www.takbook.com

کتاب جامع

مدیر شبکه ۳

نویسندگان:
فرشید فردمنش - آزاده مهرآئین

www.takbook.com

www.takbook.com

سرشناسه : فردمنش، فرشید، ۱۳٦٥-
عنوان و نام پدیدآور : کتاب جامع مدیر شبکه ۳/ نویسندگان فرشید فردمنش، آزاده مهرآئین.
مشخصات نشر : رشت: سیلاک، ۱٤۰۳.
مشخصات ظاهری : ۱۸٤۷ ص.
شابک : ۹۷۸-٦۲۲-۹۲٤۷٤-۰-۲
وضعیت فهرست نویسی : فیپا
موضوع : شبکه‌های کامپیوتری -- مدیریت
Computer networks – Management
شناسه افزوده : مهرآئین، آزاده، ۱۳٦٦-
رده بندی کنگره : TK٥۱۰٥/٥
رده بندی دیویی : ۰۰٤/٦
شماره کتابشناسی ملی: ۹۹۸٦۷٤۸
اطلاعات رکورد کتابشناسی: فیپا

انتشارات سیلاک

نام کتاب : کتاب جامع مدیر شبکه ۳
ناشر: انتشارات سیلاک
مولف : فرشید فردمنش ، آزاده مهرآئین
چاپ اول: ۱٤۰٤
طراح جلد: آزاده مهرآئین
تیراژ: ۱۰۰۰ نسخه
چاپ و صحافی: شبدا
ناظر چاپ: رحیمی
قیمت: ۱٥۰۰۰۰۰۰ ریال
شابک: ۹۷۸-٦۲۲-۹۲۴۷۴-۰-۲

کلیه حقوق برای نشر سیلاک محفوظ است. تکثیر تمامی یا قسمتی از این اثر به صورت حروفچینی یا چاپ مجدد، چاپ افست، پلی‌کپی، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی دارد.

www.takbook.com

www.takbook.com

تقدیم به تو، یار جاودانه‌ام

به همسر عزیزم،
که در هر لحظه از این سفر پر پیچ و خم زندگی،
با نور بی‌پایانت و گرمای بی‌کران،
پناهگاه و قوت قلب من بوده‌ای.

تو که با عشق بی‌دریغ و بی‌پایانت،
هر دشواری را به فرصتی برای شکوفایی،
و هر روز را به آغاز زیباترین فصل زندگی‌ام تبدیل کرده‌ای.
این کتاب، نه تنها محصول تلاش‌هایم،
بلکه بازتابی از نوری است که تو در دل و روح من افکنده‌ای.

هر واژه‌اش، همچون بذری است که تو در عمق وجودم کاشتی
و امروز، در قالب این سطور، ثمره‌اش را به جهانیان تقدیم می‌کنم.

تو برای من الهام‌بخش بوده‌ای، هستی و خواهی بود،
در هر فصل از زندگی‌ام،
همیشه و برای همیشه.

www.takbook.com



www.takbook.com

فهرست مطالب

مقدمه ۳۱
فصل اول ۳۳
مبانی شبکه ۳۳
۱-۱ قسمت اول – بررسی مدل‌ها ۳٤
۱-۱-۱ بررسی مدل OSI ۳٤
۱-۱-۱-۱ لایه‌ی Application (کاربردی) ۳٥
۱-۱-۱-۲ لایه‌ی Presentation (نمایش) ۳۷
۱-۱-۱-۳ لایه‌ی Session (جلسه) ۳۸
۱-۱-۱-٤ لایه‌ی Transport (انتقال) ۳۸
۱-۱-۱-٥ لایه‌ی Network (شبکه) ۳۹
۱-۱-۱-٦ لایه‌ی Data Link (داده) ٤۰
۱-۱-۱-۷ لایه‌ی Physical (لایه‌ی فیزیکی) ٤۰
۱-۱-۲ بررسی مدل TCP / IP ٤۲
۱-۱-۲-۱ لایه‌ی Application ٤۳
۱-۱-۲-۲ لایه‌ی Transport ٤٤
۱-۱-۲-۳ لایه‌ی Internet ٤٤
۱-۱-۲-٤ لایه‌ی Network ٤٥
۱-۱-۲-٥ تفاوت بین مدل OSI و TCP/IP ٤٥

www.takbook.com

۲-۱ قسمت دوم – Network Topologies ٤٨
۲-۱-۱ توپولوژی Star (ستاره‌ای) ٤٩
۲-۲-1 توپولوژی mesh (تو در تو) ٥١
۲-۲-3-1 توپولوژی Hybrid (دو رگه) ٥٣
فصل دوم ٥٥
کابل‌ها و کانکتورها ٥٥
۲-1 نگاهی به کابل‌ها در شبکه ٥٥
۲-۱-۱ کابل هم‌محور Coaxial ٥٥
۲-۱-۲ کابل Twisted-pair یا زوج به هم تابیده ٥٨
۲-۱-۳ سوکت زدن دو سر کابل با RJ45 ..... ٦٢
۲-۱-٤ کابل Serial ٦٧
۲-۱-٥ کابل E1 ..... ٧٠
۲-۱-٦ کابل Stacking ٧١
۲-۱-۷ کابل Console ٧٢
۲-۱-۸ کابل Octal ٧٢
۲-۱-۹ فیبر نوری ٧٣
۲-۲ بررسی سوکت‌ها ٧٩
۲-۲-۱ پورت HDMI ٧٩
۲-۲-۲ پورت VGA ٨٠
۲-۲-۳ پورت DVI ٨١
۲-۲-٤ پورت DisplayPort ٨٢

www.takbook.com

۲-۲-۵ پورت USB ۸۳
۲-۲-۶ پورت‌های کامپیوتر ۸۵
فصل سوم ۸۹
بررسی ابزار و دستگاه‌های شبکه ۸۹
3-1 مانیتور ۸۹
3-۲ کیس ۹۱
۳-۲-۱ مادربرد ۹۳
۳-۲-۲ پردازنده ۹۸
۳-۲-۳ رم ۱۰۰
۳-۲-۴ هارد دیسک ۱۰۳
۳-۲-۵ پاور ۱۱۰
۳-۲-۶ کارت گرافیک ۱۱۴
۳-۳ سوئیچ ۱۱۷
۳-۴ سوئیچ‌های متفرقه ۱۲۱
۳-۴-۱ سوئیچ HDMI ۱۲۲
۳-۴-۲ اسپلیتر HDMI ۱۲۲
۳-۴-۳ کی وی ام سوئیچ (KVM Switch) ۱۲۳
۳-۴-۵ اتصالات میز کنفرانس ۱۲۳
۳-۵ روتر ۱۲۴
۳-۶ رادیو وایرلس ۱۲۹
۳-۷ سرورهای شبکه ۱۳۰

www.takbook.com

۸-۳ یو پی اس ۱٤۱
فصل چهارم ۱٤٥
طراحی اتاق سرور ۱٤٥
٤-۱ ابعاد اتاق سرور ۱٤٦
٤-۲ سیستم سرمایش ۱٤۷
٤-۲-۱ کولر گازی ۱٤۹
٤-۲-۲ خنک کردن با روش InRow ۱٥۰
٤-۲-۳ خنک سازی از کف ۱٥۰
٤-۲-٤ خنک‌سازی از داخل رک ۱٥۱
٤-۳ سیستم اطفای حریق ۱٥۲
٤-٥ کف کاذب ۱٥٥
٤-٦ سقف کاذب ۱٥۸
٤-۷ رک‌ها ۱٥۸
٤-۷-۱ رک ایستاده ۱٥۸
٤-۷-۲ رک دیواری ۱٥۹
٤-۷-۳ نحوه‌ی قرار دادن دستگاه‌های شبکه بر روی رک ۱٦۰
٤-۷-۳-۱ تعداد دستگاه‌های شبکه ۱٦۰
٤-۷-۳-۲ کابل و منظم کردن آن در رک ۱٦۳
٤-۷-۳-۳ کیستون ۱٦٦
٤-۷-٤ پسیو کاری ساختمان ۱٦۸
فصل پنجم ۱۷۳

www.takbook.com

بررسی IPv4 و IPv6 ..... ۱۷۳
5-1 بررسی IPv4 ..... ۱۷۳
۵-۲ آدرس‌های خصوصی (Private IP) ۱۷٤
۵-۳ آدرس‌های عمومی (Public IP) ۱۷۵
5-4 الگوهای غیراستاندارد ۱۷۹
۵-٤-۱ اختصاص دادن رنج IP به شبکه سازمان ۱۸۲
۵-٤-۲ بررسی CIDR ۱۸۵
۵-۵ بررسی پروتکل IPV6 ..... ۱۹۰
5-6 روش آدرس‌دهی در IPv6 ..... ۱۹۵
5-۷ انواع آدرس‌های IPv6 ..... ۱۹٦
فصل ششم ۲۰۱
مجازی‌سازی ۲۰۱
٦-۱ مبانی اولیه ۲۰۱
٦-۱-۱ انواع مجازی‌سازی‌ها در شبکه ۲۰۳
٦-۱-۱-۱ مجازی سازی سرور (Server Virtualization) ۲۰۳
٦-۱-۱-۲ مجازی‌سازی دسکتاپ (Desktop Virtualization) ۲۰٤
٦-۱-۱-۳ مجازی‌سازی نرم‌افزار (Application Virtualization) ۲۰٤
٦-۱-۱-٤ مجازی‌سازی ذخیره‌سازها (Storage Virtualization) ۲۰۵
٦-۱-۱-۵ مجازی‌سازی شبکه (Network Virtualization) ۲۰۵
٦-۱-۱-٦ سوئیچ‌های مجازی ۲۰٦
٦-۱-۲ بررسی نرم‌افزار VMware Workstation ۲۰۷

www.takbook.com

۱-۲-۱-٦ پردازنده ۲۰۸
۲-۲-۱-٦ حافظه (رم) ۲۰۸
۳-۲-۱-٦ هارد دیسک ۲۰۸
٤-۲-۱-٦ کارت شبکه ۲۰۸
٥-۲-۱-٦ سیستم‌عامل ۲۰۹
6-1-3 نصب و راه‌اندازی نرم‌افزار VMware Workstation ۲۰۹
6-1-3-1 فعال‌سازی مجازی‌سازی در Bios ۲۱۲
6-1-3-2 ایجاد ماشین مجازی در VMware Workstation ۲۱٦
6-1-3-3 کار با تنظیمات نرم‌افزار VMware Workstation ۲۲٥
4-۱-٦ بررسی سیستم‌عامل ESXi ۲۳۱
۱-4-۱-٦ سخت‌افزار مورد نیاز برای نصب ESXi ۲۳۳
۲-4-۱-٦ RAIDبندی هارد دیسک ۲۳٤
۳-4-۱-٦ تنظیمات اولیه سرور HP ۲۳۸
٤-4-۱-٦ نصب و راه‌اندازی ESXi ۲٤٦
٥-4-۱-٦ تنظیمات سرور ESXi ۲٥٦
٦-4-۱-٦ بررسی شبکه در سرور ESXi ۲٦۰
۷-4-۱-٦ اضافه کردن هارد دیسک به سرور ESXi ۲٦٥
۸-4-۱-٦ ایجاد ماشین مجازی در ESXi ۲٦۹
۹-4-۱-٦ نصب VMware Tools در ماشین مجازی ۲۷٤
۱۰-4-۱-٦ تعریف و استفاده از کاربر در ESXI ۲۷۷
۱۱-4-۱-٦ متصل کردن ESXi به دومین کنترلر ۲۸۱

www.takbook.com

۱۲-4-۱-٦ آپلود کردن ماشین مجازی ۲۸٦
۱۳-4-۱-٦ انتقال ماشین فیزیکی و مجازی به سرور ESXi ۲۸۸
۱٤-4-۱-٦ افزایش حجم DataStore در ESXi ۲۹۱
۱٥-4-۱-٦ اضافه کردن NFS به سرور ESXi ۲۹٤
۱٦-4-۱-٦ ایجاد SnapShot از ماشین‌های ESXi ۳۰۲
۱۷-4-۱-٦ ایجاد فایل Export از ماشین مجازی در ESXi ۳۰٥
۱۸-4-۱-٦ تنظیم زمان و تاریخ سرور ۳۰۷
۱۹-4-۱-٦ روشن و خاموش شدن ماشین مجازی به صورت اتوماتیک ۳۰۹
۲۰-4-۱-٦ بررسی Swap در ESXi ۳۱۲
۲۱-4-۱-٦ فعال‌سازی سرویس‌ها در ESXi 8 ..... ۳۱۳
۲۲-4-۱-٦ فعال‌سازی ارتباط از راه دور از طریق SSH ۳۱٥
۲۳-4-۱-٦ آپدیت کردن ESXi ۳۱۹
۲٤-4-۱-٦ کار با ISCSI در ESXi ۳۲٤
۲٥-4-۱-٦ نحوه Downgrade کردن در ESXi ۳۳۹
۲٦-4-۱-٦ بررسی قسمت Monitor در ESXi ۳٤۰
فصل هفتم ۳٤۳
میکروتیک ۳٤۳
۱-۷ تاریخچه و رشد MikroTik ۳٤۳
۲-۷ ویژگی‌های متمایز MikroTik ۳٤۳
3-۷ انواع روتر میکروتیک ۳٤٤
4-۷ محصولات اصلی MikroTik ۳٤۷

www.takbook.com

۷-۵ ریست کردن روتر میکروتیک ۳٤۸
۷-٦ نصب و راه‌اندازی اولیه ۳٤۸
۷-۷ تغییر نام روتر میکروتیک ۳۵۳
۷-۸ تنظیم نام پورت های ورودی و خروجی ۳۵٤
۷-۹ آدرس شبکه‌ی داخلی ۳۵۷
۷-۱۰ فعال‌سازی اینترنت در میکروتیک ۳٦۰
۷-۱۱ فعال‌سازی دسترسی کاربران به اینترنت ۳٦۲
۷-۱۲ تنظیم DHCP در میکروتیک ۳٦٦
۷-۱۳ تنظیم DNS در میکروتیک ۳۷۱
۷-۱٤ کار با ترمینال در میکروتیک ۳۷۲
۷-۱۵ مدیریت پهنای باند کاربران ۳۷٦
۷-۱٦ کار با Script در میکروتیک ۳۸۰
۷-۱۷ مدیریت دانلود و آپلود کاربران ۳۸٤
۷-۱۸ ریست کردن Counter کاربران در مدت زمان مشخص ۳۸۸
۷-۱۹ قطع کردن اینترنت شبکه ۳۹۱
۷-۲۰ بستن سایت‌ها در میکروتیک ۳۹٤
۷-۲۱ انجام Backup و Restore در میکروتیک ۳۹۷
۷-۲۲ ایجاد Backup به صورت اتوماتیک و ارسال آن به ایمیل ٤۰۰
۷-۲۳ راه‌اندازی Hotspot در میکروتیک ٤۰٤
۷-۲۸ فعال کردن ورود آزمایشی ٤۱۳
۷-۲۹ شخصی‌سازی صفحهی ورود در HotSpot ٤۱٤

www.takbook.com

۷-۳۰ راه‌اندازی Radius Server و ارتباط آن با Hotspot ٤١٦
۷-۳۱ راه‌اندازی پروتکل L2TP ٤٢٣
۷-۳۲ راه‌اندازی پروتکل OVPN ٤٣٠
۷-۳۳ راه‌اندازی SSTP در میکروتیک ٤٤٢
۷-۳٤ راه‌اندازی تانل 6to4 ..... ٤٥٢
۷-۳٤-۱ تغییر نام میکروتیک ٤٥٦
۷-۳٤-۲ تنظیم آدرس IPv4 و IPv6 ..... ٤٥٦
۷-۳٤-۳ تانل 6to4 ..... ٤٥٨
۷-۳٤-٤ تنظیم روتر MIK-USA ٤٦٢
۷-۳٤-٥ فعال‌سازی GRE6 ..... ٤٦٥
۷-35 راه‌اندازی پروتکل EOIP ٤٧١
۷-۳٥-۱ تنظیم روتر مرکزی ٤٧٣
۷-۳٥-۲ تنظیم روتر شعبه ٤٧٦
فصل هشتم ٤٨١
مهندسی مایکروسافت ٤٨١
۸-1 تاریخچه ویندوز سرور ٤٨١
۸-۲ نیازمندی‌های سخت‌افزاری ٤٨٥
۸-۳ نصب و راه‌اندازی ویندوز سرور ۲۰۲٥ ..... ٤٨٦
۸-۳-1 تغییر نام ویندوز سرور ٤٩٦
۸-۳-۲ تخصیص آدرس IP ٤٩٨
۸-۳-۳ فعال‌سازی Remote Desktop ٥٠٣

www.takbook.com

۸-۳-٤ بررسی Firewall در ویندوز سرور ۵۰۷
۸-۳-۵ بررسی سرویس‌های ویندوز سرور 2025 ..... ۵۱۱
۸-۳-٦ سرویس DNS ۵۱۸
۸-3-6-1 بررسی فایل HOSTS در ویندوز ۵۱۸
۸-۳-٦-۲ نصب و راه‌اندازی سرویس DNS ۵۲۲
۸-3-6-3 Forward Lookup Zones ۵۲٦
۸-۳-٦-٤ Revers Lookup zones ۵۳۱
۸-۳-٦-۵ بررسی DNS Forwarders ۵٤۳
۸-3-6-6 حذف سرویس DNS ۵٤۵
۸-۳-۷ سرویس Active Directory ۵٤٦
۸-۳-۷-۱ دومین (Domain) ۵٤۷
۸-۳-۷-۲ درختان (Trees) ۵٤۸
۸-۳-۷-۳ جنگل‌ها (Forests) ۵٤۸
۸-۳-۷-٤ بررسی Domain Function Level ۵٤۸
۸-۳-۸ نصب و راه‌اندازی سرویس Active Directory ۵۵۰
۸-۳-۹ بررسی سرویس‌های Active directory ۵۵٦
۸-۳-۱۰ کار با سرویس Active Directory Users and Computers ۵۵۸
۸-۳-۱۰-۱ تعریف Organization Unit ۵۵۹
۸-۳-۱۰-۲ چگونه واحدهای سازمانی را حذف کنیم؟ ۵٦۰
۸-۳-۱۰-۳ تعریف کاربر در Active directory ۵٦۳
۸-۳-۱۰-٤ عضو کردن کلاینت در دومین ۵۷۳

www.takbook.com

۸-۳-۱۰-۵ ایجاد گروه در Active directory ۵۹۵
۸-۳-۱۰-۶ ارتباط از راه دور با سرویس Active Directory ۶۰۵
۸-۳-۱۱ سرویس DHCP ۶۰۸
۸-۳-۱۱-۱ انجام Reservation در DHCP ۶۲۱
۸-۳-۱۱-۲ فعّال کردن Mac Filtering در سرویس DHCP ۶۲۵
۸-۳-۱۱-۳ تخصیص دادن آدرس مشخّص به دستگاههای مشخّص ۶۳۰
۸-۳-۱۲ بررسی IPv6 در DHCP ۶۳۴
۸-۳-۱۳ سرویس Active Directory Administrative Center ۶۴۴
۸-۳-۱۴ سرویس Hyper-V ۶۵۲
۸-۳-۱۴-۱ نصب سرویس Hyper-v ۶۵۳
۸-۳-۱۴-۲ ایجاد ماشین مجازی ۶۶۱
۸-۳-۱۴-۳ ایجاد ماشین جدید از ماشین قبلی ۶۶۷
۸-۳-۱۴-۴ شبکه کردن ماشین مجازی ۶۷۱
۸-۳-۱۴-۵ ایجاد کارت شبکه‌ی Private ۶۷۷
۸-۳-۱۴-۶ کار با هاردهای مجازی VHDX ۶۸۰
۸-۳-۱۴-۷ فعال‌سازی Hyper-v در ویندوز ۱۱ ..... ۶۹۳
۸-۳-۱۴-۸ ابزار Replication در سرویس Hyper-V ۶۹۴
۸-۳-۱۴-۹ نصب Hyper-v سرور ۷۰۳
۸-۳-۱۵ سرویس NIC Teaming ۷۱۶
۸-۳-۱۶ سرویس Web Server (IIS) ۷۲۷
۸-۳-۱۶-۱ ایجاد وب سایت در IIS ۷۳۰

www.takbook.com

۸-۳-۱۷ سرویس FTP ۷٤٥
۸-۳-۱۸ سرویس SFTP ۷٥۲
۸-۳-۱۹ سرویس Remote Desktop ۷٦۰
۸-۳-۱۹-۱ کار با سرویس Remote Desktop از طریق Web ۷۷٦
۸-۳-۱۹-۲ اجرای نرمافزار از طریق سرویس Remote Desktop ۷۸۳
۸-۳-۱۹-۳ بررسی تنظیمات Session Collection ۷۸۷
۸-۳-۱۹-٤ فعال کردن Remote Desktop Clients ۷۹۰
۸-۳-۱۹-٥ راهاندازی Virtual Host Server ۷۹٥
۸-۳-۲۰ سرویس Remote Access ۸۱٥
۸-۳-۲۰-۱ فعالسازی سرویس PPTP ۸۱۹
۸-۳-۲۰-۲ فعالسازی سرویس L2TP ۸۳۲
۸-۳-۲۱ سرویس Active Directory Certificate ۸۳٦
۸-۳-۲۲ سرویس Windows Server update Service (WSUS) ۸٥۸
۸-۳-۲۳ سرویس Windows Deployment ۸۸٤
۸-۳-۲٤ بررسی سرویس Disk Management ۹۰٤
۸-۳-۲٤-۱ Shrink کردن ۹۰۸
۸-۳-۲٤-۲ تقسیمبندی در سرویس Disk Management ۹۱۱
۸-۳-۲٤-۳ کار با قابلیت Shadow Copy در درایوها ۹۲۸
۸-۳-۲٥ به اشتراک گذاری فایلها ۹۳۳
۸-۳-۲٦ کار با Bitlocker ۹۳۷
۸-۳-۲۷ نصب وراه اندازی Print Server ۹٤٦

www.takbook.com

۸-۳-۲۸ کار با File Server Resource Manager (FSRM).....۹۵۹
۸-۳-۲۸-۱ ایجاد درایو از طریق شبکه و محدود کردن کاربران آن ۹۶۹
۸-۳-۲۸-3 جلوگیری از کپی کردن نوع خاصی از فایل برای کاربران ۹۷۳
۸-۳-۲۹ کار با سرویس DFS یا Distributed File System.....۹۷۶
۸-۳-۳۰ نحوه‌ی ایجاد Backup و Restore.....۹۸۹
۸-۳-۳۱ بررسی سرویس PowerShell.....۹۹۶
۸-۳-۳۱-۱ مدیریت Active Directory از طریق PowerShell ۱۰۰۹
۸-۳-۳۱-۲ ایجاد گروه از طریق PowerShell.....۱۰۱۵
۸-۳-۳۱-۳ نحوه ی ایجاد Organization Unit از طریق PowerShell.....۱۰۱۶
۸-۳-۳۱-4 حذف Groups،users و Organization Unit از طریق Power Shell.....۱۰۱۷
۸-۳-۳۱-5 کار با DHCP از طریق دستورات PowerShell ۱۰۲۰
۸-۳-۳۱-6 کار با DNS Server از طریق دستورات PowerShell ۱۰۲٤
۸-۳-۳۱-۷ حذف کامپیوترهایی غیرفعال در شبکه ۱۰۲۹
۸-۳-۳۱-۸ اتوماتیک کردن کارها با PowerShell.....۱۰۳۳
۸-۳-۳۱-۹ مدیریت تنظیمات IP ۱۰۳۳
۸-۳-۳۱-10 Ping کردن هم‌زمان چند مقصد.....۱۰۳٦
۸-۳-۳۲ بررسی Server Core ۱۰٤۲
۸-۳-۳۲-۱ بررسی IP Address و عضو کردن در دومین ۱۰٤٥
۸-۳-۳۳ نصب و راه‌اندازی NANO Server.....۱۰۵۱
۸-۳-۳۳-۱ نصب ورژن ۲۰۱٦.....۱۰۵۱
۸-۳-۳۳-2 کار با Docker در ویندوز سرور ۲۰۲۵.....۱۰٦٥

www.takbook.com

۸-۳-34 کار با Group Policy ۱۰٦۸
۸-۳-۳٤-۱ بررسی قسمت Account Policy ۱۰۷۱
۸-۳-34-۲ بررسی قسمت Audit Policy ۱۰۷۹
۸-۳-34-۳ تغییر تصویر BackGround تمام کلاینت‌های شبکه ۱۰۸۱
۸-۳-۳٤-٤ غیرفعال کردن Task Manager برای تمام کلاینتها ۱۰۸٤
۸-۳-۳٤-٥ حذف کردن راست کلیک بر روی Desktop در تمام کلاینت‌ها ۱۰۸٥
۸-۳-۳٤-٦ غیرفعال کردن Remote Desktop بر روی کلاینت‌ها ۱۰۸٥
۸-۳-۳٤-۷ ارسال پیام در شبکه برای کاربران ۱۰۸۸
۸-۳-۳٤-۸ غیرفعال کردن تمام تنظیمات انجام شده در Group Policy ۱۰۹۲
۸-۳-۳٤-۹ بررسی Processing Order در Group Policy ۱۰۹۳
۸-۳-۳٤-۱۰ بررسی Starter GPO ۱۱۰۱
۸-۳-۳٤-۱۱ بررسی و کار با WMI Filtering ۱۱۰٤
۸-۳-35 کار با سرویسهای Monitoring ۱۱۰۸
۸-۳-36 کار با ویژگی‌های مختلف Domain ۱۱۱۲
۸-۳-۳۷ کار با Read Only Domain Controller ۱۱۱۳
۸-۳-۳۸ کار با Install From Media (IFM) ۱۱۲٤
۸-۳-39 حذف Read Only Domain Controller ۱۱۲۷
۸-۳-٤0 ایجاد Domain Tree ۱۱۳۱
۸-۳-٤1 نحوه ایجاد Child Domain ۱۱۳٦
۸-۳-٤۲ ایجاد Trust بین دو دومین مختلف ۱۱٤٤
۸-۳-٤3 انتقال اطلاعات Active Directory ۱۱٥٥

www.takbook.com

۸-۳-٤4 ایجاد failover در Domain و DHCP ۱۱٦۳
فصل نهم ۱۱۸۳
بررسی نرم‌افزار مانیتورینگ ۱۱۸۳
۹-۱ کار با نرم افزار PRTG ۱۱۸۳
۹-۱-۱ تغییر رمز ورود ۱۱۸۷
۹-۱-۲ عضو کردن در دومین ۱۱۸۹
۹-۱-۳ اضافه کردن دستگاه‌ها به PRTG ۱۱۸۹
۹-۱-٤ اضافه کردن شبکه دوم به PRTG ۱۱۹٦
۹-۱-٥ ارسال ایمیل در PRTG ۱۲۰۰
۹-۱-٦ اضافه کردن دستی دستگاه به PRTG ۱۲۰٦
۹-۱-۷ اضافه کردن میکروتیک به PRTG ۱۲۱۲
فصل دهم ۱۲۲۱
بررسی Failover Clustring ۱۲۲۱
۱۰-۱ Failover Clustring ۱۲۲۱
۱۰-۱-۱ تنظیمات سرور iSCSI ۱۲۲۲
۱۰-۱-۲ تنظیمات سرور Failover-1 ..... ۱۲۳۱
۱۰-۱-۳ تنظیمات سرور Failover-2 ..... ۱۲۳٥
فصل یازدهم ۱۲٥۷
System Center 2022 ..... ۱۲٥۷
۱۱-۱ نصب و راهاندازی Microsoft.System.Center. Operations.Manager ۱۲٥۹
۱۱-۲ نیازمندی‌های SQL Server 2025 ..... ۱۲٦٥

www.takbook.com

۱۱-۳ نصب و راه‌اندازی SQL Server 2022 در ویندوز ۱۲۶۷
۱۱-٤ نصب و راه‌اندازی SCOM ۱۲۷۹
۱۱-٤-۱ کار با قسمت Monitoring در System Center ۱۲۹۸
۱۱-٥سرویس Microsoft Endpoint Configuration Manager ۱۳۱۰
۱۱-٦ نصب نرم‌افزار Microsoft Endpoint Configuration Manager ۱۳۱۱
۱۱-٦-۱ نیازمندی‌های سخت‌افزاری ۱۳۱۱
۱۱-٦-۲ نیازمندی‌های نرم‌افزاری ۱۳۱۱
۱۱-٦-۳ تنظیم سرور ۱۳۱۲
۱۱-٦-٤ نصب پیش‌نیازها ۱۳۱۳
۱۱-٦-٥ نصب SQL Server ۱۳۱۷
۱۱-٦-6 نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint ۱۳۱۸
۱۱-٦-۷ بررسی روش Discovery در Endpoint ۱۳۳۰
فصل دوازدهم ۱۳۳۹
VMware VCenter Sever ۱۳۳۹
۱۲-۱ منابع مورد نیاز برای راه‌اندازی VMware Vcenter Appliance ۱۳٤۲
۱۲-۲ نصب VMware Vcenter Appliance ۱۳٤۳
۱۲-۳ نحوه اضافه کردن ESXi به سرور Vcenter ۱۳٥۹
۱۲-٤ ایجاد ماشین مجازی توسط VMware Vcenter ۱۳٦۹
۱۲-٥ ایجاد Clone از ماشین مجازی در Vcenter ۱۳۷۸
۱۲-٦ کار با Template در Vcenter ۱۳۸۱
۱۲-۷ ایجاد فایل OVF از ماشین مجازی در Vcenter ۱۳۸۷

www.takbook.com

۱۲-۸ کار با SnapShots در Vcenter ۱۳۹۱
۱۲-۹ کار با Content Libraries در Vcenter ۱۳۹۳
۱۲-۱۰ ایجاد گزارش از ماشین‌های مجازی ۱۴۰۰
۱۲-۱۱ اتصال VCenter به Active Directory ۱۴۰۱
۱۲-۱۲ راه‌اندازی قابلیت Vmotion در Vcenter ۱۴۰۸
۱۲-۱۳ بررسی DRS در VCenter ۱۴۱۷
۱۲-۱۴ بررسی High Availability (HA) در Vcenter ۱۴۲۴
فصل سیزدهم ۱۴۳۷
Veeam Backup & Replication ۱۴۳۷
نصب نرم‌افزار Veeam Backup and Replication ۱۴۳۸
۱۳-۱ اضافه کردن سرور Backup ۱۴۵۵
۱۳-۲ کار با Jobs در Veeam Backup ۱۴۶۴
۱۳-۳ استفاده از Veeam Agent ۱۴۷۵
۱۳-۴ کار با Application Item ۱۴۸۷
۱۳-۵ فعال‌سازی ایمیل در Veeam Backup ۱۴۹۳
۱۳-۶ بررسی قابلیّت Sure Backup ۱۴۹۵
۱۳-۷ گرفتن Backup از تنظیمات نرم‌افزار ۱۵۰۷
فصل چهاردهم ۱۵۱۱
Exchange Server 2019 ..... ۱۵۱۱
۱۴-۱ سخت‌افزار و نرم افزار مورد نیاز ۱۵۱۲
14-2 ایجاد کاربر ادمین با دسترسی کامل ۱۵۱۷

www.takbook.com

۱٤-۳ نصب پیش‌نیازهای Exchange 2019 ..... ۱۵۲۰
۱٤-4 بررسی صفحه مدیریتی Exchange 2019 ..... ۱۵۲٦
۱٤-5 تنظیم سرویس DNS ۱۵۲۸
۱٤-6 تنظیم گواهینامه داخلی برای کاربران ۱۵۳۰
۱٤-۷ تعریف کاربر در Exchange ۱۵۳۷
۱٤-۸ متصل شدن از طریق Outlook ۱۵٤۲
۱٤-۹ بررسی Outlook تحت وب ۱۵٤۵
۱٤-10 تغییر روش ورود کاربران به Outlook تحت وب ۱۵٤۷
۱٤-۱1 متصل شدن از طریق سرویس POP3 ..... ۱۵۵۰
۱٤-۱۲ متصل شدن از طریق سرویس IMAP ۱۵۵۷
۱٤-۱3 ایجاد گروه در Exchange 2019 ..... ۱۵٦۲
۱٤-۱4 نحوه درخواست کاربر برای عضو شدن در گروه ۱۵۷۰
۱٤-۱5 برگشت دادن ایمیلهای حذف شده ۱۵۷۳
۱٤-۱6 بررسی Resources در Exchange 2019 ..... ۱۵۷٦
۱٤-۱۷ بررسی و انتقال دیتابیس در Exchange 2019 ..... ۱۵۷۹
۱٤-۱۸ ارسال ایمیل به خارج از شبکه (اینترنت) ۱۵۸۵
۱٤-19 ایجاد دومین خارجی و تنظیم آن در Exchange ۱۵۸۹
۱٤-19-۱ تعریف دومین خارجی ۱۵۸۹
۱٤-19-۲ تعریف کاربر با دومین جدید ۱۵۹۳
۱٤-19-۳ تنظیم DNS داخلی و خارجی ۱۵۹٦
۱٤-19-٤ تعریف رکورد PTR ۱٦۰۵

www.takbook.com

۱۴-19-۵ تنظیم فایروال برای ورود به شبکه داخلی ۱۶۰۶
۱۴-19-۶ تغییر آدرس داخلی و خارجی ۱۶۰۹
۱۴-19-۷ ایجاد گواهینامه خارجی برای سرور Exchange ۱۶۱۲
۱۴-19-۸ متصل شدن Outlook از طریق Exchange ۱۶۲۱
فصل پانزدهم ۱۶۲۷
Skype For Business 2019 ..... ۱۶۲۷
۱۵-۱ پیش‌نیاز نصب Skype For Business 2019 ..... ۱۶۲۷
۱۵-۲ تنظیمات DNS برای Skyep For Business 2019 ..... ۱۶۳۲
۱۵-۳ نصب SQL Server 2022 ..... ۱۶۳۵
۱۵-۴ نصب Skype For Business 2019 ..... ۱۶۴۴
۱۵-۵ اجرای قسمت مدیریّتی Skype از طریق Web ۱۶۸۷
۱۵-۶ متصل شدن کاربر به سرور ۱۶۸۸
۱۵-۷ راه‌اندازی سرور EDGE ۱۶۹۱
۱۵-۷-۱ نصب گواهینامه داخلی و خارجی ۱۷۰۸
۱۵-۷-۲ تنظیم DNS داخلی و خارجی ۱۷۲۹
۱۵-۷-۳ فعال کردن دومین خارجی در شبکه داخلی ۱۷۳۴
فصل شانزدهم ۱۷۳۹
VMware Horizon ۱۷۳۹
۱۶-۱ اجزای کلیدی VMware Horizon ۱۷۴۰
۱۶-۲ نصب و راه‌اندازی سرور Horizon Connection Server ۱۷۴۲
۱۶-۳ تعریف لایسنس در Horizon Connection ۱۷۴۹

www.takbook.com

۱۶-۴ ایجاد ماشین مجازی برای سرویس Remote ۱۷۵۰
۱۶-۵ ایجاد Farm در Horizon Connection ۱۷۵۵
۱۶-۶ ایجاد Desktop Pool ۱۷۵۸
۱۶-۷ ایجاد Application Pool ۱۷۶۲
۱۶-۸ کار با VMware Horizon Client Web ۱۷۶۵
۱۶-۹ کار با Horizon Client Application ۱۷۶۹
۱۶-۱۰ نصب SSL و ارتباط از طریق اینترنت ۱۷۷۴
۱۶-۱۱ دسترسی Horizon به سرور VCenter ۱۷۹۴
فصل هفدهم ۱۸۰۱
امنیت شبکه ۱۸۰۱
۱۷-۱ مفاهیم امنیتی ۱۸۰۱
۱۷-۲ بررسی شرایط امنیتی ۱۸۰۱
۱۷-۳ شناخت تهدیدات شبکه فعلی ۱۸۰۴
۱۷-۳-۱ مهاجمان نهایی (Potential Attackers) ۱۸۰۴
۱۷-۳-۲ روش‌های حمله (Attack Methods) ۱۸۰۶
۱۷-۴ راه‌های حمله (Attack Vector) ۱۸۰۷
۱۷-۵ استفاده از اصول اساسی امنیت در شبکه ۱۸۰۸
۱۷-۵-۱ محرمانه بودن (Confidentiality) ۱۸۰۸
۱۷-۵-۲ یکپارچگی (Integrity) ۱۸۰۹
۱۷-۵-۳ در دسترس بودن (Availability) ۱۸۱۰
۱۷-۶ تعاریف اولیه در امنیت اطلاعات ۱۸۱۱

www.takbook.com

۱۷-۶-۱ کمترین امتیاز (Least Privilege) ۱۸۱۱
۱۷-۶-۲ دسترسی به هیچ چیز (Access to Nothing) ۱۸۱۱
17-۶-3 دفاع در عمق (Defense in Depth) ۱۸۱۱
17-۶-4 تفکیک وظایف (Separation of Duties) ۱۸۱۲
17-۶-5 چرخش کار (Job Rotation) ۱۸۱۲
۱۷-۷ مناطق امنیتی مشترک شبکه ۱۸۱۲
17-۷-1 منطقه DMZ ۱۸۱۲
۱۷-۷-۲ منطقه Interanet ۱۸۱۳
17-۷-3 منطقه Extranet ۱۸۱۳
۱۷-۷-٤ منطقه شفاف (Transparent Zone) ۱۸۱۳
۱۷-۷-٥ منطقه اعتماد (Trusted Zone) ۱۸۱۳
۱۷-۷-٦ منطقه با دسترسی محدود (Restricted Zone) ۱۸۱٤
۱۷-۷-۷ منطقه VPN (Virtual Private Network) ۱۸۱٤
۱۷-۸ طراحی شبکه و چشم‌انداز تهدیدات امنیتی ۱۸۱٤
17-۸-1 شبکه محوطه دانشگاه یا Campus-Area Network (CAN) ۱۸۱٤
17-۸-۲ شبکه Wide-Area Network (WAN) ۱۸۱٥
۱۷-۸-۳شبکه Data Center ۱۸۱٦
۱۷-۸-٤ شبکه‌های Small office/Home office ۱۸۱۷
۱۷-۸-٥ امنیت شبکه برای یک محیط مجازی ۱۸۱۸
۱۷-۹چشم انداز تهدید امنیتی شبکه ۱۸۱۹
۱۷-۹-۱ بررسی حملات انکار سرویس ۱۸۱۹

www.takbook.com

۱۷-۹-۲ بررسی روش‌های مهندسی اجتماعی ۱۸۲۰
۱۷-۱۰ روش های موجود برای شناسایی بد افزار ۱۸۲۰
۱۷-۱۱تحلیل و بررسی Dynamic Arp Inspection ۱۸۲۱
۱۷-۱۲ بررسیPort Security ۱۸۲۲
۱۷-۱۳ بررسی CoPP..... ۱۸۲۳
۱۷-۱4 تحلیل و بررسیSpoofing MAC Addresses ۱۸۲٤
فصل هجدهم ۱۸۲۷
برنامه‌نویسی پایتون در شبکه..... ۱۸۲۷
۱۸-۱ سوکت چیست..... ۱۸۲۹
۱۸-۲ کار با کتابخانه Netmiko در پایتون ۱۸۳٦
18-3 نصب Visual Studio Code (VS Code)..... ۱۸۳۸
18-4 Backup گرفتن از روتر میکروتیک..... ۱۸٤۳
۱۸-۵ خروجی گرفتن از فایروال میکروتیک و ایجاد Rule ۱۸٤٤
۱۸-۵-۱ نمایش لیست IPهای DHCP ۱۸٤٦
۱۸-۵-۲ کار با API میکروتیک در پایتون..... ۱۸٤۸
18-6 تغییر آدرس کارت شبکه‌ی ویندوز ۱۸۵۳
۱۸-۷ کار با ESXi در پایتون ۱۸۵۵
۱۸-۷-۱ نمایش ماشین‌های ESXi ۱۸۵٦
۱۸-۷-۲ ریست کردن یک ماشین مجازی در ESXi..... ۱۸۵۷
۱۸-۷-۳ ایجاد ماشین مجازی و روشن کردن آن ۱۸۵۹
۱۸-۷-٤ روشن کردن تمام ماشین‌ها در ESXi..... ۱۸٦۱

www.takbook.com

منابع کتاب ۱۸۶۵

www.takbook.com

www.takbook.com

مقدمه

در دنیای پرشتاب و در حال تغییر امروز، جایی که فناوری اطلاعات به قلب تپنده‌ی هر کسب‌وکار تبدیل شده، شبکه‌های کامپیوتری به عنوان ستون فقرات دنیای دیجیتال شناخته می‌شوند. این شبکه‌ها نه‌تنها ارتباطات و تعاملات روزانه انسان‌ها را ممکن می‌سازند، بلکه زیربنای اقتصاد دیجیتال، خدمات عمومی، امنیت ملی و حتی زندگی روزمره ما هستند. در این دوران، جایی که هر لحظه با تهدیدات و چالش‌های جدید روبه‌رو هستیم، مدیریت شبکه تبدیل به یکی از هنرهای پیچیده و استراتژیک شده است.

