

کتاب آموزشی مدیر شبکه ۲

- ✓ نصب و راه اندازی ویندوز سرور ۲۰۱۶
- ✓ راه اندازی اتاق سرور به همراه تجهیزات آن
- ✓ نصب و راه اندازی سیستم سنتر ۲۰۱۶
- ✓ نصب و راه اندازی دوربین مدار بسته
- ✓ آنتی ویروس تحت شبکه
- ✓ امنیت در شبکه
- ✓ سیستم سانترال
- ✓ و.....

Network Administrator 2

Farshid Babajani

«به نام خدایی که در این نزدیکی است»

کتاب آموزشی مدیر شبکه‌ی ۲

Network Administrator 2

نویسنده: فرشید باباجانی

ویراستار: آزاده تیشه برسر

تهران – بهار ۱۳۹۶

عنوان

صفحه

مقدّمه..... ۱
طرّاحی و پیاده‌سازی اتاق سرور..... ۲
آماده‌سازی اتاق سرور..... ۲
سیستم سرمایشی مناسب..... ۳
سیستم اطفای حریق..... ۵
انواع رک‌ها..... ۷
رک ایستاده..... ۸
انتخاب سوئیچ مناسب در شبکه..... ۹
انتخاب کابل مناسب..... ۱۱
بررسی پچ پنل در رک..... ۱۷
کیستون..... ۱۸
بررسی UPS در شبکه..... ۱۹
راه‌اندازی سرور..... ۲۱
انتخاب مادربرد..... ۲۲
انتخاب CPU..... ۲۳
انتخاب رم..... ۲۳
انتخاب هارد دیسک..... ۲۳
تفاوت بین هارد SAS با SATA..... ۲۴
ویندوز سرور ۲۰۱۶..... ۲۵
نسخه‌های مختلف ویندوز سرور ۲۰۱۶..... ۲۶
سخت‌افزار مورد نیاز ویندوز سرور ۲۰۱۶..... ۲۷
بررسی ابزارها و سرویس‌های ویندوز سرور ۲۰۱۶..... ۳۱
شبکه کردن دو سیستم با هم..... ۳۸
بررسی سرویس‌های شبکه..... ۴۱
سرویس DNS..... ۴۱
بررسی فایل HOSTS در ویندوز..... ۴۱
DNS های اینترنتی..... ۴۵
نصب و راه‌اندازی سرویس DNS..... ۴۶

غیر فعّال کردن IPV6 ..... ۵۰
بررسی سرویس DHCP ۶۴
فعّال کردن Mac Filtering در سرویس DHCP ۷۸
تخصیص دادن آدرس مشخّص به دستگاه‌های مشخّص ۸۲
سرویس Active Directory ۸۵
نصب و راه‌اندازی سرویس Active Directory ۸۶
بررسی سرویس‌های Active directory ۹۴
تعریف Organization Unit ۹۶
تعریف کاربر در Active directory ۹۷
عضو کردن کلاینت در دومین ۹۹
فعّال‌سازی Remote در سرور ۱۰۵
به اشتراک‌گذاشتن فایل‌ها و فولدرها در شبکه ۱۰۸
بررسی دسترسی‌ها به فولدرها و فایل‌ها ۱۱۴
بررسی گزینه‌ی Advanced در تب Security ۱۱۹
بررسی inheritance در Permissions ۱۲۱
ایجاد گروه در سرویس Active Directory Users and Computers ۱۲۴
عضویّت مدیر شبکه در گروه‌های اصلی ۱۳۲
ارتباط از راه دور با سرویس Active Directory ۱۳۳
ایجاد Domain controller دوّم برای پایدار بودن شبکه ۱۳۵
فعّال‌سازی سرویس NIC Teaming ۱۴۸
نصب و راه‌اندازی سرویس Hyper-V ۱۵۵
ایجاد ماشین مجازی ۱۶۱
ابزار Replication در سرویس Hyper-V ۱۶۵
نصب و راه‌اندازی NANO Server ۱۷۲
عضو کردن Nano Server به سرویس Domain ۱۷۹
نصب و راه‌اندازی سرویس Remote Desktop ۱۸۳
کار با سرویس Remote Desktop از طریق Web ۱۹۵
اجرای نرم‌افزار از طریق سرویس Remote Desktop ۲۲۱
فعّال کردن سرویس Virtual Machine Remote Desktop ۲۲۵
نصب و راه‌اندازی سرویس Remote Access ۲۳۲

راه‌اندازی سرور آنتی ویروس..... ۲۴۵
نصب و راه‌اندازی دوربین مدار بسته..... ۲۵۵
سرور مناسب برای راه‌اندازی دوربین مدار بسته..... ۲۵۷
پیدا کردن دوربین به صورت Discovery..... ۲۶۷
تنظیم نمایش دوربین‌ها..... ۲۶۸
فعّال کردن قابلیّت تشخیص حرکت یا Motion..... ۲۷۲
استخراج تصاویر دوربین..... ۲۷۴
نصب و راه‌اندازی System Center 2016..... ۲۷۶
نصب و راه‌اندازی Microsoft.System.Center. Operations.Manager..... ۲۷۸
نصب و راه‌اندازی Configuration Manager System Center..... ۳۰۴
نصب و راه‌اندازی سرور مانیتورینگ Solarwin..... ۳۴۸
کار با سیستم تحت وب نرم‌افزار مانیتورینگ..... ۳۶۷
فعّال‌سازی Discovery در نرم‌افزار Solar..... ۳۷۱
بررسی کامل سرویس NetFlow..... ۳۸۵
بررسی سرویس NetFlow در روتر میکروتیک..... ۳۸۸
کار با نقشه‌ها در SolarWins..... ۳۹۶
نصب و راه‌اندازی سیستم سانترال..... ۳۹۹
نصب و راه‌اندازی نرم‌افزار مدیریّت تلفن سانترال پاناسونیک..... ۴۰۵
فعّال‌سازی منشی تلفنی در تلفن سانترال..... ۴۱۵
مشخّص کردن تعداد خطهای آزاد برای کاربر..... ۴۱۶
مدیریّت پورت‌ها و بستن آنها در شبکه..... ۴۱۸
بررسی Policy در نرم‌افزار GFI..... ۴۲۹
ایجاد گروه در نرم‌افزار GFI..... ۴۳۹
منابع..... ۴۴۰

مقدّمه:

حدود دو سال پیش که نگارش اوّل کتاب مدیر شبکه را منتشر کردیم، در آن به موضوعات مختلفی پرداختیم که خوشبختانه این کتاب با استقبال بی‌نظیر شما عزیزان همراه بود و بنده را بر آن داشت که نسخه‌ی دوّم آن را نیز منتشر کنم؛ در نسخه‌ی دوّم این کتاب به موضوعات زیر خواهیم پرداخت:

۱- نحوه‌ی انجام کابل‌کشی ساختمان، کار سوئیچ‌ها، پچ پنل‌ها و....
۲- آماده‌سازی اتاق سرور.
۳- نصب و راه‌اندازی ویندوز سرور ۲۰۱٦ به همراه سرویس‌های مهمّ آن.
٤- نصب و راه‌اندازی دوربین مدار بسته.
٥- نصب و راه‌اندازی آنتی‌ویروس تحت شبکه‌ی Nod 32.
٦- نصب و راه‌اندازی سرور مانیتورینگ Solar.
۷- نصب و راه‌اندازی System Center.
۸- نصب و راه‌اندازی نرم‌افزار امنیّتی GFI.

مدیر شبکه در یک سازمان می‌تواند به عنوان یک عنصر کلیدی در پیشبرد اهداف آن مؤثّر باشد؛ در اهمّیّت آن باید گفت از آنجایی که یک مدیر کارآمد شبکه، سهم قابل توجّهی در کیفیّت و ارتقای کاربران ایفا می‌کند، لذا بنده را بر آن داشت تا راهکارهای صحیح مدیریّت را در قالب یک کتاب برای شما همکاران گرامی به نگارش در آورم تا دریچه‌ای هر چند کوچک در موفّقیّت هر چه بیشتر شما در عرصه‌ی فنّاوری اطّلاعات باشد.

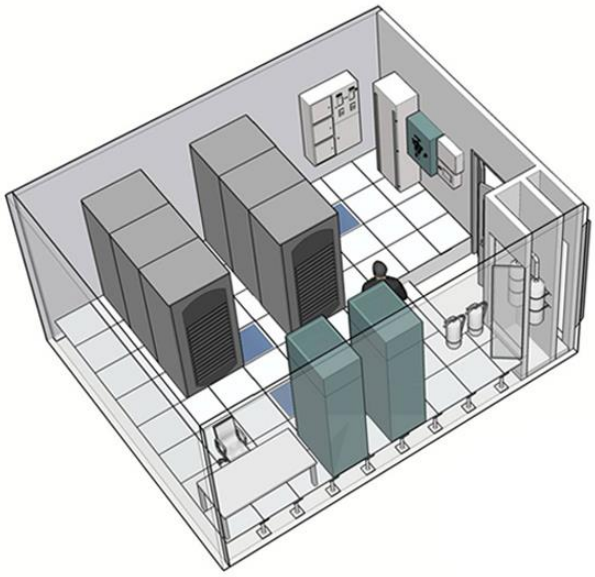
این کتاب را تقدیم می‌دارم به همسر عزیزم که در جستجوی تکانه‌های دانایی همراهم بودند و در میان شکوفه‌های شرم و حضور، بال دیگر نگاهم هستند.

ستون‌های تک تک کلماتم سرشار از احساس و نوازش‌اند، شاید گاهی تکرار واژه‌ای پشت حصار معرفت ایستاده باشد، امّا هرگز تسلیم ندانستن نمی گردد (آزاده تیشه برسر).

طرّاحی و پیاده‌سازی اتاق سرور:

بدون شک هر سازمانی برای سرورهای شبکه‌ی خود، یک اتاق چند در چند متر را در نظر می‌گیرد که در این اتاق، رک‌ها، سرورها، UPS ها و... قرار داده می‌شوند؛ برای اینکه یک اتاق سرور خوب را طرّاحی کنید باید به این نکات توجّه کنید:

اصولاً اندازه و متراژ اتاق سرور بستگی به متراژ کلّ ساختمان دارد، مثلاً برای یک ساختمان با زیربنای ۱۰۰۰ متر، یک اتاق ۱۰ متری کفایت می‌کند، هر چند این ابعاد، بستگی زیادی به تعداد رک‌ها و UPS ها و تجهیزات دیگر شما دارد، مثلاً اگر تعداد رک‌های شما، ۲ عدد باشد و تعداد UPS و یا همان منبع تغذیه، ۲ عدد باشد، یک اتاق ٤ در ٤ متر پاسخگو خواهد بود، این طرز فکر را از خود دور کنید که هر چه اتاق بزرگتر باشد، کارایی سرورها و منظّم شدن کار بهتر خواهد بود، اگر اتاق سرور بزرگتر باشد، به همان اندازه نیز به سیستم سرمایش و تهویّه‌ی خوب نیازمندیم که این موضوع باعث بالا رفتن هزینه‌ها خواهد شد، به این نکته نیز توجّه کنید که همیشه اتاق سرور در طبقه‌ی اوّل یک ساختمان قرار می‌گیرد.



آماده‌سازی اتاق سرور:



قبل از قرار دادن تجهیزات در اتاق سرور باید کارهایی را قبل از آن انجام دهید که عبارتند از:

کانال‌های عبوری برای انتقال کابل‌ها باید قبل از هر کاری مشخّص شده باشند تا در ادامه‌ی کار برای خروج کابل از اتاق به طبقات دیگر با مشکل مواجه نشوید.



برای انتقال کابل می‌توانید از قفسه‌های مورد نظر که در شکل مشاهده می‌کنید، استفاده کنید. یکی از نکات مهمّی که باید در انتقال کابل‌ها از طریق کانال به آن توجّه کنید، این است که کابل‌های برق را از کابل شبکه جدا کنید تا با مشکل نویز مواجه نشوید.

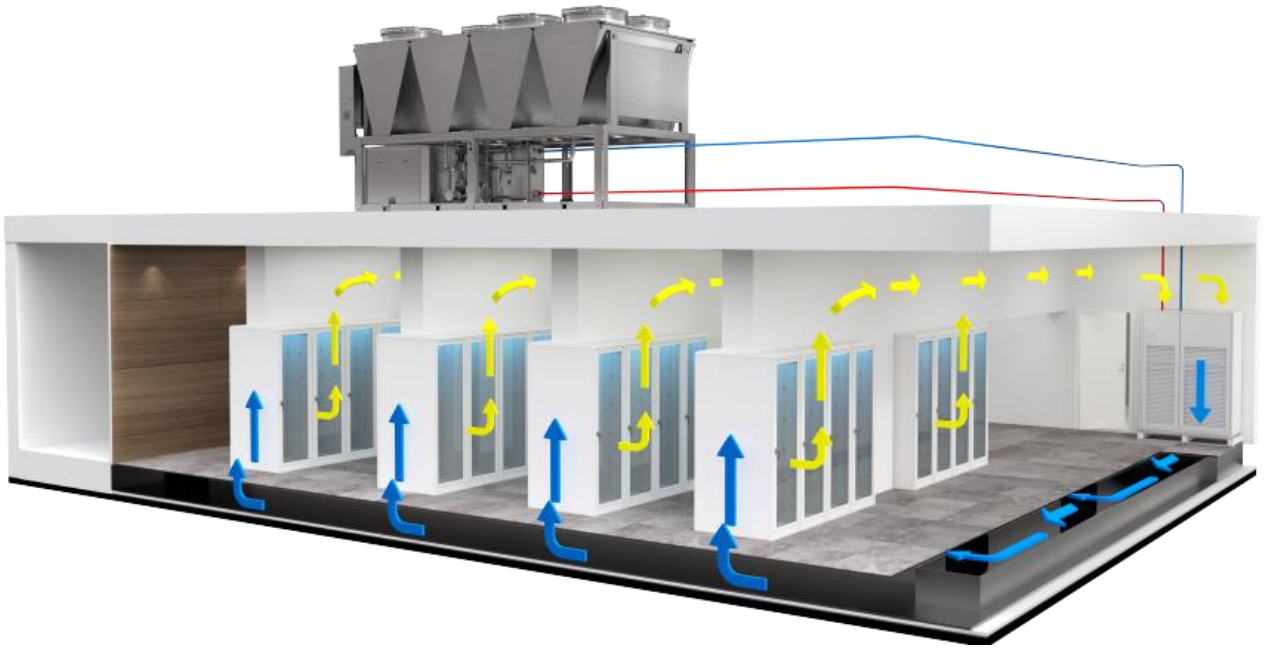
سیستم‌هایی که می‌توان در اتاق سرور برای حفظ امنیّت سرورها استفاده کرد به صورت زیر است.

سیستم سرمایشی مناسب:

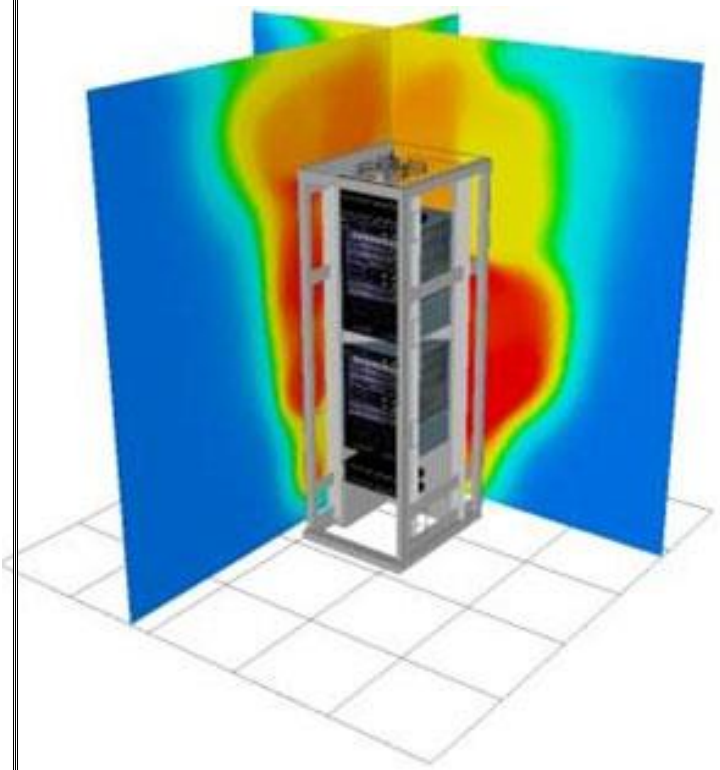
برای اینکه دستگاه‌ها، کیفیّت و کارایی خود را حفظ کنند باید از سیستم سرمایشی و تهویّه‌ی مناسب استفاده کنید که در اکثر جاها از کولرهای گازی استفاده می‌کنند، دمای اتاق باید چیزی بین ۱۸ تا ۲۳ درجه سانتیگراد باشد، برای اینکه بتوانید از حداکثر کارایی کولر استفاده کنید، بهترین کار این است که تمام منافذی که به بیرون از اتاق راه دارد را ببندید، مانند زیر درها، لبه‌ی پنجره‌ها و یا سوراخ‌هایی که وجود دارد را مثلاً با گچ پر کنید تا سیستم سرمایشی تنها در داخل اتاق عمل کند و به بیرون راه نداشته باشد.



در شکل روبرو، یک سیستم سرمایشی پیشرفته‌تر از کولرهای گازی را مشاهده می‌کنید که دستگاه تهویّه‌ی هوا در بالای ساختمان تعبیه شده و از طریق لوله‌کشی به داخل اتاق سرور انتقال داده شده است.



در شکل بالا، نوع پیشرفته‌تری از سیستم تهویّه‌ی هوا را مشاهده می‌کنید که نحوه‌ی گردش هوا در اتاق سرور مشخّص شده است، به این نکته نیز توجّه داشته باشید که این نوع سیستم‌ها، تنها برای اتاق سرورهای بزرگ کارایی دارد.



نکته‌ی مهم در قرار دادن رک در اتاق این است که اگر رک را در کنار دیوار قرار دهید، به مانند شکل روبرو، سرورها در مجاورت گرمای بیشتری قرار می‌گیرند که حتماً باید رک‌ها را در وسط اتاق قرار دهید.

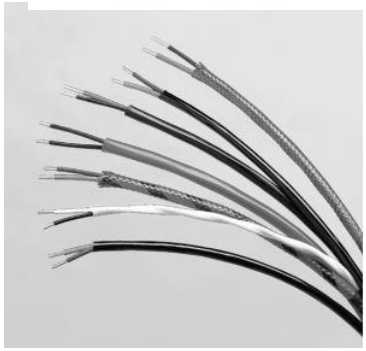
سیستم اطفای حریق:

برای اینکه بتوانید در هر لحظه، دمای اتاق سرور را کنترل کنید، بهترین راه، استفاده از سیستم‌های اطفای حریق است، در این سیستم‌ها یک سنسور حسّاس به گرما در اتاق قرار داده می‌شود که اگر میزان دمای اتاق سرور بنا به هر دلیلی، مثلاً از ۳۰ درجه سانتیگراد بالاتر رفت، آژیر خطر به صدا درآید و یا از طریق تلفن، شما را در جریان کار قرار دهد.

سیستم‌های اطفای حریق از طریق کابل خطّی، دتکتور دود، دتکتور حرارت، متوجّه‌ی وجود گرما یا دود درون اتاق سرور می‌شوند و اطّلاعات را به دستگاه کنترل ارسال می‌کنند تا آژیر به صدا در آید، اصولاً بر روی رک‌ها، دماسنجی تعبیه شده است که این دماسنج را می‌توانید به دستگاه کنترل حریق متّصل کنید تا اگر میزان دما از حدّ مجاز بالاتر رفت، آژیر به صدا در آید.



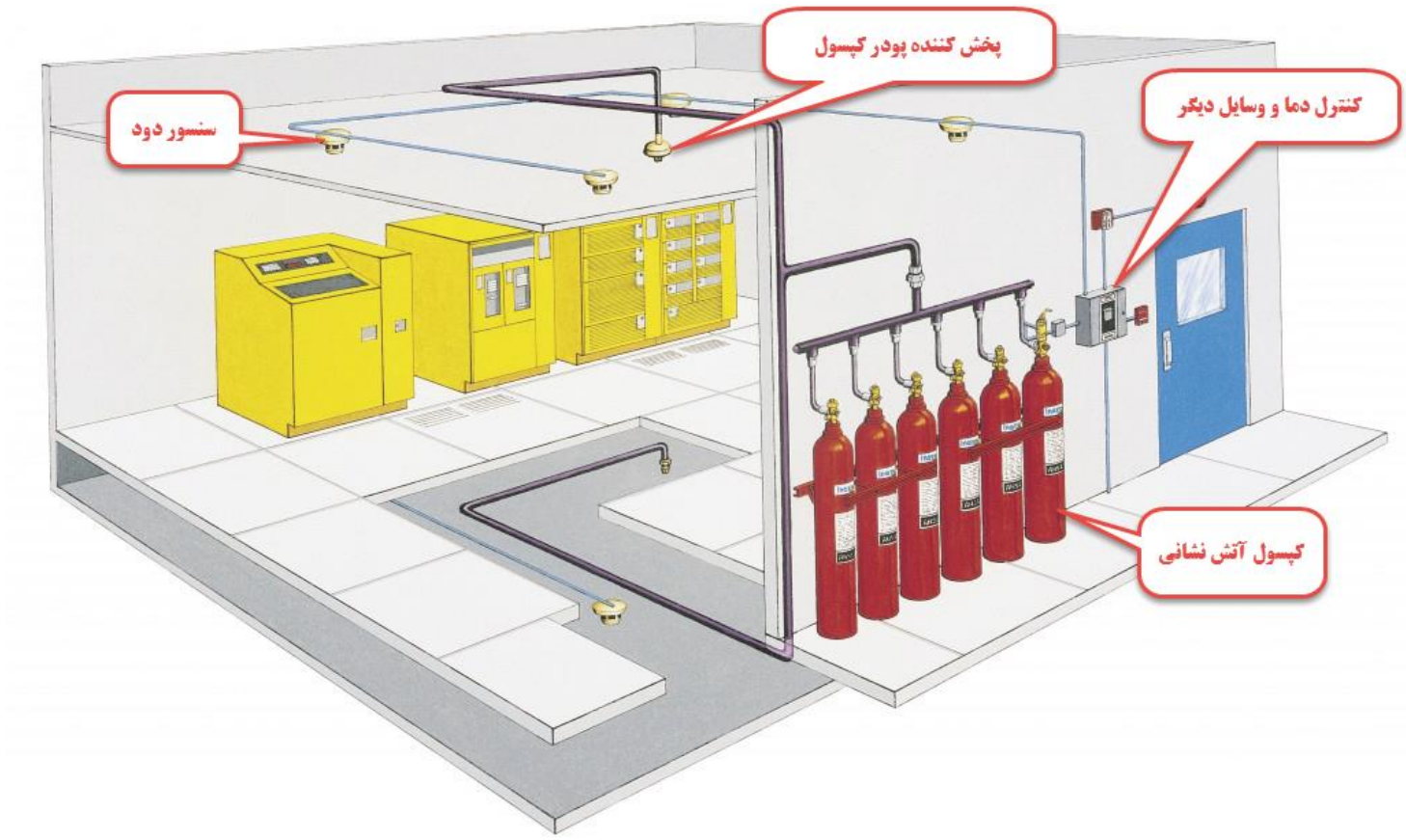
در شکل روبرو، نمونه‌ای از دتکتور دود را مشاهده می‌کنید که بعد از اینکه دود در سنسورهای آن دریافت شد، آژیر خطر به صدا در خواهد آمد.



در شکل روبرو، کابل‌های خطّی حرارتی را مشاهده می‌کنید که دمای اتاق را به دماسنج ارسال می‌کنند و با این کار، دما کنترل می‌شود.



سیستم‌های کنترل رطوبت اتاق سرور نیز وجود دارند که رطوبت داخل اتاق را اندازه‌گیری می کنند و اگر از حدّ مجاز عبور کنند، دستگاه تهویّه‌ی هوا روشن می‌شود.



در شکل بالا، نمونه‌ی طرّاحی‌شده‌ی یک اتاق سرور را مشاهده می‌کنید که بخش‌های مختلف آن در تصویر مشخّص شده است، اگر چنانچه آتش‌سوزی رخ دهد، دود و حرارت آن توسط سنسور دود که در شکل مشخّص شده است به دستگاه کنترل، فرستاده خواهد شد و همزمان، آژیر و چراغ روشن خواهد شد و بعد از آن پودر کپسول آتش‌نشانی از طریق پخش‌کننده‌ی پودر در کلّ اتاق به صورت فشار قوی پخش می‌شود و آتش مورد نظر خاموش خواهد شد.



با انجام مراحل بالا می‌توانید اتاق سرور خوب و با امنیّتی ایجاد کنید.

در شکل روبرو، یک اتاق سرور با تعداد زیادی رک و سرور را مشاهده می‌کنید که در آتش سوخته است.

انواع رک‌ها:

برای اینکه سرورها به صورت منظّم و با امنیّت بیشتر در اتاق سرور قرار دهید، بهتر است به تعداد مورد نیاز رک ایستاده تهیّه کنید، رک‌ها در مدل‌های مختلفی وجود دارند که در زیر نگاهی به آنها می‌اندازیم:

نکته: واحد اندازه‌گیری رک، یونیت می‌باشد که هر یونیت، برابر با ٤,٤٤٥ سانتیمتر است.



در شکل روبرو، یک رک ایستاده را مشاهده می‌کنید که با ارتفاع ٤٧ یونیت و با عمق ۱۰۰ سانتی‌متر است که مخصوص اتاق سرورهای معمولی است و وزنی حدود ۲۵۰ کیلوگرم را تحمّل می‌کند. انتخاب نوع رک، بستگی به تعداد سرورهای شما در آن سازمان دارد، باید ببینید تعداد سرورهای شما چند عدد است و وزن تقریبی آن را حتماً باید به دست آورید تا بتوانید رک متناسب با آن وزن را خریداری کنید، اگر چنانچه رک درستی را انتخاب نکنید، سنگینی سرورهای سوار شده روی رک باعث می‌شود پایه‌های رک بشکند و باعث واژگونی آن شود که کار جالبی نخواهد بود.

رک‌ها در مدل‌های مختلفی وجود دارند که در زیر آنها را بررسی می‌کنیم.

رک دیواری:



این مدل رک‌ها در ابعاد کوچک و برای قرار گرفتن سوئیچ‌ها در آن استفاده می‌شود، شاید این مدل رک‌ها را در سازمان‌های مختلف مشاهده کردید، رک‌های دیواری در اندازه‌های ٤، ٦، ۹، ۱۲ یونیت موجود می‌باشند که نمونه‌ای از رک ۹ یونیت را در شکل روبرو مشاهده می‌کنید.

اصولاً این نوع رک‌ها دارای یک عدد فن و چند راهی برق می‌باشند و در بیشتر مدل‌های امروزی، درب آن از هر سه طرف چپ، راست و جلو باز می‌شود.



رک ایستاده:

این نوع رک‌ها به صورت ایستاده موجود هستند و کاربرد آنها در تحت پوشش قرار دادن سرورها، سوئیچ‌ها، فایروال‌ها و... است که در بازار، در ابعاد مختلف ۱۷، ۲۲، ۲۷، ۳۲ ، ۳۷، ۴۲ موجود است که باید به اندازه‌ی نیاز خود، یک رک مناسب تهیّه کنید.

بعضی از رک‌ها به صورت پیش‌فرض بر روی خود، KVM سوئیچ دارند که این کار برای متّصل کردن همه‌ی سرورها به یک مانیتور برای مدیریّت بهتر است، البتّه در بعضی دیگر از رک‌ها، مانیتور نیز تعبیه شده است که به صورت کشویی، باز و بسته می‌شود.



در تصویر روبرو، دو رک ایستاده را در کنار هم مشاهده می‌کنید که سرورها بر روی آنها سوار شده است و بر روی یکی از این رک‌ها، مانیتور قرار داده شده است تا بتوانید از طریق سوئیچ، همه‌ی سرورها را مدیریّت کنید.

انتخاب سوئیچ مناسب در شبکه:

مهمترین چیزی که در تمام شبکه‌ها، سرعت آن را تضمین می‌کند، انتخاب یک سوئیچ مناسب برای شبکه‌ی خود است.

سوئیچ‌ها در تنوّع و برندهای متفاوتی وجود دارند که مثل همیشه، برند سیسکو بهترین انتخاب برای شما می‌باشد، هر چند دستگاه‌های سیسکو از قیمت بالاتری نسبت به برند های دیگر برخوردارند، امّا می‌توانند کیفیّت شبکه‌ی شما را تضمین کنند.

برای انتخاب سوئیچ سعی کنید، سرعت مناسب آن را با شبکه‌ی خود انتخاب کنید، در حال حاضر سرعت سوئیچ‌ها بین ۱۰/۱۰۰/۱۰۰۰ متغیّر است، انتخاب سرعت ۱۰۰۰ در سوئیچ می‌تواند مقدار سرعت شبکه‌ی شما را افزایش دهد، هر چند این انتخاب بستگی مستقیم به کابل شبکه‌ی شما دارد که کیفیّت خوبی داشته باشد.

پرفروش‌ترین و بهترین سوئیچ سیسکو در قیمت مناسب و معمول، سوئیچ ۲۹٦۰ آن است که در دو نوع ۲٤ و ٤۸ در بازار موجود است، این سوئیچ کاملاً پایدار است و اگر در شرایط خوب باشند، قطعی و خرابی در آن، خیلی کم است.



در شکل بالا، یک سوئیچ ۲۹٦۰ سیسکو را مشاهده می‌کنید که دارای ٤۸ پورت شبکه است و برای استفاده در رک، انتخاب خوبی است.

برندهای مختلفی برای سوئیچ‌ها وجود دارد، مانند Asus، Dlink، TPLink، OnLevel، 3com و... که هر کدام در جای خود می توانند خوب باشند.

اگر قصد دارید شبکه‌ی خود را طوری طرّاحی کنید که از عملکرد کاملاً پایداری بهره ببرد، بهتر آن است که از سوئیچ‌هایی با سرعت ۱۰۰۰ یا همان ۱ گیگ استفاده کنید تا شبکه در بهترین حالت خود قرار گیرد.



در شکل بالا، یک سوئیچ سیسکو مدل Cisco SG300-28 را می‌بینید که دارای ۲۸ پورت گیگا اترنت است و حداکثر سرعت انتقال آن، ۱ گیگابایت است که این سرعت برای یک شبکه، بسیار عالی است، به این نکته نیز توجّه کنید که برای به دست آوردن این سرعت باید از کابل شبکه‌های CAT 6e و CAT 7 استفاده کنید.

سوئیچ‌های دیگری نیز از برندهای دیگر وجود دارند که عملکرد خوبی از خود به جای گذاشتند، یکی از این نوع سوئیچ‌ها، TP-Link 24-Port (TL-SG1024) است که از کیفیّت خوبی برخوردار است و می‌تواند شما را در بهبود سرعت و عملکرد شبکه کمک کند، تنها به این نکته توجّه کنید که این نوع سوئیچ، توانایی مدیریّت ندارد و صرفاً یک سوئیچ است و نمی‌توانید مانند سیسکو تنظیمات خود را بر روی آن انجام دهید.



انتخاب کابل مناسب:

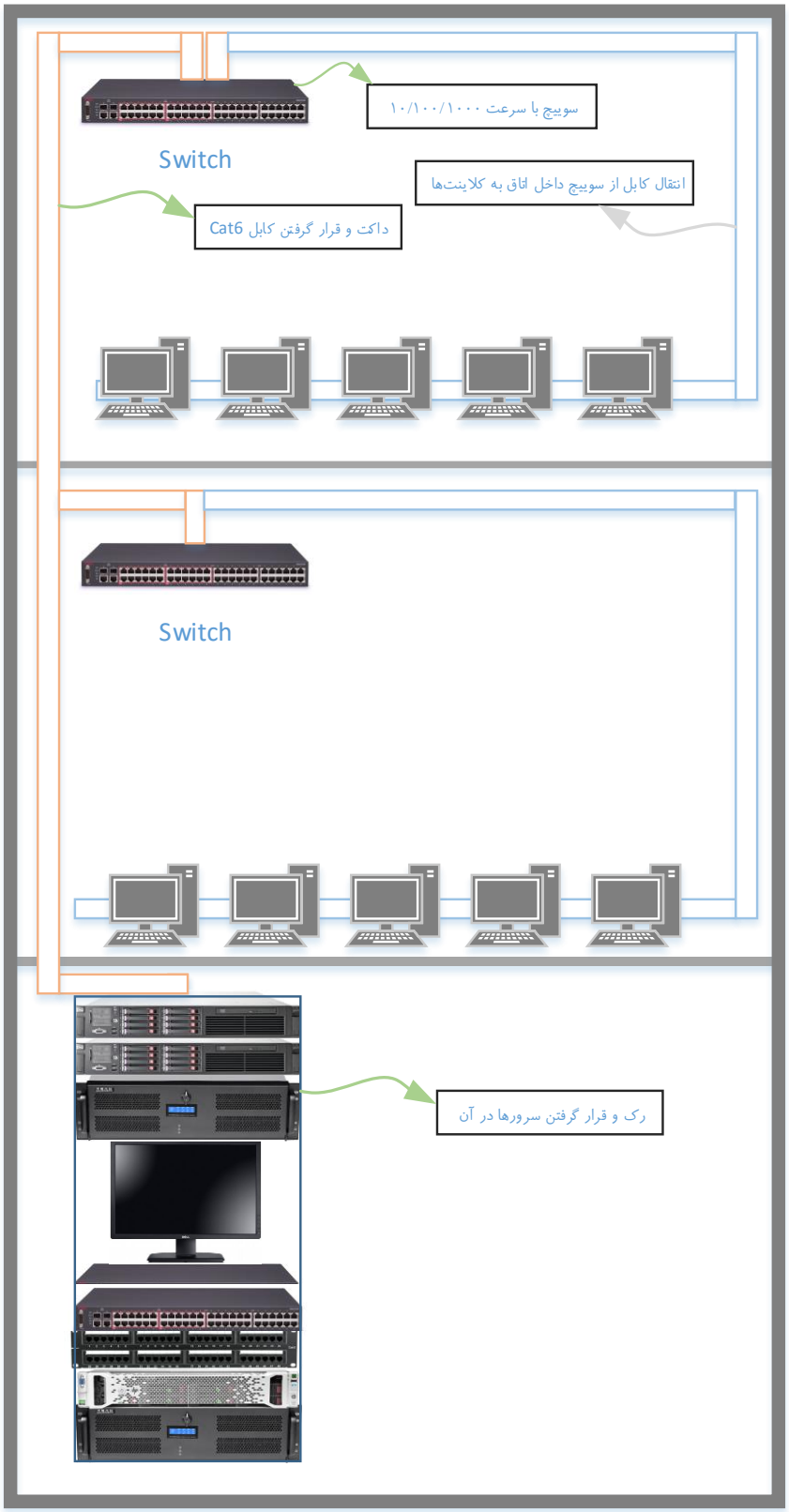
کابل شبکه یکی از زیرساخت‌های مهم در شبکه است که اگر کابل مناسب شبکه‌ی خود را انتخاب نکنید با مشکلات زیادی مواجه خواهید شد.

کابل‌ها در انواع مختلفی وجود دارند که مشخّصات آنها را در زیر مشاهده می‌کنید:

کابل	قطر کابل	حداکثر پهنای باند	حداکثر نرخ ارسال	کاربردها
Cat1	–	100 KHZ	144Kbps	**مودم و فاکس**
Cat2	–	1MHZ	2Mbps	**ISDN**
Cat3	–	16MHZ	10Mbps	**سیم‌های تلفن**
Cat4	–	20MHZ	16Mbps	**شبکه‌هایی، مثل TOKen**
Cat5	٥,٥–٤,٧	100MHZ	100Mbps	**اترنت سریع 100Base-T**
Cat5e	٥,٥–٤,٧	100MHZ	1000Mbps	**اترنت گیگابیتی**
Cat6	٦,٠–٥,٢	250MHZ	1000Mbps	**اترنت گیگابیتی**
Cat7	–	600MHZ	>1000Mbps	**اترنت ۱۰ گیگابیتی**

در حال حاضر بهترین انتخاب برای کابل شبکه در یک سازمان، کابل CAT6 است که تمام نیازمندی‌های یک شبکه را پاسخگو خواهد بود و قیمت آن نسبت به کابل CAT7 که یک کابل تازه وارد است، بسیار کمتر است. حداکثر طول ارسال کابل CAT6 برابر است با ۱۰۰ متر به بالا که این طول می‌تواند بین دو طبقه و بین دو سوئیچ کافی باشد.

به این نکته نیز توجّه کنید که به هیچ عنوان در کنار کابل شبکه، کابل برق قرار ندهید، در صورتی که کابل مورد نظر قابلیّت جذب نویز را داشته باشد در کار شبکه با اختلال مواجه خواهید شد و این می‌تواند بزرگترین مشکل در شبکه باشد، چون پیدا کردن اشکال کار در چنین مواقعی بسیار دشوار است.


سوییچ با سرعت ۱۰/۱۰۰/۱۰۰۰
Switch
انتقال کابل از سوییچ داخل اتاق به کلاینت‌ها
داکت و قرار گرفتن کابل Cat6
Switch
رک و قرار گرفتن سرورها در آن

در شکل صفحه‌ی پیش، یک ساختمان شماتیک را رسم کردیم که در طبقه‌ی همکف آن، اتاق سرور قرار دارد که در داخل این اتاق سرور، یک رک با تعدادی سرور، سوئیچ، پچ پنل و مانیتور قرار دارد، برای اینکه سرعت و کیفیّت کار افزایش پیدا کند از یک سوئیچ معمولی با سرعت ۱۰۰۰/۱۰۰/۱۰ استفاده کردیم و کابل شبکه را نیز از نوع CAT6 در نظر گرفتیم، برای انتقال کابل‌ها به طبقات و اتاق‌های دیگر باید از داکت استفاده کنیم.

داکت:

داکت به لوله‌ها و محفظه‌های پلاستیکی یا فلزی گفته می‌شود که برای انتقال کابل در شبکه مورد استفاده قرار می‌گیرد. داکت‌ها در اندازه‌ها و کیفیّت‌های مختلفی وجود دارند که هر کدام برای کار خاصّی مورد استفاده قرار می‌گیرند.



اندازه‌ی داکت‌ها به صورت زیر است:

- **داکت ۱:** با اندازه‌ی ۱۰*۱۰ میلی‌متر و طول ۲ متر برای هر شاخه.
- **داکت ۱,۵:** با اندازه‌ی ۱۵*۱۰ میلی‌متر و طول ۲ متر برای هر شاخه.
- **داکت ۲:** با اندازه‌ی ۲۰*۲۰ میلی‌متر و طول ۲ متر برای هر شاخه.
- **داکت ۲,۵:** با اندازه‌ی ۲۰*۲۵ میلی‌متر و طول ۲ متر برای هر شاخه.
- **داکت ۳ معمولی:** با اندازه‌ی ۳۰*۳۰ میلی‌متر و طول ۲ متر برای هر شاخه.
- **داکت ۳ ارتفاع کوتاه:** با اندازه‌ی ۱۵*۳۰ میلی‌متر و طول ۲ متر برای هر شاخه.
- **داکت ۳,۵:** با اندازه‌ی ٤٥*۳۵ میلی‌متر و طول ۲ متر برای هر شاخه.

- **داکت ٤:** با اندازه‌ی ۳۰*٤۰ میلی‌متر و طول ۲ متر برای هر شاخه.
- **داکت ٥:** با اندازه‌ی ۳۰*٥۰ میلی‌متر و طول ۲ متر برای هر شاخه.
- **داکت ٦ معمولی:** با اندازه‌ی ٤٥*٦۰ میلی‌متر و طول ۲ متر برای هر شاخه.
- **داکت ٦ پایه بلند:** با اندازه‌ی ٦۰*٦۰ میلی‌متر و طول ۲ متر برای هر شاخه.
- **داکت ۹ معمولی:** با اندازه‌ی ٤٥*۹۰ میلی‌متر و طول ۲ متر برای هر شاخه.
- **داکت ۹ پایه بلند:** با اندازه‌ی ٦۰*۹۰ میلی‌متر و طول ۲ متر برای هر شاخه.



داکت‌ها در انواع زمینی نیز وجود دارند که برای انتقال کابل مورد استفاده قرار می‌گیرند، در تصویر روبرو یک طرح چوبی از داکت زمینی را مشاهده می‌کنید.

برگردیم به همان شکل قبلی که در مورد شبکه‌ی ساختمان بود، بعد از اینکه داکت‌کشی را برای کلّ ساختمان انجام دادید، نوبت به کابل‌کشی ساختمان است که باید از یک کابل با کیفیّت CAT6 برای این کار استفاده کنید تا در آینده با مشکلی مواجه نشوید.

سعی کنید این نکات را در کابل‌کشی توجّه کنید:

۱- حتماً از یک کارشناس با تجربه در این خصوص بهره مند شوید.

۲- استفاده از لوله‌های PVC، مانند کانال‌های برق در دیوارها.

۳- استفاده از فضای مناسب برای تعداد کابل پیش‌بینی شده و کمی بیشتر برای مواقع ضروری.

٤- استفاده از قوس‌های مناسب در هنگام کابل‌کشی (عدم شکستن کابل در هنگام کابل‌کشی)

۵- شناسایی نودهای شبکه که بسیار مهم است، پس تا جای ممکن، بیشترین پیش‌بینی را مدّ نظر خود قرار دهید. در بسیاری از شرکت‌ها، علاوه بر اینکه پیش‌بینی‌هایی برای سخت‌افزارهای شبکه، مانند پرینترهای تحت شبکه و نیز دوربین‌های مدار بسته را انجام می‌دهند، برای هر ایستگاه کاری، ۲ نود شبکه پیش‌بینی می‌شود که در آینده، امکان استفاده از سیستم‌های تلفن دیجیتال نیز وجود داشته باشد.

٦- بسته به تعداد نودهای به کار گرفته شده در هر طبقه از یک، یا دو سوئیچ و یا بیشتر استفاده کنید.

۷- سعی کنید ارتباط طبقات با مرکز دیتا به صورت مستقیم و در یک راستا و با حداقل ۲ کابل مجزّا که یکی به عنوان Backup در نظر گرفته می شود، صورت بگیرد.

۸- در ساختمان حتماً محلّی برای انتقال کابل‌ها، پیش‌بینی کنید تا امکان کابل‌کشی‌های بیشتر را برای آینده ممکن سازد.

۹- سعی کنید در کابل‌کشی‌ها از کابل‌هایی با کیفیّت و تا جای ممکن، شیلد دار و با ضمانت تست، تهیّه و اجراکنید.

۱۰- در صورت استفاده از فایبر برای ارتباطات، حتماً از قبل محلّ عبور آن را پیش‌بینی کنید.

۱۱- اندازه‌ی patch cord های ایستگاه‌ها، بیشتر از ۳ متر نباشد.

۱۲- ارتباط میان پریزهای ایستگاه‌ها تا رک مورد نظر، بیشتر از ۹۰ متر نباشد.

۱۳- برای هر طبقه، حداقل یک عدد رک IDF وجود داشته باشد.

١٤- برای هر ساختمان، حداقل یک عدد رک MDF وجود داشته باشد.

۱۵- به ازای فضایی با شعاع ۹۰ متر باید یک رک IDF استفاده شود.

١٦- IDF ها هرگز به طور مستقیم با یکدیگر ارتباط برقرار نمی‌کنند و تمام آنها باید مستقیم با MDF ارتباط داشته باشند.

۱۷- درجه‌ی حرارت رک‌های MDF و IDF نباید بیش از ۲۵ درجه سانتیگراد باشد.

۱۸- در درون رک‌ها از لامپ‌های کم مصرف و مهتابی به دلیل ایجاد نویز استفاده نکنید.

۱۹- منابع تولید نویز در نزدیکی رک‌ها وجود نداشته باشد.

۲۰- لازم است در اتاق‌های دیتا از فیلترهای هوا استفاده شود

۲۱- امنیّت فیزیکی اتاق‌های دیتا باید کاملاً رعایت گردد.

۲۲- ارتفاع اتاق‌های دیتا نباید از ۲٫۸ متر کمتر باشد.

۲۳- درجه‌ی حرارت اتاق دیتا باید بین ۱۸ الی ۲٤ باشد.

۲٤- رطوبت اتاق دیتا، حداکثر بین ۳۰ - ۵۰ درصد می‌تواند باشد

۲۵- پیش‌بینی سیستم‌های اطفای حریق و نصب هشدار دهنده‌های دود و حرارت در این اتاق‌ها الزامی است.

۲٦- کابل‌کشی را به عنوان یک سیستم مستقل به شرکتی بسپارید که صرفاً همین کار را انجام می‌دهد.

۲۷- مستندسازی را هرگز فراموش نکنید.

۲۸- همیشه از بهترین برندها در این عرصه استفاده کنید.

۲۹- حتماً در کابل‌کشی‌های خود، یک استاندارد جهانی را دنبال کنید.

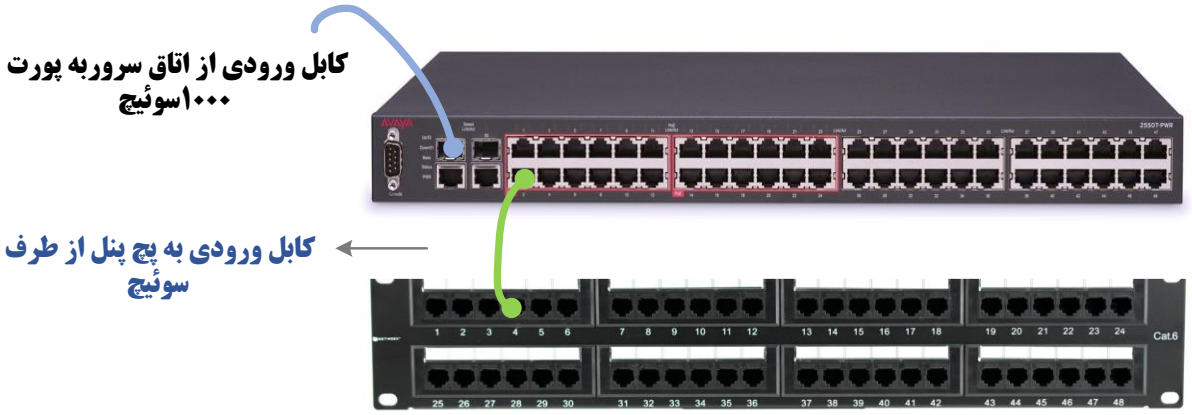
۳۰- در خصوص انتخاب کابل و تجهیزات، تنها به کیفیّت آن فکر کنید.

در گزینه‌های بالا به IDF و MDF اشاره کردیم که منظور از MDF، همان رک دیواری است که سوئیچ در آن قرار می‌گیرد و LDF، محلّ قرار گرفتن کابل‌ها در هر اتاق یک ساختمان است.

برای کابل‌کشی از اتاق سرور به اتاق کاربران می‌توانید برای هر اتاق، یک کابل مستقیم از اتاق سرور به همان اتاق بکشید و یا از سوئیچ‌های بین راه استفاده کنید، یعنی از یک کابل استفاده کنید و به سوئیچ طبقه‌ی اوّل که پورت ۱۰۰۰ دارد، متّصل کنید و دوباره از پورت ۱۰۰۰ دوّم که اصولاً بر روی سوئیچ دو پورت ۱۰۰۰ تعبیه شده است، یک کابل به طبقه‌ی بعدی که سوئیچ در آن قرار دارد، بکشید.

بررسی پچ پنل در رک:

بعد از اینکه کابل را از اتاق سرور وارد اتاق بعدی کردید و به سوئیچ متّصل شده در رک دیواری متّصل نمودید باید تمام کابل‌هایی که به کلاینت‌ها متّصل می‌شوند را به پچ پنل متّصل کنید.

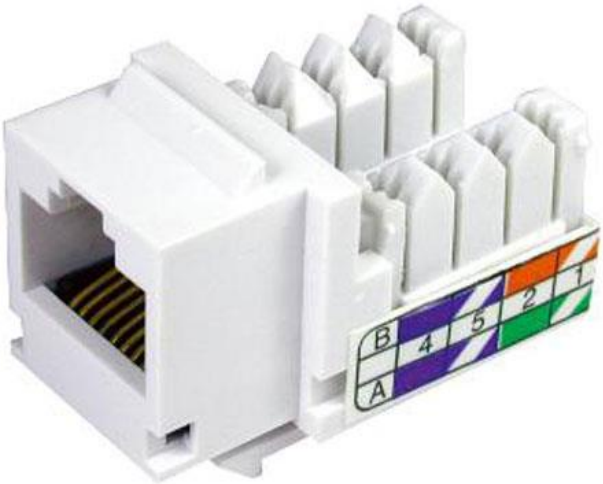


در شکل بالا، یک سوئیچ و پچ پنل را مشاهده می‌کنید که کابلی که از اتاق سرور، مثلاً به طبقه‌ی دوّم رفته، مستقیم وارد پورت ۱۰۰۰ سوئیچ شده است، بعد از آن می‌توانید از طریق سوئیچ، کابل را به پچ پنل متّصل کنید.

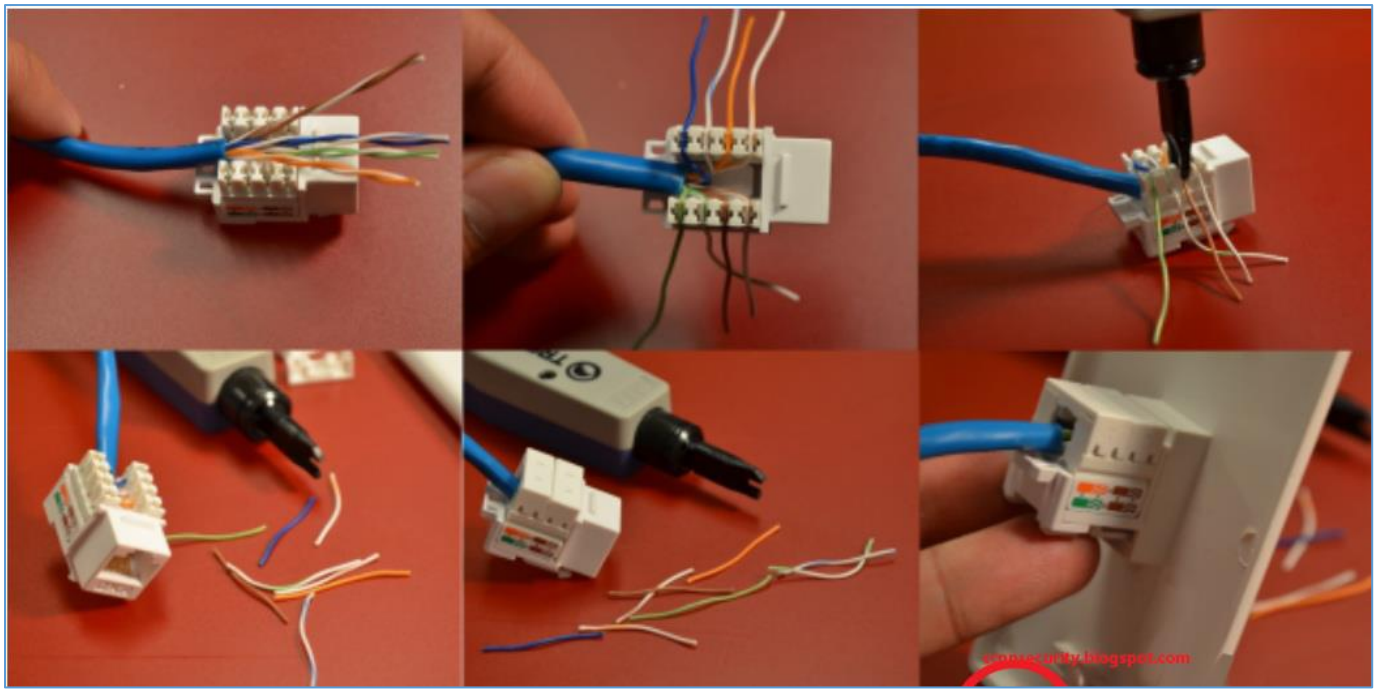


پچ پنل یک رابط بین سیستم‌ها و دستگاه‌ها در یک طبقه با سوئیچ است که ارتباط بین این دو را برقرار می‌کند، یعنی تمام کابل‌هایی که از اتاق سرور وارد رک دیواری می‌شوند، به مانند شکل روبرو به صورت مدیریّت شده بر روی پچ پنل قرار می‌گیرند و بعد از آن، یک کابل کوتاه بین سوئیچ و پچ پنل قرار می‌گیرد که ارتباط بین آنها را برقرار می‌کند.

کیستون:



کیستون یا همان پریز شبکه، قطعه‌ی ارتباطی بین کلاینت‌ها با سوئیچ، روتر و دیگر ادوات شبکه است که بسیار پرکاربرد است، در قسمت قبل که پچ پنل را بررسی کردیم، این قطعه، یعنی کیستون جزئی از پچ پنل است که کابل‌ها، به مانند شکل روبرو و بر اساس رنگ‌بندی روی آن قرار می‌گیرند.



در شکل بالا، نحوه‌ی قرار دادن کابل به صورت مشخّص نشان داده است که این کار از طریق آچار مختص به آن انجام می‌گیرد.



آچاری که برای قرار دادن کابل در کیستون مورد استفاده قرار می‌گیرد، مانند شکل روبرو است.

نکته: برای اینکه کیفیّت کار حفظ شود و در آینده با مشکل مواجه نشوید، بهتر است، پچ پنل، کیستون و کابل از یک برند باشند تا به حداکثر کیفیّت دست پیدا کنید.

بررسی UPS در شبکه:

UPS (Uninterruptible power supply) یا همان منبع تغذیه، وسیله‌ای است که در کنار یک رایانه (یا مصرف کننده‌ی برقی دیگر) نصب می‌شود و هنگام قطع یا تغییرات شدید ولتاژ ورودی، امکان ادامه‌ی کار در حالت نرمال را برای مصرف کننده فراهم می‌کند.



UPS های کوچک معمولاً درون خود، یک باتری دارند که هنگام وجود برق در حالت عادی آن را شارژ می‌کنند؛ هنگام قطع برق یا افت ولتاژ، زمانی‌که ولتاژ از یک مقدار کمتر شود، UPS به طور اتوماتیک منبع تغذیه رایانه را از برق شهر به باتری موجود درون خود تغییر می‌دهد، این کار در زمانی حدود یک یا ۲ میلی‌ثانیه انجام می‌پذیرد و در نتیجه، رایانه متوجّه‌ی قطع جریان الکتریکی نمی‌شود و به کار خود ادامه می‌دهد.



UPS ها در اندازه‌ها و قدرت‌های مختلفی وجود دارند که نمونه‌ای از آنها را در شکل روبرو مشاهده می‌کنید، بعضی از UPS ها برای شارژ دستگاه‌های شبکه از باطری جداگانه استفاده می‌کنند که در شکل زیر آن را مشاهده می‌کنید.



همانطور که مشاهده می‌کنید، باطری‌ها به صورت سری و پشت سر هم به یکدیگر متّصل شده‌اند و بعد به دستگاه UPS متّصل می‌شوند.

انتخاب قدرت UPS، بستگی مستقیم به تعداد سرورهای شما در اتاق سرور دارد.

راه‌اندازی سرورها:

بعد از اینکه اتاق سرور را آماده کردید باید سرورهای مورد نظر خود را برای راه‌اندازی یک شبکه‌ی عالی آماده کنید، این سرورها می‌توانند انواع مختلفی باشند، مانند Active Directory، Sharepoint، Backup و... که هر کدام باید به خوبی آماده و کانفیگ شوند.



برای انتخاب نوع کیس و سخت‌افزار، انتخاب‌های متفاوتی دارید، مثلاً می‌توانید یک کیس سروری خریداری کنید و آن را بر روی روی رک قرار دهید که مثالی از آن را در شکل روبرو مشاهده می‌کنید، این سرورها به صورت کشویی وارد رک شده و از چهار طرف پیچ می‌شوند.



سرورهای دیگری هم وجود دارند که به صورت یک سیستم آماده، ارائه می‌شوند، مانند سرورهای HP، Dell، IBM و... که در مورد این نوع سرورها در کتاب مدیر شبکه‌ی یک توضیحات لازم را دادیم، در شکل روبرو یک سرور HP G9 را مشاهده می‌کنید که از سخت‌افزار قدرتمندی برخوردار است و با کانفیگ آن و نصب سیستم عامل ESXi می‌توانید به راحتی چندین سرور را به صورت مجازی در آن راه‌اندازی کنید، همانطور که اشاره کردیم در مورد سرور HP و سیستم عامل قدرتمند ESXI در کتاب مدیر شبکه‌ی یک به صورت مفصّل، توضیحات لازم را دادیم که با تهیّه‌ی این کتاب می‌توانید در مورد این سرورها و نوع استفاده‌ی آنها اطّلاعات مورد نظر خودتان را دریافت کنید.

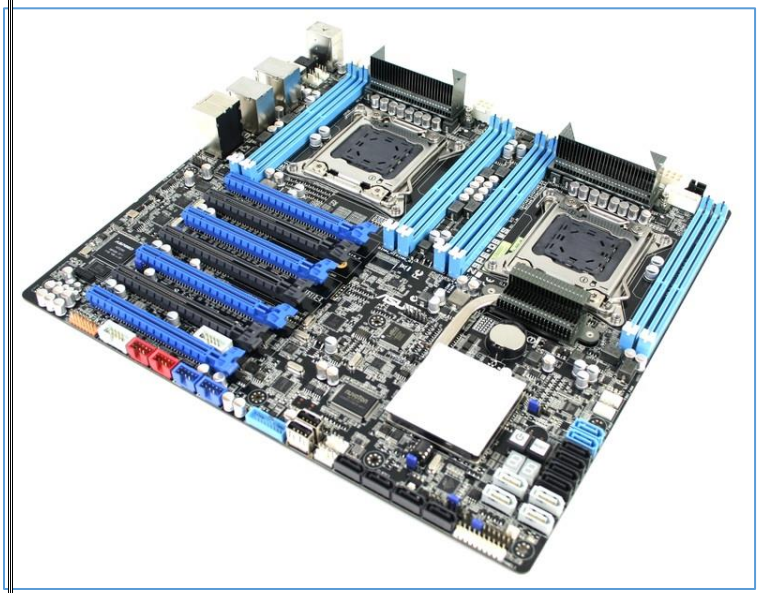


همانطور که در شکل روبرو مشاهده می‌کنید، سرور به صورت کشویی وارد رک شده و از هر چهار طرف به رک پیچ شده است، توجّه داشته باشید در زیر این سرورها، یک سینی قرار می‌گیرد تا نگه دارنده‌ی سرور باشد، برای اینکه حمل و نقل سرورها آسان‌تر باشد به آن دو دستگیره پیچ می‌کنند.

این نوع کیس‌های سرور در کیفیّت و قیمت‌های مختلفی وجود دارند که حداقل قیمت این نوع کیس‌ها را می‌توان ۱۵۰ هزار تومان تخمین زد. در ایران، بهترین مارک پر طرفدار، مارک Green است که کیفیّت نسبتاً خوبی در کیس و نیز در پاور دارد.

همانطور که گفتیم در این کتاب به بررسی کیس‌های سروری می‌پردازیم و اطّلاعات آن را بررسی می‌کنیم.

انتخاب مادربرد:



برای اینکه کیفیّت کار را در شبکه حفظ کنید باید سخت‌افزارهایی تهیّه کنید که کیفیّت لازم و دوام کافی در دراز مدّت را داشته باشند، برای تهیّه مادربرد برای سرور باید نوع مادربرد خود را از نوع سرور در نظر بگیرید، در شکل روبرو یک مادربرد سرور از برند Asus را مشاهده می‌کنید که دارای دو اسلات سی پی یو و ۸ اسلات رم است.

انتخاب CPU:



برای اینکه یک پردازنده‌ی خوب را انتخاب کنید، پیشنهاد من انتخاب سری Intel Xeon است که بار کاری بالایی را تحمّل می‌کند؛ این نوع CPU ها در سرورهای HP یا سرورهای دیگر که در بالا در مورد آنها صحبت کردیم، وجود دارند. این نوع CPU ها به نسبت دیگر CPU ها گران‌تر و قدرتمندتر هستند.

البتّه اگر سرور شما نیازی به پردازش زیاد ندارد، بهتر است از CPU های سری I3، I5 و I7 استفاده کنید.

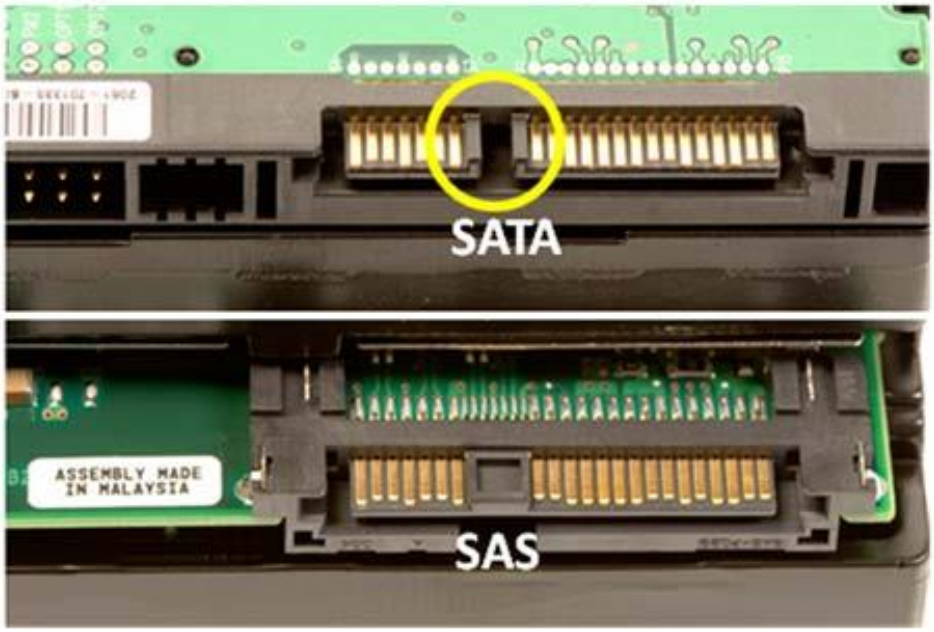
انتخاب رم:

انتخاب رم، ارتباط مستقیم با مادربرد دارد باید حتماً در جزئیّات مادربرد مشاهده کنید که این نوع مادربرد چه نوع رمی را پشتیبانی می‌کنند، توجّه داشته باشید رم سرورهای HP کاملاً متفاوت با رم‌های معمولی هستند، در رم‌های سرور قابلیّت تشخیص خطا وجود دارد که این توانایی را به سرور می‌دهد تا رم مشکل‌دار را پیدا و مشخّص کند، اگر در سیستم‌های معمولی دو رم بر روی مادربرد داشته باشید و یکی از آنها در حال کار خراب شود، کلّ سیستم شما Reset یا خاموش می‌شود، امّا در سرورها چنین نیست، تنها همان رم از رده خارج می‌شود و یک پیغام هشدار نیز به مدیر شبکه ارسال می‌شود، این هشدار می‌تواند از طریق چراغ روی سرور، یا از طریق نرم‌افزار باشد.

انتخاب هارد دیسک:

برای انتخاب هارد دیسک دو گزینه را پیش روی خود دارید، یکی اینکه با قیمت کم، هاردهای معمولی SATA را خریداری کنید و به سرور متّصل کنید که در این صورت، همه چیز به خوبی اجرا خواهد شد، امّا سرعت کار برای سرورهایی که به سرعت بالای هارد نیاز دارد کم خواهد بود؛ راه دیگر، خرید هارد SAS است که از سرعت و کیفیّت خوبی برخوردار است.

تفاوت بین هارد SAS با SATA:



در شکل روبرو، نوع کانکتورهای ارتباطی این دو هارد دیسک را مشاهده می‌کنید؛ در هارد دیسک‌های SAS، روش ارتباطی به روش ترتیبی است و سرعت چرخش این نوع هارد دیسک‌ها، ۱۰۰۰۰ تا ۱۵۰۰۰۰ است که به اصطلاح به آن RPM می‌گویند، در هاردهای SATA، سرعت چرخش تا حداکثر ۷۲۰۰ است که نسبت به SAS خیلی سرعت کمتری دارد و سرعت انتقال اطّلاعات، ۱۵۰ مگابایت است، امّا در هارد دیسک‌های SAS، سرعت انتقال اطّلاعات، ۳ گیگابایت بر ثانیه است.

با توجّه به اینکه هاردهای SAS از سرعت و کیفیّت بالاتری برخوردار هستند، پس بدون هیچ تردیدی از این نوع هاردها در شبکه‌ی خود استفاده کنید، البتّه قیمت آن نسبت به هاردهای SATA، چند برابر است، امّا ارزش کار آن را در آینده خواهید دید.

نکته: سعی کنید همیشه سروری، مانند شیرپوینت، Skype و یا ایکسچنج را بر روی هاردهای SAS، پیاده‌سازی کنید تا از حداکثر سرعت بهره ببرید.

توجّه داشته باشید که برای استفاده از هاردها در سرور سعی کنید، حتماً آنها را Raid بندی کنید تا در زمان از دست رفتن یک هارد، کلّ شبکه از کار نیفتد و بتوانید هارد را به موقع تعویض کنید؛ در مورد Raid بندی در کتاب مدیر شبکه‌ی یک و مهندسی مایکروسافت توضیحاتی دادیم که می توانید آن را مطالعه کنید.

ویندوز سرور ۲۰۱۶:

در این کتاب، ویندوز سرور ۲۰۱٦ مایکروسافت را در نظر گرفتیم که می‌تواند انتخاب خوبی برای شبکه‌ی شما باشد، مهمترین ویژگی‌های ویندوز سرور ۲۰۱٦ عبارتند از:

- ✓ بهبود سرویس‌های Active Directory و اضافه شدن سرویس AD FS.
- ✓ اضافه شدن سرویس امنیّتی Windows Server Anti-malware.
- ✓ بهبود سرویس Remote Desktop.
- ✓ تغییرات گسترده در نحوه‌ی ذخیره‌سازی و کپی داده‌ها در Storage Service.
- ✓ قابلیّت پردازش خوشه‌ای با دسترسی بالا و کاهش Failover.
- ✓ تغییرات گسترده در HTTP و HTTPS.
- ✓ معرّفی IIS 10 و پشتیبانی از HTTP/2.
- ✓ معرّفی Windows PowerShell 5.0.
- ✓ قابلیّت Soft Restart و کاهش مدّت زمان Boot.
- ✓ امکان راه‌اندازی نانو سرورها با Performance بسیار بالا.
- ✓ حذف پشتیبانی از NAP در سرویس DHCP.
- ✓ پشتیبانی از Subnet های ۳۱ و ۳۲ و ۱۲۸ در IPAM.
- ✓ راه‌اندازی Linux Secure Boot در Hyper-V.

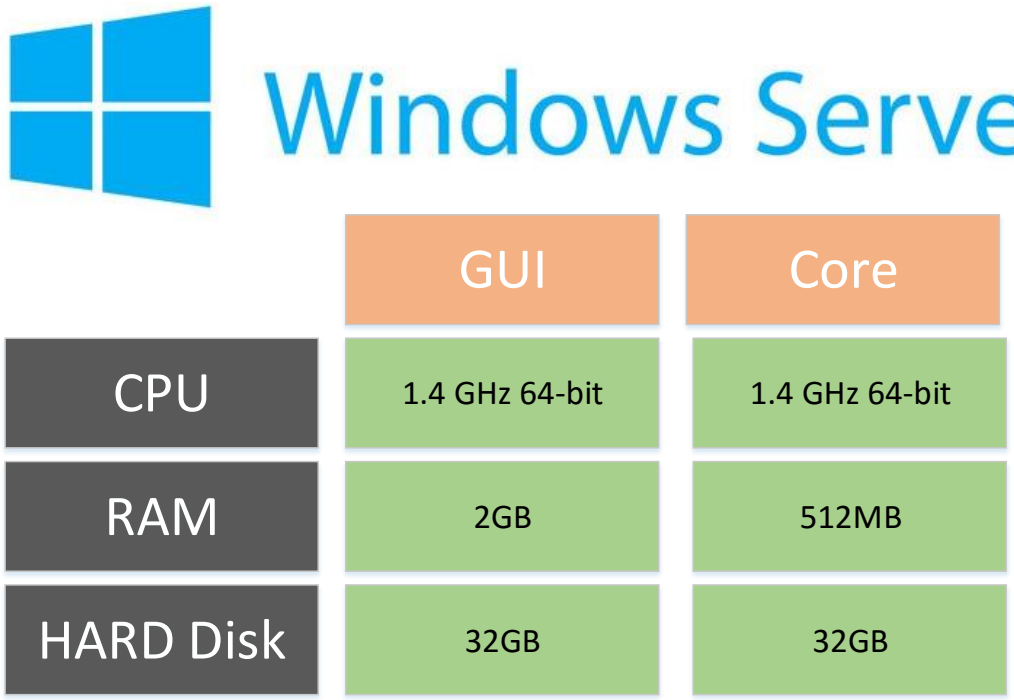
نسخه‌های مختلف ویندوز سرور ۲۰۱۶:

ویندوز سرور ۲۰۱٦ دارای دو نسخه‌ی Standard و Datacenter است که در جدول زیر، امکانات این دو ورژن را مشاهده می‌کنید، ورژن Datacenter از امکانات بالاتری برخوردار است و قیمت آن نیز بالای ٦ هزار دلار است.

Windows Server 2016 Editions		
	Datacenter	**Standard**
Core functionality of Windows Server	•	•
OSEs / Hyper-V containers*	Unlimited	2
Windows Server containers	Unlimited	Unlimited
Nano Server	•	•
New storage features including Storage Spaces Direct and Storage Replica+	•	
New Shielded Virtual Machines and Host Guardian Service+	•	
New networking stack+	•	
Price**	$6,155	$882

در این کتاب سعی کردیم، نسخه‌ی کامل آن را که Datacenter است را آموزش دهیم تا همه‌ی امکانات این ویندوز در دسترس باشد.

سخت‌افزار مورد نیاز ویندوز سرور ۲۰۱۶:



همانطور که در شکل بالا مشاهده می‌کنید، حداقل سخت‌افزار مورد نیاز برای راه‌اندازی دو ورژن ویندوز سرور ۲۰۱۶را مشاهده می‌کنید که در این کتاب و برای راه‌اندازی سرور Active Directory از ویندوز سرور ورژن Desktop استفاده می‌کنیم.

لینک دانلود ویندوز سرور ۲۰۱۶:

http://p30download.com/fa/entry/66411/

نصب ویندوز سرور در دو حالت Desktop و Core صورت می‌گیرد که در موقع نصب می‌توانید یکی از گزینه‌ها را انتخاب کنید.

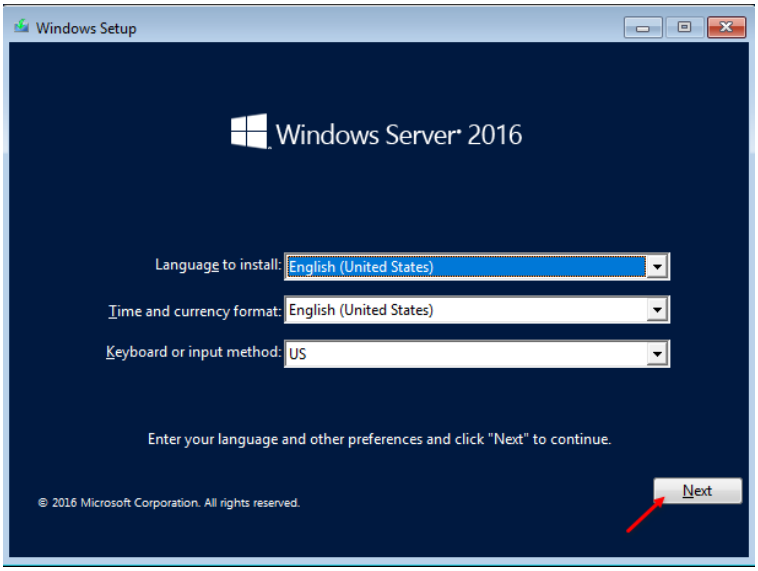
اگر چنانچه در نصب ویندوز مشکل دارید با من در تماس باشید.

@farshidbabajani

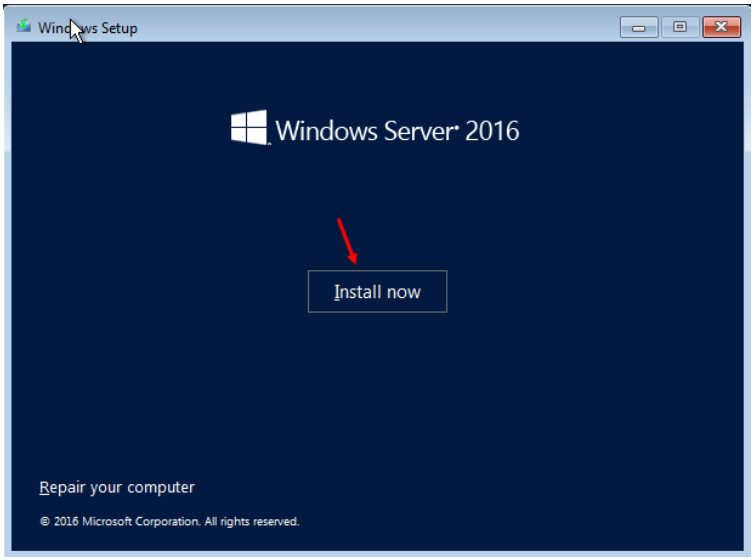
شروع نصب ویندوز سرور ۲۰۱۶:

برای اینکه از منابع سخت‌افزاری خود به درستی و به صورت کاملاً مدیریّت شده استفاده کنید، بهترین حالت این است که از نسخه‌ی Core سیستم عامل ویندوز سرور ۲۰۱٦ استفاده کنید که از منابع سخت‌افزاری پائینی استفاده می‌کند.

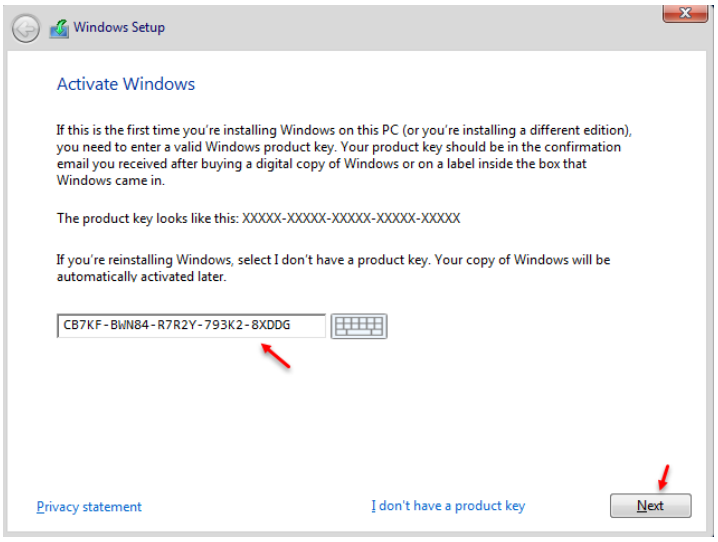
مراحل نصب ویندوز سرور نسخه‌ی Desktop ساده است، امّا این مراحل را برای دوستانی که نیاز به نصب آن را دارند، انجام می‌دهیم:



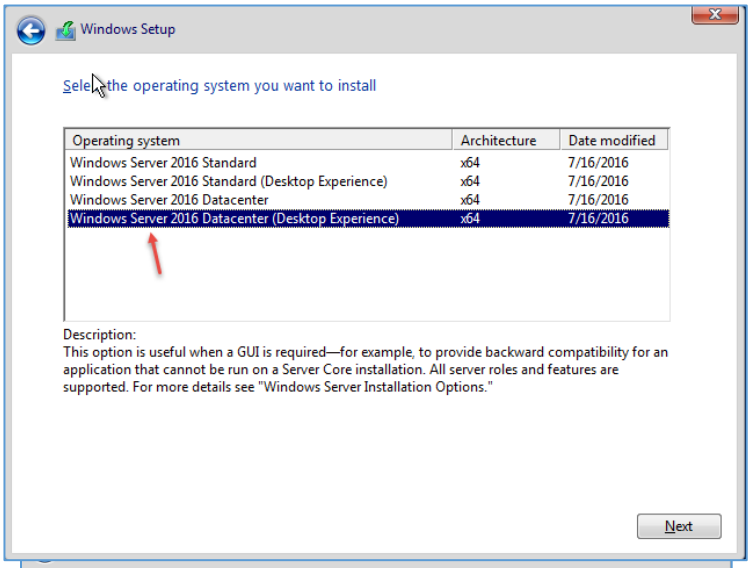
صفحه‌ی اوّل نصب ویندوز سرور را مشاهده می‌کنید که باید بعد از انتخاب زبان مورد نظر خود بر روی Next کلیک کنید.



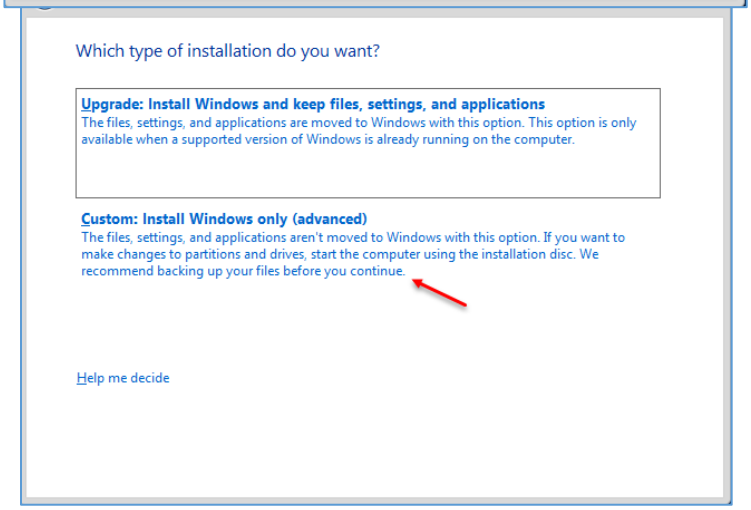
در این صفحه بر روی Install now کلیک کنید.



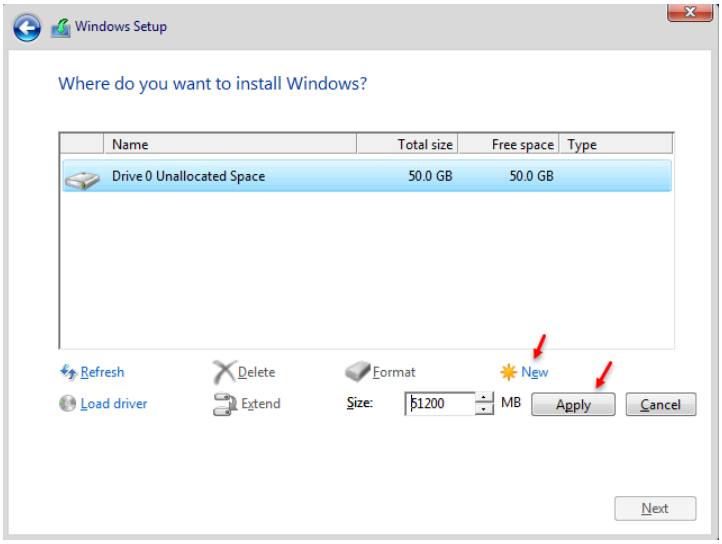
شماره‌ی سریال مورد نظر ویندوز سرور را در جای مشخّص شده وارد و بر روی Next کلیک کنید.



در این قسمت، دو ورژن مختلف از ویندوز سرور ۲۰۱۶ را مشاهده می‌کنید، همانطور که در مبحث قبلی گفتیم، برای شروع کار، ورژن Datacenter نسخه-ی Desktop را آموزش می‌دهیم، لذا گزینه‌ی آخر را انتخاب و بر روی Next کلیک می‌کنیم.



در این صفحه برای انتخاب هارد دیسک و نصب ویندوز بر روی درایو مورد نظر بر روی گزینه‌ی مورد نظر کلیک کنید.



در این قسمت از لیست، هارد دیسک مورد نظر خود را انتخاب و بر روی New کلیک کنید و مقدار فضای پارتیشن خود را وارد و بر روی Apply کلیک کنید و بعد، هارد دیسک مورد نظر خود را انتخاب و بر روی Next کلیک کنید.

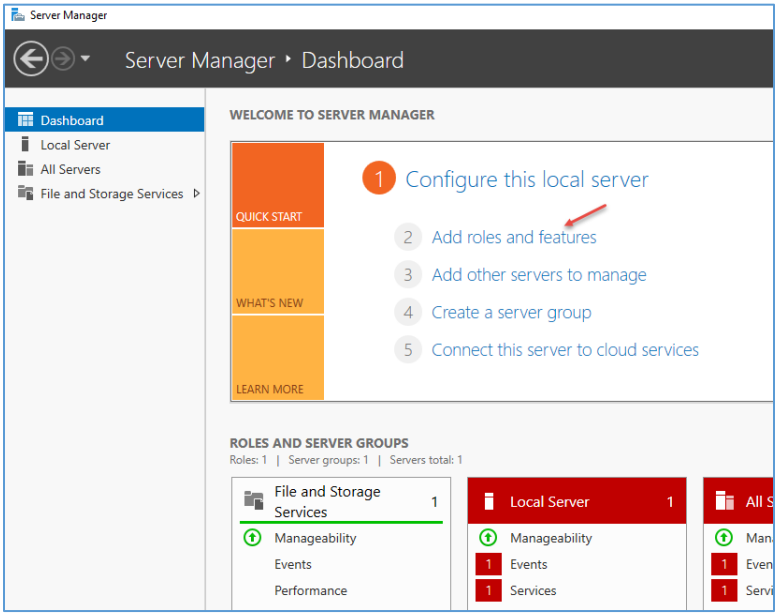
توجّه داشته باشید که دو نوع پارتیشن‌بندی MBR و GPT داریم که کلمه‌ی MBR، مخفّف Master Boot Record است و کلمه‌ی GPT، مخفّف GUID Partition Table است، ویندوز سرور ۲۰۱۶ با نوع MBR کار می‌کند که این نوع ازپارتیشن‌بندی‌ها می‌تواند تا ۲ ترابایت اطّلاعات را پشتیبانی کند، یک دیسک MBR می‌تواند تا ٤ درایو Primary داشته باشد، دیسک‌های از نوع GPT می‌توانند حجم بالای ۲ ترابایت را پشتیبانی کنند که این مورد در صورتی انجام می‌شود که هارد دیسک شما بالای ۲ ترابایت باشد.

بعد از اینکه Next کردید، ویندوز به راحتی نصب خواهد شد.

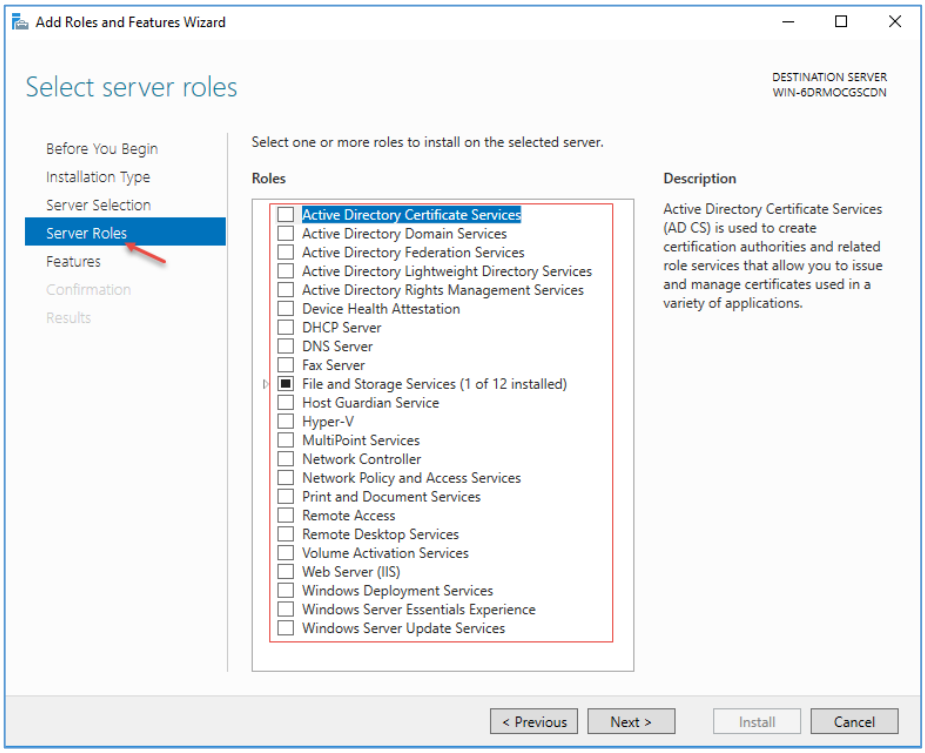


بررسی ابزارها و سرویس‌های ویندوز سرور ۲۰۱۶:

بعد از نصب ویندوز و ورود به آن، برای شما برنامه‌ی Server Manager به صورت خودکار اجرا خواهد شد، در این برنامه، انواع سرویس‌ها و ابزارهای مربوط به ویندوز سرور ۲۰۱۶ وجود دارد که در زیر همه‌ی این سرویس‌ها و ابزارها را به صورت کلّی بررسی خواهیم کرد.:



برای اجرا کردنServer Manager، می توانید بر روی Start کلیک کنید و Server Manager را اجرا کنید تا صفحه‌ی روبرو ظاهر شود، برای معرّفی سرویس‌ها بر روی Add roles and Features کلیک کنید تا شکل بعد ظاهر شود.



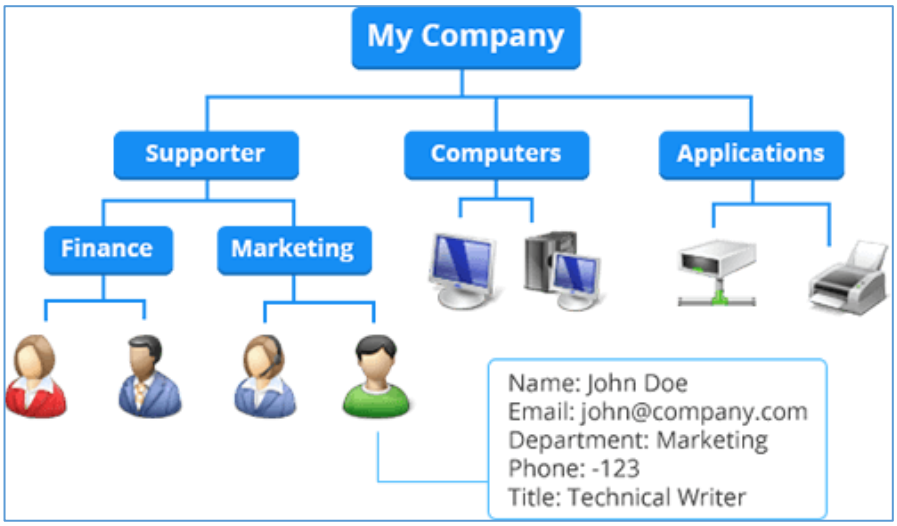
در این قسمت باید وارد صفحه-ی Server Roles شوید، تمام سرویس‌های ویندوز سرور را مشاهده می‌کنید که هر کدام برای انجام کاری ایجاد شده‌اند، برای بررسی کارایی آنها، نگاهی کلّی به آنها می‌اندازیم.

۱– سرویس Active Directory Certificate Service:

همانطور که از نام آن پیدا است، برای مدیریّت گواهینامه‌ها و دادن دسترسی‌های مجاز به سایت یا سرویس خاصّی است، با این سرویس می‌توانید سایت خود را با پروتکل SSL امن‌تر کنید و کارهای دیگری را انجام دهید، توجّه داشته باشید بعضی از نرم‌افزارها به صورت مستقیم با این سرویس کار می‌کنند، مانند Exchange و Skype که باید یک‌سری گواهینامه برای این نوع نرم‌افزارها صادر شود که این کار توسط سرویس Active Directory Certificate Service انجام می‌گیرد؛ در ادامه‌ی کتاب این سرویس را نصب و راه‌اندازی خواهیم کرد.

۲– سرویس Active Directory Domain Service:

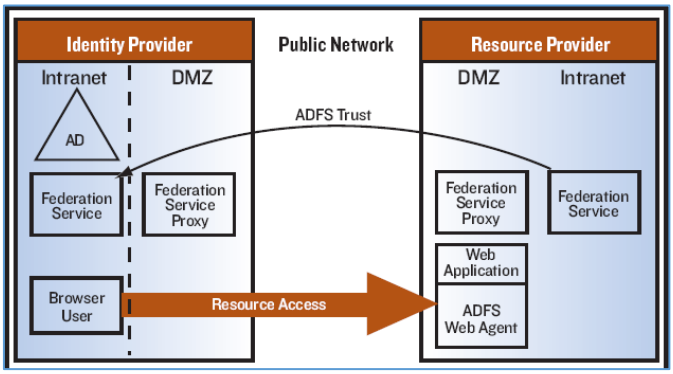
یکی از مهمترین و با اهمّیّت‌ترین سرویس‌ها در ویندوز سرور که سال‌ها در کنار مدیران شبکه و کاربران آن بوده است، برای اینکه یک شبکه‌ی مدیریّت شده داشته باشید و همه‌ی کاربران به صورت مدیریّت شده باشند، باید از این سرویس استفاده کنید، این سرویس با ایجاد یک دامنه‌ی خاص، به شما این امکان را می‌دهد تا برای کاربران خود، نام کاربری تعریف کنید، آنها را عضو گروه خاص با دسترسی خاص کنید و سیستم‌های آنها را عضو این دامنه و مدیریّت‌های خود را بر روی آنها اعمال کنید.



در شکل روبرو، مثالی از این سرویس را مشاهده می‌کنید، می‌توانید نام کاربری با اطّلاعات کامل کاربر ایجاد کنید، آنها را عضو گروه کنید، پرینتر و درایو تحت شبکه برای کاربران ایجاد کنید و کارهای مختلف دیگری انجام دهید.

۳– سرویس Active Directory Federation Service:

زمانی که یک دومین را راه‌اندازی می‌کنید و کاربران شما از منابع شبکه استفاده می‌کنند، شاید بخواهید کاربرانی که در یک دومین دیگر هستند به شبکه‌ی خود دسترسی دهید تا از منابع شما به صورت محدود استفاده کنند، این کار توسط سرویس ADFS انجام می‌شود، در این شکل نیز نحوه‌ی دسترسی بین دو دومین مختلف از طریق سرویس Active Directory Federation Service مشخّص شده است.



۴– بررسی سرویس Active Directory Lightweight Directory Services:

این سرویس برای نرم‌افزارهایی که نیاز به اطّلاعات شبکه دارند، طرّاحی شده است، این سرویس کاملاً مجزّا از سرویس Active directory Domain service ایجاد شده است و مستقل کار می‌کند و تنها اطّلاعات نرم-افزارهایی که می‌خواهند از منابع شبکه استفاده کنند، در آن ذخیره می‌شود.

نام اختصاری این سرویس، AD LDS است.

۵– بررسی سرویس Active Directory Rights Management Services:

این سرویس برای ایجاد امنیّت در شبکه استفاده می‌شود و قابلیّت‌های منحصر به فردی را در اختیار کاربران قرار می‌دهد.

۶– بررسی سرویس Device Health Attestation:

این سرویس یک قابلیّت جدید در ویندوز سرور ۲۰۱۶ و ویندوز ۱۰ است که مایکروسافت ارائه کرده است، با این سرویس شما می‌توانید دستگاه‌هایی، مانند موبایل که به شبکه‌ی شما وصل می‌شوند را بررسی کنید تا از سلامت لازم برخوردار باشند.

۷– بررسی سرویس DHCP:

DHCP یا Dynamic Host Configuration Protocol برای اختصاص دادن آدرس IP با تنظیمات مختلف به دستگاه‌های شبکه، مانند سیستم، دوربین، پرینتر و... است که شما با اختصاص دادن یک رنج IP به این سرویس و دادن آدرس‌های روتر و DNS می‌توانید آدرس IP خود را به هر یک از دستگاه‌هایی که به شبکه‌ی شما متّصل می‌شوند، بدهید؛ توجّه داشته باشید که در این سرویس می توانید دستگاه‌ها را با آدرس MAC محدود کنید تا دستگاه‌هایی غیر از شبکه شما نتوانند به شبکه‌ی شما متّصل شوند.

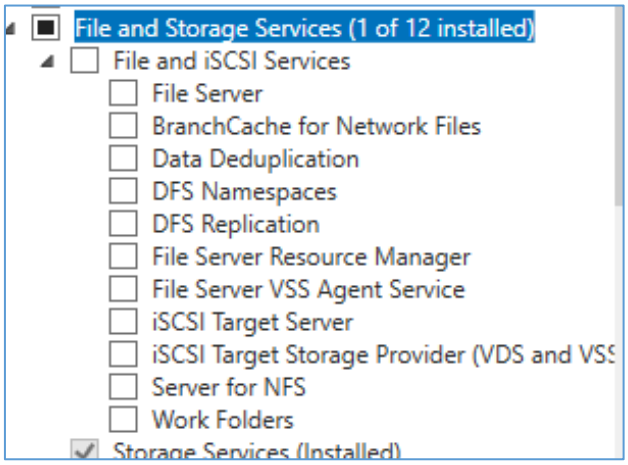
۸– بررسی سرویس DNS:

DNS یا Domain Name System، سرویسی برای نظم بخشیدن به آدرس و نام‌های دستگاه‌ها در شبکه است که کار اصلی آن تبدیل آدرس IP به اسم و یا برعکس آن است؛ این سرویس یکی از مهمترین سرویس‌ها در ویندوز سرور است که کار نظم بخشیدن و مدیریّت آدرس‌ها را بر عهده دارد، توجّه داشته باشید اگر بخواهید سرویس Active Directory را نصب کنید، این سرویس نیز به صورت خودکار نصب خواهد شد.

۹–بررسی سرویس Fax Server:

این سرویس همانطور که از نام آن پیدا است، برای فکس و کار با اسناد است و برای مدیریّت و پیکربندی سرویس فکس کاربرد دارد که در ادامه، بر روی آن بیشتر بحث خواهیم کرد.

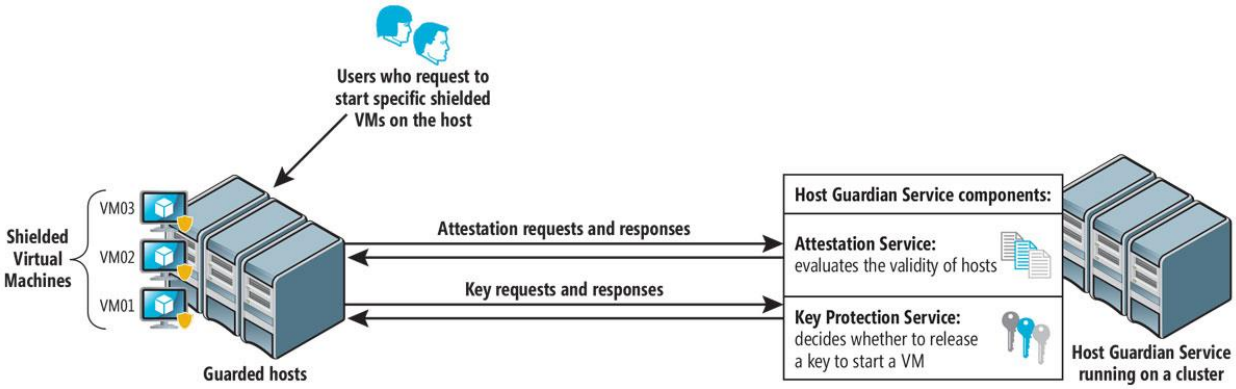
۱۰– بررسی سرویس File and Storage Service:



این سرویس، شامل چیدن ابزار است که در شکل روبرو مشاهده می‌کنید؛ این ابزارها این توانایی را به مدیر شبکه می‌دهد که بتواند به راحتی و با نظارت بالا بر روی فایل‌های Share شده نظارت داشته باشد.

۱۱– بررسی سرویس Host Gurdian:

سرویسی جدید از مایکروسافت که در ویندوز سرور ۲۰۱۶ ارائه شده است و برای حفظ امنیّت ماشین مجازی در سرویس Hyper-V کاربرد دارد؛ این سرویس با الگوریتم خاصّی، ماشین‌های مجازی را رمزگذاری می‌کند تا امنیّت اطّلاعات افزایش پیدا کند.



۱۲– بررسی سرویس Hyper-V:

این سرویس برای ایجاد ماشین مجازی از سوی مایکروسافت ارائه شده است که می‌تواند رقیب جدّی برای VMware باشد؛ این سرویس در نسخه‌ی جدید ویندوز سرور بهبود یافته و از سرعت و عمکرد بالاتری نسبت به قبل برخوردار است، در ادامه در مورد این سرویس بیشتر بحث خواهیم کرد و مثال‌های گوناگونی در این مورد خواهیم زد.

۱۳– بررسی سرویس Multipoint Service:

سرویس جدید مایکروسافت با عنوان Multipoint است که امکان جدید مانیتورینگ کلاینت‌ها و سرورها را در اختیار مدیر شبکه قرار می‌دهد، با این سرویس می‌توانید یک کلاس درس برای کاربران خود در شبکه و یا در یک محیط آموزشی فراهم کنید، این سرویس می‌تواند جایگزین نرم‌افزار محبوب Net Support باشد.

۱۴– بررسی سرویس Network Controller:

با استفاده از این سرویس می‌توانید با نرم‌افزار خاصّ خود که در اصطلاح، API نامیده می‌شود، منابع شبکه را مدیریّت کنید.

۱۵– بررسی سرویس Network Policy and Access service:

این سرویس برای ایجاد امنیّت در سرویس‌های بی‌سیم و سیمی کاربرد دارد و می‌توانید از طریق این سرویس، یک Radius سرور نیز راه‌اندازی کنید و کارهای محتلفی در آن انجام دهید.

۱۶– بررسی سرویس Print document:

برای ایجاد نظم و مدیریّت پرینترها و اسناد سازمان خود می‌توانید از این سرویس استفاده کنید.

۱۷– بررسی سرویس Remote Access:

سرویسی برای راه‌اندازی VPN، Proxy و به اشتراک‌گذاری اینترنت است که در ادامه بر روی آن، کار خواهیم کرد.

۱۸– بررسی سرویس Remote Desktop Service:

سرویسی برای مدیریّت Remote در شبکه است که به شما این امکان را می‌دهد که هم‌زمان بتوانید با چندین کاربر روی یک سرور، Remote شوید؛ به صورت پیش‌فرض، تنها ۲ کاربر می‌تواند روی سرور Remote شود، امّا با راه‌اندازی آن که البتّه از طرف مایکروسافت باید لایسنس آن را تهیّه کنید، می‌توانید با چندین کاربر به سرور، Remote بزنید، با این سرویس توانایی آن را دارید که برای کاربران خود از طریق وب، نرم‌افزار و یا ماشین مجازی خاصّی را به اشتراک بگذارید که در مورد این سرویس به صورت کامل آموزش خواهیم داد.

۱۹– بررسی سرویس Volume Activation:

برای مدیریّت کامل فعّال‌سازی ویندوز در شبکه که با ابزارهای خاصّی این کار را انجام می‌دهد، این سرویس از ویندوز ویستا به بعد را پشتیبانی می‌کند.

۲۰– بررسی سرویس Web Server (IIS):

سرویس IIS برای راه‌اندازی وب سایت می‌توانید از این سرویس استفاده کنید، با این سرویس می‌توانید امنیّت کامل سایت خود را با پروتکل SSL ایجاد کنید، سرویس FTP را راه‌اندازی کنید، ری دایرکت برای سایت‌ها و... ایجاد کنید.

۲۱– بررسی سرویس Windows Deployment:

این سرویس برای راحتی کار مدیران شبکه طرّاحی شده است که با آن می‌توانید از طریق شبکه برای کلاینت‌ها، ویندوز نصب کنید و درایورهای آن را نیز با اضافه کردن به سرویس به صورت خودکار نصب کنید؛ با این کار، کاملاً در زمان صرفه جویی خواهید کرد و کار نصب به درستی و به سرعت انجام خواهد شد.

۲۲– بررسی سرویس Windows server essential experience:

این سرویس، یک‌سری ابزارهای آنلاین را در اختیار شما قرار می‌دهد، به کمک این سرویس می‌توانید به آفیس ۳٦٥ یا ویندوز Azure متّصل شوید و اطّلاعات و کاربران خود را مدیریّت کنید.

بررسی سرویس Windows Server Update:

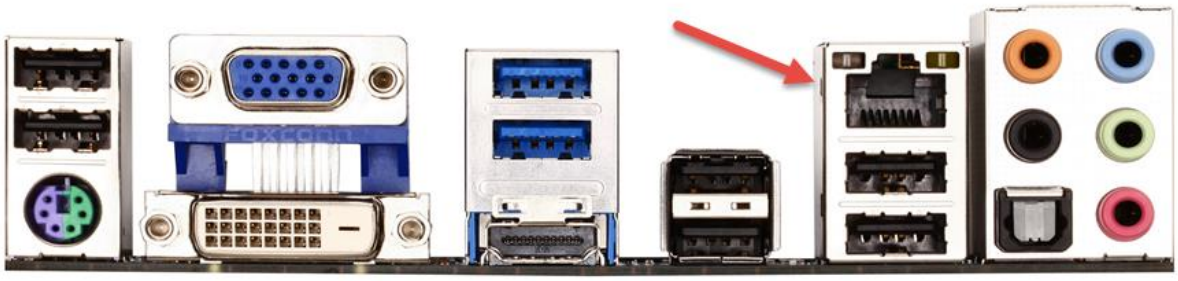
همانطور که از نام این سرویس مشخّص است، این سرویس برای مدیریّت آپدیت‌های ویندوز و نرم‌افزارهای آن کاربرد دارد و می‌توانید در یک شبکه با انتخاب ورژن ویندوز خود، همه‌ی آپدیت‌ها را به کلاینت‌ها ارسال کنید، با این تفاوت که دیگر کلاینت‌ها نیاز نیست که به صورت مستقیم از اینترنت آپدیت را دریافت کنند، بله به راحتی می‌توانند با متّصل شدن به سرور، آپدیت داخلی همه‌ی اطّلاعات جدید را از این سرور دریافت کنند.

تا این قسمت، همه‌ی سرویس‌های موجود در ویندوز سرور ۲۰۱٦ را بررسی کردیم که هر کدام در جایگاه خود می‌توانند بسیار مفید واقع شوند، به خاطر اینکه اکثر این سرویس‌ها در کتاب مهندسی مایکروسافت به طور کامل آموزش داده شده است، بنابراین در این کتاب، تنها روی سرویس‌هایی کار خواهیم کرد که ضروری باشند و اصلاً آموزشی در مورد آن نوشته نشده باشد.

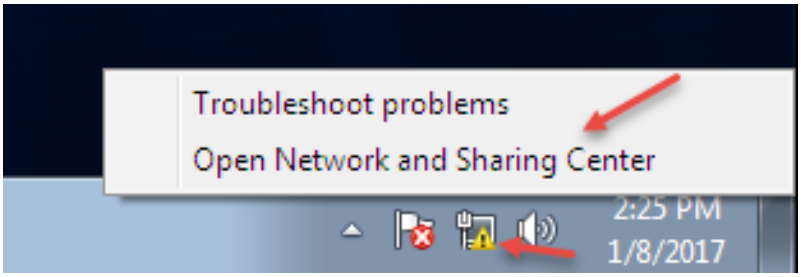
شبکه کردن دو سیستم با هم:

این قسمت از آموزش برای افراد مبتدی ایجاد شده است که تا به حال دو سیستم را نتوانستند از طریق کابل شبکه به هم متّصل کنند.

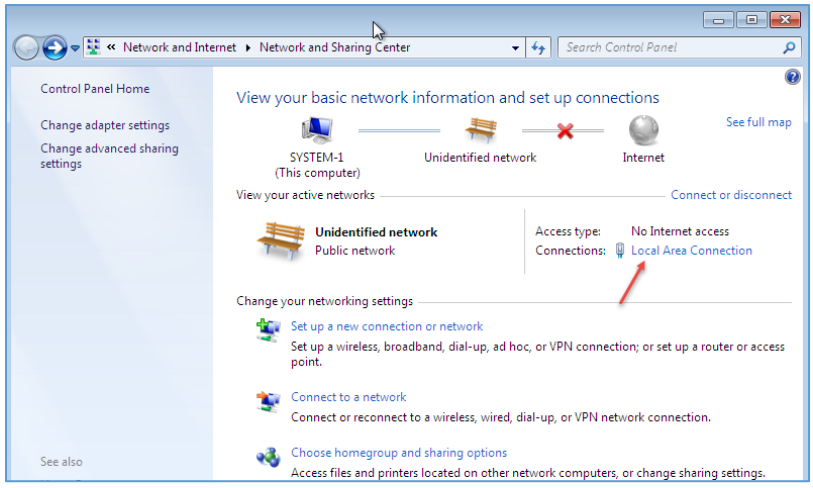
فرض را بر این می‌گیریم که دو سیستم واقعی داریم و می‌خواهیم این دو را به یکدیگر، شبکه کنیم، برای این کار نیاز به یک کابل شبکه با سوکت RG45 داریم که امیدوارم این کابل را در اختیار داشته باشید، البتّه با نرم‌افزار مجازی، مانند VMware workstation یا Hyper-V می‌توانید دو سیستم ایجاد و آنها را به صورت مجازی شبکه کنید.



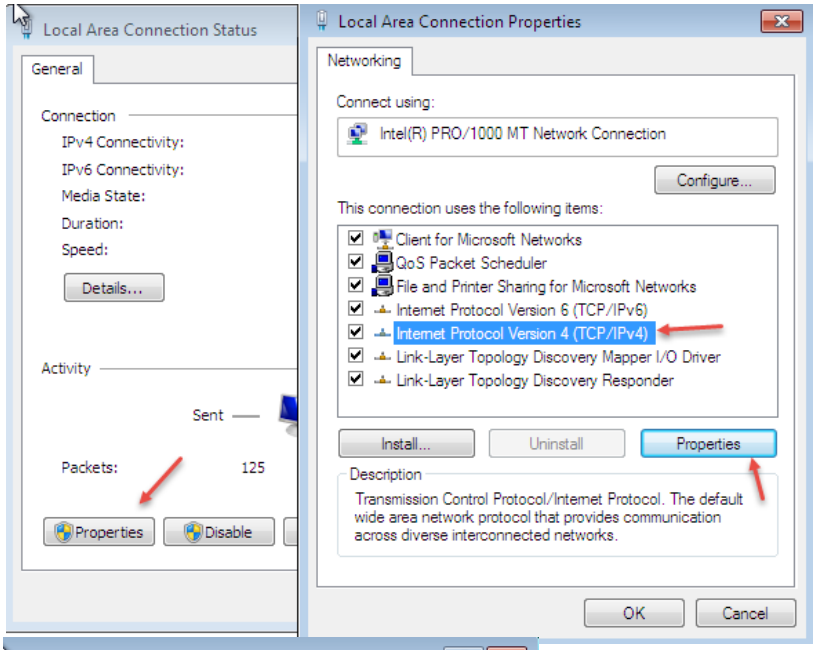
در شکل بالا، قسمت پشت یک سیستم را مشاهده می‌کنید که دارای یک پورت شبکه است و در اکثر سیستم‌های امروزی وجود دارد، شما باید کابل شبکه را در این پورت و کابل دیگر را در سیستم روبرویی خود قرار دهید، بعد از این کار می‌توانید وارد سیستم شوید و عملیّات آدرس‌دهی را آغاز کنید.



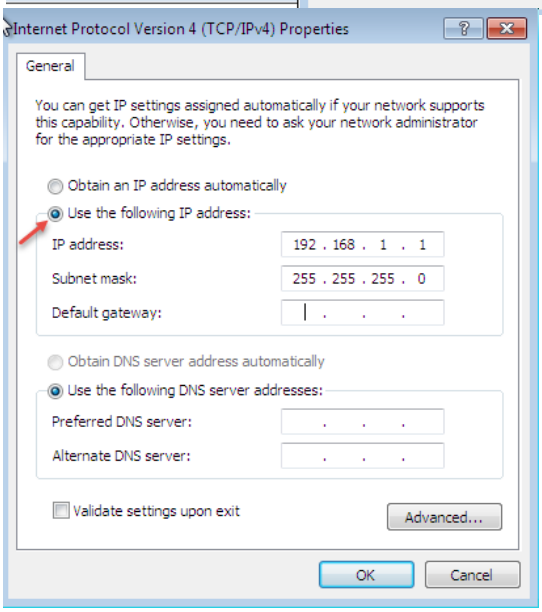
زمانی که وارد ویندوز شدید در سمت راست نوار ابزار بر روی آیکون Network کلیک راست کنید و گزینه‌ی Open Network.... را انتخاب کنید.



در این صفحه بر روی نام کارت شبکه‌ی خود که به صورت پیش‌فرض Local Area Connection است، کلیک کنید.

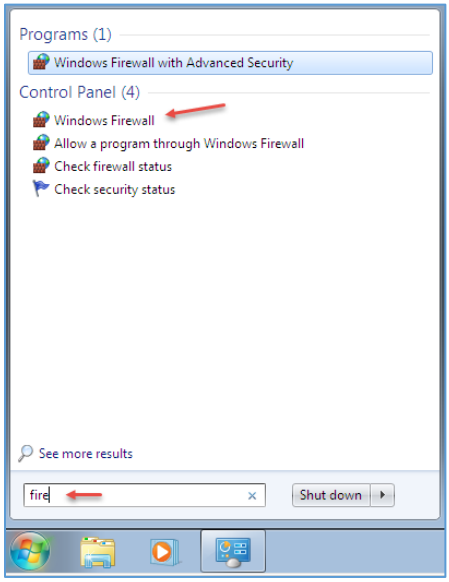


در این قسمت و در صفحه‌ی اوّل بر روی Properties کلیک کنید و در صفحه‌ی بعد از لیست مورد نظر، گزینه‌ی IPV4 را انتخاب و بر روی Properties کلیک کنید.



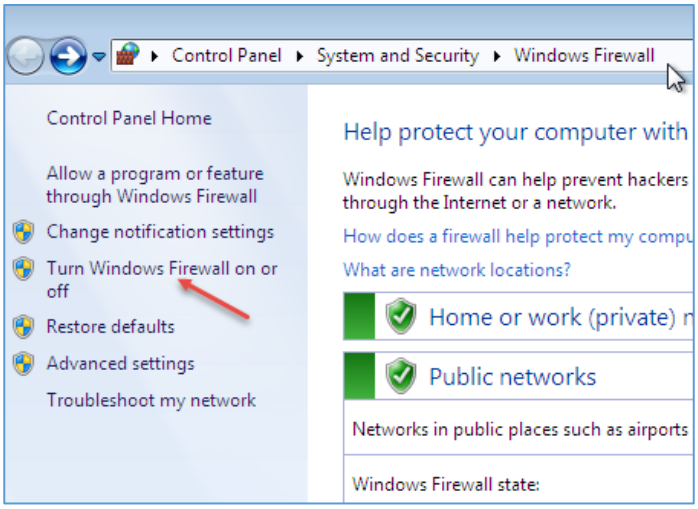
در این قسمت، گزینه‌ی Use the following Ip address را انتخاب کنید و یک آدرس IP، به مانند شکل روبرو وارد کنید، توجّه داشته باشید اگر در این سیستم، 192.168.1.1 وارد کردید در سیستم روبرو باید 192.168.1.2 وارد کنید تا مشکلی پیش نیاید، بعد از این کار بر روی OK کلیک کنید.

توجّه داشته باشید، اگر چنانچه می‌خواهید نحوه‌ی آدرس‌دهی را بیاموزید، می‌توانید کتاب CCNA بنده را مطالعه کنید.

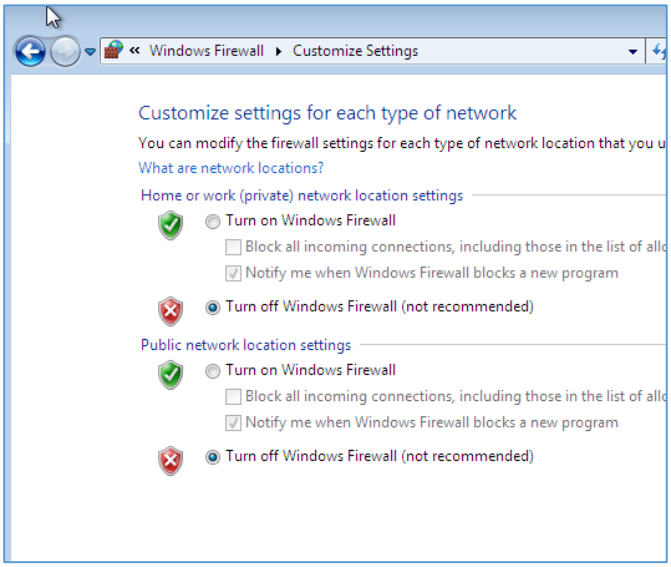


بعد از اینکه به هر دو سیستم، آدرس دادید باید سرویس Firewall آنها را نیز غیر فعّال کنید که برای این کار در منوی start، سرویس Firewall را جستجو وآن را به مانند شکل روبرو اجرا کنید.

این کار را در هر دو سیستم انجام دهید.



در این قسمت وارد Turn Windows Firewall on or off شوید.



در این صفحه، هر دو قسمت را بر روی Turn Off قرار دهید تا فایروال خاموش شود، اگر تنظیمات قبل را به درستی انجام داده باشید، دو سیستم به راحتی می‌توانند همدیگر را پیدا کنند.

بررسی سرویس‌های شبکه

سرویس DNS:

Domain Name System یا همان DNS، یکی از مهمترین موضوعات در شبکه است که فراگیری این سرویس یکی از مهمترین کارها است. برای شروع کار باید موضوعاتی را در این سرویس بررسی کنیم.

اصول کار شبکه، دانستن IP آدرس است، در کل، دو ورژن آدرس IP داریم، یکی IPV4 و دیگری IPV6 است که اگر در مورد این دو پروتکل آشنایی ندارید، می‌توانید به کتاب CCNA بنده مراجعه کنید و این دو پروتکل را به طور کامل یاد بگیرید.

لینک دانلود کتاب CCNA:

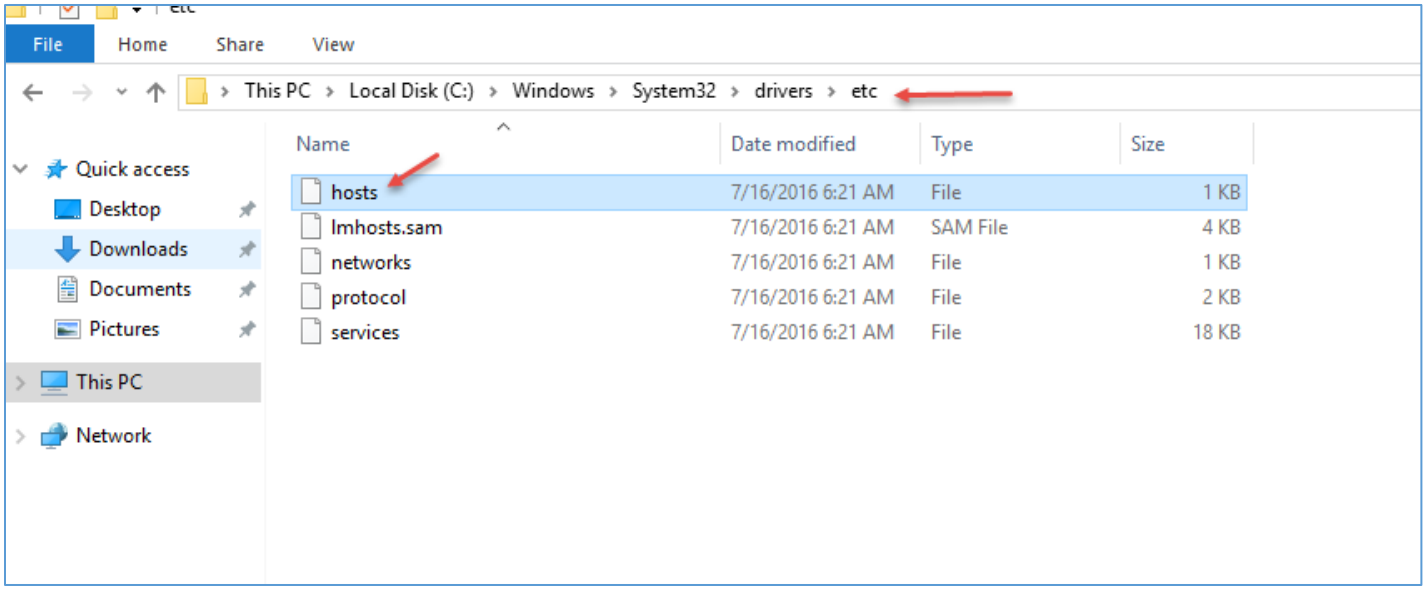
https://drive.google.com/file/d/0Bw1Nv5ua4a5-bUNQMGNCSnhOR28/view

سرویس DNS، این قابلیّت را به شما می‌دهد که بتوانید آدرس‌ها و نام‌های سیستم‌ها و سرورها را مدیریّت کنید.

به طور مثال، اگر یک سرور داشته باشید که نام آن، Application و آدرس آن، 10.180.0.1 باشد، کاربران برای متّصل شدن از طریق نام به سرور Application، نیازمند سرویسی هستند که این نام را به IP خود آن تبدیل کنند و همین‌طور سرویس DNS می‌تواند IP را به نام تغییر دهد؛ در ادامه‌ی کار با قابلیّت‌های کامل، سرویس DNS آشنا خواهیم شد.

بررسی فایل HOSTS در ویندوز:

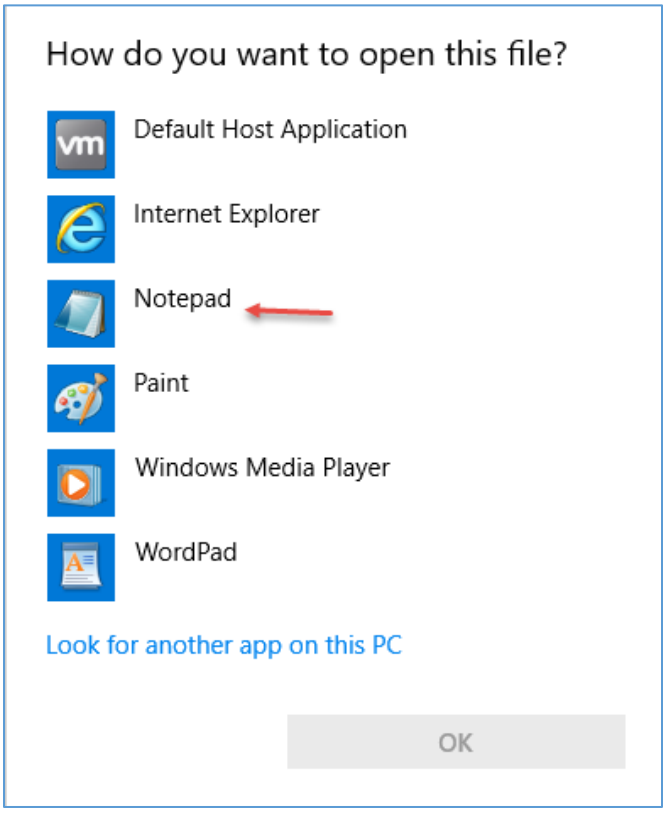
فایلی با نام Host در ریشه‌ی ویندوز وجود دارد که می‌توان آن را یک عضو کوچک از سرویس DNS نامید، شما در این فایل می‌توانید آدرس و نام‌های سرورها و سیستم‌های خود را به صورت دستی وارد کنید، یعنی اگر شما دو سیستم داشته باشید و بخواهید آنها را با هم شبکه کنید و این دو سیستم بخواهند از طریق نام، همدیگر را شناسایی کنند باید از این فایل در هر دو ویندوز استفاده کنید.



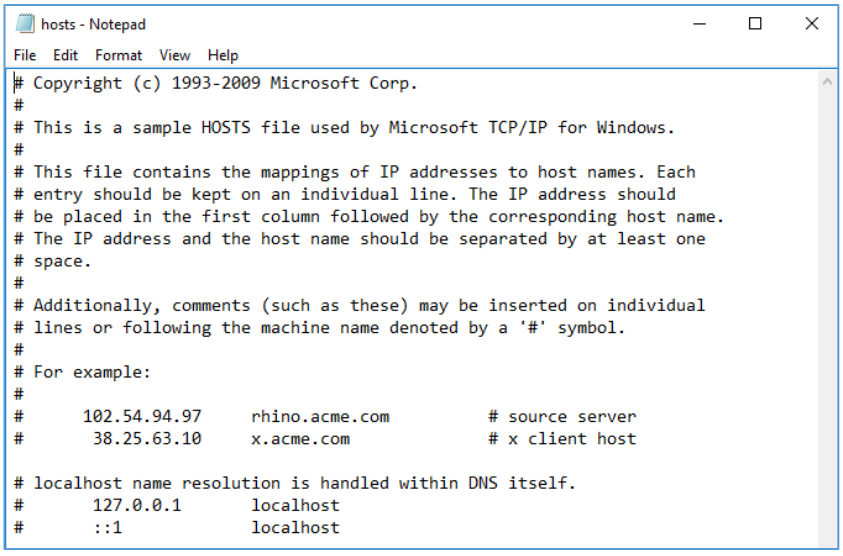
در شکل بالا وارد آدرس زیر شوید:

C:\Windows\System32\drivers\etc

در این قسمت، فایلی با نام hosts وجود دارد که اطّلاعات خود را باید در این فایل وارد کنید.



بر روی فایل مورد نظر کلیک کنید تا شکل روبرو ظاهر شود و توسط Notepad، فایل مورد نظر را باز کنید تا بتوانید فایل را ویرایش کنید.



در شکل روبرو، اطّلاعات درون فایل hosts را مشاهده می‌کنید که برای اینکه به شما کمک کند، مثالی از آدرس‌های DNS را به شما معرّفی کرده است.

در زیر یک مثال را بررسی می‌کنیم و عملکرد آن را مشاهده می‌کنیم.



192.168.1.1
System-1

192.168.1.2
System-2

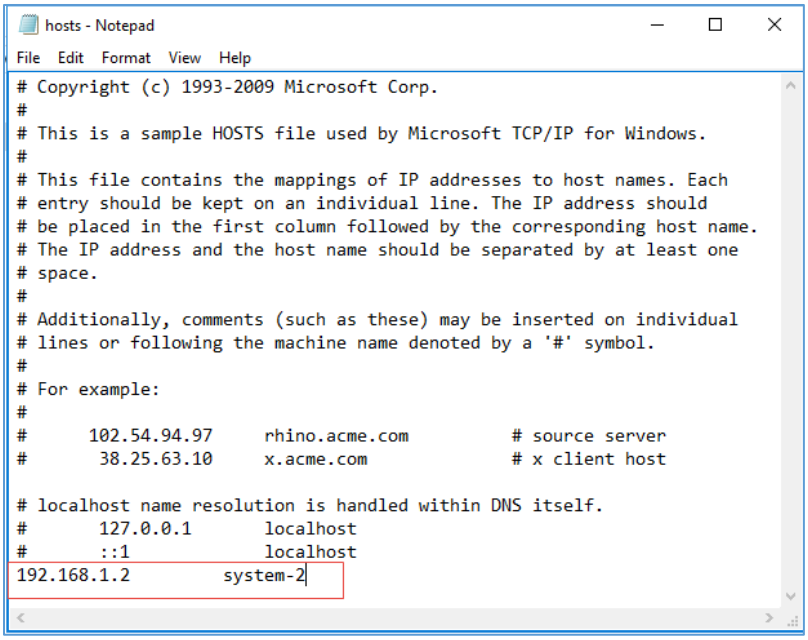
در شکل بالا، دو سیستم را مشاهده می‌کنید که هر دو با هم، شبکه شدند، به صورت پیش‌فرض، این دو سیستم می‌توانند همدیگر رااز طریق IP ببینند، امّا از طریق اسم نمی‌توانند با هم ارتباط داشته باشند، برای اینکه این سیستم‌ها از طریق اسم همدیگر را ببینند باید در فایل Hosts که در بالا باز کردیم، متن زیر را در آخر نوشته‌ها اضافه کنید:

در سیستم ۱:

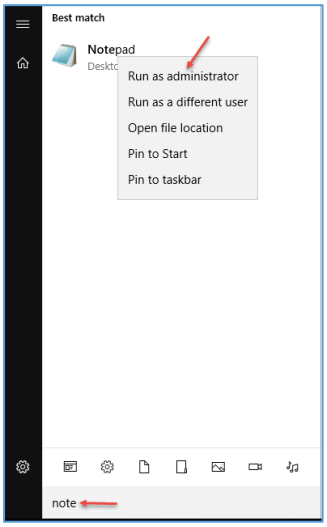
192.168.1.2 system-2

در سیستم ۲:

192.168.1.1 system-1

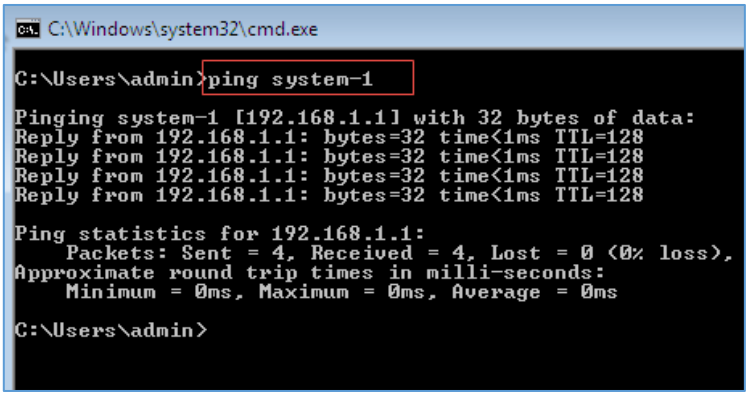


همانطور که در شکل روبرو مشاهده می‌کنید، در System-1 باید آدرس مورد نظر سیستم روبرو را وارد کنید، بعد از این کار، فایل متنی که از نوع ASCII است را ذخیره کنید و همین کار را نیز باید با تغییر آدرس در system-2 انجام دهید.



نکته‌ی مهم: در بعضی از سیستم‌ها به علّت اینکه دسترسی‌ها محدودتر هستند، نمی‌توانید به طور مستقیم فایل را بر روی همان فایل Hosts ذخیره کنید، برای این کار بهتر است، کلّ فایل متنی مورد نظر را Copy کنید و Notepad را به صورت روبرو با کاربر Administrator اجرا کنید تا دسترسی‌های لازم را داشته باشد، بعد از اجرا، فایل متنی را در آن Past کنید و در همان آدرس بر روی همان فایل ذخیره کنید.

با این کار توانستید دو سیستم در یک شبکه workgroup را با استفاده از نام به هم متّصل کنید.



به مانند شکل روبرو، system-1 با دستور Ping بررسی شده که این کار با موفّقیّت انجام شده است.

DNS های اینترنتی:

در اینترنت، خواسته و یا ناخواسته از سرورهای DNS استفاده می‌کنیم، مثلاً شرکت گوگل، دارای DNS بسیار قدرتمند است که شاید آدرس IP آن که 8.8.8.8 یا 8.8.4.4 را بشناسید و یا دیده باشید، در جدول زیر بعضی از ارائه‌دهنده‌های سرویس DNS را مشاهده می‌کنید که از سرعت و کیفیّت خوبی برخوردارند.

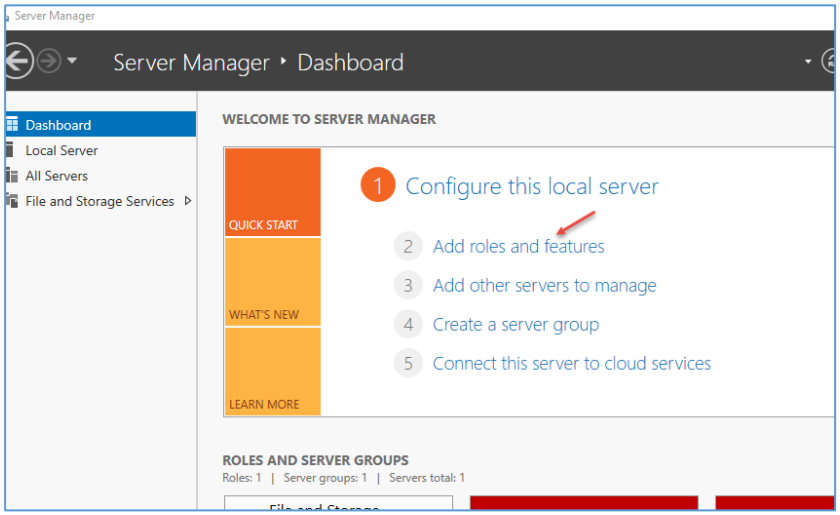
نام سرویس‌دهنده	آدرس DNS اصلی	آدرس DNS فرعی
Level3[1]	209.244.0.3	209.244.0.4
Verisign[2]	64.6.64.6	64.6.65.6
Google[3]	8.8.8.8	8.8.4.4
DNS.WATCH[4]	84.200.69.80	84.200.70.40
Comodo Secure DNS	8.26.56.26	8.20.247.20
OpenDNS Home[5]	208.67.222.222	208.67.220.220
DNS Advantage	156.154.70.1	156.154.71.1
Norton ConnectSafe[6]	199.85.126.10	199.85.127.10
GreenTeamDNS[7]	81.218.119.11	209.88.198.133
SafeDNS[8]	195.46.39.39	195.46.39.40
OpenNIC[9]	45.32.215.96	104.238.153.178
SmartViper	208.76.50.50	208.76.51.51
Dyn	216.146.35.35	216.146.36.36
FreeDNS[10]	37.235.1.174	37.235.1.177
Alternate DNS[11]	198.101.242.72	23.253.163.53
Yandex.DNS[12]	77.88.8.8	77.88.8.1
censurfridns.dk[13]	91.239.100.100	89.233.43.71
Hurricane Electric[14]	74.82.42.42	
puntCAT[15]	109.69.8.51	

بعد از معرّفی DNS خارجی باید نام دومین‌های عمومی، مانند COM یا NET را نیز بررسی کنید، در جدول زیر لیستی از محبوب‌ترین دومین‌ها را مشاهده می‌کنید.

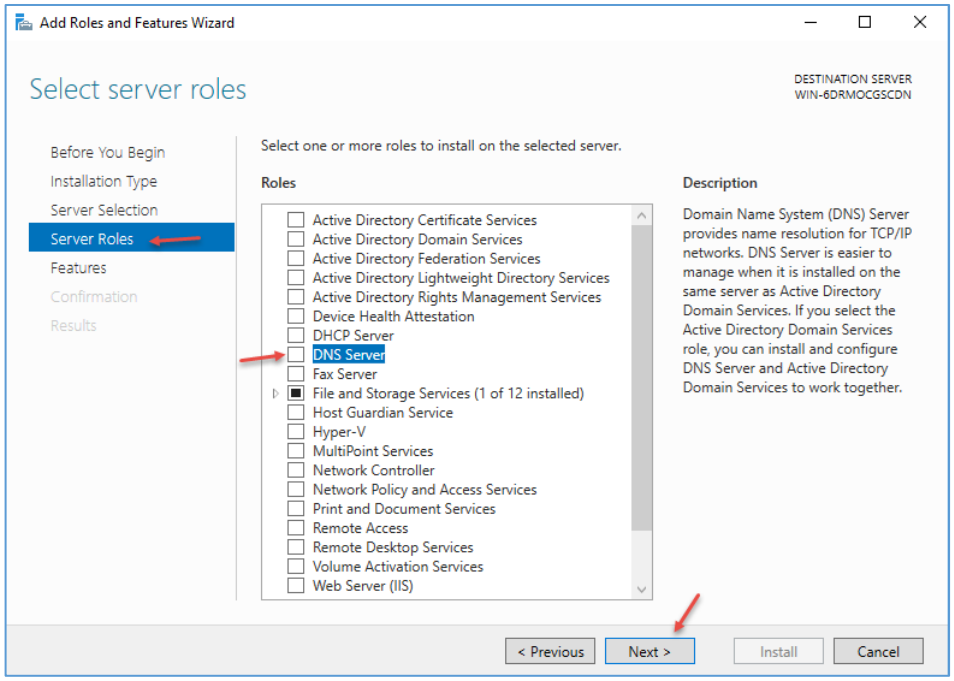
نام دومین	توضیحات
.com	تجاری
.org	سازمانی
.net	شبکه
.int	سازمان‌های جهانی
.edu	دانشگاهی
.gov	دولتی
.mil	وزارت دفاع ایالات متّحده‌ی آمریکا

همانطور که در جدول بالا مشاهده می‌کنید، چند نمونه از محبوب‌ترین دومین‌ها را مشخّص کردیم که اکثر سایت‌ها در جهان از این نام دامنه‌ها استفاده می‌کنند، البتّه نام‌های بسیاری وجود دارد که می‌توانید با یک جستجو در اینترنت به آنها دست پیدا کنید.

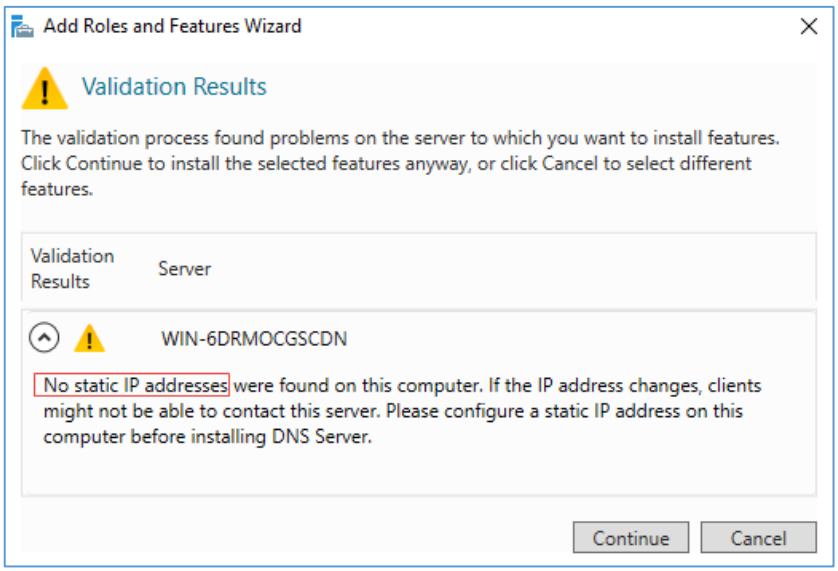
نصب و راه‌اندازی سرویس DNS:



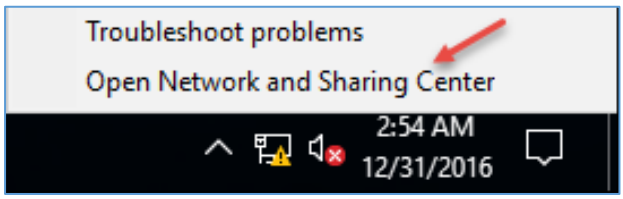
برای نصب سرویس DNS وارد ویندوز سرور شوید و Server Manager را اجرا کنید و در شکل روبرو بر روی Add roles and features کلیک کنید.



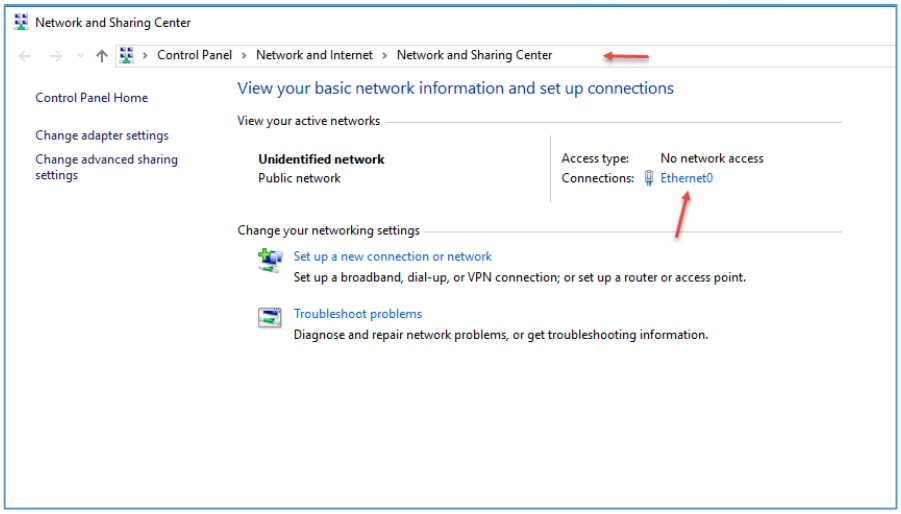
بر روی Next کلیک کنید تا به قسمت Server Roles برسید، در این قسمت بر روی DNS Servers کلیک کنید و در پنجره‌ی باز شده بر روی Add Features کلیک کنید.



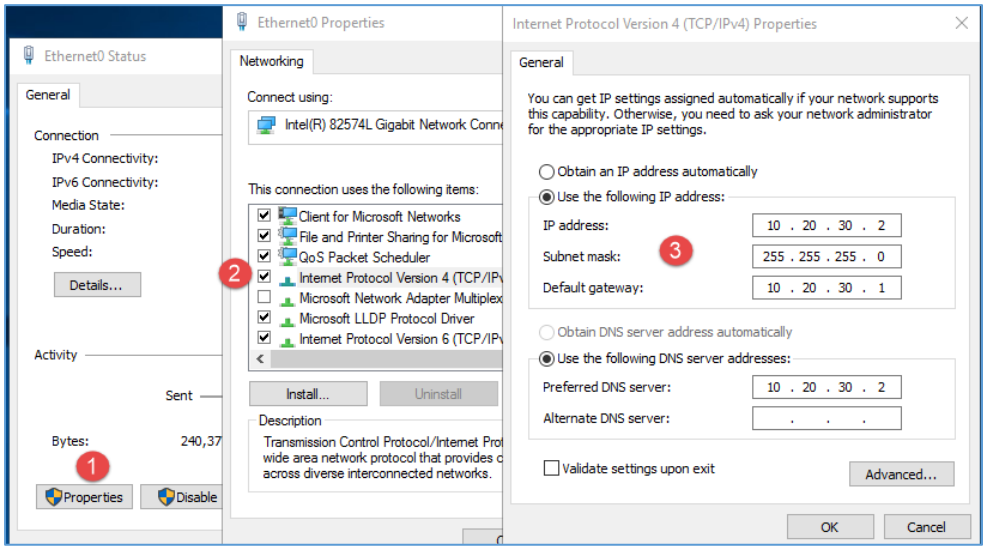
بعد از کلیک بر روی Add Features با پیغام اخطار روبرو مواجه خواهید شد که در این پیغام به این نکته اشاره دارد که آدرس IP سرور شما به صورت دستی وارد نشده است، اگر این کار را انجام ندهید در ادامه‌ی کار با مشکل مواجه خواهید شد، برای اینکه مشکلی پیش نیاید باید آدرس IP سرور را به صورت دستی وارد کنید.



در نوار Taskbar بر روی کارت شبکه خود کلیک راست کنید و گزینه‌ی Open Network and Sharing Center را انتخاب کنید.

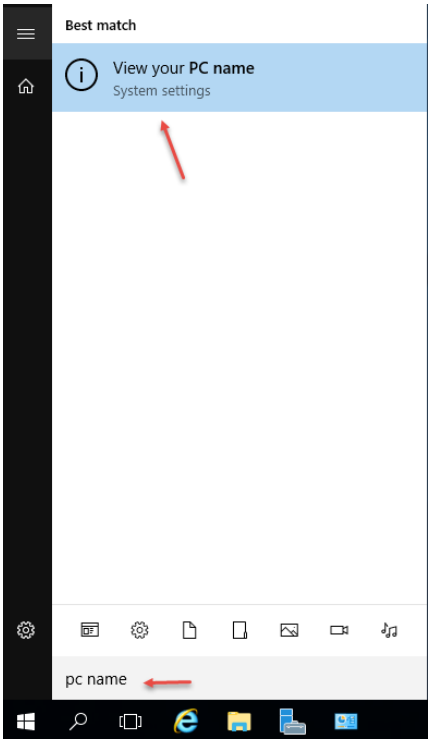


در این صفحه بر روی کارت شبکه‌ی خود کلیک کنید؛ به صورت پیش‌فرض نام کارت شبکه‌ی شما، Ethernet0 است، اگر چنانچه از چند کارت شبکه استفاده می‌کنید باید در شکل روبرو از سمت چپ بر روی Change Adaptor Settings کلیک کنید.

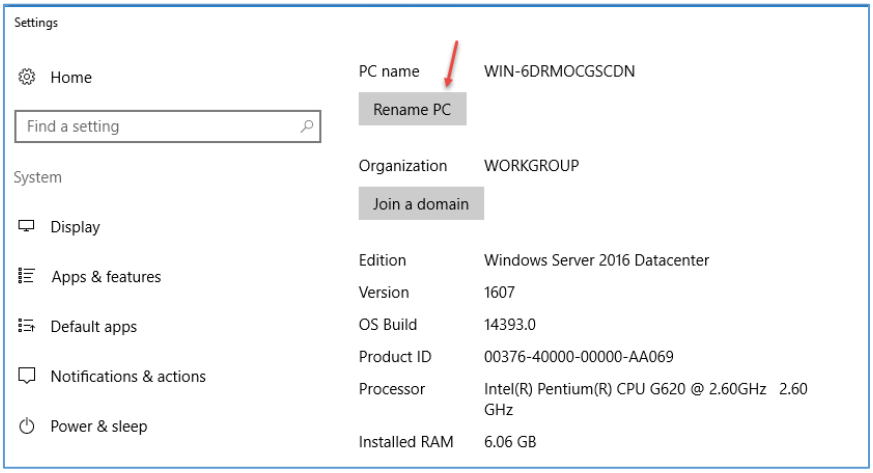


به مانند شکل روبرو در پنجره‌ی شماره‌ی یک بر روی Properties کلیک کنید و در قسمت شماره‌ی دو بر روی Internet Protocol Version 4، دو بار کلیک کنید و در قسمت آخر، آدرس IP شبکه‌ی خود را وارد کنید، سعی کنید آدرسی انتخاب کنید که در آینده مشکلی برای آن نداشته باشید؛ برای اینکه در کارهای خود منظّم باشید، سعی کنید آدرس‌های IP اوّل یک رنج و آخر یک رنج را برای سرورها و بقیّه را برای کلاینت‌ها در نظر بگیرید، البتّه در مورد این موضوع در سرویس DHCP بیشتر توضیح خواهیم داد؛ بر روی OK کلیک کنید تا اطّلاعات ذخیره شود.

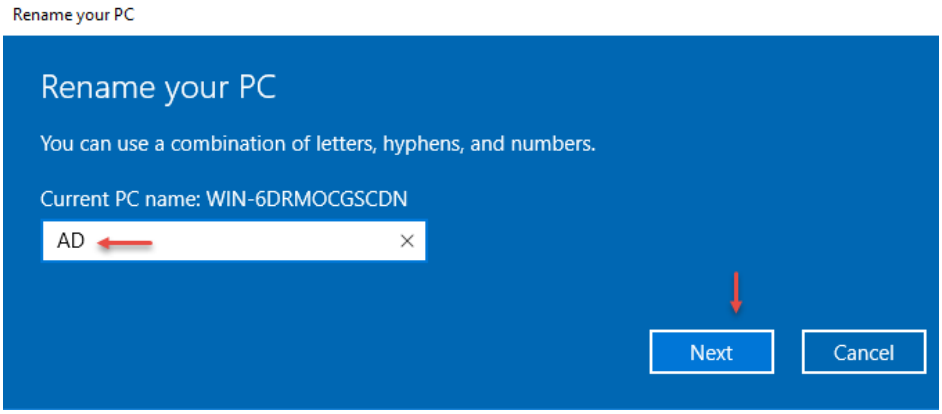
در مرحله‌ی بعد باید نام سرور اصلی خود را تغییر دهید، برای انتخاب اسم نیز سعی کنید از اسم‌های کوتاه و با معنی استفاده کنید، مثلاً AD یا DC و...، البتّه انتخاب اسم بستگی به سرور دارد، چون اوّلین سرور اصولاً Active directory در نظر گرفته می‌شود و روی آن domain فعّال می‌شود، اسم آن را نیز به این صورت در نظر بگیرید.



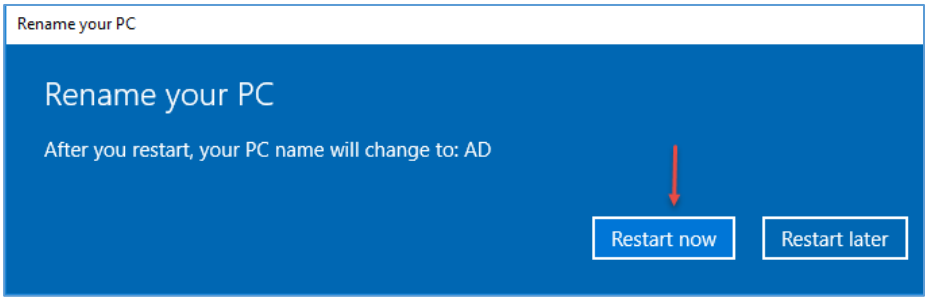
برای تغییر نام در ویندوز سرور ۲۰۱۶ وارد Start شوید و PC Name را وارد کنید و به مانند شکل روبرو بر روی گزینه‌ی View your PC name کلیک کنید تا شکل بعد ظاهر شود.



در این صفحه بر روی Rename PC کلیک کنید و نام مورد نظر خود را وارد کنید.



در این صفحه، نام سرور را وارد و بر روی Next کلیک کنید.



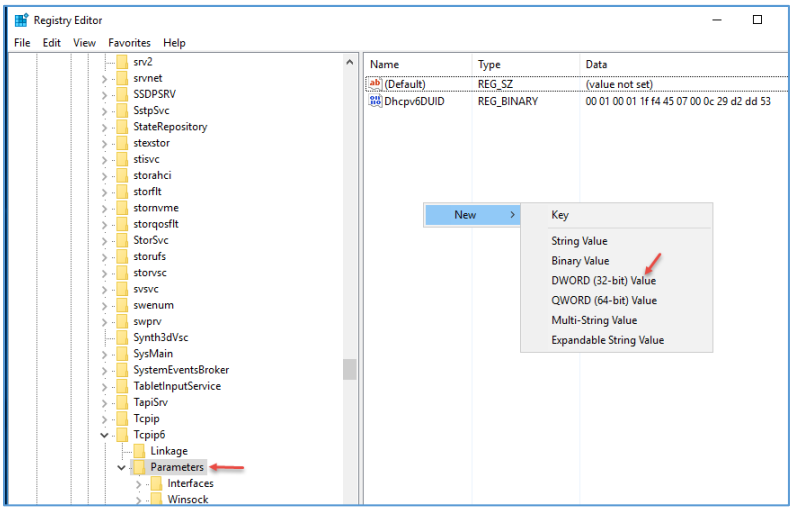
در این صفحه برای Restart شدن سرور بر روی Restart now کلیک کنید.

غیرفعّال کردن IPV6:

اگر در شبکه‌ی خود از IPV6 استفاده نمی‌کنید، بهتر است آن را در همه‌ی سرورها غیرفعّال کنید تا در ادامه‌ی کار با مشکل مواجه نشوید.

وارد Start شوید و Regedit را اجرا کنید و وارد آدرس زیر شوید.

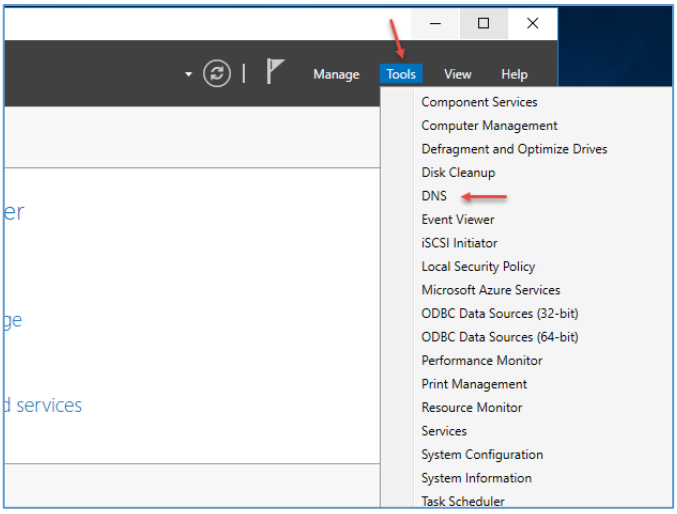
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\



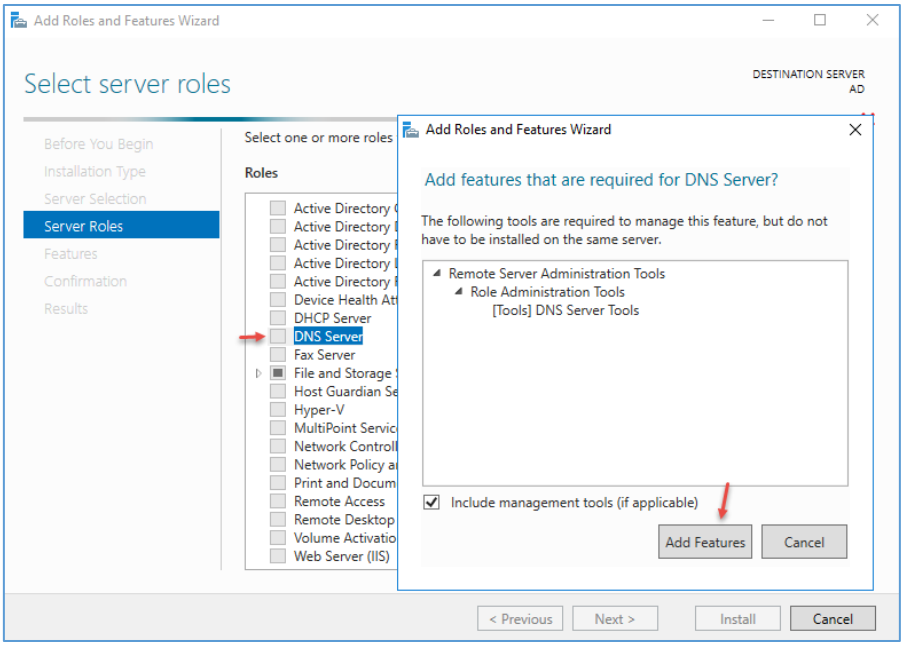
به مانند شکل در صفحه‌ی مورد نظر کلیک راست کنید و از قسمت New، گزینه‌ی DWORD (32 bit) value را انتخاب و نام زیر را وارد کنید:

DisabledComponents

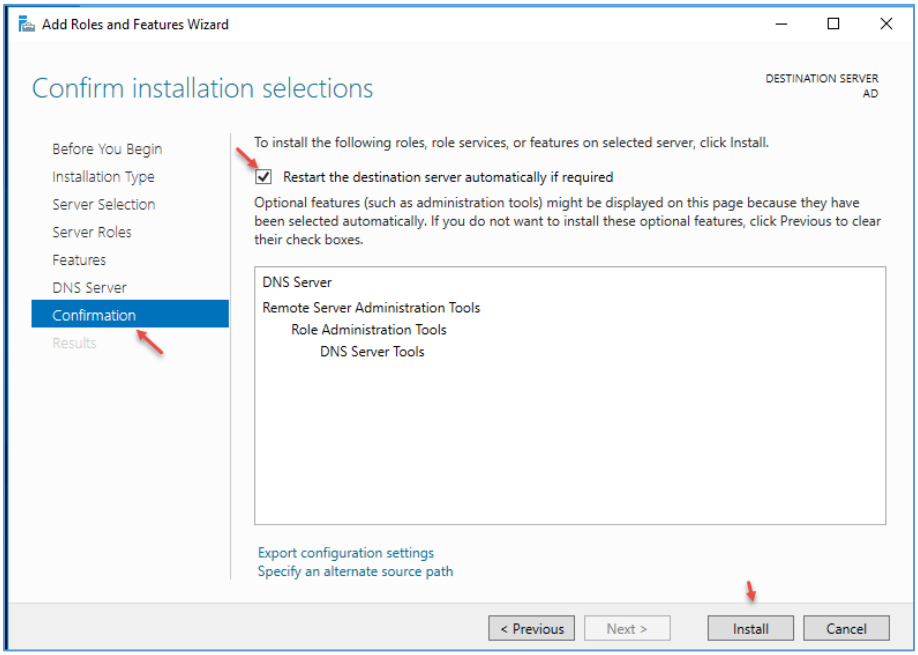
بعد از ایجاد، بر روی آن دو بار کلیک کنید و ffffffff را وارد کنید و سرور را Restart کنید.



بعد از ورود به سرور وارد Server Manager شوید و از قسمت Tools، گزینه‌ی DNS را انتخاب کنید.

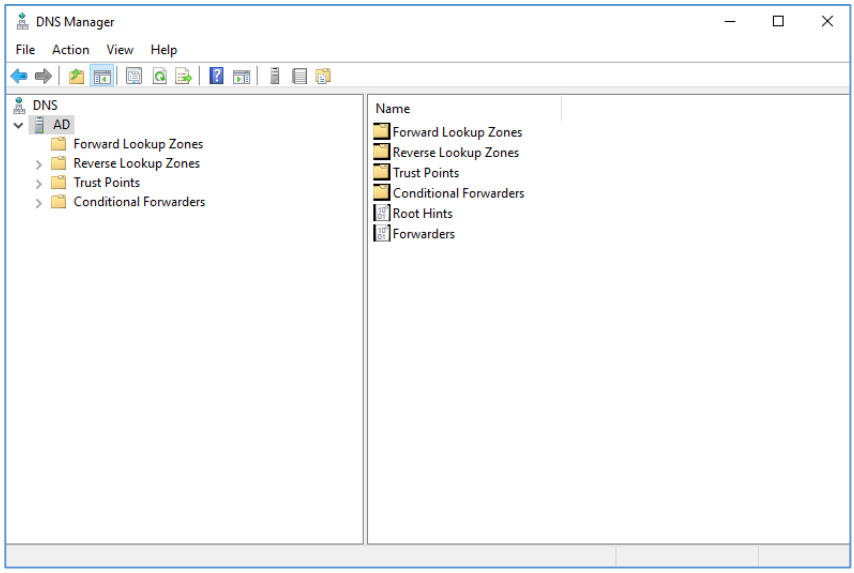


بعد از اینکه آدرس IP را وارد کردید و نام سرور را تغییر دادید، دوباره وارد Server Manager شوید و به مانند شکل روبرو در قسمت Server Roles، تیک گزینه‌ی DNS Server را انتخاب و بر روی Add Features کلیک کنید، بعد از آن بر روی Install کلیک کنید و اگر صفحه‌ی اخطار باز شد بر روی Continue کلیک کنید.



بر روی Next کلیک کنید تا به قسمت Confirmation برسید، در این صفحه، تیک گزینه‌ی Restart... را انتخاب و بر روی Install کلیک کنید.

اگر بعد از نصب، سرور Restart نشد، خودتان این کار را انجام دهید.

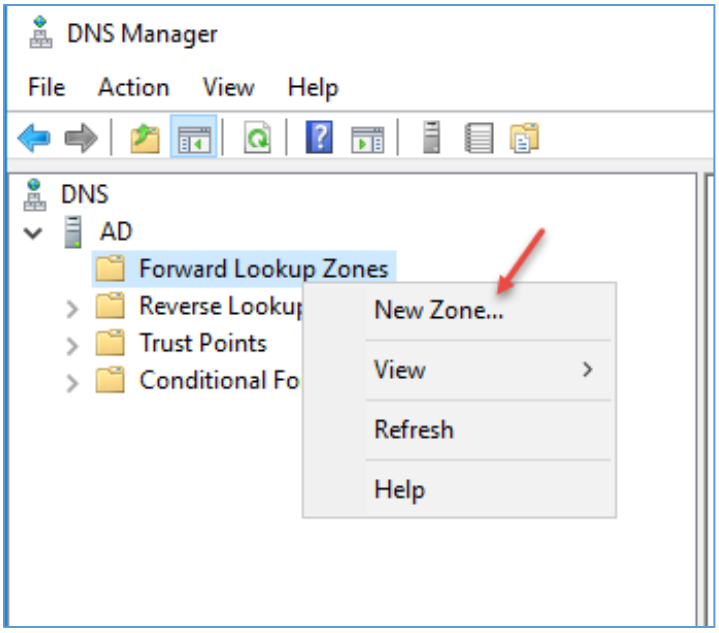


در شکل روبرو سرویس DNS را مشاهده می‌کنید، این سرویس از قسمت‌های مختلفی تشکیل شده است که گزینه‌های آن را در این قسمت بررسی خواهیم کرد.

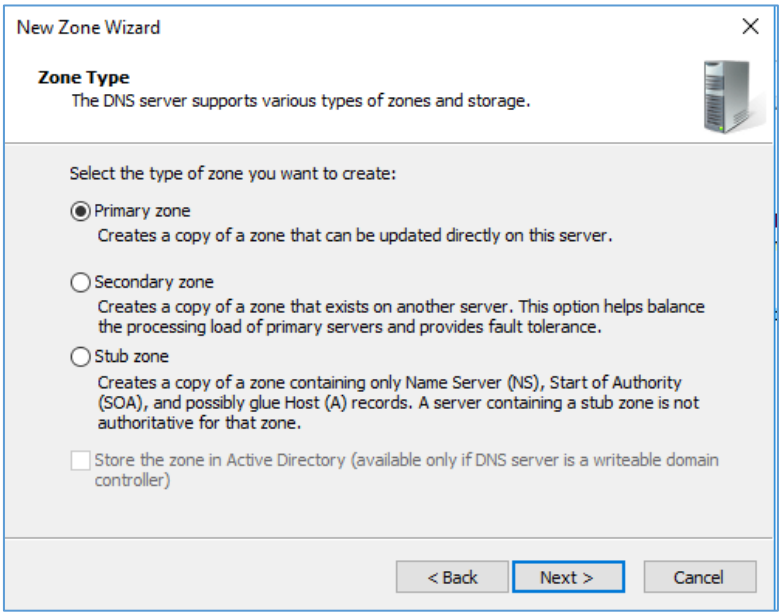
۱- Forward LoOKup Zones:

این قسمت یکی از اصلی‌ترین گزینه‌های سرویس DNS است که در آن می‌توانید Zone مورد نظر خود را تعریف کنید؛ منظور از Zone، همان نام دومین شما است که در قسمت‌های قبل توضیح دادیم، زمانی‌که شما سرویس Active Directory (در ادامه روی آن کار خواهیم کرد) را راه‌اندازی می‌کنید باید یک نام دومین برای آن در نظر بگیرید، زمانی که نام را وارد می‌کنید، آن نام به صورت خودکار در قسمت Forward LoOKup Zones ایجاد می‌شود و بعد از آن، تمام اطّلاعات سرورها و کلاینت‌ها در آن وارد می‌شود.

به طور مثال در این قسمت برای شما یک Zone ایجاد می‌کنیم تا توضیحات مورد نظر را بیان کنیم.



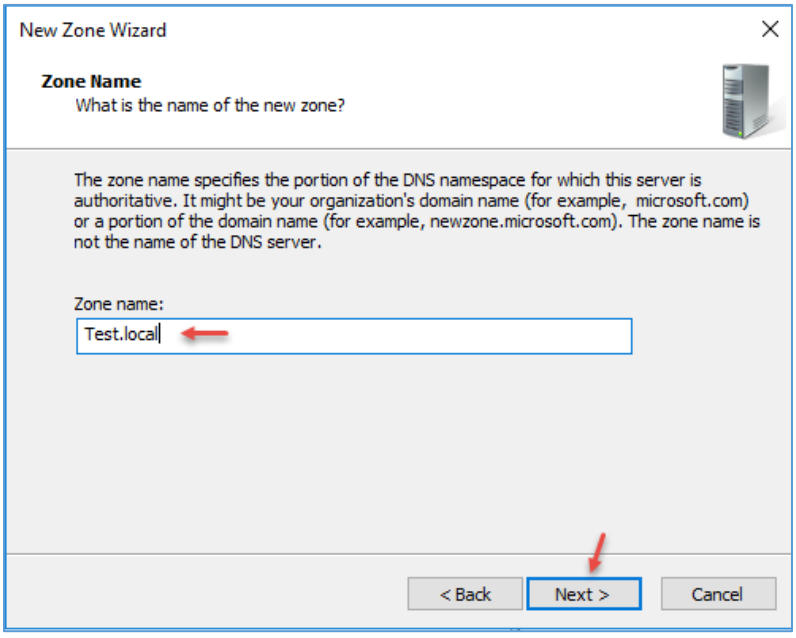
بر روی Forward LoOKup Zones کلیک راست کنید و گزینه‌ی New Zone را انتخاب کنید و در صفحه‌ی باز شده بر روی Next کلیک کنید تا شکل بعد ظاهر شود.



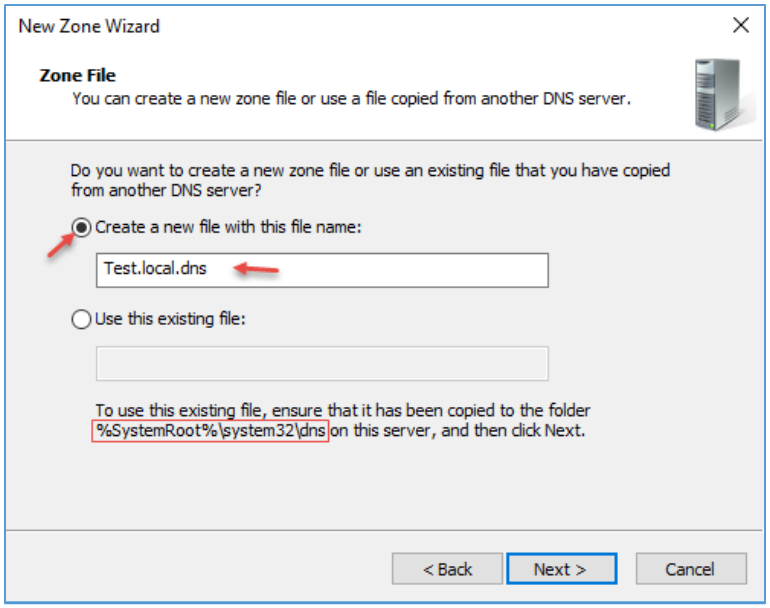
در این صفحه، سه گزینه را مشاهده می‌کنید، گزینه‌ی Primary zone، یک دیتابیس کلّی از همه‌ی اطّلاعات یک سرور است که اطلاعات در آن ذخیره می‌شود و اگر شما برای اوّلین بار می‌خواهید یک سرور DNS را راه-اندازی کنید باید این گزینه را انتخاب کنید. در ویندوز سرور، دو نوع Primary zone وجود دارد، یکی که خود Primary zone است که شما به صورت دستی، مثل الآن که انجام دادید، ایجاد می‌کنید و دیگری، Primary zone است که توسط سرور Active Directory ایجاد می‌شود.

گزینه‌ی بعدی، Secondary Zone است، همچنان که از نام آن پیداست، یک کپی از Primary Zone در یک سرور دیگر است تا بتواند هم‌زمان از دو DNS سرور استفاده کند؛ با این حال اگر در هر دو سرور، اطّلاعاتی تغییر کند، در سرور دیگر نیز تغییر خواهد کرد.

گزینه‌ی آخر، یعنی Stub zone، دقیقاً همان دیتابیس Secondary Zone است، با این تفاوت که هیچ تغییری نمی‌توانید در آن ایجاد کنید.

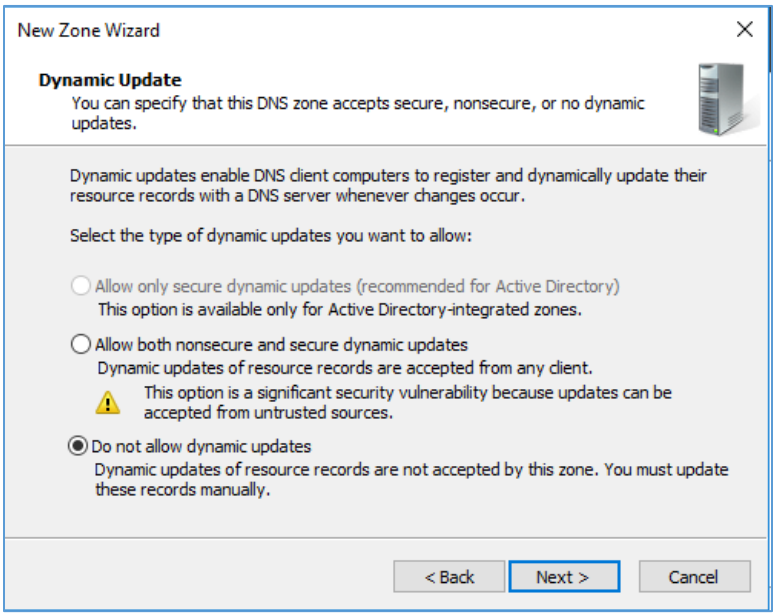


بعد از انتخاب گزینه‌ی Primary zone باید نام دومین خود را وارد کنید که در اینجا برای تست، نام Test.local را وارد کردیم، شما می‌توانید هر اسم دیگری، مانند Google.com یا MSN.com وارد کنید، البتّه این دومین‌ها، تنها در شبکه‌ی داخلی اعتبار دارند؛ بر روی Next کلیک کنید.



در این قسمت باید Zone File جدید خود را با انتخاب گزینه‌ی Create a new... و وارد کردن نام مورد نظر خود ایجاد کنید، توجّه داشته باشید اگر از قبل، Zone File ایجاد کرده باشید، می‌توانید آن را در آدرس %systemRoot%\system32\dns قرار دهید و نام آن را در قسمت Use this existing وارد کنید.

در حال حاضر، گزینه‌ی اوّل را انتخاب و بر روی Next کلیک کنید.



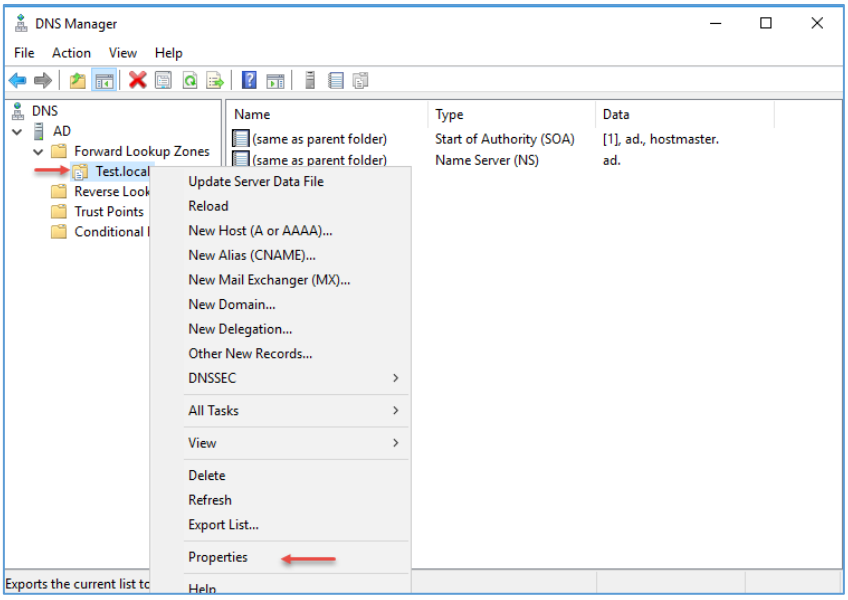
در این صفحه باید نوع Dynamic Update را انتخاب کنید، اگر شما به صورت دستی، دومین خود را ایجاد کردید، گزینه‌ی آخر را انتخاب کنید، البتّه اگر بخواهید از سرویس DHCP استفاده کنید تا بتوانید تغییرات کلاینت‌ها را در DNS ذخیره کنید باید گزینه‌ی دوّم را انتخاب کنید.

به این نوع DNS که به صورت دستی آپدیت می‌شود، به اصطلاح Non-Dynamic DNS می‌گویند که قابلیّت Update به صورت خودکار را نخواهد داشت.

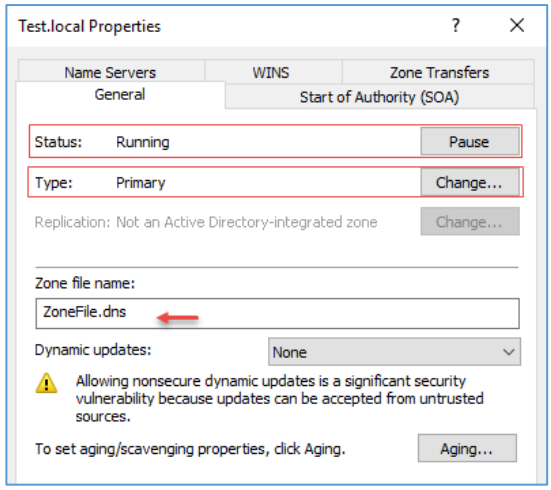
گزینه‌ی آخر را انتخاب و بر روی Next کلیک کنید.

در صفحه‌ی آخر نیز بر روی Finish کلیک کنید تا دومین مورد نظر شما یا همان، Zone جدید ایجاد شود.

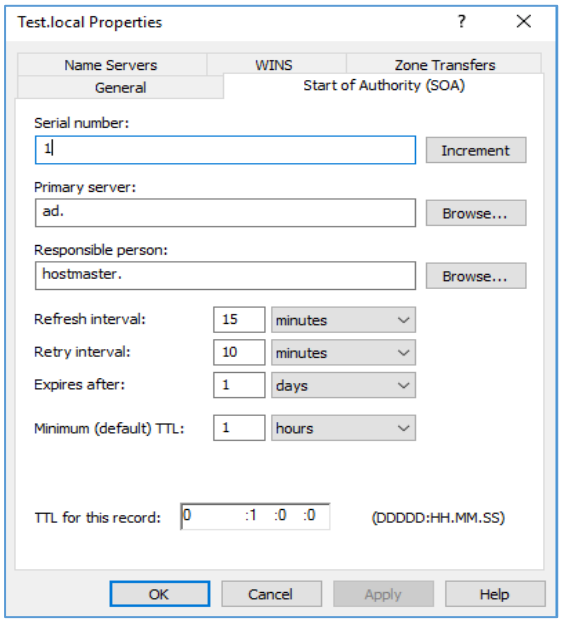
نکته: تمام این مراحل تستی است، در ادامه به صورت کامل‌تر روی آن بحث خواهیم کرد.



همانطور که در شکل روبرو مشاهده می‌کنید، دومین مورد نظر ایجاد شده است؛ برای بررسی جزئیّات کار بر روی آن کلیک راست و گزینه‌ی Properties را انتخاب کنید.



در این صفحه و در تب General، اگر دکمه‌ی Pause را جلوی Status کلیک کنید، این Zone غیر فعّال خواهد شد و توانایی دادن سرویس را نخواهد داشت، در قسمت Type نیز می‌توانید، نوع Zone خود را از Primary به Zone های دیگر تغییر دهید و در قسمت Zone File Name، نام Zone خود را مشاهده کنید.



در تب SOA، گزینه‌های مختلفی وجود دارد که با هم بررسی می‌کنیم.

Serial Number: شماره‌ای است که به دیتابیس سرویس DNS تعلّق می‌گیرد و با هر تغییر در دیتابیس، این شماره نیز تغییر خواهد کرد. در قسمت Primary Server، نام سرور اصلی DNS نوشته شده است که در اینجا، Ad است.

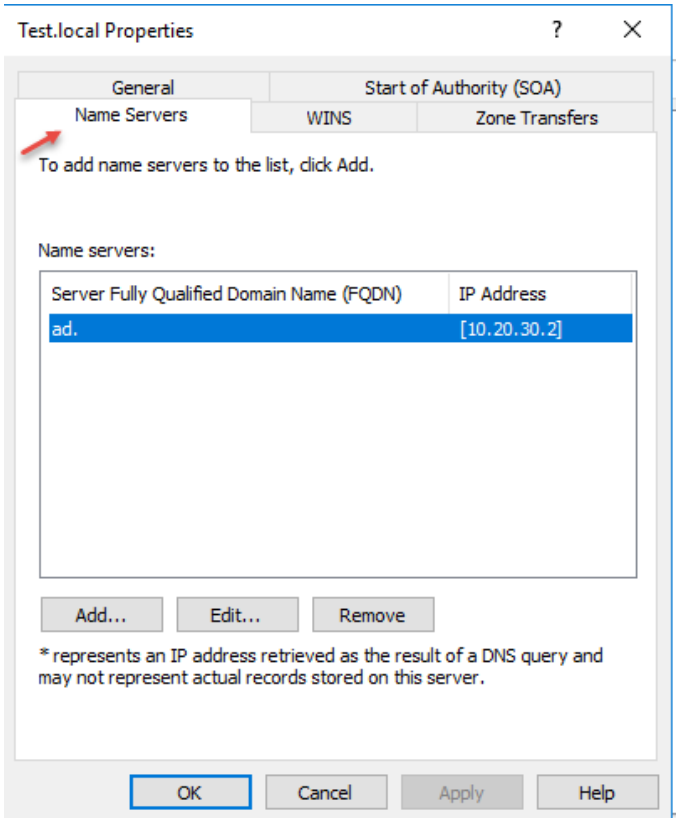
Responsible person: این فایل، شامل آدرس ایمیل مدیر سرور است که شامل علامت @ نیست؛ برای اینکه علامت @ یک علامت خاص است و قابل پذیرش نیست و به جای آن از نقطه استفاده می‌کنند.

Refresh Interval: نشان‌دهنده‌ی مدّت زمان ۱۵ دقیقه است که یک سرور دیگر، منتظر بررسی تغییر دیتابیس است، اگر دیتابیس تغییر کرده باشد، خود را با سرور اصلی هماهنگ می‌کند.

Retry interval: نشان‌دهنده‌ی مدّت زمانی است که یک خطا در آپدیت اطّلاعات رخ داده است، برای همین تا مدّت زمان مشخّص شده، صبر می‌کند و دوباره درخواست بررسی را ارسال می‌کند.

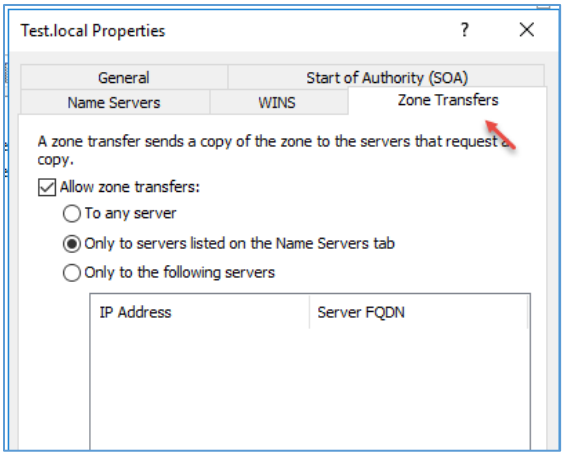
Expiration after: مدّت زمانی برای دانلود اطّلاعات از سرور است که یک روز در نظر گرفته شده است، بعد از این زمان، اطّلاعات منطقه‌ی زمانی قدیمی حذف خواهد شد.

TTL: مدّت زمان ارتباط سرورهای دیگر با کش سرور اصلی است که اجازه می‌دهد، اطّلاعات را از دیتابیس دریافت کند، بعد از این زمان، ارتباط نامعتبر خواهد بود.

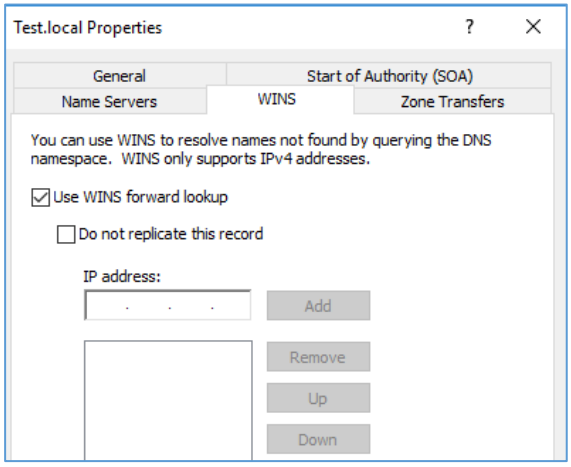


در تب **Name Servers**، شما می‌توانید نام تمام **DNS** سرورهای خود را مشاهده کنید، شاید شما به علّت وسعت شبکه‌ی خود از چندین **DNS** سرور استفاده کنید که در این قسمت، لیست این سرورها را قابل مشاهده است.

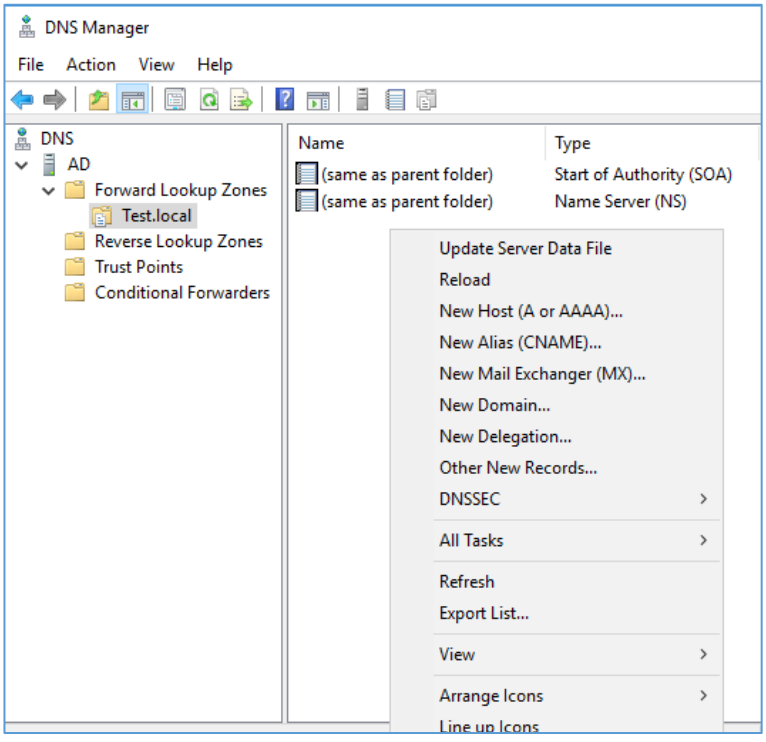
برای اینکه سرور **DNS** مشخّصی را به لیست اضافه کنید باید بر روی **Add** کلیک کنید و نام سرور خود را وارد کنید.



در قسمت Zone Transfer، می‌توانید مشخّص کنید که فایل دیتابیس شما به چه سرورهایی فرستاده شود؛ طبق شکل روبرو به صورت پیش‌فرض، گزینه‌ی دوّم انتخاب شده است که به این نکته اشاره دارد که یک کپی از فایل دیتابیس، تنها برای سرورهایی ارسال شود که نام آنها در تب Name Server آمده باشد، در غیر این صورت، این کار امکان‌پذیر نیست.



در تب WINS می‌توانید سرور WINS خود را در لیست مورد نظر وارد کنید؛ سرویس WINS، یک سرویس قدیمی برای تبدیل IP به اسم است که فعلاً کاری با آن نداریم.



اگر وارد Zone جدید خود با نام Test.local شوید و در صفحه‌ی خالی کلیک راست کنید، چندین گزینه را مشاهده می‌کنید، گزینه‌ی New Host یا AAAA که در اصطلاح به آن A record نیزمی‌گویند، برای تبدیل اسم به IP کاربرد دارد که این یکی از مهمترین کارهای DNS است.

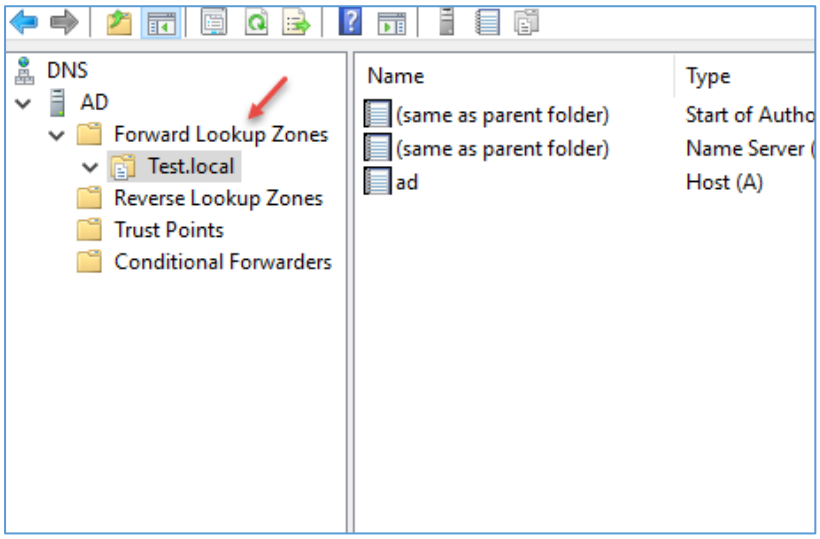
گزینه‌ی بعدی، New Alias و یا در اصطلاح عموم، CNAME است که با استفاده از این گزینه می‌توانید یک نام مستعار برای یک a record

ایجاد کنید، مثلاً اگر یک سرور با نام AD با استفاده از A Record ایجاد کردید و می‌خواهید یک نام دیگر نیز به سرور Ad اختصاص دهید، می‌توانید از این گزینه استفاده کنید. بهترین مورد استفاده از این گزینه را می‌توان در نرم‌افزار Lync یا Exchange دید که برای نصب سرویس‌های خودشان نیاز دارند تا چند اسم را به یک سرور اختصاص دهند؛ در ادامه‌ی کار به صورت عملی با این گزینه آشنا خواهید شد.

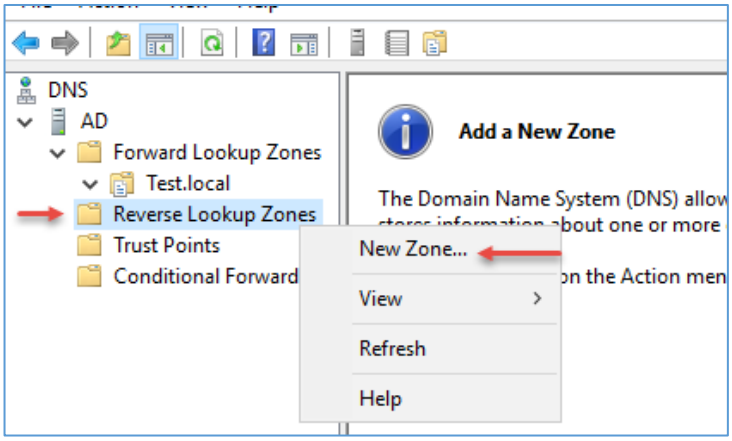
گزینه‌ی بعدی، New Mail Exchanger یا MX است که برای مشخّص کردن سرور ایمیل شبکه‌ی شما است، مثلاً اگر در شبکه‌ی خود از Exchange (ایمیل سرور) استفاده می‌کنید، می‌توانید نام آن را در این قسمت وارد کنید. این قسمت دارای اولّویت‌بندی از شماره ۱۰ به بعد است که بر فرض، اگر در شبکه‌ی خود از چندین ایمیل سرور استفاده می‌کنید، می‌توانید برای آنها اولویت‌بندی کنید.

گزینه‌ی New domain نیز برای ایجاد یک Sub domain یا دومین زیرین دومین اصلی است، مثلاً اگر، نام دومین شما Test.local باشد، با انتخاب این گزینه می‌توانید یک نام، مثلاً software به صورت Software.test.local ایجاد کنید و بعد از ایجاد آن می‌توانید نام سرورهای زیر مجموعه‌ی آن را وارد کنید.

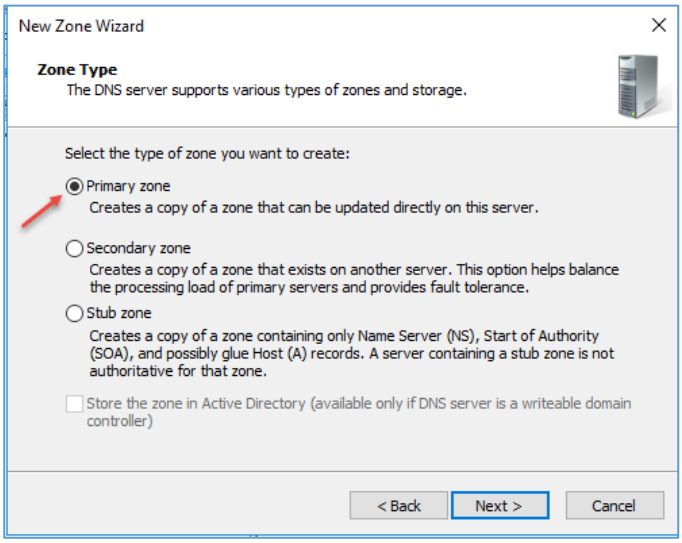
گزینه‌ی Other New Records، خود دارای چندین گزینه است که برای کارهای خاصّی ایجاد شده است.



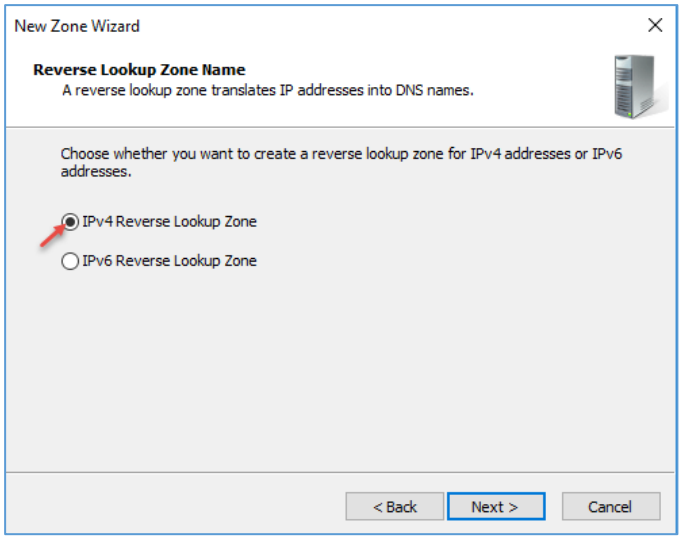
تا به اینجا، گزینه‌ی Forward LoOKup Zones را بررسی کردیم که برای ایجاد Zone یا همان دومین شما کاربرد دارد و کار اصلی آن نیز تبدیل یک نام به آدرس IP است، یعنی اگر این سرویس فعّال نباشد و ما بخواهیم یک نام را در شبکه، Ping کنیم با مشکل مواجه خواهیم شد و این کار عملی نیست، اگر عملکرد سرویس را فرا نگرفتید، نگران نباشید، چون در ادامه به صورت یک سناریوی واقعی بر روی آن بحث خواهیم کرد.



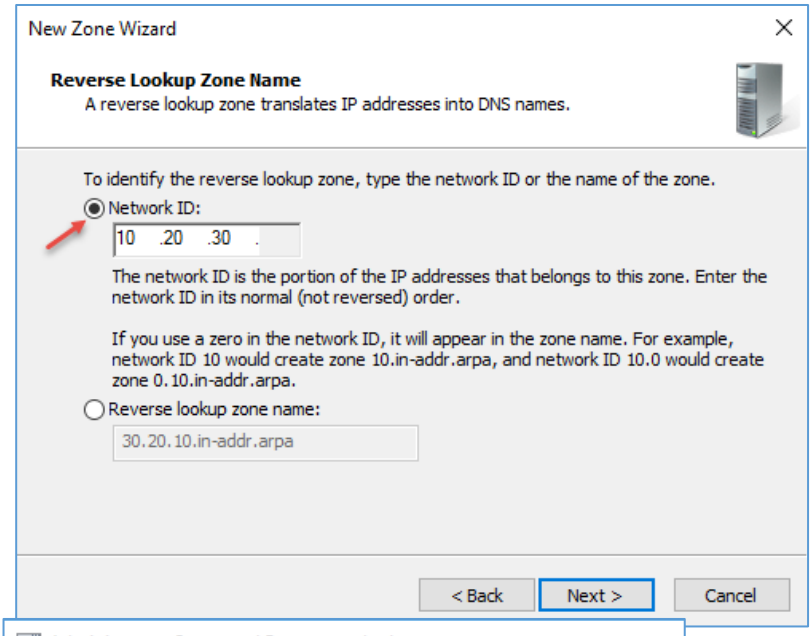
بعد از بررسی forward LoOKup Zones، نوبت به بررسی Revers LoOKup zones می‌رسد؛ این گزینه برعکس گزینه‌ی اوّل عمل می‌کند و برای تبدیل IP به اسم استفاده می‌شود، برای تست این موضوع بر روی Revers LoOKup zones کلیک راست کنید و گزینه‌ی New Zone را انتخاب کنید.



در این قسمت که قبلاً توضیحات آن را بیان کردیم، گزینه‌ی Primary Zone را ایجاد و بر روی Next کلیک کنید.

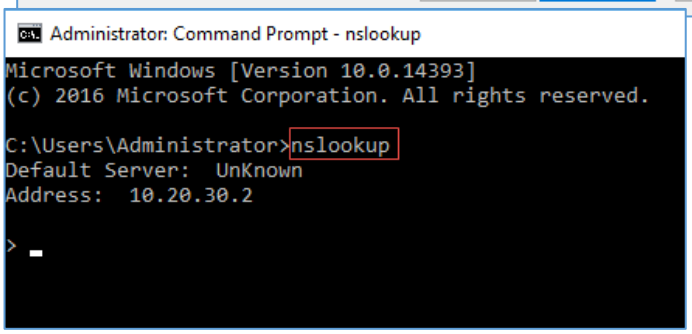


در این صفحه باید ورژن IP مورد استفاده در شبکه‌ی خود را انتخاب کنید، در این قسمت IPV4 را انتخاب کنید.

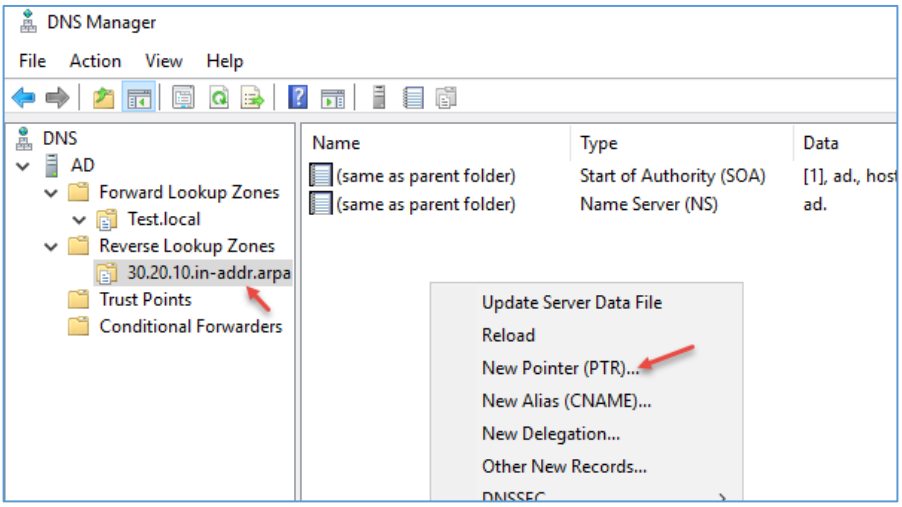


در این قسمت باید Network ID خود را وارد کنید که در شکل روبرو 10.20.30 وارد کردیم، بر روی Next کلیک کنید.

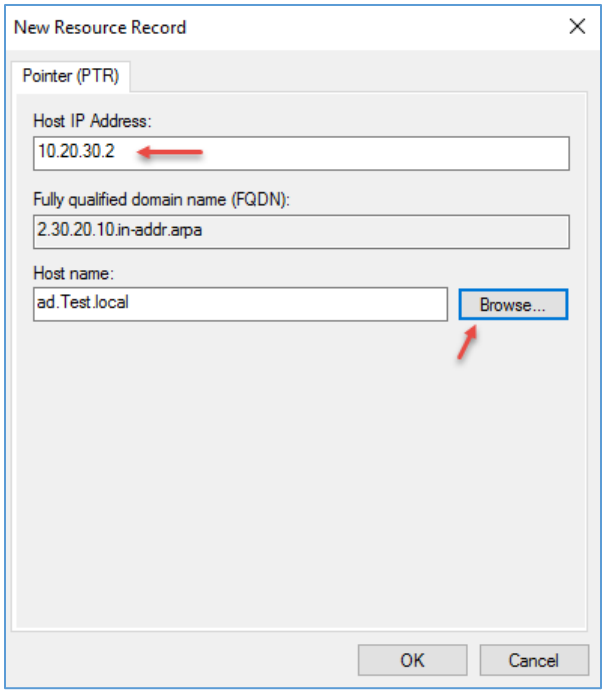
در صفحات بعد نیز بر روی Next کلیک کنید و در صفحه‌ی آخر بر روی Finish کلیک کنید.



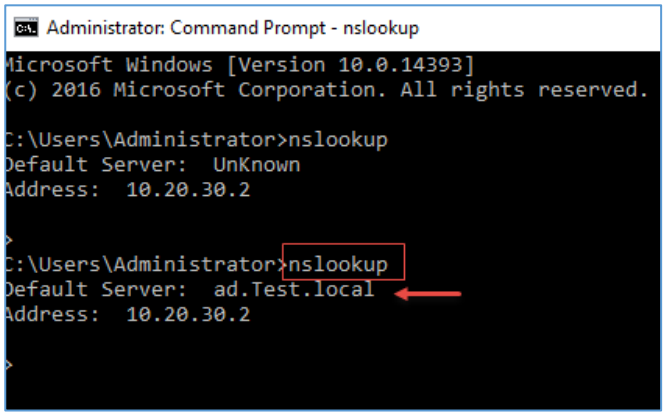
اگر وارد CMD شوید و دستور nsloOKup را اجرا کنید به شما آدرس سرور DNS را می‌دهد، امّا نام آن را نمایش نمی‌دهد که برای حلّ این مشکل باید کارهای زیر را انجام دهید.



در این صفحه وارد Zone جدید در Reverse LoOKup Zones شوید و با کلیک راست در جای مشخّص شده، گزینه‌ی New Pointer را انتخاب کنید.



در این صفحه، آدرس IP سرور DNS مشخّص شده است که برای اتّصال این آدرس به نام باید بر روی Browse کلیک کنید و از قسمت Forward LoOKup Zones، نام سرور را انتخاب و بر روی OK کلیک کنید.



بعد از ایجاد PTR یا همان، New Pointer وارد CMD شوید و دستور NSloOKup را دوباره اجرا کنید، همانطور که در شکل روبرو مشاهده می‌کنید، دستور مورد نظر به خوبی عمل کرده و عملیّات تبدیل IP به اسم انجام شده است.

برای اینکه بتوانید مشخّصات کامل کارت شبکه را مشاهده کنید باید از دستور ipconfig استفاده کنید؛ در شکل روبرو، دستور ipconfig به تنهایی اجرا شده است و اطّلاعاتی از نام قبلی کارت شبکه که Ethernet0 است و آدرس IP، Subnet mask و Default Gateway برای شما مشخّص کرده است.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.20.30.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.20.30.1

C:\Users\Administrator>
```

اگر بخواهید اطّلاعات بیشتری از شبکه به دست آورید باید از دستور ipconfig /all استفاده کنید؛ با این دستور، اطّلاعات کامل‌تری از سرور به دست می‌آورید. در شکل روبرو نام سرور، نام کارت شبکه و کارخانه‌ی تولیدی آن به همراه مک آدرس مشخّص شده است، همچنین در این دستور می‌توانید ببینید که آیا کارت شبکه در حالت DHCP (سرویسی که در شبکه به دستگاه‌های شبکه، آدرس IP به صورت خودکار اختصاص می‌دهد) قرار دارد یا نه و یا می‌توانید سرور DNS و... را ببینید.

```
Administrator: Command Prompt

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : AD
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

C:\Users\Administrator>ipconfig ?

Error: unrecognized or incomplete command line.

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                    ... Show information
    > ipconfig /all               ... Show detailed information
    > ipconfig /renew             ... renew all adapters
    > ipconfig /renew EL*         ... renew any connection that has its
                                      name starting with EL
    > ipconfig /release *Con*     ... release all matching connections,
                                      eg. "Wired Ethernet Connection 1" or
                                          "Wired Ethernet Connection 2"
    > ipconfig /allcompartments   ... Show information about all
```

دستور ipconfig از سوئیچ‌های دیگری نیز برخوردار است، برای اینکه همه‌ی سوئیچ-های مربوط به دستور ipconfig را دریابید، تنها کافی است از دستور ipconfig ? استفاده کنید؛ با این دستور، اطّلاعات کامل‌تری از سرور به دست می‌آورید. در شکل روبرو نام سرور، نام کارت شبکه و کارخانه‌ی تولیدی آن به همراه مک آدرس مشخّص شده است، همچنین در این دستور می‌توانید ببینید که آیا کارت شبکه در حالت DHCP (سرویسی که در شبکه به دستگاه‌های شبکه، آدرس IP به صورت خودکار اختصاص می‌دهد) قرار دارد یا نه و یا می‌توانید سرور DNS و... را ببینید.

استفاده کنید؛ همانطور که در شکل روبرو مشاهده می‌کنید، دستورات زیر مجموعه‌ی ipconfig مشخّص شده است، مثلاً دستور ipconfig /release برای از دست دادن آدرس IP در حالت DHCP است که در ادامه با این دستور زیاد کار خواهیم کرد و برای شما به عنوان مدیر شبکه، کارآمد خواهد بود.

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

Windows IP Configuration

    2.1.168.192.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 2.1.168.192.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 86400
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : system-2


    system-2
    ----------------------------------------
    No records of type AAAA


    system-2
    ----------------------------------------
    Record Name . . . . . : system-2
    Record Type . . . . . : 1
    Time To Live  . . . . : 86400
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168.1.2


C:\Users\Administrator>
```

به عنوان مثال، اگر از دستور ipconfig /displaydns به مانند شکل روبرو استفاده کنید، برای شما تمام آدرس‌های DNS که در آدرس

C:\Windows\System32\drivers\etc\hosts

قرار دارد را مشخّص می‌کند.

نکته‌ی مهم: همیشه اولویّت DNS داخلی که در آدرس زیر:

C:\Windows\System32\drivers\etc\hosts

قرار دارد و تنها نیز در همان کلاینت یا سرور قرار دارد، بالاتر از DNS شبکه‌ی شما است که این موضوع می‌تواند گشایش‌گر مشکلات شما در شبکه باشد.

تا به اینجا، ویندوز سرور ۲۰۱۶ را نصب کردیم و آدرس IP به آن تخصیص دادیم و اسم آن را نیز تغییر دادیم، در ادامه‌ی کار، سرویس DNS را توضیح و نصب کردیم و جزئیّات آن را نیز بررسی کردیم تا در ادامه که از این سرویس استفاده می‌کنیم با مشکل مواجه نشویم.

در ادامه‌ی کار می‌خواهیم سرویس DHCP را به شما معرّفی کنیم و آن را بر روی سرور نصب کنیم و جزئیّات این سرویس را نیز بیان کنیم.

سعی کنید کاملاً طبق کتاب پیش بروید تا تمام موضوعات را به راحتی و عالی فرا بگیرید.

نکته‌ی آخر آن است که برای اینکه یک کلاینت بتواند از سرویس DNS در شبکه استفاده کند، حتماً باید سرویس DNS Client روی آن فعّال باشد تا بتواند از DNS Server استفاده کند.

بررسی سرویس DHCP:

زمانی که یک شبکه را راه‌اندازی می‌کنید باید مشخّص کنید که چگونه می‌خواهید به دستگاه‌های موجود در شبکه، مانند دوربین‌ها، پرینترها، کلاینت‌ها و... آدرس دهید، شما می‌توانید تمام دستگاه‌های موجود در شبکه را به صورت دستی IP دهید، این کار در یک شبکه‌ی کوچک که کمتر از ۱۰ کلاینت دارد می‌تواند روش خوبی باشد، امّا برای شبکه‌های بزرگ که در هر لحظه، سیستم‌های جدید وارد و سیستم‌های قدیمی خارج می‌شوند می‌تواند کار عذاب‌آوری برای یک مدیر شبکه باشد.

برای حل این مسائل، سرویسی با عنوان Dynamic Host Configuration Protocol یا در اختصار، DHCP ایجاد شده است تا کار مدیران شبکه را راحت کند، این سرویس با گرفتن رنج IP مشخّص به تمام دستگاه‌های شبکه، یک IP مشخّص را در اختیار آنها قرار می‌دهد که این IP می‌تواند دارای مدّت انقضا نیز باشد؛ در ادامه‌ی این مبحث، آن را بر روی سرور نصب و با آن کار خواهیم کرد.

عملکرد DHCP به چهار قسمت پایه تقسیم می‌گردد:

- اکتشاف (DHCP Discovery)
- پیشنهاد (DHCP Offer)
- درخواست (DHCP Request)
- تصدیق (DHCP Acknowledgement)

این چهار مرحله به صورت خلاصه با عنوان DORA شناخته می‌شوند که هر یک از حروف، اوّل حرف مراحل بالا است.

اکتشاف (DHCP Discovery):

هر کاربر (سرویس‌گیرنده) برای شناسایی سرورهای DHCP موجود، اقدام به فرستادن پیامی در زیر شبکه‌ی خود می‌کند. مدیرهای شبکه می‌توانند مسیریاب محلّی را به گونه‌ای پیکربندی کنند که بتوانند بسته‌ی داده‌ایDHCP را به یک سرور DHCP دیگر که در زیر شبکه‌ی متفاوتی وجود دارد، بفرستد. این مهم، باعث ایجاد بسته‌ی داده با پروتکل UDP می‌شود که آدرس مقصد ارسالی آن، 255.255.255.255 و یا آدرس مشخّص ارسال زیر شبکه است، کاربر DHCP نیز می‌تواند آخرین آی پی آدرس شناخته شده‌ی خود را درخواست بدهد، اگر کاربر همچنان به شبکه متّصل باشد در این صورت IP آدرس معتبر است و سرور ممکن است که درخواست را بپذیرد، در غیر این صورت، این امر بستگی به این دارد که سرور به عنوان یک مرجع معتبر باشد، یک سرور به عنوان یک مرجع معتبر درخواست بالا را نمی‌پذیرد و کاربر را مجبور می‌کند تا برای درخواست آی پی جدید عمل کند.

پیشنهاد (Offer DHCP):

زمانی که یک سرور DHCP، یک درخواست را از کاربر دریافت می‌کند، یک IP Address را برای او رزو می‌کند و آن را با نام DHCP Offer می‌فرستد؛ این پیام، شامل MAC آدرس (آدرس فیزیکی دستگاه) کاربر، IP Address پیشنهادی توسط سرور، IP Subnet Mask و زمان تخصیص IP (lease Duration) و IP Address سروری می‌باشد که پیشنهاد را داده است.

درخواست (Request (DHCP:

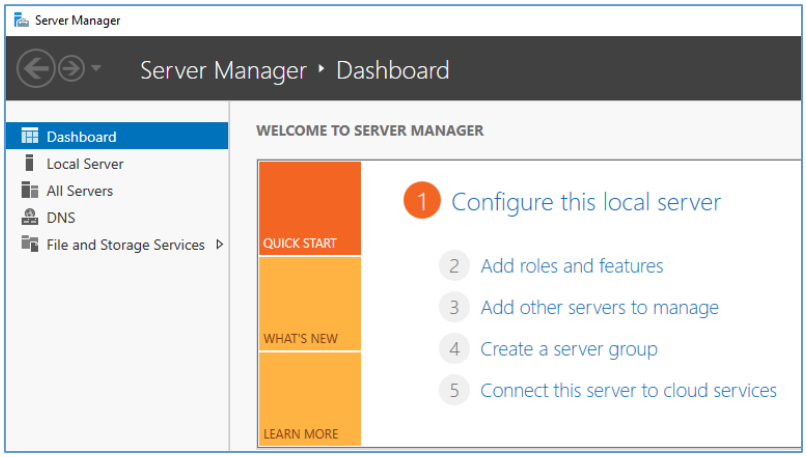
کاربر با یک درخواست به مرحله‌ی قبل پاسخ می‌دهد، یک کاربر می‌تواند پیشنهادهای مختلفی از سرورهای متفاوت دریافت کند، امّا تنها می‌تواند یکی از آنها را بپذیرد، بر اساس تنظیمات شناسایی سرور در درخواست و فرستادن پیام‌ها (identification option)، سرورها مطّلع می‌شوند که پیشنهاد کدام یک پذیرفته شده است، هنگامی که سرورهای DHCP دیگر این پیام را دریافت می‌کنند، آنها پیشنهادهای دیگری را که ممکن است به کاربر فرستاده باشند، باز پس می‌گیرند و آنها را در مجموعه‌ی آی پی‌های در دسترس قرار می‌دهند.

تصدیق (Acknowledgement (DHCP:

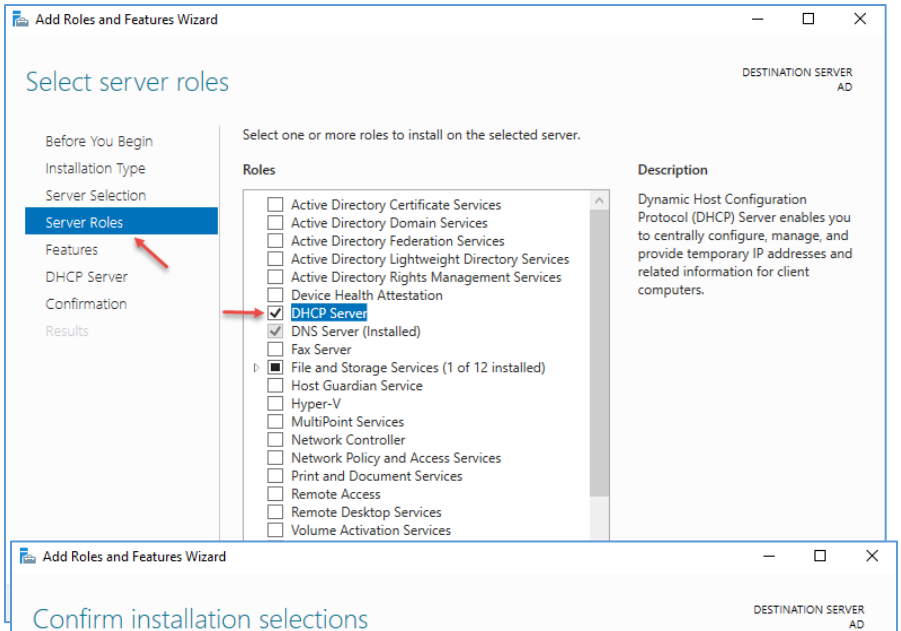
هنگامی که سرورDHCP، پیام درخواست DHCP را دریافت می‌کند، مراحل پیکربندی به فاز پایانی می‌رسد. مرحله‌ی تصدیق، شامل فرستادن یک بسته‌ی داده‌ای (DHCP Pack) به کاربر است؛ این داده‌ی بسته‌ای، شامل زمان تخصیص IP و یا هرگونه اطّلاعات پیکربندی که ممکن است که کاربر درخواست کرده باشد، است. در این مرحله، فرآیند پیکربندی IP کامل شده است و کلاینت مورد نظر دارای آدرس IP شده است.

قبل از راه‌اندازی سرویس باید این کارها را انجام دهید:

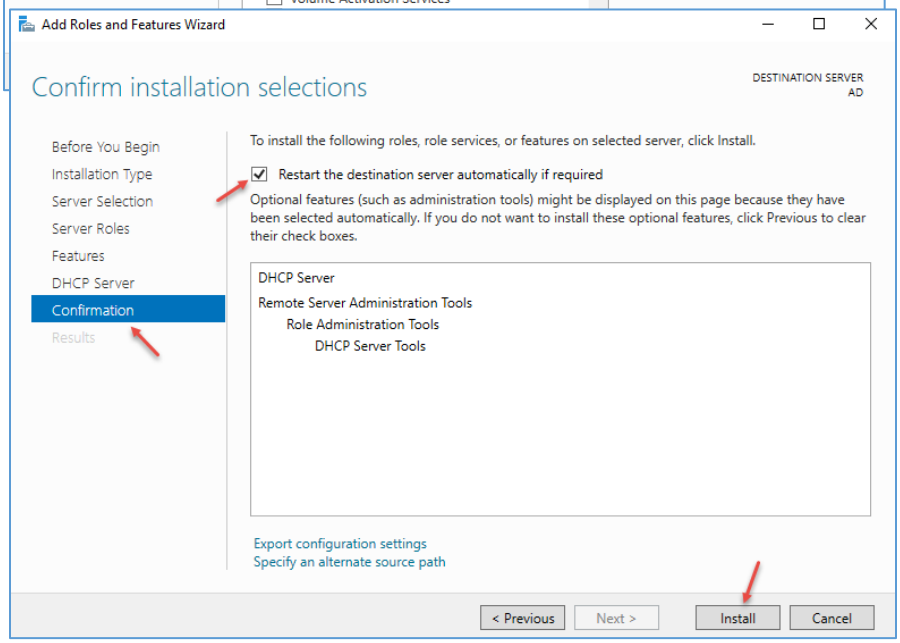
۱. رنج IP شبکه‌ی خود را باید مشخّص کنید تا بعد از راه‌اندازی سرویس آن را وارد کنید.
۲. تعداد دستگاه‌های شبکه‌ی خود را باید مشخّص کنید تا ببینید آیا یک رنج IP، جوابگوی شما خواهد بود یا نه.
۳. تعداد سرورهای خود را مشخّص کنید تا در صورت تمایل در لیست رزرو قرار داده شوند.



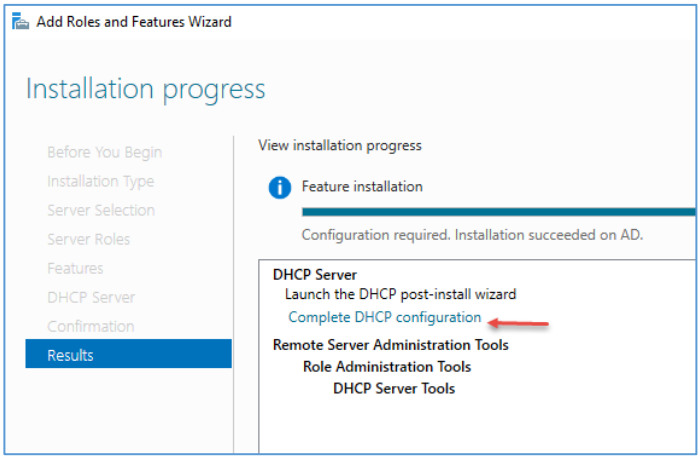
وارد Server Manager شوید و بر روی Add roles and feature کلیک کنید تا اقدام به نصب سرویس DHCP کنید.



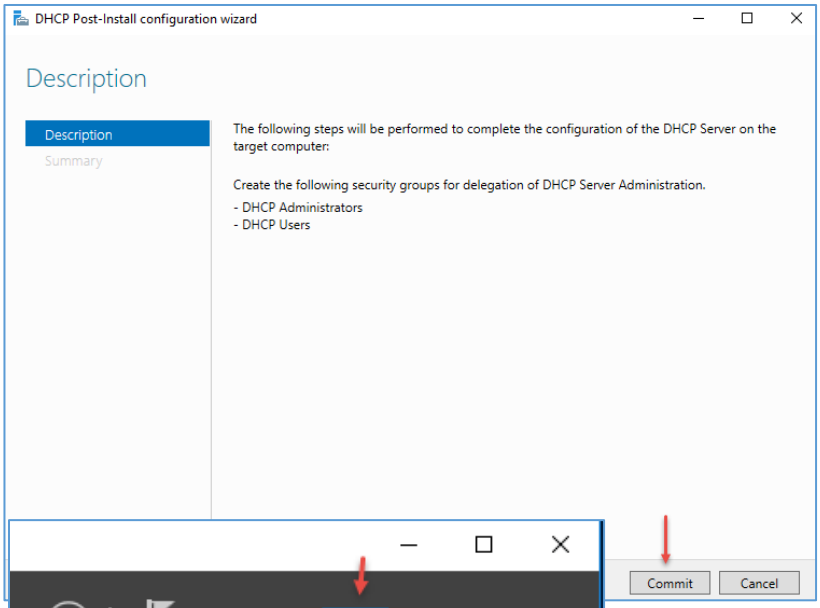
در قسمت Server Roles، تیک سرویس DHCP را انتخاب و در پنجره‌ی باز شده بر روی Add Features کلیک و بعد، بر روی Next کلیک کنید.



در این صفحه بر روی Install کلیک کنید تا کار نصب آغاز شود.

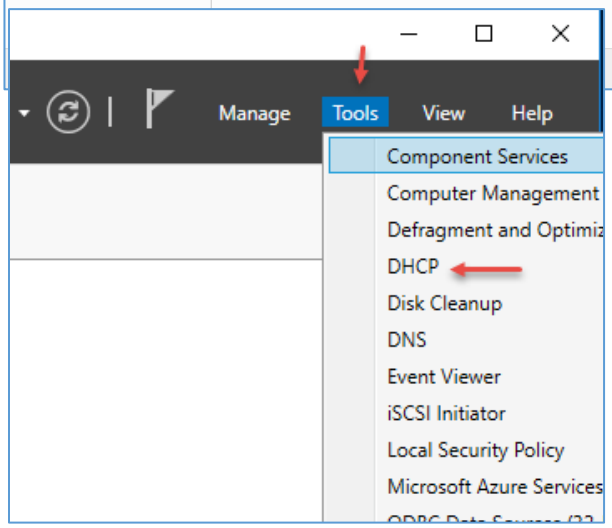


بعد از نصب سرویس، شکل روبرو ظاهر می‌شود که باید بر روی Complete DHCP configuration کلیک کنید.

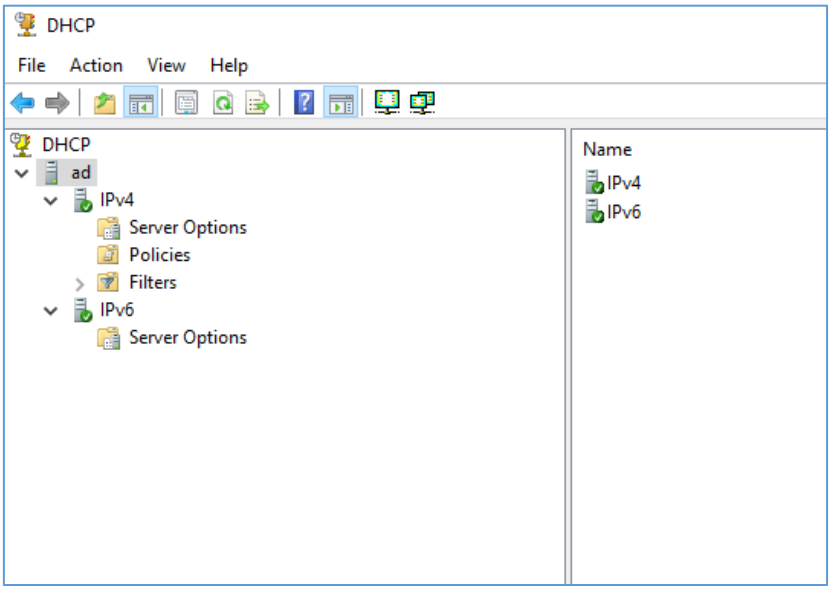


در این صفحه برای کامل شدن مراحل نصب DHCP بر روی Commit کلیک کنید، بعد از این کار، دو گروه DHCP Administrators و DHCP Users ایجاد می‌شود و کار نصب سرویس DHCP به اتمام می‌رسد.

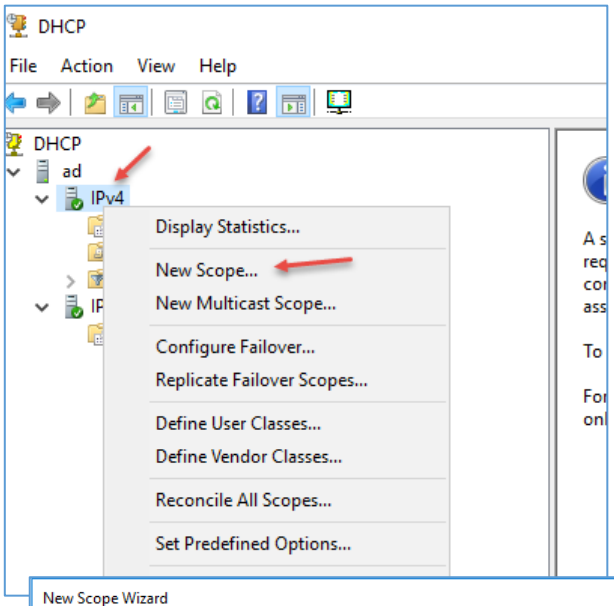
سرور را Restart کنید.



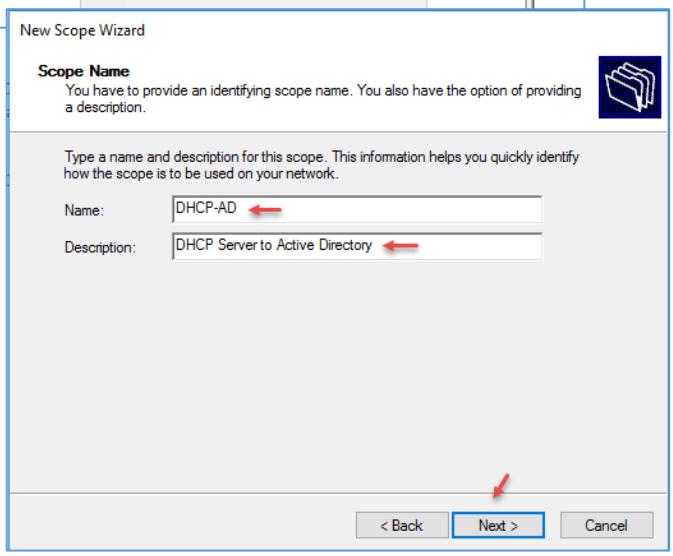
بعد از اجرا شدن سرور وارد Server Manager شوید و از منوی Tools، سرویس DHCP را اجرا کنید، از طریق منوی Start نیز می‌توانید با جستجوی DHCP، آن را اجرا کنید.



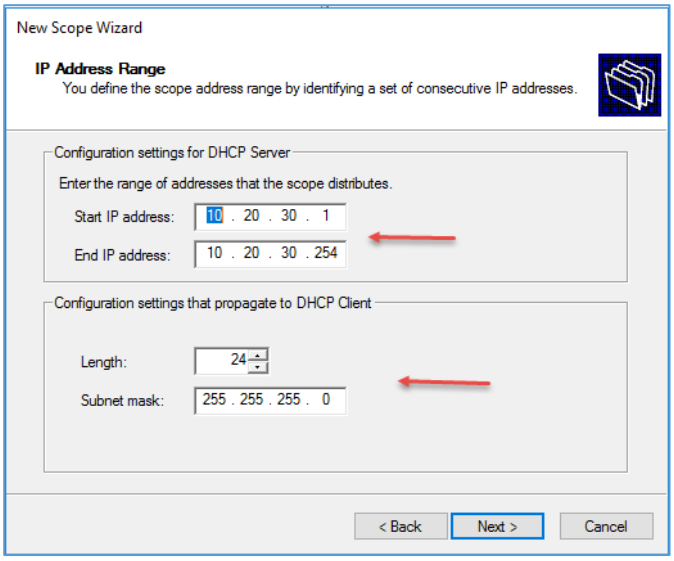
همانطور که در شکل روبرو مشاهده می‌کنید، سرویس DHCP اجرا شده است و فعّال است، امّا در حال حاضر در شبکه‌ی شما نمی‌تواند کاری انجام دهد، در سرویس DHCP، دو ورژن IP مشخّص شده است که کار اصلی در این سرویس با IPV4 است که شامل گزینه‌های مختلف است.



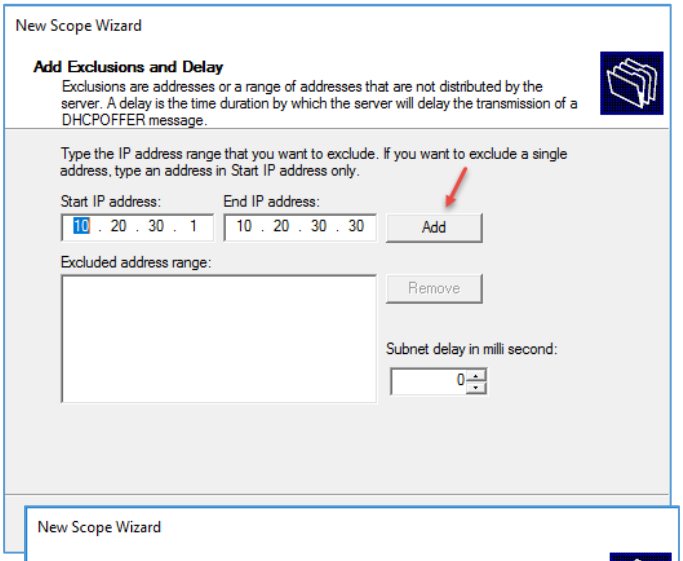
برای شروع کار باید یک Scope (به یک رنج مشخّصی از IP گویند که دارای تنظیمات خاصّی است، مانند آدرس روتر، آدرس دومین و...) ایجاد کنید، برای این کار بر روی ورژن IPV4 کلیک راست کنید و گزینه‌ی Scope را انتخاب کنید.



در این پنجره، نام و توضیحات مربوط به Scope خود را وارد و بر روی Next کلیک کنید.

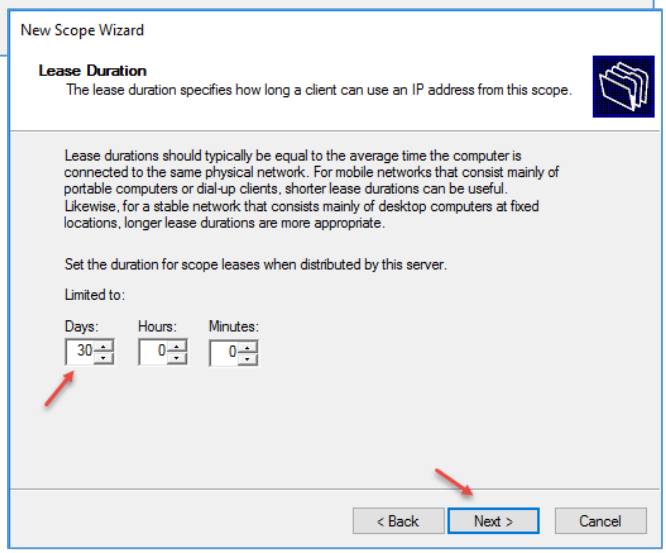


در این صفحه باید رنج آدرس شبکه‌ی خود را به همراه Subnet آن وارد کنید، به این نکته توجّه کنید که اگر تعداد دستگاه‌های شما بیشتر از یک رنج ۲۵٤ است، بهتر است به جای ۲٤ در قسمت Length، عدد پایین‌تر را در نظر بگیرید تا رنج شبکه‌ی شما افزایش پیدا کند؛ به مانند شکل، اطّلاعات را وارد و بر روی Next کلیک کنید.



