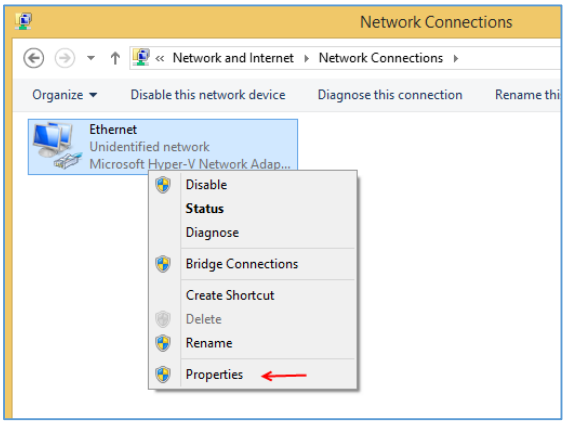
در این بخش می‌خواهیم با استفاده از ویندوز 8 به سرور اصلی متصل شویم؛ برای این کار باید ویندوز 8 را در اختیار داشته باشید. اگر با نصب ویندوز 8 مشکل دارید با من در تماس باشید، بعد از نصب و اجرای ویندوز، وارد آن شوید و بر روی آیکون کارت شبکه، کلیک راست کنید و گزینه ی Open Network and Sharing Center را انتخاب کنید.



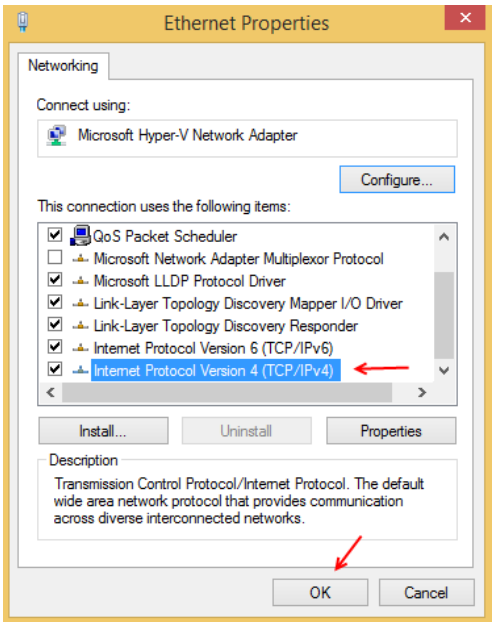
در این صفحه، از سمت چپ بر روی Change adapter settings کلیک کنید تا شکل بعد ظاهر شود.

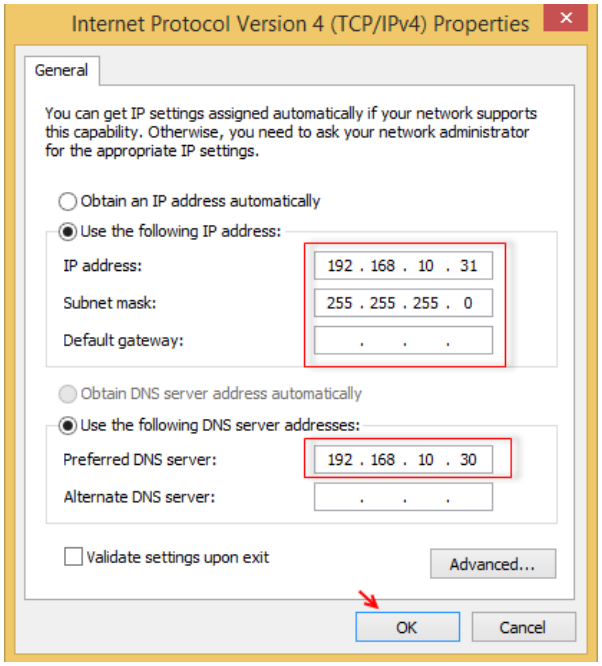


در این صفحه، بر روی آیکون کارت شبکه، کلیک راست کنید و Properties را انتخاب کنید.



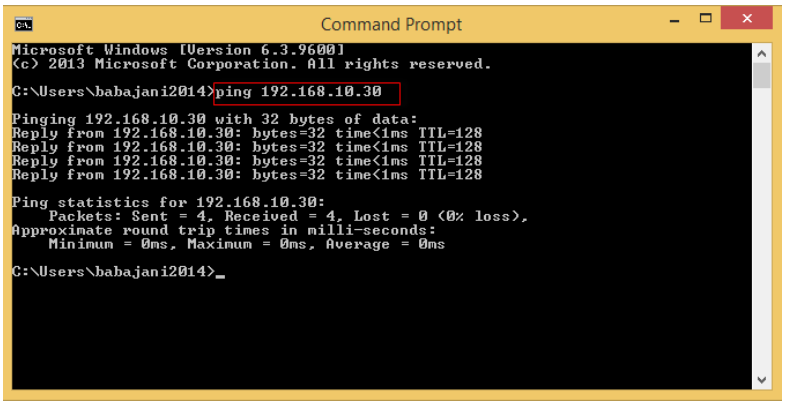
در این صفحه از لیست موجود، گزینه ی Internet Protocol Version 4 را انتخاب و بر روی Properties کلیک کنید تا شکل صفحه ی بعد ظاهر شود.



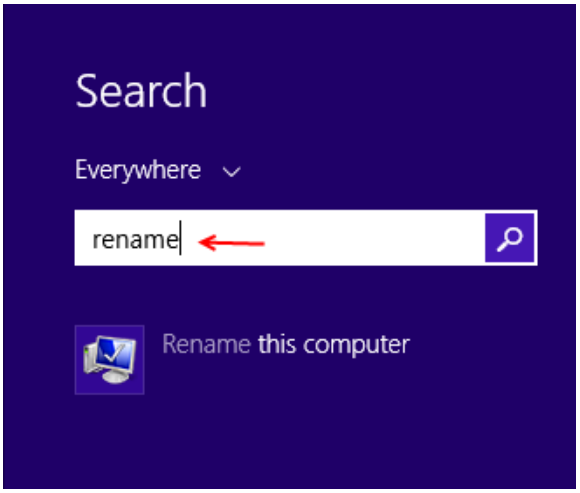


در این قسمت باید IP مربوط به ویندوز 8 را در رنج IP ویندوز سرور وارد کنید. IP address را به صورت 168.10.192. وارد کنید و Subnet mask را به صورت 255.255.255.0 وارد کنید. در قسمت DNS Server، باید آدرس سرور را که در اینجا 192.168.10.30 می‌باشد، وارد کنید؛ بعد از این کار، بر روی ok کلیک کنید.

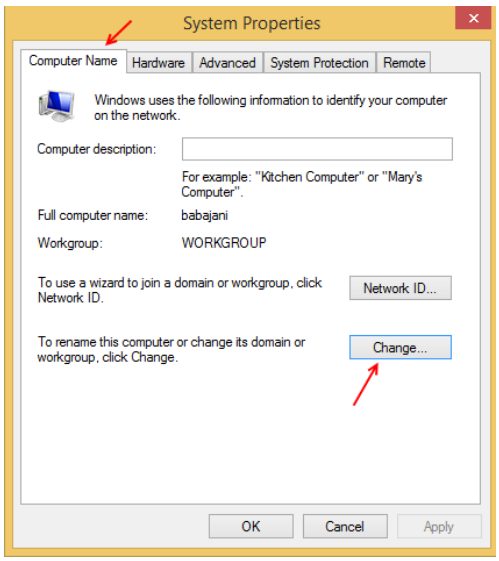
بعد از آن، باید بررسی کنیم که به سرور خود متصل شده‌ایم یا نه. برای این کار، وارد Search شوید و CMD را وارد و اجرا کنید تا شکل بعد ظاهر شود.



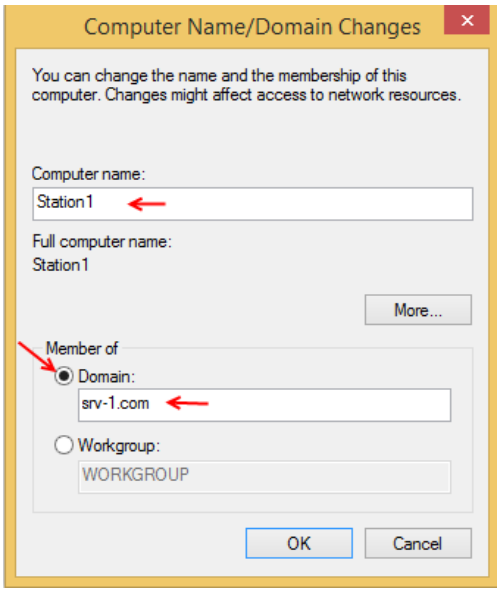
همان‌طور که در این قسمت مشاهده می‌کنید، با دستور PING 192.168.10.30، به سرور موردنظر به درستی متصل شده ایم.



بعد از تست ارتباط با سرور اصلی، باید ویندوز 8 را زیر مجموعه ی دومین SRV-1.com کنیم. برای این کار، مانند شکل روبرو وارد Search ویندوز 8 می‌شویم و کلمه ی Rename را وارد می‌کنیم و از لیست موجود، گزینه ی Rename this computer را انتخاب می‌کنیم.



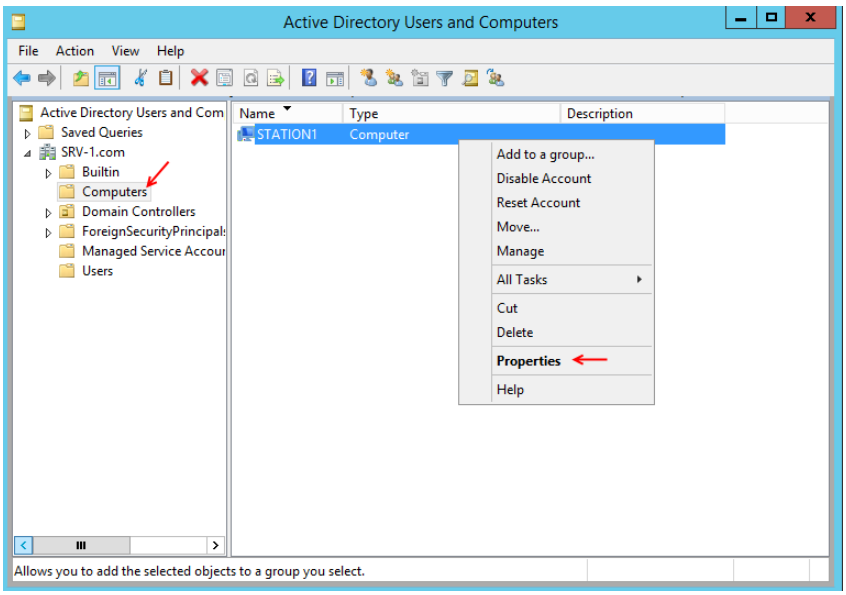
در این صفحه از تب Computer Name، گزینه ی Change را انتخاب کنید تا شکل بعد ظاهر شود.



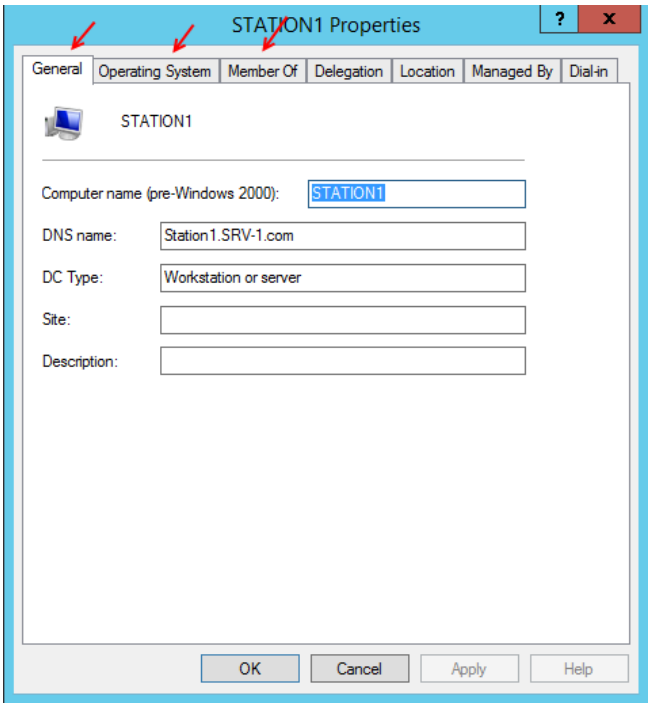
در این صفحه و در قسمت Computer name، نام کامپیوتر خود را وارد کنید که در اینجا، نام Station1 وارد شده است و مهم ترین بخش، قسمت Domain می‌باشد که باید نام دومین SRV-1.com را وارد کنید. بعد از وارد کردن اطلاعات، بر روی ok کلیک کنید. بعد از کلیک بر روی ok صفحه ای باز می‌شود که از شما، نام کاربری و رمز عبور سرور اصلی را درخواست می‌کند که نام کاربری Administrator می‌باشد. بعد از ورود، بر روی ok کلیک کنید تا صفحه ی Welcome ظاهر شود. بعد از آن، بر روی ok کلیک کنید و سیستم را Restart کنید.

بعد از اینکه سیستم را Restart کردید، زمانی که می‌خواهید وارد سیستم شوید، به صورت پیش فرض، نام کاربری قبلی فعال است و اگر وارد آن شوید، یعنی اینکه وارد سیستم local شده اید و وارد دومین نشده اید. برای ورود به دومین بر روی Other user کلیک کنید و نام کاربری را به صورت روبرو و به صورت Domain name\User وارد کنید و وارد سیستم شوید.

تا به اینجا، ویندوز 8 را نصب و به سرور 2012 R2 متصل کردیم. در ادامه، وارد ویندوز سرور می‌شویم و سرویس Active Directory Users and Computers را اجرا می‌کنیم.



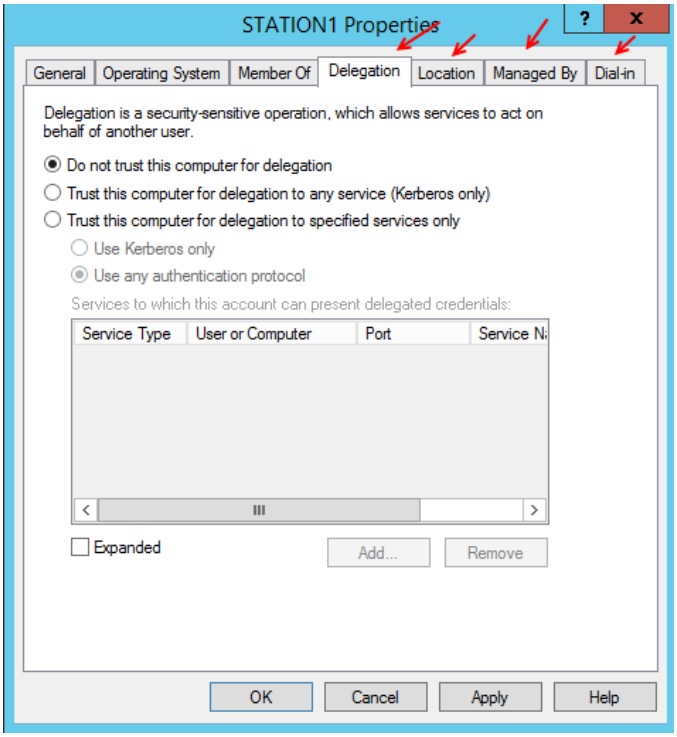
بعد از اجرای سرویس به مانند شکل روبرو، اگر از سمت چپ بر روی Computers کلیک کنید، لیست کامپیوترهایی را که به این دومین متصل شده اند را مشاهده می‌کنید، اگر قسمت متصل شدن ویندوز 8 را به دقت توجه کرده باشید، نام آن را Station1 وارد کردیم که در شکل روبرو هم همین نام را مشاهده می‌کنید. بر روی نام کامپیوتر کلیک راست کنید تا منوی موردنظر باز شود. در این منو، گزینه هایی مختلفی وجود دارد که قبلاً هم در قسمت User آن‌ها را بررسی کردیم. فقط به این نکته اشاره کنیم که اگر گزینه ی Disable Account را انتخاب کنید، سیستم موردنظر غیرفعال شده و توانایی ورود به دومین را نخواهد داشت. بر روی Properties کلیک کنید.



در تب General، نام کامپیوتر، نام DNS و نوع دومین کنترلر را مشاهده می‌کنید.

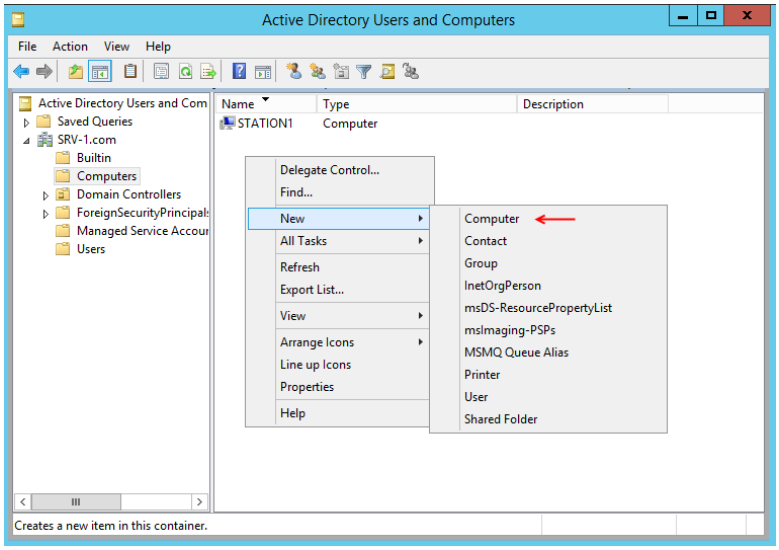
در تب Operation System، سیستم عاملی که روی کامپیوتر موردنظر نصب است را به همراه ورژن و سرویس پک به ما نشان می‌دهد.

در تب Member Of، می‌توانید کامپیوتر موردنظر را عضو گروهی کنید که با این کار کامپیوتر موردنظر مجوز های لازم را از گروه موردنظر دریافت می‌کند.

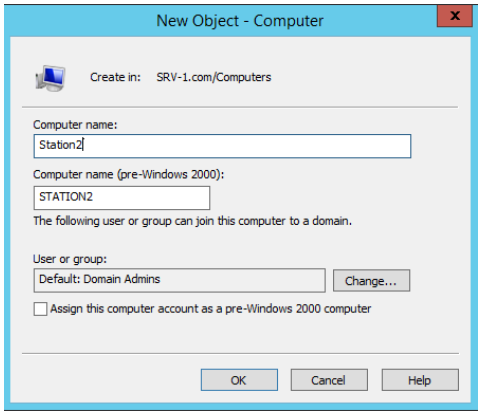


در تب Delegation، می‌توانیم این توانایی را به این کامپیوتر بدهیم که سرویس‌های درخواستی خودش را روی سرور دیگر اجرا کند؛ یعنی Trust بین کامپیوتر و سرور دیگر ایجاد کنیم و کامپیوتر بتواند از سرویس های سرور موردنظر استفاده کند.

در تب Location می‌توانید موقعیت جغرافیایی کامپیوتر موردنظر را مشخص کنید. در تب Managed By می‌توانید مشخص کنید چه کاربر و یا گروهی مدیر این کامپیوتر باشد. در تب Dial-in، می‌توانید مشخص کنید که آیا کاربری بتواند از راه دور به این سیستم متصل شود یا نه.



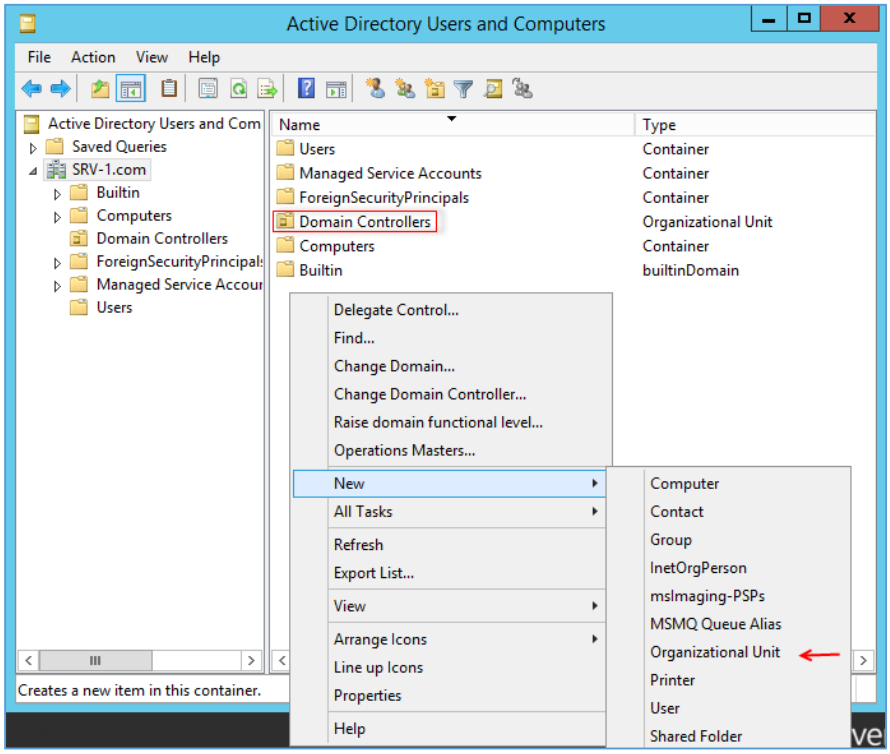
بعد از بررسی Properties مربوط به کامپیوتر Station1 در این می‌خواهیم یک کامپیوتر جدید ایجاد کنیم. برای این کار، در بخش Computer کلیک راست کنید و از قسمت New، گزینه ی Computer را انتخاب کنید تا شکل بعد ظاهر شود.



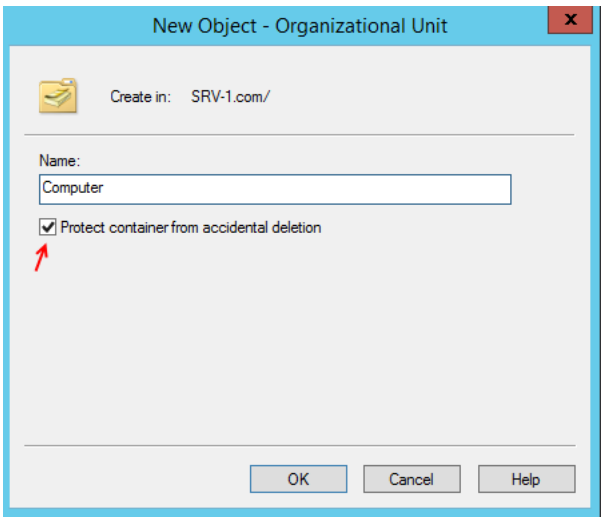
در شکل روبرو باید نام کامپیوتر خود را که می‌خواهید به دومین متصل شود را مشخص کنید که در این قسمت Station2 نوشته شده است و در قسمت User or Group، نام گروه یا کاربری که این کامپیوتر عضو آن می‌باشد را مشخص کنید و بر روی ok کلیک کنید تا کامپیوتر موردنظر ایجاد شود.

کار با Organization Unit در Active directory:

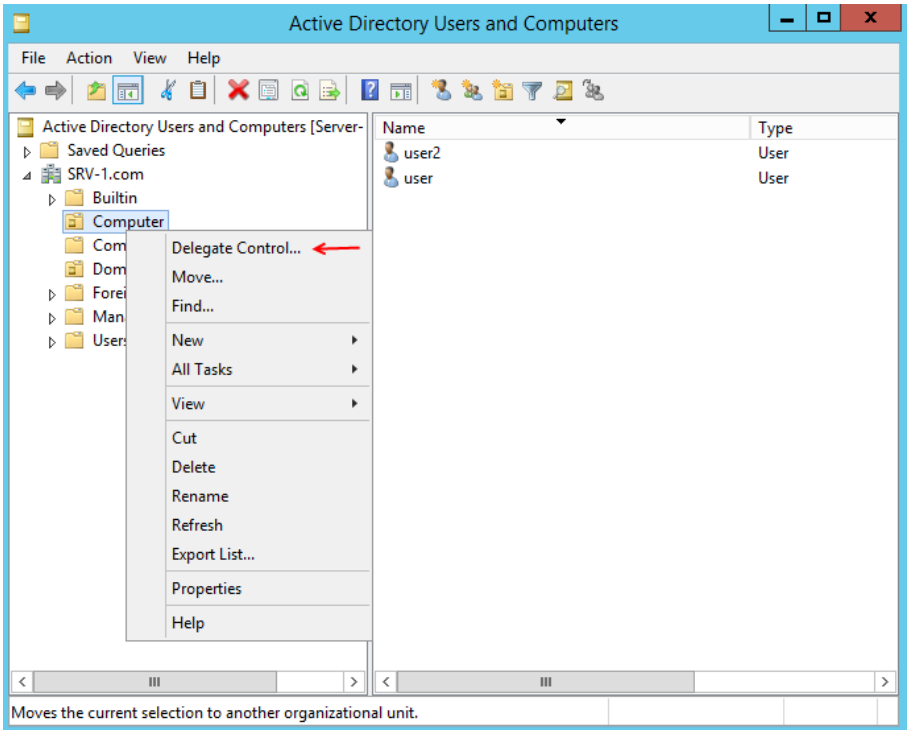
Organization Unit و یا واحد سازمانی قابلیت در اکتیو دایرکتوری می‌باشند که می‌توانید اکتیو دایرکتوری خود را سازمان دهی و طراحی کنید؛ مثلاً می‌توانید در یک سازمان که از چندین بخش تشکیل شده، برای هر بخش یک OU و یا همان Organization Unit ایجاد کنید و تمام کاربران هر بخش را زیرمجموعه ی همان بخش قرار دهید و حتی می‌توانید، یکی از کاربران را به عنوان رئیس آن گروه قرار دهید.



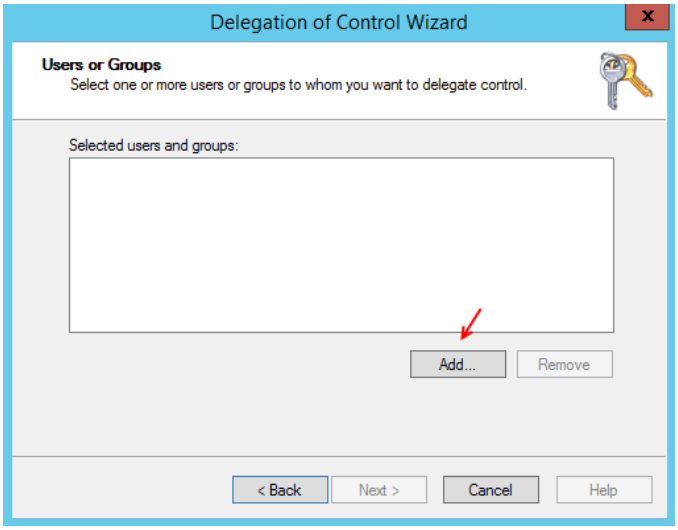
سرویس Active Directory را Users and Computers اجرا کنید. همان‌طور که در شکل هم مشخص‌شده، تنها OU بعد از نصب دومین که به صورت خودکار ایجاد می‌شود، Domain Controllers می‌باشد که برای مدیریت اجزای دومین کنترلر استفاده می‌شود. برای ایجاد OU به مانند شکل روبرو بر روی نام سرور کلیک کنید و در صفحه ی باز شده، کلیک راست کنید و از سمت قسمت New گزینه ی Organization Unit را انتخاب کنید تا شکل بعد ظاهر شود.

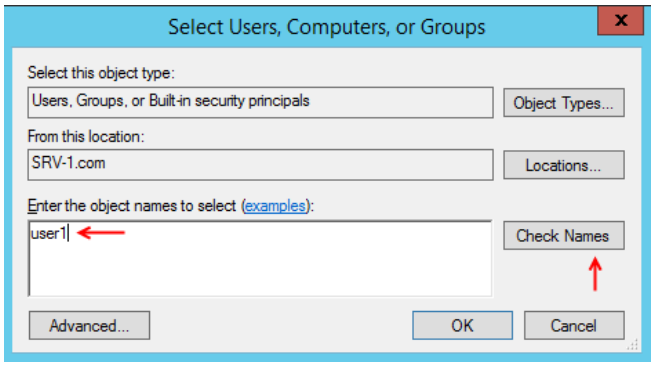


در این صفحه، نام واحد سازمانی خود را وارد کنید. توجه داشته باشید که اگر بخواهید از این OU یا شی محافظت کنید، باید تیک گزینه ی موردنظر را انتخاب کنید. با این کار این OU به راحتی حذف نخواهد شد؛ ولی اگر تیک آن را بردارید حذف خواهد شد. بر روی ok کلیک کنید تا OU موردنظر با نام Computer ایجاد شود.

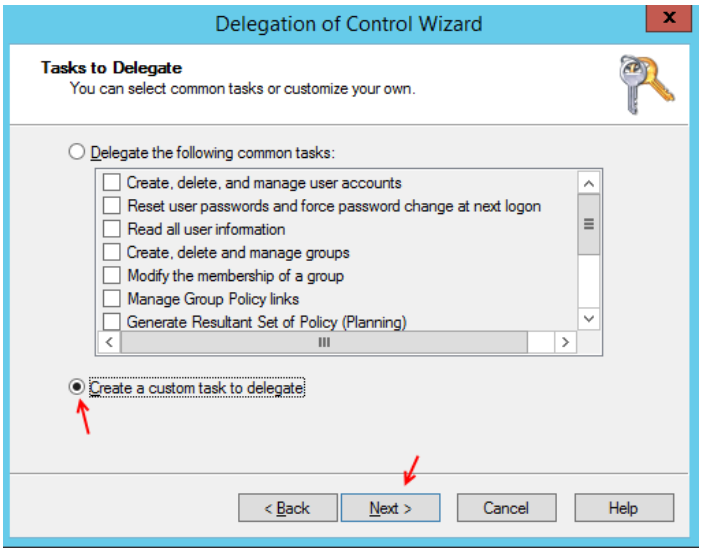


بعد از ایجاد OU موردنظر با نام Computer می‌توانید کاربران و گروه های خاص خود را عضو این واحد سازمانی کنید. همان‌طور که قبلاً گفتیم، می‌توانیم مدیریت این واحد سازمانی را به کاربر و یا گروه خاصی بسپاریم. برای این کار، بر روی واحد سازمانی جدید خود کلیک راست می‌کنیم و گزینه ی Delegate Control را انتخاب می‌کنیم و در صفحه ی باز شده بر روی Next کلیک کنید تا شکل روبرو ظاهر شود. در این شکل، برای اینکه کاربر و یا گروه موردنظر را مشخص کنیم، بر روی Add کلیک می‌کنیم تا شکل زیر ظاهر شود.

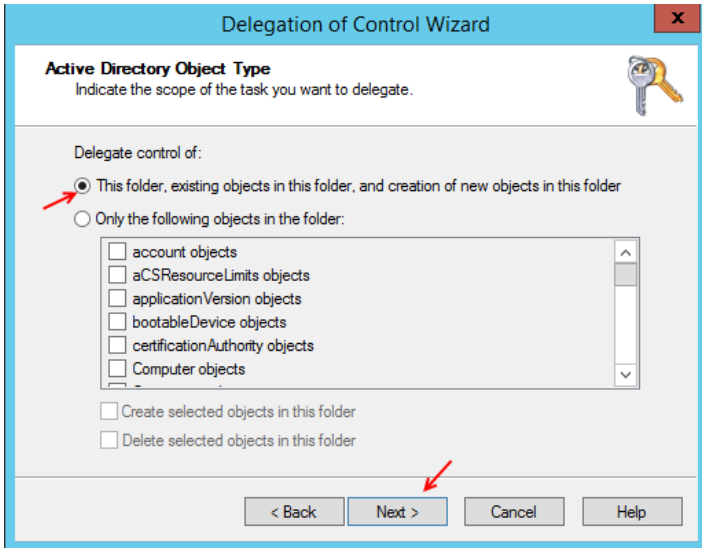




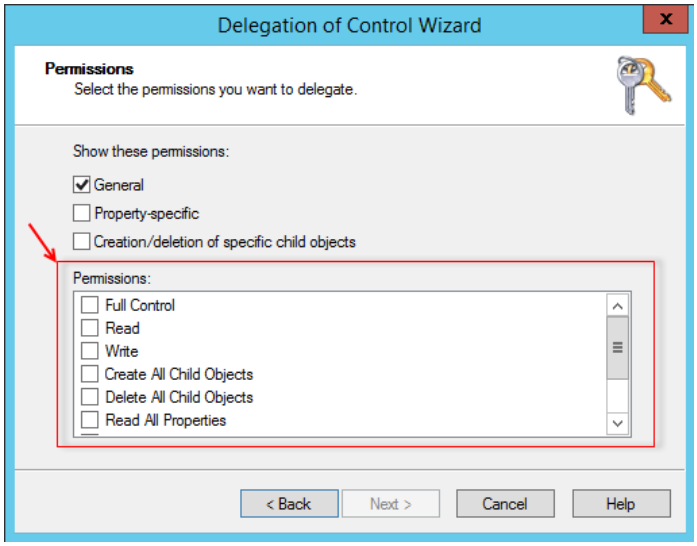
در این قسمت نام کاربر را به صورت کامل و یا نیمه کاره وارد کنید و بر روی Check Names کلیک کنید تا کاربر موردنظر پیدا شود و یا از طریق Location کاربر و یا گروه موردنظر را Search کنید.



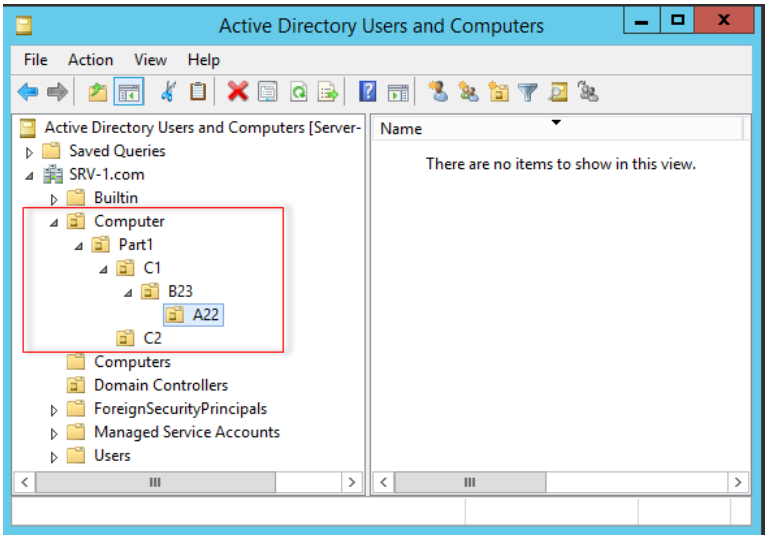
در این صفحه، گزینه ی Create a Custom task to Delegate را انتخاب و بر روی Next کلیک کنید.



در این صفحه، گزینه ی This folder... را انتخاب و برروی next کلیک کنید.

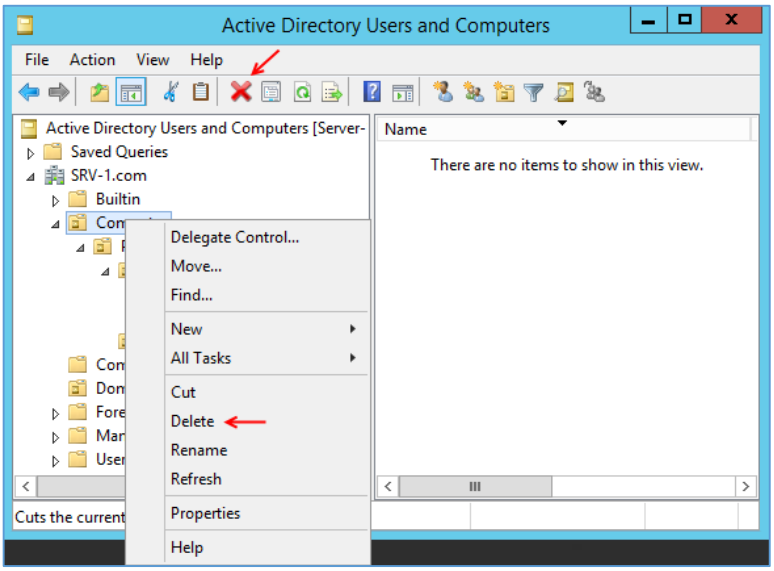


در این صفحه، باید مشخص کنید که کاربر و گروه موردنظر چه نوع مجوزی برای مدیریت گروه سازمانی داشته باشد که هر کدام از این مجوزها، داستان مربوط به خودش را دارد که در وقت خویش به آنها خواهیم پرداخت. در این قسمت، گزینه ی Full Control را انتخاب و بر روی Next کلیک کنید و در صفحه ی بعد بر روی Finish کلیک کنید.

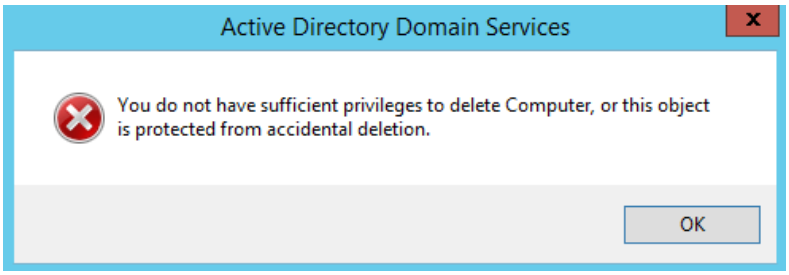


توجه داشته باشید، شما می‌توانید هر چند تا که دوست دارید واحد سازمانی OU ایجاد کنید. مانند شکل روبرو می‌توانید واحد های تو در تو ایجاد کنید.

چگونه واحدهای سازمانی یا همان Organization Unit را حذف کنیم؟

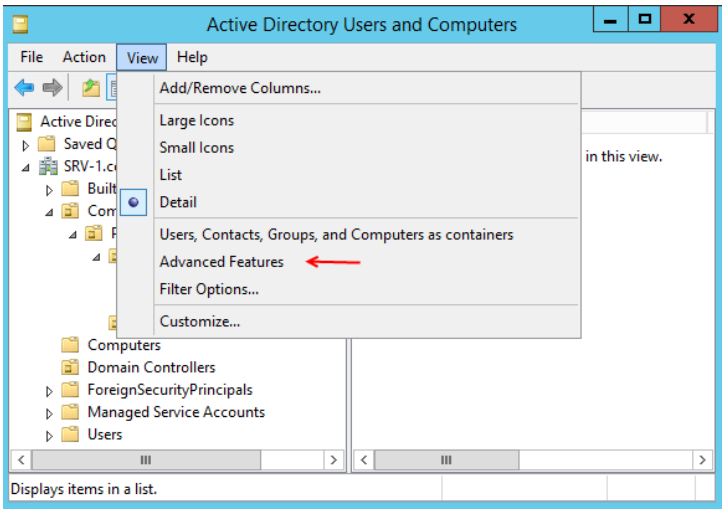


برای حذف واحد سازمانی، روی آن کلیک راست کنید و گزینه ی Delete ر انتخاب کنید و یا از نوار ابزار بر روی آیکون ضربدر کلیک کنید و در شکل باز شده، بر روی Yes کلیک کنید.

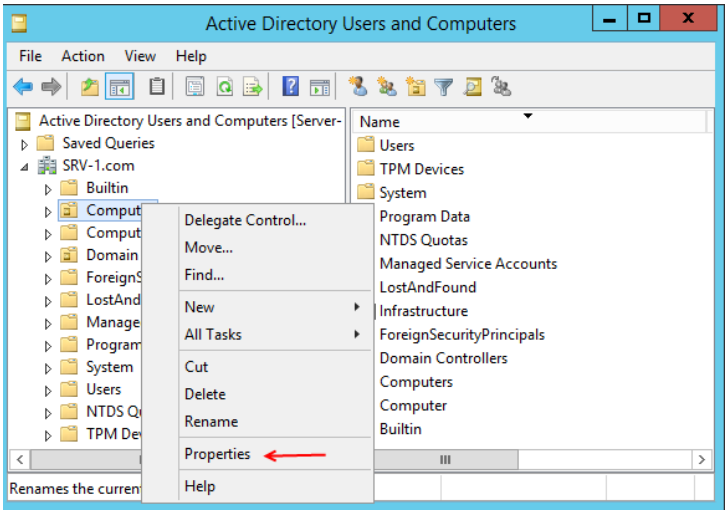


همان‌طور که مشاهده می‌کنید با Error روبرو مواجه شدیم. این Error به این نکته اشاره دارد که شما مجوز لازم برای حذف Object و یا همان شی موردنظر را ندارید. به خاطر اینکه در

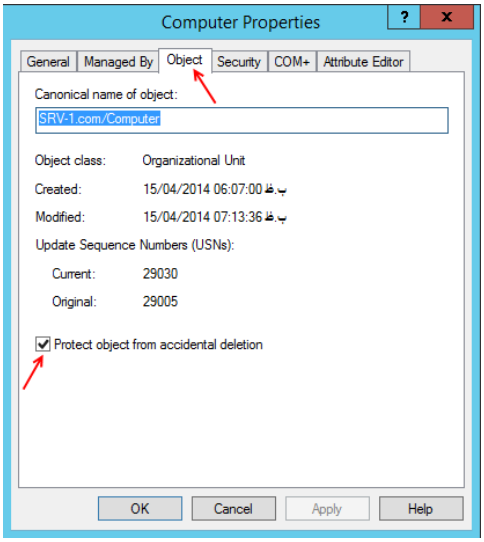
موقع ایجاد Ou تیک مربوط به گزینه ی Protect Container form accidental deletion را زده بودیم، برای حذف آن به صورت زیر عمل کنید:



بر روی منوی View کلیک کنید و گزینه ی Advanced Features را انتخاب کنید.



بعد از انجام کار بالا، بر روی واحد سازمانی موردنظر کلیک راست می‌کنیم و گزینه ی Properties را انتخاب می‌کنیم تا شکل بعد ظاهر شود.



در این صفحه، وارد تب Object شوید و به مانند شکل روبرو تیک گزینه ی Protect Container form accidental deletion را بردارید و بر رو ok کلیک کنید.

نکته مهم: برای حذف واحد سازمانی، توجه کنید که واحد سازمانی دیگر به صورت محافظت شده، زیر مجموعه ی واحد سازمانی در حال حذف نباشد؛ چون OU یا همان واحد سازمانی موردنظر حذف نخواهد شد؛ چون یک واحد سازمانی دیگر به صورت محافظت شده در زیر آن قرار دارد.

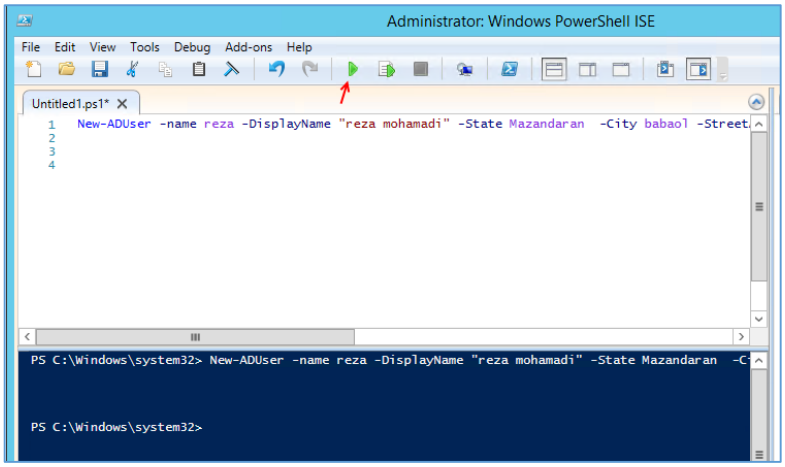
مدیریت Active Directory از طریق PowerShell:

همه ی افراد، شرکت مایکروسافت را به خاطر ویندوز و گرافیکی بودن سیستم عامل آن می‌شناسند. درست است که گرافیک کار را ساده و آسان می‌کند؛ ولی نمی‌تواند بهتر از دستورات باشد.

همان‌طور که در اول کتاب مشاهده کردید، سرویس PowerShell را با هم بررسی کردیم. در این قسمت، با دستوراتی کار خواهیم کرد که برای مدیریت Active Directory کاربرد دارد.

ایجاد کاربر از طریق PowerShell:

برای ایجاد کاربر از طریق دستورات Power Shell، سرویس Windows PowerShell ISE را با اولویت کاربر Administrator اجرا می‌کنیم.



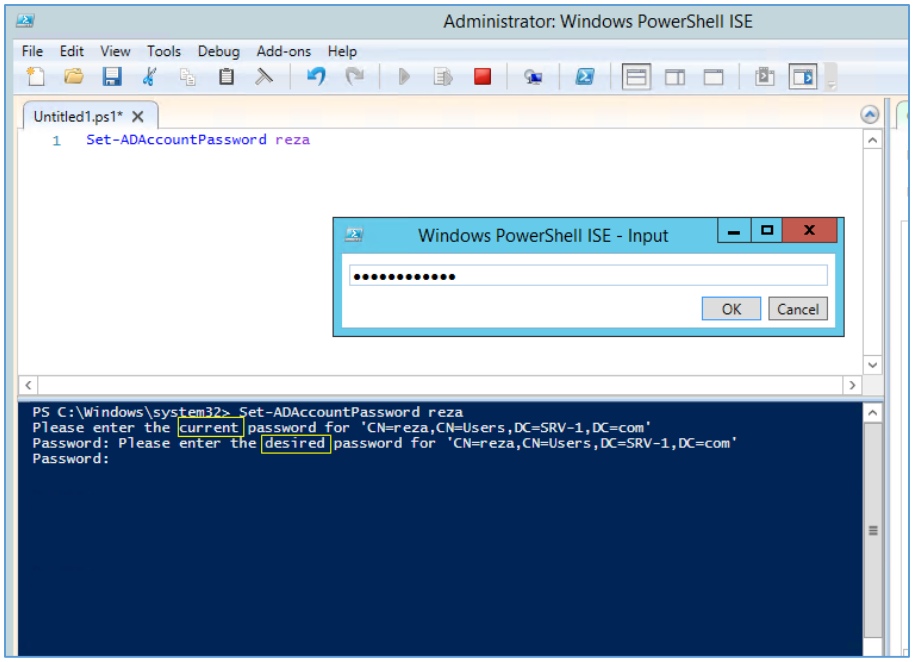
همان‌طور که در شکل مقابل مشاهده می‌کنید، وارد سرویس ISE شده ایم که قبلاً با این سرویس کار کرده بودیم. دستوراتی را که در شکل روبرو می‌بینید برای ایجاد یک کاربر با نام و مشخصات خاص می‌باشد که با هم آن‌ها را بررسی خواهیم کرد.

```
New-ADUser -name reza -DisplayName "reza mohamadi" -State Mazandaran -City babol -
StreetAddress "Shahid alehi" -HomePhone 0111 -HomePage www.3isco.ir -Department cisco
```

دستورات بالارا را کلمه به کلمه با هم بررسی می‌کنیم؛ برای ایجاد کاربر از طریق Power shell باید از دستور New-ADUser استفاده کرد که این موضوع را در دستور بالا مشاهده می‌کنید. بعد از وارد کردن این دستور باید یک تیره (-) قرار دهیم که بعد از این کار، لیست دستوراتی که با دستور New-ADUser کار می‌کنند به صورت منو باز می‌شود که بنا به نیازی که دارید از آن‌ها استفاده می‌کنید؛ بنابراین بعد از هر دستور، باید تیره قرار دهیم تا

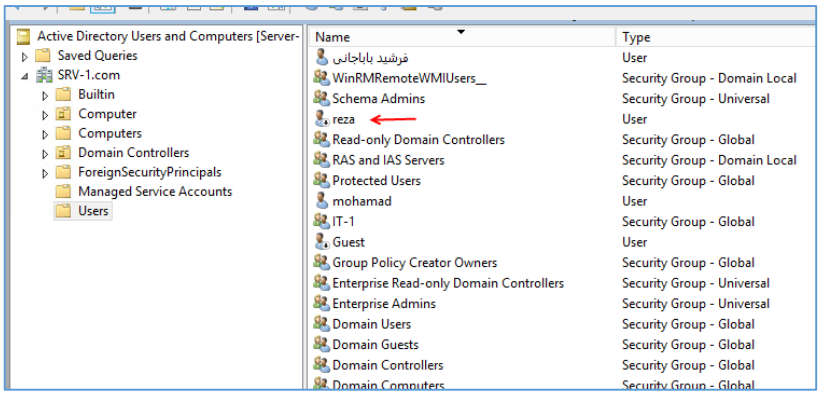
دستورات مربوط به دستور اصلی برای ما نمایش داده شود. مرحله بعدی معرفی نام کاربر می‌باشد که باید اول – Name را وارد کنید و بعد، نام کاربر را که در اینجا Reza هست را وارد می‌کنیم؛ بعد از این کار، شما می‌توانید کد موردنظر را بدون وارد کردن بقیه ی اطلاعات اجرا کنید؛ چون بقیه ی اطلاعات، تکمیل کننده ی کاربر می‌باشد با دستورDisplayName- و بعد از آن، نام کامل کاربر موردنظر را وارد می‌کنیم. نکته ی مهمی که در این قسمت وجود دارد، این است که زمانی که قرار است یک اسم را وارد کنید و آن اسم به صورت چند کلمه جدا از هم باشد، حتماً باید کلمات موردنظر را داخل دابل کوتیشن (“”) به مانند اسم "reza mohamadi" قرار داد تا با Error مواجه نشویم. بقیه ی دستورات هم برای نام استان، شهر، خیابان و غیره می‌باشد که خودتان به دلخواه وارد کنید. توجه داشته باشید که این اطلاعات، همان اطلاعاتی است که مربوط به Properties یک کاربر می‌باشد که با هم بررسی کردیم. با کلیک بر روی آیکون Run Script، این دستورات اجرا شده و کاربر موردنظر مان ایجاد می‌شود.

بعد از ایجاد کاربر، باید رمز عبور آن را وارد کنیم؛ برای این کار از دستور زیر استفاده می‌کنیم.




```
Set-ADAccountPassword reza
```

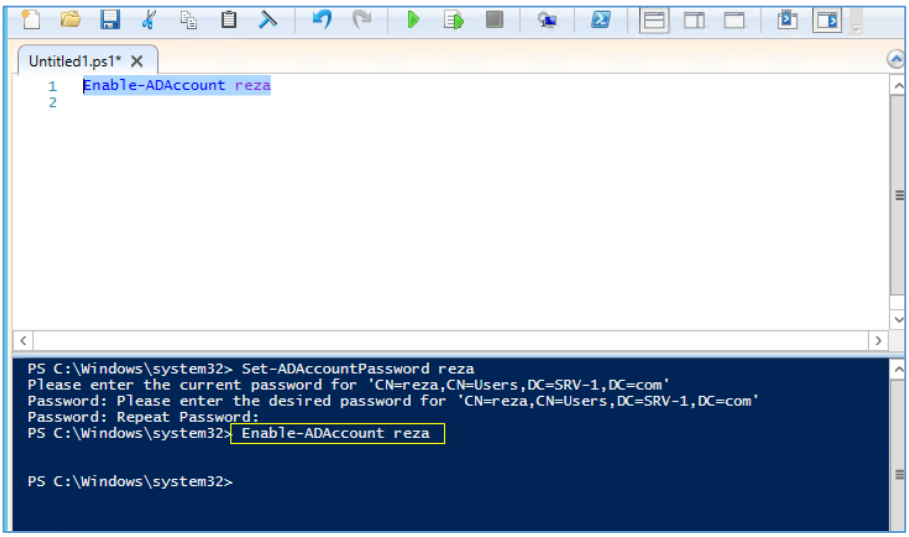
این دستور، برای قرار دادن رمز عبور بر روی کاربر موردنظر می‌باشد برای این کار، باید ابتدا دستور-Set ADAccountPassword را وارد کنید و بعد از آن، باید نام کاربر را که در قسمت name– آن وارد کردید را اینجا وارد کنید تا پنجره دریافت رمز عبور برای شما ظاهر شود. اگر کاربر شما از قبل، رمز عبور بر روی آن Set شده است، باید در پنجره ی current، رمز موردنظر را وارد کنید؛ وگرنه باید بدون وارد کردن کلمه‌ای، بر روی ok کلیک کرد و بعد، باید در قسمت Desired، رمز جدید را وارد کنید و بعد بر روی ok کلیک کنید و در پنجره آخر، رمز را دوباره تکرار کنید. بر روی ok کلیک کنید تا به کاربر موردنظر، رمز عبور تعلق گیرد.



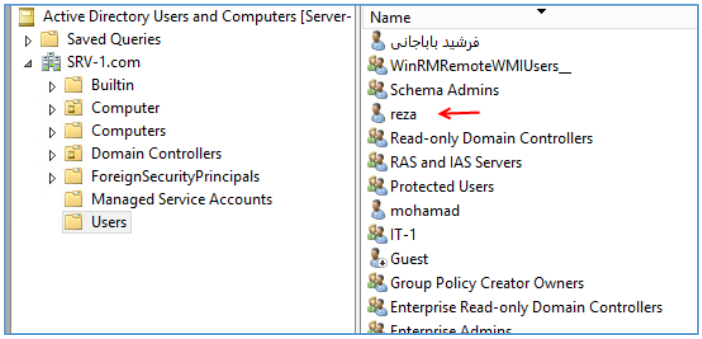
تا به اینجا یک کاربر با جزئیات مشخص‌شده، ایجاد و رمز عبور آن را هم قرار دادیم؛ ولی اگر در حال حاضر، وارد سرویس Active Directory Users and Computers شوید در قسمت Users کاربر موردنظر به مانند شکل روبرو غیر فعال خواهد بود.

برای فعال کردن کاربر موردنظر، باید از دستور زیر استفاده کنیم:

```
Enable-ADAccount reza
```



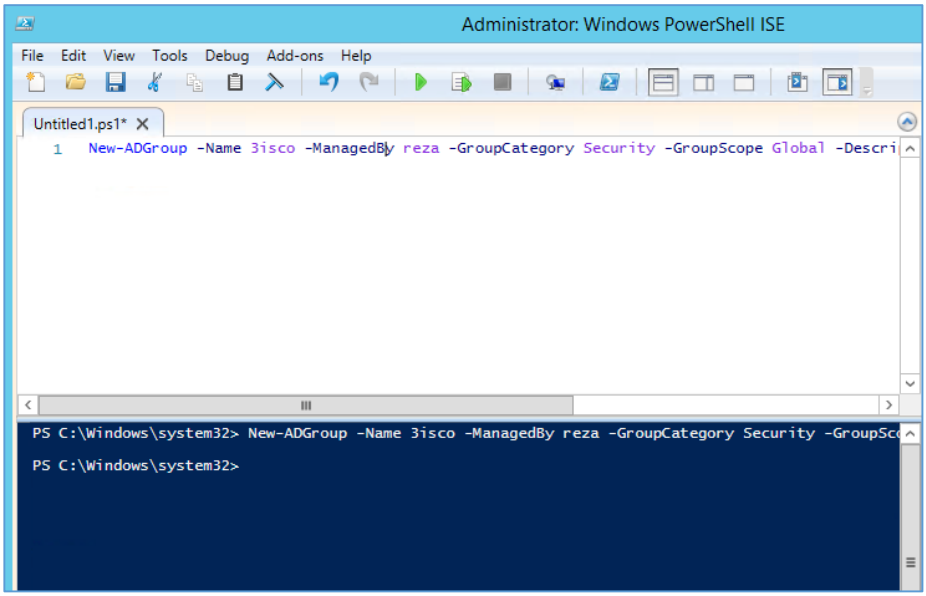
در این دستور، باید به جای Reza، نام کاربر خود را وارد کنید تا کاربر موردنظر فعال شود. همان‌طور که گفتیم برای اجرای این دستورات باید بر روی آیکون Run Script در بالای صفحه کلیک کنید.



همان‌طور که در شکل روبرو مشاهده می‌کنید، کاربر Reza فعال شده است و توانایی ورود به سیستم خود را دارد.

ایجاد Group از طریق PowerShell:

برای ایجاد گروه، وارد PowerShell ISE می‌شویم؛ دلیل ورود به این سرویس، این است که وارد کردن دستورات و یادگیری آن به نسبت PowerShell راحت‌تر است.



در این قسمت، دستورات مربوط به ایجاد گروه اجرا شده است و گروهی با نام 3isco، با تنظیمات موردنظر ایجاد شده است که در زیر، آن‌ها را بررسی می‌کنیم.

```
New-ADGroup -Name 3isco -ManagedBy reza -GroupCategory Security -GroupScope
Global -Description "Network Learning"
```

دستور New-ADGroup برای ایجاد گروه استفاده می‌شود؛ بعد از این دستور، باید نام گروه را با دستور –name وارد کنید؛ یعنی به صورت name 3isco– بعد از آن، می‌توانیم با دستور ManagedBY– مشخص کنیم که چه کاربر و یا گروهی، مدیر این گروه باشد که نام کاربری Reza را که در قسمت قبل ایجاد کرده بودیم در این قسمت وارد کردیم. بعد از آن باید نوع گروه و حوزه ی فعالیت گروه را مشخص کنیم. با دستور –GroupCategory می‌توانید مشخص کنید که گروه موردنظر از نوع Security باشد و یا از نوع Distribution و با دستور GroupScope– حوزه ی فعالیت گروه را که سه نوع می‌باشد مشخص کنید که در این قسمت، Global وارد شده است و بعد از آن می‌توانید توضیحاتی را با دستورات Description– وارد کنید.

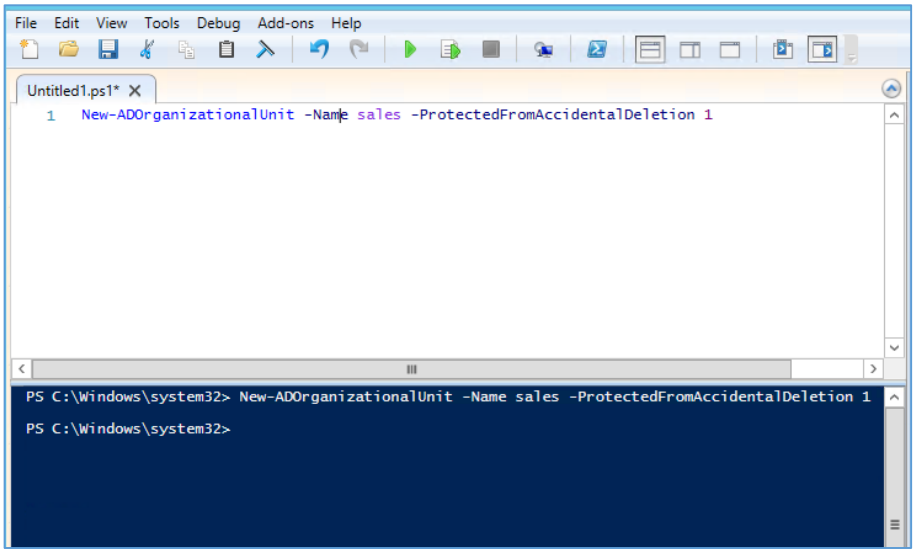
اگر وارد سرویس Active Directory Users and Computers شوید در قسمت Users می‌توانید گروه موردنظر را مشاهده کنید و با کلیک بر روی آن می‌توانید تنظیمات مربوط به آن را مشاهده کنید.

نحوه ی ایجاد Organization Unit یا واحد سازمانی از طریق PowerShell:

برای ایجاد واحد سازمانی، دوباره وارد نرم‌افزار Power shell ISE شوید و دستورات زیر را اجرا کنید:

```
New-ADOrganizationalUnit -Name sales -ProtectedFromAccidentalDeletion 1
```

با استفاده از دستور New-ADOrganizationalUnit، می‌توانیم یک واحد سازمانی در Active Directory خود ایجاد کنیم به این صورت که ابتدا دستور New-ADOrganizationalUnit را وارد می‌کنیم و بعد از آن با دستور Name– و نام واحد سازمانی که در اینجا Sales می‌باشد، می‌توانیم به راحتی یک واحد سازمانی ایجاد کنیم. در ادامه ی دستورات بالا، دستور ProtectedFromAccidentalDeletion 1– را مشاهده می‌کنید که این دستور، برای جلوگیری از حذف شدن شی و یا object موردنظر می‌باشد. زمانی که عدد جلوی آن 1 باشد یعنی اینکه این قابلیت فعال شده است و اگر صفر باشد یعنی غیر فعال شده است. توجه داشته باشید که این قسمت را قبلاً بررسی کردیم.

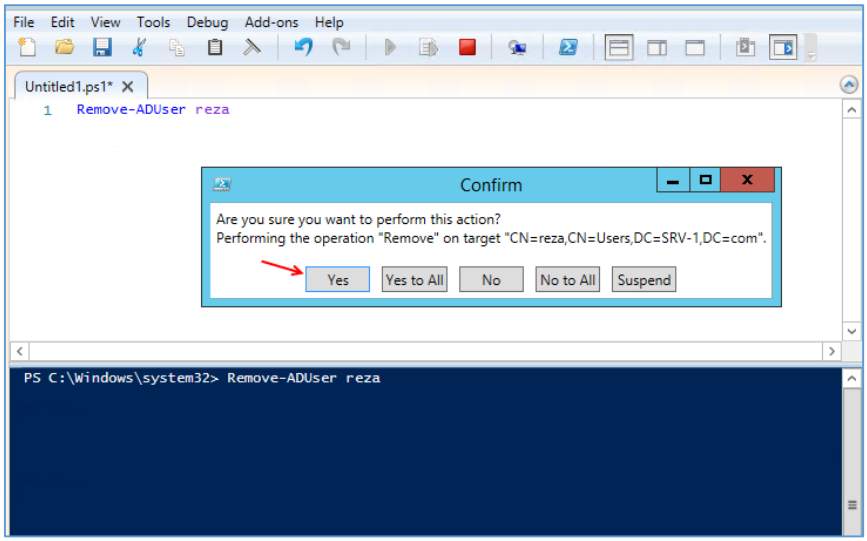


همان‌طور که در شکل مقابل مشاهده می‌کنید، گروه سازمانی مورد به درستی ایجاد شده است.

حذف users،Groups و Organization Unit از طریق Power Shell:

بعد از ایجاد کاربران و گروه های کاربری و سازمانی از طریق PowerShell، باید توانایی حذف آن را هم داشته باشیم؛ برای حذف یک کاربر از لیست Active Directory Users and Computers، باید از دستور زیر استفاده کنید:

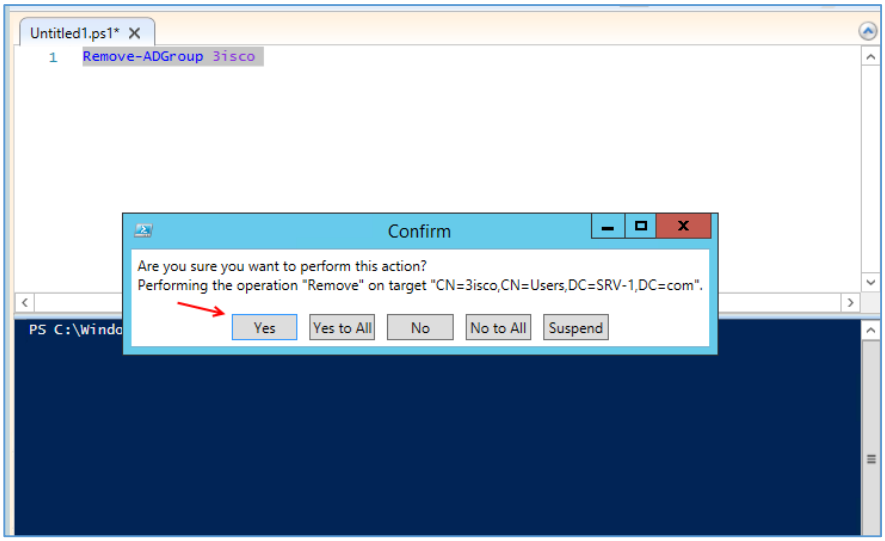
```
Remove-ADUser reza
```



بعد از اجرای دستور بالا در PowerShell، شکل روبرو ظاهر می‌شودکه از شما سوأل می‌شود که آیا می‌خواهید کاربر Reza را که در قسمت Users قرار دارد، حذف کنید؟ اگر بر روی Yes و Yes to All کلیک کنید، کاربر موردنظر حذف خواهد شد.

برای حذف گروه کاربری از دستور زیر در PowerShell استفاده می‌کنیم:

```
Remove-ADGroup 3isco
```

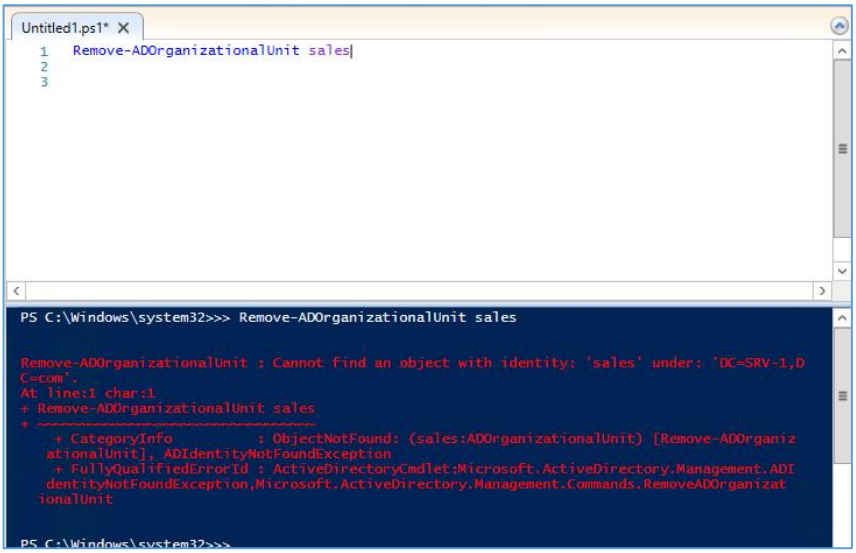


همان‌طور که در شکل روبرو مشاهده می‌کنید با دستور Remove-ADGroup و بعد از آن، نام گروه موردنظر و اجرای آن از شما سوأل می‌شود که گروه موردنظر را می‌خواهید حذف کنید یا نه؟

برای حذف واحدهای سازمانی باید از دستور زیر استفاده کنید:

```
Remove-ADOrganizationalUnit sales
```

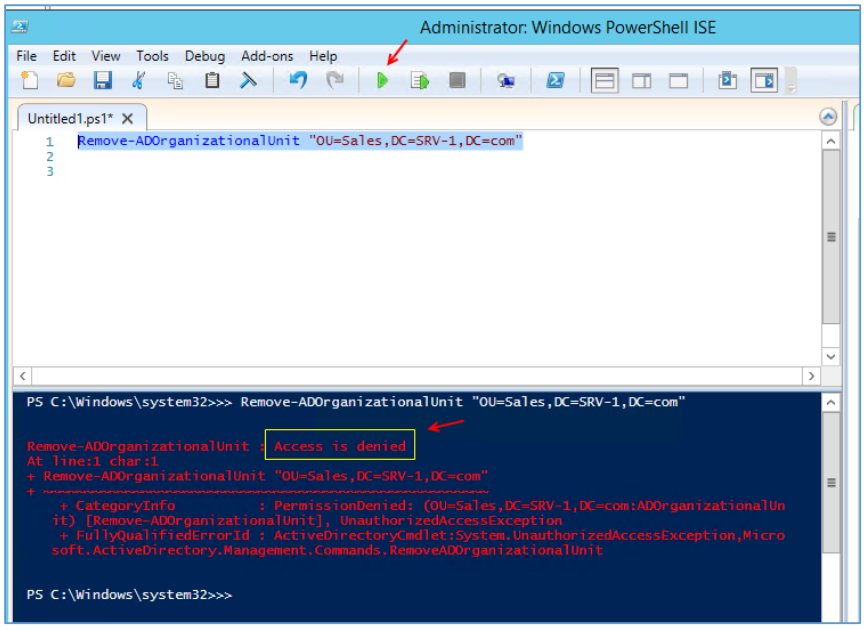
Sales، نام واحد سازمانی ما می‌باشد که در قسمت قبل ایجاد کرده بودیم و می‌خواهیم آن را حذف کنیم. بعد از اینکه دستور را اجرا کنید، با Error زیر مواجه خواهید شد.



در شکل روبرو، دستور مقابل با Error مواجه شده است. در این Error، به این نکته اشار شده است که شی موردنظر پیدا نشده است. برای حل این مشکل باید دستور مقابل را به صورت زیر تغییر دهیم تا Object یا شی موردنظر در دسترس باشد.

```
Remove-ADOrganizationalUnit "OU=Sales,DC=SRV-1,DC=com"
```

در دستور بالا، برای بدست آوردن شی Sales باید به این صورت عمل کنیم که داخل 2 تا "" باید نام OU=Sales و بعد کاما قرار دهیم و بعد DC=SERV-1 که نام دومین ما می‌باشد. بعد کاما و در آخر DC=Com را وارد می‌کنیم. این دستور به این صورت می‌باشد که باید نام واحد سازمانی و نام دومین را ذکر کنیم تا با خطا قبلی مواجه نشویم.

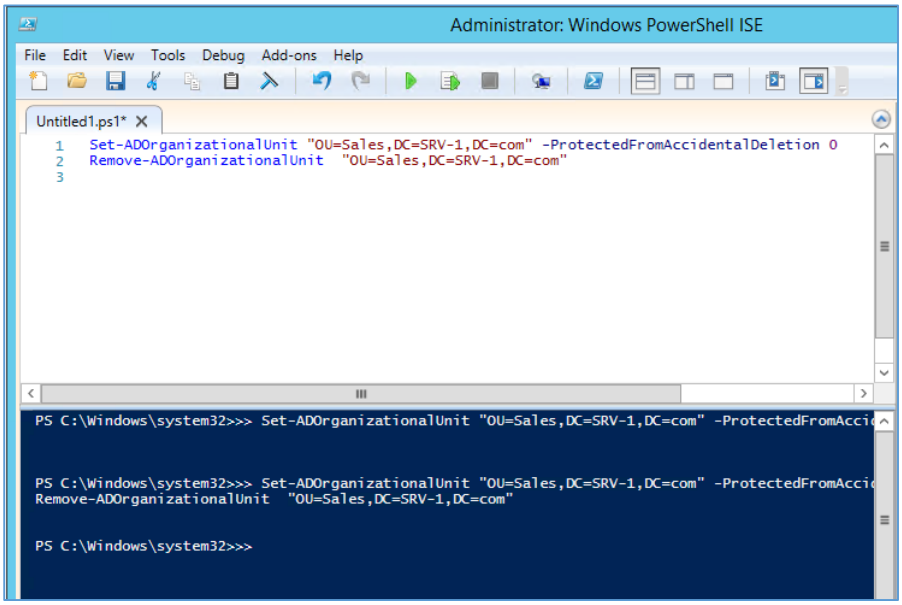


بعد از اجرای دستور موردنظر در PowerShell، با خطا مواجه شدیم که به این نکته اشاره دارد که دسترسی به شی موردنظر را نداریم. این مشکل به خاطر این است که در هنگام تعریف شی، آن را به صورت محافظت شده ایجاد کردیم. برای حل این مشکل، باید دستور محافظت کننده ی شی موردنظر را غیر فعال کنیم. برای این کار، ابتدا دستور زیر را اجرا می‌کنیم:

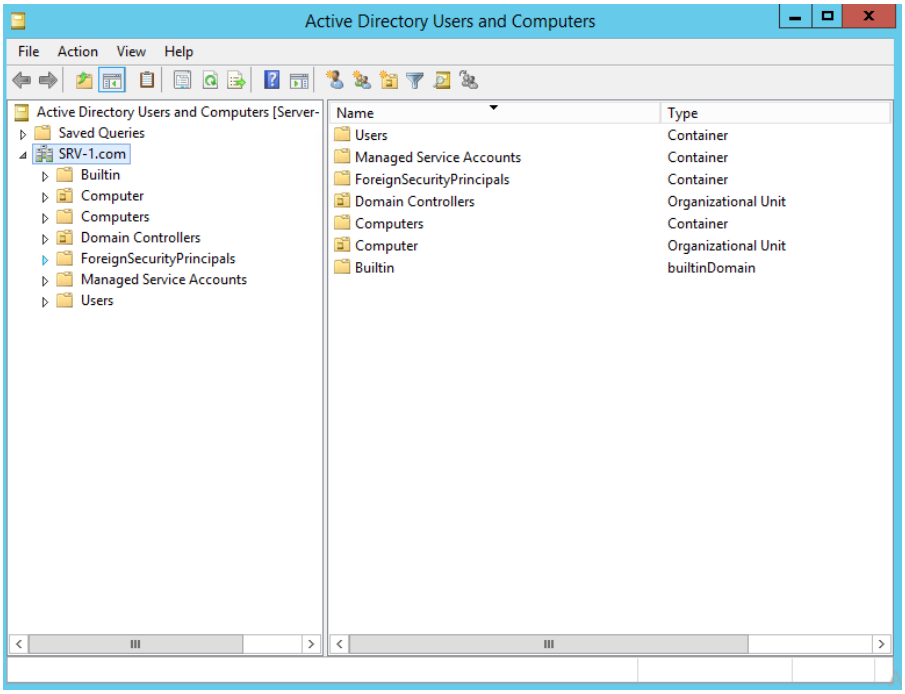
```
Set-ADOrganizationalUnit "OU=Sales,DC=SRV-1,DC=com" -ProtectedFromAccidentalDeletion 0
```

در دستور صفحه ی قبل، شی Sales را با دستور Set-ADOrganizationalUnit انتخاب کردیم و با دستور ProtectedFromAccidentalDeletion 0، محافظت کننده ی آن را غیر فعال کردیم. عدد صفر به معنی غیر فعال شدن می‌باشد.

بعد از اینکه شی موردنظر از حالت محافظت شده خارج شد، با دستور قبلی می‌توانیم OU یا واحد سازمانی را به راحتی حذف کنید.



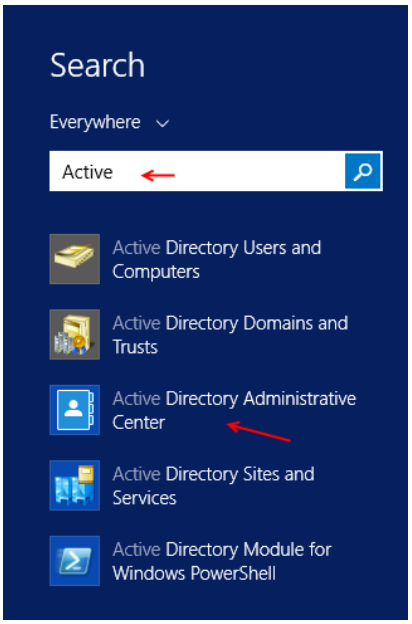
همان‌طور که در شکل روبرو مشاهده می‌کنید، دستورات به صورت پشت سر هم، در دو خط به صورت کامل اجرا شده و شی موردنظر به صورت کامل حذف شده است به همین سادگی و زیبایی.



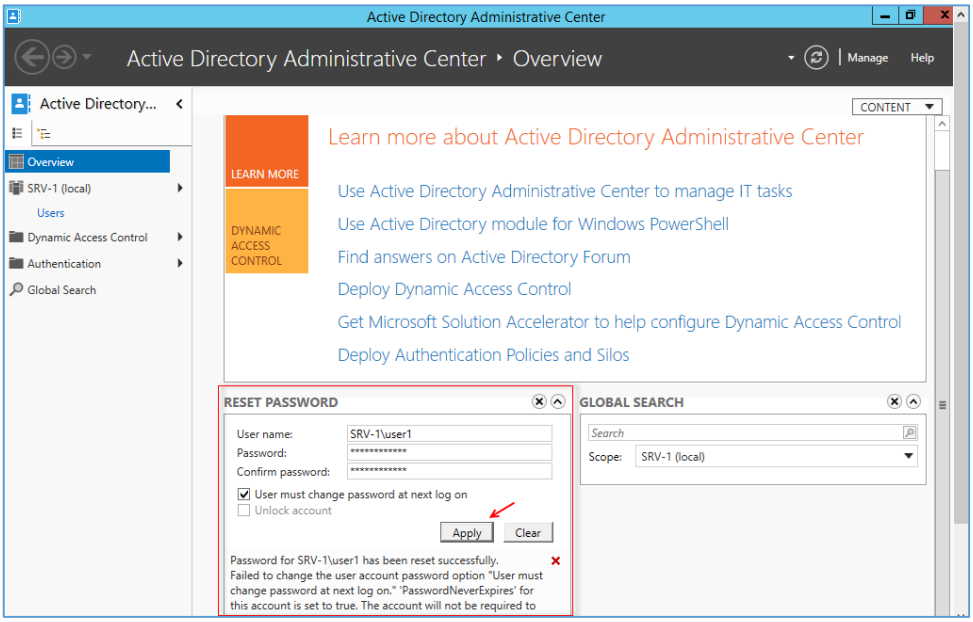
همان‌طور که مشاهده می‌کنید، گروه سازمانی با Sales به صورت کامل از لیست سرویس حذف شده است.

بررسی سرویس Active Directory Administrative Center:

این سرویس که از زمان معرفی ویندوز سرور 2008 ایجاد شده، این توانایی را به مدیر شبکه می‌دهد تا به آسانی بتواند گروه ها و کاربران و... خود را ایجاد و مدیریت کند.

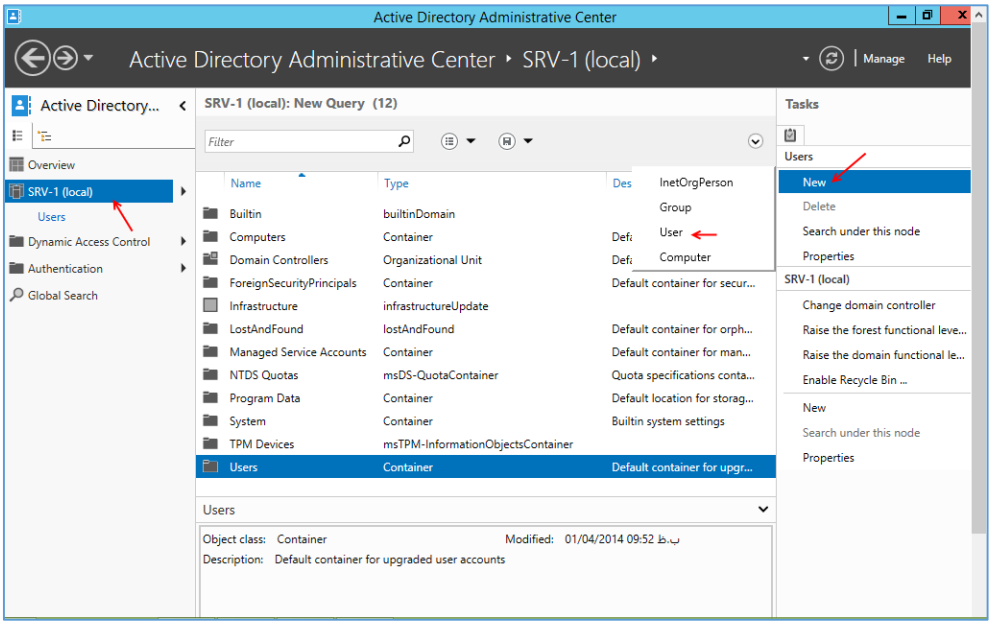


برای اجرای این سرویس، وارد Search ویندوز شوید و کلمه ی Active را وارد کنید و در گزینه های موجود، گزینه Active Directory Administrative Center را انتخاب کنید تا شکل بعد ظاهر شود.

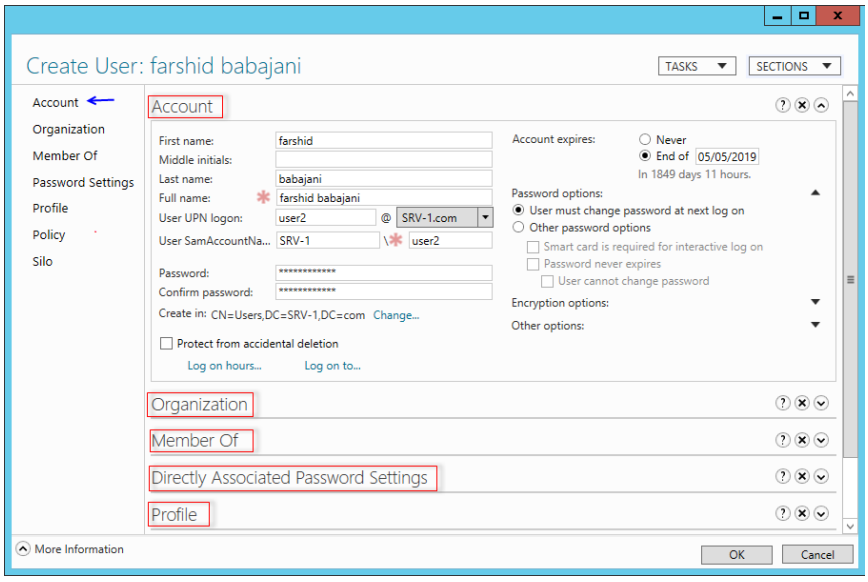


همانطور که در شکل روبرو مشاهده می‌کنید، سرویس موردنظر اجرا شده است، در صفحه ی اول یعنی، Overview بیشترین چیزی که به چشم می‌خورد، لینک های راهنمایی قرار دارد. شما می‌توانید با متصل شدن به اینترنت و کلیک بر روی هر یک از لینک‌ها، اطلاعاتی خوبی را دریافت کنید. در قسمت پائین، صفحه Reset Password وجود دارد که شما می‌توانید با وارد کردن اطلاعات کاربر موردنظر به مانند شکل و وارد کردن رمز جدید، رمز کاربر موردنظر را به

راحتی تغییر دهید. قسمت بعدی مربوط به Global Search می‌باشد که می‌توانید کاربران و گروه‌های موردنظر خود را جستجو کنید.

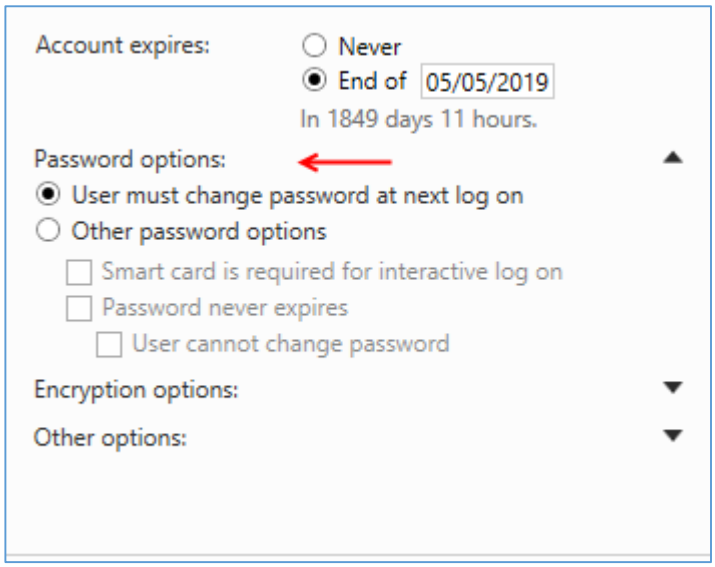


در قسمت بعد، به مانند شکل روبرو بر روی نام سرور (SRV-1) کلیک کنید تا لیست کامل اطلاعات برای شما نمایش داده شود. برای ایجاد کاربر جدید از سمت چپ بر روی New کلیک کنید و در منوی باز شده بر روی User کلیک کنید.



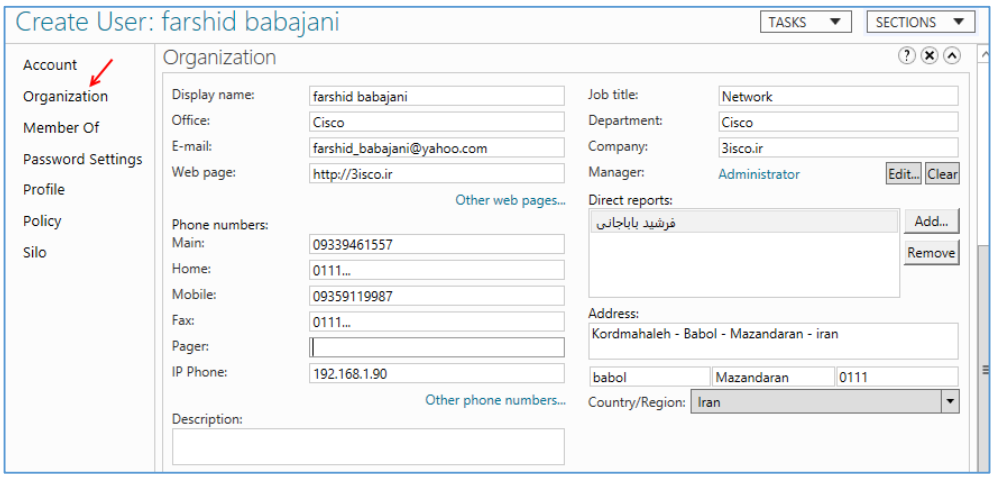
در این صفحه، هر یک از قسمت ها را با هم بررسی می‌کنیم. در قسمت Account، باید نام کاربر را در قسمت First name وارد کنید. نام فامیل آن را در قسمت Last Name وارد کنید که در قسمت Full name، نام کامل به صورت خودکار درج می‌شود. در قسمت User UPN logon که مهم‌ترین بخش می‌باشد، شما باید نام کاربری مربوط به کاربر موردنظر را وارد کنید که در اینجا user2 وارد شده است. این نام با نام هایی که در بالا وارد کرده اید تفاوت دارد و شما باید با این نام وارد سیستم شوید. در قسمت Password، یک رمز عبور به صورت پیچیده وارد کنید؛ یعنی به صورت Test@123456 که ترکیبی از حروف و ارقام و علائم می‌باشد؛ البته در درس‌های بعدی نحوه ی غیر فعال کردن پیچیدگی رمز عبور را با هم بررسی خواهیم

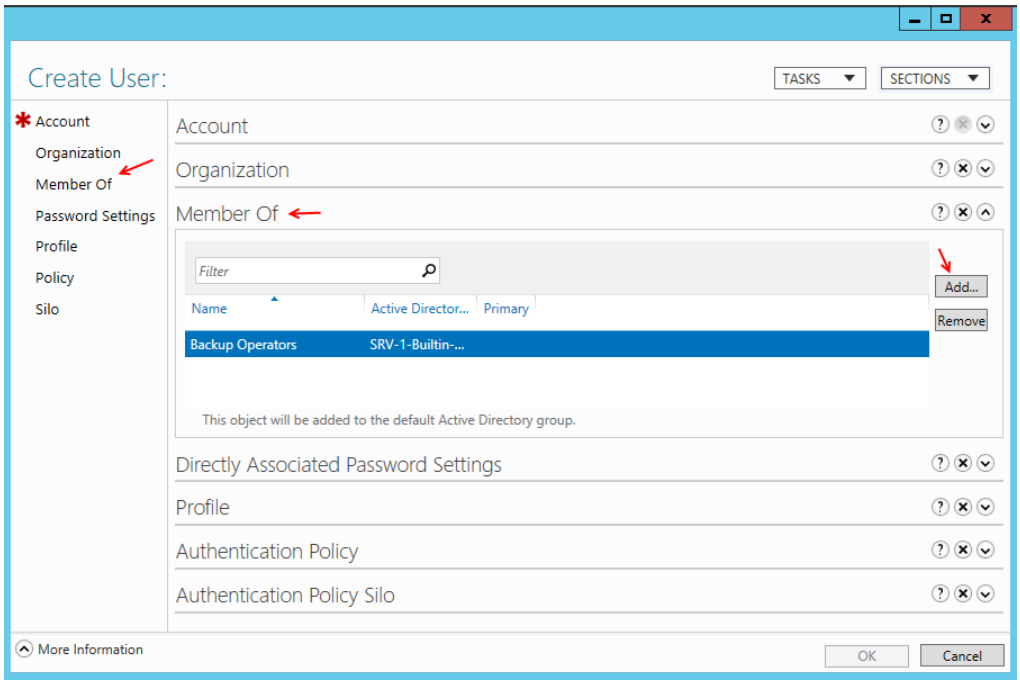
کرد. در قسمت Account Expire، تاریخ انقضای رمز عبور را برای کاربر موردنظر تعیین کنید و یا این قابلیت را با انتخاب گزینه ی Never، غیر فعال کنید. در قسمت Password options، گزینه ی User Must... به صورت پیش فرض انتخاب شده است که باعث می‌شود که کاربر در هنگام ورود، رمز دلخواه خود را وارد کند. اگر گزینه ی Other Password Options را انتخاب کنید، 2 گزینه، زیرمجموعه ی آن می‌باشند که با انتخاب گزینه ی Smart card...، کاربر باید در هنگام ورود از کارت الکترونیکی خود برای ورود استفاده کند و اگر گزینه ی Password Never Expire را انتخاب کنید رمز عبور به هیچ وجه انقضاء نخواهد شد و اگر گزینه ی User Cannot Change Password را انتخاب کنید، کاربر توانایی تغییر رمز عبور را نخواهد داشت و همان رمزی که شما برای آن قرار دادید، ثابت خواهد ماند.



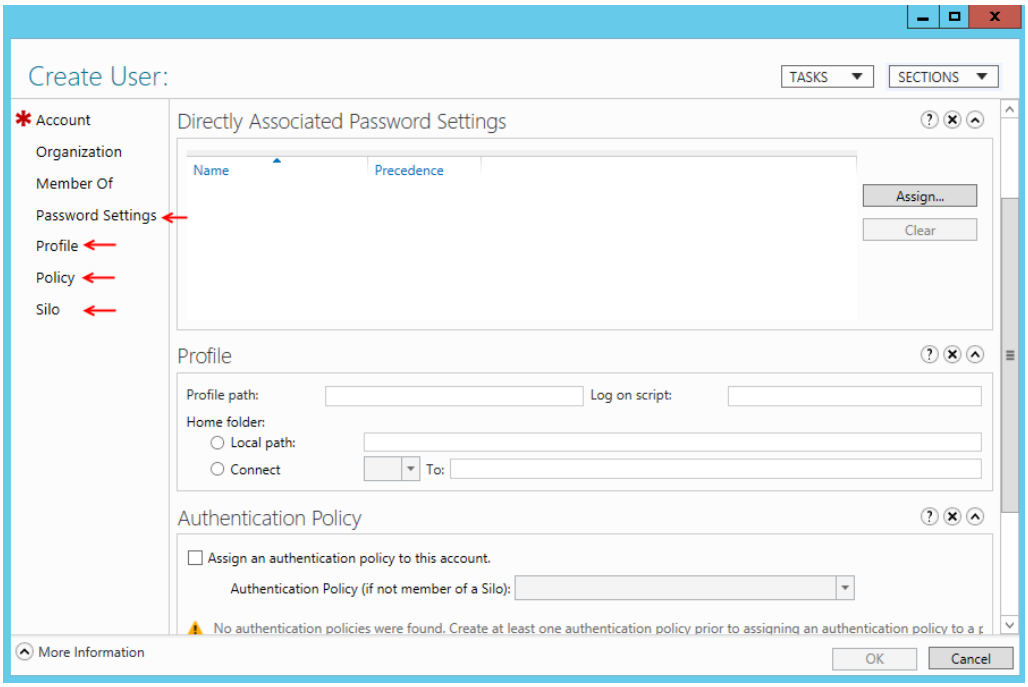
دو گزینه ی دیگر، با نام های Encryption options و Other options وجود دارد که برای رمز نگاری و فعال کردن الگوریتم رمز نگاری می‌باشد که در ادامه با آن کار خواهیم کرد.

در قسمت Organization یا همان واحد سازمانی می-توانید مشخصات کاملی از محل کار، آدرس، شماره تماس، وب سایت و ... را وارد کنید. سعی کنید این کار را برای هر کاربر انجام دهید تا اطلاعات کاملی از آن‌ها در اختیار شما باشد.



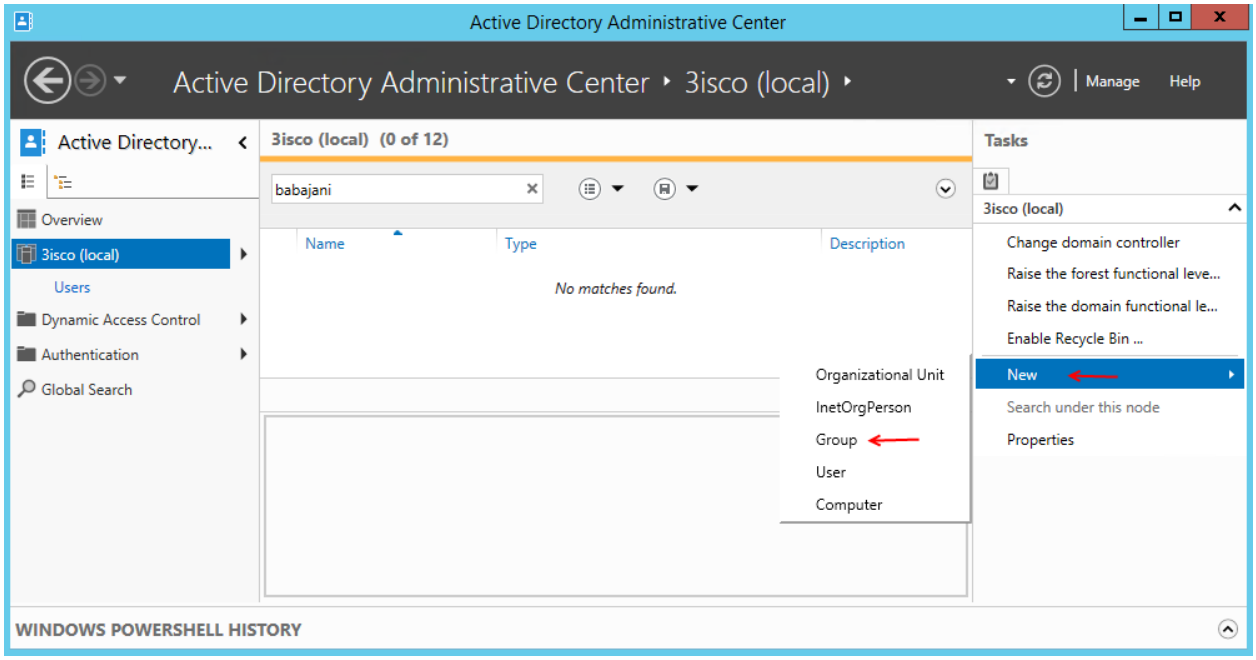


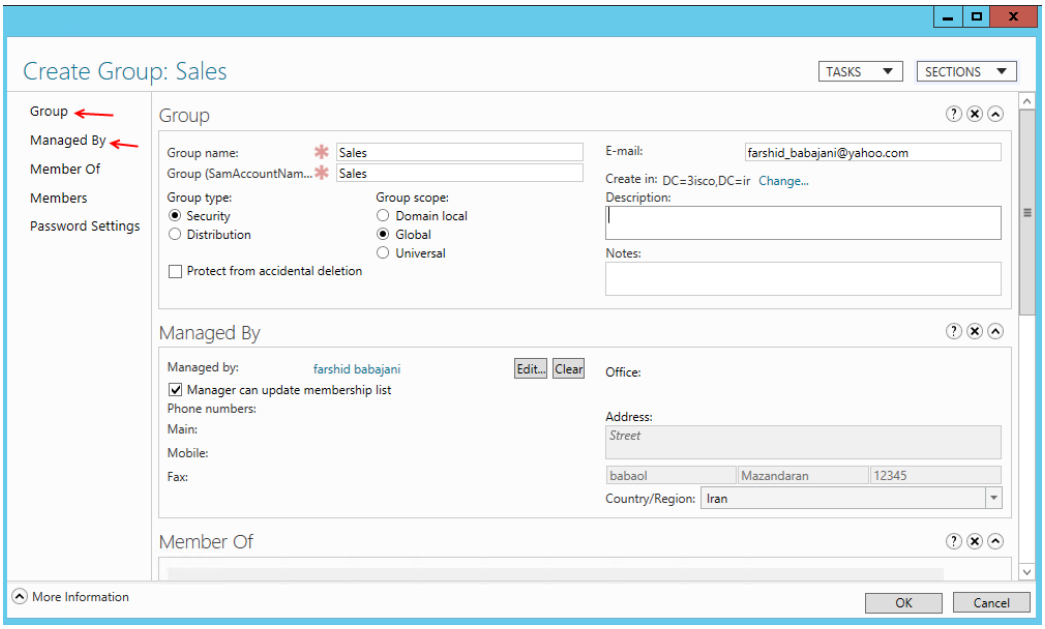
در قسمت Member Of، می‌توانید کاربر خود را عضو گروه خاصی کنید. برای این کار کافی است بر روی Add کلیک کنید و گروه موردنظر را مشخص کنید.



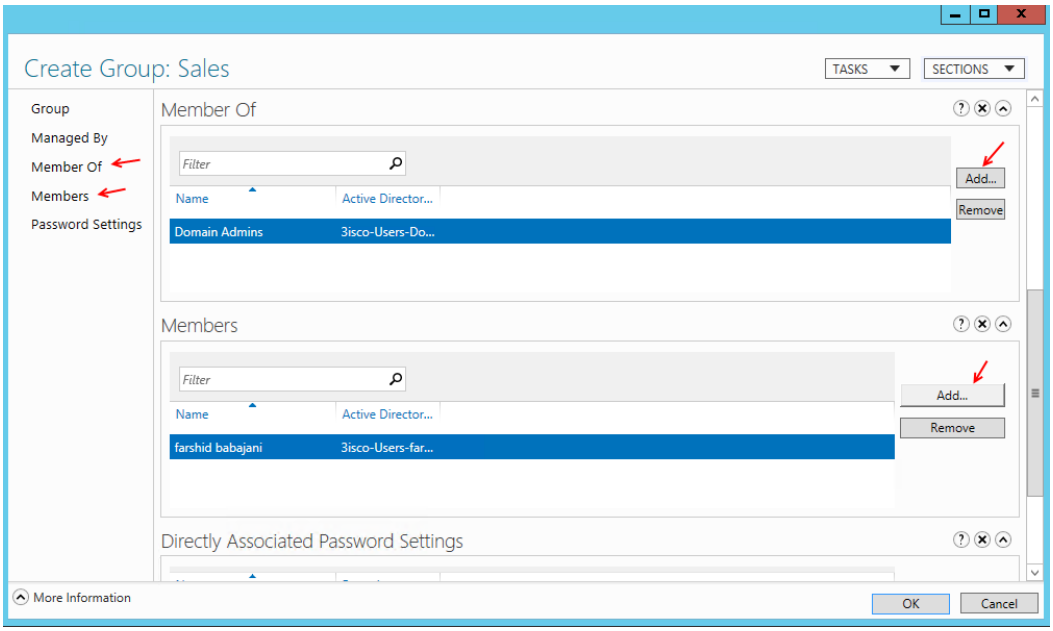
در قسمت Password Settings، باید یک Object برای Password ایجاد کنیم و به این قسمت متصل کنیم. Password Object، مشخص کننده ی حداکثر و حداقل رمز عبور و... می‌باشد. در مورد این موضوع، به صورت کامل و مفصل بحث خواهیم کرد. در قسمت Profile به مانند قبل می‌توانیم برای کاربران Profile و درایو مشخص ایجاد کنیم. قسمت‌های Policy و Silo برای تعریف احراز هویت و یا همان authentication برای کاربران می‌باشد که باید قبل از آن Policies مربوطه تعریف شود تا بتوان از این موضوع استفاده کرد.

بعد از ایجاد کاربر، نوبت به این می‌رسد که یک گروه جدید ایجاد کنیم؛ برای این کار مانند شکل زیر از سمت چپ بر روی نام دومین کلیک کنید و در صفحه ی باز شده از قسمت New گزینه ی Group را انتخاب کنید.



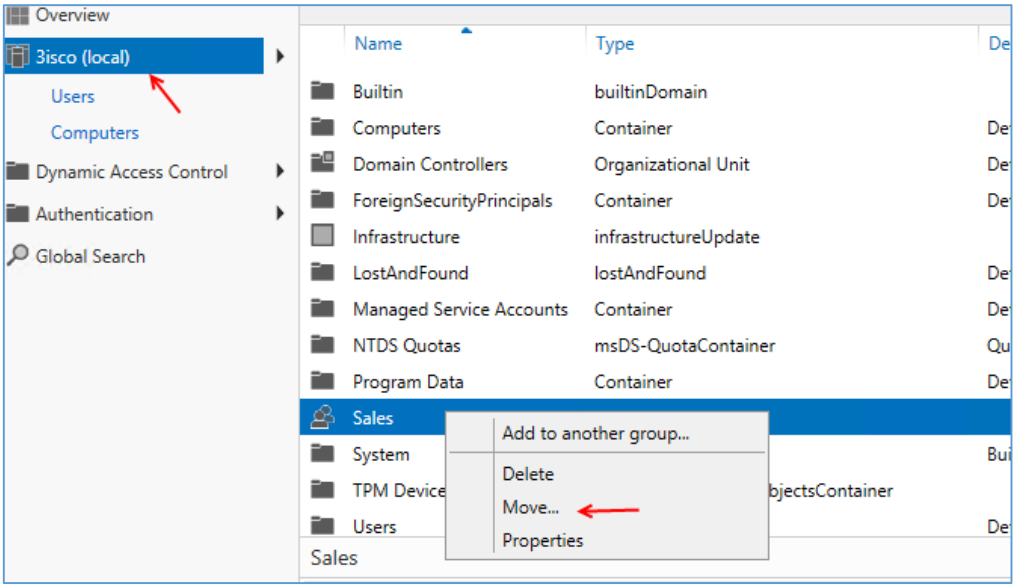


در این صفحه و در قسمت Group، باید نام گروه را در قسمت Group Name وارد کنید و در قسمت Group Type و GroupScope، نوع گروه و حوزه ی فعالیت آن را مشخص کنید که درباره ی این موضوعات قبلاً بحث کردیم. در قسمت Managed By می‌توانید یک کاربر را به عنوان مدیر این گروه مشخص کنید که با انتخاب گزینه ی Edit... می‌توانید کاربر موردنظر را انتخاب کنید و با انتخاب تیک گزینه ی Manager Can.... به کاربر موردنظر توانایی بیشتری را در مدیریت گروه موردنظر دهید.



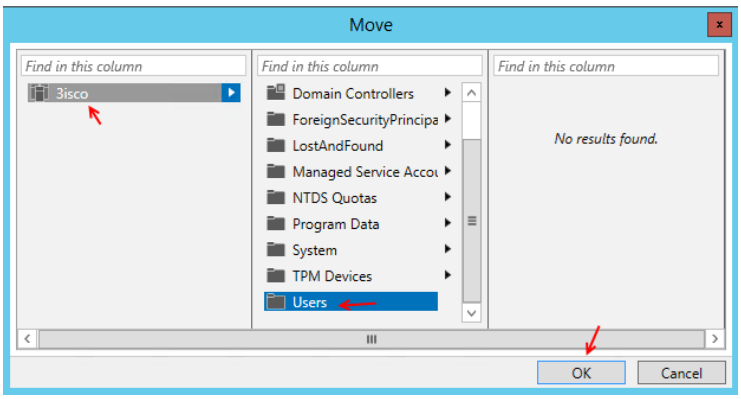
در قسمت Member Of، می‌توانیم این گروه را عضو گروه مشخص کنیم که این کار با کلیک بر روی Add امکان پذیر است و در قسمت Members می‌توانیم عضوهای این گروه را مشخص کنیم.

بر روی ok کلیک کنید تا کاربر موردنظر ایجاد شود.



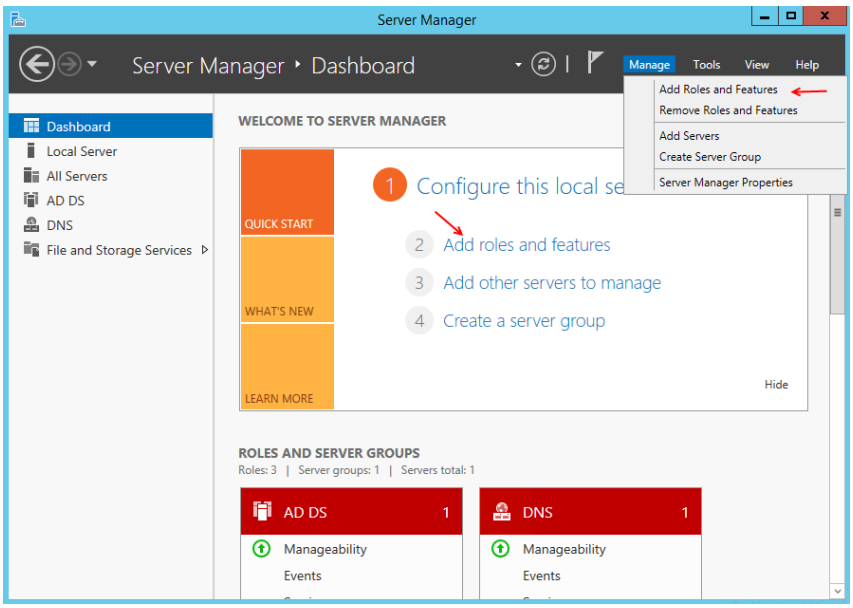
همان‌طور که در شکل روبرو مشاهده می‌کنید گروه موردنظر ایجاد شده است. برای اینکه کاربران و گروه های موردنظر خود را به جای دیگر انتقال دهید بر روی آن کلیک راست کنید و گزینه ی Move را انتخاب کنید.

در این قسمت باید لیست موردنظر و یا واحد سازمانی خود را انتخاب کنید تا گروه و یا کاربر موردنظر به قسمت موردنظر انتقال داده شود.

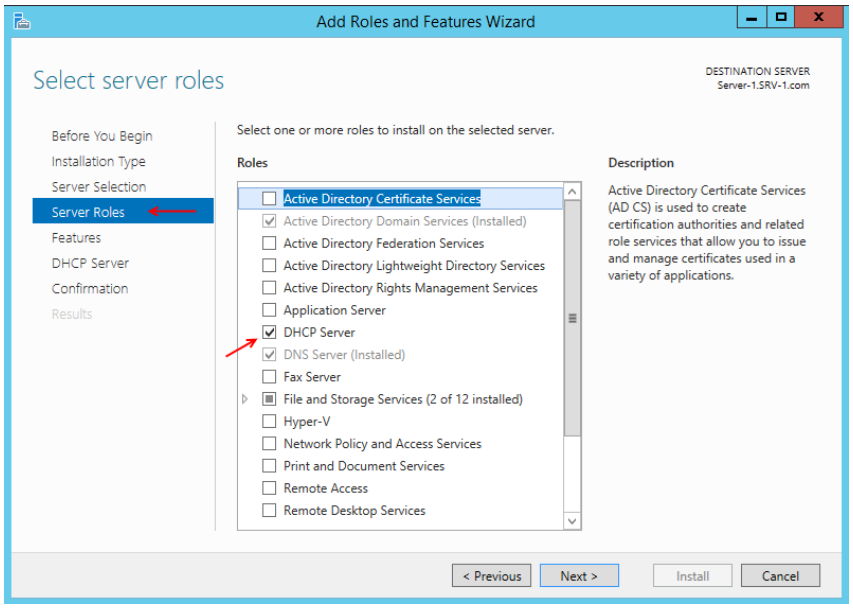


کار با سرویس DHCP:

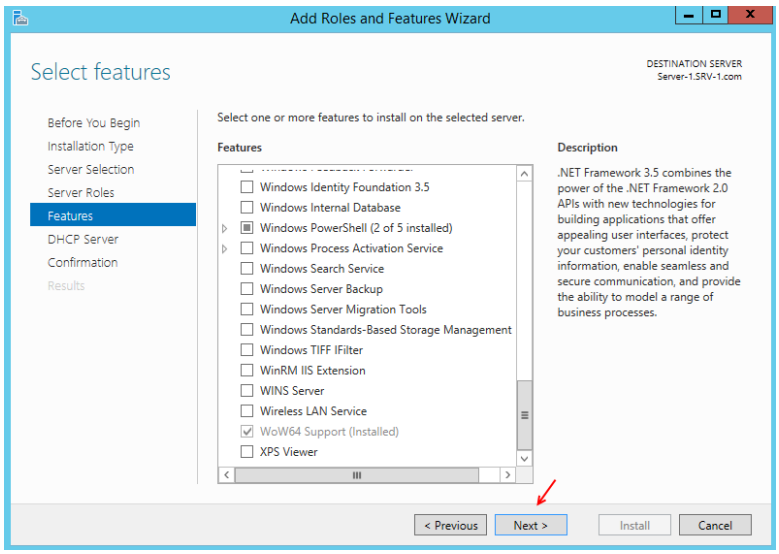
یکی از پرکاربردترین سرویس استفاده شده در شبکه های مختلف سرویس DHCP می‌باشد. این سرویس به صورت پویا به همه کلاینت های موجود در شبکه آدرس IP می‌دهد؛ مثلاً اگر در مجموعه ی شبکه ی خود 200 کامپیوتر داشته باشید، دیگر لازم نیست که پشت تک تک کامپیوترها بنشینید و IP وارد کنید؛ فقط کافی است سرویس DHCP را روی سرور اصلی فعال کنید و کامپیوترها را در حالت دریافت IP به صورت اتوماتیک قرار دهید. به همه ی کامپیوترها IP در رنج مشخص‌شده تخصیص داده خواهد شد. با هم این سرویس را نصب و راه اندازی می‌کنیم.



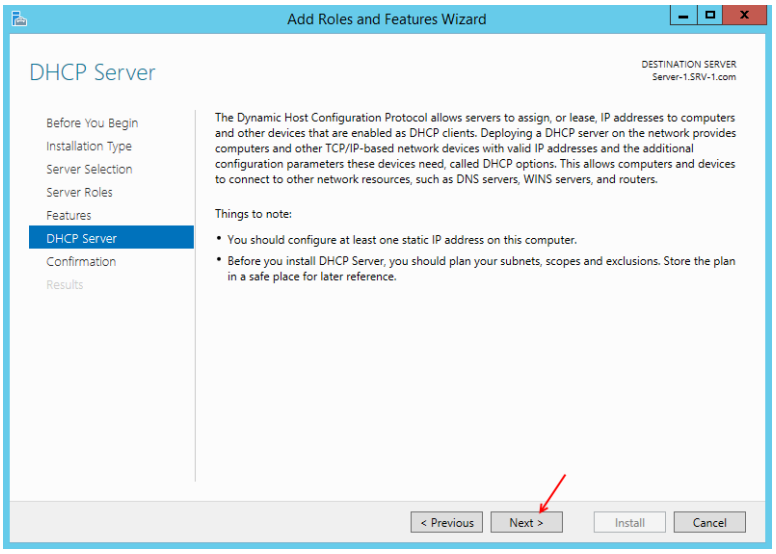
برای شروع باید سرویس DHCP را بر روی سرور اصلی خود نصب کنیم. برای این کار Server Manager را اجرا می‌کنیم و در صفحه ی باز شده به مانند شکل روبرو، بر روی Add roles and features کلیک می-کنیم. این کار را به دو صورت مشخص‌شده در شکل، می‌توان انجام داد.



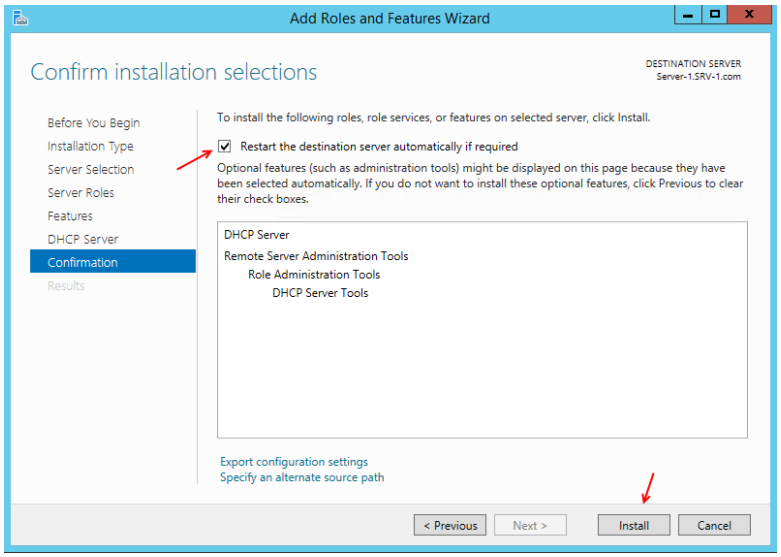
در صفحه‌ای که باز می‌شود بر روی Next کلیک کنید تا به قسمت Server Roles به مانند شکل روبرو برسیم. در این قسمت، سرویس DHCP را از لیست موجود، انتخاب و بر روی Next کلیک کنید.



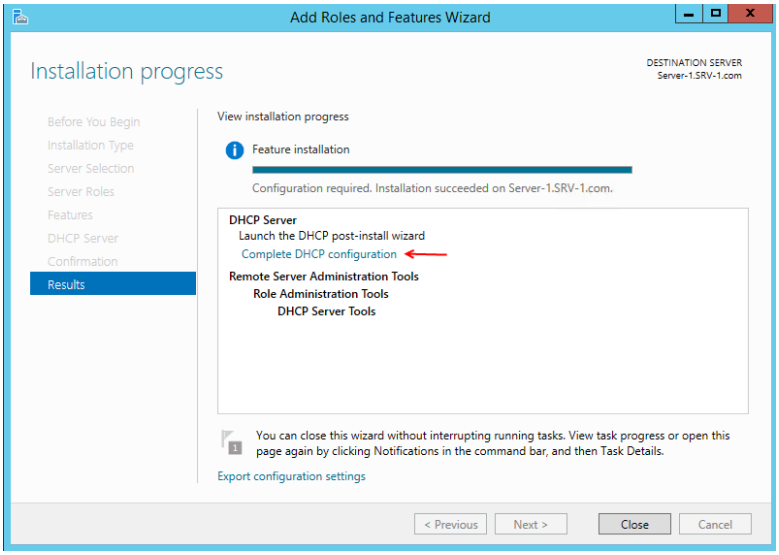
در این صفحه، به گزینه‌ای دست نزنید و بر روی Next کلیک کنید.



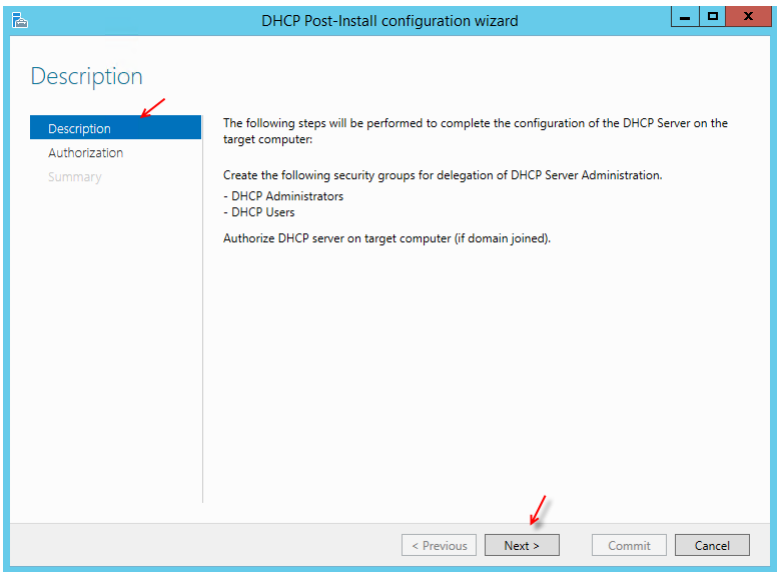
در این قسمت، توضیحاتی در مورد سرویس DHCP مشاهده می‌کنید که بعد از بررسی آن، بر روی Next کلیک کنید.



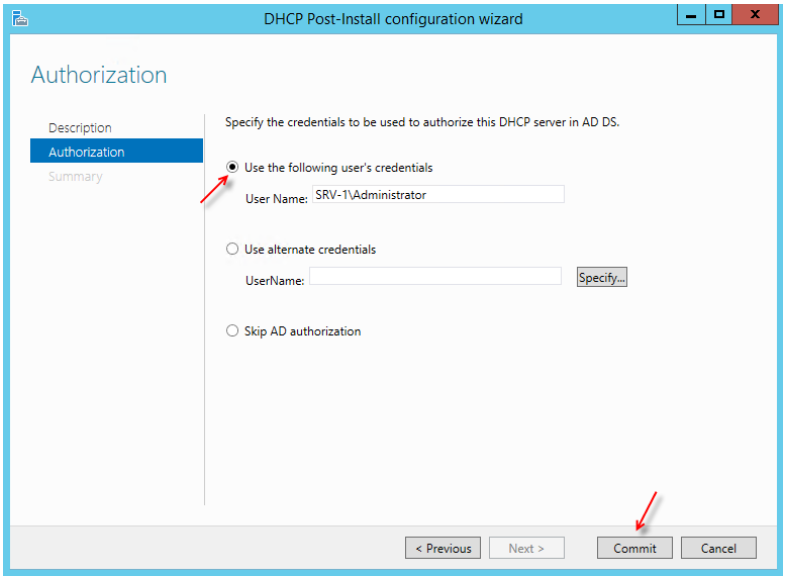
در این صفحه، تیک گزینه ی موردنظر را انتخاب کنید تا سرویس بعد از نصب به صورت اتوماتیک، Restart شود. برای نصب بر روی Install کلیک کنید.



بعد از اینکه سرویس به صورت کامل نصب شد، باید تنظیمات مربوط به سرویس را با کلیک بر روی Complete DHCP Configuration انجام داد. بر روی گزینه ی موردنظر کلیک کنید.

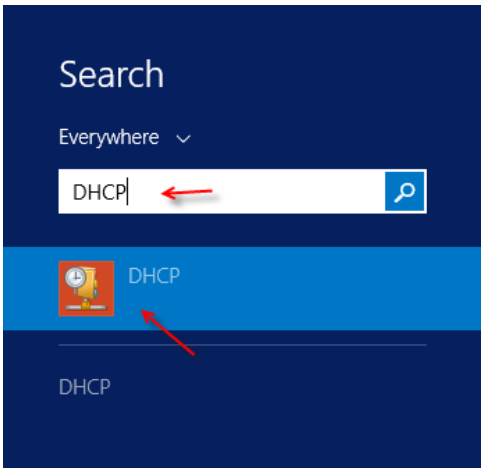


در این قسمت، توضیحاتی در مورد مدیریت سرویس DHCP می‌دهد که برای ادامه ی کار بر روی Next کلیک کنید.

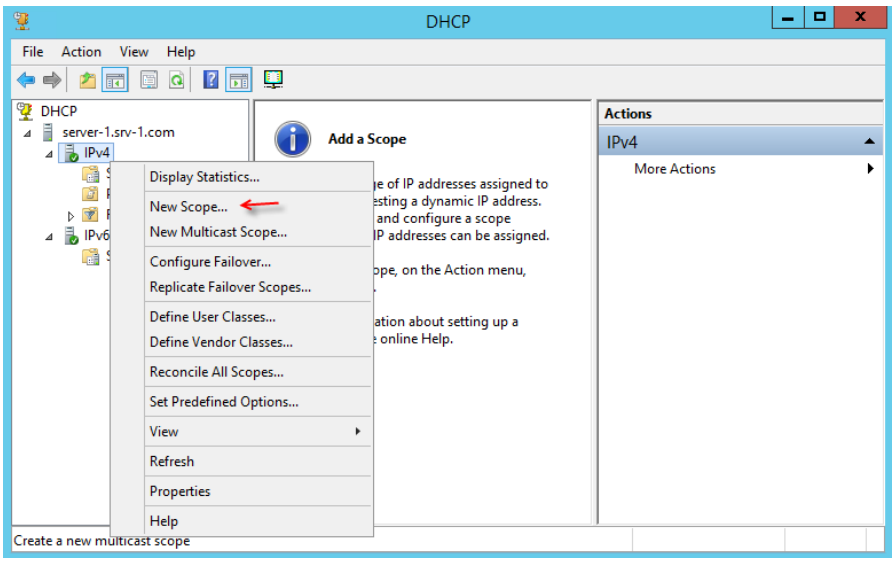


در این صفحه، شما باید مشخص کنید که چه کاربری بتواند وارد سرویس DHCP شود و تنظیمات مربوط به آن را انجام دهد. در قسمت اول می‌توانید کاربر موردنظر خود را که اصولاً Administrator می‌باشد را وارد کنید و در گزینه ی دوم می‌توانید کاربر دیگری را به عنوان نفر دوم معرفی کنید و یا گزینه ی سوم

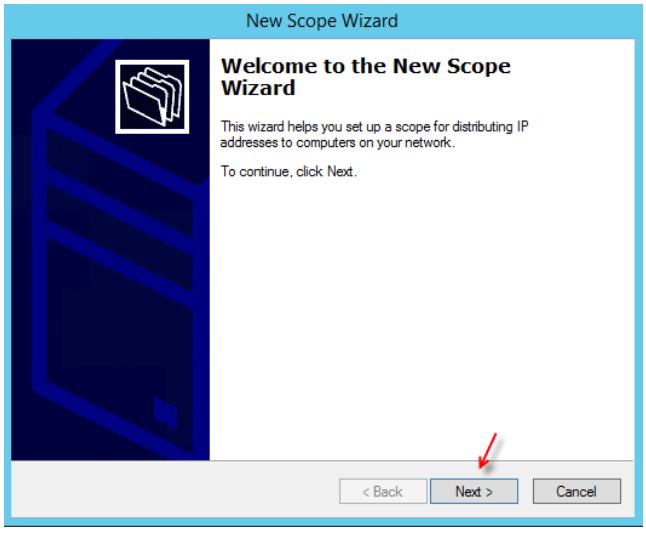
را انتخاب کنید تا عملیات Authorization انجام نشود که کار درستی از نظر امنیتی نیست. بر روی Commit کلیک کنید و اگر سیستم Restart نشد، خودتان سیستم را Restart کنید.



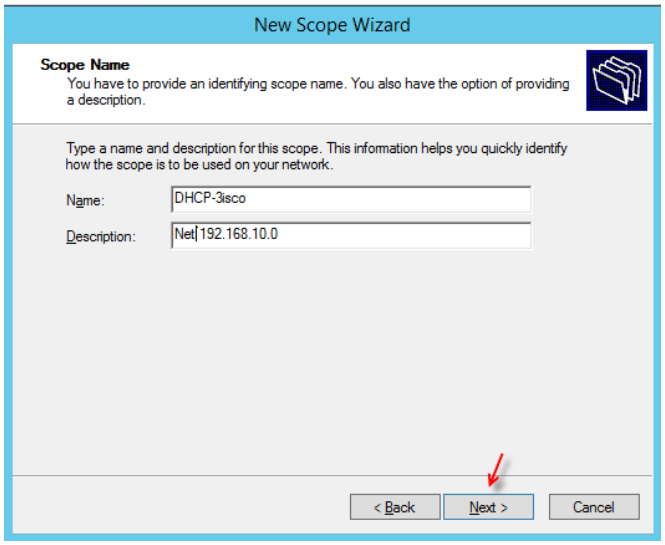
بعد از نصب سرویس DHCP، وارد Search می‌شویم و کلمه ی DHCP را وارد و سرویس DHCP را به مانند شکل روبرو اجرا می‌کنیم.



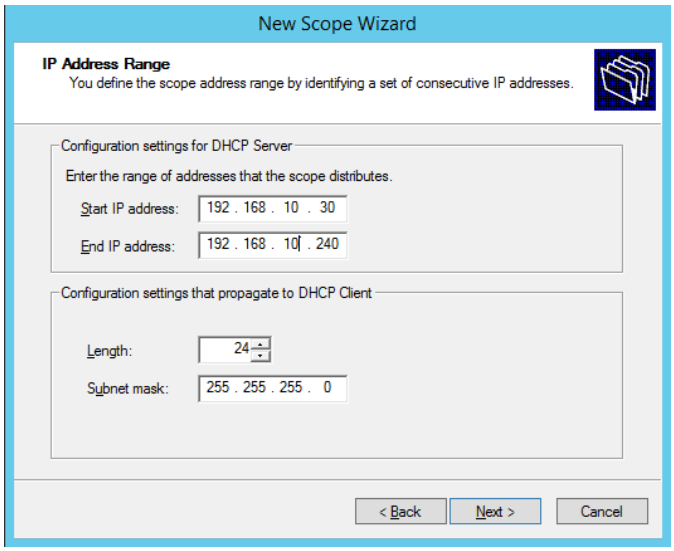
بعد از اجرای سرویس DHCP، باید برای شروع از محدوده ی موردنظر یک Scope برای رنج IP خود ایجاد کنیم. توجه کنید که به نسبت ورژن IP خود یکی از ورژن های IPV4 و IPV6 را انتخاب کنید. در این قسمت، بر روی IPV4 کلیک راست کنید و گزینه ی New Scope را انتخاب کنید.



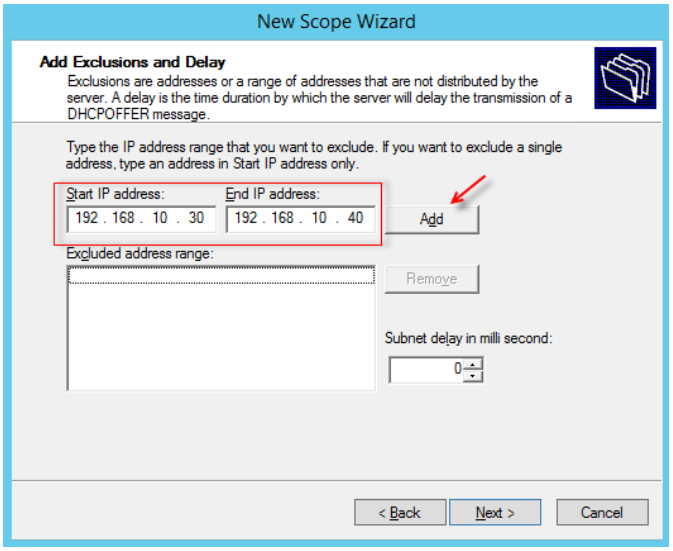
در این صفحه، بر روی Next کلیک کنید



در این صفحه، نام و توضیحاتی را برای سرویس خود وارد کنید و برروی Next کلیک کنید.

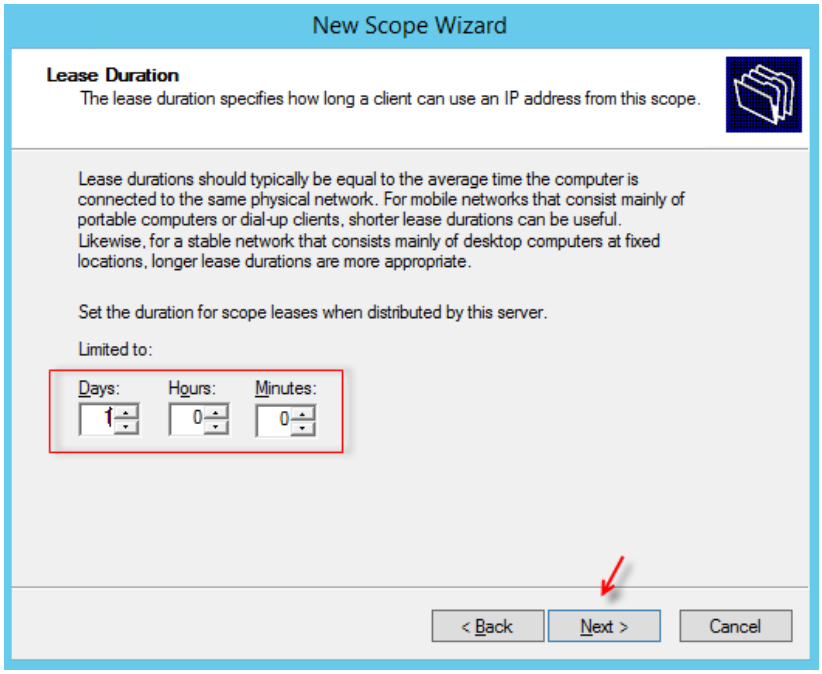


در این صفحه باید رنج IP و Subnet mask را معرفی کنیم. در قسمت Start IP address باید آدرس شروع که در اینجا 192.168.10.30 می‌باشد را وارد کنیم و در قسمت End IP address باید آدرس پایانی را که در اینجا 192.168.10.240 می‌باشد را وارد کنیم. در قسمت Length باید مقدار شبکه ی آدرس IP خود را مشخص کنیم که درباره ی Subnet mask در اول کتاب به صورت کامل توضیح دادیم. در این قسمت، عدد 24 را وارد می‌کنیم که subnet mask به صورت 255.255.255 تغییر خواهد کرد. بعد از این کار، بر روی Next کلیک کنید.

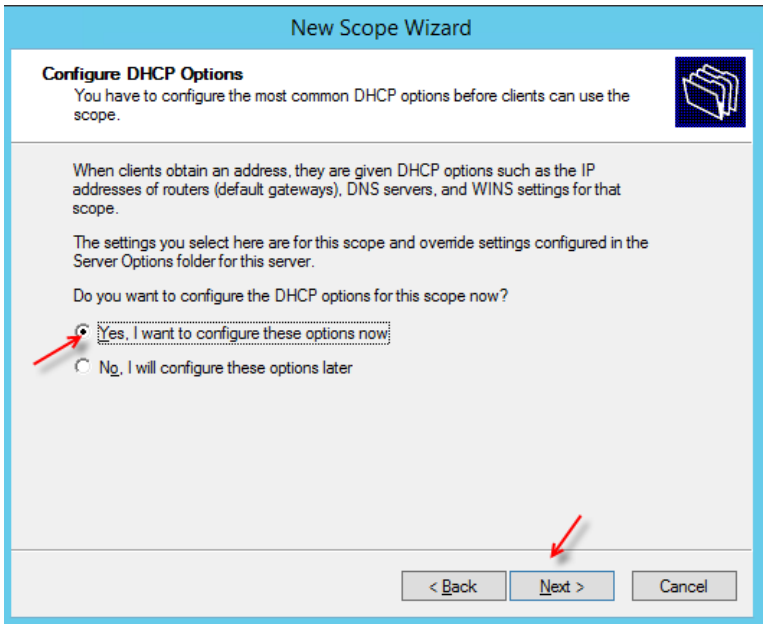


در صفحه ی روبرو که مربوط به قسمت Exclusions سرویس DHCP می‌باشد، به این منظور استفاده می‌شود که می‌توانید از بین رنج IP که در قسمت قبلی وارد کردید، رنجی را برای سرورها و کامپیوترهای خاص در نظر بگیرید؛ به این صورت که باید در قسمت Start و End، آدرس مشخص‌شده ی خود را وارد کنید که در اینجا تعداد

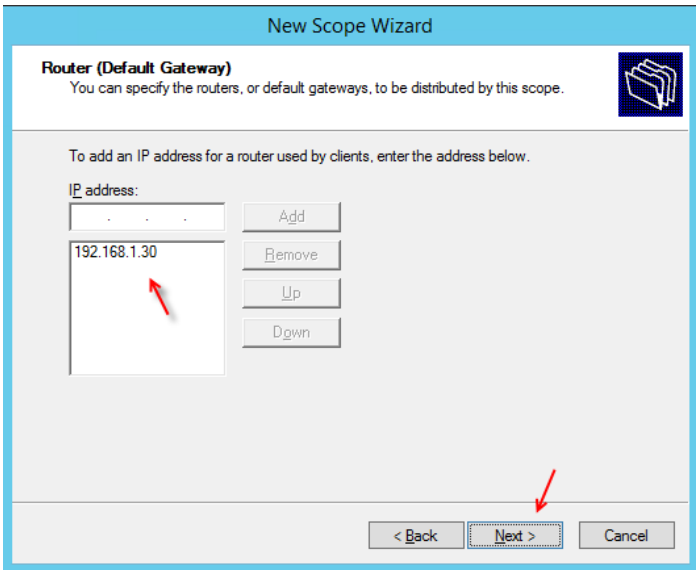
11 آدرس از آدرس اصلی جدا شده است؛ به این صورت که زمانی که سرویس DHCP می‌خواهد به کلاینت‌ها آدرس بدهد از آدرس 192.168.10.41 به بعد به همه آدرس می‌دهد و بقیه ی آدرس ها را در اختیار مدیریت قرارمی‌دهد. رنج IP مشخص‌شده در شکل صفحه ی قبل را وارد و بر روی Add کلیک کنید تا به لیست اضافه شود. برای ادامه ی کار بر روی Next کلیک کنید.



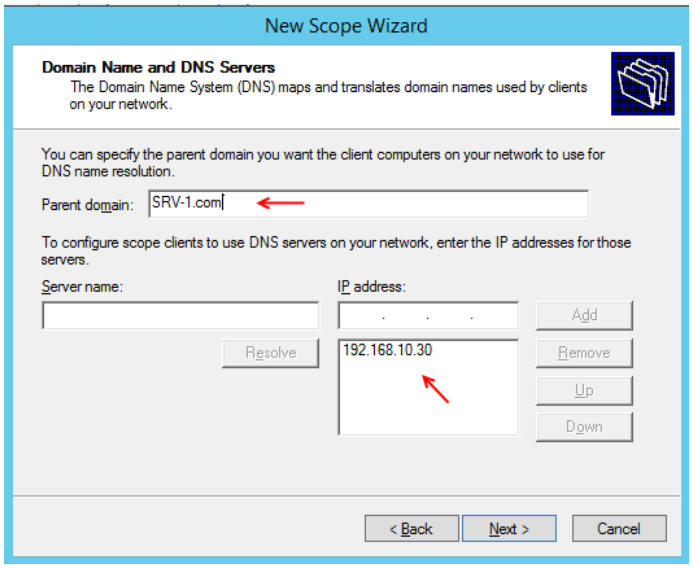
این صفحه، مربوط به این موضوع می‌باشد که زمانی که به یک کامپیوتر یک IP در رنج مشخص‌شده داده شد، اگر طبق زمان مشخص‌شده در این صفحه نتواند فعال شود، این IP از این کامپیوتر پس گرفته می‌شود و به کامپیوتر دیگر داده می‌شود؛ مثلاً اگر به یک کامپیوتر آدرس 192.168.10.41 داده شود، اگر چنانچه این کامپیوتر در زمان تعیین شده، خود را به سرویس DHCP معرفی نکند، این آدرس از وی پس گرفته خواهد شد. در این صفحه، در قسمت Day، تعداد روز، در قسمت Hours، تعداد ساعت و در قسمت Minutes، دقیقه را وارد و بر روی Next کلیک کنید.



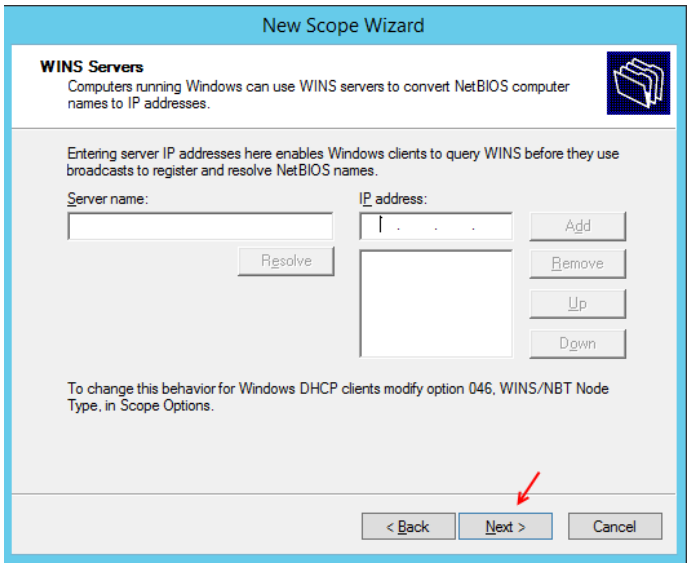
در این قسمت، بر روی گزینه ی Yes, I want to Configure ... کلیک کنید تا یک سری تنظیمات را با هم انجام دهیم.



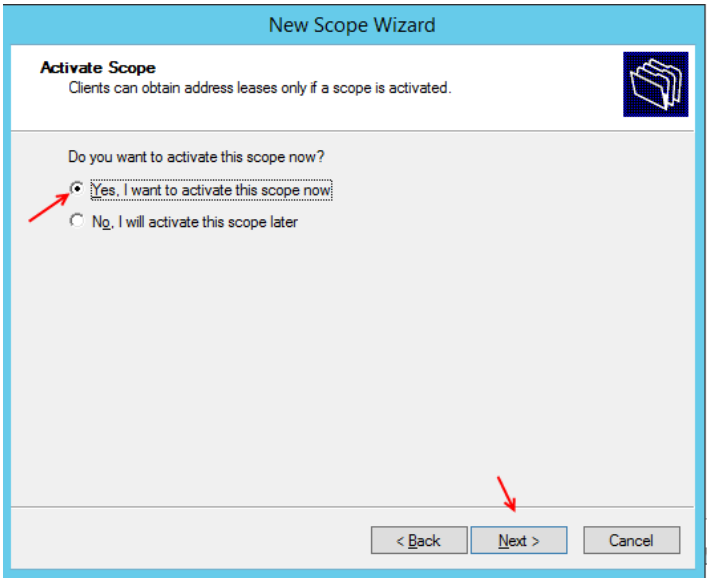
در این قسمت، باید آدرس Router و یا Default Gateway را معرفی کنیم. شاید نام Router و یا Gateway برای شما آشنا نباشد. این‌ها، پل ارتباطی با شبکه ی دیگر می‌باشند که بیشتر در شبکه های با ساختار دستگاه های روتر و سوئیچ مورد استفاده قرار می‌گیرند. برای دریافت آموزش کامل در باره ی روترها و سوئیچ‌ها در شبکه، کتاب CCNA بنده را مطالعه کنید. در این قسمت IP سرور را به عنوان IP روتر وارد می‌کنیم. در ادامه سعی می‌کنیم با این موضوعات بیشتر کار کنیم.



در این قسمت، باید نام سرور DNS و آدرس IP آن را وارد کنید. سرویس DNS برای تبدیل نام یک IP و برعکس می‌باشد. برای اینکه این موضوع را بهتر متوجه شوید، وارد CMD شوید و سایت 3isco.ir را Ping کنید تا متوجه شوید که بعد از اجرا، آدرس IP مربوط به این سایت را به ما نشان می‌دهد که آدرس آن 38.74.1.43 می‌باشد. در این صفحه، به صورت پیش فرض نام سرور اصلی و IP آدرس آن وارد شده است. بر روی next کلیک کنید.

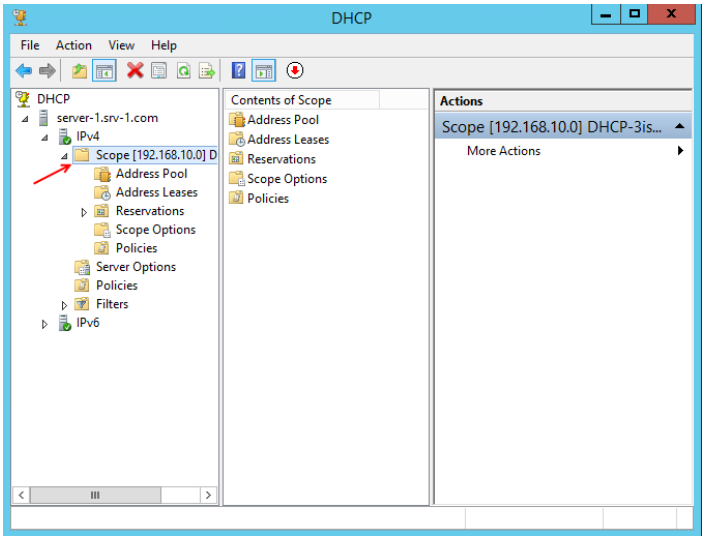


این صفحه مربوط به معرفی آدرس WINS Server می‌باشد. WINS Server، چیزی شبیه به DHCP است اما ضعیف‌تر از آن است. این سرویس مختص ویندوز-های مایکروسافت می‌باشد و برای تبدیل IP به نام دامنه کاربرد دارد. در ادامه ی کتاب با این سرویس بیشتر کار خواهیم کرد. در این صفحه چیزی وارد نکنید و بر روی NEXT کلیک کنید.

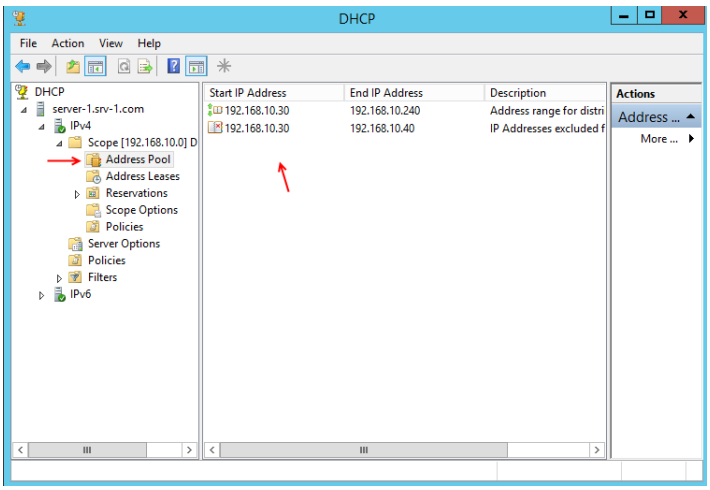


در این صفحه، گزینه ی اول را انتخاب کنید تا Scope موردنظر ما فعال شود.

بعد از این کار، بر روی Next کلیک کنید و در صفحه ی آخر بر روی Finish کلیک کنید.



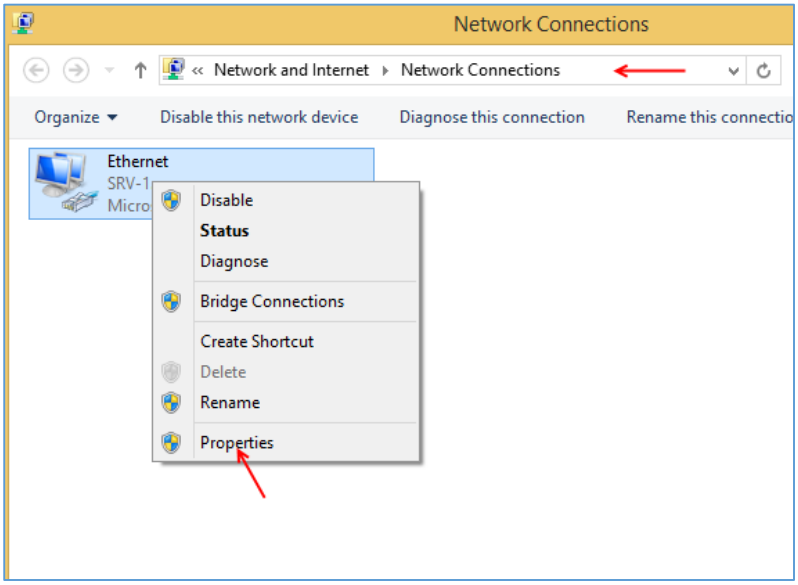
بعد از اتمام کار در قسمت قبل، Scope موردنظر به مانند شکل روبرو ایجاد شده است. اگر از سمت چپ بر روی Scope موردنظر خود کلیک کنید پنج گزینه ی متفاوت را مشاهده می‌کنید که هر کدام را با هم بررسی می‌کنیم.



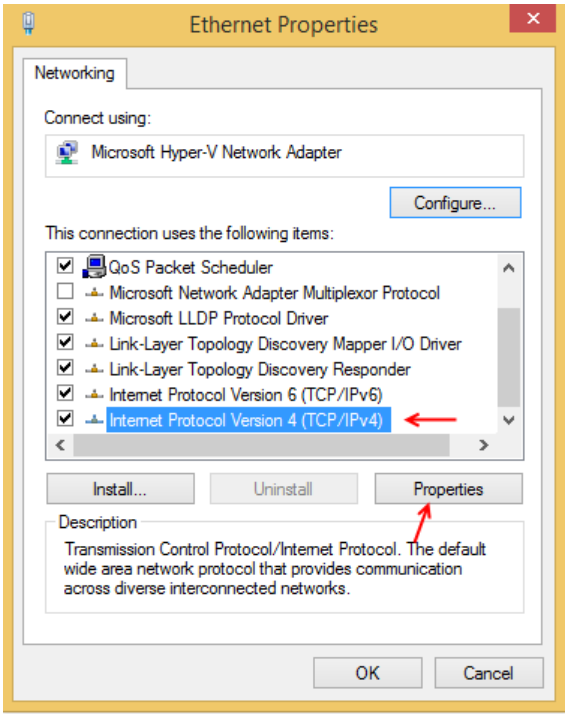
در این قسمت، بر روی Address Pool کلیک کنید. این قسمت، نشان دهنده ی رنج IP تعریف شده برای شبکه ی خود می‌باشد که این کار را در زمان ایجاد Scope انجام دادیم. توجه داشته باشید به هیچ عنوان نمی‌توانید رنج IP ایجاد شده را تغییر بدهید ولی می‌توانید آن را حذف کنید. گزینه ی دیگر به جز، رنج IP وجود دارد که نشان دهنده IP

Excluded می‌باشد که در زمان ایجاد Scope، آن را تعریف کردیم که نشان دهنده ی IP آدرس‌هایی است که از بقیه ی IP ها جدا شده و فقط مدیر شبکه می‌تواند از آن‌ها استفاده کند.

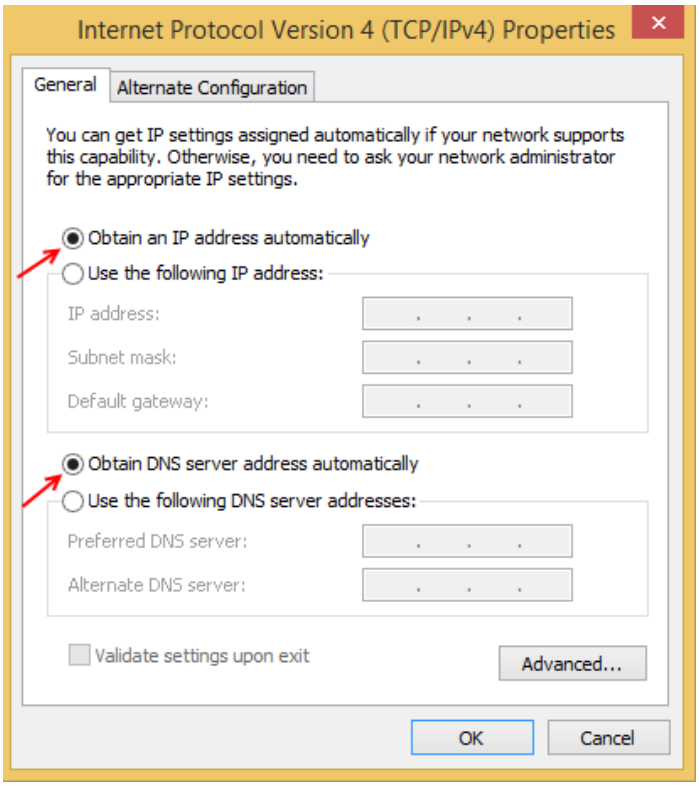
قسمت بعدی، مربوط به Address Leases می‌باشد. این قسمت مربوط به کلاینت هایی هستند که از طریق سرویس DHCP، آدرس IP دریافت کردند. با هم یکی از کلاینت ها را که روی آن ویندوز 8 نصب است را به سرویس DHCP متصل می‌کنیم.



وارد ویندوز 8 می‌شویم و به قسمت Network Connections مراجعه می‌کنیم و بر روی آیکون کارت شبکه کلیک راست می‌کنیم و گزینه ی Properties را انتخاب می‌کنیم.

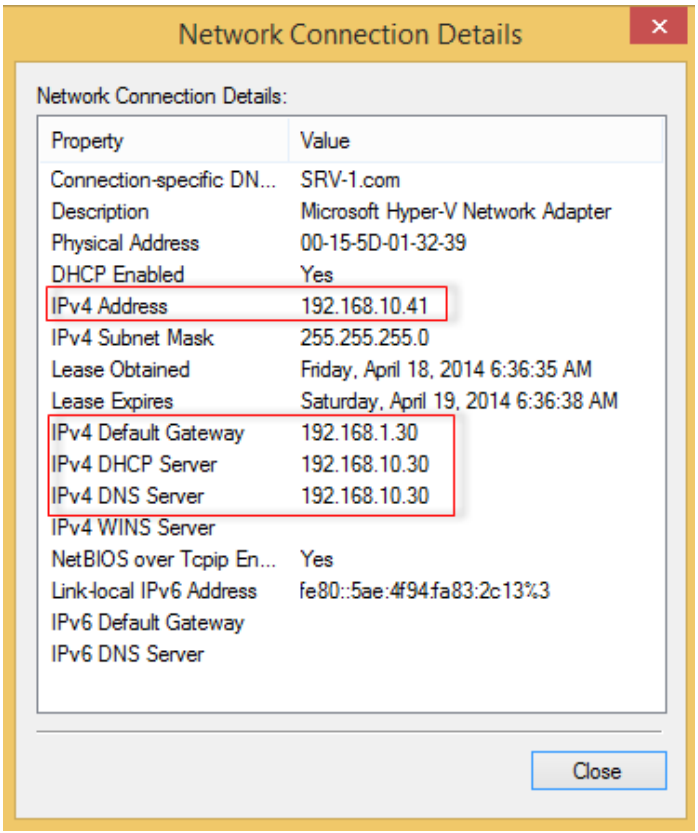


در لیست موجود بر روی Internet Protocol Version 4 کلیک کنید و بعد، بر روی Properties کلیک کنید.

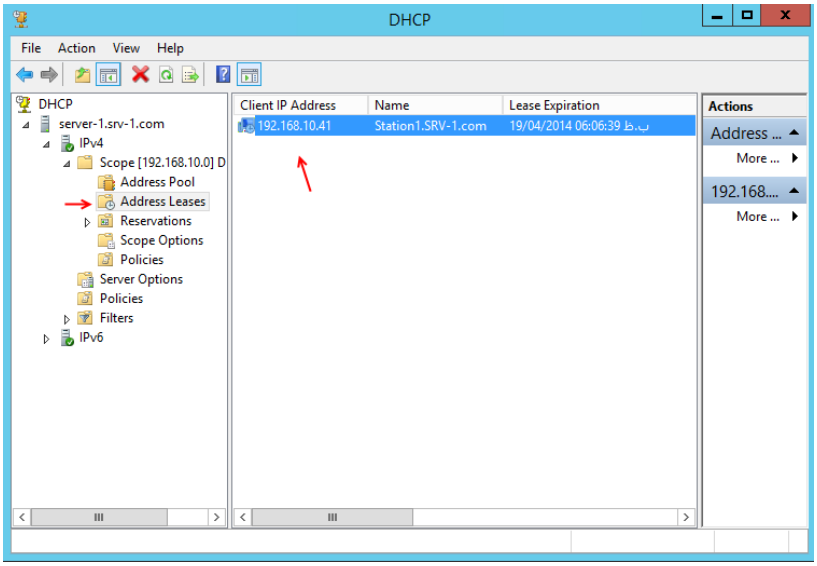


در این صفحه و در هر دو قسمت گزینه ی Obtain.. را انتخاب کنید تا کارت شبکه به صورت اتوماتیک از سرویس DHCP، آدرس IP دریافت کند. بر روی Ok کلیک کنید.

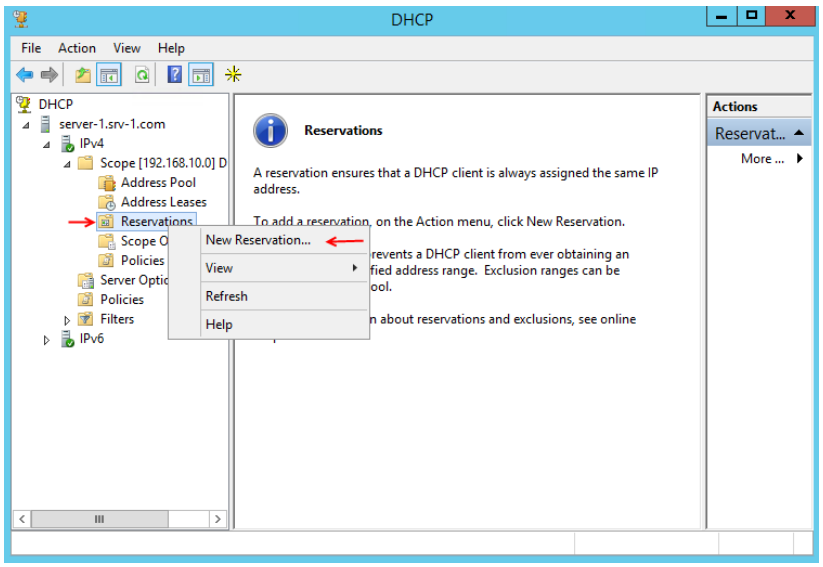
بعد از این کار، بر روی کارت شبکه دو بار کلیک کنید و در صفحه ی باز شده بر روی Details کلیک کنید تا شکل بعد ظاهر شود.



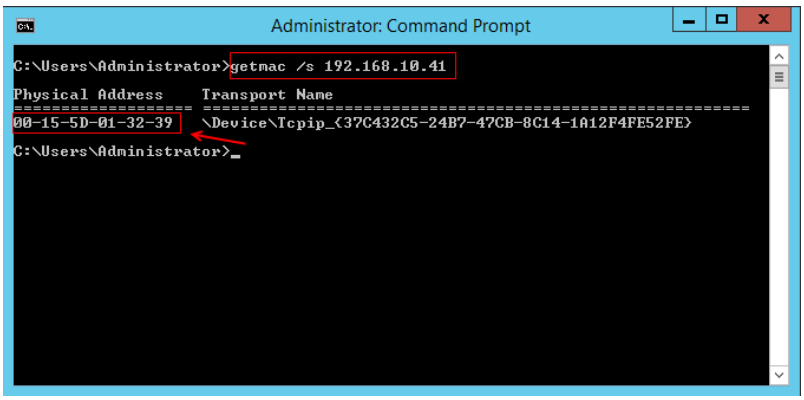
همان‌طور که در شکل روبرو مشاهده می‌کنید، کارت شبکه ی موردنظر از طریق سرویس DHCP، آدرس IP و آدرس سرور DNS و Router را به صورت کامل دریافت کرده است. توجه به آدرس IP داشته باشید که این آدرس از 192.168.10.41 شروع شده است؛ یعنی اینکه از آدرس 192.168.10.30 تا 192.168.10.40 به این کلاینت داده نشده است؛ چون قبلاً این آدرس ها را جدا کرده بودیم.



دوباره وارد ویندوز سرور 2012 شوید و سرویس DHCP را اجرا کنید و به مانند شکل روبرو وارد قسمت Address Leases شوید. همان‌طور که مشاهده می‌کنید، یک کلاینت به لیست اضافه شده است. این کلاینت، همانی است که در قسمت قبل از طریق سرویس DHCP، آدرس 192.168.10.41 را دریافت کرده است.



قسمت بعدی که در سرویس DHCP وجود دارد، بخش Reservations می‌باشد که قابلیت جالبی در این سرویس است که می‌توانید به یک کلاینت و دستگاه خاص که به شبکه متصل می‌شود، یک آدرس منحصر به فرد بدهید. این کار را با همکاری شما انجام می‌دهیم.

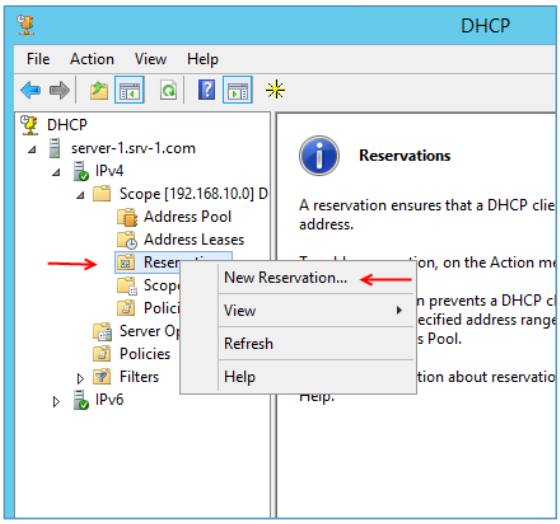


قبل از اینکه تنظیمات مربوط به این سرویس را انجام دهیم، باید Mac address مربوط به سیستم موردنظر را پیدا کنیم؛ وارد CMD می‌شویم و دستور زیررا وارد می‌کنیم:

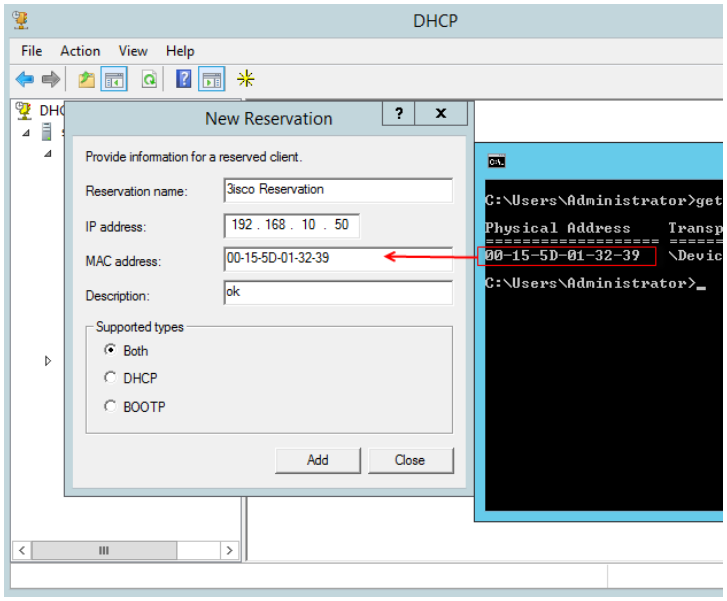
getmac/s 192.168.10.41

در این دستور، آدرس IP مربوط به سیستمی است که به شبکه ی ما متصل شده است و از طریق DHCP، آدرس IP دریافت کرده است. با این دستور، آدرس Mac کارت شبکه ی سیستم موردنظر را بدست آوردیم. روش

دیگر این است که وارد کامپیوتر موردنظر شویم و CMD را اجرا کنیم و دستور getmac را اجرا کنید تا Mac address کامپیوتر موردنظر را بدست آورید.

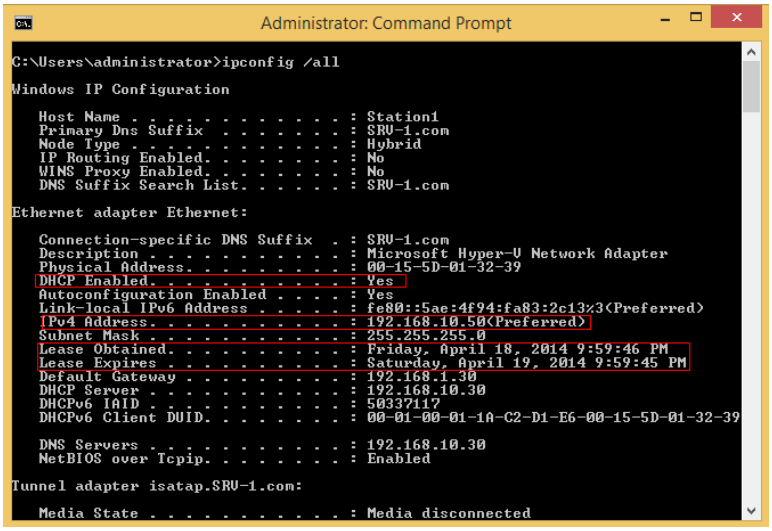


بعد از بدست آوردن Mac Address، وارد سرویس DHCP می‌شویم و روی قسمت Reservation کلیک راست کنید و گزینه ی New Reservation را انتخاب کنید تا شکل بعد ظاهر شود.

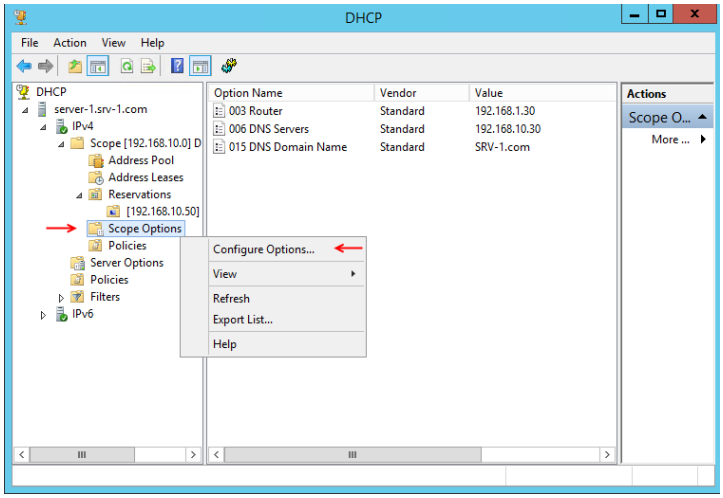


در این صفحه و در قسمت Reservation Name، نام دلخواه خود را وارد کنید. در قسمت Ip Address، آدرس IP دلخواه خود را که می‌خواهید به کلاینت موردنظر بدهید، وارد کنید؛ البته باید در رنج Scope تعریف شده باشد. در قسمت Mac address هم، آدرس Mac بدست آورده را وارد می‌کنیم که در شکل روبرو به طور واضح مشخص‌شده است. در قسمت Description توضیحاتی را وارد کنید و در قسمت Supported Type، گزینه ی Both را انتخاب کنید. در این قسمت، کلمه ی BOOTP را مشاهده می‌کنید که می‌توان گفت که این سرویس پدربزرگ سرویس DHCP می‌باشد و یک سرویس قدیمی در شبکه های قدیمی است.

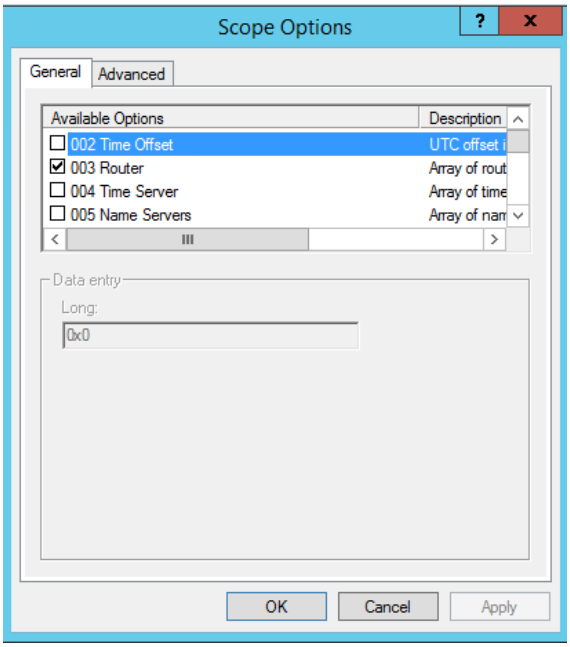
بعد از انجام کار، بر روی Add کلیک کنید تا کلاینت با آدرس موردنظر Reservation شود. بعد از این کار، وارد کلاینت موردنظر می‌شویم و دستور IPconfig /all را در CMD وارد می‌کنیم.



در شکل روبرو، دستور Ipconfig /all را وارد شده و اطلاعات مربوط به کارت شبکه ی موردنظر را در کلاینت موردنظر به ما نشان داده است. قسمت DHCP Enabled به صورت Yes می‌باشد و در قسمت IPV4 آدرس آدرس 192.168.10.50 که در سرویس DHCP فعال کرده بودیم را در این قسمت مشاهده می‌کنیم و در قسمت Lease، تاریخ و ساعت اختصاص دادن آدرس و تاریخ انقضای آن را مشاهده می‌کنید.



قسمت بعدی، مربوط به Scope Options و یا مشخصات Scope موردنظر می‌باشد. بر روی آن کلیک راست کنید و گزینه ی Configure Options را انتخاب کنید.



در این صفحه، دو تب وجود دارد که در تب اول، سرویس هایی است که برای Scope موردنظر می‌توانیم فعال کنیم و یا می‌توانیم آن‌هایی را که از قبل ایجاد کردیم را ویرایش کنیم؛ مثلاً می‌توانیم بر روی Router کلیک کنیم و آدرس آن را تغییر دهیم و یا در همین لیست بر روی DNS Server کلیک کنیم و آن را تغییر دهیم. تب Advanced برای کار با کلاس های خاصی است که در ادامه ی کتاب به آن خواهیم پرداخت. در ادامه ی کتاب به مباحث پیشرفته می‌پردازیم.

کار با DHCP از طریق دستورات PowerShell:

در این قسمت می‌خواهیم از طریق دستورات، سرویس DHCP را تنظیم کنیم و از آن استفاده کنیم.

اولین دستوری که با هم اجرا می‌کنیم، دستور Get-DhcpServerv4Scope است که با معرفی نام سرور، تعداد Scope های فعال شده روی آن را نشان می‌دهد.

Get-DhcpServerv4Scope -ComputerName Server-1

```
PS C:\Windows\system32> Get-DhcpServerv4Scope -ComputerName Server-1

ScopeId         SubnetMask      Name          State    StartRange      EndRange        LeaseDuration
-------         ----------      ----          -----    ----------      --------        -------------
192.168.10.0    255.255.255.0   DHCP-3isco    Active   192.168.10.30   192.168.10.240  1.00:00:00


PS C:\Windows\system32>
```

با اجرای دستور بالا، Scope قبلی که در سرویس DHCP، با نام DHCP-3isco ایجاد کردیم را به ما نشان داده است. در ادامه می‌خواهیم با اجرای دستور در PowerShell، یک Scope جدید ایجاد کنیم.

برای ایجاد Scope، باید از دستور Add-DhcpServerv4Scope استفاده کنیم؛ البته اگر از IP ورژن 6 استفاده می‌کنید، باید از دستور Add-DhcpServerv6Scope استفاده کنید. در این کتاب از IPv4 استفاده می‌کنیم.

با اجرای دستور زیر، یک Scope با نام PowerShell با تنظیمات مشخص‌شده ایجاد می‌شود، این دستورات را خط به خط با هم بررسی می‌کنیم.

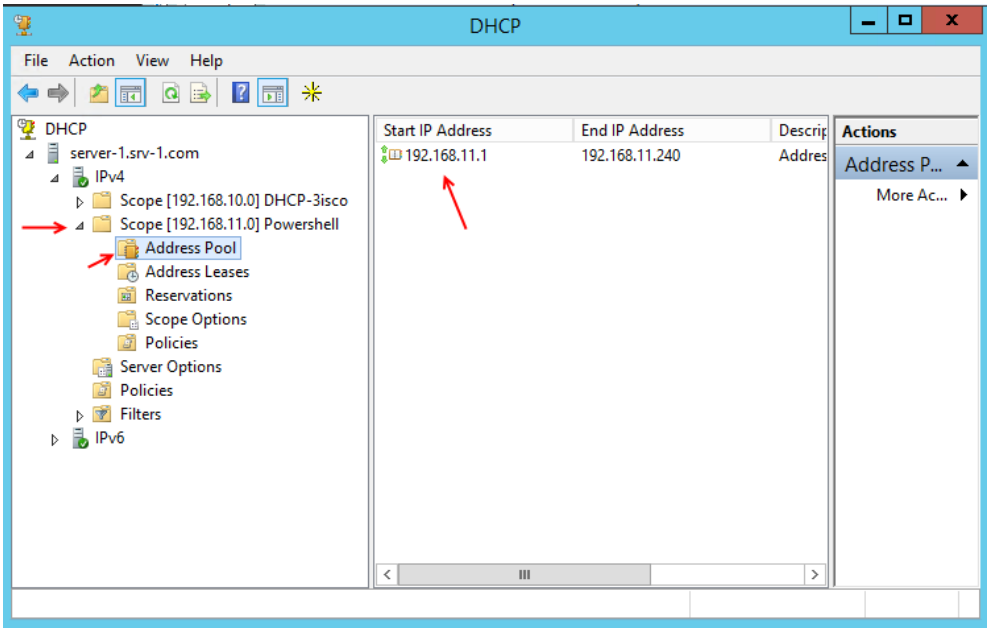
```
Add-DhcpServerv4Scope -Name Powershell -StartRange 192.168.11.1 -
EndRange 192.168.11.240 -SubnetMask 255.255.255.0 -State Active -
ComputerName Server-1 -Description "Powershell Scope" -Type Both
```

اولین دستوری که مشاهده می‌کنید، دستور Add-DhcpServerv4Scope می‌باشد که برای ایجاد Scope با IPV4 مورد استفاده قرار می‌گیرد. بعد از آن، باید تنظیمات مربوط به آن را انجام دهیم. اولین دستور بعد از آن- Name PowerShell می‌باشد که نام Scope را PowerShell در نظر می‌گیریم. شما می‌توانید هر نام دیگری

به جای آن وارد کنید، فقط توجه داشته باشید که اگر در نام خود از فاصله استفاده کردید حتماً نام موردنظر را بین دو دابل کوتیشن "" قرار دهید تا با Error مواجه نشوید. دستور بعدی 192.168.11.1 StartRange می‌باشد که نشان دهنده ی آدرس شروع Scope موردنظر می‌باشد. دستور بعدی هم EndEange 192.168.11.240 می‌باشد که آدرس پایانی آن می‌باشد و دستور بعدی،SubnetMask 255.255.255.0 است که Subnet آن را باید مشخص کنید. همان‌طور که قبلاً بیان کردیم، برای اینکه قسمت IP را متوجه شوید به ابتدای کتاب، قسمت بررسی IPV4 مراجعه کنید.

در ادامه، دستور State Active وجود دارد که برای فعال کردن Scope موردنظر می‌باشد. دستور بعدی ComputerName Server-1 است که باید به جای نام Server-1، نام کامپیوتر سرور خود را وارد کنید که زیاد هم مهم نیست. دستور Description- "Powershell Scope" هم برای ارائه ی توضیحاتی درباره ی Scope موردنظر می‌باشد که باید به جای "Powershell Scope" توضیحات خود را وارد کنید؛ البته باید توضیحات خود را بین دو دابل کوتیشن قرار دهید و در آخر هم باید نوع Scope خود را با دستور Type- Both مشخص کنید.

برای اجرای دستور، بر روی آیکون Run Script در بالای صفحه کلیک کنید. بعد از ایجاد Scope موردنظر، نگاهی به سرویس DHCP می‌اندازیم تا ببینیم که این Scope ایجاد شده است یا نه.



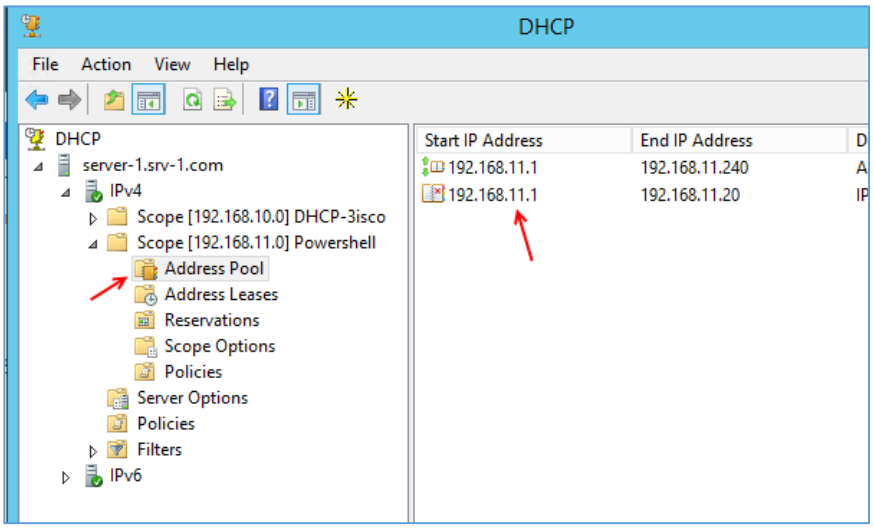
همان‌طور که در سرویس DHCP مشاهده می‌کنید، Scope با نام PowerShell و با آدرس 192.168.11.0 اضافه شده است و در Address Pool موردنظر End IP و Start IP مشخص‌شده است.

اگر متوجه باشید در قسمت Address Pool، آدرس Exclusion وجود ندارد و اگر قسمت های قبلی را به دقت خوانده باشید، Exclusion برای جدا سازی رنج IP از رنج IP اصلی برای کاربرد خاص است.