مدیران شبکه، به‌عنوان معماران نامرئی این دنیای دیجیتال، مسئولیت طراحی، پیاده‌سازی، نگهداری و مدیریت شبکه‌ها را به عهده دارند. آن‌ها نه‌تنها باید عملکرد شبکه‌ها را بهینه کنند، بلکه باید امنیت، پایداری و کارایی آن‌ها را در برابر حملات سایبری، اختلالات و مشکلات پیش‌بینی‌نشده نیز تضمین کنند. هر قطعی در شبکه، هر نشت اطلاعات و هر اختلالی می‌تواند پیامدهایی جبران‌ناپذیر برای کسب‌وکارها، سازمان‌ها و حتی زندگی روزمره کاربران به دنبال داشته باشد.

این کتاب، راهنمایی جامع و عملی برای کسانی است که می‌خواهند به مرزهای جدیدی از مدیریت شبکه دست یابند. از کسانی که در ابتدای این مسیر هیجان‌انگیز قرار دارند تا متخصصانی که به دنبال تسلط بر پیچیده‌ترین و نوآورانه‌ترین فناوری‌های مدیریت شبکه هستند. ما در این کتاب، نه‌تنها به شما مفاهیم ابتدایی شبکه را معرفی می‌کنیم، بلکه شما را با تکنولوژی‌های پیشرفته، ابزارهای مدرن و بهترین شیوه‌های موجود در این حوزه آشنا می‌سازیم.

آنچه در این کتاب خواهید آموخت:

- اصول و مبانی شبکه: شناخت معماری شبکه‌های کامپیوتری، مدل‌های ارتباطی، پروتکل‌های کلیدی و نحوه طراحی و ساخت شبکه‌های امن و مقیاس‌پذیر.
- مدیریت پیشرفته شبکه: از راه‌اندازی و بهینه‌سازی زیرساخت‌های IPv4 و IPv6 تا پیاده‌سازی و مدیریت سیستم‌های Windows Server و ابزارهای مدرن نظیر MikroTik.
- امنیت سایبری و پایداری شبکه: راهکارهای مقابله با تهدیدات سایبری، تقویت دیوارهای آتش، پیاده‌سازی رمزنگاری و تضمین تداوم خدمات در مواجهه با بحران‌ها.
- مجازی‌سازی و زیرساخت‌های نوین: آشنایی با فناوری‌هایی چون VMware ESXi و Hyper-V که شبکه‌های مدرن را دگرگون کرده‌اند.

www.takbook.com

• ابزارهای کلیدی مدیریت شبکه: بررسی سیستم‌های مانیتورینگ پیشرفته و تکنیک‌های پشتیبان‌گیری برای حفظ داده‌ها و اطلاعات حساس.

چرا این کتاب متمایز است؟

• رویکردی جامع و عملی: این کتاب شما را به دنیای واقعی مدیریت شبکه می‌برد، با سناریوهای عملی، چالش‌های روزمره و راه‌حل‌های اثبات‌شده. شما می‌آموزید چگونه با چالش‌های واقعی در دنیای شبکه مواجه شوید و چگونه به بهترین شیوه ممکن آن‌ها را حل کنید.

• همگام با تحولات دنیای فناوری: این کتاب به‌روزترین مفاهیم، ابزارها و شیوه‌های مدیریت شبکه را به شما ارائه می‌دهد. در دنیای فناوری که هر روز تحولاتی نوین در حال وقوع است، این کتاب به شما کمک می‌کند تا همیشه یک قدم جلوتر باشید.

• مناسب برای تمامی سطوح: این کتاب برای کسانی نوشته شده که می‌خواهند از مبانی اولیه شروع کرده و به سطح پیشرفته دست یابند. این مجموعه برای تازه‌کاران، متخصصان و حتی حرفه‌ای‌ها قابل استفاده است و به شما کمک می‌کند در مسیر تبدیل شدن به یک مدیر شبکه حرفه‌ای گام بردارید.

آیا آماده‌اید که در دنیای مدیریت شبکه بدرخشید؟

اگر هدف شما صرفاً یادگیری اصول نیست، بلکه تسلط بر هنر مدیریت شبکه و تبدیل شدن به یک رهبر دیجیتال است، این کتاب برای شماست. اینجا جایی است که شما نه‌تنها مهارت‌های فنی لازم را می‌آموزید، بلکه در مسیر رشد و پیشرفت در دنیای دیجیتال به یک پیشگام تبدیل خواهید شد.

به دنیای شبکه‌های کامپیوتری خوش آمدید. دنیایی که در آن مهارت‌های شما به هنر تبدیل می‌شود، و شما به عنوان مدیر شبکه، قدرت واقعی را در دنیای دیجیتال در دست خواهید گرفت.

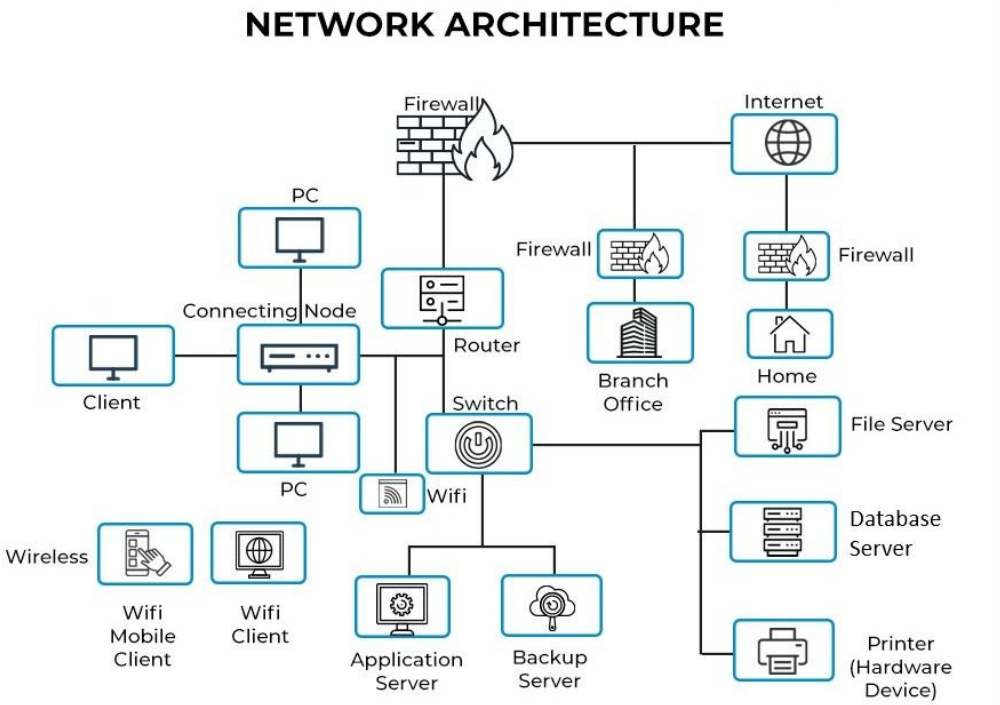
www.takbook.com

فصل اول

مبانی شبکه

شبکه چیست

شبکه ارتباط سخت‌افزارهای مختلف از طریق کابل و وایرلس است که می‌توانند اطلاعات را به همدیگر انتقال دهند و از آنها استفاده کنند، در این کتاب به طور حرفه‌ای صفر تا صد شبکه را یاد خواهیم گرفت، برای شروع کار باید مبانی اولیه کار با شبکه را یاد بگیریم، در شکل ۱-۱ یک طراحی کلی از یک شبکه را مشاهده می‌کنید که تمام دستگاه‌ها از طریق WIFI و کابل با همدیگر شبکه شده اند، البته دارای نام‌های مختلفی هستند که در ادامه به صورت حرفه‌ای روی آنها کار خواهیم کرد.



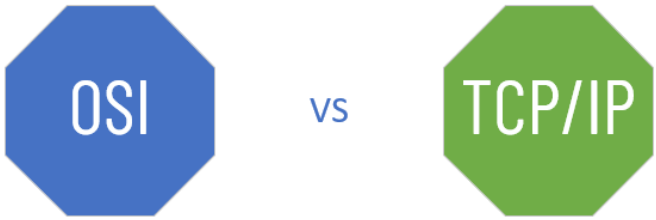
شکل ۱-۱ معماری شبکه

www.takbook.com

۱-۱ قسمت اول – بررسی مدل‌ها

برای اینکه شبکه را به صورت کامل بررسی کنیم باید قوانین اولیه آن را درک کنید، این قوانین به صورت استاندارد برای هر ارتباط شبکه‌ای به کار می‌رود و باید آن را بدانید، شاید این قوانین در مرحله نخست کمی خسته کننده و گیج کننده باشد ولی در ادامه کار با بررسی دستگاه‌ها و نرم‌افزارهای شبکه آن را بهتر درک خواهیم کرد.

در ساختار شبکه از دو مدل استفاده می‌شود که نام آنها در شکل ۱-۲ مشخص است.



شکل ۱-۲ مدل ها

۱-۱-۱ بررسی مدل OSI

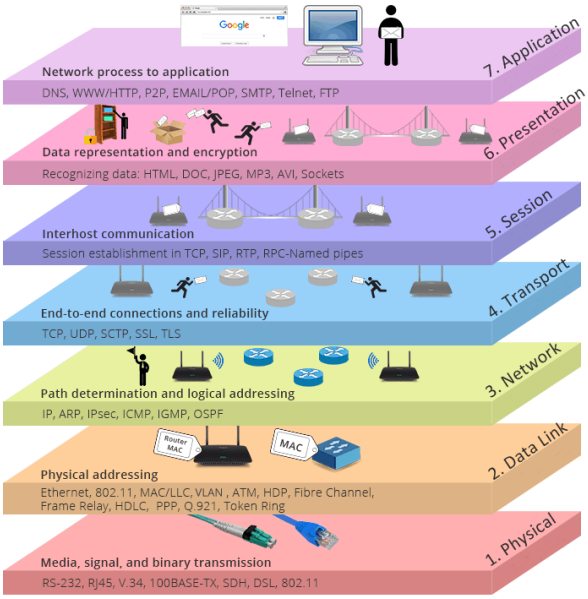
این مدل برگرفته از کلمه‌ی Open System Interconnection است و برای ارتباط بین دو کامپیوتر مبدأ و مقصد به کار می‌رود. این مدل در سال ۱۹۸۰ توسط سازمان ISO طراحی و پیاده‌سازی شده است و طبق سالیان متوالی تغییراتی روی آن صورت‌گرفته است، هرچند که همان ساختار اصلی خود را حفظ کرده است.

این مدل بر اساس یک سری قراردادها با لایه‌ی مقابل خود در کامپیوتر دیگر ارتباط برقرار می‌کند و این کار باعث افزایش سرعت و امنیت در شبکه خواهد شد.

تمام شرکت‌های نرم‌افزاری و سخت‌افزاری طبق این قرارداد محصولات خود را پیاده‌سازی می‌کنند. اگر توجه کرده باشید، بعضی از شرکت‌ها دارای گواهینامه ISO 9001,9002 و غیره هستند، یعنی اینکه طبق استاندارد این سازمان باید کار کنند.

این مدل به‌صورت قراردادی و طبق شکل ۱-۳ از هفت لایه تشکیل‌شده است که هر لایه را برای شما به طور کامل توضیح خواهیم داد.

www.takbook.com

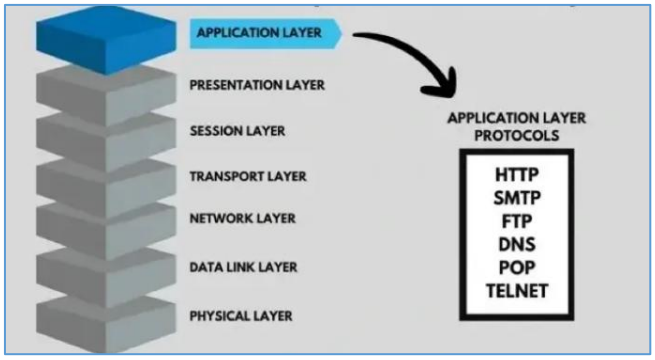


شکل ۱-۳ بررسی مدل OSI

اگر به شکل ۱-۳ توجه کنید، لایه‌های بالاتر به‌صورت نرم‌افزاری می‌باشند و هر چه به طرف لایه‌های پایین‌تر می‌آییم با سخت‌افزار کار خواهیم کرد.

۱-۱-۱-۱ لایه‌ی Application (کاربردی)

این لایه با برنامه‌های کاربردی روی سیستم‌عامل که در شبکه کار می‌کنند ارتباط دارند، مانند نرم‌افزارهای مرورگر و انواع سرویس‌های مربوط به شبکه مانند (Telnet – pop3 – mail – ftp - tftp,…)، این لایه اطلاعات دریافتی را قطعه‌قطعه می‌کند تا لایه‌ی پایینی آن بتواند این اطلاعات را درک کند. نظارت بر Error Recovery و Flow control در هنگام ارسال و دریافت اطلاعات بر عهده‌ی این لایه است، در شکل ۱-٤ نمای کلی از این لایه را مشاهده می‌کنید.



شکل ۱-۴ لایه‌ی Application

www.takbook.com

در زیر لیست کامل پروتکل‌هایی که در این لایه کار می‌کنند را مشاهده می‌کنید:

- ✓ AFP, Apple Filing Protocol
- ✓ APPC, Advanced Program-to-Program Communication
- ✓ Telnet
- ✓ SSH
- ✓ FTP
- ✓ TFTP
- ✓ BOOTP
- ✓ SNMP
- ✓ CMOT
- ✓ AMQP, Advanced Message Queuing Protocol
- ✓ Atom Publishing Protocol
- ✓ BEEP, Block Extensible Exchange Protocol
- ✓ Bitcoin
- ✓ BitTorrent
- ✓ CFDP, Coherent File Distribution Protocol
- ✓ CoAP, Constrained Application Protocol
- ✓ DDS, Data Distribution Service
- ✓ DeviceNet
- ✓ eDonkey
- ✓ ENRP, Endpoint Handlespace Redundancy Protocol
- ✓ FastTrack (KaZaa, Grokster, iMesh)
- ✓ Finger, User Information Protocol
- ✓ Freenet
- ✓ FTAM, File Transfer Access and Management
- ✓ Gopher, Gopher protocol
- ✓ HL7, Health Level Seven
- ✓ HTTP, Hypertext Transfer Protocol
- ✓ H.323, Packet-Based Multimedia Communications System
- ✓ IMAP, Internet Message Access Protocol
- ✓ IRC, Internet Relay Chat
- ✓ IPFS, InterPlanetary File System
- ✓ Kademlia
- ✓ LDAP, Lightweight Directory Access Protocol
- ✓ LPD, Line Printer Daemon Protocol
- ✓ MIME (S-MIME), Multipurpose Internet Mail Extensions and Secure MIME
- ✓ Modbus
- ✓ MQTT Protocol
- ✓ Netconf
- ✓ NFS, Network File System
- ✓ NIS, Network Information Service
- ✓ NNTP, Network News Transfer Protocol
- ✓ NTCIP, National Transportation Communications for Intelligent Transportation System Protocol
- ✓ NTP, Network Time Protocol
- ✓ OSCAR, AOL Instant Messenger Protocol
- ✓ POP, Post Office Protocol
- ✓ PNRP, Peer Name Resolution Protocol
- ✓ RDP, Remote Desktop Protocol
- ✓ RELP, Reliable Event Logging Protocol

www.takbook.com

- ✓ RFP, Remote Framebuffer Protocol
- ✓ Rlogin, Remote Login in UNIX Systems
- ✓ RPC, Remote Procedure Call
- ✓ RTMP, Real Time Messaging Protocol
- ✓ RTP, Real-time Transport Protocol
- ✓ RTPS, Real Time Publish Subscribe
- ✓ RTSP, Real Time Streaming Protocol
- ✓ SAP, Session Announcement Protocol
- ✓ SDP, Session Description Protocol
- ✓ SIP, Session Initiation Protocol
- ✓ SLP, Service Location Protocol
- ✓ SMB, Server Message Block
- ✓ SMTP, Simple Mail Transfer Protocol
- ✓ SNTP, Simple Network Time Protocol
- ✓ SSH, Secure Shell
- ✓ SSMS, Secure SMS Messaging Protocol
- ✓ TCAP, Transaction Capabilities Application Part
- ✓ TDS, Tabular Data Stream
- ✓ Tor (anonymity network)
- ✓ Tox
- ✓ TSP, Time Stamp Protocol
- ✓ VTP, Virtual Terminal Protocol
- ✓ Whois (and RWhois), Remote Directory Access Protocol
- ✓ WebDAV
- ✓ X.400, Message Handling Service Protocol
- ✓ X.500, Directory Access Protocol (DAP)
- ✓ XMPP, Extensible Messaging and Presence Protocol
- ✓ Z39.50
- ✓ DNS, Domain Name Services

۲-۱-۱-۱ لایه‌ی Presentation (نمایش)

این لایه اطلاعات دریافتی را از لایه‌ی بالایی خود دریافت می‌کند و آن‌ها را فشرده‌سازی(Compression) و رمزنگاری(encryption) می‌کند و به لایه‌ی پایینی ارسال می‌کند، البته این لایه می‌تواند اطلاعات فشرده‌سازی شده را از حالت فشرده خارج کند (DeCompression) و هم می‌تواند قفل‌گشایی کند (decryption).

در زیر لیست کامل پروتکل‌هایی که در این لایه کار می‌کنند را مشاهده می‌کنید:

- ✓ Apple Filing Protocol (AFP)
- ✓ Independent Computing Architecture (ICA), the Citrix system core protocol
- ✓ Lightweight Presentation Protocol (LPP)
- ✓ NetWare Core Protocol (NCP)
- ✓ Network Data Representation (NDR)
- ✓ Telnet (a remote terminal access protocol)
- ✓ Tox
- ✓ eXternal Data Representation (XDR)
- ✓ X.25 Packet Assembler/Disassembler Protocol (PAD)

www.takbook.com

۳-۱-۱-۱ لایه‌ی Session (جلسه)

در این لایه، ۲ کامپیوتر ارسال و دریافت‌کننده اطلاعات، دور یک میز می‌نشینند و جلسه‌ای باهم برقرار می‌کنند. در این جلسه بر نوع فایل ارسالی بحث و گفتگو می‌شود که این فایل از چه نوعی است، وقتی به نتیجه رسیدند باهم ارتباط برقرار می‌کنند، به این موضوع هم توجه داشته باشید که آغاز و اتمام یک ارتباط از طریق این لایه انجام می‌گیرد.

در زیر لیست کامل پروتکل‌هایی که در این لایه کار می‌کنند را مشاهده می‌کنید:

- ✓ ADSP, AppleTalk Data Stream Protocol
- ✓ ASP, AppleTalk Session Protocol
- ✓ H.245, Call Control Protocol for Multimedia Communication
- ✓ ISO-SP, OSI session-layer protocol (X.225, ISO 8327)
- ✓ iSNS, Internet Storage Name Service
- ✓ L2F, Layer 2 Forwarding Protocol
- ✓ L2TP, Layer 2 Tunneling Protocol
- ✓ NetBIOS, Network Basic Input Output System
- ✓ PAP, Password Authentication Protocol
- ✓ PPTP, Point-to-Point Tunneling Protocol
- ✓ RPC, Remote Procedure Call Protocol
- ✓ RTCP, Real-time Transport Control Protocol
- ✓ SMPP, Short Message Peer-to-Peer
- ✓ SCP, Session Control Protocol
- ✓ SOCKS, the SOCKS internet protocol
- ✓ ZIP, Zone Information Protocol
- ✓ SDP, Sockets Direct Protocol

٤-۱-۱-۱ لایه‌ی Transport (انتقال)

برای توضیح این لایه، باید ۲ نوع ارتباط را برای شما تشریح کنیم:

- Connection Less
- Connection Oriented

۱- در ارتباط connection Less کامپیوتر مبدأ برای کامپیوتر مقصد اطلاعات ارسال می‌کنند، اما کامپیوتر مقصد هیچ‌گونه پیامی (Acknowledge) مبنی بر دریافت اطلاعات به کامپیوتر مبدأ نمی‌دهد. این مدل را می‌توانید در نرم‌افزارهای چت که به صورت صوتی با طرف خود صحبت می‌کنید، مشاهده کنید که با این کار سرعت انتقال اطلاعات به علت عدم دریافت Acknowledge افزایش می‌یابد.

۲- در ارتباط Connection oriented که ارتباط بسیار مهمی است، کامپیوتر مبدأ اطلاعات خود را به کامپیوتر مقصد ارسال می‌کند و منتظر می‌ماند تا کامپیوتر مقصد، پیام Acknowledge را به مبدأ ارسال کند تا متوجه‌ی دریافت اطلاعات در مقصد شود. اگر این کار انجام نشود در طی زمان

www.takbook.com

مشخص، دوباره اطلاعات را برای مقصد ارسال می‌کند، تا زمانی این کار انجام می‌شود که کامپیوتر مقصد Acknowledge را ارسال کند. این روش برای ارتباطات حساس، بسیار کاربرد دارد.

Acknowledge یک تأییدی بر دریافت اطلاعات به صورت صحیح است.

در این لایه، این ۲ ارتباط که در بالا توضیح دادم مشخص می‌شود، یعنی طبق فایلی که ارسال می‌شود ارتباط آن هم مشخص می‌شود.

پروتکل‌هایی که در این لایه کار می‌کنند:

- ✓ ATP, AppleTalk Transaction Protocol
- ✓ CUDP, Cyclic UDP[3]
- ✓ DCCP, Datagram Congestion Control Protocol
- ✓ FCP, Fibre Channel Protocol
- ✓ IL, IL Protocol
- ✓ MPTCP, Multipath TCP
- ✓ RDP, Reliable Data Protocol
- ✓ RUDP, Reliable User Datagram Protocol
- ✓ SCTP, Stream Control Transmission Protocol
- ✓ SPX, Sequenced Packet Exchange
- ✓ SST, Structured Stream Transport
- ✓ TCP, Transmission Control Protocol
- ✓ UDP, User Datagram Protocol
- ✓ UDP-Lite
- ✓ µTP, Micro Transport Protocol

۵-۱-۱-۱ لایه‌ی Network (شبکه)

این لایه با ipها سروکار دارد و ip مقصد و مبدأ را به بسته‌ی ارسالی ما اضافه می‌کند و به لایه‌ی پایین‌تر می‌فرستد و وظایف کامل آن عبارت‌اند از:

- کنترل عملکرد زیر شبکه
- مسیریابی
- QOS
- به پیوستن شبکه‌های نا همگن

پروتکل‌هایی که در این لایه کار می‌کنند:

- ✓ IPv4/IPv6, Internet Protocol
- ✓ DVMRP, Distance Vector Multicast Routing Protocol
- ✓ ICMP, Internet Control Message Protocol
- ✓ IGMP, Internet Group Management Protocol
- ✓ PIM-SM, Protocol Independent Multicast Sparse Mode
- ✓ PIM-DM, Protocol Independent Multicast Dense Mode

www.takbook.com

- ✓ IPsec, Internet Protocol Security
- ✓ IPX, Internetwork Packet Exchange
- ✓ RIP, Routing Information Protocol
- ✓ DDP, Datagram Delivery Protocol
- ✓ RSMLT Routed-SMLT
- ✓ ARP, Address Resolution Protocol

٦-١-١-١ لایه‌ی Data Link (داده)

آدرس Mac کارت‌های شبکه که یک شماره اختصاصی است به بسته‌ها اضافه می‌شود. اگر به شکل لایه‌ها تصویر ١-٣ توجه کنید متوجه‌ی این موضوع خواهید شد.

در کل لایه‌ی Data Link یا پیونددداده به دو زیر لایه‌ی LLC و MAC تقسیم می‌شوند، MAC مخفف کلمه‌ی Media Access Control است و LLC هم مخفف کلمه‌ی Logical Link Control است.

پروتکل‌هایی که در این لایه کار می‌کنند:

- ✓ Address Resolution Protocol (ARP)
- ✓ ARCnet
- ✓ ATM
- ✓ Cisco Discovery Protocol (CDP)
- ✓ Controller Area Network (CAN)
- ✓ Econet
- ✓ Ethernet
- ✓ Ethernet Automatic Protection Switching (EAPS)
- ✓ Fiber Distributed Data Interface (FDDI)
- ✓ Frame Relay
- ✓ High-Level Data Link Control (HDLC)
- ✓ IEEE 802.2 (provides LLC functions to IEEE 802 MAC layers)
- ✓ IEEE 802.11 wireless LAN
- ✓ LattisNet
- ✓ Link Access Procedures, D channel (LAPD)
- ✓ LocalTalk
- ✓ Multiprotocol Label Switching (MPLS)
- ✓ Nortel Discovery Protocol (NDP)
- ✓ OpenFlow (SDN)
- ✓ Split multi-link trunking (SMLT)
- ✓ Point-to-Point Protocol (PPP)
- ✓ Serial Line Internet Protocol (SLIP) (obsolete)
- ✓ Spanning Tree Protocol
- ✓ StarLan
- ✓ Token ring
- ✓ Unidirectional Link Detection (UDLD)
- ✓ and most forms of serial communication.

٧-١-١-١ لایه‌ی Physical (لایه‌ی فیزیکی)

این لایه که پائینترین لایه‌ی در مدل OSI است، با سیگنال‌ها و کابل‌ها در ارتباط است و سیگنال را از طریق کابل به کامپیوتر مورد نظر ارسال می‌کند.

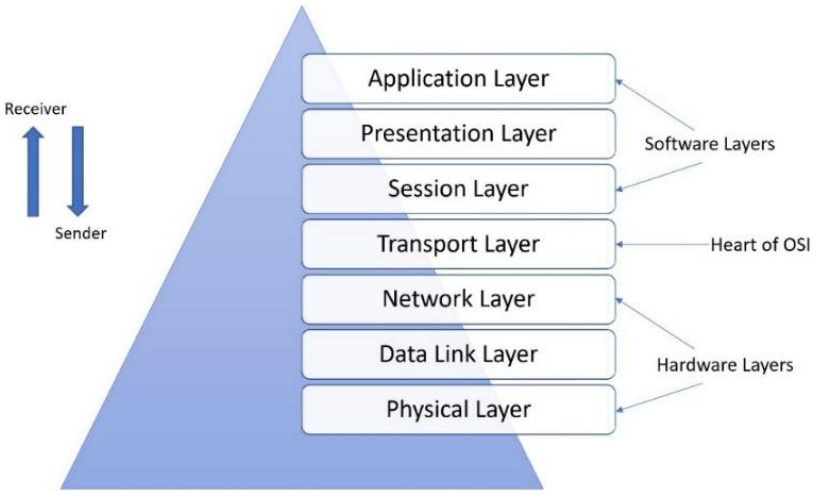
www.takbook.com

در زیر لیست تکنولوژی‌هایی که با لایه‌ی فیزیکی کار می‌کنند را مشاهده می‌کنید:

- ✓ 1-Wire
- ✓ ARINC 818 Avionics Digital Video Bus
- ✓ Bluetooth physical layer
- ✓ CAN bus (controller area network) physical layer
- ✓ DSL
- ✓ EIA RS-232, EIA-422, EIA-423, RS-449, RS-485
- ✓ Etherloop
- ✓ Ethernet physical layer Including 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-SX and other varieties
- ✓ G.hn/G.9960 physical layer
- ✓ GSM Um air interface physical layer
- ✓ IEEE 802.15.4 physical layers
- ✓ IEEE 1394 interface
- ✓ IRDA physical layer
- ✓ ISDN
- ✓ ITU Recommendations: see ITU-T
- ✓ I²C, I²S
- ✓ LoRa
- ✓ Low-voltage differential signaling
- ✓ Mobile Industry Processor Interface physical layer
- ✓ Modulated ultrasound
- ✓ Optical Transport Network (OTN)
- ✓ SMB
- ✓ SONET/SDH
- ✓ SPI
- ✓ T1 and other T-carrier links, and E1 and other E-carrier links
- ✓ Telephone network modems — V.92
- ✓ TransferJet physical layer
- ✓ USB physical layer
- ✓ Varieties of 802.11 Wi-Fi physical layers
- ✓ Visible light communication co-ordinated under IEEE 802.15.7
- ✓ X10

اگر به طور کلی بخواهیم این مدل را بررسی کنیم به مانند شکل ۱-۵ سه لایه‌ی بالایی (7,6,5) مروبط به نرم‌افزار است، لایه‌ی وسط برای انتقال و سه لایه‌ی آخر به عنوان لایه‌های سخت‌افزاری شناخته می‌شوند.

www.takbook.com



شکل ۱-۵ مدل *OSI*

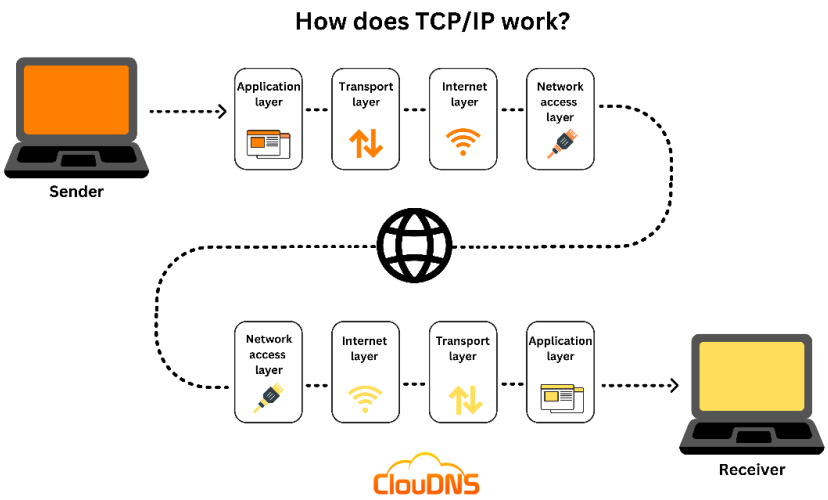
۱-۱-۲ بررسی مدل TCP / IP

مدل TCP/IP که به آن مدل اینترنت نیز گفته می‌شود، یک چارچوب استاندارد برای ارتباطات شبکه‌های کامپیوتری است. این مدل از مجموعه‌ای از پروتکل‌ها تشکیل شده که به انتقال داده‌ها بین دستگاه‌های مختلف در شبکه‌های رایانه‌ای کمک می‌کند. مدل TCP/IP به عنوان پایه و اساس شبکه‌های مدرن، از جمله اینترنت، به‌طور گسترده مورد استفاده قرار می‌گیرد و از چهار لایه‌ی اصلی تشکیل شده است. هر لایه وظایف خاصی را در فرآیند انتقال و مدیریت داده‌ها انجام می‌دهد. در ادامه، به بررسی این لایه‌ها می‌پردازیم:

یکی دیگر از ویژگی‌های این شبکه این است که وقتی کلاینتی آدرسی را دریافت کرده آن آدرس تا آخر برای آن کلاینت باقی می‌ماند به جزء اینکه آن کلاینت مسیرش تغییر کند و آدرس را از دست بدهد.

در این مدل از شبکه که با IP سرو کار دارد تغییراتی در لایه‌بندی مشاهده می‌کنید ، در مدل OSI سه‌لایه اول جدا از هم قرار گرفته‌اند ولی در مدل TCP/IP این سه لایه در یک لایه‌ی Application جمع شده‌اند و در آخر هم دولایه مورد نظر در یک لایه‌ی Network Interface قرار گرفتند، در زیر هر چهار لایه را مورد بررسی قرار می‌دهیم، اگر به شکل ۱-۶ توجه کنید در ارتباط TCP/IP بین دو سیستم چهار لایه درگیر خواهد بود که در زیر آنها را بررسی می‌کنیم.

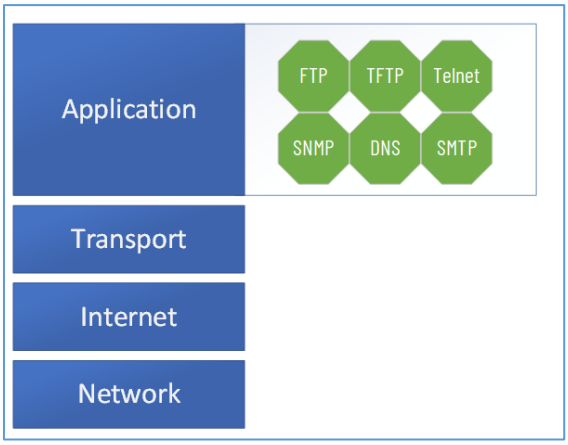
www.takbook.com



شکل ۱-۶ لایه‌ی TCP/IP

۱-۱-۲-۱ لایه‌ی Application

لایه‌یApplication ، بالاترین لایه در پشته‌ی TCP/IP است. تمامی برنامه‌ها و ابزارهای کاربردی در این لایه، با استفاده از لایه‌ی فوق، قادر به دست‌یابی به شبکه خواهند بود. پروتکل‌های موجود در این لایه، به منظور فرمت‌دهی و مبادله‌ی اطلاعات کاربران استفاده می‌گردند. HTTP و FTP دو نمونه از پروتکل‌های هستند که در این لایه کار می‌کنند و در شکل ۱-۷، بعضی از پروتکل‌هایی که در این لایه کار می‌کنند مشخص شده است.



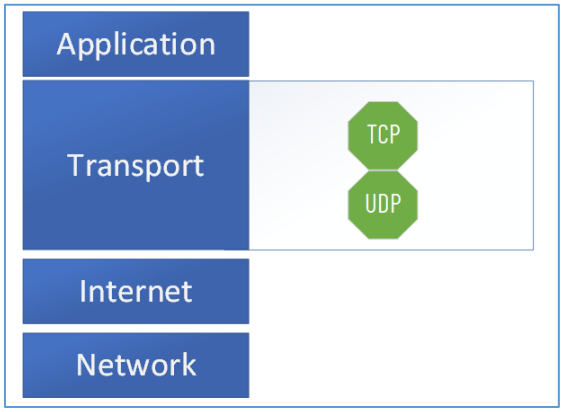
شکل ۱-۷ لایه‌یTransport

یک نکته که در این لایه باید بدانید این است که این لایه برنامه‌ها را تعریف نمی‌کند بلکه بر روی سرویس‌های آنها عمل می‌کند.

www.takbook.com

۲-۲-۱-۱ لایه‌ی Transport

لایه‌ی Transport، قابلیت ایجاد نظم و ترتیب و تضمین ارتباط بین کامپیوترها و ارسال داده به لایه‌ی application (لایه‌ی بالای خود) و یا لایه‌ی Internet (لایه‌ی پایین خود) را بر عهده دارد. لایه‌ی فوق، همچنین مشخصه‌ی منحصر به فردی از برنامه‌ای که داده را عرضه نموده است، مشخص می‌نماید. این لایه، دارای دو پروتکل اساسی است که نحوه‌ی توزیع داده را کنترل می‌نمایند.



شکل ۱-۸ لایه‌ی Transport

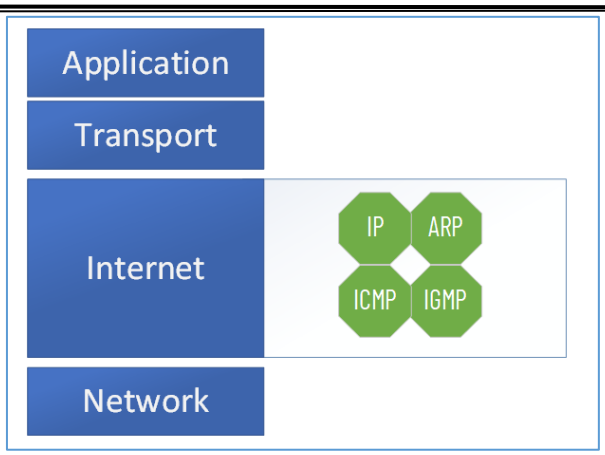
- TCP(Transmission Control Protocol)، پروتکل فوق مسئول تضمین صحت توزیع اطلاعات است
- UDP(User Datagram Protocol) پروتکل فوق، بسیار سریع عمل می‌کند و اطلاعات را به مقصد می‌رساند بدون آنکه تاییدیه‌ای از طرف مقابل خود دریافت کند.

۳-۲-۱-۱ لایه‌ی Internet

لایه‌ی اینترنت، مسئول آدرس‌دهی، بسته‌بندی و مسیریابی داده‌ها است. لایه‌ی فوق، شامل چهار پروتکل اساسی است:

- **IP**(Internet Protocol) پروتکل فوق، مسئول آدرس دهی داده‌ها به‌منظور ارسال به مقصد مورد نظر است.
- **ARP**(Address Resoulation Protocol) پروتکل فوق، مسئول مشخص نمودن آدرس MAC (Media Access Control) کارت شبکه بر روی کامپیوتر مقصد است.
- **ICMP**(Internet Control Message Protocol) پروتکل فوق، مسئول ارائه‌ی توابع عیب‌یابی و گزارش خطا در صورت عدم توزیع صحیح اطلاعات است.
- **IGMP**(Internet Group Managemant Protocol) مسئولیت مدیریت Multicasting در TCP/IP را بر عهده دارد.

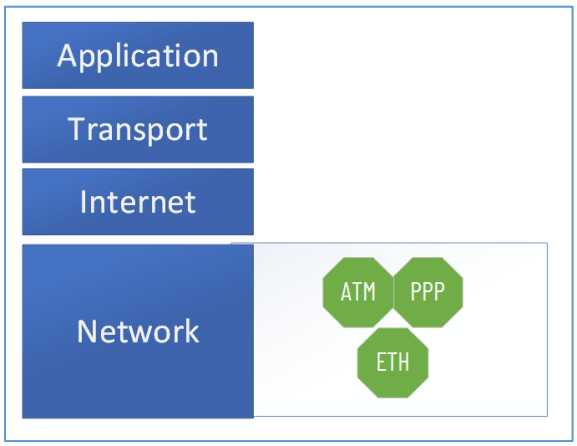
www.takbook.com



شکل ۱-۹ لایه‌ی *Internet*

۱-۱-۲-٤ لایه‌ی Network

پائین‌ترین لایه در مدل TCP/IP است و با سخت‌افزار سرو کار دارد. لایه‌ی فوق، شامل دستگاه‌های فیزیکی نظیر کابل شبکه و آداپتورهای شبکه است. کارت شبکه (آداپتور) دارای یک عدد دوازده رقمی مبنای شانزده بوده که آدرس MAC، نامیده می‌شود. پروتکل‌های ATM, PPP, Ethernet، نمونه‌هایی از پروتکل‌های موجود در این لایه هستند. پروتکل‌های فوق، نحوه‌ی ارسال داده در شبکه را مشخص می‌نمایند.