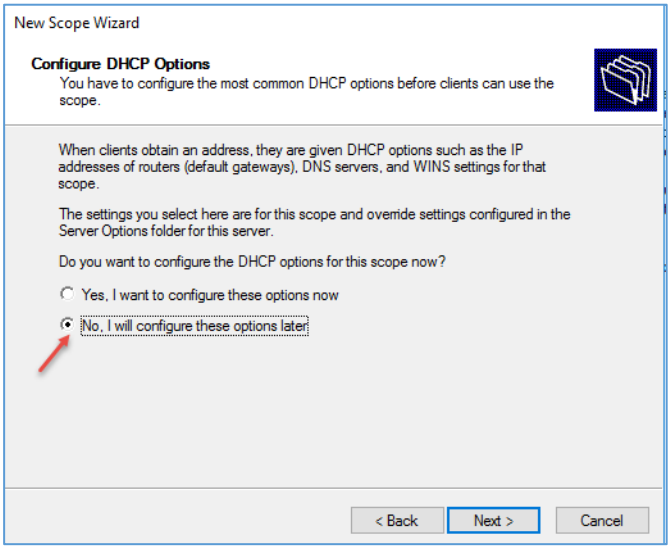
در این قسمت می‌توانید یک رنج مشخّص از داخل رنج قبلی برای تخصیص دادن به سرورها و سیستم‌های خاص و مهمّ خود انتخاب کنید، به مانند شکل روبرو ۳۰ آدرس اوّل رنج مورد نظر را از رنج اصلی جدا کنید، با این کار اگر یک کلاینت معمولی، درخواست IP دهد، آدرسی که به آن تعلّق خواهد گرفت از 10.20.30.31 به بعد خواهد بود. این نکته را با مثال، ذکر خواهیم کرد.

بر روی Next کلیک کنید.



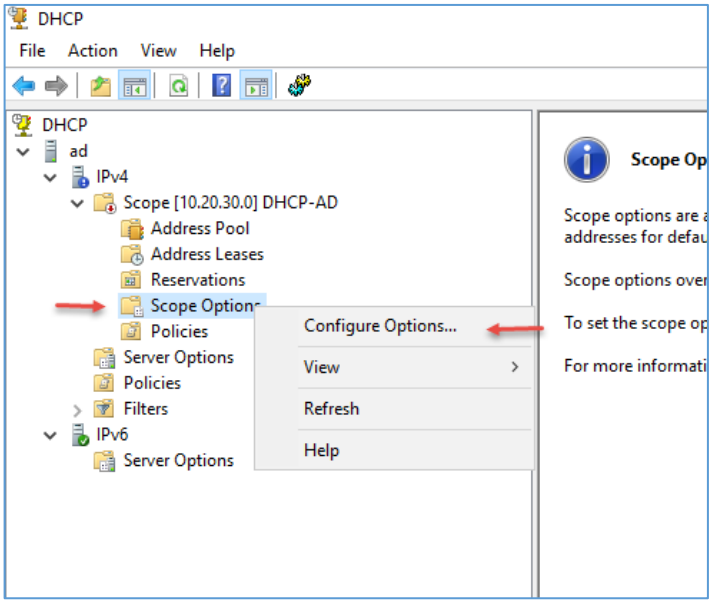
در این قسمت باید زمانی را مشخّص کنید که وقتی یک دستگاه از سرویس DHCP، آدرس IP دریافت کرد تا چند روز این آدرس برای آن دستگاه رزرو باشد که در شکل روبرو ۳۰ روز را در نظر گرفتیم که شما می‌توانید این آدرس را تغییر دهید، اگر در این ۳۰ روز، دستگاه مورد نظر، خود را به سرویس معرّفی نکند، این آدرس تخصیص داده شده از آن پس گرفته خواهد شد.

بر روی Next کلیک کنید.

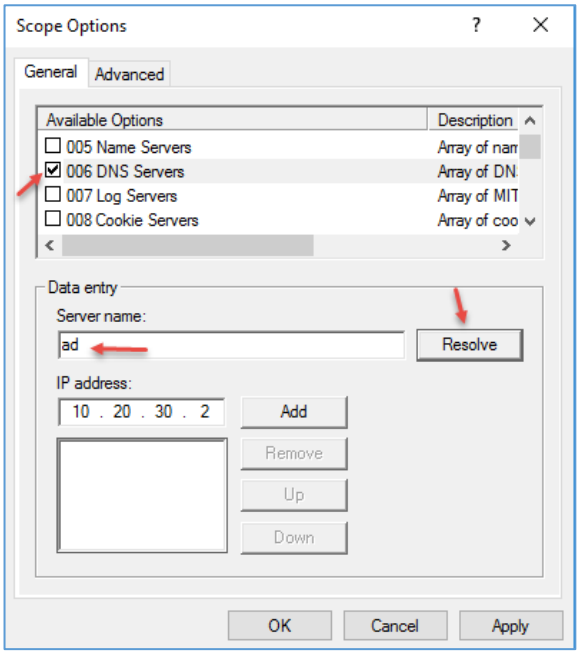


در این صفحه شما می‌توانید با انتخاب گزینه‌ی اوّل، تنظیماتی، مانند آدرس روتر، نام دومین و آدرس Wins Server را انجام دهید که فعلاً این کار را انجام نمی‌دهیم و در ادامه انجام خواهیم داد؛ گزینه‌ی No را انتخاب و بر روی Next کلیک کنید.

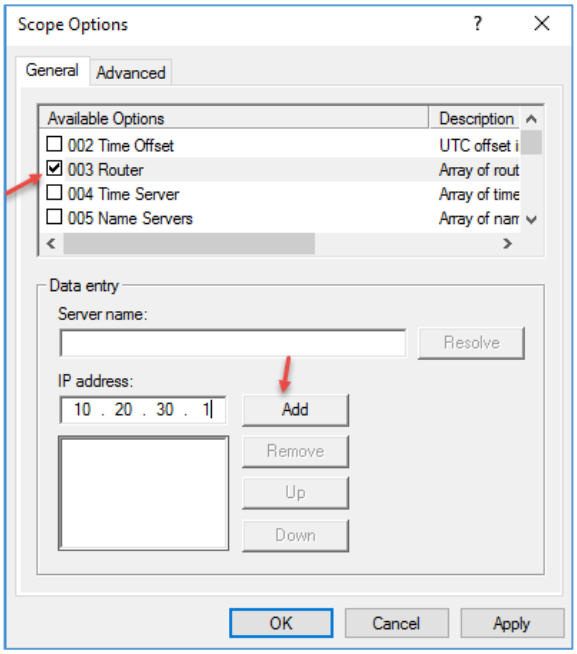
در صفحه‌ی بعد نیز بر روی Finish کلیک کنید.



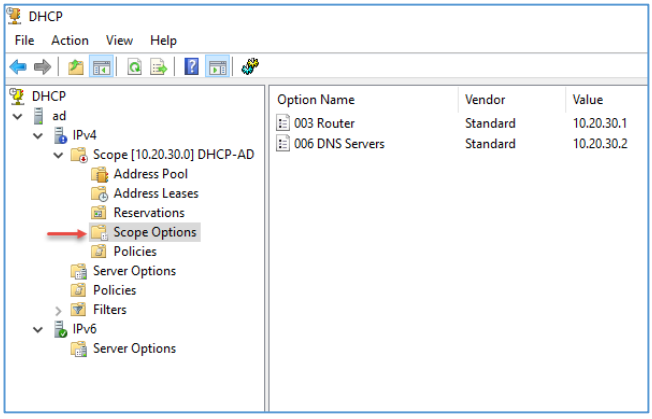
بعد از ایجاد Scope باید یک‌سری تنظیمات دیگر برای آن انجام دهید، مانند آدرس DNS Server، آدرس روتر، Time Server و... که برای اضافه کردن این آدرس‌ها باید به مانند شکل روبرو وارد Scope مورد نظر شوید و بر روی Scope Options کلیک راست و گزینه‌ی Configurations Options را انتخاب کنید.



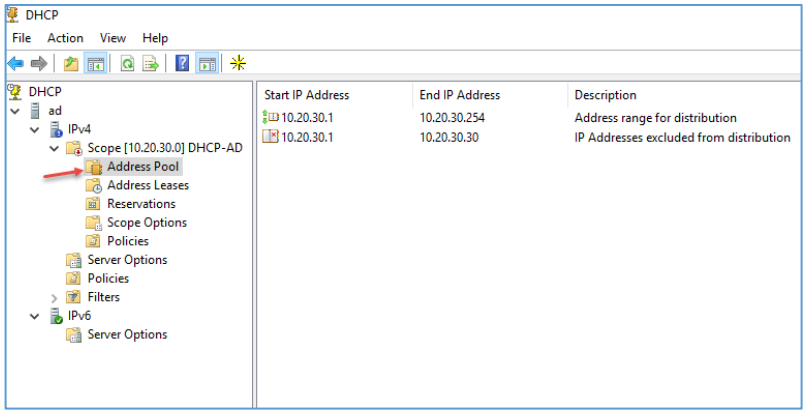
در این شکل باید از لیست، گزینه‌ی مورد نظر خود را انتخاب کنید، مثلاً برای اضافه کردن DNS سرور به Scope باید از لیست مورد نظر، تیک گزینه‌ی DNS Server را انتخاب کنید و در قسمت Server Name می‌توانید نام سروری که DNS بر روی آن اجرا شده است را وارد کنید که این کار را در سرور AD انجام دادیم، با وارد کردن نام سرور و کلیک بر روی Resolve، آدرس IP مشخّص می‌شود و با کلیک بر روی Add، آدرس سرور را به لیست اضافه کنید.



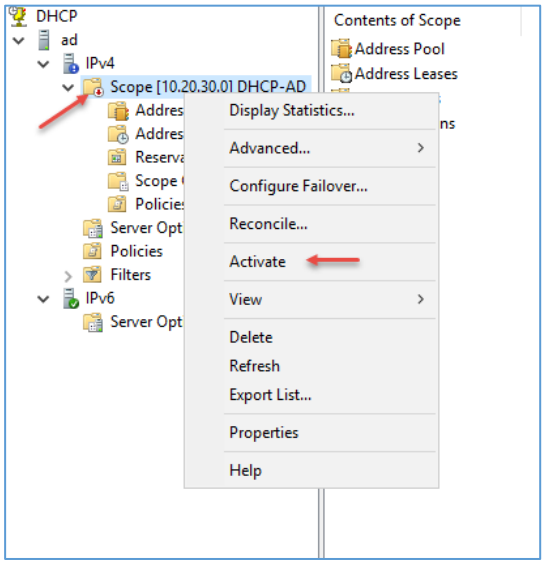
گزینه‌ی دیگر، Router است که اگر در شبکه‌ی خود از روتر استفاده می‌کنید، می‌توانید آدرس آن را به مانند شکل روبرو به لیست اضافه کنید، آدرس روتر در این کتاب، 10.20.30.1 در نظر گرفته شده است که باید در این قسمت وارد کنید، گزینه‌های دیگری نیز وجود دارد که آنهارا در خلال کتاب بررسی خواهیم کرد.



همانطور که مشاهده می‌کنید، آدرس Router و DNS به لیست اضافه شده است که در صورت نیاز می‌توانید موارد دیگر را از همین طریق به لیست اضافه کنید، توجّه داشته باشید این تنظیمات به کلاینت مورد نظر داده خواهد شد.

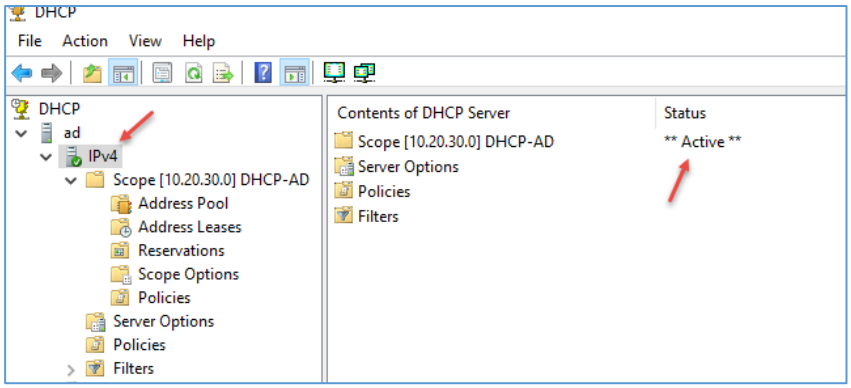


در قسمت Address Pool، رنج آدرس آن مشخّص شده است که از 10.20.30.1 تا 10.20.30.254 است و یک رنج Excluded مشخّص شده است.



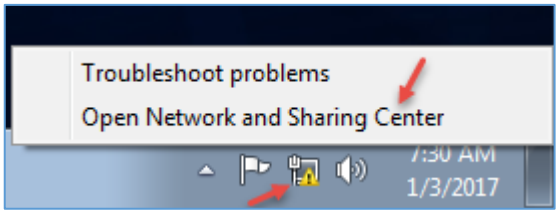
بعد از ایجاد Scope، هنوز سرویس DHCP فعّال نشده است و نمی‌تواند به کلاینت‌ها سرویس دهد، برای فعّال کردن Scope مورد نظر، به مانند شکل روبرو بر روی آن کلیک راست کنید و گزینه‌ی Activate را انتخاب کنید تا سرویس DNS به صورت کامل اجرا شود.

بعد از فعّال کردن سرویس، یک کلاینت را برای تست، اجرا و به شبکه‌ی خود متّصل کنید.

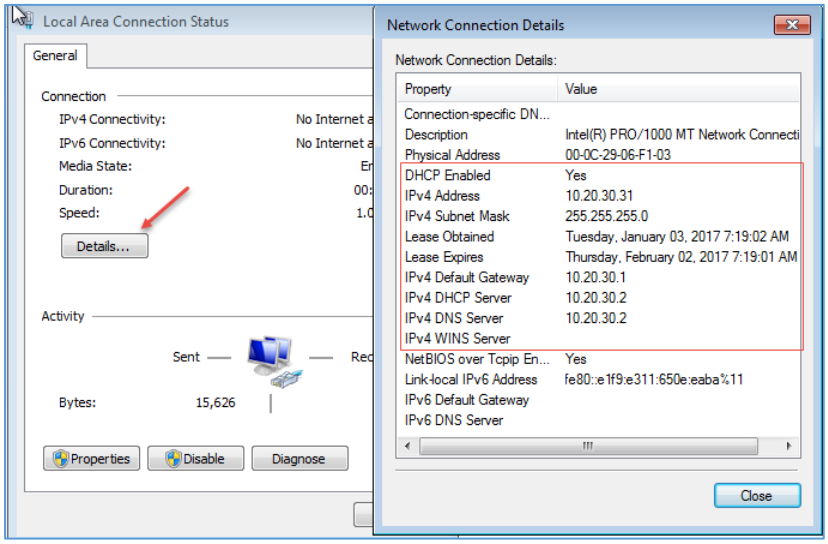


همانطور که مشاهده می‌کنید، Scope مورد نظر فعّال شده است.

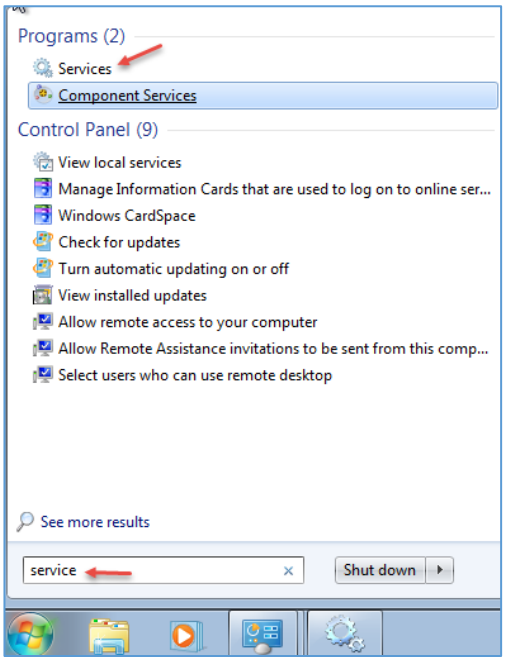
برای تست کارایی سرویس DHCP، یک کلاینت با ویندوز ۷ را به سرور متّصل کنید تا ببینید چه آدرسی را از سرویس DHCP دریافت می‌کند.



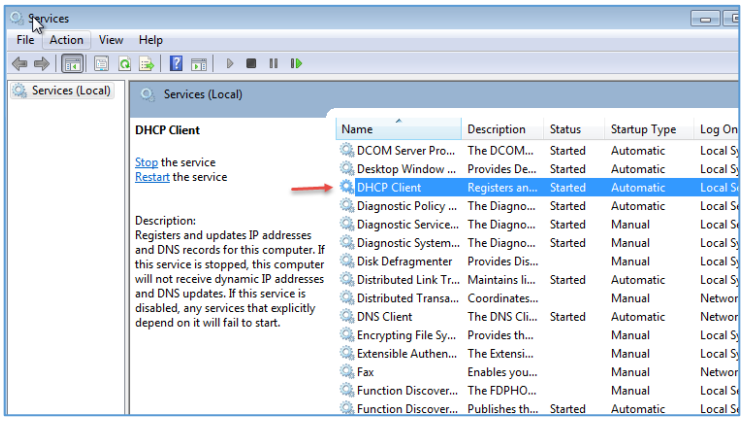
بعد از اینکه کلاینت را به شبکه‌ی ویندوز سرور متّصل کردید، وارد ویندوز ۷ شوید و بر روی کارت شبکه کلیک راست کنید و گزینه‌ی Open Network and Sharing Center را انتخاب کنید.



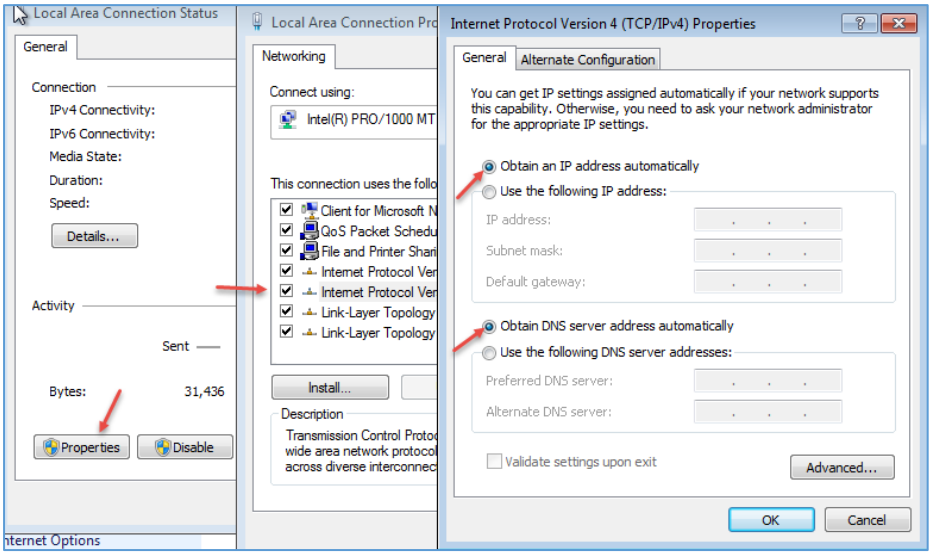
در شکل روبرو بر روی Details کلیک کنید تا اطّلاعات کارت شبکه نمایش داده شود، همانطور که مشاهده می‌کنید، DHCP Enable بر روی Yes قرار دارد، یعنی اگر در شبکه سرویس DHCP باشد، درخواست IP را به آن می‌فرستد و یک آدرس جدید دریافت می‌کند، اگر به آدرس IP توجّه کنید، 10.20.30.31 است، یعنی همان رنجی که در سرویس DHCP ایجاد کردیم، بقیّه‌ی گزینه‌ها را نیز مشاهده می‌کنید؛ آدرس Default Gateway برابر 10.20.30.1 شده است و آدرس DNS و DHCP نیز مشخّص شده است.



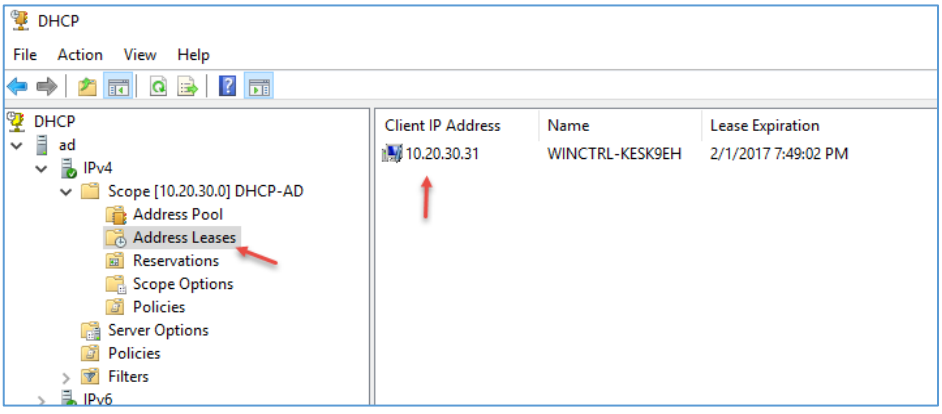
برای اینکه یک کلاینت بتواند از سرویس DHCP، آدرس جدید به صورت اتوماتیک دریافت کند باید سرویس آن فعّال باشد، برای بررسی این موضوع در کلاینت وارد start شوید و Service را اجرا کنید.



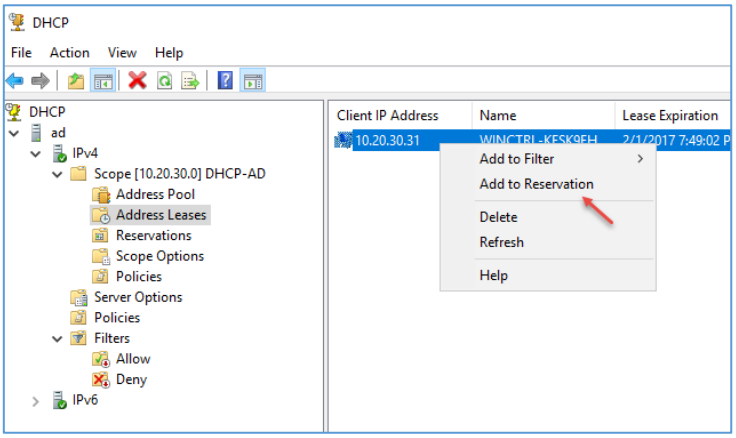
همانطور که در شکل روبرو مشاهده می‌کنید، سرویسی به نام DHCP Client در لیست قرار دارد که در حال کار است و زمانی که شما کلاینت را به شبکه متّصل می‌کنید، این سرویس درخواست خود را به DHCP Server می‌فرستد.



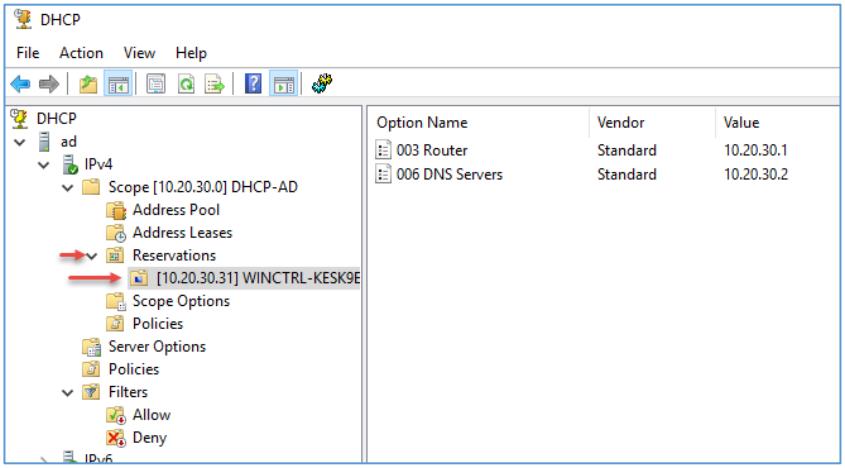
توجّه داشته باشید، کارت شبکه‌ی کلاینت و یا هر دستگاه دیگری برای دریافت اتوماتیک IP باید بر روی Obtain an IP address automatically باشد که این موضوع را در شکل روبرو مشاهده می‌کنید.



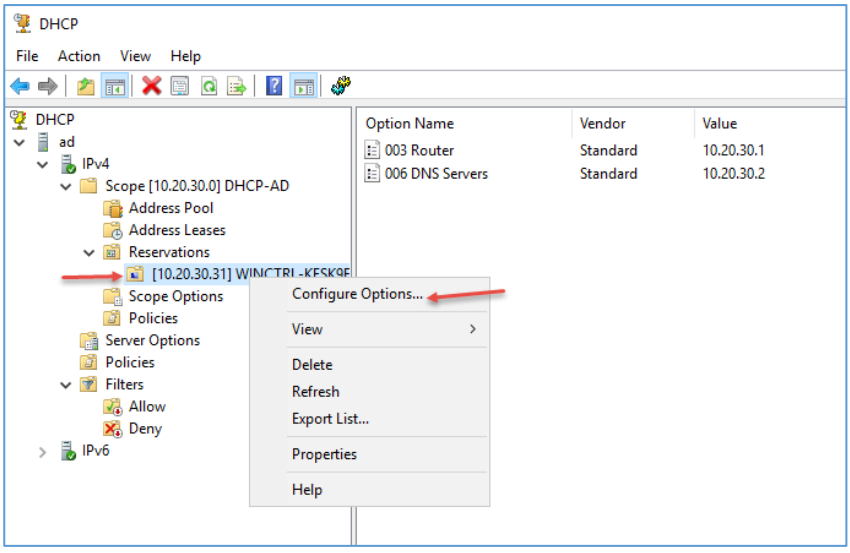
اگر وارد سرویس DHCP در ویندوز سرور شوید و از قسمت Scope وارد Address Leases شوید، می‌توانید سیستمی که IP به آن اختصاص داده شده است را ببینید.



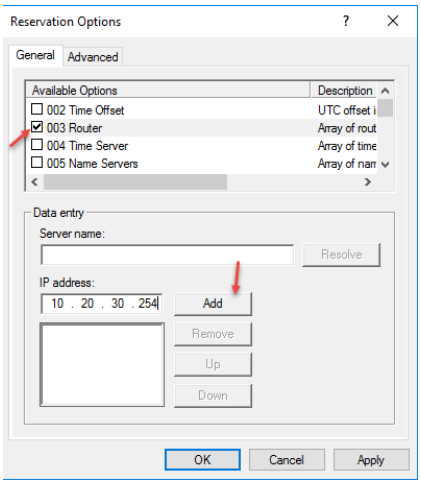
اگر بخواهید یک آدرس را برای همیشه به یک دستگاه تخصیص دهید باید در Address Leases بر روی آدرس مربوط به دستگاه مورد نظر کلیک راست کنید و گزینه‌ی Add to reservation را انتخاب کنید، با این کار این آدرس وارد لیست Reservation خواهد شد و دیگر آدرس آن تغییر نخواهد کرد.



همانطور که در شکل روبرو مشاهده می‌کنید در قسمت Reservations، آدرس دستگاه مورد نظر به لیست اضافه شده است، در این لیست شما می‌توانید تنظیمات جدیدتری را انجام دهید، یعنی اینکه می‌توانید در صورت نیاز، آدرس Router یا DNS و یا هر تنظیم خاصّ دیگری را فقط و فقط برای همین دستگاه انجام دهید.

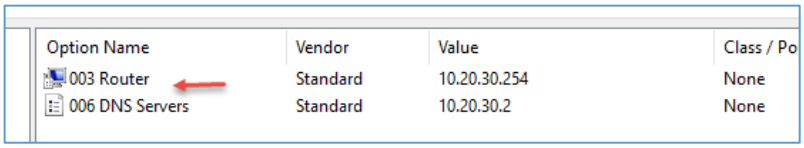


به طور مثال، اگر بخواهید آدرس Router را برای این دستگاه تغییر دهید باید به مانند شکل بر روی آن کلیک راست و گزینه‌ی Configure Options را انتخاب کنید.

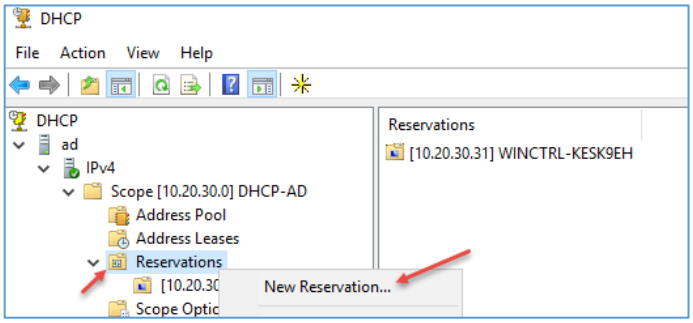


در لیست روبرو باید گزینه‌ی Router را انتخاب و آدرس آن را در قسمت مورد نظر وارد و بر روی Add کلیک کنید؛ گزینه‌های دیگری را نیز می‌توانید برای این دستگاه تغییر دهید.

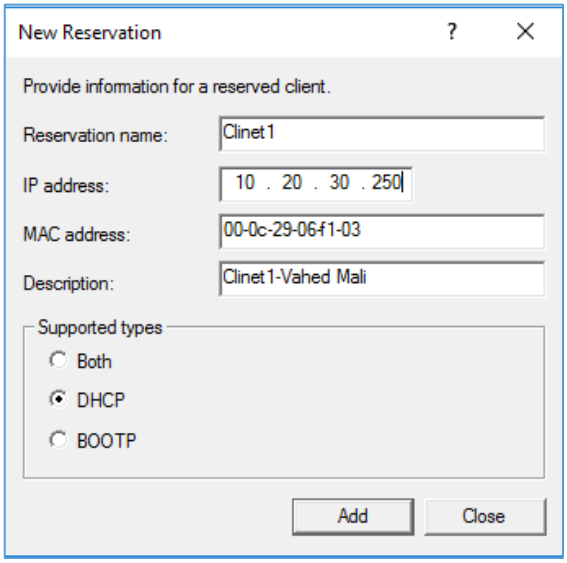
در شکل روبرو این تغییر را مشاهده می‌کنید.



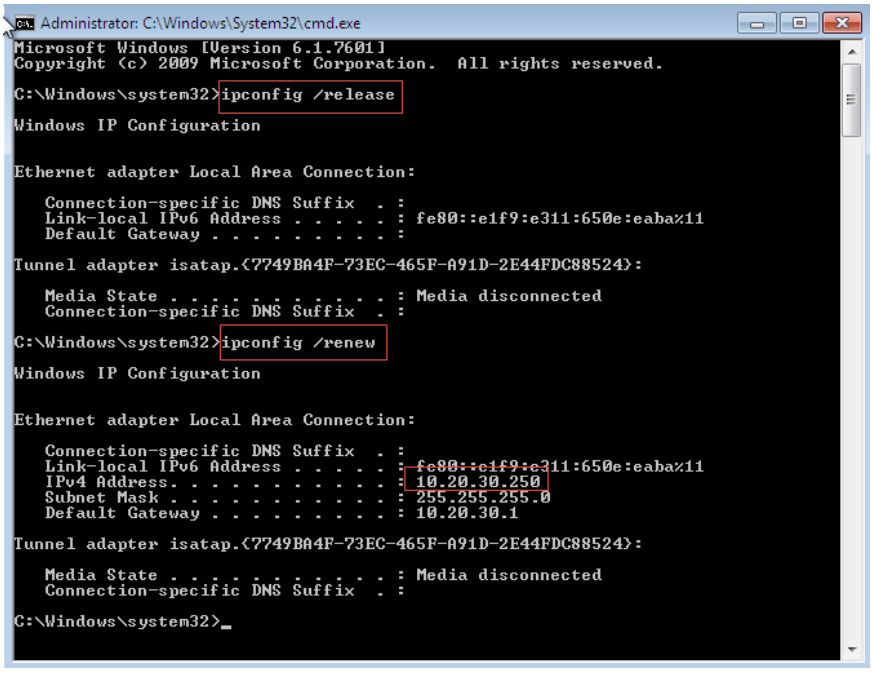
راه دیگری نیز برای رزرو کردن آدرس برای دستگاه خاص وجود دارد و شرط آن نیز این است که آدرس Mac دستگاه مورد نظر را در اختیار داشته باشید.



برای انجام این کار بر روی Reservation کلیک راست و گزینه‌ی New Reservation را انتخاب کنید.

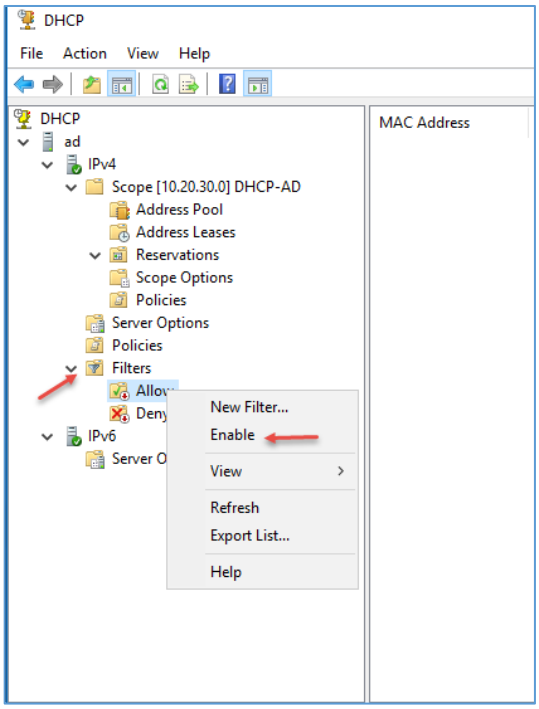


در این صفحه باید اطّلاعات مورد نظر را وارد کنید؛ آدرس مورد نظر خود را در قسمت Ip address وارد کنید و در قسمت MAC address نیز آدرس Mac را وارد کنید که برای به دست آوردن آدرس Mac می‌توانید از دستور ipconfig /all در کلاینت مورد نظر استفاده کنید که این دستور را قبلاً بررسی کردیم. در قسمت Supported types، دو گزینه‌ی DHCP و BOOTP وجود دارد که BOOTP، یک سرویس قدیمی است که در سیستم‌های جدید کارایی ندارد، شما می‌توانید گزینه‌ی DHCP را انتخاب و بر روی ADD کلیک کنید.



بعد از اینکه عملیّات Reservation را انجام دادید وارد کلاینت قبلی شوید و برای اینکه کلاینت آدرس جدید را از سرور DHCP دریافت کند، CMD را اجرا کنید و بعد از آن، دستور Ipconfig /Release را اجرا کنید؛ با این دستور، کلاینت آدرس قبلی خود را که 10.20.30.31 بود را از دست خواهد داد، برای دریافت آدرس جدید باید از دستور ipconfig /renew استفاده کنید که همانطور که در شکل روبرو مشاهده می‌کنید، آدرس جدید که به صورت رزرو شده وارد کردید به کلاینت تخصیص داده شد.

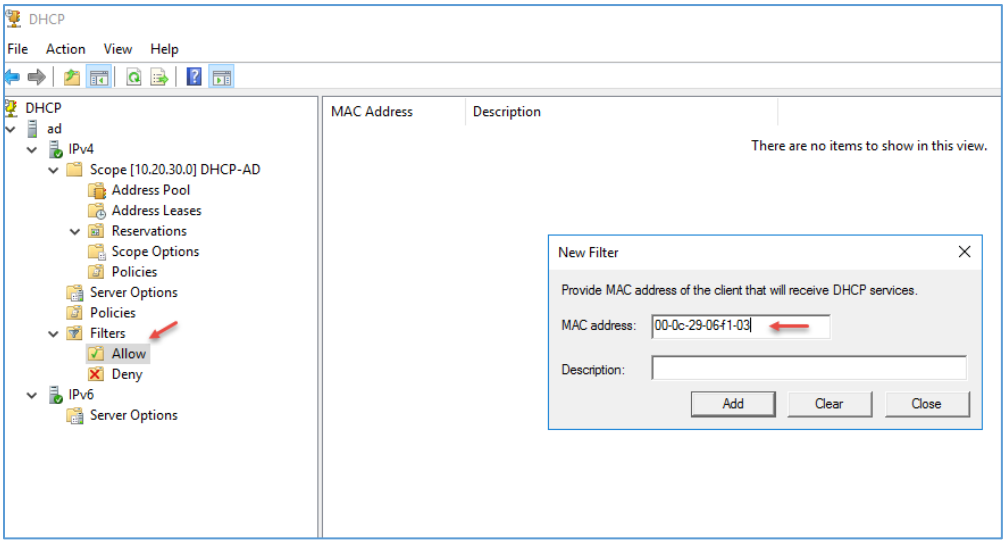
فعّال کردن Mac Filtering در سرویس DHCP:



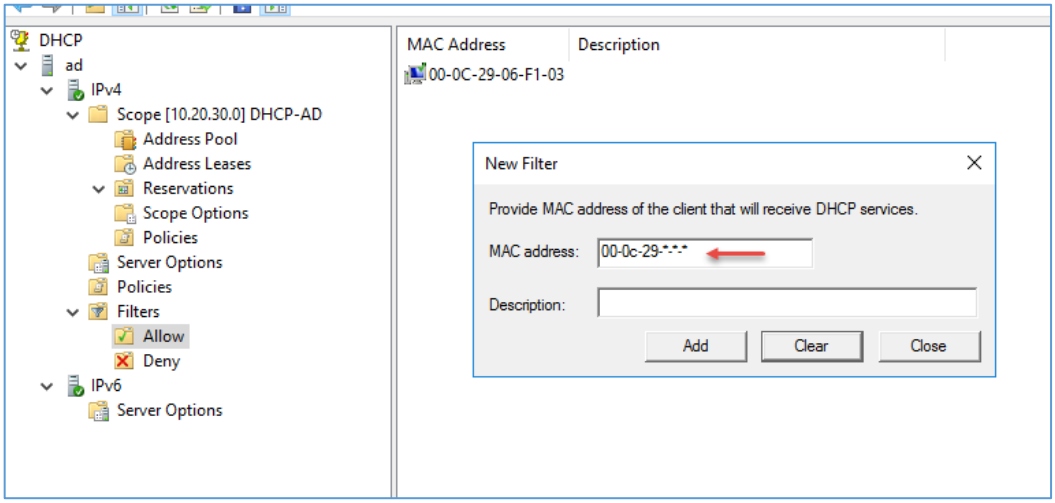
برای افزایش امنیّت شبکه‌ی خود می‌توانید از ویژگی MAC Filtering در شبکه‌ی خود استفاده کنید، با استفاده از این روش، شما می‌توانید لیستی از MAC آدرس‌های کلاینت‌ها و دستگاه‌های شبکه‌ی خود را جمع‌آوری و به سرویس DHCP اعلام کنید که تنها این سیستم‌ها اجازه دارند از شبکه، آدرس IP دریافت کنند و بقیّه‌ی سیستم‌ها این اجازه را نخواهد داشت، یعنی اگر یکی از همکاران لپ‌تاپ شخصی خود را به شبکه متّصل کند، سرویس DHCP به آن، آدرس IP تخصیص نخواهد داد.

به مانند شکل روبرو وارد قسمت Filter شوید؛ در این قسمت، دو گزینه‌ی Allow و Deny را مشاهده می‌کنید که به صورت پیش‌فرض غیر فعّال هستند و برای فعّال کردن این ویژگی باید بر روی هر دوی آنها کلیک راست کنید و گزینه‌ی Enable را انتخاب کنید.

نکته‌ی مهم: توجّه داشته باشید که بعد از فعّال کردن این ویژگی باید حتماً لیست مورد نظر خود را قبل از آن وارد کرده باشید تا مشکلی برای کلاینت‌ها پیش نیاید.



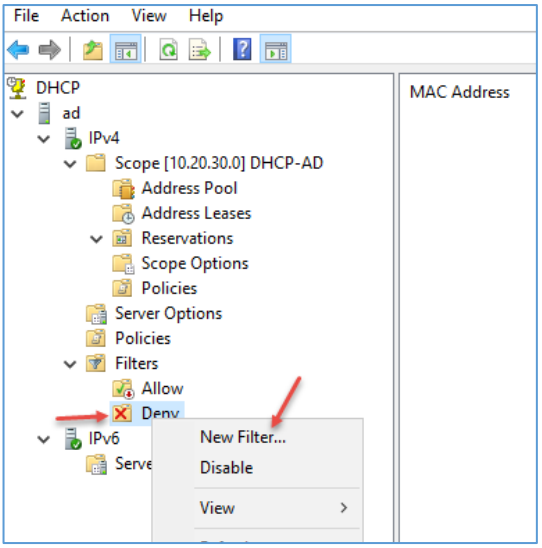
با کلیک راست بر روی Allow و انتخاب گزینه‌ی New Filter، پنجره‌ی مربوط به آن باز خواهد شد که شما باید آدرس MAC کلاینت مورد نظر خود را وارد و آن را در لیست Add کنید، با این کار تنها این سیستم توانایی دریافت آدرس را خواهد داشت. روش‌های دیگری نیز برای دادن آدرس وجود دارد، شاید شما کارت شبکه‌ی مربوط به کلاینت‌ها را از یک شرکت خاص خریداری کرده باشید و اگر اینطور باشد، شما می‌توانید آدرس MAC را به صورت کلّی در این قسمت وارد کنید.



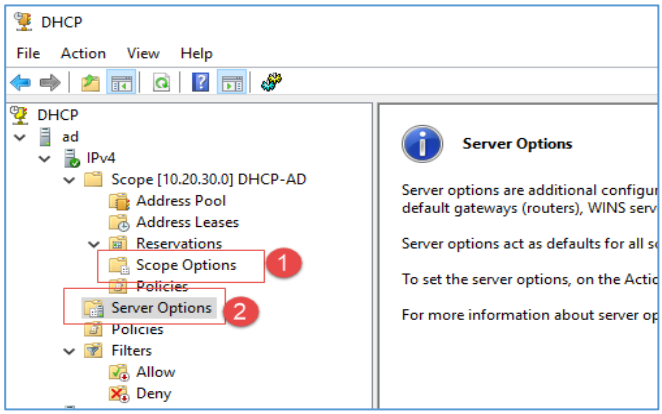
دلیل آن، این است که چند شماره‌ی اوّل کارت شبکه‌ی هر شرکتی، مختص به خود آن شرکت است که برای وارد کردن آن باید به صورت روبرو چند آدرس اوّل را وارد و بقیّه را با علامت ستاره * پر کنید:

00-0c-29-*-*-*

با این کار، تمام کارت شبکه‌هایی که اوّل آدرس آنها، 00-0c-29 است، دسترسی دارند تا از DHCP آدرس دریافت کنند.

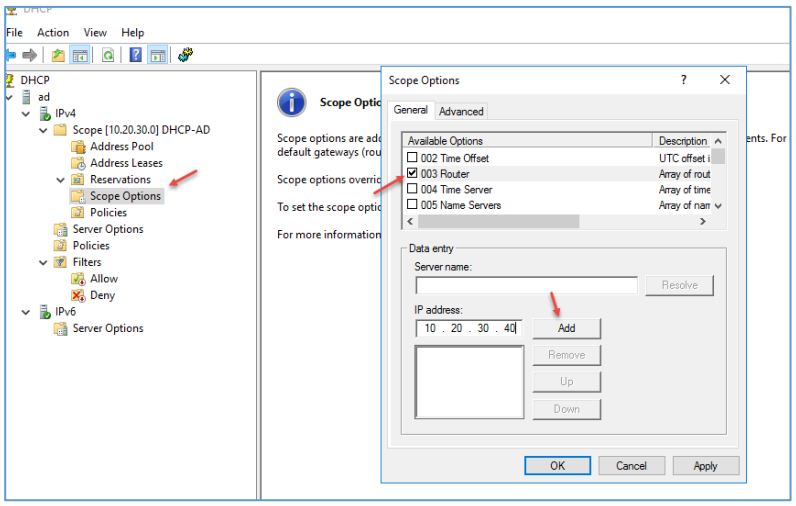


سعی کنید در یک زمان از یکی از ویژگی‌های Filters استفاده کنید، برای اینکه یک سیستم را در لیست Deny قرار دهید، به مانند شکل روبرو بر روی آن کلیک راست کنید و گزینه‌ی New Filter را انتخاب کنید و در پنجره‌ی باز شده، آدرس MAC را وارد و Add کنید، با این کار تمام سیستم‌ها به DHCP دسترسی خواهند داشت، به جز آن سیستمی که آدرس MAC آن در لیست قرار دارد.

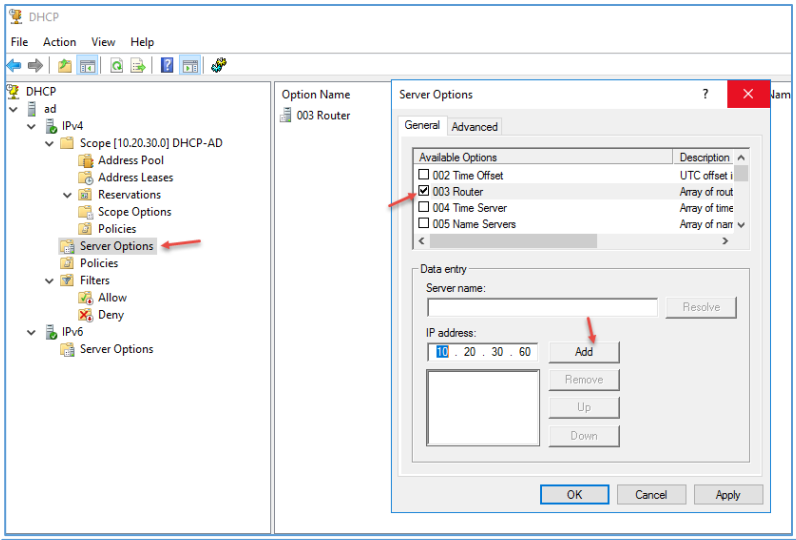


اگر به سرویس DHCP نگاهی کنید، متوجّه خواهید شد در این سرویس، دو Option وجود دارد که یکی به عنوان Server Options و دیگری به عنوان Scope Options است که می‌توانید با این گزینه‌ها، آدرس روتر، DNS و... را وارد کنید.

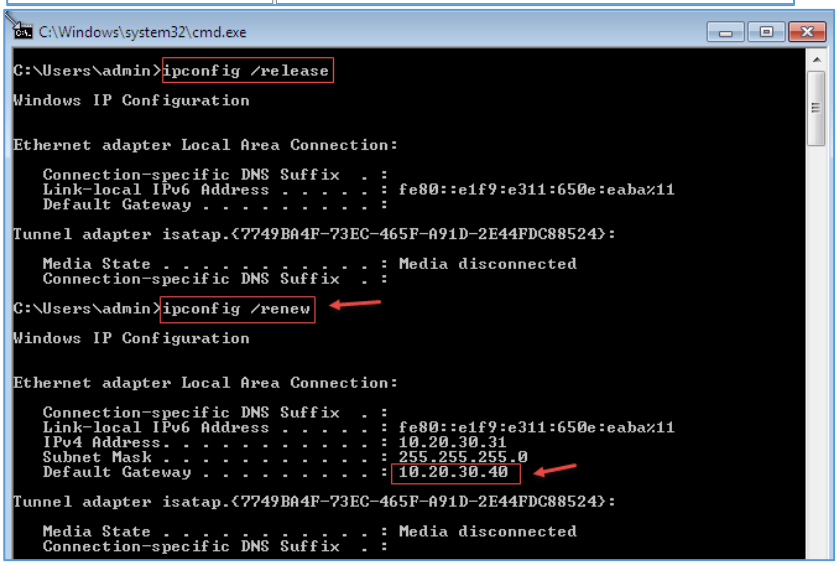
امّا اگر در هر کدام از این گزینه‌ها، مثلاً یک تنظیم مثل هم قرار دهید، کدام یک را به عنوان تنظیم اصلی قبول می‌کند؟



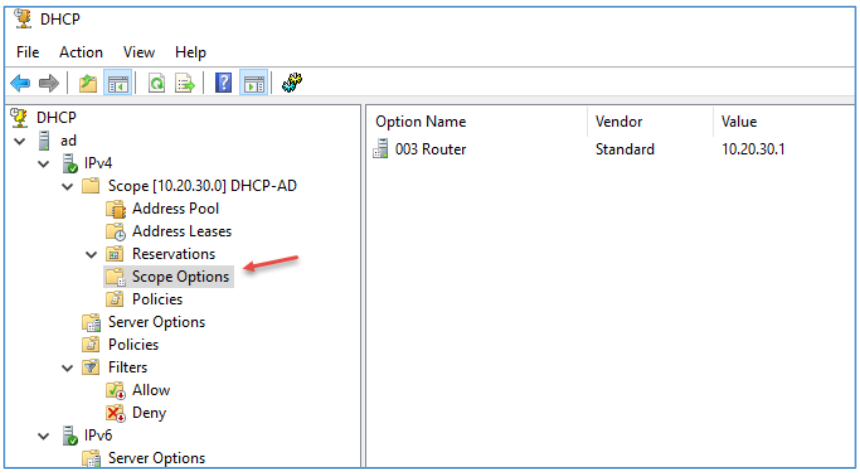
برای تست این موضوع به مانند شکل روبرو در Scope Option، یک router با آدرس 10.20.30.40 به لیست اضافه کنید.



در قسمت Server Options نیز یک Router با آدرس 10.20.30.60 به لیست اضافه کنید، بعد از این کار وارد کلاینت شوید و یک بار کارت شبکه را disable و بعد، enable کنید و یا از دستور ipconfig /release و بعد از دستور ipconfig /renew استفاده کنید تا تنظیمات جدید را از سرویس DHCP دریافت شود.



در این قسمت وارد کلاینت شدیم و همانطور که مشاهده می‌کنید، آدرس Default Gateway، برابر 10.20.30.40 شده است، این بدان معنا است که الویّت انتخاب Options، اوّل Scope Options است و اگر چنانچه این تنظیم در Scope وجود نداشته باشد از تنظیمات Server Options استفاده می‌کند.

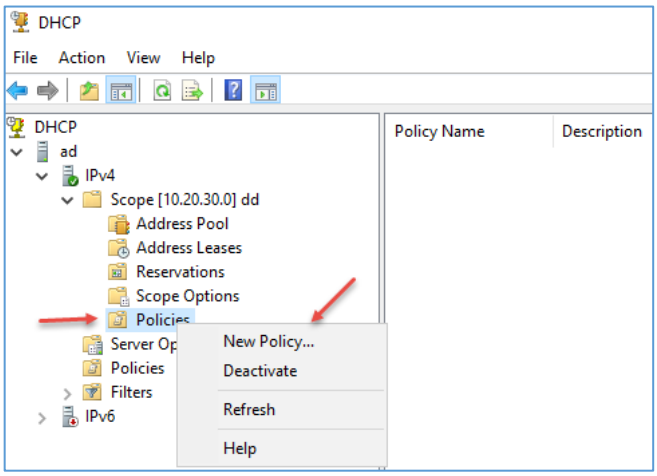


اگر تنظیمات Server Options را فعّال کنید و چیزی در Scope Options وارد نکنید، به مانند شکل از تنظیمات Server در scope استفاده می‌کند.

از طریق شکل آیکون نیز می‌توانید به این تنظیمات پی ببرید.

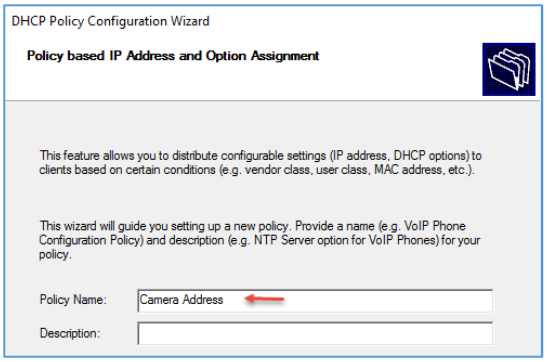
تخصیص دادن آدرس مشخّص به دستگاه‌های مشخّص:

برای اینکه در شبکه با نظم باشیم، می‌توانیم از طریق Policy در سرویس DHCP کارهایی را انجام دهیم، مثلاً اگر شما در شبکه‌ی خود از یک مدل دوربین مدار بسته استفاده کنید، حتماً آدرس مک آنها با حروف و اعداد مشخّص شروع می‌شود، با دانستن آن می‌توانید یک رنج آدرس خاص به آنها تخصیص دهید.

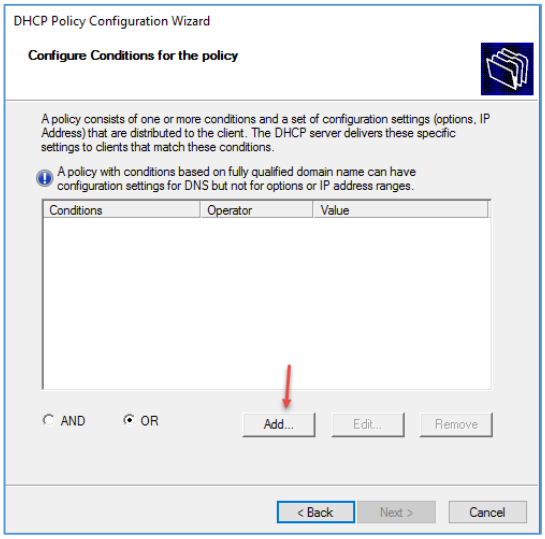


در سرویس DHCP در هر Scope، یک قسمت با نام Policies وجود دارد که اولویّت آن نسبت به Policies که در بیرون از Scope قرار دارد، بالاتر است، یعنی اگر دو Policy یک شکل تعریف شود، Policy ای که در داخل Scope قرار دارد، اجرا خواهد شد.

به مانند شکل در داخل Scope بر روی Policies کلیک راست کنید و گزینه‌ی New Policy را انتخاب کنید.

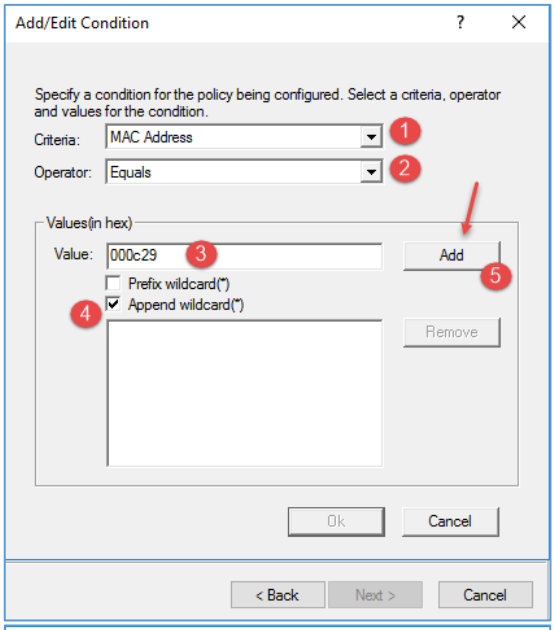


در صفحه‌ی روبرو یک نام به دلخواه خود وارد و بر روی Next کلیک کنید.

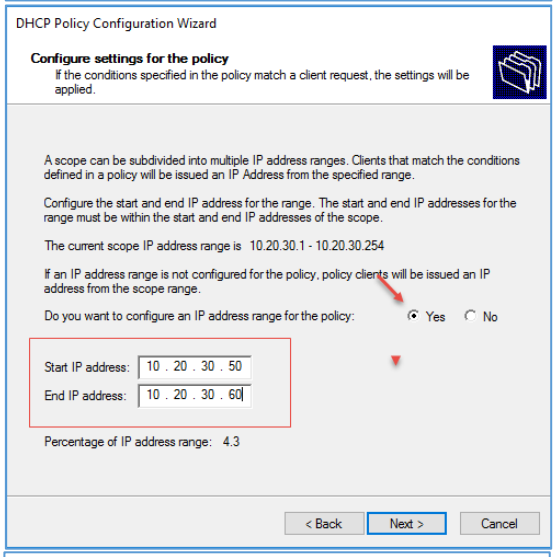


در این صفحه، دو گزینه‌ی And و OR وجود دارد که باید آنها را بسته به شرط خود انتخاب کنید، مثلاً می‌خواهید یک مک آدرس با یک اسم مشخّص استفاده کنید باید گزینه‌ی AND را انتخاب کنید.

در این قسمت، گزینه‌ی OR را انتخاب و بر روی Add کلیک کنید.

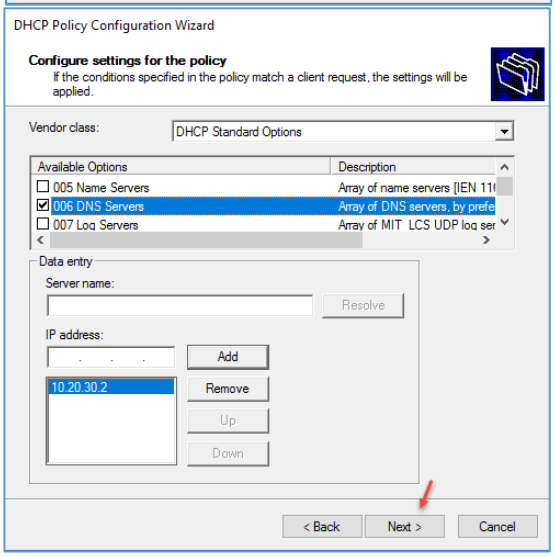


در این صفحه و در قسمت شماره‌ی یک، Mac address را انتخاب کنید و در قسمت شماره‌ی دو، Equals را انتخاب کنید، در قسمت شماره‌ی ۳ باید سه قسمت اوّل آدرس مک دستگاه‌های خود را وارد و تیک گزینه‌ی Append Wildcard را انتخاب کنید تا برای بقیّه‌ی آدرس، علامت * قرار دهد و در آخر کار بر روی Add کلیک کنید تا آدرس به لیست اضافه شود، بعد بر روی OK کلیک کنید، توجّه داشته باشید اگر گزینه‌ی Prefix wildcard را انتخاب می‌کردید، در اوّل آدرس، * قرار می‌داد و سه حرف اوّل را در آخر مک آدرس قرار می‌داد.



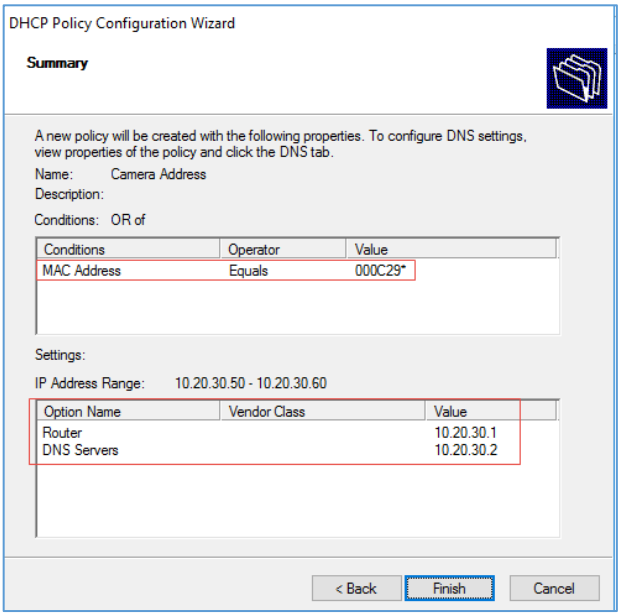
در این صفحه می‌توانید برای دستگاه‌های خود یک رنج آدرس مشخّص کنید، مثلاً اگر این سری از مک آدرس‌ها بودند، این رنج آدرس به آنها تعلّق پیدا کند، البتّه با این کار می‌توانید نظم در کار ایجاد کنید.

رنج مورد نظر خود را وارد و بر روی Next کلیک کنید.

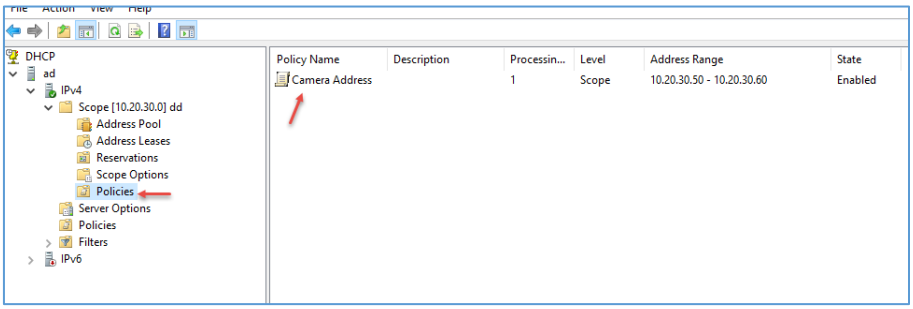


در این صفحه می‌توانید برای رنج آدرس خود، تنظیمات مشخّص نیز انجام دهید، مثلاً می‌توانید DNS آنها را تغییر دهید و یا آدرس روتر آنها را مشخّص کنید.

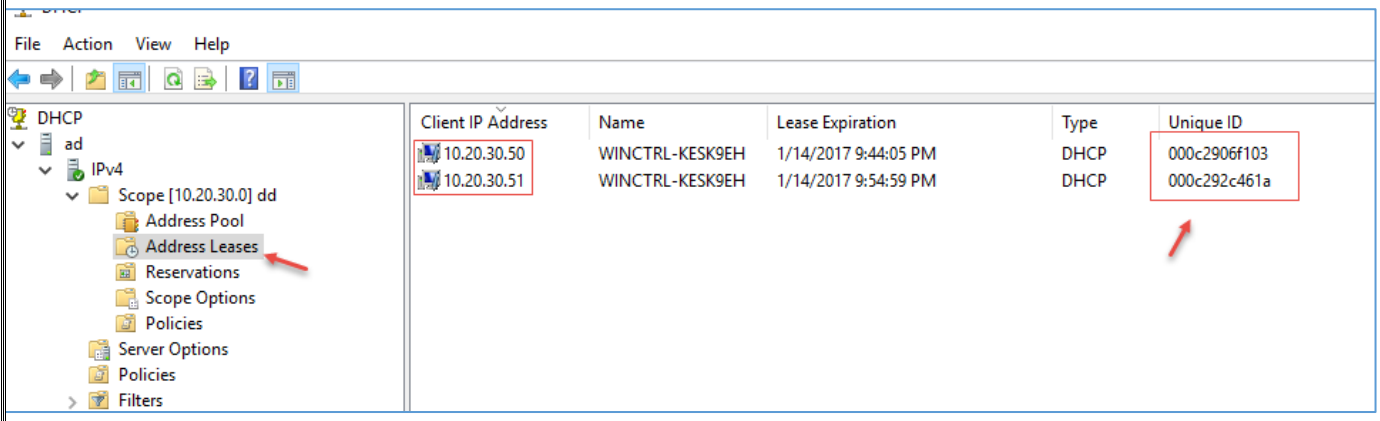
بعد از انجام این کار بر روی Next کلیک کنید.



در این صفحه می‌توانید اطّلاعات کلّی خود را مشاهده کنید، در صورت اشتباه می‌توانید به عقب برگردید و آنها را تکمیل کنید.



همانطور که مشاهده می‌کنید، Policy مورد نظر به لیست اضافه شده است، در حال حاضر اگر دستگاه‌ها را به شبکه متّصل کنید، این Policy روی آنها ست خواهد شد.



همانطور که در شکل بالا مشاهده می‌کنید، دو کلاینت به لیست اضافه شده‌اند که آدرس آنها در رنج مشخّص شده است و آدرس MAC آنها نیزمشخّص است.

سرویس Active Directory:

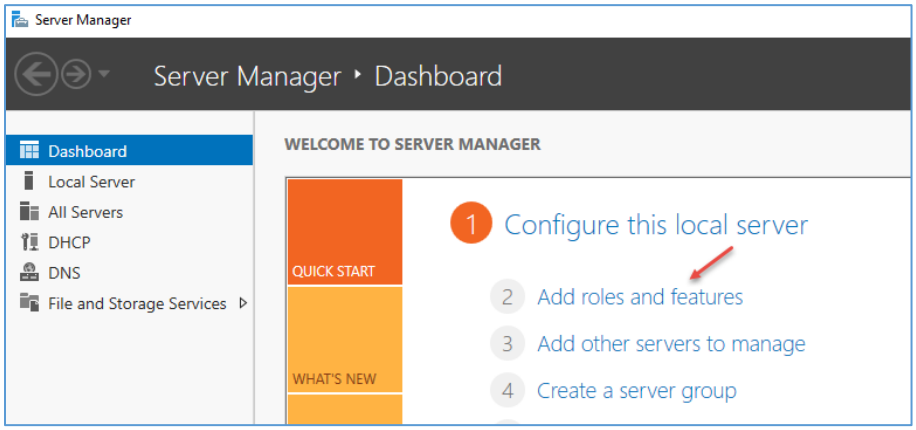
اکتیو دایرکتوری برای مدیریّت منابع شبکه است که به وسیله‌ی دامین کنترولر مدیریّت می‌شود و در اصل، یک کنترل‌کننده‌ی متمرکز شبکه است که برای سرویس‌دهنده‌های بر مبنای ویندوز سرور تهیّه شده است؛ بدون اکتیو دایرکتوری، مدیریّت منابع نیازمند مدیریّت آن‌ها به صورت جداگانه است، در حالی که توسّط اکتیو دایرکتوری مدیریّت منابع شبکه به صورت متمرکز صورت می‌گیرد. این فنّاوری طوری طرّاحی شده است که مسئولیّت رسیدگی به تعداد زیادی عملیّات خواندن و جستجو و نیز تعداد قابل توجّهی تغییرات و به روز رسانی‌های کوچک را به عهده دارد، برای مثال، برای به اشتراک گذاشتن چند فولدر بر روی شبکه در حالتی که اکتیو دایرکتوری موجود نباشد، نیازمند تعیین دسترسی هر کاربر در هر فولدر به صورت جداگانه هستید و با ایجاد تغییرات در کاربران و فولدرها باید این تغییرات به صورت جداگانه انجام دهید، در حالی که در حالت اکتیو دایرکتوری با اعمال قوانین گروهی (group policy) می‌توانید این کارها را به صورت متمرکز انجام دهید.

مثال دوّم: با به کارگیری اکتیو دایرکتوری، زمانی که کاربر تصمیم به تعویض گذر واژه‌ی خود می‌کند، تمام سیستم‌های کاربری که با اکتیو دایرکتوری Join شدند، به صورت خودکار با گذر واژه‌ی جدید شما هماهنگ می‌شوند و نیازی به تغییر جداگانه‌ی آنها نیست.

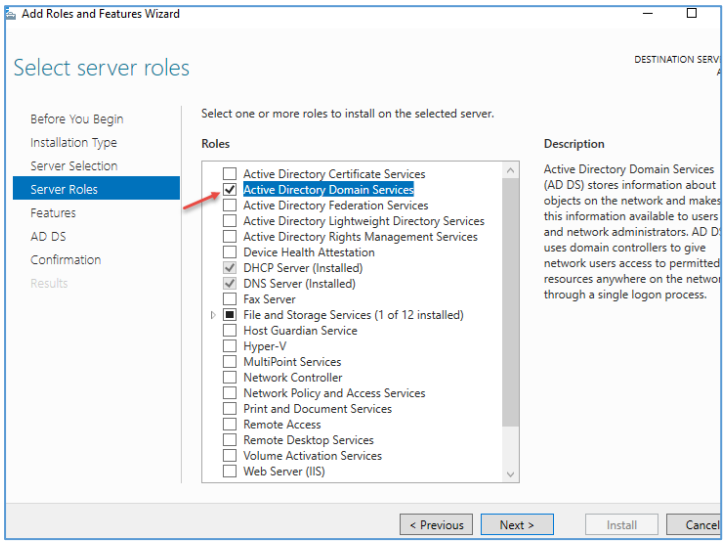
سروری که سرویس اکتیو دایرکتوری را ارائه می کند، دامین کنترولر یا DC نام دارد؛ این سیستم، وظیفه‌ی احراز هویّت و تعیین سطح دسترسی برای تمامی کاربران و کامپیوترهای متّصل به دامین را بر عهده دارد، به عنوان مثال زمانی که یک کاربر به یک کامپیوتر متّصل به دامین Login می‌کند، اکتیو دایرکتوری درستی گذر واژه را بررسی می‌کند و مشخّص می کند آن کاربر چه سطح دسترسی را دارا می باشد.

اکتیو دایرکتوری از پروتکل‌های LDAP، نسخه‌ی ۲ و ۳، کربرس و DNS استفاده می کند.

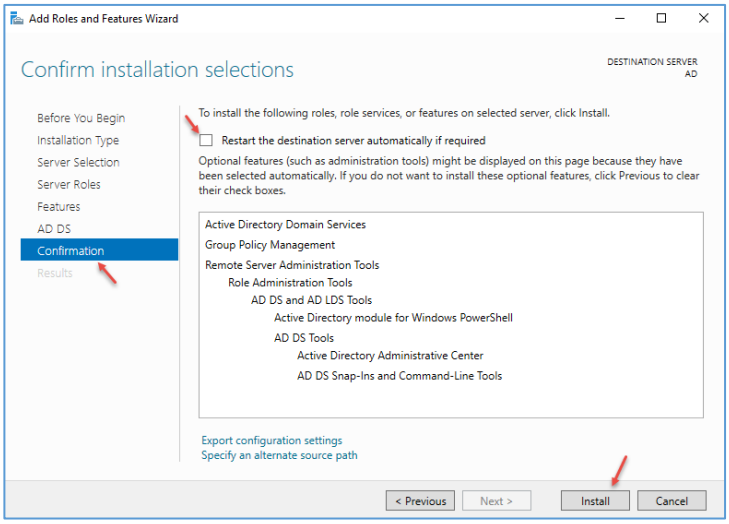
نصب و راه‌اندازی سرویس Active Directory:



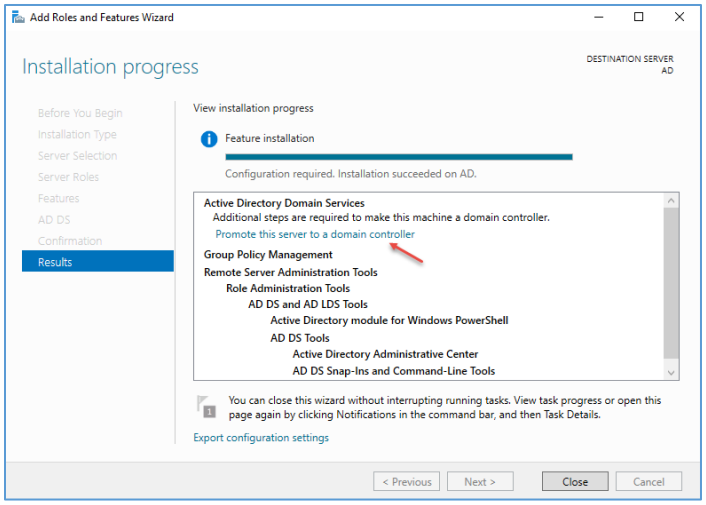
برای شروع به کار و نصب سرویس Active Directory وارد Server Manager شوید و بر روی Add roles and features کلیک کنید.



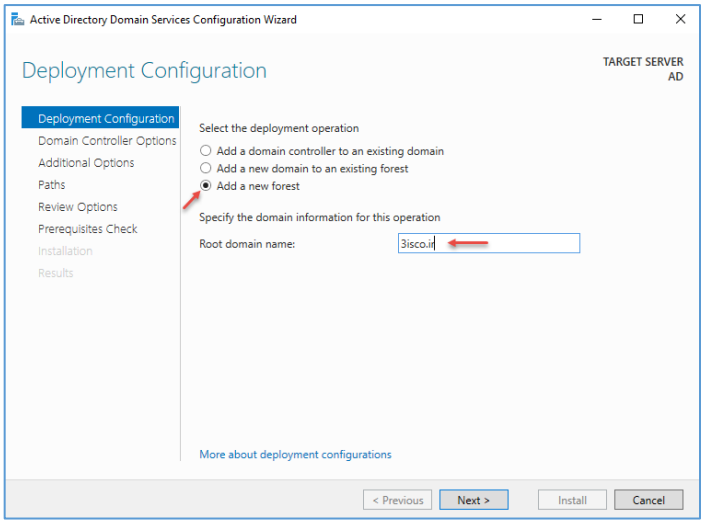
در قسمت Server Roles، سرویس Active Directory Domain Services را انتخاب و در صفحه‌ی باز شده بر روی Add Features کلیک کنید و بعد بر روی Next کلیک کنید.



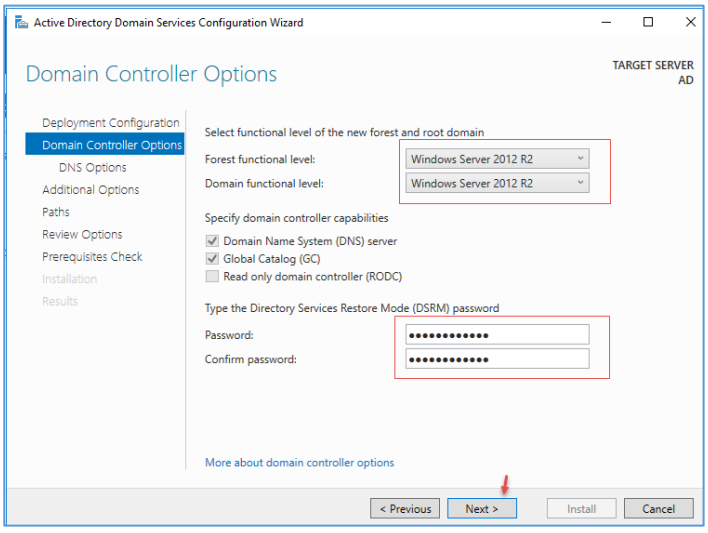
در قسمت Confirmations، تیک گزینه‌ی Restart را انتخاب و بر روی Install کلیک کنید.



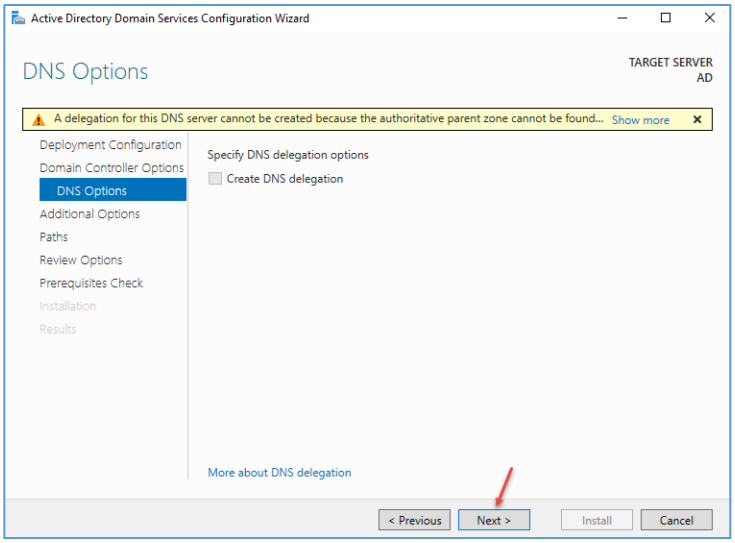
بعد از نصب اوّلیّه‌ی سرویس، شکل روبرو ظاهر می‌شود که باید آدرس دومین شبکه‌ی مورد نظر خود را معرّفی کنید، برای این کار بر روی Promote this server to a domain controller کلیک کنید.



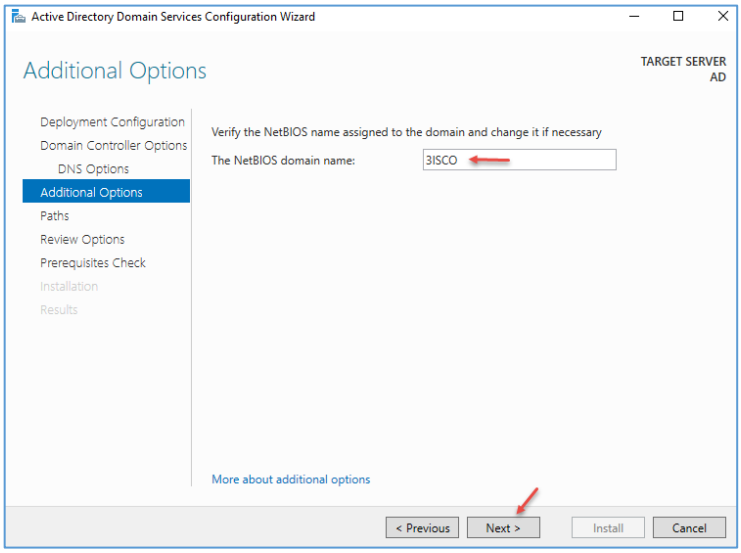
در این صفحه، چند گزینه وجود دارد که برای شروع کار و راه‌اندازی اوّلین دومین کنترلر باید گزینه‌ی Add a new forest را انتخاب و نام دومین خود را وارد کنید که در اینجا، 3isco.ir نوشته شده است، توجّه داشته باشید که اگر این نام دومین در اینترنت نیز اعتبار داشته باشد، احتمال دارد با متّصل کردن سرور به اینترنت با مشکل مواجه شوید.



در این صفحه و در قسمت اوّل می‌توانید مشخّص کنید که سرور دومین شما با چه ورژنی از ویندوز سرور در ارتباط باشد تا بتواند اطّلاعات دومین را به آنها انتقال دهد، به نظر بنده بهترین انتخاب، Windows server 2012 است؛ در قسمت پایین نیز یک رمز عبور پیچیده، مانند 3isco@2012 برای مد ریکاوری DSRM وارد و بر روی Next کلیک کنید.

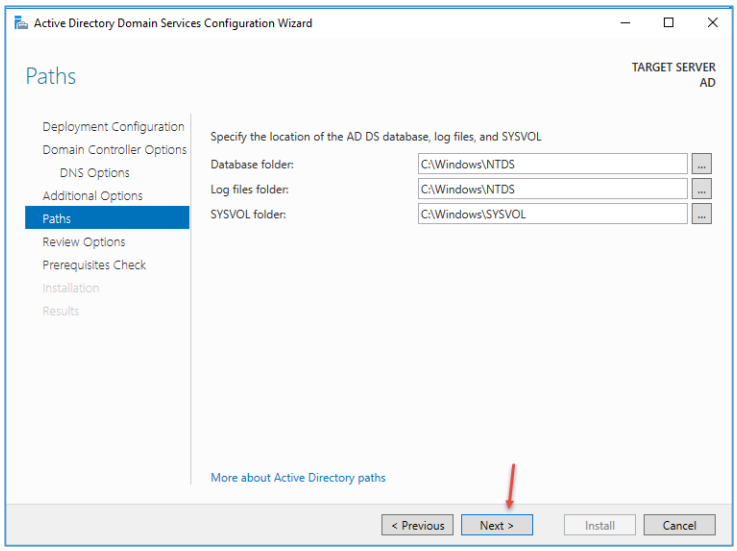


در این قسمت به پیغامی مبنی بر تنظیم نشدن DNS برای ساخت Zone مورد نظر را می‌دهد که باید بر روی Next کلیک کنید.



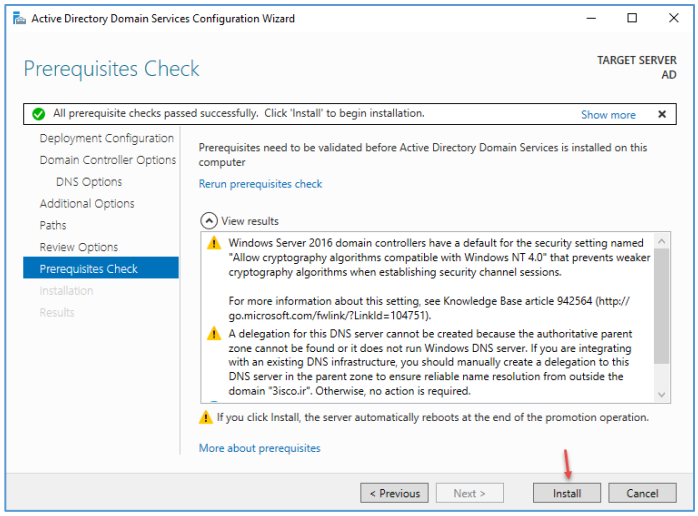
در این صفحه، نام دومین شما در صورت موجود نبودن تأیید خواهد شد؛ بر روی Next کلیک کنید.

تذکّر: اگر سرور شما به اینترنت متّصل باشد و شما یک دومین، مانند 3isco.ir را وارد کرده باشید در این قسمت با خطا مواجه خواهید شد، پس این نکته را مدّ نظر داشته باشید.



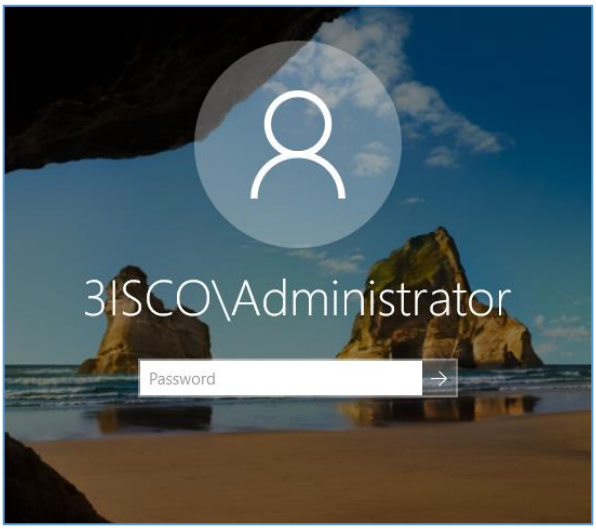
در این قسمت شما می‌توانید آدرس ذخیره شدن دیتابیس و دیگر اجزای Active Directory را مشخّص کنید که به صورت پیش‌فرض، آدرس به آن داده شده است.

در صفحه‌ی بعد، اگر اطّلاعات مورد تأیید است بر روی Next کلیک کنید.



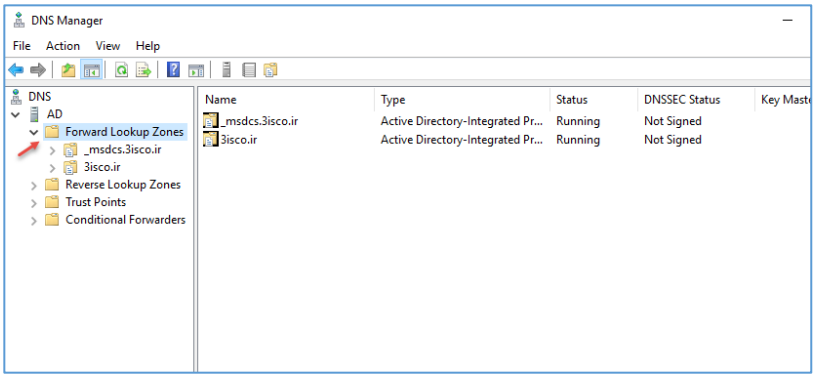
در این صفحه، تنظیمات و پیش‌نیازهای نصب مورد تأیید است؛ بر روی Install کلیک کنید.

بعد از نصب، سرور Restart خواهد شد، اگر نشد شما این کار را انجام دهید.



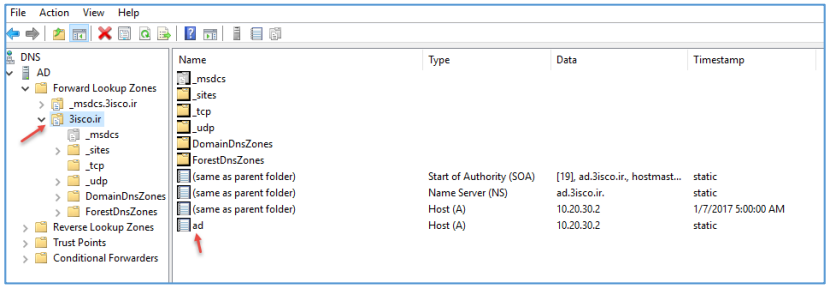
بعد از اجرا شدن سرور به مانند شکل روبرو رمز عبور مربوط به کاربر Administrator را وارد کنید.

توجّه داشته باشید، قبل از آن نام دومین نیز نوشته شده باشد.

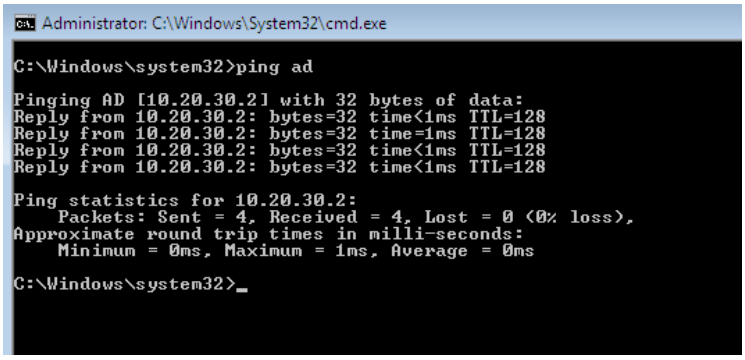


اگر بعد از نصب سرویس Active Directory به سرویس DNS مراجعه کنید، متوجّه خواهید شد که در قسمت Forward LoOKup Zones، دو Zone ایجاد شده است، Zone اوّل با عنوان _msdcs.3isco.ir ایجاد شده است که برای نگهداری تنظیمات zone اصلی با نام 3isco.ir ایجاد شده است و یک سری تنظیمات اوّلیّه در آن ذخیره شده است، در zone اصلی، یعنی 3isco.ir تمام اطّلاعات شبکه اعمّ از نام کلاینت یا سرور به همراه آدرس آنها و... ذخیره می‌شود، Zone تستی که قبلاً با نام Test.local ایجاد کرده بودیم را حذف کردیم.

در سرویس DNS به صورت پیش‌فرض زمانی که دومین را راه‌اندازی می‌کنید، تنها Forward LoOKup Zone فعّال است که این قابلیّت به سرور اجازه می‌دهد تا اسم را تبدیل به آدرس IP کند، مثلاً اگر شما یک نام را در شبکه، Ping کنید در صورت موجود و فعّال بودن ارتباط برقرار خواهد شد.

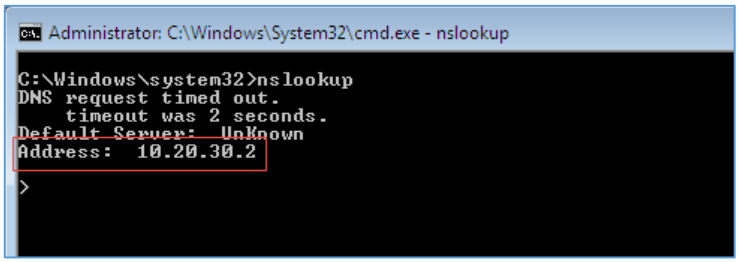


در شکل روبرو یک نام AD تعریف شده است، اگر کاربر این نام را در کلاینت خود Ping کند که در شکل زیر این قابلیّت را مشاهده می‌کنید.



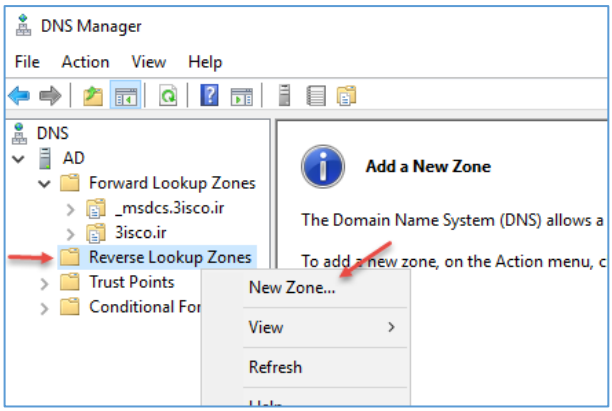
همانطور که مشاهده می‌کنید، نام AD در حال Ping شدن است و IP آن نیز، 10.20.30.2 است.

حال اگر بخواهیم آدرس IP تبدیل به اسم شود باید چه کاری انجام دهیم؟



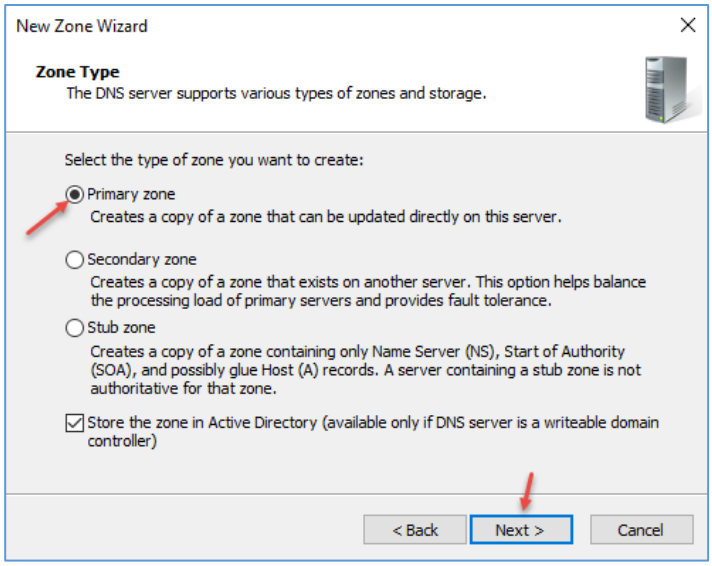
برای تست اینکه آیا در شبکه‌ی ما آدرس IP به اسم تبدیل می‌شود باید از دستور NsloOKup استفاده کنیم که در شکل روبرو استفاده شده و نام سرور دومین را پیدا نکرده است.

توجّه داشته باشید، زمانی که تنها از دستور NsloOKup استفاده می‌کنید، این دستور به دنبال آدرس DNS می‌گردد و برای اینکه یک سیستم مشخّص را صدا بزنید باید از دستور NsloOKup 10.20.30.45 استفاده کنید.

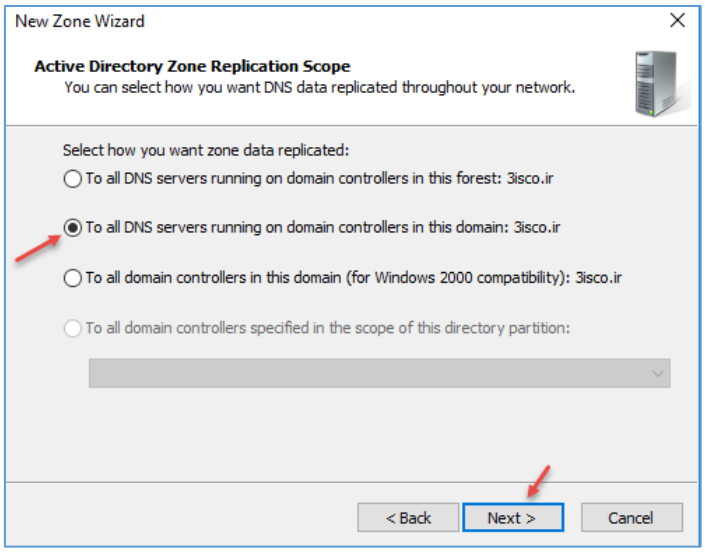


برای اینکه تبدیل آدرس IP به اسم را انجام بدهید باید در سرویس DNS بر روی Reverse LoOKup Zones کلیک راست کنید و گزینه‌ی New Zones را انتخاب کنید.

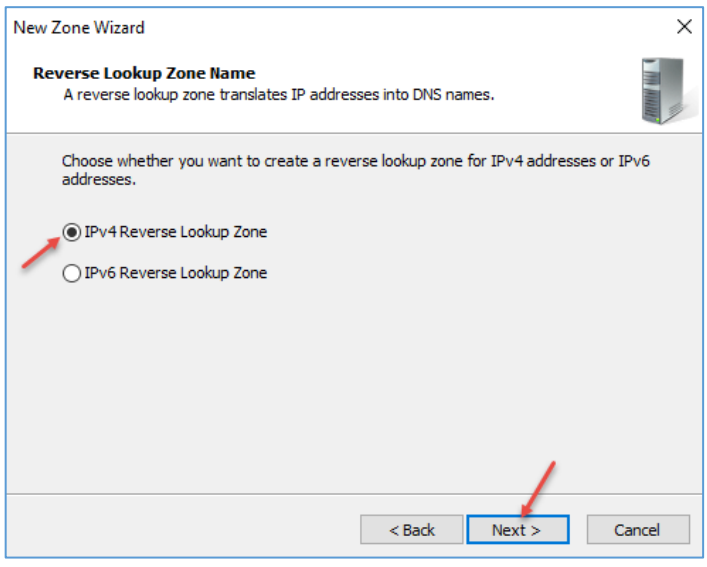
این موضوع را در اوایل کتاب بررسی کردیم.



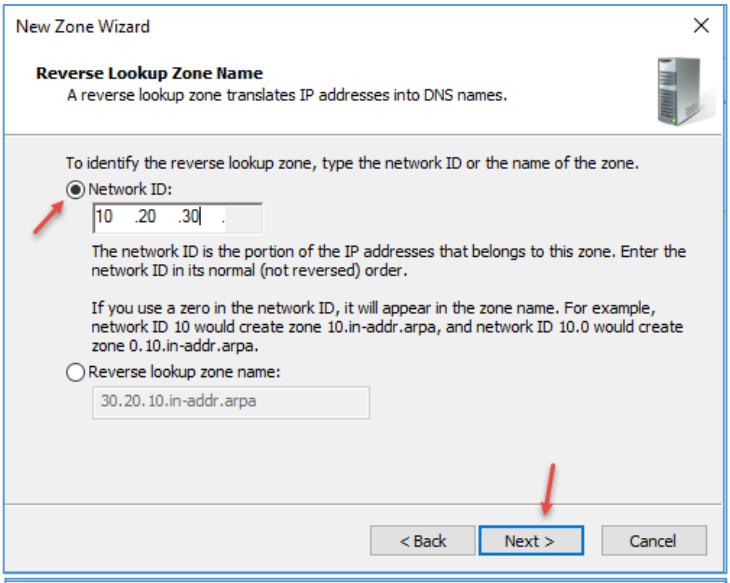
در این قسمت، گزینه‌ی Primary Zone را انتخاب کنید، البتّه این گزینه‌ها را در اوایل کتاب و در سرویس DNS نیز توضیح دادیم.



در این قسمت، گزینه‌ی دوّم را انتخاب و بر روی Next کلیک کنید.

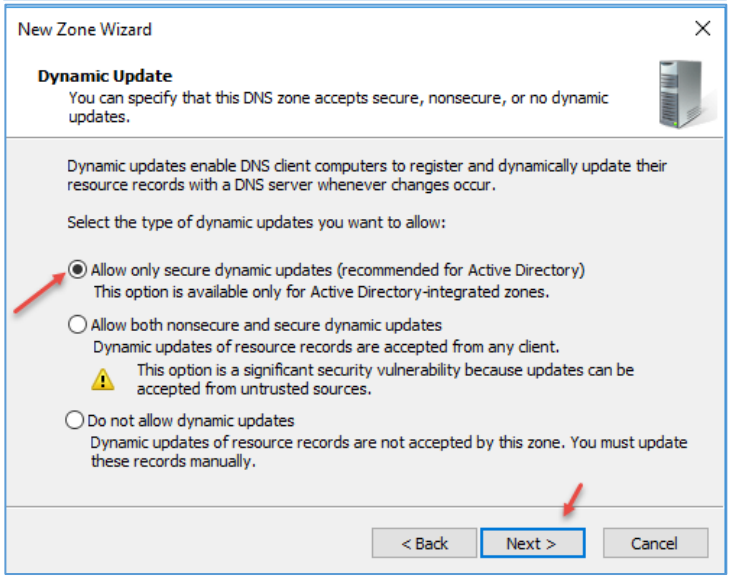


در این قسمت، گزینه‌ی IPv4 Reverse LoOKup Zone را انتخاب و بر روی Next کلیک کنید.



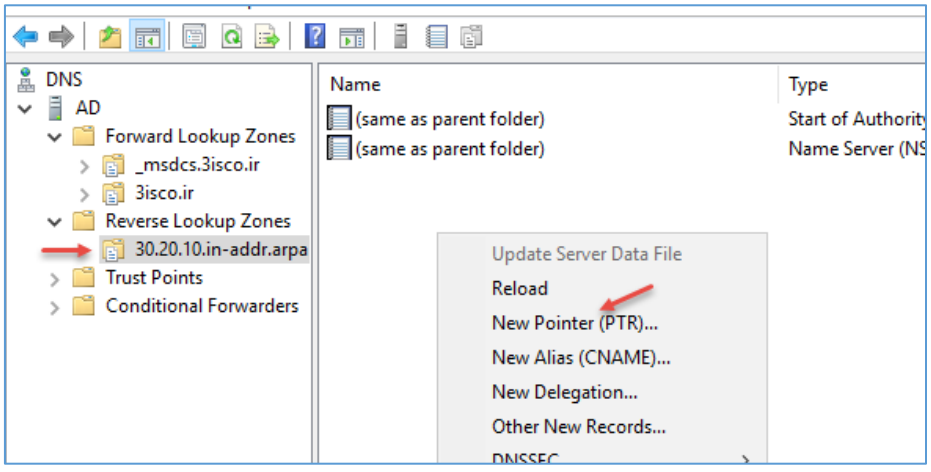
در این قسمت باید Network ID خود را وارد کنید که در اینجا، 10.20.30 است.

بر روی Next کلیک کنید.

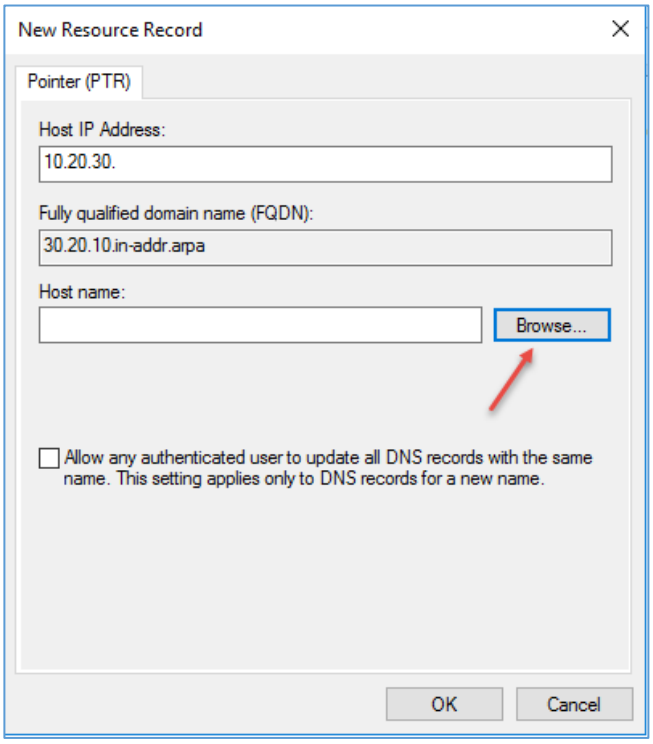


در این قسمت، گزینه‌ی یک که از نظر خود مایکروسافت، بهترین گزینه است را انتخاب و بر روی Next کلیک کنید.

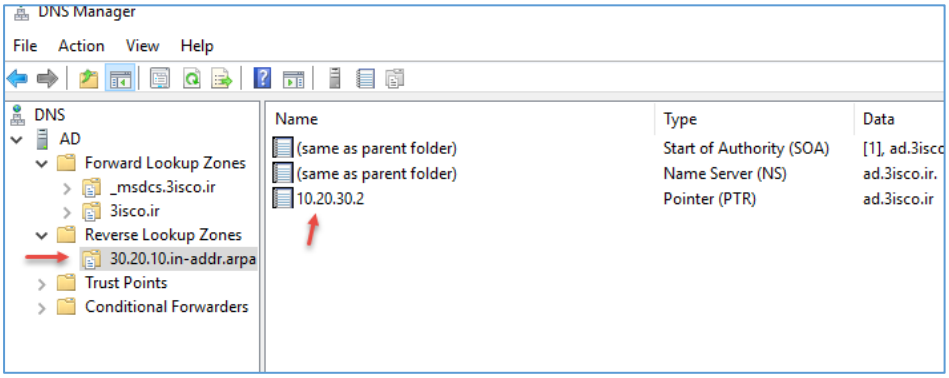
در صفحه‌ی بعد بر روی Finish کلیک کنید.



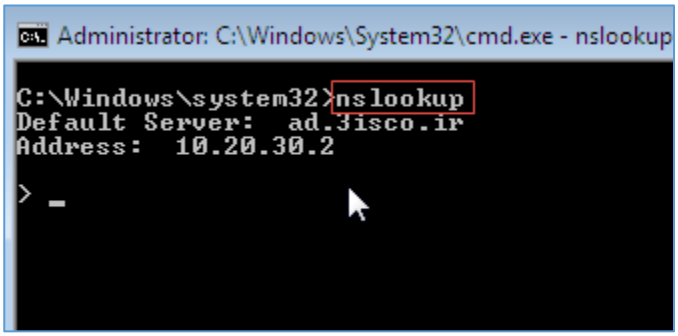
بعد از ایجاد Reverse LoOKup Zones بر روی آن کلیک کنید و در صفحه‌ی مورد نظر کلیک راست و گزینه‌ی PTR را انتخاب کنید.



در این قسمت شما می‌توانید با کلیک بر روی Browse و از طریق Forward LoOKup Zone، کلاینت و سرور مورد نظر را انتخاب کنید تا آدرس IP آنها به اسم تبدیل شود، در این قسمت سرور AD را به لیست اضافه کنید.

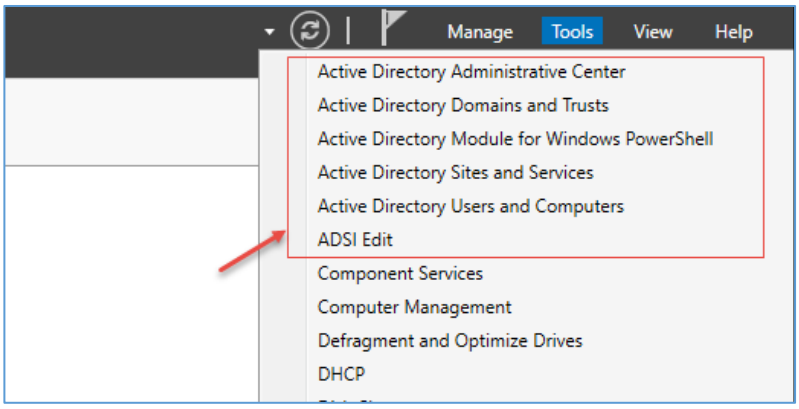


همانطور که مشاهده می‌کنید، PTR مربوط به سرور AD به لیست اضافه شده است.



در شکل روبرو با اجرای دستور NsloOKup، نام سرور DNS به همراه آدرس IP را مشاهده می‌کنید.

بررسی سرویس‌های Active directory:



اگر وارد Server Manager شوید و بر روی منوی Tools کلیک کنید، مشاهده خواهید کرد که بعد از نصب سرویس Active Directory، چند سرویس به لیست اضافه شده است که با هم آنها را بررسی می‌کنیم.

سرویس Active Directory Administrator Center:

یک سرویس جامع برای مدیریّت کاربران، گروه‌ها و... است که کار با آنها را برای مدیر شبکه آسان می‌کند، این سرویس از زمان ویندوز سرور ۲۰۰۸، ورژن R2 به بازار عرضه شد و تنها مزیّت آن نسبت به سرویس Active directory Users and Computers، سرعت دسترسی آن است.

سرویس Active Directory Domain and Trust:

این سرویس برای ایجاد یک پل ارتباطی امن بین دو دومین متفاوت ایجاد شده است، زمانی که شما یک دومین Forest یا اصلی را راه‌اندازی می‌کنید، تمام اجزای آن جدا و به تنهایی در حال کار هستند، امّا اگر بخواهید این نوع دومین را با دومین دیگر ارتباط دهید می‌توانید از این سرویس استفاده کنید.

سرویس Active directory Module for windows PowerShell:

این سرویس برای وارد کردن دستورات Active Directory در PowerShell ویندوز است که بعد از آن می‌توانید از دستورات Active directory در سرویس PowerShell استفاده کنید.

سرویس Active directory Site and service:

سرویسی برای انتقال اطّلاعات بین دو یا چند دومین مختلف در یک Forest است که اگر شما یک سرور دومین داشته باشید و بخواهید مثلاً یک دومین دیگر برای بک آپ داشته باشید، توسط این سرویس، اطّلاعات بین دو دومین انتقال داده خواهد شد که با هر تغییر در دومین اصلی در دومین دوّم نیز تغییرات اعمال خواهد شد.

سرویس Active Directory Users and Computers:

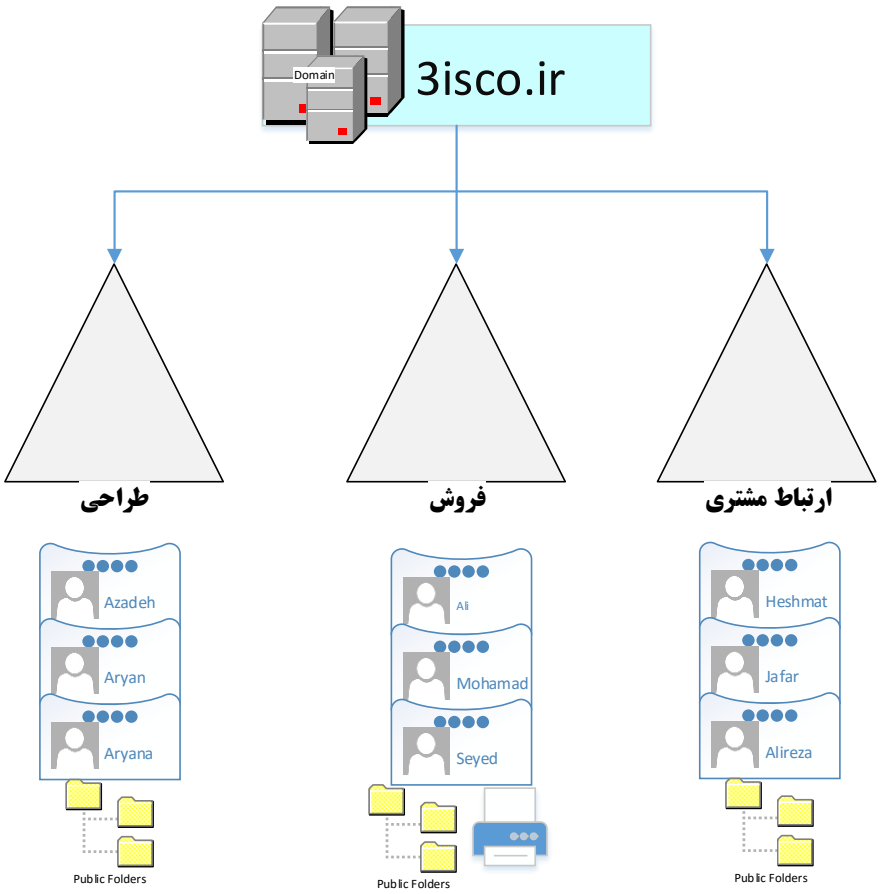
یکی از قدیمی‌ترین و مهمترین سرویس Active Directory است که برای ایجاد کاربر، گروه، پرینتر، فولدر share شده و... کاربرد دارد که در این کتاب نیز به بررسی آن خواهیم پرداخت.

سرویس ADSI:

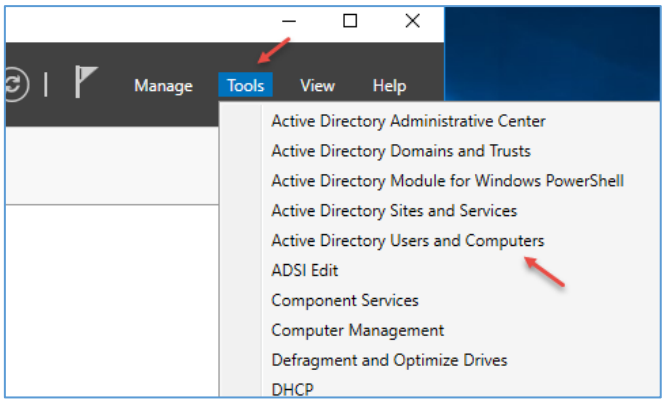
این سرویس یک دایرکتوری از اطّلاعات کلّی شبکه است که می‌توان قلب تپنده‌ی ویندوز سرور نامید که بیشتر برای استفاده‌ی برنامه‌نویسان ایجاد شده است.

کار با سرویس Active Directory Users and Computers:

برای شروع کار باید بدانید که از این سرویس چه می‌خواهید، شما زمانی که برای اوّلین بار می‌خواهید این سرویس را ایجاد کنید باید اوّل یک نقشه‌ی کلّی از شبکه‌ی خود تهیّه کنید، مثلاً سازمان شما، دارای چند بخش و چند کاربر و اطّلاعاتی از این دست است، شما می‌توانید در این سرویس برای هر بخش در سازمان خود، یک Organization Unit یا همان واحد سازمانی تعریف کنید، مانند شکل زیر:

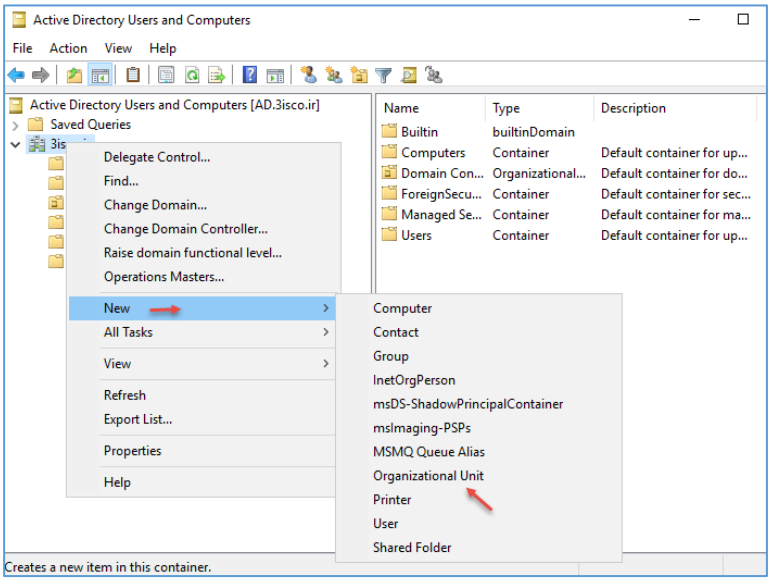


به طور مثال، اگر تصوّر کنیم که شما در سازمان خود، دارای سه بخش کلیدی به مانند شکل صفحه‌ی قبل باشید، بهترین راه برای مدیریّت بهتر کاربران، ایجاد واحدهای سازمانی مجزّا است؛ در هر بخش می‌توانید کاربران مورد نظر خود را تعریف و فولدر share شده‌ی آنها را مشخّص کنید، از طریق این روش می‌توانید دسترسی‌هایی را نیز به این واحدها دهید که در ادامه بر روی آنها بیشتر بحث خواهیم کرد.

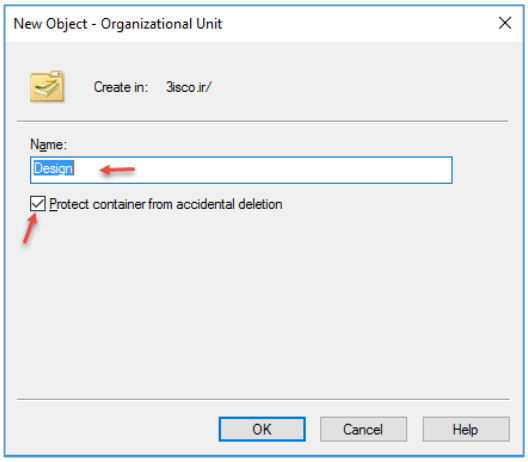


برای شروع کار وارد Server Manager شوید و از منوی Tools، گزینه‌ی Active Directory Users and Computers را انتخاب کنید.

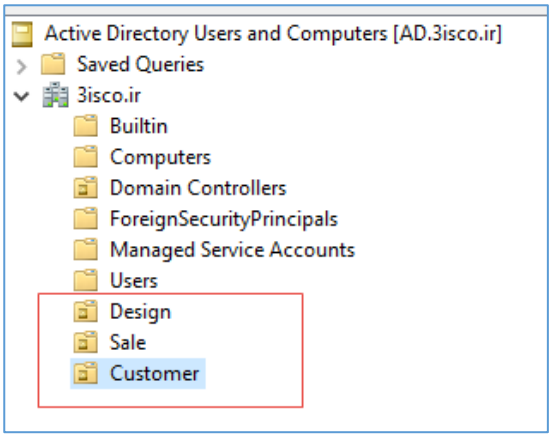
تعریف Organization Unit:



بعد از ورود به Active برای ایجاد Organization Unit یا واحد سازمانی بر روی نام دومین کلیک راست کنید و از قسمت New، گزینه‌ی Organization Unit را انتخاب کنید.



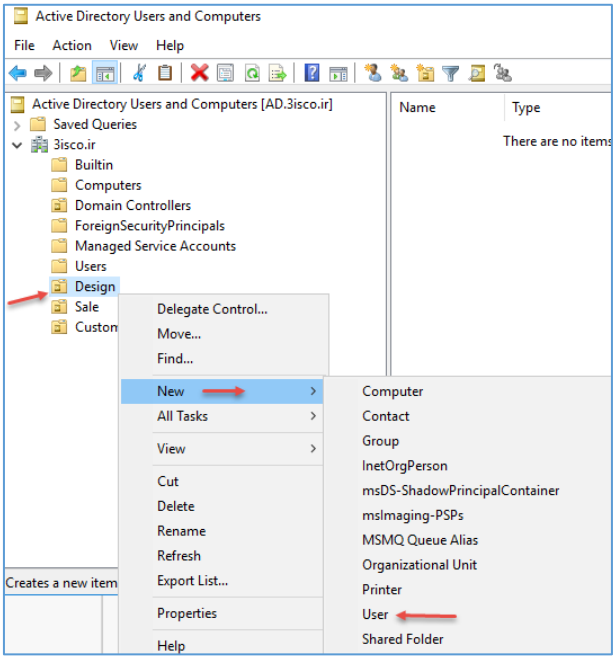
در این صفحه، نام گروه سازمانی خود را وارد و تیک گزینه‌ی Protect Container From Accidental deletion را انتخاب کنید، این گزینه باعث می‌شود شما یا هر کسی دیگر نتواند این واحد سازمانی را حذف کند، البتّه برای حذف، روشی است که در صورت نیاز بیان خواهیم کرد.



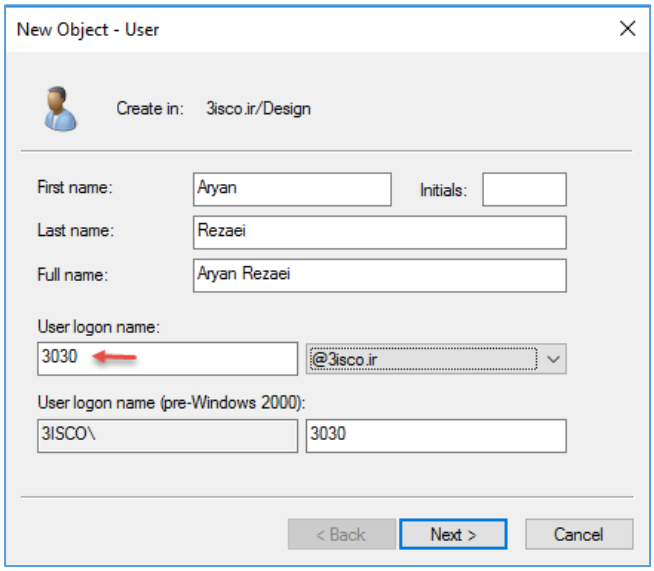
همانطور که مشاهده می‌کنید، سه گروه سازمانی برای بخش طرّاحی، فروش، و مشتری ایجاد کردیم که این عمل می‌تواند برای نظم بخشیدن به کار بسیار مؤثّر باشد.

تعریف کاربر در Active directory:

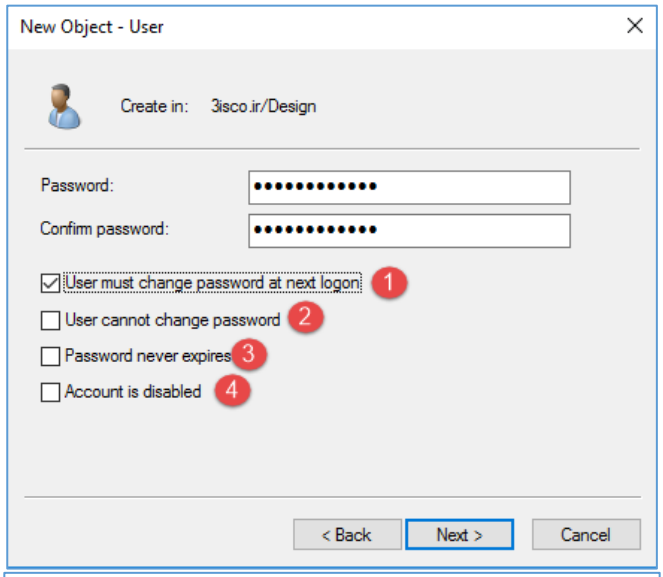
قبل از تعریف کاربر باید بدانید که چه اطّلاعاتی از کاربر نیاز دارید، برای این کار شما باید یک فرم تهیّه کنید و در اختیار کاربر قرار دهید تا آن را تکمیل کند، این فرم می‌تواند، شامل نام و نام خانوادگی، نام مستعار، شماره‌ی تماس، آدرس منزل، آدرس سایت و... باشد که می‌تواند بسیار کمک کننده باشد، سعی کنید برای هر کاربر یک کد پرسنلی تعریف کنید، مثلاً کد پرسنلی که در زمان استخدام شدن در یک سازمان به آنها داده می‌شود و یا کد دانشجویی در دانشگاه.



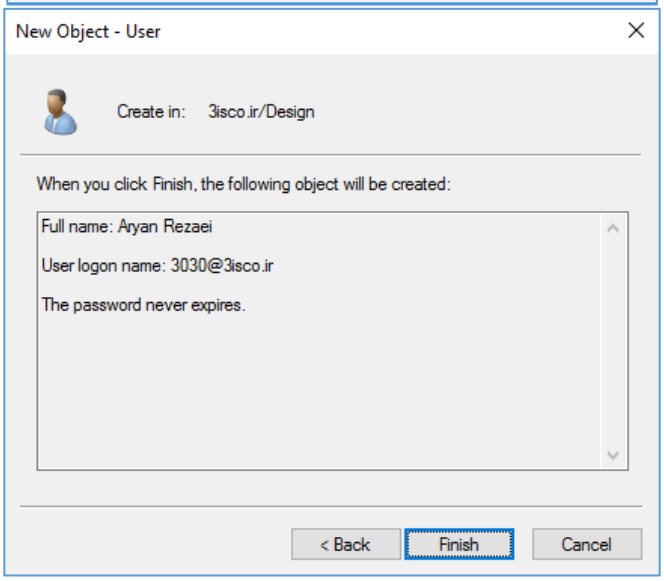
برای تعریف کاربر باید بر روی واحد مورد نظر خود کلیک راست کنید و از قسمت New، گزینه‌ی User را انتخاب کنید.



در این صفحه و در قسمت First Name، نام کاربر خود را وارد کنید و اگر این کاربر، اسم مستعار دارد، می‌توانید در قسمت Initials وارد کنید، در قسمت Last Name نیز نام خانوادگی کاربر مورد نظر را وارد کنید که بعد از ورود اطّلاعات در قسمت Full Name، نام کامل کاربر که در کلّ شبکه به نمایش در خواهد آمد را می‌بینید؛ در قسمت User logon name شما باید نام کاربری کاربر مورد نظر را وارد کنید که در اینجا از اسم استفاده نکردیم، این کاربر تنها با نام کاربری ۳۰۳۰ می‌تواند وارد شبکه شود.



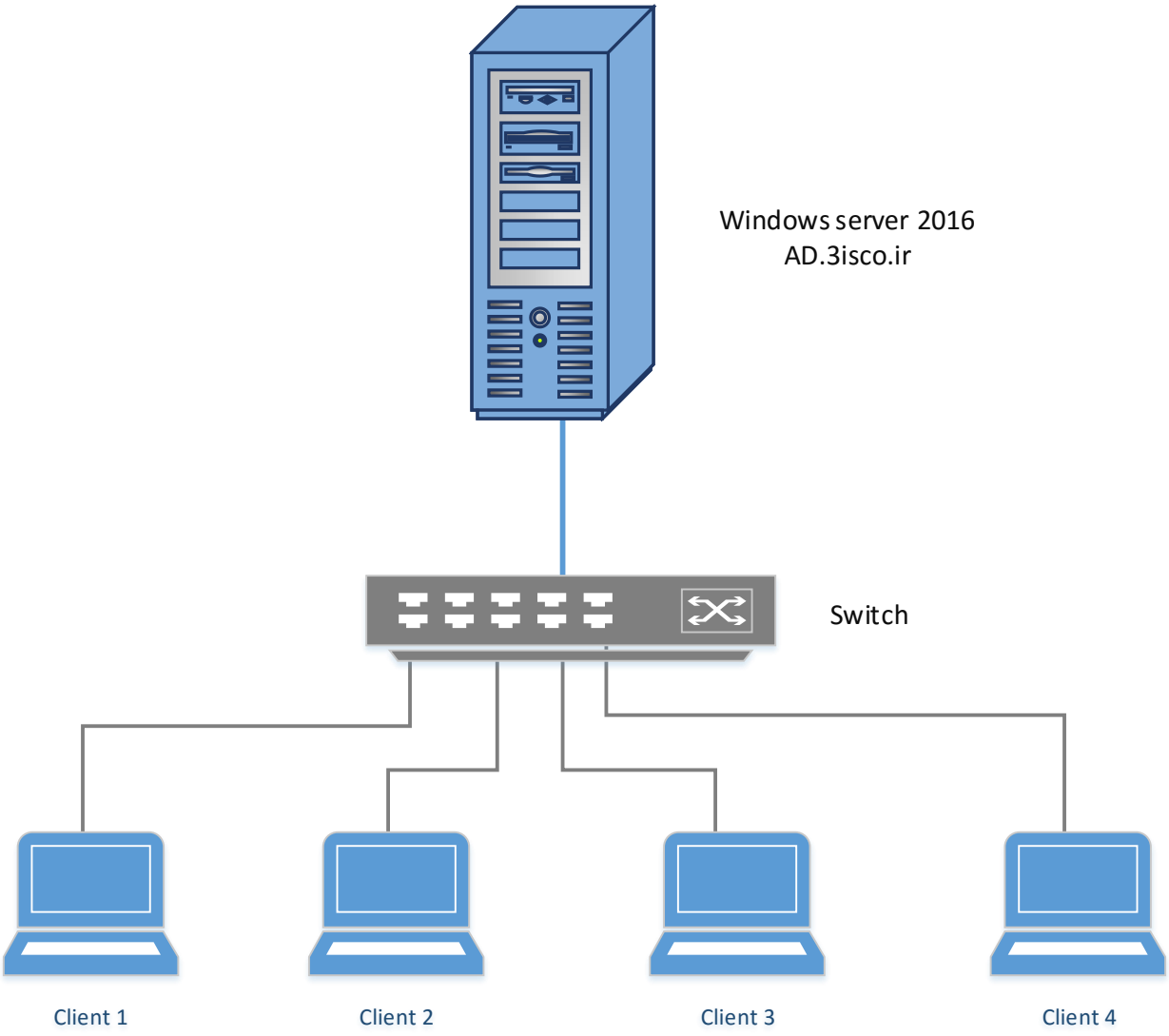
در این قسمت شما باید برای کاربر مورد نظر، یک رمز عبور پیچیده، مانند 3isco@2016 وارد کنید که البتّه می‌شود این پیچیدگی در رمز عبور را در سرویس Group Policy حذف کنید، گزینه‌های مختلفی نیز برای انتخاب وجود دارد که با انتخاب گزینه‌ی یک، کاربر مورد نظر با رمزی که وارد کردید، وارد سیستم می‌شود، امّا بعد از آن، درخواست تغییر داده می‌شود که باید رمز جدید خود را وارد کنید، اگر گزینه‌ی دوّم انتخاب شود کاربر نمی‌تواند رمز عبور تخصیص داده به خود را تغییر دهد، اگر گزینه‌ی سوّم انتخاب شود، رمز عبور مورد نظر هیچ وقت انقضا نمی‌شود. شما به عنوان مدیر شبکه می‌توانید یک مدّت مشخّص را برای تغییر رمز عبور برای کاربران در سرویس Group Policy ایجاد کنید؛ با انتخاب گزینه‌ی چهارم کاربر مورد نظر ایجاد می‌شود، امّا Account آن غیر فعّال خواهد بود و کاربر نمی‌تواند وارد شبکه شود.



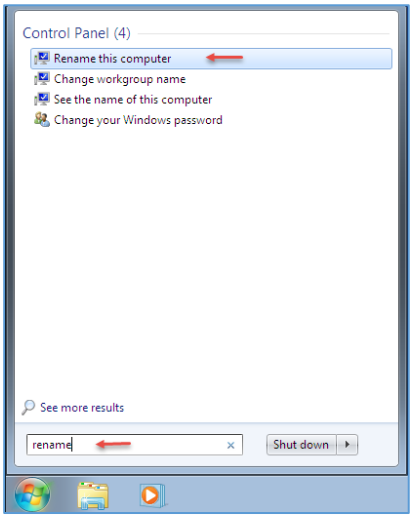
در قسمت آخر بر روی Finish کلیک کنید.

عضو کردن کلاینت در دومین:

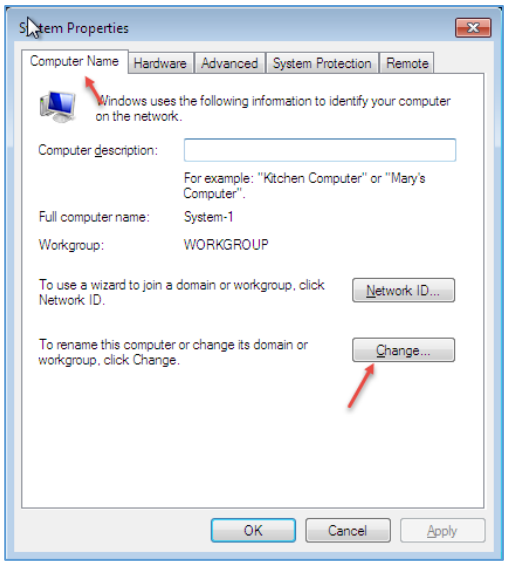
اگر یک کلاینت عضو شبکه نباشد، مدیریّت آن به شدّت سخت خواهد شد، برای اینکه مدیریّت کلاینت‌ها و کاربران آسان‌تر شود، بهتر است آنها را عضو دومین کنید تا مدیریّت آنها متمرکز شود.



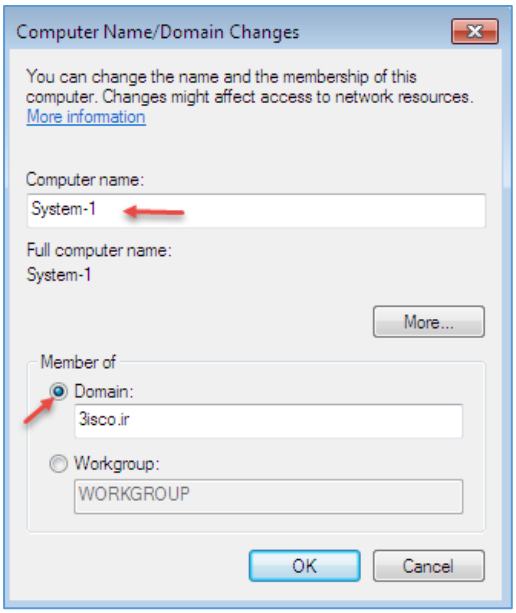
نحوه‌ی شبکه کردن به صورت Passive را قبلاً بررسی کردیم و در شکل بالا نیز نقشه‌ی کلّی از یک شبکه‌ی کوچک را مشاهده می‌کنید، اگر این کلاینت‌ها عضو شبکه‌ی 3isco.ir نباشند، مدیریّت آنها باید به صورت تکّی انجام شود و کار خیلی سخت خواهد شد، برای حل این مشکل باید تمام کلاینت‌های یک شبکه را عضو دومین کنید.



وارد یکی از کلاینت‌های خود شوید و از طریق منوی Start، گزینه‌ی Rename this Computer را جستجو و اجرا کنید.

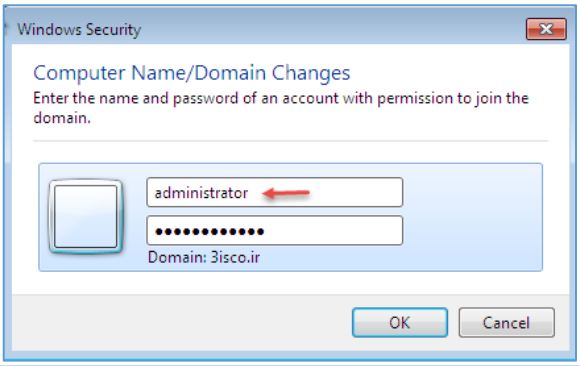


در تب Computer Name بر روی Change کلیک کنید.



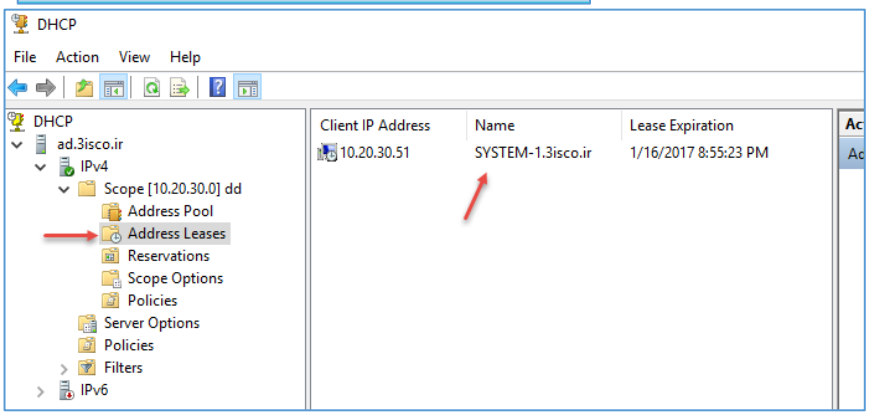
در این صفحه و در قسمت Computer name، نام کلاینت خود را وارد کنید، سعی کنید نام سیستم خود را بر اساس واحد یا بخشی که در آن قرار دارد، وارد کنید.

در قسمت Domain نیز باید نام دومینی که با هم راه‌اندازی کردیم را وارد و بر روی OK کلیک کنید، بعد از این کار، صفحه‌ای باز می‌شود که از شما، نام کاربری و رمز عبور ادمین دومین درخواست می‌کند که در اینجا، کاربر ادمین ما، Administrator است.

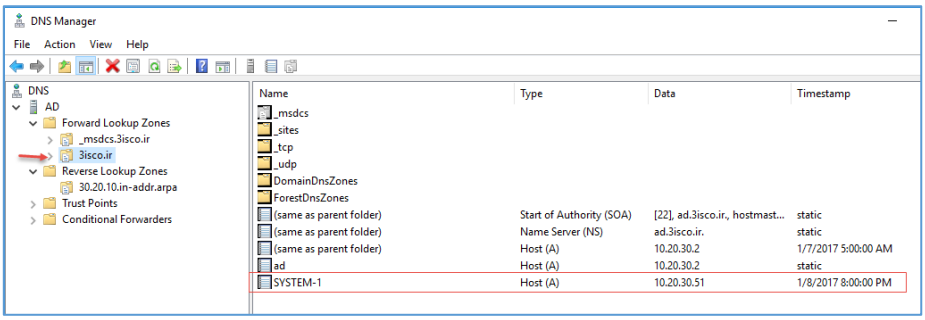


در این صفحه باید نام کاربر ادمین خود را وارد و بر روی OK کلیک کنید، با این کار کلاینت مورد نظر عضو دومین خواهد شد و نام آن در سرویس DNS و نیز Active Directory ثبت خواهد شد.

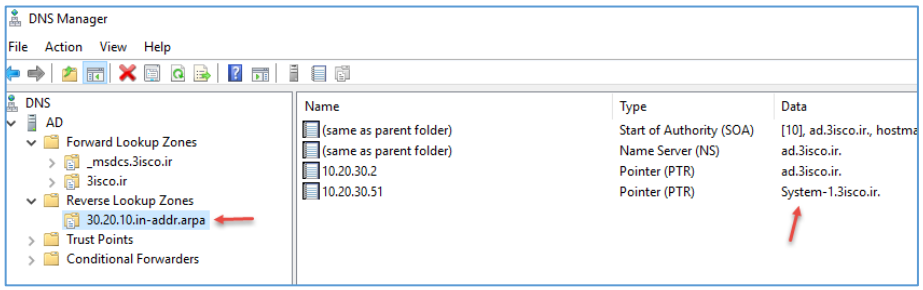
بعد از اینکه کلاینت عضو دومین شد، آن را Restart کنید.



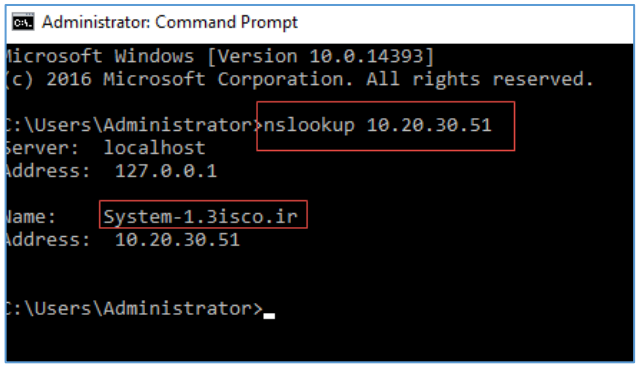
اگر سرویس‌ها را با هم بررسی کنیم در سرویس DHCP، نام کلاینت که عضو دومین شد را به همراه نام دومین آن در شکل روبرو مشاهده می‌کنید.



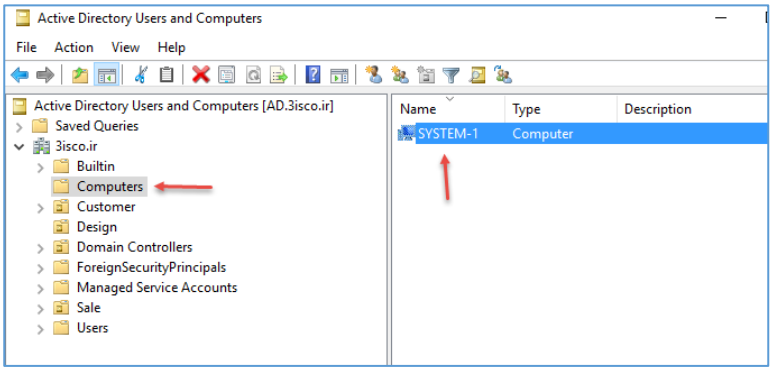
در سرویس DNS و در zone مربوطه، نام کلاینت system-1 را مشاهده می‌کنید، اگر به ستون TimeStamp توجّه کنید، زمان و تاریخ ثبت رکورد را مشاهده می‌کنید، اگر در این قسمت، Static نوشته باشد، یعنی اینکه آدرس کلاینت مورد نظر به صورت دستی وارد شده است، امّا اگر به صورت تاریخ و زمان باشد، یعنی این سیستم بر روی Automatic قرار دارد و IP دریافت می‌کند.



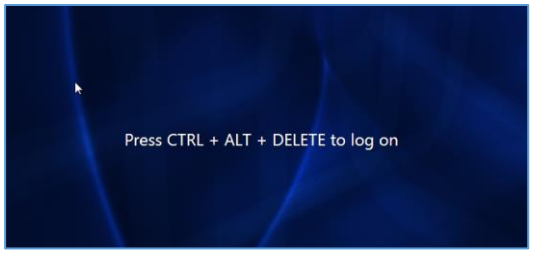
اگر وارد قسمت Reverse Zone شوید، مشاهده خواهید کرد که رکورد PTR مربوط به کلاینت System-1 نیز ایجاد شده است.



اگر درکلاینت، دستور nsloOKup 10.20.30.51 را وارد کنید، نام کلاینت را مشاهده خواهید کرد که این نیز به خاطر رکورد PTR در سرویس DNS است که البتّه قبلاً آن را بررسی کردیم.



اگر در سرویس Active Directory وارد پوشه‌ی Computers شوید، نام کلاینت system-1 را مشاهده می‌کنید که بعد از اینکه عضو دومین شد به لیست اضافه شده است، با دو بار کلیک بر روی آن می‌توانید اطّلاعات آن را مشاهده کنید.





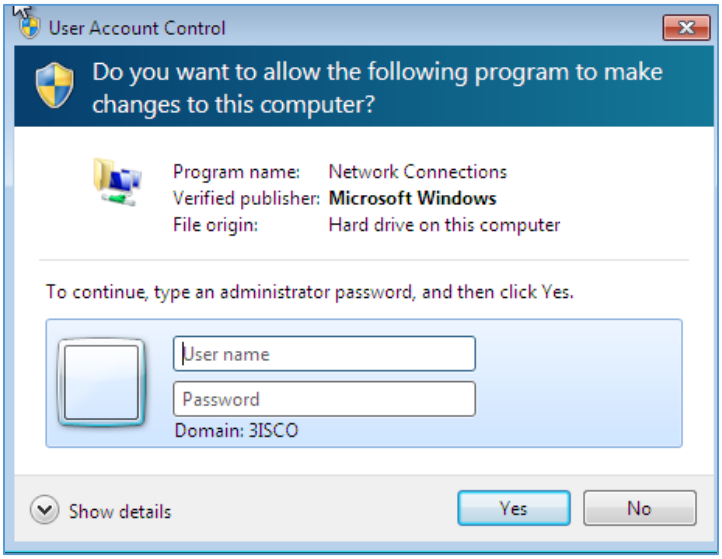
زمانی که سیستمی را عضو دومین می‌کنید، در زمان ورود این پیغام برای شما نمایش داده خواهد شد که برای ورود باید کلید ترکیبی CTRL +ALT+ DELETE را فشار دهید، البتّه می‌توانید با تغییرات در سرویس Group Policy، آن را غیر فعّال کنید، اگر به شکل روبرو نگاه کنید، نام system-1\admin نوشته شده است که این کاربر admin، مربوط به کاربر Local خود کلاینت System-1 است که اگر رمز آن را وارد کنید وارد کلاینت می‌شوید، امّا به صورت Local؛ اگر بخواهید وارد دومین شوید باید بر روی Switch User کلیک کنید.



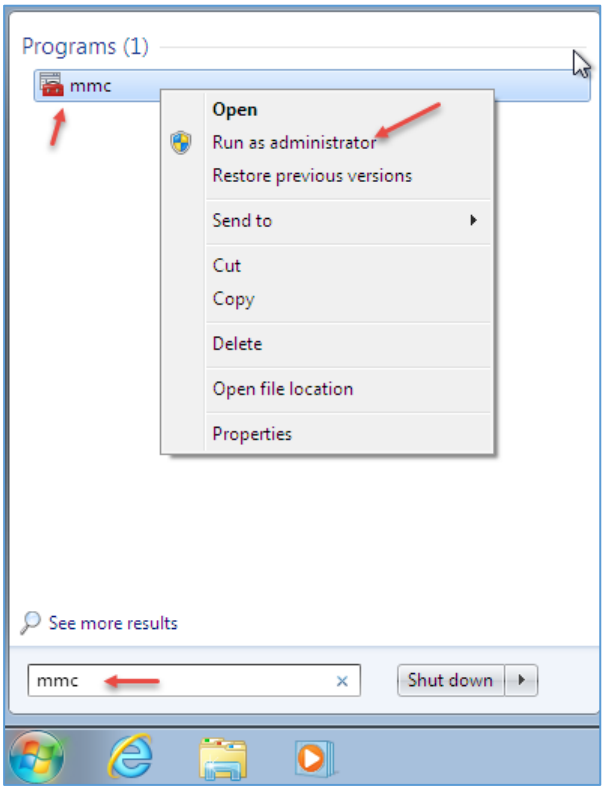
نکته: اگر چنانچه بخواهید با کاربر Local وارد کلاینتی شوید که نام آن را به خاطر نمی‌آورید، بهترین راه این است که از علامت "\." استفاده کنید، مثلاً اگر کاربر شما admin باشد، برای ورود به Local باید .\admin را وارد کنید، همانطور که مشاهده می‌کنید، نام کلاینت در جلوی Log on to نوشته شده است.

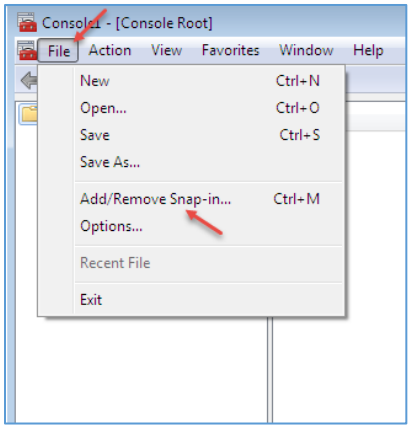


برای ورود به دومین، تنها کافی است که نام کاربری که در دومین ایجاد کردید را در شکل روبرو وارد کنید و رمز عبور مربوط به آن را نیز بنویسید؛ به قسمت Log on to توجّه کنید، نام دومین نوشته شده است.

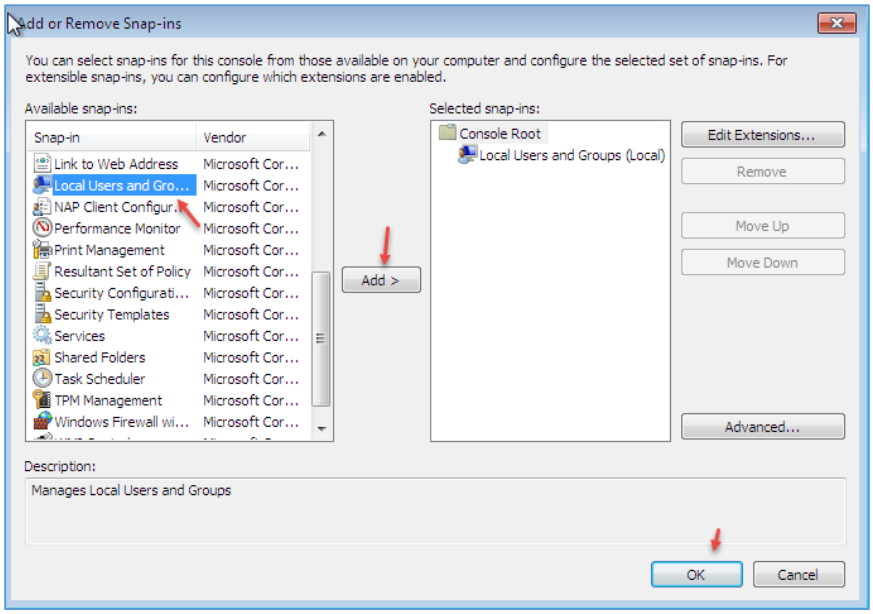


کاربر بعد از ورود می‌تواند از اطّلاعات و منابع موجود در شبکه به صورت محدود استفاده کند، کاربر دومین به صورت پیش‌فرض نمی‌تواند تغییری در کلاینت خود ایجاد کند، اگر کاربر بخواهد نرم‌افزاری نصب کند و یا آدرس IP خود را تغییر دهد، از او درخواست رمز مدیریّتی می‌شود که در شکل روبرو آن را مشاهده می‌کنید. توصیه‌ی ما این است که این روند درخواست رمز عبور را حفظ کنید تا امنیّت شبکه افزایش پیدا کند، امّا اگر بخواهید کاربر خاصّی را در سیستم او و نه در کلّ شبکه، مدیر کنید باید نام کاربری او را در گروه Administrator، داخل کلاینت Add کنید، برای این کار می‌توانید با نام کاربری Administrator وارد کلاینت شوید و کاربر را عضو گروه Administrators کنید که کمی زمان‌بر خواهد بود، بهترین حالت این است که در همان حساب کاربر مورد نظر وارد Start شوید و به مانند شکل روبرو سرویس MMC را با اولویّت کاربر Administrator اجرا کنید و در پنجره‌ی باز شده، نام کاربری ادمین را وارد کنید.

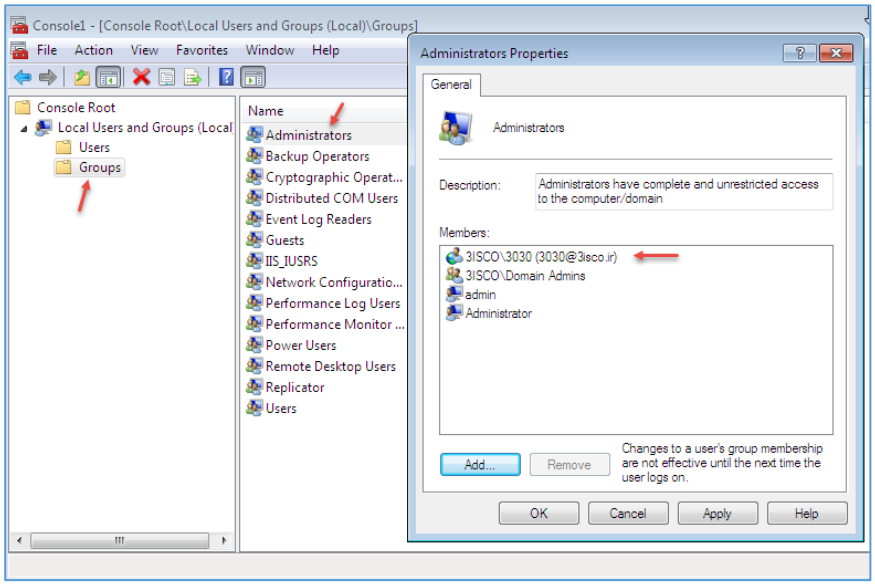




وارد منوی File شوید و گزینه‌ی Add/Remove Snap-in... را انتخاب کنید.

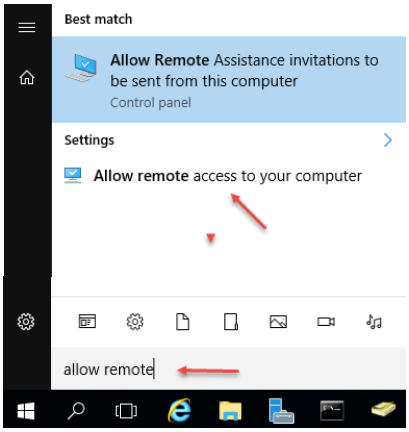


در این قسمت از لیست مورد نظر، گزینه‌ی Local Users and Groups را با کلیک بر روی Add به لیست اضافه و بر روی OK کلیک کنید.



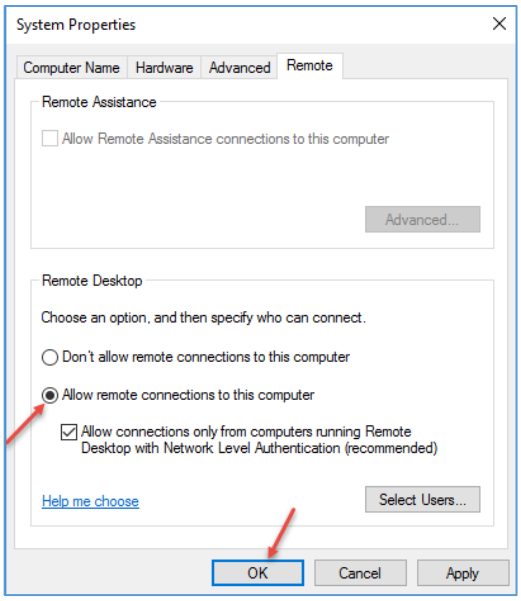
در این قسمت وارد پوشه‌ی Groups شوید و بر روی گروه Administrators، دو بار کلیک کنید و در پنجره‌ی باز شده بر روی Add کلیک کنید و کاربر مورد نظر را به لیست اضافه کنید، بعد، کلاینت را Restart کنید، بعد از این کار، کاربر مورد نظر می‌تواند تنها در آن کلاینت دسترسی کامل داشته باشد.

فعّال‌سازی Remote در سرور:



برای اینکه در هر مکانی از سازمان از طریق شبکه به سرور خود دسترسی داشته باشید باید دسترسی Remote Desktop را بر روی آن فعّال کنید.

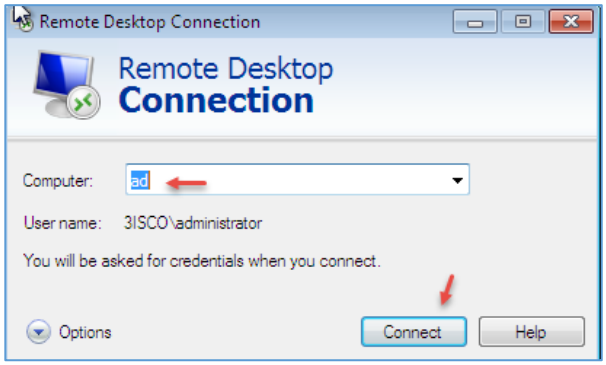
به مانند شکل روبرو در منوی Start، گزینه‌ی Allow remote access to your computer را جستجو و اجرا کنید.



در این قسمت برای دسترسی Remote، گزینه‌ی Allow remote connections to this computer را انتخاب کنید.

اگر بخواهید به کاربر خاصّی به غیر از کاربر Administrator دسترسی بدهید باید بر روی Select Users کلیک کنید و کاربر را به لیست اضافه کنید.

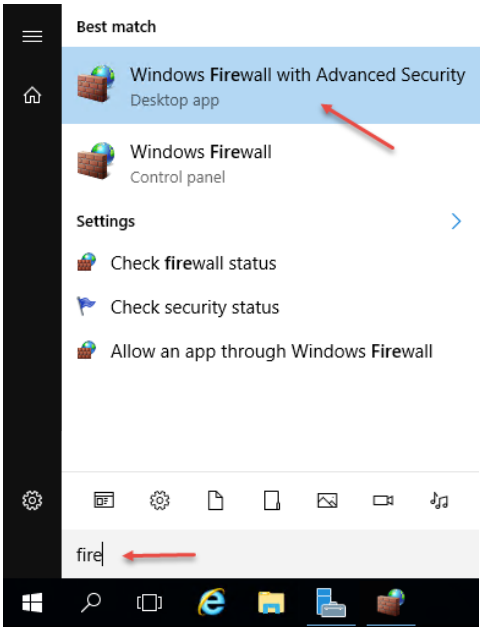
بر روی OK کلیک کنید.



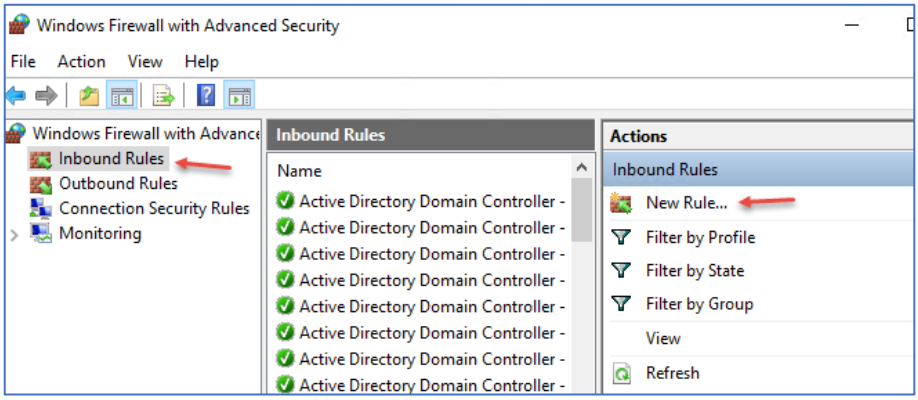
بعد از فعّال کردن Remote، شما می‌توانید با هر سیستم موجود در شبکه به سرور متّصل شوید.

اگر چنانچه نتوانستید به سرور متّصل شوید باید بررسی کنید که به سرور Ping دارید یا نه، اگر مشکلی بود باید سرویس فایروال را بررسی کنید.

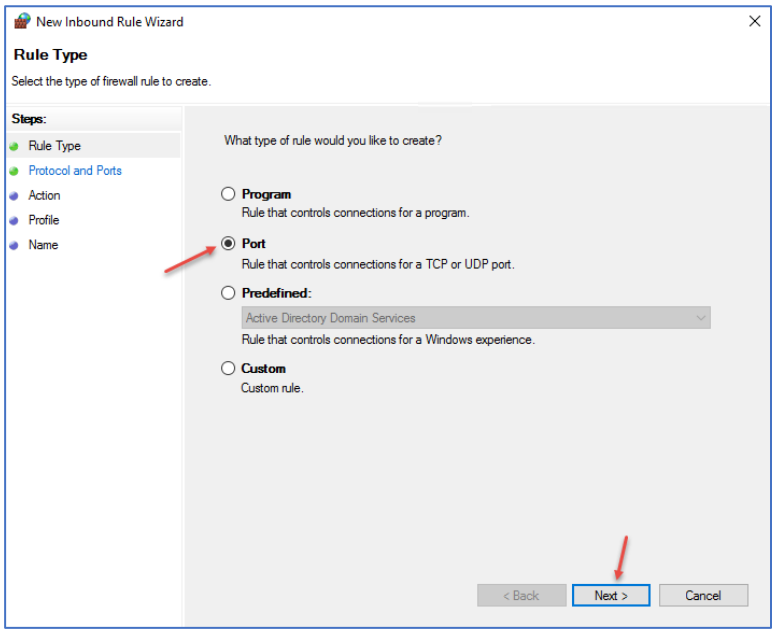
توجّه کنید که پورت پیش‌فرض Remote Desktop، شماره‌ی ۳۳۸۹ است که اگر بخواهید در فایروال به آن اجازه عبور دهید باید به مانند شکل صفحه‌ی بعد عمل کنید.



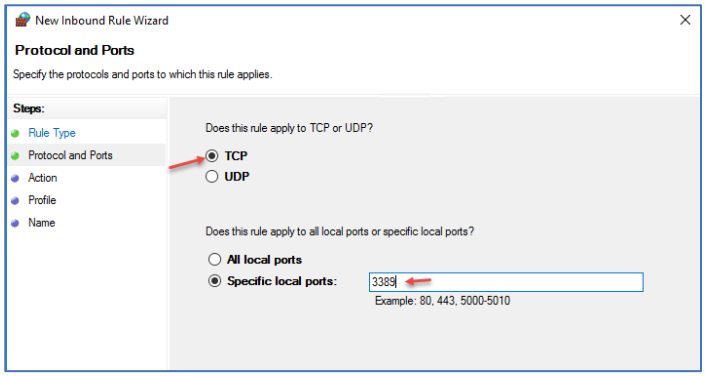
برای اجرا کردن سرویس FireWall در ویندوز سرور وارد Start شوید و به مانند شکل روبرو بر روی windows FireWall with Advanced Security کلیک کنید.



در این قسمت، دو گزینه‌ی Inbound، ورود و Outbound، خروج قرار دارد، برای اینکه بتوانید به کاربران اجازه دهید تا به این سرور، دسترسی Remote داشته باشند باید گزینه‌ی Inbound Rules را انتخاب و بر روی New Rule کلیک کنید.



در این صفحه برای اینکه دسترسی دهید باید Port مربوط به این سرویس را باز کنید، لذا گزینه‌ی Port را انتخاب و بر روی Next کلیک کنید.



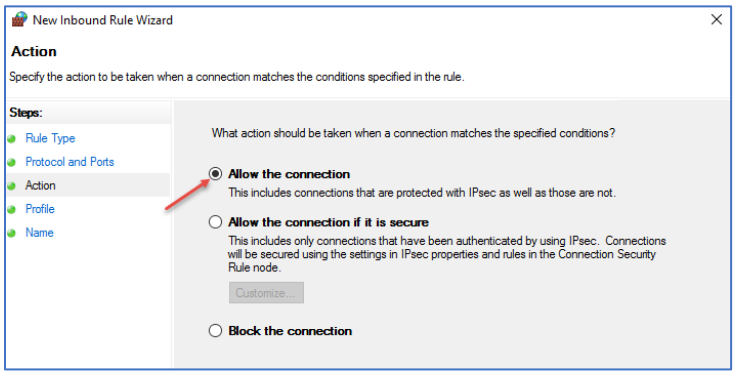
در این صفحه، پروتکل ارتباطی برای سرویس Remote Desktop را TCP در نظر می‌گیریم و شماره‌ی پورت ۳۳۸۹ را در قسمت پایین، وارد و بر روی Next کلیک می‌کنیم.

درباره‌ی TCP:

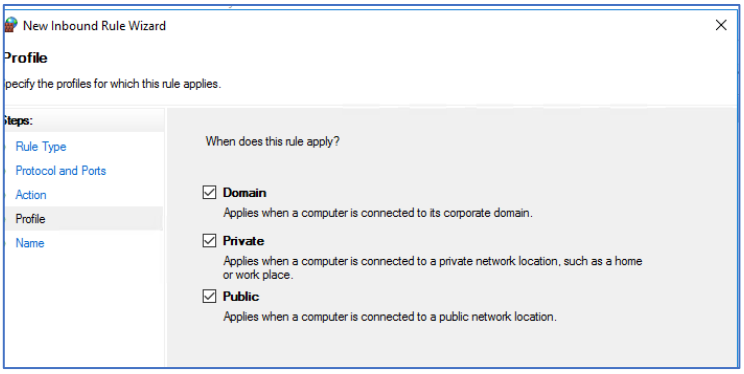
https://fa.wikipedia.org/wiki/%D9%82%D8%B1%D8%A7%D8%B1%D8%AF%D8%A7%D8%AF_%D9%87%D8%AF%D8%A7%DB%8C%D8%AA_%D8%A7%D9%86%D8%AA%D9%82%D8%A7%D9%84

درباره‌ی UDP:

https://fa.wikipedia.org/wiki/%D9%82%D8%B1%D8%A7%D8%B1%D8%AF%D8%A7%D8%AF_%D8%AF%D8%A7%D8%AF%D9%87%E2%80%8C%D9%86%DA%AF%D8%A7%D8%B1_%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1



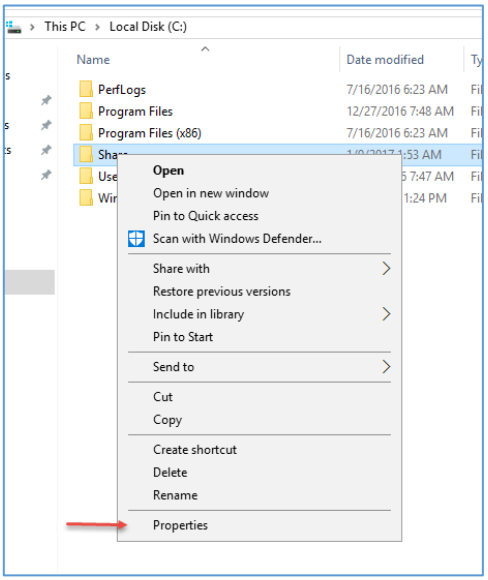
در این صفحه برای اجازه دادن به درخواست‌ها، گزینه‌ی allow the connection را انتخاب کنید، البتّه گزینه‌ی دوّم، امن‌تر است، امّا نیاز به پیش-نیازهایی دارد که فعلاً در این مرحله به آن نمی‌پردازیم، اگر گزینه‌ی آخر را انتخاب کنید دسترسی بسته خواهد شد.



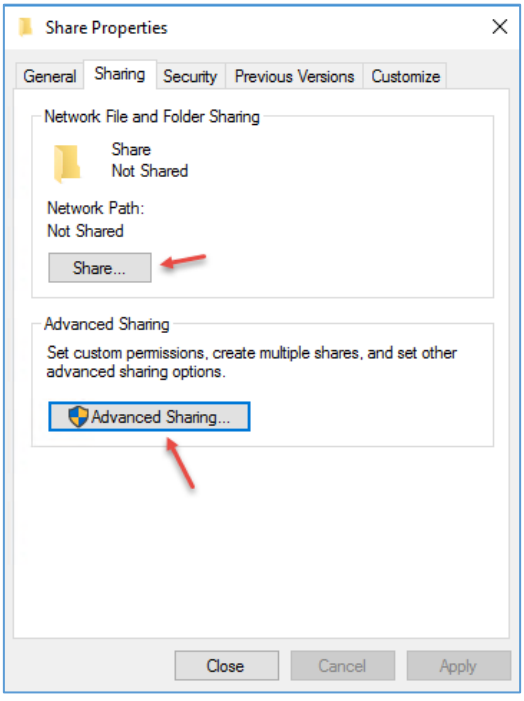
در این صفحه، حوزه‌ی فعّال بودن این Rule را مشخّص کنید، مثلاً شاید بخواهید تنها به کلاینت‌هایی که عضو دومین هستند، دسترسی دهید، پس بر روی Next کلیک کنید و در صفحه‌ی بعد، یک اسم وارد و ذخیره کنید، با این کار کاربران می‌توانند به سرور Remote بزنند.

به اشتراک‌گذاشتن فایل‌ها و فولدرها در شبکه:

یکی از مهمترین کارهایی که شبکه برای ما انجام می‌دهد، در دسترس بودن فایل‌ها و فولدرها در شبکه است، شما می‌توانید در شبکه‌ی خود، یک فایل سرور راه‌اندازی کنید و اطّلاعاتی را در آن قرار دهید و آن اطّلاعات را بنا به سطوح دسترسی در اختیار کاربران خود قرار دهید.

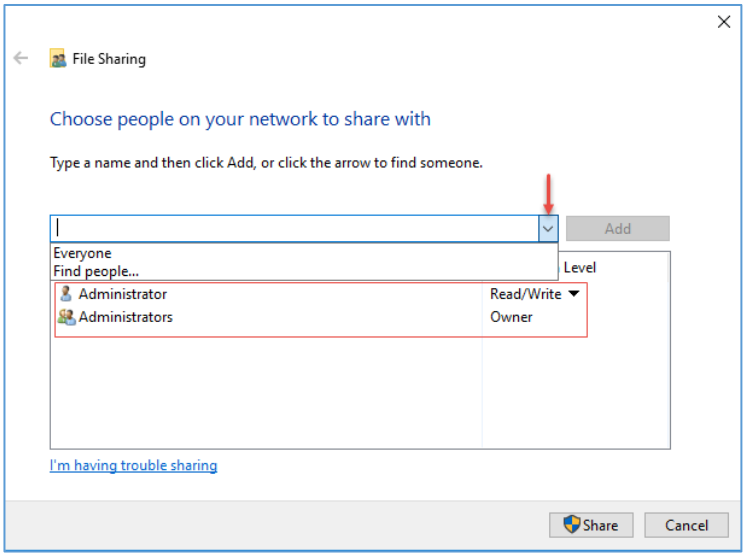


برای مثال، اگر بخواهید یک فولدر را در یک جایی از شبکه برای کاربران به اشتراک بگذارید باید به صورت روبرو بر روی پوشه‌ی مورد نظر کلیک راست کنید و گزینه‌ی Proprties را انتخاب کنید.



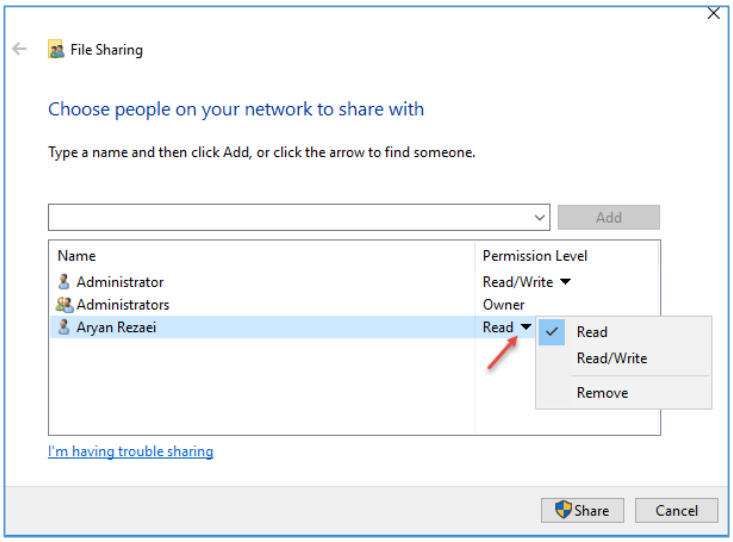
در تب Sharing، دو گزینه وجود دارد، گزینه‌ی Share برای به اشتراک‌گذاری سریع پوشه‌ی مورد نظر با همان اسم برای کاربران و گروه‌های مشخّص است و اگر بر روی گزینه‌ی Advanced Sharing کلیک کنید، می‌توانید نام فایل به اشتراک‌گذاری شده را تغییر دهید، تعداد دسترسی‌های هم‌زمان کاربران به فایل را مشخّص کنید، امنیّت را تعریف کنید و... انجام دهید.

برای اینکه این موضوع را تست بگیرید بر روی Share کلیک کنید تا شکل بعد ظاهر شود.

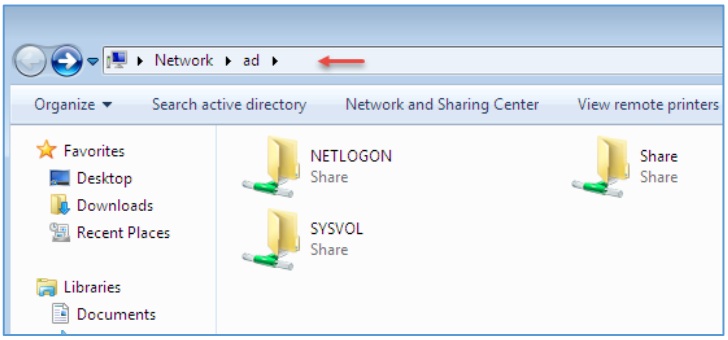


در این صفحه به صورت پیش‌فرض، نام کاربری که قرار است فایل را برای دیگران Share کند در لیست قرار دارد، یعنی کاربری که فایل خود را Share می‌کند، می‌تواند به اطّلاعات خود دسترسی داشته باشد که این موضوع درستی است، امّا اگر بخواهید این پوشه را برای فرد خاصّی به اشتراک بگذارید باید بر روی منوی کشویی کلیک کنید و بعد از آن بر روی گزینه‌ی Find people کلیک کنید.

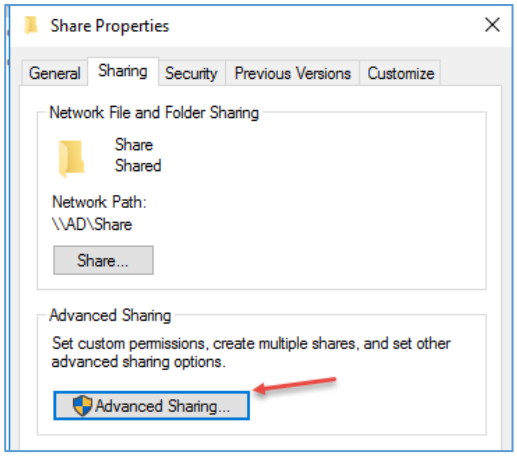
توجّه داشته باشید اگر بخواهید فایل را برای همه‌ی کاربران به اشتراک بگذارید باید گزینه‌ی Everyone را به لیست اضافه کنید.



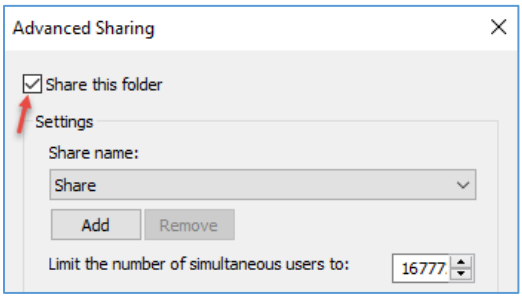
در این قسمت کاربر مورد نظر را به لیست اضافه کردیم، اگر بر روی share کلیک کنید، تنها کاربر می‌تواند به داده‌های داخل فولدر Share دسترسی داشته باشد و نمی‌تواند فایلی در آن قرار دهد، برای اینکه کاربر بتواند فایلی در آن قرار دهد باید به مانند شکل، منوی کشویی جلوی کاربر را باز کنید و گزینه‌ی Read را برای آن فعّال کنید.



بعد از اینکه فولدر مورد نظر را Share کردید، برای دسترسی به آن باید در کلاینت مورد نظر در Address bar، آدرس \\10.20.30.2 یا \\AD را وارد کنید که باید به جای نام و یا آدرس IP، آدرس سرور خود را وارد کنید، در شکل روبرو فولدر Share را مشاهده می‌کنید.

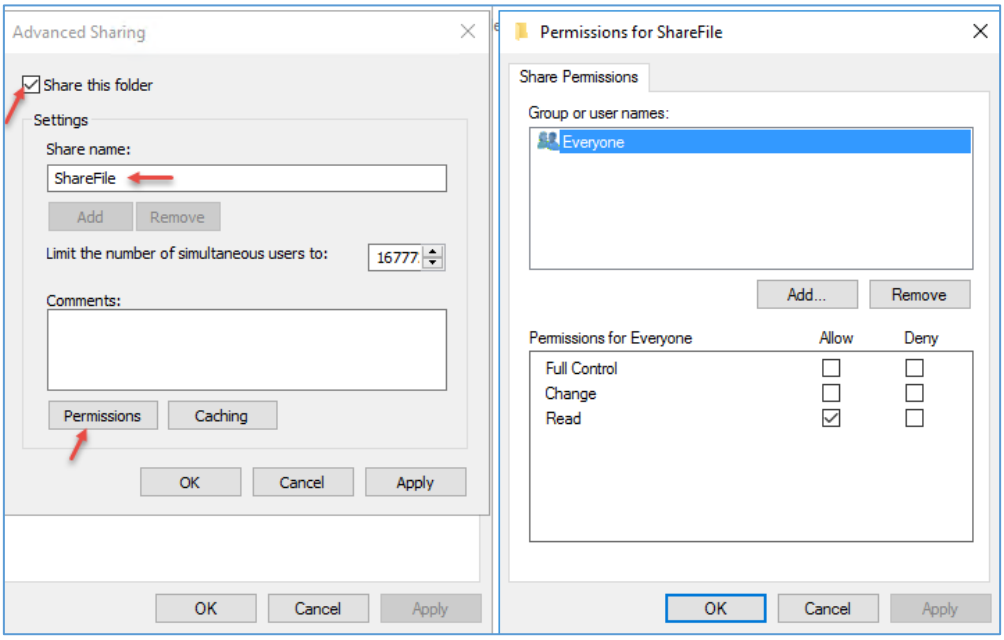


گزینه‌ی دیگر، Advanced Sharing است که تنظیمات بیشتری را در اختیار شما قرار می‌دهد.

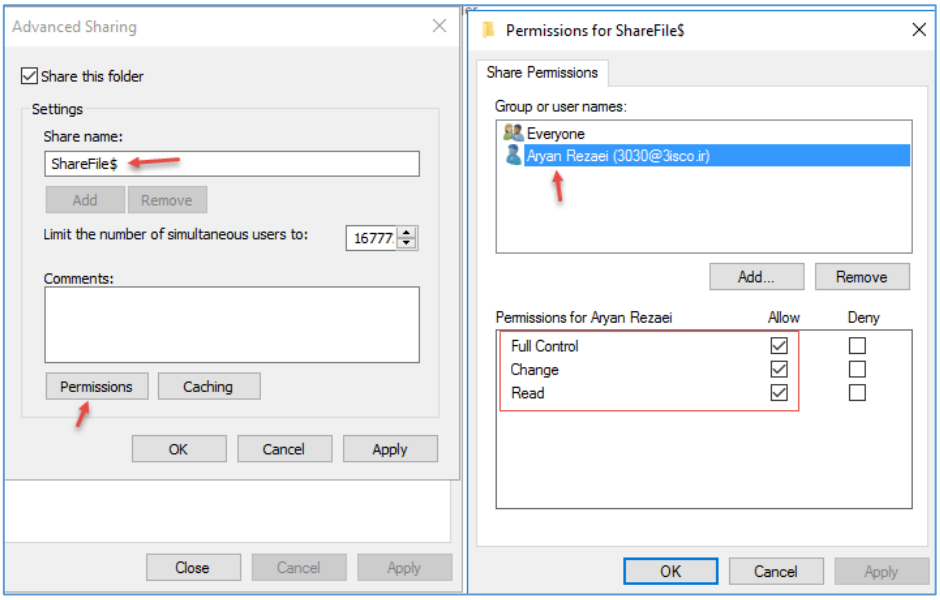


در این قسمت برای اینکه فولدر share شده‌ی قبلی را متوقّف کنید، تیک گزینه‌ی share this folder را بردارید و بر روی OK کلیک کنید، با این کار، اشتراک فولدر مورد نظر با کاربر قطع خواهد شد.

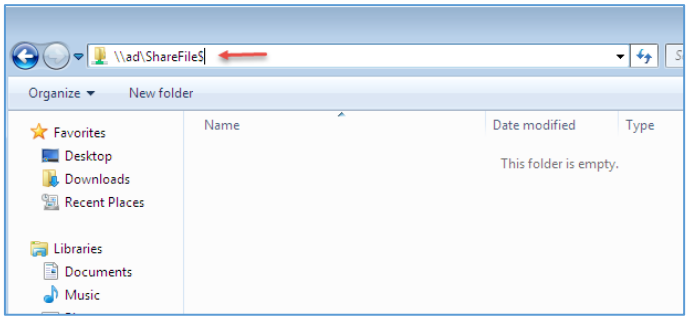
بعد از این کار، دوباره بر روی Advanced Sharing کلیک کنید.



در این قسمت برای اشتراک-گذاری باید تیک گزینه‌ی share this folder را انتخاب کنید و در قسمت share Name، نام اشتراکی فولدر خود را به دلخواه وارد کنید، توجّه داشته باشید این نام، هیچ ارتباطی با فولدر اصلی ندارد، عدد ۱۶۷۷۷ نیز تعداد هم‌زمان کاربرانی است که می‌توانند به این فولدر دسترسی داشته باشند که شما می‌توانید این تعداد را تغییر دهید، اگر بر روی Permissions کلیک کنید، پنجره‌ی دوّم نمایش داده می‌شود که می‌توانید به کاربران دسترسی بدهید، توجّه داشته باشید گروه Everyone در این حالت به صورت پیش‌فرض دسترسی دارند.

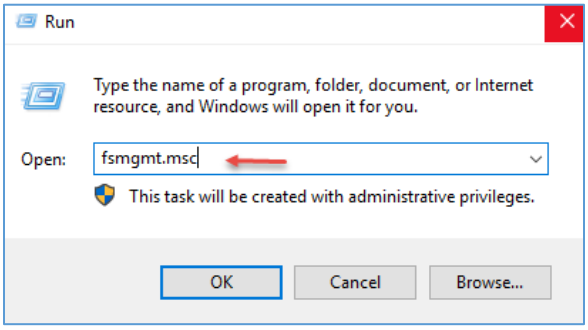


برای اینکه یک فولدر را به صورت مخفی برای کاربر خاصّی به اشتراک بگذارید باید در قسمت share Name، نام فولدر را با علامت $ وارد کنید و دسترسی لازم را به کاربر مورد نظر دهید، اگر به مانند شکل روبرو تیک گزینه‌ی Full Control را انتخاب کنید، کاربر ۳۰۳۰ به فولدر share به طور کامل دسترسی خواهد داشت.



برای باز کردن فایل مورد نظر نیز باید به مانند شکل روبرو عمل کنید و آدرس فایل را با علامت $ وارد کنید.

حال اگر بخواهید در یک سرور یا کلاینتی، فایل‌های مخفی Share شده‌ی آن را پیدا کنید باید چه کاری انجام دهید؟

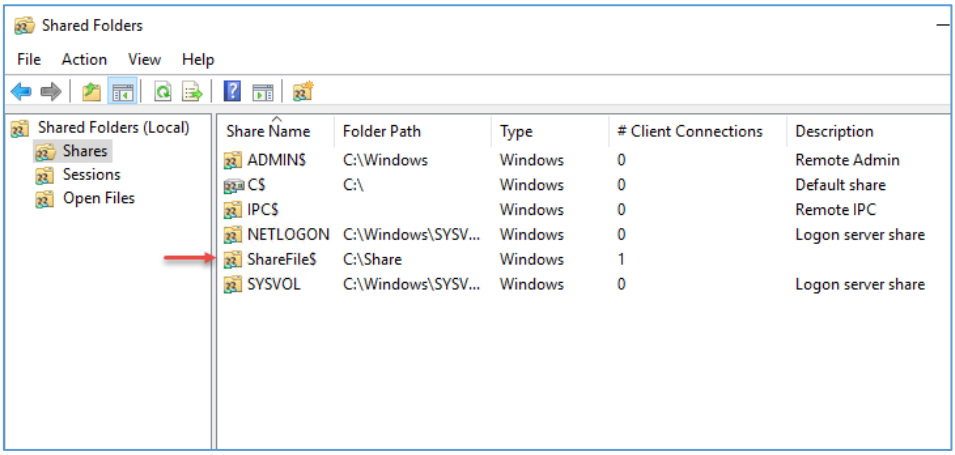


برای این کار باید سرویس Share Folder را اجرا کنید تا همه‌ی اشتراک‌گذاری‌ها را مشاهده کنید، برای اجرای این سرویس، تنها کافی است در Run، دستور fsmgmt.msc را اجرا کنید، البتّه می‌توانستید دستور MMC را اجرا کنید تا کنسول مدیریّتی باز شود و بعد، از منوی File بر روی Add کلیک و این سرویس را به لیست اضافه می‌کردید، البتّه این روش کمی وقت‌گیر است، لذا در صفحه‌ی بعد برای شما جدولی را آماده کردیم که برای دسترسی به سرویس‌های مدیریّتی، دستور سریع آن را قرار دادیم که خیلی می‌تواند در سرعت عمل شما کارایی داشته باشد.

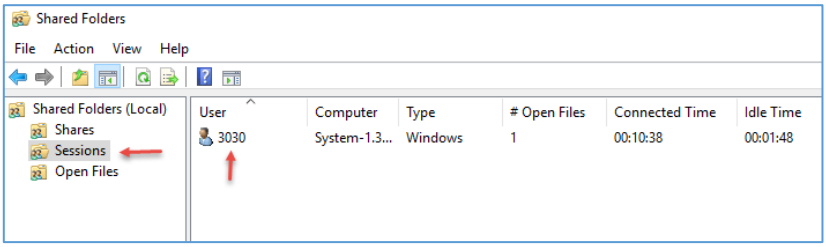
جدول دستورات سریع برای اجرای سرویس‌های مدیریّتی:

سرویس	دستور
AD Domains and Trusts	domain.msc
Active Directory Management	admgmt.msc
AD Sites and Services	dssite.msc
AD Users and Computers	dsa.msc
ADSI Edit	adsiedit.msc
Authorization manager	azman.msc
Certification Authority Management	certsrv.msc
Certificate Templates	certtmpl.msc
Cluster Administrator	cluadmin.exe
Computer Management	compmgmt.msc
Component Services	comexp.msc
Configure Your Server	cys.exe
Device Manager	devmgmt.msc
DHCP Management	dhcpmgmt.msc
Disk Defragmenter	dfrg.msc
Disk Manager	diskmgmt.msc
Distributed File System	dfsgui.msc
DNS Management	dnsmgmt.msc
Event Viewer	eventvwr.msc
Indexing Service Management	ciadv.msc
IP Address Manage	ipaddrmgmt.msc
Licensing Manager	llsmgr.exe
Local Certificates Management	certmgr.msc
Local Group Policy Editor	gpedit.msc
Local Security Settings Manager	secpol.msc
Local Users and Groups Manager	lusrmgr.msc
Network Load balancing	nlbmgr.exe
Performance Monitor	perfmon.msc
PKI Viewer	pkiview.msc
Public Key Management	pkmgmt.msc
Quality of Service Control Management	acssnap.msc
Remote Desktop	tsmmc.msc
Remote Storage Administration	rsadmin.msc
Removable Storage	ntmsmgr.msc
Removable Storage Operator Requests	ntmsoprq.msc
Routing and Remote Access Manager	rrasmgmt.msc

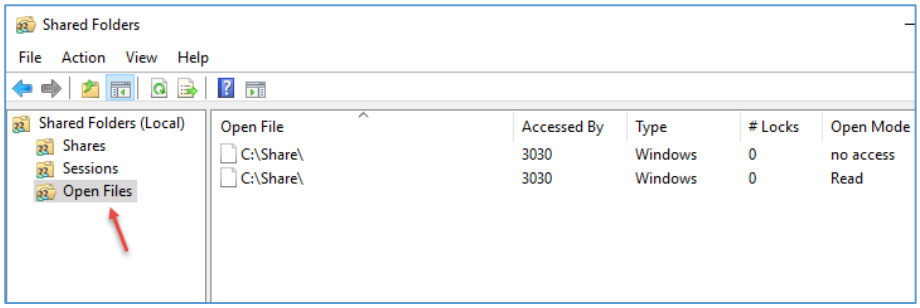
rsop.msc	Resultant Set of Policy
schmmgmt.msc	Schema management
services.msc	Services Management
fsmgmt.msc	Shared Folders
sidwalk.msc	SID Security Migration
tapimgmt.msc	Telephony Management
tscc.msc	Terminal Server Configuration
licmgr.exe	Terminal Server Licensing
tsadmin.exe	Terminal Server Manager
MSTSC	Teminal Services RDP
mstsc /v:[server] /console	Teminal Services RDP to Console
uddi.msc	UDDI Services Managment
wmimgmt.msc	Windows Mangement Instumentation
winsmgmt.msc	WINS Server manager



سرویس Share Folders را در شکل روبرو مشاهده می‌کنید که از سه قسمت تشکیل شده است، در قسمت Shares، تمام فولدرهای به اشتراک گذاشته شده، چه به صورت مخفی و چه به صورت غیر مخفی را مشاهده می‌کنید، برای اینکه فولدر Share شده را از دسترسی خارج کنید، می‌توانید بر روی فولدر مورد نظر کلیک راست کنید و گزینه‌ی Stop sharing را انتخاب کنید.



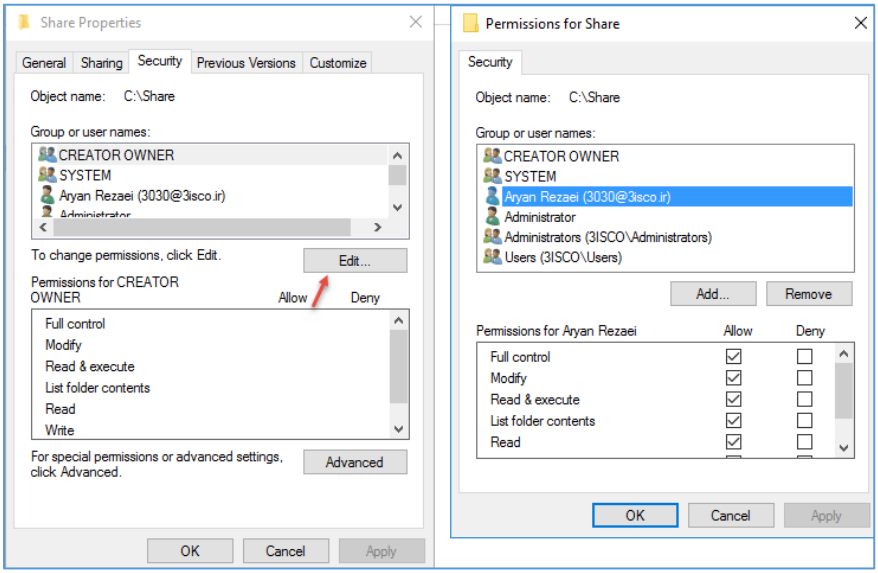
در قسمت Sessions، می‌توانید کاربرانی که از منابع Share شده در سرور استفاده می‌کنند را ببینید و اگر از آن خوشتان نیامد می‌توانید با کلیک راست بر روی آن و انتخاب Close Session، ارتباط آن را در همان لحظه قطع کنید، البتّه کاربر با یک Refresh می‌تواند Session یا جلسه‌ی دیگری را آغاز کند.



در قسمت Open File، فولدرهای باز شده توسط کاربر را می‌توانید مشاهده کنید و آنها را ببندید.

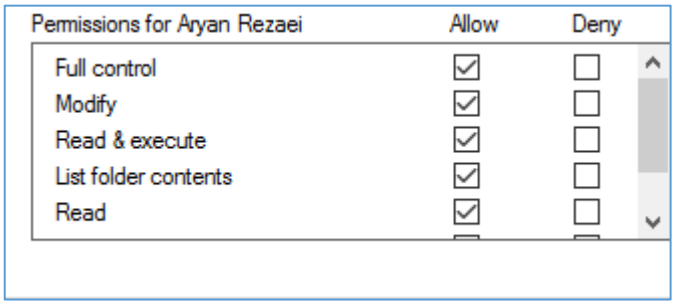
بررسی دسترسی‌ها به فولدرها و فایل‌ها:

با استفاده از Permission ها می‌توانید به کاربران خود دسترسی دهید تا تنها بتوانند یک فایل را بخوانند یا آن را ویرایش کنند و کارهای دیگری روی آن انجام دهند، در مرحله‌ی قبل این موضوع مورد بررسی قرار گرفت و یک فولدر را برای کاربری با دسترسی مشخّص به اشتراک گذاشتیم، در این قسمت می‌خواهیم کمی بیشتر با دسترسی‌ها کار کنیم.



اگر فولدری را به اشتراک گذاشته باشید و وارد تب Security شوید، دسترسی‌هایی که برای آن فولدر مشخّص شده است را مشاهده می‌کنید.

اگر بر روی Edit کلیک کنید، تمام Permission های تخصیص داده شده به کاربر یا گروه مورد نظر را می‌توانید مشاهده کنید.



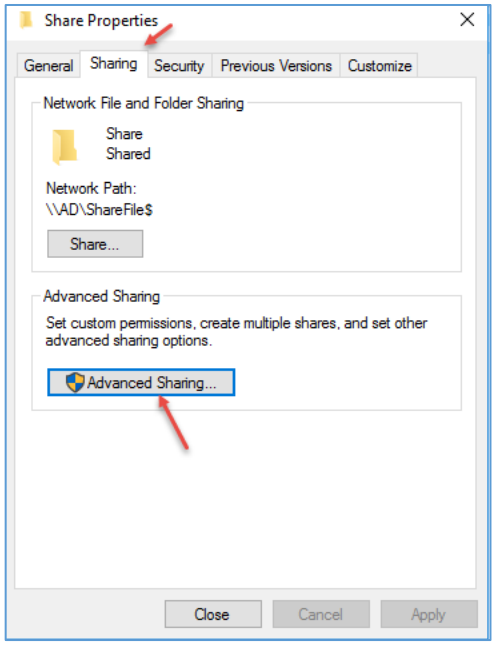
در قسمت Permissions for...، گزینه‌های مختلفی وجود دارد که در جدول صفحه‌ی بعد آنها را بررسی خواهیم کرد.

دسترسی‌ها	تأثیر آن بر روی پوشه	تأثیر آن بر روی فایل
Read	اجازه دارد تا فایل‌ها و پوشه‌ها را مشاهده کند.	اجازه‌ی مشاهده و دسترسی به محتویّات فایل را دارد.
Write	اجازه دارد تا فایل و پوشه‌ای را اضافه کند.	دسترسی دارد تا اطّلاعات را در فایل وارد کند.
Read & Execute	مشاهده‌ی فایل‌ها و پوشه‌ها و اجرای فایل‌ها و پوشه‌هایی که از بالا دستی خود ارث‌بری کرده اند.	دسترسی و مشاهده‌ی محتویّات فایل و اجرای فایل.
List Folder Contents	مشاهده‌ی فایل‌ها و پوشه‌ها و اجرای فایل‌هایی که از پوشه‌ی بالا دستی خود ارث‌بری کرده‌اند.	تأثیری ندارد.
Modify	اجازه‌ی خواندن و نوشتن فایل‌ها و پوشه‌ها و اجازه‌ی حذف فایل مورد نظر را دارد.	اجازه‌ی خواندن و نوشتن فایل‌ها و پوشه‌ها و اجازه‌ی حذف فایل مورد نظر را دارد.
Full Control	اجازه‌ی خواندن، نوشتن، تغییر دادن و حذف کردن پوشه را دارد.	اجازه‌ی خواندن، نوشتن، تغییر دادن و حذف کردن فایل را دارد.

طبق جدول بالا شما می‌توانید نیازهای خود را انتخاب کنید، باید در دادن دسترسی‌ها دقّت کنید تا در ادامه با مشکلی مواجه نشوید.

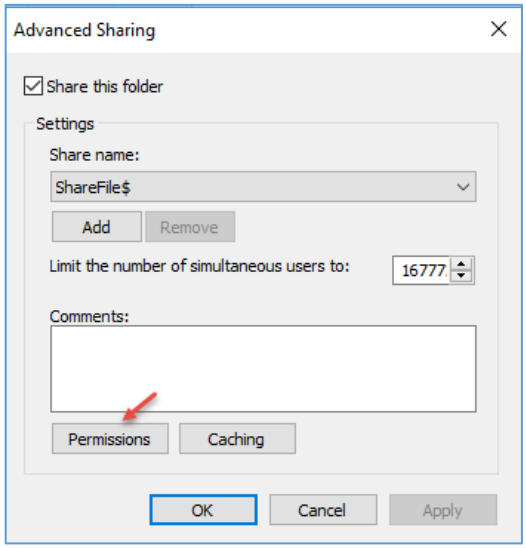
یک نکته‌ی مهم:

اگر به طور هم‌زمان، شما به کاربر مورد نظر در تب Sharing دسترسی دهید و همین کار را در تب Security انجام دهید، اولویّت کار با تب Sharing خواهد بود، این عمل را با هم تست می‌کنیم.

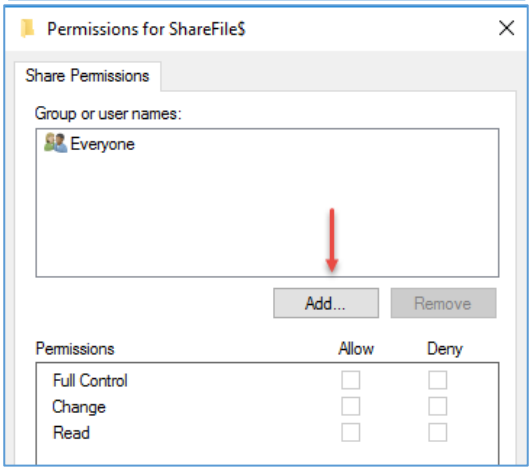


در تب Sharing بر روی Advanced Sharing کلیک کنید.

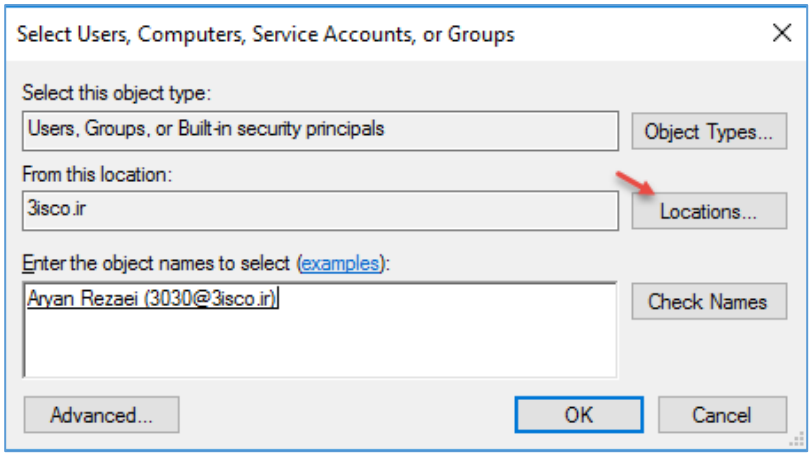
بر روی Share نیزمی‌توانید کلیک کنید و این کار را انجام دهید.



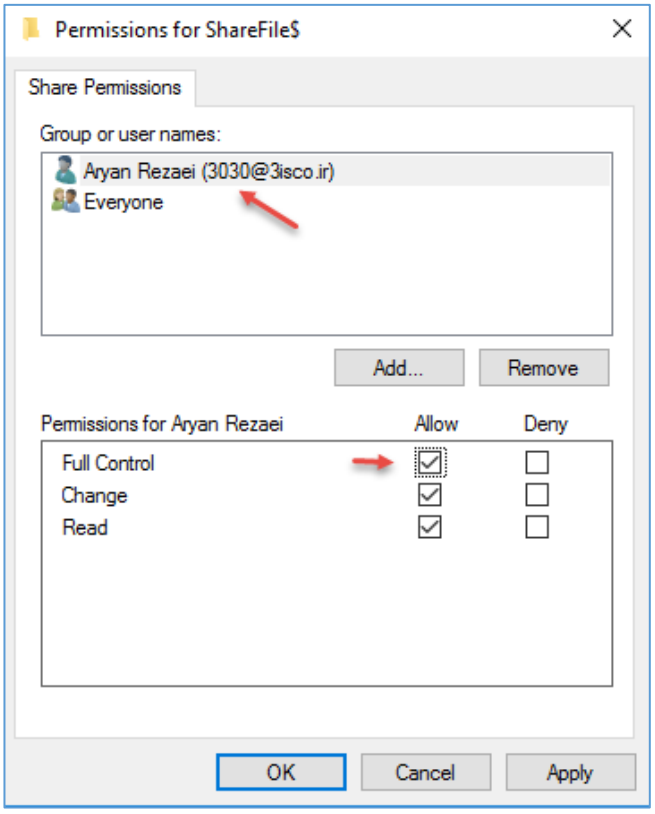
در این قسمت که از قبل، فایل مورد نظر را Share کرده بودیم، بر روی Permissions کلیک می‌کنیم تا دسترسی را بررسی کنیم.



در این صفحه بر روی Add کلیک کنید تا کاربر مورد نظر را به لیست اضافه کنید.

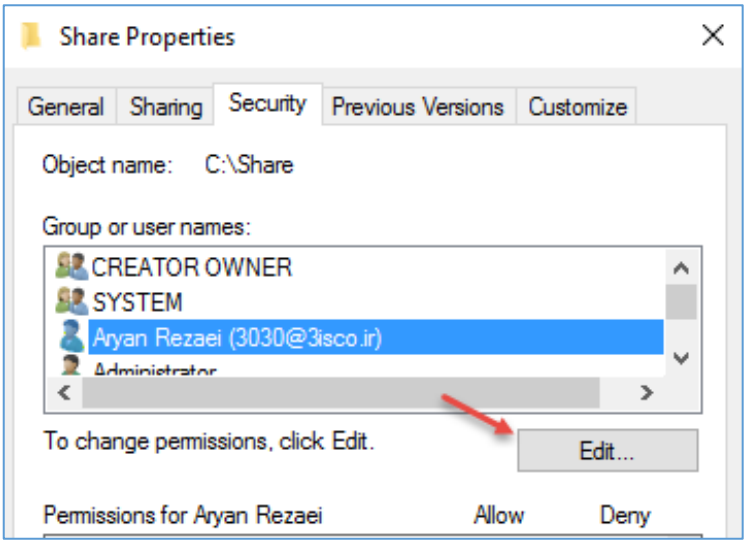


در صفحه‌ی اوّل باید Location شما بر روی دومین قرار داشته باشد تا بتوانید کاربران دومین خود را انتخاب کنید، برای این کار باید بر روی Location کلیک کنید، نام کاربری کاربر مورد نظر خود را وارد و بر روی OK کلیک کنید، اگر نام کاربری کاربر مورد نظر خود را نمی‌دانید باید بر روی Advanced کلیک و در صفحه‌ی باز شده بر روی Find New کلیک کنید و از لیست، کاربر مورد نظر خود را انتخاب و بر روی OK کلیک کنید.

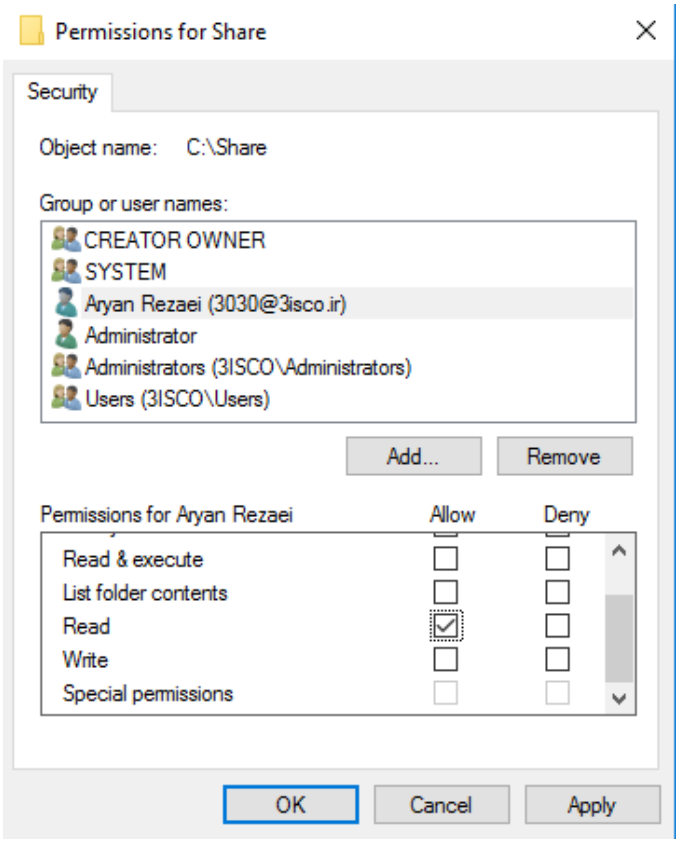


در این قسمت، کاربر ۳۰۳۰ به لیست اضافه شده است که در قسمت Permissions، دسترسی Full Control به او دادیم، با این کار، کاربر می‌تواند در فولدر Share، بنویسد، بخواند، تغییر دهد و آن را حذف کند.

اگر به لیست توجّه کنید، گروه Everyone نیز در لیست وجود دارد، این بدان معناست که تمام کاربران دومین می‌توانند به این فایل دسترسی داشته باشند که اگر این قانون را قبول ندارید، می‌توانید آن را از لیست حذف کنید.



حال اگر در همان پوشه وارد تب **Security** شوید و بر روی **Edit** کلیک کنید، می‌توانید این تغییرات را بررسی کنید.

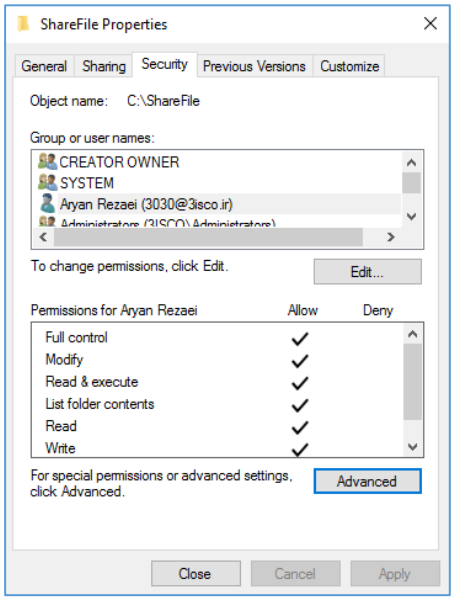


در این صفحه، کاربر مورد نظر خود را از لیست انتخاب و دسترسی‌های آن را به **Read** محدود کنید.

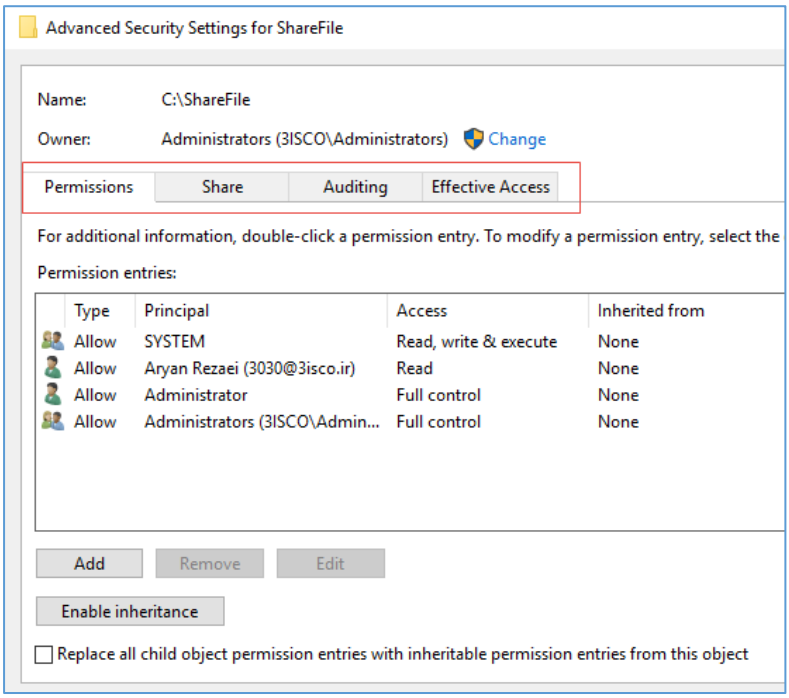
اگر کاربر مورد نظر (۳۰۳۰) وارد فولدر **Share** شود، **Full control** دسترسی خواهد داشت، چون اولویّت تب **Sharing** از تب **Security** بالاتر خواهد بود.

در کل، تب **Security** بر روی همان سرور کار خواهد کرد و تب **Sharing** برای دسترسی از راه دور کاربرد دارد.

بررسی گزینه‌ی Advanced در تب Security:

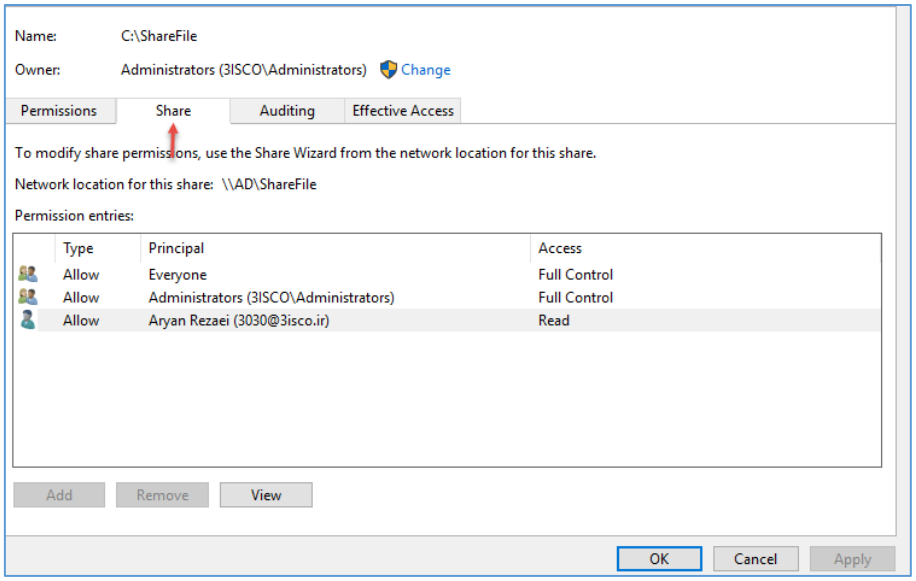


گزینه‌ای به نام Advanced در تب Security قرار دارد که تنظیمات و ویژگی‌های بیشتری را در اختیار ما قرار می‌دهد؛ برای بررسی، بر روی Advanced کلیک کنید تا شکل بعد ظاهر شود.

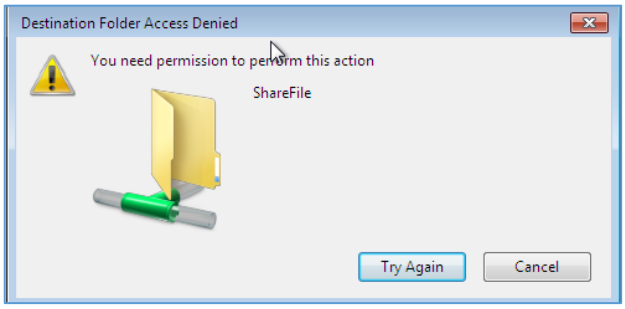


در این صفحه، ٤ تب وجود دارد که در تب Permissions، تمام دسترسی‌های کاربران و گروه‌ها به فولدر و یا فایل مورد نظر مشخّص شده است، در تب Share نیز می‌توانید ببینید که این فایل یا فولدر برای چه کسی به اشتراک گذاشته شده است.

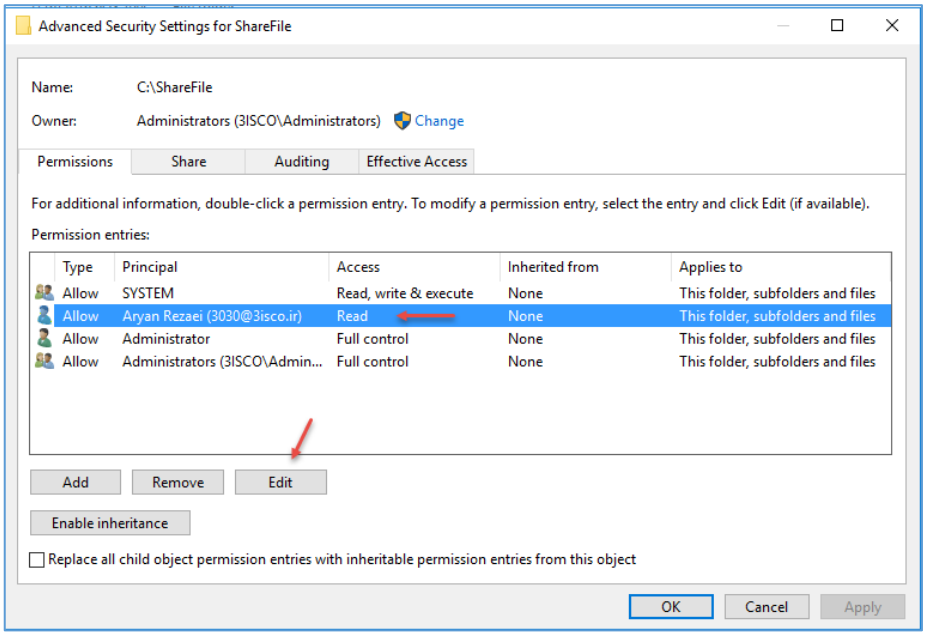
در تب Auditing یا حسابرسی می‌توانید یک کاربری را مشخّص کنید که به فایل‌هایی که دسترسی ندارد، وارد شود و آنها را بررسی کند، زمانی پیش می‌آید که کاربری، دسترسی یک فایل را برای شخص خاصّی محدود کرده است، امّا مدیر شبکه می‌خواهد محتویّات آن فایل را بررسی کند که با این روش می‌تواند این کار را انجام دهد، در ادامه این موضوع را بررسی خواهیم کرد.



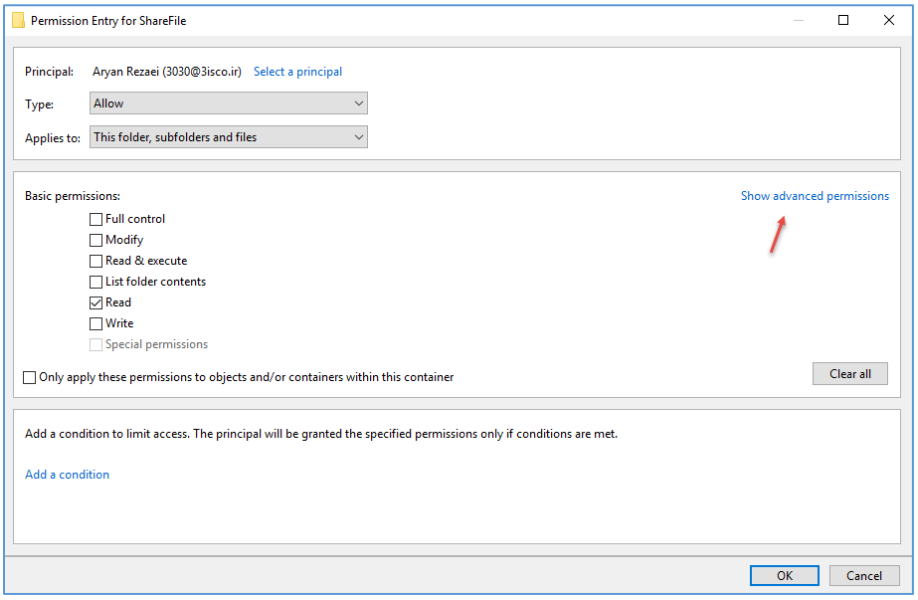
اگر به تب **Share** توجّه کنید، کاربر ۳۰۳۰ با دسترسی **Read** به فایل **ShareFile** دسترسی دارد و تنها می‌تواند فایل مورد نظر را بخواند و نمی‌تواند چیزی را تغییر دهد و یا به آن اضافه کند.



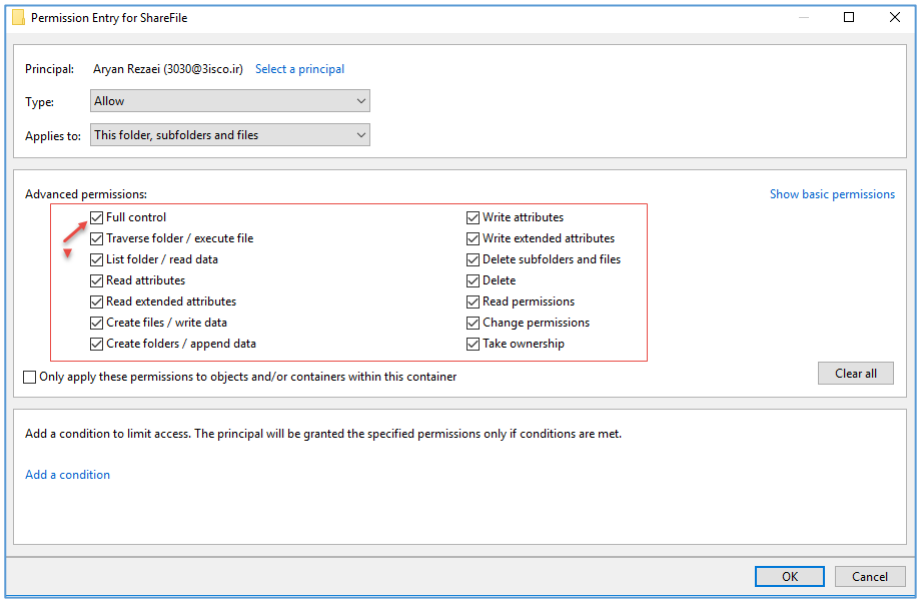
در شکل روبرو کاربر قصد داشت تا فولدری را در پوشه‌ی **ShareFile** ایجاد کند، امّا اجازه‌ی کار به او داده نشده و با اخطار روبرو مواجه شده است که دسترسی لازم به فایل را ندارد.



اگر وارد تب **Permissions** شوید، می‌توانید این دسترسی‌ها را تغییر دهید، کاربر مورد نظر را انتخاب و بر روی **Edit** کلیک کنید، اگر کاربر در لیست نیست، می‌توانید با کلیک بر روی **Add**، آن را به لیست اضافه کنید.



در این صفحه، می‌توانید دسترسی‌های خود را مشخّص کنید، اگر چنانچه بخواهید تنظیمات بیشتری از دسترسی‌ها را مشاهده کنید باید به مانند شکل بر روی Show advanced Permissions کلیک کنید.

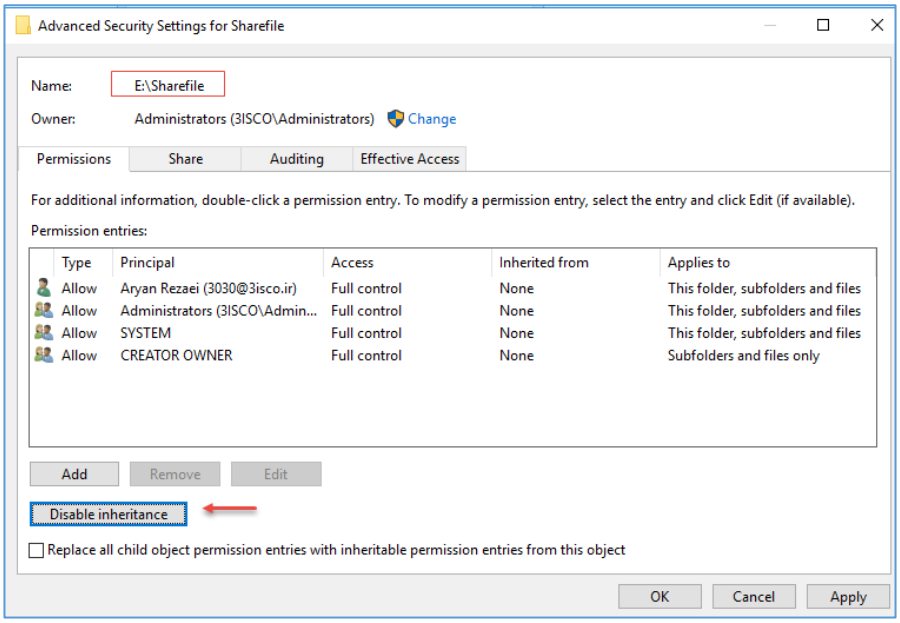


در این صفحه، همه‌ی دسترسی‌ها را مشاهده می‌کنید که می‌توانید همه یا چند گزینه‌ی مشخّص را برای کاربر مورد نظر انتخاب کنید، در این قسمت، Full Control را انتخاب کنید.

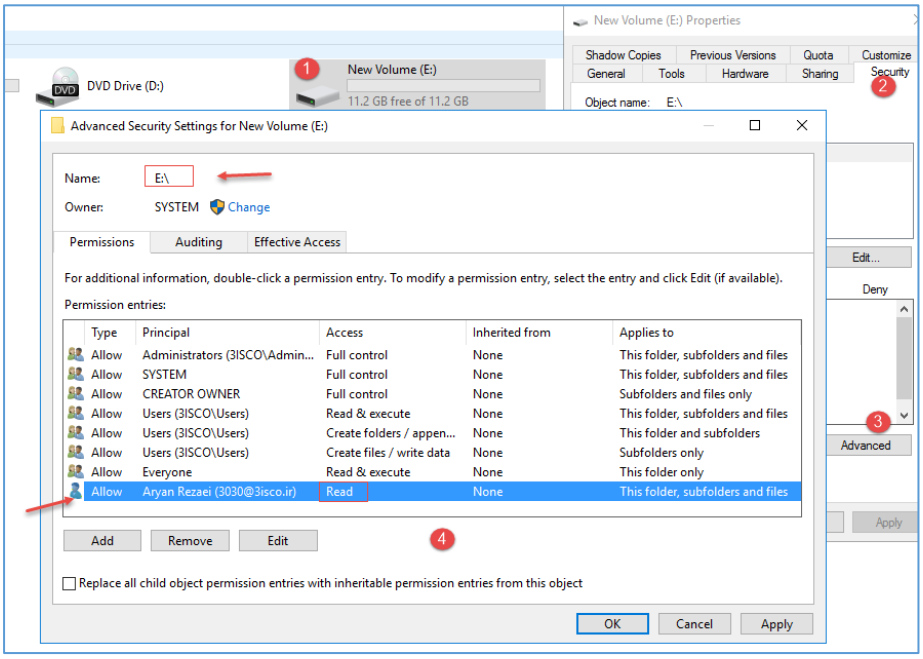
با این کار، کاربر مورد نظر بدون هیچ مشکلی می‌تواند به فایل فولدر مورد نظر دسترسی داشته باشد و تغییرات خود را در آن اعمال کند.

بررسی Inheritance در Permissions:

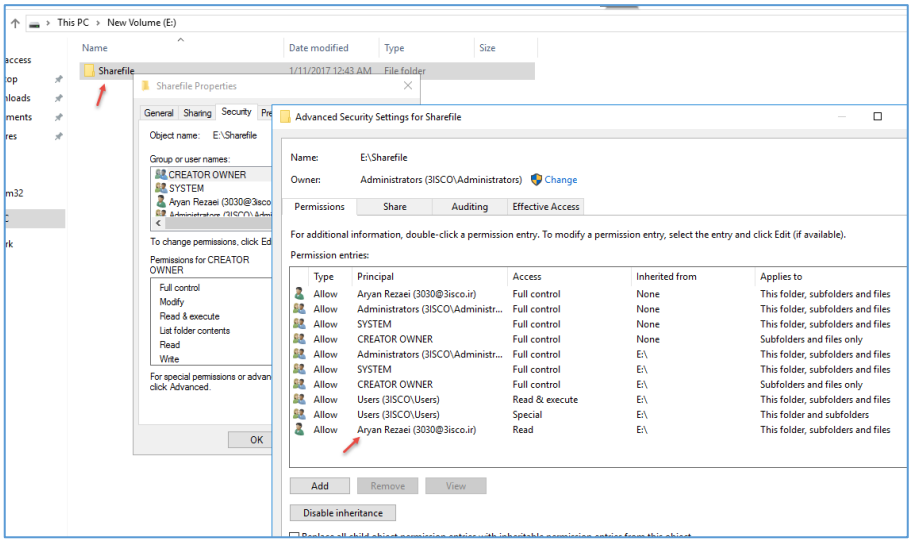
Inheritance یا همان ارثبری ویژگی‌ای در Permissions است که اگر فعّال باشد، دسترسی‌هایی را که برای کاربران و گروه‌ها تعریف کردید را می‌تواند تحت تأثیر خود قرار دهد، با هم یک نمونه را تست می‌گیریم تا با این ویژگی بیشتر آشنا شویم.



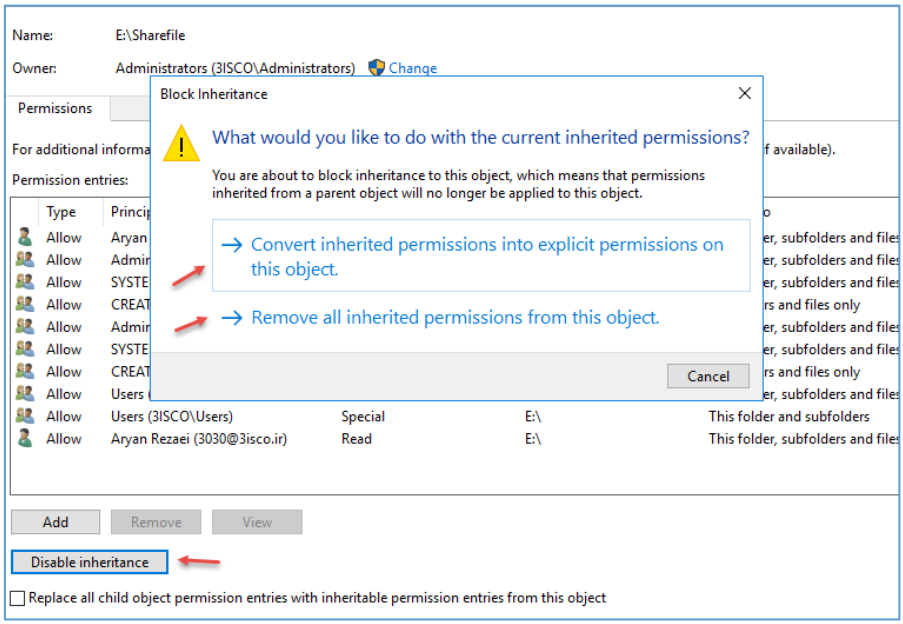
در شکل روبرو وارد تنظیمات Security فولدر ShareFile شدیم، برای اینکه متوجّه شویم که تنظیمات ارث‌بری این فولدر فعّال است یا نه باید گزینه‌ی Disable inheritance را مشاهده کنیم که این گزینه، نشان دهنده‌ی این است که ارث‌بری برای این پوشه فعّال است و از بالا سری خود تنظیمات دسترسی را دریافت می‌کند، برای تست این موضوع در لیست روبرو کاربر ۳۰۳۰ را به اضافه کردیم و به او دسترسی Full control دادیم، اگر این تنظیمات اوکی شود، کاربر مورد نظر به پوشه‌ی ShareFile دسترسی کامل دارد، امّا اگر پوشه‌ی بالا دستی یا درایو بالا، به صورت دستی تنظیمات خود را ست کند، این ویژگی از کار خواهد افتاد.



در این صفحه بر روی درایو مورد نظر که پوشه‌ی ShareFile درآن قرار دارد، کلیک راست کردیم و وارد Advanced Security شدیم، در قسمت شماره‌ی چهار، کاربر 3030 را به لیست اضافه کردیم و دسترسی Read را به او دادیم، اگر وارد تنظیمات Permission مربوط به پوشه‌ی Sharefile شوید، این موضوع را مشاهده خواهید کرد.

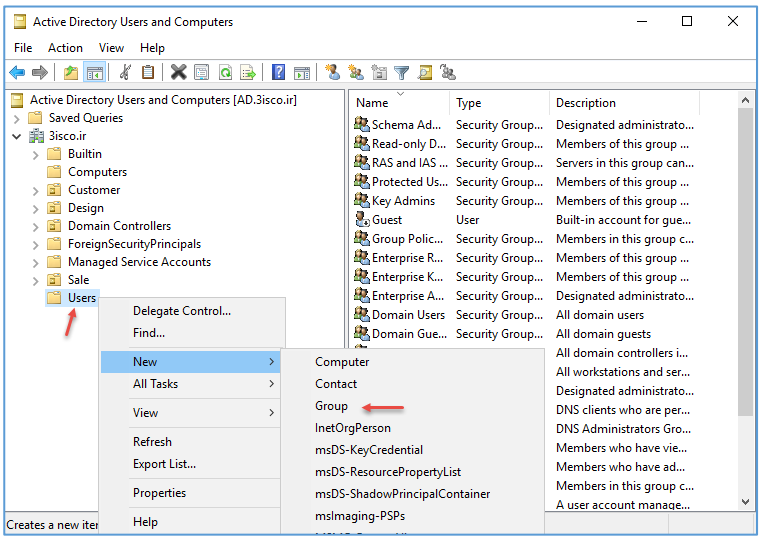


این صفحه، مربوط به تنظیمات Permission فولدر ShareFile است، اگر به لیست دقّت کنید، دو کاربر هم‌نام ۳۰۳۰ وجود دارد که یکی برای خود فولدر ShareFile و دیگری برای درایو E است که در بالادستی آن قرار دارد، این گفته را می‌توانید در همین لیست در ستون Inherited from مشاهده کنید که گروه‌ها و کاربرانی که از فولدر بالادستی خود گرفته شده را مشخّص کرده است؛ با این موارد، اگر کاربر بخواهد تغییراتی در پوشه‌ی ShareFile اعمال کند با اخطار دسترسی مواجه خواهد شد.

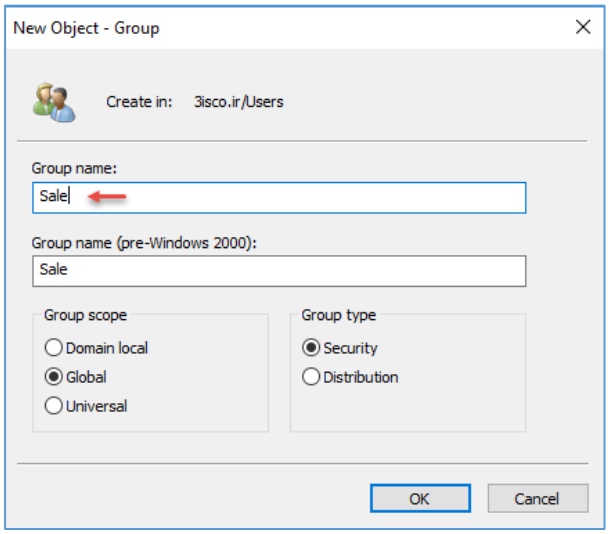


حال اگر بخواهیم این ارث‌بری را بر روی فایل حذف کنیم باید بر روی Disable inheritance کلیک کنیم که پنجره‌ی روبرو برای ما ظاهر می‌شود؛ در این پنجره، دو گزینه وجود دارد، اگر گزینه‌ی اوّل را انتخاب کنیم، ارث‌بری از بالا کلّاً قطع می‌شود، امّا گروه‌های سیستمی که خود سرور مشخّص کرده است و از بالا به ارث رسیده، برای این فولدر حفظ خواهد شد، امّا اگر بر روی گزینه‌ی Remove all inherited permissions from this object کلیک کنیم، تمام Permission هایی که از بالا دریافت شده، حذف خواهد شد.

ایجاد گروه در سرویس Active Directory Users and Computers:



گروه‌ها در Active Directory، بیشترین 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 مورد نظر کلیک می‌کنیم.