برای ایجاد IP Exclusion، وارد PowerShell می‌شویم و دستور زیر را اجرا می‌کنیم:

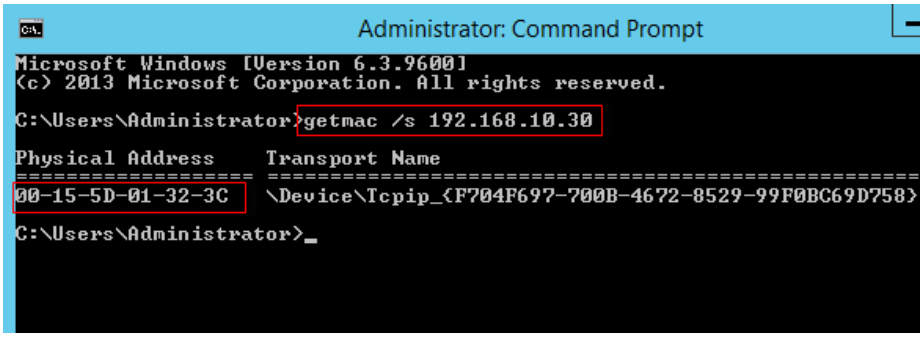
```
Add-DhcpServerv4ExclusionRange -ScopeId 192.168.11.0 -StartRange 192.168.11.1
-EndRange 192.168.11.20
```

برای ایجاد IP Exclusion از دستور Add-DhcpServerv4ExclusionRange استفاده می‌کنیم. بعد از آن باید ScopeId را به آن معرفی کنیم که ScopeId همان NetID مربوط به Scope موردنظر است که به صورت ScopeId 192.168.11.0– وارد می‌کنیم. در قسمت بعد، StartRange و EndRange را وارد می‌کنیم و دستورات را اجرا می‌کنیم.



همان‌طور که در شکل روبرو مشاهده می‌کنید، IP Exclusion به درستی وسط دستورات PowerShell ایجاد شده است.

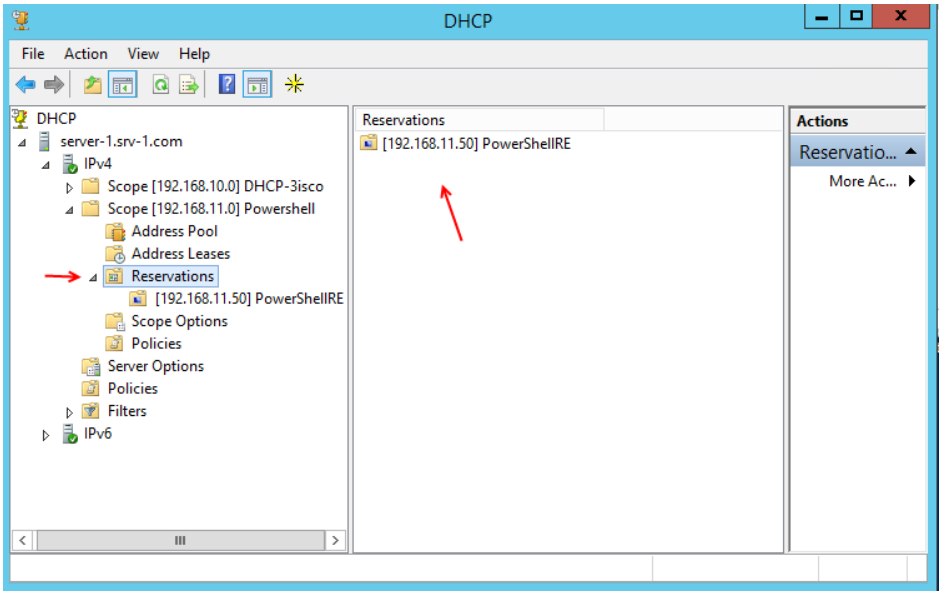
قسمت بعدی ای که باید از طریق دستورات، PowerShell ایجاد کنیم، قسمت Reservations می‌باشد که قبلاً این قسمت را در سرویس DHCP انجام دادیم.



برای ایجاد Reservations، باید Mac Address کامپیوتر موردنظر را بدست بیاورید؛ به مانند شکل روبرو از دستور getmac /s 192.168.10.30 استفاده می‌کنیم و آدرس MAC کامپیوتر موردنظر را که 00-15-5D-01-32-3C می‌باشد را بدست می‌آوریم و از آن در دستور زیر استفاده می‌کنیم:

```
Add-DhcpServerv4Reservation -ScopeId 192.168.11.0 -Name PowerShellRE -
IPAddress 192.168.11.50 -Type Both -ClientId 00-15-5D-01-32-3C
```

دستور Add-DhcpServerv4Reservation برای ایجاد Reservation مورد استفاده قرار می‌گیرد. بعد از آن باید از طریق ScopeId 192.168.11.0، آدرس NetID مربوط به Scope موردنظر را وارد کنیم که به جای 192.168.11.0، باید NetID مربوط به شبکه ی خود را وارد کنید. بعد از آن از طریق دستور Name PowerShellRE، یک نام برای آن در نظر می‌گیریم که شما باید به جای PowerShellRE، نام دلخواه خود را وارد کنید. در ادامه IPAddress 192.168.11.50 مربوط به کلاینت یا سرور موردنظر را وارد کنید و بعد، نوع آن را با دستور Type Both مشخص کنید. سپس در مهم‌ترین بخش که معرفی Mac address کلاینت یا سرور موردنظر است از طریق دستور ClientId 00-15-5D-01-32-3C، آدرس Mac مربوط به کلاینت موردنظر را وارد کنید و در آخر کار دستور موردنظر را اجرا کنید.

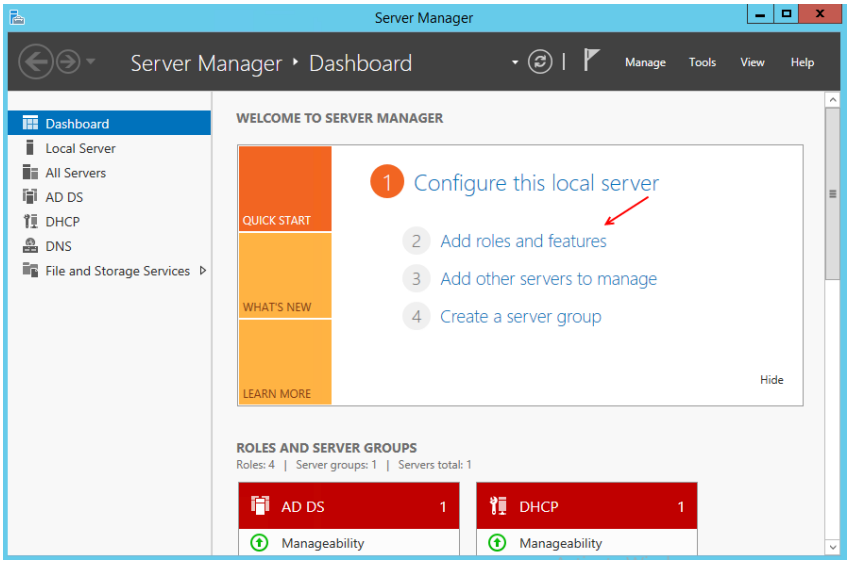


با ورود به سرویس DHCP، اگر به قسمت Reservations مراجعه کنید، مشاهده خواهید کرد که عملیات به مانند شکل روبرو با موفقیت اجرا شده است.

دستورات زیادی برای کار با DHCP در قسمت های مختلف وجود دارد که در ادامه ی کتاب به آن‌ها خواهیم پرداخت.

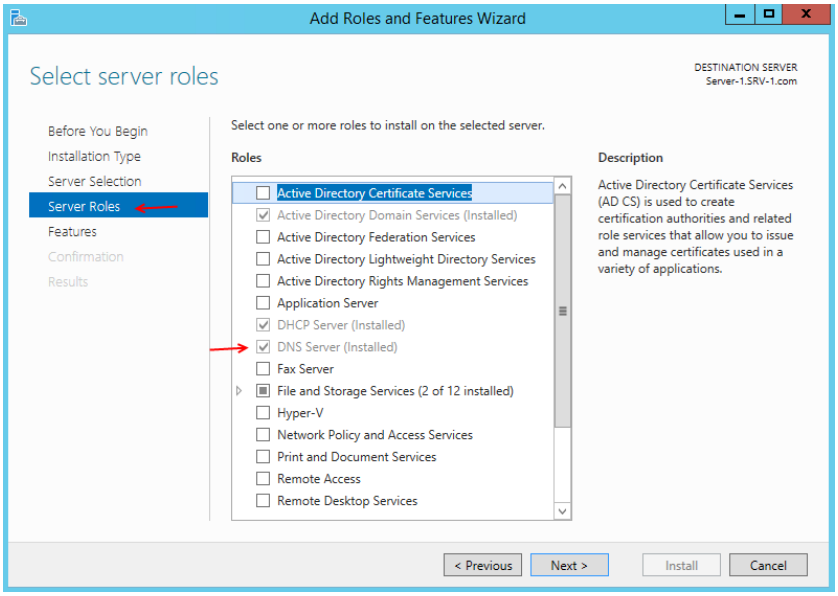
نصب و راه اندازی سرویس DNS سرور:

سرویس DNS، یک سرویس برای تبدیل نام کامپیوتر به آدرس IP و بلعکس می‌باشد که یک سرویس حیاتی در شبکه می‌باشد. زمانی که شما نام یک کامپیوتر را Ping می‌کنید، این سرویس نام کامپیوتر موردنظر را به IP مشخص‌شده تبدیل می‌کند و می‌توانید به کامپیوتر موردنظر به راحتی Ping کنید و در ارتباط باشید. با هم این سرویس را نصب و تنظیمات آن را فرا می‌گیریم.

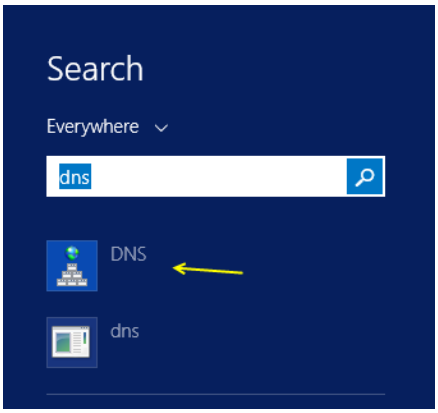


برای نصب سرویس DNS، باید وارد Server Manager شوید و بر روی Add roles and Features کلیک کنید.

تذکر: سرویس DNS، در هنگام نصب سرویس Active Directory به صورت خودکار نصب می‌شود و دیگر احتیاج به نصب این سرویس در این مرحله نیست.

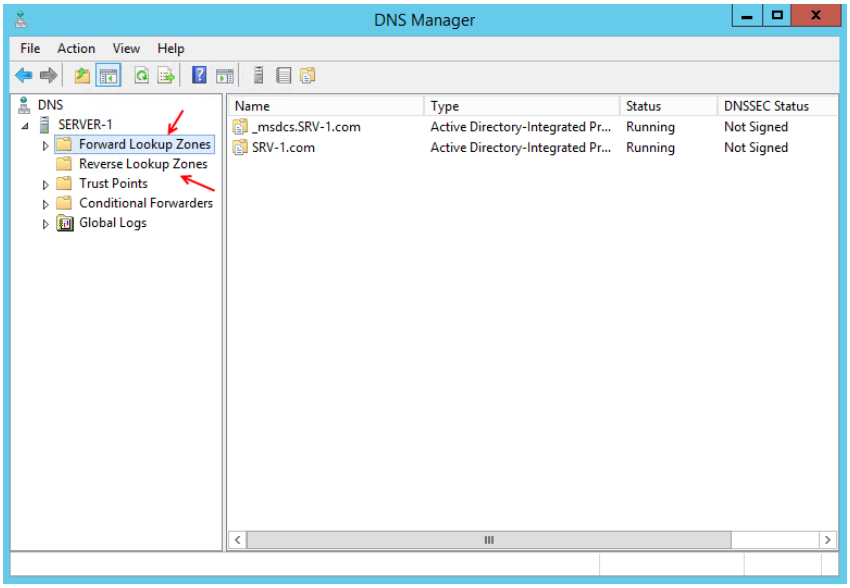


بعد از کلیک بر روی Add roles and Features در صفحه ی باز شده، بر روی Next کلیک کنید تا به قسمت Server Roles برسید. به مانند شکل روبرو، سرویس DNS را انتخاب کنید؛ البته در این شکل این سرویس از قبل نصب شده است. بعد از انتخاب بر روی Next کلیک کنید. در صفحه ی بعد بر

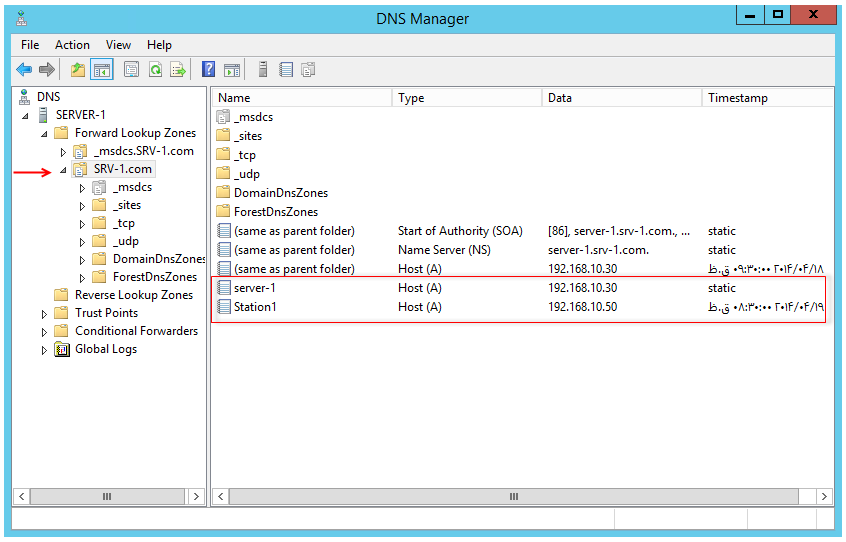


روی Next و در صفحه ی آخر بر روی Install کلیک کنید و سیستم را Restart کنید.

بعد از ورود مجدد به ویندوز، وارد Search شوید و کلمه ی DNS را وارد و سرویس DNS را اجرا کنید.

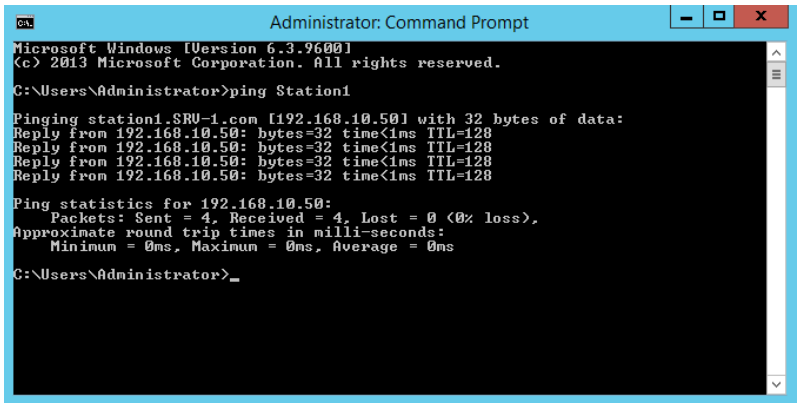


سرویس DNS، مانند شکل روبرو اجرا شده است. در این سرویس، بیش‌ترین گزینه هایی که با آن‌ها کار خواهیم کرد، Forward Lookup Zones و Reverse Lookup Zones می‌باشد. قسمت Forward Lookup Zones، برای تبدیل نام به آدرس IP و قسمت Reverse Lookup Zones، برای تبدیل IP به نام موردنظر می‌باشد که با هم این قسمت‌ها را بررسی می‌کنیم.

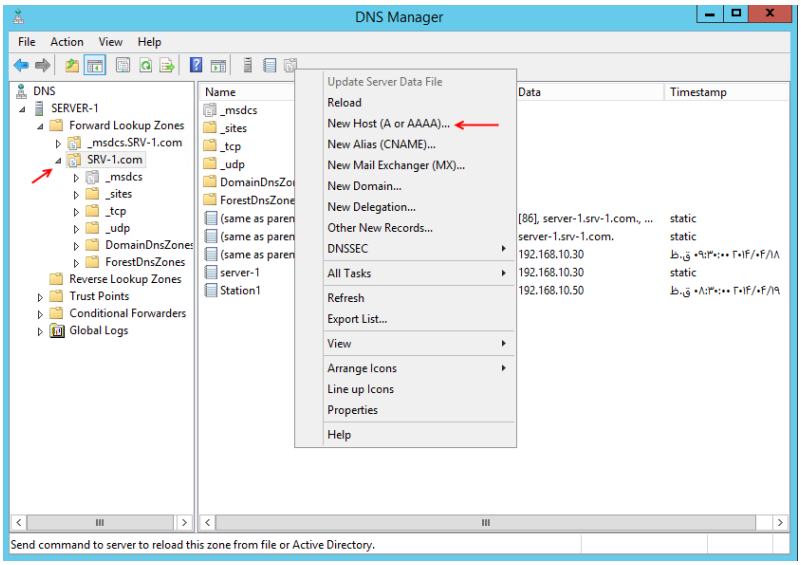


وارد قسمت Forward Lookup Zones می‌شویم. در این قسمت، نام دومین ما قرار دارد که این نام در هنگام نصب Active Directory و تعریف Domain، ایجاد شده است. به این قسمت ها یک Zone می‌گویند که دربرگیرنده ی دومین ویا چیز دیگری است. اگر بر روی SRV-1.com کلیک کنید، لیست اطلاعات مربوط

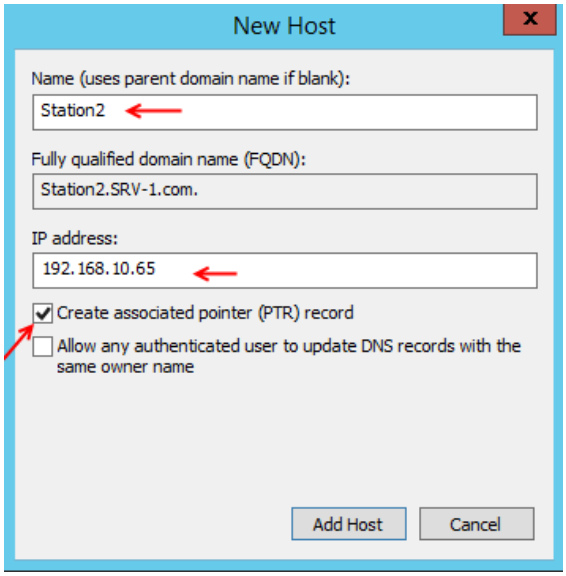
به آن را در سمت راست مشاهده می‌کنید. در این لیست، دو نام Server-1 و Station1 به ترتیب مربوط به سرور اصلی و کلاینت می‌باشد که به صورت خودکار به لیست اضافه شده اند.



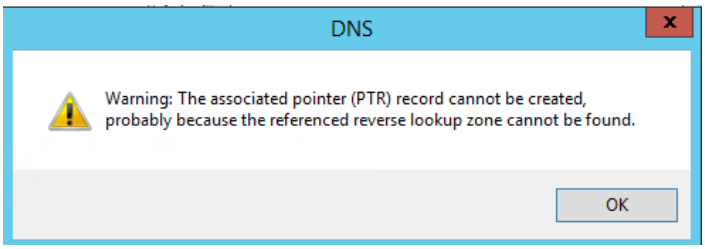
اگر وارد CMD شویم و نام Station1 را Ping کنیم باید آدرس IP مربوط به آن را به ما نشان دهد. در شکل روبرو با دستور Ping، نام station1 را pingکردیم که آدرس IP آن را به صورت کامل 192.168.10.50 به ما نشان داده است.



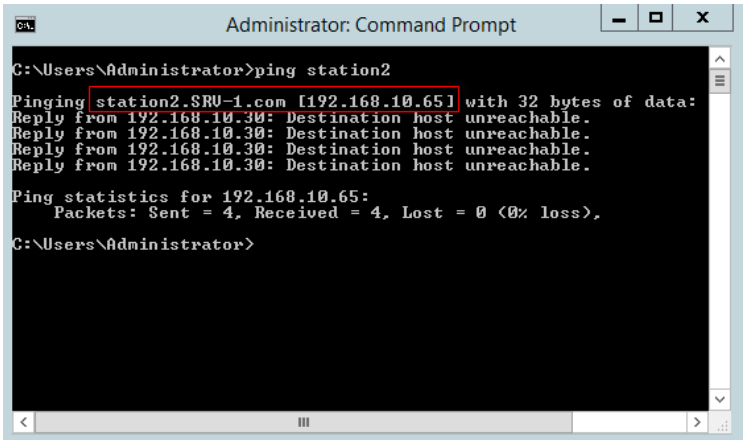
حالا می‌خواهیم خودمان یک Host ایجاد کنیم و به آن Ping کنیم. برای این کار، در قسمت SRV-1.com کلیک راست کنید و گزینه ی New Host (A or AAAA) را انتخاب کنید تا شکل بعد ظاهر شود.



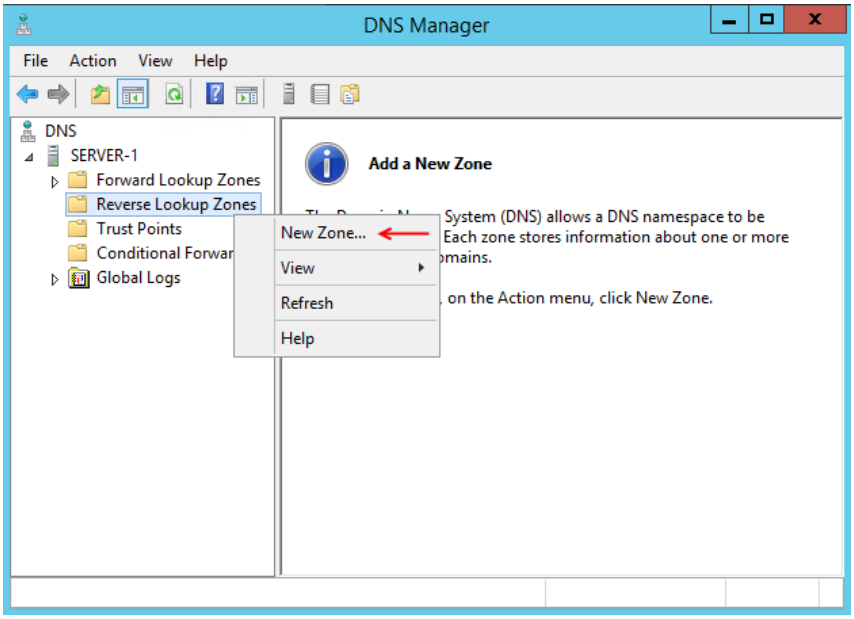
در قسمت Name نام موردنظر خود را وارد کنید و در قسمت IP address، آدرس IP مربوط به آن را وارد کنید و تیک گزینه ی موردنظر را انتخاب کنید. توجه داشته باشید که زمانی که قسمت Name را تکمیل می‌کنید، به صورت خودکار قسمت FQDN تشکیل می‌شود. بعد از تکمیل اطلاعات، بر روی Add Host کلیک کنید.



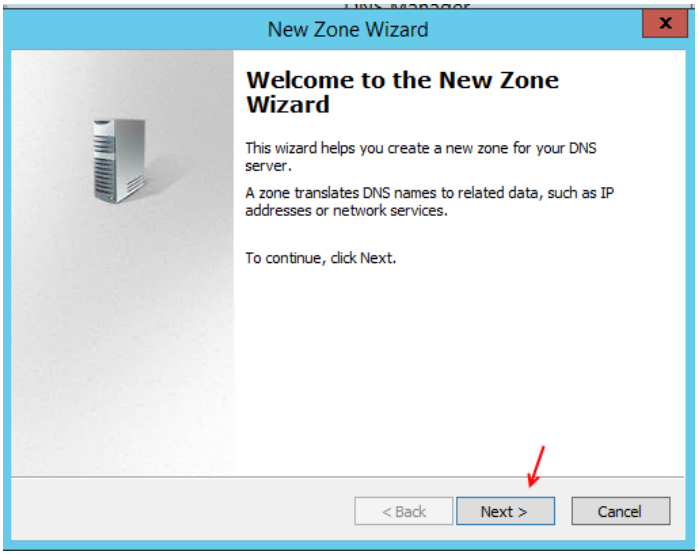
بعد از کلیک بر روی Add Host با پیغام روبرو مواجه می‌شوید. این پیغام به این نکته اشاره دارد که شما در قسمت قبل، تیک مربوط به گزینه ی Create associated pointer (PTR) را انتخاب کرده بودید؛ ولی این قسمت را باید زمانی انتخاب کنید که قسمت Reverse Lookup Zone فعال باشد که در حال حاضر فعال نیست. همان‌طور که گفتیم، قسمت Reverse Lookup Zone، مربوط به تغییر آدرس IP به نام می‌باشد. بعد از کلیک بر روی Ok فایل Host A یا A Record ایجاد می‌شود.



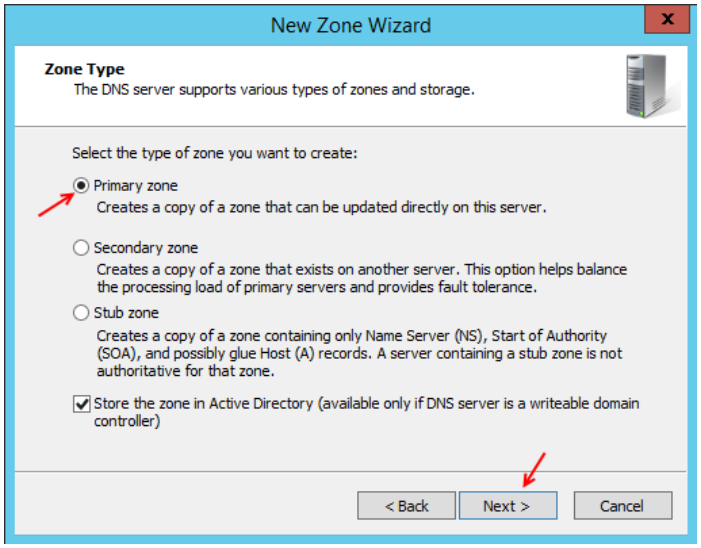
وارد CMD می‌شویم و دستور Ping Station2 را وارد و اجرا می‌کنیم. همان‌طور که در شکل روبرو مشاهده می‌کنید، بعد از اجرای دستور، سرور موردنظر پیدا شده است و IP آن هم مشخص‌شده است؛ اما به علت متصل نبودن به هیچ دستگاهی، ارتباط برقرار نمی‌شود.



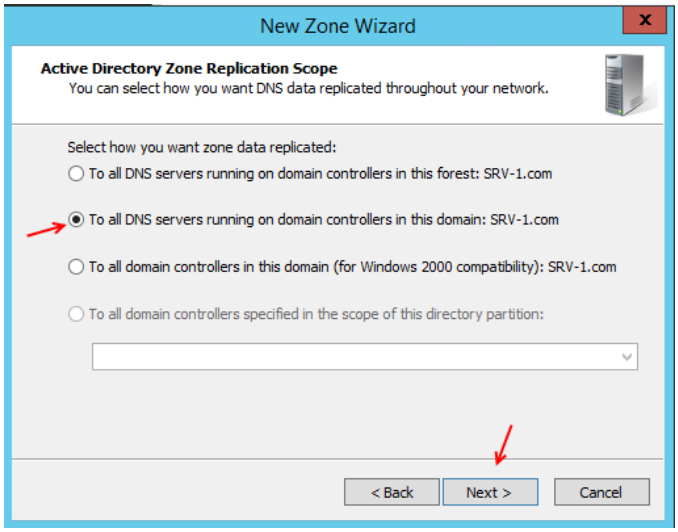
در این قسمت، می‌خواهیم تنظیمات مربوط به Reverse Lookup Zone را انجام دهیم. برای این کار، بر روی Reverse Lookup Zone کلیک راست کنید و گزینه ی New Zone را انتخاب کنید تا شکل بعد ظاهر شود.



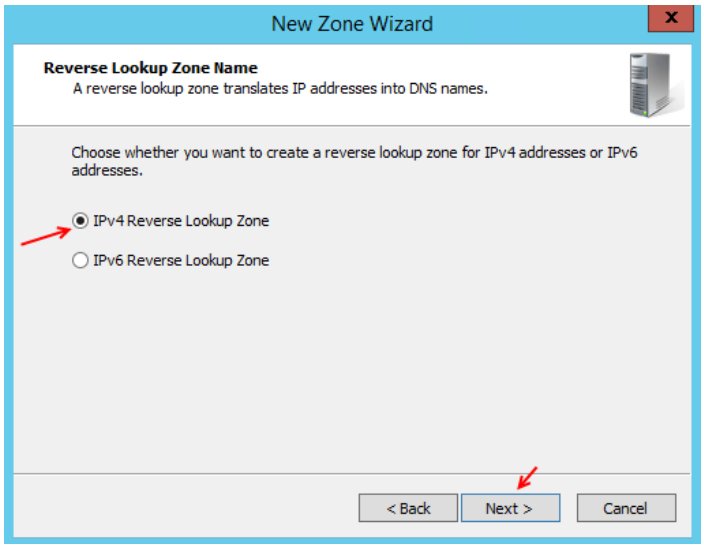
بر روی Next کلیک کنید.....



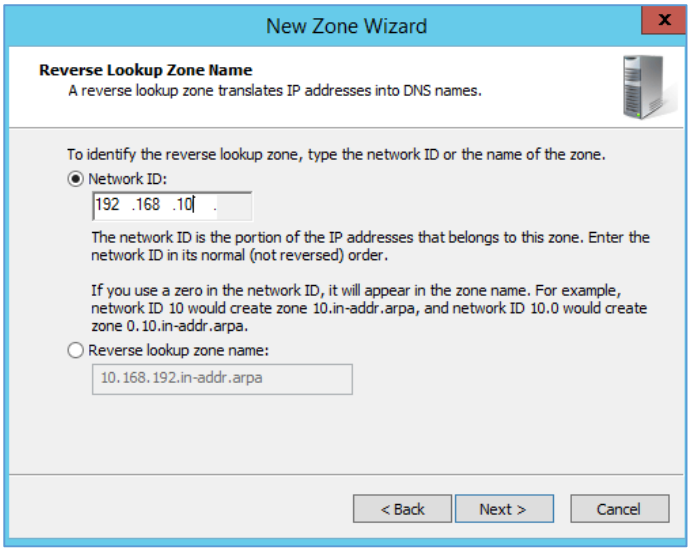
در این قسمت، سه گزینه وجود دارد که در این قسمت باید Primary Zone یا Zone اصلی را انتخاب کنید و بر روی Next کلیک کنید.



در این قسمت، گزینه ی دوم را انتخاب کنید و بر روی Next کلیک کنید.

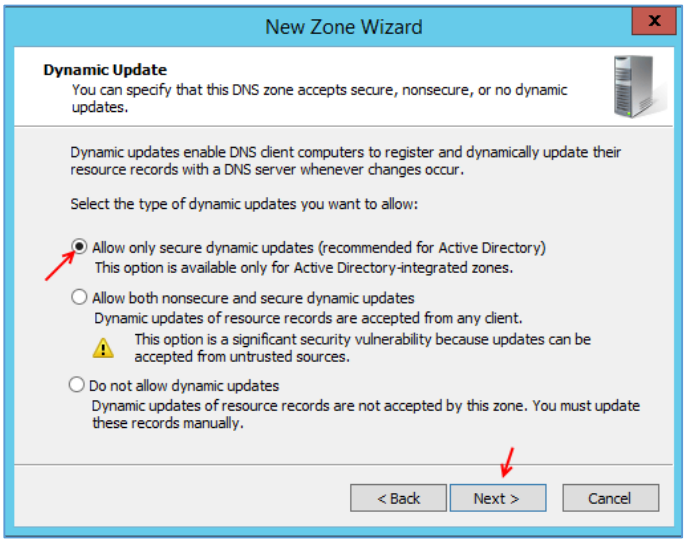


در این قسمت به نسبت پروتکل IP خود، یکی از گزینه ها را انتخاب کنید که در این قسمت، باید IPV4 را انتخاب کنید و بر روی Next کلیک کنید.



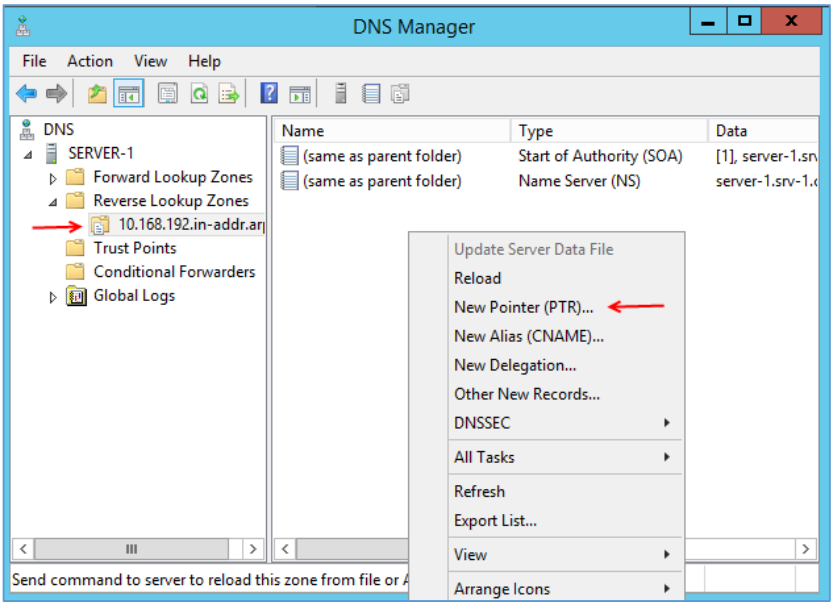
در این صفحه و در قسمت Network ID، باید آدرس NetID خود را وارد کنید که در اینجا 192.168.10 می‌باشد. درباره ی Network ID در شروع کتاب و در قسمت IPV4 صحبت کردیم.

بر روی Next کلیک کنید.

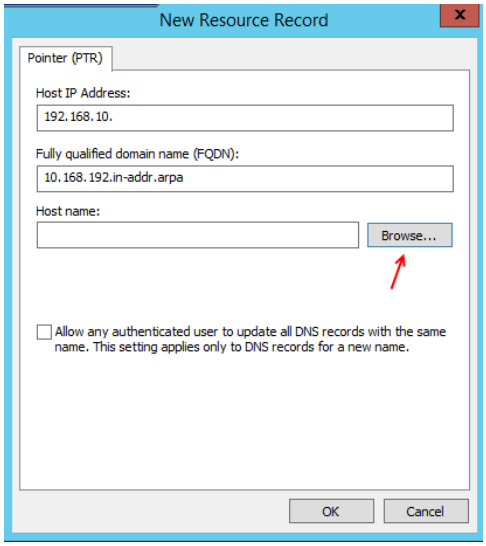


در این قسمت، گزینه ی اول را انتخاب و بر روی Next کلیک کنید.

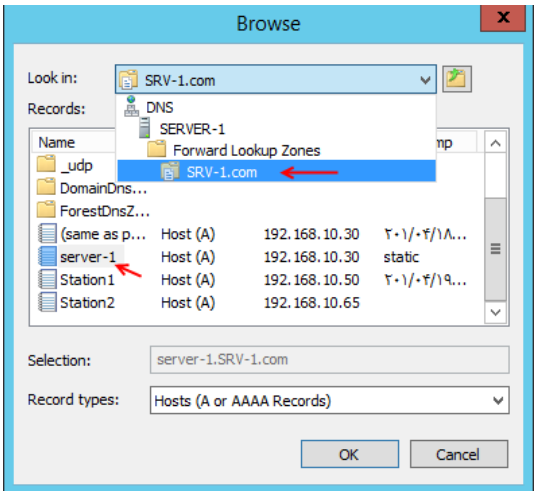
در صفحه ی آخر بر روی Finish کلیک کنید.



بعد از ایجاد Zone موردنظر بر روی آن کلیک کنید تا صفحه ی مربوط به آن باز شود و در صفحه ی موردنظر کلیک راست کنید و گزینه ی New Pointer (PTR) را که با هم کمی درباره ی آن صحبت کردیم، انتخاب کنید.



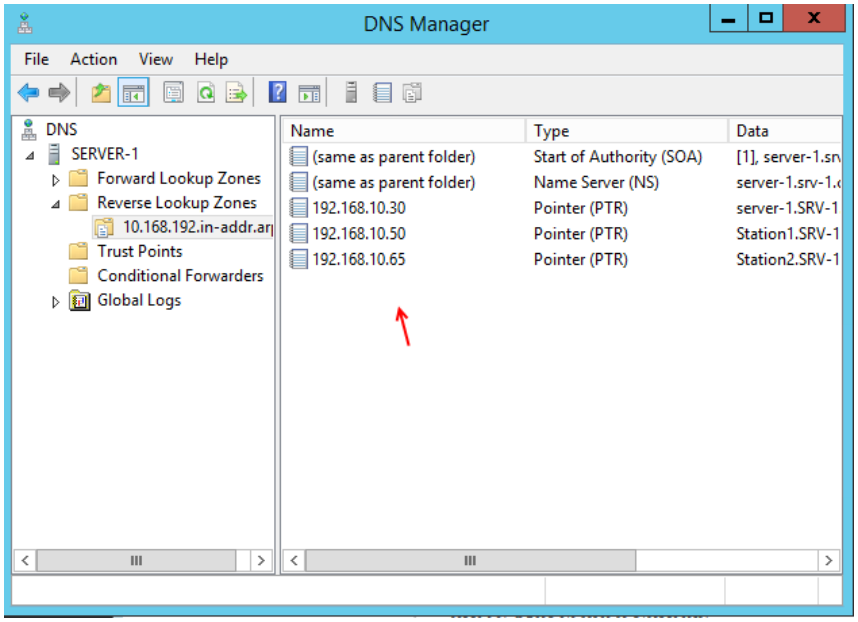
در این قسمت باید سرور و یا کلاینت موردنظر را با کلیک بر روی Browse به آن معرفی کنیم. برای این کار، بر روی Browse کلیک کنید.



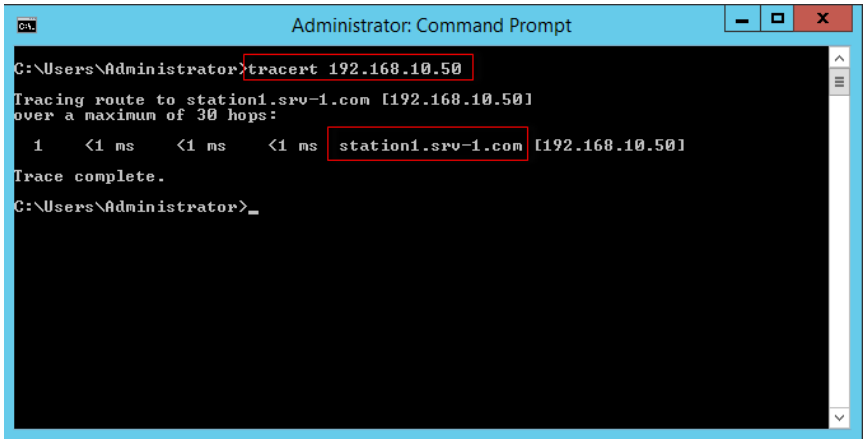
در این قسمت، وارد Zone، SRV-1.com شده‌ایم. سرور اصلی خودمان را انتخاب می‌کنیم و بر روی ok کلیک می‌کنیم.

بعد از این کار، PTR موردنظر ایجاد می‌شود. توجه داشته باشید که در قسمت قبلی در زمان ایجاد Host A، اگر تیک گزینه ی PTR را زده باشید، این قسمت به صورت خودکار ایجاد خواهد شد.

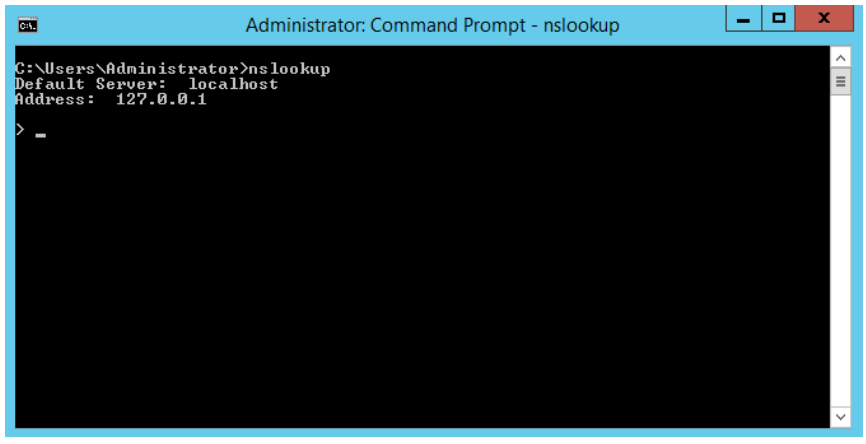
برای تمام سرورها و کلاینت ها این کار را انجام دهید.



همان‌طور که مشاهده می‌کنید، سه PTR برای سه سرور و کلاینت ایجاد شده است.

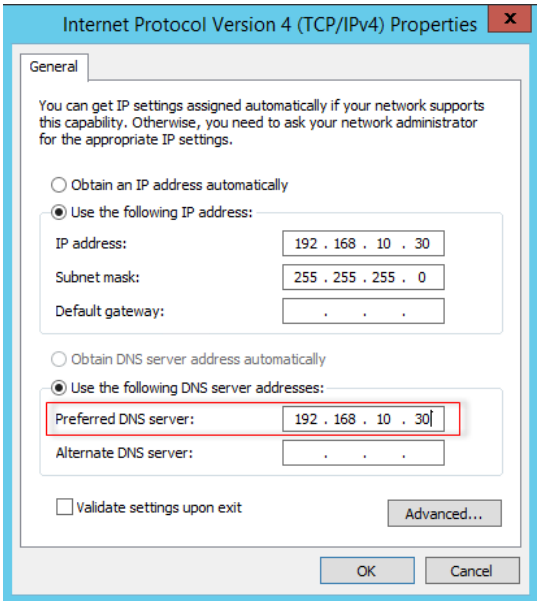


بعد از انجام کارهای بالا از دستور Tracert برای بدست آوردن نام سرور موردنظر استفاده می‌کنیم. همان‌طور که در شکل روبرو مشاهده می‌کنید، با دستور Tracert 192.168.10.50، نام کلاینت به همراه دومین به صورت کامل به ما نشان داده است. دستور Tracert برای نمایش روترها یا سرورهای سر راه یک سرور یا کلاینت می‌باشد. در این قسمت، هیچ روتری وجود نداشته است و فقط یک کلاینت وجود دارد.

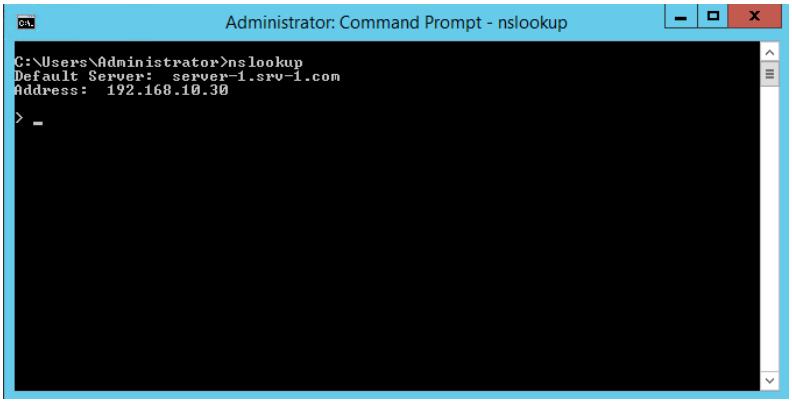


نکته بسیار مهم: زمانی که سرویس DNS نصب می‌شود، آدرس IP مربوط به DNS سرور به 127.0.0.1 تغییر حالت می‌دهد که این موضوع را با اجرای دستور Nslookup در CMD مشاهده می‌کنید.

دستور Nslookup، نشان دهنده ی نام کامل FQDN سرور و آدرس IP می‌باشد که در قسمت قبلی به علت تغییر IP سرور به 127.0.0.1 این موضوع را نشان نداد. برای حل این مشکل، وارد Network Connection می‌شویم و آدرس DNS را به آدرس سرور اصلی تغییر می‌دهیم.

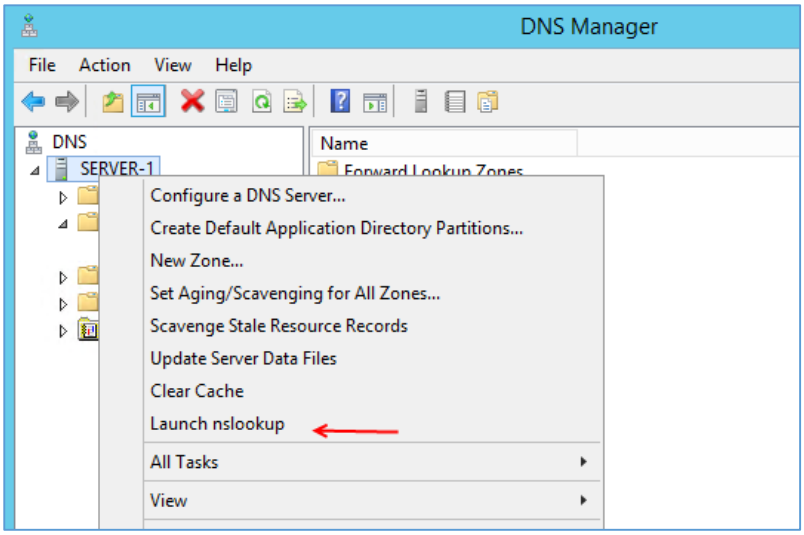


به مانند شکل روبرو در قسمت Preferred DNS Server، آدرس را به 192.168.10.30 تغییر می‌دهیم و بر روی ok کلیک می‌کنیم.

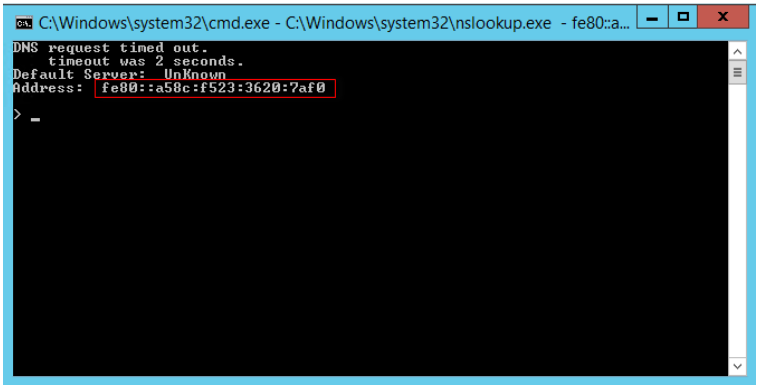


در شکل روبرو، دوباره دستور Nslookup اجرا شده و این بار به علت تغییر آدرس DNS به ما جواب داده است. به همین زیبایی.

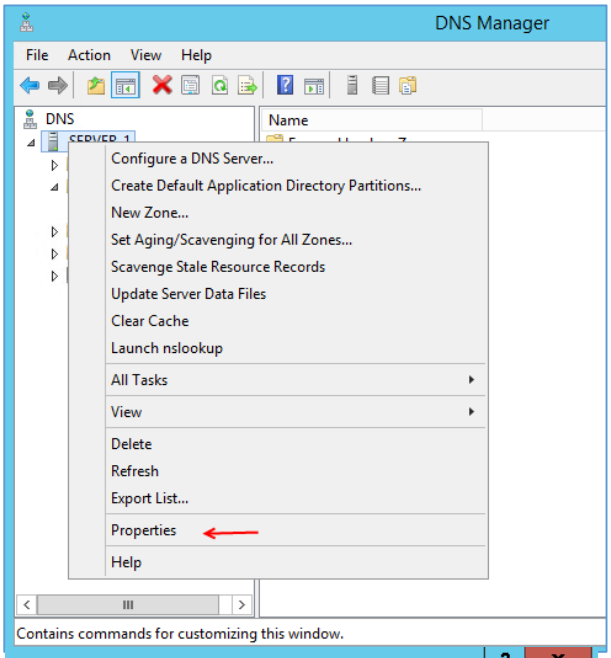
این دستور کاربرد زیادی در آینده خواهد داشت که شاید در این قسمت اهمیت آن را درک نکنیم.



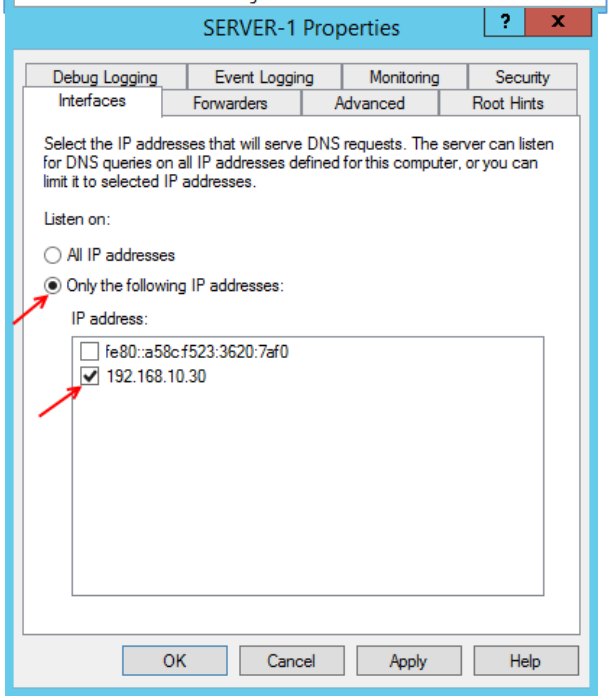
در سرویس DNS، بر روی نام سرور که در اینجا Server-1 می‌باشد کلیک راست کنید و گزینه ی Launch Nslookup را انتخاب کنید.



همانطور که در این صفحه مشاهده می‌کنید با اجرای دستور Nslookup روی سرور نام سرور به صورت ناشناخته و آدرس IP آن به صورت IPV6 می‌باشد، این در صورتی است که در این سرور از IPV4 استفاده کردیم.

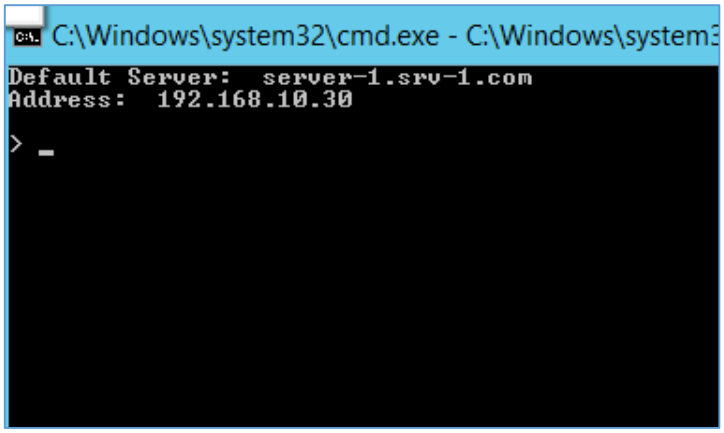


برای حل این مشکل بر روی نام سرور کلیک راست کنید و گزینه Properties را انتخاب کنید.



در تب Interfaces گزینه Only the Following IP address را انتخاب کنید و در لیست زیر آن دو IPV6 و IPV4 وجود دارد که تیک کنار گزینه IPV6 را بردارید و بر روی ok کلیک کنید.

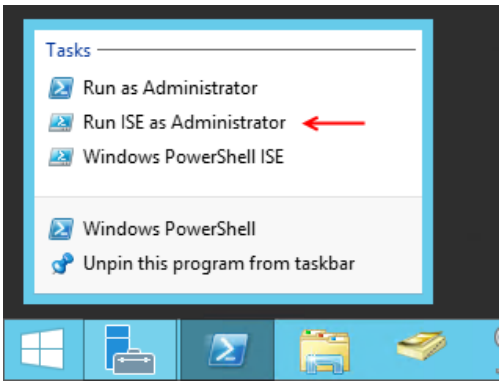
دوباره بر روی نام سرور کلیک کنید و گزینه Launch Nslookup را انتخاب کنید.



همانطور که مشاهده می‌کنید مشکل حل شده است و نام سرور به همرا آدرس IP مشخص شده است.

کار با DNS Server از طریق دستورات PowerShell:

تا به اینجا از طریق گرافیکی سرویس DNS را معرفی و راه اندازی کردیم، ولی در این قسمت می‌خواهیم از طریق دستورات PowerShell این کار را انجام دهیم.

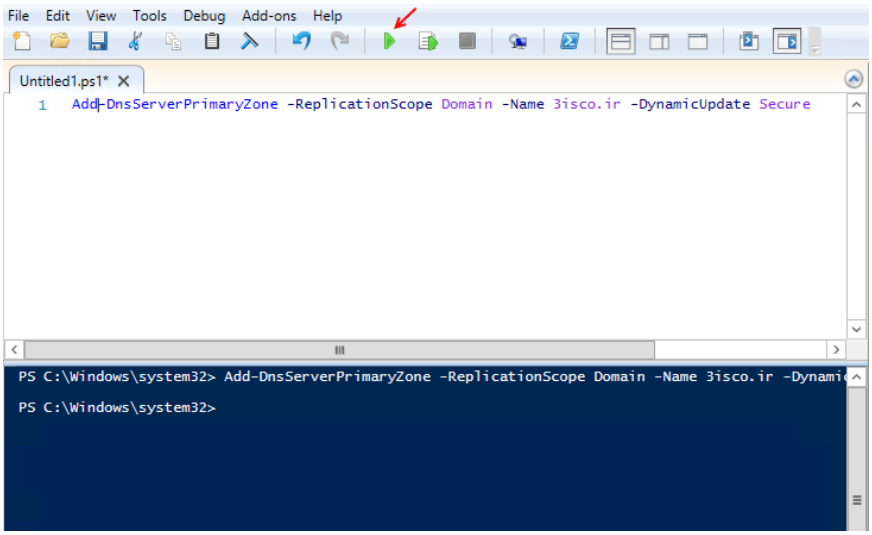


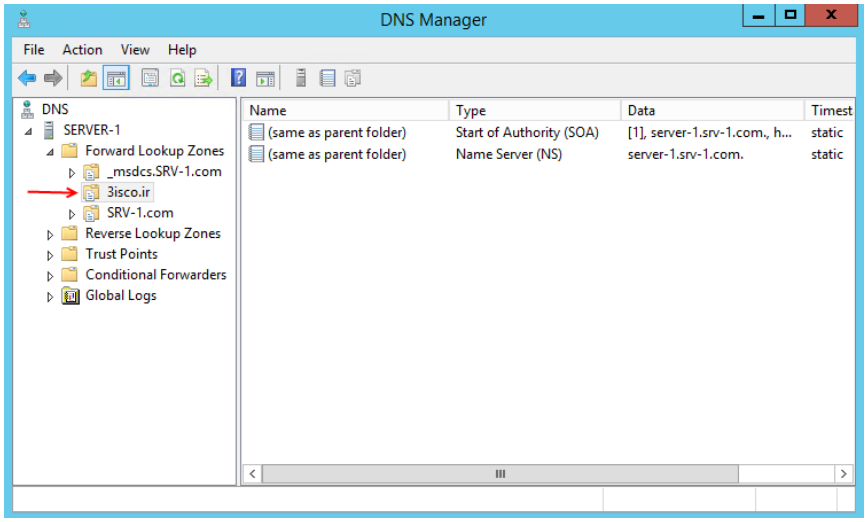
سرویس PowerShell ISE را از روی Taskbar به مانند شکل روبرو با اولویت کاربر Administrator اجرا می‌کنیم.

اولین کاری که انجام می‌دهیم ایجاد یک Forward Zone با استفاده از دستورات زیر می‌باشد:

```
Add-DnsServerPrimaryZone -ReplicationScope Domain -Name 3isco.ir -
DynamicUpdate Secure
```

دستور Add-DnsServerPrimaryZone برای ایجاد یک Zone Primary اصلی می‌باشد. بعد از آن باید نحوه استفاده از این Zone را با استفاده از دستور ReplicationScope Domain مشخص کنید، این دستور یعنی اینکه این Zone که می‌خواهیم ایجاد کنیم یک Zone اصلی می‌باشد و زیرمجموعه یا Forest کسی دیگر





نیست، بعد از این دستور باید نام Zone خود را با استفاده از دستور Name 3isco.ir مشخص کنید که باید به جای 3isco.ir نام موردنظر خود را وارد کنید و در قسمت آخر نحوه دریافت آپدیت را مشخص کند که به صورت امن باشد یا نه که در این قسمت DynamicUpdate Secure را وارد می‌کنیم. بعد ار وارد کردن دستور به مانند شکل روبرو بر روی آیکون Run Script کلیک کنید.

در شکل روبرو Zone موردنظر ما با نام 3isco.ir به درستی در سرویس DNS و در قسمت Forward Lookup ایجاد شده است.

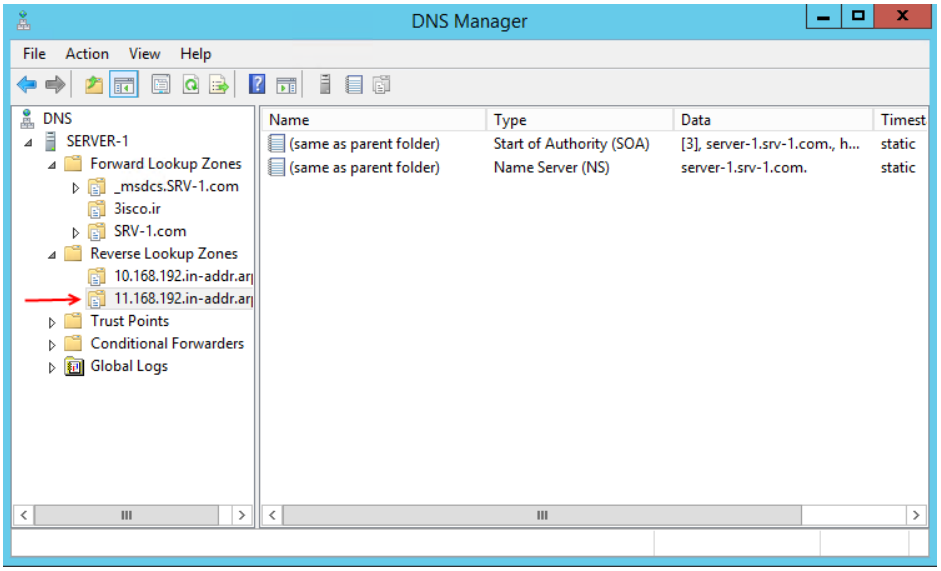
بعد از ایجاد Forward Lookup Zone باید Reverse Lookup Zone هم برای این Zone ایجاد کنیم، برای این Zone آدرس 192.168.11.0 را در نظر می‌گیریم.

با استفاده از دستور زیر یک Reverse Lookup Zone برای آدرس 192.168.11 ایجاد می‌شود:

```
Add-DnsServerPrimaryZone -NetworkId 192.168.11.0/24 -DynamicUpdate Secure -
ReplicationScope Domain
```

در دستورات بالا دستور Add-DnsServerPrimaryZone برای ایجاد یک Zone Primary یا اصلی می‌باشد، بعد باید آدرس شبکه موردنظر را وارد کنیم یعنی NetID آن را وارد کنیم که با استفاده از دستور NetworkId 192.168.11.0/24 تعریف می‌شود، توجه داشته باشید که به جای 192.168.11.0 آدرس موردنظر خود را وارد کنید و به جای 24/ باید مقدار موردنظر خود را وارد کنید 24/ یعنی 255.255.255.0

که این موضوعات در قسمت IPV4 به صورت کامل بررسی شده است، در دستور بعدی نوع دریافت آپدیت را مشخص می‌کنیم که به صورت امن می‌باشد DynamicUpdate Secure و بعد باید نوع دومین را مشخص کنیم که در اینجا دومین اصلی می‌باشد و باید از نام دومین به صورت ReplicationScope Domain استفاده کنیم.

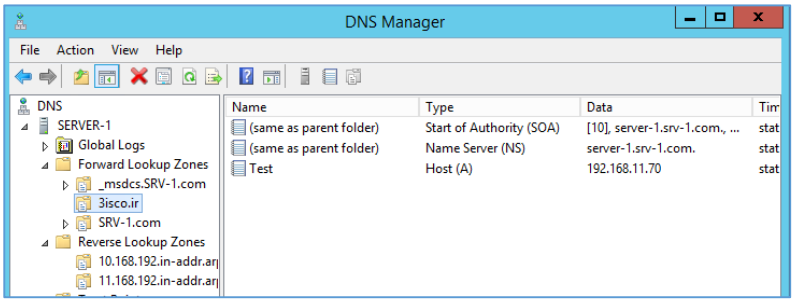


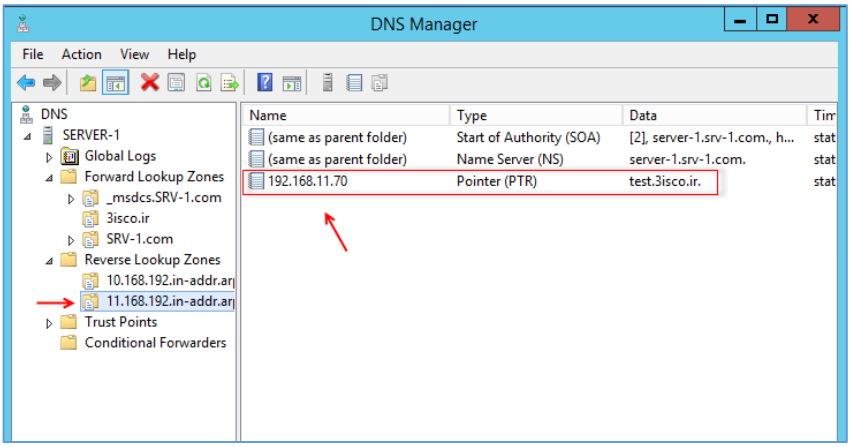
بعد ازوارد کردن دستورات بالا آنها را اجرا کنید تا به صورت شکل مقابل Zone موردنظر در قسمت Reverse Lookup Zone ایجاد شود.

بعد از اینکه Reverse Lookup Zone را ایجاد کردیم باید در داخل 3isco.ir یک Host A از طریق فرامین PowerShell ایجاد کنیم، برای این کار از دستورات زیر برای ایجاد Host A استفاده می‌کنیم:

```
Add-DnsServerResourceRecordA -Name Test -IPv4Address 192.168.11.70 -
CreatePtr -ZoneName 3isco.ir
```

دستور Add-DnsServerResourceRecordA برای ایجاد Host A یا همان A Record در Zone موردنظر است، بعد از آن باید نام A Record خود را بادستور Name Test وارد کنیم که به جای Test نام موردنظر خود را وارد کنید، در دستور بعدی IP Address را وارد کنید که در این قسمت آدرس 192.168.11.70 را در نظر می‌گیریم، دستور بعدی CreatePtr می‌باشد که برای ایجاد Record PTR در قسمت Revers Lookup Zone می‌باشد که این کار به صورت خودکار انجام می‌شود، در آخر هم باید نام Zone موردنظر خود را وارد کنید که در اینجا 3isco.ir می‌باشد.



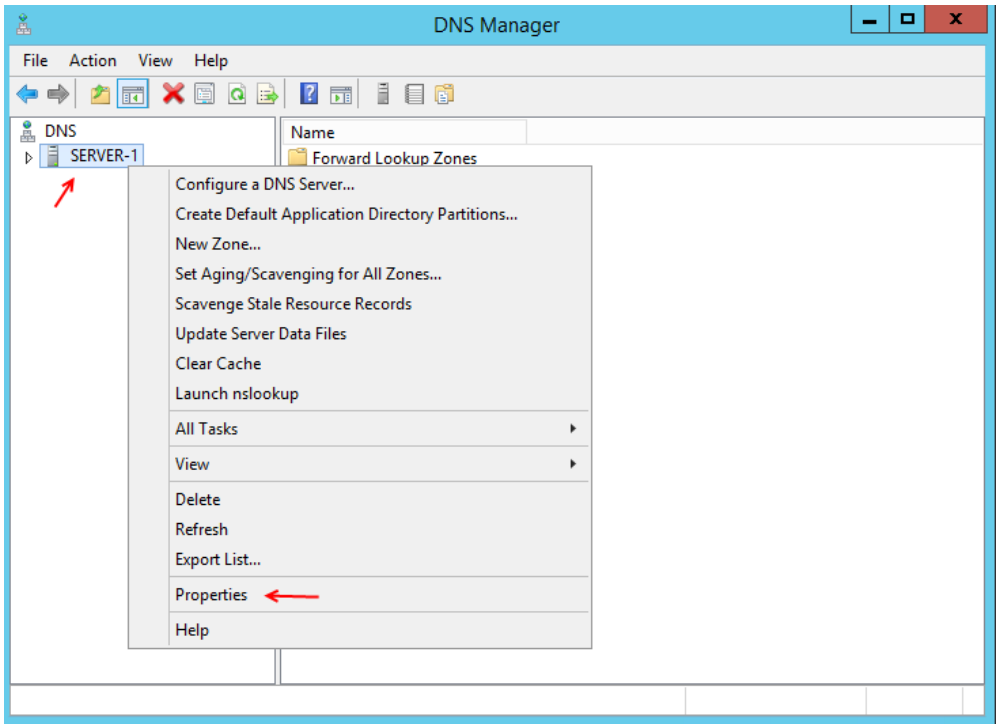


در شکل مقابل بعد از دستور بالا در 3isco.ir یک Host A با نام Test ایجاد شده است، توجه داشته باشید، با اجرای دستور بالا یک Record PTR هم در قسمت Reverse به صورت خودکار ایجاد شده است.

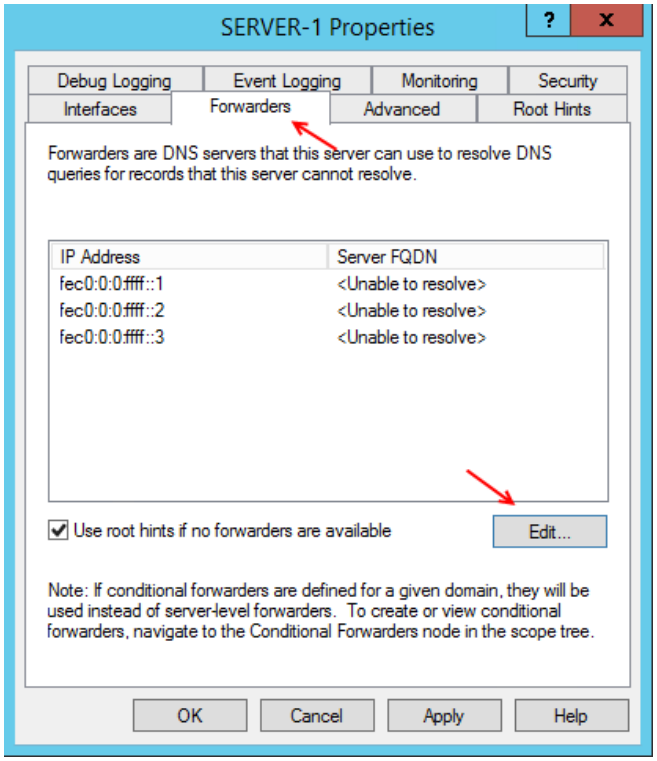
بررسی DNS Forwarders:

یکی از امکانات سرویس DNS امکان DNS Forwarders می‌باشد که این امکان به شما این اجازه را می‌دهد زمانی که یک کلاینت به دنبال یک آدرس خاص می‌باشد و آن آدرس درون سرویس DNS وجود ندارد و می‌توانید DNS دیگر را به DNS خود متصل کنید و زمانی که آدرس در DNS فعلی پیدا نشود سرویس موردنظر به صورت خودکار کلاینت را به DNS Server دیگر بفرستد.

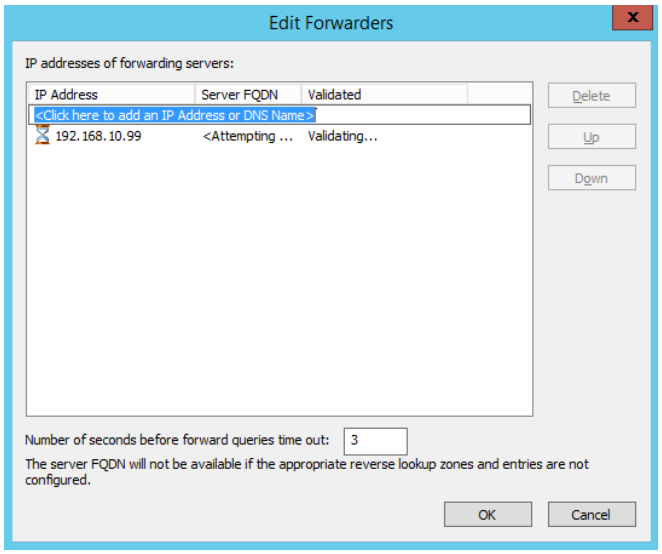
برای معرفی سرور DNS دیگر به سرویس DNS فعلی به این صورت عمل کنید:



بر روی نام سرور در سرویس DNS Server کلیک راست کنید و گزینه Properties را انتخاب کنید تا شکل بعد ظاهر شود.



در این صفحه وارد تب Forwarders شوید. در این تب همانطور که مشاهده می‌کنید سه آدرس IPV6 درج شده است که این آدرس ها به صورت پیشفرض از قبل قرار دارند، اگر به نوشته جلوی آنها توجه کنید نوشته Unable To Resolve به این معنی است که نمی‌تواند سرور موردنظر را شناسایی کند، برای معرفی DNS Server خود بر روی Edit کلیک کنید.

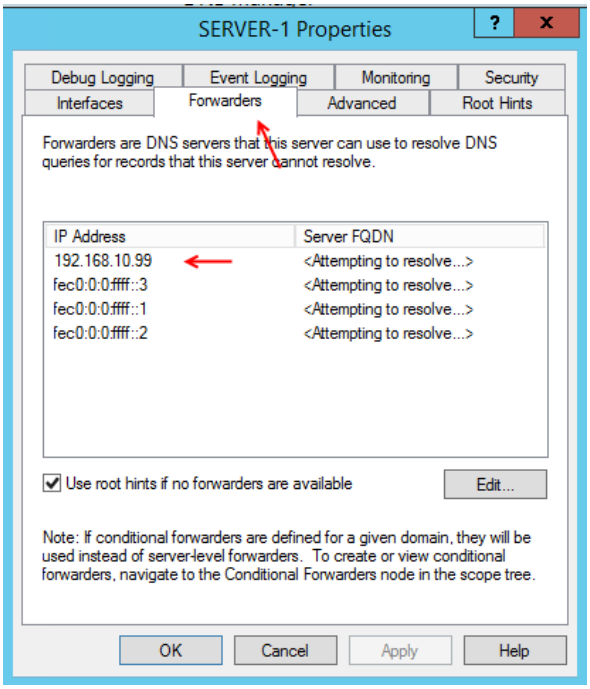


در این صفحه، می‌توانید سرورهای قبلی را انتخاب و بر روی Delete کلیک کنید تا حذف شوند و بعد سرور جدید خود را وارد کنید که بعد از این کار سرویس به دنبال سرور موردنظر می‌گردد، اگر در سروری که آدرس آن را وارد کردید سرویس DNS فعال باشد به شما تایید می‌دهد، بعد از این کار بر روی ok کلیک کنید تا کار به اتمام برسد.

برای ایجاد Forwarders از طریق دستورات PowerShell باید از دستورات زیر استفاده کنید:

```
Add-DnsServerForwarder -IPAddress 192.168.10.99 -PassThru
```

دستور Add-DnsServerForwarder برای ایجاد سرور Forwarders می‌باشد که بعد از آن باید IP address مربوط به سرور موردنظر را وارد کنیم و درآخر هم بایددستور PassThru را وارد کنید تا اجازه دسترسی به قسمت Forwarders داده شود.



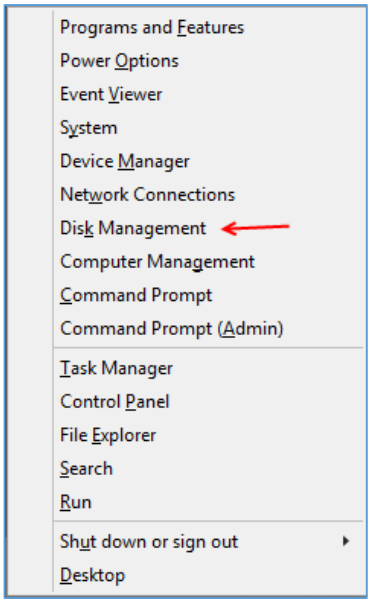
بعد از اجرای دستور صفحه قبل اگر دوباره به قسمت Forwarders مراجعه کنیم متوجه می‌شویم که IP Address موردنظر به لیست اضافه شده است.

توجه داشته باشید اگر به مانند شکل روبرو IP Address خود را در لیست مشاهده نمی‌کنید، سرویس DNS را ببندید و دوباره باز کنید.

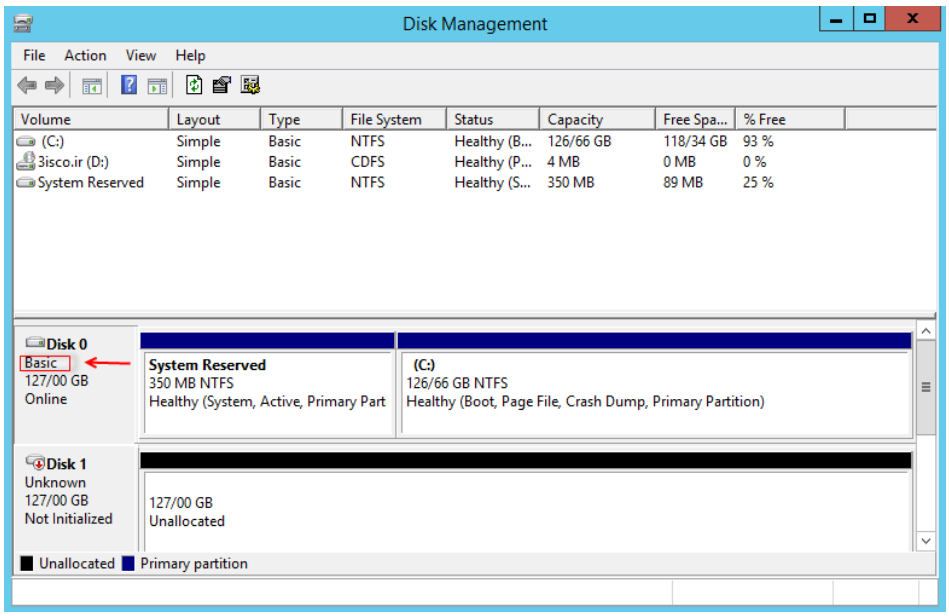
سرویس DNS یک سری امکانات پیشرفته تر دیگری هم دارد که احتمالاً در ادامه کتاب روی آنها کار خواهیم کرد.

بررسی سرویس Disk Management و کار با آن:

این سرویس برای مدیریت هارد دیسک ها و درایور ها می‌باشد که می‌تواند عملیات سودمندی را برای بهره وری بالاتر سرورها انجام دهد، این سرویس بصورت پیش فرض بر روی ویندوز سرور نصب است و برای اجرای آن کافی است در Run سرور خود کلمه Diskmgmt.msc را وارد و enter کنید و یا از طریق Search به آن دست پیدا کنید.



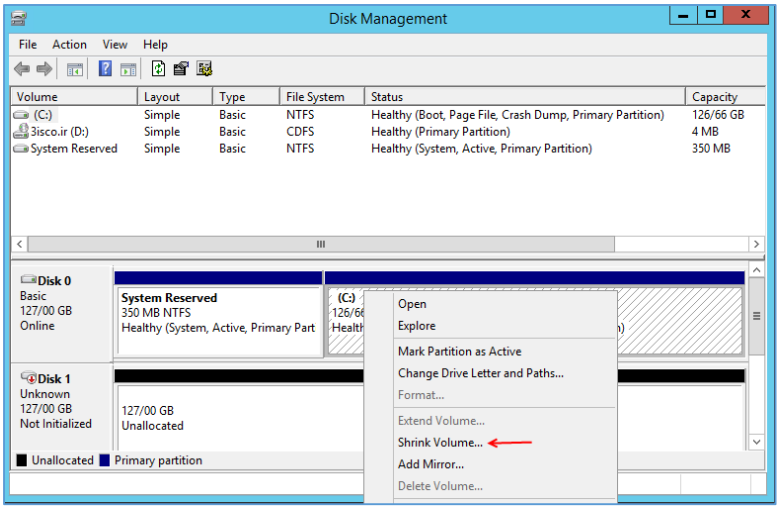
برای اجرای این سرویس کلید ترکیبی Win + X را فشار دهید، منظور از Win همان دکمه پنجره روی صفحه کلید می‌باشد. بعد از باز شدن منوی موردنظر بر روی Disk Management کلیک کنید تا سرویس موردنظر باز شود. توجه داشته باشید در این منو سرویس ها و قسمت های مختلف ویندوز وجود دارد که می‌توانید خیلی سریع به آنها دسترسی داشته باشید.



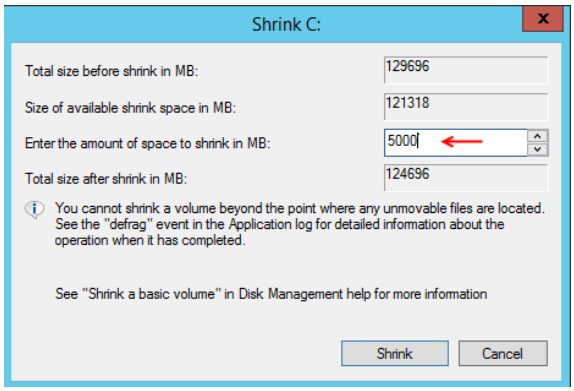
در این سرویس دو هارد دیسک را مشاهده می‌کنید که یکی در حال کار و دیگری، فعال نیست.

نوع دیسک در این قسمت Basic در نظر گرفته شده است. که می‌توان آن را به Dynamic تغییر داد.

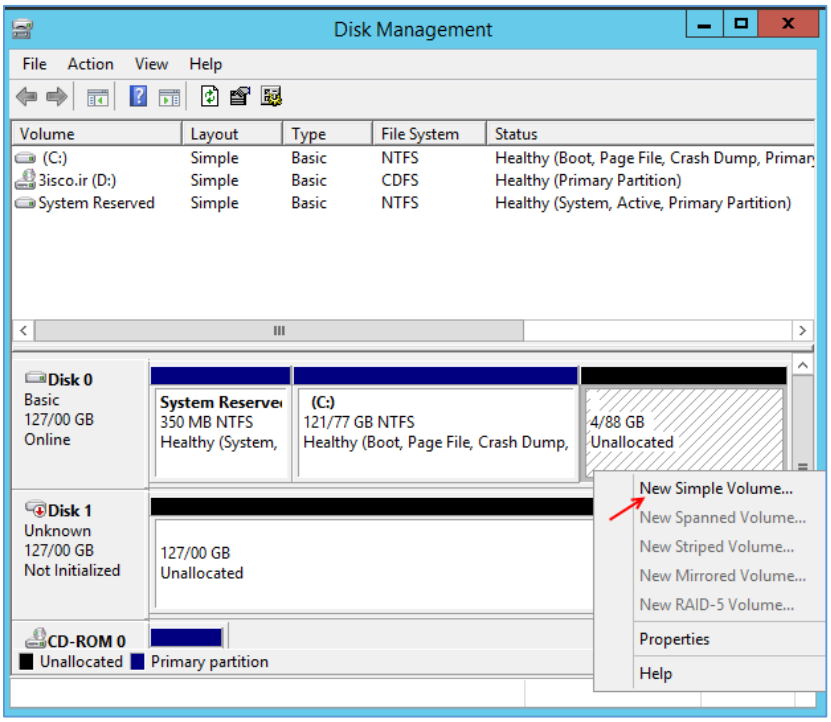
Shrink کردن یک دیسک به این صورت است که از مقدار فضای موجود بر روی یک درایو یک درایو جدید از آن به وجود می‌آید به طور مثال اگر یک درایو C داشته باشید و مقدار 20 گیگابایت فضا خالی داشته باشد می‌توانید از این مقدار فضای خالی یک پارتیشن از نوع shrink ایجاد کنید.



در این قسمت بر روی نام درایو و یا به مانند شکل در قسمت Disk 0 بر روی درایو C کلیک راست کنید و گزینه shrink Volume را انتخاب کنید.



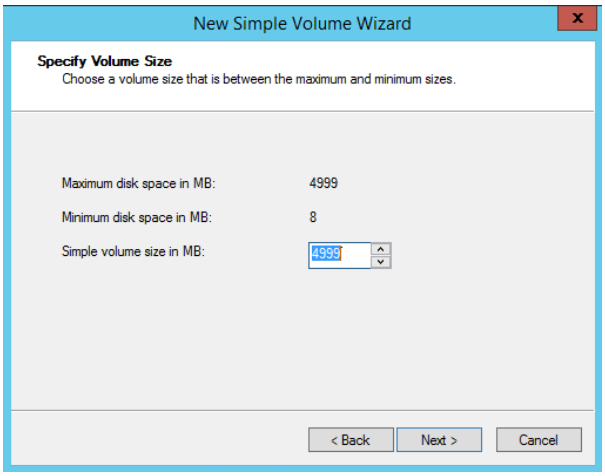
در این صفحه و در قسمت Total Size Before Shrink in MB مقدار فضای کل درایو موردنظر نوشته شده است، در قسمت Size of... مقدار فضای در دسترس نوشته شده است که باید در قسمت سوم مقدار فضایی را که برای ایجاد پارتیشن نیاز دارید را وارد کنید و بر روی Shrink کلیک کنید.



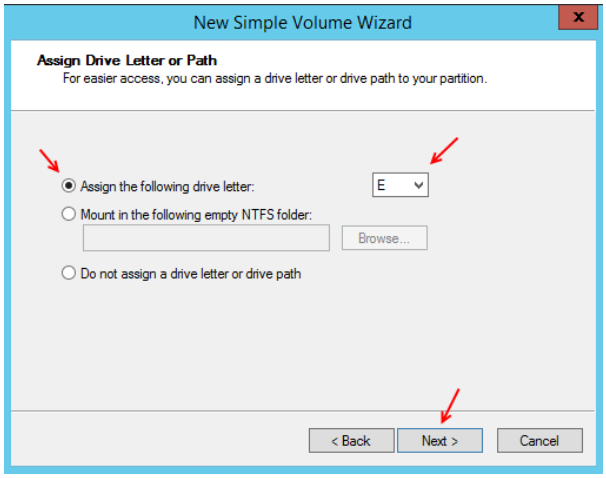
بعد از ایجاد پارتیشن موردنظر بر روی آن کلیک راست می‌کنیم و گزینه New Simple Volume را انتخاب می‌کنیم،

البته در این قسمت گزینه های غیر فعال دیگر وجود دارد که با هم در ادامه آنها را بررسی می‌کنیم.

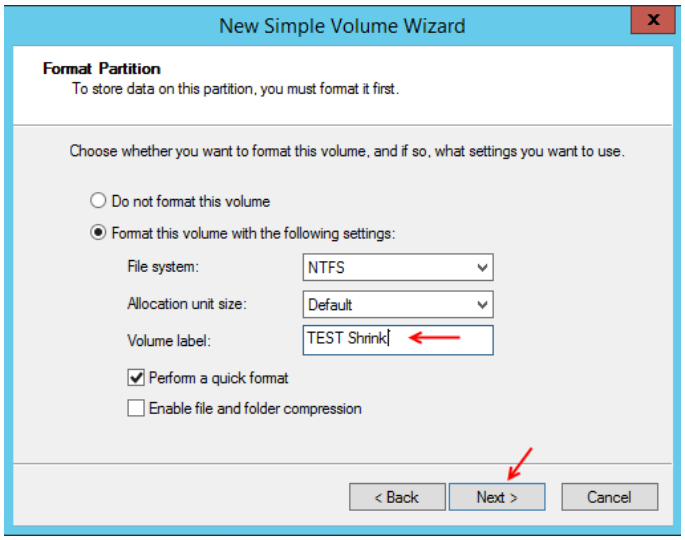
در صفحه باز شده بر روی Next کلیک کنید تا شکل زیر ظاهر شود.



در این قسمت مقدار فضای مورد نیاز خود را برای ایجاد درایوجدیدی وارد کنید و بر روی Next کلیک کنید.

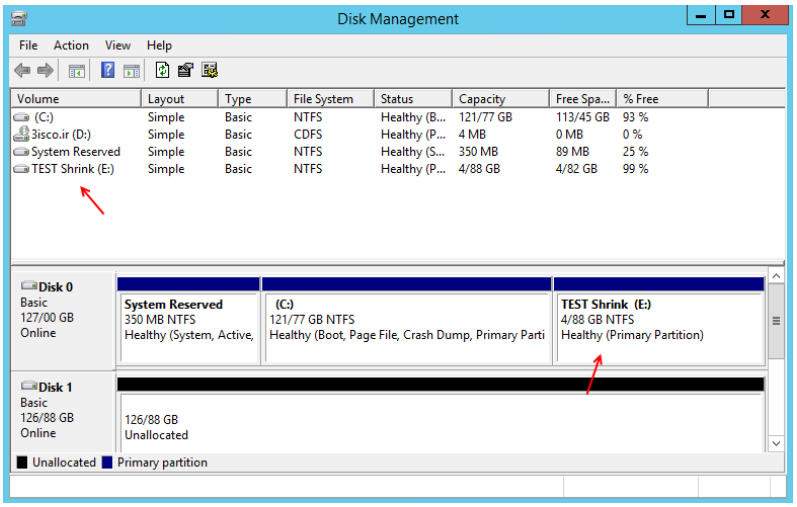


در این قسمت گزینه اول را انتخاب و نام درایو موردنظر خود را انتخاب کنید و بر روی Next کلیک کنید.



در این صفحه اگر می‌خواهید درایو موردنظر شما بعد از ایجاد فرمت شود، گزینه Format this... را انتخاب کنید و بر روی Next کلیک کنید.

در صفحه بعد هم بر روی Finish کلیک کنید تا درایو موردنظر آماده به کار شود.



همانطور که در شکل روبرو مشاهده می‌کنید، درایو Shrink با موفّقیت ایجاد شده است و می‌توانید از آن مانند یک درایو استفاده کنید.

تذکر مهم: درایو Shrink زیر مجموعه درایوی است که از آن ایجاد شده و اگر حذف شود بر روی درایو اصلی تأثیری ندارد ولی اگر درایو اصلی که در اینجا درایو C است حذف شود درایو Shrink ایجاد شده هم حذف خواهد شد، پس هیچ وقت به این درایوها اعتماد نکنید.

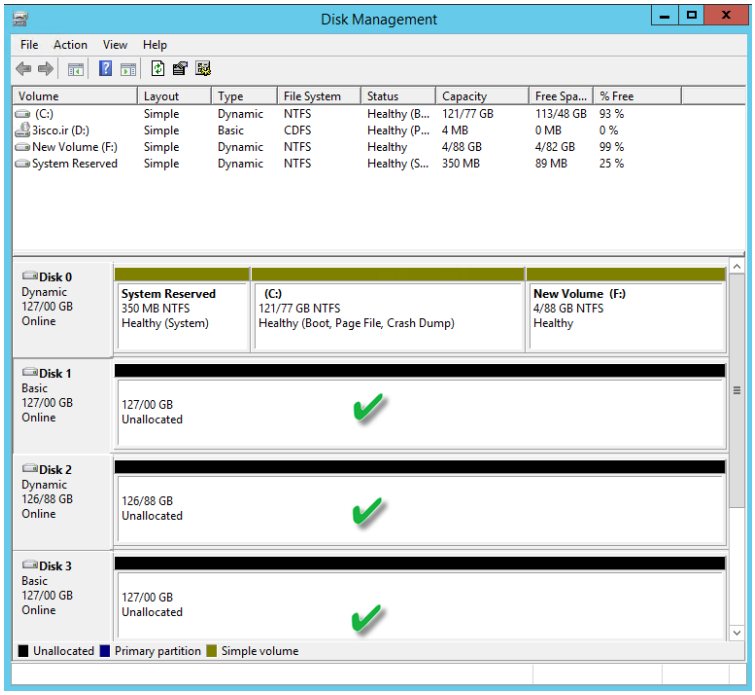
تقسیم بندی در سرویس Disk Management:

در حال حاضر اطلاعات برای هر سازمانی بسیار مهم است و تمام تلاش خود را می‌کنند تا این اطلاعات را حفظ کنند، سرویس Disk Management امکاناتی را در اختیار شما قرار می‌دهد تا با استفاده از چندین هارد دیسک از اطلاعات خود نسخه پشتیبان تهیه کنید، به این صورت نیست که پشتیبان گیری به صورت دستی انجام شود بلکه زمانی که در یک هارد دیسک اطلاعاتی راوارد می‌کنید در هارد دیسک دیگر این اطلاعات به صورت خودکار کپی می‌شود و همین کار باعث می‌شود که زمانی که یک هار دیسک از کار افتاد هارد دیسک دیگر شروع به فعالیت کند و یا از اطلاعات خود استفاده کند.

تقسیم بندی به چهار صورت زیر انجام می‌شود:

- Spanned Volume ✓
- Striped Volume ✓
- Mirrored Volume ✓
- RAID – 5 ✓

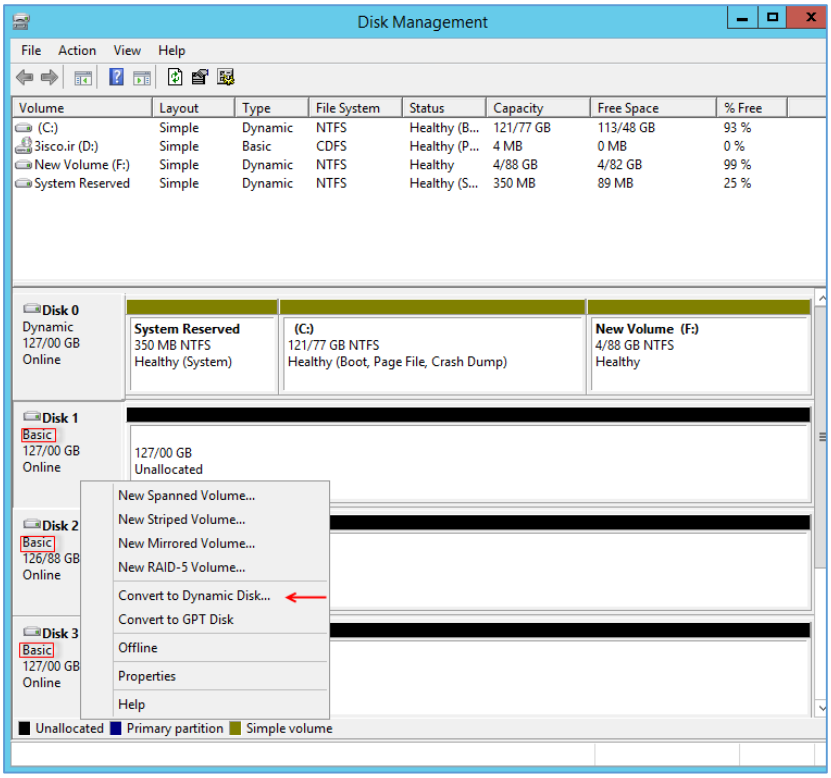
این تقسیم بندی ها را با هم بررسی می‌کنیم و نتیجه کار را مشاهده می‌کنیم، قبل از شروع 3 هارد دیسک مجازی و یا اگر از سیستم واقعی استفاده می‌کنید از هارد دیسک واقعی استفاده کنید.



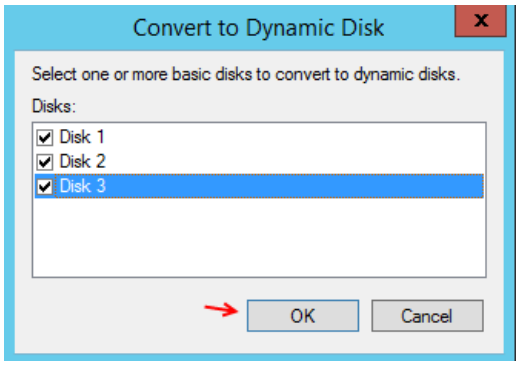
همانطور که در شکل روبرو مشاهده می‌کنید، سه هارد دیسک به لیست اضافه شده، البته به صورت مجازی این کار انجام شده، یعنی با استفاده از سرویس Hyper-v که مختص مایکروسافت می‌باشد که می‌توانید در این کتاب به قسمت بررسی سرویس Hyper-v مراجعه کنید، البته می‌توانید از نرم افزار مجازی سازی VMware 10 استفاده کنید که آموزش آن در سایت 3isco.ir موجود است.

بررسی Spanned Volume:

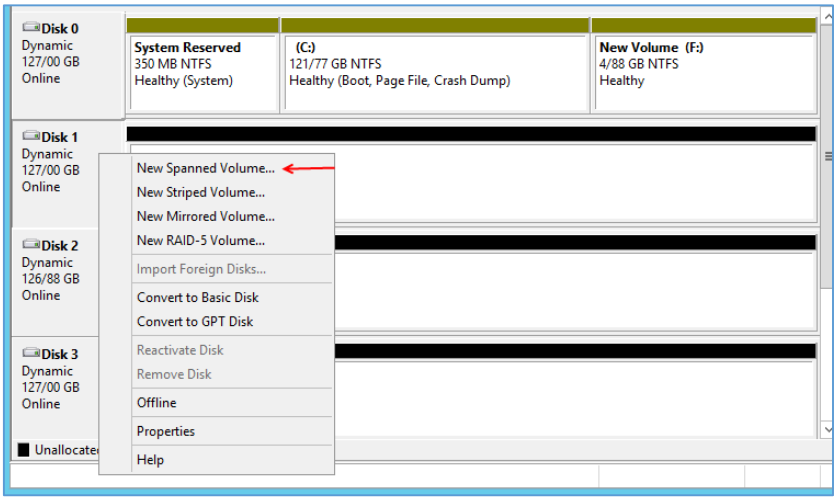
تقسیم بندی Spanned به این صورت می‌باشد که می‌توانیم از 2 هارد دیسک تا 32 هارد دیسک در این تقسیم بندی استفاده کنیم، Spanned به این صورت عمل می‌کند که اطلاعات موردنظر خود را هم زمان در چندین دیسک وارد می‌کند و اگر یکی از دیسک ها از کار افتاد کل اطلاعات از بین خواهد رفت، با هم این موضوع را بررسی می‌کنیم تا متوجه شویم این تقسیم بندی زیاد هم جالب نخواهد بود.



با دقت به این صفحه نگاه کنید، 3 دیسکی که به لیست اضافه شده است از نوع Basic می‌باشد که برای استفاده از عملیات تقسیم بندی باید به حالت Dynamic تغییر حالت دهد، برای تغییر حالت به Dynamic بر روی یکی از سه هارد موردنظر کلیک راست کنید و گزینه Convert to Dynamic Disk... را انتخاب کنید تا شکل زیر ظاهر شود.

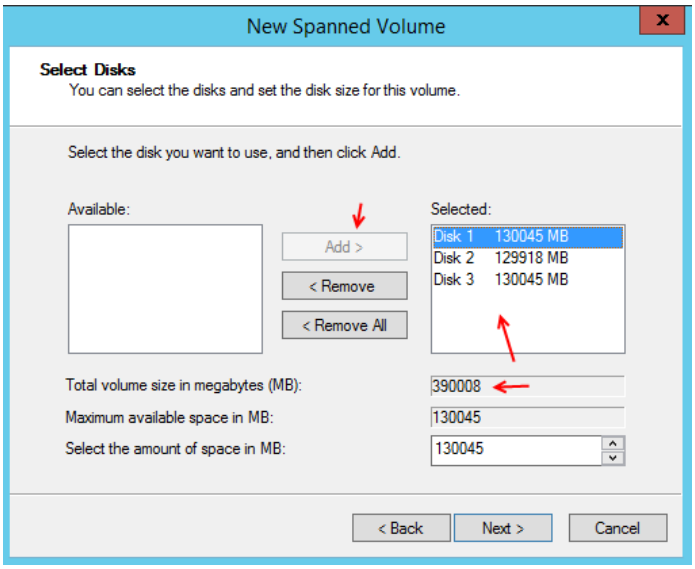


در این قسمت تیک هر سه هارد دیسک را انتخاب و بر روی Ok کلیک کنید تا همه آنها به Dynamic تغییر حالت دهند.

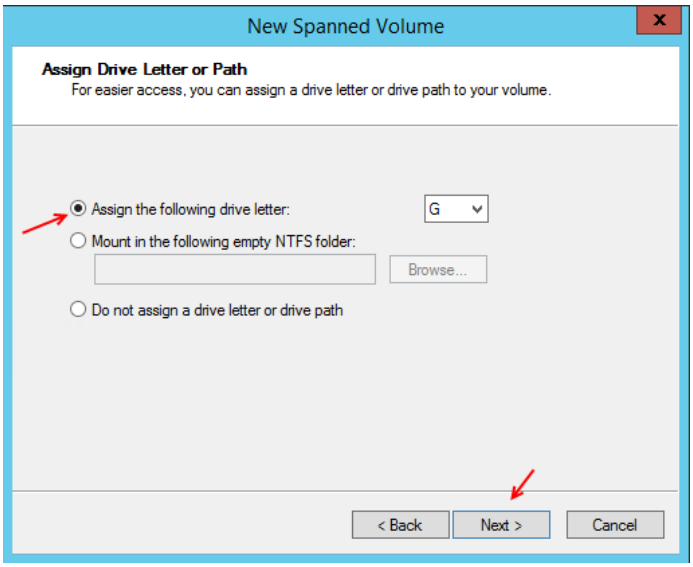


بعد از تبدل به حالت Dynamic بر روی یکی هارد دیسک کلیک راست کنید و گزینه New Spanned Volume را انتخاب کنید.

در صفحه باز شده بر روی Next کلیک کنید تا شکل صفحه بعد ظاهر شود.



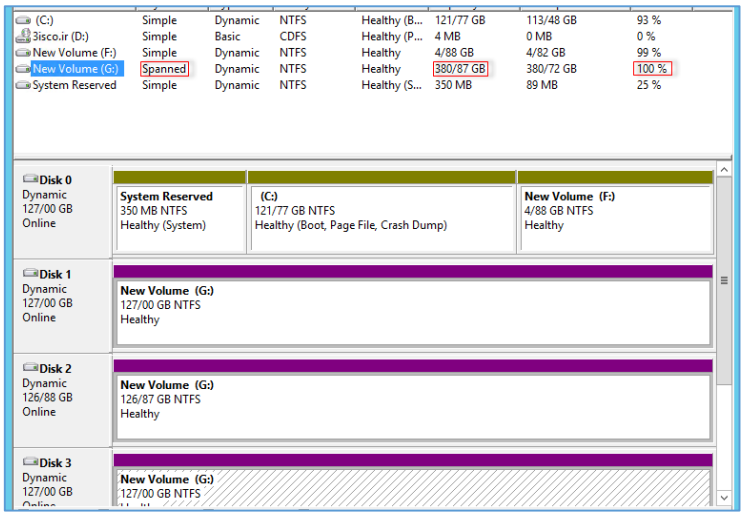
در این قسمت 3 هارد دیسک موردنظر انتخاب شده است، اگر به قسمت Total Volume size in Megabytes توجه کنید، کل فضای 3 هارد دیسک را نوشته است، بر روی Next کلیک کنید.



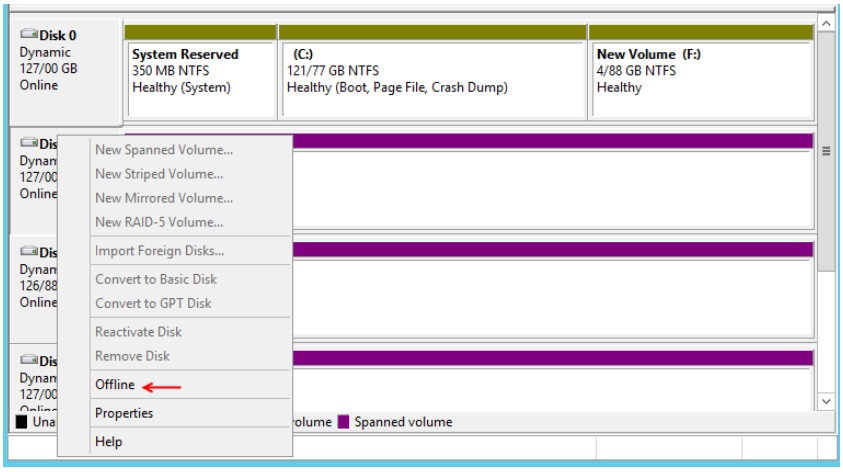
در این قسمت گزینه اول را انتخاب و نام درایو موردنظر خود را انتخاب کنید و بر روی Next کلیک کنید.

در صفحه Format دیسک هم به گزینه‌ای دست نزنید و بر روی Next کلیک کنید و در صفحه آخر هم بر روی Finish کلیک کنید.

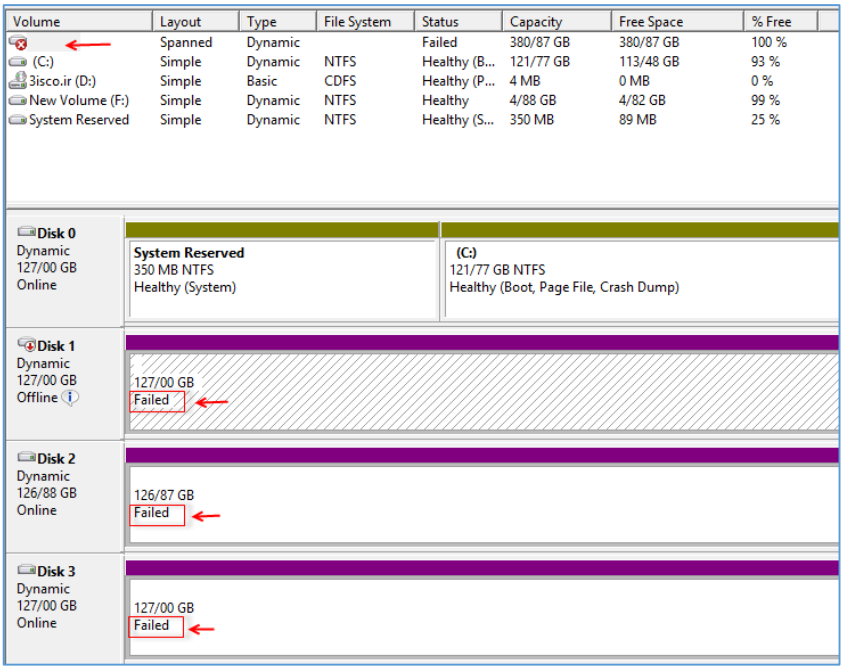
بعد از انجام کارهای بالا هر 3 هارد دیسک به صورت هم زمان Format می‌شوند.



همانطور که در شکل روبرو مشاهده می‌کنید، هارد دیسک‌های موردنظر، به صورت یک هارد با نوع Spanned تبدیل شده است، اگر به درایو G در بالا نگاه کنید نوع آن Spanned و مقدار حافظه آن را 380 در نظر گرفته است که این فضای کل هر 3 هارد دیسک می‌باشد و در قسمت Free عدد 100% نوشته شده است، یعنی اینکه این نوع هار دیسک هیچ



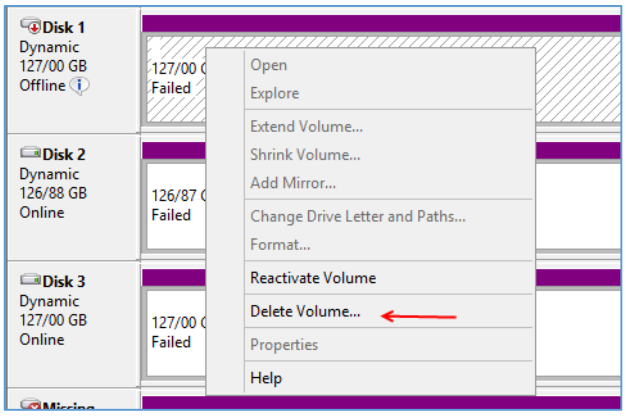
گونه امنیتی ندارد و با خراب شدن یک هارد تمام اطلاعات از بین خواهد رفت، با هم این موضوع را تست می‌کنیم، روی یکی از هارد دیسک‌ها کلیک راست کنید و گزینه Offline را انتخاب کنید تا هارد دیسک انتخاب شده از کار انداخته شود.



در این شکل مشاهده می‌کنید که هر 3 هارد دیسک از رده خارج شدند و این همان موضوعی است که استفاده از این نوع هارد دیسک‌ها با تقسیم بندی Spanned زیاد امنیت ندارد، خوبی این روش فقط استفاده از کل فضای هارد ها به عنوان یک هارد است.

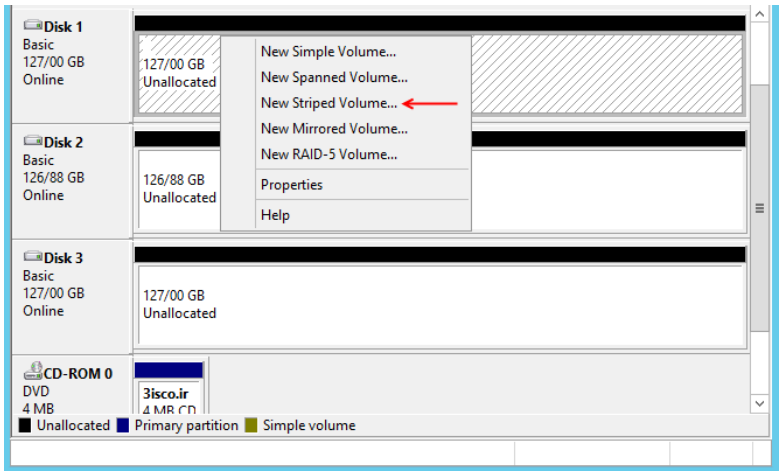
سعی کنید رنگ مربوط به هر تقسیم بندی را حفظ کنید.

بررسی Striped Volume:

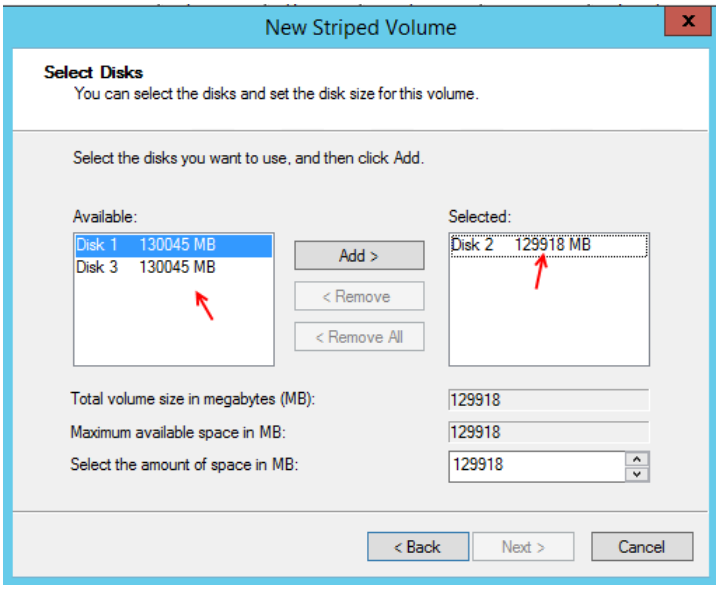


قبل از اینکه از این تقسیم بندی استفاده کنیم، برای استفاده از هارد دیسک‌های قبلی در این قسمت بر روی یکی هارد دیسک‌ها موردنظر کلیک راست کنید و گزینه Delete Volume را انتخاب کنید تا عملیات قبلی بر روی این سه هارد دیسک حذف شود. و بعد بر روی هارد دیسک موردنظر کلیک راست کنید و گزینه Online را انتخاب کنید.

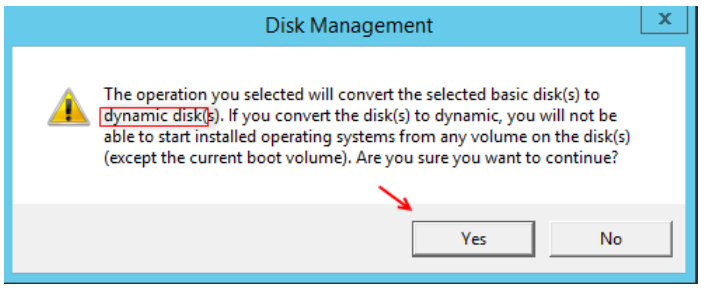
تقسیم بندی Striped به این صورت می‌باشد که در این تقسیم بندی به مانند قبل از 2 تا 32 هارد دیسک می‌توانید استفاده کنید، تقسیم بندی Striped به این صورت عمل می‌کند که به مانند قبل اگر 3 هار دیسک داشته باشیم ظرفیت همه آنها را با هم جمع می‌کند و به عنوان یک هارد دیسک در اختیار ما قرار می‌دهد که با از رده خارج شدن یکی از آنها بقیه آنها هم از کار خواهند افتاد.



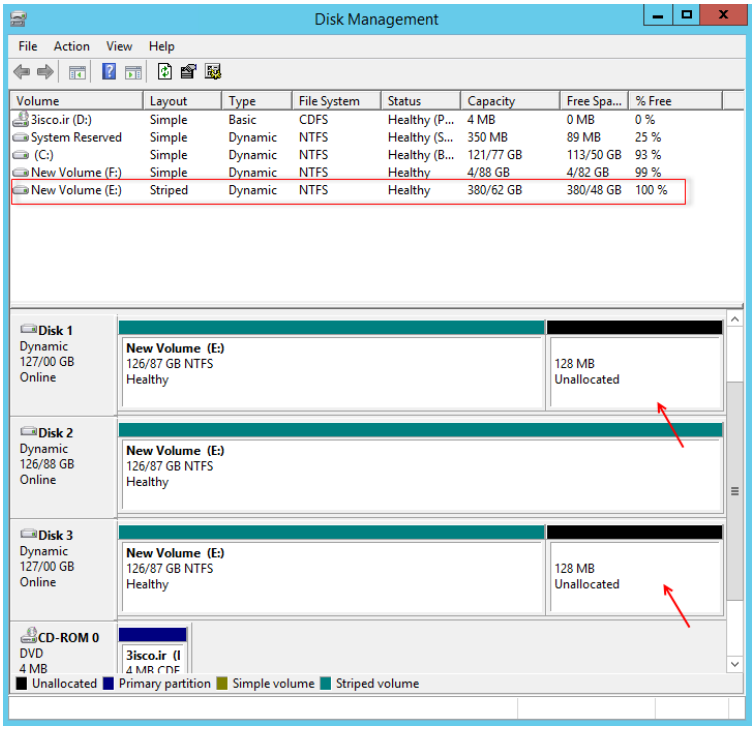
وارد سرویس موردنظر شوید و بر روی یکی از درایو ها کلیک راست کنید و گزینه New Striped Volume را انتخاب کنید، توجه داشته باشید نوع دیسک Basic می‌باشد که بعد از انتخاب گزینه New Striped Volume از شما سوأل خواهد شد که برای استفاده از این قابلیت باید دیسک تبدیل به نوع Dynamic شود، البته می‌توانید بر روی هارد دیسک های موردنظر کلیک راست کنید و گزینه Convert To Dynamic Disk را انتخاب کنید.



در قسمت قبلی با کلیک برروی New Striped Volume صفحه موردنظر اجرا می‌شود که برای شروع بر روی Next کلیک کنید تا این صفحه را مشاهده کنید، در این صفحه باید هاردهای موردنظر خود را انتخاب کنیم، یک نکته اساسی در این قسمت وجود دارد و آن این است که در هارد های موجود یکی از هاردها با حجم 129918 MB می‌باشد که زمانی که هارد های دیگر را به لیست اضافه کنید مقدار فضای آنها به این هارد که فضای آن 129918 MB می‌باشد تغییر حالت می‌دهید، یعنی اینکه هاردهای در لیست بالا با ظرفیت 130045 MB به ظرفیت 129918 MB تغییر حالت می‌دهند، بعد از انتخاب هر سه هارد بر روی Next کلیک کنید و در دو صفحه بعد بر روی Next کلیک کنید و در صفحه آخر بر روی Finish کلیک کنید تا هارد دیسک موردنظر با ظرفیت مشخص‌شده از نوع Striped ایجاد شود.



بعد از اینکه بر روی Finish کلیک کنید، شکل روبرو ظاهر می‌شود که به این موضوع اشاره دارد که برای استفاده از قابلیت تقسیم بندی دیسک باید تمام هارد دیسک‌ها به Dynamic تغییر حالت دهند، بر روی Yes کلیک کنید تا عملیات اعمال شود.



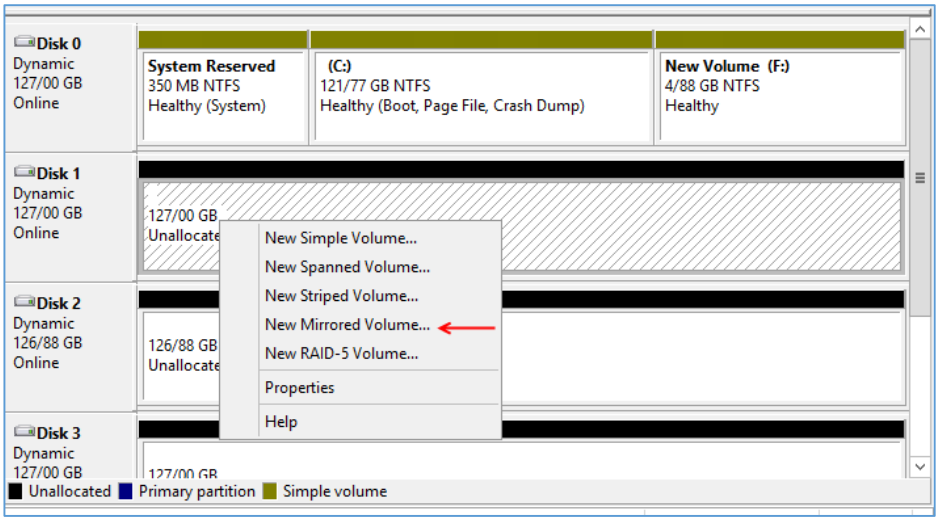
همانطور که در شکل روبرو مشاهده می‌کنید هارد دیسک موردنظر از نوع Striped ایجاد شده است، اگر به مقدار فضای آنها نگاهی بیندازید، متوجه خواهید شد 2 هارد دیسک فضای خود را با هارد دیسکی که از بقیه فضای کمتر داشت برابر کردند و به خاطر همین مقدار 128 مگابایت فضا بدون استفاده رها شده است.

این نوع تقسیم بندی به مانند تقسیم بندی قبلی بدون امنیت می‌باشد و با خرابی یک هارد دیسک بقیه آنها از کار خواهند افتاد.

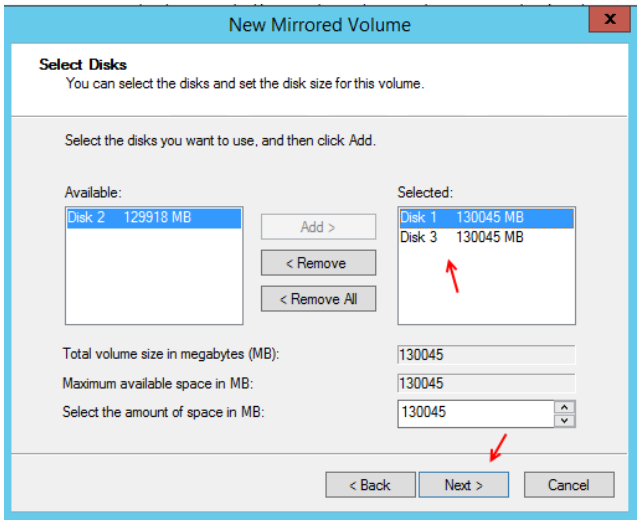
بررسی Mirroring Volume:

این تقسیم بندی با قسمت‌های قبلی تفاوتی دارد و آن این است که از امنیت کاملی برخوردار است و با از کار افتادن یکی از هارد دیسک‌ها هارد دیگر به کار خود ادامه می‌دهد، در این نوع تقسیم بندی فقط از دو هارد دیسک استفاده می‌شود که بر روی یکی از هارد دیسک ها اطلاعات قرار می‌گیرد و هم زمان بر روی هارد دیگر اطلاعات کپی می‌شود.

همانطور که قبلاً گفتم برای استفاده مجدد از هارد دیسک های قبلی بر روی یکی از آنها کلیک راست کنید و گزینه Delete Volume را انتخاب کنید و بعد بر روی آنها کلیک کنید و به Dynamic تبدیل کنید.

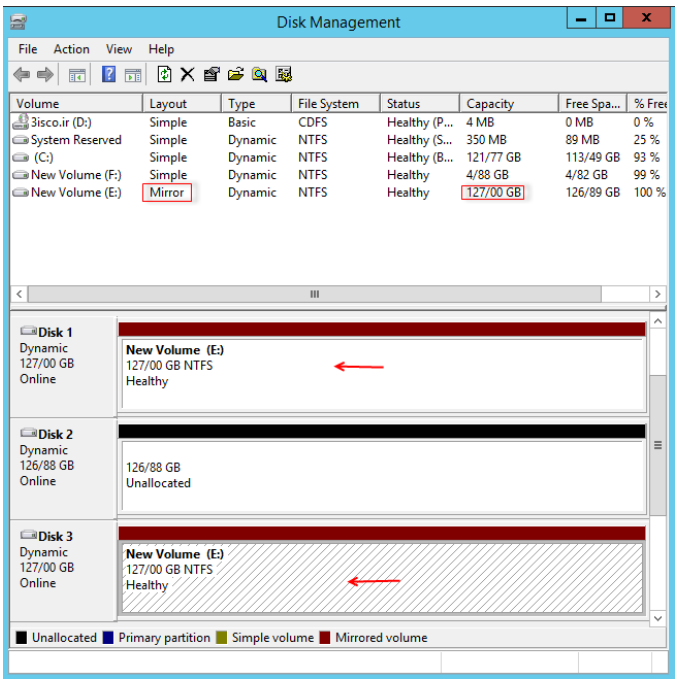


در این شکل بر روی یکی از هارد دیسک‌ها کلیک راست کنید و گزینه New Mirrored Volume را انتخاب کنید و در شکل باز شده بر روی Next کلیک کنید تا شکل زیر ظاهر شود.

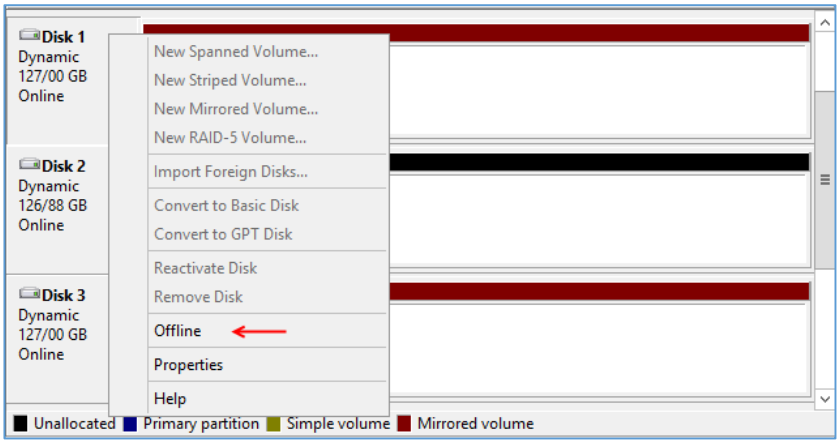


در این قسمت فقط دو هارد دیسک می‌تواند به لیست اضافه شود و هارد دیسک دیگری نمی‌تواند به لیست اضافه شود، اگر به مقدار فضای کل هارد دیسک نگاهی بیندازید متوجه خواهید شد که فقط از فضای یک هارد دیسک استفاده می‌شود.

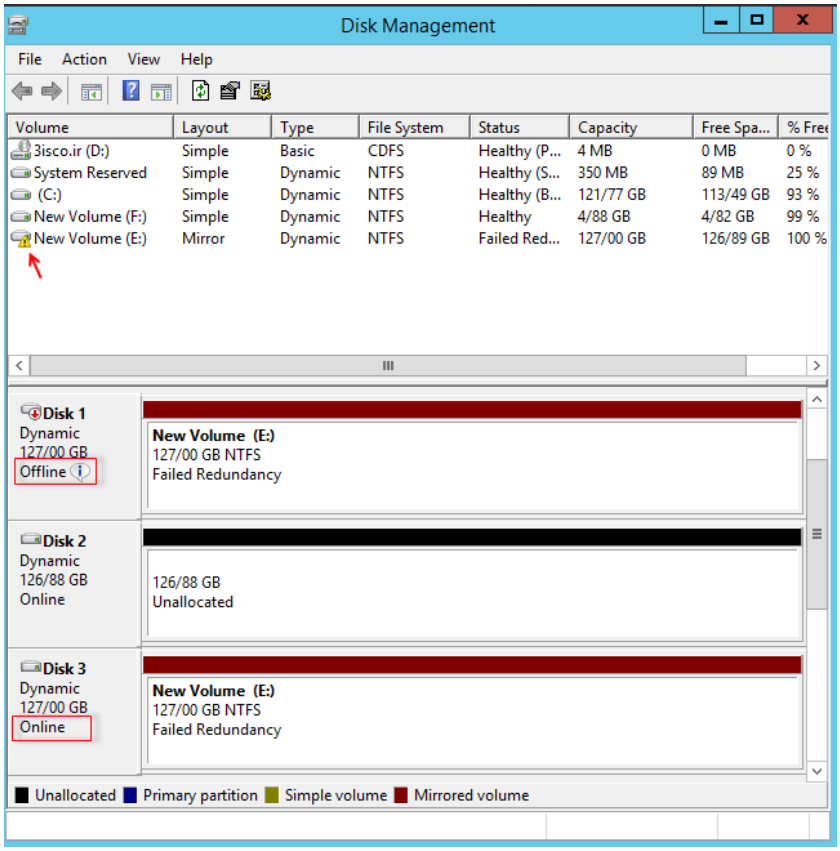
بر روی Next کلیک کنید و در دو صفحه بعد بر روی Next کلیک کنید و در صفحه آخر بر روی Finish کلیک کنید.



در شکل روبرو هارد دیسک موردنظر با قالب Mirror ایجاد شده است که امنیت اطلاعات در این نوع تقسیم بندی‌ها 100 می‌باشد، برای درک بهتر این موضوع در صفحه بعد یکی از هارد دیسک ها را از رده خارج می‌کنیم.

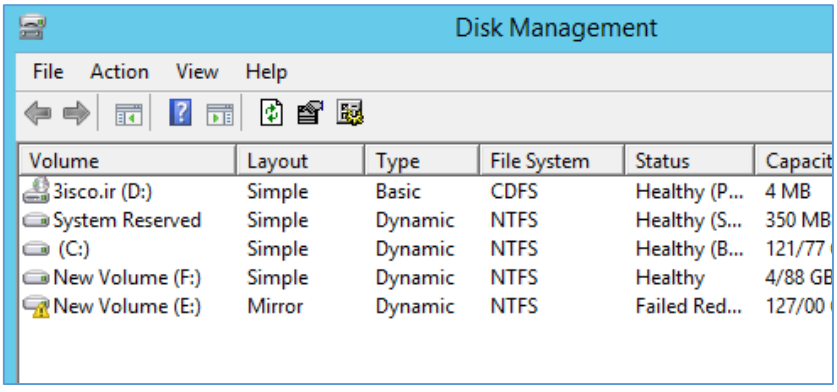


بر روی یکی از هارد دیسک‌ها که عملیات Mirror روی آن انجام شده کلیک راست کنید و گزینه Offline را انتخاب کنید تا هارد موردنظر از کار انداخته شود.

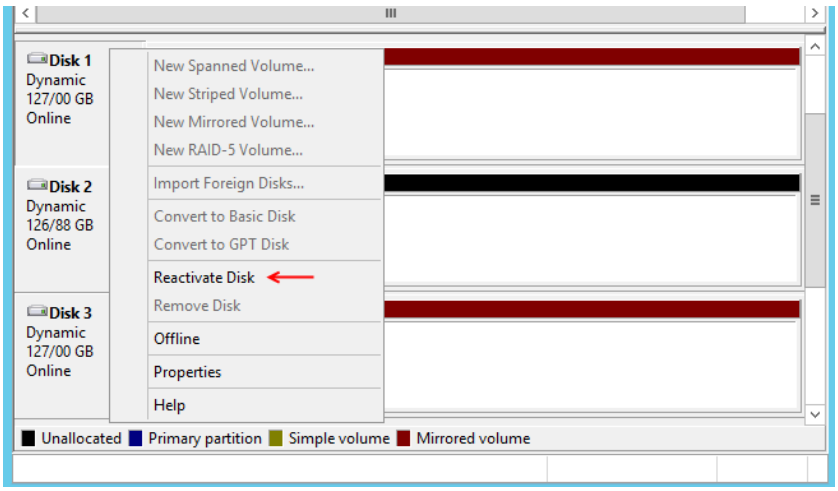


همانطور که مشاهده می‌کنید، هارد دیسک شماره 1 از کار افتاده، بعد از این عمل علامت اخطار روی درایو نمایان شده است و در قسمت پائین نوشته Failed Redundancy ظاهر شده است که نشان دهنده این است که یکی از هارد دیسک‌ها از کار افتاده و هارد دوم در حال کار می‌باشد و باید هارد اول را درست کنید.

برای حل این مشکل برروی هارد دیسکی که با مشکل مواجه شده کلیک راست می-کنیم و گزینه Online را انتخاب می‌کنیم البته در واقعیت باید هارد را تعمیر یا تعویض کنید و بعد این کار را انجام دهید.



به شکل روبرو توجه کنید که بعداز اینکه هارد دیسک را فعال کردیم، هنوز در حالت Failed Redundancy قرار دارد که برای حل این مشکل به شکل بعد توجه کنید.



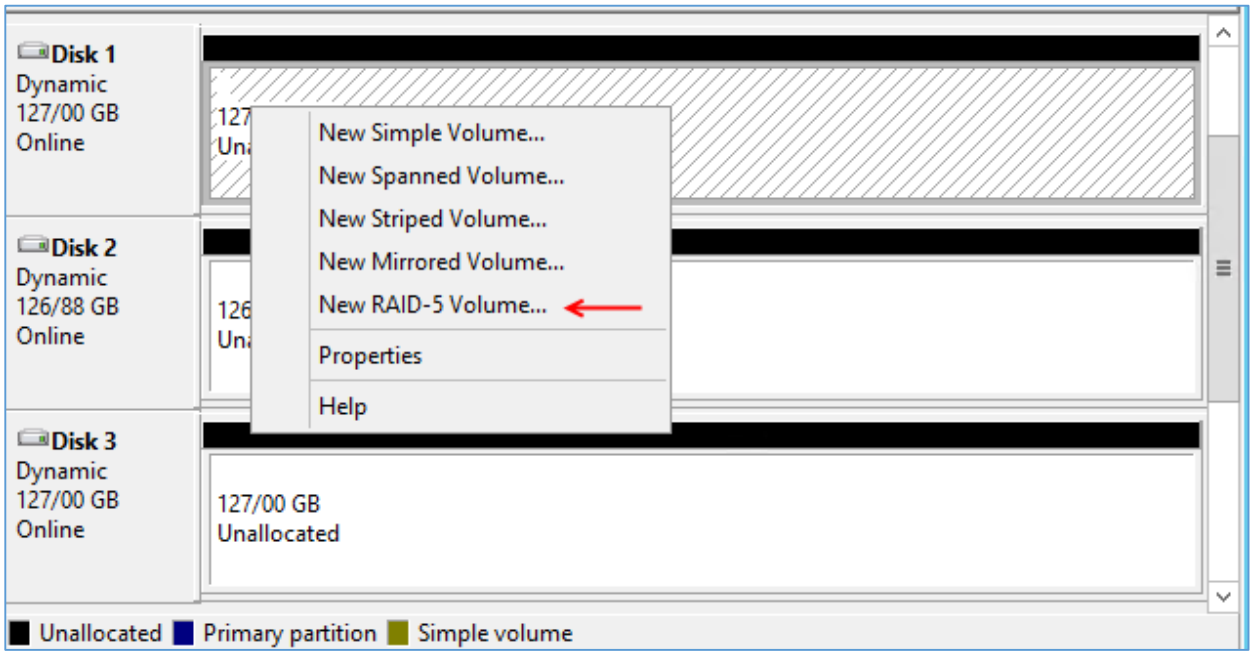
بر روی هارد دیسک دارای مشکل کلیک راست کنید و گزینه Reactivate Disk را انتخاب کنید تا همسانسازی بین دو دیسک انجام شود.

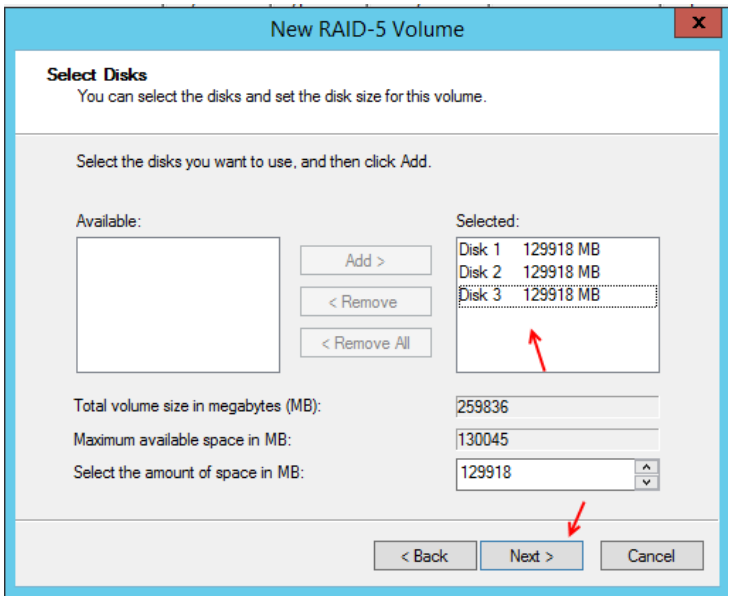
کمی باید صبر کنید تا عملیات انجام شود.

بررسی RAID – 5:

یکی از قویترین حالت های تقسیم بندی دیسک با امنیت بسیار بالا که حداقل هارد دیسک مورد نیاز برای این حالت 3 عدد می‌باشد که اطلاعات به طور همزمان بر روی هر سه هارد دیسک نوشته می‌شود و با از کار افتادن یک هارد، بقیه هاردها به کار خود ادامه می‌دهند ولی اگر دوتا از هاردها از کار انداخته شود هارد سوم هم از کار انداخته خواهد شد.

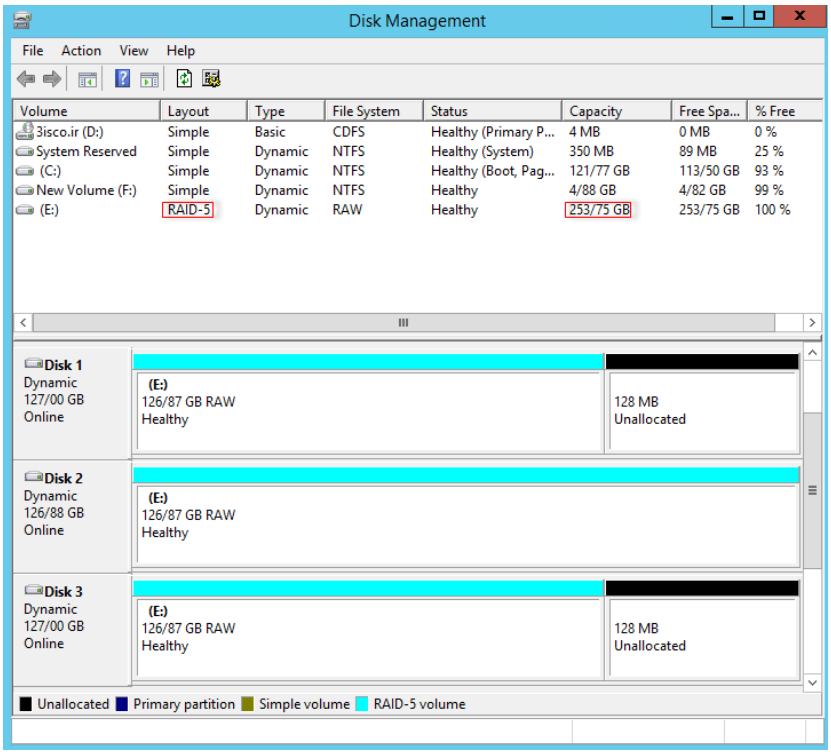
به مانند شکل زیر بر روی یکی از هاردهای زیر کلیک راست کنید و گزینه New RAID-5 را انتخاب کنید.





در این صفحه هر سه هارد دیسک را به لیست اضافه کنید و بر روی Next کلیک کنید.

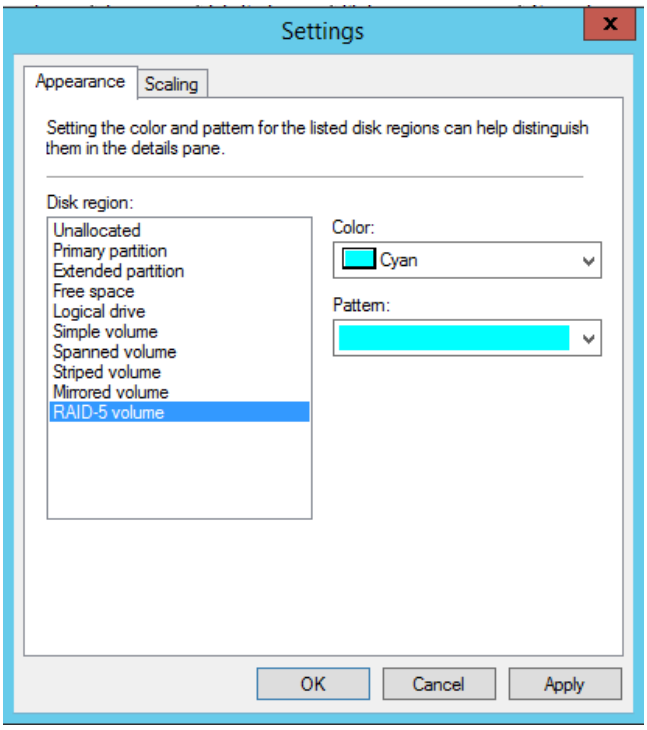
در دو صفحه بعدی بر روی Next کلیک کنید و در صفحه آخر بر روی Finish کلیک کنید تا کار ایجاد هارد با قالب RAID-5 ایجاد شود. بسته به ظرفیت هارد دیسک شما کمی زمان بر خواهد بود.



همانطور که در این قسمت مشاهده می‌کنید، هارد دیسک‌ها با قالب RAID-5 ایجاد شده‌اند، به این نکته توجه کنید که مقدار فضای کل هارد برابر با 33% از هر هارد می‌باشد و بقیه برای پشتیبان گیری و امنیت مورد استفاده قرار می-گیرند.

در این حالت اگر یک هارد از کار بیفتد، دو هارد دیگر به کار خود بدون مشکل با حفظ اطلاعات خود ادامه می‌دهند.

در شکل روبرو هارد شماره یک غیر فعال شده ولی بقیه هاردها به کارخود ادامه می‌دهند.

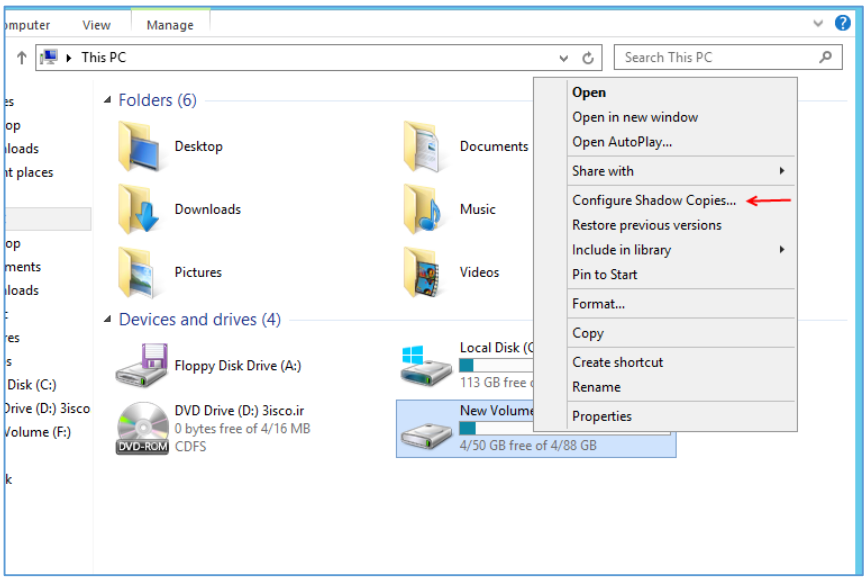


اگر به نوع دیسک‌ها توجه کرده باشید، همه قالب هایی ایجاد کرده بودیم، دارای رنگبندی خاصی بودن که به صورت پیش فرض تعریف شده بود، برای تغییر این رنگبندی ها وارد منوی View شوید و گزینه Settings را انتخاب کنید.

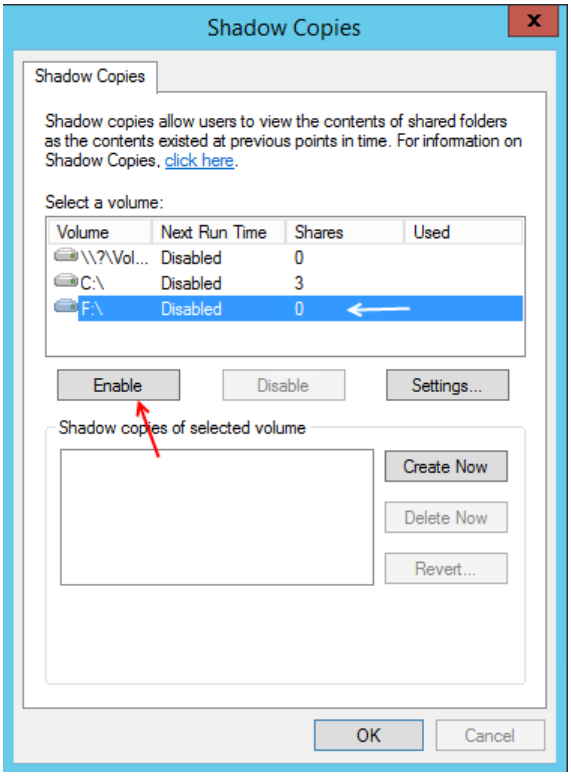
در این شکل شما می‌توانید گزینه موردنظر خود را انتخاب و رنگ آن را به دلخواه خود تغییر دهید.

کار با قابلیت Shadow Copy در درایوها:

یکی از امکانات فوق العاده در ویندوز سرور استفاده از قابلیت Shadow Copy می‌باشد که این امکان را در اختیار شما قرار میدهد تا زمانی که اطلاعاتی را داخل درایو موردنظر خود قرار می‌دهید یک کپی از آن اطلاعات در زمان خاص ایجاد کند تا موقع از دست رفتن اطلاعات دوباره بتوان به صورت سریع آنها را برگشت داد که کار جالبی خواهد بود، این کار را با هم به صورت عملی انجام می‌دهیم.

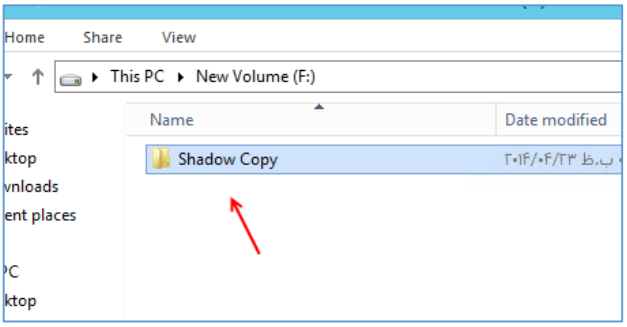


به دو طریق می‌توانید وارد تنظیمات Shadow Copy شوید، یکی اینکه روی درایو موردنظر کلیک راست کنید و گزینه Properties را انتخاب کنید و به تب Shadow Copy مراجعه کنید یا به صورت شکل روبر بر روی درایو

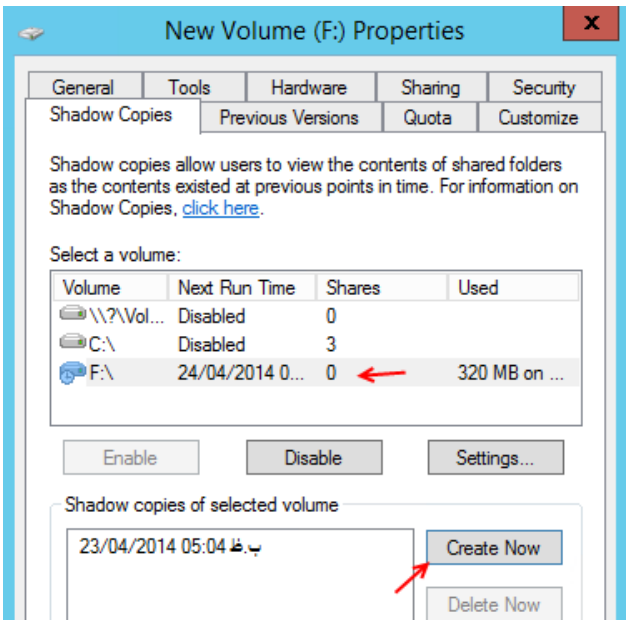


موردنظر کلیک راست کنید و گزینه Configure Shadow Copies را انتخاب کنید تا شکل روبرو ظاهر شود، در این صفحه اول باید نام درایو مورد نظر را انتخاب کنید و بعد برای فعال سازی این فابلیت بر روی Enable کلیک کنید و در صفحه باز شده بر روی Yes کلیک کنید تا قابلیت Shadow روی درایو مشخص‌شده فعال شود.

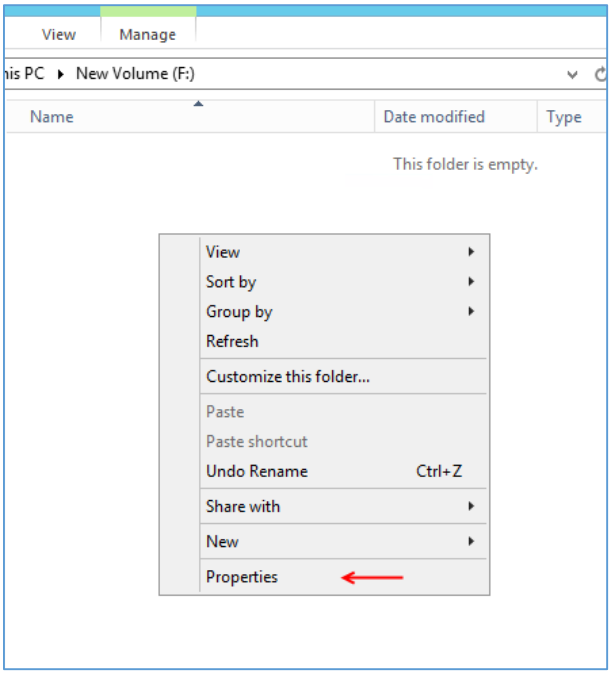
بعد از این کار می‌خواهیم یک پوشه در درایو موردنظر ایجاد کنیم و بعد یک Shadow از درایو موردنظر ایجاد کنم و بعد پوشه موردنظر را حذف کنیم و بعد برگشت دهیم.



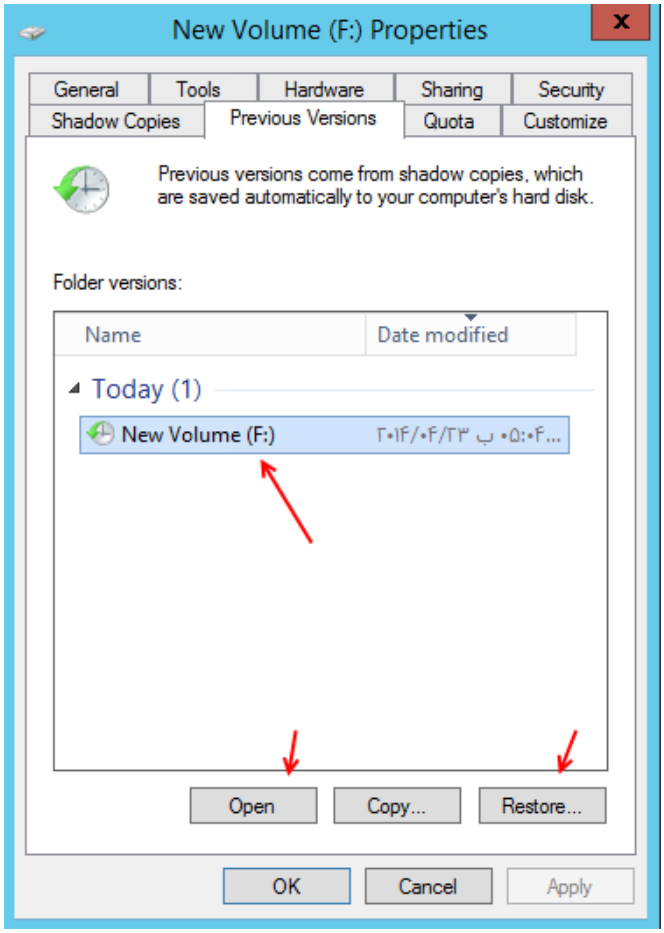
در این قسمت، پوشه موردنظر در درایو موردنظر ایجاد می‌کنیم، بعد از آن دوباره به قسمت shadow Copies مربوط به درایو موردنظر مراجعه می‌کنیم و یک Shadow از اطلاعات داخل درایو ایجاد می‌کنیم.



به مانند شکل روبرو وارد تب Shadow Copies می‌شویم و نام درایو را از لیست انتخاب می‌کنیم و بر روی Create Now کلیک می‌کنیم تا عملیات Shadow انجام شود، بعد از آن بر روی ok کلیک کنید و پوشه ایجاد شده قبلی را حذف کنید.



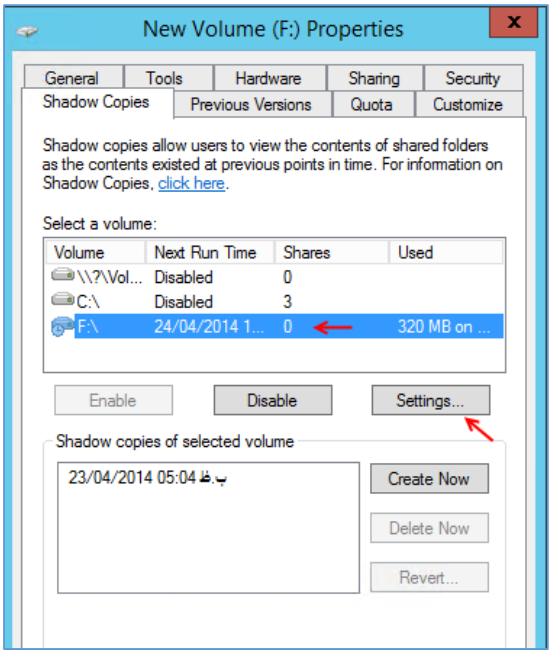
در شکل روبرو پوشه ایجاد شده با نام Shadow Copy حذف شده است و می‌خواهیم با استفاده از قابلیت Shadow اطلاعات از دست داده را برگردانیم، برای این کار در قسمت خالی صفحه کلیک راست می‌کنیم و گزینه Properties را انتخاب می‌کنیم.



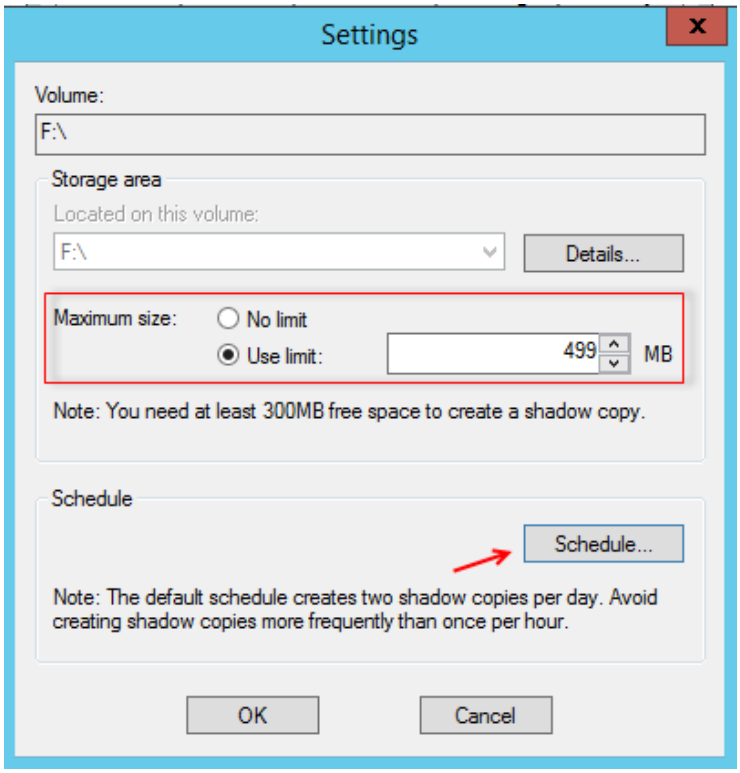
وارد تب Previous Versions می‌شویم و همانطور که مشاهده می‌کنید یک نسخه از درایو موردنظر در زمان و تاریخ مشخص‌شده ایجاد شده است، اگر بر روی Open کلیک کنید پوشه قبلی را مشاهده خواهید کرد، برای برگشت اطلاعات به حالت مشخص‌شده قبل بر روی Restore کلیک کنید و در صفحه باز شده بر روی Restore کلیک کنید.

نکته: زمانی که قابلیت Shadow Copies را روی یک درایو فعال می‌کنید، اگر اطلاعات داخل یک پوشه تغییر کرده است و می‌خواهید آن را به حالت قبل برگردانید دیگر لازم نیست که روی درایو این کار را انجام دهید بلکه فقط کافی است روی پوشه موردنظر کلیک راست کنید و Properties را انتخاب کنید و به تب Previous Versions مراجعه کنید.

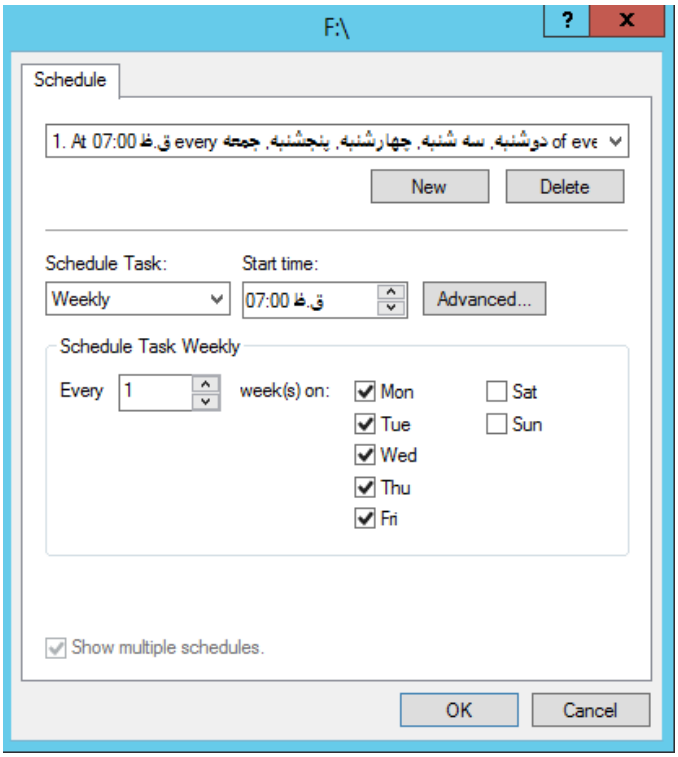
تا به اینجا نحوه فعال سازی و کارکرد قابلیت Shadow Copies را فرا گرفتیم و در این قسمت می‌خواهیم زمان بندی را برای اجرای عملیات Shadow ایجاد کنیم، برای ایجاد زمان بندی بر روی درایو موردنظر کلیک راست کنید و گزینه Configure Shadow Copy را انتخاب کنید تا شکل زیر ظاهر شود.



در تب Shadow Copies بر روی نام درایو کلیک کنید و بعد بر روی Settings کلیک کنید.



در این صفحه می‌توانید در قسمت Maximum Size مشخص کنید که مقدار فضا برای عملیات Shadow چقدر باشد و یا با انتخاب گزینه No Limit مقدار نامحدود را به آن بدهید، برای ایجاد زمان بندی بر روی Schedule... کلیک کنید تا شکل صفحه بعد ظاهر شود.

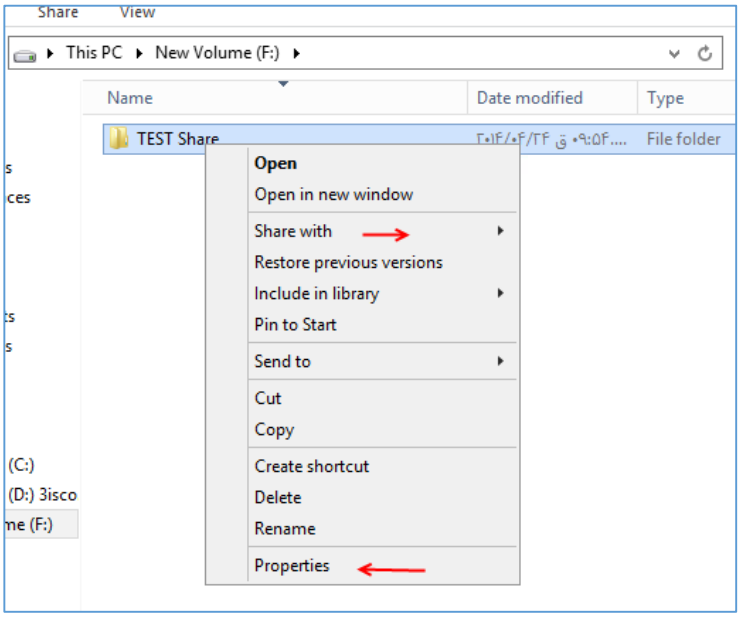


همانطور که مشاهده می‌کنید، به صورت پیش فرض مقدار اولیه به برنامه داده شده است و در روزهای مشخص‌شده روزی یک بار این کار را در ساعت 7 صبح انجام می‌دهد که شما می‌توانید این زمان و روزها را تغییر دهید.

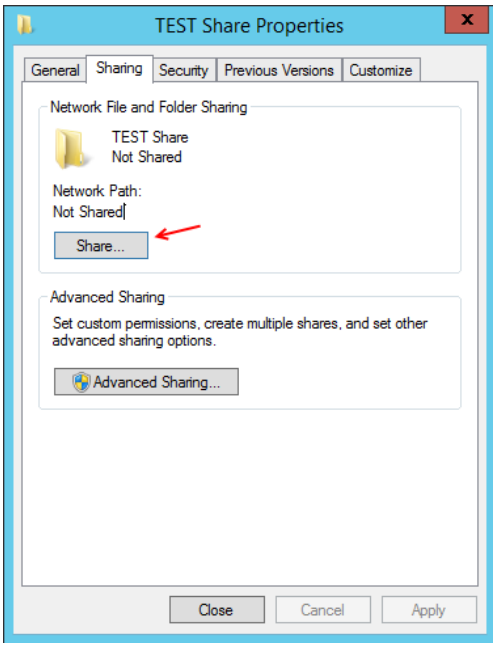
بر روی ok کلیک کنید تا تنظیمات موردنظر ذخیره شود.

به اشتراک گذاری فایل‌ها:

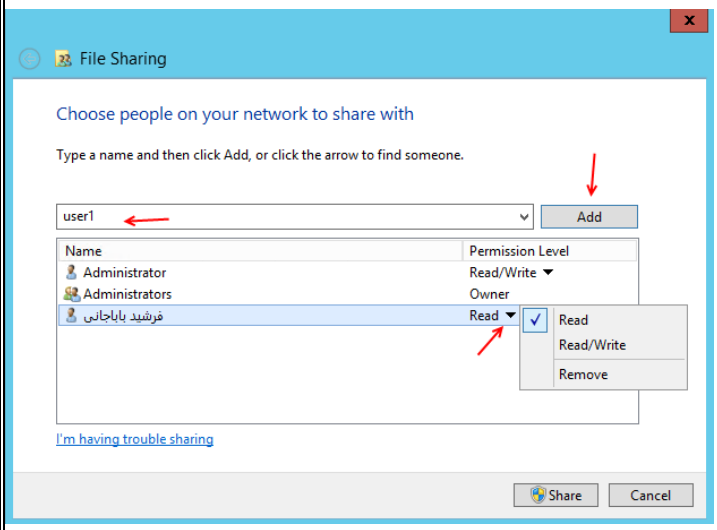
به اشتراک گذاری یا همان Share کردن فایل‌ها یکی از قابلیت های ابتدایی هر سیستم عامل در حال حاضر می‌باشد که توانسته کمک خوبی برای اشتراک گذاری فایل‌ها در شبکه باشد. در این قسمت یک پوشه را با هم Share می‌کنیم و نحوه ایجاد امنیت در به اشتراک گذاری فایل‌ها را بررسی می‌کنیم.



وارد درایو موردنظر خود می‌شویم و یک پوشه با نام TEST Share ایجاد می‌کنیم، بعد از آن بر روی آن کلیک راست می‌کنیم و گزینهProperties را انتخاب می‌کنیم، البته می‌توانیم از طریق قسمت Share With به قسمت share دست پیدا کنیم.



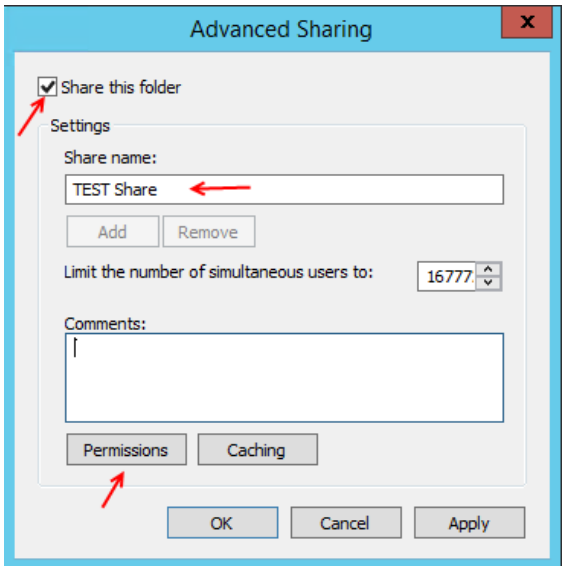
در این صفحه به دو طریق می‌توان فایل موردنظر را برای کاربر موردنظر با مجوز خاص share کرد که فعلاً در این قسمت گزینه Share... را انتخاب می‌کنیم.



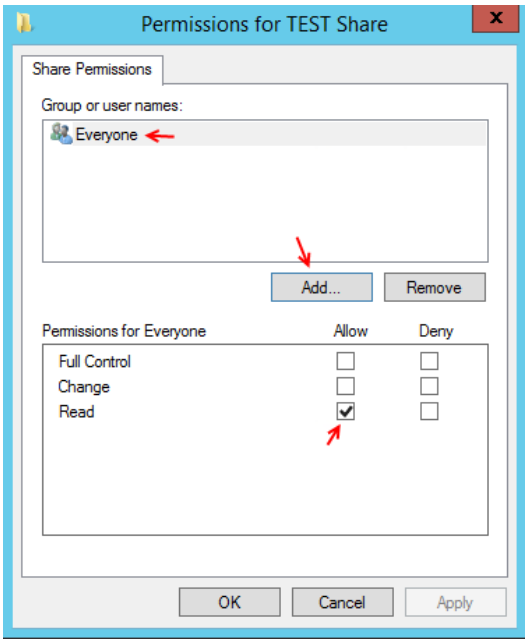
در این قسمت باید نام کاربر موردنظر را در قسمت مشخص‌شده که User1 نوشته شده وارد کنید و بعد بر روی Add کلیک کنید تا به لیست اضافه شود و یا می‌توانید بر روی منوی کشویی که User1 وارد شده کلیک کنید و بعد بر روی Find People کلیک کنید.

بعد از اضافه کردن کاربر موردنظر به لیست بر روی منوی کشویی جلوی آن کلیک کنید در این منو شما می‌توانید مجوز Read یعنی فقط کاربر می‌تواند فایل را بخواند و نمی‌تواند آن را ویرایش و حذف کند و گزینه Read/Write همان Full Control می‌باشد که کاربر موردنظر توانایی حذف فایل را هم دارد. گزینه آخر هم Remove می‌باشد که برای حذف کاربر از لیست است، بعد از انتخاب کاربر و دادن مجوز لازم بر روی Share کلیک کنید تا پوشه موردنظر Share شود.

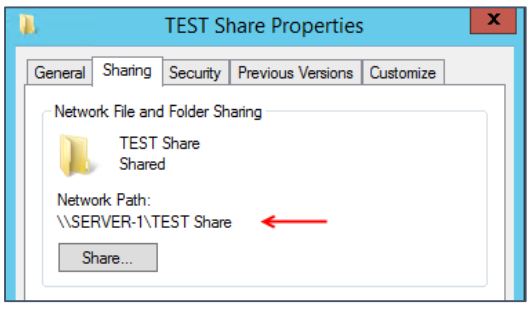
روش پیشرفته تری هم وجود دارد که می‌توانیم فایل یا پوشه خود را برای دیگران Share کنیم، برای این کار زمانی که وارد تب Sharing فایل موردنظر می‌شویم، بر روی Advanced Sharing کلیک کنید تا شکل زیر ظاهر شود.



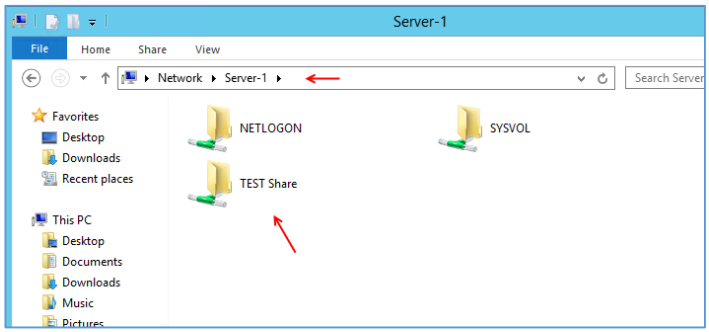
در این صفحه تیک گزینه Share this folder را انتخاب کنید و در قسمت Share Name نام فایلی که می‌خواهید Share شود را وارد کنید، توجه داشته باشید که هر چیز که در این قسمت وارد کنید همان هم در قسمت Share برای دیگران نمایش داده می‌شود. در قسمت Limit the number... تعداد کاربران استفاده از این فایل را مشخص کنید که به صورت پیش فرض 16777 وارد شده است، اگر بر روی Apply کلیک کنید فایل موردنظر Share خواهد شد ولی اگر بخواهید این فایل را فقط برای کاربر خاصی Share کنید باید بر روی Permissions کلیک کنید.



اگر به لیست کاربران و گروه‌ها توجه کنید، فقط گروه Everyone قرار دارد که نشان دهنده این است که این پوشه برای تمام کاربران با دسترسی Read اشتراک گذاشته شده، اگر می‌خواهید این پوشه را برای کاربر خاصی Share کنید، گروه Everyone را انتخاب و بر روی Remove کلیک کنید تا گروه موردنظر از لیست حذف شود، بعد برای اضافه کردن کاربر موردنظر بر روی Add کلیک کنید و کاربر موردنظر را به لیست اضافه کنید.

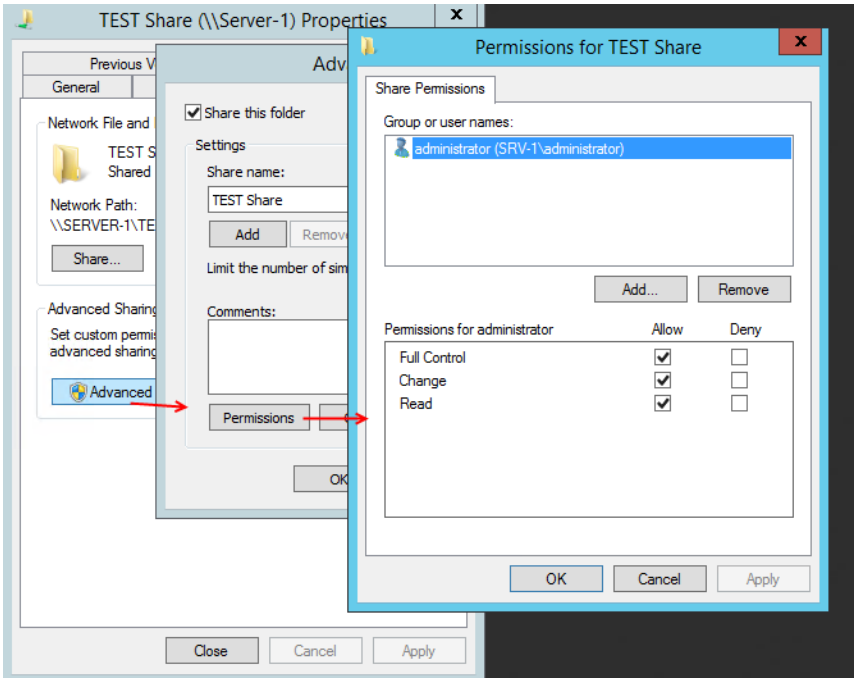


بعد از اینکه فایل را Share کردین در قسمت Network Path مسیر فایل در شبکه مشخص می‌شود یعنی با وارد کردن آدرس موردنظر در Address bar می‌توانید به فایل موردنظر دسترسی پیدا کنید.

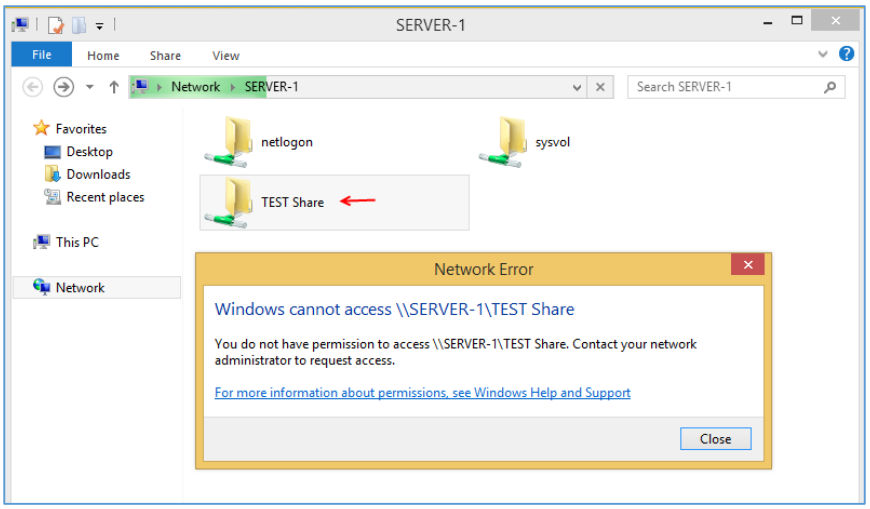


برای ورود به قسمت Share باید از آدرس \\ServerName استفاده کنید که به جای ServerName باید نام سرور خود و یا آدرس IP آن را وارد کنید. به مانند شکل روبرو عمل کند.

\\Server-1\



زمانی که یک پوشه را برای یک کاربر خاص Share کنید و به بقیه کاربران دسترسی ندهید، کاربران دیگر به جزء کاربران موجود در لیست روبرو نمی‌توانند به فایل موردنظر دسترسی داشته باشند. در شکل روبرو پوشه Test Share فقط برای کاربر Administrator اشتراک گذاشته شده است و کاربران دیگر مجوز دسترسی به این فایل را ندارند، برای تست این موضوع با کاربر User1 که قبلاً ایجاد کرده بودیم وارد ویندوز 8 خود می‌شویم که قبلاً آن را به شبکه متصل کرده بودیم.

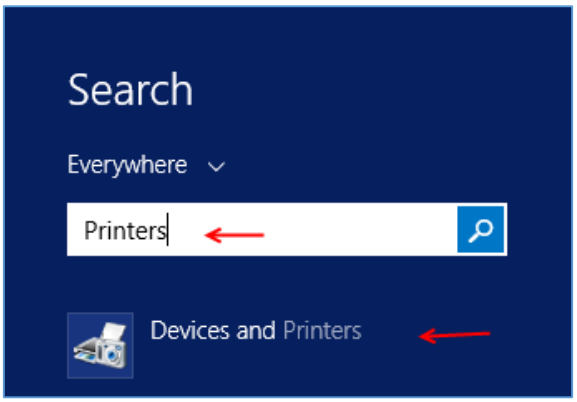


در شکل روبرو وارد آدرس \\Server-1 شده‌ایم که فایل های Share شده ویندوز سرور را برای ما لیست کرده است که با دابل کلیک بر روی پوشه Test Share با پیغام روبرو مواجه شده‌ایم در این پیغام به شما خسته نباشید گفته و به این موضوع اشاره دارد که این پوشه

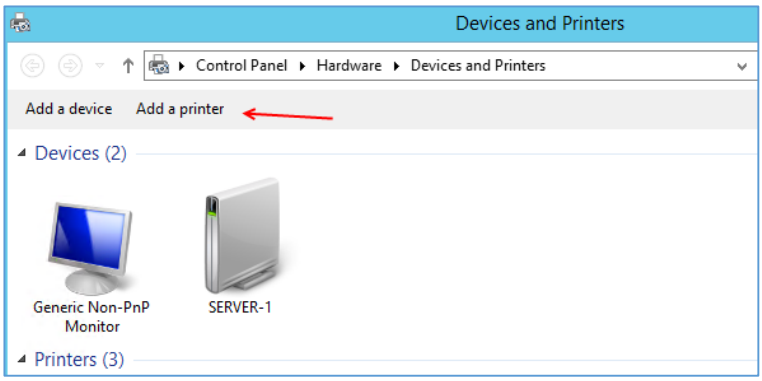
توسط صاحب آن برای شما Share نشده است و مجوز دسترسی به شما داده نشده است. پس اگر در جایی دیگر با این پیغام مواجه شدید بدانید که فایل موردنظر برای شما Share نشده است.

نصب وراه اندازی Print Server:

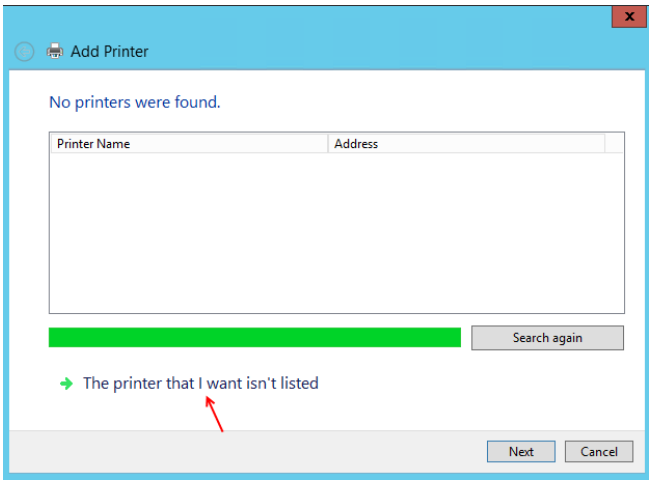
استفاده از Printer در شبکه ها یکی از مقدماتی ترین کارها در سازمان‌ها می‌باشد که استفاده گسترده‌ای از آن می‌شود، در این بخش در اول کار یک پرینتر را نصب و نحوه Share کردن آن برای دسترسی در کل شبکه را بررسی می‌کنیم.