شکل ۱-۱۰ لایه‌ی *Network*

۱-۱-۲-۵ تفاوت بین مدل OSI و TCP/IP

مدل‌های OSI و TCP/IP دو مدل استاندارد برای توصیف و طبقه‌بندی شبکه‌های رایانه‌ای هستند. هر دو مدل به انتقال داده‌ها بین دستگاه‌های مختلف کمک می‌کنند، اما از نظر ساختار و تعداد لایه‌ها تفاوت‌هایی دارند. در ادامه به بررسی تفاوت‌های اصلی بین این دو مدل می‌پردازیم:

www.takbook.com

تعداد لایه‌ها

مدل OSI: شامل ۷ لایه است:

- لایه فیزیکی (Physical Layer)
- لایه پیوند داده‌ها (Data Link Layer)
- لایه شبکه (Network Layer)
- لایه انتقال (Transport Layer)
- لایه نشست (Session Layer)
- لایه نمایش (Presentation Layer)
- لایه کاربرد (Application Layer)

مدل TCP/IP: شامل ۴ لایه است:

- لایه پیوند داده‌ها (Link Layer)
- لایه اینترنت (Internet Layer)
- لایه انتقال (Transport Layer)
- لایه کاربرد (Application Layer)

هدف اصلی این دو مدل چیست؟

- مدل OSI: به‌عنوان یک مدل مفهومی و نظری طراحی شده است تا فرآیندهای ارتباط شبکه را توصیف کند و استانداردی برای تولید محصولات شبکه‌ای مختلف ایجاد نماید.
- مدل TCP/IP: بیشتر به‌عنوان یک مدل، پیاده‌سازی شده و عملی طراحی شده و پروتکل‌های مورد استفاده در اینترنت و شبکه‌های رایانه‌ای مبتنی بر آن ساخته شده‌اند.

سازگاری با پروتکل‌ها

- مدل OSI: یک مدل عمومی است و برای هر نوع شبکه طراحی شده است. پروتکل‌های اختصاصی به‌صورت جداگانه توسعه یافته‌اند.
- مدل TCP/IP: پروتکل‌هایی مانند TCP و IP به‌طور مستقیم با این مدل مرتبط هستند و مدل TCP/IP خود بر اساس پروتکل‌های شبکه اینترنت توسعه یافته است.

لایه‌های مختلف و وظایف آن‌ها

www.takbook.com

- مدل OSI دارای لایه‌های نشست (Session) و نمایش (Presentation) است که در مدل TCP/IP وجود ندارند. این دو لایه وظایف مربوط به مدیریت ارتباطات (نشست) و ترجمه، رمزگذاری، و فشرده‌سازی داده‌ها (نمایش) را انجام می‌دهند.
- در مدل TCP/IP، این وظایف در لایه کاربرد (Application Layer) انجام می‌شوند.

سادگی و پیچیدگی

- مدل OSI: پیچیده‌تر است و شامل لایه‌های بیشتر با جزئیات دقیق‌تری از وظایف شبکه است. هر لایه در این مدل به وضوح تعریف شده و مسئول انجام کارهای خاصی است.
- مدل TCP/IP: ساده‌تر و عملی‌تر است. برخی از لایه‌های مدل OSI در این مدل ترکیب شده‌اند، مانند لایه‌های نشست و نمایش که در لایه کاربرد ادغام شده‌اند.

رویکرد توسعه

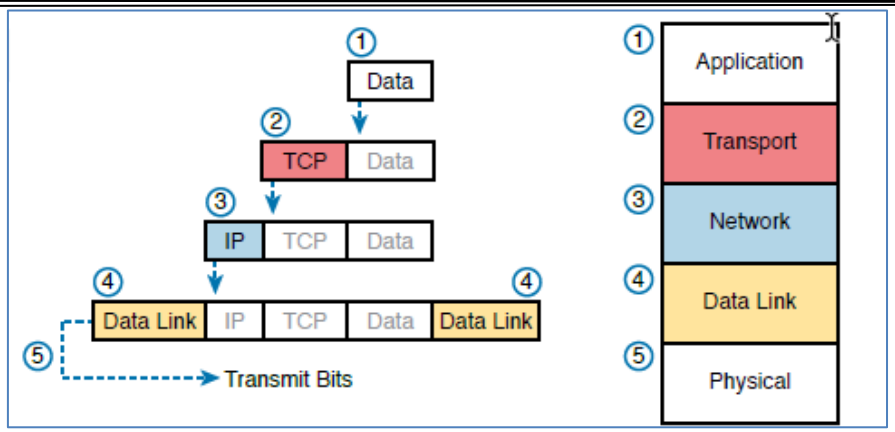
- مدل OSI: ابتدا به عنوان یک مدل نظری توسعه داده شد و سپس سعی شد که پروتکل‌های سازگار با آن طراحی شوند.
- مدل TCP/IP: ابتدا به‌عنوان یک مجموعه پروتکل برای شبکه‌های عملی طراحی و پیاده‌سازی شد و سپس مدل TCP/IP به‌عنوان چارچوبی برای توضیح این پروتکل‌ها ایجاد شد.

کاربرد عملی

- مدل OSI: امروزه بیشتر به‌عنوان یک مدل مرجع مفهومی استفاده می‌شود و به‌صورت مستقیم در پروتکل‌های شبکه به‌کار نمی‌رود.
- مدل TCP/IP: به‌صورت عملی در اینترنت و اکثر شبکه‌های رایانه‌ای جهان استفاده می‌شود.

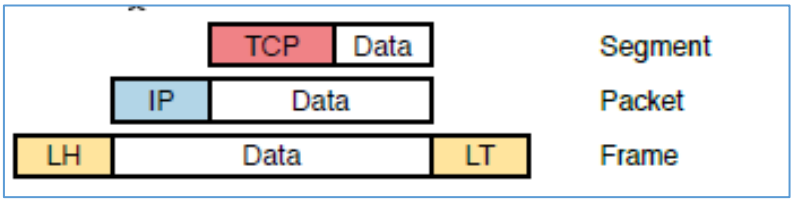
زمانی که داده‌ها در مدل **TCP/IP** در حال انتقال هستند، در هر مرحله از انتقال، بخشی از اطلاعات کنترلی (هدر) به داده اضافه می‌شود. این فرآیند که به **Encapsulation** معروف است، به داده‌ها اجازه می‌دهد در هر لایه از مدل **TCP/IP** اطلاعات لازم برای پردازش و انتقال صحیح را به دست آورند.
در شکل ۱-۱۱ چنین موضوعی قابل مشاهده است.

www.takbook.com



شکل ۱-۱۱ *Data Encapsulation*

هر قسمت از این مراحل دارای نام‌های مختلف هستند که در شکل ۱-۱۲ مشاهده می‌کنید.



شکل ۱-۱۲ نام مراحل *Encapsulation*

Segment : وقتی داده‌ها در لایه انتقال (TCP یا UDP) قرار می‌گیرند، بخشی از اطلاعات کنترلی به داده‌ها اضافه می‌شود. این داده‌ها در این مرحله سگمنت نامیده می‌شوند.

Packet : وقتی سگمنت به لایه اینترنت می‌رسد، هدر IP به آن اضافه می‌شود. پس از اضافه شدن هدر IP (که شامل آدرس‌های IP مبدأ و مقصد است)، داده‌ها، پکت نامیده می‌شوند.

Frame : در لایه دسترسی به شبکه، پکت همراه با هدر و تریلر مربوط به شبکه (مانند آدرس‌های MAC و اطلاعات کنترلی لینک) Frame نامیده می‌شود.

۱-۲ قسمت دوم – Network Topologies

توپولوژی شبکه به نحوه طراحی و آرایش فیزیکی و منطقی دستگاه‌ها، گره‌ها و اتصالات در یک شبکه اشاره دارد. این توپولوژی‌ها تعیین می‌کنند که چگونه دستگاه‌ها با یکدیگر ارتباط برقرار می‌کنند و اطلاعات در شبکه منتقل می‌شود. توپولوژی‌ها به دو دسته کلی تقسیم می‌شوند: توپولوژی فیزیکی و توپولوژی منطقی.

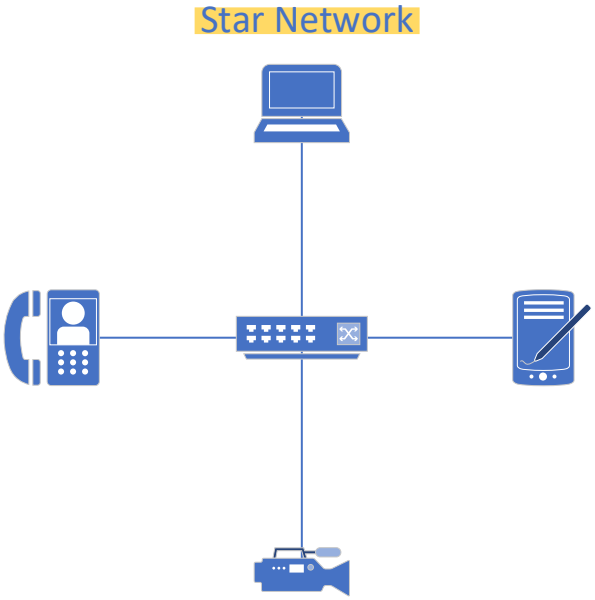
توپولوژی فیزیکی به نحوه اتصال دستگاه‌ها و کابل‌ها در یک شبکه به صورت واقعی و قابل مشاهده اشاره دارد.

www.takbook.com

توپولوژی منطقی به نحوه جریان اطلاعات در شبکه، بدون توجه به نحوه اتصال فیزیکی دستگاه‌ها، اشاره دارد.

۱-۲-۱ توپولوژی Star (ستاره‌ای)

در این نوع از شبکه، کامپیوترها و یا ادوات دیگر شبکه به‌وسیله‌ی یک دستگاه مرکزی مانند Hub یا Switch به همدیگر متصل می‌شوند که امروزه هم در اکثر جاها از این شبکه استفاده می‌کنند و در این کتاب به صورت مفصل این موضوع را بررسی خواهیم کرد، در شکل۱-۱۳ این نوع شبکه را مشاهده می‌کنید.



شکل ۱-۱۳ شبکه‌ی Star

مزایای استفاده از توپولوژی ستاره‌ای (Star Topology)

- مدیریت متمرکز

توپولوژی ستاره‌ای دارای یک دستگاه مرکزی (هاب، سوئیچ یا روتر) است که باعث می‌شود مدیریت و نظارت بر شبکه بسیار آسان‌تر باشد. در صورت بروز مشکل، می‌توان به راحتی به دستگاه مرکزی مراجعه کرد.

- ایزوله‌سازی دستگاه‌ها

www.takbook.com

اگر یکی از دستگاه‌ها یا ارتباطات آن دچار مشکل شود، تأثیری بر روی سایر دستگاه‌ها نخواهد داشت. این ویژگی باعث افزایش تحمل خطا و استقامت شبکه می‌شود.

- سادگی در اضافه کردن یا حذف دستگاه‌ها

اضافه یا حذف دستگاه‌ها از شبکه بسیار ساده است و بدون نیاز به قطع سایر اتصالات انجام می‌شود. این ویژگی باعث می‌شود که شبکه به راحتی گسترش یابد.

- قابلیت مقیاس‌پذیری

توپولوژی ستاره‌ای به راحتی مقیاس‌پذیر است و می‌توان به راحتی دستگاه‌های جدید به شبکه اضافه کرد. در بیشتر موارد، فقط کافی است یک کابل جدید به دستگاه مرکزی متصل کنید.

- بهبود عملکرد

با توجه به اینکه هر دستگاه به‌صورت مستقل به دستگاه مرکزی متصل می‌شود، ترافیک شبکه بهینه‌تر مدیریت می‌شود. این موضوع می‌تواند به کاهش تداخل‌ها و بهبود عملکرد شبکه کمک کند.

- تشخیص خطا آسان

با وجود یک نقطه مرکزی، شناسایی و حل مشکلات شبکه آسان‌تر است. مدیران شبکه می‌توانند به سرعت تشخیص دهند که کدام دستگاه یا ارتباط دچار مشکل شده است.

- استفاده از تجهیزات استاندارد.
- توپولوژی ستاره‌ای معمولاً از تجهیزات استانداردی استفاده می‌کند که در بازار به راحتی در دسترس هستند. این موضوع باعث کاهش هزینه‌ها و سهولت در نگهداری می‌شود.

معایب استفاده از توپولوژی ستاره‌ای (Star Topology)

- نقطه‌ی شکست واحد

بزرگ‌ترین معضل توپولوژی ستاره‌ای این است که اگر دستگاه مرکزی (هاب یا سوئیچ) خراب شود، کل شبکه از کار خواهد افتاد. این موضوع می‌تواند باعث ایجاد وقفه‌های جدی در کار شبکه شود.

- هزینه‌ی بالای تجهیزات:

نیاز به خرید هاب یا سوئیچ مرکزی به همراه کابل‌کشی بیشتر، می‌تواند هزینه‌ها را افزایش دهد. این موضوع به‌ویژه در شبکه‌های بزرگ‌تر و در مواقعی که نیاز به تجهیزات پیشرفته‌تر باشد، مشهود است.

- نیاز به کابل‌کشی بیشتر:

www.takbook.com

در مقایسه با توپولوژی‌های دیگر مانند توپولوژی باس، توپولوژی ستاره‌ای به کابل‌کشی بیشتری نیاز دارد. این می‌تواند منجر به پیچیدگی در نصب و نگهداری شود.

- عملکرد

اگر تعداد زیادی دستگاه به‌طور همزمان به دستگاه مرکزی ارتباط برقرار کنند، ممکن است دستگاه مرکزی به افت سرعت روبرو شود و عملکرد شبکه کاهش یابد.

- حساسیت به کیفیت کابل‌ها

کیفیت کابل‌ها و اتصالات می‌تواند بر عملکرد شبکه تأثیر بگذارد. در صورت استفاده از کابل‌های بی‌کیفیت، ممکن است مشکلاتی در انتقال داده‌ها ایجاد شود.

- مشکلات امنیتی

با وجود یک نقطه مرکزی، اگر کسی به دستگاه مرکزی دسترسی پیدا کند، می‌تواند به تمامی داده‌ها و ارتباطات شبکه دسترسی داشته باشد. بنابراین، نیاز به امنیت بیشتری برای دستگاه مرکزی وجود دارد.

- پیچیدگی در مدیریت شبکه بزرگ:

در شبکه‌های بزرگ، مدیریت و پیکربندی دستگاه‌های متعدد متصل به دستگاه مرکزی می‌تواند پیچیده و زمان‌بر باشد.

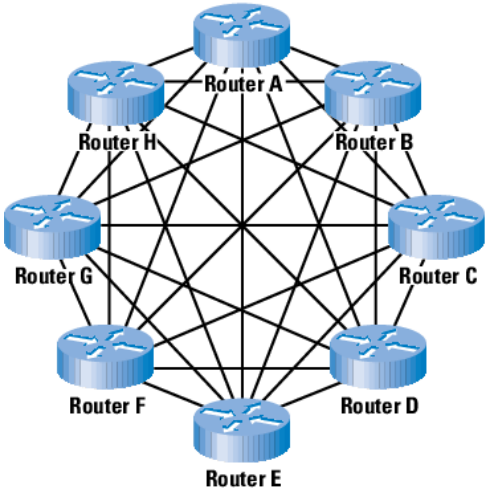
۲-۲-۱ توپولوژی mesh (تو در تو)

Mesh topology (توپولوژی مش یا تو در تو) یکی از پیشرفته‌ترین و مقاوم‌ترین ساختارهای شبکه‌ای است که در آن همه دستگاه‌ها (گره‌ها) به صورت مستقیم به یکدیگر متصل هستند. در این توپولوژی، هر گره می‌تواند به چندین گره دیگر متصل شود و یک مسیر پویا برای انتقال داده‌ها ایجاد کند. این نوع توپولوژی در شبکه‌های بزرگ و حساس به‌کار می‌رود.

در این توپولوژی هر گره به‌طور مستقیم، بدون هیچ واسطه‌ای با کلیه‌ی گره‌های دیگر در ارتباط است؛ بنابراین با فرض N گره در توپولوژی، هر گره باید دارای N-1 پورت باشد. اگر یک گره به کلیه‌ی گره‌ها متصل باشد به آن Full Mesh هم می‌گویند و بیشتر در مکان‌های نظامی کاربرد دارد.

Partial mesh هم به مانند Full Mesh است با این تفاوت که ارتباط هر دستگاه با هر دستگاه دیگر در شبکه وجود دارد اما حتماً مستقیم نیست، این موضوع را در شکل ۱-۱۴ مشاهده می‌کنید.

www.takbook.com



شکل ۱-۱۴ شبکه‌ی Mesh

مزایای توپولوژی Mesh

- مقاومت بالا در برابر خطا: به دلیل وجود مسیرهای متعدد بین گره‌ها، حتی اگر یک مسیر یا چند گره از کار بیفتند، داده‌ها می‌توانند از مسیرهای جایگزین عبور کنند و ارتباط شبکه همچنان حفظ می‌شود.
- ارتباط مستقیم بین دستگاه‌ها: هر گره می‌تواند مستقیماً با گره‌های دیگر ارتباط برقرار کند، که باعث کاهش زمان تأخیر در ارسال داده‌ها می‌شود.
- کارایی بالا: در صورت پیاده‌سازی به صورت کامل، شبکه‌های مش می‌توانند عملکرد بالایی داشته باشند زیرا ازدحام کمتری وجود دارد و داده‌ها سریع‌تر به مقصد می‌رسند.
- مقیاس‌پذیری: این توپولوژی می‌تواند به راحتی با اضافه کردن گره‌های جدید گسترش یابد و گره‌ها می‌توانند با هر تعداد گره دیگر ارتباط برقرار کنند.

معایب توپولوژی Mesh

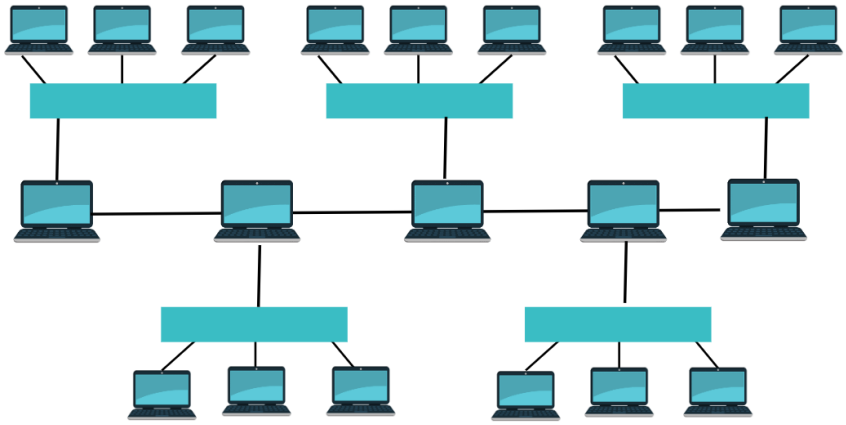
- هزینه بالا: توپولوژی Mesh، به‌ویژه Mesh کامل، به دلیل نیاز به تعداد زیادی کابل و تجهیزات شبکه (مانند روترها و سوئیچ‌ها) هزینه‌بر است.
- پیچیدگی در مدیریت و نصب: پیاده‌سازی این توپولوژی به دلیل اتصالات زیاد بین گره‌ها، پیچیدگی بیشتری نسبت به سایر توپولوژی‌ها دارد و مدیریت آن در شبکه‌های بزرگ می‌تواند دشوار باشد.

www.takbook.com

- نیاز به فضای فیزیکی بیشتر: تعداد زیاد کابل‌ها و تجهیزات باعث می‌شود که برای نصب و نگهداری فضای بیشتری مورد نیاز باشد.

۳-۲-۱ توپولوژی Hybrid (دو رگه)

نوعی از توپولوژی شبکه است که از ترکیب دو یا چند توپولوژی دیگر (مانند ستاره‌ای، باس، حلقه‌ای، یا مش) تشکیل شده است. این توپولوژی به گونه‌ای طراحی شده که مزایای چندین توپولوژی را به‌طور هم‌زمان فراهم می‌کند و برای شبکه‌های بزرگ و پیچیده که نیازهای مختلفی دارند، بسیار مفید است، در شکل ۱-۱۵ این نوع توپولوژی را مشاهده می‌کنید.



شکل ۱-۱۵ شبکه‌ی Hybrid

مزایای توپولوژی Hybrid

- انعطاف‌پذیری بالا: توپولوژی Hybrid به دلیل انعطاف‌پذیری بالا می‌تواند برای شبکه‌های مختلف و نیازهای خاص طراحی شود. این توپولوژی می‌تواند به راحتی با تغییرات در ساختار شبکه سازگار شود.
- مقیاس‌پذیری: می‌توان به راحتی بخش‌های جدیدی به شبکه Hybrid اضافه کرد بدون اینکه بر کل شبکه تأثیر بگذارد. به همین دلیل این توپولوژی برای شبکه‌های بزرگ و در حال رشد مناسب است.
- عملکرد بهینه: با ترکیب توپولوژی‌های مختلف، می‌توان بهترین عملکرد را از هر توپولوژی استفاده کرد. برای مثال، در بخش‌هایی که سرعت انتقال داده مهم است از توپولوژی مش و در بخش‌های دیگر از توپولوژی ستاره‌ای استفاده می‌شود.

www.takbook.com

- تحمل خطا: اگر در طراحی از توپولوژی‌هایی مانند مش استفاده شود، شبکه می‌تواند به راحتی در برابر خطاها مقاومت کند و ارتباطات جایگزین ایجاد کند.

معایب توپولوژی Hybrid

- پیچیدگی در طراحی و مدیریت: به دلیل ترکیب چندین توپولوژی مختلف، مدیریت و نگهداری توپولوژی Hybrid پیچیده‌تر از سایر توپولوژی‌ها است. همچنین طراحی آن نیاز به برنامه‌ریزی و دانش فنی بالا دارد.
- هزینه‌ی بالا: پیاده‌سازی توپولوژی Hybrid ممکن است به دلیل استفاده از چندین نوع توپولوژی و تجهیزات مختلف، هزینه‌بر باشد. نیاز به کابل‌کشی بیشتر و تجهیزات پیشرفته نیز می‌تواند هزینه‌ها را افزایش دهد.
- نیاز به پیکربندی دقیق: هر بخش از توپولوژی باید به‌درستی با بخش‌های دیگر هماهنگ شود. اگر این هماهنگی به‌درستی انجام نشود، ممکن است کارایی شبکه کاهش یابد.

www.takbook.com

فصل دوم

کابل‌ها و کانکتورها

۲-۱ نگاهی به کابل‌ها در شبکه

کابل‌ها بخش مهمی از زیرساخت شبکه‌های کامپیوتری هستند و نقش حیاتی در انتقال داده‌ها بین دستگاه‌ها و شبکه‌ها دارند. در شبکه‌های کامپیوتری، کابل‌ها از انواع مختلفی برخوردارند که هرکدام ویژگی‌ها و کاربردهای خاص خود را دارند. در اینجا به توضیح انواع کابل‌های رایج در شبکه می‌پردازیم.

کل شبکه‌های امروزی از یکی از گروه‌های کابلی زیر استفاده می‌کند.

- کابل هم‌محور(coaxial)
- زوج تابیده‌شده(twisted-pair)
- فیبر نوری(fiber-optic)
- کابل سریال
- کابل Console

۲-۱-۱ کابل هم‌محور Coaxial

این نوع کابل معمولاً در بیشتر شبکه‌های امروزی استفاده می‌شود، اما فقط در استفاده‌های خاص در ساده‌ترین شکل آن، کابل coaxial تشکیل‌شده است از یک هسته‌ی ساخته‌شده از مس خالص که توسط روکشی پوشیده شده است. یک روکش فلزی توری مانند و یک روکش بیرونی. هسته‌ی کابل coaxial حامل سیگنال‌های الکتریکی است که در واقع همان اطلاعات ما را تشکیل می‌دهد.

این نوع کابل‌ها از یک روکش توری استفاده می‌کنند که کابل را در برابر امواج مزاحم یا همان Noise دور می‌کند. کلاً این نوع کابل برای ارتباط راه دور استفاده می‌شود، چون در ارتباط راه دور، افت سیگنال ندارد و نسبت به کابل Twisted Pair بهتر است، در زیر دو نوع کابل Coaxial را مشاهده می‌کنید.

- نازک(Thinnet)
- ضخیم (Thicknet)

کابل نوع Thinnet

Thinnet یک کابل coaxial انعطاف‌پذیر به ضخامت ۰/۲۵ اینچ است، به خاطر انعطاف و سادگی استفاده، تقریباً در نصب هر نوع شبکه‌ای می‌توان از آن استفاده کرد. این نوع کابل می‌تواند سیگنال را تقریباً ۱۸۵ متر بدون افت سیگنال حمل نماید. کابل thninnet در خانواده‌ای از کابل‌ها به نام RG- ۵۸ قراردارد و

www.takbook.com

امپدانس معادل ۵۰ اهم دارد. امپدانس، مقاومت سیم است که برحسب اهم، اندازه‌گیری شده است. اختلاف اصلی در کابل‌های خانواده‌ی RG-۵۸، هسته‌ی کابل است که ممکن است به شکل تک رشته یا چند رشته باشد، در شکل ۲-۱ و ۲-۲ دو نمونه از این کابل را مشاهده می‌کنید.



شکل ۲- ۱ کابل Thinnet



شکل ۲- ۲ کابل Thinnet

کابل نوع Thicknet

Thicknet یک کابل coaxial ضخیم به قطر ۰/۵ اینچ است. هرچه هسته‌ی مس ضخیم‌تر باشد، به همان اندازه کابل می‌تواند سیگنال را به فاصله‌ی طولانی‌تر حمل کند. این بدین معناست که کابل‌های Thicknet سیگنال را بیشتر از کابل‌های Thinnet می‌توانند حمل کنند. کابل Thicknet می‌تواند سیگنال را تا ۵۰۰ متر حمل کند. توجه داشته باشید که به این کابل Ethernet هم می‌گویند، چون برای اولین بار در این شبکه استفاده شده است. به دلیل اینکه این کابل می‌تواند در فاصله‌ی دورتر سیگنال را انتقال دهند. معمولاً از آن به عنوان ارتباط‌دهنده‌ی چندین شبکه محلی استفاده می‌کنند. به این موضوع هم توجه داشته باشید که

www.takbook.com

این کابل برای انتقال تصاویر متحرک و صوت در فواصل دور استفاده می‌شود، شکل ۲-۳ نمونه‌ای از کابل‌های Thicknet را نشان می‌دهد.



شکل ۲- ۳ کابل *Thicknet*

انواع connectorهایی که در کابل Coaxial استفاده می‌شوند را می‌توانید در شکل ۲-٤ مشاهده کنید.



شکل ۲- ۴ *connector* کابل *Thicknet*

کارت شبکه‌ای که برای این کابل استفاده می‌شود، مخصوص همین کابل طراحی شده است. به شکل ۲-۵ توجه کنید.



شکل ۲- ۵ کارت شبکه‌ی کابل *Thicknet*

www.takbook.com

برای ارتباط کابل Thinnet به کابل Ticknet از وسیله‌ای به نام Tranciver استفاده می‌شود که شکل ۲–۶ را مشاهده می‌کنید.



شکل ۲- ۶ *Tranciver*

همان‌طور که گفتیم حداکثر طول انتقال سیگنال‌ها توسط این دو نوع کابل coaxial، 185 و 500 متر است و بعد از آن بر روی آن noise تأثیرگذار می‌شود و عملاً کابل از مسیر خارج می‌شود. برای حل این مشکل از وسیله‌ای به نام Repeater استفاده می‌کنند که سیگنال‌ها را تقویت می‌کند و به کابل بعدی می‌فرستد که در شکل ۲–۷ این دستگاه را مشاهده می‌کنید.



شکل ۲- ۷ *Repeater*

۲–۱–۲ کابل Twisted-pair یا زوج به هم تابیده

کابل زوج تابیده (Twisted Pair Cable) به عنوان یکی از اصلی‌ترین اجزای زیرساخت شبکه، نقش بسیار مهمی در ارتباطات دیتا و مخابرات ایفا می‌کند. این نوع کابل از دو رشته سیم مسی تشکیل شده که به صورت تابیده شده‌اند. تابیدن این سیم‌ها به صورت خاص طراحی شده است تا چندین مزیت را به ارمغان بیاورد.

در ساده‌ترین شکل، کابل Twisted-pair دارای یک زوج سیم به هم تابیده از مس که دارای روکش است.

دو نوع کابل Twisted-pair وجود دارد:

- روکش‌دار یا STP (Shielded Twisted-pair)
- بدون روکش یا UTP(Unshielded Twisted-pair)

www.takbook.com

این کابل از noiseهای مزاحم با استفاده از پیچیدگی‌هایی که دارد جلوگیری می‌کند، البته استاندارد ساخت این کابل‌ها برای کارخانه‌ها مهم است. اگر این کابل‌ها به‌درستی تابیده نشوند، به مشکل بر می‌خورند.

کابل روکش‌دار یا (STP)

کابل روکش‌دار یا STP (Shielded Twisted Pair) یکی از انواع کابل‌های زوج تابیده است که دارای ویژگی‌های خاصی برای بهبود کیفیت سیگنال و کاهش تداخل الکترومغناطیسی می‌باشد.

این نوع کابل به هم تابیده شده، معمولاً توسط غلافی پوشیده می‌شوند تا در برابر امواج الکترومغناطیسی محافظت شوند. از آنجا که این غلاف‌ها فلزی هستند، می‌توانند نقش سیم ارت را نیز ایفا کنند، اما معمولاً این نوع کابل‌ها دارای رشته سیمی به همین منظور هستند که به آن، سیم تخلیه (drain wire) نیز می‌گویند، در شکل ۲-۸ این نوع کابل مشخص شده است.



شکل ۲- ۸ کابل STP

SSTP (Shielded Screened Twisted Pair) نوعی از کابل‌های شبکه است که برای کاهش تداخل‌های الکترومغناطیسی (EMI) و تداخل‌های رادیویی (RFI) طراحی شده است. این کابل‌ها معمولاً در محیط‌های صنعتی یا جاهایی که مقدار زیادی نویز الکترومغناطیسی وجود دارد، استفاده می‌شوند.

ویژگی‌های SSTP

- شیلد محافظ: SSTP دارای دو لایه محافظ است. اولین لایه محافظ به دور هر جفت سیم تابیده شده قرار می‌گیرد و لایه دوم به دور کل کابل قرار دارد. این دو لایه باعث می‌شود که نویزهای خارجی به کمترین حد خود برسد که در شکل ۲-۹ مشاهده می‌کنید.
- کاهش تداخل: این کابل‌ها به دلیل داشتن شیلدهای متعدد، تداخل بین جفت سیم‌ها و همچنین تداخل‌های خارجی را به حداقل می‌رسانند.

www.takbook.com

- کاربرد: کابل‌های SSTP معمولاً در محیط‌هایی که تداخل الکترومغناطیسی بالاست، مانند کارخانه‌ها، مراکز داده، و مناطق صنعتی استفاده می‌شوند.



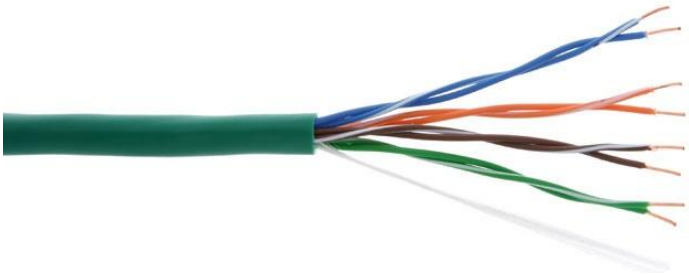
شکل ۲- ۹ ***SSTP Cable***

کابل‌های بدون روکش یا UTP (Unshielded Twisted-pair)

معمول‌ترین نوع کابل Twisted-pair، نوع بدون روکش آن است که مشخصه‌ی آن " 10 Base T " است که به‌عنوان یکی از محبوب‌ترین نوع کابل‌کشی برای شبکه‌ی LAN شناخته شد. این کابل‌ها در شبکه‌های امروزی استفاده می‌شود، مثلاً مودم ADSL شما از طریق همین کابل به کارت شبکه‌ی کامپیوتر شما متصل می‌شود.

شما می‌توانید این کابل‌ها را در سیستم‌های تلفن خانگی و اداره‌ی مخابرات مشاهده کنید که تمامی از این نوع کابل‌ها استفاده می‌کنند.

این نوع کابل‌ها، بسیار نازک و انعطاف‌پذیر است و به خاطر کوچک بودنشان برای سیم‌کشی به‌صرفه است، اما در برابر ضربه زیاد دوام ندارد، در شکل ۲–۱۰ این نوع کابل مشخص شده است.



شکل ۲- ۱۰ *UTP Cable*

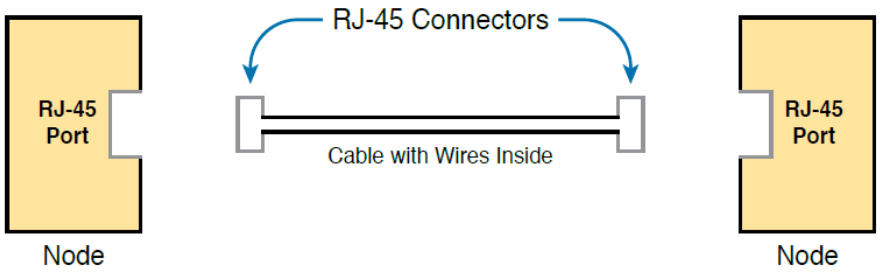
در جدول ۱–۱ انواع کابل‌های UTP (Unshielded Twisted Pair) را همراه با توضیحاتی درباره هر نوع و کاربردهای مرتبط با آن ارائه می‌دهم. در نظر داشته باشید که هر نوع کابل UTP ویژگی‌ها و استانداردهای خاص خود را دارد که در انتخاب آن‌ها برای کاربردهای مختلف تأثیرگذار است.

www.takbook.com

جدول ۲- ۱ کابل‌های UTP

نوع کابل	سرعت انتقال داده	حداکثر طول	کاربردها
Cat 5	حداکثر ۱۰۰ مگابیت بر ثانیه	100متر	شبکه‌های محلی (LAN) و تلفن‌های آنالوگ
Cat 5e	حداکثر ۱ گیگابیت بر ثانیه	100متر	اترنت گیگابیتی، تلفن‌هایVoIP ، دوربین‌های مدار بسته(CCTV)
Cat 6	حداکثر ۱۰ گیگابیت بر ثانیه	55متر (در ۱۰ گیگابیت)	شبکه‌های با پهنای باند بالا، کاربردهای تجاری و صنعتی
Cat 6a	حداکثر ۱۰ گیگابیت بر ثانیه	100متر	شبکه‌های با نیاز بالا، انتقال داده‌های ویدئویی
Cat 7	حداکثر ۱۰ گیگابیت بر ثانیه	100متر	محیط‌های با نویز بالا، دیتاسنترها و اتصالات پیشرفته
Cat 8	حداکثر ۲۵-۴۰ گیگابیت بر ثانیه	30متر	دیتاسنترها و کاربردهای با نیاز پهنای باند بسیار بالا

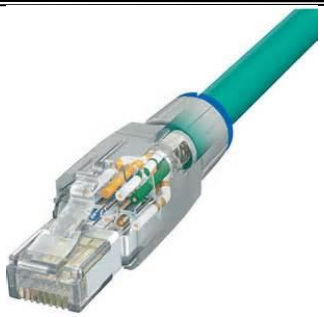
در اکثر مواقع برای متصل شدن کلاینت‌ها به هم از این نوع کابل‌ها (Cat5, Cat5e, Cat6) استفاده می‌شود، در دو سر هر کابل یک کانکتور RJ45 نصب می‌شود و این کانکتور وارد کارت شبکه متصل به کلاینت می‌شود که در شکل ۲-۱۱ این موضوع را مشاهده می‌کنید.



شکل ۲- ۱۱ RJ-45 Connectors

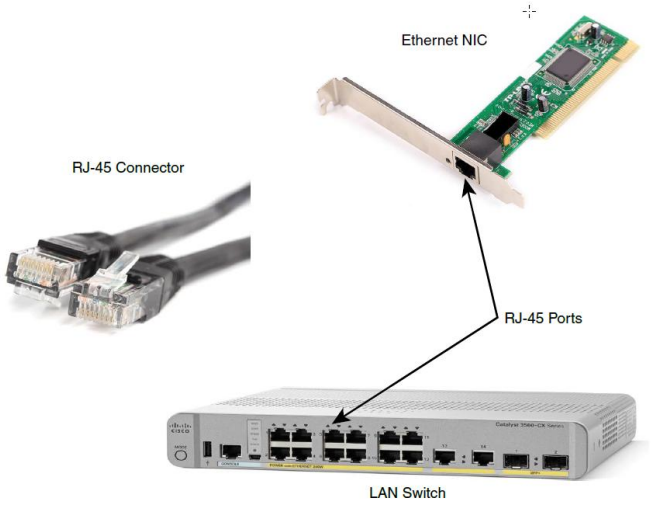
کانکتورهای استاندارد برای کابل‌های UTP در شبکه‌های LAN به نام RJ45 هستند که در شکل ۲-۱۲ آن را مشاهده می‌کنید.

www.takbook.com



شکل ۲-۱۲ *Socket*

در شکل ۲-۱۳ کارت شبکه، سوئیچ و کابل RJ45 را مشاهده می‌کنید که نحوه ارتباط آنها مشخص شده است.



شکل ۲-۱۳ *Connection*

۲-۱-۳ سوکت زدن دو سر کابل با RJ45

برای اینکه بر روی کابل‌های UTP یا STP کانکتور RJ45 بزنیم باید به دو دسته کابل توجه کنیم که نحوه ارتباط آنها متفاوت است.

- Straight (به صورت مستقیم – برای دستگاه‌های غیرمشابه)
- Cross (برای به هم بستن دستگاه‌های شبیه به هم)

نکته مهم : در شبکه‌های امروزی در بیشتر دستگاه‌ها کابل Straight کاربرد دارد و دستگاه‌ها به راحتی به همدیگر متصل می‌شوند و نیازی به استفاده از کابل Cross نیست.

www.takbook.com

کابل Straight

سوکت زدن دو سر کابل با RJ45 (Registered Jack 45) یکی از مراحل مهم در ایجاد اتصالات شبکه است. این نوع سوکت معمولاً برای کابل‌های UTP و STP استفاده می‌شود و برای اتصال به دستگاه‌هایی مانند روتر، سوئیچ، و کامپیوترها به کار می‌رود.

برای شروع حدود ۲ تا ۳ سانتی‌متر از عایق بیرونی کابل را با کاتر جدا کنید. دقت کنید که به رشته‌های سیم داخلی آسیب نزنید، در شکل ۲-۱۴ این موضوع را مشاهده می‌کنید.



شکل ۲-۱۴ ابزار کاتر

در ادامه، مراحل سوکت زدن دو سر کابل با RJ45 را توضیح می‌دهم:

جدول ۲-۲ Straight Cable

کابل طرف سوئیچ		رنگ‌بندی	کابل طرف کامپیوتر	
سفید نارنجی	(+TD)		(+TD)	سفید نارنجی
نارنجی	(–TD)		(–TD)	نارنجی
سفید سبز	(+RD)		(+RD)	سفید سبز
آبی	(NC)		(NC)	آبی
سفید آبی	(NC)		(NC)	سفید آبی
سبز	(–RD)		(–RD)	سبز
سفید قهوه‌ای	(NC)		(NC)	سفید قهوه‌ای

www.takbook.com

قهوه‌ای	(NC)		(NC)	قهوه‌ای

نکته : برای کابل‌های UTP، معمولاً از دو استاندارد T568A یا T568B استفاده می‌شود. ترتیب رنگ‌ها به شرح زیر است:

T568A

- سفید–سبز
- سبز
- سفید–نارنجی
- آبی
- سفید–آبی
- نارنجی
- سفید–قهوه‌ای
- قهوه‌ای

T568B

- سفید–نارنجی
- نارنجی
- سفید–سبز
- آبی
- سفید–آبی
- سبز
- سفید–قهوه‌ای
- قهوه‌ای

ترتیب رنگ‌ها باید در هر دو سر کابل یکسان باشد، منظور این است که اگر از استاندارد T568B استفاده می‌کنید باید در طرف مقابل هم دقیقاً از استاندارد رنگبندی T568B استفاده کنید.