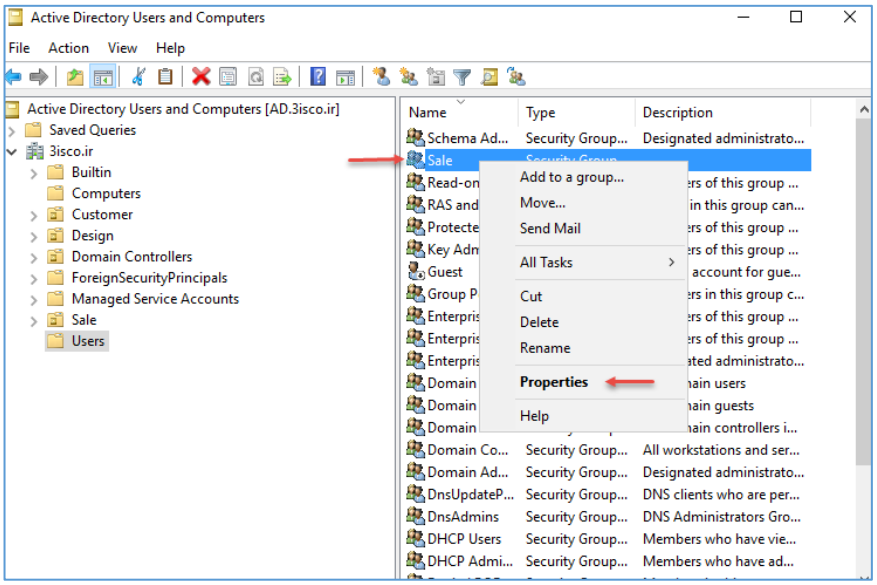


در این صفحه، در قسمت Group name، نام گروه را وارد می‌کنیم؛ گروه‌ها اصولاً از تقسیمات Group Scope و Group type استفاده می‌کنند که با هم این گزینه‌ها را بررسی می‌کنیم.

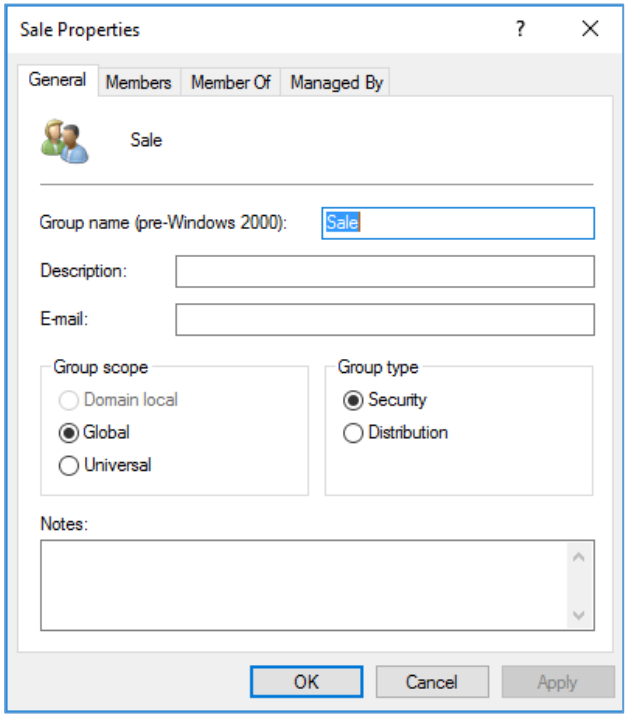
در قسمت Group Scope، سه گزینه وجود دارد؛ گزینه ی Domain Local که با انتخاب این گزینه، گروه مورد نظر توانایی عضوگیری کاربران از داخل دومین خود و دومین‌های Forest که به دومین اصلی، Trust می‌باشند را دارد، امّا گزینه‌ی Global که توانایی عضوگیری، تنها از دومین خود و زیرمجموعه‌ی خود را دارد، توانایی دسترسی از تمام Forest ها و دومین‌ها را دارد؛ گزینه‌ی Universal، توانایی عضوگیری از هر دومین و یا Forest را دارد، یعنی اگر از چند دومین اصلی در شبکه‌ی خود استفاده می‌کنید، در صورت Trust بودن، می‌توانید کاربران هر دومینی را عضو این گروه کنید.

درباره ی Trust کردن دومین‌ها، به صورت مفصّل 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.

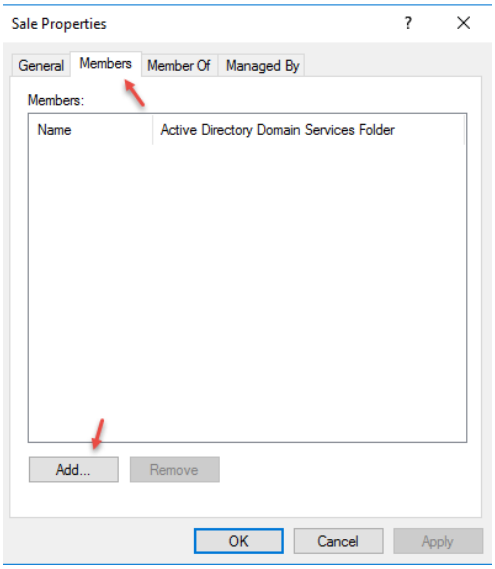
بعد از انتخاب گزینه‌ی Global، قسمت دیگری با نام Group Type وجو دارد که در این دو گزینه است؛ اگر گزینه ی Security را انتخاب کنید، این گروه می‌توانند مجوّز یا Permission لازم را دریافت کنند و برای ارسال پیام گروهی در دومین استفاده می‌شوند، امّا گزینه‌ی Distribution، این امکان را ندارد که Permission دریافت کند، امّا می‌تواند به اعضای خود پیام ارسال کند؛ برای اتمام کار، گزینه‌ی Global و Security را انتخاب و بر روی OK کلیک کنید.



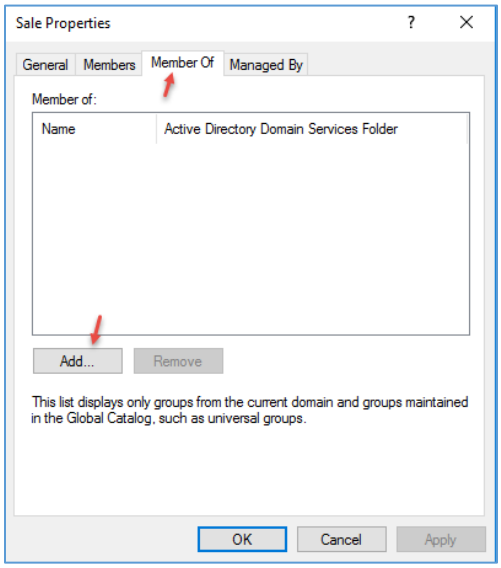
بعد از ایجاد گروه موردنظر، بر روی آن کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



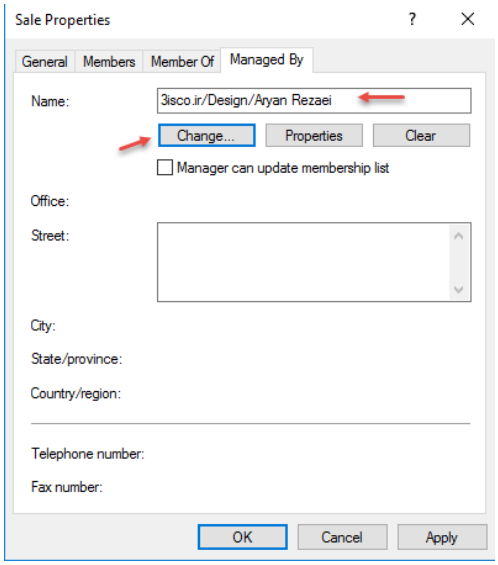
در این صفحه و در تب General، می‌توانید نوع گروه و Scope آن را مشاهده کنید و آن‌ها را تغییر دهید، به این نکته توجّه کنید که اگر Scope یک گروه را Global در نظر بگیرید، نمی‌توانید آن را به Domain Local تغییر دهید و یا برعکس؛ توضیحات و آدرس ایمیل مربوط به این گروه را وارد کنید.



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

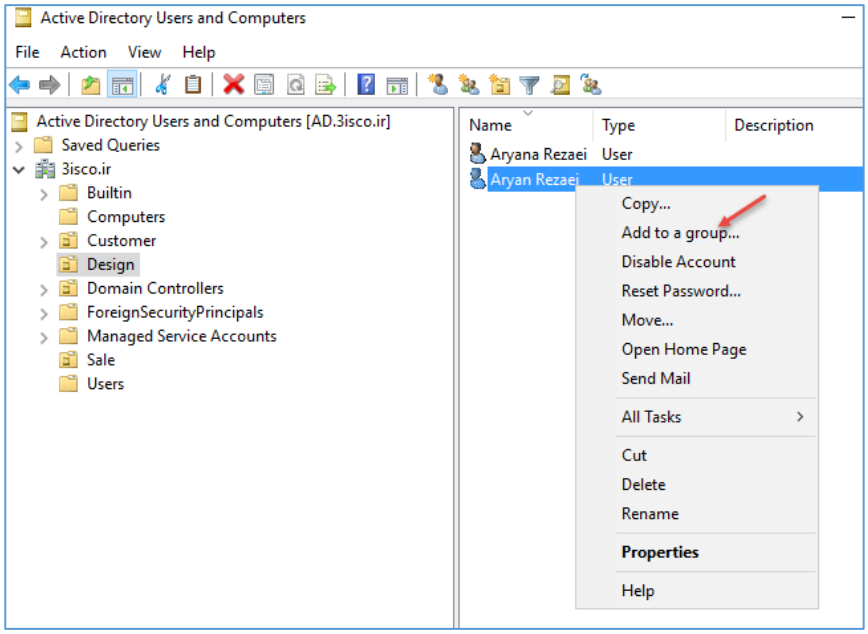


در تب **Member Of**، می‌توانید این گروه را عضو گروه دیگری کنید و از مجوّزهای آن استفاده کنید؛ برای این کار، بر روی **Add** کلیک کنید و گروه مورد نظر را به مانند شکل روبرو به لیست اضافه کنید.

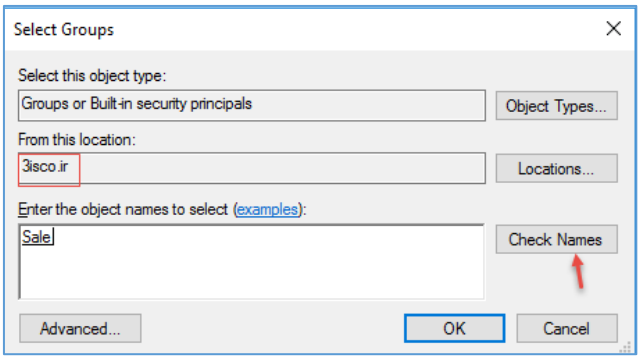


در تب **Managed By**، می‌توانید مشخّص کنید که چه کاربر و گروهی، رئیس گروه مورد نظر باشد، یعنی با انتخاب آن، تنها همان گروه یا کاربر موردنظر می‌تواند، کاربران دیگر را عضو این گروه کند.

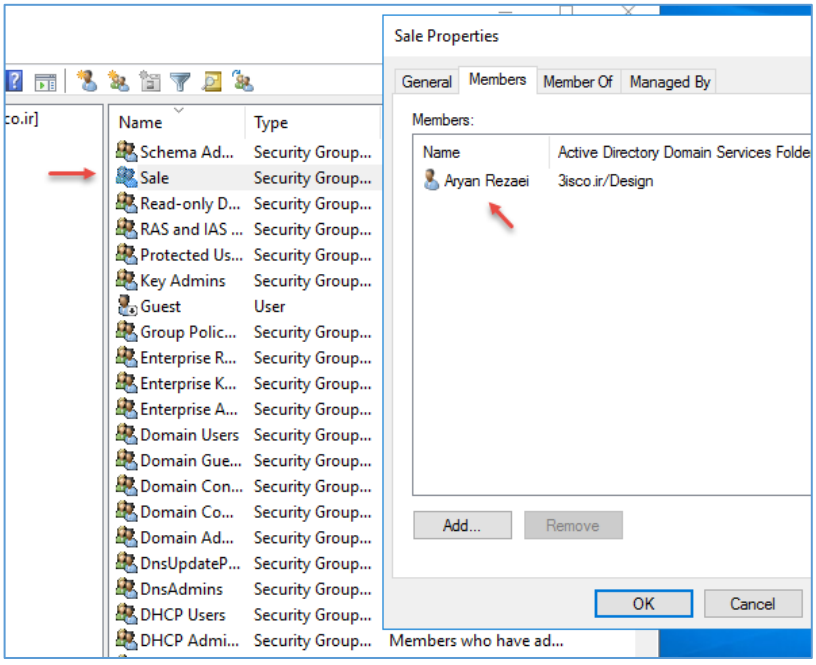
بر روی **OK** کلیک کنید.



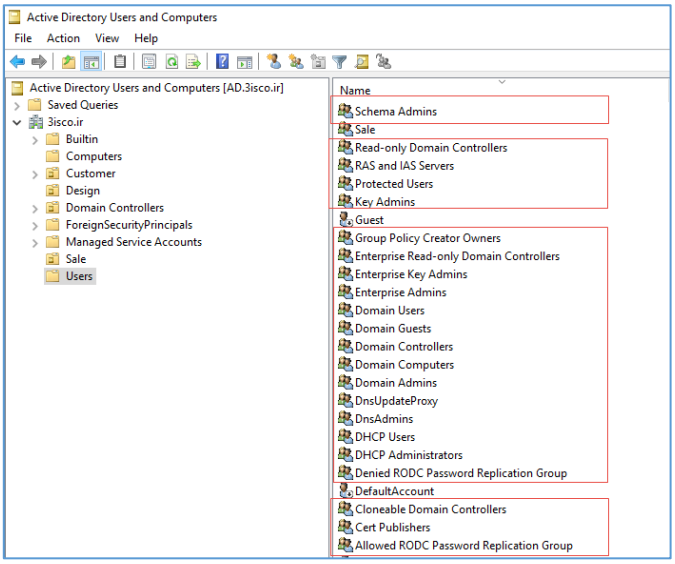
با استفاده از گروه، شما می‌توانید کاربران را عضو آن گروه کنید و دسترسی مختص به آن را مشخّص کنید، مثلاً می‌خواهید یک گروه خاص به فایل به اشتراک گذاشته شده، دسترسی داشته باشند، برای این کار می‌توانید کاربران خود را به مانند شکل، عضو گروه مورد نظر کنید، بر روی کاربر مورد نظر کلیک راست کنید و گزینه‌ی Add to a Group را انتخاب کنید.



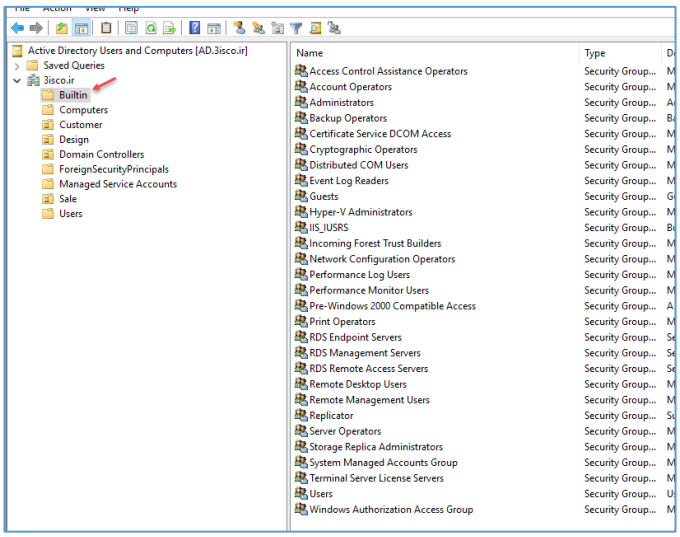
در این قسمت، Location شما باید بر روی دومین قرار داشته باشد و اگر نام گروه یا چند کلمه‌ی اوّل گروه را می‌دانید در جای مشخّص شده وارد کنید و بر روی Check Names کلیک کنید.



در شکل روبرو در قسمت Members مربوط به گروه Sale، کاربر Aryan Rezaei به لیست اضافه شده است، اکنون شما می‌توانید این گروه را به فایل‌های به اشتراک-گذاری شده دسترسی دهید.



یک‌سری گروه‌ها در قسمت Users وجود دارد که این گروه‌ها با نصب و حذف سرویس‌ها، کم و زیاد می‌شوند، در زیر، تعدادی از این گروه‌ها و نحوه‌ی عملکرد آنها در شبکه را مورد بررسی قرار خواهیم داد.



در قسمت Builtin نیز یک‌سری گروه تعریف شده است که به بررسی بعضی از آنها خواهیم پرداخت.

گروه Access Control Assistance Operators:

اعضای این گروه می‌توانند از راه دور به سیستم مورد نظر query یا پرس و جو بزنند، این گروه از سرور ۲۰۰۸ به بعد، تغییری نداشته است.

گروه Account Operators:

اعضای این گروه، دسترسی‌های اوّلیّه برای ایجاد کاربر را دارند و توانایی ورود به سرور دومین به صورت محلّی یا همان، Local را دارند.

گروه Administrators:

این گروه یگ گروه با دسترسی کامل و نامحدود به شبکه و کامپیوترها است که یک کنترل‌کننده‌ی دامنه و اعضای آن، بدون محدودیّت می‌توانند در دامنه‌ی مورد نظر دسترسی کامل داشته باشند، پس باید مراقب باشید که بدون بررسی کاربری را عضو این گروه نکنید.

گروه Allowed RODC Password Replication Group:

این گروه مربوط به RODC یا Read Only Domain controller است که رمز عبور در مرحله‌ی ریکاوری که هنگام نصب Active Directory وارد می‌شود را چک می‌کند تا تکراری نباشد و باعث مشکل نشود.

گروه Backup Operators:

این گروه برای ایجاد پشتیبان از سرور و یا سیستم دیگری ایجاد شده است و اعضای این گروه توانایی دارند تا به طور کامل از سرور، پشتیبان تهیّه و آنها را دوباره ریکاوری کنند، اعضای این گروه همچنین می‌توانند وارد سرور شوند و آن را خاموش کنند.

گروه Certificate Service DCOM Access:

اعضای این گروه توانایی دارند تا در بالاترین سطح به سرویس Certificate یا همان، گواهینامه‌های امنیّتی در شبکه متّصل شوند و آنها را ایجاد و مدیریّت کنند.

گروه Cloneable Domain Controllers:

اعضای این گروه، توانایی ایجاد یک دومین مجازی از دومین اصلی را دارا هستند که در صورت نیاز، این گروه را بررسی خواهیم کرد.

گروه Cryptographic Operators:

اعضای این گروه، توانایی انجام رمزنگاری در شبکه را دارا می‌باشند؛ این گروه از ویندوز ویستا به بعد ایجاد شده است.

گروه Denied RODC Password Replication Group:

اعضای این گروه نمی‌توانند رمز عبور RODC را تغییر دهند.

گروه Distributed COM Users:

اعضای این گروه، توانایی ارتباط با اشیا در Active directory را دارند، این گروه مختصّ برنامه‌نویسانی است که می‌خواهند با اشیای Com سرویس Active Directory در شبکه ارتباط برقرار کنند و اطّلاعات را ایجاد و تغییر دهند.

گروه DnsUpdateProxy:

اعضای این گروه، توانایی ارتباط با سرویس DNS را برای ایجاد رکورد دارند، این اعضا توانایی ایجاد A record و PTR رکورد برای آپدیت سرور DNS را دارند؛ این گروه به صورت پیش‌فرض، اعضایی ندارد.

گروه DnsAdmins:

این گروه، دسترسی کامل به سرویس DNS دارد و اعضای آن می‌توانند اطّلاعات سرویس DNS را بخوانند، ویرایش، حذف و مدیریّت کنند.

گروه Domain Admins:

این گروه که خود یکی از زیرمجموعه‌های گروه Administrators است برای مدیریّت کامل دومین کاربرد دارد، اعضای این گروه به تمامی تنظیمات در دومین دسترسی دارند و در کلّ شبکه نیز اعتبار دارند، مثلاً برای اینکه سیستمی را عضو دومین کنید، می‌توانید از این گروه استفاده کنید، اصولاً مدیر شبکه باید در این گروه قرار داشته باشد.

گروه Domain Computers:

اعضای این گروه توانایی عضو کردن کلاینت‌ها به شبکه را خواهند داشت و نیز می‌توانند کلاینت‌ها را از شبکه خارج کنند.

گروه Domain Controllers:

اعضای این گروه، توانایی اضافه کردن دومین‌های مختلف را به دومین root دارند، به صورت پیش‌فرض گروه Denied RODC Password Replication Group، زیر مجموعه‌ی این گروه است.

گروه Domain Guests:

گروه مهمان که توانایی دارد وارد دومین شود و پروفایل ایجاد کند؛ سطح دسترسی آن در شبکه بسیار پایین است.

گروه Domain Users:

تمام کاربرانی که در Active directory ایجاد می‌کنید به صورت پیش‌فرض عضو این گروه هستند، مثلاً اگر بخواهید یک پرینتر را برای همه‌ی کاربران شبکه به اشتراک بگذارید باید به این گروه دسترسی بدهید تا همه‌ی کاربران به پرینتر دسترسی داشته باشند.

گروه Enterprise Admins:

این گروه در سرور دومین اصلی کار می‌کنند و توانایی ایجاد Child دومین را دارد، مدیران شبکه باید عضو این گروه باشند تا دسترسی آنها در شبکه کامل شود.

گروه Enterprise Read-Only Domain Controllers:

اعضای این گروه فقط خواندنی، توانایی خواندن اطّلاعات Active directory را خواهند داشت، امّا نمی‌توانند تغییری بر روی آنها ایجاد کنند.

گروه Hyper-V Administrators:

اعضای این گروه، توانایی مدیریّت کامل ابزار Hyper-V را دارا خواهند بود.

گروه Schema admin:

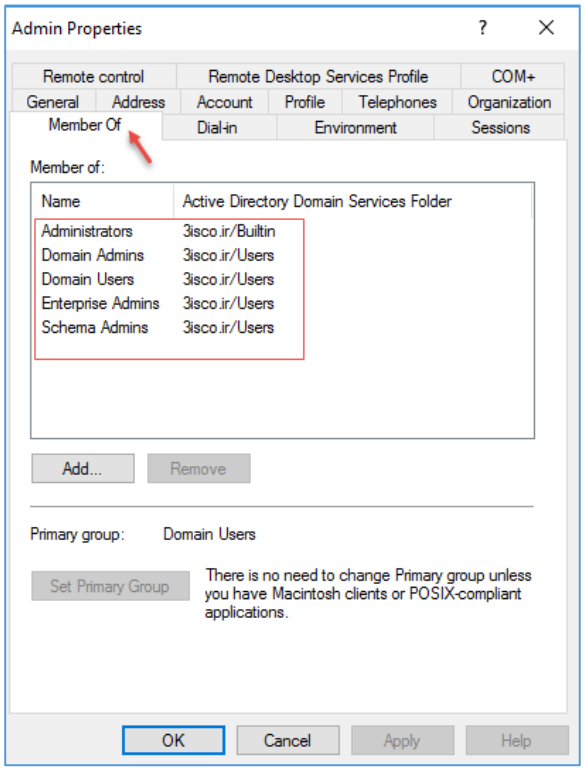
اعضای این گروه، توانایی تغییر Schema در سرویس Active Directory را دارا می‌باشند.

تا به اینجا، گروه‌های مهم در شبکه را بررسی کردیم که به صورت خواه، ناخواه با آنها کار خواهیم کرد، گروه‌های دیگری نیز هستند که در صورت امکان، نحوه‌ی عملکرد آنها را نیز بررسی خواهیم کرد.

عضویّت مدیر شبکه در گروه‌های اصلی:

برای اینکه مدیر یک شبکه بر کلّ اطّلاعات شبکه دسترسی داشته باشد باید عضو گروه‌های خاصّی شود که در زیر این گروه‌ها را مشاهده می‌کنید.

Administrator - Schema Admins – Domain Admins – Enterprise Admins



در قسمت Member OF، کاربر مورد نظر عضو گروه‌های مورد نظر در لیست بالا شده است که این کاربر می‌تواند دسترسی کامل به منابع شبکه و تنظیمات آن داشته باشد.

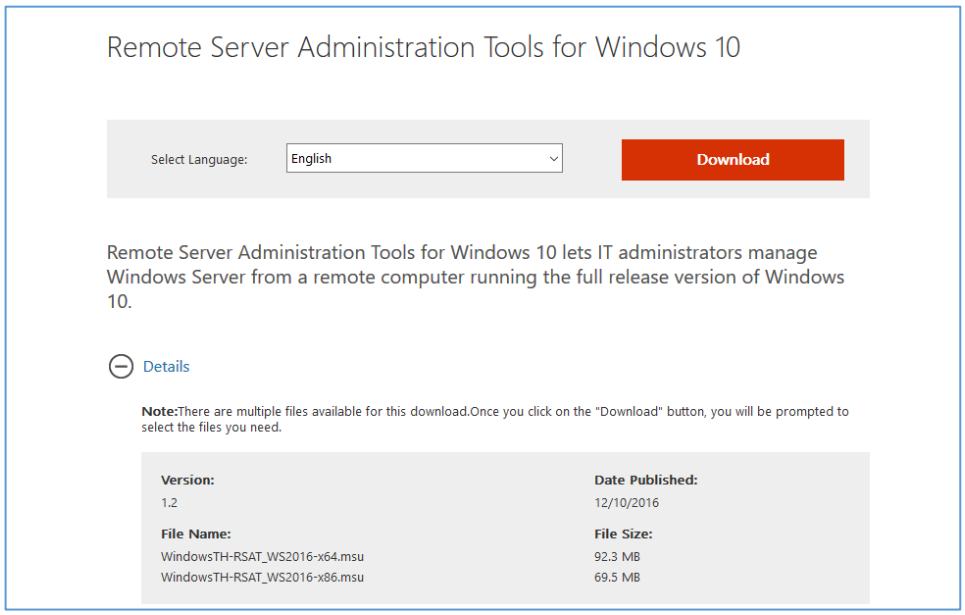
تذکّر: مواظب باشید که کاربران عادّی را عضو این گروه‌ها نکنید.

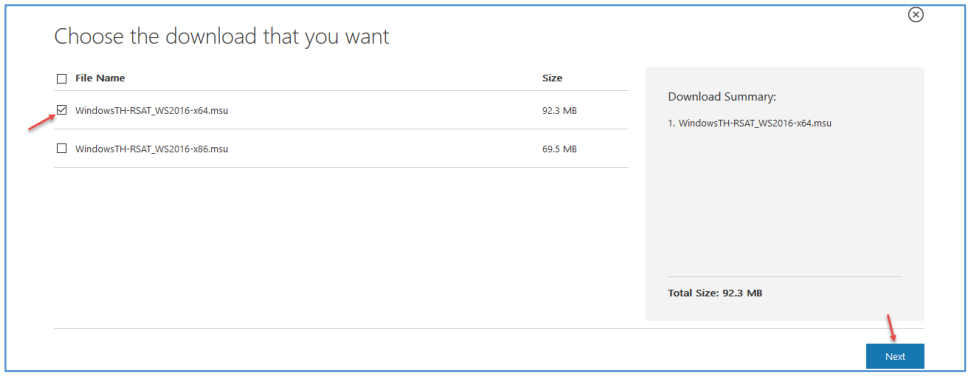
ارتباط از راه دور با سرویس Active Directory:

برای اینکه مدیر شبکه بتواند همه‌ی سرورها و سرویس‌ها را بر روی سیستم خود کنترل کند باید روش‌هایی را پیاده‌سازی کند تا همه‌ی سرویس‌ها و سرورها در دسترس باشد.

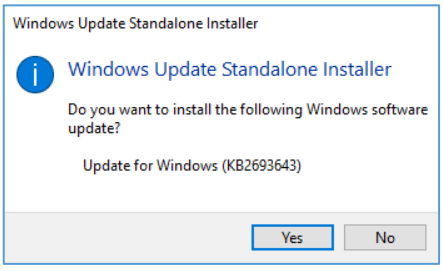
برای اینکه سرویس Active Directory را در یک ویندوز معمولی، مانند ویندوز ۷، ۸، ۸٫۱ و ۱۰ در دسترس باشد باید سرویس Administrative Tools را نصب کنید که باید برای هر ویندوز جدا دانلود کنید.

- ویندوز ۷
- ویندوز ۸
- ویندوز ۸٫۱
- ویندوز ۱۰



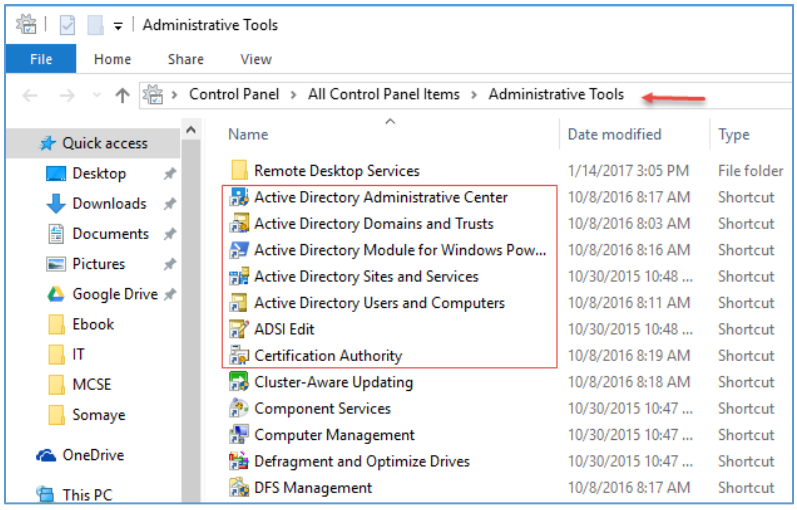


برای تست این موضوع، این کار را بر روی ویندوز ۱۰ انجام می‌دهیم؛ بر روی لینک ویندوز ۱۰ کلیک کنید و به مانند شکل روبرو بر روی Download کلیک کنید و بنا به نوع ویندوز خود که ٦٤ یا ٣٢ بیتی است، یکی را انتخاب، بر روی Next کلیک کنید تا فایل دانلود شود.



توجّه داشته باشید، سرویس Update باید قبل از اجرای فایل فعّال شده باشد، اگر فعّال نباشد با خطا مواجه خواهید شد، بر روی Yes کلیک کنید تا آپدیت مورد نظر بر روی کلاینت ویندوز ۱۰ اعمال شود.

بعد از نصب آپدیت، حتماً کلاینت مورد نظر را Restart کنید تا تنظیمات جدید اعمال شود.

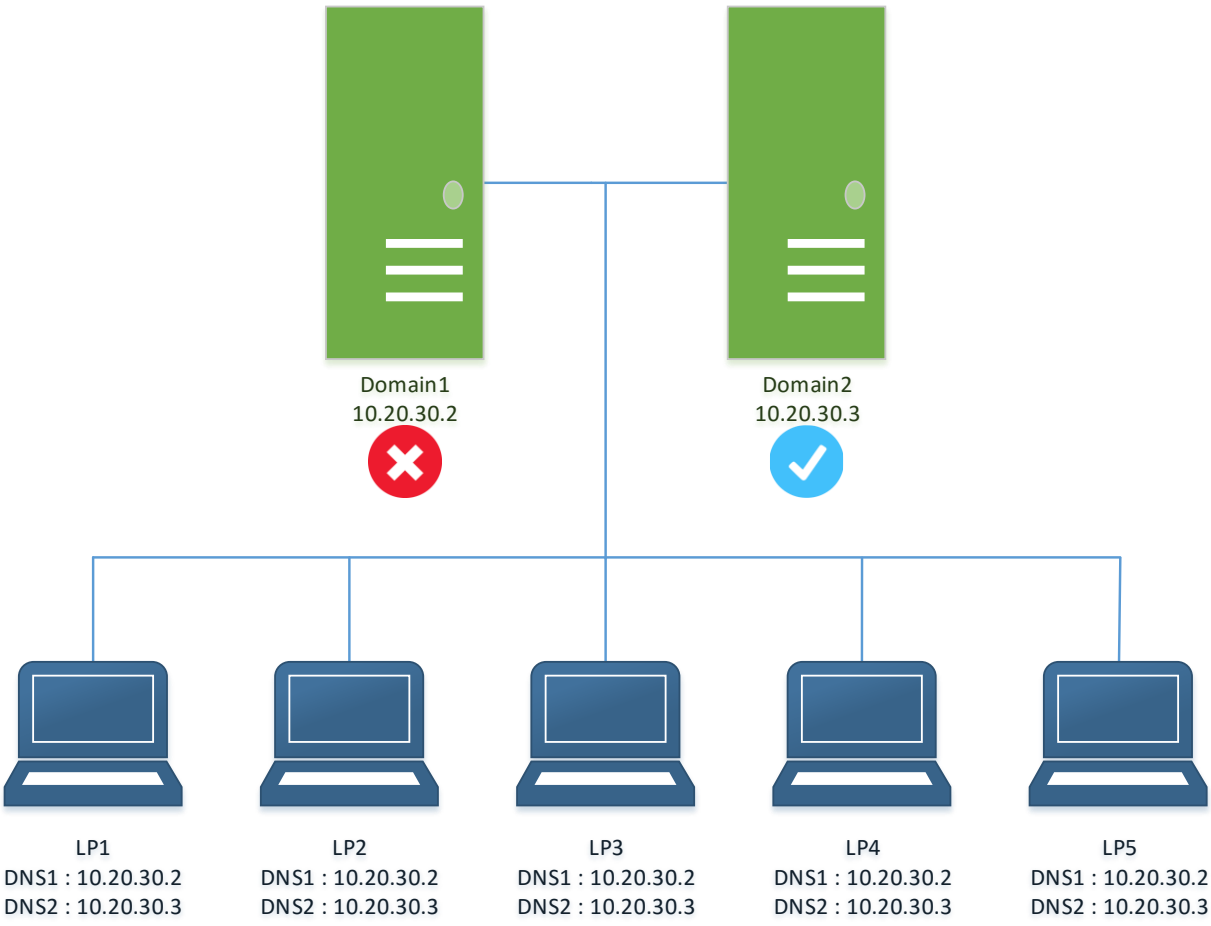


بعد از اجرا شدن کلاینت وارد ویندوز شوید و به آدرس روبرو مراجعه کنید، همانطور که مشاهده می‌کنید، سرویس‌های مورد نظر به لیست اضافه شده است.

نکته: کلاینتی که این آپدیت را بر روی آن نصب می‌کنید باید عضو دومین باشد.

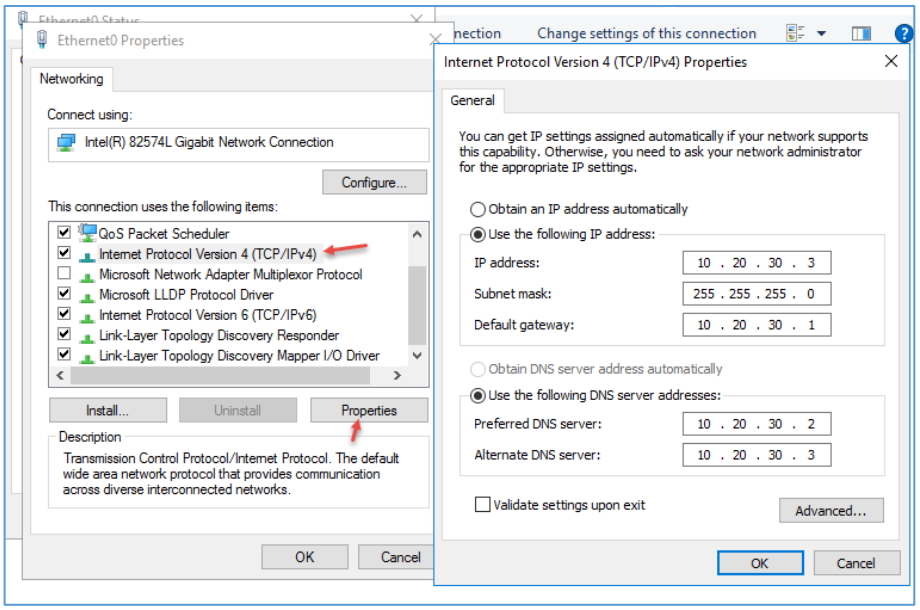
ایجاد Domain controller دوّم برای پایدار بودن شبکه:

زمانی که شما به عنوان مدیر شبکه انتخاب می‌شوید باید طوری شبکه‌ی خود را پیاده‌سازی کنید که با از دست دادن یک سرور، سرور دیگری به عنوان پشتیبان، شبکه را حفظ کند تا کاربران برای دسترسی به شبکه با مشکل مواجه نشوند، برای این کار باید نقشه‌ی خوبی داشته باشد.

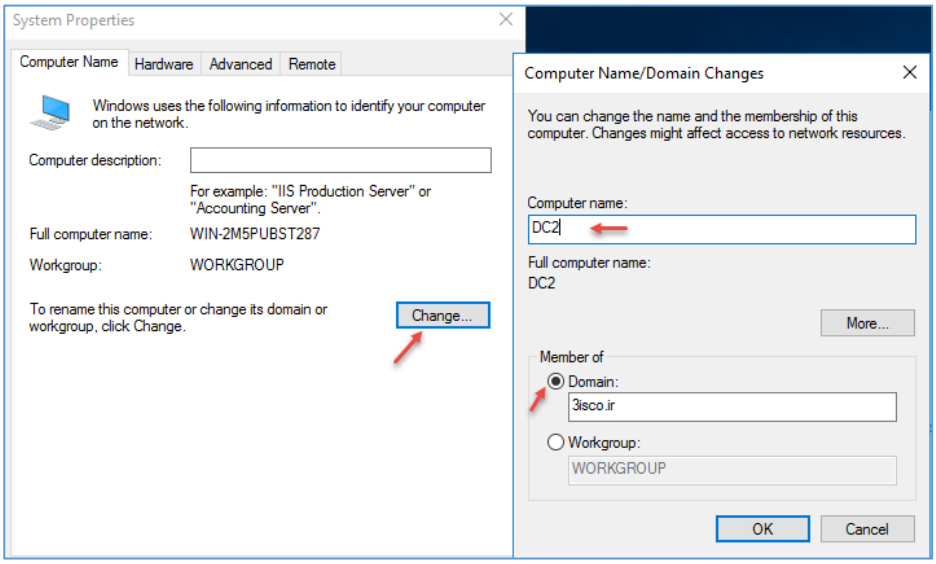


در شکل بالا، دو سرور دومین در شبکه فعّال است و از طریق سرویس DHCP، آدرس آنها به کلاینت‌ها داده شده است، اگر چنانچه Domain1 با آدرس 10.20.30.2 از رده خارج شود، Domain 2 با آدرس 10.20.30.3، شبکه را پایدار نگه می‌دارد و کاربران می‌توانند از این سرور سرویس بگیرند، این تجربه در شبکه برای بنده اتّفاق افتاده است که با این روش به راحتی توانستم مشکل را حل کنم.

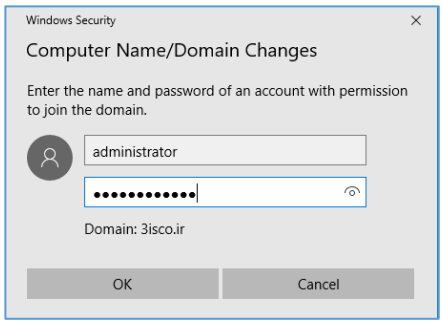
برای این منظور، ما یک سرور دیگر با مشخّصات سرور دومین اصلی آماده کردیم و ویندوز سرور ۲۰۱۶ را بر روی آن نصب کردیم و به مانند شکل روبرو بر روی آن، آدرس 10.20.30.3 را set کردیم، توجّه داشته باشید آدرس DNS اوّل را باید آدرس سرور DC که همان، 10.20.30.2 است را وارد کنید و در قسمت دوّم باید آدرس خود سرور را وارد کنید یا می‌توانید به جای آدرس 10.20.30.3 از آدرس 127.0.0.1 استفاده کنید که این آدرس، مختصّ خود سرور است؛ بر روی OK کلیک کنید و بعد وارد Rename computer شوید.



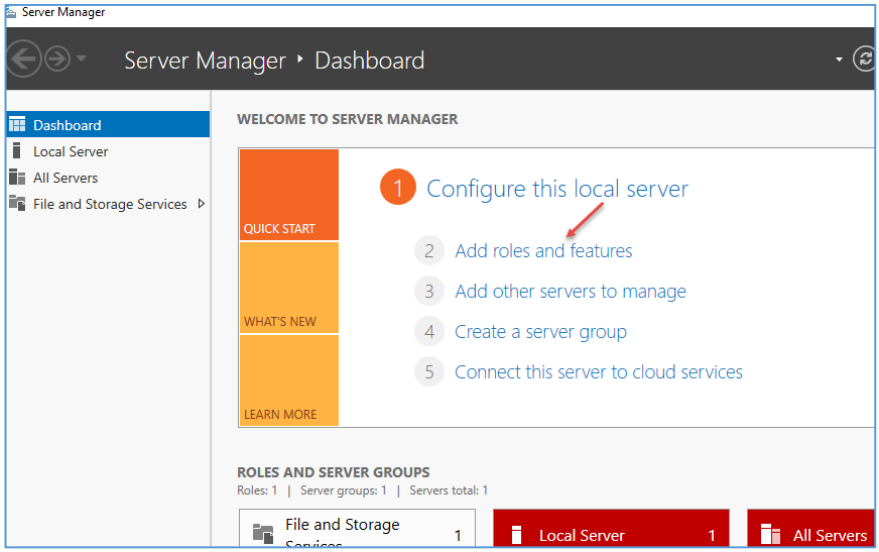
در این صفحه وارد Computer Name شوید و بر روی Change کلیک کنید و نام سرور را DC2 و نام دومین را، 3isco.ir وارد و بر روی OK کلیک کنید.



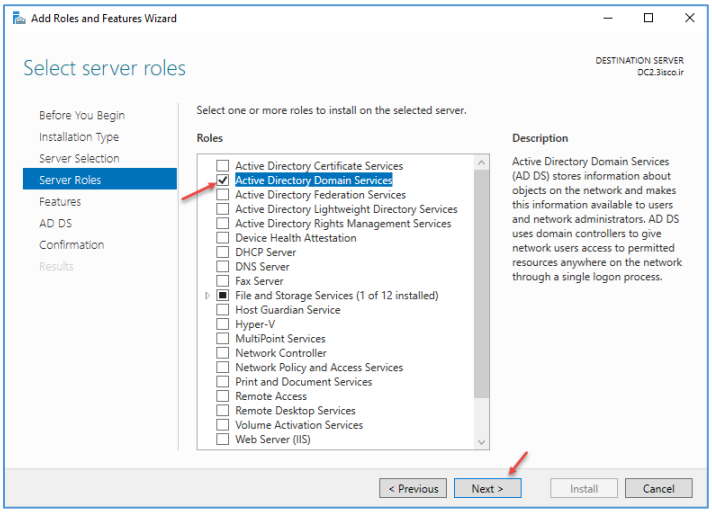
بعد از این کار، رمز عبور کاربر Administrator را وارد و بعد، سرور را Restart کنید.



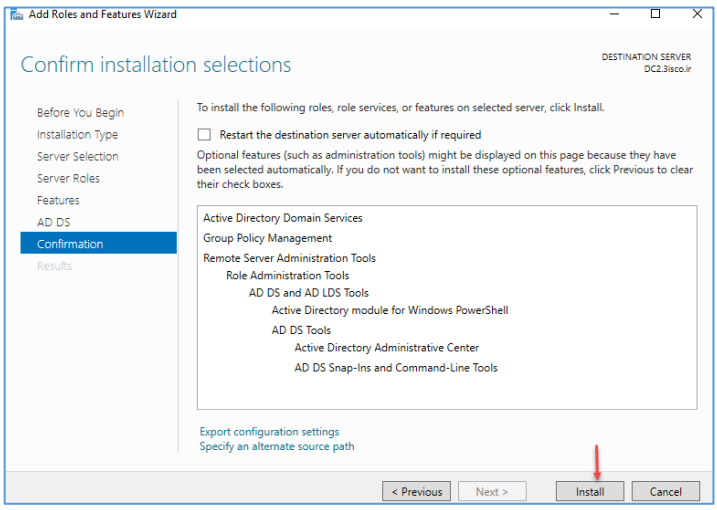
بعد از اینکه سرور را عضو دومین کردید باید سرویس Active directory را بر روی آن راه‌اندازی کنید تا به دومین اصلی متّصل شوید.



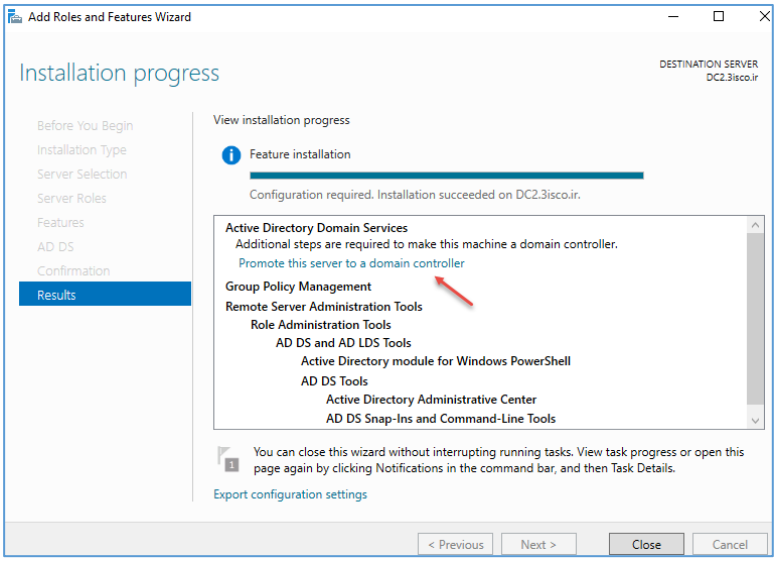
وارد Server Manager شوید و بر روی Add role and Features کلیک کنید.



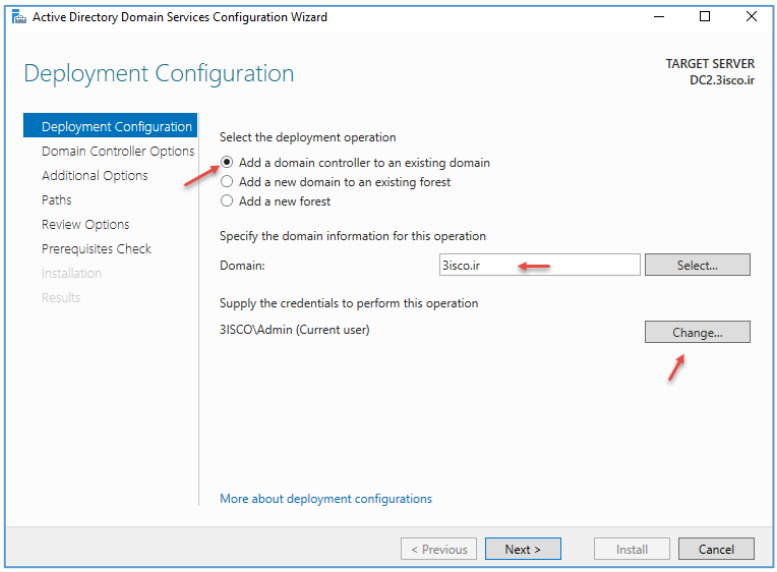
وارد Server Roles شوید و از لیست سرویس‌ها، گزینه‌ی Active directory domain and Services را انتخاب و بر روی Next کلیک کنید.



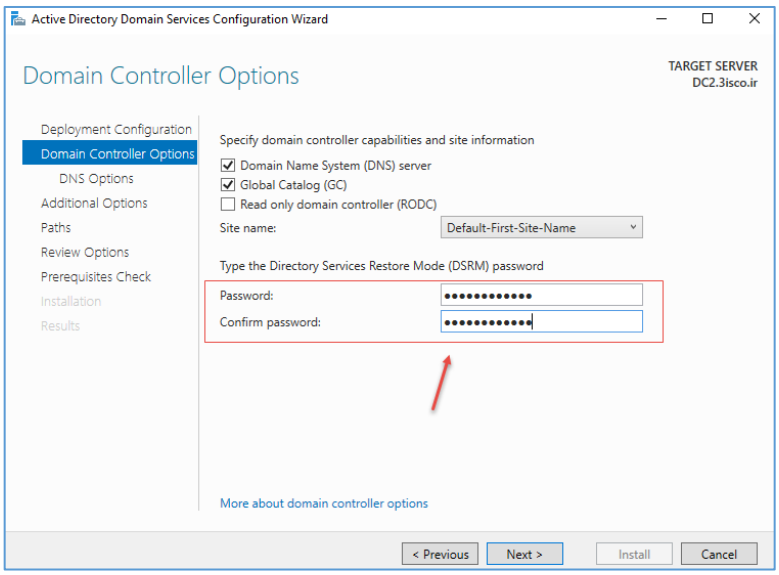
بر روی Next کلیک کنید تا به صفحه‌ی مورد نظر برسید و بر روی Install کلیک کنید تا سرویس نصب شود.



در این صفحه، بعد از نصب باید سرویس را تنظیم کنید، برای این کار بر روی Promote this server to a domain controller کلیک کنید.



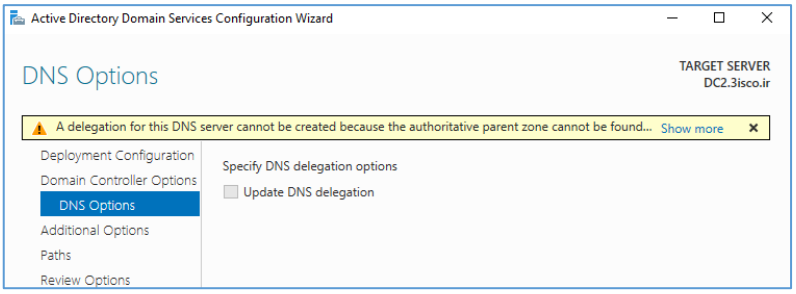
در این صفحه، چون از قبل دومین فعّال شده است باید گزینه‌ی اوّل را انتخاب کنید و در قسمت Domain باید بررسی کنید که نام دومین (3isco.ir) درست انتخاب شده است یا نه، در قسمت آخر نیز باید کاربری را با انتخاب گزینه‌ی Change وارد کنید که دسترسی لازم را داشته باشد، اصولاً کاربری انتخاب می‌شود که با آن در حال نصب سرویس هستید.



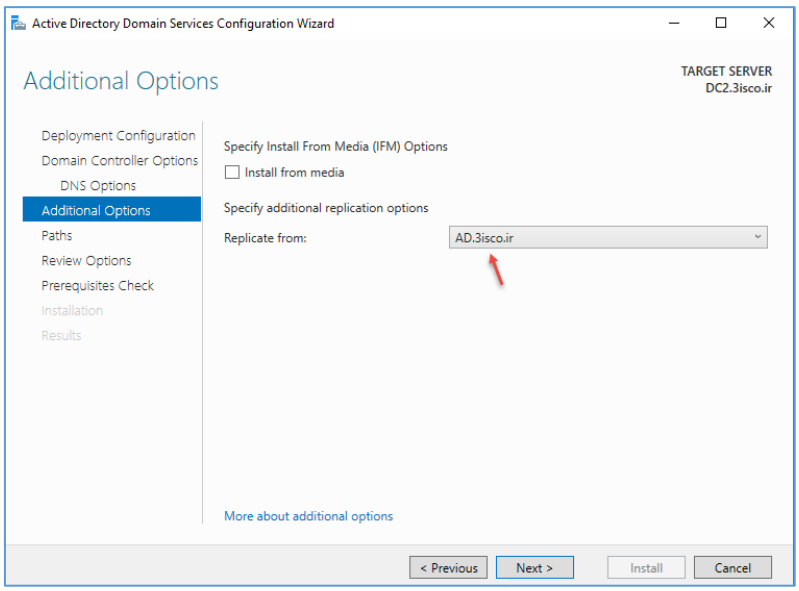
در این قسمت باید رمز ریکاوری سرویس Active directory را با عنوان DSRM وارد و بر روی Next کلیک کنید.

این رمز نیازی نیست که با رمزی که در نصب اوّلین دومین کنترلر استفاده کردید، یکی باشد.

در این قسمت بر روی Next کلیک کنید.

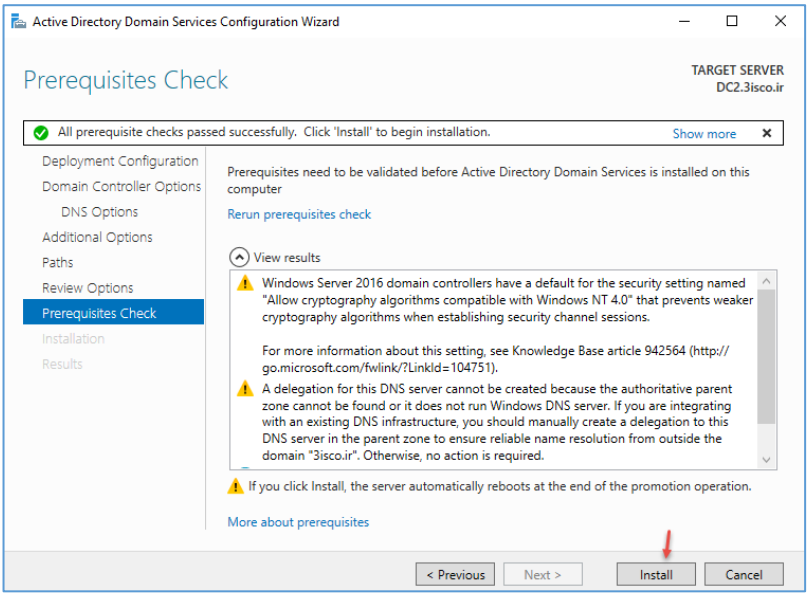


در قسمت Replicate باید نام سرور دومین اصلی خود را انتخاب کنید، توجّه داشته باشید گزینه‌ای با نام IFM یا همان، Install from media وجود دارد که این ویژگی به شما کمک می‌کند تا بار کمتری بر روی سرور در شبکه‌های بزرگ اعمال شود؛ شما با این روش می‌توانید یک فایل از Domain خود، ایجاد و در این قسمت، آدرس آن را وارد کنید تا نیاز نباشد با سرور اصلی، عملیّات Replicate انجام شود، در لینک زیر آموزش این کار انجام شده است:

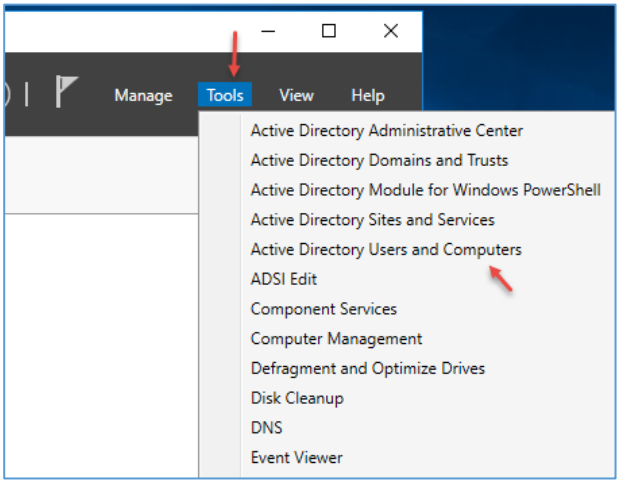


http://www.msserverpro.com/Install -an-additional-domain-controller-from-ifm-Install -from-media-in-windows-server-2012/

بر روی Next کلیک کنید تا به صفحه‌ی آخر برسید، در این صفحه، پیش‌نیازها بررسی می‌شود و اگر اوکی بود، اجازه‌ی نصب سرویس صادر می‌شود؛ بر روی Install کلیک کنید تا کار آغاز شود.

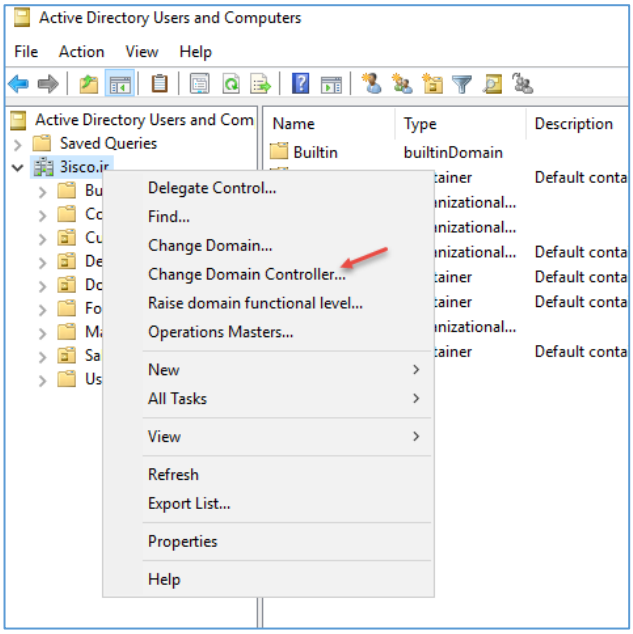


بعد از نصب، سرور را Restart کنید.

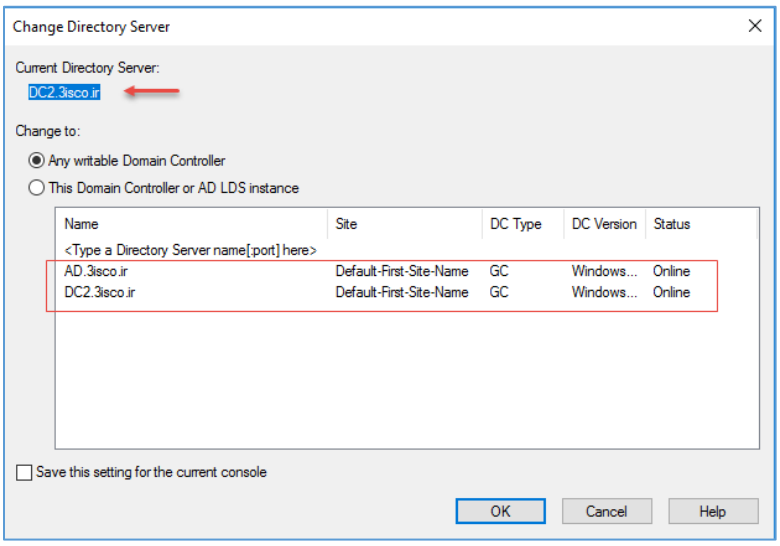


بعد ار ورود به سرور DC2 می‌توانید سرویس‌های اضافه شده به Server Manager را مشاهده کنید.

بر روی Active Directory Users and computers کلیک کنید.

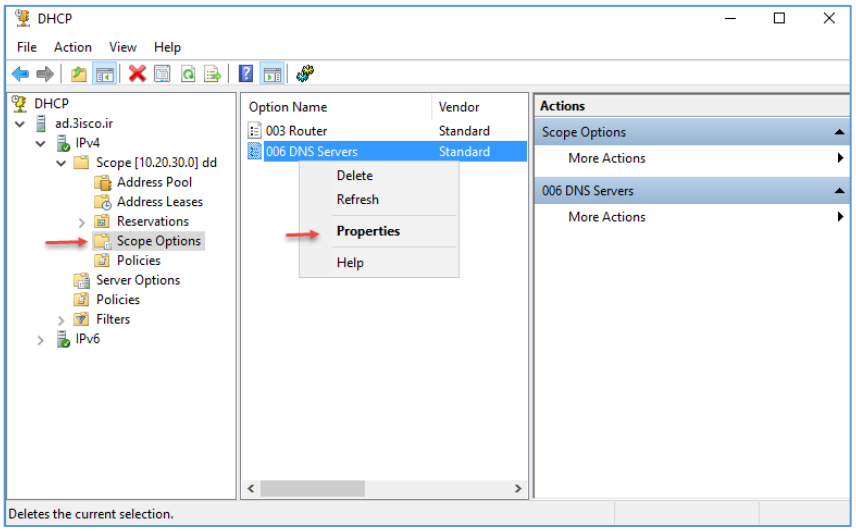


در این قسمت بر روی نام دومین خود کلیک راست کنید و گزینه‌ی Change Domain Controller را انتخاب کنید.

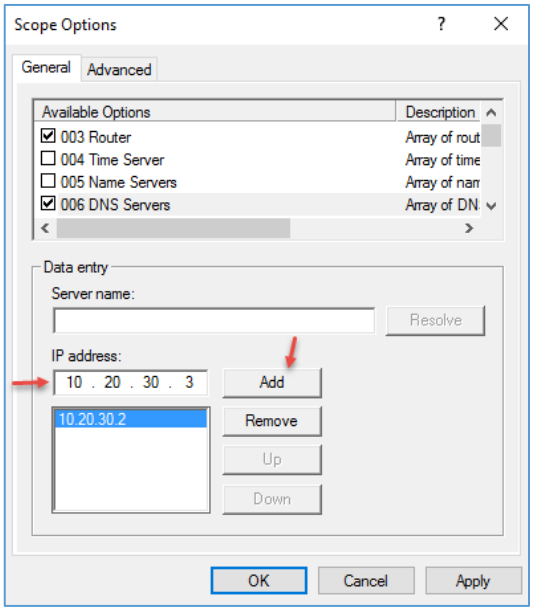


درقسمت Current Directory Server می‌توانید مشاهده کنید که کدام سرور دومین انتخاب شده است و اگر می‌خواهید سرور را تغییر دهید، می‌توانید از لیست زیری آن، دومین کنترلر مورد نظر خود را انتخاب کنید، اگر به ستون Status نگاه کنید، متوجّه خواهید شد هر دو سرور در حالت Online و فعّال قرار دارند.

بعد از اینکه دومین دوّم را با نام DC2 به شبکه اضافه کردید باید این موضوع را به کلاینت‌های خود اطّلاع دهید، برای اطّلاع باید از سرویس DHCP استفاده کنید و به کلاینت‌ها بگویید که سرور DNS دوّم با آدرس 10.20.30.3 ایجاد شده است.



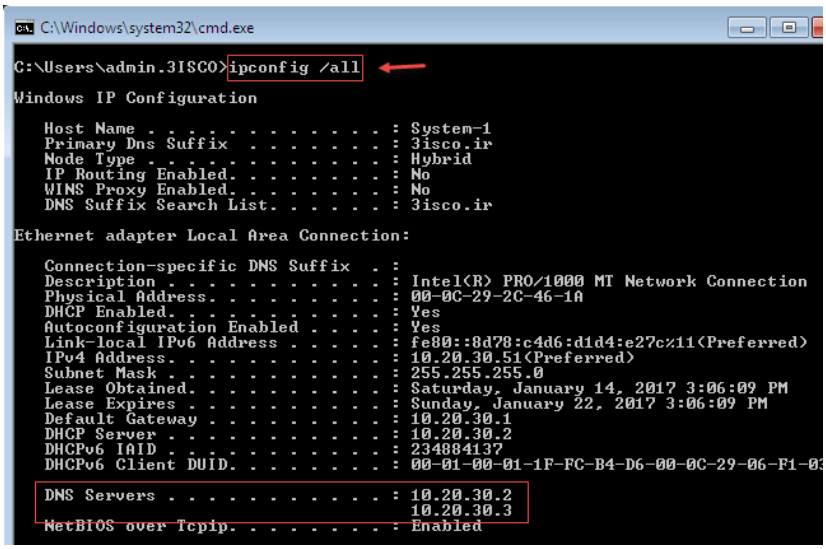
وارد سرور اوّل، AD شوید و سرویس DHCP را اجرا کنید و به مانند شکل روبرو در Scope مورد نظر بر روی Scope Options کلیک کنید و در صفحه‌ی باز شده بر روی DNS Server کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



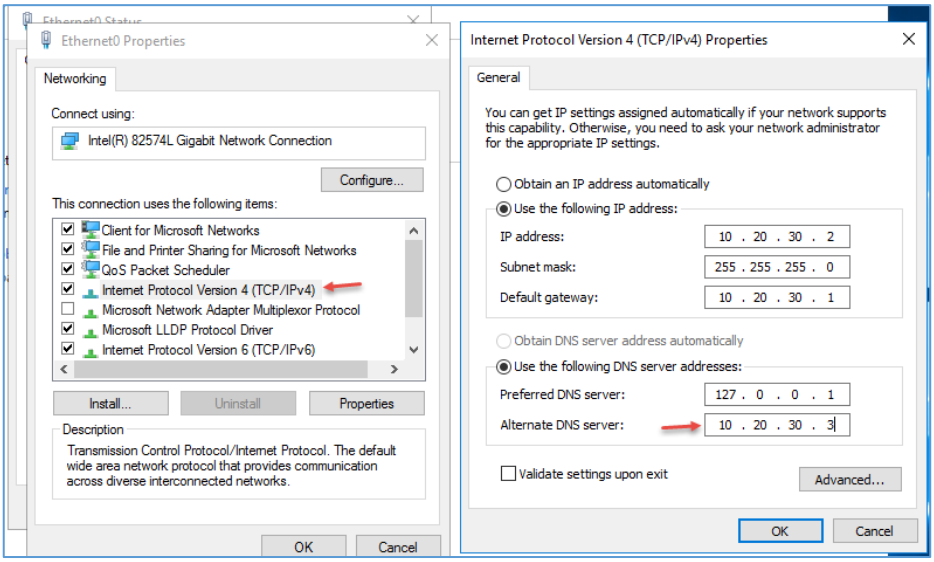
در این قسمت باید آدرس سرور دومین DC2 را وارد و بر روی Add کلیک کنید، توجّه داشته باشید با کلیدهای UP و Down می‌توانید اولویّت سرورها را تغییر دهید، سعی کنید سرور اصلی، اوّل و سرور فرعی، دوّم باشد.

بر روی OK کلیک کنید تا تنظیمات جدید اعمال شود.

بعد از انجام کار وارد یکی از کلاینت‌ها شوید و برای اینکه آخرین تغییرات را به صورت سریع از سرویس DHCP دریافت کنید از دستور Ipconfig /release و بعد، از دستور ipconfig /Renew استفاده کنید. این دستورات را در اوایل کتاب بررسی کردیم.

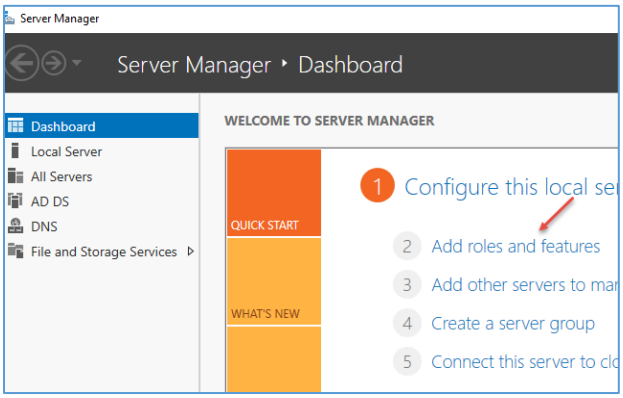


همانطور که مشاهده می‌کنید با اجرای دستور Ipconfig /all، آدرس هر دو سرور در قسمت DNS مشخّص شده است که می‌تواند کاملاً به شبکه‌ی شما کمک کند.

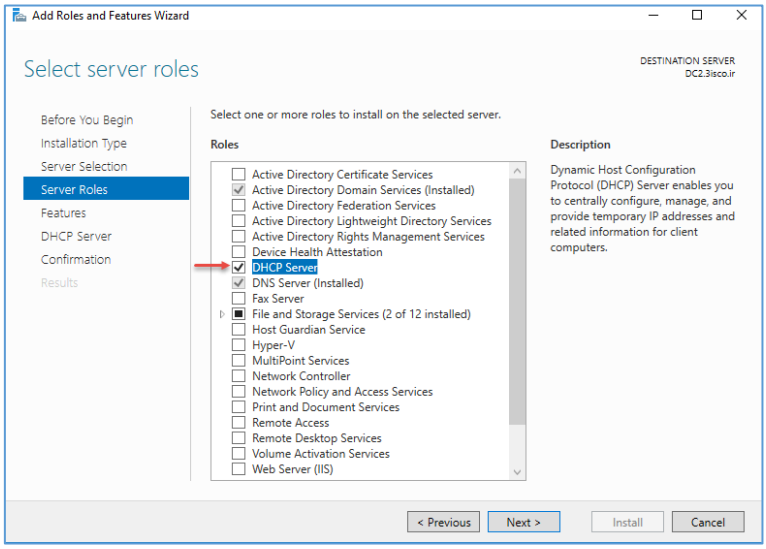


یک نکته‌ی مهم این است که بعد از انجام کارهای بالا در سرور اوّل، آدرس سرور دوّم را نیز وارد کنید تا همه چیز اوکی شود.

با این کار، هر دو سرور مکمّل هم خواهند بود و با قطع شدن یکی از آنها، دیگری به کاربران در شبکه سرویس خواهد داد.

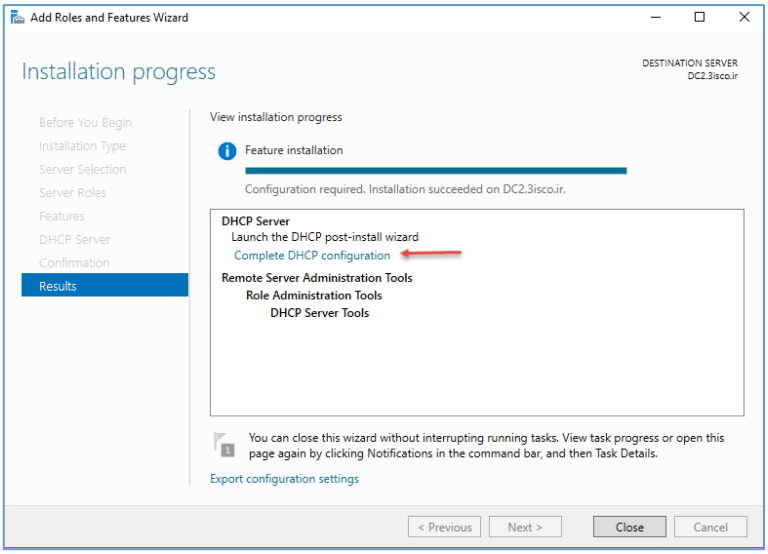


برای اینکه یک مجموعه‌ی کامل از سرویس‌ها را در هر دو سرور داشته باشید باید سرویس DHCP را روی سرور DC2 نصب کنید و آن را با سرویس DHCP سرور AD هماهنگ‌سازی کنید که در این قسمت، آن را انجام خواهیم داد؛ وارد Server Manager در سرور DC2 شوید و بر روی Add role and Features کلیک کنید.

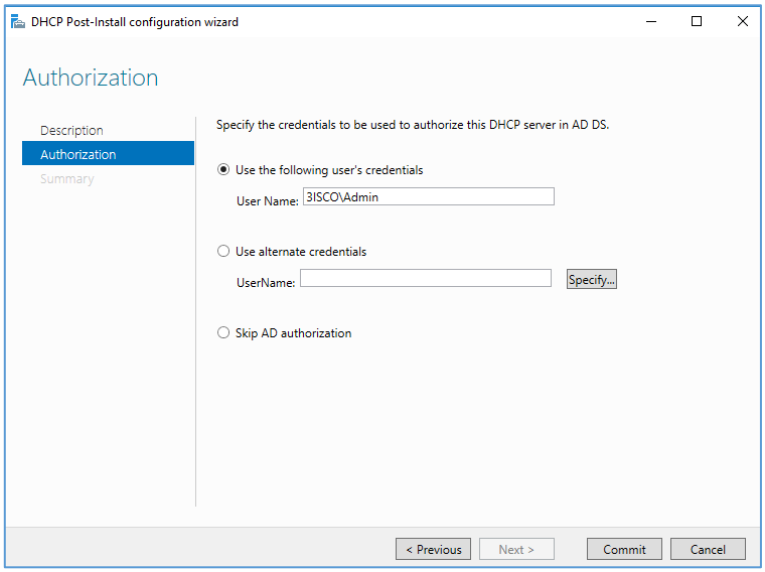


سرویس DHCP را از لیست انتخاب کنید و در پنجره‌ی باز شده بر روی Add Feature کلیک کنید.

در صفحات بعد بر روی Next کلیک و در صفحه‌ی آخر نیز بر روی Install کلیک کنید تا سرویس نصب شود.

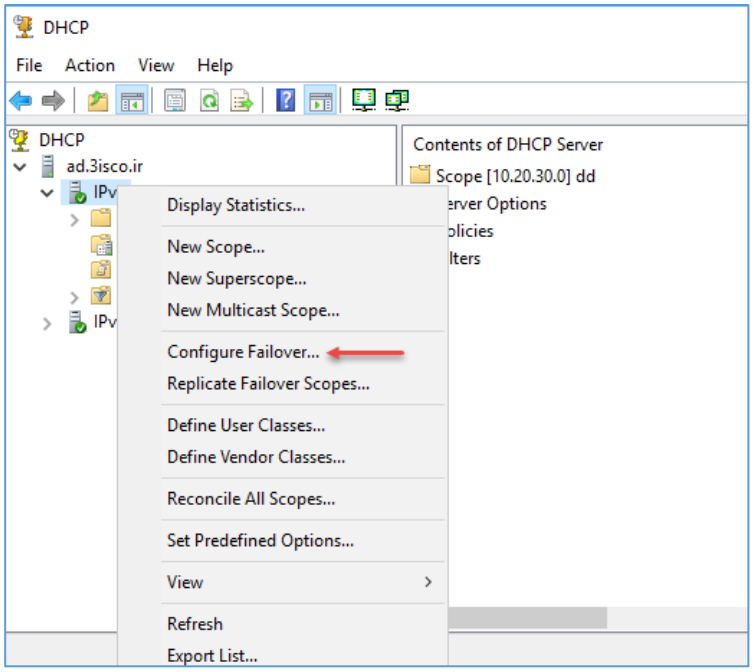


در این صفحه برای کامل کردن سرویس DHCP بر روی گزینه‌ی مشخّص‌شده در عکس، کلیک کنید.

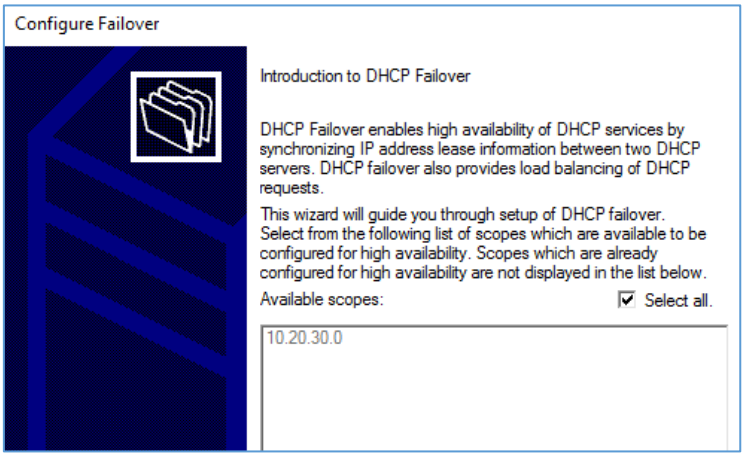


در این صفحه باید کاربری را مشخّص کنید که دسترسی کامل به شبکه داشته باشد که به صورت پیش‌فرض، کاربری انتخاب می‌شود که با آن سرویس را نصب کردید، بر روی Commit کلیک کنید تا عملیّات احراز هویّت با سرور انجام شود.

بعد از این کار، سرور را Restart کنید.

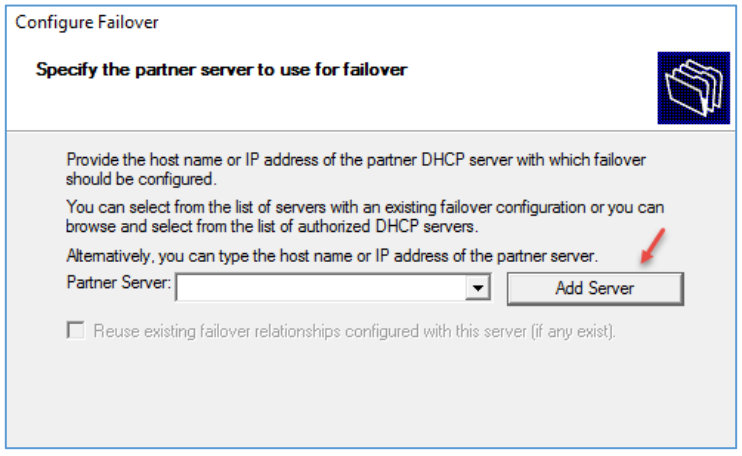


بعد از نصب سرویس در سرور DC2 باید وارد سرور AD که در اوایل کتاب بر روی آن، سرویس DHCP را فعّال کردیم، شوید و به مانند شکل روبرو بر روی IPV4 کلیک راست و گزینه‌ی Configure Failover را انتخاب کنید.

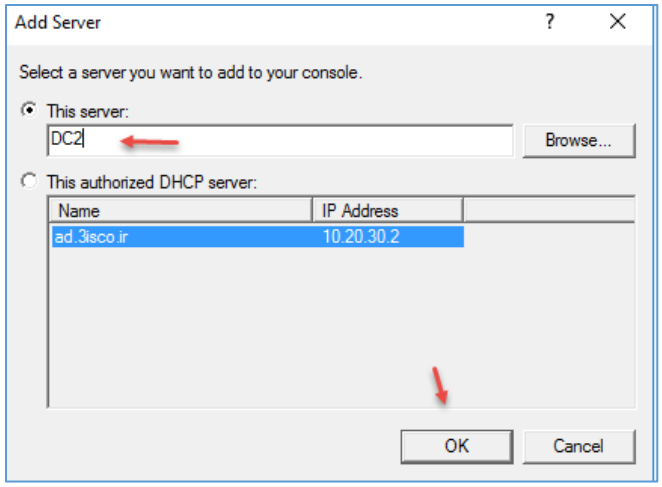


در این صفحه، Scope شما که 10.20.30.0 است، مشخّص شده است، اگر چند Scope داشته باشید، در این لیست مشخّص می‌شود که می‌توانید یک یا چند تا از آنها را انتخاب کنید.

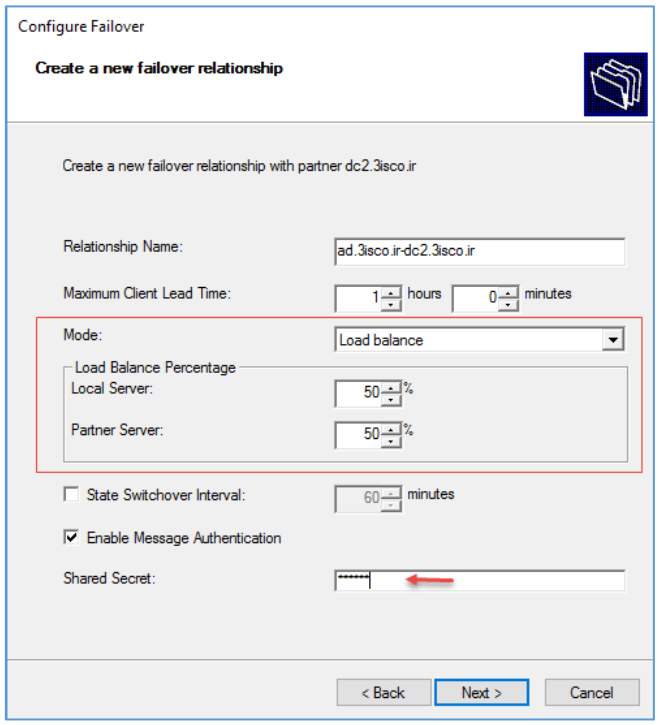
بر روی Next کلیک کنید.



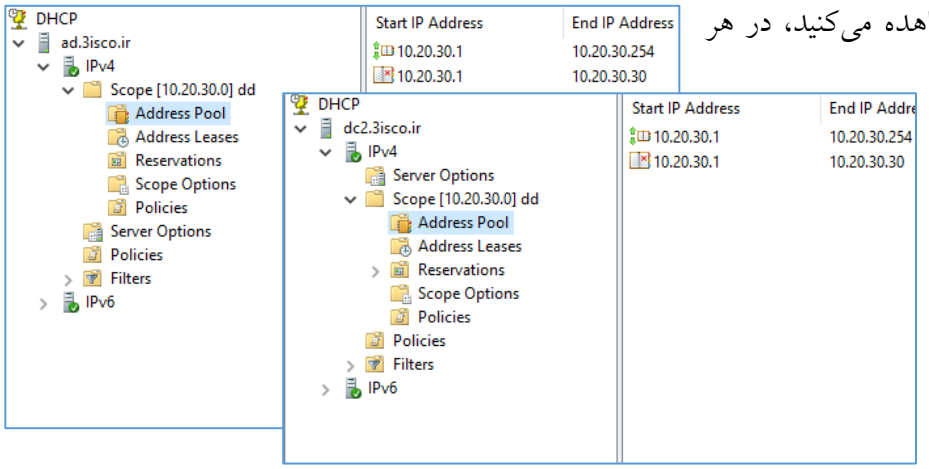
در این قسمت باید سرور دوّم، یعنی DC2 که روی آن سرویس DHCP را فعّال کردید را انتخاب و بر روی Add Server کلیک کنید.



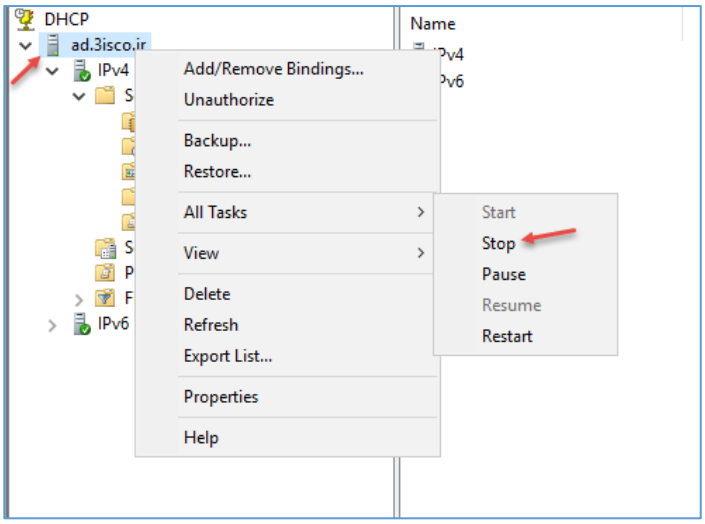
در این صفحه با کلیک بر روی دکمه‌ی Browse می‌توانید سرور دوّم، DC2 را به لیست، اضافه و بر روی OK کلیک کنید و در صفحه‌ی قبل بر روی Next کلیک کنید.



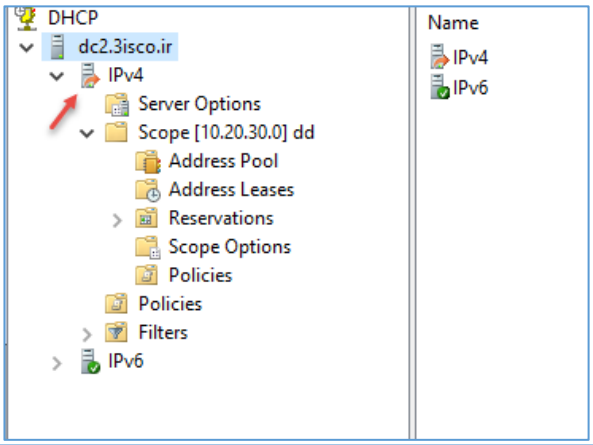
در این صفحه، یک نام ارتباطی مشخّص شده است و در قسمت Mode می‌توانید مشخّص کنید که این دو سرور AD و DC2 به چه صورت با هم ارتباط برقرار کنند، اگر گزینه‌ی Load balance را انتخاب کنید، هر دو سرور به صورت هم‌زمان کار خواهند کرد و شما می‌توانید درصد استفاده‌ی آنها را بنا به نوع سرور تغییر دهید، گزینه‌ی دوّم، در قسمت Mode، گزینه‌ی Hot Standby است که یک سرور فعّال است و دیگری منتظر می‌ماند تا سرور اصلی از شبکه خارج شود، در قسمت آخر نیز یک رمز عبور برای برقراری ارتباط دو سرور DHCP انتخاب کنید تا امنیّت آن حفظ شود؛ بر روی Next کلیک کنید.



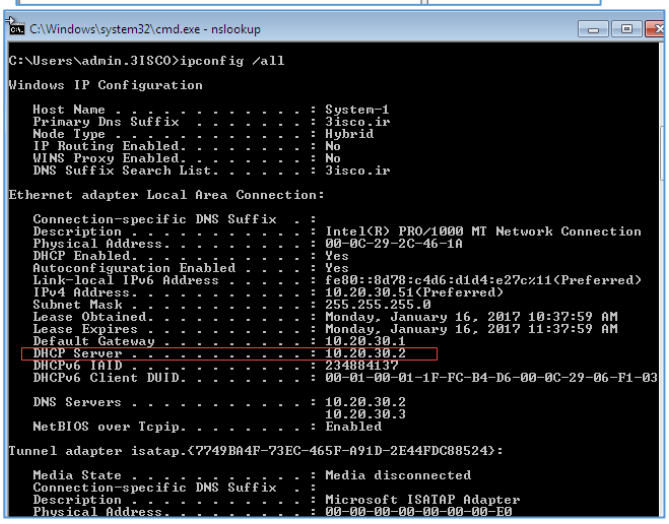
همانطور که در دو شکل روبرو مشاهده می‌کنید، در هر دو سرور، سرویس DHCP فعّال شده است و هم‌زمان به شبکه سرویس می‌دهند.

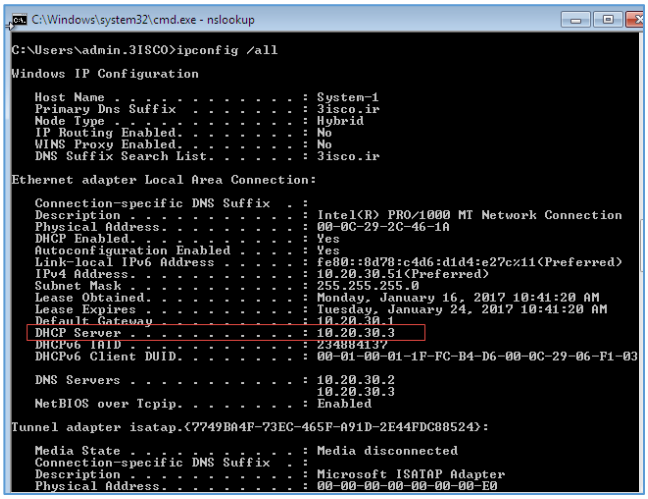


حال، اگر در سرور AD، سرویس DHCP را به مانند شکل روبرو Stop کنید، سرور DC2 به کار خود ادامه خواهد داد و شبکه با مشکلی مواجه نخواهد شد.

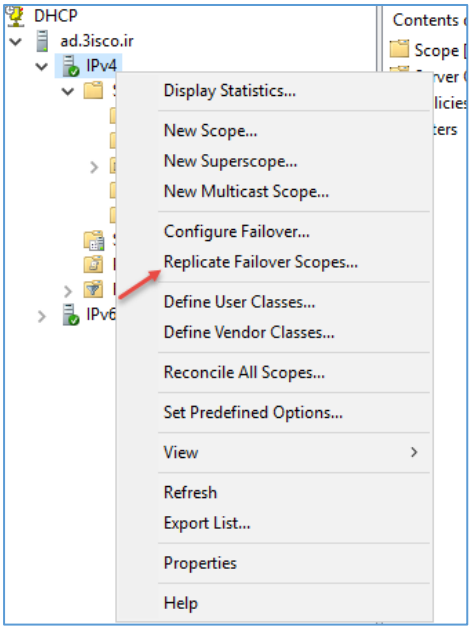


همانطور که مشاهده می‌کنید، بعد از اینکه سرور اصلی، یعنی AD غیر فعّال شد، نوع آیکون IPV4 در سرور دوّم، یعنی DC2 تغییر کرده است و این، نشان دهنده‌ی این است که سرور روبرو از کار افتاده است و این سرور در حال کار است.

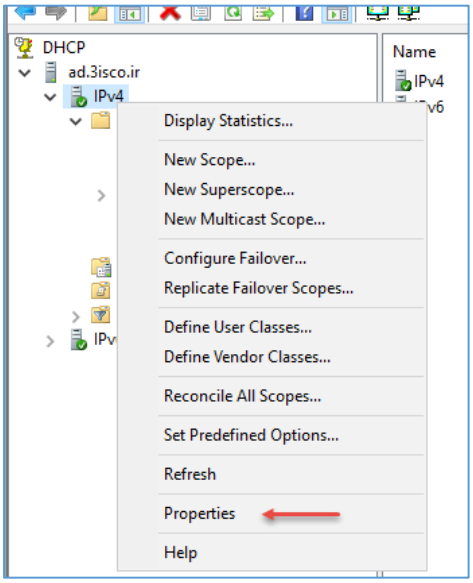




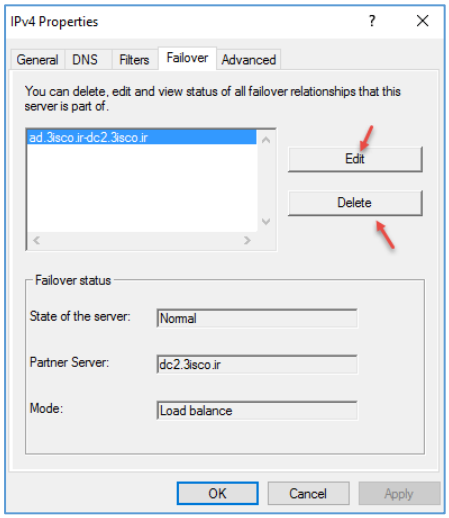
در شکل سمت چپ، کلاینت درخواست IP داده است که سرور اصلی، یعنی 10.20.30.2 به آن IP تخصیص داده است، امّا بنا به دلایلی، سرور اوّل از کار افتاده است و کلاینت، دوباره درخواست IP داده است که سرور دوّم، یعنی 10.20.30.3 (DC2) که در شکل سمت راست مشخّص شده است به آن IP تخصیص داده است.



اگر بخواهید دو سرور DHCP، آخرین تغییرات را به صورت سریع به هم ارسال کنند باید بر روی IPV4 کلیک راست کنید و به مانند شکل بر روی Replicate Failover Scopes کلیک کنید و در شکل باز شده بر روی Yes کلیک کنید تا آخرین تغییرات بین دو سرور با هم ردّ و بدل شود.



حال، اگر بخواهید تنظیمات Failover را در هر دو سرور تغییر دهید و یا اینکه آن را حذف کنید باید بر روی IPV4 کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



در این صفحه، نام Failover مورد نظر که با هم ایجاد کردیم، مشخّص شده است و شما برای ویرایش اطّلاعات آن باید بر روی Edit کلیک کنید و یا اگر می‌خواهید این قابلیّت را غیر فعّال کنید باید بر روی Delete کلیک کنید.

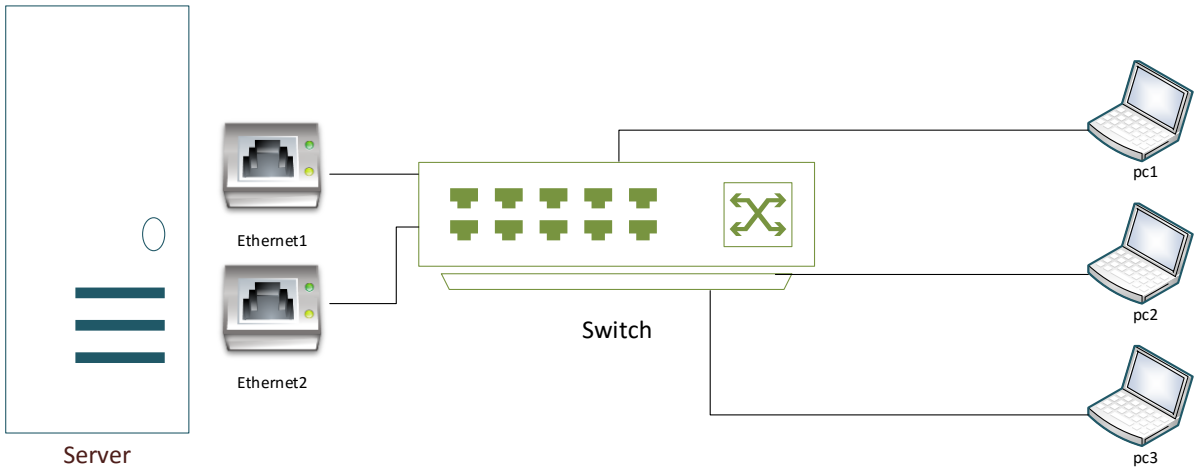
فعّال‌سازی سرویس NIC Teaming:

یکی از بهترین و پرکاربردترین سرویس‌هایی که توسّط مایکروسافت در ویندوز سرور ارائه شده، استفاده از ابزار NIC Teaming برای ایجاد Load Balancing و Redundancy در شبکه است.

مثلاً اگر در شبکه‌ی خود از File Server و یا هر سرور ذخیره‌ساز دیگری استفاده می‌کنید و اصلاً دوست ندارید، حتّی برای چند لحظه، دسترسی به آن را از دست دهید باید از این سرویس استفاده کنید؛ تا زمانی که یک خطّ شبکه قطع شد، خطّ دیگری شروع به کار کند و جای خطّ قبلی را بگیرد.

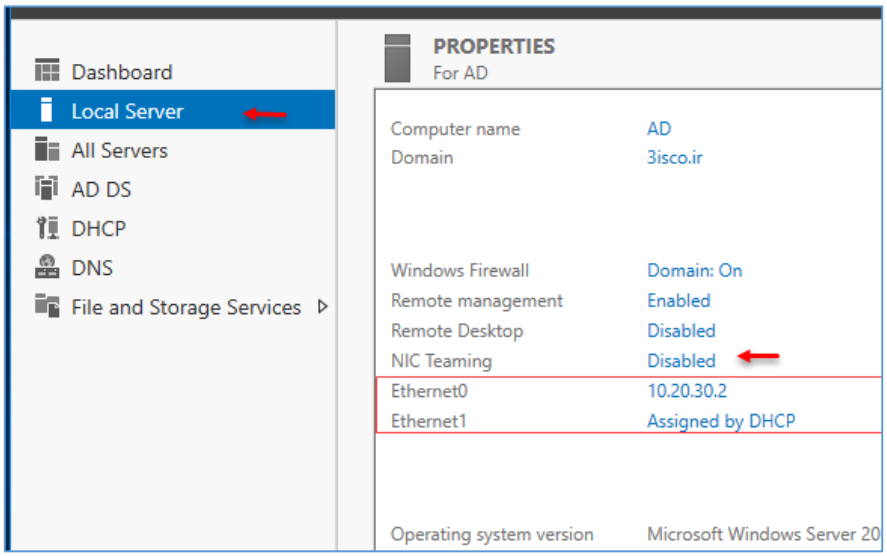
این فنّاوری قبلاً به صورت سخت‌افزاری بر روی سرورهایی، مانند hp وجود داشته که همین امر باعث ایجاد Redundancy در شبکه شده است، امّا به صورت نرم‌افزاری وجود نداشته و برای اوّلین بار، شرکت مایکروسافت، این فنّاوری را در ویندوز سرور ۲۰۱۲ ارائه داد که با هم آن را بررسی می‌کنیم.

برای شروع کار به شکل زیر توجّه کنید.



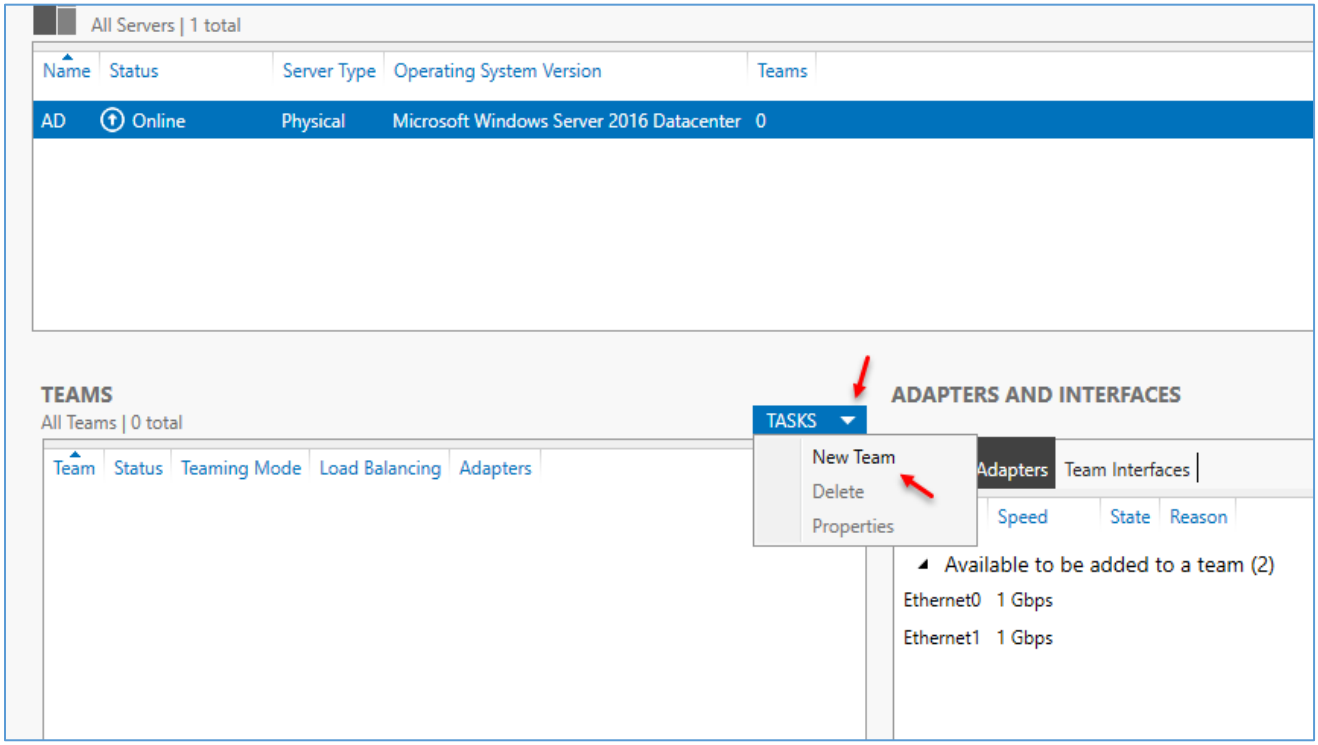
در شکل بالا، یک سرور قرار دارد که دارای دو کارت شبکه است و این دو کارت شبکه از طریق کابلی به سوئیچ در شبکه متّصل شده‌اند و کلاینت‌ها و یا همان، PC ها از طریق سوئیچ و بعد از طریق این دو کارت به سرور متّصل هستند؛ به صورت پیش‌فرض هر کارت شبکه، یک آدرس IP مختص به خود دارد و جدا از هم به کاربران سرویس می‌دهند، امّا در این قسمت قصد داریم، یک آدرس را به این دو کارت شبکه تخصیص دهیم تا کاربران، تنها از یک آدرس استفاده کنند، با این تفاوت که از هر دو کارت شبکه به صورت هم‌زمان می‌شود استفاده کرد.

برای شروع کار به سرور خود، دو کارت شبکه اضافه می‌کنیم، در اینجا از سرور AD استفاده می‌کنیم که آدرس IP آن، 10.20.30.2 بوده است.

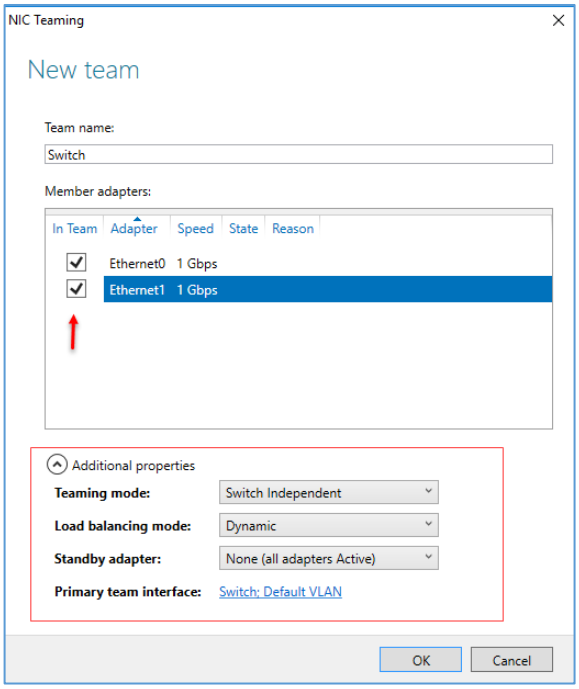


پس در حال حاضر، سرور AD دارای دو کارت شبکه است، امّا هنوز تنظیماتی روی آن اعمال نشده است.

برای شروع وارد Server Manager شوید و از سمت چپ بر روی Local Server کلیک کنید و در صفحه‌ی باز شده، مقابل جلوی گزینه‌ی NIC Teaming، بر روی Disabled کلیک کنید تا صفحه‌ی مورد نظر ظاهر شود؛ در شکل بالا دو کارت شبکه که بر روی سرور قرار گرفته شده، مشخّص است.



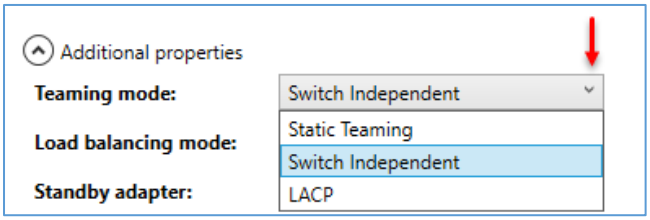
در صفحه‌ی بالا از قسمت TASKS، گزینه‌ی New Team را انتخاب کنید.



در این قسمت باید تنظیمات اصلی خود را اعمال کنید، در قسمت Team Name، یک اسم به دلخواه خود وارد کنید و در قسمت Member Adapter، کارت شبکه‌های خود را انتخاب کنید، شما می‌توانید از تعداد کارت شبکه‌ی بیشتری استفاده کنید.

در قسمت Additional Properties، تنظیمات مربوط به Switch وجود دارد که هر کدام را با هم بررسی می‌کنیم.

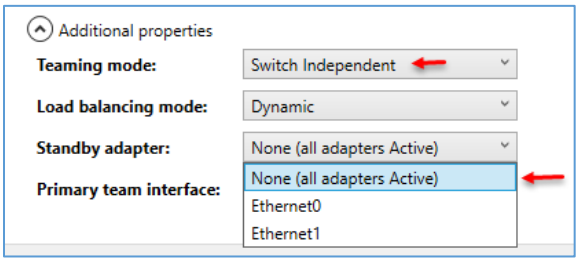
در قسمت Teaming Mode، سه گزینه وجود داردکه در شکل زیر آن را مشاهده می‌کنید.



:Switch independent

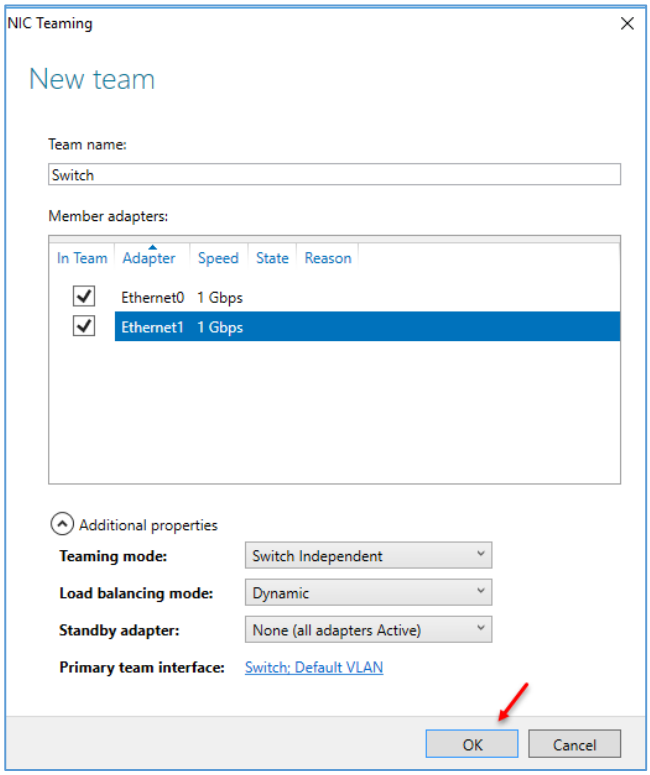
این گزینه به صورت پیش‌فرض انتخاب شده است و اگر فعّال شود، کارت شبکه به صورت Load Balancing کار خواهد کرد، یعنی هر دو کارت شبکه به صورت پیش‌فرض فعّال خواهد بود که این کار باعث افزایش پهنای باند خواهد شد و سرعت دسترسی برای کاربران افزایش پیدا خواهد کرد.

نکته: سعی کنید برای کار در این حالت از ۳ کارت شبکه و بیشتر به بالا استفاده کنید تا در صورت از کار افتادن یکی از کارت‌های شبکه، پهنای باند زیاد دچار مشکل نشود.



در شکل روبرو، اگر Switch independent را انتخاب کنید، قسمت Standby adapter فعّال خواهد شد واگر گزینه‌ی اوّل را انتخاب کنید، یعنی اینکه هر دو کارت شبکه به طور هم‌زمان فعّال خواهد بود که این کار باعث ایجاد Load Balancing خواهد شد، امّا اگر دو گزینه‌ی دیگر، یعنی هر یک از کارت شبکه‌ها را انتخاب کنید، در زمان کار، یکی از کارت‌های شبکه

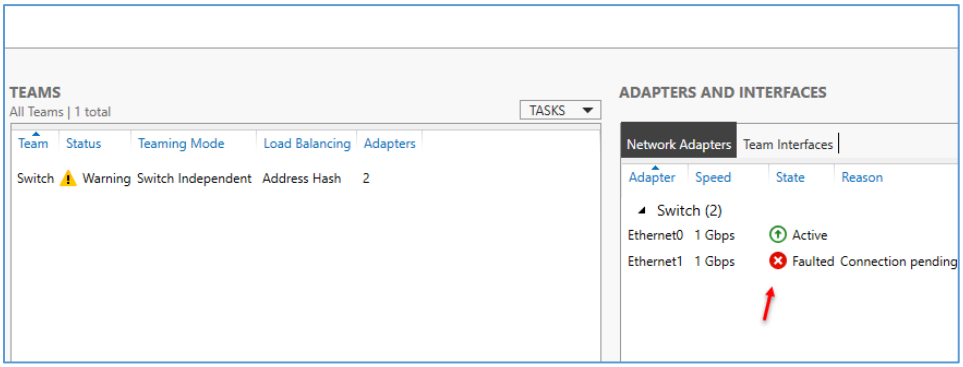
به صورت پیش‌فرض فعّال خواهد بود و دیگر به صورت آماده به کار و یا همان Standby قرار خواهد گرفت تا زمانی که کارت شبکه‌ی اوّل از کار افتاد، کارت شبکه دوّم شروع به کار کند و به کلاینت‌ها سرویس دهد.



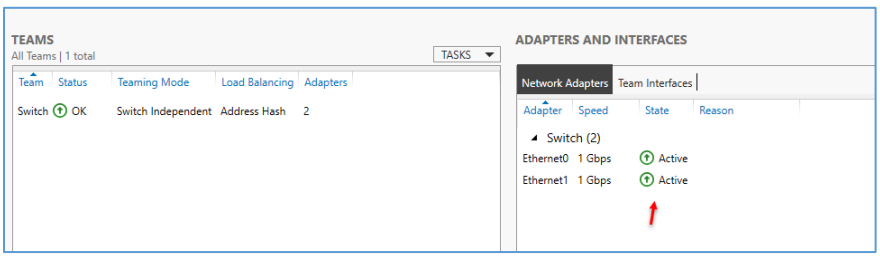
برای تست این موضوع تنظیمات را به مانند شکل روبرو انجام دهید و بر روی OK کلیک کنید.

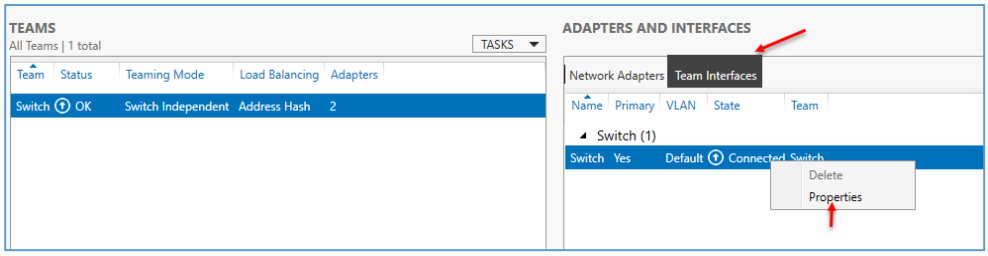
نکته مهم: اگر از ماشین مجازی استفاده می‌کنید، این حالت با خطا مواجه خواهد شد و شما باید در قسمت Load Balancing mode، گزینه‌ی Address Hash را انتخاب کنید.

نکته: انتخاب حالت Switch independent باعث می‌شود که این سرور با هر نوع سوئیچی ارتباط برقرار کند.

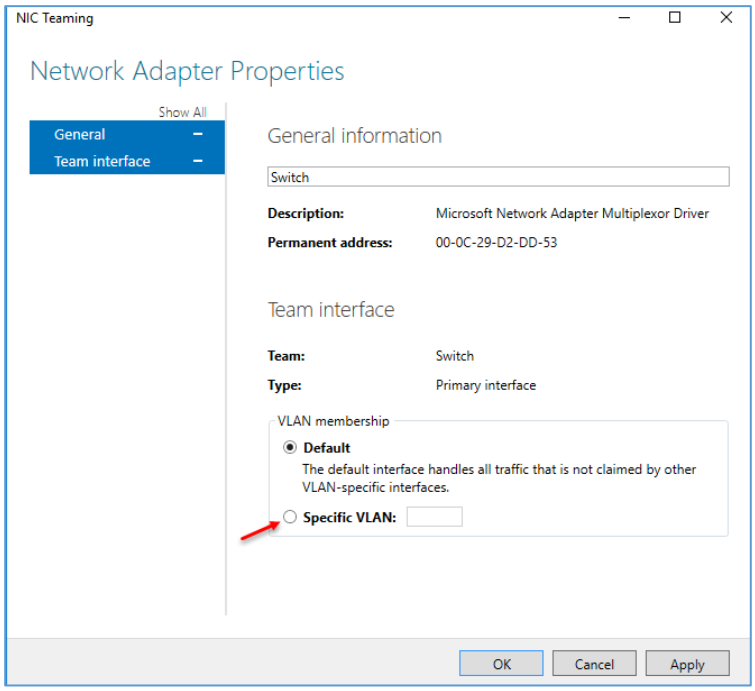


بعد از اینکه بر روی OK کلیک کردید، عملیّات انجام خواهد شد و شکل روبرو برای شما به نمایش در خواهد آمد؛ در چند ثانیه‌ی اوّل، شاید یکی از کارت-های شبکه شما با خطا Faulted... روبرو شود که بعد از چند ثانیه به حالت پایدار بر خواهد گشت و سرویس با قدرت، شروع به کار خواهد کرد که در شکل روبرو مشاهده می‌کنید.



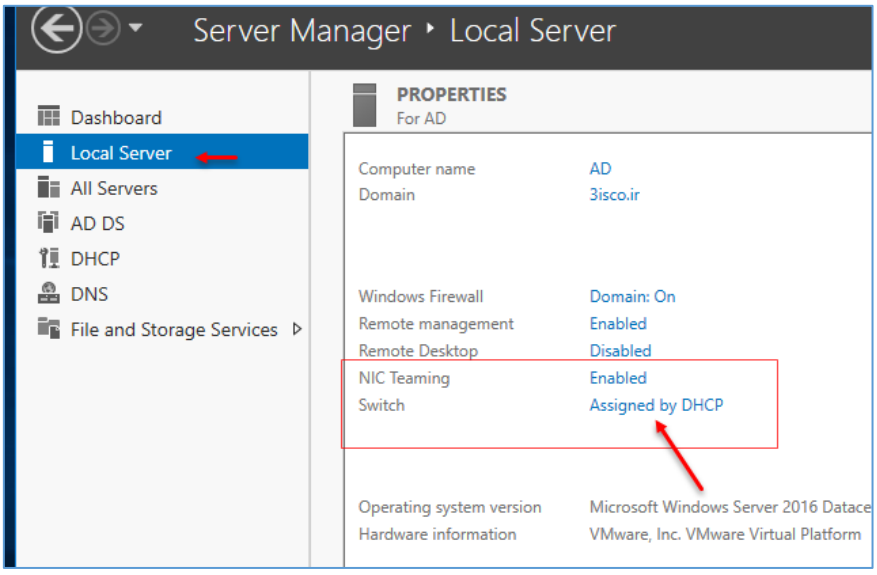


اگر در سوئیچ اصلی خود در شبکه از شماره‌ی VLAN خاصّی استفاده می‌کنید، می‌توانید وارد Team Interface شوید و به مانند شکل، بر روی نام مورد نظر خود که ایجاد کردید، کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.

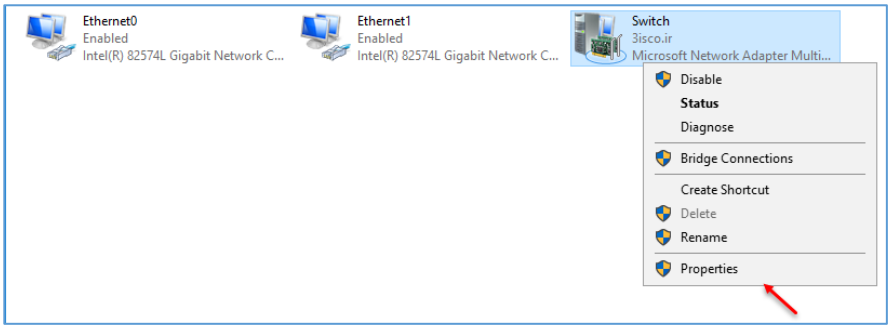


به مانند شکل، اگر شماره‌ی Vlan خاصّی تعریف کردید، می‌توانند گزینه‌ی Specific VLAN را انتخاب و نام شماره‌ی Vlan را وارد کنید تا سرور با سوئیچ ارتباط برقرار کند و دچار مشکل نشود.

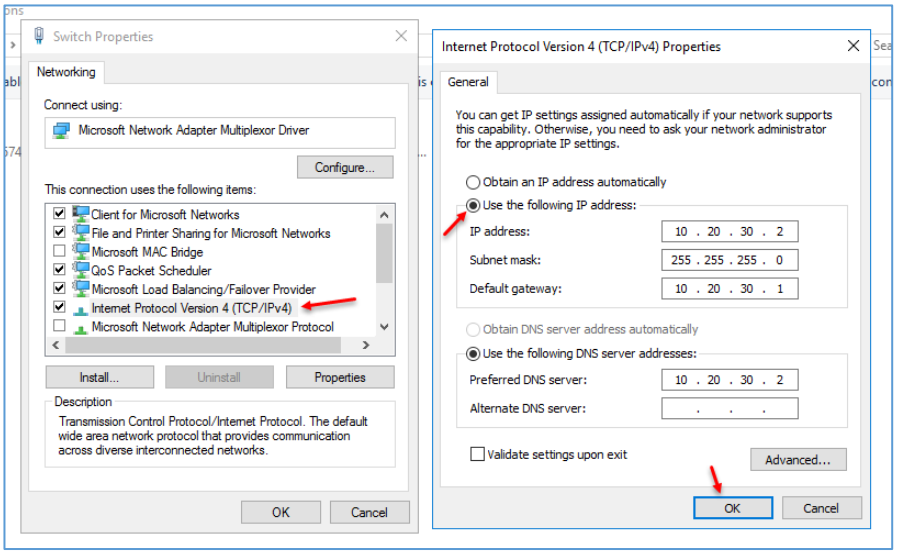
نکته: اگر در مورد VLAN، اطّلاعاتی ندارید، می‌توانید کتاب CCNA بنده را از سایت 3isco.ir دریافت و مطالعه کنید.



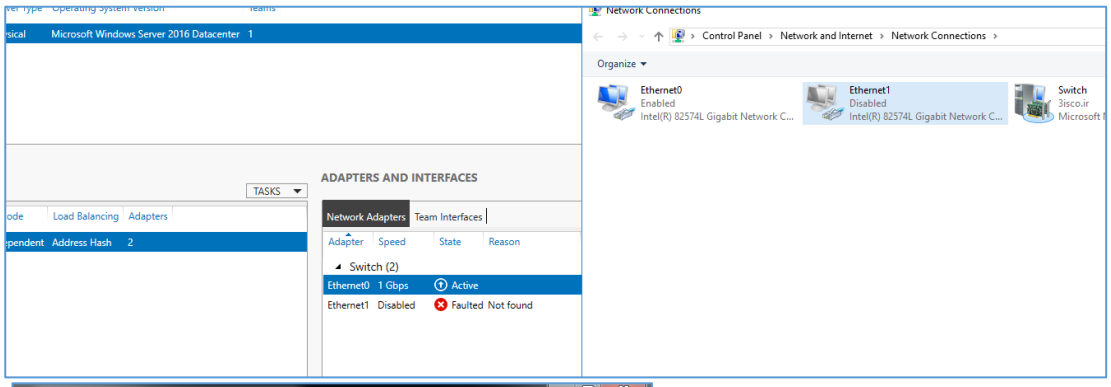
بعد از انجام عملیّات بالا، دوباره وارد Local Server شوید و اگر به قسمت NiC Teaming توجّه کنید، Enabled شده است و برای اینکه آدرس IP سرور را ست کنید باید بر روی Assigned by DHCP کلیک کنید.



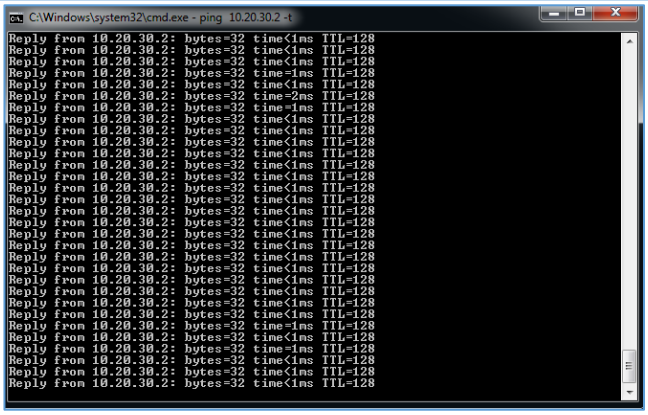
در این صفحه، دو کارت شبکه را مشاهده می‌کنید، به همراه نام Switch که با هم ایجاد کردیم را مشاهده می‌کنید، برای اینکه آدرس IP سرور را ست کنید باید بر روی Switch کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.

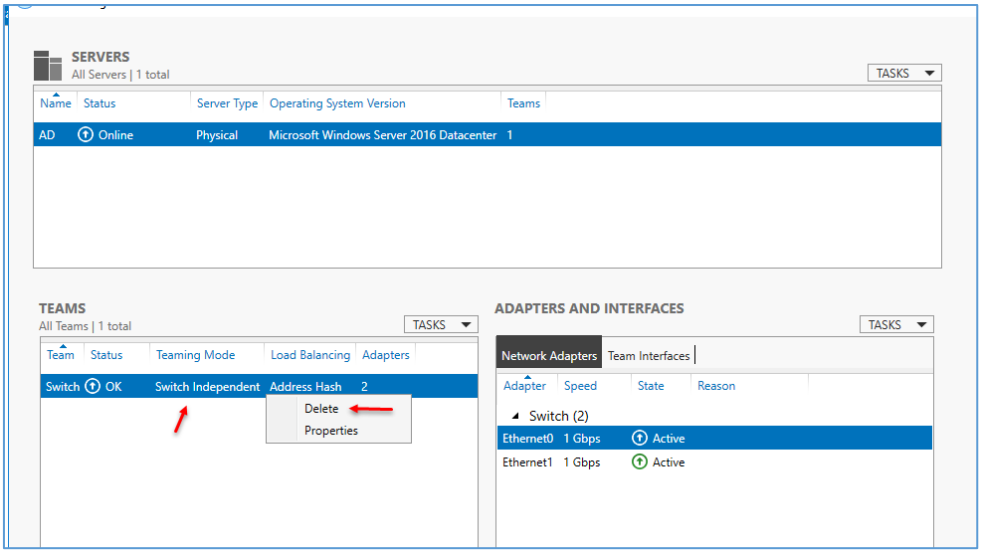


به مانند شکل روبرو آدرس سرور را وارد و بر روی OK کلیک کنید.

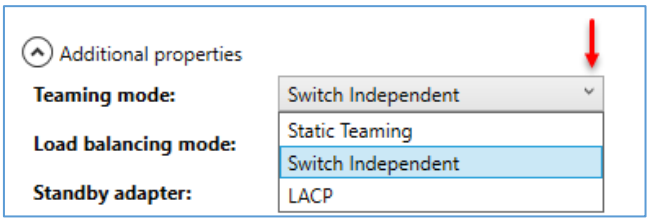


بعد از فعّال شدن سرویس، اگر یکی از کارت‌های شبکه به هر دلیل از کار بیفتد، دسترسی به سرور حتّی برای چند لحظه نیز قطع نخواهد شد و دسترسی پایدار خواهد بود؛ در شکل روبرو Ping سرور مورد نظر، یعنی سرور AD را مشاهده می‌کنید که هیچگونه Time out مشاهده نشده است.





تا اینجا، کار با این سرویس را فرا گرفتیم و حال می‌خواهیم این سرویس را غیر فعّال کنیم که برای این کار باید به مانند شکل در قسمت TEAMS بر روی Team مورد نظر خود کلیک راست کنیم و گزینه‌ی Delete را انتخاب کنیم.



روش‌های دیگری، مانند Static Teaming و LACP وجود دارد که این روش‌ها اگر انتخاب شوند باید سوئیچ-هایی مربوط به آنها نیز در این حالت تنظیم شوند تا بتوانند با هم ارتباط برقرار کنند.

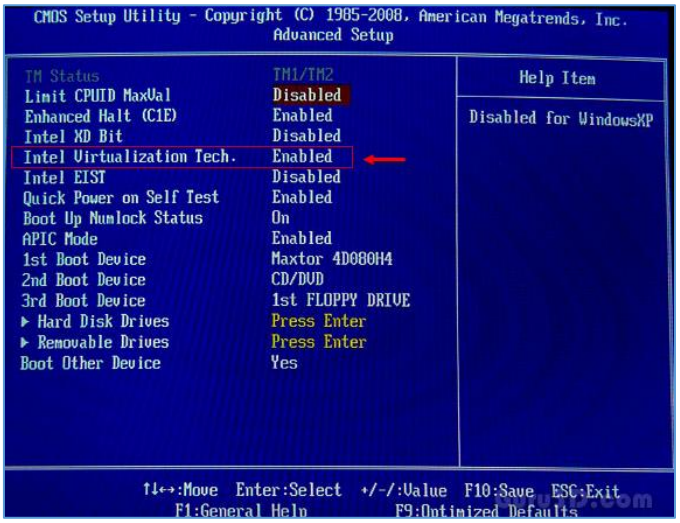
پس در کل، نتیجه می‌گیریم حالت پیش‌فرض، بهترین حالت است و از عملکرد بسیار عالی در شبکه برخوردار است و با هر سوئیچی کار خواهد کرد، توجّه داشته باشید از این سرویس می‌توانید در سرورهایی که انتقال اطّلاعات در آن زیاد است، مانند فایل سرور، دیتابیس و... استفاده کنید تا دسترسی به اطّلاعات برای کاربران به سرعت انجام پذیرد.

نصب و راه‌اندازی سرویس Hyper-V:



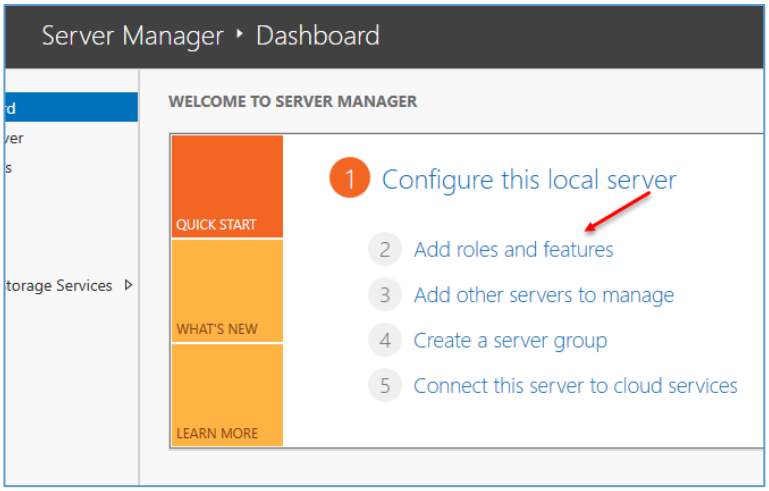
این سرویس، یک سرویس مجازی‌سازی است که در نسخه‌های قبلی ویندوز سرور وجود داشت و در نسخه‌ی ۲۰۱۶ با کیفیّت بهتری ارائه شده است، در ادامه با نحوه‌ی کار و راه‌اندازی آن آشنا خواهیم شد.

برای راه‌اندازی سرور Hyper-V باید سرور شما از مجازی‌سازی پشتیبانی کند، یعنی پردازنده‌ی شما باید این امکان را داشته باشد؛ در بیشتر پردازنده‌های جدید این امکان وجود دارد و برای فعّال‌سازی Virtalization و یا همان، مجازی‌سازی در هر سیستم باید وارد Bios مربوط به Mainboard شوید و بعد از آن در تنظیمات مربوط به CPU باید گزینه‌ی Intel Virtualization را فعّال کنید.

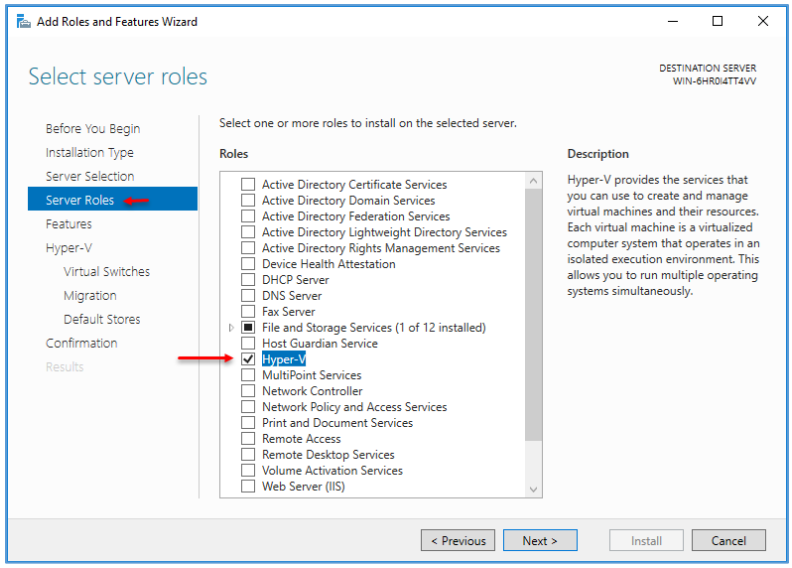


در هر Mainboard، گرافیک کار فرق می کند، امّا گزینه‌های آن، به مانند شکل روبرو ثابت است.

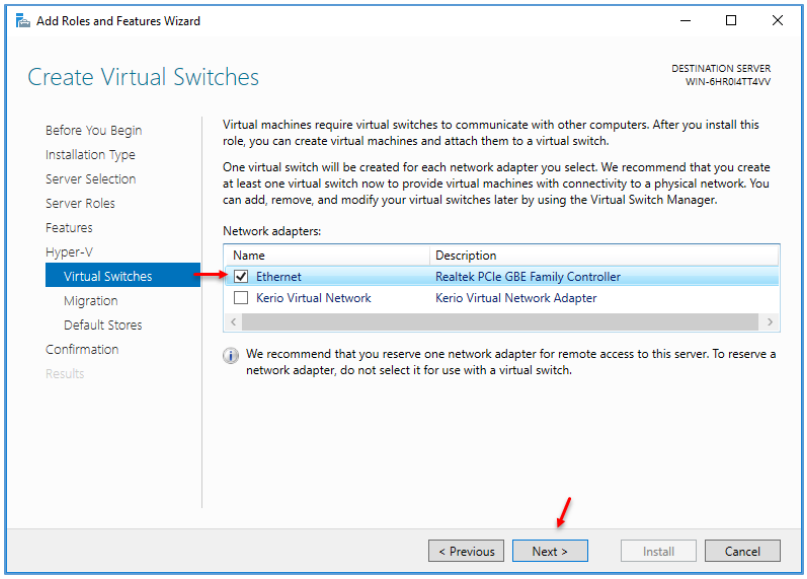
از نظر سخت‌افزاری، سروری که بر روی آن، سرویس Hyper-V نصب می‌شود باید منابع خوبی داشته باشد، مانند رم بالا، CPU با سرعت و تعداد هسته‌ی بالا، هارد دیسک با سرعت و حجم بالا، در کل باید سرور از نظر سخت‌افزاری، کارایی لازم را برای مجازی‌سازی داشته باشد.



برای راه‌اندازی سرویس Hyper-V وارد ویندوز سرور ۲۰۱۶ شوید و Server Manager را اجرا کنید و در صفحه‌ی باز شده بر روی Add roles and features کلیک کنید.

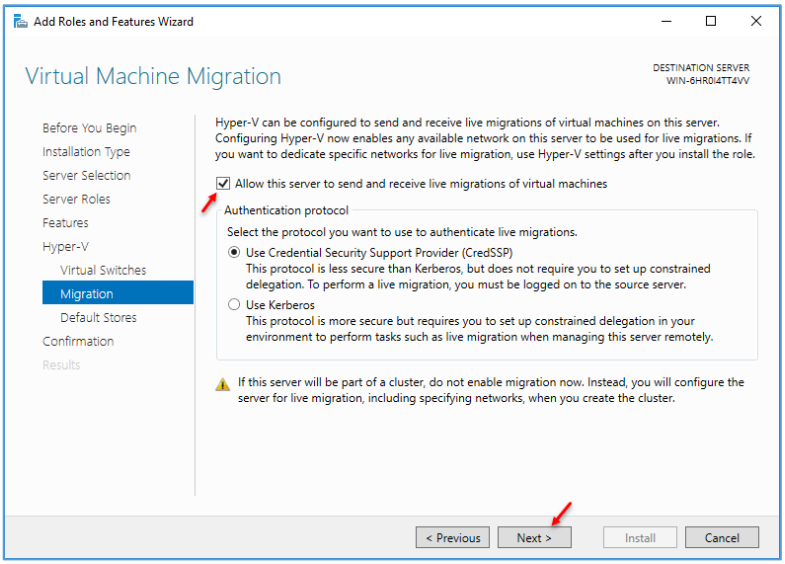


در این صفحه، گزینه‌ی Hyper-v را انتخاب و بر روی Next کلیک کنید و در آخر بر روی Install کلیک کنید تا سرویس مورد نظر نصب شود.



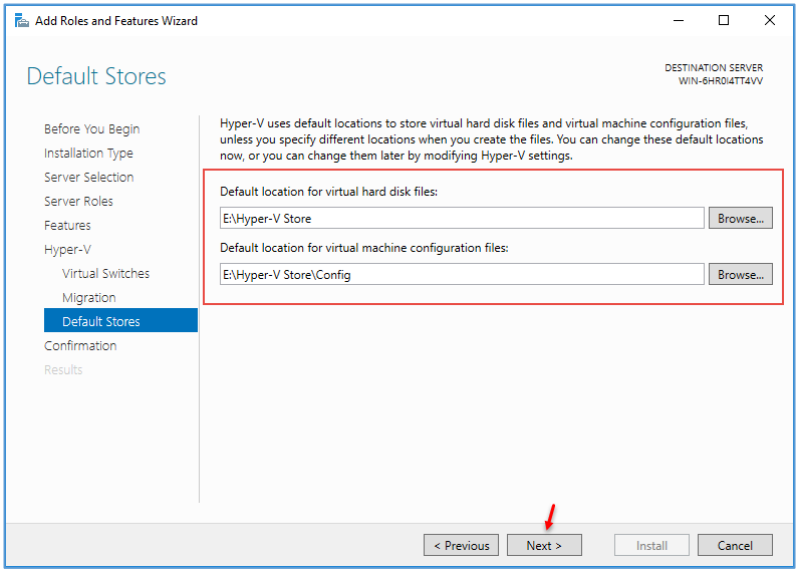
در این صفحه باید کارت شبکه‌ی اصلی سیستم خود را انتخاب کنید تا عملیّات سوئیچینگ روی آن انجام شود.

بر روی Next کلیک کنید.



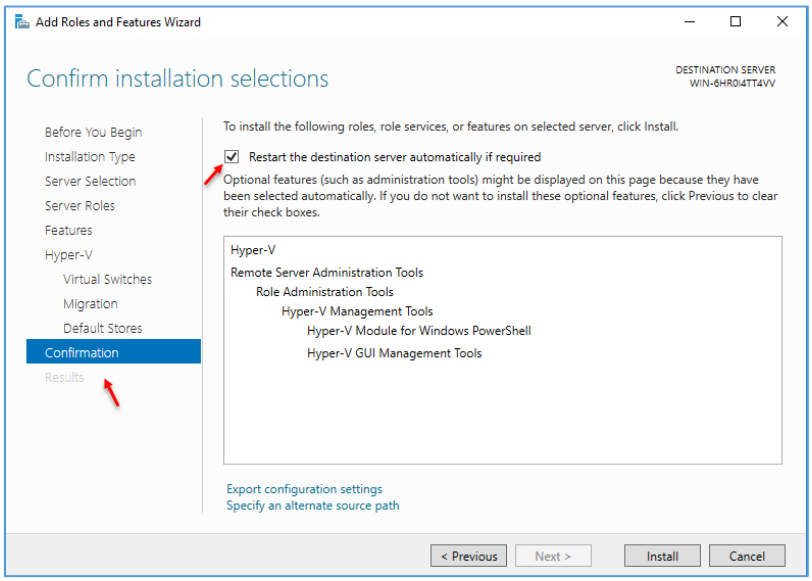
در این صفحه، تیک گزینه‌ی مورد نظر را انتخاب کنید که با این کار به این سرور و این سرویس، اجازه‌ی ارتباط با سرور و سرویس دیگر در محلّ دیگر را می‌دهید که در ادامه، در مورد این موضوع بحث خواهیم کرد.

بر روی **Next** کلیک کنید.

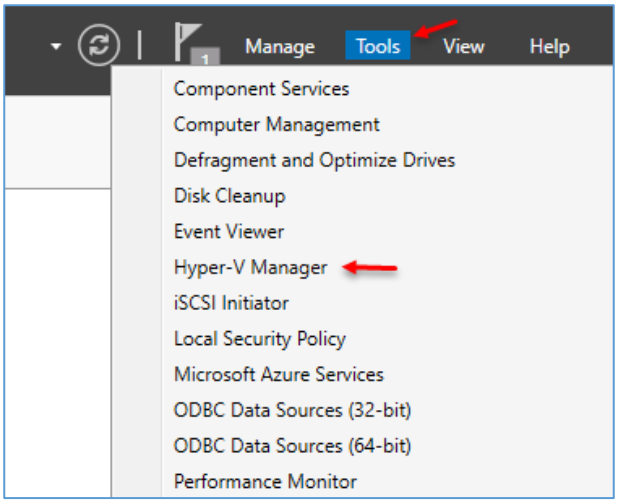


در این صفحه باید محلّ ذخیره‌سازی اطّلاعات هارد دیسک و تنظیمات ماشین مجازی را وارد کنید، سعی کنید محلّ مورد نظر دارای حجم باشد.

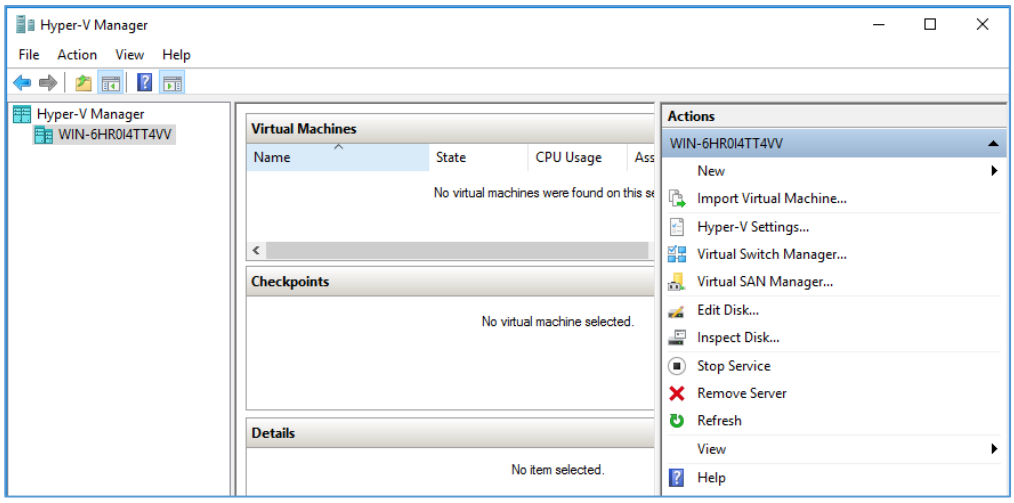
بر روی **Next** کلیک کنید.



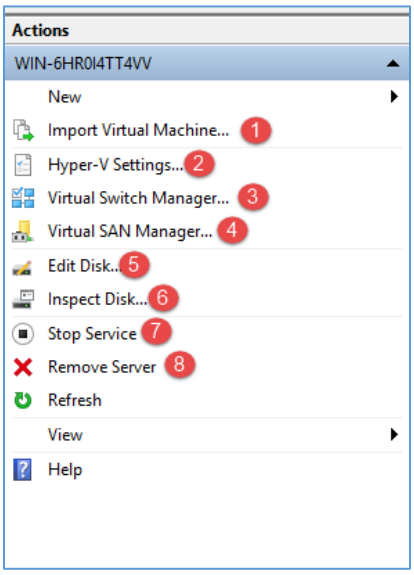
در این صفحه، تیک گزینه‌ی **Restart** را انتخاب و بر روی **Install** کلیک کنید.



بعد از نصب وارد Server Manager شوید و از منوی Tools، گزینه‌ی Hyper-V Manager را اجرا کنید.

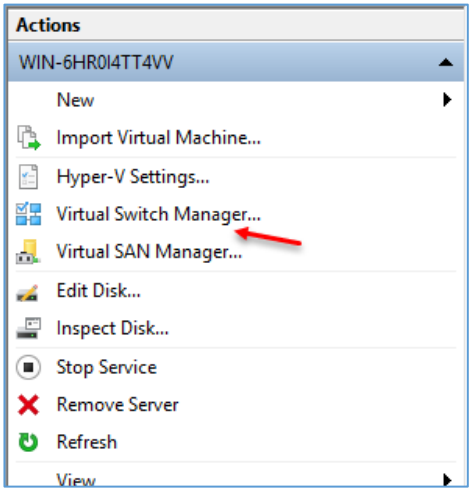


در شکل روبرو، سرویس Hyper-V را مشاهده می‌کنید که نسبت به ورژن ۲۰۱۲، تغییر خاصّی نداشته است؛ در سمت چپ، نام سرور یا سیستم شما نوشته شده است و در سمت راست، ابزارهایی جهت ایجاد، مدیریّت و حذف ماشین مجازی قرار دارد و در وسط صفحه، وضعیّت ماشین‌های مجازی که در ادامه ایجاد می‌کنید، مشخّص می‌شود.

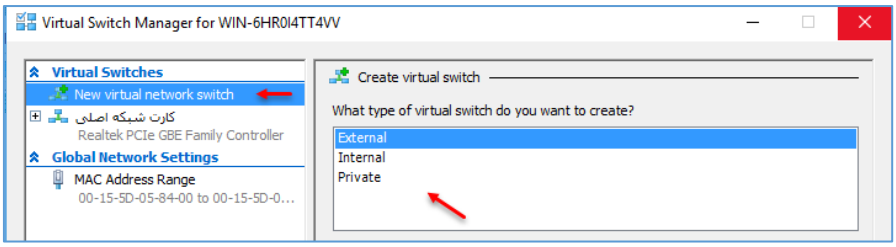


در قسمت سمت راست سرویس، گزینه‌های مختلفی را مشاهده می‌کنید، گزینه‌ی یک برای وارد کردن یک ماشین مجازی است که آن را قبلاً ایجاد کردید، گزینه‌ی دوّم مربوط به تنظیمات سرویس Hyper-V است که در ادامه، توضیحات لازم را خواهیم داد، گزینه‌ی سوّم مربوط به Switch سرویس است که برای ایجاد کارت شبکه‌ی مجازی کاربرد دارد، گزینه‌ی چهارم مربوط به SAN یا همان، Storage Area Network که روشی برای ذخیره‌سازی اطّلاعات است که در این سرویس، تنظیماتی برای ارتباط با آنها تعبیه شده است.

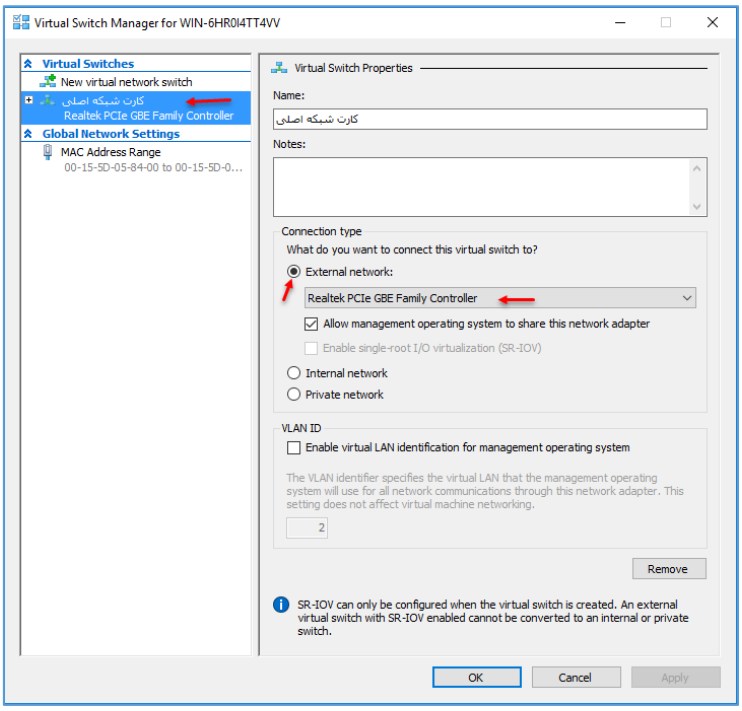
گزینه‌ی شماره‌ی پنج برای مدیریّت هارد دیسک‌های مجازی است که آنها را موقع ایجاد ماشین مجازی و یا از جایی دیگر، ایجاد می‌کنید، شماره‌ی شش، یعنی Inspect disk برای نمایش جزئیّات یک هارد دیسک مجازی است که می‌توانید اطّلاعاتی از حجم، زمان ایجاد و... را دریافت کنید، گزینه‌ی هفت برای غیر فعّال کردن سرویس Hyper-V است و گزینه‌ی هشت نیز برای حذف کردن سرور در لیست سرویس Hyper-V است.

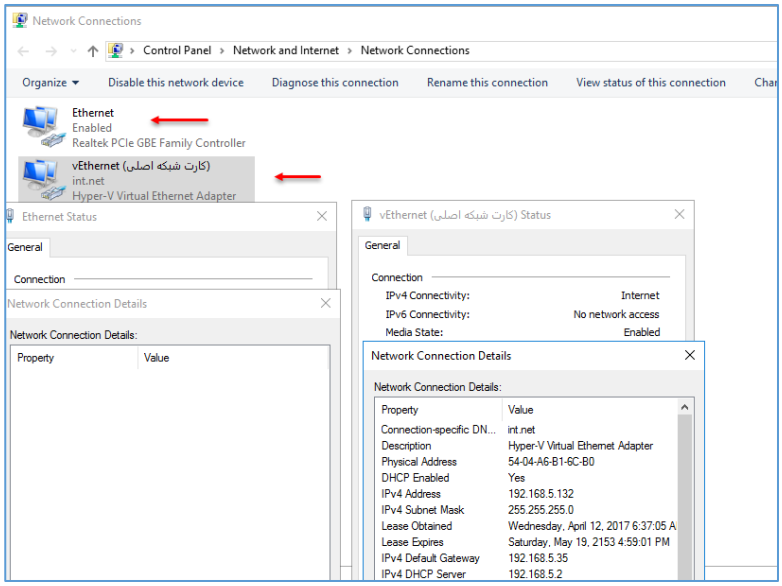


برای شروع کار باید کارت شبکه‌ی مربوط به سرویس Hyper-V را تنظیم کنید، برای این کار از سمت راست بر روی Virtual Switch Manager کلیک کنید.

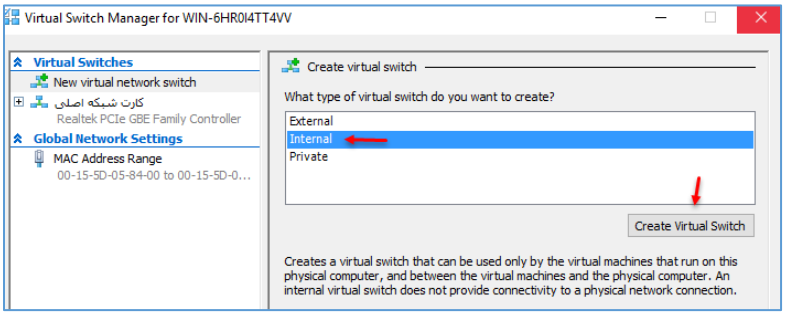


اگر در این صفحه، از سمت چپ بر روی New Virtual Network Switch کلیک کنید، سه گزینه برای شما به نمایش در خواهد آمد که اگر External را انتخاب کنید، می‌توانید یک کارت شبکه‌ی مجازی ایجاد کنید که توانایی ارتباط با کارت شبکه‌ی اصلی را داشته باشد، به صورت پیش‌فرض، یک کارت شبکه از نوع External ایجاد شده است و به مانند شکل روبرو به کارت شبکه‌ی اصلی سیستم شما که نام آن، Realtek... است متّصل شده است، توجّه داشته باشید در قسمت Name می‌توانید به دلخواه، اسم کارت شبکه را به فارسی و انگلیسی وارد کنید.

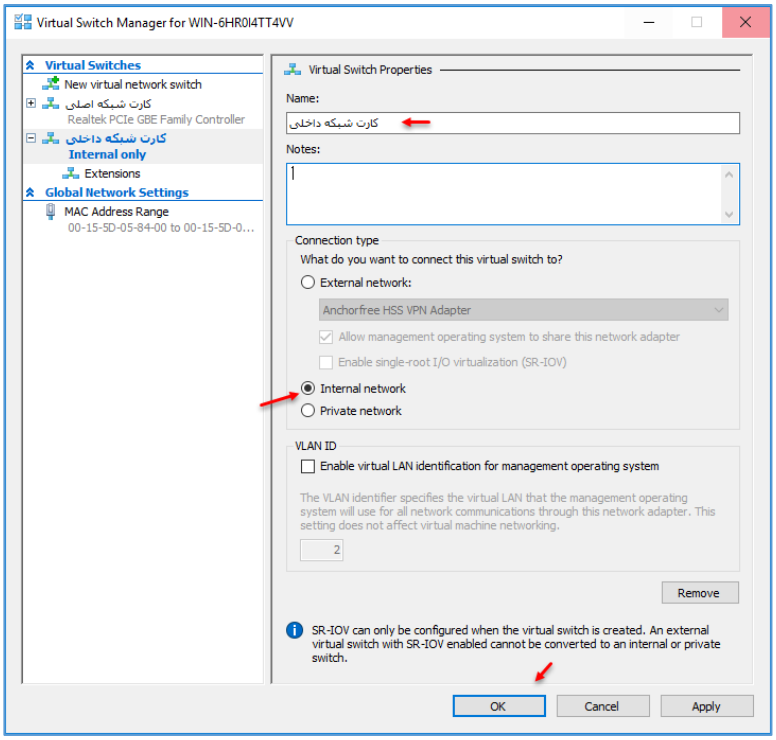




اگر وارد Network Connections شوید، به مانند شکل روبرو، دو کارت شبکه را مشاهده خواهید کرد که Ethernet، همان کارت شبکه-ی اصلی ما است و در قسمت اطّلاعات IP، هیچ گزینه‌ای ندارد، امّا کارت شبکه vEthernet، همان کارت شبکه‌ی مجازی است که با هم ایجاد کرده بودیم و اطّلاعات IP آن نیز مشخّص شده است.

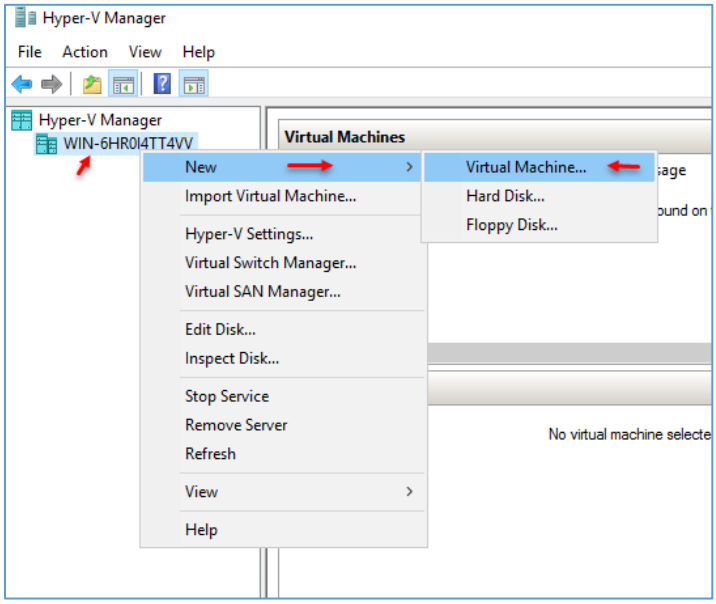


کارت شبکه‌ی دیگری که در لیست وجود دارد، Internal است که مختصّ ارتباط ماشین مجازی با ماشین مجازی دیگر است و توانایی ارتباط با کارت شبکه‌ی خارجی یا همان اصلی را دارد، امّا اگر گزینه‌ی Private را انتخاب کنید، می‌توانید یک ارتباط داخلی بین ماشین مجازی با ماشین مجازی دیگر ایجاد کنید و دیگر نمی‌توانید با سیستم‌های اصلی یا فیزیکی ارتباط برقرار کنید.

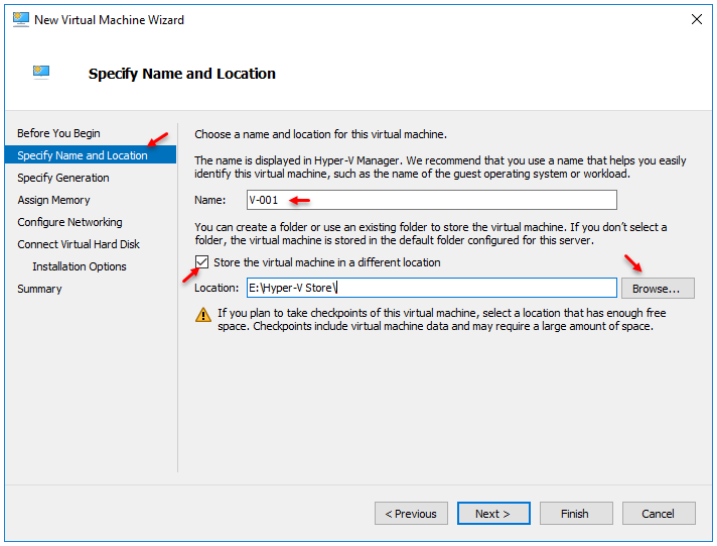


برای شروع کار با کلیک بر روی Create Virtual Switch، یک کارت Internal ایجاد کنید.در شکل روبرو می‌توانید، نام کارت شبکه‌ی خود را در قسمت Name وارد کنید و گزینه‌ی Internal Network را انتخاب و بر روی OK کلیک کنید.

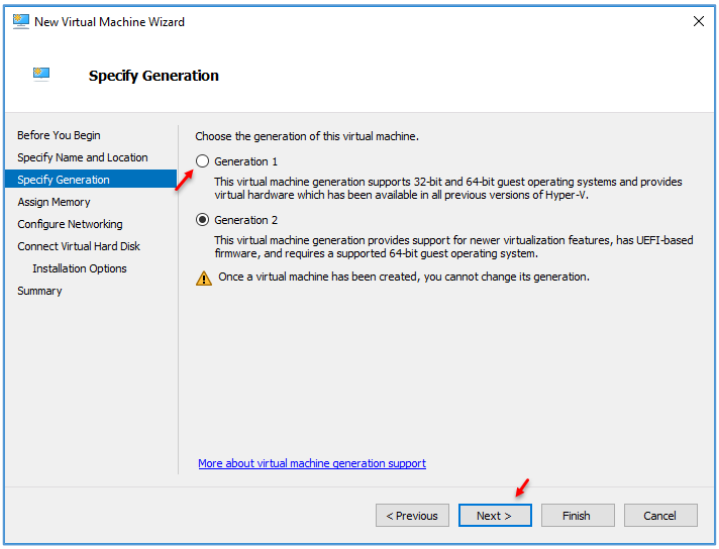
ایجاد ماشین مجازی:



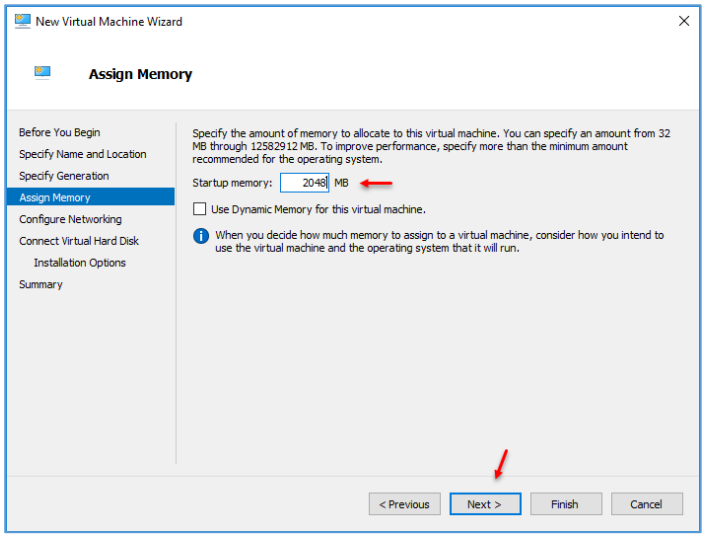
بعد از تنظیم کارت شبکه می‌توانید ماشین مجازی خود را ایجاد کنید، برای ایجاد ماشین مجازی وارد سرویس Hyper-V شوید و بر روی نام سرور خود کلیک راست کنید و از قسمت New، گزینه‌ی Virtual Machine انتخاب کنید.



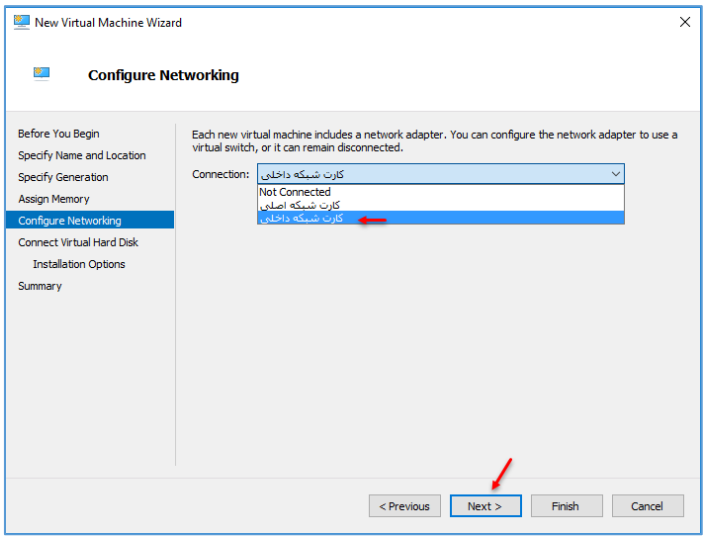
در این قسمت باید نام ماشین مجازی خود را در قسمت Name وارد کنید و اگر بخواهید محلّ ذخیره‌سازی ماشین مجازی را تغییر دهید باید تیک گزینه‌ی Store the virtual... را انتخاب و بر روی Browse کلیک کنید و مسیر را مشخّص کنید.



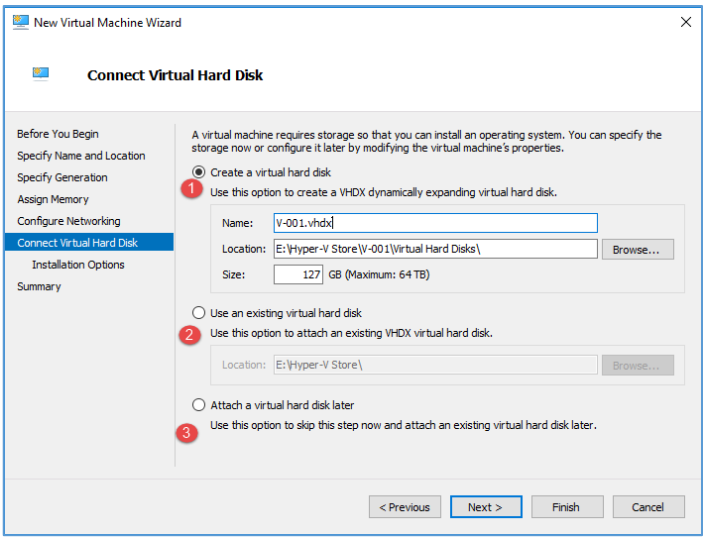
در این صفحه، دو گزینه وجود دارد که گزینه‌ی اوّل برای سیستم‌هایی که ورژن 32 bit را پشتیبانی می‌کنند و گزینه‌ی دوّم برای سخت‌افزارهای جدید که 64 bit را پشتیبانی می‌کنند، است؛ گزینه‌ی اوّل را انتخاب و بر روی Next کلیک کنید.



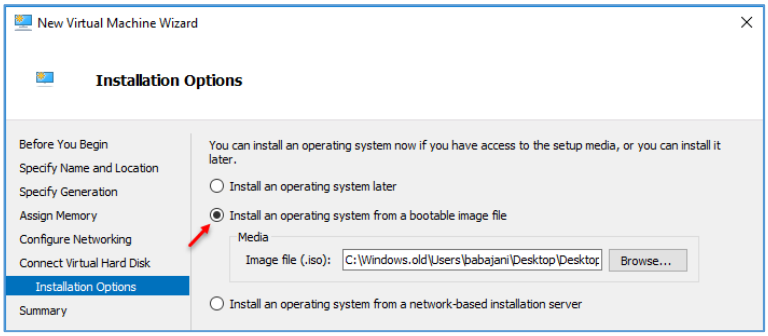
در قسمت Memory Startup، مقدار حافظه‌ی مورد نیاز که می‌خواهید به سرور مجازی خود اختصاص دهید را وارد کنید، اگر تیک گزینه‌ی Dynamic Use Memory را فعّال کنید، در صورت نیاز از حافظه‌ی رم استفاده خواهد کرد، یعنی اگر این گزینه، فعّال باشد، شاید حافظه‌ی رم بیشتر و یا کمتر از مقداری شود که شما وارد کرده‌اید،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



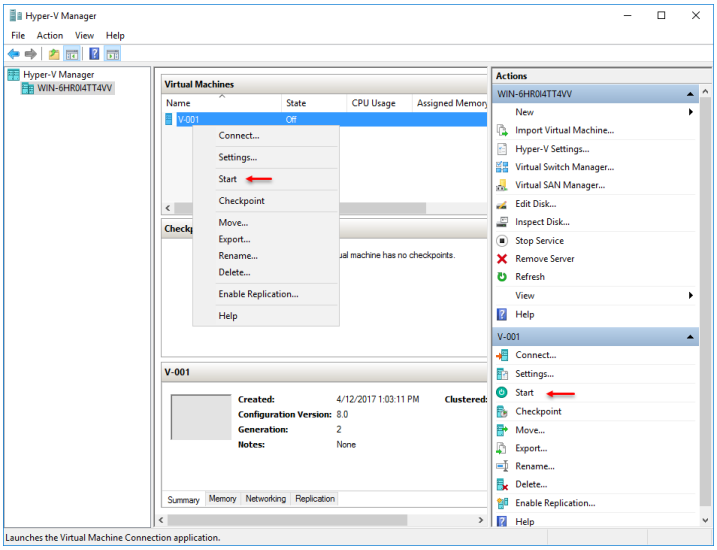
در این صفحه باید کارت شبکه‌ای که با هم ایجاد کردیم را انتخاب کنید، کارت شبکه‌ی داخلی را انتخاب و بر روی Next کلیک کنید.



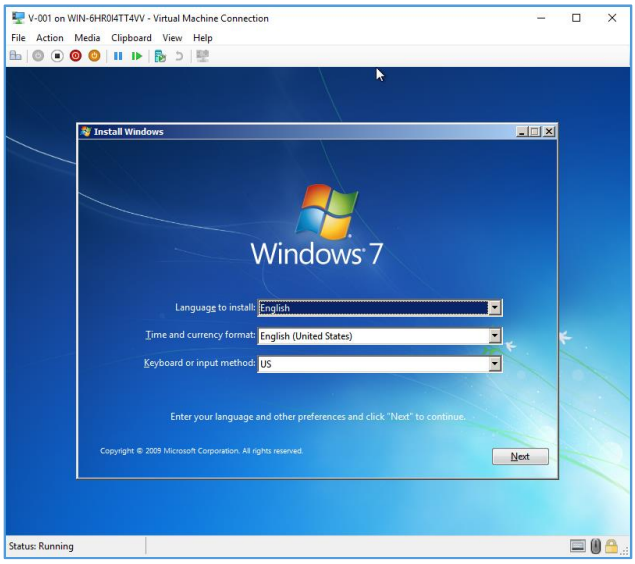
در قسمت اوّل می‌توانید نام هارد دیسک مجازی خود را وارد و مسیر آن را مشخّص کنید که در همان مسیری که قبلاً وارد کردید، ذخیره خواهد شد، بعد از آن مقدار حافظه‌ی آن را تخصیص دهید. در قسمت دوّم می‌توانید از هارد دیسک‌هایی استفاده کنید که قبلاً ایجاد کرده‌اید و با انتخاب قسمت سوّم می‌توانید این قسمت را بعداً انجام دهید، فعلاً گزینه‌ی اوّل را انتخاب و بر روی Next کلیک کنید.



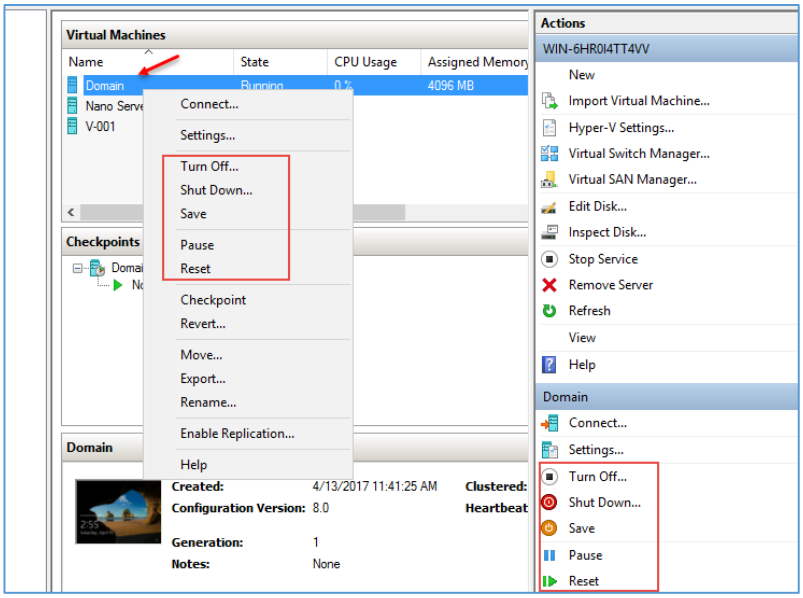
در این قسمت باید DVD مربوط به ویندوز مورد نظر خود را در سیستم قرار دهید و گزینه‌ی Physical DVD/CD را انتخاب کنید و یا اگر از ویندوز، Image تهیّه کردید، می‌توانید در قسمت File Image بر روی Browse کلیک کنید و فایل Image مورد نظر را معرّفی کنید، بعد از انجام این کار بر روی Next کلیک کنید.



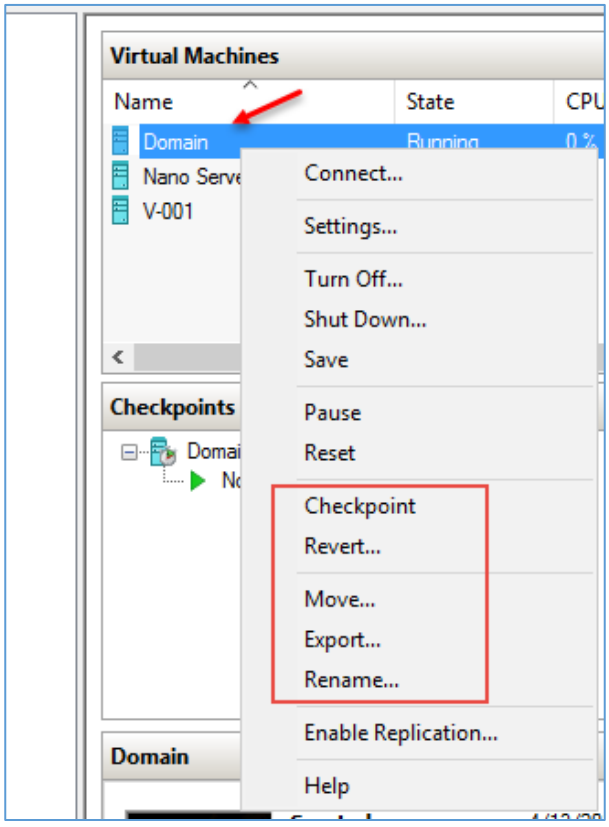
بعد از ایجاد ماشین مجازی، نام آن در لیست قابل مشاهده است که با کلیک کردن بر روی Start، ماشین مجازی روشن می‌شود، البتّه همین کار را به مانند شکل از سمت راست نیز می‌توانید انجام دهید.



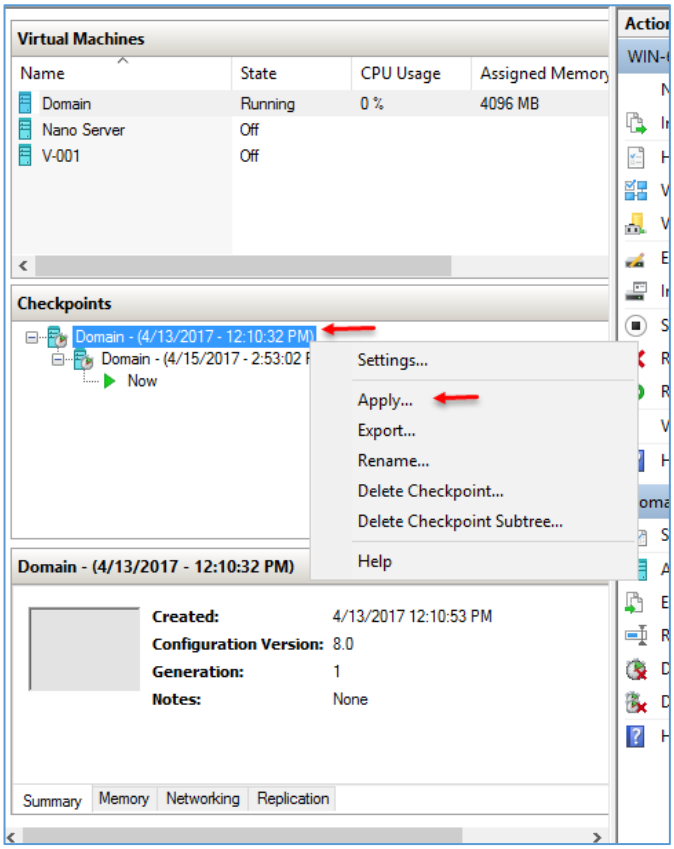
همانطور که مشاهده می‌کنید، ماشین مورد نظر روشن شده است و ویندوز ۷ برای نصب آماده است، ویندوز را نصب کنید تا در ادامه از آن استفاده کنید.



گزینه‌هایی دیگری نیز بعد از روشن کردن ماشین مجازی فعّال می‌شوند، مانند Turn Off که برای خاموش کردن سریع ماشین مجازی می‌باشد، مانند این است که برق یک سیستم را قطع کنید. گزینه‌ی shutdown برای خاموش کردن نرم‌افزاری سرور است، مانند اینکه داخل ویندوز بر روی shutdown کلیک کنید، گزینه‌ی Save در هر حالتی که ماشین مجازی قرار دارد، اطّلاعات را ذخیره و ماشین را غیر فعّال می‌کند که اگر دوباره فعّال شود، همان نرم‌افزارها با همان حالت قبل، فعّال خواهند شد، گزینه‌ی Pause برای توقّف سریع ماشین است که تفاوت آن با حالت Save این است که اطّلاعات در حافظه ذخیره نمی‌شوند، بلکه عملکرد ماشین متوقّف می‌شود که با فعّال کردن دوباره‌ی ماشین، کار خود را ادامه می‌دهد، این حرکت برای زمانی به کار می‌آید که ماشین مجازی شما رم زیادی را استفاده کرده باشد و بخواهید آن را برای دقایقی متوقّف کنید، گزینه‌ی Reset نیز برای Restart کردن سریع ماشین کاربرد دارد.



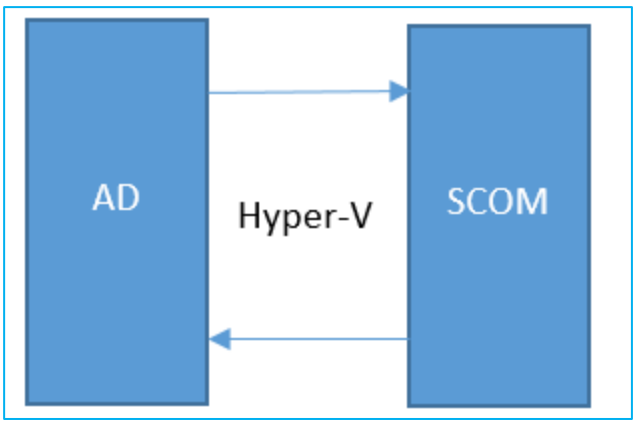
گزینه‌های دیگری نیز وجود دارد، گزینه‌ی Checkpoint برای ایجاد یک کپی از ماشین مورد نظر تا آن تاریخ است که اگر بعد از آن تاریخ، ماشین شما دچار مشکل شد، می‌توانید وضعیّت ماشین را به همان تاریخی برگردانید که Checkpoint را روی آن فعّال کردید، اگر توجّه کنید در وسط صفحه، وضعیّت Checkpoint نوشته شده است، گزینه‌ی Revert برای برگرداندن ماشین به آخرین Checkpoint است، گزینه‌ی Move برای انتقال ماشین مجازی از یک مکان به مکان دیگر است، گزینه‌ی Export نیز برای ایجاد یک نسخه از ماشین در محلّ دیگر با حفظ نسخه‌ی اوّلیّه در همان محل است، گزینه‌ی Rename نیز برای تغییر نام ماشین کاربرد دارد.



زمانی که شما از ابزار Checkpoints استفاده می‌کنید، به مانند شکل روبرو در قسمت Checkpoints تمام تاریخ‌هایی که از این ابزار استفاده کردید، مشخّص شده است، اگر بخواهید از آن تاریخ مورد نظر استفاده کنید باید بر روی همان تاریخ کلیک راست کنید و گزینه‌ی Apply را انتخاب کنید تا ماشین مورد نظر به همان تاریخ مورد نظر برگردد، گزینه‌ی Export نیز برای استخراج ماشین مجازی در یک مکان جدید برای همان تاریخ است.

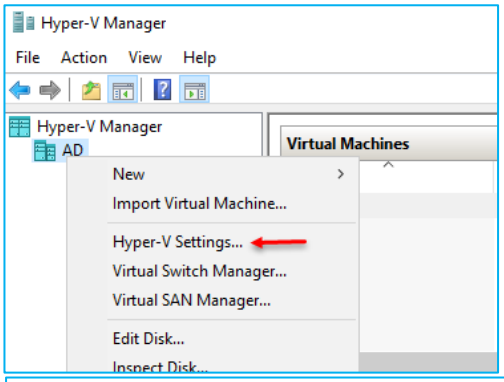
ابزار Replication در سرویس Hyper-V:

یک ابزار خوب و کاربردی برای ایجاد Failover در سرویس Hyper-V است، با استفاده از این ابزار می‌توانید دو سرور Hyper-v داشته باشید و ماشین مجازی که در یک سرور ایجاد می‌کنید، به صورت اتوماتیک در یک سرور دیگر نیز ایجاد شود تا در صورت از دست رفتن سرور اوّل، بتوانید از ماشین مجازی سرور دوّم استفاده کنید، البتّه باید یک زمان برای ارتباط دو سرور مشخّص کنید تا آخرین تغییرات بین سرورها ردّ و بدل شود.

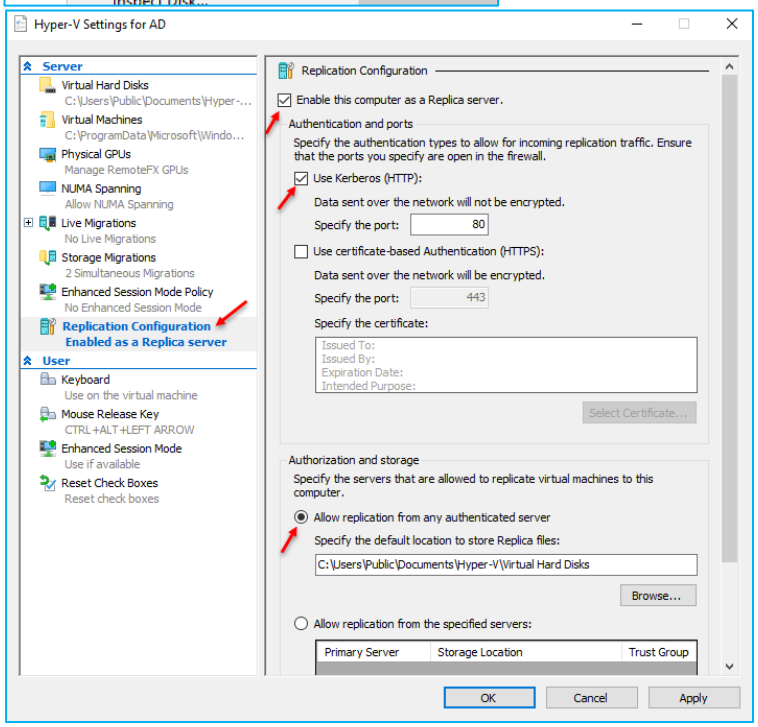


در شکل روبرو دو سرور در نظر گرفتیم که هر کدام دارای ویندوز سرور ۲۰۱۶ هستند و بر روی هر دوی آنها، سرویس Hyper-V فعّال شده است.

در سرور AD، یک ماشین مجازی ایجاد شده که بر روی آن، ویندوز ۷ نصب شده است، در ادامه می‌خواهیم این ماشین را به سرور دیگر انتقال دهیم.



برای شروع وارد سرور AD شوید و سرویس Hyper-V را فعّال کنید، بر روی نام سرور، کلیک راست کنید و گزینه‌ی Hyper-V Settings را انتخاب کنید.

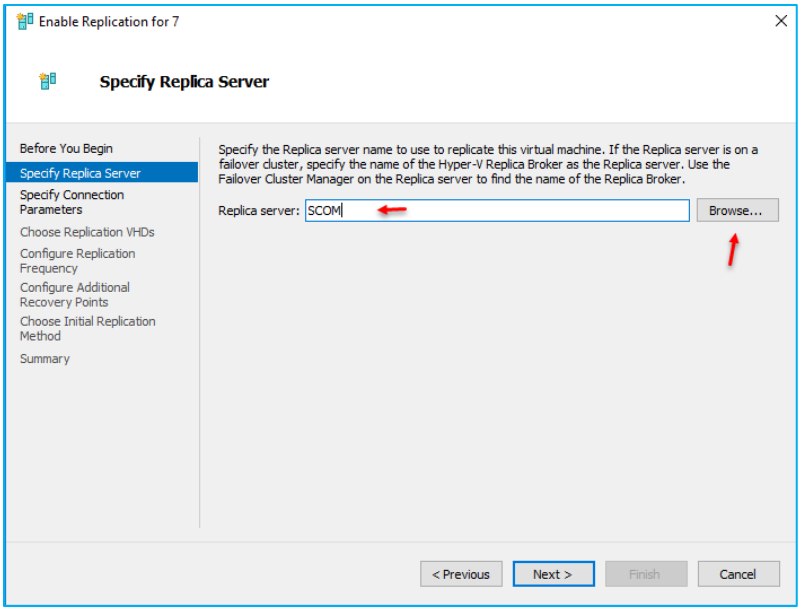


در این صفحه، از سمت چپ وارد گزینه‌ی Replication configuration... شوید، تیک گزینه‌ی Enable this computer... را انتخاب کنید، بعد از این کار می‌توانید روش ارتباط بین دو سرور را انتخاب کنید که در حال حاضر باید گزینه‌ی اوّل، HTTP را انتخاب کنید. در پایین صفحه با انتخاب گزینه‌ی Allow replication from... می‌توانید یک مسیر برای ذخیره‌ی اطّلاعات و فایل‌های ابزار Replica مشخّص کنید؛ بر روی OK کلیک کنید.

نکته‌ی ۱: دقیقاً همین کار را در سرور دوّم انجام دهید، در این قسمت، سرور دوّم، SCOM در نظر گرفته شده است، همانطور که اشاره کردیم، سرویس Hyper-V بر روی آن سرور نیز فعّال شده است.

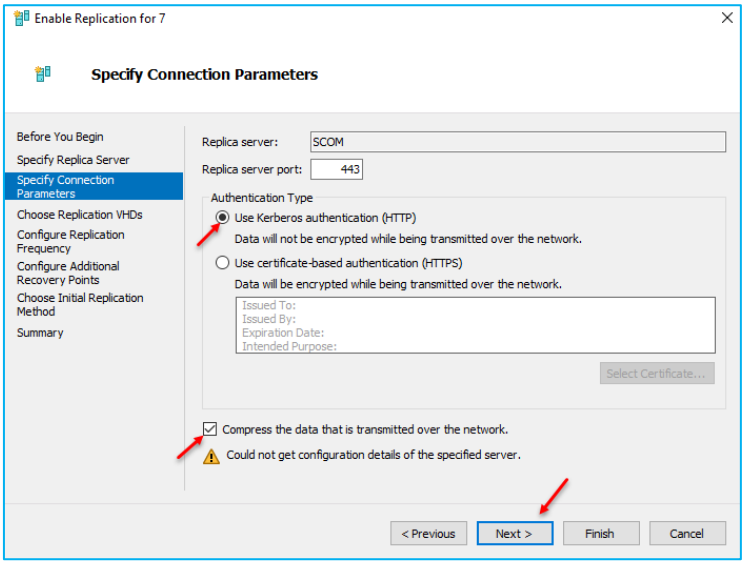
نکته‌ی ۲: هر دو سرور باید به دومین، join شده باشند تا در ارتباط با مشکلی مواجه نشوید.

نکته‌ی ۳: اگر می‌خواهید از این امکان در یک جای واقعی استفاده کنید باید سخت‌افزاری که برای سرور در نظر می‌گیرید، از کیفیّت خوبی برخوردار باشد.

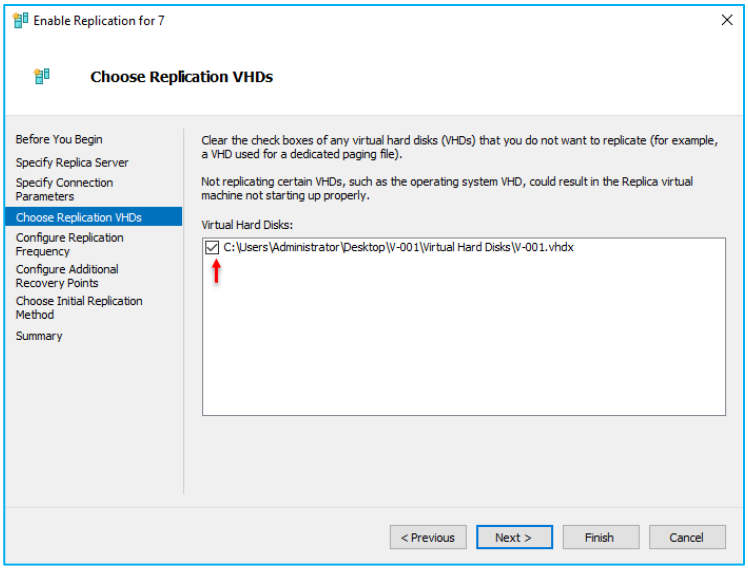


در این صفحه باید نام سرور روبرو برای انجام Replicate را وارد کنید، نام سرور را SCOM وارد کنید، یک بار دیگر بیان می‌کنیم که در سرور روبرو، سرویس Hyper-V فعّال شده است.

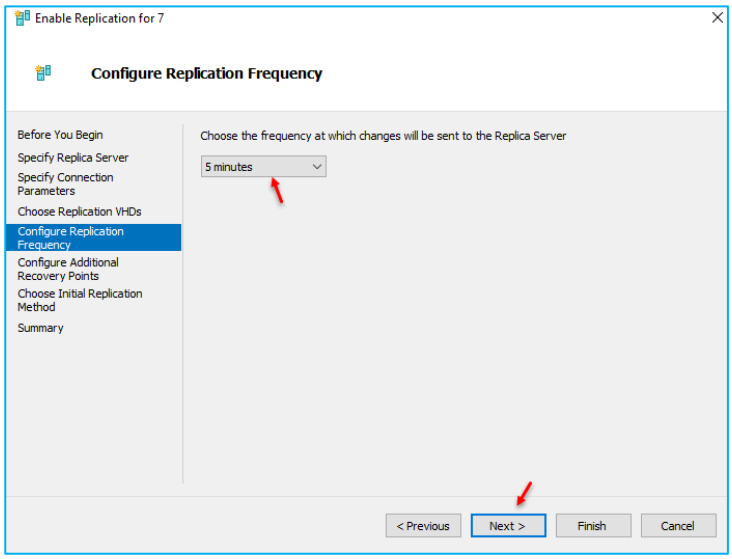
بر روی Next کلیک کنید.



در این صفحه، بعد از تأیید سرور SCOM باید نوع ارتباط امنیّتی را مشخّص کنید، برای ادامه‌ی کار، گزینه‌ی Use Kerberos authentication (HTTP) را انتخاب و بر روی Next کلیک کنید.

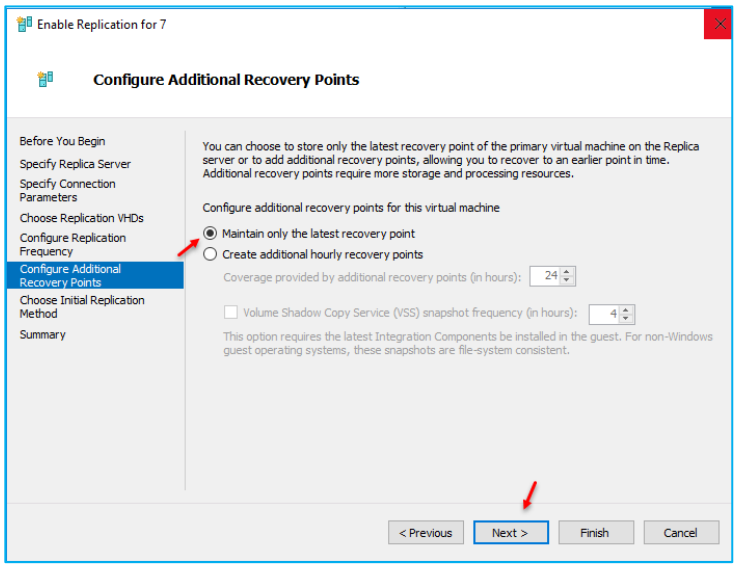


در این صفحه باید هارد دیسک مربوط به ماشین انتخابی مورد نظر را انتخاب و بر روی Next کلیک کنید.

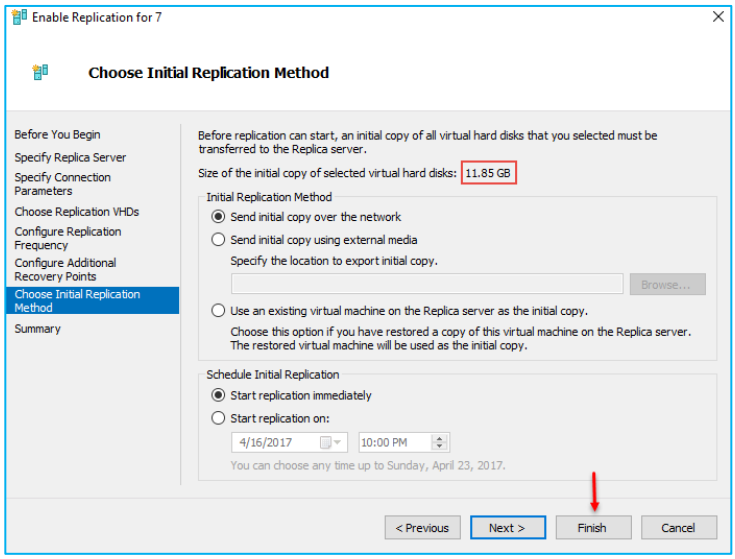


در این قسمت می‌توانید، زمانی را برای ارتباط دو سرور برای انتقال اطّلاعات مشخّص کنید، سعی کنید این زمان، نه زیاد و نه خیلی کم باشد.

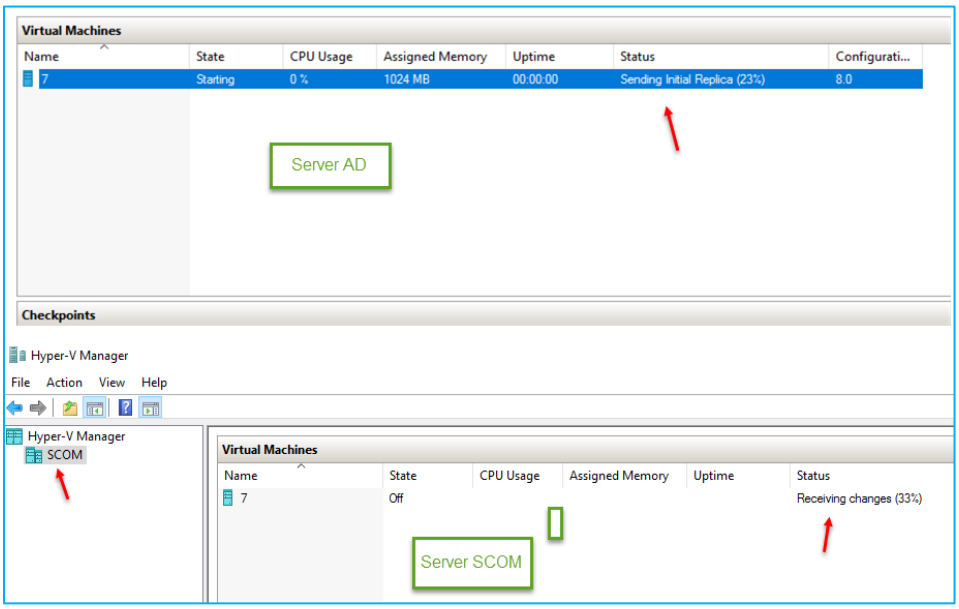
بر روی Next کلیک کنید.



این قسمت، مربوط به ایجاد Recovery Point است تا در صورت بروز خطا بتوانید ماشین را به یک حالت پایدار برگردانید که اگر گزینه‌ی اوّل را انتخاب کنید، یک Recovery Point از ماشین مورد نظر ایجاد می‌کند، گزینه‌ی آخر برای انجام Recovery Point در ساعت‌های مختلف است که تعداد این کار را افزایش می‌دهد؛ بر روی Next کلیک کنید.

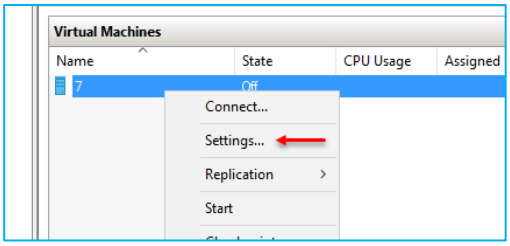


در این صفحه به شما اعلام می‌دارد که هارد دیسک ماشین مجازی مورد نظر، 11.5 گیگ فضا دارد و برای اینکه عملیّات Replicate انجام شود، اوّل باید این هارد به سرور SCOM روبرویی انتقال داده شود که سرور SCOM باید دارای این فضا باشد، در پایین صفحه نیز می‌توانید مشخّص کنید که در چه زمانی این کار انجام شود، بر روی Finish کلیک کنید تا عملیّات Replicate آغاز شود.

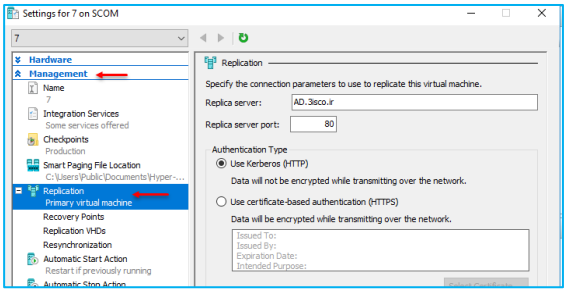


در شکل روبرو، هر دو سرور AD و SCOM در کنار هم قرار گرفته است، اگر به قسمت Status هر یک از سرورها توجّه کنید، در حال انجام Replica هستند که سرور AD در حال Sending و یا همان، ارسال است و سرور SCOM، در حال دریافت اطّلاعات است.

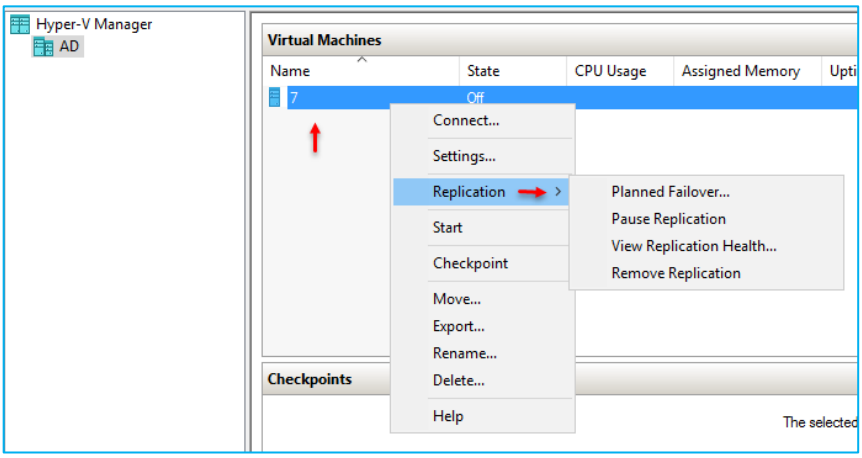
بعد از چند دقیقه، ماشین مورد نظر به صورت کامل به سرور SCOM انتقال داده می‌شود و اگر بعد از این، تغییری در سرور اوّل، یعنی AD بر روی ماشین 7 انجام شود، در سرور دوّم نیز بعد از زمان مشخّص‌شده اعمال می‌شود.



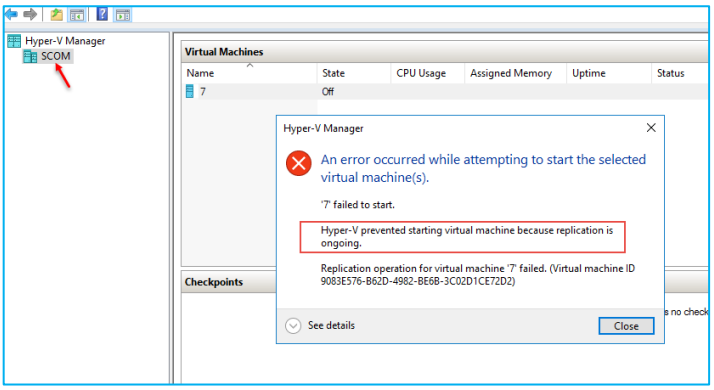
اگر بخواهید دوباره به تنظیمات Replica خود، سری بزنید باید بر روی ماشین مورد نظر کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید.



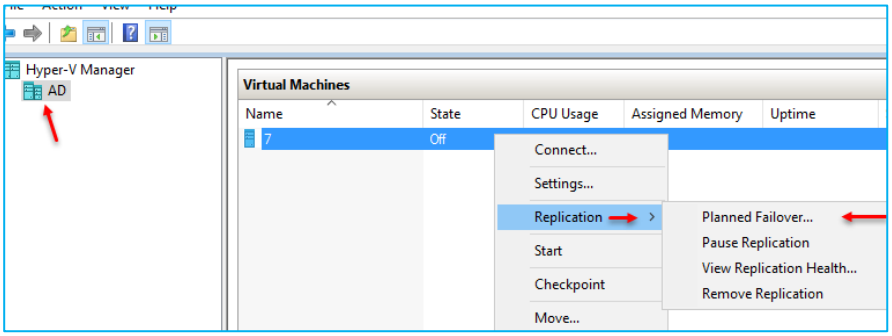
در این صفحه، از سمت چپ وارد قسمت Management شوید و گزینه‌ی Replication را انتخاب کنید، در این صفحه می‌توانید تنظیمات مورد نظر را تغییر دهید.



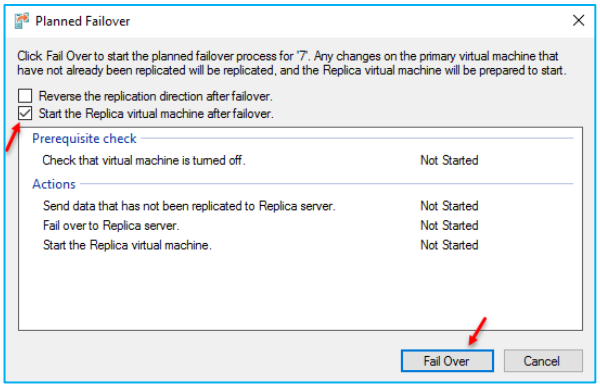
اگر بعد از انجام عملیّات Replica، بر روی ماشین مورد نظر کلیک راست کنید، یک گزینه‌ی جدید با نام Replication ایجاد شده است که دارای چهار گزینه است؛ گزینه‌ی اوّل برای انتقال سرور اجرا کننده‌ی ماشین به سرور دوّم است، گزینه‌ی دوّم، Pause Replication برای متوقّف کردن عملیّات Replicate بین دو سرور است، یعنی اگر تغییری در سرور اوّل ایجاد شود، در سرور دوّم اعمال نخواهد شد، گزینه‌ی سوّم برای بررسی حالت Replication است و گزینه‌ی آخر نیز برای حذف این ابزار بر روی این ماشین مجازی است.



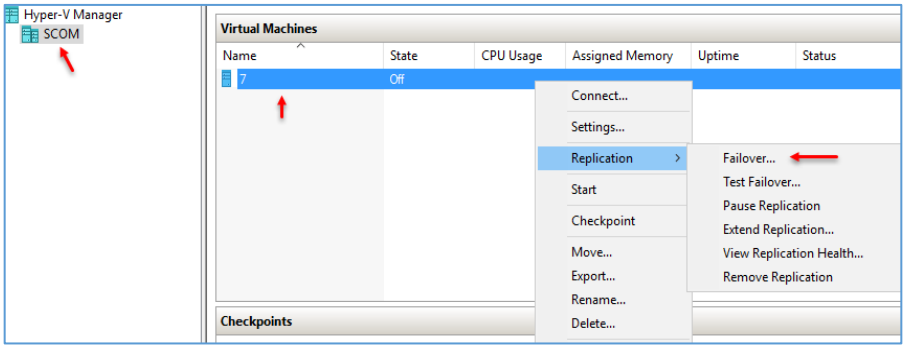
اگر چنانچه بخواهید در سرور دوّم که ماشین به آن انتقال داده شده است، ماشین را روشن کنید با خطای روبرو مواجه می‌شوید که به شما اعلام می‌دارد که ابزار Replication، بر روی سرور دیگر فعّال است، یعنی اینکه سرور اصلی، سرور AD است و ماشین تنها بر روی آن اجرا می‌شود.



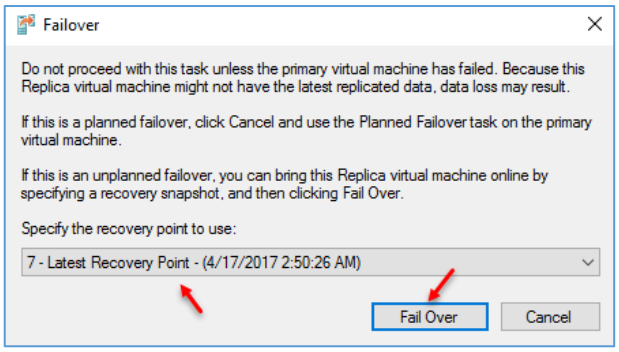
حال اگر بخواهید، سرور دوّم را به عنوان سرور اصلی برای سرویس Replicate در نظر بگیرید باید به مانند شکل روبرو در سرور اصلی، AD بر روی ماشین مورد نظر کلیک راست و از قسمت Replication، گزینه‌ی Planned Failover را انتخاب کنید.



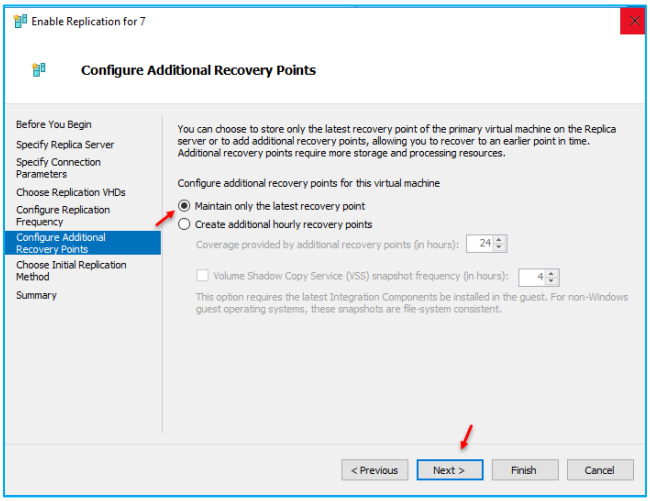
در این صفحه برای انتقال، تیک گزینه‌ی مورد نظر را انتخاب و بر روی Fail Over کلیک کنید تا عملیّات انتقال انجام شود.



اگر چنانچه سرور اصلی از کار بیفتد باید از سرور دوّم برای اجرای ماشین مجازی استفاده کنید، برای این کار باید در سرور دوّم، SCOM بر روی ماشین مجازی مورد نظر کلیک راست کنید و از قسمت Replication، گزینه‌ی Failover را انتخاب کنید.



در این صفحه، آخرین کپی با عنوان Latset Recovery را مشاهده می‌کنید که با انتخاب و کلیک بر روی آن، عملیّات برگشت‌پذیری انجام می‌شود و ماشین مورد نظر بر روی سرور دوّم اجرا خواهد شد.

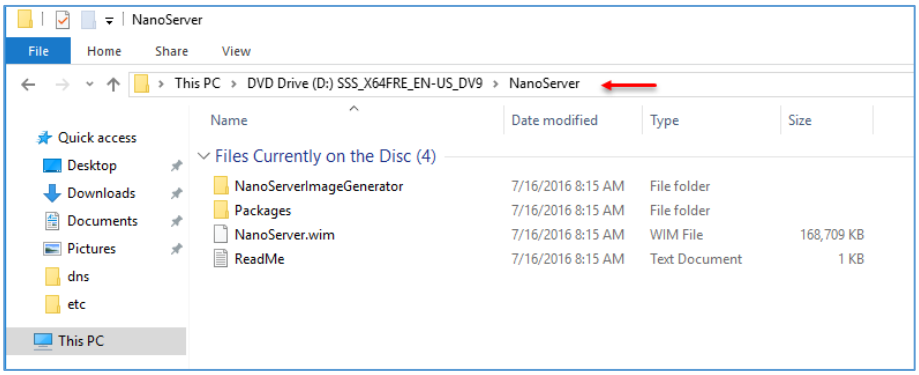


توجّه کنید، اگر در زمان فعّال کردن Replicate، در شکل سمت راست، گزینه‌ی دوّم را انتخاب می‌کردید، حالا در شکل بالا، دارای چندین زمان مختلف برای Latset Recovery بودید.

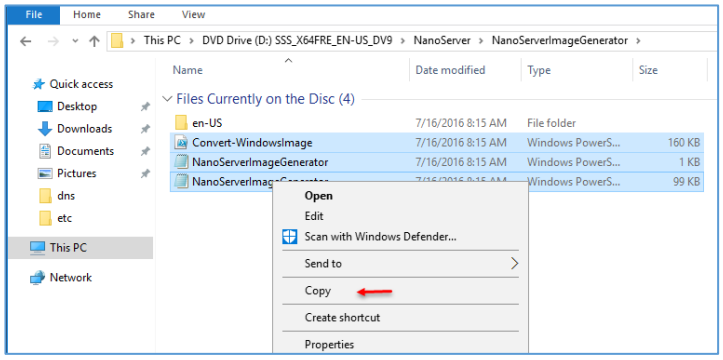
نصب و راه‌اندازی NANO Server:

Nano Server، یک سیستم عامل بسیار کوچک و سریع از مایکروسافت است که برای ارائه‌ی سرویس‌های مختلف ایجاد شده است، این سرویس‌ها می‌تواند، سرویس IIS، DNS و... باشد که این سرویس را در زیر بررسی خواهیم کرد.

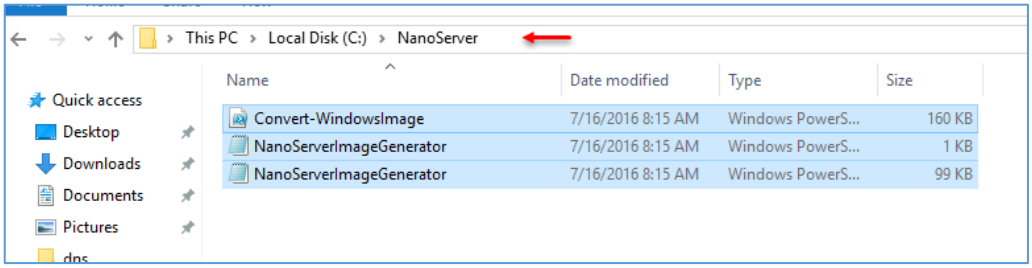
برای شروع، DVD مربوط به ویندوز سرور ۲۰۱۶ را درون دستگاه قرار دهید و وارد ویندوز سرور ۲۰۱۶ شوید.



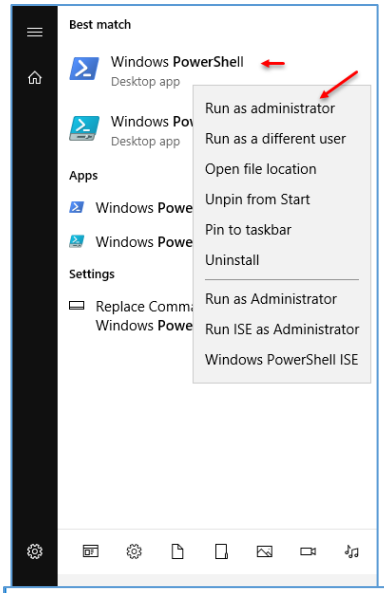
اگر وارد DVD مربوط به ویندوز سرور ۲۰۱۶ شوید، یک پوشه با عنوان NANO Server وجود دارد که اجزای آن، به مانند شکل روبرو است.



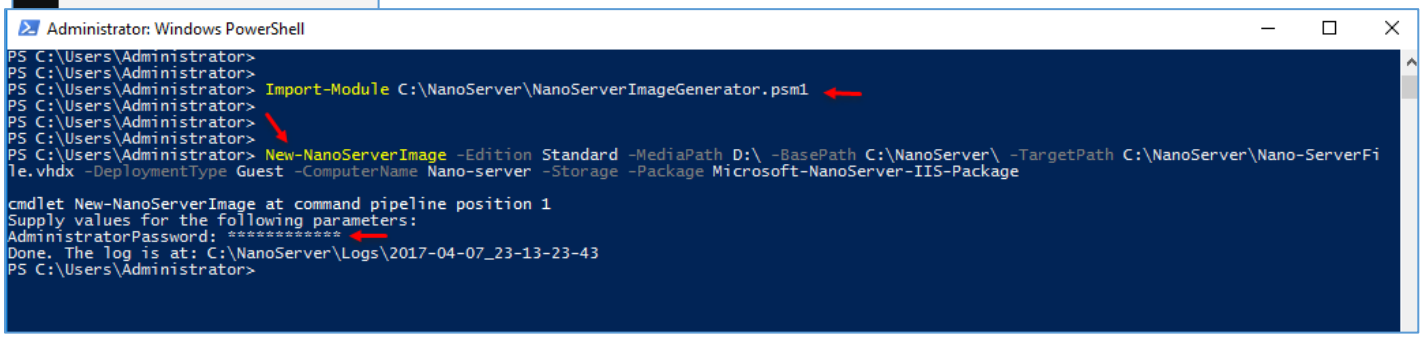
وارد پوشه‌ی NanoServerImageGenerator شوید و سه فایل انتخاب‌شده را Copy بگیرید و به دلخواه خود، یک پوشه در درایو C قرار دهید.



همانطور که مشاهده می‌کنید، فایل‌های مورد نظر در درایو C و در پوشه‌ی NanoServer قرار گرفته‌اند.



وارد Start شوید و سرویس Powershell را با دسترسی کاربر Administrator، اجرا کنید.



بعد از باز شدن سرویس PowerShell باید دستورات مورد نظر آن را وارد کنید که این کار را در زیر انجام دادیم:

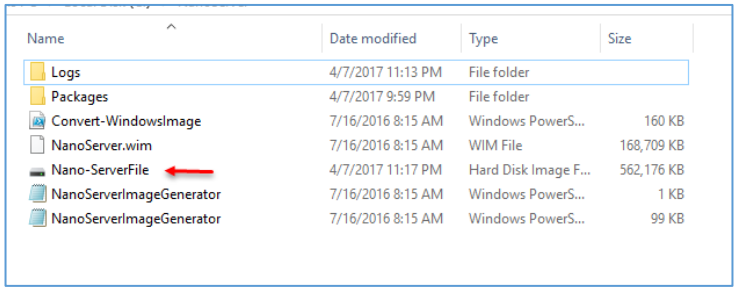
```
Import-Module C:\NanoServer\NanoServerImageGenerator.psm1
```

با استفاده از دستور بالا، فایل NanoServerImageGenerator.psm1 را اجرا کنید تا دستورات مربوط به Nano Server وارد PowerShell شود.

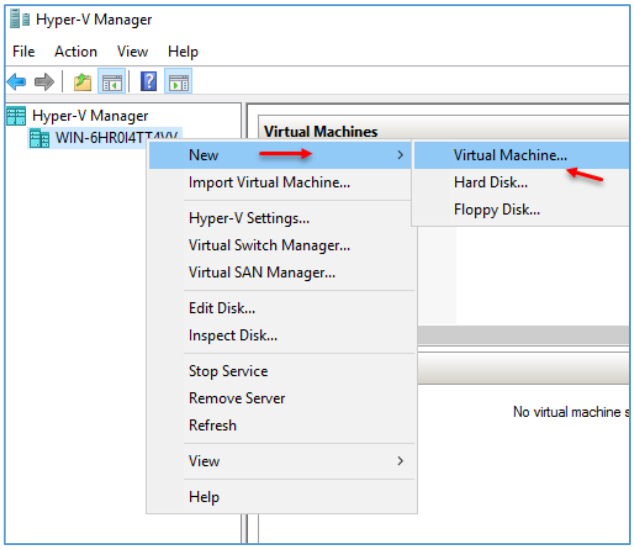
```
New-NanoServerImage -Edition Standard -MediaPath D:\ -BasePath
C:\NanoServer\ -TargetPath C:\NanoServer\Nano-ServerFile.vhdx -
DeploymentType Guest -ComputerName Nano-server -Storage –Package
Microsoft-NanoServer-IIS-Package
```

در قسمت بعد باید دستورات بالا را وارد کنید تا فایل مورد نظر خود را اجرا کنید، در دستور بالا به جای D:\ باید آدرس درایوی را وارد کنید که ویندوز سرور ۲۰۱۶ در آن قرار دارد، در قسمت BasePath، آبی رنگ باید آدرس محلّ فایل کپی‌شده که با هم انجام دادیم را وارد کنید و در قسمت TargetPath، سبز رنگ باید آدرس

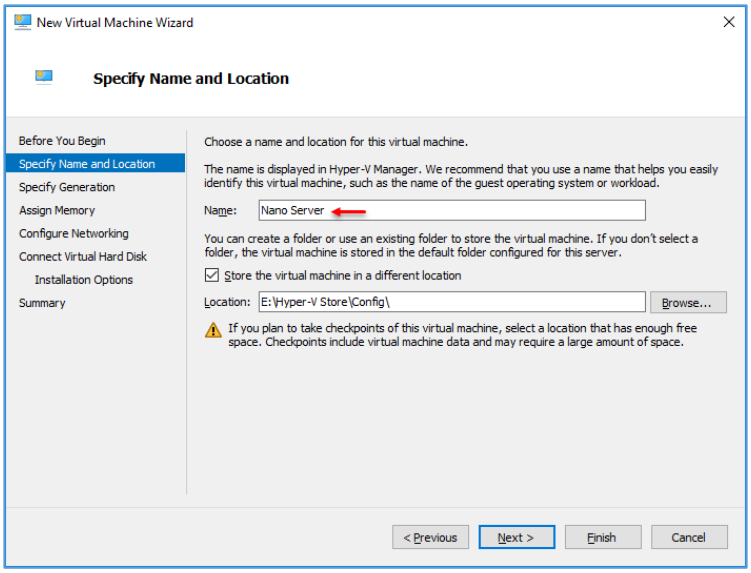
فایل ذخیره‌سازی که با پسوند VHDX است را وارد کنید، در قسمت ComputerName باید یک نام به دلخواه خود وارد کنید که این نام، همان نام سرور خواهد بود، در ادامه نیز Microsoft-NanoServer-IIS-Package وارد شده است که مربوط به سرویس IIS است که بعد از اجرا، این Nano Server قابلیّت این را دارد که یک وب سرور را اجرا کند، توجّه داشته باشید هر سرویسی که نیاز دارید را باید در اوّل کار معرّفی کنید.



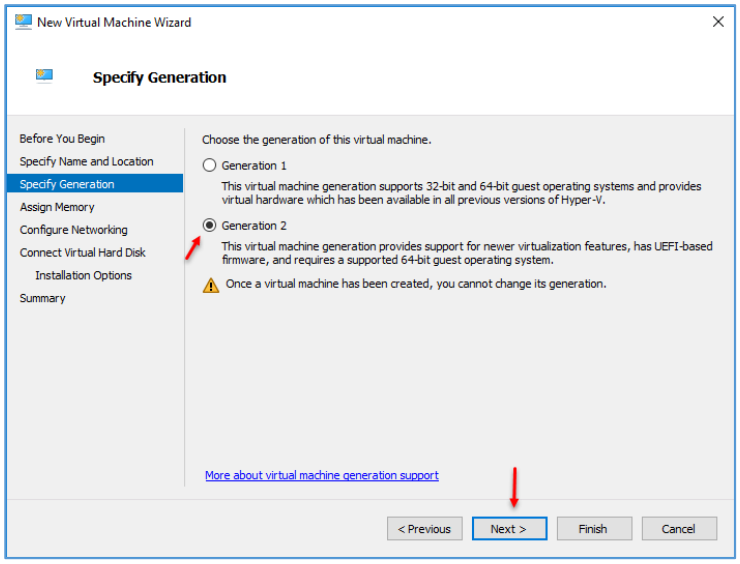
بعد از اینکه دستورات بالا را وارد و بر روی Enter فشار دادید از شما یک رمز عبور برای سرور درخواست می‌شود که آن را وارد و دوباره enter کنید تا فایل مورد نظر به مانند شکل روبرو ظاهر شود.



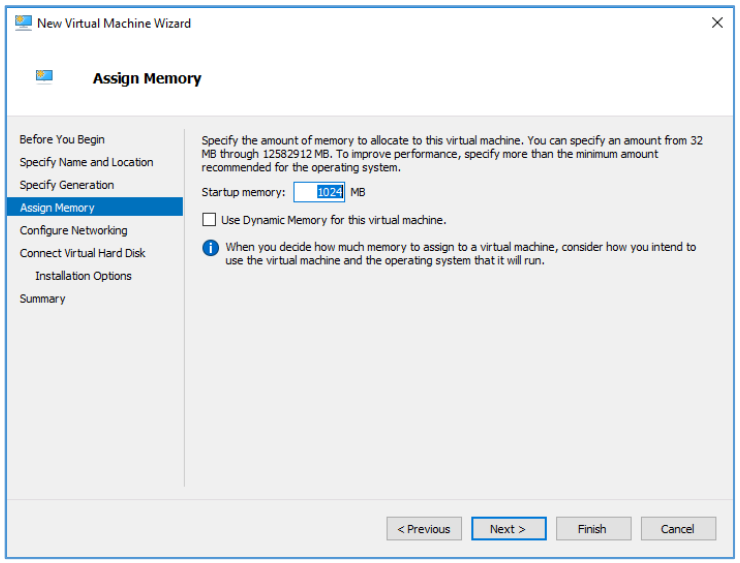
بعد از ایجاد هارد دیسک مورد نظر در قسمت قبل، وارد سرویس Hyper-V شوید و برای ایجاد ماشین مجازی جدید بر روی نام سرور، کلیک راست کنید و گزینه‌ی Virtual Machine را انتخاب کنید.



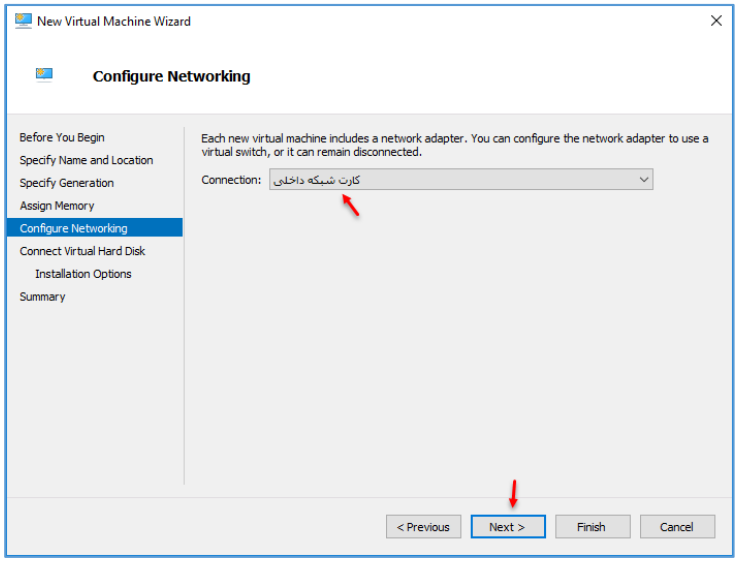
در این صفحه، نام سرور Nano را وارد کنید و محلّ ذخیره‌سازی این ماشین را مشخّص و بر روی Next کلیک کنید.



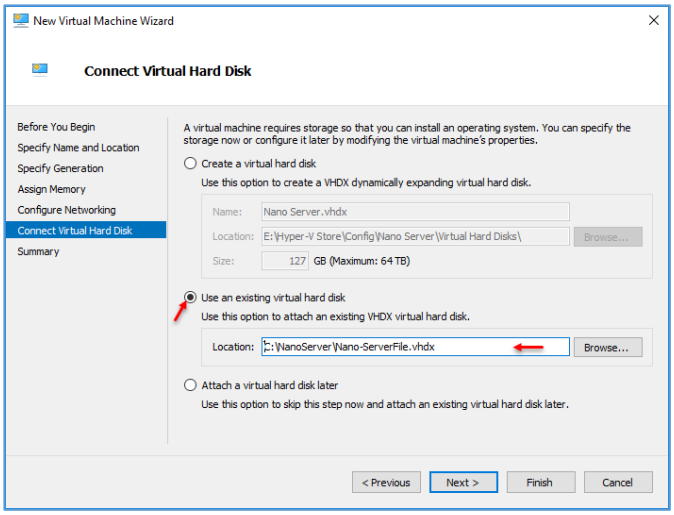
در این صفحه، گزینه‌ی مورد نظر را انتخاب و بر روی Next کلیک کنید.



در این قسمت، مقدار رم این سرور را مشخّص کنید که همانطور که قبلاً گفتیم، مقدار رم سرور می‌تواند ۵۱۲ مگابایت نیز باشد، امّا برای بهره‌وری بهتر، بهتر است، حداقل ۱ گیگ در نظر بگیرید.

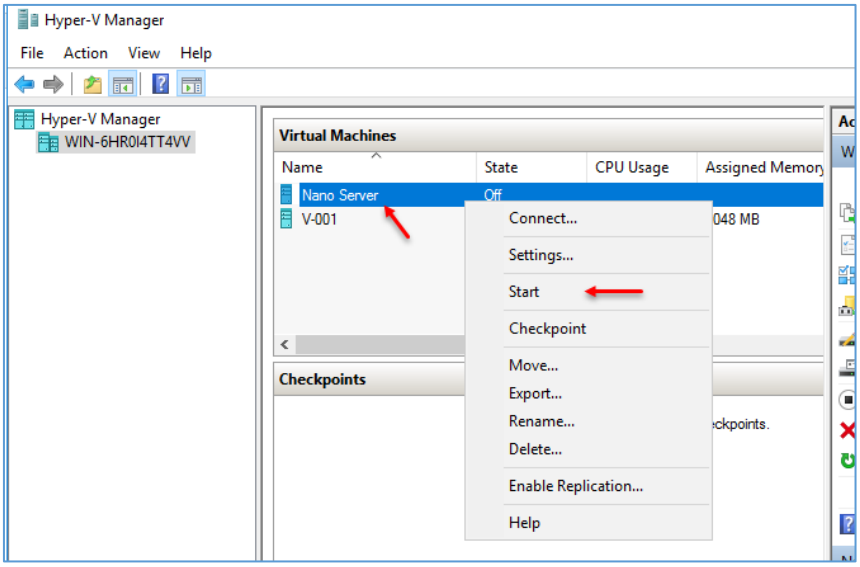


در این صفحه باید کارت شبکه‌ی مورد نظر خود را انتخاب کنید که فعلاً برای تست کار باید کارت شبکه‌ی داخلی را انتخاب کنید.

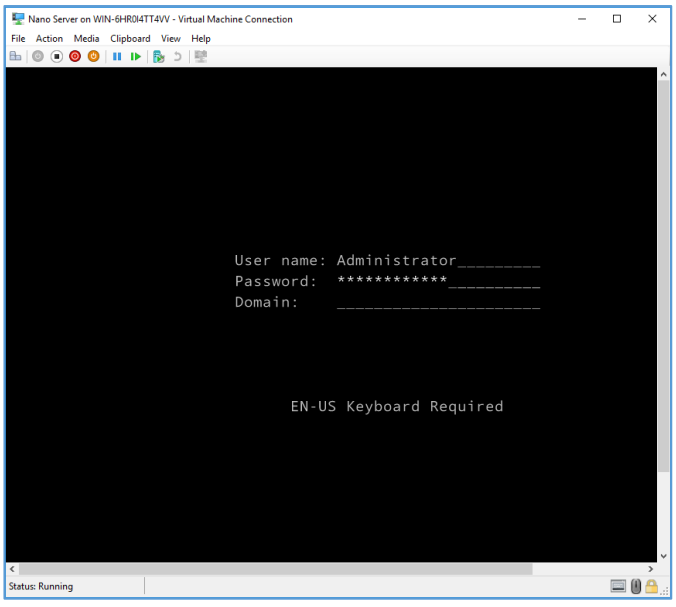


در این صفحه باید گزینه‌ی دوّم را انتخاب کنید و فایل هارد دیسک مجازی مربوط به Server Nano که با هم ایجاد کردیم را به آن معرّفی کنید تا اطّلاعات از آنها خوانده شود.

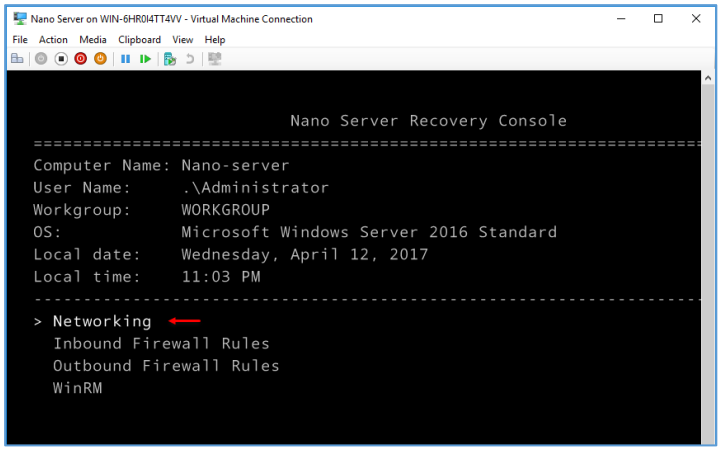
بر روی Next کلیک کنید و در صفحه‌ی آخر نیز بر روی Finish کلیک کنید.



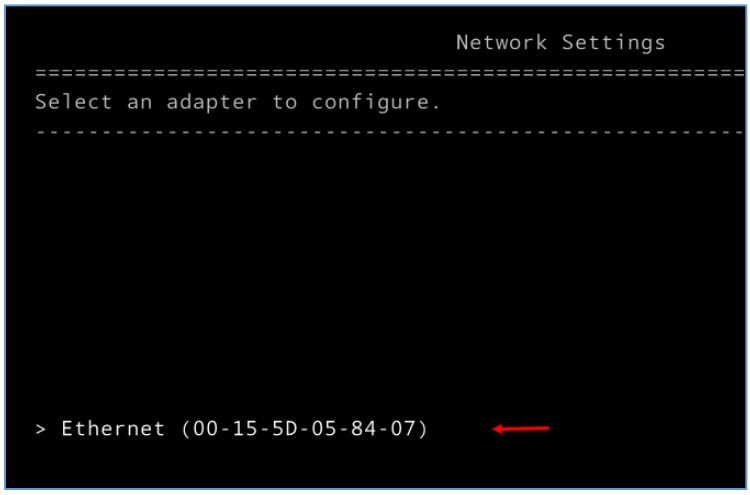
بعد از ایجاد ماشین مجازی، بر روی آن کلیک راست کنید و بعد بر روی Start کلیک کنید تا ماشین روشن شود.