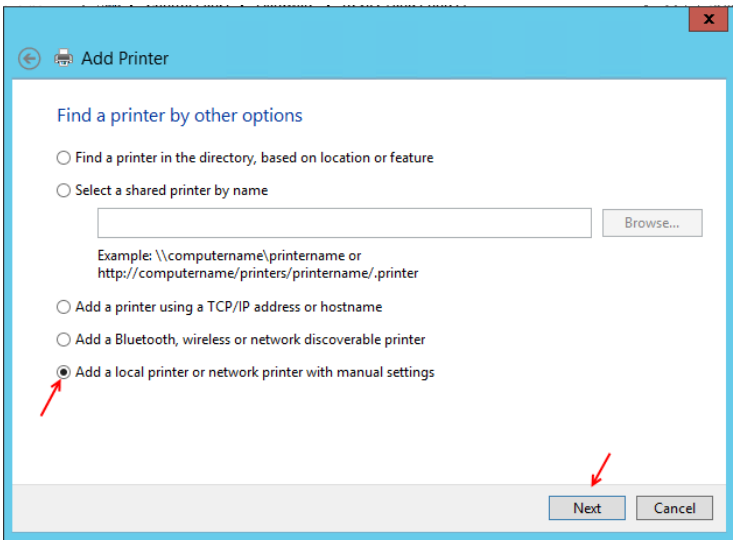
وارد ویندوز سرور 2012 شوید و در قسمت Search کلمه Printers را وارد کنید و در نتیجه جستجو بر روی Device and Printers کلیک کنید.



در این صفحه باید پرینتر خود را به لیست اضافه کنیم، برای این کار بر روی Add a Printer کلیک کنید تا شکل بعد ظاهر شود.

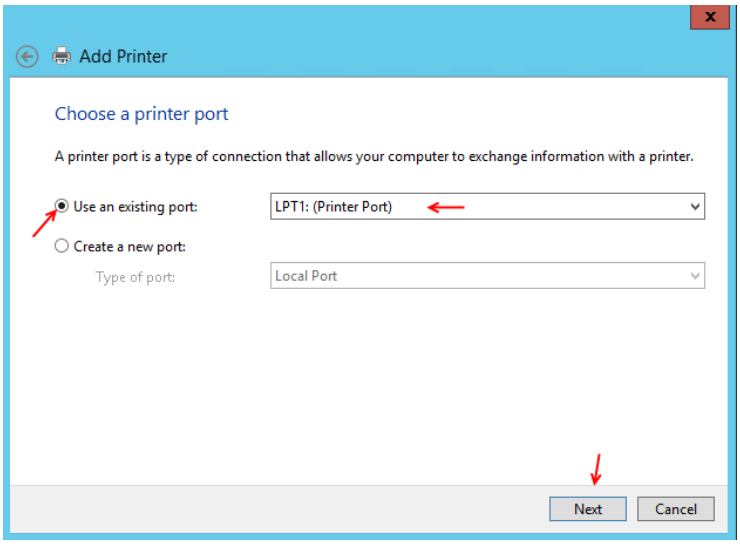


در این صفحه، عملیات جستجو برای یافتن دستگاه جدید آغاز می‌شود که اگر عملیات بدون نتیجه بود بر روی The Printer that I want isn’t listed کلیک کنید.

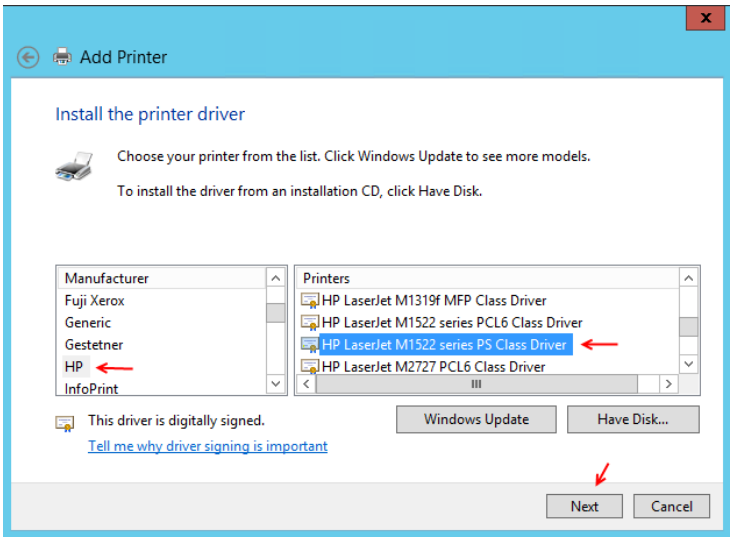


در این قسمت گزینه های مختلفی برای، انتخاب Printer موردنظر قرار دارد که همه آنها را بررسی خواهیم کرد، در حال حاضر گزینه آخر را انتخاب کنید تا بتوانید یک پرینتر به صورت پیش فرض تعریف کنیم.

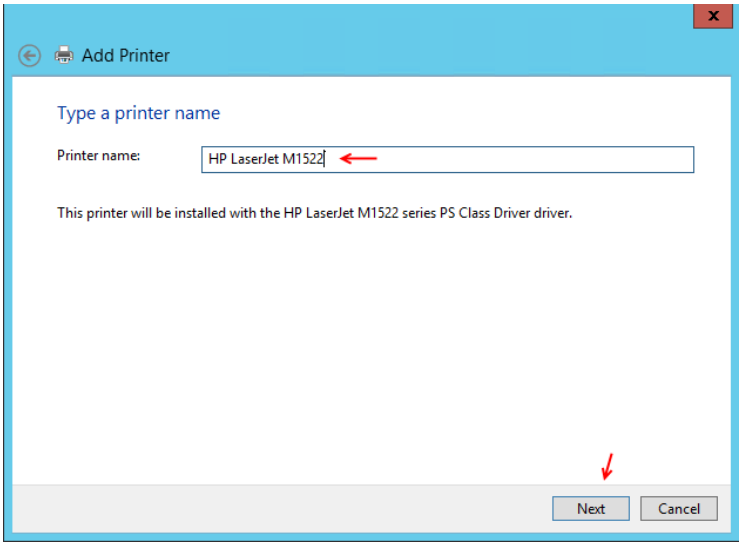
بر روی Next لیک کنید.



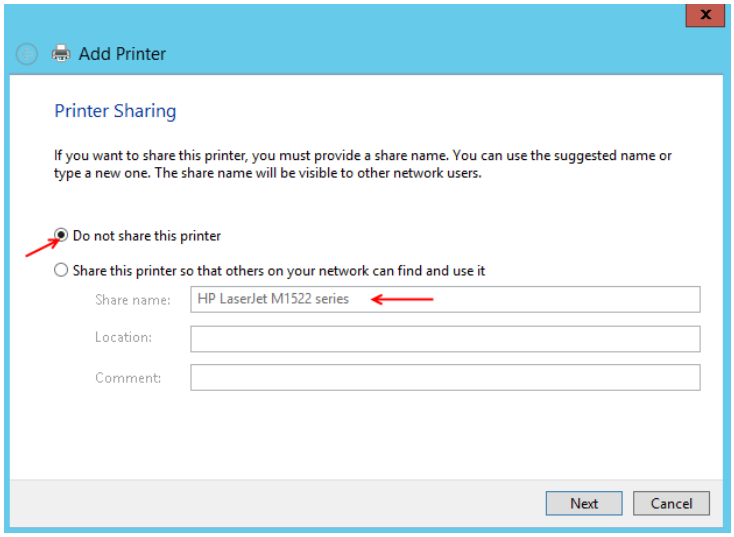
در این قسمت گزینه اول را انتخاب و پورت LPT1 را انتخاب کنید، وبعد بر روی Next کلیک کنید.



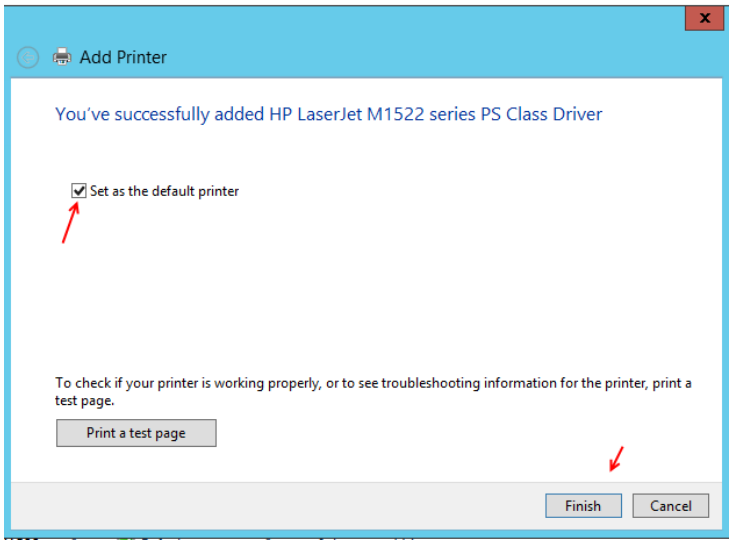
در این صفحه نام کارخانه سازنده و مدل پرینتر را انتخاب و برروی Next کلیک کنید.



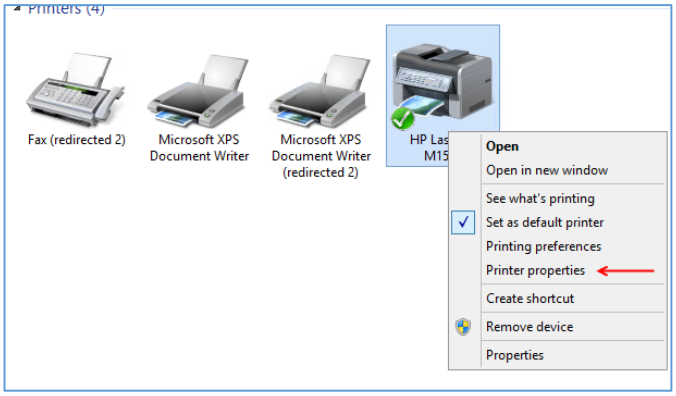
در این قسمت نام پرینتر خود را وارد کنید و بر روی Next کلیک کنید



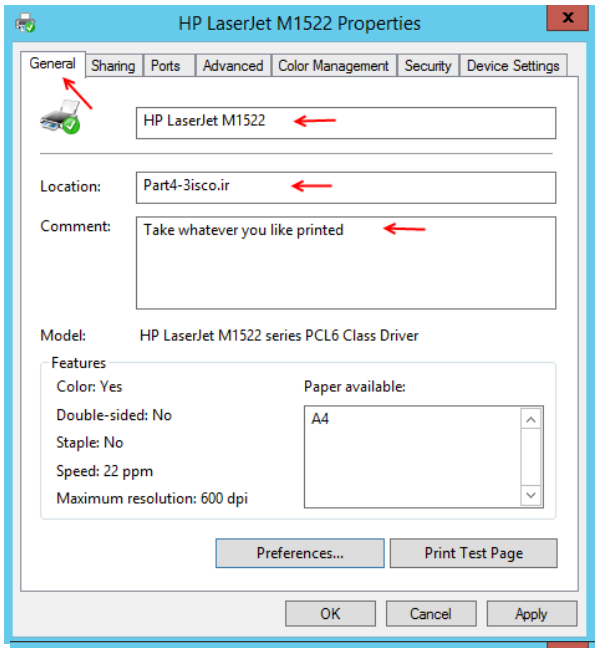
این قسمت مربوط به share کردن Printer می-باشد که در حال حاضر گزینه اول را انتخاب و بر روی Next کلیک کنید.



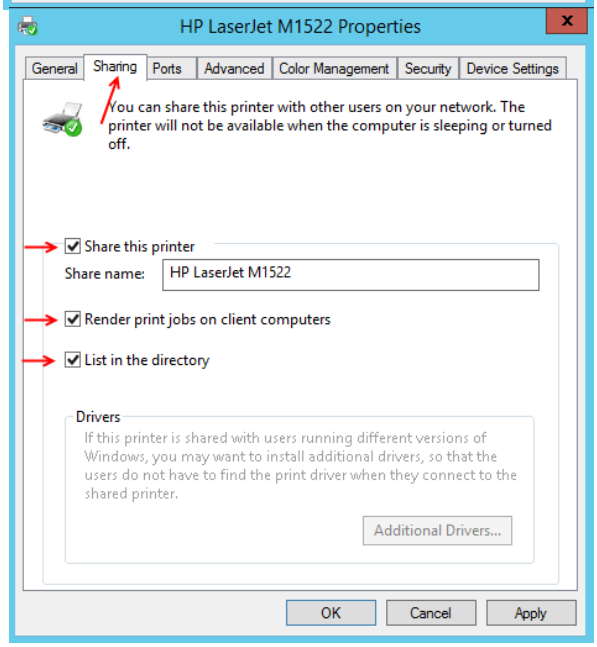
در این قسمت تیک گزینه Set as the default printer را انتخاب تا به عنوان Printer پیش فرض انتخاب شود. بر روی Finish کلیک کنید تا Printer موردنظر ایجاد شود.



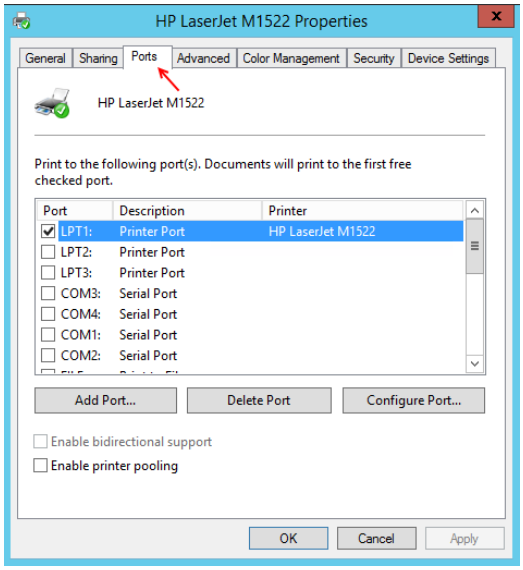
بعد از ایجاد Printer موردنظر بر روی آن کلیک راست کنید و گزینه Printing Properties را انتخاب کنید.



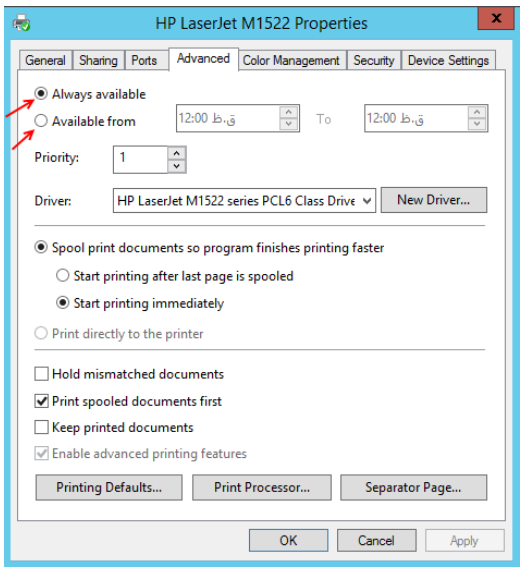
در این صفحه وارد تب General می‌شویم، در این تب در قسمت اول می‌توانید نام Printer خود را تغییر دهید، در قسمت Location منطقه قرار گیری Printer را مشخص کنید، در قسمت Comment پیغامی را قرار دهید. در قسمت پائین صفحه با انتخاب Preferences می‌توانید اندازه کاغذ، نوع کاغذ، سیاه و سفید بودن و یا رنگی بودن و..... را می توانید مشخص کنید.



در تب Sharing می‌توانید Printer موردنظر خود را برای کاربران دیگر Share کنید، تیک گزینه Share this printer را انتخاب کنید و نام پرینتر خود را وارد کنید و دو گزینه دیگر درقسمت زیری آن را هم انتخاب کنید.

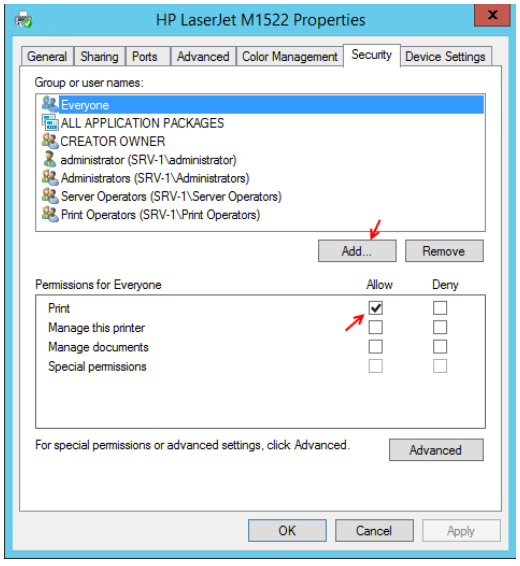


در تب Ports می‌توانید نوع پورت موردنظر Printer خود را تغییر دهید و یا پورت جدید تعریف کنید که زیاد هم به کار شما نخواهد آمد مگر در شرایط خاص.



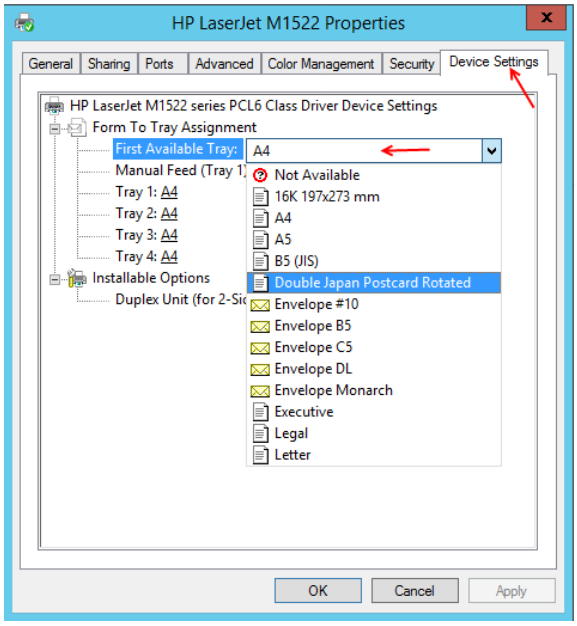
در تب Advanced می‌توانید بر کارکرد Printer خود مدیریت داشته باشید، مثلاً اگر گزینه Always Available را انتخاب کنید دستگاه Printer در تمام ساعت آماده به کار می‌باشد. ولی اگر گزینه Available from را انتخاب کنید می‌توانید ساعت کار موردنظر خود را وارد کنید تا کاربران فقط در ساعت خاص بتوانند از این دستگاه استفاده کنند.

تب Color Management مربوط به تنظیمات رنگبندی دستگاه موردنظر می‌باشد که بسته به هر دستگاه متفاوت است.



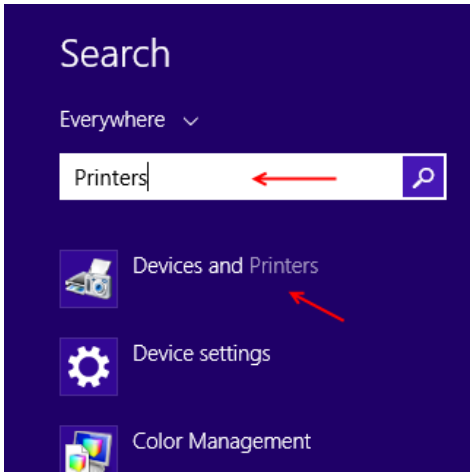
در تب Security که مهمترین قسمت می‌باشد شما می‌توانید مشخص کنید که چه کاربر و گروهی می‌تواند به Printer دسترسی داشته باشد و می‌تواند چه کاری انجام دهد، مثلاً در شکل روبرو گروه Everyone فقط مجوز Print را دریافت کرده است و کار دیگه ای را نمی‌تواند انجام دهد، به این موضوع توجه کنید که تمام کاربرانی که ایجاد می‌کنید به صورت پیش فرض عضو گروه Everyone هستند و توانایی Print را خواهد داشت، اگر این موضوع برای شما جالب

نیست و فقط می‌خواهید که کاربری را که در لیست بالا وارد می‌کنید توانایی Print داشته باشد باید گروه Everyone را از لیست حذف کنید. در لیست بالا گروهی با نام Print Operations وجود دارد که مدیریت کاملی بر روی Printer دارد و مجوز دسترسی آن Full می‌باشد و اگر یک کاربر را عضو این گروه کنید توانایی بالایی در مدیریت Printer خواهد داشت.



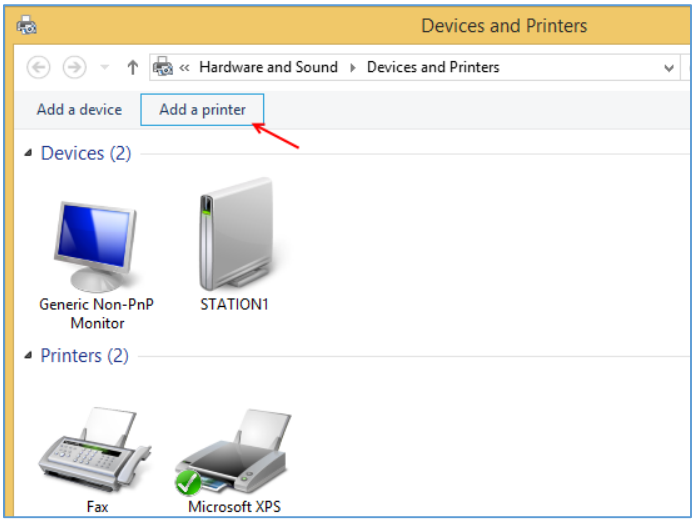
در تب آخر یعنی Device Settings می‌توانید اندازی کاغذ Printer را برای چاپ به مانند شکل روبرو انتخاب کنید.

تا به اینجا Printer را نصب کردیم و با تنظیمات آن آشنا شدیم و Printer را در شبکه به اشتراک گذاشتیم، حالا می‌خواهیم از طریق کلاینت ویندوز 8 به Printer به اشتراک گذاشته شده دسترسی پیدا کنیم.

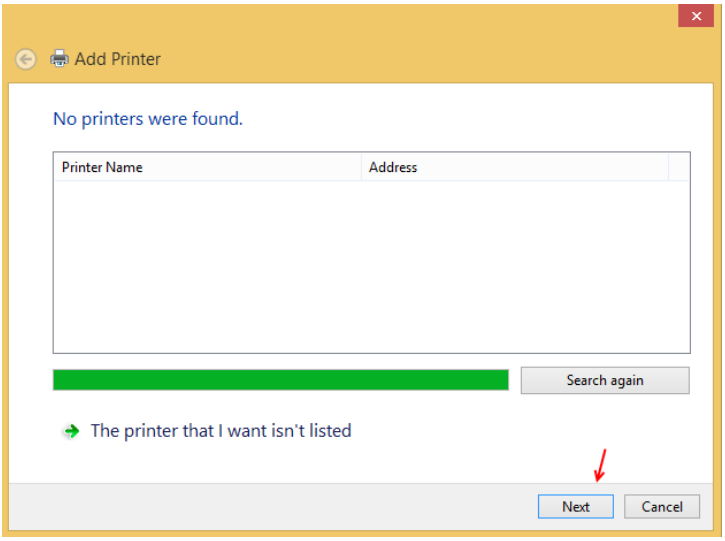


وارد Search شوید و کلمه Printers را وارد کنید و در نتایج جستجو بر روی Device and Printers کلیک کنید.

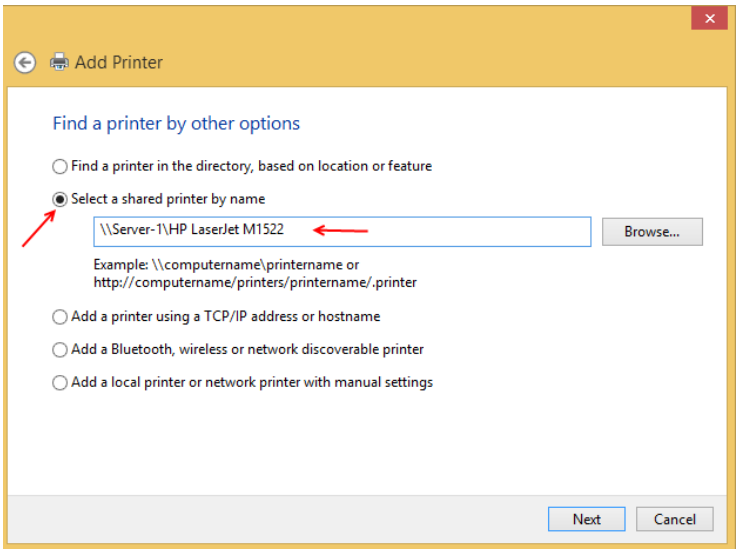
سعی کنید همیشه از سرویس فدرتمند جستجوی ویندوز 8 یا ویندوز سرور 2012 استفاده کنید تا در کار خود پیشرفت کنید.



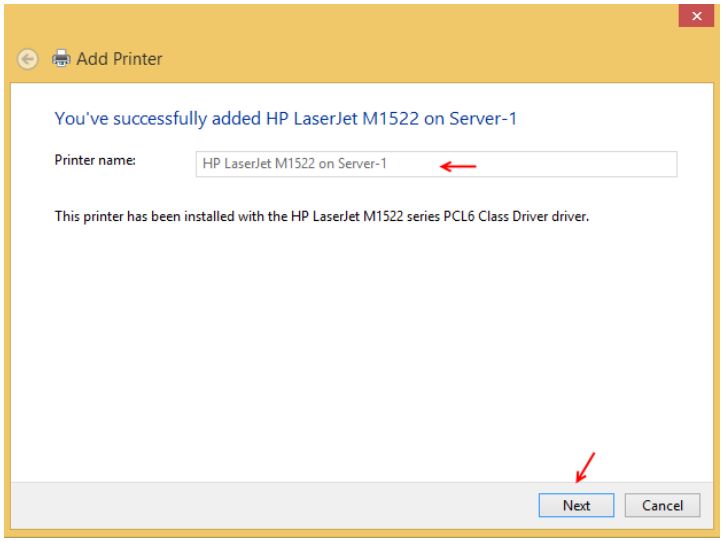
در این صفحه برای اضافه کردن Printer موردنظر بر رو Add a Printer کلیک کنید.



در این قسمت بر روی Next کلیک کنید.



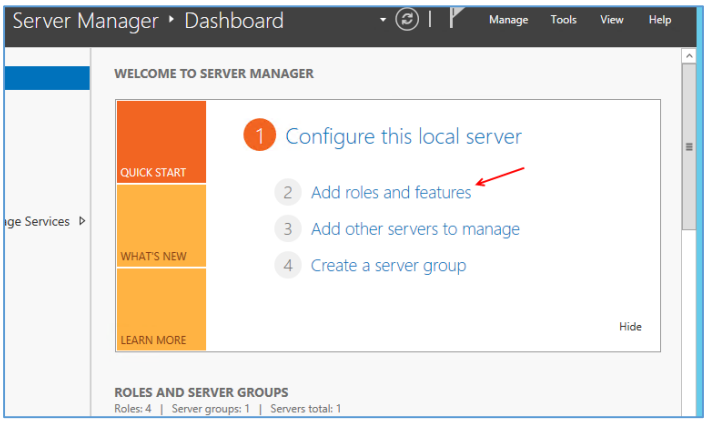
در این صفحه گزینه Select a shared Printer by name را انتخاب کنید و آدرس Printer موردنظر را به صورت مشخص‌شده وارد کنید، شما باید به جای Server-1 نام و یا IP سروری را وارد کنید که Printer روی آن نصب است و اگر بعد از وارد کردن اسم از بک اسلش استفاده کنید نام Printer به صورت خودکار نمایان می‌شود. برروی Next کلیک کنید.



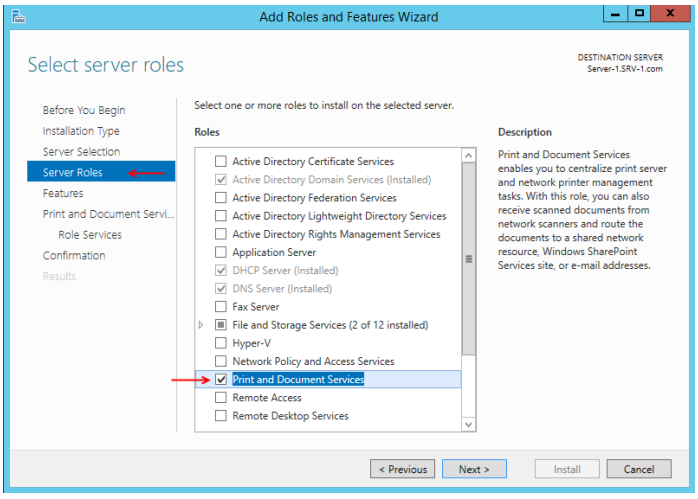
همانطور که مشاهده می‌کنید، Printer موردنظر با موفقیت نصب شده است، بر روی Next کلیک کنید.

در صفحه بعد بر روی Finish کلیک کنید تا Printer موردنظر به لیست اضافه شود.

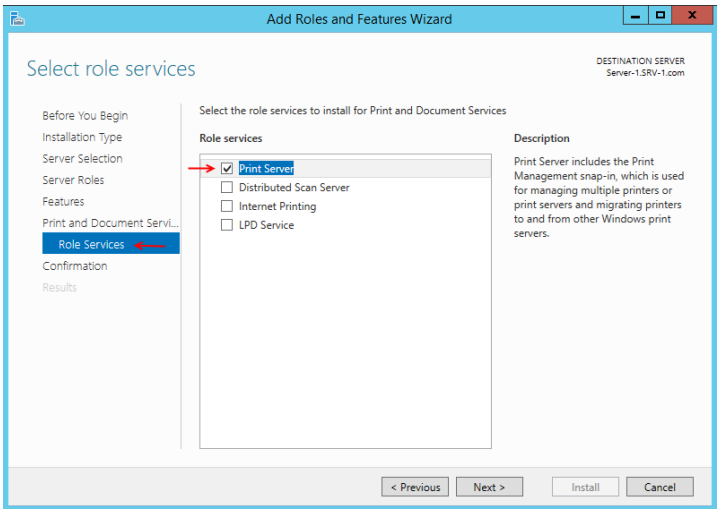
بعد از اجرا و پیاده سازی عملیات نصب Printer و Share کردن آن، حالا می‌خواهیم سرویس Print and Document را بر روی سرور نصب کنیم.



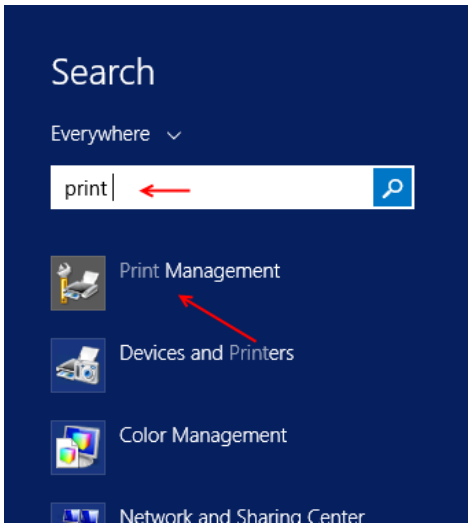
وارد ویندوز سرور شوید و Server Manager را اجرا کنید و در صفحه باز شده به مانند شکل روبرو بر رویAdd rolesand features کلیک کنید.



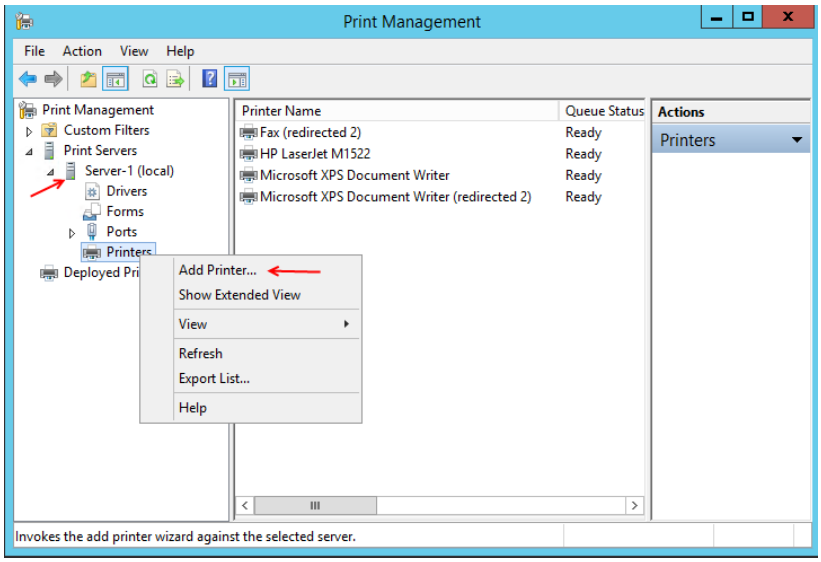
برای رسیدن به این صفحه باید بر روی Next کلیک کنید تا به قسمت Server Roles برسید و از لیست Role ها گزینه Print and document Services را انتخاب کند و در پنجره‌ای که باز می‌شود بر روی Add Feature کلیک کنید.



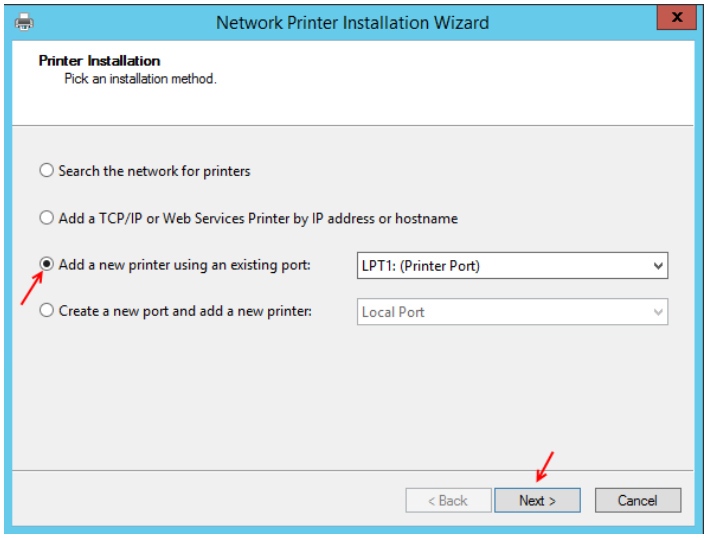
تمام قسمت‌ها را رد کنید تا به قسمت Role Service برسید که در این قسمت به مانند شکل روبرو Print Server را انتخاب کنید و بر روی Next کلیک کنید، در صفحه آخر بر روی Install کلیک کنید تا سرویس موردنظر نصب شود.



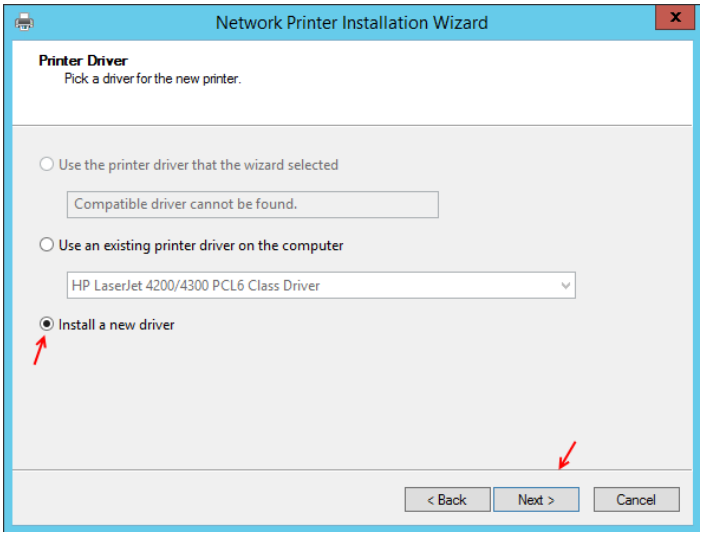
بعد ار نصب سرویس موردنظر وارد Search شوید و کلمه Print را وارد کنیدو در نتایج جستجو گزینه Print Management را انتخاب کنید.



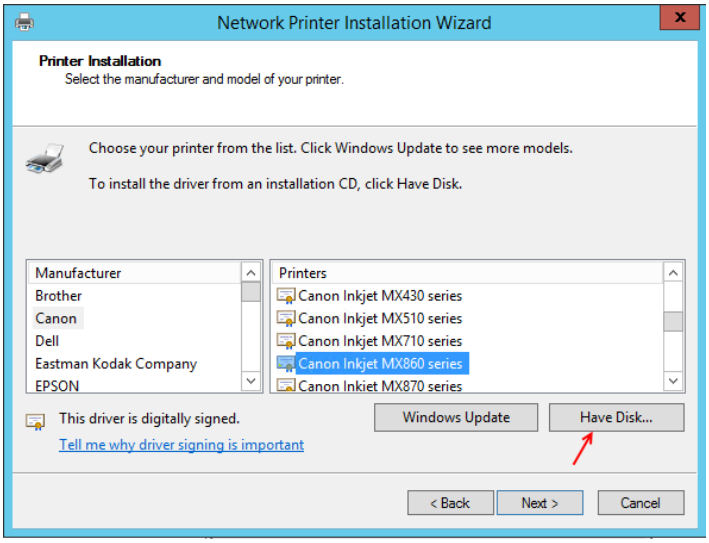
همانطور که مشاهده می‌کنید سرویس موردنظر به درستی اجرا شده است و اگر از سمت چپ نام سرور خود را که در اینجا Server-1 می-باشد انتخاب کنید و در لیست باز شده بر روی Printers کلیک کنید، باید کار به مانند شکل روبرو لیست Printer های نصب شده روی سرور را مشاهده کنید. برای اضافه کردن یک Printer به لیست باید روی Priners کلیک



راست کنید و گزینه Add Printer را انتخاب کنید تا شکل روبرو ظاهر شود، در این شکل به مانند قبل می-توانید از روش های مختلف پرینتر موردنظر خود را به لیست اضافه کنید، در این قسمت گزینه سوم را انتخاب و بر روی Next کلیک کنید.

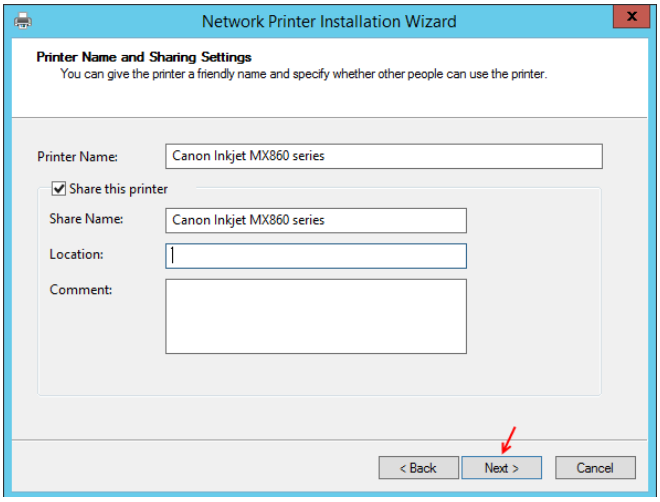


در این قسمت گزینه سوم یعنی Install a new driver را انتخاب و بر روی Next کلیک کنید.



در این قسمت می‌توانید نام کارخانه سازنده به همراه مدل Printer را در صورت موجود بودن انتخاب کنید و یا اگر CD یا DVD مربوط به پرینتر موردنظر را در اختیار دارید، بر روی Have Disk کلیک کنید و درایور موردنظر را به برنامه معرفی کنید.

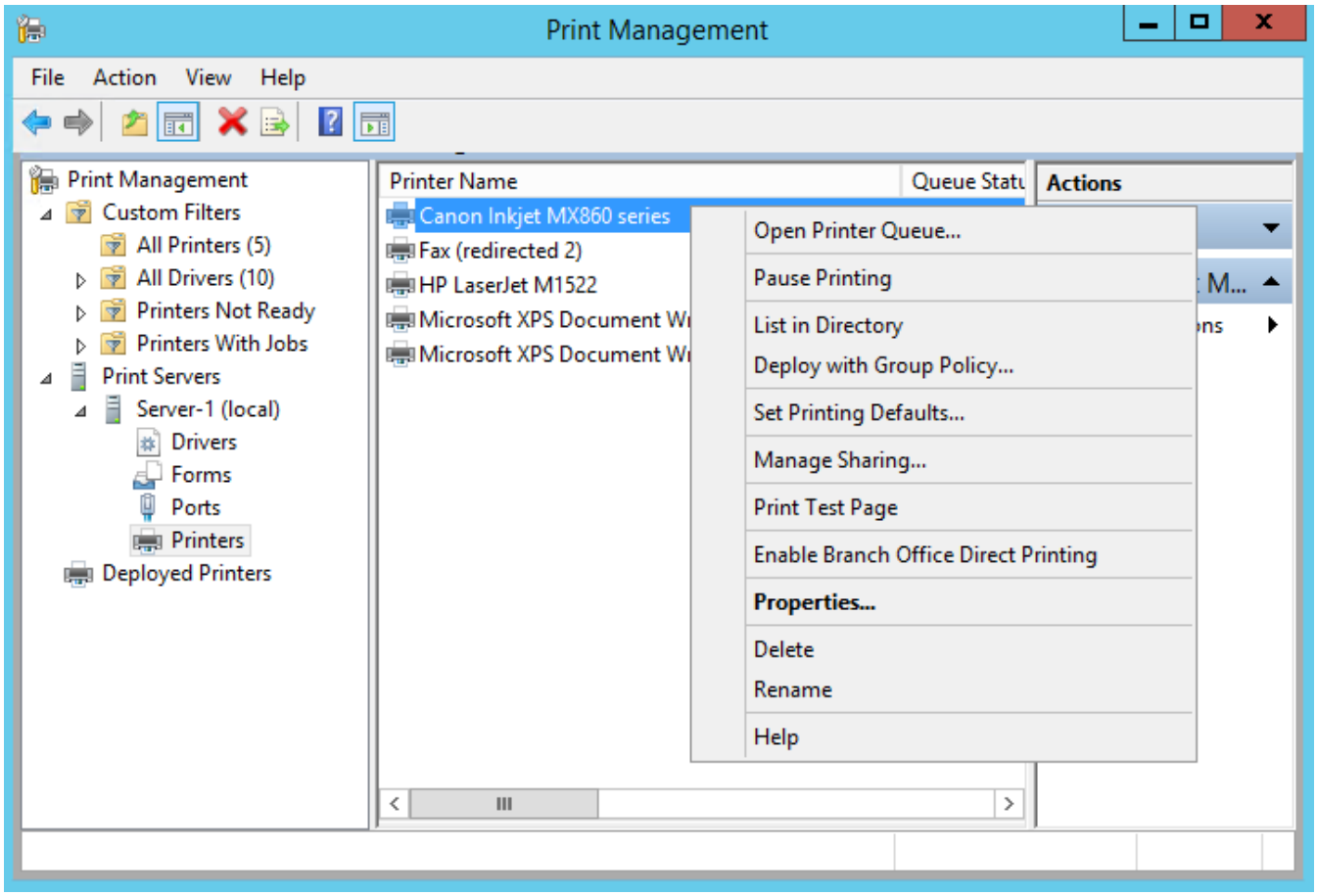
بر روی Next کلیک کنید.



در این صفحه می‌توانیم نام Printer خود را مشاهده و یا ویرایش کنید، اگر می‌خواهید Printer موردنظر را در شبکه Share کنید تیک گزینه Share this printer را انتخاب کنید و در قسمت Share Name نام Printer خود را زمانی که share می‌شود را وارد کنید در قسم Location هم محل قرار گیری Printer را وارد کنید و بر روی Next کلیک کنید.

در صفحه بعد هم بر روی Next کلیک کنید و در صفحه آخر هم بر روی Finish کلیک کنید.

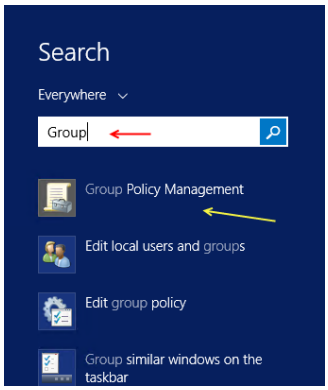
بعد از ایجاد Printer به مانند شکل زیر بر روی آن کلیک راست کنید، در منوی باز شده یک سری امکانات در اختیار شما قرار می‌دهد.



کار با Group Policy در ویندوز سرور 2012:

Group Policy امکانی است در ویندوز سرور که به کمک آن می‌توانید تنظیمات خاصی را در آن انجام دهید، همانطور که می‌دانید زمانی که می‌خواهیم برای یک کاربر رمز عبور تعریف کنیم، حتماً باید یک رمز پیچیده و تعداد مشخص استفاده کنیم که کنترل پیچیدگی رمز عبور و حداکثر و حداقل آن و.... توسط سرویس Group Policy انجام می‌پذیرد که این کار یکی از صدها کار این سرویس می‌باشد که در این قسمت با هم آن را بررسی بررسی می‌کنیم.

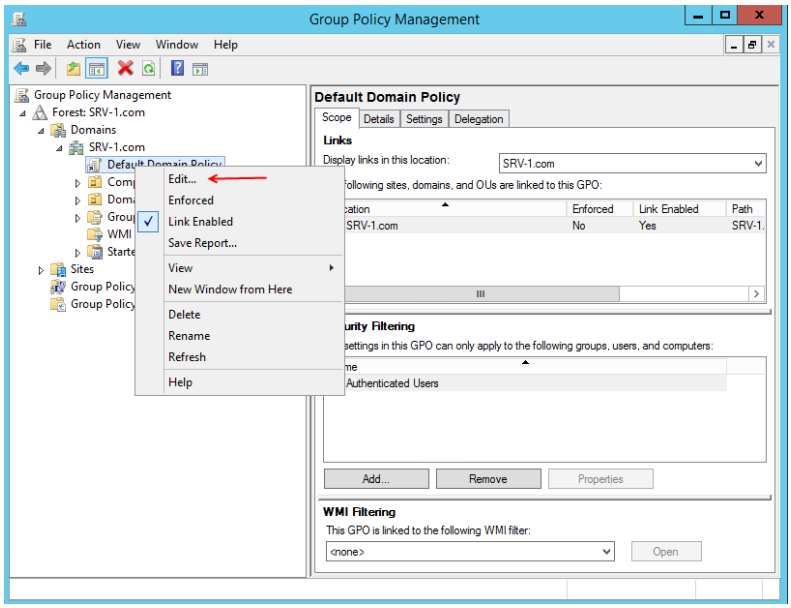
نکته مهم: قبل از اینکه Domain Controller را روی سرور نصب کنید، Group Policy به صورت Local Group Policy در دسترس است و می‌توانید تنظیمات آن را تغییر دهید ولی اگر Domain Controller روی سرور شما نصب باشد دیگر Local Group policy کاربرد ندارد و گزینه های آن غیر فعال می‌شوند و در عوض Group Plicy مربوط به Domain فعال می‌شود که در زیر بررسی خواهیم کرد.



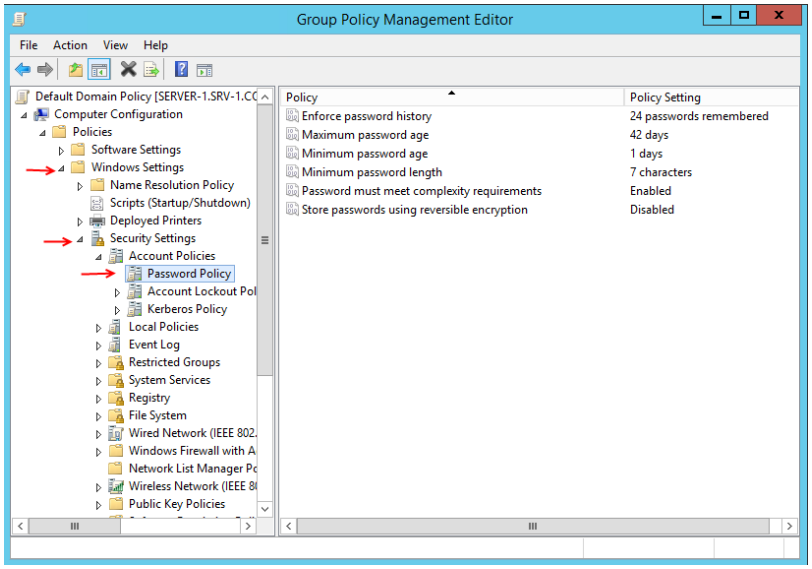
برای اجرای سرویس Group Policy می‌توانید به آدرس زیر مراجعه کنید:

Control Panel\System and Security\Administrative Tools\Group Policy Management.lnk

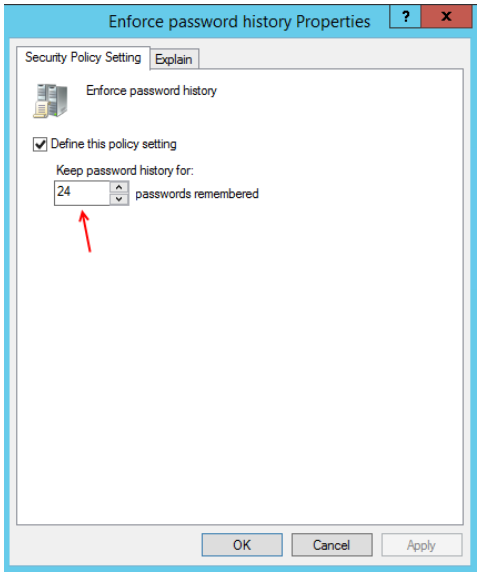
یا می‌توانید وارد Search شوید و کلمه Group را وارد کنید و در نتیجه جستجو سرویس Group Policy Management را انتخاب کنید.



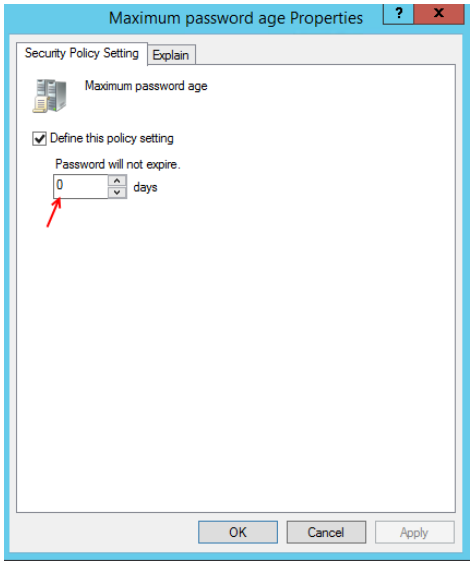
همانطور که مشاهده می‌کنید وارد سرویس Group Policy شدیم، کم کم با تمام اجزای این سرویس آشنا خواهید شد، برای شروع باید وارد قسمت ویرایش اطلاعات Group Policy شویم، برای این کار به مانند شکل بر روی Default Domain Policy کلیک راست کنید و گزینه Edit را انتخاب کنید.



برای شروع کار قسمت Password Policy را با هم بررسی می‌کنیم، در این قسمت می‌توانیم حداقل طول یک Password را کم یا زیاد کنیم و یا پیچیدگی آن را تغییر دهیم، برای این کار به مانند شکل روبرو وارد قسمت Password Policy می‌شویم که در این قسمت 6 گزینه را مشاهده می‌کنید که در زیر آنها را بررسی می‌کنیم.

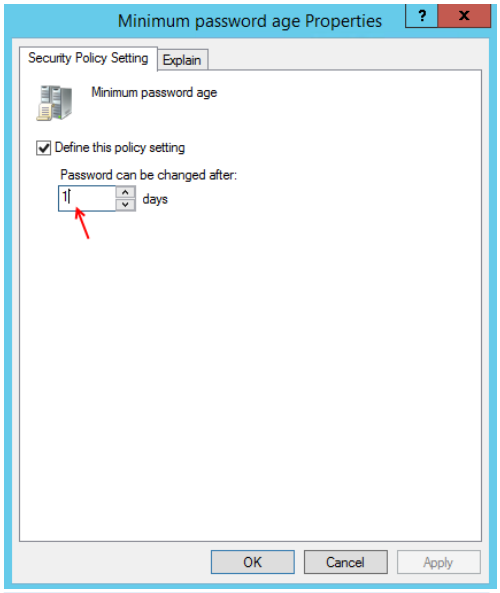


در قسمت Enforce Password history می‌توانید مشخص کنید که چه تعداد از رمز عبورهایی که توسط مدیر و کاربران شبکه وارد شده است در Domain ذخیره شود تا کسی دیگر نتواند رمزی شبیه به رمز دیگران ایجاد کند که در این شکل عدد 24 قرار دارد که تا 24 رمز عبور را در خود ذخیره می‌کند و شما می‌توانید این عدد را به راحتی تغییر دهید، بعد از تغییر بر روی ok کلیک کنید.



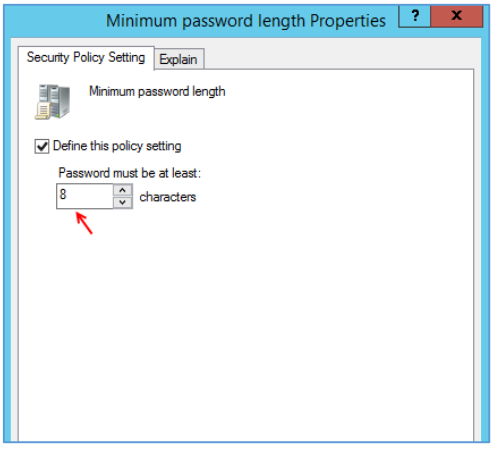
در قسمت Maximim Password age می‌توانید مشخص کنید که یک رمز عبور تا چند روز اعتبار داشته باشد، در شکل روبرو عدد 42 را به صفر تغییر دادیم و اگر به دقت به شکل توجه کنید بالای عدد صفر نوشته Password will not expire که به این معنا است که رمز به هیچ عنوان انقضاء نخواهد شد، اگر به یاد داشته باشید در زمان ایجاد کاربر گزینه‌ای با نام Password Never Expire وجود داشت که با انتخاب آن کاربر نمی‌توانست رمز عبور را تغییر دهد، در این قسمت هم

با وارد کردن عدد صفر دیگر لازم نیست تیک گزینه Password Never Expire را در موقع ایجاد کاربر انتخاب کنیم.

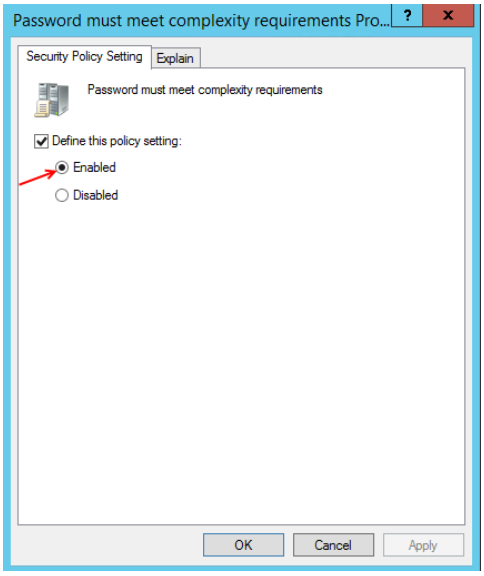


در قسمت Minimum Password age می‌توانید مشخص کنید که زمانی که یک کاربر رمز عبور خود را تغییر داد تا چه زمانی فرصت دارد که رمز عبور خود را دوباره تغییر دهد که این عدد به صورت پیش فرض بر روی 1 روز قرار دارد که می‌تواند عددی بین 1 تا 998 باشد.

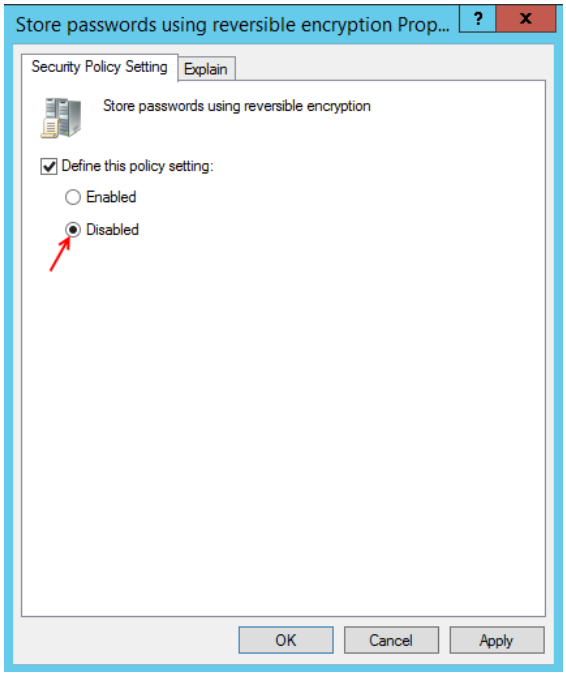
نکته اساسی: زمانی که عدد قسمت Maximim Password age را به صفر تغییر دهید دیگر Minimum Password age هیچ گونه تاثیری ندارد، فقط توجه داشته باشید Minimum Password age باید کوچکتر از Maximim Password age باشد، جزءاینکه Maximim Password age به صفر تغییر کرده باشد.



قسمت بعدی مربوط به Minimum Password length می‌باشد که طول رمز عبور را مشخص می‌کند که به صورت پیش فرض برای دومین 7 می‌باشد که می‌توانید این مقدار را تغییر دهید که در این قسمت این عدد به 8 کاراکتر تغییر کرده است، سعی کنید مقدار رمز عبور را از 8 به بالا وارد کنید تا امنیت اطلاعات کامل‌تر شود.

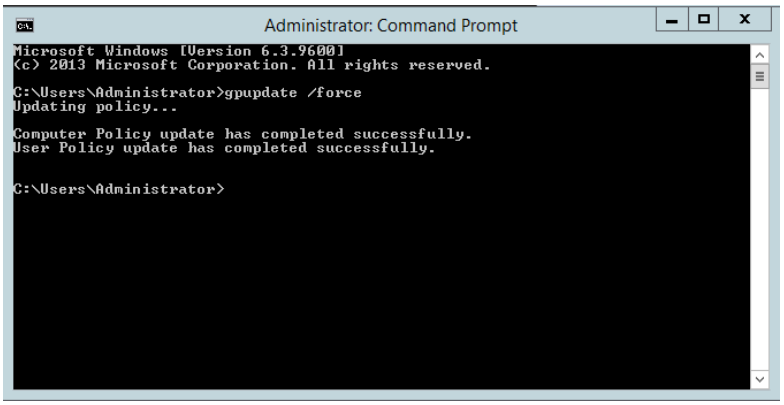


در قست Password must meet Complexity requirements می‌توانید مشخص کنید که آیا رمز عبور باید به صورت پیچیده وارد شود به طور مثال Test@123456 ترکیبی از حروف، اعداد و علائم باشد و یا با انتخاب گزینه Disabled نیازی به وارد کردن رمز به صورت پیچیده نیست.



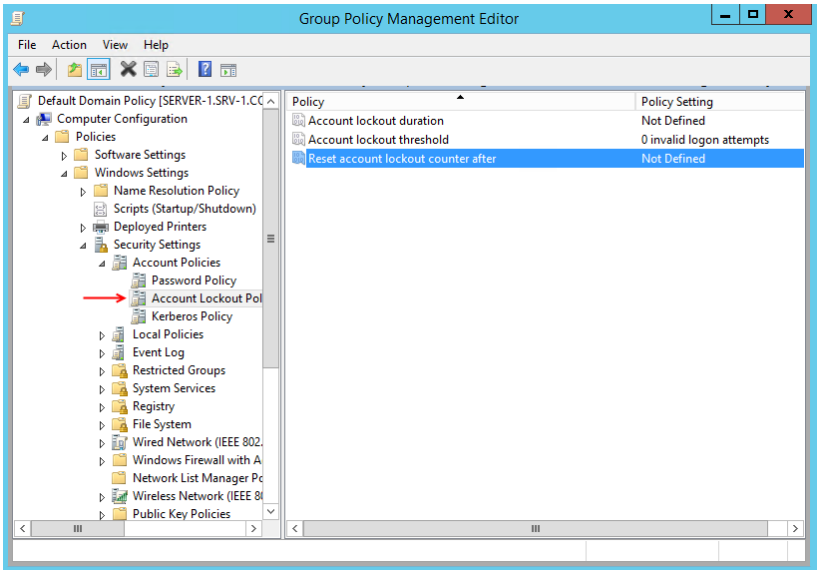
در قسمت Store Passwords Using Reversible encryption با انتخاب Enabled رمز عبور به صورت Clear Text در شبکه فعال می‌شود و امنیت اطلاعات بسیار کاهش می‌یابد که سعی کنید در صورت نیاز آن را فعال کنید.

این سیاست رمز نگاری از نرم افزارهایی حمایت می‌کنند که احتیاج به پروتکل رمز نگاری برای تأیید هویت کاربران دارند. این گزینه به صورت پیش فرض غیر فعال شده است.

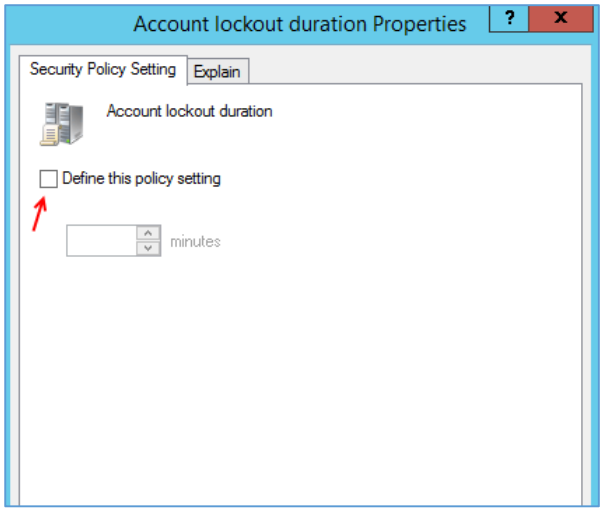


نکته مهم: بعد از اینکه تنظیمات Group Plicy را تغییر دادید، برای اینکه این تنظیمات روی سرور شما به صورت سریع اعمال شود باید از دستور Gpupdate /Force در CMD استفاده کنید.

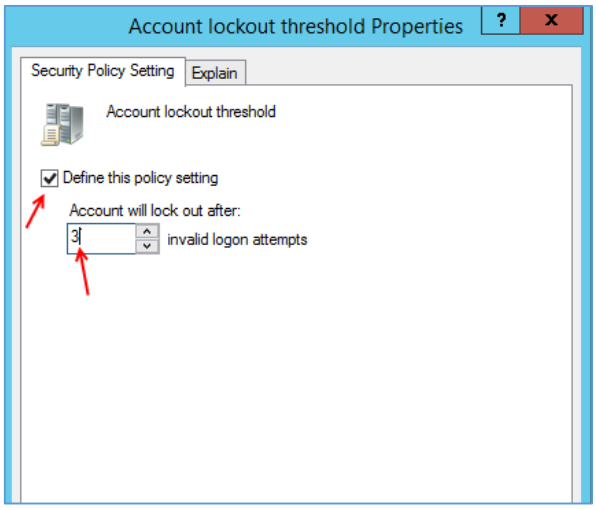
با این دستور تنظیمات بر روی سرور اعمال شده است.



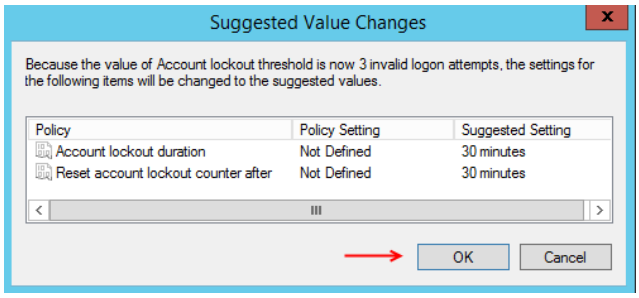
قسمت بعدی که با هم بررسی می‌کنیم، Account Lookout Policy می‌باشد، به مانند شکل از سمت چپ بر روی Account Lookout Policy کلیک کنید تا صفحه مربوط به آن باز شود، در این صفحه سه گزینه وجود دارد که با هم مورد بررسی قرار می-دهیم.



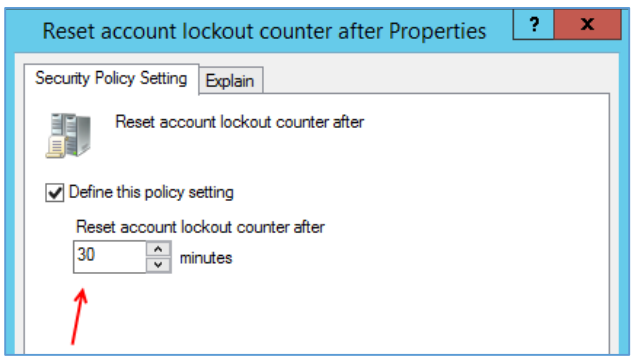
در قسمت Account Lockout duration می‌توانید مشخص کنید که، یک حساب زمانی که قفل شد تا چه مدت قفل بماند و بعد فعال شود، مثلاً در این قسمت گزینه Define this policy setting را انتخاب کنید و یک عدد بر حسب دقیقه مثلاً 30 وارد کنید این عدد به این معنا است که کاربر زمانی که به دلایل گوناگون مثلاً اشتباه وارد کردن رمز عبور به دفعات متعدد و یا غیرفعال کردن حساب توسط مدیر شبکه بعد از این 30 دقیقه حساب موردنظر دوباره فعال می‌شود.



در قسمت Account will Lock out after شما می‌توانید مشخص کنید که کاربر بعد از اینکه به تعداد مشخص‌شده مثلاً 3 بار رمز ورود را به اشتباه وارد کرد حساب آن قفل شود، البته بعد از زمان مشخص‌شده در قسمت Account Lockout duration این حساب فعال می‌شود.

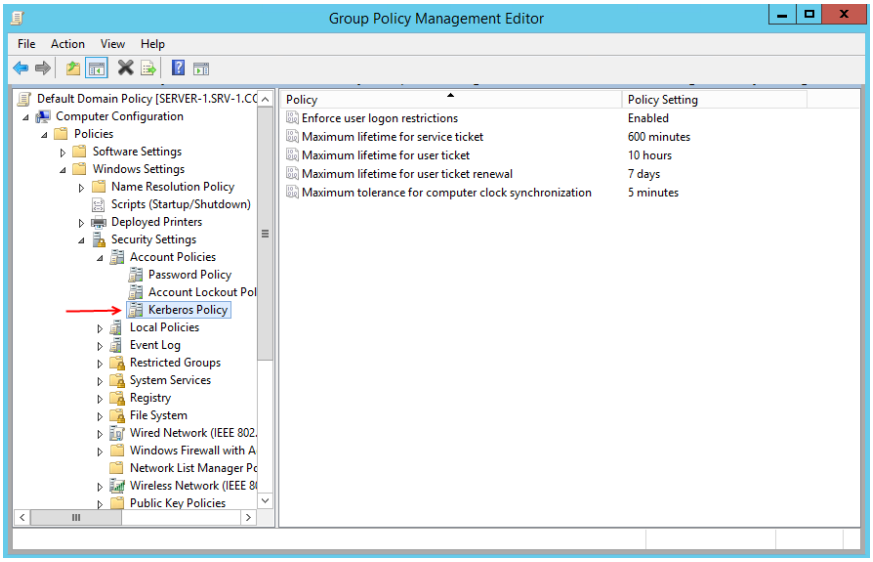


زمانی که در قسمت قبل بر روی ok کلیک کنید شکل روبرو ظاهر می‌شود، در این قسمت این پیغام به شما داده می‌شود که اگر می‌خواهید این قسمت فعال شود باید هر دو قسمت Account Lockout duration و Reset Account تنظیم شوند که به صورت پیش فرض 30 دقیقه می‌باشد.

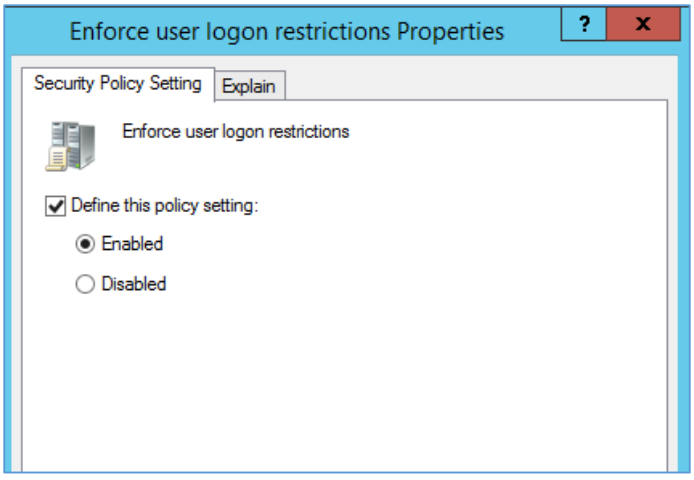


در قسمت Reset Account lockout counter after باید عددی را مساوی یا کمتر از عدد قسمت Account Lockout duration تعریف کنید که زمانی که کاربر ورود اشتباه داشت اطلاعات ذخیره شده در داخل دایرکتوری حذف شود، یعنی اینکه مثلاً تعداد ورود کاربر 3 بار شد این اطلاعت

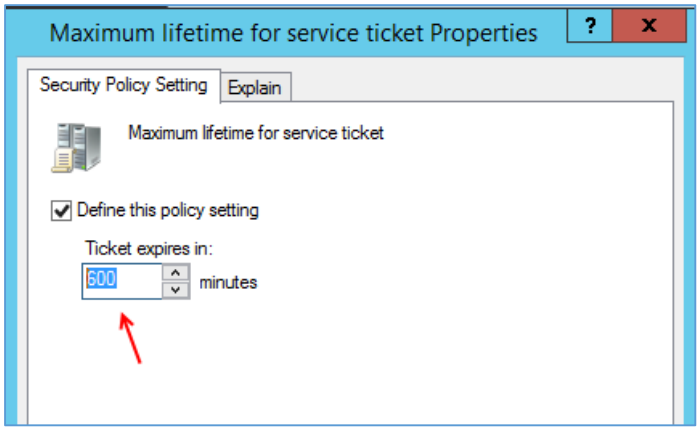
در اکتیو دایرکتوری به صورت یک شمارنده ثبت می‌شود که با اعمال زمان مناسب در این قسمت این شمارنده صفر خواهد شد.



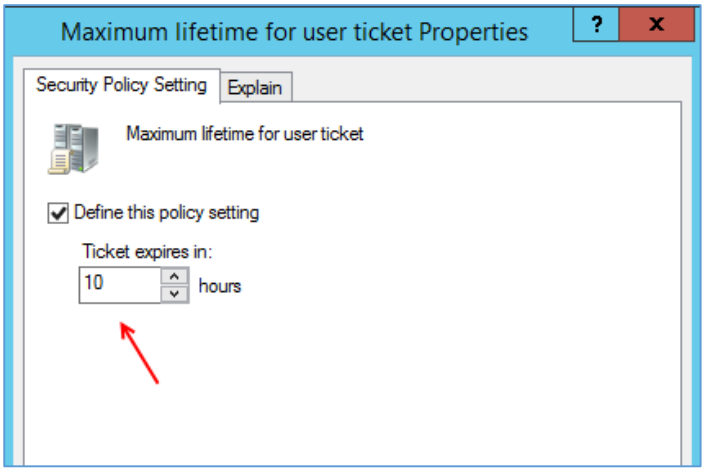
قسمت بعدی که مورد بررسی قرار می-دهیم Kerberos Policy می‌باشد که مربوط به امنیت کاربران می‌باشد که تک تک این پنج گزینه را با هم مورد بررسی قرار می‌دهیم.



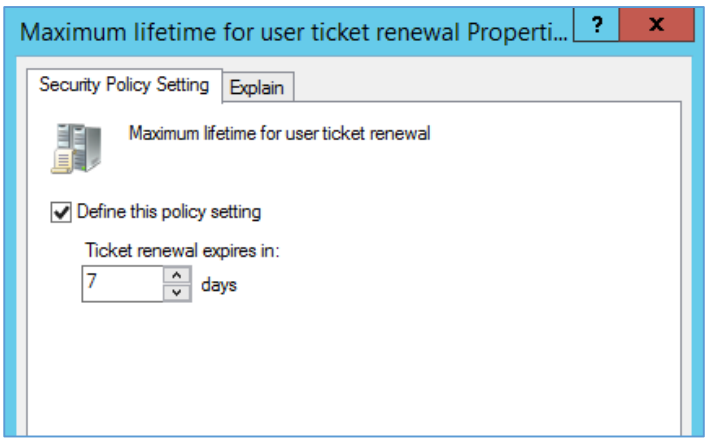
قسمت Enforce user logon restrictions مربوط به ورود کاربران می‌باشد که به صورت پیش فرض فعال است و زمانی که یک کاربر وارد سیستم می‌شود یک گواهینامه امنیتی برای آن صادر می‌شود.



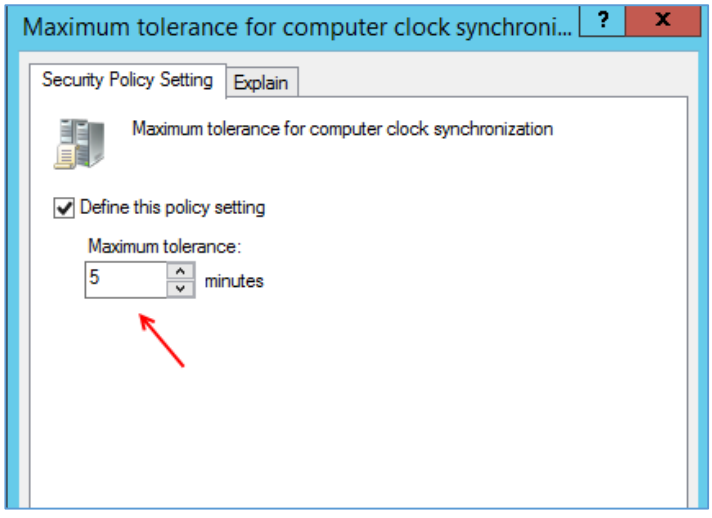
در قسمت Maximum lifetime for Service ticket می‌توانید مشخص کنید که مدت زمان گواهینامه اعتباری برای یک سرویس فعال چقدر باشد. که بعد از اتمام این زمان سرویس انقضاء شده و در سرور نمی‌تواند به دیگران سرویس دهد.



در قسمت Maximum lifetime for user ticket می‌توانید مقدار زمانی را که یک کاربر می‌تواند از گواهینامه تخصیص داده شده به وی در زمان ورود استفاده کند. که این عدد باید بین 0 تا 9999 قرار گیرد که اگر صفر باشد گزینه بعدی آن هم غیر فعال می‌شود.

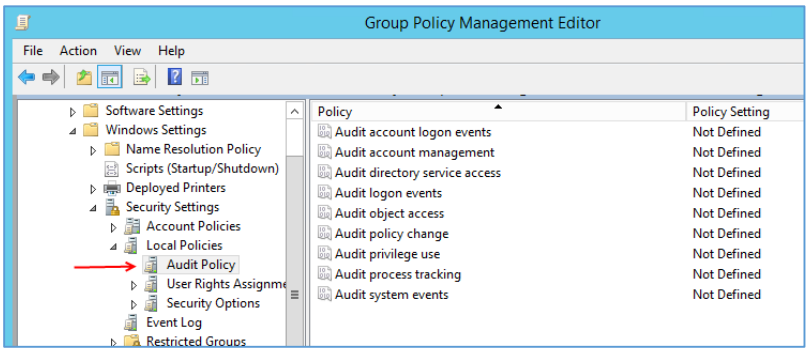


در قسمت Maximum lifetime for user ticket renewal تعداد روز فعال بودن گواهینامه یا بلیط داده شده به کاربر را مشخص می‌کند که بعد از آن گواهینامه یا بلیط موردنظر انقضاء می‌شود.



در قسمت Maximum tolerance for computer clock synchronization به این منظور استفاده می‌شود که در زمان مشخص‌شده مثلاً هر 5 دقیقه کامپیوتر سرور با کامپیوتر کلاینت تارخ و زمان خود را با هم هماهنگ سازی کنند چون الگوریتم Kerbros شدیداً به برابر بدون زمان بین سرور و کلاینت نیاز دارد تا گواهینامه برای سرویس کاربر موردنظر تعریف و محاسبه کند.

بررسی قسمت Audit Policy:

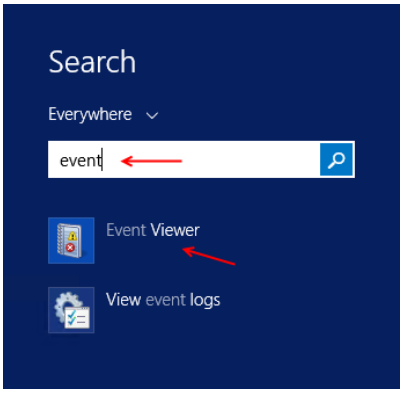


قسمت Audit Policy مربوط به ثبت رویداد های مربوط به ورود کاربران و ایجاد تغییرات و تغییر رمز عیور و ... می‌باشد که در صورت نیاز می‌توانید هر یک از قسمت های موجود را فعال کنید، در شکل روبرو وارد قسمت Audit Policy می‌شویم که در این قسمت 9 گزینه مختلف وجود دارد که هر کدام برای منظور خاصی طراحی شده اند که در جدول زیر همه آنها را بررسی می‌کنیم.

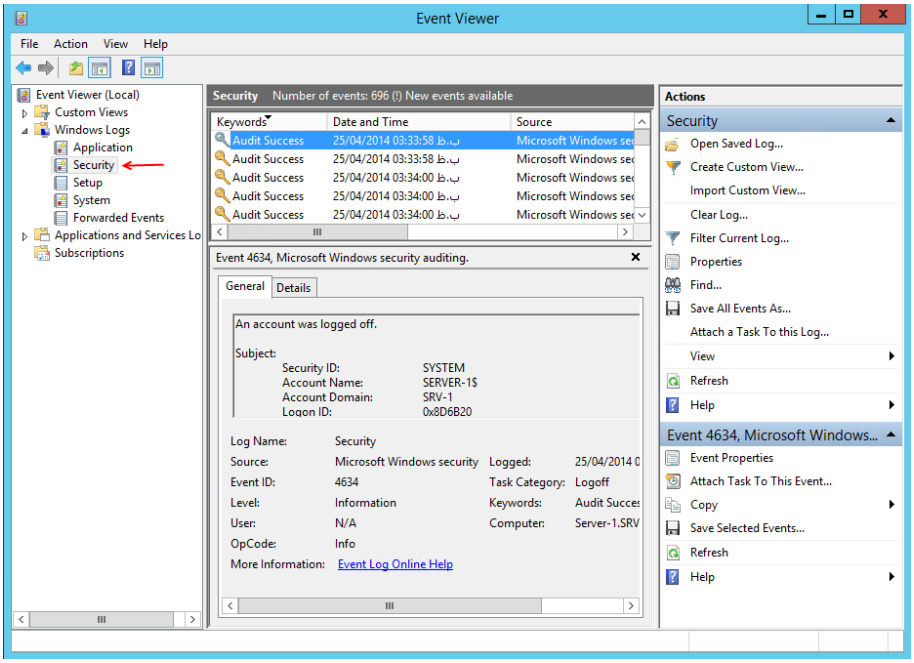
Audit account logon events	این گزینه زمانی که فعال شود ورود کاربران را به سیستم ثبت می‌کند.
Audit account management	برای ثبت رویدادهایی مانند ایجاد کاربر، حذف، تغییر نام و... به کار می‌رود.
Audit directory service access	ثبت رویدادهای مربوط به دسترسی کاربران به فایل ها می‌باشد.
Audit logon events	این قسمت هم برای ثبت رویدادهای ورود و خروج و ورودهای با اشتباه کاربران به کار می‌رود.
Audit object access	این گزینه اگر فعال شود باعث ثبت رویدادهای مربوط به دسترسی کاربران به شی موجود در اکتیو دایرکتوری می‌شود.
Audit policy change	رویدادهای مربوط به تغییر سیاست های بر روی سیستم ثبت می‌شود.
Audit privilege use	رویدادهای مربوط تغییرات در ریجیستری و ... ثبت می‌شود.
Audit process tracking	این قسمت هم بر روی حسابرسی سیستم عامل بر روی فرایند ها کاربرد دارد.

Audit system events	ثبت رویدادهایی مانند تغییر ساعت سیستم، تاریخ، برنامه های Startup و ...

زمانی که این تغییرات را اعمال کردید، در کدام قسمت این رویدادها ثبت می‌شوند؟



همه رویدادهای سیستم یا همان Event یا Log در سرویس Event Viewer ثبت می‌شود، برای اجرای این سرویس وارد Search شوید و کلمه event را وارد کنید و سرویس Event Viewer را اجرا کنید.



همان‌طور که در شکل روبرو مشاهده می‌کنید، وارد سرویس Event Viewer شدیم، در این سرویس تمام ردپای ویندوز ثبت می‌شود، یعنی شما هیچ کاری را نمی‌توانید انجام دهید که در اینجا ثبت نشود.

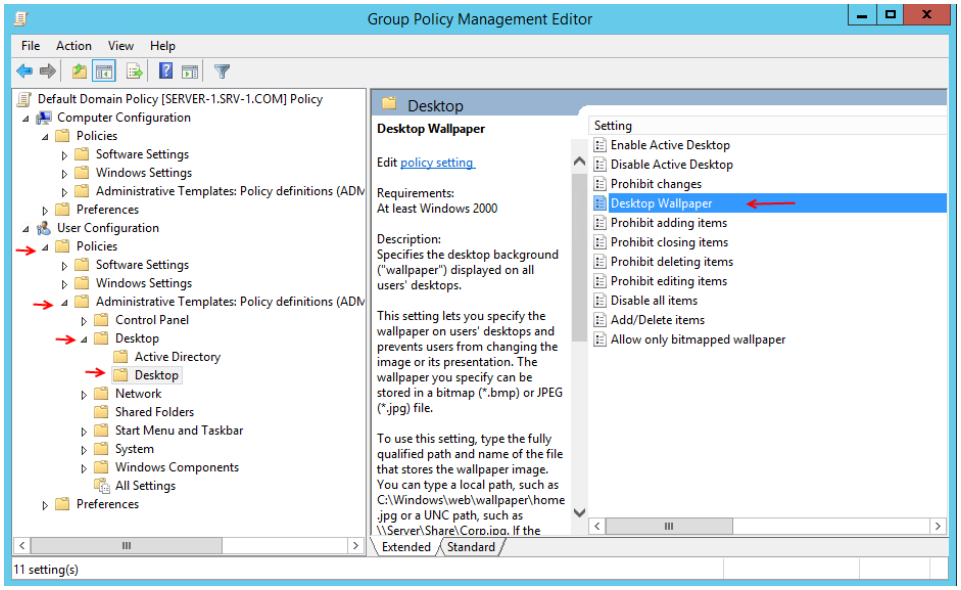
برای مشاهده رویدادهای بخش امنیتی که در قسمت قبل در Group Policy تنظیم کردیم باید از سمت چپ وارد قسمت Windows Logs شوید و گزینه Security را انتخاب کنید تا تمام رویدادهای مربوط به قسمت امنیتی ظاهر شود. اگر به‌مانند شکل بر روی یکی از رویدادها کلیک کنید در قسمت General اطلاعات در مورد رویداد موردنظر ظاهر می‌شود که می‌توانید از آن‌ها استفاده کنید.

با این سرویس می‌توانید مشخص کنید که چه کاربری یا کامپیوتری در چه زمان و تاریخی وارد سیستم شده است، در کل این سرویس فقط از طریق مدیر شبکه اجرا می‌شود و از دسترس کاربران معمولی خارج است.

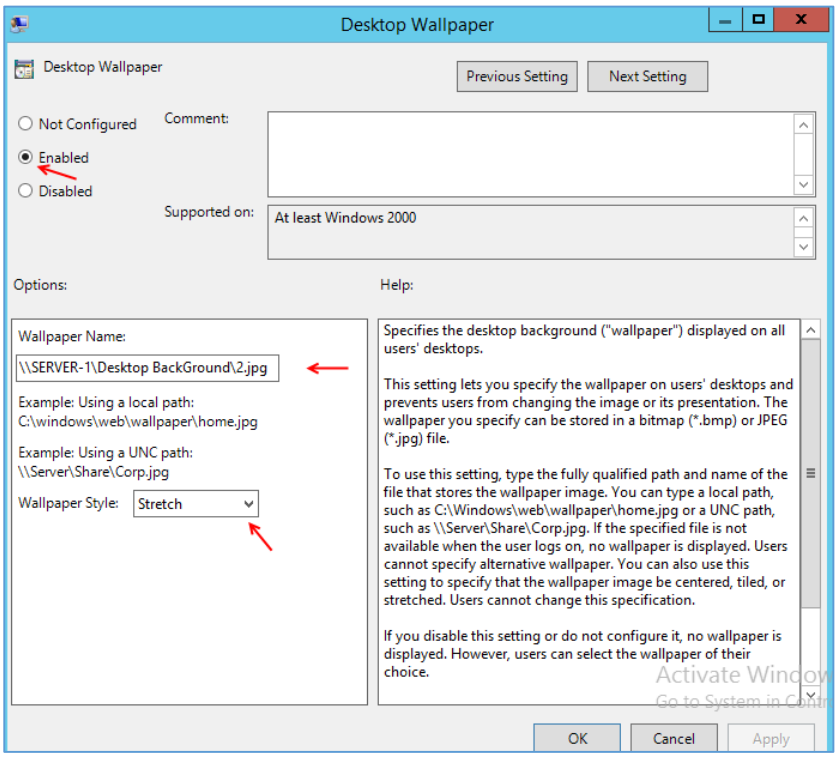
در ادامه کار به بررسی بعضی از کاربردهایی مهم و پرکاربرد سرویس Group Policy در شبکه می‌پردازیم.

تغییر تصویر BackGround تمام کلاینت‌های شبکه:

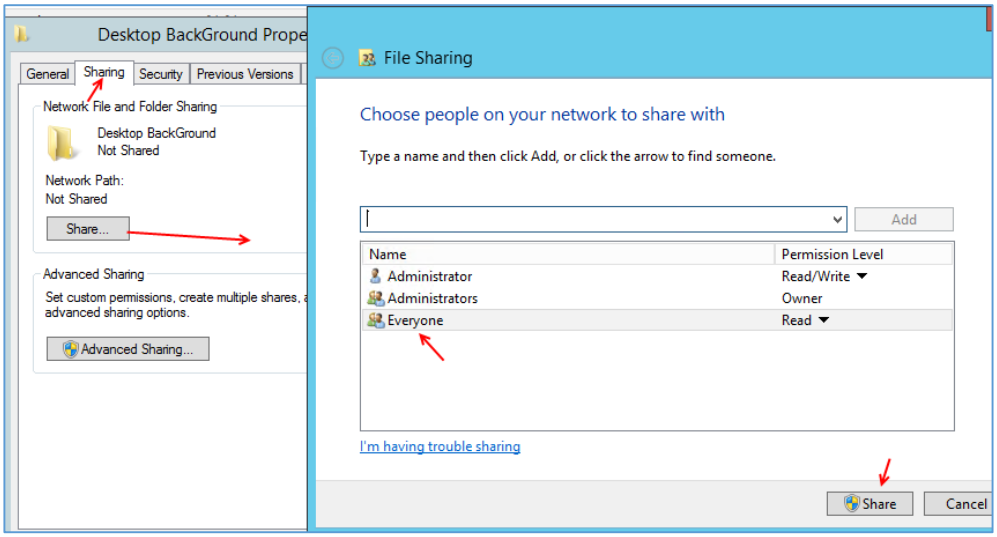
در این قسمت می‌خواهیم یک تصویر را به‌عنوان تصویر زمینه تمام کلاینت‌های متصل به شبکه دومین قرار دهیم،



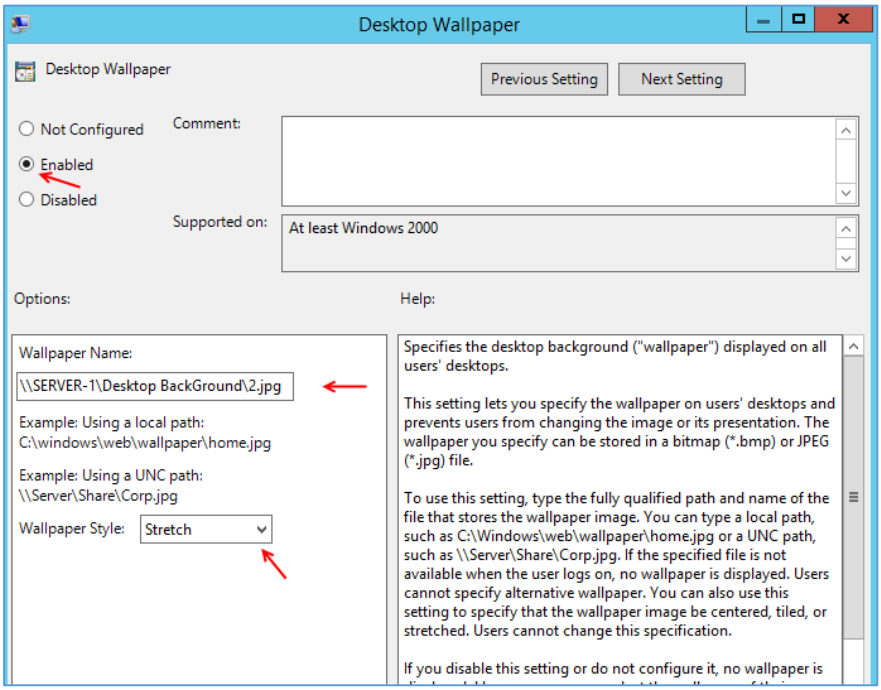
این کار توسط سرویس Group Policy به‌راحتی امکان‌پذیر است، برای شروع سرویس Group Policy را اجرا کنید و به مسیر مشخص‌شده در شکل روبرو بروید، در لیست بازشده مربوط به Desktop بر روی Desktop Wallpaper دو بار کلیک کنید.



در این قسمت، گزینه Enable را در بالای صفحه انتخاب کنید و در قسمت Wallpaper Name که مهم‌ترین بخش است، باید آدرس عکس موردنظر خود را وارد کنید، همان‌طور که مشاهده می‌کنید آدرس موردنظر به‌صورت شبکه‌ای واردشده است، شما باید یک پوشه در سرور خود ایجاد کنید و عکس موردنظر خود را داخل آن قرار دهید و بعدازآن باید پوشه موردنظر را برای تمام کاربران Share کنید.



در این قسمت، یک پوشه بانام Desktop BackGround ایجادشده است و برای گروه Everyone اشتراک گذاشته-شده است، تمام کاربران داخل شبکه عضو گروه Everyone می‌باشند که فقط مجوز Read را به آن دادیم.



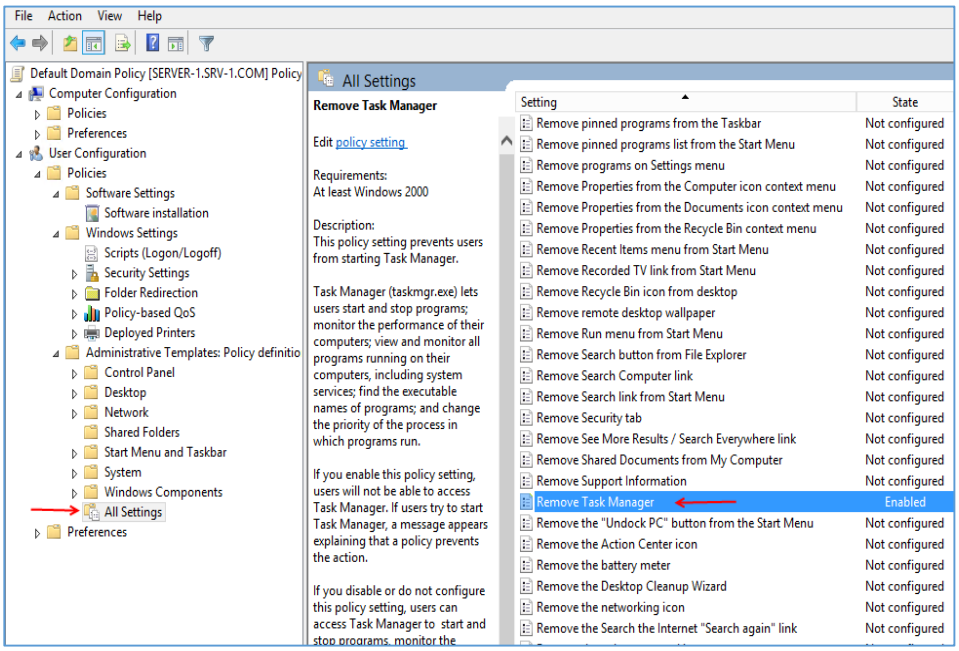
دوباره به قسمت قبل برمی‌گردیم، در بخش Wallpaper Name آدرس شبکه عکس داخل پوشه Desktop BakGround را وارد می‌کنیم:

\\SERVER-1\Desktop BackGround\2.jpg

در این آدرس باید به‌جای Server-1 نام یا IP سرور خود را وارد کنید.

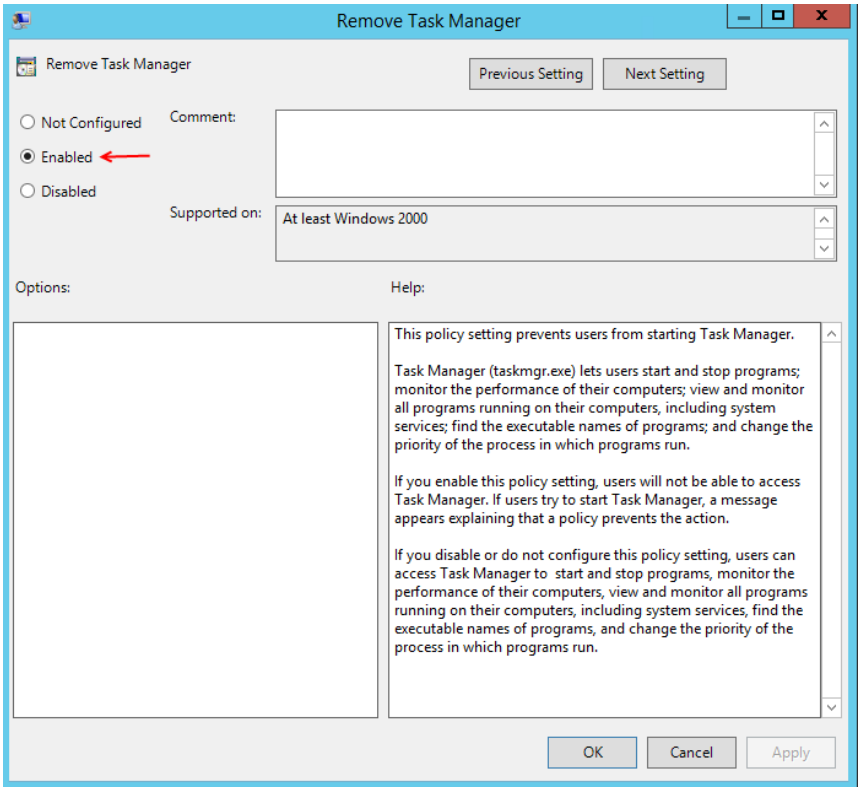
در قسمت Wallpaper Style باید سایز عکس موردنظر خود را بر روی Desktop کلاینت‌ها مشخص کنید که در اینجا Stretch را انتخاب می‌کنیم تا کل صفحه Desktop را برای کلاینت پر کند. در حال حاضر اگر بر روی ok کلیک کنید، تمام Background کلاینت‌ها به‌عکس موردنظر تغییر کرده است، مثلاً می‌توانید لوگوی شرکت خود را روی کلاینت‌ها قرار دهید.

غیرفعال کردن Task Manager برای تمام کلاینت‌ها:



برای اینکه Task Manager را برای تمام کلاینت‌های داخل شبکه غیرفعال کنید، وارد سرویس Group Policy شوید.

از سمت چپ بر روی All Settings کلیک کنید و در لیست بازشده بر روی گزینه Remove Task Manager دو بار کلیک کنید.



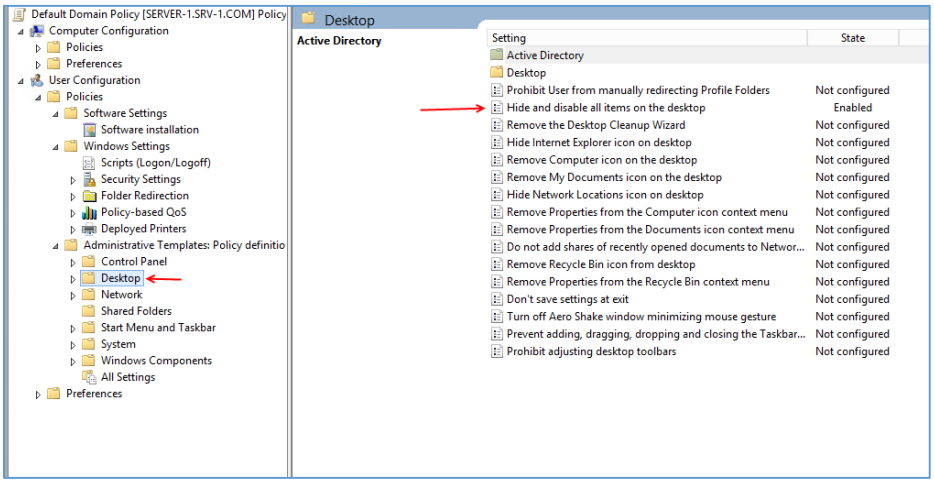
در این صفحه برای فعال کردن این موضوع بر روی Enabled کلیک کنید و بعد بر روی ok کلیک کنید.

با این کار هیچ کلاینتی نمی‌تواند Task Manager را اجرا کند.

همان‌طور که از قبل گفتم بعدازاین که تنظیمات مربوط به Group Plicy را انجام دادید حتماً دستور Gpupdate /Force را در CMD اجرا کنید تا تغییرات اعمال به شه.

حذف کردن راست کلیک بر روی Desktop در تمام کلاینت‌ها:

در این قسمت می‌خواهیم راست کلیک کردن بر روی Desktop مربوط به کلاینت‌ها را غیرفعال کنیم برای این کار

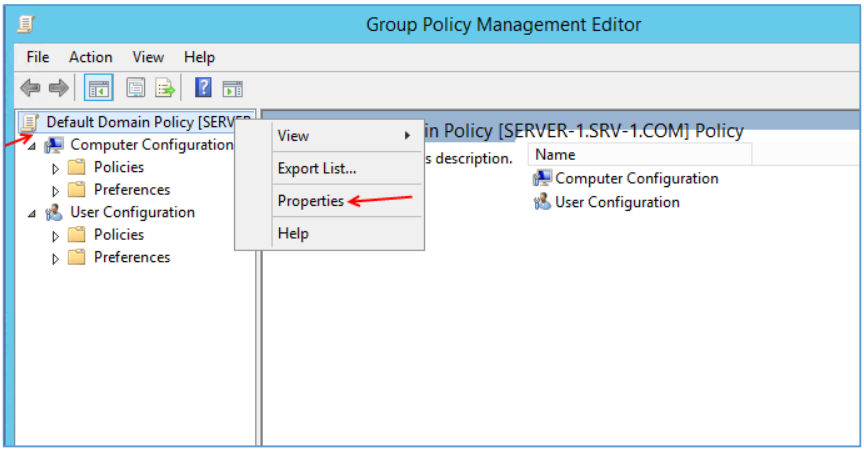


برای ورود به این قسمت از قسمت Administrative Templates گزینه Desktop را انتخاب کنید و در لیست بازشده بر روی گزینه Edit and disable all items on the desktop دو بار کلیک کنید.

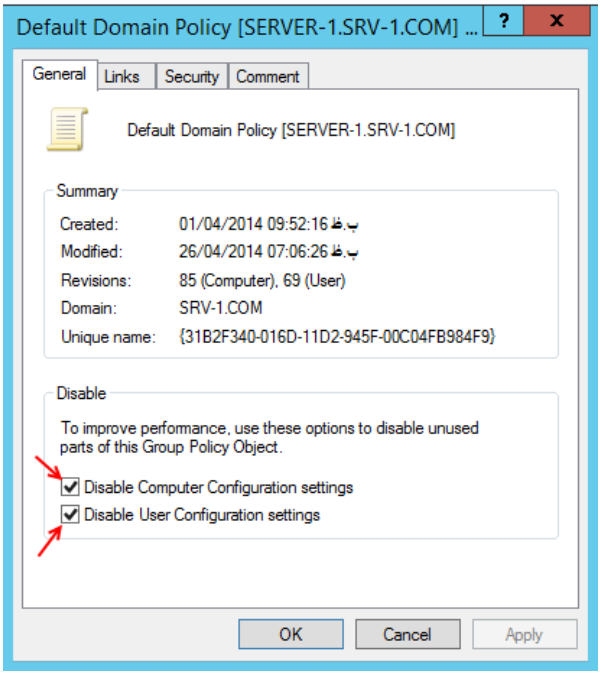
در صفحه بازشده گزینه Enable را انتخاب و بر روی ok کلیک کنید، بعد از این کار هیچ کاربری نمی‌تواند روی کلاینت خود کلیک راست کند.

در شکل بالا کارهایی دیگری می‌توان انجام داد مثلاً با Enable کردن گزینه Remove Computer Icon on the Desktop می‌توانید آیکون My computer را روی Desktop حذف کنیم و یا با فعال کردن گزینه Remove Properties from the computer icon context menu می‌توانید گزینه Properties مربوط به آیکون My Computer را حذف کنید، به همین راحتی.

غیر فعال کردن تمام تنظیمات انجام شده در Group Policy:



برای اینکه تمام تنظیمات اعمال شده روی Group Policy را به صورت سریع غیر فعال کنیم، بر روی Default Domain Policy کلیک راست می‌کنیم و گزینه Properties را انتخاب می‌کنیم.



در صفحه باز شده وارد تب General می‌شویم و تیک دو گزینه زیری آن را به مانند شکل روبرو انتخاب می‌کنیم و بعد بر روی ok کلیک می‌کنیم، با این کار تمام تنظیمات به حالت اولیه برمی‌گردد.

در ادامه سعی می‌کنیم تنظیمات پیشرفته Group policy را با هم بررسی کنیم.

نصب و پیکربندی سرویس مجازی سازی Hyper-V:

با توجه به پیشرفت سیستم عامل ویندوز در سال های اخیر، شاهد اضافه شدن امکان مجازی سازی در ویندوز بودیم که کاملاً حرکت جدیدی از طرف شرکت مایکروسافت است که توانست کاربران زیادی را به طرف خود جذب کند، این سرویس را می‌توان رقیبی در برابر VMware دانست, البته به قدرت VMware نمی‌تواند برسد ولی من که از این سرویس استفاده می‌کنم کاملاً راضی هستم و توانسته جای VMware را برای من بگیرد. خوبی این سرویس سبکتر بودن به نسبت VMware می‌باشد.

نرم افزار مورد نیاز:

برای راه اندازی این سرویس نیاز به سیتم عامل های زیر دارید:

Operating system	Version
Windows Server 2008	Standard, Enterprise, Datacenter, x64 bit
Windows Server 2008 R2	Standard, Enterprise, Datacenter, x64 bit
Windows Server 2012	Standard, Datacenter, x64 bit
Windows 8	Standard, Enterprise,x64 bit

همان‌طور که در جدول بالا مشاهده می‌کنید این سرویس فقط روی ویندوزهای 64 بیت نصب خواهد شد.

سخت‌افزار موردنیاز:

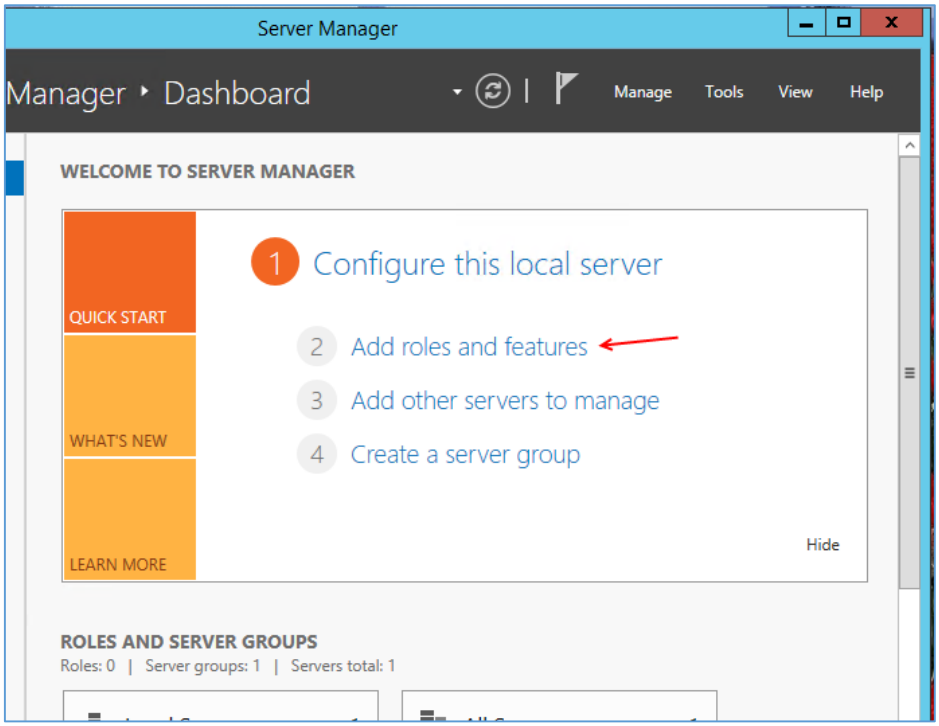
حداقل رم موردنیاز برای راه‌اندازی این سرویس 2GB است و حداکثر رم برای ویندوز سرور 2008 به حدود 1TB و ویندوز سرور 2012 حدوداً 4TB می‌باشد.

حداقل فضای هارددیسک برای راه‌اندازی این سرویس 10GB است و حداکثر آن سقفی ندارد.

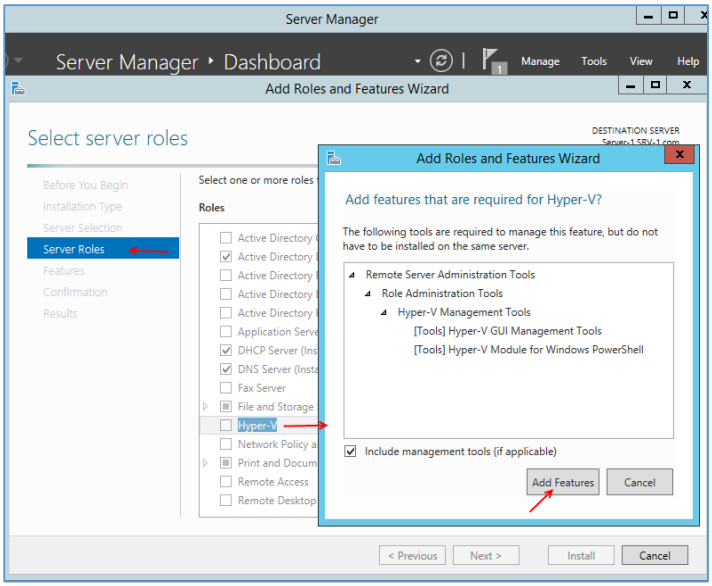
CPU موردنیاز این سیستم باید توانایی پشتیبانی از 64 bit را داشته باشد و باید توانایی پشتیبانی از Virtualization یا مجازی‌سازی را داشته باشد.

نصب سرویس Hyper-V:

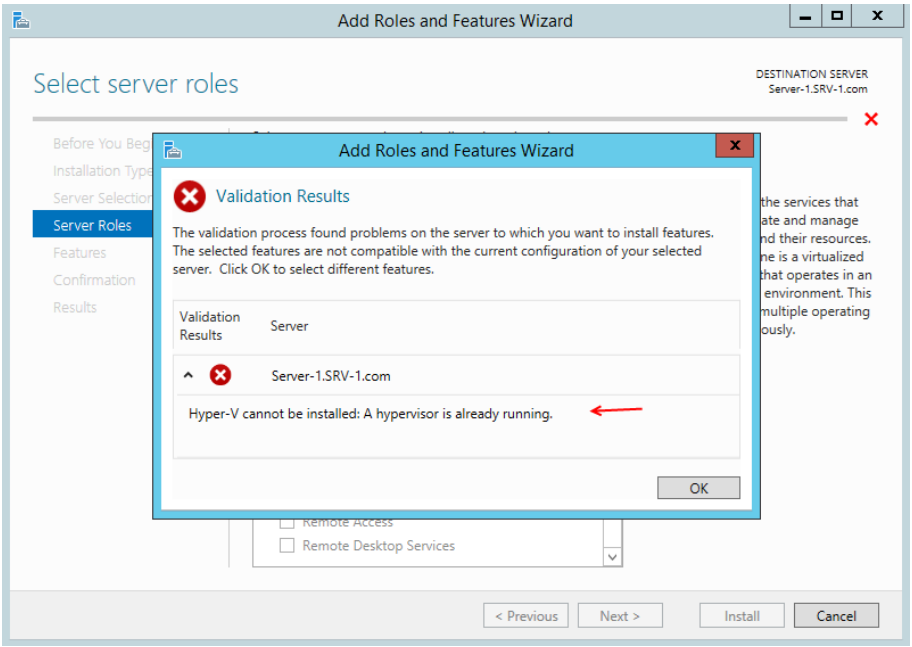
برای نصب سرویس Hyper-V باید وارد Server Manager بشویم و آن را نصب کنیم، در همین اول کار به یک نکته اساسی اشاره‌کنم که زمانی که ویندوز سرور شما روی سرویس Hyper-V نصب‌شده باشد که در این کتاب هم تمام سرویس‌ها بر روی Hyper-V نصب‌شده است، برای نصب سرویس Hyper-V به مشکل خواهی خرد، البته اگر ویندوز سرور روی سیستم اصلی نصب‌شده باشد نصب Hyper-V بدون مشکل انجام خواهد شد، باهم این موضوع را بررسی می‌کنیم.



Server Manager را اجرا کنید و به‌مانند شکل روبرو بر روی Add roles and features کلیک کنید.

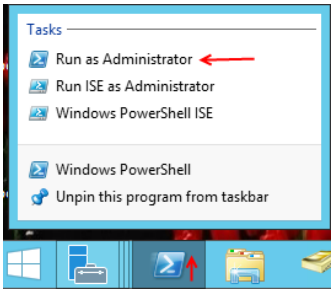


از سمت چپ وارد قسمت Server Roles شوید در این صفحه به‌مانند شکل گزینه Hyper را انتخاب کنید و در صفحه بازشده بر روی Add Features کلیک کنید.



بعد از کلیک بر روی Add Features در قسمت قبل با پیغام خطای روبرو مواجه می‌شوید که کاملاً نامفهوم است.

این خطابه این دلیل است که ویندوز روی ماشین مجازی بر روی سرویس Hyper-V نصب‌شده است و به این دلیل با پیغام خطای روبرو مواجه خواهید شد، توجه داشته باشید اگر از سیسم واقعی استفاده می‌کنید با هیچ خطایی مواجه نخواهید شد و می‌توانید با کلیک بر روی Next ادامه کار را انجام دهید، اما برای حل مشکل بالا باید دستورات زیر را در PowerShell اجرا کنیم تا Hyper-V نصب شود.



برای شروع سرویس PowerShell را با اولویت کاربر Administrator اجرا کنید.

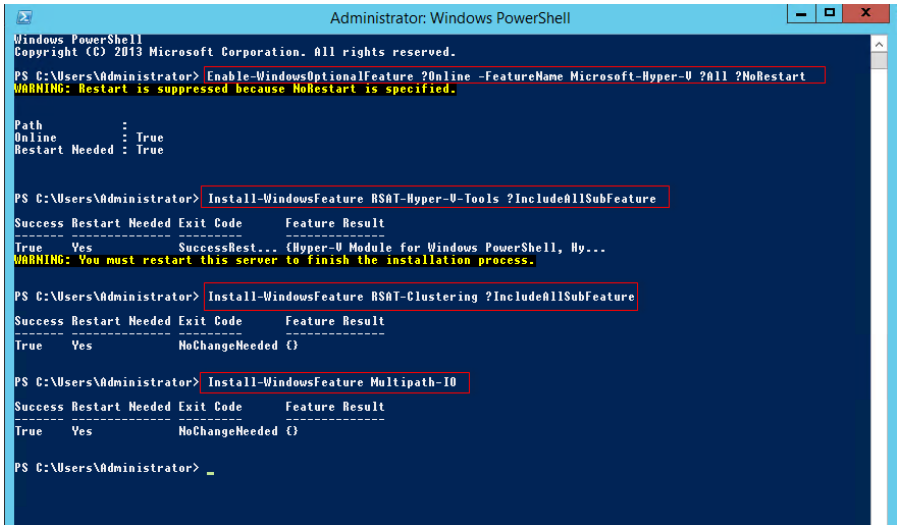
هرکدام از دستورات زیر را جدا از هم و به ترتیب در PowerShell اجرا کنید.

Enable-WindowsOptionalFeature –Online -FeatureName Microsoft-Hyper-V –All –NoRestart

Install-WindowsFeature RSAT-Hyper-V-Tools –IncludeAllSubFeature

Install-WindowsFeature RSAT-Clustering –IncludeAllSubFeature

Install-WindowsFeature Multipath-IO

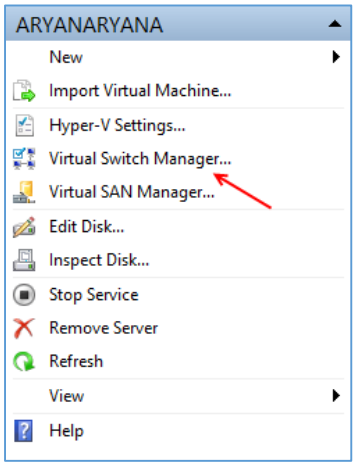


همان‌طور که در شکل روبرو مشاهده می‌کنید تمام دستورات بالا به‌درستی اجراشده است بعدازاین کار سیستم را Restart می‌کنیم.

بعد از اجرای ویندوز وارد search شوید و کلمه Hyper-V را وارد کنید و از بین گزینه‌های موجود گزینه Hyper-V Manager را انتخاب کنید.

سرویس Hyper-V را هم می‌توانید روی ویندوز 8 خود نصب کنید و سیستم‌های مجازی موردنیاز خود را روی آن پیاده‌سازی کنید.

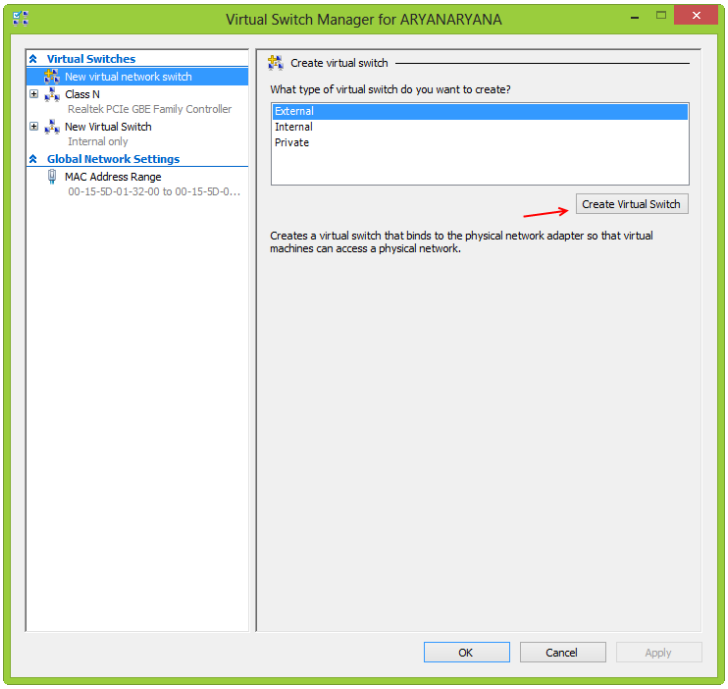
ایجاد کارت شبکه مجازی



این سرویس زمانی که راه‌اندازی می‌شود کارت شبکه مجازی را به‌صورت خودکار ایجاد نمی‌کند، بلکه باید به‌صورت دستی کارت شبکه خود را ایجاد کنیم.

برای این کار از سمت چپ بر روی گزینه Virtual Switch Manager کلیک کنید تا شکل بعد ظاهر شود.

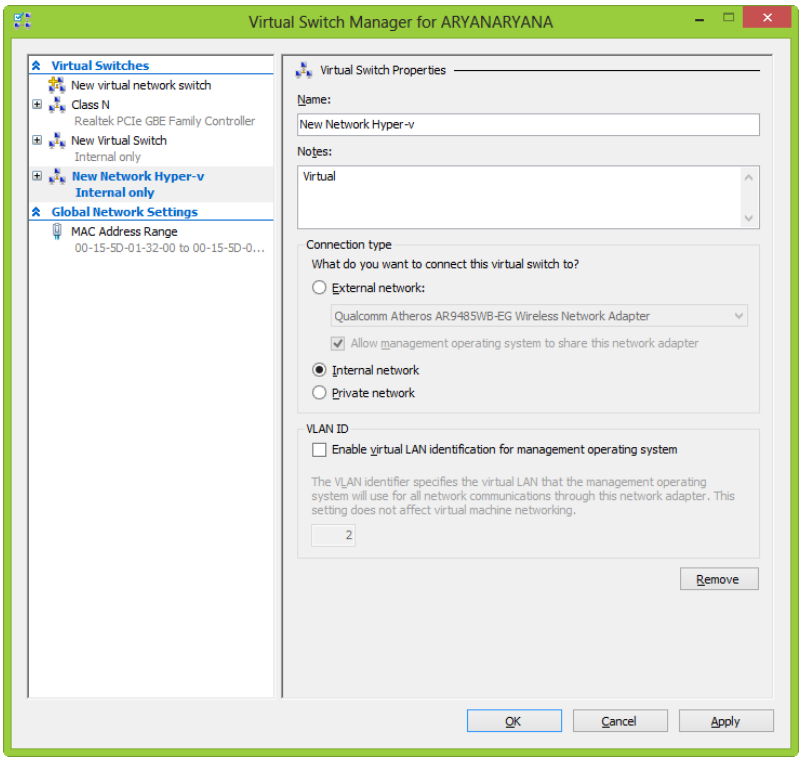
در شکل زیر سه گزینه وجود دارد که هرکدام را باهم بررسی خواهیم کرد فعلاً فقط بر روی Create Virtual Switch کلیک کنید.



گزینه‌هایی که در این قسمت وجود دارند به‌صورت زیر می‌باشند:

1- External: این گزینه برای ارتباط با کارت های شبکه واقعی سیستم شما می‌باشد که بسیار مفید و کاربردی است و در این آموزش هم روی آن کار خواهیم کرد.

2- Internal: این گزینه برای ارتباط داخلی سیستم شما می باشد که شما می‌توانید با سیستم واقعی خود ارتباط برقرار کنید.



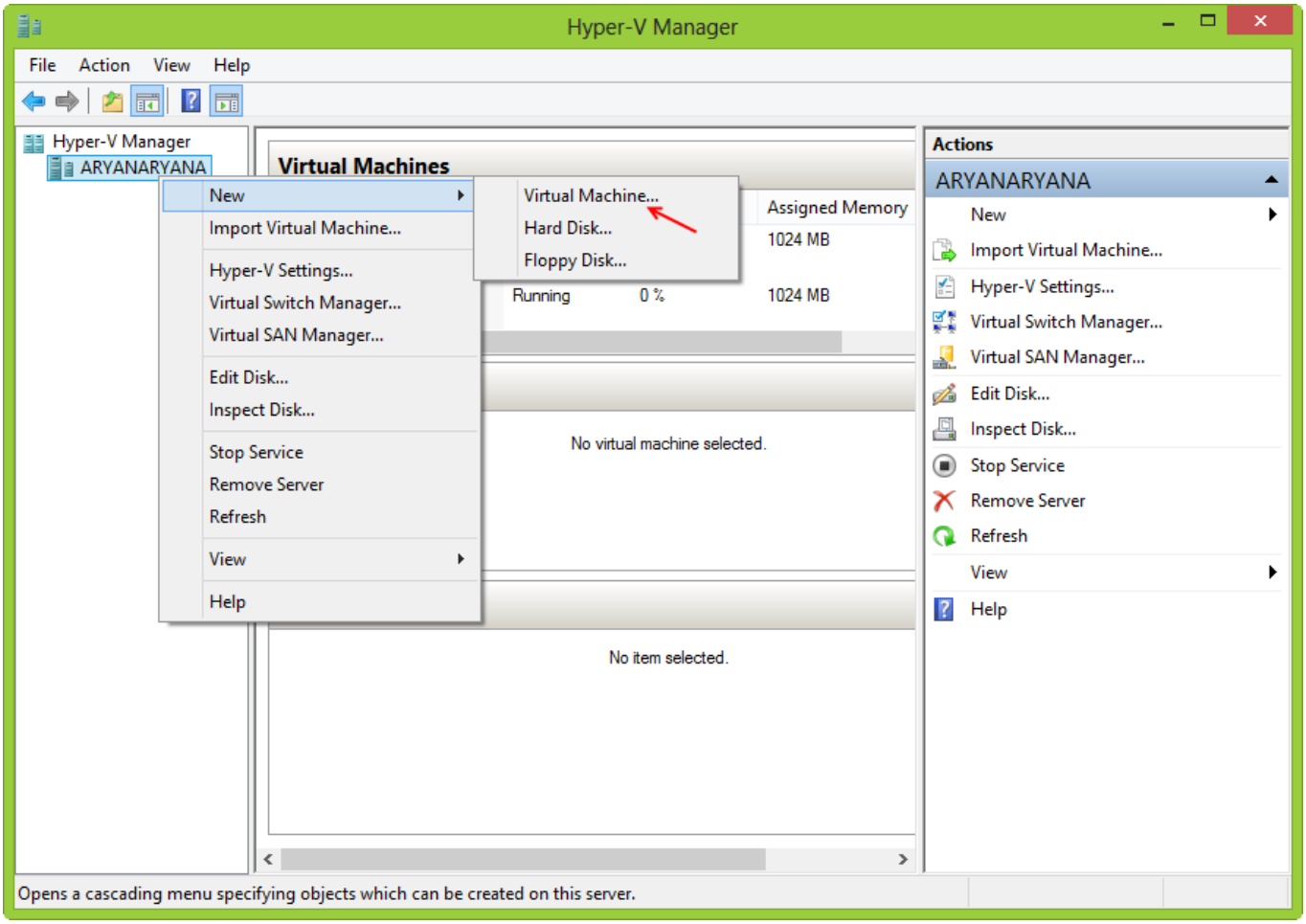
3- Private: این گزینه برای ارتباط ماشین های مجازی با هم است و ارتباطی با بیرون ندارد شاید درعین‌حال با گزینه Internal تفاوتی نداشته باشد، اما گزینه Internal می‌تواند با سیستم واقعی شما ارتباط برقرار کند ولی Private نمی‌تواند این کار را انجام دهد، در ادامه روی این موضوع بحث کوهیم کرد.

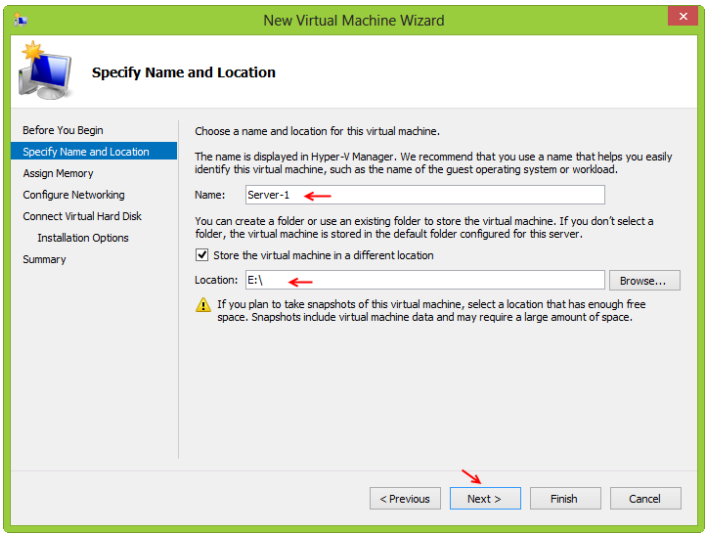
در قسمت Name نام ماشین مجازی خود را وارد کنید و در قسمت Notes توضیحاتی را درباره این ماشین مجازی وارد کنید. در قسمت Connection Type گزینه دوم یعنی Internal Network را انتخاب و بر روی Ok کلیک کنید.

بعد ایجاد کارت شبکه مجازی، شروع به ایجاد ماشین مجازی می‌کنیم و نحوه اجرای آن را باهم پیگیری می‌کنیم.

ایجاد ماشین مجازی

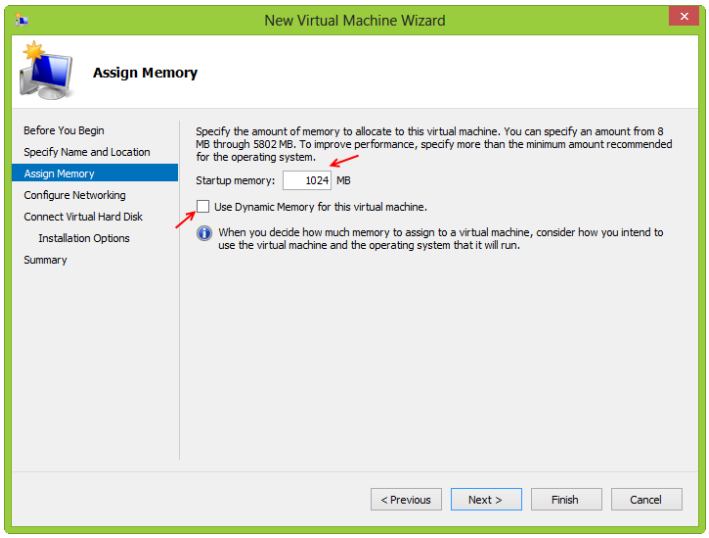
برای این کار مانند شکل زیر بر روی نام سرور خود کلیک راست می‌کنیم و از طریق گزینه New بر روی Virtual Machine.. کلیک می‌کنیم.



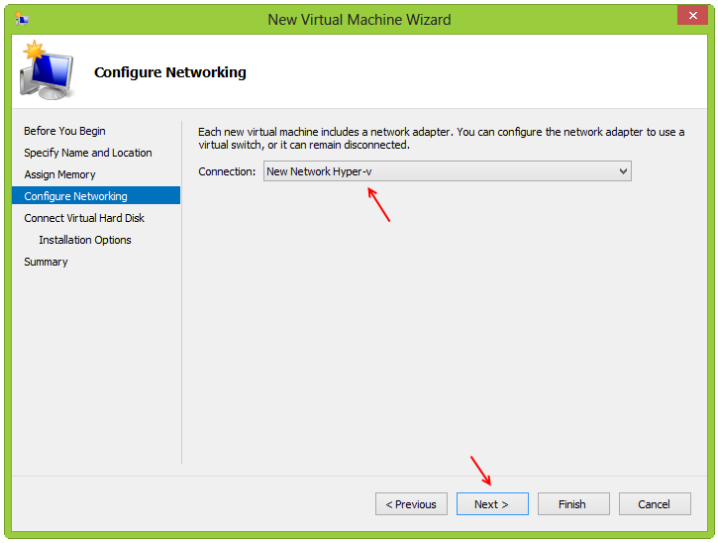


در قسمت Name یک نام برای سرور مجازی خود وارد کنید و بعد می‌توانید با کلیک بر روی گزینه Store the Virtual.... مسیر موردنظر خود را برای ذخیره‌سازی ماشین مجازی انتخاب کنید.

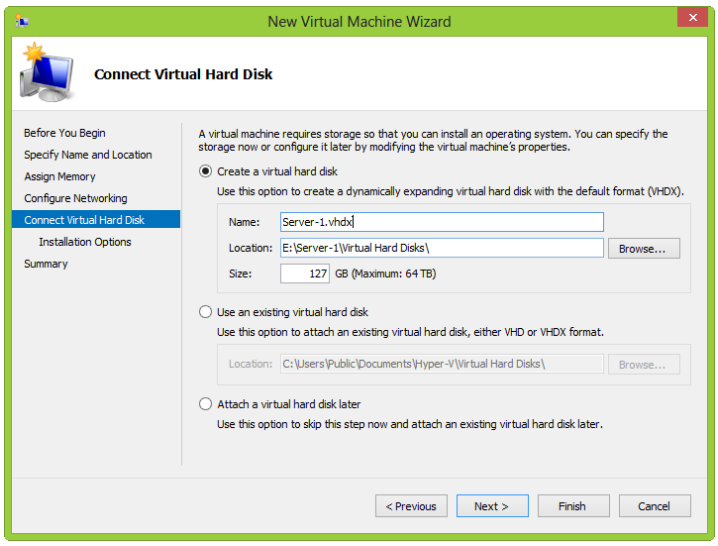
بر روی Next کلیک کنید.



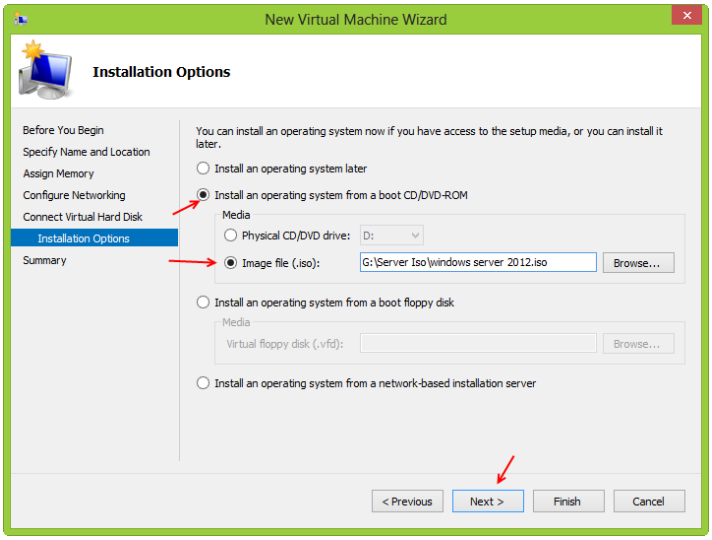
در قسمت Startup Memory مقدار حافظه موردنیاز که می‌خواهید به سرور مجازی خود اختصاص دهید را وارد کنید و اگر تیک گزینه Use Dynamic Memory را فعال کنید، از حافظه رم در صورت نیاز استفاده خواهد کرد، یعنی اگر این گزینه فعال باشد شاید حافظه رم بیشتر از مقداری شود که شما وارد کرده‌اید یا کمتر، در کل برای بالانس حافظه بین چند ماشین مجازی به کار می‌رود.



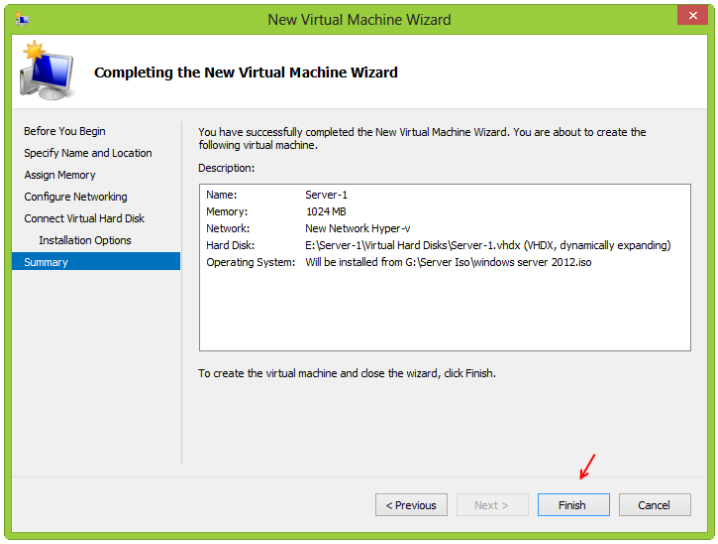
در این صفحه کارت شبکه‌ای که قبلاً باهم ایجاد کرده-ایم را انتخاب می‌کنیم و بر روی Next کلیک کنید.



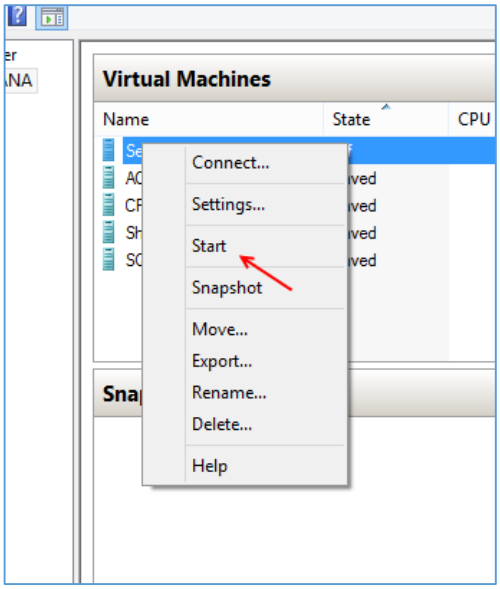
در قسمت اول می‌توانید نام هارددیسک مجازی خود را وارد و مسیر آن را مشخص کنید و بعد مقدار حافظه آن را تخصیص دهید. در قسمت دوم می‌توانید از هارددیسک‌هایی استفاده کنید که قبلاً ایجاد کرده‌اید و با انتخاب قسمت سوم می‌توانید این قسمت را بعداً انجام دهید، فعلاً گزینه اول را انتخاب و بر روی Next کلیک کنید.



در این قسمت باید DVD مربوط به ویندوز موردنظر خود را در سیستم قرار دهید و گزینه Physical CD/DVD را انتخاب کنید و یا اگر از ویندوز Image تهیه کردید می‌توانید در قسمت Image File بر روی Browse کلیک کنید و فایل Image موردنظر را معرفی کنیم، بعد از انجام این کاربر روی Next کلیک کنید.



در این قسمت بر روی Finish کلیک کنید.

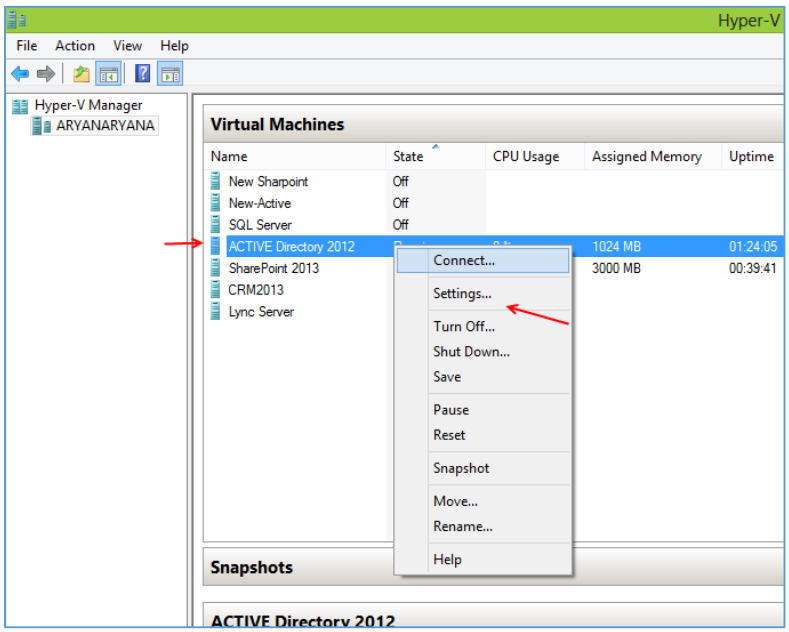


بعد از ایجاد Virtual Machine مانند شکل روبرو بر روی ماشین مجازی کلیک راست کنید و بر روی Start کلیک کنید تا سیستم شروع به کار کند. شما می‌توانید ویندوز موردنظر خود را به راحتی نصب کنید. در این آموزش ویندوز سرور 2012 سرور نصب‌شده است.

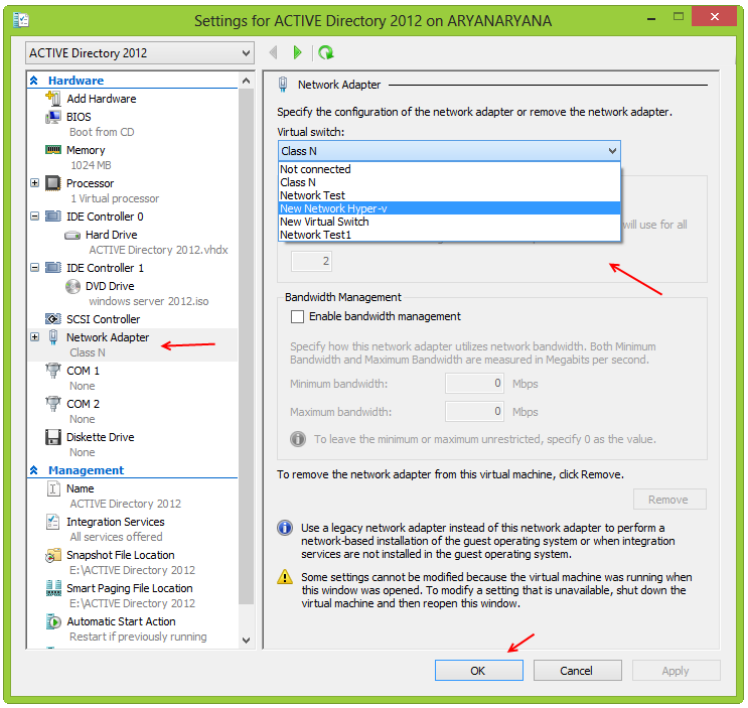
نصب ویندوز سرور در اوایل کتاب بررسی‌شده است که با خواندن آن مشکلات شما حل خواهد شد.

چگونه ماشین‌های مجازی را باهم شبکه کنیم:

برای انجام این کار شما باید اول‌ازهمه کارت شبکه ماشین‌های مجازی خود را بر روی یک کارت شبکه مشابه قرار دهید و بعد وارد هر یک از ماشین‌های مجازی شده و ip در یک رنج مثلاً 172.16.20.0 قرار دهید تا ارتباط برقرار شود، توجه داشته باشید Firewall هم باید خاموش باشد و یا اگر روشن است باید اجازه عبور به این سیستم‌ها را بدهد، باهم این موضوع را بررسی می‌کنیم.

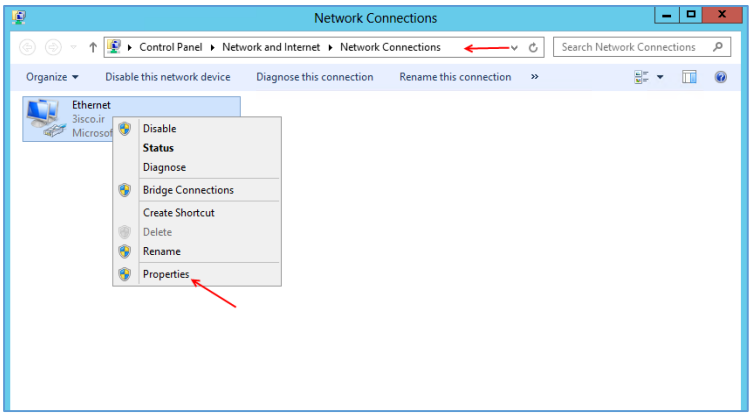


در این قسمت شما چندین ماشین مجازی مشاهده می‌کنید که در شکل هم مشخص‌شده است، ما می‌خواهیم سرور Active Directory و سرور SharePoint 2013 را باهم شبکه کنیم، توجه داشته باشید روی هرکدام از سرورها ویندوز سرور 2012 نصب‌شده است، برای شروع روی سرور Active به‌مانند شکل کلیک راست می‌کنیم و گزینه Settings را انتخاب می‌کنیم تا شکل بعد ظاهر شود.

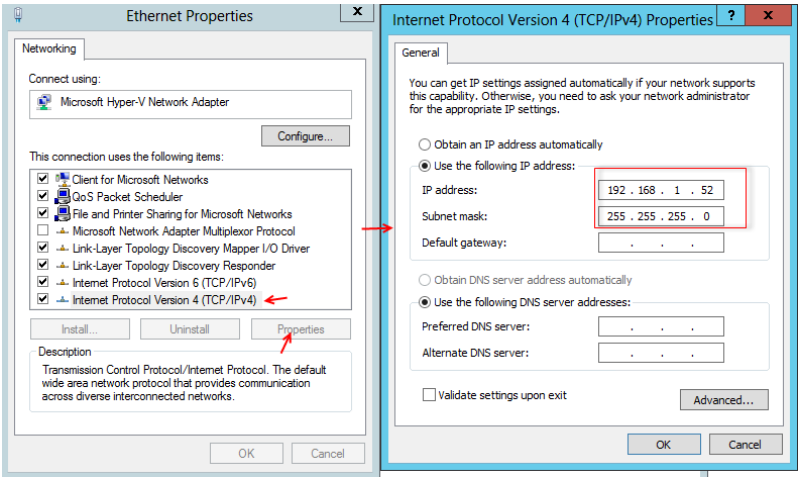


در این قسمت از سمت چپ گزینه Network Adapter را انتخاب کنید و در صفحه بازشده و در قسمت Virtual Switch کارت شبکه موردنظر خود را انتخاب کنید.

نکته: کارت شبکه‌ای که برای این سرور در نظر می‌گیرید حتماً باید در سرور دوم که در اینجا سرور SharePoint2013 است هم همین کارت شبکه را انتخاب کنید. برای ادامه کاربر روی ok کلیک کنید.



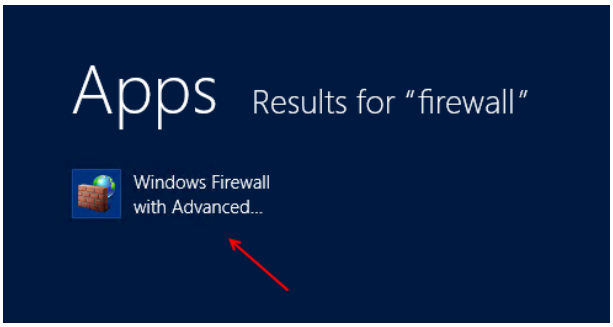
بعدازاین که کارت شبکه هر دو سرور را انتخاب کردیم وارد هر یک از سرورها می‌شویم و وارد قسمت Network connections می‌شویم، در این قسمت بر روی کارت شبکه خود کلیک راست کنید و Properties را انتخاب کنید.

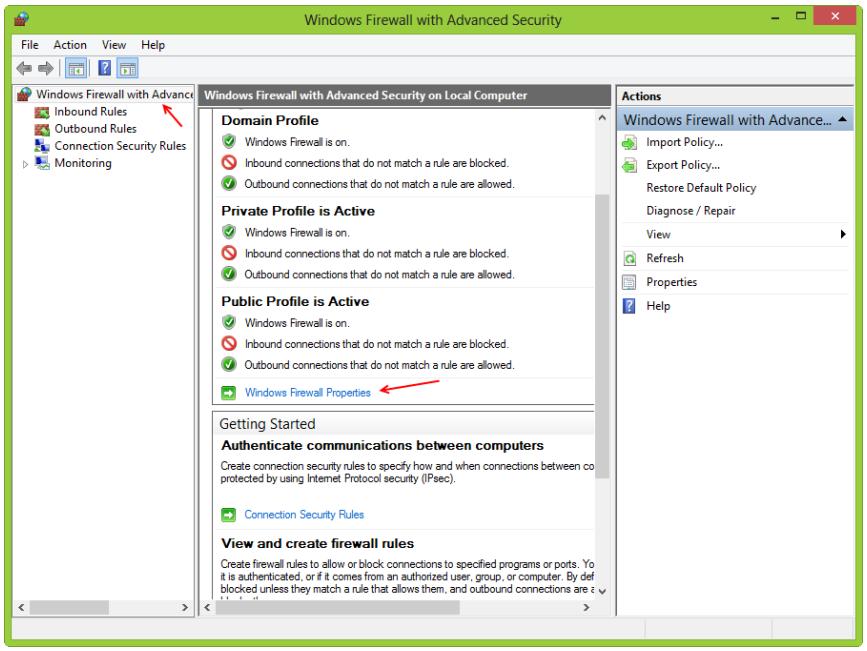


در این شکل باید IP موردنظر خود را وارد کنید که در اینجا 192.168.1.52 برای سرور SharePoint واردشده است و همین رنج IP در سرور Active هم واردشده است یعنی 192.168.1.50 و IP مربوط به DNS را روی 192.168.1.50 قراردادیم.

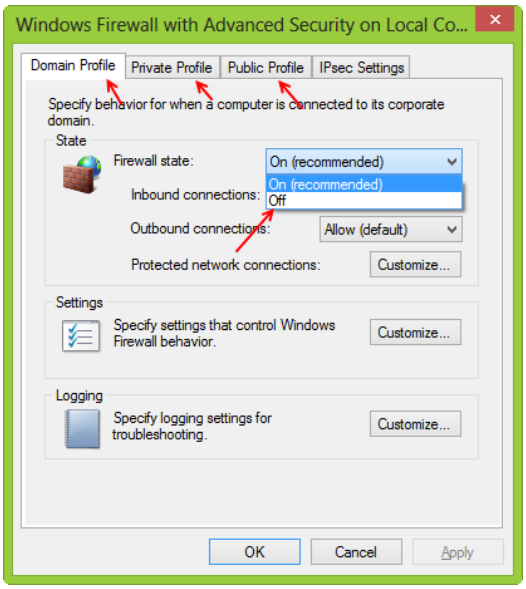
بر روی ok کلیک کنید تا تنظیمات ذخیره شود.

بعدازاین کار باید فایروال مربوط به هر دو سرور را خاموش کنیم، برای این کار وارد Start شوید و در قسمت جستجو کلمه Firewall را وارد کنید و در نتیجه جستجو بر روی Windows Firewall with advanced... کلیک کنید تا شکل بعد ظاهر شود.





مانند شکل بالا در وسط صفحه بر روی Windows Firewall Properties کلیک کنید.



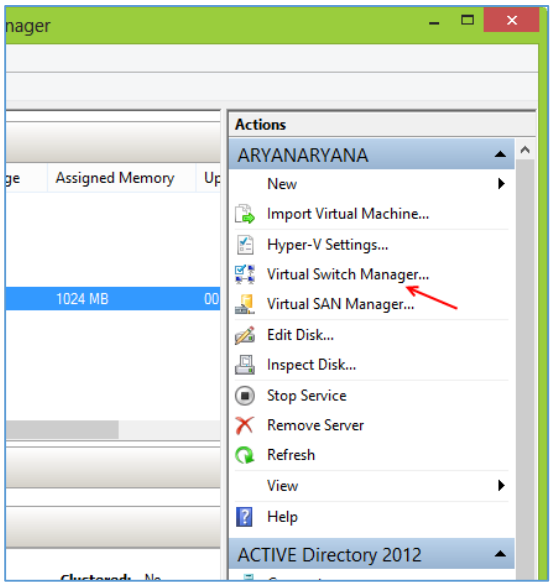
در این صفحه سه Tab با نام های Domain Profile, Private Profile, Public Profile وجود دارد که باید بر روی همه آن ها کلیک کنید و از قسمت Firewall State لیست کشویی را باز کنید و گزینه Off را انتخاب کنید بعد از این کار Firewall برای همیشه از روزگار محو خواهد شد ولی این کار را در سازمان خود انجام ندهید این کار فقط برای تست می باشد.

حالا می‌توانید وارد هر یک از سرور ها شوید و سرور مقابل را Ping کنید.

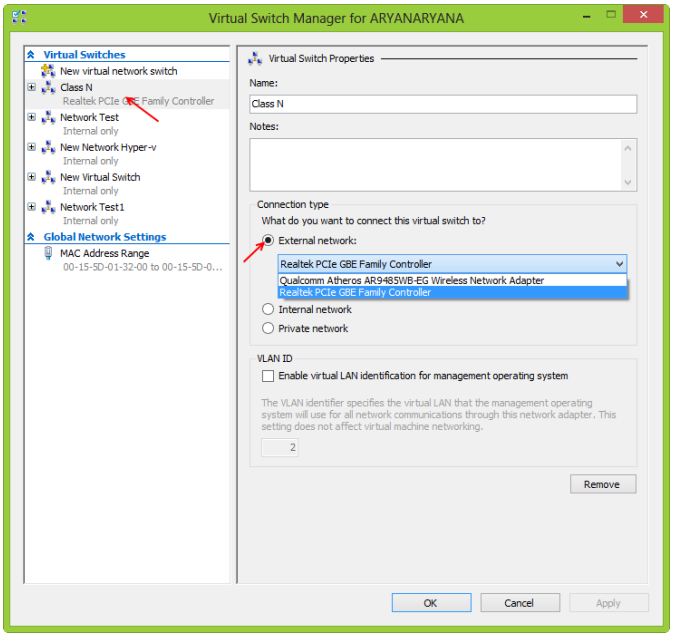
چگونه ماشین مجازی را به سیستم واقعی ارتباط دهیم:

یکی از بهترین روش هایی که می‌توان از ماشین مجازی استفاده کرد این است که بتوانیم ماشین‌های مجازی را به سیستم واقعی متصل کنیم تا بتوانیم از منابع سیستم‌های واقعی استفاده کنیم و یا بتوانیم ماشین های مجازی را از راه دور مدیریت کنیم.

برای شروع کار به مانند قبل یک ماشین مجازی روی سرویس Hyper-V راه‌اندازی می‌کنیم، روی این ماشین مجازی سیستم عامل ویندوز سرور 2012 نصب می‌کنیم و نحوه ارتباط آن را با سیستم واقعی بررسی می‌کنیم.



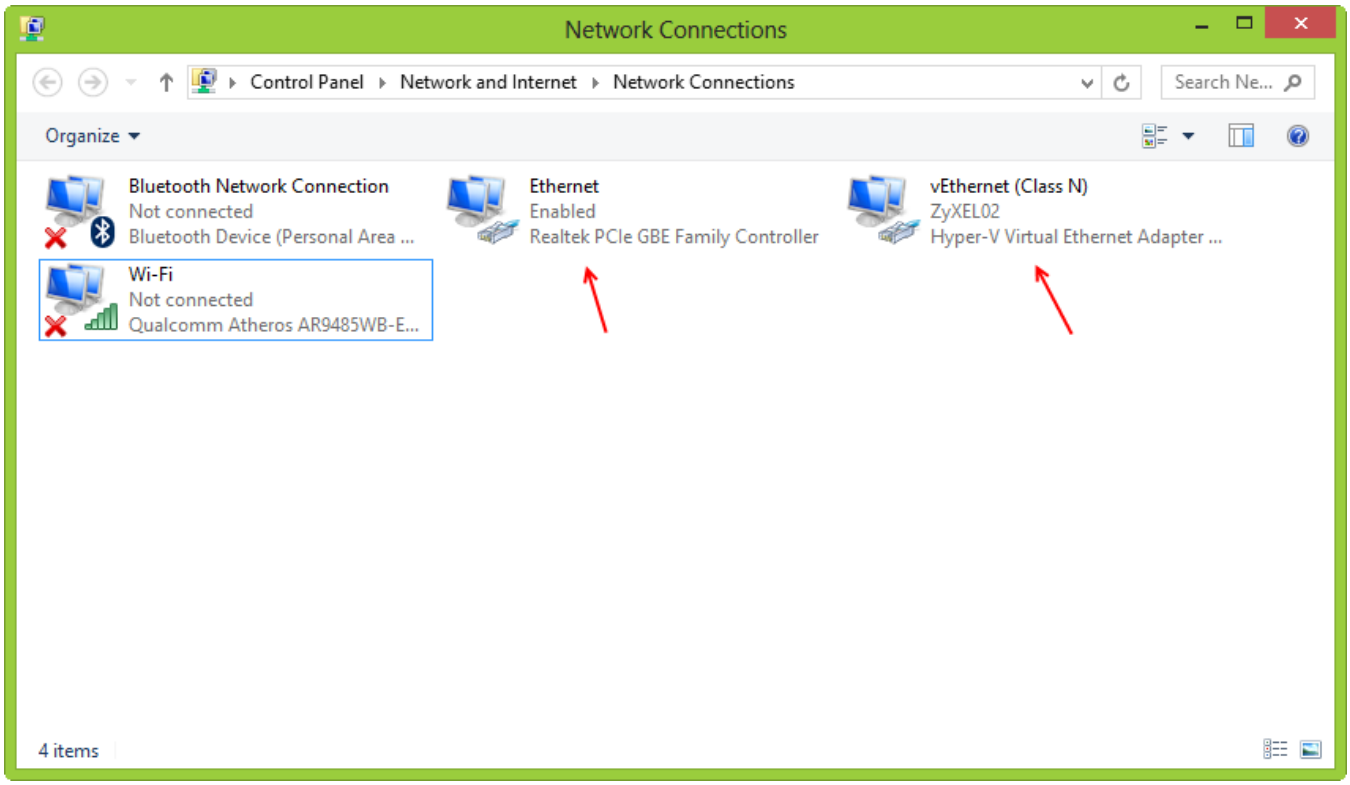
سرویس Hyper-V را اجرا می‌کنیم و در سمت راست قسمت Actions گزینه Virtual Switch Manager را انتخاب می‌کنیم تا شکل بعد ظاهر شود.



در این صفحه از قسمت Virtual Switch در سمت چپ کارت شبکه مجازی خود را که قبلاً ایجاد کرده‌ایم انتخاب می‌کنیم و در صفحه باز شده در سمت راست آن که با فلش هم مشخص‌شده است گزینه External network را انتخاب می‌کنیم، در لیست مشخص‌شده دو کارت شبکه را مشاهده می‌کنیم که یکی برای وایرلس و دیگری برای LAN می‌باشد که هر کدام را می‌توانیم انتخاب کنیم، فعلاً کارت شبکه LAN را انتخاب می‌کنیم

که در سیستم شما هم همین کارت شبکه با نام دیگر موجود است، بعد از انتخاب کارت شبکه بر روی ok کلیک کنید تا تنظیمات موردنظر اعمال شود.

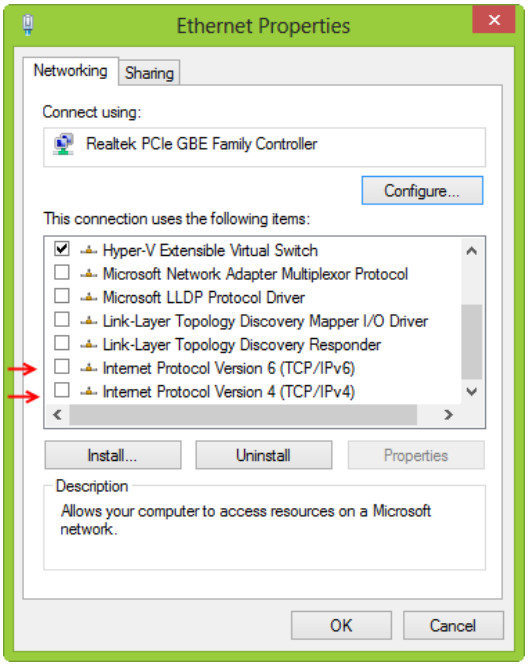
بعد از انجام تنظیمات بالا وارد Network Connections سیستم واقعی می‌شویم، همانطور که در شکل زیر مشاهده می‌کنید دو کارت شبکه مشخص‌شده است، کارت شبکه با نام Ethernet کارت شبکه واقعی می‌باشد



و کارت شبکه با نام vEthernet (Class N) کارت شبکه مجازی می‌باشد که به کارت شبکه واقعی (Ethernet) متصل کردیم.

نکته مهم: زمانی کارت شبکه مجازی می‌تواند به شبکه واقعی سیستم شما متصل شود که کارت شبکه اصلی شما فعال باشد، یعنی اینکه مثلاً به یک مودم ADSL متصل باشد.

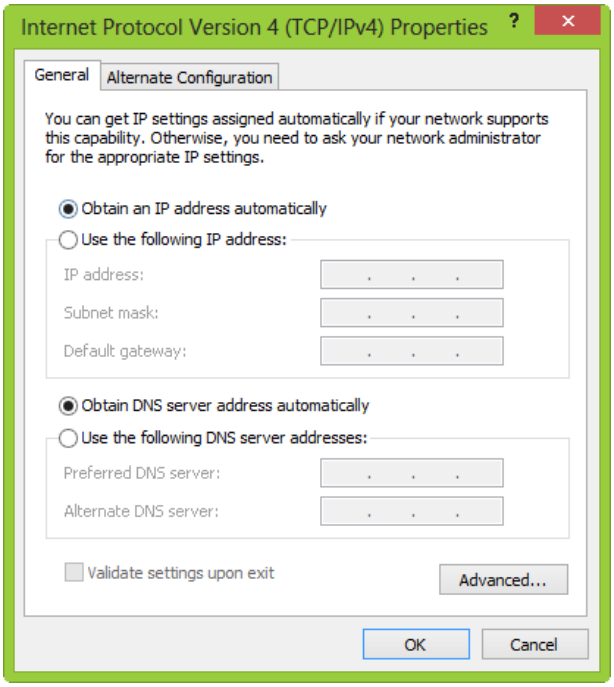
نکته: در حال حاضر اگر سیستم واقعی شما به اینترنت متصل باشد و تنظیمات کارت شبکه را بر روی Obtain an IP Address Automatically قرار داشته باشد، سیستم مجازی می‌تواند به اینترنت متصل شود.



روی کارت شبکه واقعی (Ethernet) کلیک راست کنید و گزینه Properties را انتخاب کنید تا صفحه روبرو باز شود.

همانطور که در این صفحه مشاهده می‌کنید، در لیست موجود تمام پروتکل‌ها غیر فعال شده است و فقط پروتکل مربوط به سرویس Hyper-V با نام Hyper-V Extensible Virtual Switch فعال است، یعنی تمام کار این کارت شبکه به کارت شبکه vEthernet (Class N) انتقال داده شده است و کنترل می‌شود.

برای ارتباط سیستم واقعی با ماشین مجازی روی کارت شبکه مجازی (vEthernet (Class N)) خود کلیک راست کنید و گزینه Properties را انتخاب کنید و از لیست موجود بر روی Internet Protocol Version4 دو بار کلیک کنید. تا شکل روبرو باز شود.

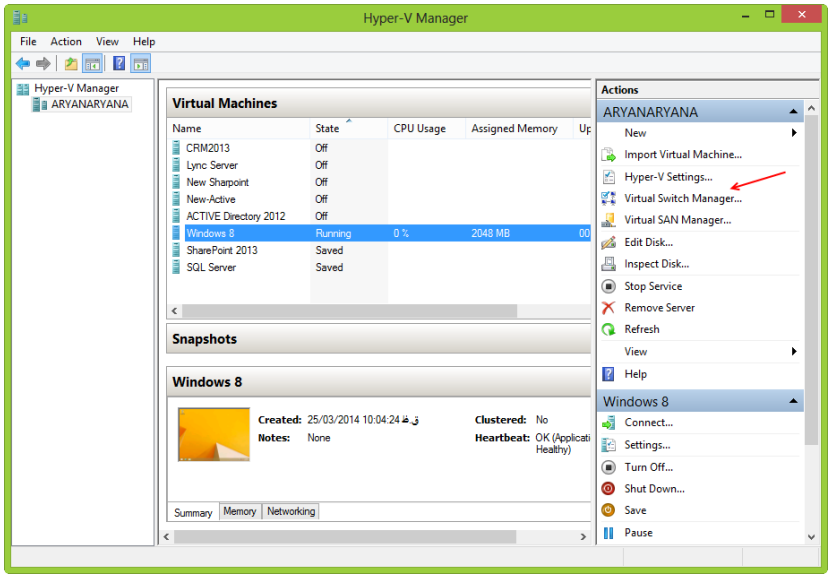


در این شکل اگر کارت شبکه شما به مودم ADSL متصل است می‌توانید روی حالت Obtain an IP Address Automatically قرار دهید تا مستقیم از طریق سرویس DHCP مربوط به مودم IP دریافت کند؛ و بعد از این کار باید وارد ماشین مجازی شوید و کارت شبکه آن را در حالت Obtain an IP Address Automatically قرار دهید تا از طریق مودم IP دریافت کند که با این کار هم به سیستم واقعی دسترسی دارد و هم به اینترنت مربوط به مودم ADSL.

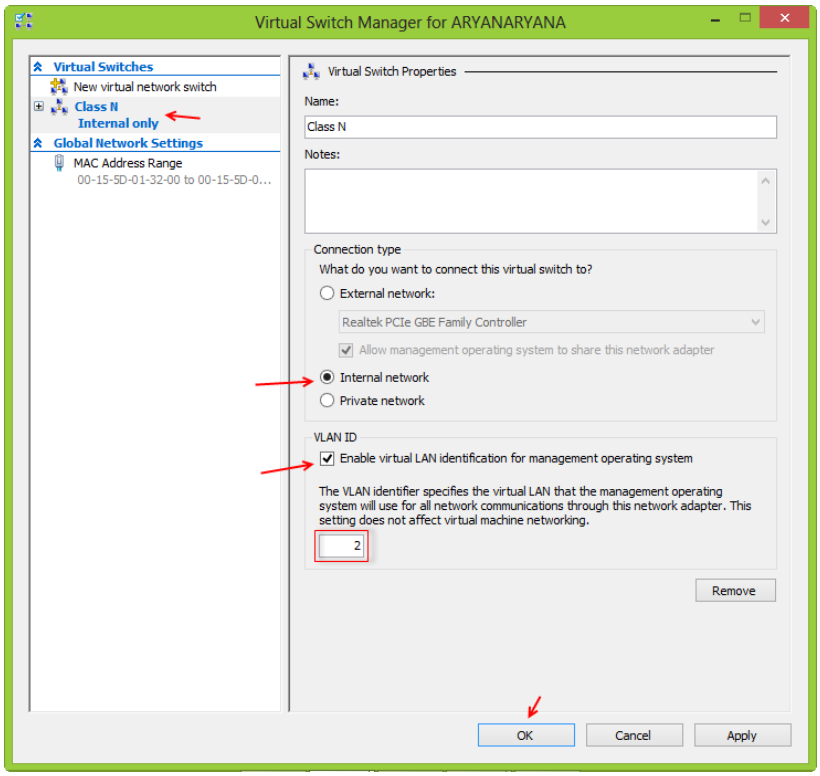
در این قسمت سوألی داشتید با من در تماس باشید.

ارتباط سیستم واقعی با ماشین مجازی بدون فعال بودن کارت شبکه واقعی:

در قسمت قبلی زمانی که کارت شبکه مجازی به کارت شبکه واقعی متصل می‌شد، در صورتی با هم ارتباط برقرار می‌کردند که کارت شبکه اصلی فعال باشد یعنی به مودم ADSL یا به دستگاهی دیگر متصل باشد، ولی شاید بخواهید بدون فعال بودن کارت شبکه اصلی، از طریق سیستم واقعی به ماشین مجازی متصل شوید برای این کار باید کارهای زیر را با آرامش انجام دهید.

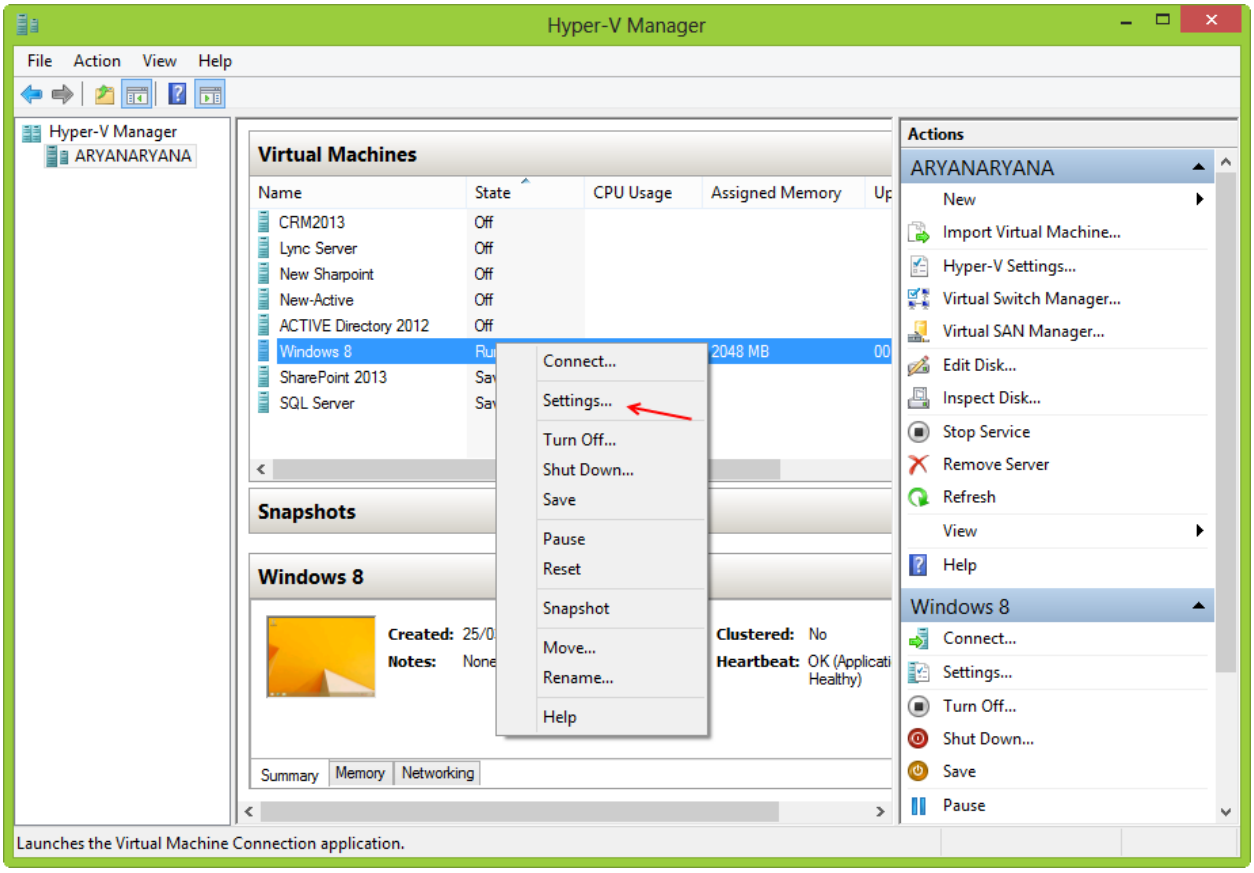


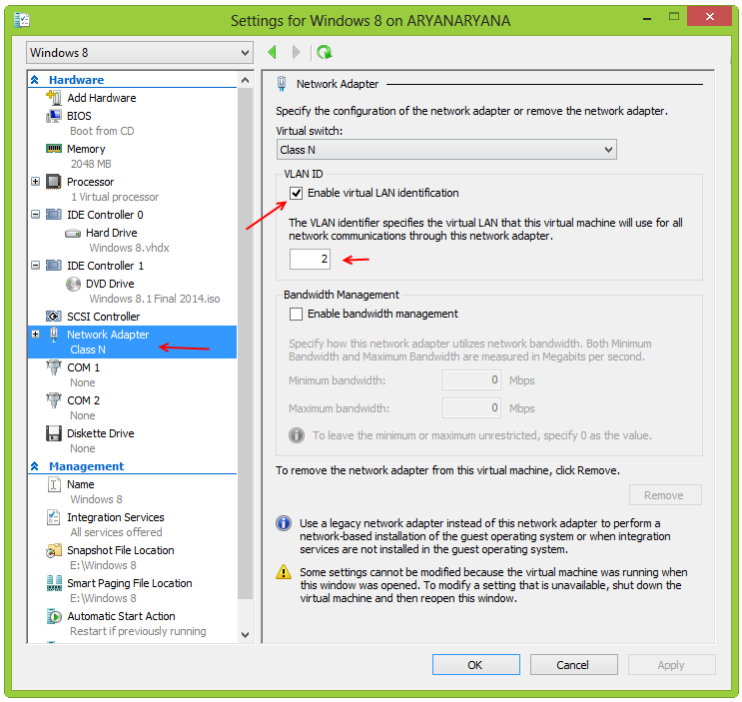
برای شروع کار وارد سرویس موردنظر شوید واز سمت راست بر روی Virtual Switch Manager... کلیک کنیدتا شکل بعد ظاهر شود.



در این قسمت از سمت چپ بر روی کارت شبکه موردنظر خود کلیک کنید تا صفحه مربوط به آن به مانند شکل باز شود، در این صفحه در قسمت Connection type گزینه Internal Network را انتخاب کنید، بعد از این کار حتما تیک مربوط به Enable .... Virtual LAN را انتخاب کنید و یک عدد از 1 تا 4094 وارد کنید. این گزینه همان VLAN در سوئیچ‌ها می‌باشد که یک مسیر مجازی را برای ما ایجاد می‌کند بعد از این کار بر روی ok کلیک کنید.

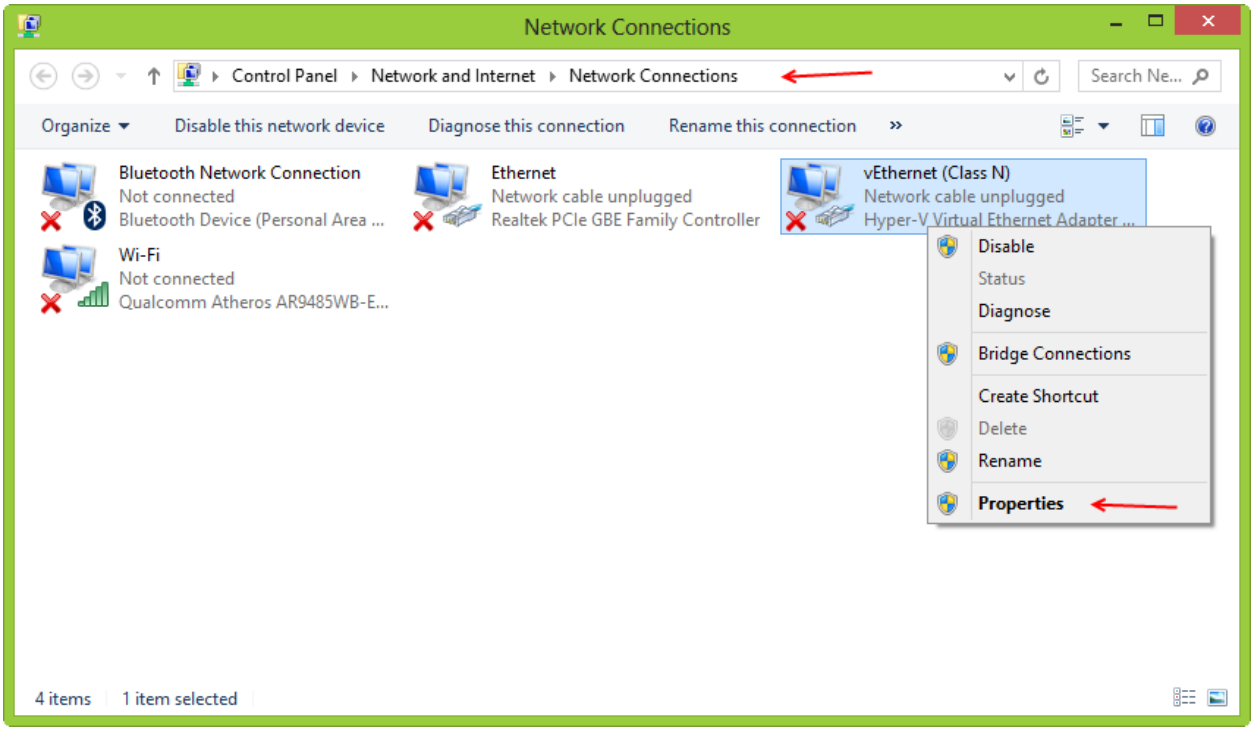
بعد از انجام کارهای بالا به مانند شکل زیر بر روی ماشین مجازی که می‌خواهید با سیستم واقعی در ارتباط باشد، کلیک راست کنید و گزینه Settings... را انتخاب کنید.



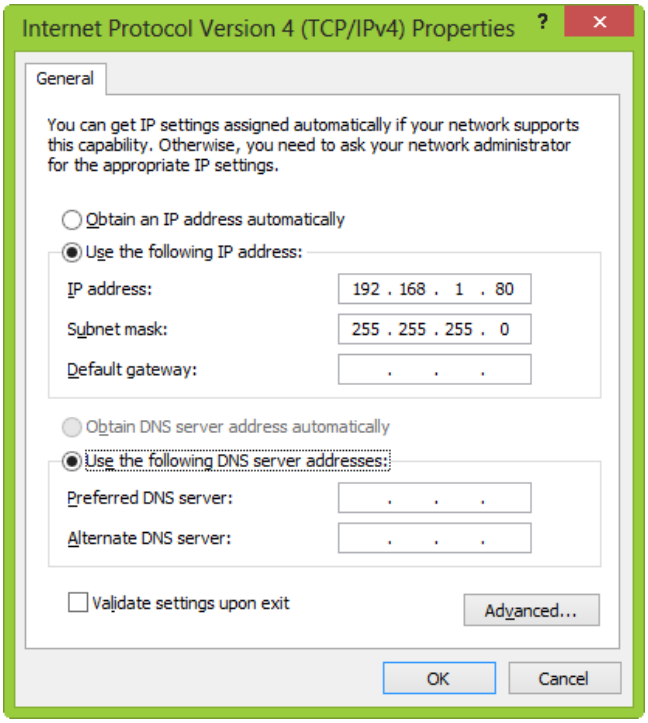


در این شکل از سمت چپ کارت شبکه را انتخاب کنید و در صفحه باز شده می‌توانید در قسمت Virtual Switch کارت شبکه موردنظر خود را انتخاب کنید، این کارت شبکه باید همان کارت شبکه ای باشد که در قسمت قبل تنظیم کردیم، بعد از این کار حتماً .... Enable Virtual LAN را انتخاب کنید و عدد 2 که در قسمت قبل هم همین عدد را وارد کردیم در این قسمت وارد می‌کنیم و بر روی ok کلیک می‌کنیم.