رشته‌ها را در سوکت RJ45 به آرامی وارد کنید. دقت کنید که هر رشته به درستی در جای خود قرار گیرد و سوکت کاملاً به رشته‌ها بچسبد.

از دستگاه سوکت زن استفاده کنید تا سوکت RJ45 به کابل بچسبد. این کار باعث می‌شود که اتصالات محکم و پایدار باشند.

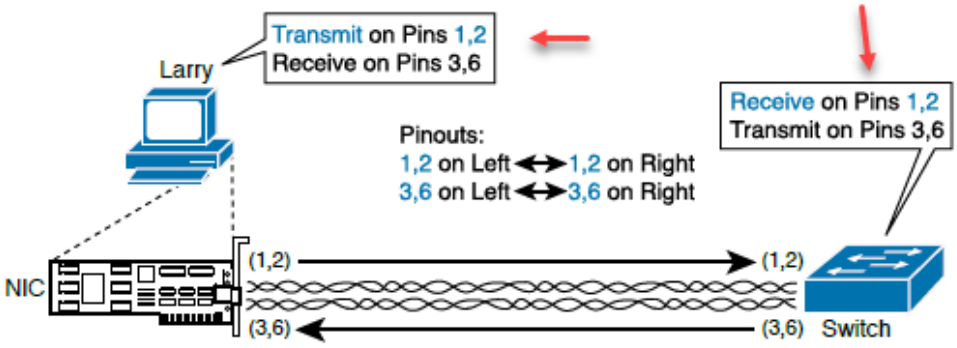
www.takbook.com

از دستگاه کابل تستر استفاده کنید، تا مطمئن شوید که اتصالات به درستی انجام شده‌اند و کابل به درستی کار می‌کند، در شکل ۲-۱۵ این دستگاه را مشاهده می‌کنید



شکل ۲- ۱۵ کابل تستر

اگر به شکل ۲-۱٦ توجه کنید متوجه ارتباط دو دستگاه سوئیچ و کلاینت خواهید شد، نحوه‌ی ارتباط این دو دستگاه به این صورت است که برای دریافت و ارسال اطلاعات از طریق کابل فقط از رشته‌های شماره‌ی 1,2,3,6 استفاده می‌کنند، به این صورت که مثلاً کلاینت برای ارسال اطلاعات از رشته‌ی 1,2 استفاده می‌کند و سوئیچ از 3,6 و همین‌طور برعکس آن برای دریافت انجام می‌شود.



شکل ۲- ۱۶ Connection

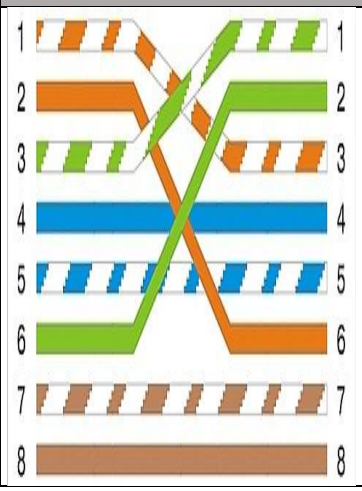
کابل Cross

کابل Cross (Cross-over Cable) نوعی کابل شبکه است که برای اتصال مستقیم دو دستگاه مشابه به یکدیگر استفاده می‌شود. به طور معمول، این نوع کابل برای اتصال دو کامپیوتر یا دو سوئیچ به کار می‌رود، بدون نیاز به یک سوئیچ یا روتر. در زیر، اطلاعات بیشتری درباره کابل Cross و کاربردهای آن ارائه می‌دهم:

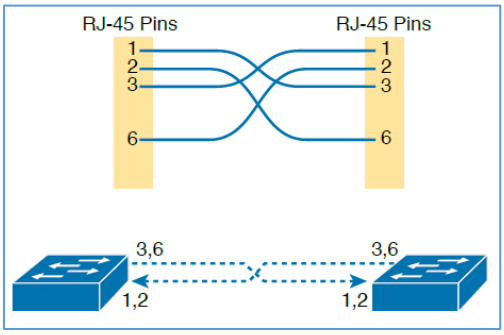
ترتیب سیم‌ها در دو سر کابل Cross را در جدول ۱-۳ مشاهده میکنید.

www.takbook.com

جدول ۲-۳ Cable Cross

کابل طرف PC2		رنگ‌بندی	کابل طرف PC1	
سفید سبز	(+TD)		سفید نارنجی	(+TD)
سبز	(–TD)		نارنجی	(–TD)
سفید نارنجی	(+RD)		سفید سبز	(+RD)
آبی	(NC)		آبی	(NC)
سفید آبی	(NC)		سفید آبی	(NC)
نارنجی	(–RD)		سبز	(–RD)
سفید قهوه‌ای	(NC)		سفید قهوه‌ای	(NC)
قهوه‌ای	(NC)		قهوه‌ای	(NC)

این رنگ‌ها در همه‌ی کابل‌ها ثابت است و یک استاندارد است که همه‌ی کارخانه‌های تولیدی، آن را پیروی می‌کنند. در شکل ۲–۱۷ طبق رنگبندی که در بالا مشاهده کردید، ارتباط کمی متفاوت است و پین شماره‌ی ۱ به ۳ و پین شماره‌ی ٦ به ۲ و برعکس متصل می‌شود که این موضوع نکته‌ی مهم این کار است.



شکل ۲-۱۷ *Crossover Ethernet Cable*

در جدول ۱–٤ نحوه‌ی ارتباط دو دستگاه را از طریق کابل مربوطه مشاهده می‌کنید:

جدول ۲-۴ *Cable Connection*

	هاب	سوئیچ	روتر	کامپیوتر
هاب	Crossover	Crossover	Straight	Straight
سوئیچ	Crossover	Crossover	Straight	Straight
روتر	Straight	Straight	Crossover	Crossover
کامپیوتر	Straight	Straight	Crossover	Crossover

www.takbook.com

نکته: کامپیوترهایی که از یک برند کارت شبکه استفاده می‌کنند می‌توانند با کابل Straight هم به هم متصل شوند.

٤-١-٢ کابل Serial

کابل Serial، نوعی کابل است که برای انتقال داده‌ها به صورت سریالی، یعنی انتقال یک بیت داده در هر زمان، استفاده می‌شود. این نوع کابل به ویژه در ارتباطات بین دستگاه‌ها و تجهیزات مختلف، مانند کامپیوترها، پرینترها، و تجهیزات شبکه، کاربرد دارد. در ادامه، جزئیات بیشتری درباره کابل Serial و کاربردهای آن ارائه می‌دهم.

انتقال داده‌ها: در کابل‌های سریال، داده‌ها به صورت خطی (سریالی) و یک بیت در هر زمان منتقل می‌شوند. این فرآیند باعث می‌شود که کابل‌ها به تعداد کمتری رشته نیاز داشته باشند.

پروتکل‌ها: کابل‌های سریال معمولاً با پروتکل‌های خاصی کار می‌کنند، مانند RS-232، RS-422 و RS-485. هر یک از این پروتکل‌ها ویژگی‌ها و کاربردهای خاص خود را دارند.

در زیر انواع کابل Serial را با هم بررسی می‌کنیم:

کابل RS-232

یکی از رایج‌ترین نوع کابل‌های سریال است و به طور معمول برای اتصال کامپیوترها به تجهیزات جانبی مانند مودم‌ها و پرینترها استفاده می‌شود، دارای ۹ یا ۲۵ پین است و می‌تواند فاصله‌های تا ۱۵ متر را پشتیبانی کند که در شکل ۲-۱۸ این کابل را مشاهده می‌کنید.

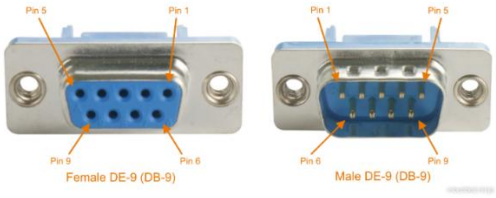


شکل ۲- ۱۸ کابل RS-232

کابل RS-422

این نوع کابل برای انتقال داده‌ها در فواصل طولانی‌تر و با سرعت‌های بالاتر طراحی شده است، می‌تواند فاصله‌های تا ۱۲۰۰ متر را با سرعت‌های حداکثر ۱۰ مگابیت بر ثانیه پشتیبانی کند.

www.takbook.com



شکل ۲- ۱۹ کابل *RS-422*

کابل RS-485

این کابل معمولاً در سیستم‌های صنعتی و ارتباطات چند نقطه‌ای استفاده می‌شود.

می‌تواند تا ٤٠٠٠ فوت (تقریباً ۱۲۰۰ متر) فاصله را پشتیبانی کند و به چندین دستگاه اجازه می‌دهد تا در یک حلقه ارتباط برقرار کنند.

دو مفهوم کلی برای کابل‌های سریال وجود دارد:

- DTE (Data Terminal Equipment)
- DCE (Data Communications Equipment)

DTEها از یک کانکتور ۹ پین یا ۲۵ پین که به این کانکتور مادگی می‌گویند تشکیل می‌شوند و طرف دیگر DTE هم به همین صورت است که از یک کانکتور ۹ پین یا ۲۵ پین استفاده می‌کند که به آن نری می‌گویند که در شکل ۲-۲۰ هر دو پین ۹ و ۲۵ را مشاهده می‌کنید.



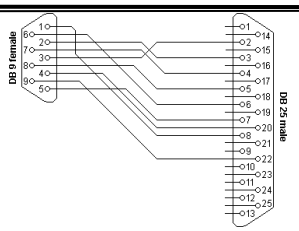
شکل ۲- ۲۰ *DTE Serial Cable*

تفاوت DCE با DTE

تفاوت این دو در این است که طرف کابلی که DTE است، مربوط به شبکه‌ی خودمان است و طرف دیگر که DCE است مربوط به مخابرات و یا همان Service Provider است که آن‌طرفی که DCE است، باید روی آن سرعت یا همان Clock Rate را تنظیم کند.

در شکل ۲-۲۱ نحوه‌ی بستن کابل‌های ۹ پین و ۲۵ پین را مشاهده می‌کنید.

www.takbook.com



شکل ۲- ۲۱ تفاوت DCE با DTE

کابل‌های سریال به انواع مختلفی تقسیم می‌شوند که در زیر انواع آن‌ها را مشاهده می‌کنید

کابل DTE Smart Serial

کابل DTE Smart Serial نوعی کابل سریال است که به طور خاص برای اتصال دستگاه‌های DTE (Data Terminal Equipment) به تجهیزات DCE (Data Communication Equipment) طراحی شده است. این نوع کابل معمولاً در شبکه‌های صنعتی، تجهیزات نظارتی و ارتباطات داده‌ای استفاده می‌شود.



شکل ۲- ۲۲ DTE Smart Serial Cables

کابل DCE Smart Serial

کابل DCE Smart Serial نوعی کابل سریال است که به طور خاص برای اتصال دستگاه‌های DCE (Data Communication Equipment) به تجهیزات DTE (Data Terminal Equipment) طراحی شده است. این کابل‌ها معمولاً برای تسهیل ارتباطات داده‌ای در شبکه‌های صنعتی، تجهیزات نظارتی و سایر سیستم‌های ارتباطی استفاده می‌شوند، این کابل را در شکل ۲-۲۳ مشاهده می‌کنید.



شکل ۲- ۲۳ DCE Smart Serial Cables

www.takbook.com

۵-۱-۲ کابل E1

کابل E1 یکی از استانداردهای انتقال داده در شبکه‌های مخابراتی است که برای انتقال داده‌ها با سرعت بالا استفاده می‌شود. استاندارد E1 بخشی از سیستم‌های PDH (Plesiochronous Digital Hierarchy) است که برای انتقال اطلاعات دیجیتال در شبکه‌های تلفنی و دیتا به کار می‌رود.

مشخصات کابل E1:

سرعت انتقال

- E1 توانایی انتقال داده با سرعت ۲.۰۴۸ مگابیت بر ثانیه را دارد. این سرعت در اصل برای ارتباطات تلفنی و انتقال صدا طراحی شده بود، اما امروزه برای انتقال داده در شبکه‌های مختلف هم استفاده می‌شود.

کانال‌ها

- یک لینک E1 شامل ۳۲ کانال است که هر کدام از این کانال‌ها دارای ظرفیت انتقال ٦٤ کیلوبیت بر ثانیه هستند.
- از این ۳۲ کانال، ۳۰ کانال برای انتقال داده یا صوت استفاده می‌شود. یک کانال برای سیگنالینگ (کنترل ارتباطات) و یک کانال دیگر برای همزمان‌سازی استفاده می‌شود.

کاربردها

- مخابرات: کابل‌های E1 عمدتاً برای انتقال داده‌های صوتی و ارتباطات تلفنی بین مراکز مخابراتی استفاده می‌شوند.
- شبکه‌های داده: از کابل E1 برای اتصال شعب شرکت‌ها به دفاتر مرکزی و همچنین برای ارتباطات بین شهری و بین کشوری استفاده می‌شود.
- ارتباطات صوتی و تصویری: به دلیل پهنای باند مناسب، از این کابل‌ها برای ارتباطات ویدیویی و انتقال داده‌های صوتی با کیفیت بالا استفاده می‌شود.
- رابط‌های فیزیکی:

کابل‌های E1 معمولاً از کابل‌های مسی (Twisted Pair) یا فیبر نوری استفاده می‌کنند.

اتصالات معمولاً از کانکتورهای BNC برای کابل‌های هم‌محور (Coaxial) یا RJ-45 برای کابل‌های زوج سیم تابیده (Twisted Pair) استفاده می‌کنند.

www.takbook.com



شکل ۲- ۲۴ *E1 Cable*

۶-۱-۲ کابل Stacking

کابل Stacking نوعی کابل است که برای اتصال و شبکه‌بندی چندین سوئیچ به یکدیگر استفاده می‌شود تا آنها را به عنوان یک واحد واحد مدیریت کنیم. این روش به عنوان Stacking Switches یا "استک کردن سوئیچ‌ها" شناخته می‌شود. به کمک این کابل‌ها، چندین سوئیچ فیزیکی به صورت منطقی با هم ترکیب می‌شوند و به عنوان یک سوئیچ واحد کار می‌کنند. این نوع کابل‌ها عمدتاً در شبکه‌های سازمانی استفاده می‌شوند که نیاز به مقیاس‌پذیری، عملکرد بهتر و مدیریت آسان‌تر دارند.

مزایای استفاده از کابل Stacking

- افزایش ظرفیت شبکه

با استفاده از کابل‌های Stacking، می‌توان چندین سوئیچ را به هم متصل کرد و ظرفیت و پهنای باند شبکه را بدون نیاز به افزودن تجهیزات پیچیده افزایش داد.

- مدیریت ساده‌تر

با استک کردن سوئیچ‌ها، تمام سوئیچ‌های متصل به عنوان یک دستگاه واحد مدیریت می‌شوند. این یعنی به جای مدیریت جداگانه هر سوئیچ، می‌توانید کل استک را به صورت یک واحد تنظیم و کنترل کنید.

- افزایش قابلیت اطمینان

در صورت خرابی یک سوئیچ در استک، سایر سوئیچ‌ها به کار خود ادامه می‌دهند، که این موضوع موجب افزایش پایداری و کاهش زمان خرابی (Downtime) شبکه می‌شود.

- استفاده بهتر از پهنای باند

کابل‌های Stacking معمولاً سرعت‌های بالایی را ارائه می‌دهند (مثلاً ۱۰ گیگابیت بر ثانیه یا بیشتر)، که این امر امکان انتقال داده‌ها با سرعت بالا بین سوئیچ‌ها را فراهم می‌کند.

- مقیاس‌پذیری بالا

www.takbook.com

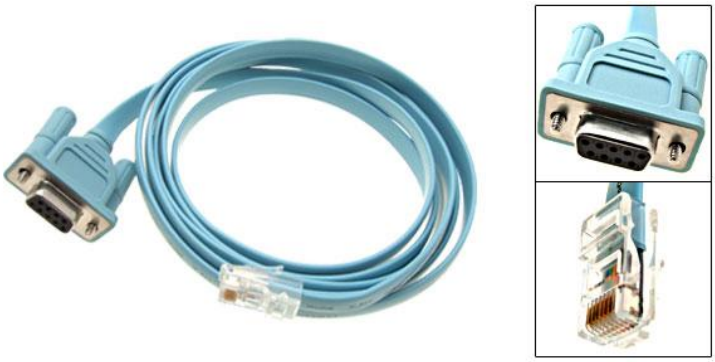
با کابل‌های Stacking، می‌توانید به راحتی سوئیچ‌های بیشتری به شبکه خود اضافه کنید، بدون اینکه نیاز به تغییرات اساسی در پیکربندی شبکه داشته باشید.



شکل ۲- ۲۵ ***Stacking Cable***

۲-۱-۷ کابل Console

این نوع کابل که یک‌طرف آن از کانکتور RJ45 و در طرف دیگر از پورت COM استفاده می‌کند و هم به رنگ آن در اکثر مواقع آبی است برای اتصال روتر یا سوئیچ به یک کامپیوتر برای تنظیم کردن روتر است.



شکل ۲- ۲۶ *Console Cable*

۲-۱-۸ کابل Octal

کابل Octal نوعی کابل شبکه است که در ارتباطات سریال برای اتصال چندین دستگاه شبکه به یک روتر یا سوئیچ استفاده می‌شود. این کابل به دلیل داشتن چندین پورت در یک سمت و یک کانکتور مرکزی در سمت دیگر، برای اتصال چندین دستگاه به یک پورت واحد مورد استفاده قرار می‌گیرد. معمولاً کابل Octal برای مدیریت پورت‌های کنسول (Console Ports) در تجهیزات شبکه مورد استفاده قرار می‌گیرد.

ساختار کابل Octal

www.takbook.com

- هشت شاخه (Octal): کابل Octal شامل هشت کابل مجزا است که در یک سمت به یک کانکتور واحد، مانند کانکتور RJ-45 یا DB-25، متصل می‌شوند و در سمت دیگر، هر کابل دارای یک کانکتور سریال (مانند RJ-45 یا DB-9) است.
- کانکتورها: در انتهای هر شاخه، معمولاً کانکتورهای سریال (مانند RJ-45 یا DB-9) قرار دارد که به پورت‌های کنسول تجهیزات شبکه (مانند سوئیچ‌ها، روترها و فایروال‌ها) متصل می‌شود.

کاربرد کابل Octal

- اتصال چندین دستگاه به یک روتر یا سوئیچ: این کابل معمولاً برای اتصال چندین دستگاه شبکه، مانند روترها یا سوئیچ‌ها، به یک دستگاه مدیریت مرکزی (مانند یک روتر یا سوئیچ مدیریتی) استفاده می‌شود.
- مدیریت پورت‌های کنسول: یکی از کاربردهای اصلی کابل Octal در پورت‌های کنسول تجهیزات شبکه است. با استفاده از این کابل، می‌توان چندین دستگاه را از طریق پورت کنسول مدیریت کرد. به عنوان مثال، در دیتاسنترها و مراکز شبکه، مدیران شبکه از این کابل برای اتصال همزمان چندین روتر یا سوئیچ به یک سیستم مدیریتی استفاده می‌کنند.
- صرفه‌جویی در پورت‌ها و کابل‌کشی: استفاده از کابل Octal باعث کاهش تعداد کابل‌ها و ساده‌سازی مدیریت تجهیزات شبکه می‌شود. به جای استفاده از چندین کابل مجزا برای اتصال دستگاه‌ها، کابل Octal این امکان را فراهم می‌کند که با استفاده از یک کابل واحد، چندین اتصال را برقرار کنید.



شکل ۲- ۲۷ کابل Octal

۹-۱-۲ فیبر نوری

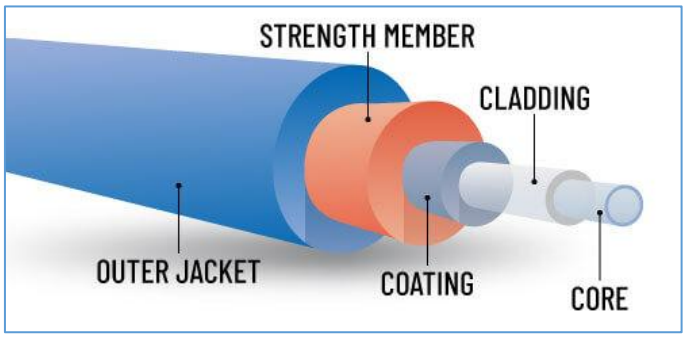
کابل‌های فیبرهای نوری تشکیل شده‌اند از یک استوانه‌ی شیشه‌ای بسیار نازک به نام هسته (Core) که توسط لایه‌ی ضخیم‌تر از شیشه پوشیده شده است که به این لایه، Cladding می‌گویند.

سرعت انتقال اطلاعات بر روی فیبر نوری، به خاطر استفاده از نور به‌جای سیگنال، خیلی سریع است.

فیبرهای نوری فقط یک‌طرفه هستند و امواج را از یک‌طرف ارسال می‌کنند، به همین دلیل در داخل آن از دو مسیر برای انتقال و دریافت استفاده می‌کنند.

www.takbook.com

یک فیبر نوری از پنج بخش متفاوت تشکیل شده است که در شکل ۲–۲۸ این بخش‌ها را مشاهده می‌کنید.



شکل ۲- ۲۸ *Optical Cable*

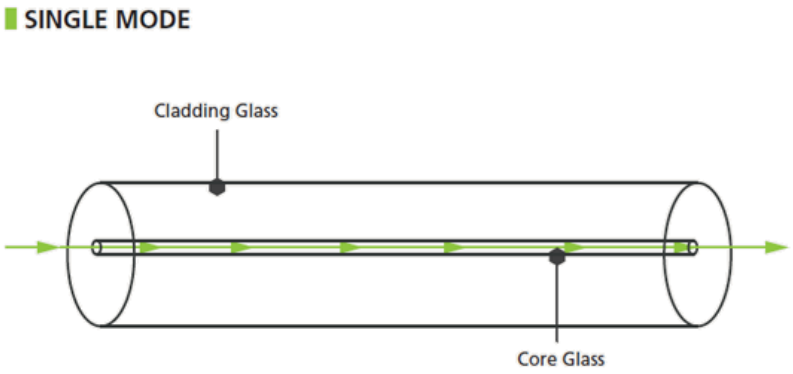
- هسته (Core): در مرکز کابل فیبر نوری یک لوله شیشه ای نازک به نام هسته (core) قرار دارد که پالس‌های نور تولید شده توسط لیزر یا دیود ساطع کننده نور (LED) را منتقل می‌کند. هسته‌های تک حالته معمولاً ۸.۳ یا ۹ میکرومتر هستند، در حالی که هسته‌های چند حالته در قطرهای ۵۰ و ٦۲.۵ میکرومتر موجود هستند.
- روکش (Cladding): لایه نازکی از شیشه که از هسته فیبر محافظت می‌کند و آن را احاطه می‌کند و نور را به داخل هسته بازتاب می‌دهد و باعث می‌شود امواج نور در طول فیبر حرکت کنند.
- پوشش اولیه (Buffer Coating یا Primary Coating): این لایه از پلاستیک ضخیم تر به عنوان بافر اولیه نیز شناخته می‌شود. برای جذب ضربه، جلوگیری از خم شدن بیش از حد و تقویت هسته فیبر، طراحی شده است.
- عضو استحکام یا الیاف تقویت‌کننده (Strength Member or Strengthening Fibers): در این نوع الیاف از ژل استفاده می‌شود تا کابل را در برابر نیروهای کششی و خرد شدن بیش از حد، به ویژه در حین نصب، جلوگیری کند.
- ژاکت بیرونی (Outer Jacket) – ژاکت بیرونی یا ژاکت کابل، آخرین لایه محافظتی را برای هادی هسته فراهم می‌کند و کابل را بیشتر تقویت می‌کند. ژاکت برای شناسایی نوع فیبر نوری در کابل دارای کد رنگی است: زرد برای حالت تک، نارنجی برای چند حالته و غیره. ژاکت‌های کابل همچنین دارای درجه‌بندی آتش مانند OFNR، OFNP یا LSZH هستند.

فیبرهای نوری در دو گروه عمده ارائه می‌گردند:

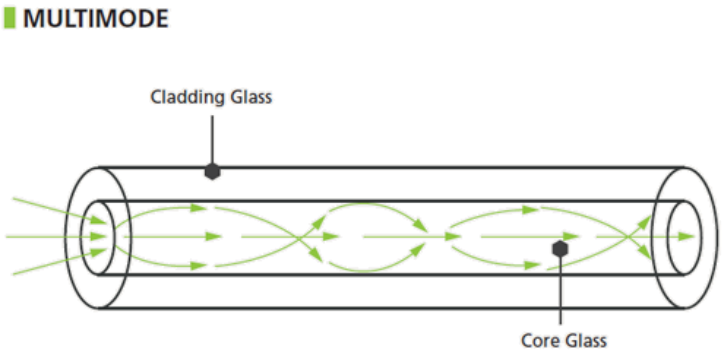
فیبرهای تک‌حالته (Single-Mode)

www.takbook.com

فیبرهای چندحالته (Multi-Mode)



شکل ۲- ۲۹ *Single Mode*



شکل ۲- ۳۰ *Multimode Mode*

تفاوت Single Mode و Multi Mode برای ارسال اطلاعات در شبکه به صورت زیر می‌باشد.

- منبع نور (source of light)

منبعی که نور را داخل آنها می‌تاباند، برای گروه Single mode نور لیزری مادون قرمز است و برای گروه multi Mode همان لیزر است که می‌تواند نورLED نیز باشد.

- سایز هسته (core size)

هسته Single Mode معمولاً ۸ تا ۹ دهم میکرون قطر دارد و هسته MultiMode معمولا ۵۰ تا ۶۲.۵ میکرون قطر دارد.

- مسافت ارسال اطلاعات در شبکه

www.takbook.com

همان‌طور که می‌دانیم در نوع Singl Mode فقط یک سیگنال ارسال می‌کند که می‌توانید در مسافت‌های بالا برای سرعت‌های بسیار زیاد استفاده کنید و در نوع multimode در شبکه‌هایی مانند دیتاسنتر استفاده می‌شود و هر چقدر قطر هسته بیشتر باشد؛ برای مسافت کمتر استفاده می‌شود و یا هر چقدر قطر هسته کمتر باشد؛ برای مسافت بیشتر مورد استفاده قرار می‌گیرد.

- طول موج (Wavelength)

Single mode حدوداً طول موج ۱۳۰۰ تا ۱۵۵۰ نانومتر و multimode حدوداً طول موج ۸۵۰ تا ۱۳۰۰ نانو متر را ساپورت می کند پس نتیجه می‌گیریم single mode طول موج بیشتری را نسبت به نوع multimode ساپورت می‌کند.

کابل‌های فیبر نوری از لحاظ طراحی، نحوه‌ی قرار گرفتن تارها و نوع پوشش به سه دسته کلی تقسیم می‌شوند:

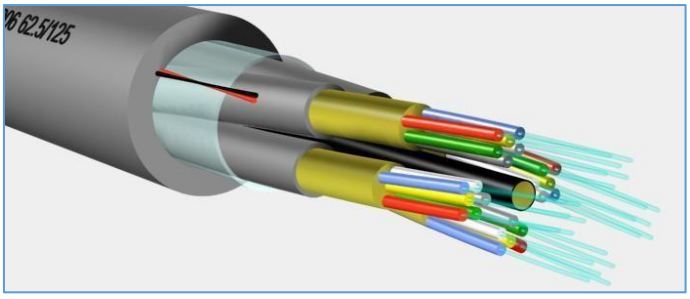
- Indoor (Tight Buffer)
- Outdoor (Loose tube)
- Indoor & Outdoor

اگر بخواهیم ریزتر به جزئیات نگاه کنیم، کابل فیبر نوری به سه دسته کلی تقسیم می‌شود:

- Breakout
- Distribution
- Interconnect

۱-۲-۶-۱ فیبرهای نوری Breakout

این کابل امکان خیلی کمی برای خم کردن دارد و چون از تعداد زیاد فیبر تشکیل شده است، این کابل را برای ارتباط Datacenterها مناسب کرده است. از این کابل‌ها برای زیر دریاها و زیر خاک استفاده می‌شود، چون مقاومت آن به علت لایه‌های متعدد محافظتی بسیار زیاد است. در زیر، شکل این کابل را مشاهده می‌کنید.

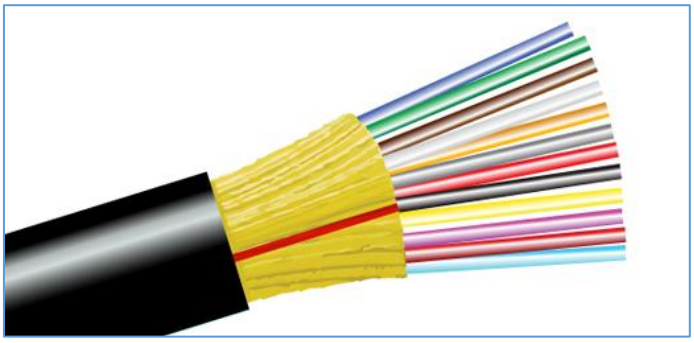


شکل ۲- ۳۱ Breakout Cable

www.takbook.com

۲-۶-۲-۱ فیبرهای نوری Distribution

این نوع کابل‌ها به نسبت کابل قبلی کمی خم می‌شوند و تعداد رشته‌ها در آن زیاد است و برای ارتباط کابل‌های Backbone با یک rack به کار می‌رود که شکل آن را می‌توانید مشاهده کنید.



شکل ۲-۳۲ *Distribution Cable*

۲-۶-۲-۱ فیبرهای نوری Interconnect

این نوع کابل که از یک پوشش پلاستیکی استفاده می‌کند، امکان خمش بالایی دارند و عموماً در داخل Rack استفاده می‌شود (Rack تجهیزاتی است که در داخل آن روتر، سوئیچ، فایروال و.... قرار می‌گیرد)، شکل ۲-۳۲ این نوع کابل را نشان می‌دهد.

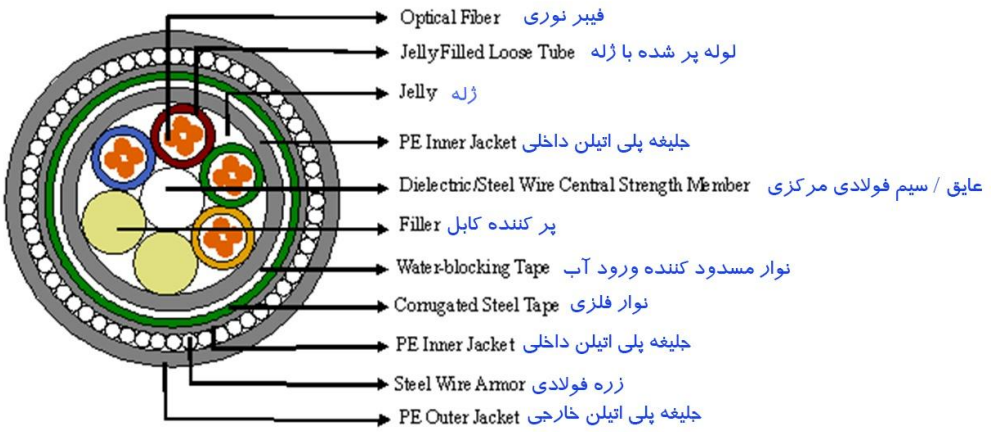


شکل ۲-۳۳ *Interconnect Cable*

www.takbook.com

٤-٦-٢-١ انواع لایه‌ها در فیبر نوری

فیبرهای نوری در درون خود از چندین لایه تشکیل شده‌اند که هرکدام از آن‌ها، کار خاصی را انجام می‌دهند.



شکل ۲-۳۴ Optical Cable Layers

همان‌طور که در شکل ۲-۳٤، مشاهده می‌کنید، انواع لایه‌های محافظ در این کابل وجود دارد که البته این کابل برای زیر دریاها و زیر خاک بسیار کاربرد دارد. ماده‌ی ژله‌ای که در این کابل وجود دارد، باعث می‌شود فیبر نوری داخل آن کمی متحرک باشد که اگر کمی خمیده شد، مشکلی برای آن پیش نیاید.

مزایای کابل فیبر نوری (Fiber Optic Cable) در مقابل کابل مسی (Copper Cable) به صورت زیر می‌باشد.

- سرعت انتقال داده‌ها بیشتر

فوتون‌هایی که با سرعت نور حرکت می‌کنند صد برابر سریع‌تر از الکترون‌هایی هستند که روی یک رسانای مسی حرکت می‌کنند. در مقایسه سرعت انتقال داده فیبر و مس، فیبر به راحتی برنده می‌شود. سرعت مس در حال حاضر ٤٠ گیگابیت در ثانیه است، در حالی که فیبر OM5 به سرعت ۱۰۰ گیگابیت در ثانیه می‌رسد، در مورد فوتون (photon) باید گفت که یک ذره ریز است که از امواج تابش الکترومغناطیسی تشکیل شده است. فوتون‌ها فقط میدان‌های الکتریکی هستند که در فضا حرکت می‌کنند. فوتون ها فاقد بار، جرم ساکن هستند و با سرعت نور حرکت می‌کنند.

- پهنای باند بیشتر

کابل‌های فیبر نوری نسبت به کابل‌های مسی ظرفیت پهنای باند بسیار بیشتری دارند و امکان انتقال داده‌های بیشتری را در یک زمان فراهم می‌کنند.

- فواصل انتقال طولانی‌تر

www.takbook.com

در مسافت‌های طولانی، کابل‌های مسی و فیبر هر دو از دست دادن سیگنال را تجربه می‌کنند، اما این تضعیف با مس بسیار بیشتر است. در ۱۰۰ متر، تخمین زده می‌شود که فیبر تنها ۳٪ از قدرت سیگنال خود را از دست می‌دهد، در حالی که مس ۹٤٪ را در همان فاصله از دست می‌دهد.

- مصونیت در برابر تداخل الکترومغناطیسی (EMI)

سیم‌های مسی میدان تداخل الکترومغناطیسی ایجاد می‌کنند که می‌تواند باعث خطاهای سیگنالینگ در کابل‌های دیگر شود. کابل‌های فیبر نوری جریان الکتریسیته را هدایت نمی‌کنند و به EMI حساس نیستند.

- جداسازی الکتریکی

از آنجایی که کابل های فیبر نوری برق را حمل نمی‌کنند، نیازی به زمین کردن فرستنده و گیرنده نیست. همچنین خطر برق گرفتگی، قوس الکتریکی، گرما یا آتش‌سوزی وجود ندارد.

- کابل سبک‌تر و نازک‌تر

کابل‌های فیبر نوری تقریباً یک چهارم قطر و یک دهم وزن کابل‌های مسی هستند که نصب آن‌ها را آسان‌تر می‌کند و باعث جریان بهتر هوا در محفظه‌های رک می‌شود.

- قابلیت اطمینان بهتر

کابل‌های فیبر نوری نسبت به کابل‌های مسی بادوام‌تر و کمتر آسیب‌پذیر هستند و به همین دلیل برای انتقال داده‌ها با سرعت بالا قابل اعتمادتر هستند.

- امنیت

کابل‌های فیبر نوری از کابل های مسی ایمن تر هستند زیرا انتقال داده برای کاربران غیرمجاز دشوار است.

- سازگار با محیط زیست

کابل‌های فیبر نوری از شیشه یا پلاستیک ساخته شده‌اند که مواد سازگار با محیط زیست هستند، در حالی که کابل‌های مسی از مس ساخته شده‌اند که منابع آن محدود است.

۲-۲ بررسی سوکت‌ها

در ادامه بررسی کابل‌ها می‌خواهیم انواع سوکت‌های دستگاه‌های الکترونیکی را با هم بررسی کنیم و مشخص کنیم که یک سوکت نری مربوط به کدام سوکت مادگی است.

۲-۲-۱ پورت HDMI

پورت HDMI (High-Definition Multimedia Interface) یک استاندارد صنعتی برای انتقال همزمان ویدئو و صدای دیجیتال با کیفیت بالا از یک دستگاه به دستگاه دیگر است. این پورت معمولاً در تلویزیون‌ها،

www.takbook.com

مانیتورها، پروژکتورها و سایر دستگاه‌های صوتی و تصویری یافت می‌شود، در جدول ۲-۵ پورت HDMI را مشاهده می‌کنید.

جدول ۲- ۵ پورت HDMI

شکل سوکت نری	شکل سوکت مادگی	نام	توضیحات
		Type A 13.9mm x 4.45mm	برای استفاده در تلویزیون‌های جدید، کامپیوترها و مانیتورها و ... کاربرد دارد.
		Type C Mini HDMI 10.42mm - 2.42mm	در دستگاه‌هایی مانند دوربین‌های دیجیتال، تبلیت و... استفاده می‌شود.
		Type D Micro HDMI 6.4mm – 2.8mm	برای استفاده در تبلت، دوربین دیجیتال و ... به کار می‌رود.

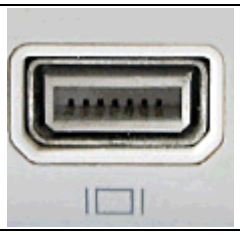
۲-۲-۲ پورت VGA

پورت VGA (Video Graphics Array) یک نوع اتصال آنالوگ است که به طور گسترده‌ای برای انتقال سیگنال‌های ویدئویی بین دستگاه‌ها، به ویژه بین کامپیوترها و نمایشگرها، استفاده می‌شود. این پورت به عنوان یکی از استانداردهای قدیمی و مهم در دنیای گرافیک کامپیوتری شناخته می‌شود، در جدول ۲-٦ پورت VGA را مشاهده می‌کنید.

جدول ۲- ۶ پورت VGA

شکل سوکت نری	شکل سوکت مادگی	نام	توضیحات

www.takbook.com

برای استفاده در مانیتورهای قدیمی و جدید، پروژکتور و...	VGA 17mm x 8.5mm		
استفاده در تب لت و لپ تاپ	MINI VGA 10.6mm - 5mm		

۳-۲-۲ پورت DVI

پورت DVI (Digital Visual Interface) یک استاندارد اتصال ویدئویی است که برای انتقال سیگنال‌های ویدئویی دیجیتال و آنالوگ بین کامپیوترها و نمایشگرها طراحی شده است. DVI به ویژه برای انتقال تصویر با کیفیت بالا به کار می‌رود و به عنوان یک پل میان فناوری‌های آنالوگ و دیجیتال شناخته می‌شود، در جدول ۲-۷ پورت DVI را مشاهده می‌کنید.

جدول ۲-۷ پورت DVI

شکل سوکت نری	شکل سوکت مادگی	نام	توضیحات
		DVI – A (Analogue) 25mm x 8mm	کامپیوترهای شخصی، مانیتور و تلوزیون
		DVI – D (Digital) 25mm x 8mm	کامپیوترهای شخصی، مانیتور و تلوزیون

www.takbook.com

		DVI - I (Analogue&Digital) 25mm x 8mm	کامپیوترهای شخصی، مانیتور و تلوزیون
		MINI DVI (Analogue&digital) 11.2mm x 7.1mm	کامپیوترهای شخصی، مانیتور و تلوزیون

۲-۲-٤ پورت DisplayPort

پورت DisplayPort یک استاندارد اتصال ویدئویی دیجیتال است که به طور خاص برای انتقال سیگنال‌های ویدئویی و صوتی با کیفیت بالا بین کامپیوترها، مانیتورها و سایر دستگاه‌ها طراحی شده است. این پورت به ویژه در محیط‌های حرفه‌ای و صنعتی و همچنین در نمایشگرهای با کیفیت بالا و کارت‌های گرافیک مدرن بسیار رایج است، در جدول ۲-۸ پورت DisplayPort را مشاهده می‌کنید.

جدول ۲- ۸ پورت DisplayPort

شکل سوکت نری	شکل سوکت مادگی	نام	توضیحات
		DisplayPort 17mm x 8.5mm	برای استفاده در کارت‌های گرافیک، کامپیوترهای Apple و...