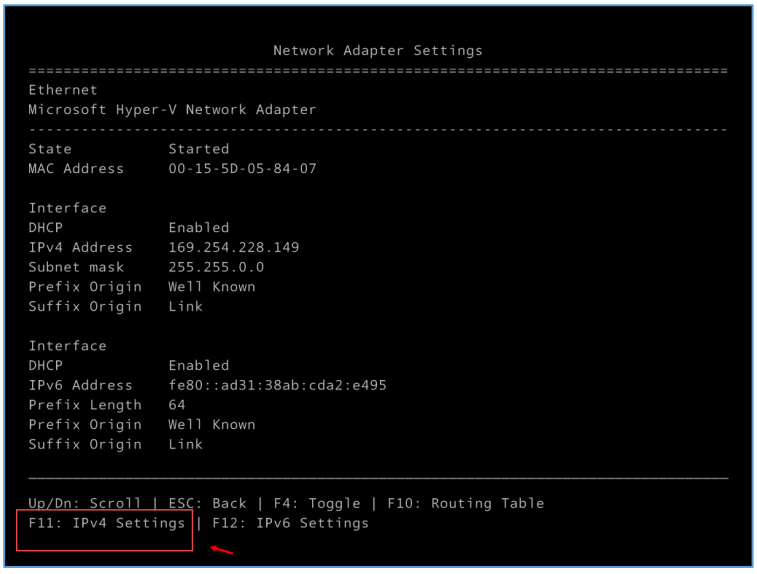
بعد از روشن شدن ماشین مجازی، صفحه‌ای ظاهر می‌شود که از شما نام کاربری، رمز عبور و نام دومین دریافت می‌شود که برای ورود باید نام کاربری Administrator را به همراه رمز عبوری که در هنگام نصب وارد کردید را دوباره در اینجا تکرار کنید و بر روی Enter فشار دهید.



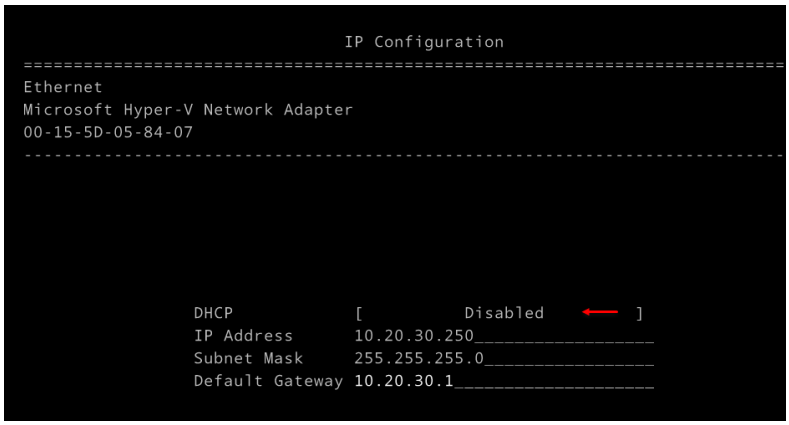
در این صفحه، اطّلاعاتی از سرور را مشاهده می‌کنید، مثلاً نوع سیستم عامل را ویندوز سرور ۲۰۱۶ استاندارد در نظر گرفته است و...، برای اینکه یک وب سرور از طریق Nano Server ایجاد کنید باید وارد قسمت Networking شوید و یک آدرس IP برای سرور تخصیص دهید.



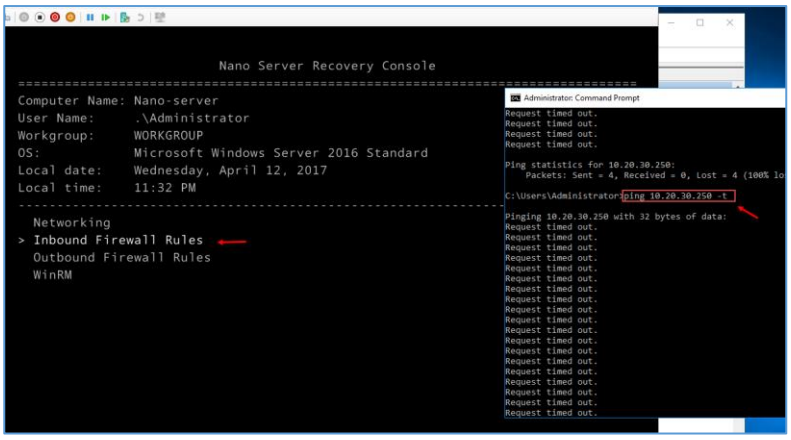
در این قسمت، تعداد کارت شبکه‌ی تخصیص‌داده شده به سرور مشخّص می‌شود که فعلاً یکی است، بر روی Enter فشار دهید تا وارد آن شوید و آدرس IP را وارد کنید.



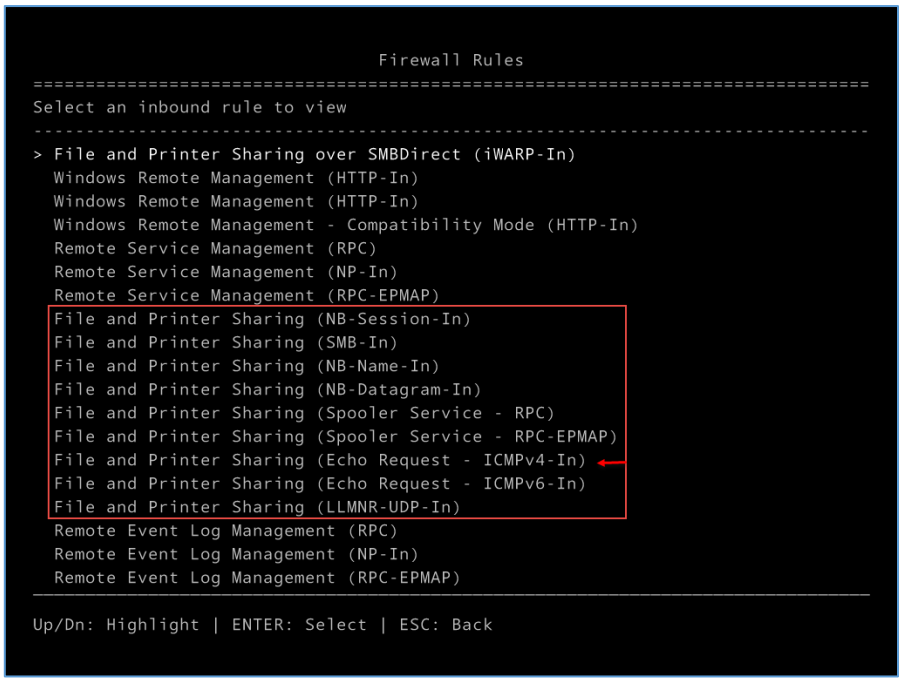
در این صفحه، اگر سرویس DHCP در شبکه‌ی شما فعّال باشد، سرور Nano به صورت اتوماتیک، آدرس IP دریافت می‌کند و اگر چنانچه بخواهید به صورت دستی آدرس وارد کنید باید به پایین صفحه مراجعه کنید که برای تنظیم آدرس IPV4 باید بر روی F11 کلیک کنید و برای IPV6 بر روی F12 کلیک کنید.



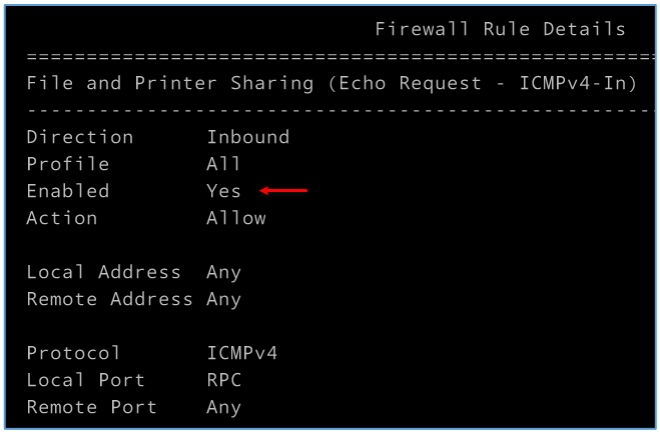
در این صفحه، اوّل باید با کلید بر روی F4، سرویس DHCP را غیر فعّال کنید تا از طریق سرویس DHCP، آدرس دریافت نکند، بعد از این کار با کلید بر روی TAB، آدرس IP سرور را به همراه Gateway و Subnet وارد کنید و بر روی Enter کلیک کنید تا اطّلاعات ذخیره شود.



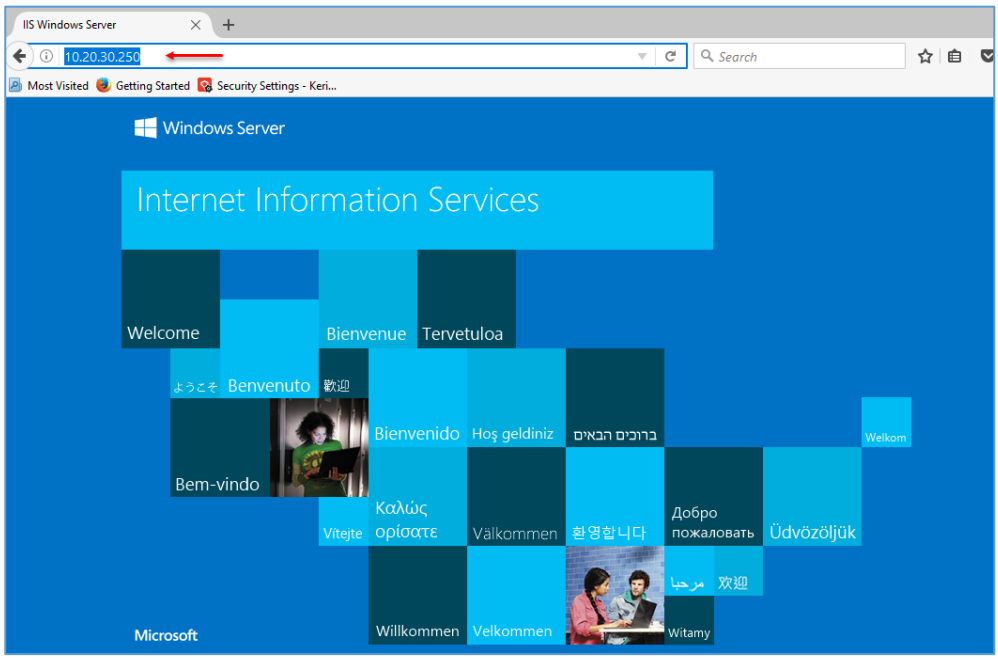
بعد از اینکه آدرس‌دهی کردید، می‌توانید با یک عملیّات Ping این موضوع را تست بگیرید، همانطور که در شکل روبرو مشاهده می‌کنید از ویندوز اصلی، سرور Nano را Ping گرفتیم که با خطای Timed out روبرو شدیم، برای حلّ آن باید فایروال را دستکاری کنید، لذا ابتدا وارد Nano Server شوید و بعد از آن وارد قسمت Inpound Firewall Rules شوید.



در شکل روبرو، گزینه‌های مختلفی را مشاهده می‌کنید، اگر تنها بخواهید عملیّات Ping را تکمیل کنید باید وارد گزینه‌ای که با فلش مشخّص شده است، شوید و بعد از آن، کلید F4 را فشار دهید تا فعّال شود و بعد، بر روی Esc کلید کنید، با این کار Ping فعّال خواهد شد، امّا اگر بخواهید دسترسی به کلّ سرور برای راه‌اندازی وب سرور داشته باشید باید وارد همه‌ی گزینه‌هایی



که مشخّص شده است، شوید و با کلیک بر روی دکمه‌ی F4، آنها را فعّال کنید که در شکل روبرو، یکی از این گزینه‌ها را مشاهده می‌کنید که با کلید بر روی F4، سرویس آن Enabled شده است.

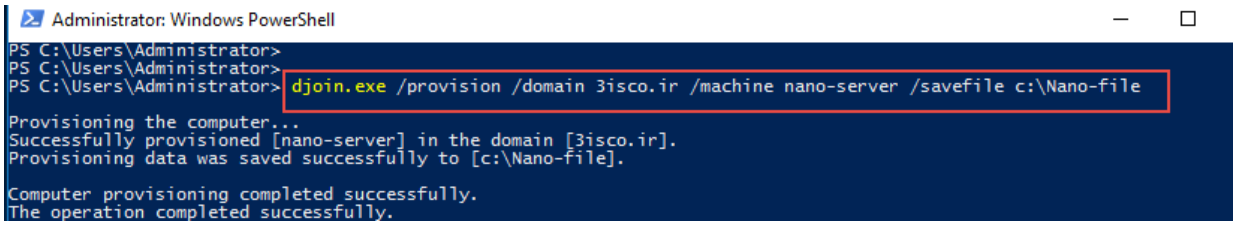


اگر آدرس سرور Nano را داخل مرورگر وارد کنید، سرویس IIS را مشاهده می‌کنید که فعّال شده و در دسترس است.

عضو کردن Nano Server به سرویس Domain:

برای اینکه بتوانید سرور Nano را عضو دومین کنید و از منابع آن، تحت کنترل دومین استفاده کنید باید به صورت زیر عمل کنید.

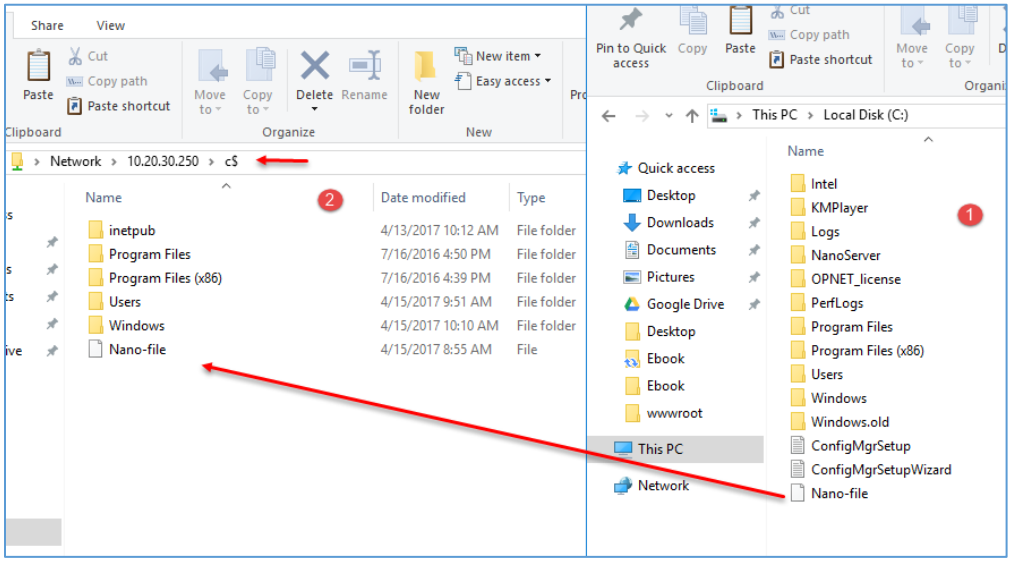
وارد یکی از سرورهای خود، مثل دومین یا همان، AD که قبلاً با آن کار کردیم، شوید و سرویس Powershell را با دسترسی کاربر Administrator اجرا کنید.



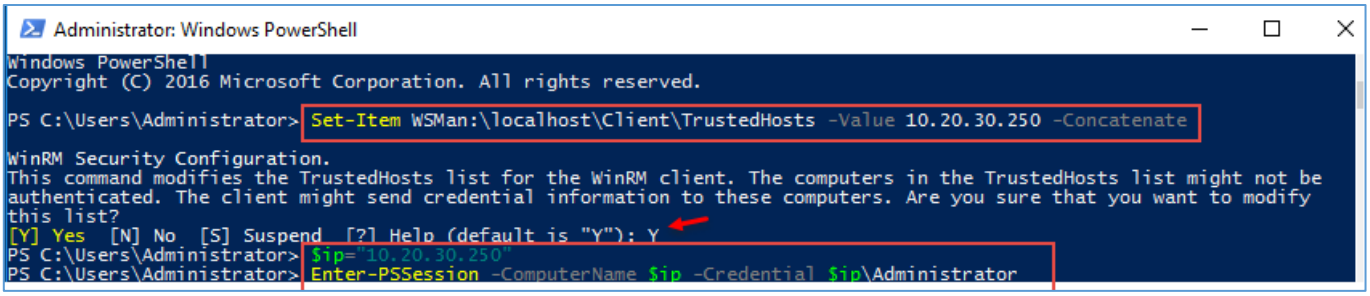
همانطور که در شکل بالا مشاهده می‌کنید، دستوری به شکل زیر وارد شده است:

djoin.exe /provision /domain ۳isco.ir /machine nano-Server /savefile c: \Nano-file

با این کار، یک فایل با عنوان Nano-file که دارای محتویّات نام دومین و نام سرور نانو است، در درایو C ذخیره می‌شود.



همانطور که در شکل روبرو مشاهده می‌کنید، در قسمت شماره‌ی یک که مربوط به سرور AD است بر روی آن، Powershell را اجرا کردیم و بعد از آن دستور بالا را اجرا کردیم، فایلی با عنوان Nano-file در درایو C ایجاد شده است که باید این فایل را در سرور Nano کپی کنیم، برای این کار باید آدرس \\10.20.30.250\c$ را وارد کنیم، بعد از آن وارد درایو C مربوط به Nano سرور می‌شویم و فایل Nano-file را از درایو C سیستم AD به درایو C سرور Nano انتقال می‌دهیم تا در ادامه از این فایل استفاده کنیم.



بعد از اینکه فایل را درست کردید و به سرور Nano انتقال دادید باید دستورات بالا را به صورت زیر اجرا کنید:

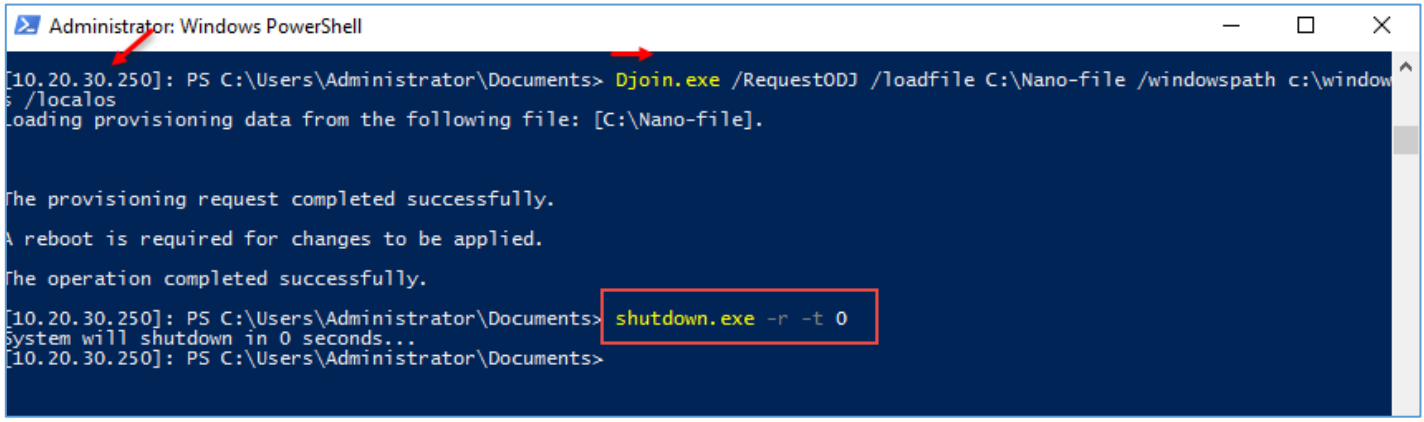
```
Set-Item WSMan:\localhost\Client\TrustedHosts  "10.20.30.250" -Concatenate
```

با دستور بالا، به صورت مستقیم به سرویس PowerShell سرور Nano متّصل می‌شوید که بعد از آن می‌توانید عملیّات Join به دومین را انجام دهید، در دستور بالا به جای آدرس 10.20.30.250 باید آدرس سرور Nano خود را وارد و بر روی Enter فشار دهید، بعد از آن، کلمه‌ی Y را وارد کنید تا به سرور Nano متّصل شوید، بعد از متّصل شدن باید نام کاربری Administrator را برای اجرای دستورات فعّال کنید، برای این کار از دستور زیر استفاده کنید:

```
$ip = “10.20.30.250”
Enter-PSSession -ComputerName $ip -Credential  -$ip\Administrator
```

در دستورات بالا و خط اوّل، یک متغیّر با نام IP تعریف کنید و آدرس سرور Nano را در آن قرار دهید و بر روی Enter کلید کنید.

در خط دوّم با استفاده از دستور Enter-PSSession، نام سرور را به همراه کاربر دسترسی آن وارد کنید، بعد از Enter، از شما رمز عبور کاربر Administrator دریافت خواهد شد که در این قسمت باید وارد و بر روی OK کلیک کنید.



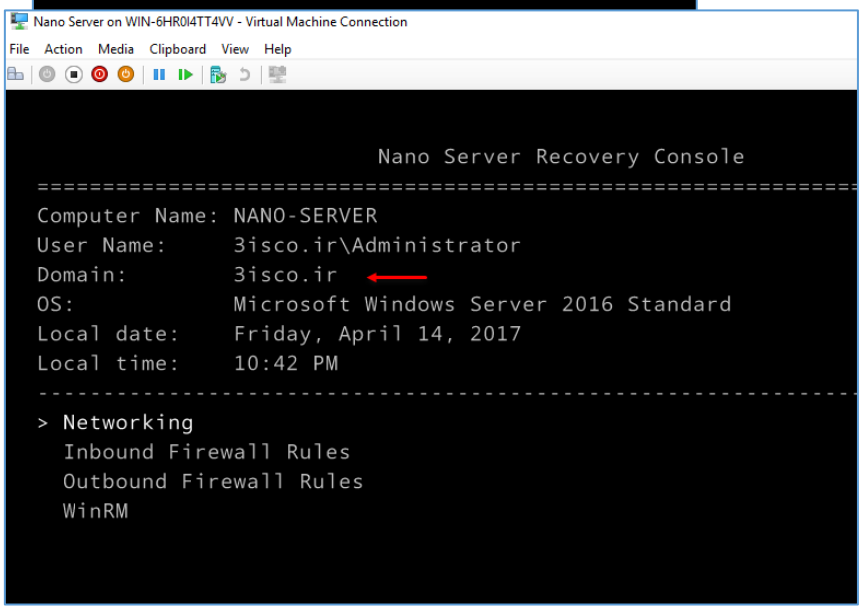
اگر به اوّل دستورات بالا توجّه کنید، به سرور 10.20.30.250 که همان، سرور Nano است از طریق Powershell متّصل شدیم که بعد از متّصل شدن باید عملیّات Join به دومین را با فایلی که قبلاً ایجاد کردیم و در ریشه‌ی درایو C سرور Nano کپی کردیم، انجام دهیم.

djoin /requestodj /loadfile c:\Nano-file /windowspath c:\windows /localos

با استفاده از دستور بالا، فایل مورد نظر، c:\Nano-file خوانده می‌شود و عملیّات Join به دومین با موفّقیّت انجام می‌پذیرد، بعد از این کار با دستور Shutdown.exe –r –t 0، سرور را Restart کنید تا عملیّات تکمیل شود.

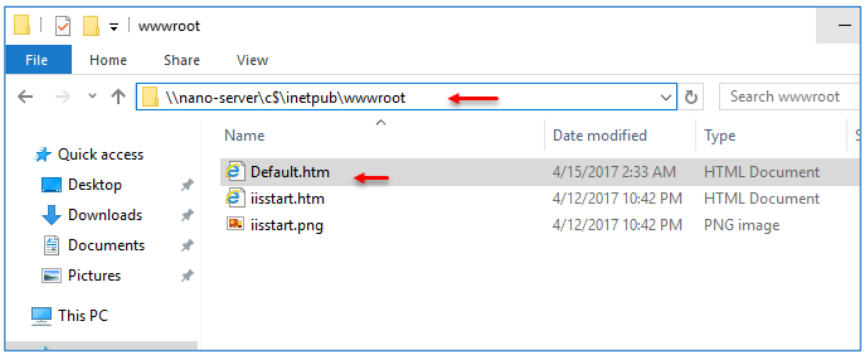


بعد از اجرا شدن سرور به مانند شکل روبرو، نام دومین را نیز در هنگام ورود وارد کنید و بر روی Enter فشار دهید.

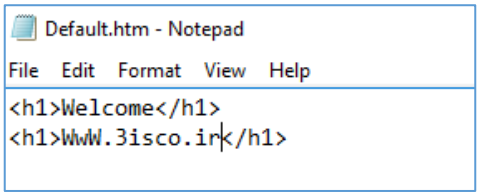


همانطور که مشاهده می‌کنید، سرور مورد نظر، عضو دومین 3isco.ir شده و در شبکه مورد تأیید است.

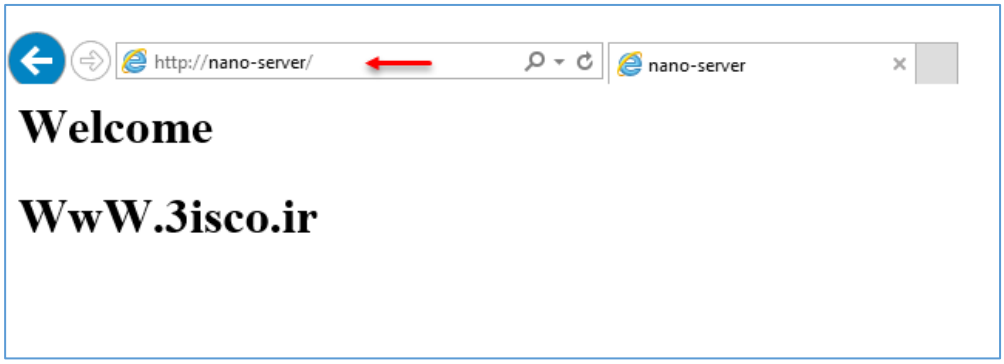
برای اینکه یک وب سایت به صورت آزمایشی اجرا کنید باید به صورت زیر عمل کنید.



به مانند شکل وارد آدرس مورد نظر در سرور Nano شوید و یک فایل htm با عنوان Default.htm ایجاد کنید و یک نوشته به مانند شکل زیر وارد کنید.



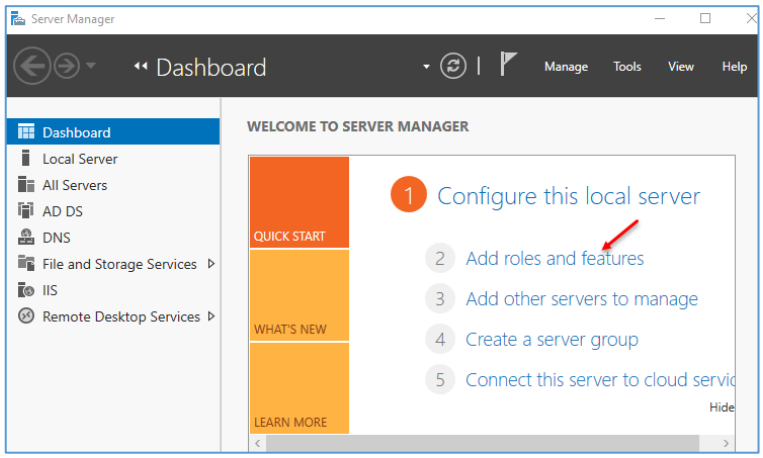
در شکل روبرو، متن HTML وارد شده است و در محلّ مورد نظر با نام مورد نظر ذخیره شده است.



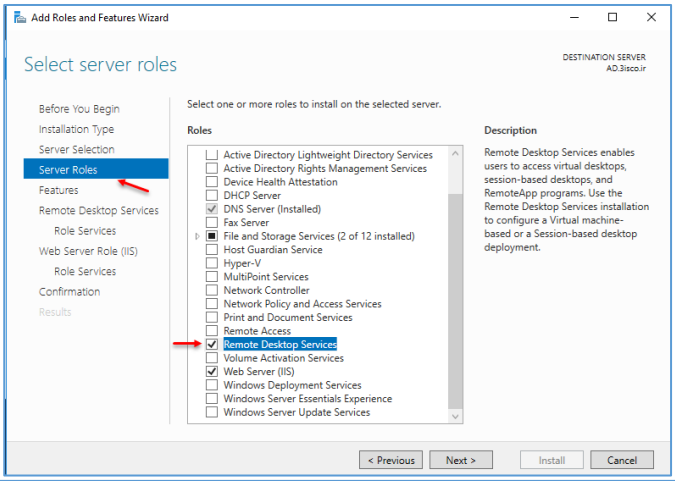
بعد از انجام کارهای بالا، وارد مرورگر هر یک از سرورهای داخل شبکه شوید؛ در آدرس روبرو باید به جای Nano-server، نام سرور Nano خود را وارد کنید تا مشاهده کنید سایت مورد نظر برای شما باز خواهد شد.

نصب و راه‌اندازی سرویس Remote Desktop:

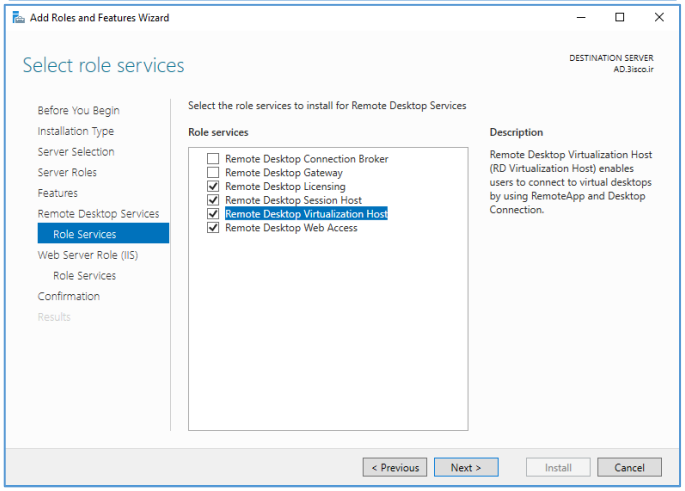
این سرویس، یک سرویس یا ابزار کارآمد برای دسترسی به منابع شبکه است که از اجزای مختلفی تشکیل شده است؛ یکی از ویژگی‌ها، آن است که شما می‌توانید با چندین کاربر به صورت هم‌زمان بر روی یک ویندوز سرور، Login کنید، امّا به صورت Remote و یا اینکه اگر در شبکه‌ی خود از ماشین مجازی استفاده می‌کنید، آنها را در دسترس کاربران به صورت وب سرویس قرار دهید.



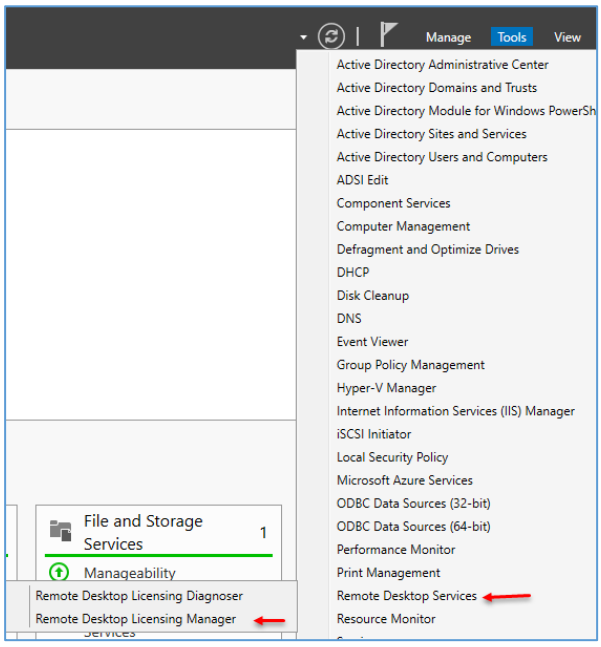
برای شروع وارد Server Manager شوید و بر روی گزینه‌ی Add roles and features کلیک کنید.



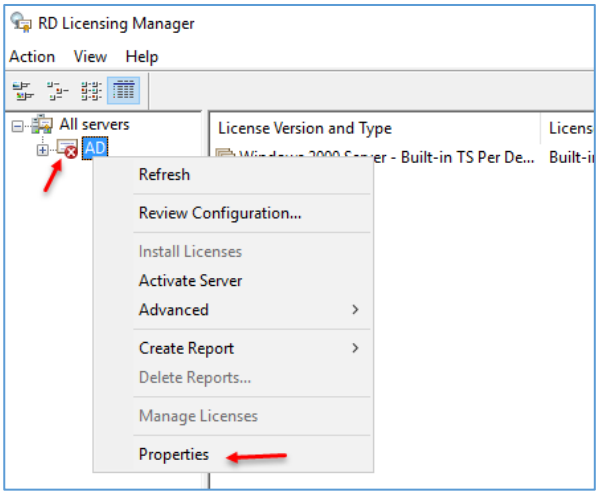
در این صفحه، سرویس Remote Desktop Services را انتخاب و بر روی Next کلیک کنید.



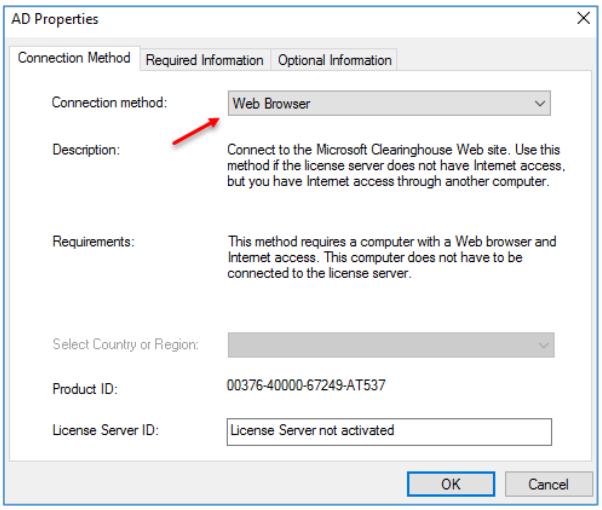
در قسمت Role Services، هر چهار گزینه‌ی مورد نظر را انتخاب و بر روی Next کلیک کنید.



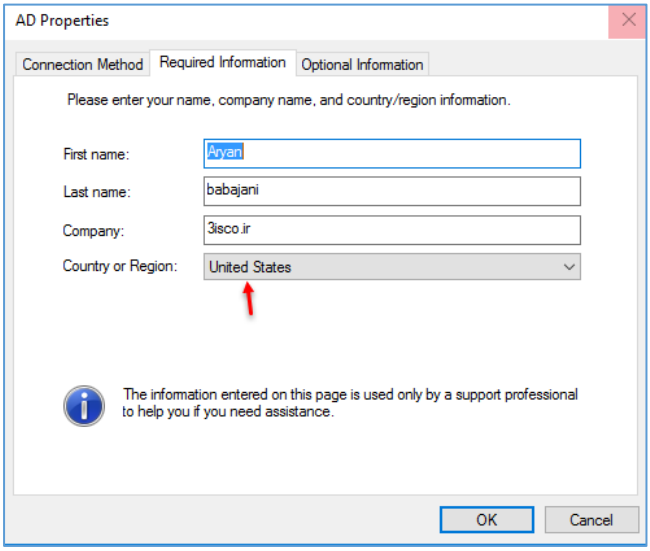
بعد از نصب سرویس و Restart شدن سرور وارد Server Manager شوید و از قسمت Tools، گزینه‌ی Remote Desktop Licensing Manager را انتخاب کنید.



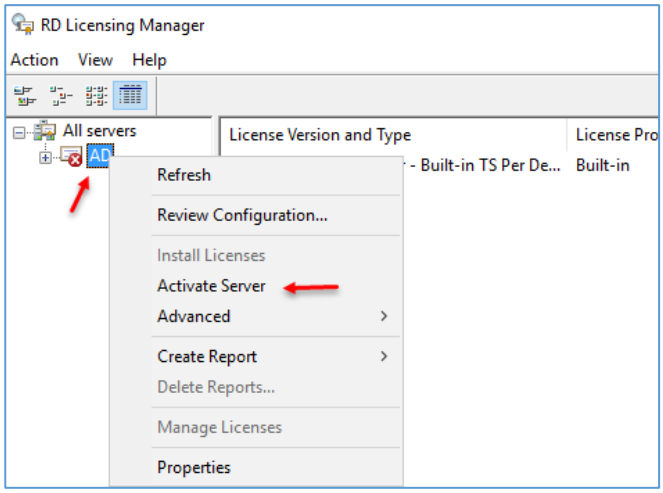
بعد از باز شدن سرویس Remote Desktop Licensing Manager، به مانند شکل بر روی نام سرور کلیک راست و بر روی Properties کلیک کنید.



در این صفحه، از قسمت Connection method، گزینه‌ی Web Brwser را وارد کنید و در ادامه، وارد تب Required information شوید.

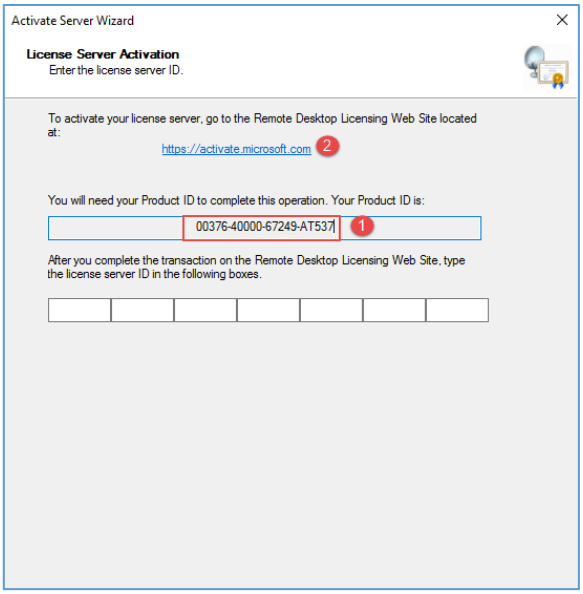


در این تب باید اطّلاعات خود را وارد کنید و در قسمت Country نیز نام کشور آمریکا را انتخاب و بر روی OK کلیک کنید.



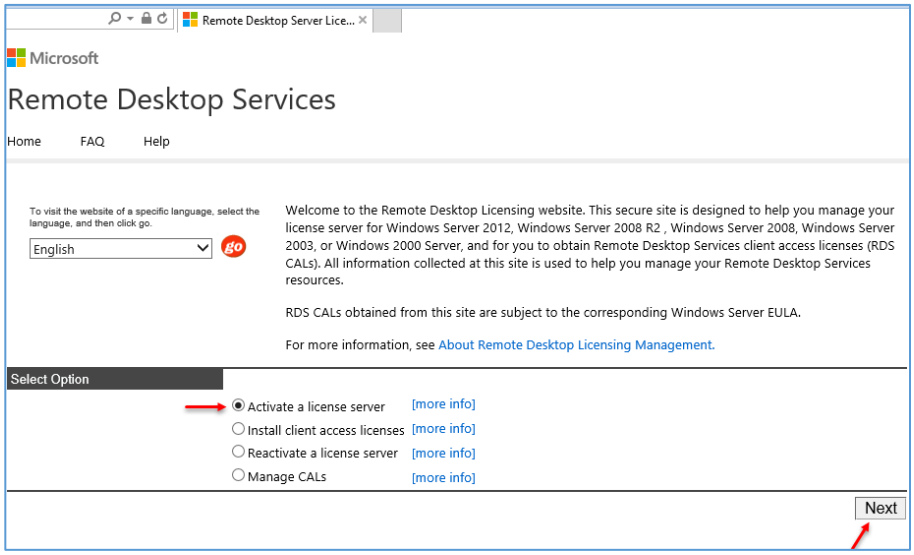
بعد از انجام مراحل بالا، دوباره بر روی نام سرور کلیک راست کنید و گزینه‌ی Activate Server را انتخاب کنید.

نکته: در ادامه، سرور باید به اینترنت متّصل باشد.

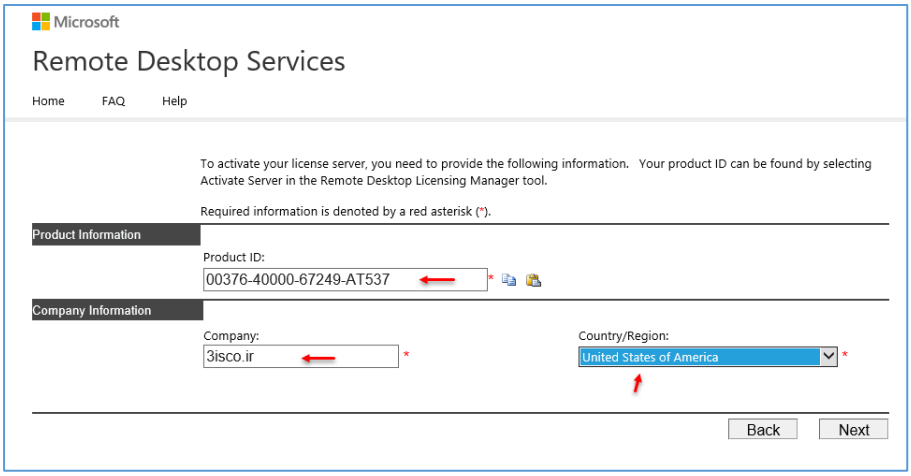


در صفحه‌ی روبرو و در قسمت شماره‌ی یک، برای سرور شما یک Product ID مشخّص شده است، قبل از هر چیز، این شماره را در یک جای مناسب ذخیره کنید تا در ادامه از آن استفاده کنید.

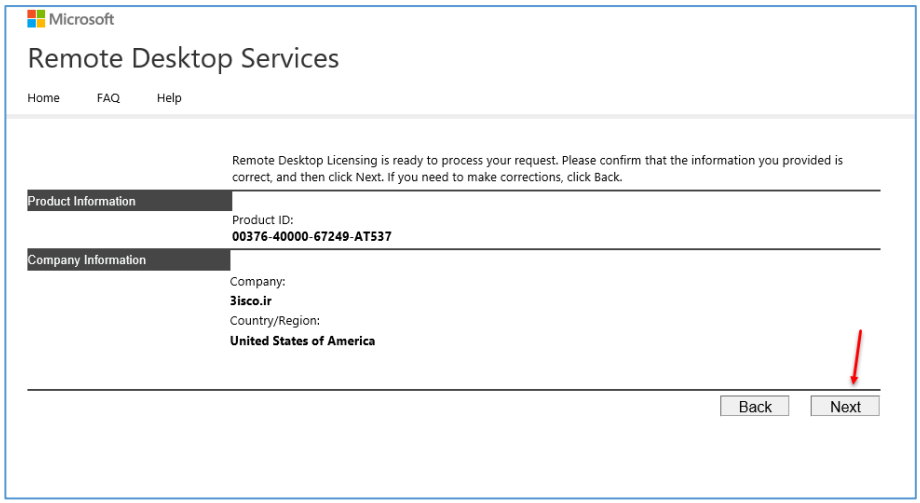
در ادامه بر روی لینک شماره‌ی دو در صفحه کلیک کنید.



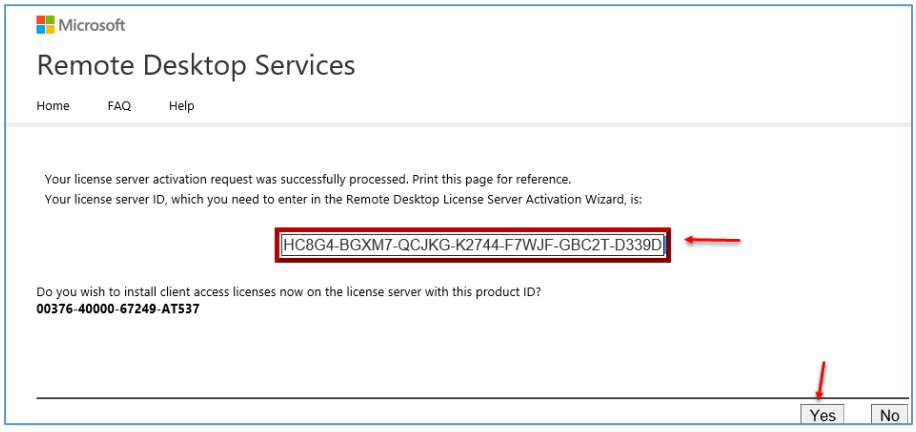
در شکل روبرو، صفحه‌ی مربوط به Active ظاهر می‌شود، گزینه‌ی Activate a license Server را انتخاب و بر روی Next کلیک کنید.



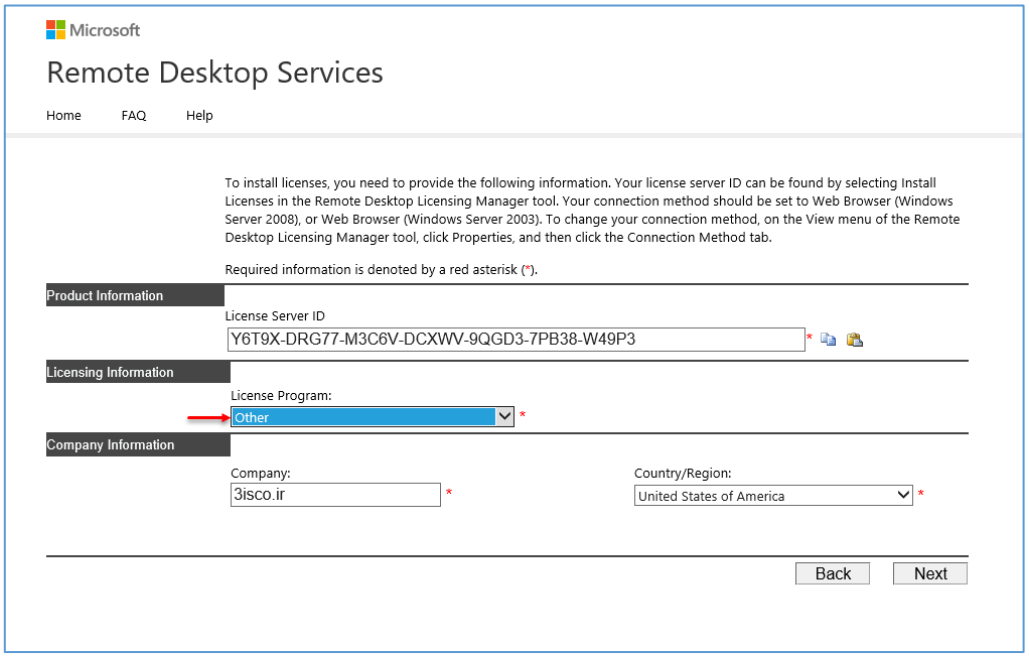
در این صفحه و در قسمت **Product ID**، شماره‌ای که در اوّل کار در یک فایل **Copy** کردید را وارد کنید، بعد در قسمت **Company**، نام شرکتی که در قسمت قبل وارد کردید را وارد و نام کشور را آمریکا انتخاب و بر روی **Next** کلیک کنید.



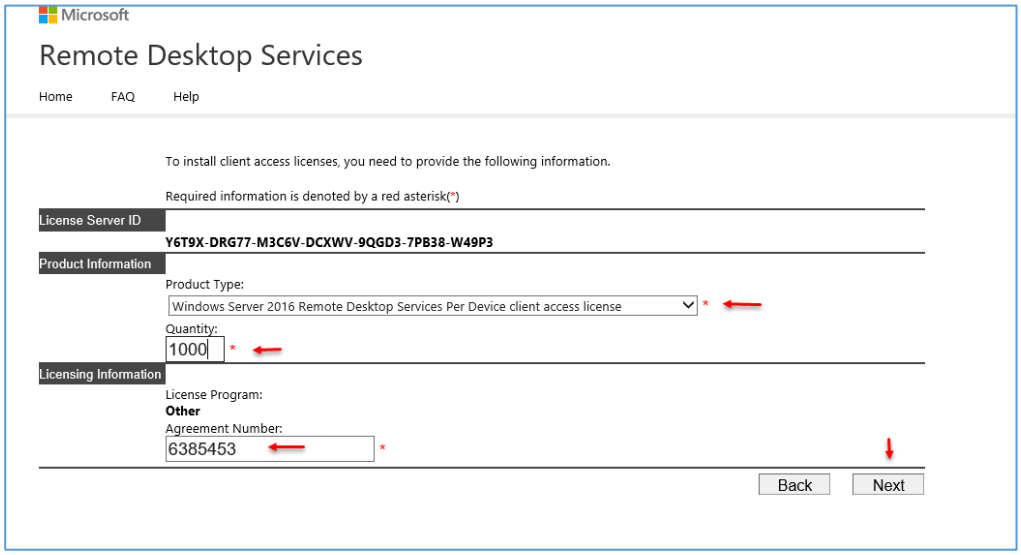
در این صفحه، اگر اطّلاعات شما مورد تأیید است، بر روی **Next** کلیک کنید.



در این صفحه، یک شماره‌ی دوّم به شما داده می‌شود که این شماره را نیز کپی کنید و در کنار همان شماره-ای قرار دهید تا در ادامه از آن استفاده کنید؛ بر روی **Yes** کلیک کنید.

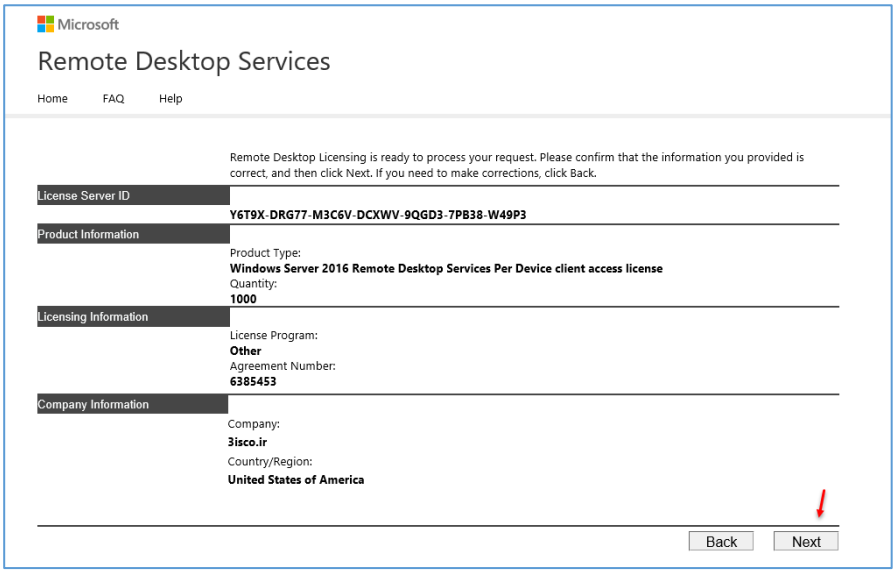


در این صفحه برای ایجاد لایسنس در قسمت License Program، گزینه‌ی Other را انتخاب و بر روی Next کلیک کنید.

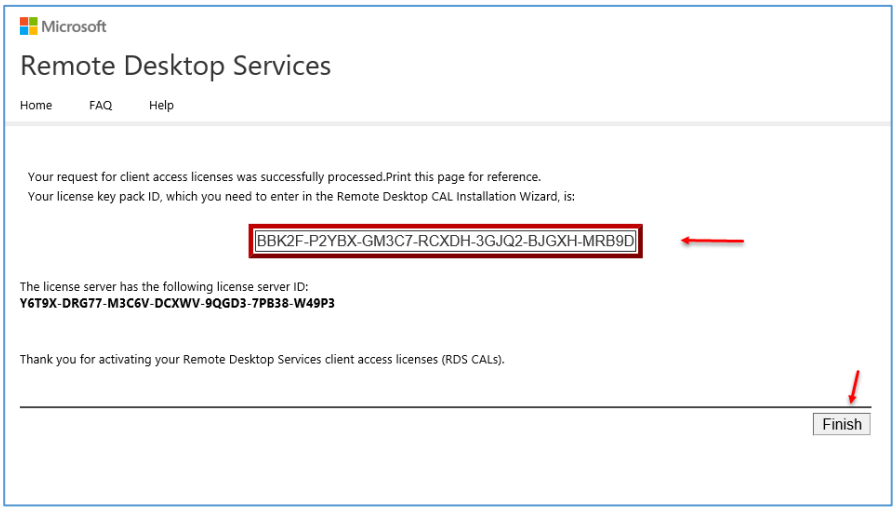


در این صفحه و در قسمت Product Type، سرویس Windows Server 2016 Remote Desktop Services per... را انتخاب کنید، در قسمت Quantity، عدد ۱۰۰۰ را وارد و در قسمت آخر نیز عدد 6385453 را وارد و بر روی Next کلیک کنید.

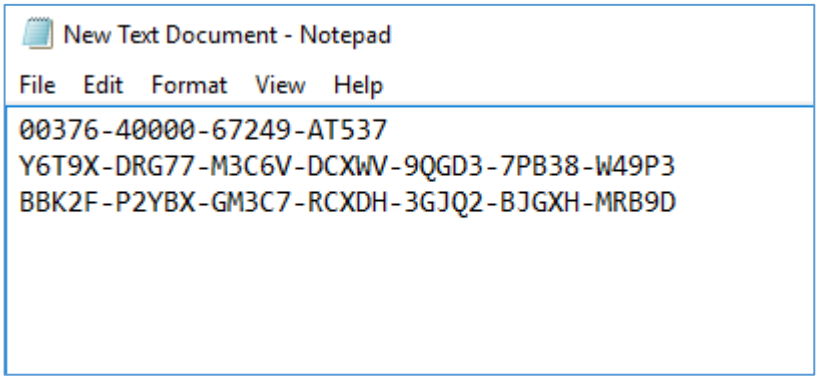
تذکّر: اگر در هنگام راه‌اندازی این قسمت با مشکلی روبرو شدید، با من در تماس باشید.



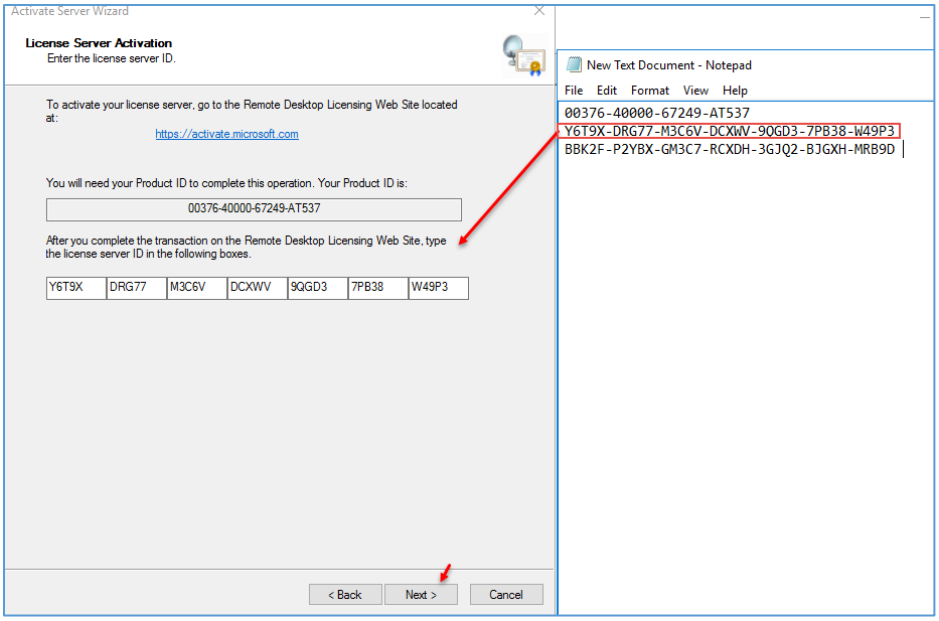
اگر در این صفحه، اطّلاعات مورد تأیید است، بر روی Next کلیک کنید.



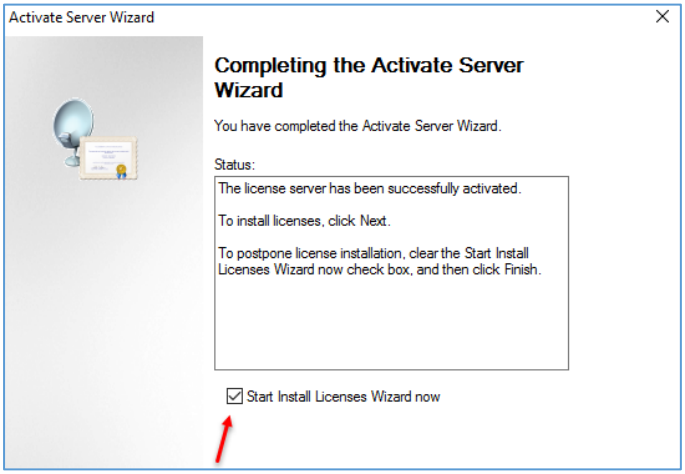
در این صفحه نیز یک سریال نهایی به شما داده خواهد شد که این شماره را نیز کنار همان شماره‌ها قرار دهید و بر روی Finish کلیک کنید.



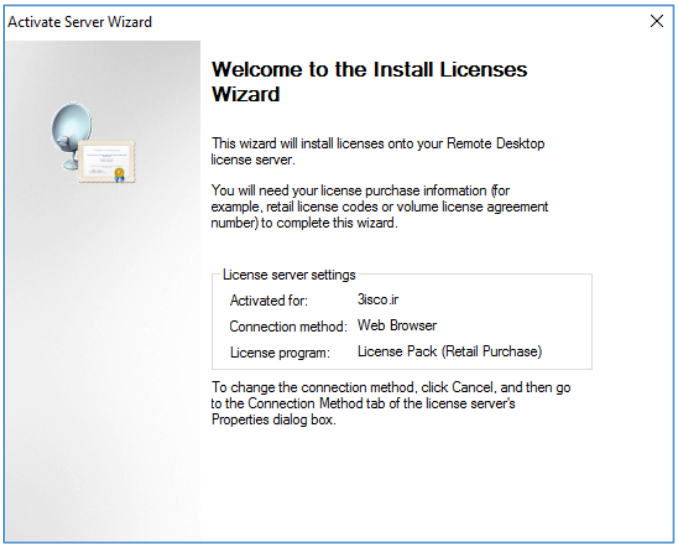
همانطور که در شکل روبرو مشاهده می‌کنید، هر سه سریال در کنار هم قرار داده شده است، در ادامه برای اجرای نهایی سرویس از دو سریال پائینی استفاده می-کنیم.



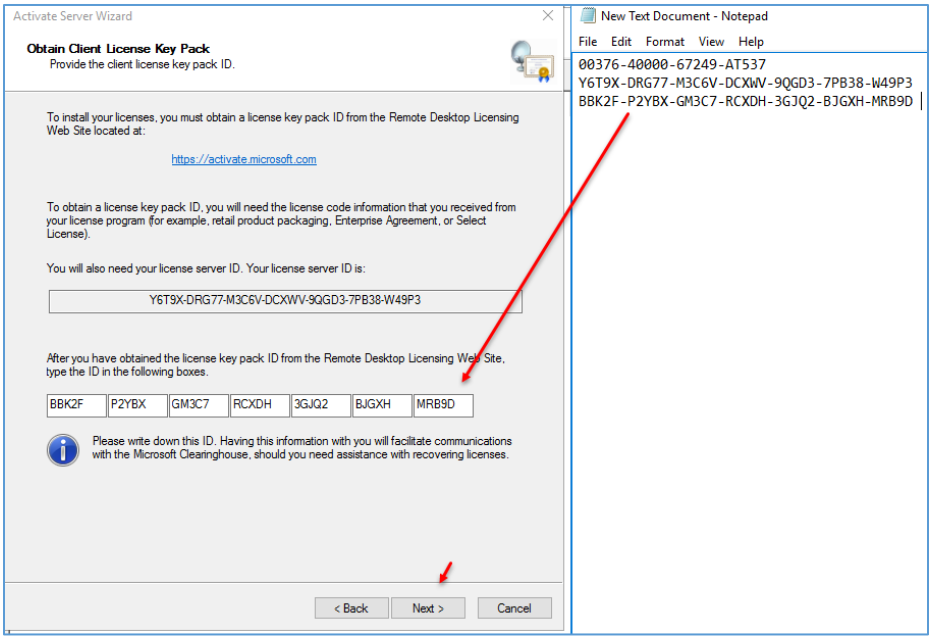
در ادامه، شماره‌ی سریال دوّم را در قسمت مورد نظر وارد و بر روی Next کلیک کنید تا سرور، Active شود.



در ادامه و بعد از تأیید نهایی سرور باید لایسنس آن را نیز فعّال کنید، تیک گزینه‌ی Start Install Licenses Wizard now را انتخاب و بر روی Next کلیک کنید.

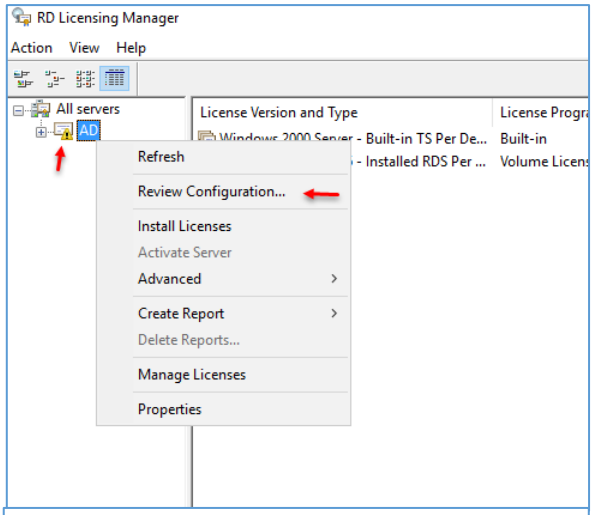


صفحه‌ی Welcome ظاهر می‌شود، بر روی Next کلیک کنید.

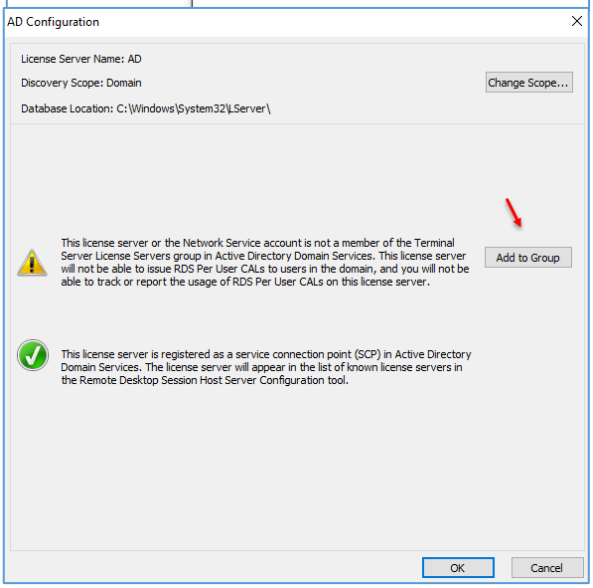


در این صفحه باید سریال سوّم را در قسمت مورد نظر کپی و بر روی Next کلیک کنید تا سرور به صورت کامل فعّال شود.

در صفحه‌ی بعد نیز بر روی Finish کلیک کنید.



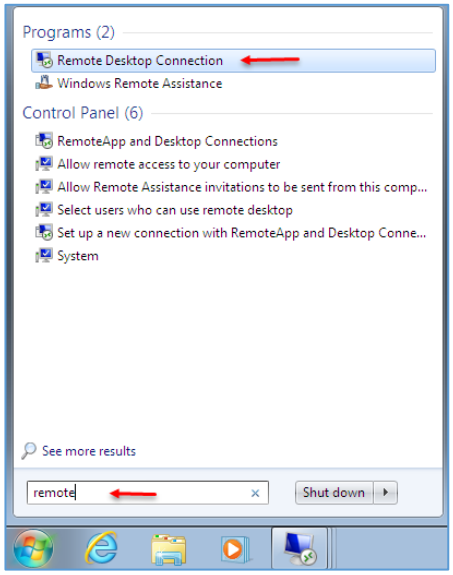
بعد از انجام عملیّات بالا، یک علامت اخطار بر روی سرور شما ظاهر می‌شود که برای حلّ این مشکل باید بر روی آن کلیک راست کنید و گزینه‌ی Review Configuration را انتخاب کنید.



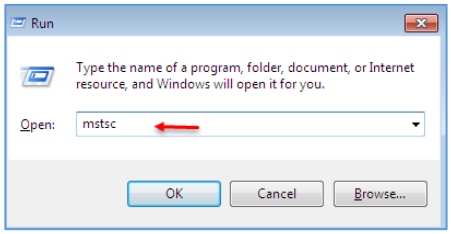
در این قسمت، یک پیغام برای شما ظاهر می‌شود که به شما این پیام را می‌دهد که اکانت Network Service، عضو گروه‌های گفته‌شده، نیست که در ادامه باید این کار انجام شود، برای حلّ مشکل بر روی Add to Group کلیک کنید و در صفحات باز شده بر روی OK کلیک کنید و حتماً بعد از آن سرور را Restart کنید.

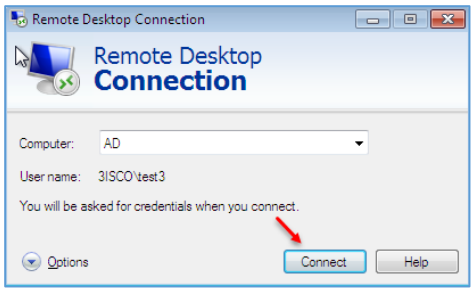
بعد از انجام مراحل بالا، همه چیز آماده است تا کاربران بتوانند به سرور دسترسی Remote داشته باشند، در حالت عادّی، تنها دو کاربر می‌توانند به صورت همزمان، به سرور Remote بزنند که با اجرای این سرویس و فعّال کردن آن، چندین کاربر به طور همزمان می‌توانند به سرور متّصل شوند.

برای تست کارایی سرویس، سه کاربر با نام‌های user1, user2, user3 در Active ایجاد کردیم و می‌خواهیم این عملیّات را بررسی کنیم.

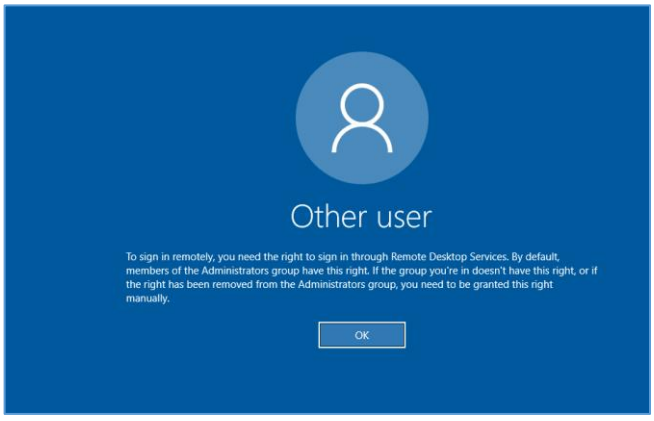


برای تست از یک کلاینت که دارای ویندوز 7 است و عضو شبکه‌ی ما شده است، استفاده می‌کنیم، برای شروع وارد start شوید و سرویس Remote Desktop را اجرا کنید، یا اینکه وارد Run شوید و دستور MSTSC را اجرا کنید.



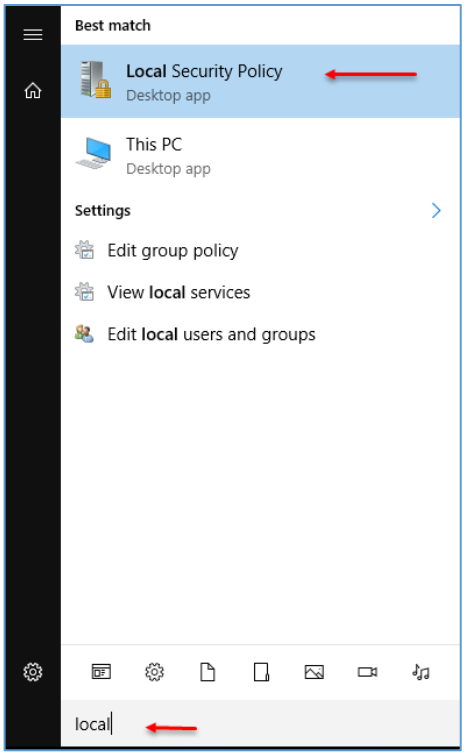


در این صفحه باید نام سرور خود را که سرویسRemote Dekstop را بر روی آن فعّال کردید را وارد و بر روی Connect کلیک کنید و بعد از آن برای ورود، نام کاربری مورد نظر خود را وارد کنید.

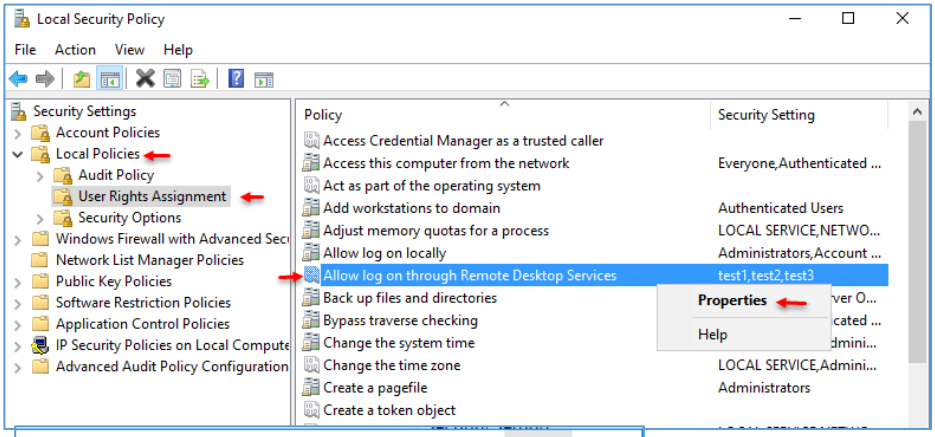


بعد از ورود به سرور با خطای مقابل روبرو می‌شوید که در این پیغام به شما اعلام می‌دارد که کاربر شما عضو گروه Administrator نیست و به همین خاطر دسترسی به سرور ندارد.

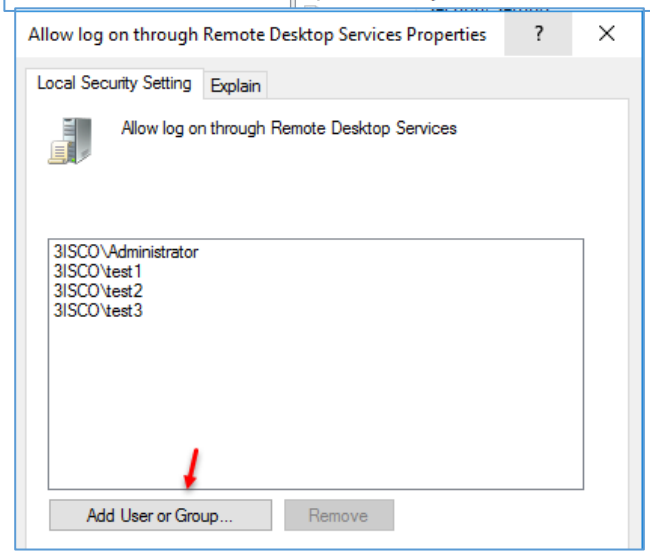
برای حلّ این مشکل به صفحه‌ی بعد مراجعه کنید.



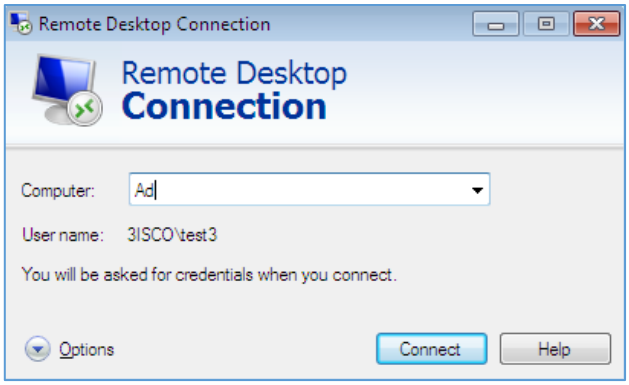
وارد سرور اصلی که در اینجا همان، AD است شوید و در Start، سرویس Local Security Policy را اجرا کنید تا تنظیمات مورد نیاز برای Remote را انجام دهید.



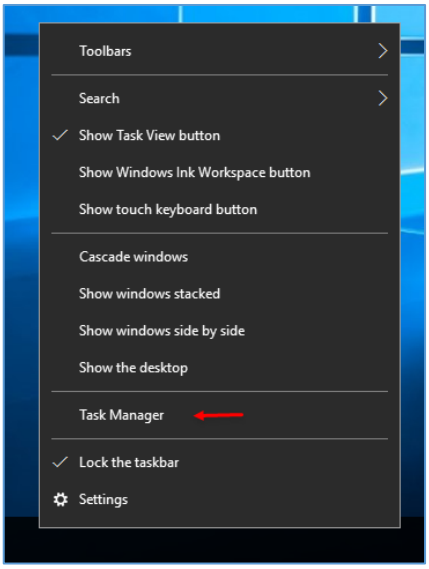
در این صفحه، از سمت چپ وارد قسمت User Rights assignment شوید و در لیست بازشده بر روی گزینه‌ی Allow log on th... کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



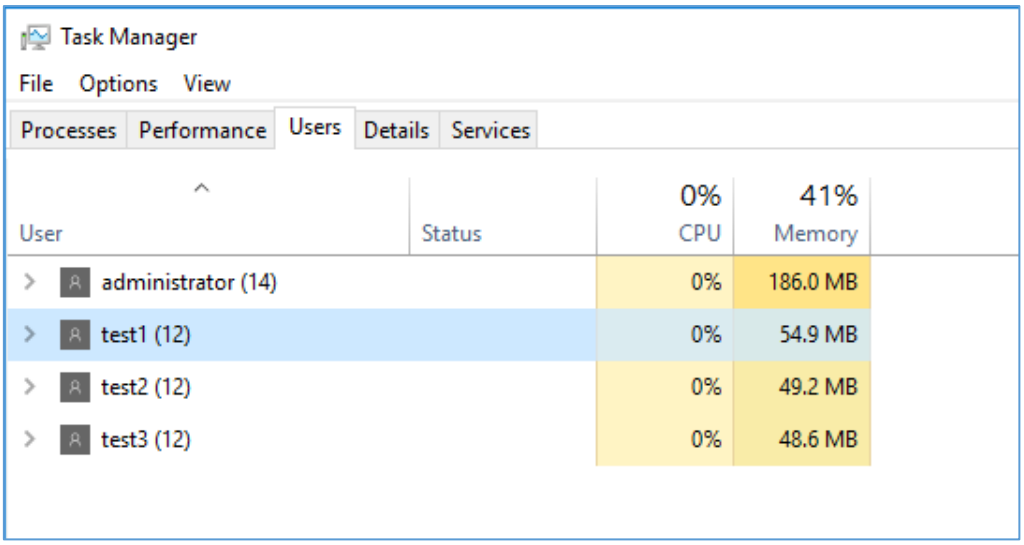
در این صفحه باید کاربرانی که می‌خواهند به این سرور دسترسی داشته باشند را با کلیک بر روی Add User or Group به لیست اضافه کنید، همانطور که مشاهده می‌کنید، سه کاربر با نام‌های Test1, Test2, Test3 به لیست اضافه شده است.



بعد از انجام مراحل بالا، دوباره وارد ویندوز ۷ شوید و سرویس Remote Dektop connection را اجرا کنید و به سرور AD با کاربرهای مشخّص‌شده، Remote بزنید.



بعد از اینکه با کاربرهای مورد نظر به سرور AD ریموت زدید، وارد آن شوید و سرویس Task Manager را اجرا کنید.



در این صفحه، وارد تب User شوید، در این تب همه‌ی کاربرانی که وارد سیستم شده‌اند، مشخّص شده است که اگر توجّه کنید، به جز کاربر Administrator، بقیّه‌ی کاربران Test1, Test2, Test3 از طریق ریموت وارد سیستم شده‌اند که چندین کاربر دیگر نیز می‌توانند به صورت هم‌زمان وارد شوند.

کار با سرویس Remote Desktop از طریق Web:

یک ویژگی خوب از این سرویس آن است که شما در هر جایی می‌توانید از طریق یک وب سایت به نرم‌افزارها و ماشین‌های مجازی خود از طریق Remote دسترسی داشته باشید که این خود می‌تواند کمک زیادی به شما کند.



Active Directory
RD License
SQL Server

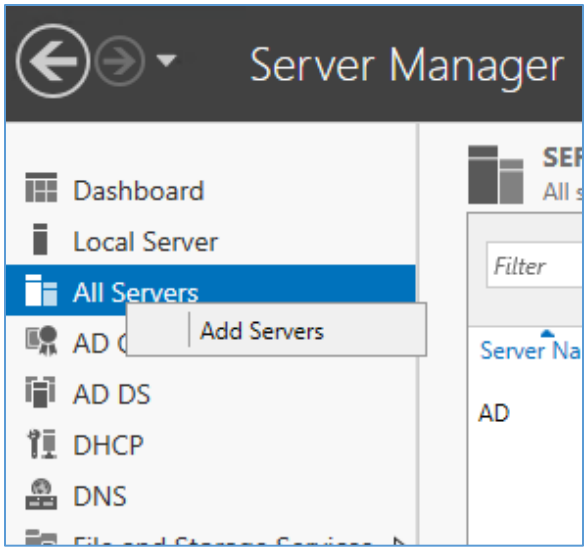
AD



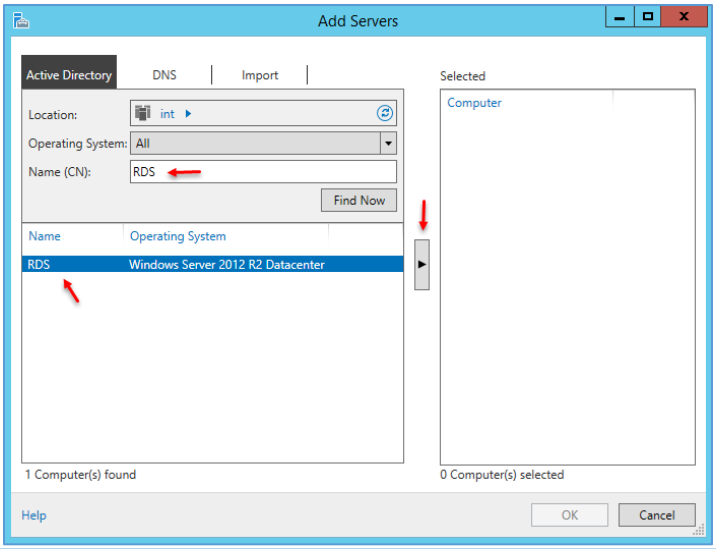
Remote Desktop Service

RDS

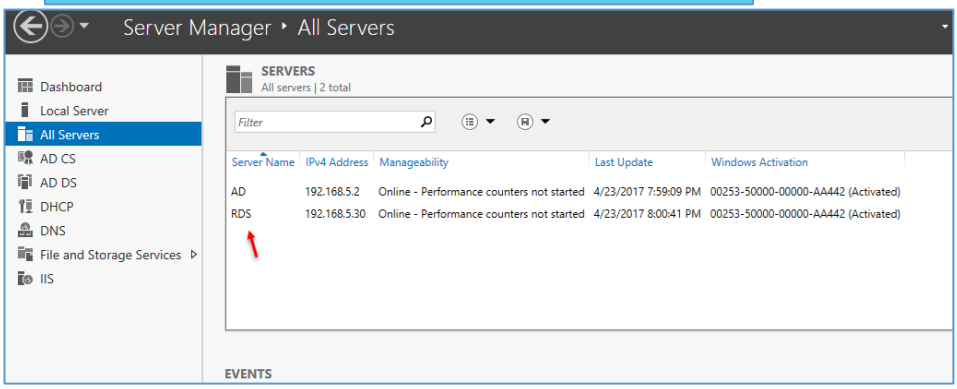
برای راه‌اندازی این سرویس، نیاز به دو سرور دارید که یکی از سرورها، Active Directory، SQL و Remote Dektop Licence است که در اینجا سرور AD را برای این کار انتخاب کردیم، سرور دوّم با نام RDS ایجاد کنید که بر روی این سرور نیز باید ویندوز سرور ۲۰۱۶ نصب و آن را عضو دومین کنید.



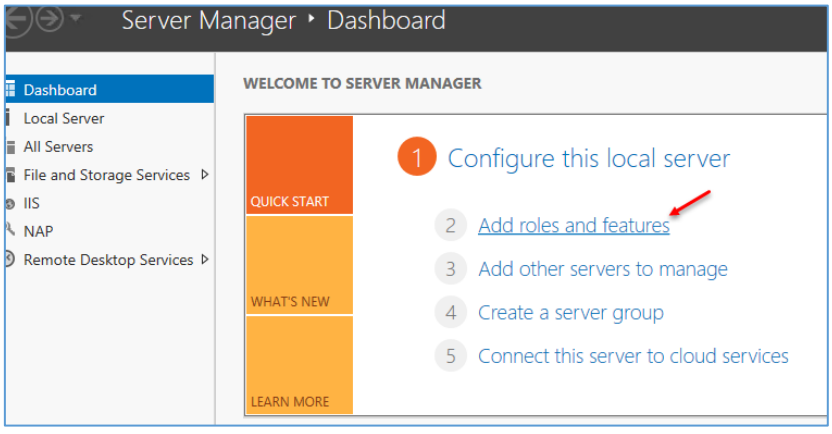
برای شروع کار وارد سرور AD شوید و Server Manager را اجرا کنید، از سمت چپ بر روی ALL Servers، کلیک راست کنید و بر روی Add Servers کلیک کنید.



به مانند شکل، در قسمت Name، نام سروری را که ایجاد کردید را وارد کنید که در اینجا سرور ما، RDS بوده است، بعد از پیدا کردن آن بر روی جهت‌نما کلیک و سرور را به لیست اضافه کنید و بر روی OK کلیک کنید.

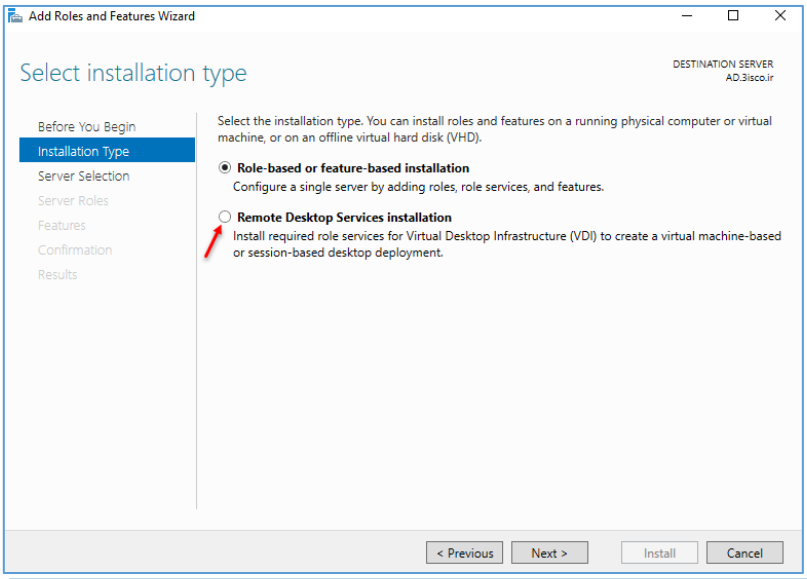


در این قسمت، هر دو سرور را مشاهده می‌کنید، در ادامه، همه‌ی کارها را در سرور AD انجام خواهیم داد.

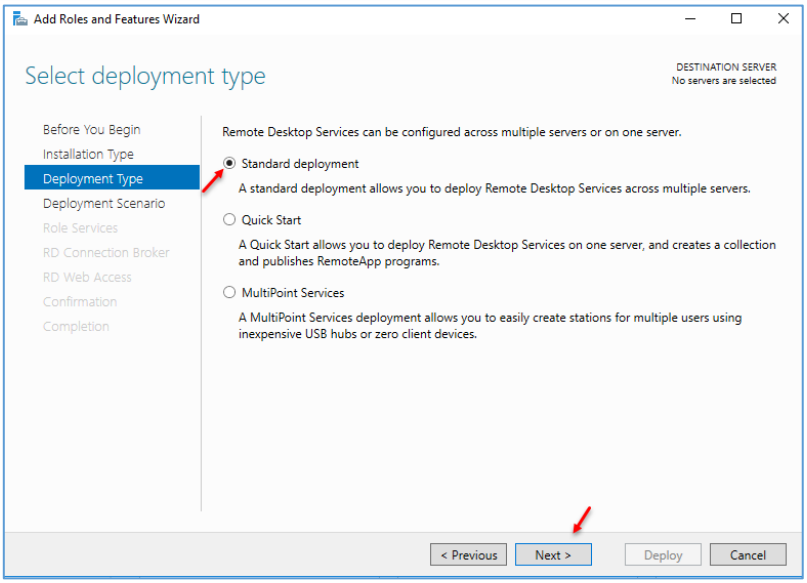


برای شروع کار وارد Dashboard شوید و بر روی Add roles and Feature کلیک کنید.

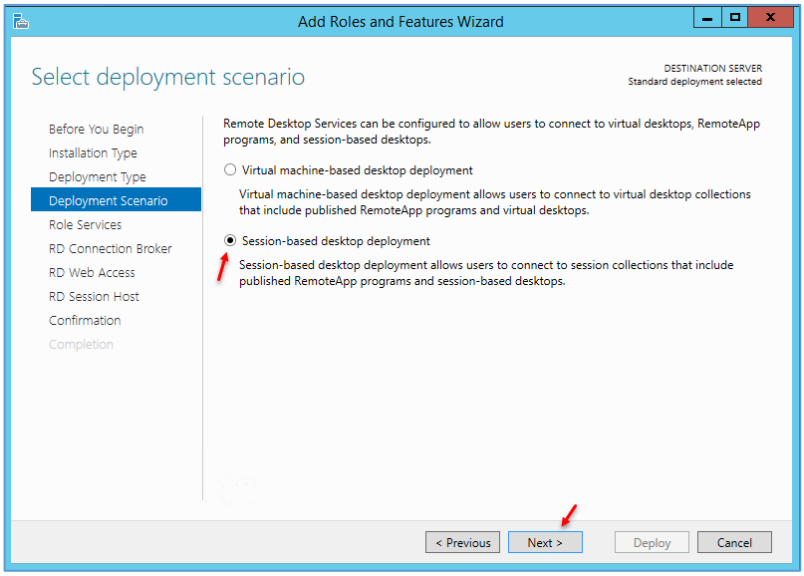
تذکّر: همه‌ی عملیّات در سرور AD انجام می‌شود.



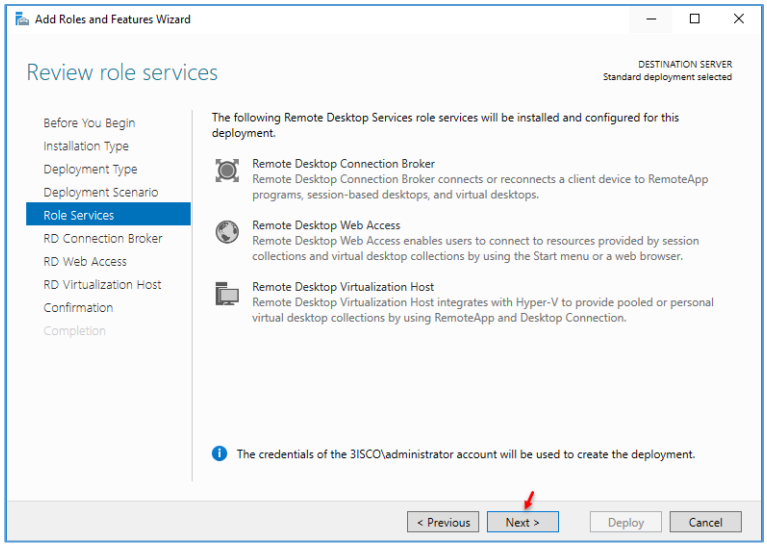
در این صفحه، گزینه‌ی Remote Desktop Services Install ation را انتخاب و بر روی Next کلیک کنید.



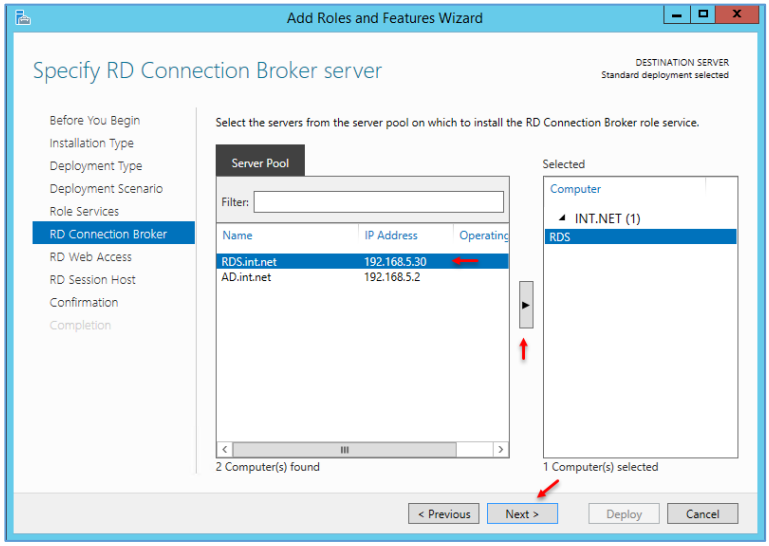
در این صفحه، گزینه‌ی Standard را انتخاب و بر روی Next کلیک کنید.



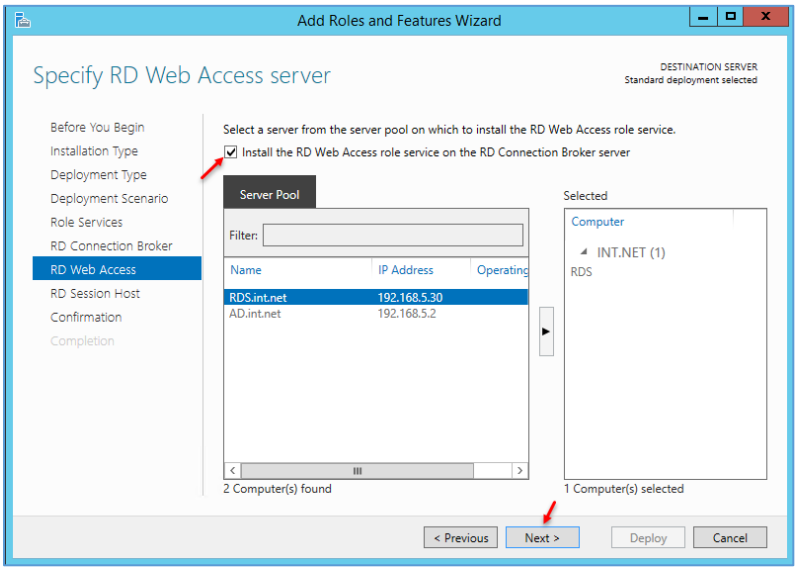
در این قسمت، گزینه‌ی Session-based desktop deployment را انتخاب و بر روی کلیک Next کنید.



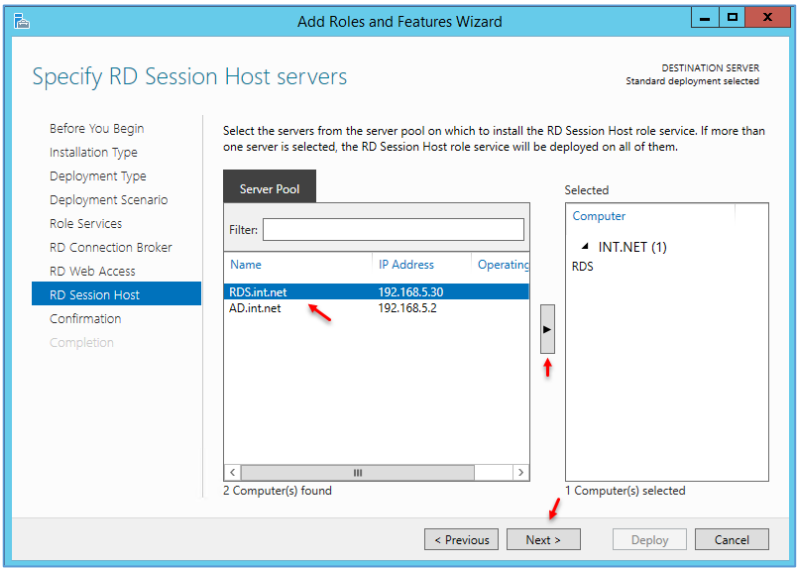
در این صفحه بر روی Next کلیک کنید.



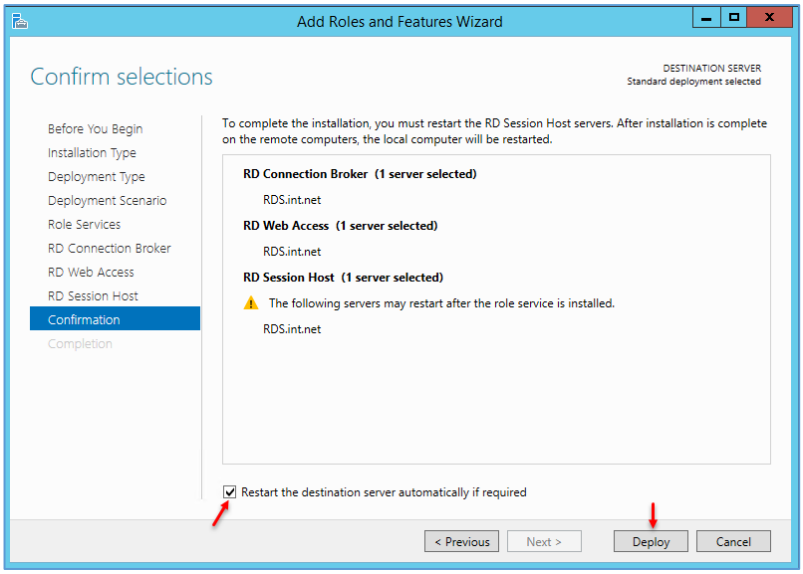
در این صفحه، هر دو سرور RDS و AD مشخّص شده است که در این مرحله باید گزینه‌ی RDS را انتخاب و به لیست اضافه کنید و بر روی Next کلیک کنید.



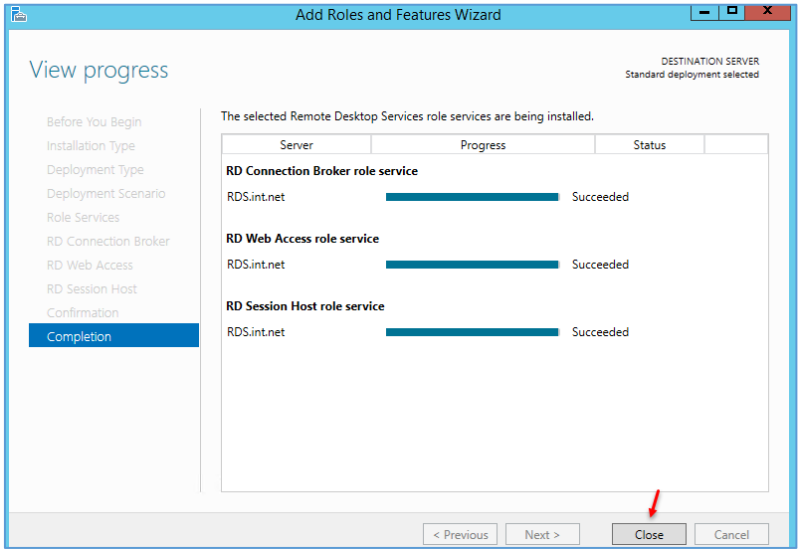
در این قسمت، تیک گزینه‌ی Install the RD web access roles را انتخاب و بر روی Next کلیک کنید.



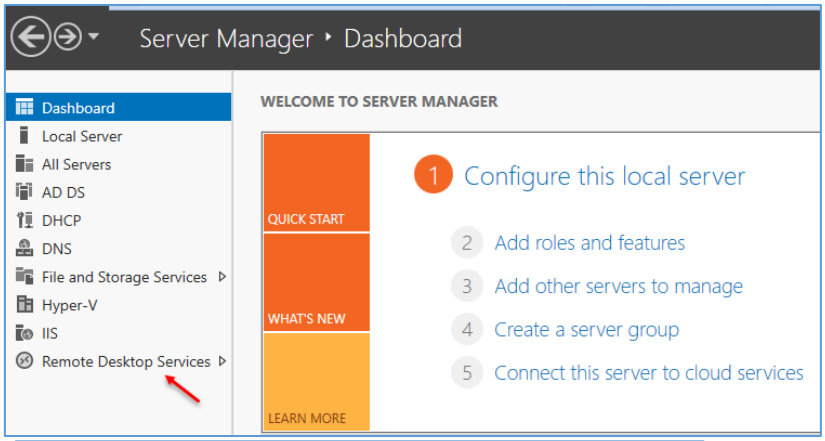
در این صفحه بر روی جهت‌نما کلیک کنید و سرور RDS را به لیست اضافه و بر روی Next کلیک کنید.



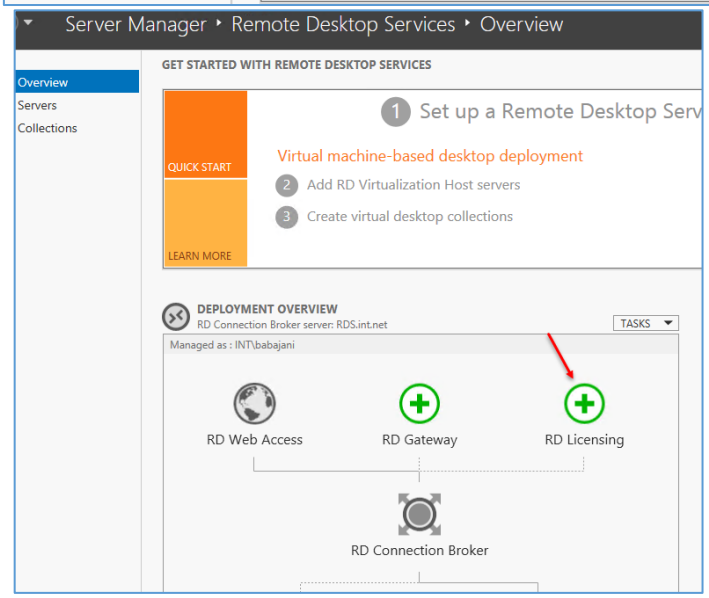
در این صفحه، تیک گزینه‌ی Restart... را انتخاب و بر روی Deploy کلیک کنید تا کار پیکربندی آغاز شود، بعد از پایان کار، سرور RDS به صورت از راه دور Restart خواهد شد.



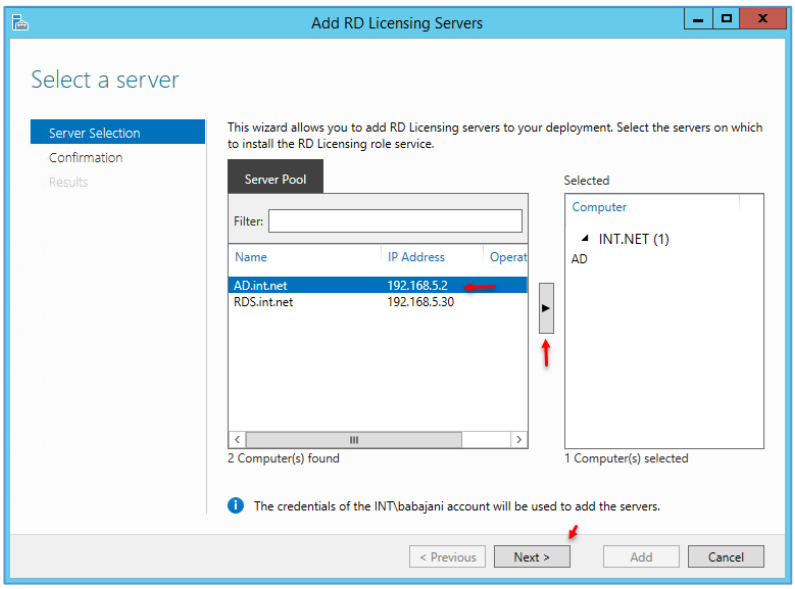
بعد از Restart شدن سرور، شکل روبرو ظاهر خواهد شد که به شما اعلام می‌دارد، هر سه قسمت به درستی پیکربندی شده است.



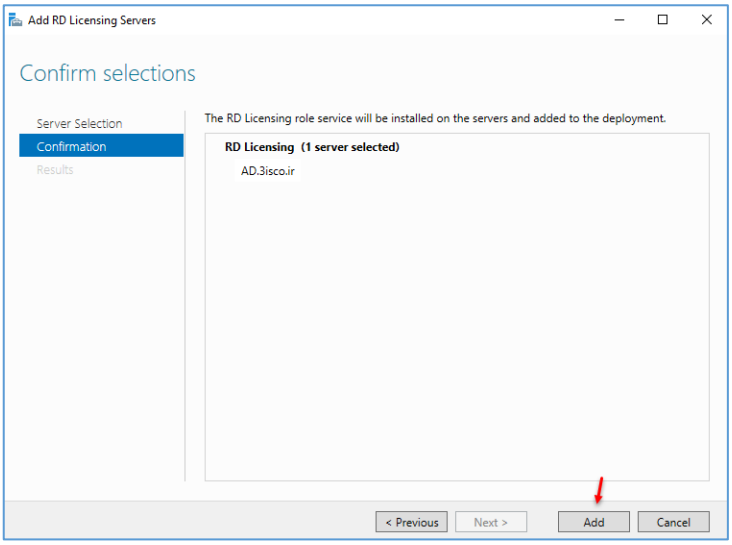
بعد از انجام عملیّات بالا، وارد Server Manager شوید و از سمت چپ بر روی Remote Desktop Services کلیک کنید.



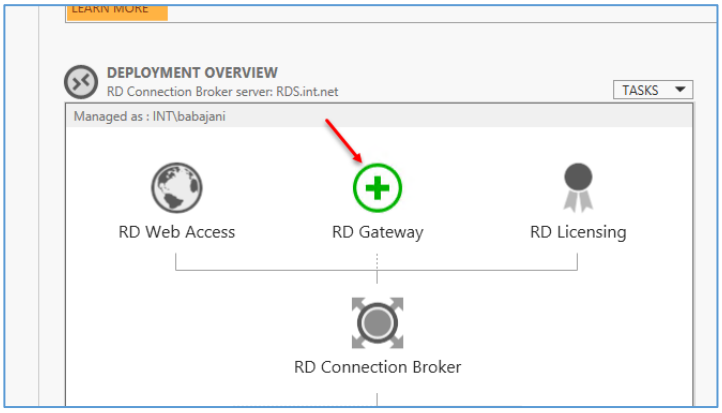
در این صفحه بر روی RD Licensing کلیک کنید تا شکل بعد ظاهر شود.



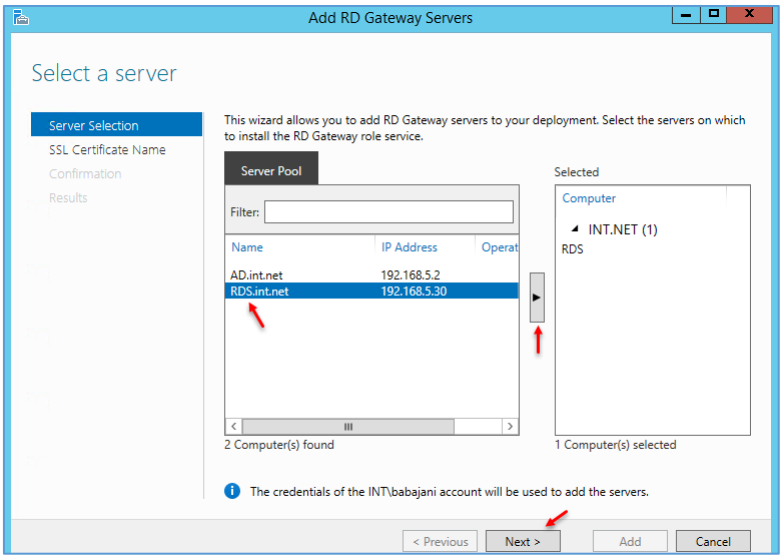
در این صفحه، سرور دومین که به عنوان لایسنس انتخاب شده است را انتخاب و بر روی جهت‌نمای مورد نظر کلیک و سرور را به لیست اضافه کنید و بر روی Next کلیک کنید.



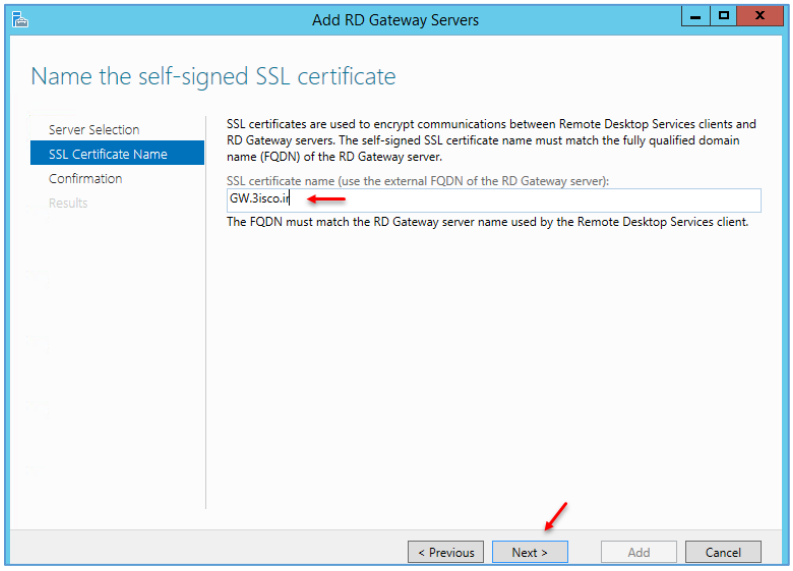
در این صفحه بر روی Add کلیک کنید تا عملیّات نصب انجام شود.



در ادامه بر روی RD Gateway کلیک کنید تا شکل بعد ظاهر شود.

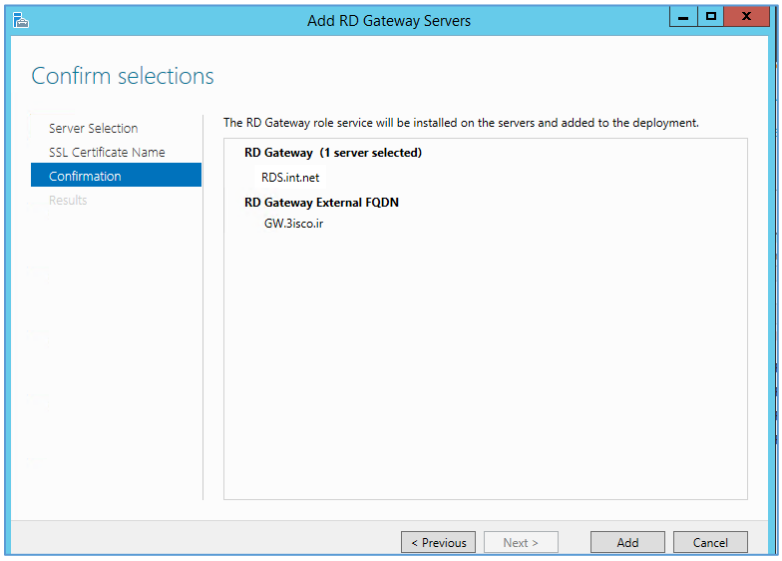


در این قسمت بر روی فلش مورد نظر کلیک و سرور را به لیست اضافه و بر روی Next کلیک کنید.

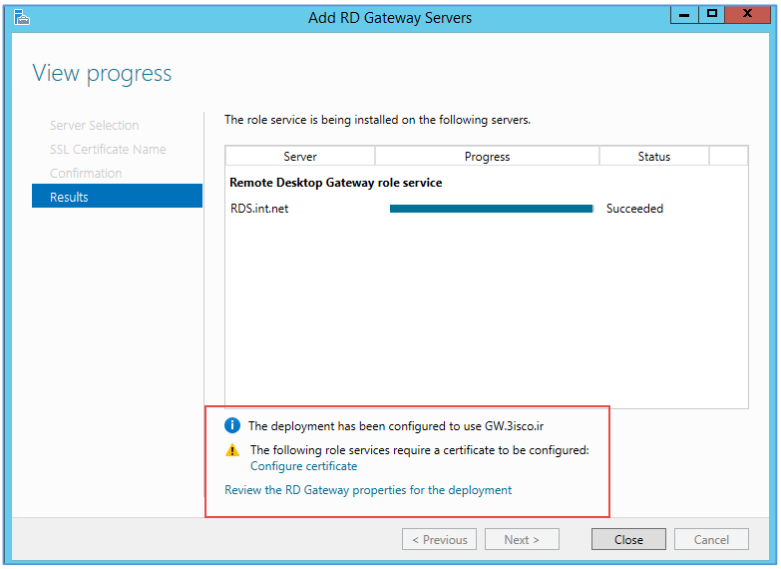


در این صفحه، نیاز به یک نام خارجی دارید که به سرور RDS متّصل باشد، در اینجا، نام GW را به همراه نام دومین خارجی وارد کنید و بعد از آن باید در DNS، این نام را به سرور RDS ارتباط دهید.

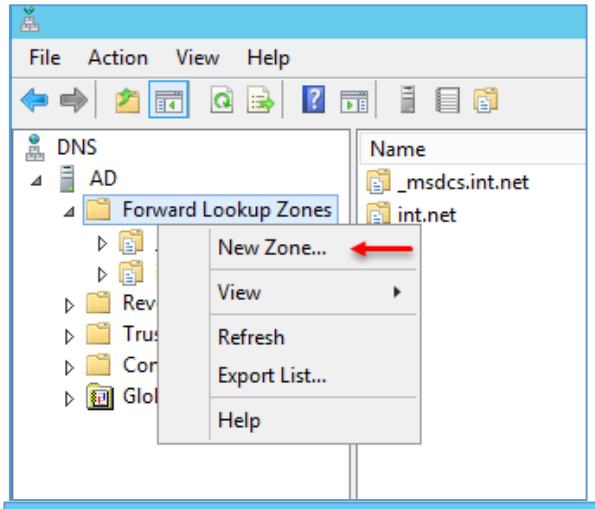
بر روی Next کلیک کنید.



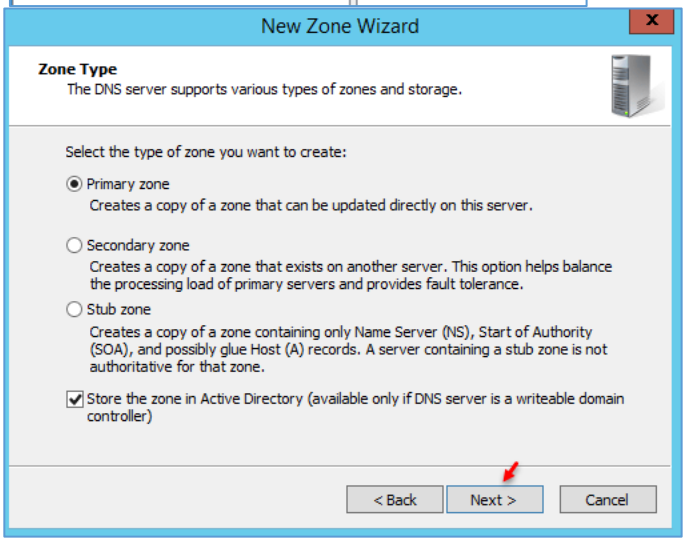
در این قسمت بر روی Add کلیک کنید تا عملیّات انجام شود.



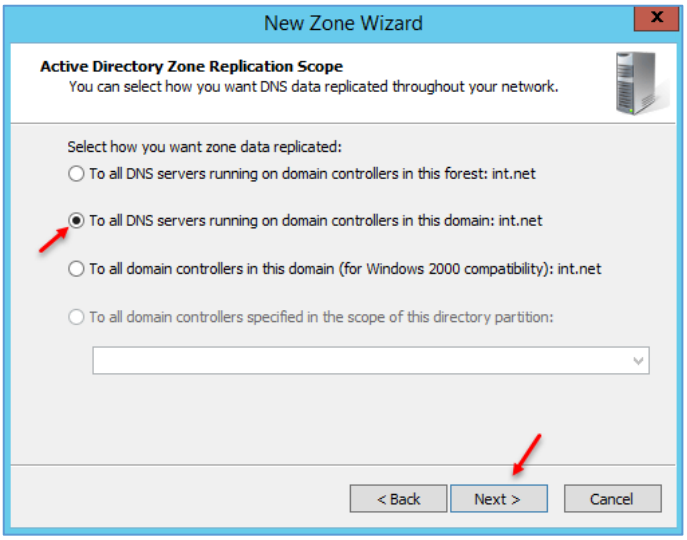
در این قسمت، بعد از نصب با پیغام Configure Certificate مواجه می‌شوید که در ادامه، آن را تکمیل خواهیم کرد، بر روی Close کلیک کنید.



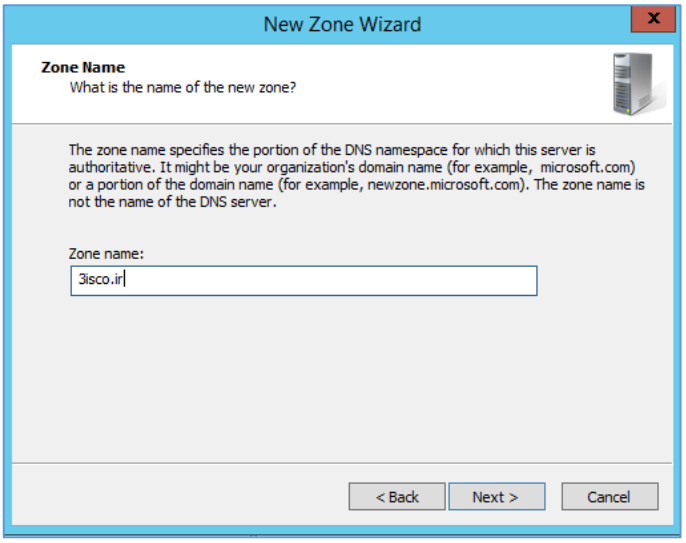
بعد از انجام مراحل بالا باید آن نام که وارد کردیم (GW.3isco.ir) را در سرویس DNS ایجاد کنیم، لذا باید سرویس DNS را اجرا و به مانند شکل روبرو بر روی forward LoOKup Zones کلیک راست و گزینه‌ی New Zone را انتخاب کنیم.



در این صفحه، گزینه‌ی Primary Zone را انتخاب و بر روی Next کلیک کنید.



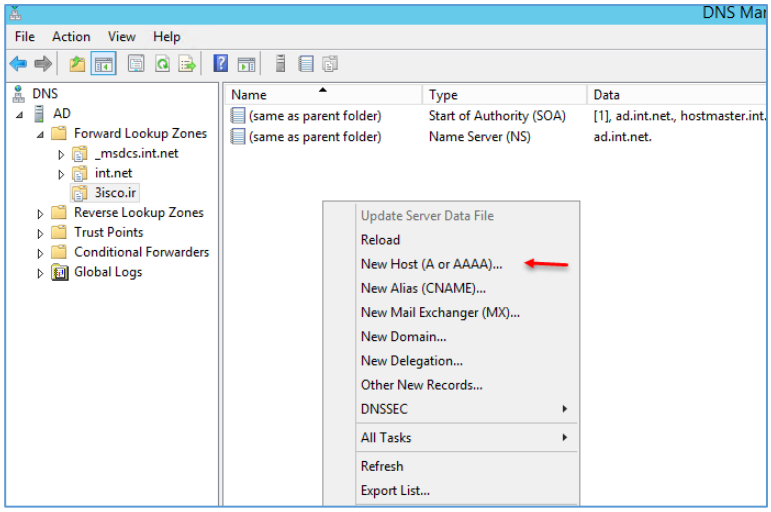
در این صفحه، گزینه‌ی دوّم را انتخاب و بر روی Next کلیک کنید.



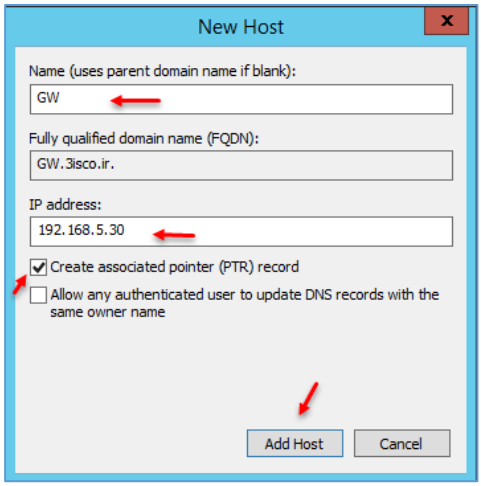
در این صفحه، نام دومین خارجی خود را وارد و بر روی **Next** کلیک کنید.



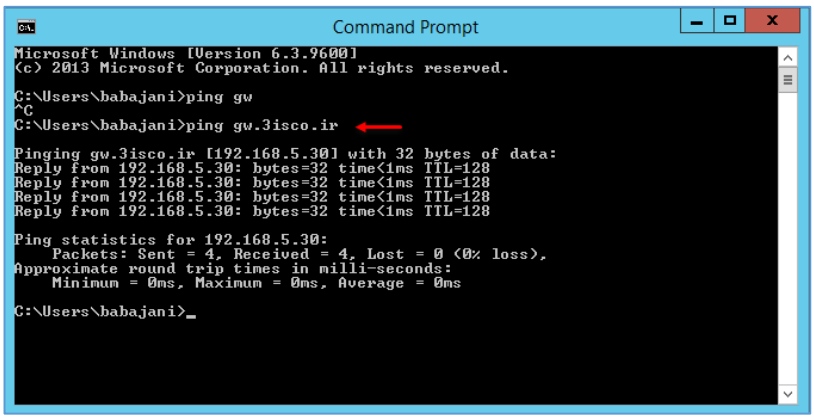
در این صفحه، گزینه‌ی اوّل را انتخاب و بر روی **Next** کلیک کنید و در آخر کار نیز بر روی **Finish** کلیک کنید.



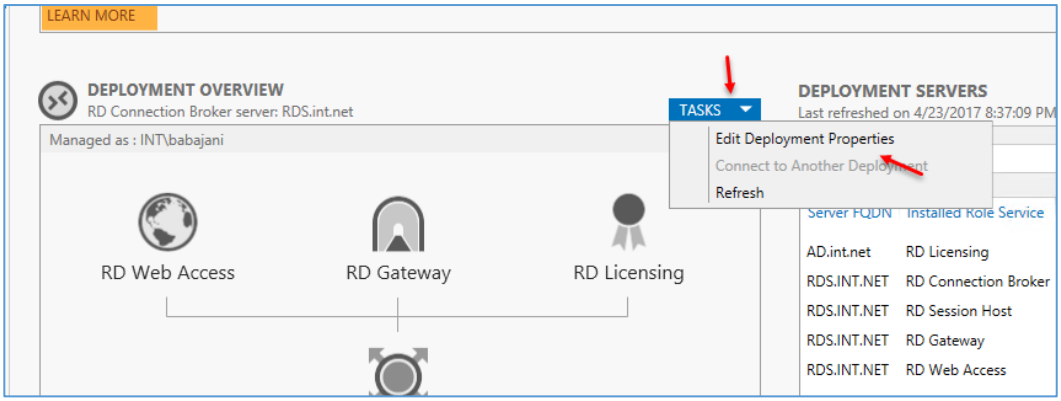
بعد از ایجاد دومین، از سمت چپ بر روی نام دومین کلیک کنید و در صفحه‌ی باز شده کلیک راست کنید و گزینه‌ی **New Host** را انتخاب کنید.



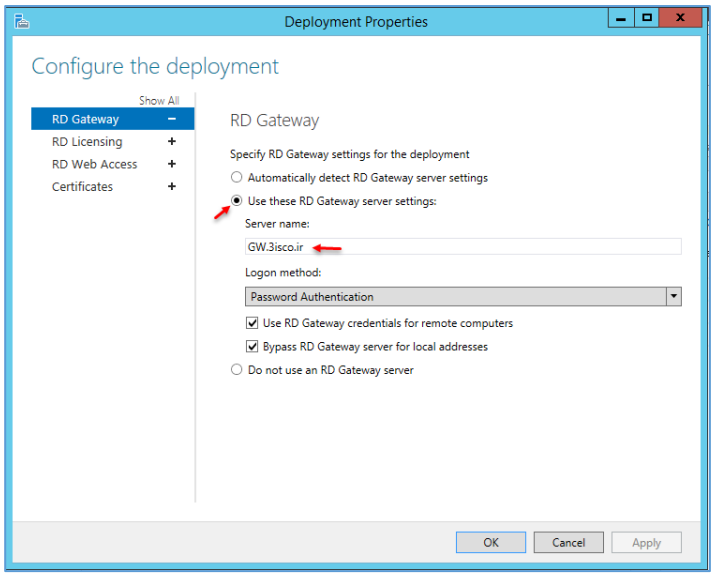
در این صفحه و در قسمت Name، نام سروری که در قسمت قبل وارد کردیم را وارد می‌کنیم و IP آن را همان، آدرس سرور RDS قرار می‌دهیم و در آخر، تیک گزینه‌ی Create Associated را انتخاب و بر روی Add Host کلیک می‌کنیم.



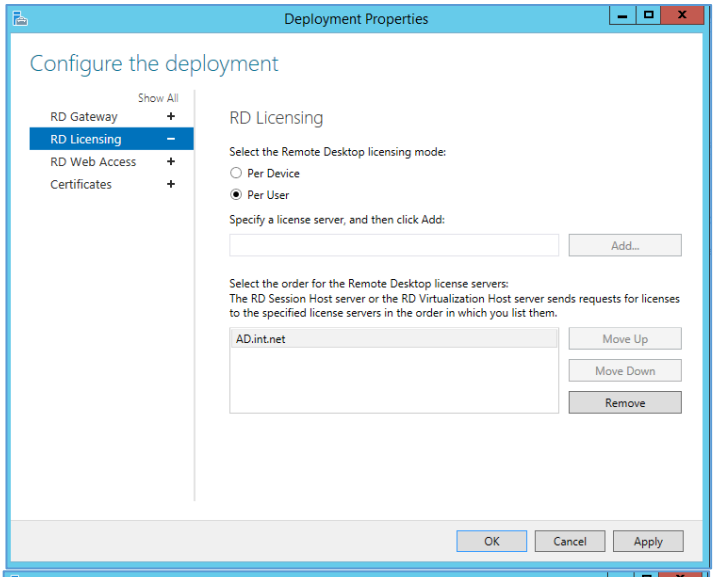
بعد از ایجاد تنظیمات در DNS، اگر نام را به همراه نام دومین Ping کنیم، نتیجه به مانند شکل روبرو مشخّص خواهد شد.



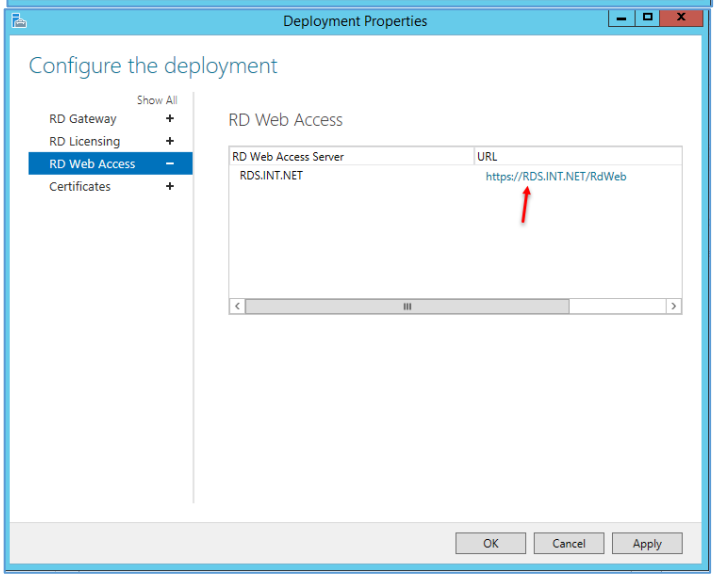
در ادامه بر روی Tasks کلیک کنید و گزینه‌ی Edit Deployment Properties را انتخاب کنید.



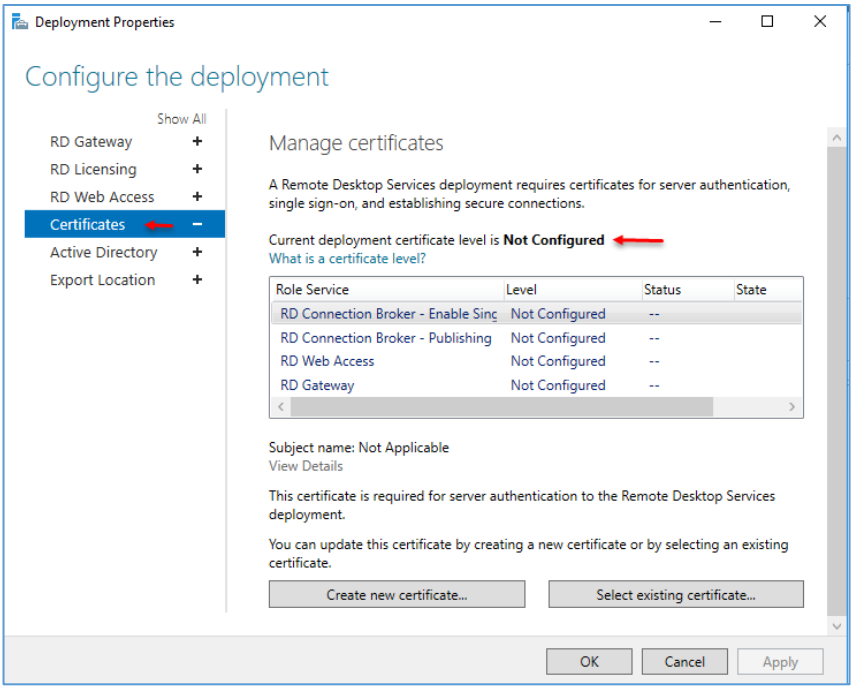
در این صفحه، تیک گزینه‌ی Use these RD Gateway Server Settings را انتخاب کنید و در ادامه، وارد تب RD Licensing شوید.



در این قسمت، گزینه‌ی Per User را انتخاب کنید و وارد تب RD Web Access شوید.



در این صفحه می توانید آدرس دسترسی به سرویس را از طریق وب سایت مشاهده کنید که در ادامه از آن استفاده خواهیم کرد؛ وارد Certificates شوید.



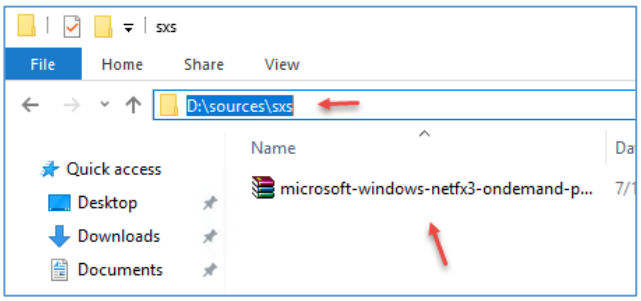
در قسمت Certificate باید یک‌سری گواهینامه را پیکربندی کنید که قبل از آن باید نرم افزار SQL را نصب کنید و به سرویس Remote Desktop متّصل کنید تا این سرویس بتواند اطّلاعات خود را در SQL قرار دهد.

برای دانلود نرم‌افزار SQL 2016 از لینک زیر استفاده کنید:

http://p30download.com/fa/entry/51495/%D8%AF%D8%A7%D9%86%D9%84%D9%88%D8%AF-microsoft-sql-server-2014-sp2-x86

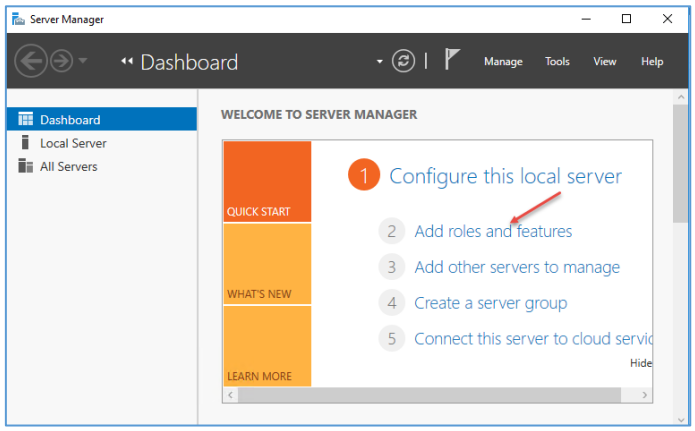
نصب Net FramWork 3.5:

به صورت پیش‌فرض، Net 3.5 بر روی ویندوز ۲۰۱۶ نصب نشده است و برای نصب آن، نیاز به DVD مربوط به آن دارید تا فایل Net 3.5 را دریافت کنید، برای این کار DVD را داخل دستگاه قرار دهید و وارد آدرس زیر شوید.

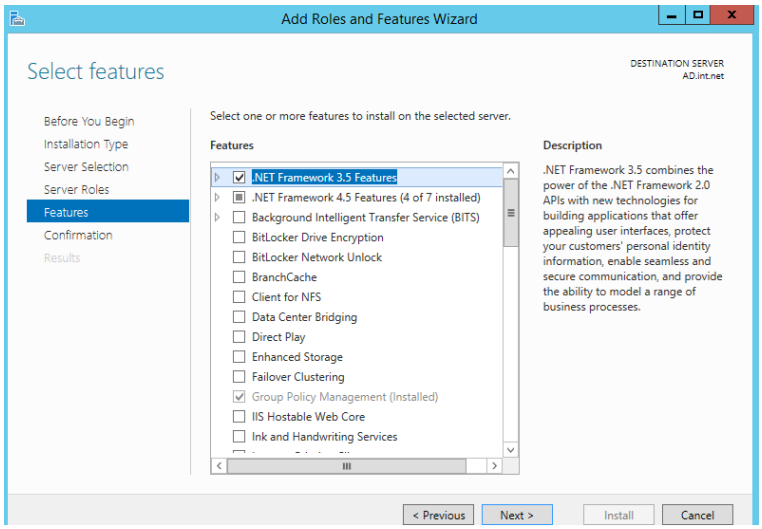


به مانند شکل، آدرس مورد نظر را کپی کنید تا در ادامه از آن استفاده کنید.

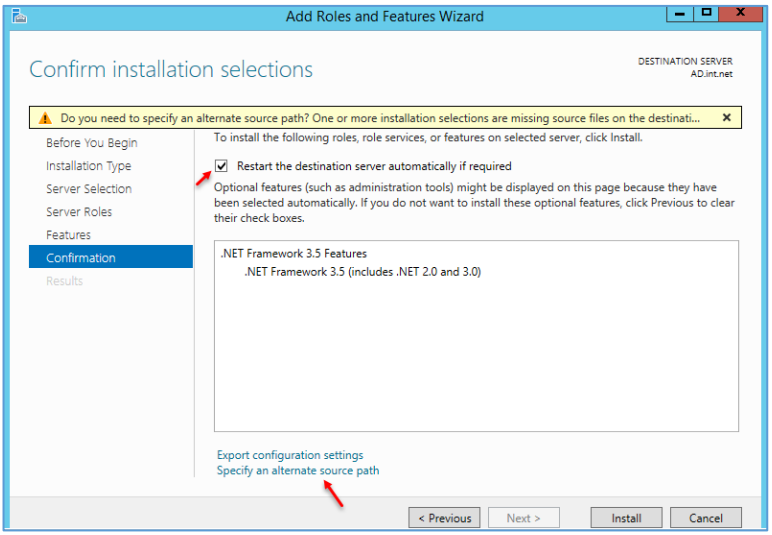
نکته: در هر دو سرور باید Net 3.5 نصب شود.



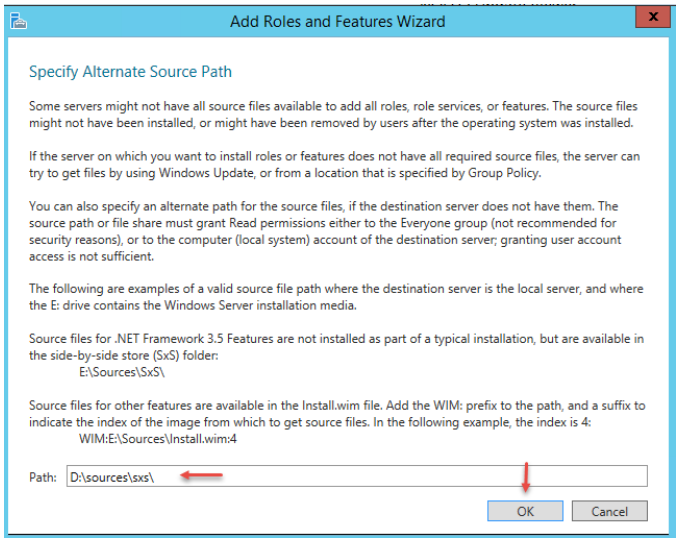
بعد از کپی کردن آدرس وارد Server Manager شوید و بر روی Add roles and Features کلیک کنید.



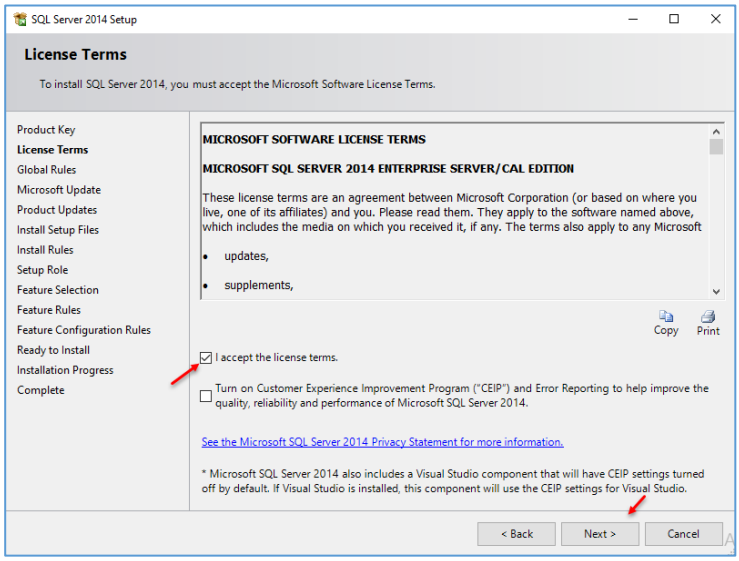
در صفحه‌ی Features، تیک گزینه‌ی .NET Framework 3.5 را انتخاب و بر روی Next کلیک کنید.



در این صفحه بر روی Export Configuration settings کلیک کنید.

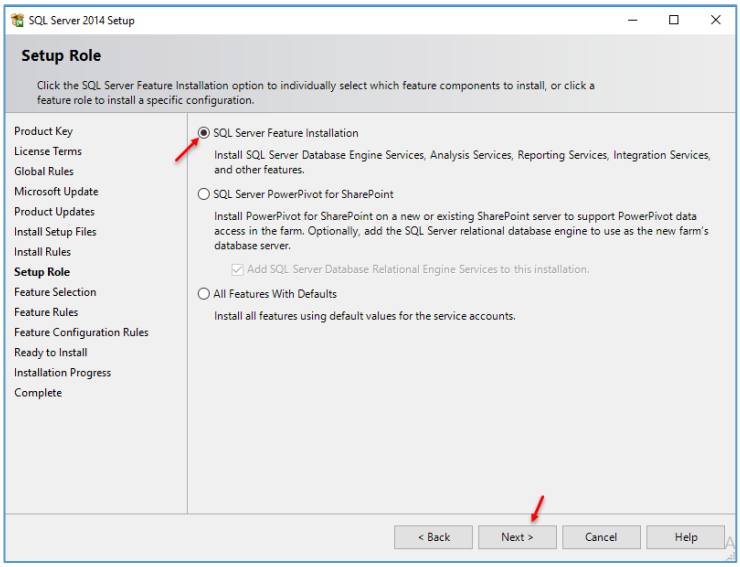


در این قسمت، آدرس مورد نظر را که از قبل کپی کردید، وارد و بر روی OK کلیک کنید و در صفحه‌ی بعد بر روی Install کلیک کنید تا Net 3.5 بر روی سرور نصب شود.

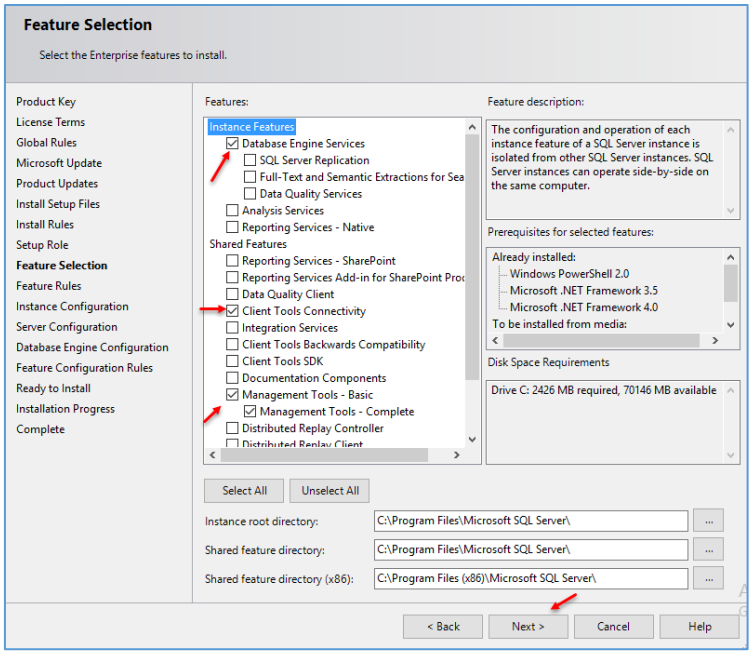


بعد از نصب Net 3.5 بر روی فایل Setup نرم‌افزار SQL کلیک کنید.

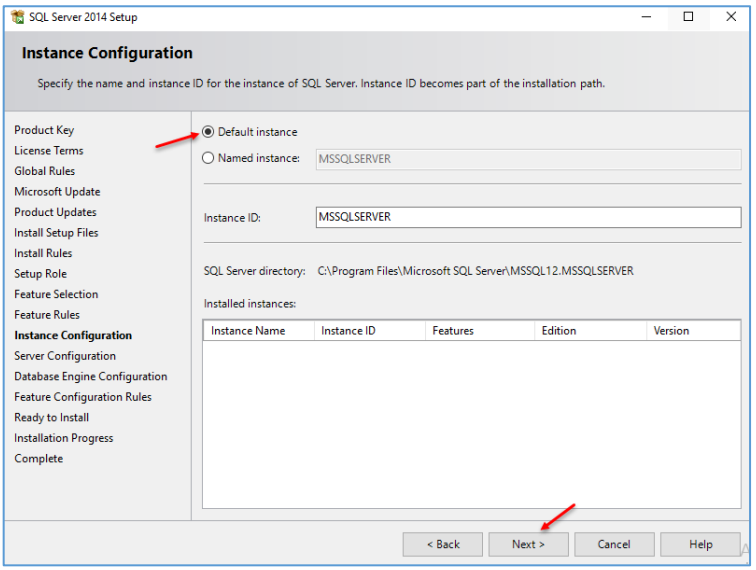
اگر در این صفحه، قرارداد استفاده از نرم‌افزار را قبول دارید، گزینه‌ی I accept the license terms را انتخاب و بر روی Next کلیک کنید.



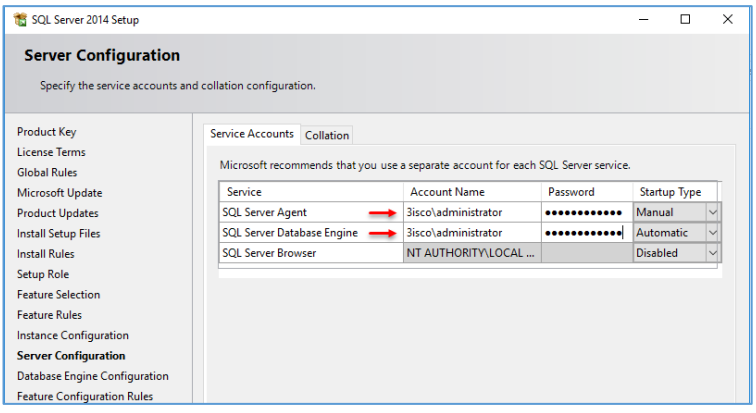
در این صفحه، گزینه‌ی SQL Server Feature Install ation را انتخاب و بر روی Next کلیک کنید.



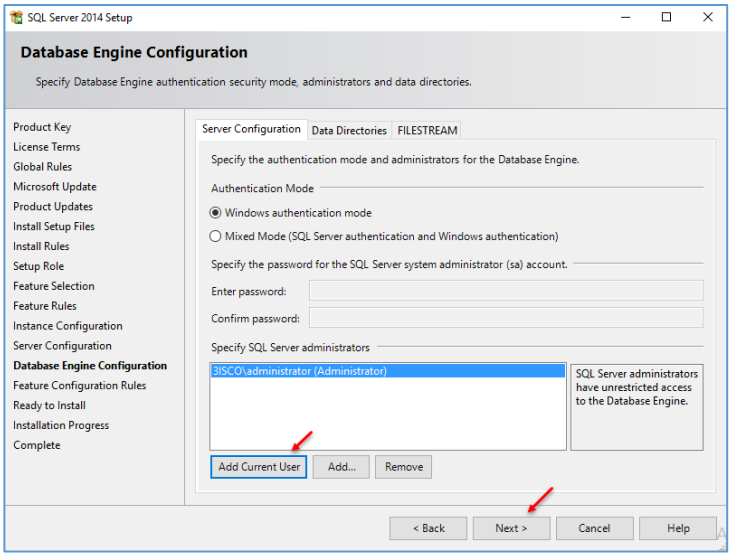
در این صفحه باید Feature های خود را انتخاب کنید، به مانند شکل عمل کنید و بر روی Next کلیک کنید.



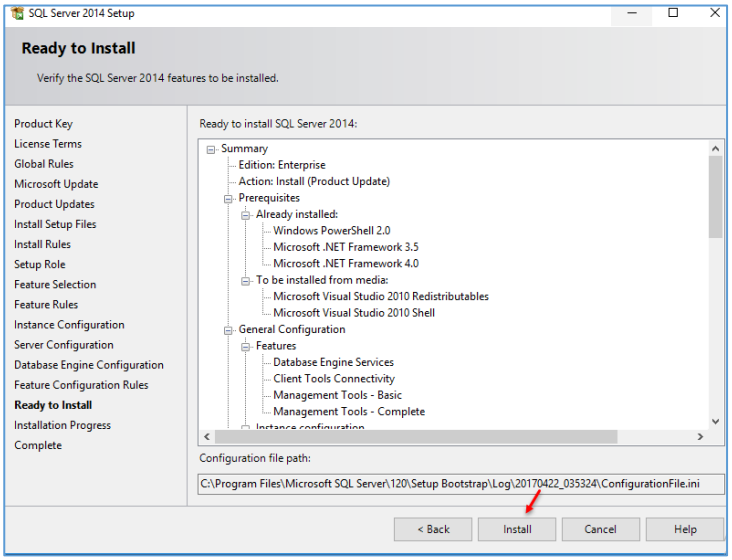
در این قسمت، گزینه‌ی پیش‌فرض را انتخاب و بر روی Next کلیک کنید.



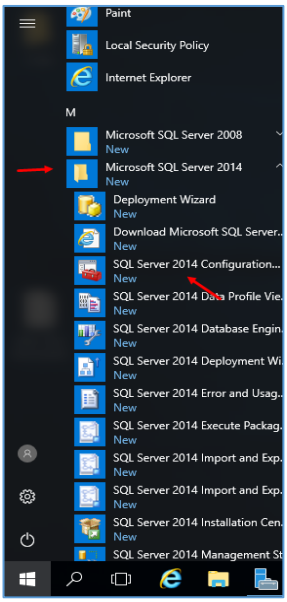
در این صفحه، نام کاربری اصلی شبکه‌ی خود را به همراه نام دومین در جای مشخّص‌شده وارد و بر روی Next کلیک کنید.



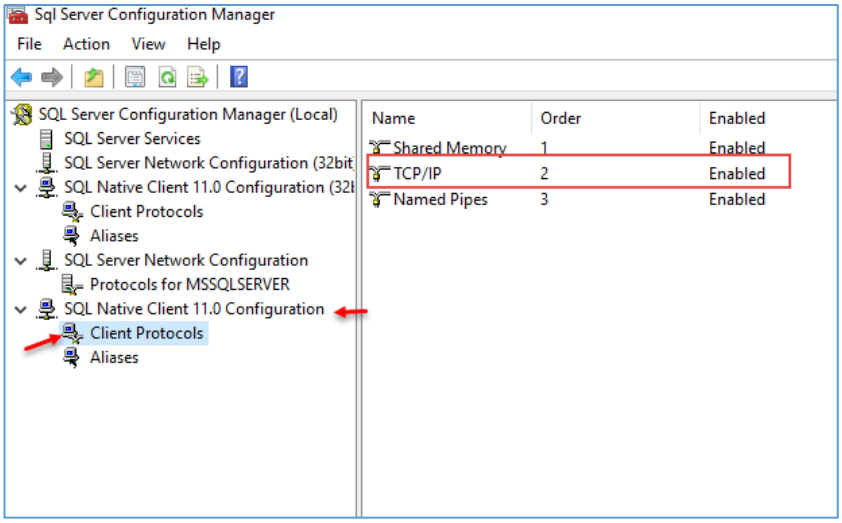
در این صفحه بر روی Add Current User کلیک کنید و کاربر مورد نظر خود را به لیست، اضافه و بر روی Next کلیک کنید؛ با این کار، کاربری که با آن اقدام به نصب SQL می‌کنید، دسترسی کامل به سرور را خواهد داشت.



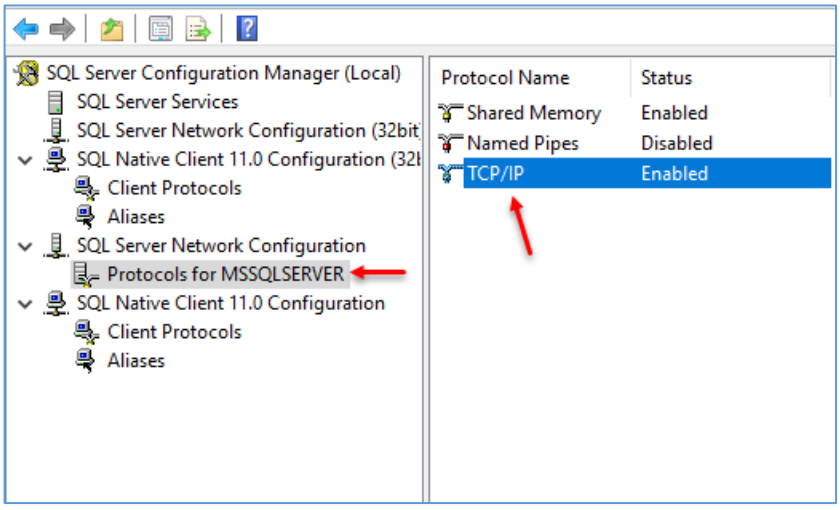
در قسمت آخر نیز بر روی Install کلیک کنید تا کار نصب آغاز شود، بعد از نصب، سرور را Restart کنید.



وارد سرور شوید و از قسمت Start وارد Microsoft SQL Server 2014 شوید و گزینه‌ی مورد نظر را اجرا کنید.

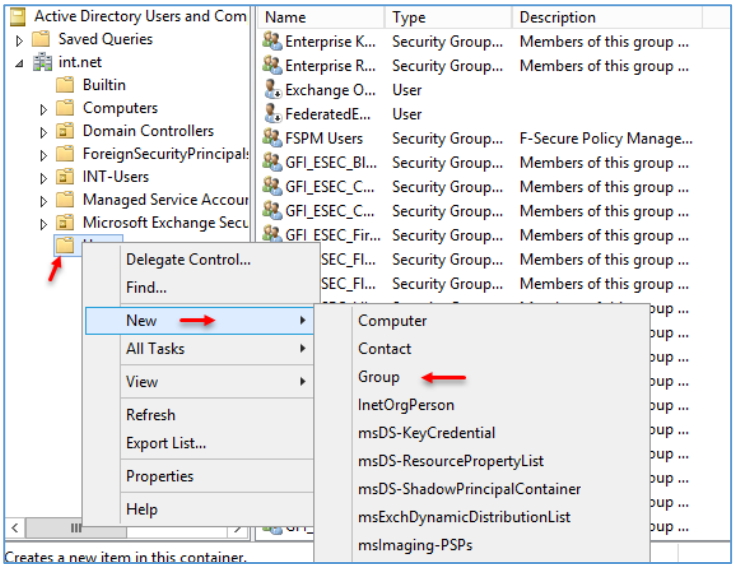


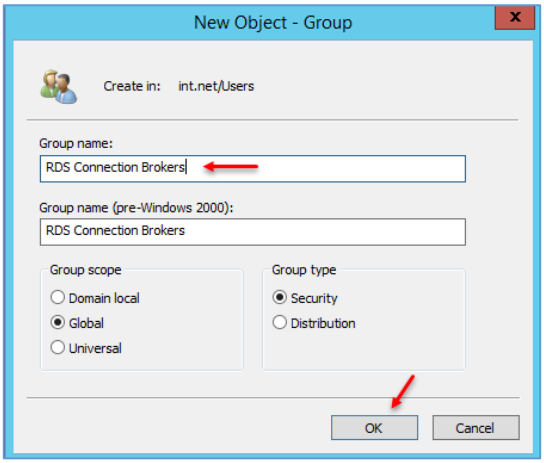
در این صفحه باید به مانند شکل روبرو گزینه‌ی TCP/IP فعّال شده باشد.



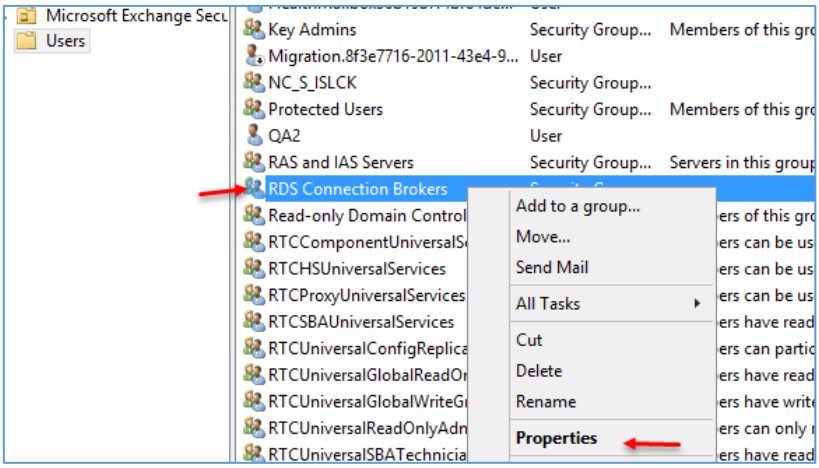
در این صفحه نیز باید گزینه‌ی TCP/IP فعّال باشد.

بعد از انجام تنظیمات مربوط به نرم‌افزار SQL، برای راه‌اندازی سرویس Remote Desktop نیاز دارید تا یک گروه با نام RDS Connection BrOKers در سرویس Active Directory ایجاد کنید و هر دو سرور خود را عضو این گروه کنید و در ادامه، در نرم‌افزار SQL به این گروه برای ایجاد دیتابیس دسترسی لازم را بدهید؛ برای شروع وارد سرویس Active Directory users and computers شوید و بر روی Users کلیک راست کنید و از قسمت New، گزینه‌ی Group را انتخاب کنید.

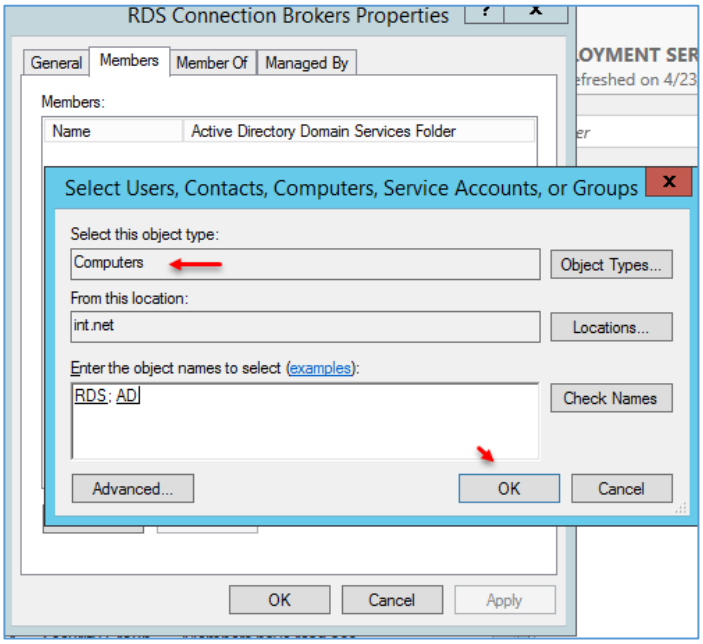




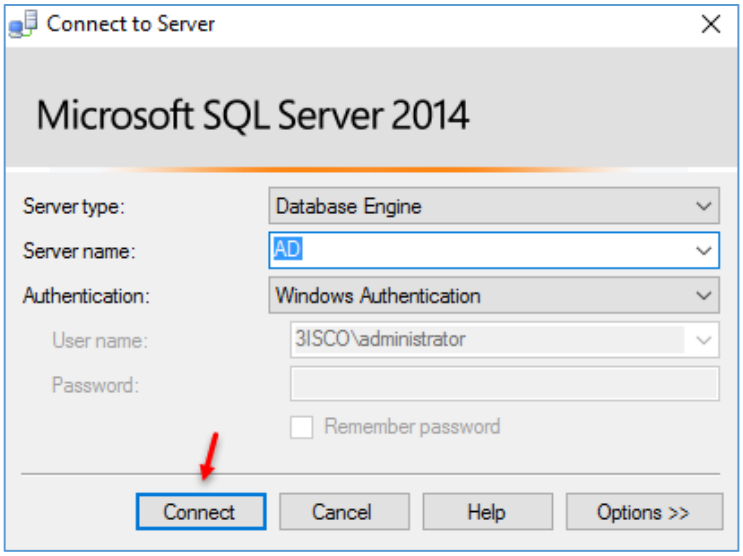
در این صفحه، نام گروه که RDS Connection BrOKers است را وارد و بر روی OK کلیک کنید.



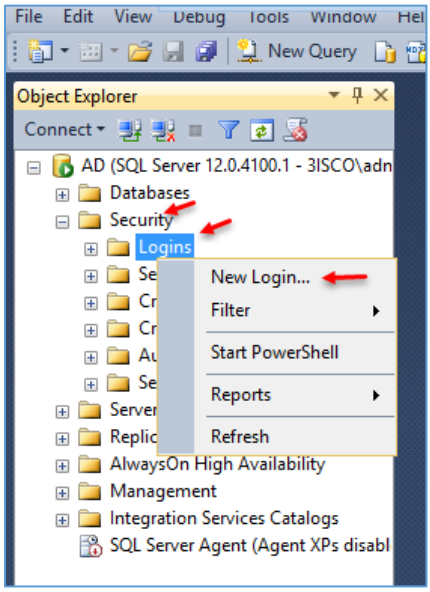
در ادامه بر روی گروهی که ایجاد کردید، کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



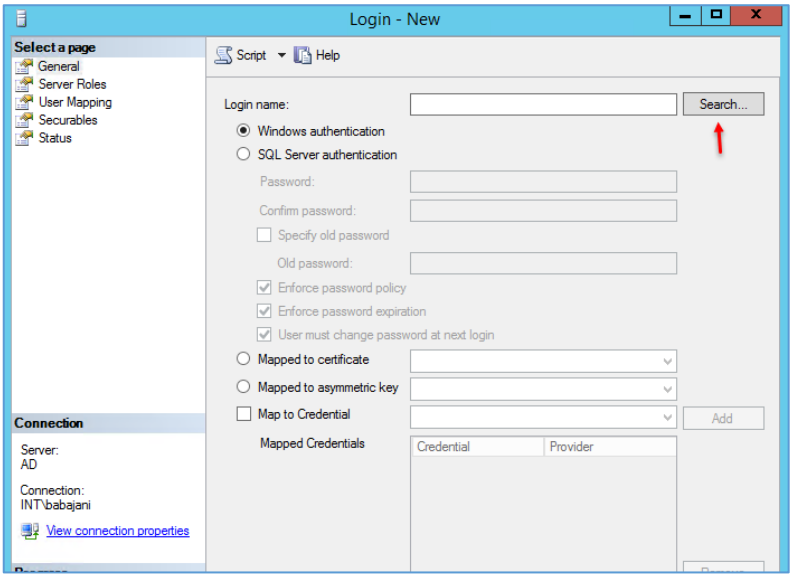
در این صفحه وارد تب Members شوید و بر روی Add کلیک کنید و در صفحه‌ی بازشده، از قسمت Object، گزینه‌ی Computers را انتخاب کنید و در صفحه‌ی مورد نظر، به مانند شکل روبرو نام هر دو سرور را وارد و بر روی OK کلیک کنید.



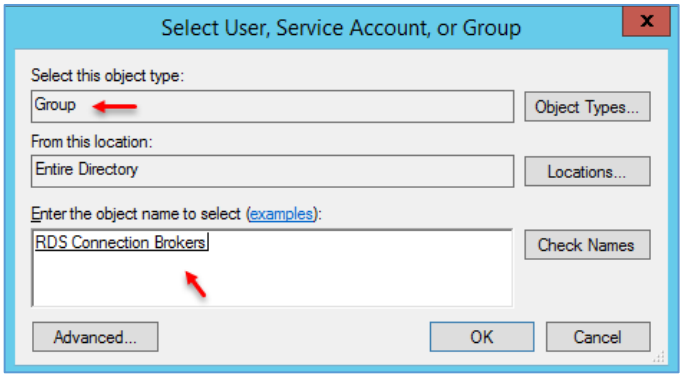
بعد از انجام عملیّات بالا از طریق start، سرویس SQL Server Management studio را اجرا کنید و در شکل بازشده بر روی Connect کلیک کنید.



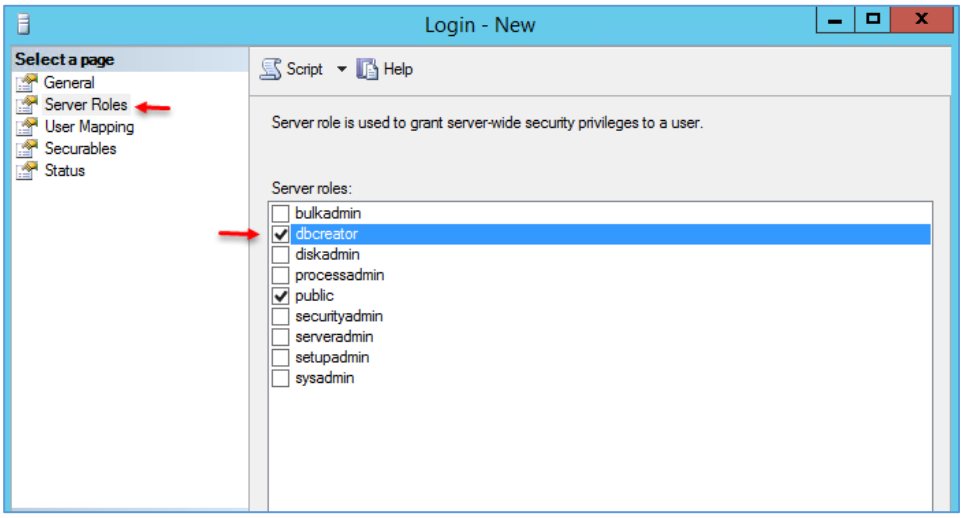
در قسمت Security بر روی Login کلیک راست کنید و گزینه‌ی New Login را انتخاب کنید.



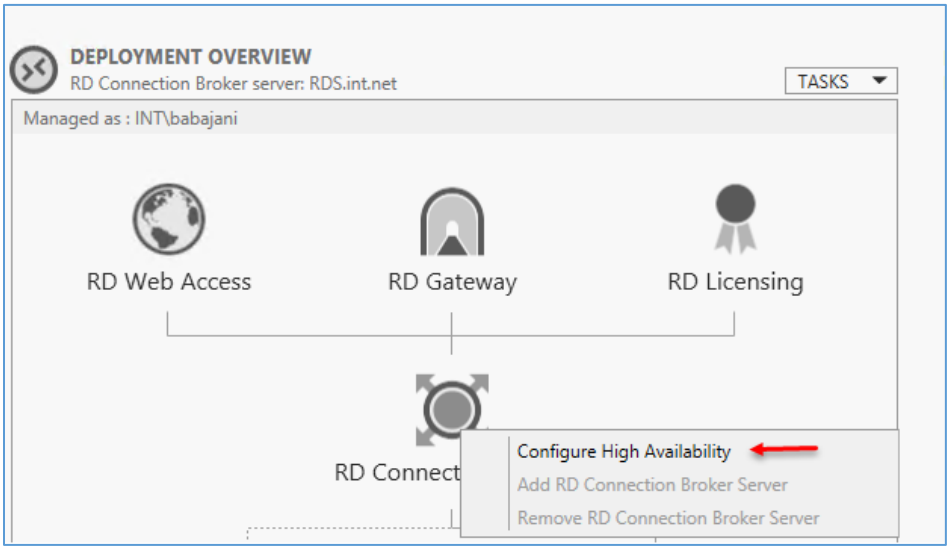
در این صفحه، برای اینکه گروه خود را اضافه کنید باید بر روی Search کلیک کنید.



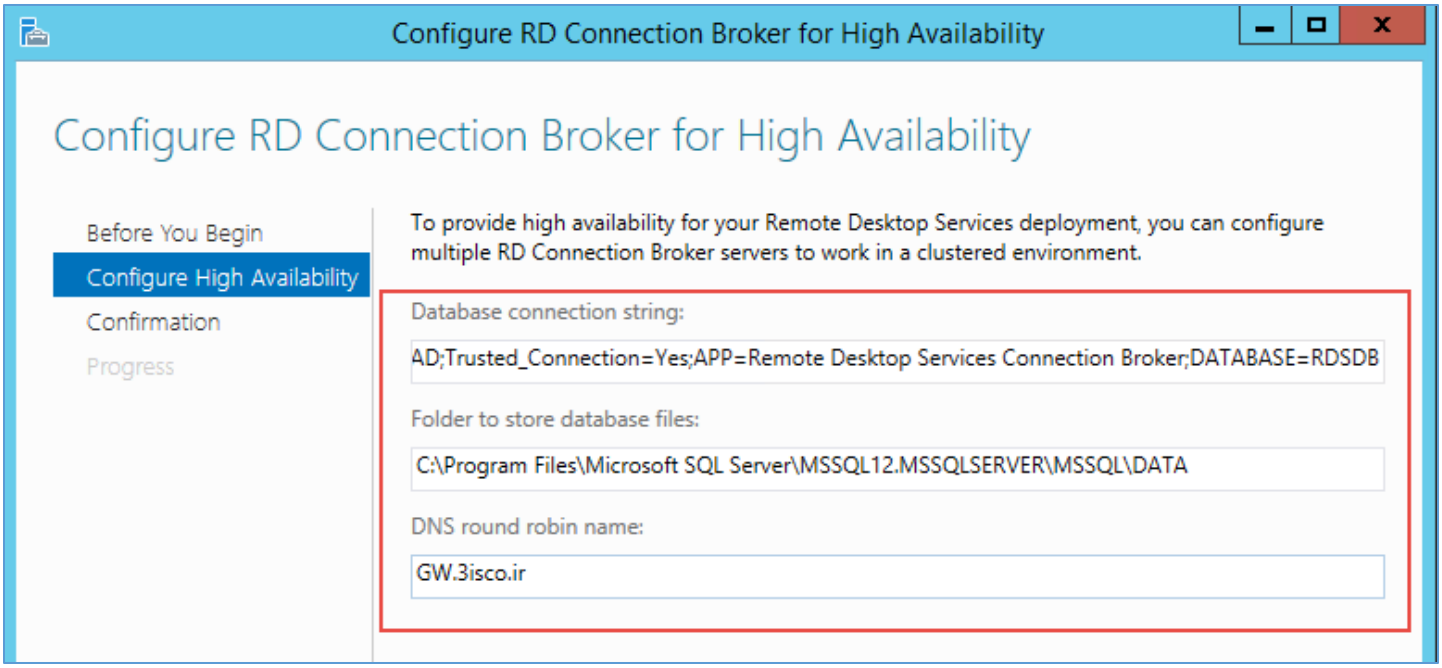
در این شکل از قسمت Object، گزینه‌ی Group را انتخاب کنید و نام گروه را در لیست وارد و بر روی OK کلیک کنید.



در این صفحه و در ادامه، وارد تب Server Roles شوید؛ برای اینکه گروه دسترسی لازم برای ایجاد دیتابیس را داشته باشد، تیک گزینه‌ی dbcreator را انتخاب و بر روی OK کلیک کنید.



بعد از انجام تنظیمات در SQL وارد Server Manager شوید و در قسمت Remote Desktop بر روی RD Connection BrOKer کلیک راست کنید و گزینه‌ی Configure High Availity را انتخاب کنید.



در صفحه‌ی بالا باید یک ارتباط بین این سرویس و نرم‌افزار SQL ایجاد کنید تا این سرویس بتواند دیتابیسی که به آن معرّفی می‌کنید را در SQL ایجاد کند، پس در قسمت Database Connection string، دستور زیر را وارد کنید:

DRIVER=SQL Server Native Client 11.0;SERVER=AD;Trusted_Connection=Yes;APP=Remote Desktop Services Connection BrOKer;DATABASE=RDSDB

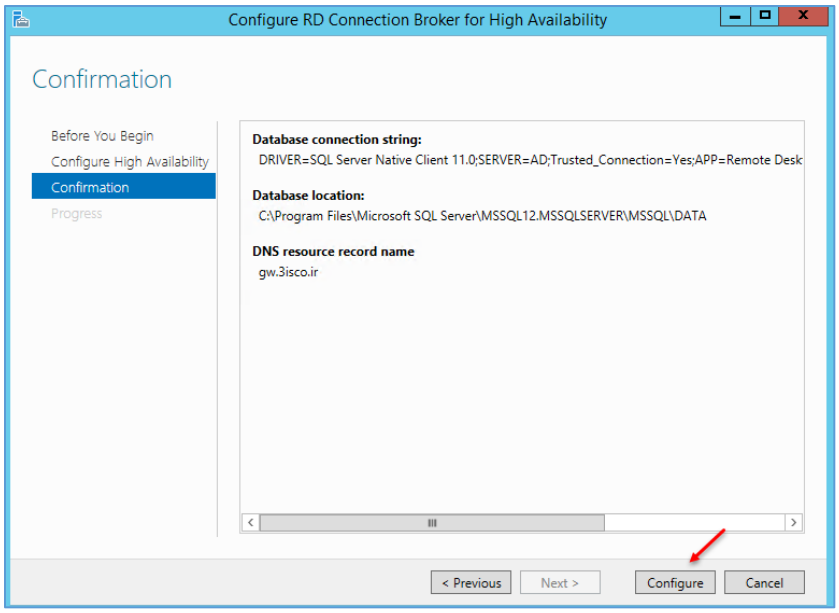
در دستور بالا به جای AD باید نام سرور دومین خود و به جای RDSDB، نام دیتابیس دلخواه خود را وارد کنید، در قسمت دوّم نیز باید آدرس فولدری که دیتابیس‌های SQL در آن ذخیره شده است را وارد کنید که به صورت پیش‌فرض در مسیر زیر ذخیره می‌شود:

C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA

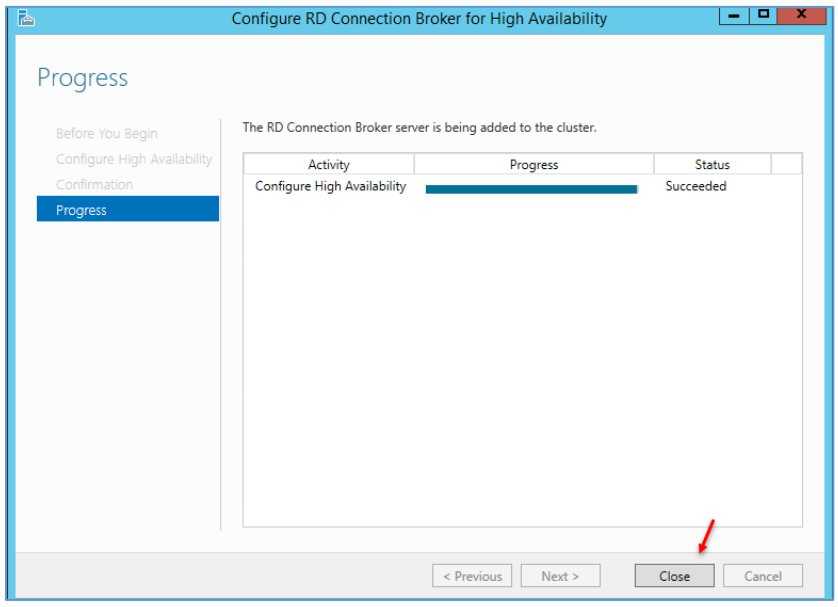
در قسمت آخر نیز باید همان، آدرس خارجی GW.3isco.ir را وارد و OK کنید.

اگر با خطا روبرو شدید، این موارد را بررسی کنید:

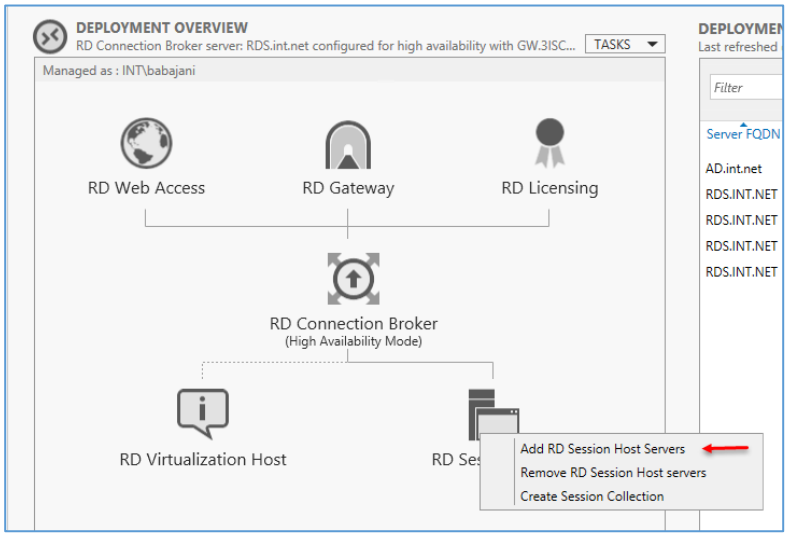
- در هر دو سرور، کامپونت SQL Native Client را با استفاده از لینک زیر دانلود و نصب کنید:
  https://drive.google.com/file/d/0Bw1Nv5ua4a5-X3drd2F1VGw5UzQ/view?usp=sharing
- باید سرویس فایروال در هر دو سرور خاموش باشد، یا اینکه به پورت ۱۴۳۳ دسترسی لازم داده شود.
- هر دو سیستم را Restart کنید.
- مراحل ساخت گروه و دسترسی به SQL را دوباره بررسی کنید تا اشتباهی رخ نداده باشد.



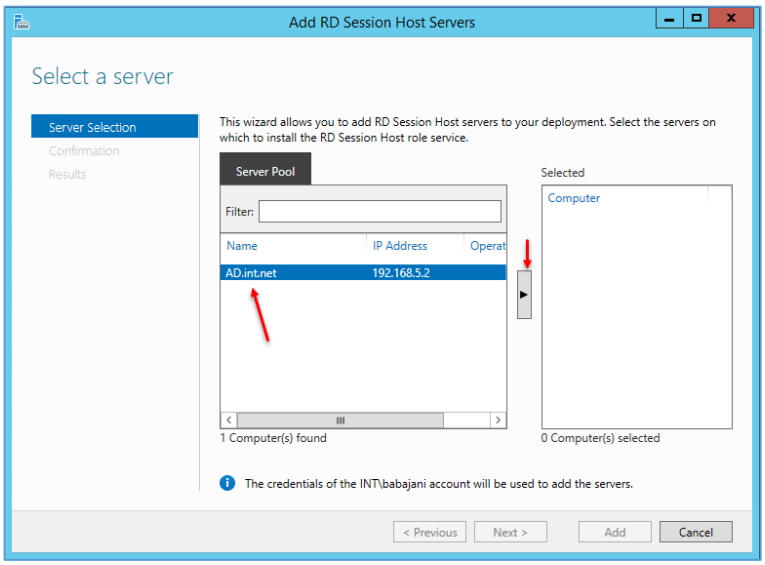
همانطور که مشاهده می‌کنید، تنظیمات و داده‌های ارتباطی با SQL تأیید شد، برای ایجاد دیتابیس بر روی Configure کلیک کنید.



همانطور که مشاهده می‌کنید، تنظیمات به درستی انجام شده است و اگر اکنون به SQL مراجعه کنید، مشاهده خواهید کرد یک دیتابیس با نام RDSDB ایجاد شده است.

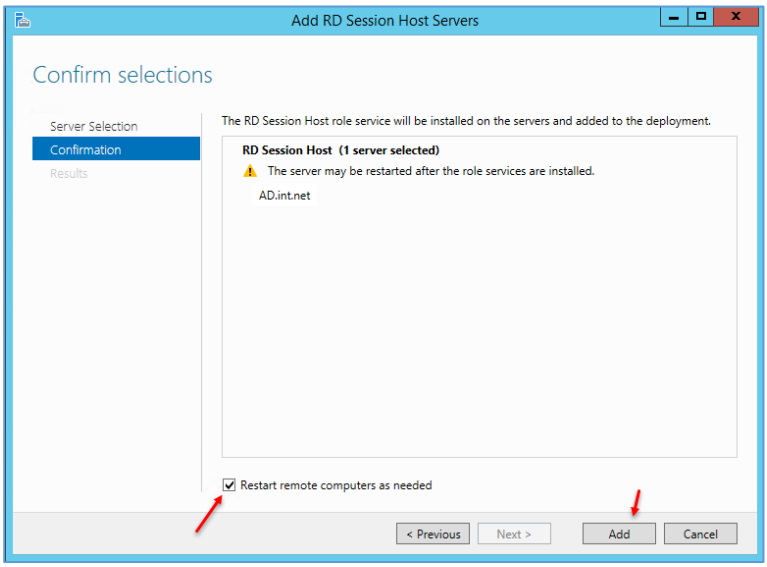


بعد از انجام مراحل قبل، دوباره وارد Remote Desktop شوید و بر روی RDSession Host Servers کلیک راست کنید و طبق شکل، گزینه‌ی اوّل را انتخاب کنید.

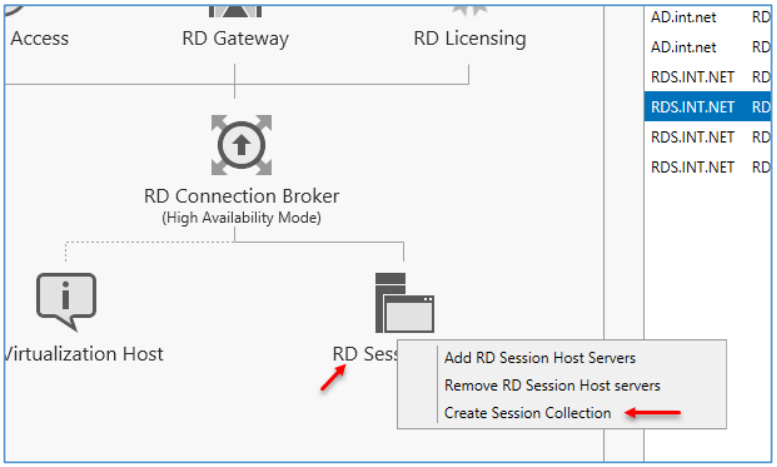


در این صفحه، سرور مورد نظر را به لیست اضافه و بر روی Next کلیک کنید.

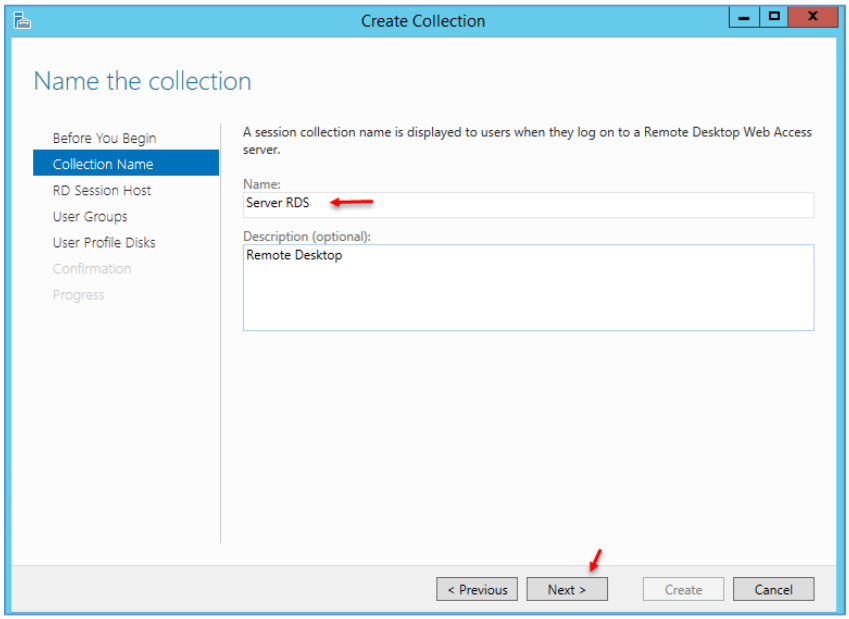
توجّه داشته باشید، سرور RDS از قبل به لیست اضافه شده است و در لیست روبرو وجود ندارد.



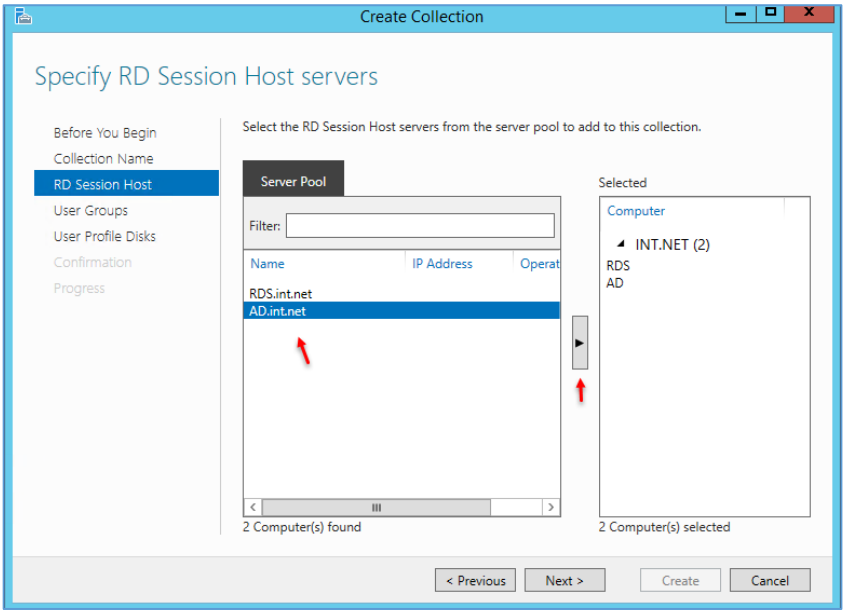
در این صفحه، تیک Restart remote... را انتخاب و بر روی Add کلیک کنید تا عملیّات انجام شود.



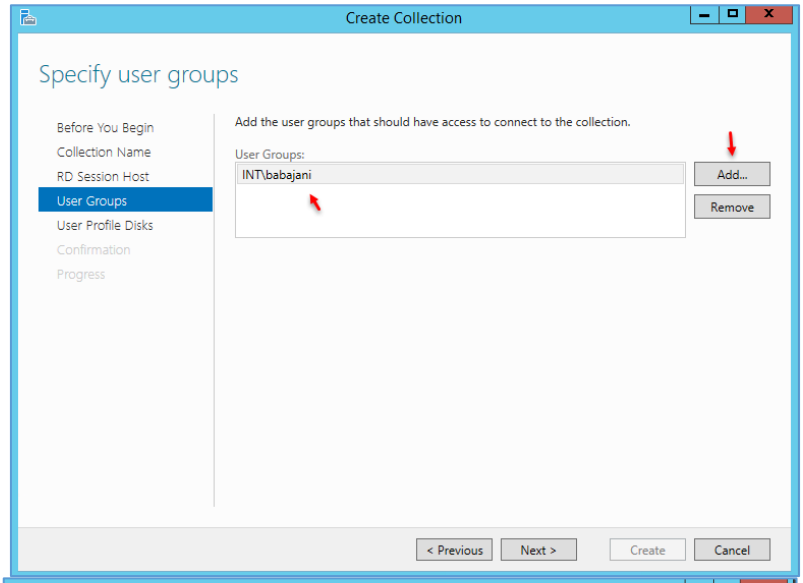
بعد از اضافه کردن سرور به قسمت Session، بار دیگر بر روی آن کلیک راست کنید و گزینه‌ی Create Session Collection را انتخاب کنید.



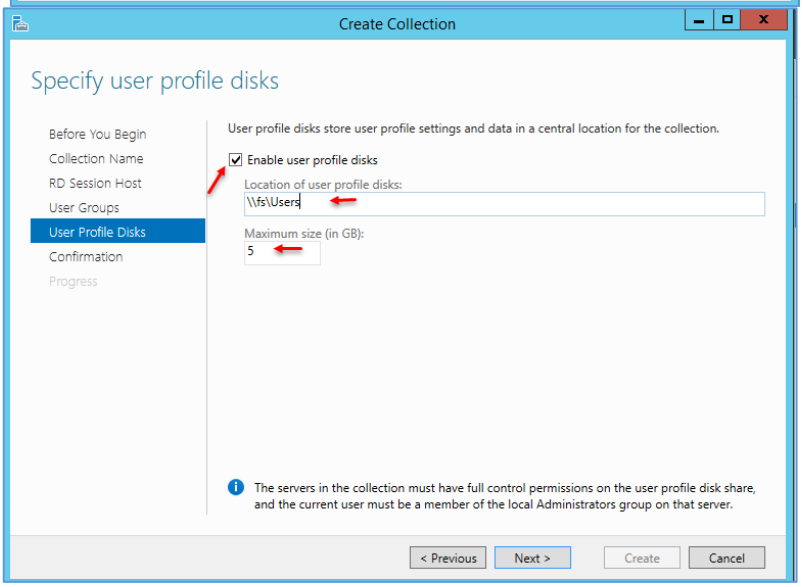
در این قسمت، یک نام وارد و بر روی Next کلیک کنید.



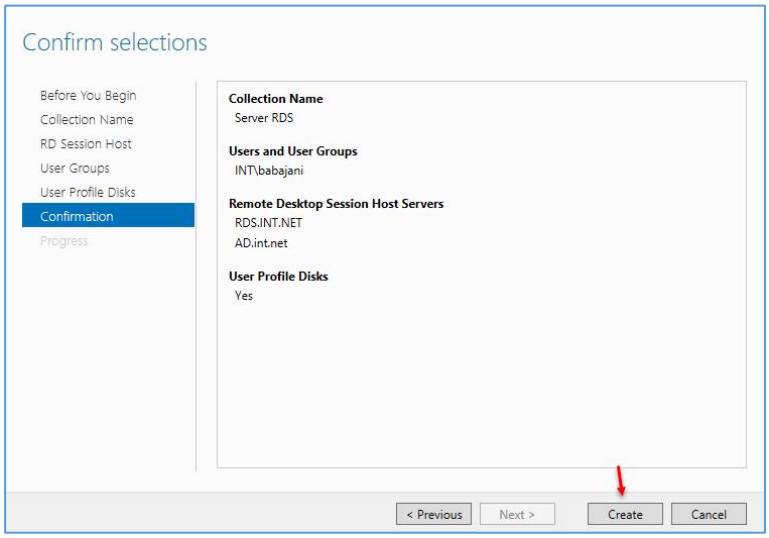
در این صفحه، هر دو سرور را به لیست اضافه کنید و بر روی Next کلیک کنید.



در این صفحه می‌توانید مشخّص کنید که چه کاربرانی به این Collection دسترسی داشته باشند؛ بر روی Next کلیک کنید.



در این قسمت، تیک گزینه‌ی Enable user profile disks را انتخاب کنید و مسیری را برای ذخیره کردن اطّلاعات کاربرانی که به صورت Remote وارد سرور می‌شوند، انتخاب کنید، در قسمت آخر نیز می‌توانید حداکثر حجم آن را که در اینجا، ۵ گیگابایت وارد کردید را وارد کنید.



در این صفحه بر روی Create کلیک کنید تا عملیّات تکمیل شود.

بعد از اتمام کار، حال نوبت آن است که از طریق سایت به اطّلاعات سرور دست پیدا کنید، وارد مرورگر خود شوید و آدرس زیر را اجرا کنید:

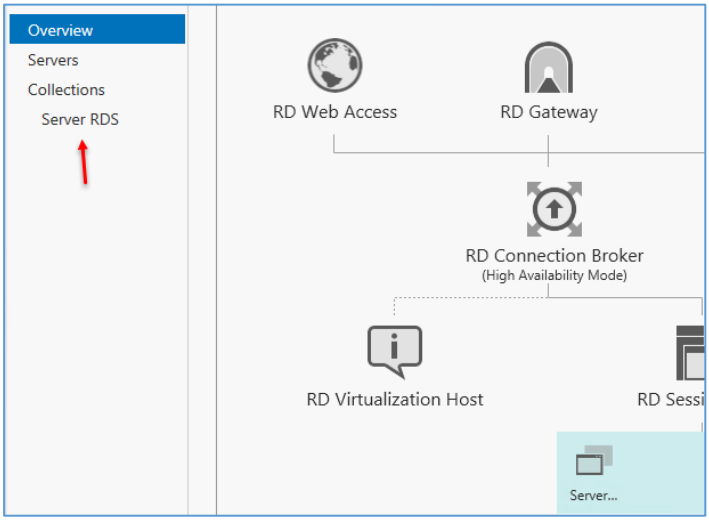
https://rds.int.net/RDWeb/

شما باید به جای آدرس مشخّص‌شده، آدرس سرور خود را وارد کنید تا شکل زیر ظاهر شود.

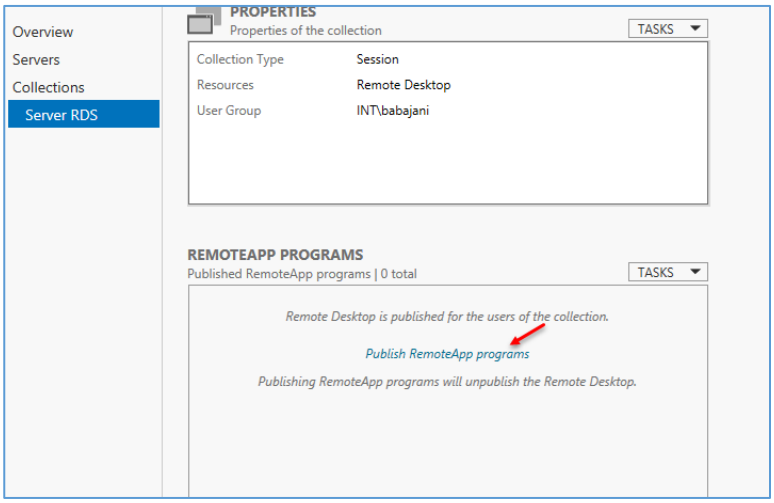


در این صفحه باید نام کاربری را به همراه نام دومین خود وارد و بر روی Sign in کلیک کنید.

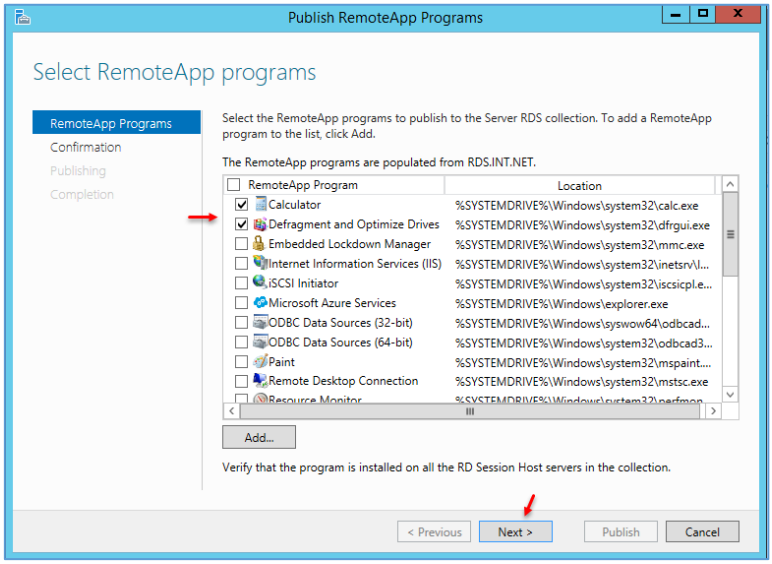
اجرای نرم‌افزار از طریق سرویس Remote Desktop:



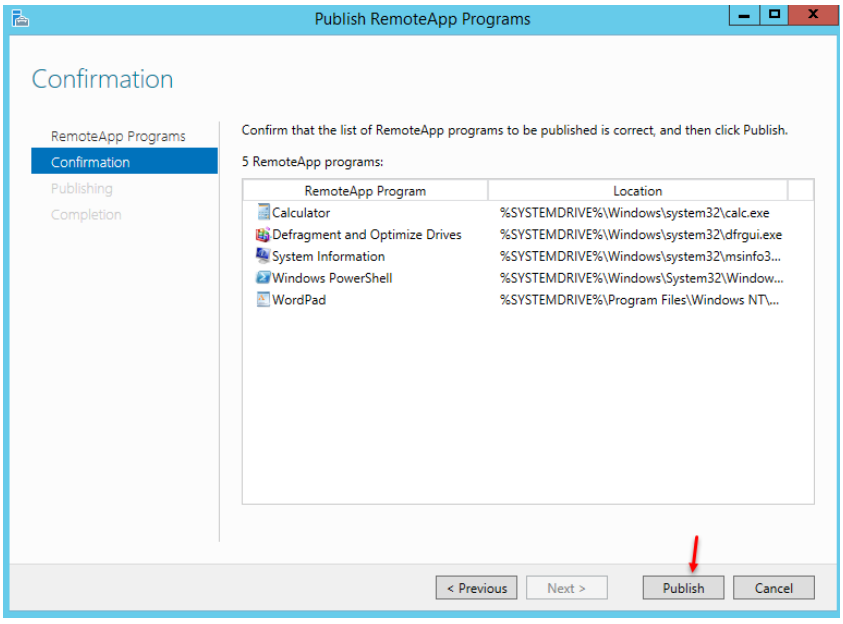
در این قسمت می‌خواهیم نرم‌افزارهایی که در سرور نصب شده است را به صورت تحت وب اجرا کنیم، برای این کار بر روی سروری که با هم در قسمت قبل ایجاد کردیم، کلیک و در سمت چپ بر روی Server RDS کلیک می‌کنیم.



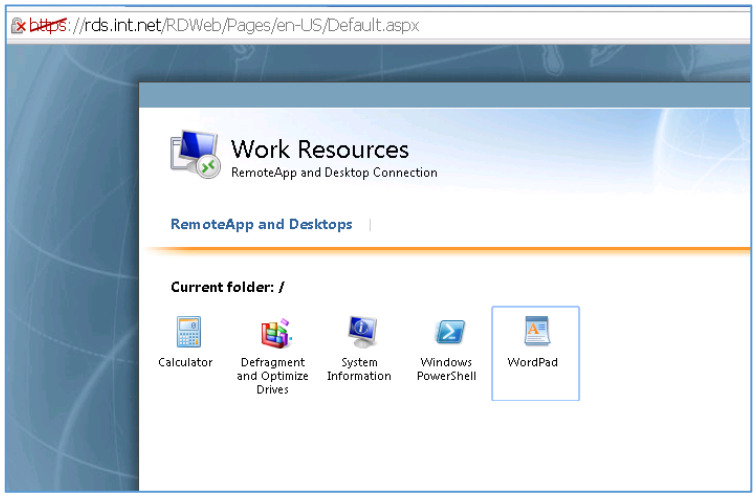
در این صفحه، در قسمت Remotapp Programs بر روی Publish RemoteApp programs کلیک کنید.



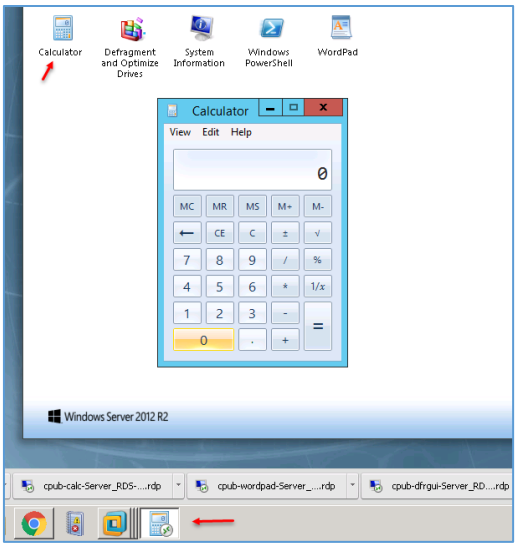
در این صفحه، شما لیستی از نرم‌افزارها را مشاهده می‌کنید که مربوط به پوشه‌ی system32 در سرور RDS است که اگر بخواهید نرم‌افزار دیگری را به لیست اضافه کنید باید بر روی Add کلیک کنید، چند نرم‌افزار را انتخاب و بر روی Next کلیک کنید.



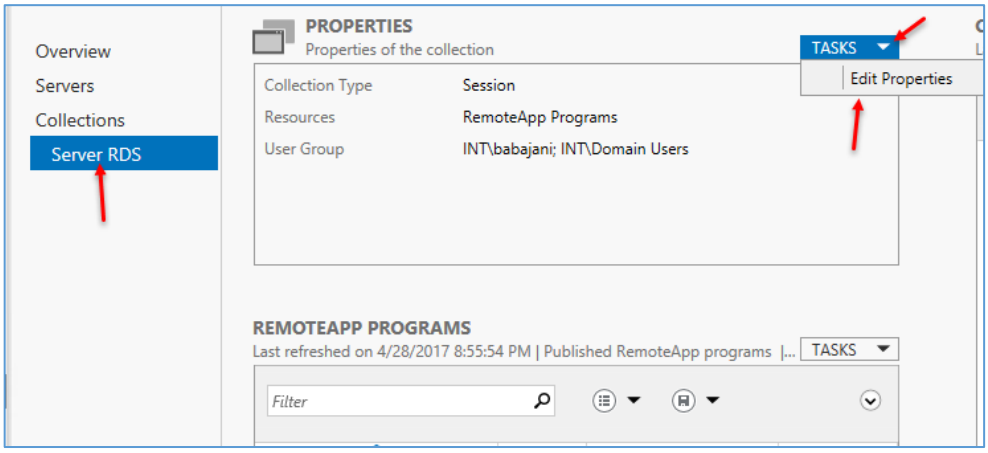
در این صفحه بر روی Publish کلیک کنید تا نرم‌افزارها از طریق سایت قابل دسترس باشند.



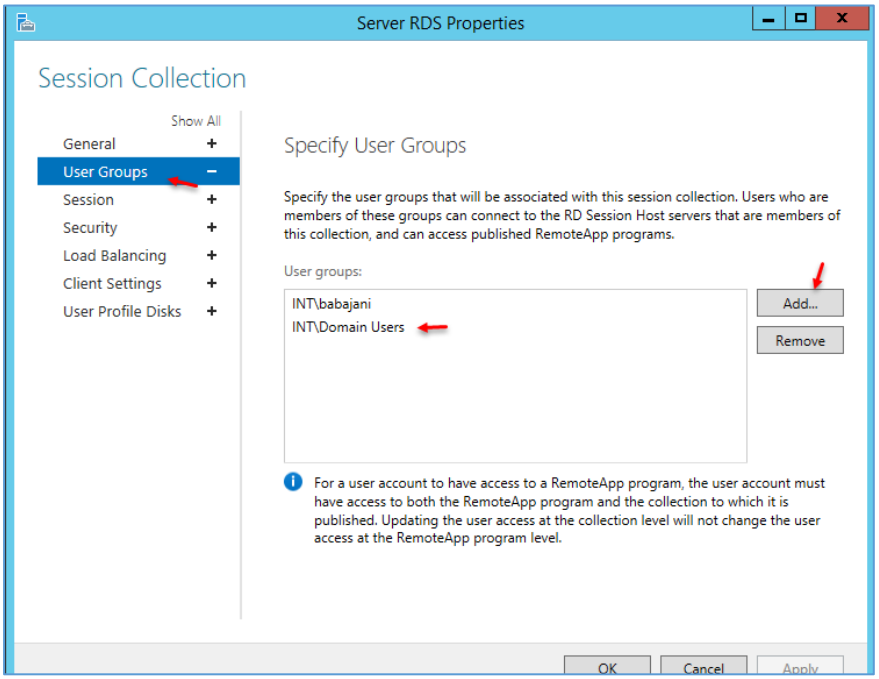
بعد از انجام عملیّات بالا وارد آدرس روبرو شوید و همانطور که مشاهده می‌کنید، نرم‌افزارهای مورد نظر از طریق وب در دسترس است و اگر بر روی آنها کلیک کنید، از شما نام کاربری و رمز عبور شبکه دریافت می‌شود و نرم‌افزار تحت وب اجرا خواهد شد.



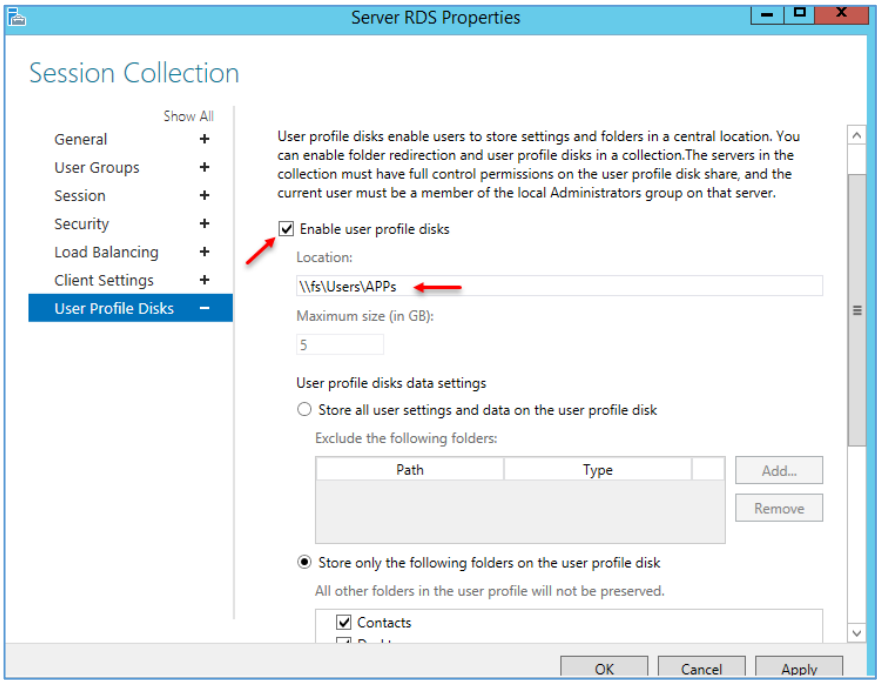
در شکل روبرو، نرم‌افزار ماشین حساب فعّال شده است که آیکون ماشین حساب نیز در حالت Remote قرار گرفته است.



اگر چنانچه در مرحله‌ی قبل، نرم‌افزارهای تحت وب اجرا نشد، در Server Manager و در قسمت Properties بر روی Tasks کلیک کنید و گزینه‌ی Edit Properties را انتخاب کنید.



در این صفحه وارد تب **User Groups** شوید و بر روی **Add** کلیک کنید و بعد از آن، گروه **Domains Users** را به لیست اضافه کنید تا همه‌ی کاربران، دسترسی لازم را داشته باشند.



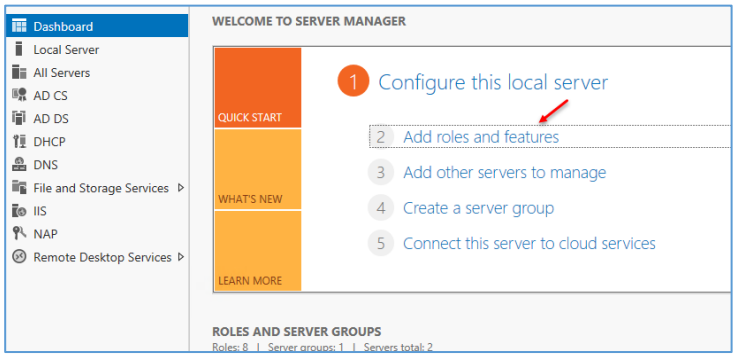
در تب **User Profile Disks** از طریق شبکه باید یک مسیر برای ذخیره‌ی اطّلاعات کاربر در هنگام کار مشخّص کنید، برای این کار تیک گزینه‌ی **Enable user profile disks** را انتخاب و مسیر مورد نظر را برای کاربر مشخّص کنید، سعی کنید کاربر مورد نظر دسترسی لازم را داشته باشد، با این کار در اجرای نرم‌افزار مشکلی نخواهید داشت.

تا به اینجا، نرم افزارها را از طریق سرویس **Remote Desktop** اجرا کردیم و این خود می‌تواند یک ویژگی خوب از این سرویس باشد، در ادامه قصد داریم ماشین مجازی را از طریق وب اجرا کنیم.

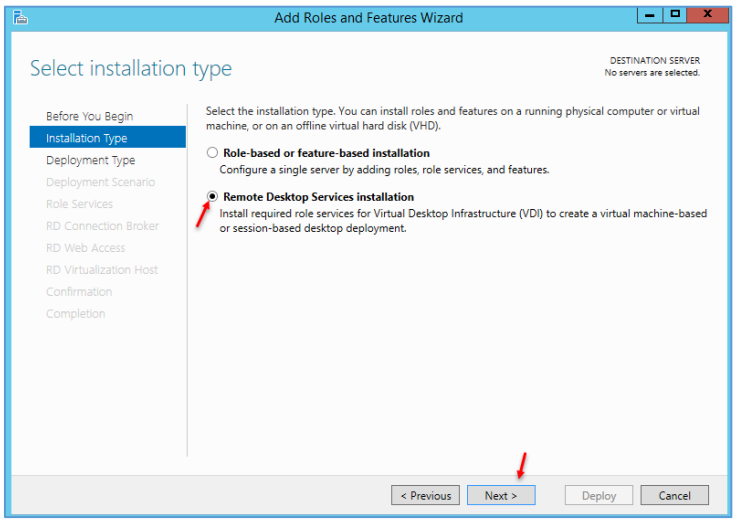
فعّال کردن سرویس Virtual Machine Remote Desktop:

با استفاده از این سرویس می‌توانید یک یا چند ماشین مجازی در سرور خود، ایجاد و دسترسی لازم را به کاربران خود بدهید تا بتوانند از طریق وب به ماشین مورد نظر دسترسی داشته باشند و ریموت بزنند.

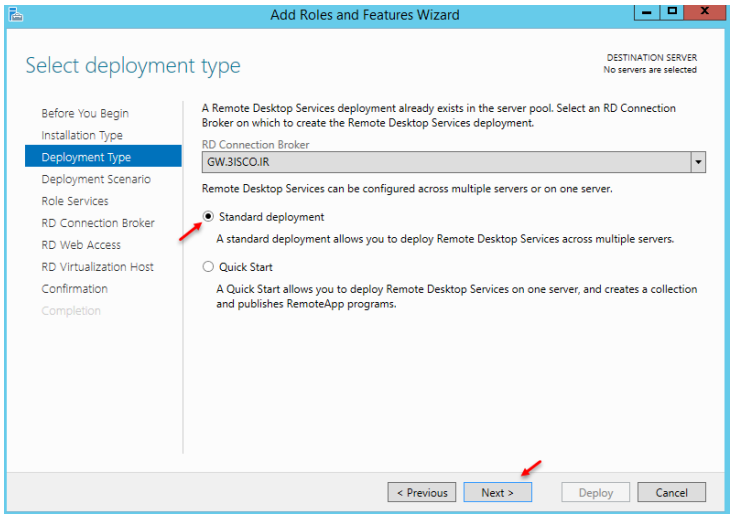
برای شروع وارد Server Manager شوید و بر روی Add roles and Features کلیک کنید.



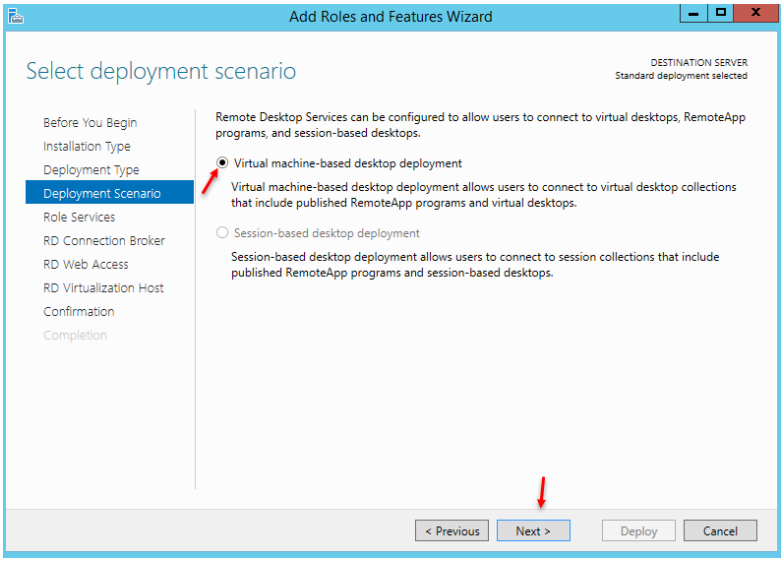
در این قسمت، گزینه‌ی Remote Desktop Services Install ation را انتخاب و بر روی Next کلیک کنید.



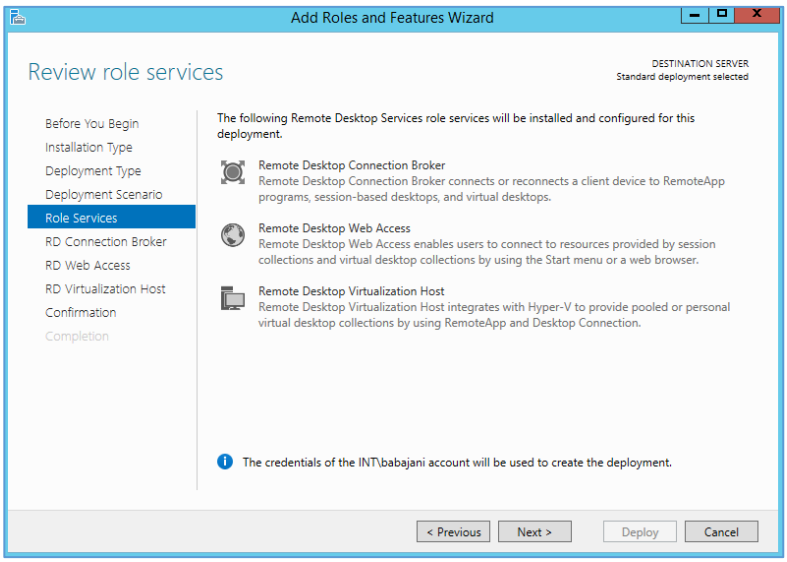
در این صفحه، گزینه‌ی Remote Desktop Services Install ation را انتخاب و بر روی Next کلیک کنید.



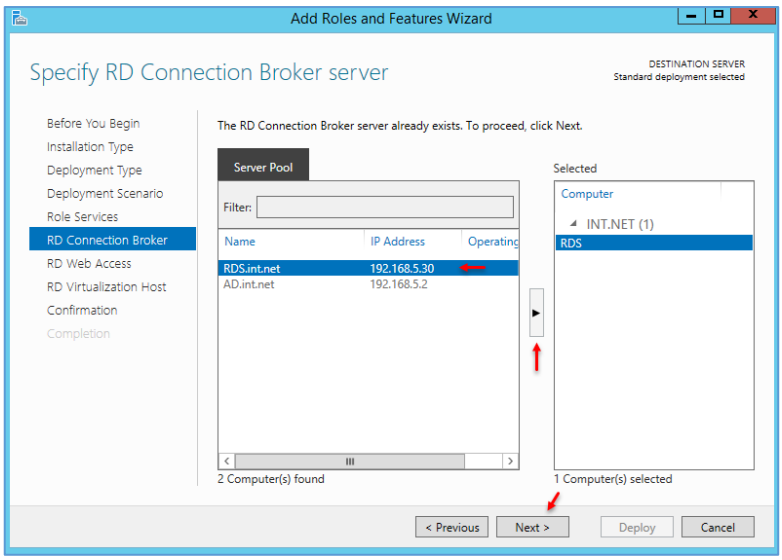
در این صفحه، گزینه‌ی Standard deployment را انتخاب و بر روی Next کلیک کنید.



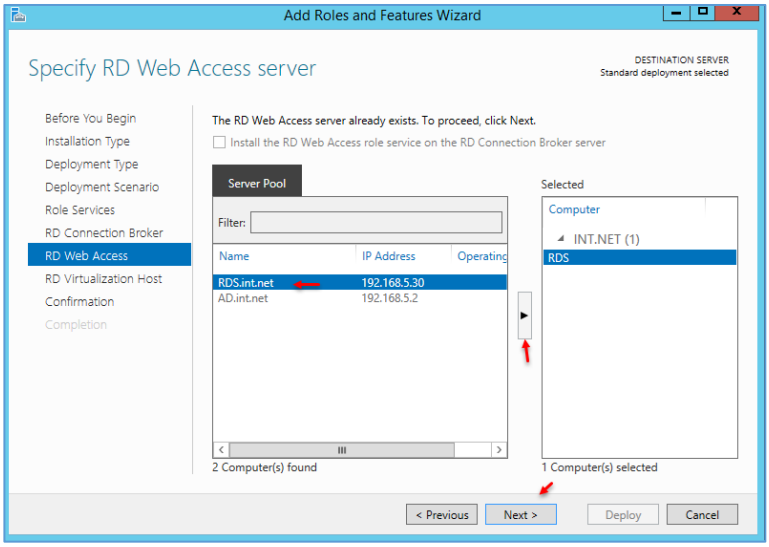
اگر در این قسمت توجّه کنید، گزینه‌ی Session-based که قبلاً روی آن کار کردیم، غیر فعّال است و از قبل نصب شده است، گزینه‌ی Virtual machine-based... را انتخاب و بر روی Next کلیک کنید.



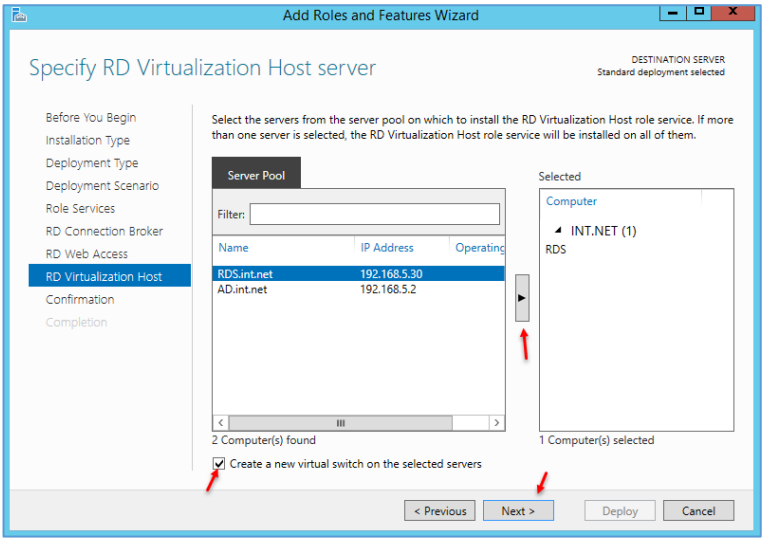
بر روی Next کلیک کنید.



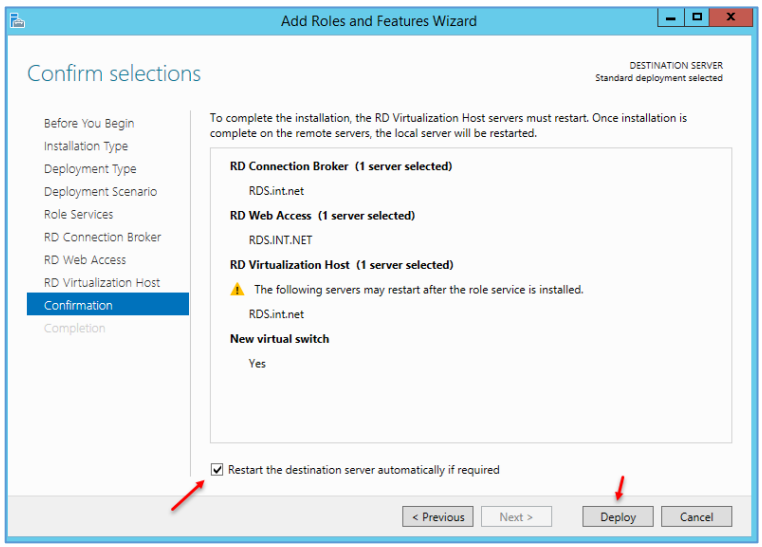
در این صفحه، سرور RDS را انتخاب و بر روی Next کلیک کنید.



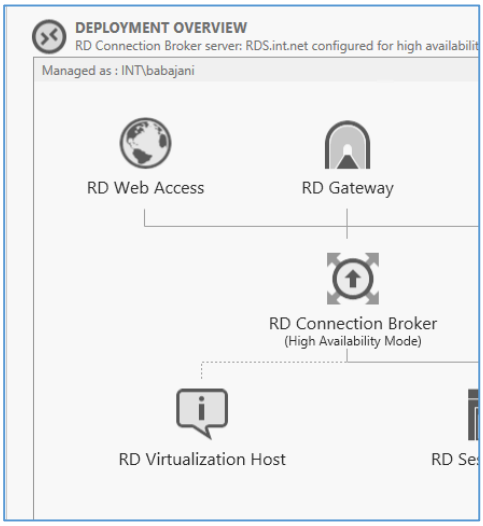
در این صفحه نیز سرور RDS را انتخاب و بر روی Next کلیک کنید، البتّه از آنجایی که قبلاً این عملیّات را بر روی این سرور انجام دادیم به صورت پیش‌فرض انتخاب شده است.



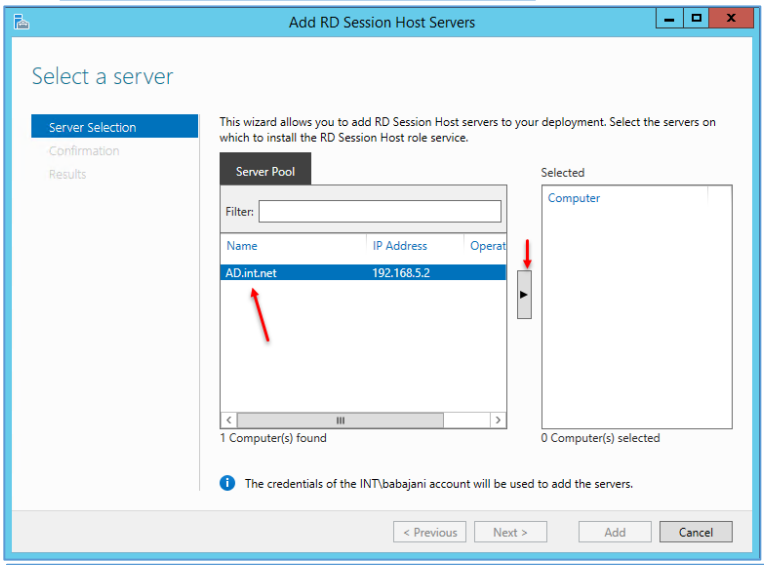
تیک گزینه‌ی مورد نظر را انتخاب و سرور RDS را به لیست اضافه کنید و بر روی Next کلیک کنید.



در این قسمت نیز تیک گزینه‌ی مورد نظر را انتخاب و بر روی Deploy کلیک کنید تا تنظیمات بر روی سرور RDS انجام شود.

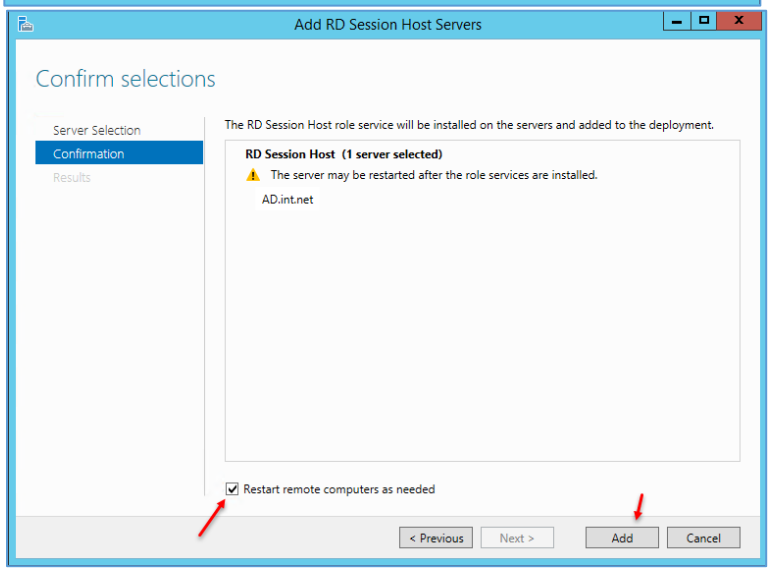


بعد از انجام مراحل قبل، دوباره وارد Remote Desktop شوید و بر روی RD Virtualization Host کلیک راست کنید و مطابق شکل، گزینه‌ی اول را انتخاب کنید.

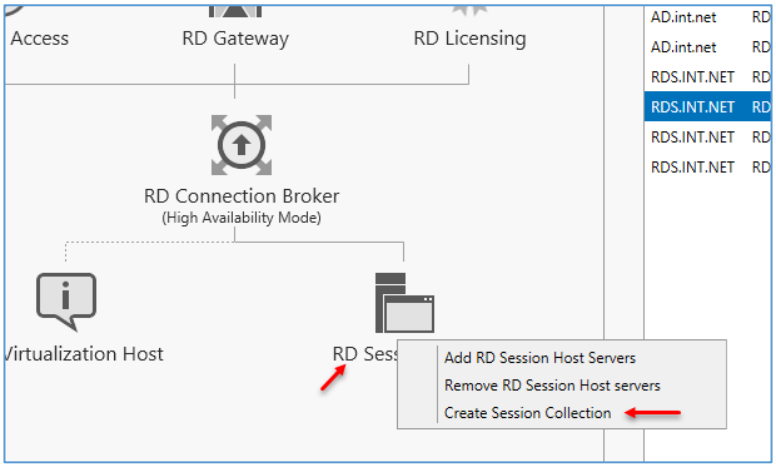


در این صفحه، سرور مورد نظر را به لیست اضافه و بر روی Next کلیک کنید.

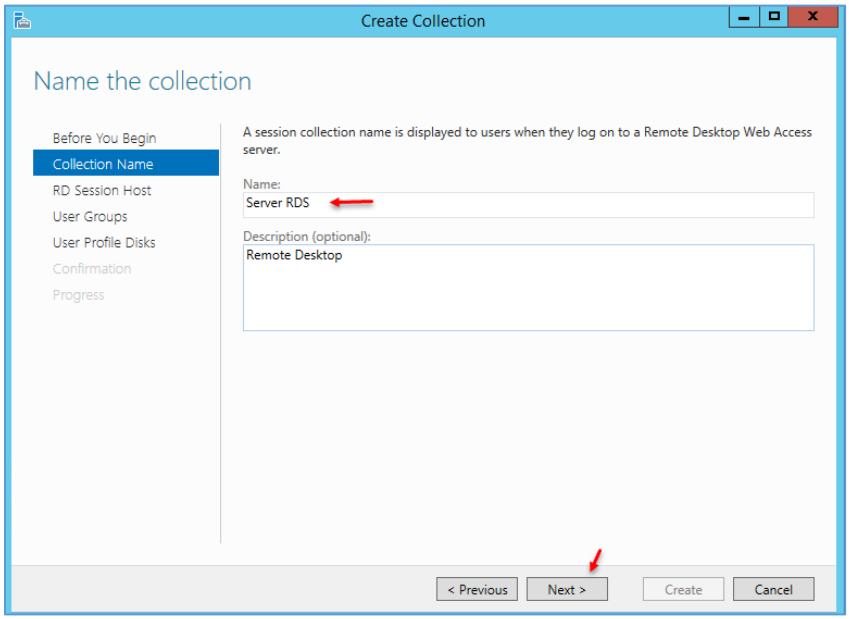
توجه داشته باشید، از قبل سرور RDS به لیست اضافه شده است و در لیست روبرو وجود ندارد.



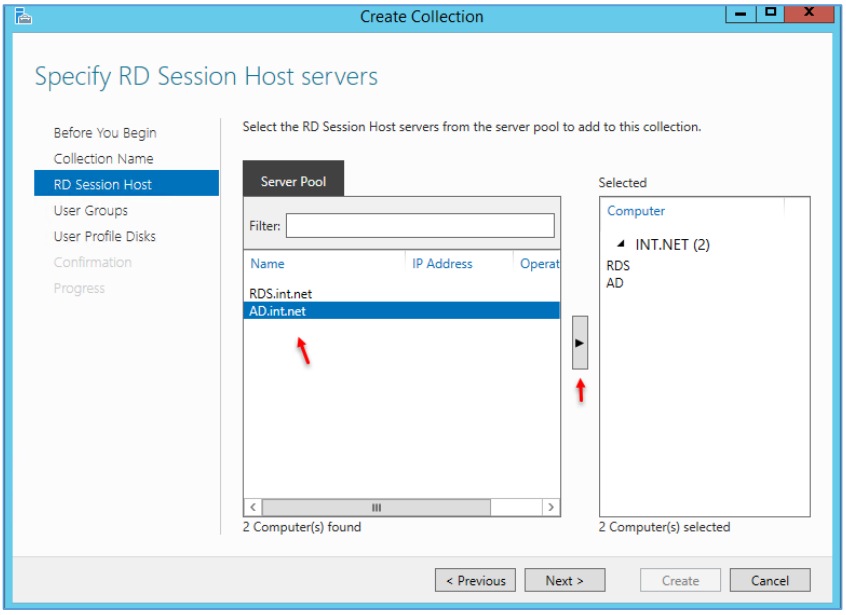
در این صفحه، تیک Restart remote... را انتخاب کنید و بر روی Add کلیک کنید تا عملیّات انجام شود.



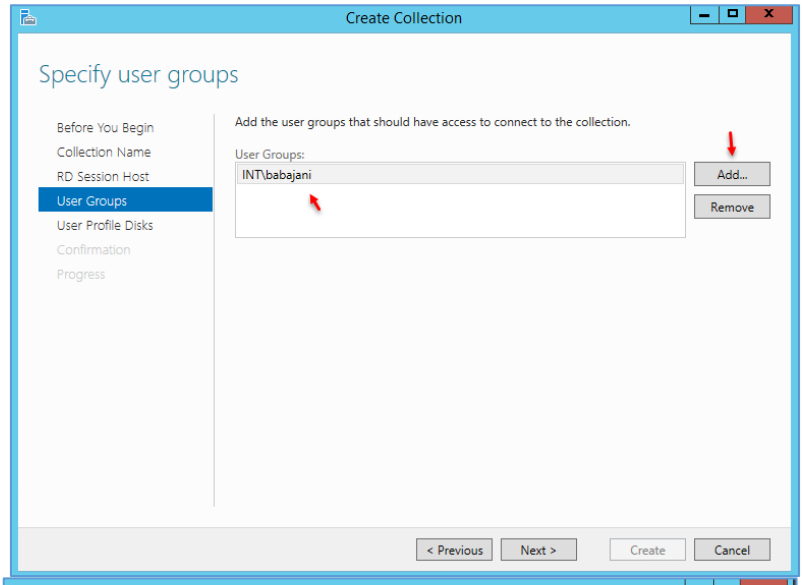
بعد از اضافه کردن سرور به قسمت Session بر روی آن دوباره کلیک راست کنید و گزینه‌ی Create Session Collection را انتخاب کنید.