بعد از انجام کارهای بالا وارد Network Connections در سیستم واقعی می‌شویم و روی کارت شبکه مجازی خود کلیک راست می‌کنیم و بر روی Properties کلیک می‌کنیم و در صغحه باز شده بر روی



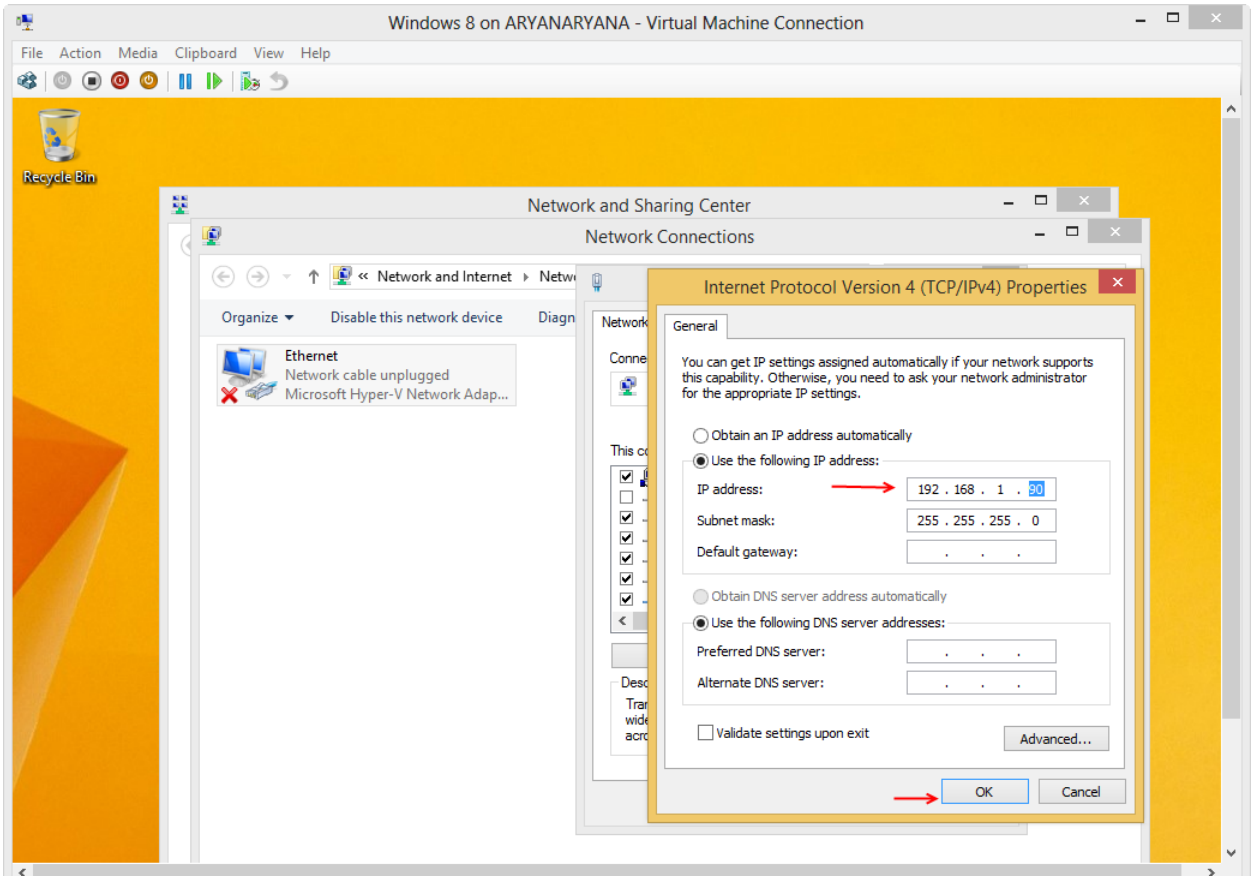
Internet Protocols Version 4 دو بار کلیک کنید تا شکل بعد ظاهر شود.



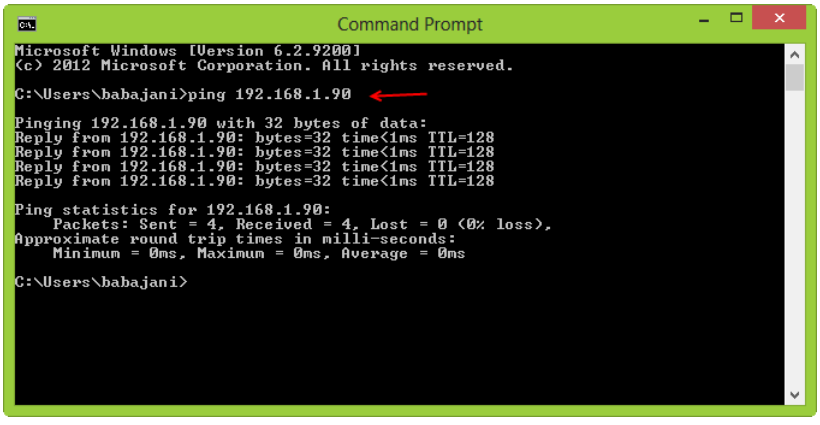
در این صفحه IP Address موردنظر خود را وارد کنید که در این قسمت 192.168.1.80 وارد شده است، بر روی ok کلیک کنید.

بعد از این کار وارد ماشین مجازی خود می‌شویم و به کارت شبکه موردنظر آن در همین رنج IP می‌دهیم.

همانطور که در شکل زیر مشاهده می‌کنید، وارد ماشین مجازی خود شده‌ایم و به کارت شبکه موردنظر آدرس 192.168.1.90 را داده‌ایم که در رنج سیستم واقعی ما می‌باشد، بعد از این کار بر روی ok کلیک کنید تا همه چیز برای ارتباط آماده باشد.



حالا می‌توانید از هر کدام از سیستم ها نحوه ارتباط را تست کنیم.



همانطور که مشاهده می‌کنید، از طریق سیستم اصلی به سیستم مجازی Ping کردیم و به درستی به ما پاسخ داد این در صورتی بود که کارت شبکه واقعی به هیچ دستگاهی متصل نبود.

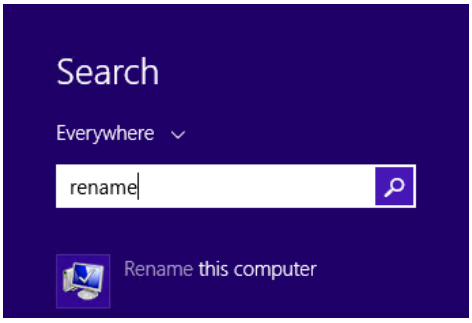
در این قسمت سوألی داشتید با من در تماس باشید.

چگونه فایل های داخل سیستم واقعی را وارد ماشین مجازی کنیم:

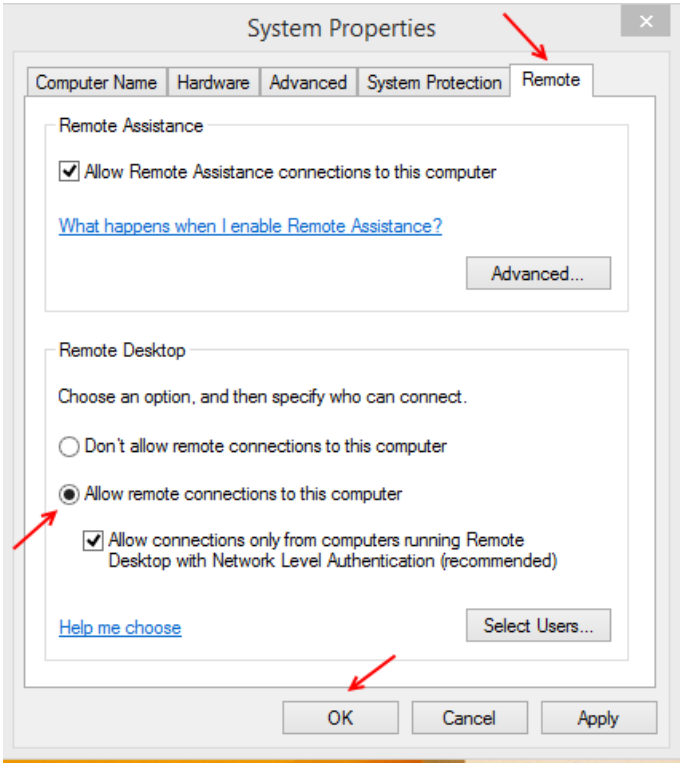
برای اینکه بتوانیم فایلی را از سیستم واقعی وارد سیستم مجازی کنیم و یا بلعکس، اولین کاری که باید انجام دهیم این است که مانند روش قبلی ارتباط دو ماشین مجازی را برقرار کنیم و بعد از آن می‌توانید از فایل های هر دو سیستم استفاده کنیم.

اولین کاری که می‌توانیم انجام دهیم این است که فایل موردنظر خود را share کنیم و از آن در سیستم مجازی و یا بلعکس استفاده کنیم که کار کاملاً ساده ای می‌باشد اگر در این قسمت مشکلی دارید به من ایمیل بزنید.

روش بعدی که از روش قبلی بهتر می‌باشد استفاده از سرویس Remote Desktop Connection می‌باشد که به راحتی می‌توانیم فایل‌های موردنظر خود را وارد سیستم کنیم.

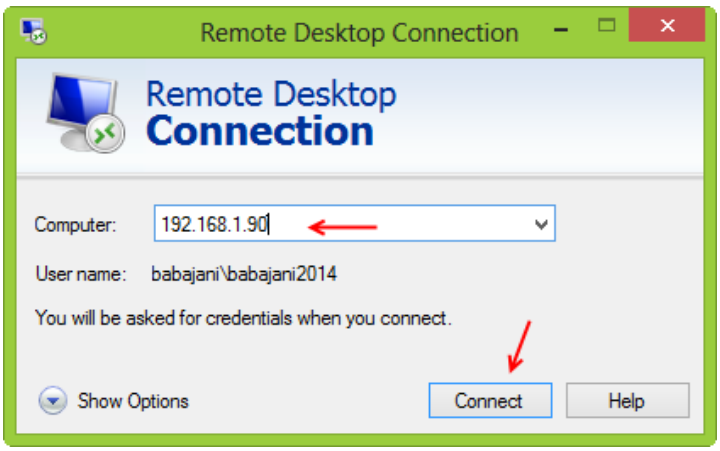


برای انجام این کار اول باید قابلیت Remote را در سیستم مجازی فعال کنیم، برای همین وارد سیستم مجازی می‌شویم و در Search کلمه Rename را وارد می‌کنیم و بعد گزینه Rename this Computer را انتخاب می‌کنیم تا شکل بعد ظاهر شود.

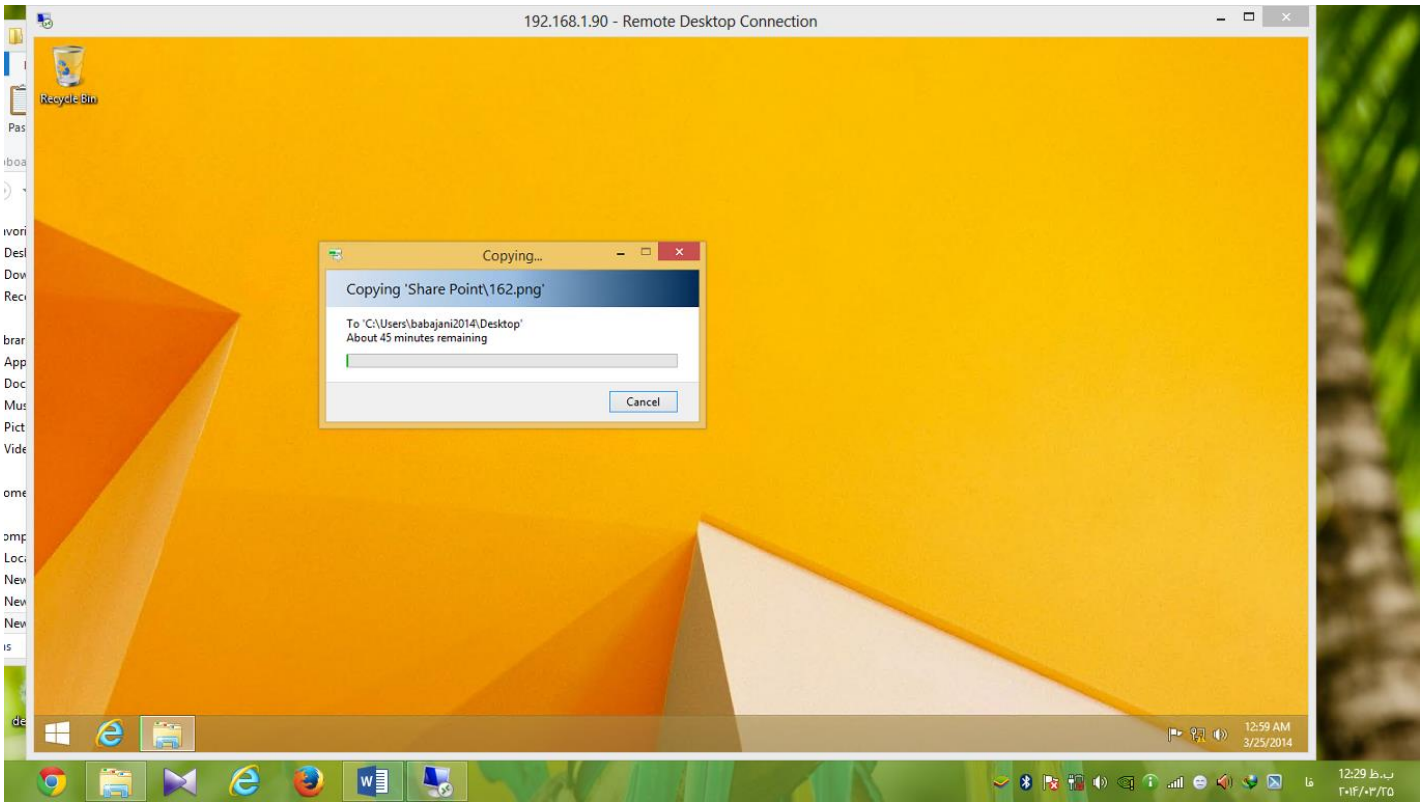


در این صفحه بر روی تب Remote در بالا کلیک کنید و در صفحه باز شده گزینه Allow remote... را به مانند شکل انتخاب و بر روی ok کلیک کنید تا مجوز دسترسی به افراد دیگر برای ارتباط از راه دور داده شود البته می‌توانید به هر کاربر مجوز دسترسی بدهید.

بعد از انجام کارهای بالا وارد سیستم اصلی می‌شویم و سرویس Remote Desktop Connection را اجرا می‌کنیم، برای بدست آوردن این سرویس آن را درSearch وارد کنید.



در این قسمت باید آدرس ماشین مجازی خود را که در قسمت قبل وارد کرده بودیم را در این قسمت وارد کنید و بعد بر روی Connect کلیک کنید بعد رمز مربوط به ویندوز مجازی را وارد کنید.

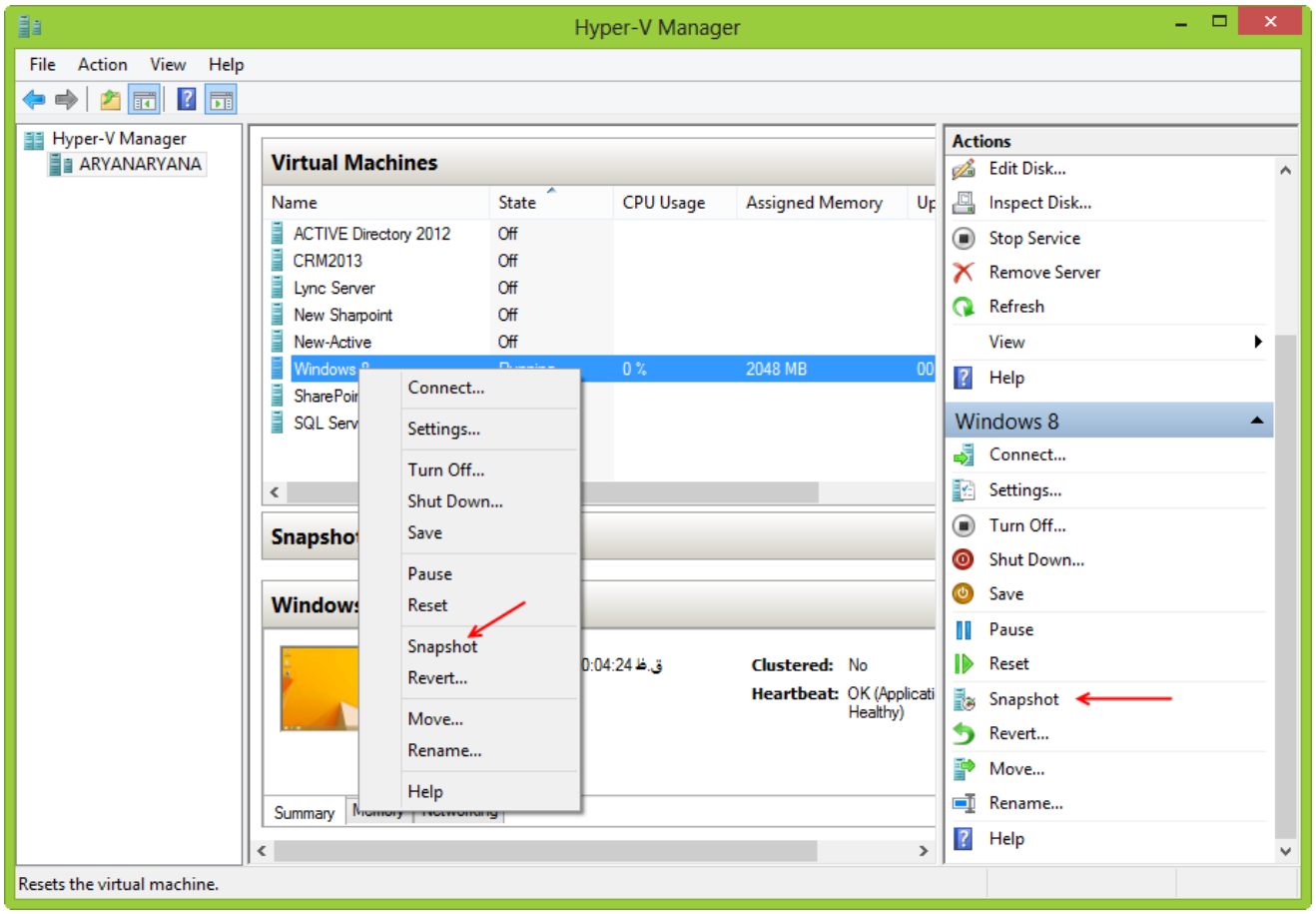


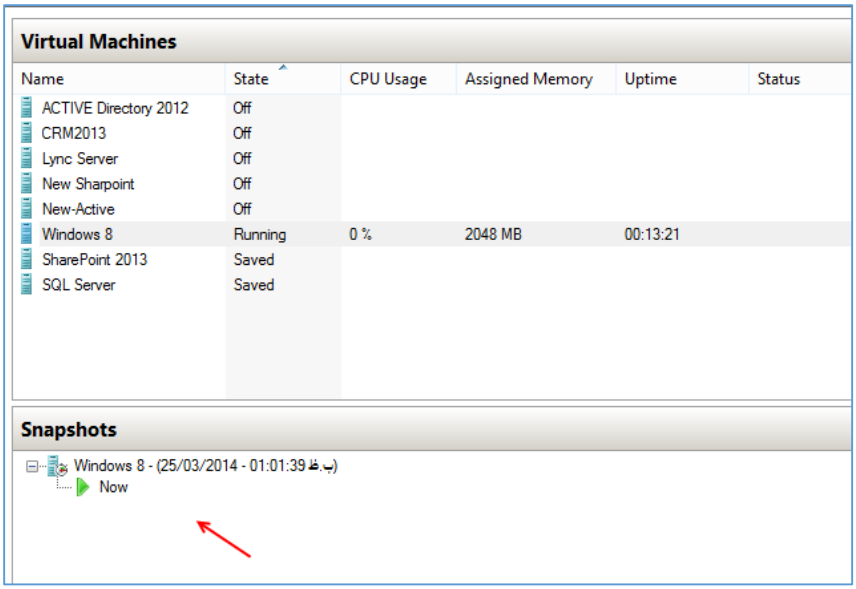
همانطور که در شکل بالا مشاهده می‌کنید، فایل موردنظر از سیستم واقعی در حال کپی شدن در سیستم مجازی می‌باشد که این کار به صورت عکس آن هم صورت می‌پذیرد.

کار با Snapshot در سرویس Hyper-V:

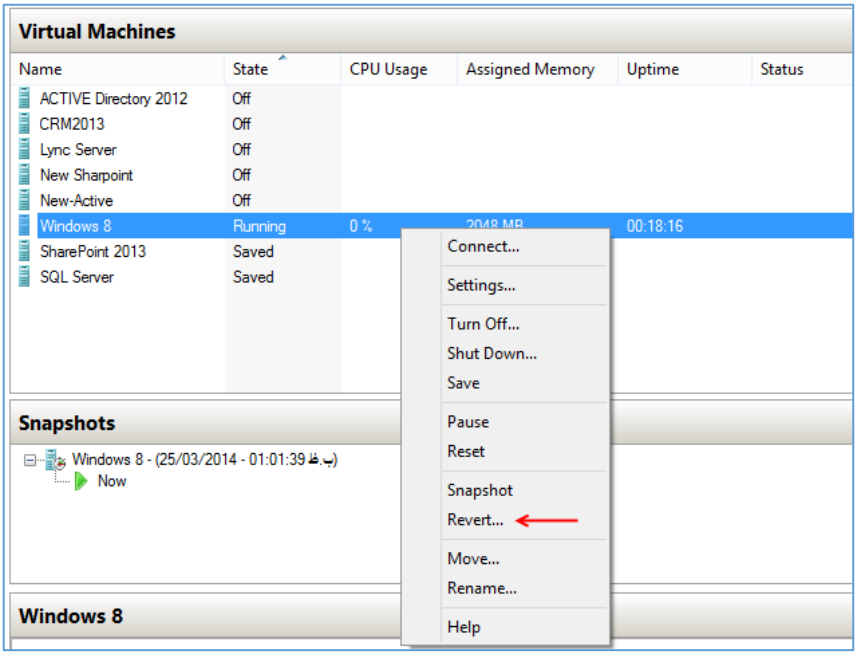
بهترین کاری که در سرویس های مجازی سازی می‌توان انجام داد ایجاد Snapshot از ماشین مجازی موردنظر می‌باشد تا در موقعی که این ماشین دچار مشکل شد Snapshot قبلی آن را جایگزین ماشین مجازی فعلی کنیم. در کل Snapshot یک نسخه از یک ماشین مجازی ایجاد می‌کند و در موقع نیاز می‌توانید این نسخه را جایگزین کنید.

برای انجام این کار به مانند شکل زیر به دو روش می‌توانید به گزینه Snapshot دسترسی داشته باشید، روی ماشین مجازی موردنظر خود کلیک راست کنید و گزینه Snapshot را انتخاب کنید و یا از سمت راست می‌توانید به این گزینه دسترسی داشته باشید.



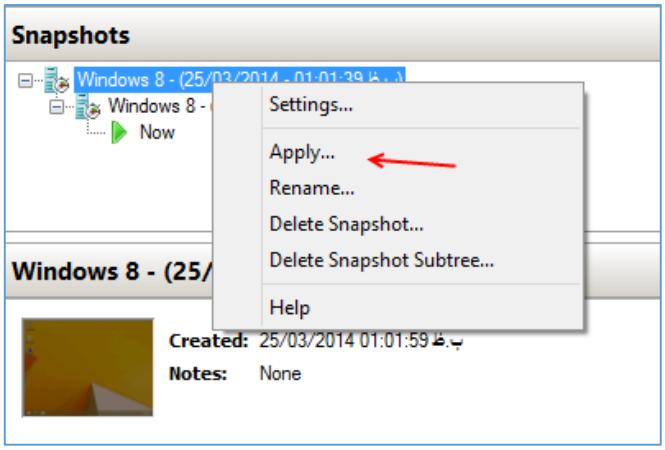


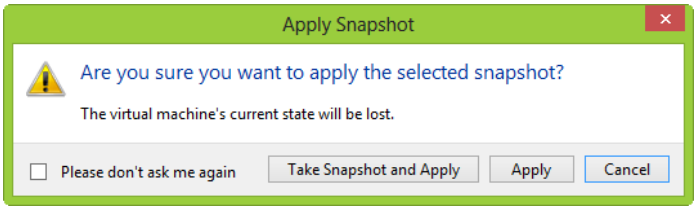
همانطور که در این قسمت مشاهده می-کنید در قسمت Snapshot یک نسخه از آن ایجاد شده است.



برای استفاده از نسخه Snapshot باید بر روی ماشین مجازی موردنظر کلیک راست کنید و گزینه Revert را انتخاب کنید که این عمل باعث می‌شود آخرین نسخه گرفته شده در Snapshot جایگزین سیستم فعلی شود.

اما اگر از سیستم خود چندین نسخه Snapshot تهیه کردید و می‌خواهید یکی از آنها را جایگزین کنید با مانند شکل روبرو در قسمت Snapshots یکی از نسخه های موردنظر خود را انتخاب کنید و بر روی آن کلیک راست کنید و گزینه Apply... را انتخاب کنید تا شکل صفحه بعد ظاهر شود.

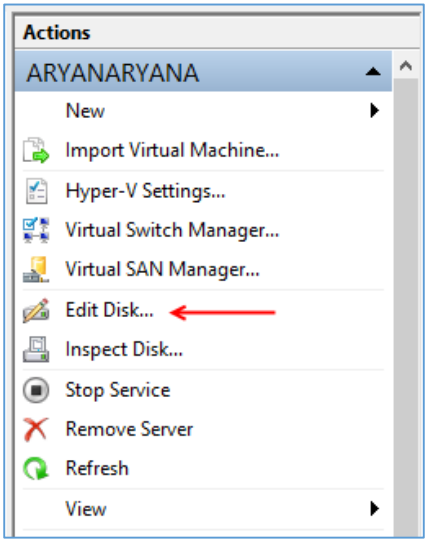




در این شکل اگر بر روی Take Snapshot and Apply کلیک کنید از سیستم حال حاضر یک نسخه تهیه می‌کند و بعد نسخه موردنظر شما را جایگزین می‌کند ولی اگر بر روی Apply کلیک کنید نسخه Snapshot موردنظر جایگزین می‌شود.

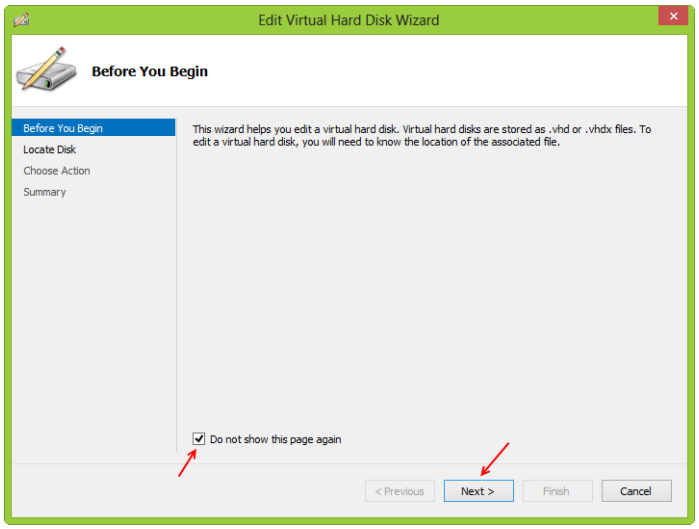
چگونه فضای هار دیسک را بعد از راه‌اندازی ماشین مجازی تغییر دهیم:

در زمان ایجاد ماشین مجازی، مقدار هارد دیسک آن را مشخص می‌کنید که به صورت پیش فرض بر روی 127 گیگابات قرار دارد که می‌توانید این مقدار را تغییر دهید و ماشین مجازی موردنظر خود را ایجاد کنید. ولی زمانی که ماشین مجازی را ایجاد می‌کنید، به روش معمول نمی‌توانید این مقدار را تغییر دهید.

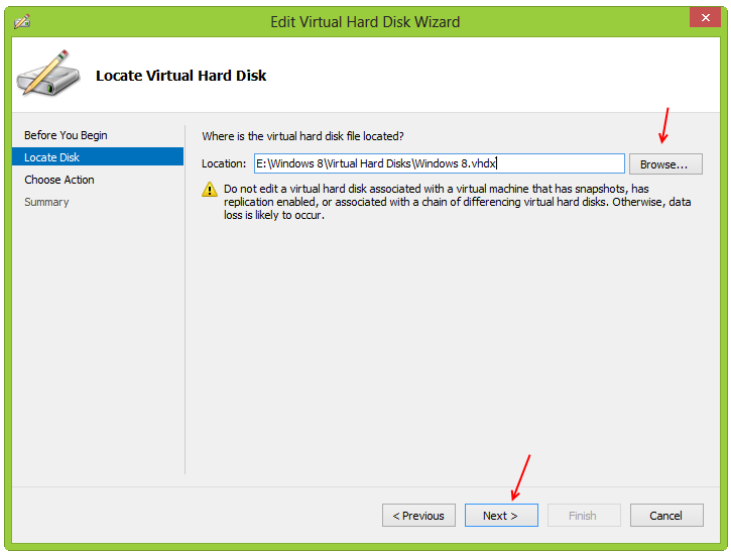


در سرویس Hyper-v این قابلیت وجود دارد که مقدار هارد دیسک مربوط به ماشین مجازی موردنظر را تغییر دهید.

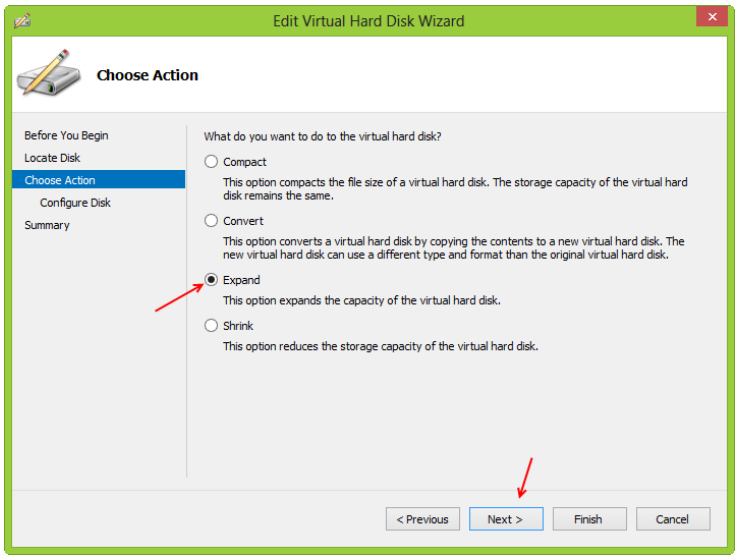
برای شروع وارد سرویس Hyper-v شوید و از سمت راست در قسمت Actions بر روی Edit Disk کلیک کنید تا شکل بعد ظاهر شود.



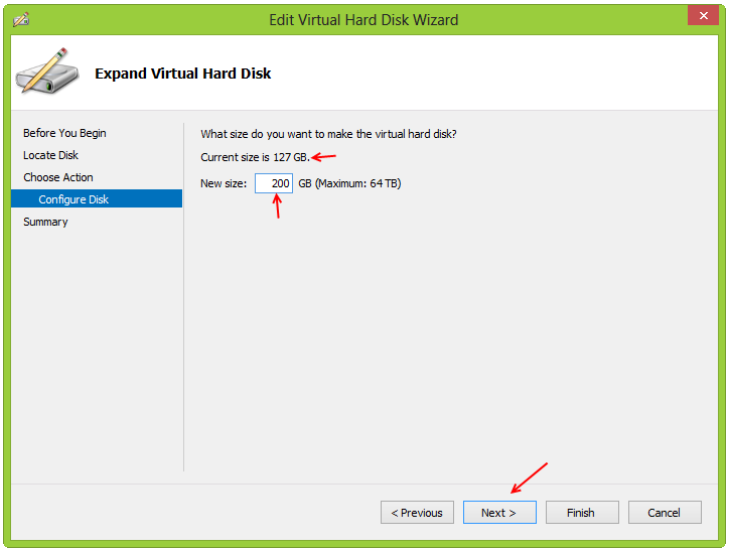
در این صفحه تیک گزینه موردنظر را زده و بر روی Next کلیک کنید.



در این قسمت باید هارد دیسک مجازی مربوط به ماشین مجازی موردنظر را از طریق دکمه Browse... به سرویس موردنظر معرفی کنید که در اینجا هارد دیسک مربوط به ویندوز 8 را که قبلاً ایجاد کرده بودیم را به آن معرفی کردیم، بعد از این کار بر روی Next کلیک کنید.

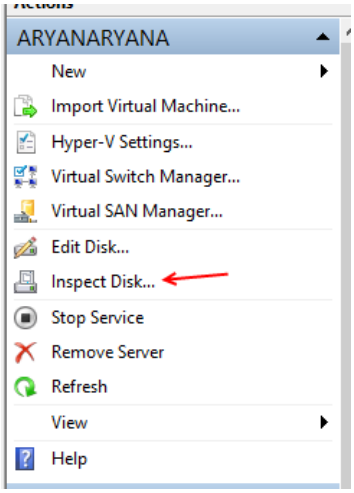


در این قسمت گزینه Expand را انتخاب و بر روی Next کلیک کنید.

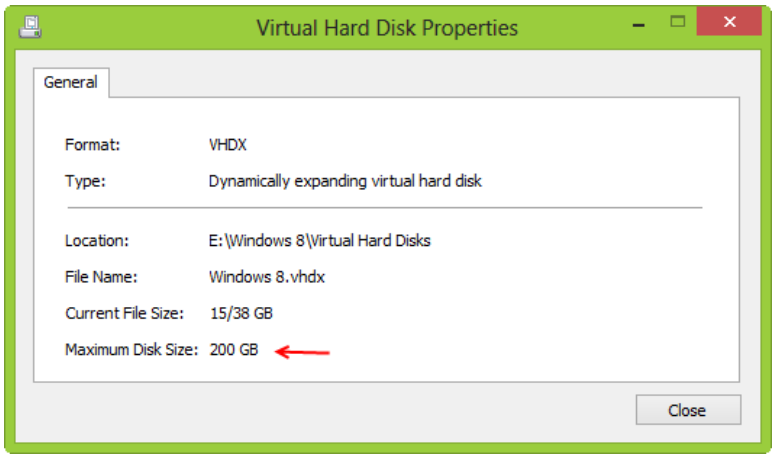


همانطور که در این قسمت مشاهده می‌کنید مقدار هارد موردنظر برای این ماشین 127 گیگابایت می‌باشد که آن را به 200 گیگابایت تغییر دادیم، بعد از این کار بر روی Next کلیک کنیدو بعد بر روی Finish کلیک کنید تا ظرفیت هارد دیسک به 200 گیگابایت تغییر کند.

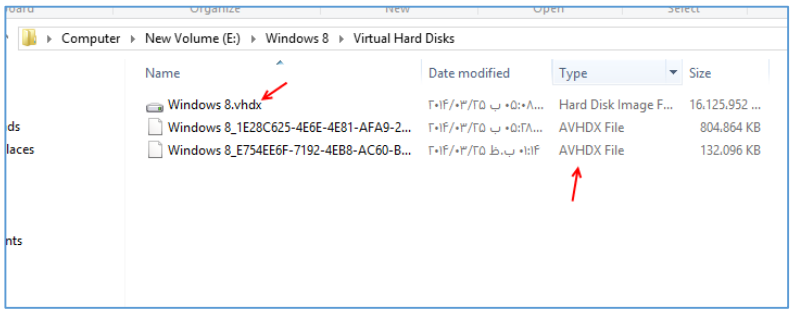
نکته: در موقع انجام این کار ماشین مجازی باید خاموش باشد تا تغییرات بتواند به درستی اعمال شود.



برای اینکه متوجه شویم مقدار ظرفیت دیسک تغییر کرده است یا نه وارد سرویس Hyper-V می‌شویم و از سمت راست و در قسمت Actions بر روی Inspect Disk کلیک می‌کنیم، بعد از باز شدن صفحه آدرس هارد دیسک موردنظر خود را به آن معرفی می‌کنیم تا شکلی شبیه به شکل بعد ظاهر شود.



همانطور که در تصویر روبرو مشاهده می‌کنید، می‌توانید مقدار هارد دیسک مربوطه را مشاهده کنید.

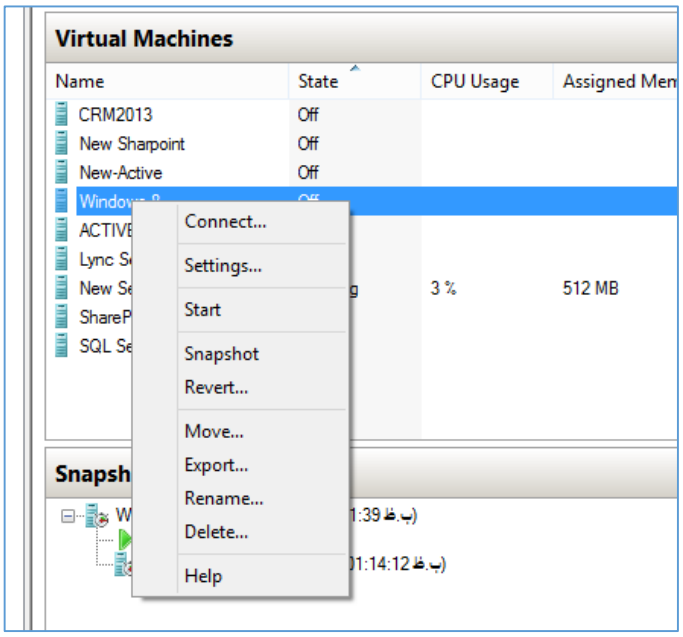


نکته: اگر به پوشه مربوط به هارد دیسک موردنظر خود در سیستم اصلی مراجعه کنید متوجه چند فایل به مانند شکل روبرو می‌شوید، توجه کنید که فایل با پسوند vhdx فایل اصلی ما می‌باشد که مقدار کل فضا به آن اختصاص داده شده و فایل های دیگر با پسوند AVHDX فایل هایی هستند که تغییرات مربوط به ماشین مجازی در آنها ذخیره می‌شود این کار به این خاطر می‌باشد، زمانی که یک هار دیسک مجازی با ظرفیت 200 گیگابایت ایجاد می‌شود در همان لحظه کل فضای هارد دیسک اصلی مان رادر بر نخواهد گرفت بلکه با استفاده از فایل هایی با پسوند AVHDX به مرور زمان فضای هارد دیسک پر خواهد شد تا به ظرفیت 200 گیگابایت برسد، امیدوارم متوجه شده باشید اگر هم متوجه نشدید با من در تماس باشید.

بررسی جزئیات سرویس Hyper-V:

در این قسمت به برخی از ریزه کاری‌های این سرویس می‌پردازیم تا آموزش این سرویس به صورت کامل صورت گیرد.

زمانی که روی یک ماشین مجازی کلیک راست می‌کنید یک منو باز می‌شود که چندین گزینه مختلف را در اختیار ما قرار می‌دهد، اولین گزینه از پائین Help می‌باشد که یکسری اطلاعات در مورد سرویس Hyper-V در اختیار ما قرار می‌دهد، گزینه بعدی Delete می‌باشد که ماشین مجازی موردنظر را حذف خواهد کرد. اگر بر روی Rename کلیک کنید می‌توانید نام ماشین مجازی خود را تغییر دهید. اگر بر روی Export کلیک کنید یک پنجره باز خواهد شد که می‌توانید آدرس موردنظر خود راوارد کنید تا ماشین مجازی به صورت کامل در آدرس موردنظر Export شود این در حالی است که جایگاه قبلی ماشین مجازی تغییر نمی‌کند، این کار همانند Copy و Past کردن است. گزینه Move برای انتقال کامل یک ماشین مجازی از آدرس فعلی به آدرس جدید که آدرس قدیمی آن حذف خواهد شد. گزینه های Revert, Snapshot در قسمت های قبل توضیح داده شده است. گزینه بعدی Start می‌باشد که برای اجرا کردن ماشین مجازی موردنظر می‌باشد.



در قسمت بعد گزینه Settings وجود دارد که تنظیمات و اطلاعات مربوط به سخت افزار ماشین مجازی موردنظر را در اختیار ما قرار می‌دهد که با هم این قسمت را بررسی کردیم.

با کلیک بر روی Connect... کنسول مدیریتی ماشین مجازی موردنظر اجرا می‌شود که شما می‌توانید وارد سیستم عامل ماشین موردنظر خود شوید.

کار با کلید های ترکیبی:

سرویس Hyper-V به مانند سرویس‌ها و نرم‌افزارهای دیگر از کلید های ترکیبی مختلفی برای خود استفاده می‌کند.

Ctrl + Alt + Break: با فشردن این کلید ترکیبی صفحه موردنظر به صورت Full Screen تغییر حالت می‌دهید و کل صفحه نمایش را پر خواهد کرد، واگر دوباره روی آن کلیک کنید به حالت اولبه خود بر می‌گردد.

Ctrl + Alt+ End: این کلید همان کلید Ctrl + Alt + Delete در ویندوز واقعی می‌باشد.

Ctrl + D: برای خاموش کردن ماشین مجازی استفاده می‌شود.

Ctrl + S: برای start کردن ماشین مجازی به کار می‌رود.

Ctrl + A: برای Save کردن ماشین مجازی به کار خواهد رفت.

Ctrl + N: برای گرفتن Snapshot از ماشین مجازی به کار می‌رود.

Ctrl + E: برای Restore کردن آخرین Snapshot به کار می‌رود.

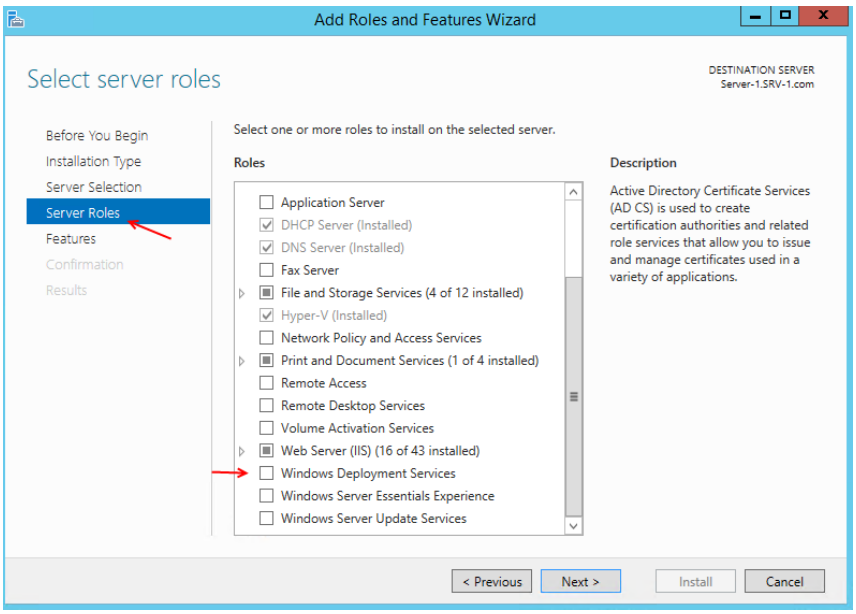
Ctrl + O: برای نمایش Setting سرویس Hyper-V به کار خواهد رفت.

کار با سرویس Windows Deployment(نصب ویندوز از طریق شبکه)

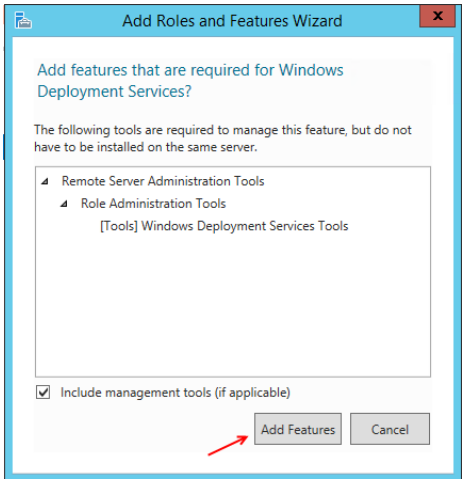
جالب ترین سرویسی که مایکروسافت در ویندوز سرور خود ارئه داده، سرویس Windows Deployment می‌باشد که با انجام تنظیمات لازم روی این سرویس می‌توانید بدون اینکه بر روی تک تک کلاینت ها حضور داشته باشید، ویندوز را از طریق شبکه نصب کنید که برای مدیران شبکه کار پر اهمیتی است.

در این قسمت با هم این سرویس را نصب می‌کنیم و نحوه کارکرد آن را با هم بررسی می‌کنیم.

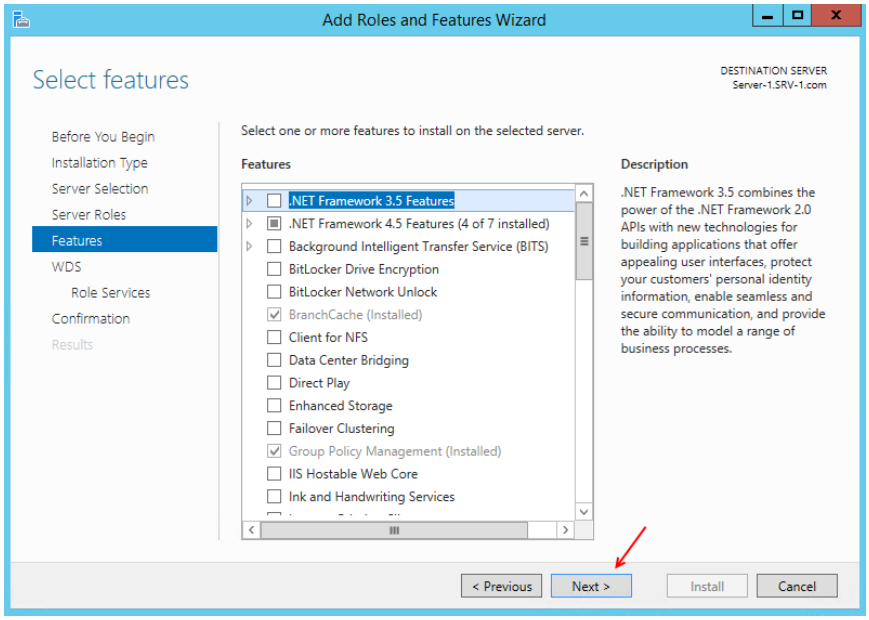
برای شروع وارد Server Manager شوید و بر روی Add Roles and Feature کلیک کنید.



از سمت چپ بر روی Server Roles کلیک کنید و از لیست Roles گزینه Windows Deployment Services را انتخاب کنید تا شکل بعد ظاهر شود.

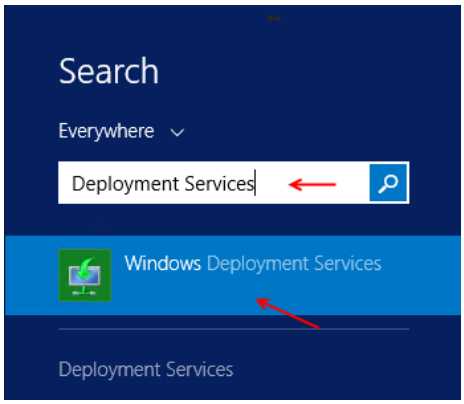


در صفحه روبرو بر روی Add Features کلیک کنید و بعد بر روی Next کلیک کنید.

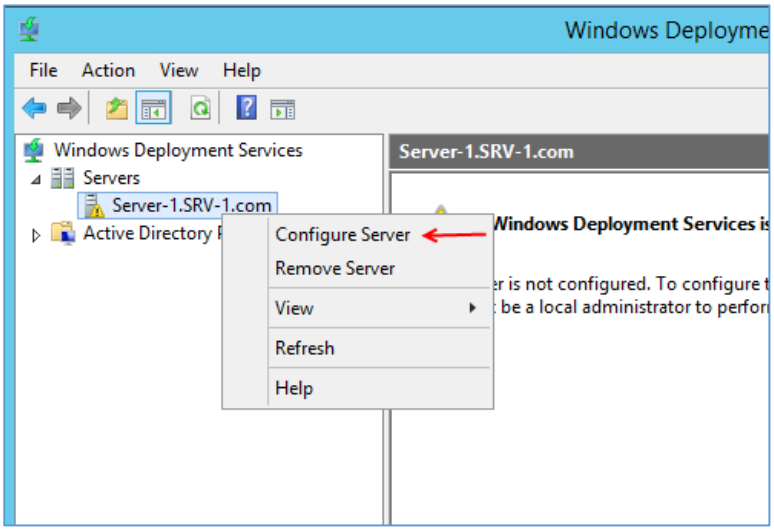


در این صفحه به گزینه ای دست نزنید و بر روی Next کلیک کنید.

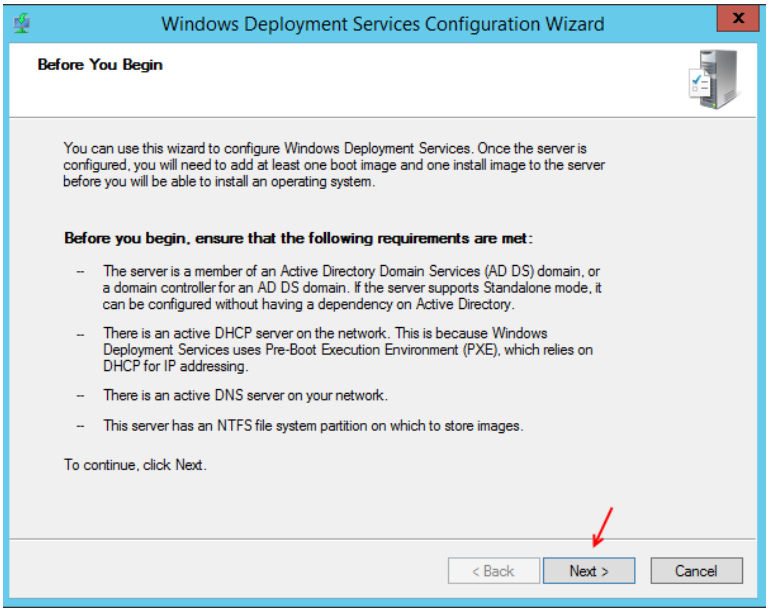
در صفحات بعد هم بر روی Next کلیک کنید و در صفحه آخر هم بر روی install کلیک کنید تا سرویس موردنظر نصب شود.



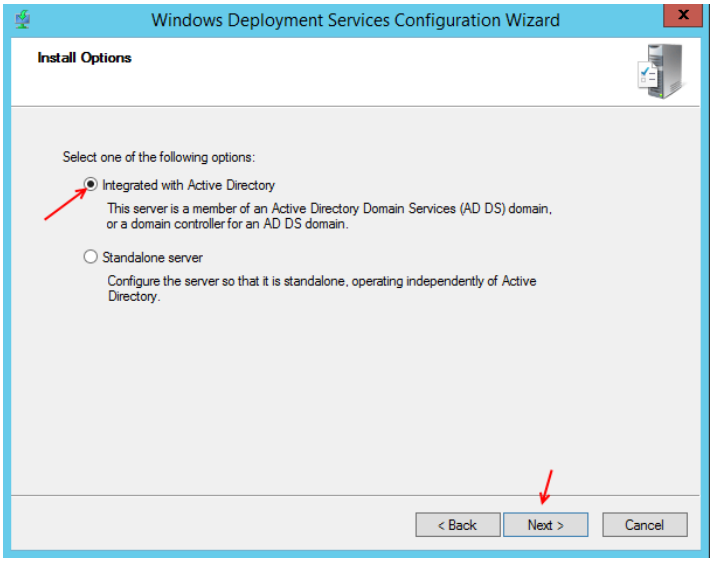
بعد از نصب وارد Search شوید و جمله Deployment Service را وارد و بعد سرویس موردنظر را اجرا کنید، سعی کنید با کلیک راست کردن روی سرویس موردنظر آن را وارد Start و یا وارد Taskbar کنید.



بعد از ورود به سرویس موردنظر وارد قسمت Servers شوید و بر روی نام سرور خود کلیک راست کنید و گزینه Configure Server را انتخاب کنید تا تنظیمات مربوط به این سرویس را انجام دهیم.

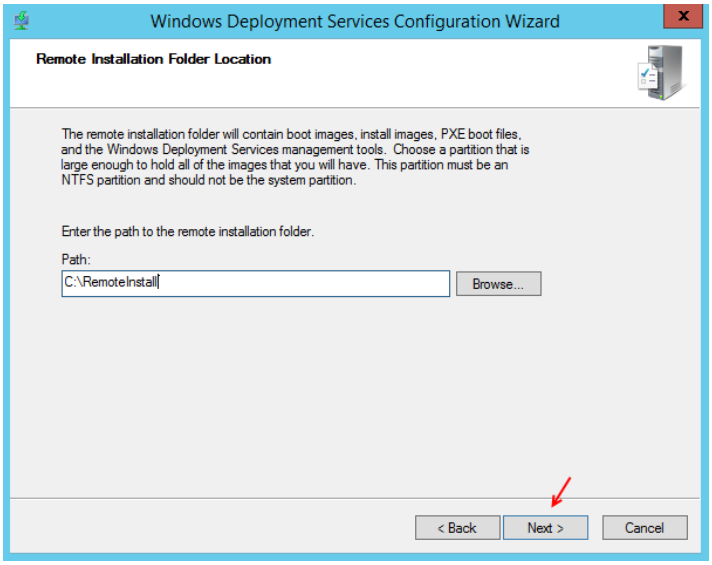


در این صفحه بر روی next کلیک کنید.



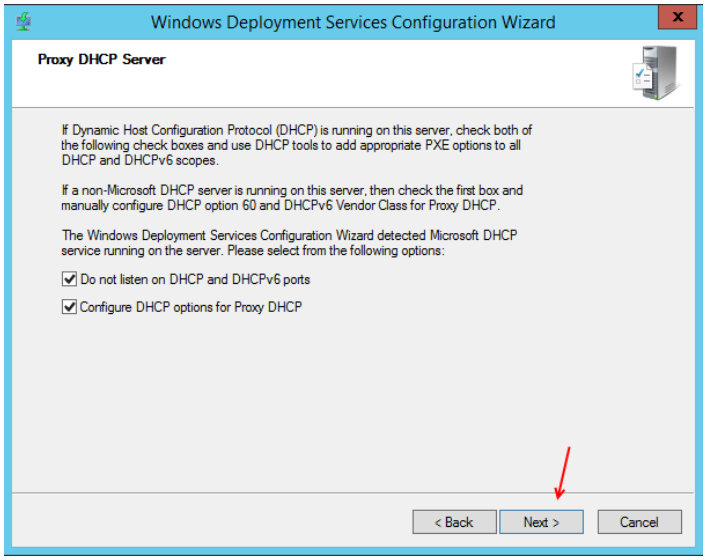
در این صفحه گزینه Integrated with Active Directory را انتخاب کنید تا سرویس موردنظر با Active خود را هماهنگ کند.

بر روی Next کلیک کنید.

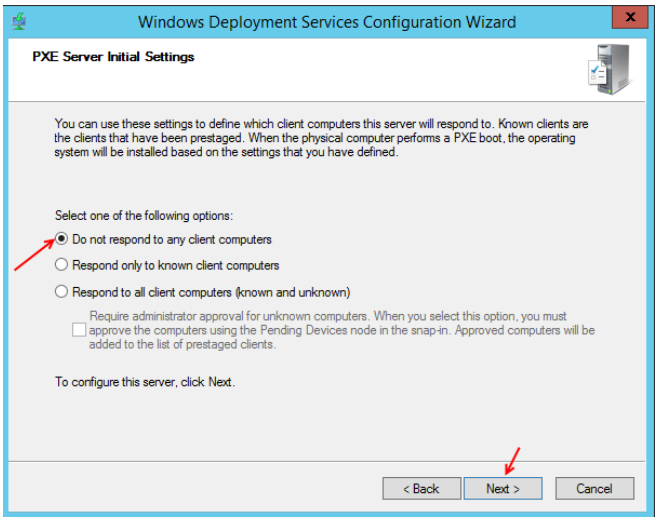


در این صفحه باید آدرسی را وارد کنید تا اطلاعاتی مانند ویندوز در آدرس موردنظر کپی شود تا کلاینت‌ها بتوانند از این آدرس استفاده کنند، البته این آدر Share خواهد شد.

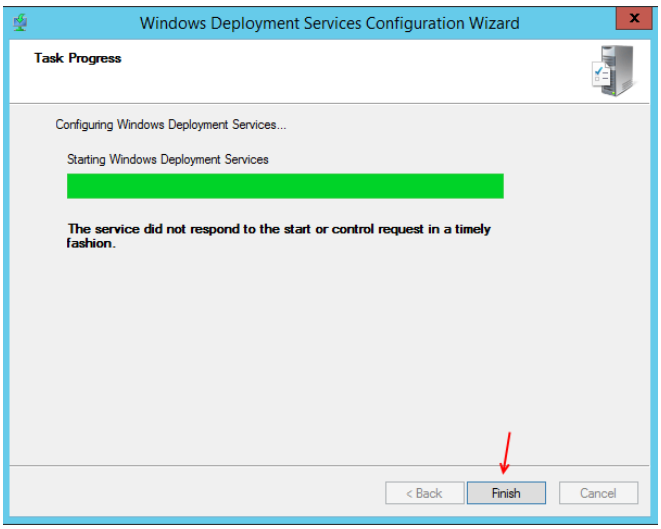
بعد از کلیک بر روی Next پنجره‌ای باز می‌شود که به این نکته اشاره دارد که درایوی که انتخاب کردید درایو System می‌باشد یعنی ویندوز شما روی آن نصب شده است، بهتر است درایو دیگری را انتخاب کنید تا امنیت اطلاعات و کیفیت افزایش پیدا کند.



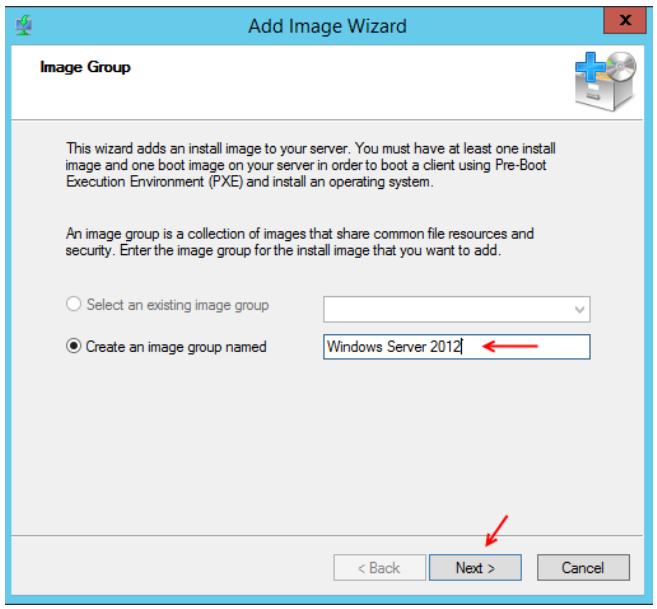
در این قسمت بر روی Next کلیک کنید.



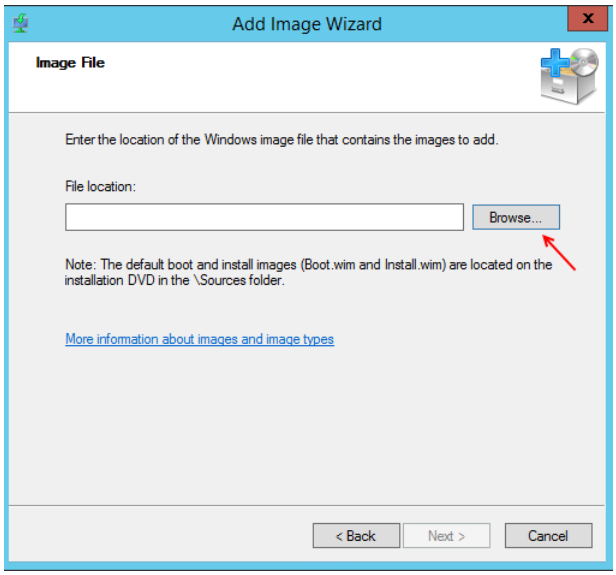
در این صفحه گزینه اول را انتخاب کنید و بر روی Next کلیک کنید.



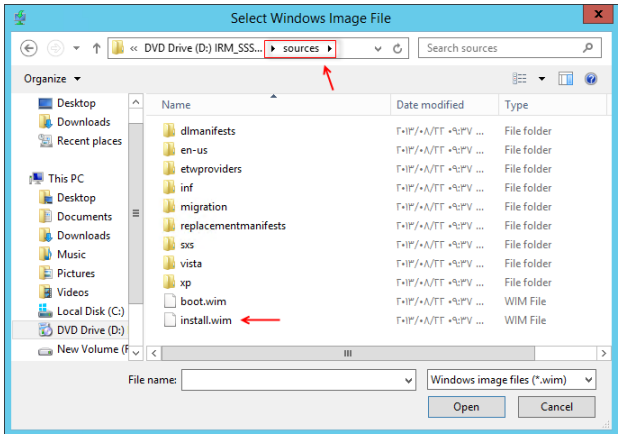
همانطور که مشاهده می‌کنید عملیات با موفقیت انجام شده است بر روی Finish کلیک کنید.



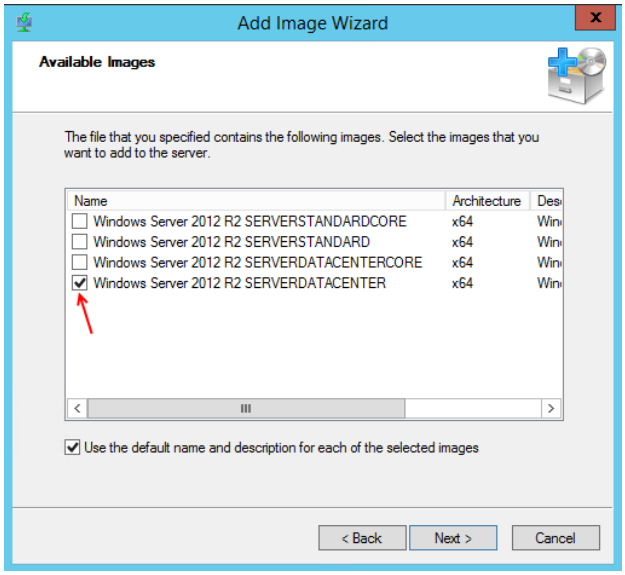
در این قسمت نام Image خود را وارد کنید، مثلاً در اینجا Windows Server 2012 وارد شده است. بر روی Next کلیک کنید.



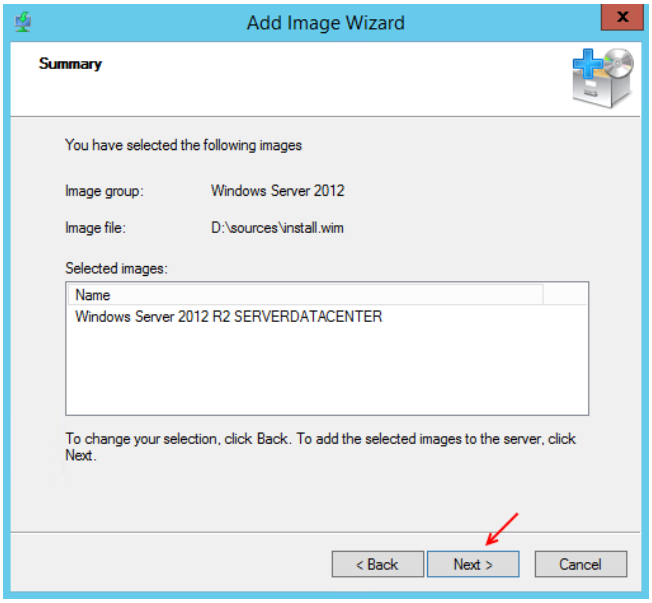
در این صفحه باید وارد DVD ویندوز خود شویم و فایل Install.wim را به آن معرفی کنیم برای این کار بر روی Browse کلیک کنید.



در این قسمت باید وارد پوشه Source از ویندوز سرور 2012 شوید و فایل install.wim را انتخاب کنید.

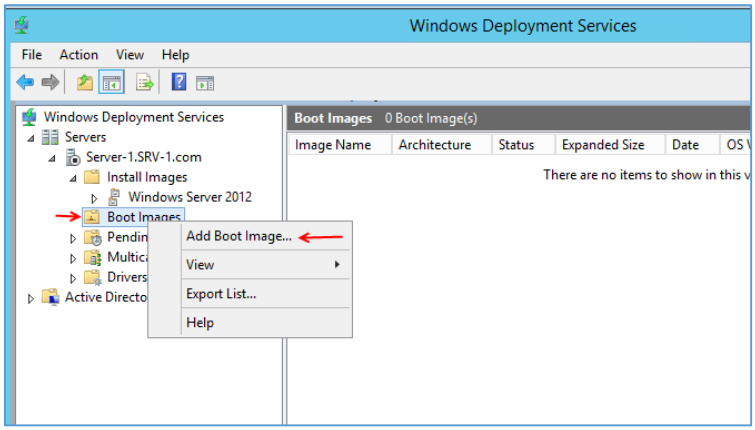


در این قسمت لیست ورژن های مختلف ویندوز سرور نمایش داده می‌شوید که می‌توانید یکی یا همه آنها را انتخاب کنید. بر روی Next کلیک کنید.

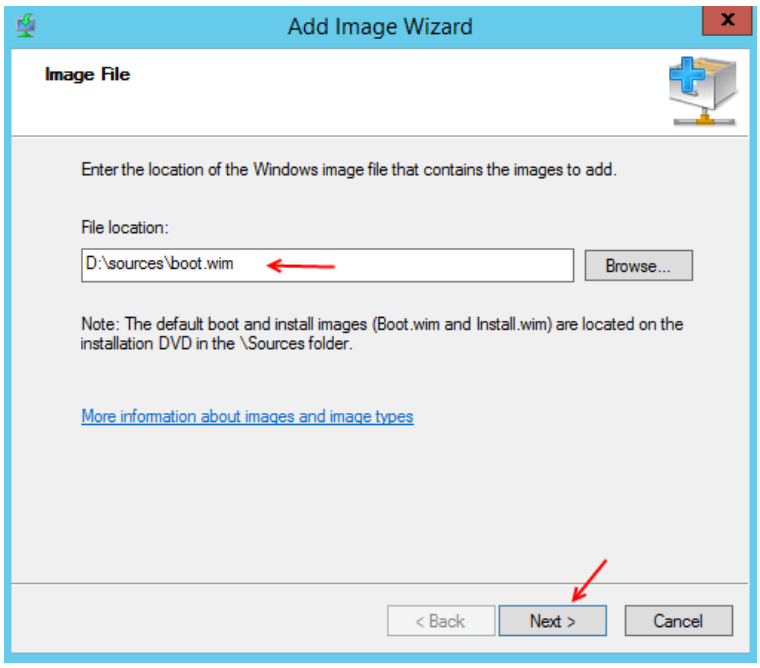


در این قسمت بر روی Next کلیک کنید.

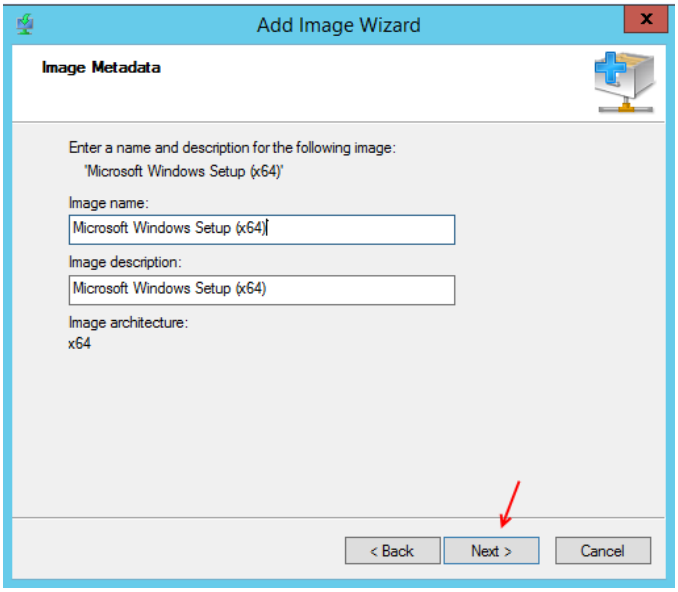
بعد از کلیک بر روی Next کار ایجاد Image از ویندوز سرور 2012 شروع می‌شود و تا چند دقیقه زمان خواهد برد.



بعد از ایجاد Install Image نوبت به نصب Boot Image می‌رسد برای این کار به مانند شکل روبرو بر روی Boot image کلیک راست کنید و گزینه Add Boot images را انتخاب کنید.

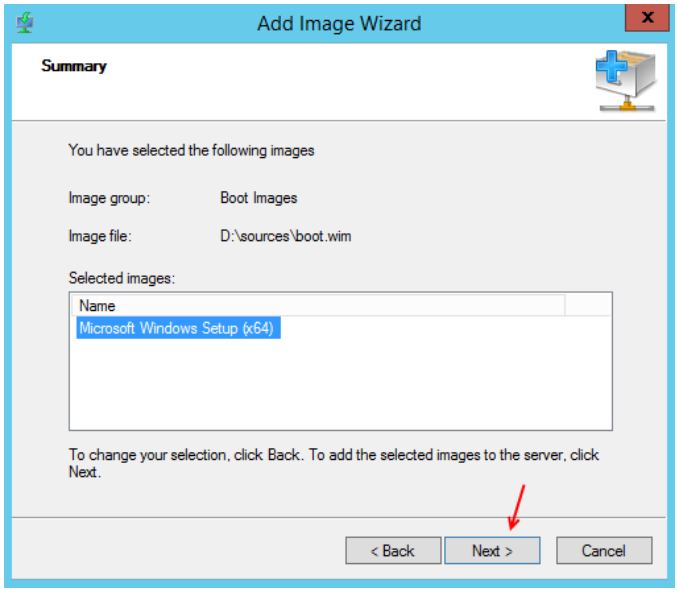


در این صفحه باید آدرس Boot.wim مربوط به ویندوز موردنظر را وارد کنید، بر روی Next کلیک کنید.



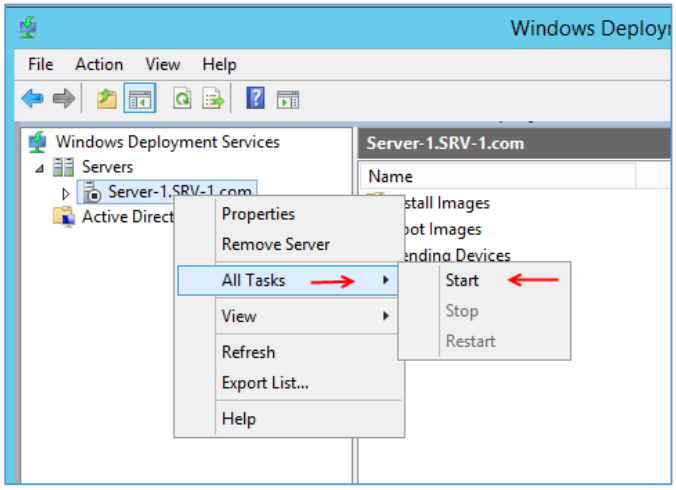
در این قسمت می‌توانید نام وتوضیحات موردنظر خود را وارد کنید.

بر روی Next کلیک کنید.

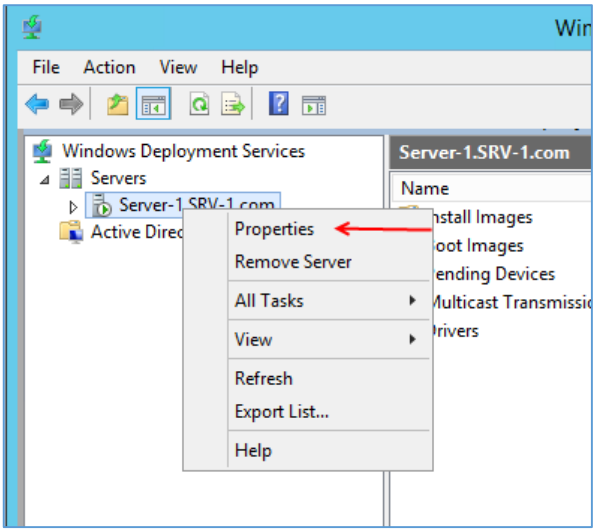


بر روی Next کلیک کنید.

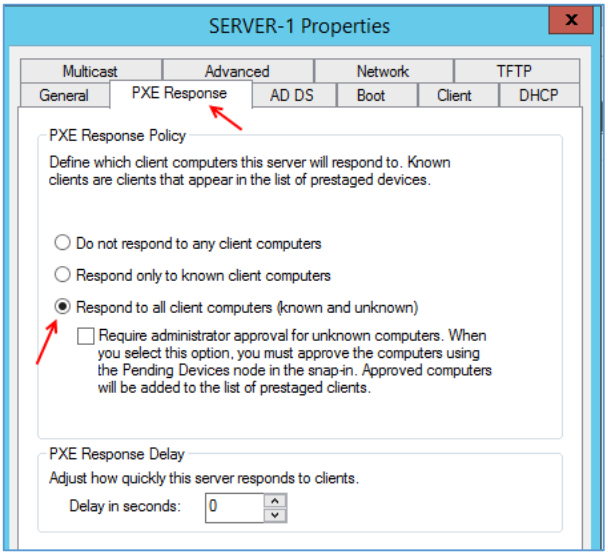
بعد از ایجاد image برروی Finish کلیک کنید.



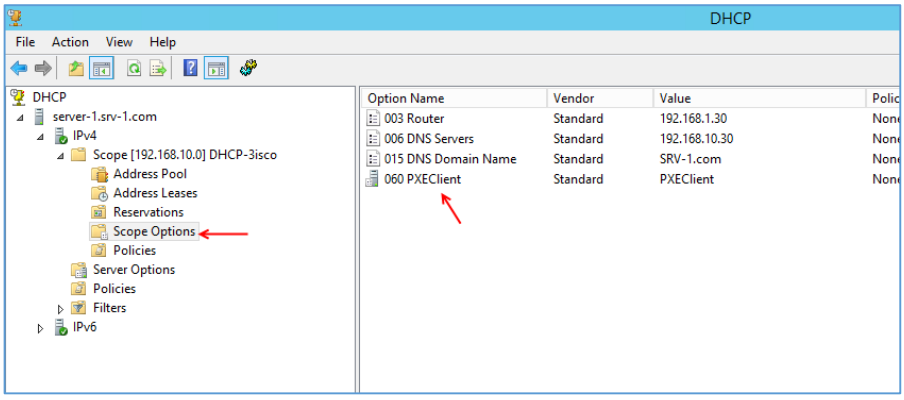
بعد از ایجاد هر دو Image موردنظر بر روی سرور اصلی کلیک راست کنید و از قسمت All Tasks گزینه Start را انتخاب کنید تا سرویس موردنظر فعال شود.



بعد از اینکه سرویس را Start کردیم بر روی نام سرور کلیک راست می‌کنیم و گزینه Properties را انتخاب می‌کنیم.



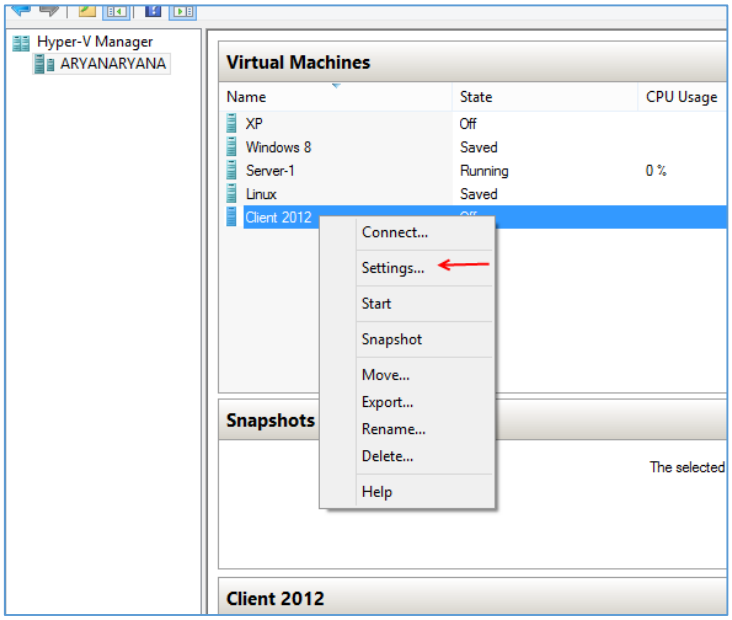
در این صفحه وارد تب PXE Response شوید و گزینه Respond to all Client Computer را انتخاب کنید تا کلاینت‌ها زمانی که روشن می‌شوند از طریق سرویس DHCP بتوانند به سرویس Deployment متصل شوند و ویندوز را اجرا کنند.



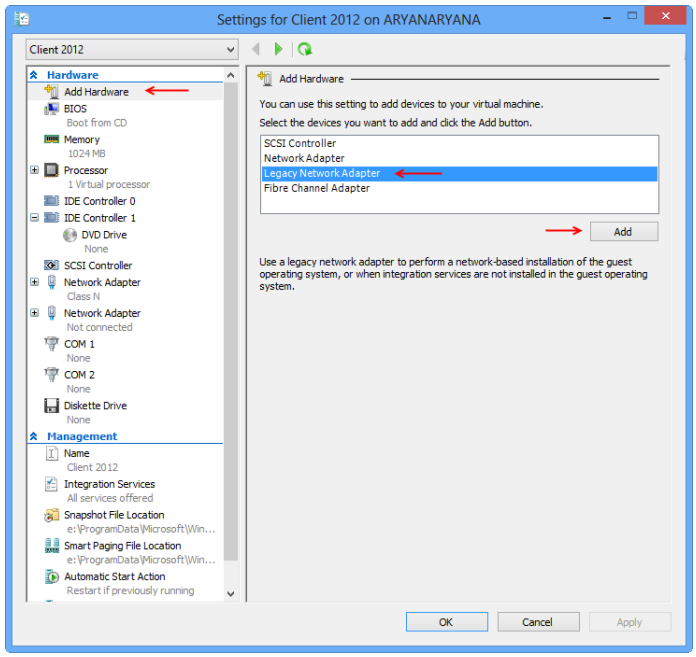
بعد از اتمام کار به سرویس DHCP نگاهی می‌اندازیم، اگر به قسمت Scope Options مراجعه کنید، گزینه ای را با نامPXEClient ایجاد شده است که مربوط به سرویس Deployment می‌باشد.

نکته مهم: برای استفاده از قابلیت سرویس Deployment حتماً باید سرویس DHCP، Active Directory و DNS را قبل از آن نصب کنید که در این کتاب این کار قبل از آن انجام شده است.

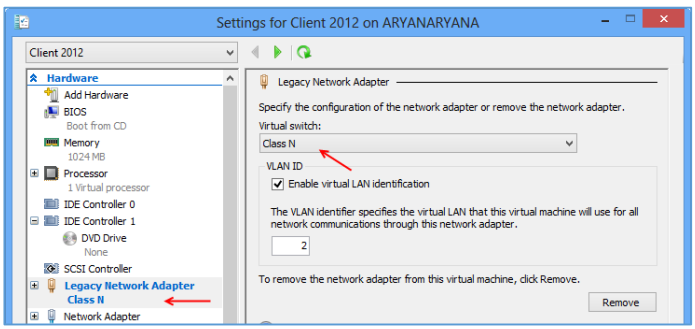
حالا می‌خواهیم، از طریق سرویس Hyper-V یک ماشین مجازی ایجاد کنیم که از طریق شبکه ویندوز آن را نصب کنیم.

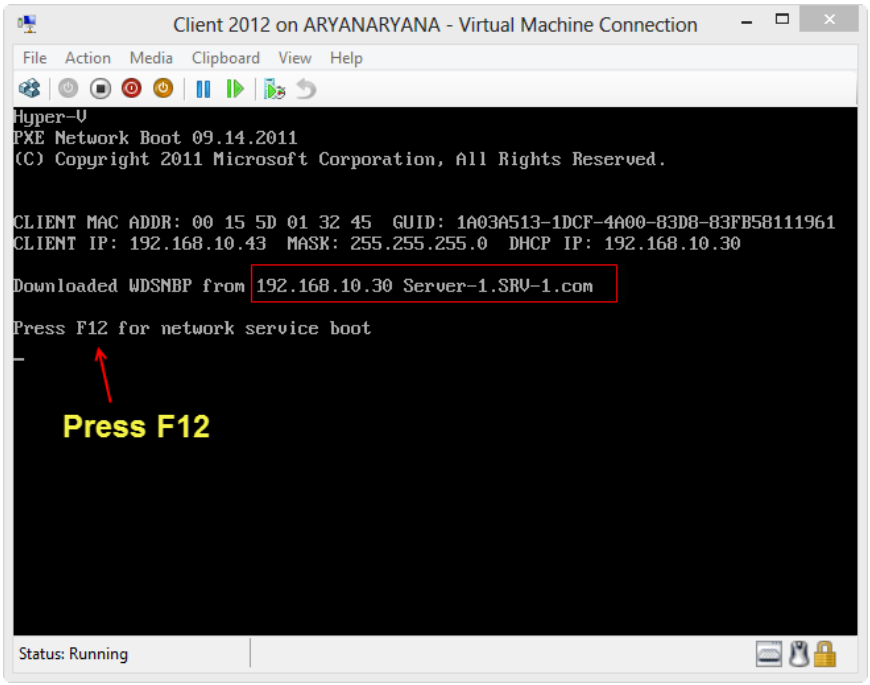


در درس قبلی نحوه ایجاد ماشین مجازی در سرویس Hyper-V را با هم بررسی کردیم، بعد از ایجاد ماشین مجازی به مانند شکل روبرو بر روی آن کلیک راست کنید و گزینه Settings را انتخاب کنید.



در این صفحه از سمت چپ اولین گزینه یعنی Add Hardware را انتخاب کنید و در لیست موردنظر گزینه Legacy Network Adapter را انتخاب و بر روی Add کلیک کنید تا کارت شبکه موردنظر که مخصوص این کار است و سرویس DHCP را پشتیبانی می‌کند ایجاد شود، توجه داشته باشید این سرویس Hyper-V بر روی ویندوز 8 قرار دارد و سرویس Hyper-V بر روی ویندوز سرور این گزینه را به صورت پیش فرض در خود دارد و نیاز به اضافه کردن آن نیست، بر روی ok کلیک کنیدو به مانند شکل روبرو کارت شبکه موردنظر را برای کارت شبکه Legancy انتخاب کنید، توجه داشته باشید کارت شبکه موردنظر باید به سرور متصل باشد.

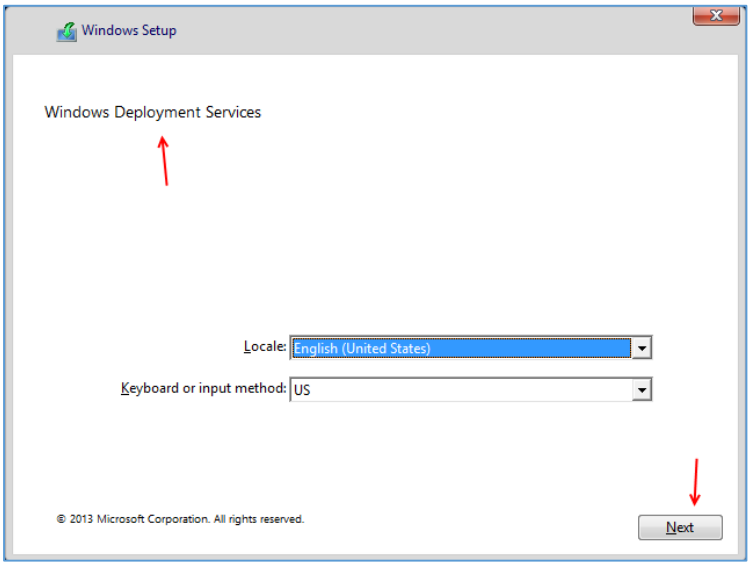




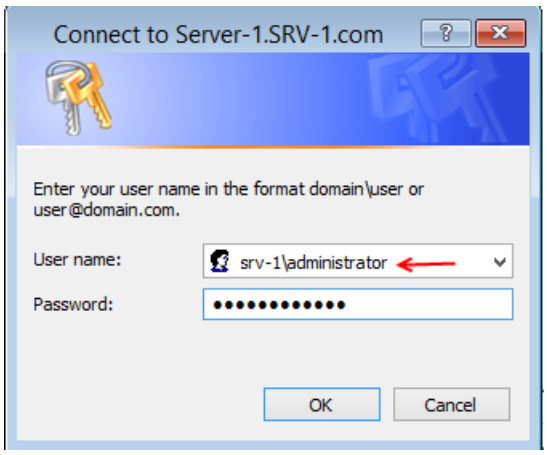
بعد ورود به ماشین مجازی آن را روشن می‌کنیم، زمانی که ماشین مجازی موردنظر را روشن کنید سرویس DHCP فعال می‌شود و از طریق کارت شبکه موردنظر PXE مربوط به سرویس Deployment را پیدا می‌کند و با کلیک بر روی کلید F12 می‌توانید به قسمت نصب ویندوز بروید و ویندوز خود را از طریق شبکه نصب کنید.

همانطور که مشاهده می‌کنید سیستم از طریق شبکه در حال دریافت فایل از سرور 192.168.10.30 می‌باشد.

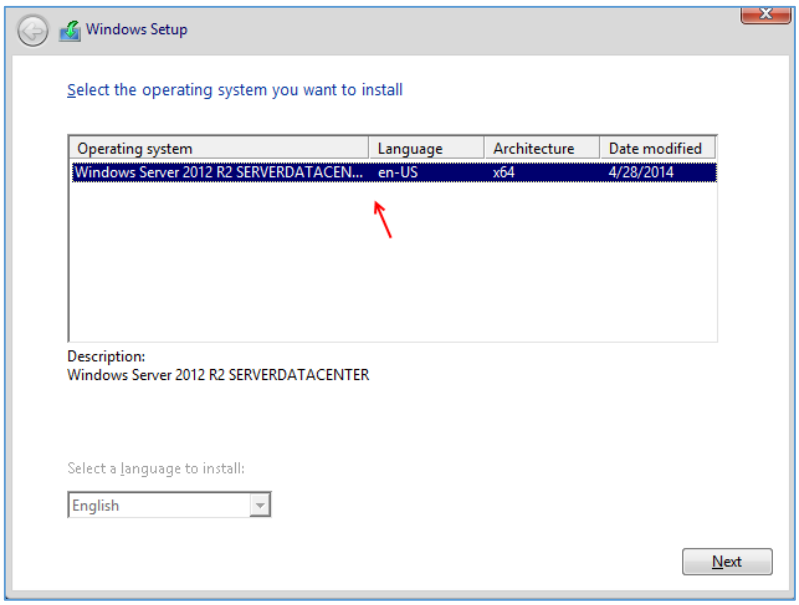
نکته: در سیستم های واقعی برای متصل شدن به سرویس DHCP باید وارد منوی Boot شوید و Network را انتخاب کنید تا بتوانید به شبکه متصل شوید.



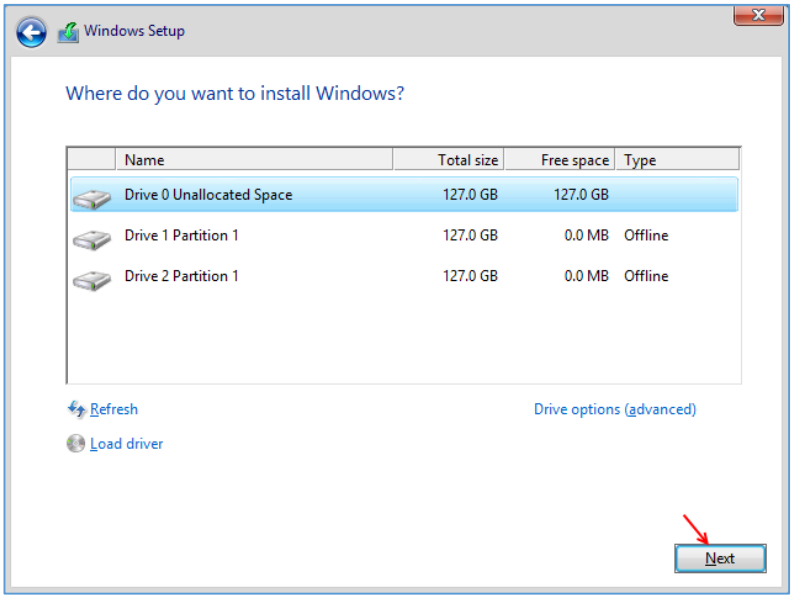
همانطور که در این شکل مشاهده می‌کنید پنجره نصب ویندوز ظاهر شده است که نشان می‌دهد این ویندوز ازطریق Windows Deployment Services فعال شده است برای ادامه بر روی Next کلیک کنید.



در این قسمت، باید نام کاربری و رمز عبور مدیر شبکه را وارد کنیم، یعنی مدیر سرور اصلی و بعد بر روی ok کلیک کنید.

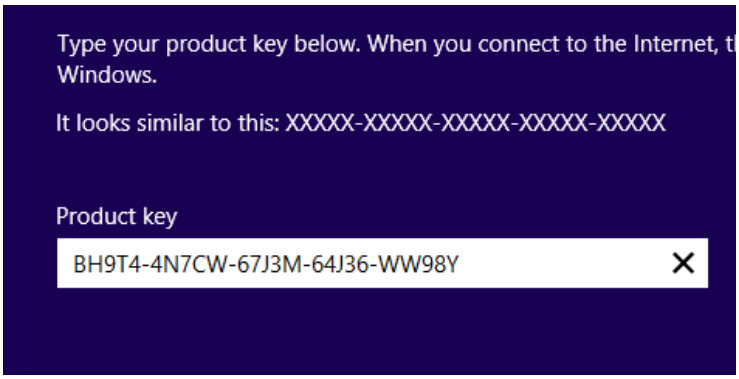


در این صفحه بین 4 ورژنی که برای نصب ویندوز وجود داشت، فقط یک ورژن آن در دسترس است به این دلیل که قبلاً در هنگام تعریف Install Image در سرویس Deployment یک ورژن انتخاب شده است، بر روی Next کلیک کنید.



در این قسمت هارد دیسک موردنظر خود را انتخاب و بر روی Next کلیک کنید تا نصب ویندوز آغاز شود.

بعد از نصب ویندوز این صفحه ظاهر می‌شود که منطقه جغرافیایی و زبان موردنظر خود را انتخاب و بر روی Next کلیک کنید.

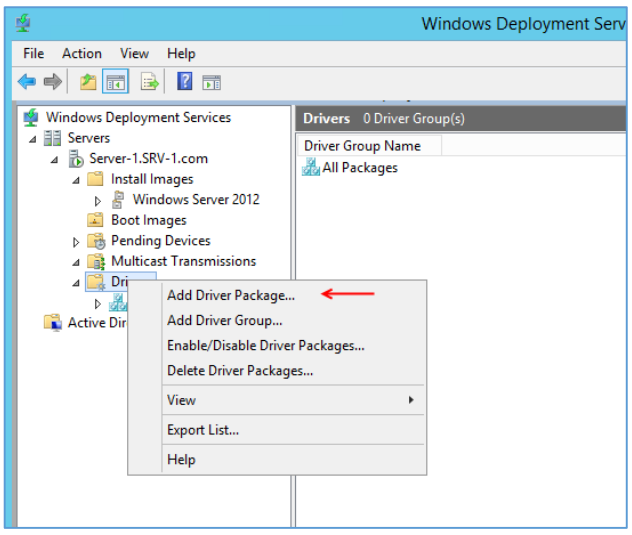


در این قسمت، شماره سریال ویندوز را وارد و بر روی Next کلیک کنید.

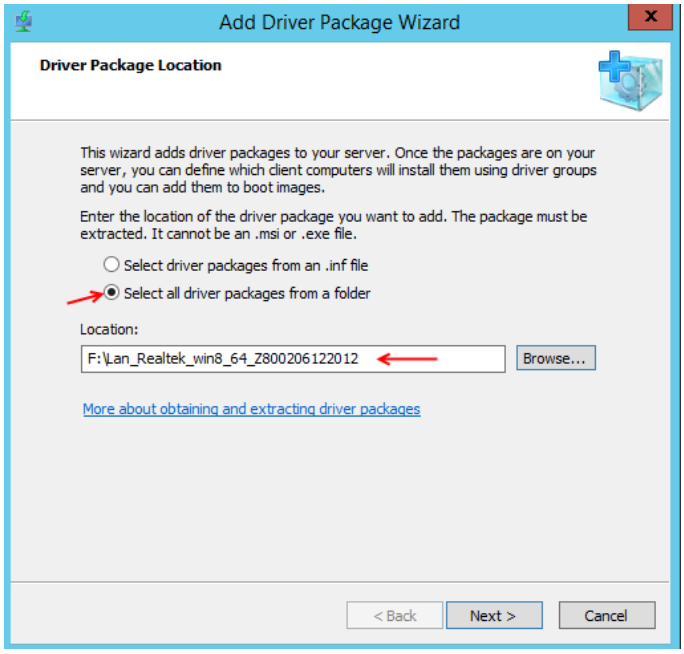
در صفحه بعد بر روی I accept کلیک کنید و در صفحه آخر رمز عبور دلخواه خود را برای ورود به ویندوز را وارد کنید.

به این ترتیب توانستیم ویندوز را از طریق شبکه بر روی کلاینت موردنظر نصب کنیم.

نکته: تمام کلاینت هایی که به این صورت ویندوز روی آنها نصب می‌شود به صورت خودکار عضو دومین موردنظر می‌شوند و دیگر لازم نیست به خودتان زحمت بدید و بروی تک تک کلاینت ها عملیات Join به دومین را انجام دهید.

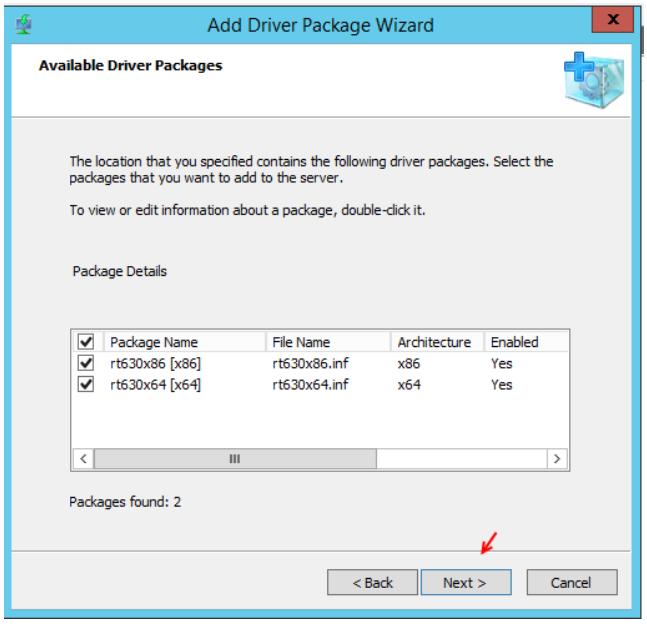


بعد از نصب ویندوز از طریق شبکه شاید شما نیاز داشته باشید که درایورهای مربوط به کلاینت ها هم به صورت خودکار از طریق این سرویس نصب شود، برای انجام این کار سرویس Deployment را اجرا کنید و از سمت چپ بر روی Drivers کلیک راست کنید و بر روی Add Driver Package کلیک کنید.



در این قسمت دو روش برای معرفی درایور موردنظر وجود دارد که با انتخاب گزینه اول می‌توانید فایل INF مربوط به درایور موردنظر را به آن معرفی کنید و یا با انتخاب گزینه دوم پوشه مربوط به درایو موردنظر را به مانند شکل روبرو معرفی کنید.

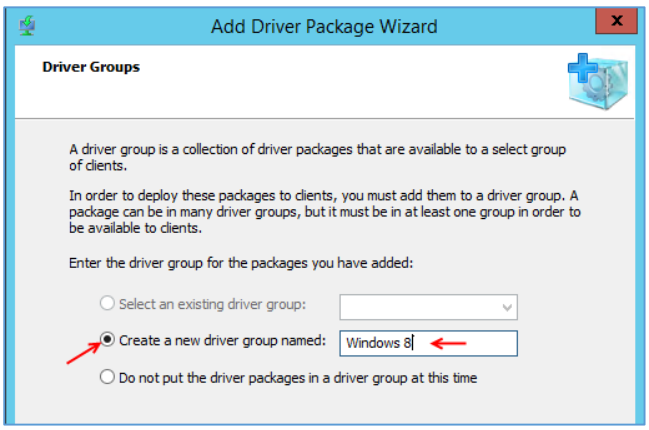
بر روی next کلیک کنید.



بعد از بررسی انجام شده در این صفحه، دو ورژن برای این درایو پیدا شده است که می‌توانید هر دو و یا یکی از آنها را انتخاب کنید.

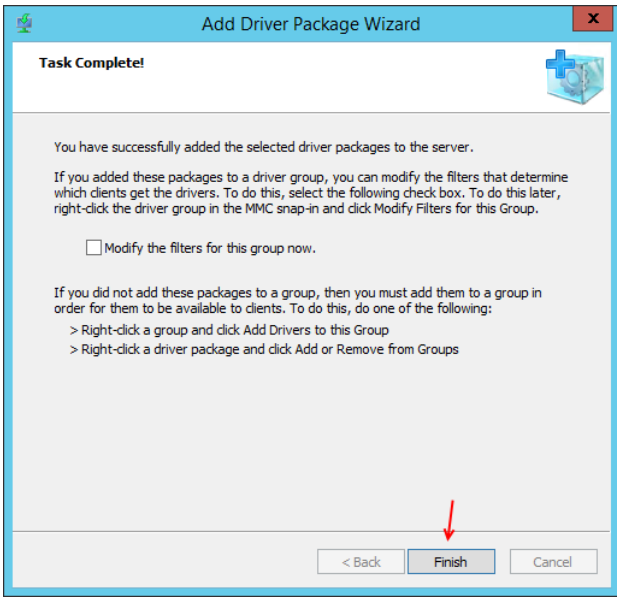
بر روی Next کلیک کنید.

دو بار دیگر بر روی Next کلیک کنید تا درایور موردنظر در سرویس Deployment ثبت شود.



در این قسمت می‌توانید برای درایو موردنظر خود یک گروه ایجاد کنید، مثلاً اگر درایو مربوط به ویندوز 8 می‌باشد یک گروه با نام Windows 8 ایجاد کنید.

بر روی Next کلیک کنید.



دراین قسمت تیک گزینه موردنظر را بردارید و بر روی Finish کلیک کنید.

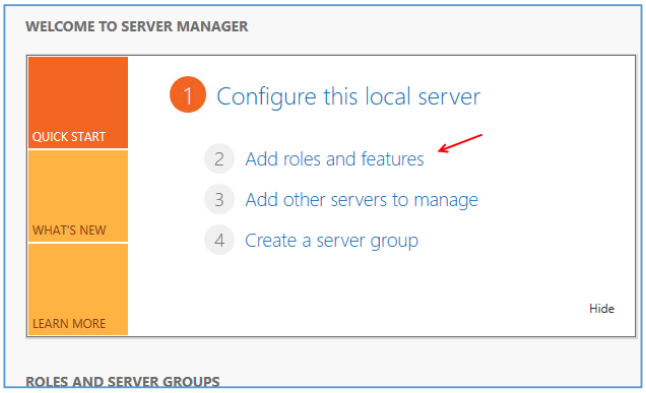
با این کار درایور آماده نصب می‌باشد و زمانی یک کلاینت اقدام به نصب ویندوز کند این درایور در صورت نیاز بر روی آن به صورت خودکار نصب خواهد شد.

نصب و راه اندازی سرویس Windows Server update Service (WSUS):

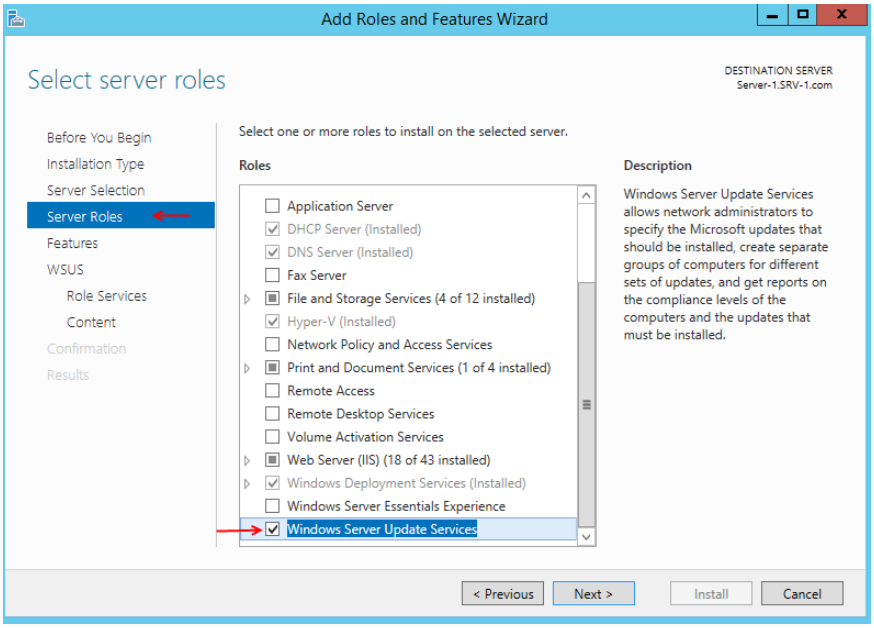
فرض کنید شما در شبکه خود 200 کلاینت داشته باشید و همه آنها به اینترنت متصل باشند، اگر همه این کلاینت ها در یک زمان بخواهند خود را آپدیت کنند چه اتفاقی برای پهنای باند شبکه می‌افتد؟ خوب مسلماً حجم بالایی از پهنای باند مصرف می‌شود و کل شبکه کند می‌شود و از همه مهمتر هزینه افزایش پیدا می‌کند.

برای حل این مشکل تیم مایکروسافت سرویس WSUS یا همان Windows Server Update Service را معرفی کرد، این سرویس بر روی ویندوز سرور نصب می‌شود و تمام آپدیت ها را از سایت مایکروسافت برای تمام محصولات آن دریافت می‌کند و کلاینت های موجود در شبکه می‌توانند از طریق این سرویس اطلاعات خود را آپدیت کنند که نحوه تنظیم این سرویس در زیر بررسی می‌شود.

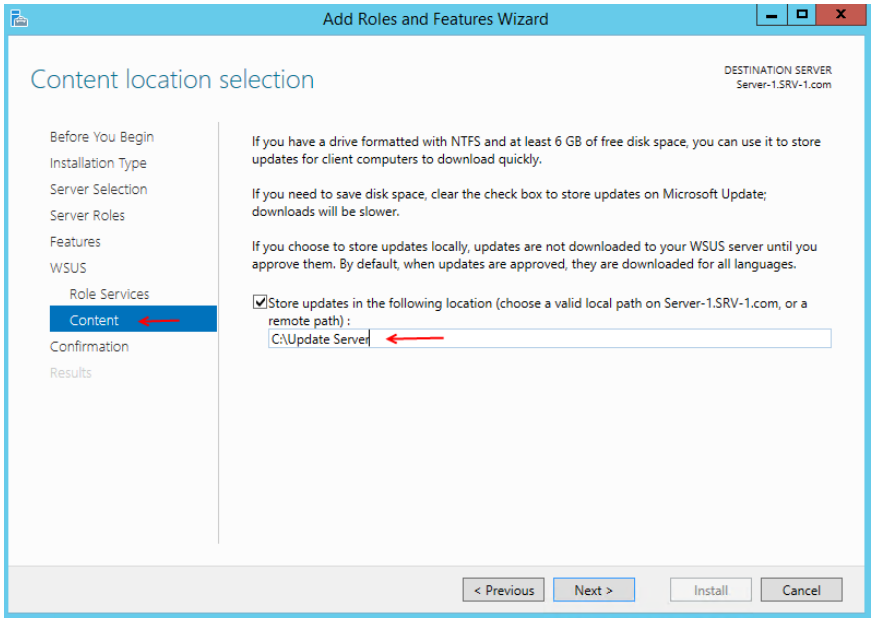
نکته مهم: قبل از شروع کار سرور خود را به اینترنت متصل کنید، برای متصل کردن سرور مجازی به اینترنت به قسمت بررسی سرویس Hyper-V مراجعه کنید و یا به کتاب Vmware 10 که لینک آن در سایت وجود دارد مراجعه کنید.



برای شروع وارد Server Manager شوید و بر روی Add Roles and Feature کلیک کنید.

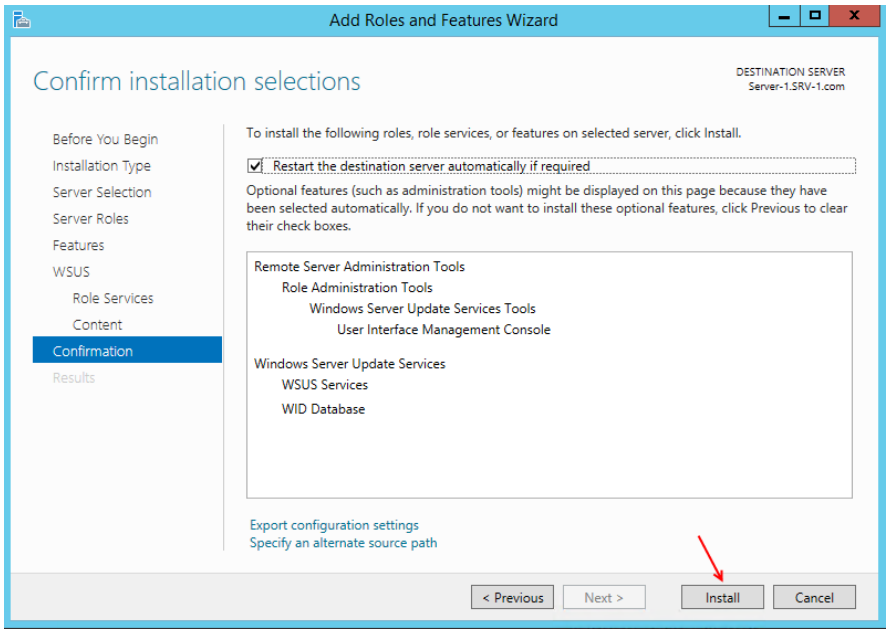


بر روی Next کلیک کنید تا به قسمت Server Roles برسید، در این قسمت از لیست Role های موجود گزینه Windows Server Update Services را انتخاب کنید و در پنجره باز شده بر روی Add Feature کلیک کنید و بر روی Next کلیک کنید.



بر روی Next کلیک کنید تا به قسمت Content برسید، در این قسمت باید آدرس مناسبی را وارد کنید که درایو آن بیشتر از 6 گیگابات فضا داشته باشد تا فایل‌های آپدیت زمانی که دانلود می-شوند در این آدرس قرار بگیرد.

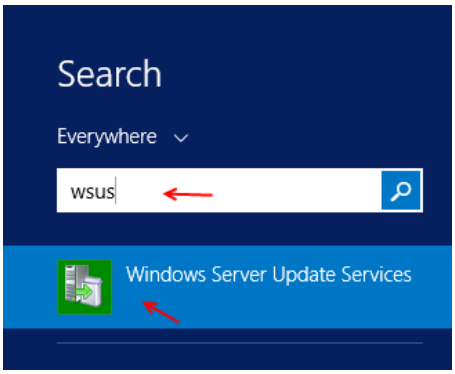
بر روی Next کلیک کنید.



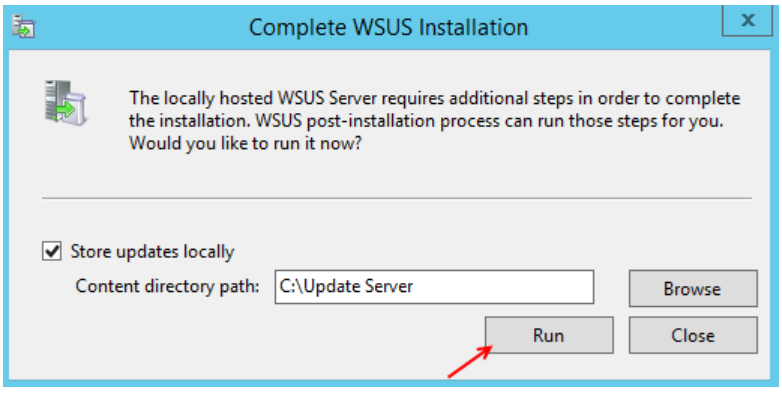
در این قسمت بر روی Install کلیک کنید تا نصب سرویس آغاز شود.

سیستم را بعد از نصب Restart کنید.

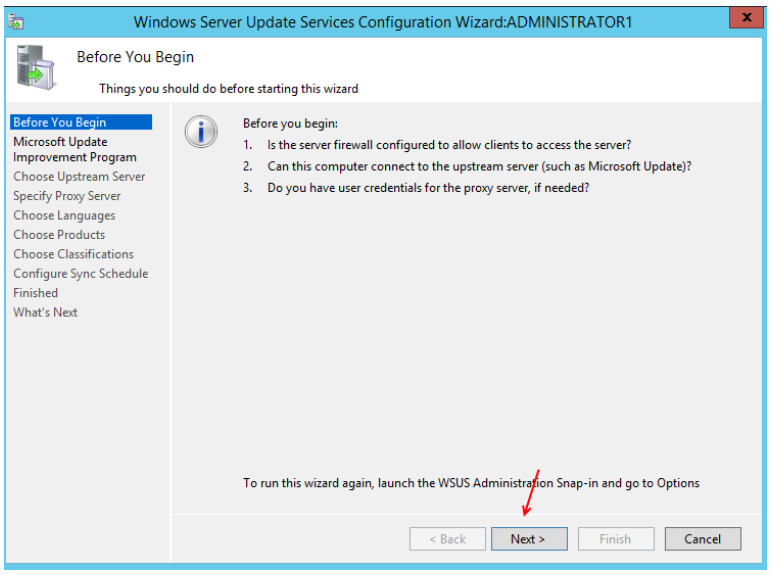
بعد از نصب سرویس WSUS و قبل از اجرای آن حتماً سرور را به اینترنت متصل کنید تا تنظیمات به درستی انجام شود، اگر اینترنت فعال نباشد این کار امکان پذیر نیست.



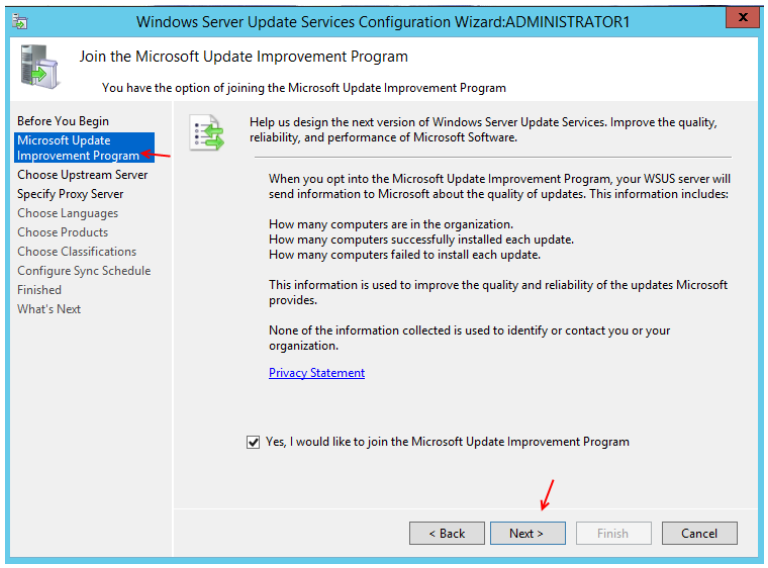
وارد Serach شوید و کلمه wsus را وارد کنید و در گزینه های موجود بر روی Windows Server Update Service کلیک کنید.



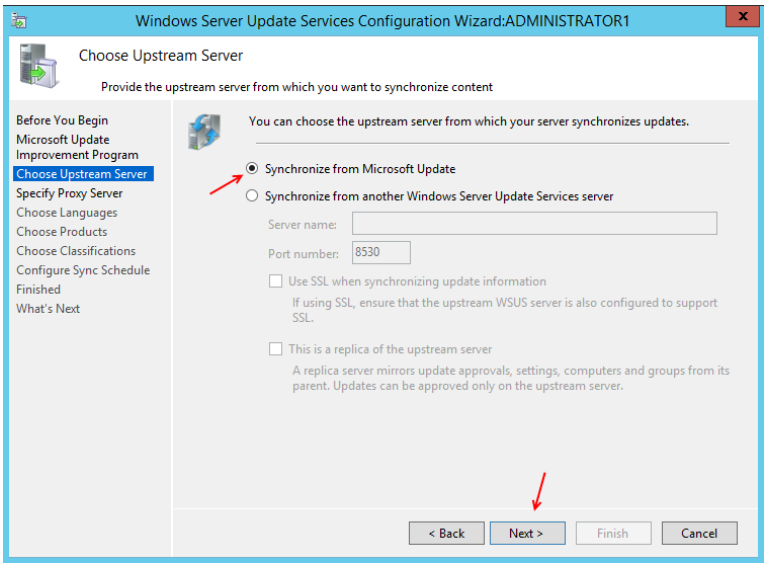
در این قسمت آدرسی که قبلاً در هنگام نصب سرویس وارد کرده‌ایم را مشاهده می‌کنید که می‌توانید آدرس موردنظر را تغییر بدهید، بر روی Run کلیک کنید. و بعد از ایجاد



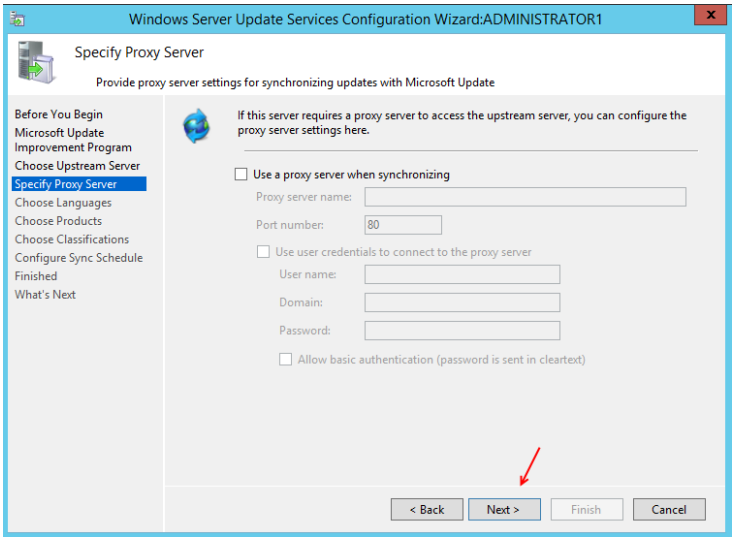
بعد از اینکه در قسمت قبل بر روی Close کلیک کردین پنجره روبرو برای شما باز می‌شود که برای تنظیم سرویس بر روی Next کلیک کنید.



در این قسمت هم توضیحاتی در مورد نحوه آپدیت شدن به شما می‌دهد که آن را مطالعه و بر روی Next کلیک کنید.

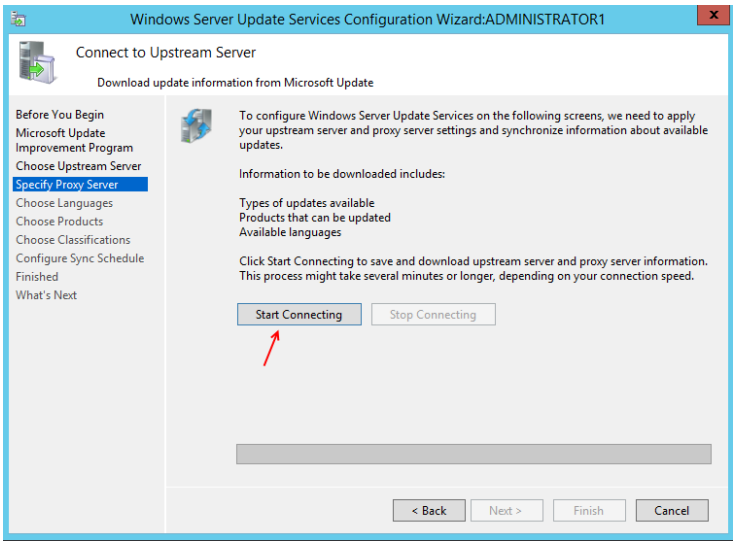


در این قسمت با انتخاب گزینه اول سرور شما به صورت مستقیم از طریق اینترنت با سرور مایکروسافت Syn و یا هماهنگ می‌شود، ولی اگر سرور دیگری دارید که می‌خواهید به آن متصل شوید باید گزینه دوم را فعال و آدرس سرور موردنظر را به همراه پورت آن وارد کنید.

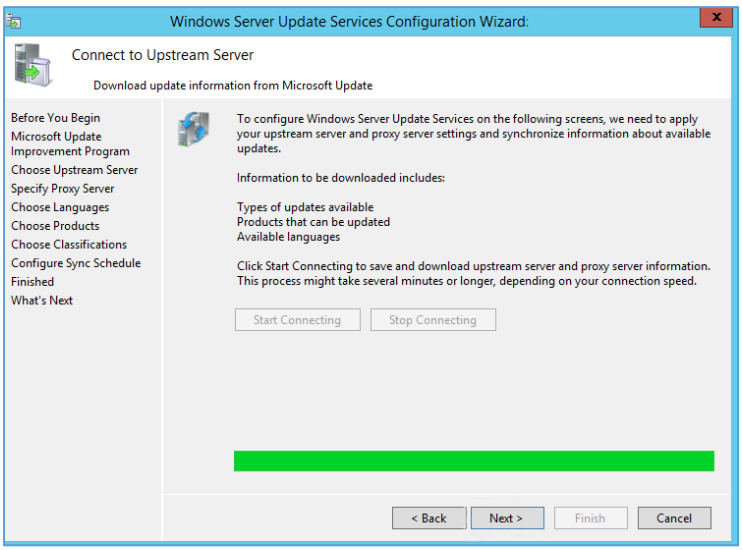


در این قسمت اگر از سرور Proxy خاصی استفاده می‌کنید می‌توانید آدرس آن را با فعال کردن گزینه Use a Proxy... وارد کنید.

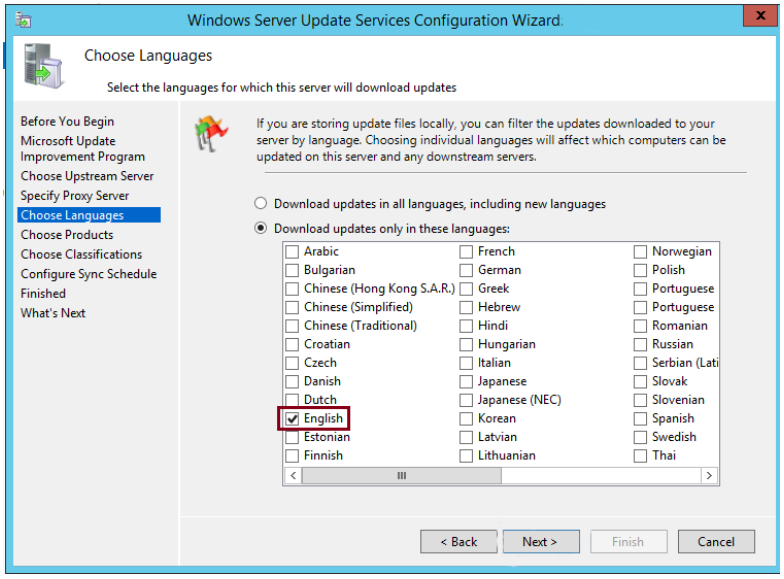
بر روی Next کلیک کنید.



در این قسمت برای اینکه به سرور Upstream مایکروسافت متصل بشویم حتماً باید به اینترنت متصل باشیم وگرنه اجازه ادامه کار را به شما نمی-دهد. بر روی Start Connecting کلیک کنید تا عملیات آغاز شود.

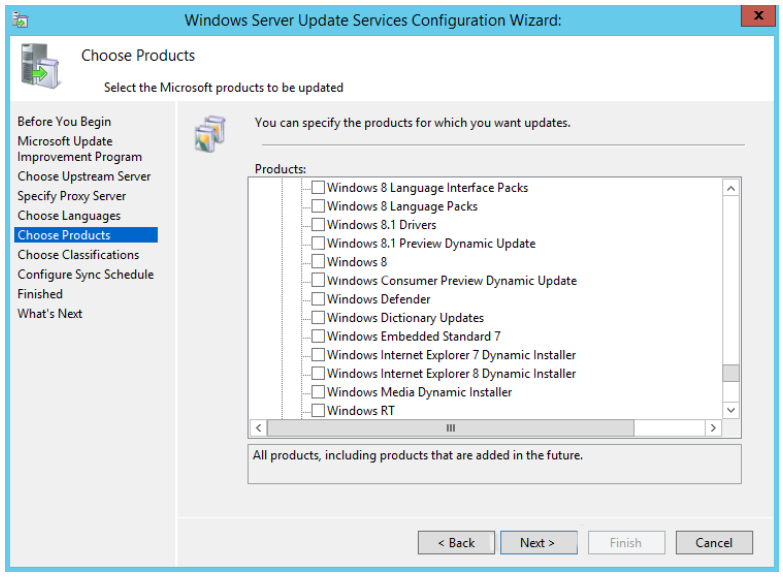


در این قسمت با موفقیت به سرور مایکروسافت متصل شده‌ایم، برای ادامه کار بر روی Next کلیک کنید.



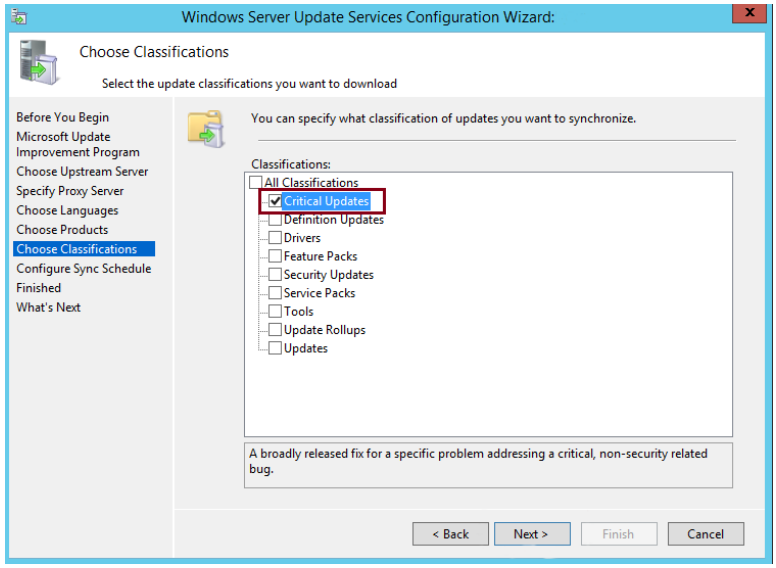
در این قسمت زبان موردنظر خود را انتخاب کنید تا آپدیت های موردنظر به زبان موردنظر دریافت شود.

بر روی Next کلیک کنید.



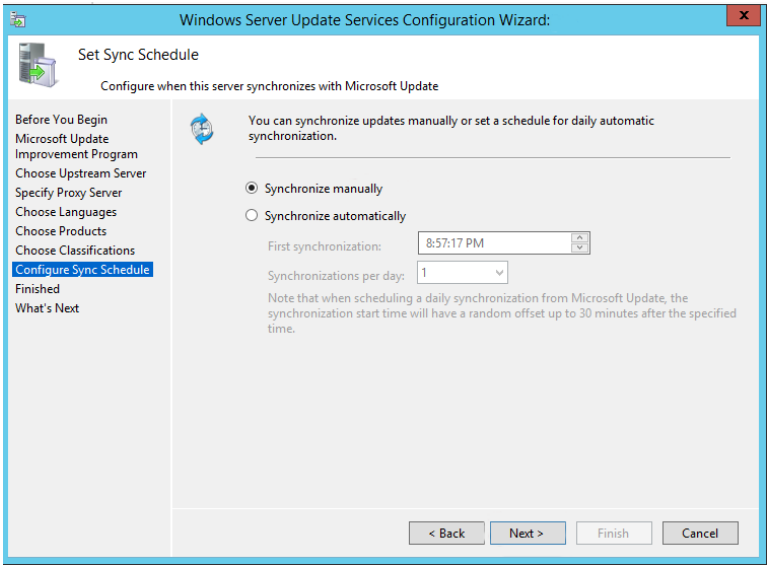
به این قسمت توجه کنید، شما باید بسته به نیاز سازمان خود محصولات موردنظر خود را از لیست انتخاب کنید، مثلاً اگر کلاینت های شبکه شما از ویندوز 8 بهره می‌برند، باید در این قسمت تیک ویندوز 8 را انتخاب کنید و یا مثلاً تیک ویندوز 7 را انتخاب کنید.

بر روی next کلیک کنید.

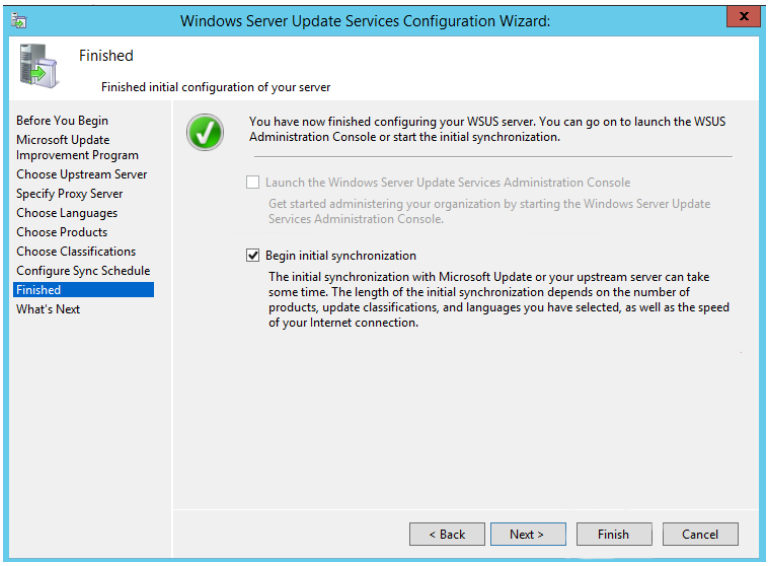


در این قسمت نوع آپدیت خود را انتخاب کنید مثلاً اگر می‌خواهید درایور های ویندور خود را آپدیت کنید گزینه Drivers را انتخاب کنید.

در این قسمت گزینه Critical Updates را انتخاب کنید و بر روی Next کلیک کنید.

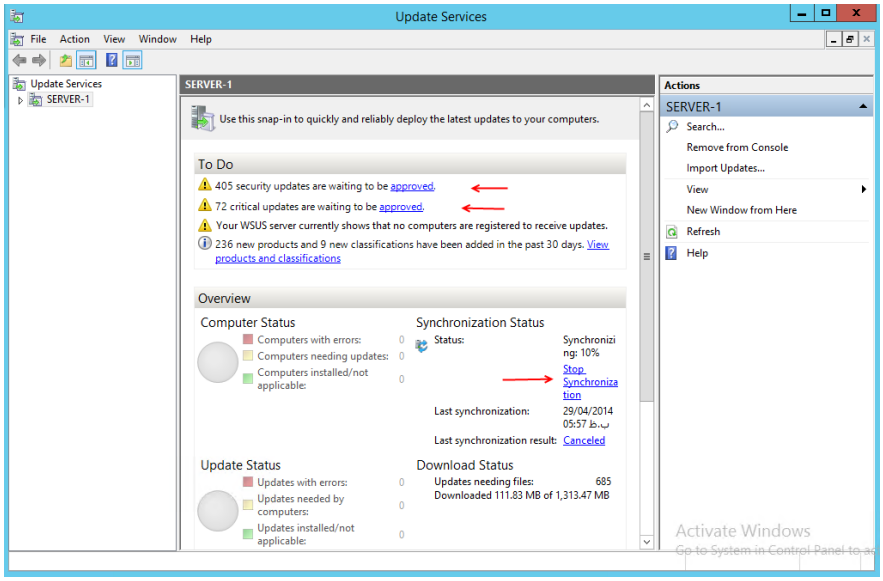


در این قسمت باید مشخص کنید که آیا می-خواهید همسان سازی یا Synchronize به صورت دستی انجام شود که با انتخاب گزینه اول این کارامکان پذیر است ویا با انتخاب گزینه دوم به صورت اتوماتیک در زمان مشخص‌شده انجام شود. گزینه اول را انتخاب و بر روی Next کلیک کنید.

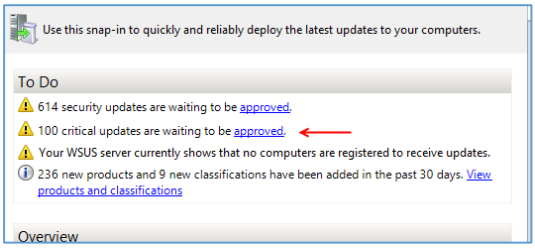


در این صفحه با انتخاب گزینه Begin initial Synchronize کار همسانسازی سرور اصلی با سرور مایکروسافت برای دریافت آپدیت بعد از بست این پنجره آغاز خواد شد.

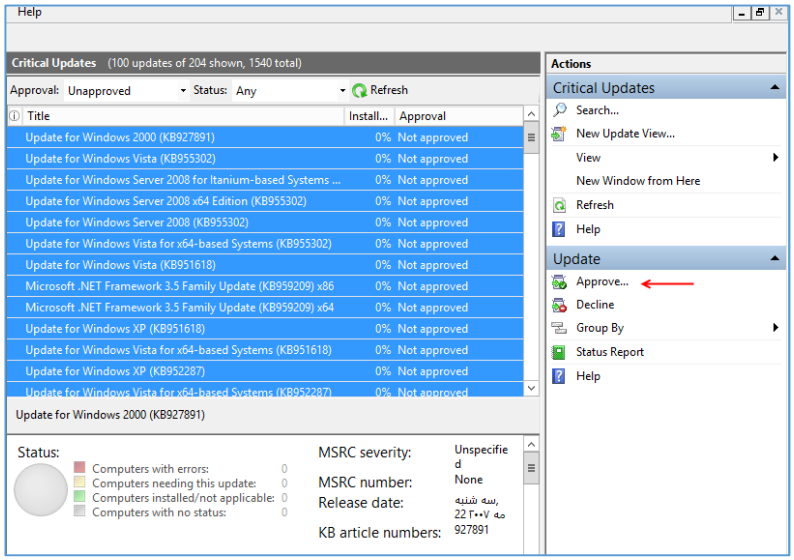
بر روی Finish کلیک کنید.



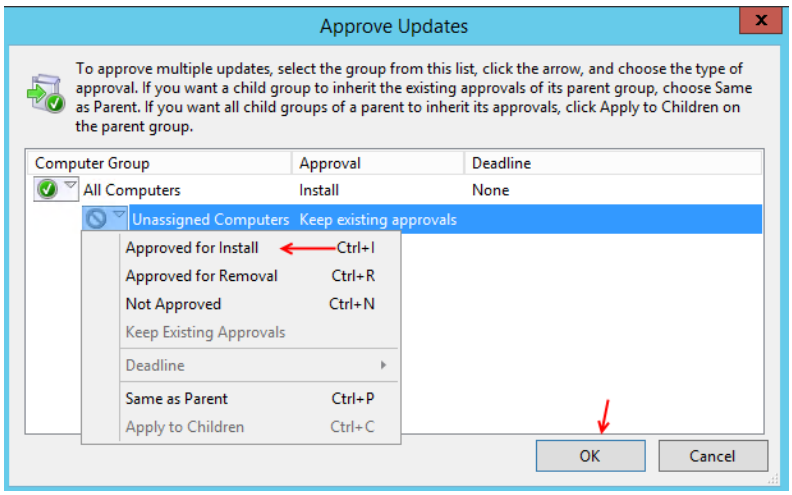
در این صفحه سرویس wsus اجرا شده است و اگر به وسط صفحه نگاه کنید کار Synchronize به صورت اتوماتیک آغاز شده است و در بالای آن تعداد 405 Security Update و 72 تا Certical Updates دریافت کرده است.



بعد از اتمام Synchronize برروی Approved مربوط به Certical Updates کلیک کنید.

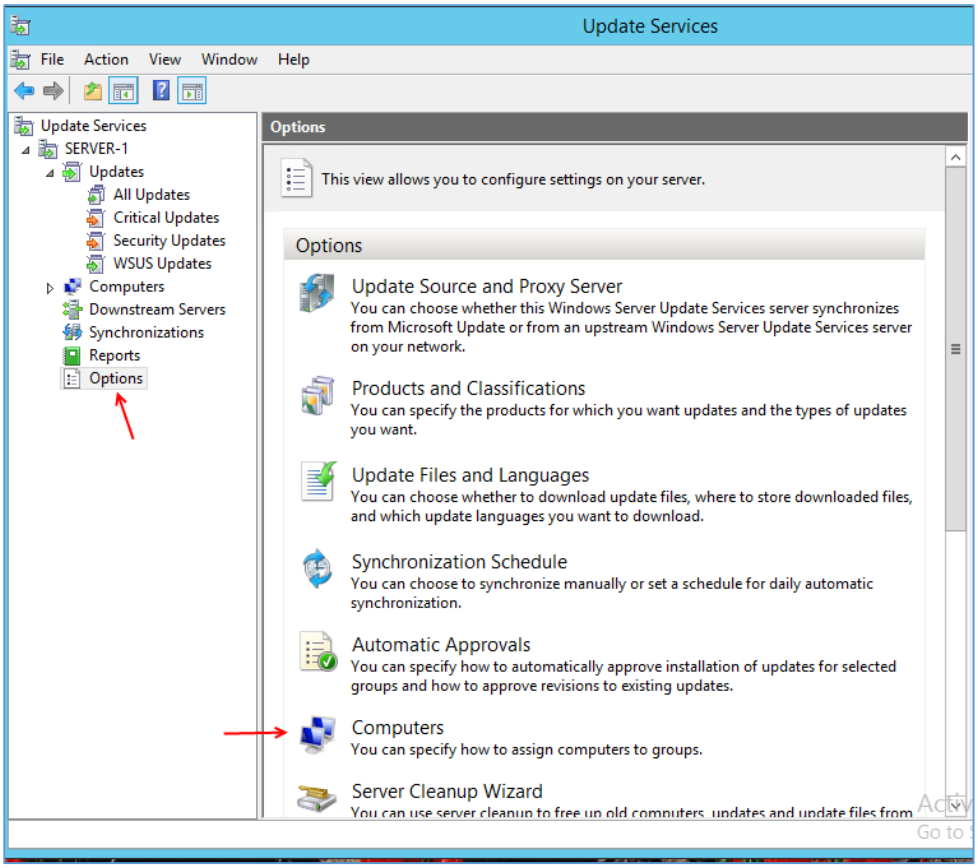


در این قسمت آپدیت ها مربوط به قسمت Certical Updates را مشاهده می‌کنید، برای این که این آپدیت ها دانلود شوند همه آنها را انتخاب کنید و از سمت راست بر روی Approve کلیک کنید.

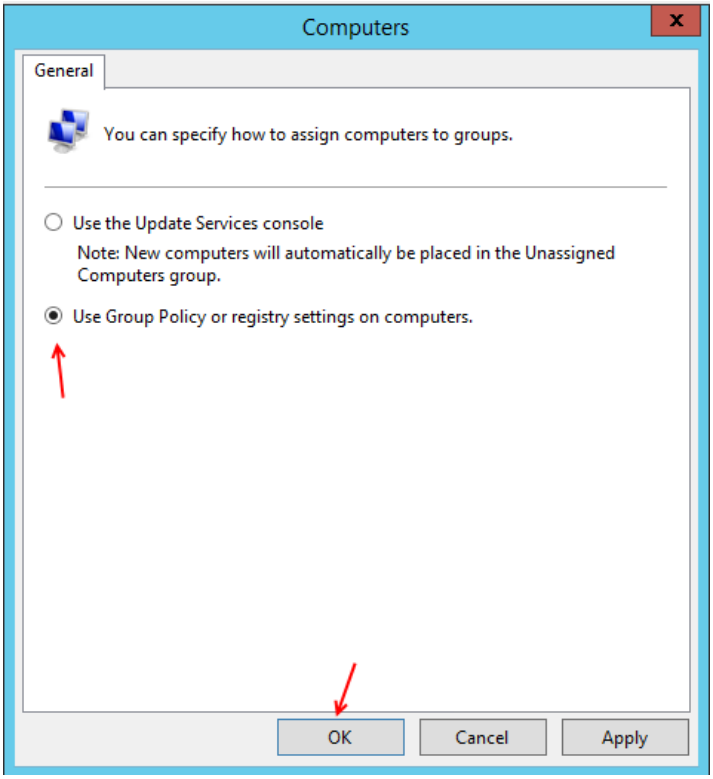


در این قسمت باید بر روی هر یک از گزینه ها کلیک کنید تا منوی موردنظر باز شود و بعد گزینه Approved for install را انتخاب کنید. توجه داشته باشید قبل از این کار باید تنظیمات مربوط به کلاینت ها برای دریافت آپدیت را انجام دهیم.

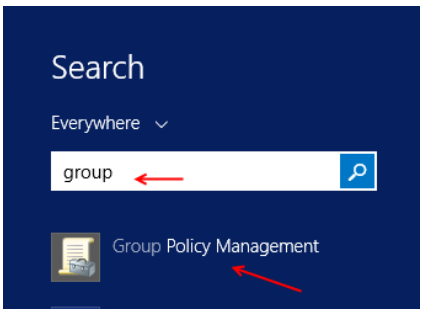
برای اینکه تمام کلاینت ها بتوانند آپدیت را دریافت کنند لازم نیست وارد هر کلاینت بشویم و تنظیمات مربوط به آن را جداگانه انجام دهیم، فقط کافی است که وارد سرور اصلی بشویم و از طریق سرویس wsus و Group Policy تنظیمات مربوط به آن را انجام دهیم تا تمام کلاینت‌های عضو شبکه موردنظر از آپدیت موردنظر استفاده کنند.



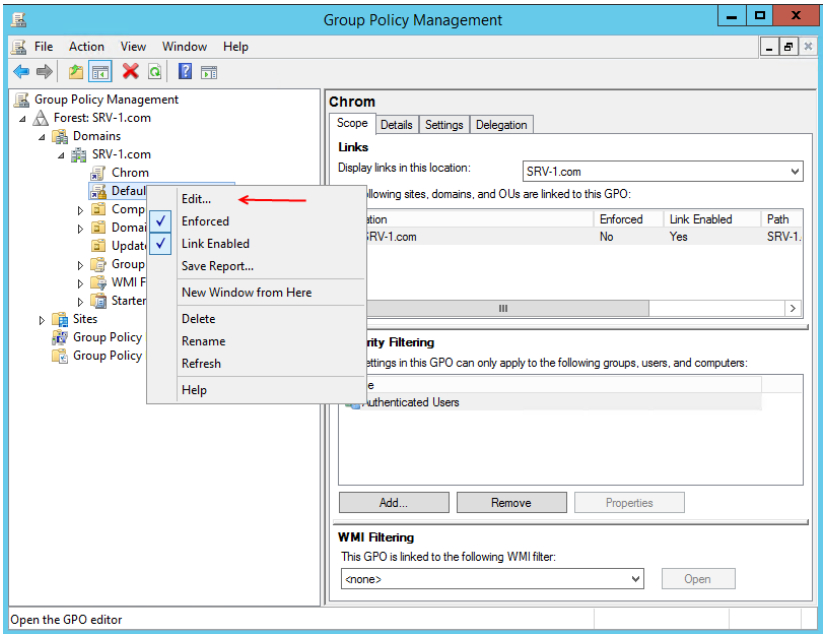
برای شروع کار در سرویس wsus از سمت چپ بر روی Options کلیک کنید و در صفحه باز شده بر روی Computers کلیک کنید تا شکل زیر ظاهر شود.



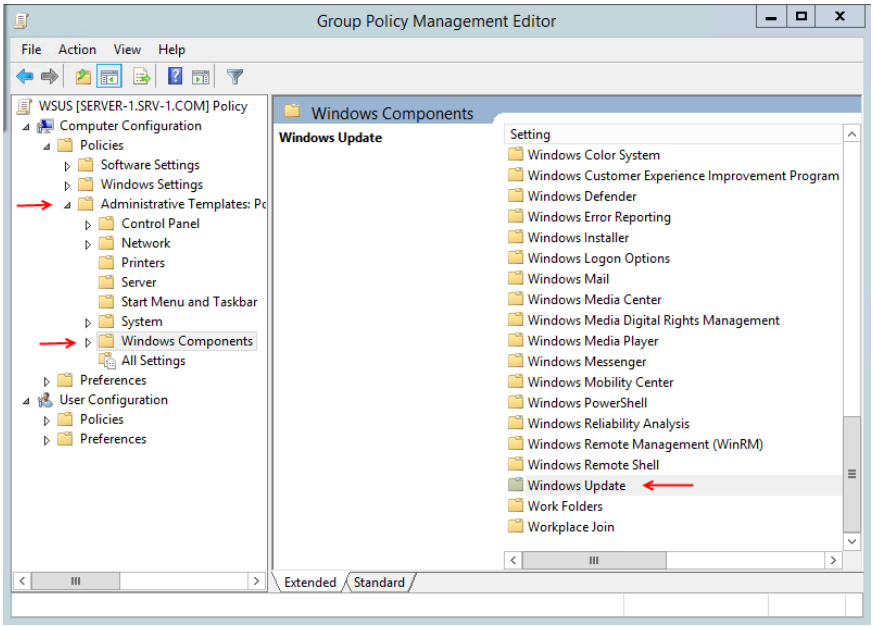
در این صفحه گزینه Use Group Policy or registry settistry on computers را انتخاب کنید و بر روی ok کلیک کنید.



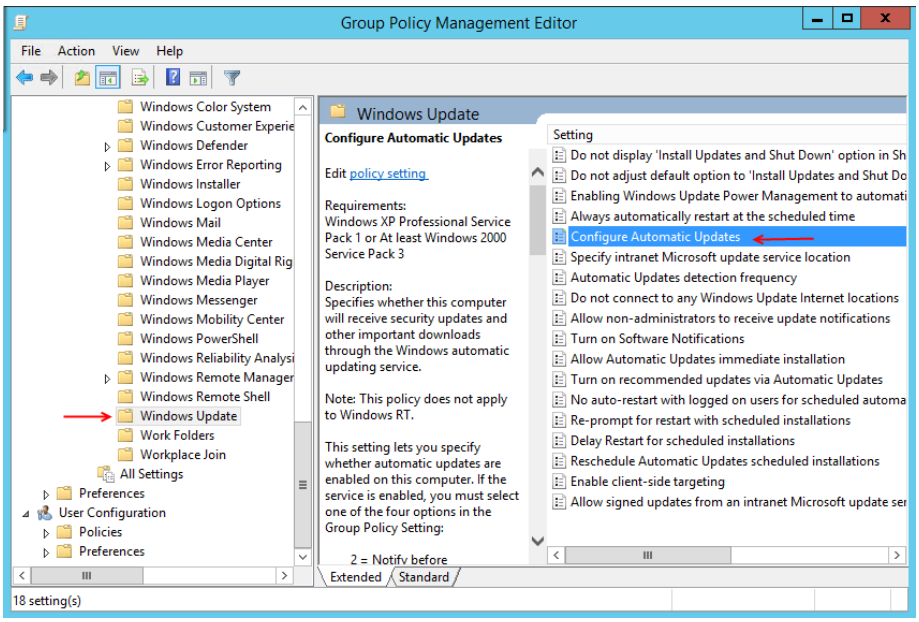
بعد از انجام کار بالا وارد Search شوید و به مانند شکل روبرو Group Policy Management را انتخاب کنید.



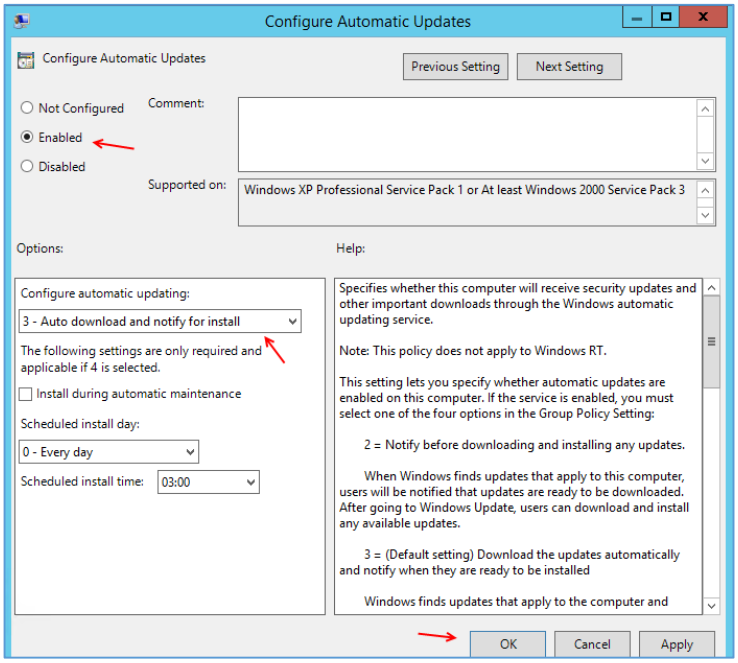
در این قسمت از سمت چپ بر روی Default Domain Poolicy کلیک راست کنید و گزینه Edit را انتخاب کنید.



در این صفحه از سمت چپ اول Administrative Templates.. را انتخاب و بعد Windows Components را انتخاب کنید و در لیست باز شده وارد Windows Update شوید.

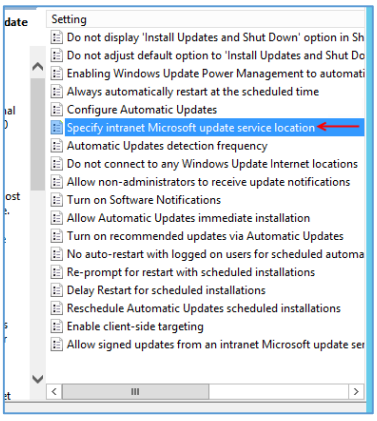


در این قسمت بر روی گزینه Configure Automatic Update دو بار کلیک کنید تا شکل بعد ظاهر شود.

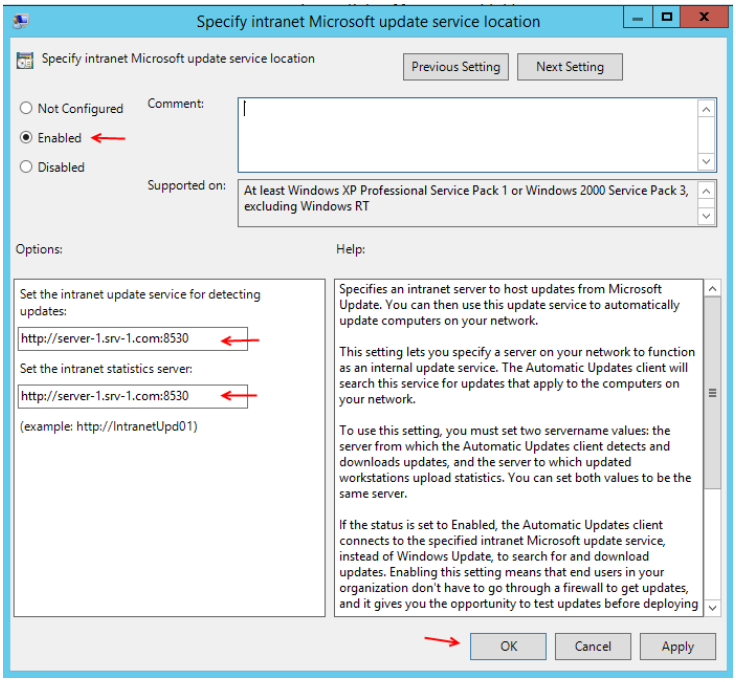


در این صفحه گزینه Enabled را انتخاب کنید و در قسمت Configure automatic updating گزینه سوم را انتخاب کنید تا آپدیت به صورت اتوماتیک دانلود و نصب شود البته می‌توانید با انتخاب گزینه دوم برای آن زمان بندی هم تعریف کنید.

بر روی ok کنید.



بعد انجام کار بالا دوباره در همان صفحه بر روی Specifies intranet Microsoft...دو بار کلیک کنید.

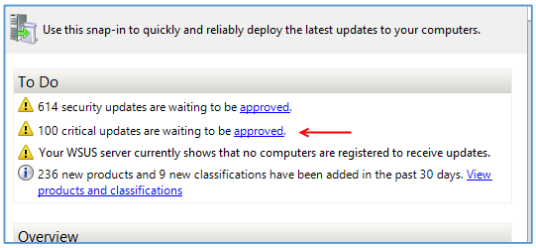


در این قسمت باید آدرس سرور داخلی خود را به کلاینت‌ها اعلام کنیم تا کلاینت ها بتوانند از طریق این آدرس آپدیت خود را دریافت کنند، برای این کار بر روی enable کلیک کنیدو در دو قسمت مشخص‌شده آدرس زیر را وارد کنید:

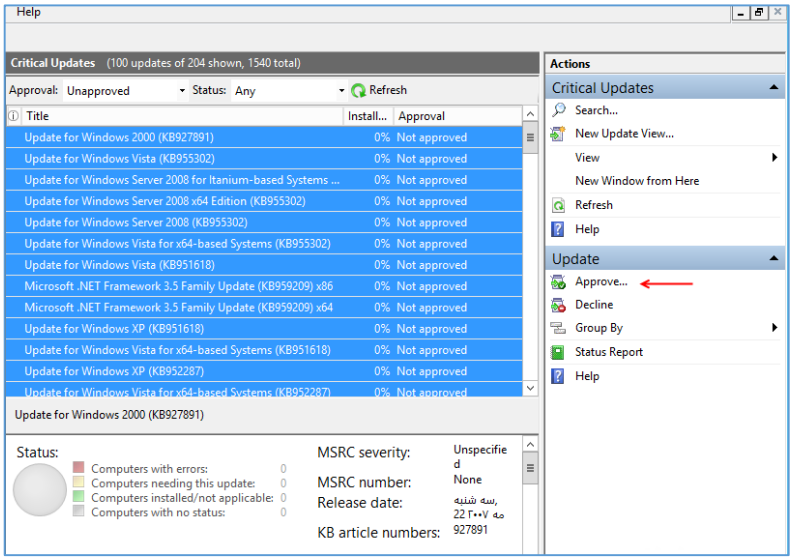
http://server-1.srv-1.com:8530

در این آدرس باید به جای Server-1 نام سرور خود را وارد کنیدو به جای Srv-1.com نام دومین خود را وارد کنید و پورت 8530 هم برای سرویس WSUS ثابت می‌باشد. بعد از این کار بر روی ok کلیک کنید.

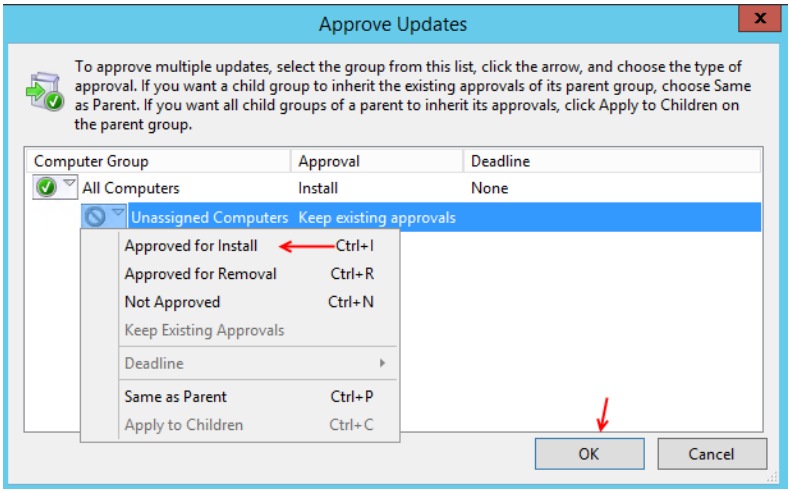
بعد از اتمام کار وارد CMD شوید و دستور gpupdate /force را اجرا کنید تا Group Plicy بدون نیاز به Restart آپدیت شود.



بعد از انجام عملیات بالا باید وارد سرویس WSUS شویم و از قسمت To do یکی از آپدیت ها را انتخاب کنید

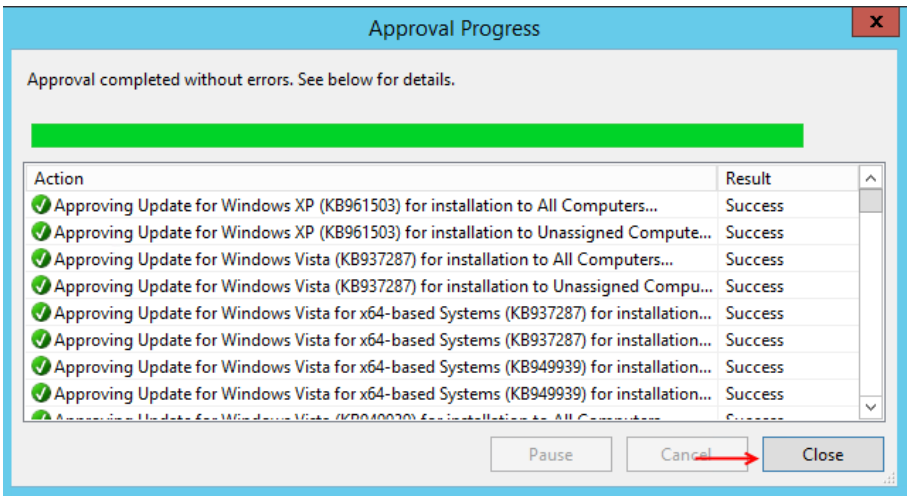


در این قسمت به مانند قبل باید آپدیت هایی که از سایت مایکروسافت دریافت شده را انتخاب کنید و بعد بر روی Approve کلیک کنید.



در این قسمت به مانند شکل بر روی هر یک از قسمت ها کلیک کنید تا منوی موردنظر باز شود، در این منو گزینه Approved For install را انتخاب کنید.

بر روی ok کلیک کنید.

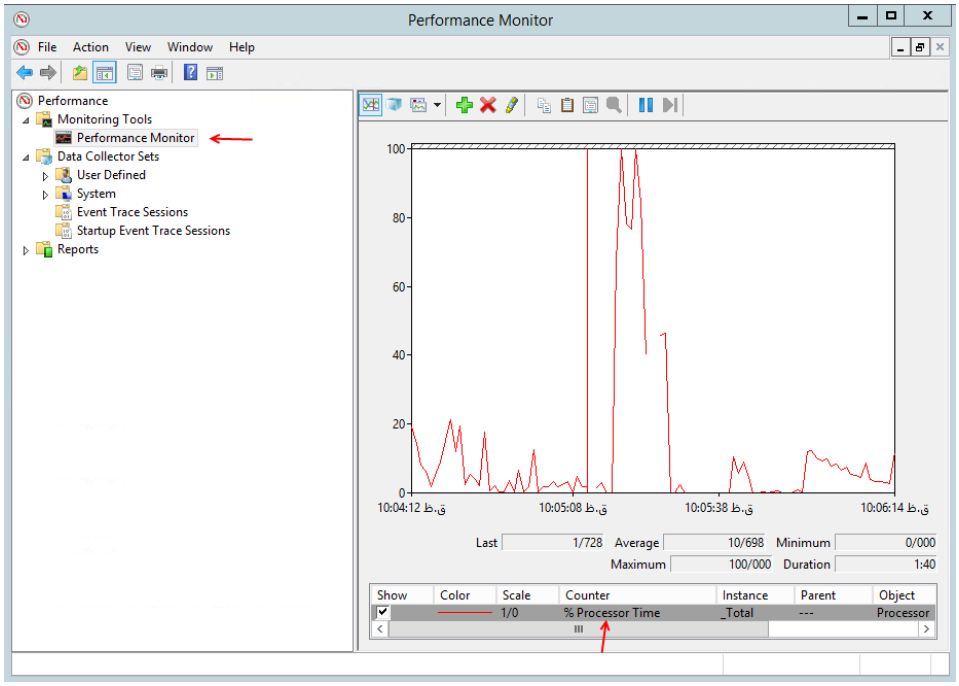


همانطور که در این قسمت مشاهده می‌کنید آپدیت های موردنظر از سرور مایکروسافت دانلود شده و درون کامپیوتر سرور قرار گرفته و کلاینت ها با استفاده از آدرس سرور می‌توانند این آپدیت ها را دریافت کنند.

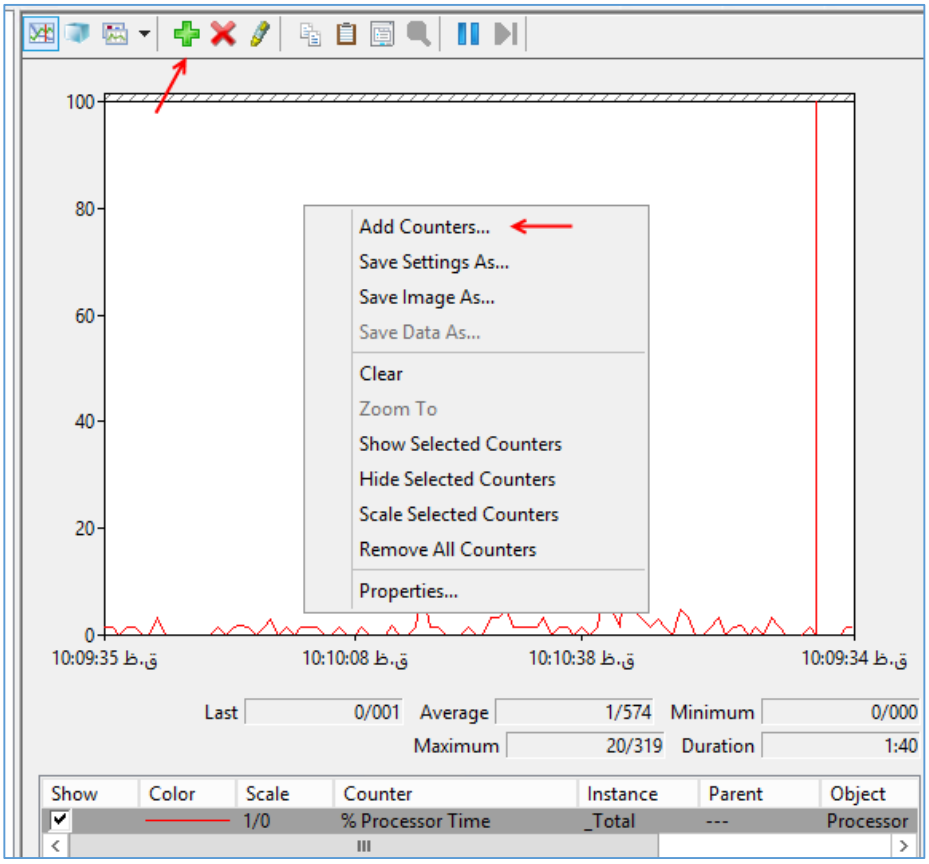
کار با سرویس‌های Monitoring:

در ویندوز سرور سرویس‌ها و ابزارهایی وجود دارد که می‌توانیم بر روی تمام اجزای سرور خود از Cpu گرفته تا ارتباط اینترنت، نظارت کامل داشته باشیم، سرویس‌هایی مانند Performance Monitor و Event Viewer وجود دارد که با سرویس Event Viewer تا حدودی در قسمت‌های قبلی کتاب کار کردیم که در اینجا هم با این سرویس بیشتر آشنا می‌شویم.

در ابتدا سرویس Performance Monitor را بررسی می‌کنیم، این سرویس به صورت پیش فرض بر روی ویندوز سرور نصب است و نیاز به نصب نیست، برای اجرای این سرویس به مانند قبل وارد Search شوید و کلمه Performance Monitor را وارد کنید. و بعد اجرا کنید.

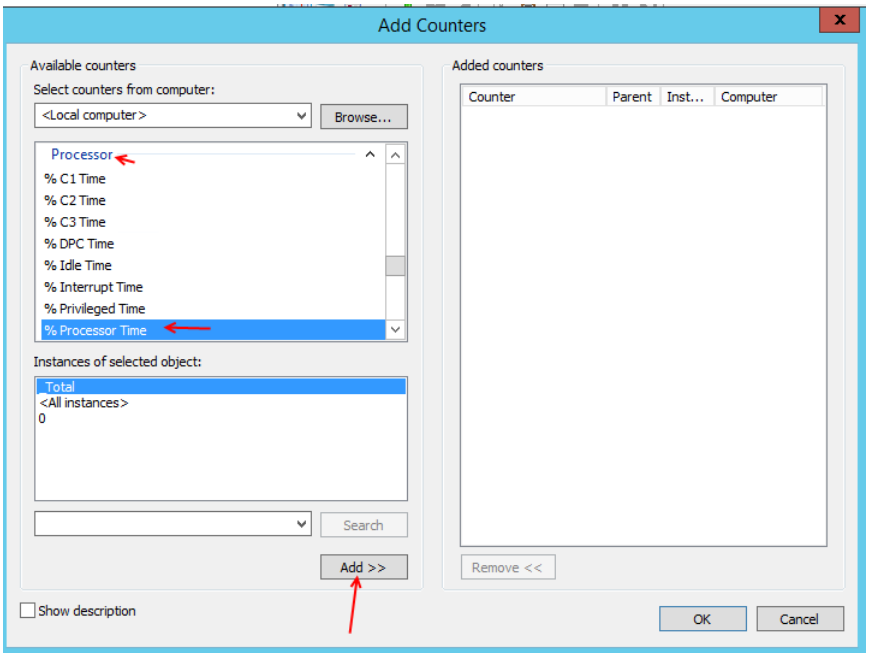


همانطور که در شکل زیر مشاهده می‌کنید سرویس Performance Monitor اجرا شده است، اگر از سمت چپ بر روی Performance Monitor کلیک کنید، یک شمارنده مربوط به Processor Time را مشاهده می‌کنید که نشان دهنده کارکرد CPU می‌باشد.



در این قسمت می‌خواهیم یک شمارنده جدید به لیست اضافه کنیم تا نحوه کارکرد آن را بررسی کنیم، برای این کار به مانند شکل روبرو در قسمت مشخص‌شده کلیک راست کنید و گزینه Add Counters را انتخاب کنید و یا از نوار ابزار بالا بر روی آیکون + کلیک کنید.

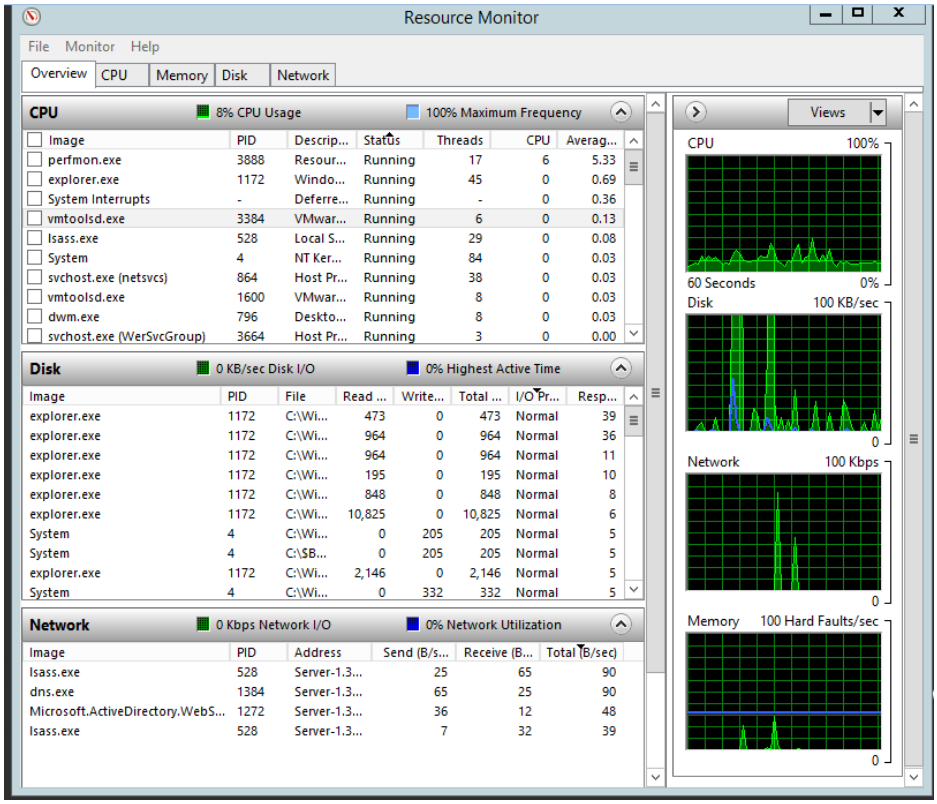
شمارنده های مختلفی را می‌توانیم به این لیست اضافه کنیم.



در این قسمت لیست تمام شمارنده های موجود رامشاهده می‌کنید.

مثلاً در این شکل شمارنده Processor خود دارای زیر مجموعه و یا ریز اطلاعات می‌باشد که می‌تواند کل مجموعه و یا یکی از آنها را انتخاب کنید.

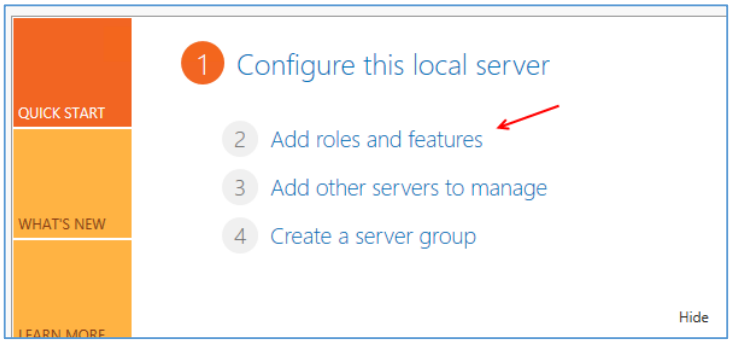
توجه داشته باشید در بالای شکل Local Computer نوشته که نشان دهنده این است که این شمارنده ها مربوط به این Computer می‌باشد که می‌توانید با کلیک بر روی Browse کامپیوتر دیگر را به لیست اضافه کنید و اطلاعات و شمارنده های آن را مورد بررسی قرار دهید.



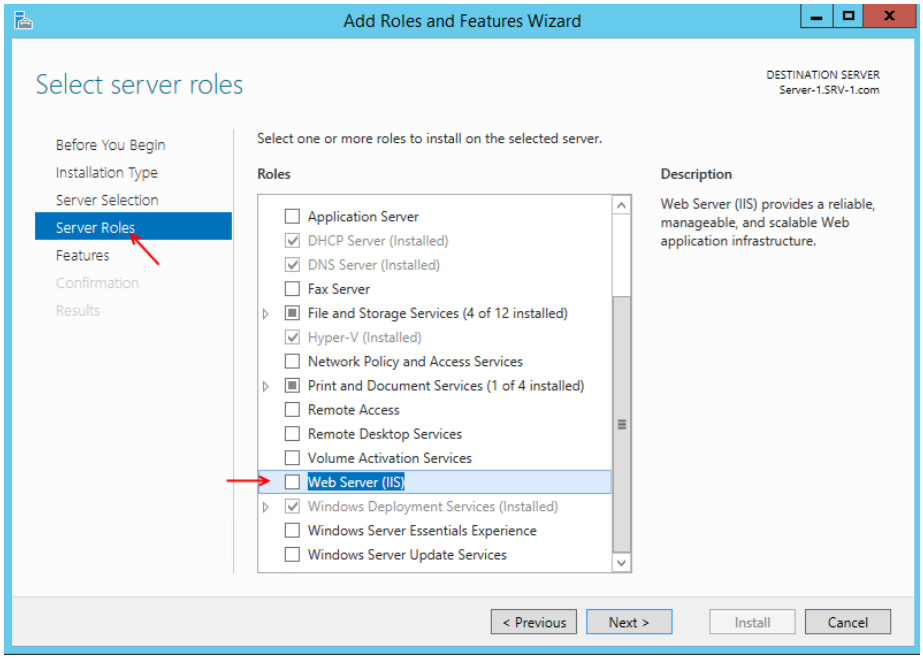
سرویس دیگری با نام Resource Monitor وجود دارد که می‌توانی از طریق Serach آن را اجرا کنید، این سرویس به صورت خلاصه شده کارکرد پردازنده، Ram، Hard شبکه را مانیتور می‌کند، در این سرویس تمام نرم‌افزارها و سرویس-هایی که از منابع استفاده می‌کنند در این سرویس لیست شده است که کار مانیتورینگ سرور را آسان کرده است.

کار با Web Server (IIS):

در این بخش می‌خواهیم وب سرور را روی ویندوز سرور راه اندازی کنیم تا بتوانیم وب سایت های خود را روی سرور 2012 اجرا کنیم، البته با نصب سرویس هایی قبلی که با هم بررسی کردیم سرویس iiS به صورت خودکار روی سرور نصب شده است، ولی در این قسمت از اول این سرویس را بررسی خواهیم کرد و از نصب سرویس IIS و یا همان Web Server آغاز خواهیم کرد. توجه داشته باشید به همراه این سرویس سرویس DNS که قبلاً بررسی کرده‌ایم در این قسمت بررسی خواهد شد، چون این سرویس کاملاً با سرویس DNS در ارتباط است.

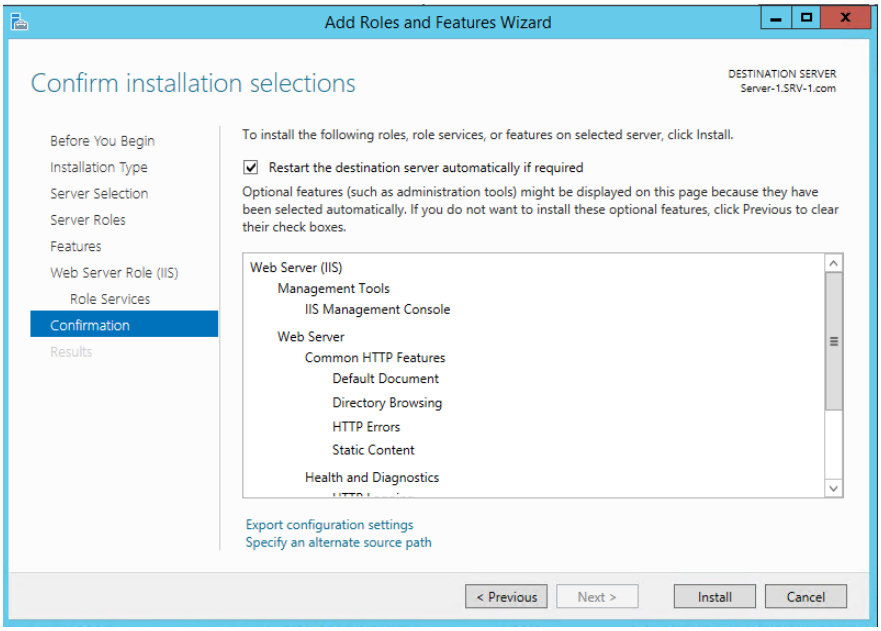


برای شروع وارد Server Manager شوید و بر روی Add Roles and Features کلیک کنید.



بر روی Next کلیک کنید تا به شکل روبرو یعنی قسمت Server Roles برسید، در این قسمت بین گزینه‌های موجود گزینه Web Servers (IIS) را انتخاب کنید و در پنجره باز شده بر روی Add Features کلیک کنید.