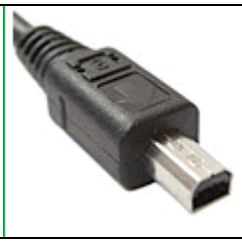
www.takbook.com

		MINI DisplayPort & Thunderbolt 7.5mm - 4.5mm	برای استفاده در نوت بوک Apple.

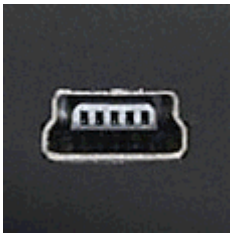
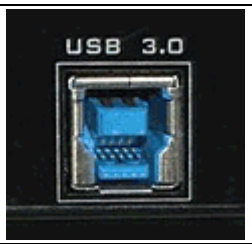
۵-۲-۲ پورت USB

پورت USB (Universal Serial Bus) یک استاندارد اتصال برای انتقال داده‌ها و تأمین برق بین دستگاه‌های الکترونیکی مختلف است. USB به عنوان یک رابط عمومی و جهانی برای اتصال و ارتباط بین دستگاه‌های کامپیوتری، موبایل، دوربین‌ها، چاپگرها و بسیاری از دستگاه‌های دیگر طراحی شده است، در جدول ۲-۹ پورت USB را مشاهده می‌کنید.

جدول ۲- ۹ پورت USB

شکل سوکت نری	شکل سوکت مادگی	نام	توضیحات
		USB Type A 12mm x 4.2mm	برای استفاده در ضبط ماشین، لپ تاپ، کامپیوتر و ...
		USB Type B 8mm x 7mm	برای استفاده در هارد دیسک اکسترنال، پرینتر و...
		Mini USB 4 pin 4.5mm x 3.5mm	برای دوربین های دیجیتال مانند شرکت Kodak و ..

www.takbook.com

هارد های قابل حمل، دوربین، موبایل و	Mini USB 5-pin 7mm x 3mm		
موبایل های اندرویدی، جی پی اس، تبلیت و...	Micro USB 7mm x 2mm		
کامپیوترهای شخصی، لپ تاپ، هارد و ..	USB 3.0 Type A 12mm x 4.2mm		
برای هاردهای اکسترنال، پرینتر و ...	USB 3.0 Type B 8mm x 10.5mm		
برای هاردهای اکسترنال، پرینتر و ...	USB 3.0 Micro B 12.5mm x 2mm		
	USB 3.1 Type-C 8.2mm x 2.4mm		

www.takbook.com

۶-۲-۲ پورت‌های کامپیوتر

در این قسمت پورت‌های مختلفی که بر روی کیس کامپیوتر شما قرار دارد را بررسی می‌کنیم.

پورت SATA (Serial ATA) یک استاندارد اتصال برای دستگاه‌های ذخیره‌سازی مانند هارد دیسک‌ها و SSDها (درایوهای حالت جامد) است. این پورت به منظور انتقال داده‌ها با سرعت بالا و بهبود کارایی در سیستم‌های کامپیوتری طراحی شده است.

eSATA (External Serial ATA) یک استاندارد اتصال است که برای اتصال دستگاه‌های ذخیره‌سازی خارجی، مانند هارد دیسک‌های خارجی و SSDها، به سیستم‌های کامپیوتری طراحی شده است. این استاندارد به گونه‌ای توسعه یافته که بتواند از مزایای سرعت SATA برای دستگاه‌های خارجی استفاده کند.

IDE (Integrated Drive Electronics) یک استاندارد اتصال برای هارد دیسک‌ها و درایوهای نوری است که به طور عمده در کامپیوترهای قدیمی‌تر استفاده می‌شود. این استاندارد به دستگاه‌های ذخیره‌سازی این امکان را می‌دهد که به مادربرد متصل شوند و به طور مستقیم از طریق رابط‌های IDE کنترل شوند.

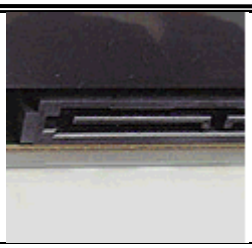
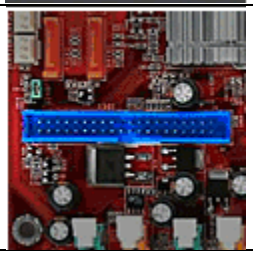
ROM Audio به طور کلی به نوعی حافظه فقط خواندنی (Read-Only Memory) اشاره دارد که برای ذخیره‌سازی داده‌های صوتی به کار می‌رود. این نوع حافظه معمولاً در دستگاه‌های صوتی و سیستم‌های الکترونیکی مختلف استفاده می‌شود.

FireWire 400 (همچنین به عنوان IEEE 1394a شناخته می‌شود) یک استاندارد اتصال برای انتقال داده‌ها است که به ویژه در دستگاه‌های صوتی و تصویری و همچنین در انتقال داده‌های سریع بین کامپیوترها و تجهیزات جانبی استفاده می‌شود، در جدول ۲-۱۰ پورت‌های مربوط به یک سیستم کامپیوتری را مشاهده می‌کنید.

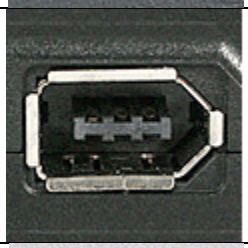
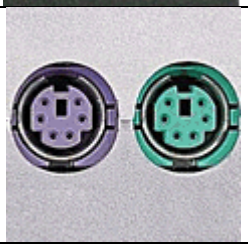
جدول ۲- ۱۰ پورت‌های کامپیوتر

شکل سوکت نری	شکل سوکت مادگی	نام	توضیحات
		SATA Data 14mm x 3.5mm	برای استفاده هارد دیسک، DVD RW و...

www.takbook.com

کابل برق مربوط به هارد دیسک، DVD RW و...	SATA Power		
رای هاردهای اکسترنال و قابل حمل که دارای سرعت انتقال ۳ گیگ است.	eSATA		
برای هارد و DVD rw قدیمی به کار می‌رود که در حاتل حاضر دیگر استفاده نمی‌شود.	IDE		
کابل برق مربوط به هارد دیسک، DVD RW که نوع قدیمی آن است.	Molex Power		
برای استاده در PC DVD and CD ROM	Rom Audio		
برای استفاده در نوت بوک Apple، دوربین دیجیتال و	Firewire 400 4-pin		

www.takbook.com

برای استفاده در نوت بوک Apple، دوربین دیجیتال و	Firewire 400 6-pin		
برای استفاده در نوت بوک Apple، دوربین دیجیتال و	Firewire 800		
			

www.takbook.com

www.takbook.com

فصل سوم

بررسی ابزار و دستگاه‌های شبکه

بعد از اینکه کابل‌ها و سوکت‌ها را با هم بررسی کردیم در این قسمت می‌خواهیم یک سری دستگاه‌های شبکه را با هم بررسی و تحلیل کنیم و یاد بگیرم هر کدام از این دستگاه‌ها چه کاربردی دارند.
ابزار و دستگاه‌های شبکه به مجموعه‌ای از سخت‌افزارها و تجهیزات اطلاق می‌شود که برای ایجاد، مدیریت و پشتیبانی از شبکه‌های کامپیوتری استفاده می‌شوند. این ابزارها نقش مهمی در انتقال داده، بهبود عملکرد شبکه و افزایش امنیت دارند. در ادامه، به برخی از مهم‌ترین ابزار و دستگاه‌های شبکه اشاره می‌کنیم.

۳-۱ مانیتور

عمومی‌ترین دستگاهی که می‌توان در هر سازمان پیدا کرد مانیتور است، مانیتورها دارای ویژگی‌های خاصی هستند، مانند سایز مانیتور، رنگ، پاسخگویی، پورت‌هایی که پشتیبانی می‌کنند و... مثلاً اگر بخواهید از مانیتور خود برای کارهای عمومی استفاده کنید، قطعاً کیفیت صفحه نمایش و سایز آن بسیار مهم خواهد بود.
مانیتورها را می‌توانید برای کارهای مختلف زیر خریداری کنید که هر کدام دارای ویژگی‌های خاص هستند.

۱- کار روزانه یا فعالیت‌های کامپیوتری عادی
۲- بازی‌های ویدئویی سطح بالا
۳- کارهای هنری/حرفه‌ای و طراحی گرافیک
۴- مانیتورهای چندمنظوره

در شکل ۳-۱، مانیتور سامسونگ مدل Curved S39C Essential را مشاهده می‌کنید که شکل منحنی دارد و ۲۷ اینچ است و برای اکثر کارها استفاده می‌شود.

www.takbook.com



شکل ۳ - ۱ مانیتور

اگر به تصویر پشت مانیتور در شکل ۳-۲ نگاه کنیم، این مانیتور دارای ٦ پورت است که هر کدام از آنها در عکس نوشته شده است، و وقتی یک مانیتور از پورت‌های بیشتری پشتیبانی کند قطعاً انتخاب بهتری برای کاربران خواهد بود.



شکل ۳ - ۲ مانیتور

در این مانیتور، سایز صفحه‌ی نمایش ۲۷ اینچ است و کیفیت تصویر آن Full HD 1080p است و تا ۱۹۲۰ x 1080 را پشتیبانی می‌کند.

برای انتخاب یک مانیتور خوب باید به ویژگی‌های زیر دقت کنیم:

۱- نوع پنل

هر مانیتور دارای پنل مشخص است که می‌توان به پنل‌های IPS, TN, VA اشاره کرد که بهترین فناوری را در حال حاضر در بازار ایران IPS دارد که یک تصویر درخشان و با کیفیت را ارائه می‌دهد.

www.takbook.com

۲- وضوع تصویر

مانیتورها دارای وضوع‌های مختلفی هستند مانند HD, FHD, QHD, 4K, 5K, 8K که در بین آنها 8K که به با نام اولترا اچدی شناخته می‌شود دارای ۷٦۸۰ در ٤۳۲۰ پیکسل هستند و برای بازی‌سازی و تدوین فیلم استفاده خواهد شد.

۳- اندازه صفحه نمایش

مانیتورهای دارای اندازه‌های مختلف هستنند مانند 21,23,27 و ... که باید بسته به نیاز خود آن را انتخاب کنید.

۴- فناوری به کار رفته

فناوری‌هایی که در مانیتورها استفاده شده را می‌توان به فناوری HDR، همگام‌سازی تطبیقی FreeSync در مقابل G-Sync و ... اشاره کرد.

۵- خمیده بودن یا صاف بودن

اگر می‌خواهید مانیتور را برای بازی استفاده کنید بهتر است یک مانیتور خمیده درجه یک خریداری کنید تا لذت بازی را درک کنید.

۲-۳ کیس

یکی از انتخاب‌های که می‌تواند به سلیقه‌ی شما ربط داشته باشد انتخاب کیس است، همان‌طور که می‌دانید کیس‌ها در سایزها وطراحی‌های مختلفی وجود دارند و باید یکی از آنها را انتخاب کنید، به این نکته توجه کنید که تمام کیس‌ها از یک استاندارد مشخص برای طراحی داخلی خود استفاده می‌کنند، مثلاً وقتی یک مادربرد خریداری می‌کنید و بخواهید آن را بر روی پنل نصب کنید فاصله پیچ‌ها دقیقاً در همه کیس‌ها برابر خواهد بود، اما در بعضی مواقع یک مادربرد بسیار کوچک است و یک مادربرد بسیار بزرگ و در یک کیس جا نمی‌شود و شما باید طبق مادربردی که خریداری می‌کنید، کیس مورد نظر خود را انتخاب کنید.

در شکل ۳-۳ یک کیس با طراحی زیبا از شرکت MSI را مشاهده می‌کنید.

www.takbook.com



شکل ۳ - ۳ کیس

یک کیس دارای فرم فاکتورهای مختلفی است که مربوط به مادربرد است و طبق آن باید کیس را تهیه کنید، اندازه‌های زیر از بزرگتر Extended ATX به کوچکتر Mini-ITX نوشته شده است.

- ✓ Extended ATX (E-ATX) 12-inch x 13-inch or 305mm x 330mm
- ✓ ATX 12-inch x 9.6-inch or 305mm x 244mm
- ✓ Micro-ATX (M-ATX) 9.6-inch x 9.6-inch or 244mm x 244mm
- ✓ Mini-ITX (Mini-ITX) 6.7-inch x 6.7-inch or 170mm x 170mm

یکی از مهمترین فاکتورهایی که یک کیس باید داشته باشد قطعاً قسمت خنک کننده‌ی آن است که این می‌تواند فن‌های مختلف در جاهای مختلف کیس باشد و یا اینکه از فناوری خنک کننده استفاده کنید، در شکل ۳-٤، یک کیس با اندازه Extended ATX را مشاهده می‌کنید که دارای فناوری خنک کننده مایع است و برای خنک کردن CPU و کارت گرافیک به کار می‌روند.

www.takbook.com



شکل ۳ - ۴ کیس

در ادامه می‌خواهیم دستگاه‌ها و ابزارهایی که داخل یک کیس استفاده می‌شود را بررسی کنیم تا از جزئیات کامل آن با خبر شویم و بتوانیم یک کیس را به صورت کامل پیاده‌سازی کنیم.

۳-۲-۱ مادربرد

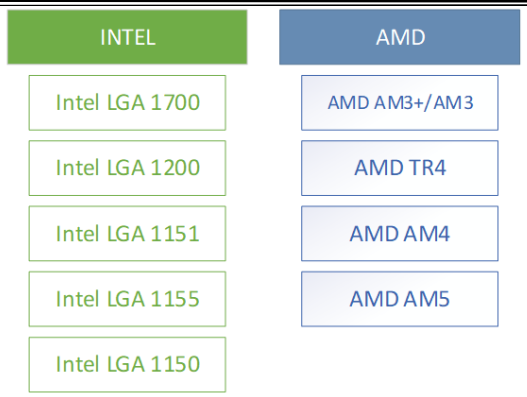
انتخاب مادربرد یکی از مهمترین کارهایی است که شما به عنوان مدیر شبکه باید انجام دهید، اول باید ببینید که این مادربرد را برای چه کاری نیاز دارید، بعد باید ببینید این مادربرد چه ادواتی را پشتیبانی می‌کند، مثلاً چه نوع CPU,Ram,Hard,Graphic و... در این قسمت به طور کامل آن را بررسی می‌کنیم.

برای انتخاب مادربرد به موارد زیر باید دقت کنید:

۳-۲-۱-۱ انتخاب سوکت پردازنده

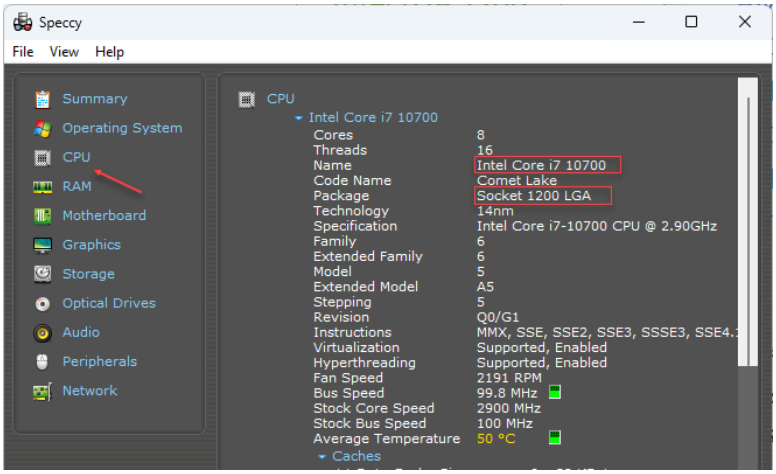
یکی از مهمترین فاکتورهای انتخاب یک مادربرد این است که باید ببینید که آن ماردبرد کدام یک از CPUهای INTEL یا AMD را پشتیبانی می‌کند، و بعد از انتخاب نوع پردازنده باید مشخص کنید که چه سوکتی را پشتیبانی می‌کند، در شکل ۳-۵، سوکت‌های مربوط به پردازنده‌های Intel و AMD را مشاهده می‌کنیم.

www.takbook.com



شکل ۳ - ۵ انتخاب سوکت پردازنده

این سوکت‌ها بدین معنا است که در زمان خرید پردازنده باید دقت کنید که شماره‌ی سوکت پردازنده با سوکت مادربرد یکی باشد وگرنه پردازنده شما بی‌مصرف خواهد بود و نمی‌توانید از آن استفاده کنید، اگر می‌خواهید به صورت دقیق سوکت پردازنده کامپیوتر خود را مشاهده کنید، می‌توانید از نرم‌افزار Speccy یا CPU-Z استفاده کنید، همان‌طور که در شکل ۳-۶ مشاهده می‌کنید، نرم‌افزار Speccy بر روی کامپیوتر من نصب شده و سری پردازنده به همراه شماره‌ی سوکت را مشخص کرده است.



شکل ۳ - ۶ نرم‌افزار Speccy

منظور از سری پردازنده همان نسل پردازنده است که حتماً این کلمه را شنیدید که می‌گویند پردازنده نسل ۱۱ و ... در شکل ۳-۶ در قسمت name مدل Intel Core i7 10700 نوشته شده است که شماره‌ی 10700 همان سری ۱۰ پردازنده است و باید به ان هم دقت کرد، در قسمت Package شماره‌ی سوکت LGA 1200 نوشته

www.takbook.com

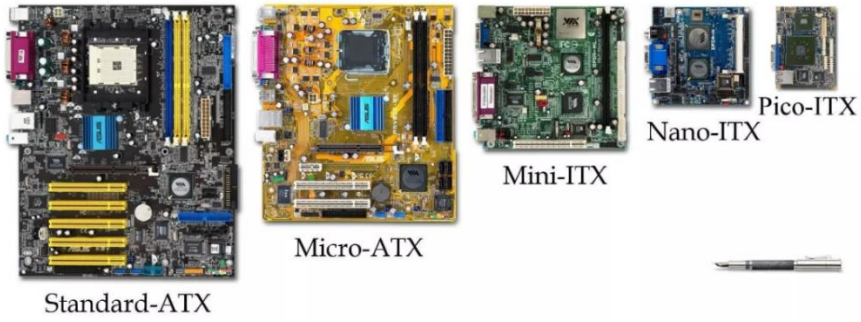
شده است، یعنی مادربرد سوکت 1200 LGA را پشتیبانی می‌کند و پردازنده‌ای که بر روی آن قرار دارد مربوط به همین سوکت است.

۳-۲-۱-۲ فرم فاکتور

همان‌طور که بیان کردیم وقتی که یک کیس را می‌خواهید خریداری کنید، باید به فاکتور فرم آن دقت کنید تا مادربردی که خریداری می‌کنید، در کیس مورد نظر جای شود.

دقیقاً همین موضوع در مادربرد هم وجود دارد و شما باید به فرم فاکتور آن دقت کنید تا با کیس مورد نظر هم‌خوانی داشته باشد.

به شکل ۳-۷ دقت کنید پنج نوع از مادربرد با فرم فاکتورهای مختلف را مشاهده می‌کنید که باید به اندازه‌های آن دقت کنید.



شکل ۳ - ۷ فرم فاکتور

در شکل ۳-۸، دقیقاً مشخص شده است که هر فرم فاکتور دارای چه ابعادی است، در قسمت ابعاد هم به صورت اینچ نوشتیم و هم به صورت سانتیمتر تا درک برای شما آسان‌تر باشد، توجه داشته باشید که فرم ATX یک فرم استاندارد است که بیشتر استفاده می‌شود و فرم Micro-ATX هم طرفدار خوبی دارد.

فرم فاکتور	سازنده و تاریخ	ابعاد
Standard-ATX	Intel 1995	12 × 9.6in 30 × 24.3cm
Micro-ATX	Intel 1997	9.6 × 9.6 in 24.3 × 24.3cm
Micro-ATX	VIA 2001	6.7 × 6.7 in 17.01 × 17.0.1cm
Nano-ITX	VIA 2003	4.7 × 4.7 in 11.93 × 11.93cm
Pico-ITX	VIA 2007	3.9 × 2.8 in 9.90 × 7.11cm
Mobile-ITX	VIA 2009	2.4 × 2.4 in 6.09 × 6.09cm

شکل ۳ - ۸ فرم فاکتور

www.takbook.com

۳-۱-۲-۳ اسلات‌های PCI

وقتی مادربرد تهیه می‌کنید بعد از آن اقدام به نصب کارت شبکه، کارت صدا و یا کارت‌های دیگر بر روی آن می‌کنید و باید به یک سری موارد دقت کنید، باید دقت کنید کارتی که می‌خرید آیا اسلات PCI در مادربرد این کارت را می‌پذیرد یا نه، برای این کار باید به اسلات PCI دقت کنیم، از قدیم تا به امروز این اسلات‌های PCI کاملاً تغییر کردند و باید دقیق مشخص شود به چه اسلاتی نیاز دارید.

در حالت کلی چهار نوع اسلات PCI در مادربردها وجود دارد که عبارت‌اند از:

- PCIهای ٦٤ بیتی
- PCIهای ۳۲ بیتی
- PCI-X سریع تر از PCI
- PCI Express (PCI-E)

در حال حاضر بهترین اسلات همان PCI Express است که دارای عملکرد دو طرفه است و بهترین سرعت و کیفیت را ارائه می‌دهد.

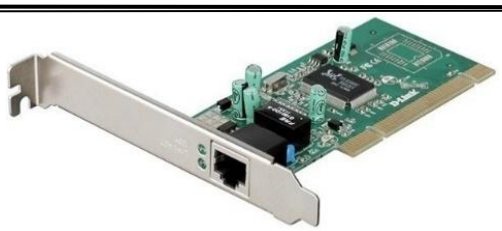
مثلاً کارت شکه بی‌سیم شکل ۳-۹ را در نظر بگیرید که دارای اسلات PCI Express است و در اکثر مادربردهای جدید به علت عملکرد بهتر و کم بودن فضایی که می‌گیرد از آن استفاده می‌کنند.



شکل ۳ - ۹ کارت شبکه بی‌سیم

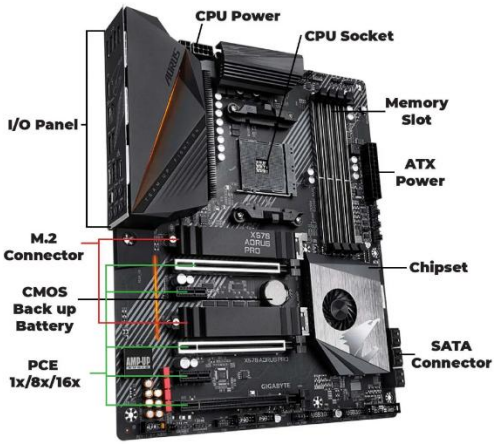
اما در مادربردهای قدیمی‌تر و بعضاً جدید از اسلات PCI که شکل ۳-۱۰ مربوط به همین اسلات است مشاهده می‌کنید.

www.takbook.com



شکل ۳ - ۱۰ کارت شبکه

به مادربرد شکل۳-۱۱ توجه کنید که اجزای مختلفی از آن به نمایش گذاشته شده است، اگر به قسمت PCI دقت کنید، پنج PCI وجود دارد که دو تا از آنها کوچک هستند و همان PCI Express هستند که به آنها PCI Express X1 می‌گویند و یکی دیگر از PCI Expressها که در شکل مشاهده می‌کنید و بزرگ است به آنها PCI Express X16 می‌گویند که مختص کارت گرافیک است.



شکل ۳ - ۱۱ مادربرد

یک نکته مهم هنگام نصب مادربرد بر روی کیس این است که قبل از نصب باید پیچ‌های برنجی که در شکل ۳-۱۲ مشاهده می‌کنید را بر روی مادربرد نصب کنید و بعد از آن مادربرد را بر روی آن قرار دهید، اگر این کار را نکنید مادربرد دچار اتصالی می‌شود و می‌سوزد.



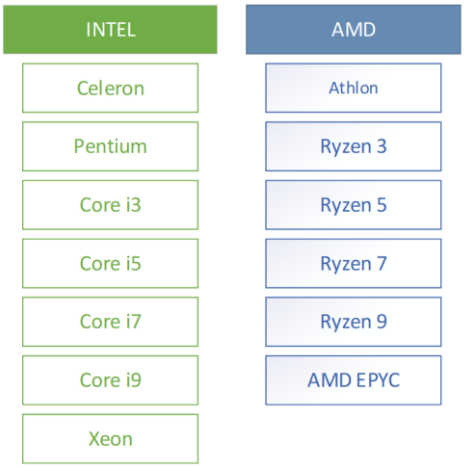
شکل ۳ - ۱۲ پیچ‌های برنجی

www.takbook.com

۳-۲-۲ پردازنده

CPU یکی از مهمترین سخت‌افزار موجود در کامپیوتر خواهد بود و باید درست انتخاب شود، قبل از هر کاری باید ببینید CPU را برای چه کاری نیاز دارید.

دو شرکت مهم در این زمینه INTEL و AMD هستند که هر کدام دارای ویژگی خاصی هستند، که آنها را با هم بررسی می‌کنیم، در شکل ۳-۱۳ سری‌های هر دو شرکت را مشاهده می‌کنید.



شکل ۳ - ۱۳ نوع پردازنده

اگر بخواهیم از نظر سهم بازار حساب کنیم، CPUهای شرکت INTEL دارای فروش بیشتری هستند و از نظر کیفیت هم شاید در مواردی مانند بازی‌های کامپیوتری عملکرد بهتری داشته باشند چون از اورکلاکینگ بهتری استفاده می‌کنند، ولی اگر بخواهیم از نظر هزینه حساب کنیم، CPUهای شرکت AMD از قیمت پایینتری برخوردار هستند و می‌توانند برای بودجه‌های کمتر مناسب‌تر باشند.

باید به این نکته اشاره کنیم که هر دو شرکت برای سرورها یک CPU مخصوص طراحی کردند که برای شرکت Intel با نام Xeon و برای شرکت AMD با نام AMD EPYC است که در جدول بالا هم مشخص است.

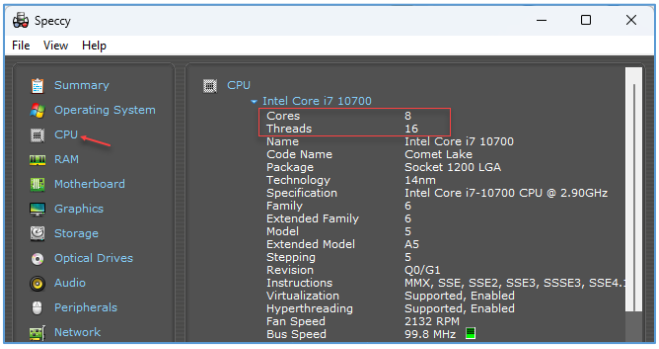
برای استفاده از CPU در سرور بهترین انتخاب از نظر بنده که تجربه چندین سال کار شبکه را دارم، مدل Xeon شرکت Intel است که دارای عملکرد فوق‌العاده است که شکل ۳-۱۴ یک مدل از این نوع است.

www.takbook.com



شکل ۳ - ۱۴ CPU

یک دیگر از فاکتورهای انتخاب، تعداد هسته‌های CPU است، هسته (Core) یک نوع پردازش در داخل پردازنده اصلی است که نقش قدرتمندی در محاسبات دارد، اگر دوباره وارد نرم‌افزار Speccy شویم و به قسمت CPU مراجعه کنیم، همان‌طور که در شکل ۳-۱۵ مشاهده می‌کنید تعداد Cores برابر با ۸ است و تعداد رشته (Threads) برابر با 16 است، تعداد رشته دو برابر Core است و رشته‌ها همیشه در Core کار می‌کنند و کار اصلی رشته‌ها این است که به پردازنده اجازه می‌دهند چندین کار را به صورت همزمان انجام دهند، در همین CPU که مقدار رشته برابر با ۱۶ است یعنی ۱۶ کار می‌تواند به صورت هم زمان انجام شود.



شکل ۳ - ۱۵ Speccy

و نکته آخر این است که برای خرید CPU و مادبرد باید به شماره‌ی سوکت و نسلی که مادربرد پشتیبانی می‌کند دقت کنید که در این مورد در قسمت مادربرد به صورت کامل صحبت کردیم.

در شکل ۳-۱۶ یک مادربرد ایسوس مدل TUF GAMING H770-PRO WIFI را مشاده می‌کنید که از سوکت LGA 1700 شرکت Intel پشتیبانی می‌کند، و برای این که CPU برای آن تهیه کنیم باید سوکت آن هم 1700 باشد که در شکل ۳-۱۶، CPU مدل Core i5-12400F Tray انتخاب شده است که نسل ۱۲ است و سوکت آن 1700 است.

www.takbook.com



شکل ۳ - ۱۶ CPU و مادبرد

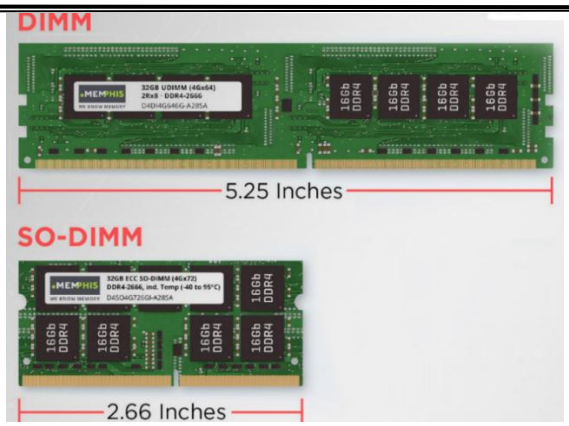
یک نکته مهم در انتخاب CPU این است که مثلاً اگر می‌خواهید از مدل INTEL استفاده کنید باید دقت کنید که در نام مدل حرف F نوشته شده است یا خیر، اگر نوشته باشد شما حتماً باید یک کارت گرافیک هم برای مادربرد خود خریداری کنید چون، CPU کارت گرافیک خود مادربرد را پشتیبانی نمی‌کند و باید جداگانه خریداری شود، در شکل ۳-۱۶، هم CPU دارای حرف F در مدل خود است و برای اینکه تصویر داشته باشید باید یک کارت گرافیک برای مادربرد خریداری کنید.

۳-۲-۳ رم

RAM یا Random Access Memory گونه‌ای از حافظه برای ذخیره‌سازی داده‌هاست که اجازه می‌دهد فایل‌ها در مدت زمانی کوتاه نوشته و خوانده شوند؛ بدون اینکه در این خواندن و نوشتن تقدم و تأخر زمانی اهمیتی داشته باشد، رم‌ها ارتباط مستقیم با CPU دارد و CPU زمانی که می‌خواهد یک برنامه را اجرا کند آن برنامه را در داخل رم قرار می‌دهد و رم چون سرعت بالایی دارد با قدرت و سرعت زیاد برنامه مورد نظر را اجرا می‌کند و همین موضوع باعث می‌شود که انتخاب رم بسیار فاکتور مهمی در یک سیستم باشد. انتخاب رم، ارتباط مستقیم با مادربرد دارد باید حتماً در جزئیّات مادربرد مشاهده کنید که این نوع مادربرد چه نوع رمی را پشتیبانی می‌کنند.

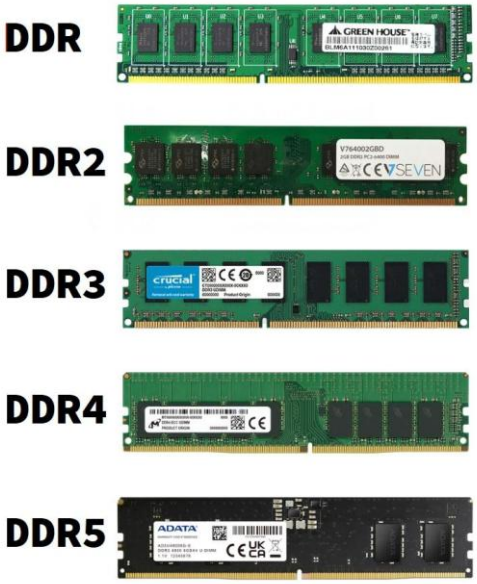
دو نوع رم برای کامپیوترهای شخصی و لپ‌تاپ داریم، نوع DIMM برای کامپیوترهای شخصی و رم SO-DIMM برای لپ‌تاپ کاربرد دارد که شکل ۳-۱۷ نشان دهنده‌ی این دو رم است، سایز مربوط به رم کامپیوتر برابر با ۵.۲۵ اینچ (۱۳.۳ سانتیمتر) و سایز مربوط به رم لپ‌تاپ برابر با ۲.۶۶ اینچ (۶.۷۶ سانتیمتر است)، پس برای خرید رم‌های لپ‌تاپ باید مدل SO-DIMM را انتخاب کنید تا مشکلی پیش نیاید.

www.takbook.com



شکل ۳ - ۱۷ رم

رم‌ها دارای ویژگی دیگری با نام DDR (Double Data Rate) به معنی انتقال اطلاعات دو برابر است، اکثر مردم برای خرید رم به قسمت DDR آن توجه می‌کنند که این قسمت حتماً باید با مادربرد شما هماهنگی داشته باشد، در شکل۳-۱۸، مدل‌های مختلف DDR را مشاهده می‌کنید، از ورژن یک تا ورژن ۵، برای شناسایی این نوع رم‌های باید به شکاف زیری آن دقت کنید که در شکل ۳-۱۸، هم مشخص شده است، در حال حاضر مدل DDR وجود ندارد، DDR 2 خیلی قدیمی است و شاید در سیستم‌های قدیمی وجود داشته باشد، ولی از DDR3 تا DDR5 در سیستم‌های امروزی وجود دارد که البته DDR4 بیشتر کاربرد را در این سال یعنی 2024 دارد.



شکل ۳ - ۱۸ انواع رم

www.takbook.com

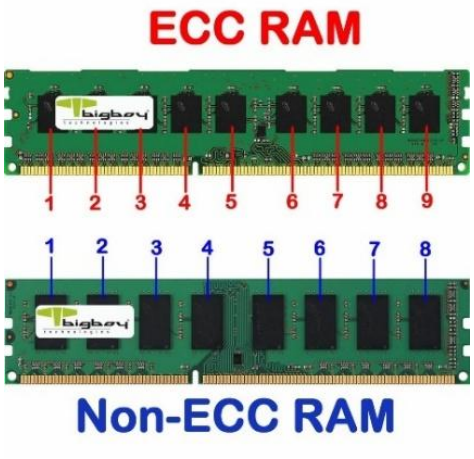
یکی دیگر از مهمترین ویژگی‌هایی که باید برای انتخاب رم درنظر گرفت، سرعت انتقال داده است که واحد آن مگاهرتز است که بسیار مهم خواهد بود، در شکل ۳-۱۹ رم شرکت VENGEANCE را مشاهده می‌کنید که یک رم ۳۲ گیگابایت DDR4 با سرعت ۳۲۰۰ مگاهرتز است که یک سرعت خیلی خوب را ارائه می‌دهد.
در هنگام خرید مادربرد دقیقاً نوشته است که حداکثر چه رمی با چه ظرفیت و سرعتی را پشتیابنی می‌کند، توجه داشته باشید اگر سرعت رم بیشتر از سرعت مادربرد باشد، مادربرد فقط تا جایی که می‌تواند از آن سرعت استفاده می‌کند، یعنی اینکه اگر مادربرد تا سرعت 2400 مگاهرتز را پشتیبانی کند و شما رم 3200 خریداری کنید، مادربرد تنها از همان 2400 مگاهرتز پشتیبانی خواهد کرد.
نکته‌ی دیگر که باید در انتها بگویم این است که سعی کنید رم‌ها را از یک شرکت خریداری کنید، مثلاً اگر بخواهید بر روی سیستم خود دو رم قرار دهید بهتر است دارای یک سرعت باشند و از یک برند باشند، در بعضی مواقع رم‌هایی که برای یک شرکت نباشند باعث ریست شدن سیستم می‌شوند.



شکل ۳ - ۱۹ انواع رم

یکی دیگر از انواع رم‌ها، رم سرور است که کاملاً با رم‌های دسکتاپی متفاوت است و دنیای دیگری برای خود دارند.
تکنولوژی به نام ECC (Error Correction Codes) یا همان تشخیص خطا وجود دارد که در رم‌های سرور تعبیه شده و این یکی از مهمترین تفاوت‌های رم سروی با رم دستکتاپ است.
با تکنولوژی ECC می‌توانیم امنیت اطلاعات خود را حفظ کنیم و در حین کار رمی که خراب باشد را تشخیص و تعویض کنیم.
برای تشخیص یک رم که ECC دارد یا نه به شکل ۳-۲۰ توجه کنید، اگر تعداد تراشه‌های موجود بر روی رم در هر دو طرف زوج باشد یعنی اینکه رم مورد نظر ECC ندارد ولی اگر یک طرف آن فرد باشد یعنی رم دارای ECC و تشخصی خطا است و می‌توانید از آن در سرور استفاده کنید.
توجه داشته باشید در ادامه کار به طور کامل نحوهی کار با سرور و قطعات آن مانند رم را بررسی خواهیم کرد.

www.takbook.com



شکل ۳ - ۲۰ تشخیص خطا

۳-۲-٤ هارد دیسک

هارد را می‌توانم یکی از مهمترین سخت‌افزار برای کاربران دانست که وجود آن بسیار حائز اهمیت است، هاردها در سایزها و نوع‌های مختلفی در بازار وجود دارند که بسته به سخت‌افزار و هزینه‌ی خود آنها را انتخاب می‌کنید.

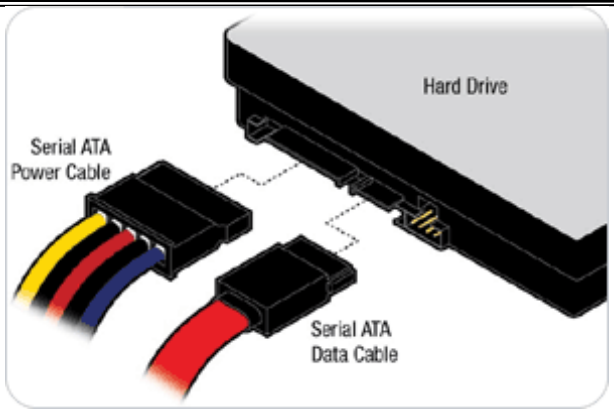
در حال حاضر چهار نوع هارد بیشترین استفاده را در سیستم‌های کامپیوتری و سرور دارند که عبارتند از :

- SATA
- SSD
- NVME
- SAS

۳-۲-٤-۱ SATA

هارد SATA (Serial Advanced Technology Attachment) در سال ۲۰۰۳ معرفی شد، به خاطر وجود کابل‌هایی که در شکل ۳-۲۱ مشخص است، این هاردها به نام SATA یاد می‌شوند ولی در کل این نوع هاردها به صورت یک مستطیل هستند که درون آن از صفحات گرد استفاده می‌شود و از طریق هد اطلاعات خوانده می‌شود، در شکل ۳-۲۱ یک هارد را مشاهده می‌کنید که کابل‌های دیتا و پاور SATA به آن متصل شده است.

www.takbook.com



شکل ۳ - ۲۱ هارد SATA

ظرفیت‌های این نوع هاردها در حال حاضر از ۵۰۰ گیگابایت تا ۲۰ ترابایت متفاوت است و بسته به نیاز خود باید از آنها استفاده کنید.

یکی از مهمترین ویژگی هارد داشتن سرعت چرخش مناسب هست، سرعت چرخش دیسک‌ها در دقیقه یا همان RPM نامیده می‌شود که هر چه بیشتر باشد کیفیت هارد بالاتر و سرعت بهتر است.

یک حافظه با نام CASHE وجود دارد که سرعت بالایی دارد و آخرین فایل‌های باز کاربران در آن قرار می‌گیرد و در هنگام خرید هارد شاید دیده باشید که نوشته شده 64 مگابایت کش که به همین نکته اشاره می‌کند.

شکل ۳-۲۲، داخل یک هارد را نشان می‌دهد که صفحات گرد آن مشخص است و از طریق یک بازو که سر آن به هد متصل است اطلاعات خوانده خواهد شد، در این نوع هاردها یک آهن ربای خیلی قوی تعبیه شده است که نگه دارنده هد است.