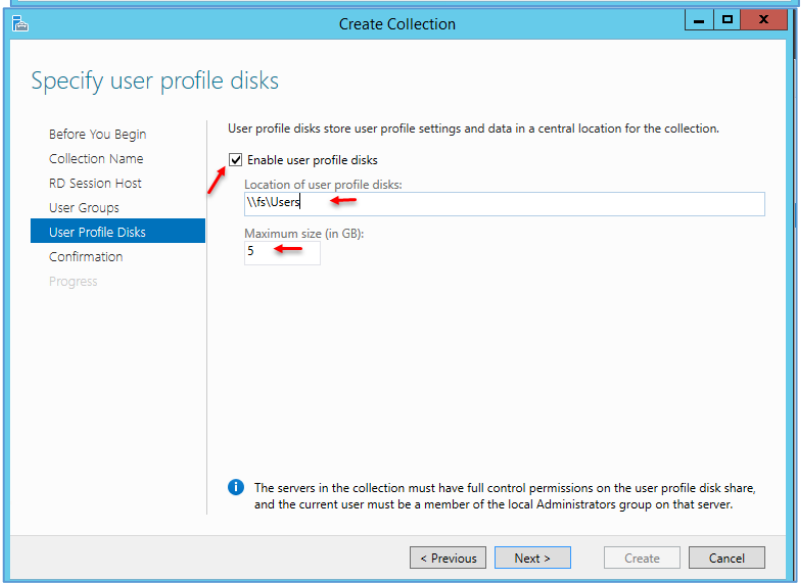
در این قسمت، یک نام وارد و بر روی Next کلیک کنید.



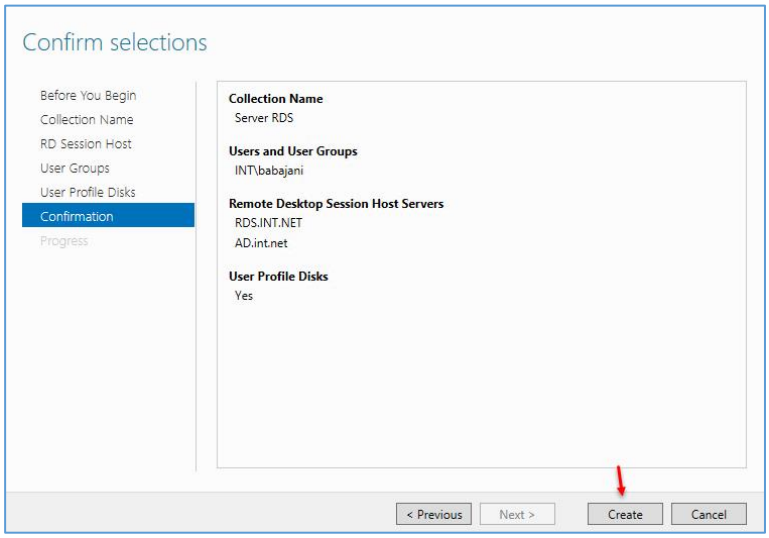
در این صفحه، هر دو سرور را به لیست اضافه و بر روی Next کلیک کنید.



در این صفحه می‌توانید مشخّص کنید که چه کاربرانی به این Collection دسترسی داشته باشند، بر روی Next کلیک کنید.



در این قسمت، تیک گزینه‌ی Enable user profile disks را انتخاب کنید و برای ذخیره کردن اطّلاعات کاربرانی که به صورت Remote وارد سرور می‌شوند، مسیری را انتخاب کنید و در قسمت آخر نیز می‌توانید حداکثر حجم آن را که ۵ گیگابایت است را وارد کنید.



در این صفحه بر روی Create کلیک کنید تا عملیّات تکمیل شود.

بعد از اتمام کار، حال نوبت این است که از طریق سایت به سرور دست پیدا کنید، وارد مرورگر خود شوید و آدرس زیر را اجرا کنید:

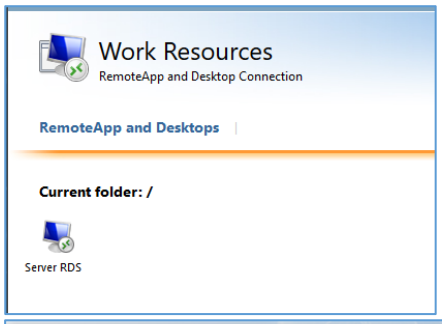
https://rds.int.net/RDWeb/

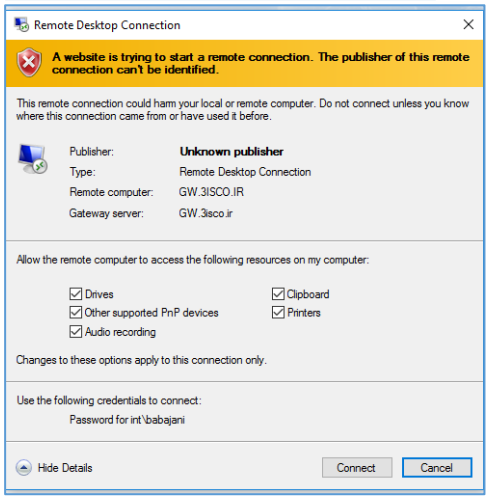
شما باید به جای آدرس مشخّص‌شده، آدرس سرور خود را وارد کنید تا شکل زیر ظاهر شود.



در این صفحه باید نام کاربری را به همراه نام دومین خود وارد و بر روی Sign in کلیک کنید.

همانطور که مشاهده می‌کنید، سروری که ایجاد کردید در لیست قرار گرفته است و از این طریق می‌توانید از راه دور به آن دسترسی داشته باشید.

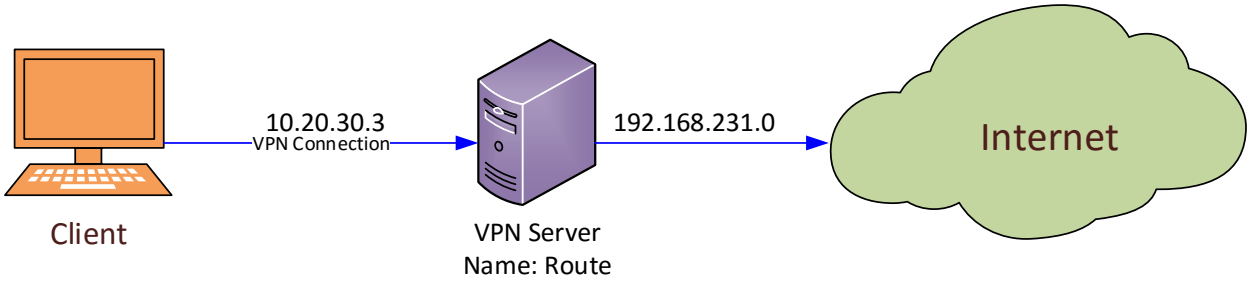




بعد از کلیک بر روی Server، شکل روبرو ظاهر می‌شود که نام سرور را به همراه گزینه‌های دسترسی در اختیار شما قرار می‌دهد؛ با کلیک بر روی Connect می‌توانید به سرور متصل شوید.

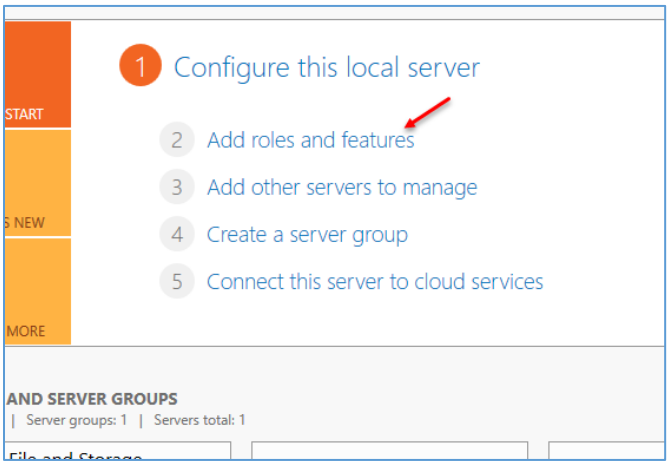
نصب و راه‌اندازی سرویس Remote Access:

در این سرویس می‌توانید به کاربران خود این امکان را دهید تا با سرور شما از طریق VPN ارتباط برقرار کنند یا می‌توانید دو سرور را از طریق VPN به هم متّصل کنید، حتّی می‌توانید دو شبکه‌ی جدا از هم را به هم ارتباط دهید.

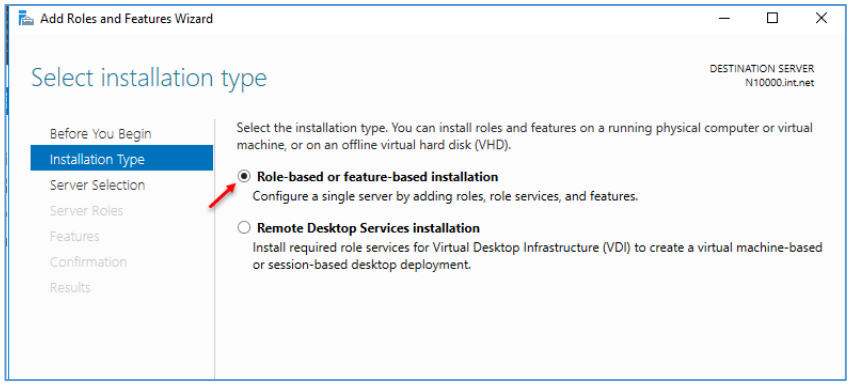


در شکل بالا، یک سرور VPN وجود دارد که کلاینت‌های شبکه از طریق آن می‌توانند به اینترنت متّصل شوند، برای این کار باید در سرور VPN تنظیمات لازم را انجام دهید.

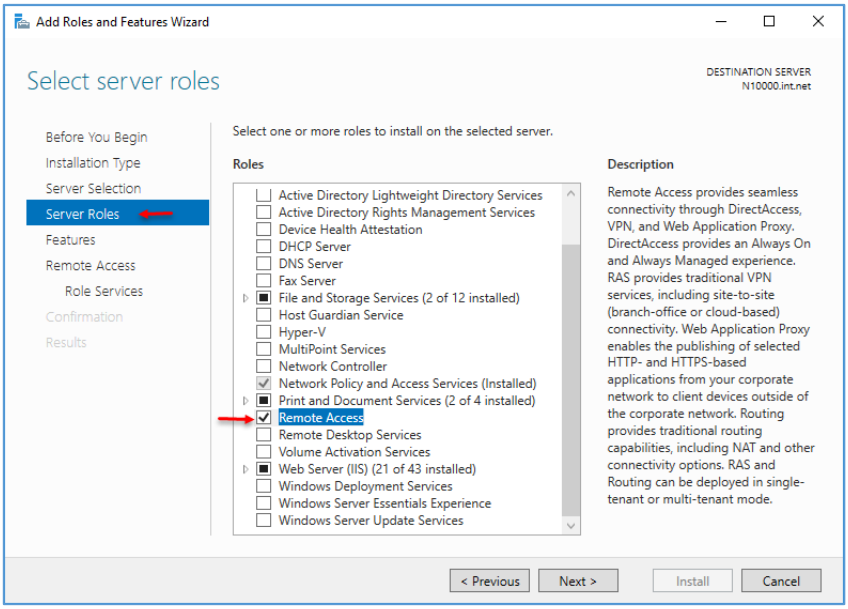
سرور VPN باید دارای دو کارت شبکه باشد که یکی با شبکه‌ی داخلی و دیگری با شبکه‌ی خارجی ارتباط داشته باشد که در این قسمت نیز کارت شبکه‌ی Ethernet 0 با شبکه‌ی خارجی (اینترنت) با رنج 192.168.231.0 ارتباط دارد و کارت شبکه‌ی Ethernet 1 با شبکه‌ی داخلی با رنج 10.20.30.0 ارتباط دارد که کلاینت‌ها نیز برای ارتباط از طریق کانکشن VPN با آدرس سرور 10.20.30.3 که مربوط به سرور VPN است، ارتباط برقرار می‌کنند و از این طریق به اینترنت دست پیدا خواهند کرد.



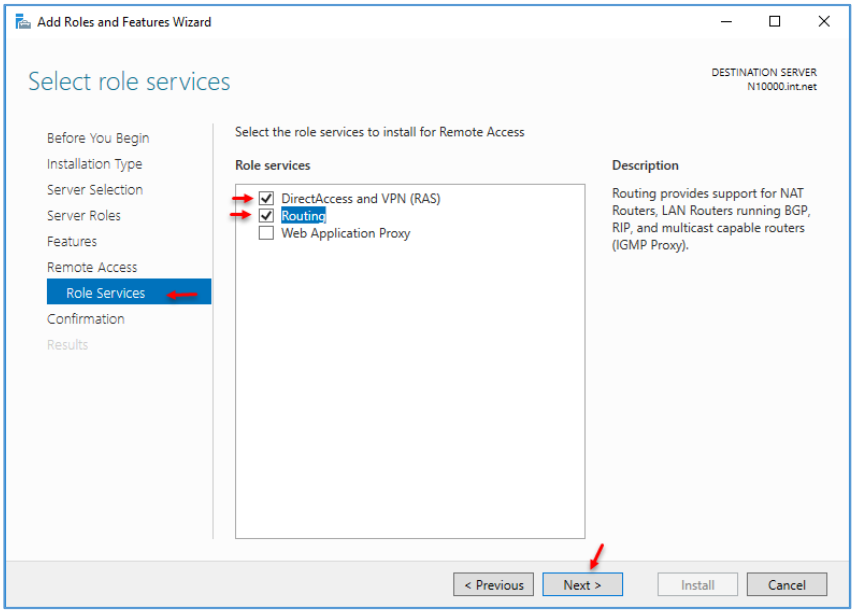
برای شروع وارد Server Manager مربوط به سرور Route یا همان، VPN شوید و بر روی Add roles and features کلیک کنید.



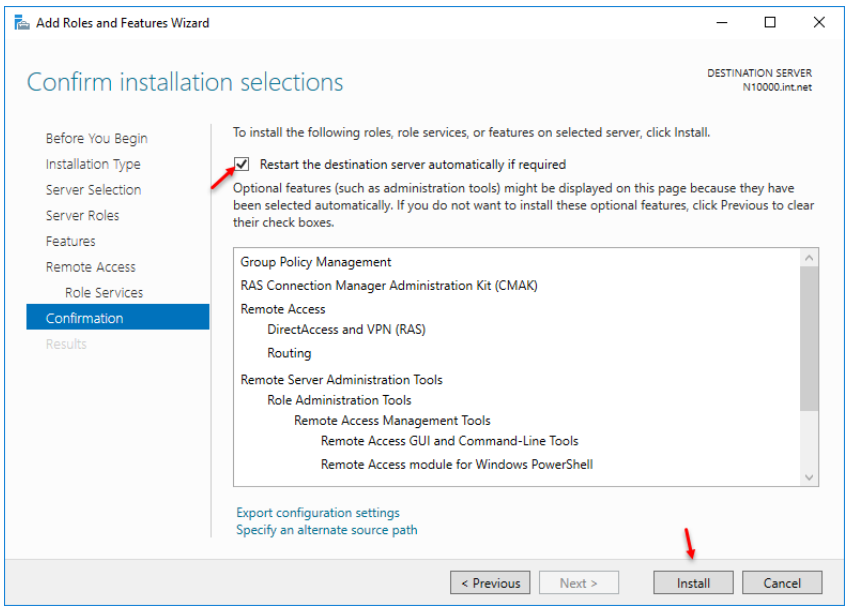
گزینه‌ی اوّل را انتخاب و بر روی Next کلیک کنید.



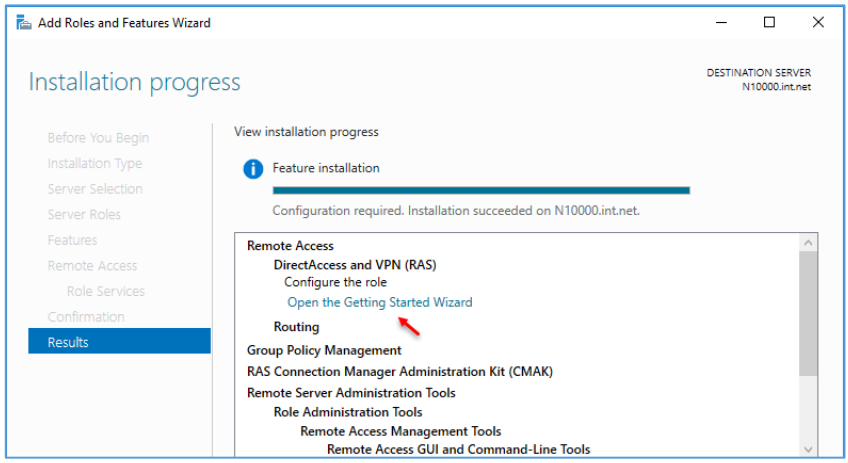
در این قسمت، گزینه‌ی Remote Access را انتخاب و بر روی Next کلیک کنید.



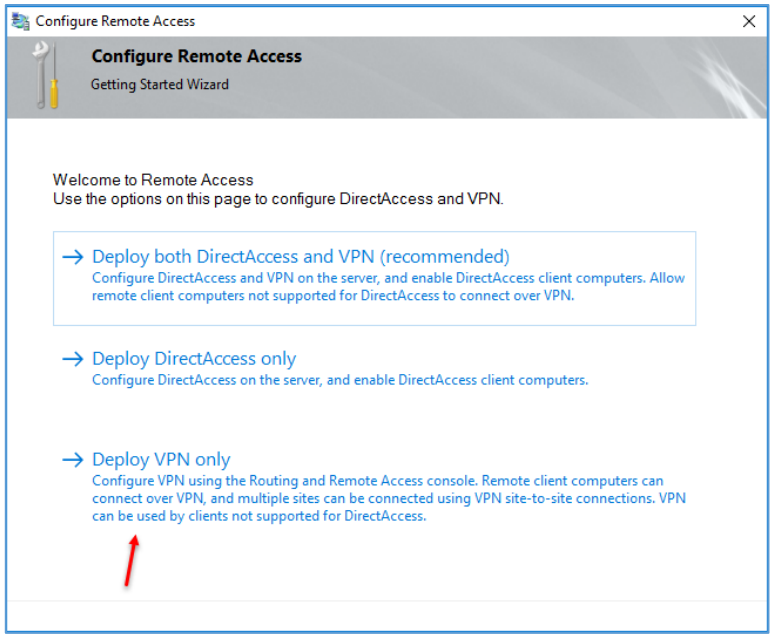
در این صفحه، دو گزینه‌ی DirectAccess and VPN (RAS) و Routing را انتخاب و بر روی Next کلیک کنید.



در این قسمت، تیک گزینه‌ی Restart را انتخاب و بر روی Install کلیک کنید.

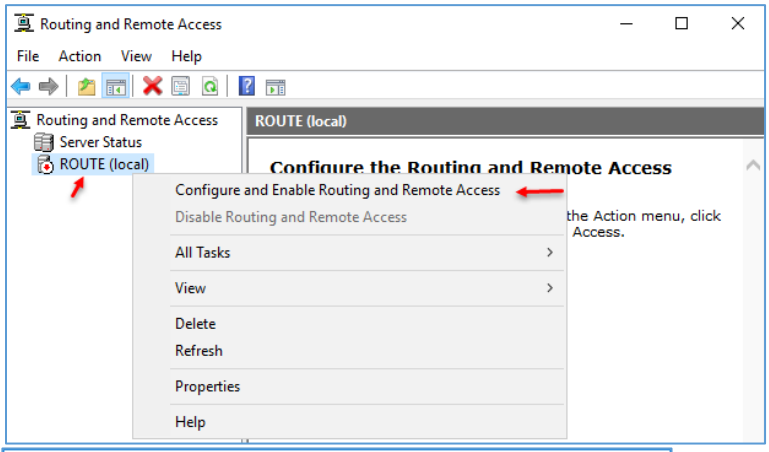


در این صفحه بعد از نصب، بر روی Open the Getting started Wizard کلیک کنید.

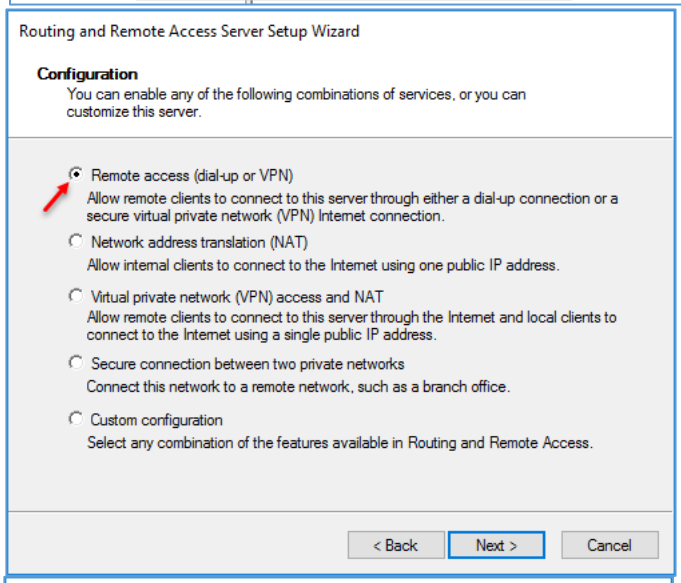


در این صفحه، سه گزینه را مشاهده می‌کنید که برای شروع باید گزینه‌ی Deploy VPN only را انتخاب کنید.

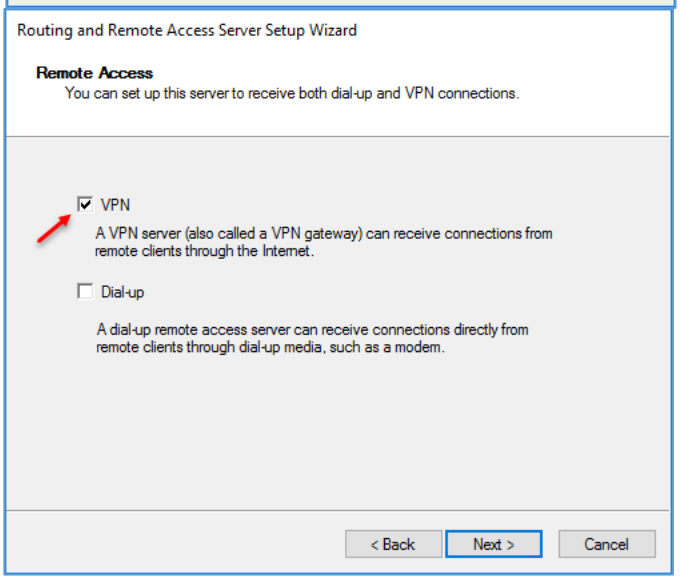
در این صفحه بر روی نام سرور کلیک راست کنید و گزینه‌ی مورد نظر را انتخاب کنید.

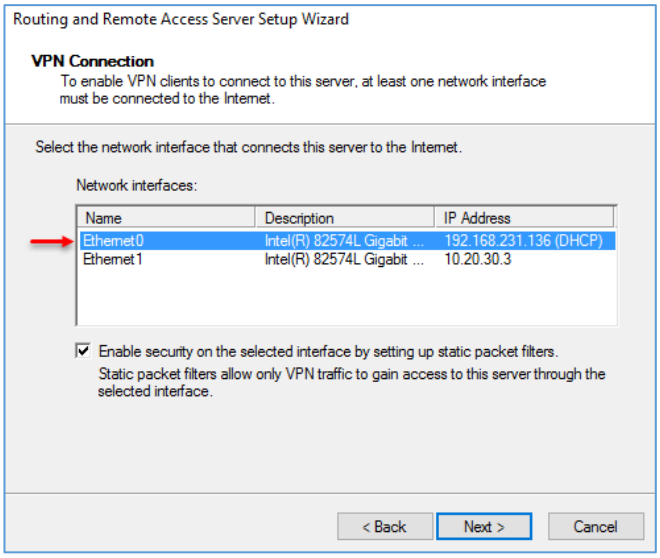


در این قسمت، گزینه‌ی Remote Access را انتخاب کنید تا بتوانید VPN را بر روی این سرور راه‌اندازی کنید.

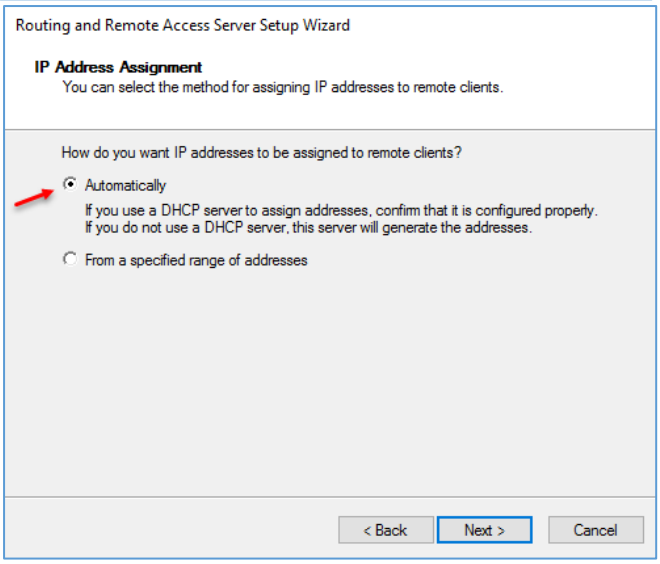


در این صفحه، تیک گزینه‌ی VPN را انتخاب و بر روی Next کلیک کنید.

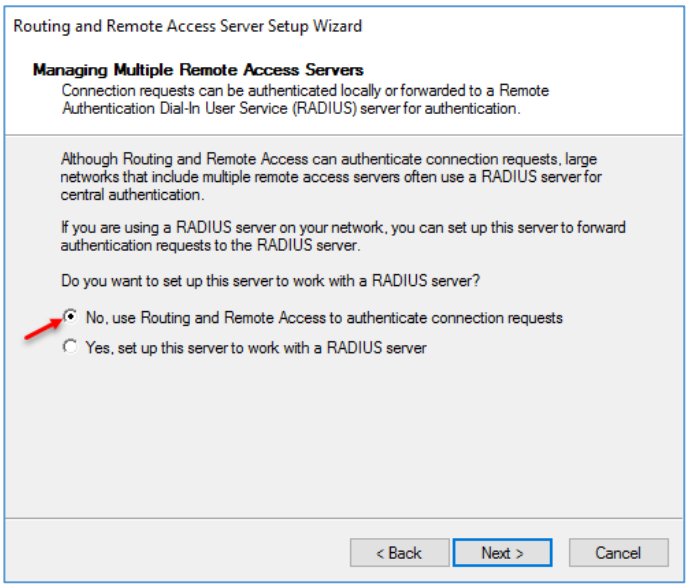




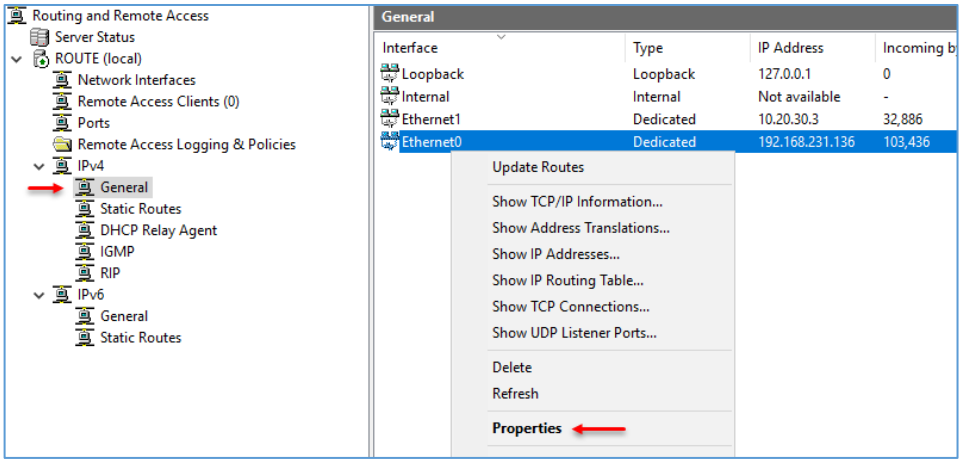
در این قسمت، دو کارت شبکه را مشاهده می‌کنید که برای ارتباط کاربران باید کارت شبکه‌ای را انتخاب کنید که داخلی باشد و آدرس شبکه‌ی داخلی بر روی آن تعریف شده باشد.



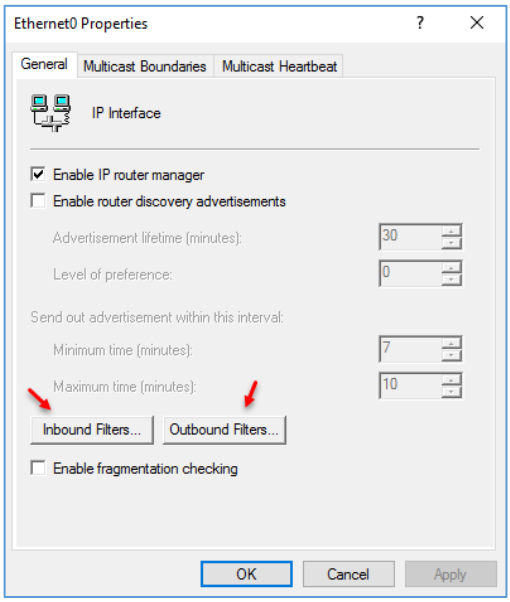
در این قسمت می‌توانید برای کاربرانی که از طریق VPN به سرور متّصل می‌شوند با انتخاب گزینه‌ی From a specified...، یک رنج IP خاص به آنها اختصاص دهید یا گزینه‌ی Automatically را انتخاب کنید تا از طریق سرویس DHCP به آنها IP داده شود.



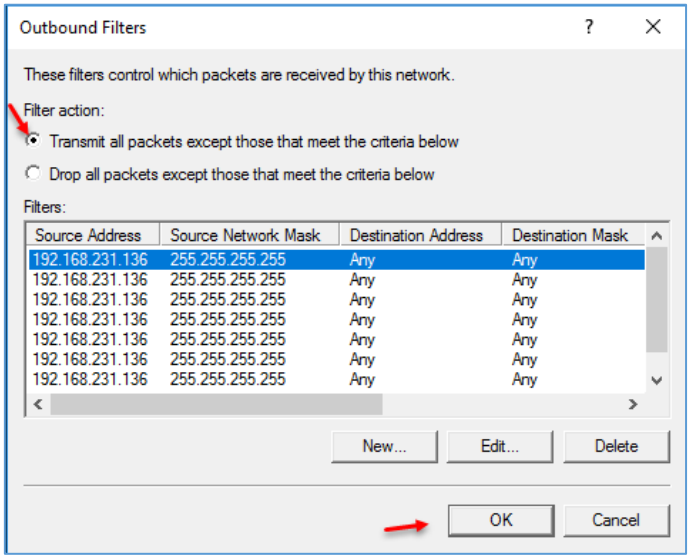
اگر در این صفحه، نیاز به تنظیم Radius Server دارید، می‌توانید گزینه‌ی Yes را انتخاب کنید، در غیر این صورت، گزینه‌ی اوّل را انتخاب و بر روی Next کلیک کنید.



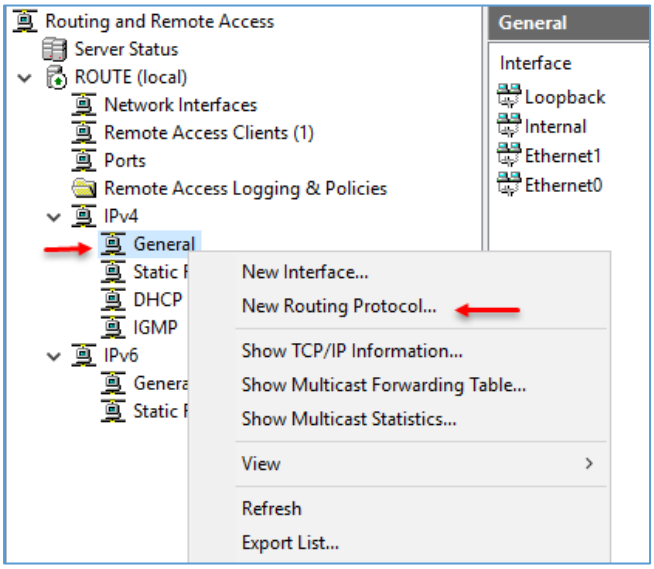
بعد از فعّال کردن سرویس، برای اینکه به درخواست‌های ورودی و خروجی اجازه عبور دهید باید به مانند شکل روبرو بر حسب IP، آدرس شبکه‌ی خود را وارد کنید و به قسمت General بروید و بر روی کارت شبکه‌ای که به اینترنت متّصل است که در اینجا، Ethernet0 است، کلیک راست و گزینه‌ی Properties را انتخاب کنید.



در شکل روبرو، دو گزینه‌ی Inboound Filters و Outbound Filters را مشاهده می‌کنید، اگر بخواهید تنها همین سرور به اینترنت دسترسی داشته باشد باید بر روی گزینه‌ی Outbound Filters کلیک کنید.

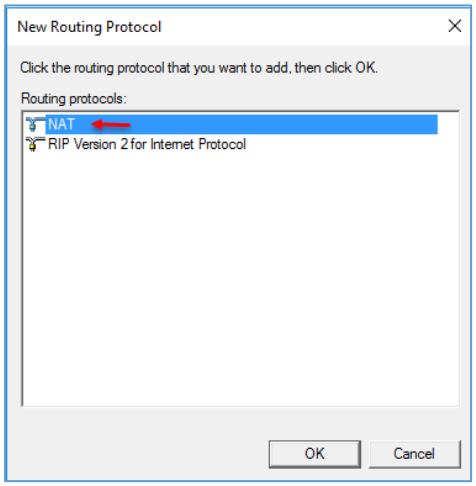


در این قسمت، برای اینکه اجازه‌ی عبور به اطّلاعات دهید باید گزینه‌ی Transmit All packets... را انتخاب و بر روی OK کلیک کنید، در صفحه‌ی بعد نیز بر روی OK کلیک کنید، با این کار سرور VPN توانایی ارتباط با اینترنت را از طریق کارت شبکه با IP 192.168.231.136 دارا خواهد بود.

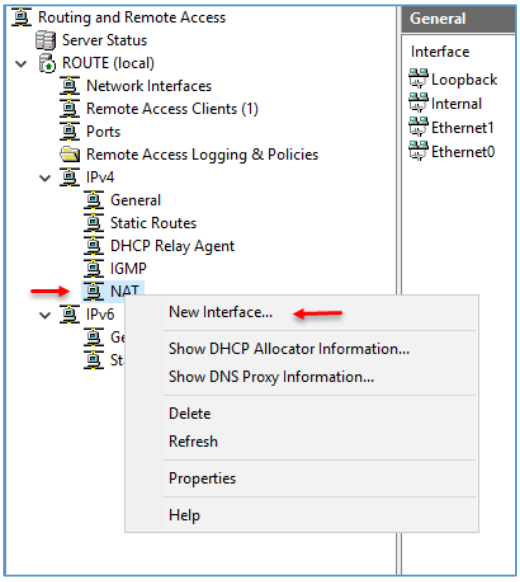


بعد از این که سرور Route به اینترنت دسترسی پیدا کرد باید عملیّات NAT را برای دسترسی کاربرانی که از طریق VPN به سرور متّصل می‌شوند، انجام دهید تا کاربران بتوانند به اینترنت متّصل شوند.

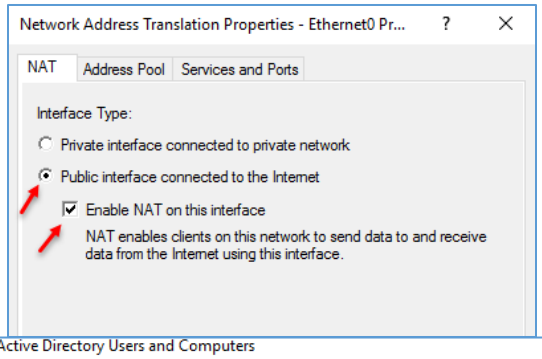
برای انجام این کار بر روی General کلیک راست کنید و گزینه‌ی New routing Protocol را انتخاب کنید، البتّه بستگی به این دارد که پروتکل شبکه‌ی شما، IPV4 یا IPV6 باشد.



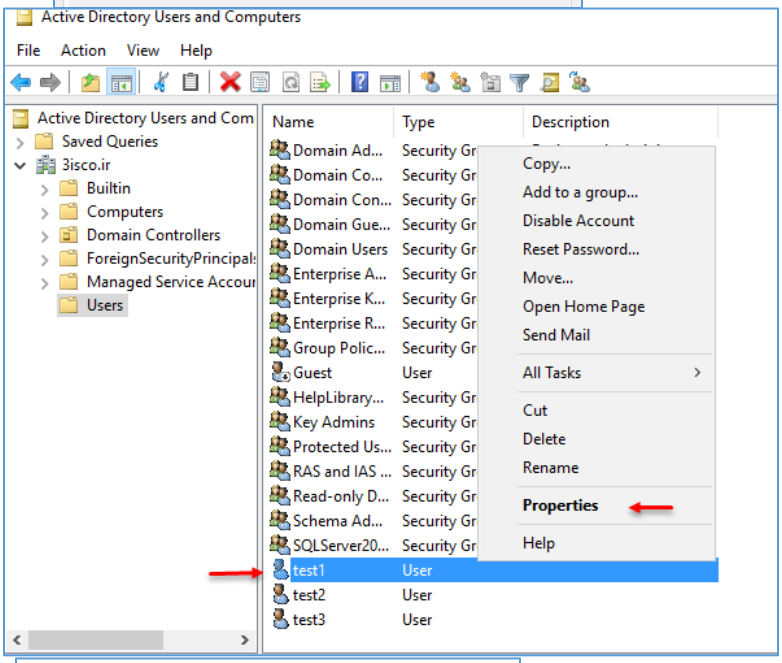
در صفحه‌ی روبرو پروتکل NAT را انتخاب کنید تا آدرس‌های شبکه‌ی داخلی به آدرس‌های قابل فهم در شبکه‌ی اینترنت تبدیل شود.



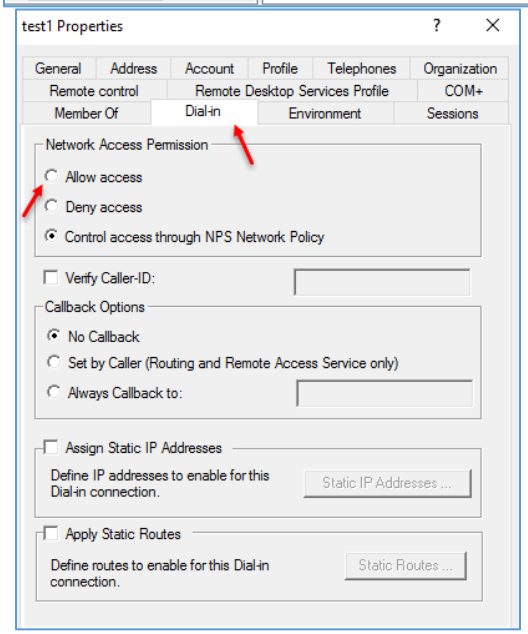
در این صفحه، گزینه‌ی NAT به لیست اضافه شده است، بر روی آن کلیک راست کنید و گزینه‌ی New Interface را انتخاب کنید.



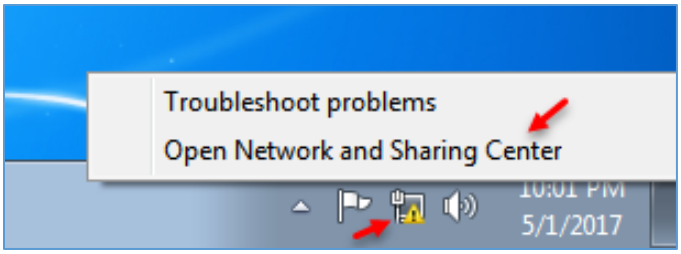
در این صفحه، گزینه‌ی Public Interface connected to private network را انتخاب کنید و تیک گزینه‌ی Enable NAT on this interface را انتخاب و بر روی OK کلیک کنید.



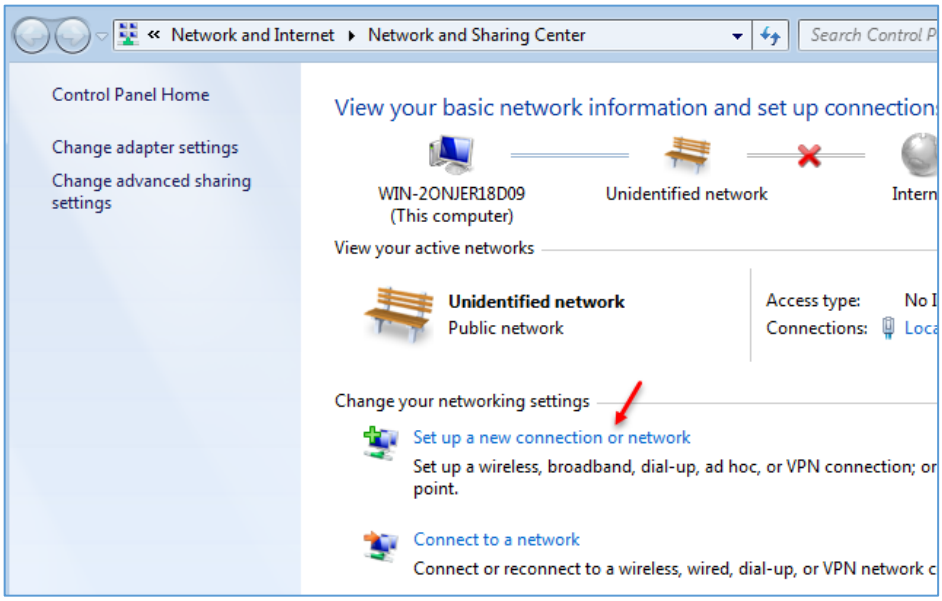
بعد از اینکه سرویس را آماده کردید باید به کاربران خود در شبکه دسترسی دهید تا بتوانند به سرور Route، یک کانکشن VPN بزنند، برای این کار وارد Active Directory Users and Computers شوید و بر روی نام کاربر خود کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



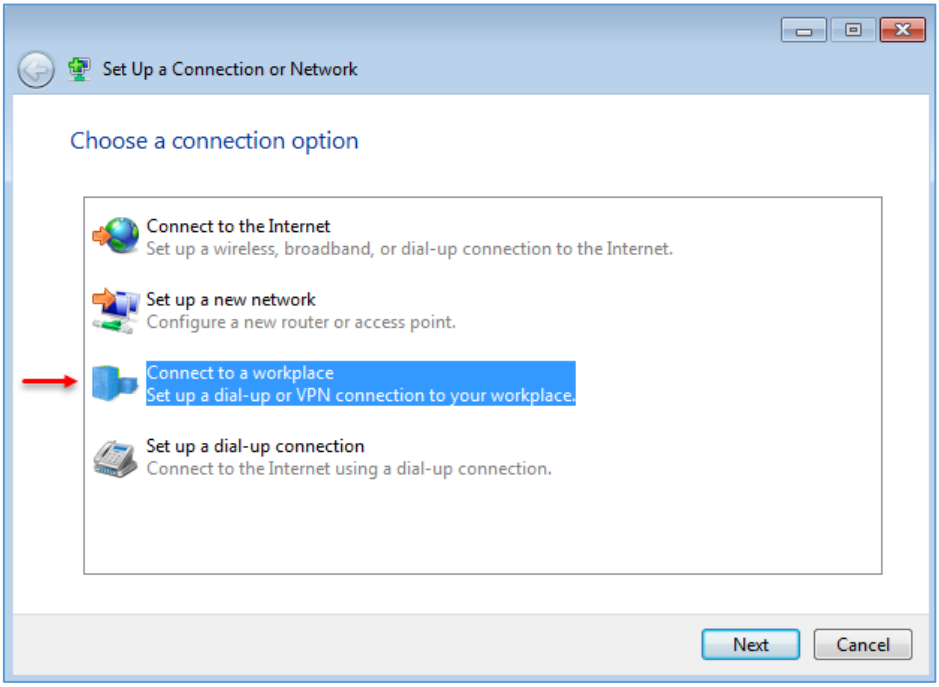
در این قسمت وارد تب Dial-in شوید و تیک گزینه‌ی Allow Access را انتخاب و بر روی OK کلیک کنید.



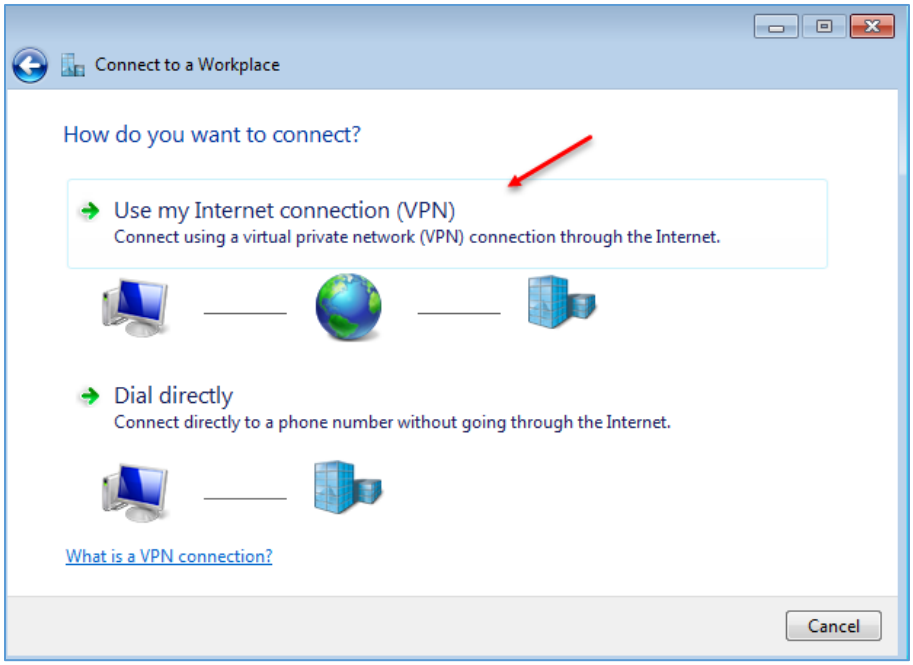
برای تست موضوع وارد یکی از کلاینت‌های شبکه که ویندوز ۷ نیز بر روی آن نصب شده است، شوید و بر روی کارت شبکه کلیک راست کنید و گزینه‌ی Open Network and Sharing Center را انتخاب کنید.



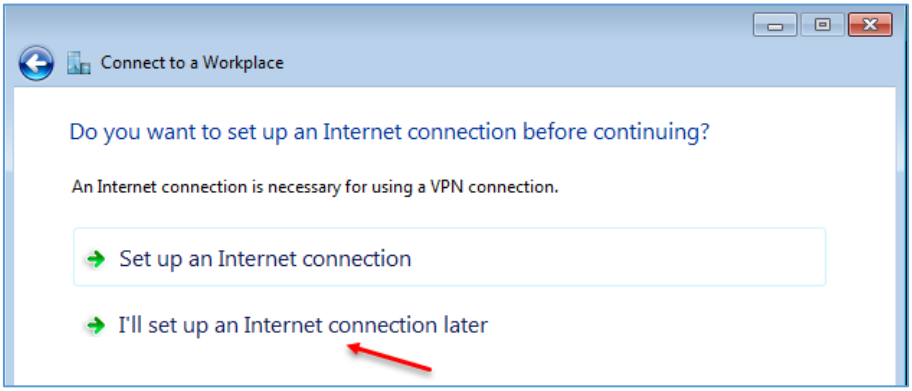
در این قسمت بر روی Set Up a New Connection or network کلیک کنید.



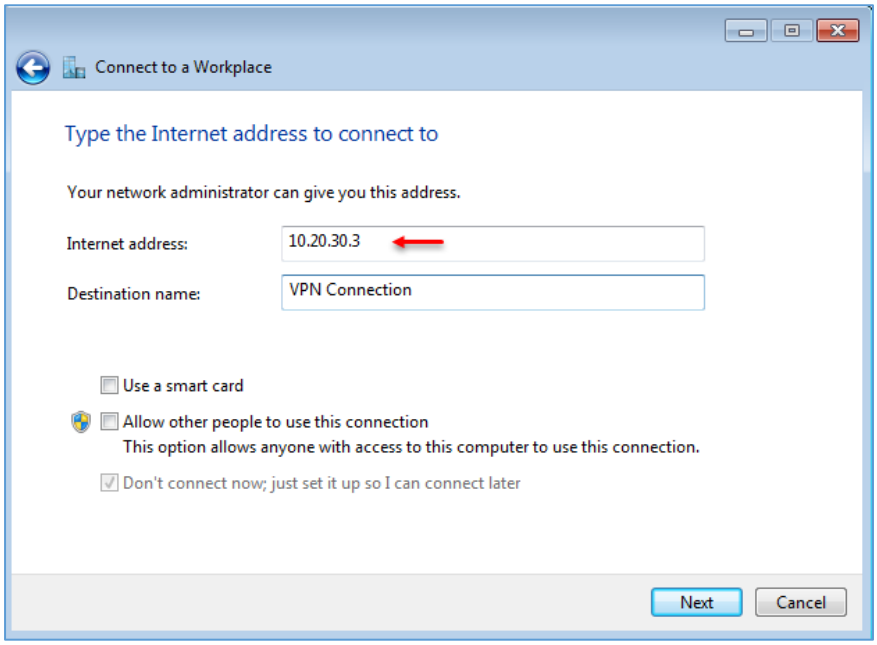
در این صفحه، گزینه‌ی Connect to Workplace را انتخاب و بر روی Next کلیک کنید.



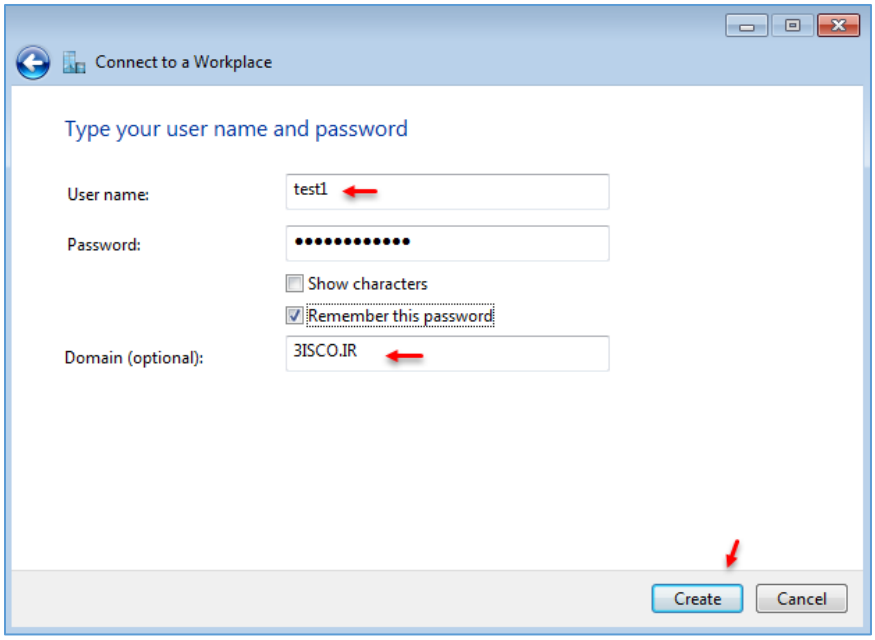
در این قسمت، گزینه‌ی اوّل را انتخاب و بر روی Next کلیک کنید.



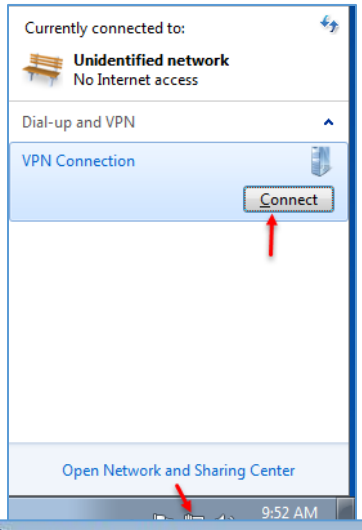
در این صفحه، گزینه‌ی دوّم را انتخاب و بر روی Next کلیک کنید.



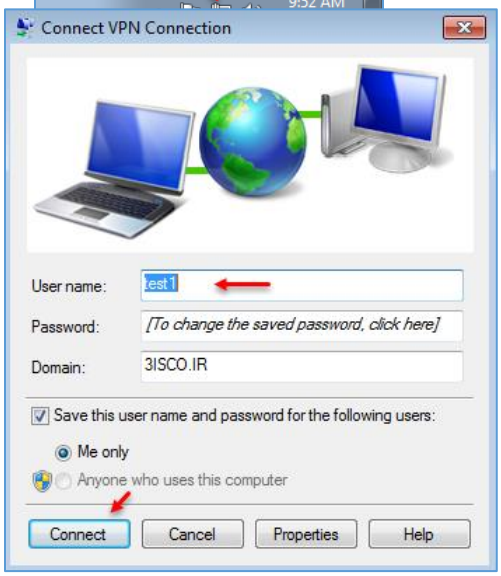
در این قسمت، آدرس سرور Route که سرویس VPN بر روی آن فعّال است را وارد و بر روی Next کلیک کنید.



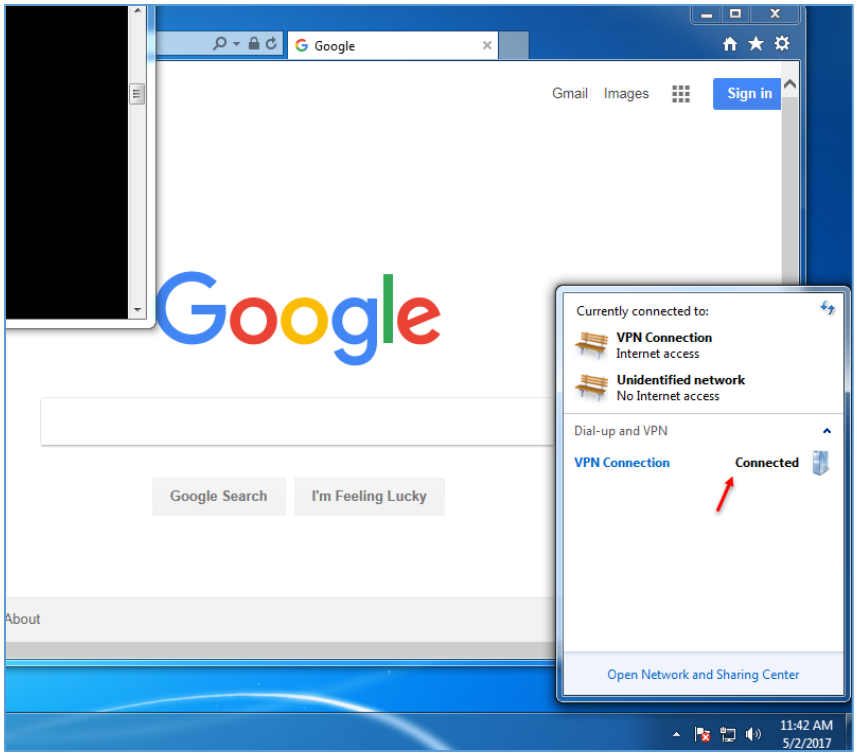
در این صفحه باید نام کاربری که در قسمت‌های قبل در Active directory فعّال کردید را وارد و رمز عبور آن را نیز وارد کنید، اگر چنانچه از خارج از شبکه‌ی دومین و در WorkGroup قصد ارتباط دارید باید نام دومین را وارد و بر روی Create کلیک کنید.



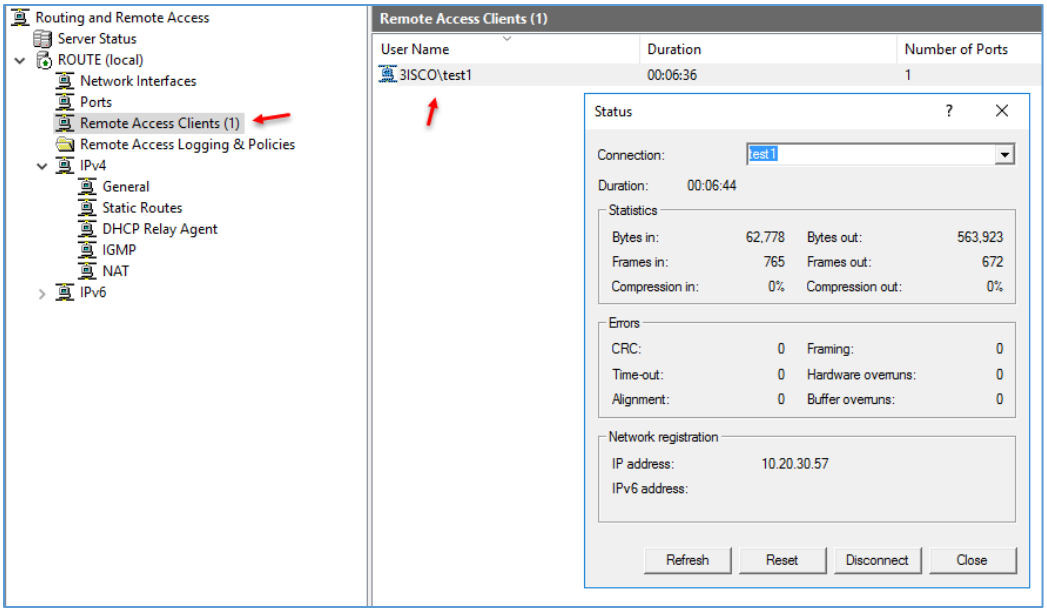
بعد از ایجاد Connection بر روی آیکون کارت شبکه کلیک کنید تا کانکشن خود را مشاهده کنید، بر روی آن کلیک و بعد، بر روی Connect کلیک کنید.



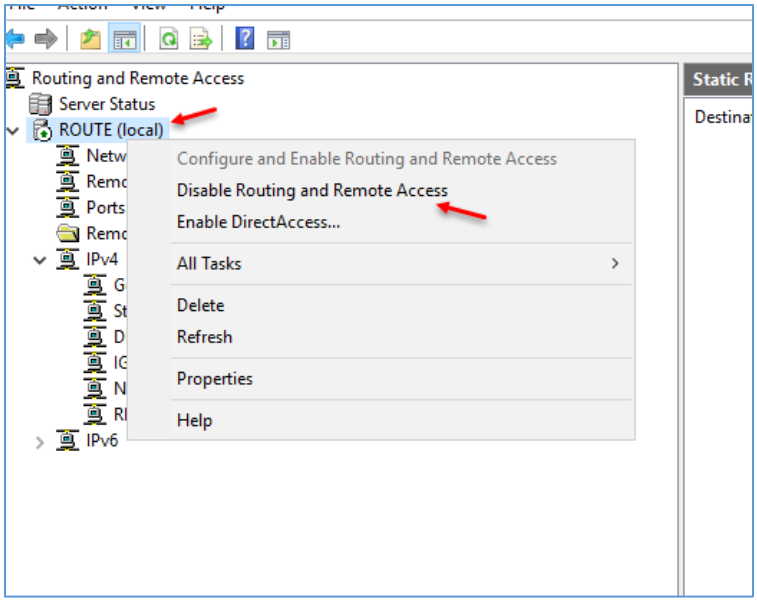
در این قسمت، اطّلاعاتی که وارد کردید از قبل ذخیره شده است و شما برای ارتباط باید بر روی connect کلیک کنید.



همانطور که در شکل روبرو مشاهده می‌کنید، کانکشن VPN برقرار شده است و کلاینت مورد نظر می‌تواند صفحات اینترنت را باز کند.



بعد از ارتباط، اگر وارد سرویس Routing شوید و بر روی Remote Access Client کلیک کنید، مشاهده می‌کنید که یک کاربر به لیست اضافه شده است و زمان ارتباط آن را مشاهده می‌کنید، برای اینکه وضعیّت آن را بهتر مشاهده کنید باید بر روی آن کلیک راست کنید و گزینه‌ی Status را انتخاب کنید که شکل آن را مشاهده می‌کنید و اگر بخواهید آن را قطع کنید باید گزینه‌ی Disconnect را انتخاب کنید.



برای حذف تنظیمات انجام داده شده در سرویس Routing and Remote access باید بر روی نام سرور کلیک راست کنید و گزینه‌ی Disable Routing and Remote Access را انتخاب کنید

راه‌اندازی سرور آنتی ویروس:

برای اینکه یک شبکه‌ی امن داشته باشید، نیاز صد در صد به یک آنتی ویروس خوب دارید که امنیّت شبکه‌ی شما را تضمین کند، در دنیای فنّاوری اطّلاعات، آنتی ویروس‌های مختلفی با کارکردهای مختلفی وجود دارند که هر کدام دارای ویژگی‌های خوب و بدی هستند.

در سایت زیر می‌توانید به صورت آنلاین، رنکینگ بهترین آنتی ویروس‌ها را مشاهده کنید:

http://chart.av-comparatives.org/chart1.php

در لیست زیر، قدرت آنتی ویروس‌ها را مشاهده می‌کنید.



در این کتاب بر روی آنتی ویروس Eset تمرکز خواهیم کرد و می‌آموزیم که چگونه از این نرم‌افزار به صورت شبکه‌شده استفاده کنیم، البتّه به صورت رایگان این کار را انجام خواهیم داد.

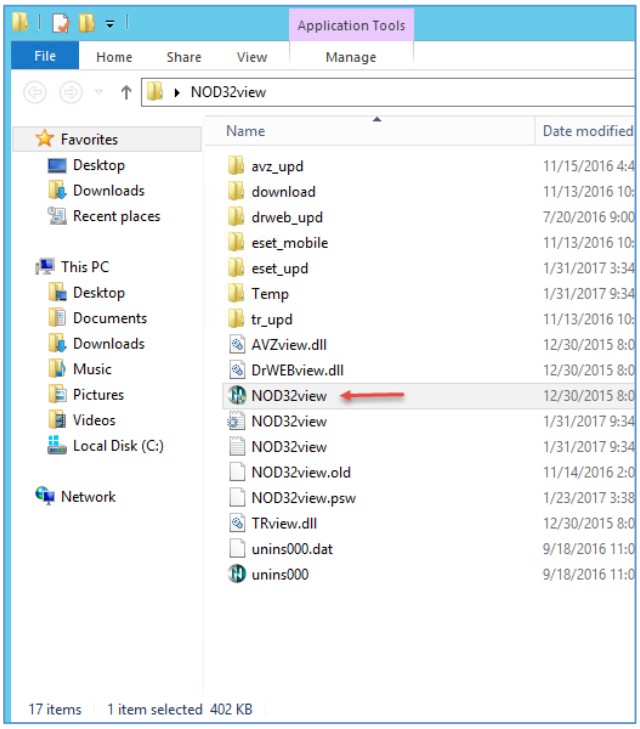
برای این کار، نیاز به یک سرور دارید که مدام به اینترنت متّصل باشد که بر روی آن باید نرم‌افزار تحت شبکه‌ی Nod را نصب کنید، البتّه این نرم‌افزار ساخت روسیه است و ارتباطی با نرم‌افزار اصلی شرکت Nod ندارد.

برای شروع کار، نرم‌افزار Nod32View را از لینک زیر دانلود کنید:

https://drive.google.com/file/d/0Bw1Nv5ua4a5-QXBoVmI4MENCOGc/view

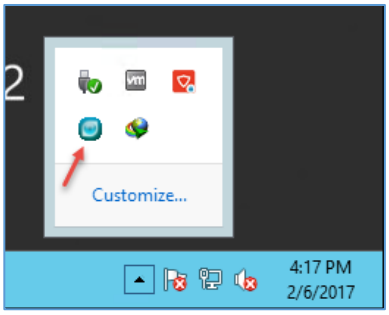
این نرم‌افزار، توانایی ارتباط با سرورهای Nod را دارد و با دادن رمز عبور به آن، آخرین آپدیت‌ها را دریافت می‌کند.

یک سرور در شبکه‌ی خود ایجاد کنید که بر روی آن می‌توانید ویندوز دلخواه خود را نصب کنید، مانند ویندوز ۷ و بعد از این کار، نام سرور را Anti در نظر بگیرید و آدرس آن را مشخّص و آن را عضو دومین کنید.

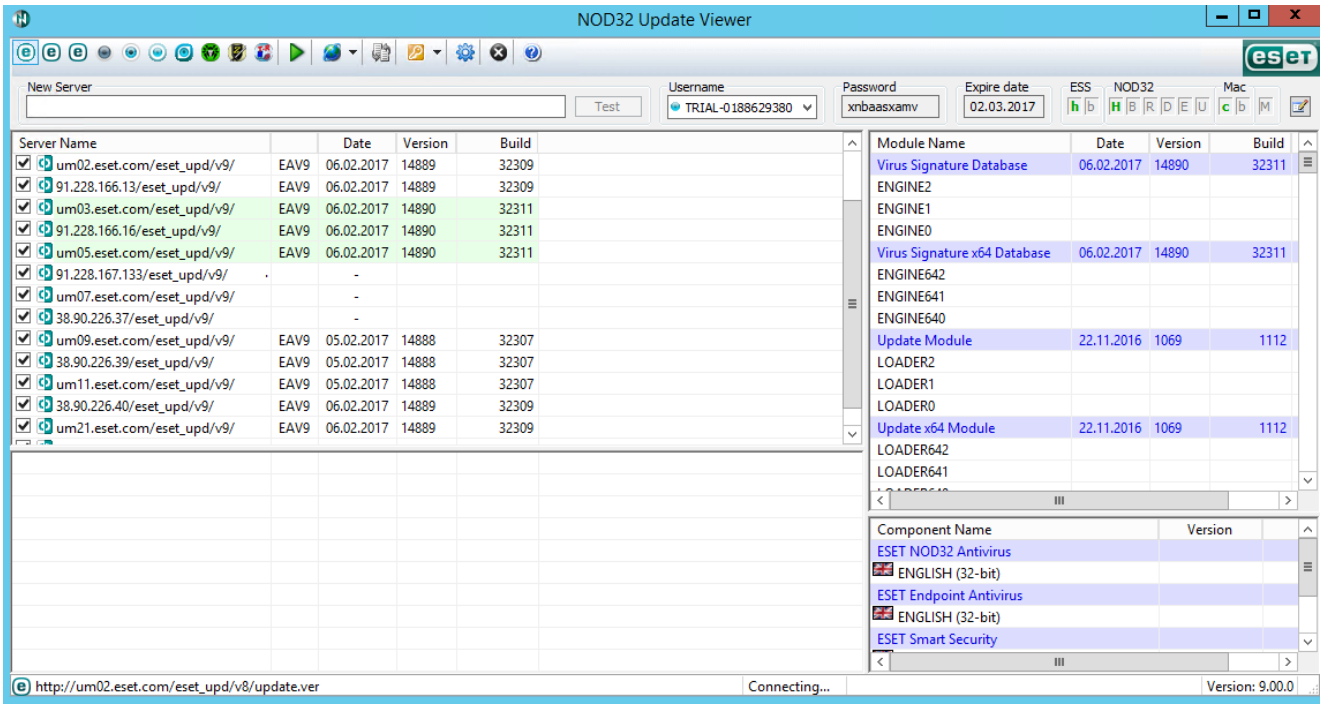


بعد از اینکه سرور را آماده و عضو دومین کردید باید آن را به اینترنت متّصل کنید، بعد وارد پوشه‌ی نرم‌افزار NodView شوید و بر روی Nod32View کلیک راست کنید و گزینه‌ی Run as Admin را انتخاب کنید.

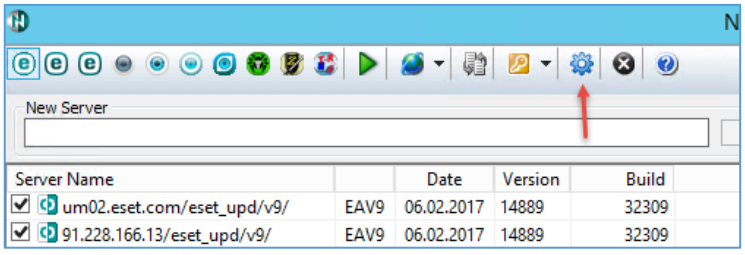
نکته: به هیچ عنوان بر روی سرور آنتی ویروس، نرم‌افزار کلاینتی آنتی ویروس را نصب نکنید تا با مشکلی مواجه نشوید.



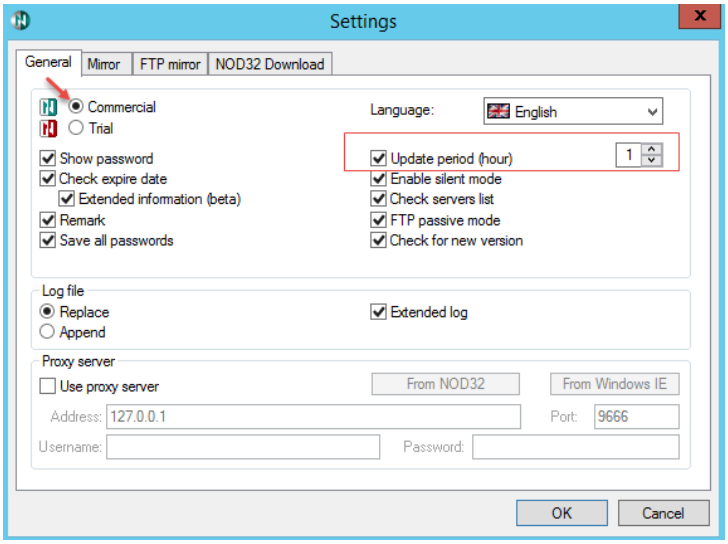
دو بار بر روی آیکون نرم‌افزار Nod32View کلیک کنید تا شکل بعد ظاهر شود.



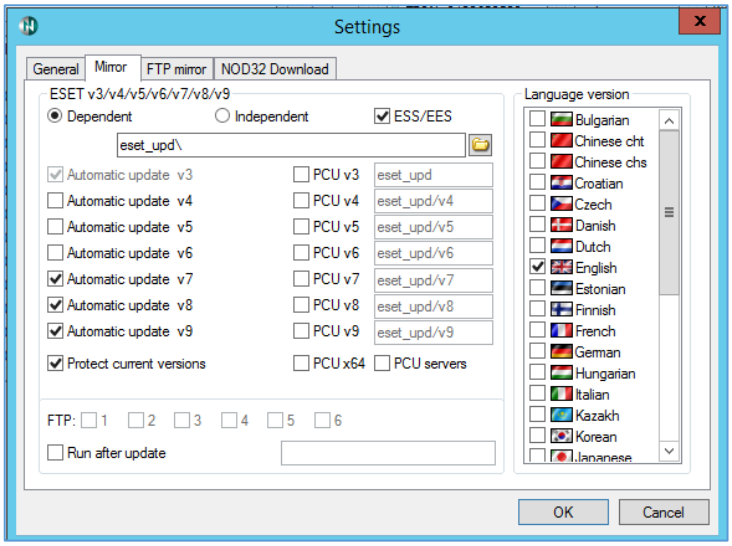
در شکل بالا، نمای کلّی نرم‌افزار را مشاهده می‌کنید، البتّه این نرم‌افزار در حال کار است و شاید برای شما شکل دیگری نمایش داده شود که آن را در ادامه کامل خواهیم کرد.



به مانند شکل روبرو، بر روی آیکون Settings کلیک کنید.

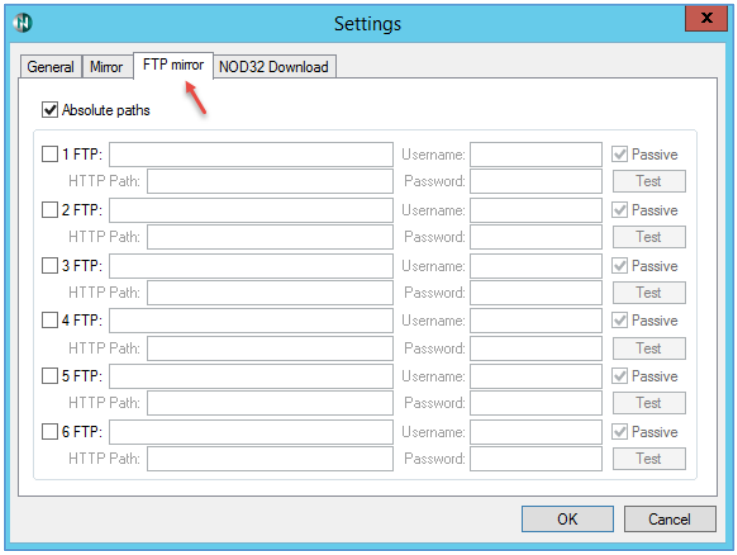


در این صفحه و در تب General، دو گزینه‌ی Commercial و Trial وجود دارد که باید گزینه‌ی اوّل را انتخاب کنید، در قسمت Update Period می‌توانید مشخّص کنید که سرور چند ساعت به چند ساعت، آخرین آپدیت‌ها را از سایت Nod دریافت کند.

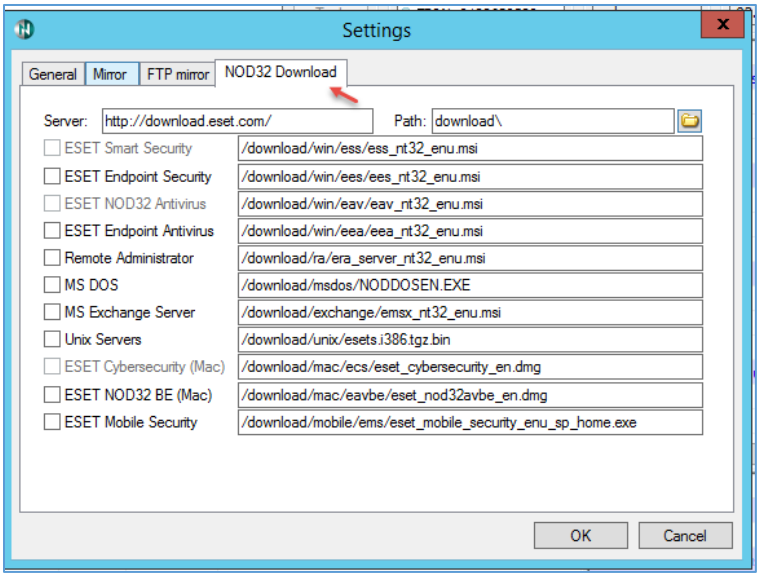


در تب Mirror می‌توانید مشخّص کنید که آپدیت کدام ورژن آنتی ویروس از سایت Nod32.com دریافت شود که در این کتاب، ورژن ۸ آن بررسی خواهد شد.

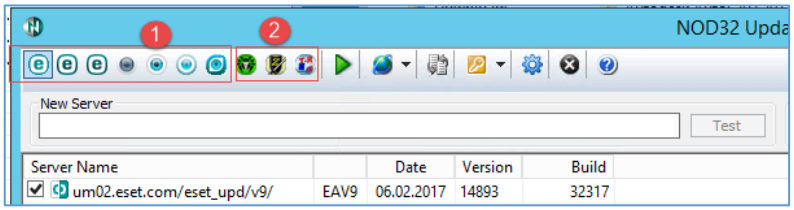
در قسمت Language version می‌توانید زبان آنتی ویروس خود را برای دریافت آپدیت، انتخاب کنید.



در این قسمت می‌توانید از سرورهای FTP دیگران که آخرین آپدیت‌های خود را در آن قرار می‌دهند، استفاده کنید، مانند سایت: Softgozar.com.



در این قسمت می‌توانید آخرین ورژن‌های نرم‌افزار Eset را از سایت آن دانلود کنید که بعد از دانلود، از آدرس http://download.eset.com/ در پوشه‌ی download\ قرار می‌گیرد که شما می‌توانید آن را تغییر دهید.



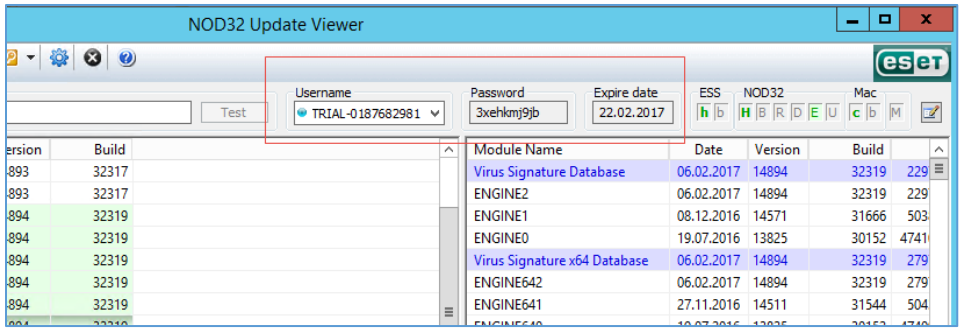
در بالای نرم‌افزار، آیکون‌های مختلفی را مشاهده می‌کنید، در قسمت شماره‌ی یک، ورژن‌های مختلف آنتی ویروس از ۳ تا ۹ را مشاهده می‌کنید که می‌توانید با کلیک بر روی آن، آدرس سرورهای آپدیت و ورژن دیتابیس آنها را مشاهده کنید، در قسمت شماره‌ی دو، سه ابزار برای یافتن تروجان‌ها و... وجود دارد که یکی، آپدیت نرم‌افزار امنیّتی سایت drweb.com است که می‌توانید با ورود به سایت و دانلود نرم‌افزار آن از سرور، جدیدترین آپدیت‌ها را دریافت کنید، دیگری ابزار سایت z-oleg.com است که از لینک زیر می‌توانید نرم‌افزار آن را دانلود کنید:

http://z-oleg.com/avz4.zip

ابزار بعدی، Trojan Remover است که برای شناسایی و حذف تروجان‌ها کاربرد دارد که از آدرس زیر می‌توانید آخرین ورژن آن را دریافت کنید:

https://www.simplysup.co.uk/download/dl/trjsetup695.exe

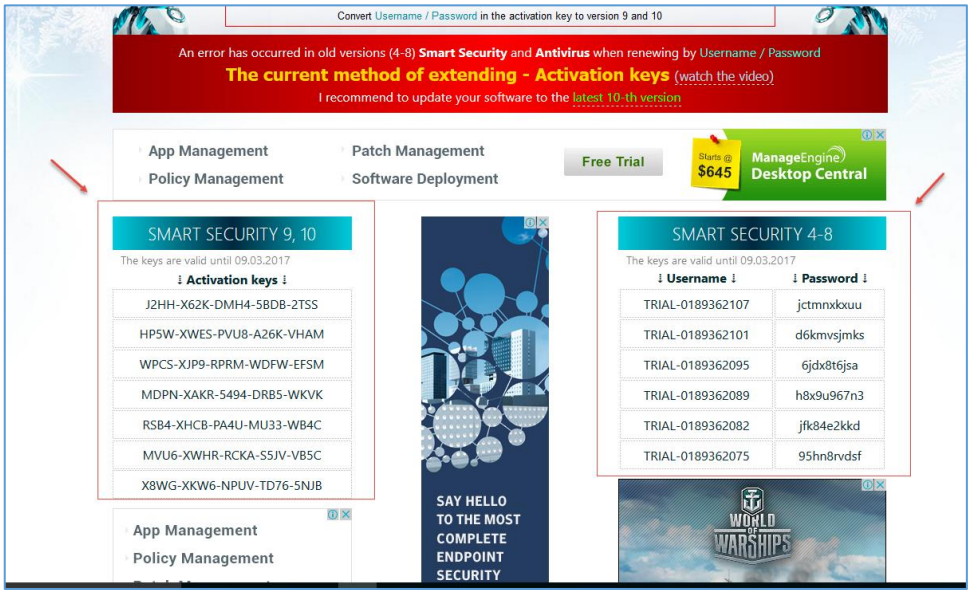
این ابزارها می‌توانند در کنار آنتی ویروس شما به شما در حفظ امنیّت سیستم‌هایتان کمک کنند که در حال حاضر با این ابزارها کاری نداریم و آنها را فعّال نمی‌کنیم.



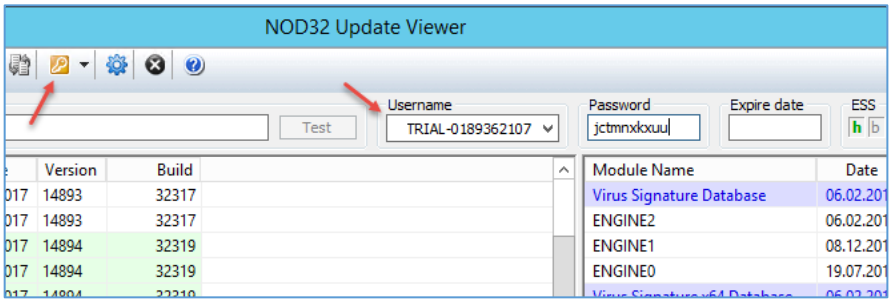
برای اینکه سرور خود را همیشه آپدیت نگه دارید باید نام کاربری و رمز عبوری را که از سایت ESET دریافت می‌کنید، در قسمت Username و Password وارد کنید تا بعد از بررسی و تأیید نرم‌افزار بتواند آپدیت‌های جدید را از سایت ESET دریافت کند.

برای دریافت آخرین رمزهای شرکت ESET به سایت زیر مراجعه کنید:

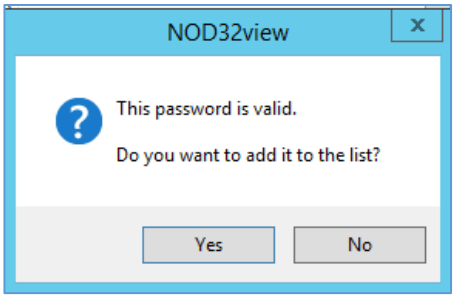
https://t2bot.ru/en/esetkeys/



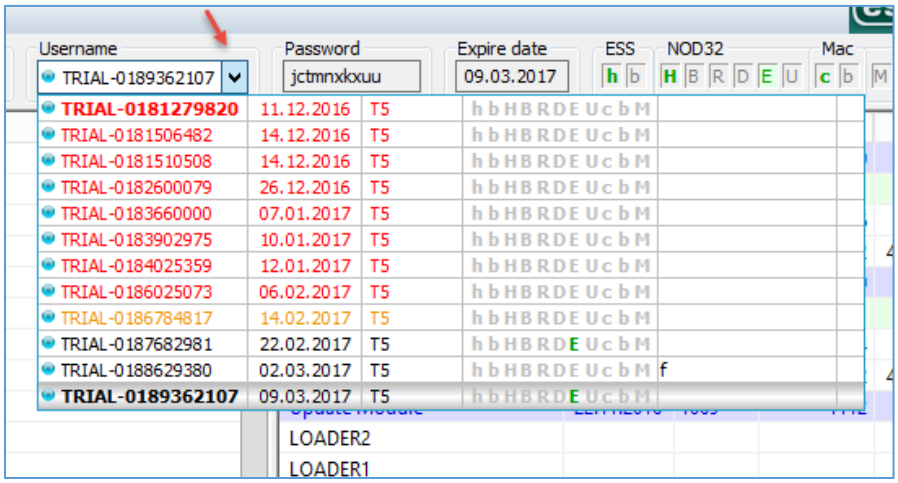
نام کاربری و رمز عبور مربوط به شرکت ESET را در ورژن‌های مختلف مشاهده می‌کنید، شما باید این رمز را در قسمت مشخّص‌شده‌ی نرم‌افزار وارد کنید.



در شکل روبرو و در قسمت Username، نام کاربری و رمز عبور جدید وارد شده است، بعد از ورود اطّلاعات باید بر روی آیکون Check Password کلیک کنید، اگر رمز عبور مورد تأیید بود در نرم‌افزار ثبت خواهد شد، بعد از آن، نرم‌افزار شروع به دریافت آخرین آپدیت خواهد کرد.



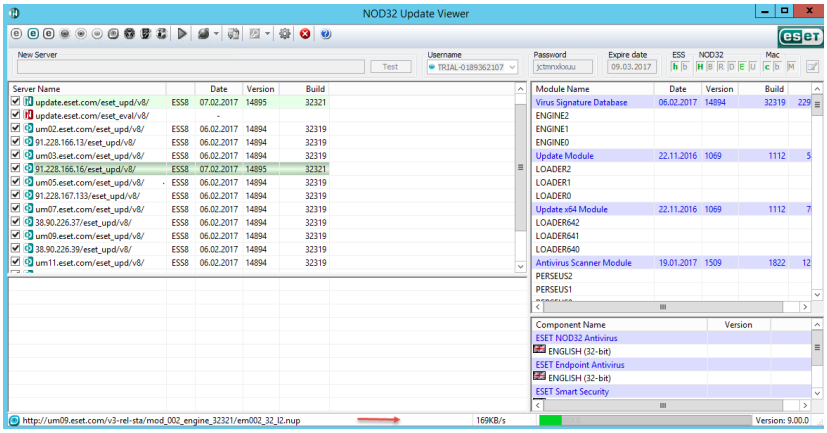
اگر رمز عبور مورد تأیید بود با پیغام روبرو مواجه خواهید شد که به شما اعلام می‌کند، رمز عبور مورد تأیید است، اگر مایل هستید آن را به لیست خود اضافه کنید.



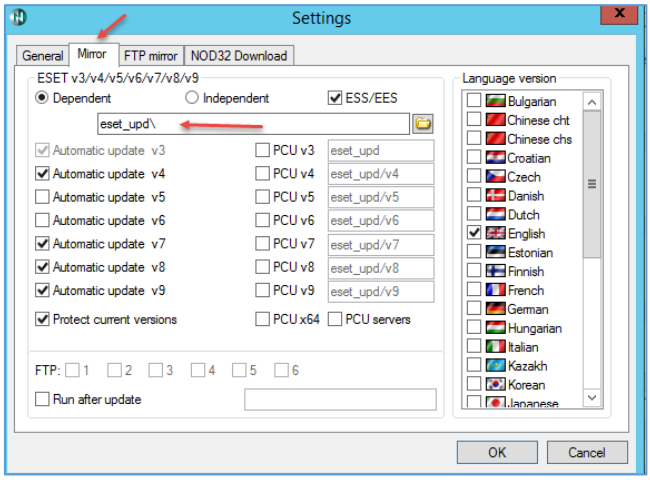
اگر چندین رمز عبور را ست کرده باشید با کلیک بر روی فلش رو به پایین کنار Username، لیست همه‌ی آنها را مشاهده خواهید کرد، در شکل روبرو چندین نام کاربری را با رنگ‌های مختلف مشاهده می‌کنید که رنگ قرمز، به معنی به اتمام رسیدن سررسید است و رنگ زرد، یعنی نزدیک به انقضا شدن است و رنگ سیاه نیز بدون مشکل خواهد بود. شما می‌توانید تاریخ انقضای هر رمز عبور را مشاهده کنید.



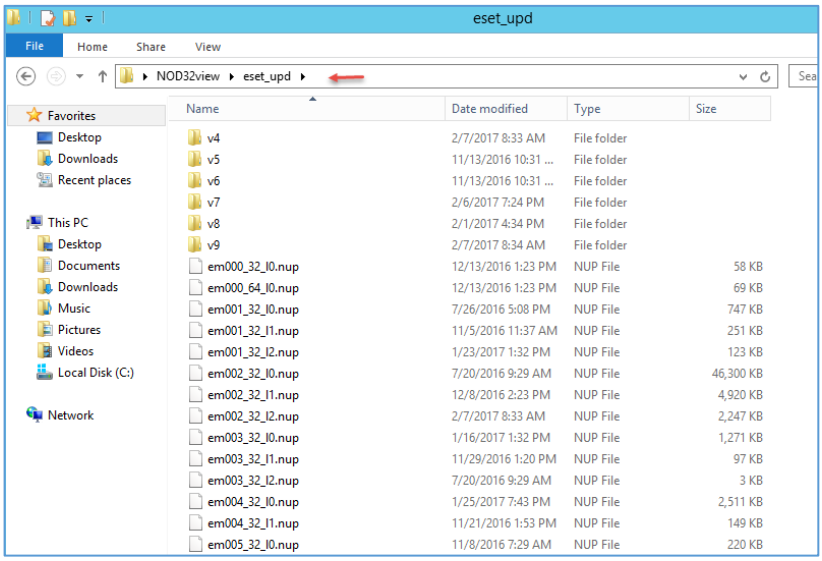
بعد از اینکه رمز عبور را ست کردید، دو آیکون در بالای صفحه به مانند شکل روبرو مشاهده می‌کنید که اگر بر روی آیکون Check All Servers کلیک کنید، تمام آدرس سرورهای جدید از سایت Eset دریافت خواهد شد، بعد از این کار بر روی شماره‌ی دو، یعنی Run automatic Update کلیک کنید.



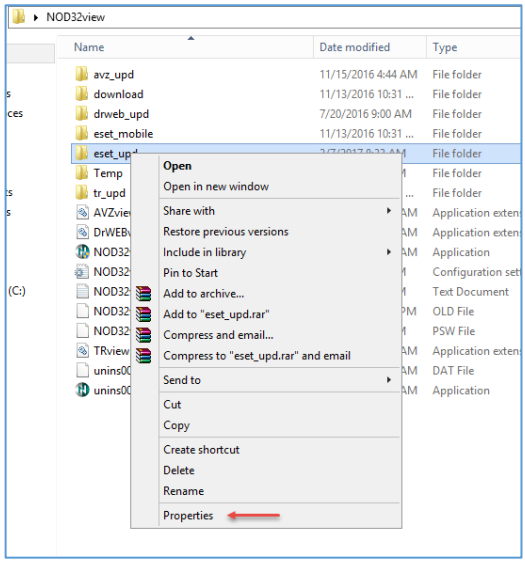
همانطور که در شکل روبرو مشاهده می‌کنید، نرم‌افزار در حال دریافت آخرین آپدیت‌ها به صورت مستقیم ازسایت Eset است که این اطّلاعات در پوشه‌ای که در Settings وجود دارد، ذخیره می‌شود.



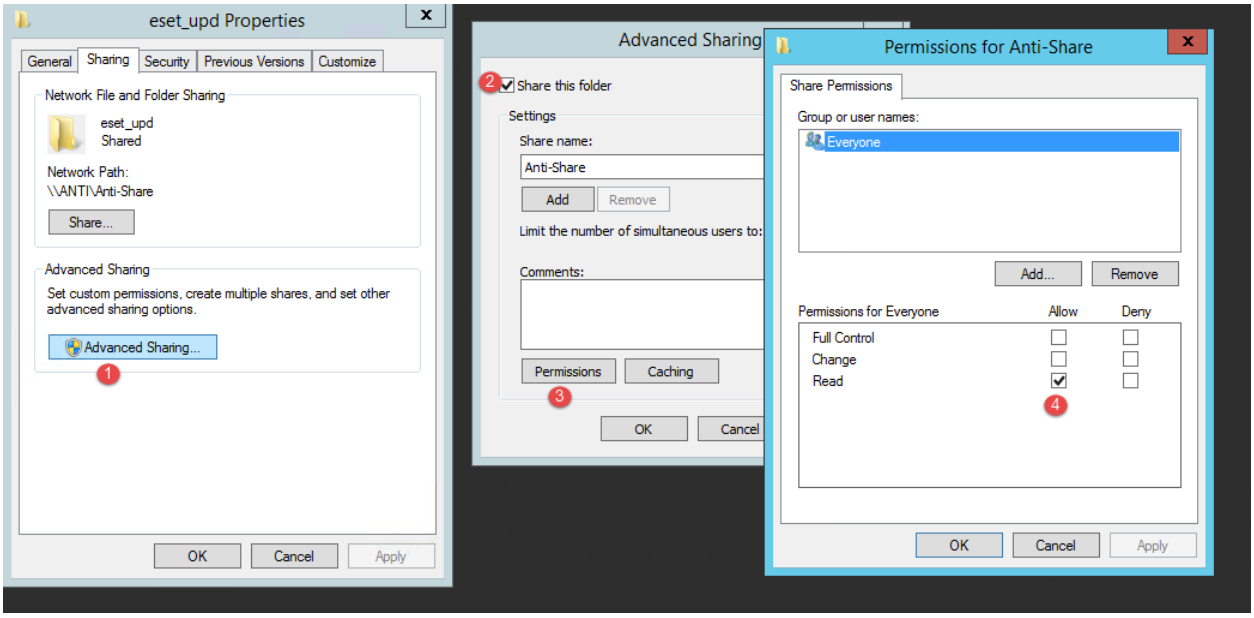
این صفحه را در قسمت‌های قبل بررسی کردیم که در تب Mirror، پوشه‌ای که در آن آپدیت ذخیره می‌شود، مشخّص شده است، شما نیز می‌توانید این پوشه را تغییر دهید.



در این صفحه، تمام آپدیت‌هایی که از سایت Eset دریافت شد را مشاهده می‌کنید که برای اینکه از این آپدیت‌ها استفاده کنید باید این پوشه را برای کاربران خود، share کنید.



بر روی پوشه‌ی مورد نظر کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.

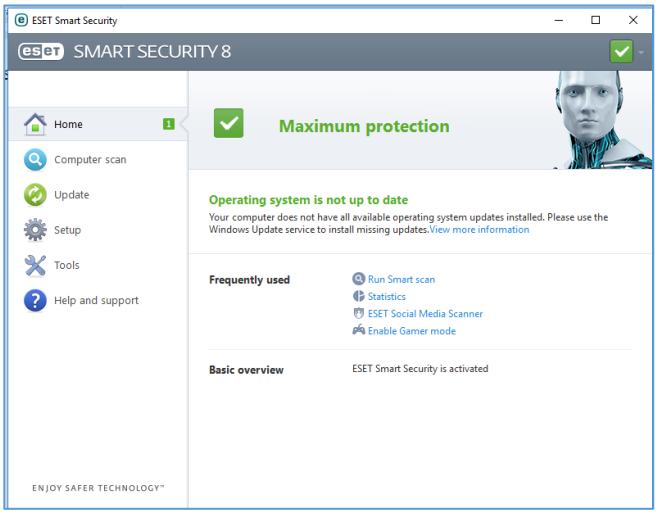


به مانند شکل بالا بر روی Advanced Sharing کلیک کنید و در صفحه‌ی بازشده، تیک گزینه‌ی Share this folder را انتخاب و بر روی شماره‌ی۳، یعنی Permissions کلیک کنید و در صفحه‌ی جدید بر روی Everyone کلیک و دسترسی Read را انتخاب کنید و همه را OK کنید.

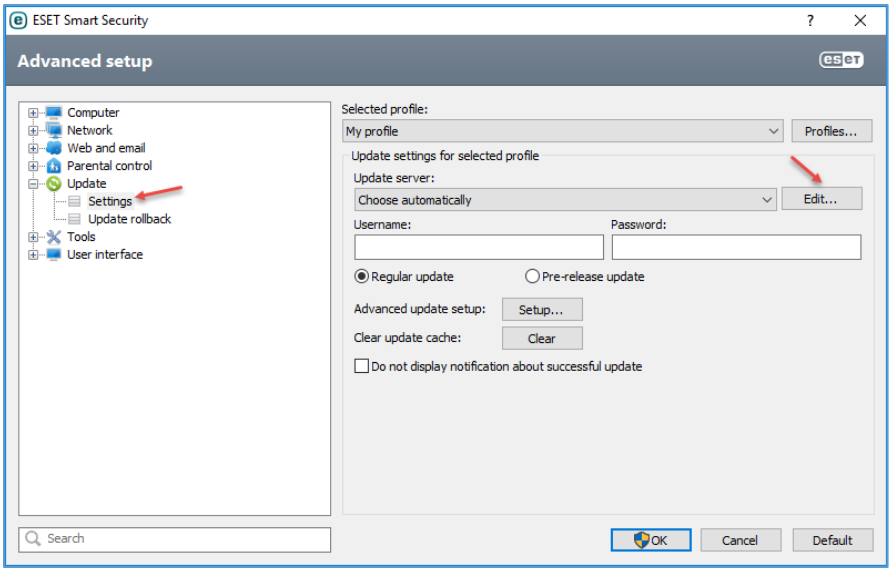
بعد از انجام مراحل بالا باید آنتی ویروس خود را بر روی کلاینت مورد نظر خود نصب کنید و تنظیم آپدیت آن را به صورت زیر انجام دهید.

برای دریافت آنتی ویروس کلاینت ESET می‌توانید از لینک زیر استفاده کنید:

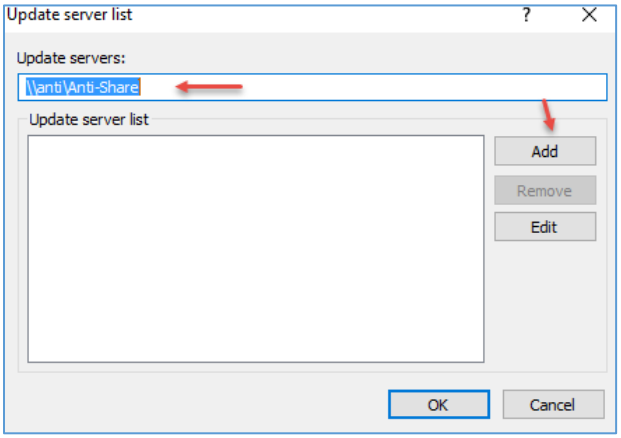
https://www.softgozar.com/download/3615/eset-smart-security-8-0-319-0-x86-x64-(update-12000)-2015-07-27



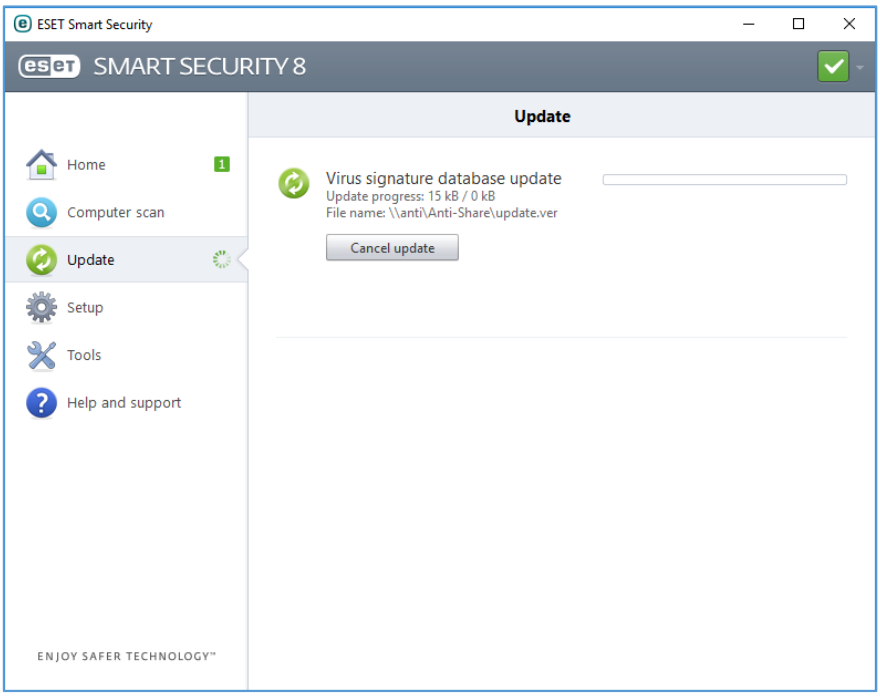
بعد از دانلود، آن را نصب کنید که کار ساده‌ای است، بعد از نصب، نرم‌افزار را اجرا کنید و بر روی F5 فشار دهید تا وارد تنظیمات آنتی ویروس شوید.



به مانند شکل روبرو از قسمت Update وارد قسمت Settings شوید و بر روی Edit کلیک کنید.



در قسمت Update server، آدرس به اشتراک گذاشته شده‌ی فایل قبلی را که با هم انجام دادیم در این قسمت وارد کنید که در این قسمت ANTI، همان نام سرور آنتی ویروس شما است، بعد از این کار بر روی Add کلیک کنید تا آدرس به لیست اضافه شود و بعد بر روی OK کلیک کنید.



بعد از انجام مراحل بالا، اگر بر روی Update کلیک کنید، آخرین آپدیت‌ها از محلّ پوشه‌ی به اشتراک گذاشته شده، دریافت و کلاینت مورد نظر آپدیت خواهد شد.

اگر پرسشی در این زمینه داشتید از طریق تلگرام در ارتباط باشید.

@farshidbabajani

نصب و راه‌اندازی دوربین مدار بسته:

یکی از امکاناتی که یک مدیر شبکه باید در یک سازمان پیاده‌سازی کند، دوربین مدار بسته است تا بتواند تمام رویدادها را در آن سازمان ثبت و ضبط کند.

یکی از مکان‌های مهمّی که باید از دوربین مدار بسته استفاده کنید، اتاق سرور است تا بتوانید تمام رفت و آمدها به این اتاق را کنترل کنید تا در زمان به وجود آمدن مشکل بتوانید آخرین نفری که به اتاق سرور مراجعه کرده است را مشخّص کنید.

برای راه‌اندازی دوربین مدار بسته، راه‌های مختلفی وجود دارد، یکی از این راه‌ها این است که دستگاه DVR آماده تهیّه کنید و دوربین‌ها را به آن متّصل کنید یا اینکه یک سرور خودتان راه بندازید و دوربین‌ها را به آن سرور متّصل کنید که در این کتاب، مورد دوّم که مشکل‌تر است را بررسی می‌کنیم.

برای راه‌اندازی دوربین مدار بسته به موارد زیر نیاز دارید:

- سرور با سخت‌افزار مناسب.
- دوربین با کیفیّت برای هر طبقه.
- کابل‌کشی برای دوربین‌ها.
- سوئیچ POE یا آداپتور برای هر دوربین.
- نرم‌افزار مورد نیاز برای ارتباط و مدیریّت دوربین‌ها.

انواع دوربین مداربسته:

دوربین‌های مدار بسته از نظر نوع سیگنال به سه دسته‌ی کلّی تقسیم می‌شوند:

۱. دوربین های آنالوگ:

این دوربین‌ها، نسل ابتدایی دوربین‌های مداربسته است که برای دریافت و ارسال اطّلاعات، صدا و تصویر از امواج آنالوگ استفاده می کنند؛ صدا و تصویر این دوربین‌ها، هر یک توسّط کابل دو رشته‌ای جداگانه منتقل می‌شوند که یک رشته از سیم‌ها نقش جلوگیری از نویز بر سیم اصلی را ایفا می‌کنند. کابل متداول برای



تصویر این دوربین‌ها، کابل کواکسیال rg59 است، اگر چه ارتباط تصویر این دوربین‌ها با کابل‌های مختلف بر حسب نیاز امکان‌پذیر است، کیفیّت این دوربین‌ها به خاطر آنالوگ بودن پایین است و همیشه امواج مزاحم بر روی تصاویر آنها تأثیر خواهد گذاشت.

۲. دوربین‌های ip تحت شبکه:

دوربین‌های IP یا همان، دیجیتال توانایی آن را دارند تا به راحتی به سوئیچ شبکه متّصل شوند و به صورت یک سیستم جداگانه، آدرس IP دریافت کنند، این دوربین‌ها از کیفیّت بالایی برخوردار هستند. در زیر بعضی از ویژگی‌های مفید آنها را بررسی می‌کنیم:

۱. کیفیّت بالای دوربین دیجیتال.
۲. امکان استفاده‌ی بهینه از کابل‌های ارتباطی.
۳. امکان ارتباط بی‌سیم با امنیّت و کیفیّت بالا.
٤. امکان ارسال هم‌زمان تصویر، صدا و برق در بستر شبکه.
۵. ارتباط دوربین‌های دیجیتال با بستر اینترنت و کنترل آنها از طریق اینترنت.
٦. هیچ گونه تبدیل کننده‌ای بر سر راه آن قرار ندارد و مستقیم به سرور NVR متّصل می‌شود.
۷. برق این نوع دوربین‌ها یا از طریق آداپتور و یا از طریق سوئیچ POE تأمین می‌شود، این نوع سوئیچ‌ها روی پورت‌های خود برق را تأمین می‌کنند و این برق از طریق کابل شبکه به دوربین ارسال می‌شود و دوربین مقصد باید ویژگی POE را پشتیبانی کند.

در شکل زیر، دوربین دیجیتالی را مشاهده می‌کنید که تنها دارای یک پورت شبکه است و صدا، تصویر و برق تنها از طریق این پورت ارسال و دریافت می‌شود.



سرور مناسب برای راه‌اندازی دوربین مدار بسته:

برای اینکه یک سرور مناسب برای دوربین داشته باشید باید حداقل، امکانات سخت‌افزاری زیر را تهیّه کنید:

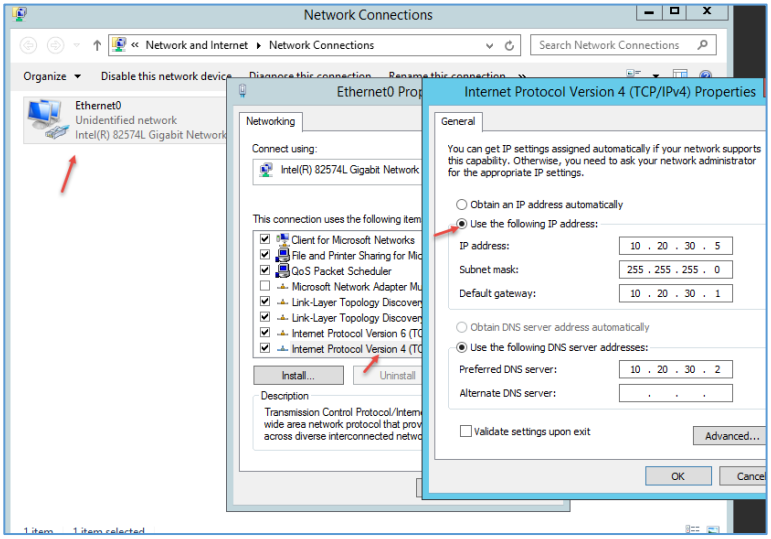
- ✓ هارد دیسک ۲ ترابایت معمولی.
- ✓ رم ٦ گیگابایت DDR3.
- ✓ سی پی یو CORE I3 با سرعت ۲,٤ گیگاهرتز.

توجّه داشته باشید شما می‌توانید از یک سرور HP، مانند G6 یا G7 نیز برای این کار استفاده کنید.

بعد از اینکه سرور را آماده کردید باید بر روی آن ویندوز مناسب نصب کنید، این ویندوز می‌تواند ۷ یا نسخه‌های بالاتر از آن باشد، برای این کار از ویندوز سرور نیز می‌توانید استفاده کنید.

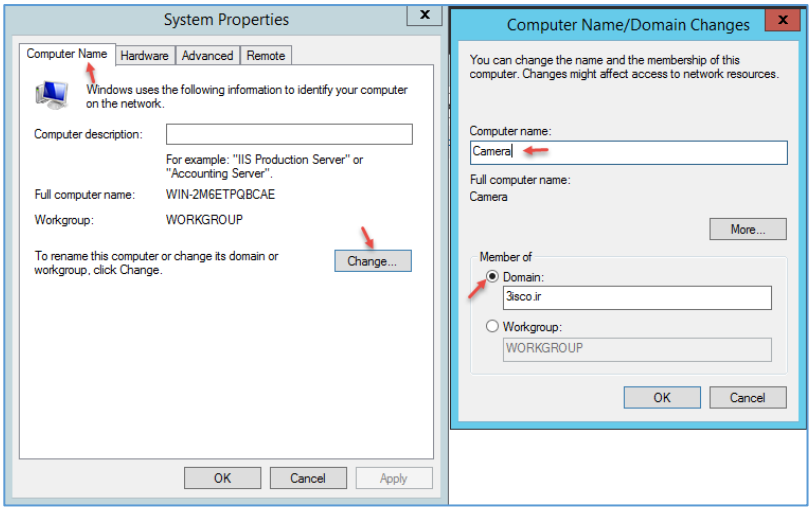
در این کتاب برای راه‌اندازی سرور دوربین از ویندوز ۷، ورژن ٦٤ بیت استفاده می‌کنیم، بعد از اینکه سیستم را آماده کردیم، بر روی آن ویندوز ۷ را نصب می‌کنیم.

برای سرور دوربین‌ها، نرم‌افزار Aimetis Symphony را در نظر گرفتیم که یک نرم‌افزار قدرتمند در این زمینه است، با استفاده از این نرم‌افزار، تمام قابلیّت‌های DVR های مختلف در اختیار شما قرار دارد.

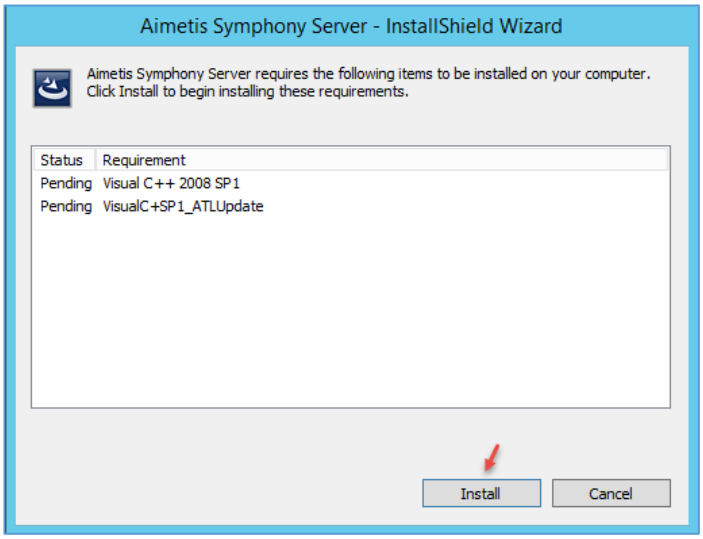


بعد از نصب ویندوز باید نام و آدرس IP آن را تغییر دهید و آن را تحت دومین قرار دهید، برای این کار وارد ویندوز شوید و به مانند شکل روبرو، آدرس سرور دوربین را تغییر دهید.

آدرس IP سرور دوربین را به 10.20.30.5 تغییر دهید.

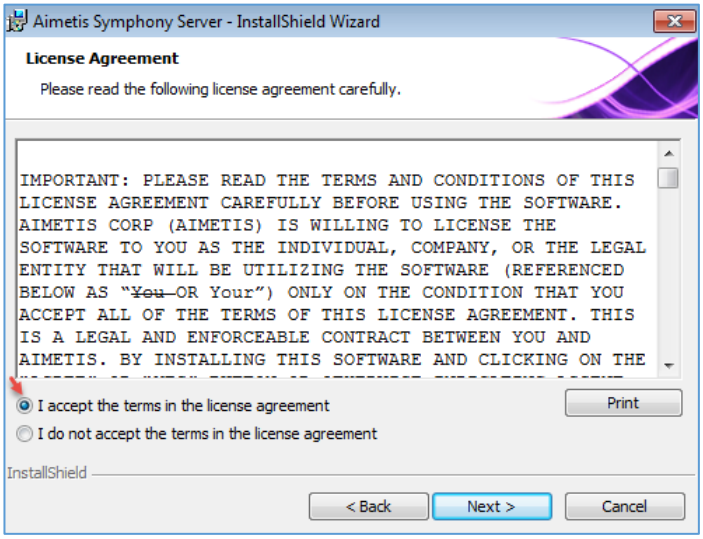


برای تغییر نام، به مانند شکل عمل کنید و نام سرور را به Camera تغییر دهید و عضو دومین 3isco.ir کنید، بعد از این کار سرور را Restart کنید.

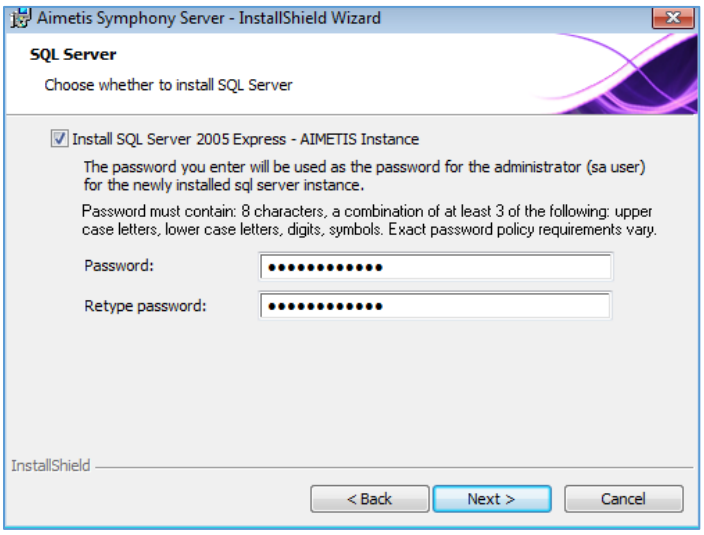


بعد از اینکه سرور را اجرا کردید با کاربر ادمین وارد سرور شوید تا نرم‌افزار را نصب کنید.

در صفحه‌ی روبرو بر روی Install کلیک کنید تا پیش‌نیازهای مورد نظر بر روی سرور نصب شود.



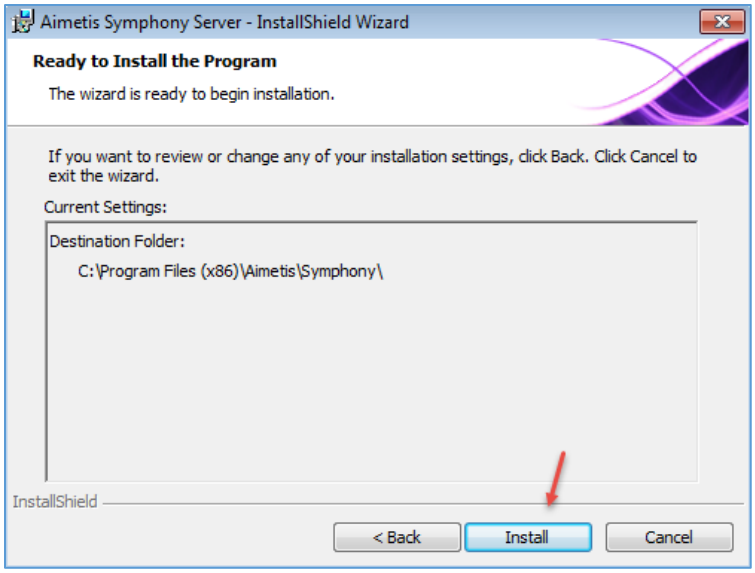
اگر در این صفحه، شرایط نرم‌افزار را قبول دارید، گزینه‌ی I accept... را انتخاب و بر روی Next کلیک کنید.



در این قسمت، یک رمز عبور برای کاربر SQL با عنوان sa user وارد کنید که باید ترکیبی از حروف بزرگ و کوچک و عدد باشد و حداقل ۸ کاراکتر باشد، مانند:

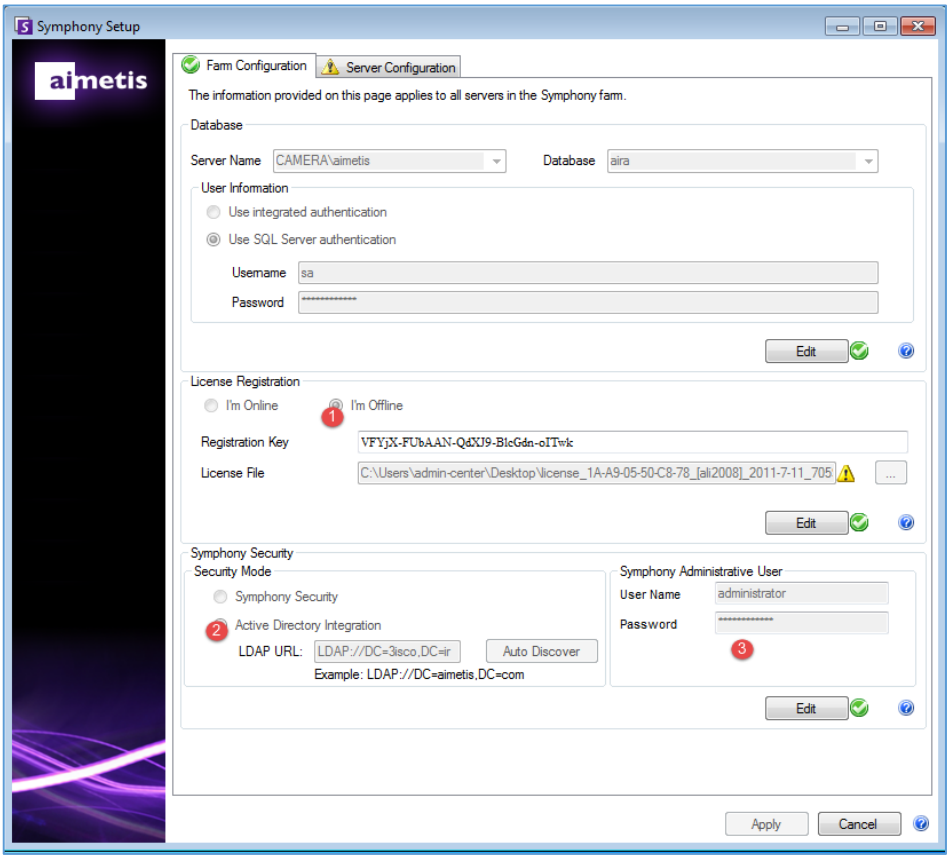
Test12345678

که در رمز بالا، T با حرف بزرگ وارد شده است.



بر روی Install کلیک کنید تا کار نصب آغاز شود.

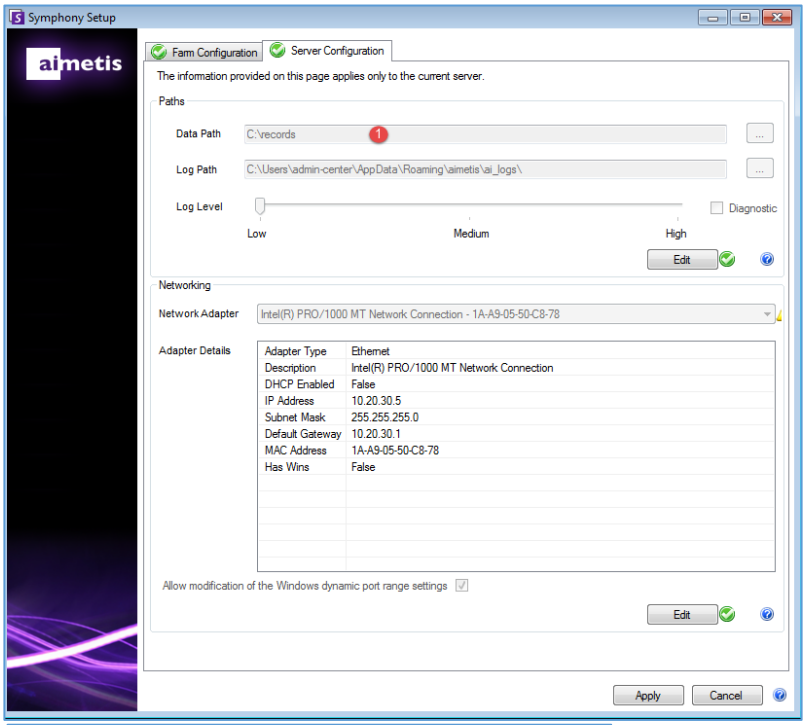
بعد از نصب بر روی Finish کلیک کنید تا نرم‌افزار اجرا شود.



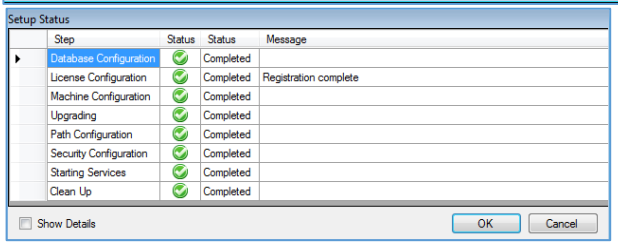
زمانی که نرم‌افزار اجرا می‌شود، این صفحه برای شما ظاهر خواهد شد که مربوط به کانفیگ نرم‌افزار است، در قسمت Farm Configuration و در قسمت شماره‌ی یک باید لایسنس نرم‌افزار را به سیستم معرّفی کنید و در قسمت شماره‌ی دو، طبق شکل، نام دومین خود را به صورت زیر وارد کنید:

LDAP://DC=3isco.DC=ir

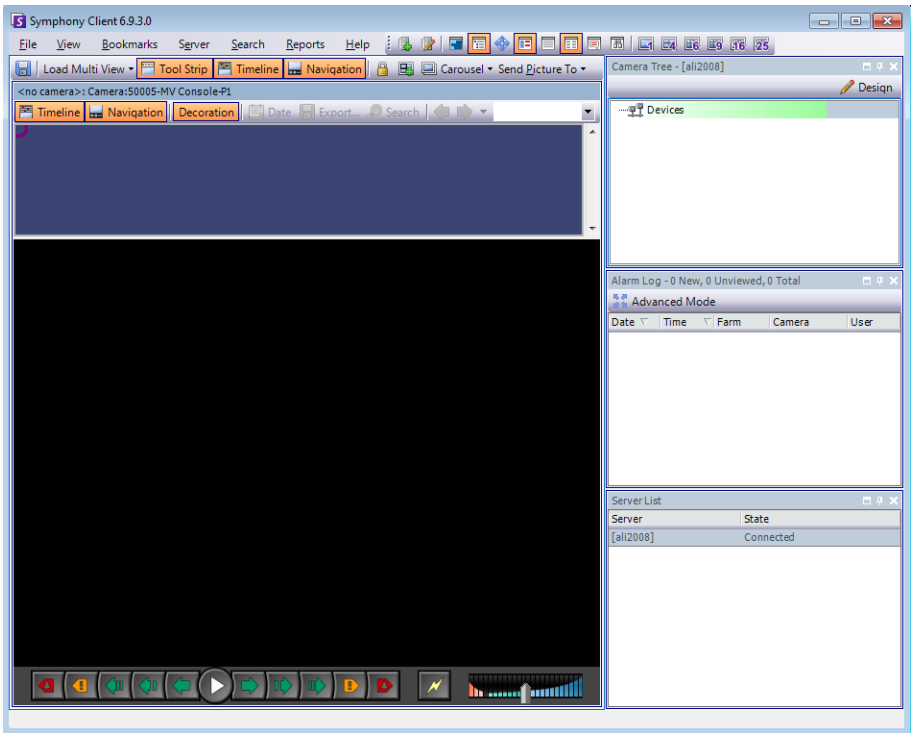
و در قسمت شماره‌ی سه باید یک نام کاربری و رمز عبور برای مدیریّت نرم‌افزار وارد کنید و در آخر بر روی Verify کلیک کنید تا مانند شکل بالا، هر سه قسمت تأیید شود.



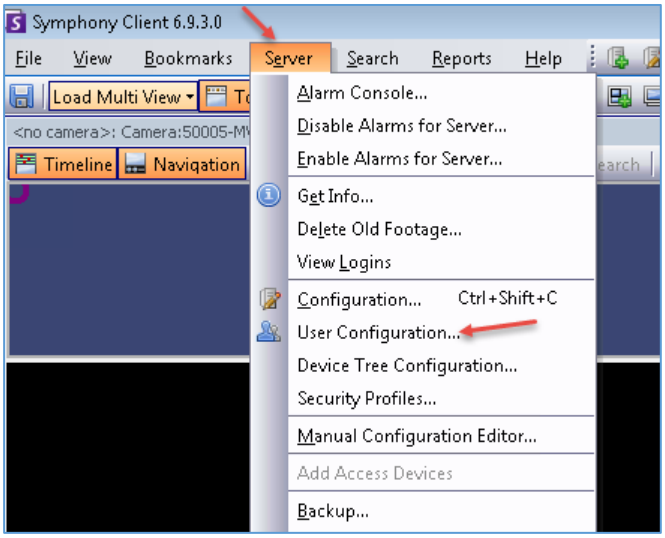
در تب Server Configuration و در قسمت Data Path باید یک آدرس برای ذخیره‌سازی تصاویر دوربین و داده‌های نرم-افزار وارد کنید، سعی کنید بسته به تعداد دوربین از حجم بالایی برخوردار باشد تا در موقع ذخیره‌سازی با کمبود فضا مواجه نشوید؛ بر روی Verify کلیک کنید تا اطّلاعات تأیید شود، بعد از این کار بر روی apply کلیک کنید.



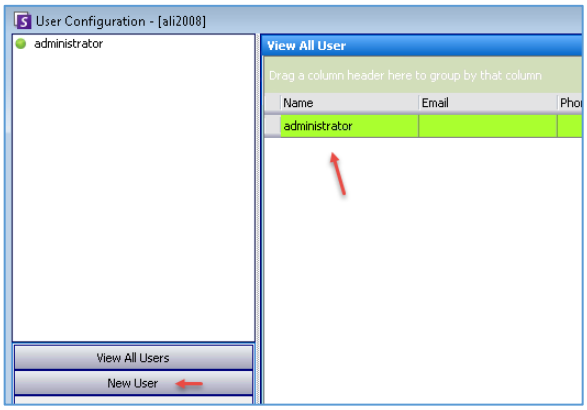
بعد از اینکه بر روی Apply کلیک کردید، اطّلاعات سرور به طور کلّی بررسی و به صورت شکل روبرو تأیید می‌شود، بر روی OK کلیک کنید تا نرم افزار اجرا شود.



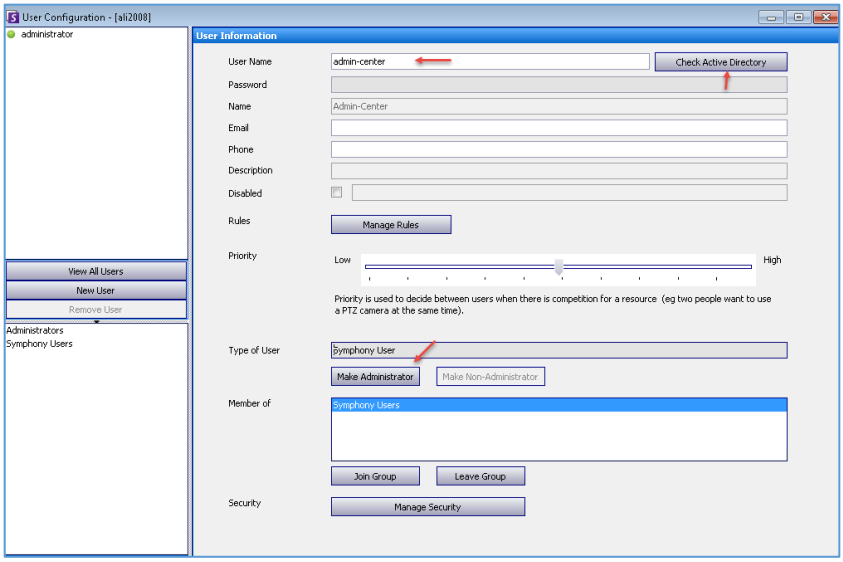
همانطور که در شکل روبرو مشاهده می‌کنید، نرم‌افزار به صورت کامل اجرا شده است که در ادامه باید تنظیمات دیگر آن را انجام دهید.



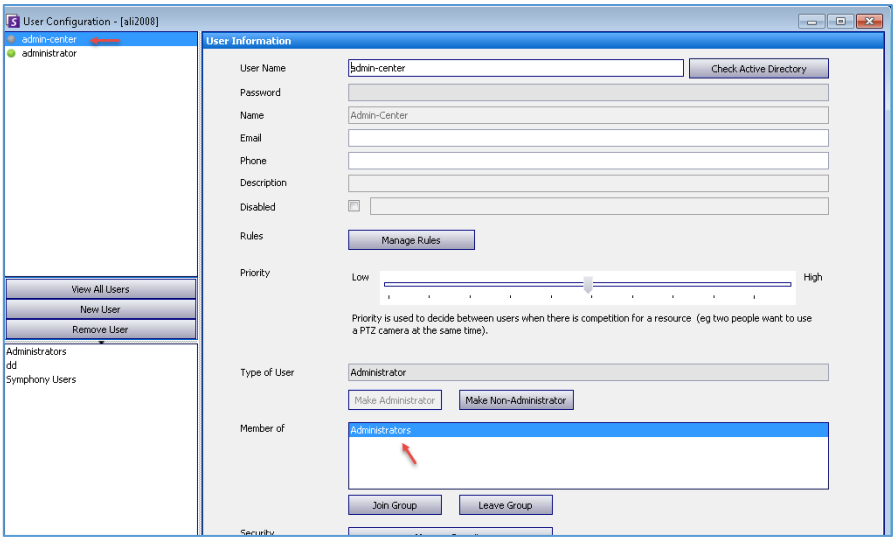
اوّلین کاری که انجام می‌دهید، بررسی کاربران در دسترسی به سرور دوربین‌ها است، برای این کار وارد منوی Server شوید و User Configuration را اجرا کنید.



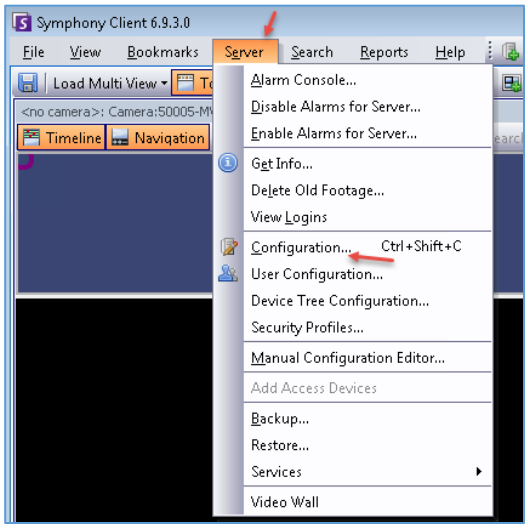
در این صفحه، کاربری که در هنگام تنظیمات در صفحات قبل وارد کردید را مشاهده می‌کنید که یک کاربر محلّی است و تنها در خود نرم‌افزار ایجاد شده است، به مانند شکل روبرو برای ایجاد کاربر جدید بر روی New User کلیک کنید.



در این صفحه، اگر بخواهید کاربر خود را از Active Directory انتخاب کنید باید به مانند شکل، نام آن را وارد و بر روی Check Active Directory کلیک کنید، اگر اسم را درست وارد کرده باشید، نام آن در قسمت Name وارد می‌شود، به صورت پیش‌فرض کاربری که ایجاد می‌کنید، دسترسی کامل به تمام تنظیمات سرور ندارد و در گروه Symphony User قرار می‌گیرد، برای اینکه در گروه مدیریّتی قرار دهید باید بر روی Make Administrator کلیک کنید.

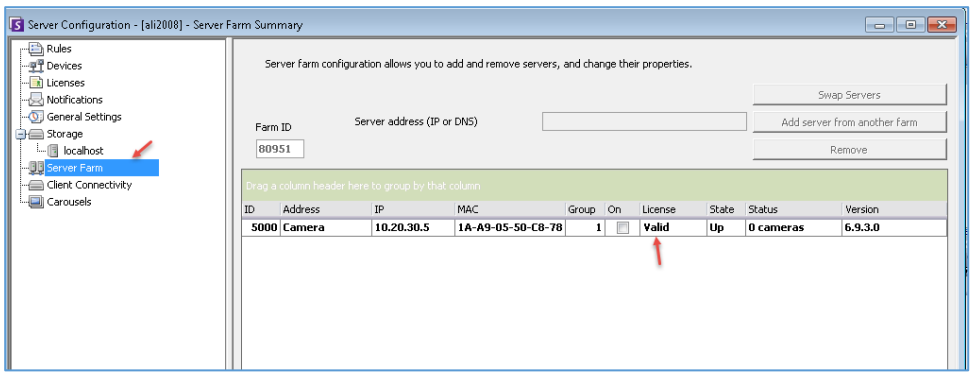


همانطور که مشاهده می‌کنید، کاربر Admin-user به لیست اضافه شده و در گروه Administrator قرار گرفته است، با این کار، کاربر مورد نظر به کلّ اطّلاعات سرور دسترسی خواهد داشت.

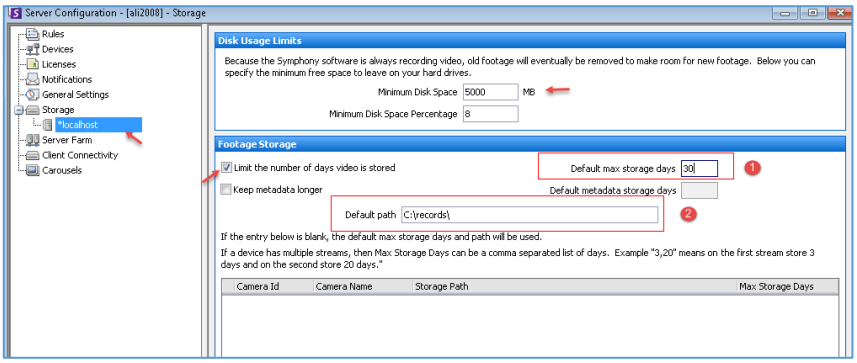


در مرحله‌ی بعد، تنظیمات اصلی نرم‌افزار را بررسی کنید، برای شروع کار، یک دوربین را به نرم‌افزار اضافه کنید.

وارد منوی Server شوید و بر روی Configuration کلیک کنید.

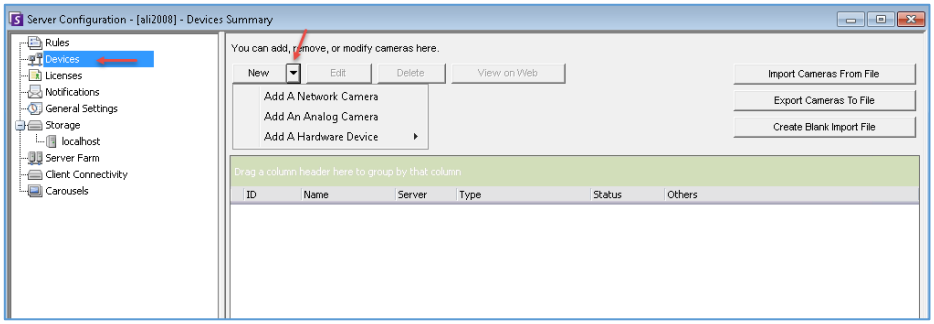


در این صفحه برای بررسی لایسنس و اطّلاعات نرم‌افزار وارد قسمت Server Farm شوید، در این صفحه، آدرس سرور به همراه آدرس Mac آن مشخّص شده است و در قسمت License، کلمه‌ی Valid یا همان تأیید وارد شده است که نشان می‌دهد این لایسنس مورد تأیید نرم‌افزار است، در قسمت Status نیز تعداد دوربین‌های فعّال وارد شده است که فعلاً دوربینی را برای این منظور فعّال نکردیم.



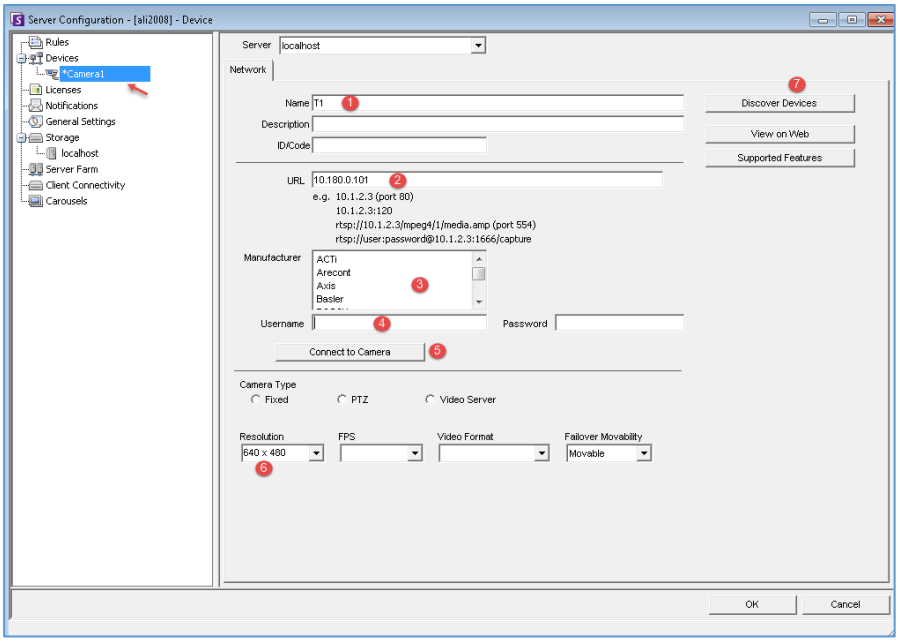
در قسمت بعد وارد Storage شوید، در این قسمت که مربوط به ذخیره-سازی داده‌های نرم‌افزار است در قسمت Minimum Disk Space می‌توانید مشخّص کنید که حداقل فضای ذخیره‌سازی چقدر باشد، برای شروع کار، اگر ظرفیّت دیسک شما محدود باشد، برای اینکه داده‌های دوربین‌ها در فواصل منظّم، مثلاً یک ماه ذخیره و بعد از آن پاک شود باید تیک گزینه‌ی Limit the number of daye video is stored را انتخاب کنید و در قسمت شماره‌ی یک، حداکثر تعداد روز ذخیره‌سازی اطّلاعات را وارد کنید که در اینجا ۳۰ روز وارد شده است، بنده در شرکت خود از ۱۲ دوربین استفاده کردم که با کیفیّت متوسط در ۳۰ روز، حداکثر یک و نیم ترابایت فضا مصرف می‌کنند.

در قسمت شماره‌ی دو باید محلّ ذخیره‌سازی را مشخّص کنید که قبلاً این کار را انجام دادیم، تنها باید محلّ ذخیره‌سازی، فضای کافی برای ذخیره‌ی تصاویر دوربین داشته باشد.

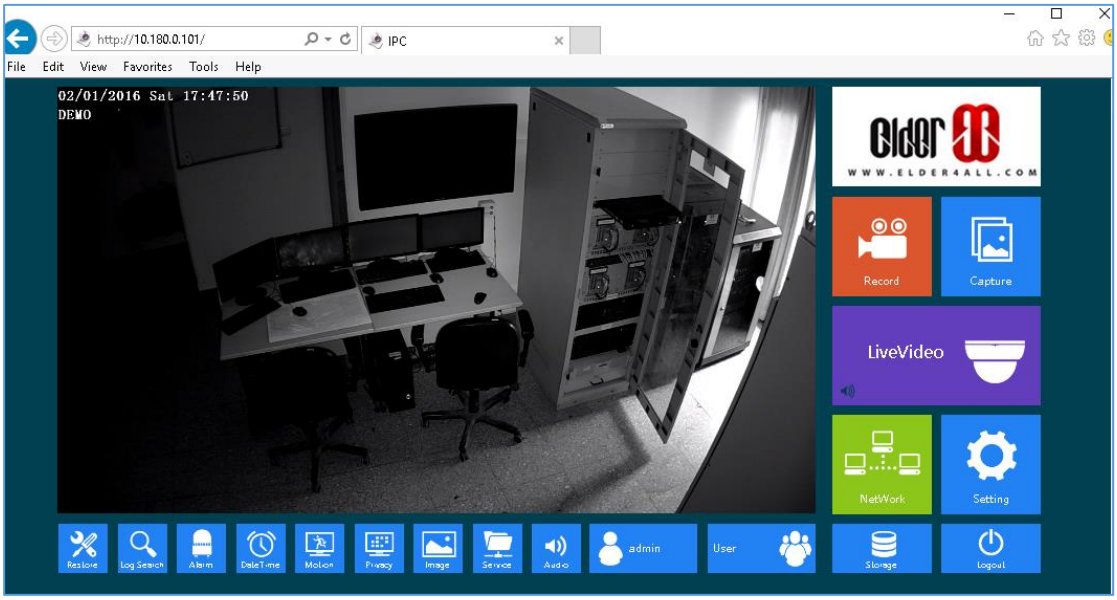


در قسمت Device شما می‌توانید دوربین‌های شبکه‌ی خود را اضافه کنید و لیست آنها را مشاهده کنید، برای اضافه کردن دوربین بر روی فلش کنار New کلیک کنید که سه گزینه برای شما ظاهر خواهد شد که اگر دوربین شما از نوع دیجیتال باشد باید گزینه‌ی اوّل و اگر آنالوگ باشد، گزینه‌ی دوّم و در نهایت، اگر دستگاه خاصّی باشد باید گزینه‌ی سوّم را انتخاب کنید، برای شروع کار، گزینه‌ی اوّل، یعنی Add A Network Camera را انتخاب کنید.

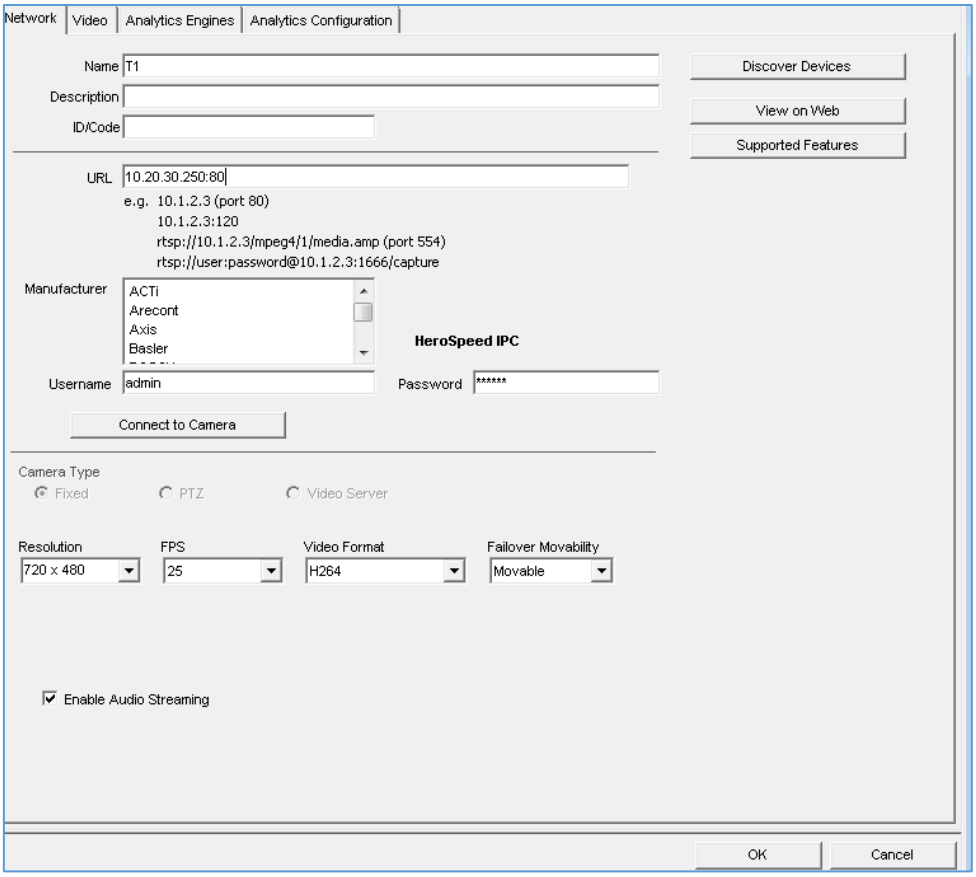
در مورد دوربین‌های دیجیتال و آنالوگ در صفحات قبل توضیح دادیم، برای بررسی بیشتر باید به آن بخش مراجعه کنید.



در این صفحه و در قسمت شماره‌ی یک باید نام دوربین خود را بنا به موقعیّت آن وارد کنید، در قسمت شماره‌ی دو باید آدرس IP دوربین را به همراه پورت دسترسی آن وارد کنید، در قسمت شماره‌ی سه باید کارخانه‌ی سازنده را مشخّص کنید و در قسمت شماره‌ی چهار باید نام کاربری و رمز عبور مربوط به دوربین را وارد کنید و اگر اطّلاعات شما درست وارد شده باشد با کلیک بر روی شماره‌ی پنج، یعنی Connect to Camera، نرم‌افزار به دوربین متّصل خواهد شد و بعد از متّصل شدن در قسمت شماره‌ی شش، کیفیّت دوربین مشخّص می‌شود که شما می‌توانید آن را تغییر دهید.

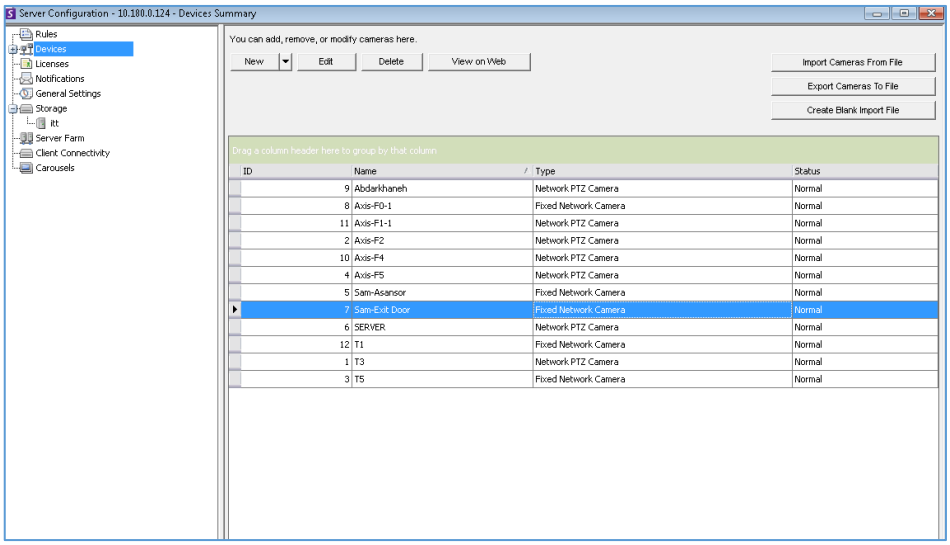


برای مثال، یک دوربین دیجیتال آماده کردیم و IP آن را 10.20.30.250 در نظر گرفتیم که تصویر آن را در شکل روبرو مشاهده می‌کنید، در این شکل به کنترل پنل دوربین متّصل شدیم که هر دوربین، تنظیمات مختص به خود را دارد، برای اینکه این دوربین را به لیست نرم‌افزار خود اضافه کنیم باید به این صورت عمل کنیم.



در این صفحه، اطّلاعات دوربین را وارد می‌کنیم و در قسمت Manufacturer باید نام سازنده‌ی دوربین را انتخاب کنیم که اگر وجود نداشت می‌توانیم یک نام به دلخواه خود انتخاب کنیم، در قسمت username و Password، نام کاربری و رمز عبور را وارد می‌کنیم، برای تست ارتباط بر روی Connect to camera کلیک می‌کنیم.

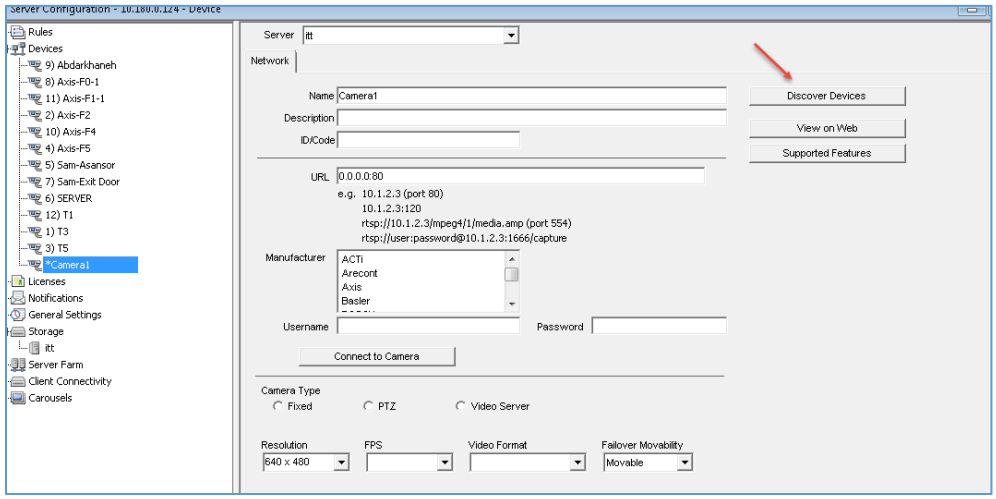
اگر در قسمت پایین صفحه، می‌خواهید تصاویر ضبط شده به همراه صدا باشد، تیک گزینه‌ی Enable Audio Streaming را انتخاب کنید، در قسمت Resolution نیز می‌توانید کیفیّت ذخیره‌سازی تصویر دوربین را مشخّص کنید؛ بر روی OK کلیک کنید تا دوربین مورد نظر به لیست اضافه شود.



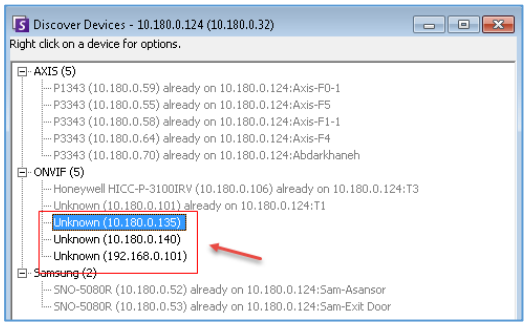
همانطور که در شکل روبرو مشاهده می‌کنید، دوربین‌های مختلفی را به لیست اضافه کردیم که در کل، ۱۲ دوربین از نقاط مختلف یک سازمان است.

پیدا کردن دوربین به صورت Discovery:

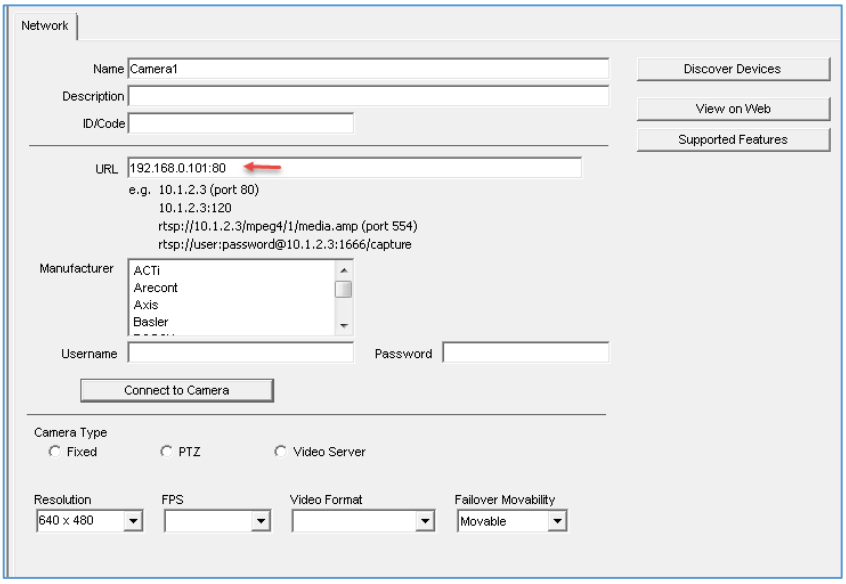
زمانی پیش می‌آید که شما دوربین را به شبکه متّصل کردید و دوربین از طریق سرویس DHCP، یک آدرس دریافت کرده است که شما نیز آدرس آن دوربین را نمی‌دانید، برای پیدا کردن دوربین در شبکه بهتر است از سرویس Discovery استفاده کنید.



به مانند شکل روبرو بر روی Discover Devices کلیک کنید.



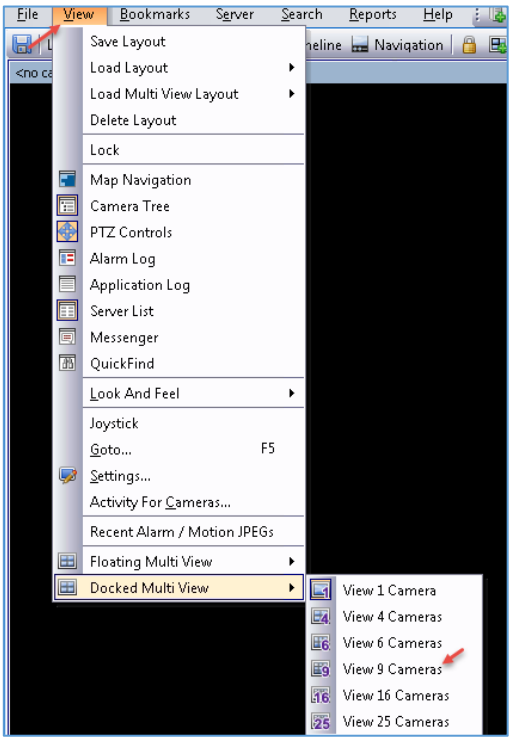
با این کار، به مانند شکل روبرو دوربین‌هایی که در شبکه وجود دارند و آدرس دریافت کرده‌اند و هنوز قابل شناسایی نیستند، لیست می‌شوند؛ باید بر روی تک تک آنها که با Unknown شروع می‌شوند، دوبار کلیک کنید و رمز مربوط به دوربین را به مانند قبل وارد کنید.



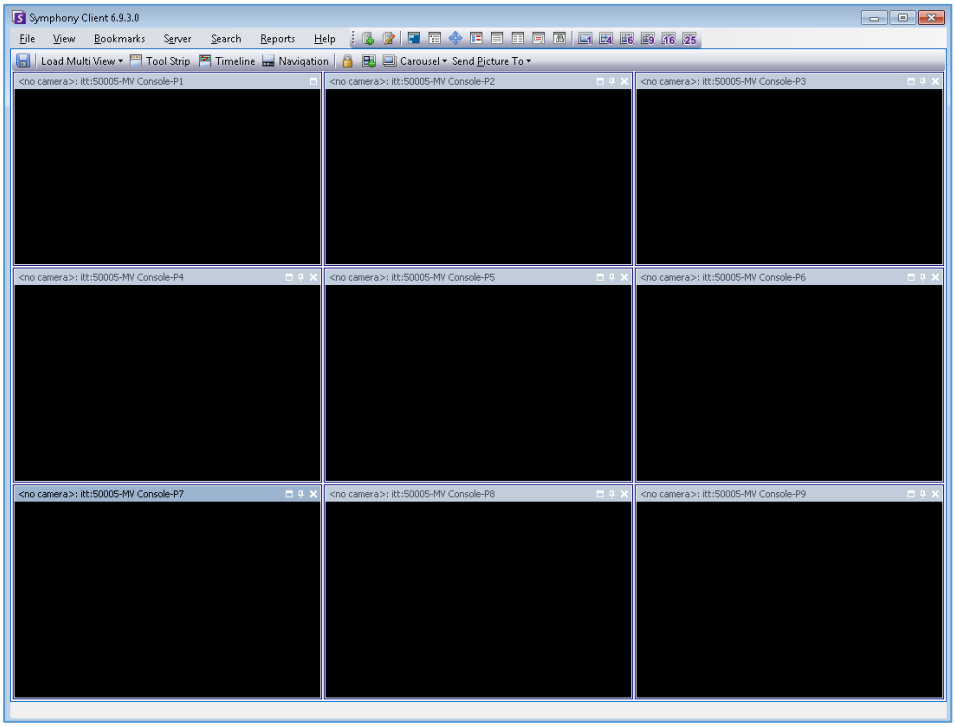
در شکل روبرو آدرس IP که در شکل بالا پیدا شد، با دو بار کلیک کردن به لیست روبرو اضافه شده است که شما باید نام کاربری و رمز عبور مربوط به دوربین مورد نظر را وارد کنید و تست بگیرید، در بعضی مواقع نیز این آدرس‌ها مختصّ دوربین نیستند و شاید مختصّ دستگاه دیگری باشند که قابل استفاده نخواهد بود.

تنظیم نمایش دوربین‌ها:

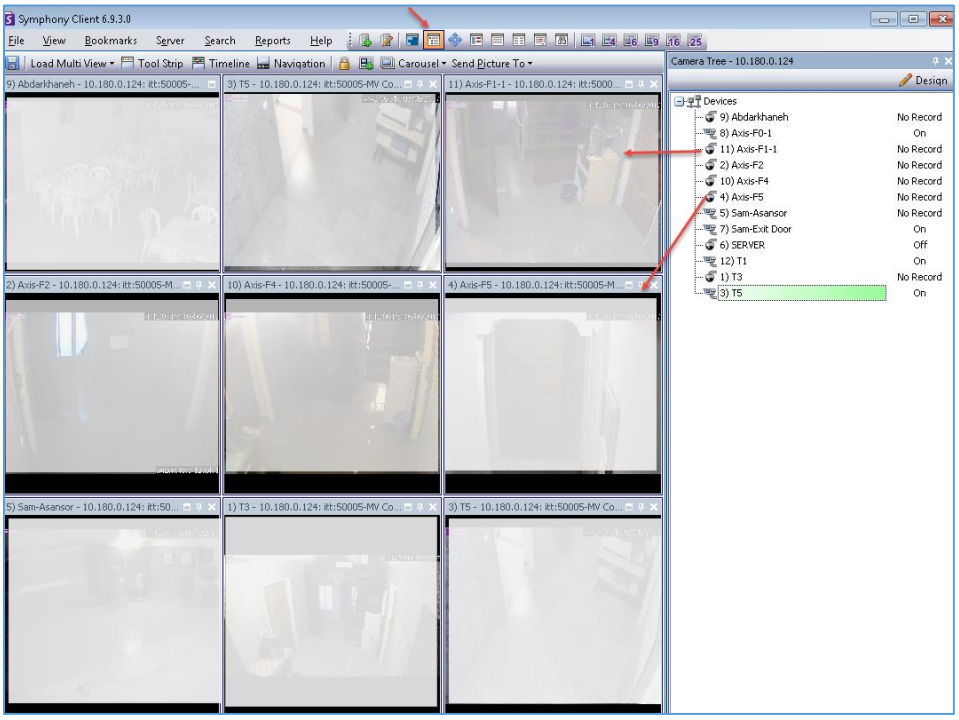
اگر در سازمان خود از چندین دوربین استفاده می‌کنید، برای اینکه تصاویر همه‌ی آنها را به صورت آنلاین بر روی صفحه‌ی نمایش داشته باشید باید صفحه را به بخش‌های چندتایی تقسیم کنید تا دوربین‌ها در آنها قرار بگیرند؛ در این قسمت، این کار را انجام می‌دهیم.



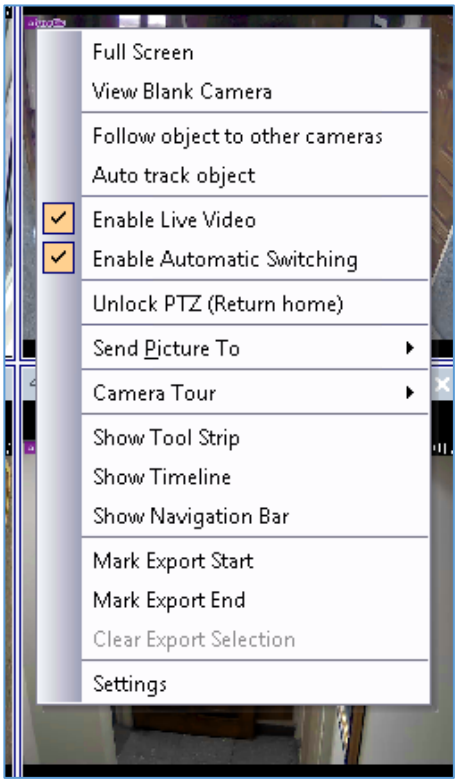
برای شروع وارد منوی View شوید و در آخر منو، دو گزینه‌ی Floating و Docked وجود دارد که اگر بخواهید تصاویر دوربین در یک پنجره‌ی جدا از دوربین نمایش داده شود باید از گزینه‌ی Floating استفاده کنید و اگر بخواهید تصاویر دوربین‌ها را در دل نرم‌افزار مشاهده کنید باید گزینه‌ی Docked را انتخاب کنید که در این قسمت شما باید از قسمت Docked، گزینه‌ی مورد نظر خود را بنا به تعداد دوربین‌های خود انتخاب کنید.



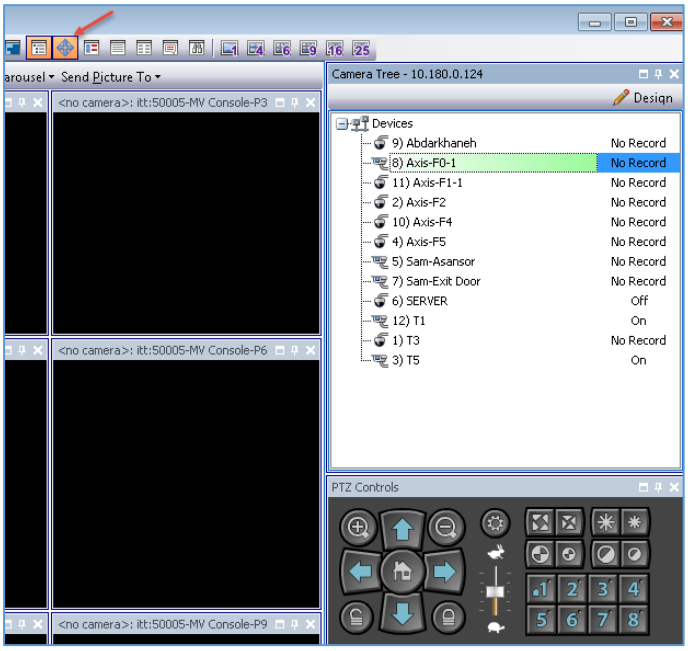
۹ قسمت برای دوربین مشخّص شده است که در شکل روبرو مشاهده می‌کنید، برای اینکه دوربین‌های خود را به هر یک از قسمت‌ها اضافه کنید باید ابزار Camera Tree را فعّال کنید که در ادامه این کار را انجام خواهیم داد.



به مانند شکل روبرو در نوار ابزار بالایی بر روی Camera Tree کلیک کنید و یا از منوی View، این کار را انجام دهید تا پنجره‌ی مربوط به آن در سمت راست نرم‌افزار ظاهر شود، همانطور که مشاهده می‌کنید، لیستی از دوربین‌ها در آن قرار دارد که برای اینکه از تصاویر این دوربین‌ها استفاده کنید می‌توانید دوربین مورد نظر را انتخاب و با نگه داشتن و حرکت دادن آن در یکی از قسمت‌ها از تصاویر آن استفاده کنید، در شکل بالا تصاویر غیر واضح است که دلیل آن به علّت مسائل امنیّتی سازمان است.

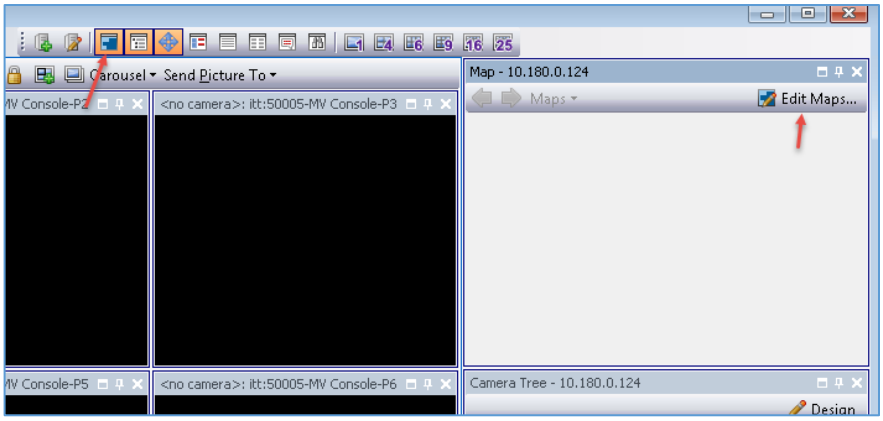


اگر در صفحه بر روی هر یک از دوربین‌ها کلیک راست کنید، گزینه‌های مختلفی را مشاهده خواهید کرد، برای اینکه تصویر دوربین را تمام‌صفحه کنید باید بر روی گزینه‌ی Full Screen کلیک کنید، گزینه‌ی View Blank Camera برای حذف دوربین از پنجره‌ی مورد نظر است، گزینه‌های دیگری نیز وجود دارد که در ادامه به آنها خواهیم پرداخت.

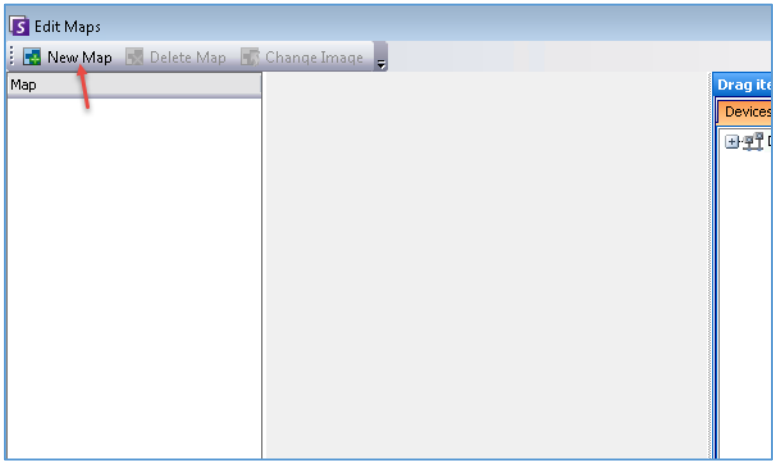


ابزار دیگری با عنوان PTZ Controls وجود دارد که می‌توانید با استفاده از آن، تصاویر دوربین را بزرگ‌نمایی، کوچک‌نمایی، حرکت به چهار طرف در صورت امکان دوربین، کم و زیاد کردن رنگ صفحه و... را با آن انجام دهید.

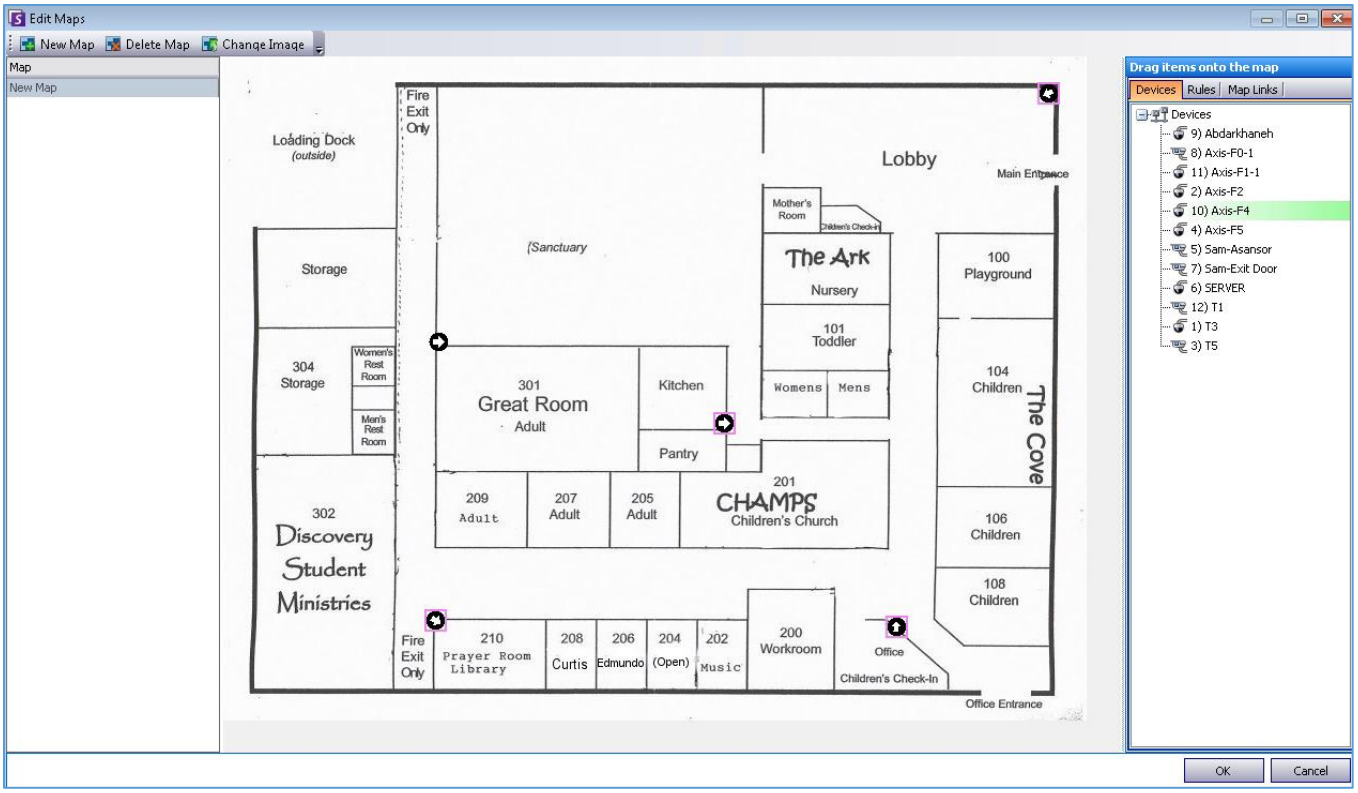
برای دسترسی به این ابزار به مانند شکل روبرو بر روی آیکون PTZ Controls کلیک کنید و یا این گزینه را از منوی View انتخاب کنید.



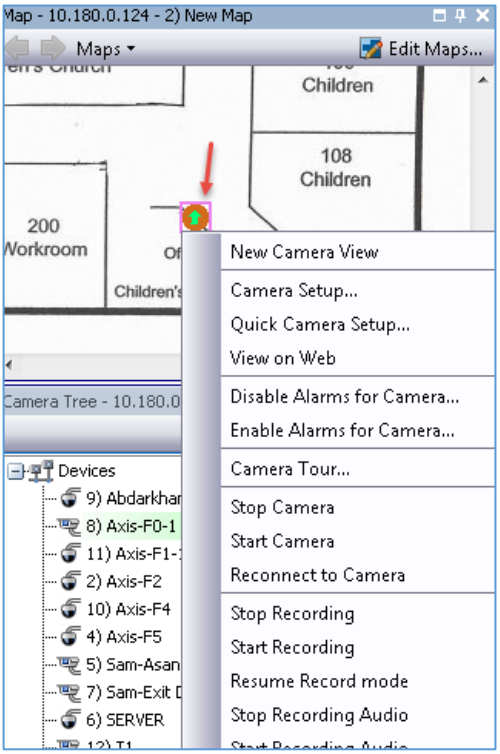
ابزار دیگری با عنوان Map navigation وجود دارد که با استفاده از آن می‌توانید یک عکس که شامل نقشه‌ی قرارگیری دوربین‌ها است را به لیست اضافه کنید و دوربین‌ها را در جای مشخّص شده‌ی آن قرار دهید، برای انجام این کار، طبق شکل بر روی آیکون MAP کلیک کنید و در پنجره‌ی باز شده، گزینه‌ی Edit Maps را انتخاب کنید.



در این صفحه باید نقشه‌ای که از قبل آماده کردید را به صفحه اضافه کنید که برای این کار باید بر روی New Map کلیک کنید.



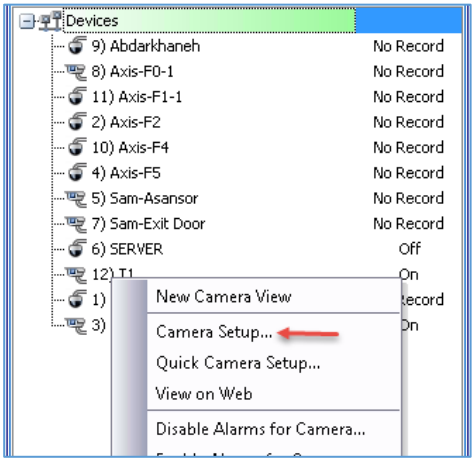
در شکل بالا، یک تصویر از یک ساختمان به نرم‌افزار داده شده است و شما باید طبق جایگاه دوربین، آنها را یکی یکی از لیست، انتخاب و در محلّ مناسب آن قرار دهید، بعد از اتمام کار بر روی OK کلیک کنید.



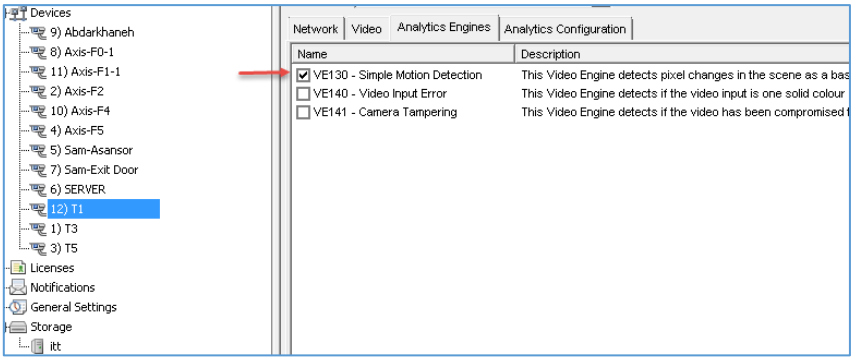
در این قسمت، نقشه به صفحه اضافه شده است و دوربین مورد نظر به رنگ سبز، یعنی آنلاین تغییر شکل داده است و با کلیک راست بر روی آن می‌توانید به تنظیمات آن دست پیدا کنید.

فعّال کردن قابلیّت تشخیص حرکت یا Motion:

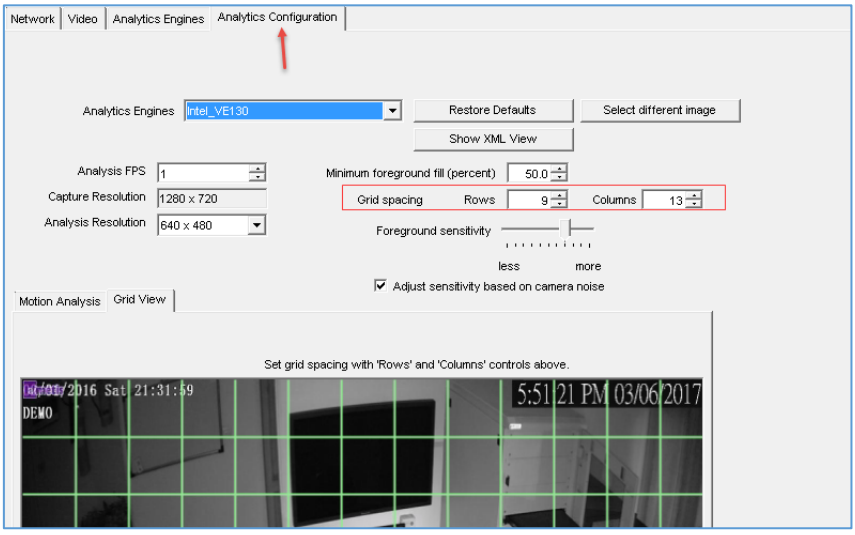
این ابزار، یک سرویس بسیار سودمند برای صرفه‌جویی در هارد دیسک است، اگر این ابزار را فعّال نکنید، نرم‌افزار در طول فعّال بودن دوربین، تمام تصاویر را ذخیره می‌کند و این باعث می‌شود فضای هارد دیسک شما بسیار سریع پر شود، برای حلّ این مشکل باید از فنّاوری تشخیص حرکت یا Motion استفاده کنید، با این کار تنها زمانی تصاویر ذخیره خواهد شد که در دوربین حرکتی دیده شود.



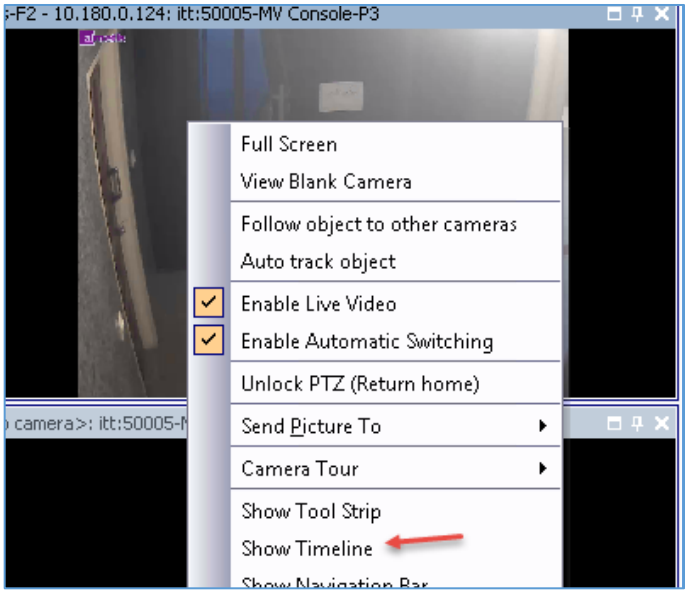
بر روی یکی از دوربین‌ها کلیک راست کنید و گزینه‌ی Camera Setup را انتخاب کنید.



در این قسمت وارد تب Analytics Engines شوید و گزینه‌ی اوّل، یعنی Simple Motion Detection را انتخاب کنید.



در تب Analytices Engines می‌توانید پیکسل صفحه را مشخّص کنید تا این قابلیّت بر روی حرکت حسّاس‌تر شود که این کار با تغییر Size در قسمت Grid امکان‌پذیر است؛ بر روی OK کلیک کنید.



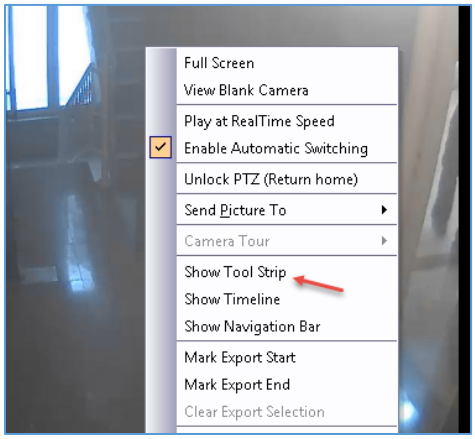
در ادامه برای بررسی بیشتر این قابلیّت باید نحوه‌ی ذخیره‌سازی تصویر را در دوربین مورد نظر تست کنید، بر روی دوربین مورد نظر کلیک راست کنید و گزینه‌ی Show TimeLine را انتخاب کنید.



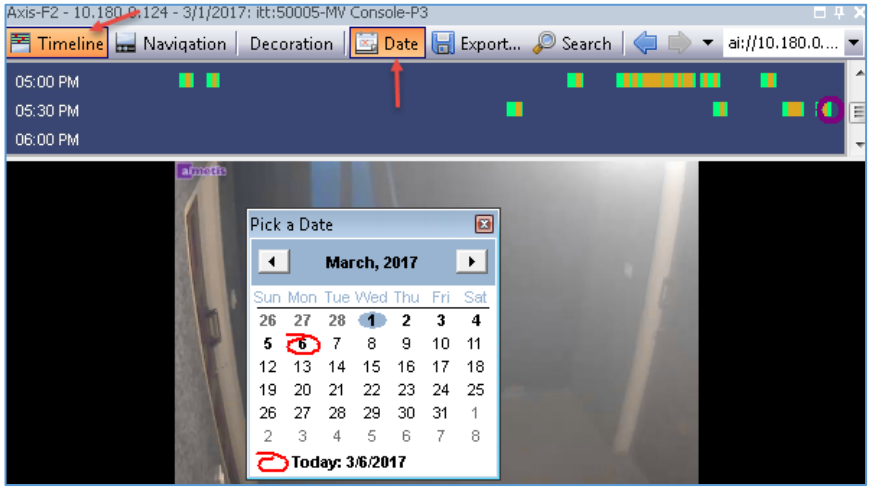
یک نوار TimeLine در بالای دوربین در شکل روبرو، اضافه و در کنار آن، ساعت آن را در همان روز مشخّص کردیم، یک-سری علامت سبز و زرد در شکل وجود دارد که همان حرکت فرد است که با استفاده از فنّاوری Motion انجام دادیم، در تصویر روبرو بر روی یکی از این علامت‌های سبز و زرد کلیک می‌کنیم که فرد را در تصویر برای شما نشان می‌دهد؛ رنگ سبز، شروع به کار Motion است و رنگ زرد، خود فرد مورد نظر در حال حرکت است، این فنّاوری کمک به‌سزایی در هزینه‌ها می‌کند، البتّه بعضی از همکاران دوست دارند در طول کار همه‌ی تصاویر را داشته باشند که برای این کار باید از هارد دیسک‌های بیشتری با فضای ذخیره‌سازی بالایی استفاده کنند تا بتواند این حجم از تصاویر را در خود جای دهد.

استخراج تصاویر دوربین:

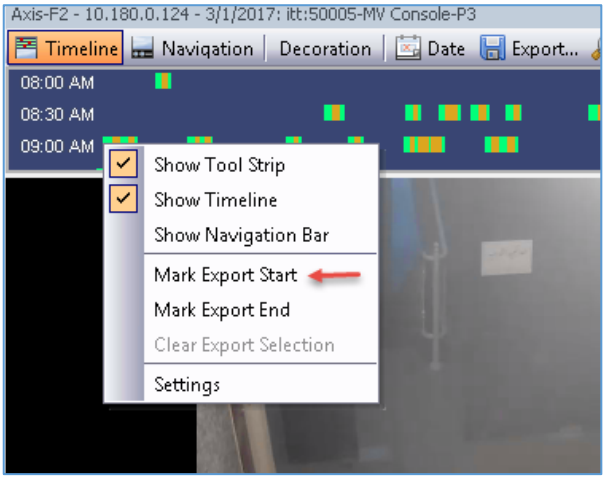
وقتی تصاویر دوربین در محلّ مشخّص‌شده ذخیره می‌شوند، نمی توانید به صورت مستقیم به تصاویر آن دست پیدا کنید، باید در خود نرم‌افزار، ساعت و تاریخ را مشخّص کنید و تصاویر را از دوربین مشخّص‌شده استخراج کنید.



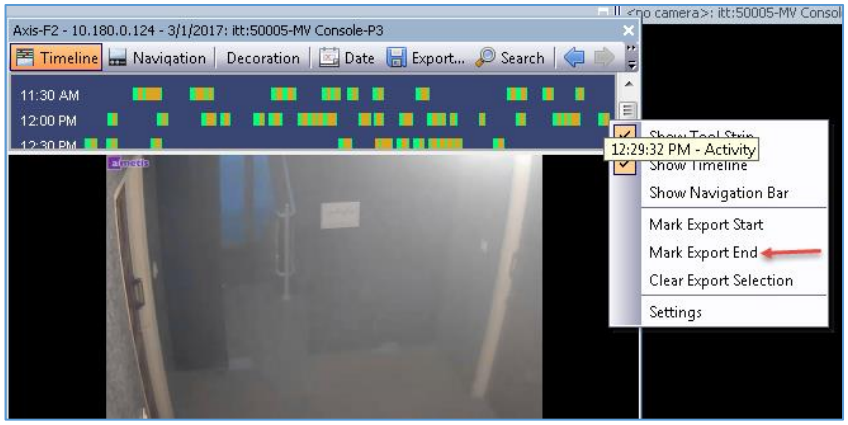
برای انجام این کار بر روی دوربین مورد نظر کلیک راست و گزینه‌ی Show Tool Strip را انتخاب کنید.



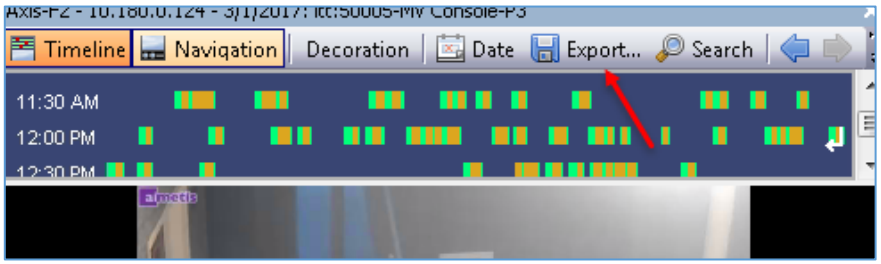
همانطور که مشاهده می‌کنید، یک نوار در بالای دوربین اضافه شده است، برای اینکه ساعت دوربین را داشته باشید بر روی Timeline کلیک کنید و برای مشخّص کردن تاریخ دوربین باید بر روی Data کلیک کنید و تاریخ مورد نظر را انتخاب کنید.



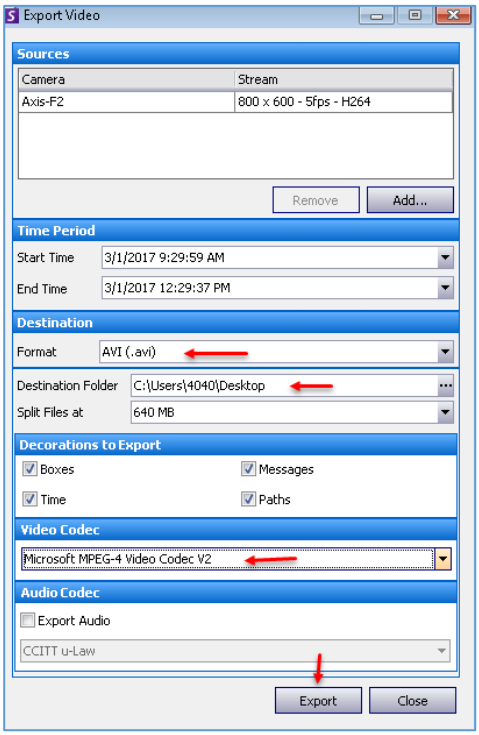
بر فرض می‌خواهید تصاویر ساعت ۹ صبح تا ۱۲ ظهر را در محلّ خاصّی ذخیره کنید، یا به فرد خاصّی بدهید، برای این کار طبق شکل روبرو بر روی ساعت مشخّص‌شده کلیک راست کنید و گزینه‌ی Mark Export Start را انتخاب کنید.



در ادامه بر روی ساعت ۱۲ ظهر کلیک راست کنید و گزینه‌ی Mark Export End را انتخاب کنید، با این کار ساعت استخراج تصاویر مشخّص می‌شود.



بعد از انجام کار بالا بر روی آیکون Export کلیک کنید تا صفحه‌ی بعد ظاهر شود.



در این صفحه باید نوع فایل ویدئویی خود را مشخّص کنید که بهترین انتخاب، پسوند AVI است و بعد، در قسمت Destination Folder باید محلّ ذخیره‌سازی آن را مشخّص کنید و در قسمت Video Codec می‌توانید کیفیّت تصویر را تغییر دهید، بعد از انجام این کارها بر روی Export کلیک کنید تا فیلم در ساعت مشخّص‌شده و در مسیری که انتخاب کردید، ذخیره شود.

اگر در نصب و راه‌اندازی این سرور با مشکلی مواجه شدید، می توانید با بنده در تماس باشید.

برای دانلود این نرم‌افزار که به صورت سروری و کلاینتی است از لینک زیر استفاده کنید:

https://www.aimetis.com/xnet/AccountCreate.aspx?m=Trial

این نرم‌افزار دارای لایسنس ۳۰ روزه است که بعد از اتمام باید لایسنس آن را خریداری کنید، اگر نیاز به نرم‌افزار با لایسنس بی‌نهایت داشتید، می‌توانید با بنده در تماس باشید.

نصب و راه‌اندازی System Center 2016:

مجموعه نرم‌افزارهای System Center برای مدیریّت کامل شبکه توسط مایکروسافت ایجاد شده‌اند که دارای ٦ زیرمجموعه با نام‌های زیر است:

١- Microsoft.System.Center.Configuration.Manager:

مجموعه ابزارهای مدیریّتی برای مدیریّت هر چه بهتر بر روی منابع سخت‌افزاری و نرم‌افزاری است، با این نرم-افزار می‌توانید آخرین آپدیت‌های امنیّتی را بر روی شبکه‌ی خود اعمال کنید، از دیگر امکانات این نرم‌افزار، گزارش‌گیری کامل از تمام اطّلاعات شبکه است که این کار برای مدیر شبکه بسیار کارآمد خواهد بود.

٢- Microsoft.System.Center.Data.Protection.Manager:

یک سازمان نیاز به این دارد که اطّلاعات آن همیشه در دسترس باشد و اگر مشکلی برای اطّلاعات در شبکه ایجاد شده است، توانایی برگشت آن وجود داشته باشد که این کار نیاز به یک سیستم و برنامه‌ی خاص است که Data.Protection، توانایی این کار را دارد که به شما این امکان را دهد تا به صورت امن از اطّلاعات کلّ شبکه‌ی خود، یک نسخه‌ی پشتیبان تهیّه کنید و در موقع نیاز از آن استفاده کنید.

Data.Protection.Manager یا DPM دارای چهار ویژگی است که در زیر آنها را مشاهده می‌کنید.

- ✓ Application-aware backup

  برای انجام پشتیبان‌گیری از نرم‌افزارها و سرویس‌ها، مانند SQL، Exchange، Sharepoint و... کاربرد دارد.

- ✓ File backup

  برای پشتیبان‌گیری از فایل‌ها، پوشه‌ها و درایوها در ویندوز سرور و ویندوز کلاینت کاربرد دارد.

- ✓ System backup

  پشتیبان‌گیری از کلّ اطّلاعات یک سیستم و انتقال آن به هارد دیگر و....

- ✓ Hyper-V backup

  پشتیبان‌گیری از ماشین مجازی ویندوز و لینوکس که بر روی سرویس Hyper-V ایجاد شده است.

این اطّلاعات پشتیبان می‌توانند بر روی هارد دیسک، Microsoft Azure و برای ذخیره‌سازی طولانی مدّت بر روی Tape، ذخیره شوند.

۳- Microsoft.System.Center.Operations.Manager:

یک نرم‌افزار متمرکز و خوب برای مانیتور کردن و مدیریّت بر کلّ دستگاه‌های شبکه است که با استفاده از مانیتورینگ، این امکان را به شما می‌دهد تا با آن بر کلّ سیستم‌های شبکه اشراف داشته باشید و در صورت خرابی یکی از سیستم‌ها از آن مطّلع شوید، امکانات دیگری نیز در این نرم‌افزار وجود دارد تا با استفاده از Policy خاص، دستوراتی را به سیستم‌ها بدهید تا طبق قانون شما رفتار کنند.

٤- Microsoft.System.Center.Orchestrator:

این نرم‌افزار یک سیستم ایجاد گردش کار یا همان، WorkFlow است که این امکان را به مدیر شبکه می‌دهد که با ایجاد یک جریان کاری به صورت اتوماتیک بر روی شبکه، توانایی ایجاد منابع، مانیتور کردن و... را داشته باشد.

٥- Microsoft.System.Center.Service.Manager:

این برنامه جهت رفع مشکل، رخداد، کنترل تغییرات و مدیریّت چرخه‌ی عمر دارایی‌ها در شبکه‌ی سازمان طرّاحی شده است، این نرم‌افزار به کاربران از طریق یک پایگاه دانش کمک می‌کند که راحت‌تر بتوانند کارهای خود را به انجام برسانند که از طریق پلتفرم منحصر به فرد خود، توانایی یکپارچه‌سازی و هماهنگ نمودن دانش، فرآیندها و فعّالیّت‌ها را در کلّ مجموعه‌ی Microsoft System Center ایجاد می‌نمایند که در نتیجه‌ی آن، هزینه‌ها کاهش می‌یابد، مدّت زمان بازیابی خطاها کم می‌شود و کیفیّت فعّالیّت‌های شبکه افزایش می‌یابد.

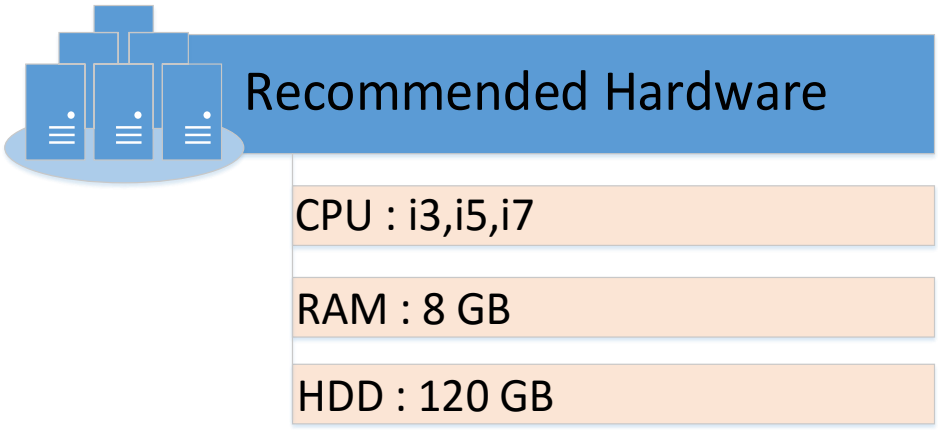
٦- Microsoft.System.Center.Virtual.Machine.Manager:

یک نرم‌افزار برای دیتاسنترها است که برای مدیریّت ماشین‌های مجازی کاربرد دارد و می‌توانید کارهای مختلفی، مانند پشتیبان‌گیری و... را بر روی آنها انجام دهید.

نصب و راه‌اندازی Microsoft.System.Center. Operations.Manager:



برای راه‌اندازی این نرم‌افزار در شبکه، نیاز به یک سرور با سخت‌افزار خوب داریم که در زیر، پیش‌نیازهای آن را بررسی می‌کنیم.



سخت‌افزاری که برای این سرویس در نظر گرفته شده است باید یک سیستم قدرتمند باشد تا بتواند به درستی نرم‌افزار را اجرا کند؛ پیشنهادی که در بالا ارائه شده است، می‌تواند یک پیشنهاد خوب باشد.

در ادامه با نصب این نرم‌افزار و کار با آن آشنا خواهیم شد.

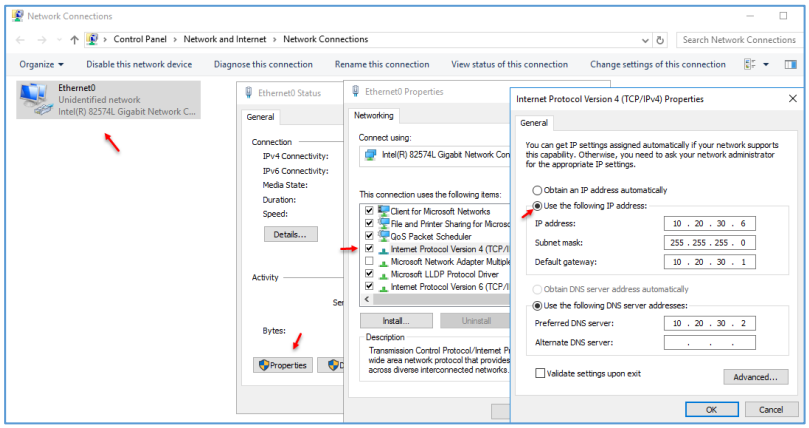
برای شروع کار می‌توانید مجموعه نرم‌افزارهای System Center 2016 را از لینک زیر دریافت کنید:

http://p30download.com/fa/entry/68149/

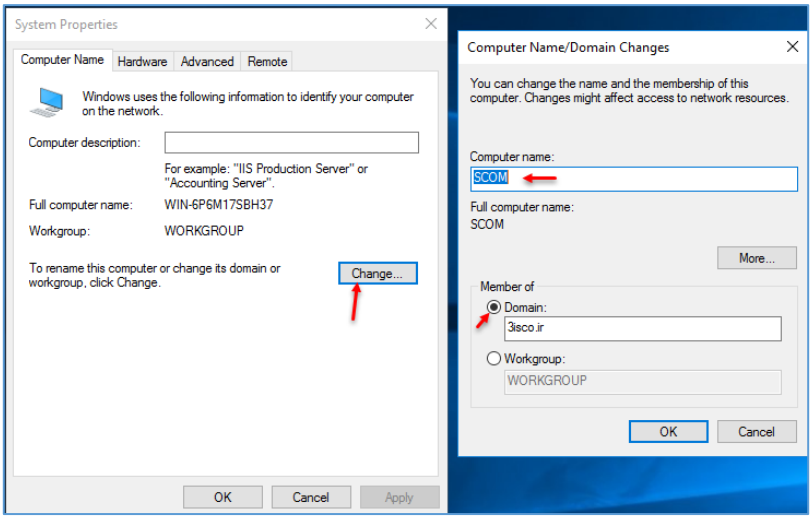
برای نصب این نرم‌افزار نیاز به پیش‌نیازهای نرم‌افزاری دارید که عبارتند از:

ویندوز سرور ۲۰۱۲ R2 و یا ویندوز سرور ۲۰۱۶ که در این کتاب از ویندوز سرور ۲۰۱۶ استفاده می‌کنیم. شما می‌توانید این سیستم را بر روی یک ماشین مجازی ایجاد کنید و یا اینکه آن را در یک سیستم واقعی پیاده‌سازی کنید که راه حلّ دوّم، اصولی‌تر خواهد بود.

ما در این کتاب، یک سیتسم واقعی با 16 گیگابایت رم در نظر گرفتیم که البتّه هر چقدر رم بیشتر باشد، عملکرد نرم‌افزار نیز بهتر خواهد بود.



بعد از نصب ویندوز بر روی سیستم جدید باید آدرس IP آن را مشخّص کنید، برای این سرور، آدرس IP را به صورت 10.20.30.6 در نظر بگیرید و به مانند شکل روبرو اطّلاعات را وارد کنید.

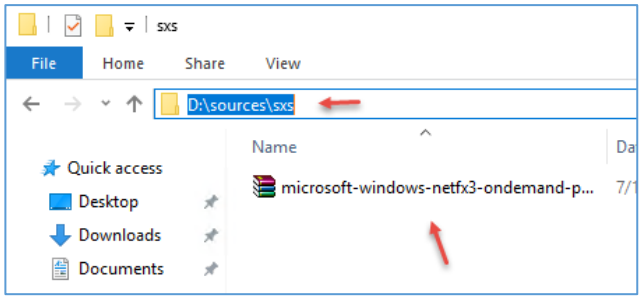


بعد از وارد کردن آدرس، نام سرور را به SCOM تغییر دهید و آن را عضو دومین 3isco.ir کنید که این عمل را در شکل روبرو مشاهده می‌کنید.

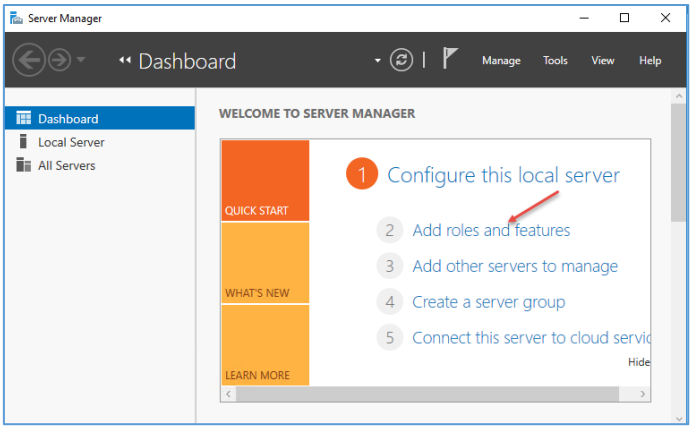
بعد از اینکه سیستم را عضو دومین و آن را Restart کردید باید یک‌سری پیش‌نیازها را قبل از نرم‌افزار Microsoft.System.Center. Operations.Manager نصب کنید تا این نرم‌افزار به خوبی بر روی سرور نصب شود.

نصب Net FramWork 3.5:

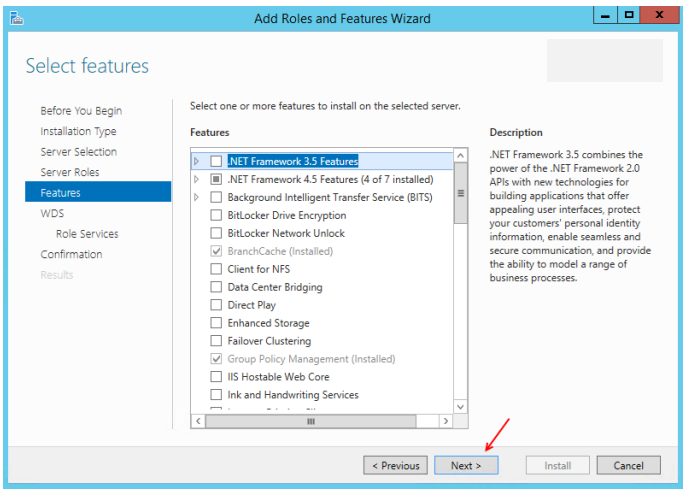
به صورت پیش‌فرض Net 3.5 بر روی ویندوز ۲۰۱۶ نصب نشده است و برای نصب آن، نیاز به DVD مربوط به آن دارید تا فایل Net 3.5 را دریافت کنید، برای این کار DVD را داخل دستگاه قرار دهید و وارد آدرس زیر شوید.



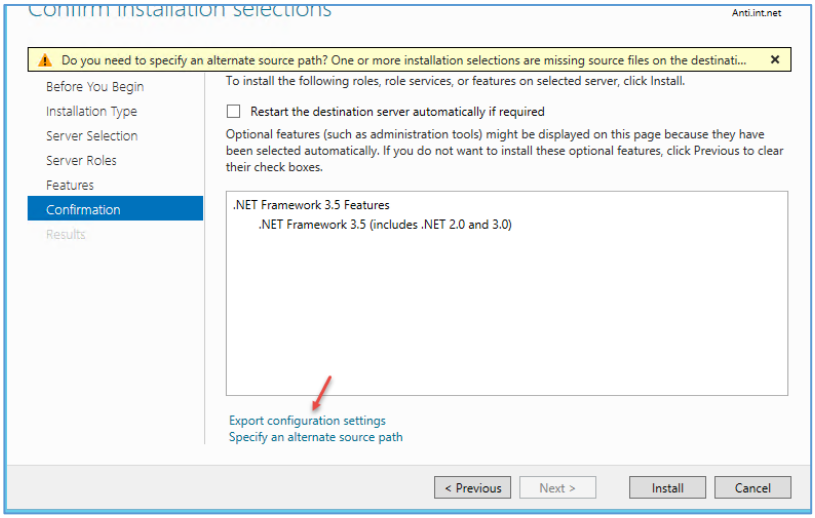
به مانند شکل، آدرس مورد نظر را کپی کنید تا در ادامه از آن استفاده کنید.



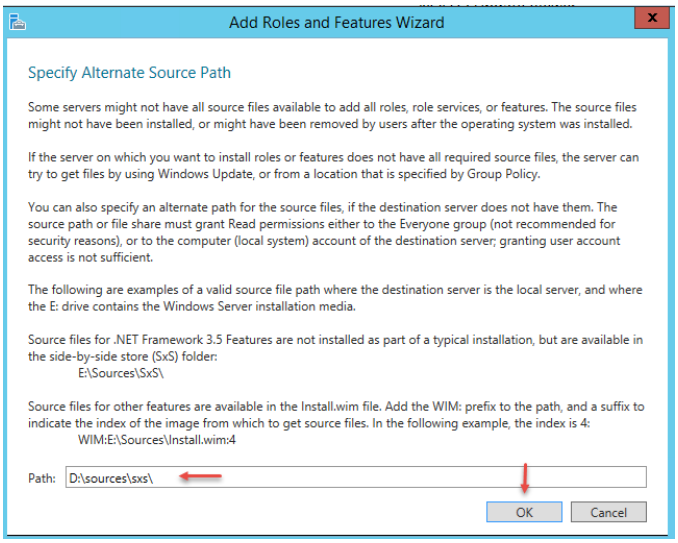
بعد از کپی کردن آدرس وارد Server Manager شوید و بر روی Add roles and Features کلیک کنید.



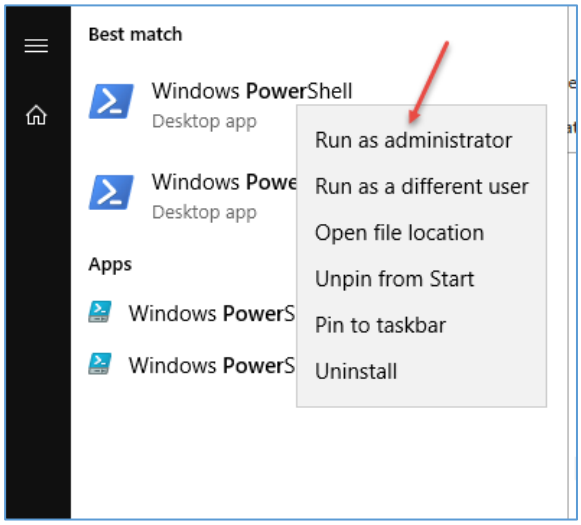
در صفحه‌ی Features، تیک گزینه‌ی .NET Framework 3.5 را انتخاب و بر روی Next کلیک کنید.



در این صفحه بر روی Export Configuration settings کلیک کنید.



در این قسمت، آدرس مورد نظر را که از قبل کپی کردید، وارد و بر روی OK کلیک کنید و در صفحه‌ی بعد بر روی Install کلیک کنید تا Net 3.5 بر روی سرور نصب شود.

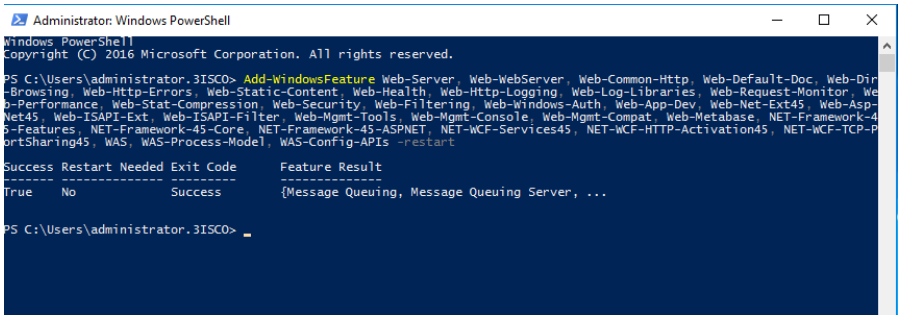


بعد از نصب Net3.5 باید یک‌سری سرویس‌ها را با استفاده از دستورات PowerShell نصب کنید، برای این کار باید سرویس Powershell را با کاربر Administrator اجرا کنید.

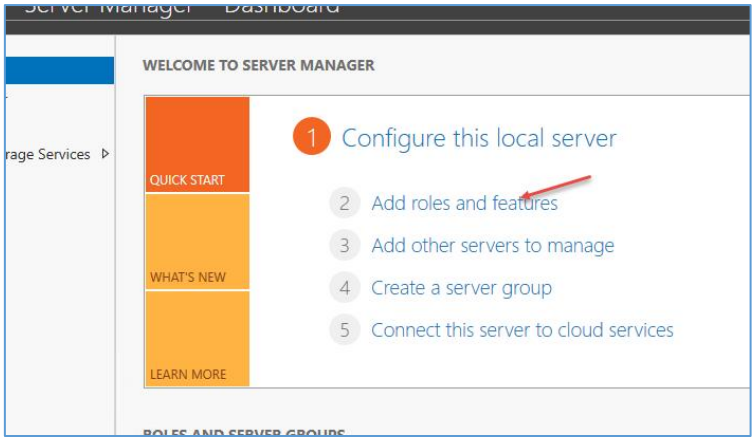
به مانند شکل روبرو عمل کنید.

دستور مورد نظر:

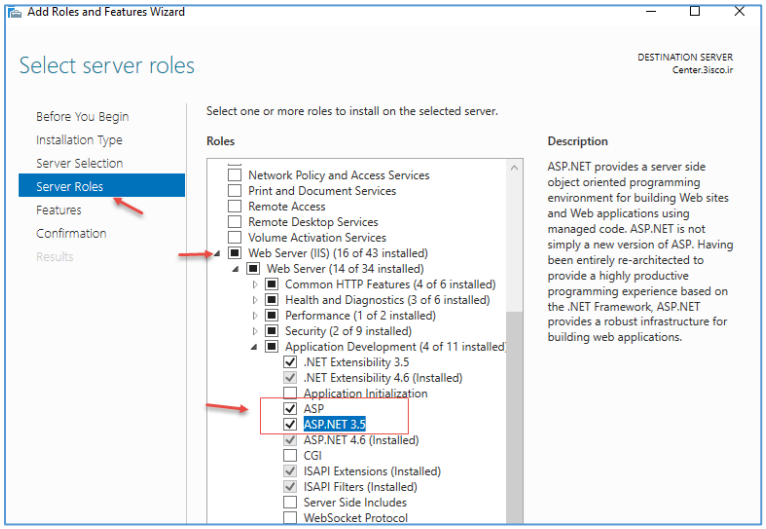
```
Add-WindowsFeature Web-Server, Web-WebServer, Web-Common-Http, Web-Default-
Doc, Web-Dir-Browsing, Web-Http-Errors, Web-Static-Content, Web-Health, Web-
Http-Logging, Web-Log-Libraries, Web-Request-Monitor, Web-Performance, Web-
Stat-Compression, Web-Security, Web-Filtering, Web-Windows-Auth, Web-App-Dev,
Web-Net-Ext45, Web-Asp-Net45, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Mgmt-
Tools, Web-Mgmt-Console, Web-Mgmt-Compat, Web-Metabase, NET-Framework-45-
Features, NET-Framework-45-Core, NET-Framework-45-ASPNET, NET-WCF-Services45,
NET-WCF-HTTP-Activation45, NET-WCF-TCP-PortSharing45, WAS, WAS-Process-Model,
WAS-Config-APIs -restart
```



همانطور که در شکل روبرو مشاهده می‌کنید، دستورات به خوبی اجرا شده و پیش‌نیازها نصب شده است، بعد از این کار، سرور را Restart کنید.



بعد از این که وارد سرور شدید، وارد Server Manager شوید و بر روی Add roles and Features کلیک کنید.



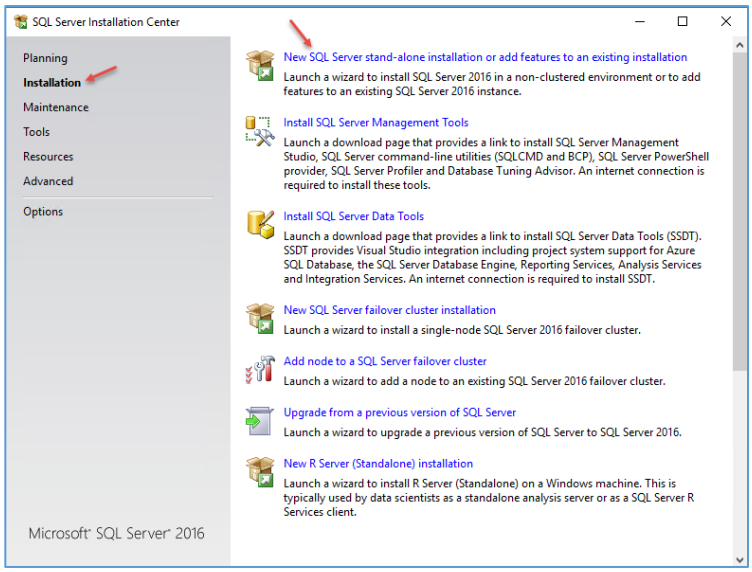
در قسمت Server Roles، دو گزینه‌ی ASP و ASP .NET 3.5 را انتخاب و بر روی Next کلیک کنید و در آخر بر روی Install کلیک کنید تا این دو ابزار نیز که از پیش‌نیازهای این نرم‌افزار است بر روی سرور نصب شود.

بعد از انجام مراحل بالا، نیاز به نرم‌افزار SQL دارید که در این کتاب از SQL Server 2016 استفاده کردیم که آخرین ورژن این نرم‌افزار محبوب است.

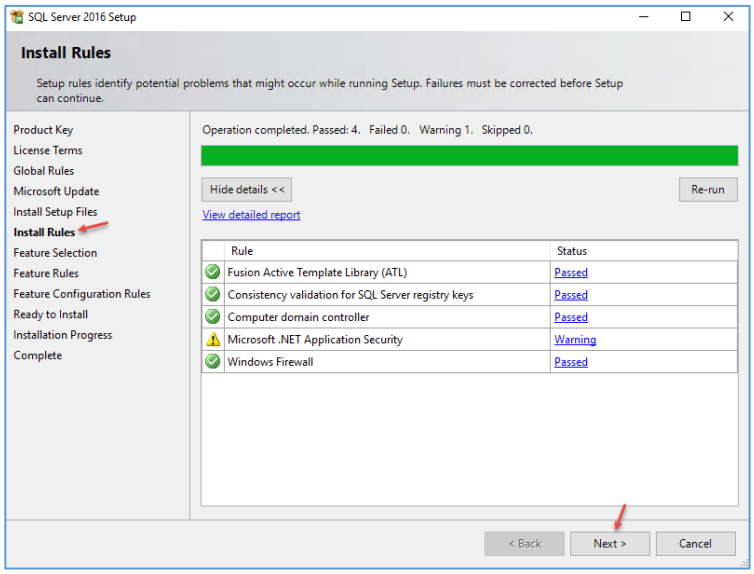
برای دانلود SQL Server 2016 از لینک زیر استفاده کنید:

http://p30download.com/fa/entry/66102/%D8%AF%D8%A7%D9%86%D9%84%D9%88%D8%AF-microsoft-sql-server-2016-x64

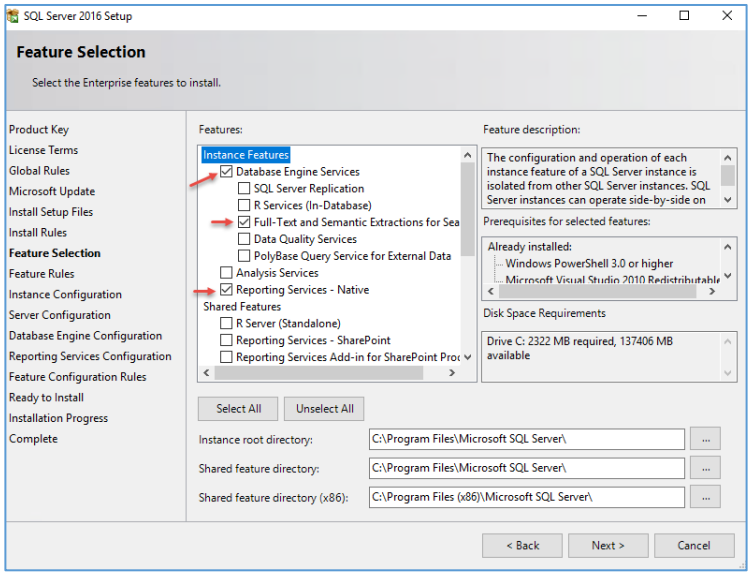
شما می‌توانید سرور SQL را به صورت جداگانه نصب و راه‌اندازی کنید، امّا در این قسمت، SQL را بر روی سرور SCOM، یعنی همین سرور نصب کنید.



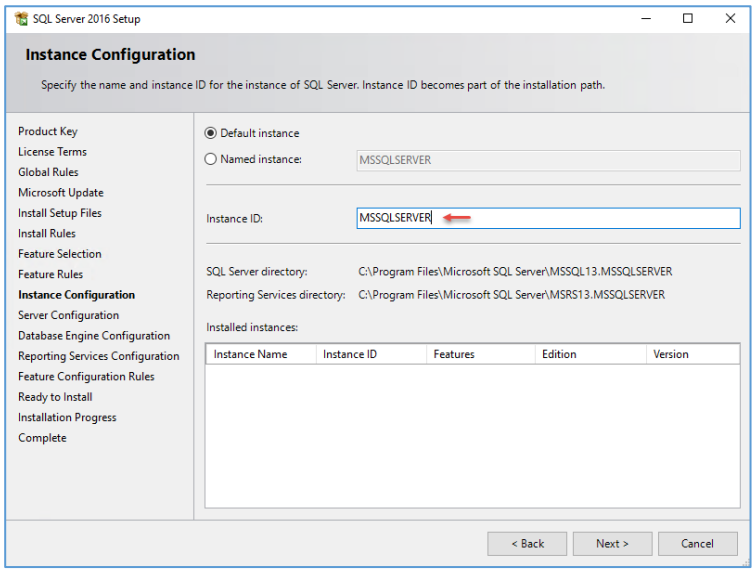
بعد از دانلود، دو بار بر روی فایل Setup کلیک کنید و در شکل باز شده‌ی روبرو به قسمت Install ation مراجعه کنید و بر روی New SQL Server stand-alone کلیک کنید.



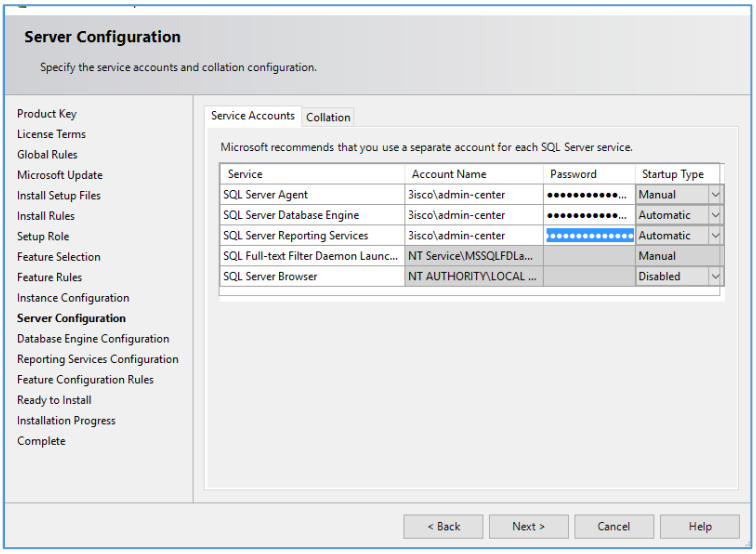
بر روی Next کلیک کنید تا به این صفحه برسید، اگر در این صفحه با خطایی مواجه نشدید، بر روی Next کلیک کنید، اگر در این قسمت فایروال را تنظیم نکرده باشید و Net3.5 را نصب نکرده باشید با خطا روبرو می‌شوید که این کار را قبلاً انجام دادیم.



در قسمت Feature Selection باید سرویس‌های مورد نظر خود را انتخاب کنید، از لیست روبرو گزینه‌های مشخّص‌شده را انتخاب و بر روی Next کلیک کنید.

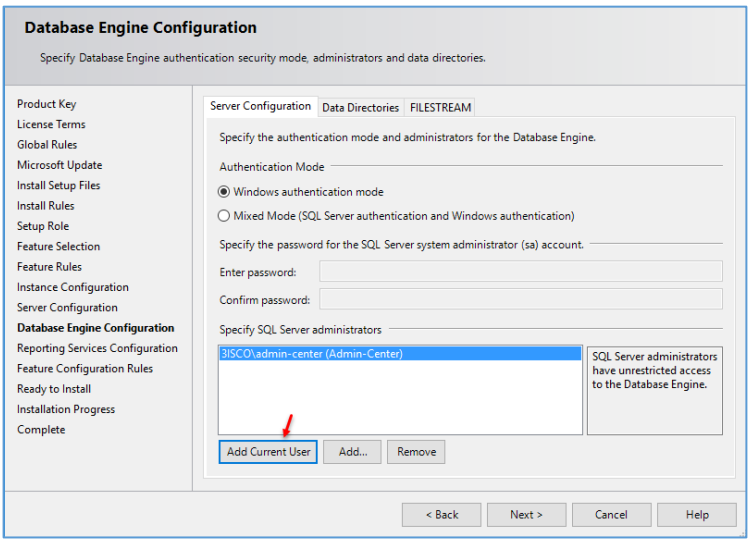


در این صفحه باید Instance خود را مشخّص کنید که به صورت پیش‌فرض، MSSQLSERVER تعریف شده است و اگر برای اوّلین بار است که اقدام به نصب SQL می‌کنید، این نام فعّال می‌شود، امّا اگر از قبل، SQL نصب کرده باشید باید یک Instance جدید تعریف کنید، اگر زیاد با SQL کار نکردید، می‌توانید کتاب آموزشی آن را از اینجا دانلود کنید.

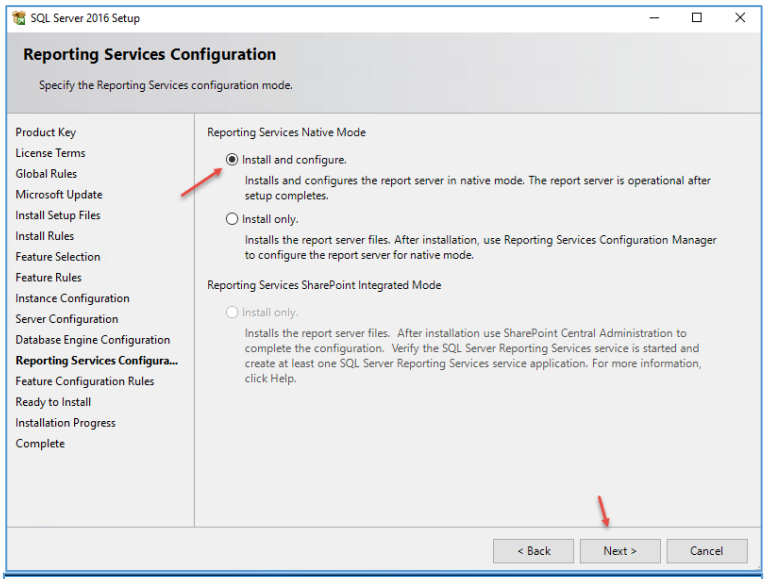


در این قسمت باید برای سرویس‌های مورد نظر خود، یک کاربر با دسترسی بالا وارد کنید که در سه سرویس اوّل، کاربر admin-center به صورت 3isco\admin-center وارد شده است که دسترسی کامل دارد، بعد از این کار بر روی Next کلیک کنید.

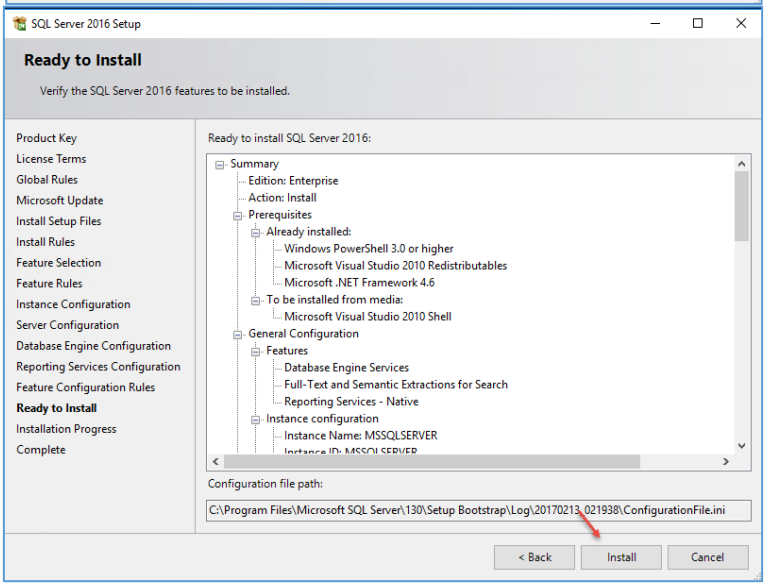
در این قسمت باید کاربر Admin نرم‌افزار SQL را مشخّص کنید که اگر با کاربر Admin یا کاربری که دسترسی کامل به شبکه دارد در حال نصب SQL هستید، می‌توانید بر روی Add Current User کلیک کنید، یا اگر می‌خواهید کاربر دیگری را به لیست اضافه کنید باید بر روی Add کلیک کنید.

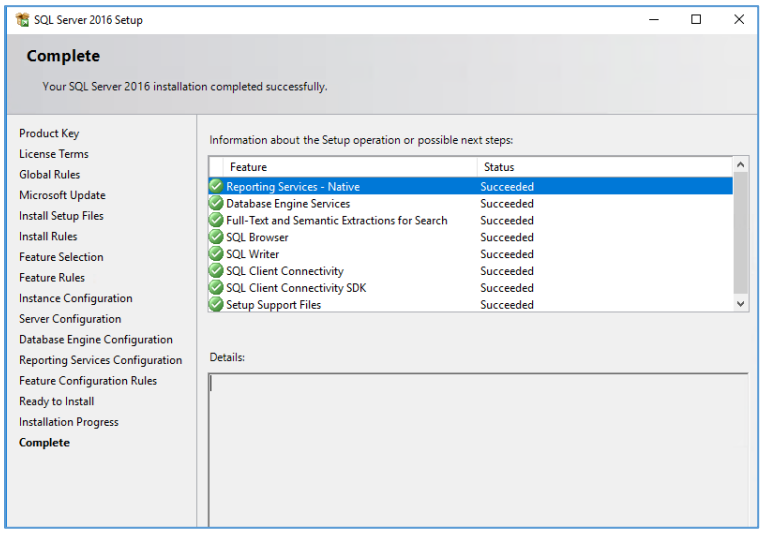


در این صفحه، گزینه‌ی اوّل، یعنی Install and Configure را انتخاب و بر روی Next کلیک کنید.