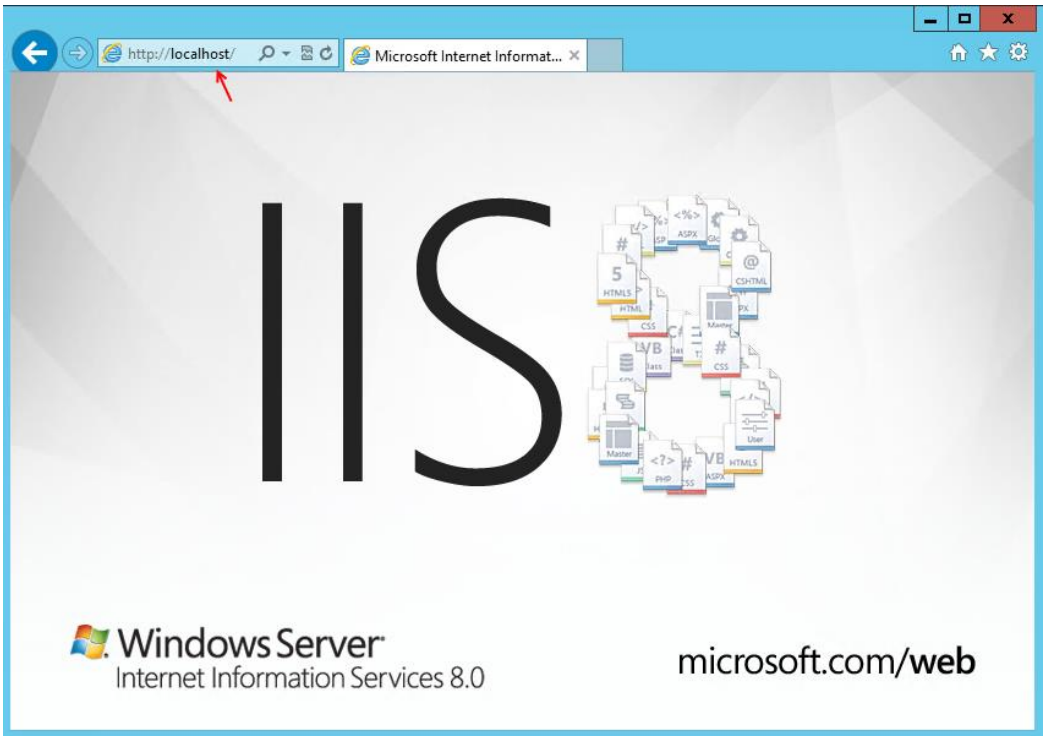
بر روی Next کلیک کنید تا به شکل بعد برسیم.

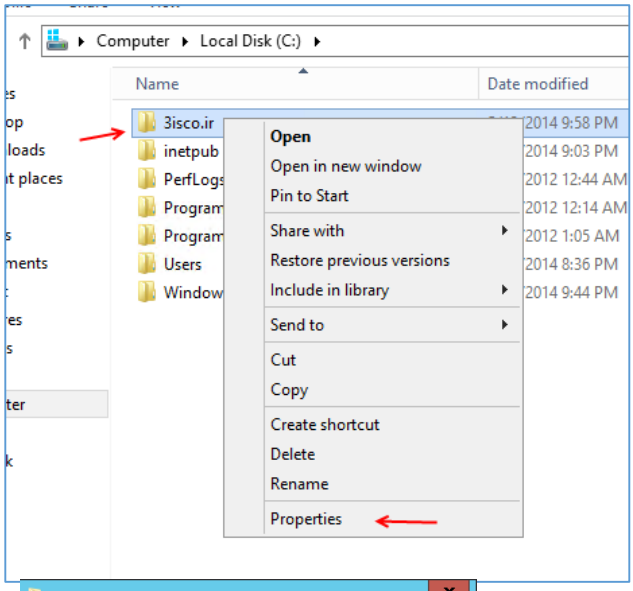


بر روی Next کلیک کنید تا به صفحه موردنظر برسید در این صفحه تیک گزینه موردنظر را زده و بر روی Install کلیک کنید.

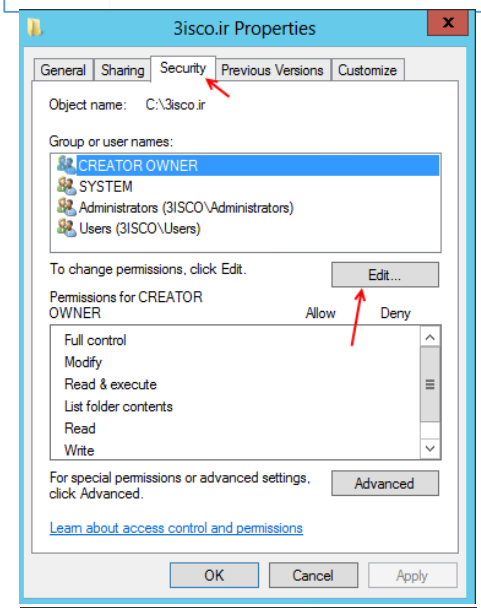
بعد از این که سرویس iiS را نصب کردید، باید تست کنیم که سرویس به درستی کار می‌کند و قابل اجرا است، برای این کار Internet Explorer را اجرا کرده و آدرس Http://localhost را اجرا کنید.

همانطور که در شکل زیر مشاهده می‌کنید با اجرای آدرس بالا مشخص‌شده است که سرویس IIS به درستی در حال کار می‌باشد.

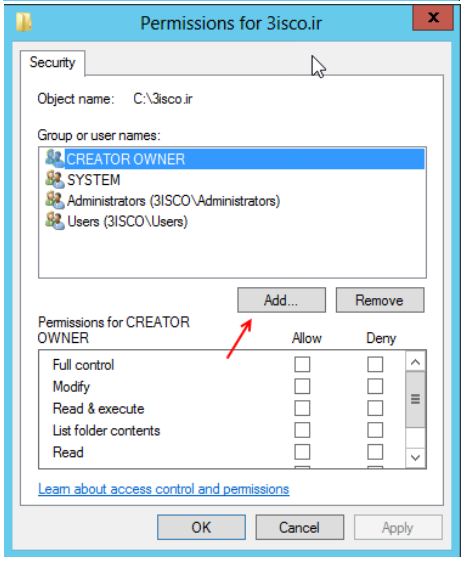




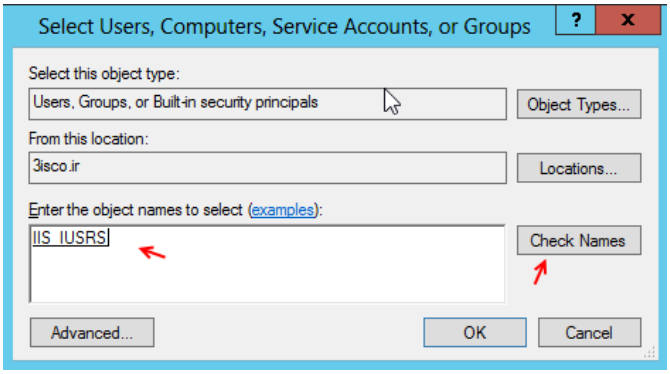
برای شروع باید یک پوشه در یکی از درایوهای خود ایجاد و فایل های مربوط به وب سایت خود را در آن قرار دهیم، برای شروع فعلاً یک فایل HTML با نام Index.html را در پوشه‌ای با نام 3isco.ir در درایو C ایجاد می‌کنیم. بعد از این کار باید یک سری مجوزهای لازم را برای دسترسی کاربران عضو دومین به وب سایت موردنظر انجام دهیم، برای این کار به مانند شکل روبرو بر روی پوشه موردنظر کلیک راست کنید و Properties را انتخاب کنید.



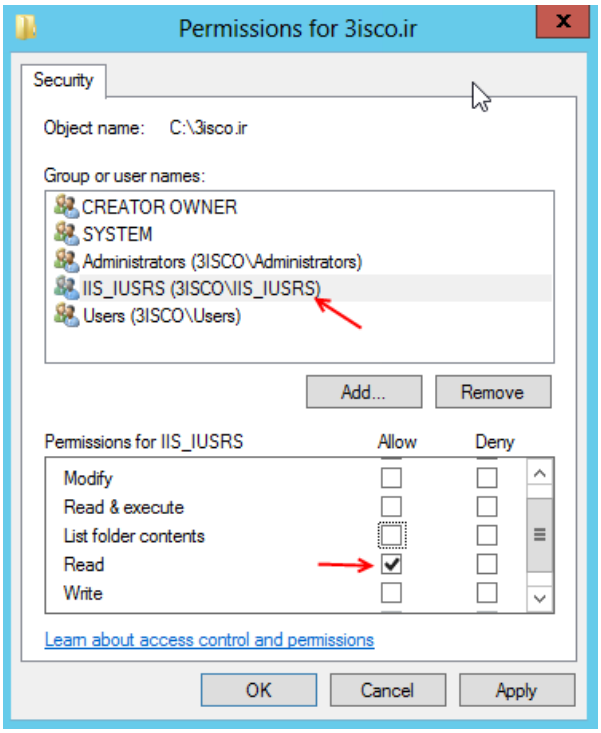
در این قسمت، وارد تب Security شوید و برای شروع کار بر روی Edit کلیک کنید تا شکل بعد ظاهر شود.



در این قسمت باید گروه برای دسترسی همه کاربران عضو دومین به وب سایت موردنظر، به گروه IIS_IUSRS مجوز دسترسی به پوشه موردنظر را بدهیم، چون تمام کاربران به صورت پیش‌فرض عضو این گروه می‌باشند برا این کار بر روی Add کلیک کنید.

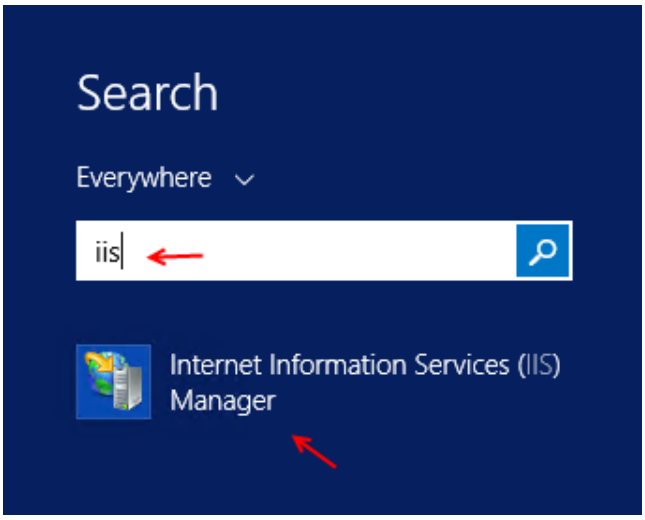


در این قسمت اگر کلمه IIS را وارد کنید و بعد بر روی Check Names کلیک کنید گروه IIS IUSRS به صورت خودکار به لیست اضافه می‌شود، بعد از این کار بر روی Ok کلیک کنید.

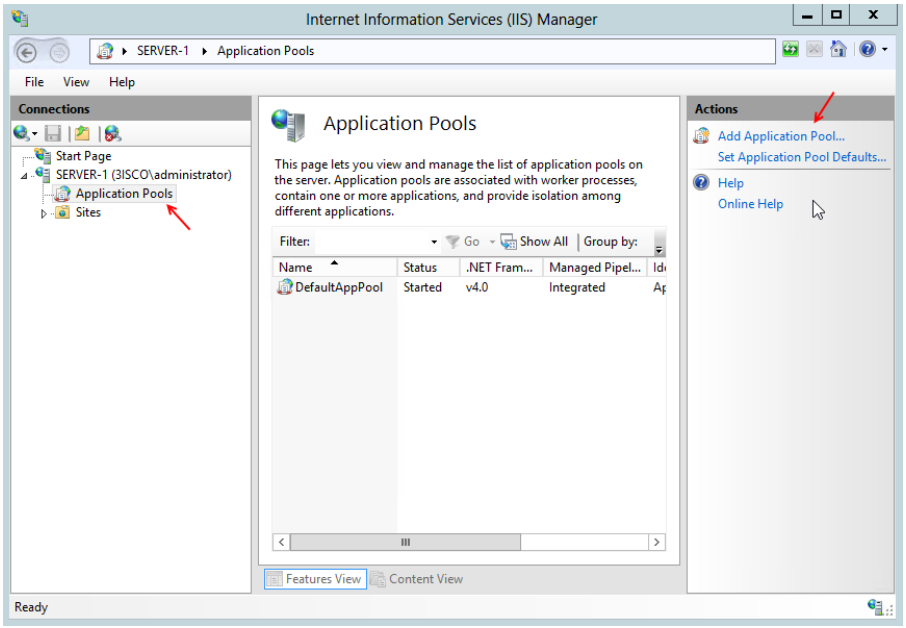


بعد از اضافه شدن گروه موردنظر در لیست، بر روی آن کلیک کنید تا مجوزهای آن مشخص شود، در مجوزهای موردنظر فقط گزینه Read را انتخاب کنید تا کاربران فقط بتوانند سایت موردنظر را اجرا کنند.

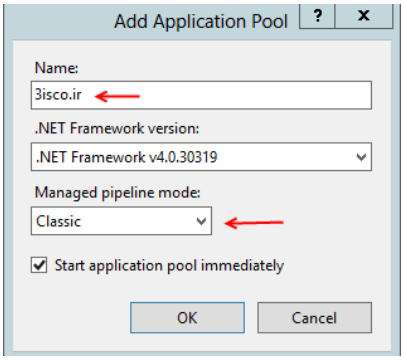
بر روی ok کلیک کنید.

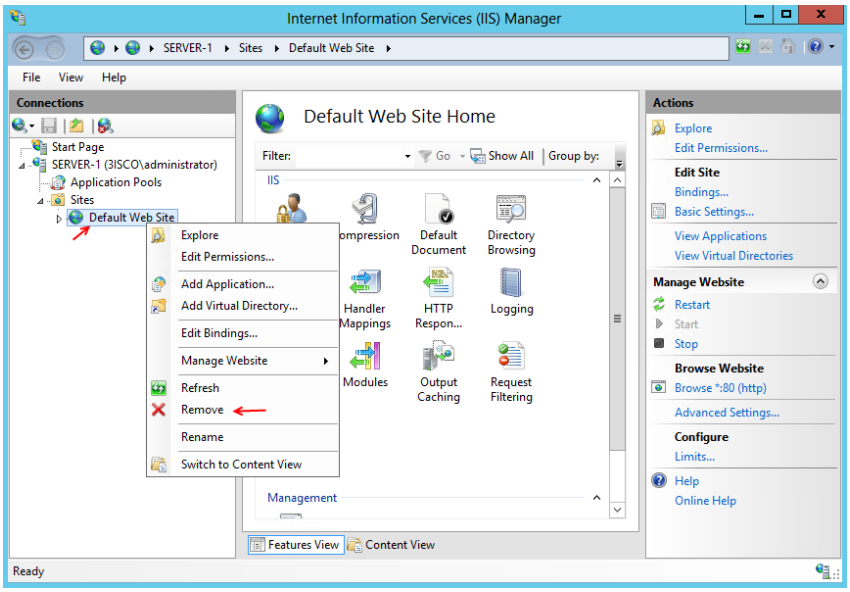


بعد از انجام عملیات قبل وارد Search شوید و کلمه IIS را وارد کنید و در گزینه های موجود بر روی Internet Information Services کلیک کنید.

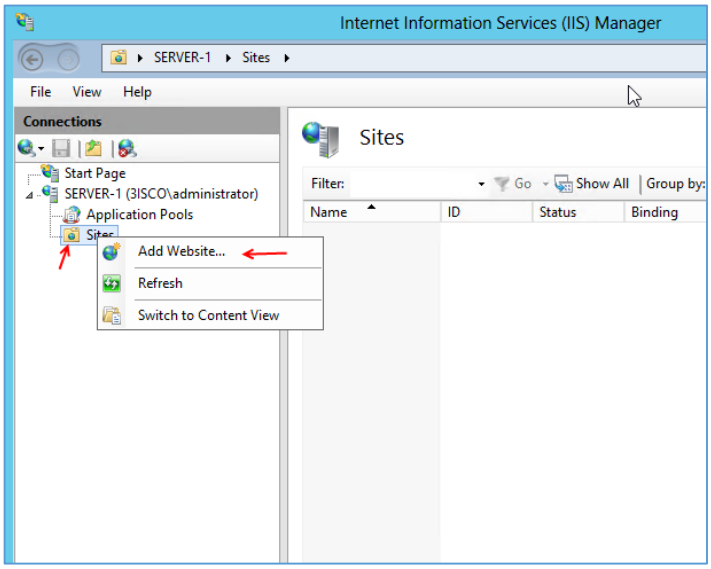


همانطور که در شکل روبرو مشاهده می‌کنید، سرویس IIS به صورت کامل اجرا شده است، برای شروع کار باید یک Application Pool ایجاد کنیم، Application Pool به یک محوطه ای گفته می‌شود که چندین سایت در آن قرار دارند و در کنار هم کار می‌کنند، اگر دو سایت در دو Pool مختلف قرار داشته باشند، هیچ ارتباطی با هم نخواهند داشت و نمی‌توانند با هم ارتباط برقرار کنند، برای شروع از سمت چپ بر روی Application Pools کلیک کنید و گزینه Add Application Pool را انتخاب کنید. در این شکل در قسمت Name نام دلخواه خود را وارد کنید و در قسمت Managed Pipeline Mode که مهمترین بخش می‌باشد حتماً گزینه Classic را انتخاب کنید. و اگر تیک گزینه آخر را انتخاب کنید این Pool بعد از ایجاد شروع به کار می‌کنید و Start می‌شود.

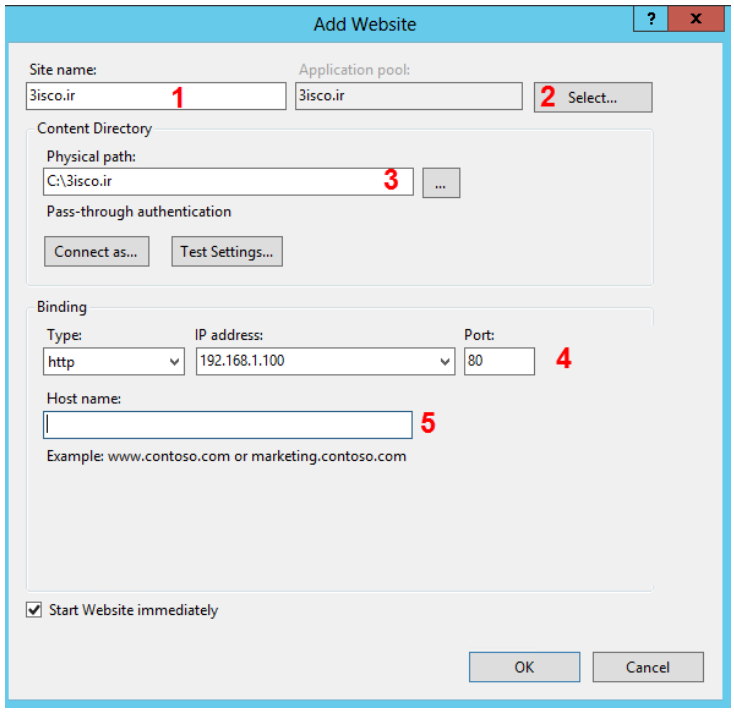




بعد از ایجاد Application Pool وارد بخش Site می‌شویم و به مانند شکل روبرو وب سایت پیش‌فرض با نام Default Web Site وجود دارد که در این قسمت آن را حذف می‌کنیم، بر روی آن کلیک راست کنید و گزینه Remove را انتخاب و بر روی Yes کلیک کنید.



بعد از حذف سایت پیش‌فرض بر روی Site مجدداً کلیک راست کنید و بر روی Add Website کلیک کنید تا شکل بعد ظاهر شود.



در این شکل به ترتیب شماره‌های مشخص‌شده قسمت های مختلف را بررسی می‌کنیم:

1- در این قسمت شما باید نام دلخواه وب سایت خود را وارد کنید.

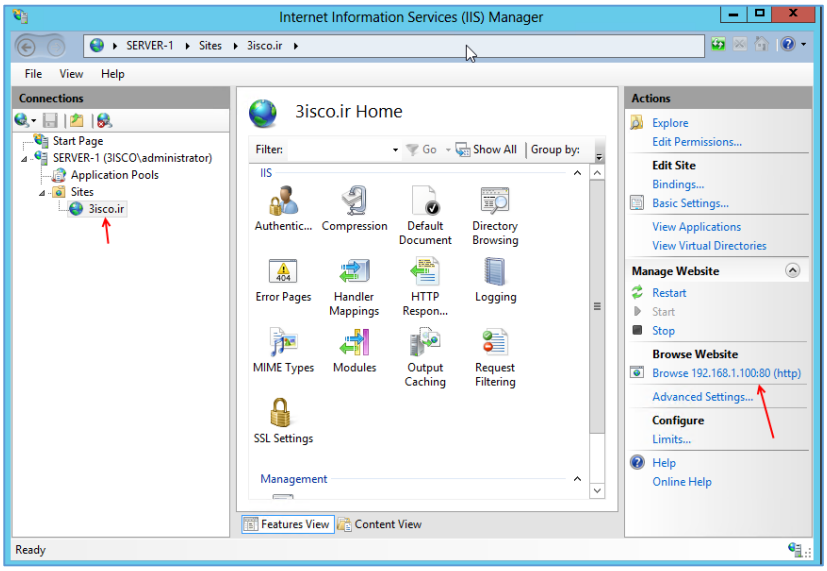
2- در قسمت Application Pool که بسیار مهم می‌باشد شما باید Application Pool که قبلاً با نام 3isco.ir ایجاد کردیم را با کلیک بر روی Select انتخاب کنید.

3- در قسمت Physical Path باید آدرس فیزکی وب سایت خود را در شبکه و یا درایو موردنظر خودتون مشخص کنید، این آدرس را قبلاً ایجاد کردیم و دسترسی های مشخص را به آن تخصیص دادیم.

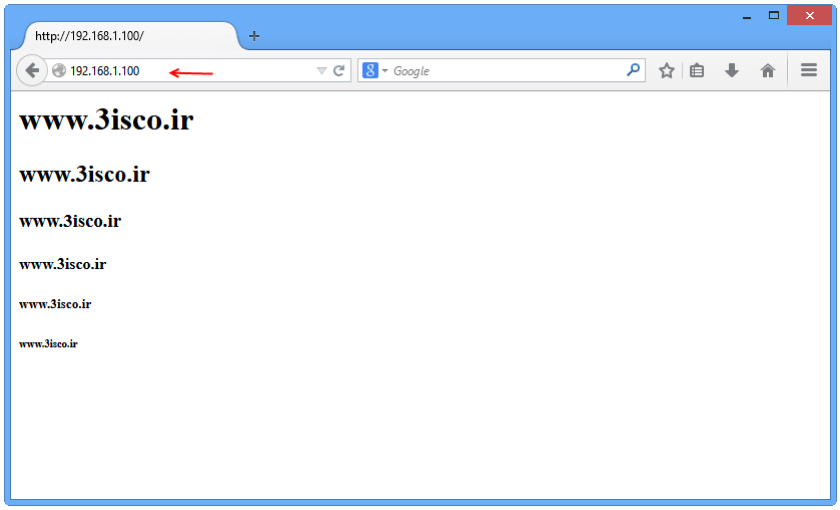
4- در قسمت شماره 4 شما باید نوع http و آدرس سرور را انتخاب کنیدو شماره پورت را بر روی 80 قرار دهید که این شماره پیش‌فرض برای سرویس IIS می‌باشد.

5- در قسمت Host Name باید آدرس وب سایت خود را مشخص کنیم که فعلاً کاری با این قسمت نداریم و در قسمت بعدی این موضوع را بررسی می‌کنیم.

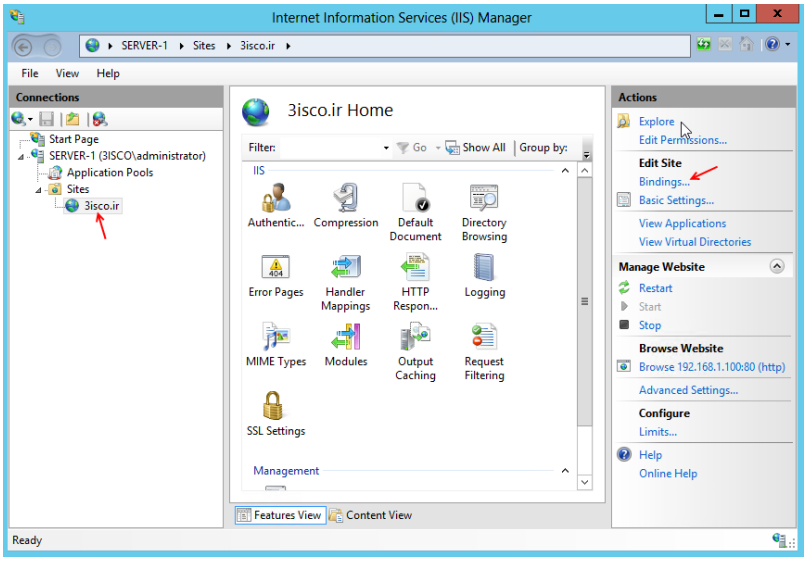
بعد از انجام عملیات بالا بر روی Ok کلیک کنید تا وب سایت موردنظر ایجاد شود.



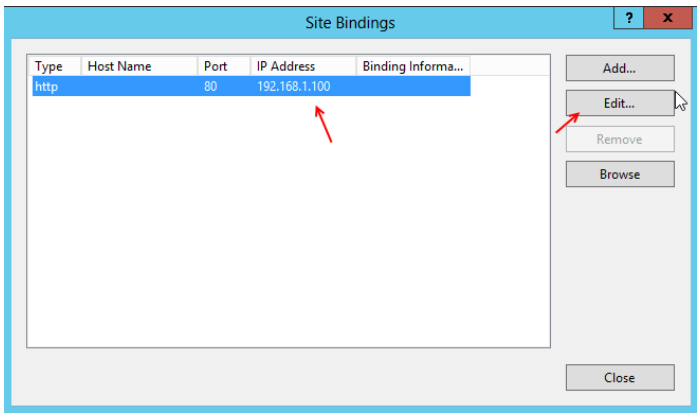
همانطور که در این قسمت مشاهده می‌کنید، وب سایت موردنظر به درستی ایجاد شده است، برای اجرای آن از سمت راست بر روی Browse 192.168.1.100:80 کلیک کنید و یا وارد Internet Explorer شوید و آدرس بالا را در Address bar وارد کنید.



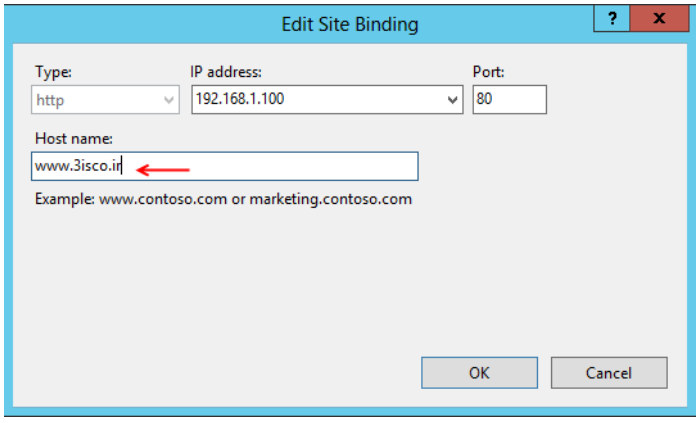
وب سایت موردنظر به درستی اجرا شده است، خوب حالا می‌خواهیم از طریق آدرس، وب سایت را اجرا کنیم، مثلاً با وارد کردن آدرس www.3isco.ir وب سایت موردنظر اجرا شود.



وارد سرویس IIS شوید و وب‌سایت موردنظر خود را انتخاب کنید و از سمت راست بر روی Bindings کلیک کنید.

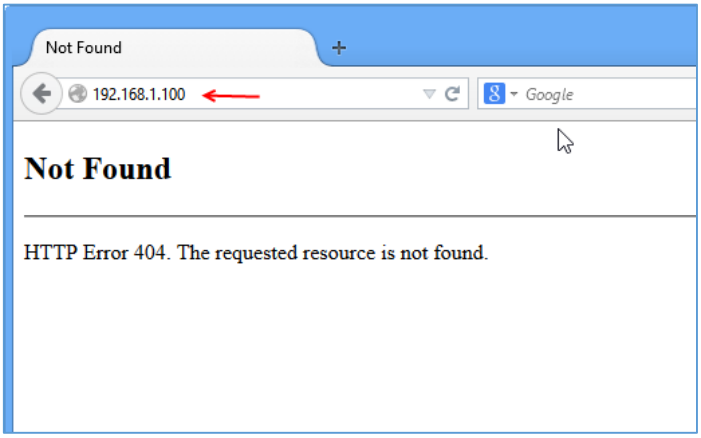


در این شکل بر روی Ip Address موردنظر کلیک کنید و بر روی Edit کلیک کنید تا ویرایش مورد نیاز را انجام دهیم.

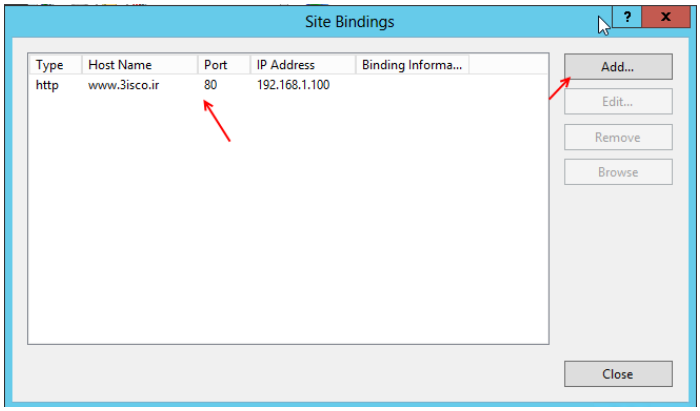


در این صفحه و در قسمت Host name نام وب سایت خود را وارد کنید که در این قسمت آدرس www.3isco.ir وارد شده است.

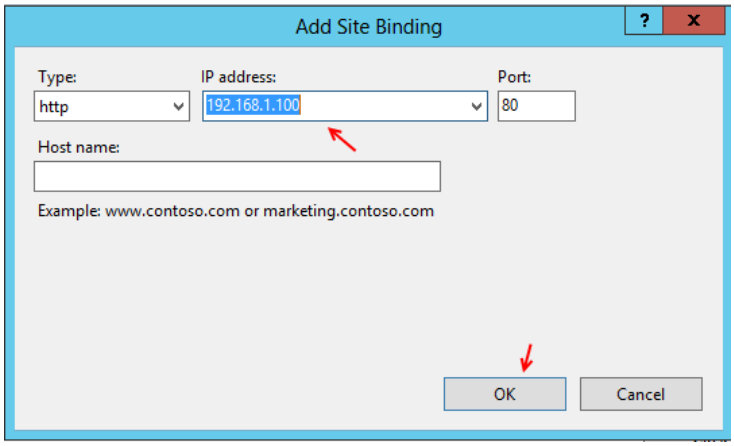
بعد از وارد کردن اطلاعات موردنظر بر روی ok کلیک کنید.



نکته: بعد از این کار دیگر نمی‌توانید از طریق آدرس IP به وب سایت موردنظر دسترسی داشته باشید، همانطور که در شکل روبرو مشاهده می‌کنید، با اجرای IP موردنظر هیچ صفحه‌ای برای نمایش ظاهر نشد.



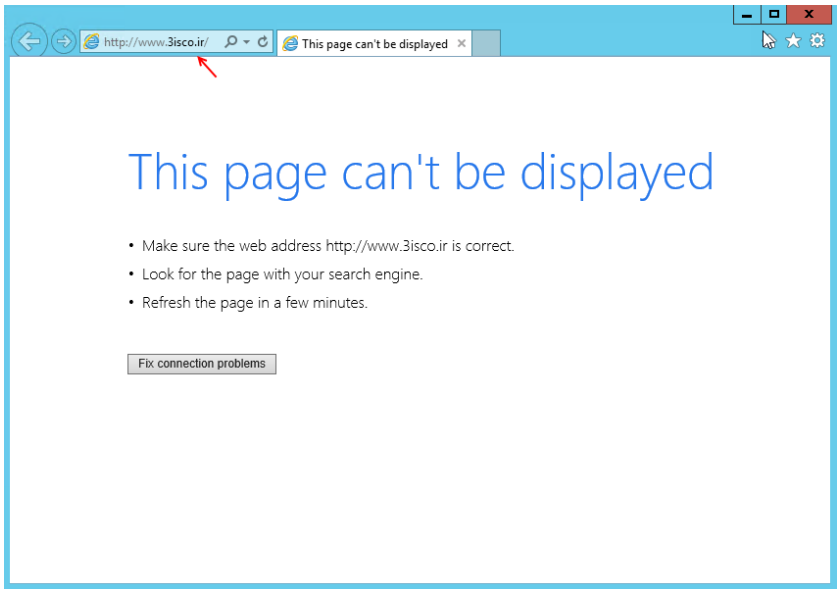
برای حل این مشکل دوباره به قسمت Bindings مراجعه می‌کنیم، همانطور که مشاهده می‌کنید آدرس قبلی که ویرایش کرده بودیم را مشاهده می‌کنید، برای حل مشکل بر روی Add کلیک کنید.



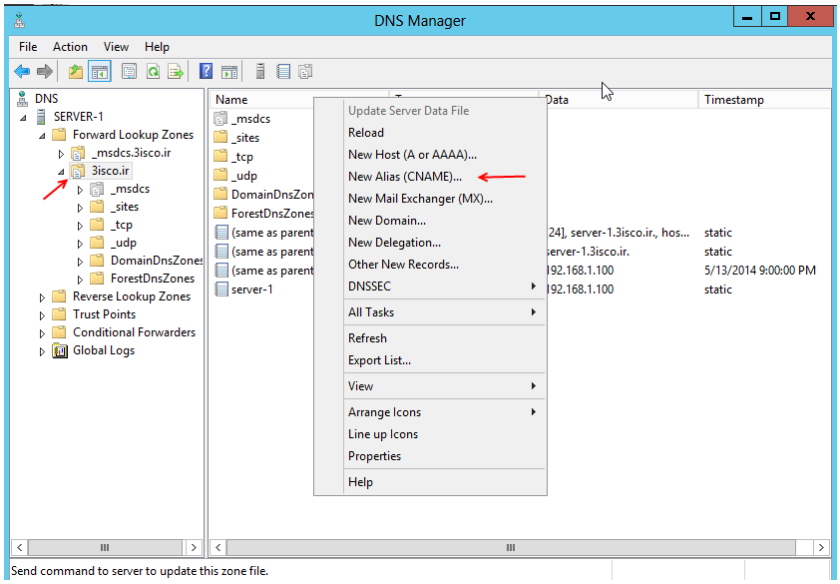
در قسمت Ip address باید آدرس سرور را انتخاب کنید و بر روی ok کلیک کنید، توجه کنید پورت را تغییر ندهید.

بعد از این کار با آدرس IP هم می‌توانید سایت خود را اجرا کنید.

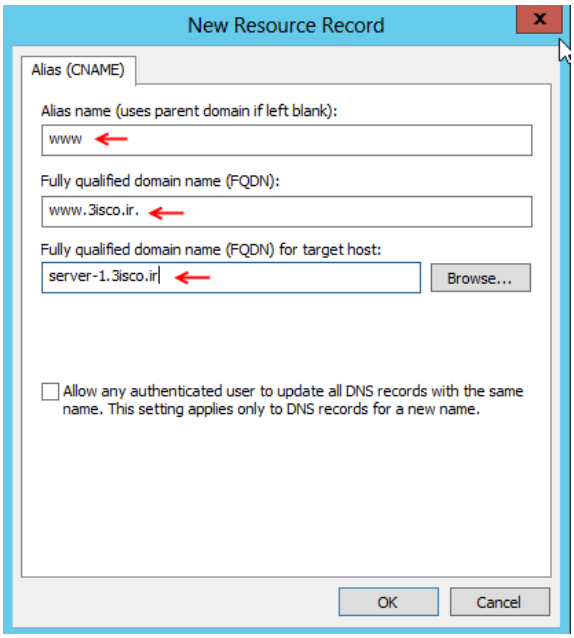
خوب حالا می‌خواهیم وب سایت را با آدرس www.3isco.ir اجرا کنیم، وارد Browser می‌شویم آدرس موردنظر را اجرا می‌کنیم.



همانطور که در شکل روبرو مشاهده می‌کنید با اجرای آدرس موردنظر با پیغام خطای This page can't... مواجه شدیم که این مشکل به خاطر این است که سرور آدرس www.3isco.ir را نمی‌شناسد، همانطور که قبلاً گفتیم سرویس DNS کار بررسی آدرس و IP را انجام می‌دهد و باید در این سرویس تعریف شود.

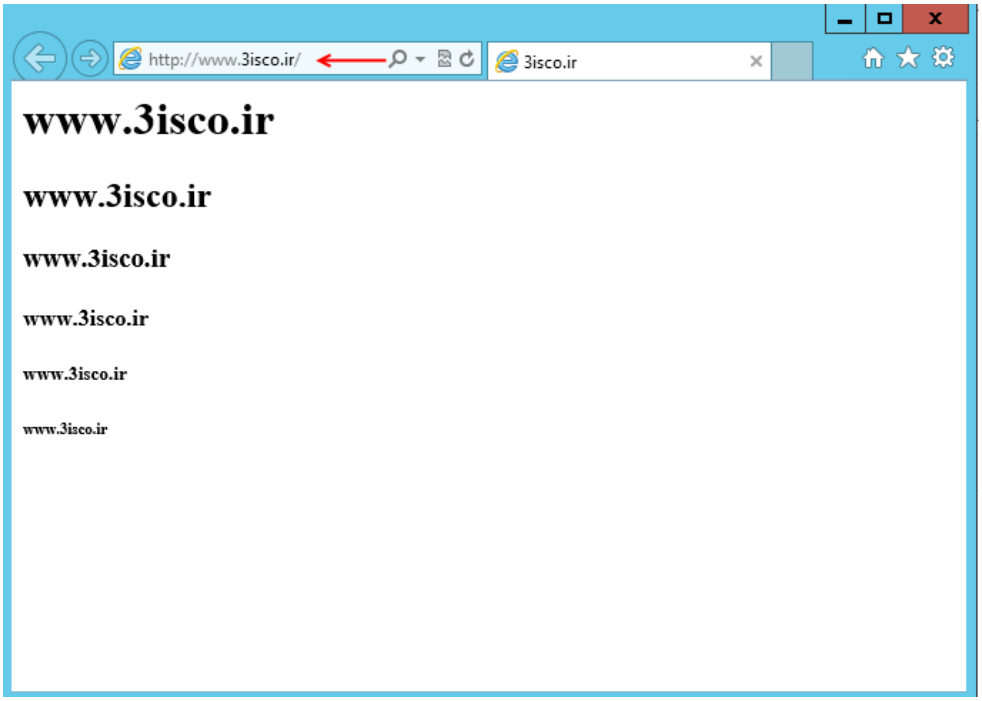


برای حل این مشکل وارد سرویس DNS می‌شویم. در این قسمت از قبل Zone با نام 3isco.ir قبلاً ایجاد شده است، شما باید Zone را از قبل ایجاد کنید، برای درک این موضوع به بخش بررسی سرویس DNS



مراجعه کنید. در ادامه برروی 3isco.ir کلیک می‌کنیم و در صفحه باز شده کلیک راست کرده و گزینه CNAME را انتخاب می‌کنیم.

در این صفحه و در قسمت Alias Name کلمه www را وارد کنید که همزمان در قسمت Fully Qualified آدرس www.3isco.ir به صورت خودکار درج می‌شود، در قسمت Host بر روی Browse کلیک کنید و در صفحه باز شده وارد دومین 3isco.ir شوید و کامپیوتر سرور را انتخاب کنید این کار به این منظور است که کاربر بعد از اجرای آدرس www.3isco.ir به کدام کامپیوتر هدایت شود. بر روی ok کلیک کنید.

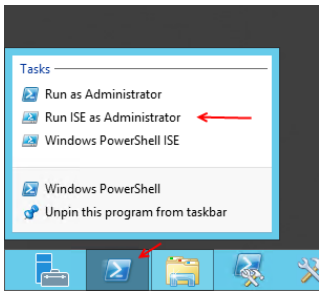


همانطور که در این قسمت مشاهده می‌کنید، بعد از انجام تنظیمات موردنظر در سرویس DNS سایت موردنظر از طریق سرویس DNS اجرا شده است.

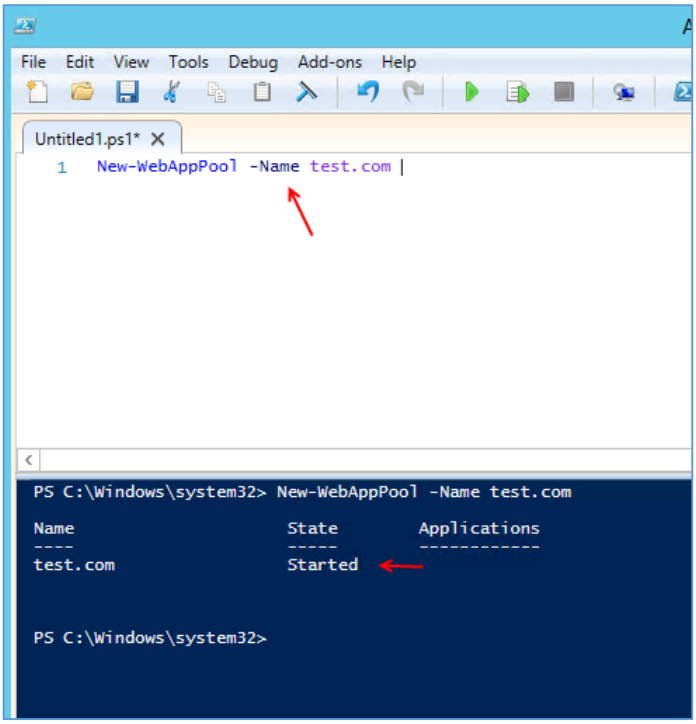
تا این قسمت سرویس IIS را فعال و توانستیم سایت خود را راه‌اندازی و از طریق IP و آدرس اجرا کنیم.

در ادامه با یک سری دستورات Powershell برای کار با سرویس IIS آشنا می‌شویم.

استفاده از دستورات PowerShell در سرویس IIS:



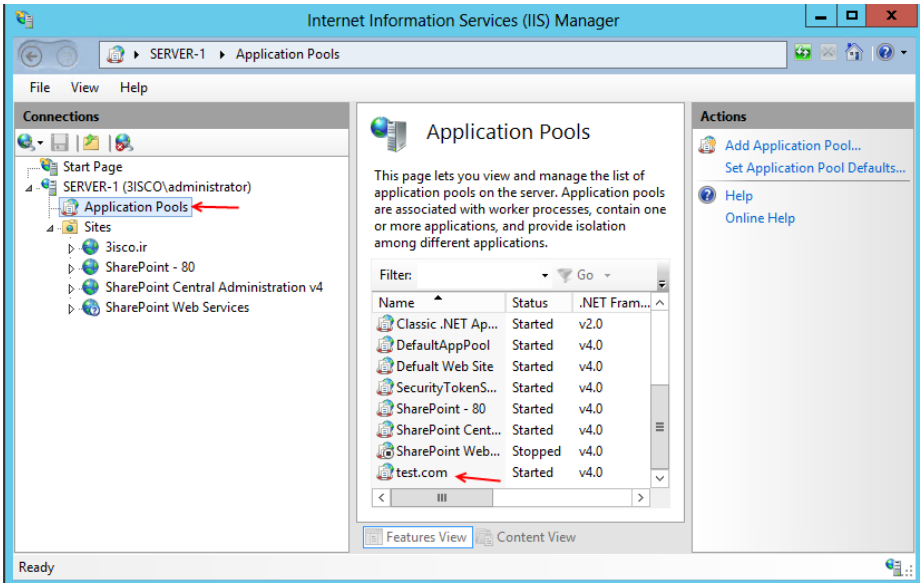
در این قسمت می خواهیم از طریق دستورات PowerShell یک وب سایت را به صورت کامل ایجاد کنیم، برای این کار روی نوار Taskbar بر روی آیکون PowerShell کلیک راست کنید و گزینه Run ISE as Administrator را انتخاب کنید.



برای شروع، اول یک Pool با نام وب سایت جدید خود از طریق دستور زیر ایجاد می‌کنیم:

```
New-WebAppPool -Name test.com
```

در دستور بالا New-WebAppPool برای ایجاد Pool به کار می‌رود و بعد از آن با دستور name– باید نام AppPool خود را وارد کنید که در ایجاد Test.com وارد شده است.

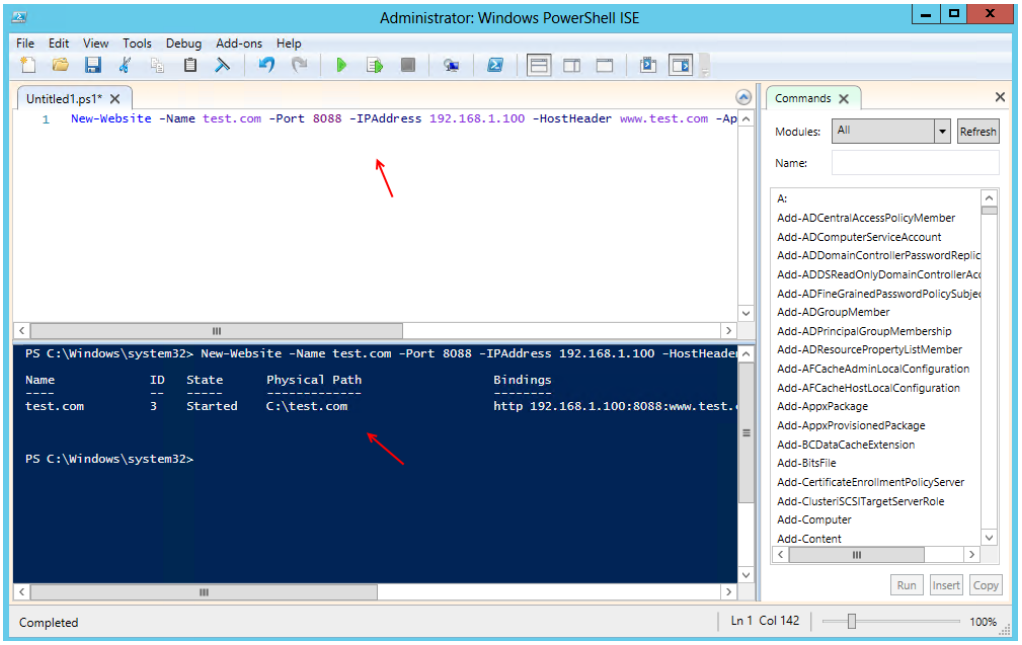


اگر وارد سرویس IIS شویم و به قسمت Application Pools مراجعه کنید، مشاهده خواهید کرد که Pool موردنظر با نام Test.com ایجاد شده است.

بعد از ایجاد Pool باید وب سایت خود را ایجاد کنیم، برای این کار دوباره وارد PowerShell می‌شویم و از دستورات زیر استفاده می‌کنیم:

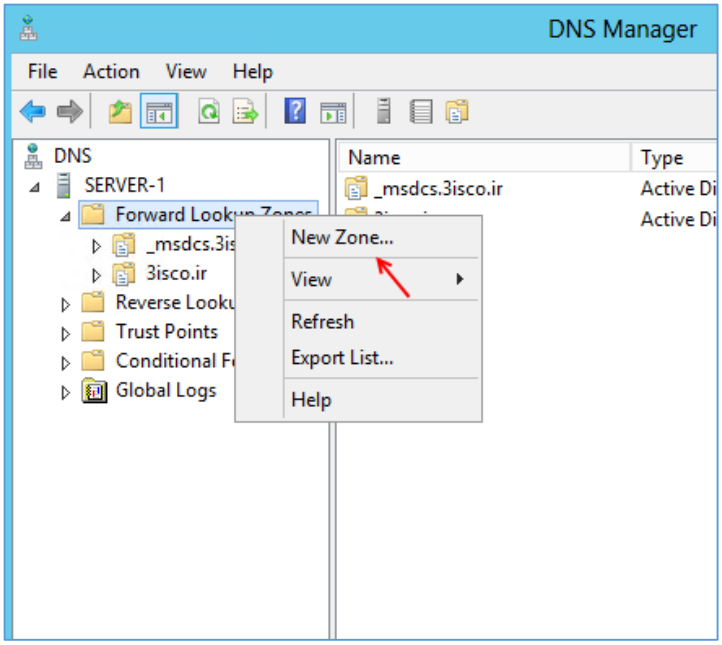
```
New-Website -Name test.com -Port 8088 -IPAddress 192.168.1.100 -HostHeader
www.test.com -ApplicationPool test.com -PhysicalPath C:\test.com
```

با استفاده از دستورات بالا یک وب سایت با نام Test.com ایجاد می‌شود، این دستورات را با هم بررسی می‌کنیم، با دستور New-Website شروع می‌کنیم این دستور برای ایجاد یک وب سایت جدید به کار می‌رود، بعد از این دستور تمام دستورات بعدی زیر مجموعه این دستور و یا تنظیمات مربوط به ایجاد سایت جدید می‌باشد، با دستور Name نام سایت را وارد می‌کنیم که در اینجا test.com وارد شده است. دستور بعدی برای تعریف Port مربوط به این وب سایت می‌باشد که اگر یادتان باشد در قسمت قبل که وب سایت 3isco.ir را ایجاد کردیم به صورت پیشفرض پورت 80 به آن نسبت داده شده است و در کل این پورت اشغال شده است، برای همین باید یک پورت جدید ایجاد کنیم که در این دستور از پورت 8088 استفاده کردیم، در ادامه با دستور IP Address باید آدرس IP سروری که این وب سایت روی آن فعال می‌شود را وارد کنیم، با دستور HostHeader باید آدرس وب سایت خود را وارد کنیم که در این دستور www.test.com وارد شده است، در ادامه باید ApplicationPool را که قبلا با نام test.com ایجاد کرده‌ایم معرفی کنیم. و در آخر باید آدرس فیزیکی وب سایت خود را که فایل‌های موردنظر در آن قسمت قرار دارد را وارد کنید. نکته مهم در این قسمت این است که به مانند قبل که بر روی پوشه 3isco.ir به گروه IIS_IUSRS مجوز Read دادیم به این پوشه هم همین مجوز را بدهید.



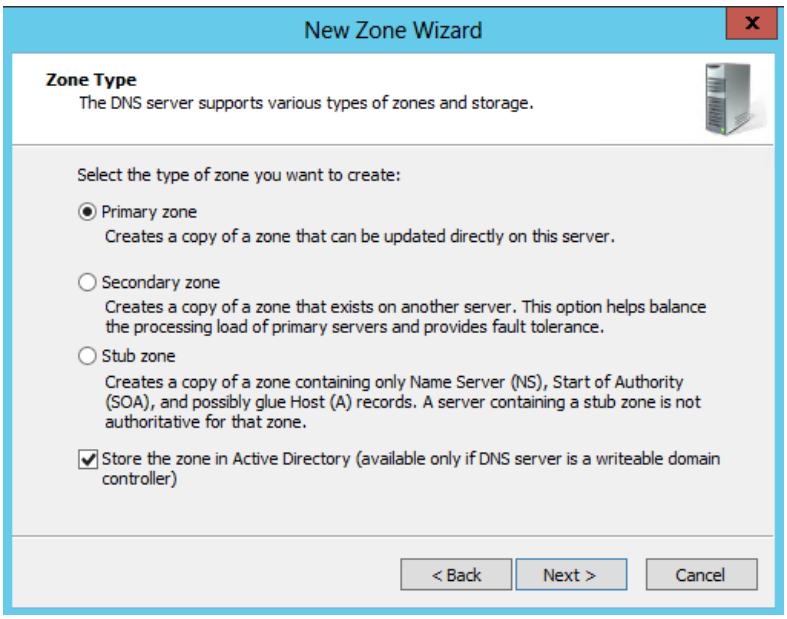
همانطور که در شکل روبرو مشاهده می‌کنید، دستور بالا در این قسمت به صورت صحیح اجرا شده و نتیجه آن را در قسمت پائینی شکل مشاهده می‌کنید.

بعد از اجرای دستورات بالا نوبت به اجرای سایت می‌باشد، اگر وارد Internet Explorer شوید و آدرس سایت را وارد کنید مشخصاً با Error مواجع خواهید شد، این موضوع به خاطر این است که هنوز آدرس www.test.com توسط سرویس DNS قابل شناسایی نیست، پس باید در سرویس DNS یک Zone با نام test.com ایجاد کنیم و تنظیمات آن را انجام دهیم.



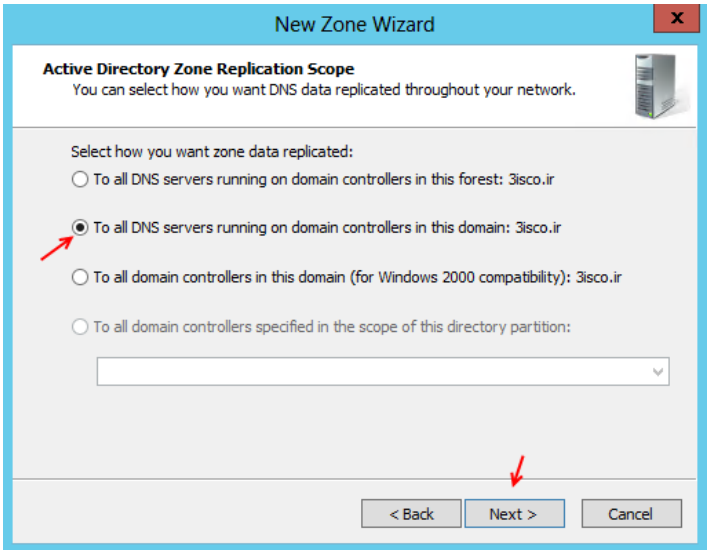
وارد سرویس DNS شوید و در قسمت Forward Lookup Zone کلیک راست کرده و گزینه New Zone را انتخاب کنید.

درصفحه باز شده بر روی Next کلیک کنید تا شکل بعد ظاهر شود.

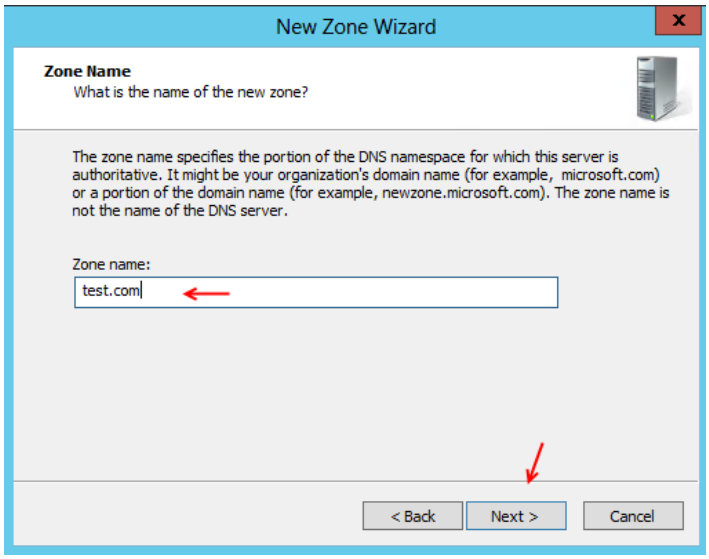


در این صفحه گزینه Primary Zone را انتخاب کنید، چون Zone اصلی می‌باشد و زیر مجموعه Zone دیگری نمی‌باشد.

بر روی Next کلیک کنید..

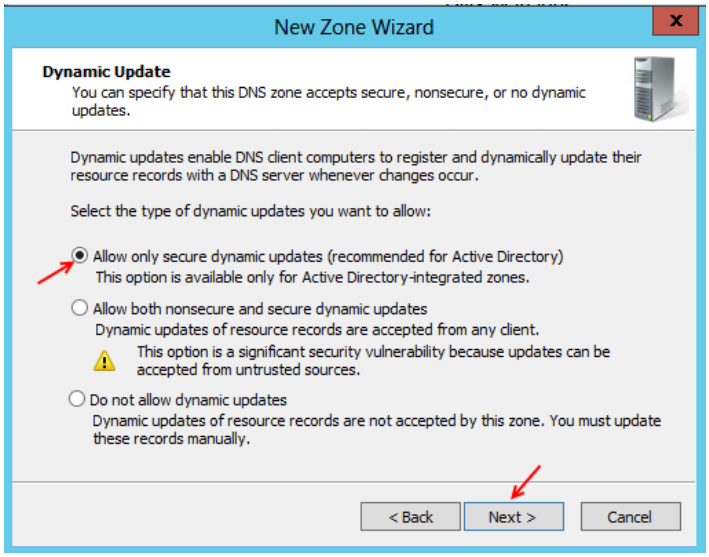


در این قسمت، گزینه دوم را انتخاب و بر روی Next کلیک کنید..



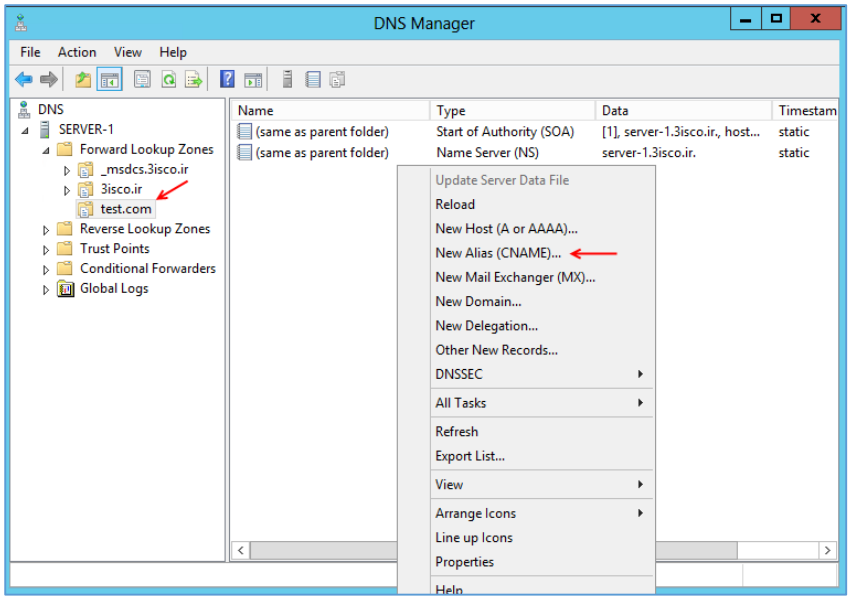
در این صفحه باید نام Zone خود را وارد کنید که در اینجا Test.com وارد شده است.

بر روی Next کلیک کنید.....

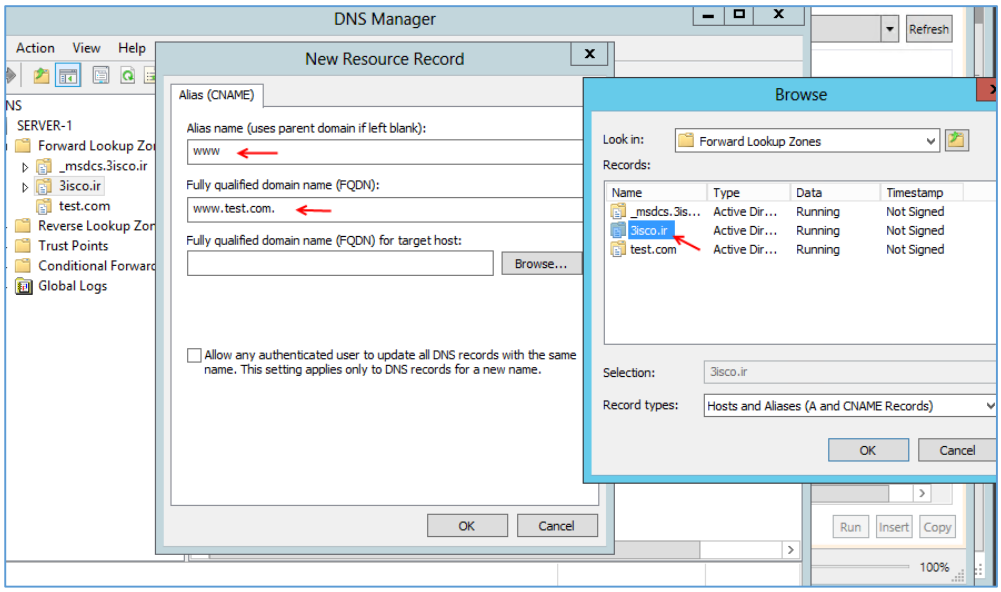


در این قسمت گزینه اول را انتخاب کنید و بر روی Next کلیک کنید.

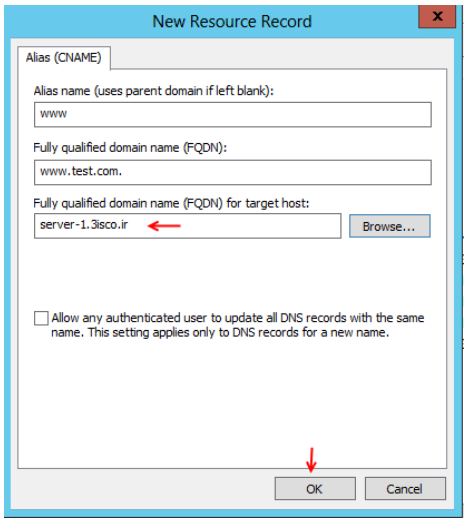
در صفحه بعد هم بر روی Finish کلیک کنید تا Zone موردنظر با نام Test.com ایجاد شود.



بعد از ایجاد Zone موردنظر از سمت چپ به مانند شکل روبرو بر روی آن کلیک کنید و در صفحه باز شده کلیک راست کنید و گزینه New Alias(CNAME) را انتخاب کنید تا نام www را قبل از نام Test.com وارد کنیم.

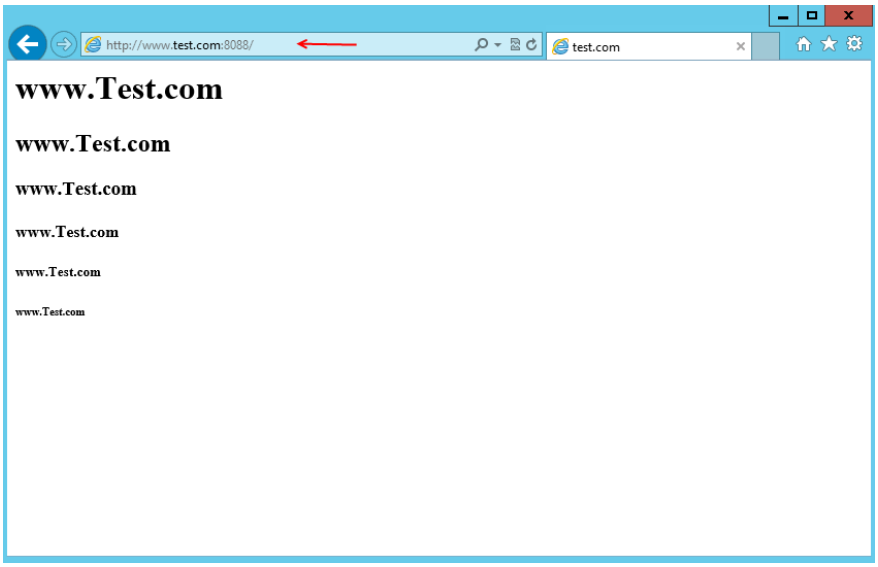


در صفحه New Resource Record باید در قسمت Alias name نام WWW را وارد کنید و با کلیک بر روی Browse شکل آن ظاهر می‌شود که باید وارد دومین اصلی شوید و سرور اصلی که وب سایت روی آن قرار دارد را انتخاب کنید.



همانطور که در این قسمت مشاهده می‌کنید، نام سرور اصلی انتخاب شده است، بعد از این کار بر روی ok کلیک کنید تا Cname موردنظر ایجاد شود.

بعد از این کار می‌توانید آدرس www.test.com را اجرا کنید.

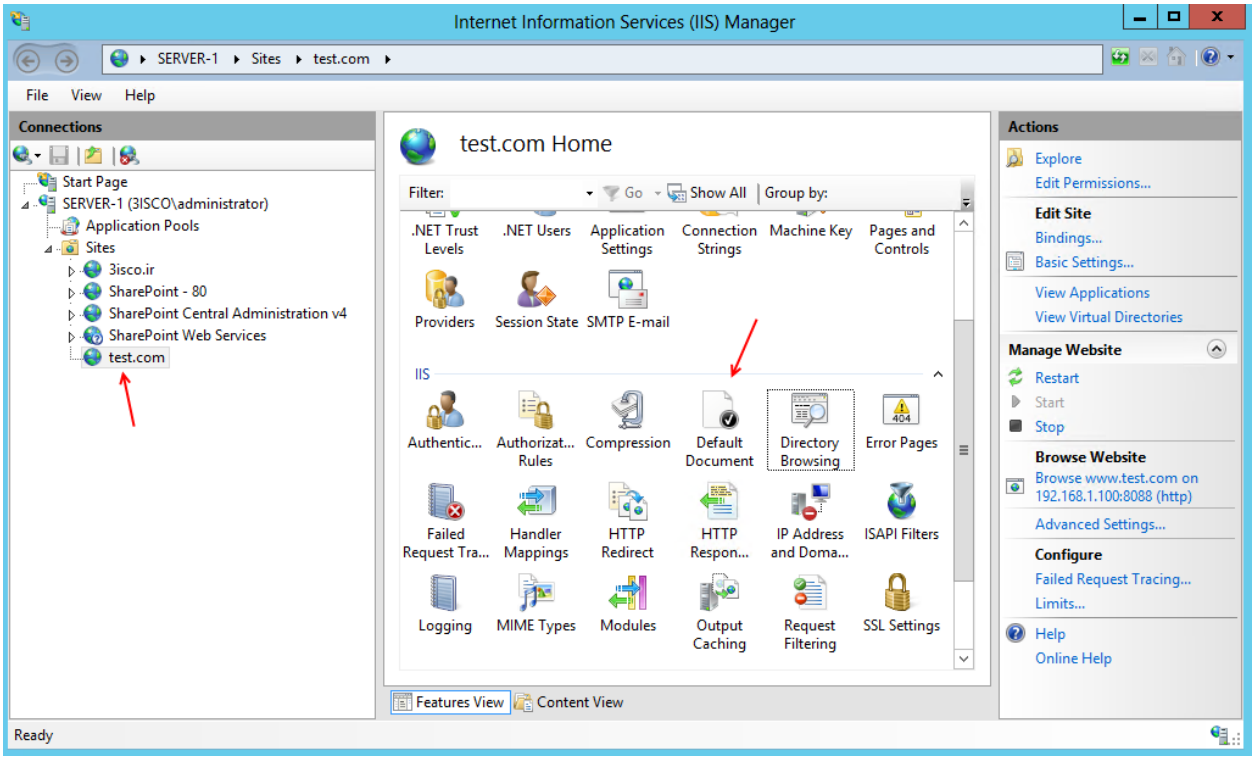


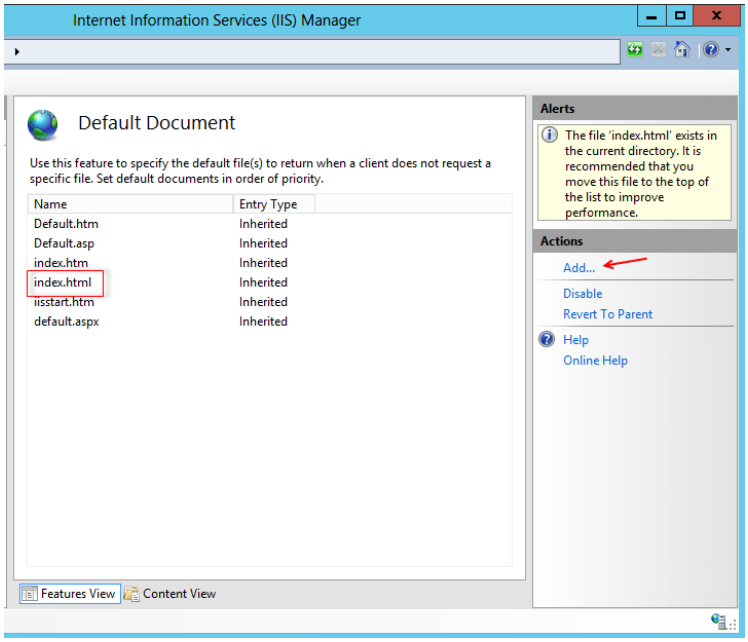
همانطور که مشاهده می‌کنید، با اجرای آدرس

http://www.test.com:8088

صفحه اول سایت موردنظر اجرا شده است. به همین سادگی...

خوب شاید بگوئید که چگونه وب سایت موردنظر متوجه می‌شود که چه صفحه‌ای را باید به عنوان صفحه اصلی خود انتخاب کند، درباره این موضوع در اوایل بررسی سرویس IIS کمی بحث کردیم، برای روشن تر شدن این موضوع وارد سرویس IIS می‌شویم و بر روی یکی از وب سایت‌های ایجاد شده کلیک می‌کنیم و در صفحه باز شده به مانند شکل زیر بر روی Default Document کلیک می‌کنیم.



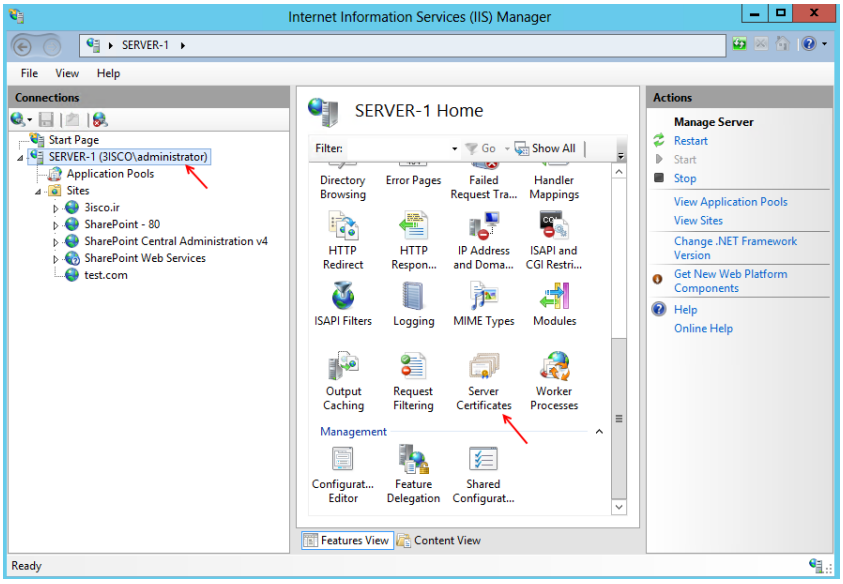


در این قسمت چند نوع فایل با اسم‌های مختلف وجود دارد، اگر توجه کرده باشید فایل صفحه اول ما برای وی سایت‌ها Index.html بود که در این صفحه هم این گزینه وجود دارد یعنی اگر این گزینه را حذف کنیم، دیگر وب سایت‌های ما اجرا نخواهد شد، در این قسمت هم می‌توانید با کلیک بر روی Add یک نام مشخص با پسوند آن ایجاد کنید.

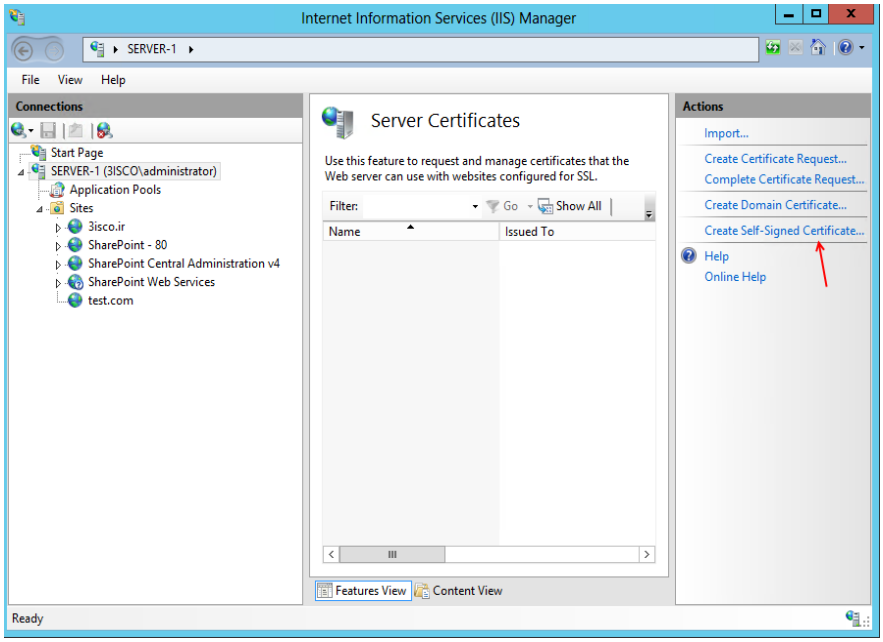
دسترسی به سایت از طریق پروتکل SSL:

یکی از راه های امن کردن سایت ها در سرور ها استفاده از پروتکل محبوب و دوست داشتنی SSL می‌باشد که شما آن را در اینترنت با نام HTTPS می‌شناسید که سایت هایی مانند گوگل، فیس بوک و دیگر سایت ها از این پروتکل استفاده می‌کنند.

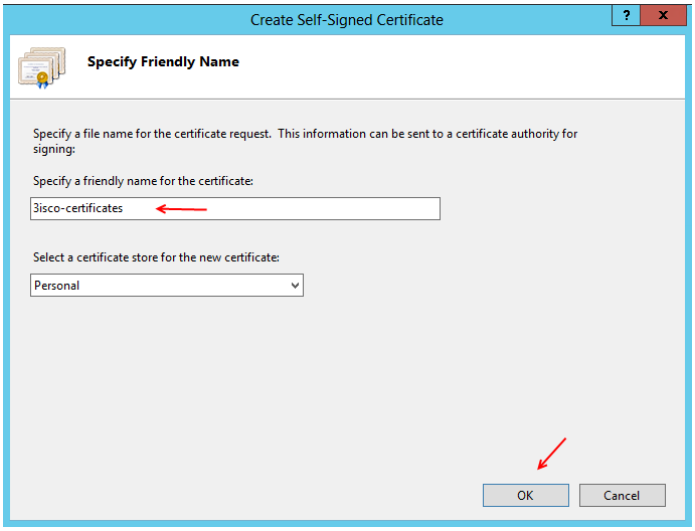
برای شروع کار وارد سرور اصلی می‌شویم و سرویس IIS را اجرا می‌کنیم. شما میتوانید نام این سرویس را در Search وارد کنید تا به سرویس موردنظر دست پیدا کنید و آن را اجرا کنید.



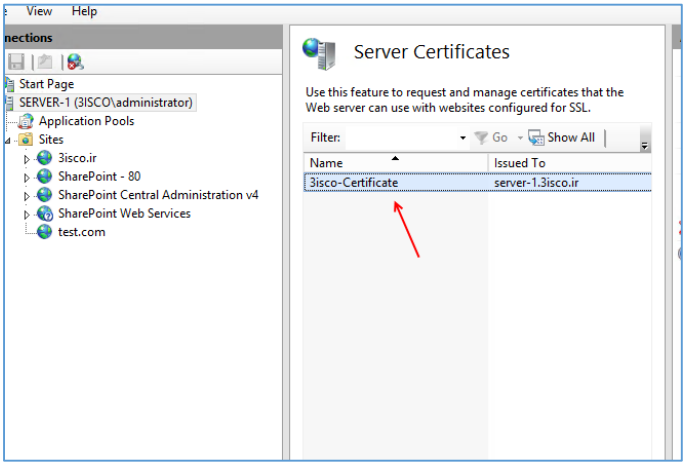
در این صفحه بر روی سرور خود کلیک می‌کنیم و در سمت راست بر روی گزینه Server Certificates دو بار کلیک می‌کنیم تا اجرا شود.



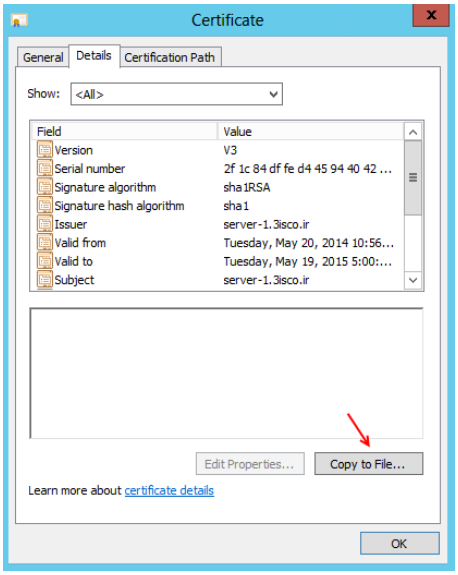
در این قسمت بر روی Create Self-Signed Certificates کلیک کنید تا شکل بعد ظاهر شود.



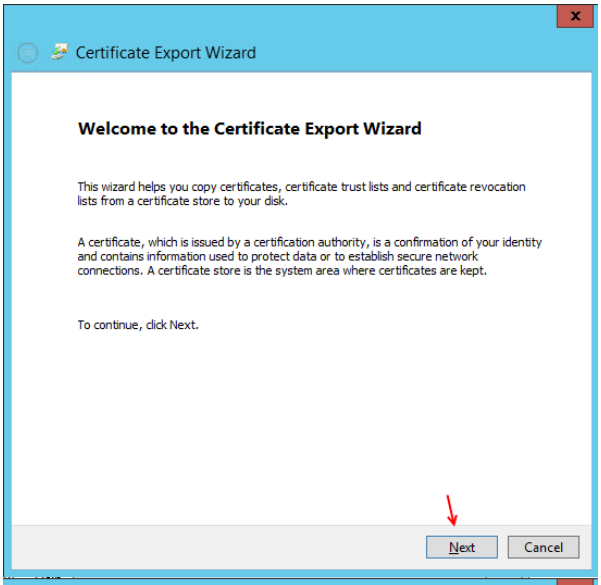
در این قسمت نام موردنظر خود را وارد و بر روی ok کلیک کنید.



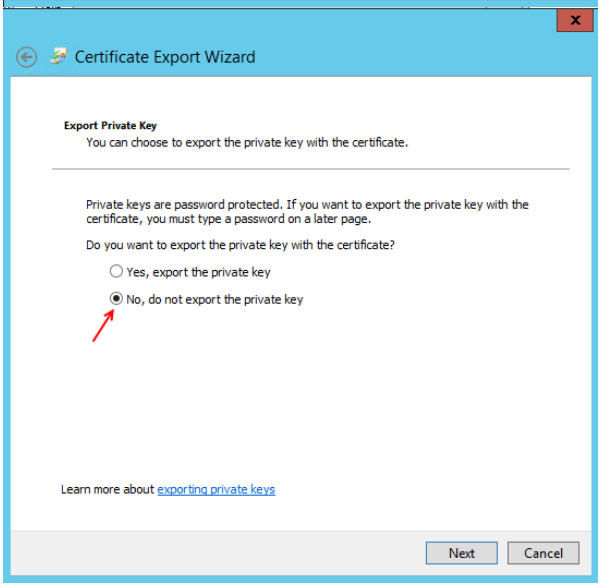
بعد از ایجاد Certificates موردنظر بر روی آن دو بار کلیک کنید تا اجرا شود.



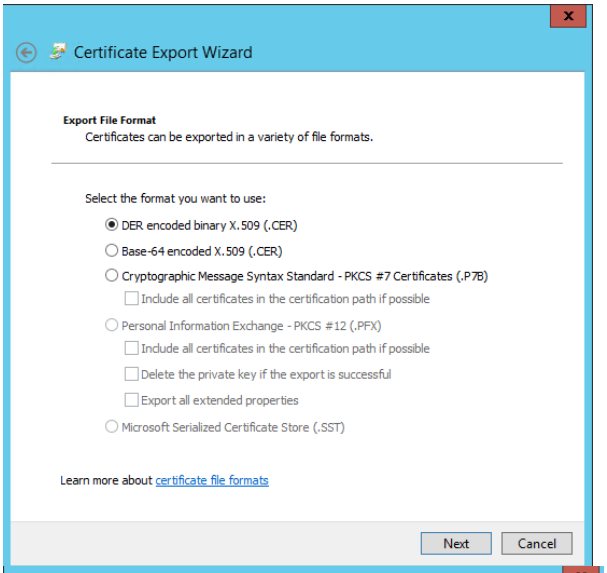
در این قسمت به تب Details می‌رویم و بر روی Copy To File کلیک می‌کنیم.



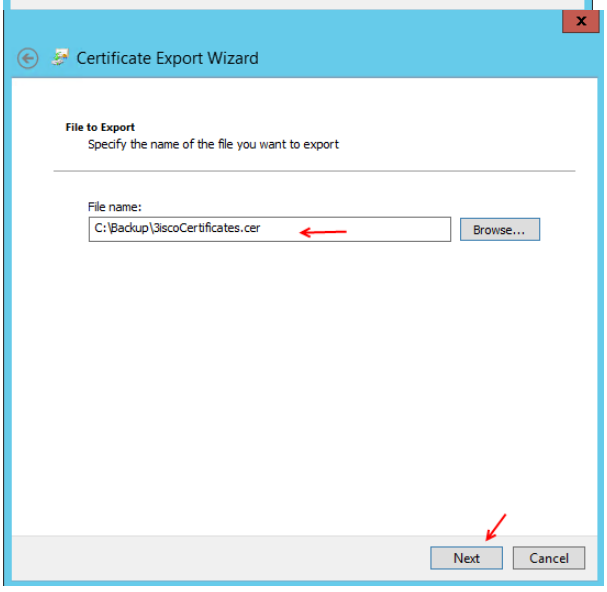
دراین صفحه بر روی next کلیک کنید.



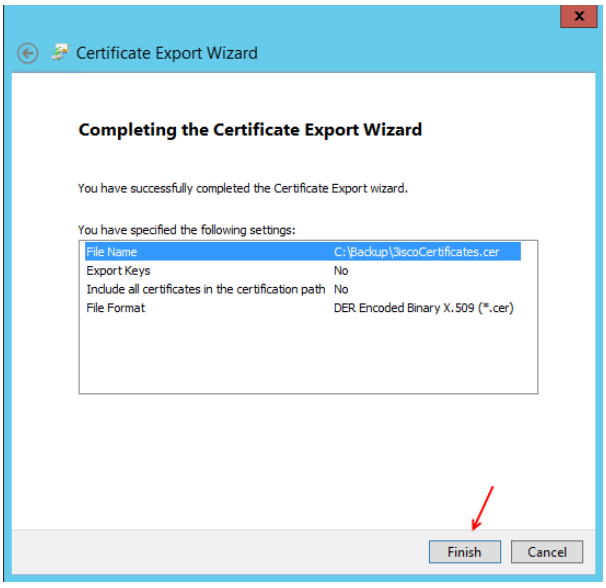
در این صفحه گزینه دوم را انتخاب کنید و بر روی Next کلیک کنید، گزینه اول برای ذخیره سازی Private Key هستش که فعلا کاربردی برای ما ندارد.



این قسمت مربوط به نوع فایل می‌باشد که باید ذخیره کنیم، برای این کار گزینه اول را انتخاب می‌کنیم و بر روی Next کلیک می‌کنیم.



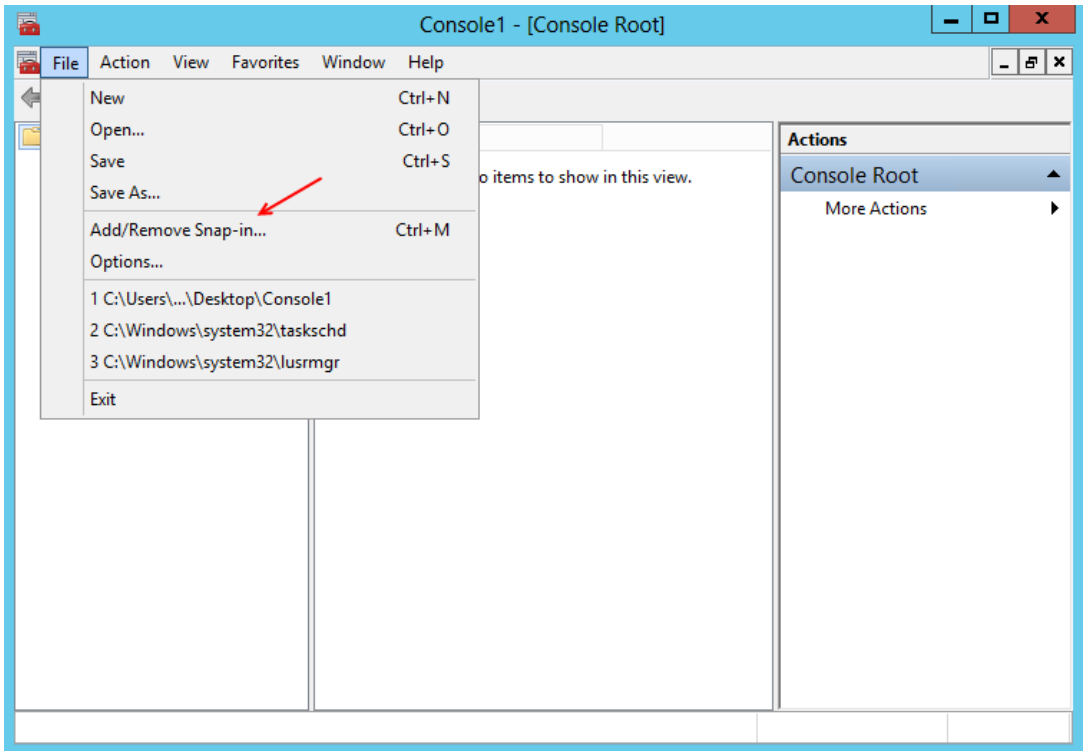
در این قسمت آدرس محل ذخیره سازی این فایل را مشخص می‌کنیم و بر روی Next کلیک می‌کنیم.

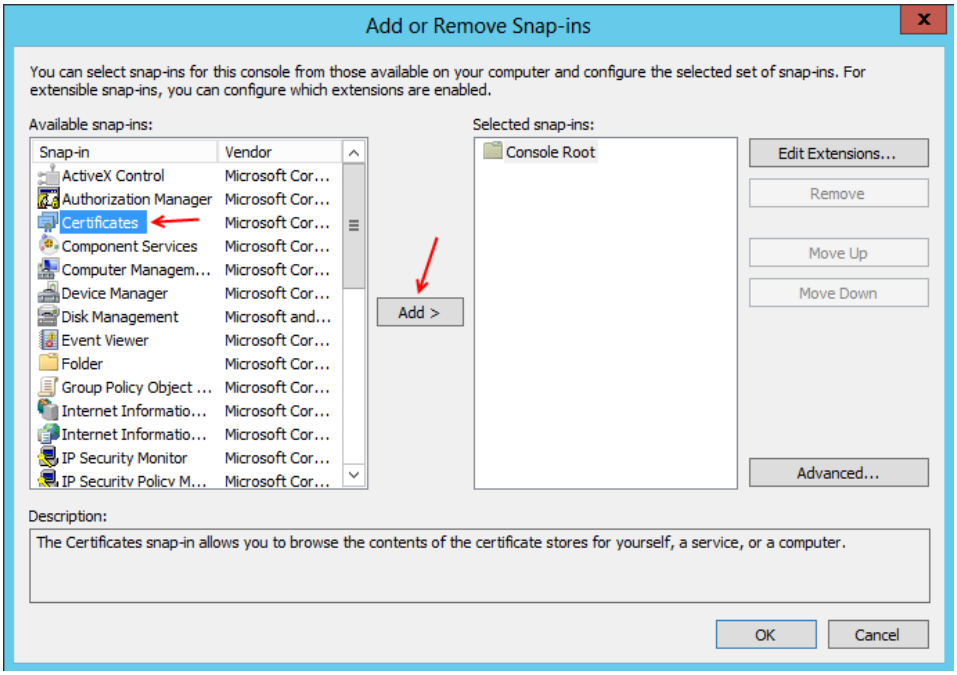


در این قسمت هم بر روی Finish کلیک کنید.

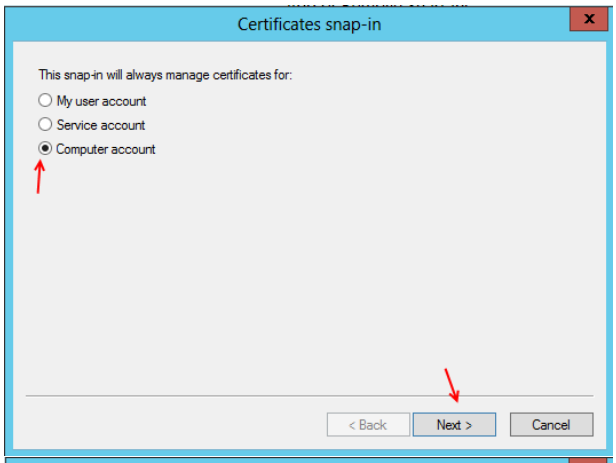
خوب تا اینجا فایل Certificate را ایجاد و در محل مناسب آن را ذخیره کردیم، حالا باید وارد سرویس Certificate شویم و این فایل را به آن معرفی کنیم.

وارد Search شوید و دستور MMC را اجرا کنید تا کنسول مدیریتی مایکروسافت اجرا شود، بعد از اجرا به مانند شکل از منوی File گزینه Add/Remove Snap-in را انتخاب کنید.

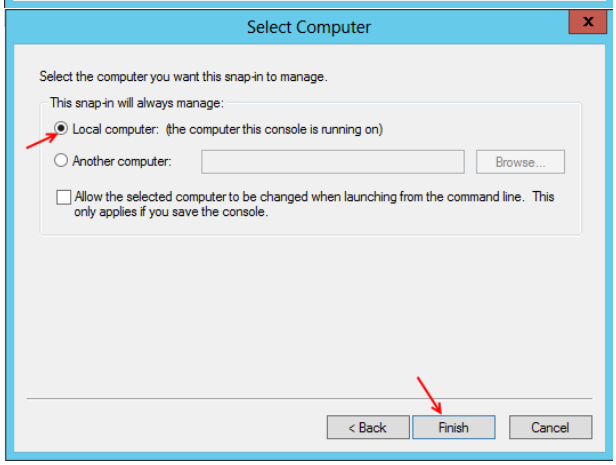




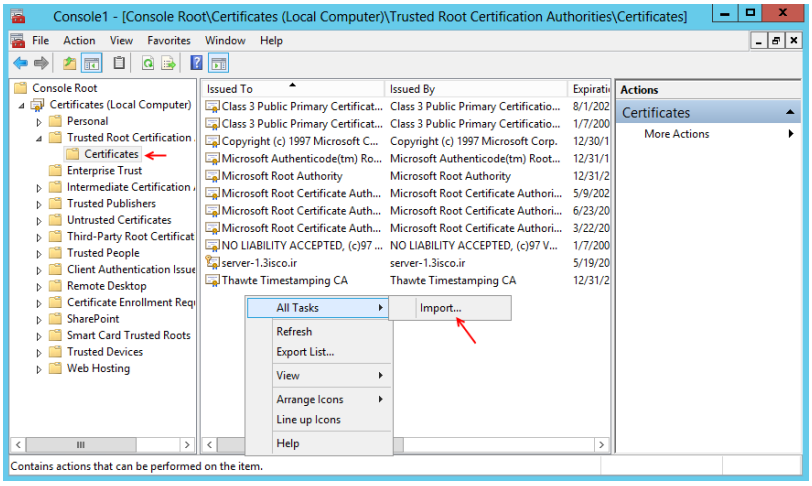
در این صفحه از لیست سرویس های سمت چپ گزینه Certificates را انتخاب کنید و بر روی Add کلیک کنید.



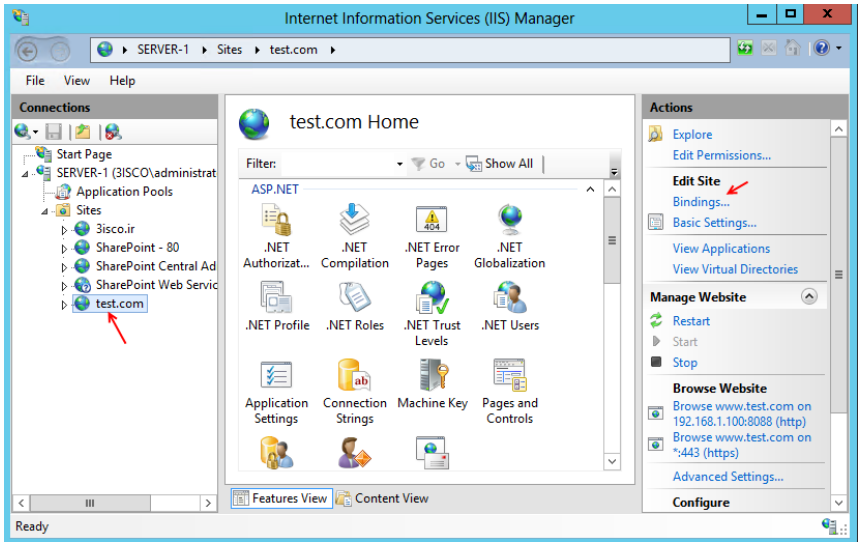
در این قسمت گزینه Computer Account را انتخاب کنید و بر روی Next کلیک کنید.



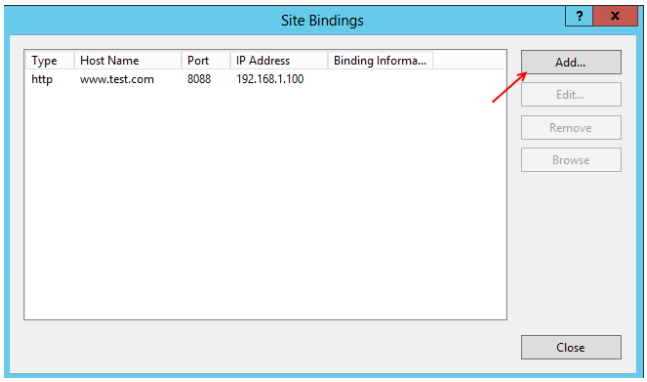
در این صفحه گزینه Local Computer را انتخاب و بر روی Next کلیک کنید.



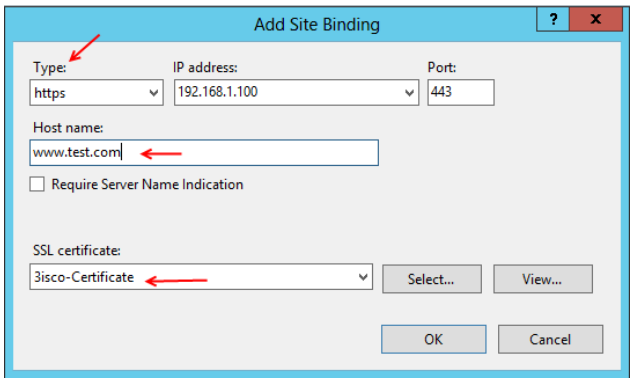
همانطور که مشاهده می‌کنید به سرویس Certificates متصل شده ایم، برای ادامه کار از لیست سمت چپ گزینه Trusted Root Certification را انتخاب و بعد بر روی Certificates را انتخاب کنید، بعد از انتخاب لیستی از Certificate های ویندوز را مشاهده خواهید کرد در جای خالی کلیک راست کنید و از قسمت All Tasks گزینه Import را انتخاب کنید و فایل Certificate که قبلاً ایجاد کرده ایم را انتخاب و بر روی ok کلیک می‌کنیم، با این کار Certificate موردنظر در سرویس Certificate قابل اعتماد می‌باشد و زمانی که بخواهیم از آن استفاده کنیم، به ما Error نخواهد داد.



بعد از انجام کارهای صفحات قبل وارد IIS می‌شویم و از سمت چپ سایت موردنظر خود را انتخاب و از سمت راست بر روی Bindings کلیک می-کنیم.



در این قسمت باید پروتکل https را به لیست اضافه کنیم برای این کار بر روی Add کلیک کنید.

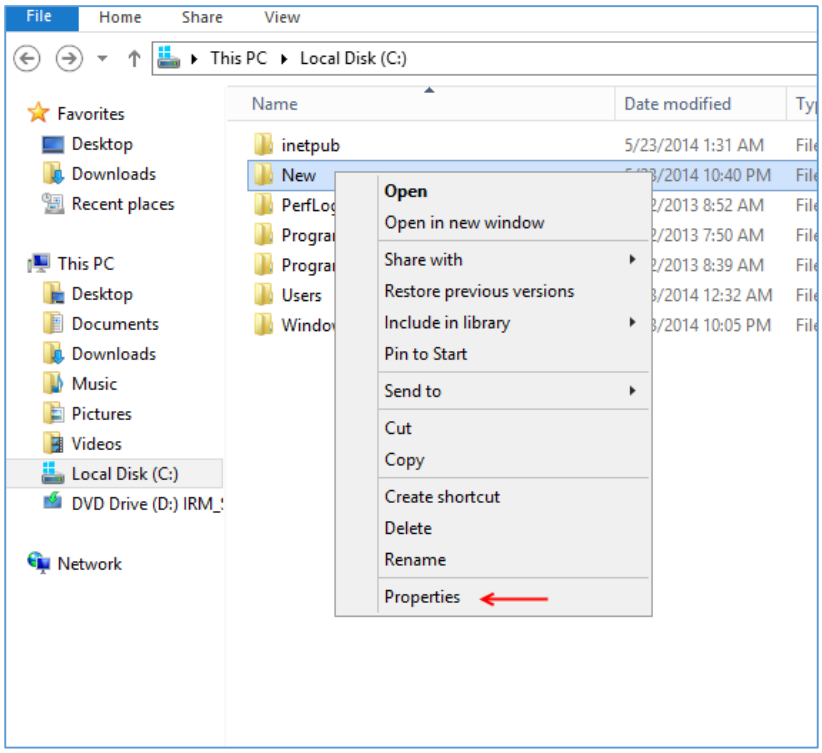


در قسمت Type باید نوع https را انتخاب کنید که بعد از انتخاب آن پورت 443 که یک پورت پیشفرض است برای آن مشخص می‌شود، در قسمت Host name هم آدرس کامل سایت و در مهمترین بخش که قسمت SSL certificate می‌باشد باید Certificate موردنظر را از لیست کشویی انتخاب کنیم و بعد بر روی ok کلیک کنیم.

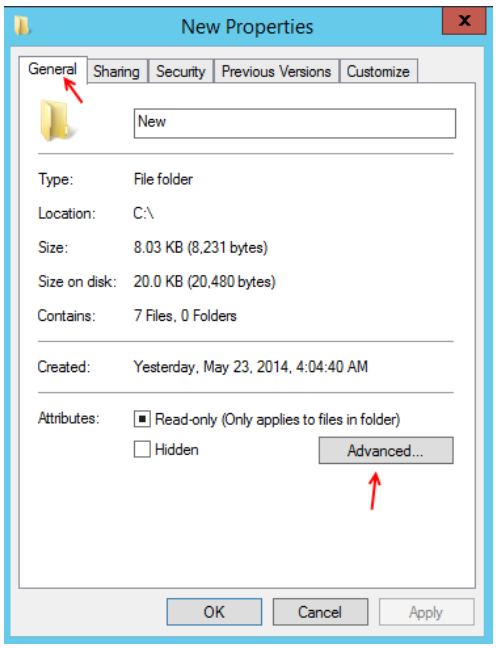
بعد از این کار سیستم را Restart کنید و بعد از اجرای ویندوز با آدرس https://www.test.com به صورت امن وارد سایت شوید، اگر در این قسمت با Error مواجع شدید با من در تماس باشید.

رمزنگاری روی فایل‌ها و پوشه‌ها:

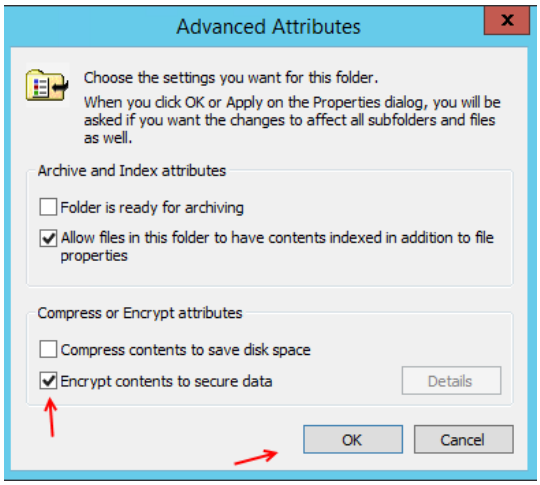
یکی دیگر از امکانات مهم در سیستم عامل ویندوز ایجاد رمز نگاری روی فایل‌ها و پوشه‌های موردنظر خود است، با استفاده از این امکان شما دسترسی به پوشه ها را محدود به کاربر خاصی می‌کنید و کاربر دیگر توانایی ورود، ویرایش و حذف آن را نخواهد داشت.



برای شروع یک پوشه در درایو C با نام New ایجاد می‌کنیم و بر روی آن کلیک راست کرده و گزینه Properties را انتخاب می‌کنیم.



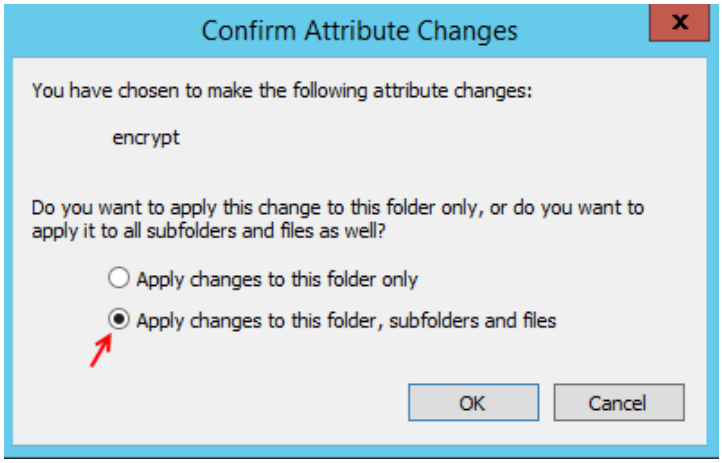
در تب General بر روی Advanced کلیک کنید تا شکل صفحه بعد ظاهر شود.



در این صفحه گزینه Encrypt contents to secure data را انتخاب کنید تا پوشه موردنظر برای رمزنگاری آماده شود.

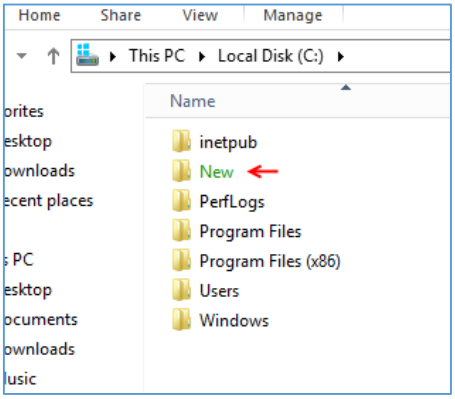
بر روی ok کلیک کنید.

و بعد بر روی Apply کلیک کنید تا شکل زیر ظاهر شود.

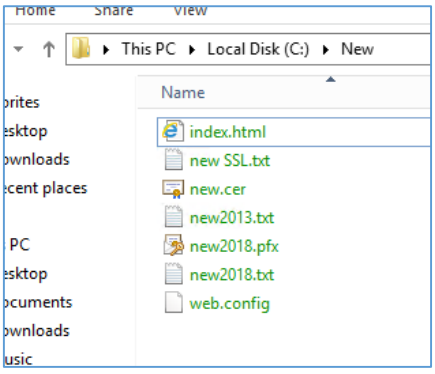


در این قسمت گزینه دوم را انتخاب کنید تا رمزنگاری روی پوشه موردنظر و تمام پوشه‌ها و فایل‌های داخل آن اعمال شود.

بر روی ok کلیک کنید.



همانطور که در شکل روبرو مشاهده می‌کنید، نوشته پوشه موردنظر به رنگ سبز درآمده است.

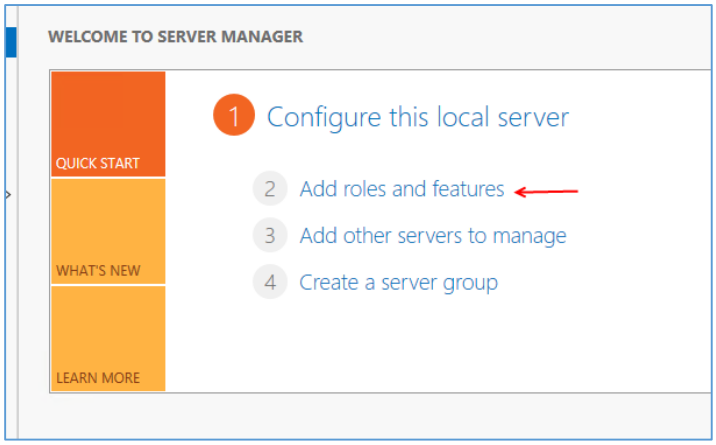


در شکل روبرو وارد پوشه New شدیم که تمام فایل های داخل آن هم رمزنگاری شدند. البته می‌توانید وارد Properties هر فایل شود و بر روی Advanced کلیک کنید و در صفحه باز شده بر روی Details کلیک کنید و یک کاربر خاص را معرفی کنید.

نصب و پیکربندی VPN:

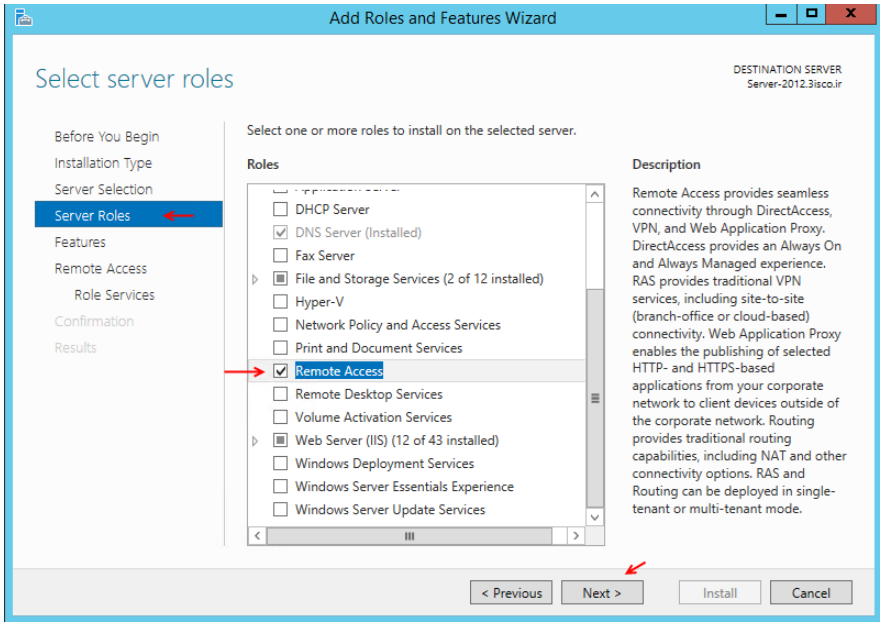
VPN یک ارتباطی بین یک سرور در مکان مشخص با یک سرور در مکان دیگر است، ارتباط این دو سرور به صورت امن انجام می‌شود، ارتباط VPN به دو صورت Remote Access و Site To Site انجام می‌پذیرد که آنها را بررسی خواهیم کرد.

برای شروع نیاز به یک سرور 2012 و یک ویندوز دیگر که در اینجا ویندوز 8 می‌باشد داریم، وارد ویندوز سرور می‌شویم و عملیات نصب را آغاز می‌کنیم.

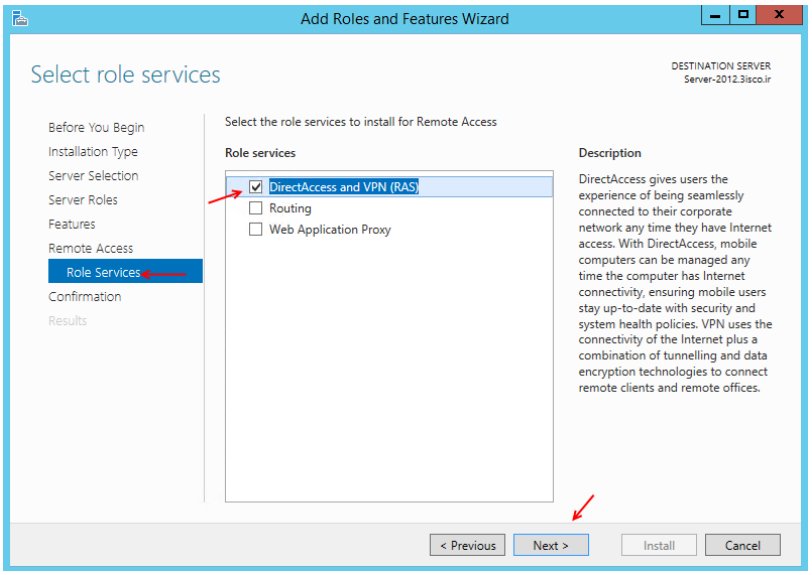


Server Manager را اجرا کنید و مانند شکل روبرو بر روی Add Roles And Features کلیک کنید.

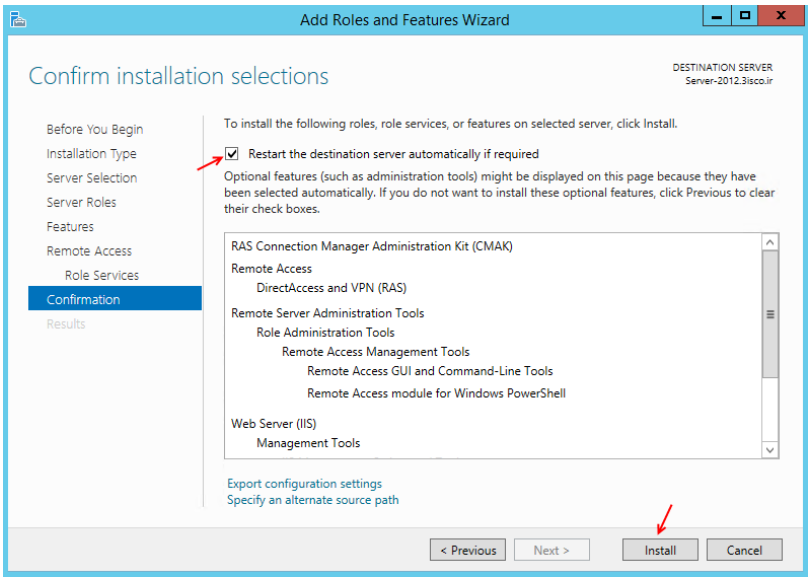
تذکر مهم: برای کار با VPN نیاز به دو کارت شبکه می‌باشد که یکی به اینترنت و دیگری مربوط به شبکه داخلی باشد.



بر روی Next کلیک کنید تا به قسمت Server Roles برسید، در این صفحه گزینه Remote Access را انتخاب کنید و بر روی Next کلیک کنید.

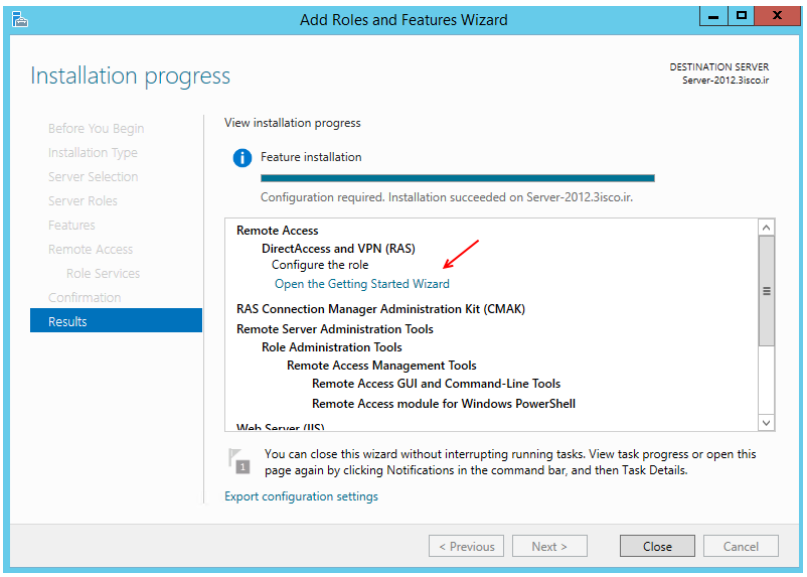


بر روی Next کلیک کنید تا به قسمت Role Services برسید، در این قسمت چند گزینه وجود دارد که در حال حاضر گزینه DirectAccess and VPN (RAS) را انتخاب کنید و بر روی Next کلیک کنید.

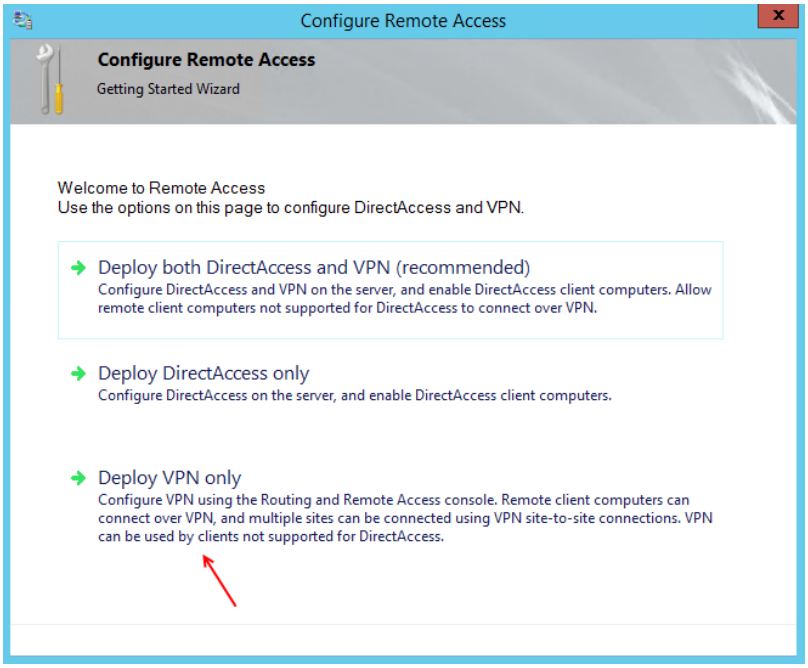


در این قسمت تیک گزینه Restart.. را انتخاب کنید و بر روی Install کلیک کنید.

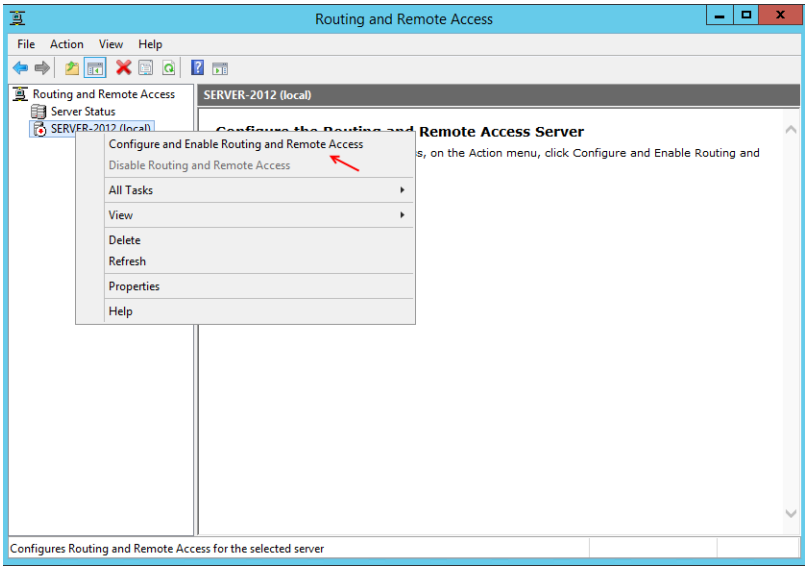
نکته: توجه داشته باشیدکه روی سروری که این سرویس نصب می‌شود IP Address را باید به صورت Static و یا همان دستی وارد کنید.



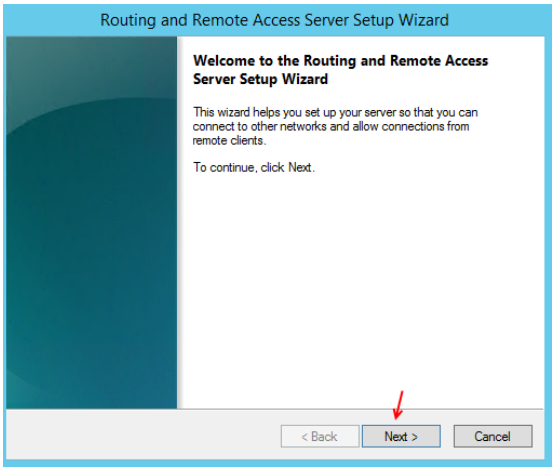
بعد از نصب سرویس باید بر روی Open the Getting Started Wizard کلیک کنید تا شکل بعد ظاهر شود.



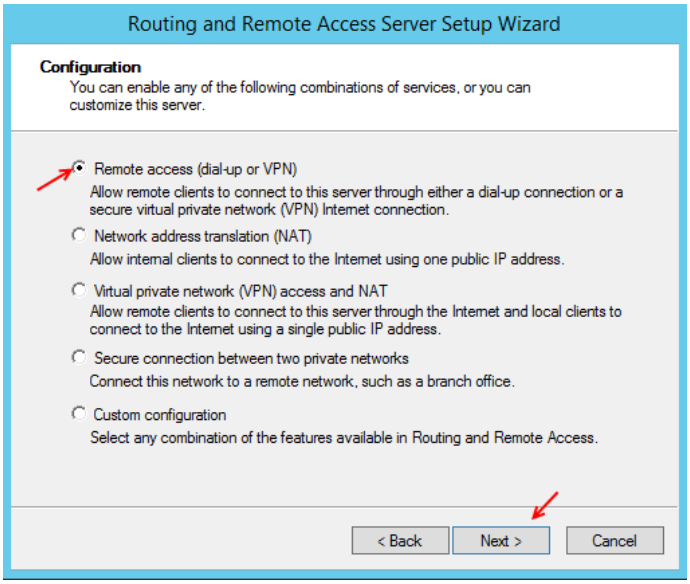
در این صفحه، برای تظیم VPN بر روی گزینه سوم یعنی Deploy VPN Only کلیک کنید.



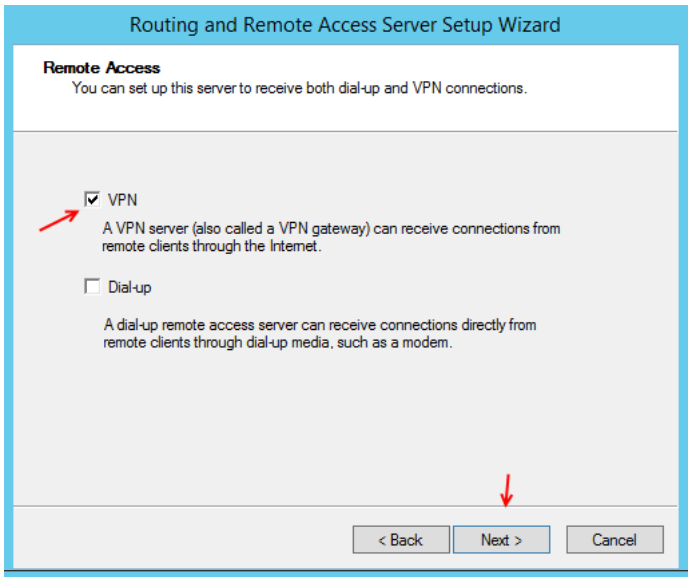
در این صفحه از سمت چپ بر روی نام سرور کلیک راست کنید و گزینه Configure and Enable Routing and Remote Access را انتخاب کنید.



بعد از ظاهر شدن صفحه خوش آمد گویی بر روی Next کلیک کنید.

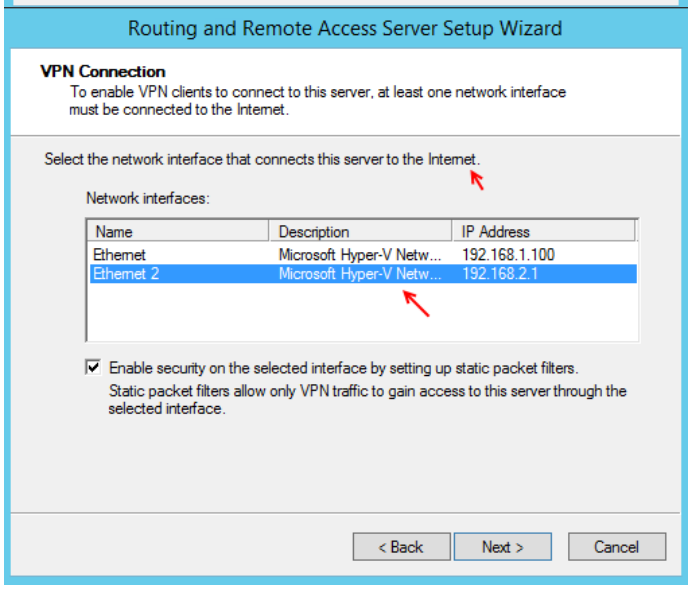


در این قسمت چندین گزینه وجود دارد که فعلاً گزینه اول را انتخاب و بر روی Next کلیک کنید.

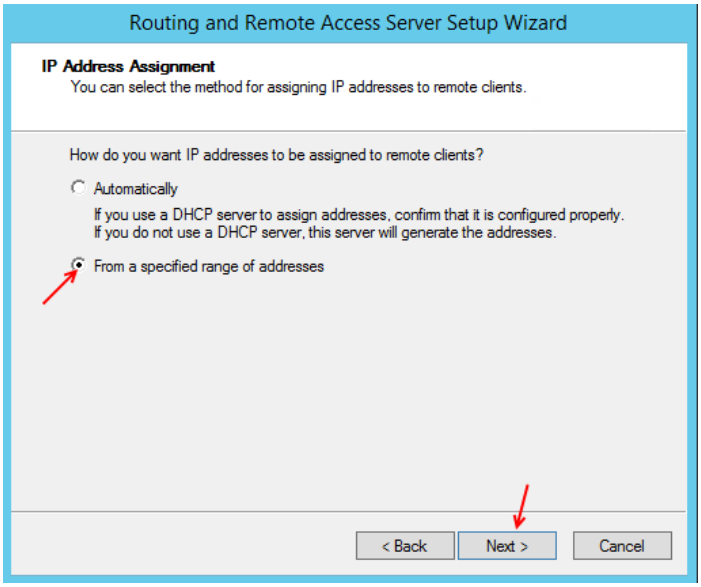


در این قسمت گزینه VPN را انتخاب کنید و بر روی Next کلیک کنید.

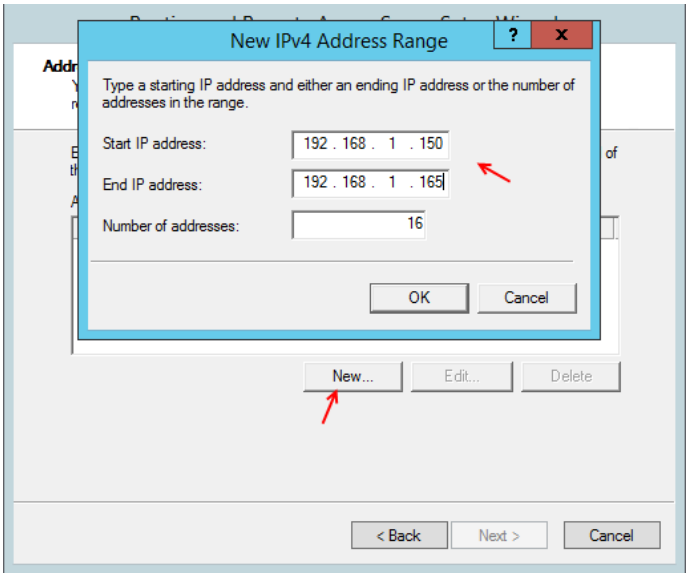
بعد از Next اگر دو کارت شبکه بر روی سرور خود نداشته باشید به شما Error خواهد داد.



در این قسمت باید کارت شبکه‌ای را انتخاب کند که سرور شما از طریق آن به اینترنت متصل است، در این قسمت Ethernet2 را انتخاب می‌کنیم و بر روی Next کلیک می‌کنیم.



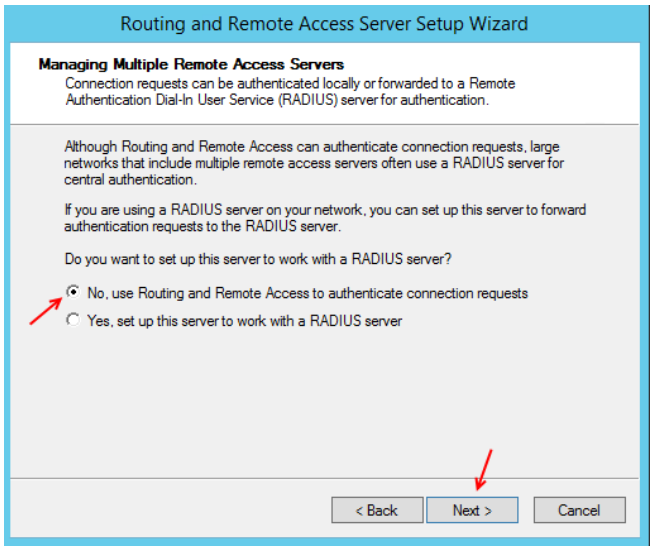
در این قسمت دو گزینه وجود دارد که برای تخصیص دادن Ip address به کلاینت‌هایی است که از طریق VPN به سرور متصل می‌شوند که در اینجا گزینه From a Specifed..... را انتخاب کنیدو بر روی Next کلیک کنید.



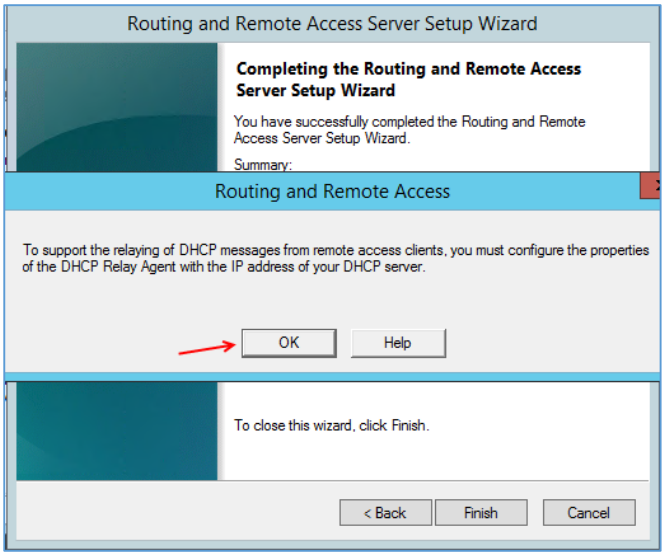
در صفحه باز شده بر روی New کلیک کنید تا شکل روبر ظاهر شود، در این قسمت باید Range آدرس IP خود را که در رنج آدرس کارت شبکه داخلی می‌باشد وارد کنید و بر روی ok کلیک کنید.

در این قسمت 16 آدرس برای اختصاص دادن به کلاینت‌ها انتخاب شده است.

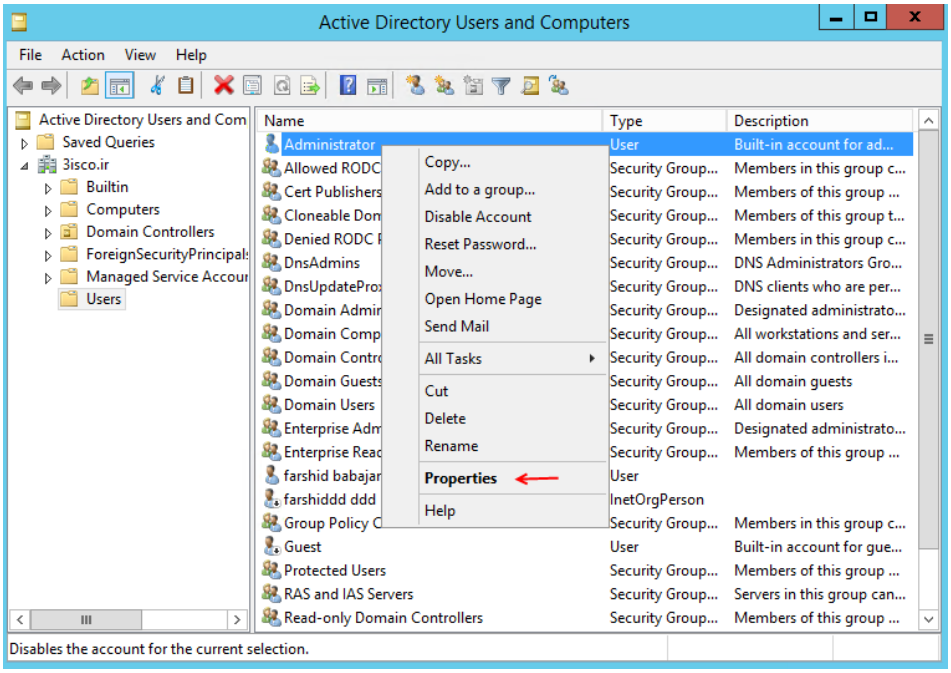
بر روی next کلیک کنید.



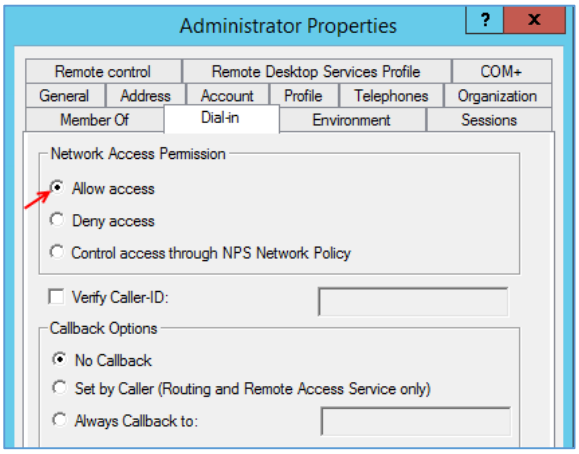
در این قسمت گزینه اول را انتخاب و بر روی Next کلیک کنید.



بعد از کلیک بر روی Finish شکل روبرو ظاهر می‌شود که یکی سری توضیحات مربوط به سرویس DHCP را گوش‌زد می‌کند، بر روی ok کلیک کنید تا تنظیات اعمال شود.

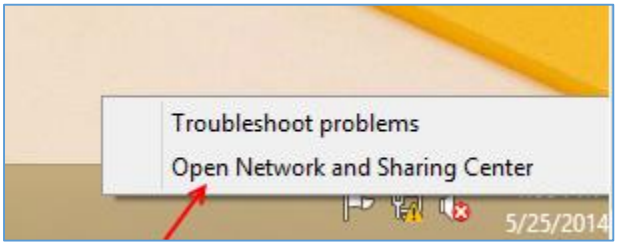


بعد از این کار باید به کاربر موردنظر اجازه ارتباط از راه دور دهیم، برای این کار وارد سرویس Active Directory Users and Computer می‌شویم و بر روی کاربر موردنظر خود کلیک راست کنید و گزینه Properties را انتخاب کنید.

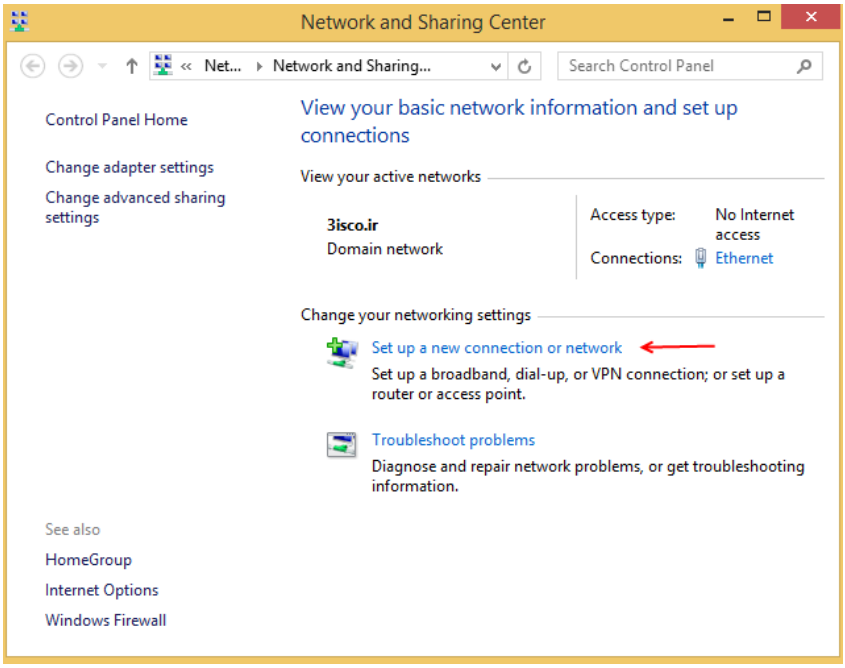


بعد از باز شدن صفحه وارد تب DIAL-IN شوید و در قسمت Network Access Permission گزینه Allow access را انتخاب کنیدو بر روی ok کلیک کنید، با این کار به کاربر موردنظر اجازه ارتباط از راه دور با سرور خود را می‌دهیم.

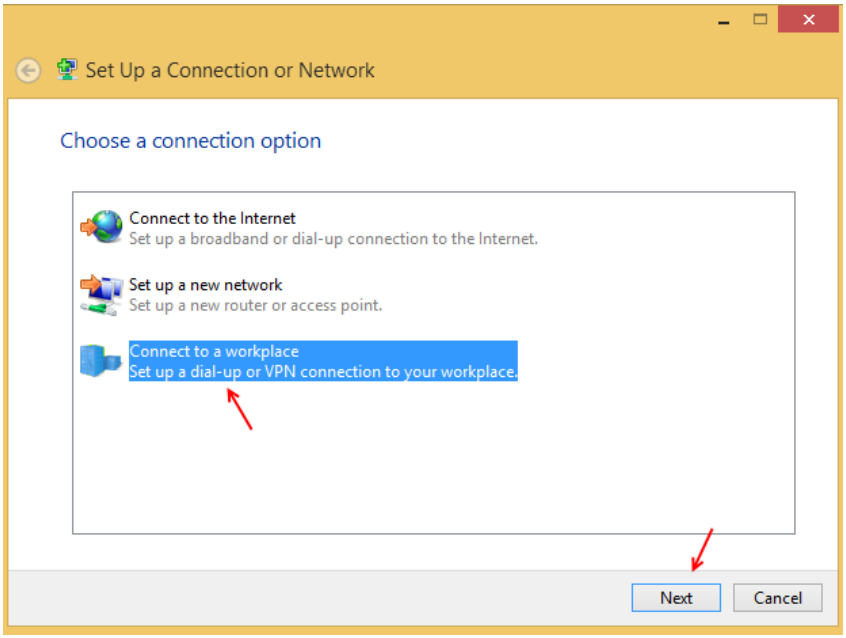
بعد از اتمام تنظیمات در سرور اصلی، حالا می‌خواهیم از طریق ویندور 8 به سرور VPN بزنیم، برای این کار وارد ویندوز 8 می‌شویم و بر روی آیکون کارت شبکه کلیک راست می‌کنیم و گزینه Open Network and Sharing Center را انتخاب می‌کنیم.

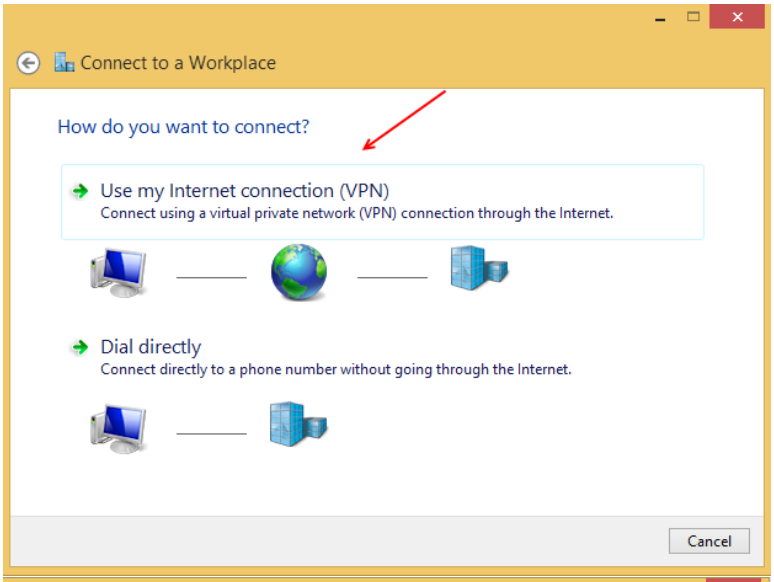


در این صفحه بر روی Set up a New connection or network کلیک کنید.

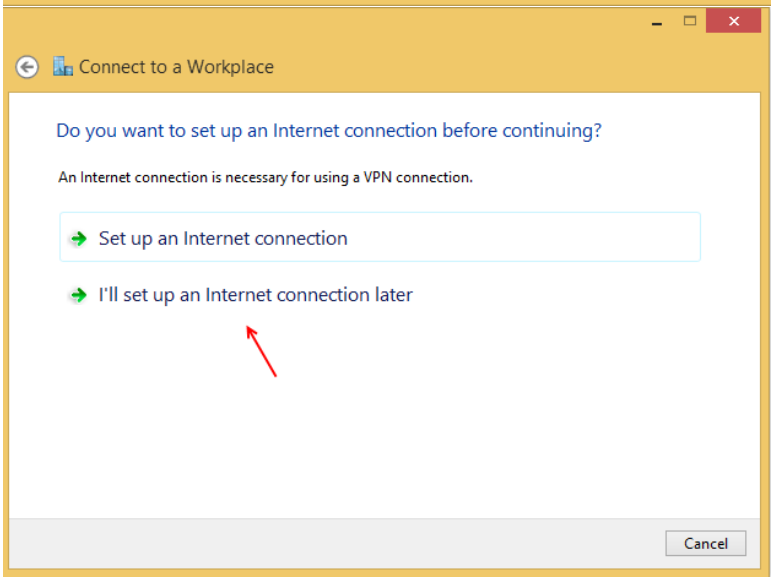


در این قسمت گزینه Connect to a workplace را انتخاب کنید و بر روی next کلیک کنید.

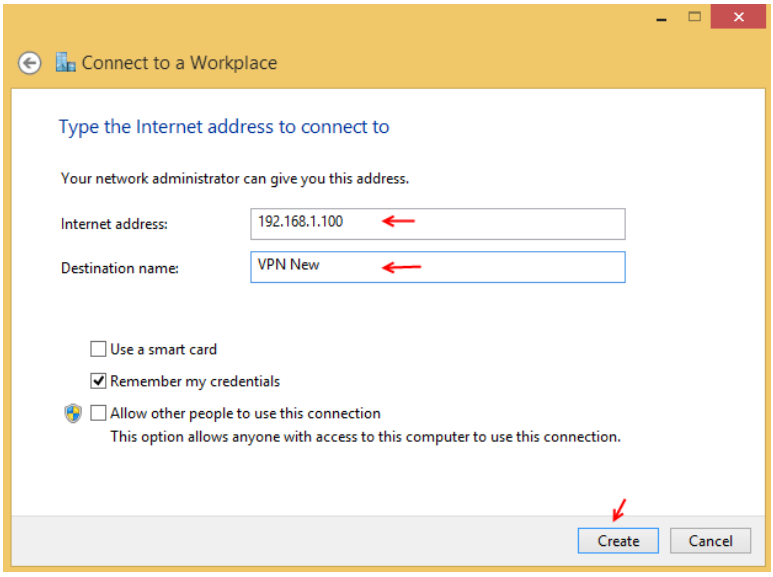




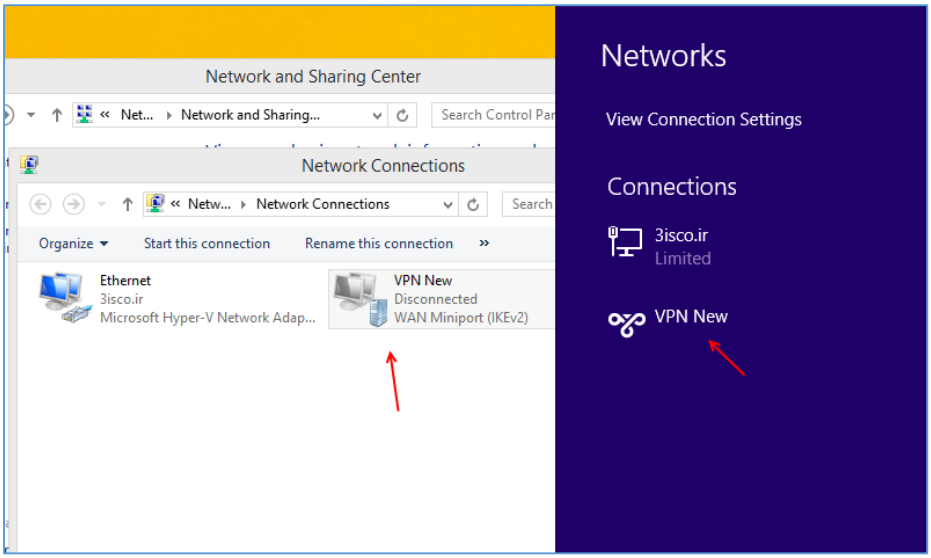
در این قسمت گزینه Use my Internet Connection را انتخاب کنید.



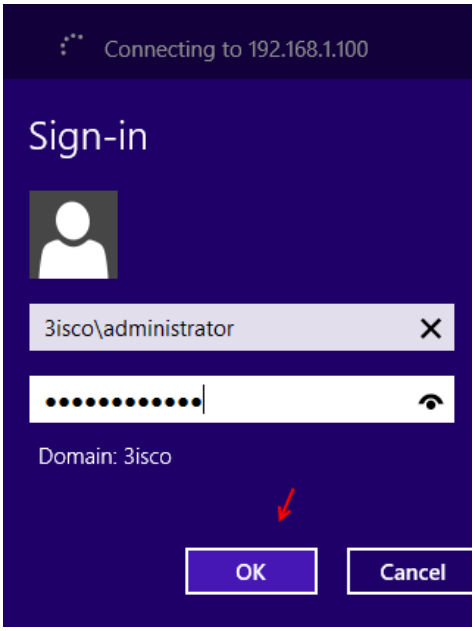
در این قسمت گزینه دوم یعنی I'll set up an internet connection later را انتخاب کنید.



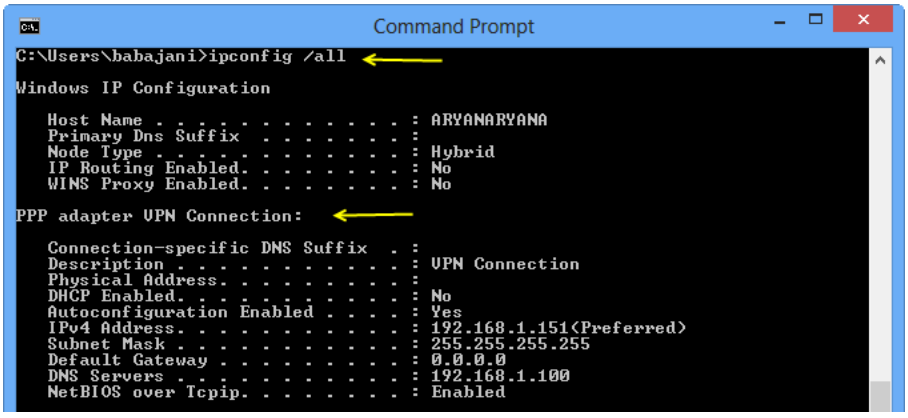
در این صفحه و در قسمت Internet Address باید آدرس سرور خود را وارد کنید و در قسمت Destination Name نام کانکشن خود را وارد کنید و بر روی Create کلیک کنید.



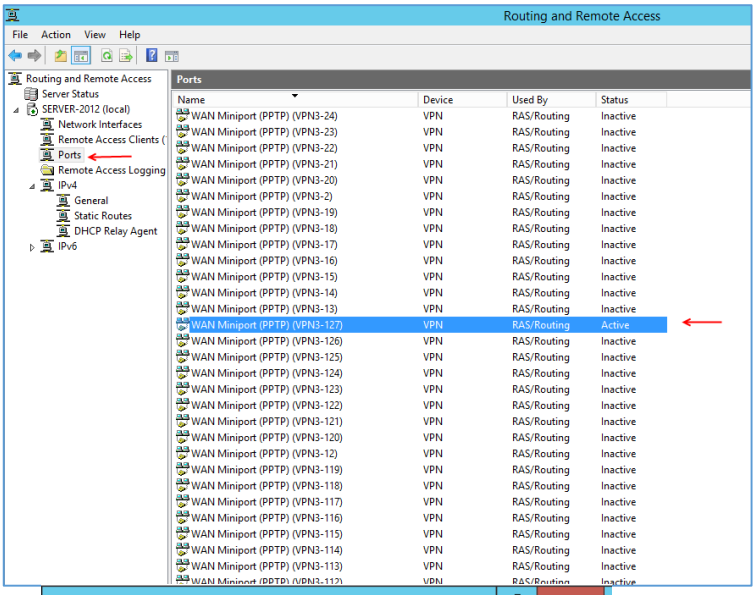
بعد از ایجاد کانکشن بر روی آن کلیک کنید تا نام کاربری و رمز عبور از شما درخواست شود.



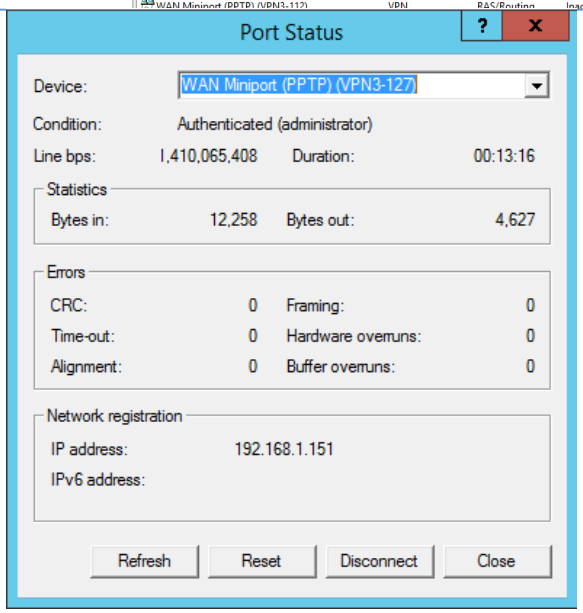
در این قسمت باید نام کاربری و رمز عبور را وارد کنید تا VPN برقرار شود. بعد از وارد کردن اطلاعات بر روی ok کلیک کنید تا ارتباط برقرار شود. توجه داشته باشید که کاربری را که در این قسمت وارد می‌کنید باید حتماً در تب Dial-in گزینه Allow access انتخاب شده باشد که این کار را در قسمت قبل انجام دادیم.



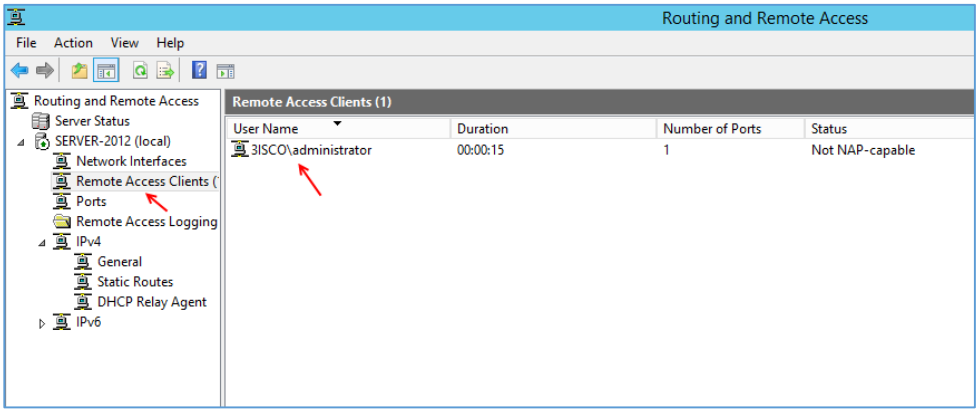
بعد از این کار وارد CMD شوید و به مانند شکل روبرو دستور Ipconfig /all را وارد کنید، همانطور که مشاهده می‌کنید، کانکشن VPN به درستی به سرور متصل شده است.



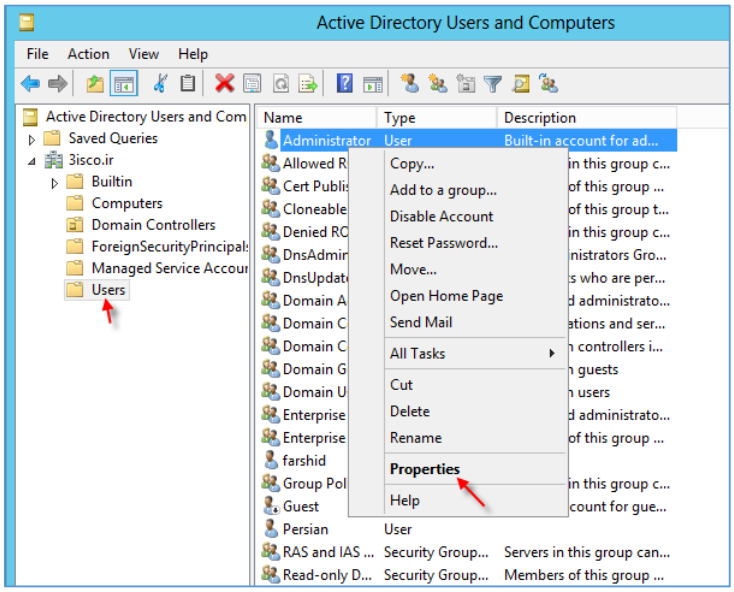
دوباره وارد سرور اصلی شوید و سرویس Routing and Remote access را اجرا کنید و به مانند شکل از سمت چپ بر روی Port کلیک کنید، در این قسمت تمام پورت‌های فعال و غیرفعال مربوط به VPN نمایش داده می‌شود، در بین این پورت‌ها یکی از آنها Active می‌باشد، این همان کانکشن VPN می‌باشد که اجرا کردیم بر روی آن دو بار کلیک کنید.



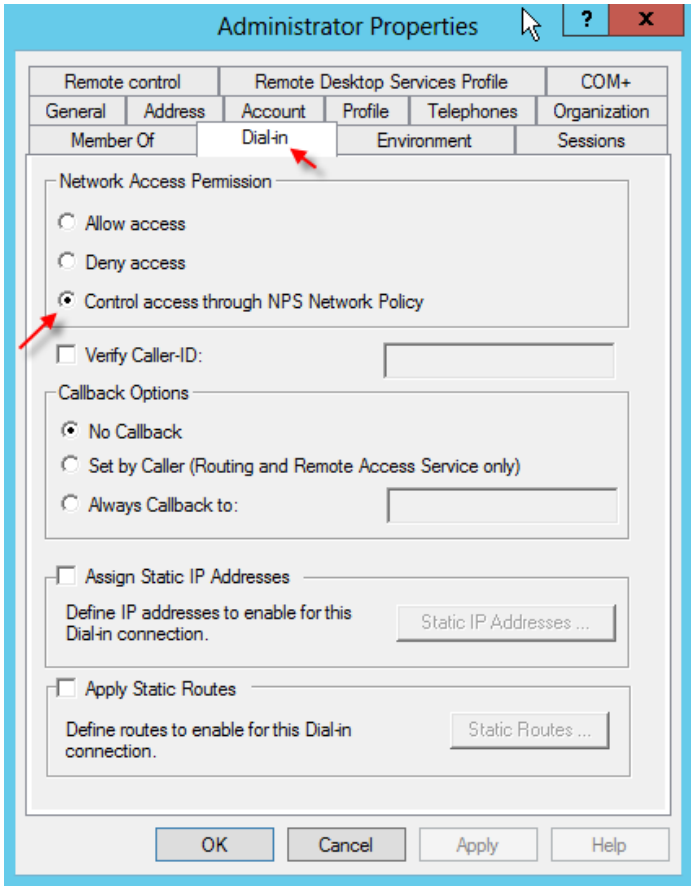
این صفحه مربوط به اطلاعات کانکشن VPN موردنظر است که، شما توانایی Disconnect و یا Reset آن را خواهید داشت، شمارنده‌ای هم در این قسمت وجود دارد که مدت زمان اتصال کانکشن به سرور را نشان می‌دهد.



اگر به قسمت Remote Access Clients مراجعه کنید، می‌توانید کانکشن‌های متصل به سرویس را مشاهده و کنترل کنید.



تا به اینجا از طریق Remote Access توانستیم یک VPN ایجاد کنیم و از طریق کاربران اکتیو به سرور اصلی VPN بزنیم دوباره وارد سرویس Active Directory Users and Computers شوید و بر روی یکی ازکاربران خود کلیک راست کنید و گزینه Properties را انتخاب کنید.

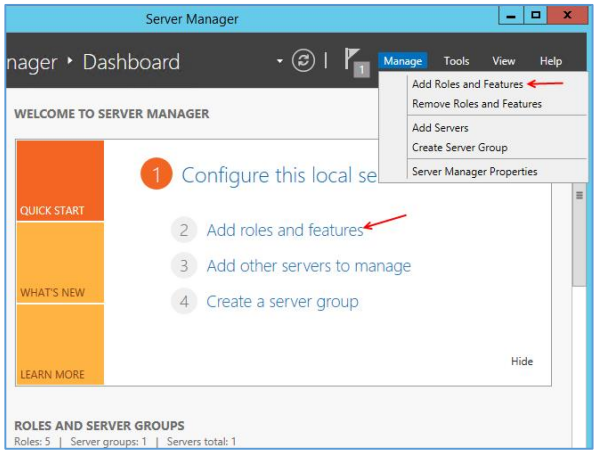


در این صفحه وارد تب Dial-in می‌شویم، اگر به قسمت Network Access Permission توجه کنید، گزینه‌ای با نام Control Access Through NPS Network Policy وجود دارد که این گزینه به کنترل کاربران از طریق سرویس NPS اشاره دارد که در این قسمت این گزینه را که به صورت پیش‌فرض برای تمام کاربران انتخاب شده است را انتخاب و سرویس NPS را در زیر نصب می‌کنیم و نحوه ارتباط آن را با هم بررسی می‌کنیم.

کار با سرویس Network Policy Server :

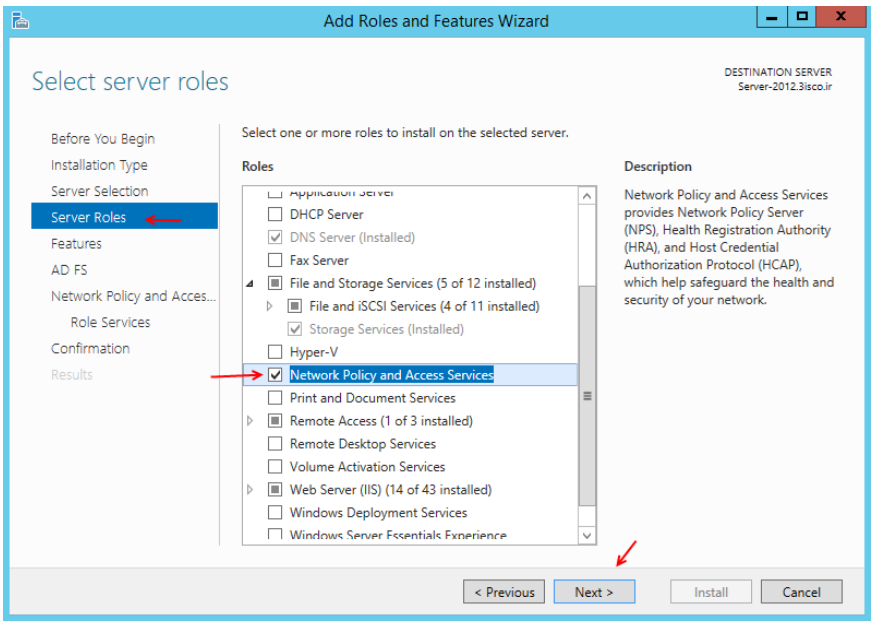
در این سرویس با استفاده از Policy کاربران را برای ارتباط از طریق VPN کنترل می‌کنیم، روال کار به این صورت است که اول سرویس Network Policy Server را فعال و تنظیم می‌کنیم و بعد از آن وارد سرویس Network Policy Server می‌شویم و تنظیمات را انجام می‌دهیم و بعد VPN را اجرا می‌کنیم.

تذکر: در این قسمت سرویس Routing and Remote Access از قبل نصب شده است، شما برای نصب آن می‌توانید به عنوان قبلی یعنی نصب و پیکربندی VPN مراجعه کنید.



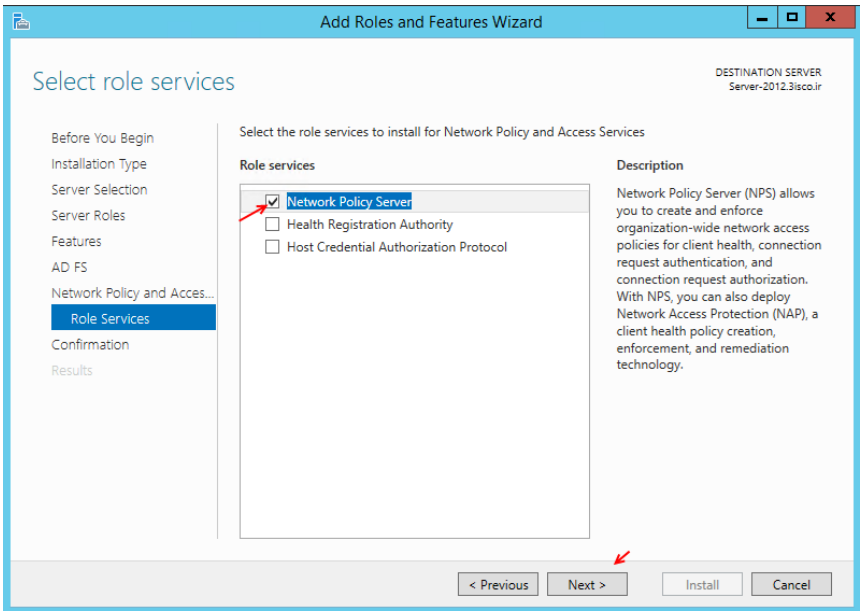
برای شروع وارد Server Manager می‌شویم و در صفحه باز شده بر روی Add Roles and Features کلیک می‌کنیم.

در صفحه باز شده بر روی Next کلیک کنید تا به شکل زیر برسید.



در این صفحه باید گزینه Network Policy and Access Services را انتخاب کنید.

بر روی Next کلیک کنید.



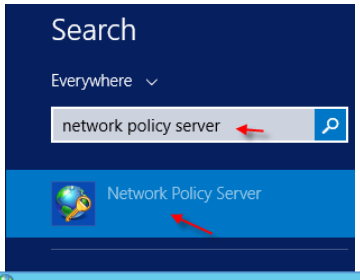
در قسمت Role Service گزینه Network Policy Server را انتخاب کنیدو بر روی Next کلیک کنید.

در صفحه آخر بر روی Install کلیک کنید تا سرویس موردنظر نصب شود.

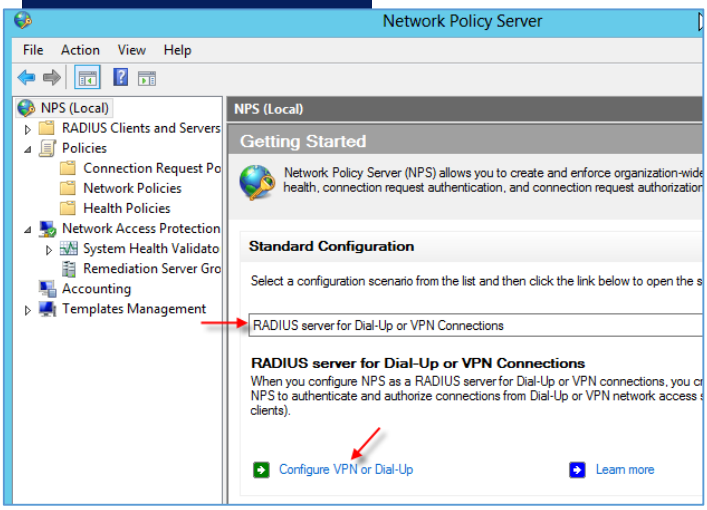
با استفاده از دستور PowerShell زیر هم می‌توانید به صورت سریع این سرویس را نصب کنید.

Install-WindowsFeature –name napas-policy-server –includemanagementtools

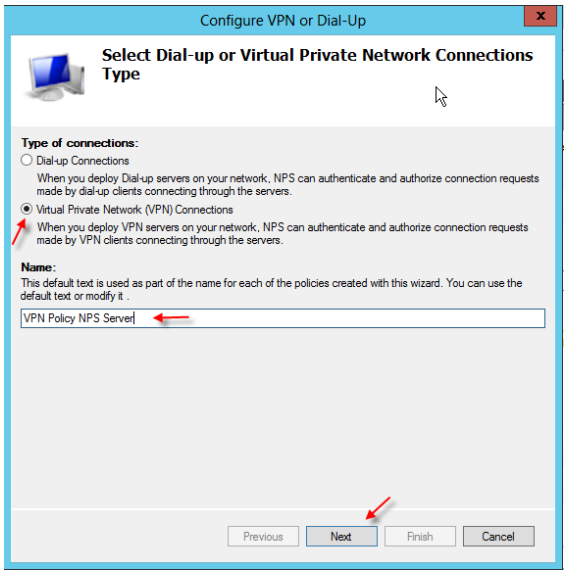
بعد از نصب سرویس Network Policy Server وارد Search شوید و این سرویس را به صورت شکل روبرو اجرا کنید.



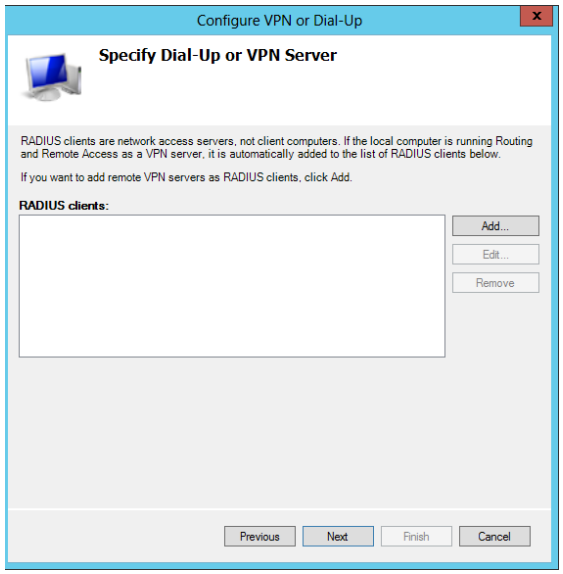
بعد از نصب سرویس وارد Search شوید و سرویس Network Policy Server را اجرا کنید.



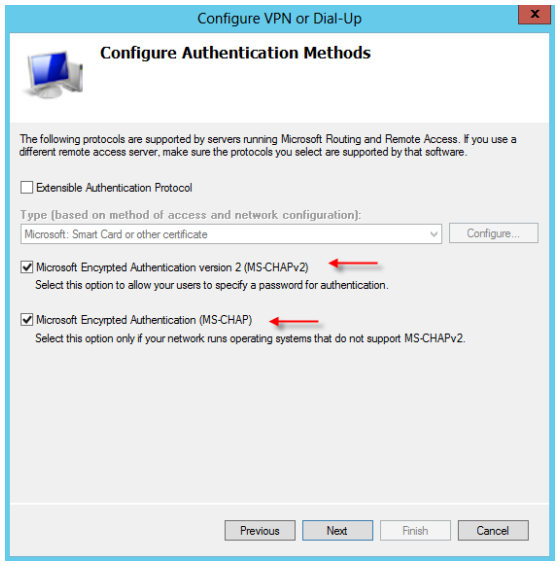
بعد از اجرای سرویس به مانند شکل روبرو در قسمت NPS(Local)، از لیست کشوییموردنظر گزینه Radius Server for Dial-Up or VPN Connections را انتخاب کنید و بعد بر روی Configure VPN or Dial-Up کلیک کنید.



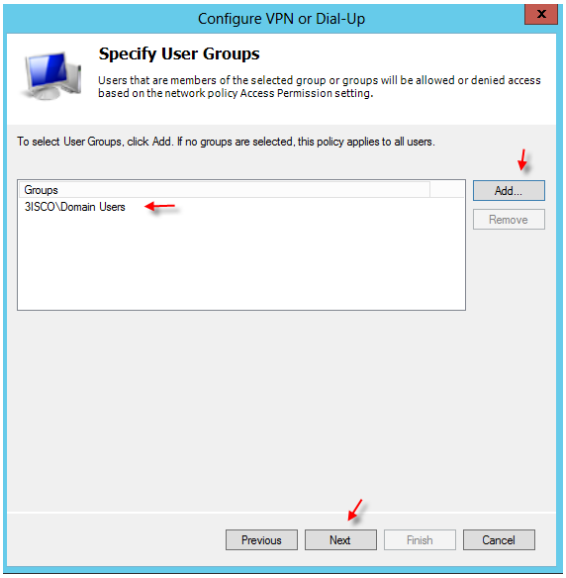
در این صفحه گزینه دوم یعنی Virtual Private Network (VPN) Connections را انتخاب کنید و یک نام به دلخواه خود وارد کنیدو بعد بر روی Next کلیک کنید تا شکل بعد را مشاهده کنید.



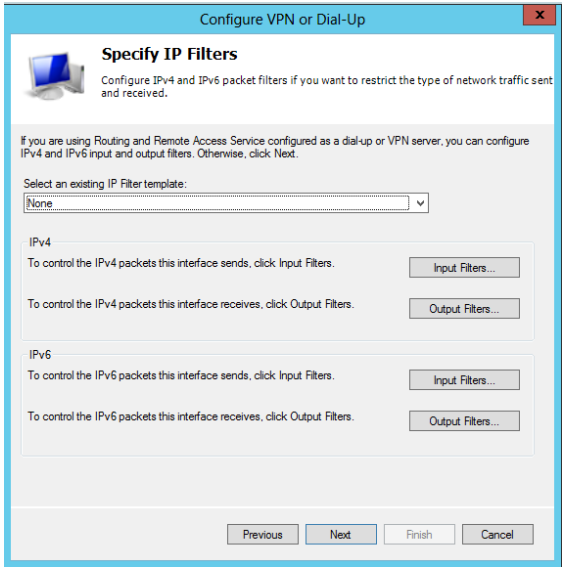
در این صفحه اگر در شبکه خود می‌خواهید از Radius Server استفاده کنید باید بر روی Add کلیک کنید و مشخصات آن را وارد کنید، مثلاً اگر در شبکه خود از روتر میکروتیک استفاده می‌کنید، برای استفاده از سرویس HotSpot باید یک Radius Server بین روتر و ویندوز راه بندازید تا بتوانید از نام‌های کاربری موجود در ویندوز برای سرویس HotSpot روتر میکروتیک استفاده کنید که اگر نیاز به این کار داشتید به من ایمیل بزنید. حالا بر روی Next کلیک کنید.



در این صفحه باید پروتکل رمزنگاری را انتخاب کنید، پروتکل‌هایی که در اینجا وجود دارد عبارت اند از MS-CHAPv2 و MS-CHAP که بنا به نیاز خود یکی یا هر دو آنها را انتخاب کنید، روش دیگزی هم وجود دارد که می‌توانید با ارائه گواهینامه امنیتی به هر یک از کلاینت‌ها که نیاز به ارتباط VPN دارند این ارتباط را برقرا کنید که برای این کار باید گزینه اول را انتخاب کنید، البته باید قبل از آن یک Certificate برای سرور اصلی که VPN روی آن ایجاد می‌شود تعریف شده باشد. بر روی Next کلیک کنید.



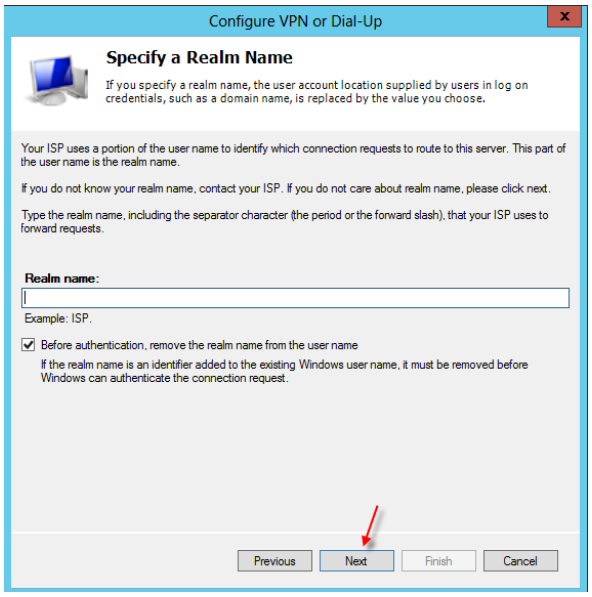
در این قسمت بسته به اینکه به چه کاربر و گروهی اجازه ارتباط VPN می‌دهید، با کلیک بر روی Add کاربر و گروه موردنظر را به مانند شکل به لیست اضافه کنید که در این بخش گروه Domain Users که دربرگیرنده تمام کاربران عضو دومین می-باشد به لیست اضافه شده است.



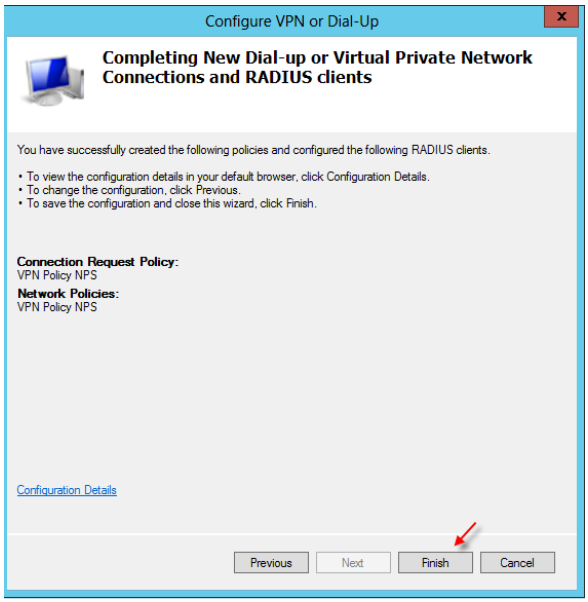
در این قسمت می‌توانید مشخص کنید که چه رنج آدرسی بتواند وارد شبکه و یا خارج شود که قبل آن باید نوع آدرس IP خود را مشخص کنید و اگر برای شبکه داخلی خود می‌خواهید دسترسی ایجاد کنید باید بر روی Input Filters کلیک کنید و یا برای دسترسی خارجی بر روی Output Filters کلیک کنید.

بر روی Next کلیک کنید.

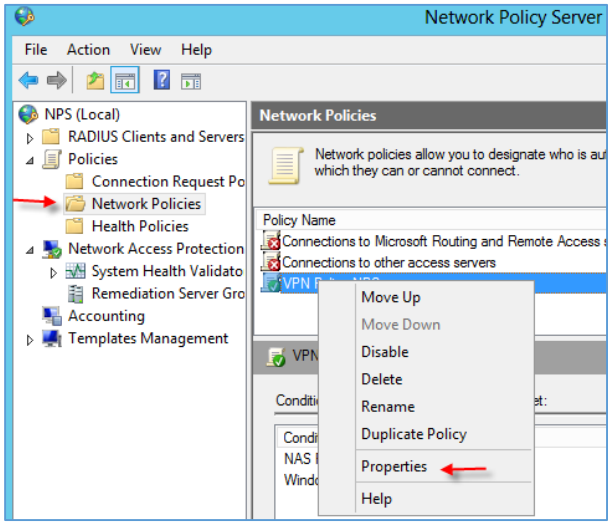
در این صفحه اگر امنیت اطلاعات برای شما که مدیر شبکه یک سازمان هستید مهم است، اندازی رمزنگاری اطلاعات را مشخص کنید که در این بخش هر چه عدد موردنظر بزرگتر باشد مثلاً 128 بیت باشد رمزنگاری اطلاعات به صورت حرفه‌ای تر صورت خواهد گرفت. بعد از انتخاب گزینه موردنظر بر روی Next کلیک کنید.