شکل ۳ - ۲۲ هارد SATA

www.takbook.com

یک نکته مهم در انتخاب سایز هارد دیسک این است که اگر بخواهید هارد دیسک را برای لپ‌تاپ خود استفاده کنید باید از سایز 2.5 اینچی استفاده کنید و اگر می‌خواهید برای سیستم خانگی خود استفاده کنید می‌توانید هم از سایز ۳.۵ و هم از ۲.۵ استفاده کنید، در شکل ۳-۲۳ هر دو سایز هارد دیسک را مشاهده می‌کنید.



شکل ۳ - ۲۳ اندازه هارد

۳-۲-٤-۲ SSD

یک مدل دیگر هارد که امروزه بیشترین استفاده را دارد مدل SSD (Solid-state drive) است، سرعت این نوع هارد دیسک‌ها به علت اینکه از مکانیک استفاده نمی‌کنند بسیار بالاتر است، در شکل ۳-۲٤ این نوع هارد را مشاهده می‌کنید که سوکت ورودی آن دقیقاً شبیه به هاردهای SATA است ولی سایز آنها 2.5 اینچ است و مخصوص لپ تاپ یا کامپیوتر خانگی طراحی شده‌اند.



شکل ۳ - ۲۴ هارد SSD

ما در سازمان خود از این نوع هاردها برای نصب ویندوز استفاده می‌کنیم، یک هارد SSD دارای ظرفیت‌های مختلفی است اما هزینه‌ی خرید آنها بالا است و بهتر است مثلاً یک هارد SSD 256 GB خریداری کنید و سیستم عامل مورد نظر خود را بر روی آن قرار دهید و در کنار آن می‌توانید یک هارد سنتی

www.takbook.com

SATA خریداری کنید با ظرفیت 1 ترابیت و فایل‌های حجیم خود را بر روی آن ذخیره کنید، چون هزینه‌ی هاردهای سنتی خیلی پاینتر از SSD است.

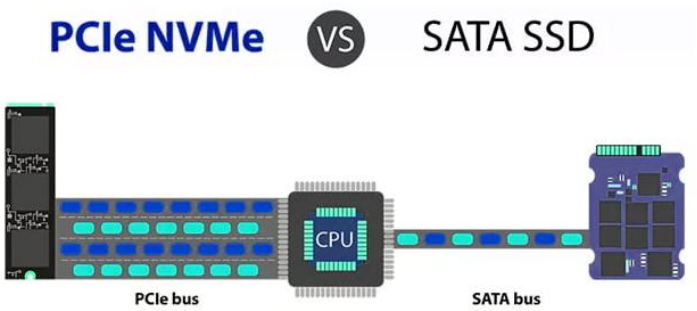
۳-۲-٤-۳ NVME

NVME مخفف nonvolatile memory express است و به معنی حافظه‌ی پرسرعت غیر فرار است. این نوع هاردها ساختار بسیار متفاوتی در طراحی و سرعت دارند، در شکل ۳-۲۵ یک هارد NVME با ظرفیت یک ترابایت را مشاهده می‌کنید که خیلی کوچک است و به مانند کارت‌های PCI که قبلاً بررسی کردیم بر روی شکاف مختص به خود یعنی PCIE متصل می‌شوند، همچنین سرعت ارسال و دریافت اطلاعات در این نوع هاردها بسیار بالا است، به این نوع هاردها مدل M.2 هم گفته می‌شود.



شکل ۳ - ۲۵ هارد NVM

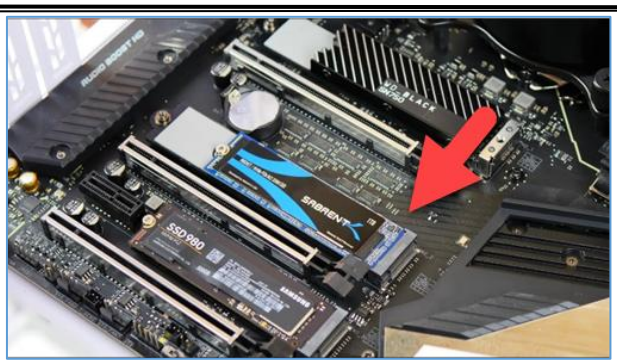
در شکل ۳-۲٦ ارتباط دو هارد SSD و NVME را با CPU بررسی می‌کنیم که مشاهده می‌کنید هاردهای NVME چوت از شکاف‌های PCIE استفاده می‌کنند، گذرگاه بیشتری برای آنها در نظر گرفته شده است و به خاطر همین سرعت انتقال اطلاعات بسیار بیشتر است.



شکل ۳ - ۲۶ ارتباط هارد با CPU

اگر بخواهیم جایگاه اسلات PCIE را بر روی مادربرد مشخص کنیم، می‌توانید شکل زیر را مشاهده کنید که یک هارد NVME بر روی شکاف PCIE که در شکل ۳-۲۷ مشخص کردیم نصب شده است.

www.takbook.com



شکل ۳ - ۲۷ جایگاه اسلات PCIE

توجه داشته باشید که این شکاف‌ها در ماردبردهای جدید وجود دارد و برای اینکه بر روی مادربرد قدیمی این نوع هاردها را نصب کنید نیاز به کارت‌هایی دارید که این نوع هارد را پشتیبانی کنند، در شکل ۳-۲۸ این نوع کارت را مشاهده می‌کنید که بر روی اسلات PCIe نصب می‌شود و به آن هارد NVME اضافه می‌شود، این کارت از شرکت معروف icydock است.



شکل ۳ - ۲۸ icydock

یک سری هارد دیگر با عنوان U.2 وجود دارند که در سایز ۲.۵ اینچی هستند و در داخل خود هاردهای M.2 را جای می‌دهند که شکل ۳-۲۹ نشان دهنده این نوع هارد است، نام دیگر این نوع هارد SFF-8639 است.

www.takbook.com



شکل ۳ - ۲۹ هارد *SFF-8639*

مدل دیگری که برای هاردهای NVME وجود دارد مدل U.3 است که دقیقاً همان U.2 است اما قابلیت پشتیبانی از SATA,SAS و NVME را دارا می‌باشد که شکل ۳-۳۰ نشان دهنده این هارد است.



شکل ۳ - ۳۰ هاردهای *NVME*

۳-۲-٤-٤ SAS

هاردهای SAS (Serial Attached SCSI) چیزی شبه به SATA هستند ولی از نظر سرعت و کیفیت و همچنین از نظر سوکت ورودی کاملاً متفاوت هستند.

هاردهای SAS را به عنوان هاردهای سروری می‌شناسند و مخصوص سرور طراحی شده است، شکل ۳-۳۱ را مشاهده می‌کنید.

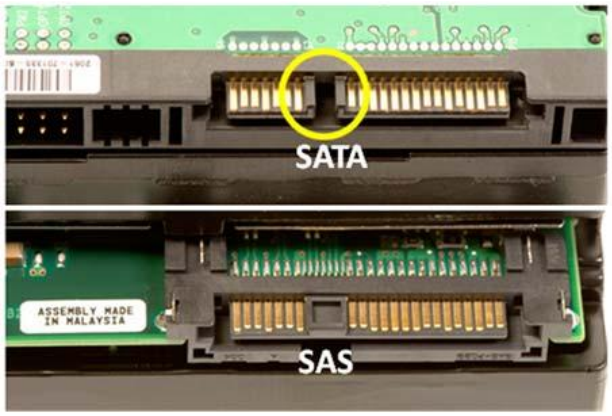
www.takbook.com



شکل ۳ - ۳۱ هارد SAS

اگر به شکل ۳-۳۱ توجه کنید هاردهای SAS و SATA از نظر ظاهری دقیقاً شبیه به هم هستند ولی در سوکت ورودی متفاوت هستند در شکل ۳-۳۲، 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، 128 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.



شکل ۳ - ۳۲ تفاوت سوکت SAS و SATA

یکی دیگر از نکاتی که باید در مورد هاردهای SAS بدانیم این است که طول عمر آنها 1.2 میلیون ساعت است، اما هاردهای سنتی SATA برابر با 700 هزار ساعت است و همین موضوع باعث می‌شود از این نوع هاردها در سرورها استفاده شود.

www.takbook.com

همان‌طور که بیان کردیم سرعت چرخش هاردهای SAS برابر با 10K و 15K است که به معنی 10 هزار و 15 هزار دور در دقیقه است که به آن RPM گفته می‌شود.

نکته آخر در مورد هاردهای SAS است که ظرفیت‌های آن محدود است و در حال حاضر بیشتر از 1.2 ترابایت ظرفیت موجود نیست اما هاردهای SATA ظرفیتی بالای 20 ترابایت هم دارند.

توجه داشته باشید در قسمت بررسی سرورهای HP نحوه نصب این نوع هاردها را به صورت کامل توضیح خواهیم داد.

۳-۲-۵ پاور

انتخاب پاور یکی از مهمترین فاکتورهای یک سیستم خواهد بود و انتخاب درست آن می‌تواند در عملکرد سخت‌افزار تاثیرگذار باشد.

اولین چیزی که باید در انتخاب پاور (POWER) در نظر داشته باشید این است که باید بدانیم به چند وات نیاز داریم، در بازار ایران پاورهایی با قدرت 200 وات تا 1800 موجود هست، شما باید بدانید قطعاتی که در یک کیس استفاده می‌کنید چند وات نیاز دارند، برای دانستن این موضوع باید به توان تقریبی آنها یعنی TDP را بررسی کنید.

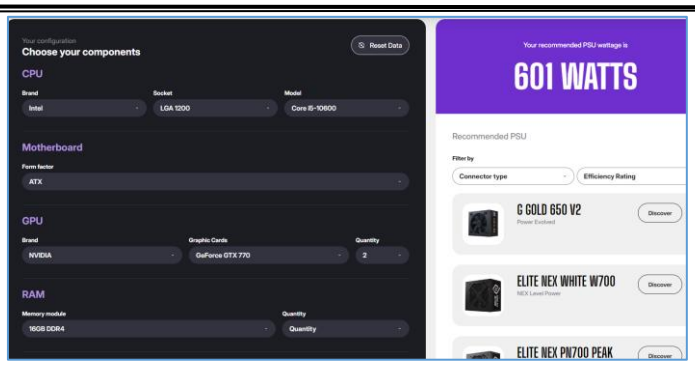
در شرکت خومد برای انتخاب پاور مناسب، بررسی می‌کنم قطعاتم به چند وات نیاز دارند، اگر مثلاً به 300 وات نیاز داشته باشند اصولاً باید یک پاور با قدرت 600 تهیه کنم تا مشکلی ایجاد نشود، البته این در صورتی است که نخواهیم قطعات داخل کیس را ارتقاء دهیم اگر قصد ارتقاء داریم باید پاور با وات بالاتر خریداری کنیم، شکل ۳-۳۳ یک پاور را نشان می‌دهد.



شکل ۳ - ۳۳ پاور

بهترین راه برای محاسبه‌ی مقدار وات مورد نیاز کیس شما استفاده از سایت‌های آنلاین است که می‌توانید از سایت coolermaster.com استفاده کنید، در شکل ۳-۳٤ قطعات کیس را انتخاب کردم و وات پاور به همراه برند پاور را مشخص کرده است.

www.takbook.com



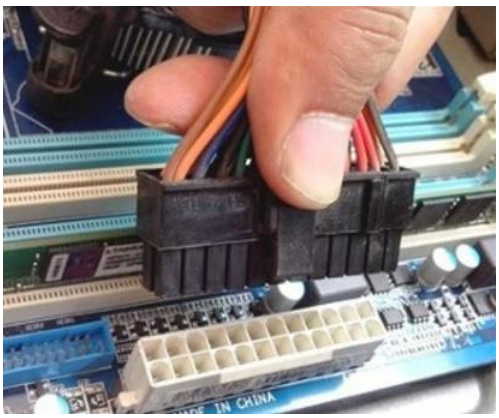
شکل ۳ - ۳۴ محاسبه پاور

یکی دیگر از ویژگی‌های مهم در انتخاب پاور کانکتورهایی است که یک سیستم نیاز دارد، کانکتور پاور، SATA، کارت گرافیک و ...، است توجه داشته باشید که کانکتور برق اصلی بر روی یک مادربرد، کانکتور 24 پین است که شکل ۳-۳۵ نشان دهنده‌ی آن است.



شکل ۳ - ۳۵ کانکتور پاور

در شکل ۳-۳٦، نری ۲٤ پین پاور را مشاهده می‌کنید که بر روی مادگی ۲٤ پین مادربرد قرار می‌گیرد.



شکل ۳ - ۳۶ کانکتور پاور

www.takbook.com

کانکتورهای برق SATA به صورت شکل ۳-۳۷ هستند که بر روی هارد دیسک و DVD/RW قرار می‌گیرند، در شکل ۳-۳۷، کانکتور مشکی رنگ همان کانکتور برق SATA است و کانکتور سفید رنگ به کانکتور Molex معروف است و برای سخت‌افزارهای قدیمی‌تر کاربرد دارد و در حال حاضر به فن‌های کیس متصل می‌شود.



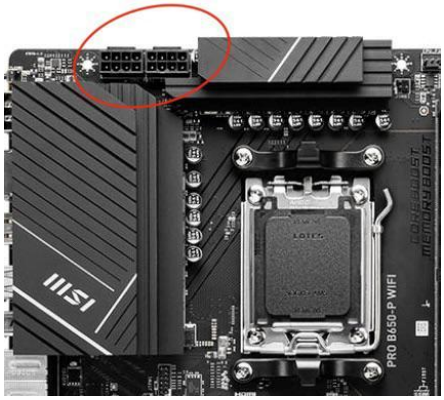
شکل ۳ - ۳۷ کانکتور برق

کانکتور بعدی که باید به آن توجه کنیم، کانکتور ٦ پین است که بیشتر برای استفاده در کارت گرافیک‌ها و CPU است که شکل ۳-۳۸ نشان دهنده‌ی آن است، این کانکتور به کانکتور 6+2 معروف است.



شکل ۳ - ۳۸کانکتور برق CPU

همان‌طور که در شکل ۳-۳۹ مشاهده می‌کنید بر روی مادربرد دو کاکتور ۸ پین وجود دارد که مختص CPU است و اگر این کانکتورها نصب نباشد تصویری نخواهید داشت و CPU روشن نخواهد شد.



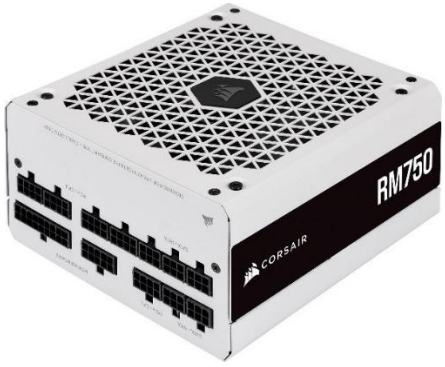
شکل ۳ - ۳۹کانکتور CPU

www.takbook.com

توجه داشته باشید در سیستم‌های قدیمی این کانکتورها 4 پین بودند.

یک نکته مهم در خرید پاور این است که باید دقت کنید وزن آن سبک نباشد، هر چقدر یک پاور سنگین‌تر باشد کیفیت و قدرت قطعاتی که داخل آن استفاده شده قطعاً بیشتر است و این موضوع ساده بهترین ویژگی یک پاور خواهد بود و می‌توانید به راحتی یک پاور را انتخاب کنید.

یکی دیگر از ویژگی‌های یک پاور خوب این است که ماژولار باشد، اگر به شکل ۳-۴۰ دقت کنید، پاور مورد نظر کابلی ندارد و تمام کابل‌ها از آن به راحتی جدا می‌شوند و همین موضوع یعنی پاور مورد نظر ماژولار است و اگر کابلی خراب شود به راحتی می‌توان آن را تعویض کرد.



شکل ۳ - ۴۰ پاور ماژولار

نکته‌ی آخر در انتخاب پاور این است که باید دقت کنید که آیا علامت شکل ۳-۴۱، بر روی پاور قرار دارد یا خیر، این علامت نشان دهنده‌ی این است که پاور مورد نظر بهترین رادمان را دارد، پاورهایی که بهترین بازدهی را داشته باشند و بیش از ۸۰ درصد از عملکرد و توان خروجی را به نمایش بگذارند دارای علامت شکل ۳-۴۱ خواهند بود و باید به آن دقت کرد.



شکل ۳ - ۴۱ رادمان پاور

محل نصب پاور بر روی کیس به صورت شکل ۳-۴۲، مشخص شده است، در کیس‌های جدید، پاور در زیر کیس نصب می‌شود و در کیس‌های قدیمی در بالای آن نصب می‌شود.

www.takbook.com



شکل ۳ - ۴۲ محل نصب پاور

٦-۲-۳ کارت گرافیک

کارت گرافیک یکی از کاربردی‌ترین سخت‌افزار در یک کیس، لپ‌تاپ یا موبایل می‌باشد که بسته به نوع کاری که دارید می‌توانید از آن استفاده کنید، اما انتخاب یک مدل مشخص برای استفاده، یک کار تخصصی است و باید دقیق باشید.

کارت گرافیک وظیفه رندر کردن تصاویر را دارد، مثلاً برای انجام بازی باید یک کارت گرافیک قدرتمند داشته باشید تا توانایی رندر کردن تصاویر را با قدرت بالا داشته باشد.

کارت‌های گرافیک خودشان دارای یک پردازنده مرکزی هستند که با نام واحد پردازش گرافیکی (Graphics Processing Unit) شناخته می‌شوند که نام اختصار آن GPU است، این پردازنده از پردازنده اصلی سیستم شما جدا است و فقط برای پردازش تصاویر و رندر کردن آن به کار می‌رود، در شکل ۳-٤۳ یک کارت گرافیک ایسوس مدل ROG Strix GeForce RTX 4070 Ti OC Edition را مشاهده می‌کنید که کیفیت خوبی در همه کارها دارد مخصوصاً بازی‌های کامپیوتری.



شکل ۳ - ۴۳ کارت گرافیک

www.takbook.com

کارت گرافیک‌ها در مدل‌های مختلفی وجود دارند که با هم آنها را بررسی می‌کنیم.

کارت گرافیک‌های یکپارچه (Integrated)

اگر مادربرد خریده باشید در اکثر آنها خروجی کارت گرافیک به مانند شکل ۳-٤٤ وجود دارد، که توان بالایی ندارند ولی برای کارهای روزمره و عادی خوب خواهند بود، مثلاً برای یک سازمان که کارمندان آن می‌خواهند با آفیس کارکنند انتخاب خوبی خواهد بود ولی برای پردازش‌های سنگین باید کارت گرافیک خریداری شود.



شکل ۳ - ۴۴ کارت گرافیک onboard

کارت گرافیک مستقل (Dedicated)

همان‌طور که در بالا بیان کردیم برای اینکه کارت گرافیک قدرتمند داشته باشید باید به صورت مستقل کارت گرافیک خریداری کنیم.

نکته مهم این است که اگر بر روی یک سیستم دو کارت گرافیک داخلی و مستقل داشته باشید، کارت گرافیک مستقل فعال خواهد بود و تصویر می‌دهد.

در شکل ۳-٤٥ کارت گرافیک مستقل را مشاهده می‌کنید که بر روی مادربرد نصب شده است.



شکل ۳ - ۴۵ کارت گرافیک مستقل

یک کارت گرافیک مستقل دیگری داریم که با عنوان کارت گرافیک eGPU شناخته می‌شود، دوستانی که لپ‌تاپ دارند، چون نمی‌توانند کارت گارفیک لپ تاپ خود را ارتقاءدهند باید از این مدل استفاده کنند که

www.takbook.com

شکل ۳-٤٦ نشان دهنده‌ی این مدل از کارت گرافیک است، این کارت گرافیک خارج از سیستم کار می‌کند و از طریق رابط به سیستم متصل می‌شود.

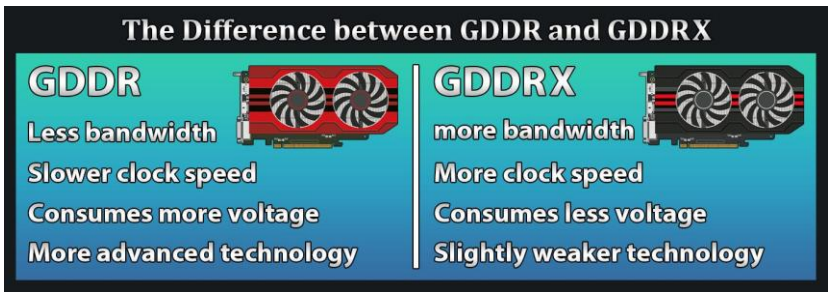


شکل ۳ - ۴۶ کارت گرافیک خارجی

مهمترین فاکتور در انتخاب یک کارت گرافیک مقدار حافظه‌ی آن است، حافظه‌های کارت گرافیک با عنوان GDDR شناخته می‌شوند و کارشان مختص گرافیک است و شبیه به رم اصلی سیستم نیستند، هر چقدر مقدار GDDR بیشتر باشد کیفیت کارت گرافیک بیشتر است و سرعت آن بیشتر خواهد بود، البته کارت‌های گرافیک، نسل‌های مختلف دارد و حتماً حافظه GDDR بالا در نسل پایینتر از حافظه کمتر GDDR در نسل بالاتر بهتر نخواهد بود.

در حال حاظر نسل‌های حافظه از GDDR تا GDDR6X متغیر است و آخرین فناوری GDDR6X است که از سرعت فوق‌العاده ٢٤ گیگابایت برخوردار است.

تفاوت‌های دو حافظه‌ی GDDR و GDDRX در شکل ۳-٤٧ بیان شده است که مشخص است، حافظه‌های جدید GDDRX از پهنای باند بیشتر و سرعت بالاتری برخوردارند.



شکل ۳ - ۴۷ تفاوت‌های دو حافظه‌ی GDDR و GDDRX

www.takbook.com

فاکتور بعدی در انتخاب کارت گرافیک خنک‌کننده‌های آن است که باید به آن توجه کرد، اگر به کارت گرافیک دقت کرده باشید، دارای فن‌های مختلف از یکی تا چنتا هستند که بسته به نیاز خود می‌توانید آنها را انتخاب کنید، به این نکته هم توجه کنید که انتخاب کارت گرافیک ارتباط مستقیم با پاور سیستم شما دارد و باید ببینید که پاور سیستم شما توانایی اجرا را دارد یا نه.

۳-۳ سوئیچ

سوئیچ‌ها قلب تپنده‌ی یک شبکه هستند و در هر سازمانی یک یا چند سوئیچ برای ارتباط سیستم‌ها با هم وجود دارد، این سوئیچ‌ها در انواع و اقسام مختلف هستند که بسته به نیاز خود از آنها استفاده می‌کنیم.
سوئیچ‌ها بر دو نوع هستند:

۱- غیر مدیریتی (Unmanaged)
۲- مدیریتی (Managed)

سوئیچ‌های غیر مدیریتی، همان‌طور که از نامش پیداست هیچ تغییری در تنظیمات آن نمی‌شود اعمال کرد، و فقط ارتباط دستگاه‌های مختلف را با هم برقرار می‌کند، در زیر سوئیچ غیر مدیریتی را مشاهده می‌کنید که دارای ۸ پورت است و می‌توانید هم زمان ۸ دستگاه را به آن متصل کنید.
به این نکته توجه کنید که نحوه‌ی ارتباط دستگاه‌ها را در ادامه بررسی خواهیم کرد.



شکل ۳ - ۴۸ سوئیچ غیر مدیریتی

سوئیچ‌های مدیریتی، همان‌طور که از نامشان پیداست یک سوئیچ قابل تنظیم است و به هر نحو که دوست دارید می‌توانید سوئیچ مورد نظر را تنظیم کنید، مثلاً از نظر امنیتی می‌توانید محدودیت‌هایی را برای دستگاه‌ها ایجاد کنید، یکی از قدرتمندترین سوئیچ‌های مدیریتی بازار، سوئیچ‌های سیسکو است که در انواع و اقسام مختلف وجود دارد، در زیر سوئیچ سیسکو مدل C1000-48T-4G-L را مشاهده می‌کند که یک سوئیچ مدیریتی است و دارای 52 پورت است، که 48 پورت آن 10/100/1000 است.



شکل ۳ - ۴۹ سوئیچ مدیریتی

www.takbook.com

چون در این کتاب با سوئیچ‌های مدیریتی کار می‌کنیم می‌خواهیم سوئیچ‌های سیسکو را برای شما تشریح کنیم که از چه قطعاتی تشکیل شده است.

۱- پورت

یک سوئیچ از ٤ پورت تا ٤٨ پورت تشکیل شده است که شما می‌توانید به هر کدام از این پورت‌ها یک سیستم، دوربین، پرینتر و ... نصب کنید و آنها را به هم شبکه کنید.

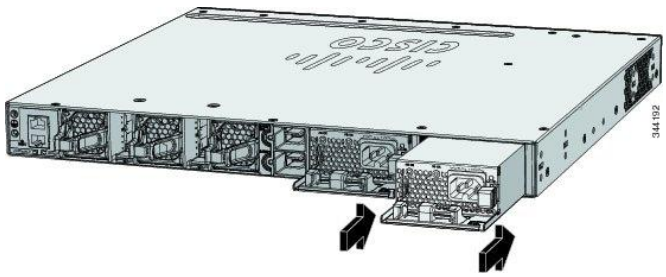
۲- ماژول پاور

سوئیچ‌های جدید از دو پاور برای Load Balance استفاده می‌کنند که هر موقع یکی از پاورها خراب شد یکی دیگر فعال باشد و سوئیچ خاموش نشود، در شکل ۳-۵۰ پاور مربوط به سوئیچ را مشاهده می‌کنید که یک پاور 220V است.



شکل ۳ - ۵۰ پاور سرور

نحوه‌ی قرار گیری آن بر روی سوئیچ به صورت شکل ۳-۵۱ است که در پشت آن به صورت ماژولار وارد می‌شود.



شکل ۳ - ۵۱ قرار گیری پاور بر روی سوئیچ

۳- ماژول فن

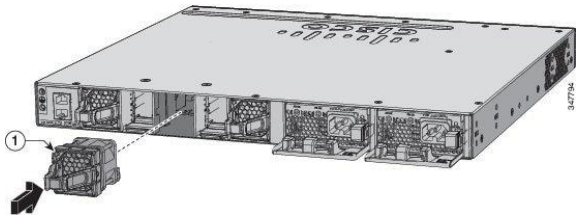
در سوئیچ‌های جدید، فن‌ها به صورت ماژولار بر روی سوئیچ نصب می‌شوند، در شکل ۳-۵۳ این نوع فن را مشاهده می‌کنید.

www.takbook.com



شکل ۳ - ۵۲ ماژول فن

نحوه‌ی قرارگیری آن داخل سوئیچ به صورت شکل ۳-۵۳ است که به صورت یک ماژول وارد سوئیچ می‌شود، البته یک سوئیچ می‌تواند از یک تا سه فن داشته باشد.



شکل ۳ - ۵۳ جایگاه ماژول فن

روی سوئیچ‌ها به ازای هر پورتی که وجود دارد، یک چراغ چشمک‌زن هم وجود دارد که این چراغ به رنگ‌های مختلف نمایانگر می‌شود که هر رنگ آن را طبق جدول ۳-۱ مورد بررسی قرار می‌دهیم:

جدول ۳- ۱ چراغ سوئیچ

سبز	به این پورت کابلی متصل شده است، اما فعال نشده است.
سبز چشمک‌زن	این پورت فعال و در حال ارسال و دریافت اطلاعات است.
سبز و کهربایی	در این حالت یک collision در سوئیچ رخ داده است.
کهربایی	در این حالت پورت Disable شده، اما به صورت دستی.
off	به پورت کابلی متصل نشده است.

چراغ‌های دیگری هم وجود دارند که در زیر آنهارا بررسی می‌کنیم:

UTL LED: این چراغ‌ها نشان‌دهنده‌ی پهنای باند مصرفی در سوئیچ می‌باشند.

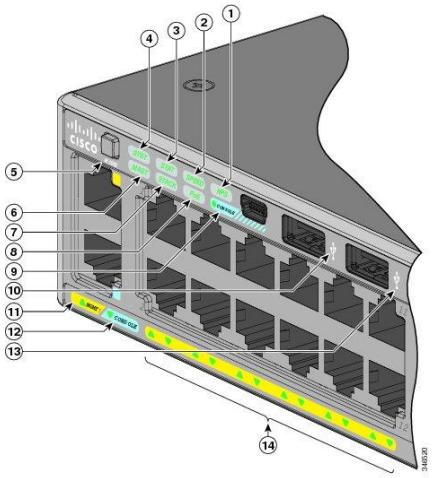
STST LED: زمانی که سوئیچ روشن شود، این چراغ هم روشن می‌شود.

FDUP LED: در این حالت پورت‌ها در دو حالت Half-duplex و Full-duplex قرار دارند و اگر چراغ پورت خاموش باشد، یعنی در حالت Half-duplex قرار دارد و اگر روشن باشد و سبز در حالت Full-duplex قرار دارد.

www.takbook.com

100 یا Speed Led: این چراغ نشان‌دهنده‌ی سرعت یک پورت است که اگر خاموش باشد، یعنی از ۱۰ مگابایت استفاده می‌کند و اگر روشن و سبز باشد، یعنی از حداکثر سرعت استفاده می‌کند.

در شکل ۳-٥٤ یک شمای کلی از جلوی سوئیچ مدل 2960X را مشاهده می‌کنید که شامل چراغ‌ها و پورت‌های مشخص است که در جدول ۳-۲ همه چیز مشخص شده است.



شکل ۳ - ۵۴ چراغ‌های تعبیه شده بر روی سوئیچ

جدول ۳- ۲بررسی چراغ های سوئیچ

شماره	توضیحات
۱	چراغ RPS است که مربوط به پاور سوئیچ است و برای Redundancy کاربرد دارد، یعنی اینکه اگر بر روی سوئیچ از دو پاور همزمان استفاده کنید این چرا غ به کار می‌رود
۲	چراغ SPEED LED نشان‌دهنده‌ی سرعت یک پورت است که اگر خاموش باشد، یعنی از ۱۰ مگابایت استفاده می‌کند و اگر روشن و سبز باشد، یعنی سرعت آن ۱۰۰ مگابایت است و در آخر اگر چراغ سبز خاموش روشن می‌شود سرعت آن از ۱۰۰ تا ۱۰۰۰ مگابایت است.
۳	چراغ STAT LED زمانی که سوئیچ روشن شود، این چراغ هم روشن می‌شود.
٤	چراغ SYS LED اگر روشن نباشد یعنی سوئیچ خاموش است، اگر سبز باشد یعنی سوئیچ در حالت نرمال قرار دارد، اگر در حالت چشمک زن قرار داشته باشد یعنی اینکه سوئیچ در حال اجرای نرم‌افزار است، اگر رنگ آن به کهربایی تغییر کند یعنی اینکه دستگاه در حال اجرا و دریافت نیرو است اما به درستی کار نمی‌کند و در آخر

www.takbook.com

	اگر چراغ به صورت کهربایی و چشمک زن باشد یعنی اینکه در شبکه، تامین نیرو و یا ماژول فن مشکل وجود دارد.
٥	دکمه Mode هم برای ریسیت کردن سوئیچ به کار می‌رود که بعد از ریست به حالت Setup Mode خواهد رفت، فقط توجه داشته باشید برای فعال کرن آن باید دکمه را چند ثانیه نگه دارید.
٦	سوئیچ Master به سوئیچی گفته می‌شود که در یک مجموعه به صورت اتوماتیک اطلاعات IOS را بین اعضای جدید اعمال می‌کند یعنی با این کار وقتی یک سوئیچ می‌خواهد به مجموعه‌ای اضافه شود هیچ افتی در سرعت کار پیش نخواهد آمد. چراغ Master LED اگر خاموش باشد یعنی اینکه سوئیچ Master نیست، اگر سبز باشد یعنی اینکه یک سوئیچ Master است.
۷	چراغ STACK نشان دهنده‌ی این است که سوئیچ مورد نظر در یک STACK قرار دارد که این مجموعه‌ی STACK می‌تواند شامل ۸ سوئیچ باشد.
۸	چراغ POE نشان دهنده‌ی این است که پورت مورد نظر فعال شده است، این نوع پورت‌ها دارای برق هم هستند و بیشتر برای دوربین‌های مدار بسته مورد استفاده قرار می‌گیرند، در فصل دوازدهم در مورد این پورت به صورت مفصل بحث خواهیم کرد.
۹	چراغ USB mini-Type B console port زمانی فعال خواهد شد که از کابل Console دستگاه استفاده کنید.
۱۰	پورت USB Type A
۱۱	پورت MGMT یا پورت مدیریتی
۱۲	چراغ CONSOLE
۱۳	پورت USB Type A
۱٤	چراغ تمام پورت‌های سوئیچ که در هر ردیف دو چراغ وجود دارد که چراغ سمت چپ برای پورت بالایی و سمت راست برای پورت پائینی.

٤-۳ سوئیچ‌های متفرقه

در مورد سوئیچ های متفرقه، باید گفت، یکی سری سوئیچ‌ها در شبکه استفاده می‌شوند و سوئیچ‌های هستند که مربوط به تصاویر هستند، اگر وارد یک اتاق جلسات شده باشید، متوجه می‌شوید که یک تصویر برای چندین سیستم به اشتراک گذاشته شده است که این کار را از طریق سوئیچ تصویر انجام می‌دهند که در زیر آنها را بررسی می‌کنیم.

www.takbook.com

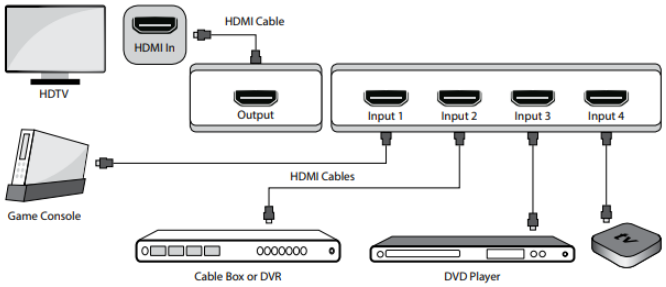
۳-٤-۱ سوئیچ HDMI

یکی از پرکاربردترین سوئیچ‌های تصویر، سوئیچ HDMI است که برای اینکه تصویر چند سیستم را بر روی یک مانیتور پخش کنید باید از آن استفاده کنید، مثلاً در شکل ۳-۵۵، یک سوئیچ 3 به 1 را مشاهده می‌کنید که همزمان سه تا سیستم می‌توانند به آن متصل شوند و با دکمه‌ای که بر روی آن تعبیه شده بین سیستم‌ها سوئیچ کرد و تصویر آنها را در مانیتور مشاهده کرد، بعضی از این سوئیچ‌ها کنترل هم دارند تا کار با آنها آسان باشد.



شکل ۳ - ۵۵ سوئیچ HDMI

در شکل ۳-٥٦، دقیقاً مشخص است که چندین دستگاه وارد سوئیچ (Input) می‌شوند و در قسمت خروجی (Output) که به ورودی مانیتور متصل می‌شود و تصویر نمایش داده می‌شود.



شکل ۳ - ۵۶ سوئیچ HDMI

۳-٤-۲ اسپلیتر HDMI

اسپلیر؛ سیگنال HDMI را از یک منبع ورودی (مثل کامپیوتر، دستگاه بازی، یا دستگاه پخش ویدئو) گرفته و آن را به چند خروجی HDMI تقسیم می‌کند. به عبارت دیگر، این دستگاه به شما اجازه می‌دهد که تصویر و صدای یک دستگاه را به چندین نمایشگر یا تلویزیون به صورت همزمان انتقال دهید، در شکل ۳-۵۷ این نوع دستگاه را مشاهده می‌کنید.



شکل ۳ - ۵۷ اسپلیتر HDMI

www.takbook.com

۳-٤-۳ کی وی ام سوئیچ (KVM Switch)

فرض کنید یک مانیتور و دو سیستم دارید و باید آن را به هم متصل کنید، برای اینکار نیاز به دستگاهی به نام KVM Switch داریم تا تصویر هر کدام از دستگاه‌ها را به همراه صفحه نمایش و کیبورد را در اختیار کاربر قرار دهد، در شکل ۳-۵۸ یک KVM Switch ساده و ارزان را مشاهده میکنید که ٤ سیستم به طور همزمان به آن متصل می‌شوند و دارای ورودی USB هم است که می‌توان به آن کیبورد و موس هم اضافه کرد و با فشار دادن دکمه که روی آن قرار دارد تصویر هر کدام از سیستم ها را نمایش داد.



شکل ۳ - ۵۸ کی وی ام سوئیچ

KVM Swichها در انواع و اقسام مختلف وجود دارد که هم برای VGA و هم برای HDMI طراحی شده‌اند، و بسته به نیاز خود باید یکی را انتخاب کنید.

۳-٤-۵ اتصالات میز کنفرانس

یکی دیگر از ابزارهایی که در دنیای شبکه کاربرد دارد، استفاده از قابلیت اتصال میز کنفرانس (Conference Table Connectivity) است که به کاربرانی که در پشت هر صندلی می‌نشینند یک سری دسترسی می‌دهد، مثلاً اگر کاربر مورد نظر داری یک لپ‌تاپ باشد و بخواهد تصویر لپ‌تاپ خودش را به اشتراک بگذارد دیگر نیاز نیست لپ تاپ خود را به سوئیچ اسپلیتر متصل کند بلکه این کار را به اتصال کابل HDMI خود به ورودی اتصالات میز کنفرانس انجام می‌دهد، در شکل ۳-۵۹، این سوئیچ را مشاهده می‌کنید که دارای ورودی های مختلفی مانند پورت شبکه، پورت HDMI، پورت USB و ... است که کاربر در صورت نیاز به هر کدام می‌تواند از آنها استفاده کند.

www.takbook.com



شکل ۳ - ۵۹ اتصالات میز کنفرانس

توجه داشته باشید که باید برای هر کدام از این اتصالات یک کابل از سیستم یا اسپلیتر به زیر آن متصل می‌شود.

۳-۵ روتر

روتر (Router) یک دستگاه شبکه است که وظیفه انتقال داده‌ها بین شبکه‌های مختلف را بر عهده دارد. روترها داده‌ها را از یک شبکه به شبکه دیگر هدایت می‌کنند و به عنوان یک مسیردهنده (Forwarder) عمل می‌کنند. این دستگاه‌ها معمولاً برای ارتباط بین شبکه‌های داخلی (LAN) و شبکه‌های خارجی (WAN) استفاده می‌شوند، مانند اینترنت یا شبکه‌های دیگر.

روترها بر اساس آدرس‌های IP کار می‌کنند. وقتی دستگاهی (مثل کامپیوتر، تلفن هوشمند یا هر دستگاه دیگری) در یک شبکه، داده‌ای را ارسال می‌کند، روتر آن داده‌ها را دریافت می‌کند و بر اساس آدرس مقصد، بهترین مسیر را برای ارسال آنها انتخاب می‌کند. این فرآیند به روتر اجازه می‌دهد که داده‌ها را از یک شبکه به شبکه دیگر، یا از شبکه‌ی محلی به اینترنت و برعکس، هدایت کند.

وظایف و ویژگی‌های روتر:

- مسیریابی بسته‌های داده: روتر بر اساس جدول مسیریابی که دارد، تصمیم می‌گیرد که هر بسته‌ی داده را به کدام شبکه ارسال کند.
- ارتباط بین شبکه‌ها: روترها معمولاً برای اتصال شبکه‌های محلی (LAN) به اینترنت (WAN) استفاده می‌شوند.
- مدیریت ترافیک شبکه: روترها با بررسی ترافیک ورودی و خروجی، می‌توانند به بهینه‌سازی مسیرهای داده و جلوگیری از ترافیک بیش از حد کمک کنند.
- امنیت شبکه: بسیاری از روترها دارای قابلیت‌های امنیتی هستند، مثل فایروال (Firewall) برای مسدود کردن ترافیک‌های ناخواسته یا مشکوک.

www.takbook.com

- ترجمه آدرس شبکه (NAT): روترها از تکنیکی به نام NAT استفاده می‌کنند تا دستگاه‌های داخل شبکه محلی بتوانند از یک آدرس IP عمومی برای ارتباط با اینترنت استفاده کنند.
- پشتیبانی از DHCP: روترها به دستگاه‌های داخل شبکه به طور خودکار آدرس IP اختصاص می‌دهند.