در این صفحه، اگر تنظیمات مورد قبول شما است بر روی Install کلیک کنید تا SQL نصب شود.





همانطور که مشاهده می‌کنید، نرم‌افزار SQL به صورت کامل بر روی سرور نصب شده است، بعد از نصب، سرور را Restart کنید.

بعد از اینکه SQL را نصب کردید، دو پیش‌نیاز دیگر نیز وجود دارد:

Microsoft® SQL Server® 2014 Feature Pack

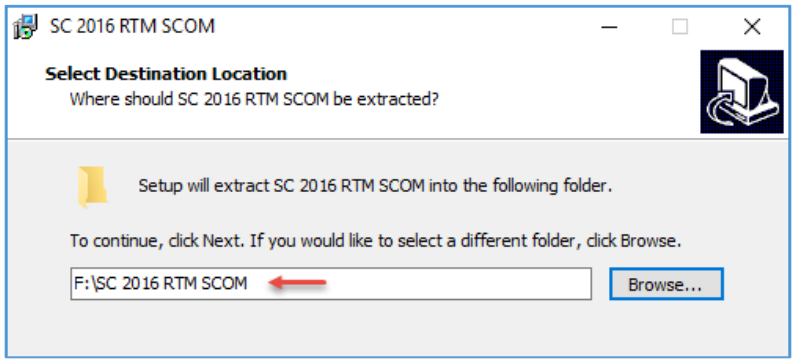
MICROSOFT® REPORT VIEWER 2015 RUNTIME

آنها را از لینک‌های زیر دانلود کنید:

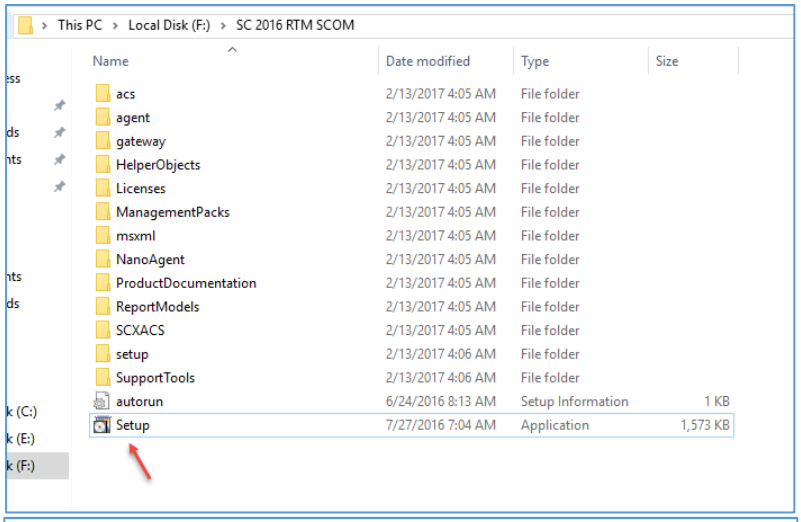
https://download.microsoft.com/download/1/3/0/13089488-91FC-4E22-AD68-5BE58BD5C014/ENU/x64/SQLSysClrTypes.msi

https://www.microsoft.com/en-us/download/details.aspx?id=45496&751be11f-ede8-5a0c-058c-2ee190a24fa6=True

همه چیز برای نصب نرم‌افزار Microsoft.System.Center. Operations.Manager آماده است.



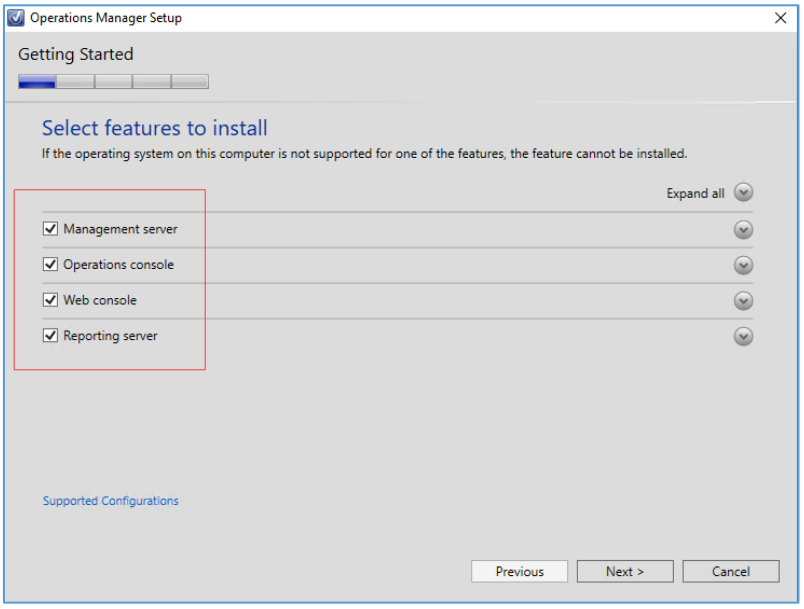
بر روی فایل Setup کلیک کنید برای استخراج کردن فایل‌های نرم‌افزار، یک مسیر را در سرور انتخاب و بر روی Next کلیک کنید تا این کار انجام شود.



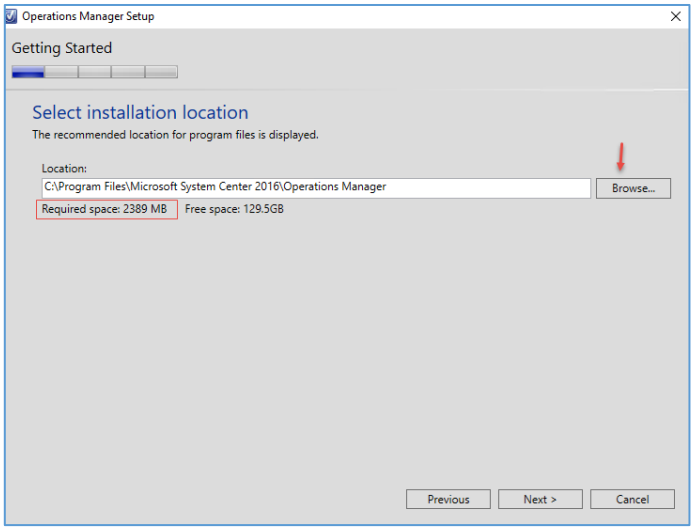
بعد از استخراج شدن فایل، دوبار بر روی Setup، کلیک کنید تا کار نصب را آغاز کنید.



صفحه‌ی اوّل Operation Manager را مشاهده می‌کنید، برای شروع کار بر روی Install کلیک کنید.

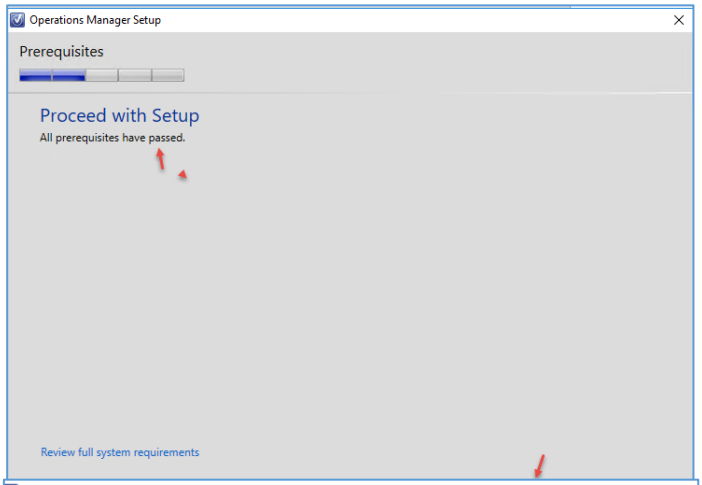


در این صفحه، تیک هر چهار گزینه را انتخاب و بر روی Next کلیک کنید.



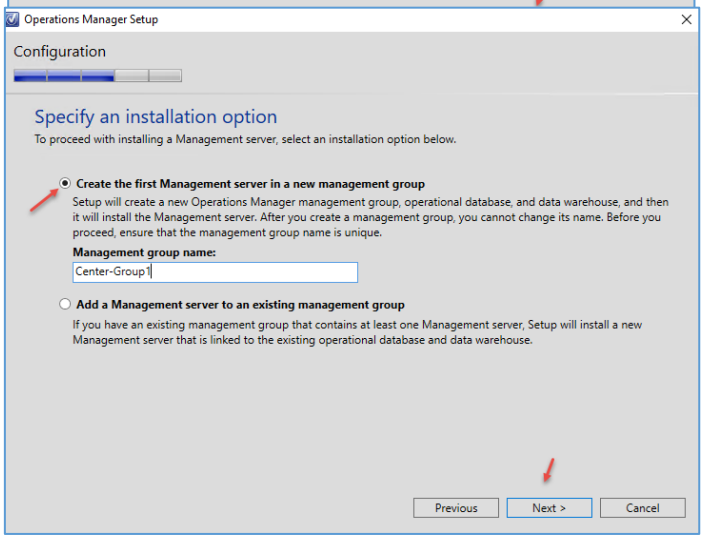
در این قسمت، آدرس محلّ نصب نرم‌افزار را مشخّص کنید، توجّه داشته باشید محلّ مورد نظر دارای ظرفیّت حداقل، ۲۳۸۹ مگابایت باشد.

بر روی **Next** کلیک کنید.



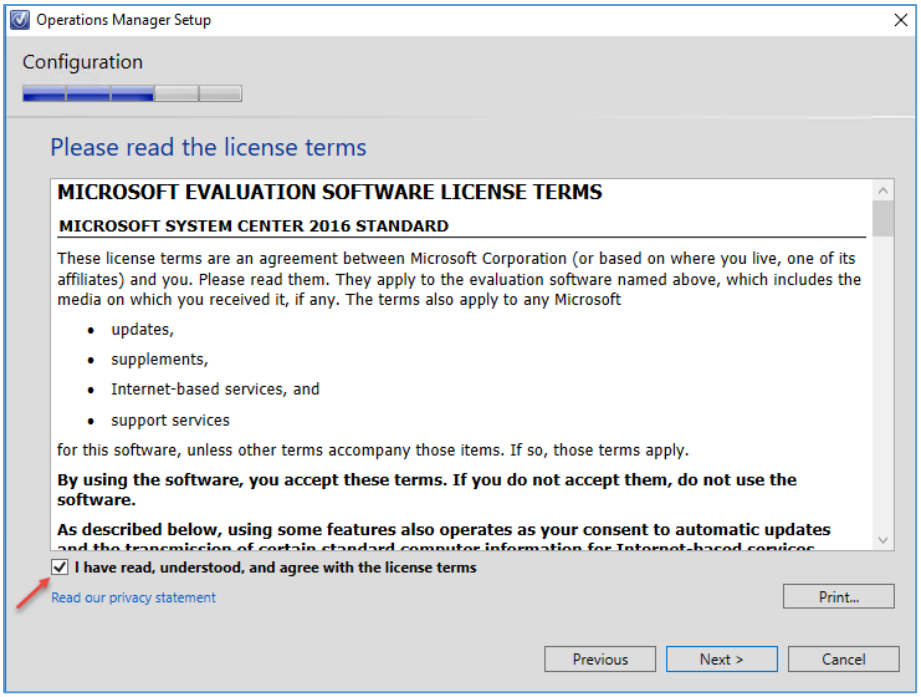
همانطور که در این صفحه مشاهده می‌کنید، تمام پیش-نیازها که از قبل نصب کردید، به درستی تأیید شده است.

بر روی **Next** کلیک کنید.

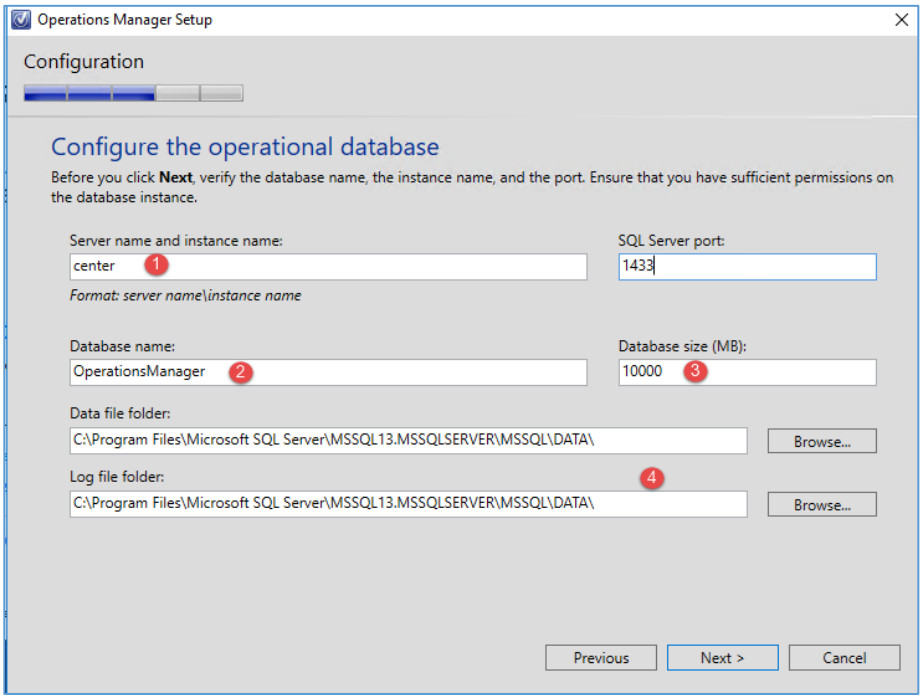


در این صفحه باید یک گروه برای شبکه‌ی خود ایجاد کنید که در اینجا، نام **Center-Group1** را وارد کردیم، توجّه داشته باشید، اگر می‌خواهید از گروه‌هایی که قبلاً ایجاد کردید، استفاده کنید باید گزینه‌ی دوّم را انتخاب و نام گروه را در قسمت مورد نظر وارد کنید.

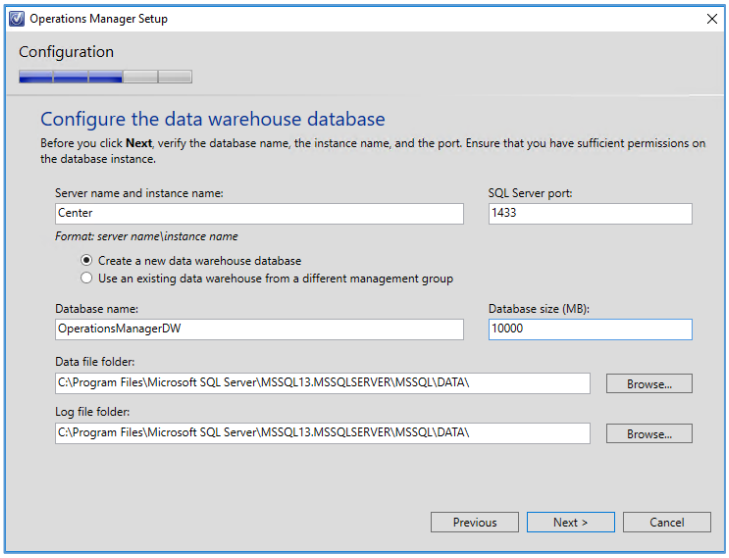
بر روی **Next** کلیک کنید.



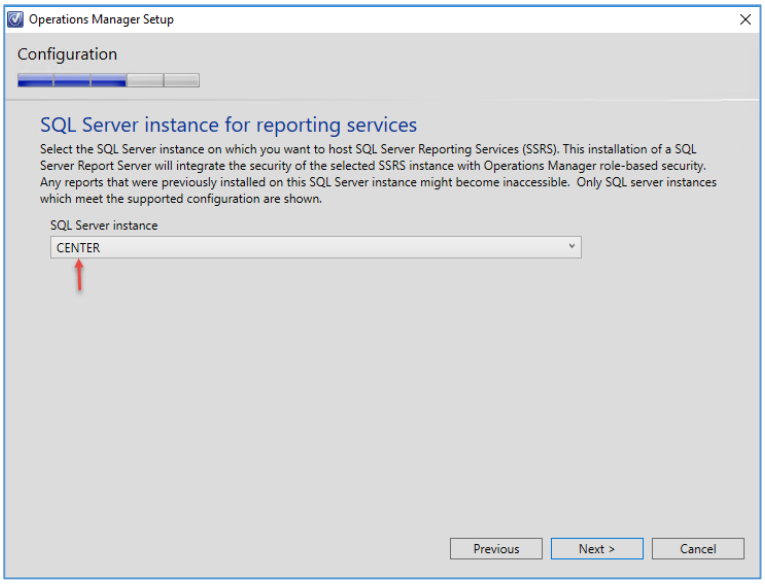
در این صفحه، اگر توافقنامه‌ی استفاده از نرم‌افزار مورد تأیید است، تیک مورد نظر را انتخاب و بر روی Next کلیک کنید.



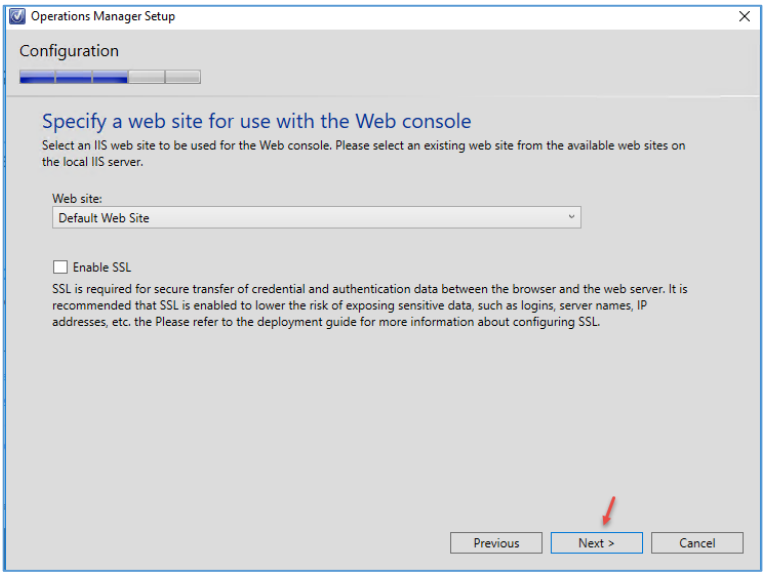
در این صفحه و در قسمت شماره‌ی یک، نام سروری که SQL را بر روی آن نصب کردید را وارد کنید که در این کتاب، SQL را بر روی سرور SCOM نصب کردیم، در قسمت شماره‌ی ۲ باید نام دیتابیس خود را مشخّص کنید که به صورت پیش‌فرض، یک نام وارد شده است، در قسمت شماره‌ی ۳، اندازه‌ی دیتابیس را بیشتر کنید که در اینجا، ۱۰ گیگابایت در نظر گرفته شده است و در قسمت شماره‌ی ٤ می‌توانید آدرس ذخیره شدن دیتابیس خود را در سرور تغییر دهید.



در این صفحه نیز به مانند صفحه‌ی قبل عمل کنید و نام سرور Center را وارد کنید و حجم دیتابیس را تغییر دهید و بر روی Next کلیک کنید.

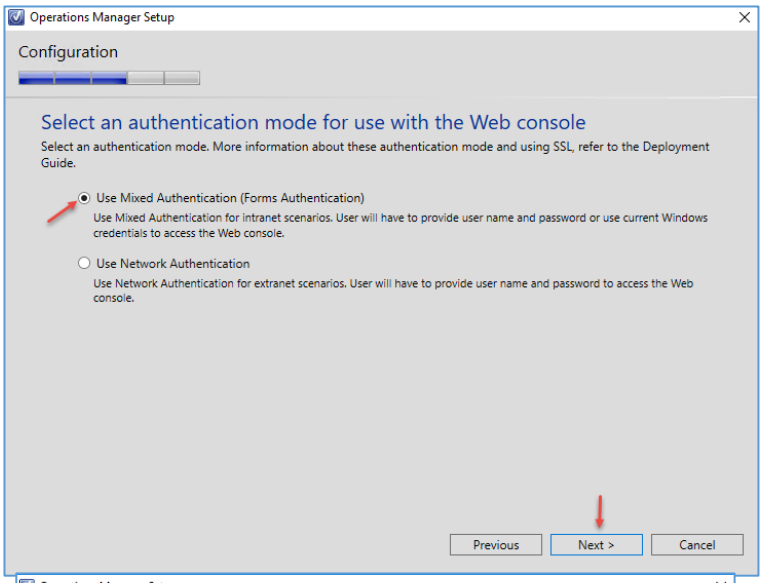


در این صفحه باید Instance مربوط به سرویس Reporting را مشخّص کنید که این سرویس را در موقع نصب SQL فعّال کردیم، به این دلیل Instance به صورت خودکار شناسایی می‌شود.

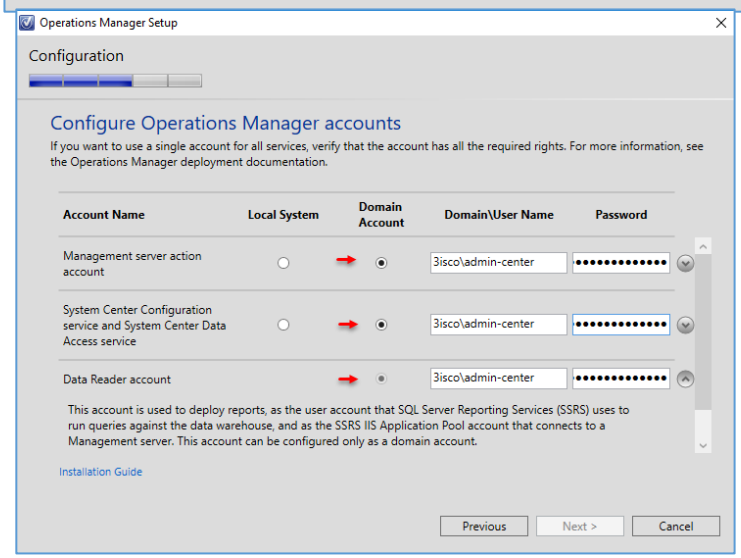


در این قسمت، یک وب سایت از سرویس IIS انتخاب می‌شود تا بر روی آن، کنسول وب این نرم-افزار فعّال شود.

بر روی Next کلیک کنید.

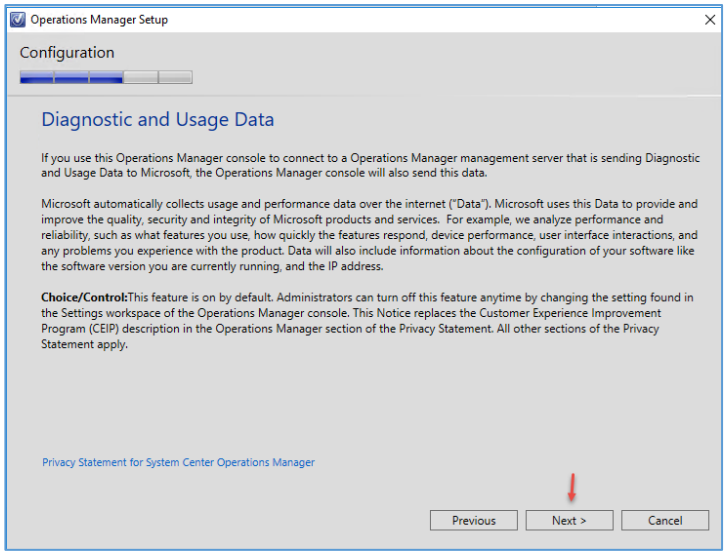


در این قسمت باید روش احراز هویّت را مشخّص کنید که در حال حاضر باید گزینه‌ی اوّل را انتخاب و بر روی Next کلیک کنید.

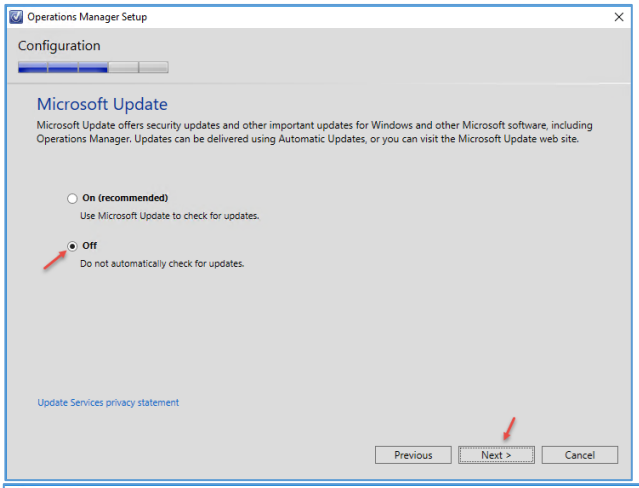


در این قسمت، Account ادمین شبکه را وارد کنید، البتّه اگر این اکانت Administrator نباشد، بهتر خواهد بود.

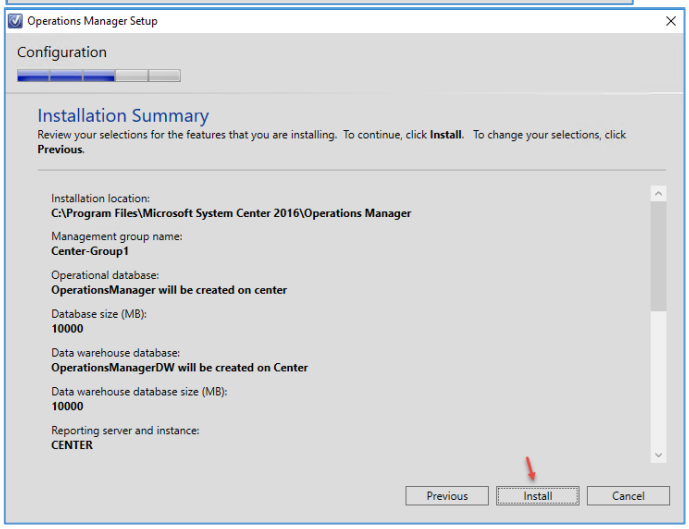
به مانند شکل، نام کاربری و رمز عبور مربوط را وارد و بر روی Next کلیک کنید.



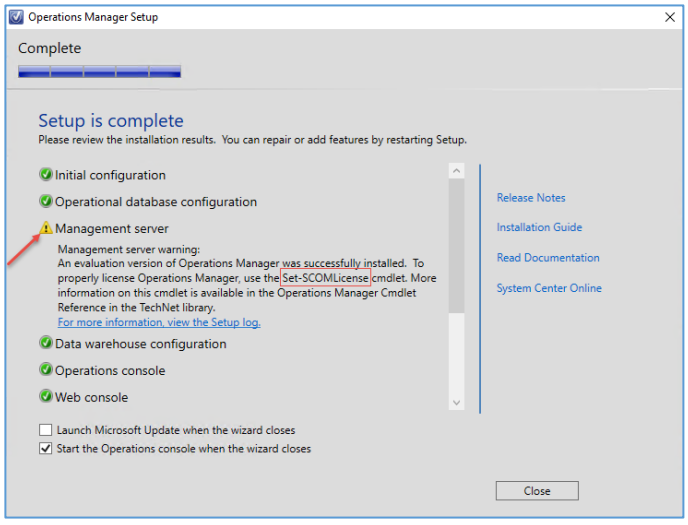
در این صفحه بر روی Next کلیک کنید.



در این صفحه، اگر مایل بودید که نرم‌افزار شما آپدیت شود، گزینه‌ی On را انتخاب کنید، در غیر این صورت، گزینه‌ی Off را انتخاب کنید و بر روی Next کلیک کنید.



در این صفحه، اگر تنظیماتی که انجام دادید، مورد تأیید است بر روی Install کلیک کنید.



همانطور که مشاهده می‌کنید، نرم‌افزار به صورت کامل نصب شده است، امّا با اخطاری مواجه شده است که در این اخطار اعلام می‌دارد که لایسنس نرم‌افزار فعّال نشده است.

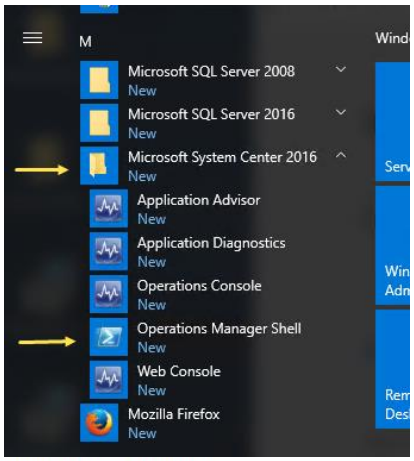
تیک گزینه‌ی مورد نظر را بردارید و بر روی Close کلیک کنید، حتماً سرور را Restart کنید.

برای فعّال‌سازی آن باید به صورت زیر عمل کنید:

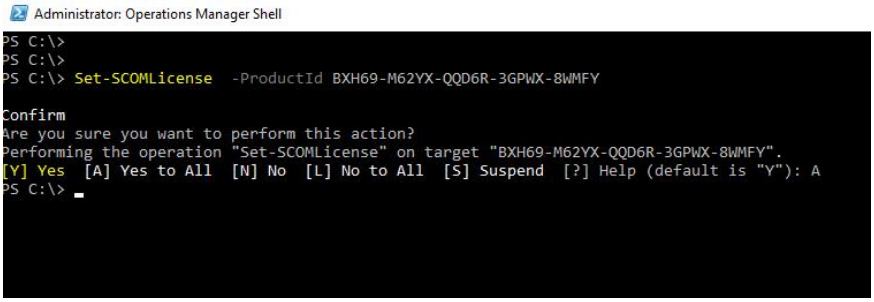
برای انجام این کار باید از سرویس PowerShell مربوط به همین نرم‌افزار استفاده کنید و دستور زیر را در آن اجرا کنید:

```
Set-SCOMLicense  -ProductId XXXXX-XXXX-XXXXX-XXXXX-XXXX
```

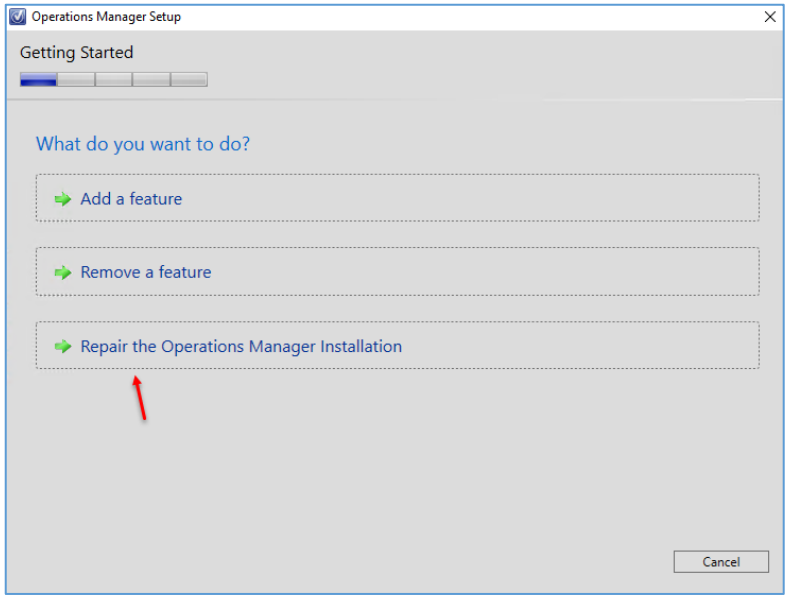
در دستور بالا، شما باید به جای X، سریال نرم‌افزار را وارد کنید.



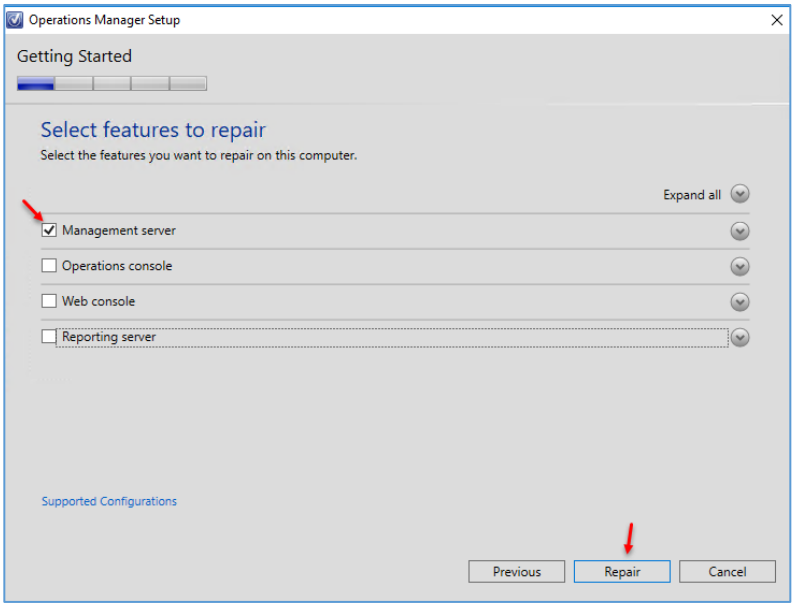
بعد از نصب نرم‌افزار وارد Start شوید و پوشه‌ی مربوط به System Center 2016 را باز کنید و به مانند شکل روبرو، سرویس Operation Management Shell را اجرا کنید.



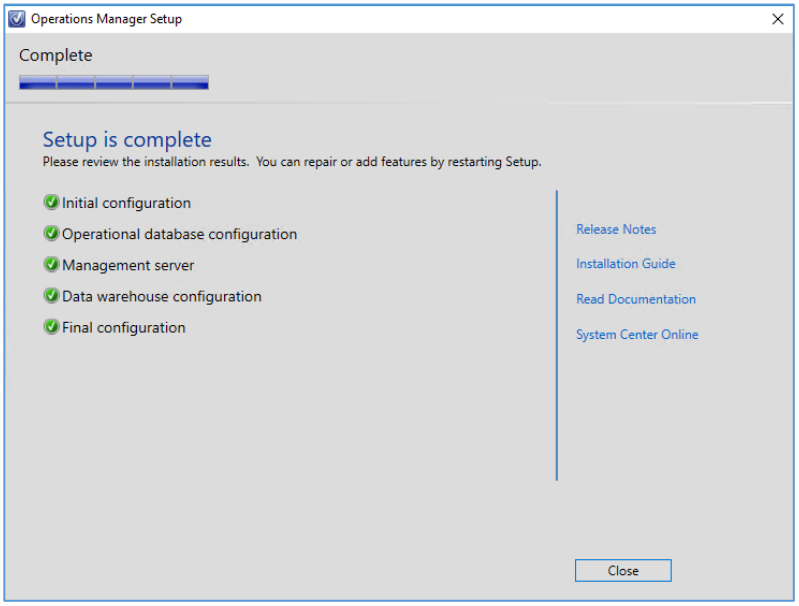
همانطور که مشاهده می‌کنید، لایسنس مورد نظر بر روی سرور فعّال شده است.



بعد از اینکه لایسنس نرم‌افزار را وارد کردید، دوباره فایل Setup مربوط به نرم‌افزار Operations Manager را اجرا کنید که شکل روبرو ظاهر خواهد شد، در این قسمت بر روی Repair the Operations کلیک کنید تا بار دیگر، نرم‌افزار با لایسنس جدید نصب شود.

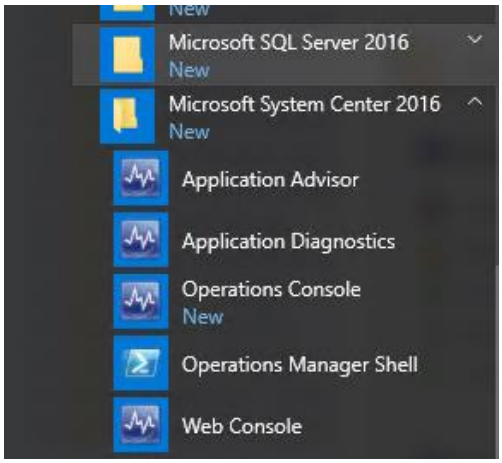


در این صفحه، تنها گزینه‌ی Management Server را که در قسمت قبل با اخطار لایسنس روبرو شده است را انتخاب و بر روی Repair کلیک کنید تا عملیّات انجام شود.

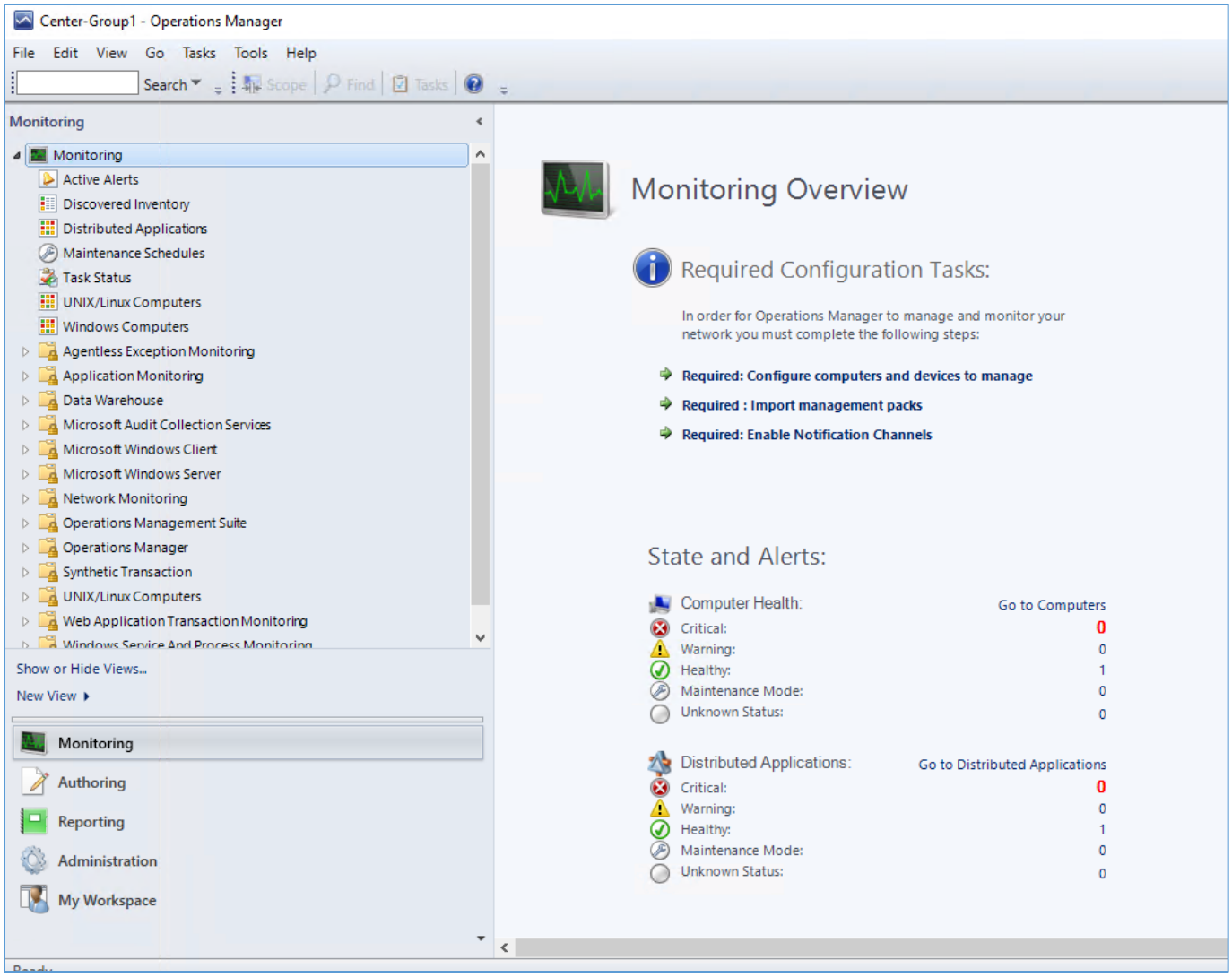


همانطور که مشاهده می‌کنید، عملیّات به طور کامل انجام شده و سیستم، آماده‌ی کار است.

برای بار آخر، سرور را Restart کنید تا کار خود را با این نرم‌افزار آغاز کنید.



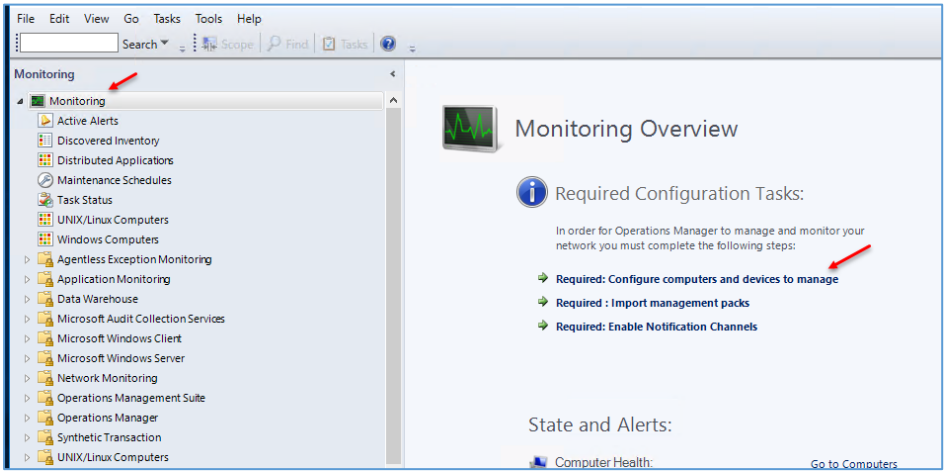
این نرم افزار، بعد از نصب دارای چندین ابزار است که در شکل روبرو مشاهده می کنید، برای شروع کار بر روی Operations Console کلیک کنید.



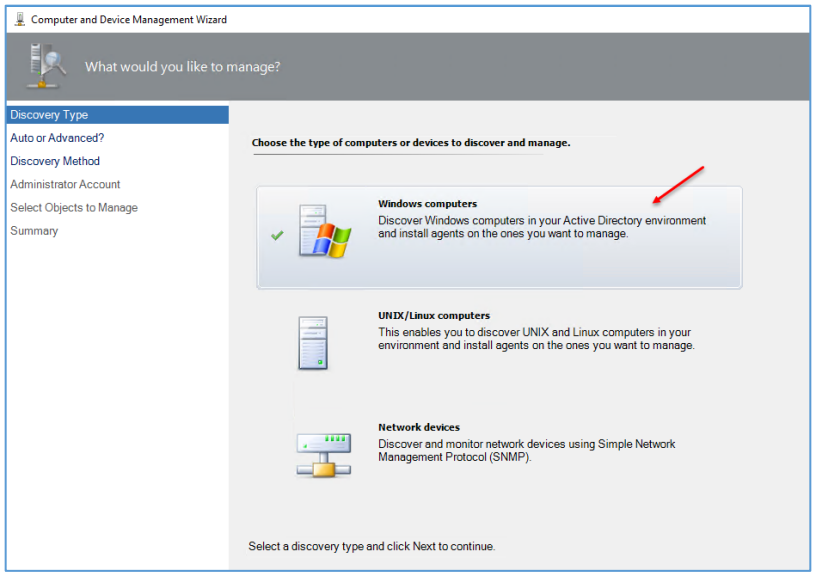
در شکل بالا، صفحه‌ی مدیریّتی نرم‌افزار Operations Manager را مشاهده می‌کنید که دارای ابزارهای مختلف برای مدیریّت هر چه بهتر شبکه است، در سمت چپ، ٦ قسمت را مشاهده می‌کنید که قسمت Monitoring، همانطور که از نامش پیداست، برای مانیتور کردن شبکه کاربرد دارد که این قسمت، خود از ابزارهای زیادی تشکیل شده است.

قسمت Authoring برای نمایش اطّلاعاتی از نرم‌افزارها، پکیج‌ها، دیتابیس‌ها و... کاربرد دارد، قسمت Reporting نیز برای ارائه‌ی گزارش از عملکرد نرم‌افزار کاربرد دارد و قسمت Administration، ابزارهایی را برای مدیریّت دستگاه‌های شبکه در اختیار شما قرار می‌دهد.

کار با قسمت Monitoring:

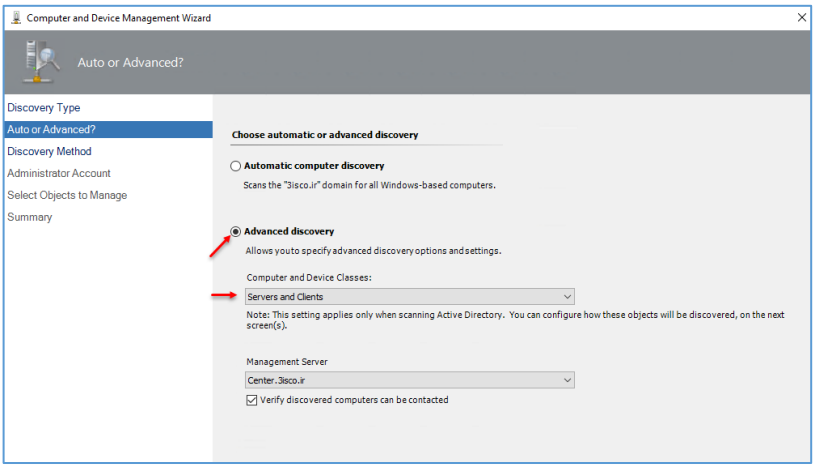


برای شروع و مانیتور کردن کلّ شبکه وارد قسمت Monitoring شوید و به مانند شکل روبرو بر روی Requires: Configure computers and devices to manage را انتخاب کنید.

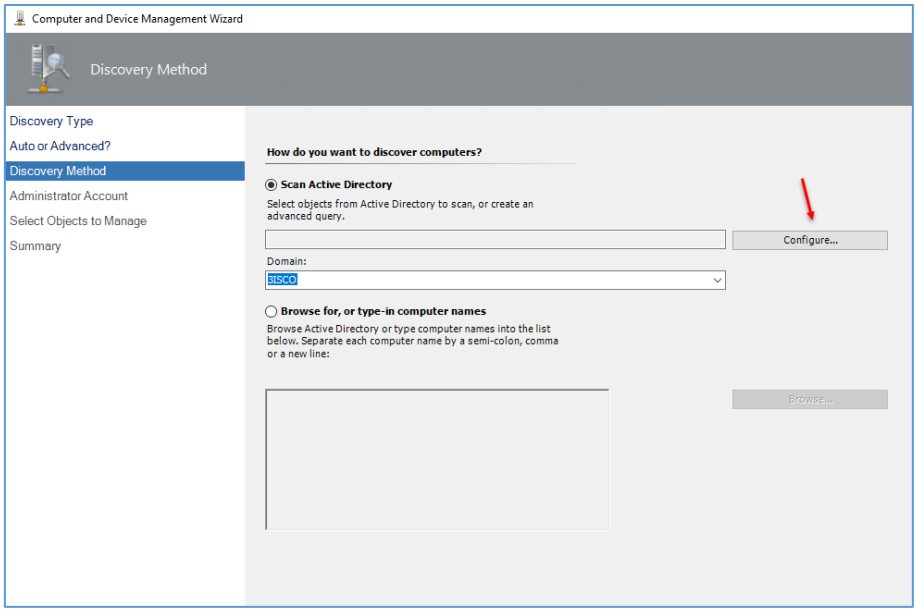


در این صفحه، سه گزینه وجود دارد؛ گزینه‌ی اوّل برای سیستم‌هایی است که با سیستم عامل ویندوز کار می‌کنند، گزینه‌ی دوّم سیستم‌هایی است که با سیستم عامل لینوکس کار می‌کنند و گزینه‌ی آخر نیز برای سیستم‌هایی است که پروتکل SNMP روی آنها فعّال شده است و می‌خواهید از آن اطّلاعات دریافت کنید.

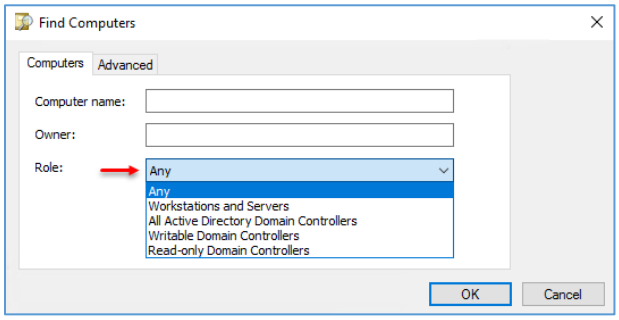
در این قسمت بر روی گزینه‌ی اوّل کلیک کنید.



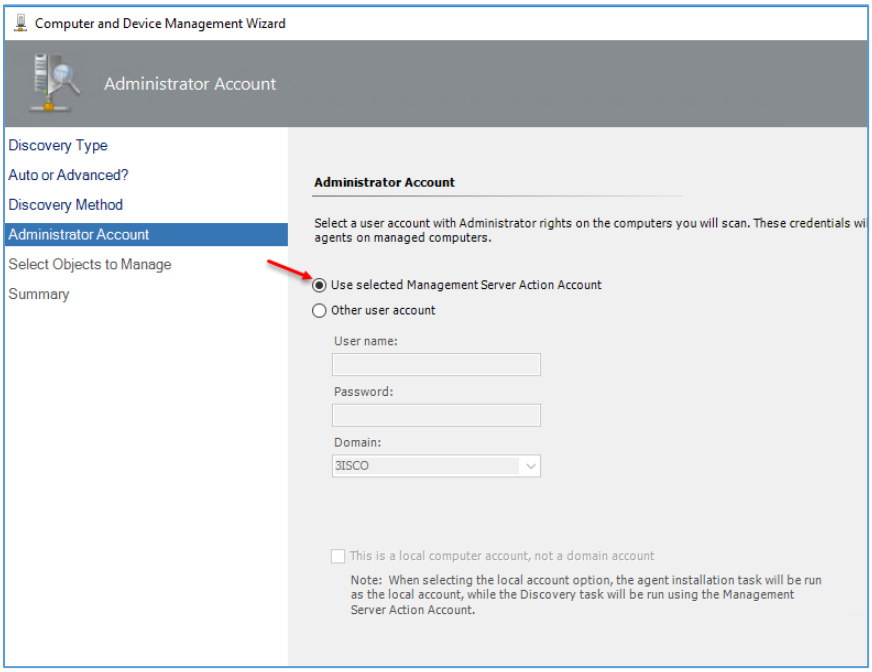
در این صفحه، دو گزینه وجود دارد که اگر گزینه‌ی اوّل را انتخاب کنید، کلّ سیستم‌هایی که با سیستم عامل ویندوز فعّال هستند، در شبکه شناسایی خواهند شد و اگر گزینه‌ی دوّم را انتخاب کنید، می‌توانید نوع سیستم را از نظر سرور یا کلاینت مشخّص کنید.



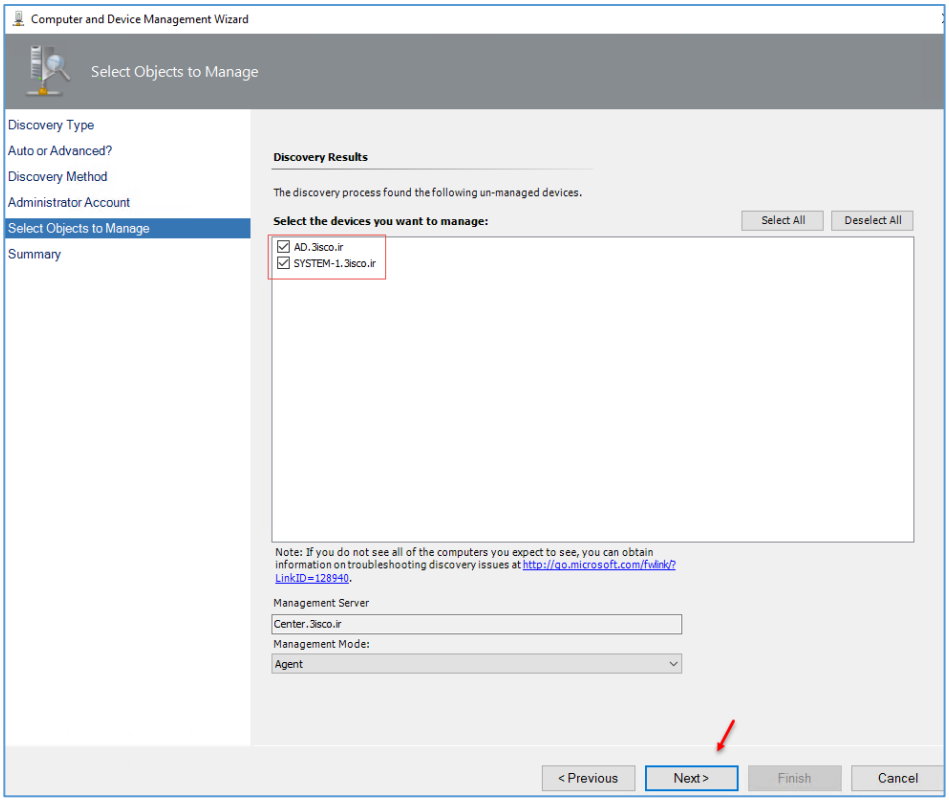
در این قسمت، اگر گزینه‌ی اوّل را انتخاب کنید، تمام سیستم‌های داخل Active Directory بررسی خواهند شد و اگر بخواهید عملیّات را تنها بر روی یک سیستم خاص انجام دهید باید گزینه‌ی دوّم را انتخاب و نام سیستم را وارد کنید.



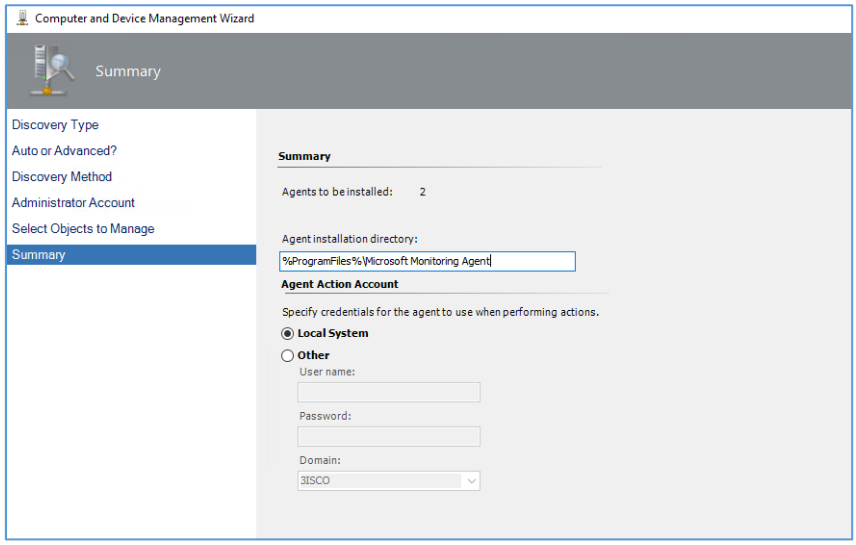
در قسمت بالا، گزینه‌ی اوّل را انتخاب و بر روی Configure کلیک کنید، در صفحه‌ی روبرو می‌توانید نوع Active Directory را مشخّص کنید که باید گزینه‌ی Any ر انتخاب کنید.



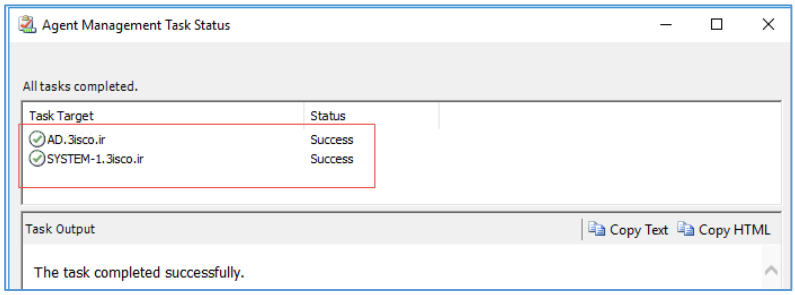
در این صفحه باید یک اکانت با دسترسی کامل وارد کنید، می‌توانید گزینه‌ی اوّل را انتخاب کنید تا با همان اکانتی که نرم‌افزار Operation Manager را نصب کردید، کار مانیتورینگ انجام شود و یا اگر می‌خواهید اکانت دیگری را وارد کنید باید گزینه‌ی Other user account را انتخاب و اکانت مورد نظر را وارد کنید، گزینه‌ی اوّل را انتخاب کنید و بر روی Discover کلیک کنید.



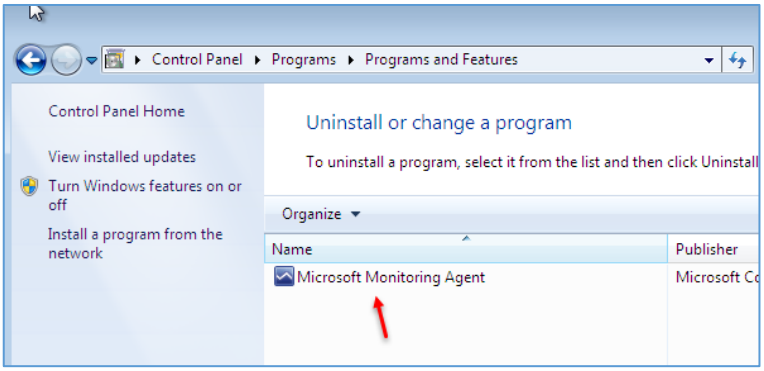
در شکل روبرو بعد از بررسی شبکه، دو سیستم در دسترس بوده است و در لیست قرار گرفتند، برای اینکه عملیّات مانیتورینگ را بر روی آنها انجام دهید، آنها را انتخاب کنید تا بعد از **Next**، یک نرم‌افزار **Agent** که مربوط به این **Operations Maneger** است، در سیستم مقصد نصب شود تا اطّلاعات آن سیستم برای سرور ارسال شود.



در این قسمت، مسیر نصب **Agent** در سیستم مقصد مشخّص شده است که در **ProgramFiles** انجام می‌شود، شما می‌توانید برای این نرم‌افزار یک اکانت خاص وارد کنید تا اجرا شود و یا آن را بر روی **Local System** قرار دهید.



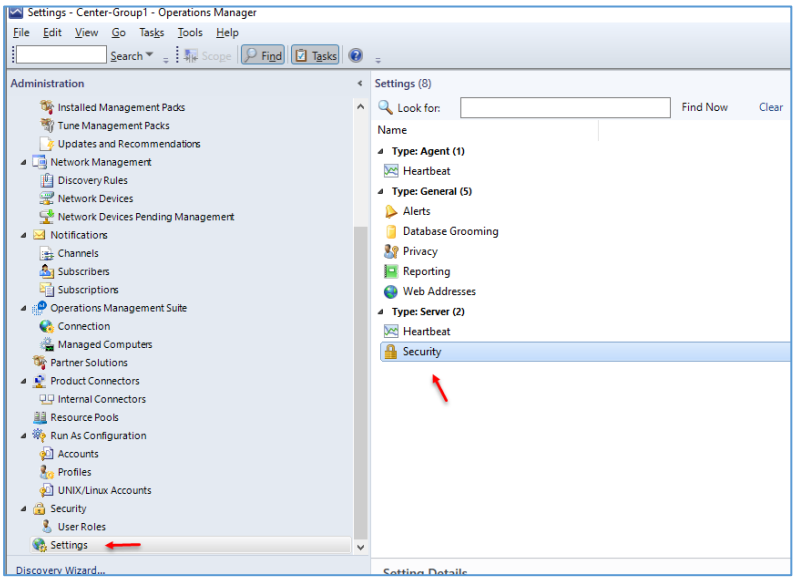
در شکل روبرو به درستی، نرم‌افزار **Agent** در دو سیستم نصب شده است.



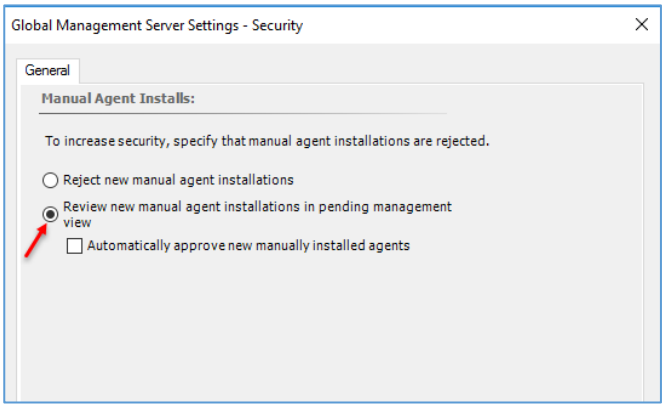
اگر در یکی از سیستم‌هایی که این نرم‌افزار نصب شده است وارد قسمت Program and Features شوید، به مانند شکل روبرو نرم‌افزار Agent را مشاهده خواهید کرد.

نصب Agent در کلاینت و تأیید آن در سرور:

راه دیگری نیز وجود دارد و آن این است که شما یا کاربران شما می‌توانند نرم‌افزار Agent را بر روی سیستم خود نصب کنند، امّا بعد از نصب، یک تأییدیّه به سرور یا همان، نرم‌افزار Operation Manager ارسال می‌شود که اگر آن را تأیید کنید، کلاینت زیر مجموعه‌ی نرم‌افزار خواهد شد.



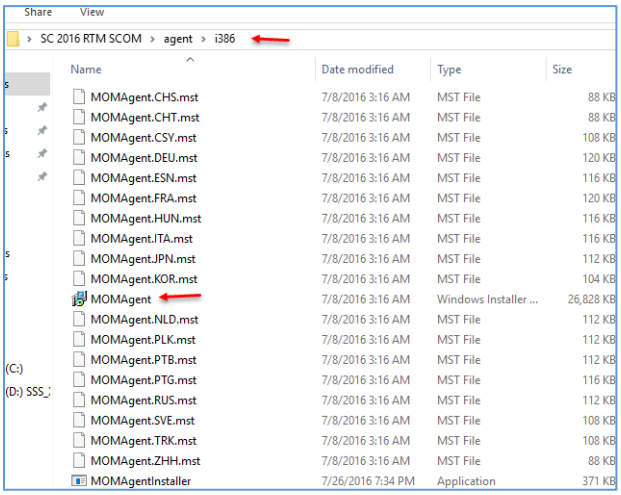
از سمت چپ وارد قسمت Settings شوید و بر روی گزینه‌ی Security کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



در این صفحه، دو گزینه وجود دارد که اگر گزینه‌ی اوّل را انتخاب کنید، به هیچ وجه آن Agent که به صورت دستی در کلاینت نصب شود، مورد تأیید نیست و به صورت اتوماتیک رد خواهد شد، امّا اگر گزینه‌ی دوّم را انتخاب کنید، بعد از نصب Agent، یک تأییدیّه برای سرور ارسال خواهد کرد.

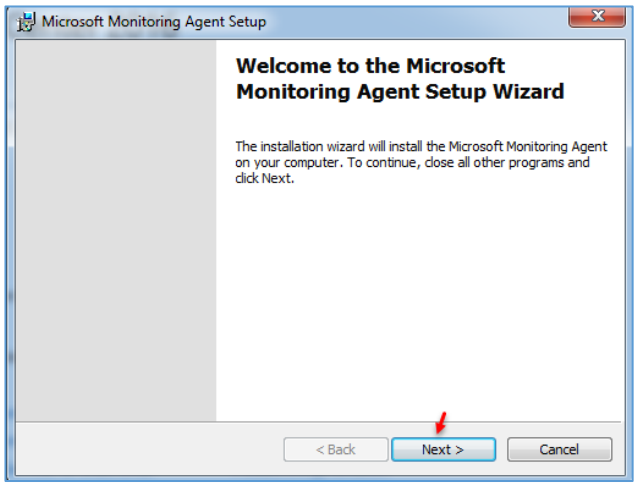


برای این که Agent را بر روی یک کلاینت نصب کنید، می‌توانید از بسته‌ی خود نرم‌افزار SCOM استفاده کنید و به مانند شکل روبرو فایل Setup اصلی را اجرا کنید و بر روی Local Agent کلیک کنید تا Setup آن اجرا شود، راه دیگر این است که از خود فایل Agent استفاده کنید.



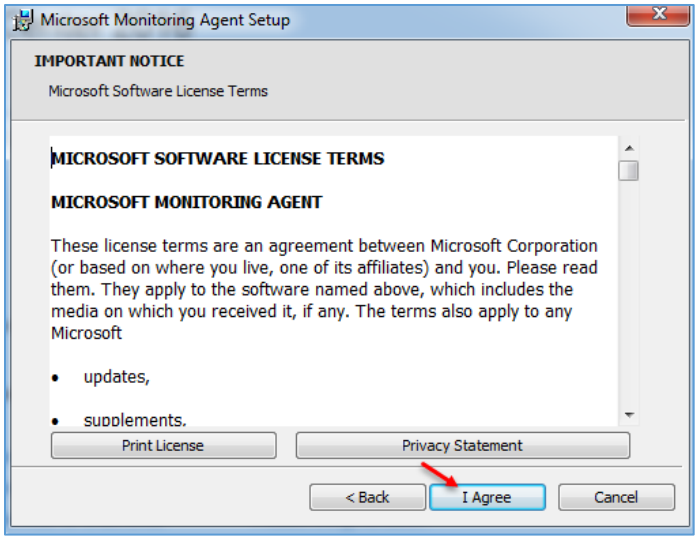
همانطور که در شکل روبرو مشاهده می‌کنید، نرم‌افزار Agent در پوشه‌ی Agent وجود دارد که می‌توانید این پوشه را برای کاربران خود، Share کنید تا بتوانند آن را نصب کنند و یا پوشه را برای آنها کپی کنید (روش اوّل پیشنهاد می‌شود).

در هر صورت، این فایل را اجرا کنید و بر روی کلاینت نصب کنید.

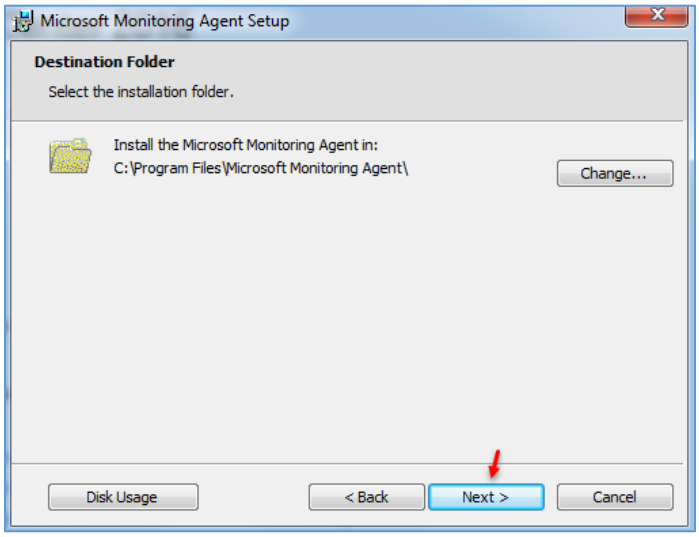


بر روی Next کلیک کنید.

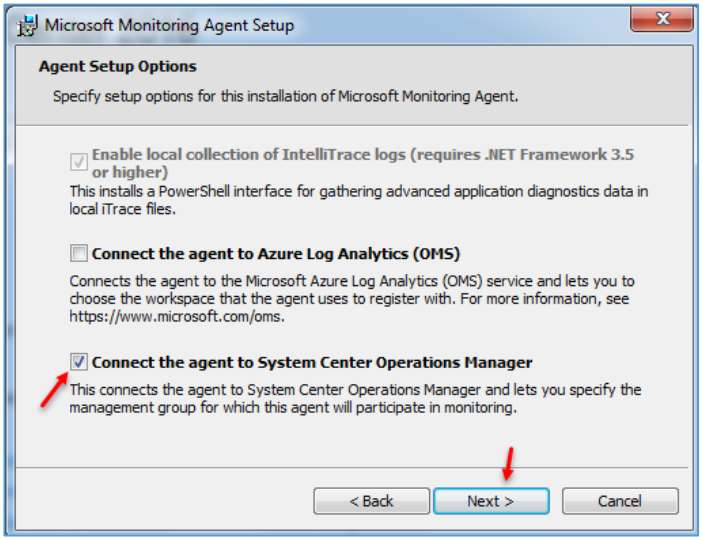
بر روی I Agree کلیک کنید.

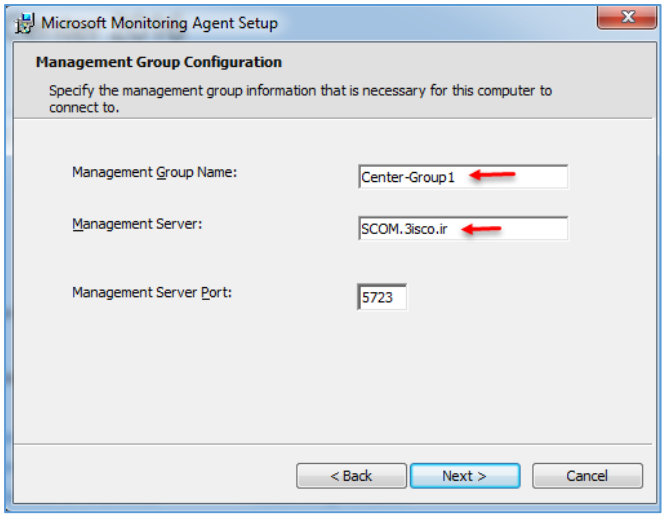


در این صفحه می‌توانید مسیر ذخیره‌سازی را مشخّص کنید و بعد بر روی Next کلیک کنید.

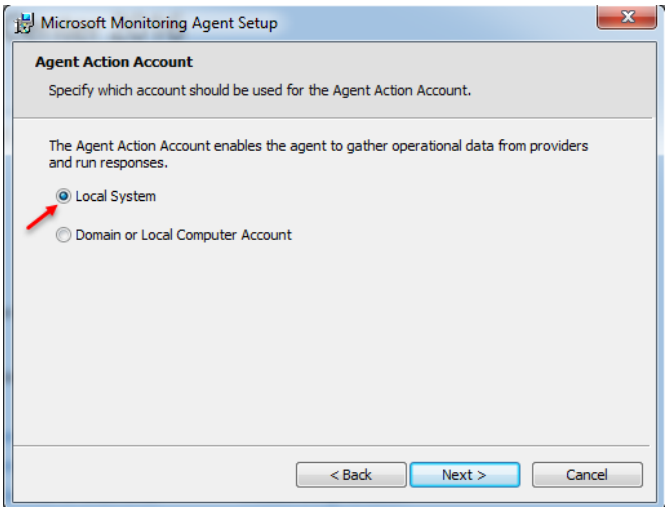


در این صفحه برای متّصل شدن به سرور SCOM، تیک گزینه‌ی آخر را انتخاب و بر روی Next کلیک کنید.

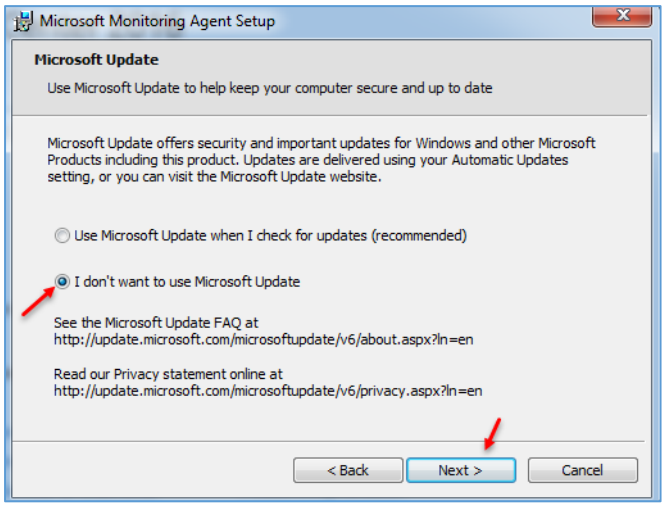




در این صفحه و در قسمت اوّل باید نام گروهی که در هنگام نصب وارد کردید را وارد کنید که در این کتاب، نام را Center-Group1 وارد کردیم، در قسمت دوّم باید نام سرور را وارد کنید و به پورت پیش‌فرض آن دست نزنید و بر روی Next کلیک کنید.

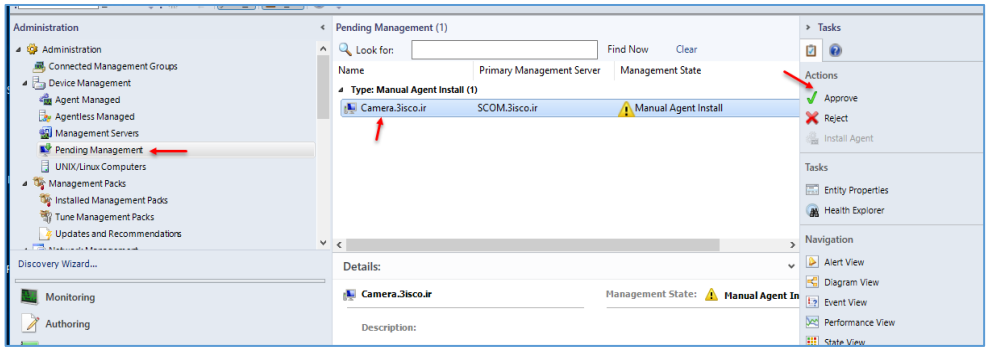


در این قسمت، Local System را انتخاب و بر روی Next کلیک کنید، اگر چنانچه می‌خواهید از یک اکانت دیگر تحت دومین که دسترسی لازم را دارد، استفاده کنید باید گزینه‌ی دوّم را انتخاب و نام اکانت مورد نظر را وارد کنید.

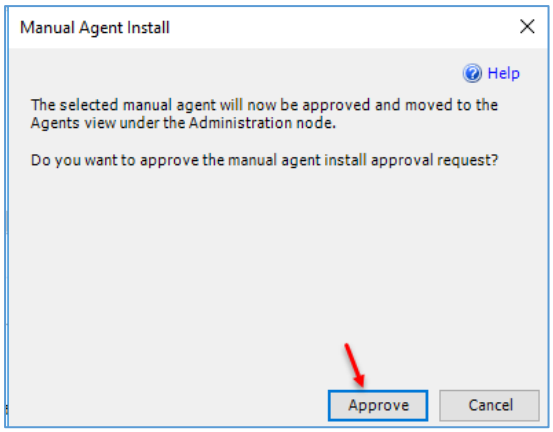


در این قسمت، گزینه‌ی دوّم را انتخاب و بر روی Next کلیک کنید.

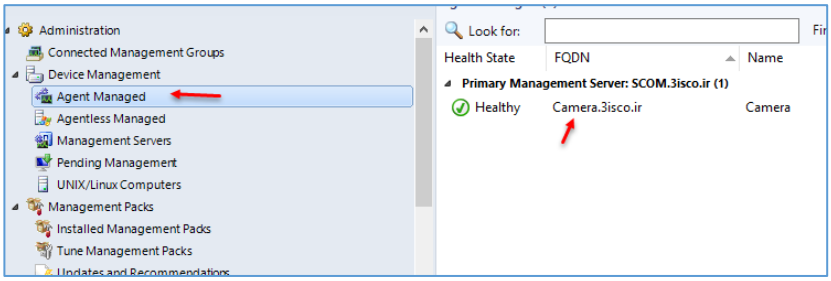
در صفحه‌ی بعد بر روی Install کلیک کنید.



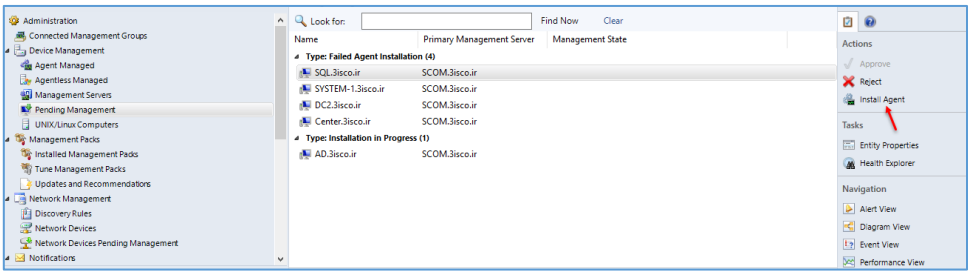
زمانی که Agent نصب شد، در داخل نرم‌افزار SCOM و از قسمت Pending Management، یک درخواست مشاهده خواهید کرد که اگر سیستم مورد نظر مورد تأیید باشد، می‌توانید بر روی Approve در سمت راست کلیک کنید و ادامه‌ی کار سیستم را تأیید کنید و اگر مورد تأیید نباشد، می‌توانید آن را Reject یا رد کنید.



اگر به قسمت Agent Managed مراجعه کنید، مشاهده خواهید کرد که سیستم مورد نظر تأیید و به لیست اضافه شده است.

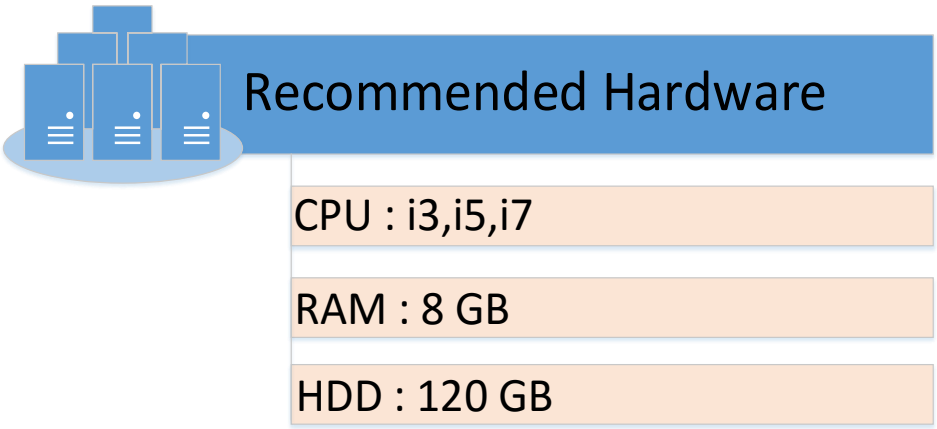


اگر گزینه‌ی تأیید را فعّال کرده باشید، کلاینت‌هایی که به صورت اتوماتیک توسّط ابزار Discovery پیدا می‌شوند، در قسمت Pending Management قرار می‌گیرند که باید هر کدام از آنها را که نیاز دارید، انتخاب کنید و از سمت راست بر روی Install agent کلیک کنید، البتّه این در صورتی است که سیستم مورد نظر روشن نباشد، امّا اگر روشن باشد، Agent نصب می‌شود که می‌توانید آن را Reject کنید.



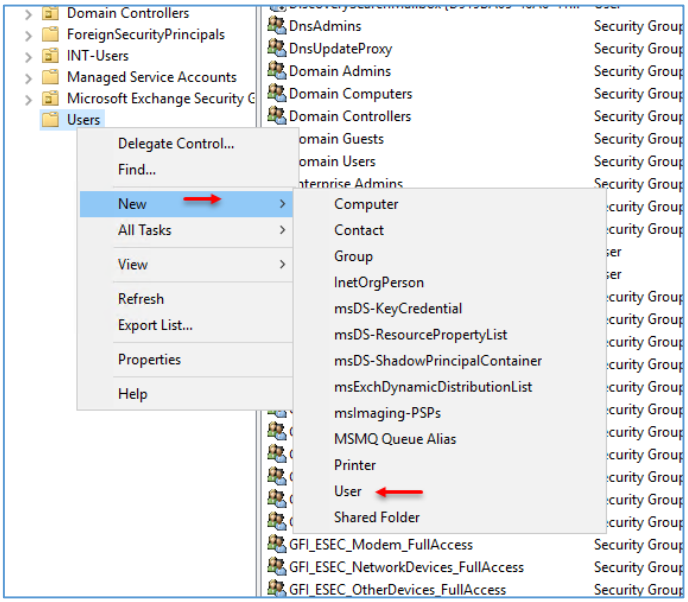
نصب و راه‌اندازی System Center Configuration Manager:

سخت‌افزار مورد قبول برای راه‌اندازی این سرور:

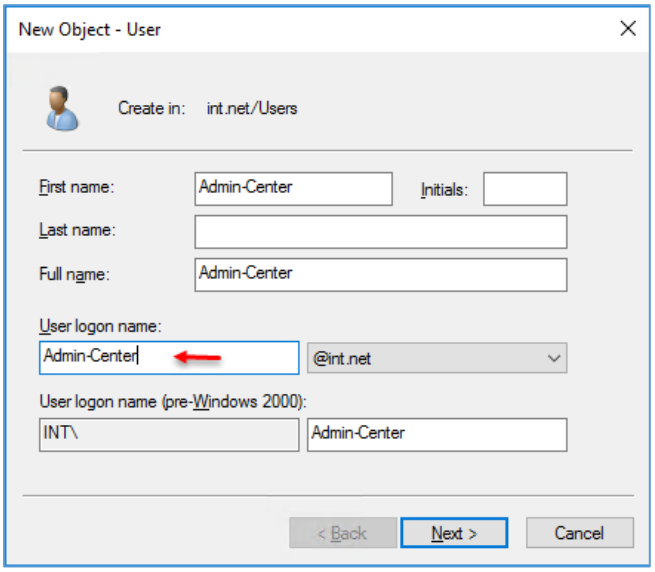


مرحله‌ی اوّل – تعریف کاربر:

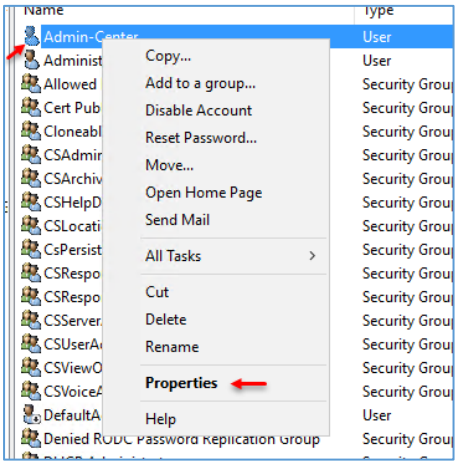
برای اینکه نرم‌افزار Configuration Manager System Center را به درستی نصب کنید، به کاربری نیاز دارید که جدا از کاربر Administrator باشد و دسترسی کامل به شبکه داشته باشد.



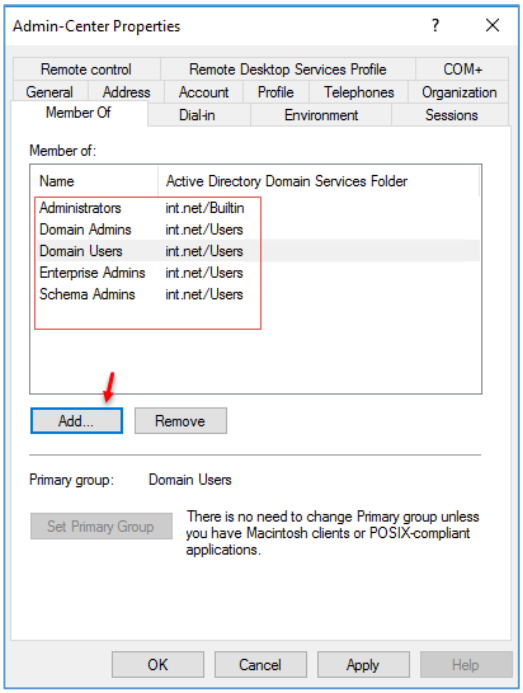
وارد سرور دومین شوید و به مانند شکل روبرو سرویس Active Directory User and Computers را اجرا کنید و بر روی Users یا واحد سازمانی مورد نظر خود کلیک راست کنید و از قسمت New، گزینه‌ی User را انتخاب کنید.



در این قسمت باید نام کاربری کاربر مورد نظر را که در اینجا، Admin-Center است را وارد کنید، البتّه این نام می‌تواند به دلخواه شما باشد، بر روی Next کلیک کنید و رمز عبور خود را وارد و بر روی Finish کلیک کنید تا کاربر مورد نظر ایجاد شود.



بعد از ایجاد کاربر باید دسترسی‌های مدیریّتی را به کاربر مورد نظر تخصیص دهید، برای این کار بر روی کاربر مورد نظر کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



به مانند شکل روبرو وارد تب Member Of شوید و بر روی Add کلیک کنید و کاربر مورد نظر را عضو گروه‌های زیر کنید:

- Enterprise Admins
- Schema Admins
- Domain Admins
- Administrator

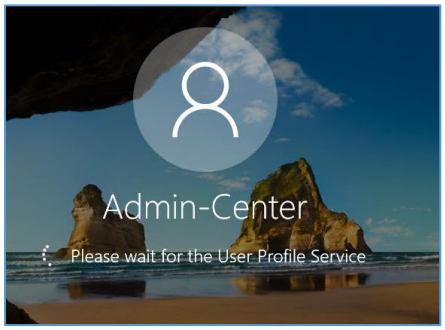
مرحله‌ی دوّم – نصب نرم‌افزار SQL:

در مرحله‌ی دوّم، اقدام به نصب نرم‌افزار SQL می‌کنیم، ورژن این نرم‌افزار می‌تواند از ۲۰۱۲ به بالا باشد، امّا ورژن ۲۰۱۲ باید آخرین آپدیت را داشته باشد، برای اینکه به مشکلی بر نخوریم از SQL Server 2016 برای این کتاب استفاده می‌کنیم.

برای دانلود SQL Server 2016 ار لینک زیر استفاده کنید:

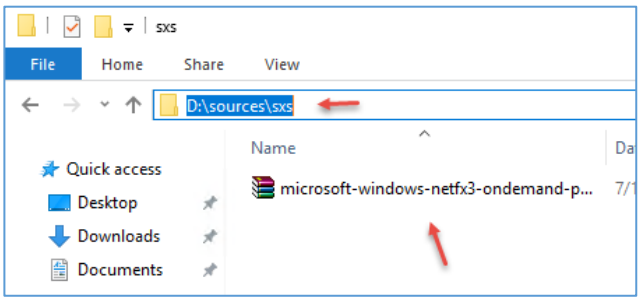
http://p30download.com/fa/entry/66102/دانلود-microsoft-sql-server-2016-x64

برای راحتی کار، SQL را بر روی سرور Center نصب کنید، قبل از نصب SQL باید پیش‌نیاز Net FramWork 3.5 را بر روی سرور نصب کنید که برای این کار باید به صورت زیر عمل کنید:

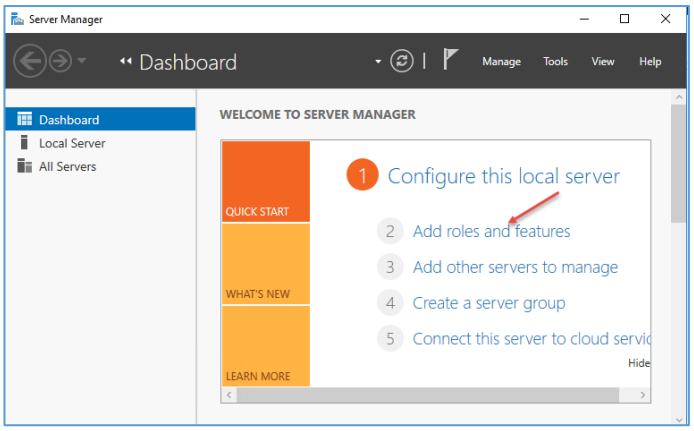


تذکّر: لطفاً با کاربری که در قسمت قبل ایجاد کردیم وارد سرور شوید و کار نصب SQL را انجام دهید.

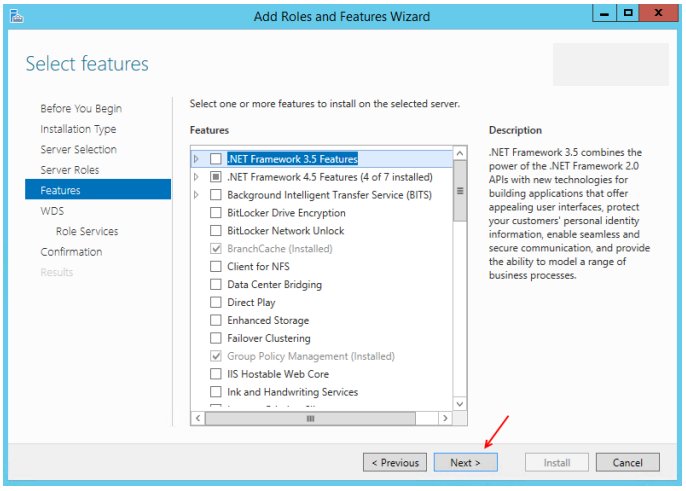
به صورت پیش‌فرض، Net 3.5 بر روی ویندوز ۲۰۱۶ نصب نشده است که برای نصب آن نیاز به DVD مربوط به آن دارید تا فایل Net 3.5 را دریافت کنید، برای این کار، DVD را داخل دستگاه قرار دهید و وارد آدرس زیر شوید:



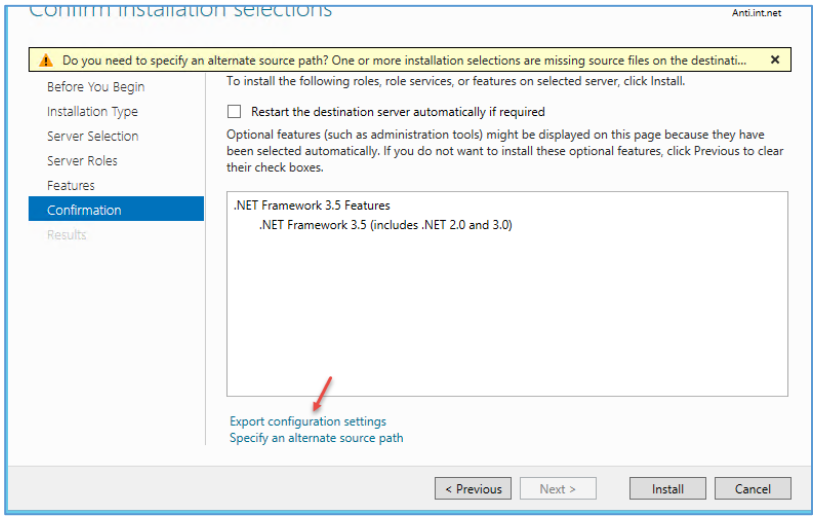
به مانند شکل، آدرس مورد نظر را کپی کنید تا در ادامه از آن استفاده کنید.



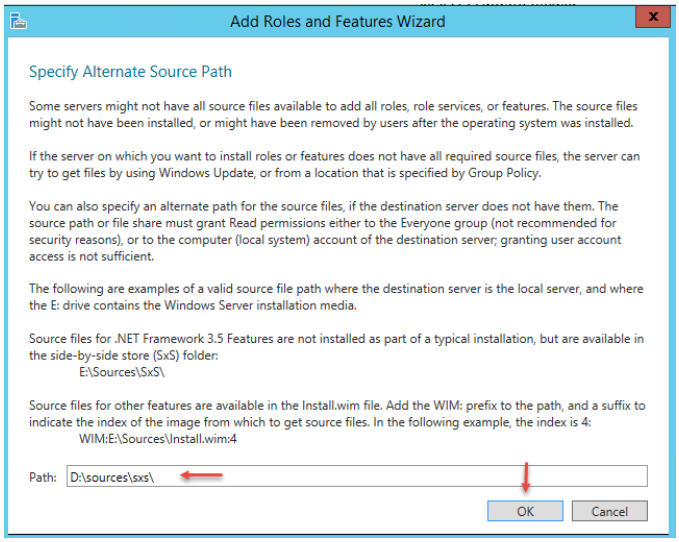
بعد از کپی کردن آدرس وارد Server Manager شوید و بر روی Add roles and Features کلیک کنید.



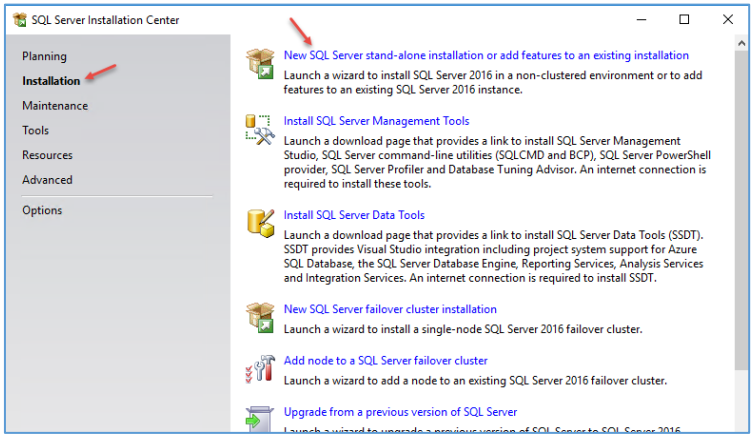
در صفحه‌ی Features، تیک گزینه‌ی .NET Framework 3.5 را انتخاب و بر روی Next کلیک کنید.



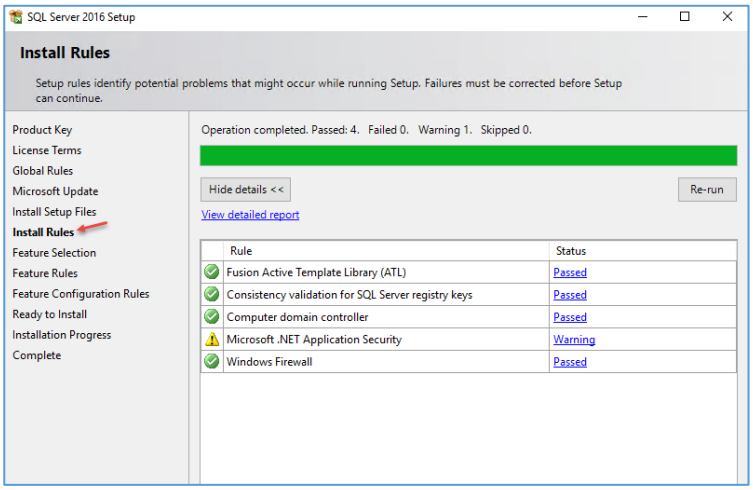
در این صفحه بر روی Export configuration settings کلیک کنید.



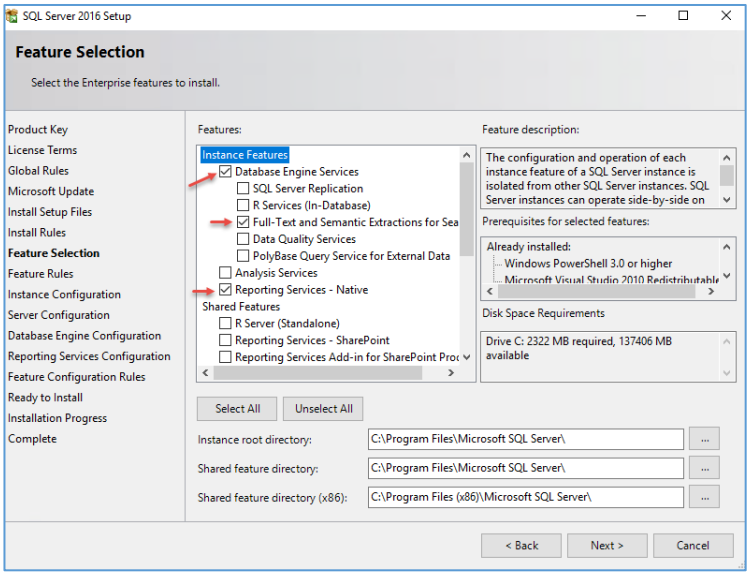
در این قسمت، آدرس مورد نظر را که از قبل کپی کردید، وارد و بر روی OK کلیک کنید و در صفحه‌ی بعد بر روی Install کلیک کنید تا Net 3.5 بر روی سرور نصب شود.



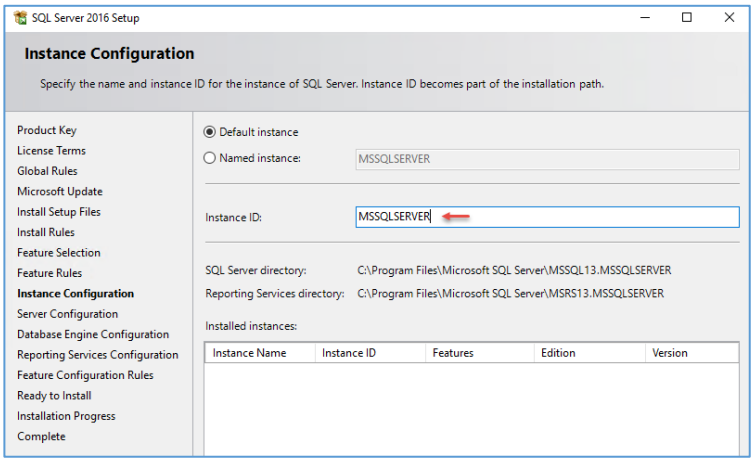
بعد از دانلود، دوبار بر روی فایل Setup کلیک کنید و در شکل باز شده‌ی روبرو به قسمت Installation مراجعه کنید و بر روی New SQL Server stand-alone کلیک کنید.



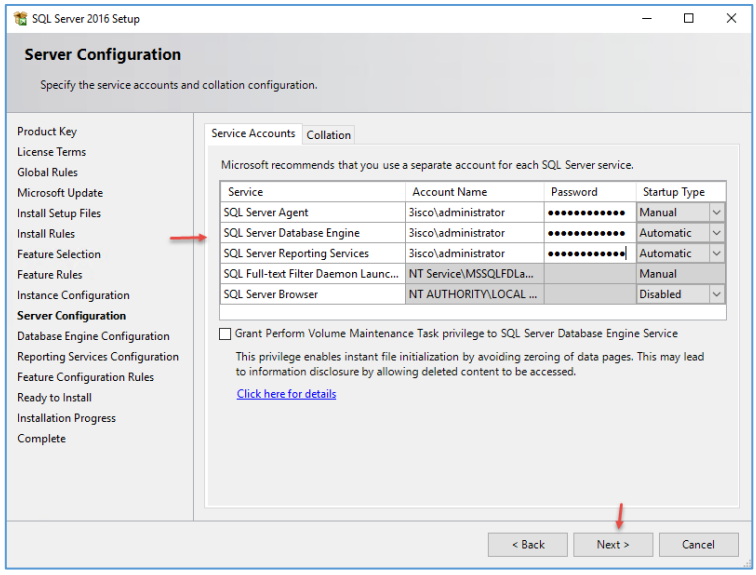
بر روی Next کلیک کنید تا به این صفحه برسید، در این صفحه، اگر خطایی نداشتید بر روی Next کلیک کنید، اصولاً اگر در این قسمت فایروال را تنظیم نکرده باشید و Net3.5 را نصب نکرده باشید با خطا روبرو می‌شوید که این کار را قبلاً انجام دادیم.



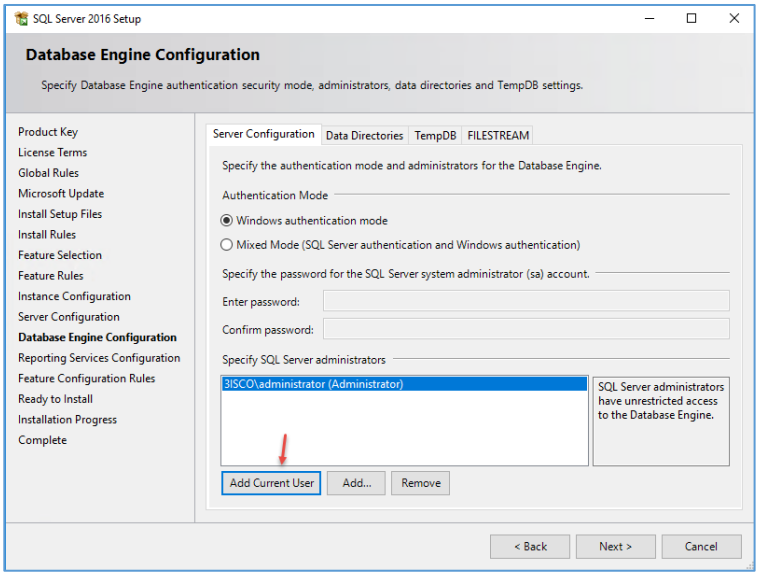
در قسمت Feature Selection، سرویس‌های مورد نظر خود را انتخاب کنید که باید از لیست روبرو گزینه‌های مشخّص‌شده را انتخاب و بر روی Next کلیک کنید.



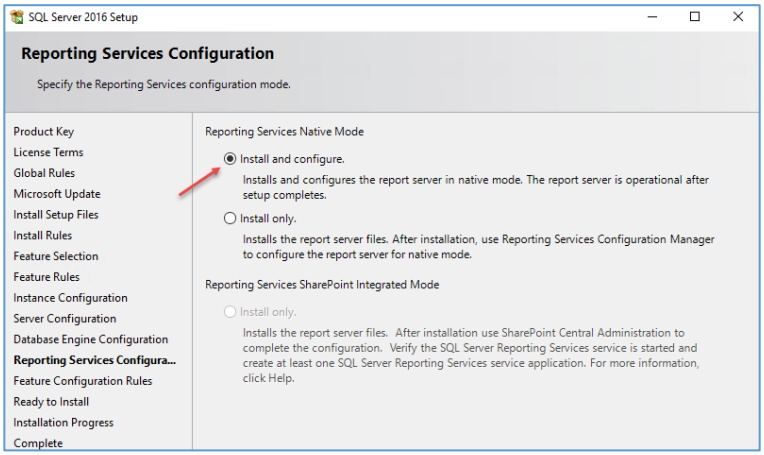
در این صفحه باید Instance خود را مشخّص کنید که به صورت پیش‌فرض، MSSQLSERVER تعریف شده است و اگر برای اوّلین بار است که اقدام به نصب SQL می‌کنید، این نام فعّال می‌شود، امّا اگر از قبل SQL نصب کرده باشید باید یک Instance جدید تعریف کنید، اگر زیاد با SQL کار نکردید، می‌توانید کتاب آموزشی آن را از اینجا دانلود کنید.



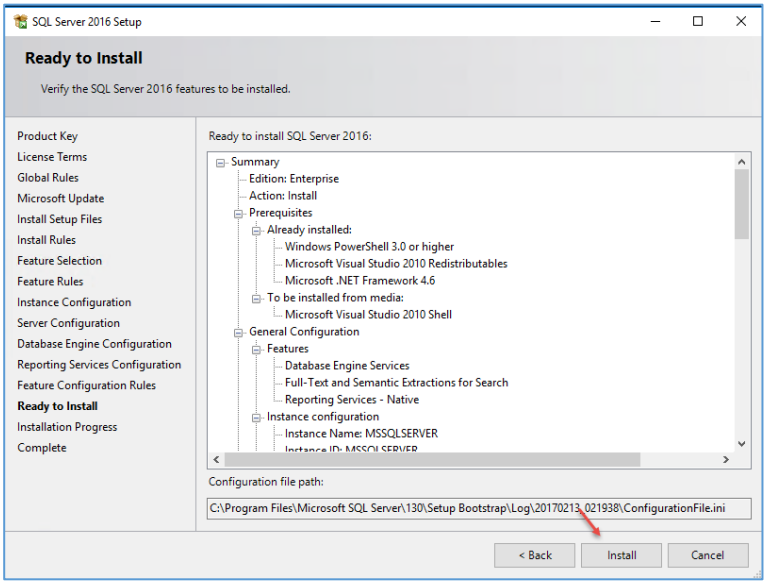
در این قسمت باید برای سرویس‌های مورد نظر، یک کاربر با دسترسی بالا وارد کنید که در سه سرویس اوّل، کاربر Administrator به صورت 3isco\administrator وارد شده است که دسترسی کامل دارد، بعد از این کار بر روی Next کلیک کنید.



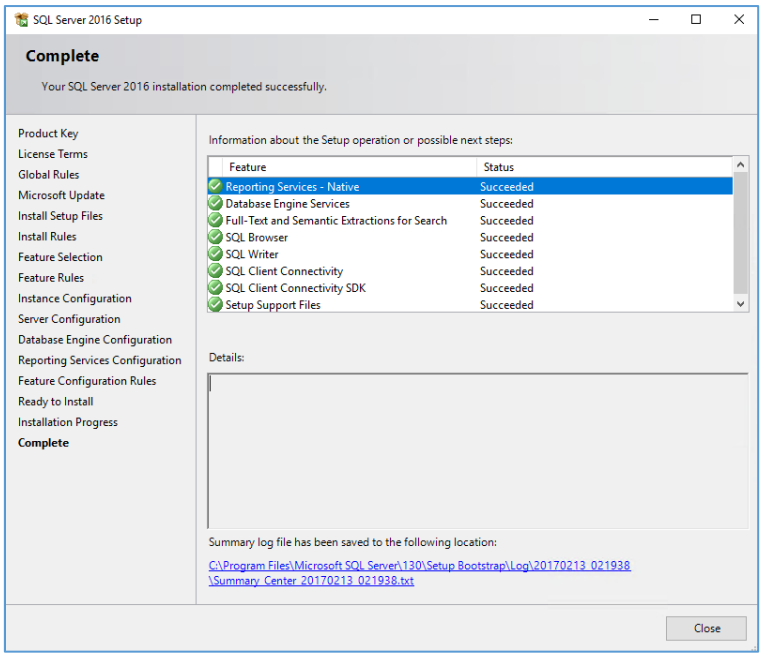
در این قسمت باید کاربر Admin نرم‌افزار SQL را مشخّص کنید که اگر با کاربر Admin یا با کاربری که دسترسی کامل به شبکه دارد، در حال نصب SQL هستید، می‌توانید بر روی Add Current User کلیک کنید و یا اگر می‌خواهید کاربر دیگری را به لیست اضافه کنید باید بر روی Add کلیک کنید.



در این صفحه، گزینه‌ی اوّل، یعنی Install and Configure را انتخاب و بر روی Next کلیک کنید.



در این صفحه، اگر تنظیمات مورد قبول شما است، بر روی Install کلیک کنید تا SQL نصب شود.



همانطور که مشاهده می‌کنید، نرم‌افزار SQL به صورت کامل بر روی سرور نصب شده است، بعد از نصب، سرور را Restart کنید.

مرحله‌ی سوم – نصب ابزارهای مورد نیاز:

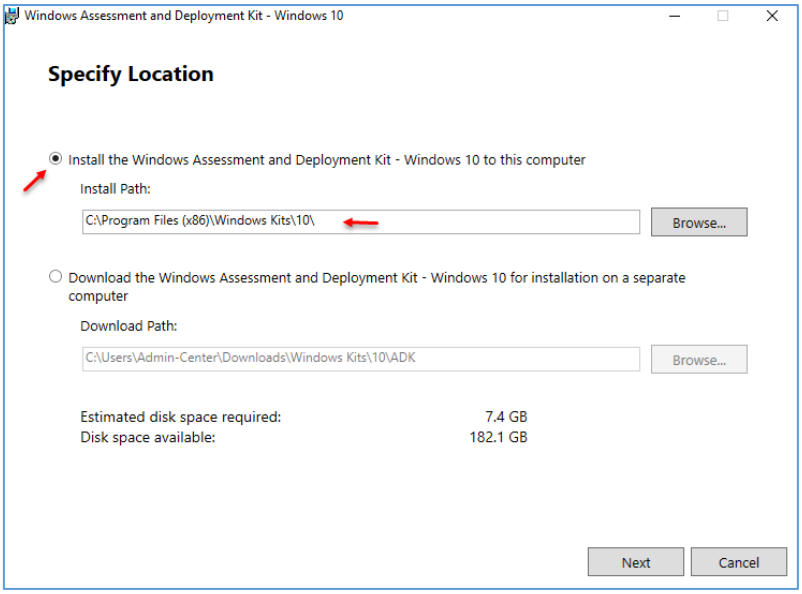
در این مرحله، قبل از نصب نرم‌افزار باید یک‌سری از کامپوننت‌ها و ابزارهای مورد نیاز نصب شود.

برای این کار، نرم‌افزار ADK را از آدرس زیر دانلود کنید:

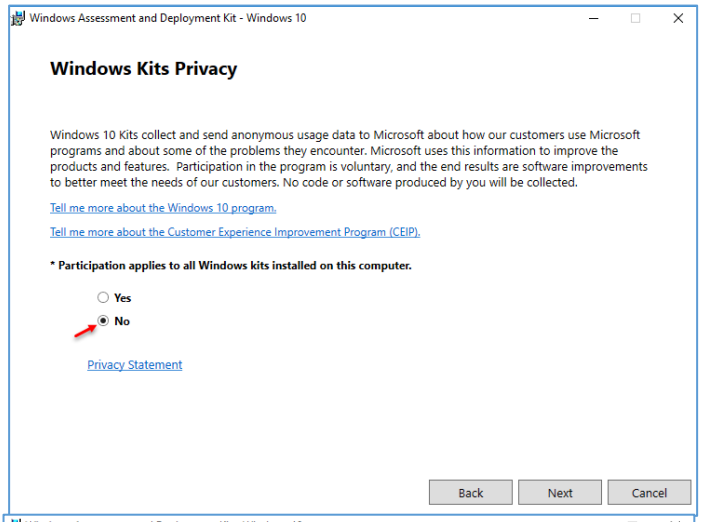
https://developer.microsoft.com/en-us/windows/hardware/windows-assessment-deployment-kit

توجّه کردید که مراحل نصب SQL که در بالا انجام دادیم، دقیقاً همان مراحل نصب نرم‌افزار Microsoft.System.Center. Operations.Manager است.

نکته: قبل از اجرای نرم‌افزار، سرور Center را به اینترنت متّصل کنید.

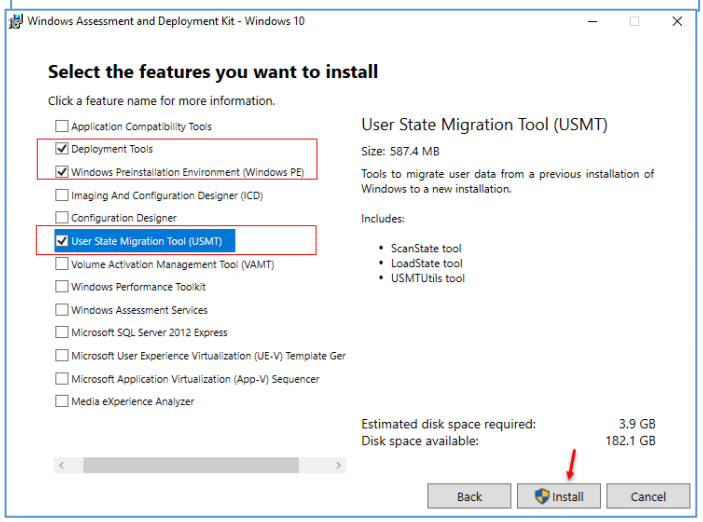


به مانند شکل روبرو نرم‌افزار ADK را اجرا کنید، اگر برای اوّلین بار است که می‌خواهید این کار را انجام دهید، گزینه‌ی اوّل را انتخاب کنید که فضایی معادل ۷٫٤ گیگابایت نیاز دارد تا تمام کامپیوننت‌ها دانلود شوند و در آدرس مشخّص شده قرار گیرند، امّا اگر از قبل دانلود کردید، می‌توانید گزینه‌ی دوّم را انتخاب و آدرس را مشخّص کنید.



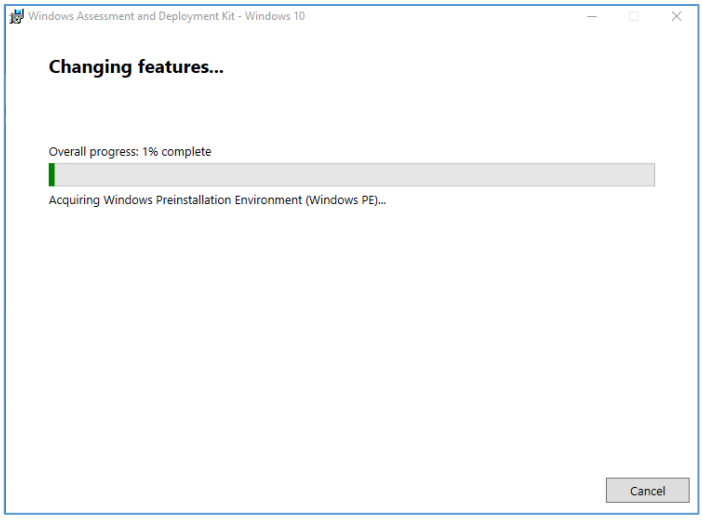
در این صفحه، گزینه‌ی No را انتخاب کنید و بر روی Next کلیک کنید.

در صفحه‌ی بعد بر روی Accept کلیک کنید.

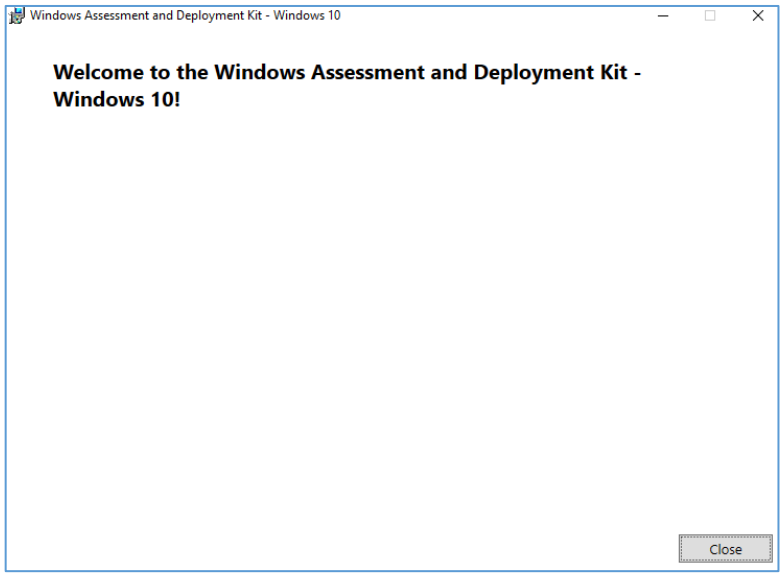


در این صفحه باید گزینه‌های مشخّص شده در لیست را انتخاب کنید، توجّه داشته باشید که حجم این سه گزینه، ۳٫۹ گیگابایت است که از طریق اینترنت دانلود خواهد شد و به همین مقدار باید فضا برای ذخیره‌سازی در اختیار داشته باشید.

در حال دانلود...

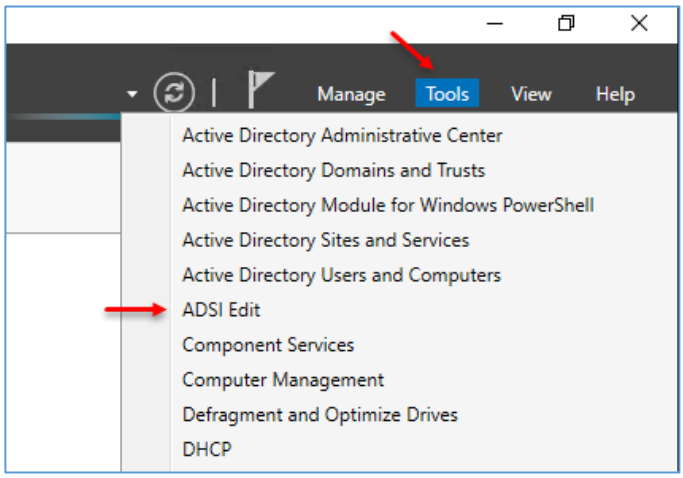


در این صفحه، کار دانلود به پایان رسید، بر روی close کلیک کنید.

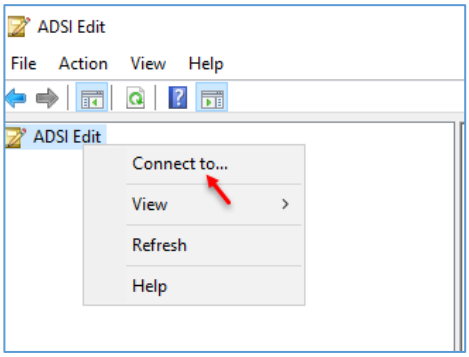


مرحله‌ی چهارم – کار با سرویس ADSI:

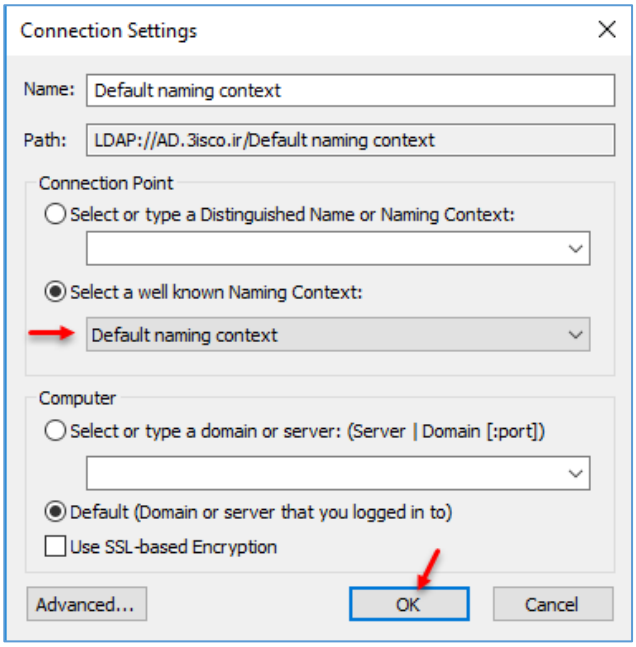
در این مرحله باید یک شی در سرویس ADSI با نام System Management ایجاد کنید و دسترسی‌های لازم را به آن دهید تا نرم‌افزار System Center بتواند بر روی سرور نصب شود و به Active Directory دسترسی داشته باشد.



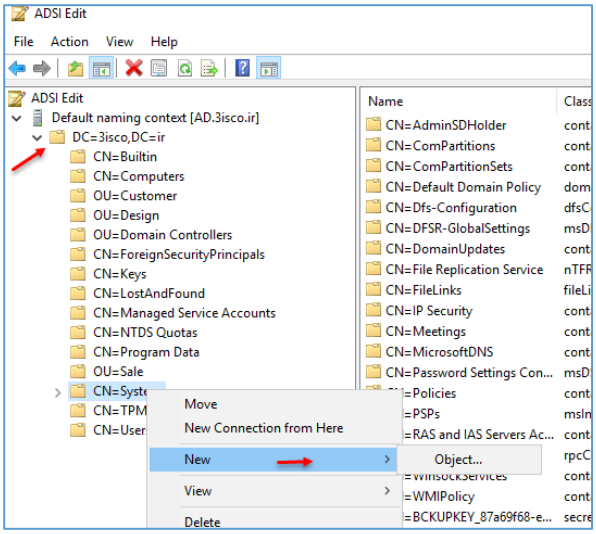
به مانند شکل روبرو وارد Server Manager شوید و سرویس ADSI را اجرا کنید.



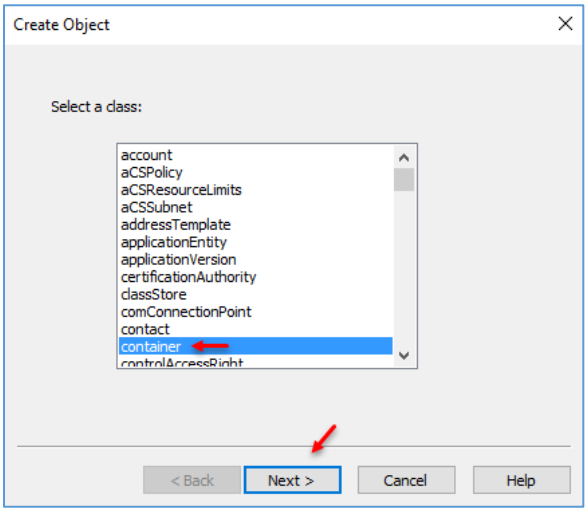
بعد از اجرا شدن سرویس، به مانند شکل روبرو بر روی ADSI Edit کلیک راست کنید و بر روی گزینه‌ی Connect to... کلیک کنید.



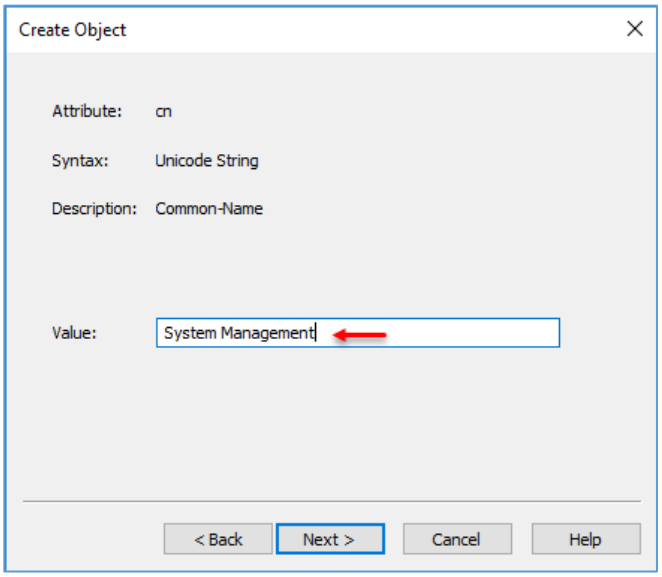
در این قسمت، گزینه‌ی Default naming context را انتخاب و بر روی OK کلیک کنید.



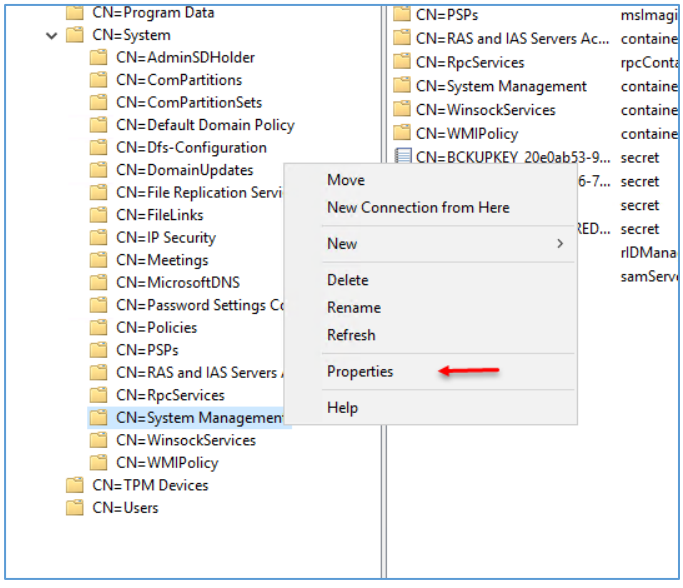
در این صفحه، به مانند شکل بر روی گزینه‌ی System کلیک راست کنید و از قسمت New، گزینه‌ی Object را انتخاب کنید.



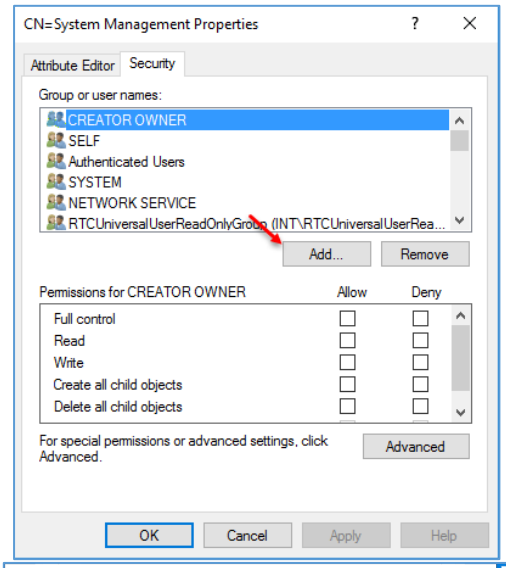
در این قسمت، گزینه‌ی Container را انتخاب و بر روی Next کلیک کنید.



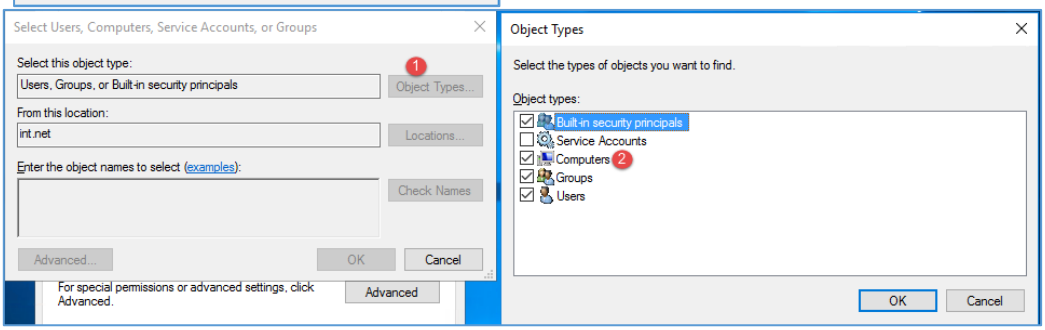
در این قسمت، نام System Management را وارد و بر روی Next کلیک کنید و در صفحه‌ی آخر بر روی Finish کلیک کنید تا شی مورد نظر ایجاد شود.



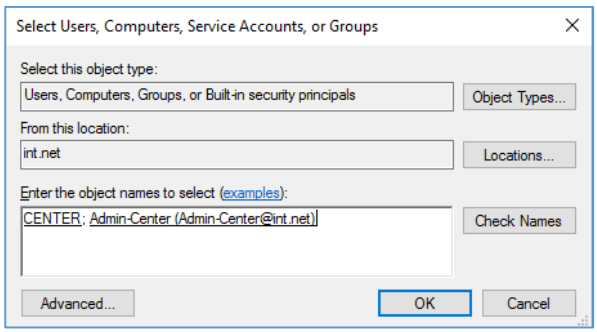
بعد از ایجاد گزینه‌ی مورد نظر، به مانند شکل روبرو بر روی آن کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



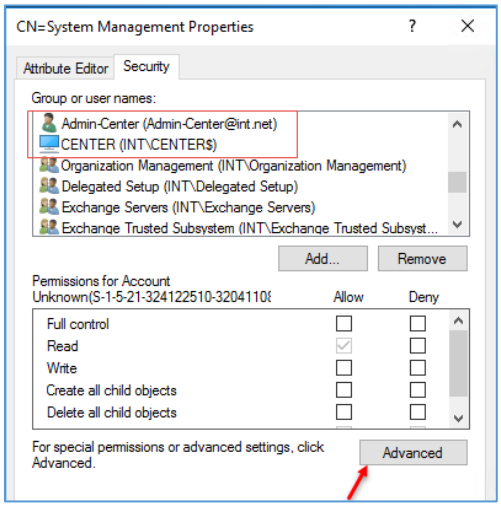
در این صفحه باید کاربر جدید خود را که دسترسی‌های لازم را به آن دادید، به لیست اضافه کنید و همچنین باید نام سیستم Center را به لیست اضافه کنید و دسترسی لازم را به آنها بدهید، برای این کار بر روی Add کلیک کنید.



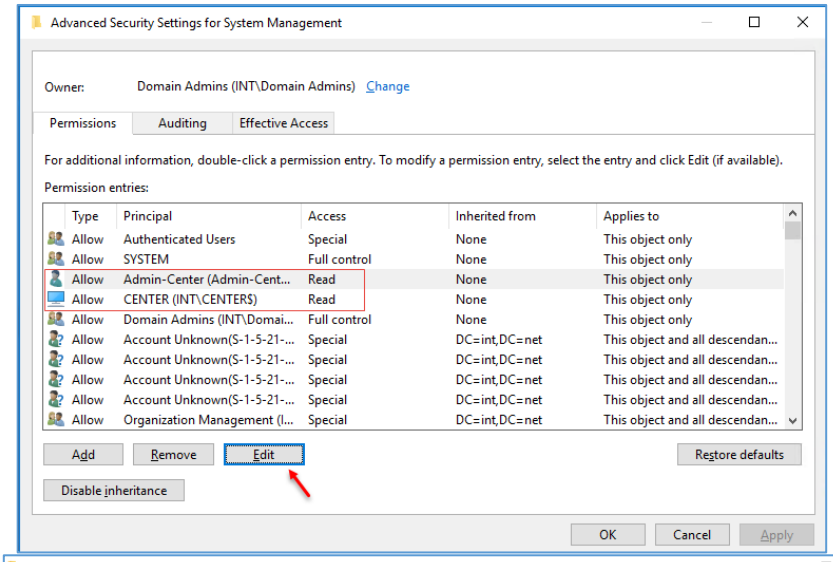
در این صفحه، اوّل بر روی Object Types کلیک کنید و گزینه‌ی Computers را انتخاب کنید.



به مانند شکل، نام سیستم و نیز نام کاربر را به لیست اضافه و بر روی OK کلیک کنید.

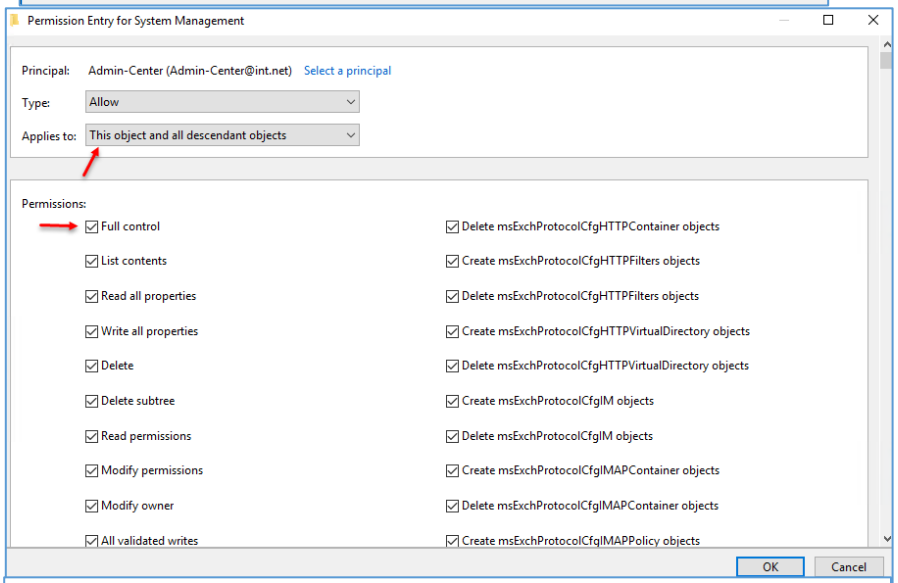


دو گزینه‌ی کاربر و سیستم در شکل روبرو در لیست قرار گرفته‌اند که برای تنظیمات بیشتر و دسترسی کامل به این شی باید بر روی Advanced کلیک کنید.

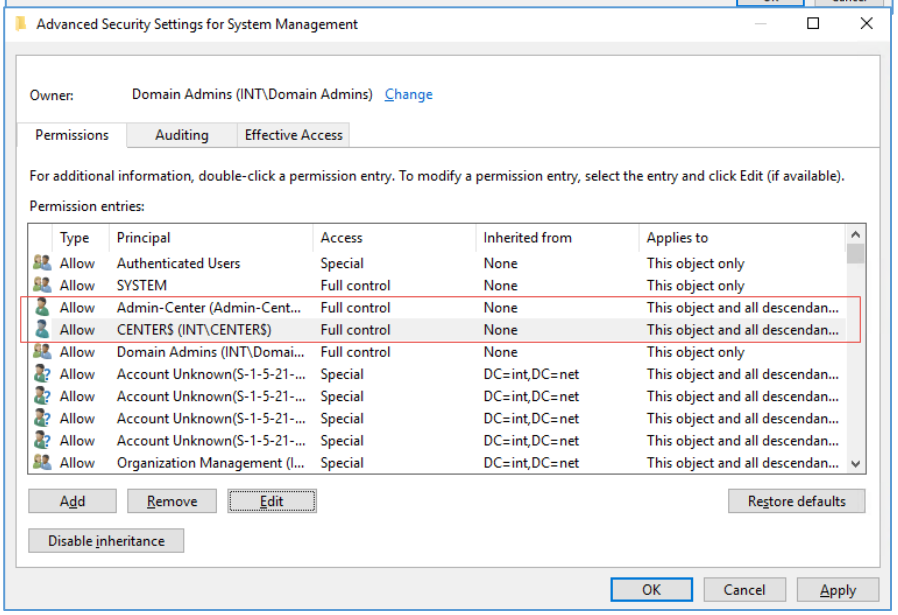


در این صفحه بر روی هر یک از گزینه‌های مشخّص شده کلیک و بعد بر روی Edit کلیک کنید.

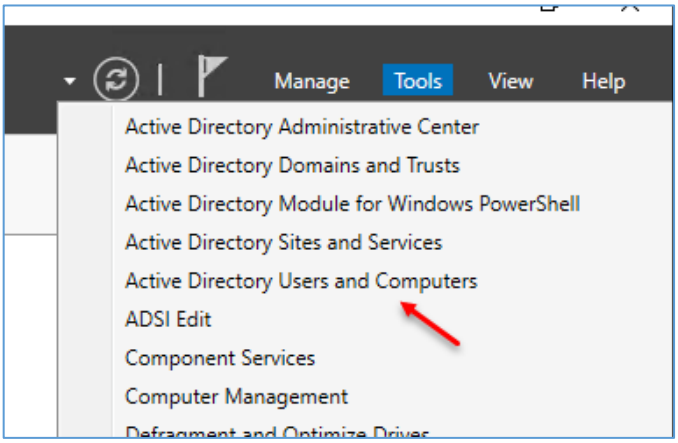
این کار باید بر روی هر دو گزینه انجام شود.



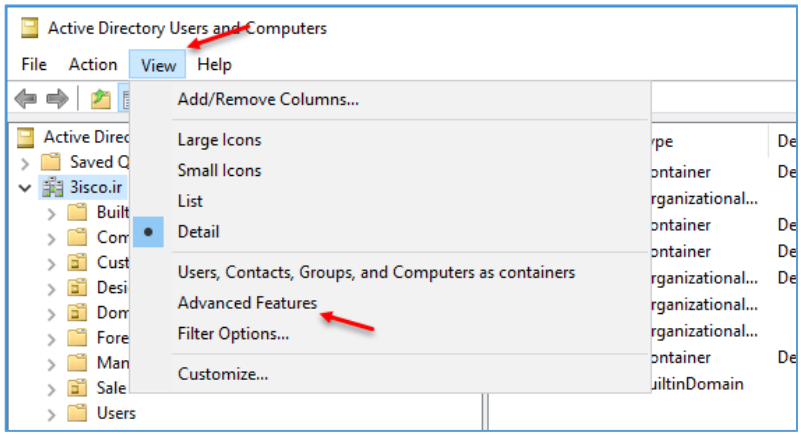
در این صفحه و از قسمت Applies to، گزینه‌ی... This object and all را انتخاب کنید و بعد، تیک گزینه‌ی Full Control را انتخاب کنید و بر روی OK کلیک کنید، دقیقاً همین کار را برای نام Center که نام سیستم است، انجام دهید.



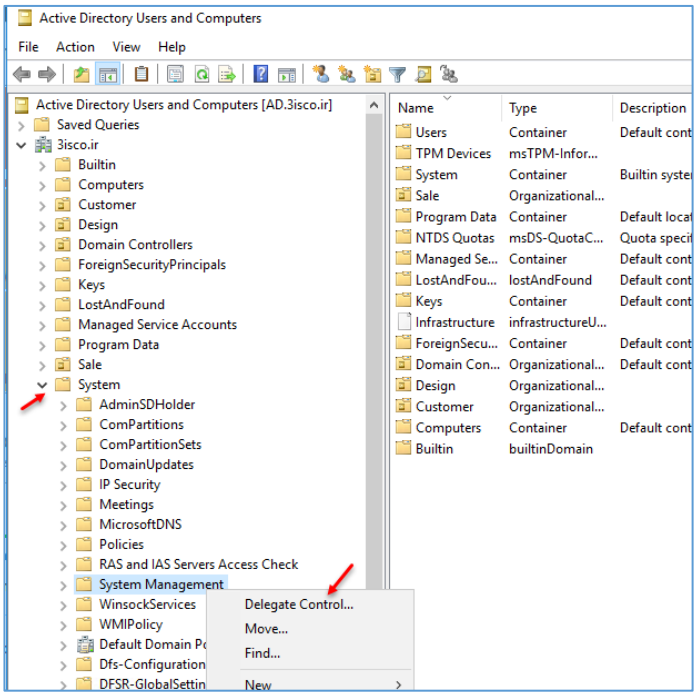
همانطور که مشاهده می‌کنید، به دو گزینه‌ی کاربر و سیستم دسترسی Full داده شده است.



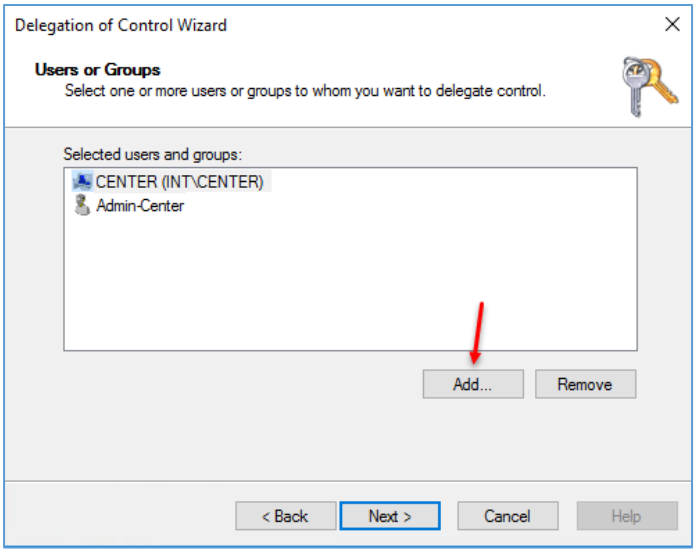
بعد از انجام مراحل بالا وارد Server Manager شوید و سرویس Active Dircetory Users and Computers را اجرا کنید.



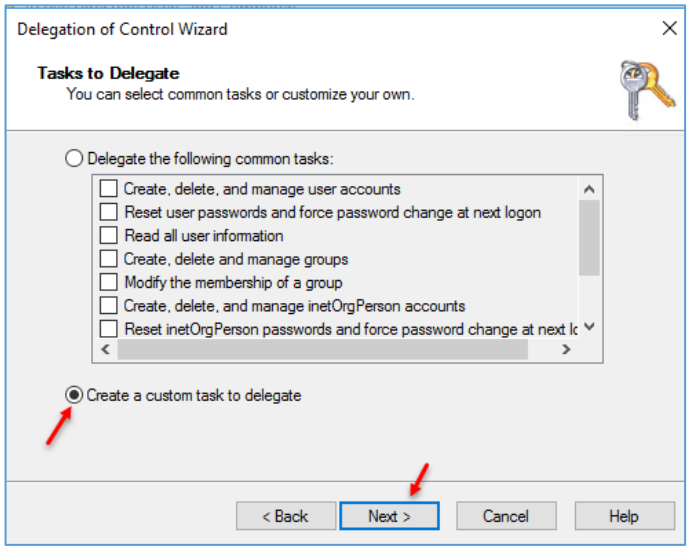
بعد از اجرای سرویس وارد منوی View شوید و بر روی گزینه‌ی Advanced Features کلیک کنید تا تنظیمات پیشرفته باز شود.



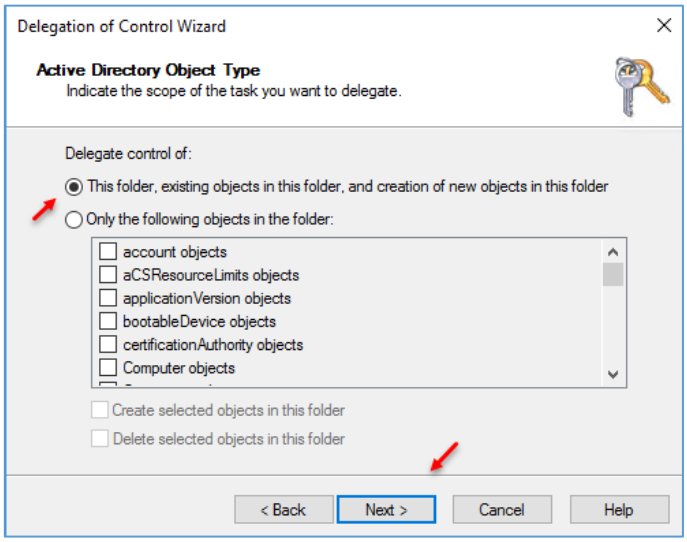
در این صفحه و از قسمت System بر روی گزینه‌ی جدید، System Management کلیک راست کنید و گزینه‌ی Delegate Control را انتخاب کنید.



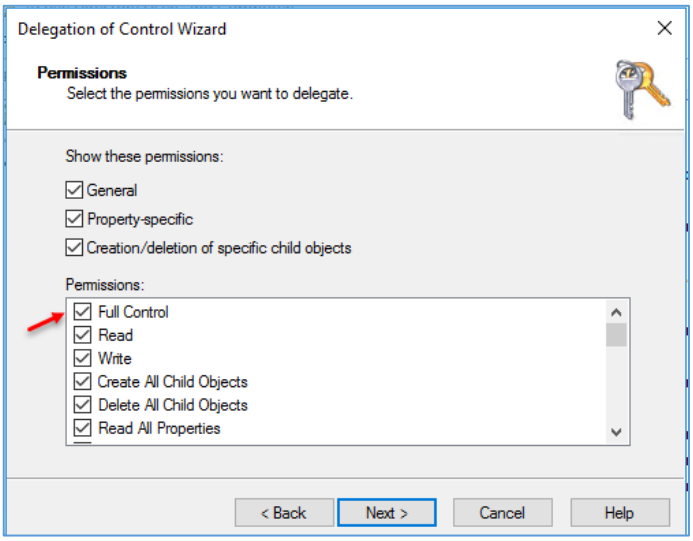
به مانند شکل روبرو بر روی Add کلیک کنید و کاربری را که با آن قصد دارید، نرم‌افزار را نصب کنید به لیست اضافه کنید و نیز نام سیستم را به لیست اضافه کنید و بر روی Next کلیک کنید.



در این قسمت، گزینه‌ی Create a coustom task to delegate را انتخاب و بر روی Next کلیک کنید.

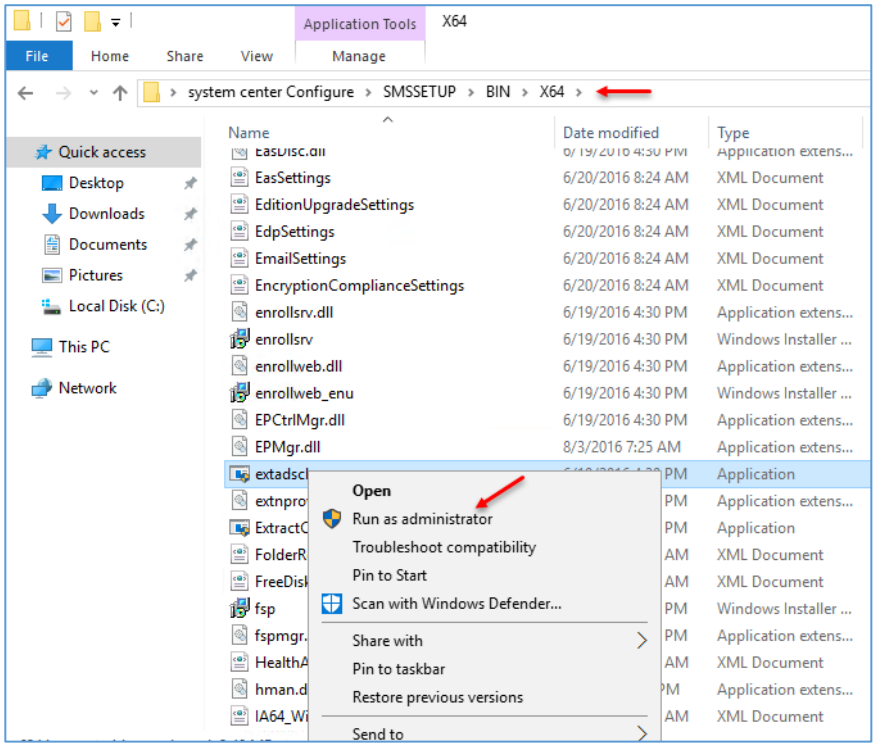


در این صفحه بر روی Next کلیک کنید.

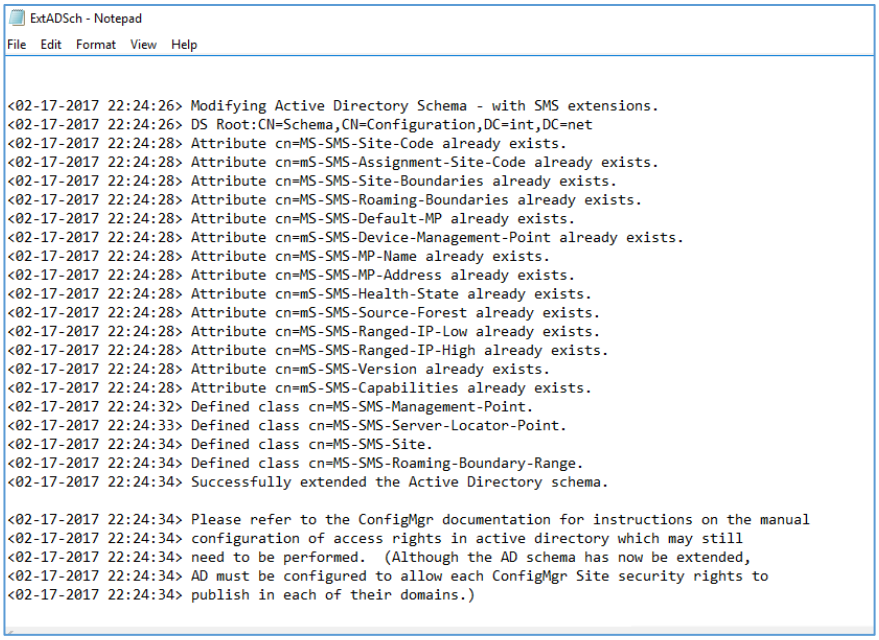


در این قسمت، گزینه‌ی Full Control را انتخاب و بر روی Next کلیک کنید و در صفحه‌ی آخر بر روی Finish کلیک کنید.

بعد از دادن دسترسی‌ها وارد سرور Center شوید و بعد وارد پوشه‌ی برنامه‌ی Systemn Center Configure شوید و بعد از آن وارد آدرس زیر شوید:



به مانند شکل وارد آدرس مورد نظر شوید و بر روی فایل extadsch کلیک راست کنید و گزینه‌ی Run as administrator را انتخاب کنید، با این کار تنظیمات نرم‌افزار در Active Directory اضافه می‌شود.



بعد از اجرای فایل بالا وارد درایو C شوید و فایل متنی ExtADSch را اجرا کنید، متوجّه خواهید شد که اطّلاعات به درستی در سرور Active Directory نصب شده است.

اگر در این قسمت با خطایی روبرو شدید، به طور قطع در جایی از تنظیمات اشتباهی رخ داده است.

مرحله‌ی پنجم – نصب ابزارها و پیش‌نیازها:

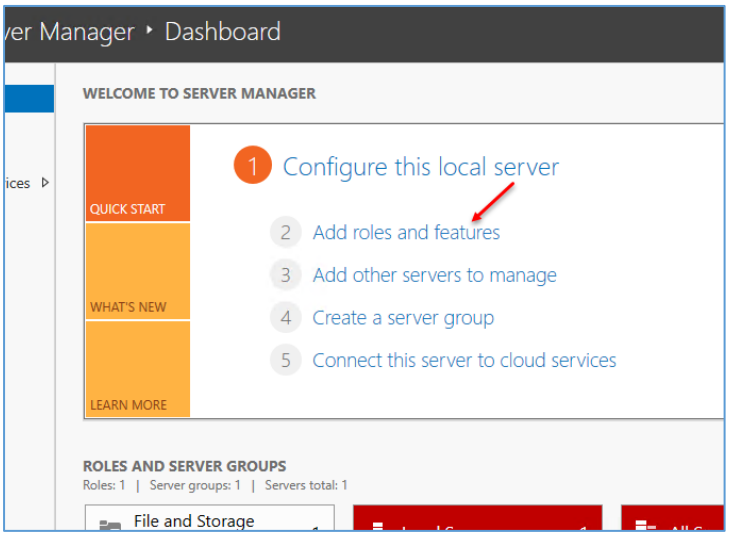
نصب Remote Desktop Connection Manager:

این ابزار را از لینک زیر می‌توانید دانلود کنید:

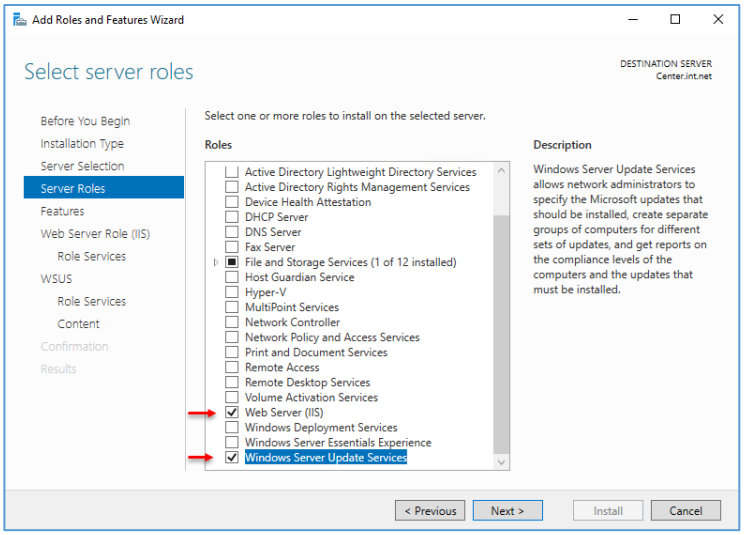
https://www.microsoft.com/en-us/download/details.aspx?id=44989

نصب این ابزار، ساده است و با اجرا کردن Setup و Next کردن به راحتی نصب خواهد شد.

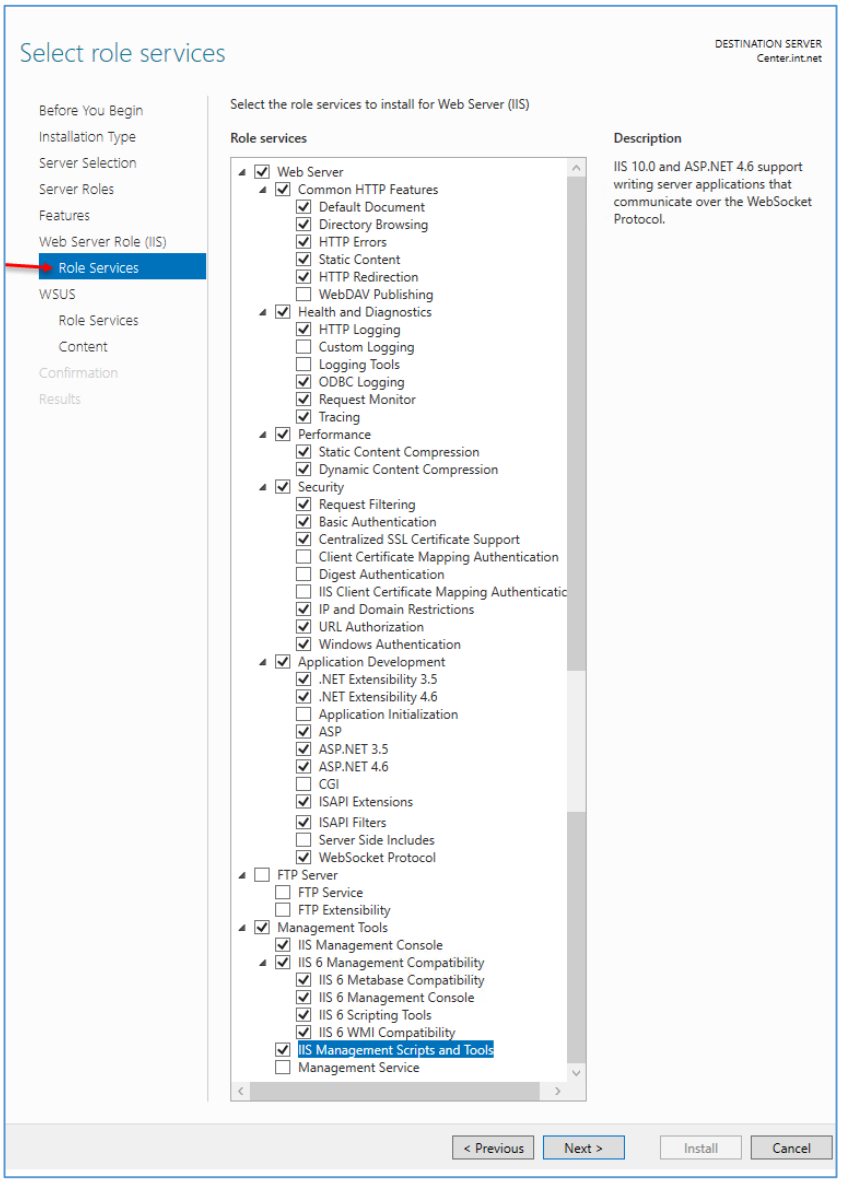
نصب سرویس WSUS، IIS و دیگر پیش‌نیازها:



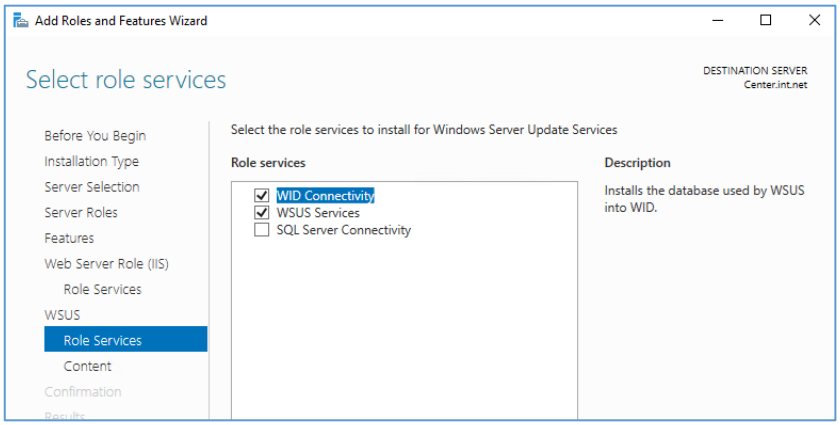
برای شروع کار وارد سرور Center شوید و Server Manager را اجرا کنید و بر روی Add Roles and Features کلیک کنید.



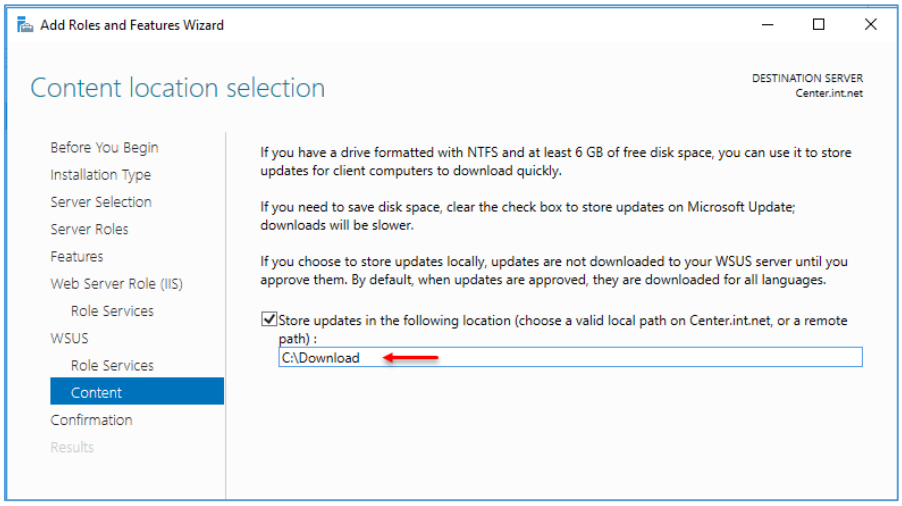
در قسمت Server Roles، تیک دو گزینه‌ی Web Server (IIS) و Windows Server Update Service را انتخاب و بر روی Next کلیک کنید.



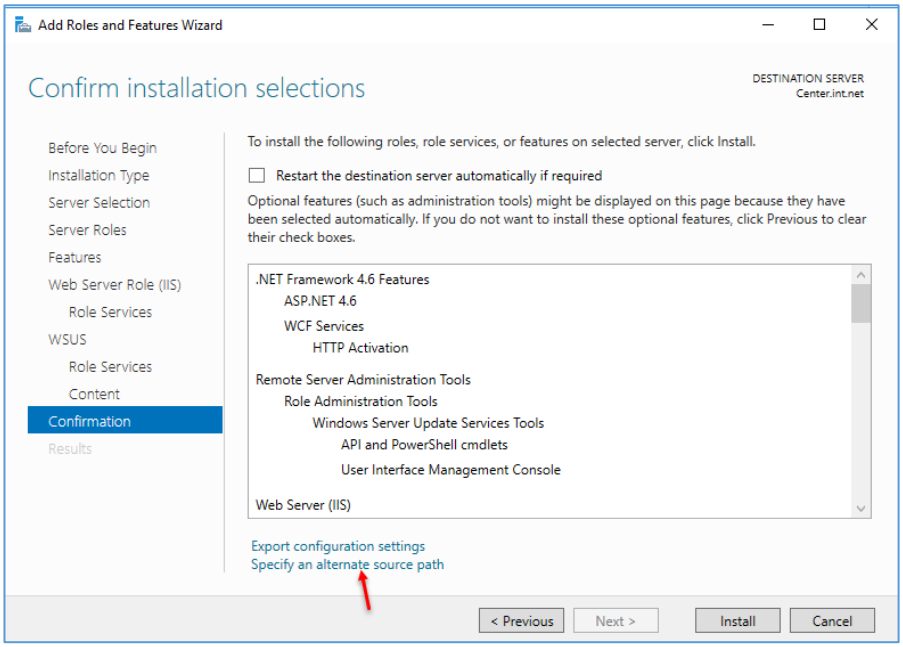
در صفحه‌ی Role Service، به مانند شکل روبرو تمام گزینه‌های مشخّص شده را انتخاب کنید، لطفاً در انتخاب گزینه‌ها دقّت کنید و بر روی Next کلیک کنید.



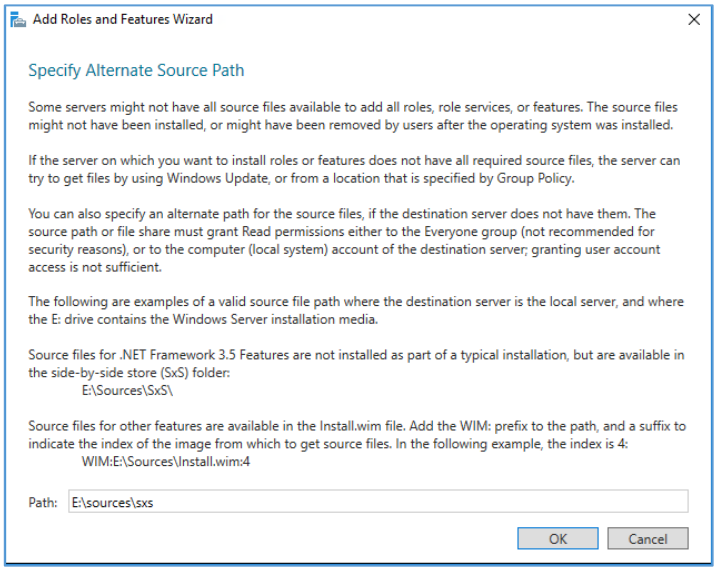
در این صفحه به گزینه‌ای دست نزنید وتنها بر روی Next کلیک کنید.



در این صفحه باید یک مسیر برای سرویس WSUS و یا همان، Update Service انتخاب کنید تا بتواند در این مسیر، فایل‌های آپدیت را ذخیره کند.



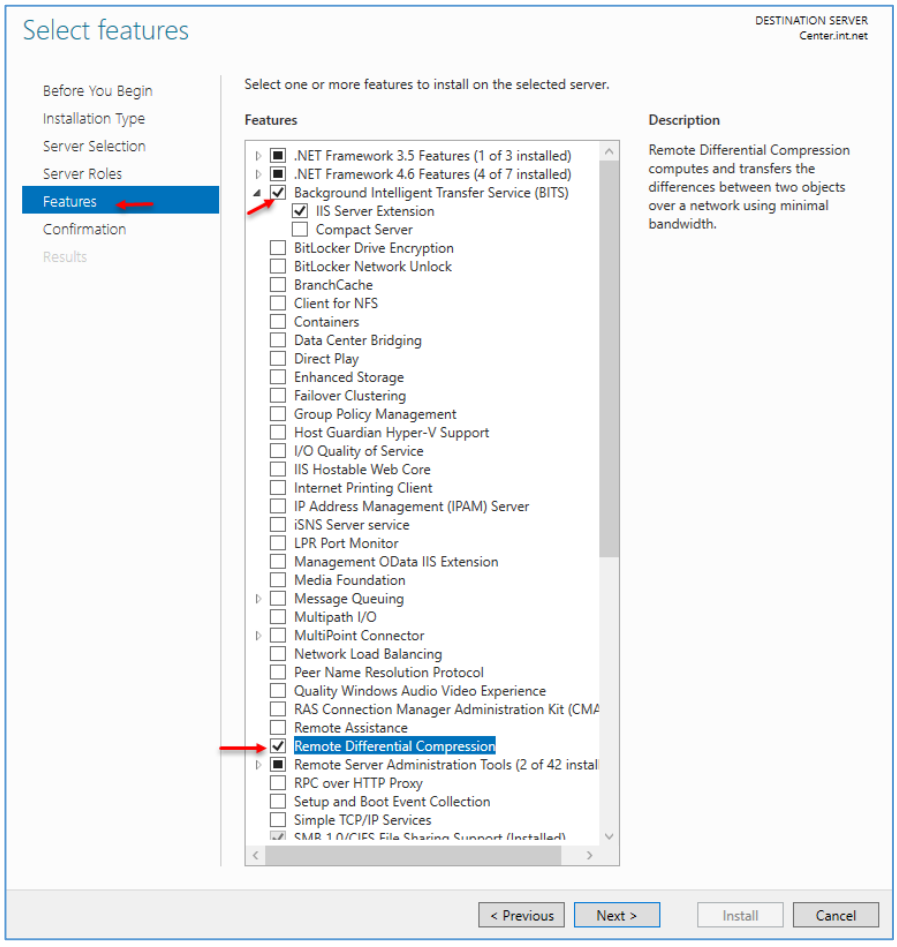
در این قسمت باید وارد DVD مربوط به Windows server 2016 شوید و آدرس مشخّصی را در قسمت Specify an alternate source path وارد کنید، برای انجام این کار بر روی گزینه‌ی مشخّص‌شده کلیک کنید.



در قسمت Path باید آدرس مشخّص‌شده را وارد و بر روی OK کلیک کنید.

بعد از آن بر روی Install کلیک کنید تا کار نصب آغاز شود.

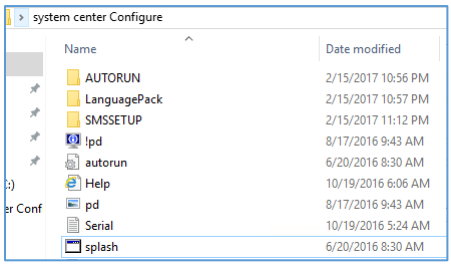
بعد از نصب، سرور را Restart کنید.



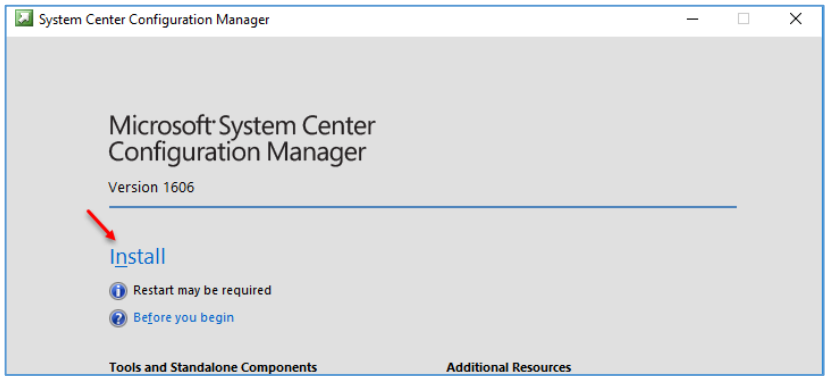
بعد از نصب پیش‌نیازهای صفحه‌ی قبل و اجرا شدن سرور، دوباره وارد Server Manager شوید و از قسمت Features، به مانند شکل روبرو گزینه‌های مورد نظر را انتخاب و بر روی Next کلیک کنید.

بعد از نصب، سرور را Restart کنید تا کار نصب نهایی آغاز شود.

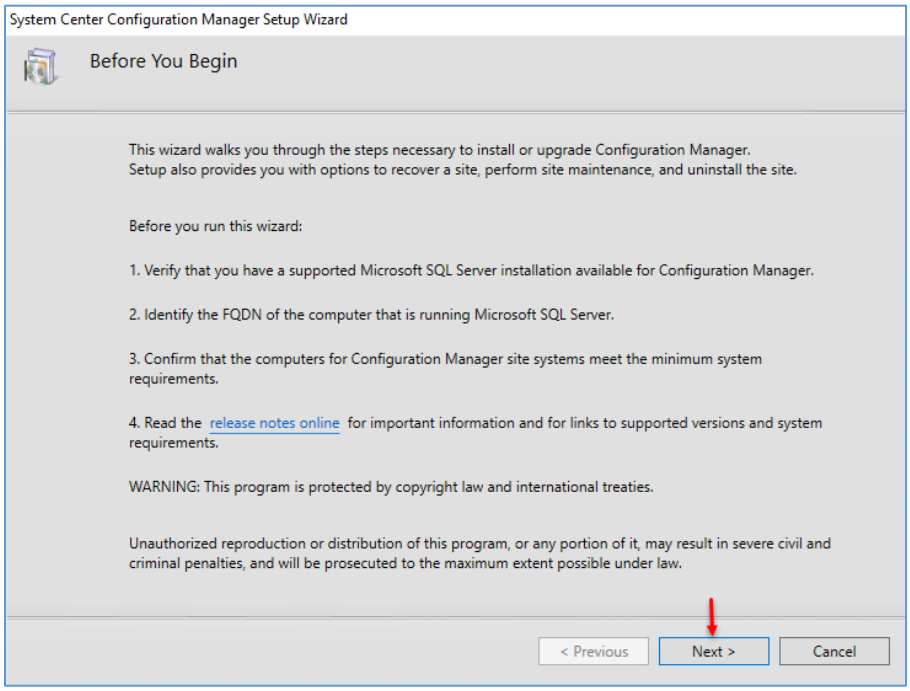
مرحله‌ی آخر – نصب System Center Configure Manager:



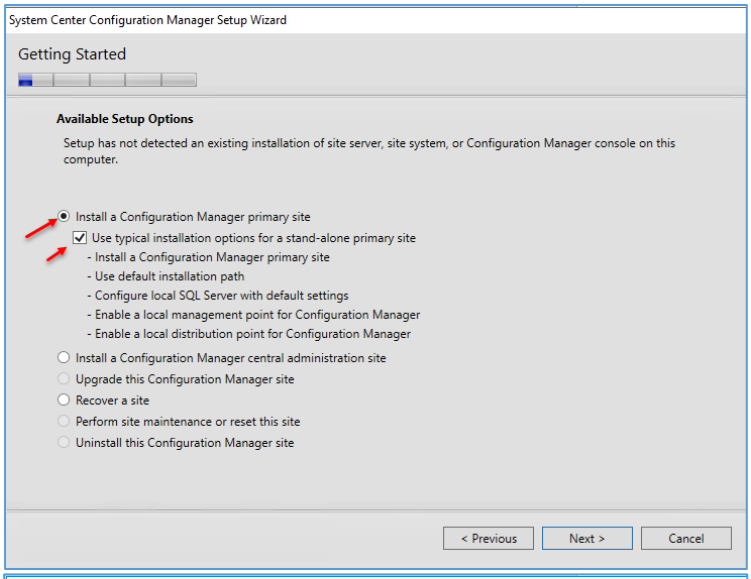
بعد از انجام تمام مراحل بالا، نوبت به نصب نرم‌افزار می‌رسد، وارد پوشه‌ی آن شوید و فایل Splash را اجرا کنید.



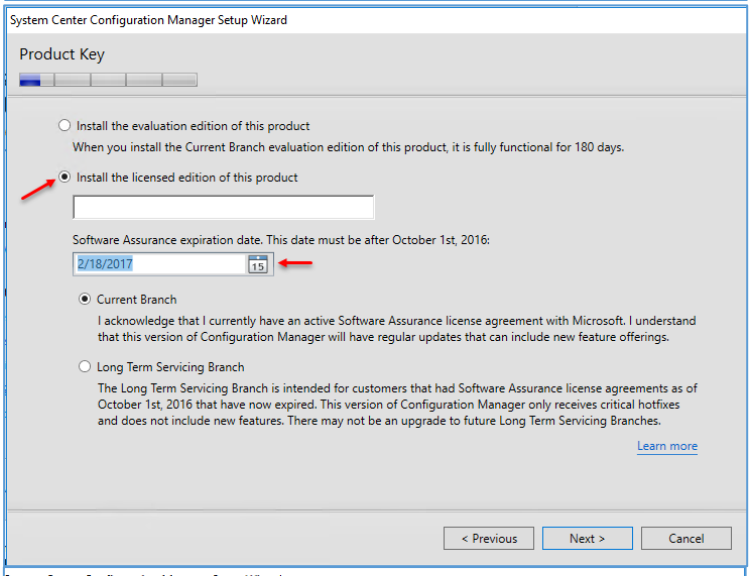
در این صفحه برای آغاز نصب بر روی Install کلیک کنید.



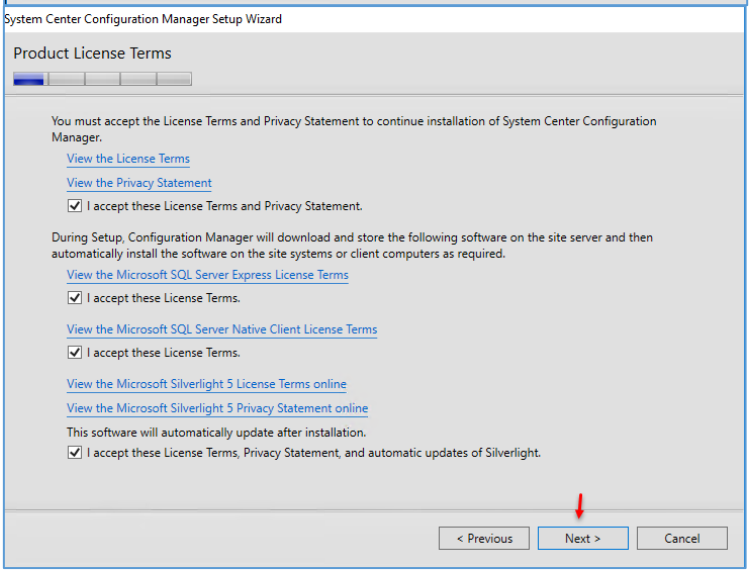
بر روی Next کلیک کنید.



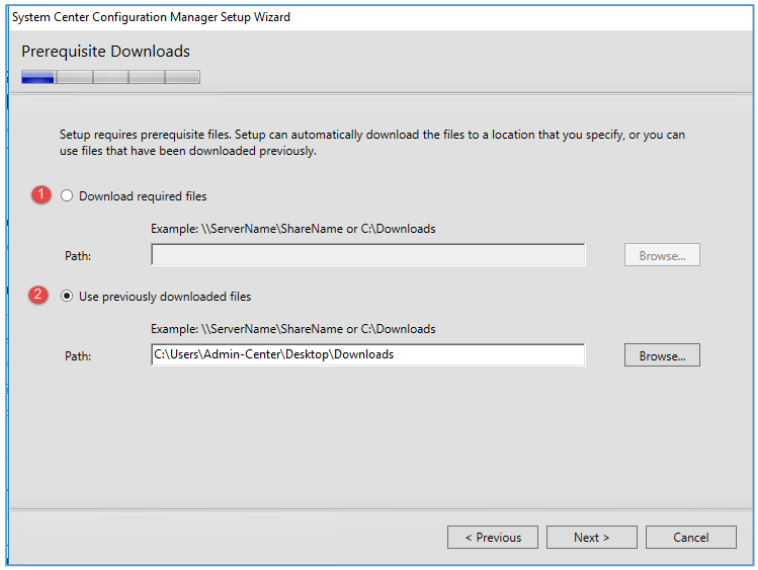
در این صفحه، اگر برای اوّلین بار می‌خواهید System Center Configure را نصب کنید، گزینه‌ی اوّل را انتخاب کنید و اگر تمام سرویس‌ها و نرم‌افزارهای پیش‌نیاز بر روی یک سرور نصب شده است، می‌توانید تیک گزینه‌ی Use typical Install ation... را انتخاب و بر روی Next کلیک کنید.



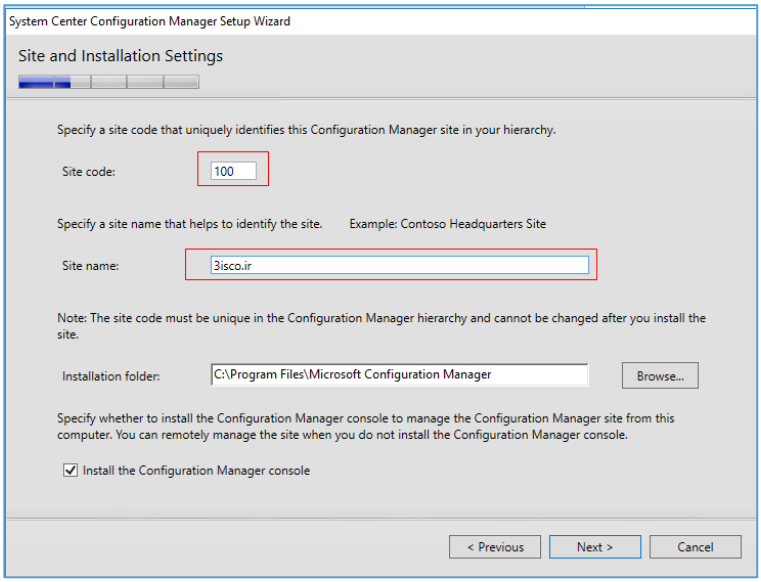
در این صفحه، لایسنس نرم‌افزار را در قسمت مشخّص‌شده وارد و تاریخ همان روز را برای آن ثبت کنید و بر روی Next کلیک کنید.



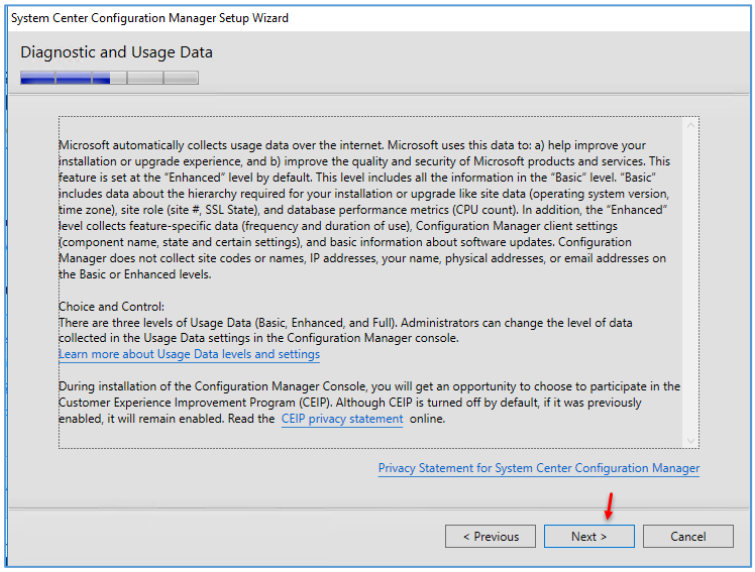
توافقنامه را بعد از مطالعه، تأیید کنید و بر روی Next کلیک کنید.



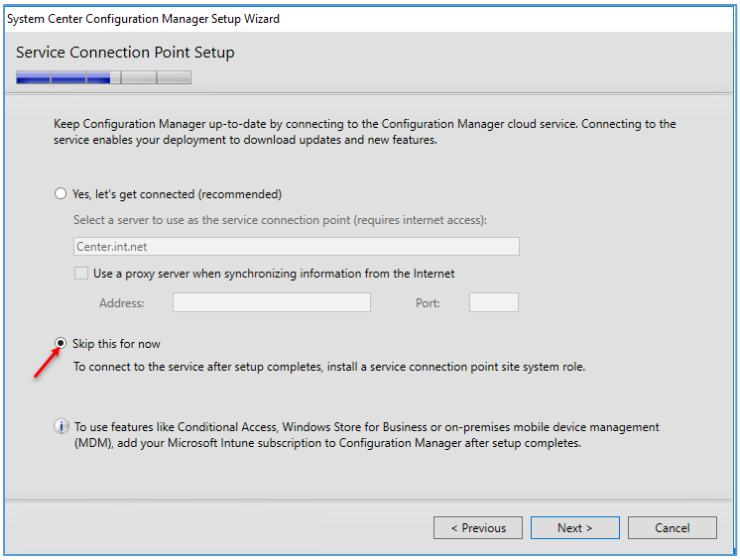
در این صفحه، نرم‌افزار نیاز به پیش‌نیازهایی دارد که باید از اینترنت دریافت شود، اگر گزینه‌ی یک را انتخاب کنید باید برای نرم‌افزار، یک مسیر در هارد مشخّص کنید که بعد از **Next**، حدوداً ۷۷۰ مگابایت فایل را دانلود می‌کند و در مسیر مشخّص‌شده قرار می‌دهد، اگر چنانچه این فایل را قبلاً دانلود کردید، آدرس آن را در قسمت شماره‌ی دو وارد کنید و بر روی **Next** کلیک کنید.



در این صفحه برای سایت خود، به دلخواه یک شماره‌ی سه رقمی وارد کنید که در اینجا، ۱۲۰ وارد شده است، در قسمت **Site name** نیز نام سایت خود را به دلخواه وارد کنید و در قسمت آخر، محلّ ذخیره‌سازی اطّلاعات را مشخّص کنید.

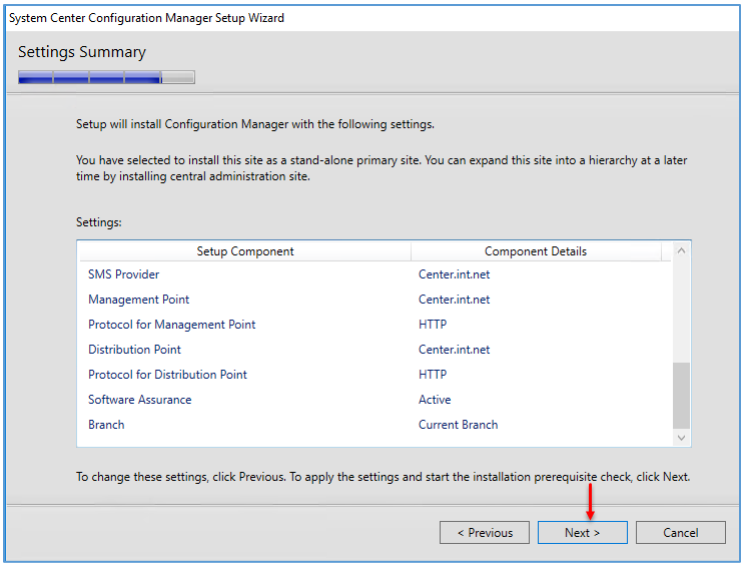


بر روی **Next** کلیک کنید.

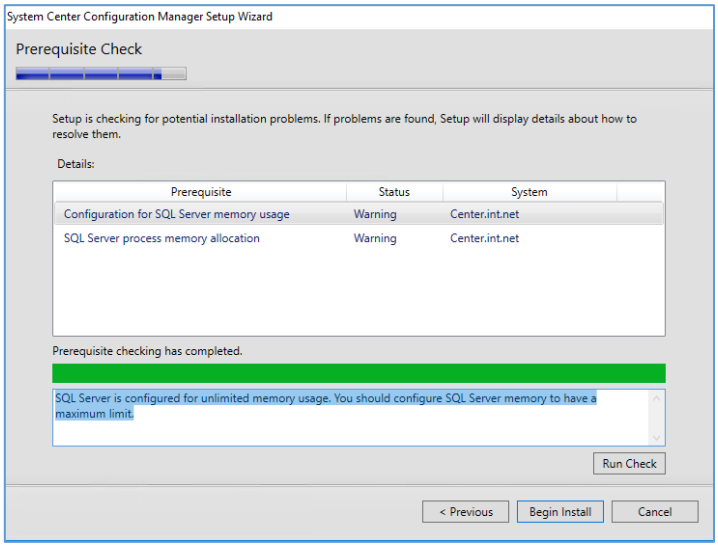


در این قسمت، گزینه‌ی Skip this for now را انتخاب و بر روی Next کلیک کنید.

اگر گزینه‌ی اوّل را انتخاب می‌کردید، قبل از راه‌اندازی، سایت مورد نظر تست می‌شد که با اخطار مواجه می‌شدید.

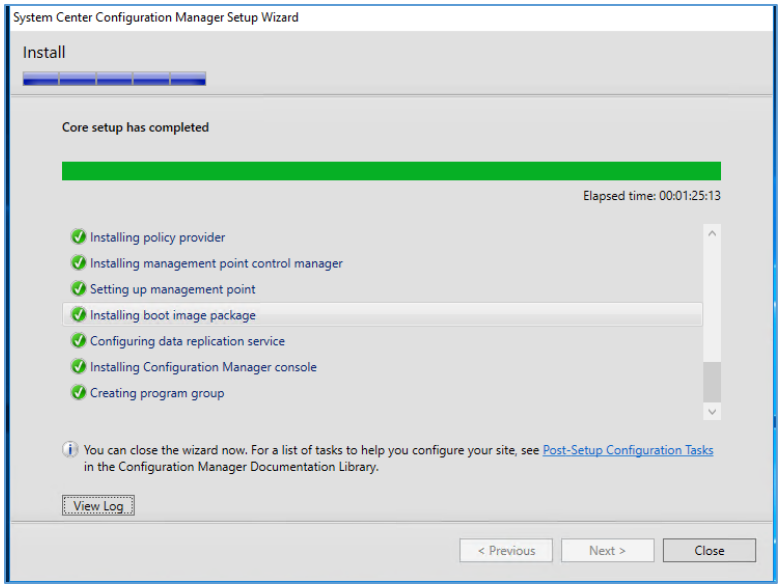


در این صفحه، اگر تنظیمات درست بود، بر روی Next کلیک کنید.



در این صفحه، پیش‌نیازها بررسی خواهد شد که اگر با گزینه‌ی Faild روبرو شوید، یعنی آن گزینه را نصب و یا فعّال نکردید، در شکل روبرو تنها دو اخطار مشخّص شده است که آن نیز مربوط به SQL است، برای اینکه این اخطار را حل کنید باید به لینک زیر مراجعه کنید و حافظه‌ی SQL را افزایش دهید.

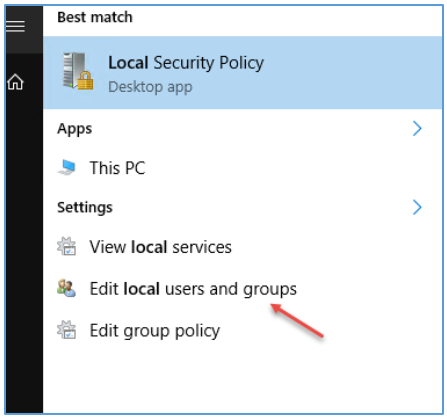
https://community.rackspace.com/products/f/18/t/1693



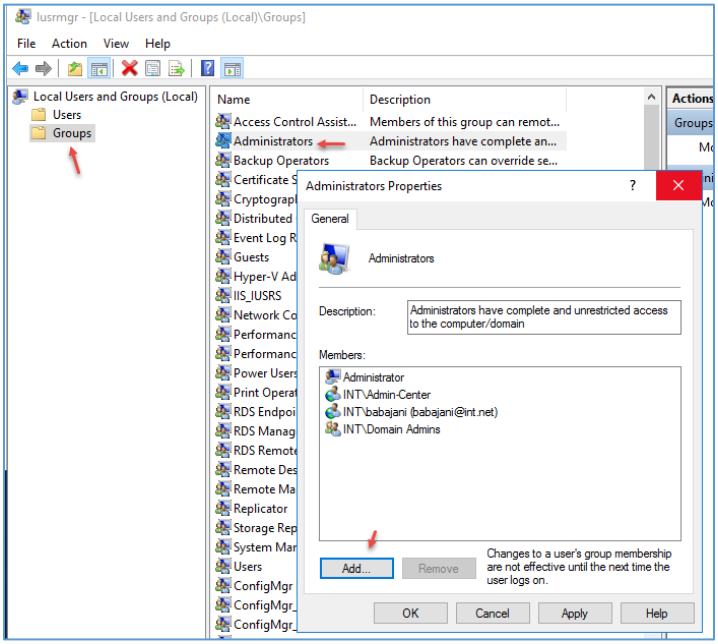
بعد از اتمام کار بر روی Begin Install کلیک کنید، همانطور که مشاهده می‌کنید، نرم‌افزار با موفّقیّت نصب شده است، البتّه بسته به نوع سخت‌افزار شما زمان‌بر خواهد بود.

سرور Center را Restart کنید.

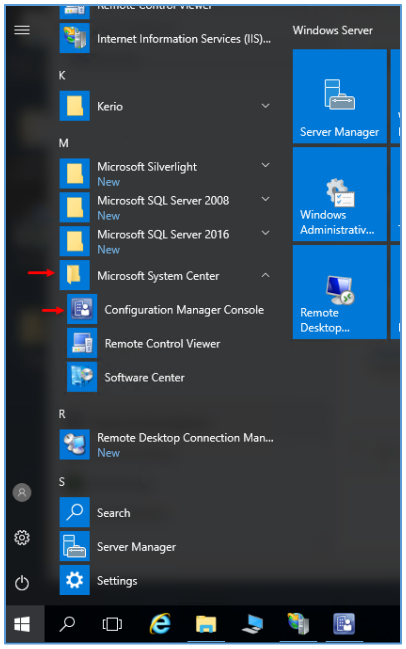
عضو کردن کاربر در گروه Administrators محلّی:



برای اینکه دسترسی کاربر به تمامی منابع در سرور اصلی کامل باشد باید آن را عضو گروه Administrators در سرور Center کنید، برای این کار در Start، ابزار Edit local users and group را اجرا کنید.

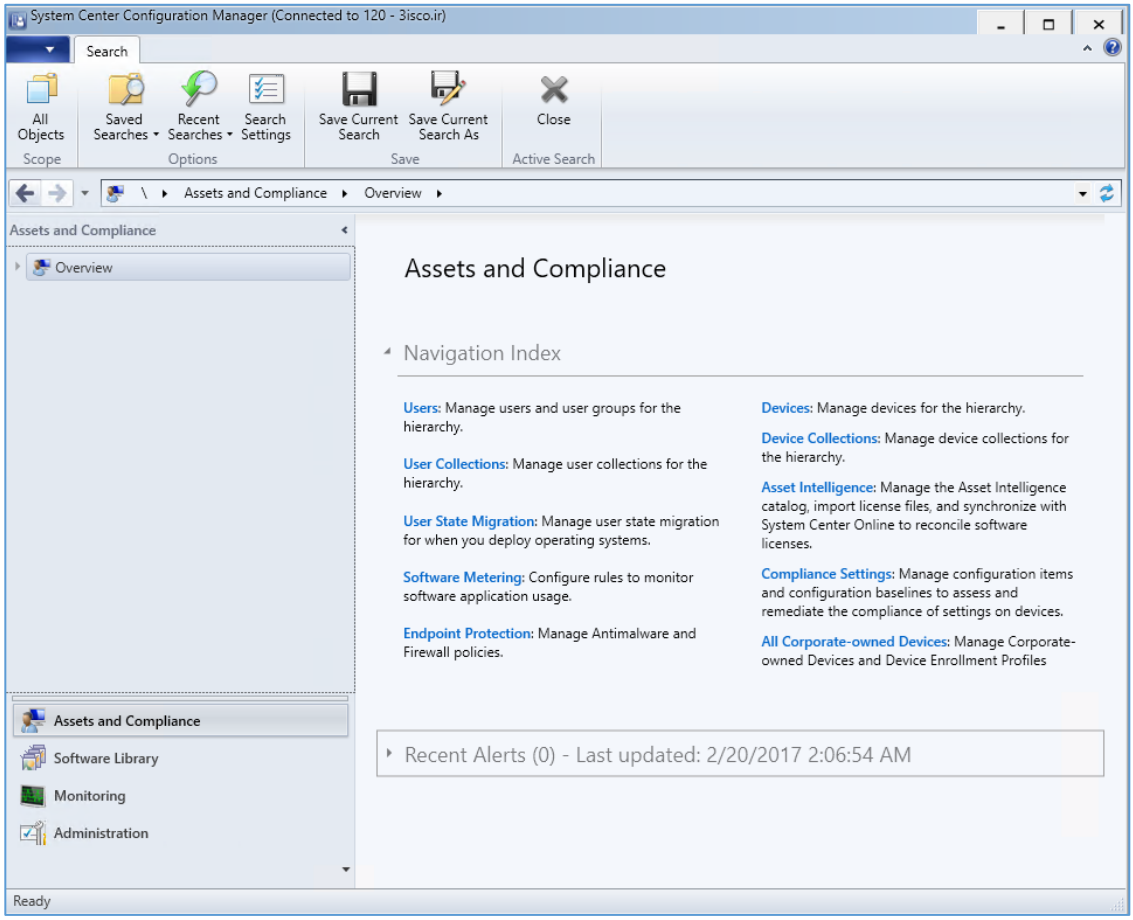


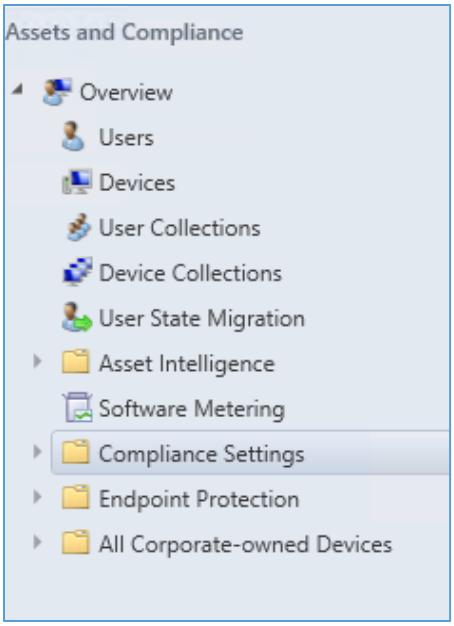
در این صفحه وارد Group شوید و دو بار بر روی گروه Administrators، کلیک کنید و بعد در صفحه‌ی باز شده بر روی Add کلیک کنید و کاربر اصلی را که با آن قصد انجام کارها را دارید، عضو گروه کنید و بر روی OK کلیک کنید.



بعد از Restart کردن سرور و اجرای آن وارد آن شوید و به مانند شکل روبرو از منوی Start، نرم‌افزار System Center Configuration Manager را اجرا کنید.

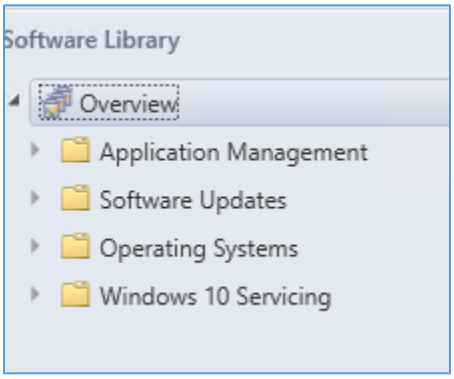
در شکل زیر، نرم افزار SCCM یا همان، Configuration Manager System Center را مشاهده می‌کنید، این نرم‌افزار دارای قسمت‌های مختلف با کاربردهای مختلف است که در ادامه، آنها را بررسی خواهیم کرد.





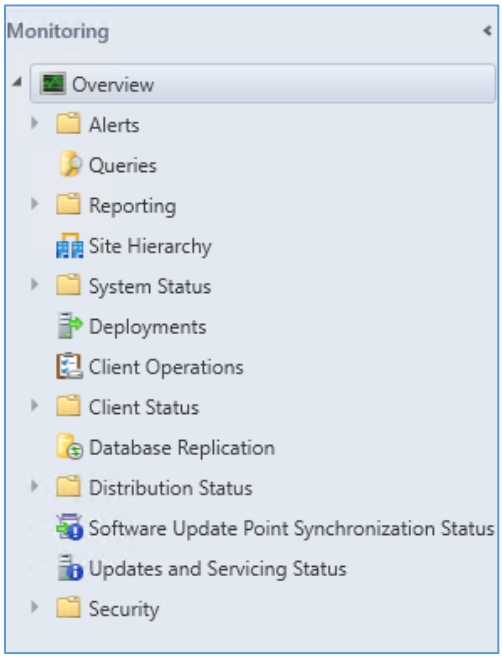
قسمت اوّل – Assets and compliance:

در برگیرنده‌ی مدیریّت نام کاربری کاربران، نام کلاینت‌ها، مجموعه‌ی کاربران و کلاینت‌ها، فایروال‌ها و... است که در صورت نیاز، همه‌ی گزینه‌ها را بررسی خواهیم کرد.



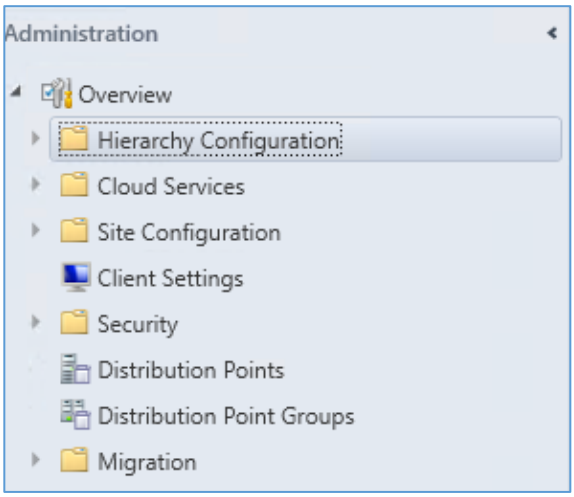
قسمت دوّم – Software Library:

همانطور که از نامش پیدا است، برای مدیریّت نرم‌افزار در شبکه کاربرد دارد که از جمله‌ی آن می‌توان به مدیریّت ویندوز ۱۰، مدیریّت آپدیت نرم‌افزارها و... اشاره کرد.



قسمت سوّم – Monitoring:

برای مانیتور کردن کلّ عملکرد شبکه کاربرد دارد و تمام رویدادها در این قسمت ثبت خواهد شد.

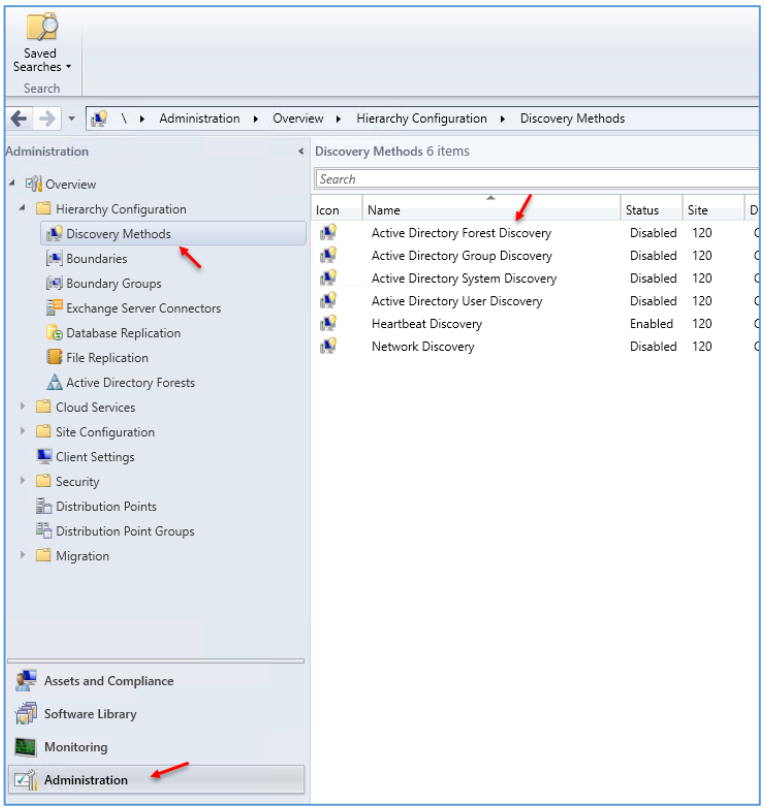


قسمت چهارم – Administration:

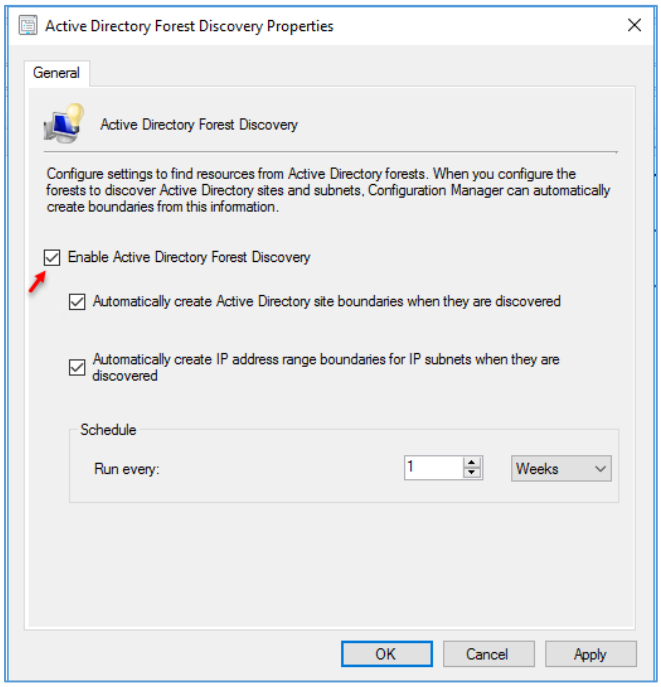
این قسمت برای مدیریّت شبکه کاربرد دارد که با این قسمت، زیاد کار خواهیم کرد، برای اضافه کردن کاربران و سیستم‌ها به نرم‌افزار باید از این قسمت استفاده کنید.

کار با نرم‌افزار SCCM:

برای شروع کار با نرم‌افزار، قبل از هر چیز باید تمام کاربران و سیستم‌ها را از Active Directory بخوانید و وارد نرم‌افزار کنید.



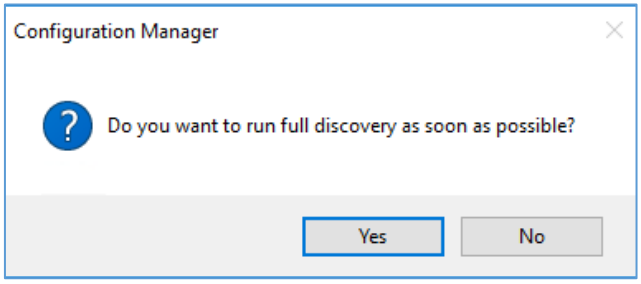
برای شروع وارد نرم‌افزار SCCM شوید و به مانند شکل روبرو از سمت چپ بر روی Administration، دوبار کلیک کنید و بعد از این کار بر روی گزینه‌ی دوّم، یعنی Discovery Methods کلیک کنید که صفحه‌ی روبروی آن باز خواهد شد که دارای گزینه‌های مختلف است، برای شروع کار، اوّل Forest را فعّال کنید، برای انجام آن بر روی گزینه‌ی Acive Directory Forest Discovery، دو بار کلیک کنید.



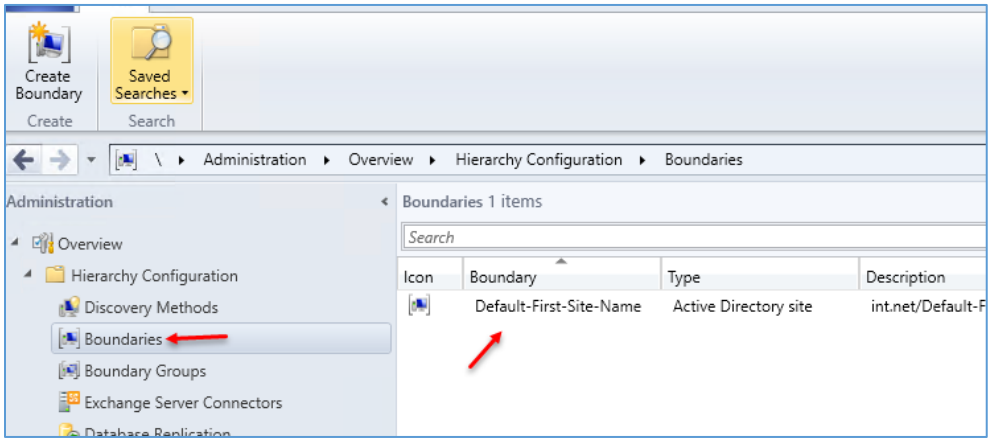
در این صفحه، تیک گزینه‌ی Enable Active Directory Forest Discovery را انتخاب کنید.

دو گزینه بعدی که یکی برای ایجاد سایت و دیگری برای ایجاد رنج IP شبکه به صورت خودکار در SCCM است.

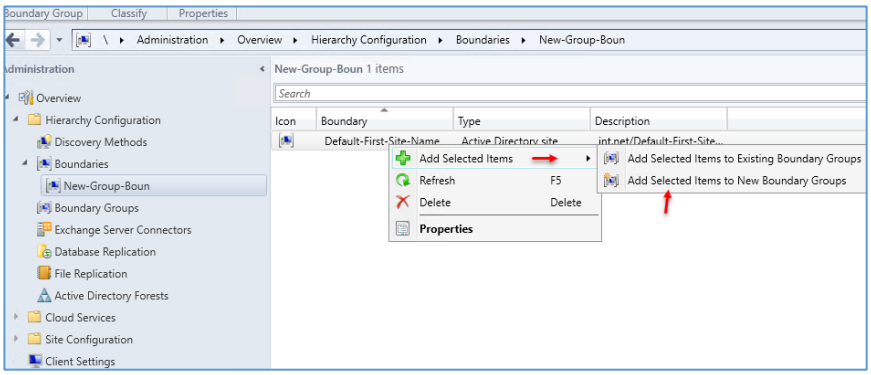
گزینه‌ی آخر برای زمان‌بندی ایجاد شده است که به صورت پیش‌فرض یک هفته در نظر گرفتیم که شما می‌توانید این زمان را تغییر دهید.



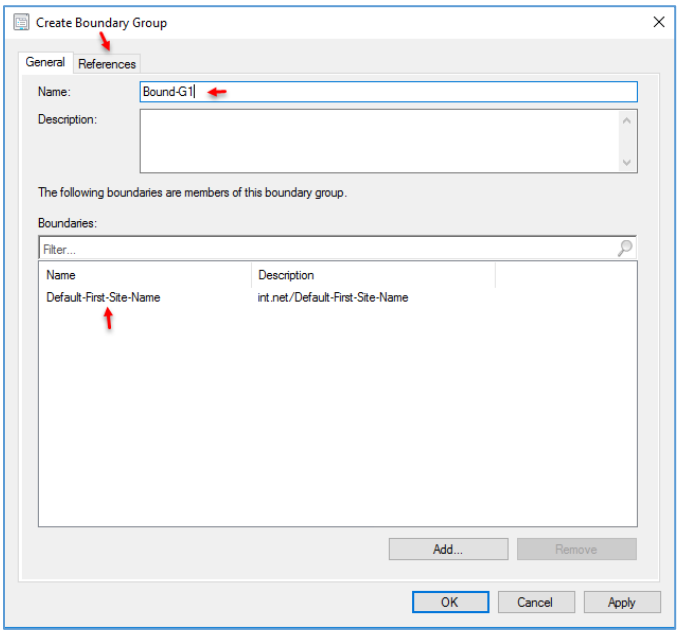
بعد از اینکه بر روی OK کلیک کردید، صفحه‌ی روبرو ظاهر می‌شود که با کلیک بر روی Yes، کار بررسی و وارد شدن اطّلاعات از Active Directory به نرم‌افزار SCCM آغاز می‌شود.



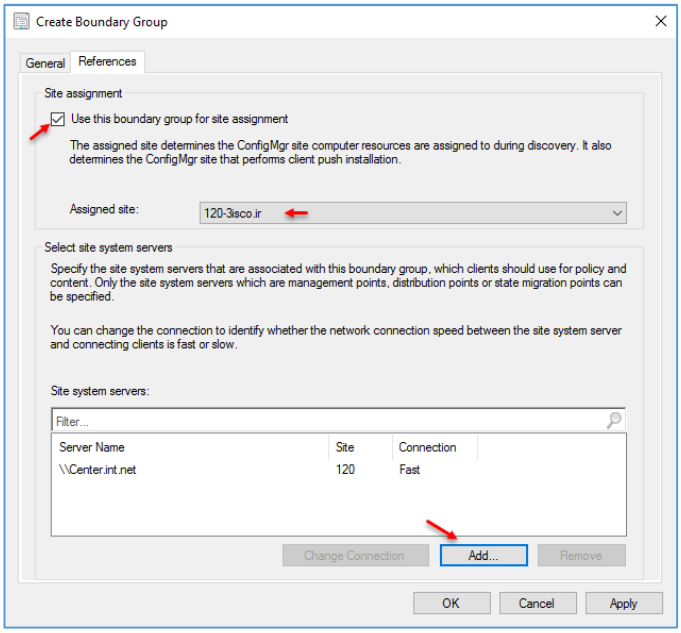
بعد از انجام عملیّات قبل، اگر از سمت چپ بر روی Boundaries کلیک کنید، متوجّه خواهید شد که Site مربوط به Active Directory در این قسمت ایجاد شده است.



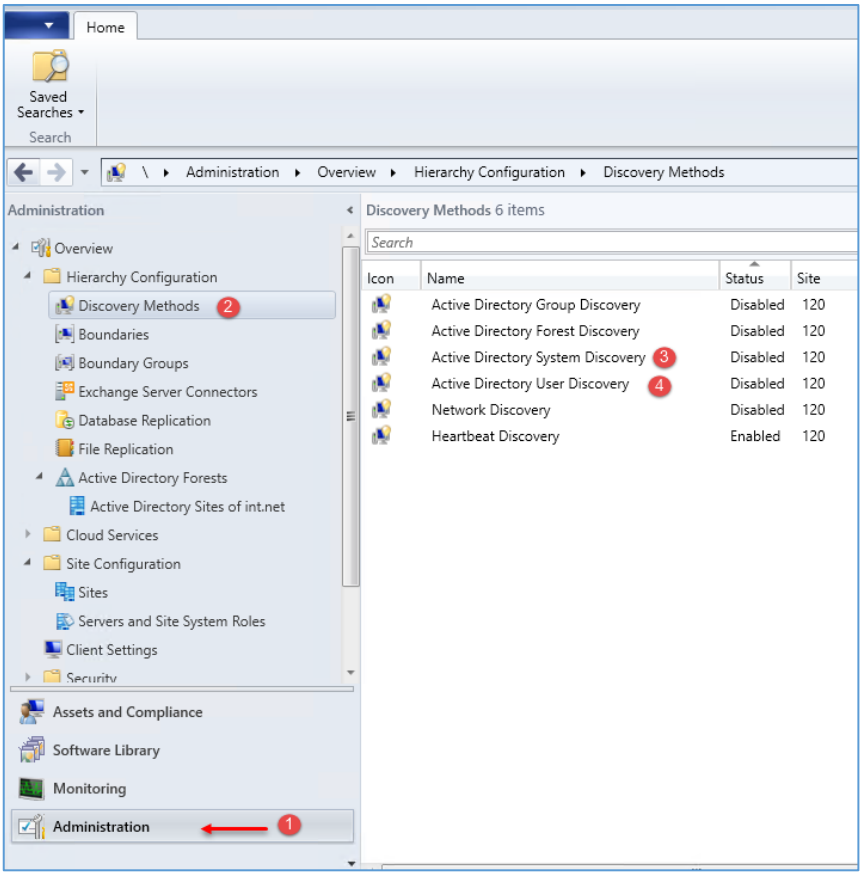
بعد از ایجاد Site باید یک گروه ایجاد کنید تا تمام کاربران، منابع شبکه و... زیر مجموعه‌ی این گروه قرار بگیرند، بر روی Site کلیک راست کنید و گزینه‌ی مورد نظر را انتخاب کنید.



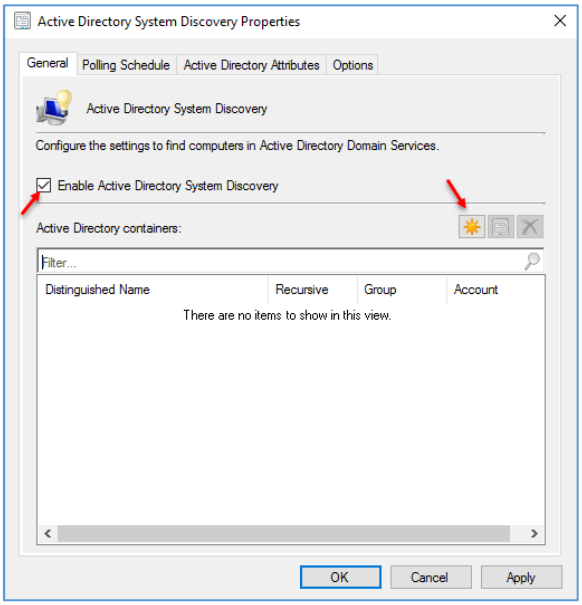
در این صفحه، یک اسم به دلخواه خود وارد کنید و نام سایت را در زیر آن انتخاب کنید و بعد از آن وارد تب Refrences شوید.



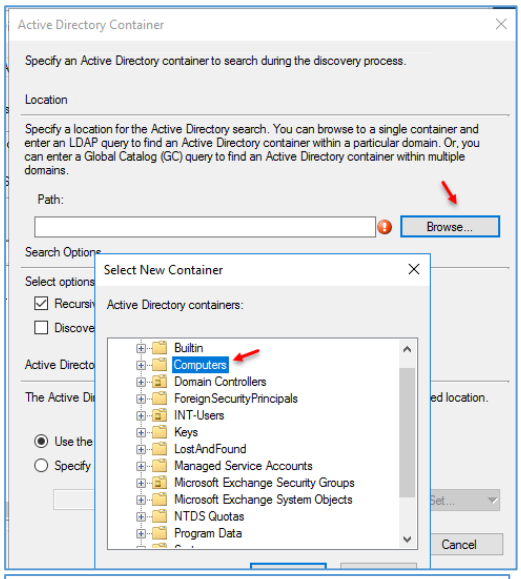
در تب Refrences، تیک گزینه‌ی مورد نظر و نام سایت خود را در قسمت Assiged site انتخاب کنید که در این کتاب، نام سایت را 120-3isco.ir در نظر گرفتیم، در قسمت آخر نیز بر روی Add کلیک کنید و Site System مورد نظر خود را انتخاب و بر روی OK کلیک کنید.



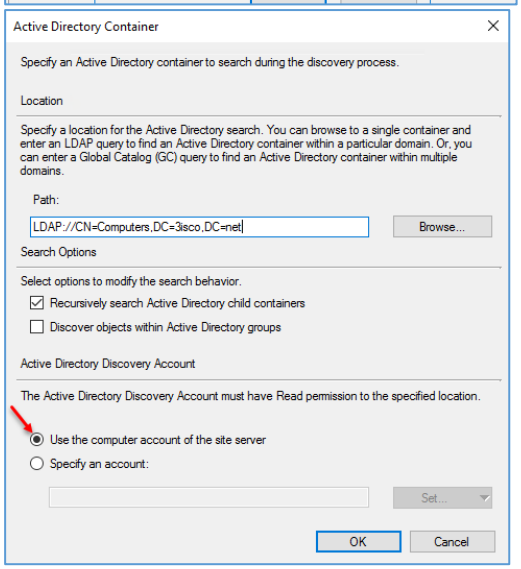
در مرحله‌ی بعد باید سیستم‌ها و کاربران را به نرم‌افزار اضافه کنید، برای اینکه سیستم‌ها را به نرم‌افزار اضافه کنید باید بر روی شماره‌ی سه، دو بار کلیک کنید و برای کاربران نیز باید بر روی شماره‌ی چهار کلیک کنید.



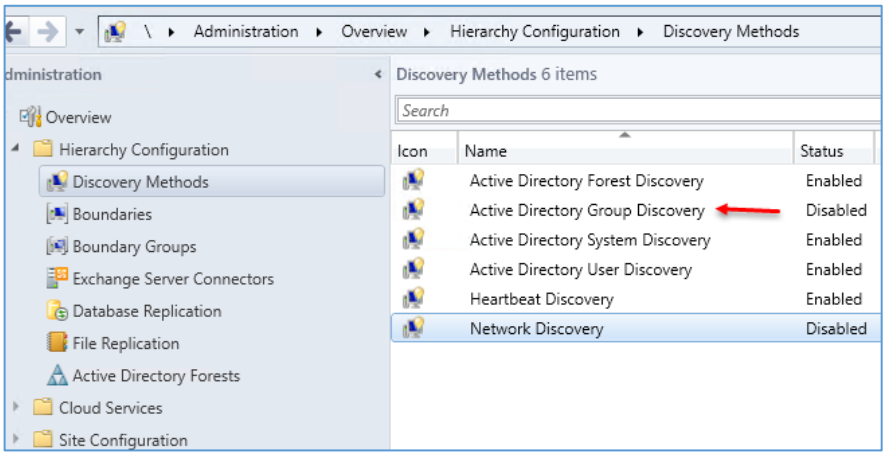
در تب General، تیک گزینه‌ی Enable Active Directory System Discovery را انتخاب کنید و بعد از آن بر روی آیکون ستاره کلیک کنید تا مسیر Active Directory را مشخّص کنید.



در این صفحه باید آدرس سیستم‌ها را در سرویس Active Directory Users and Computers مشخّص کنید برای همین باید بر روی Browse کلیک کنید و به مانند شکل، Computers را از لیست انتخاب و بر روی OK کلیک کنید.

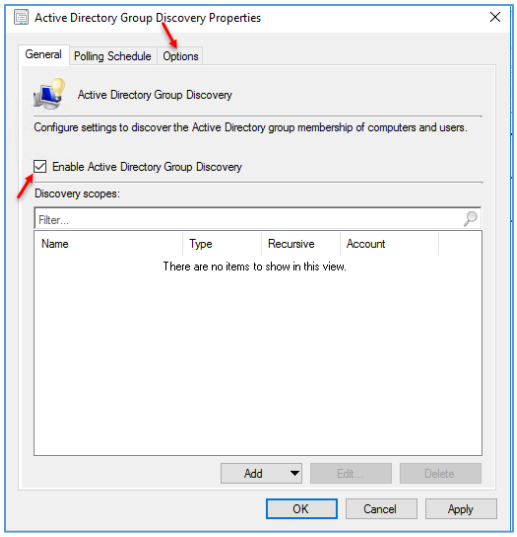


در این صفحه، مسیر مورد نظر انتخاب شده است و اگر کاربر شما، دسترسی لازم به شبکه را ندارد، می‌توانید در پایین صفحه، کاربر مورد نظر خود را با انتخاب Specify an account وارد کنید.

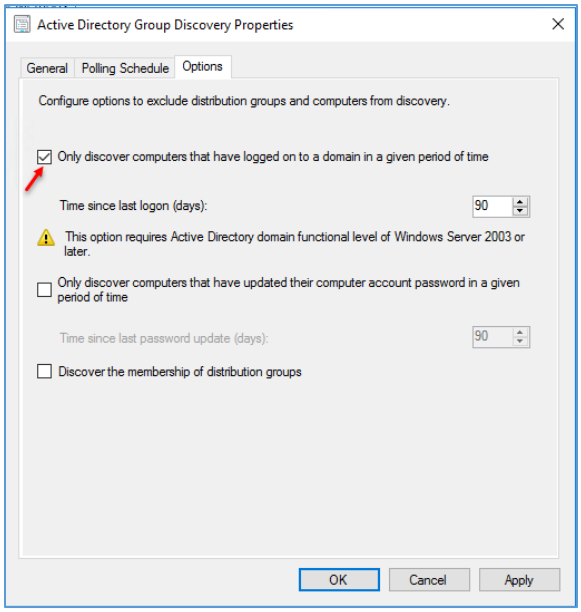


بعد از فعّال کردن User و System باید Group را فعّال کنید.

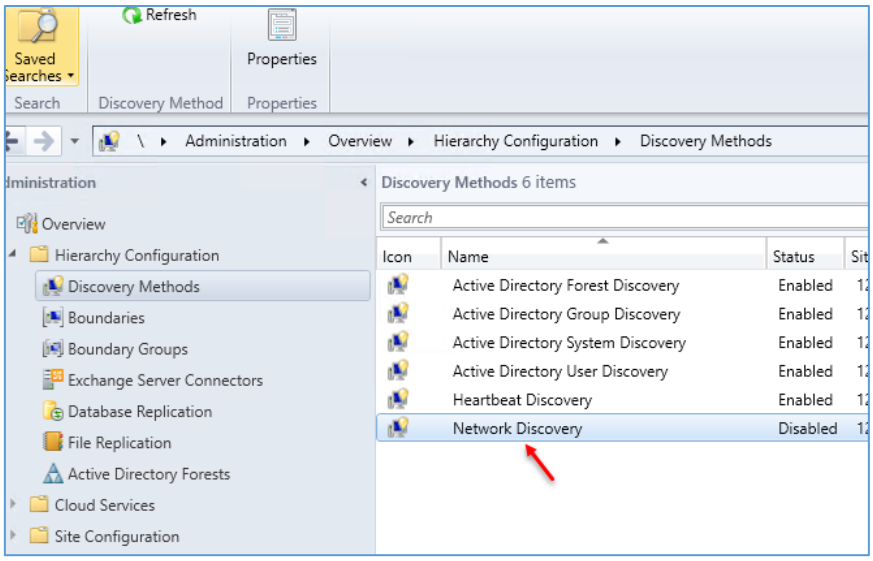
برای این کار به مانند شکل روبرو، دو بار بر روی Group، کلیک کنید.



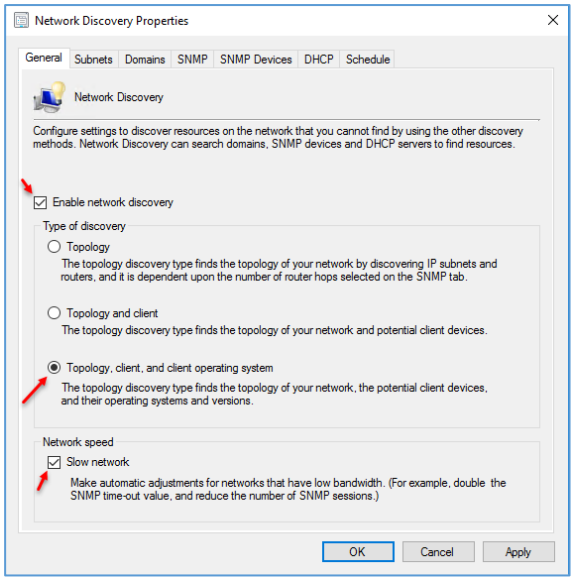
در این قسمت، تیک گزینه‌ی مورد نظر را انتخاب کنید و بعد از آن وارد تب Options شوید.



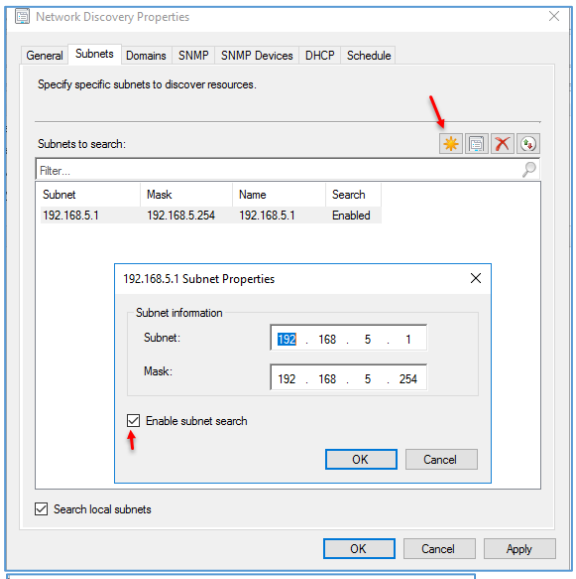
در تب Options، تیک گزینه‌ی only discover computer را انتخاب کنید، با این کار تنها سیستم‌هایی انتخاب خواهند شد که حداکثر تا ۹۰ روز پیش، خود را با Active آپدیت کردند، البتّه شما می‌توانید این زمان را تغییر دهید.



در مرحله‌ی آخر باید برای پیدا کردن کلاینت‌ها، پرینترها و دستگاه‌های دیگر بر روی Network Discovery، دو بار کلیک کنید.

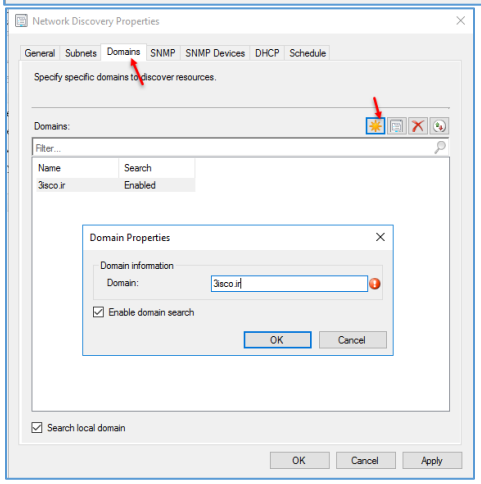


در این صفحه، این قابلیّت با انتخاب گزینه‌ی Enable network discovery فعّال خواهد شد، در زیر این گزینه، سه گزینه وجود دارد که برای اینکه به صورت کامل، کلّ شبکه با تمام دستگاه‌های موجود آن بررسی شود باید گزینه‌ی سوّم را انتخاب کنید و در آخر صفحه، تیک گزینه‌ی Slow network را انتخاب کنید تا عملیّات discovery با سرعت پایین انجام شود تا مشکلی برای پهنای باند شبکه ایجاد نشود، وارد تب Subnet شوید.