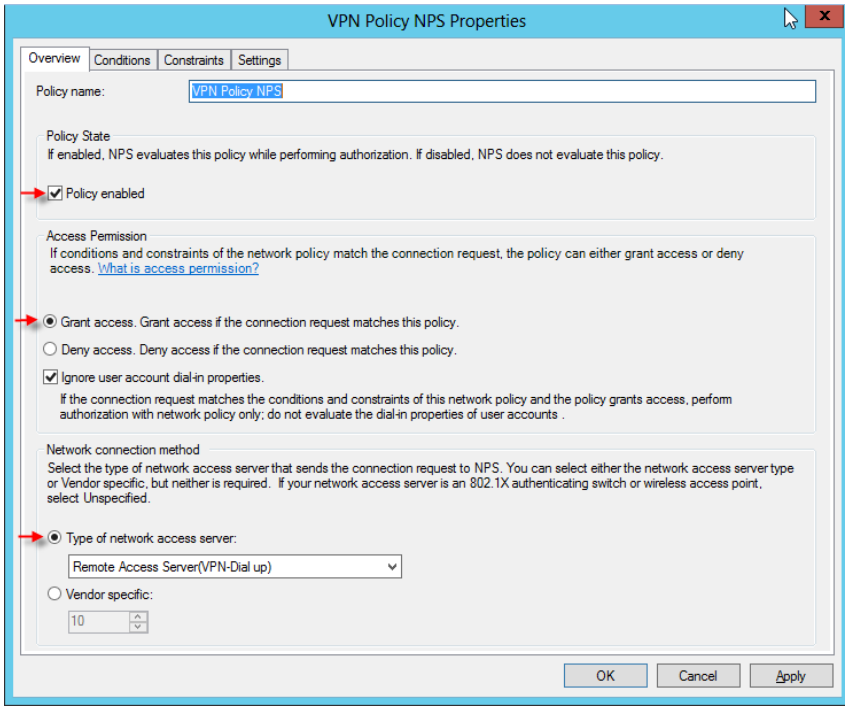
در این صفحه بر روی Next کلیک کنید.



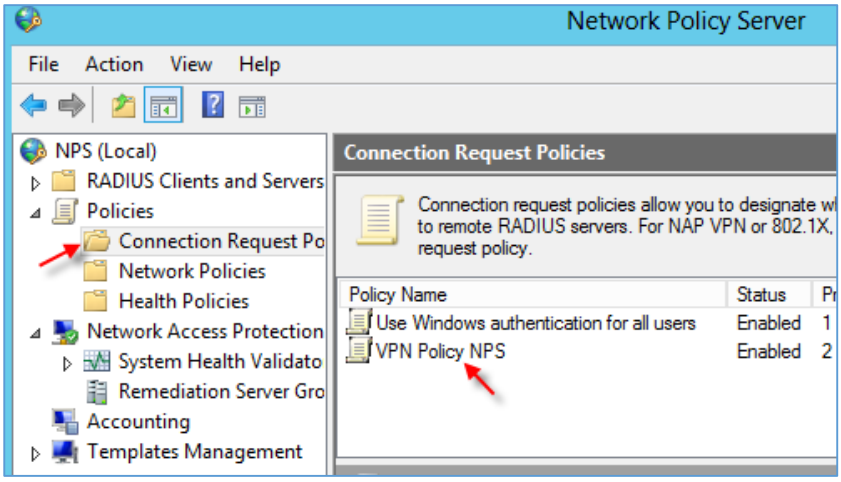
در این صفحه بر روی Finish کلیک کنید تا Policy VPN موردنظر ایجاد شود.

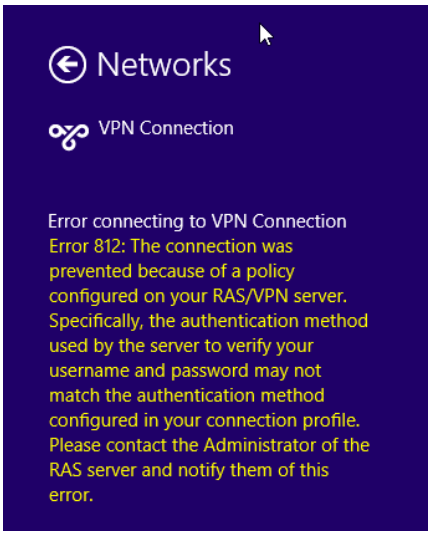


اگر دوباره به سرویس NPS مراجعه کنید و از سمت چپ بر روی Network Policies کلیک کنید، متوجه خواهید شد که یک Policy با نام موردنظر خودتان ایجاد شده است، بر روی آن کلیک راست کنید و Properties را انتخاب کنید.

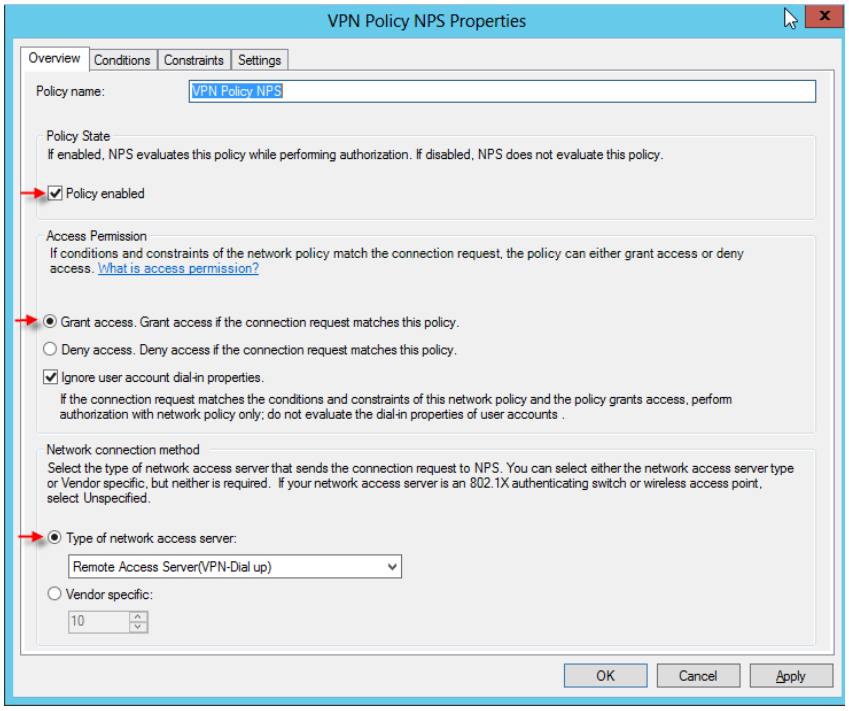


در تب Overview گزینه‌های مختلفی وجود دارد که با هم آنها را بررسی می‌کنیم، اگر تیک کنار گزینه Policy Enabled را بردارید Policy موردنظر غیر فعال خواهد شد و کاربران نمی‌توانند به سرور اصلی VPN بزنند البته یک نکته مهم هم در این قسمت وجود دارد که اگر این گزینه را غیر فعال کنیم باز هم کاربران می‌توانند VPN بزنند، برای اینکه Policy دیگری در قسمت Connection Reauest Policies وجود دارد که در شکل مقابل آن را مشاهده می‌کنید که باید بر روی آن هم کلیک راست کنید و وارد Properties شود و در تب Overview تیک کنار گزینه Policy Enable را بردارید.

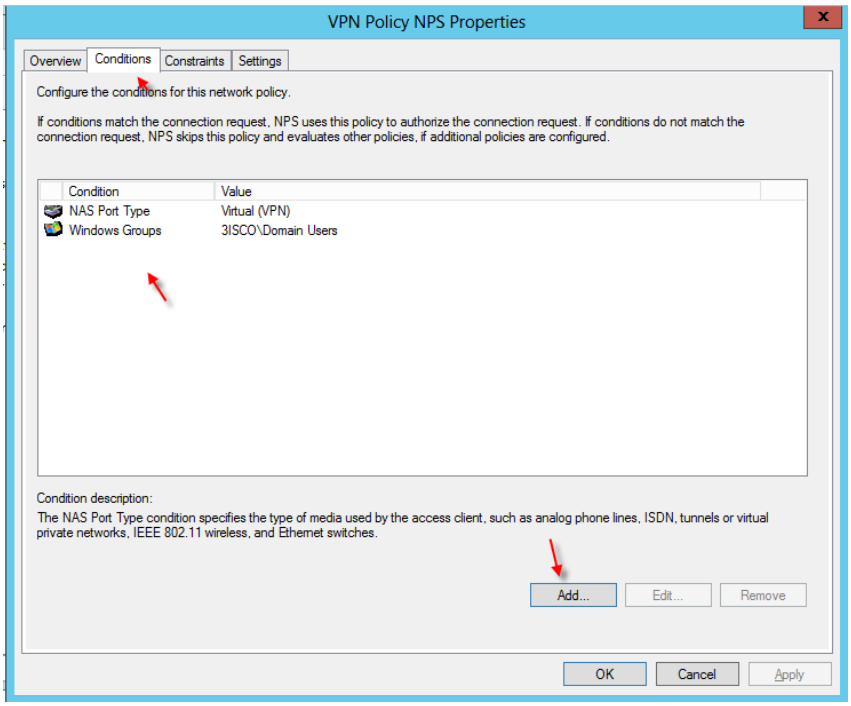




بعد از این کار زمانی که کاربر موردنظر بخواهد VPN بزند با Error مقابل مواجه خواهد شد.

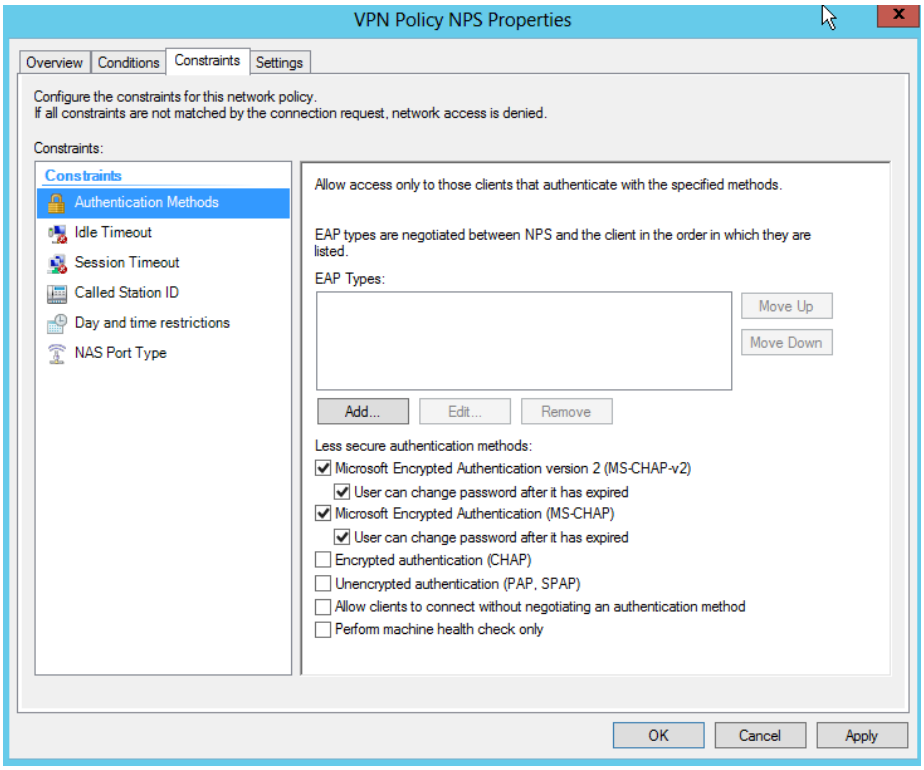


درادامه دوگزینه دسترسی وجود دارد که اگر می‌خواهید کاربران از طریق VPN به شبکه موردنظر دسترسی داشته باشند گزینه Grant Access را انتخاب کنید و اگر نمی‌خواهید به شبکه دسترسی داشته باشند گزینه Deny access را انتخاب کنید و در قسمت آخر هم نوع دسترسی به شکه را می‌توانید مشخص کنید.

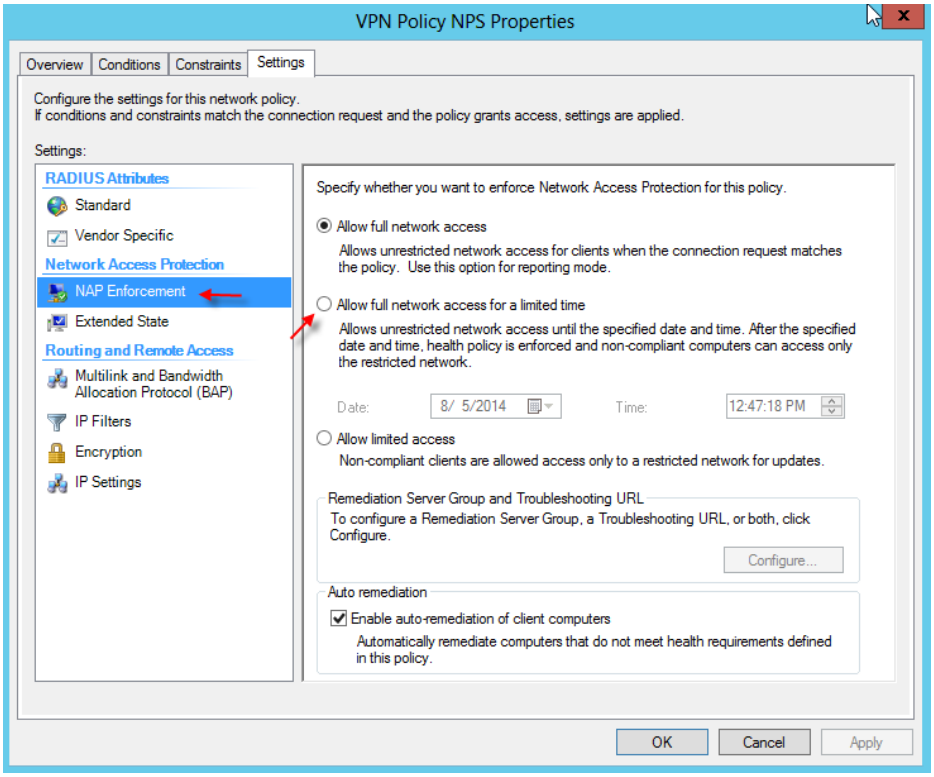


در تب Conditions می‌توانیم، یک سری تنظیمات جدید را به لیست اضافه کنیم، برای این کار بر روی Add کلیک کنید و از لیست موجود گزینه موردنظر خود را انتخاب کنید.

مثلاً می‌توانید بر روی Authentications کلیک کنید و نوع جدیدی را به مانند PAP or Chap به لیست اضافه کنید که این کار باعث می‌شود کاربران بتوانند از طریق این دو پروتکل هم به شبکه از طریق VPN متصل شوند.

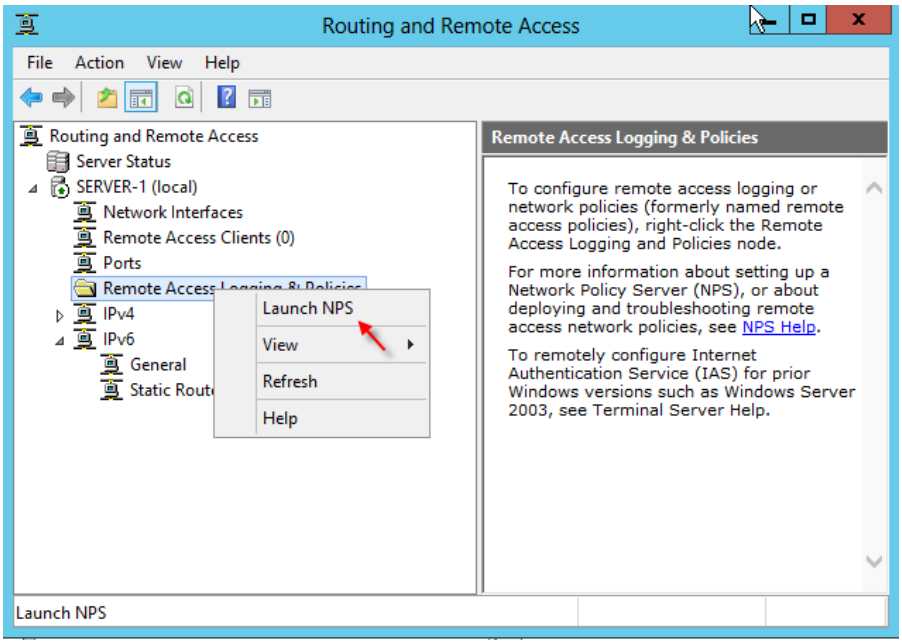


در تب Constraints تنظیمات مختلف وجود دارد که از مهمترین آنها می‌توان به Idle Timeout اشاره کرد که زمانی که یک کاربر به از طریق VPN به شبکه متصل شده است و در حال کار با سیستم نیست می‌توانید مدت زمانی را به دقیقه مشخص کنید تا ارتباط کاربر با شبکه قطع شود. گزینه Session Timout هم وجود دارد که مقدار زمان یک ارتباط را بر حسب دقیقه حساب می‌کند، مثلاً اگر یک ارتباط به 1 ساعت رسید قطع شود.

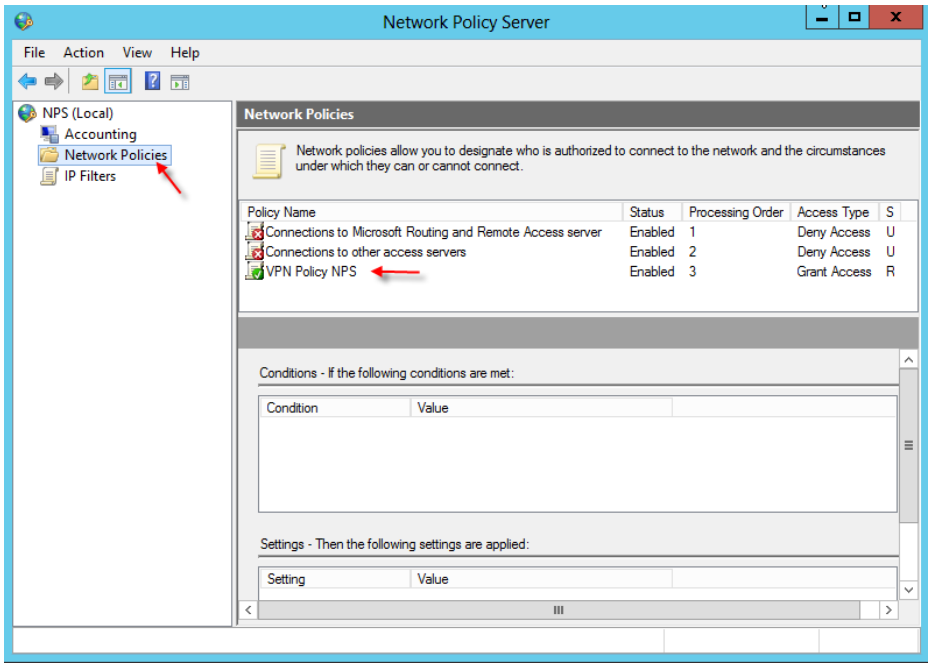


در تب Settings گزینه های مختلف دیگر وجود دارد، مثلاً می‌توانید تنظیمات مربوط به RADIUS Server را انجام دهید، اگراز سمت چپ بر روی NAP Enforcement کلیک کنید می‌توانید مشخص کنید که کاربران در چه زمان و ساعتی می‌توانند به سرور دسترسی داشته باشند.

با این تنظیماتی که در قسمت قبل انجام دادیم کاربران می‌توانند از طریق VPN و به کمک سرویس NPS به شبکه متصل شوند.



راه دیگر برای دسترسی به سرویس NPS وجود دارد که این کار از طریق سرویس Remote Access قابل اجرا است به این صورت که سرویس Remote access را به مانند شکل روبرو اجرا می‌کنیم و بعد بر روی Remote access Logging & Policies کلیک راست کنید و گزینه Launch NPS را انتخاب کنید.

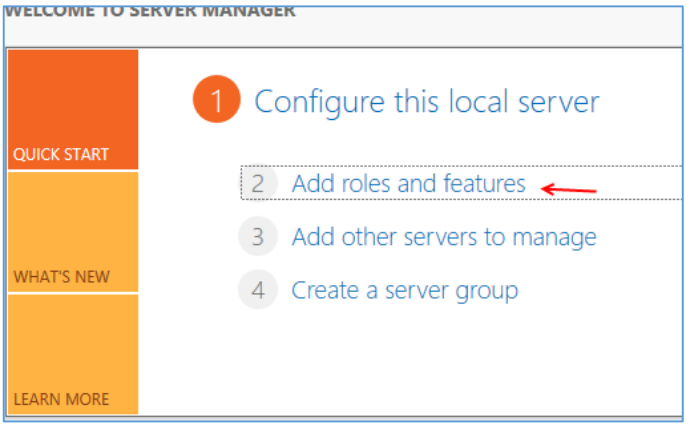


همانطور که مشاهده می‌کنید سرویس NPS اجرا شده است و اگر از سمت چپ بر روی Network policies کلیک کنید می‌توانید Policy قبلی را که با هم ایجاد کردیم مشاهده کنید.

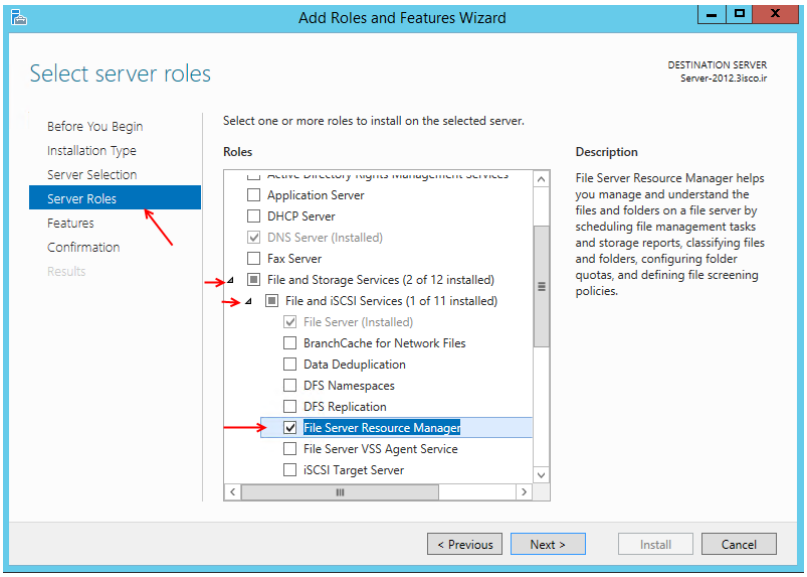
برای تعریف Policy جدید بر روی Network policies کلیک راست کنید و گزینه New را انتخاب کنید.

کار با File Server Resource Manager (FSRM):

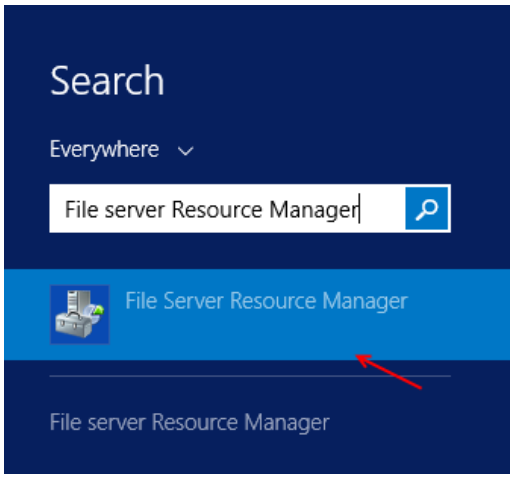
این سرویس یک سری از سرویس‌های ذخیره سازی داده‌ها را در کنار هم قرار داده است و کار مدیریت این گونه سرویس‌ها را آسان کرده است.



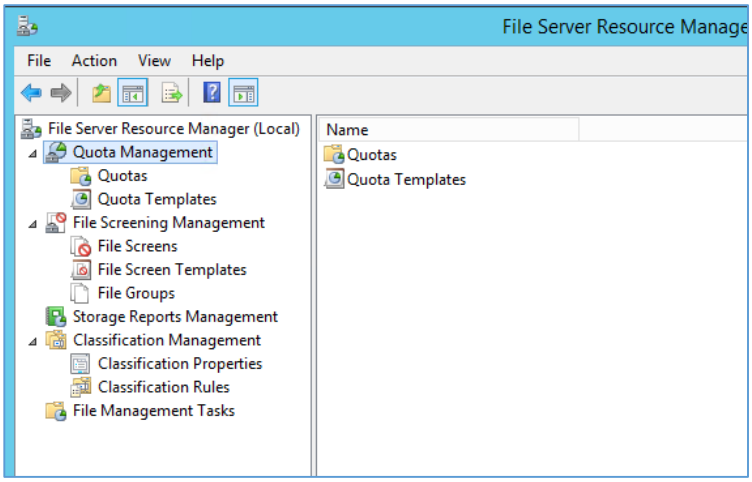
برای شروع کار وارد Server Manager را اجرا کنید و مانند شکل روبرو بر روی Add Roles and Features کلیک کنید.



بر روی Next کلیک کنید تا به قسمت Server Roles برسید، در این صفحه بر اول File and Storage... و بعد File and iSCSI... را انتخاب کنید و در زیر مجموعه آن گزینه File Server Resource Manager را انتخاب کنیدو بر روی Next کلیک کنید.



بعد از نصب سرویس وارد Search شوید و File Server Resource Manager را وارد کنید و گزینه موردنظر را انتخاب کنید.

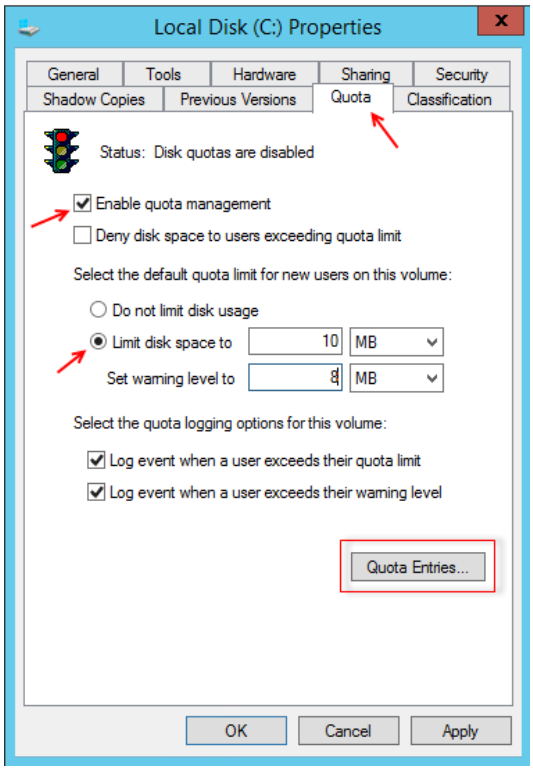


همانطور که مشاهده می‌کنید سرویس موردنظر به درستی اجرا شده است این سرویس از قسمت های مختلفی مانند Quota, Screening,... تشکلی شد است که با هم این قسمت ها را بررسی می‌کنیم.

کار با Quota Management:

Quota قابلیتی در ویندوز می‌باشد که از طریق آن میتوانید فضای هار دیسک را برای کاربران محدود کنید تا کاربر نتواند بیشتر از آن، از فضای هار دیسک استفاده کند، در این سرویس اگر فضای کاربر به حد موردنظر نزدیک شود، این سرویس به روش‌های مختلف به شما اخطار خواهد داد.

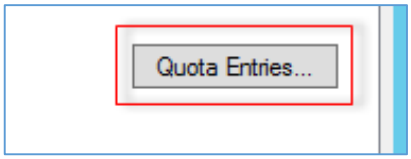
برای شروع وارد My Computer شوید و بر روی یکی از درایوهای خود کلیک راست کنید و گزینه Properties را انتخاب کنید.



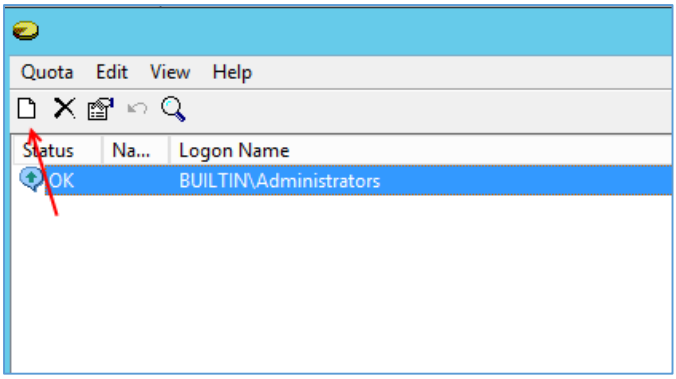
تذکر مهم: برای استفاده از این قابلیت، پارتیشن موردنظر حتماً باید از نوع NTFS باشد.

در این صفحه وارد تب Quota شوید و برای فعال کردن این قابلیت گزینه Enable quota management انتخاب کنید. برای محدود کردن فضای دیسک باید گزینه Limit disk Space to را انتخاب کنید و حجم موردنظر خود را وارد کنید که در اینجا 10 مگابایت وارد شده است یعنی اینکه کاربر می‌تواند تا همین مقدار از فضای دیسک استفاده کند، در قسمت Set warning level to اگر کاربر از 8 مگابایت فضای دیسک استفاده کرد یک اخطار برای مدیر شبکه ارسال خواهد شد. دو گزینه آخر صفحه را انتخاب کنید

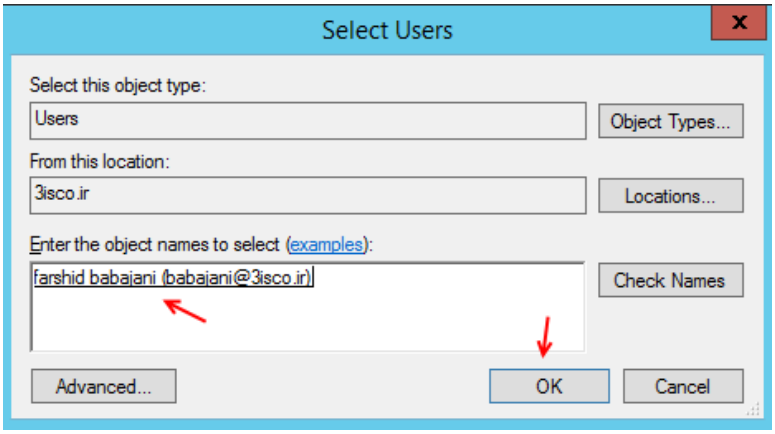
تا Log برای مدیر شبکه ارسال شود، حالا چگونه می‌توان این فضا را به یک کاربر خاص نسبت داد، برای این کار باید بر روی گزینه Quota Entries کلیک کنید.



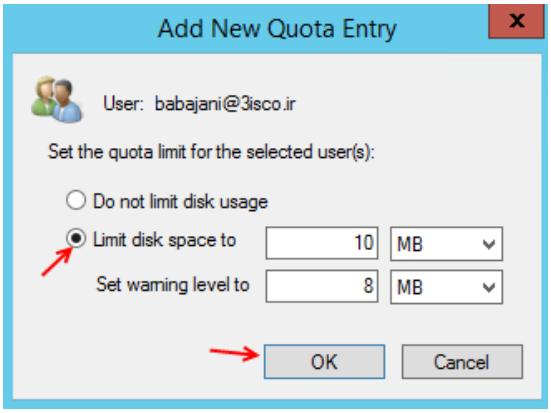
در این صفحه برای اینکه مقدار فضای خود را به یک کاربر نسبت دهیم باید بر روی آیکون New Quota کلیک کنید.



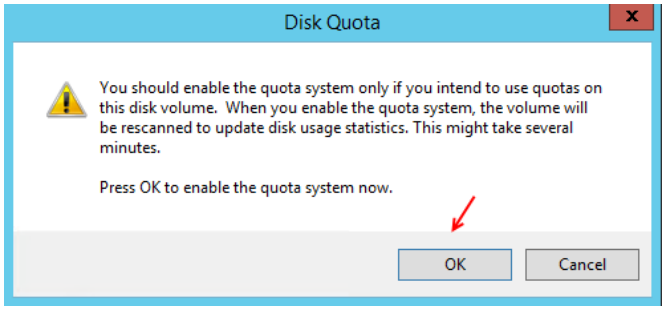
در این قسمت کاربر موردنظر خود را به لیست اضافه می‌کنیم، برای این کار می‌توانید از گزینه Advanced استفاده کنید، بعد از اضافه کردن کاربر موردنظر بر روی ok کلیک کنید.



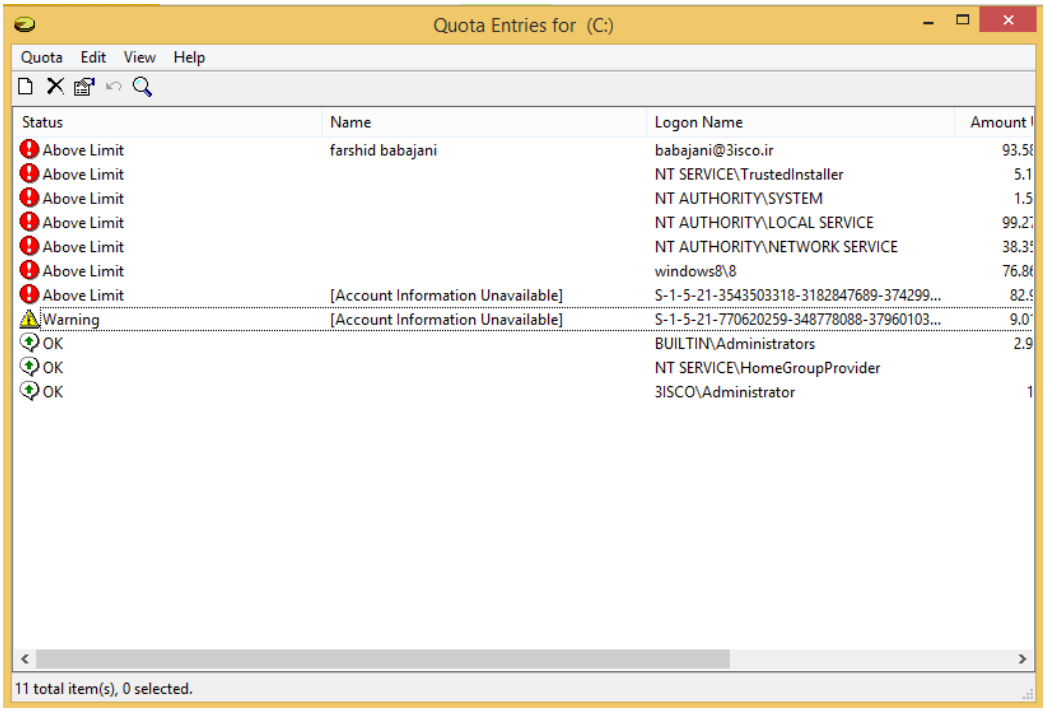
در این قسمت مقدار فضای موردنظر را برای کاربر موردنظر مشخص می‌کنیم، در این قسمت کاربر نمی‌تواند بیش از 10 مگابایت از فضای هارد دیسک استفاده کند، البته اگر کاربر به مرز 8 مگابایت رسید یک اخطار برای کاربر موردنظر ارسال می‌شود.



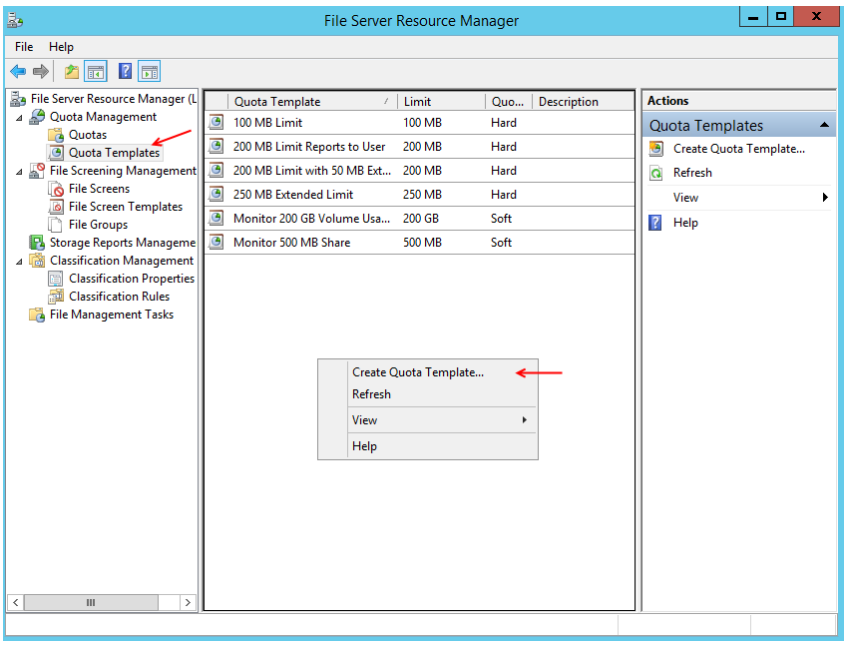
بر روی ok کلیک کنید تا اطلاعات ثبت شود، بعد از آن صفحه موردنظر را ببندید و در صفحه Properties بر روی ok کلیک کنید.



زمانی که در صفحه قبل بر روی ok کلیک کردید، این صفحه ظاهر می‌شود که، به شما این اخطار را می‌دهد که سرویس Quota را روی درایو سیستمی می‌خواهید فعال کنید که این کار درستی نخواهد بود، چون بعد از اینکه بر روی ok کلیک کنید صفحه‌ای شبیه به شکل زیر را مشاهده خواهید کرد.



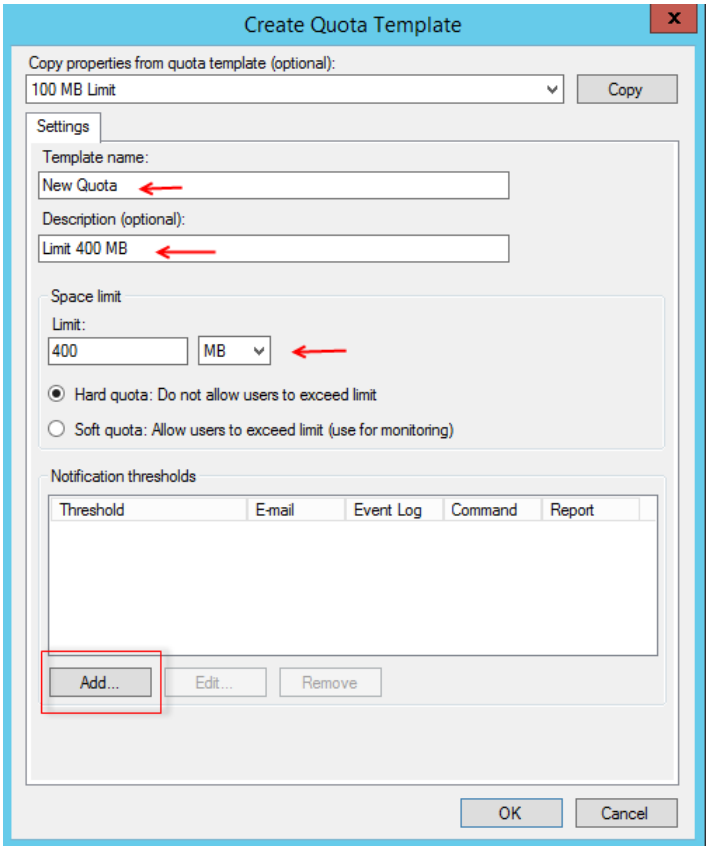
این قسمت مربوط به Quota Entries می‌باشد که با هم کاربر خود را به آن اضافه کردیم، همانطور که مشاهده می‌کنید سرویس‌هایی که از منابع سرور استفاده می‌کردند محدود شده اند و این نشان دنده این است که نباید Quota را روی درایو سیستم که اصولاً درایو C است فعال کنیم، پس این نکته را هیچ وقت فراموش نکنید.



بعد از این که سرویس Quota را روی درایو موردنظر بررسی کردیم دوباره وارد سرویس File Server Resource می‌شویم و از سمت چپ گزینه Quota Templates را

انتخاب کنید و در صفحه باز شده کلیک راست کنید و گزینه Creat Quota Templates را انتخاب کنید.

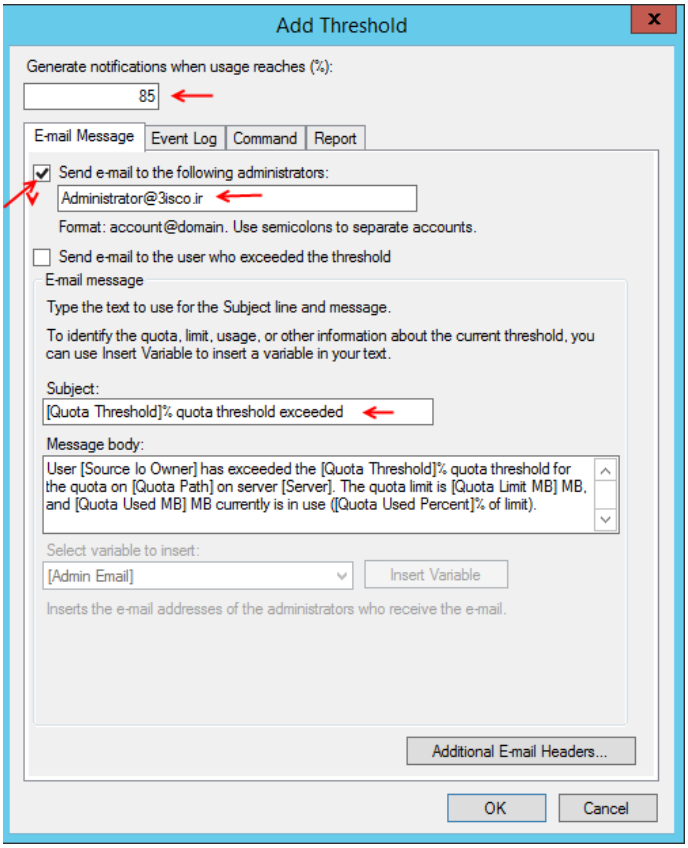
در این قسمت می‌خواهیم یک Quota Template ایجاد کنیم و یک مقدار خاص را به آن اختصاص دهیم و از طریق Quota به یک درایو و یا پوشه موردنظر اختصاص دهیم.



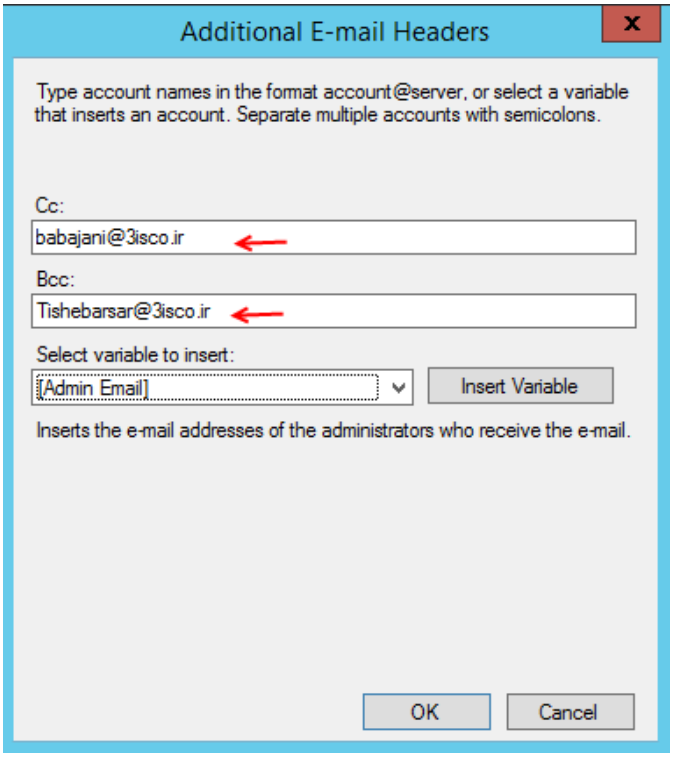
در این صفحه، در قسمت Template Name نام دلخواه خود را وارد کنید و در قسمت Description توضیحات آن را وارد کنید. در بخش Space limit باید در فیلد Limit حداکثر فضای مصرفی را وارد کنید و در جلوی آن یکی از مقادیر MB,GB,.... را انتخاب کنید که در اینجا 400 MB وارد شده است. دو گزینه Hard Quota و Soft Quota وجود دارد که در این قسمت گزینه Hard Quota را انتخاب کنید.

Hard Quota یعنی اینکه یک کاربر نمی‌تواند بیشتر از حجم مورد استفاده کند ولی گزینه Soft Quota به این منظور است که زمانی کاربر بیشتر از حجم موردنظر استفاده کرد، برای شما فقط اخطار ارسال می‌شود.

در این قسمت Hard Quota را انتخاب کنید، در قسمت Notification Thresholds باید یک سری Log به مجموعه اضافه کنیم که مثلاً اگر حجم مصرفی به 85% رسید به مدیر شبکه ایمیل داده شود و یا Log ارسال شود، این روش‌ها برای Monitoring شبکه بسیار مهم می‌باشند و مدیر شبکه باید این توانایی را در اشکال‌زدایی مشکلات توسط Log داشته باشد، برای این کار بر روی Add کلیک کنید.



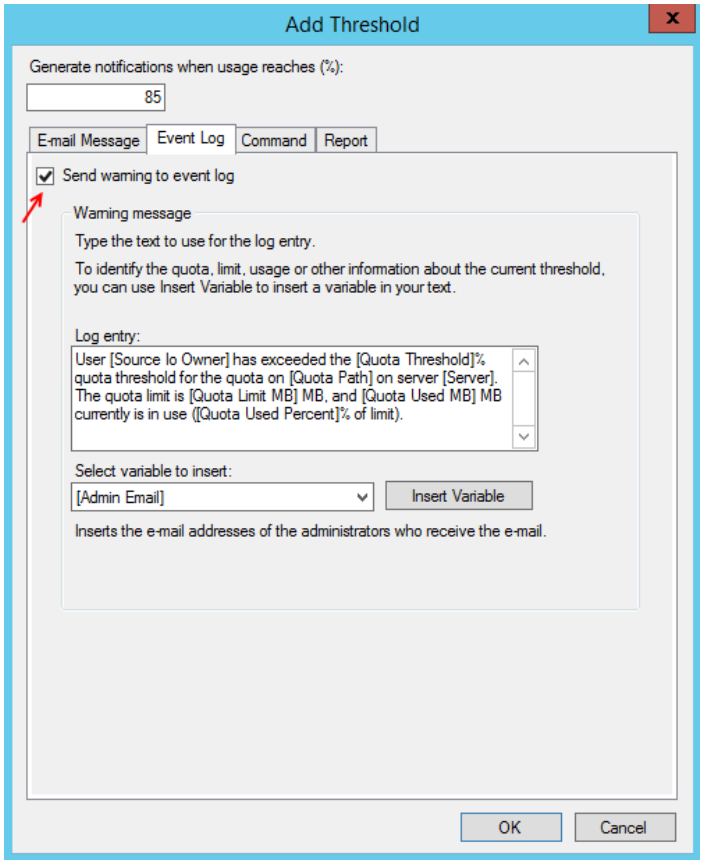
در این صفحه وارد تب E-mail Message شوید، در قسمتی که 85 نوشته به این منظور است که زمانی که کاربر از 85 درصد کل فضای 400 مگابایت استفاده کرد کارهای زیر آن انجام بگیرد یعنی اینکه تیک گزینه Send e-mail... را انتخاب کنید و ایمیل مدیر شبکه را وارد کنید، البته باید سرویس SMTP از قبل فعال شده باشد، در قسمت Subject عنوان ایمیل را وارد می‌کنید که به جای Quota Thresholds مقدار 85% قرار خواهد گرفت، در قسمت Message body هم اطلاعات مربوط به Quota قرار دارد که به همراه ایمیل ارسال خواهد شد، برای اینکه این اطلاعات به ایمیل‌های دیگر ارسال شود باید بر روی Additional E-mail Headers کلیک کنید.



در این صفحه باید ایمیل‌های دیگر خود را در قسمت CC, Bcc وارد کنید.

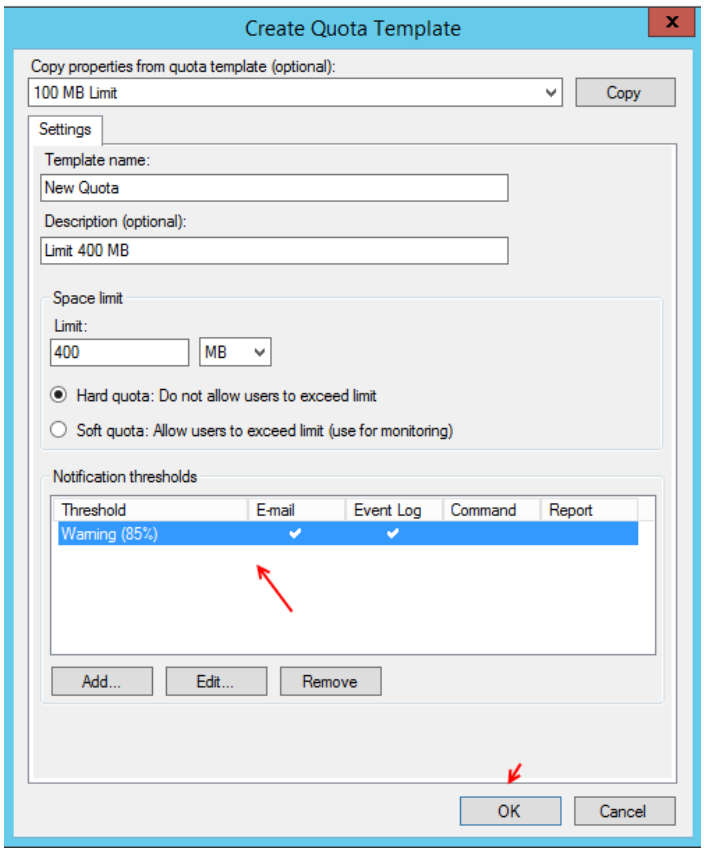
برای اضافه کردن یک Variable جدید بر روی Insert Variable کلیک کنید.

بر روی ok کلیک کنید تا اطلاعات ثبت شود.



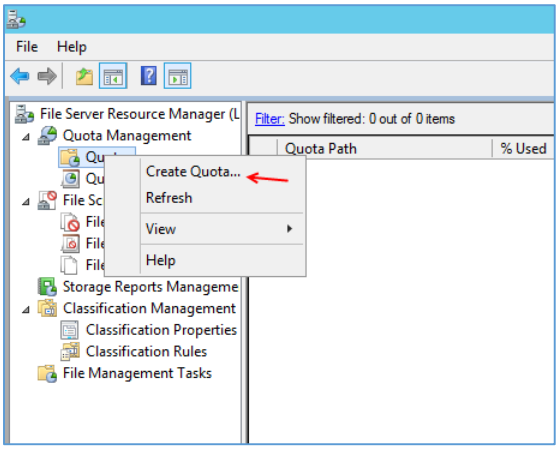
در تب Event Log با فعال کردن Send warning to event log و انتخاب Log entry مشخص برای شما Log فرستاده می‌شود، تب Command هم برای اجرای Script مشخص است و تب Report هم برای ارسال گزارش با جزئیات مشخص به ایمیل خاص است.

بر روی ok کلیک کنید.

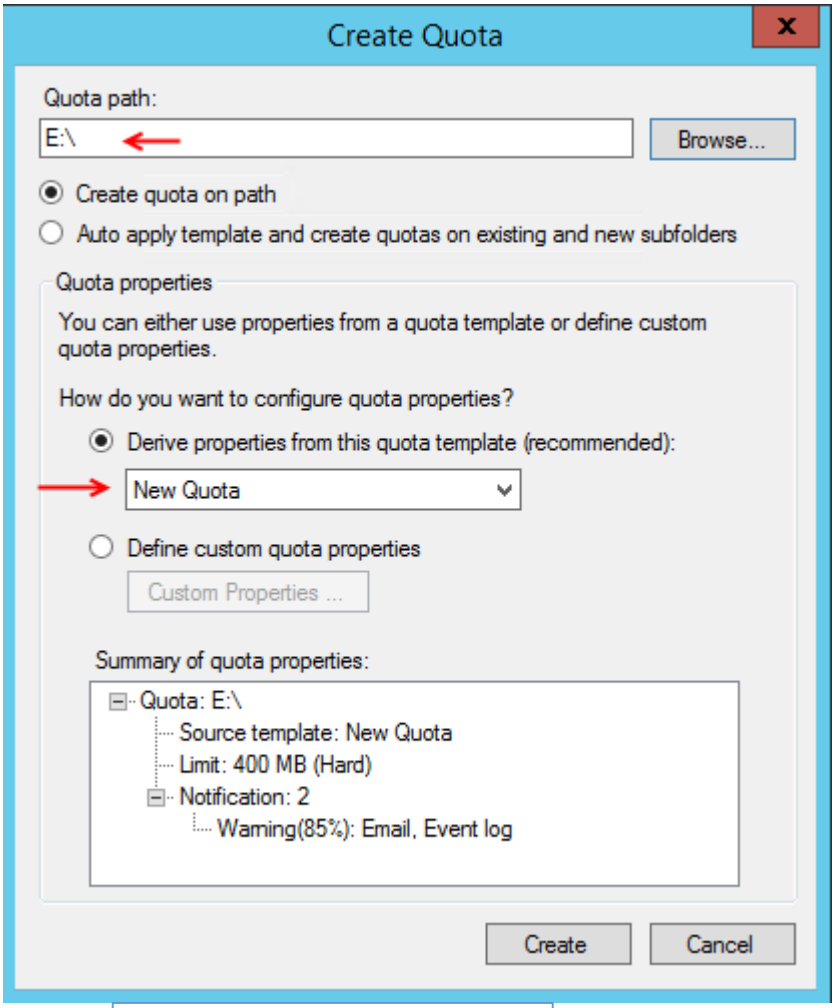


همانطور که در این قسمت مشاهده می‌کنید Notification موردنظر به لیست اضافه شده که عدد آن 85% را نشان می‌دهد که ما از قبل این موضوع را مشخص کردیم.

بر روی ok کلیک کنید تا Quota Template موردنظر ایجاد شود.

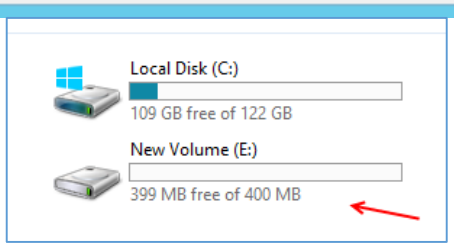


بعد از ایجاد Quota Template از سمت چپ بر روی Quota کلیک کنید و بر روی آن کلیک راست کنید و گزینه Create Quota را انتخاب کنید.



در این صفحه، در قسمت Quota Path باید درایو و وفولدری را که می‌خواهید Quota روی آن اجرا شود را انتخاب کنید که در اینجا درایو E انتخاب شده است، در قسمت Derive properties from this.... باید همان Quota Template را انتخاب کنید که در مرحله قبل ایجاد کرده بودیم که بعد از انتخاب New Quota اطلاعات آن در قسمت Summary of Quota نمایش داده شده است.

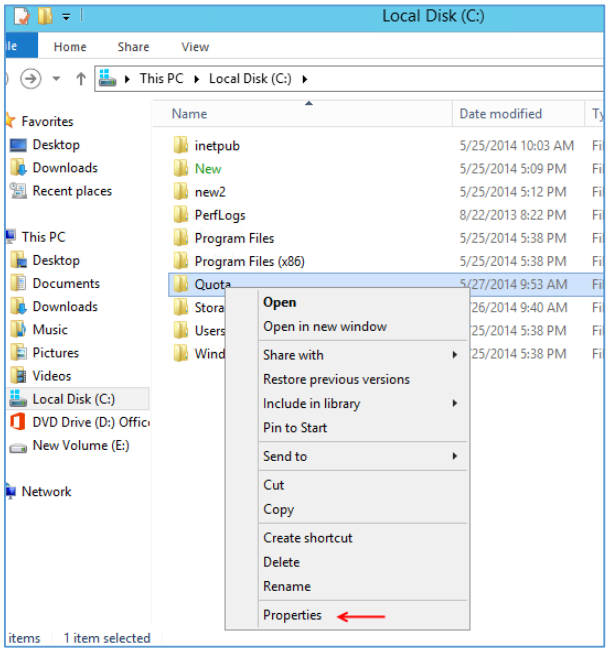
بر روی Create کلیک کنید تا Quota موردنظر ایجاد شود و درایو موردنظر محدود شود.



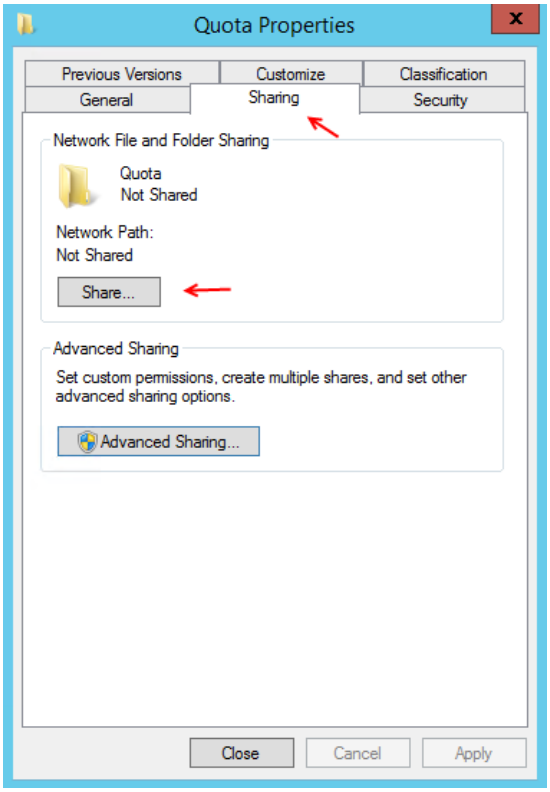
همانطور که در شکل روبرو مشاهده می‌کنید درایو E محدود شده است و فقط 400 مگابایت حجم قابل استفاده دارد.

ایجاد درایو از طریق شبکه و محدود کردن کاربران آن:

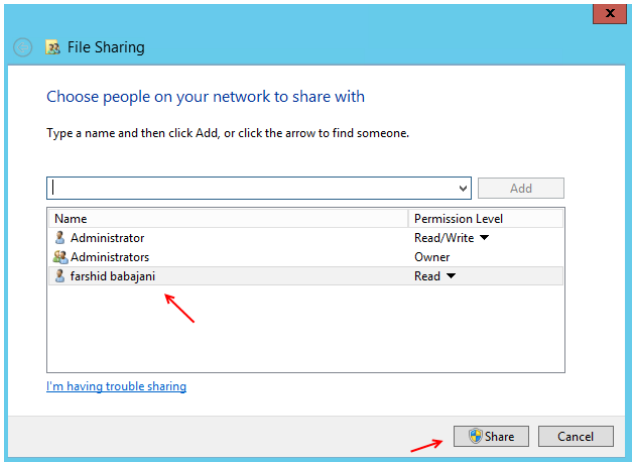
یکی از بیشترین کاربردهای استفاده از شبکه در سامان‌های بزرگ ایجاد درایو از طریق شبکه برای تمام کاربران است، در این قسمت می‌خواهیم یک درایو شبکه‌ای ایجاد کنیم و کاربران را محدود کنیم تا فقط از حجم مشخصی استفاده کنند، برای شروع باید یک پوشه در یکی از درایوهای سرور ایجاد کنیم البته می‌توان این کار را روی یک درایو هم انجام داد.



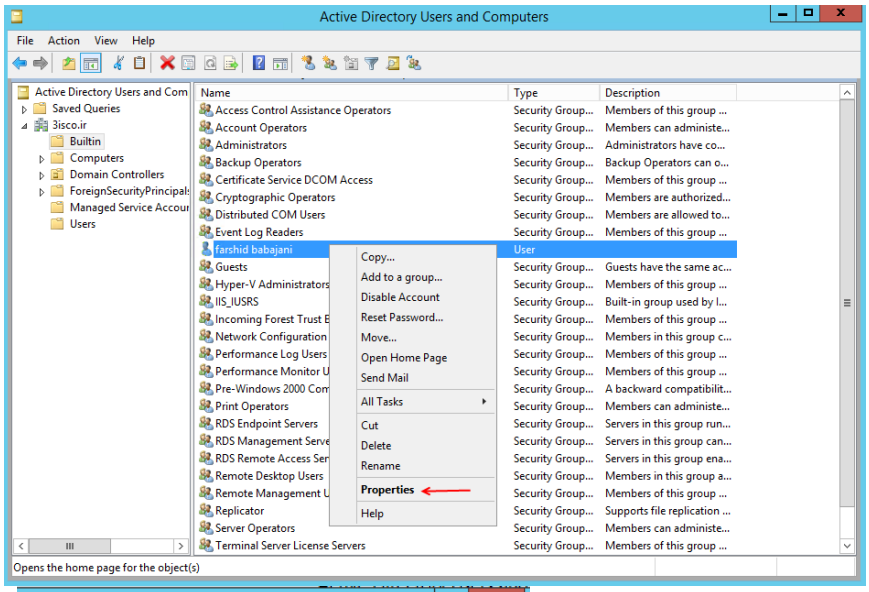
وارد درایو C می‌شویم و یک پوشه با نام Quota ایجاد می‌کنیم، البته شما می‌توانید با هر اسمی این پوشه را ایجاد کنید، بر روی آن کلیک راست می‌کنیم و گزینه Properties ر انتخاب می‌کنیم.



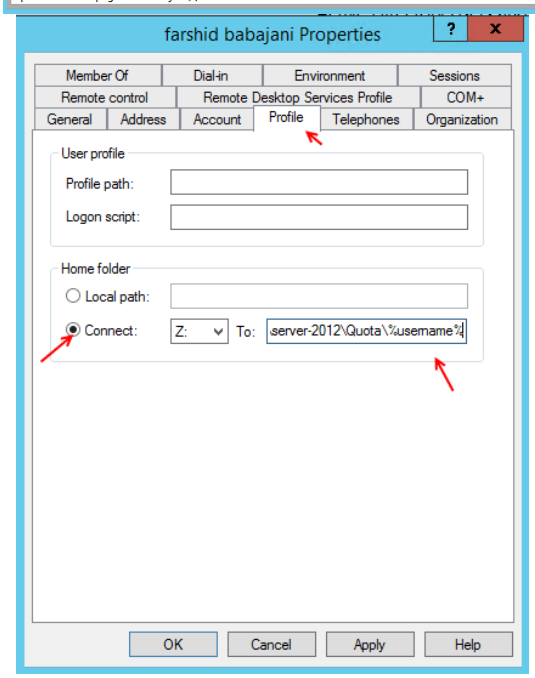
در این صفحه وارد تب Sharing شوید و گزینه Share را انتخاب کنیدتا شکل بعد ظاهر شود.



در این قسمت باید کاربر خود را با کلیک بر روی Add به لیست اضافه کنید و توانایی Read را به آن بدهید و بعد بر روی Share کلیک کنید.



بعد از انجام کارهای مشخص‌شده بالا، وارد Active Directory Users and Computer شوید و بر روی کاربر موردنظر خود کلیک راست کنید و گزینه Properties را انتخاب کنید.

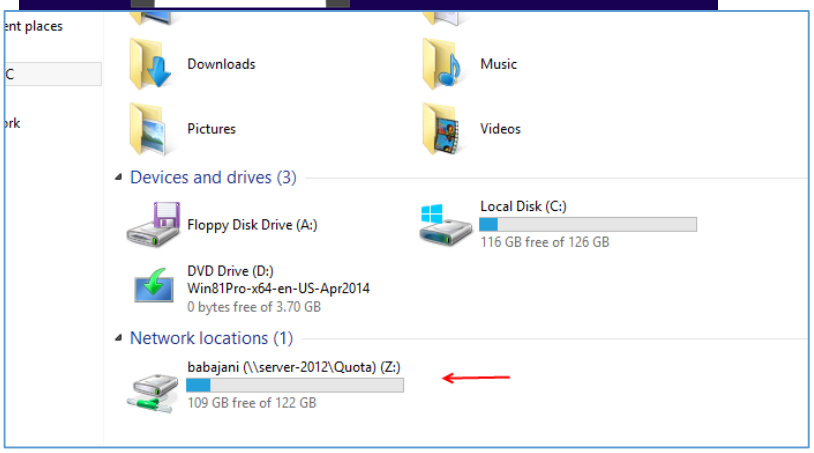


در این صفحه وارد تب Profile شوید و گزینه Connect را انتخاب کنبد و یکی از نام های درایو را مثلاً Z را انتخاب کنید و در جلوی آن آدرس زیر را وارد کنید:

\\Server-2012\Quota\%username%

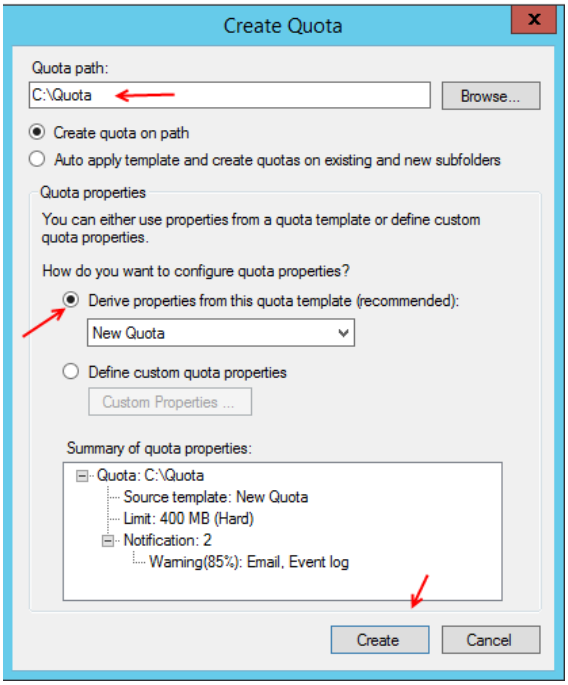
در این دستور به جای Server-2012 باید نام سرور خود را وارد کنید و به جای Qouta باید نام پوشه خودتان را وارد کنید، در قسمت آخر می‌توانید نام کاربر را وارد کنید و یا %username% وارد کنید. بر روی ok کلیک کنید تا اطلاعات ثبت شود.

بعد از آن با کاربر موردنظر وارد یکی از کلاینت‌ها می‌شویم، این موضوع را در شکل مقابل مشاهده می‌کنید.



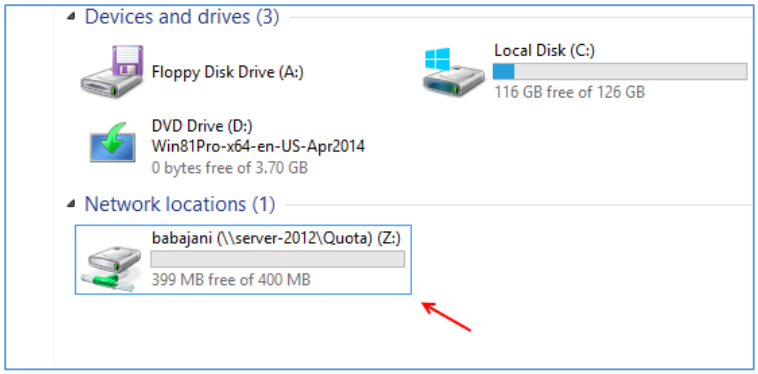
اگر وارد My Computer شویم درایو موردنظر را مشاهده می‌کنیم، حجم این درایو برابر کل درایو C در سرور اصلی می‌باشد ولی ما باید این حجم را توسط دوست عزیزمان Quota محدود کنیم.

وارد سرور اصلی شوید و سرویس File Server Resource Manager را اجرا کنید و وارد Quota شوید، بر روی Quota کلیک راست کنید و گزینه Create Quota را انتخاب کنید.



در قسمت Quota Path آدرس همان پوشه‌ای را بدهید که در قسمت قبل آن را محدود کردیم و در قسمت Derive Properties from this... همان Template که قبلاً ایجاد کردیم را انتخاب کنید تا پوشه موردنظر به 400 مگابایت محدود شود.

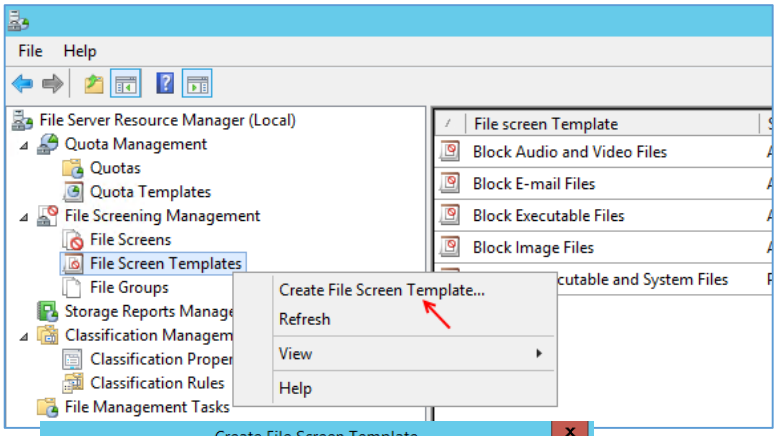
بر روی Create کلیک کنید تا Quota روی پوشه موردنظر فعال شود.



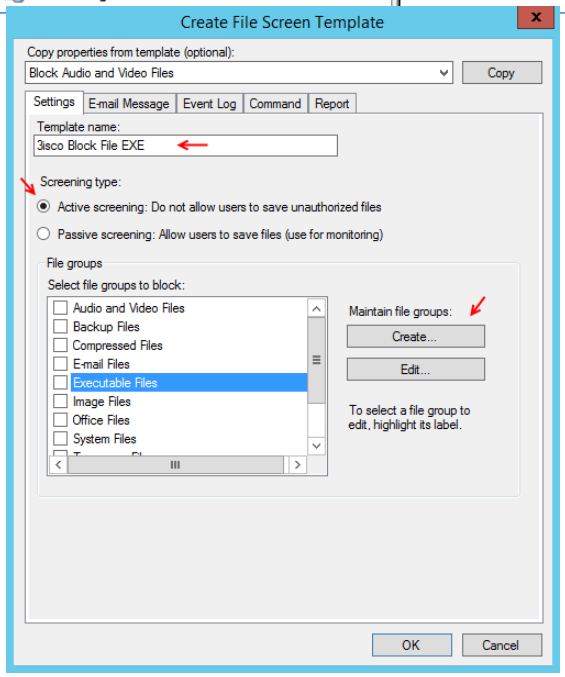
بعد از ایجاد محدودیت دوباره وارد کلاینت می-شویم و همانطور که در شکل روبرو مشاهده می-کنید Quota کار خود را انجام داده است و پوشه موردنظر محدود شده است.

جلوگیری از کپی کردن نوع خاصی از فایل برای کاربران:

در این قسمت به بررسی توانایی دیگر سرویس File Server Resource Manager می‌پردازیم، این سرویس با نام File Screen می‌باشد که به مدیر شبکه این توانایی را می‌دهد تا از کپی کردن یک فایل با نوع خاص مثلاً MP3, JPEG و یا نوع دیگر جلوگیری کند.

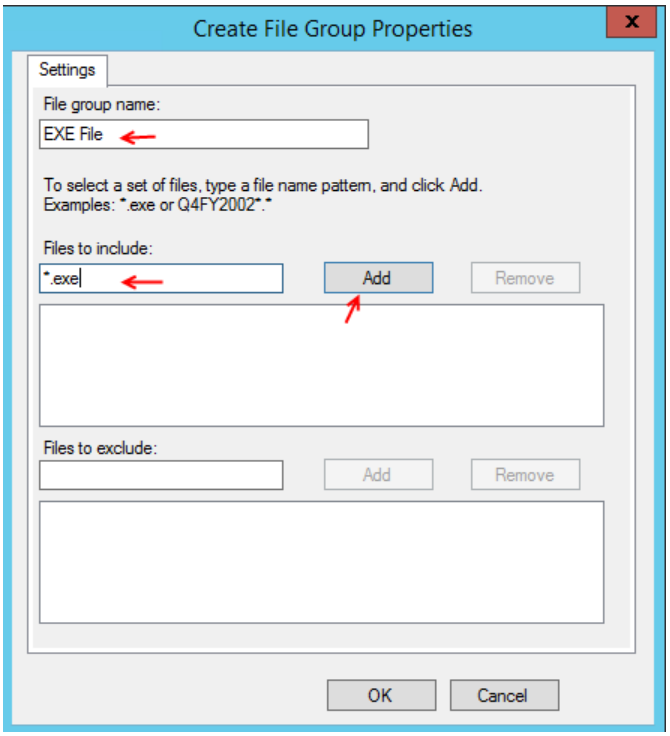


برای شروع وارد سرویس File Server Resource Manager شوید و از سمت چپ بر روی File Screen Template کلیک راست کنید و گزینه Create File Screen Template را انتخاب کنید.



در این صفحه، در قسمت Template name نام موردنظر خود را وارد کنید و در قسمت Screening type یکی از گزینه های Active Screening و Passive Screening را انتخاب کنید، اگر گزینه Active Screening را انتخاب کنید، از کپی شدن فایل موردنظر جلوگیری می‌کند، ولی اگر گزینه Passive Screening را انتخاب کنید، فایل موردنظر کپی خواهد شد و یک اخطار و یا ایمیل برای مدیر شبکه ارسال خواهد شد که مثلاً کاربر X از فایل با نوع MP3 استفاده کرده است و داخل پوشه کپی کرده است.

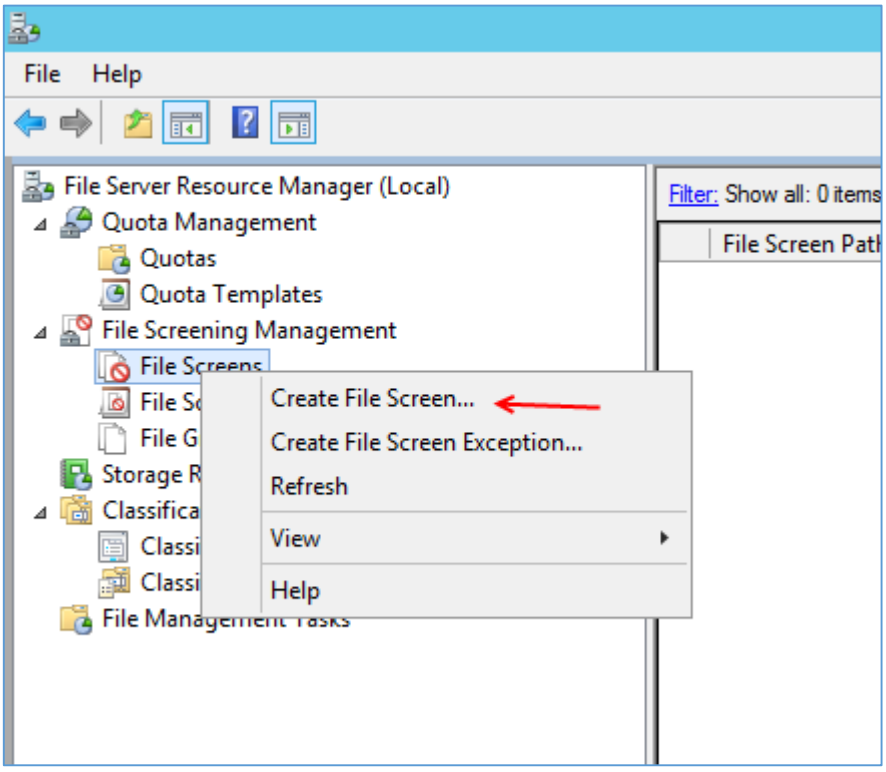
اگر به قسمت File Groups نگاه کنید، یک سری آیتم از قبل ایجاد شده است که هر کدام پسوندهای متفاوتی را شامل می‌شوند، مثلاً Executable Files شامل نوع‌های Exe,Bat,.... است، برای اینکه یک پسوند جدید خودمان ایجاد کنیم در شکل صفحه قبل بر روی Create کلیک کنید..



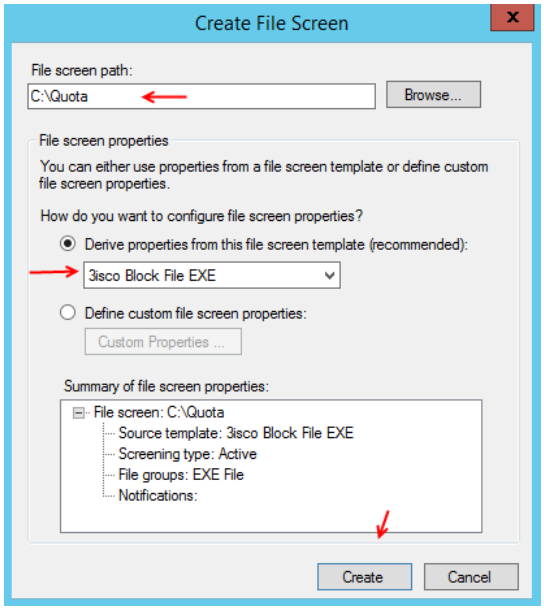
درون صفحه در قسمت File Group Name بایدنام مشخص خود را وارد کنید و در قسمت File to include باید نوع فایل خود را که در اینجا *.exe وارد شده است، وارد کنید و بعد بر روی Add کلیک کنید تا پسوند موردنظر به لیست اضافه شود.

قسمت File to Exclude به این معنی است اگر پسوند فایلی را وارد کنید، یعنی اینکه با این پسوند کاری نداشته باش.

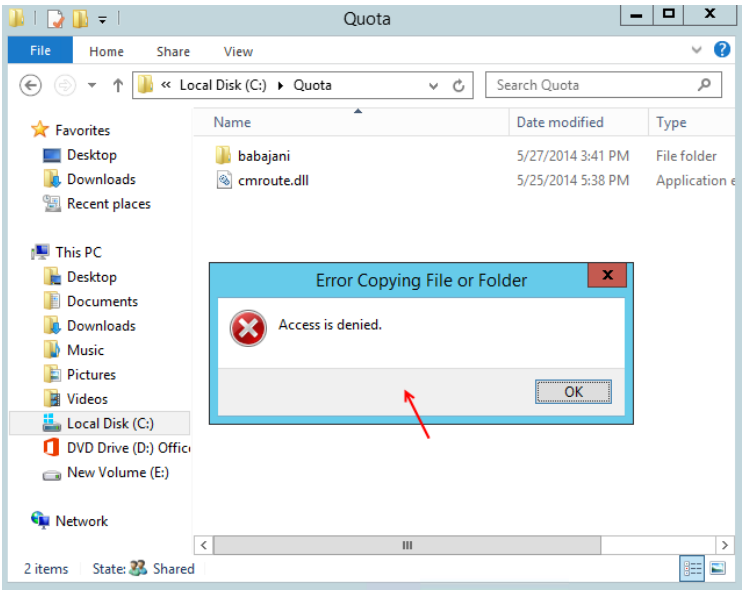
بر روی ok کلیک کنید و در صفحه بعد هم بر روی ok کلیک کنید تا Template موردنظر ایجاد شود.



بعد از ایجاد Template بر روی File Screen کلیک راست کنید و گزینه Create File Screen کلیک کنید تا شکل بعد ظاهر شود.



در این صفحه باید با کلیک بر روی دکمه Browse مسیر پوشه یا درایوی که می‌خواهید این محدودیت روی آن اعمال شود را انتخاب کنید، بعد از آن در قسمت Derive properties from باید همان Template را انتخاب کنید که در قسمت قبل ایجاد کردیم، در پایان بر روی Create کلیک کنید تا محدودیت اعمال شود.



همانطور که در شکل مقابل مشاهده می‌کنید، با کپی کردن فایل با پسوند EXE با Error روبرو مواجع شدیم.

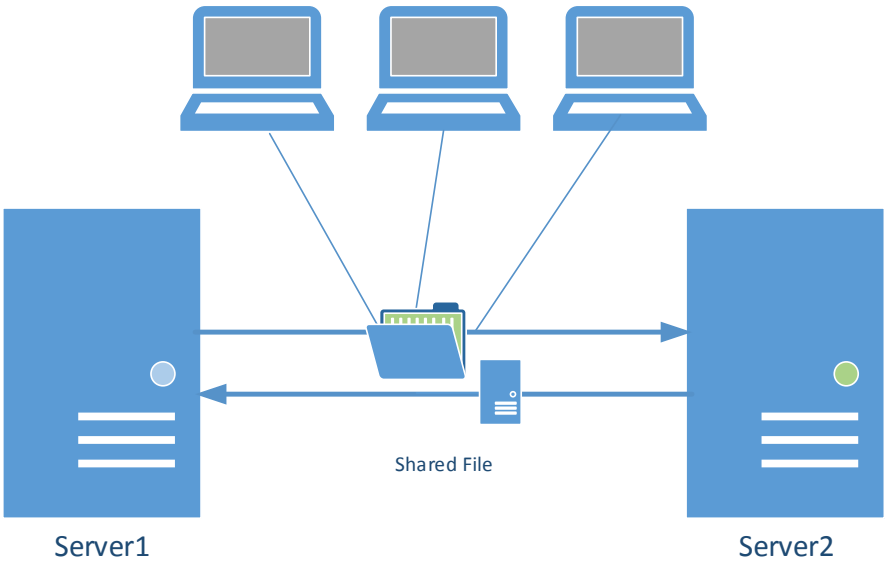
این روش بیشتر در دانشگاه‌ها مشاهده شده است که از کپی فایل‌های Zip و یا MKV و .... جلوگیری می‌شود.

خوب سرویس File Server Resource Manager کاربردهای خاصی دارد که شما حتماً در شبکه خود از این سرویس استفاده کنید.

اگر درباره این سرویس سوالی داشتید، از طریق ایمیل با من در تماس باشید.

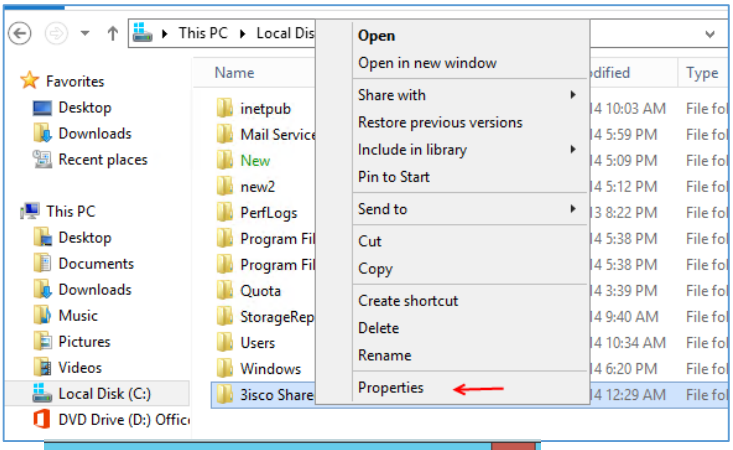
کار با سرویس DFS یا Distributed File System:

شاید در سازمانی که کار می‌کنید از چند سرور مختلف استفاده می‌کنید و روی هر کدام از آنها فایل‌های خود را Share می‌کنید و برای بدست آوردن فایل‌ها باید هر کدام از آدرس‌های سرور را جداگانه وارد کنید که همین کار باعث هدر رفت زمان خواهد شد، با استفاده از سرویس DFS شما می‌توانید فایل‌های Share مربوط به پوشه خاص را با هم Synchroniz کنید، یعنی اینکه اگر در یک سرور پوشه‌ای با نام X را Share کردید و در سرور دیگر پوشه‌ای با نام Y را Share کردید، می‌توانید با استفاده از این سرویس این دو پوشه در دو سرور مختلف را داخل یک پوشه قرار دهید. شکل زیر این موضوع را نمایش می‌دهد.

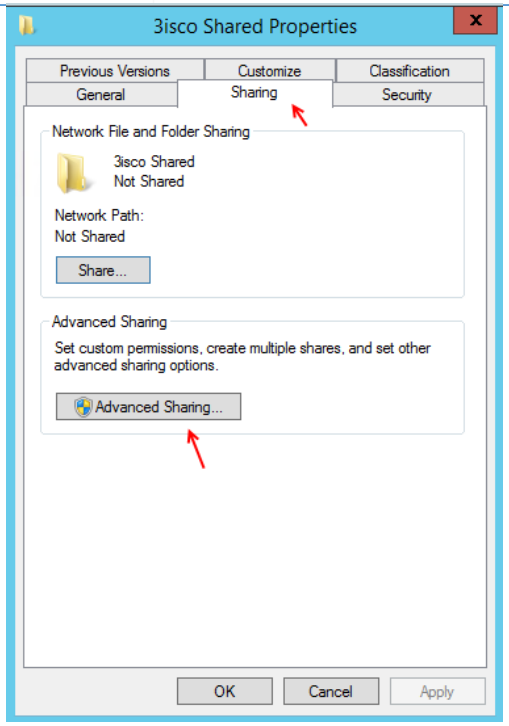


برای شروع کار نیاز به دو سرور داریم که بر روی آنها ویندوز سرور 2012 نصب شده است، روال کار به این صورت است که اول در هر دو سرور یک پوشه را به دلخواه خود Share می‌کنیم و یک سری دسترسی ها را به آن می‌دهیم، بعد از آن سرویس‌های DFS را روی هر دو سرور نصب می‌کنیم و عملیات انتقال را انجام می‌دهیم.

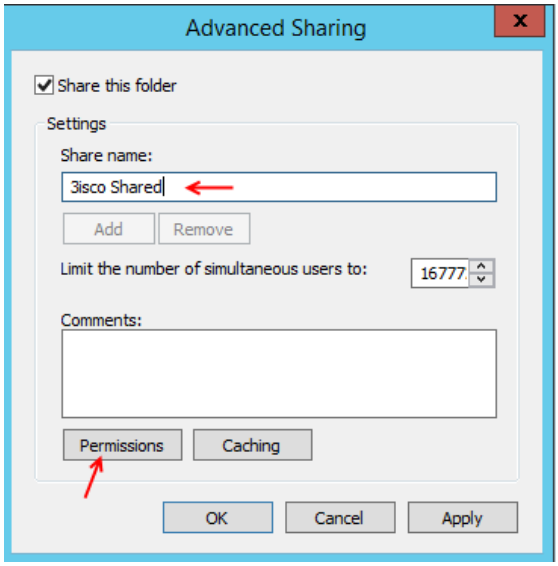
در این سناریو یک سرور به عنوان سرور اصلی که روی آن سرویس Active Directory فعال شده است و سرور دیگر زیر مجموعه سرور اول می‌باشد، در کل تفاوتی ندارد که حتماً Active Directory نصب شده باشد، دو سرور اگر با هم شبکه شده باشند می‌توان این موضوع را انجام داد.



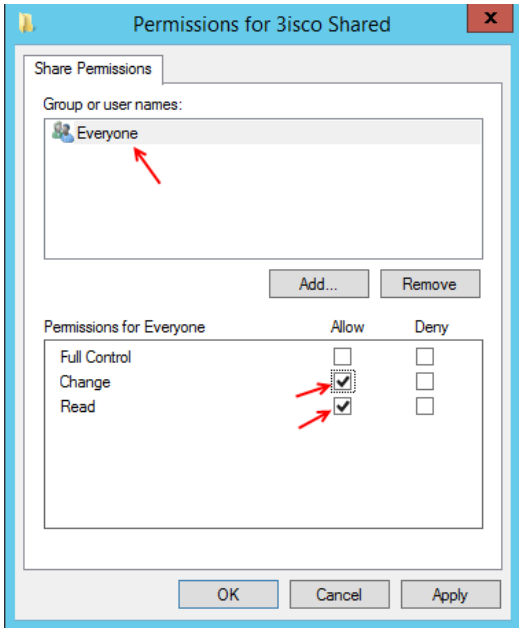
وارد سرور اول می‌شویم و یک پوشه با نام 3isco Shared ایجاد می‌کنیم و بعد بر روی آن کلیک راست می‌کنیم و گزینه Properties را انتخاب می‌کنیم.



در این صفحه وارد تب Sharing شوید و بر روی Advanced Sharing کلیک کنید تا شکل بعد ظاهر شود.



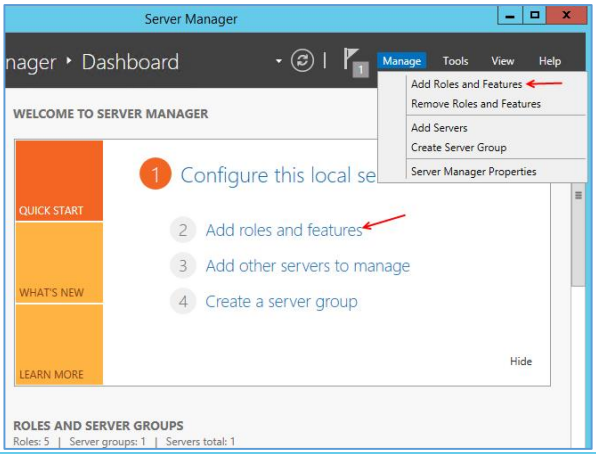
در قسمت Share name نام موردنظر خود را وارد کنید و در قسمت Comments بر روی Permissions کلیک کنید.



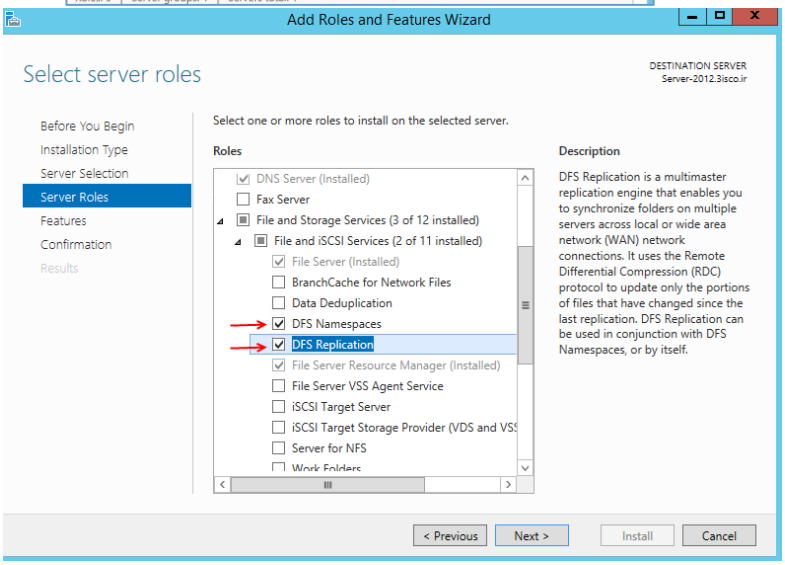
در این صفحه گروه Everyone را انتخاب کنید و مجوزهای Change و Read را برای آن فعال کنید، توجه داشته باشید تمام کاربران در شبکه عضو این گروه می‌باشند.

بر روی ok کلیک کنید تا پوشه موردنظر Share شود، دقیقاً همین کار را در سرور دیگر انجام دهید و پوشه‌ای در درایو موردنظر خود ایجاد و آن را با مجوزهای لازم به مانند شکل روبرو Share کنید.

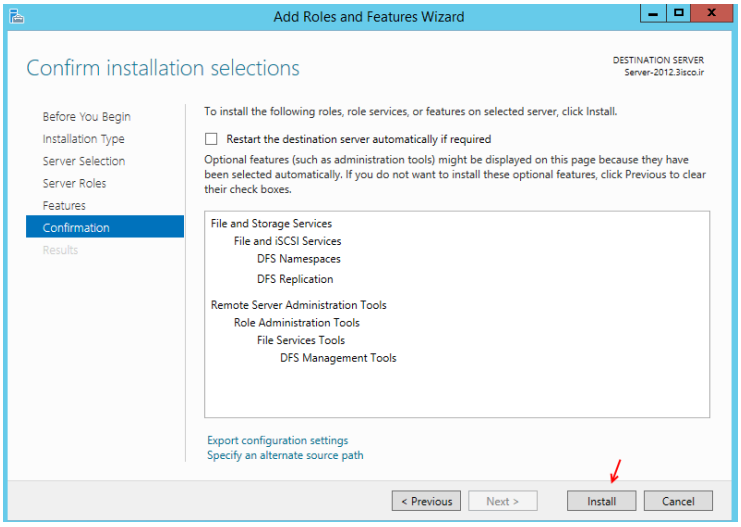
بعد از share کردن فایل نوبت به نصب سرویس می‌رسد، توجه داشته باشید که نصب سرویس باید در هر دو سرور به مانند یکدیگر انجام شود.



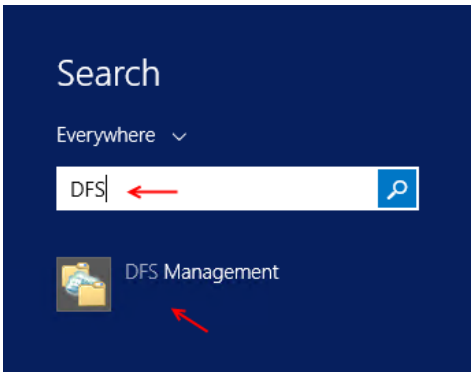
برای شروع وارد Server Manager می‌شویم و در صفحه باز شده بر روی Add Roles and Features کلیک می‌کنیم. توجه داشته باشید این کار را هم می‌توانیم از طریق منوی Manage انجام دهید.



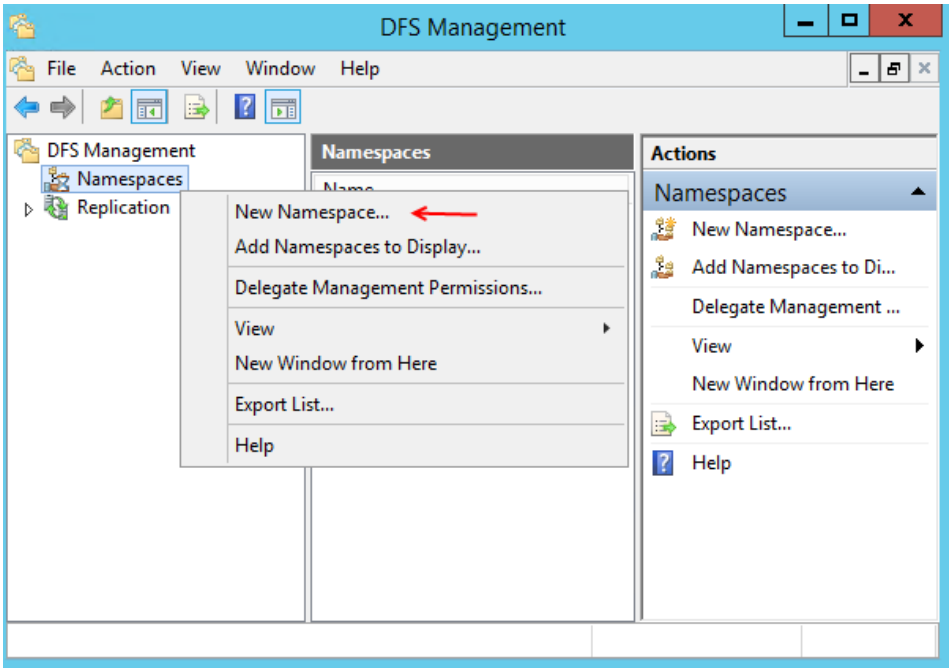
وارد قسمت Server Roles شوید و از Role های موجود وارد قسمت File and storage.. بعد وارد File and iSCSI... شوید و دو گزینه DFS Namespaces و DFS Replication را انتخاب و بر روی Next کلیک کنید تا به قسمت Configuration که شکل آن را در صفحه بعد مشاهده می‌کنید برسید.



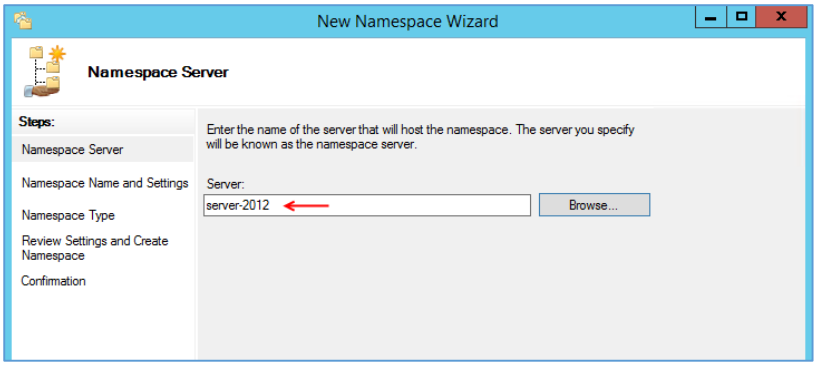
در این صفحه برای نصب سرویس موردنظر بر روی install کلیک کنید.



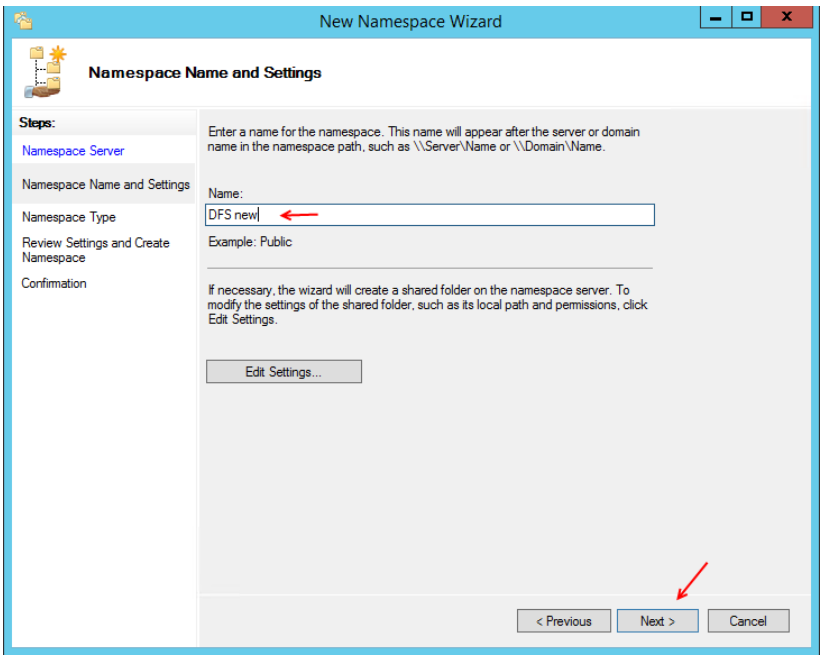
بعد از نصب سرویس از طریق Search سرویس DFS را به مانند شکل روبرو اجرا کنید.



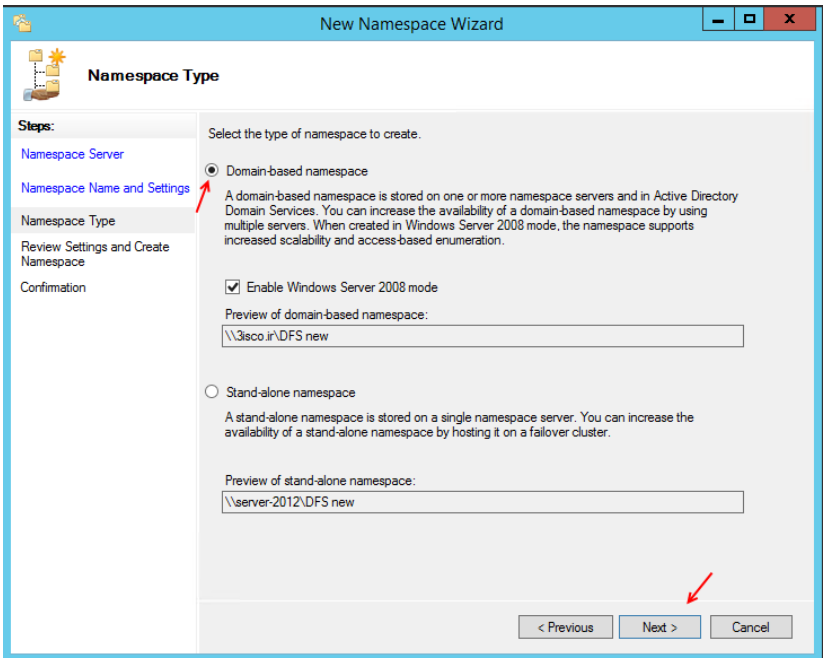
بعد از اجرای سرویس موردنظر از سمت چپ بر روی Namespace کلیک کنید و یا می‌توانید گزینه New Namespace را از سمت راست سرویس انتخاب کنید.



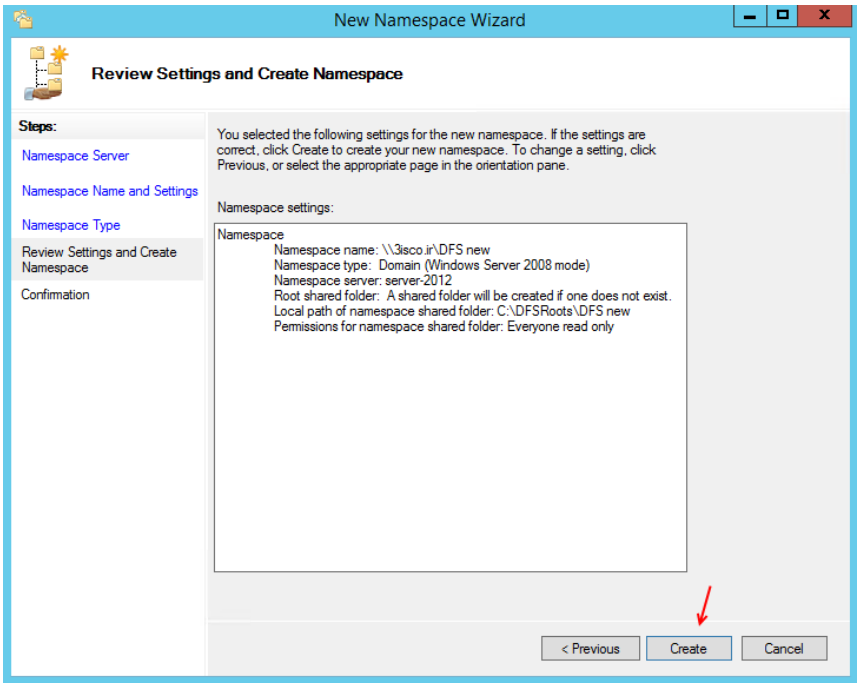
در این صفحه باید نام سرور خود را وارد کنید، اگر دقیق نمی‌دانید می‌توانید با کلیک بر روی Browse نام سرور موردنظر را پیدا کنید. برای ادامه کار بر روی Next کلیک کنید.



در این صفحه یک اسم به دلخواه خود وارد کنید و بر روی Next کلیک کنید.



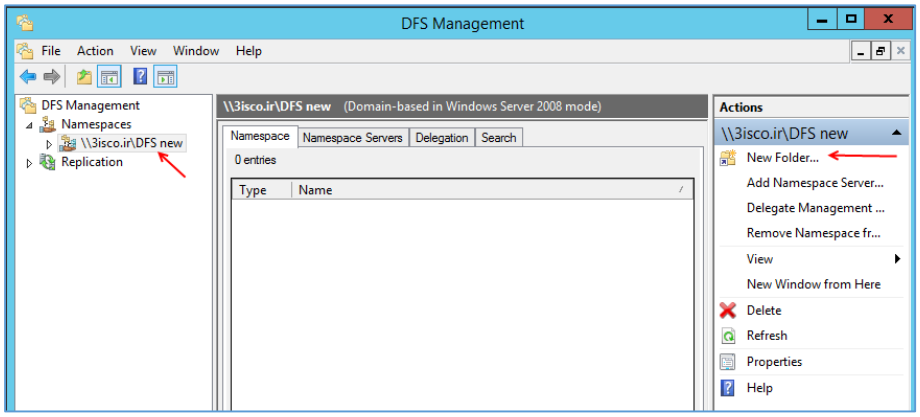
در این صفحه دو گزینه وجود دارد که گزینه Domain-based namespace را انتخاب کنید، تفاوت این گزینه با گزینه Stand-alone این است که می‌تواند چندین سرور را هم زمان پشتیبانی کند. بر روی Next کلیک کنید.



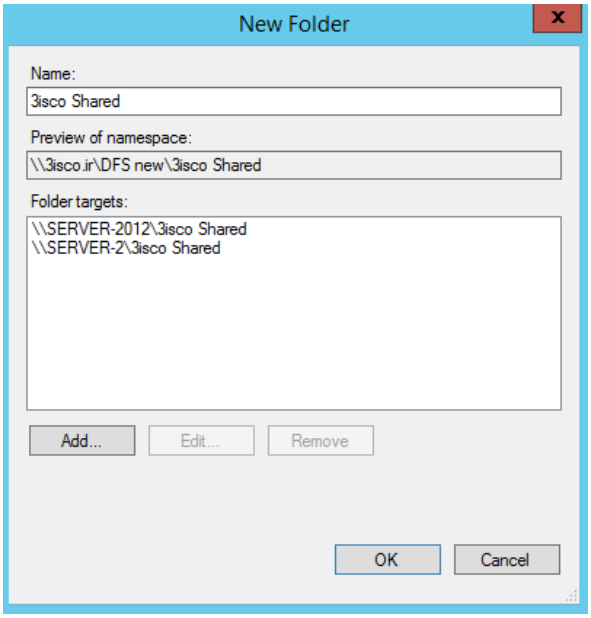
در این صفحه اطلاعات کامل نمایش داده می‌شود و برای ایجاد Namespace بر روی Create کلیک کنید.

کمی زمان خواهد برد....

بعد از ایجاد Namespace موردنظر بر روی Close کلیک کنید.

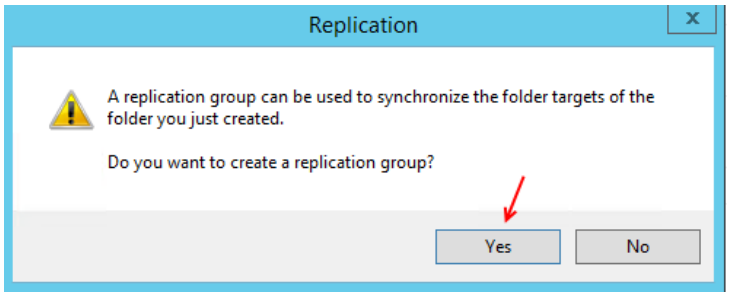


از سمت چپ Namespace جدید را انتخاب کنید و از سمت راست بر روی New Foldr کلیک کنید.

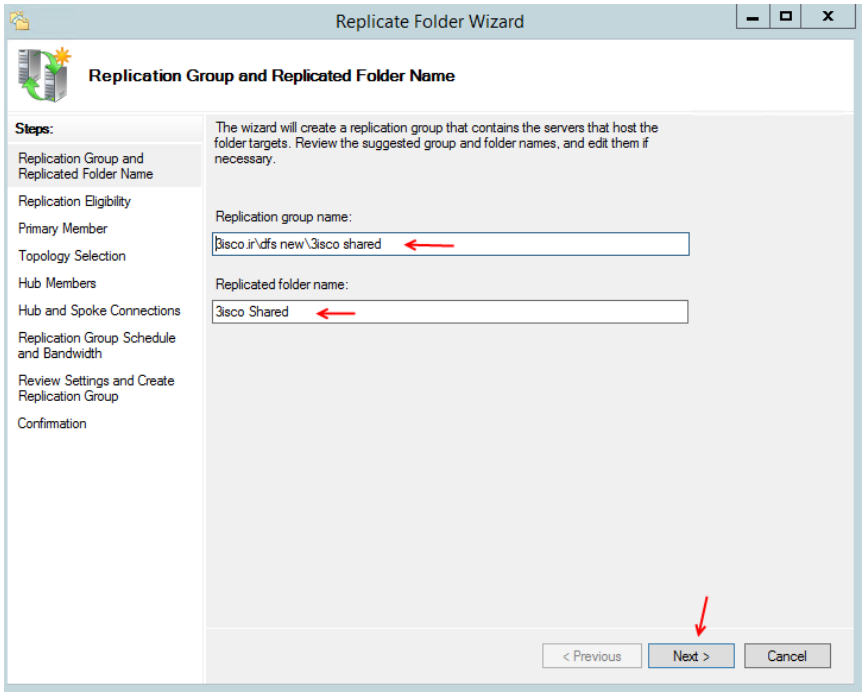


در این صفحه، در قسمت Name نام دلخواه خود را وارد کنید و در مهمترین بخش با کلیک بر روی Add پوشه share شده را که از قبل تنظیم کرده بودیم را انتخاب می‌کنیم و به لیست اضافه می‌کنیم. توجه داشته باشید در این قسمت باید پوشه های Share شده هر دو سرور به لیست اضافه شوند.

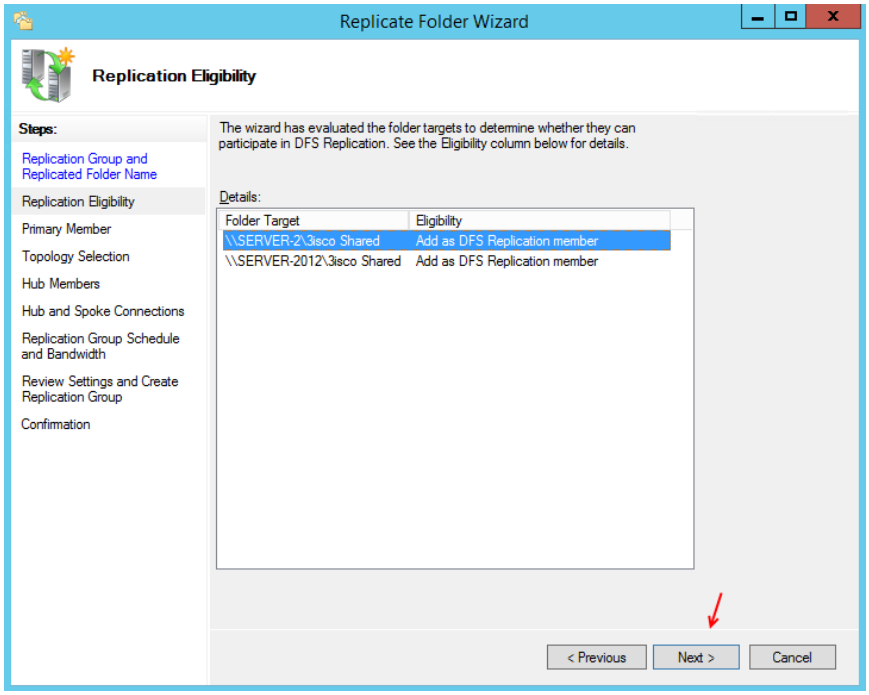
بر روی ok کلیک کنید تا New Folder ایجاد شود.



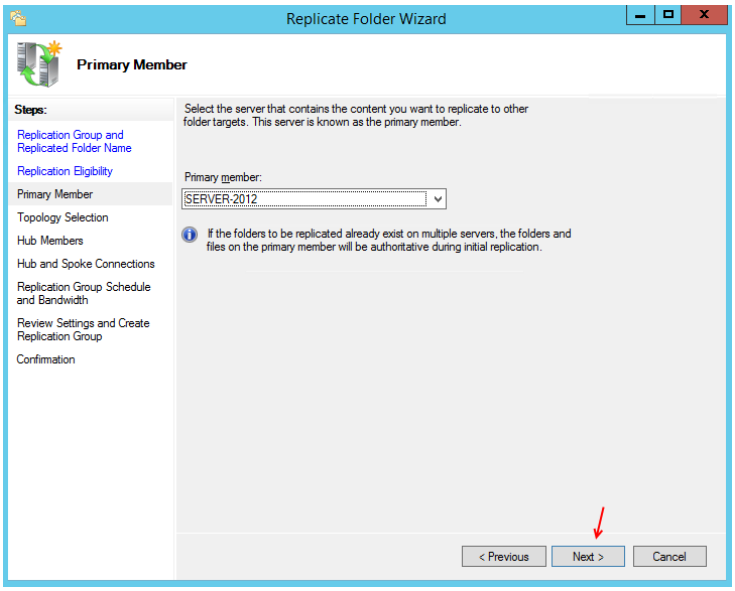
در این قسمت از شما سوال می‌شود که آیا می‌خواهید دو سرور را با هم Synchronize کنید که باید بر روی Yes کلیک کنید.



در این صفحه بر روی next کلیک کنید.

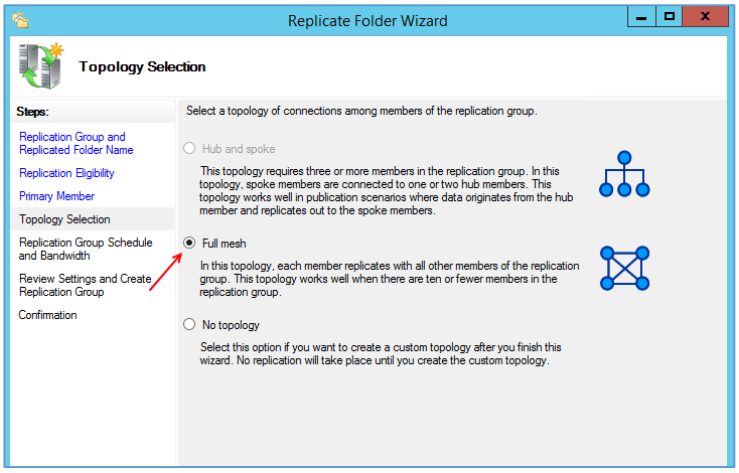


در این قسمت بر روی Next کلیک کنید.

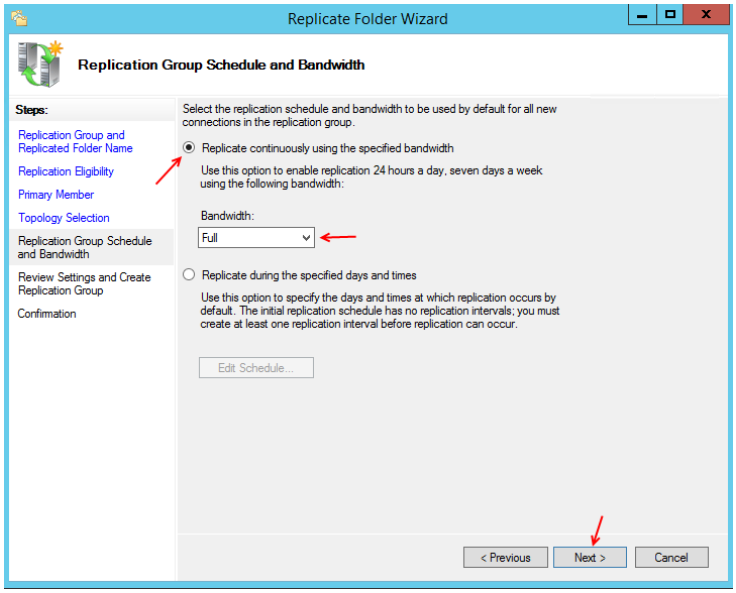


در این قسمت باید از لیست کشویی سروری را انتخاب کنید که ارجحیت بیشتری نسبت به سرور دیگر دارد، در اینجا Server-2012 سرور Active Dircetory می‌باشد.

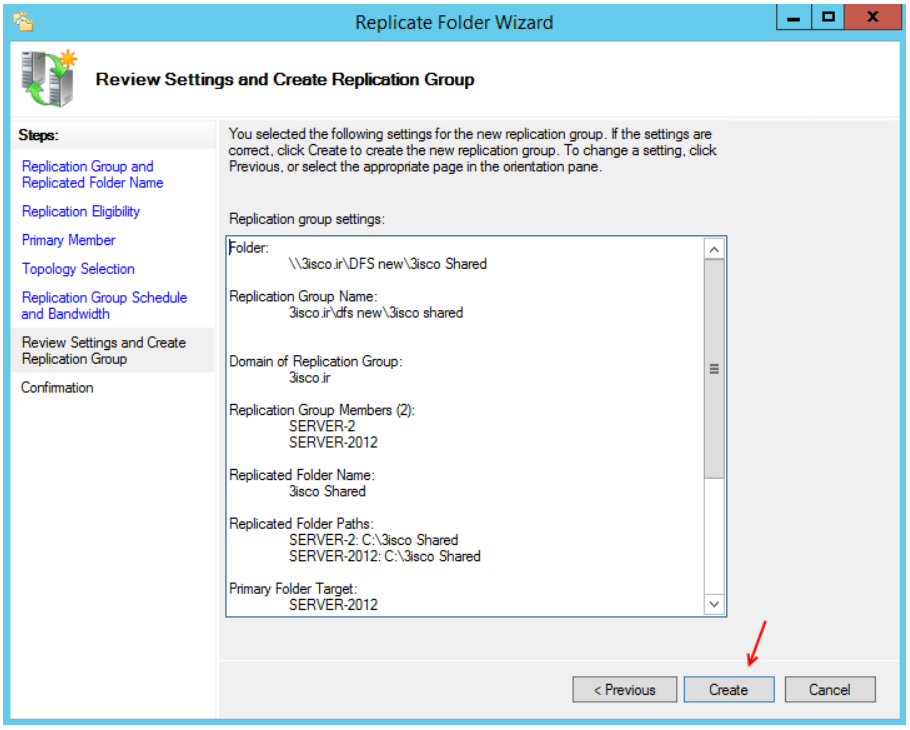
بر روی next کلیک کنید.



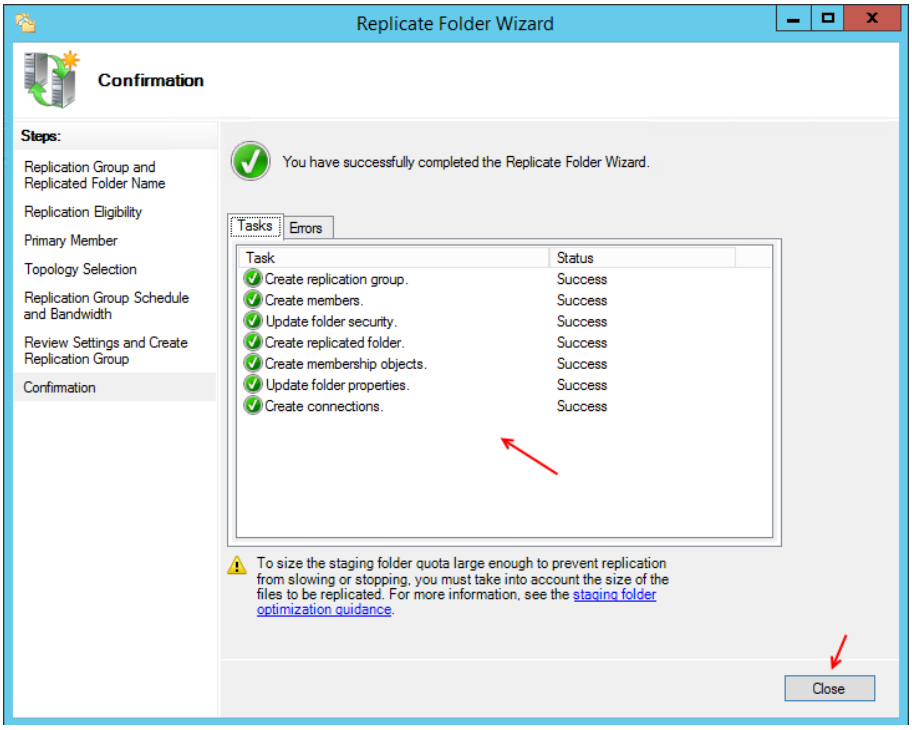
در این قسمت باید توپولوژی شبکه را مشخص کنید که درباره توپولوژی در کتاب CCNA خودم به صورت کامل صحبت کردم که، در این قسمت گزینه Full Mesh را انتخاب و بر روی Next کلیک کنید.



در این صفحه شما می‌توانید مشخص کنید زمانی که بین دو سرور اطلاعات در حال انتقال است چقدر از حجم مصرفی شبکه را مصرف کند که در این قسمت گزینه Full انتخاب شده است، ولی اگر نیاز به زمان بندی دارید می‌توانید گزینه Replicate during the... را انتخاب کنید و بر روی Edit Schedule کلیک کنید. برای ادامه کار بر روی next کلیک کنید.

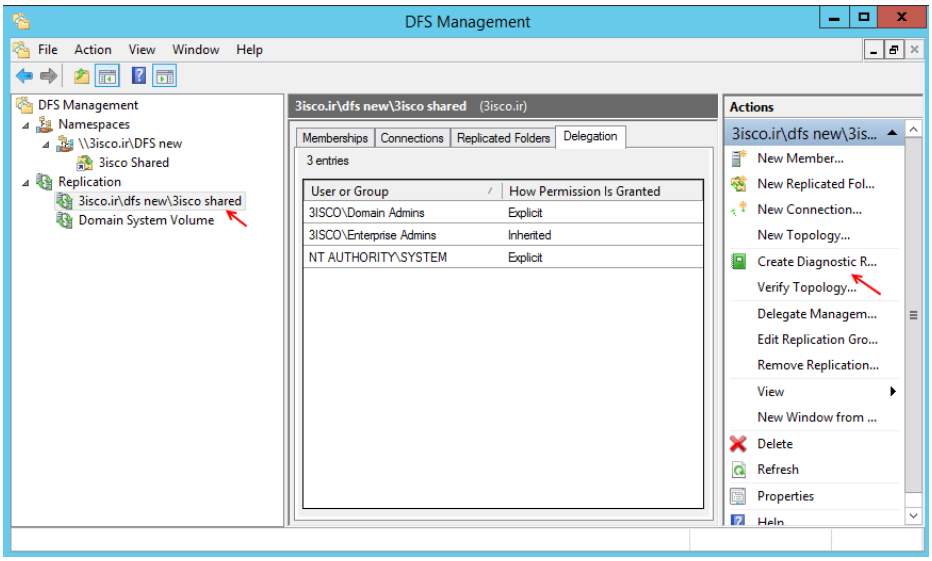


در آخر کار بر روی Create کلیک کنید تا عملیات همسان سازی انجام شود.

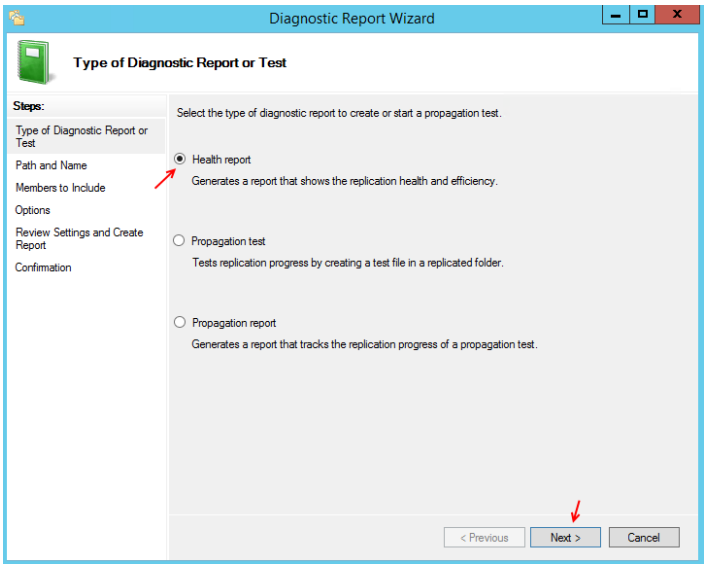


همانطور که مشاهده می‌کنید، تنظیمات به درستی انجام شد. بر روی close کلیک کنید.

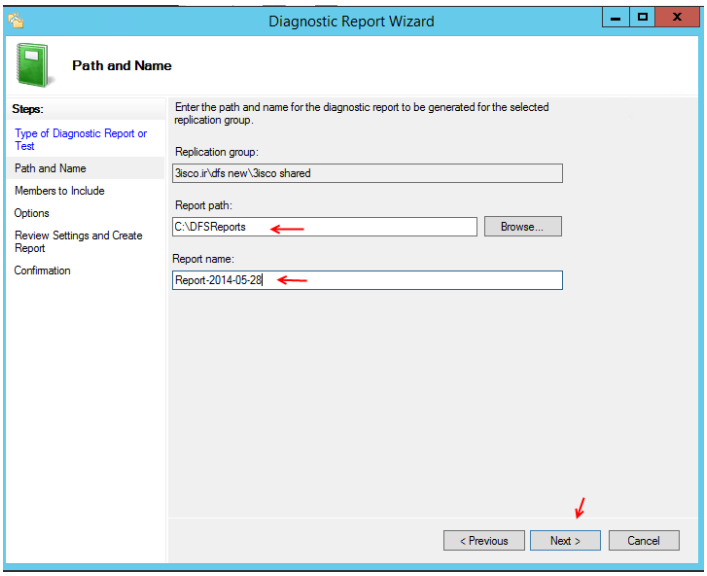
بعد ار ایجاد Replicate موردنظر از این پس در هر یک از سرورها فایلی در پوشه موردنظر قرار داده شود، این اطلاعات فقط در یک پوشه و توسط همه افراد داخل شبکه در دسترس است.



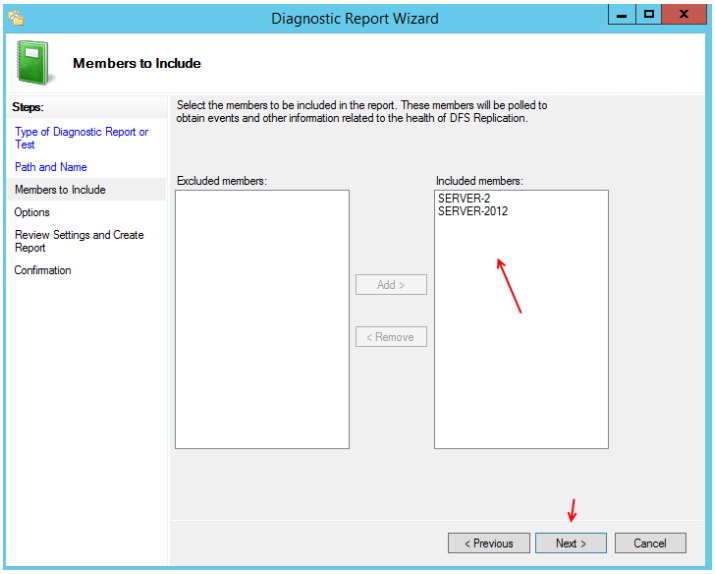
برای گزارش گیری از وضعیت Replication موجود از سمت چپ بر روی آن کلیک کنید و از سمت راست بر روی Creat Diagnostic Report کلیک کنید.



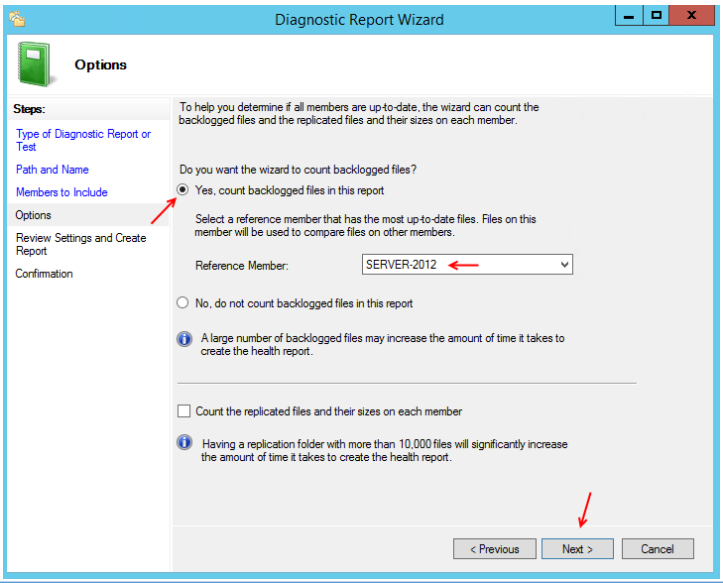
در این صفحه گزینه اول را انتخاب و بر روی Next کلیک کنید.



در این صفحه در قسمت Report Path مسیر ذخیره سازی گزارشات را می‌توانید مشخص کنید و در قسمت Report Name هم نام گزارش خود را وارد کنید.

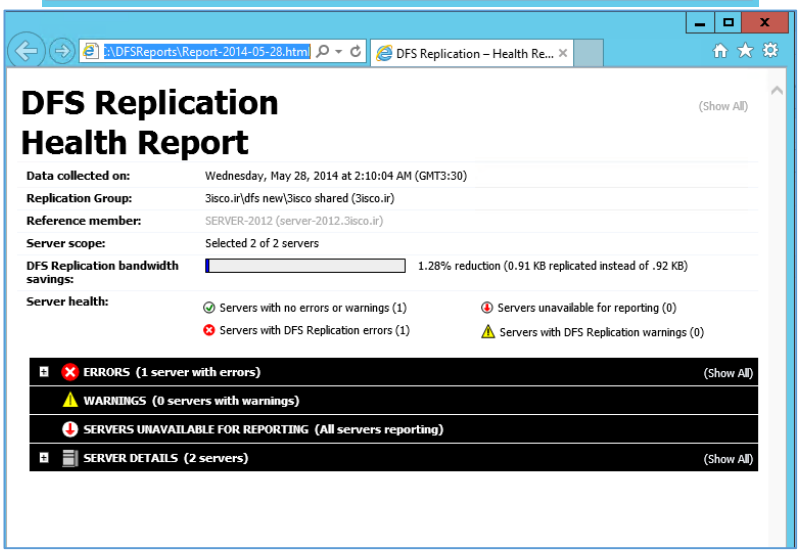


در این صفحه هر دو سرور باید در قسمت Included members قرار داشته باشند، بر روی Next کلیک کنید.



در این قسمت گزینه اول را انتخاب و از لیست کشویی سرور اصلی را انتخاب و بر روی Next کلیک کنید.

در صفحه آخر هم بر روی Create کلیک کنید تا یک فایل با پسوند HTML ایجاد شود.

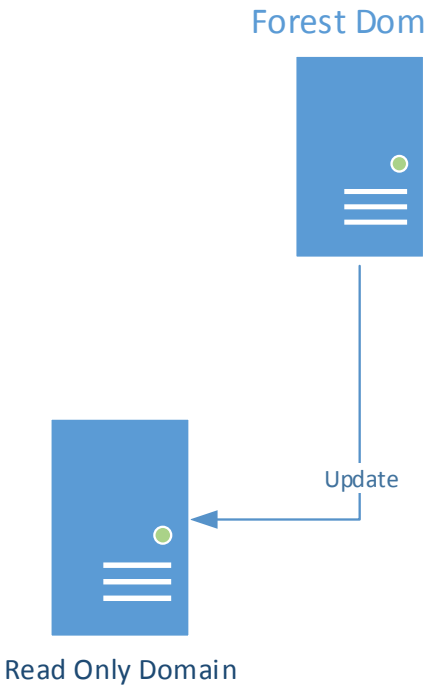


وارد آدرس C:\DFSReport می‌شویم و گزارش موردنظر را که با نام Report-2014-05-28 بود را روی Internet Explorer اجرا می‌کنیم. همانطور که در شکل روبرو مشاهده می‌کنید گزارش موردنظر اجرا شده است و می‌توانید اطلاعات را بررسی کنید.

کار با Read Only Domain Controller:

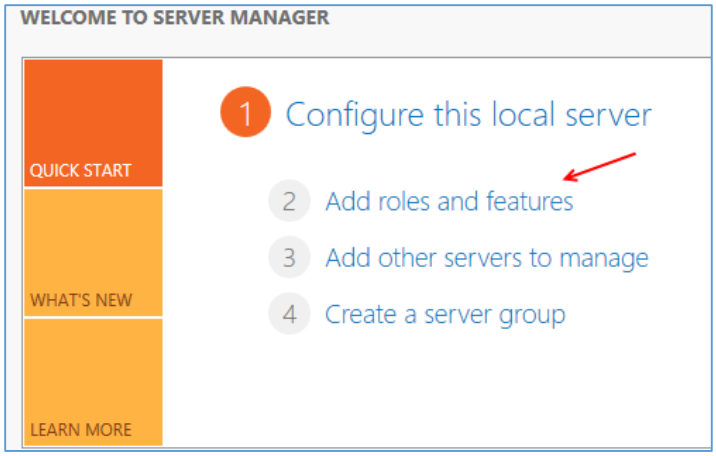
کار با سرویس Active Directory یکی از مهمترین بخش‌ها می‌باشد که امنیت آن برای یک شرکت یا سازمان بسیار اهمیت دارد، شما باید به عنوان مدیر شبکه کارهای امنیتی لازم را برای جلوگیری از دسترسی نامعتبر انجام دهید، یکی از راه‌های ایجاد امنیت استفاده از Read Only Domain Controller یا RODC است این یعنی یک دومین کنترلر فقط خواندنی و ایجاد تغییر در آن غیر ممکن است.

دلیل آن این است که این دومین کنترلر زیر مجموعه دومین کنترلر دیگر است و فقط یک کپی از اطلاعات دومین کنترلر اصلی را در خود نگه می‌دارد و هیچ تغییر را نمی‌تواند به صورت مستقیم در دومین کنترلر اصلی انجام دهد. در کل تغییرات توسط دومین کنترلر اصلی اعمال یا Replicate می‌شود.



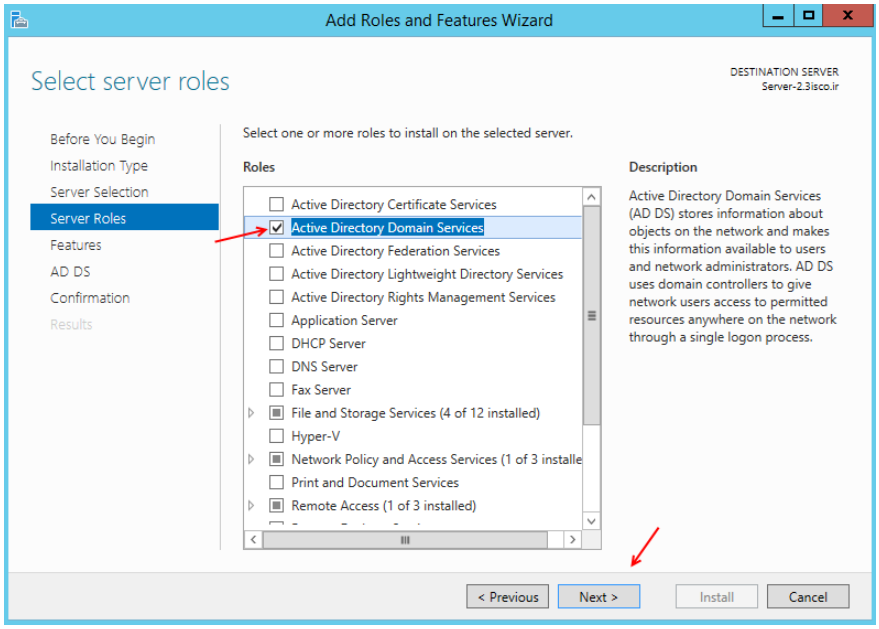
در این شکل هم سرور Forest سرور اصلی می‌باشد و آپدیت‌ها به صورت یک طرفه به سرور Read Only فرستاده می‌شود.

برای شروع کار ما نیاز به یک Domain Controller اصلی داریم که این دومین کنترلر از قبل نصب شده است، بعد از آن یک سرور جدید را در کنار سرور اصلی قرار می‌دهیم و روی آن ویندوز سرور 2012 نصب می‌کنیم و بعد از آن شروع به راه اندازی سرویس Read Only Domain Controller می‌کنیم.

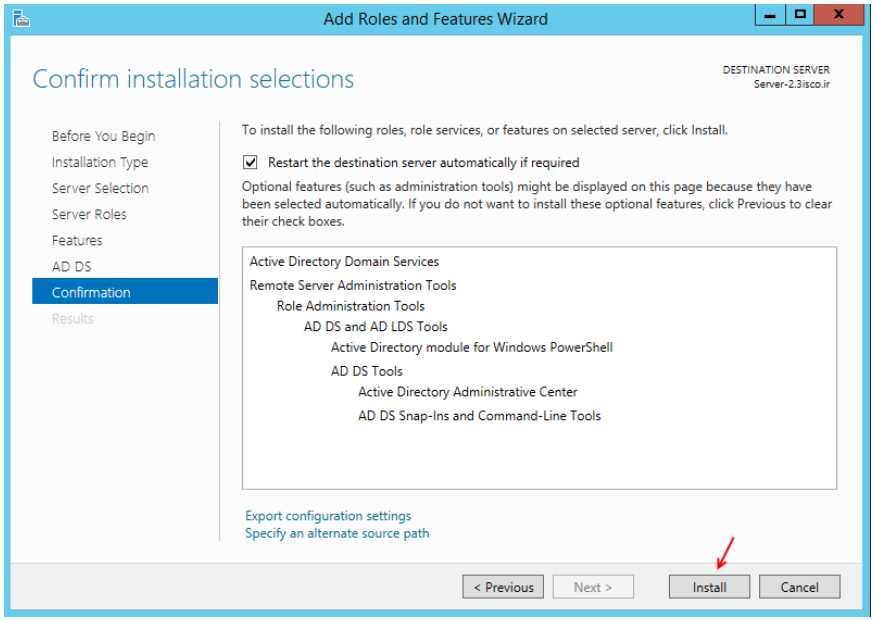


وارد سرور دوم شوید و Server Manager را اجرا کنیدو به مانند شکل روبرو بر روی Add roles and features کلیک کنید.

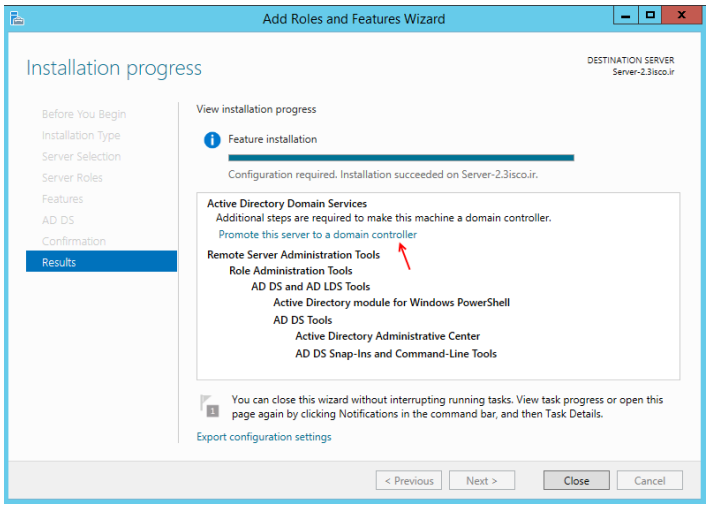
نکته: این سرور زیرمجموعه دومین سرور اصلی می-باشد.



در صفحه Server Roles گزینه Active Directory Domain Services را انتخاب کنید و در شکل باز شده بر روی Add Feature کلیک کنید و بعد بر روی Next کلیک کنید تا به صفحه Confirmation برسیم.

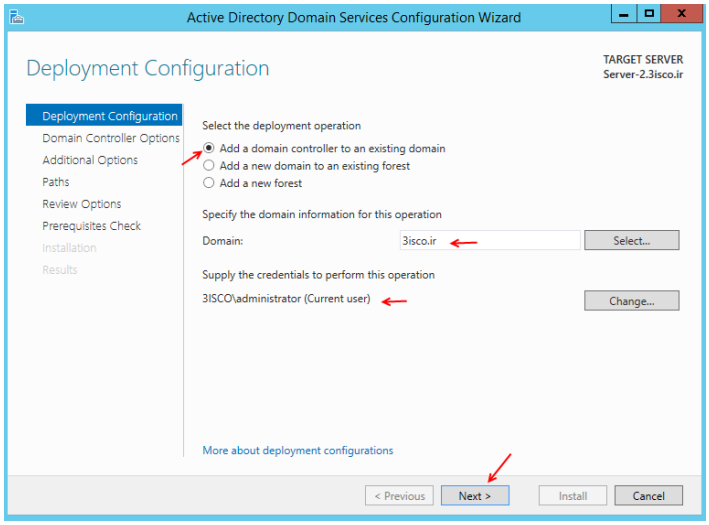


در این صفحه برای نصب سرویس بر روی Install کلیک کنید.

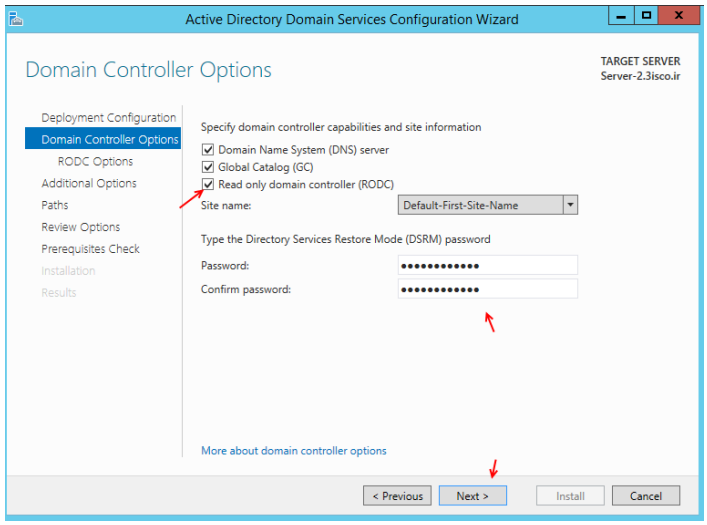


بعد از نصب سرویس، در همان صفحه بر روی Promote this server to a domain controller کلیک کنید تا تنظیمات RODC را انجام دهیم.

(RODC همان Read Only Domain Controller است)

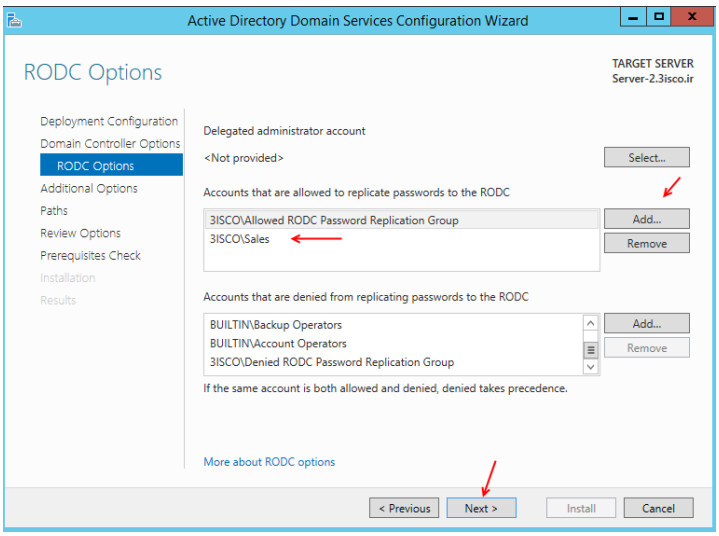


در این صفحه گزینه Add a domain controller to an existing domain را انتخاب کنید، همانطور که مشاهده می‌کنید دومین 3isco.ir شناسایی شده است، برای ادامه کار بر روی Next کلیک کنید.



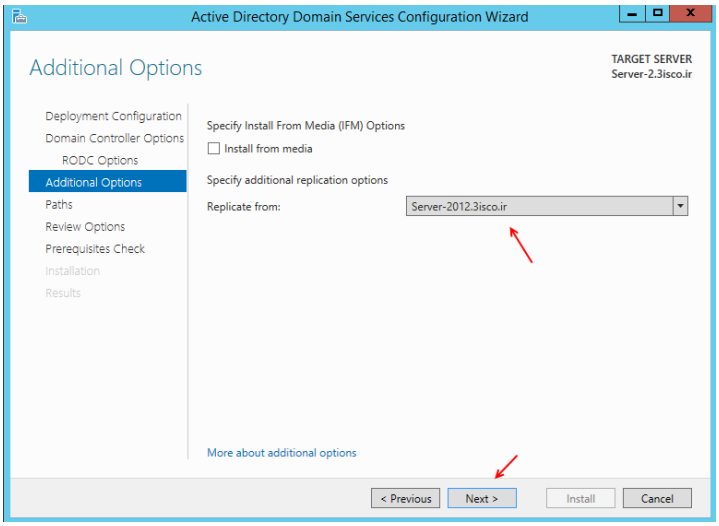
در این قسمت، مهمترین کار انتخاب گزینه Read Only domain Controller است و بعد یک رمز برای Restore Mode می‌باشد.

بر روی Next کلیک کنید.

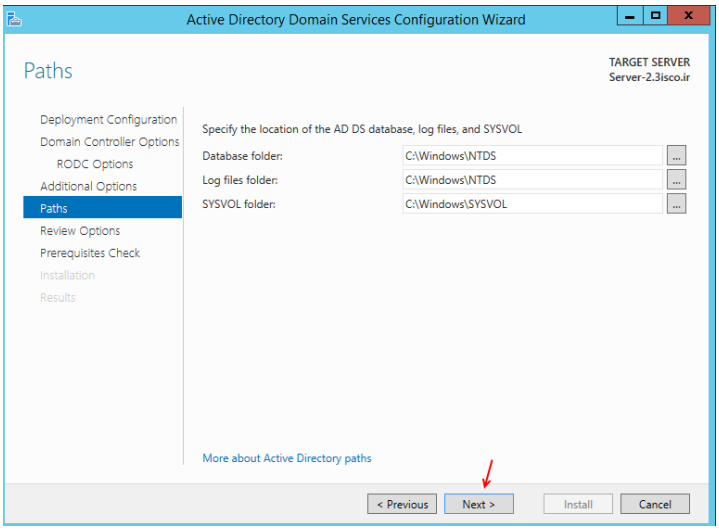


در این قسمت می‌توانید با کلیک بر روی Add گروه یا کاربرموردنظر خود را به لیست اضافه کنید.

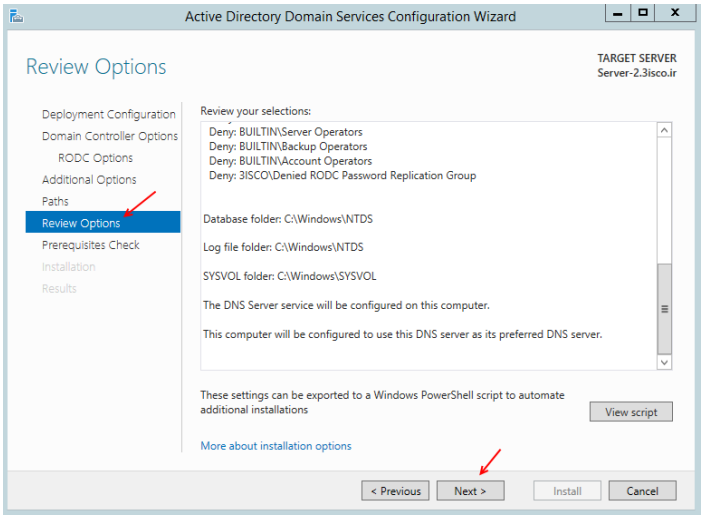
بر روی Next کلیک کنید.



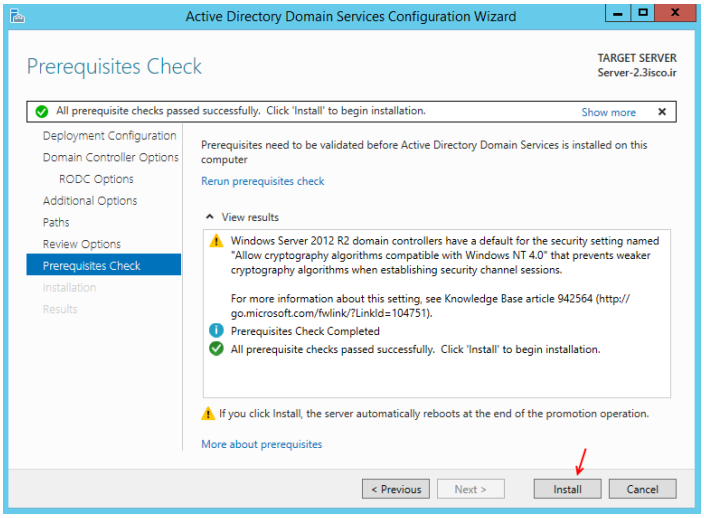
در این قسمت از لیست کشویی سرور اصلی خود را که دومین کنترلر اصلی روی آن نصب است را انتخاب و بر روی Next کلیک کنید.



در این قسمت، بر روی Next کلیک کنید.

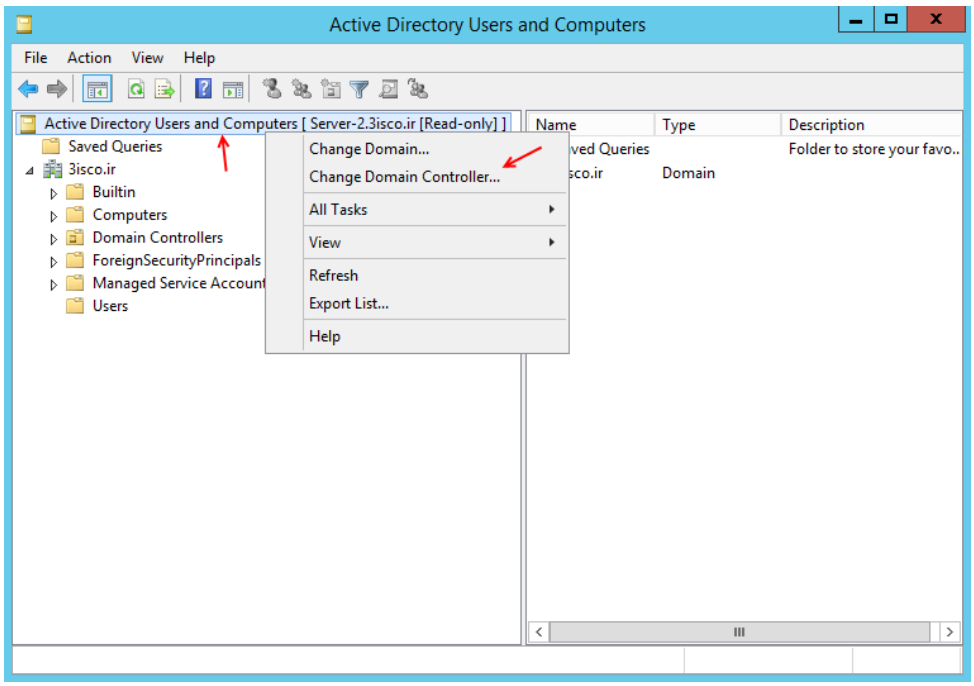


در این صفحه که مربوط به اطلاعات کاملی از نصب دومین می‌باشد که آن را بررسی و بر روی Next کلیک کنید



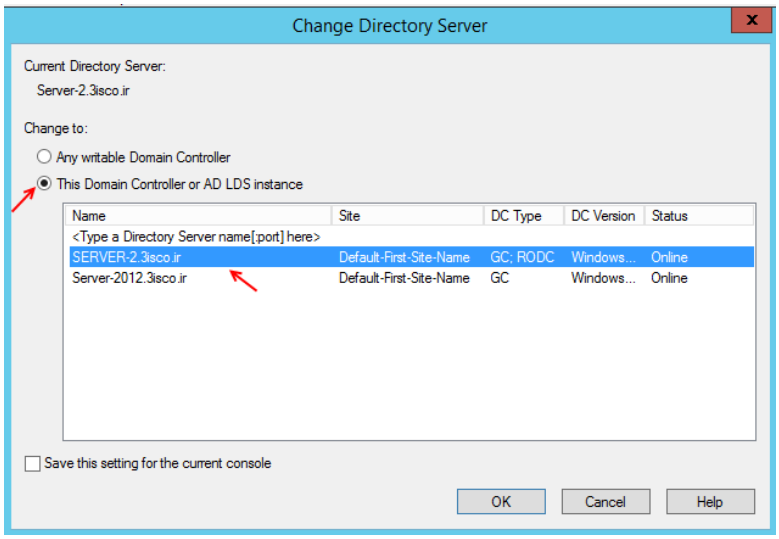
در این صفحه برای نصب سرویس بر روی install کلیک کنید.

بعد از چند دقیقه سرویس موردنظر نصب و سیستم Restart می‌شود، البته زمانی Restart می‌شود که تیک گزینه Restart را موقع نصب انتخاب کرده باشید.

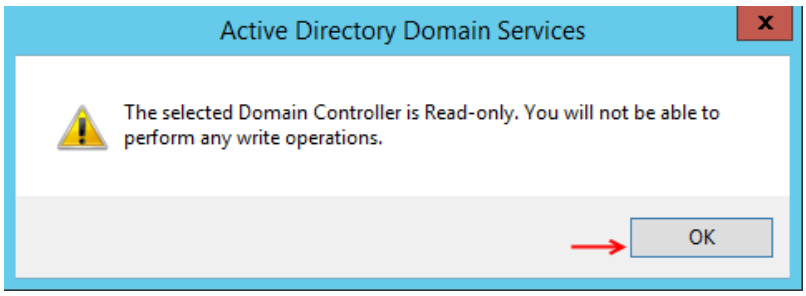


بعد از نصب سرویس سرویس Active Directory users and computers را روی سرور دوم اجرا کنید، نکته ای که در اینجا مشاهده می‌شود این است که در حال حاضر سیستم دومین بر روی RODC قرار ندارد، برای تنظیم آن بر روی نام

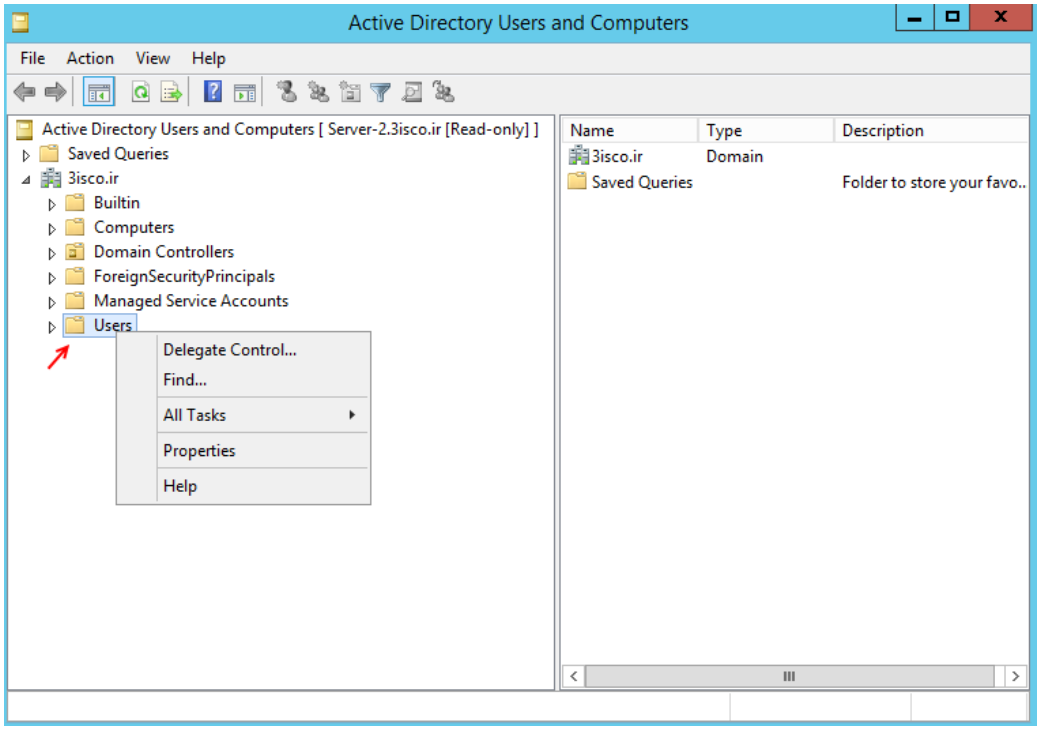
سرور به مانند شکل کلیک راست کنید و گزینه Change Domain controller را انتخاب کنید.



در این قسمت گزینه The Domain Controller or AD LDS instance را انتخاب کنید و بین گزینه های موجود نام سروری را انتخاب کنبد که به عنوان دومین فقط خواندنی معرفی کردیم که در اینجا سرور Server-2 به عنوان RODC انتخاب شده است، بعد از انتخاب بر روی Ok کلیک کنید.



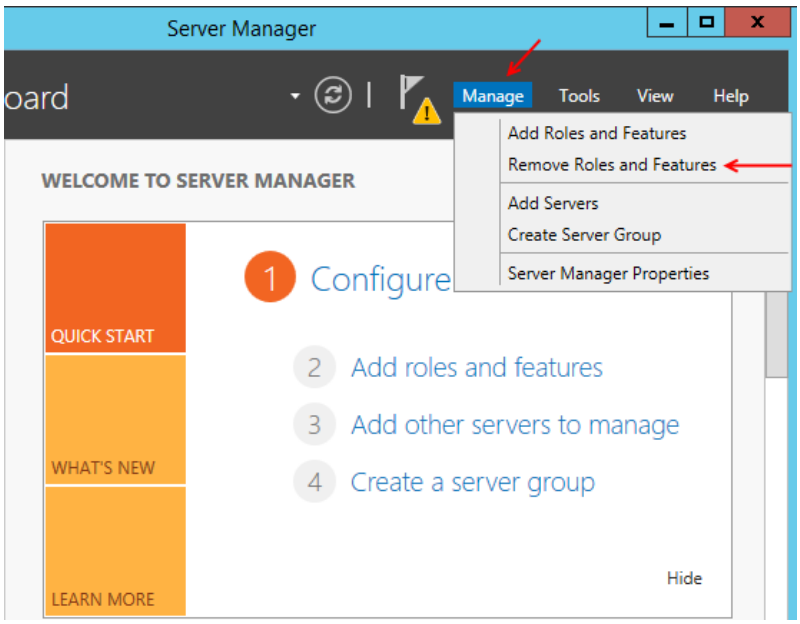
بعد از کلیک بر روی ok شکل روبرو ظاهر می‌شود و به شما این اخطار را می‌دهد که این دومین کنترلر به فقط خواندنی تبدیل می‌شود و دیگر نمی‌توانید روی آن بنویسید.Ok کنید.



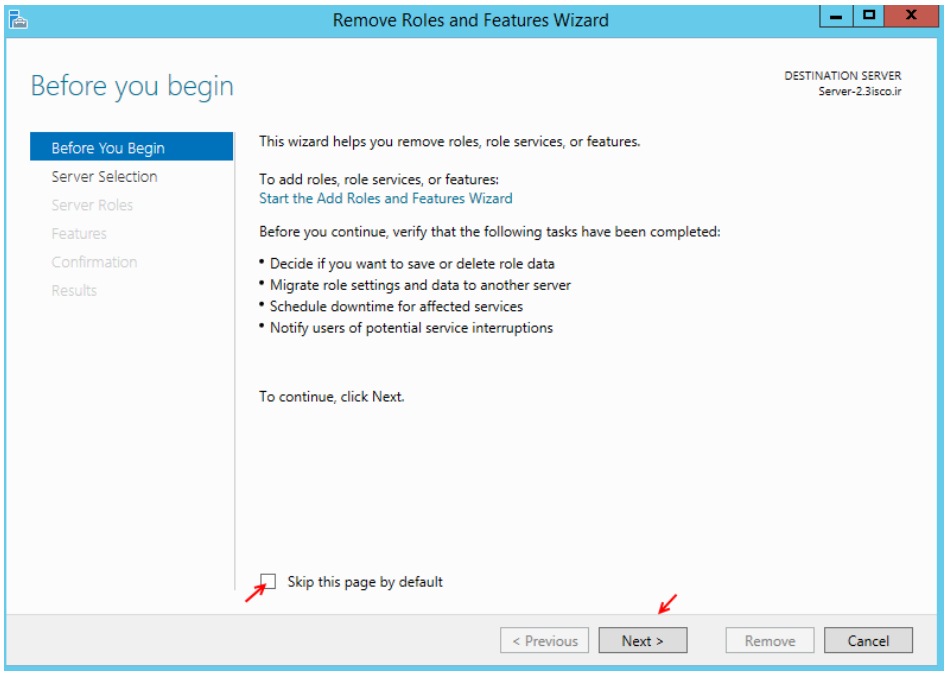
خوب اگر روی قسمت User کلیک راست کنید متوجه خواهید شد که نمی‌توانیم یک شی جدید مانند گروه یا کاربر ایجاد کنیم، به خاطر اینکه دومین کنترلر در حالت Read Only قرار دارد.

حذف و خداحافظی با Active Directory:

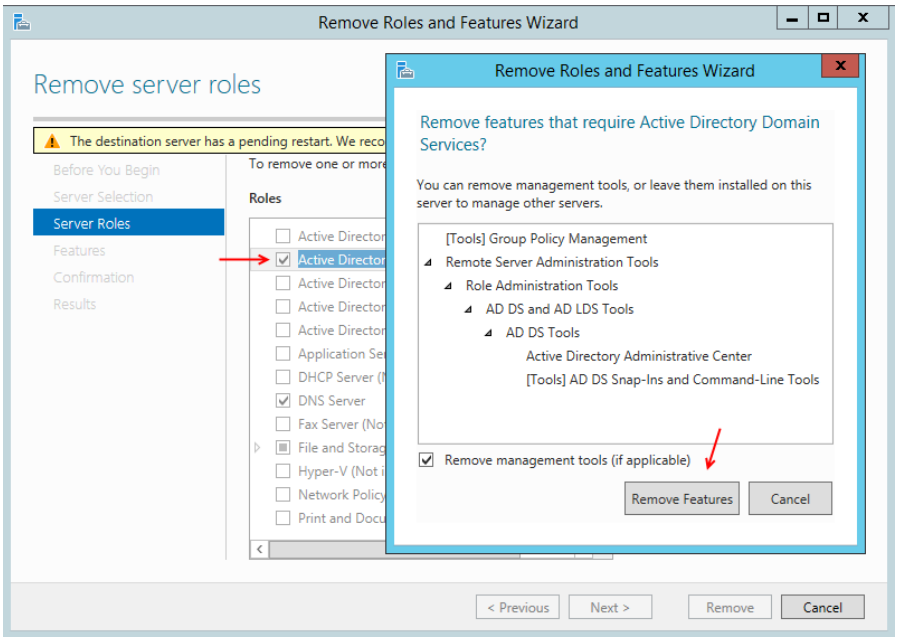
هر چیزی که در هر جایی نصب می‌شود، زمانی می‌آید که باید از آن قسمت حذف شود که Active Directory هم به همین صورت است، در قسمت های قبلی کتاب، سرویس Active Directory به همراه دومین نصب و راه اندازی شد، حالا می‌خواهیم این سرویس را حذف کنیم.



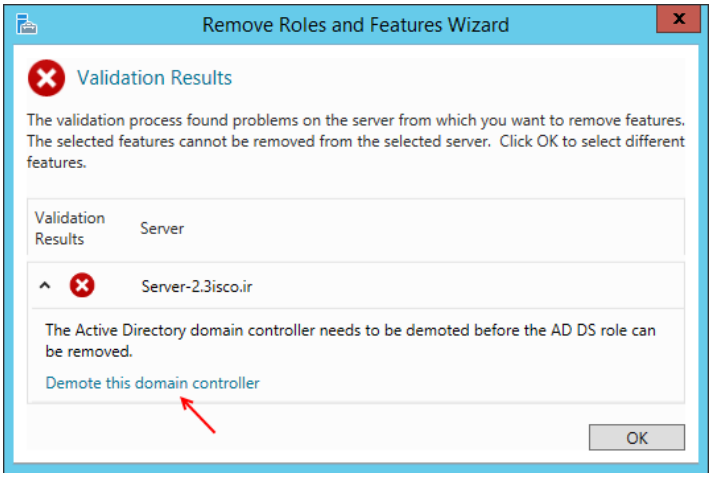
برای شروع وارد Server Manager شوید و به مانند شکل روبرو از منوی Manage گزینه Remove Roles and Features را انتخاب کنید.



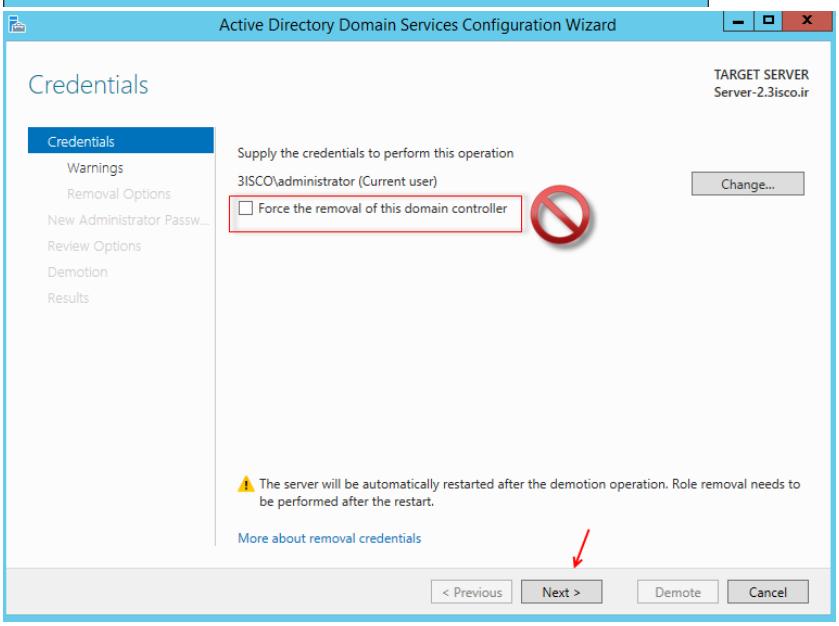
در این صفحه بر روی Next کلیک کنید، در صفحه Server Selection هم بر روی Next کلیک کنید.



در این قسمت اول باید بین Role های موردنظر گزینه Active Directory Domain Services را انتخاب کنید تا شکل موردنظر ظاهر شود در این شکل برروی Remove Features کلیک کنید.

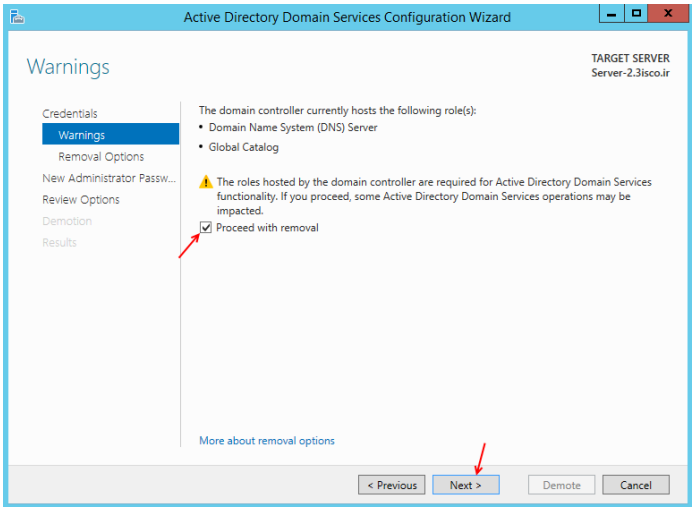


این شکل ظاهر می‌شود که به اعلام می‌کند که قبل از حذف Active Directory باید Domain را حذف کرد. برای این کاربر روی Demote this domain Controller کلیک کنید.

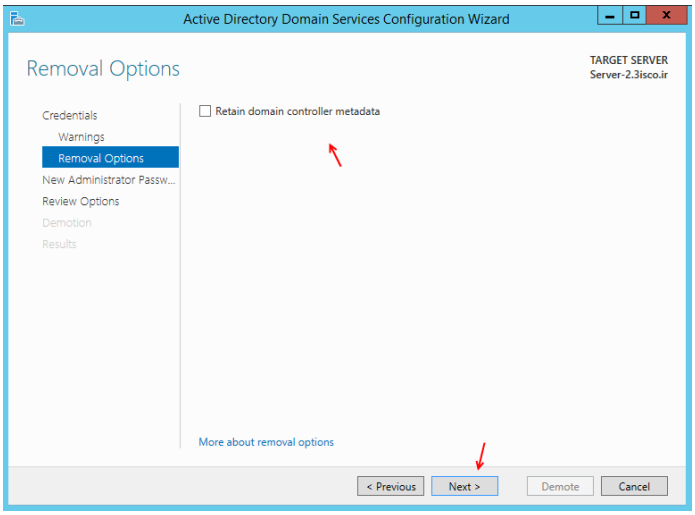


در این قسمت، گزینه‌ای وجود دار با نام Force the removal... که این گزینه زمانی به کار ما می‌آید که به صورت معمول نتوانید دومین را حذف کنیم، در صورت انتخاب این گزینه و حذف دومین باید بعد از آن به صورت دستی باید

Metadata آن را هم حذف کنید که کار دردسر سازی خواهد بود، پس در این قسمت به این گزینه دست نزنید و بر روی Next کلیک کنید.

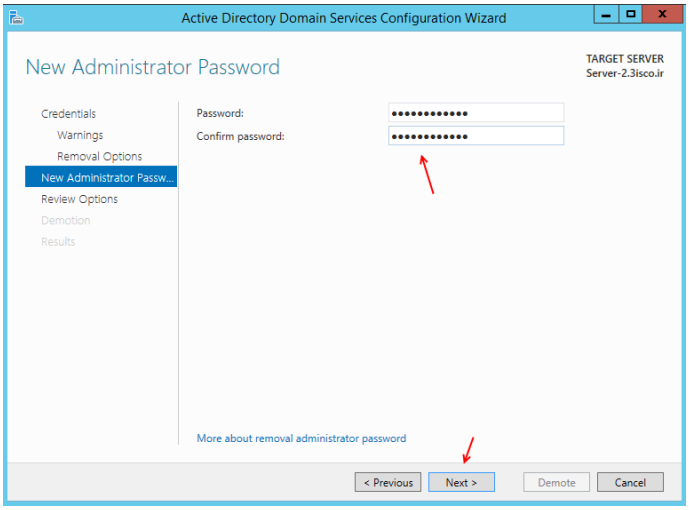


در این قسمت، گزینه proceed with removal را انتخاب کنید تا سرویس‌های فعال هم غیر فعال شوند، برای ادامه کار بر روی Next کلیک کنید.



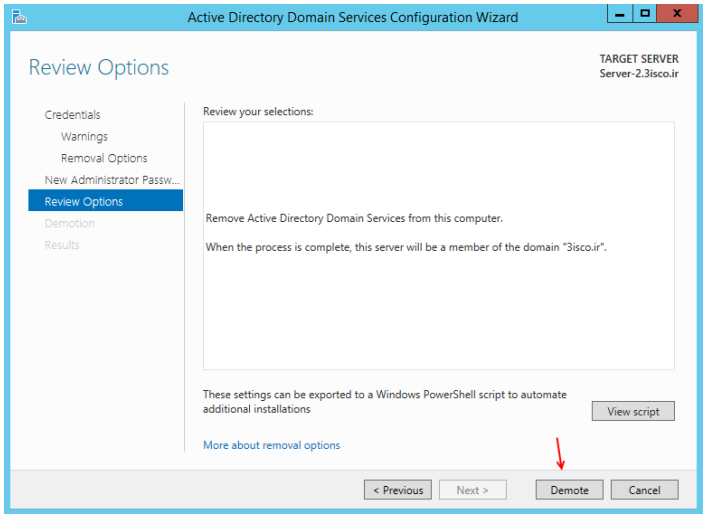
در این قسمت اگر گزینه Retain domain controller Metadata را انتخاب کنید، MetaData حفظ خواهد شد که در این قسمت این گزینه را انتخاب نکنید.

بر روی Next کلیک کنید.

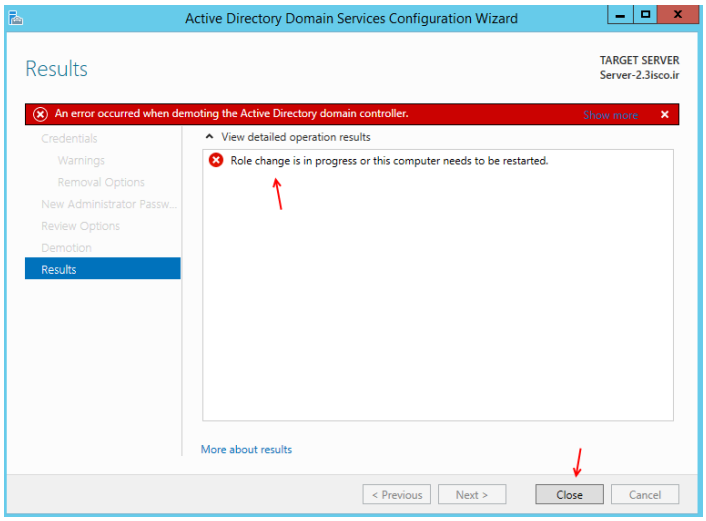


در این قسمت، باید یک رمز عبور جدید برای کاربر administrator خود وارد کنید، البته می‌توانید از همان رمز قدیمی دوباره استفاده کنید.