انواع روترها

- روترهای خانگی

این روترها برای استفاده در شبکه‌های خانگی یا کوچک طراحی شده‌اند. آنها معمولاً دارای قابلیت‌های اولیه برای اتصال به اینترنت و مدیریت چندین دستگاه به‌طور همزمان هستند.

- **روترهای تجاری و سازمانی**

این روترها برای استفاده در سازمان‌ها و شرکت‌های بزرگ طراحی شده‌اند و امکانات پیشرفته‌تری مانند امنیت، مسیریابی پیچیده، و قابلیت‌های مدیریت ترافیک را فراهم می‌کنند.

- **روترهای هسته (Core Routers)**:

این روترها در هسته شبکه‌های بزرگ اینترنتی یا شرکت‌های بزرگ قرار دارند و توانایی مسیریابی داده‌ها در مقیاس وسیع را دارند. آنها معمولاً قادر به پردازش حجم زیادی از ترافیک در سرعت بالا هستند.

- **روترهای مجازی (Virtual Routers)**

این نوع روترها نرم‌افزاری هستند و معمولاً در محیط‌های مجازی‌سازی استفاده می‌شوند. آنها قابلیت انجام مسیریابی را دارند بدون اینکه نیازی به سخت‌افزار فیزیکی داشته باشند، مانند روتر میکروتیک که در این کتاب به طور کامل آن را بررسی کردیم.

اجزای اصلی روتر

- **پورت‌های شبکه**

روترها معمولاً دارای چندین پورت هستند که به آنها اجازه می‌دهد به شبکه‌های مختلف متصل شوند. این پورت‌ها می‌توانند Ethernet (برای LAN) یا پورت‌های سریال (برای WAN) باشند.

- **جدول مسیریابی**

جدول مسیریابی، اطلاعاتی در مورد مسیرهای موجود در شبکه را ذخیره می‌کند و به روتر این امکان را می‌دهد که بسته‌ها را به مقصد صحیح ارسال کند.

- **سیستم‌عامل روتر**

www.takbook.com

روترها معمولاً دارای یک سیستم‌عامل مخصوص به خود هستند که وظیفه مدیریت ترافیک، تنظیمات و مسیریابی را انجام می‌دهند. برخی از سیستم‌عامل‌های معروف روتر عبارتند از: Cisco IOS، Juniper Junos، MikroTik RouterOS.

- **پردازنده و حافظه**

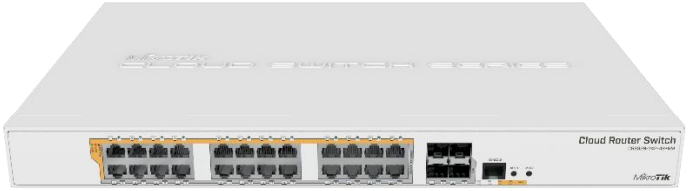
روترها برای انجام وظایف مسیریابی نیاز به پردازنده‌های قدرتمند و حافظه کافی دارند. هر چه پیچیدگی شبکه بیشتر باشد، نیاز به پردازنده‌های سریع‌تر و حافظه بیشتری وجود دارد.

در شکل ۳-۶۰ یک روتر میکروتیک مدل hAP lite TC را مشاهده می‌کنید که برای یک شبکه‌ی خانگی و کوچک مورد استفاده قرار می‌گیرید، این روتر دارای چهار پورت، وای فای و روتینگ است و بسیار کار راه‌انداز است و در ادامه کتاب تنظیمات آن بررسی خواهد شد، روترهای میکروتیک دارای یک OS هستند با نام RouterOS که تنظیمات روتر را بر روی آن انجام می‌دهیم.



شکل ۳ - ۶۰ روتر میکروتیک

توجه داشته باشید روترهای میکروتیک در انواع و اقسام مختلف وجود دارند، در شکل ۳-۶۱ دستگاه سوئیچ و روتر میکروتیک را مشاهده می‌کنید که هم می‌تواند به عنوان سوئیچ عمل کند و هم می‌تواند به عنوان روتر، اصولاً به این نوع دستگاه‌ها، دستگاه لایه‌ی سوم می‌گویند، نگران کار با این دستگاه‌ها نباشید در ادامه نحوه‌ی راه اندازی آن را یاد می‌گیریم.



شکل ۳ - ۶۱ سوئیچ سیسکو

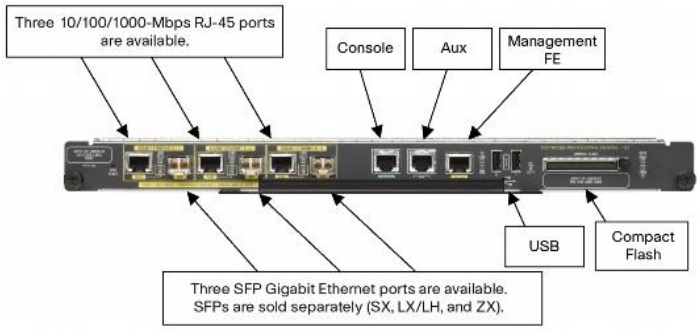
www.takbook.com

روترهای شرکت سیسکو در انواع و اقسام مختلف وجود دارند و برای شبکه‌های مختلف طراحی شده‌اند، در شکل ۳-٦۲، روتر سیسکو مدل Cisco 5000 را مشاهده می‌کنید، در ادامه اجزای یک روتر را بررسی می‌کنیم.



شکل ۳ - ۶۲ سیسکو مدل Cisco 5000

در شکل ۳-٦۳، روتر سیسکو مدل 7200 را مشاهده می‌کنید که دقیقاً تمام اجزای پشت آن مشخص شده است، پورت‌های شبکه با سرعت 10/100/1000، پورت‌های SFP و ...

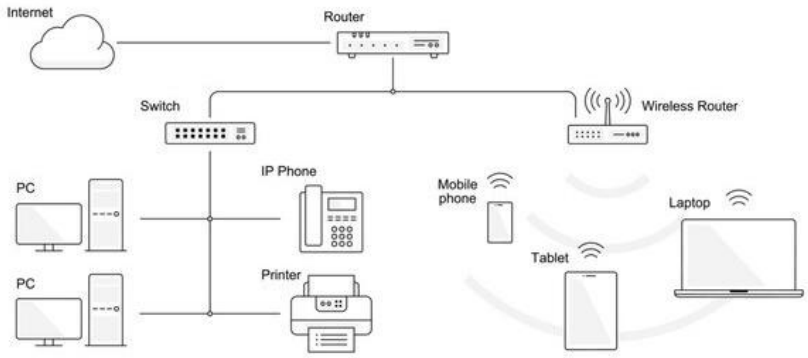


شکل ۳ - ۶۳ روتر سیسکو مدل 7200

توجه داشته باشید که دوستانی که می‌خواهند با این روترها کار کنند، ولی نمی‌توانند آنها را به خاطر هزینه‌ی بالایشان خریداری کنند باید از Imageهای مربروط به روتر سری 7200 در نرم‌افزارهایی مانند GNS3 استفاده کنند.

همیشه به یاد داشته باشید که روتر در جایی از شبکه‌ی سازمان شما قرار دارد که مرز بین شبکه‌ی اینترنت و شبکه‌ی داخلی است و باید جوری تنظیم شود تا از دسترسی غیر مجاز به شبکه‌ی شما جلوگیری شود، در شکل ۳-٦٤ دقیقاً این موضوع مشخص شده است.

www.takbook.com



شکل ۳ - ۶۴ نحوه‌ی قرارگیری روتر

روترهایی دیگری که همه افراد به صورت عمومی استفاده می‌کنند با نام مودم یا روتر ADSL است که کار اصلی آن این است که کاربران را از طریق خطوط تلفن و از طریق فناوری ADSL به اینترنت متصل کند، در شکل ۳-٦٥، یک مودم VDSL/ADSL را مشاهده می‌کنید که برای شرکت تی پی-لینک است و دقیقاً برای استفاده سبک می‌توان از آن استفاده کرد.

در تکنولوژی ADSL کاربران بر روی یک خط می‌توانند هم از تلفن استفاده کنند و هم از دیتا که در فناوری جدید آن که سرعتی به مراتب بهتر دارد از VDSL استفاده می‌کنند، ADSL از طریق سیم مسی در دسترس است ولی فناوری VDSL ترکیبی از فیبر نوری و سیم مسی است و به خاطر همین کیفیت خط به مراتب بهتر است، مثلاً من در شرکت خود یک خط ADSL از مخابرات گرفته بودم که حداکثر سرعت دانلود آن 2 مگابایت بوده ولی با تغییر خط به VDSL سرعت به ۸ مگابایت تغییر کرده، توجه داشته باشید مودم شما حتماً باید VDSL را پشتیبانی کند.



شکل ۳ - ۶۵ مودم VDSL/ADSL

www.takbook.com

برخی از مودم‌ها وجود دارند که نیاز به کابل ندارند و از طریق سیم کارت به اینترنت متصل می‌شوند، شرکت‌هایی مانند مبین‌نت، ایرانسل و... این سرویس را ارائه می‌دهند، توجه داشته باشید برای استفاده از این خدمات باید مودمی تهیه کنید که سیم کارت قبول کند و خود سیم کارت را از شرکت ارائه دهنده‌ی خدمات دریافت کنید، البته شرکت‌ها هم مودم و هم سیم کارت را ارئه می‌دهند تا با محصولات آنها هماهنگی داشته باشد، در شکل ۳-٦٦ یک مودم از شرکت ایرانسل را مشاهده می‌کنید که سیسم کارت خور است.



شکل ۳ - ۶۶ مودم ایرانسل

تمام این مودم‌ها دارای امکاناتی مانند Port Forwarding، VPN، Firewall و... هستند و می‌توانید بنا به نیاز خود تغییراتی را در آن ایجاد کنید.

اکثر روترها و مودم‌های امروزی داری وایرلس هستند و دستگاهایی مانند موبایل و سیستم‌هایی که دارای دانگل وایرلس هستند می‌توانند به آنها متصل شوند و خدمات دریافت کنند، در مورد این موارد در قسمت‌های بعدی صحبت خواهیم کرد.

۳-٦ رادیو وایرلس

یکی دیگر از امکانات خوب وایرلس این است که اگر شما دارای چند شعبه در یک شهر باشید، برای ارتباط بین شعبات از رادیو وایرلس استفاده کنید، در این روش هر یک از شعبه‌ها از طریق آنتنی به مانند شکل ۳-٦٧ به شعبه‌ی اصلی متصل می‌شوند و با هم اربتاط برقرار می‌کنند، بیشترین آنتنی که در ایران استفاده می‌شود برای شرکت میکروتیک است که آنتن شکل ۳-٦٧ هم برای همین شرکت است.

www.takbook.com



شکل ۳ - ۶۷ رادیو وایرلس

در سازمان‌های ارائه دهنده‌ی سرویس‌های سازمانی از طریق آنتن‌های رادیویی به شما اینترنت می‌دهند، به این صورت است که قبل از راه‌اندازی یک کارشناس به سازمان شما می‌آید و از طریق دوربین مسیرهایی که به رادیو شرکت آنها متصل می‌شود را بررسی می‌کند، در صورتی که رادیو آنها در چند کیلومتری شرکت و در دسترس باشد، سرویس مورد نظر را برای شما راه‌اندازی می‌کنند.
توجه داشته باشید که سایزهای آنتن‌های رادیویی متفاوت است، هر چه آنتن بزرگتر باشد برای فواصل طولانی‌تر مناسب‌تر است، مخصوصاً آنتن‌هایی که به صورت دیش طراحی شده اند.

۳-۷ سرورهای شبکه

اصولاً وقتی نام سرور را می‌شنوید، به دو چیز فکر می‌کنید، یکی سرور سخت‌افزاری و دیگری سرور نرم‌افزاری، سرورهای سخت‌افزاری مشخص و داخل اتاق سرور شما قرار دارند و سرورهای نرم‌افزاری مانند سرور Active Directory در داخل همین سرورهای فیزیکی قرار می‌گیرند و اجرا می‌شوند.
یکی از مهم‌ترین دستگاهایی که در هر سازمان وجود دارد سرورهای شبکه هستند که برای عملیات‌های خاصی طراحی شده‌اند، برای ذخیره‌سازی داده‌ها، برای راه‌اندازی مجازی‌سازی و... می‌توان از سرورهای گوناگون استفاده کرد.
سروهای HP، IBM، Dell و... شرکت‌هایی هستند که کار آنها تولید سرورهای تخصصی است و از کیفیت بالایی برخوردارند، در کشور ایران هم اکثراً از سرورهای شرکت HP استفاده می‌کنند که در شکل ۳-۶۸ یک نمونه از سرور را بررسی و تجهیزات داخل آن را بررسی خواهیم کرد.
سرورهای HP در انواع و اقسام مختلف وجود دارند که سعی می‌کنیم بعضی از مهمترین آنها را بررسی کنیم تا دید کلی از آنها داشته باشیم.
سرورهای اچپی شامل مدل‌های زیر است:

- HPE Proliant

www.takbook.com

- HPE Senergy
- HPE Edgeline
- HPE Simplivity
- HPE Superdome Flex
- HPE Apollo HPE Cloudline
- HPE Composable Rack

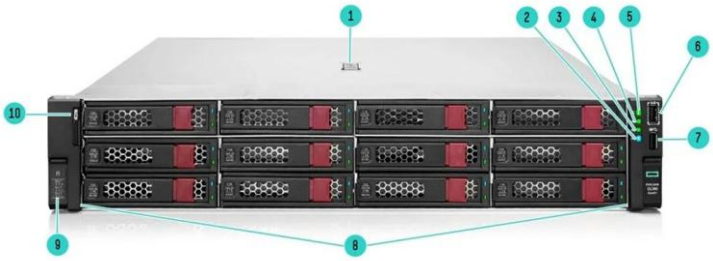
توجه داشته باشید نام اصلی شرکت HP به صورت Hewlett-Packard-Enterprise(HPE) است، در ادامه سرورهای HPE Proliant را با هم بررسی می‌کنیم و با سخت‌افزارهای آن بیشتر آشنا می‌شویم.

در شکل ۳-۶۸ سرور HPE ProLiant DL380 Gen11 را مشاهده می‌کنید، این نوع سرورها یکی از پر کاربردترین سرورهای مورد علاقه مدیران شبکه است.



شکل ۳ - ۶۸ سرور HP

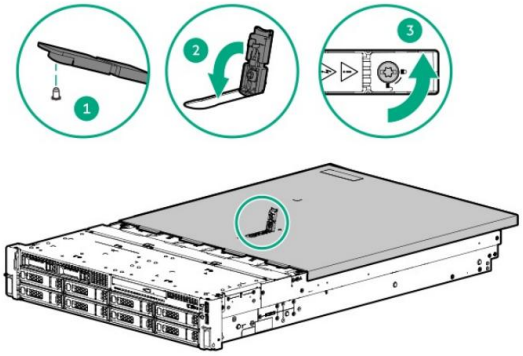
شکل ۳-۶۹، جلوی سرور HP را نشان می‌دهد که هر کدام از اجزای آن را با شماره مشخص کردیم که با هم بررسی می‌کنیم.



شکل ۳ - ۶۹ جلوی سرور HP

۱- بر روی سرور یک درپوش قرار دارد و یک شاسی هم دارد که می‌توانید این درپوش را قفل و یا باز کنید که در شماره‌ی یک مشخص شده است، در شکل ۳-۷۰ دقیقاً این ضامن مشخص شده است و نحوه‌ی باز و بسته کردن آن را مشاهده می‌کنید.

www.takbook.com



شکل ۳ - ۷۰ درب سرور HP

۲- مربوط به دکمه UID/LED است، این دکمه زمانی به کار می‌آید که در یک مکان از چندین سرور استفاده کنید و اگر بخواهید پشت سرور را بررسی کنید نمی‌دانید کدام سرور است و اشتباه خواهید شد، با روشن کردن این دکمه یک نور آبی در پشت سرور نمایان خواهد شد و سرور مورد نظر مشخص خواهد شد که در شکل ۳-۷۱ این دکمه را مشاهده می‌کنید.



شکل ۳ - ۷۱ چراغ UID

۳- LED وضعیت کارت شبکه است که اگر خراب باشد به شما نمایش داده می‌شود.

۴- LED مربوط به سلامت سرور است که قانون‌های خاص خودش را دارد ومثلاً با تعداد فلش‌هایی که می‌زند مشخص می‌کند CPU و یا دستگاه دیگری خراب است.

۵- LED مربوط به خاموش و روشن شدن سرور است و اینکه دکمه خاموش و روشن شدن هم است.

۶- مربوط به پورت ILO است که در قسمت سرورها و تنظیم آنها به آن می‌پردازیم، فقط به این نکته اشاره کنیم که این پورت برای مدیریت سرور است و حتی سرور اگر خاموش باشد هم می‌توانید به تنظیمات سرور دسترسی داشته باشید و وضعیت را چک کنید.

۷- پورت USB 3.0 که می‌توانید به آن فلش و یا هر دستگاهی که نیاز به USB دارد را متصل کنید.

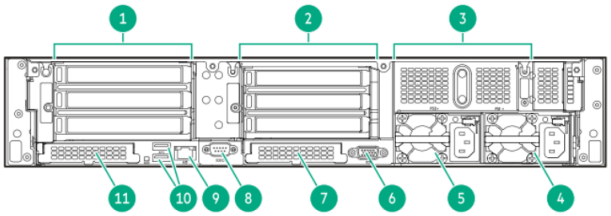
۸- تعداد ورودی‌های Hrad disk است که برای این سرور X12 است که با LFF نشان داده می‌شود، منظور از LFF همان Large Form Factor است که به هاردهای بزرگ 3.5 اینچی گفته می‌شود.

www.takbook.com

۹- مربوط به برچسب پشتیبانی سرور است.

۱۰- مربوط به شناسنامه سرور است و در آن نام کاربری و رمز عبور مربوط به ILO نوشته شده است که در آینده بررسی خواهیم کرد و همچنین سریال دستگاه.

بعد از اینکه جلوی سرور را بررسی کردیم حالا می‌خواهیم بررسی کنیم، در پشت سرور HP چه قسمت‌های وجود دارد، دوستان عزیز توجه داشته باشید سرورها در طراحی‌های مختلفی وجود دارند و شاید سروری که شما در سازمان خود دارید با سروری که در این قسمت بررسی می‌کنیم کاملاً متفاوت باشد.

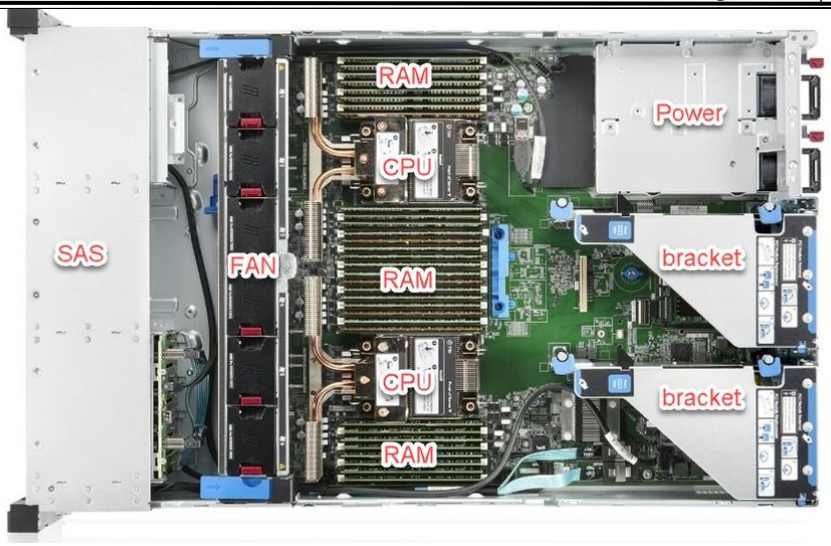


شکل ۳ - ۷۲ پشت سرور HP

در شکل ۳-۷۲، قسمت‌های شماره‌ی 1,2,3,11,7 مربوط به Slot هستند و می‌توانید کارت‌های مورد نظر خود را به سرور اضافه کنید و از آن خروجی تهیه کنید، کارت‌هایی مانند کارت گرافیک، کارت شبکه و ... در قسمت شماره‌ی 10 که مربوط به پورت‌های USB 3.0 است، قسمت شماره‌ی 8 مربوط به پورت سریال است، قسمت شماره‌ی 8 پورت VGA و برای خروجی مانیتور است، قسمت شماره‌ی 9 مربوط به پورت ILO است و در آخر قسمت‌های 4,5 مربوط به ماژول پاور است که بر روی سرور همیشه دو پاور قرار می‌گیرد تا LoadBalance باشد و خاموش نشود.

بعد از بررسی پشت سرور باید داخل سرور که مهترین بخش است را بررسی کنیم، در شکل ۳-۷۳ نمای داخلی سرور را مشاهده می‌کنید که باید هر کدام از قسمت‌های آن را توضیح دهیم، سرورهای HP دارای دو سوکت CPU و تعداد ۳۲ سوکت رم هستند، که در شکل ۳-۷۳، دقیقاً مشخص شده است.

www.takbook.com



شکل ۳ - ۷۳ داخل سرور HP

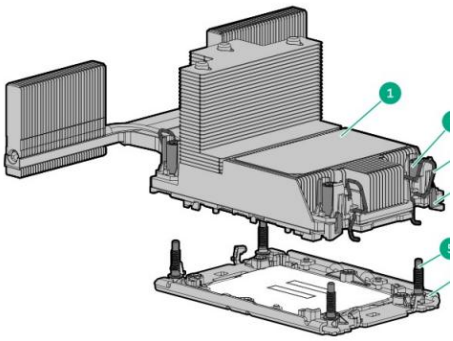
برای این سرور (HP DL380 G11) باید CPU مدل Xeon نسل ٥ را تهیه کنید البته نسل 4 هم پشتیبانی می‌کند، در شکل ۳-۷٤، CPU شرکت اینتل را مشاهده می‌کنید که نسل پنجم این نوع CPU است و دارای ٦۰ هسته محاسباتی است، این نوع CPUها از ۲۲.٥ تا ۱۱۲.٥ حافظه Cash دارند که می‌تواند بسیار خوب باشد.



شکل ۳ - ۷۴ CPU XEON

توجه داشته باشید بر روی سرورهای HP اصولاً دو CPU قرار می‌گیرد، بر روی این CPUها دو Heatsink برای خنک کردن قرار می‌گیرد که شکل کلی آن به صورت شکل ۳-۷٥ است.

www.takbook.com



شکل ۳ - ۷۵ Heatsink

برای اینکه گرمای داخل سرور خارج شود از 6 تا فن پر سرعت استفاده می‌شود که شکل ۳-۷۶، همین فن را نشان می‌دهد، این نوع فن‌ها به صورت ماژولار بر روی سرور نصب می‌شوند و زمانی که برای اولین بار سرور را روشن می‌کنید صدای خیلی بلندی دارند.



شکل ۳ - ۷۶ فن

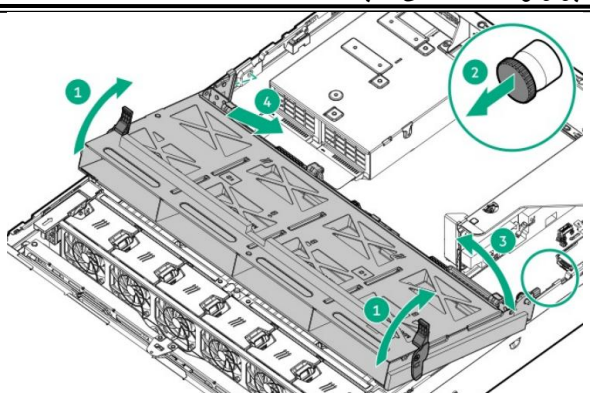
همان‌طور که گفتیم تعداد Fanهای داخل سرور HP شش عدد است و برای اینکه این فن‌ها جهت باد درستی داشته باشند باید از درپوش مخصوص جریان هوا مانند شکل ۳-۷۷ استفاده کنید، به این قطعه Plastic Airflow یا بافل جریان هوا گفته می‌شود که بر روی رم و CPU قرار می‌گیرد و باعث خنک شدن هر چه بهتر آنها خواهد شد.



شکل ۳ - ۷۷ درپوش CPU

در شکل ۳-۷۸ نحوه‌ی قرار گیری بافل جریان هوا در سرور را به صورت گرافیکی مشاهده می‌کنید.

www.takbook.com



شکل ۳ - ۷۸ نحوه‌ی قرارگیری درپوش CPU

اگر بخواهیم در مورد رم صحبت کنیم، باید بگوییم که تعداد رم‌هایی که پشتیبانی می‌شود، ۳۲ رم DDR5 است که دارای سرعت ٤٨٠٠ مگاهرتز هستند، که در شکل ۳-۷۹ این مدل از رم را مشاهده می‌کنید.

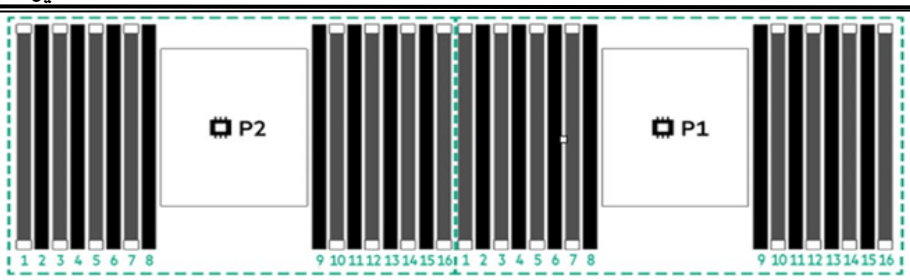


شکل ۳ - ۷۹ رم سرور

نکته مهمی که در استفاده از رم وجود دارد این است که باید بدانید، رم خود را در کدام اسلات قرار دهید، ما فرض را بر این میگذاریم که سرور شما دارای دو CPU است که در شکل ۳-۸۰، هم مشخص شده است، در سرور G11 هر CPU دارای 16 اسلات رم است که باید به شماره‌های زیر Slot دقت کنید، اگر دو رم دارید و دو CPU باید در اسلات یک هر کدام از CPUها یک رم قرار دهید تا وقتی سیستم روشن می‌شود با خطا روبرو نشوید.

پس اگر ۱۰ عدد رم دارید باید به صورت نصف به نصف یعنی 5تا برای CPU اول که در اسلات‌های ۱ تا ٥ قرار می‌گیرد و 5 تا رم دیگر در اسلات‌های CPU دوم قرار می‌گیرد تا بار کاری بین هر دو CPU پخش شود، یکی از ویژگی‌های سرورهای HP این است که اگر یکی از رم‌ها خراب شود سرور از کار نخواهد افتاد و فقط مشخص می‌کند کدام رم مشکل دارد و باید عوض شود.

www.takbook.com



شکل ۳ - ۸۰ چینش رم‌ها در سرور

توجه داشته باشید، شرکت HPE یک جدول برای قرار دادن رم در سرور مشخص کرده است، مثلاً برای سرور HP G11 باید از شکل ۳-۸۱ استفاده کنید؛ در این شکل اگر یک رم دارید یعنی 1 DIMM باید آن را در Slot شماره‌ی 10 قرار دهید، اگر ۸ رم دارید باید آن را در Slotهای 1,3,5,7,10,12,14,16 قرار دهید، تا بهترین کارایی و عملکرد را داشته باشد، پس بهتر است طبق این جدول عمل کنید.

HPE ProLiant DL360/DL380/ML350/DL560 Gen11 servers 16 slots per CPU DIMM population order

1 DIMM									10						
2 DIMMs[1]			3						10						
4 DIMMs[1]			3			7			10				14		
6 DIMMs			3		5	7			10				14		16
8 DIMMs[1,2]	1		3		5	7			10		12		14		16
12 DIMMs	1	2	3		5	6	7		10	11	12		14	15	16
16 DIMMs[1,2]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

* HPE DL560 is a 4-socket server (uses P3, P4)
[1] Support Hemi
[2] Support SGX

شکل ۳ - ۸۱ نحوه‌ی قرارگیری رم در سرور HP

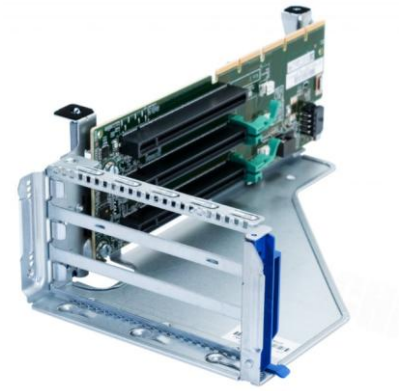
سرورهای HP دارای دو پاور ماژولار هستند که برای Load balance کردن برق سرور به کار می‌روند و اگر یکی از آنها خراب شود دیگری به کار خود ادامه می‌دهد، این نوع پاورها در مدل‌های 800,1000,1600 وات وجود دارند، در جلوی سرورها چراغ وضعیت پاور وجود دارد که در صورت خرابی پاورها به شما هشدار می‌دهد.



شکل ۳ - ۸۲ پاور سرور

www.takbook.com

قسمت دیگری که باید در سرور بررسی کنیم قسمت RISER BRACKET است که کارت‌هایی مانند کارت گرافیک، شبکه و کارت‌هایی دیگر بر روی آن سوار می‌شوند و بر روی اسلات مورد نظر قرار می‌گیرند، در شکل ۳-۸۳، RISER BRACKET را مشاهده می‌کنید، بعد از اینکه کارت‌ها بر روی آن قرار گرفتند به سادگی بر روی Main اصلی سرور پیچ می‌شود، در شکل ۳-۸۳ RISER BRACKET را مشاهده می‌کنید که سه کارت را پشتیبانی می‌کند.



شکل ۳ - ۸۳ *RISER BRACKET*

اگر به قسمت هاردها مراجعه کنیم، هاردهایی که بر روی سرور DL380 G11 قرار می‌گیرند، می‌توانند از نوع‌های مختلف باشند، اما هاردهای عمومی‌تر که همه سازمان‌ها از آن استفاده می‌کنند، SAS است که از سرعت و کیفیت خوبی برخوردار است، توجه داشته باشید یکی از ویژگی‌های سرورها شبکه این است که هاردها را به صورت Raidبندی منظم می‌کنند، در مورد Raidبندی در سرور HP در ادامه به صورت مفصل صحبت خواهیم کرد اما باید به این نکته اشاره کنیم که عملیات Raidبندی به صورت نرم‌افزاری و سخت‌افزاری انجام می‌شود که در سرورهای HP با استفاده از قطعه‌ای به نام Raid Controller این عملیات را انجام می‌دهند، انواع مختلفی از Raid Controller وجود دارد، یکی به صورت کارت است که در شکل ۳-۸٤ مشاهده می‌کنید.



شکل ۳ - ۸۴ کارت *Raid Controller*

www.takbook.com

دیگری هم در قسمت مشخصی بر روی مین اصلی نصب می‌شود که دقیقاً در شکل ۳-۸۵ جایگاه آن را مشخص کردیم.



شکل ۳ - ۸۵ کارت *Raid Controller*

توجه داشته باشید که Raid Controller از سرعت و کیفیت مختلفی برخوردار است مثلاً برای سرور HP G11 می‌توانیم از مدل HP Smart Array P440ar 2GB Cache 8 Port 12G SAS 6G SATA Raid Controller استفاده کنید که شکل ۳-۸۶ نشان دهمده‌ی این کارت است، این مدل با ۲ گیگبایت کش و دارای ۸ پورت ۱۲ گیگ برای هاردهای سرور است.



شکل ۳ - ۸۶ کارت *Raid Controller*

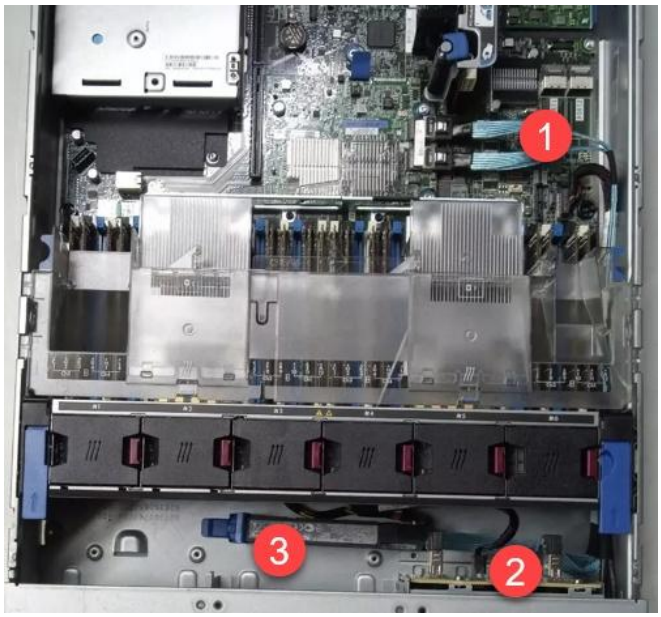
نکته بسیار مهم این است که زمانی که هاردهای خود را Raidبندی می‌کنید، دستگاه Raid Controller حتماً باید به باتری متصل باشد تا در زمان قطعی برق تنظیماتی که برای هاردها انجام دادید از بین نرود، در شکل ۳-۸۷، Raid Controller به همراه یک باتری را مشاهده می‌کنید که این باتری مسئول حفظ برق این دستگاه است و باعث نگه داشتن تظیمات آن می‌شود.

www.takbook.com



شکل ۳ - ۸۷ باتری Raid Controller

توجه داشته باشید، یک سری کابل اصولاً با رنگ آبی وجود دارد که متصل به قسمت جلویی سرور و هاردها هستند و به صورت پیش‌فرض در قسمت سمت راست سرور نصب هستند که آنها را باید جدا کنید و به Raid Controller متصل کنید تا اطلاعات از این قطعه دریافت شود، در شکل ۳–۸۸ دقیقاً این موضوع مشخص شده است، در قسمت شماره‌ی یک کابل‌های آبی رنگ را مشاهده می‌کنید که به Raid Controller متصل شده‌اند و در قسمت شماره‌ی دو همان کابل آبی رنگ پشت ورودی سوکت هاردهای سرور متصل شده است و در قسمت شماره‌ی سه می‌توانید باتری مربوط به Raid Controller را که در بالا بررسی کردیم را مشاهده کنید.



شکل ۳ - ۸۸ جایگاه باتری در سرور

www.takbook.com

۸-۳ یو پی اس

UPS (Uninterruptible power supply) یا همان منبع تغذیه بدون وقفه، 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 معمولاً درون خود، باتری دارند که هنگام وجود برق در حالت عادی آن را شارژ می‌کنند؛ هنگام قطع برق یا افت ولتاژ، زمانی که 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.

UPSها در اندازه‌ها و قدرت‌های مختلفی وجود دارند که نمونه‌ای از آنها را در شکل ۳-۸۹ مشاهده می‌کنید، بعضی از UPS ها برای شارژ دستگاه‌های شبکه از باتری جداگانه استفاده می‌کنند.

برای انتخاب UPS مناسب باید با متخصص این کار صحبت کنید تا دقیقاً طبق نیازمندی شما یک مدل مناسب معرفی کند.

یوپی‌اس‌ها را از نظر عملکرد داخلی غالباً در سه دسته تقسیم‌بندی می‌کنند:

- آفلاین
- آنلاین
- لاین اینتراکتیو

آفلاین

این نوع UPSها در سایزهای کوچک هستند و عموماً از ۲۰ تا ۳۰ دقیقاً برق را حفظ می‌کنند، و برای حفاظت از سیستم‌های کاربران کاربرد دارد، مثلاً در این زمان کاربر می‌تواند با آرامش برنامه‌های خود را ذخیره و ببندد و سیستم را خاموش کند، در شکل ۳-۸۹، نمونه‌ای از UPS آفلاین را مشاهده می‌کنید، توجه داشته باشید که در بعضی از مدل‌ها می‌توانید به شبکه متصل کنید و از Log آن بفهمید که UPS در چه وضعیتی قرار دارد، نکته‌ی دیگر در مورد این UPSها این است که از فن خنک کننده استفاده نمی‌کنند و کاملاً بی‌صدا هستند.

www.takbook.com



شکل ۳ - ۸۹ UPS



شکل ۳ - ۹۰ UPS

آنلاین

این نوع UPSها از قدرت بالاتری برخوردارند و مختص اتاق سرور طراحی شده است و دارای چندین باتری هستند که به صورت سری به هم متصل هستند، در شکل ۳-۹۱ یک UPS مدل APC Smart-UPS On-Line, 10kVA/10kW را مشاهده می‌کنید که کیفیت خوبی دارد.

در ایران برای خرید UPS به مقدار کاوا نگاه می‌کنند، هر چقدر مقدار کاوا (kW) بالاتر باشد قدرت UPS بیشتر و زمان بیشتری می‌تواند برق را نگه دارد.



شکل ۳ - ۹۱ UPS

www.takbook.com



شکل ۳ - ۹۲ UPS

لاین اینتراکتیو

یکی از ویژگی‌های UPS اینتراکتیو این است که زمانی که برق قطع می‌شود در زمان خیلی کم بین ۲ تا ٤ میلی ثانیه سوئیچینگ را انجام می‌دهد و همین زمان کم باعث می‌شود دستگاهایی که به برق متصل هستند چیزی متوجه نخواهند شد و این عملکرد روی مدارات الکترونیکی تاثیر خوبی خواهد داشت و با نوسانات برقی روبرو نخواهند شد، در شکل ۳-۹۳ این دستگاه را مشاهده می‌کنید.



شکل ۳ - ۹۳ لاین اینتراکتیو

www.takbook.com

www.takbook.com

فصل چهارم

طراحی اتاق سرور

بعد از اینکه دستگاه‌ها و ابزار مختلف را در قسمت قبلی بررسی کردیم نوبت آن می‌رسد تا در مورد طراحی یک دیتاسنتر و اتاق سرور خوب صحبت کنیم و تمام تجهیزات آن را بررسی کنیم.

اولین قدم بررسی نیازهای سازمان شما است، که باید بدانید به چه مقدار فضا برای طراحی اتاق سرور نیاز دارید، مثلاً باید تعداد سرورهایی که می‌خواهید استفاده کنید را بدانید، تعداد رک‌هایی که می‌خواهید مستقر کنید، تعداد باتری‌های UPS و...

دیتاسنتر

مرکز داده یا دیتاسنتر (Data Center) به مجموعه‌ای از سرویس‌ها، زیرساخت‌های ارتباطی/امنیتی و تجهیزات الکترونیکی گفته می‌شود که برای نگهداری و پشتیبانی از سرویس‌های تحت شبکه بکار برده می‌شوند. سازمان‌ها، شرکت‌ها و افراد می‌توانند با به‌کارگیری سرویس‌های ارائه شده از طرف مرکز داده، اطلاعات و سرویس‌های مبتنی بر شبکه خود را بر روی اینترنت (اینترانت/اکسترانت) راه‌اندازی کنند. مرکزداده، بسته به نوع کاربردی که برای آن تعریف شده‌است، می‌تواند به عنوان یک مرکز پردازشی، مرکز ذخیره داده، مرکز جمع‌آوری داده یا تمامی این موارد عمل کند. مراکز داده بسیار عظیم و متنوعی در سرتاسر شبکه جهانی اینترنت در حال سرویس‌دهی هستند که برخی از این مراکز استفاده تجاری محدود درون سازمانی دارند و برخی دیگر در اینترنت به صورت تجاری یا عمومی قابل استفاده هستند، مانند دیتاسنتر شرکت گوگل که به استفاده از لینک زیر می‌توانید این دیتاسنتر فوق العاده را مشاهده کنید:
https://www.youtube.com/watch?v=swlKPGOmW4s



شکل ۴- ۱ مرکز دیتاسنتر

www.takbook.com

مراکز داده را با توجه به اندازه و کارکرد به دسته‌های زیر تقسیم می‌کنیم:

۱- شبکه‌های سازمانی، تجاری یا دانشگاهی
۲- شهرک یا پردیس مرکز داده
۳- شبکه‌های خصوصی WAN
۴- فراهم‌کننده‌های سرویس (SP)
۵- مراکز داده اینترنتی (IDC)
۶- مراکز داده فراسازمانی (Extranet)
۷- مراکز داده محلی (Intranet)

قطعاً طراحی دیتاسنتر یک تیم فوق‌العاده می‌خواهد و یک سری استانداردهایی که باید آنها را رعایت کرد، برای بررسی استانداردهای طراحی یک دیتاسنتر خوب باید از استاندارد TIA942 استفاده کنید، که در این استاندارد تمامی موارد طراحی یک دیتاسنتر را به شما می‌گوید.