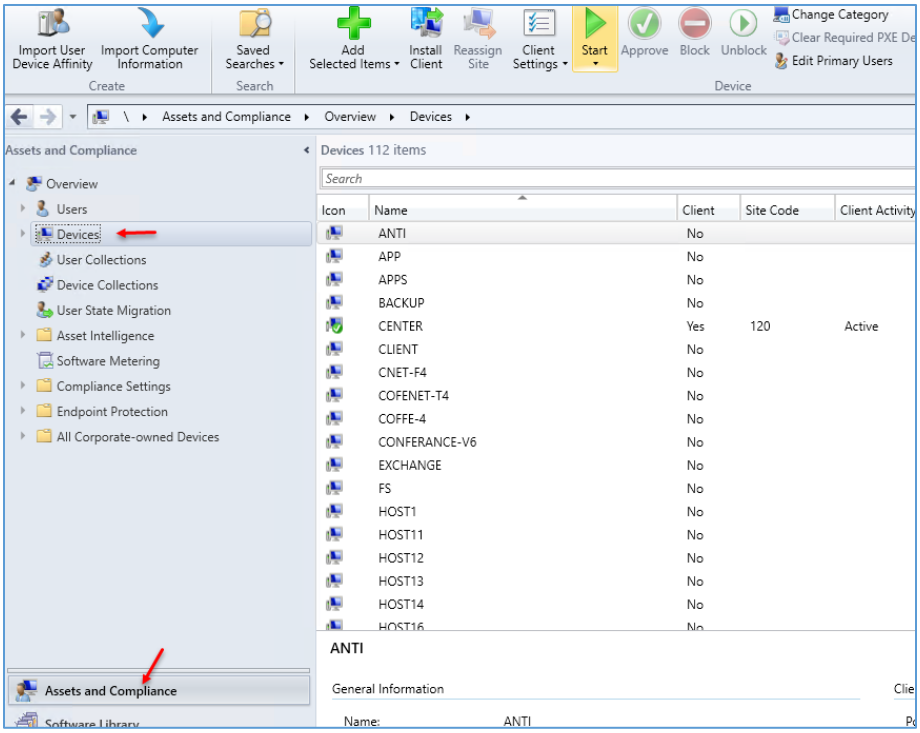
در این صفحه بر روی علامت ستاره کلیک کنید و در پنجره‌ی باز شده، Subnet و Mask شبکه‌ی خود را وارد و بر روی OK کلیک کنید.

وارد تب Domain شوید.



در قسمت دومین نیز نام دومین شبکه‌ی خود را وارد و بر روی OK کلیک کنید.

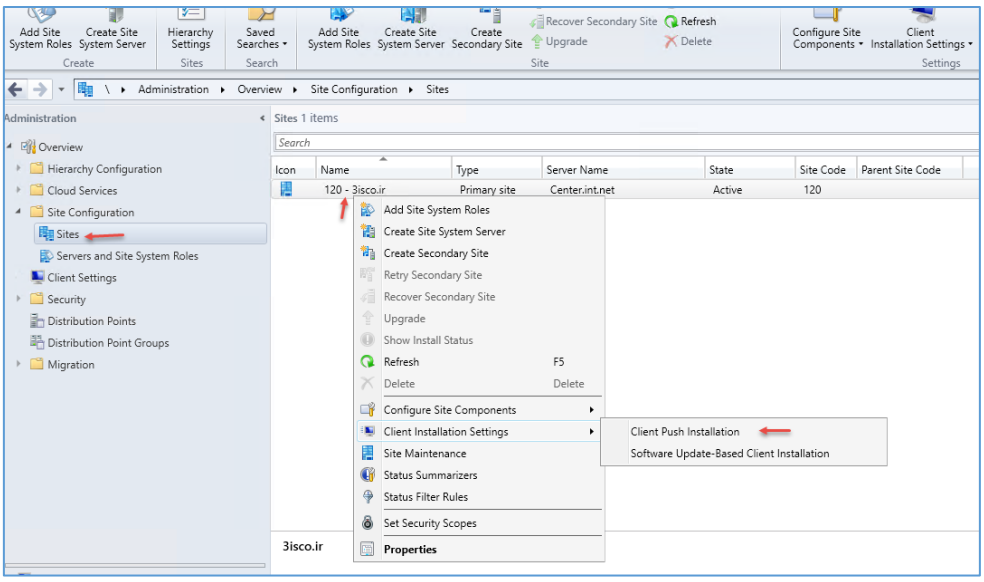
در تب DHCP، آدرس سرور DHCP را وارد کنید که در این کتاب، سرور AD، همان سرور DHCP است، بعد از انجام کارهای بالا بر روی OK کلیک کنید تا تنظیمات اعمال شود.



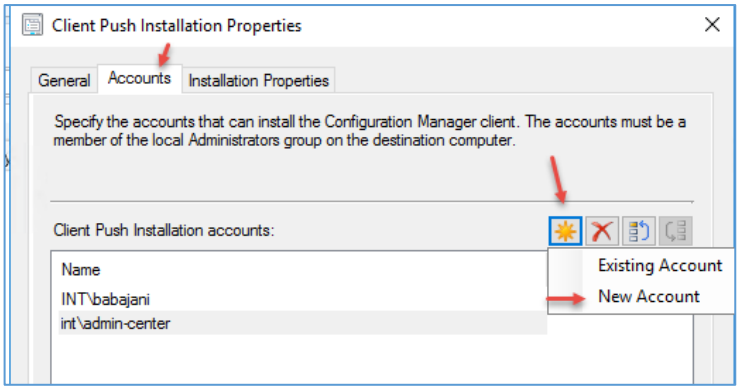
برای مشاهده‌ی سیستم‌ها و کاربران باید به مانند شکل زیر وارد Assets and Compliance شوید و بر روی Device و یا Users کلیک کنید، همانطور که مشاهده می‌کنید، سیستم‌ها از Active Directory به لیست اضافه شده است.

تنظیمات Client Setting:

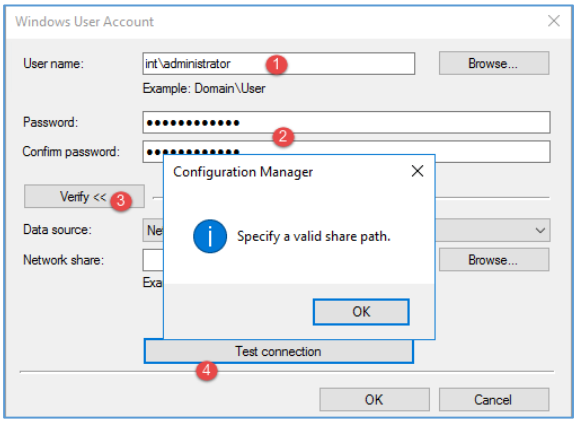
بعد از اینکه Discovery را برای کلّ شبکه فعّال کردید و تمام کاربران به همراه تمام دستگاه‌های شبکه وارد نرم‌افزار SCCM شدند باید تنظیمات Client ها را انجام دهید تا بتوانید به منابع آنها دسترسی داشته باشید.



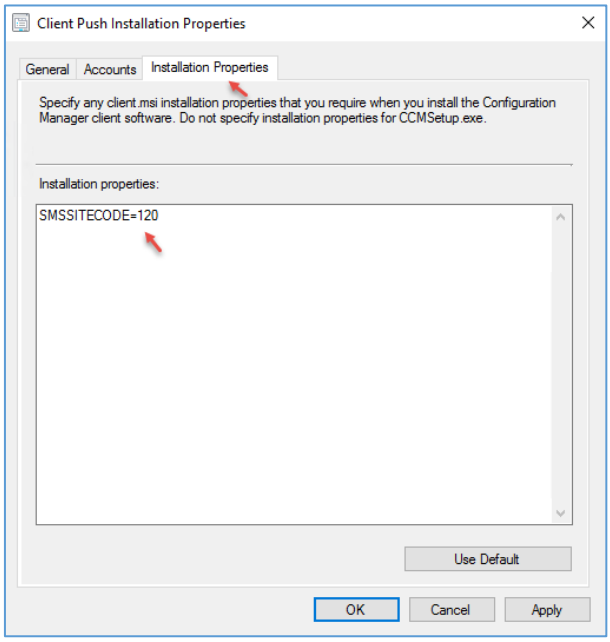
برای شروع کار وارد Sites شوید و بر روی سایت خود، کلیک راست کنید و از قسمت Client Intsallation Settings، گزینه‌ی Client Push Installation را انتخاب کنید.



در این صفحه باید وارد تب Accounts شوید و نام کاربری را وارد کنید که دسترسی کامل به شبکه داشته باشد، برای این کار باید بر روی آیکون ستاره کلیک و گزینه‌ی New Account را انتخاب کنید، اگر با همان نام کاربری Admin وارد سرور شدید و در حال اجرا هستید، می‌توانید گزینه‌ی Existing Account را انتخاب کنید.

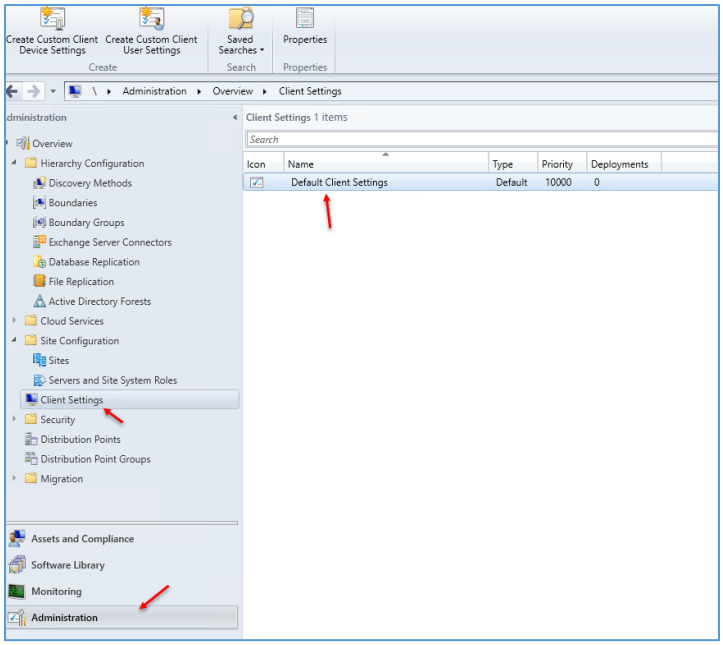


در این صفحه و در قسمت User Name، نام کاربری را به همراه نام دومین وارد کنید و رمز عبور آن را در قسمت شماره‌ی۲ وارد و برای تست کارایی بر روی شماره‌ی ۳ کلیک کنید و در آخر بر روی Test کلیک کنید.

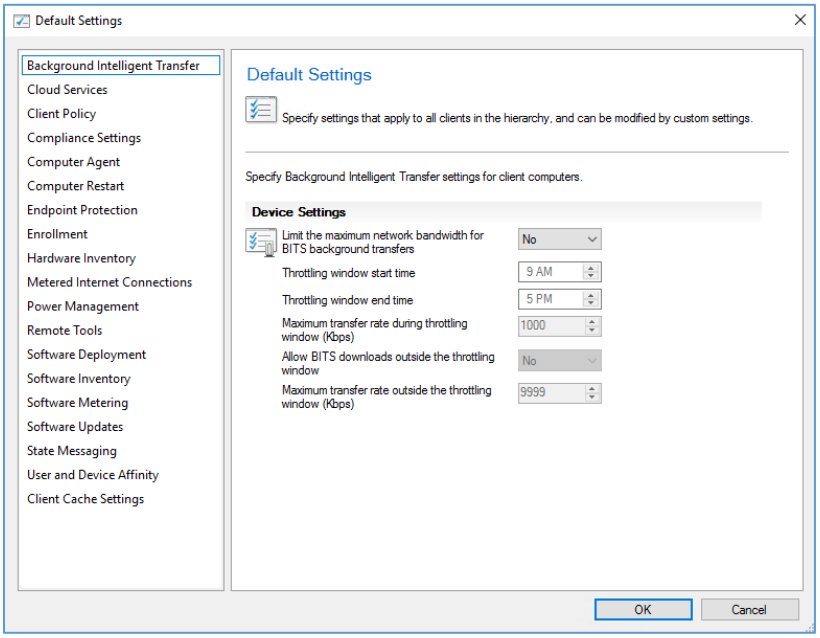


در قسمت Installation Properties باید نام سایت قرار داشته باشد، اگر به مانند شکل درست بود بر روی OK کلیک کنید.

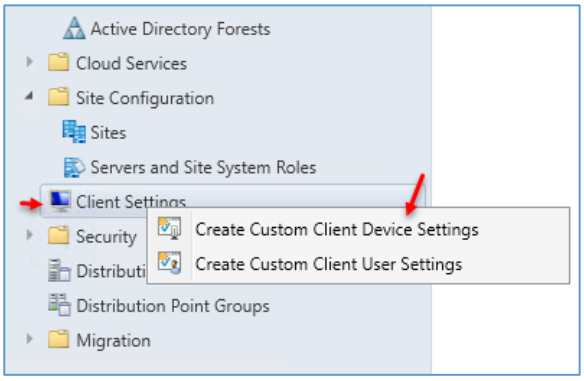
در این صفحه وارد قسمت Administration شوید و در گزینه‌های موجود بر روی Client Settings کلیک کنید.



در صفحه‌ی باز شده، دو بار بر روی Default Client Settings کلیک کنید.

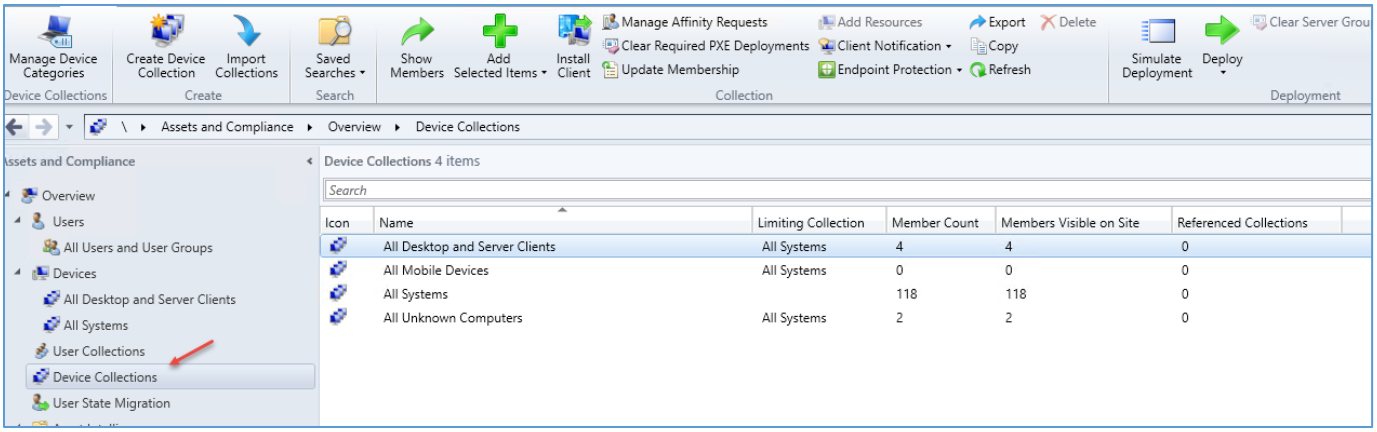


در این صفحه، کلّ تنظیمات مربوط به کلاینت‌ها را مشاهده می‌کنید که در صورت نیاز آنها را تغییر خواهیم داد.

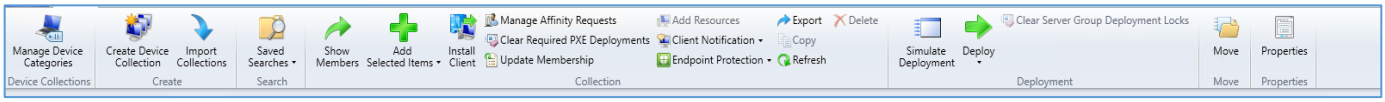


اگر بخواهید، یک گزینه‌ی جدید برای تنظیمات ایجاد کنید بر روی Client Settings کلیک راست کنید و گزینه‌ی Create Custom Client Device Settings و تنظیمات جدید خود را انتخاب کنید.

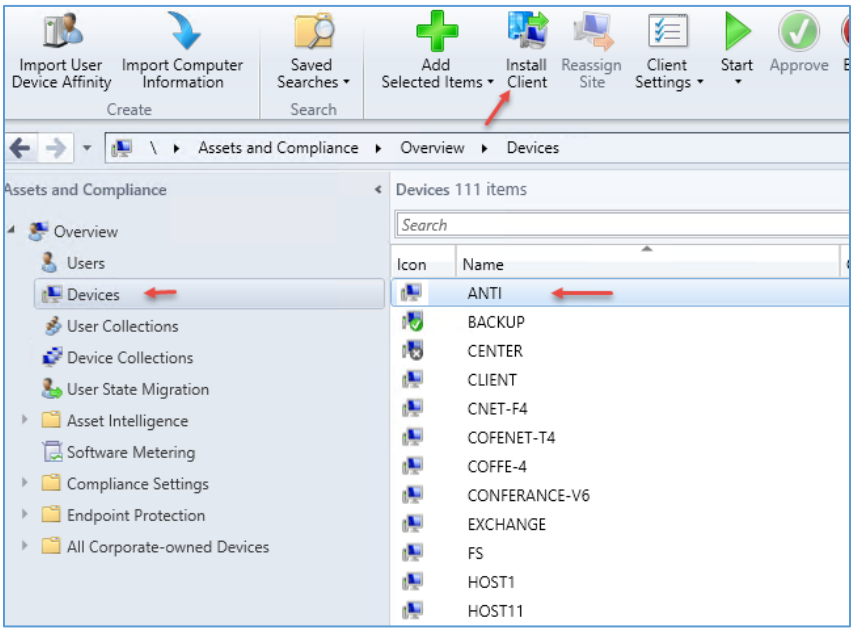
نصب سرویس Client:



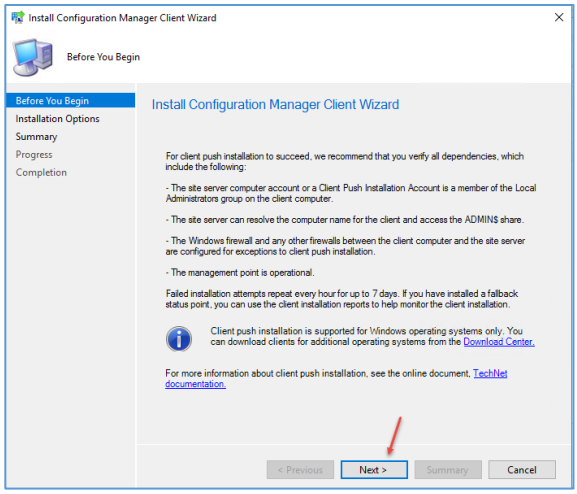
در شکل بالا وارد قسمت Device Collections شوید، همانطور که مشاهده می‌کنید در این صفحه، چهار Collection وجود دارد که هر کدام مختصّ گروهی خاص است، در قسمت All Systems، تمام دستگاه‌های شناسایی‌شده قرار دارند، برای اینکه دستگاه‌های شبکه را مدیریّت کنید باید نرم‌افزار Client و یا همان، Agent را بر روی دستگاه‌ها نصب کنید.



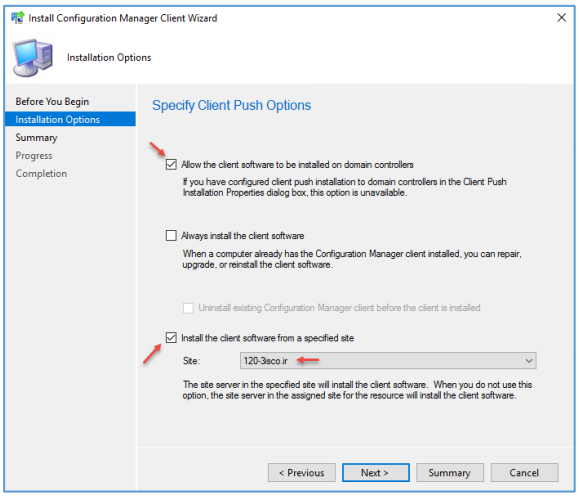
در بالای صفحه، تنظیمات متعدّدی وجود دارد که در صفحات قبل در قسمت Client Setting بررسی کردیم.



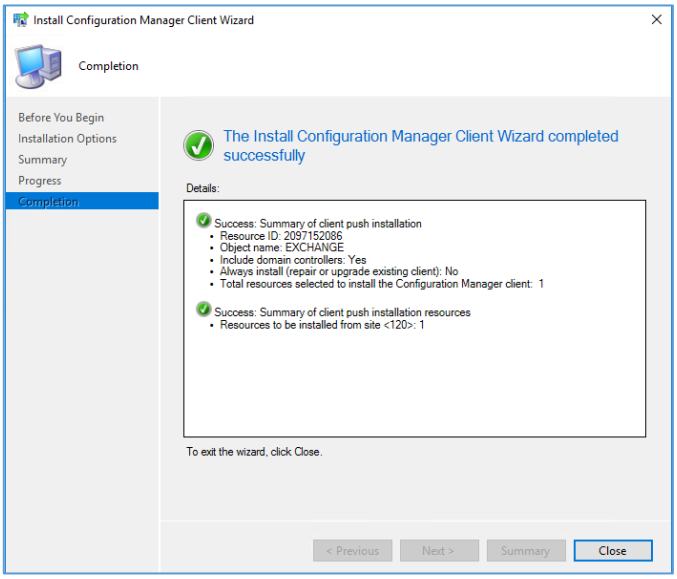
در این صفحه برای نصب Client بر روی Devices کلیک کنید و سرور مورد نظر خود را از لیست انتخاب و بر روی گزینه‌ی Install Client کلیک کنید و یا بر روی دستگاه مورد نظر کلیک راست کنید و بر روی گزینه‌ی Install Client کلیک کنید.



در این صفحه به یک‌سری نکات اشاره شده است، مثلاً باید کاربری که با آن قصد نصب Client را بر روی دستگاه‌های شبکه دارید را مشخّص کنید و باید به پوشه‌ی ADMIN$ نیز که به صورت مخفی در سرور Center به اشتراک گذاشته شده است، دسترسی داشته باشد.

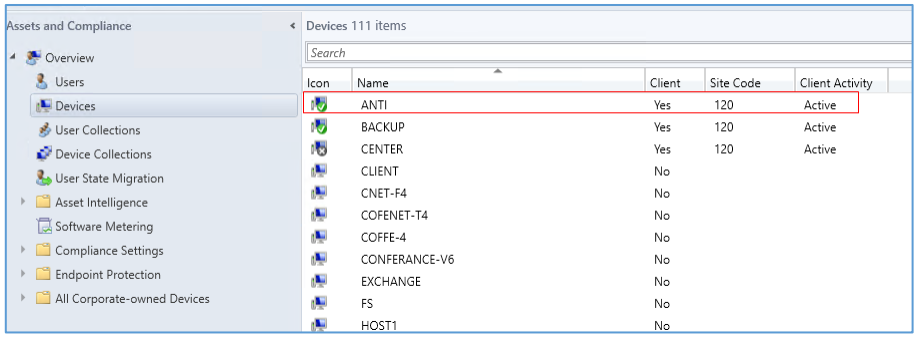


در این صفحه، تیک گزینه‌ی اوّل را انتخاب کنید تا دسترسی لازم به کلاینت در دومین داده شود و بعد، تیک آخر را انتخاب کنید و از لیست کشویی، نام سایت خود را انتخاب و بر روی Next کلیک کنید.

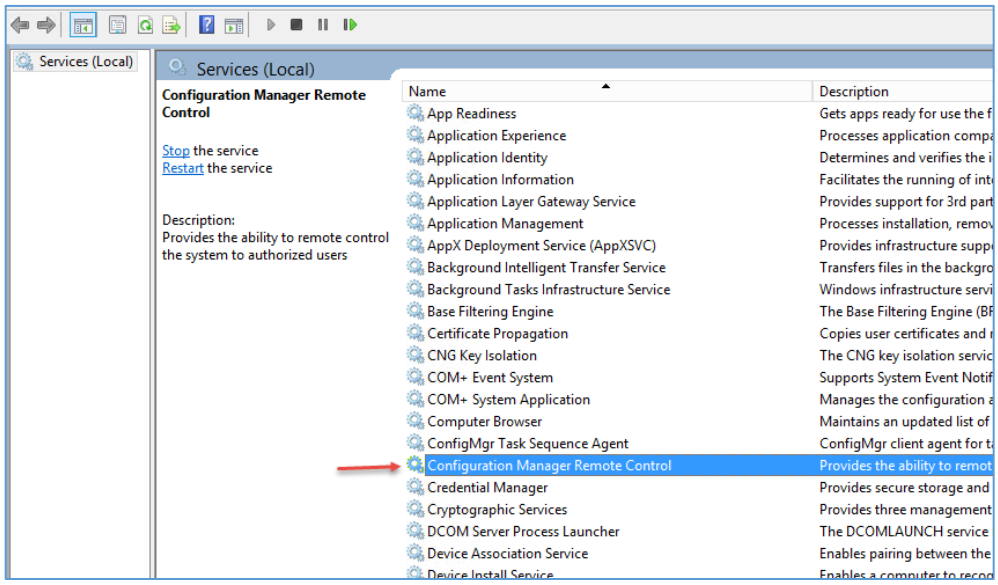


همانطور که در شکل روبرو مشاهده می‌کنید، Client در سرور Anti برای نصب آماده شده است، اگر سرور Anti و یا هر سروری که بر روی آن، این سرویس را فعّال کردید، Restart کنید، این سرویس بر روی آن اجرا خواهد شد.

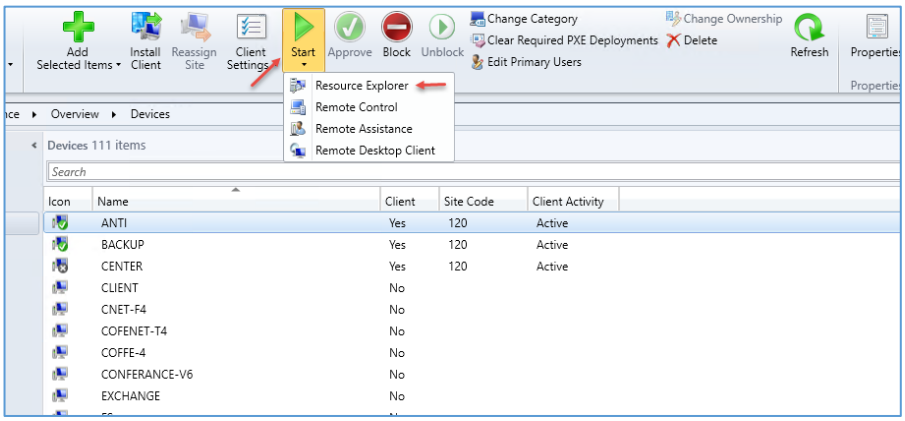
برای تست این موضوع، یک بار سرور Anti را Restart کنید.



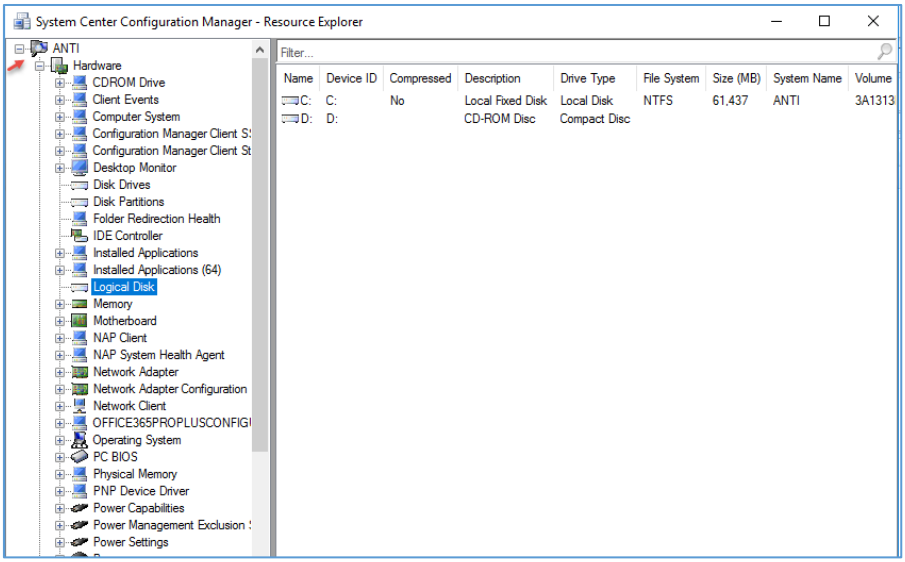
در شکل روبرو آیکون سرور Anti تغییر کرده و Client بر روی آن نصب شده است.



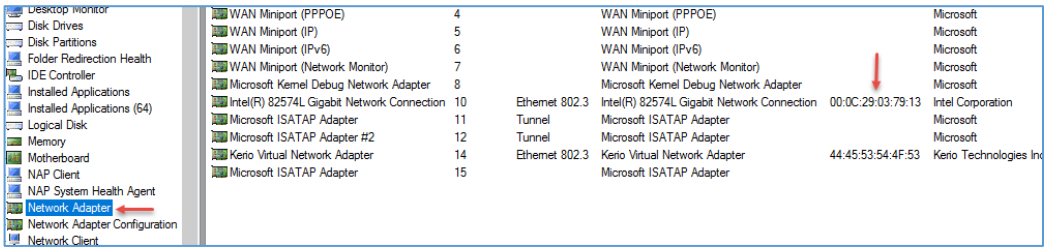
برای اینکه این موضوع را بهتر درک کنید وارد سرور Anti شوید و Services را اجرا کنید، در لیست سرویس‌ها، نام Configuration Manager Remote Control را مشاهده می‌کنید.



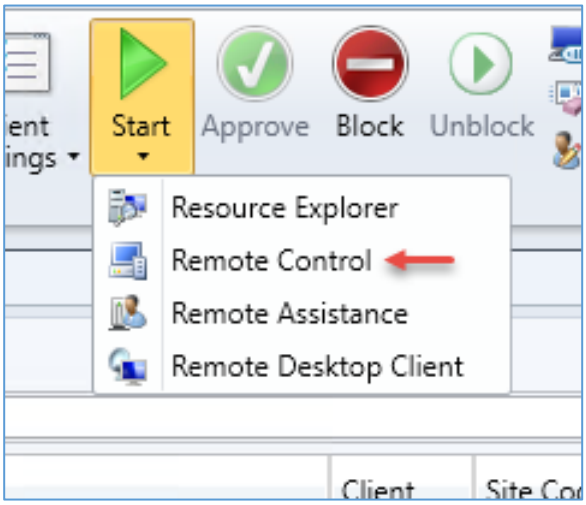
زمانی که کلاینت بر روی سیستم مورد نظر نصب می‌شود، یک‌سری دسترسی‌ها به منابع آن سیستم در دسترس قرار می‌گیرد، به مانند شکل روبرو بر روی سرور مورد نظر کلیک کنید، یک‌سری ابزار در اختیار شما قرار می‌گیرد، مثلاً برای نمایش اطّلاعات سخت‌افزار سیستم مورد نظر، به مانند شکل بالا بر روی Start کلیک کنید و گزینه‌ی Resource Explorer را انتخاب کنید.



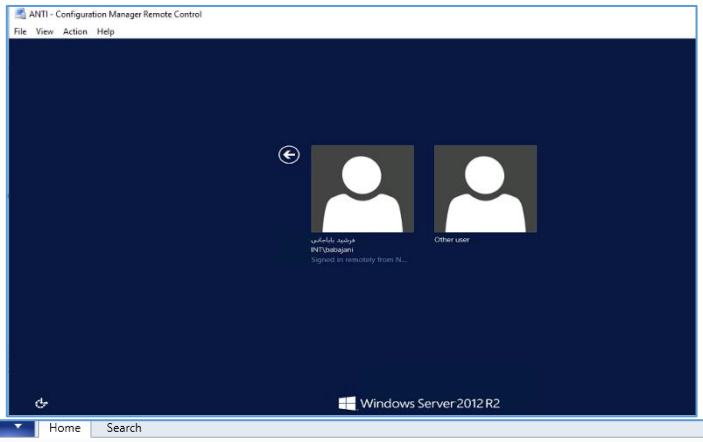
در شکل روبرو تمام اطّلاعات سخت-افزاری و نرم‌افزاری سرور Anti مشخّص شده است که شما می‌توانید از طریق این اطّلاعات، سرور را به خوبی بررسی کنید.



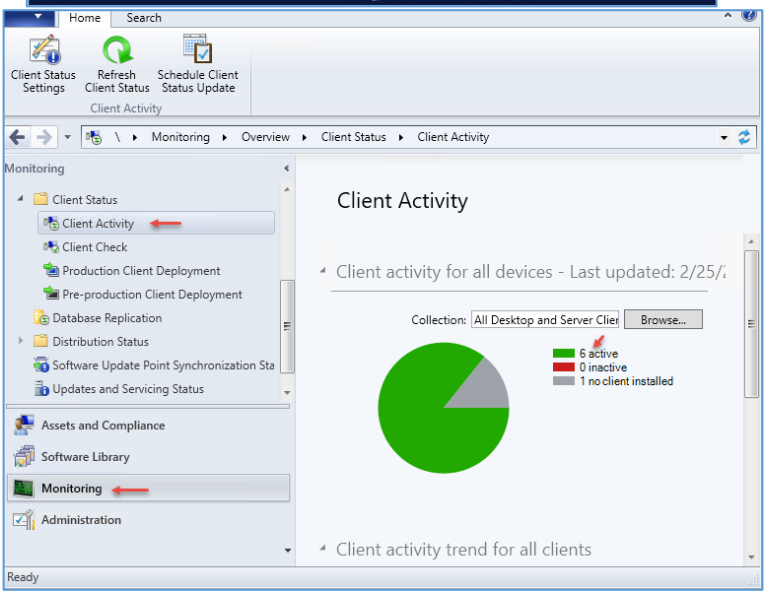
بر فرض برای پیدا کردن مک آدرس سیستم مورد نظر باید از لیست سمت چپ، گزینه‌ی Network Adaptor را انتخاب کنید، در صفحه‌ی باز شده، همه‌ی کارت شبکه‌های سرور را نمایش می‌دهد که می‌توانید آدرس مورد نظر خودتان را از ستون Mac Address پیدا کنید.



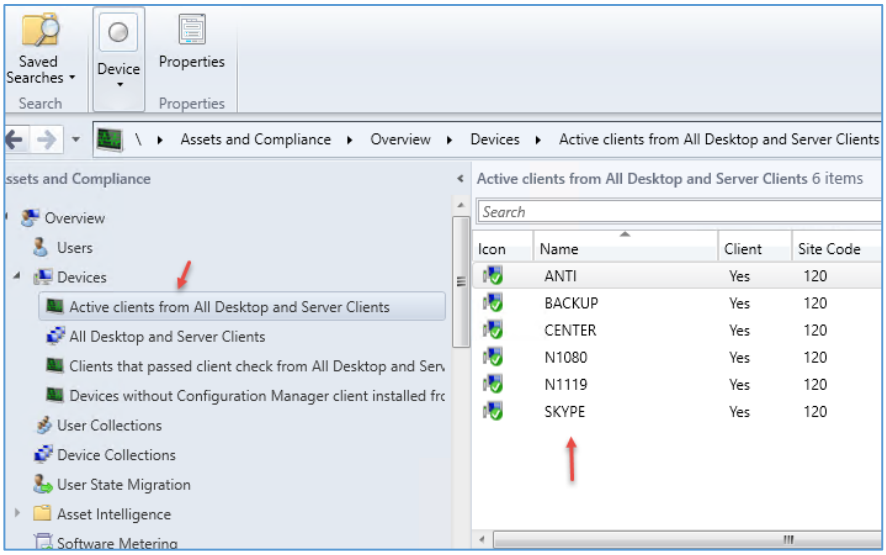
گزینه‌ی دیگری که وجود دارد، Remote Control است که از طریق این ابزار می‌توانید کنترل سرور مورد نظر را در دست بگیرید.



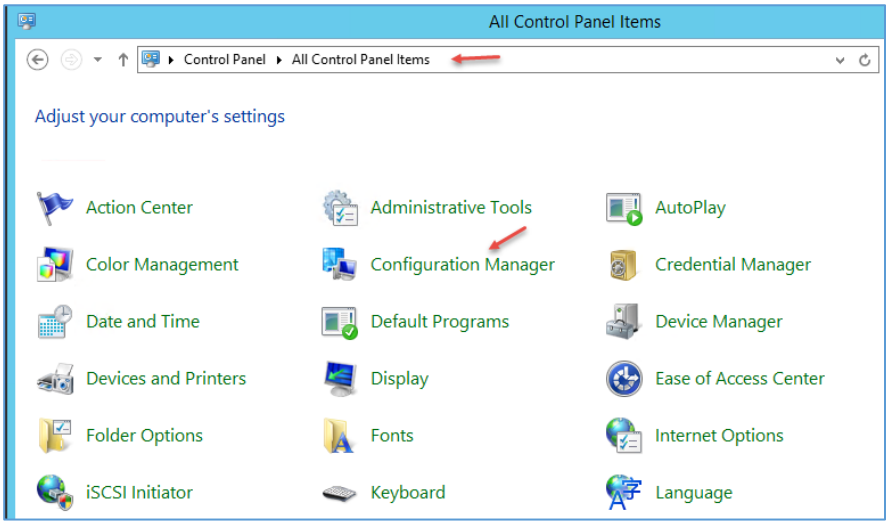
در شکل روبرو صفحه‌ی سرور مورد نظر را مشاهده می‌کنید که در منوی بالایی، یک‌سری تنظیمات، مانند Full کردن صفحه یا قفل کردن کیبورد و... وجود دارد، گزینه‌های دیگری نیز وجود دارد که در صورت نیاز آنها را بررسی می‌کنیم.



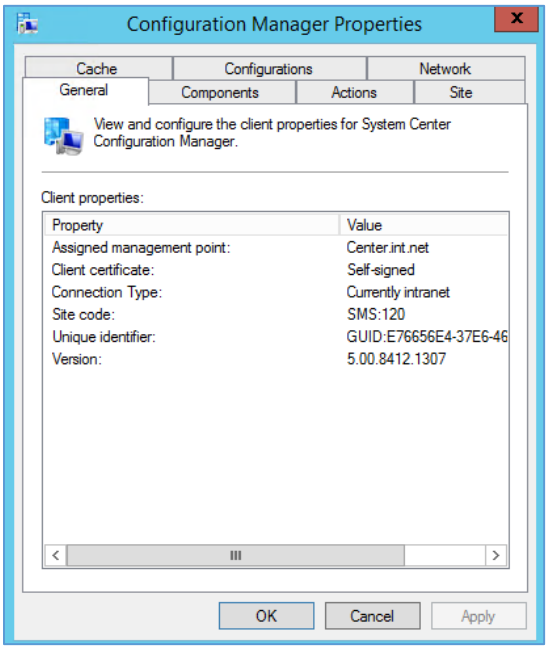
برای اینکه دقیقاً متوجّه شوید که نرم‌افزار Client بر روی چند سیستم نصب شده است، به مانند شکل روبرو می‌توانید وارد قسمت Monitoring شوید و از قسمت Client Status، گزینه‌ی Client Activity را انتخاب کنید، در این صفحه، تعداد کلاینت‌هایی که بر روی آنها نرم‌افزار نصب شده است، برابر ٦ است که با کلیک بر روی آن می‌توانید نام آنها را مشاهده کنید.



وقتی بر روی Active کلیک کنید، به مانند شکل روبرو یک زیر مجموعه در زیر Devices ایجاد می‌شود و نام سیستم‌ها مشخّص می‌شود.



اگر وارد Control Panel یکی از کلاینت‌ها شوید، مشاهده خواهید کرد که یک گزینه با عنوان Configuration Manager به لیست اضافه شده است

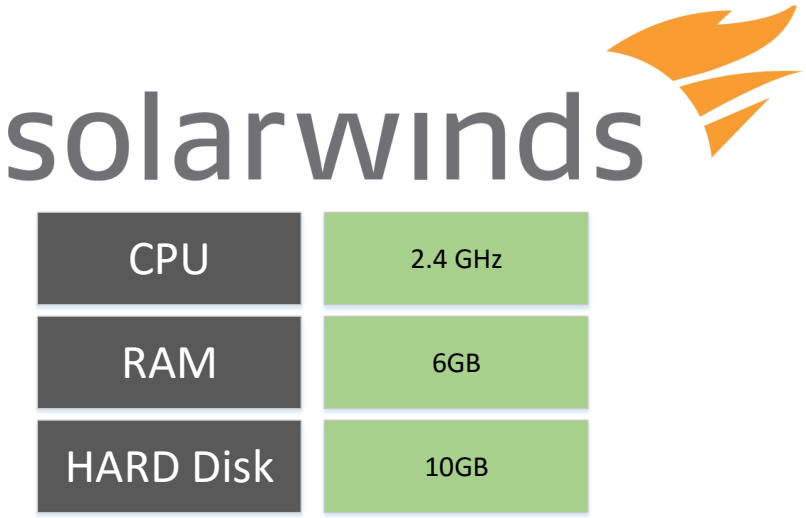


در تب General، اطّلاعات مربوط به سرور Center به همراه نام سایت و ورژن آن مشخّص شده است.

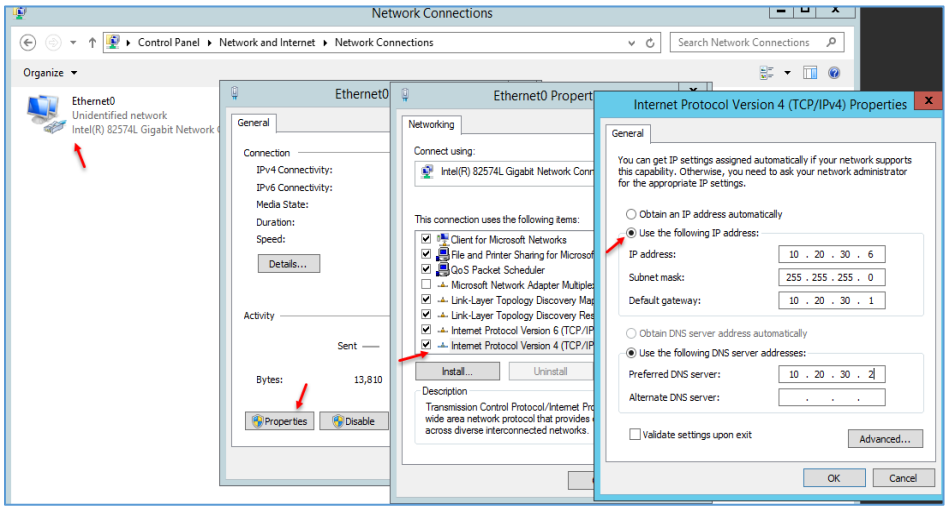
نصب و راه‌اندازی سرور مانیتورینگ Solarwin:

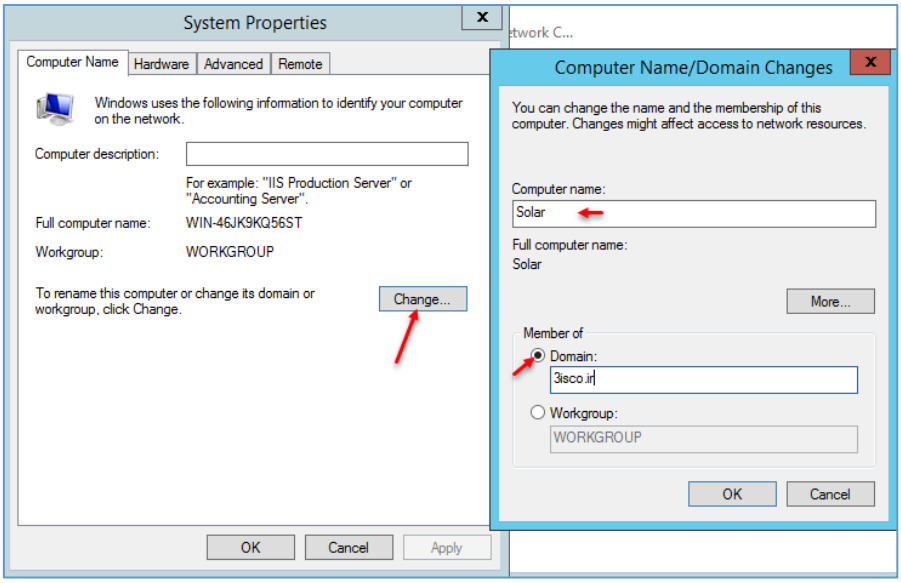
یک نرم‌افزار قدرتمند در بحث مانیتورینگ که برای هر شبکه‌ای نیاز است که راه‌اندازی شود، نرم‌افزارهای دیگری نیز در این بخش فعّالیت داشتند که اگر خاطر شما باشد در کتاب مدیر شبکه‌ی یک، نرم‌افزار PRTG را بررسی کردیم.

برای راه‌اندازی این سرور نیاز به منابع سخت‌افزاری زیر دارید:



مثل همیشه، هر چقدر سخت‌افزار قویتر باشد، عملکرد سرور بهتر خواهد بود، در حالت معمول با سخت‌افزار بالا، نرم‌افزار مانیتورینگ به درستی کار خواهد کرد. ویندوز سروری که برای این نرم‌افزار انتخاب کردیم، ویندوز سرور 2012 R2 است که کار نصب آن را از قبل انجام دادیم، بعد از نصب ویندوز سرور ۲۰۱۲ وارد Network Connection شوید و به مانند شکل، آدرس آن را وارد کنید.

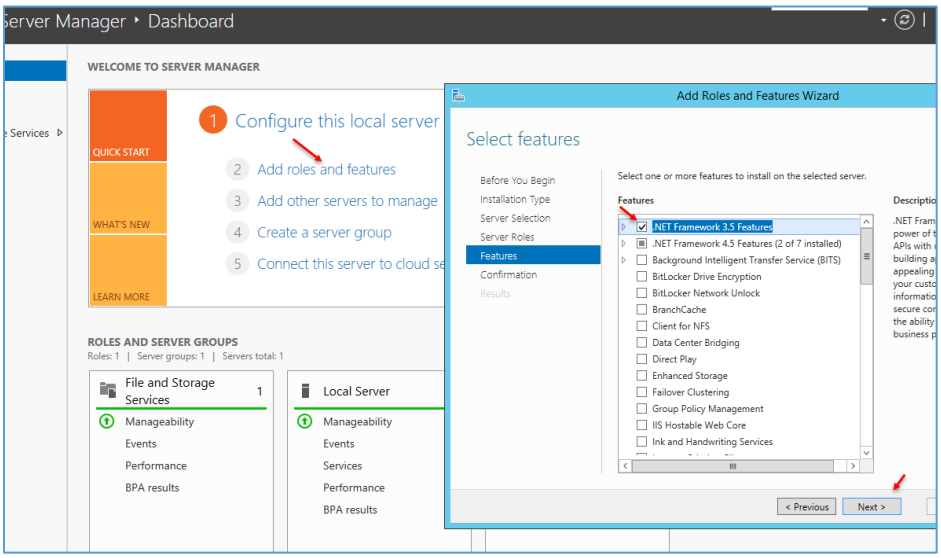




بعد از ست کردن آدرس IP وارد System Properties شوید و به مانند شکل، نام سیستم را تغییر دهید و آن را عضو دومین کنید که در اینجا، دومین شما 3isco.ir است.

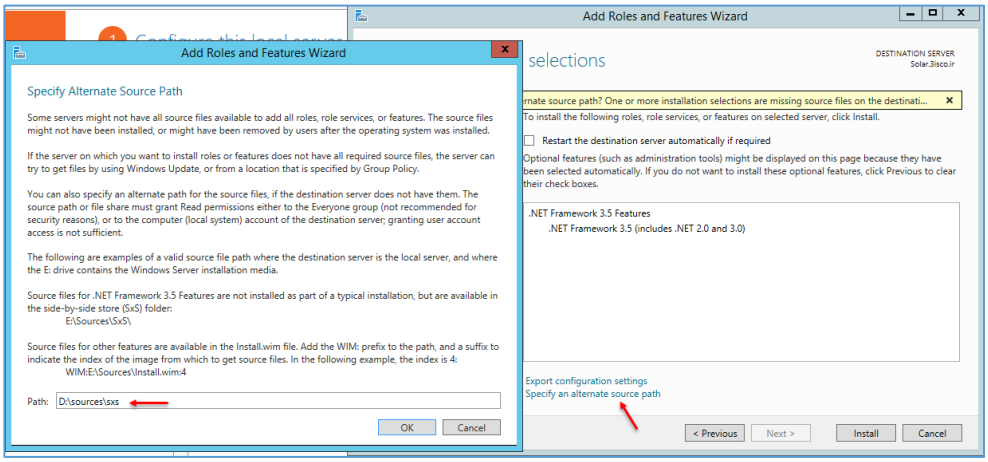
بعد از اینکه سرور را عضو دومین کردید باید شروع به نصب نرم‌افزار SolarWins کنید، این نرم‌افزار نیاز به SQL دارد که باید بر روی این سرور راه‌اندازی کنید، البتّه می‌توانید SQL را در یک سرور دیگر راه‌اندازی کنید و به این نرم‌افزار معرّفی کنید؛ در این کتاب SQL را در سرور Solar نصب می‌کنیم.

برای نصب SQL، مثل همیشه نیاز به نصب کامپونت Net FramWork 3.5 دارید که برای نصب باید به صورت زیر عمل کنید.



برای نصب Net FramWork 3.5 وارد Server Manager شوید و بر روی Add roles and Features کلیک کنید و تیک گزینه‌ی Net Framwork 3.5 را انتخاب و بر روی Next کلیک کنید.

در این صفحه بر روی source path Specify an alternate کلیک کنید و آدرس مربوط به ویندوز سرور ۲۰۱۲ را در قسمت مشخّص شده، وارد و بر روی OK و در آخر بر روی Install کلیک کنید.



بعد از اینکه Net 3.5 را نصب کردید، نوبت به نصب SQL است.

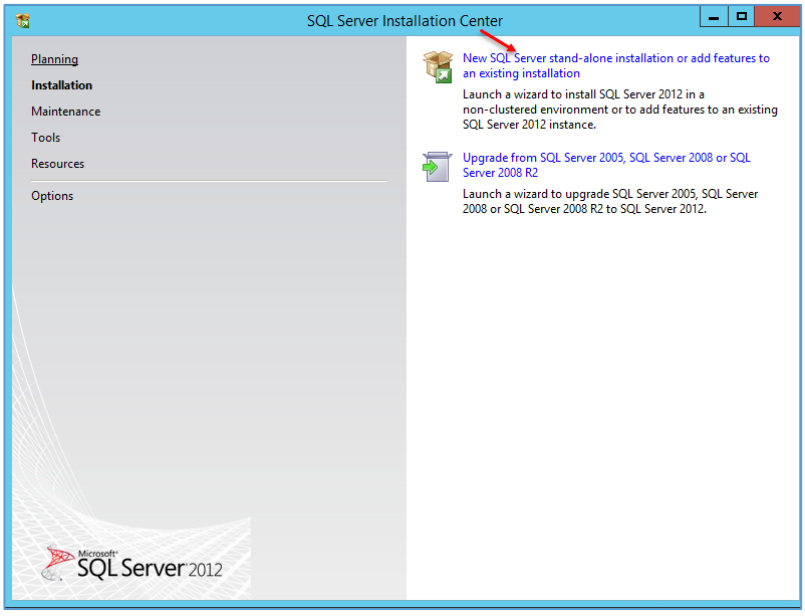
ورژن‌هایی که نرم‌افزار Solar آنها را پشتیبانی می‌کنند، عبارتند از:

SQL Server 2005 SP1 or later (32-bit or 64-bit)
SQL Server 2008 RTM or later (32-bit or 64-bit)
SQL Server 2008 R2 RTM or later (32-bit or 64-bit)
SQL Server 2012 RTM or later (32-bit or 64-bit)

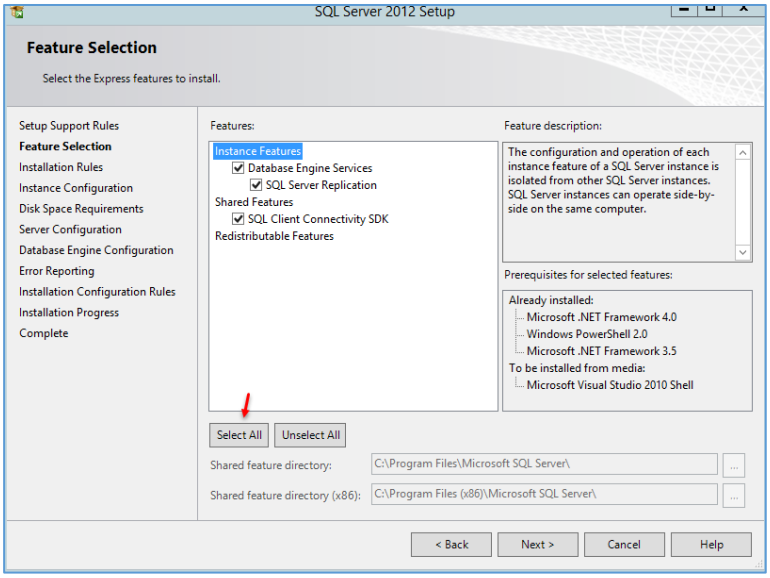
برای این سرور، ورژن ۲۰۱۲ را انتخاب کردیم که شما نیز می‌توانید از لینک زیر دانلود کنید:

https://www.microsoft.com/en-us/download/details.aspx?id=29062

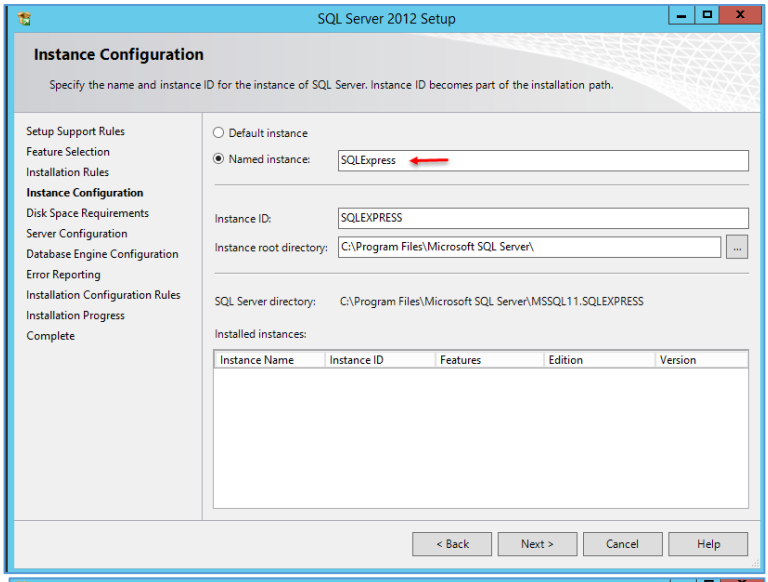
بعد از دانلود، دو بار بر روی فایل اجرایی کلیک کنید.



در این صفحه برای شروع نصب بر روی New SQL Server... کلیک کنید.

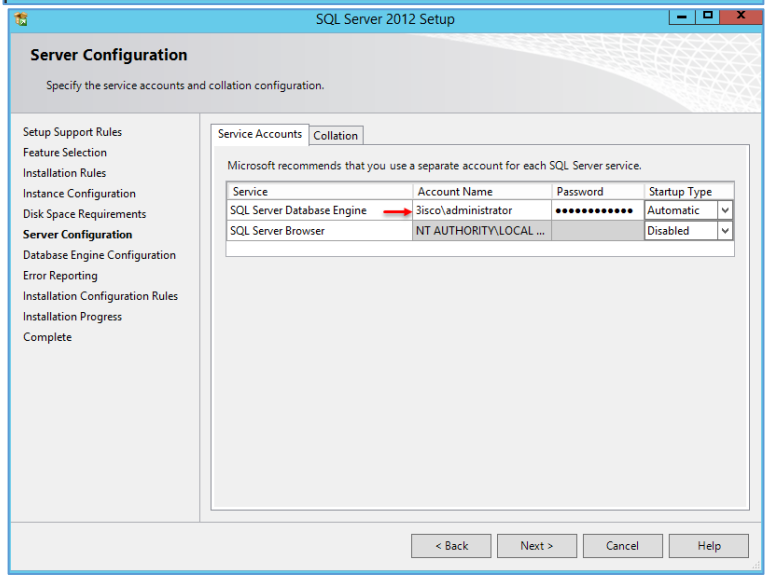


در این صفحه بر روی Select All کلیک و بعد بر روی Next کلیک کنید.

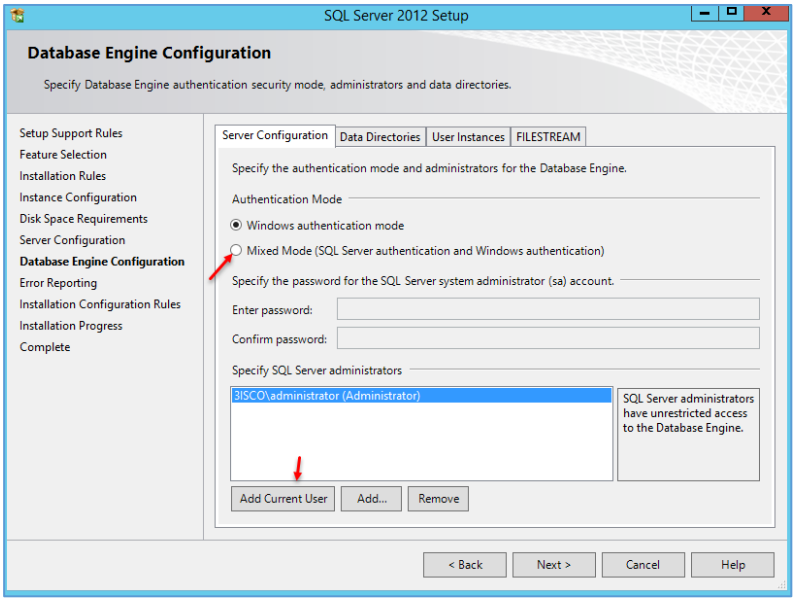


در این صفحه باید نام Instance برای SQL تعریف کنید که به صورت پیش‌فرض، SQLEXPRESS تعریف شده است که می‌توانید این نام را به هر نامی تغییر دهید.

بر روی Next کلیک کنید.

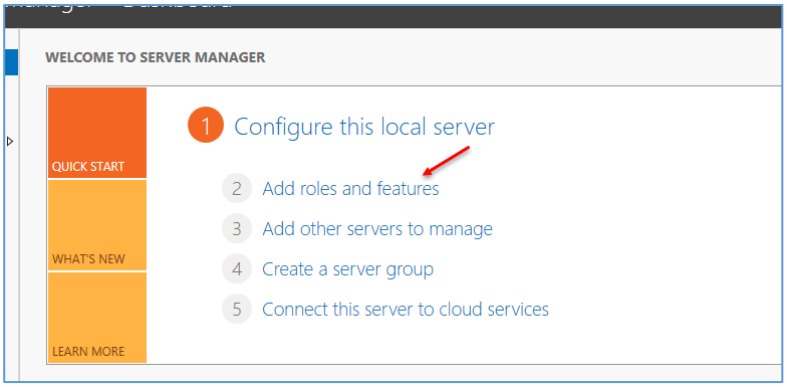


در این صفحه، یک نام کاربری را با دسترسی بالا، به صورت روبرو وارد کنید و رمز عبور آن را نیز در قسمت Password وارد و بر روی Next کلیک کنید.

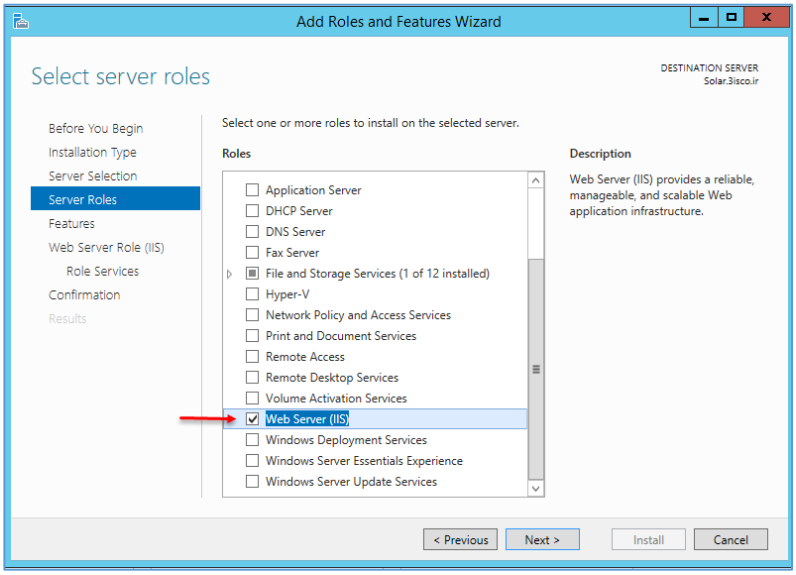


در این صفحه، گزینه‌ی Mixed Mode را انتخاب کنید و یک رمز برای آن تعیین کنید و در پایین صفحه، یک کاربر برای مدیریّت SQL وارد کنید که می‌توانید بر روی Add Current User کلیک کنید.

بر روی Next کلیک کنید تا کار نصب آغاز شود.



بعد از نصب SQL نیاز است تا سرویس IIS را قبل از نصب نرم‌افزار مانیتورینگ، راه‌اندازی کنید، برای این کار وارد Server Manager شوید و بر روی Add Roles and Features کلیک کنید.



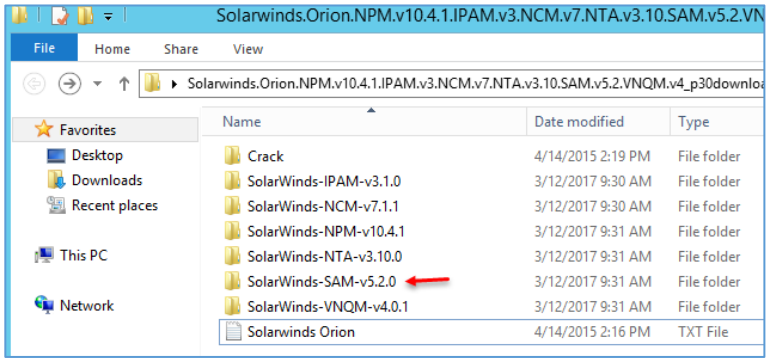
در قسمت Server Roles، تیک گزینه‌ی IIS را انتخاب و بر روی Next کلیک کنید و در آخر بر روی Install کلیک کنید تا کار نصب آغاز شود.

بعد از نصب، حتماً سرور را Restart کنید.

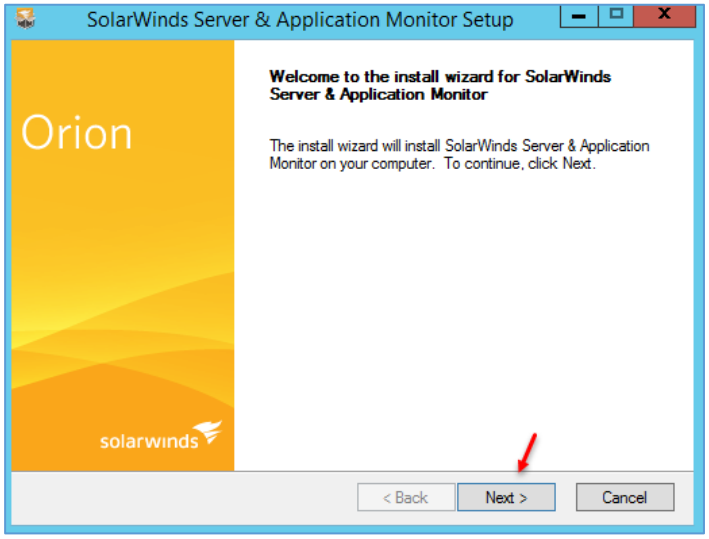
برای نصب برنامه‌ی مانیتورینگ Solar، آن را از لینک زیر دانلود کنید:

http://p30download.com/fa/entry/58415/

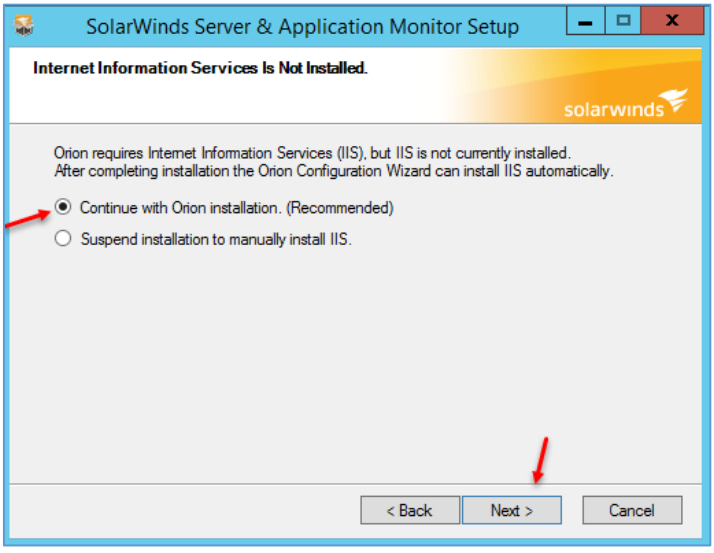
بعد از نصب نرم‌افزار، آن را به سرور انتقال دهید و به مانند زیر شروع به نصب کنید.



بعد از دانلود برای شروع کار وارد پوشه‌ی SolarWinds –SAM –v5.2.0 شوید و دو بار بر روی فایل اجرایی کلیک کنید.



بر روی Next کلیک کنید.

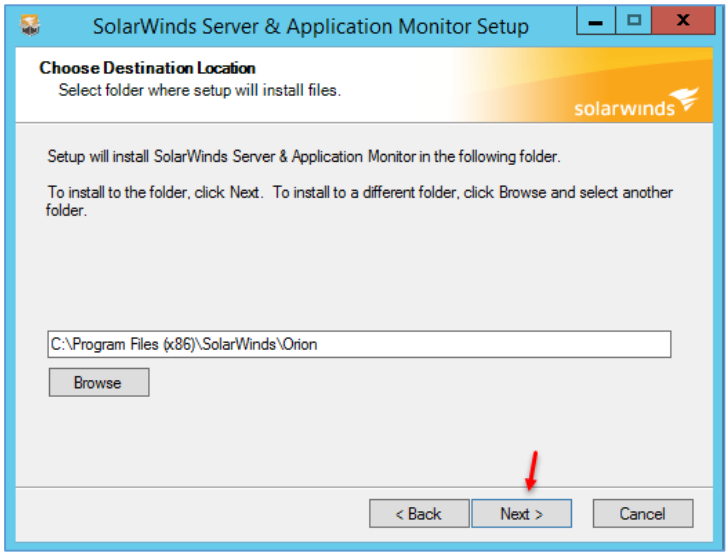


در این صفحه، اگر می‌خواهید نرم‌افزار به صورت اتوماتیک سرویس IIS را کانفیگ کند، گزینه‌ی اوّل و اگر می‌خواهید، بعداً خودتان سرویس IIS را نصب کنید، گزینه‌ی دوّم را انتخاب کنید.

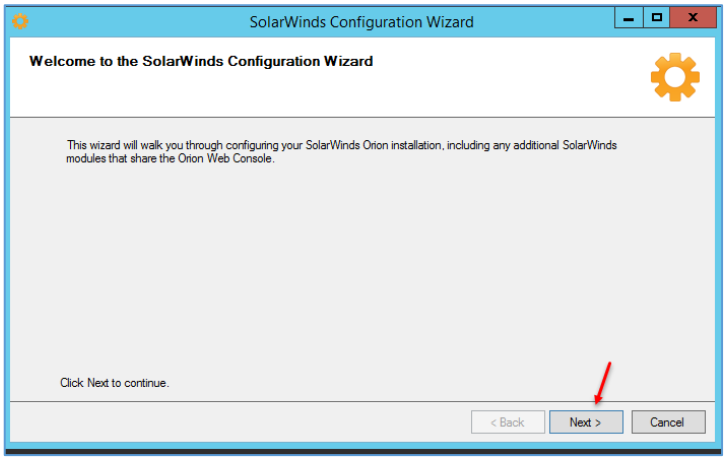
در این صفحه، گزینه‌ی اوّل را انتخاب و بر روی Next کلیک کنید.



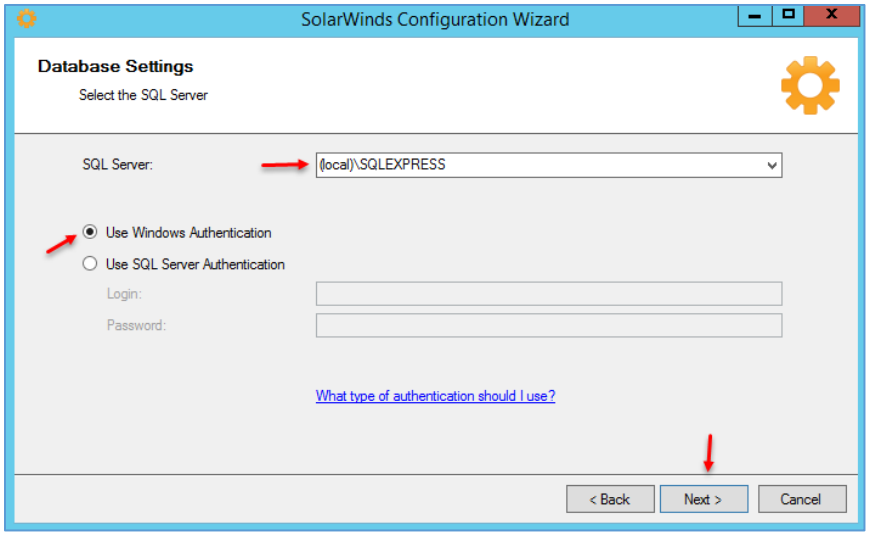
در این قسمت، اگر توافقنامه‌ی استفاده از نرم‌افزار را قبول دارید، می‌توانید تیک گزینه‌ی ...I accept را انتخاب و بر روی Next کلیک کنید.



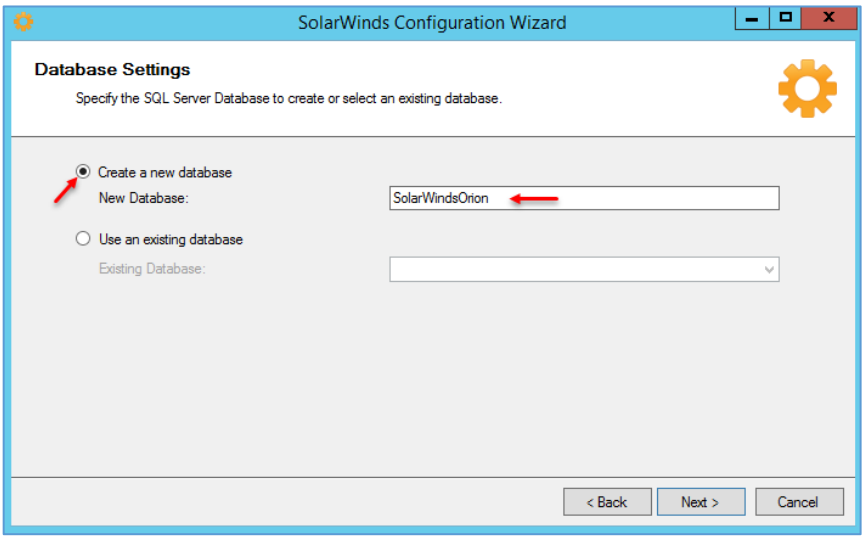
در این قسمت می‌توانید مسیر ذخیره‌سازی نرم‌افزار را مشخّص کنید، توجّه داشته باشید باید محلّ مورد نظر، فضای کافی داشته باشد، بر روی Next کلیک کنید.



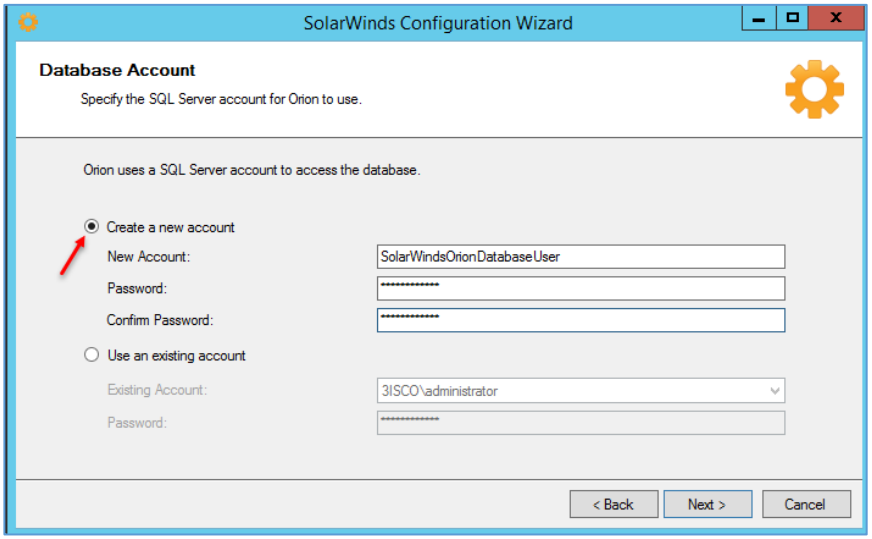
بعد از نصب، این صفحه ظاهر می‌شود که برای Config کردن نرم‌افزار است، برای شروع بر روی Next کلیک کنید.



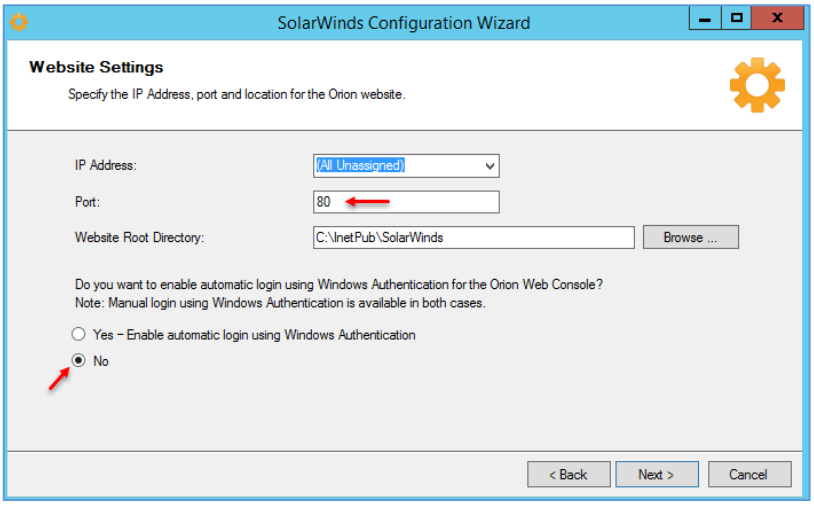
در این صفحه باید SQL سرور خود را انتخاب کنید و از آنجایی که SQL در داخل خود سرور مانیتورینگ نصب شده است، گزینه‌ی Local به همراه نام SQLEXPRES ظاهر می‌شود که نام آن را در قسمت‌های قبل در زمان نصب SQL وارد کردیم، در قسمت احراز هویّت نیز گزینه‌ی Use Windows Authentication را انتخاب و بر روی Next کلیک کنید.



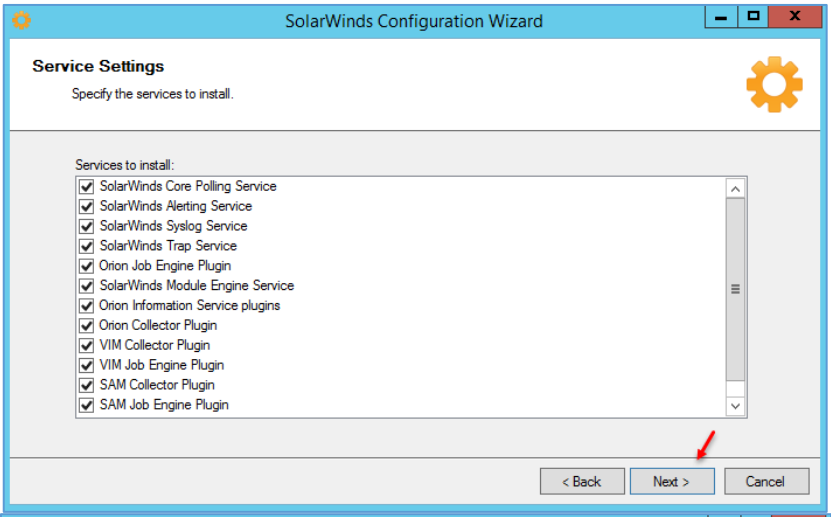
در این صفحه باید نام دیتابیس خود را مشخّص کنید که به صورت پیش-فرض، نام SolarWindsOrion وارد شده است که می‌توانید نام دلخواه خود را وارد و بر روی Next کلیک کنید.



در این صفحه باید یک کاربر جدید ایجاد کنید که در SQL دسترسی لازم به دیتابیس Solar داشته باشد، به مانند شکل، گزینه‌ی اوّل را انتخاب و نام کاربر و رمز عبور آن را وارد کنید و بر روی Next کلیک کنید.

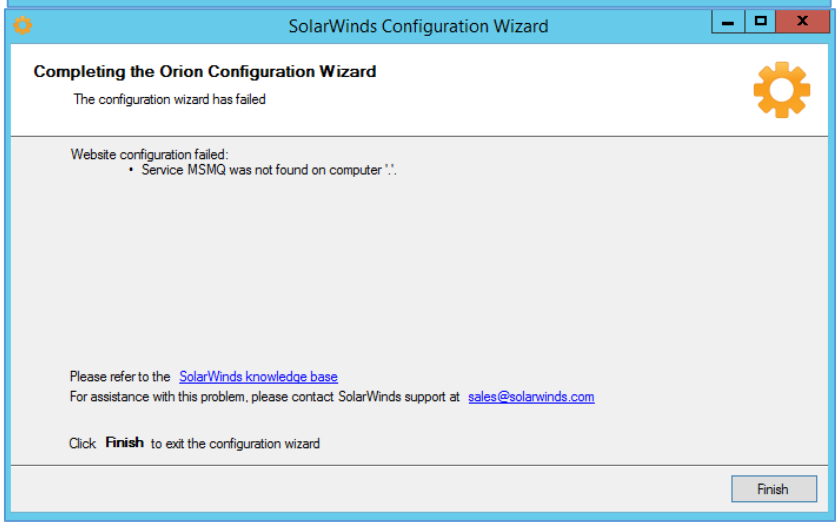


در این قسمت برای متّصل شدن به سرویس تحت وب می‌توانید در بخش اوّل، آدرس سرور خود را از لیست انتخاب کنید و در بخش دوّم، پورت مورد نظر آن را مشخّص کنید که به صورت پیش‌فرض بر روی ۸۰ قرار دارد و در قسمت آخر، اگر گزینه‌ی Yes را انتخاب کنید، زمانی که کاربر با نام کاربری که دسترسی به سایت دارد، وارد کلاینت خود شود، در صورت اجرای آن، سایت به صورت اتوماتیک برای او باز خواهد شد، فعلاً گزینه‌ی No را انتخاب کنید تا در زمان وارد شدن به سایت از شما، نام کاربری و رمز عبور درخواست شود.

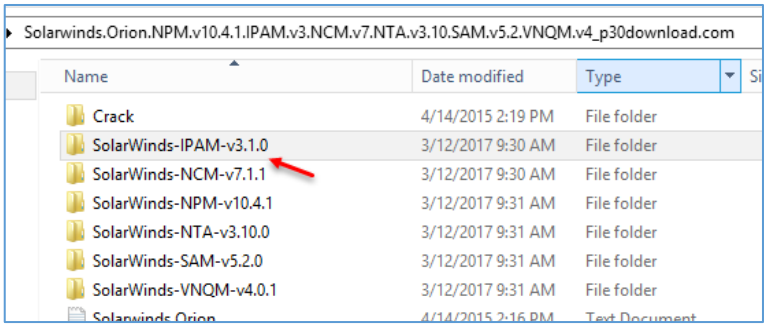


در این صفحه، سرویس‌هایی که مختصّ نرم‌افزار SolarWinds است را مشاهده می‌کنید که باید بر روی سرور اجرا شوند.

بر روی Next کلیک کنید و در صفحه‌ی بعد نیز بر روی Next کلیک کنید تا کار نصب آغاز شود.



همانطور که مشاهده می‌کنید، سرویس مورد نظر به خوبی بر روی سرور نصب شده است، بر روی Finish کلیک کنید.



بعد از اینکه نرم‌افزار SAM را با موفّقیّت نصب کردید، باید نرم‌افزار IPAM یا همان، IP Address Manager را نصب کنید، به مانند شکل روبرو وارد پوشه‌ی آن شوید.

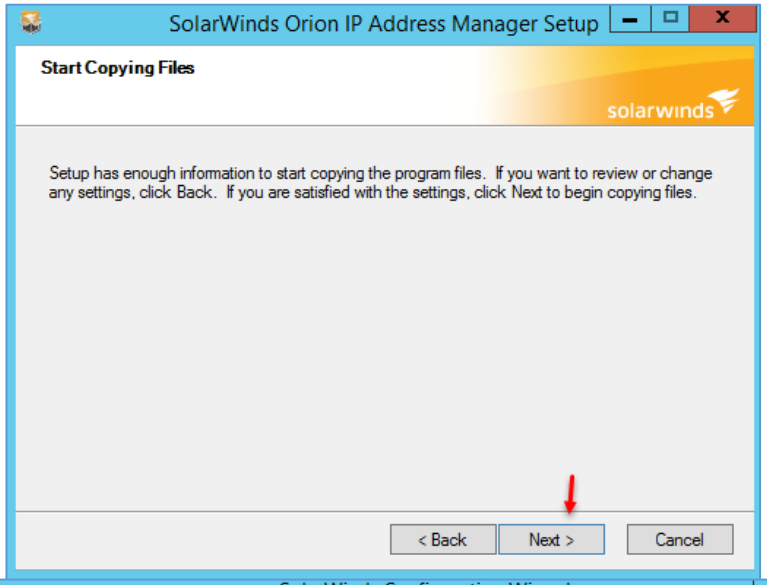


در این صفحه بر روی Next کلیک کنید.

نکته: از آنجایی که در قسمت قبل، دیتابیس و سرویس‌ها را آماده کردیم در ادامه، نصب نرم‌افزارها سریعتر انجام خواهد گرفت.

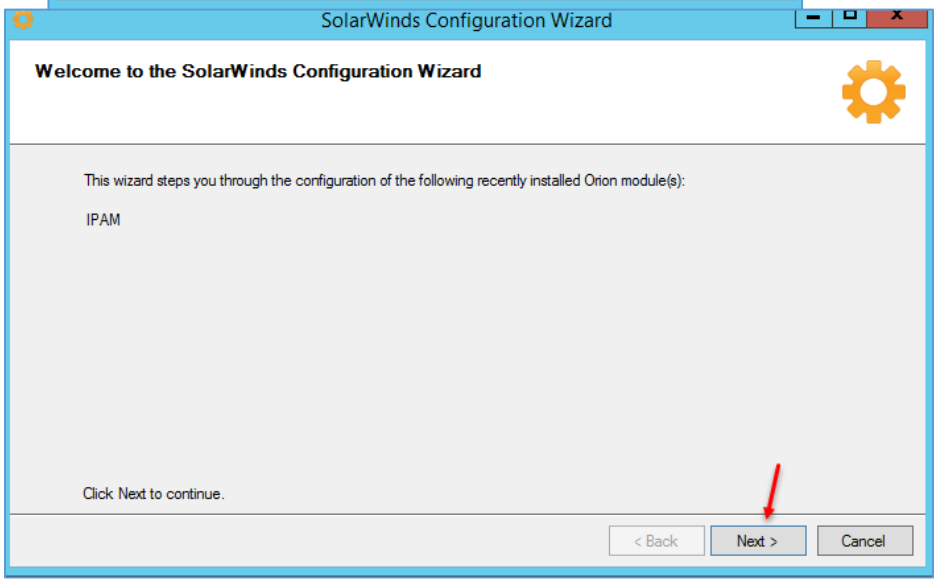


در این صفحه، تیک گزینه‌ی I Accept را انتخاب و بر روی Next کلیک کنید.

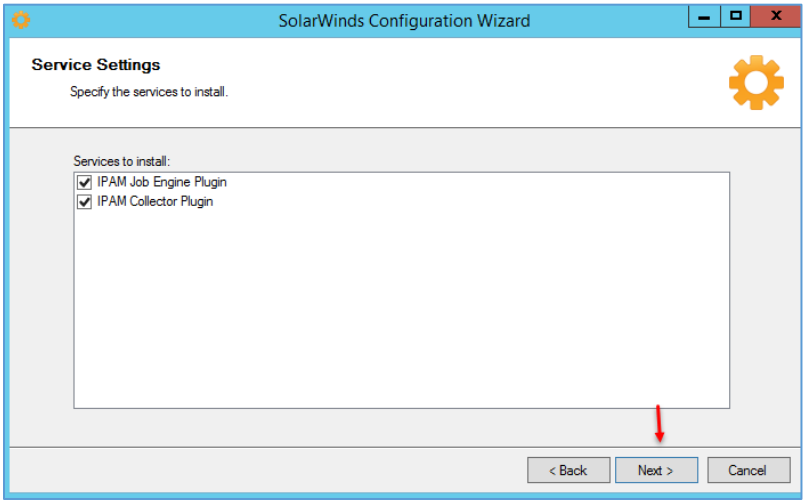


در این قسمت بر روی Next کلیک کنید تا کار نصب آغاز شود.

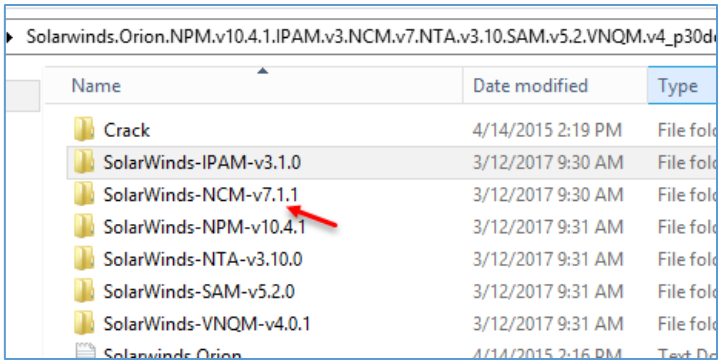
اگر در هنگام نصب با خطایی که مربوط به فایل CLR نرم‌افزار SQL است، روبرو شدید از اینجا فایل را دانلود و بر روی سرور نصب کنید.



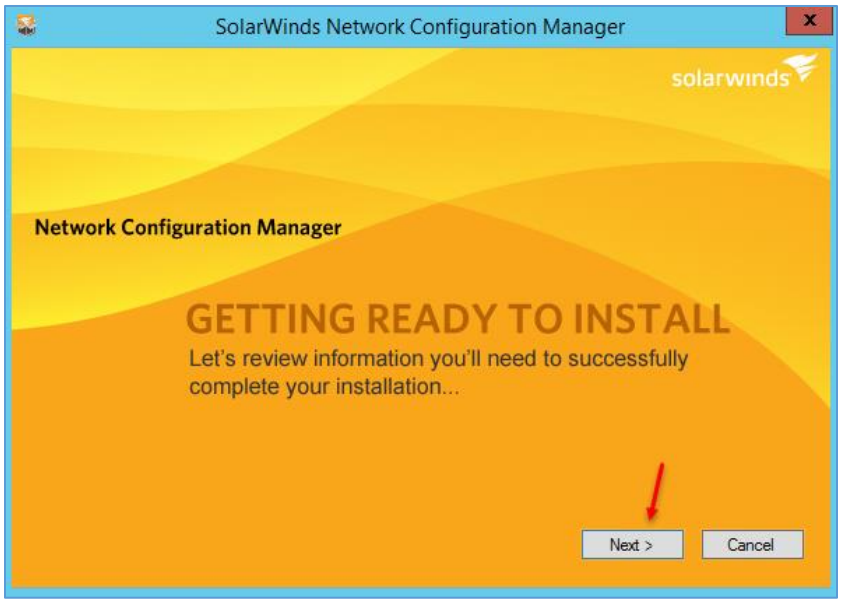
بعد از اتمام نصب و کلیک بر روی Finish، شکل روبرو ظاهر می‌شود که برای راه‌اندازی سرویس‌های IPAM است، بر روی Next کلیک کنید.



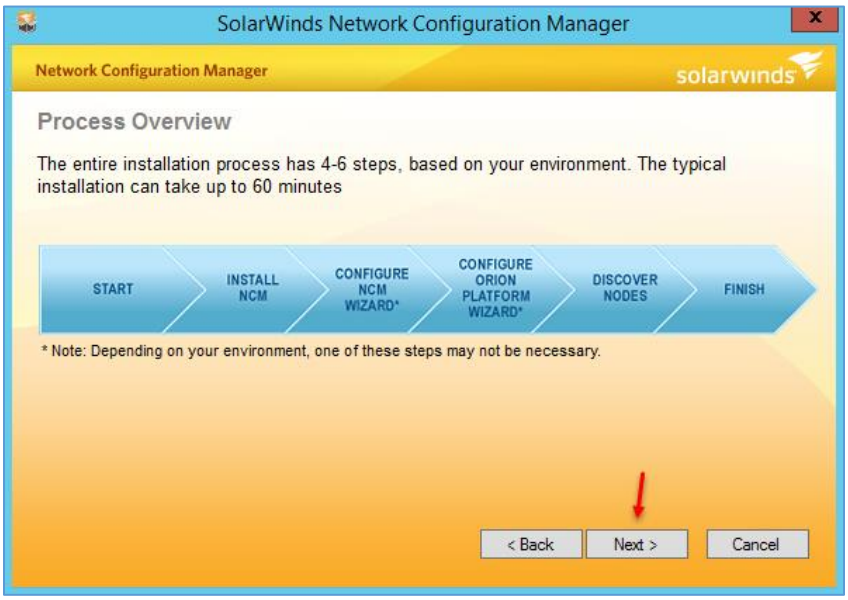
در این صفحه بر روی Next کلیک کنید و در صفحه‌ی بعد نیز بر روی Next کلیک کنید تا سرویس‌های مورد نظر راه‌اندازی شود.



بعد از نصب IPAM وارد پوشه‌ی NCM یا همان، Network Configuration Manager شوید و فایل را اجرا کنید.

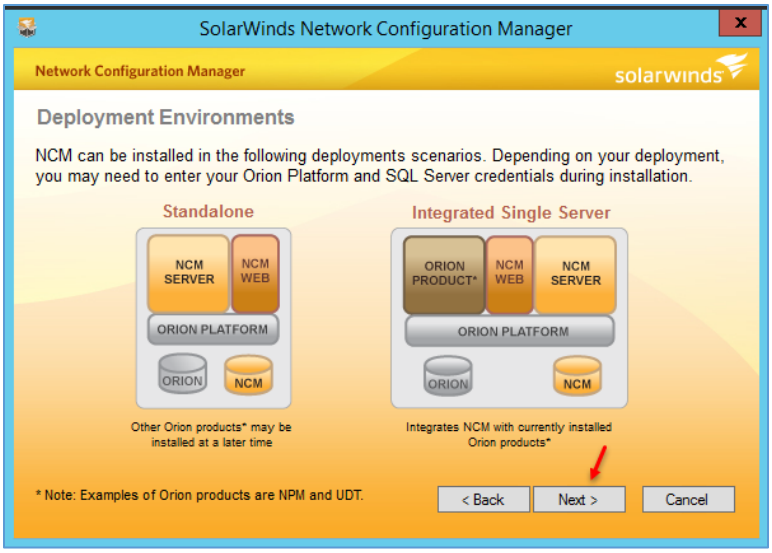


در صفحه‌ی اوّل بر روی Next کلیک کنید.

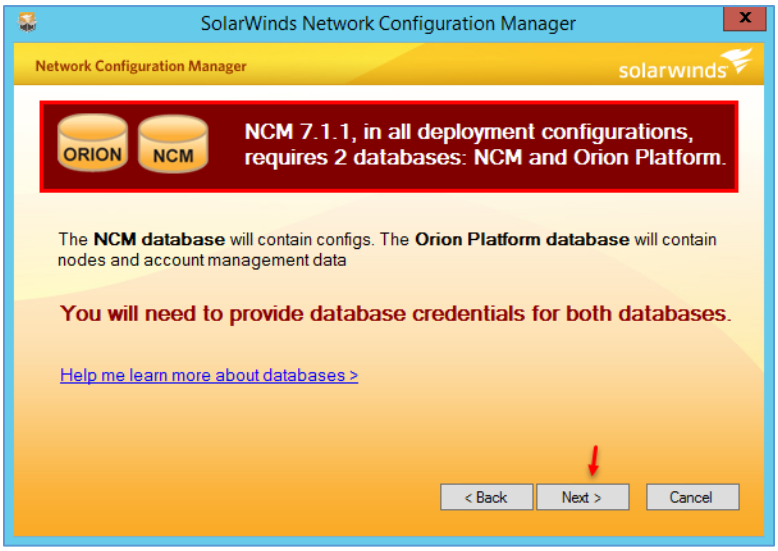


در این صفحه، مراحل نصب به ترتیب مشخّص شده است، بر روی Next کلیک کنید.

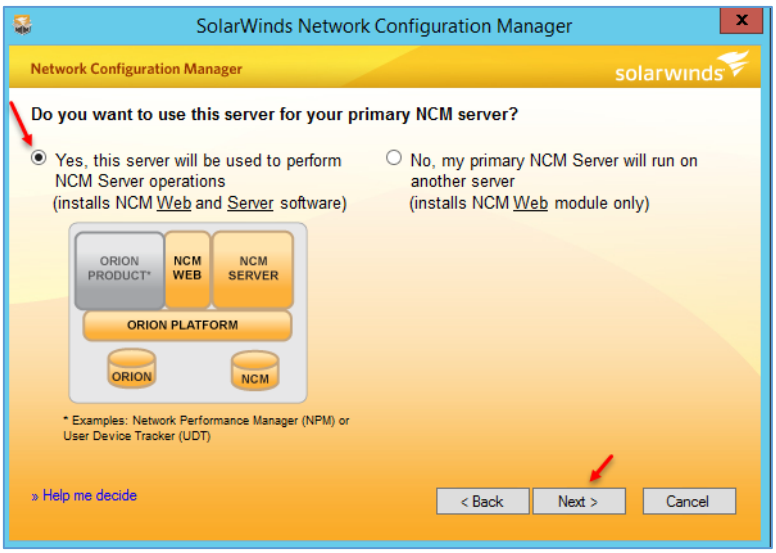
در این صفحه بر روی Next کلیک کنید.



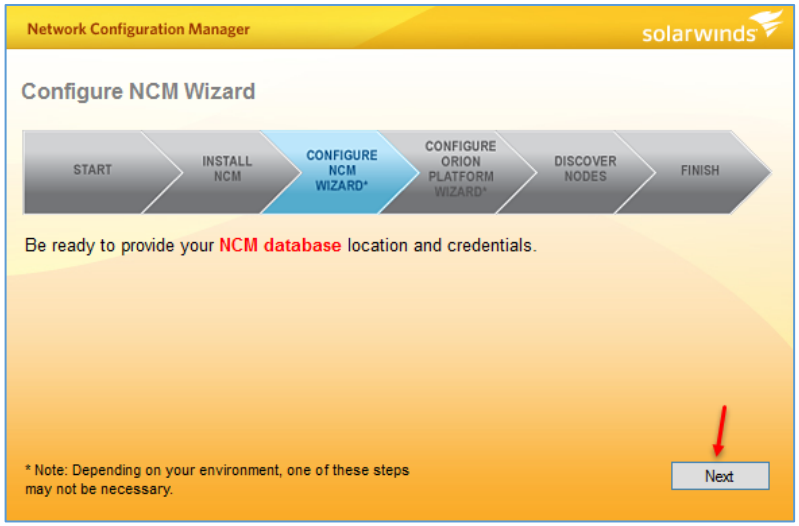
در این صفحه بر روی Next کلیک کنید.



در این صفحه، اگر گزینه‌ی اوّل را انتخاب کنید، همین سرور به عنوان سرور اصلی انتخاب می‌شود و اگر سرور اصلی شما در جایی غیر از این سرور باشد، می‌توانید گزینه‌ی دوّم را انتخاب و آدرس سرور را ست کنید، بر روی Next کلیک کنید.

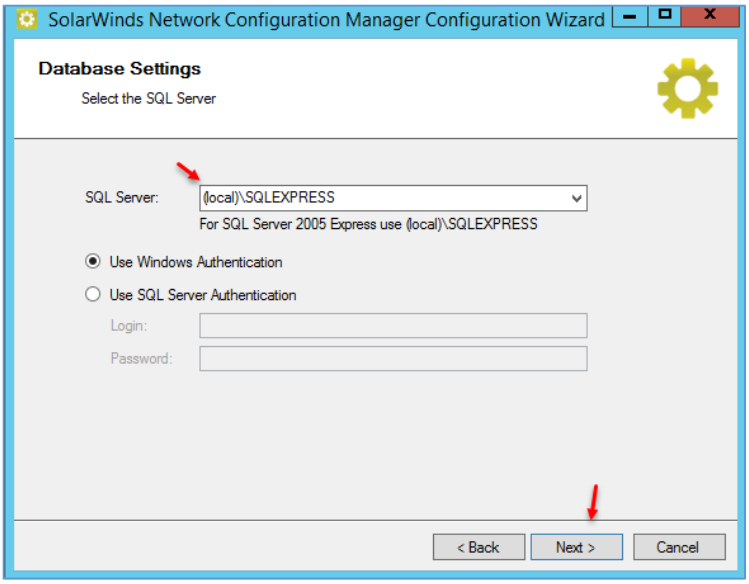


در صفحات بعد نیز بر روی Next کلیک کنید تا کار نصب آغاز شود.

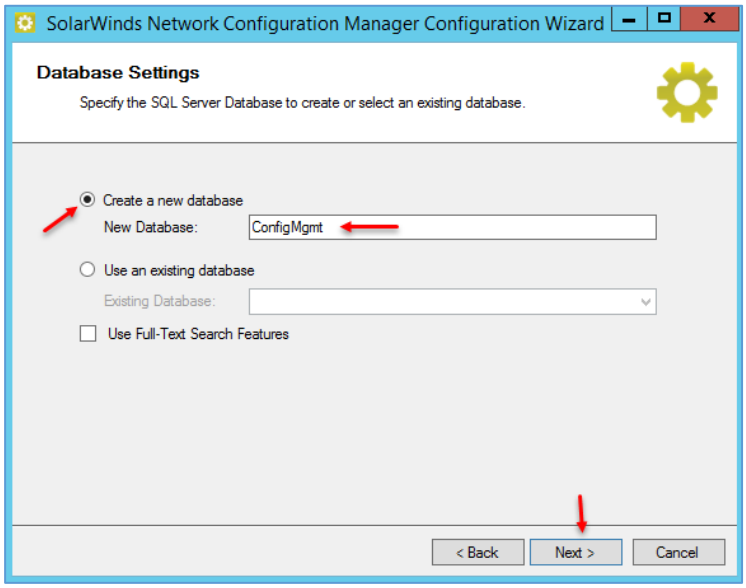


بعد از نصب، شکل روبرو ظاهر می‌شود که باید کار کانفیگ NCM را انجام دهید.

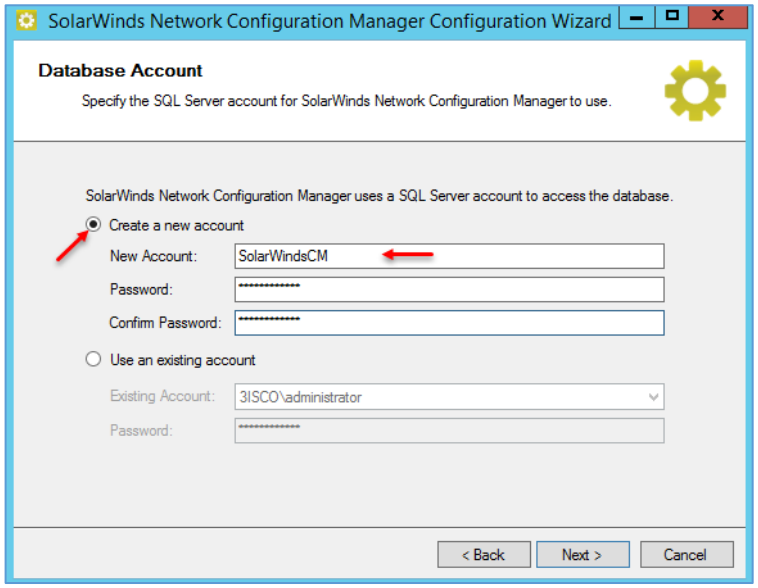
بر روی Next کلیک کنید.



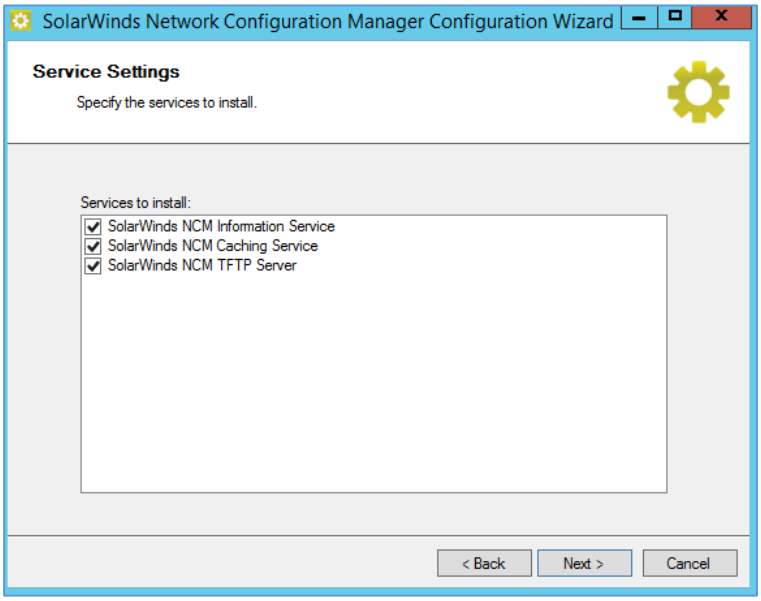
در این قسمت باید SQL خود را مشخّص کنید، مانند قبل باید SQL که بر روی همین سرور Solar نصب کردید را انتخاب کنید و در پایین صفحه، گزینه‌ی Use windows Authentication را انتخاب کنید.



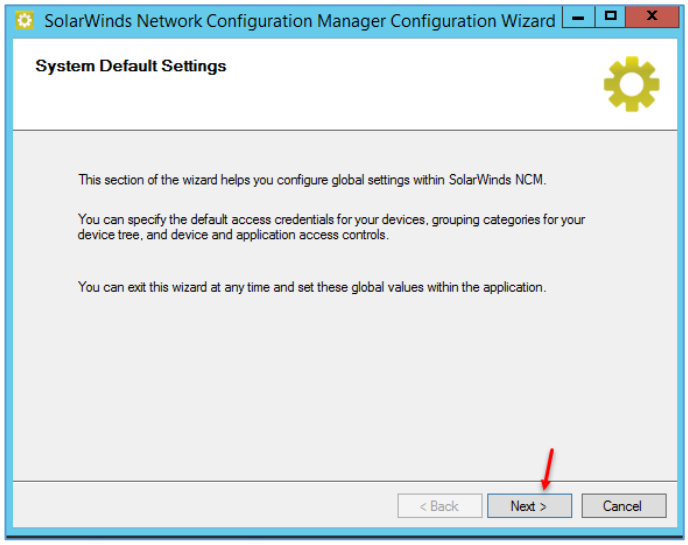
در این قسمت باید یک دیتابیس جدید برای نرم-افزار NCM ایجاد کنید، یک اسم پیش‌فرض در شکل روبرو وارد شده است که شما می‌توانید نام مورد نظر خود را وارد کنید.



یک کاربر جدید نیز برای دسترسی به دیتابیس برای نرم‌افزار NCM ایجاد کنید، نام این کاربر را می‌توانید تغییر دهید و به دلخواه، رمز عبور مربوط به آن را وارد کنید.

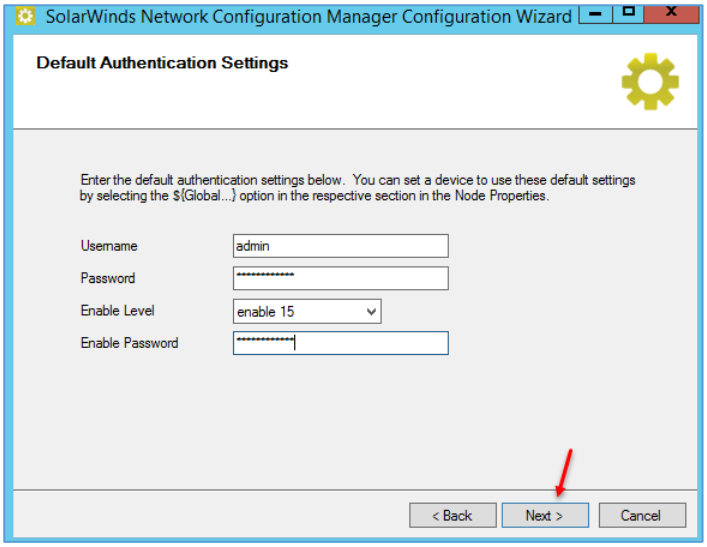


در این صفحه، سرویس‌های مربوط به نرم‌افزار NCM را مشاهده می‌کنید که با کلیک بر روی Next، کار نصب آغاز خواهد شد.



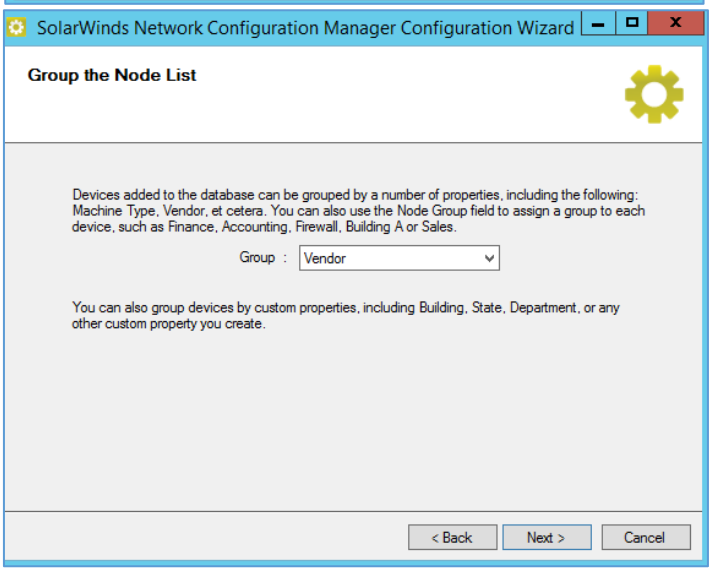
در این قسمت باید تنظیمات دسترسی به نرم‌افزار و شبکه را وارد کنید.

بر روی Next کلیک کنید.

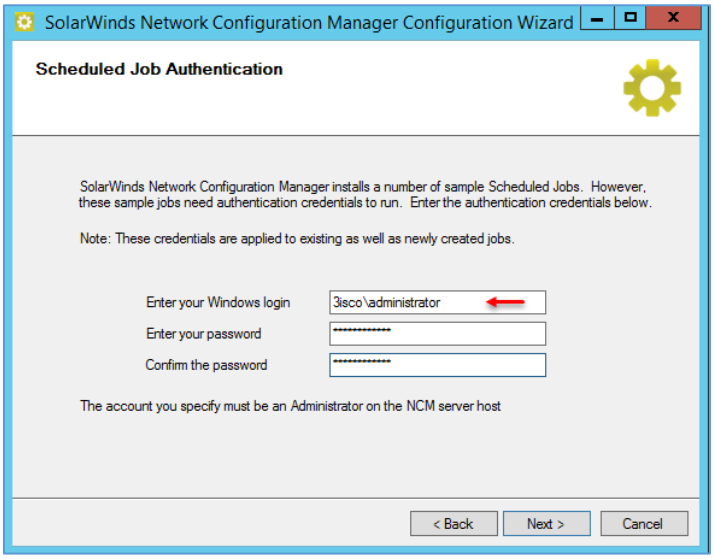


در این صفحه باید یک کاربر پیش‌فرض برای دسترسی به نرم‌افزار تعریف کنید و رمز عبور مربوط به آن را وارد کنید.

در پایین آن باید سطح دسترسی را مشخّص کنید که Enable 15، بالاترین سطح است که برای آن نیز باید رمز عبور تعریف کنید و بر روی Next کلیک کنید.



در این صفحه بر روی Next کلیک کنید.

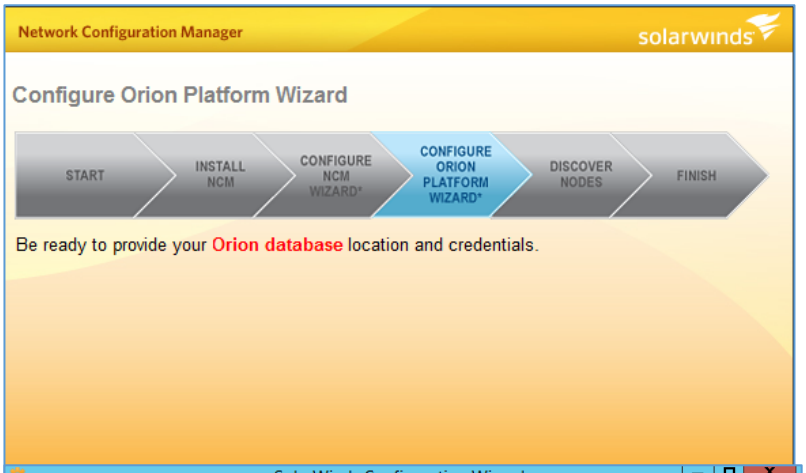


در این صفحه باید یک کاربر تعریف کنید که دسترسی لازم به کلّ شبکه را داشته باشد که در اینجا، کاربر Administrator به همراه نام دومین وارد شده است.

بر روی Next کلیک کنید.

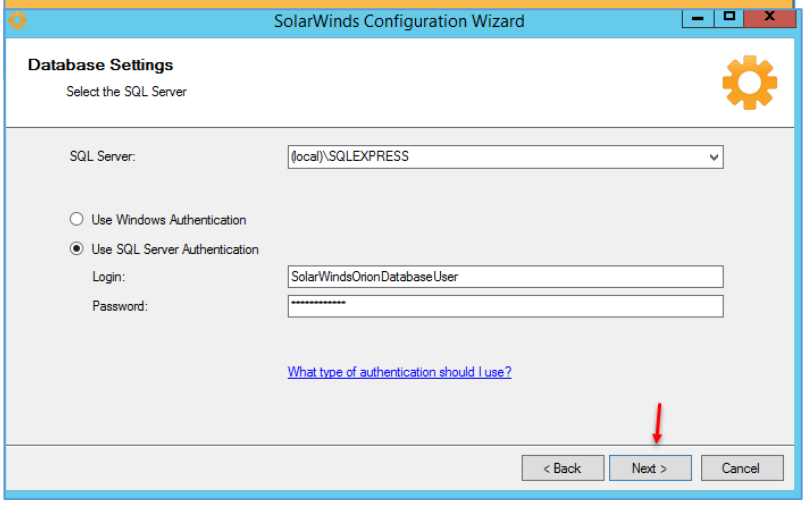
در صفحات بعد نیز بر روی Next کلیک کنید تا کار تنظیمات به پایان برسد.

در ادامه بر روی Next کلیک کنید.

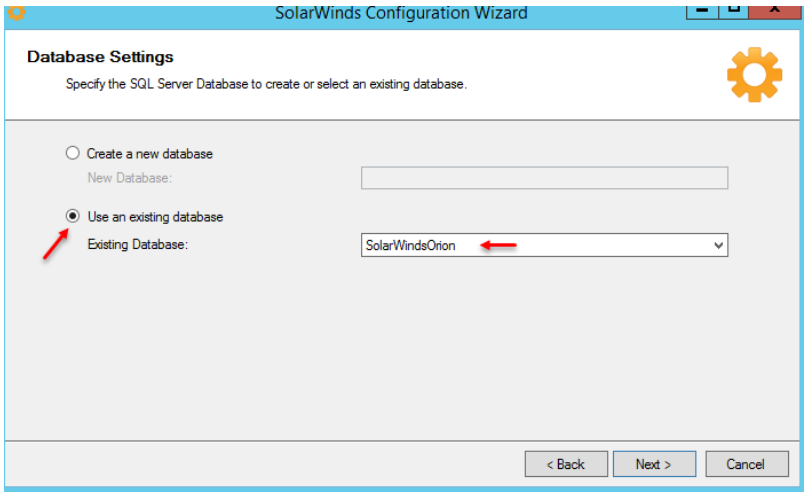


در این صفحه، همه چیز به صورت پیش-فرض وارد شده است، چون از قبل این گزینه‌ها را تنظیم کرده بودید.

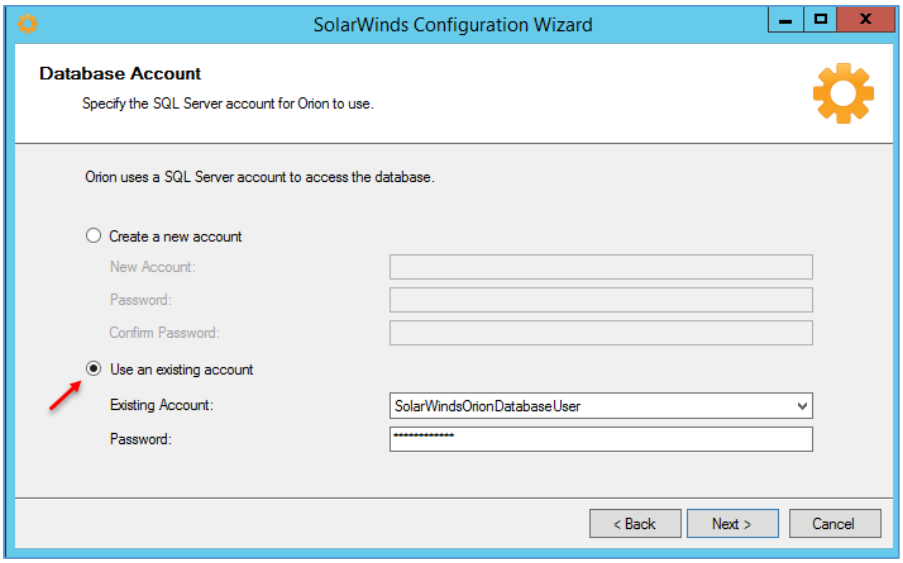
بر روی Next کلیک کنید.



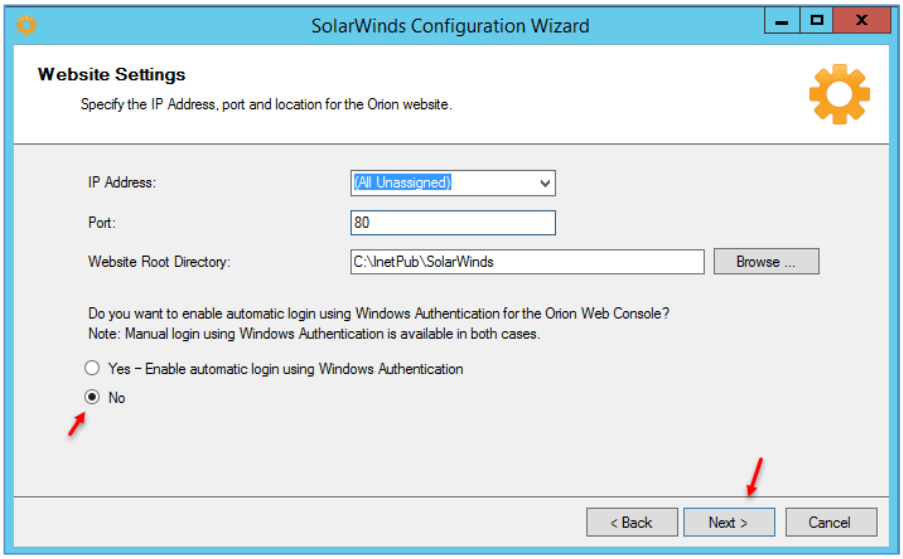
بر روی Next کلیک کنید.



بر روی Next کلیک کنید.

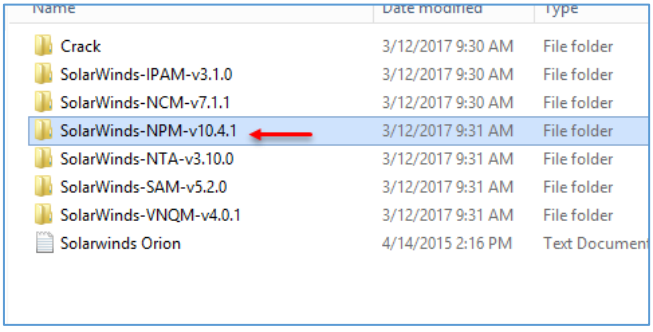


در این صفحه، به گزینه‌ای دست نزنید و بر روی Next کلیک کنید.



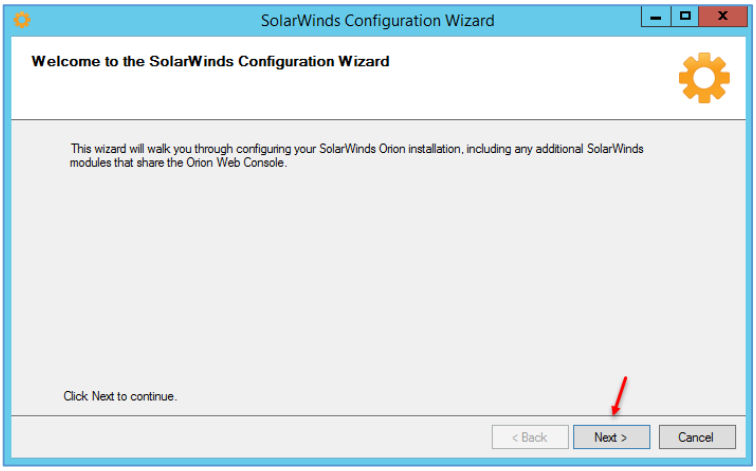
در صفحات بعد نیز بر روی Next کلیک کنید.

در پایان کار بر روی Finish کلیک کنید.

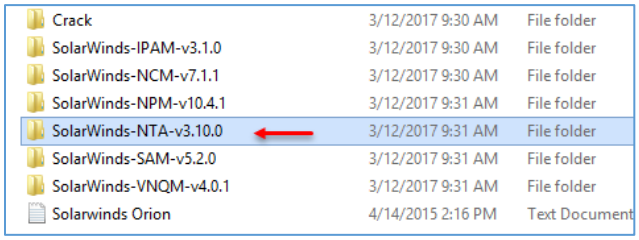


بعد از نصب NCM وارد پوشه‌ی NPM که همان، Network Performance Monitor شوید و دو بار بر روی فایل اجرایی کلیک کنید.

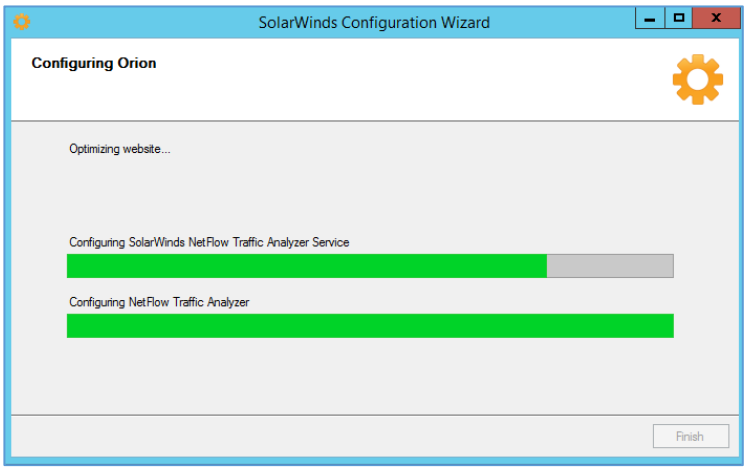
برای اینکه زمان را از دست ندهید، در صفحه‌ای که باز می‌شود، چند بار بر روی Next کلیک کنید تا کار نصب آغاز شود.



بعد از نصب، صفحه‌ی کانفیگ، به مانند شکل روبرو ظاهر می‌شود، در تمام مراحل بر روی Next کلیک کنید تا کانفیگ نرم‌افزار انجام شود و در صفحه‌ی آخر بر روی Finish کلیک کنید.

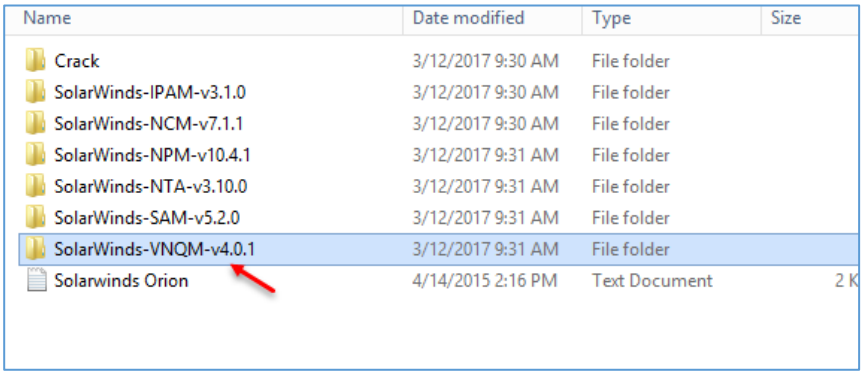


بعد از نصب این نرم‌افزار وارد پوشه‌ی NTA شوید و بر روی فایل اجرایی کلیک کنید؛ NTA، مخفّف NetFlow Traffic Analyzer است.



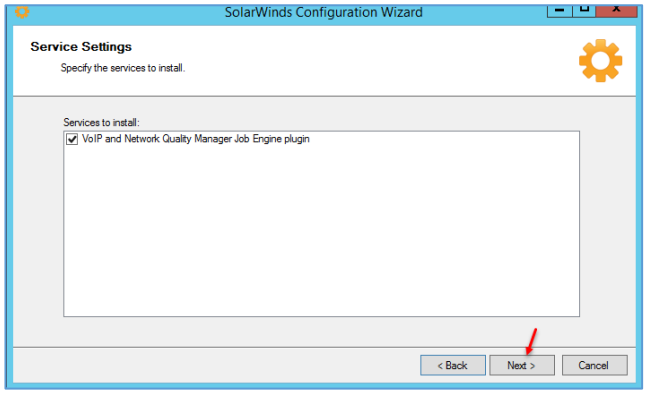
در صفحه‌ی باز شده بر روی Next کلیک کنید و نرم‌افزار را نصب کنید.

بعد از نصب، صفحه‌ی کانفیگ آن ظاهر می‌شود، بر روی Next کلیک کنید تا به مانند شکل روبرو کانفیگ به صورت اتوماتیک انجام شود.



بعد از نصب NTA، نوبت به نصب VNQM و یا همان، Voip and Network Qulity می‌رسد، وارد پوشه‌ی آن شوید و دو بار بر روی فایل اجرایی کلیک کنید.

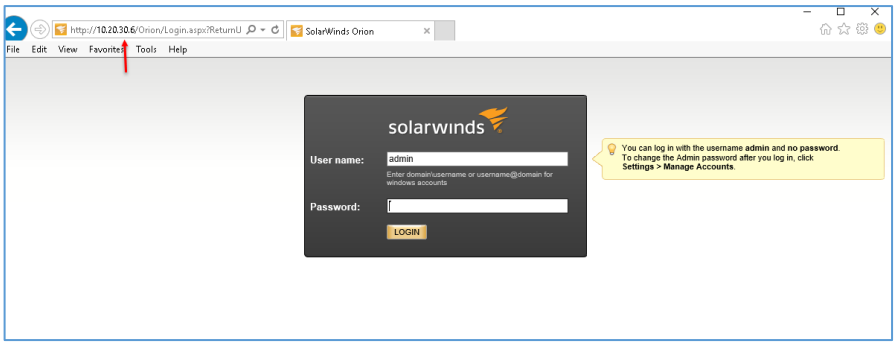
در صفحه‌ی باز شده بر روی Next کلیک کنید تا کار نصب آغاز شود.



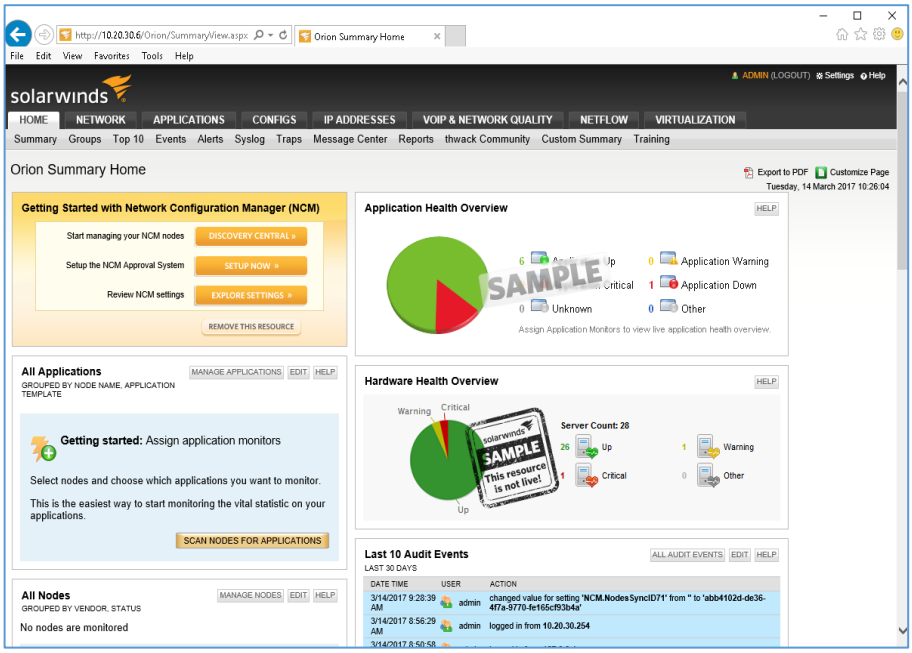
بعد از نصب، به مانند نرم‌افزارهای قبلی، قسمت تنظیمات و یا همان، کانفیگ ظاهر می‌شود که باید بر روی Next کلیک کنید تا کار تنظیمات انجام شود.

کار با سیستم تحت وب نرم‌افزار مانیتورینگ:

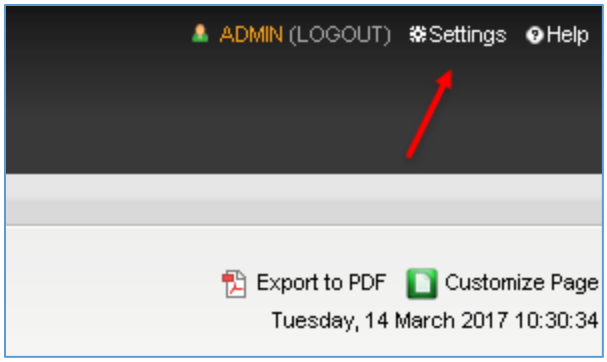
بعد از نصب تمام سرویس‌های نرم‌افزار SolarWinds باید کار با آنها را بیاموزید، این نرم‌افزارها با لایسنس خاصّی عمل می‌کنند که باید آن را خریداری کنید.



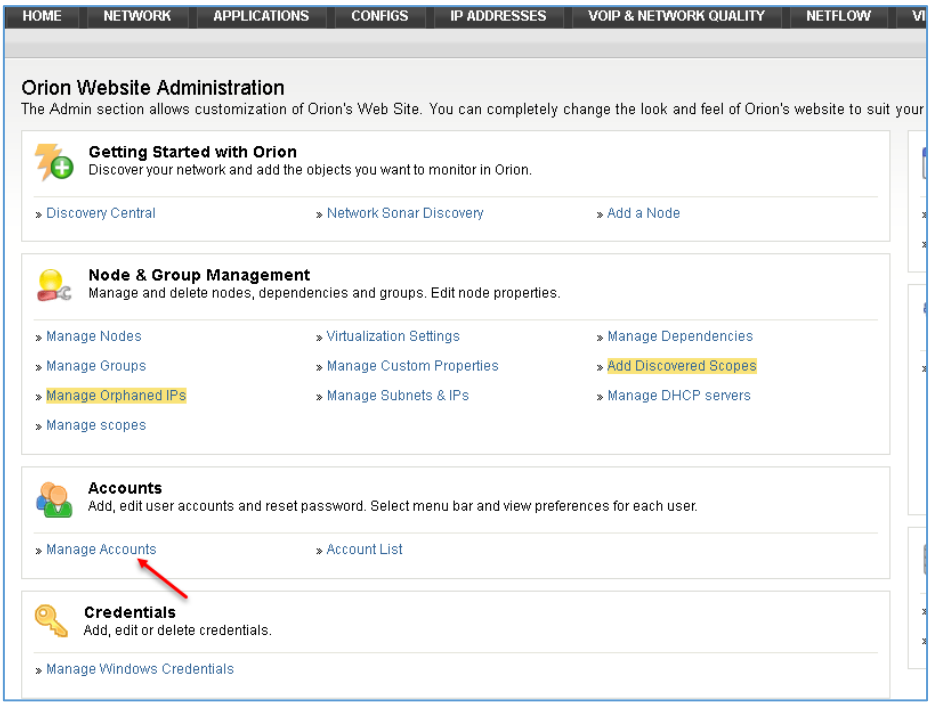
برای اینکه نرم‌افزار Solarwinds را اجرا کنید، آدرس IP سرور را در مرورگر وارد کنید تا شکل روبرو ظاهر شود، برای ورود به سرور به صورت پیش‌فرض کاربر admin وارد شده است که رمز عبوری نیز برای آن ست نشده است که بعد از کلیک بر روی Login باید اوّلین کار شما این باشد که برای آن رمز عبور قرار دهید.



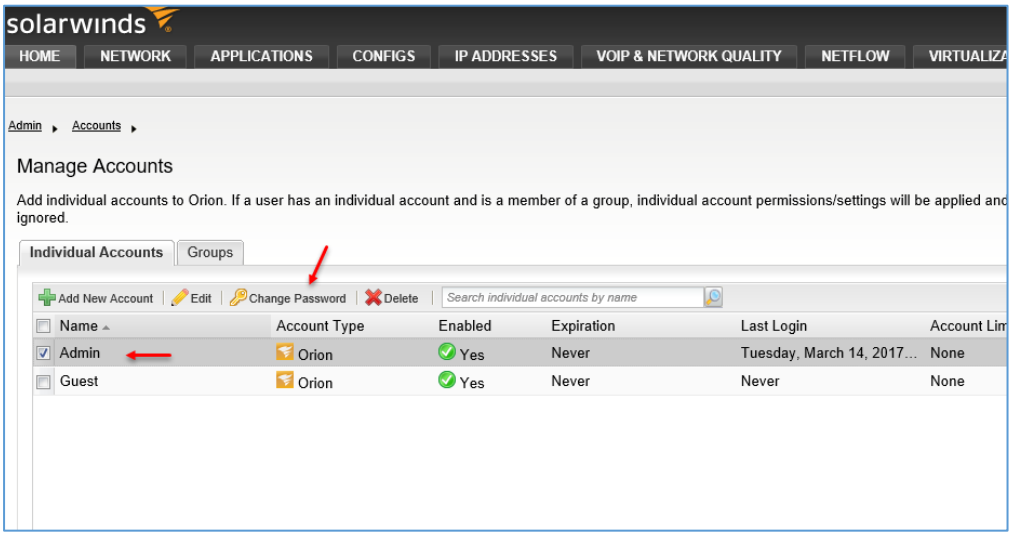
همانطور که در شکل روبرو مشاهده می‌کنید، نرم‌افزار SolarWinds به خوبی اجرا شده است که دارای تنظیمات و ابزارهای خاصّی است که در ادامه به آن‌ها خواهیم پرداخت.



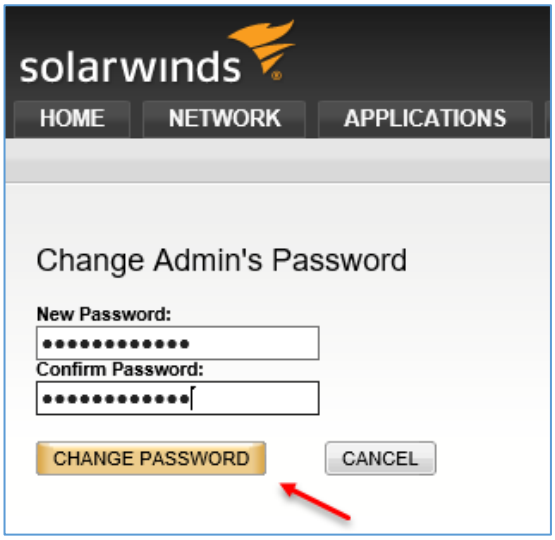
اوّلین کاری که باید در این نرم‌افزار انجام دهید، قرار دادن رمز عبور بر روی کاربر Admin است که برای این کار، به مانند شکل در سمت راست بر روی Settings کلیک کنید.



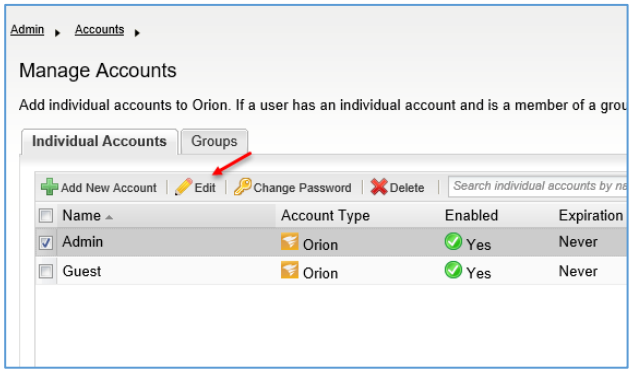
در صفحه روبرو در قسمت Accounts بر روی Manage Accounts کلیک کنید.



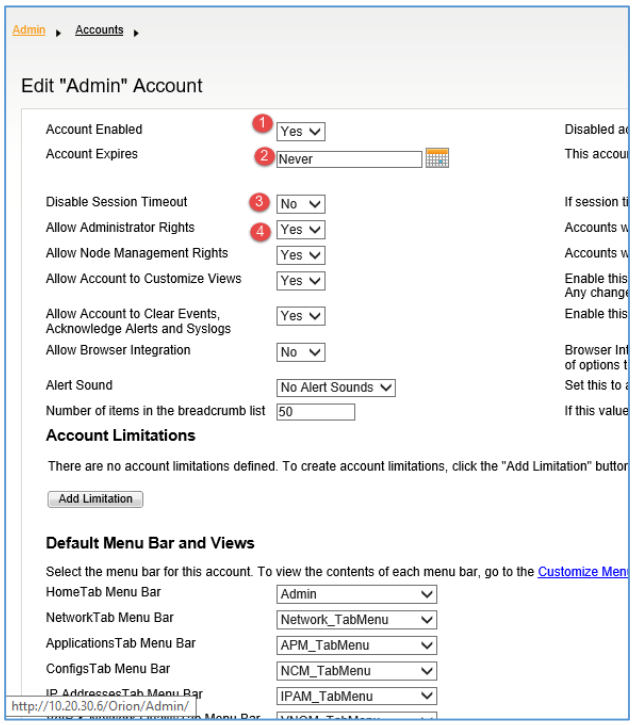
در این صفحه که اکانت‌های مورد نظر این نرم‌افزار را مشاهده می‌کنید، برای اینکه رمز عبور مربوط به کاربر مورد نظر را تغییر دهید باید تیک آن را انتخاب و بر روی Change Password کلیک کنید.



در این صفحه، رمز جدید خود را وارد و بر روی Change Password کلیک کنید تا کاربر Admin دارای رمز عبور شود.

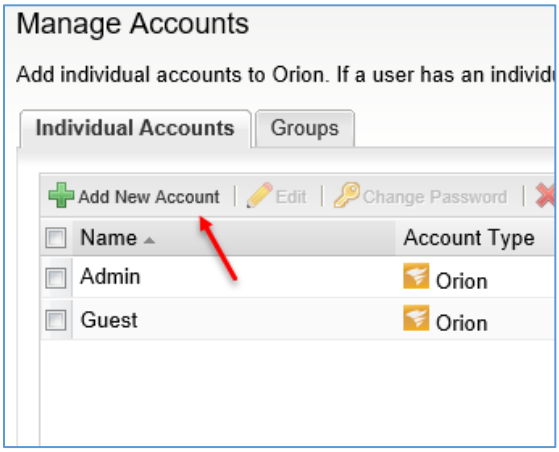


برای اینکه خصوصیّات یک اکانت را مشاهده کنید، به مانند شکل روبرو بر روی Edit کلیک کنید.

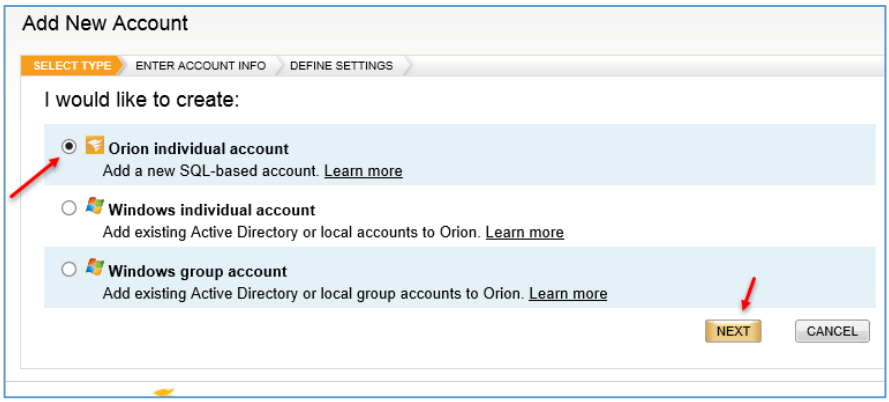


در این صفحه، گزینه‌های مختلفی را مشاهده می‌کنید، گزینه‌ی اوّل، اگر بر روی No قرار گیرد، اکانت Admin غیر فعّال خواهد شد، گزینه‌ی دوّم مربوط به تاریخ انقضای اکانت است که اگر برای آن، تاریخ تعیین شود، اکانت مورد نظر انقضا خواهد شد و دیگر کار نخواهد کرد که به صورت پیش‌فرض بر روی Never قرار گرفته است، گزینه‌ی سوّم نیز برای این است که زمانی که با کاربر مورد نظر وارد نرم‌افزار می‌شوید، اگر این گزینه بر روی Yes قرار داشته باشد، کاربر هیچ وقت نیاز ندارد که دوباره رمز عبور را در زمان بیکاری سیستم وارد کند که انتخاب خوبی نخواهد بود و باید بر روی No قرار داشته باشد.

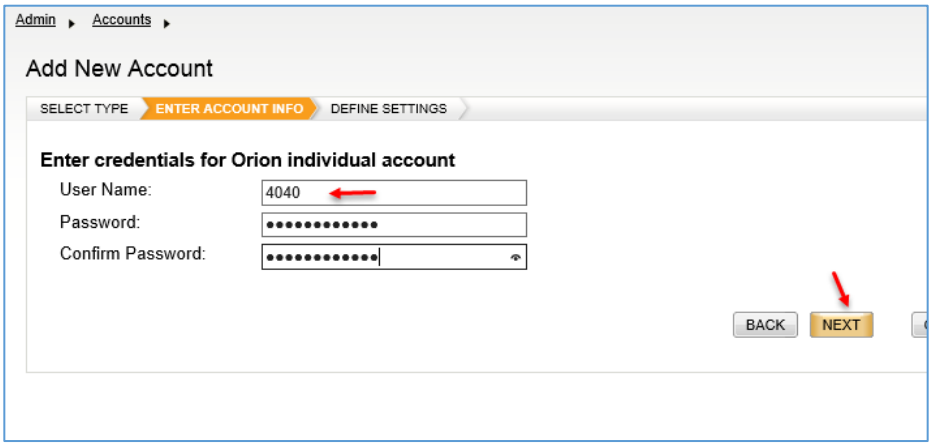
در قسمت شماره‌ی چهار نیز با انتخاب Yes، دسترسی کامل مدیریّتی به کاربر Admin داده خواهد شد، گزینه‌های زیاد دیگری نیز وجود دارد که در صورت نیاز آنها را بررسی خواهیم کرد.



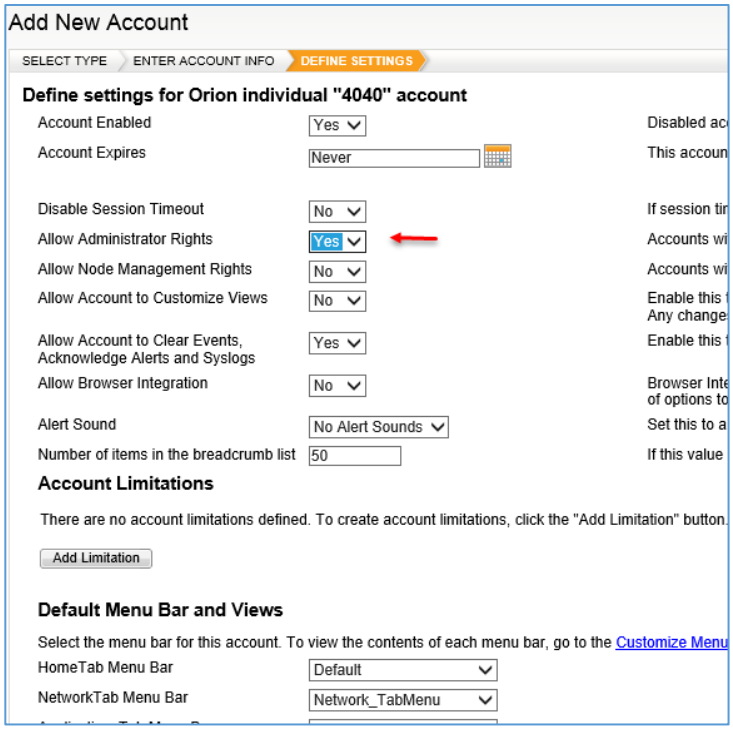
برای اینکه اکانت تعریف کنید باید بر روی Add New Account کلیک کنید



در این قسمت، گزینه‌های مختلفی وجود دارد که اگر گزینه‌ی Orion را انتخاب کنید، یک اکانت از نوع SQL به صورت محلّی در نرم‌افزار ایجاد می‌شود، گزینه‌های دوّم و سوّم برای ایجاد کاربر و گروه از طریق سرویس Active Directory است که در این قسمت باید گزینه‌ی اوّل را انتخاب و بر روی Next کلیک کنید.



در این صفحه باید نام کاربری و رمز عبور کاربر مورد نظر را وارد و بر روی Next کلیک کنید تا کاربر مورد نظر ایجاد شود.

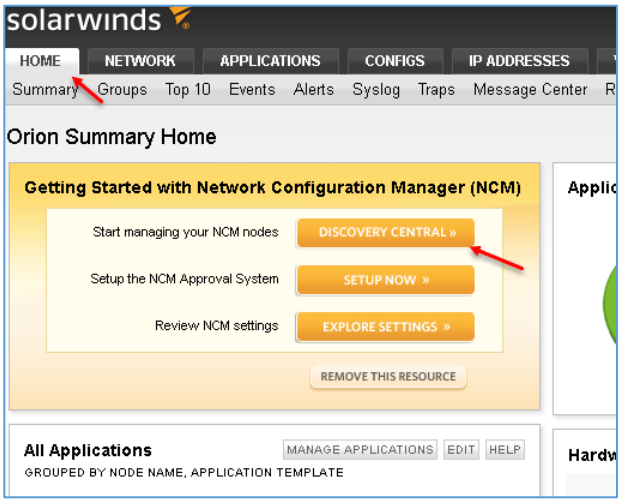


در این صفحه که در قسمت‌های قبلی آن را بررسی کردیم، می‌توانید تنظیماتی را برای کاربر اعمال کنید، مثلاً می‌توانید به مانند شکل روبرو کاربر مورد نظر را در گروه Administrator قرار دهید تا دسترسی کامل به نرم‌افزار داشته باشد.

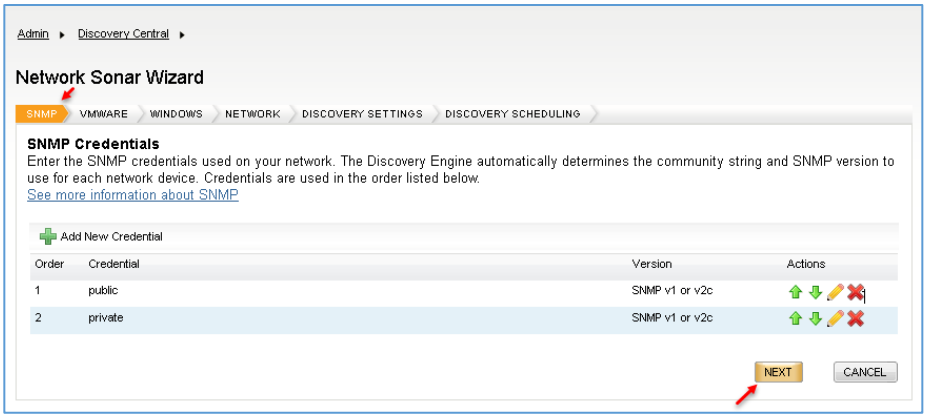
بعد از انجام تنظیمات بر روی OK کلیک کنید.

بعد از اینکه توانستید کاربر مورد نظر خود را ایجاد کنید و تنظیمات خود را بر روی آن اعمال کنید باید کار اصلی خود را در نرم‌افزار آغاز کنید.

فعّال‌سازی Discovery در نرم‌افزار Solar:



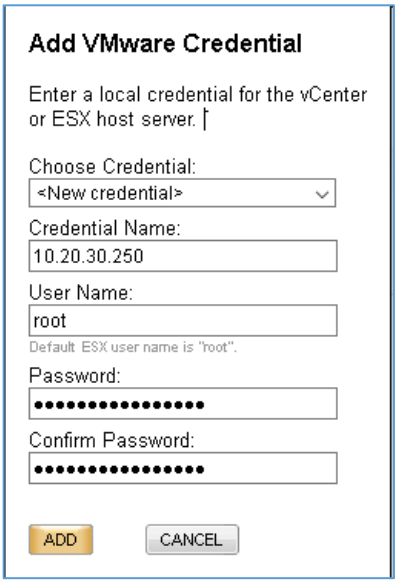
برای اینکه نرم‌افزار مانیتورینگ را بر روی شبکه فعّال کنید تا بتواند بر روی تمام دستگاه‌های شبکه نظارت داشته باشد باید به مانند شکل وارد صفحه‌ی اوّل نرم‌افزار شوید و بر روی Discovery Centeral کلیک کنید.

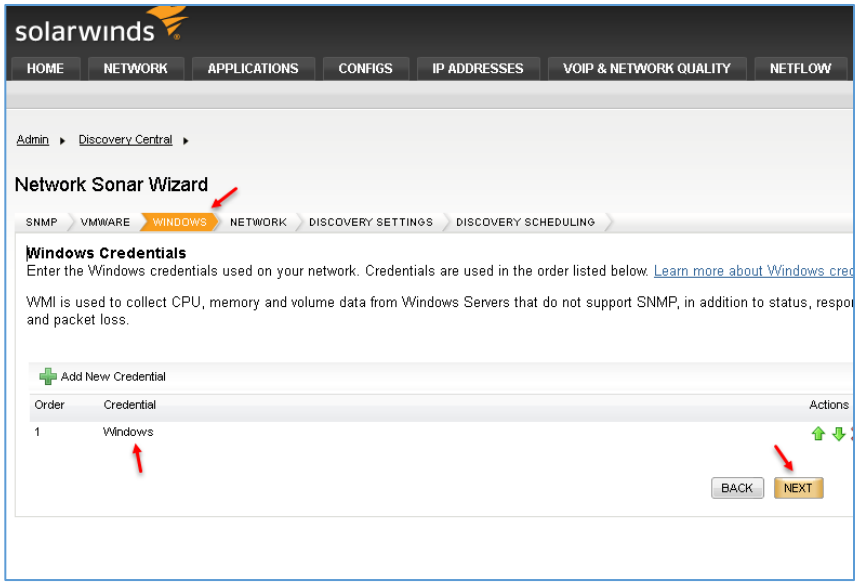


در این صفحه، گزینه‌های مختلفی وجود دارد که در تب اوّل، گزینه‌ی SNMP را مشاهده می‌کنید که به طور پیش‌فرض، دو گزینه‌ی Public و Private وارد شده است، اگر شما در شبکه‌ی خود دستگاهی یا نرم‌افزاری دارید که سرویس SNMP آنها فعّال باشد به صورت پیش‌فرض، دو نام کاربری Public و Private تعریف شده است تا به صورت اتوماتیک به آنها متّصل شود، اگر چنانچه نام کاربری خاصّی تعریف کردید باید بر روی Add New Credentials کلیک کنید و نام کاربری و رمز عبور مورد نظر خود را وارد کنید، بر روی Next کلیک کنید.

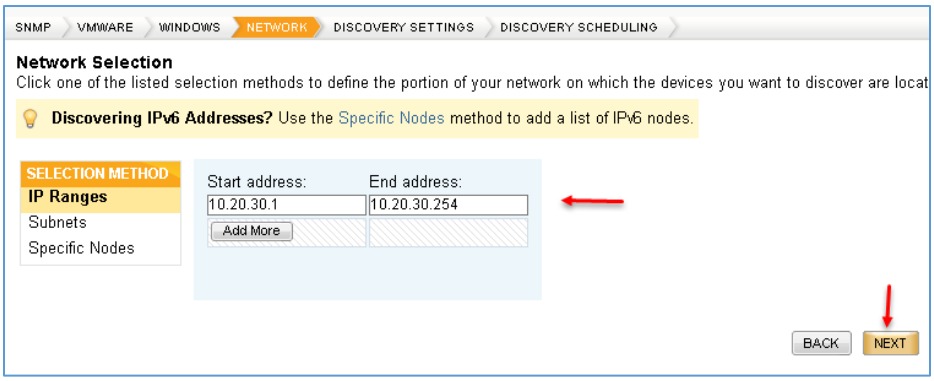


اگر در تب VMWARE از نرم-افزارهای این شرکت در شبکه‌ی خود استفاده می کنید، مانند ESXI یا VCenter باید نام کاربری را به همراه آدرس سرور وارد کنید، زمانی که شما اطّلاعات را وارد می‌کنید، خود نرم‌افزار Solar به صورت اتوماتیک به سرور متّصل خواهد شد و اطّلاعات آن را برای شما مانیتور خواهد کرد، مثلاً در شکل روبرو باید در قسمت Cerdential Name، نام سرور مورد نظر را وارد و بعد، نام کاربری و رمز عبوری را که به سرور مورد نظر متّصل می‌شود را وارد کنید، شما باید همه‌ی رمزهای سرورها را وارد کنید تا مشکلی در ارتباط ایجاد نشود.



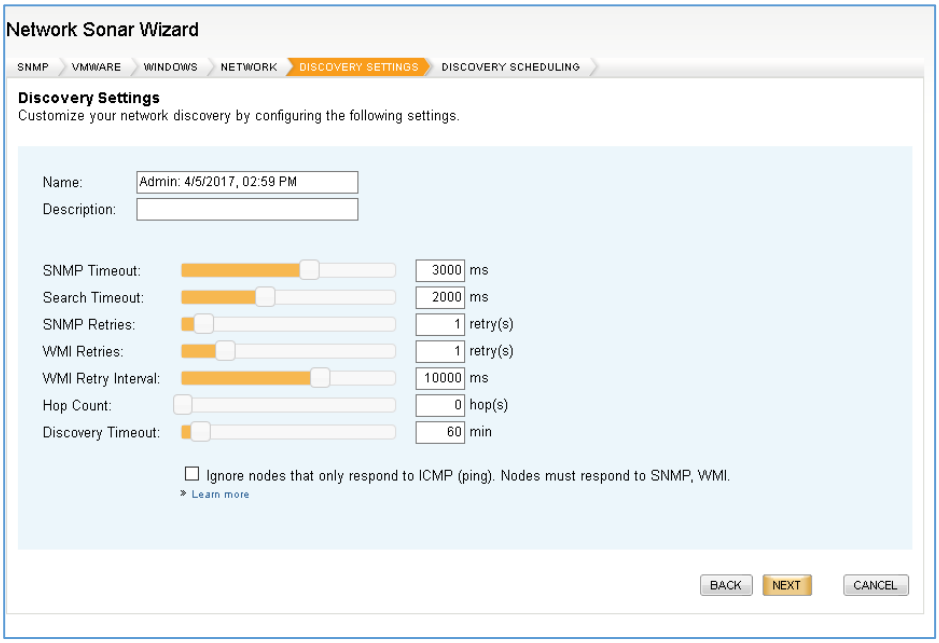


در تب Windows باید بر روی Add New Credential کلیک کنید و نام کاربری‌ای که به کلّ شبکه‌ی شما دسترسی دارد را وارد و بر روی Next کلیک کنید.



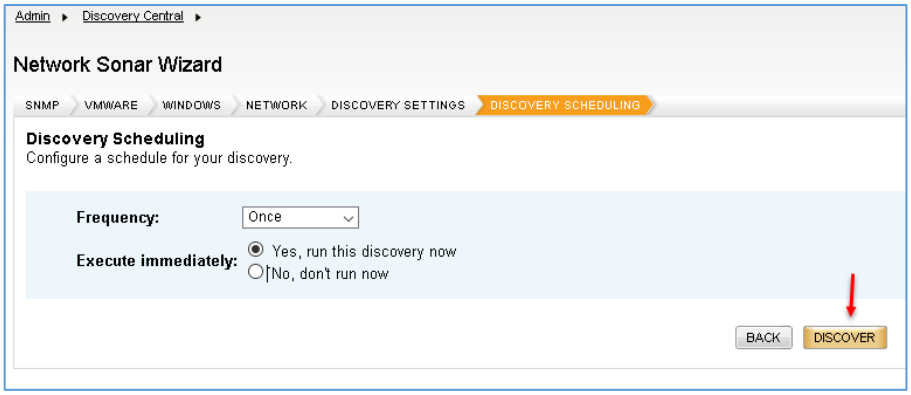
در قسمت Network باید آدرس شبکه‌ی خود را وارد کنید، مثلاً در شکل روبرو رنج آدرس شبکه‌ی مورد نظر وارد شده است.

بر روی Next کلیک کنید.

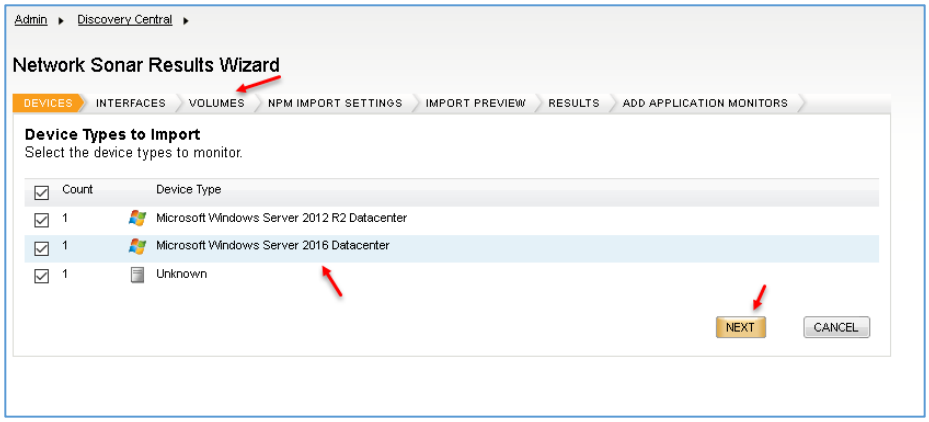


در این صفحه می‌توانید زمان وقفه-ی هر سرویس را برای ارتباط با دستگاه‌ها وارد کنید.

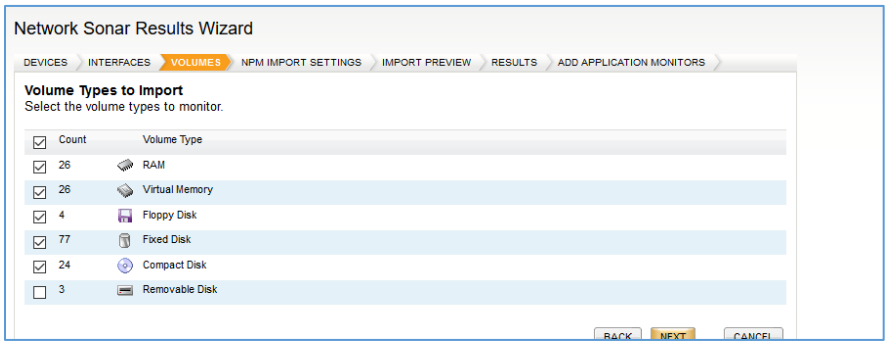
بر روی Next کلیک کنید.



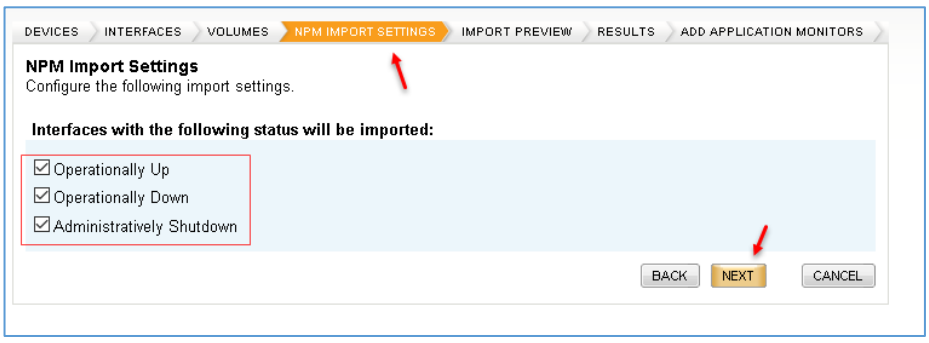
در این قسمت می‌توانید زمان شروع به Discovery را مشخّص کنید که به صورت پیش‌فرض بر روی Once قرار دارد که بعد از کلیک بر روی Discover، نرم‌افزار شروع به کار می‌کند و کلّ شبکه را بررسی خواهد کرد.



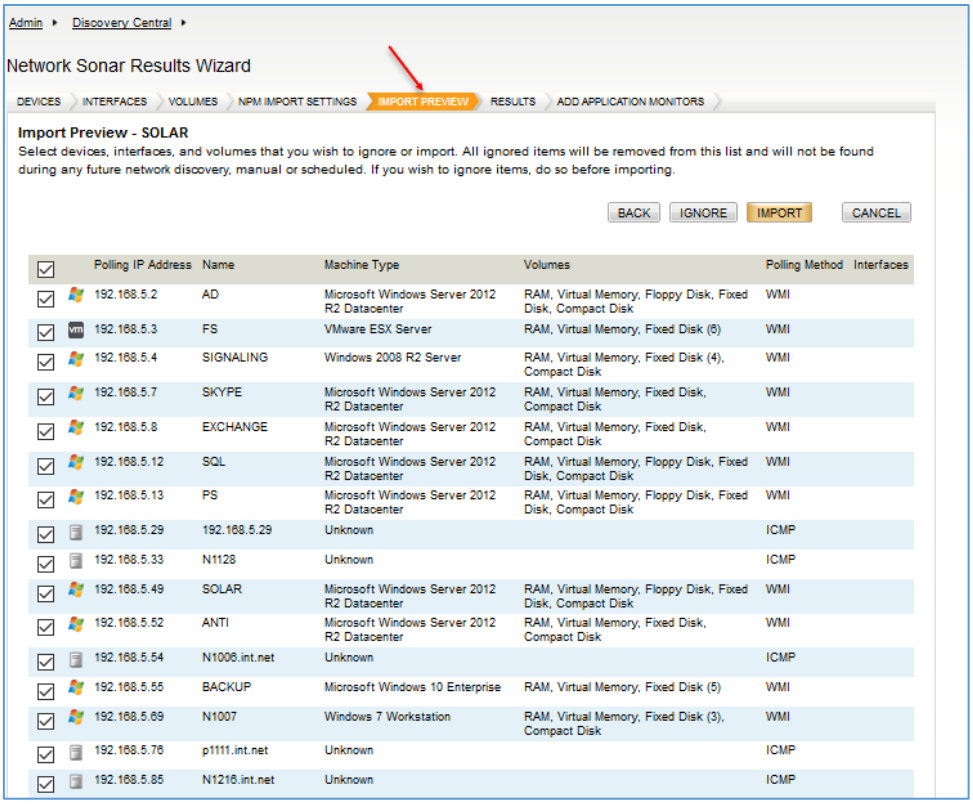
بعد از اینکه عملیّات Discovery انجام شد، لیستی از سرورها و کلاینت‌ها برای شما به نمایش گذاشته می‌شود که اگر می‌خواهید اطّلاعات آنها بررسی و مانیتور شود، می‌توانید تیک آنها را انتخاب کنید و یا اینکه تیک آنها را بردارید تا بررسی نشود، بر روی Next کلیک کنید.



در قسمت Volumes می‌توانید نوع اطّلاعاتی که باید بررسی شود را انتخاب و بر روی Next کلیک کنید.

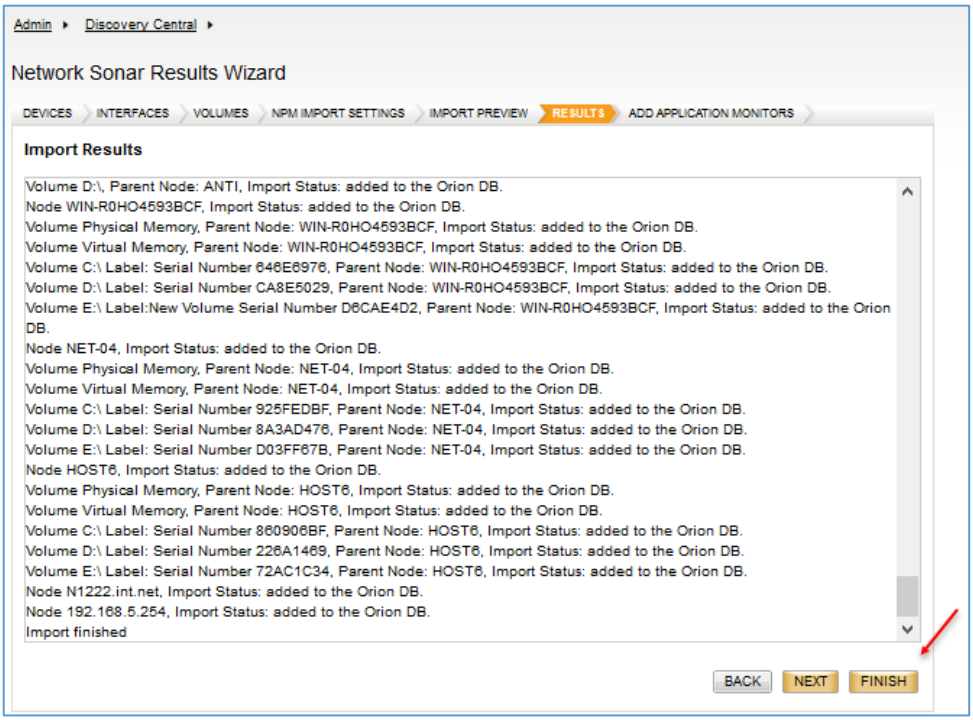


در این قسمت می‌توانید مشخّص کنید که تنها سیستم‌هایی که آنلاین، خاموش و یا در شبکه قرار دارند، به نرم‌افزار اضافه شوند.



در تب Import Preview می‌توانید تمام کلاینت‌ها و دستگاه‌هایی که توسّط نرم‌افزار در شبکه شناسایی شده است را مشاهده کنید، هر یک از آنهایی که نیاز دارید را می‌توانید انتخاب کنید و یا تیک آنها را بردارید.

بر روی Import کلیک کنید.

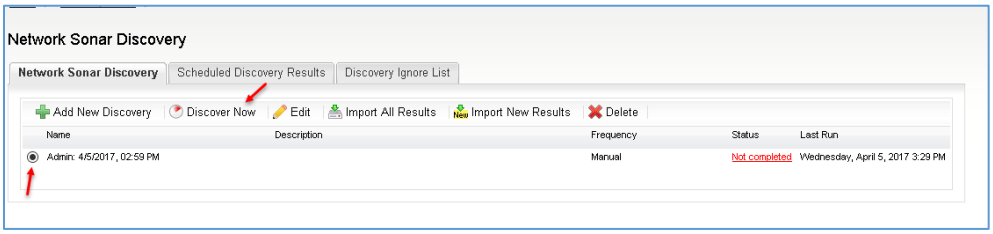


در این قسمت، کلاینت‌ها و سرورهایی که انتخاب کردید، Volume های آنها به لیست اضافه شده است، بر روی Finish کلیک کنید تا کار به اتمام برسد.



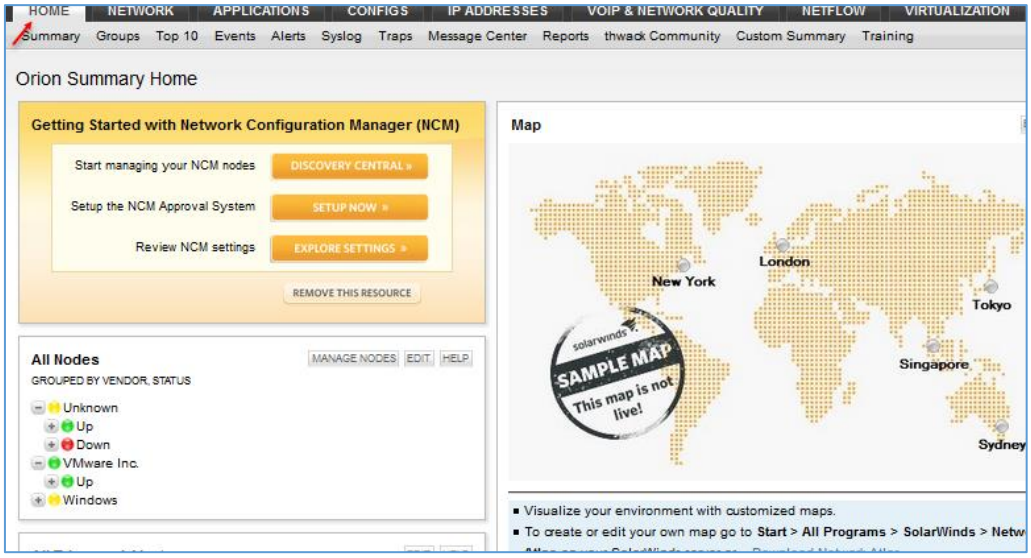
بعد از اینکه عملیّات نهایی انجام شد، صفحه‌ای به مانند شکل روبرو ظاهر می‌شود که اطّلاعات کلّی را نشان می‌دهد، مثلاً در شکل روبرو برای مانیتورینگ، ۳ دستگاه به همراه ٦ اجزا شناسایی شده است.

اگر بخواهید بار دیگر، عملیّات discovery را انجام دهید باید به مانند شکل روبرو بر روی Discovery My Networks کلیک کنید.

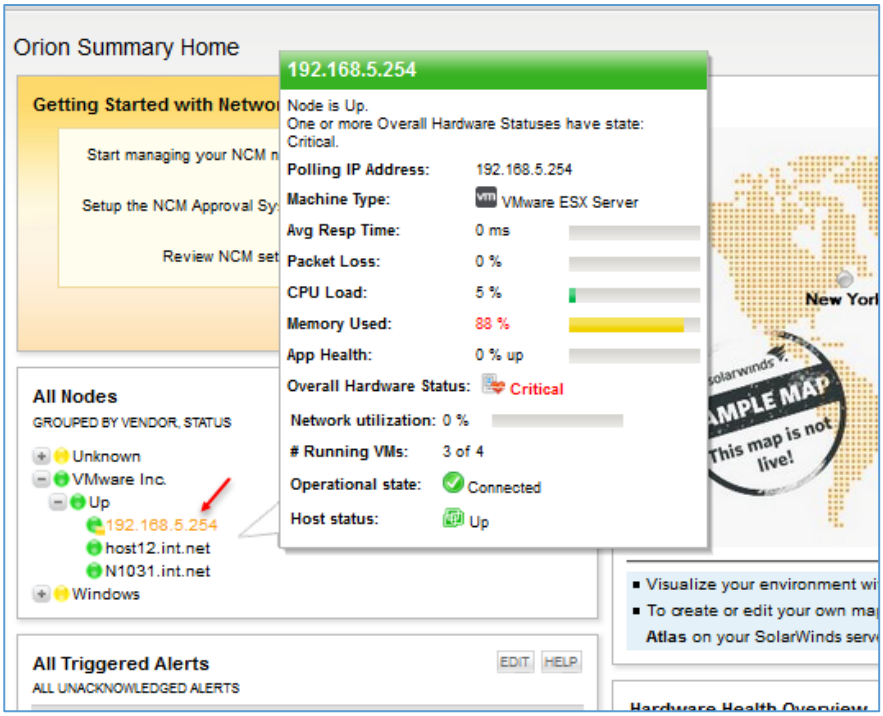


در این قسمت، شما نام Discovery خود را که از قبل ایجاد کردید را مشاهده می‌کنید، برای اینکه دوباره عملیّات discovery را انجام دهید باید در این شکل، گزینه‌ی Admin را انتخاب و بر روی Discover Now کلیک کنید تا بار دیگر، عملیّات انجام شود.

سعی کنید، زمانی عملیّات discovery را انجام دهید که بار کاری شبکه پایین باشد، مثلاً آخر وقت اداری یا در هنگام شب انجام دهید.

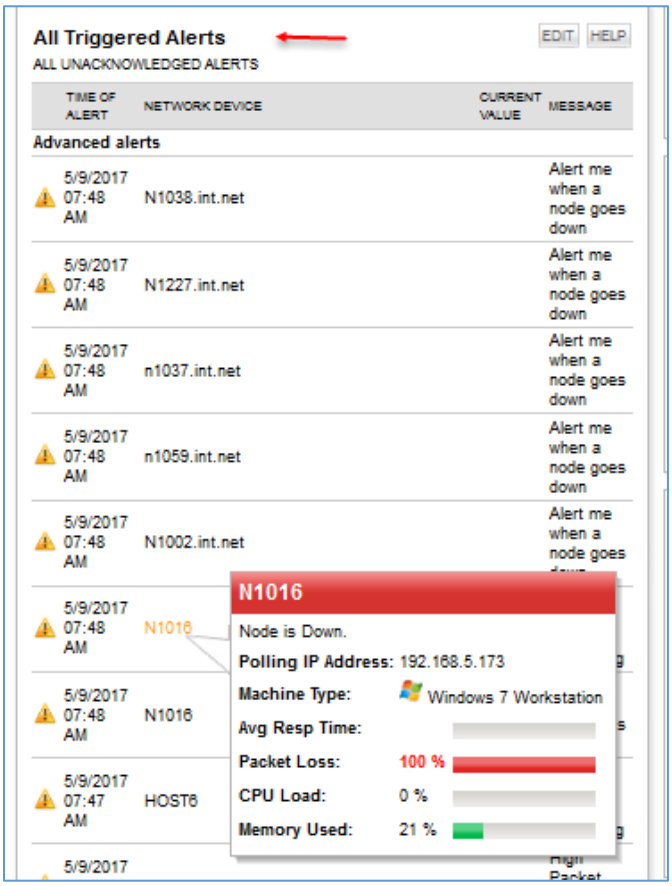


در تب Home، یک‌سری اطّلاعات کلّی از شبکه شما قرار دارد، مثلاً در قسمت All Nodes، تمام کلاینت‌ها و سرورها به ترتیب با عنوان‌های مختلف نمایش داده شده که حتّی وضعیّت آنها نیز مشخّص شده است.

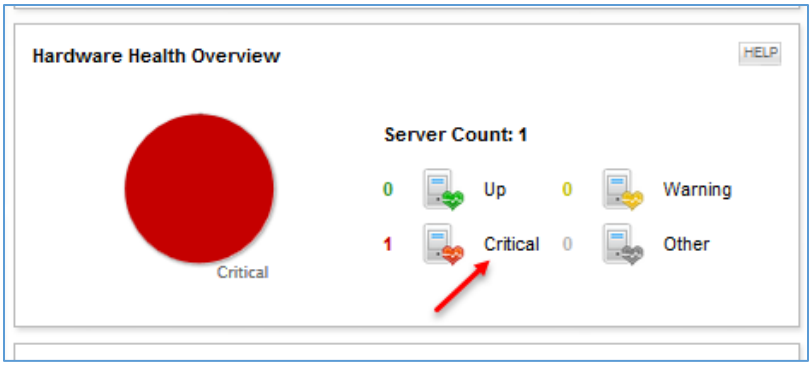


اگر بخواهید وضعیّت یک سرور یا سیستم را از نظر مقدار مصرف رم، CPU و... بررسی کنید، می‌توانید به مانند شکل روبرو نشانگر ماوس را بر روی سرور نگه دارید تا پنجره‌ای باز شود که در آن توضیحات و اطّلاعات لازم به نمایش گذاشته می‌شود.

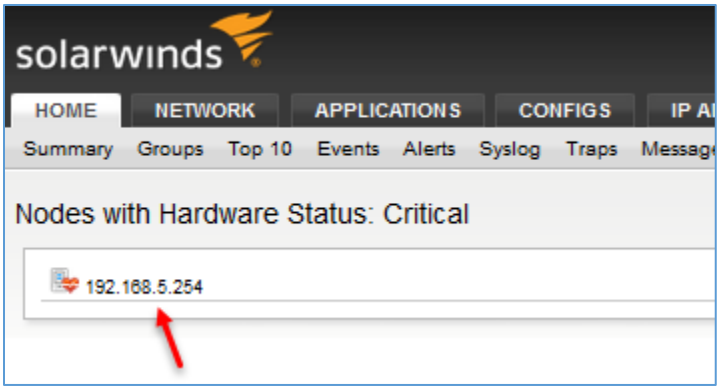
اگر در شکل روبرو توجّه کنید، سیستم-ها را برای شما دسته‌بندی کرده است، مثلاً سیستم عامل ویندوز را در یک قسمت و VMware را در قسمت دیگر قرار داده است تا کار با آنها آسان‌تر باشد.



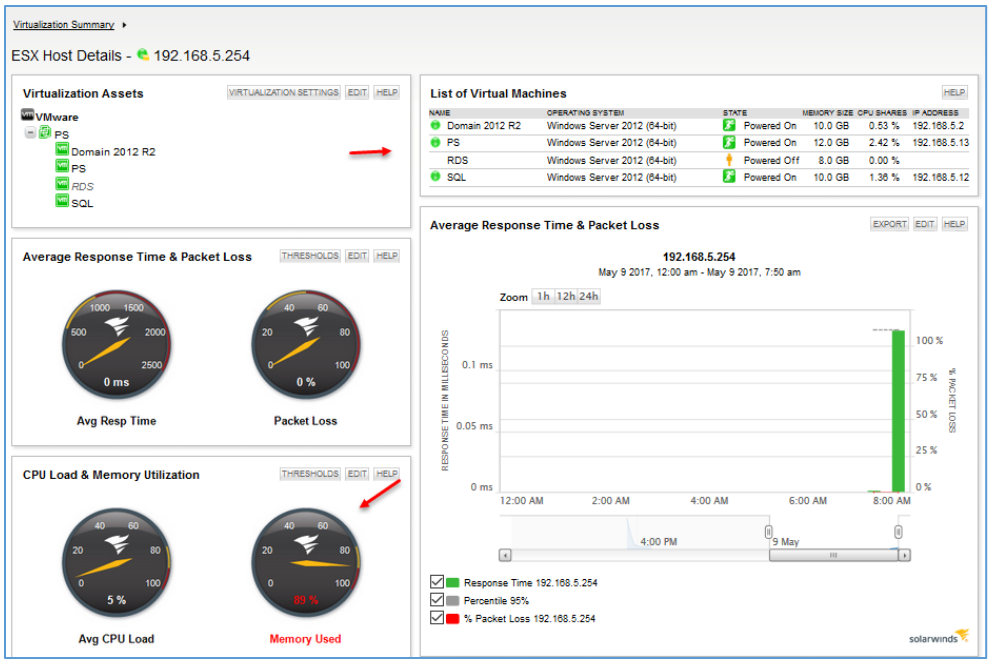
در قسمت پایین‌تر صفحه، قسمت All Triggered Alerts وجود دارد که مربوط به تمام هشدارهای سیستم‌های موجود در شبکه است که به شما برای مدیریّت هر چه بهتر کمک می‌کند.



در قسمت دیگر، Hardware Health Overview یا همان، سلامتی سخت‌افزار وجود دارد که به شما نشان می‌دهد، چه سخت‌افزاری در معرض خطر است، در شکل روبرو یک سیستم پیدا شده است که اگر بر روی آن کلیک کنید، شکل بعد ظاهر می‌شود.

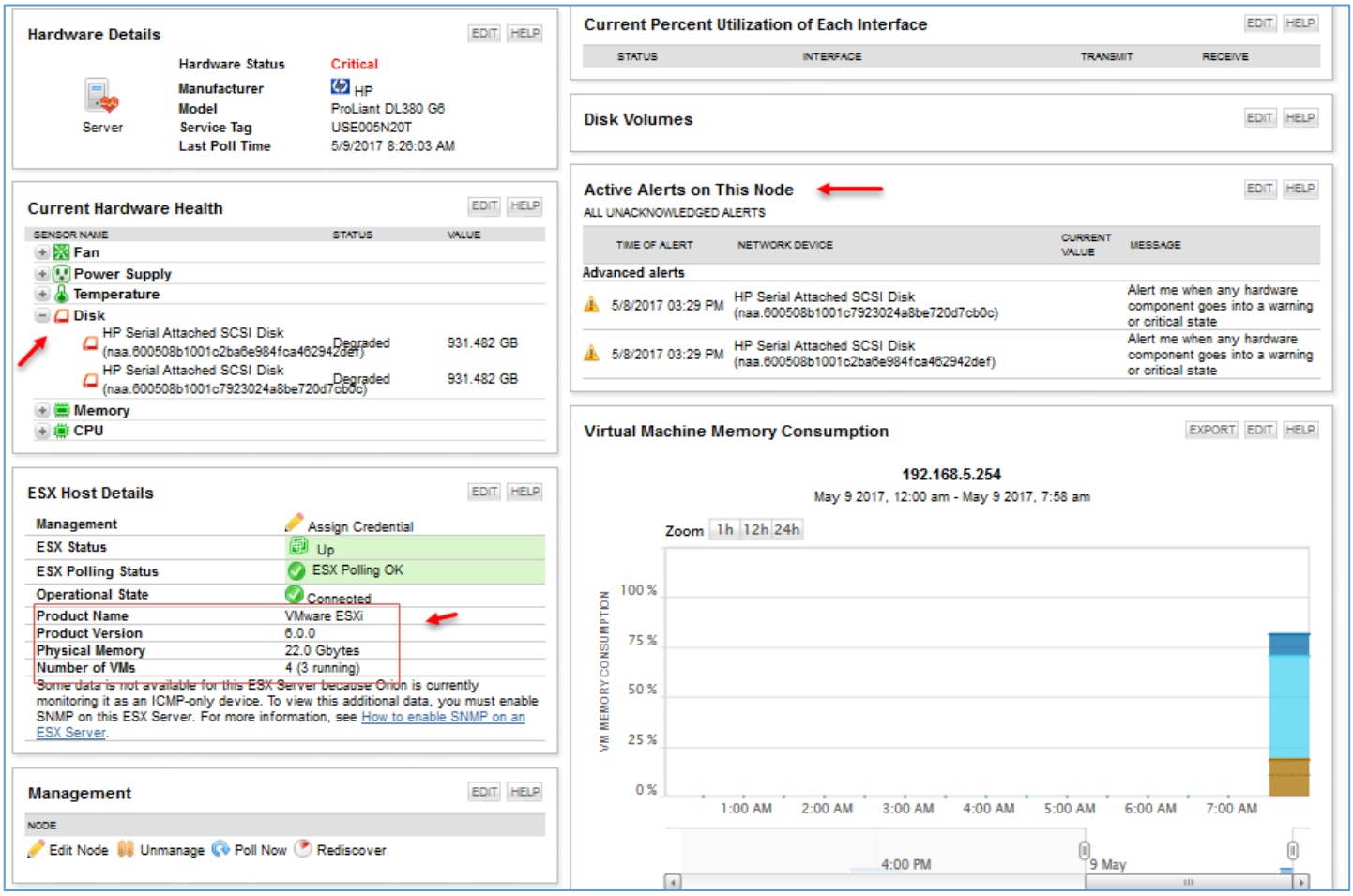


در شکل روبرو یک آدرس سیستم برای شما مشخّص شده است که برای اطّلاع از وضعیّت خرابی یا هشدار آن باید بر روی آدرس کلیک کنید.

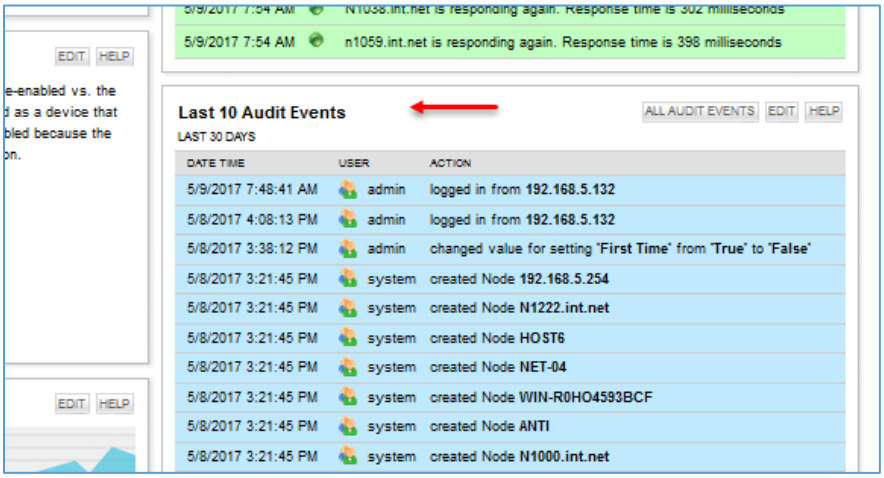


در شکل روبرو یک سرور HP مشخّص شده است که بر روی آن، سیستم عامل ESXI نصب شده است که دارای چهار ماشین مجازی است که نام آنها نیز مشخّص شده است.

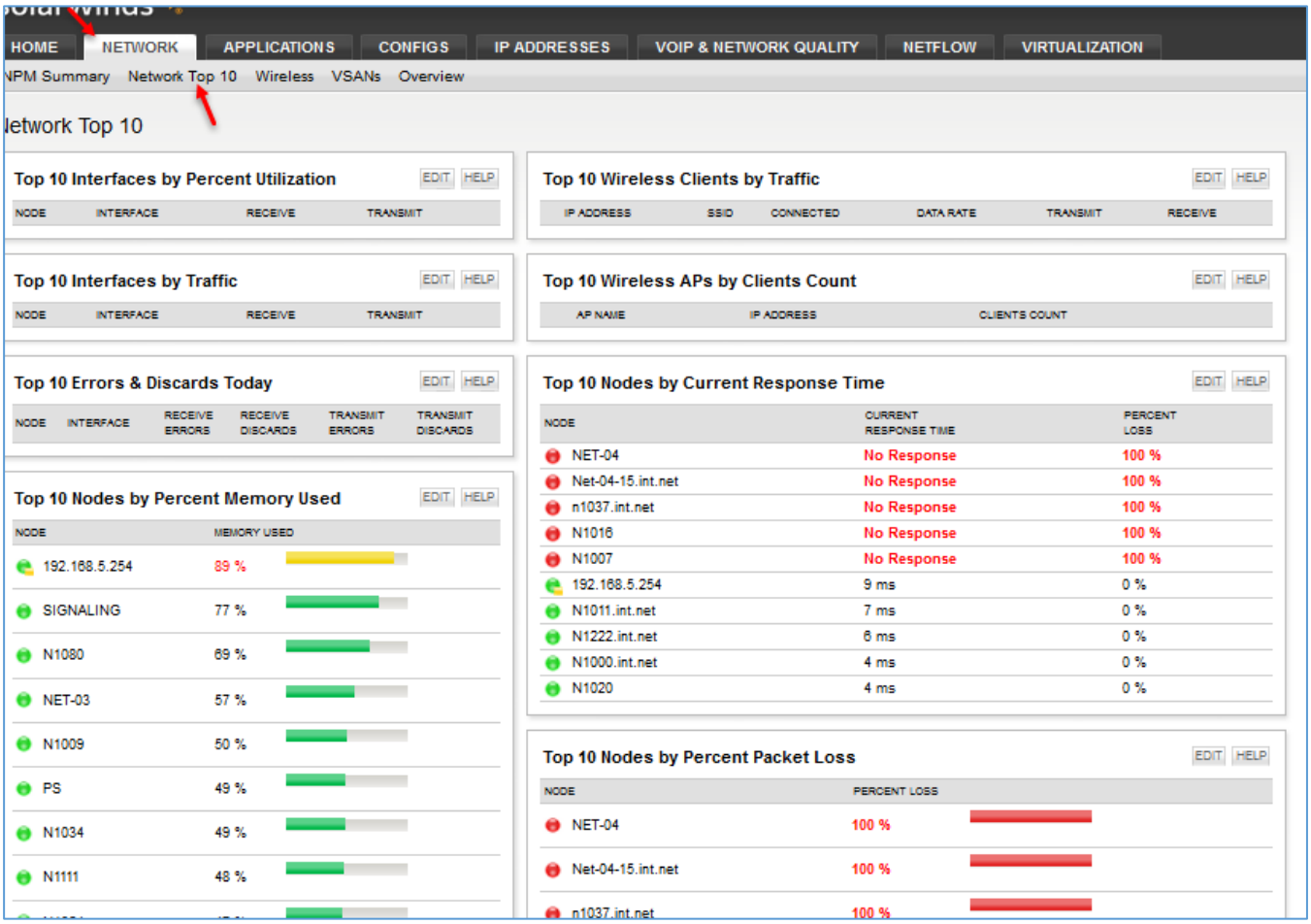
در سمت چپ صفحه، چند کنترلر وجود دارد که مشخّص-کننده‌ی مصرف CPU، RAM و... است که اگر خوب به شکل توجّه کنید، مقدار رم در حدّ نرمال نیست که باید رم سرور را برای عملکرد بهتر سخت‌افزار بهبود ببخشید.



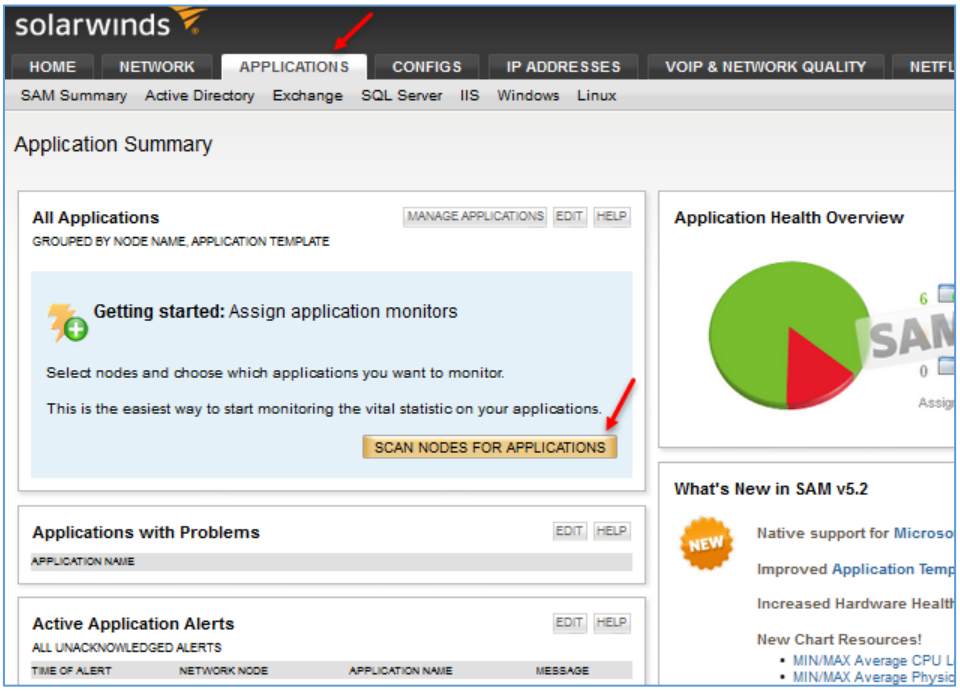
در شکل بالا و در قسمت Current Hardware Health، عملکرد سخت‌افزار کلّ سرور مشخّص شده است که آنهایی که در وضعیّت نرمال قرار دارند با رنگ سبز و آنهایی که دارای مشکل هستند با رنگ قرمز مشخّص شده است، مثلاً در شکل بالا، هارد دیسک‌های این سرور در حال پر شدن است که باید چاره‌ای برای آن اندیشید، در قسمت ESX Host Details نیز مشخّصات سیستم عامل ESXI نوشته شده است که ورژن ٦ آن بر روی سرور نصب شده است (در کتاب مدیر شبکه‌ی یک، در مورد نرم‌افزارهای شرکت VMware توضیح کامل دادیم)، در قسمت Virtual Machine Memory Consumption، هر ماشین مجازی به یک رنگ مشخّص شده است که اگر ماوس را بر روی رنگ مورد نظر نگه دارید، مشخّص می‌شود که مربوط به کدام ماشین است و مقدار مصرف رم آن نیز مشخّص خواهد شد، در قسمت پایین صفحه نیز اطّلاعات دیگری از مقدار مصرف ماشین‌های مجازی از شبکه مشخّص شده است، دوباره به صفحه‌ی اوّل، یعنی Home باز گردید.



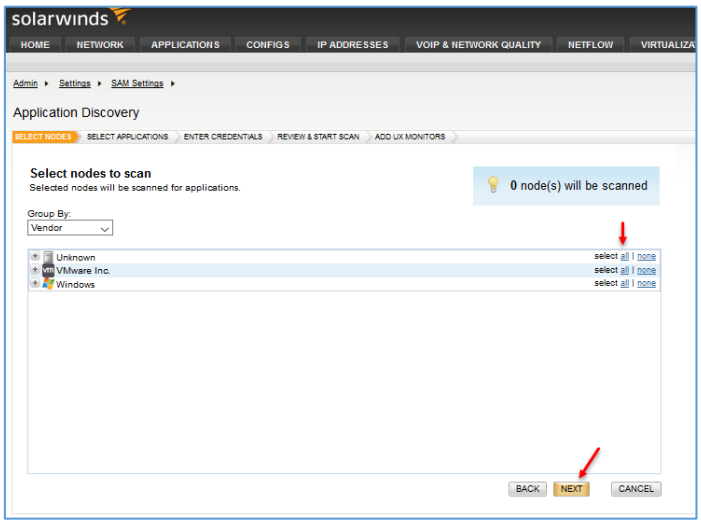
در تب Home و در قسمت آخر صفحه، قسمت Last 10 Audit Events وجود دارد که ۱۰ کار آخر، مانند ایجاد کاربر، ایجاد Node جدید، ورود کاربر از سیستم خاص به سرور Solar و... مشخّص شده است.



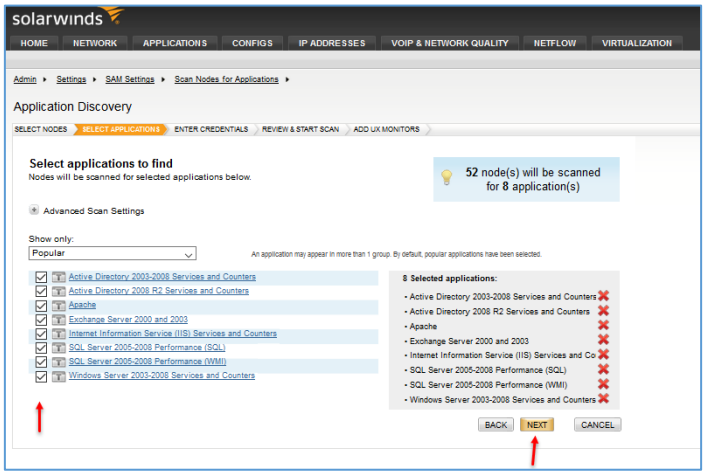
اگر در قسمت Networking بر روی Network Top 10 کلیک کنید، آمارهای مختلفی از وضعیّت کارایی سخت‌افزار شبکه‌ی مربوط به هر سیستم را مشاهده خواهید کرد.



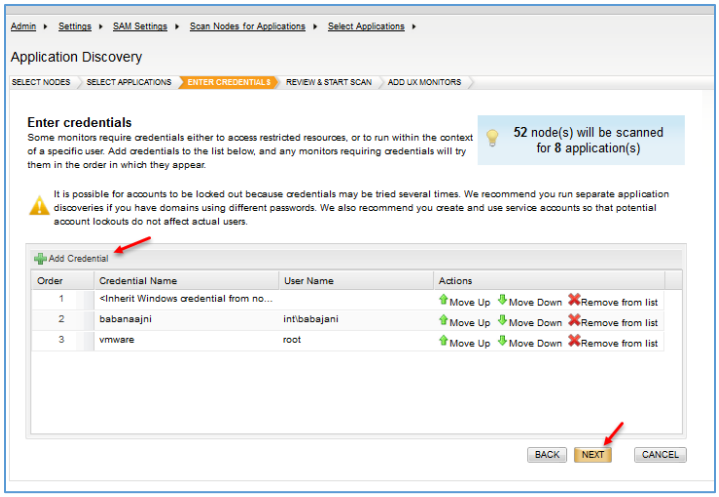
در قسمت APPLICATIONS می‌توانید همه‌ی نرم‌افزارها و سرویس‌های شبکه‌ی خود را جمع‌آوری کنید و کنترل کلّی بر روی آنها داشته باشید، برای شروع بر روی Scan Nodes For Applications کلیک کنید.



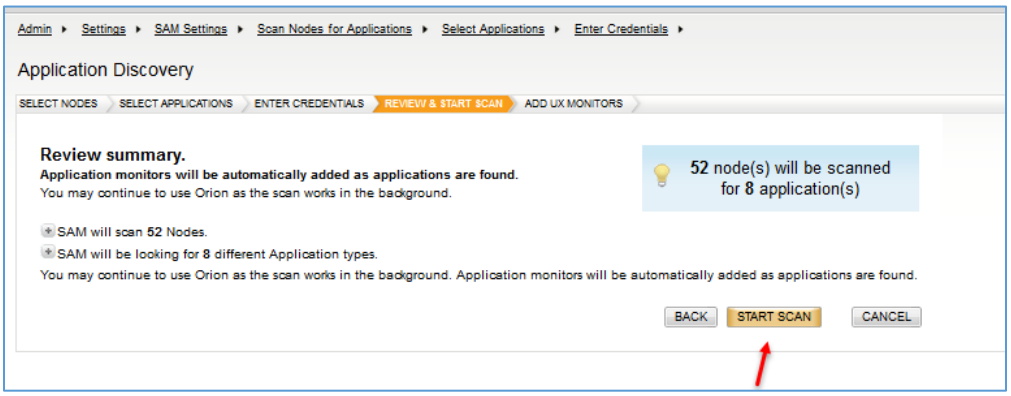
در این قسمت، شما می‌توانید کلاینت و سرورها را از نظر نرم‌افزاری و سرویس‌ها بررسی کنید، بعد از انتخاب بر روی Next کلیک کنید.



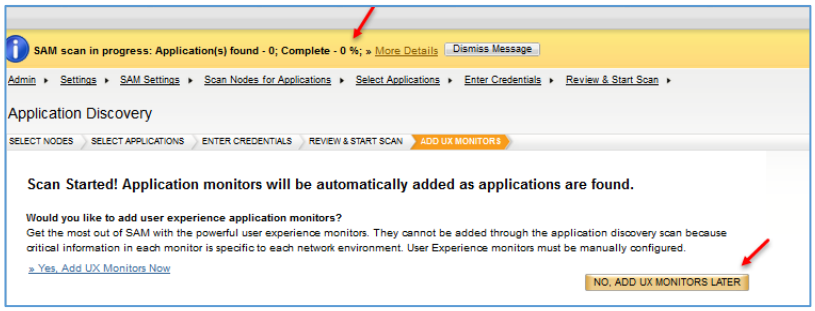
در این قسمت، یک‌سری گروه در قسمت Show only وجود دارد که به صورت پیش‌فرض، گزینه‌ی Popular یا برگزیده انتخاب شده است که لیست آن را مشاهده می‌کنید، بعد از انتخاب بر روی Next کلیک کنید.



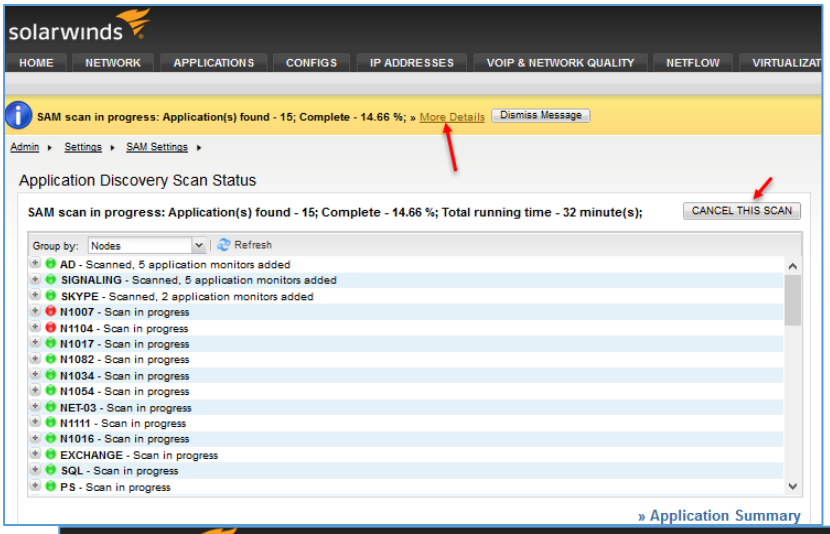
در این قسمت باید بر روی Add Cerdential کلیک کنید و یک یا چند نام کاربری را که دسترسی کامل به کلّ شبکه دارند را وارد کنید، اگر سرورهای مختلف با کاربران مختلف دارید باید همه‌ی آنها را وارد کنید.



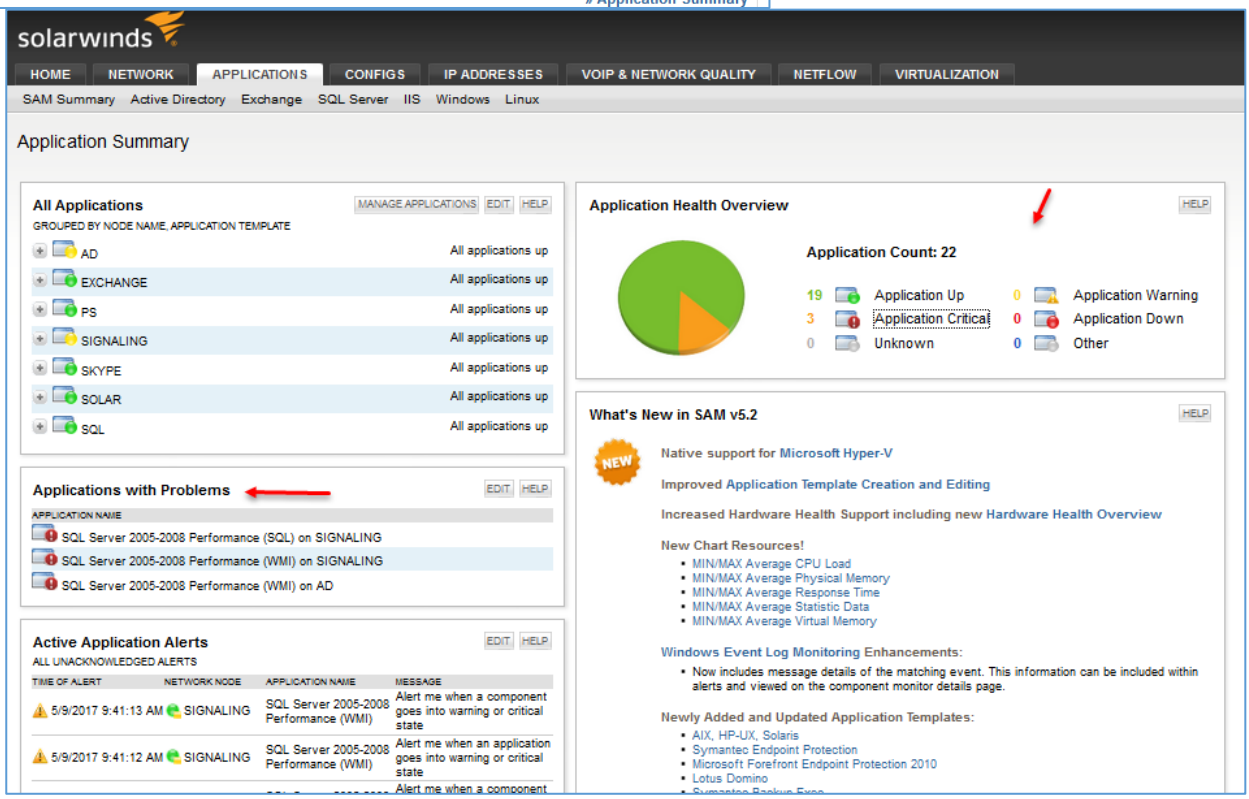
در این صفحه بر روی START SCAN کلیک کنید تا کار آغاز شود.



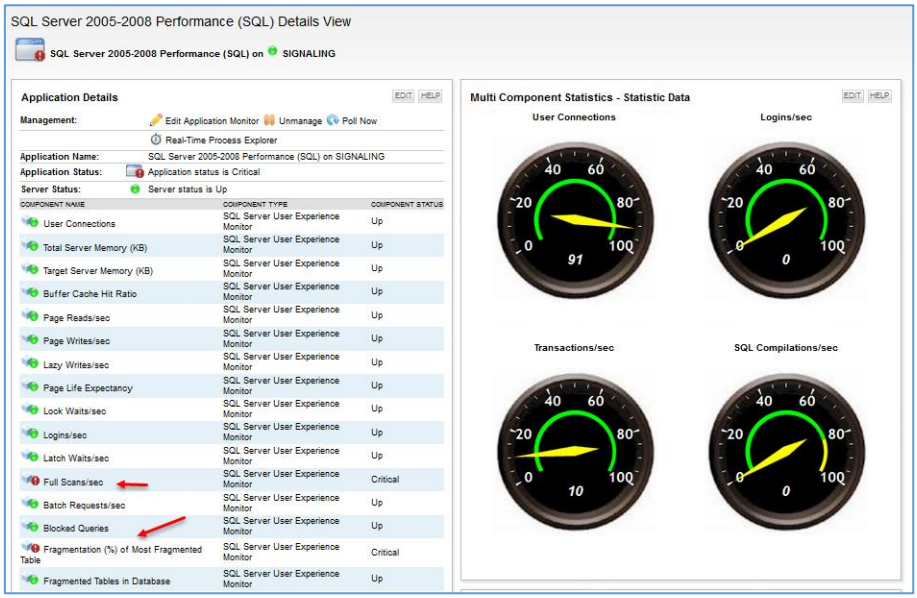
بعد از اجرا، یک نوار در قسمت بالای صفحه ظاهر می‌شود که درصد آن نیز برای شما مشخّص شده است که زمان اجرای این کار طولانی است.



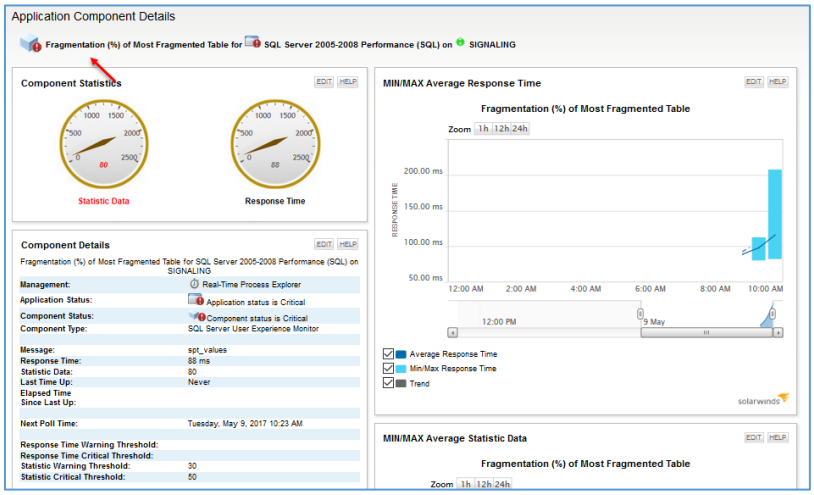
در این صفحه برای نمایش اطّلاعات نرم-افزارها و سرویس‌ها باید بر روی More Details کلیک کنید تا مانند شکل روبرو تمام آنها را مشاهده کنید، اگر بخواهید این عملیّات جستجو را Cancel کنید، بر روی CANCEL THIS SCAN کلیک کنید.



در صفحه‌ی اوّل Applications، اطّلاعات کلّی در قسمت‌های مختلف به شما نمایش داده می‌شود، مثلاً در قسمت Applications with Problems، مشکلات نرم‌افزار SQL نمایش داده شده است، بر روی آن کلیک کنید تا مشکل آن را دریابید.



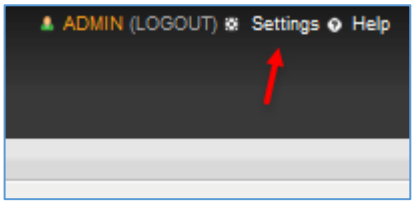
در این صفحه که مربوط به نرم-افزار SQL سرور Signaling است، دو مشکل پیدا شده که در شکل مشخّص شده است، اگر بر روی هر مشکل کلیک کنید، توضیحاتی برای آن به نمایش گذاشته خواهد شد.



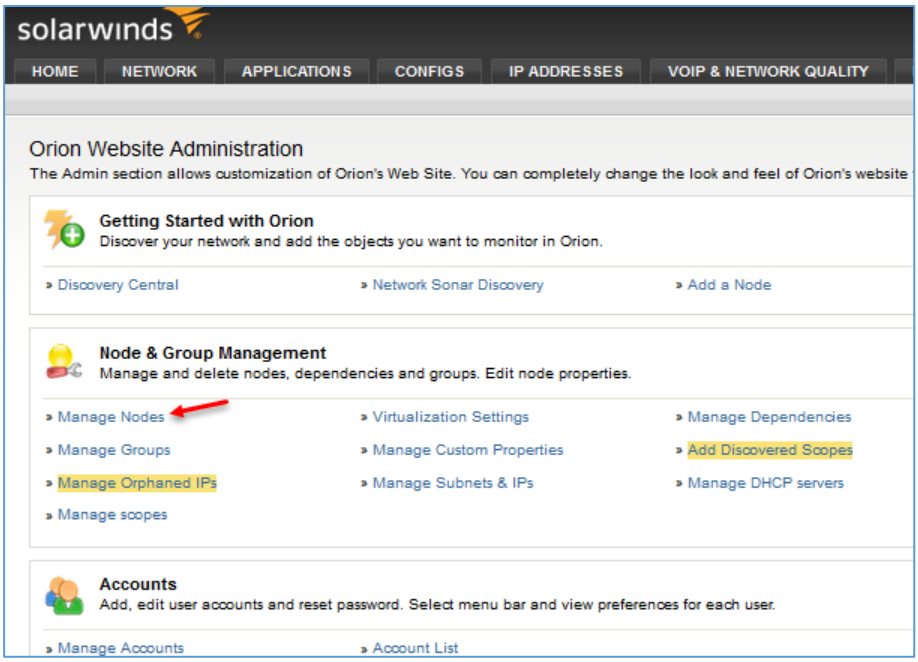
در شکل روبرو مشکل Fragment شدن SQL نمایش داده شده است که همان، تیکه تیکه شدن اطّلاعات است که این موضوع به خاطر ورود و خروج زیاد اطّلاعات در جداول است که با دستوری می‌توانید این موضوع را در SQL اصلاح کنید.

اگر چنانچه در مورد عناوینی که در گزارش‌ها اعلام می‌شود، اطّلاعاتی می‌خواهید، می توانید به آدرس زیر مراجعه کنید:

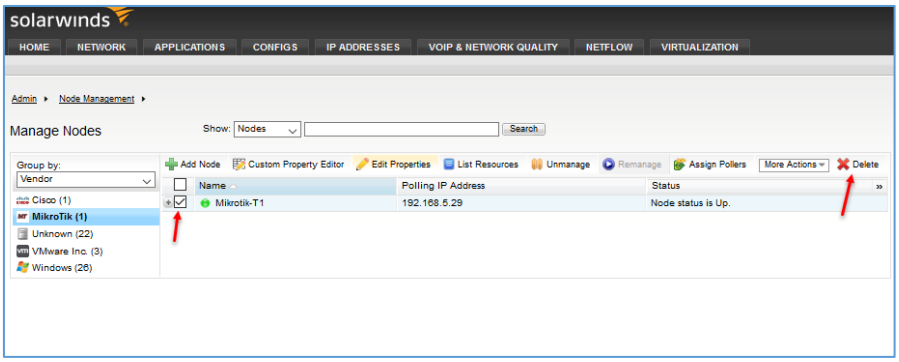
https://thwack.solarwinds.com/docs/DOC-170641



اگر بخواهید سیستم‌هایی که به لیست اضافه شده است را ویرایش کنید، بهتر است به صورت روبرو وارد قسمت Settings شوید.



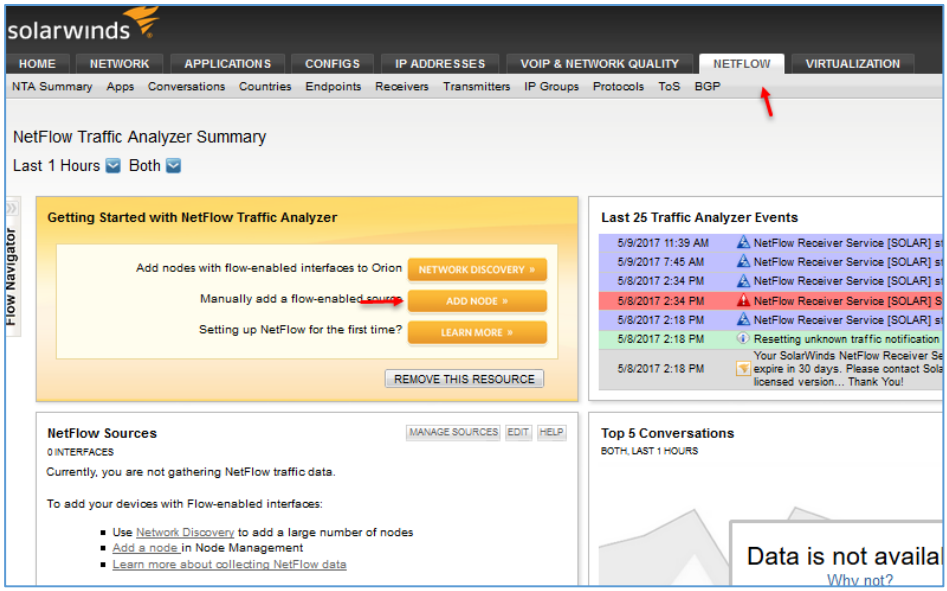
همانطور که مشاهده می‌کنید در قسمت Settings، گزینه‌های زیادی وجود دارد، برای مدیریّت سیستم‌ها باید بر روی Manage Nodes در قسمت Node & Group Management کلیک کنید.



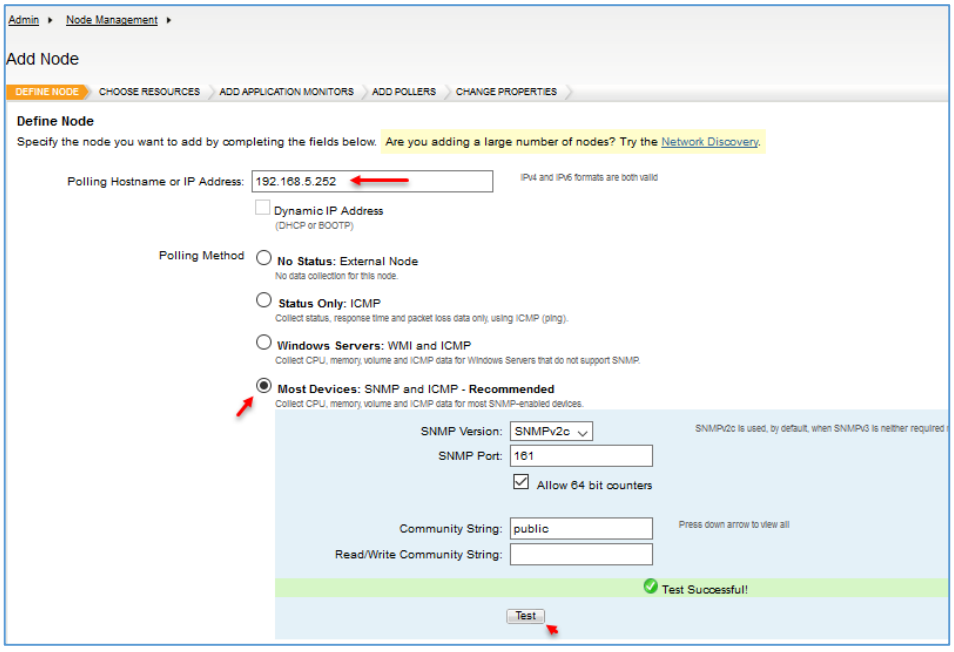
در این صفحه، لیست کلاینت‌ها و سرورها را در سمت چپ مشاهده می‌کنید که با انتخاب هر یک از آنها می‌توانید تغییراتی را بر روی آنها ایجاد کنید، مثلاً برای Delete کردن کلاینت یا سرور مورد نظر باید به مانند شکل، انتخاب و بر روی Delete کلیک کنید.

بررسی کامل سرویس NetFlow:

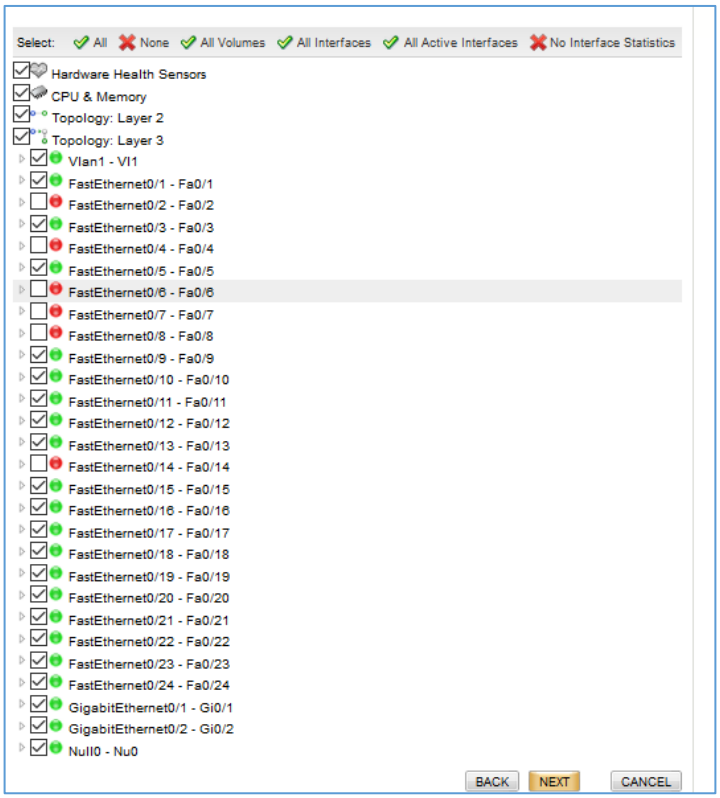
یکی از مهمترین ویژگی‌های یک نرم‌افزار مانیتور خوب، سرویس NetFlow آن است، شما به عنوان مدیر شبکه باید بدانید چه اطّلاعاتی در شبکه‌ی شما در حال ردّ و بدل است که برای این کار باید از این سرویس استفاده کنید، این سرویس، این امکان را به شما می‌دهد که کارت شبکه‌های روی سیستم را مشخّص و اطّلاعات ارسالی و دریافتی بر روی هر کارت شبکه را مانیتور کنید، تنها به این نکته توجّه کنید که سخت‌افزار شما باید این سرویس را پشتیبانی کند.



برای فعّال‌سازی NetFlow در نرم‌افزار Solarwins باید به مانند شکل روبرو وارد تب NetFlow شوید و برای اضافه کردن سیستم به این قسمت باید بر روی Add Node کلیک کنید، توجّه داشته باشید در این قسمت می‌خواهیم یک سوئیچ سیسکو را به نرم‌افزار اضافه کنیم، البتّه اگر بخواهیم کلّ شبکه بررسی شود باید گزینه‌ی Network discovery را انتخاب کنیم.

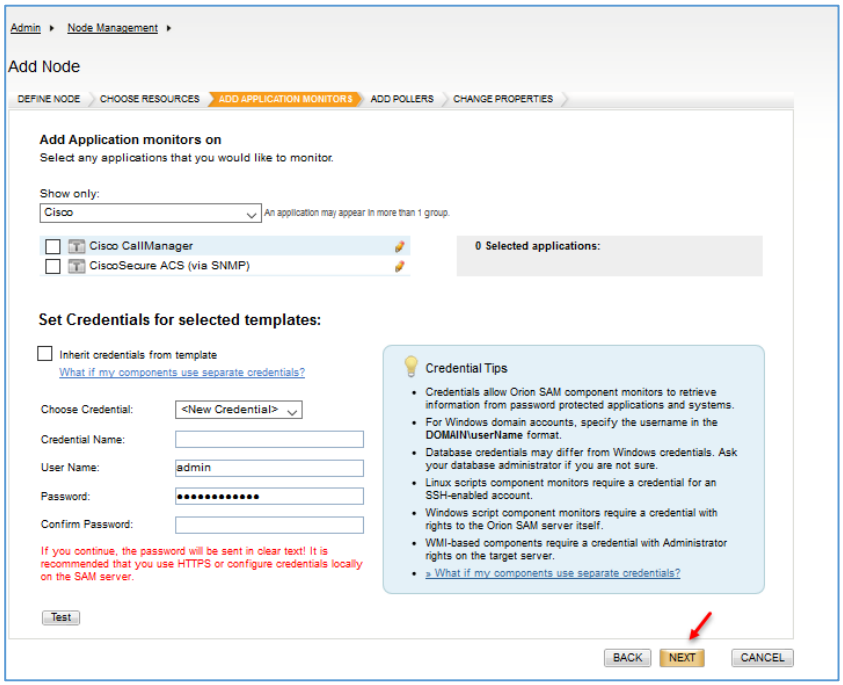


در این صفحه باید نام سرور خود را در قسمت Polling Hostname or IP Address وارد کنید و در قسمت Polling Method نیز باید نوع ارتباط را مشخّص کنید، برای اینکه با دستگاه‌ها ارتباط داشته باشید، بهتر است پروتکل SNMP آنها را فعّال کنید که این کار را در سوئیچ سیسکو انجام دادیم که به صورت پیش‌فرض، SNMPv2 فعّال است و نام Community String به صورت پیش‌فرض Public است، اگر اطّلاعات را درست وارد کرده باشید با کلیک بر روی Test با پیغام Test Successful روبرو خواهید شد، بعد از انجام مراحل بالا بر روی Next کلیک کنید.



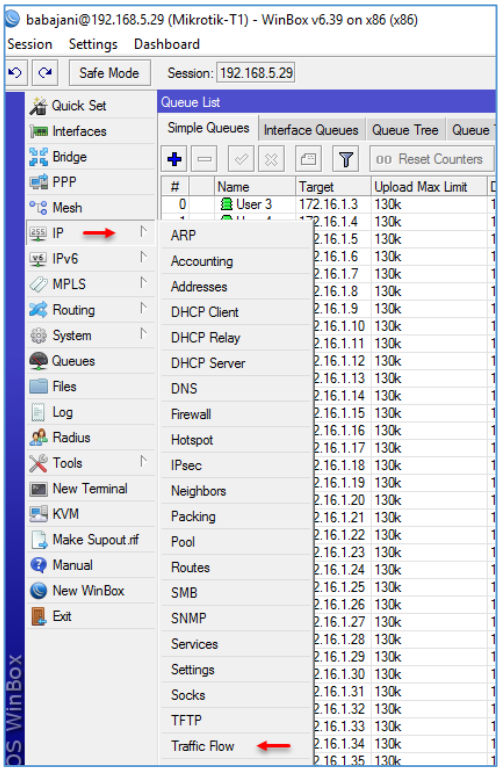
در این قسمت، کلّ ساختار دستگاه به نمایش گذاشته شده است که اگر می‌خواهید آنالیز بر روی همه‌ی آنها انجام شود باید همه‌ی گزینه‌ها را انتخاب کنید، در غیر این صورت باید تیک آنها را بردارید، در شکل روبرو پورت‌های سوئیچ را مشاهده می‌کنید که بعضی از آنها روشن (سبز) و بعضی از آنها خاموش (قرمز) هستند.

بر روی Next کلیک کنید.



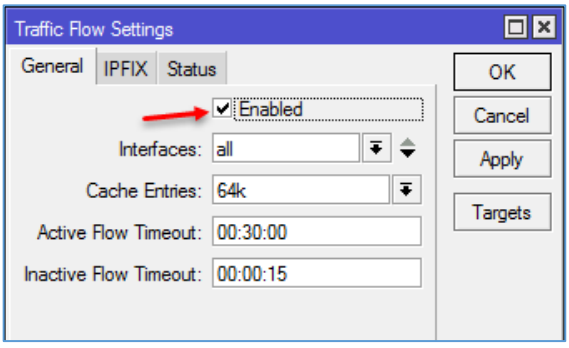
در این قسمت می‌توانید نرم‌افزارهایی که بر روی سرور اجرا شده است و می‌خواهید آنها را نیز آنالیز کنید باید گزینه‌ی مربوط به آن را انتخاب کنید و در قسمت Cerdential باید نام کاربری و رمز عبوری که دسترسی کامل داشته باشد را وارد و بر روی Next کلیک کنید، از آنجایی که در قسمت روبرو Cisco را انتخاب کردید، نیاز نیست گزینه‌ای را انتخاب کنید و تنها باید بر روی Next کلیک کنید، در صفحات بعد نیز بر روی Next و در صفحه‌ی آخر بر روی OK کلیک کنید.

بررسی سرویس NetFlow در روتر میکروتیک:

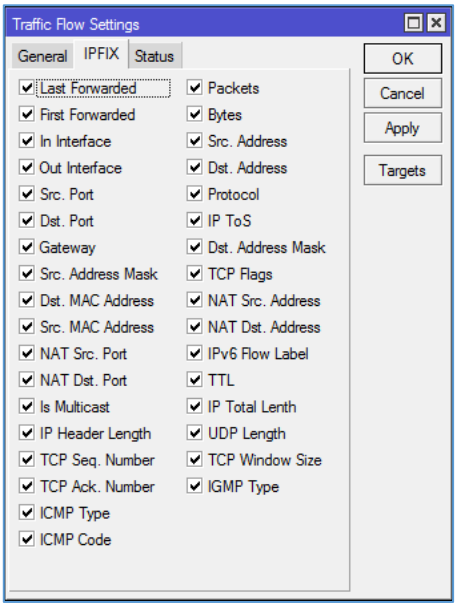


میکروتیک، یک روتر کارآمد و ارزان قیمت در ایران است که طرفداران زیادی دارد، از ویژگی‌های مهمّ آن، پشتیبانی از NetFlow است که این ویژگی را بررسی می‌کنیم.

با نرم‌افزار Winbox به روتر میکروتیک خود متّصل شوید و از قسمت IP بر روی گزینه‌ی Traffic Flow کلیک کنید.