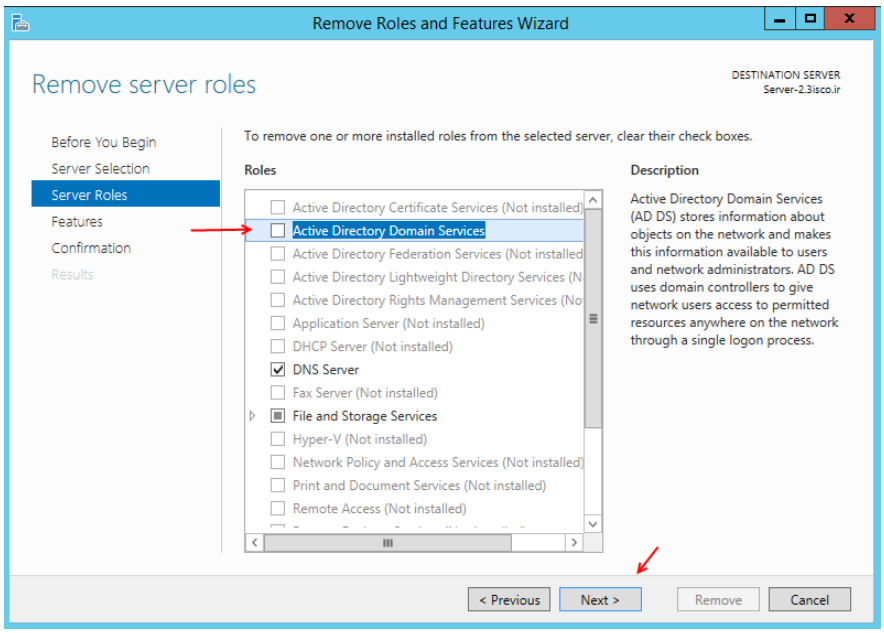
بعد از وارد کردن اطلاعات بر روی Next کلیک کنید.



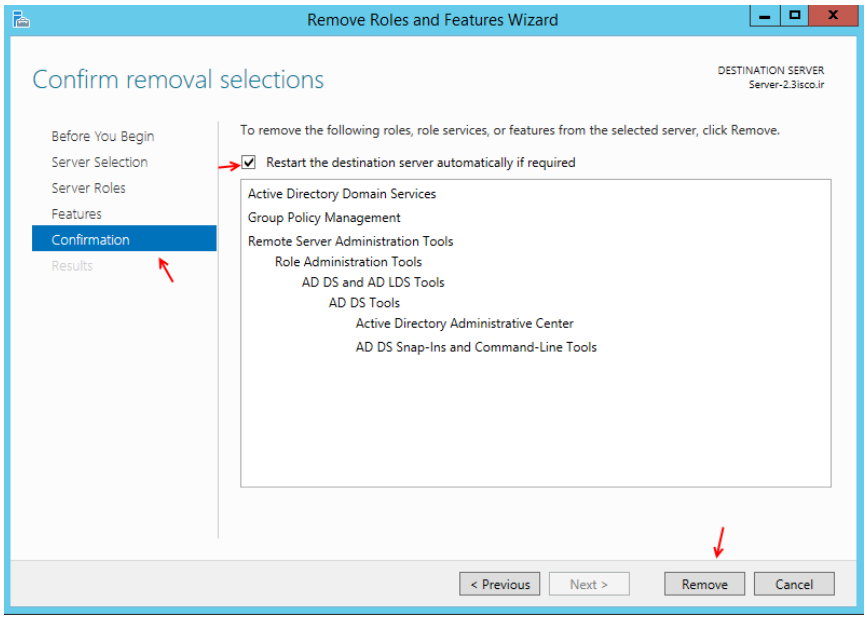
در این قسمت بر روی Demote کلیک کنید تا کار حذف Domain Controller آغاز شود.



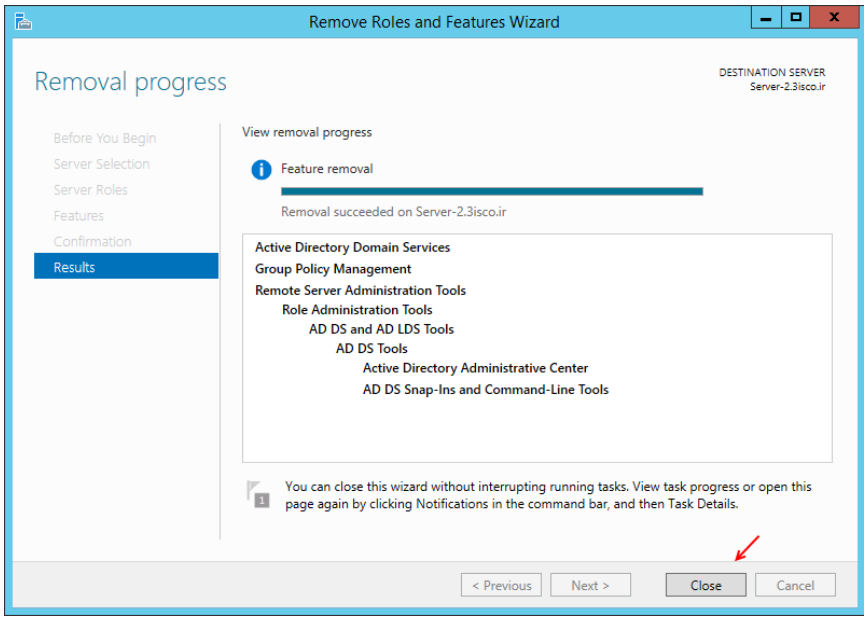
اگر بعد از اینکه بر روی Domote کلیک کردید و شکل روبرو ظاهر شد بر روی Close کلیک کنید و یک بار سرور را Restart کنید و دوباره مراحل نصب را به ترتیب انجام دهید تا دومین کنترلر به صورت کامل حذف شود.



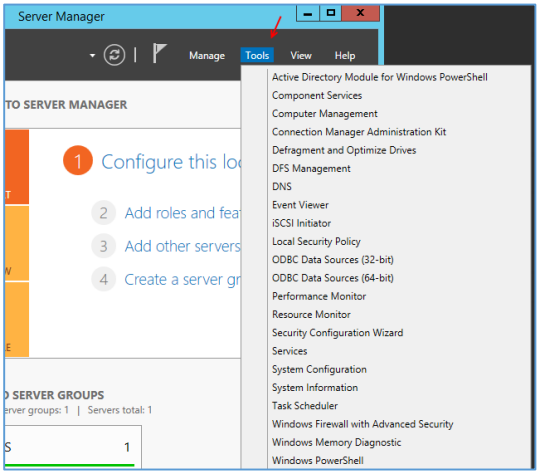
بعد از حذف دومین کنترلر دوباره وارد Server Manager شوید و از منوی Manage گزینه Remove Roles and Features را انتخاب کنید. بعد در شکل باز شده وارد قسمت Server Roles شوید و تیک کنار گزینه Active Directory Service را بردارید. در ادامه بر روی Next کلیک کنید.



بر روی Next کلیک کنید تا مانند شکل روبرو وارد قسمت Confirmation شوید، در این قسمت تیک گزینه Restart... را انتخاب و بر روی Remove کلیک کنید.



در این قسمت هم سرویس موردنظر حذف شده است، در ادامه کار بر روی Close کلیک کنید و سیستم را Restart کنید.

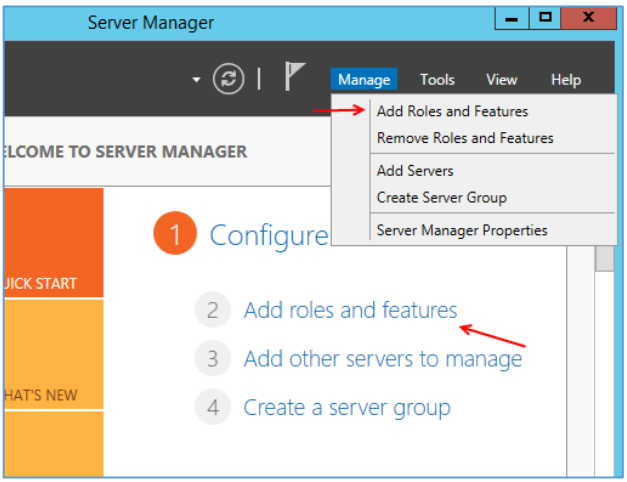


همانطور که در شکل روبرو مشاهده می‌کنید، سرویس موردنظر در منوی Tools قرار ندارد و حذف شده است.

ایجاد Domain Tree:

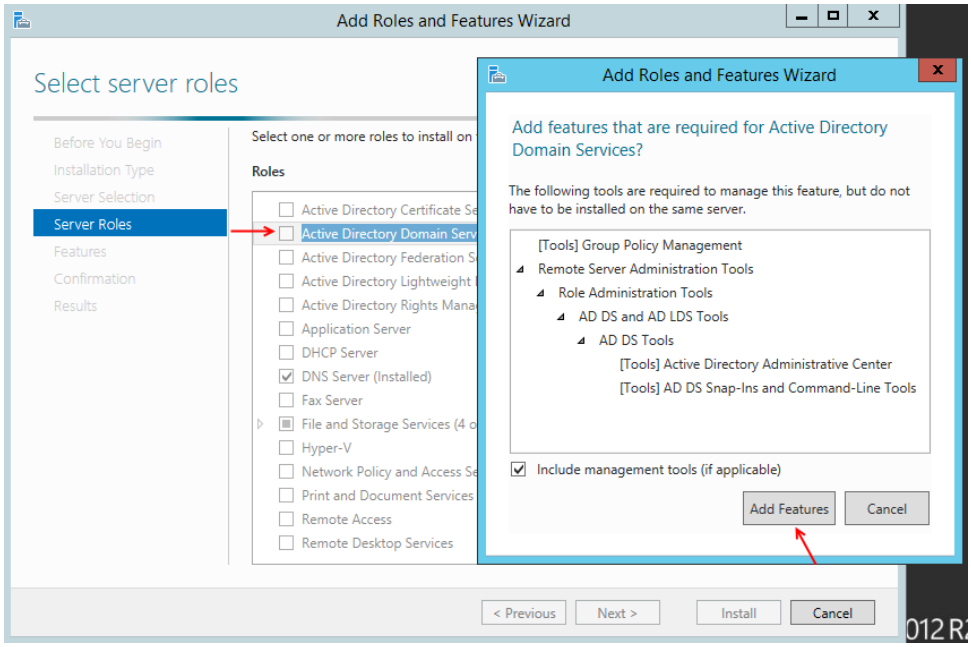
در این قسمت می‌خواهیم یک Domain Tree ایجاد کنیم، این نوع دومین‌ها توانایی ارتباط مستقیم با دومین اصلی را دارند یعنی اینکه Trust و یا همان اعتماد بین دو دومین برقرار است.

برای ایجاد Domain Tree باید از قبل یک دومین فعال (Root) داشته باشیم، توجه داشته باشید که سروری که روی آن Domain Tree فعال می‌شود به سرور اصلی شبکه شده است.

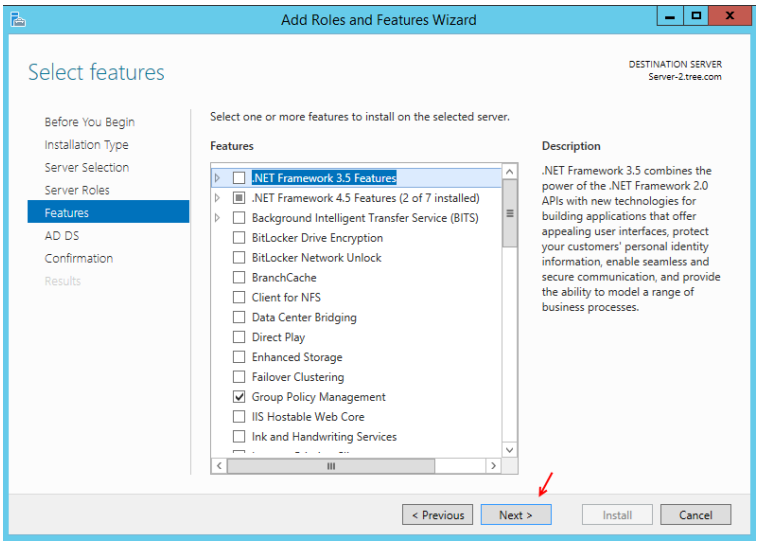


برای شروع وارد سرور دوم شوید و Server Manager را اجرا کنید.

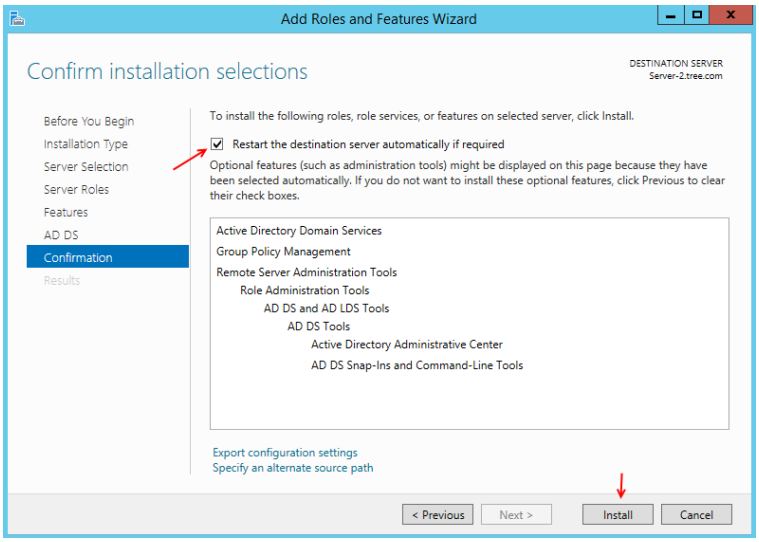
با مانند شکل به دو روش مختلف می‌توانید بر روی Add roles and features کلیک کنید.



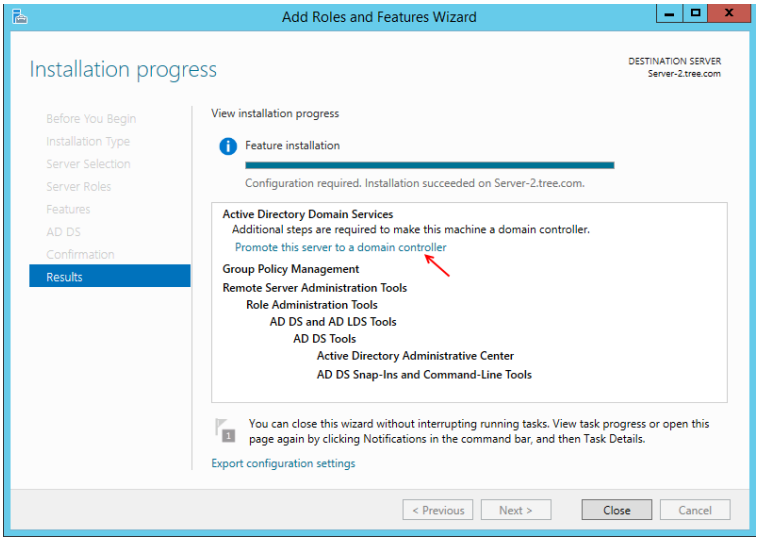
در این شکل از سمت چپ بر روی Server Roles کلیک کنید و از لیست Roles گزینه Active Directory Domain Service را انتخاب کنید و در شکل باز شده بر روی Add Features کلیک کنید و بر روی Next کلیک کنید.



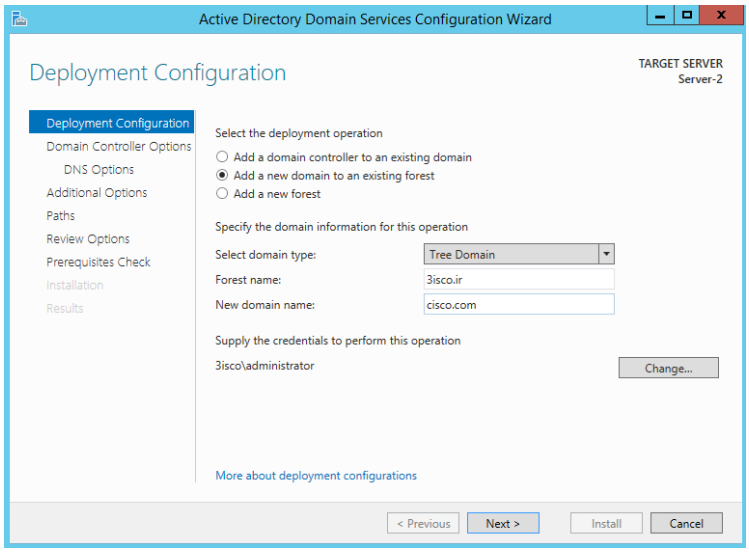
در این قسمت بدون انتخاب گزینه‌ای بر روی Next کلیک کنید.



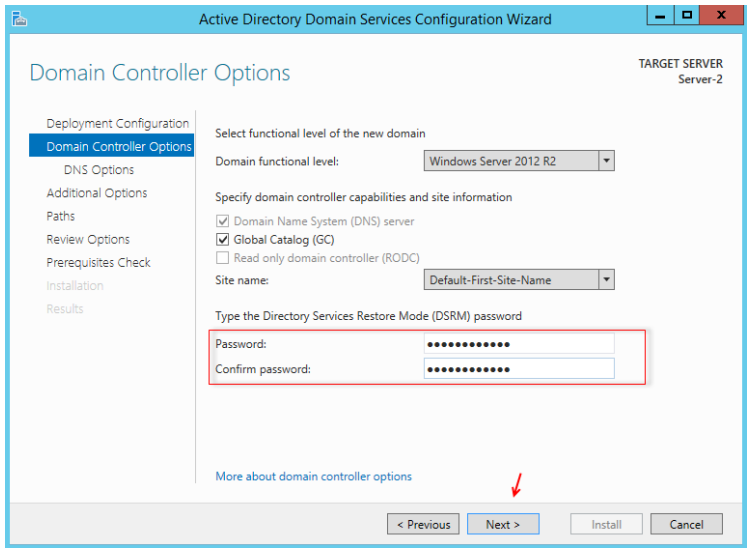
در این قسمت گزینه Restart the destination را انتخاب و بر روی install کلیک کنید تا Active Directory نصب شود.



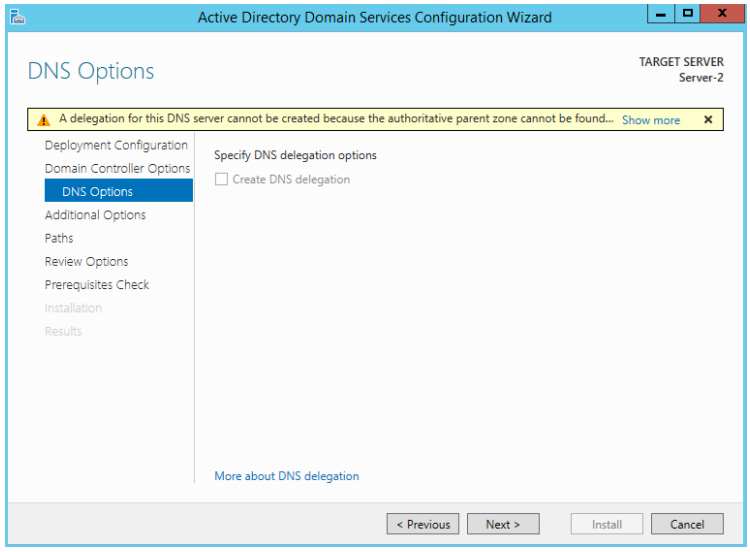
در این قسمت، بر روی Promote this server to a domain controller کلیک کنید.



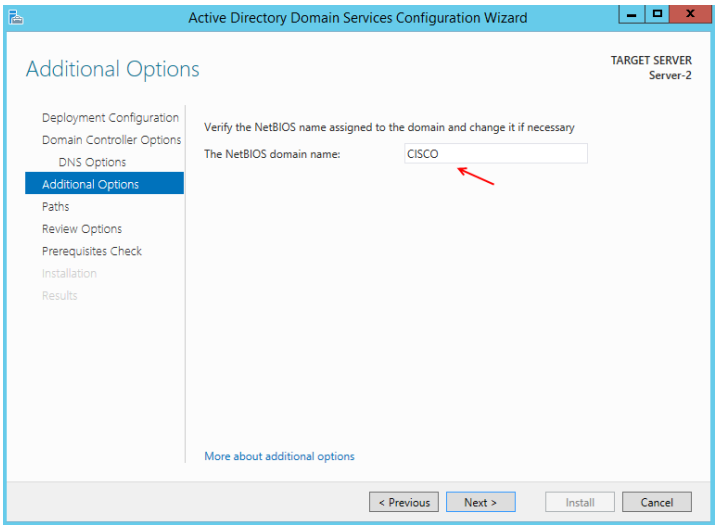
در این قسمت، اول گزینه Add a new domain to an existing forest را انتخاب کنید، در قسمت Select domain type گزینه Tree Domain را انتخاب کنید و در قسمت Forest name نام دومین Root خود را وارد کنید و در قسمت New Domain name نام دومین جدید خود را وارد کنید، توجه داشته باشید با کلیک بر روی Change نام کاربری را وارد کنید که در دومین اصلی (Forest) که در اینجا 3isco.ir می‌باشد اعتبار داشته باشد، برای ادامه کار بر روی Next کلیک کنید.



در این قسمت رمز مربوط به Restore Mode را که قبلاً توضیح دادم به دلخواه خود وارد کنید و بر روی Next کلیک کنید.

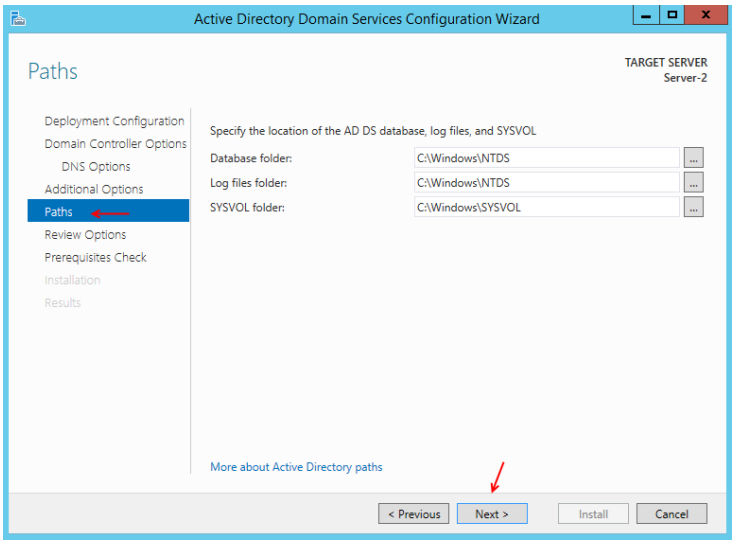


در این قسمت بر روی Next کلیک کنید.



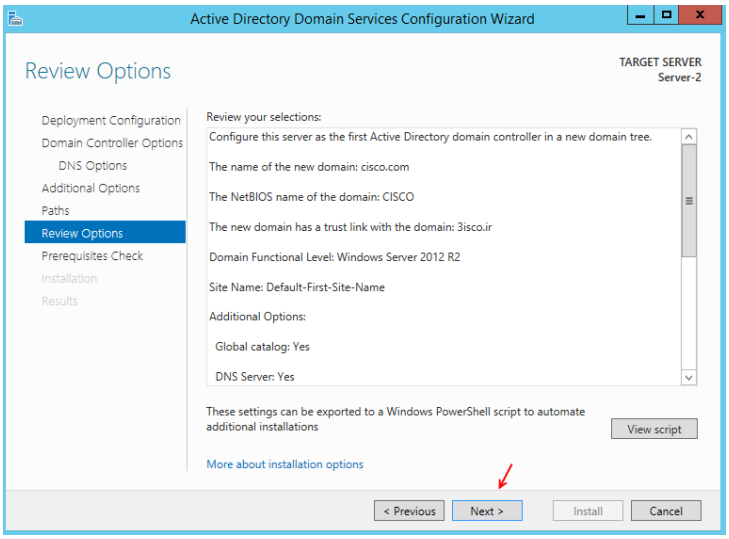
در این صفحه اگر نام دومین شما از قبل وجود نداشته باشد به مانند شکل روبرو تایید می‌شود، توجه داشته باشید اگر به اینترنت متصل باشید و این نام در اینترنت وجود داشته باشد، به هیچ عنوان تایید نخواهد شد.

بر روی Next کلیک کنید.

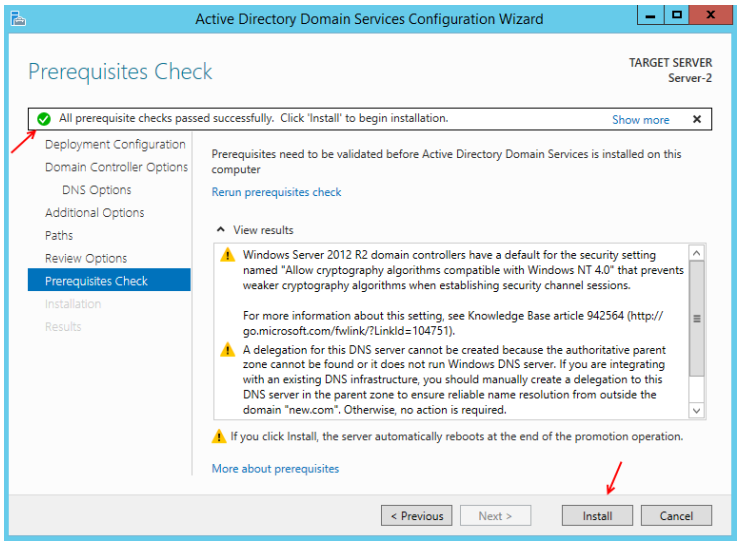


در این قسمت مسیر مربوط به فولدرهای Database, Log File, SYSVOL را می‌توانید مشخص کنید که پیشنهاد می‌شود بر روی پیش فرض قرار داشته باشد.

بر روی Next کلیک کنید.

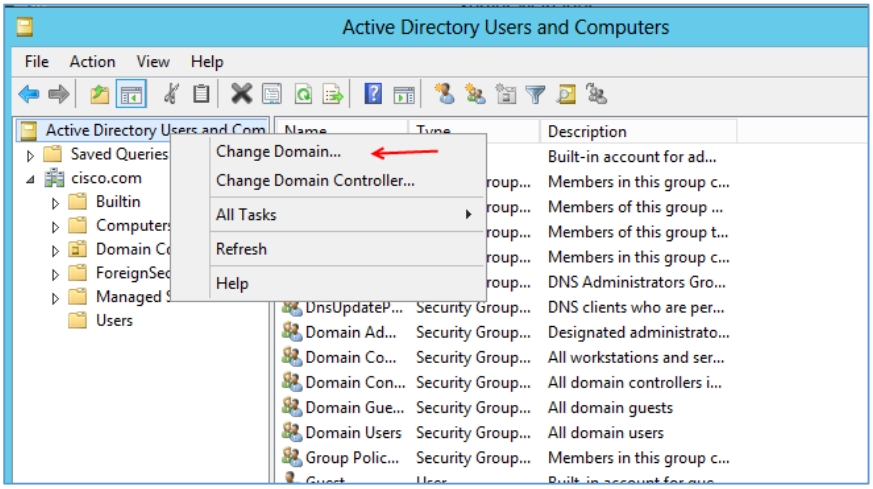


در این قسمت اطلاعات کلی از اطلاعات وارد شده را مشاهده می‌کنید اگر مورد تایید است بر روی Next کلیک کنید.



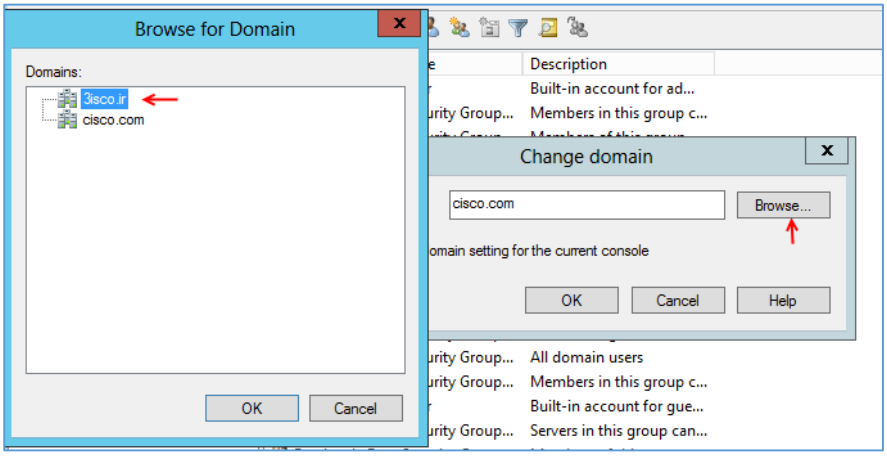
در این صفحه بعد از بررسی سیستم به شما مجوز نصب داده می‌شود، برای نصب سرویس بر روی install کلیک کنید.

توجه داشته باشید بیشترین مشکلی که در این قسمت شاید به وجود بیاید تنظیم نکردن IP به صورت Static می‌باشد.



بعد از نصب، سرویس Active Directory Users and Computers را اجرا کنید.

به مانند کل روبرو برروی عنوان موردنظر کلیک راست کنید و گزینه Change Domain را انتخاب کنید.

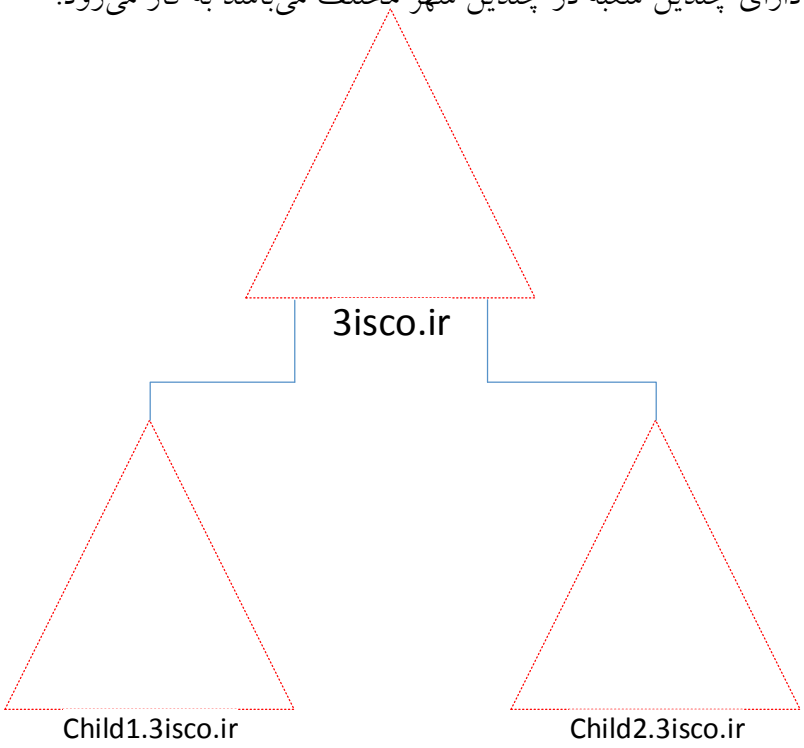


در این قسمت بر روی Browse کلیک کنیدو همانطور که در شکل روبرو هم مشاهده می‌کنید هر دو دومین در دسترس است که در این قسمت دومین 3isco.ir را انتخاب و بر روی ok کلیک می‌کنیم.

با این کار می‌توانید از طریق سرور دوم دومین اصلی را به راحتی مدیریت کنید، چگونگی ایجاد شدن این ارتباط از طریق سرویس Active Directory Domain and Trust انجام می‌شود که در ادامه به صورت کامل نحوه کار با این سرویس را برای ارتباط دو دومین کنترلر جدا از هم را می‌آموزیم.

نحوه ایجاد Child Domain:

این نوع دومین، زیر مجموعه دومین اصلی شما خواهد شد، یعنی اینکه اگر شما یک دومین با نام 3isco.ir داشته باشید، دومین Child به صورت مثلاً Child.3ico.ir ایجاد می‌شود. بیشترین کاربرد این نوع دومین ها در شرکت‌های بزرگ که دارای چندین شعبه در چندین شهر مختلف می‌باشد به کار می‌رود.

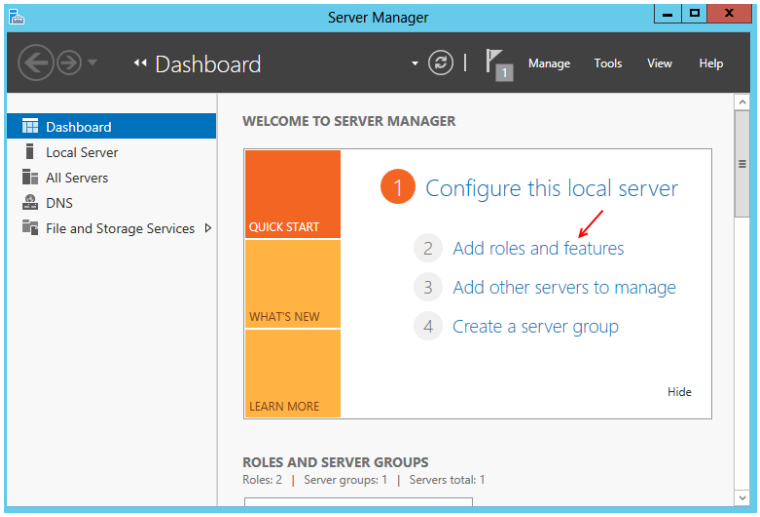


برای ایجاد Child Domain نیاز به یک دومین اصلی که در اینجا 3isco.ir می‌باشد و یک دومین دیگر که کار Child را انجام دهد، به فرض مثال دومین 3isco.ir از قبل نصب و راه اندازی شده است و روی سرور دوم هم ویندوز سرور 2012 نصب شده است و آدرس IP در رنج سرور اصلی تنظیم شده است.

توجه داشته باشید که این دو سرور باید با هم شبکه شوند.

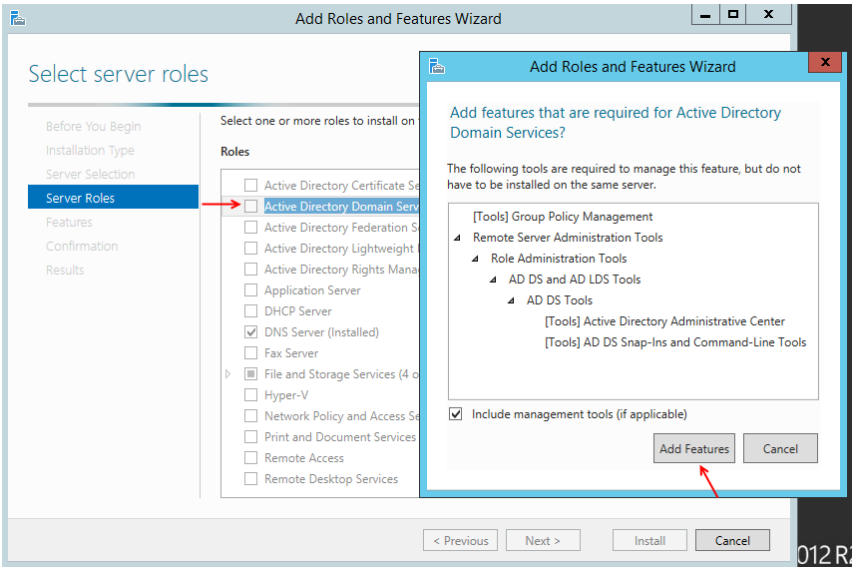
Root
Domain: 3isco.ir
IP Address: 192.168.1.102
DG:255.255.255.0
DNS: 192.168.1.102
Windows Server 2012

Child Domain
Domain: Child.3isco.ir
IP Address: 192.168.1.103
DG:255.255.255.0
DNS: 192.168.1.102
Windows Server 2012

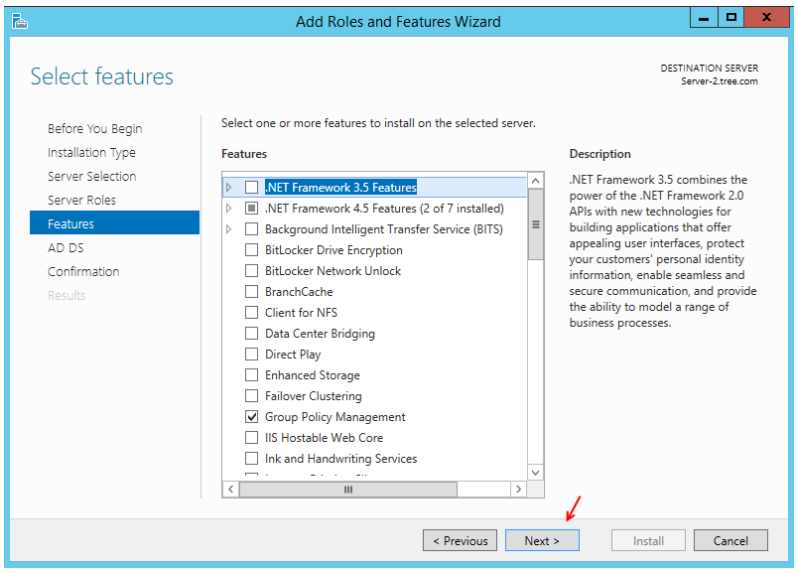


برای شروع وارد سرور دوم شوید و Server Manager را اجرا کنید.

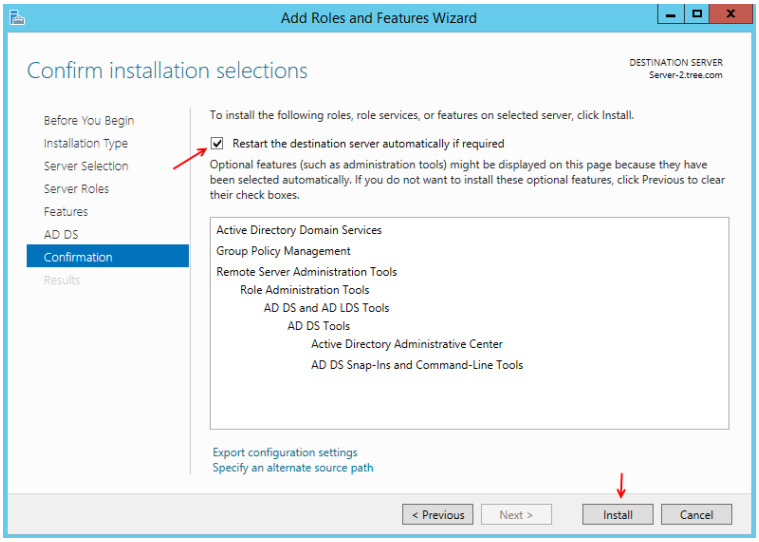
بر روی Add roles and features کلیک کنید.



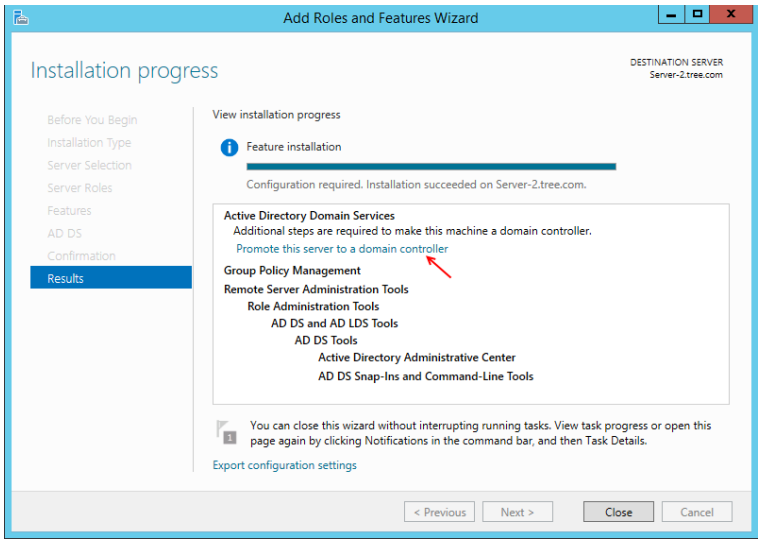
در این شکل از سمت چپ بر روی Server Roles کلیک کنید و از لیست Roles گزینه Active Directory Domain Service را انتخاب کنید و در شکل باز شده بر روی Add Features کلیک کنید و بر روی Next کلیک کنید.



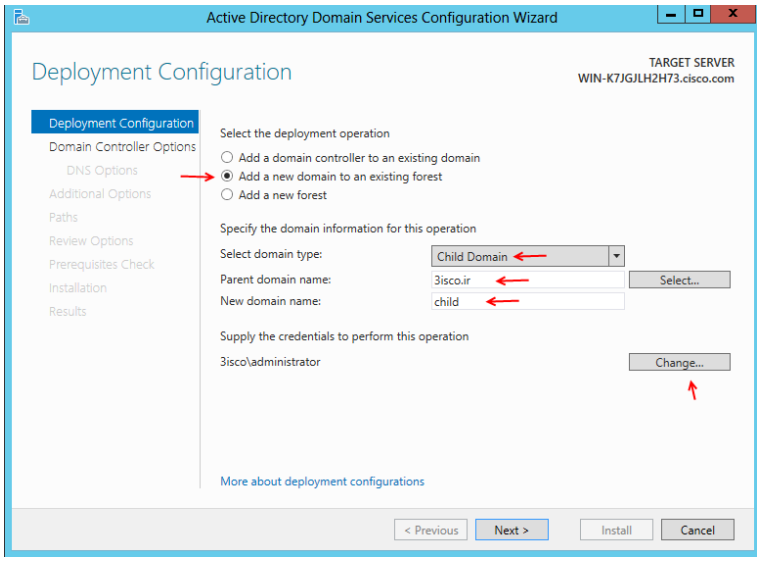
در این قسمت بدون انتخاب گزینه‌ای بر روی Next کلیک کنید



در این قسمت گزینه Restart the destination را انتخاب و بر روی install کلیک کنید تا Active Directory نصب شود.

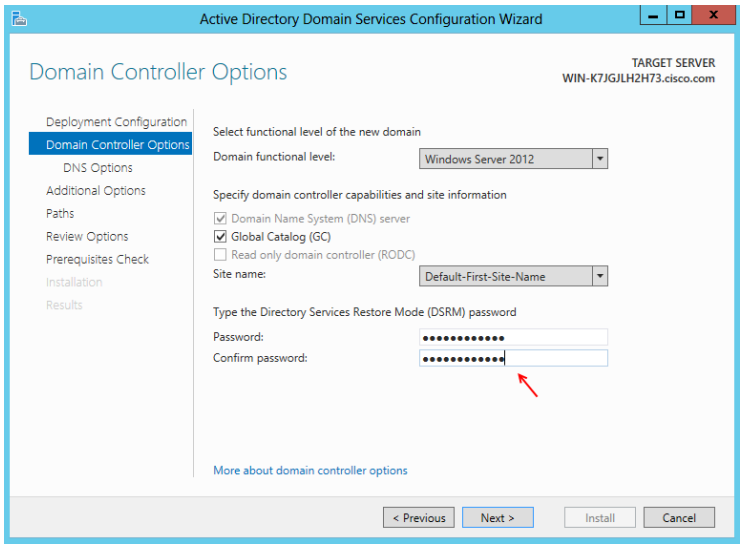


در این قسمت، بر روی Promote this server to a domain controller کلیک کنید.



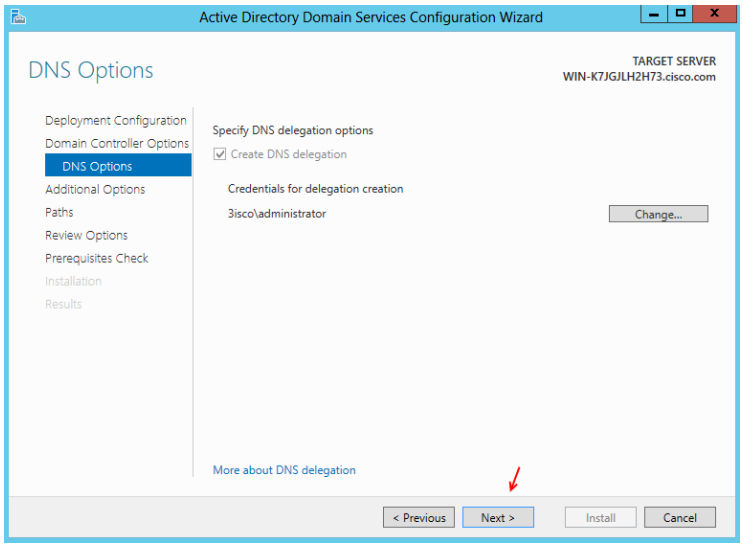
در این قسمت، اول گزینه Add a new domain to an existing forest را انتخاب کنید، در قسمت Select domain type گزینه Child Domain را انتخاب کنید و در قسمت Forest name نام دومین Root خود را وارد کنید و در قسمت New Domain name نام دومین جدید خود را وارد کنید، توجه داشته باشید با کلیک بر روی Change نام کاربری را وارد

کنید که در دومین اصلی (Forest) که در اینجا 3isco.ir می‌باشد اعتبار داشته باشد، برای ادامه کار بر روی Next کلیک کنید.



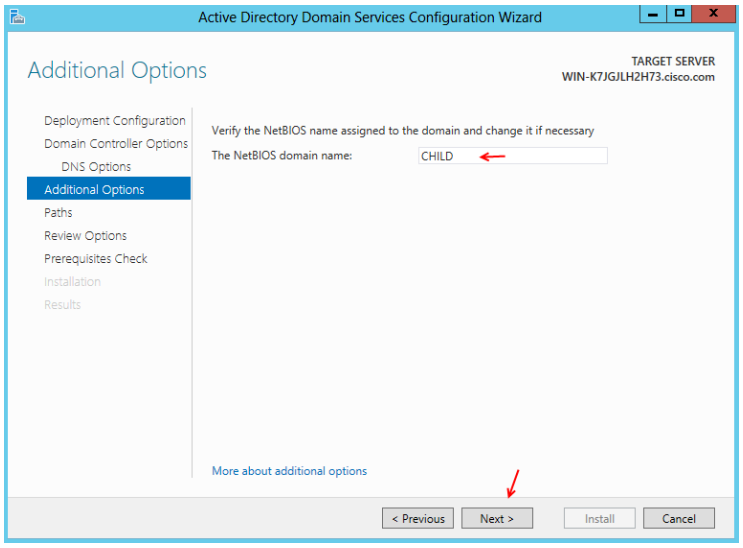
در این قسمت، یک رمز عبور برای Restore Mode در نظر بگیرید.

بر روی Next کلیک کنید.

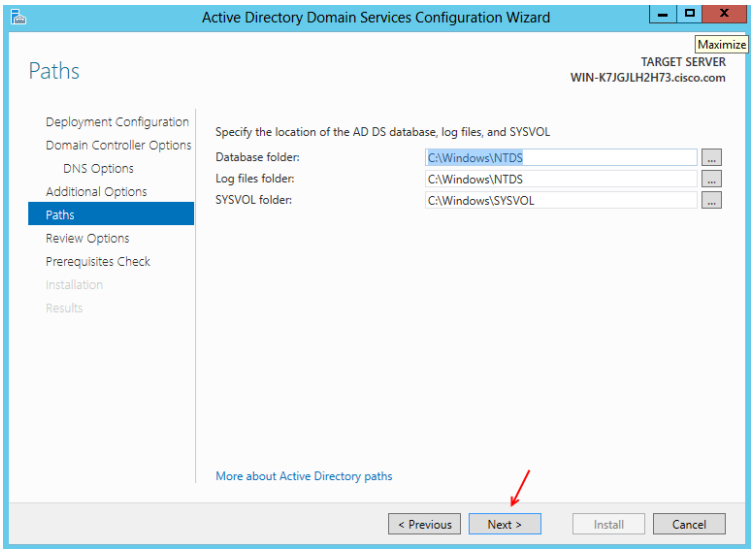


در این قسمت می‌توانید نام کاربری را وارد کنید که اولویت بالایی در دسترسی به سرویس DNS را داشته باشد.

بر روی Next کلیک کنید.

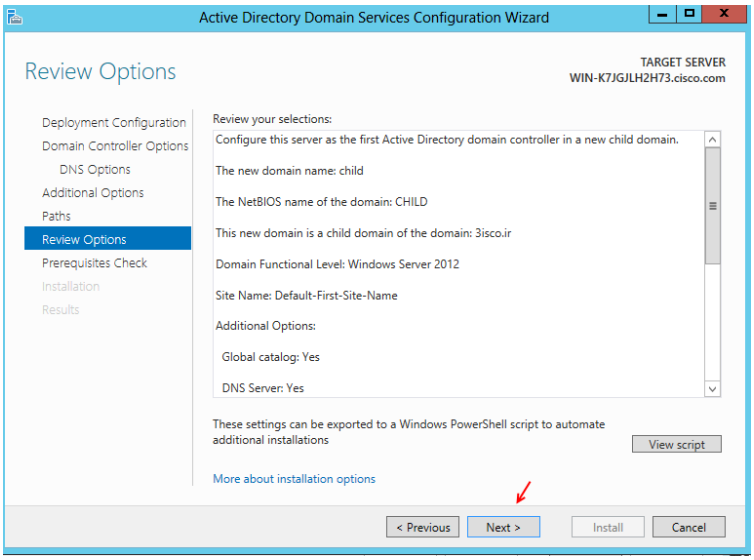


در این قسمت، نام Child تایید شده و می‌توانیم بر روی Next کلیک کنیم.

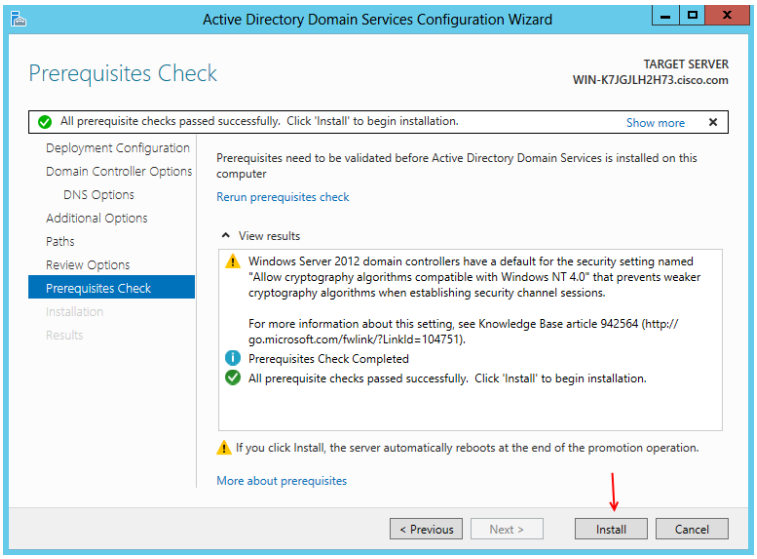


در این صفحه مسیر فولدرهای مشخص‌شده را می-توانید تغییر دهید که سعی کنید بر روی پیش فرض قرار داشته باشد.

بر روی **Next** کلیک کنید.



بر روی **Next** کلیک کنید.

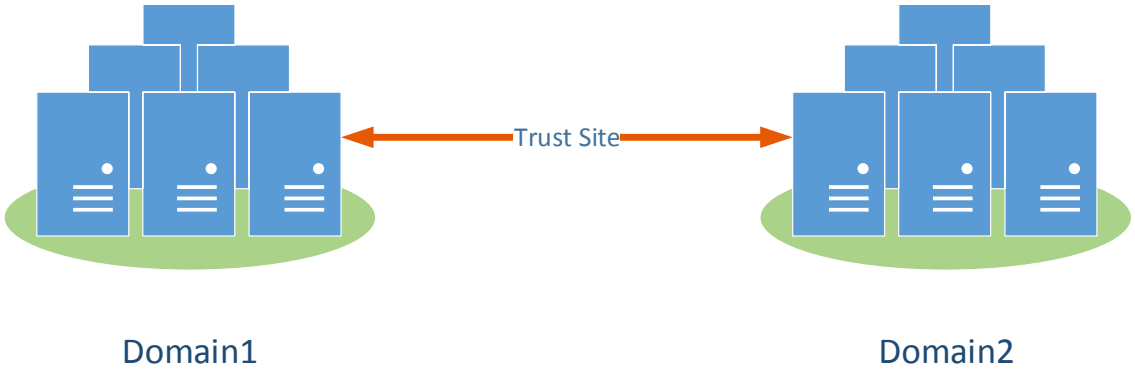


در این قسمت بعد از تایید اطلاعات بر روی **install** کلیک کنید تا کار نصب **Child domain** آغاز شود.

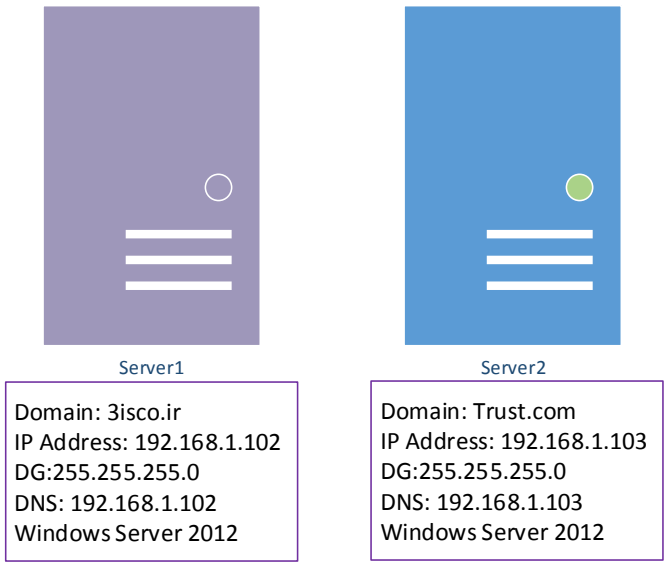
به این ترتیب **Child domain** به راحتی ایجاد شده است و می‌توانید از آن استفاده کنید.

ایجاد Trust بین دو دومین مختلف:

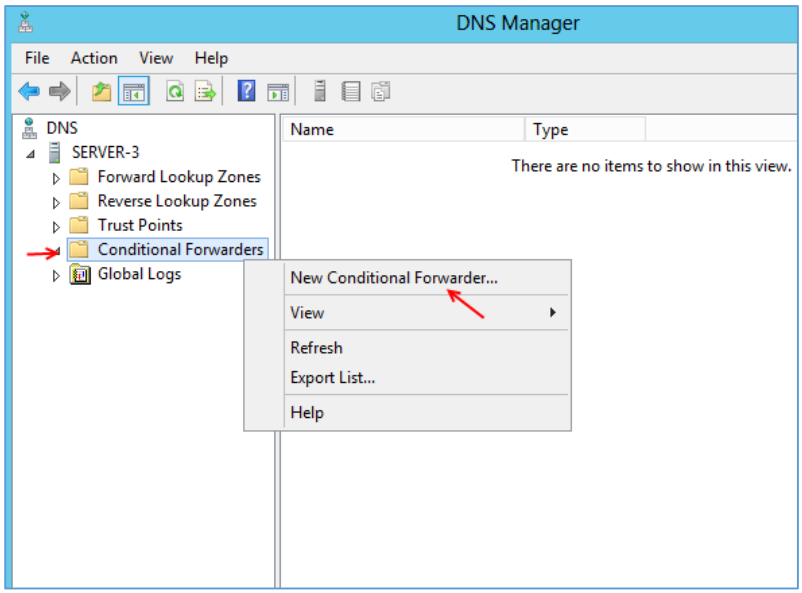
در این بخش می‌خواهیم دو دومین جدا از هم که هیچ گونه ارتباطی با هم ندارند را به هم ارتباط دهیم، این کار توسط سرویس Active Directory Domain and Trust انجام می‌شود که در این بخش با هم این سرویس را به صورت کامل بررسی می‌کنیم.



برای شروع از قبل دو دومین کنترلر آماده شده است که یکی با نام 3isco.ir و دیگری با نام Trust.com می‌باشد. توجه داشته باشید که رنج IP هر دو شبکه در یک رنج مشخص قرار دارد.

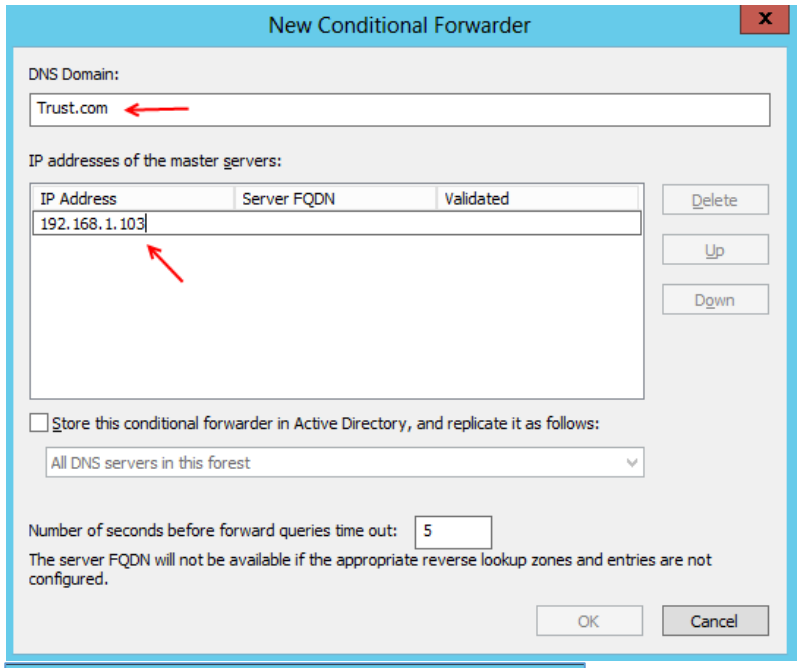


اولین کاری که باید انجام دهیم، تنظیم سرویس DNS می‌باشد، برای اینکار اول وارد سرور isco.ir3 می‌شویم و سرویس DNS را اجرا می‌کنیم.

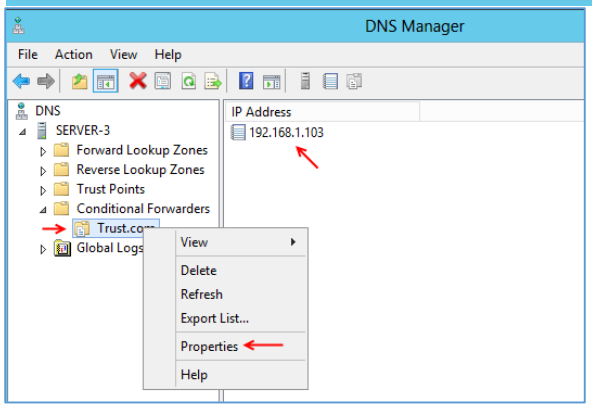


در این صفحه از سمت چپ بر روی Conditional Forwarders کلیک راست کنید و گزینه New Conditional Forwarder را انتخاب کنید.

همانطور که گفتم در حال حاضر سروری که دومین 3isco.ir بر روی آن فعال است بررسی می‌شود.

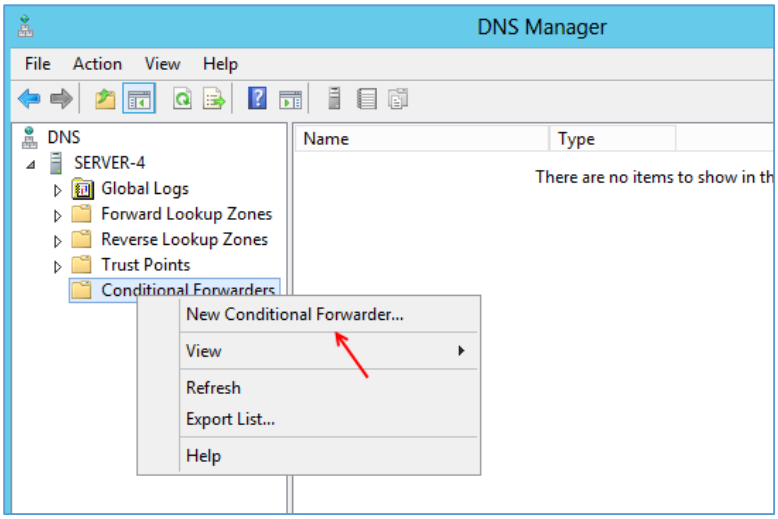


در این صفحه در قسمت DNS Domain نام دومین روبرو خود را که می‌خواهید با آن Trust برقرار کنید را وارد کنید، بعد از آن در قسمت IP Address آدرس IP موردنظر شبکه Trust.com را وارد کنید، همانطور که گفتم این دو شبکه باید در یک رنج قرار داشته باشند، بعد از آن بر روی Enter فشار دهید و بعد OK کنید.

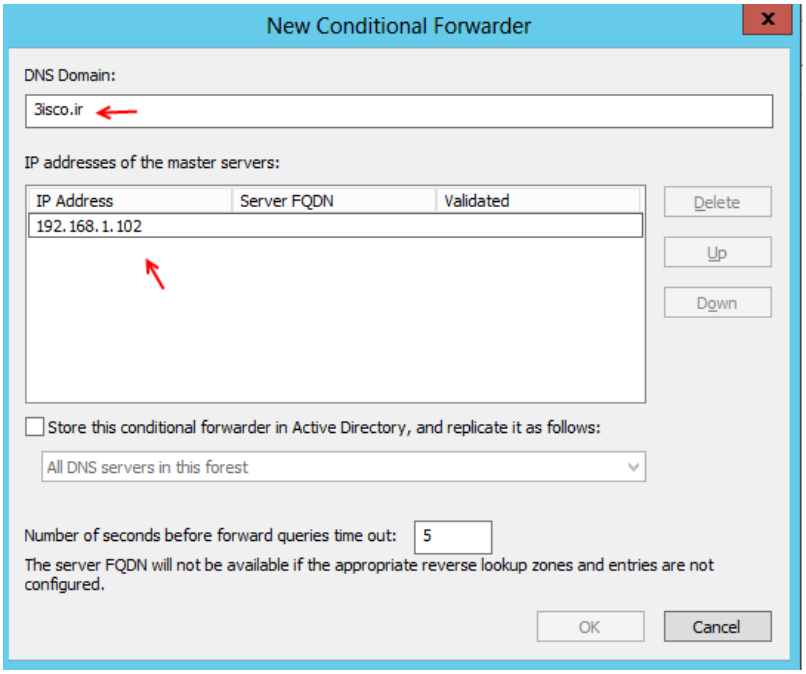


بعد از ایجاد ارتباط دهنده موردنظر می‌توانید برای اینکه متوجه شوید که ارتباط با سرور روبرو انجام گرفته بر روی Properties کلیک کنید و در شکل باز شده بر روی Edit کلیک کنید، اگر ارتباط برقرار باشد با آیکون سبز مشخص‌شده است.

بعد از انجام کار بالا باید وارد سرور دوم شویم و همین کار را برای سرور Trust.com برای انتقال اطلاعات به سرور 3isco.ir انجام دهیم.



وارد سرویس DNS شوید و بر روی Conditional Forwarders کلیک راست کنید و گزینه New Conditional Forwarder را انتخاب کنید.

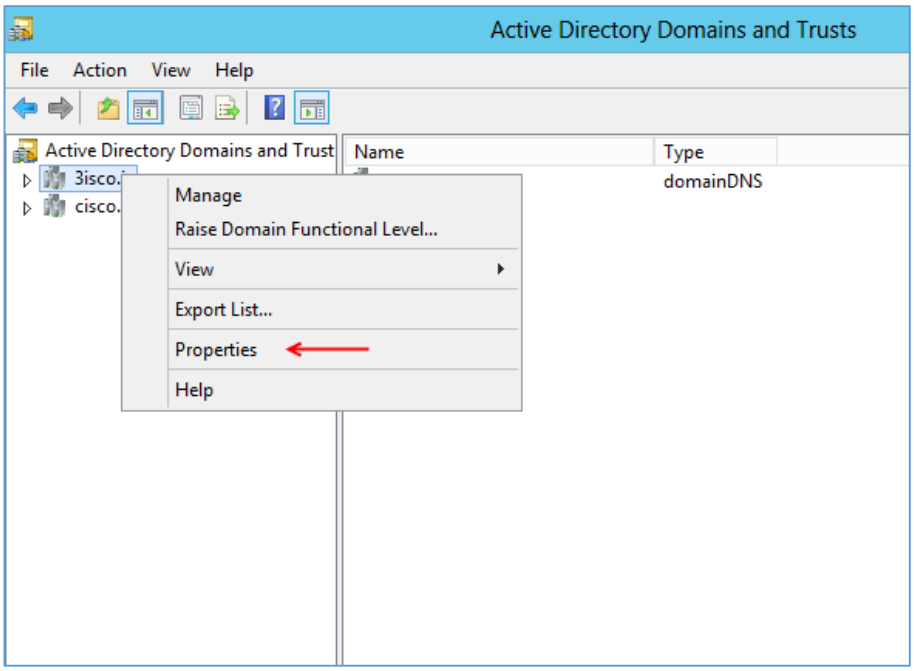


در این صفحه در قسمت DNS Domain نام دومین روبرو خود را که می‌خواهید با آن Trust برقرار کنید را وارد کنید، بعد از آن در قسمت IP Address آدرس IP موردنظر شبکه 3isco.ir را وارد کنید، همانطور که گفتم این دو شبکه باید در یک رنج قرار داشته باشند، بعد از آن بر روی Enter فشار دهید و بعد OK کنید.

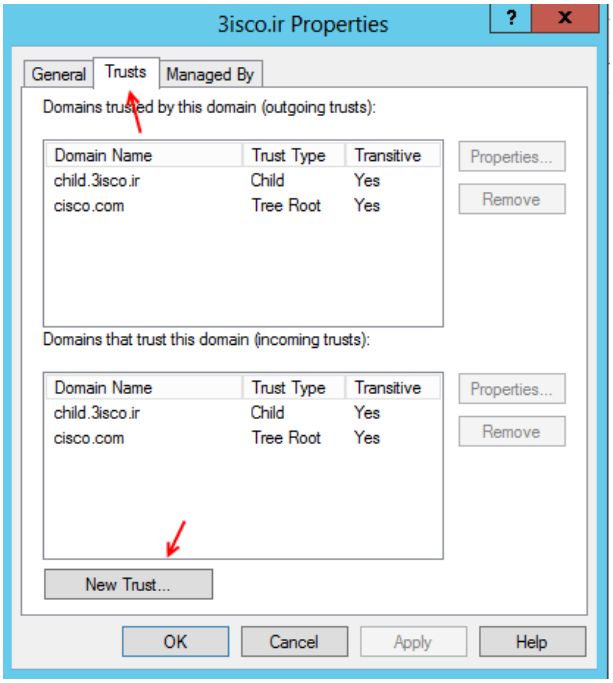
با انجام کارهای بالا همه اطلاعات مربوط به DNS Server به همدیگر ارسال می‌شود، یعنی اینکه اگر شما یک Host در یکی از سرویس های DNS ایجاد کنید، در طرف دیگر این Host ایجاد می‌شود.

در ادامه باید سرویس Active Directory Domain and Trust را برای ارتباط دو دومین با هم تنظیم کنیم.

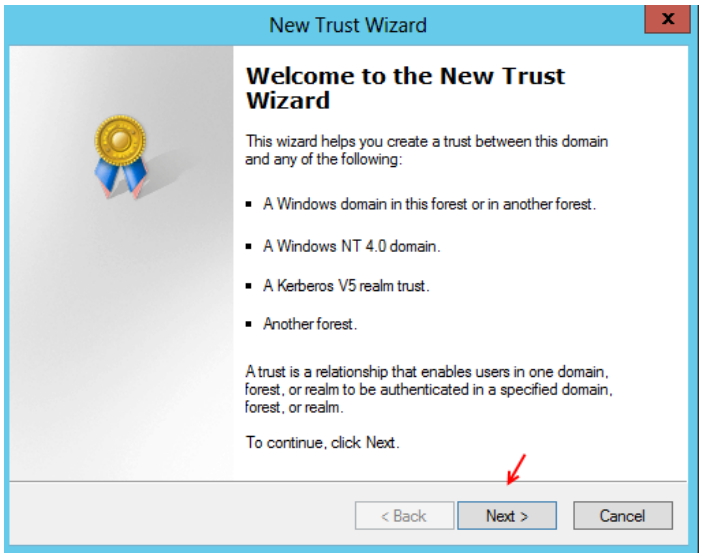
وارد سرور اول یعنی سروری که دومین 3isco.ir روی آن فعال است می‌شویم و سرویس Active Directory Domain and Trust را در Serach اجرا می‌کنیم.



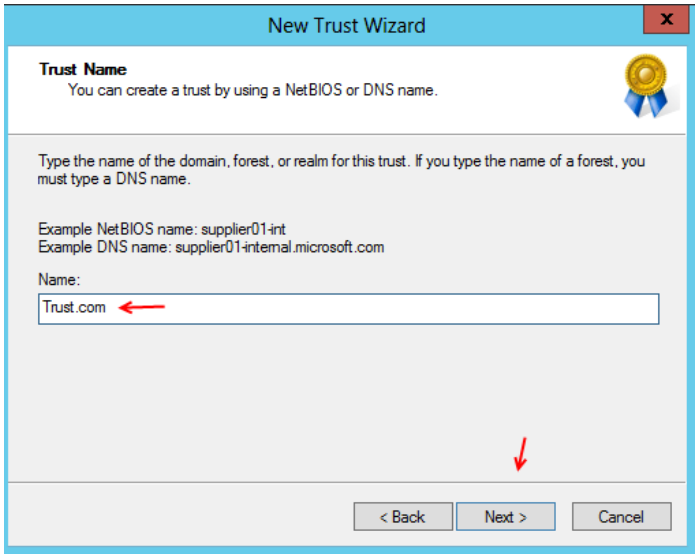
بعد از اجرای سرویس روی نام دومین خود کلیک راست کنید و گزینه Properties را انتخاب کنید.



در این قسمت، وارد تب Trusts شوید و برای ایجاد ارتباط بین دو دومین موردنظر بر روی New Trust کلیک کنید.

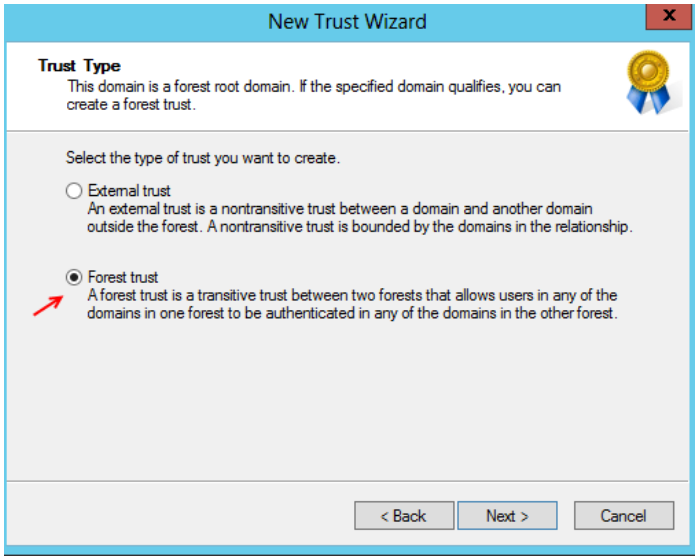


بر روی Next کلیک کنید.

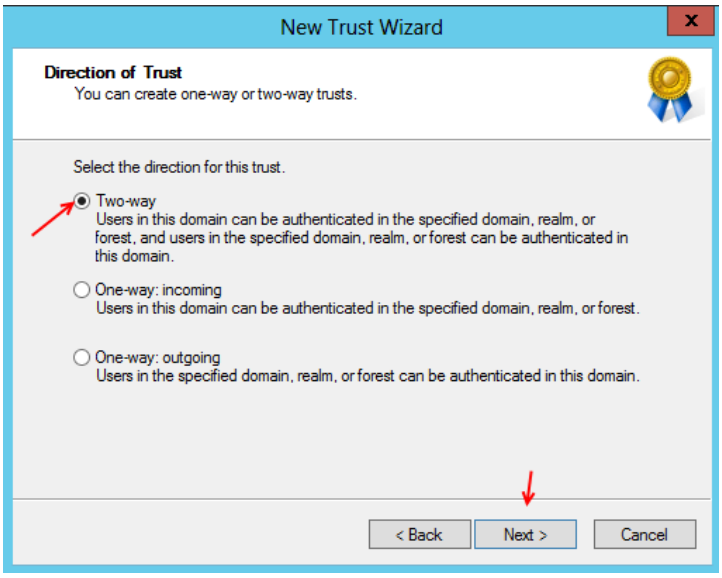


در این قسمت باید نام دومین روبرو را وارد کنید که در این قسمت Trust.com وارد شده است.

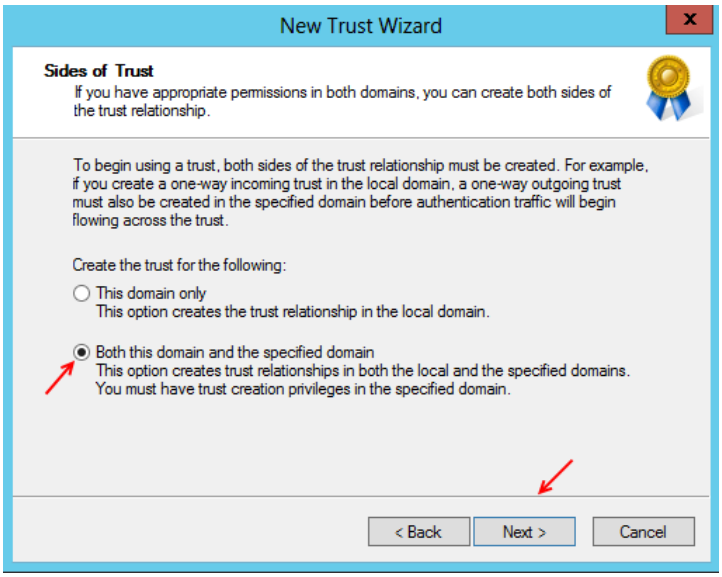
بر روی Next کلیک کنید.



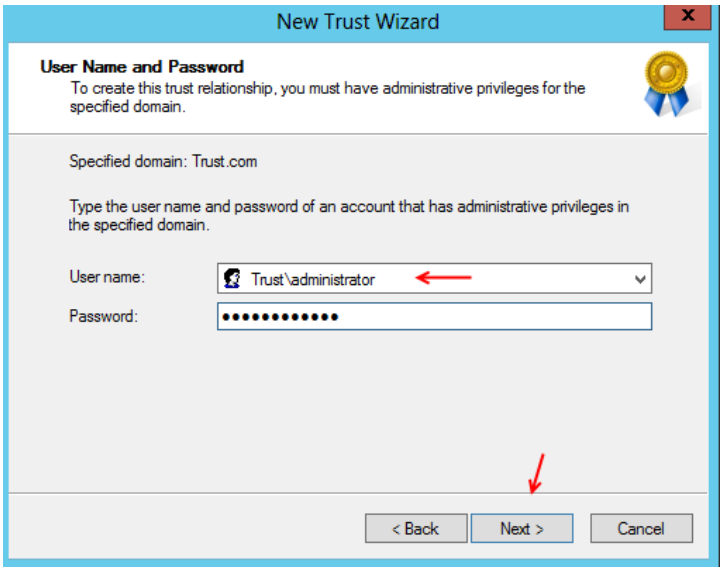
در این قسمت برای انتقال اطلاعات از دومین اصلی به دومین دیگر گزینه Forest trust را انتخاب کنید و بر روی Next کلیک کنید.



در این قسمت باید مشخص کنید که ارتباط بین دو دومین به چه صورت باشد، آیا می‌خواهید فقط اطلاعات ارسال شود و یا فقط دریافت شود و یا می‌خواهید هم ارسال و هم دریافت شود که باید گزینه اول یعنی Two-way را انتخاب کنید. و بر روی next کلیک کنید.

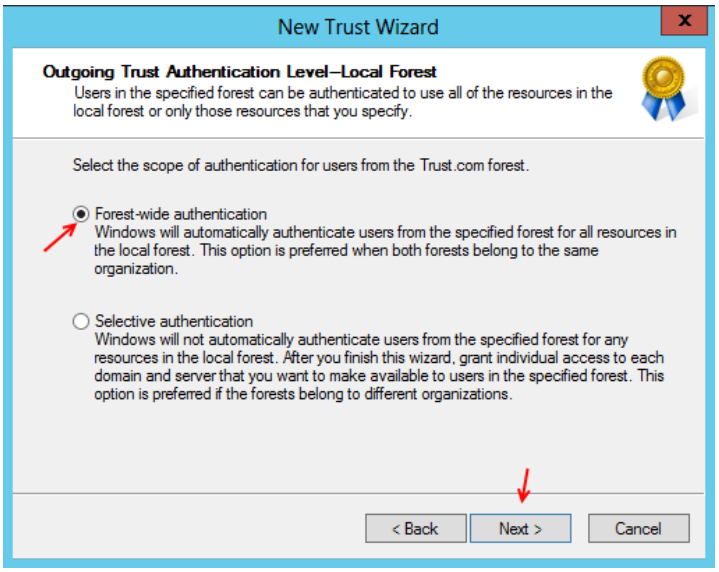


دراین قسمت گزینه Both this domain... را انتخاب و بر روی next کلیک کنید.

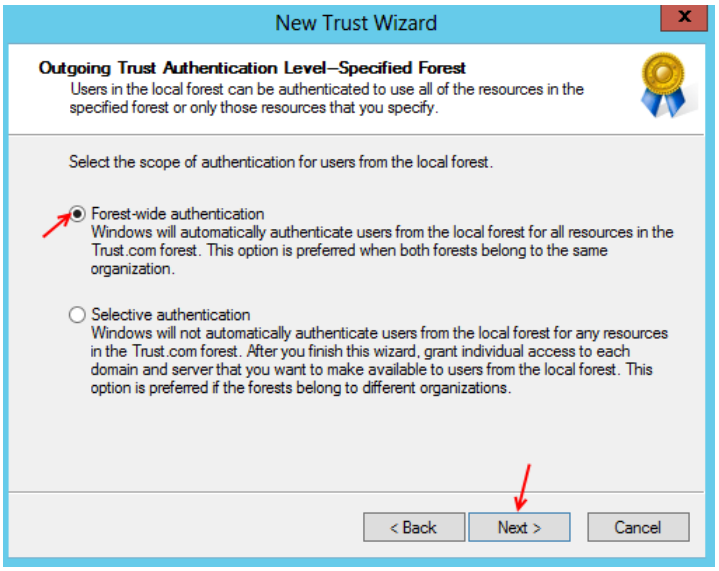


در این قسمت باید نام کاربری را وارد کنید که در دومین Trust.com یعنی دومین روبرویی اعتبار داشته باشد.

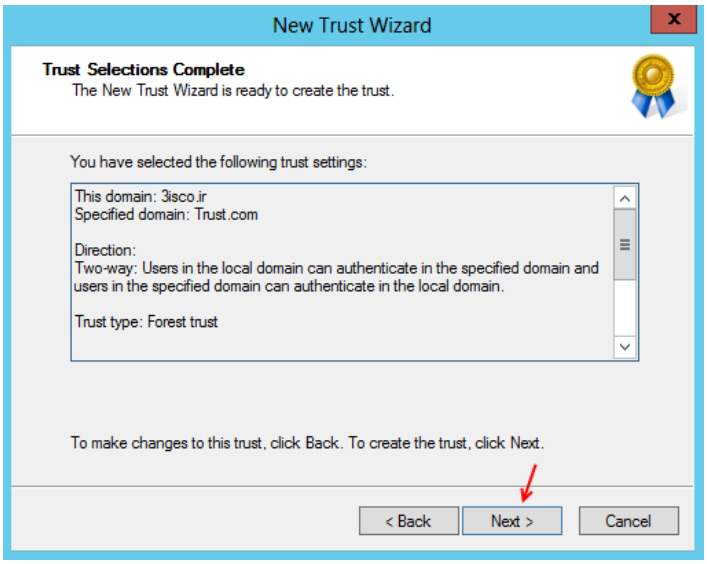
بعد از وارد کردن اطلاعات بر روی Next کلیک کنید.



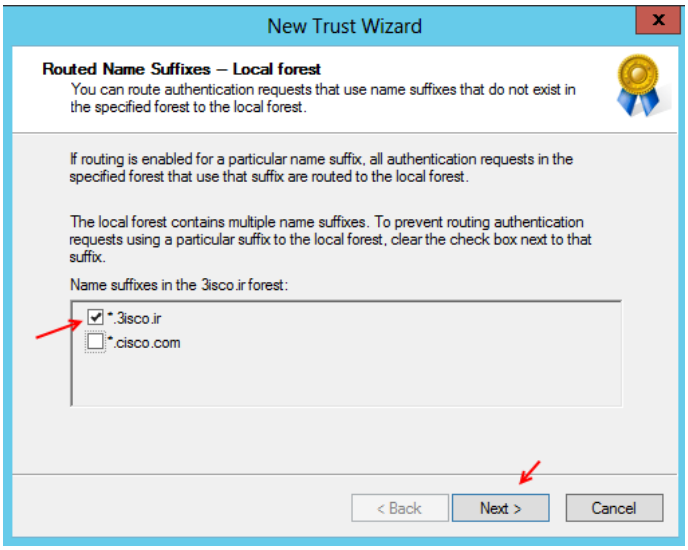
در این قسمت نحوه ایجاد امنیت را می‌توانید انتخاب کنید که در این بخش گزینه اول را انتخاب و بر روی Next کلیک کنید.



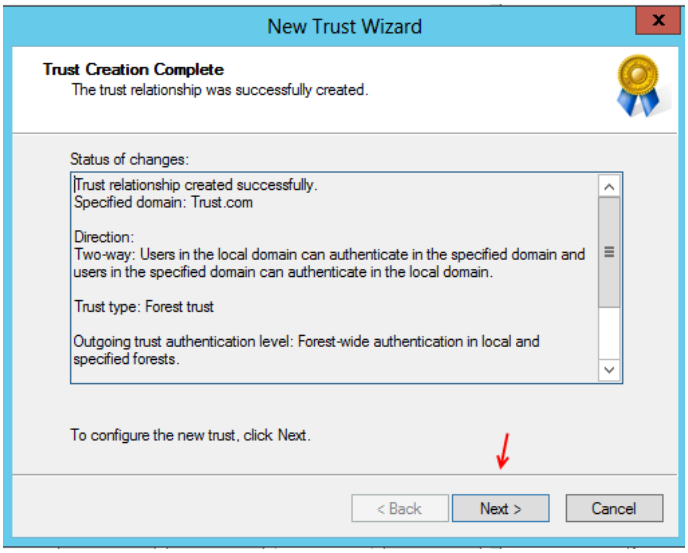
در این صفحه گزینه اول را انتخاب و بر روی Next کلیک کنید.



در این صفحه بر روی Next کلیک کنید....

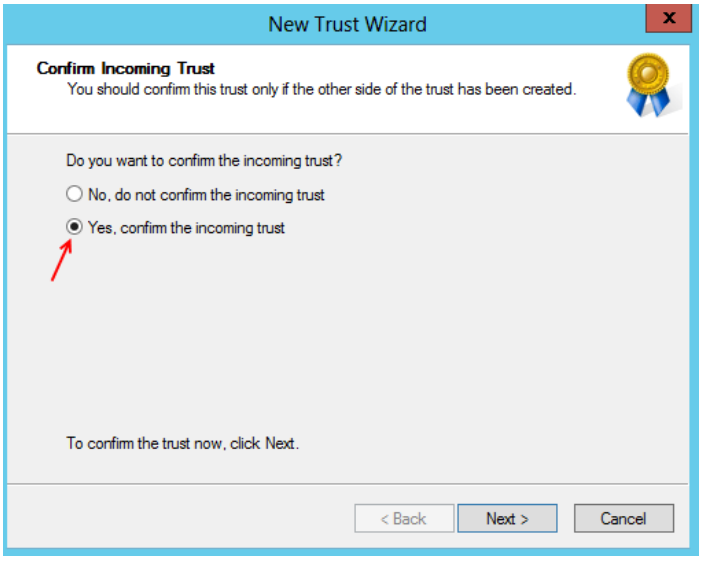


اگر در سرور خود از چندین دومین استفاده می‌کنید و یا استفاده می‌کردید در این قسمت لیست دومین‌ها را برای شما لیست می‌کنید که شما باید دومین موردنظر خود را انتخاب و بر روی Next کلیک کنید.



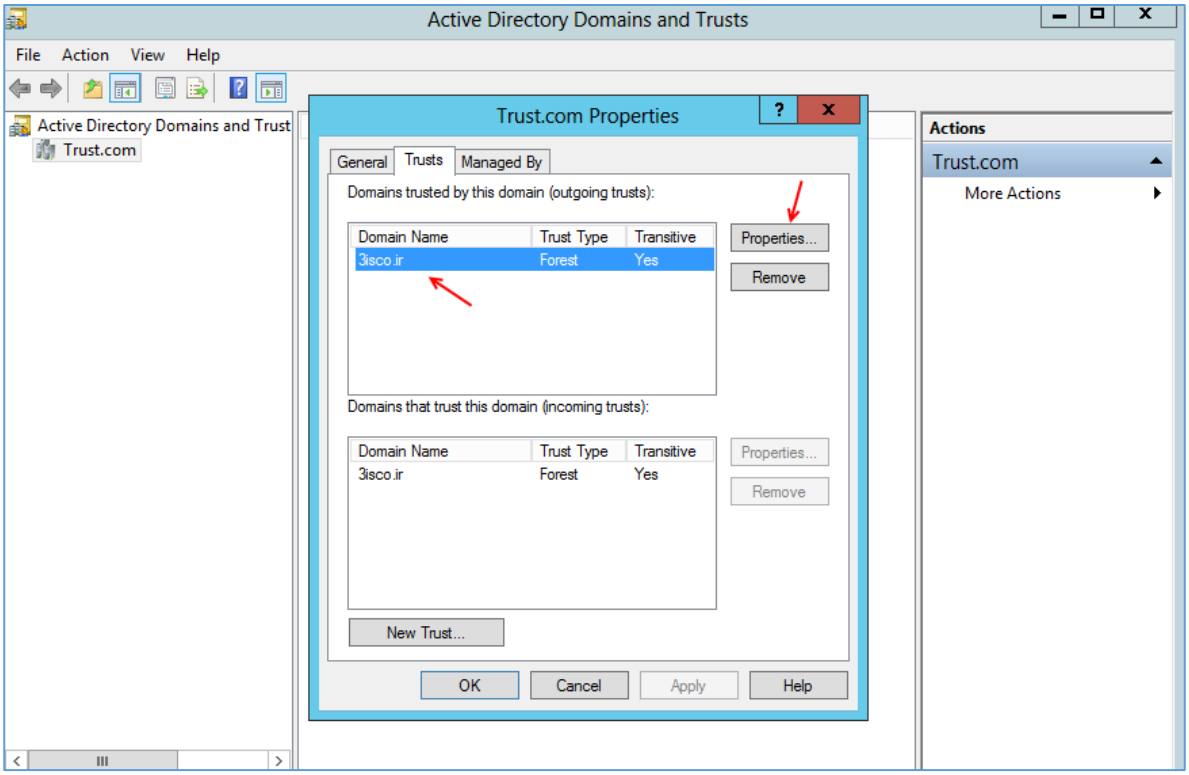
در این قسمت بر روی Next کلیک کنید.

این قسمت مربوط به تنظیم Outgoing Trust می‌باشد که باید گزینه Yes را انتخاب کنید و بر روی Next کلیک کنید.

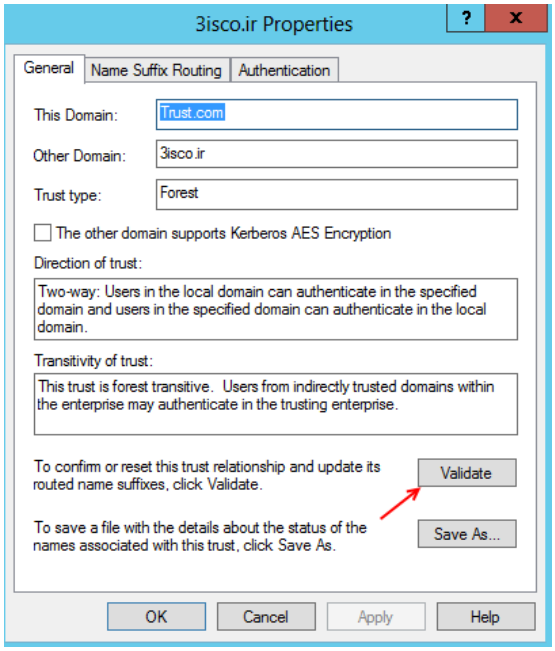


در این قسمت هم گزینه ..Yes را انتخاب و بر روی next کلیک کنید.

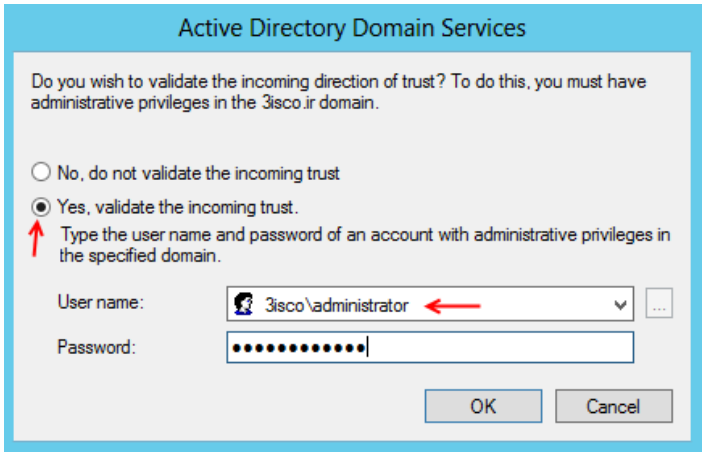
در صفحه آخر بر روی Finish کلیک کنید.



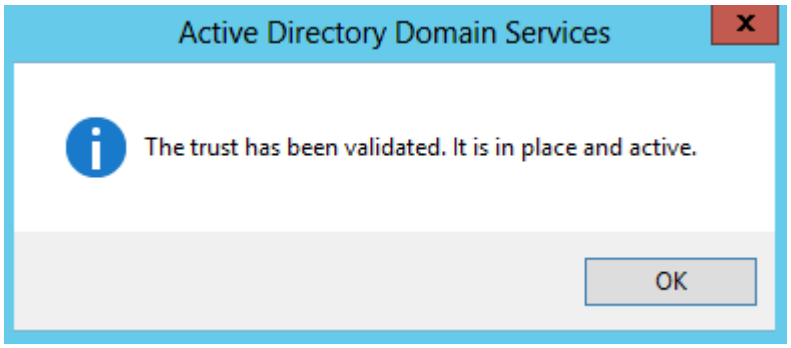
بعد از ایجاد Trust در دومین 3isco.ir حالا باید وارد سرور دوم شویم، همانطور که در شکل روبرو مشاهده می‌کنید سرور دوم یعنی دومین Trust.com به صورت خودکار تنظیمات ارتباطی را از سرور 3isco.ir دریافت کرده است. برای اینکه متوجه بشویم که ارتباط با سرور روبرو به صورت کامل برقرار شده است روی دومین موردنظر کلیک کنید و گزینه Properties را انتخاب کنید.



در این بخش در تب General بر روی گزینه Validate کلیک کنید تا شکل بعد ظاهر شود.



در این قسمت، باید نام کاربری که در دومین 3isco.ir اعتبار دارد را وارد کنید و بر روی ok کلیک کنید.



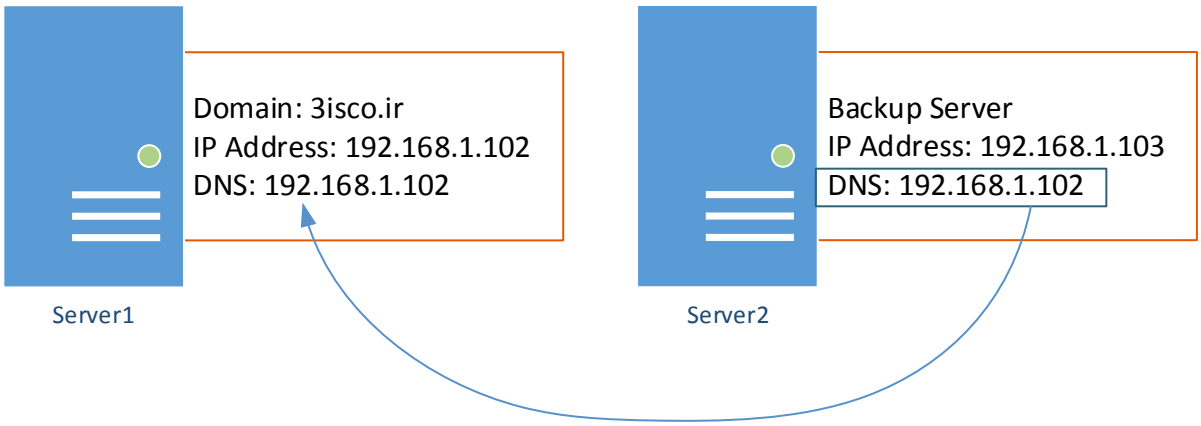
بعد از کلیک بر روی ok این پیغام مبنی بر انجام صحیح ارتباط با دومین روبرویی ظاهر می‌شود.

در ادامه نحوه انتقال اطاعات یک اکتیو دایرکتوری به یک اکتیو دایرکتوری دیگر را با هم بررسی می‌کنیم.

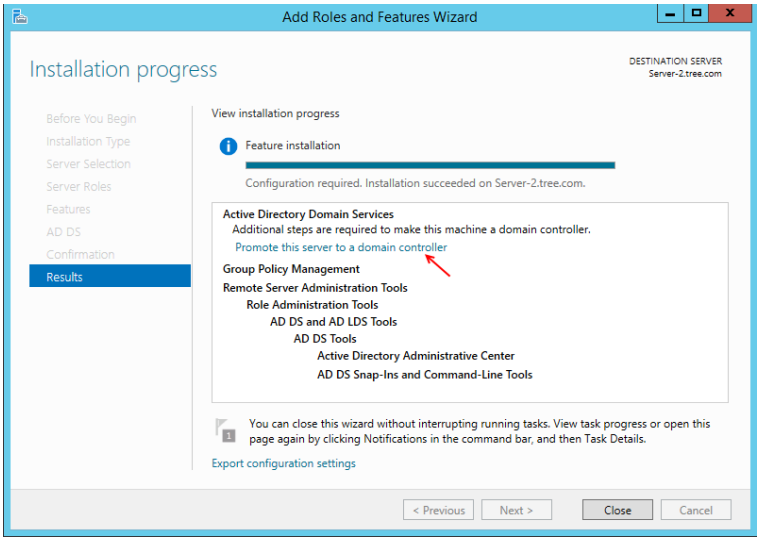
انتقال اطلاعات Active Directory از یک سرور به یک سرور دیگر

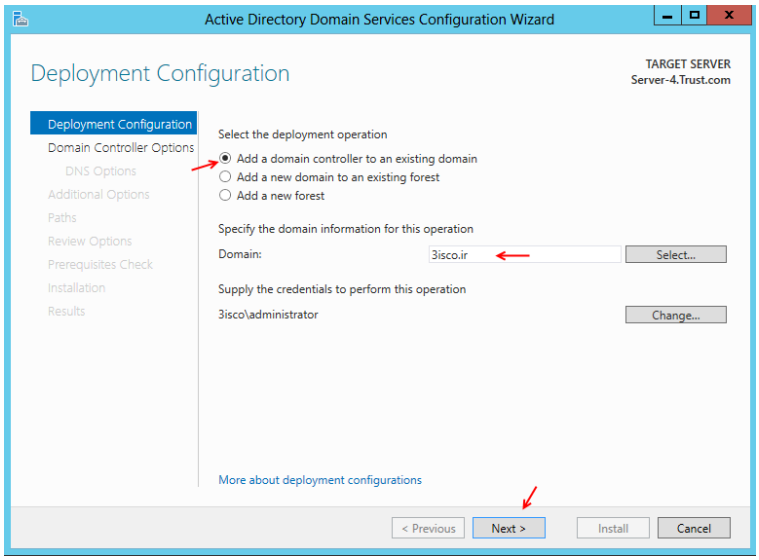
اگر شما مدیر یک شبکه بزرگ یا کوچک باشید و بعد از تلاش‌های بسیار یک دومین کنترلر به همراه چندین کاربر و گروه و ... ایجاد کرده باشید، حتماً دوست ندارید با ایجاد مشکل در سرور اصلی همه اطلاعات از بین برود، برای اینکه اطلاعات خود را که بسیار مهم است، حفظ کنیم، می‌توانیم یک سرور جدید آماده کنیم و اطلاعات مربوط به دومین کنترلر خود را به صورت کامل در طی فواصل زمانی مشخص به سرور دیگر انتقال دهیم.

برای این کار نیاز به یک سرور اصلی داریم که اطلاعات کاربران، گروه‌ها و ... روی آن قرار دارد که در این قسمت دومین 3isco.ir این نقش را بازی می‌کند، یک سرور دیگر در کنار سرور اول قرار می‌دهیم و رنج IP آن را در رنج IP سرور اصلی قرار می‌دهیم، توجه داشته باشید آدرس DNS باید آدرس سرور اصلی باشد.

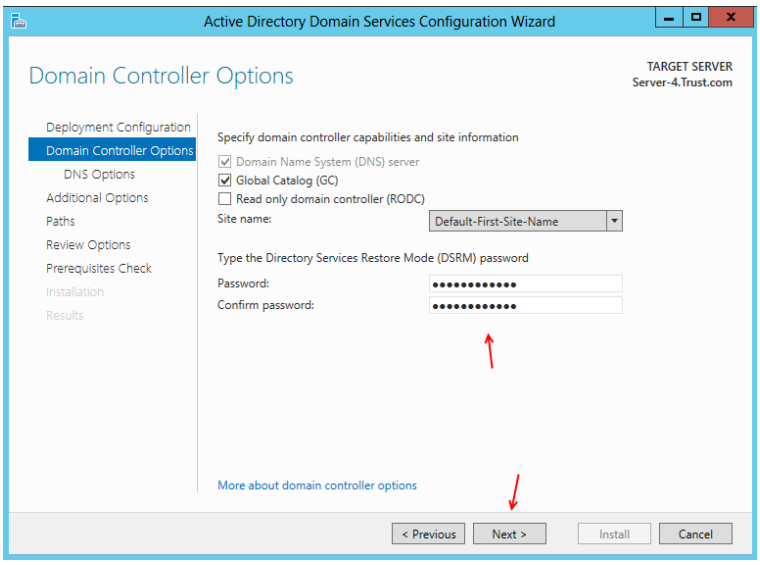


برای شروع وارد سرور دوم می‌شویم و Server Manager را اجرا می‌کنیم، بعد از اجرا بر روی Add Roles And Features کلیک کنید، در صفحه باز شده بر روی Next کلیک کنید تا به Server Roles برسید در این قسمت گزینه Active Directory Domain Services را انتخاب کنید و بر روی Next کلیک کنید و سرویس را نصب کنید. بعد از نصب به مانند شکل روبرو بر روی Promote this server to a domain controller کلیک کنید.

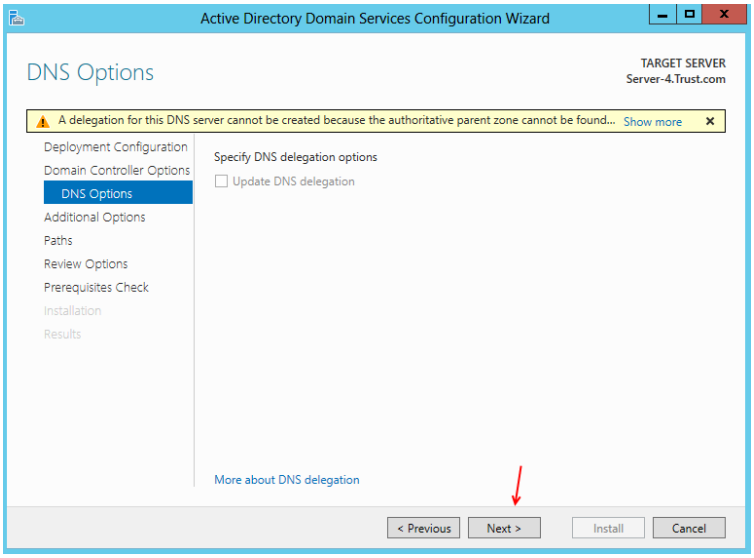




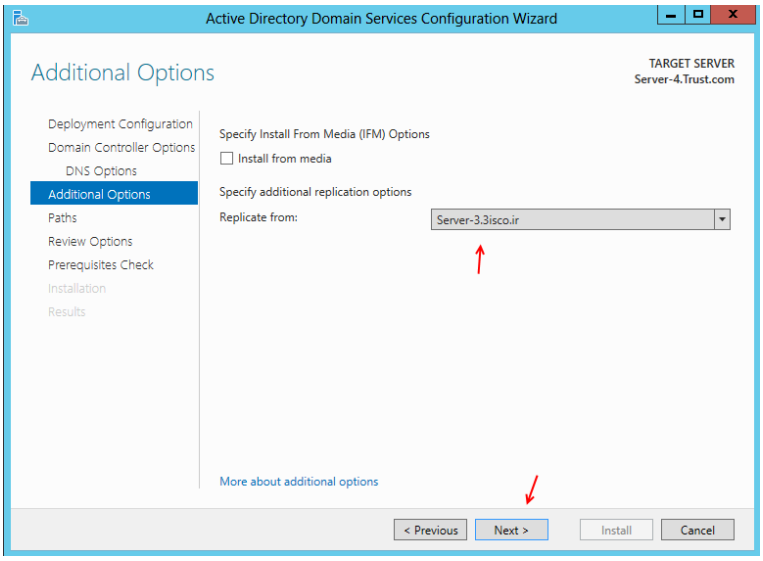
در این صفحه گزینه Add a domain controller to an existing domain را انتخاب و در قسمت Domain نام دومین خود را به مانند شکل وارد کنید و در قسمت Supply the cre... یک نام کاربری که در دومین 3isco.ir اعتبار دارد را وارد کنید و بر روی Next کلیک کنید.



در این قسمت، رمز عبور برای Restore Mode وارد کنید و بر روی Next کلیک کنید.



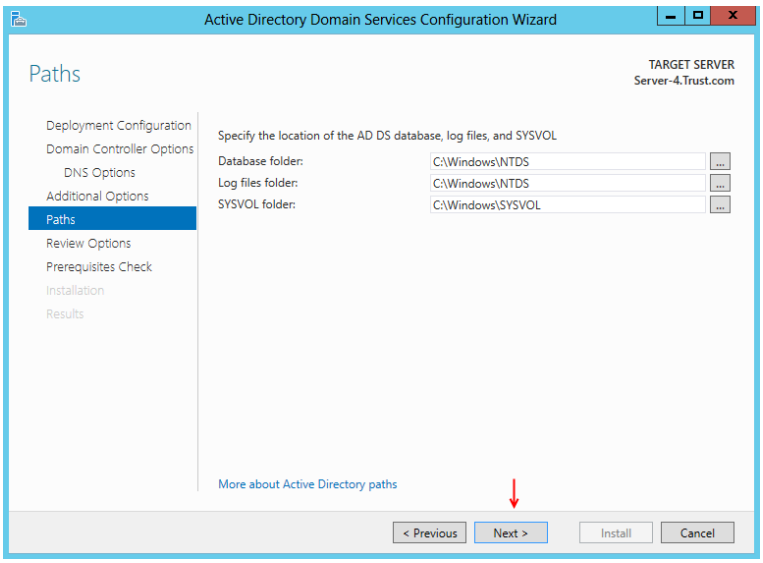
در این قسمت، بر روی Next کلیک کنید.



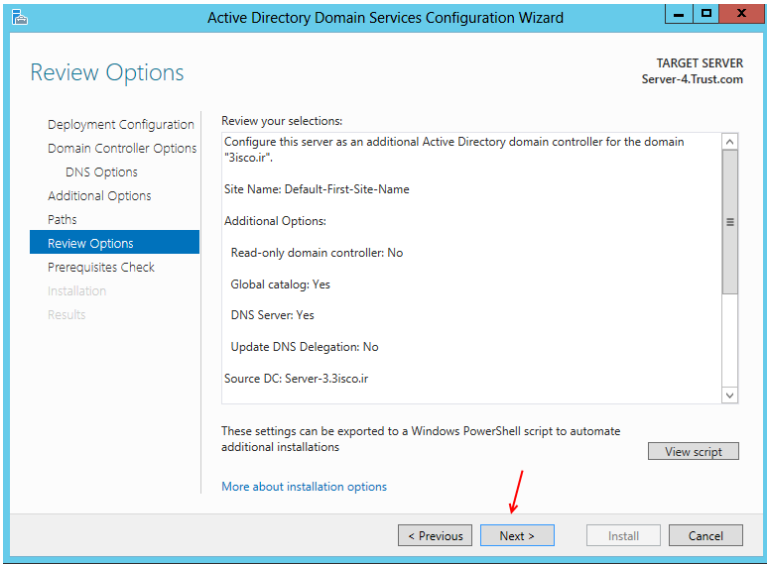
در این صفحه از قسمت Replicate from از منوی کشویی سرور موردنظر خود که دومین 3isco.ir روی آن فعال است را انتخاب کنید.

Server-3 نام سروری است که دومین روی آن فعال است.

بر روی Next کلیک کنید.



در این قسمت بر روی Next کلیک کنید.

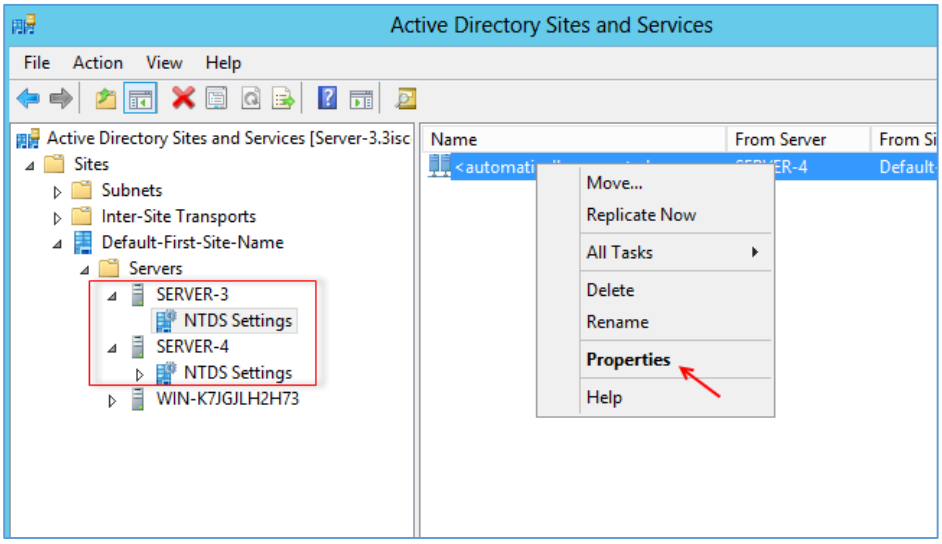


در این قسمت بر روی next کلیک کنید.

در صفحه آخر هم بر روی Install کلیک کنید تا دومین موردنظر فعال شود.

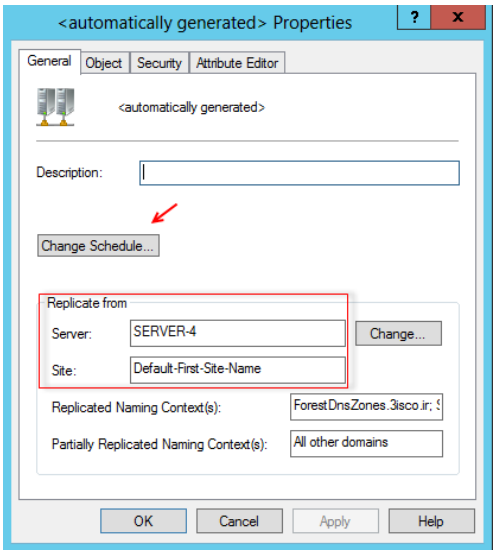
بعد از این که تنظیمات موردنظر را انجام دادید، تمام اطلاعات از دومین اصلی یعنی3isco.ir به سرور دوم انتقال داده باشد، اگر هم یک کاربر ایجاد کنید چند ثانیه بعد این کاربر به سرور دوم انتقال داده می‌شود، به نظرشما کار انتقال اطلاعات Active را چه سرویسی انجام می‌دهد؟

کار انتقال اطلاعات بین دو سرور توسط سرویس Site and Service انجام می‌شود که برای اجرای آن وارد سرور اصلی که دومین 3isco.ir روی آن قرار دارد شوید و در Search به مانند شکل روبرو سرویس Site And Service را اجرا کنید.

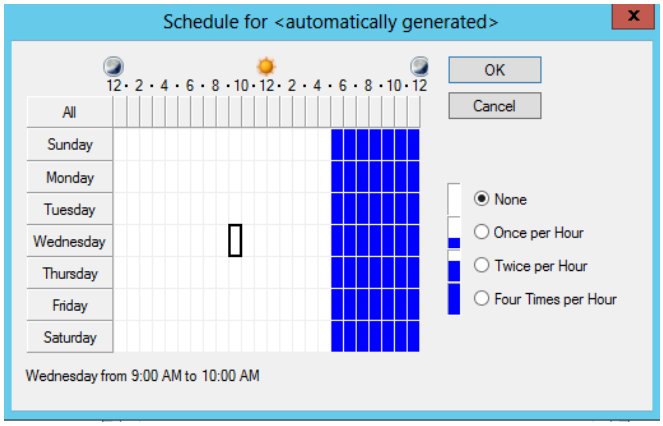


همانطور که مشاهده می‌کنید سرویس موردنظر اجرا شده است، اگر از سمت چپ وارد Server شوید مشاهده می‌کنید که دو سرور با نام‌های Server-3 و Server-4 ایجاد شده است که ارتباط بین دو سرور از این طریق انجام می‌شود.

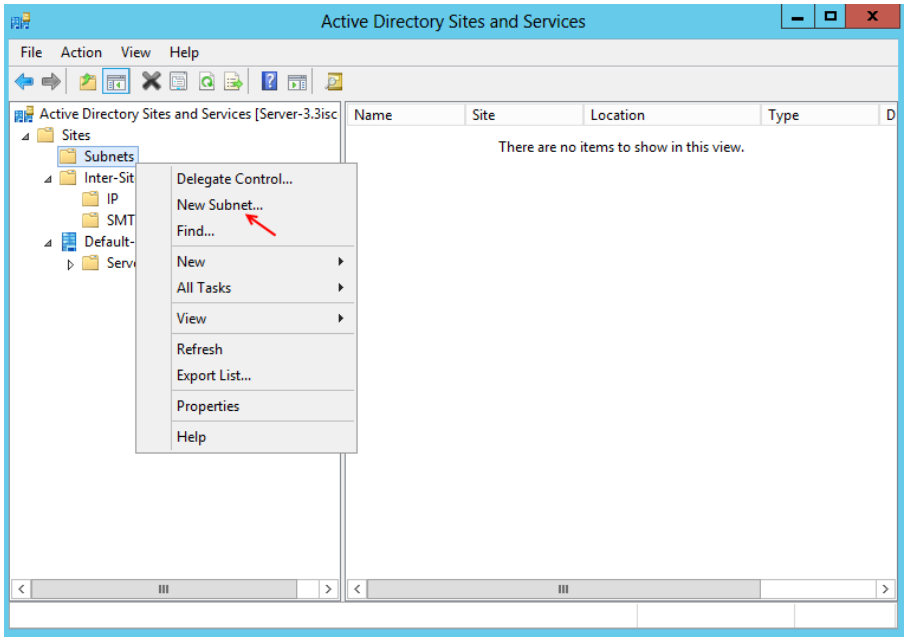
اگر برروی NTDS Settings در قسمت Server- 3 کلیک کنید در صفحه باز شده بر روی <Automatically generated> کلیک راست کنید و Propertoes را انتخاب کنید.



در این صفحه اگر به قسمت Replicate from توجه کنید نام سرور را Server-4 می‌باشد و در قسمت Site نام Link ارتباطی به صورت پیش فرض وارد شده است. برای اینکه مشخص کنید که چه زمانی اطلاعات Active Directory بین دو سرور انتقال داده شود، بر روی Change Schedule کلیک کنید.

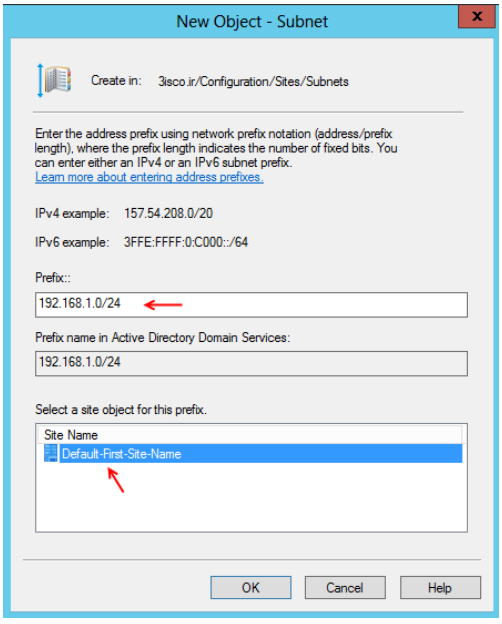


در این قسمت با بررسی شرایط سازمان خود ساعات و روزهای مورد نیاز خود را برای انتقال اطلاعات بین دو سرور را انتخاب کنید، سعی کنید این کار را در ساعات کم کاری انجام دهید، اگر همه مستطیل‌های موردنظر را انتخاب کنید و بر روی None کلیک کنید همه آنها به رنگ سفید در می‌آیند.

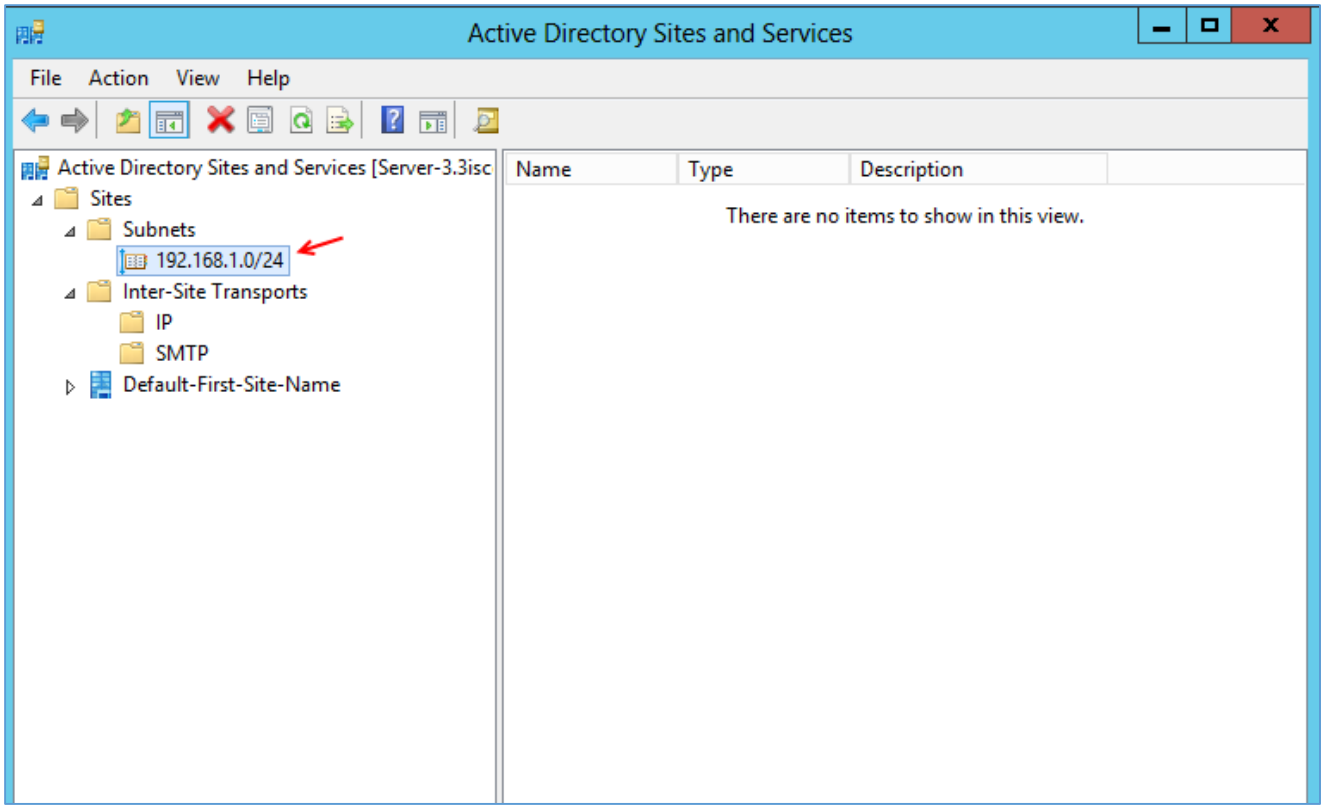


بعد از انجام عملیات بالا از سمت چپ بر روی Subnets کلیک راست کنید و گزینه New Subnet را انتخاب کنید،

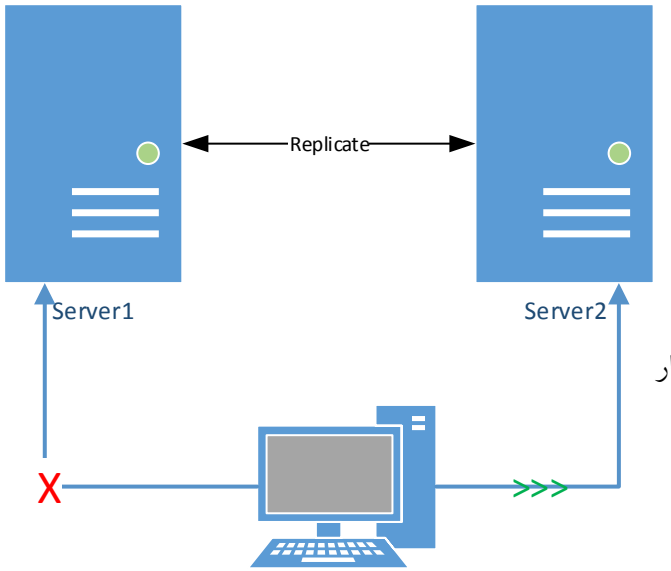
این قسمت برای تعریف Subnet شبکه موردنظر می‌باشد.



در این صفحه در قسمت Prefix آدرس Net شبکه خود را وارد کنید، یعنی اگر آدرس به صورت 192.168.1.102 و subnet به صورت 255.255.255.0 بود سه تا 255 به این معنی است که سه قسمت اول IP ثابت است و چون هر قسمت 8 بیتی است 3 تا 8 تا می‌شود 24 بیت که آدرس به صورت 192.168.1.0/24 وارد می‌کنیم. بعد از وارد کردن اطلاعات Site Name را انتخاب و بر روی ok کلیک کنید.



همانطور که در شکل بالا مشاهده می‌کنید Subnet موردنظر ایجاد شده است، توجه داشته باشید با ایجاد Subnet در یکی از سرورها در سرور دیگر هم این Subnet به صورت خودکار ایجاد می‌شود.

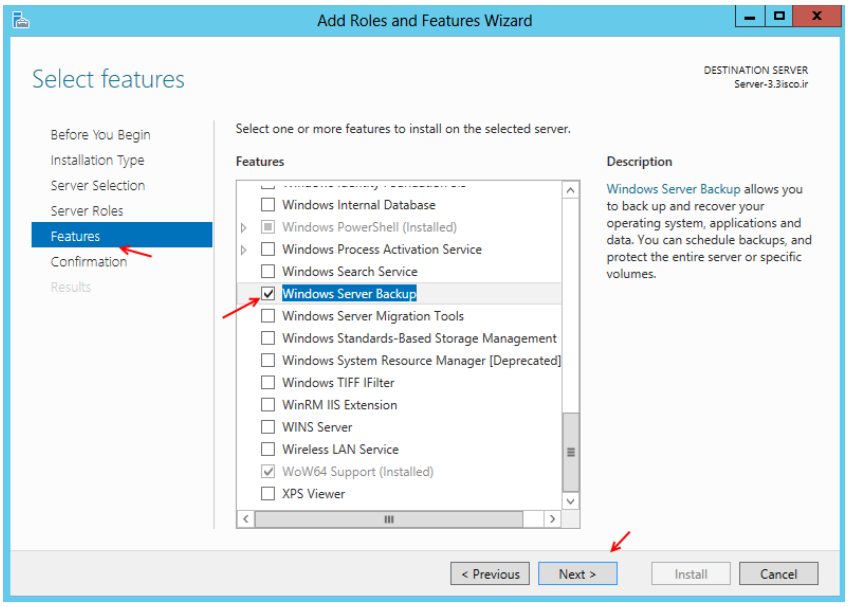


بیشترین کاربرد این سرویس این است که تمام اطلاعات موجود در سرور اصلی که در اینجا Server1 می‌باشد به Server2 انتقال داده می‌شود و اگر چنانچه server1 کارایی خود را از دست بدهد، شبکه به هیچ عنوان قطع نخواهد شد و تمام کاربران به Server 2 منتقل می‌شوند که کار بسیار جالبی خواهد بود.

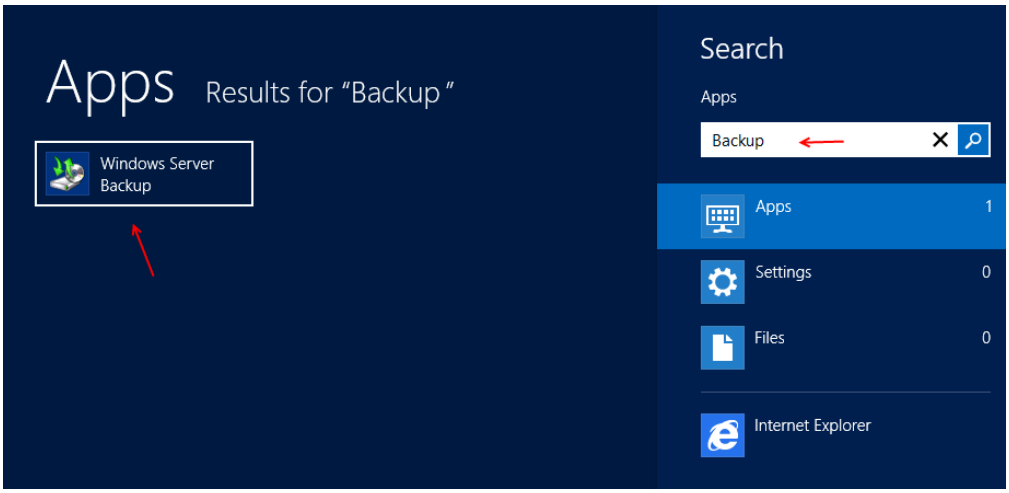
نحوه Backup **و** Restore **کردن:**

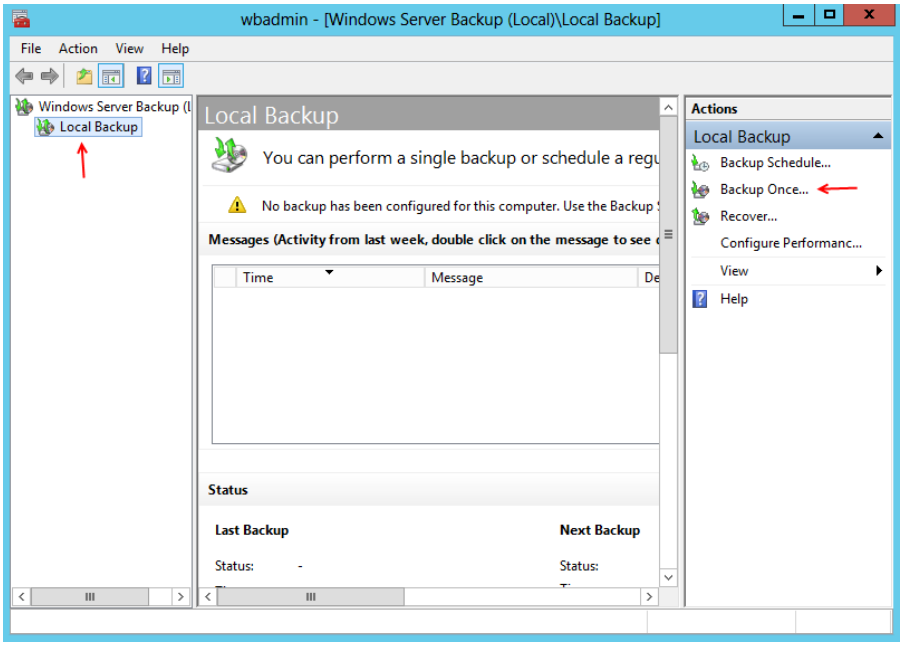
یکی از مهمترین کارهایی که در یک شبکه انجام می‌شود گرفتن Backup کامل از اطلاعات موجود بر روی سرور است این اطلاعات می‌تواند، اطلاعات Active Directory ویا اطلاعات سرویس‌های دیگر بر روی سرور باشد، برای انجام این کار به روش زیر عمل کنید.

وارد سرور خود شوید و Server Manager را اجرا کنید و در صفحه باز شده بر روی Add Roles and Features کلیک کنید و در صفحه باز شده بر روی Next کلیک کنید تا به قسمت Features برسید، در این قسمت به مانند شکل گزینه Windows Server Backup را انتخاب کنید و بر روی Next کلیک کنید و در آخر بر روی Install کلیک کنید.

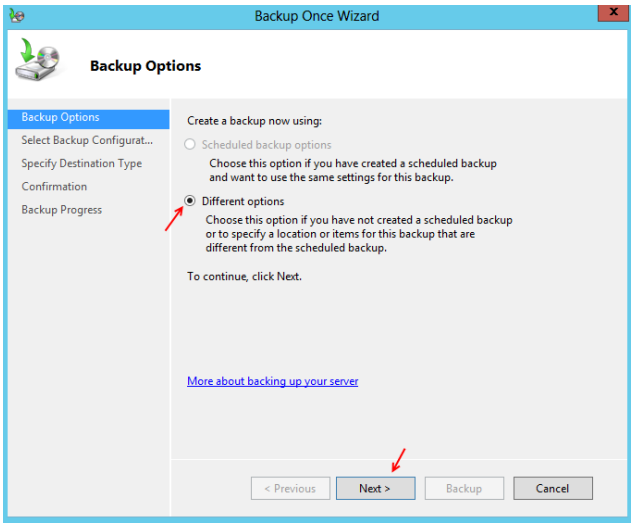


بعد از نصب سرویس وارد Serach شوید و سرویس Windows server Backup را اجرا کنید.

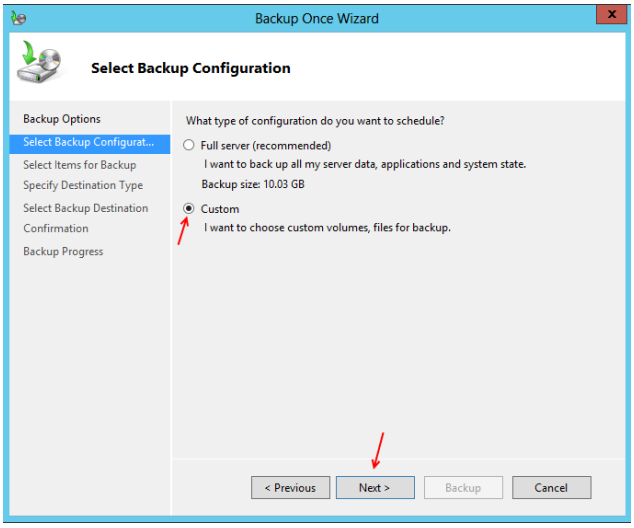




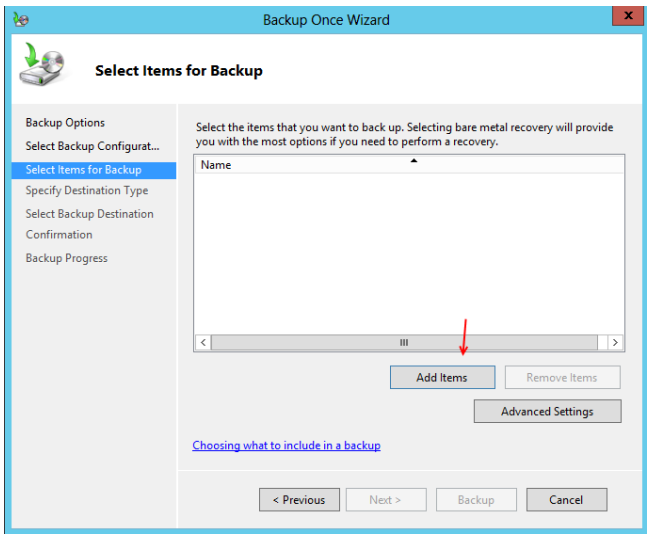
بعد از اجرای سرویس از سمت چپ بر روی Backup Once کلیک کنید، تاشکل بعد ظاهر شود.



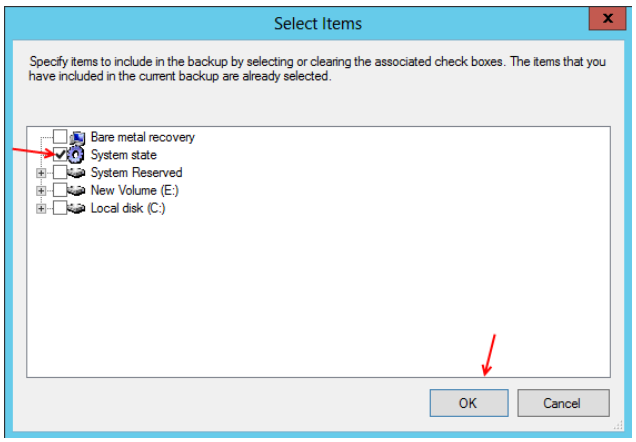
در این قسمت گزینه different options را انتخاب کنید وبر روی next کلیک کنید.



دراین صفحه اگر گزینه Full Server را انتخاب کنید تمام بخش های سرور شما، مانند فایل‌ها، اسناد، سرویس‌ها و... Backup گرفته می‌شود که حجمی حدود 10 گیگابایت را برای این سرور نیاز دارد که فکر نکنم کار واجبی باشه، برای اینکه گزینه های موردنظر خود را انتخاب کنیم، Custom را انتخاب و بر روی next کلیک کنید.

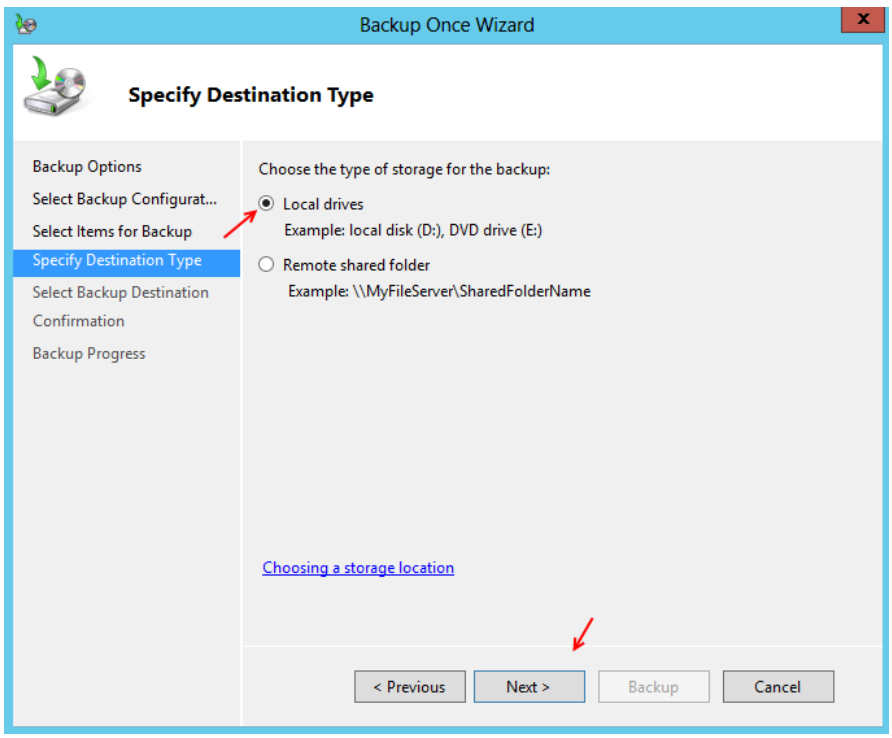


در این صفحه باید قسمت موردنظر خود را برای گرفتن Backup انتخاب کنیم برای این کار بر روی Add item کلیک کنید.



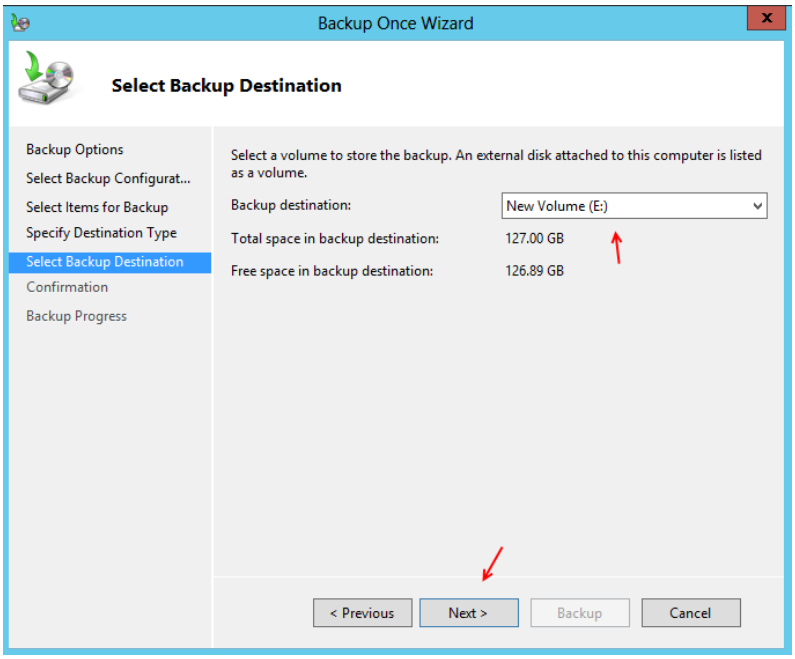
در این قسمت برای اینکه از اطلاعات Active Directory یک backup تهیه کنیم، گزینه System state را انتخاب کنید و بر روی ok کلیک کنید.

بعد از اضافه شدن به لیست موردنظر بر روی next کلیک کنید.



در این قسمت باید محل ذخیره سازی Backup خود را انتخاب کنید، به این نکته توجه کنید که محل ذخیره سازی نمی‌تواند درایو ویندوز که به صورت پیش فرض درایو C است باشد، شما می‌توانید یک آدرس در شبکه را وارد کنید.

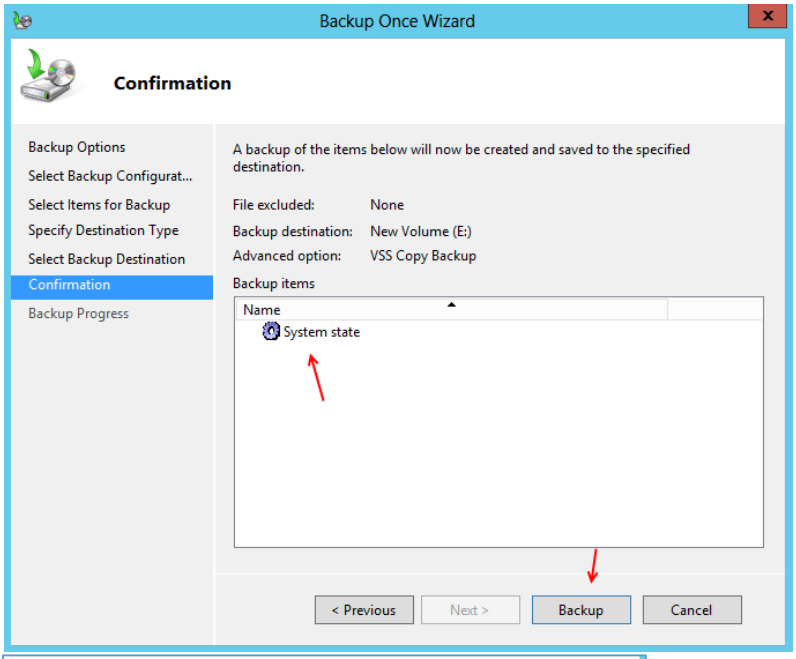
در این قسمت گزینه local drives را انتخاب کنید و بر روی next کلیک کنید.



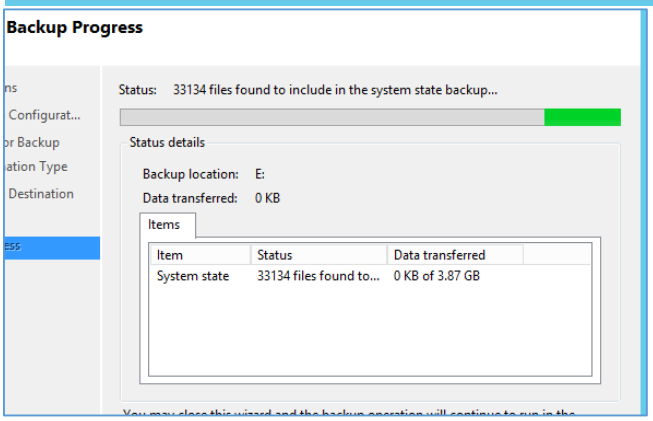
در این قسمت درایو موردنظر خود را انتخاب کنید، اگرتوجه کنید در اینجا درایو E انتخاب شده است.

اگر از ماشین مجازی استفاده می‌کنید، سرور را Shutdown کنید و یک هارد مجازی به آن اضافه کنید.

بر روی Next کلیک کنید.



در این صفحه بر روی Backup کلیک کنید تا Backup از قسمت System state تهیه شود.



در حال ایجاد Backup از قسمت system state...

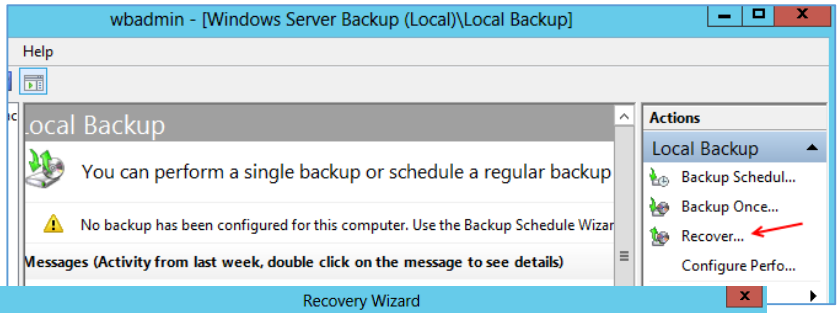
بسته به حجم سرور زمان بر خواهد بود.

با انجام کارهای بالا توانستیم از قسمت system state یک Backup تهیه کنیم که این Backup شامل تمام سرویس‌های فعال در سرور است خصوصاً سرویس Active Directory که از اهمیت بالایی برخوردار است.

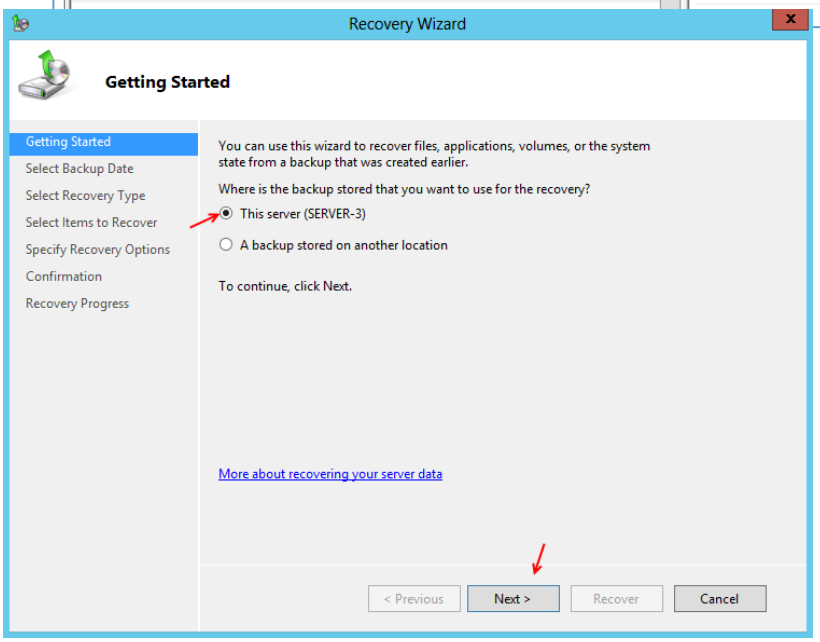
توجه داشته باشید که شما می‌توانید یک زمانبندی مشخص انجام دهید تا از سیستم خود، هر چند وقت به صورت خودکار Backup تهیه کنید.

Restore کردن Backup:

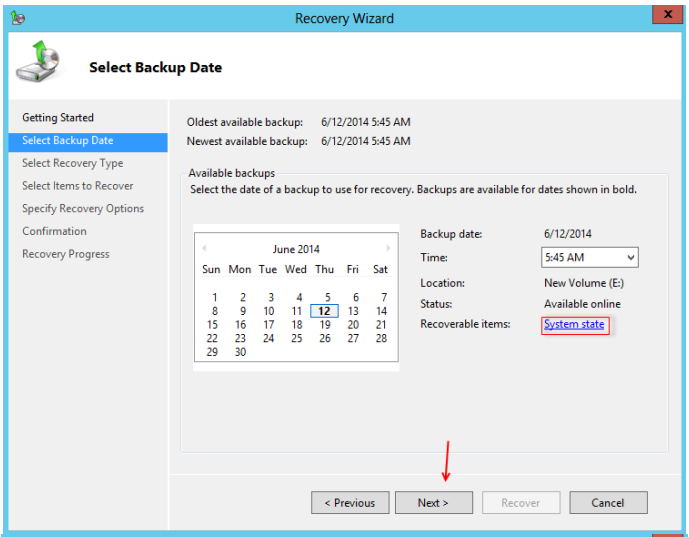
شاید، خدایی نکرده زمانی برای شما پیش خواهد آمد که تمام اطلاعات موجود در سرور خود را از دست می‌دهید، ولی نگران نیستید، چون از قبل یک Backup از کل سرویس‌ها و اطلاعات تهیه کردید و می‌توانید در این قسمت آن را به راحتی Restore کنید.



برای شروع وارد سرویس Backup شوید و بر روی ..Recover کلیک کنید.

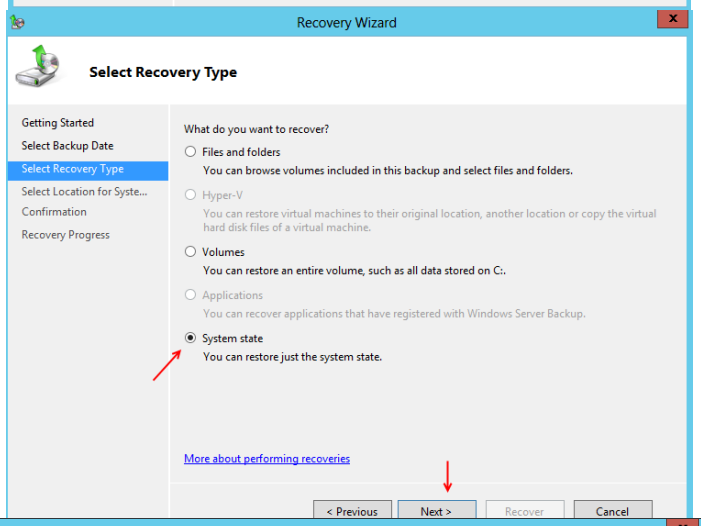


در این صفحه گزینه This Server را انتخاب کنید و بر روی next کلیک کنید.

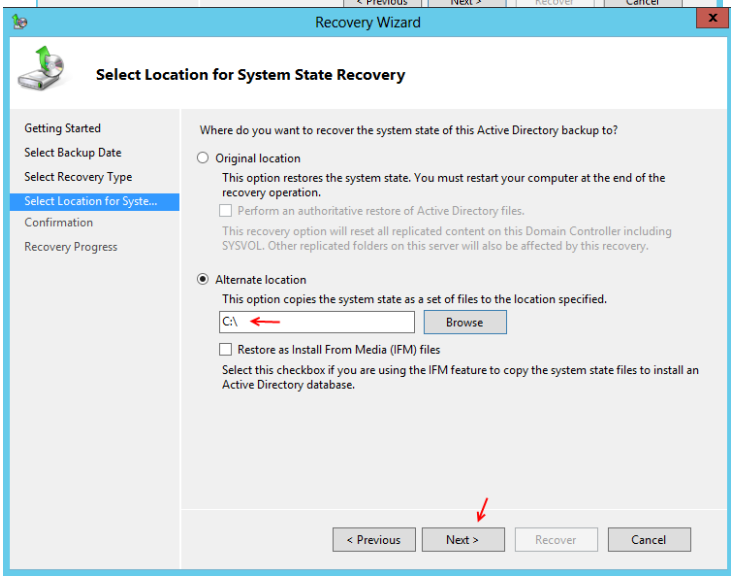


در این قسمت مشخص‌شده است که کدام قسمت می-خواهد Recover شود، اگر توجه کنید زمان آخرین Backup گرفته شده از سیستم را نشان می‌دهد.

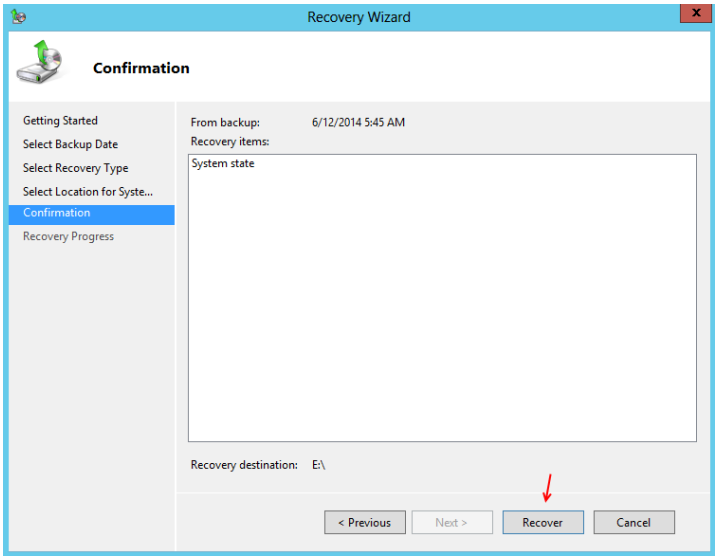
در قسمت Recoverable items نوع backup را مشخص کرده است که از کدام قسمت backup تهیه شده است.



در این قسمت گزینه System State را انتخاب کنید وبر روی Next کلیک کنید.

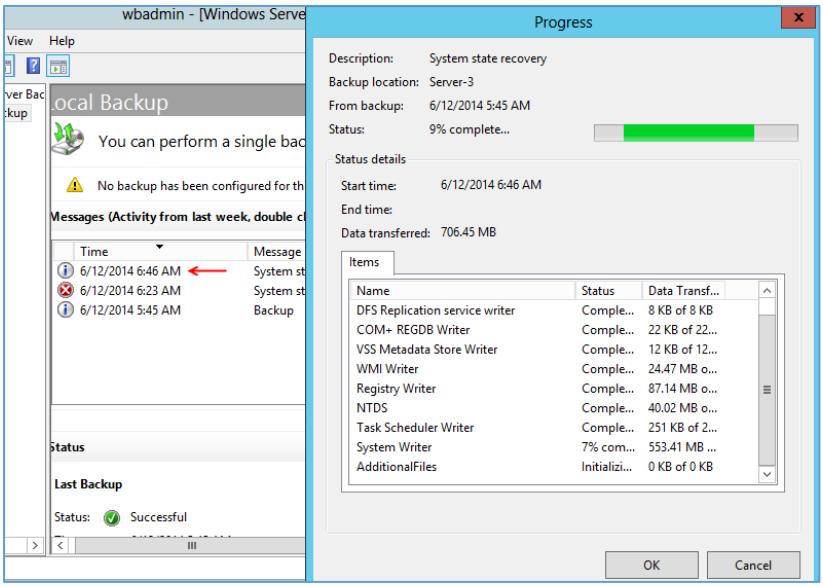


در این صفحه گزینه Alternate location را انتخاب کنید و آدرس جایی که از آن Backup تهیه کردید را وارد کنید که همیشه این نکته را در نظر داشته باشید که درایوی را انتخاب کنید که درایو سیستم است و ویندوز روی آن نصب شده است. بر روی Next کلیک کنید.



در این قسمت برای انجام عملیات بر روی Recover کلیک کنید.

در صفحه بعد از شروع کار بر روی Close کلیک کنید.



اگر از لیست موردنظر بر روی Recover دوبار کلیک کنید قسمت Progress ظاهر می‌شود که نحوه انتقال اطلاعات را در قسمت-های موردنظر مشخص کرده است.

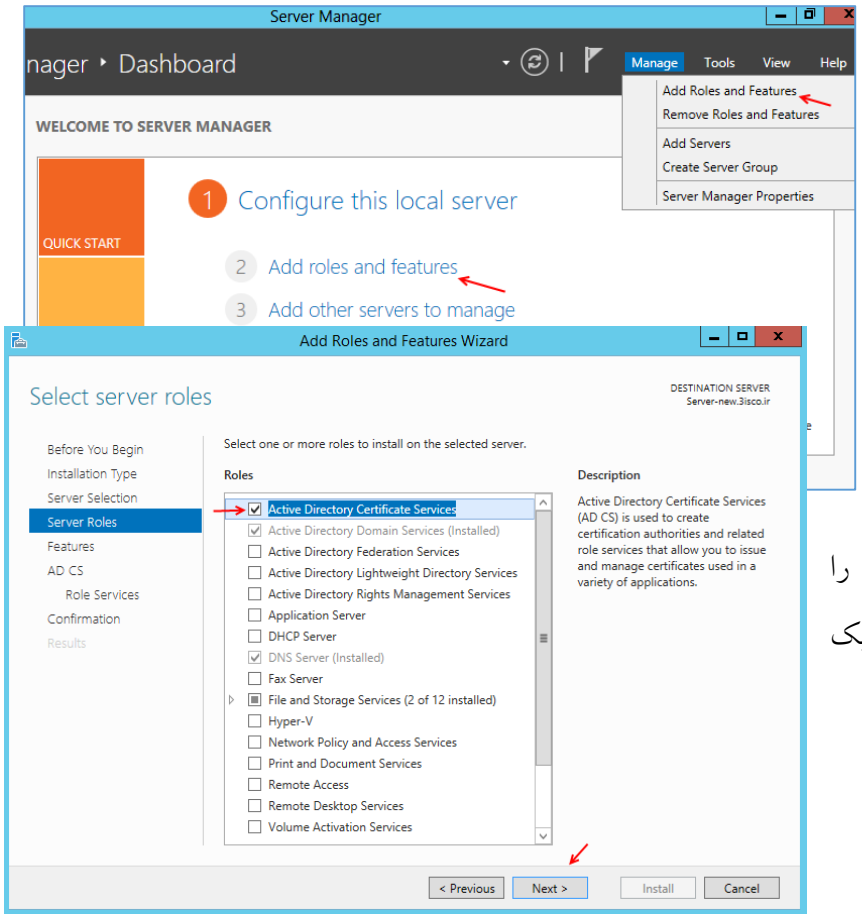
برای اینکه زمانبندی را ایجاد کنید در سرویس موردنظر از سمت راست بر روی Backup Schedul کلیک کنید در صفحه باز شده بر روی Next کلیک کنید، در صفحه بعد custom را انتخاب و گزینه system state را به مانند قبل به لیست اضافه کنید و بر روی Next کلیک کنید، در صفحه Time باید ساعت مشخص ایجاد Backup را مشخص کنید، بر روی Next کلیک کنید. در صفحه Destination Type گزینه دوم را انتخاب و بر روی Next کلیک کنیدو در صفحه بعد درایوی را برای ذخیره کردن Backup وارد کنید و در صفحه آخر بر روی Finish کلیک کنید تا در زمان مشخص‌شده این کار انجام گیرد.

نصب و راه اندازی سرویس Active Directory Certificate:

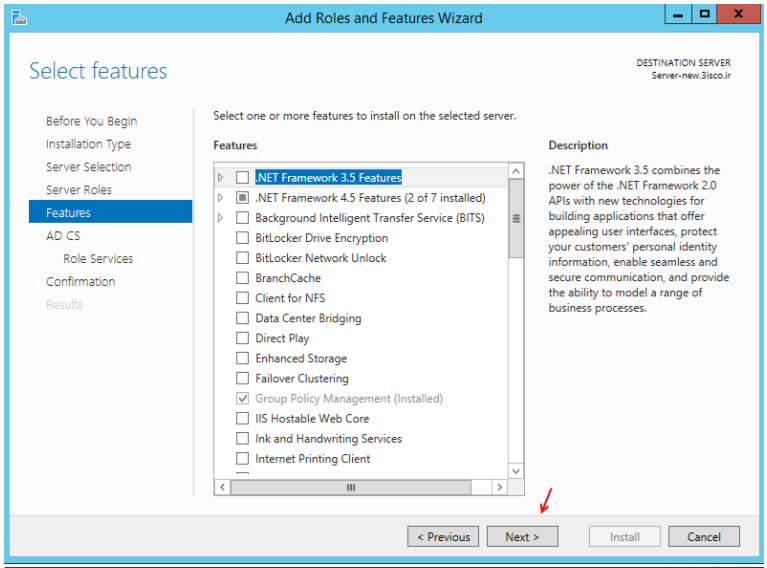
این سرویس برای صادر کردن گواهینامه‌های امنیتی در شبکه کاربرد دارد که از طریق این گواهینامه ها به کاربران مجوز دسترسی به منابع موردنظر در شبکه را می‌دهد.

به طور مثال شما زمانی که به سایت فیسبوک متصل می‌شوین این گواهینامه برای دسترسی به سایت از طریق پروتکل HTTPS فعال می‌شود، اگر زمان و تاریخ سیستم شما دقیق نباشد با مشکلات امنیتی مواجع می‌شوید و دسترسی به سایت به صورت کامل امکانپذیر نخواهد بود. شاید زمانی برای شما پیش آمده باشد که سایت فیسبوک را باز می‌کنید، همه چیز درهم است و شکل و قالب سایت تغییر کرده است که این به خاطر تنظیم نبودن ساعت و تاریخ سیستم است.

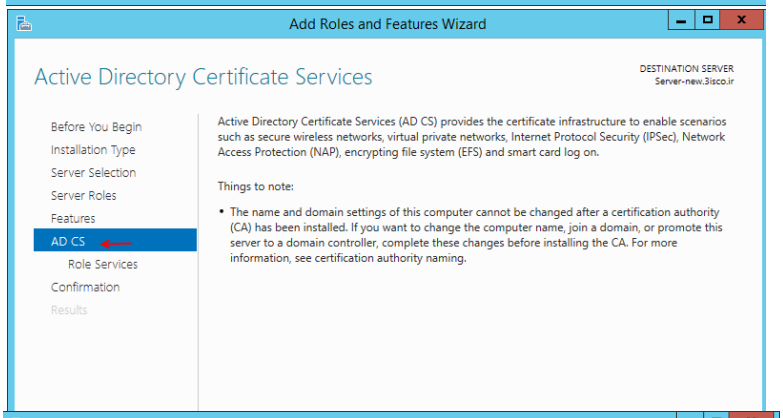
برای شروع وارد ServerManager می‌شویم و بر روی Add Roles and Features کلیک می‌کنیم.



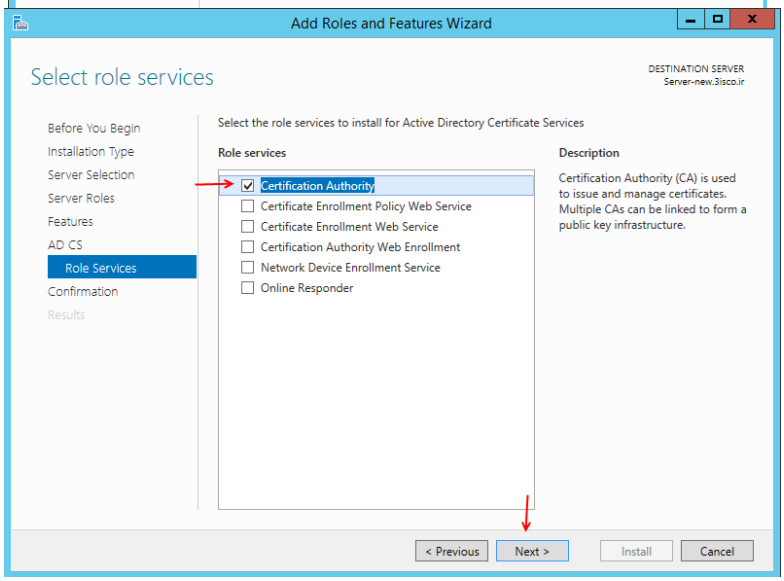
بر روی Next کلیک کنید تا به قسمت Server Roles برسید، در این قسمت از میان Roleهای موجود گزینه Active Directory Certificate Service را انتخاب و بر روی Add Features کلیک کنید و بعد بر روی Next کلیک کنید.



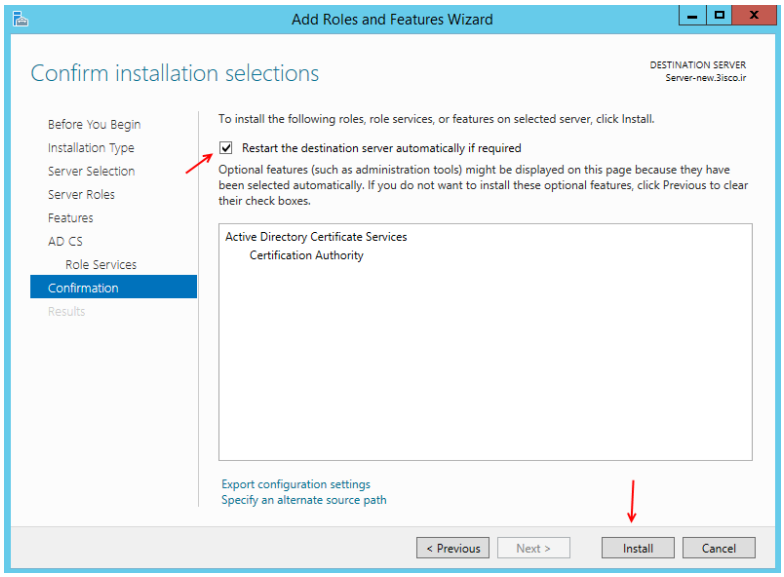
در این صفحه به گزینه‌ای دست نزنید و بر روی Next کلیک کنید.



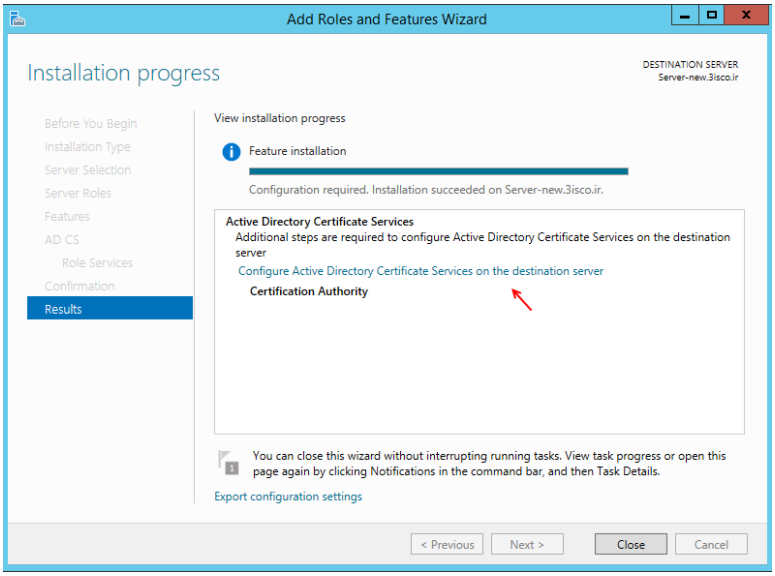
این قسمت توضیحاتی در مورد سرویس انتخاب شده است که بعد از مطالعه بر روی Next کلیک کنید.



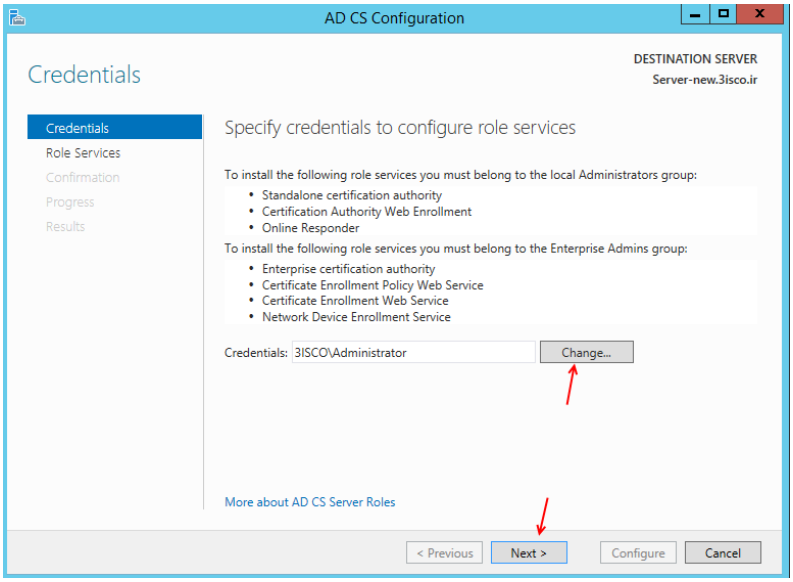
در این صفحه گزینه Certification Authority را انتخاب و بر روی Next کلیک کنید.



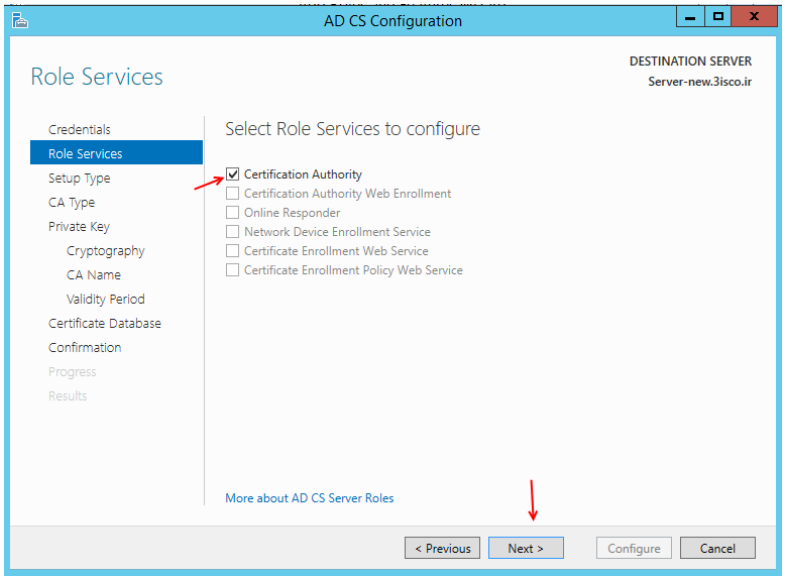
برای نصب سرویس در این صفحه بر روی install کلیک کنید.



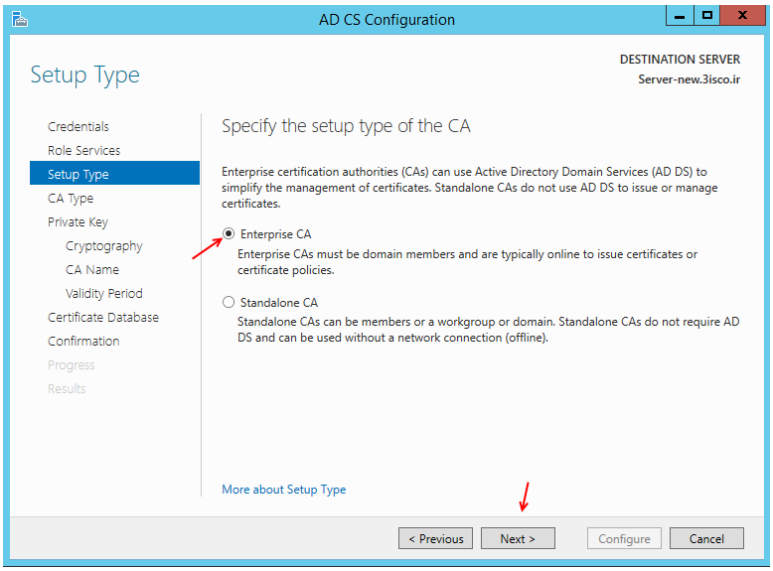
در این قسمت، بعد از نصب سرویس باید بر روی Configuration Active... کلیک کنید تا سرویس را تنظیم و فعال کنیم.



در این صفحه در قسمت Credentials باید یک کاربر با اولویت بالا که معمولاً Administrator است را وارد کنید. البته به طور پیش فرض این کاربر تعریف می‌شود، بر روی Next کلیک کنید.

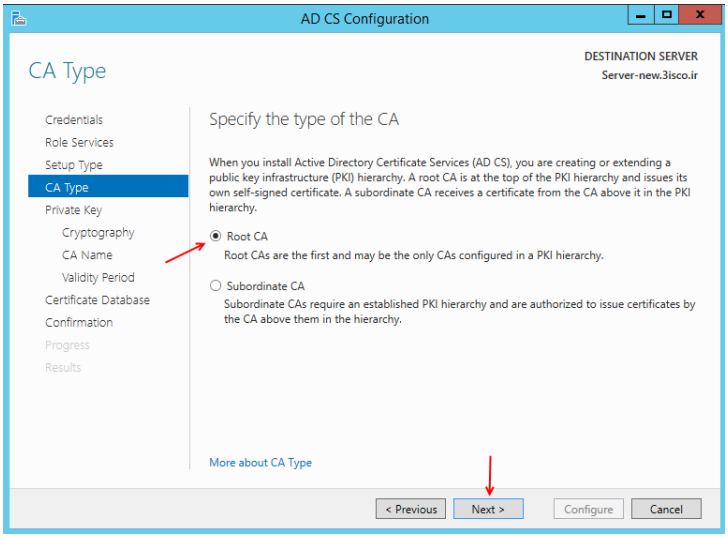


در این صفحه گزینه Certification Authority را انتخاب و بر روی Next کلیک کنید.

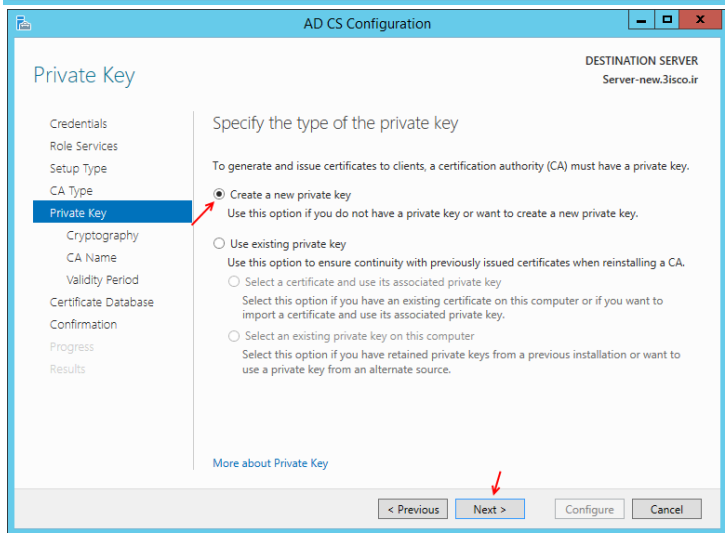


در این صفحه، گزینه Enterprise CA را انتخاب کنید، توجه داشته باشید زمانی این گزینه فعال می‌شود که سرویس Active Directory Domain فعال شده باشد، وگرنه باید گزینه standalone CA را انتخاب کنید.

بر روی Next کلیک کنید

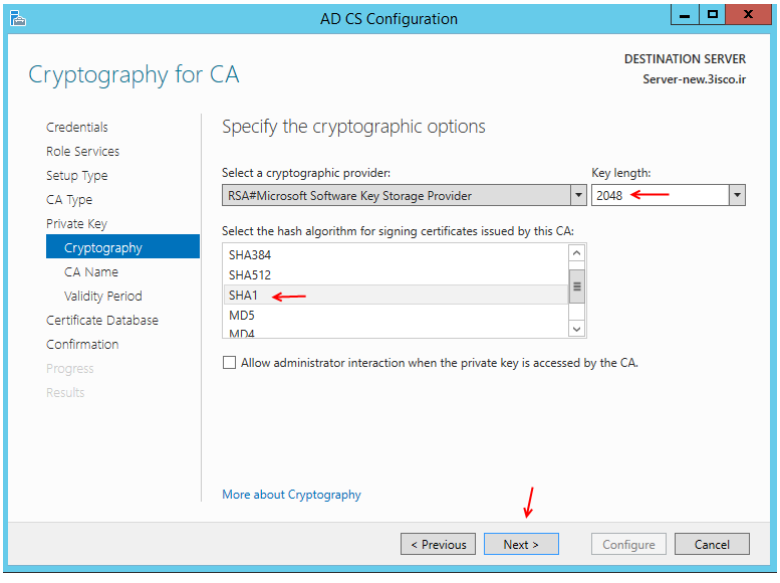


در این صفحه گزینه Root CA را انتخاب کنید چون این سرور زیر مجموعه سرور دیگری یا سرویس Certificate دیگری نیست و برای اولین بار این سرویس نصب می‌شود به خاطر همین باید به عنوان Root در نظر گرفته شود. بر روی Next کلیک کنید.

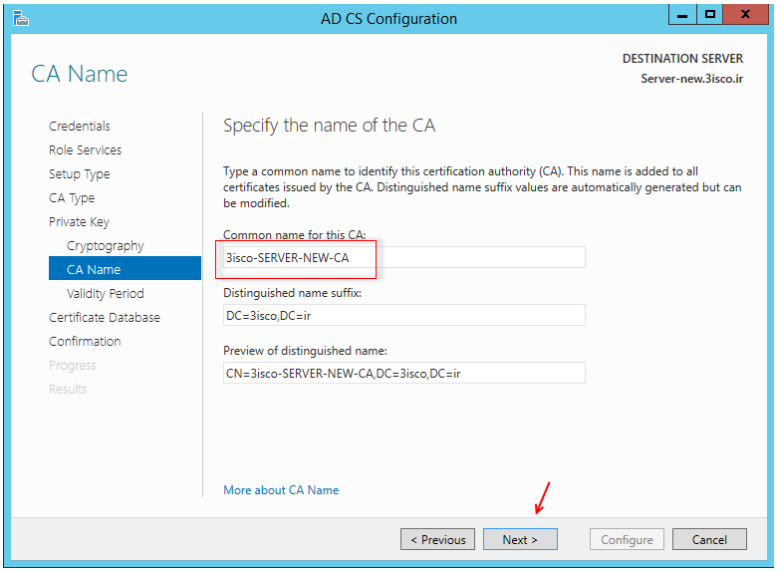


در این صفحه باید یک دسته کلید ایجاد کنیم، اگر برای اولین بار است باید گزینه اول را انتخاب کنید و یا اگر از قبل ایجاد کرده‌اید گزینه دوم را انتخاب کنید.

بر روی Next کلیک کنید.

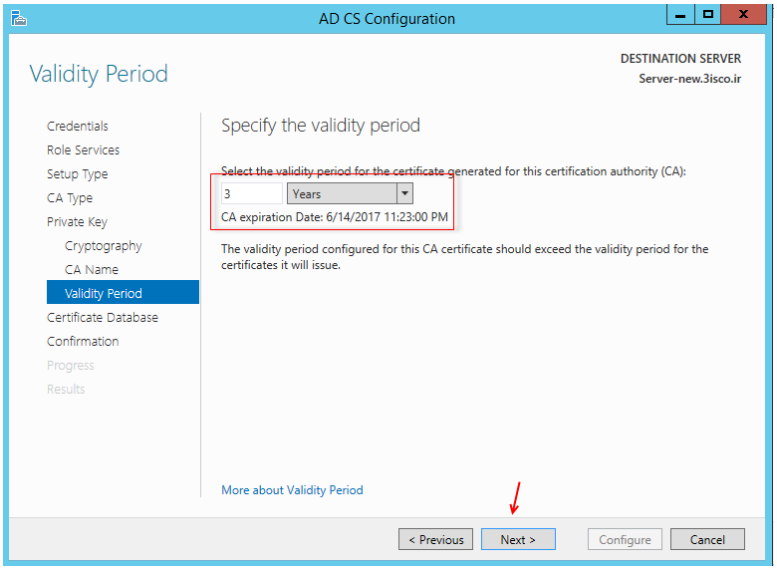


در این صفحه، باید الگوریتم رمزنگاری را برای این سرویس انتخاب کنید، توجه داشته باشید که الگوریتم SHA1 بهترین انتخاب می‌باشد و به صورت پیش‌فرض انتخاب شده است و طول کلید هم 2048 انتخاب شده است که انتخاب خوبی است، بر روی Next کلیک کنید.



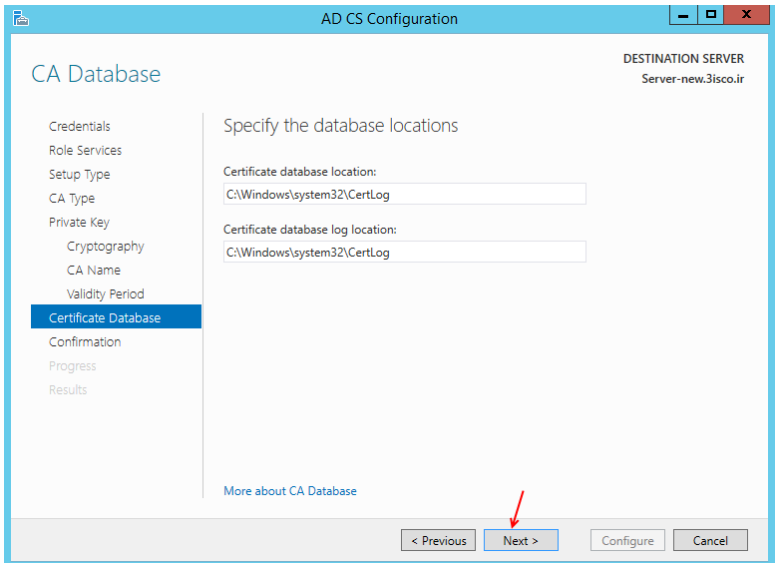
در این صفحه سعی کنید نوشته قسمت Common name for this CA را به خاطر داشته باشید، شاید در آینده به کار شما بیاید.

بر روی Next کلیک کنید.



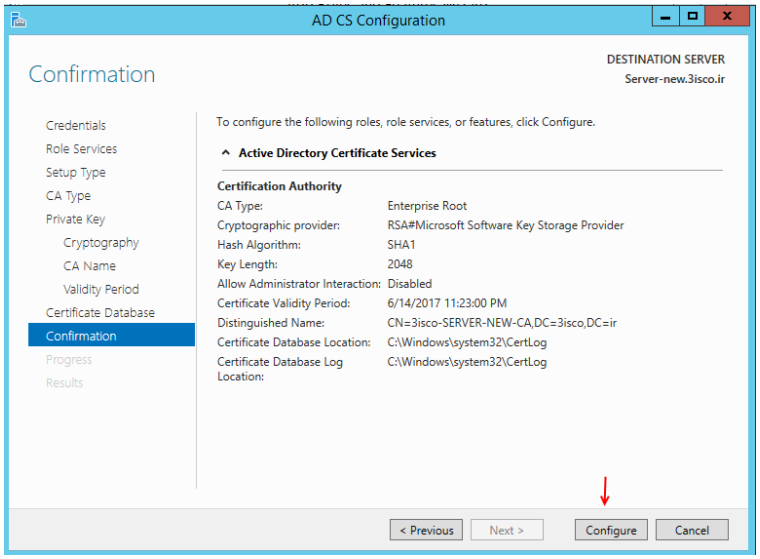
در این قسمت، باید مدت اعتبار گواهینامه خود را وارد کنید که می‌تواند بر طبق روز، هفته، ماه، سال باشد که در این قسمت 3 سال وارد شده است.

بر روی next کلیک کنید.



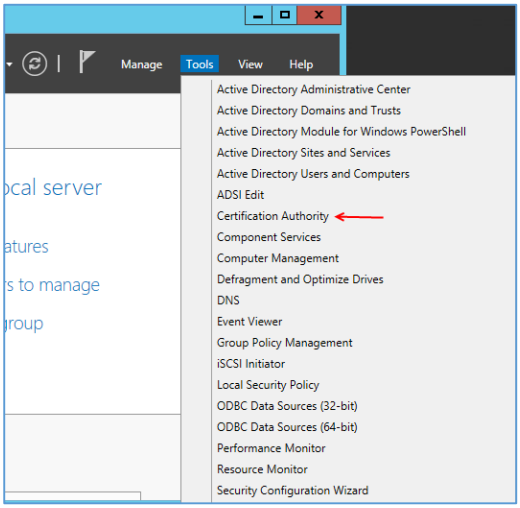
در این قسمت باید محل ذخیره سازی دیتابیس این سرویس را وارد کنید که سعی کنید بر روی پیش فرض قرار دهید.

بر روی Next کلیک کنید.

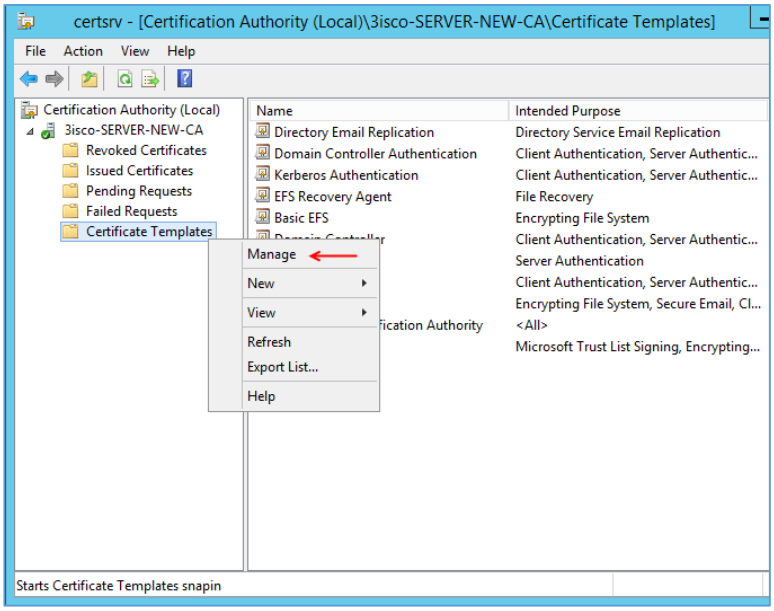


در این قسمت، اگر اطلاعات لیست شده را قبول دارید بر روی configure کلیک کنید تا تنظیمات اعمال شود.

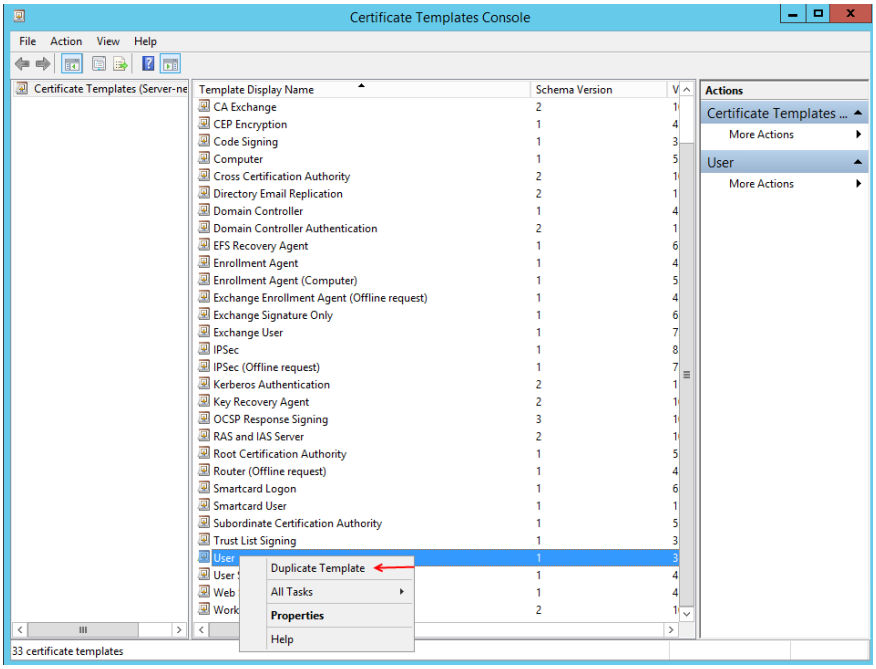
در آخر بر روی Close کلیک کنید و سیستم را Restart کنید.



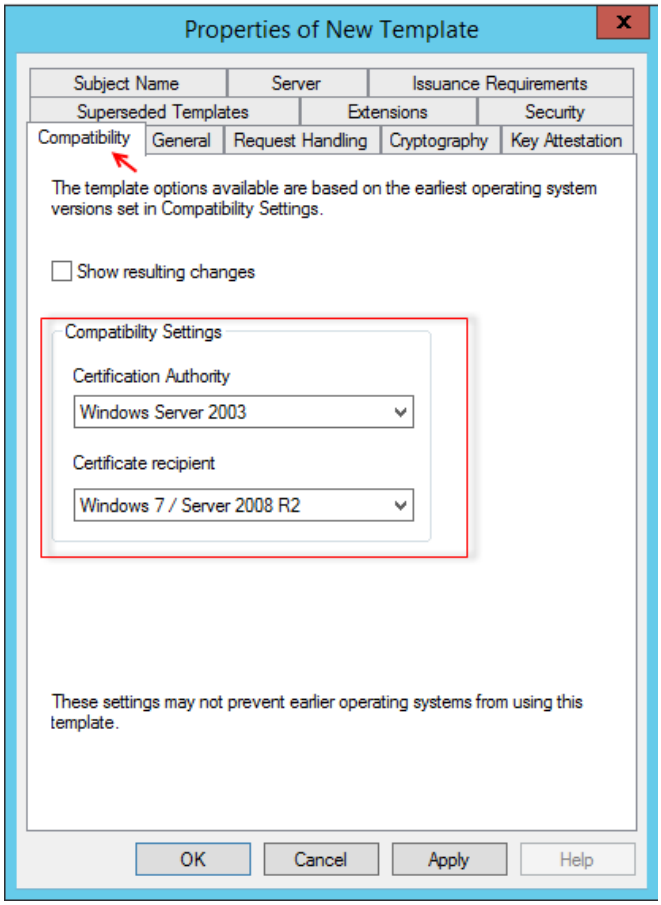
بعد از اجرا شدن سرویس، می‌توانید وارد Search شوید و سرویس موردنظر را اجرا کنید و یا می‌توانید از طریق Server Manager و از منوی Tools بر روی Certification Authority کلیک کنید.



در شکل روبرو سرویس موردنظر را مشاهده می‌کنید، برای شروع باید وارد قسمت Certificate Templates شویم، این قسمت یک سری گواهینامه‌های امنیتی آماده را برای قسمت‌های مختلف ویندوز از قبل آماده کرده است، در این قسمت می‌خواهیم یک قالب برای کاربران خود ایجاد کنیم، برای همین کاربر روی Certificate Templates کلیک راست کنید و گزینه Manage را انتخاب کنید.

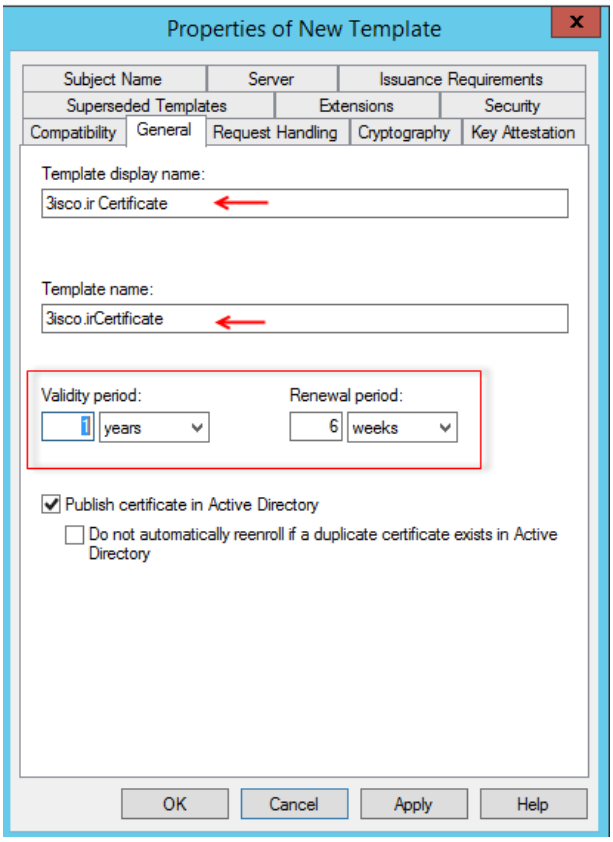


در این صفحه انواع قالب‌های مختلف در زمینه‌های مختلف را مشاهده می-کنید، از بین آن‌ها بر روی User کلیک راست کنید و گزینه dublicate Template را انتخاب کنید. توجه داشته باشید این قالب‌ها یک سری تنظیماتی هستند که از قبل انجام‌شده است، که مثلاً برای استفاده کاربران از قالب Template استفاده می‌کنیم.



در این صفحه یعنی تب Compatibility گزینه‌های برای انتخاب حداقل ویندوزهایی که می‌خواهند از این گواهینامه امنیتی استفاده کنند وجود دارد که می‌توانید بسته به سازمان خود که از چه ویندوزهایی استفاده می‌کند، گزینه موردنظر را انتخاب کنید.

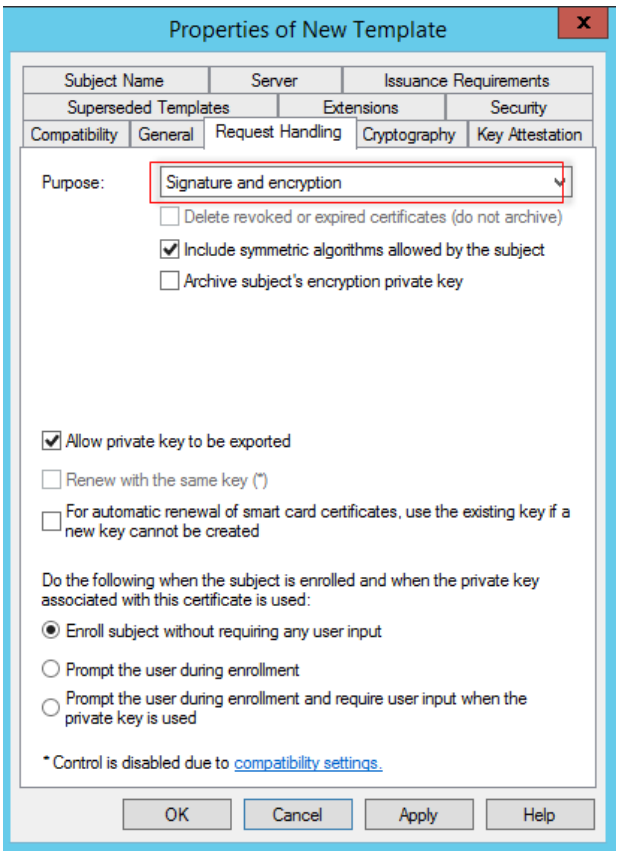
بر روی تب General کلیک کنید.



در تب General باید در قسمت Template Display Name نام موردنظر خود را وارد کنید، با واردکردن آن در قسمت Template name به‌صورت خودکار این اسم نوشته می‌شود.

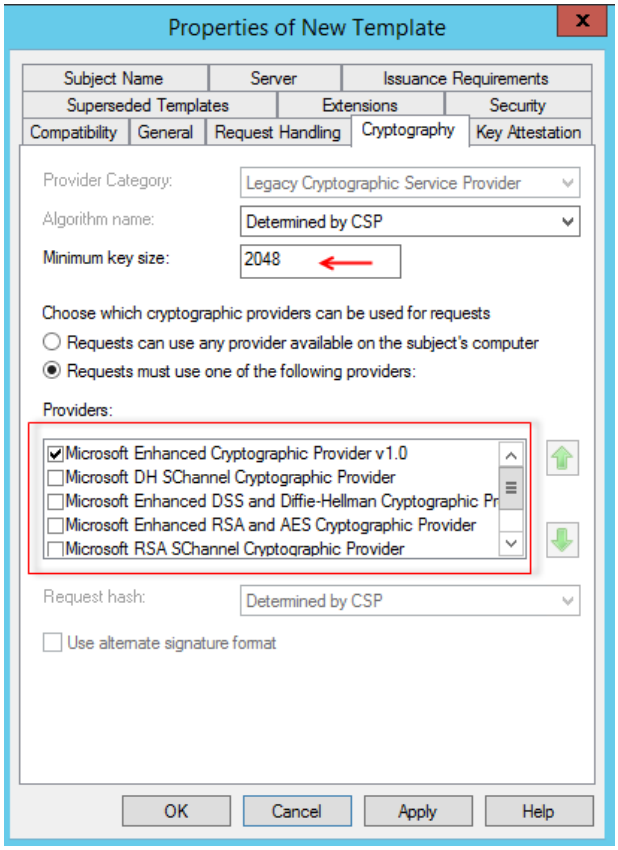
در قسمت Validity Period باید حداکثر اعتبار این گواهینامه را مشخص کنید که در این قسمت 1 سال انتخاب‌شده است و در قسمت Renewal Period باید مقدار زمان هشدار تا رسیدن به‌اندازه Validity Period را مشخص کنید که در اینجا 6 هفته مشخص‌شده است.

بر روی تب Request Handling کلیک کنید.



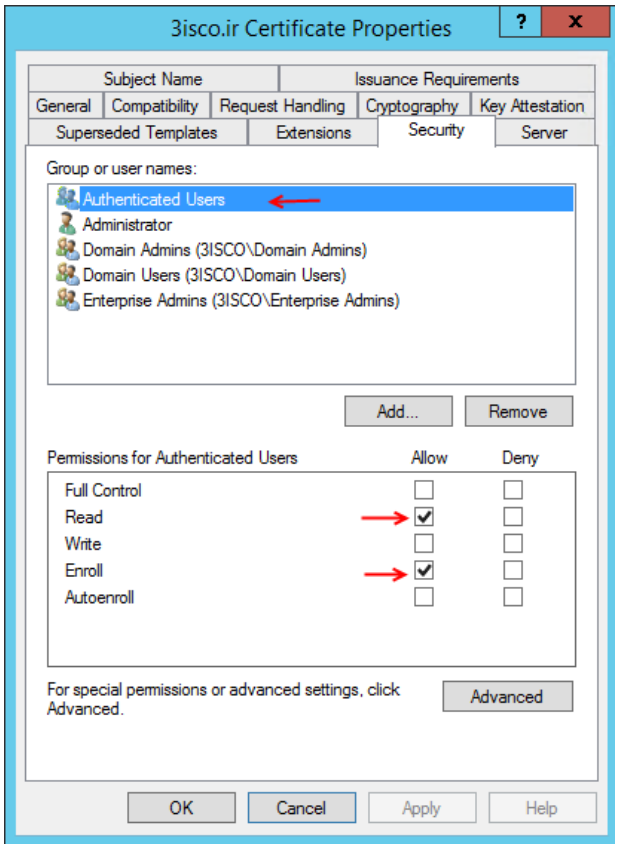
در تب Request Handling می‌توانید در قسمت Purpose نوع گواهینامه خود را مشخص کنید، مثلاً اگر در سازمان خود از کارت‌های هوشمند استفاده می‌کنید گزینه Smart Card را انتخاب کنید و یا گزینه دیگر را برای سازمان خود انتخاب کنید البته در حالت پیش‌فرض گزینه رمزنگاری و امضاء دیجیتال انتخاب‌شده است.

اگر تیک گزینه Allow Private Key to be Exported را بردارید، به‌هیچ‌عنوان نمی‌توانید کار Export را انجام دهید.

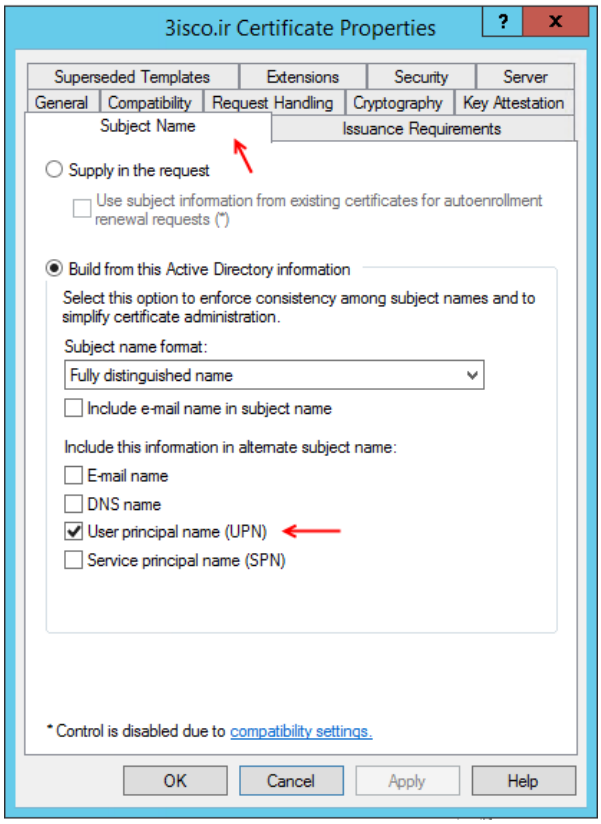


در تب Cryptography می‌توانید، نوع Provider گواهینامه موردنظر را تغییر دهید و طول کلید را تغییر دهید، هر چه طول کلید بیشتر باشد، امنیت کار افزایش پیدا می‌کند، هرچند عدد 2048 هم‌عددی بزرگی است.

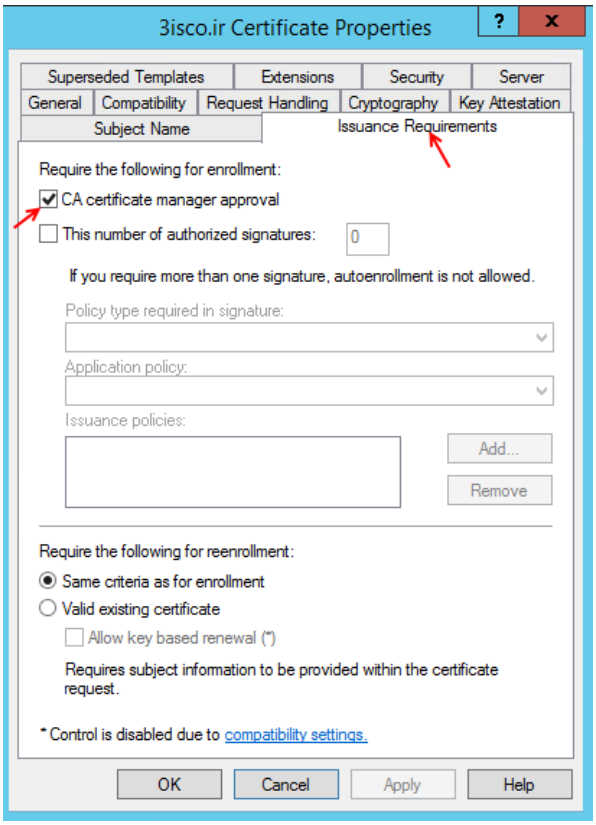
برای ادامه کاربر روی Ok کلیک کنید تا قالب موردنظر ایجاد شود.



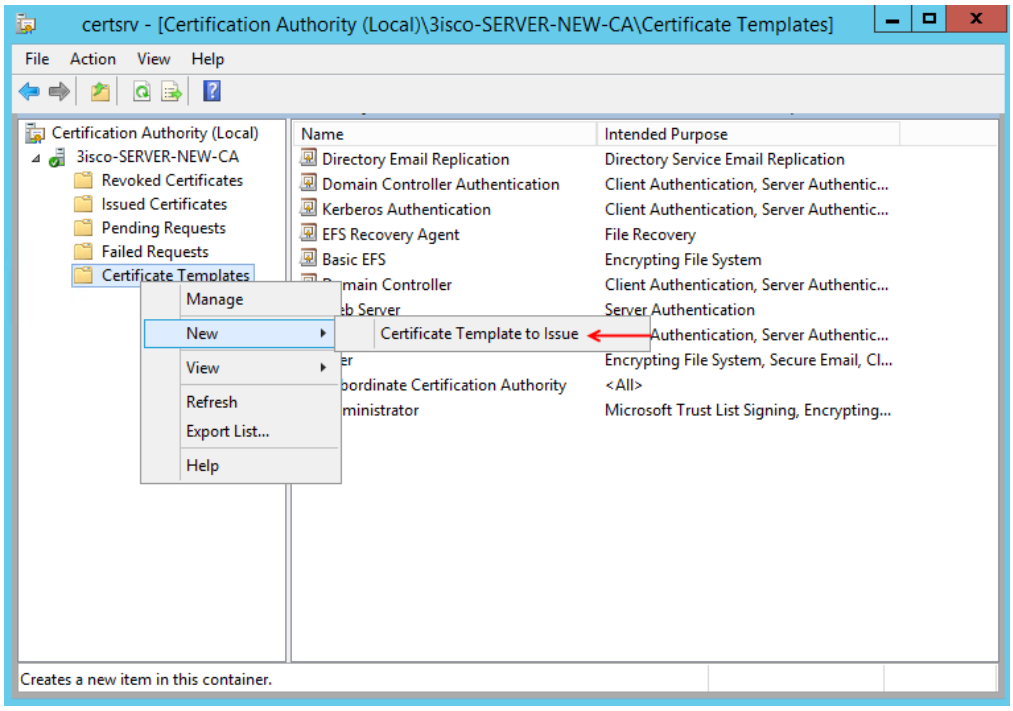
در تب Security از لیست موردنظر گروه Authenticated Users را انتخاب کنید و در قسمت Permissions گزینه‌های Read و Enroll را انتخاب کنید.



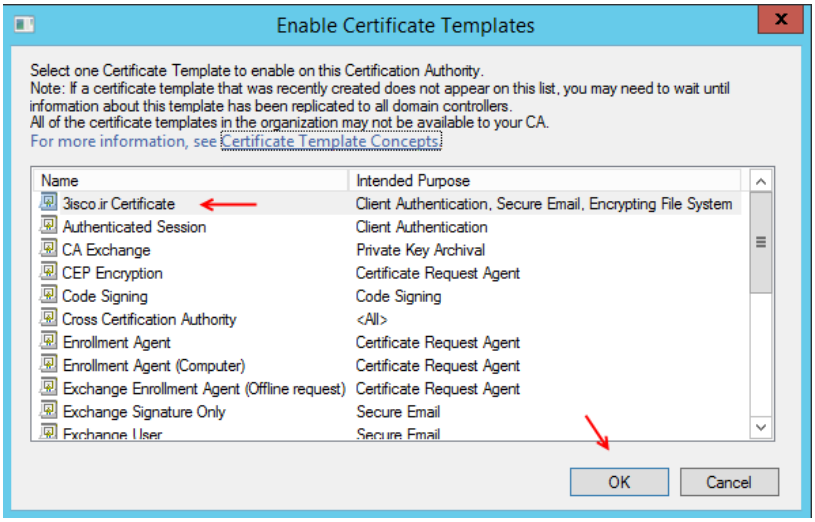
در تب Subject Name فقط تیک گزینه UPN را که با فلش مشخص‌شده انتخاب کنید، البته اگر در سرور خود از ایمیل استفاده می‌کنید می‌توانید گزینه E-mail name را انتخاب کنید.



در تب Issuance Requirements گزینه Cacertificate manager approval را انتخاب کنید و بر روی ok کلیک کنید تا تنظیمات اعمال شود.

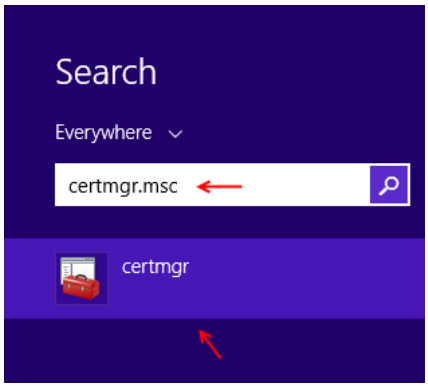


بعد از ایجاد قالب موردنظر وارد سرویس Certificate شوید و از سمت چپ بر روی Certificate Template کلیک راست کنید و از قسمت New گزینه Certificate Template to issue را انتخاب کنید.



در این صفحه باید قالبی را که در قسمت قبل ایجاد کردیم را انتخاب کنیم که در اینجا باید 3isco.ir Certificate را انتخاب کنید. اگر به قسمت Intended Purpose توجه کنید، می‌توانید مشاهده کنید که این قالب در چه جاهایی از ویندوز استفاده می‌شود.

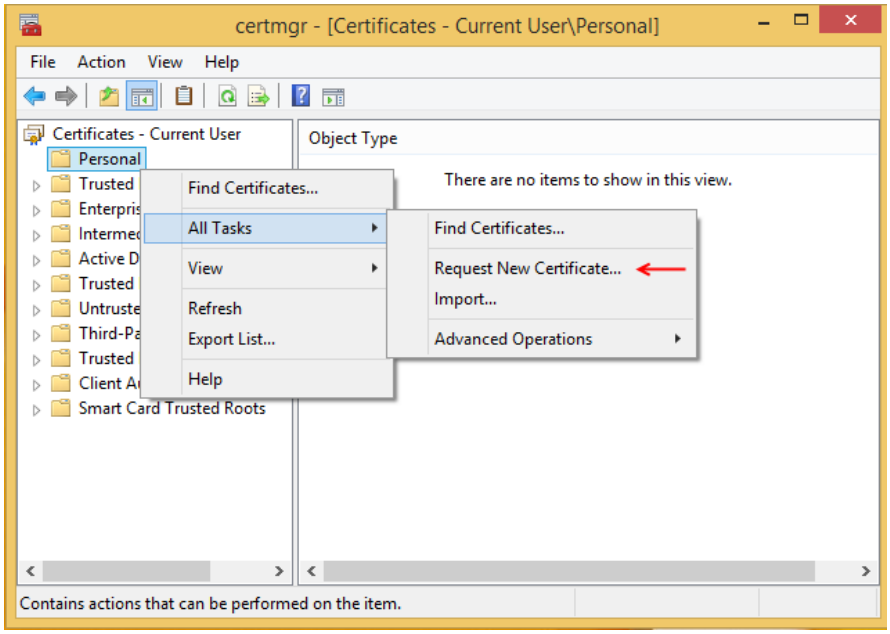
بر روی ok کلیک کنید تا قالب موردنظر به لیست اضافه شود.



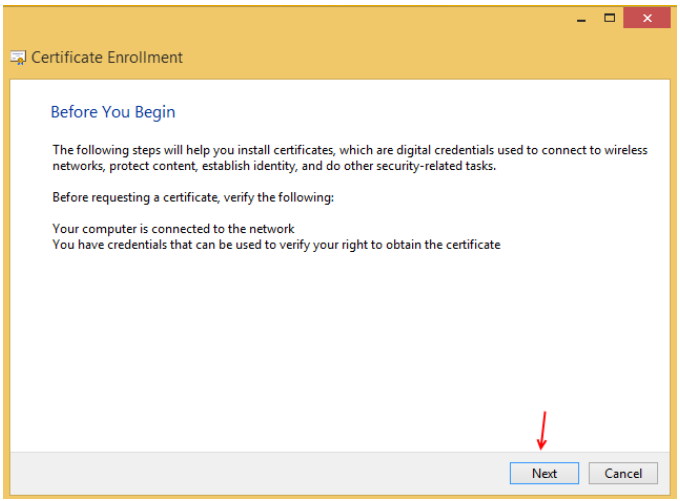
بعدازاین کار حالا می‌خواهیم این گواهینامه را برای کلاینتی در شبکه تعریف کنیم، این کلاینت دارای ویندوز8 است و زیرمجموعه دومین 3isco.ir می‌باشد.

وارد ویندوز 8 می‌شویم و در قسمت Search گزینه Certmgr.msc را اجرا می‌کنیم تا کنسول مدیریتی Certificate اجرا شود.

همان‌طور مشاهده می‌کنید سرویس Certificate اجراشده است، البته می‌توانیم از طریق کنسول مدیریتی MMC به این سرویس دست پیدا کنیم، راه‌های مختلفی برای معرفی Certificate موردنظر در این سرویس وجود دارد که در این قسمت بر روی Personal کلیک راست کنید و از قسمت All Tasks گزینه Request New Certificate را انتخاب کنید تا از طریق Active Directory به گواهینامه موردنظر خود که در قسمت قبل بانام 3isco.ir Certificate ایجاد کردیم دست پیدا کنیم.

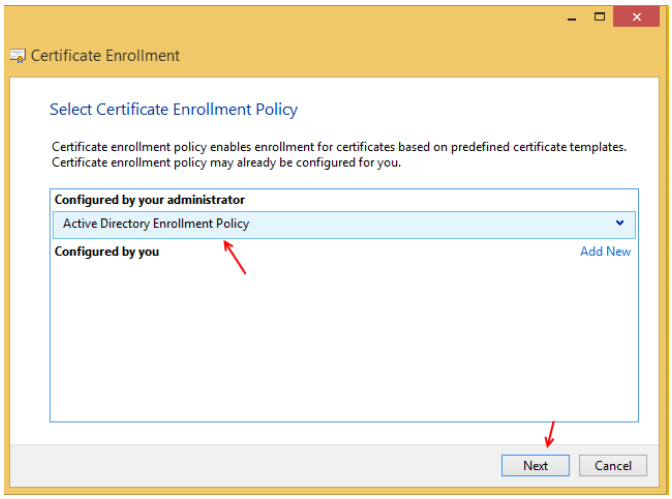


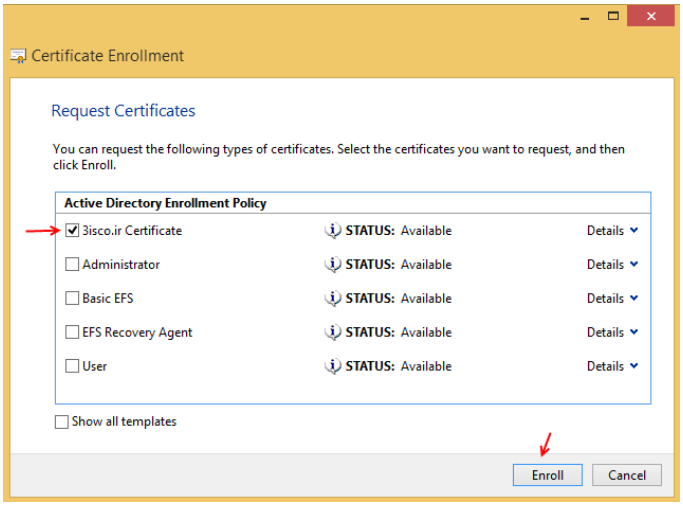
در این صفحه بر روی Next کلیک کنید.



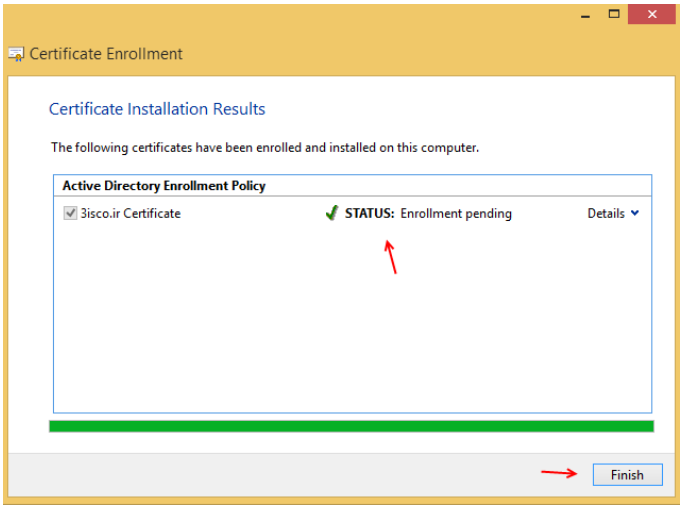
در این قسمت، همان‌طور که مشاهده می‌کنید سرویس Active Directory به‌صورت خودکار شناسایی‌شده است که این به خاطر این است که این کلاینت عضو دومین 3isco.ir شده است.

بر روی Next کلیک کنید.



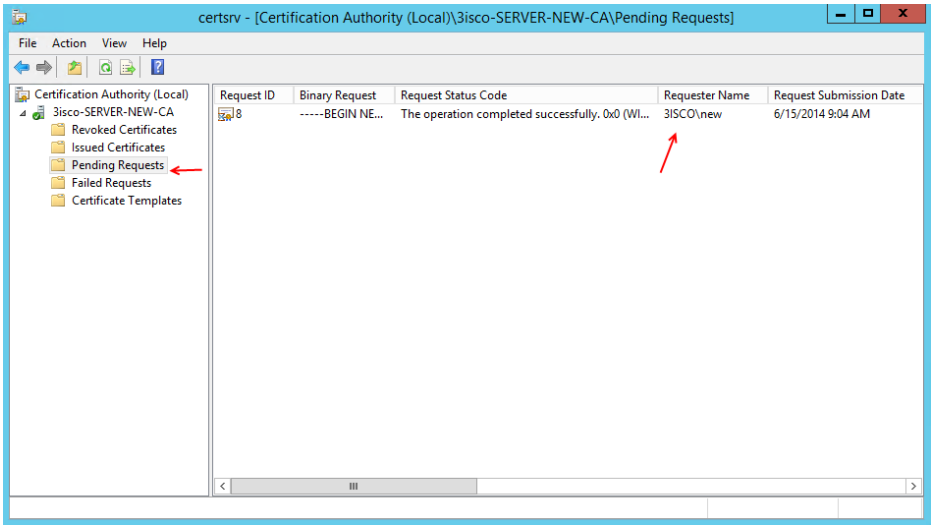


اگر به‌دقت به این صفحه توجه کنید قالبی را که قبلاً ایجاد کرده بودیم در این قسمت وجود دارد، آن را انتخاب کنید وبر روی Enroll کلیک کنید.

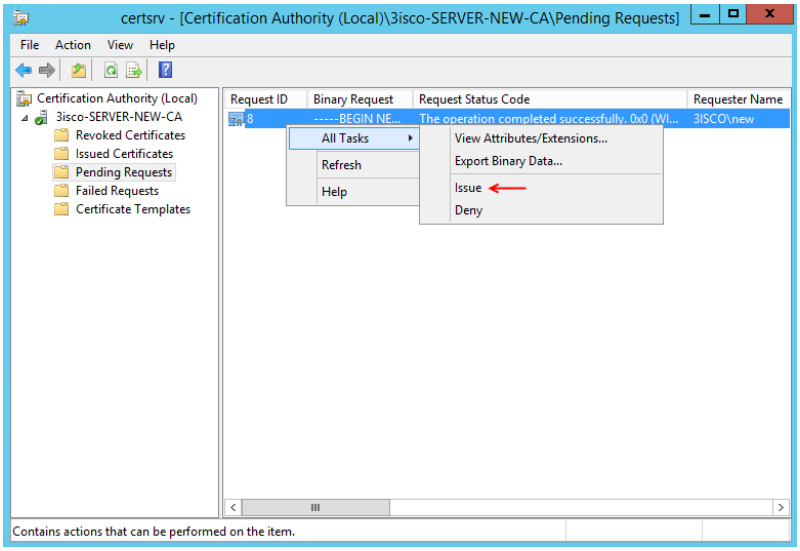


همان‌طور که مشاهده می‌کنید، قالب موردنظر با موفقیت به لیست اضافه‌شده است.

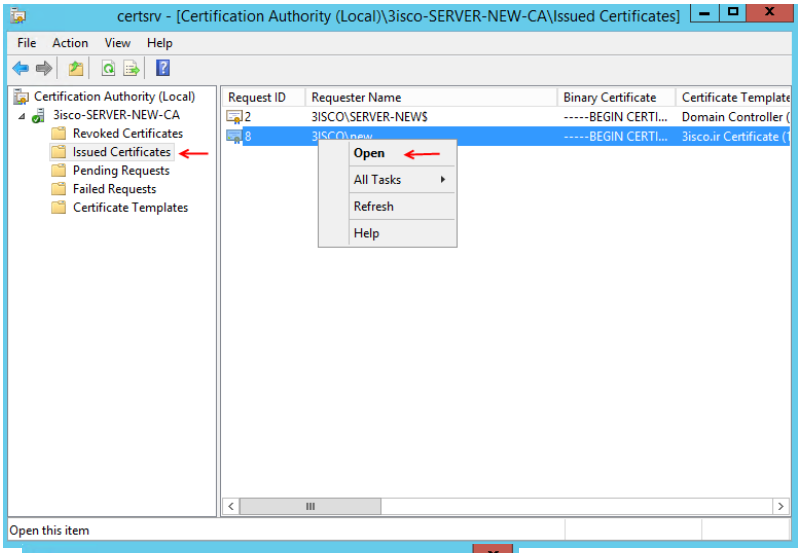
بر روی Finish کلیک کنید.



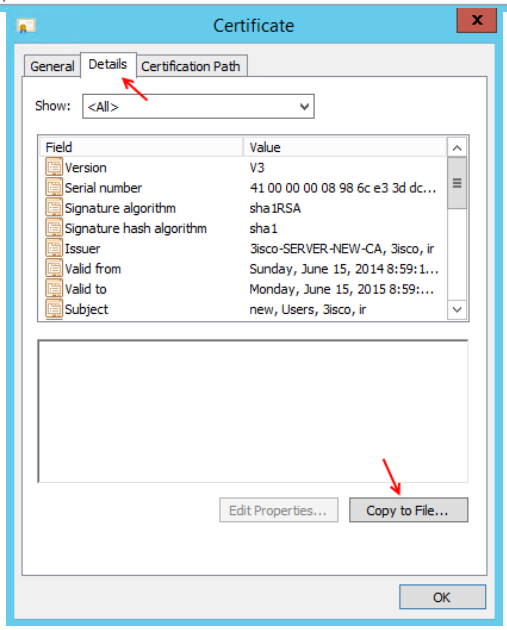
بعد از انجام عملیات بالا وارد سرور اصلی شوید و سرویس Certificate را اجرا کنید، اگر از سمت چپ بر روی Pending Requests کلیک کنیم، مشاهده خواهید کرد که یک درخواست از طرف کاربری بانام New که در شکل هم مشاهده می‌کنید، به همراه تاریخ و ساعت آن ثبت‌شده است.



در ادامه اگر این درخواست را به‌عنوان مدیر شبکه قبول دارید بر روی آن کلیک راست کنید و از قسمت All Tasks گزینه Issue را انتخاب کنید که بعدازاین انتخاب درخواست موردنظر تأیید و به قسمت Issued Certificates منتقل می‌شود. درصورتی‌که این درخواست را قبول ندارید می‌توانید گزینه Deny را انتخاب کنید.



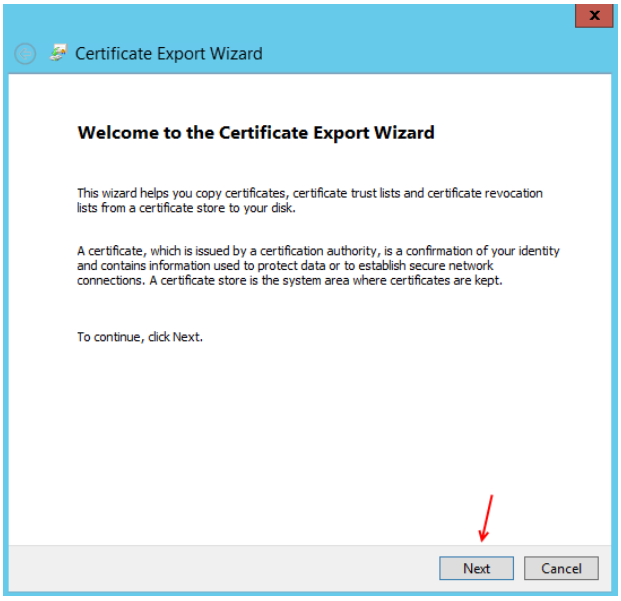
بعد از انجام کار بالا وارد قسمت Issued Certificates می‌شویم و همان‌طور در شکل هم مشاهده می‌کنید درخواست موردنظر به این قسمت منتقل‌شده است، بر روی آن کلیک راست کنید و Open را انتخاب کنید.



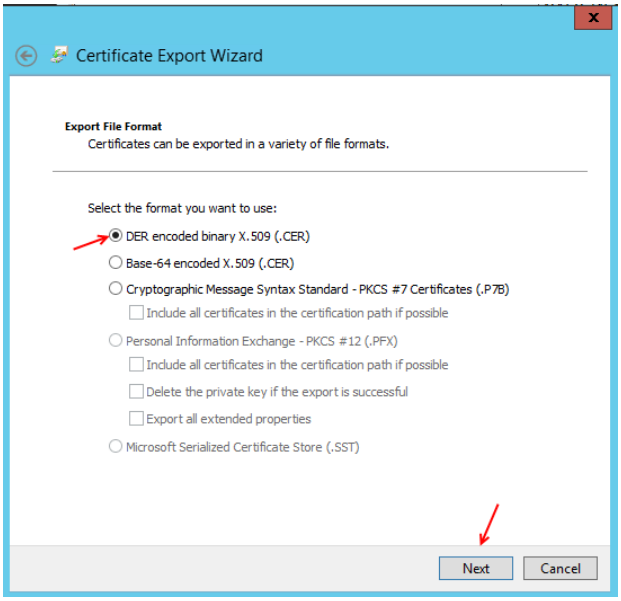
در این صفحه می‌خواهیم یک کپی از این گواهینامه امنیتی را برای کاربر موردنظر که درخواست کرده بود بفرستیم تا کاربر موردنظر آن را در سرویس Certificate خود Import کند.

در این صفحه وارد تب Details شوید و بر روی Copy to File کلیک کنید.

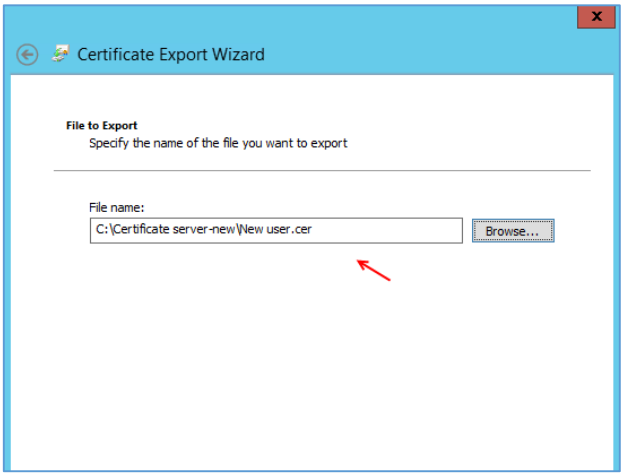
در این صفحه بر روی Next کلیک کنید.

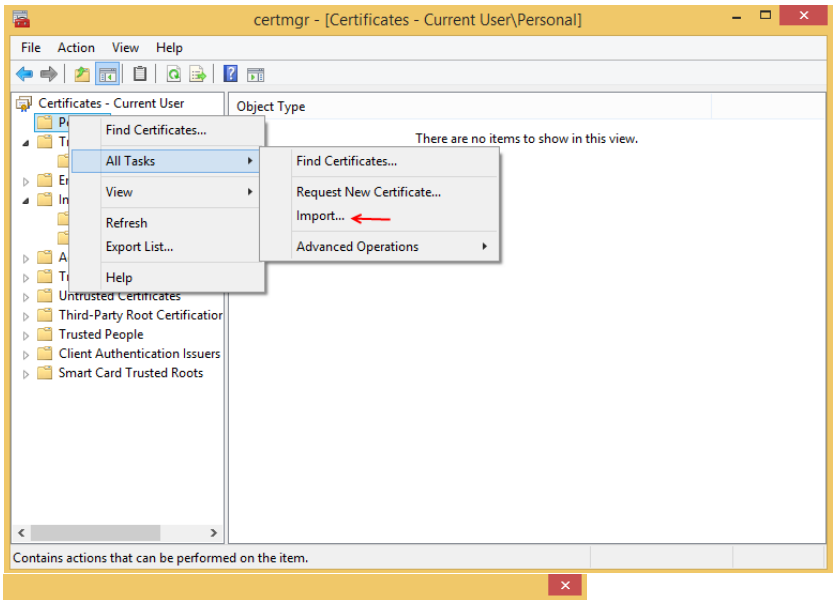


در این بخش، گزینه DER را انتخاب کنید و بر روی Next کلیک کنید.

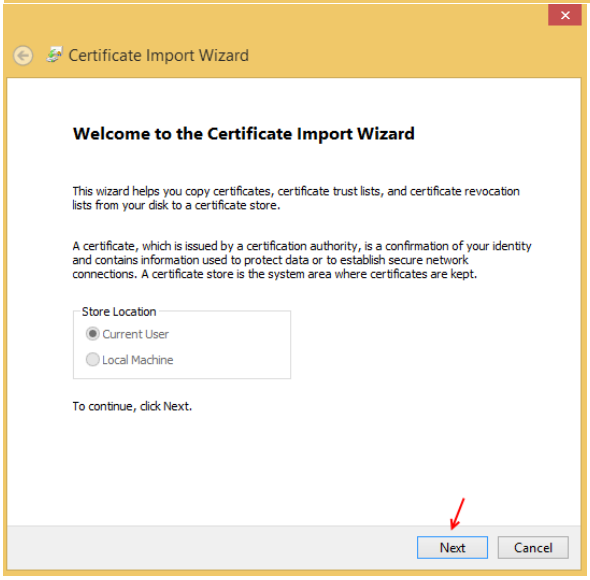


در این بخش محل ذخیره‌سازی گواهینامه موردنظر را مشخص کنید و نام آن را هم در آخر وارد کنید، توجه داشته باشید پوشه‌ای که این گواهینامه‌ها در آن قرار دارد Share شود تا بتوان از طریق شبکه به آن دسترسی داشت. بر روی Next کلیک کنید و در صفحه آخر هم بر روی Finish کلیک کنید.

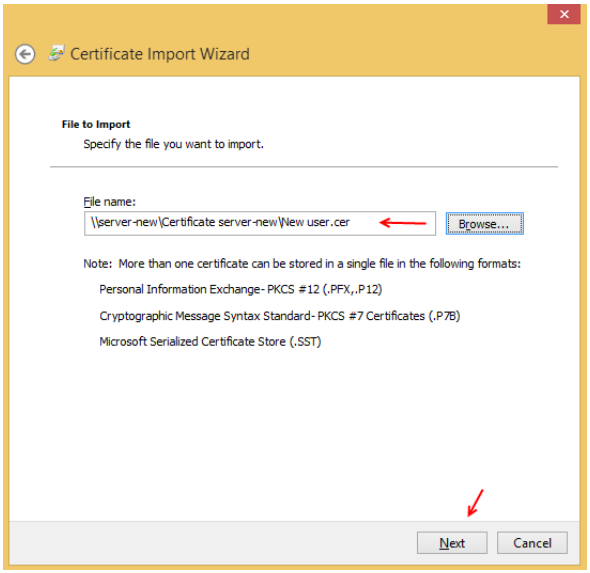




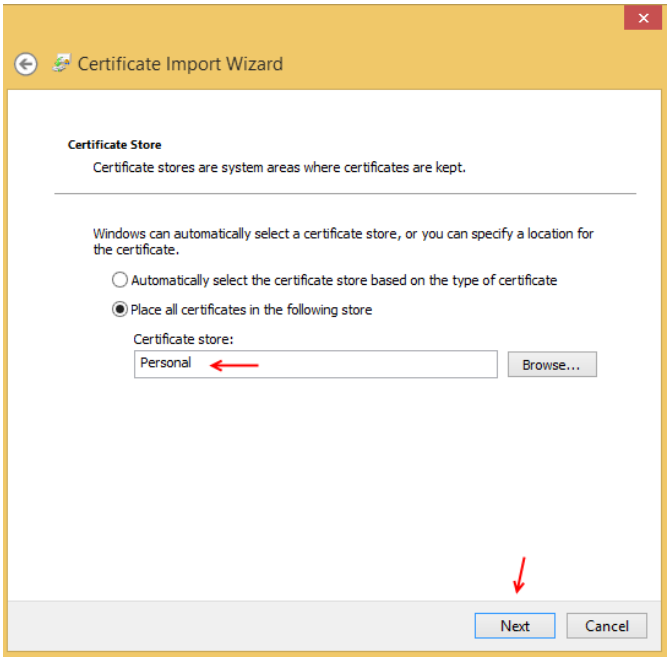
بعد از انجام کارهای قسمت قبل دوباره وارد ویندوز 8 شوید و سرویس Certificate را به‌مانند قبل اجرا کنید و از سمت چپ بر روی Personal کلیک راست کنید و از قسمت All Tasks گزینه Import را انتخاب کنید.



در این صفحه بر روی next کلیک کنید.



در این صفحه، آدرس گواهینامه امنیتی را که در بخش قبل در سرور اصلی ذخیره و Share کردیم را وارد کنید و بر روی Next کلیک کنید.



در این قسمت شما می‌توانید محل قرارگیری گواهینامه امنیتی را با کلیک بر روی Browse تغییر دهید.

بر روی Next کلیک کنید و در صفحه آخر بر روی Finish کلیک کنید.

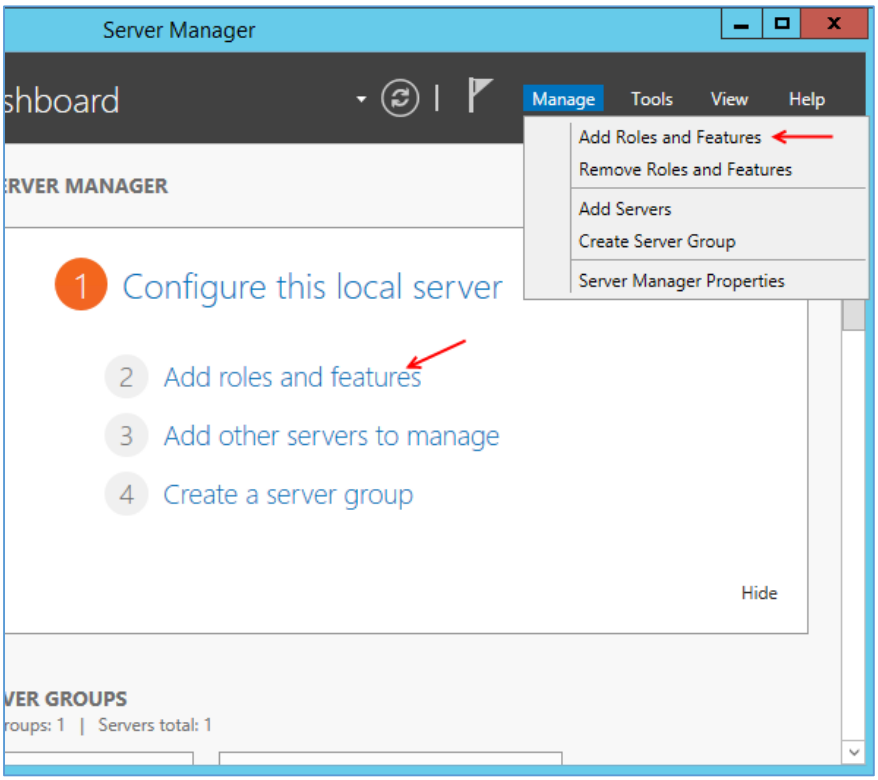
با این کار کلاینت موردنظر دارای گواهینامه امنیتی شده که این گواهینامه از طریق سرور اصلی برای این کلاینت صادرشده است.

مشکلات خود را در این بخش از طریق ایمیل با من در میان بگذارید.

کار با سرویس Active Directory Right Management:

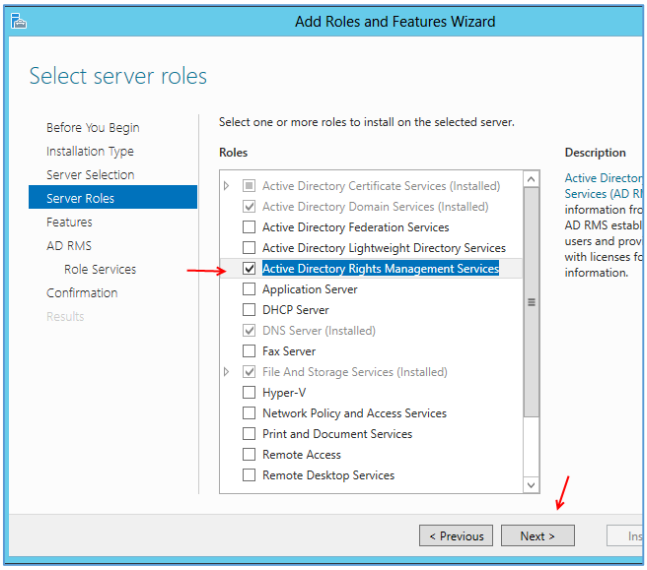
از اولویت‌های یک سازمان حفظ امنیت اسناد و مدارک موجود آن است که هرکسی نتواند به اسناد موردنظر دسترسی داشته باشد، یکی از راه‌کارهایی که شرکت مایکروسافت در اختیار مدیران شبکه قرار داده است استفاده از سرویس Active Directory Right Management است که قوی‌ترین سرویس در حفظ امنیت اسناد و مدارکی است که توسط نرم‌افزارهای مختلف ایجاد می‌شود، این سرویس با ایجاد امنیت روی هر یک از فایل‌ها مانند Word و یا Excel.. به کسانی که عضو زیرمجموعه سازمان نیستند اجازه دسترسی نمی‌دهد، این سرویس از نرم‌افزارهای زیر پشتیبانی می‌کند:

- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office 2013
- Adobe Acrobat

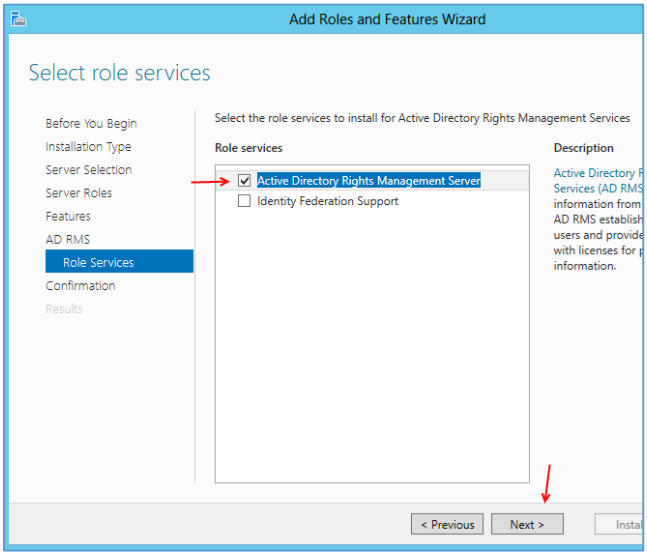


برای شروع وارد Server Manager شوید و بر روی Add Roles and Features کلیک کنید.

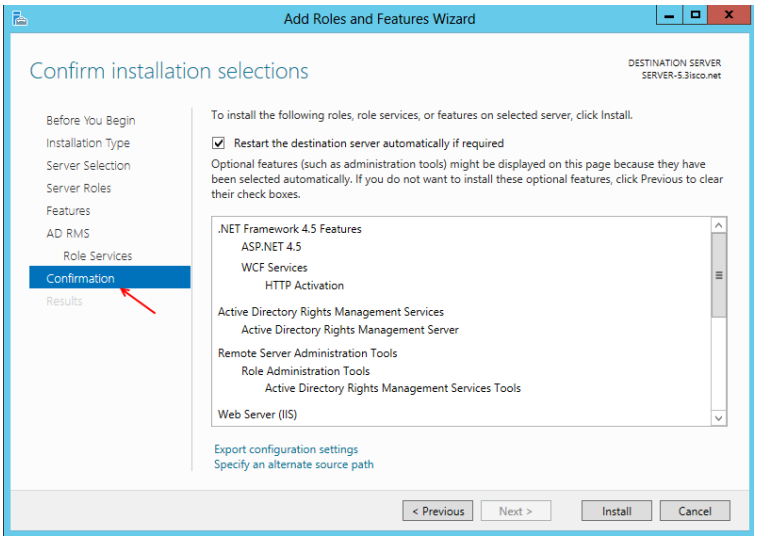
همان‌طور که مشاهده می‌کنید از دو طریق می‌توانید به این گزینه دسترسی داشته باشید.



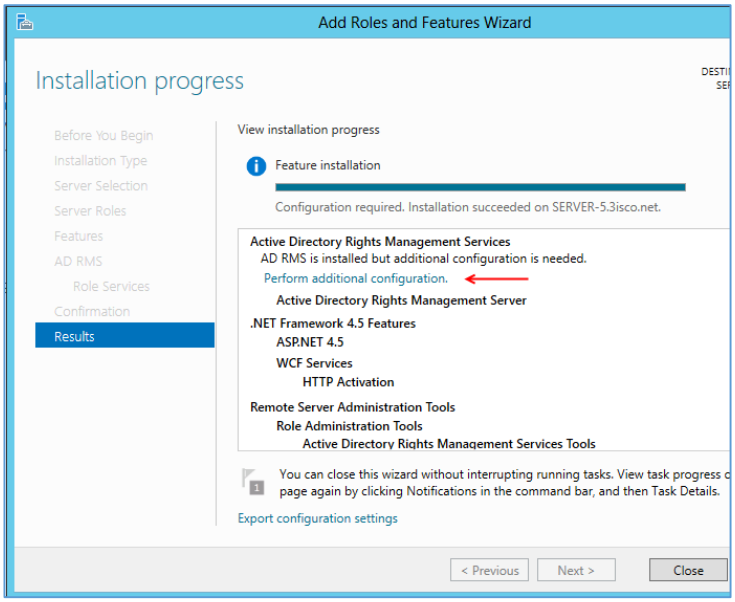
بر روی Next کلیک کنید تا به قسمت Server Roles برسید در این قسمت از بین Roles های موجود گزینه Active Directory Rights Management Services را انتخاب کنید و بر روی Next کلیک کنید.



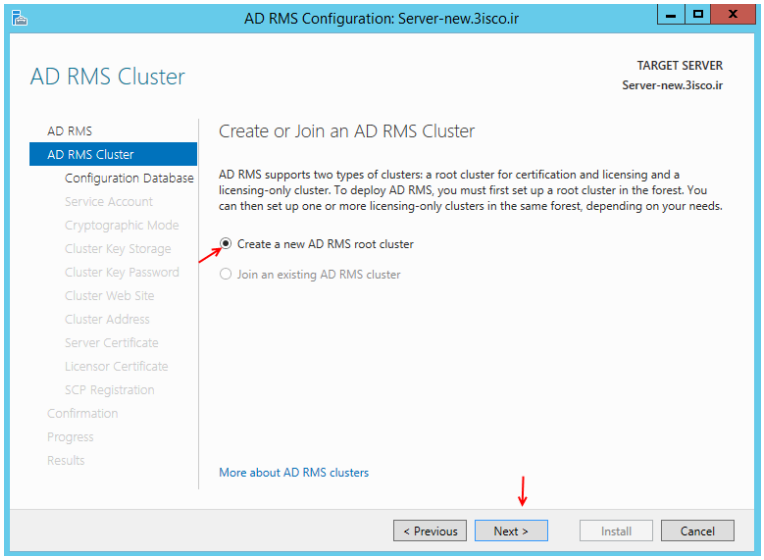
بر روی Next کلیک کنید تا به قسمت Role Services برسید در این قسمت گزینه اول را انتخاب و بر روی Next کلیک کنید.



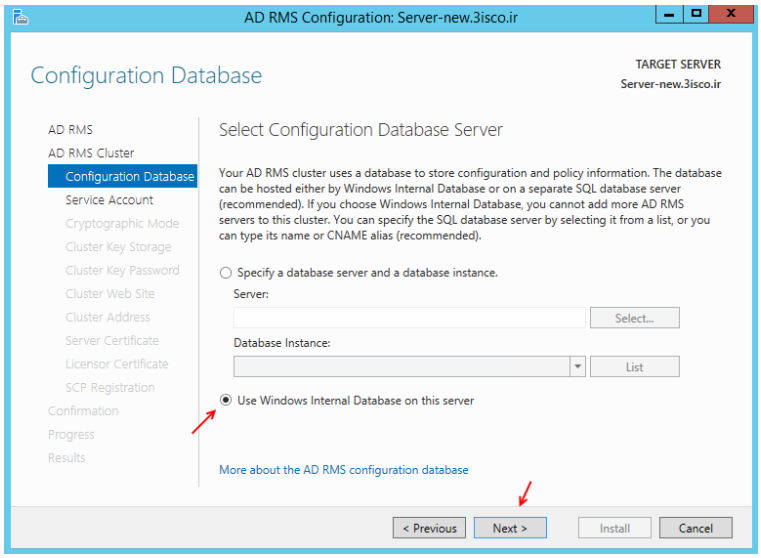
در این قسمت بر روی Install کلیک کنید تا کار نصب سرویس آغاز شود.



بعد از نصب سرویس به‌مانند شکل روبرو بر روی perform additional Configuration کلیک کنید تا ادامه تنظیمات این سرویس ر انجام دهیم.

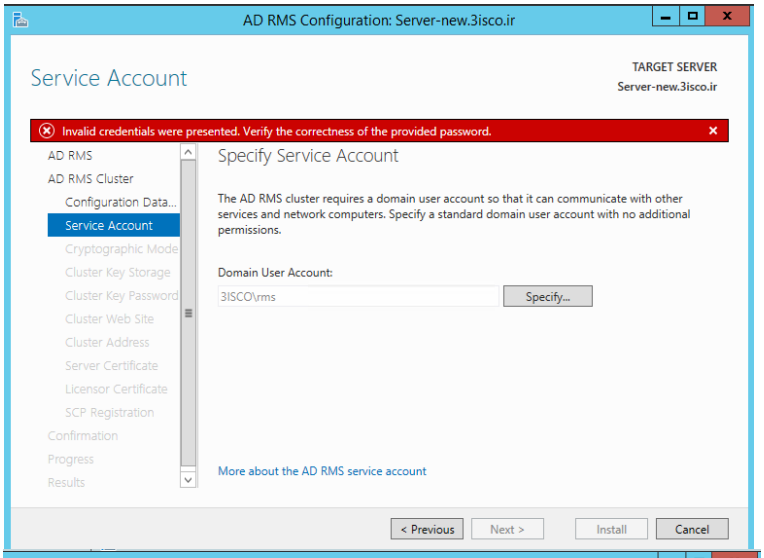


در صفحه AD RMS بر روی Next کلیک کنید تا به این صفحه مراجعه کنید، در این قسمت چون از قبل هیچ سرویس RMS دیگری وجود نداشت، فقط گزینه اول فعال است و گزینه دوم غیرفعال پس گزینه اول را انتخاب و بر روی Next کلیک کنید.



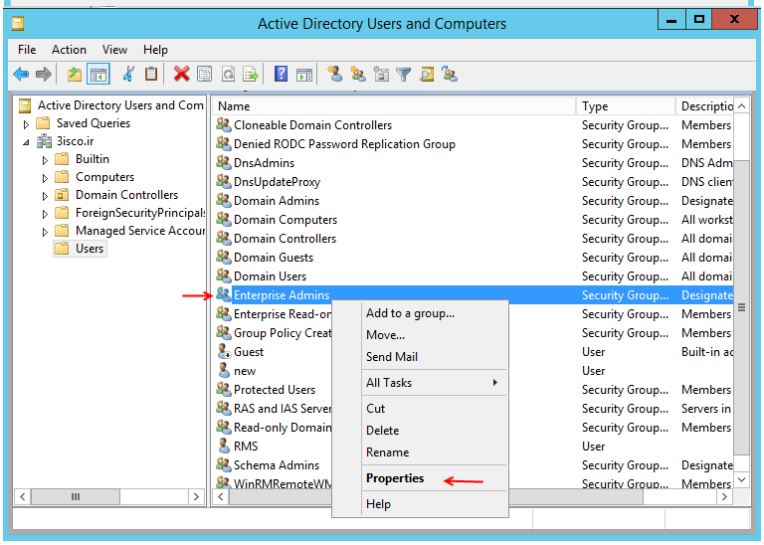
در این قسمت، باید یک Database را معرفی کنیم تا اطلاعات روی Database موردنظر ذخیره شود، چون Database خاصی در دسترس نیست گزینه Use Windows internal Database را انتخاب کنید، این‌یک Database آماده‌شده از قبل در ویندوز است.

بر روی Next کلیک کنید.

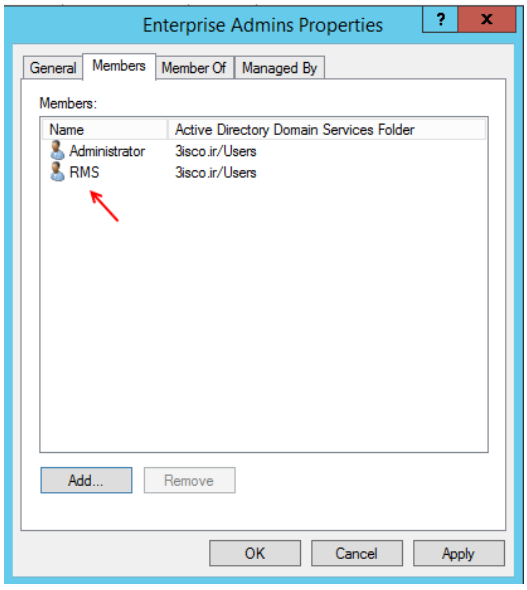


در این قسمت باید یک کاربر معرفی کنیم، ولی با معرفی یک کاربر با خطا روبرو مواجه شدیم که مشکل از اینجاست که کاربر موردنظر حتماً باید عضو گروه Enterprise Admins باشد.

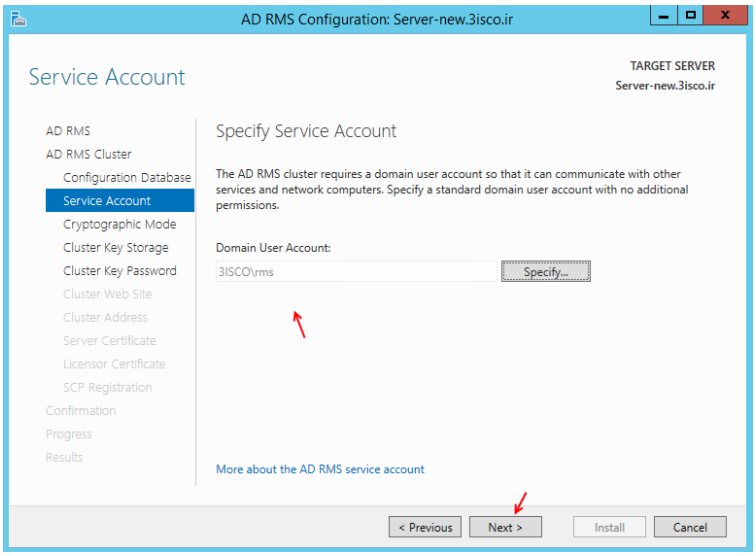
برای معرفی کاربر به گروه موردنظر باید از سرویس Active Directory Users and Computers استفاده کنیم.



وارد سرویس Active Directory Users and Computers می‌شویم و از سمت چپ گزینه User را انتخاب می‌کنیم و بعد از لیست موردنظر بر روی گروه Enterprise Admins کلیک راست می‌کنیم و گزینه Properties را انتخاب می‌کنیم.

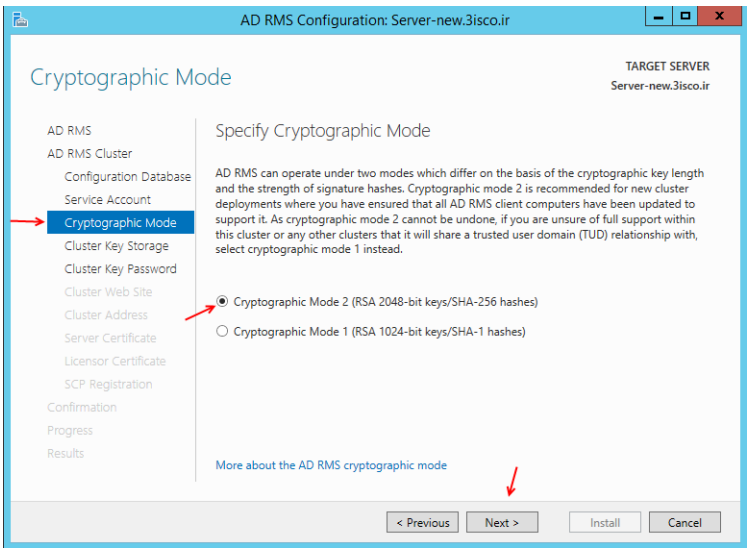


در این صفحه با کلیک بر روی Add می‌توانیم کاربر موردنظر را به لیست گروه موردنظر اضافه کنیم، بعدازاین کار بر روی Ok کلیک کنید تا تنظیمات اعمال شود.



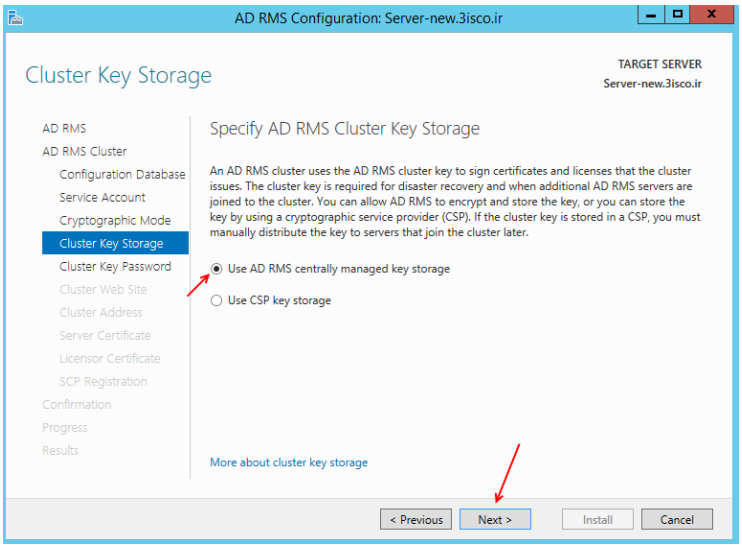
دوباره به تنظیم سرویس موردنظر برمی‌گردیم و با کلیک بر روی Specify کاربر موردنظر را دوباره وارد می‌کنیم که این بار بدون خطا کاربر موردنظر را پذیرفت.

بر روی Next کلیک کنید.



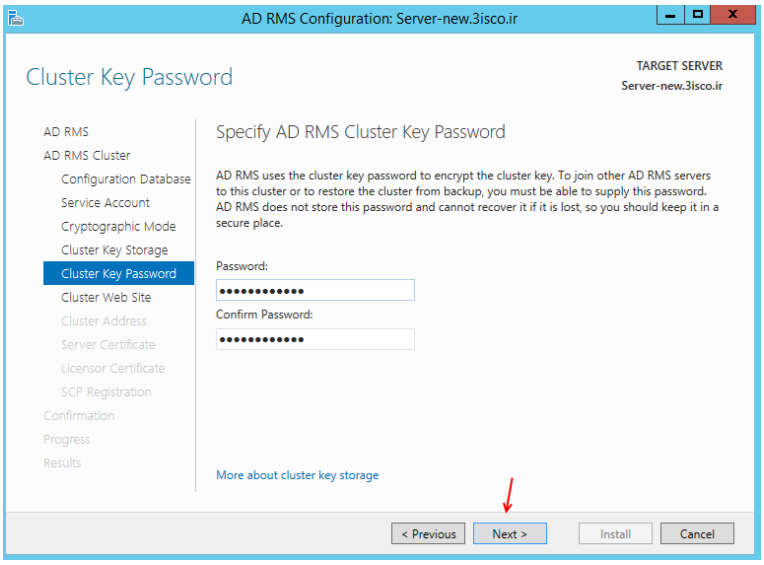
در این قسمت گزینه اول را انتخاب کنید چون طول کلید آن بیشتر است و همان‌طور که می‌دانید هر چه طول کلید بیشتر امنیت اطلاعات بالاتر است.

بر روی next کلیک کنید.

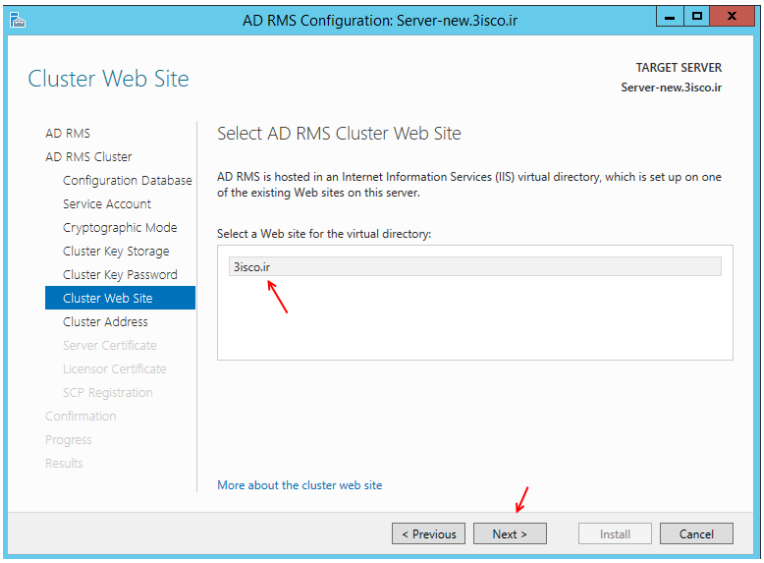


در این قسمت گزینه اول را انتخاب کنید تا سرویس موردنظر بر روی Key Storage مدیریت داشته باشد

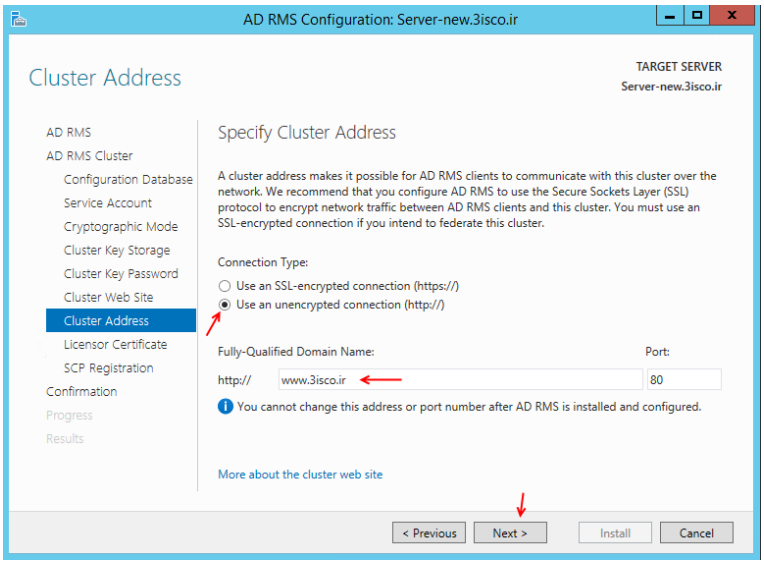
بر روی Next کلیک کنید.



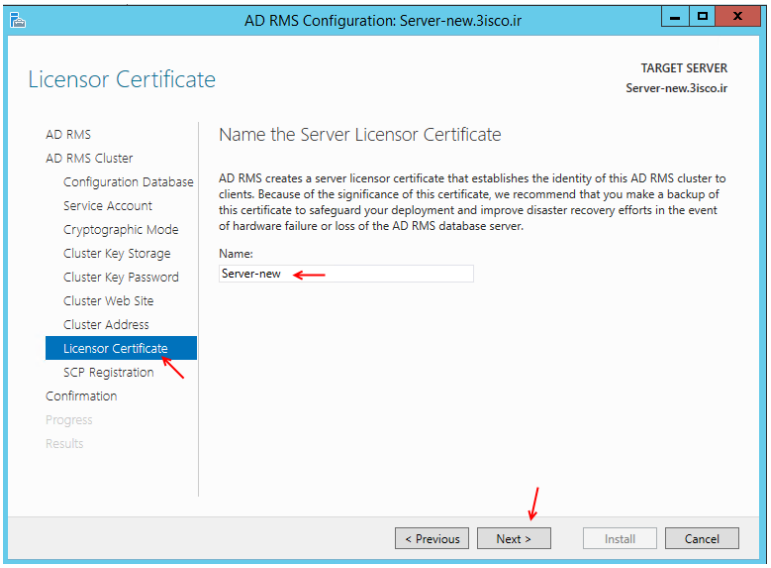
در این صفحه رمز عبوری را به‌دلخواه وارد کنید، این رمز عبور برای زمانی به کار می‌آید که سرویس RMS دیگری بخواهد به سرویس حال حاضر ما متصل شود و یا موقعی که بخواهیم این سرویس را Restore کنیم به کار ما می‌آید. بعد از وارد کردن کلمه عبور بر روی Next کلیک کنید.



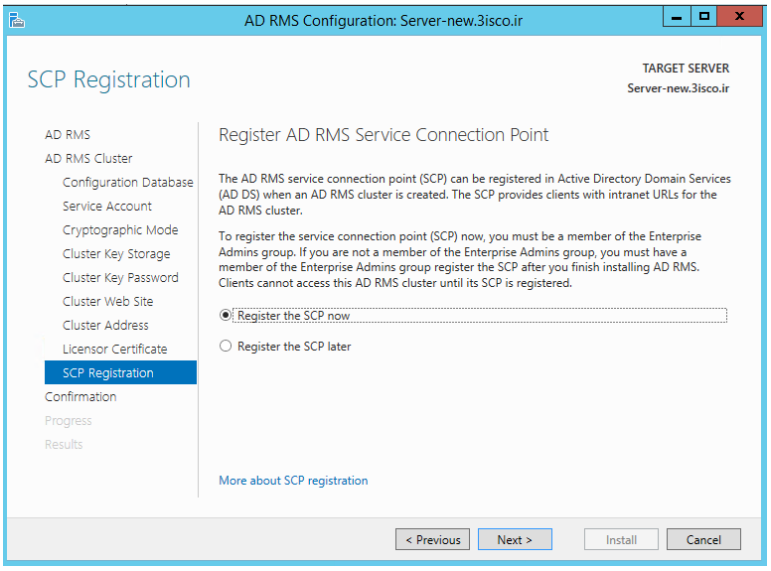
در این قسمت باید وب‌سایت موردنظر خود را انتخاب کنید، اگر از قبل وب‌سایتی ایجاد نکرده باشید به‌صورت پیش‌فرض Default Web site وجود دارد ولی اگر به‌مانند شکل روبرو در سرویس IIS یک سایت ایجاد کرده باشید در این قسمت می‌توانید آن را انتخاب کنید و بر روی Next کلیک کنید.



در این قسمت اگر وب‌سایت شما از پروتکل HTTPS پشتیبانی می‌کند گزینه Use an SSL را انتخاب کنید وگرنه گزینه دوم را انتخاب و در قسمت موردنظر آدرس کامل وب‌سایت خود را وارد کنید. اگر از آدرس پیش‌فرض استفاده می‌کنید باید به‌صورت Computer Name Domain وارد کنید.

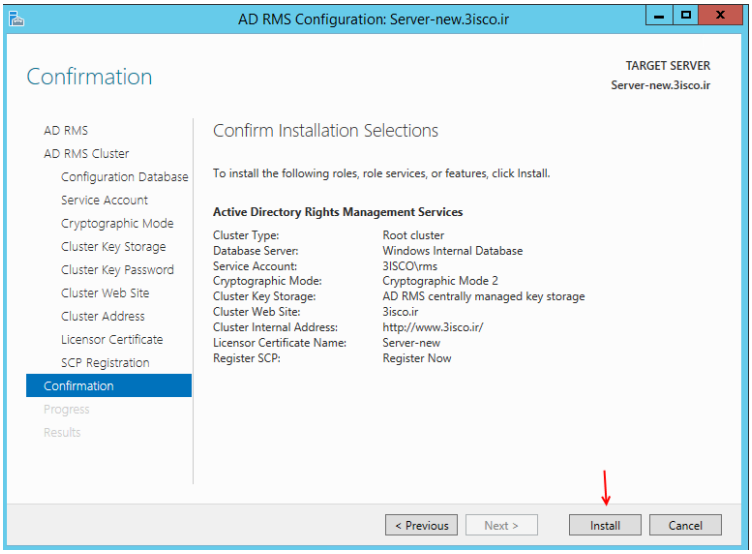


در این قسمت نام سرور خود را که سرویس موردنظر روی آن نصب‌شده است را وارد و بر روی Next کلیک کنید.

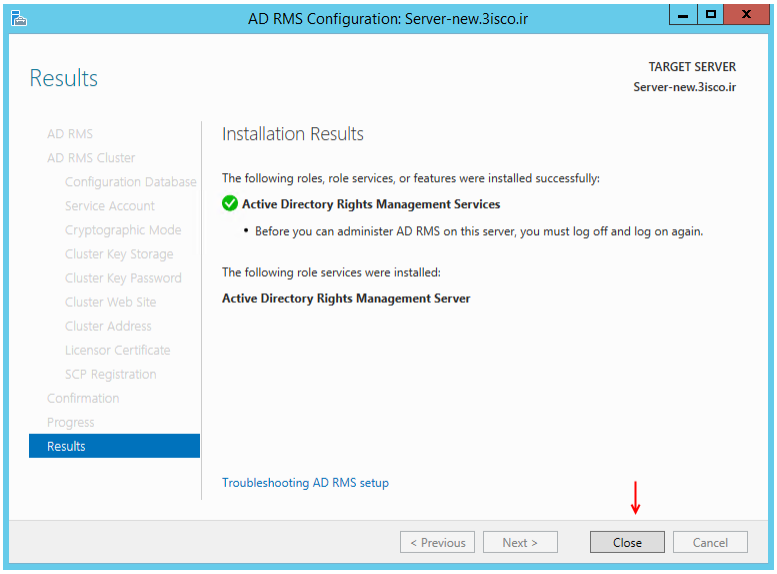


در این قسمت گزینه Register the SCP now را انتخاب کنید تا ارتباط بین سرویس Active Directory Domain با سرویس RMS ایجاد شود.

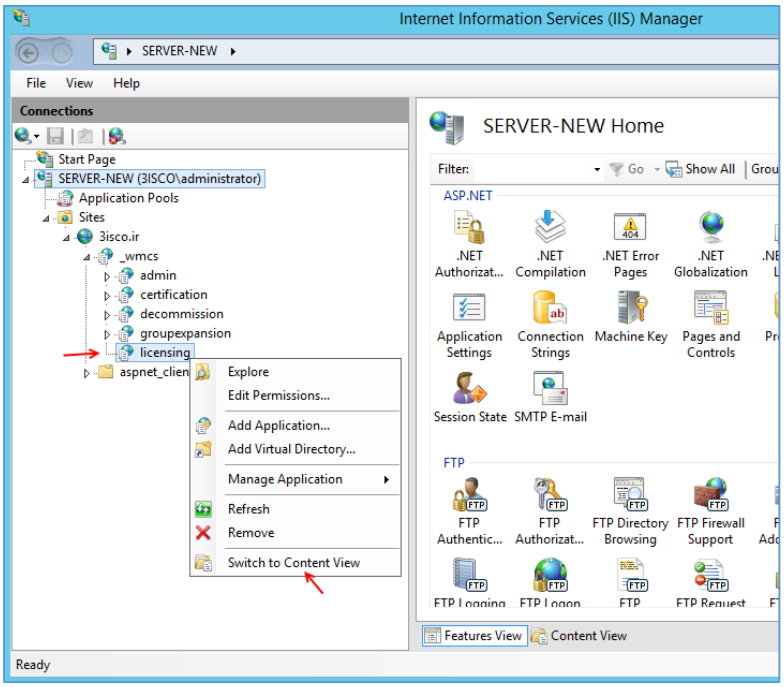
بر روی next کلیک کنید.



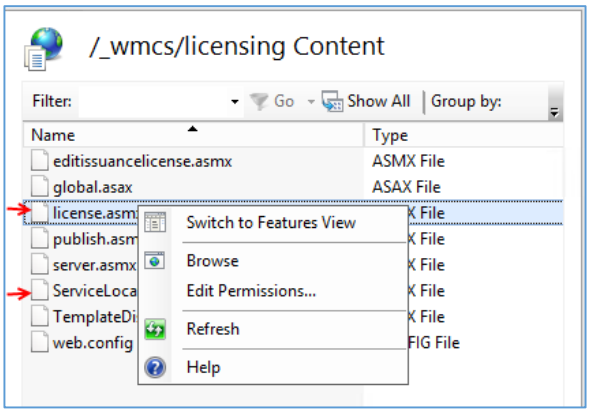
در این قسمت بر روی Install کلیک کنید تا سرویس موردنظر به‌صورت کامل نصب شود.



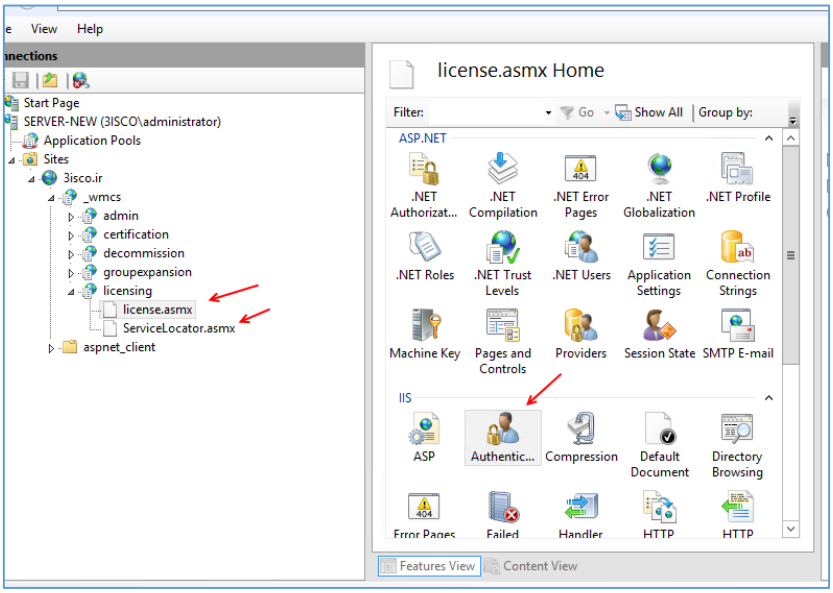
بعد از نصب بر روی Close کلیک کنید و سیستم را حتماً Restart کنید تا تنظیمات به‌صورت کامل اعمال شود.



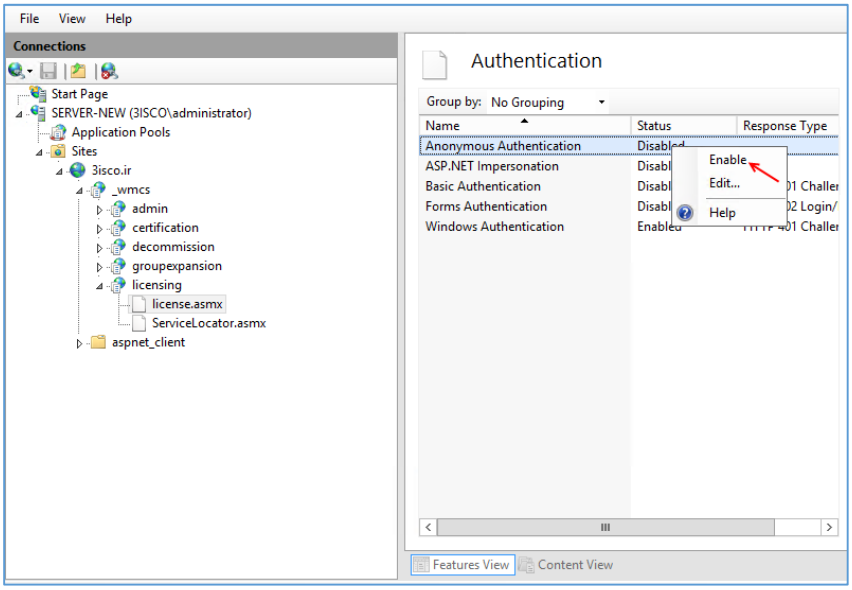
بعد از نصب کامل سرویس وارد سرویس IIS می‌شویم، همان‌طور که مشاهده می‌کنید روی وب‌سایتی که به سرویس موردنظر معرفی کردیم اطلاعات اعمال‌شده است، به‌مانند شکل بر روی Licensing کلیک راست کنید و گزینه Switch to Content View را انتخاب کنید.



در این قسمت، بر روی License.asmx کلیک راست کنید و گزینه Switch to Features view کلیک کنید، همین کار را هم برای گزینه ServiceLocator انجام دهید.

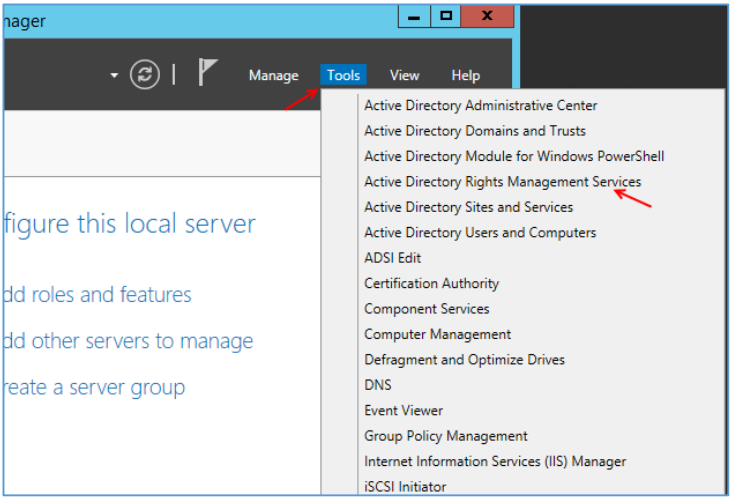


به شکل روبرو توجه کنید دو گزینه موردنظر به زیرمجموعه Licensing اضافه‌شده است، بر روی هرکدام از آن‌ها کلیک کنید و در صفحه بازشده بر روی Authentication دو بار کلیک کنید.

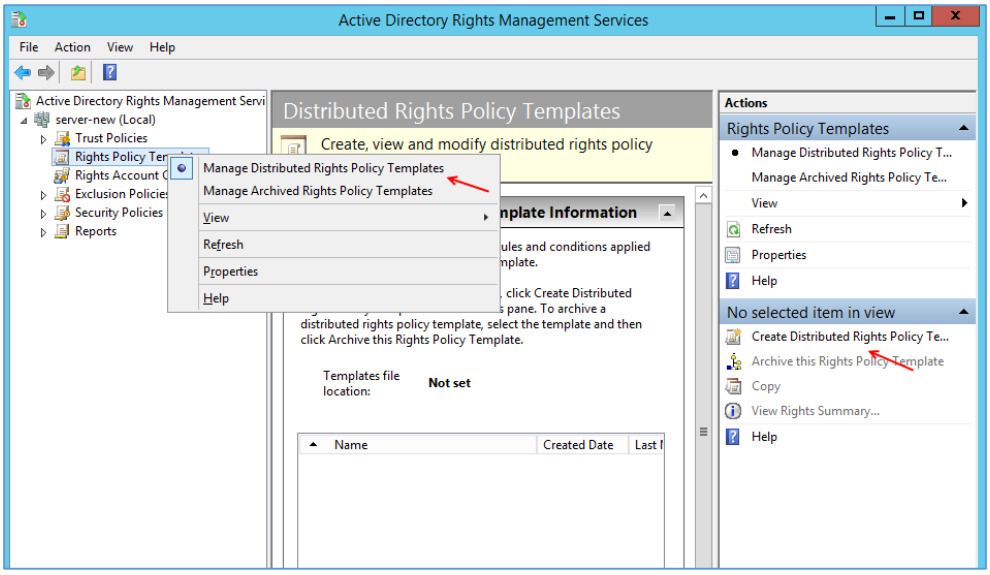


در این قسمت در قسمت Status گزینه Anonymous Authentication کلیک راست کنید و گزینه Enable را انتخاب کنید.

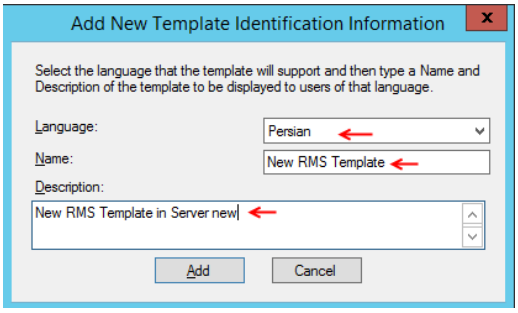
بعد از انجام این کار بر روی هر دو گزینه License و ServiceLocator سرویس IIS را بسته و وارد Server Manager شوید.



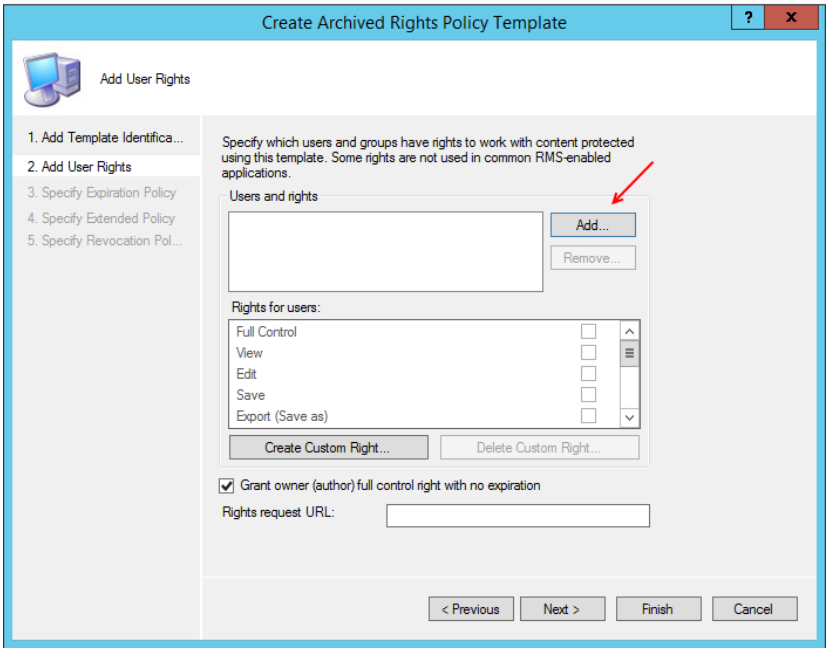
در این صفحه بر روی منوی Tools کلیک کنید و گزینه Active Directory Rights Management Services را انتخاب کنید، البته از طریق Search می‌توانید به این سرویس دست پیدا کنید.



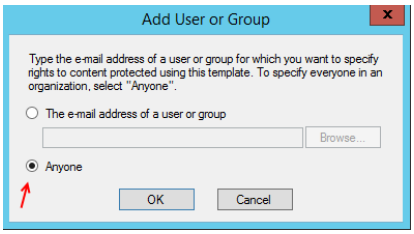
بعد از اجراشدن سرویس به-مانند شکل روبرو از سمت چپ بر روی Rights Policy Templates کلیک راست کنید و گزینه اول را انتخاب کنید و در ادامه از سمت راست گزینه Create Distributed Rights کلیک کنید.

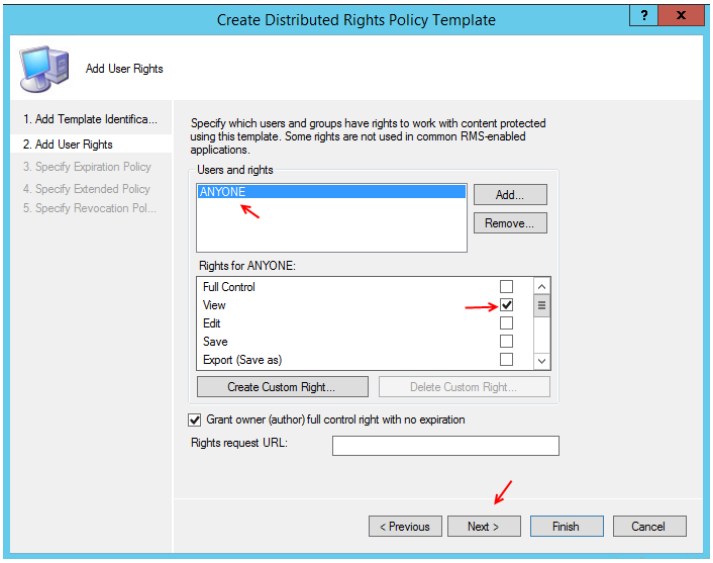


در صفحه بازشده بر روی Add کلیک کنید تا شکل مقابل ظاهر شود که باشد زبان موردنظر خود را انتخاب و یک اسم به‌دلخواه به همراه توضیحات آن در قسمت موردنظر وارد کنید وبر روی Add کلیک کنید. و در صفحه بعد بر روی Next کلیک کنید.

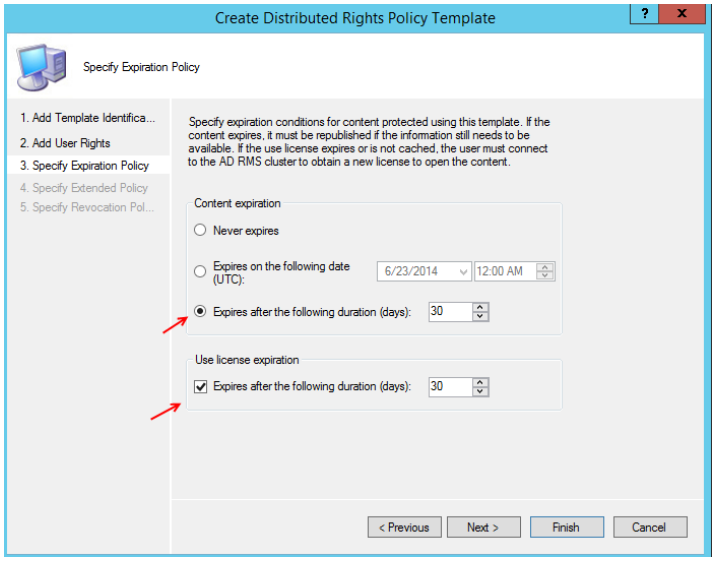


در این صفحه بر روی Add کلیک کنید و در صفحه بازشده گزینه Anyone را به‌مانند شکل زیر انتخاب کنید.

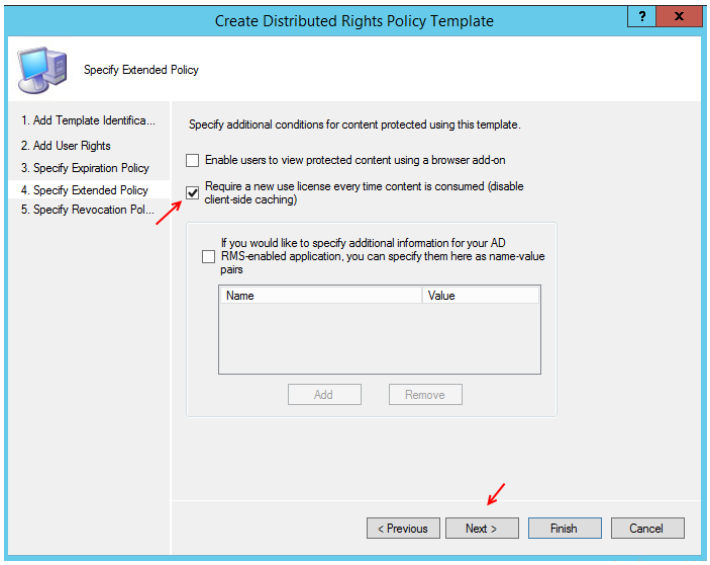




همان‌طور که مشاهده می‌کنید گروه Anyone به قسمت موردنظر اضافه‌شده است و در قسمت Rights for ANYONE گزینه view را انتخاب کنید و بر روی Next کلیک کنید.

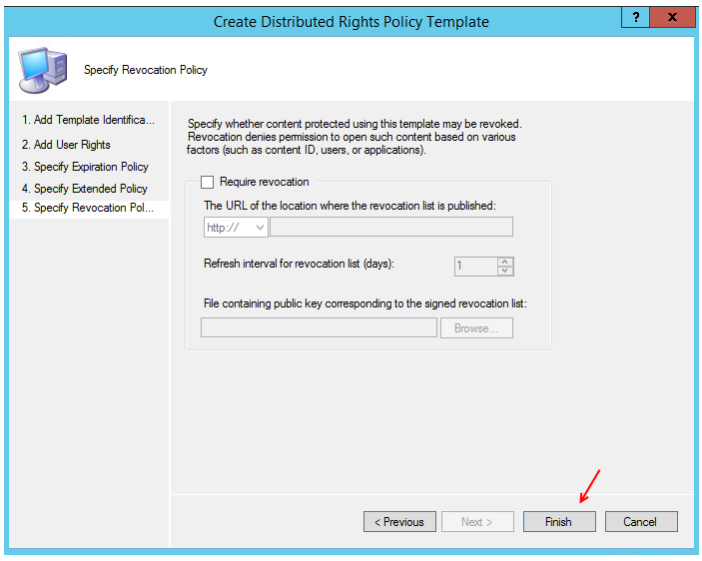


در این قسمت، می‌توانید مشخص کنید که این Template تا چه زمانی اعتبار داشته باشد که در اینجا گزینه سوم انتخاب‌شده و مدت 30 روز وارد-شده است که بعدازاین 30 روز این Template اعتباری در سرور نخواهد داشت. بر روی Next کلیک کنید.

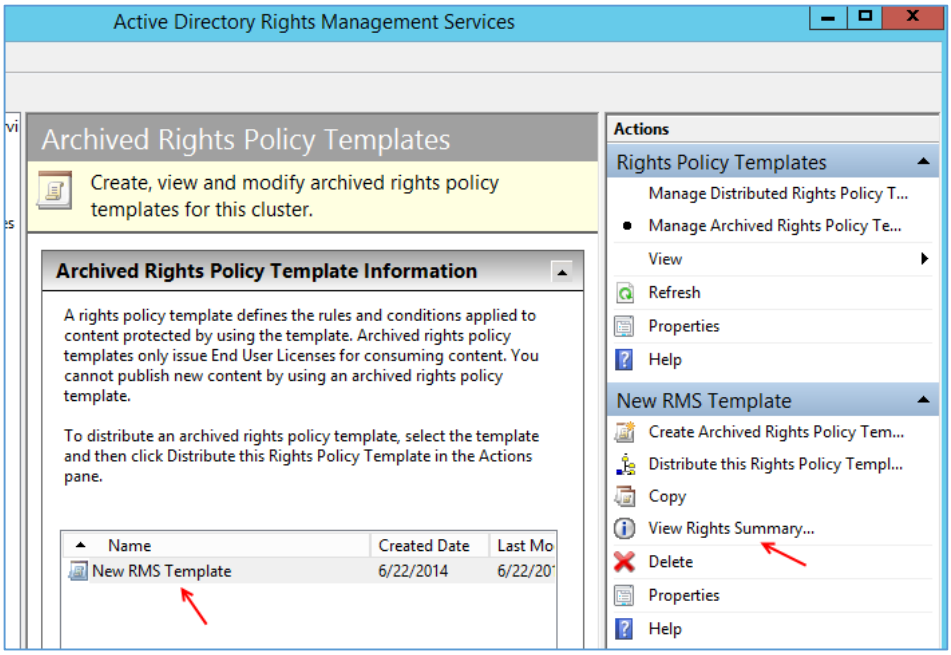


در این قسمت، گزینه Require a new use license every time را انتخاب کنید تا کاربران در هر بار استفاده از این Template یک درخواست جدید بفرستند و هیچ‌وقت این درخواست‌ها در کلاینت ذخیره نشود.

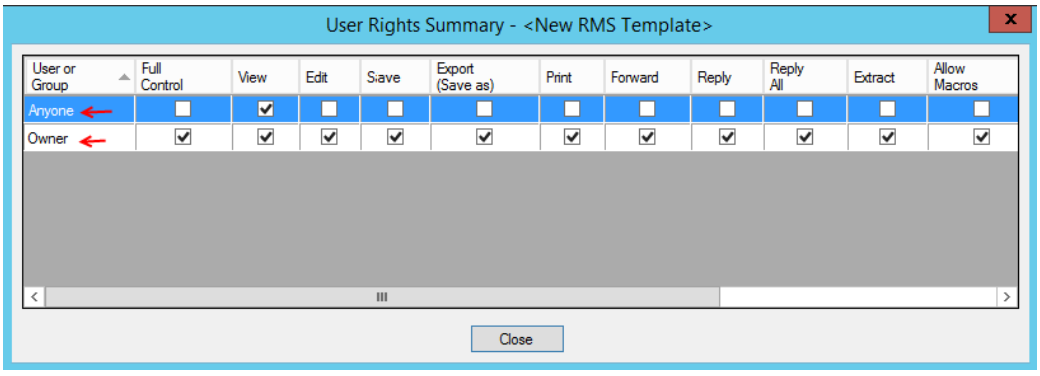
بر روی Next کلیک کنید.



در این صفحه کار به اتمام می‌رسد و برای ایجاد Template بر روی finish کلیک کنید.



بعد از ایجاد Template موردنظر به‌مانند شکل بر روی آن کلیک کنید و از سمت راست بر روی View Rights Summary را انتخاب کنید.



در این صفحه اگر به Owner توجه کنید، مشاهده می‌کنید که دسترسی کامل به Template موردنظر دارد ولی گروه Anyone که تمام کاربران عضو آن هستند فقط دسترسی View به آن داده‌شده است.

ارتقاء اکتیو دایرکتوری 2003 به 2012:

چند ماه پیش که به شرکتی برای مشاوره شبکه رفته بودم، مشخص شد که این دوستان تو سال 2014 هنوز هم از ویندوز سرور 2003 استفاده می‌کنند، به رئیس شرکت گفتم که این ویندوز سرور در حال حاضر توسط مایکروسافت تولید نمی‌شود و ازنظر امنیت و سرعت مشکلات زیادی دارد، به آن‌ها پیشنهاد کردم که از ویندوز سرور 2012 و اکتیو دایرکتوری 2012 استفاده کنند، در این قسمت می‌خواهیم تا با کمک شما این کار را انجام دهیم.

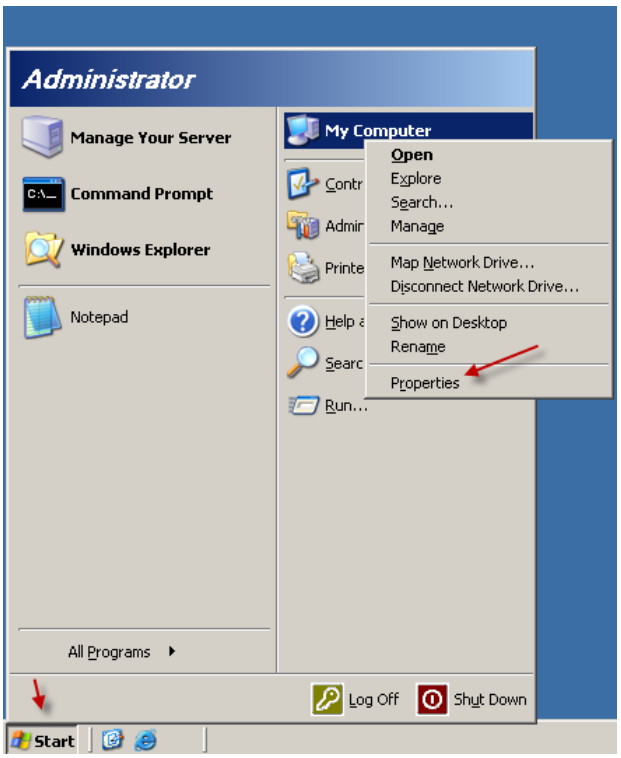
مواردی که برای شروع کار نیاز است:

1- ویندوز سرور 2003 با آخرین آپدیت:

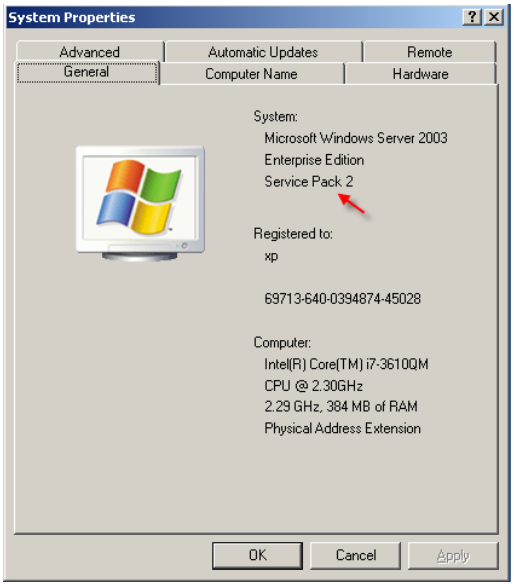
ویندوز سروری که روی آن دومین کنترلر راه‌اندازی شده است باید R2 باشد و آخرین آپدیت را داشته باشد.

2- ویندوز سرور 2012 با آخرین آپدیت (ضرورتی ندارد که آخرین آپدیت‌ها را داشته باشد).

فرض مثال بر این گذاشتیم که سرور 2003 نصب شده است و اکتیو دایرکتوری روی آن فعال شده است، پس برای شروع کار وارد سرور 2003 می‌شویم.

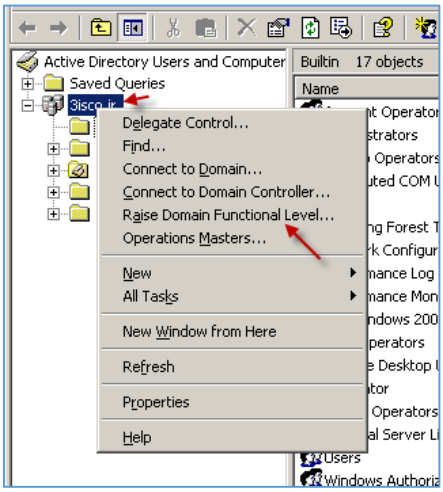


بر روی Start کلیک کنید و بعد بر روی My Computer کلیک راست کنید و گزینه Properties را انتخاب کنید تا متوجه شویم که آیا ورژن این ویندوز Service pack 2 هست یا نه؟

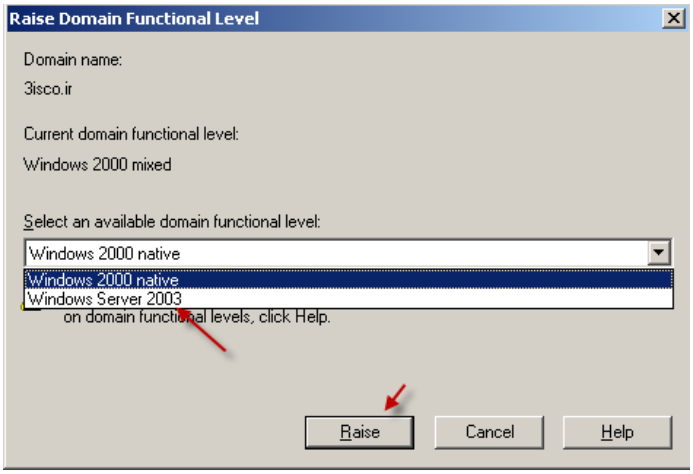


همان‌طور که در شکل مقابل مشاهده می‌کنید این ویندوز سرویس پک 2 است که برای انتقال اطلاعات به سرور 2012 مناسب می‌باشد.

وارد Start شوید و از قسمت Administrative Tools گزینه Active Directory Users and Computers را انتخاب کنید.

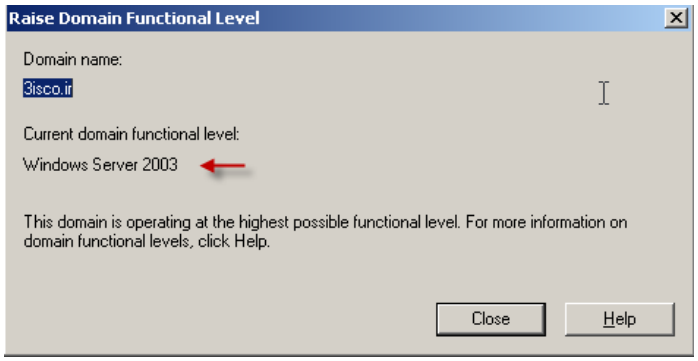


بعد از اجرای سرویس بر روی نام دومین خود که در اینجا 3isco.ir است کلیک راست کنید و گزینه Raise Domain Functional Level را انتخاب کنید.



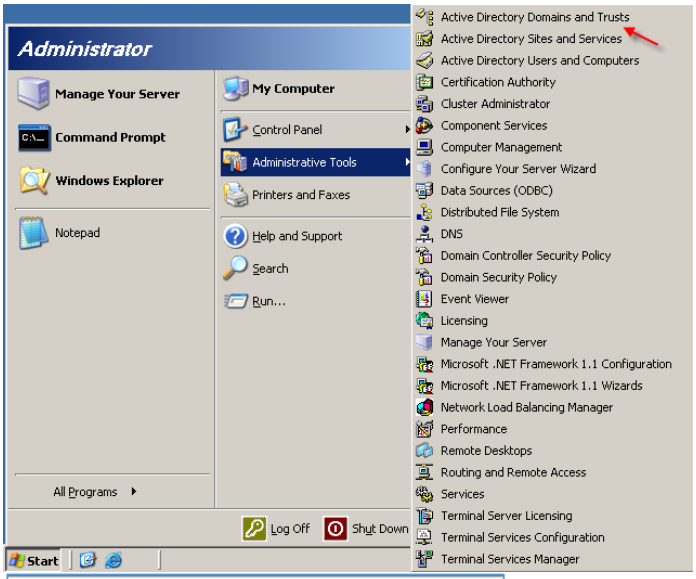
در این شکل و در قسمت Functional Level گزینه Windows Server 2003 را انتخاب کنید و گزینه Raise را انتخاب کنید تا Level تغییر کند.

بعد از کلیک بر روی Raise دو پیغام پشت سر هم مشاهده می‌کنید که بر روی ok کلیک کنید.

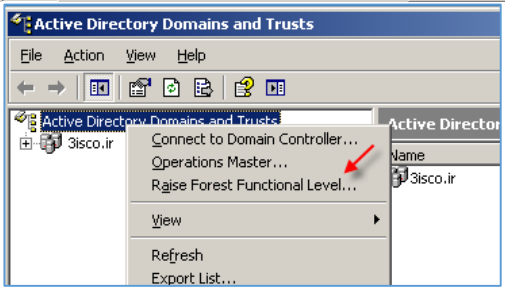


اگر دوباره مسیر قبلی را اجرا کنید با شکل روبرو مواجه می‌شوید که نشان‌دهنده این است که سطح Level آن تغییر کرده است.

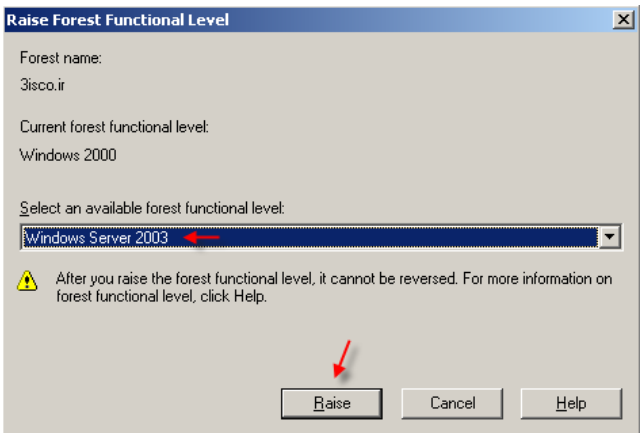
بر روی Close کلیک کنید.



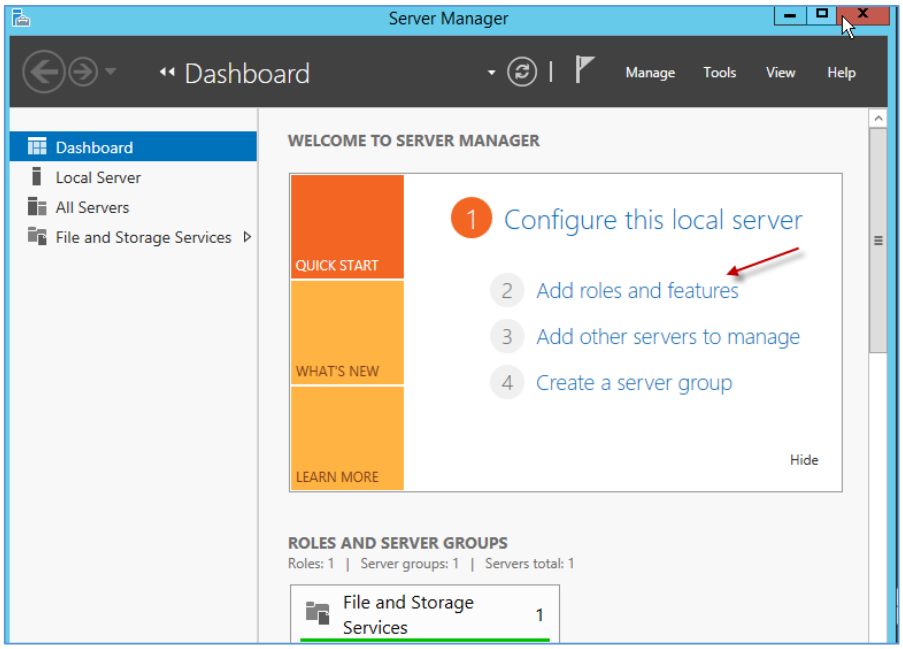
بعد از تغییر Domain Functional باید Forest Functional Level را هم باید تغییر دهید برای این کار بر روی Start کلیک کنید و از قسمت Administrative Tools گزینه Active Directory Domains and Trusts را انتخاب کنید.



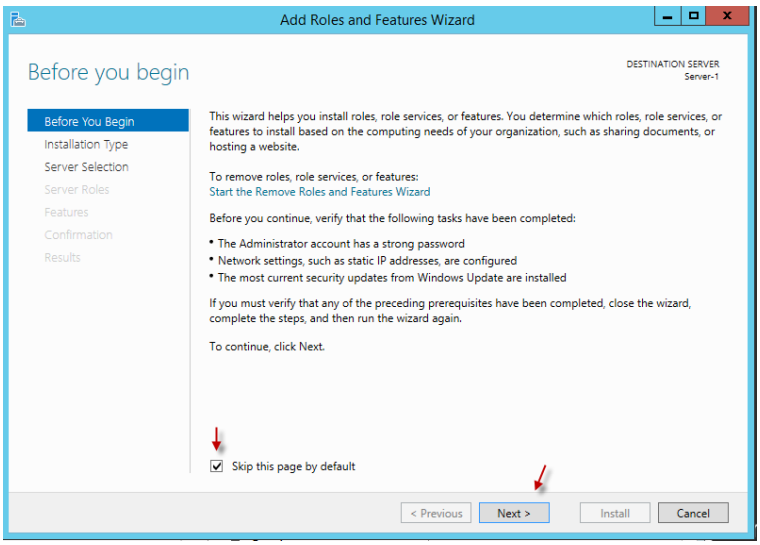
بعد از اجرای سرویس بر روی Active Directory Domains and Trusts کلیک راست کنید و گزینه Raise Forest Functional Level را انتخاب کنید.



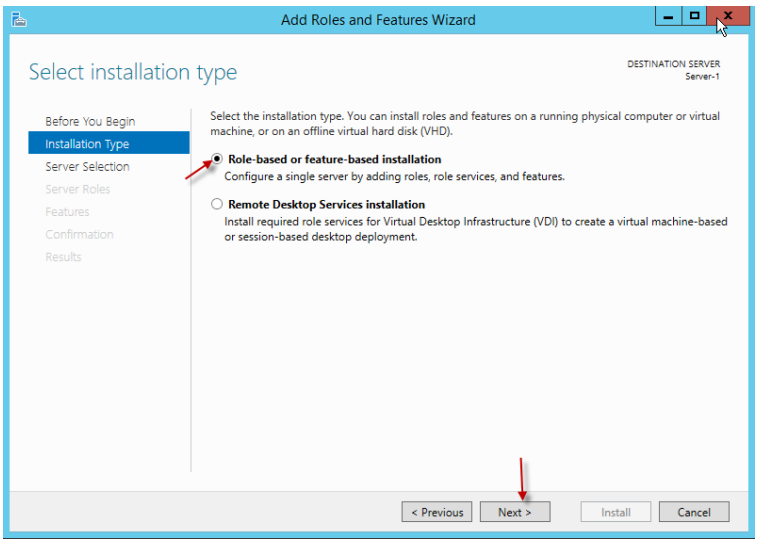
در این قسمت گزینه Windows Server 2003 را انتخاب کنید و بر روی Raise را کلیک کنید.



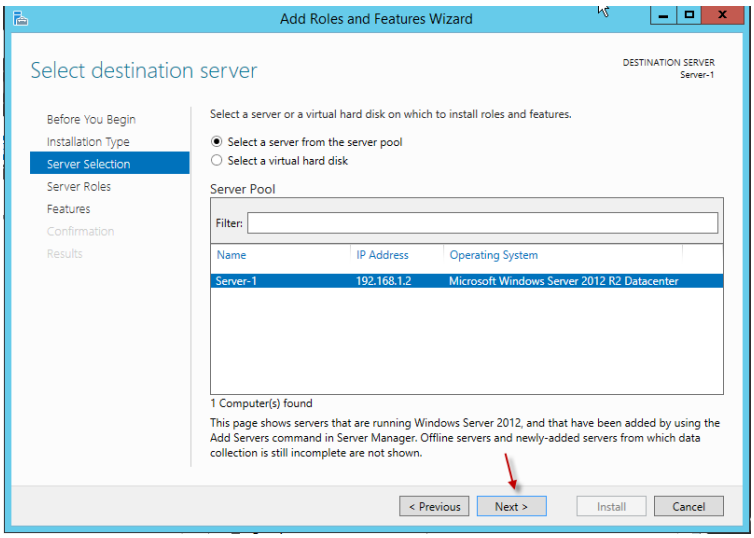
بعد از انجام کارهای بالا وارد ویندوز سرور 2012 می‌شویم و Server Manager را اجرا می‌کنیم و بعد از اجرا بر روی Add Roles and Features کلیک می‌کنیم تا شکل صفحه بعد ظاهر شود.



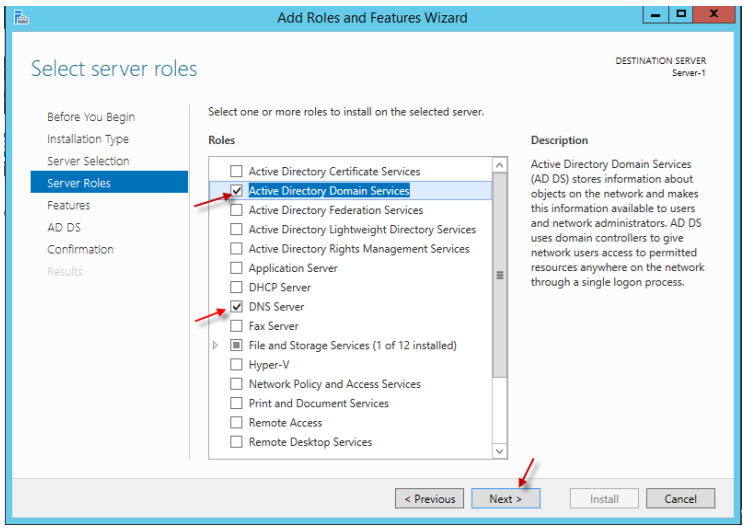
در این صفحه بر روی Next کلیک کنید.



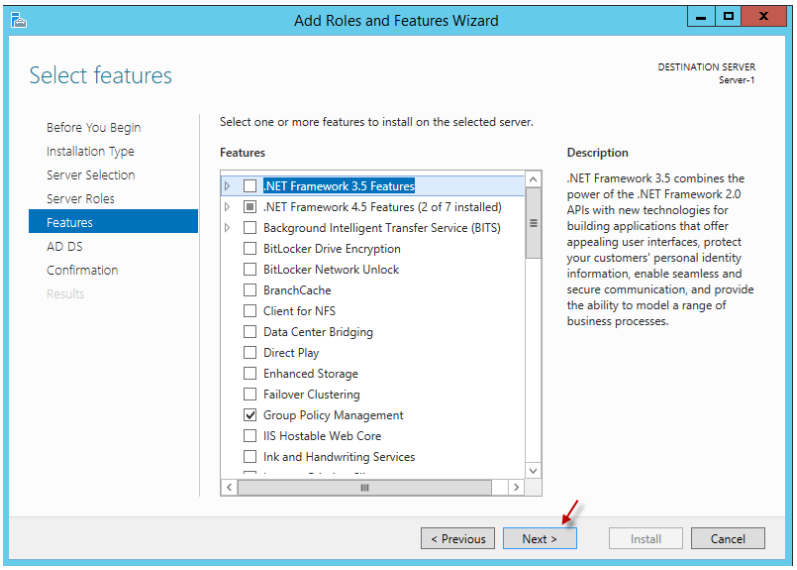
در این صفحه اگر می‌خواهید Role موردنظر را روی همین سیستم نصب کنید گزینه اول را انتخاب کنید و یا اگر می‌خواهید بر روی سیستم دیگری این کار را انجام دهید گزینه دوم را انتخاب کنید، برای ادامه کار گزینه اول را انتخاب و بر روی Next کلیک کنید.



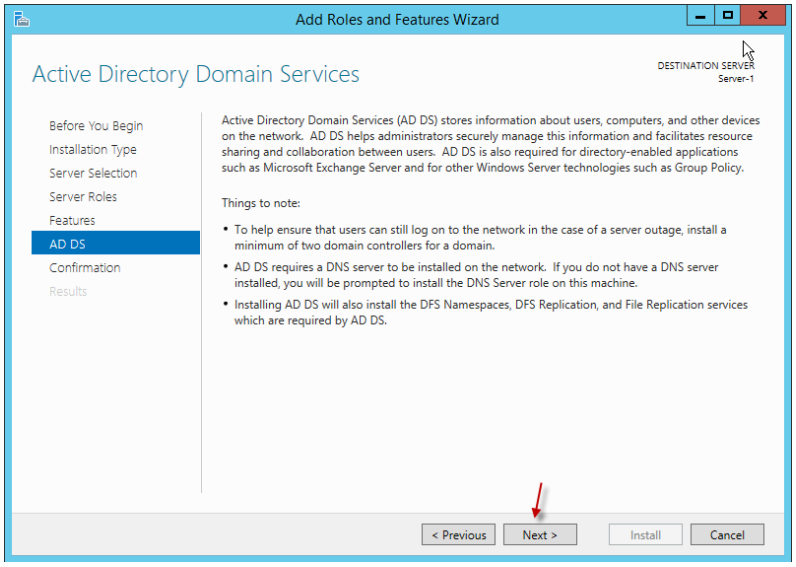
در این قسمت گزینه اول را انتخاب و بر روی Next کلیک کنید.



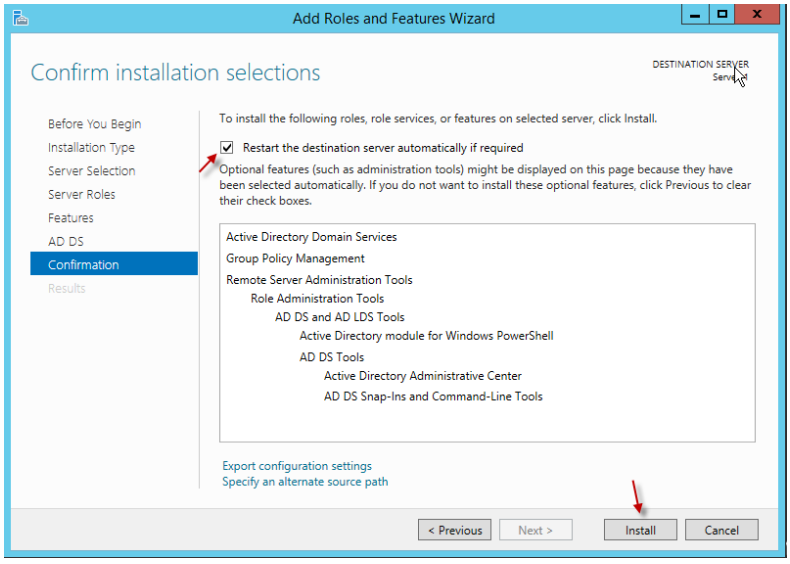
در این صفحه از بین Role های موجود گزینه Active Directory Domain Services و DNS را انتخاب کنید و بر روی Next کلیک کنید.



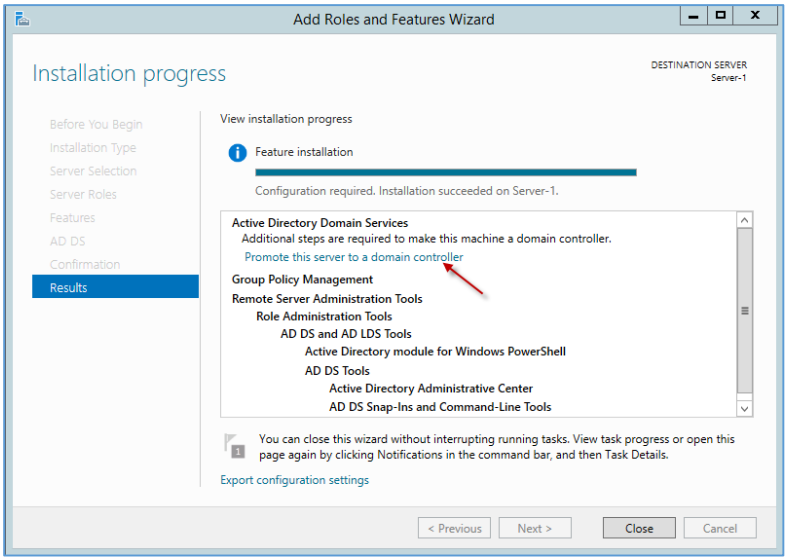
در این قسمت به گزینه‌ای دست نزنید و بر روی Next کلیک کنید.



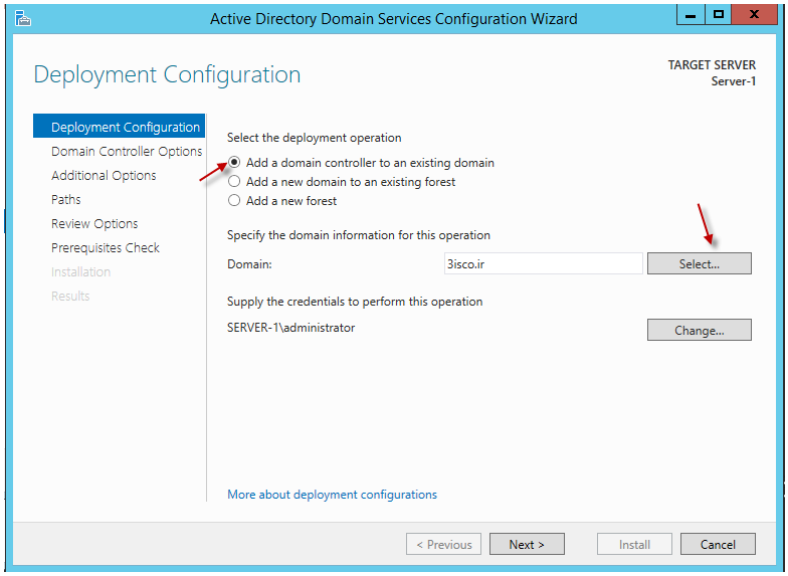
در این قسمت هم بر روی next کلیک کنید.



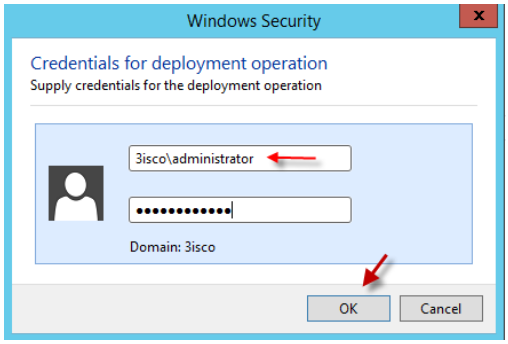
در این قسمت تیک گزینه موردنظر را انتخاب کنید و بر روی install کلیک کنید تا سرویس Active Directory نصب شود.

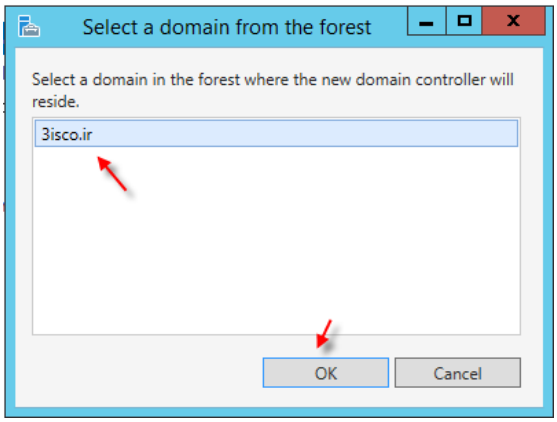


بعد از نصب سرویس و برای تنظیم آن بر روی Promote this server to a domain controller کلیک کنید تا شکل بعد ظاهر شود.

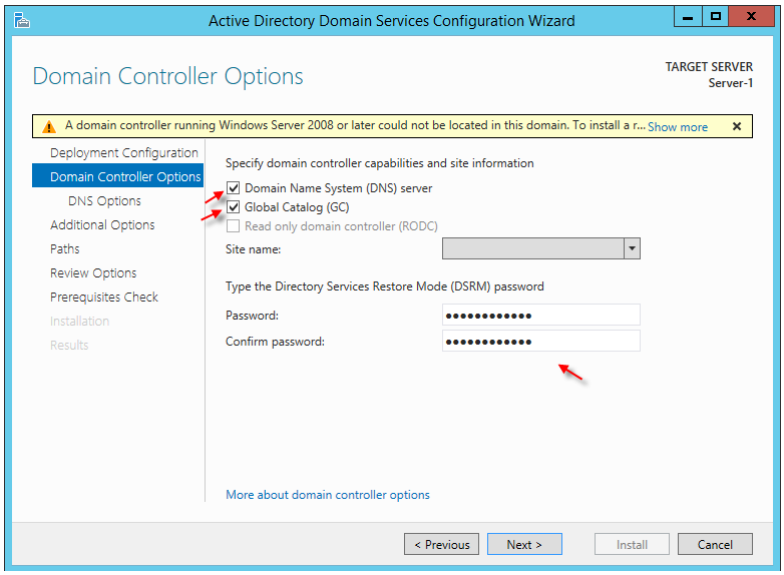


در این قسمت باید گزینه اول را انتخاب کنید تا دومین جدید بتواند همه اطلاعات را از دومین 2003 دریافت کند، بعد از انتخاب گزینه اول بر روی Select کلیک کنید و نام مدیر سرور 2003 را به همراه رمز عبور وارد کنید



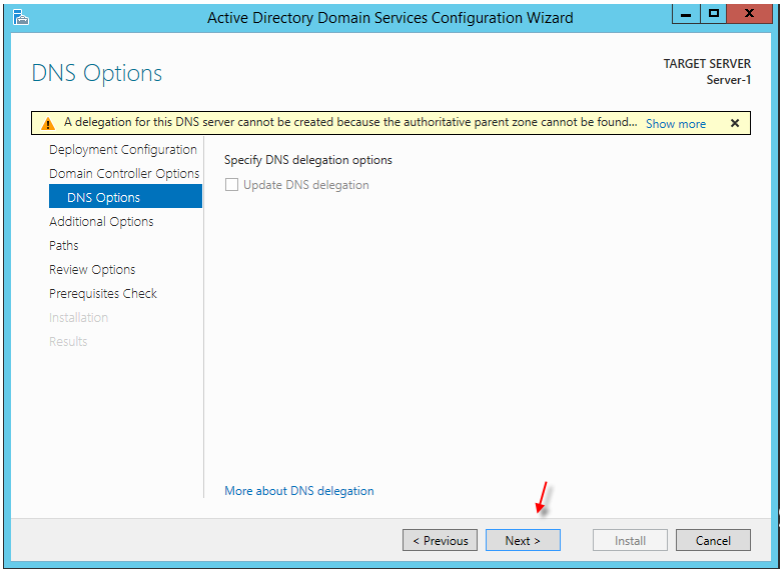


توجه داشته باشید، نام دومین را هم قبل از آن به‌مانند شکل وارد کنید، البته اگر سرور 2012 عضو دومین 2003 باشد این قسمت به صورت خودکار تکمیل می‌گردد، بعد از کلیک بر روی ok شکل روبرو ظاهر می‌شود که نام دومین را انتخاب کنید و بر روی ok کلیک کنید و در صفحه اصلی بر روی next کلیک کنید.

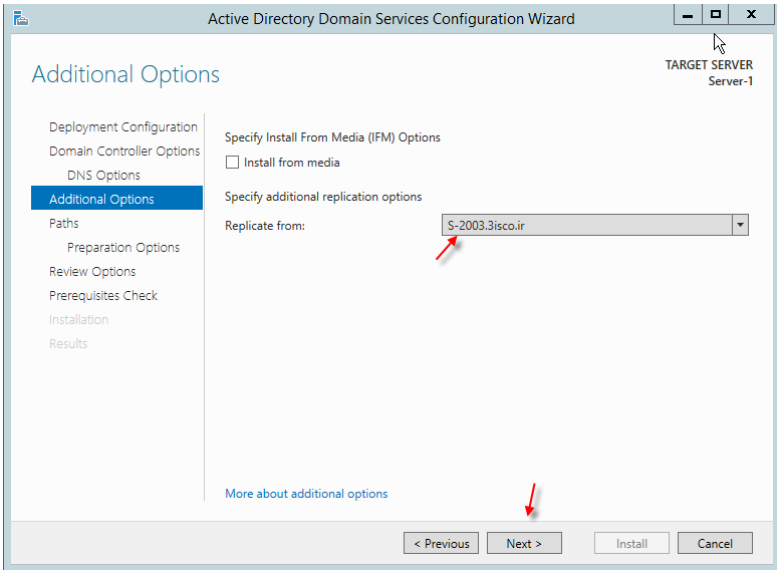


در این قسمت گزینه‌های Domain Name System (DNS) server و Global Catalog را انتخاب کنید و یک کلمه عبور برای DSRM وارد کنید که برای Restore کردن اطلاعات هست و در مواقع ضروری کاربرد دارد.

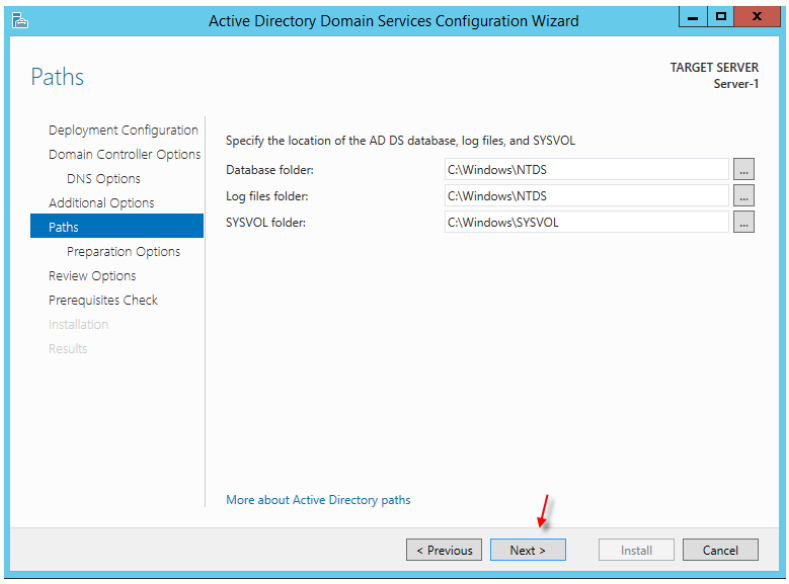
بر روی Next کلیک کنید.



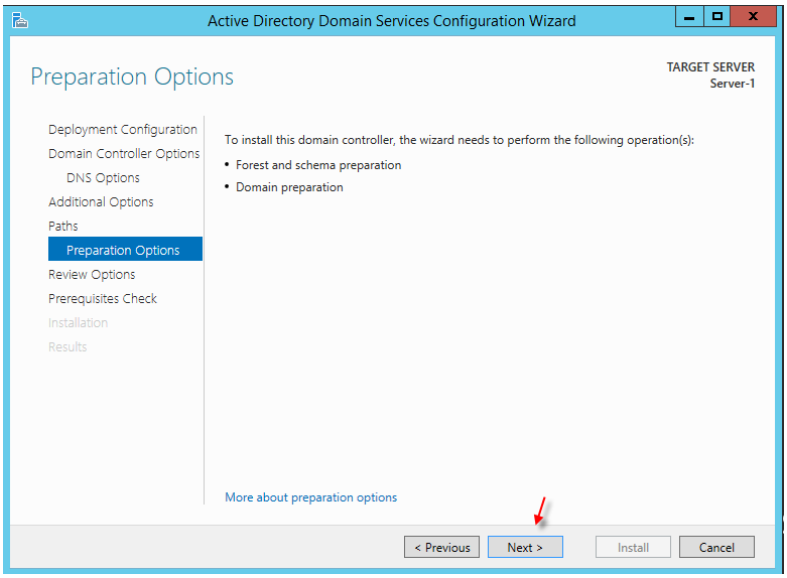
در این قسمت بر روی Next کلیک کنید.



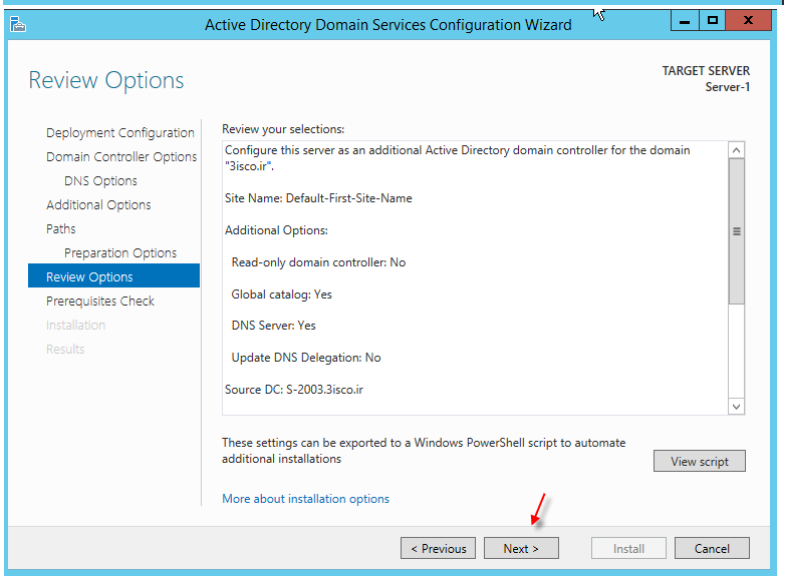
در این صفحه و در قسمت Replicate from نام دومین خود را انتخاب کنید و بر روی Next کلیک کنید.



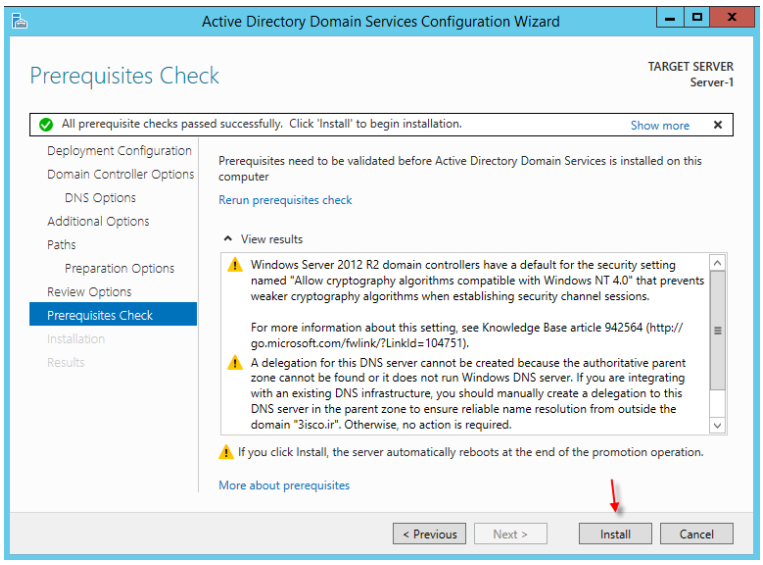
در این قسمت می‌توانید مسیر مشخص برای ذخیره‌سازی فایل‌های موردنظر مشخص کنید. بر روی Next کلیک کنید.



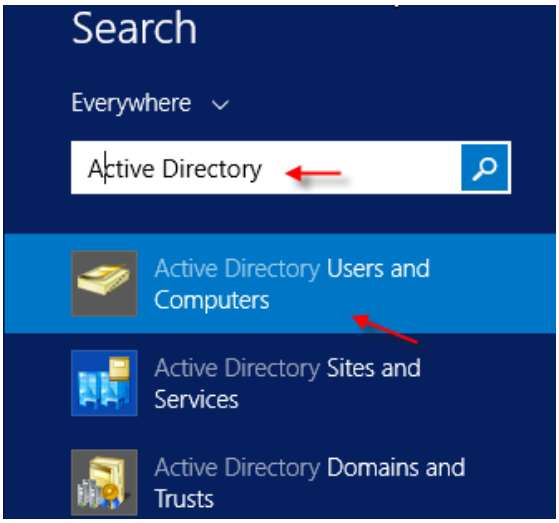
در این قسمت بر روی Next کلیک کنید.



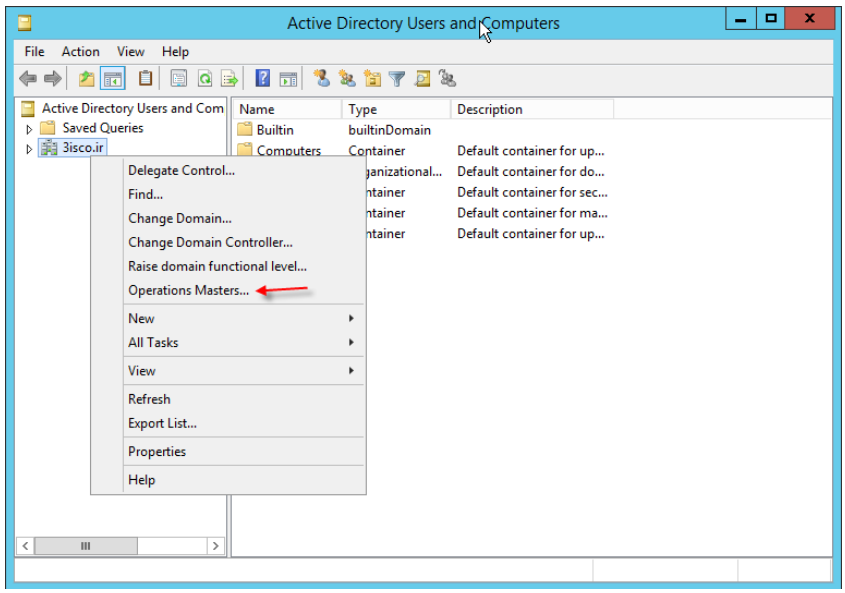
در این قسمت بر روی Next کلیک کنید.



در این قسمت بعدازاینکه پیش‌نیازهای موردنظر به‌مانند شکل روبرو تأیید شد بر روی install کلیک کنید تا دومین کنترلر نصب شود.

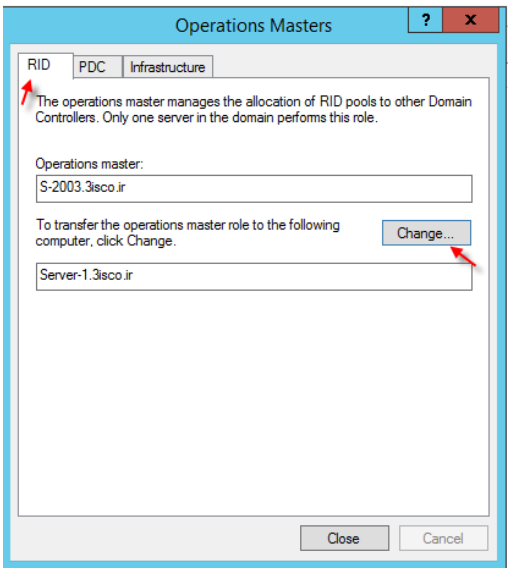


بعد از نصب Domain در ویندوز سرور 2012 وارد Search شوید و سرویس Active Directory Users and Computers را انتخاب کنید.

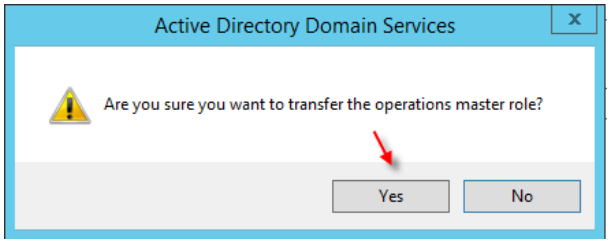


بعد از اجزای سرویس بر روی نام دومین که در اینجا 3isco.ir است کلیک راست کنید و گزینه Operations Masters را انتخاب کنید.

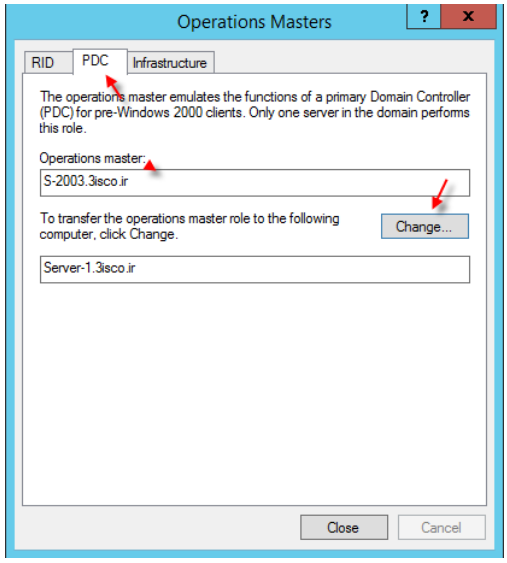
در این صفحه در تب RID برای اینکه وظایف دومین کنترلر را از 2003 به 2012 انتقال دهیم بر روی Change کلیک کنید.



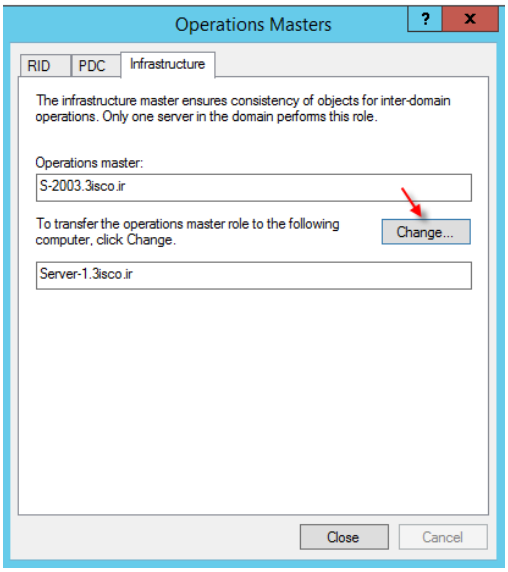
در شکل زیر بر روی Yes کلیک کنید.

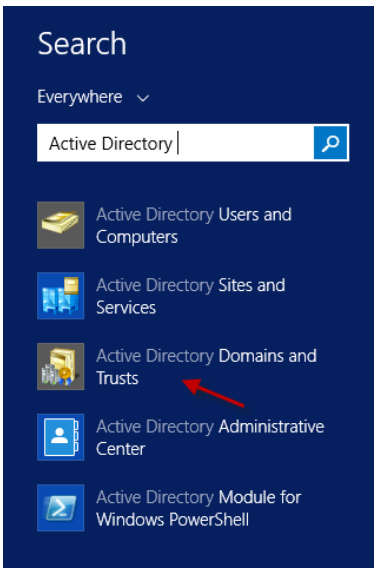


در تب PDC بر روی Change کلیک کنید و بعد بر روی Yes کلیک کنید.



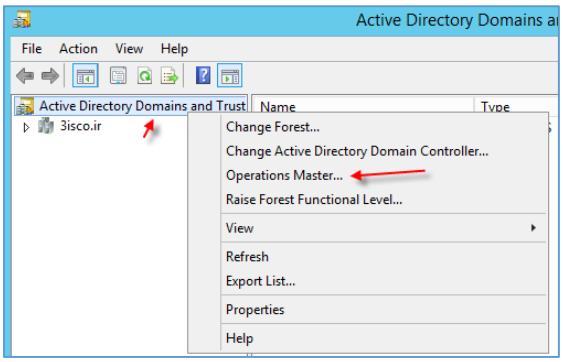
در تب Infrastructure بر روی Change کلیک کنید و در شکل باز شده بر روی Yes کلیک کنید.

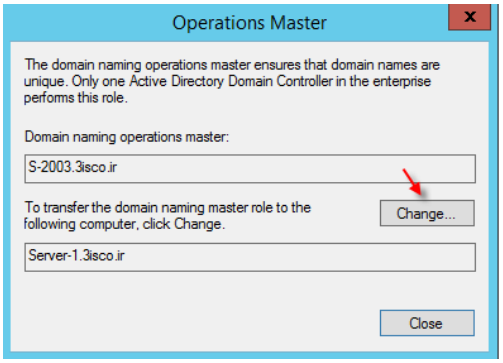




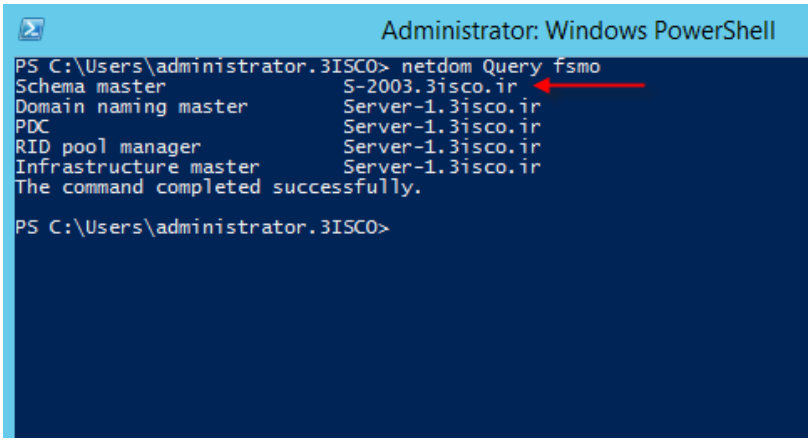
بعد از انجام کارهای بالا وارد Search شوید و سرویس Active Directory Domains and Trusts را انتخاب کنید.

بعد از اجرای سرویس بر روی Active Directory Domains and Trusts به مانند شکل زیر کلیک راست کنید و گزینه Operations Master را انتخاب کنید.

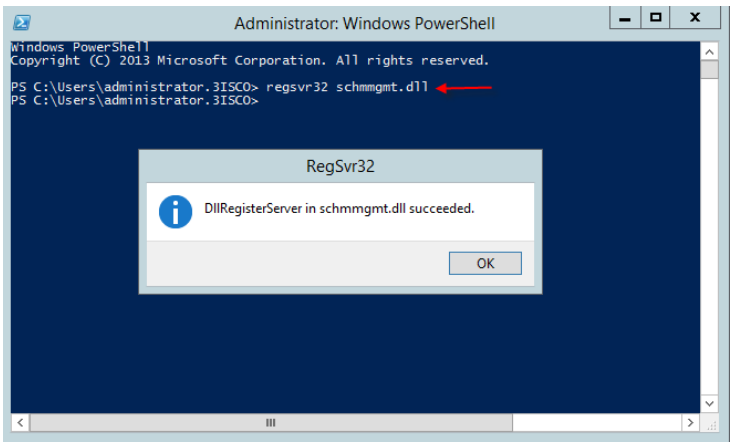




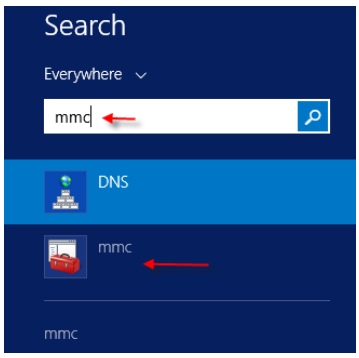
در این قسمت بر روی Change کلیک کنید تا انتقال اطلاعات از 2003 به 2012 انجام شود.



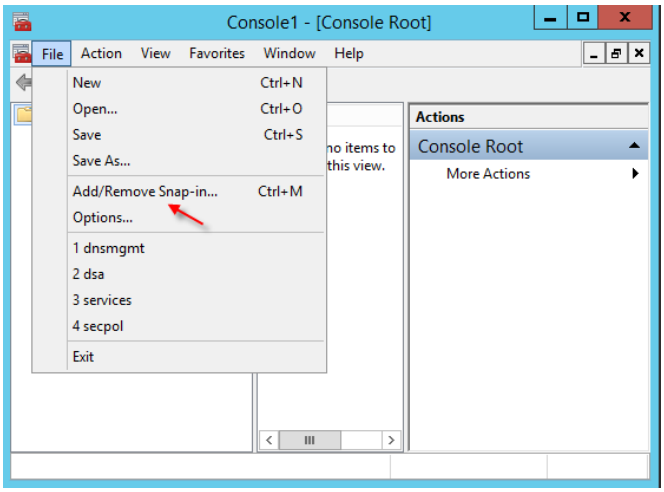
بعد از انجام عملیات بالا به‌صورت کامل سرویس PowerShell را با اولویت کاربر Administrator اجرا کنید، و دستور netdom Query fsmo را وارد کنید و خروجی آن باید به‌صورت شکل روبرو باشد، در این شکل مشخص‌شده است که از بین پنج قسمت موجود چهار قسمت به سرور 2012 انتقال داده شد و فقط قسمت اول که Schema Master باشد به سرور 2012 انتقال داده نشده که برای انتقال آن باید کارهای زیر را انجام دهیم.



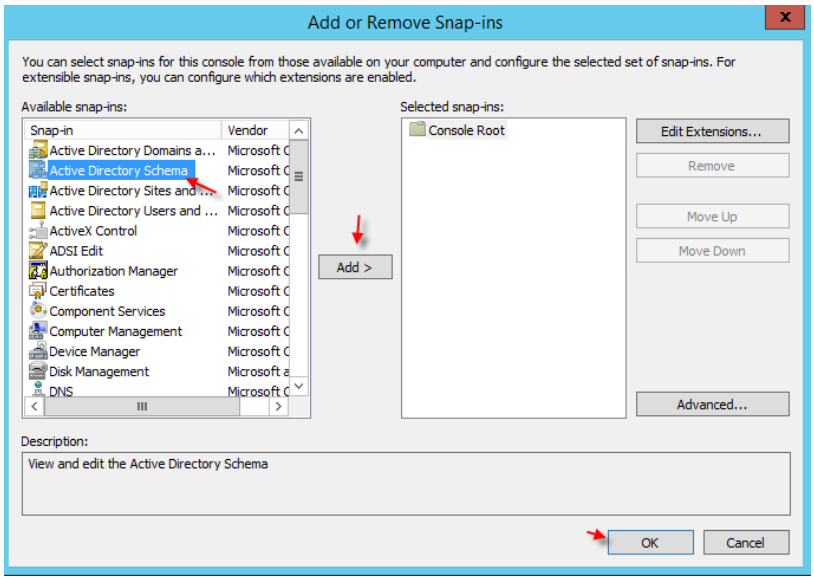
سرویس PowerShell را اجرا کنید و دستور regsvr32 schmmgmt.dll را اجرا کنید تا سرویس Schema Master از طریق کنسول مایکروسافت در دسترس باشد.



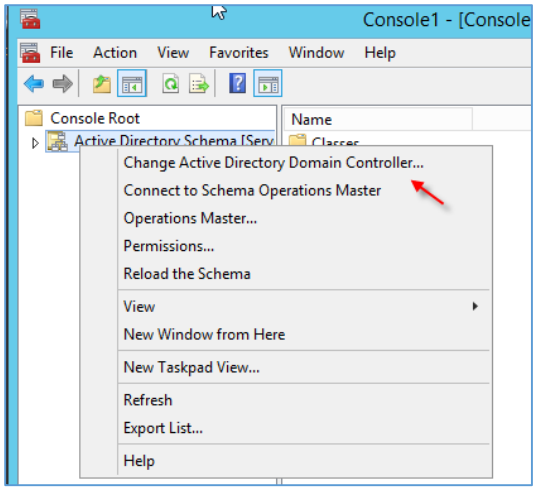
بعد از انجام کار بالا وارد Search شوید و سرویس MMC را به مانند شکل روبرو اجرا کنید.



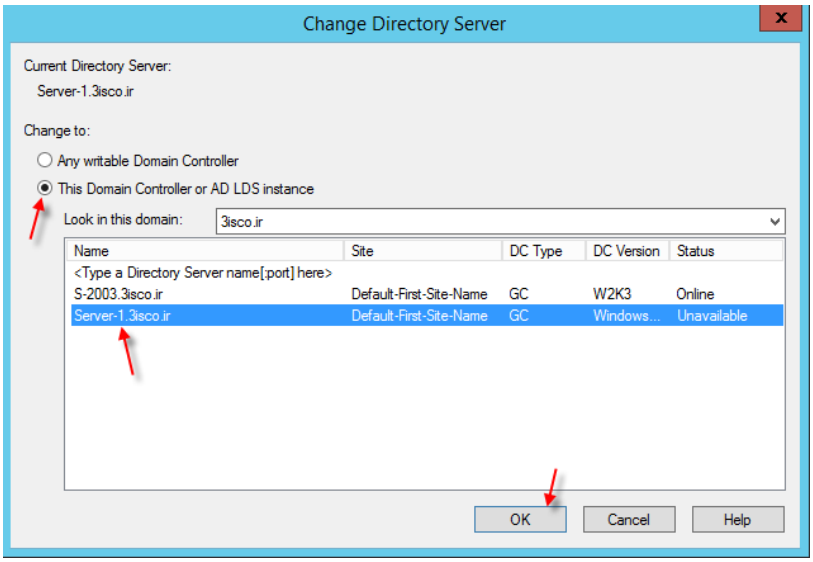
بعد از اجرای سرویس وارد File شوید و بر روی Add/Remove Snap-in را انتخاب کنید.



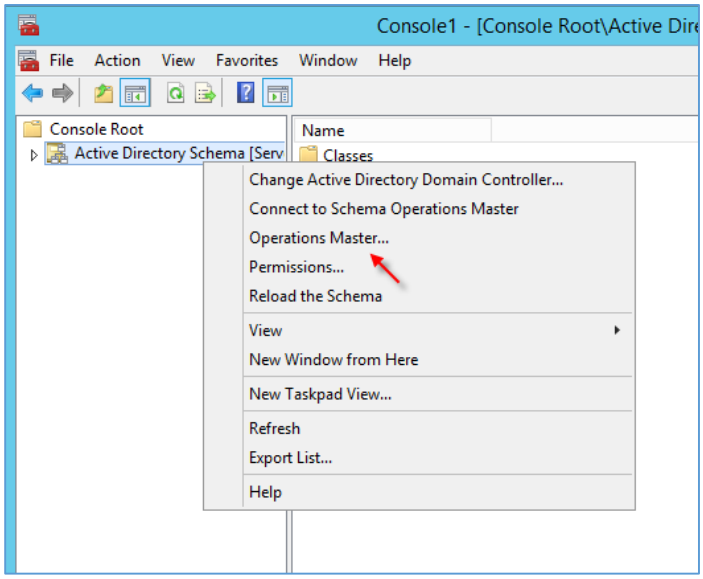
در این صفحه از سمت چپ گزینه Active Directory Schema را انتخاب کنید و بر روی Add کلیک کنید تا به لیست اضافه شود و بعد بر روی ok کلیک کنید.



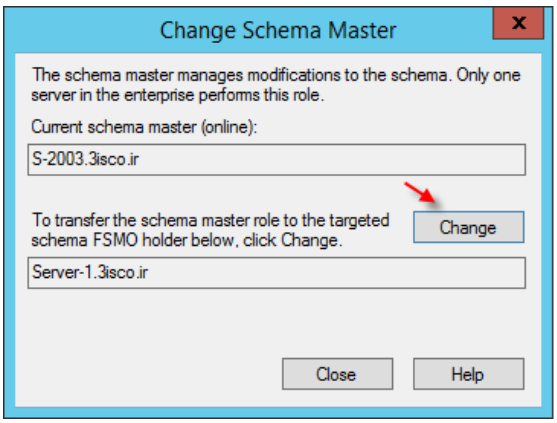
در این صفحه بر روی Active Directory Schema کلیک راست کنید و گزینه Change Active Directory Domain Controller را انتخاب کنید.



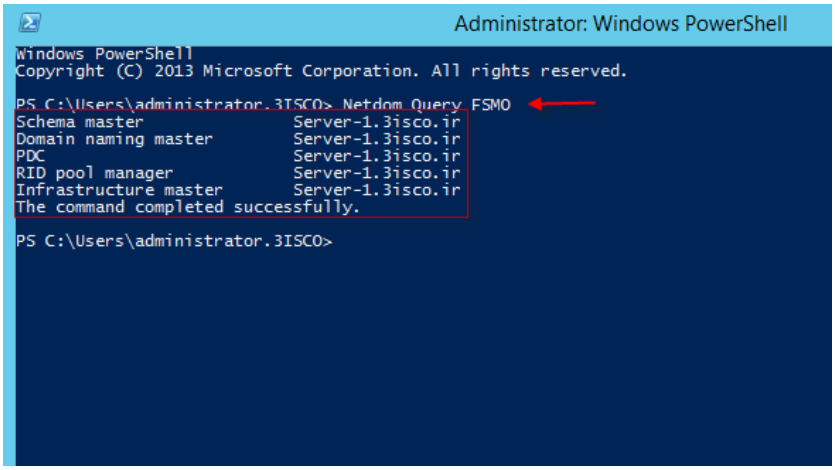
در این صفحه گزینه This Domain Controller or AD LDS instance را انتخاب کنید و از بین سرورهای موجود، سرور 2012 را انتخاب کنید و بر روی ok کلیک کنید.



بعد از انجام کار بالا دوباره بر روی Active Directory Schema کلیک راست کنید و بر روی Operations Master کلیک کنید تا شکل بعد ظاهر شود.



در این قسمت بر روی Change کلیک کنید تا کار انتقال اطلاعات از 2003 به 2012 انتقال داده شود.



وارد PowerShell شوید و دستور Netdom Query FSMO را دو بار اجرا کنید، همان‌طور که مشاهده می‌کنید کار انتقال اطلاعات از سرور 2003 به سرور 2012 به‌صورت کامل در پنج مرحله تمام‌شده است و حالا می‌توانید سرور 2012 را به‌عنوان سرور اصلی در شبکه معرفی کنید و سرور 2003 را به‌عنوان سرور کمکی به کار ببرید و یا می‌توانید آن را حذف کنید، سعی کنید این عملیات را به‌دقت انجام دهید تا اطلاعات به‌صورت کامل به سرور جدید منتقل شود تا زمانی که از کار خود مطمئن نشدید سرور قدیمی را حذف نکنید.

تماس با ما:

Farshid_babajani@live.com

Farshid_babajani@yahoo.com

http://3isco.ir

آدرس کانال :

https://telegram.me/ciscopress

آدرس گروه آموزش شبکه :

https://t.me/joinchat/BkXe4z8z-z2iSC8H_J-UUQ

زندگی پایان رؤیاها نیست، حتّی پایان غم‌ها هم نیست، زندگی در تب و تاب و در برگ‌ریز ثانیه هایی گرفتار است که قدرش را ندانیم و من درامتداد تمام بودن‌های ناپایدار دانستم که پژواک پرواز قاصدک‌های عشق هنوز هم پابرجاست (آزاده تیشه برسر).

به پایان آمدیم دفتر، حکایت همچنان باقیست...