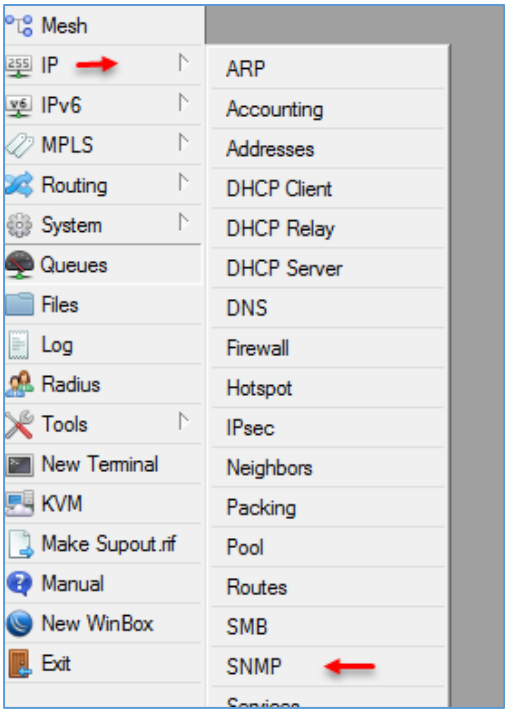


در این صفحه، تیک گزینه‌ی Enabled را انتخاب کنید تا این سرویس فعّال شود، در قسمت Interface می‌توانید همه‌ی آنها را انتخاب و یا کارت شبکه‌ای را انتخاب کنید که به کاربران سرویس می‌دهد.

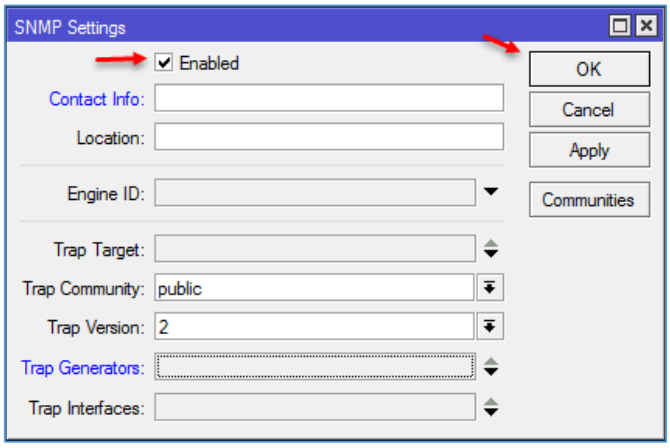


در تب IPFIX می‌توانید مشخّص کنید که چه گزینه‌هایی در نرم‌افزارهای مانیتورینگ بررسی شود.

بر روی OK کلیک کنید تا تنظیمات اعمال شود.

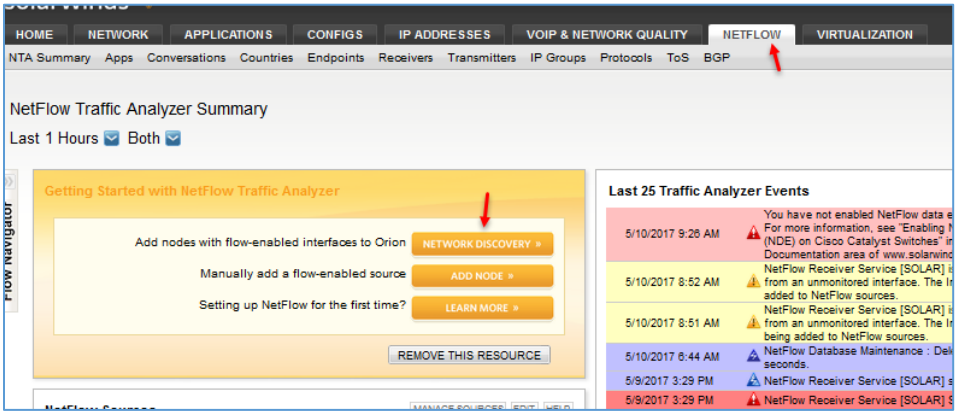


بعد از فعّال کردن سرویس Netflow باید سرویس SNMP را نیز برای دسترسی به اطّلاعات روتر میکروتیک فعّال کنید، برای این کار از قسمت IP، گزینه‌ی SNMP را انتخاب کنید.

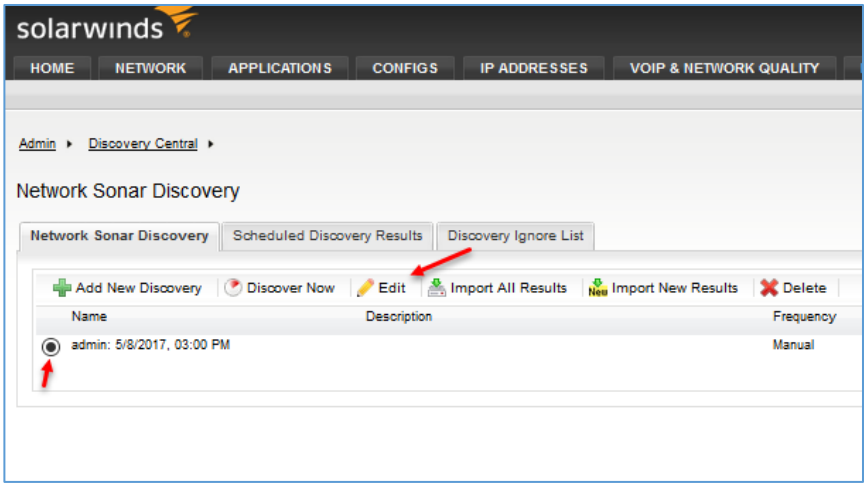


در این صفحه، تیک گزینه‌ی Enable را انتخاب و بر روی OK کلیک کنید.

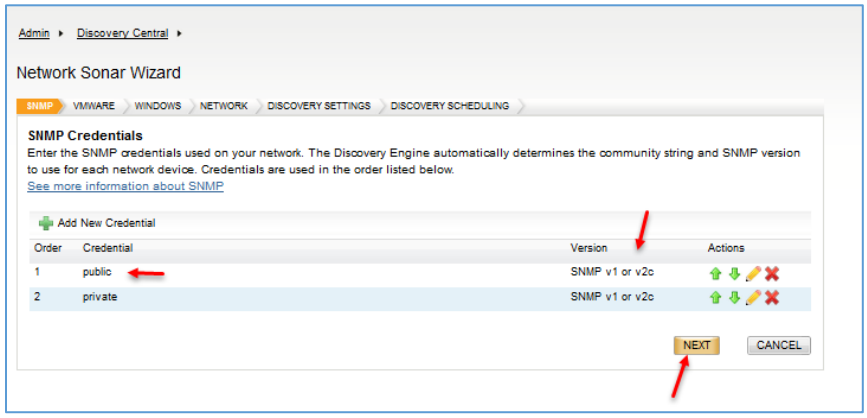
با این کار، همه چیز برای ارتباط Solarwins با میکروتیک آماده است.



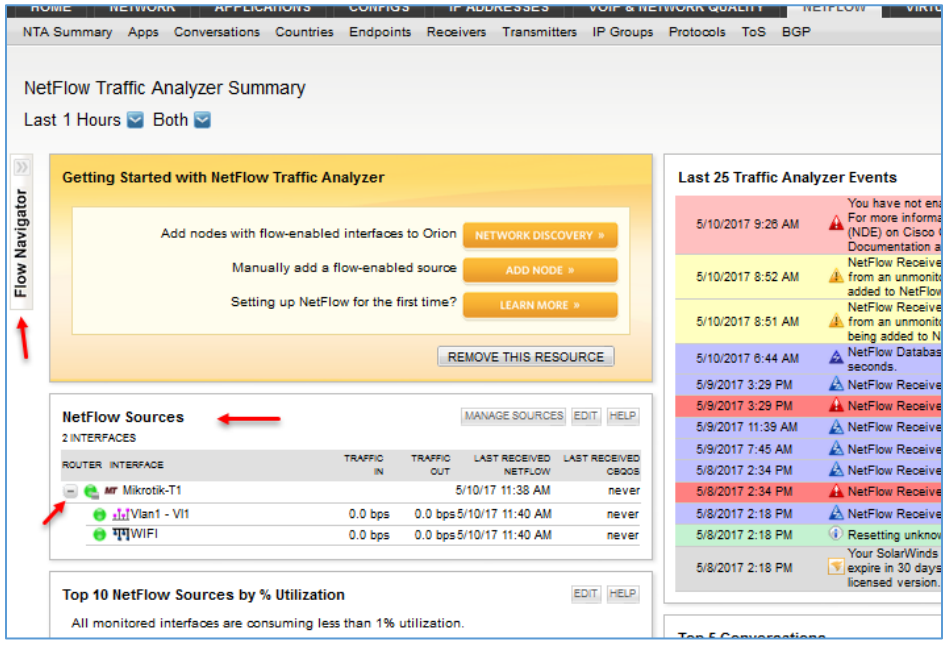
وارد نرم‌افزار Solarwins شوید و در قسمت Netflow که قبلاً کار کردید بر روی Network Discovery کلیک کنید و به مانند قبل، این کار را انجام دهید.



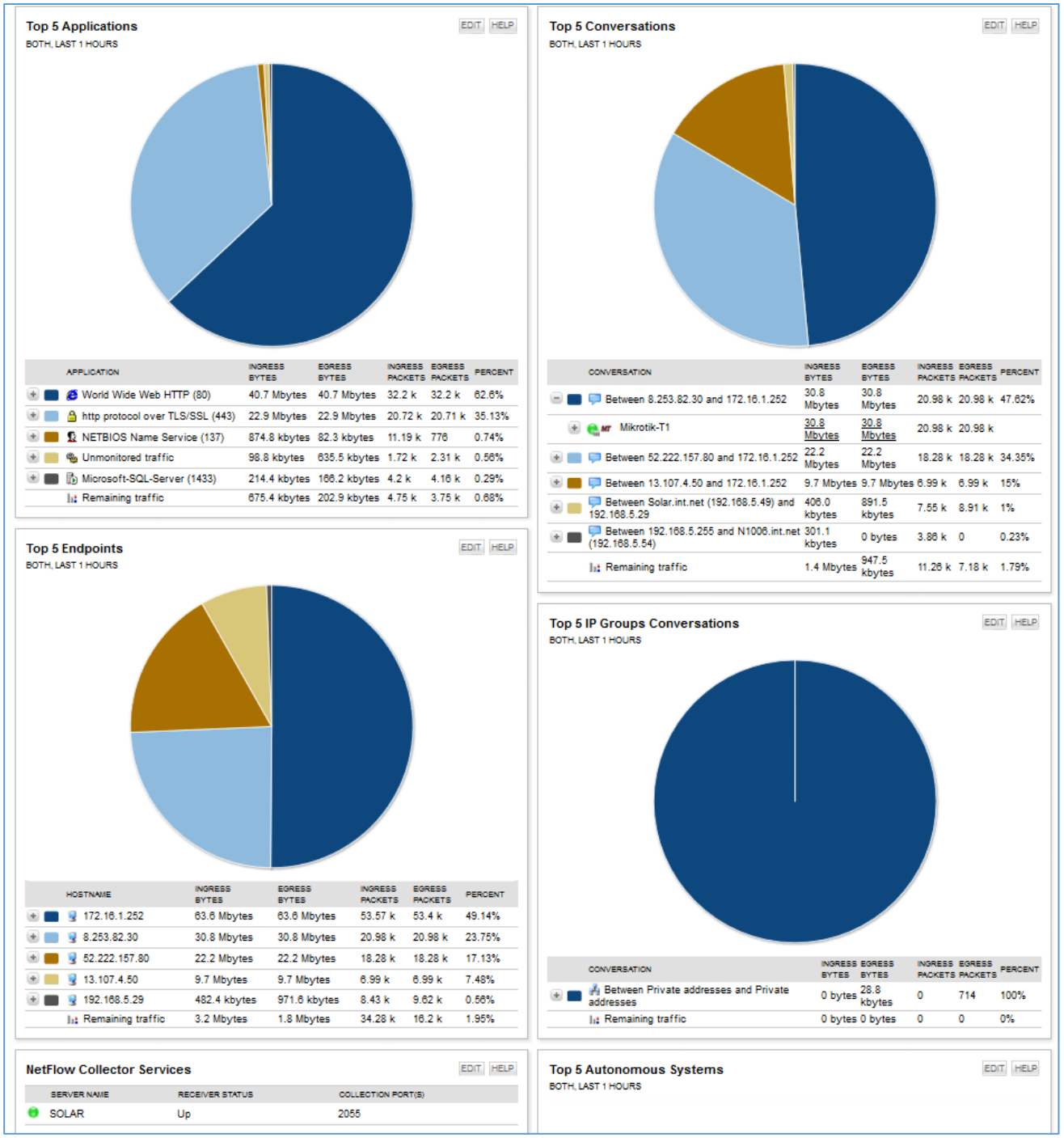
در این صفحه، از آنجایی که قبلاً عملیّات Discover را انجام دادید، این گزینه را مشاهده می‌کنید، اگر بخواهید تنظیمات آن را دوباره بررسی کنید باید گزینه‌ی مورد نظر را انتخاب و بر روی Edit کلیک کنید.



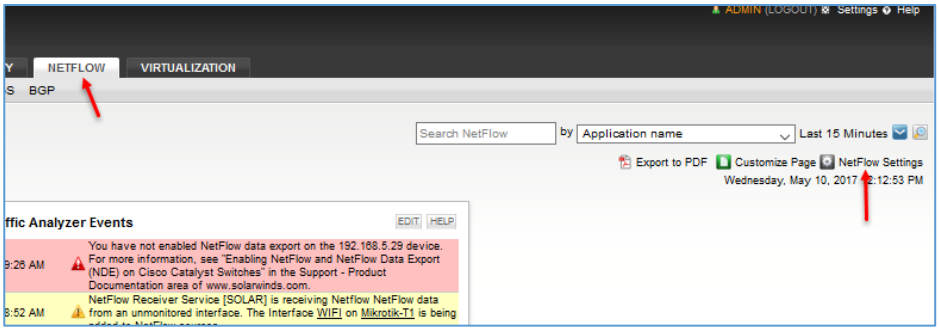
در این صفحه که مربوط به سرویس SNMP است باید نام کاربری که به سرویس SNMP دسترسی داشته باشد را وارد کنید که به صورت پیش‌فرض دو گزینه‌ی Public و Private وجود دارد که همین دو گزینه در بیشتر دستگاه‌ها وجود دارند. سرویس SNMP دارای ورژن های ۱، ۲، ۳ است که در هر سطح، امنیّت آن نیز افزایش یافته است و شما می‌توانید در سطح ۳ برای خود، یک نام کاربری و رمز عبور تعریف کنید تا امنیّت کار در ارتباط با آن دستگاه بالا برود.



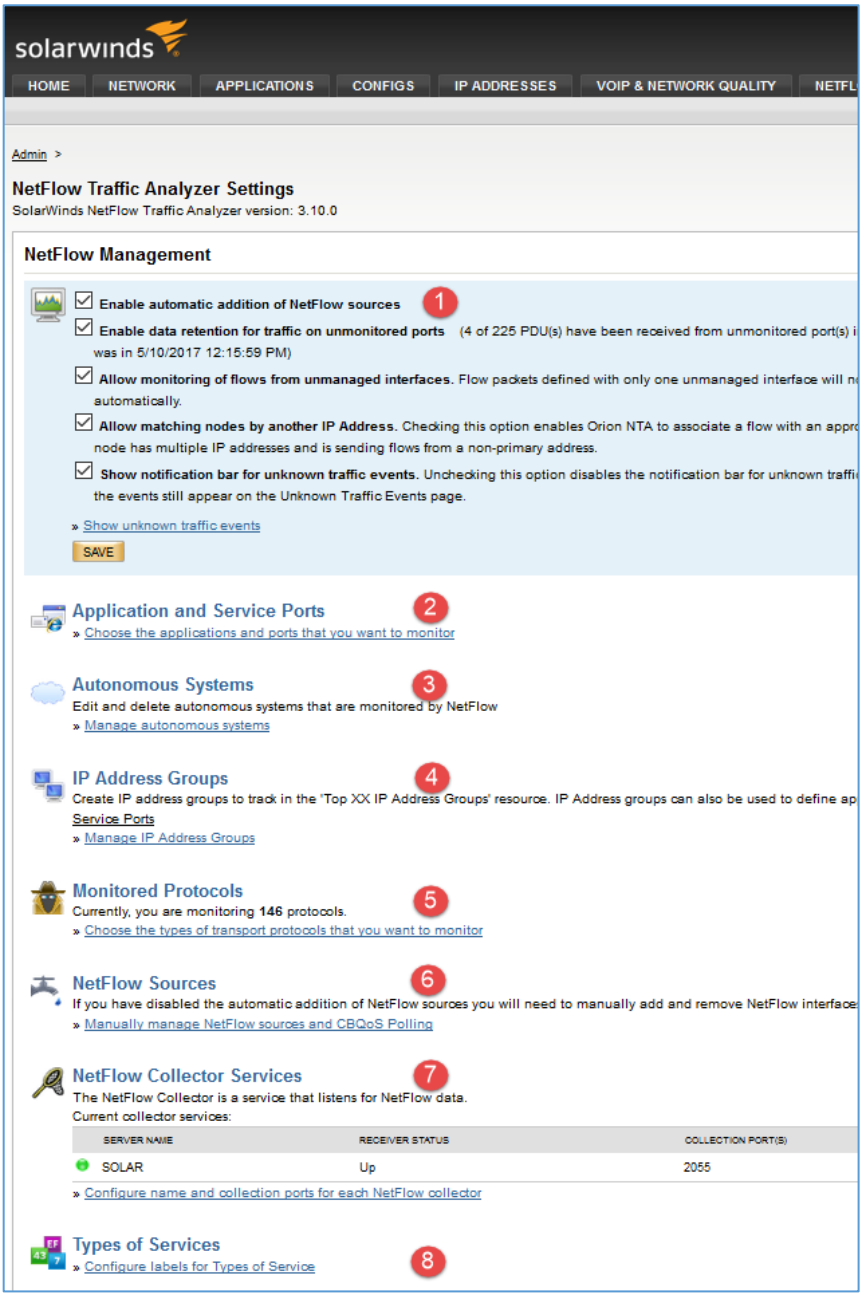
بعد از چند دقیقه که عملیّات Discovery انجام شد، اگر وارد Netflow شوید در قسمت NetFlow Source روتر میکروتیک را مشاهده خواهید کرد که Interface های آن نیز مشخّص شده است.



در شکل بالا، اطّلاعات مربوط به روتر میکروتیک را مشاهده می‌کنید، مانند اینکه حداکثر میزان ترافیک توسّط چه سیستم و آدرسی استفاده شده است و یا اینکه چه نوع نرم‌افزار و پروتکلی از ترافیک شبکه در حال استفاده است، این موارد یکی از کوچکترین عملکرد نرم‌افزار Solarwins است که اگر خوب در آن دقّت کنید می‌توانید به نتایج خوبی دست یابید.

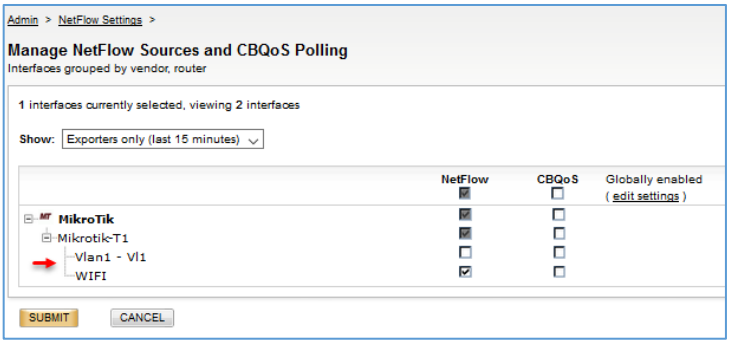


برای بررسی تنظیمات Netflow، به مانند شکل روبر وارد تب Netflow شوید و بر روی NetFlow Settings کلیک کنید.



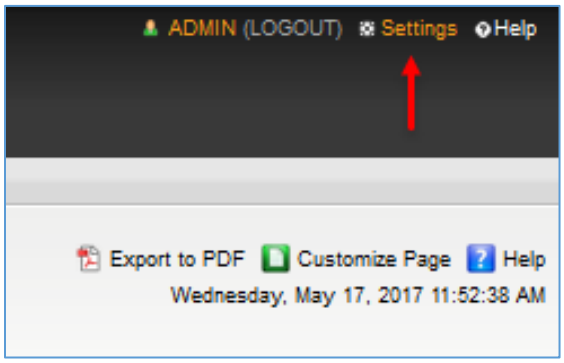
در این صفحه، گزینه‌های مختلفی وجود دارد، در قسمت شماره‌ی یک می‌توانید به نرم‌افزار اعلام کنید که کار NetFlow برای بررسی شبکه به صورت اتوماتیک انجام نشود و گزینه‌های دیگر؛ در قسمت شماره‌ی دو می‌توانید تعداد پورت‌هایی که برای Netflow و برای ارتباط با نرم-افزار و دستگاه در نظر گرفته شده است را ببینید که خود نیز می‌توانید پورت‌های مختص به یک نرم‌افزار خاص را وارد کنید، در قسمت شماره‌ی سه نیز یک‌سری سیستم‌هایی به صورت پیش‌فرض تعریف شده است، در قسمت شماره‌ی چهار، تمام رنج آدرس‌هایی که چه به صورت اتوماتیک و چه به صورت دستی وارد کردید، در لیست وجود دارد که شما می‌توانید آنها را حذف و یا به لیست اضافه کنید، در قسمت شماره پنج، لیستی از پروتکل‌هایی که مانیتور می‌شود، مشخّص شده است، در قسمت شماره‌ی شش، لیستی از اینترفیس‌هایی که از دستگاه‌های مختلف شناسایی شده،

مشخّص شده است، این موضوع را می‌توانید در شکل روبرو مشاهده کنید، در روتر میکروتیک شناسایی‌شده که قبلاً عملیّات را انجام دادیم، دو اینترفیس پیدا شده است که شما می‌توانید یکی از آنها را برای عملیّات NetFlow انتخاب کنید، البتّه همیشه اینترفیسی انتخاب می‌شود که به کاربران سرویس می‌دهد.

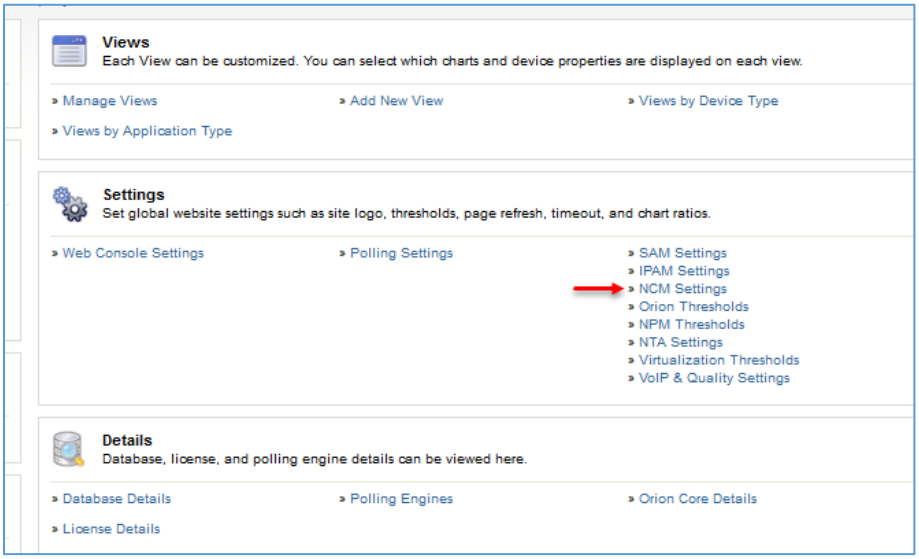


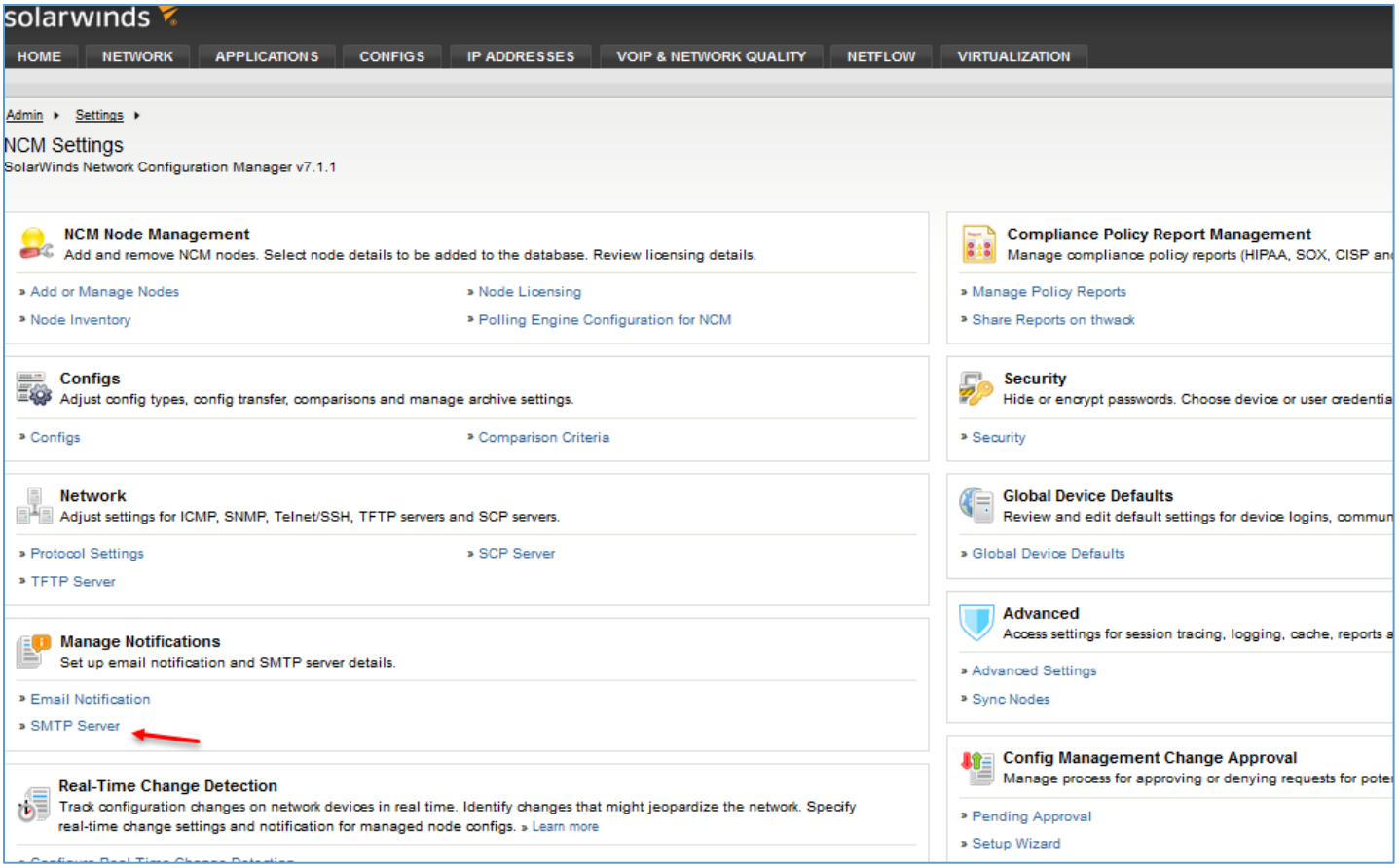
در صفحه‌ی قبل و شماره‌ی هفت، لیست سرورهایی که عملیّات مانیتورینگ Netflow را انجام می‌دهند به همراه پورت مشخّص شده است، در قسمت شماره‌ی هشت نیز لیستی از سرویس‌ها تعریف شده است که سرویس NetFlow از آنها برای دریافت اطّلاعات استفاده می‌کند.

زمانی که نرم‌افزار Solar با هشداری روبرو می‌شود، برای اینکه یک نسخه از آن را به آدرس ایمیل خاصّی ارسال کند باید تنظیمات مربوط به ایمیل را انجام دهید.

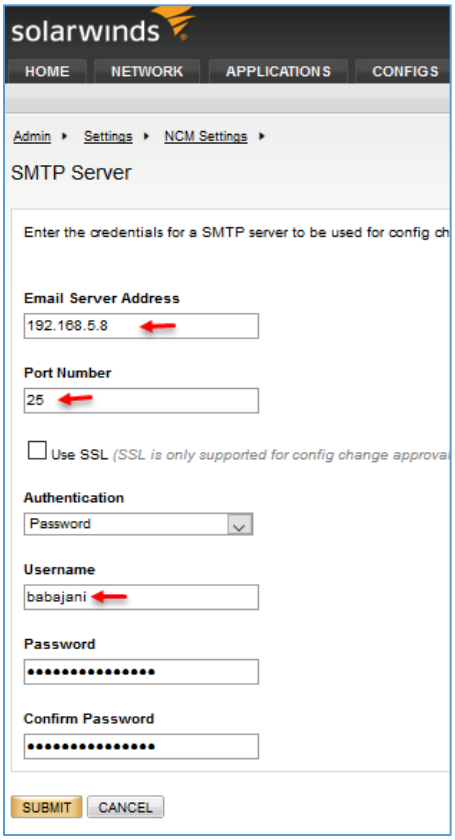


در این صفحه و از قسمت Settings بر روی NCM Settings کلیک کنید.



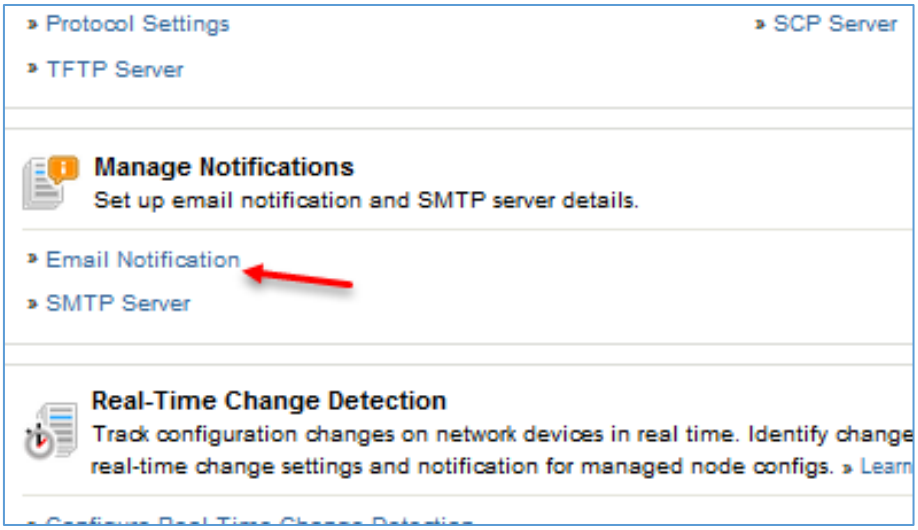


در صفحه‌ی بالا و در قسمت Manage Notifications بر روی گزینه‌ی SMTP Server کلیک کنید.

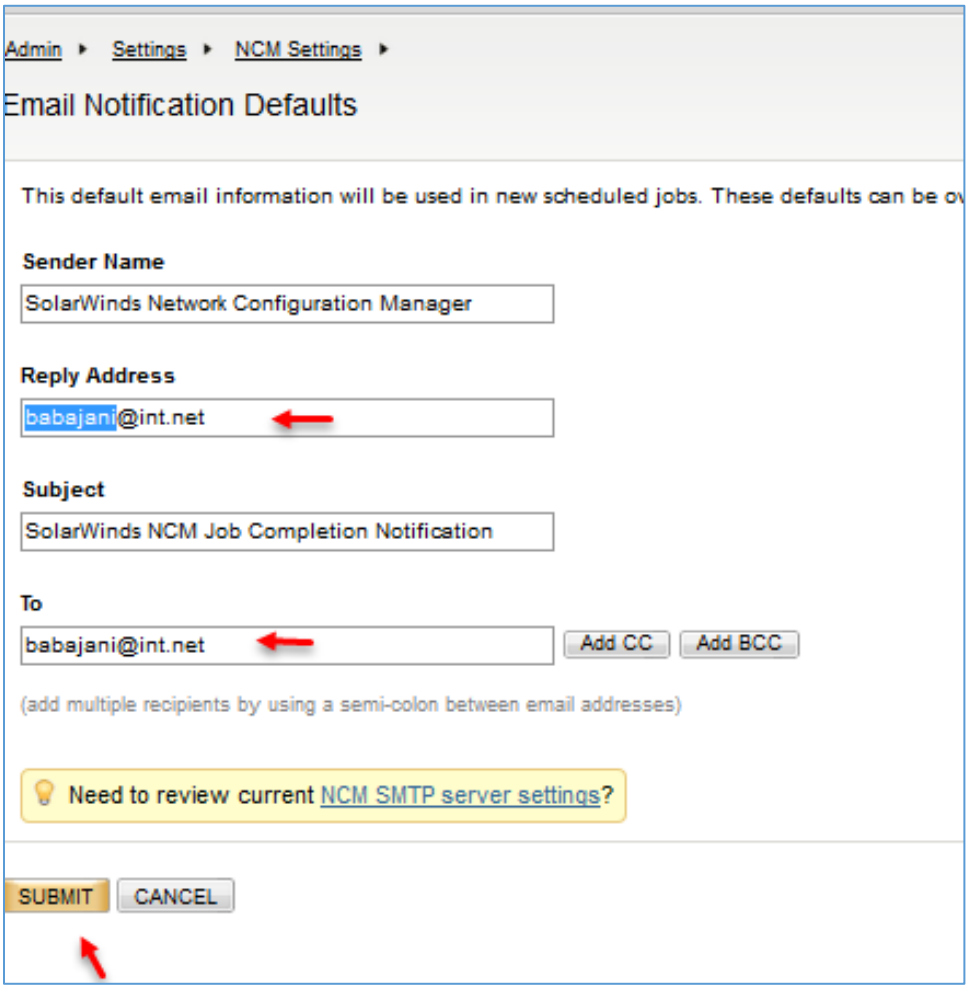


در صفحه‌ی روبرو و در قسمت Email Server Address، نام سرور ایمیل خود را وارد کنید و در قسمت Port باید آدرس پورت سرور ایمیل خود را وارد کنید که به صورت پیش‌فرض ۲۵ است، اگر چنانچه از پروتکل SSL استفاده می‌کنید باید تیک گزینه‌ی Use SSL را انتخاب کنید که پورت پیش‌فرض آن ۵۸۷ است، در قسمت آخر نیز یک نام کاربری که به سرور ایمیل دسترسی داشته باشد را وارد کنید و بر روی Submit کلیک کنید.

با این کار، تنظیمات ایمیل شما فعّال می‌شود.



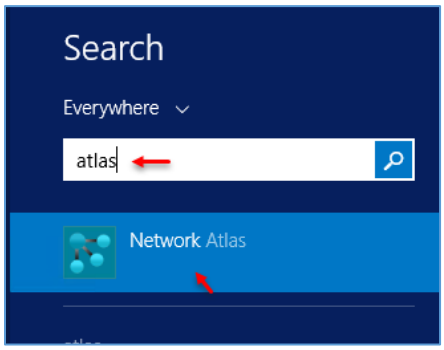
بعد از تنظیم ایمیل باید یک آدرس ایمیل نیز به عنوان فرستنده وارد نرم‌افزار کنید، برای این کار به مانند شکل روبرو بر روی Email Notification کلیک کنید.



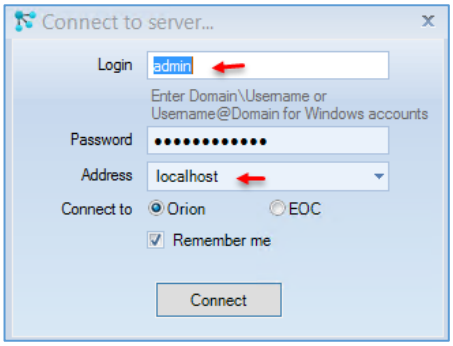
در این صفحه باید یک آدرس ایمیل در جای مشخّص‌شده وارد کنید تا اطّلاعات، هشدارها و تغییرات به آن ایمیل ارسال شود، بعد از وارد کردن اطّلاعات بر روی Submit کلیک کنید.

کار با نقشه‌ها در SolarWins:

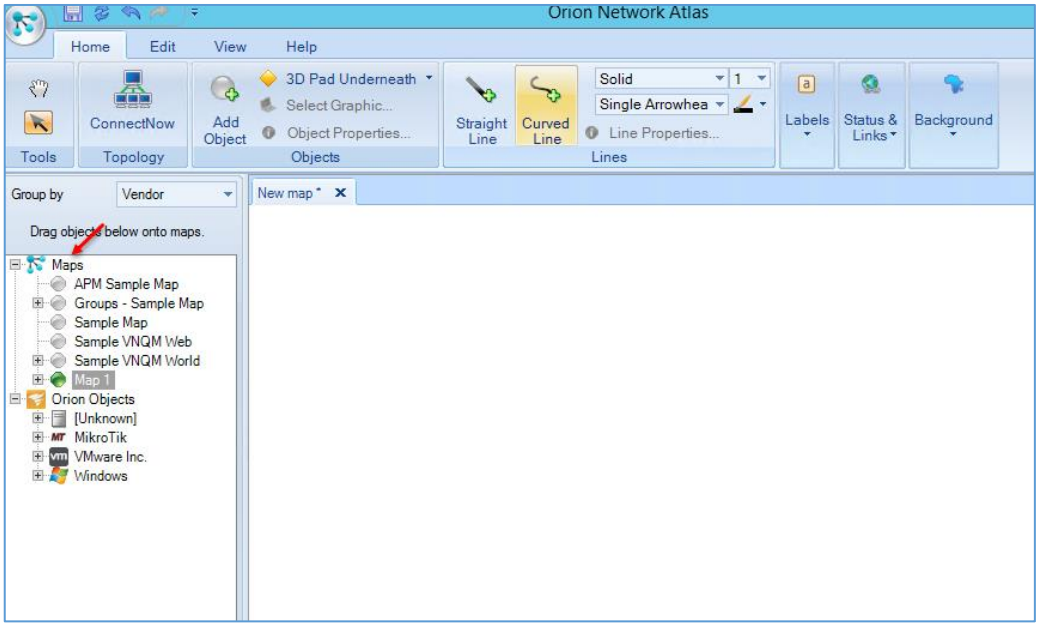
یکی از ویژگی‌های SolarWins این است که می‌توانید با سرویس Orion Network Atlas، یک نقشه از ساختمان خود تهیّه کنید و کلاینت‌ها و سرورهای خود را در آن لیست قرار دهید و آن نقشه را در صفحه‌ی اوّل Solar به نمایش بگذارید.



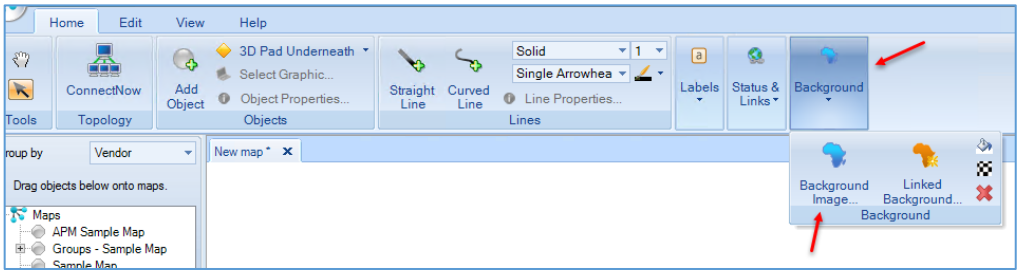
برای اجرای Orion Network Atlas وارد سرور Solar شوید و در منوی Start نرم‌افزار را اجرا کنید.



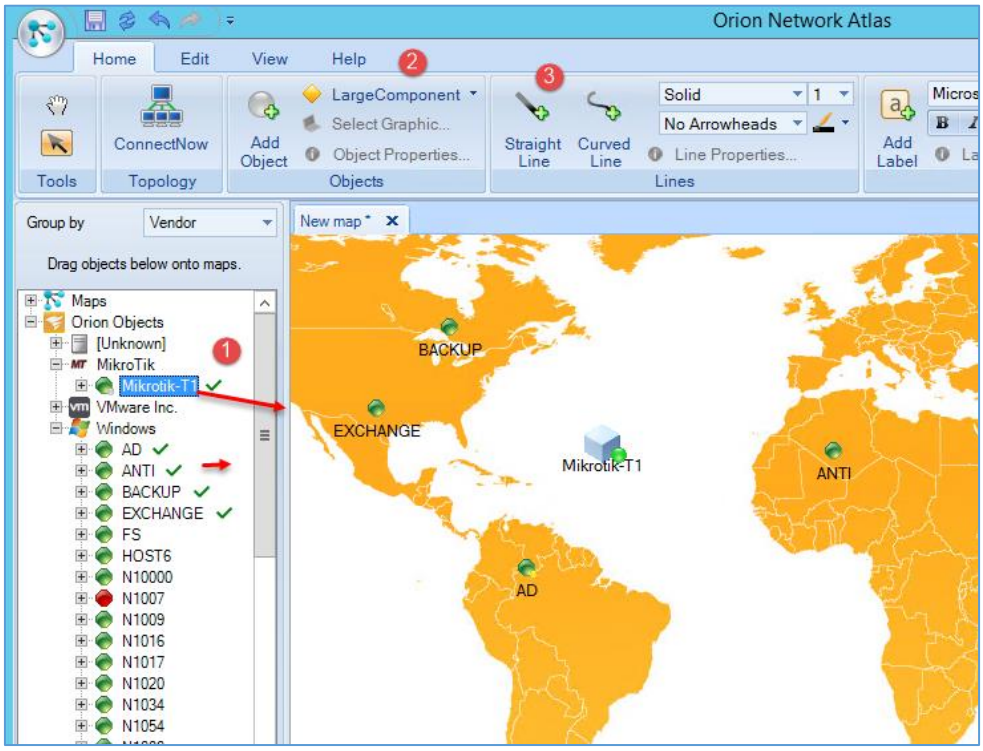
بعد از اجرا، شکل روبرو ظاهر می‌شود که باید در قسمت Login، نام کاربری را وارد و رمز آن را در قسمت Password وارد کنید، توجّه داشته باشید این نام کاربری، همان نامی است که در نرم‌افزار تحت وب وارد می‌کنید، در قسمت آدرس نیز باید نام سرور را وارد کنید.



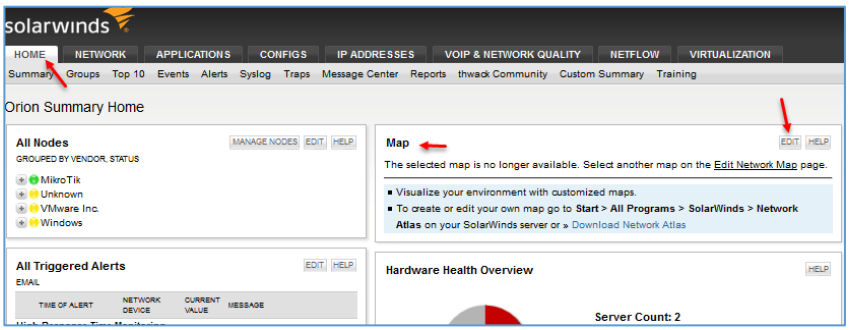
همانطور که در شکل روبرو مشاهده می‌کنید، نرم‌افزار Atlas اجرا شده است که دارای گزینه‌های مختلف است.

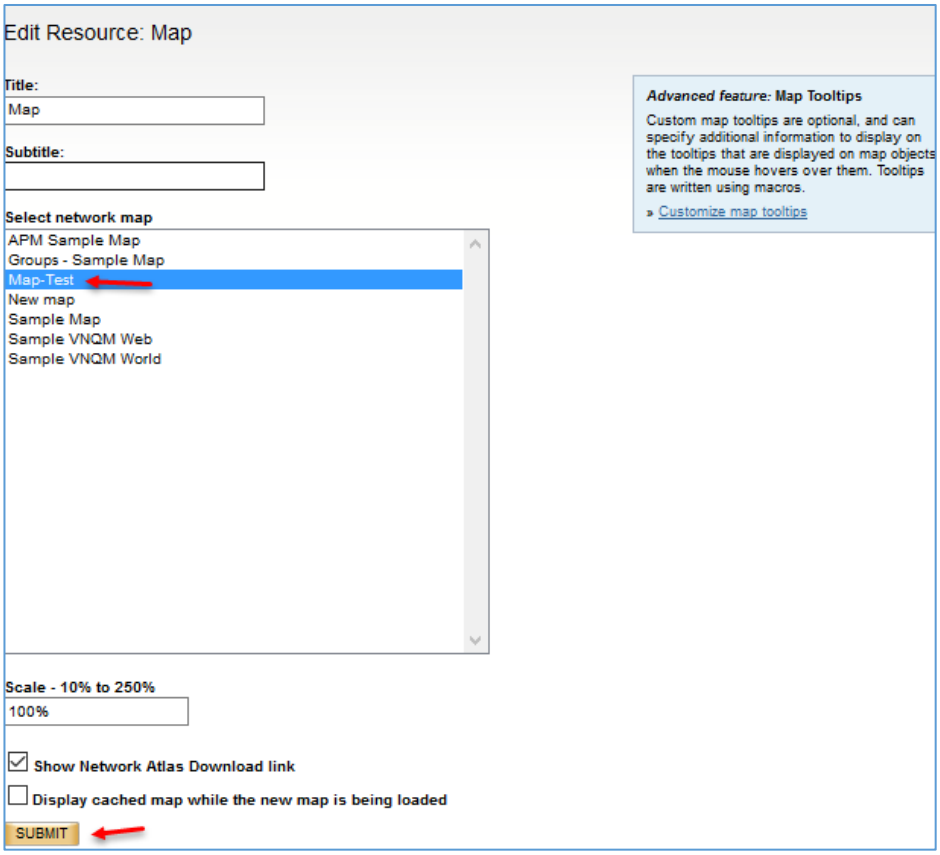


برای شروع و طرّاحی نقشه باید نقشه‌ای از ساختمان، یا منطقه‌ی جغرافیایی خود تهیّه کنید، برای وارد کردن نقشه بر روی Background کلیک کنید و گزینه‌ی Background image را انتخاب و عکس مورد نظر خود را وارد صفحه کنید.

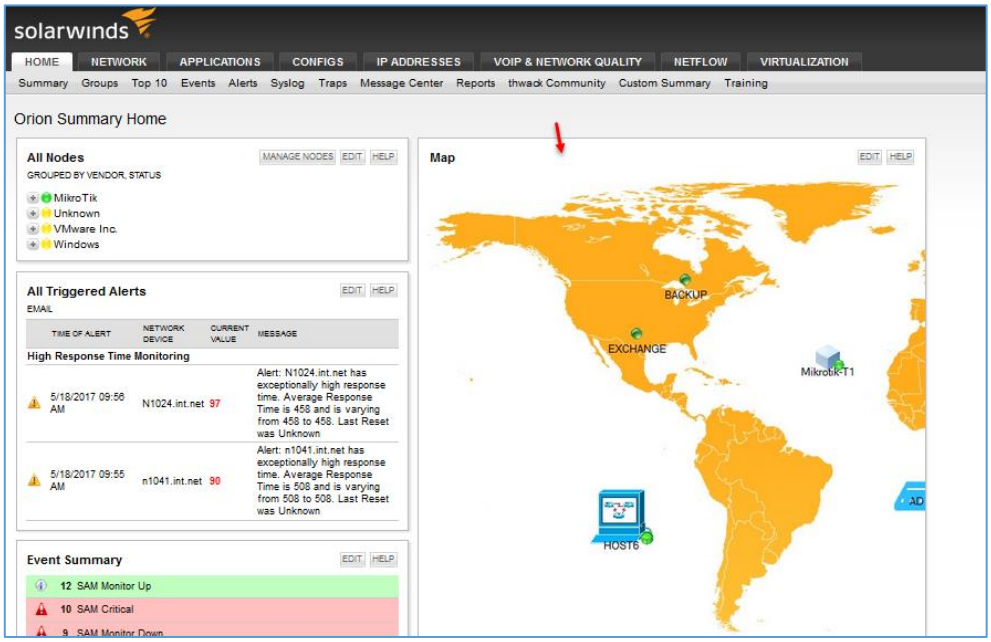


برای مثال در این صفحه، یک نقشه وارد کردیم که شما می‌توانید کلاینت‌های خود را از سمت چپ، انتخاب کنید و به داخل نقشه بکشید و رها کنید که این کار را در شکل روبرو مشاهده می‌کنید، با انتخاب Node های مورد نظر در نقشه و انتخاب یکی از گزینه‌های شماره دو می‌توانید آیکون آنها را تغییر دهید، قسمت شماره سه نیز برای ایجاد ارتباط بین Node ها است، بعد از انجام عملیّات بالا، این نقشه را ذخیره کنید و دوباره وارد صفحه‌ی اوّل نرم‌افزار Solarwins شوید و به مانند شکل روبرو در قسمتی که مربوط به MAP یا همان، نقشه است بر روی Edit کلیک کنید.





در این صفحه شما می‌توانید از قسمت Select Network Map، همان نقشه‌ای را که در قسمت قبل ایجاد و ذخیره کردید را در این قسمت، مشاهده و انتخاب کنید تا در صفحه‌ی اوّل به نمایش گذاشته شود.



همانطور که در شکل روبرو مشاهده می‌کنید، نقشه‌ی مورد نظر به صفحه‌ی اوّل اضافه شده است، توجّه داشته باشید این نقشه به صورت آنلاین است و Node ها بر روی آن نیز کار می‌کنند، این نقشه تنها برای مثال بیان شده است که بهتر است شما برای استفاده، یک نقشه‌ی خوب از ساختمان و اتاق‌ها داشته باشید تا مدیریّت سرورها و کلاینت‌ها آسان‌تر شود.

نصب و راه‌اندازی سیستم سانترال:

سانترال :

به منظور ایجاد یک شبکه‌ی خصوصی در یک مجموعه (شرکت) مورد استفاده قرار می‌گیرد که در آن با به اشتراک گذاشتن تعدادی از خطوط شهری، امکان استفاده برای تمام داخلی‌ها (با تنظیم امکانات و محدودیّت‌ها) به وجود خواهد آمد، در واقع یک دستگاه سانترال، حکم یک مرکز مخابرات کوچک را خواهد داشت که در اختیار یک مجموعه قرار می‌گیرد. امکانات بالقوّه‌ی دستگاه و تلفن سانترال، شرکت‌ها و حتّی فروشگاه‌ها را ملزم به استفاده از این دستگاه می‌کند، از جمله‌ی این امکانات می‌توان به اشتراک گذاشتن خطوط شهری تلفن گویا، دسترسی آسان و بدون هزینه‌ی داخلی‌ها به یکدیگر، اشتراک لوازم مخابراتی بین داخلی‌ها و... اشاره کرد. سانترال‌ها را می‌توان با توجّه به ظرفیّت و یا نحوه‌ی برقراری ارتباط بین داخلی‌های خود تقسیم‌بندی کرد.

این دسته برای کسب و کارهای کوچک و متوسّط، طرّاحی شده است، طوری که می‌توان نیازهای یک اداره، یا یک شرکت متوسّط را به شکل کامل و مناسب پوشش دهد و تا ظرفیّت ٢٤ خطّ داخلی و ٨ خطّ شهری قابل افزایش هستند. این دستگاه‌ها با توجّه به امکانات و ویژگی‌های بسیار متنوّع و بالقوّه‌ی خود می‌توانند گزینه‌ی مناسبی برای سامان‌دهی به تماس‌های ورودی و داخلی و حتّی کنترل آنها باشند. دستگاه‌های کم ظرفیّت پاناسونیک علی رقم قیمت بسیار مناسب، بخش عظیمی از امکانات دستگاه‌های پیشرفته‌ی موجود در بازار را فراهم می‌کنند و می‌توانید آنها را نسبت به محیط کار و نیاز اختصاصی خود، قابل برنامه ریزی و ارتقا کنید تا نهایت لذّت را از محیط کار خود ببرید.



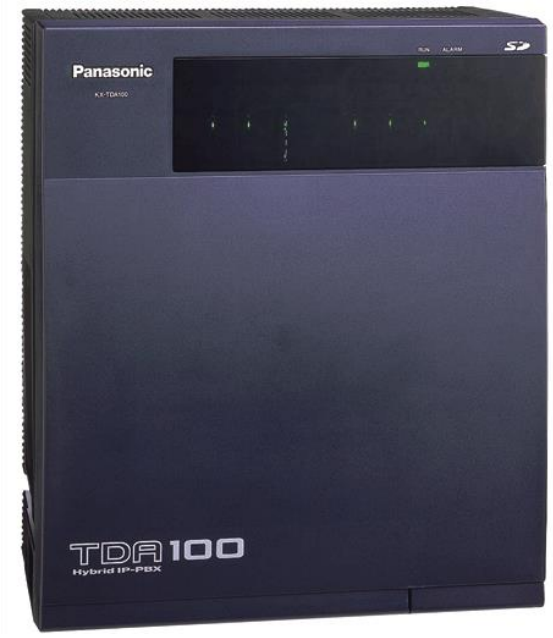
پاناسونیک، یکی از قوی‌ترین شرکت‌ها در این زمینه است که دستگاه‌های سانترال را در مدل‌های مختلف به بازار ارائه کرده است که این دستگاه‌ها دارای ظرفیّت‌ها و امکانات متفاوتی است.

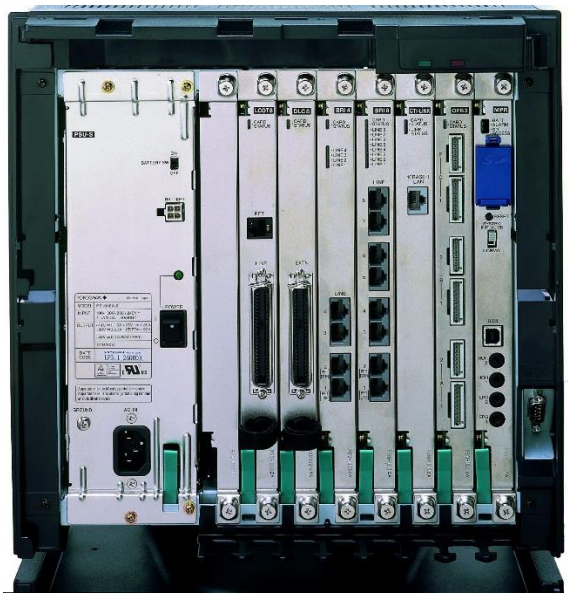
تجهیزات سانترال پاناسونیک:

هر سیستم تلفنی تجهیز شده با سانترال پاناسونیک، دارای چند بخش اصلی است، بخش اوّل، دستگاه سانترال، بخش دوّم، گوشی‌های تلفن، بخش سوّم، کارت‌های تلفنی که در دستگاه سانترال، ممکن است از ابتدا همراه دستگاه بوده باشد و یا به صورت جداگانه، آن کارت به دستگاه مرکزی سانترال اضافه شود و بخش چهارم، تجهیزات جانبی دستگاه است که ممکن است وجود آنها بر اساس نیاز بوده باشد و وجود آنها اختیاری است.

دستگاه مرکزی سانترال:

دستگاه مرکزی سانترال بر اساس دو پارامتر اصلی و چند پارامتر فرعی مورد بررسی قرار می‌گیرد؛ موضوع اصلی، ظرفیّت فعلی و ظرفیّت نهایی دستگاه است، یعنی این دستگاه در حال حاضر، چند خطّ شهری و داخلی را پشتیبانی می‌نماید و نهایتاً گنجایش ظرفیّت چند خطّ شهری و چه تعداد داخلی را دارد، امّا سیگنالینگ سانترال موضوع بعدی است، یعنی این دستگاه قابلیّت سرویس‌دهی به چه نوع گوشی‌ها و خطوط شهری را دارد.





گوشی‌های تلفن سانترال:



تلفن‌های سانترال پاناسونیک در تیپ‌های متفاوت تولید می‌شوند؛ برای کاربری‌های کارمندی ومدیریّتی، مدل‌های مختلفی وجود دارد که گوشی‌های کارمندی با قابلیّت‌های مشخّص و محدود برای کاربری‌های عمومی و هزینه‌ی کم طرّاحی شده است و گوشی‌های مدیریّتی برای استفاده‌های حرفه‌ای‌تر تولید می‌شوند.

اگر قرار است یک گوشی سانترال خریداری نمایید، توصیه می‌کنیم مدل‌های مختلف و قابلیّت‌های متفاوت گوشی‌ها را در تلفن سانترال بررسی نمایید و قبل از خرید با مشاهده‌ی تصاویر و قابلیّت‌های هر گوشی، اطّلاعات کافی را به دست آورید.

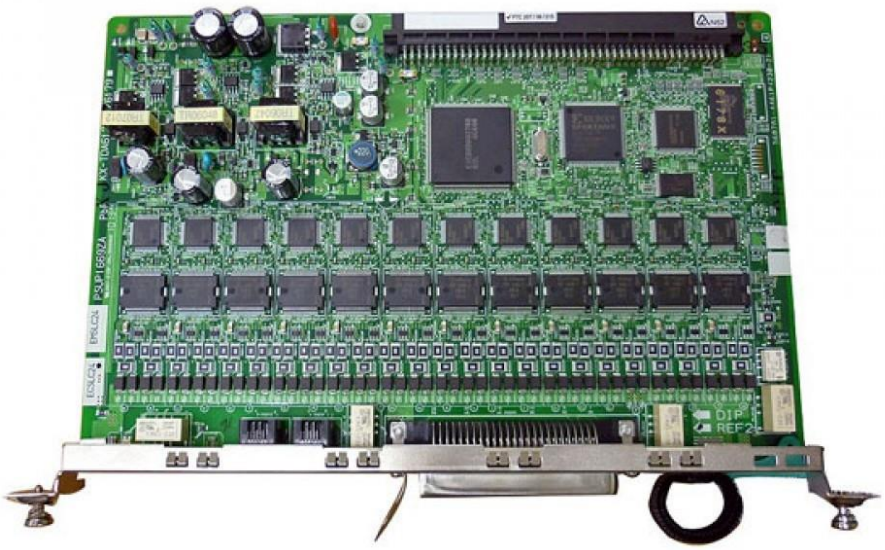
کارت‌های خطوط شهری:



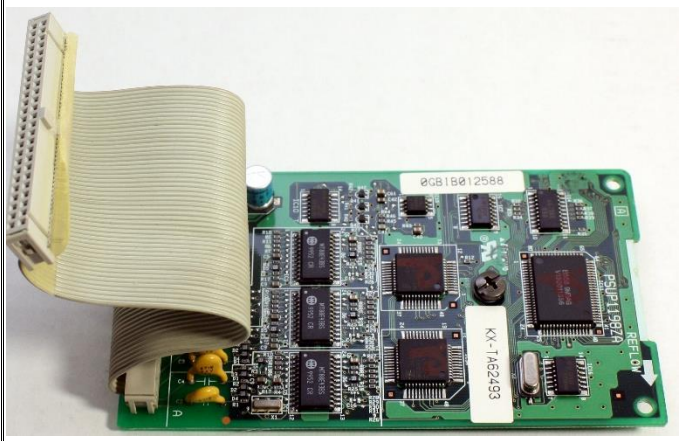
برای برقراری ارتباط خطوط شهری با دستگاه مرکزی سانترال از کارت‌های خطوط شهری استفاده می‌شود، این کارت‌ها بر روی دستگاه مرکزی قرار گرفته است و خطوط شهری را به مرکز تلفن متّصل می‌کنند؛ کارت‌های شهری در ظرفیّت‌ها و انواع مختلف تولید می‌شوند.

کارت خطوط داخلی سانترال:

کارت‌های داخلی، گوشی‌های تلفن را به باکس سانترال متّصل می‌کنند، این کارت‌ها باید با توجّه به نوع گوشی سانترال که می‌خواهید استفاده کنید، انتخاب شوند. کارت‌های داخلی از طریق کابل آنفولان به پست تلفن مرتبط می‌شوند و کابل‌های مخابراتی خطّ داخلی را تا میز کارمندان می‌رسانند و به این ترتیب، ارتباط داخلی‌ها با سانترال مرکزی برقرار می‌شود.



کارت‌های دیگر:



این کارت‌ها، کاربردی متفاوت از کارت‌های شهری و داخلی دارند و برقرار کننده‌ی ارتباط بین خطوط و دستگاه سانترال نیستند، این کارت‌ها قابلیّت‌هایی را متناسب با مدلی که دارند به سانترال پاناسونیک اضافه می‌کنند، مثل کارت کالرآیدی که قابلیّت نمایش شماره‌ی تماس گیرندگان را فراهم می‌کند و یا کارت دیزا که تلفن گویا را به دستگاه سانترال اضافه می‌کند.



تجهیزات جانبی سانترال:

تجهیزات جانبی غالباً به شکل باکس‌هایی هستند که قابلیّت‌های دیگری را به دستگاه سانترال اضافه می‌کنند؛ دستگاه ضبط مکالمات که شکل آن را در روبرو مشاهده می‌کنید، صندوق صوتی و گزارشات تماس از نمونه دستگاه‌های جانبی سانترال پاناسونیک هستند. TVM ها در مدل‌های مختلف، امکاناتی، نظیر آنچه گفته شد را به سانترال اضافه می‌کنند.

قبل از نصب سانترال پاناسونیک به این نکات توجّه کنید:

در این بخش به ۵ نکته‌ی مهم در مورد نصب سانترال اشاره می‌کنیم، با رعایت این موارد در زمان خود صرفه‌جویی و با نظم ایجاد شده، سرعت عیب‌یابی سیستم را افزایش دهید.

نکته‌ی اوّل، انتخاب مکان نصب سانترال:

ابتدا باید محلّ مناسبی برای قرارگیری دستگاه سانترال بر روی دیوار در نظر بگیرید، این محل باید از کف زمین دارای فاصله‌ی مناسبی باشد تا رطوبت و گرد و خاک کمتری به سانترال منتقل شود، موضوع بعدی در نظر گرفتن فاصله‌ی مناسب بین ۱ تا ۲ متر با پست مخابراتی است که کار توزیع خطوط در ساختمان و ارتباط آنها با خطوط مرکز تلفن را انجام می‌دهد. محلّ قرارگیری سانترال تا جای ممکن باید در وسط مسیر قرارگیری داخلی‌ها باشد تا متراژ کابل‌کشی کاهش یابد.

نکته‌ی دوّم، تهیّه‌ی نقشه‌ی مخابراتی:

اوّلین کار، تعیین مسیر خطوط مخابراتی از خطوط ورودی مخابرات تا سانترال و کاربران است، بعد از مشخّص کردن مسیر باید یک نقشه‌ی کامل از رنگ‌بندی خطوط مخابراتی، شماره‌ی خط، رنگ‌بندی کابل‌های داخلی تهیّه کنید؛ در هر نقطه که اتّصالی، مانند ترمینال و پست دارید باید به تفکیک رنگ، زوج سیم‌های ورودی و خروجی

و شماره‌ی هر پورت را در نقشه درج کنید، پس از برنامه‌ریزی مرکز و تعیین زنگ‌خورها و سطح دسترسی کاربران این نقشه تکمیل می‌شود.

نکته‌ی سوم، سیم‌بندی داخلی‌ها و آرایش پست:

موضوع بعدی در نظر گرفتن نحوه‌ی سیم‌بندی داخلی‌ها است، یعنی با در نظر گرفتن رنگ‌بندی کابل مخابراتی و نوع داخلی که دیجیتال، آنالوگ یا هایبرید است، زوج سیم‌های مربوط به داخلی‌ها را از مرکز تلفن تا کابل آنفولان و سپس تا پست مخابراتی و نهایتاً از پست تا پریز تلفن کاربر آرایش دهید. برای داخلی‌های آنالوگ و دیجیتال، یک زوج سیم، شامل دو رشته سیم کشیده است و برای داخلی‌های هایبرید، دو زوج سیم که زوج اوّل برای بوق و زوج دوّم برای دیتا است، کشیده می‌شود، نهایتاً سیم‌ها در پریزهای تلفن قرار می‌گیرند که برای داخلی‌های آنالوگ و دیجیتال در دو پین مرکزی و برای داخلی‌های هایبرید، دو رشته بوق در دو پین مرکزی و دو رشته دیتا در دو پین کناری پریز تلفن بسته می‌شود.

نکته‌ی چهارم، نصب سانترال و تجهیزات جانبی:

در این بخش بر اساس دستور موجود در دفترچه‌ی راهنمای دستگاه، ابتدا باید پایه یا پیچ‌های لازم بر روی دیوار و بعد، مرکزتلفن را در محلّ خود قرار دهید، حال در صورت وجود تجهیزات جانبی، مانند موزیک پشت خط، دستگاه ضبط مکالمات، باطری بکاپ و... این دستگاه‌ها را در محلّ خود قرار دهید و به سانترال متّصل کنید، پس از اطمینان از درستی نصب دستگاه و آرایش خطوط، وارد مرحله‌ی بعد شوید.

نکته‌ی پنجم، انجام تنظیمات سانترال:

در این بخش، یکی از دو روش برنامه‌ریزی تلفنی و یا کامپیوتری را انتخاب کنید و با آماده کردن دفترچه‌ی راهنمای برنامه‌ریزی، فرآیند انجام تنظیمات را شروع کنید، برای انجام تنظیمات، ابتدا تنظیمات عمومی، شامل تاریخ سیستم، تعیین شماره و نام داخلی‌ها را انجام دهید، سپس خطوط شهری بر روی سیستم طبقه‌بندی شده و بر اساس نیاز کارفرما، سطح دسترسی و زنگ‌خور هر خطّ شهری برای داخلی‌ها را انجام دهید، در نهایت اگر کارفرما، تنظیمات سفارشی، مانند تلفن گویا، ساعات کاری، گروه زنگ‌خور و... را مدّ نظر دارد، تنظیمات مربوط به آن را انجام دهید.

نصب و راه‌اندازی نرم‌افزار مدیریّت تلفن سانترال پاناسونیک:

زمانی که شما تلفن مرکزی سانترال را در شرکت خود پیاده‌سازی می‌کنید و کارت‌های مختص به آن را نصب می‌کنید باید تنظیمات اصلی آن را در نرم‌افزار آن انجام دهید، این گونه سیستم‌ها دارای کابل شبکه، کابل USB و... برای ارتباط با سیستم دارند تا بتوانید آنها را از طریق نرم‌افزار مختص به خودشان تنظیم کنید.

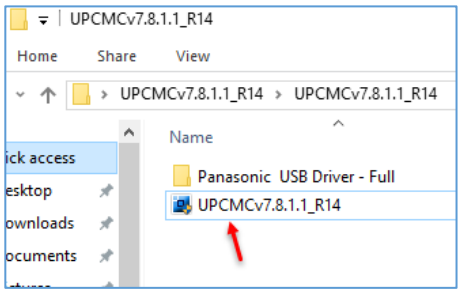
در این کتاب، نرم‌افزار مختصّ پاناسونیک را با نام اختصاری UPCMC بررسی می‌کنیم.



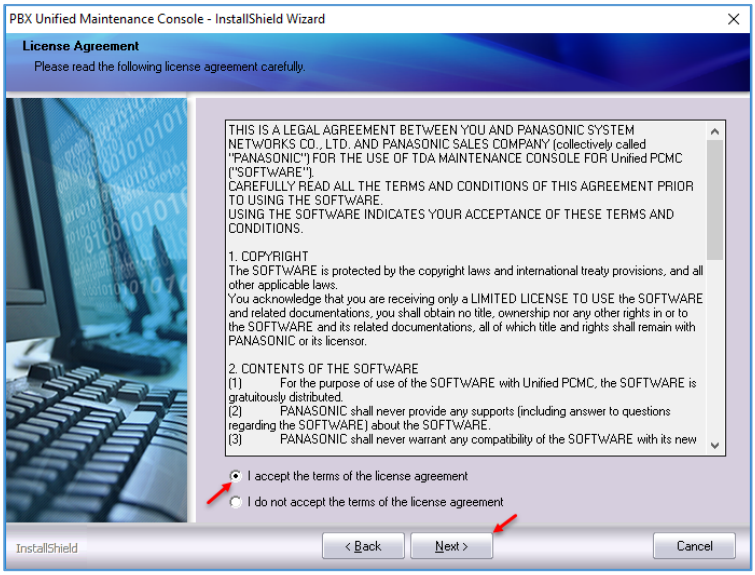
اگر داخل دستگاه پاناسونیک خود را نگاه کنید، در قسمت سمت راست و کارت اوّل، پورت‌های ارتباطی را مشاهده خواهید کرد، بر روی همان کارت، یک کارت ذخیره‌سازی که ظرفیّت پیش‌فرض آن، ۱۲۸ مگابایت است، قرار داده شده است که در شکل روبرو محلّ آن به صورت آبی‌رنگ مشخّص شده است. تمام اطّلاعات این سیستم در این کارت ذخیره می‌شود و این کارت به عنوان یک سیستم عامل برای دستگاه به کار می‌رود، زمانی که دستگاه روشن می‌شود، اطّلاعات خود را از این کارت دریافت می‌کند و سیستم اجرا می‌شود، این اطّلاعات می‌تواند، شامل تعداد خطوط ورودی به سانترال، شماره تلفن‌های این خطوط، نام و شماره‌ی تماس کاربران داخلی، سیستم تماس صوتی و... باشد.

برای اینکه بر روی این اطّلاعات کار کنید، نیاز به نرم‌افزار پاناسونیک دارید که عنوان این نرم‌افزار، UPCMC است که آن را از طریق لینک زیر می‌توانید دانلود کنید:

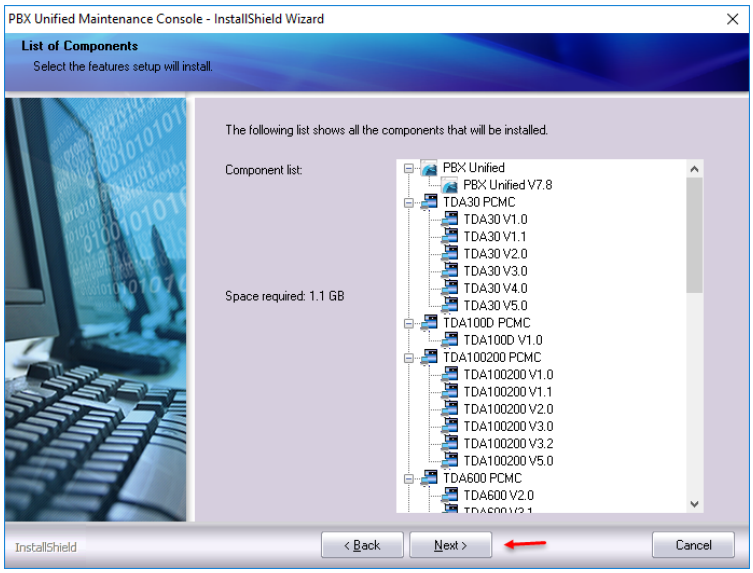
http://www.duivestein.nu/download/UPCMCv7.8.1.1_R14.zip



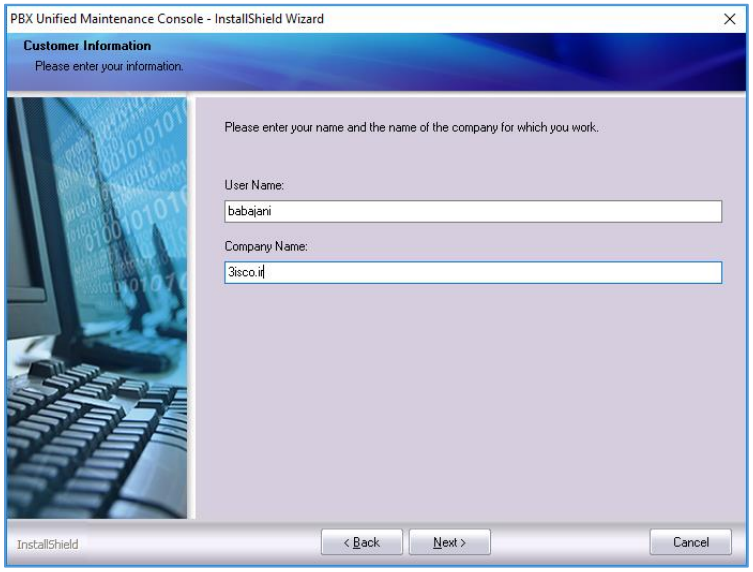
بعد از دانلود نرم‌افزار بر روی فایل اجرایی، به مانند شکل روبرو دوبار کلیک کنید.



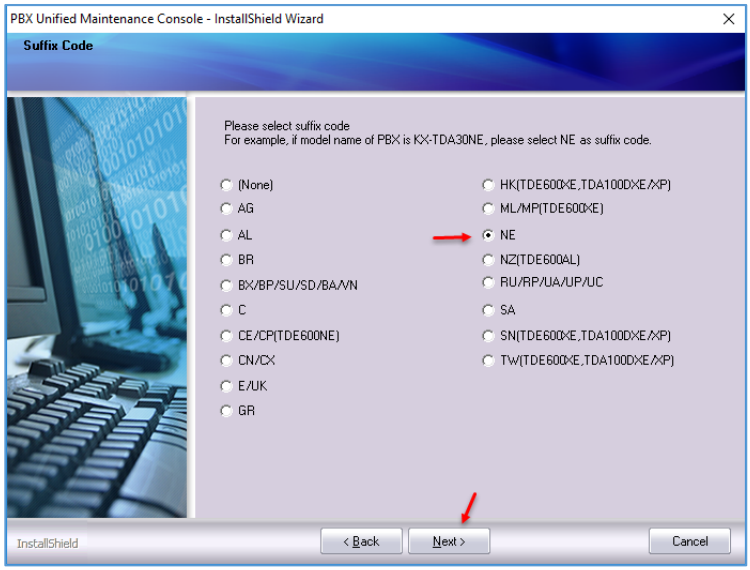
قراردادنامه را تأیید کنید و بر روی **Next** کلیک کنید.



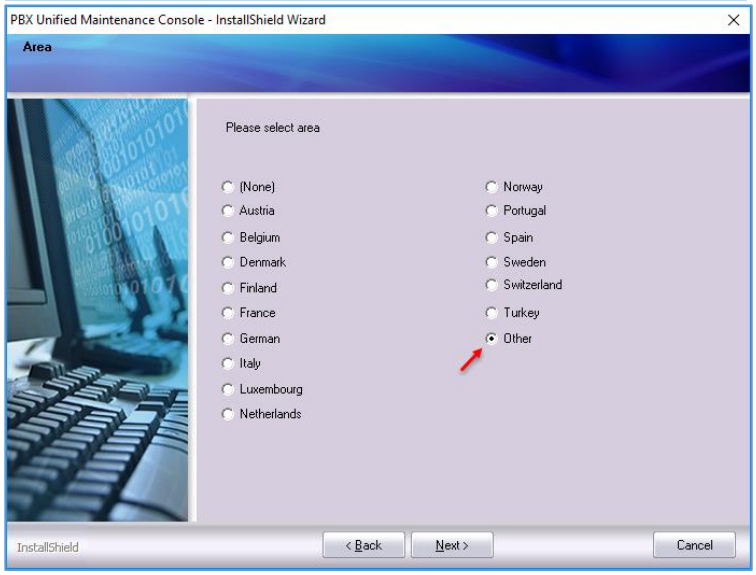
در این قسمت، تمام کامپوننت‌ها که برای مدل-های مختلف در نظر گرفته شده، مشخّص شده است، بر روی **Next** کلیک کنید.



در این قسمت، یک نام کاربری به دلخواه خود و یک نام برای شرکت خود به دلخواه وارد و بر روی **Next** کلیک کنید.

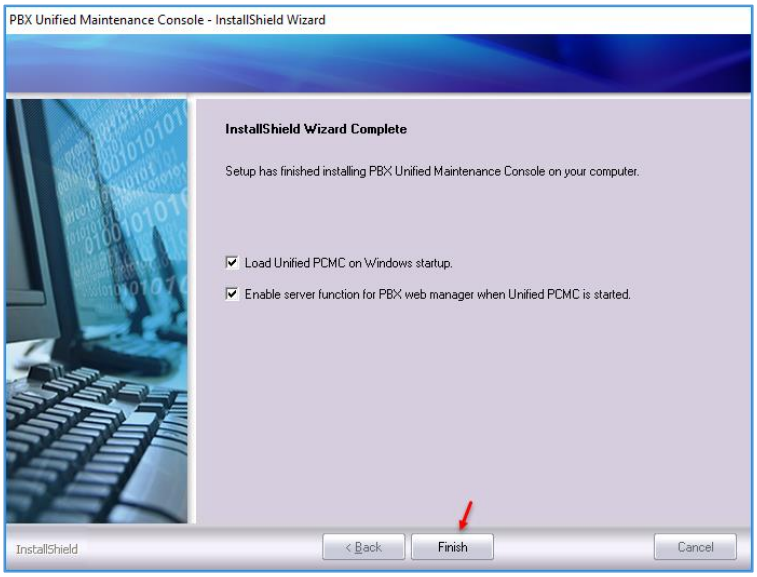


در این صفحه، بسته به نوع تلفن سانترال خود باید گزینه‌ی مورد نظر را مشخّص کنید که در اینجا، گزینه‌ی NE را انتخاب و بر روی Next کلیک کنید.

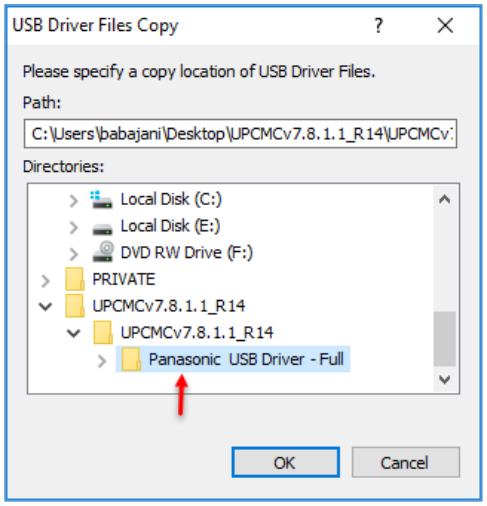


در این صفحه، منطقه‌ی خود را انتخاب کنید، اگر چنانچه منطقه‌ی شما در لیست نبود، گزینه‌ی Other را انتخاب و بر روی Next کلیک کنید.

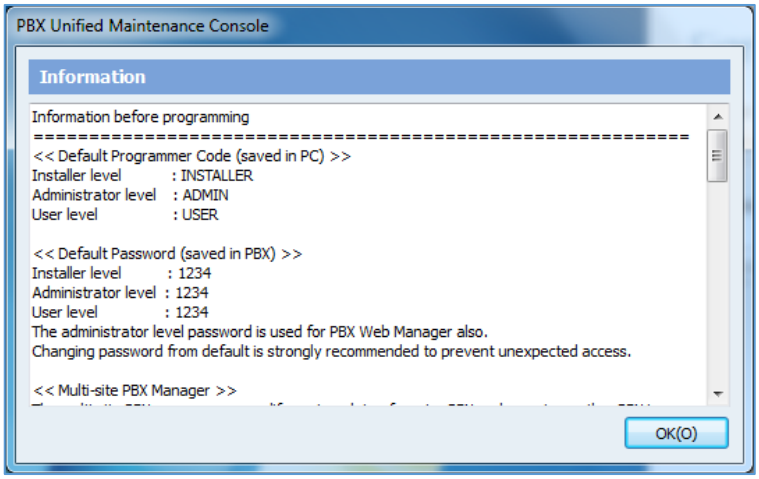
در صفحات بعد نیز بر روی Next کلیک کنید تا به صفحه‌ی زیر برسید.



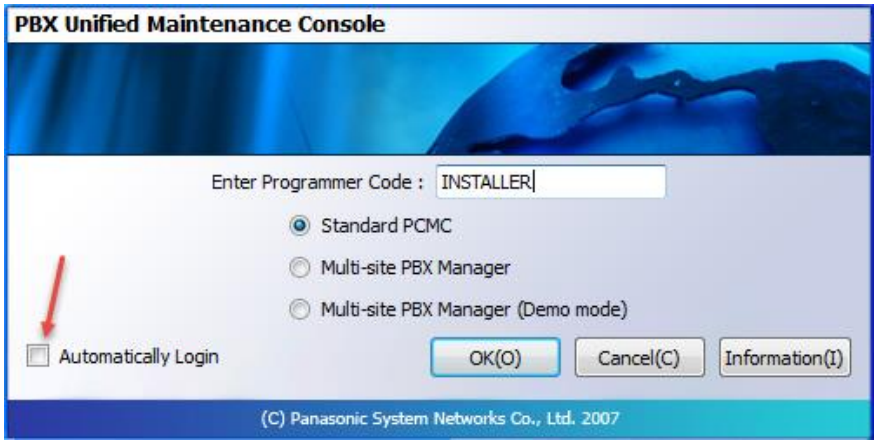
در این صفحه، دو گزینه‌ی مورد نظر را انتخاب و بر روی Finish کلیک کنید.



بعد از اینکه در مرحله‌ی قبل بر روی Finish کلیک کردید، صفحه‌ی روبرو ظاهر می‌شود که از شما درخواست می‌کند، به مانند شکل روبرو، درایور مربوط به سانترال پاناسونیک را برای USB به آن معرّفی کنید.



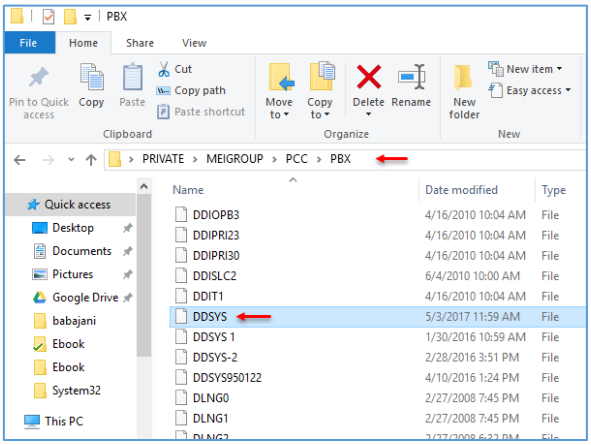
بعد از نصب، نرم‌افزار را اجرا کنید، در شکل روبرو صفحه‌ی اوّلیّه‌ی نرم‌افزار ظاهر می‌شود که به شما دستوراتی را اعلام می‌کند، برای اینکه وارد نرم‌افزار شوید باید از کلمه‌ی INSTALLER استفاده کنید تا دسترسی کامل به تمام اجزای نرم‌افزار را داشته باشید، پس کلمه‌ی INSTALLER را کپی بگیرید و بر روی OK کلیک کنید.



به مانند شکل روبرو، کلمه‌ی INSTALLER را کپی کنید و اگر می‌خواهید این کد در دفعات بعد از شما درخواست نشود، تیک گزینه‌ی Automaticaly Login را انتخاب و بر روی OK کلیک کنید.



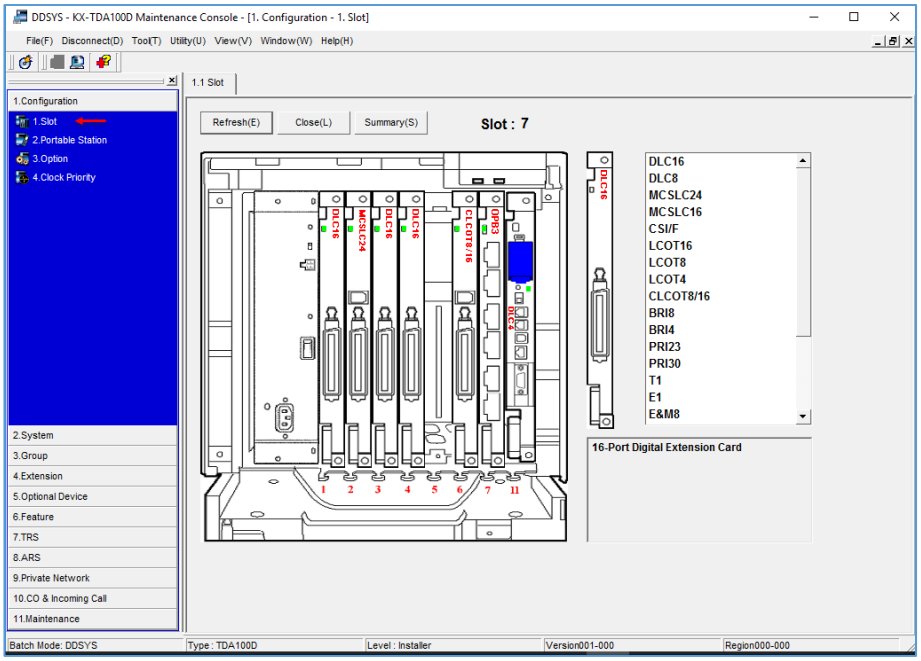
در این صفحه، گزینه‌های مختلفی را مشاهده می‌کنید، برای ارتباط با دستگاه سانترال از طریق کابل Lan، Modem، USB و... باید بر روی گزینه‌ی Connect(C) کلیک کنید، در این قسمت بر فرض اینکه هیچ راه ارتباطی با دستگاه وجود ندارد باید دستگاه را تنظیم کنید، برای این کار باید رم یا همان، حافظه‌ی ذخیره‌سازی آبی‌رنگ که اصولاً، ۱۲۸ مگابایت است را ار دستگاه خارج کنید و بر روی سیستمی که نرم‌افزار را نصب کردید، قرار دهید و در شکل روبرو با کلیک بر روی Open وارد آدرس زیر در رم شوید:



G:\PRIVATE\MEIGROUP\PCC\PBX

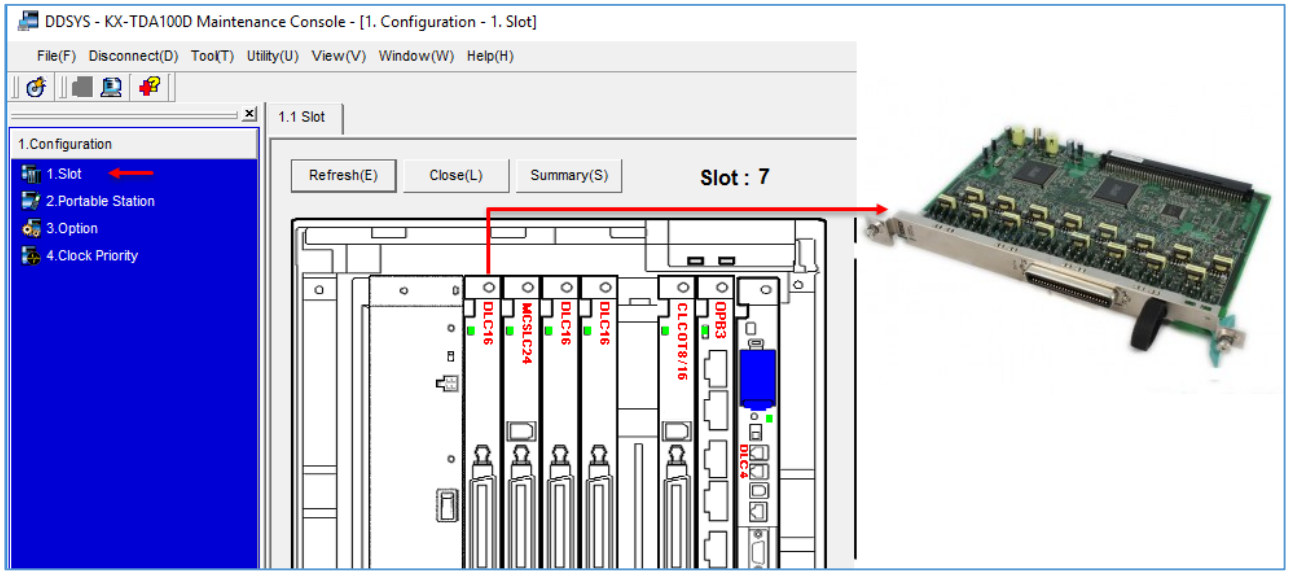
در آدرس بالا، G همان درایو رم است، بعد از ورود به این صفحه، فایل DDSYS را انتخاب و بر روی OK کلیک کنید.

نکته: زمانی که سانترال در حال کار است، اگر رم را خارج کنید، هیچ اتّفاقی برای دستگاه پیش نخواهد آمد و بعد از تغییرات بر روی رم باید آن را بر روی دستگاه قرار دهید و دستگاه را خاموش و روشن کنید. در شکل روبرو، صفحه‌ی مدیریّتی سانترال را مشاهده می‌کنید، اگر از سمت چپ بر روی گزینه‌ی Slot کلیک کنید، همه‌ی کارت‌هایی که بر روی دستگاه قرار داده شده با نام



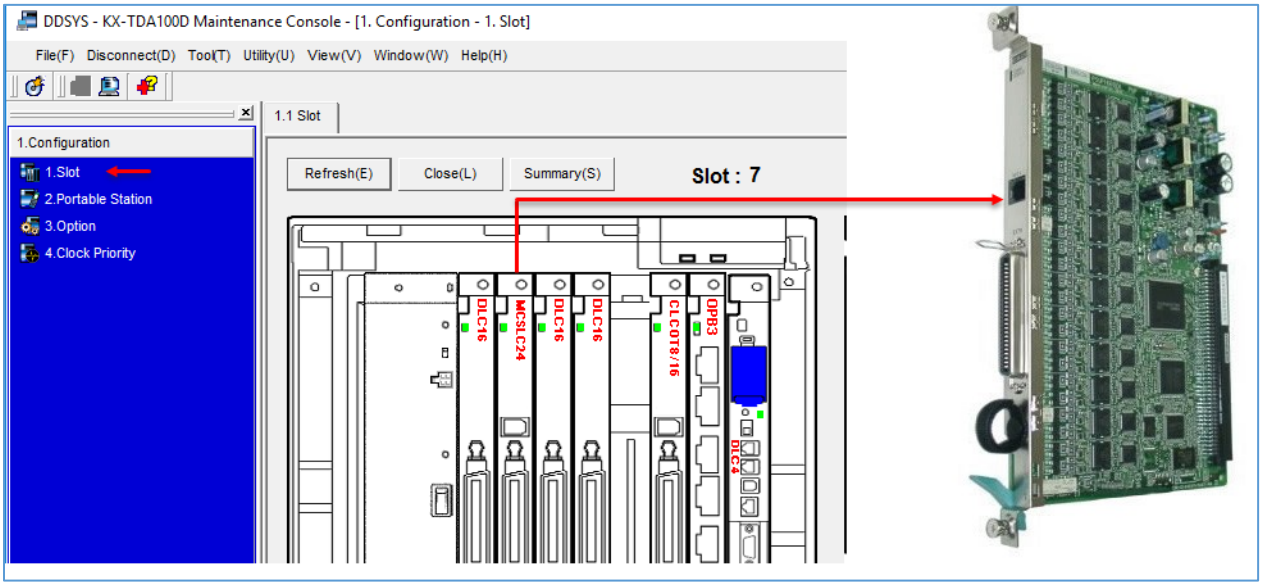
مشخّص شده است که در زیر این کارت‌ها را بررسی می‌کنیم.

کارت DLC16:



به عنوان کارت داخلی ۱۶ تایی دیجیتال مورد استفاده در دستگاه‌های سانترال است، با این کارت می‌توانید تا ۳۶ خطّ داخلی در یک سازمان ایجاد کنید، تمام تلفن‌های سانترال نیز با این کارت کار خواهند کرد.

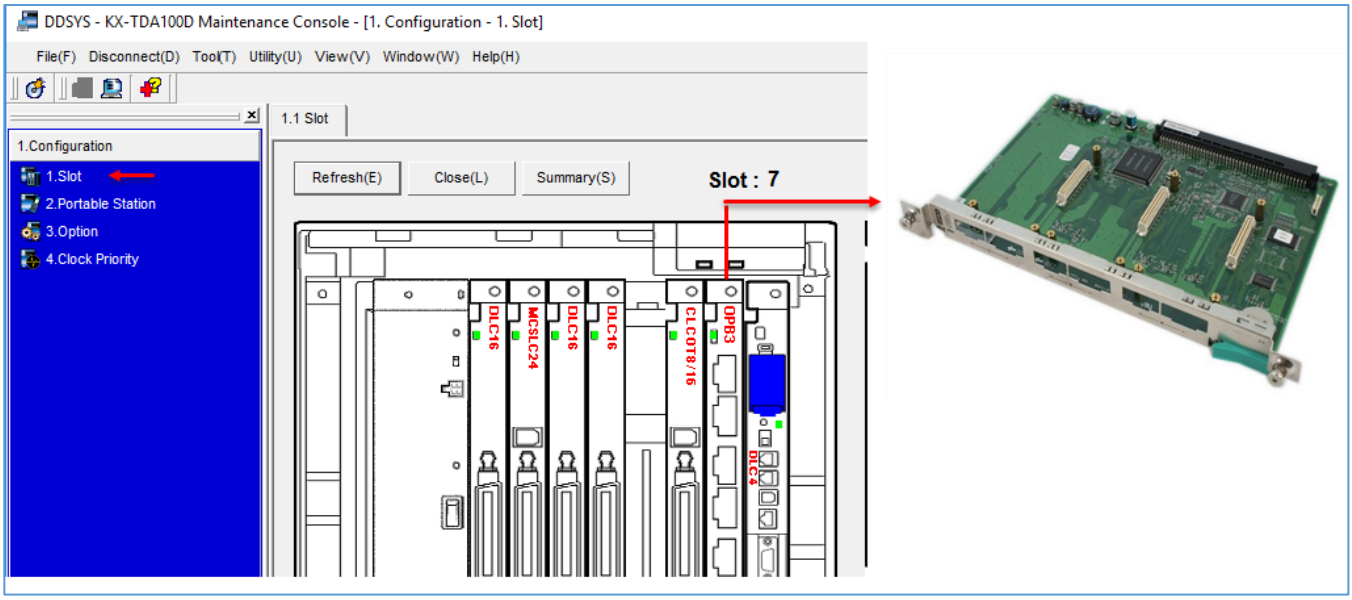
کارت آنالوگ MCSLC24:



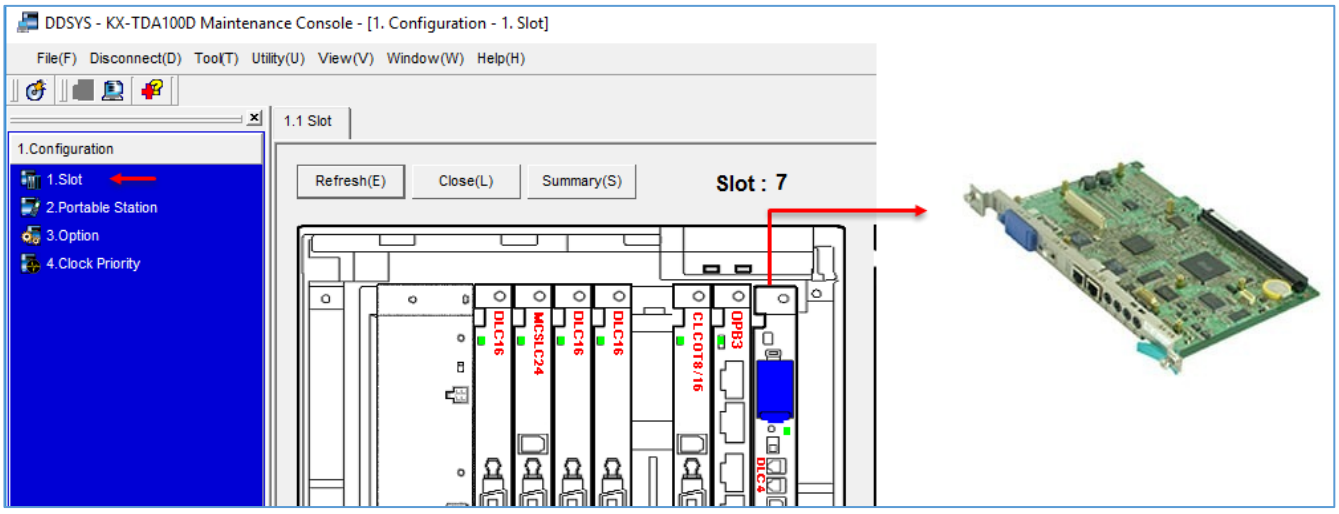
این کارت تا ۲۴ خطّ آنالوگ داخلی را برای یک سازمان فراهم می‌کند و از ویژگی‌های دیگر آن، داشتن Caller ID برای نمایش شماره تماس بر روی تلفن است.

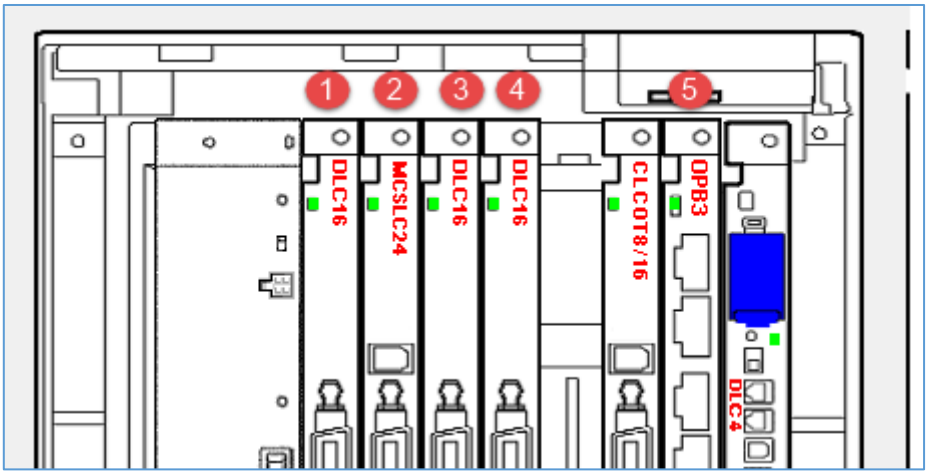
کارت CLCOT8/16:

فراهم کننده‌ی ۱۶ خطّ شهری برای ورود به سانترال است، یعنی اینکه شما می‌توانید ۱۶ خطّ شهری را با استفاده از این کارت وارد سانترال کنید.

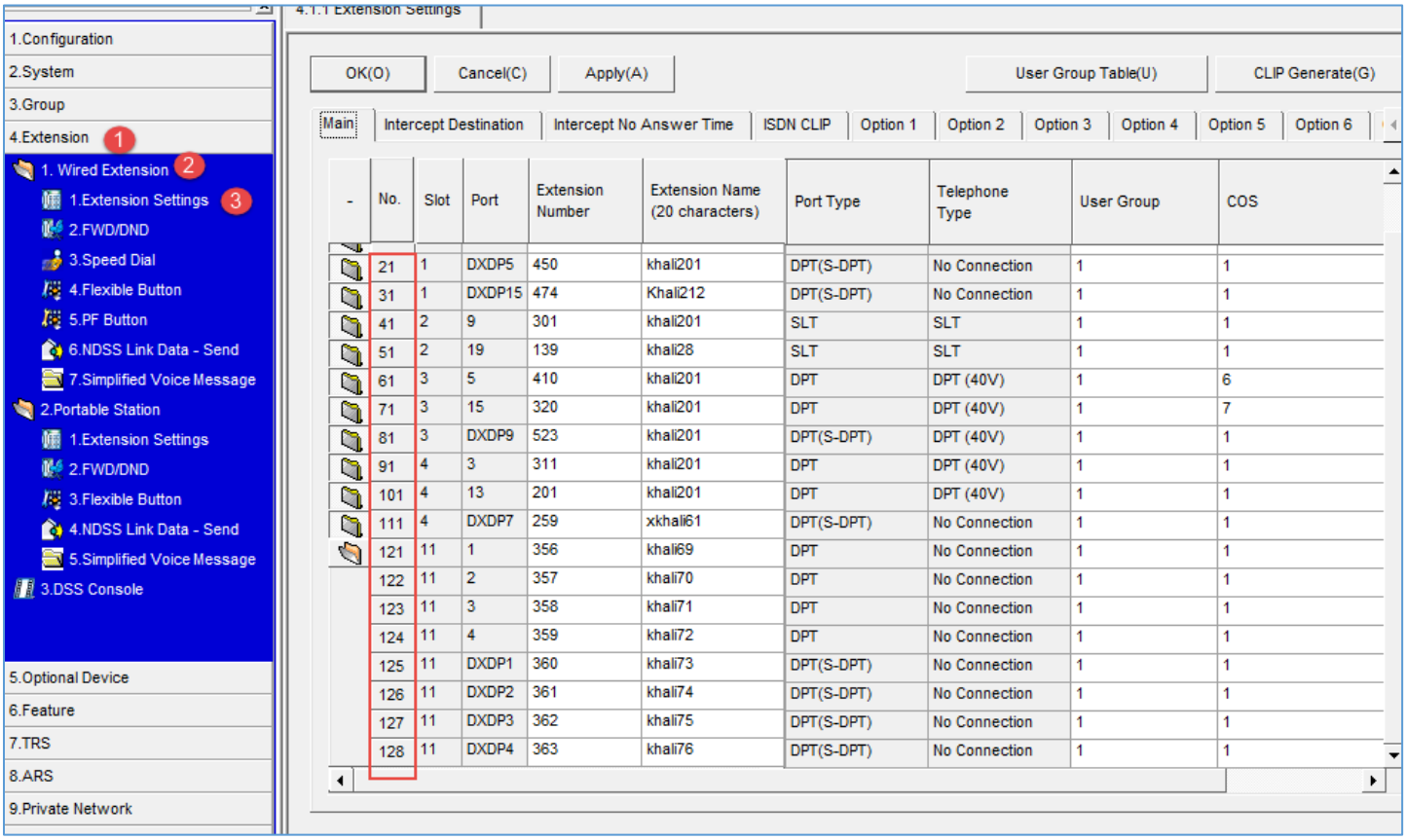


کارت آخر نیز برای ارتباط با سانترال و قرار دادن رم بر روی آن است که در شکل زیر مشخّص شده است.

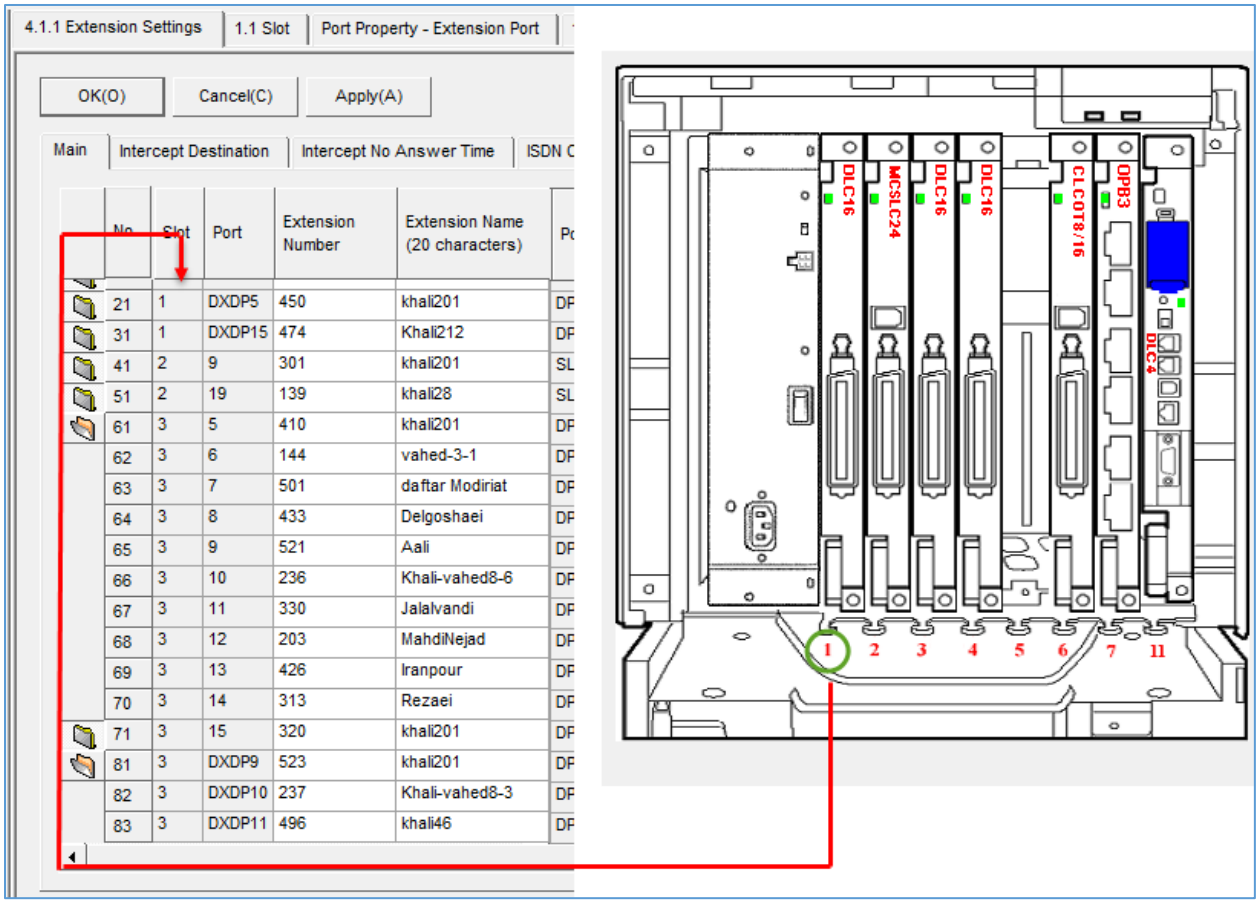




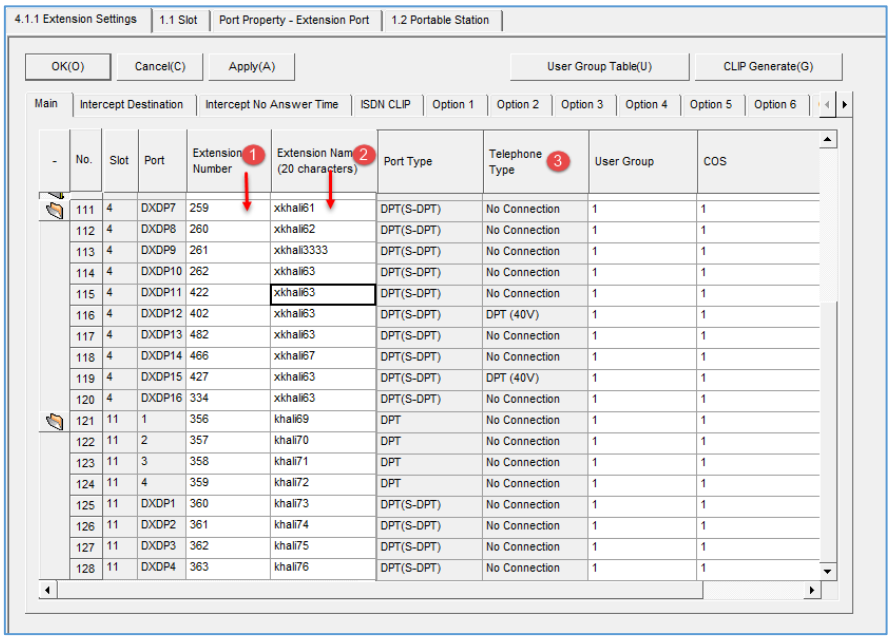
در این دستگاه، پنج کارت وجود دارد که گزینه‌های ۱، ۲ و ۳ دارای ۳۲ خط هستند و شماره‌ی ۲ دارای ۲٤ و شماره‌ی ۵ نیز دارای ۸ خط است که با هم، ۱۲۸ خطّ داخلی هستند.



در صفحه‌ی بالا از سمت چپ طبق شماره، بر روی گزینه‌ی ۱، ۲ و ۳ کلیک کنید، همانطور که مشاهده می‌کنید ۱۲۸ خط برای شما مشخّص شده است که در قسمت **Slot**، شماره‌های کارت مشخّص شده است، این شماره‌ها مربوط به کارت‌های شکل قبلی هستند که تعداد شماره‌های آنها را حساب کردیم.

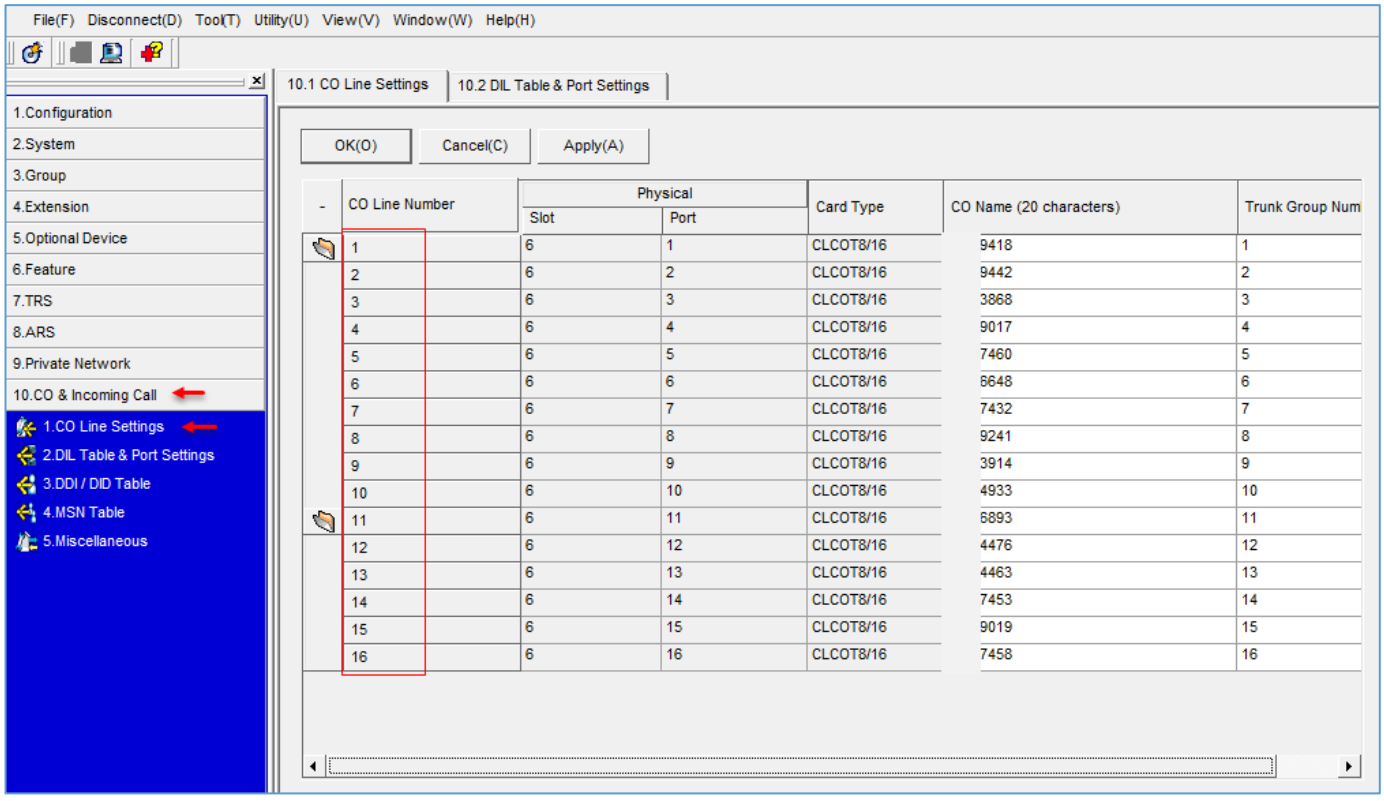


اگر به شکل بالا دقّت کنید، شماره‌ی اسلات هر کارت در صفحه‌ی Slot با شماره‌ی Slot در صفحه‌ی Extentions برابر است و از این طریق می‌توانید متوجّه شوید که این شماره‌ها مربوط به کدام کارت است.

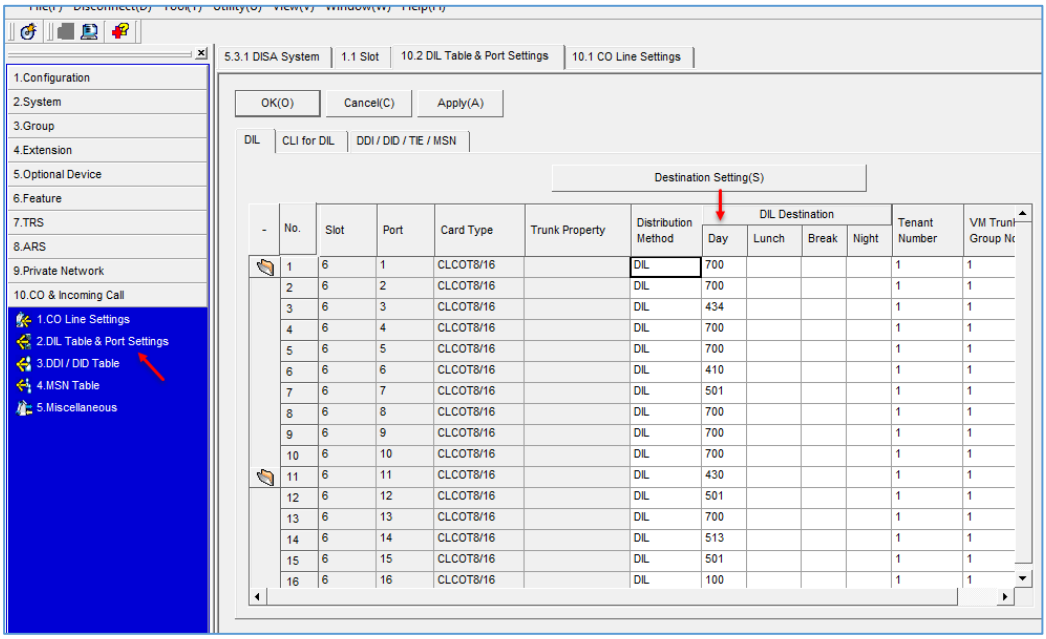


در قسمت Extention، شماره‌هایی برای ستون‌ها مشخّص شده است، در قسمت شماره‌ی یک، اگر در اتاق خود، تلفن را به سانترال متّصل کنید، شماره‌ای در این قسمت بسته به پورت و اسلات قرار می‌گیرد که در قسمت شماره‌ی دو، نام آن نوشته می‌شود، برای اینکه نام شخص را تغییر دهید باید در این قسمت، شماره‌ی آن را پیدا کنید و

می‌توانید شماره و نیز نام آن را تغییر دهید، به این نکته توجّه کنید که شماره‌ها نمی‌توانند یکی باشند، چون بعد از اینکه بر روی OK کلیک کردید با خطا روبرو خواهید شد، در قسمت شماره‌ی سه نیز توع تلفن مشخّص شده است، مثلاً تلفن دیجیتال با گزینه‌ی DPT (40V) و تلفن آنالوگ نیز با نام SLT مشخّص می‌شوند، در ادامه بر روی بقیّه‌ی ستون‌ها کار خواهیم کرد.



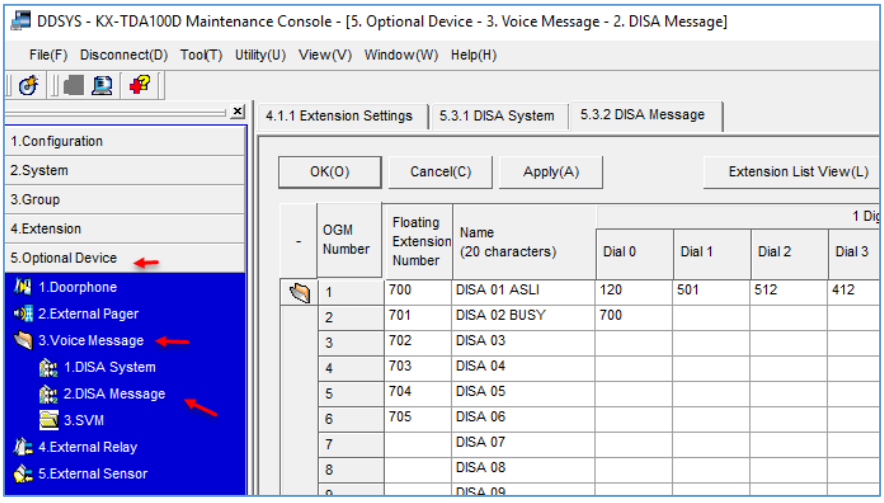
در شکل بالا وارد قسمت CO & Incoming Call شوید و بر روی CO Line Settings کلیک کنید، این قسمت مربوط به کارت CLCOT8/16 است که مربوط به خطّ شهری است که تا ١٦ خط را پشتیبانی می‌کند، در اینجا باید شماره‌ی خط‌ها را طبق ورودی‌ای که در کارت قرار دادید از ١ تا ١٦ وارد کنید.



در قسمت DLI Table & Port Settings می‌توانید هر خطّ ورودی به سانترال را به یک خطّ داخلی متّصل کنید، اگر به شکل روبرو توجّه کنید در ستون Day در مقابل هر خطّ ورودی، یک خطّ داخلی نوشته شده است، مثلاً اگر خط اوّل را از بیرون از سازمان شماره‌گیری کنید، به شماره‌ی ۷۰۰ متّصل می‌شوید، توجّه داشته باشید که در این قسمت می‌توانید مشخّص کنید که چه خط‌هایی به منشی تلفنی و چه خط‌هایی به تلفن داخلی دیگر افراد متّصل شوند، شاید این سؤال به ذهن شما خطور کند که منشی تلفنی چگونه فعّال می‌شود، در مبحث بعدی بر روی این موضوع کار خواهیم کرد.

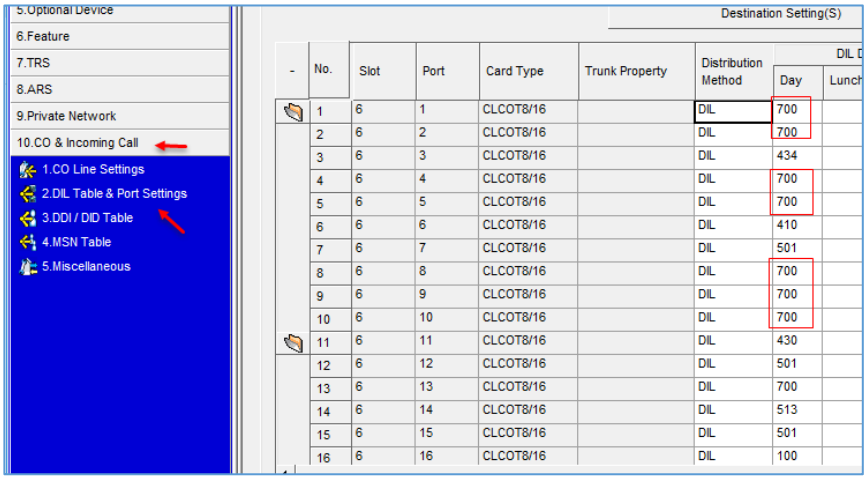
فعّال‌سازی منشی تلفنی در تلفن سانترال:

یکی از ویژگی‌های تلفن‌های سانترال، داشتن منشی تلفنی است که بسیار می‌تواند در مدیریّت تماس‌های ورودی کمک‌کند، سیستم منشی تلفن در سانترال با نام DISA یاد می‌شود.



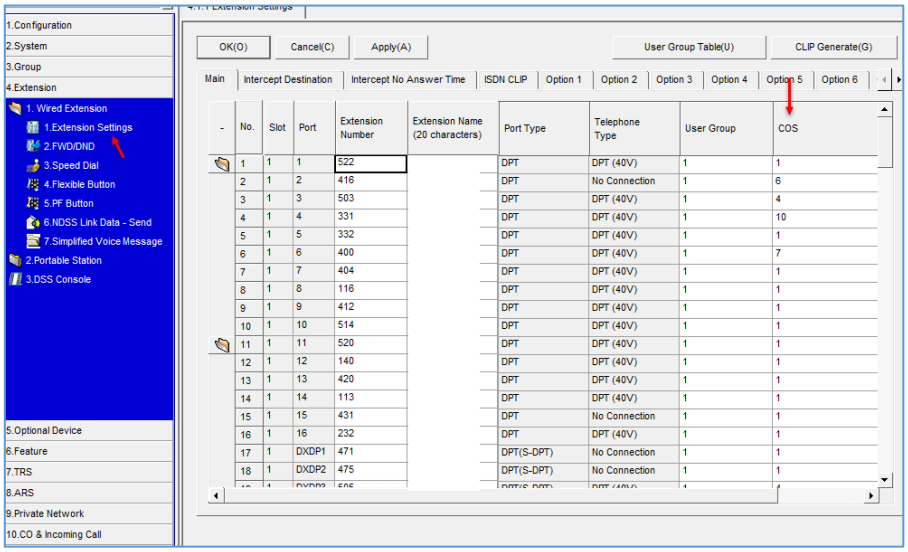
برای ورود به سیستم DISA از سمت چپ بر روی Optional Devices، بعد بر روی Voice Massage و سپس بر روی Disa Message کلیک کنید، در شکل روبرو و در ستون Floating Extension Number، چند عدد از ۷۰۰ تا ۷۰۵ نوشته شده

است که این اعداد برای مراحل منشی تلفنی است، مثلاً در مقابل عدد ۷۰۰ به دلخواه، DISA 01 ASLI نوشته شده است که این همان، DISA است که وقتی از بیرون به شرکت زنگ بزنید، منشی تلفن اجرا می‌شود و شما را به یکی از شماره‌های روبرو ارجاع می‌دهد، در مقابل آن، چند ستون از Dial0، Dial1، Dial2، Dial3 و... قرار دارد و در زیر آنها، یک شماره‌ی داخلی قرار داده شده است؛ در منشی تلفنی، زمانی که منشی صحبت می‌کند و می‌گوید، مثلاً با کلیک بر روی عدد ۱ وارد قسمت مالی شوید، عدد یک، همان داخلی ۵۰۱ که مربوط به ستون Dial1 است، می‌باشد و کاربر با گرفتن این شماره به داخلی مورد نظر متّصل می‌شود، توجّه داشته باشید اگر کاربر شماره‌ای را انتخاب نکند به داخلی اوّل، یعنی شماره‌ی ۱۲۰ متّصل می‌شود.



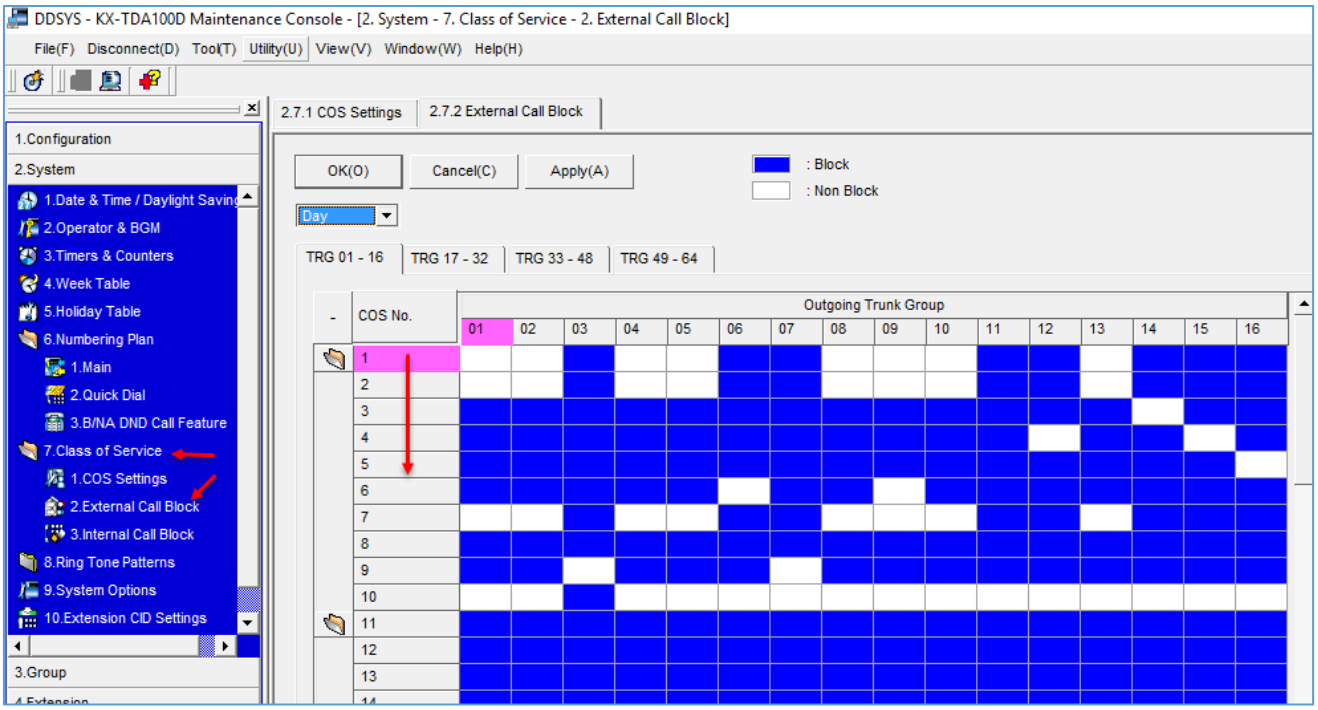
دوباره وارد قسمت CO & Incoming Call شوید و بر روی CO Line Settings کلیک کنید، همانطور که مشاهده می‌کنید در مقابل بعضی از شماره‌های ورودی، عدد ۷۰۰ نوشته شده است، این بدان معنا است که کسانی که با این شماره‌ها از بیرون به سازمان زنگ می‌زنند، مستقیم به منشی تلفنی متّصل می‌شوند.

مشخّص کردن تعداد خطهای آزاد برای کاربر:

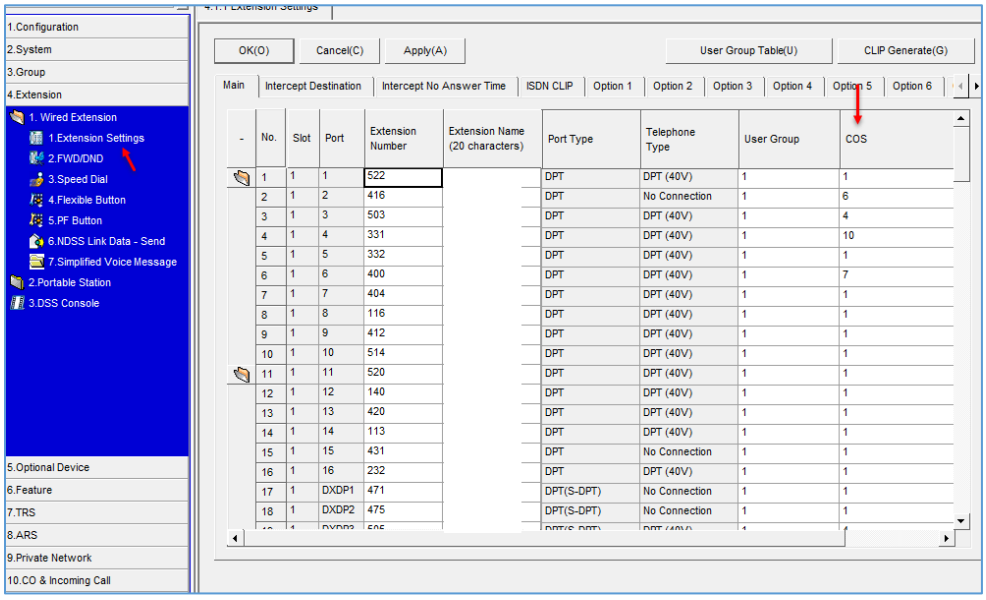


در قسمت Extension Settings، ستونی با نام COS وجود دارد، این اعداد مربوط به تعداد خطهای آزادی است که به شماره خطهای داخلی داده خواهد شد، این بدان معنا است که کاربری که پشت میز خود نشسته است، آیا اجازه دارد با بیرون از سازمان

تماس بگیرد یا نه، در این قسمت این موضوع را بررسی می‌کنیم.



در شکل بالا وارد Class of Service و بعد، External Call Block شوید، در این صفحه شما می‌توانید چند گروه ایجاد کنید و مشخّص کنید که مثلاً، داخلی‌هایی که در گروه یک قرار دارند، می‌توانند به خط‌های شهری یا همان، خطّ آزاد دسترسی داشته باشند؛ در سطر یک، ١٦ خط را مشاهده می‌کنید که خطّ ١، ٢، ٤، ٥، ٨، ٩، ١٠ و ١٣ آن انتخاب و آزاد شده است، اگر کاربر در این گروه قرار بگیرد، می‌تواند به تمام این خط‌ها دسترسی داشته باشد.



دوباره به شکل قبلی باز گردید، اگر توجّه کنید در قسمت COS، شماره‌هایی که در COS Setting مشخّص کردید وارد شده است، مثلاً شماره‌ی داخلی ٥٢٢ در گروه شماره‌ی یک قرار دارد و به خط‌های بالا دسترسی دارد.

مدیریّت پورت‌ها و بستن آنها در شبکه:

یکی از قویترین و بهترین روش‌ها در امنیّت اطّلاعات یک سازمان، بستن پورت‌هایی، مانند پورت USB، CD-Rom و... است که این روش می‌تواند کمک زیادی در حفظ امنیّت یک شبکه باشد.

نرم‌افزار GFI EndPoint Security در شبکه‌های متوسّط و بزرگ مورد استفاده قرار می‌گیرد و نظارت کاملی بر همه‌ی تجهیزات متّصل‌شده به کامپیوتر را دارد.

با این نرم‌افزار می‌توانید مدیریّت و نظارت کاملی بر نحوه‌ی عملکرد Portable Device (به خصوص فلش درایوها)، سی دی درایوها، فلاپی درایوها، اسکنرها، پرینترها و سریال پورت‌ها داشته باشید و مانع از دسترسی غیر مجاز کاربران به اطّلاعات داخل شبکه‌ی خود شوید.

با استفاده از GFI EndPoint Security می‌توانید اطّلاعات درون فلش دیسک‌ها را Encrypt کنید و به کاربران اجازه دهید، تنها فایل با پسوند مشخّصی را بر روی فلش درایو خود کپی کنند.

از ویژگی‌های موجود در نرم‌افزار GFI EndPoint Security، کنترل دسترسی کاربران برای حفاظت از شبکه، دسترسی به حافظه‌های ذخیره‌سازی اطّلاعات، ارائه‌ی گزارش از فعّالیّت‌های حافظه‌های جانبی متّصل‌شده به سیستم، مانند USB Flash ها، سازگاری با پیکره‌بندی Active Directory ، نظارت مداوم واقعی بر سیستم و نمایش هشدار در صورت بروز مشکل، دادن دسترسی زمانی به یک Device خاص و قرار دادن گروه خاصّی از سخت‌افزارها در White List و Blacklist است.

برای دانلود نرم‌افزار GFI EndPoint Security از لینک زیر استفاده کنید:

http://dl.fileniko.com/f/2014/04/GFI.End.Point.Security.6.0.Build.20130719.www.fileniko.com.rar

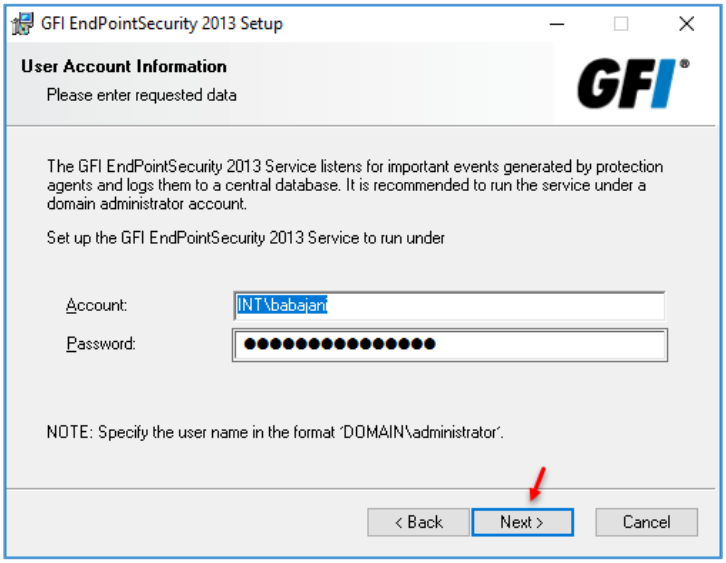


بعد از نصب بر روی فایل Setup کلیک کنید، توجّه داشته باشید، قبل از هر کاری اینترنت را بر روی سیستم خود قطع کنید.

در این صفحه بر روی Next کلیک کنید.

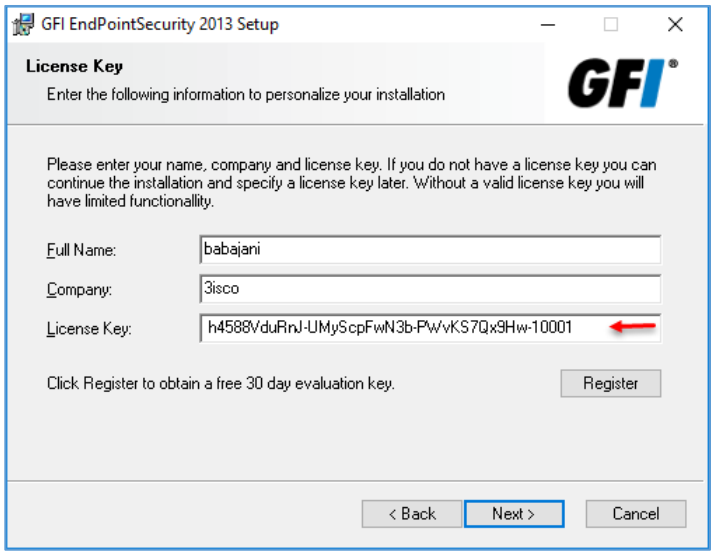


در این صفحه، گزینه‌ی مورد نظر را انتخاب و بر روی Next کلیک کنید.



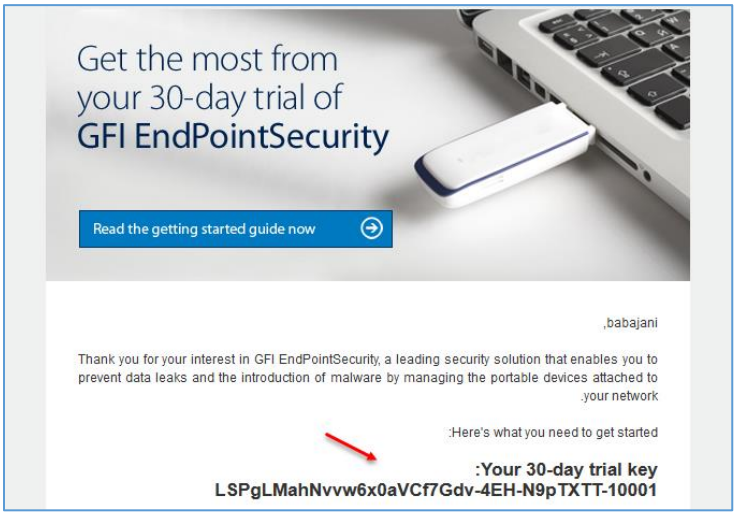
در این صفحه باید یک کاربر به همراه رمز عبور آن وارد کنید که در شبکه دسترسی کامل داشته باشد، نرم‌افزار از طریق این کاربر بر روی سیستم‌ها، Agent نصب خواهد کرد و کلاینت کاربر را در دست خواهد گرفت.

بر روی Next کلیک کنید.



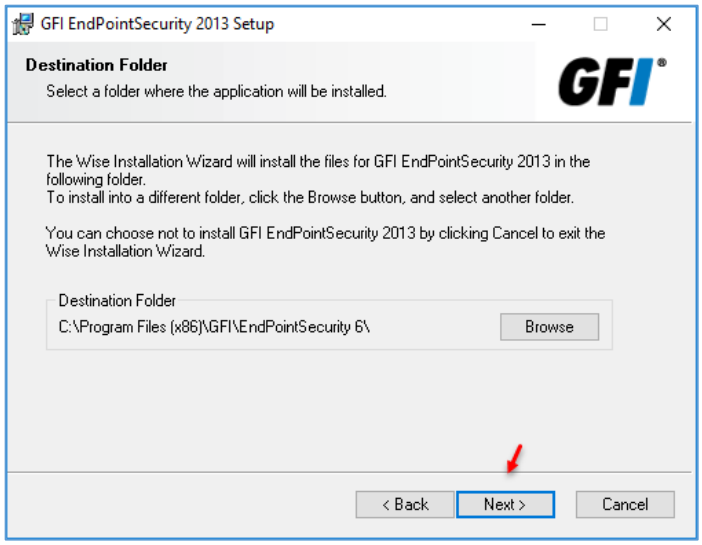
در این قسمت باید لایسنس Trial که ۳۰ روزه است را وارد کنید، توجّه داشته باشید این لایسنس را می‌توانید از خود سایت نرم‌افزار و از آدرس زیر دریافت نمایید:

https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-endpointsecurity/download

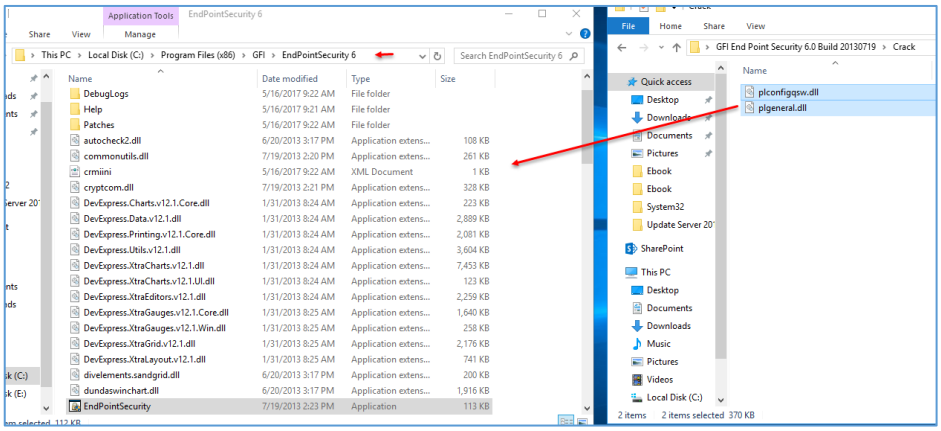


بعد از ورود به سایت، اطّلاعات خود را وارد و بعد از تأیید، نرم‌افزار به همراه لایسنس به شما نمایش داده می‌شود، البتّه این لایسنس به ایمیل شما ارسال خواهد شد.

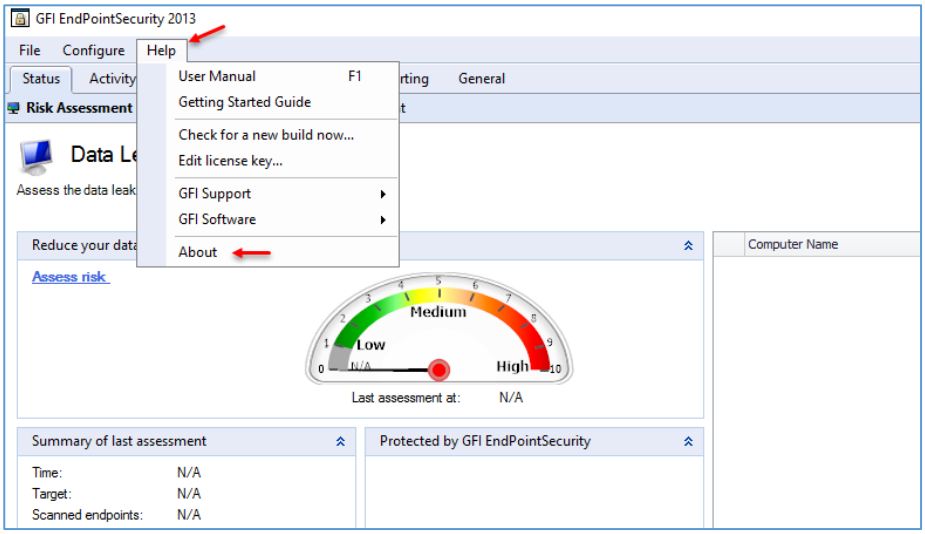
در شکل روبرو لایسنس را مشاهده می‌کنید که به ایمیل ارسال شده است.



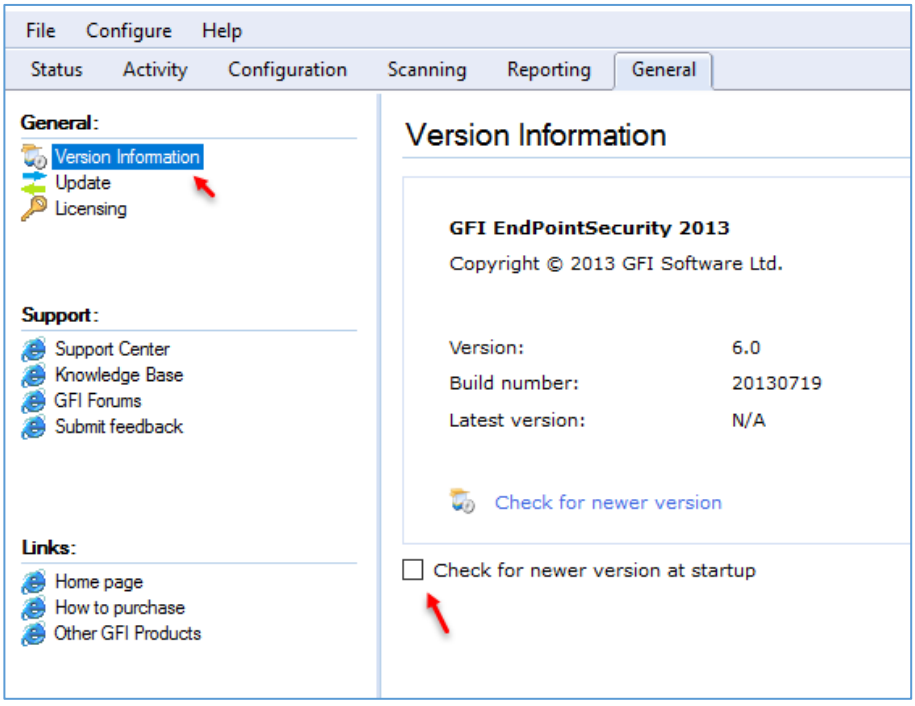
در این صفحه می‌توانید مسیر نصب نرم‌افزار را مشخّص و بر روی Next کلیک کنید.



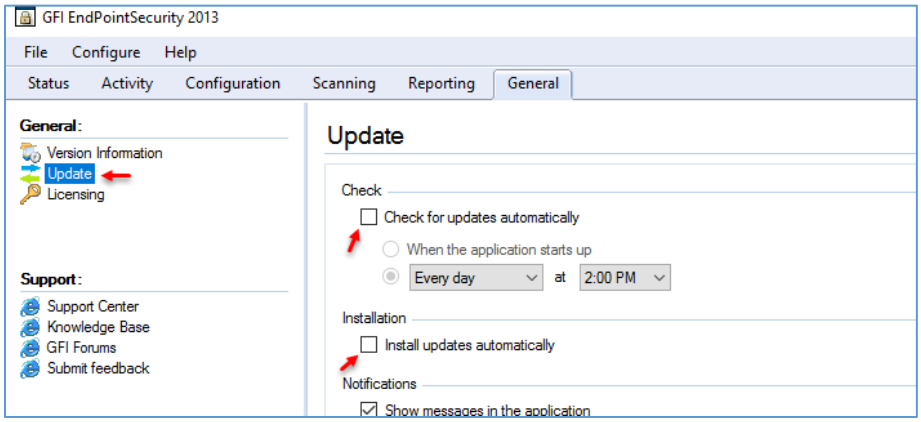
بعد از نصب کامل نرم‌افزار، آن را اجرا نکنید، بعد از آن، اگر تمایل دارید که نرم‌افزار را کرک کنید، به مانند شکل روبرو وارد پوشه‌ی کرک شوید و دو فایل را در مسیر نصب نرم‌افزار کپی کنید، بعد از آن می توانید نرم‌افزار را اجرا کنید.



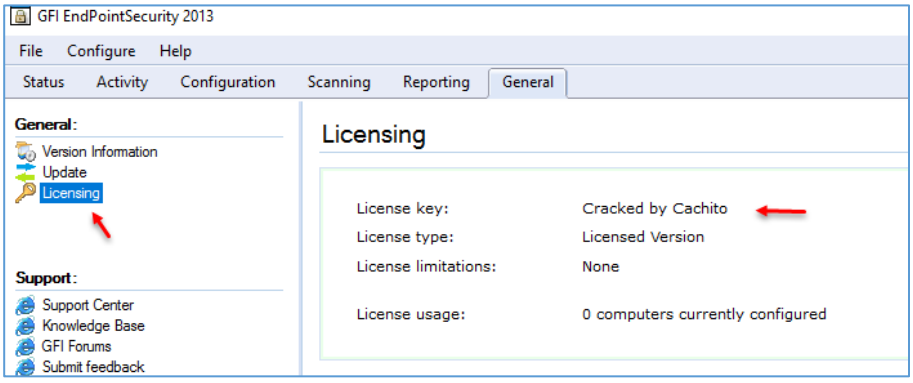
همانطور که مشاهده می‌کنید، نرم-افزار مورد نظر اجرا شده است و برای اینکه تنظیمات آپدیت آن را انجام دهید بر روی Help کلیک کنید و در منوی باز شده بر روی About کلیک کنید.



در این صفحه، اگر چنانچه نرم‌افزار را کرک کردید، تیک گزینه‌ی Check for newer version at startup را بردارید تا نرم‌افزار، خود را آپدیت نکند.



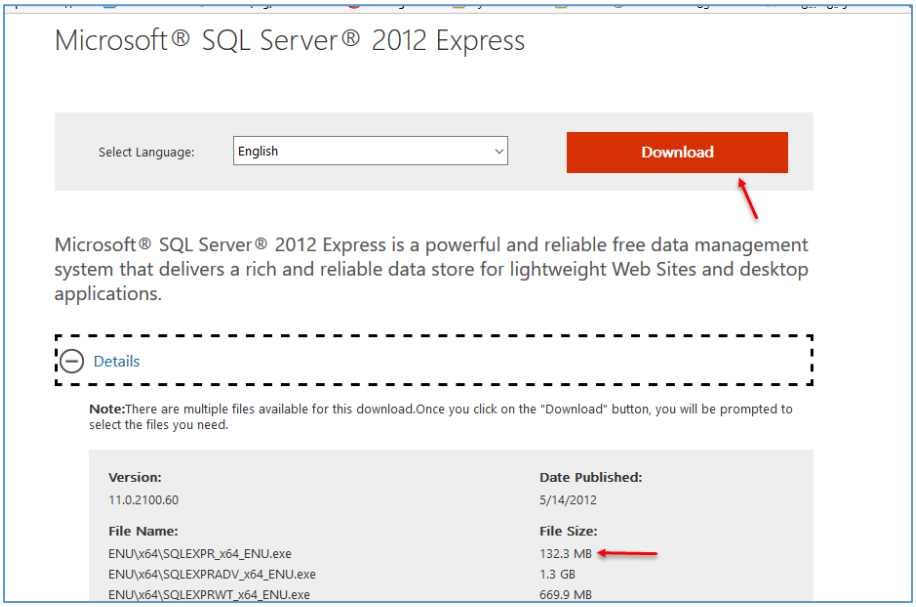
در این صفحه و در قسمت Update، تیک هر دو گزینه را بردارید.



در قسمت لایسنس باید گزینه‌های روبرو را مشاهده کنید تا نرم‌افزار بعد از ۳۰ روز از کار نیفتد.

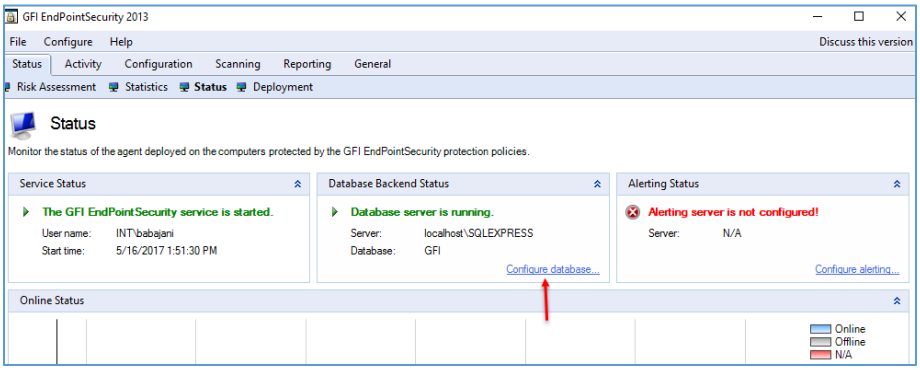
برای اینکه تنظیمات نرم‌افزار GFI را کامل کنید، نیاز به نرم‌افزار SQL دارید تا با استفاده از دیتابیسی که نرم‌افزار GFI در SQL ایجاد می‌کند، تنظیمات خود را تکمیل کنید، برای دانلود SQL از لینک زیر می‌توانید استفاده کنید:

https://www.microsoft.com/en-us/download/details.aspx?id=29062

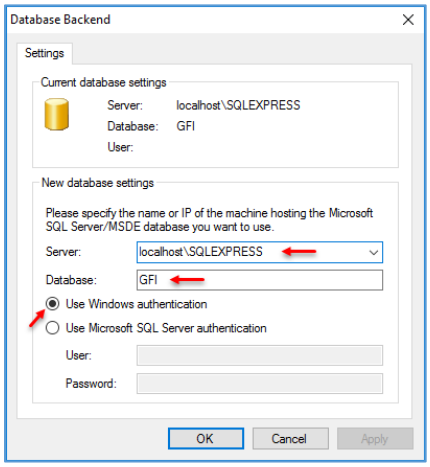


در صفحه‌ی دانلود و بعد از کلیک بر روی Download، تنها گزینه‌ی ۱۳۲,۳ مگابایتی را از لیست، انتخاب و دانلود کنید.

نصب این نرم‌افزار را در قسمت‌های قبلی کتاب و در راه‌اندازی سرویس Remote Desktop توضیح دادیم.

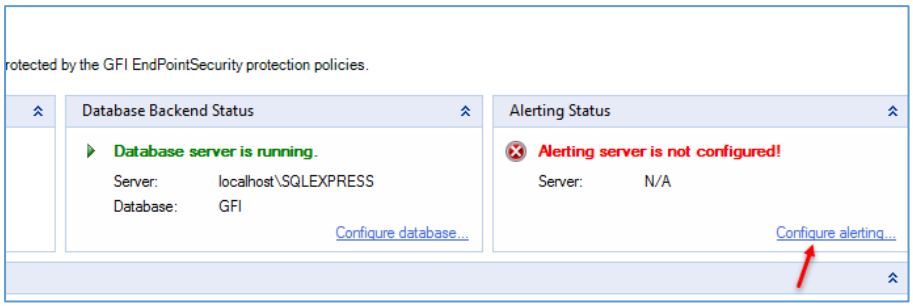


برای تنظیم دیتابیس وارد تب Satus شوید و بر روی Configure database کلیک کنید، توجّه کنید در شکل روبرو از قبل این کار را انجام دادیم، امّا برای آموزش، یک بار دیگر این موضوع را بررسی می کنیم.

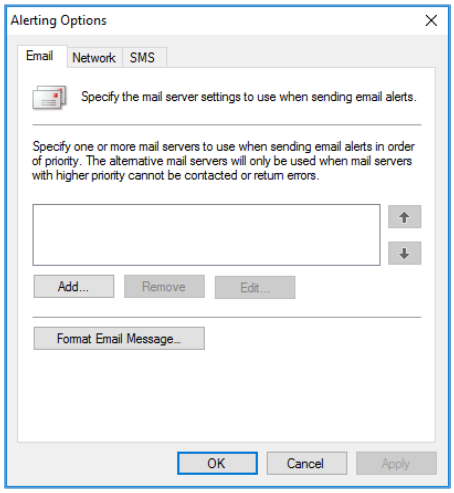


در این صفحه باید در قسمت سرور، اوّل نام سرور و بعد از آن، نام Distance وارد کنید، البتّه اگر نرم‌افزار بالایی را دانلود کرده باشید، همان SQLEXPRESS است، مانند SQL\SQLEXPRESS که در این نوشته، SQL، نام سرور و SQLEXPRESS، نام Distance است، در قسمت Database نیز یک نام به دلخواه خود وارد کنید.

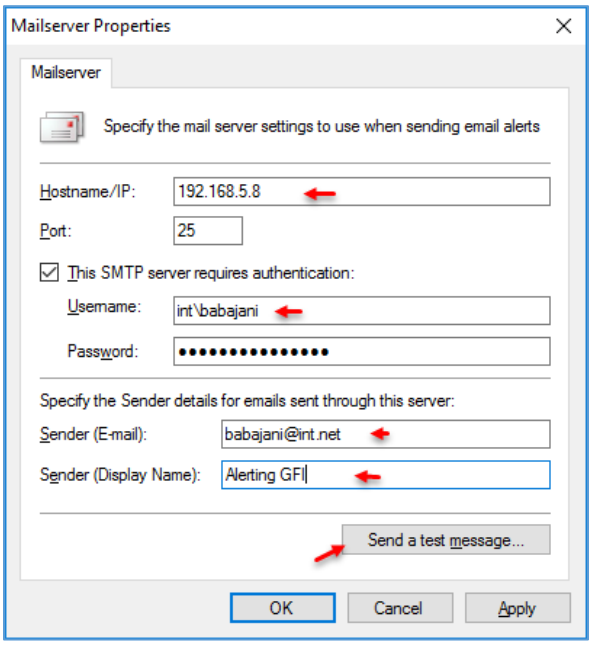
در قسمت آخر نیز باید نوع تأیید هویّت خود را مشخّص کنید و بر روی OK کلیک کنید.



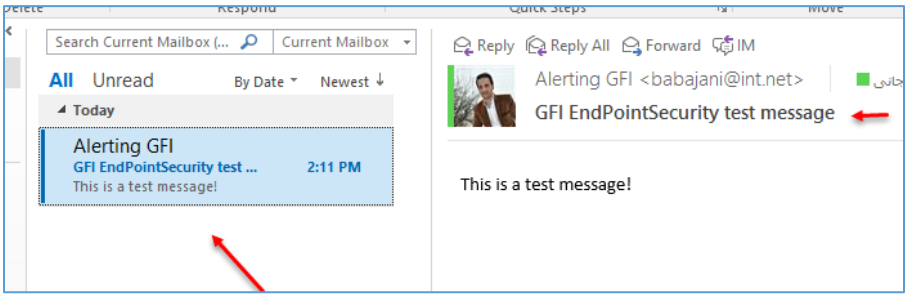
به مانند شکل روبرو باید دیتابیس شما ایجاد و وضعیّت کار سبز شده باشد، برای تنظیم Alert بر روی Configure alerting کلیک کنید.



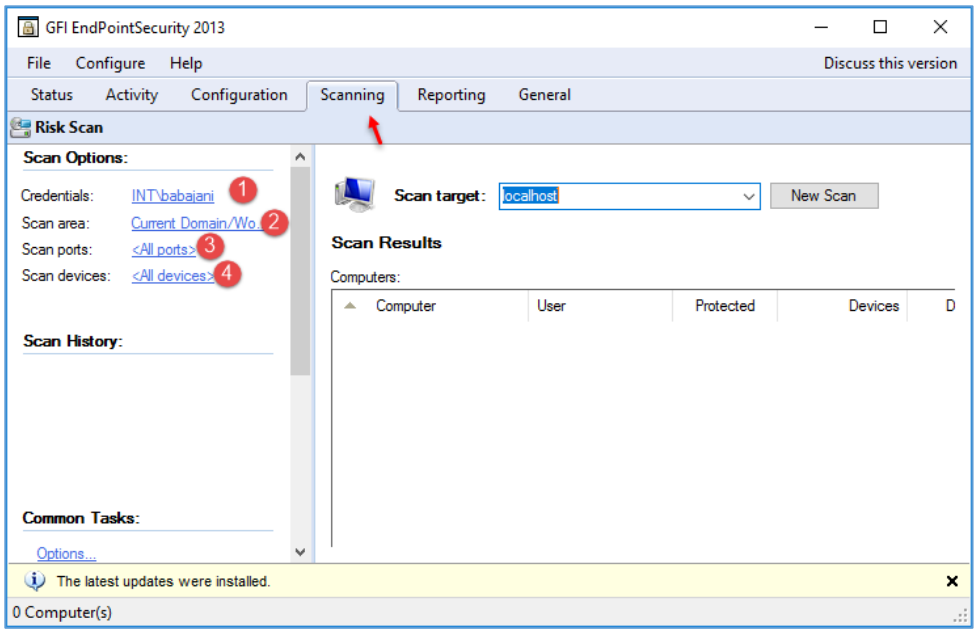
در این قسمت، اگر از سرور ایمیل خاصّی استفاده می‌کنید، می‌توانید اطّلاعات آن را به نرم‌افزار اضافه کنید، برای این کار بر روی Add کلیک کنید.



در این صفحه باید نام یا آدرس سرور ایمیل خود را در قسمت Hostname/IP وارد کنید که پورت پیش‌فرض آن، ۲۵ است که اگر از پورت‌های دیگری استفاده می‌کنید باید پورت آن را به عدد مورد نظر تغییر دهید، در قسمت دوّم، یک نام کاربری وارد کنید که دسترسی لازم را به سرور ایمیل داشته باشد، در قسمت آخر نیز باید فرستنده‌ی ایمیل را به همراه موضوع ایمیل وارد کنید و اگر می‌خواهید تنظیمات انجام داده‌ی خود را تست بگیرید باید بر روی Send a test message کلیک کنید.

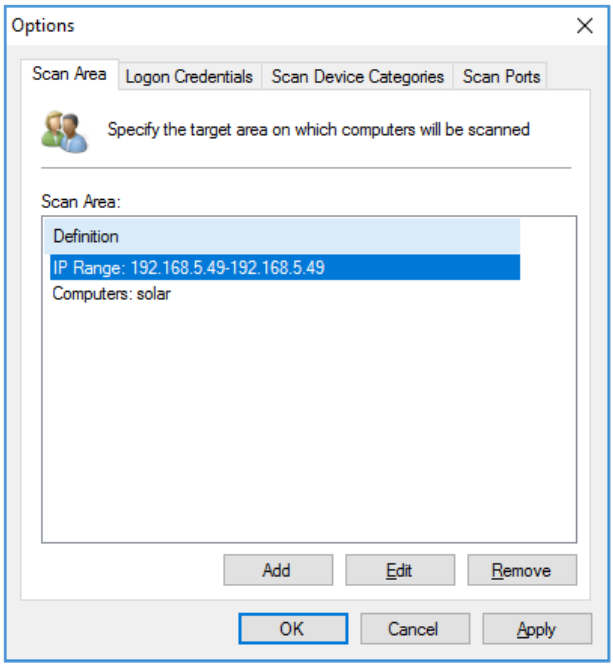


همانطور که مشاهده می‌کنید، ایمیل مورد نظر از نرم‌افزار GFI به سرور ایمیل ارسال شده است.

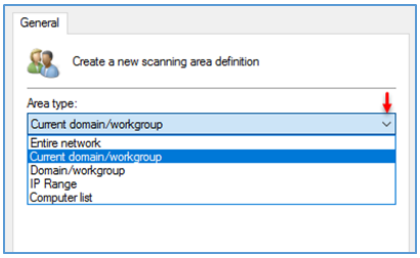


برای تست کار وارد قسمت Scanning شوید که مربوط به اسکن اطّلاعات شبکه است، در این صفحه از سمت چپ، چهار گزینه وجود دارد که با هم بررسی می‌کنیم.

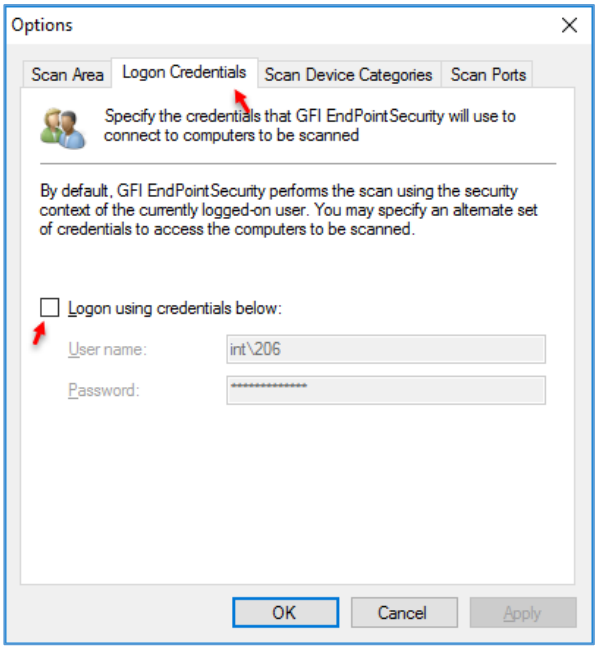
بر روی یکی از گزینه‌ها کلیک کنید.



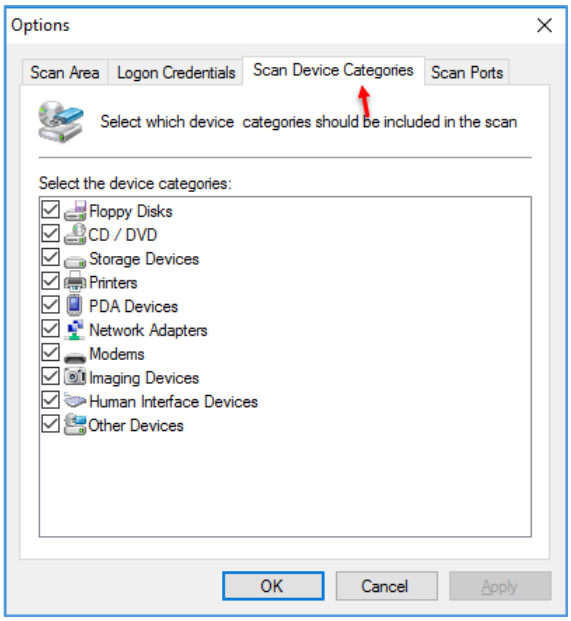
در این صفحه و در تب Scan Area شما با کلیک بر روی Add که پنجره‌ی زیر باز می‌شود، می‌توانید مشخّص کنید که باید کدام قسمت از شبکه یا کدام آدرس و اسم بررسی شود و تنظیمات بر روی آن اعمال شود.



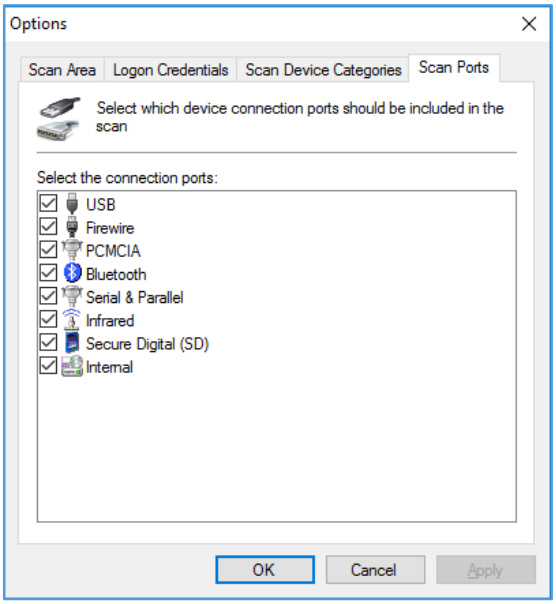
در شکل روبرو یک رنج IP و یک اسم سرور مشخّص شده است، البتّه اگر بخواهید کلّ شبکه را چه از نظر دومین و چه از نظر WorkGroup بررسی کنید باید در پنجره‌ی Add، گزینه‌ی Current domain/Workgroup را انتخاب کنید، به این نکته نیز توجّه کنید که بهتر است، برای تست، به مانند بالا، تنها یک کلاینت را به صورت تستی انتخاب کنید و بعد از اینکه کاملاً بر روی نرم‌افزار تسلّط پیدا کردید، کلّ شبکه را با نرم‌افزار درگیر کنید.



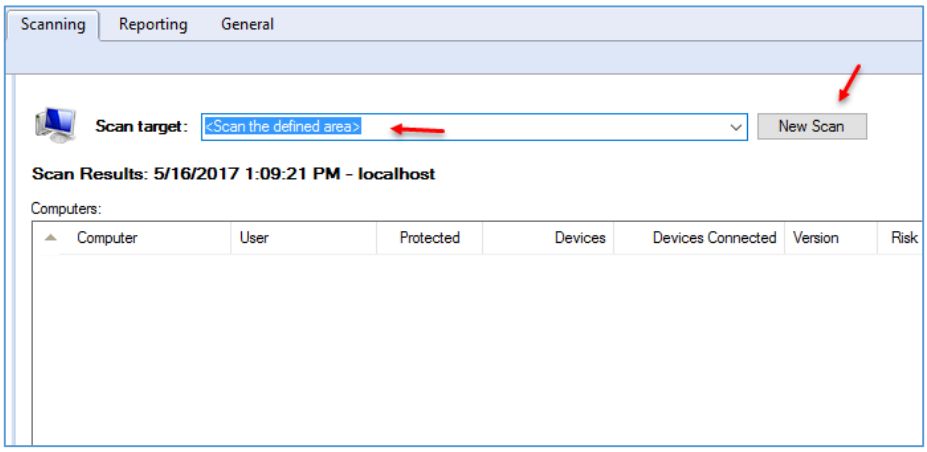
در تب Logon Cerdentials می‌توانید یک کاربر با دسترسی کامل را معرّفی کنید تا در ورود به سیستم‌ها و دسترسی به آنها با مشکل مواجه نشوید، البتّه اگر در هنگام نصب یک کاربر با دسترسی کامل معرّفی کردید که دیگر نیازی به این کار نیست.



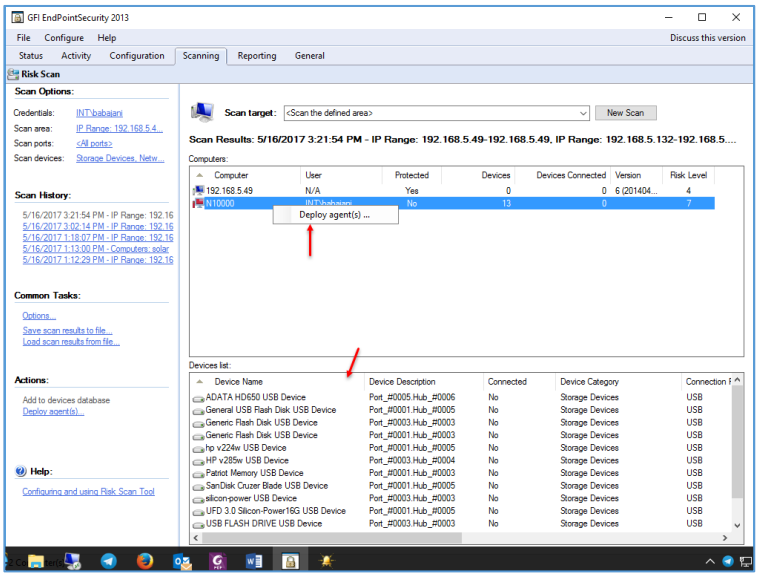
در تب Scan Device Categories می‌توانید دسته‌های خود را برای بررسی مشخّص کنید، مثلاً برای راحتی کار، بهتر است گزینه‌هایی را از لیست خارج کنید، مانند پرینتر، مودم و....



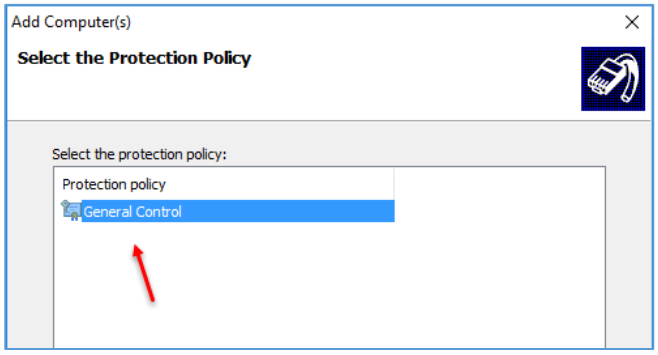
در این صفحه می‌توانید پورت خاصّ خود را که قرار است، اسکن شود را انتخاب و بقیّه را غیر فعّال کنید.



بعد از انجام تنظیمات بالا در تب Scanning بر روی New Scan کلیک کنید، توجّه داشته باشید که از لیست کشویی، گزینه‌ی Scan the defined area را انتخاب کرده باشید.

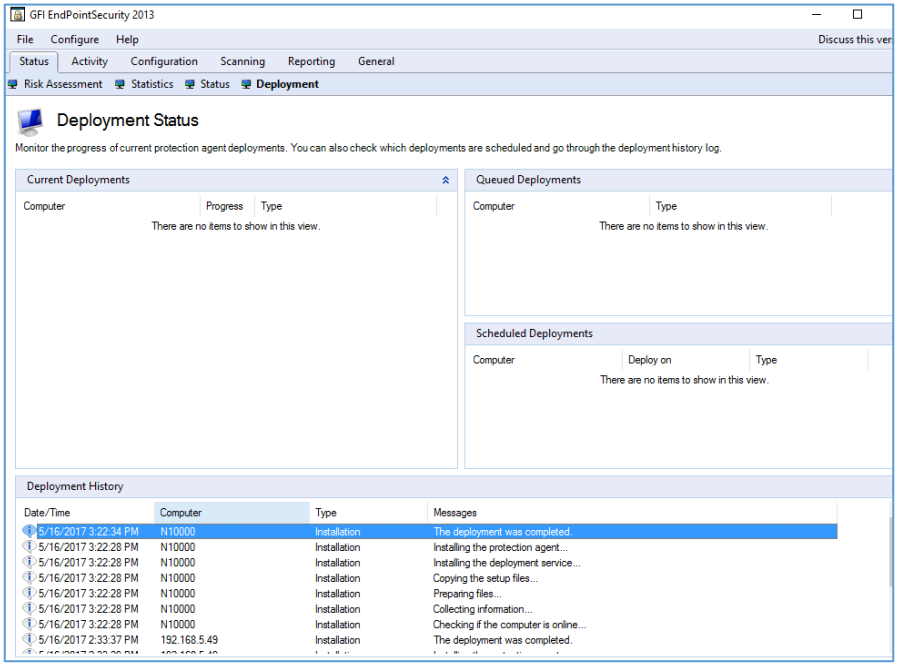


همانطور که مشاهده می‌کنید، یک سیستم N10000 پیدا شده است، بعد از اینکه کلاینت یا سرور مورد نظر وارد لیست شد باید بر روی آن کلیک راست کنید و گزینه‌ی Deploy Agent را انتخاب کنید، در شکل روبرو تمام دستگاه‌هایی که به این سیستم متّصل شده است، مشخّص شده است.

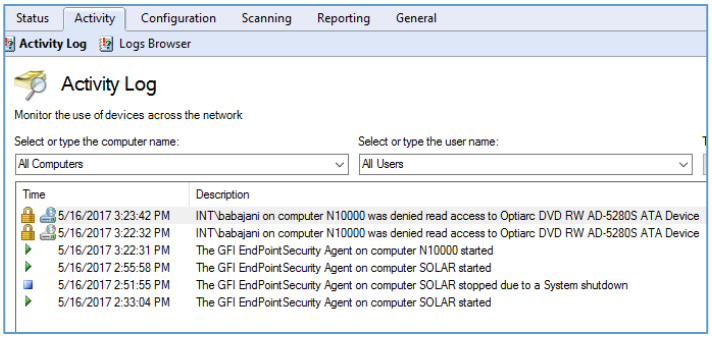


در این قسمت باید Policy های مشخّص‌شده را انتخاب کنید، به صورت پیش‌فرض، یک policy با نام General Control وجود دارد که یک‌سری تنظیمات بر روی آن انجام شده است، مانند تعداد پورت‌های قابل بررسی و...؛ در ادامه، در مورد این موضوع بحث خواهیم کرد.

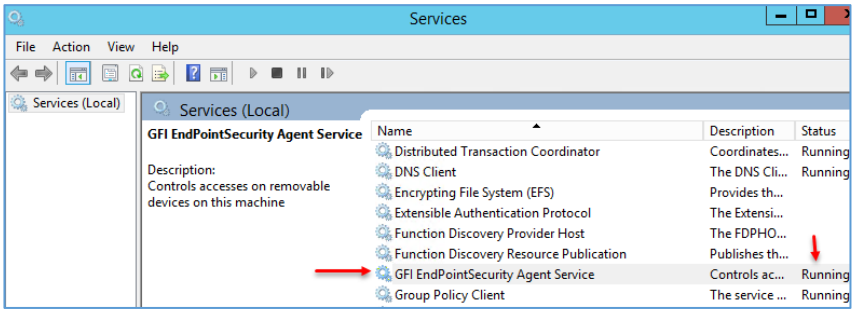
بر روی Finish کلیک کنید.



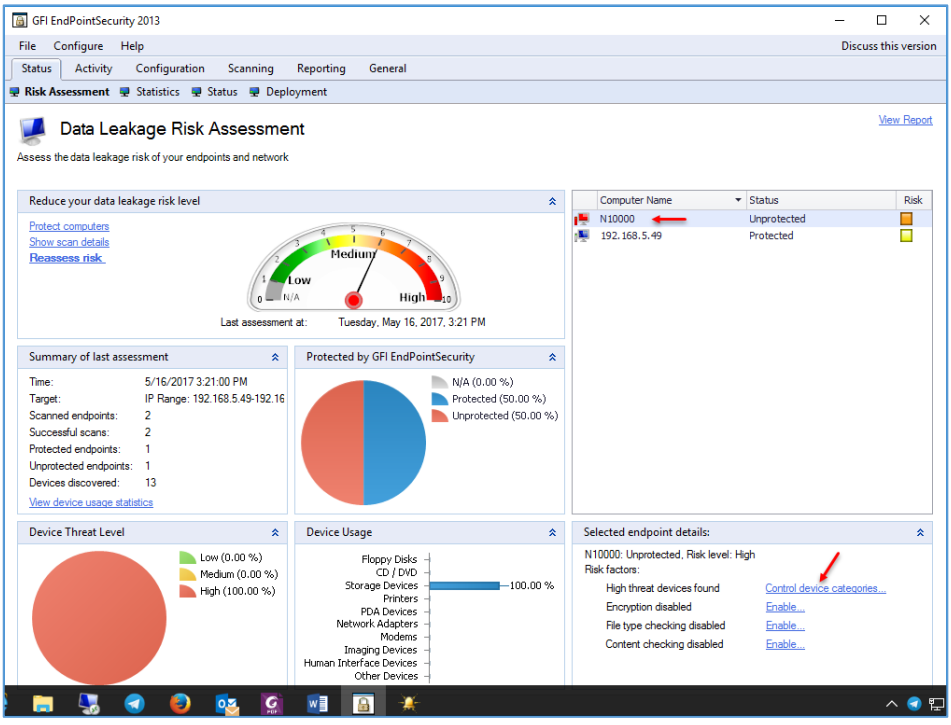
بعد از کلیک بر روی Finish، عملیّات نصب Agent بر روی سرور انجام خواهد شد و شما به صفحه‌ی Deployment ارجاع داده خواهید شد، اگر به پایین صفحه نگاه کنید، تمام مراحل نصب Agent در زیر مشخّص شده است و Agent، بدون مشکل بر روی سرور یا کلاینت نصب شده است.



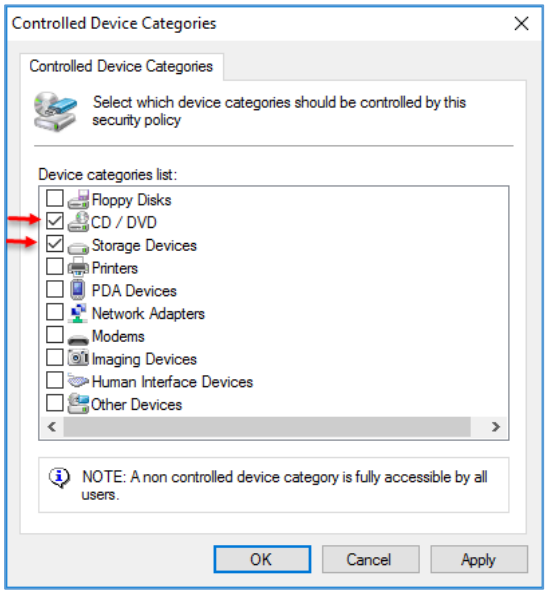
اگر وارد تب Activity شوید، مشاهده خواهید کرد که در تاریخ و ساعت مشخّص، نرم‌افزار Agent بر روی همان سرور که نام آن، N10000 نوشته شده، نصب شده است.



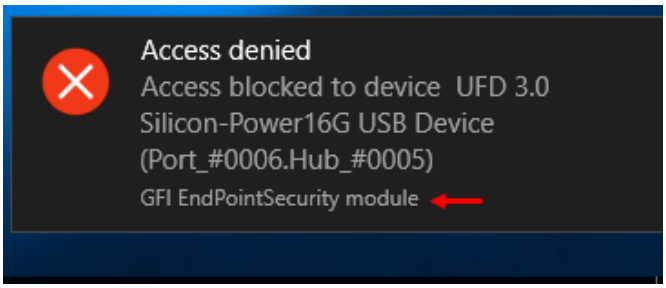
در اینجا وارد سروری می‌شویم که Agent بر روی آن نصب شده است، اگر وارد Services شوید، سرویس GFI را مشاهده می‌کنید که در حال کار است.



در تب Status وارد قسمت Risk Assessment شوید، در این قسمت به شما اعلام می‌دارد که شبکه‌ی شما در چه وضعیّتی قرار دارد، در حال حاضر وضعیّت کار، Unprotected است و هنوز در حالت نرمال قرار ندارد، در پایین صفحه بر روی گزینه‌ی Control device categoris کلیک کنید.



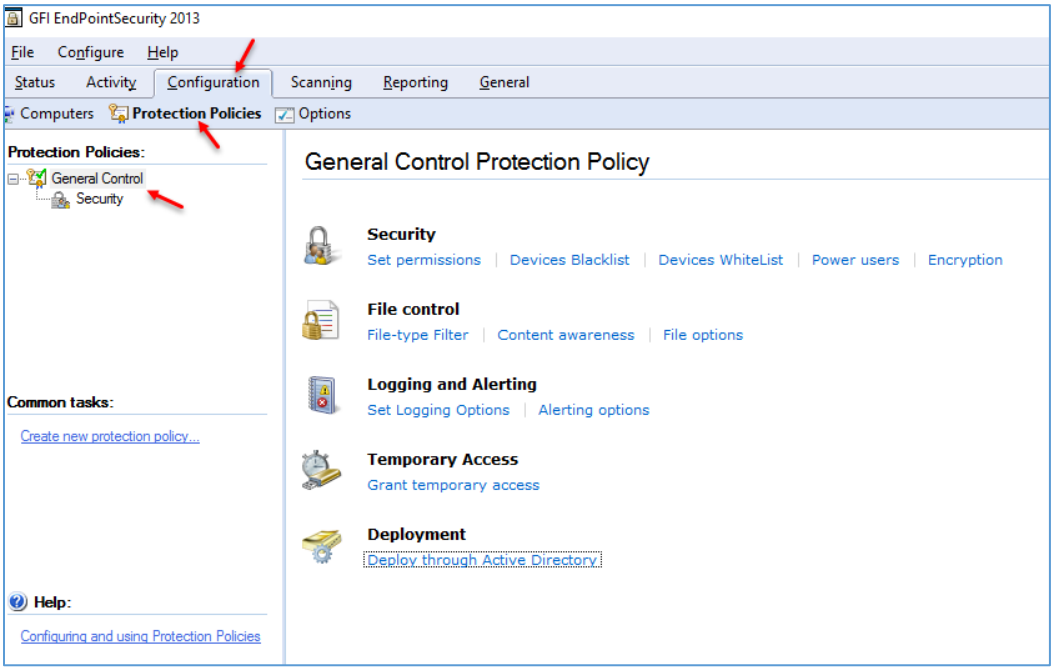
در این قسمت می‌توانید هر کدام از دستگاه‌هایی که اجازه‌ی ارتباط با کلاینت مورد نظر را نداشته باشد را انتخاب کنید که در اینجا، دو گزینه‌ی CD /DVD و Storage Devices انتخاب شده است، بر روی OK کلیک کنید.



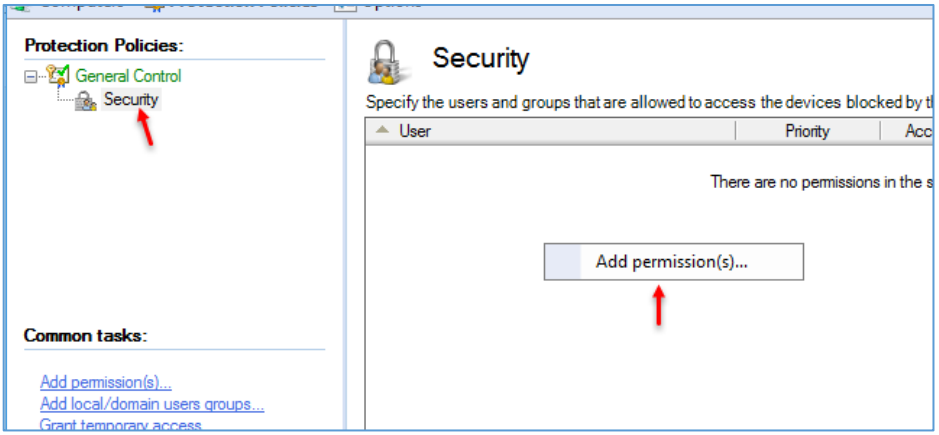
حال، اگر بخواهید حافظه‌ی فلشی را به سیستم N10000 متّصل کنید با خطای شکل روبرو مواجه خواهید شد.

در خطای روبرو که مربوط به فلش Silicon-power16G است، دسترسی توسّط نرم‌افزار GFI بسته شده است.

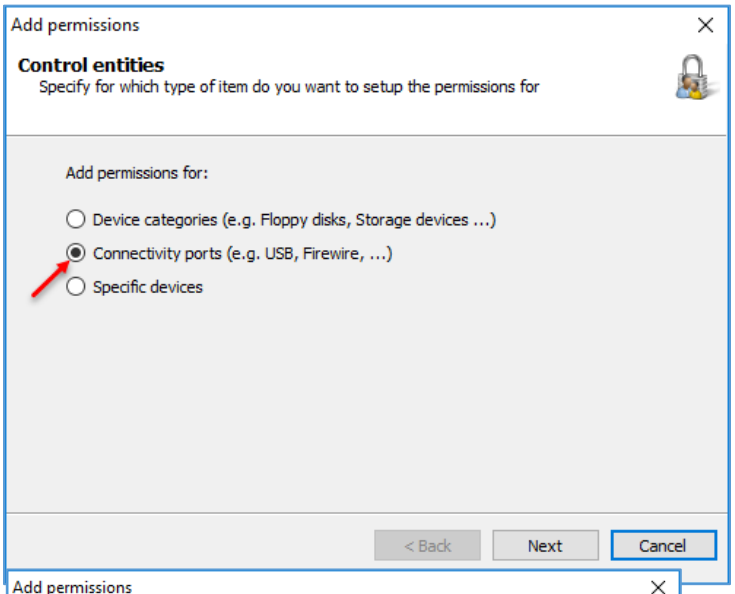
بررسی Policy در نرم‌افزار GFI:



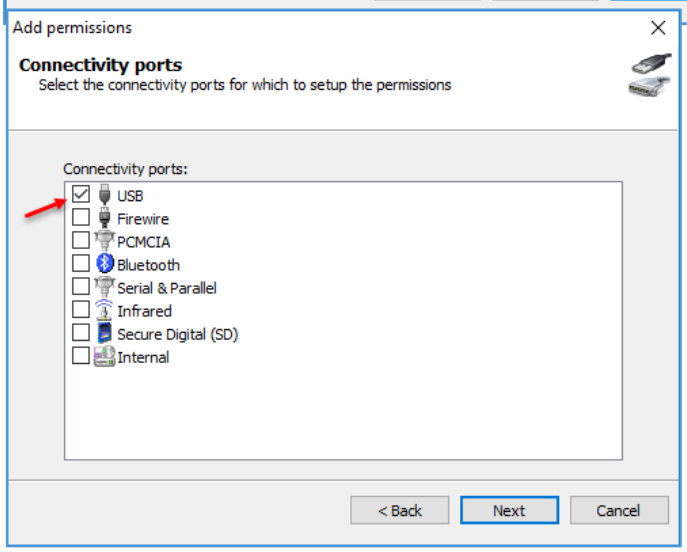
برای ورود به قسمت Policy باید وارد configuration و بعد وارد Protection Policies شوید، در این قسمت، یک Policy به صورت پیش‌فرض تعریف شده است، در سمت راست و در قسمت Security، چند



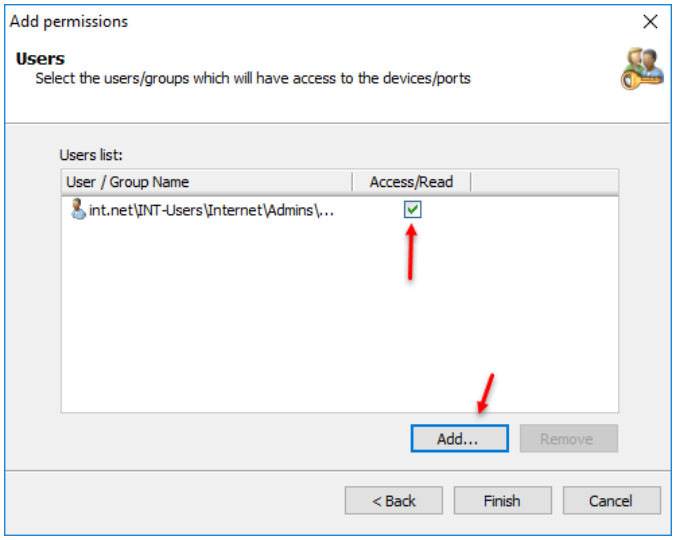
گزینه وجود دارد، بر روی قسمت Set Permissions کلیک کنید و در صفحه‌ی باز شده، کلیک راست کنید و گزینه‌ی Add Permissions را انتخاب کنید.



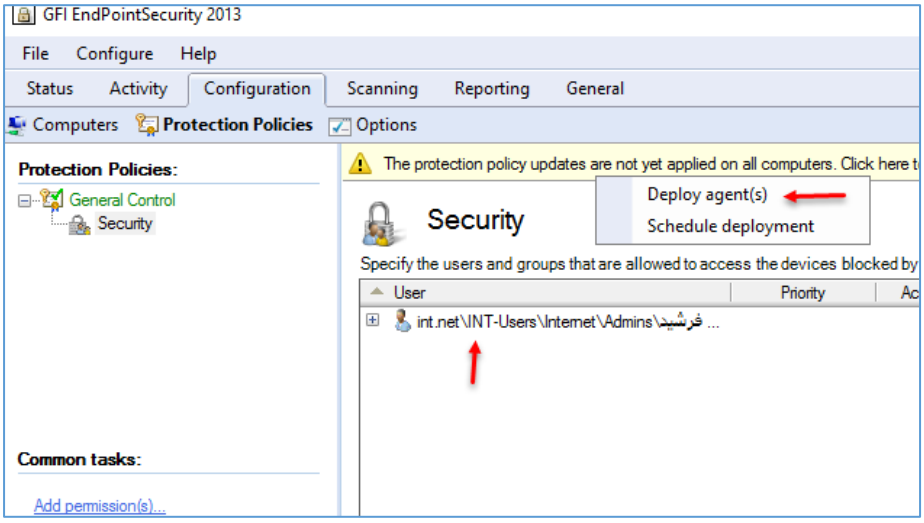
در این قسمت می‌توانید به کاربران خود، این امکان را بدهید تا به پورت یا دستگاه‌های متّصل به کلاینت دسترسی داشته باشند یا نداشته باشند، گزینه‌ی اوّل برای مجموعه‌ی طبقه‌بندی شده‌ی دستگاه‌ها است، گزینه‌ی دوّم برای بستن پورت مشخّص و گزینه‌ی سوّم برای بستن دستگاه‌هایی با شماره‌ی خاص و برند خاص است، گزینه‌ی دوّم را انتخاب و بر روی Next کلیک کنید.



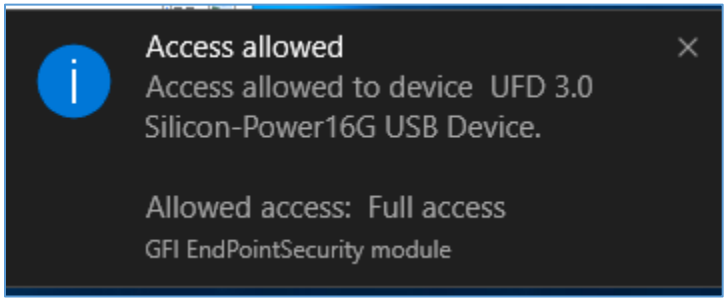
در این قسمت برای تست موضوع، گزینه‌ی USB را انتخاب و بر روی Next کلیک کنید.



در این قسمت باید کاربر خود را مشخّص کنید، برای این کار بر روی Add کلیک کنید و کاربر مورد نظر را به لیست اضافه کنید، توجّه داشته باشید، اگر تیک گزینه‌ی Access/Read را انتخاب کنید، کاربر مورد نظر به پورت‌های تمام سیستم‌هایی که در لیست قرار دارد، دسترسی خواهد داشت، بر روی Finish کلیک کنید.



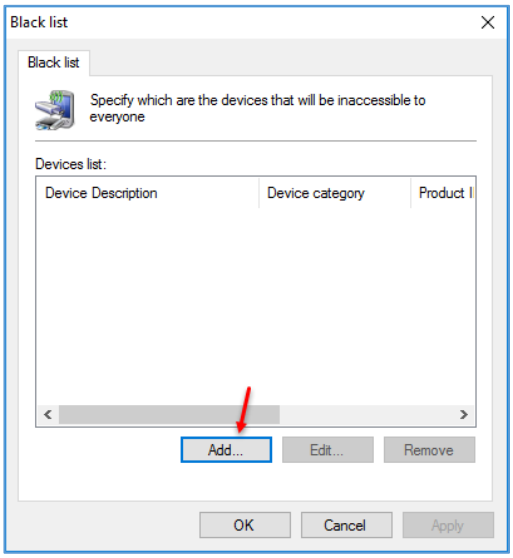
بعد اضافه کردن کاربر مورد نظر و دادن دسترسی به پورت USB، یک نوار زرد رنگ ظاهر می‌شود که این نوار برای این است که شما با کلیک راست بر روی آن و انتخاب گزینه‌ی Deply agent، یک آپدیت به کلاینت‌هایی که در لیست قرار دارد، بفرستید تا آخرین تغییرات را دریافت کنند.



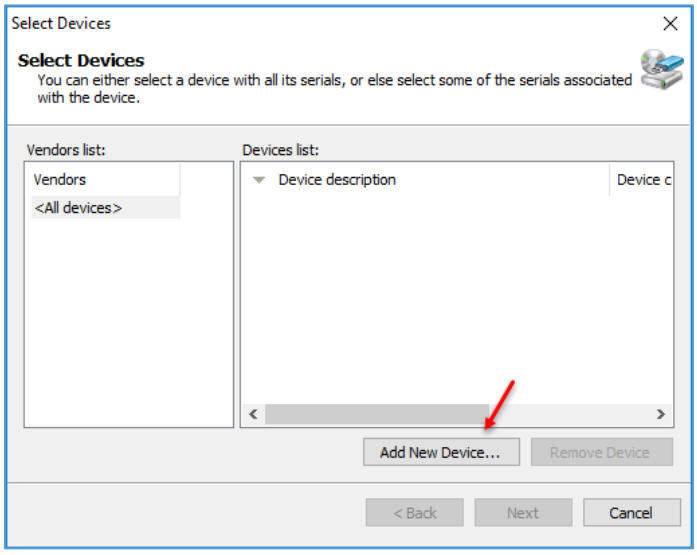
اگر دوباره، حافظه‌ی فلش را متّصل کنید با پیغام روبرو مواجه خواهید شد که اعلام می‌کند به فلش مورد نظر دسترسی دارید.



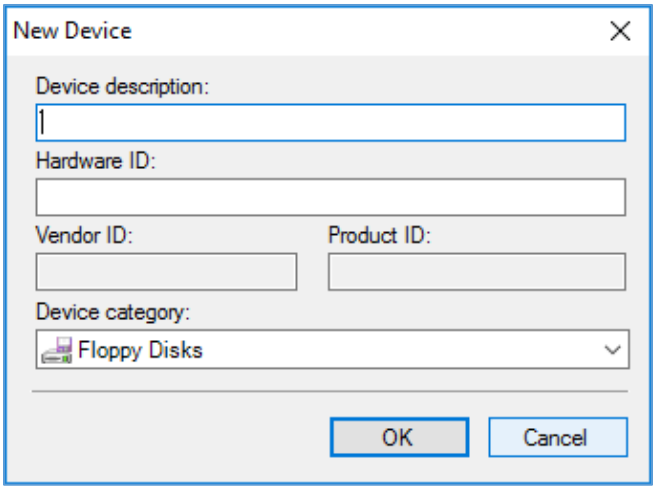
دوباره به قسمت General Control بر می‌گردیم، در این قسمت، گزینه‌ی Device Blacklist که مربوط به دستگاه‌هایی است که اجازه ندارند به شبکه متّصل شوند و گزینه‌ی Device whitelist که اجازه دارند به شبکه متّصل شوند، وجود دارند که این دو گزینه را بررسی می‌کنیم.



برای اضافه کردن دستگاه بر روی Add کلیک کنید.

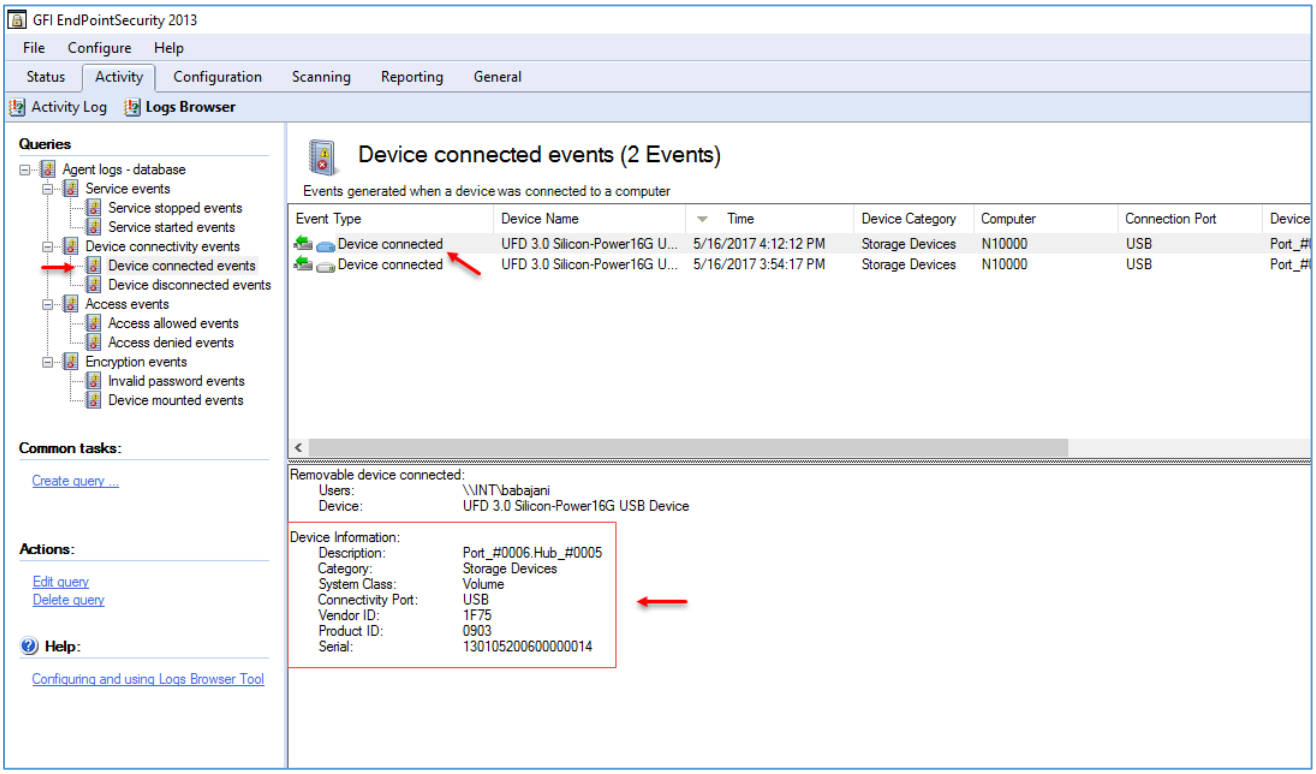


در این قسمت باید دستگاه مورد نظر خود را اضافه کنید که در حال حاضر، دستگاهی در لیست قرار ندارد، برای اضافه کردن دستگاه بر روی Add New Device کلیک کنید.

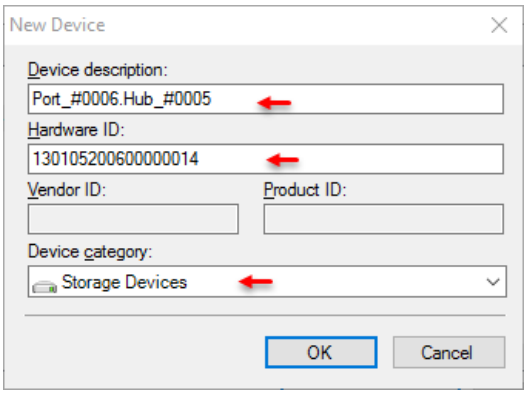


در صفحه‌ی روبرو باید اطّلاعات دستگاه خود را وارد کنید، حال این سؤال برای شما پیش می‌آید که این اطّلاعات را از کجا به دست آوریم؟

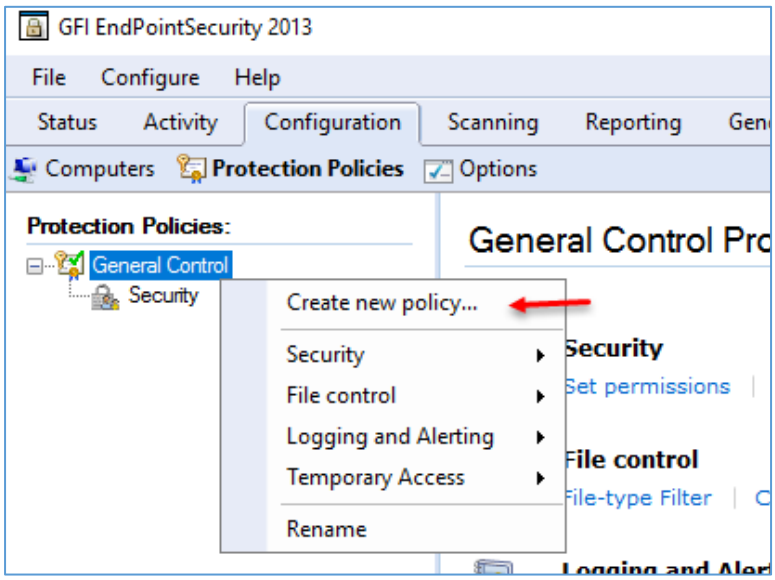
برای پیدا کردن اطّلاعات به صفحه‌ی بعد مراجعه کنید و بعد از دریافت اطّلاعات، دوباره به همین قسمت، مراجعه و اطّلاعات را وارد کنید.



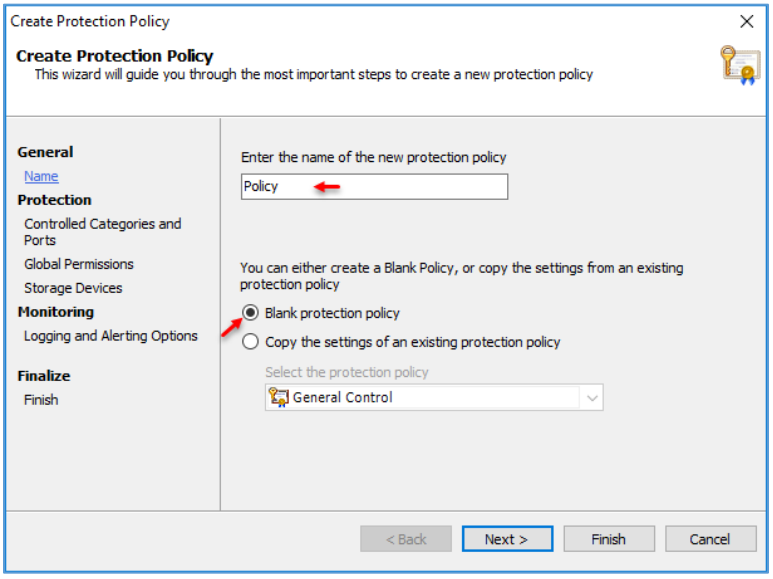
وارد تب **Activity** شوید و بر روی **Log Browser** کلیک کنید، در این صفحه، تمام **Log** ها و اتّفاقاتی که در شبکه رخ می‌دهد، ثبت می‌شود، مثلاً برای دسترسی به اطّلاعات دستگاه‌هایی که به کلاینت‌ها متّصل شده است باید از سمت چپ بر روی **Device connected events** کلیک کنید، همانطور که در شکل بالا مشاهده می‌کنید، دو رخداد ثبت شده است که مربوط به همان، حافظه‌ی فلش است که در مرحله‌ی قبل از آن استفاده کردید، اگر بر روی آن کلیک کنید، اطّلاعات آن را در زیر مشاهده می‌کنید، این همان اطّلاعاتی است که باید وارد کنید.



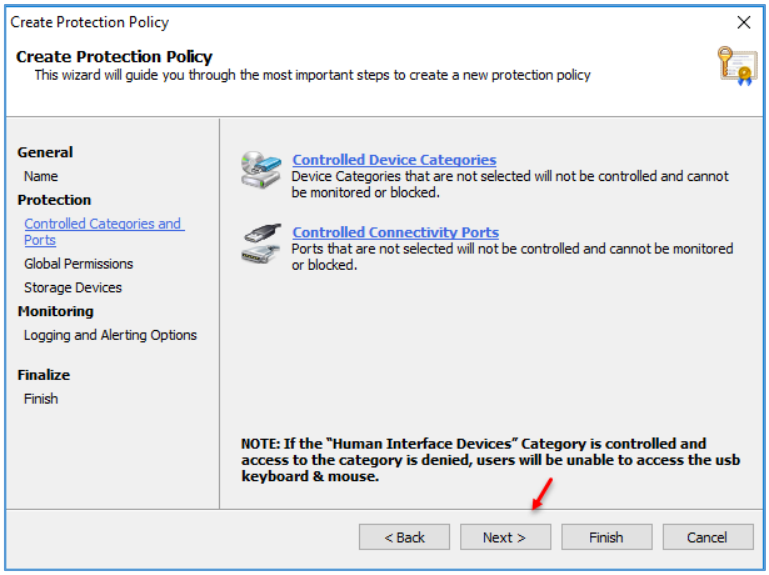
همانطور که مشاهده می‌کنید، اطّلاعات در قسمت‌های مشخّص‌شده وارد شده است، بعد از کلیک بر روی OK، دیگر این فلش با این اطّلاعات به شبکه دسترسی نخواهد داشت، توجّه داشته باشید، بهتر است فلش‌های سازمانی را در لیست سفید قرار دهید تا فلش‌هایی به غیر از این فلش‌ها در شبکه کارایی نداشته باشند.



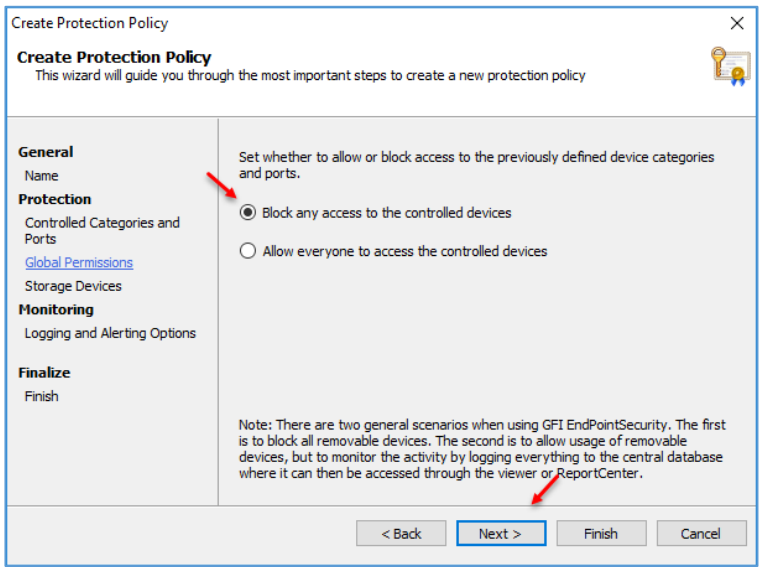
برای ایجاد Policy باید به مانند شکل روبرو بر روی General Control کلیک راست کنید و گزینه‌ی Create new policy را انتخاب کنید.



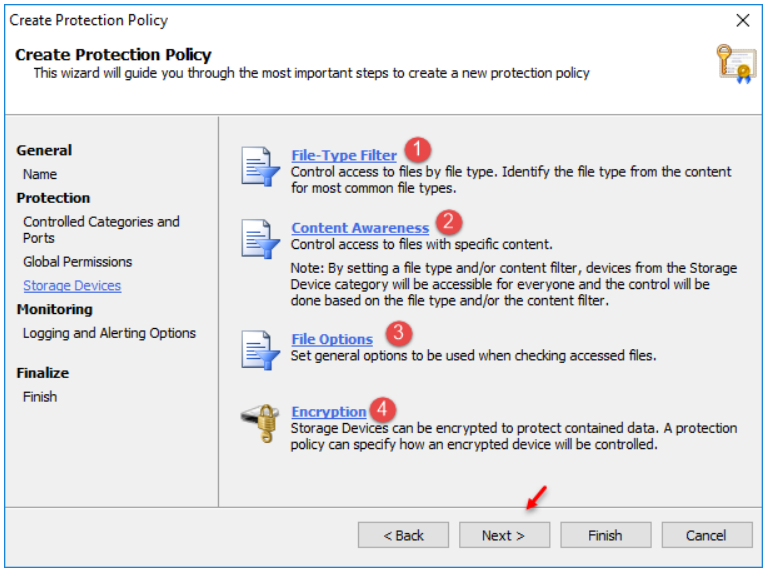
در این صفحه، یک نام برای Policy خود انتخاب کنید و در قسمت پایین صفحه، گزینه‌ی Blank را انتخاب کنید، اگر می‌خواهید از تنظیمات Policy پیش‌فرض استفاده کنید باید گزینه‌ی دوّم را انتخاب کنید.



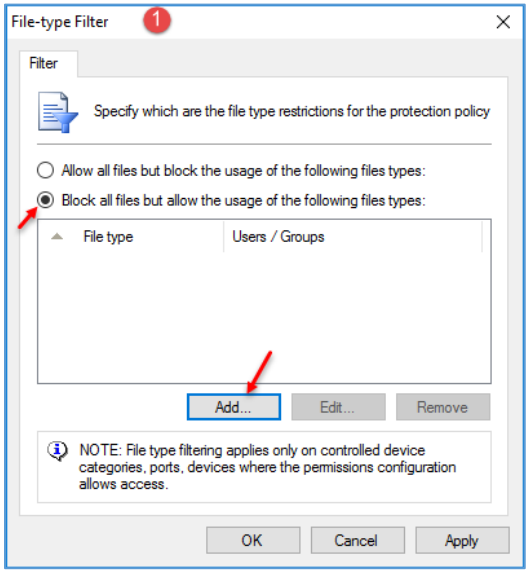
در این قسمت، دو گزینه وجود دارد که برای مشخّص کردن دستگاه‌هایی است که قرار است محدود شوند و حتّی در گزینه‌ی دوّم می‌توانید پورت مورد نظر خود را که می‌خواهید بر روی آن این Policy اعمال شود را انتخاب کنید.



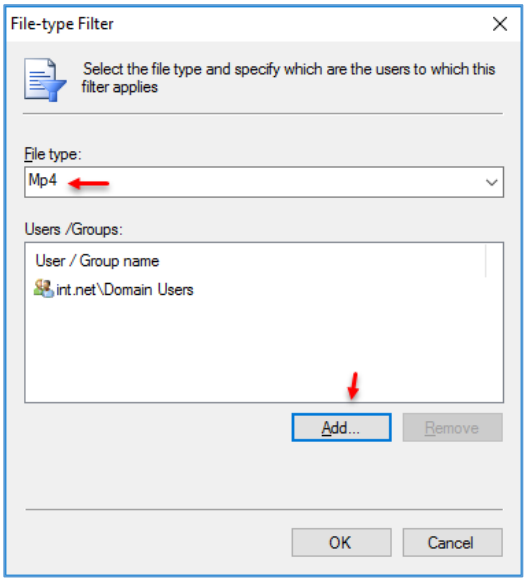
در این قسمت می‌توانید مشخّص کنید که کلاینت‌هایی که بر روی آنها این Policy، ست می‌شود، آیا دسترسی به دستگاه‌ها داشته باشند یا خیر، اگر گزینه‌ی اوّل را انتخاب کنید کلاینت‌ها، دسترسی به دستگاه‌ها و پورت‌های مشخّص‌شده را ندارند و گزینه‌ی دوّم برعکس این عمل خواهد کرد.



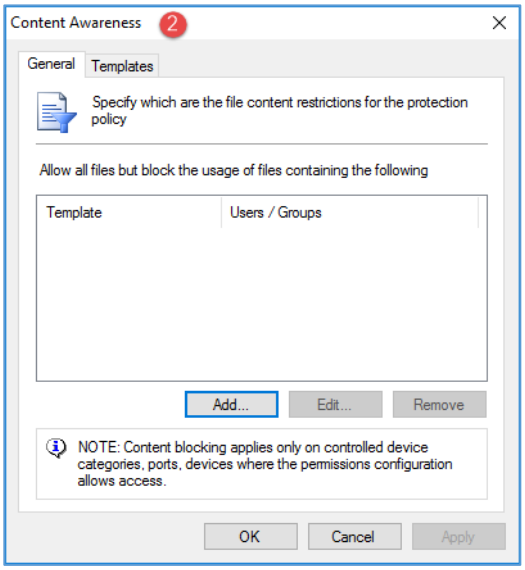
در این قسمت، ٤ گزینه وجود دارد که آنها را بررسی می‌کنیم.



در قسمت شماره‌ی یک، این امکان را دارید تا برای کاربران خود به هر نوع پسوندی از فایل، اجازه‌ی دسترسی بدهید یا ندهید، به عنوان مثال می‌خواهید پسوند MP4 را برای تمام کاربران ببندید، برای این کار گزینه‌ی Block all را انتخاب و بر روی Add کلیک کنید.

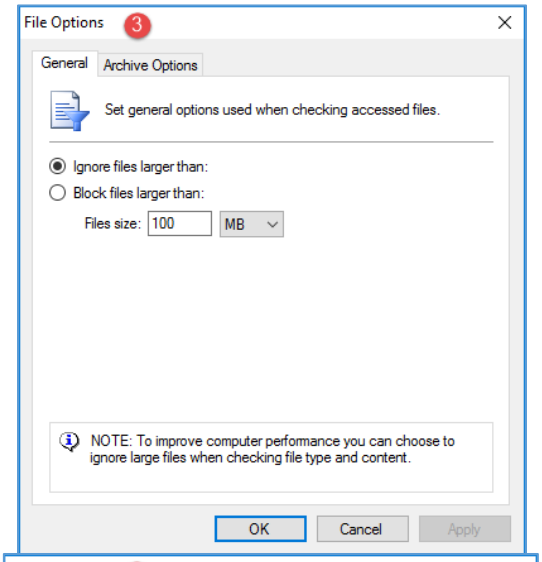


در این صفحه و در قسمت File type می‌توانید نوع پسوند فایل را به صورت دستی وارد و یا بر روی منوی کشویی کلیک کنید و پسوند خود را انتخاب کنید، برای انتخاب کاربر یا گروه بر روی Add کلیک کنید و کاربر یا گروه مورد نظر را به لیست اضافه کنید و بر روی OK کلیک کنید.

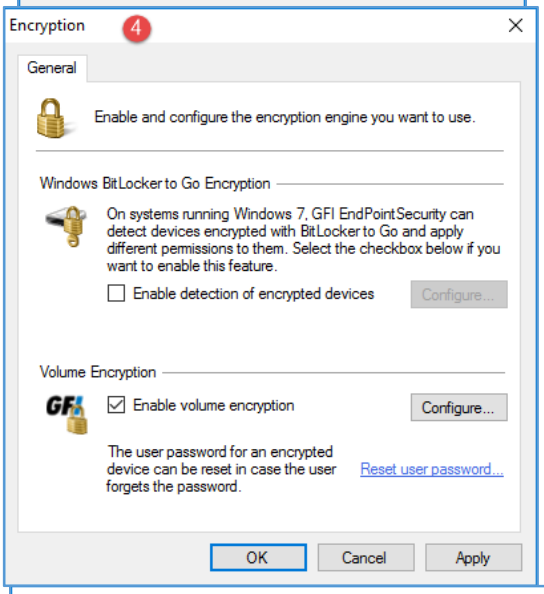


در قسمت شماره‌ی دو که مربوط به Content Awareness است، شما می‌توانید یک‌سری کلمات کلیدی مشخّص کنید که اگر این کلمات در پورت‌های ورودی، مانند USB و... پیدا شود، آن پورت بسته خواهد شد.

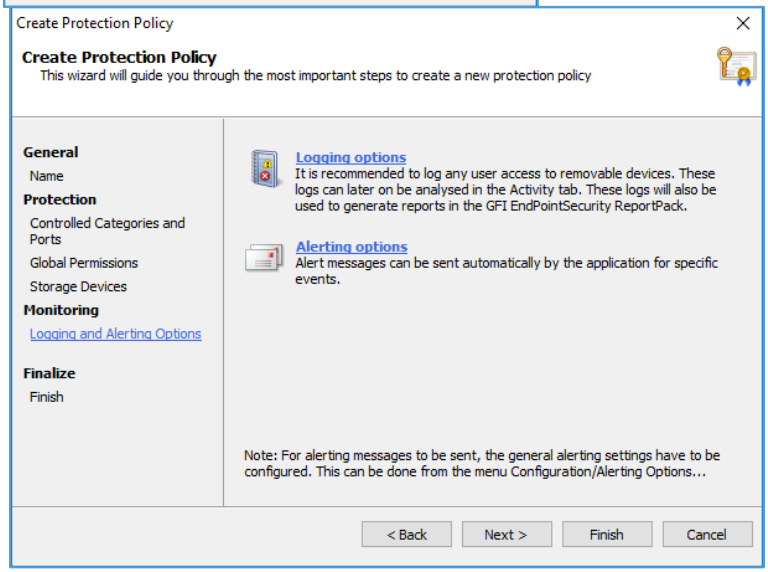
در تب Templates می‌توانید کلمات کلیدی خود را مشخّص کنید، البتّه به صورت پیش‌فرض کلمات کلیدی از قبل وارد شده است.



در قسمت شماره‌ی سه می‌توانید مشخّص کنید که اگر فایل‌ها از مقدار حجم مشخّص‌شده که در اینجا، ۱۰۰ مگابایت است، بیشتر شود، آن فایل را Block کند تا باز نشود.



در قسمت شماره‌ی چهار می‌توانید بر روی پورت‌ها، مانند فلش، عملیّات رمزنگاری را با استفاده از Bitlocker انجام دهید؛ در قسمت پایین، از کاربر برای انجام عملیّات Encryption بر روی درایوها، رمز عبور درخواست می‌شود.

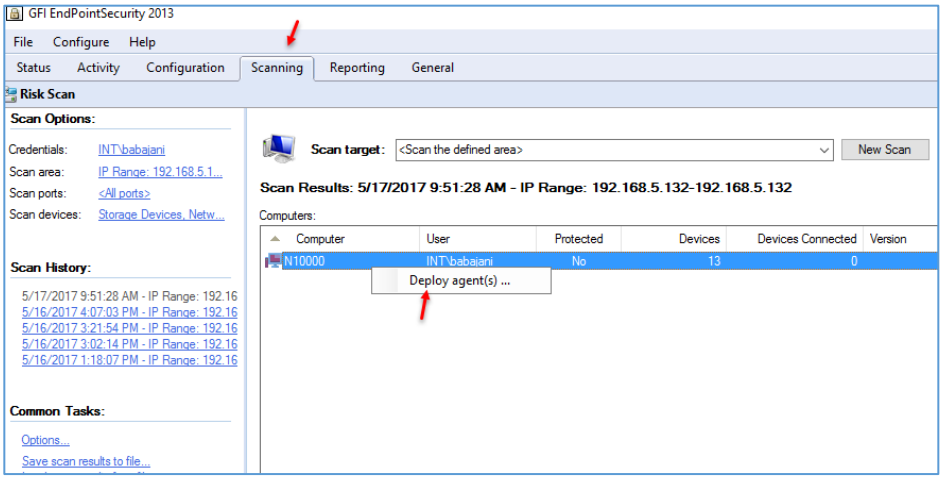


در این صفحه می‌توانید مشخّص کنید که از کدام قسمت‌ها، Log گرفته شود، در قسمت Alert نیز می‌توانید مشخّص کنید که هشدارها از چه طریقی به کاربران ارسال شود، از طریق ایمیل، اس ام اس و یا موارد دیگر.

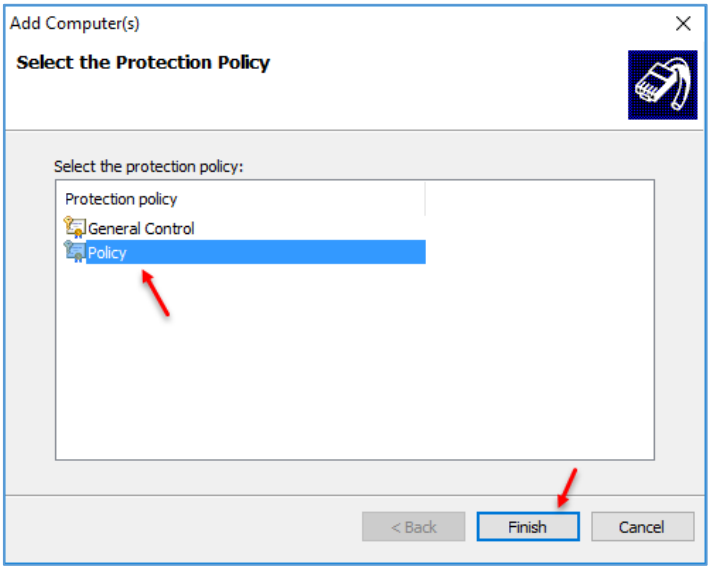
بر روی Finish کلیک کنید تا Policy مورد نظر ایجاد شود.



همانطور که مشاهده می‌کنید، یک Policy جدید ایجاد شده است، اگر بخواهید کاربران از این Policy پیروی کنند باید این Policy را بر روی آنها اعمال کنید.

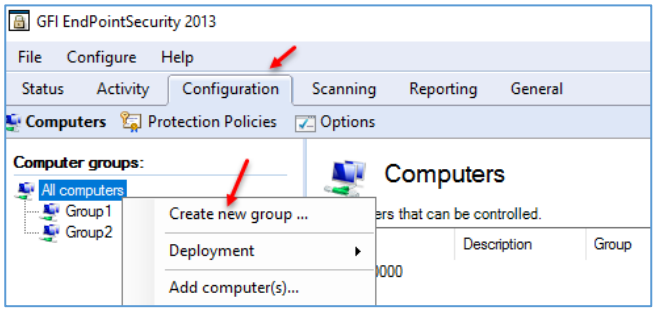


بعد از ایجاد Policy باید وارد Scaning شوید و بر روی سیستم یا سیستم‌های مورد نظر کلیک راست کنید و گزینه‌ی Deploy agent را انتخاب کنید، البتّه این کار را از طریق تب Configuration نیز می‌توانید انجام دهید.

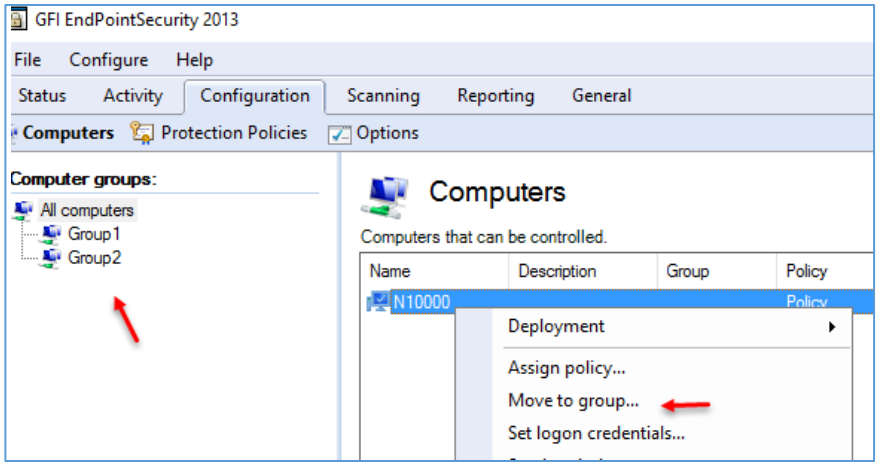


در این صفحه باید Policy ای که در قسمت قبل، ایجاد کردید را انتخاب و بر روی Finish کلیک کنید، با این کار تمام تنظیماتی که بر روی Policy انجام دادید، بر روی کلاینت مورد نظر اعمال خواهد شد.

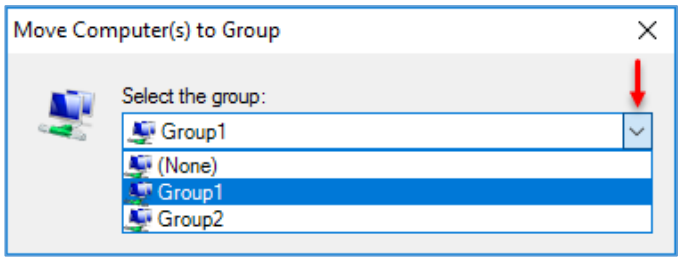
ایجاد گروه در نرم‌افزار GFI:



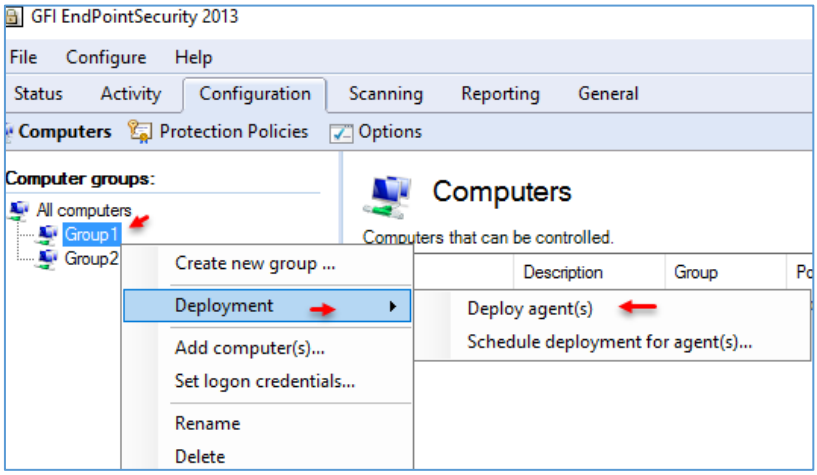
در نرم‌افزار GFI می‌توانید گروه‌هایی با نام دلخواه ایجاد کنید و کلاینت‌ها را در آن گروه قرار دهید، برای این کار وارد تب Configuration شوید و بر روی All computer کلیک راست کنید و گزینه‌ی Create new group را انتخاب کنید.



بعد از ایجاد گروه که در شکل روبرو نیز مشاهده می‌کنید، می‌توانید بر روی کلاینت مورد نظر یا کلاینت‌های مورد نظر کلیک راست کنید و گزینه‌ی Move to group را انتخاب کنید.



در این قسمت باید نام گروه مورد نظر خود را انتخاب و بر روی OK کلیک کنید.



یکی از ویژگی‌های ایجاد گروه این است که شما می‌توانید به هر یک از گروه‌ها، یک Policy مختص به خودش تخصیص دهید تا تنظیمات آن متفاوت باشد، در شکل روبرو بر روی نام گروه کلیک راست کنید و از قسمت Deployment باید Policy مورد نظر خود را برای اعمال شدن بر روی گروه، انتخاب کنید.

منابع:

http://microsoft.com

http://cisco.com

http://panasonic.com/

https://www.ibm.com/us-en/

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...