در این کتاب سعی کردیم یک اتاق سرور کامل (مراکز داده محلی) با تمام تجهیزات آن را بررسی کنیم که البته اگر در ابعاد بزرگ بخواهیم این کار را انجام دهیم هم شدنی و کاربردی است.

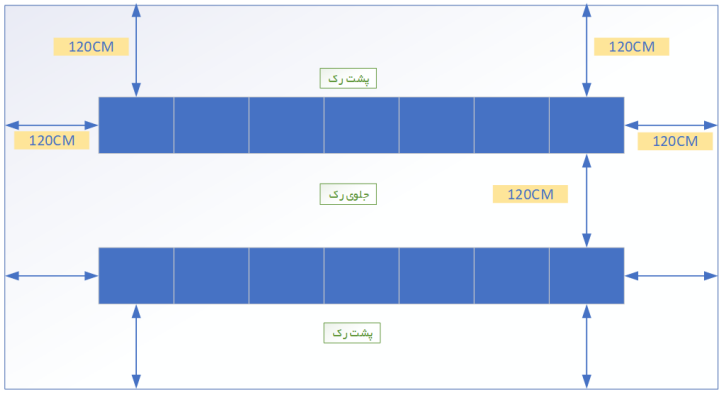
۱-٤ ابعاد اتاق سرور

اولین کاری که باید برای طراحی اتاق سرور در نظر بگیرد انتخاب محلی مناسب برای این کار است، شما باید بدانید که این اتاق در چه طبقه‌ای از سازمان شما قرار می‌گیرد، بهترین طبقه برای انتخاب این اتاق طبقات پایین ساختمان است تا در برابر خطراتی مانند زلزله و ... مقاوم‌تر باشد.

ابعاد یک اتاق استاندارد به این صورت است که سقف آن حداقل باید ۲ متر و ۷۰ سانتی متر طول داشته باشد و عرض آن هم به تعداد رک‌های موجود در اتاق بستگی دارد، در مورد رک در قسمت بعدی توضیح خواهیم داد.

در شکل ٤-۲، یک اتاق سرور را مشاهده می‌کنید که در آن چندین رک به صورت چسبیده وجود دارد، نکته‌ای که در این شکل وجود دارد این است که رک‌های حداقل باید فضای 120CM را با دیوار کناری و جلوی خود داشته باشند تا درهای رک بتواند باز و بسته شوند و شخص مسئول هم بتواند به راحتی بین رک‌ها حرکت کند.

www.takbook.com



شکل ۴- ۲ چیدمان اتاق سرور

توجه داشته باشید که باید در زیر اتاق سرور کف کاذب بزنیم که حداقل ۲۰ سانتی متر باشد و در بالای اتاق سرور سقف کاذب با حداقل ۱۵ سانتیمتر فضا داشته باشد.

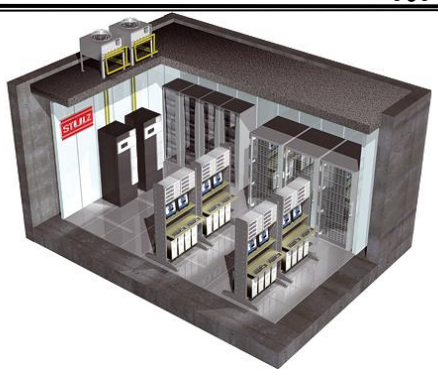
در قسمت قبل، یک استاندارد اولیه از ابعاد اتاق سرور ا مشاهده کردیم که اگر بخواهیم به این اتاق سرور رک‌ها، دستگاه UPS، باتری و... اضافه کنیم باید اتاق بزرگتری در نظر بگیریم.

۲-٤ سیستم سرمایش

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.

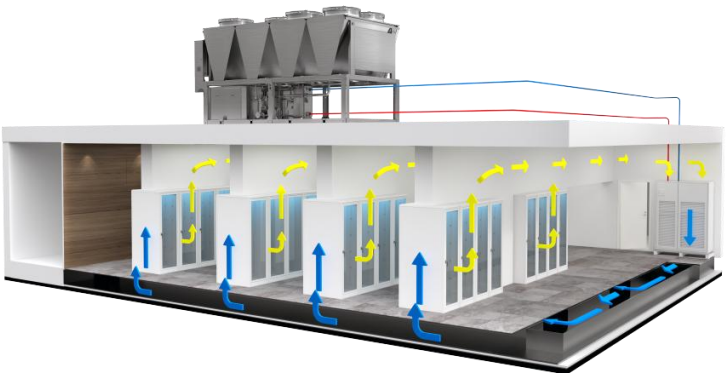
در شکل ٤-۳، یک سیستم سرمایشی پیشرفته‌تر از کولرهای گازی را مشاهده می‌کنید که دستگاه تهویّه‌ی هوا در بالای ساختمان تعبیه شده و از طریق لوله‌کشی به داخل اتاق سرور انتقال داده شده است.

www.takbook.com



شکل ۴- ۳ سیستم سرمایش

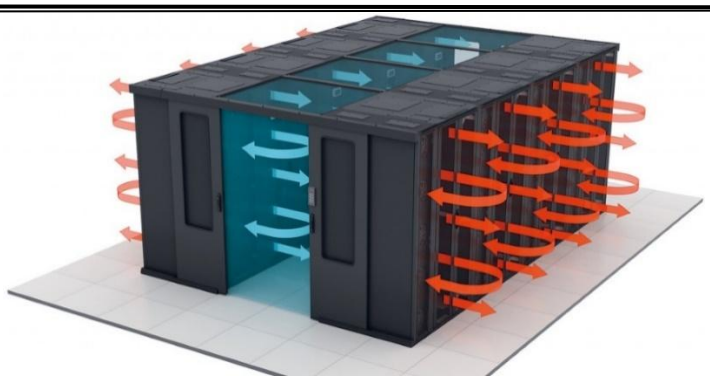
در شکل ٤-٤، نوع پیشرفته‌تری از سیستم تهویّه‌ی هوا را مشاهده می‌کنید که نحوه‌ی گردش هوا در اتاق سرور مشخّص شده است، به این نکته نیز توجّه داشته باشید که این نوع سیستم‌ها، تنها برای اتاق سرورهای بزرگ کارایی دارد.



شکل ۴- ۴ سیستم سرمایش

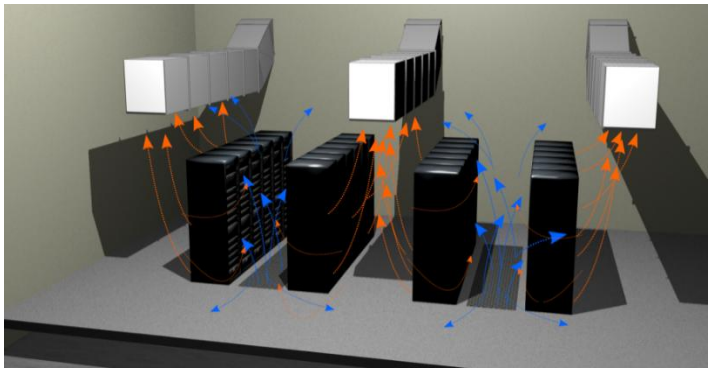
توجه داشته باشید که در یک اتاق سرور رک‌های مختلفی قرار دارد و روی این رک‌های سرور قرار می‌گیرد، نکته‌ای که در مورد سرمایش سرورها وجود دارد این است که سرورها خودشان دارای فن هستند که قبلاً هم بررسی کردیم، این فن‌ها هوا را از جلو به داخل سرور می‌کشند و از پشت سرور خارج می‌کنند، پس مهم است که سیستم خنک کننده جلوی رک‌ها را سرد کند، تا هوای خنک وارد سرورها شود و هوای گرم از پشت سرور خارج شود، در شکل ٤-٥ دقیقاً این موضوع مشخص شده است که هوای سرد از جلوی رک وارد می‌شود و از پشت رک خارج می‌شود.

www.takbook.com



شکل ۴- ۵ سیستم سرمایش

نکته‌ی دیگری که وجود دارد این است که در دیتا سنترها و اتاق سرورها رک‌ها دقیقاً کنار هم قرار دارند و به مانند شکل ٤-٦ دو مسیر ایجاد می‌شود که یکی مسیر سرد و دیگری مسیر گرم است.



شکل ۴- ۶ سیستم سرمایش

۱-۲-٤ کولر گازی

حالا اگر بخواهیم به صورت دقیق یک سیستم سرمایشی انتخاب کنیم باید ببینیم که ابعاد اتاق سرور و تجهیزاتی که در آن قرار دارد چقدر است، اگر برای یک اتاق سرور کوچک می‌خواهید سیستم سرمایشی قرار دهید، ارزان‌ترین راه استفاده از کولر گازی است. که شکل ٤-٧



شکل ۴- ۷ کولر گازی

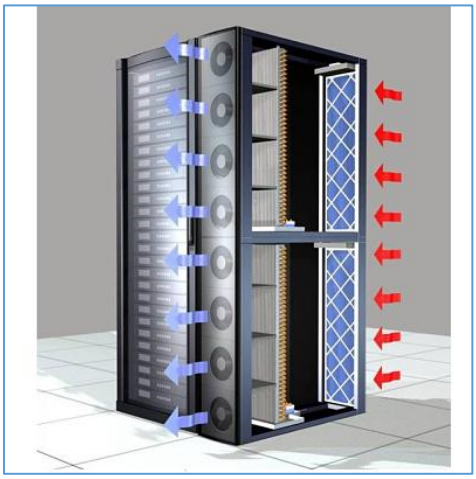
www.takbook.com

معایب استفاده از کولر گازی این است که احتمال خرابی آن در مدت زمان طولانی وجود دارد، چون همیشه باید روشن باشد، مشکل دیگری که وجود دارد این است که کولر گازی رطوبت اتاق را به صفر می‌رساند و این خوب نخواهد بود چرا که طبق استانداردها رطوبت اتاق سرور باید بین ٤٠ تا ٥٥ درصد باشد تا آسیب کمتری به دستگاه‌های شبکه برسد.

توجه به این نکته مهم است که برای اتاق سرور بهتر است از کولرهای اینورتردار استفاده کنید که هم در کاهش هزینه‌ها کمک خواهد کرد و هم در زمستان بهترین کارایی را خواهد داشت.

٤-٢-٢ خنک کردن با روش InRow

در این روش سیستم خنک کننده بین رک‌ها قرار می‌گیرد و هوای خنک را به جلوی رک ارسال می‌کند و هوای گرم را از پشت رک دریافت و به بیرون از اتاق انتقال می‌دهد، این سیستم هم کار خنک‌سازی اتاق را انجام می‌دهد و هم طراحی خوبی به اتاق سرور شما می‌بخشد، در شکل ٤-٨ این روش را مشاهده می‌کنید.



شکل ۴- ۸ روش InRow

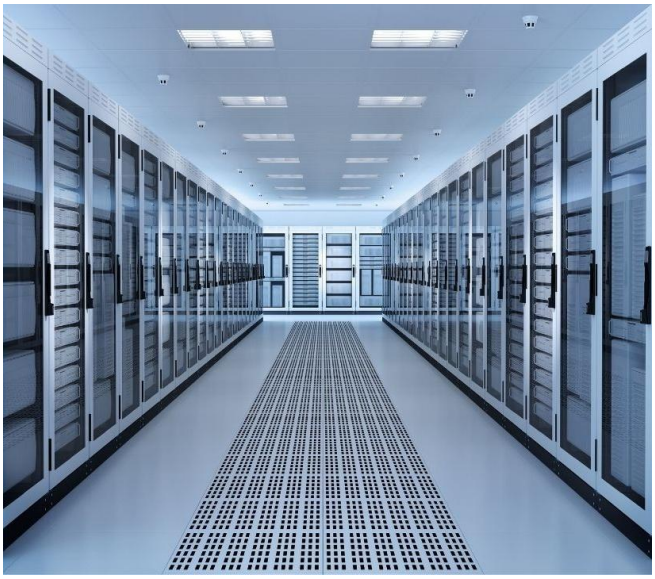
٤-٢-٣ خنک سازی از کف

در این روش خنک‌سازی، هوای سرد از زیر کف کاذب هدایت شده و به جلوی سرور انتقال داده می‌شود که شکل ٤-٩ و ٤-١٠، نشان ندهده‌ی این موضوع است.

www.takbook.com



شکل ۴- ۹ خنک سازی از کف

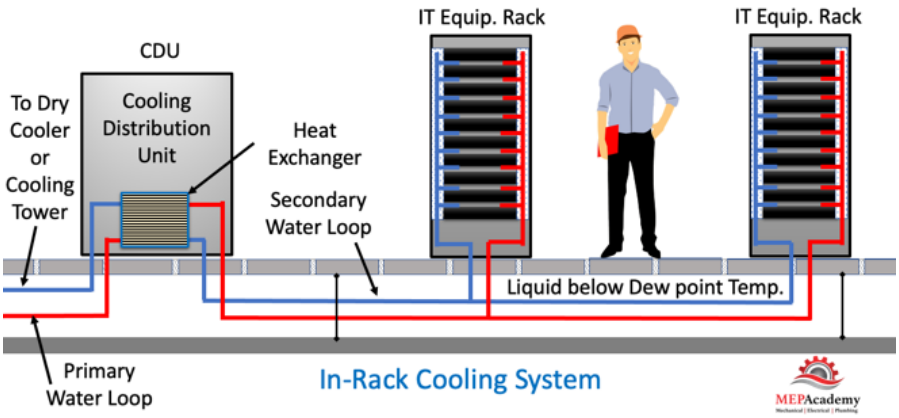


شکل ۴- ۱۰ خنک سازی از کف

٤-۲-٤ خنک‌سازی از داخل رک

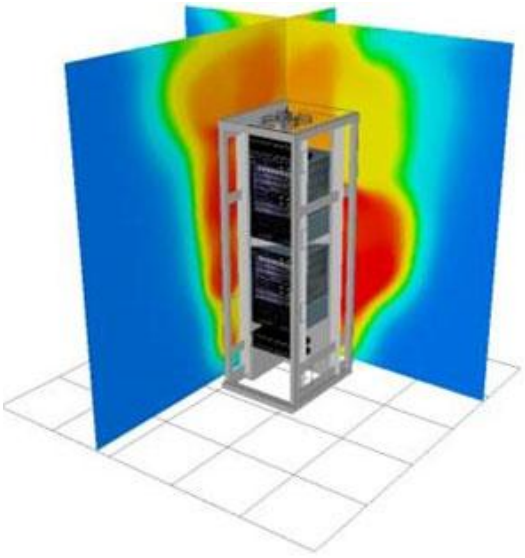
روش دیگری هم وجود دارد که خنک‌سازی از داخل رک اجرا می‌شود، در این روش هوای سرد به داخل رک انتقال داده می‌شود و هوای گرم از آن خارج می‌شود که شکل ٤-۱۱ نشان دهنده‌ی این روش است.

www.takbook.com



شکل ۴- ۱۱ خنک‌سازی از داخل رک

نکته‌ی مهم در مورد قرار دادن رک در اتاق این است که اگر رک را در کنار دیوار قرار دهید، به مانند شکل ۱۲-٤، سرورها در مجاورت گرمای بیشتری قرار می‌گیرند که حتماً باید رک‌ها را در وسط اتاق قرار دهید، یا فصله ۱۲۰ سانتی متر را رعایت کنید.



شکل ۴- ۱۲ نحوه‌ی قرارگیری رک در اتاق سرور

۳-٤ 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

www.takbook.com

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 درآید، 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 درآید، در شکل ٤-١٣ یک دماسنج را مشاهده می‌کنید که بر روی رک بسته می‌شود و مقدار دمای محیط را کنترل می‌کند.



شکل ۴-۱۳ دماسنج

اطلاعاتی که به دماسنج ارسال می‌شود از طریق یک سنسور کوچک است که در اتاق قرار دارد و به دماسنج ارسال می‌شود که در شکل ٤-١٤ این دماسنج مشخص است.



شکل ۴-۱۴ دماسنج

در نوع دیگری از دستگاه‌های اطفای حریق از سنسور دود استفاده می‌شود، در شکل ٤-١٥، نمونه‌ای از دتکتور دود را مشاهده می‌کنید که بعد از اینکه دود در سنسورهای آن دریافت شد، آژیر خطر به صدا در خواهد آمد.

www.takbook.com



شکل ۴- ۱۵ سنسور دود

توجه داشته باشید، بعد از اینکه از طریق سنسورهای دما و دود، اطلاعات دریافت شد به دستگاه مرکزی ارسال خواهد شد و بعد از بررسی اگر مقدار دما بالاتر از حد باشد و دود هم دریافت شود آژیر خطر به صدا در خواهد آمد، در شکل ٤-١٦ یک آژیر را مشاهده می‌کنید که اصولاً بیرون از اتاق سرور نصب می‌شود.



شکل ۴- ۱۶ آژیر خطر

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 که نمونه‌ی آن را در شکل ٤-١٧ مشاهده می‌کنید.

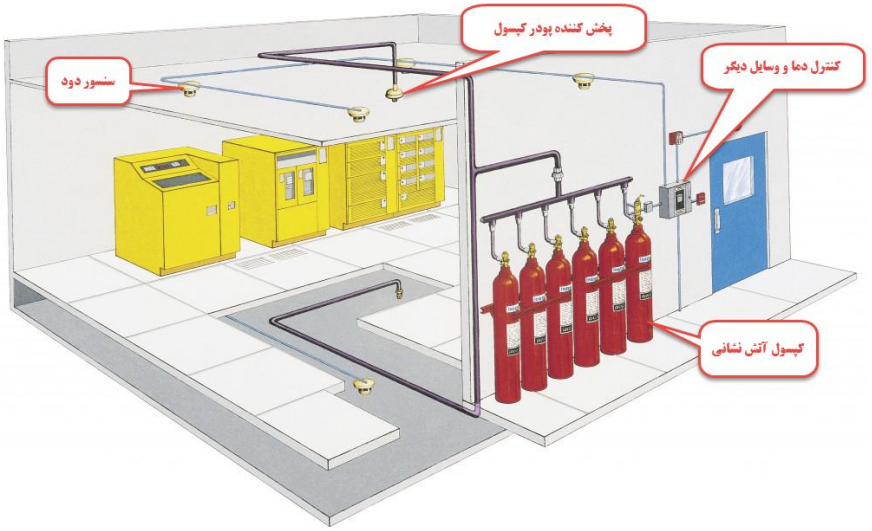


شکل ۴- ۱۷ کنترل رطوبت اتاق

در شکل ٤-١٨، 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

www.takbook.com

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، نکته‌ای که در اینجا باید به آن اشاره کنیم این است که دستگاه کنترل دما که در شکل ٤-١٨ مشخص است دارای باتری ذخیره می‌باشند و در صورتی که برق قطع شود دستگاه به کار خود ادامه خواهد داد.



شکل ۴- ۱۸ نمونه‌ی طرّاحی‌شده‌ی یک اتاق سرور

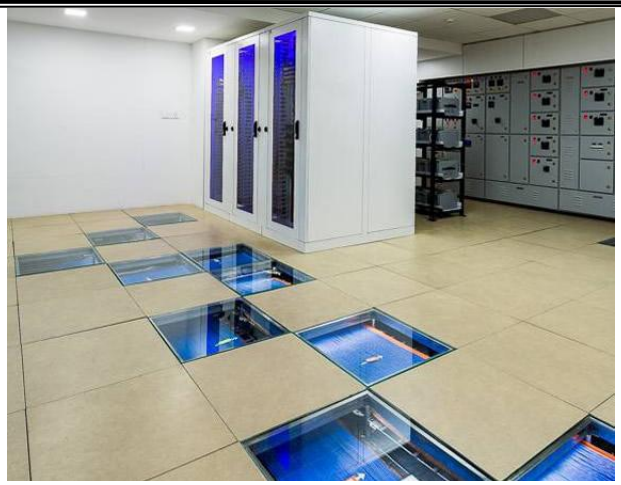
دستگاه‌های دیگری هم در اتاق سرور برای اعلام آتش‌سوزی و خطر وجود دارد ، مانندستگاه تلفن کننده که در صورتی که اطلاعات خطر را دریافت کردن با شماره‌ی خاصی تماس می‌گیرند و پیغام‌های ضبط شده‌ای را ارسال می‌کنند.

سیستم‌های پیامکی هم وجود دارند که در صورت دریافت مشکل با شماره‌ی خاصی پیامک می‌دهند.

٥-٤ کف کاذب

در اتاق سرور و مخصوصاً دیتاسنترهای بزرگ برای اینکه ایمنی و استاندارد را پیاده‌سازی کنیم باید از کف کاذب استفاده کنیم، مهمترین دلیل استفاده از کف کاذب این است، به عنوان ارت عمل می‌کند و قابلیت جذب الکتریسیته را داشته باشد، در شکل ٤-١٩ نمای کلی از کف کاذب را در یک اتاق سرور مشاهده می‌کنید.

www.takbook.com



شکل ۴- ۱۹ کف کاذب

اگر به شکل ٤-۲۰ توجه کنید کف کاذب دارای پایه می‌باشد و دقیقاً این کف‌ها کنار هم قرار می‌گیرند.



شکل ۴- ۲۰ کف کاذب

توجه داشته باشید که روکش‌هایی با عنوان HPL و PVC وجود دارد که برای برای جذب الکتریسیته ساکن کاربرد دارند که البته بر روی کف‌های کاذب فولادی و آلومینیومی کاربرد دارند، اما بعضی از کف کاذب‌ها خودشان قطعه‌ای به نام تایل ارتینگ دارند که کار آن جذب الکتریسیته ساکن است و انتقال آن به چاه ارت است، در شکل ٤-۲۱، قطعه‌ی تایل ارتینگ را مشاهده می‌کنید که بر روی کف کاذب نصب می‌شود، توجه داشته باشید طبق استاندارد در هر ٦ متر مربع باید یک قطعه از این بر روی کف کاذب نصب شود تا الکتریسیته‌ی کاذب از محیط مورد نظر دفع شود.

www.takbook.com



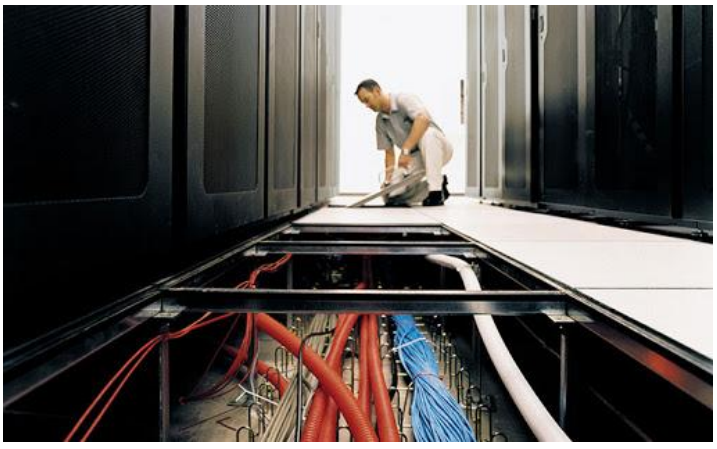
شکل ۴- ۲۱ روکش‌های HPL و PVC

بعد از نصب تایل ارتینگ بر روی کف کاذب از طریق سیم ارت الکتریسیته‌ی ساکن به شین ارت مرکزی متصل می‌کنیم و از آن طریق الکتریسیته‌ی ساکن جذب می‌شود، در شکل ٤-۲۲، قطعه‌ی شین ارت را مشاهده می‌کنید که کابل‌ها به آن متصل شده و به چاه ارت انتقال داده می‌شوند.



شکل ۴- ۲۲ شین ارت مرکزی

یکی دیگر از ویژگی‌های کف کاذب این است که شما می‌توانید تمام کابل‌های مورد نیاز خود را از این کف عبور دهید و نظم خاصی را به اتاق خود ببخشید، در شکل ٤-۲۳ این موضوع مشخص شده است و کابل‌های مربوط به رک‌ها و دیگر موارد از کف عبور داده شده است.



شکل ۴- ۲۳ کف کاذب

www.takbook.com

٤-٦ سقف کاذب

یکی دیگر از موضوعات مهم در طراحی اتاق سرور سقف آن است، برای اینکه لوله کشی‌های مربوط به سیستم اطفای حریق، کابل‌های شبکه و دوربین‌های مدار بسته و... را انجام دهیم نیاز به سقف کاذب در اتاق سرور داریم، در شکل ٤-٢٤ نمونه‌ای از کف کاذب را مشاهده می‌کنید.



شکل ۴- ۲۴ سقف کاذب

٤-٧ رک‌ها

برای اینکه سرورها به صورت منظّم و با امنیّت بیشتر در اتاق سرور قرار دهید، بهتر است به تعداد مورد نیاز رک 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.

رک‌ها در شبکه به به دو نوع تقسیم می‌شوند:

۱- ایستاده

۲- دیواری

٤-٧-١ رک ایستاده

در شکل ٤-٢٥، یک رک ایستاده را مشاهده می‌کنید که ارتفاع ٤٧ یونیت و با عمق ١٠٠ سانتی‌متر است که مخصوص اتاق سرورهای معمولی است و وزنی حدود ٢٥٠ 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

www.takbook.com

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.



شکل ۴- ۲۵ رک ایستاده

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

کاربرد رک‌های ایستاده در تحت پوشش قرار دادن سرورها، سوئیچ‌ها، فایروال‌ها و... است که در بازار، در ابعاد مختلف ۱۷، ۲۲، ۲۷، ۳۲ ، ۳۷، ۴۲ و ... 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.

۲-۷-٤ 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 ٤-۲٦، مشاهده می‌کنید.

www.takbook.com



شکل ۴- ۲۶ رک دیواری

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.

۳-۷-٤ نحوه‌ی قرار دادن دستگاه‌های شبکه بر روی رک

در این قسمت می‌خواهیم بررسی کنیم که چطوری یک سرور، سوئیچ، روتر و.... بر روی یک رک در اتاق سرور قرار می‌گیرند.

قبل از هر چیز باید بگوییم که استانداردهای رک و دستگاهایی که به آن متصل می‌شود دقیق مشخص است و شرکت‌های تولید کننده‌ی آن این استاندارد را رعایت می‌کنند.

۱-۳-۷-٤ تعداد دستگاه‌های شبکه

اولین قدیم این است که باید ببینیم چه تعداد دستگاه شبکه مانند سرور یا سوئیچ داریم و اندازه‌ی آنها را بررسی کنیم تا یک رک مناسب برای آنها انتخاب کنیم.

سرورهای HP که در قسمت‌های قبلی بررسی کردیم در اندازه‌های 1,2,3,4 وجود دارند، مثلاً اگر تعداد ۱۰ تا سرور 3Unit داشته باشید پس نیاز به حداقل 30UNIT رک دارید که البته فضاهایی 1UNIT هم باید بین آنها در نظر بگیرید، که جمعاً 10UNIT دیگر هم به آن نیاز دارید و می‌شود یک رک 40Unit که باید تهیه شود.

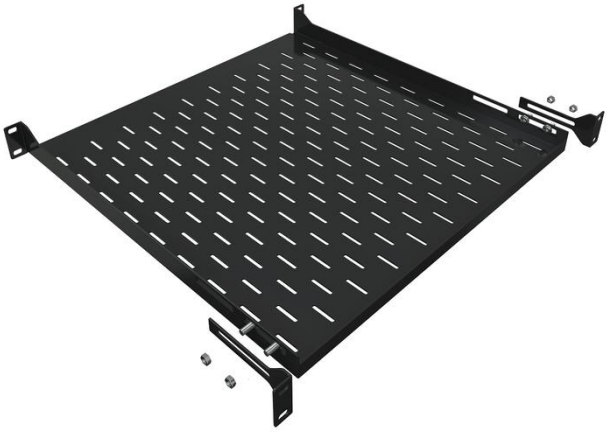
در شکل ٤-۲۷ یک سرور HPE ProLiant DL580 G10 Rack Server را مشاهده می‌کنید که یک سرور با اندازه 4UNIT است که باید بر روی رک سوار شود، همان‌طور که بیان کردیم باید وزن هر سرور را مشخص کنیم و ببینیم رکی که تهیه می‌کنیم این وزن را تحمل می‌کند یا نه.

www.takbook.com



شکل ۴- ۲۷ سرور HPE ProLiant DL580 G10 Rack Server

برای قرار دادن سرور بر روی رک، اول باید سینی‌های مخصوص به این کار را بر روی رک ببندیم، در شکل ٤-۲۸، این سینی را مشاهده می‌کنید که در کناره‌های آن پیچ و مهره برای بستن بر روی رک مشخص شده است.



شکل ۴- ۲۸سینی رک

در شکل ٤-۲۹، سینی مورد نظر به رک بسته شده است.



شکل ۴- ۲۹سینی در داخل رک

www.takbook.com

برای بستن سینی یا تجهیزاتی مانند سوئیچ و فایروال باید از پیچ و مهره مخصوص به رک شبکه استفاده کنید، در شکل ٤-۳۰ این پیچ و مهره را مشاهده می‌کنید.



شکل ۴- ۳۰ پیچ و مهره رک

نکته مهم این است که برای نصب سرور بر روی رک حتماً باید از سینی یا ریل مخصوص به سرور استفاده کنید، تا تحمل وزن آن را داشته باشد، ریل مخصوص سرور به صورت شکل ٤-۳۱، است که بر روی رک سوار می‌شود و سرور را نگه می‌دارد، البته این نوع ریل مخصوص شرکت HP است و نگه دارنده سرورهای این شرکت است.



شکل ۴- ۳۱ ریل مخصوص به سرور

یکی از ویژگی‌های مهم این ریل‌ها این است که وقتی سرور بر روی آن قرار می‌گیرد دیگر نیازی نیست برای تعمیر یا بررسی سرور کلاً سرور را از رک خارج کنیم بلکه به راحتی می‌توان سرور را از رک بیرون بیاورید و تغییرات مورد نظر را بر روی آن اعمال کنید، در شکل ٤-۳۲ مشاهده می‌کنید که سرور مورد نظر از رک بیرون آماده و درپوش آن باز شده تا تغییرات سخت‌افزاری مانند اضافه کردن رم انجام شود.

www.takbook.com



شکل ۴- ۳۲ ریل سرور

برای قرار دادن سوئیچ شبکه یا روتر شبکه که وزن بالایی ندارند می‌توانید فقط از پیچ و مهره به مانند شکل ٤-۳۳ استفاده کنید.



شکل ۴- ۳۳ نصب دستگاه‌های شبکه بر روی رک

۲-۳-۷-٤ کابل و منظم کردن آن در رک

بعد از اینکه سرورها و دستگاه‌های مربوط به شبکه را بر روی رک با استفاده از سینی و ریل نصب کردید، باید کابل‌های پشت آنها را متصل و منظم کنید، چند نوع کابل می‌توانیم در پشت رک مشاهده کنیم، یکی مربوط به کابل‌های شبکه است که هم به صورت عمومی آن یعنی مسی و هم به صورت فیبر نوری است، دیگری کابل برق است و در آخر کابل مربوط به KVM سوئیچ.

قبل از هر کاری باید به این نکته اشاره کنم که مسیر کابلهای برق و کابل دیتا باید از هم جدا باشد تا نویزی ایجاد نشود و شبکه با اختلال روبرو نشود.

برای اینکه کابل‌ها را در پشت رک مرتب کنیم باید از داکت‌های شیاردار استفاده کنیم که شکل ٤-۳٤ را مشاهده می‌کنید.

www.takbook.com



شکل ۴- ۳۴ داکت‌های شبکه

این داکت‌ها به صورت افقی پشت رک متصل می‌شوند و کابل‌ها از سرور به داخل شیارهای داکت وارد می‌شوند و از زیر یا بلای رک خارج می‌شوند.

در جلوی سرور هم وقتی کابل‌های یک اتاق را به سوئیچ متصل می‌کنیم باید از سیم جمع‌کن استفاده کنیم که شکل ٤-٣٥، را مشاهده می‌کنید، این قطعه جلوی رک متصل می‌شود و سیسم‌هایی که در جلوی رک به سوئیچ متصل می‌شوند را در خود نگه می‌دارد و بعد درب آن بسته می‌شود تا نمای خوبی داشته باشد.



شکل ۴- ۳۵ سیم جمع کن

در شکل ٤-٣٦، مدیریت کابل در جلوی رک را مشاهده می‌کنید که به صورت منظم چیده شده‌اند.

www.takbook.com



شکل ۴- ۳۶ سیم جمع کن

اگر به شکل ٤-٣٦، توجه کنید ارتباط بین سوئیچ و دیگر دستگاه‌های شبکه از طریق قطعه‌ی به نام پچ پنل انجام شده است.

پچ پنل یک رابط بین سیستم‌ها و دستگاه‌ها در اتاق سرو و در یک طبقه با سوئیچ است که ارتباط بین این دو را برقرار می‌کند، یعنی تمام کابل‌هایی که در یک طبقه وارد اتاق سرور می‌شوند به این قطعه متصل می‌شوند، شکل ٤-٣٧، نشان دهنده‌ی پچ پنل است.



شکل ۴- ۳۷ پچ پنل

در داخل پچ پنل قطعه‌ای با نام کیستون وجود دارد که کابل‌ها به آن متصل می‌شوند و یک خروجی مادگی RJ45 به ما می‌دهد که می‌توانیم کابل مورد نظر خود را به آن متصل و ارتباط سیستم مورد نظر با سوئیچ را برقرار کنیم.

www.takbook.com

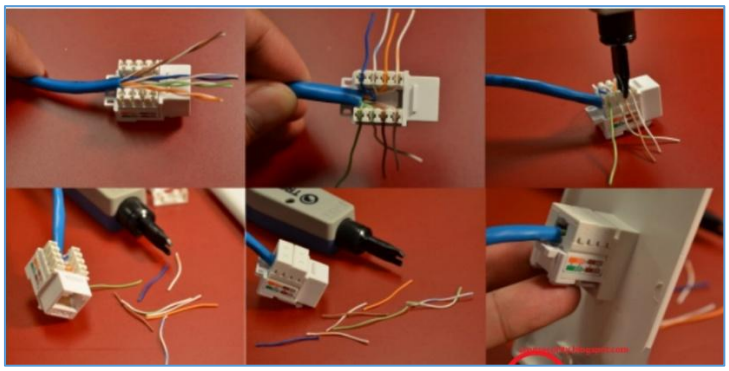
۳-۳-۷-٤ کیستون

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 پچ‌پنل است که کابل‌ها، به مانند شکل٤-۳۸ و بر اساس رنگ‌بندی روی آن قرار می‌گیرند.



شکل ۴- ۳۸ کیستون

در شکل ٤-۳۹، نحوه‌ی قرار دادن کابل به صورت مشخّص نشان داده است که این کار از طریق آچار مختص به آن انجام می‌گیرد.



شکل ۴- ۳۹ نحوه‌ی آماده کردن کیستون

آچاری که برای قرار دادن کابل در کیستون مورد استفاده قرار می‌گیرد، مانند شکل ٤-٤۰ است.

www.takbook.com



شکل ۴- ۴۰ آچار کیستون

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.

توجه داشته باشید وقتی یک رک را با دستگاه‌های مختلف و پچ پنل و کابل جمع کن آماده می‌کنید فضاهای خالی در رک به وجود می‌آید که باعث می‌شود هم شکل زیبایی نداشته باشند و هم اینکه سرما در رک به خوبی جریان نداشته باشد و به سرورها نرسد، برای اینکه این فضاهای خالی را پر کنیم، باید از بلنک پنل که شکل ٤-٤١ نشان دهنده‌ی آن است، استفاده کنیم.



شکل ۴- ۴۱ بلنک پنل

شکل نهایی آن بر روی رک به صورت شکل ٤-٤٢ خواهد بود که یک نمای زیباتری به رک می‌دهد.



شکل ۴- ۴۲ بلنک پنل

www.takbook.com

٤-٧-٤ پسیو کاری ساختمان

بعد از اینکه یک اتاق سرور را راه‌اندازی کردیم و در مورد رک هم صحبت کردیم، باید نقشه شبکه را ساختمان خود را طراحی کرده باشیم تا بتوانیم پسیو کاری آن را انجام دهیم، منظور از Passive همان کارهای فیزیکی است که انجام می‌شود مانند ترانکینگ، داکت‌کشی، کابل‌کشی و ...

کسی که می‌خواهد کار پسیوکاری ساختمان را انجام دهد باید موارد زیر را در نظر بگیرد.

۱- برآورد هزینه و تجهیزات

برای اینکه شبکه یک سازمان را را راه‌اندازی کنیم اول باید ببینیم که این سازمان دارای چند سیستم است که می‌خواهند به شبکه متصل شوند و بعد از اینکه تعداد سیستم‌ها به دست آمد طبق آن هزینه را بررسی و پسیو شبکه را راه‌اندازی می‌کنیم، در این بخش باید کل ساختمان را بازدید کنید و نقشه‌ای کامل از کابل کشی کل ساختمان را بدست بیاورید و طبق این نقشه باید تجهیزات لازم را تهیه کنید.

۲- نصب تجهیزات پسیو

بعد از اینکه نقشه‌ی ساختمان را تهیه و قطعات مربوط به پسیو را آماده کردید باید آن را بر روی ساختمان نصب کنیم.

اولین کاری که انجام می‌دهیم باید داکت‌کشی و ترانکینگ را انجام دهیم، اصولاً ترانک اصلی ساختمان به صورت شکل ٤-٤٣ می‌باشد که بر روی دیواره‌ها پیچ می‌شوند و کابل‌ها را در خود جای می‌دهند.



شکل ۴- ۴۳ ترانکینگ

در قسمت‌هایی از دیوار که قرار است درجه ترانک تغییر کنید از زاویه ترانک استفاده می‌کنند که مثل یک نبشی عمل می‌کند، که شکل ٤-٤٤ نشان دهندهی آن است.

www.takbook.com



شکل ۴- ۴۴ زاویه ترانک

توجه داشته باشید دو نوع ترانک و داکت، در کل یک کار را انجام می‌دهند، اما نوع ترانک در خود می‌تواند پریز برق، سوکت شبکه و تلفن و... را جای دهد که شکل٤-٤٤ نشان دهندهی آن است، اما داکت در انواع و اقسام مختلف وجود دارد و برای محافظت از کابل‌ها به کار برده می‌شود که یک نوع از آن را در شکل ٤-٤٥ مشاهده می‌کنید، به این نوع داکت، داکت کف خواب می‌گویند و شیارهایی که دارد از آنها کابل عبور می‌کند و آنها را نگه می‌دارد.



شکل ۴- ۴۵ داکت کف خواب

بعد ازاینکه ترانک را در تمام اتاق‌ها و تمام طبقات ساختمان نصب کردید باید رک‌های دیواری را نصب کنید، قبلاً در قسمت قبل در مورد رک‌های ایستاده و دیواری صحبت کردیم، در این رک یک پچ پنل قرار می‌گیرد و کابل‌ها به آن متصل می‌شوند.



شکل ۴- ۴۶ رک دیواری

www.takbook.com

بعد از نصب رک باید کیستون شبکه و پریز برق را در داکت یا ترانک نصب کنید، البته باید ببینید به چه تعداد نیاز دارید، در ٤-٤٧ شکل کیستون و پریز برق را مشاهده می‌کنید.

۳- کابل‌کشی ساختمان

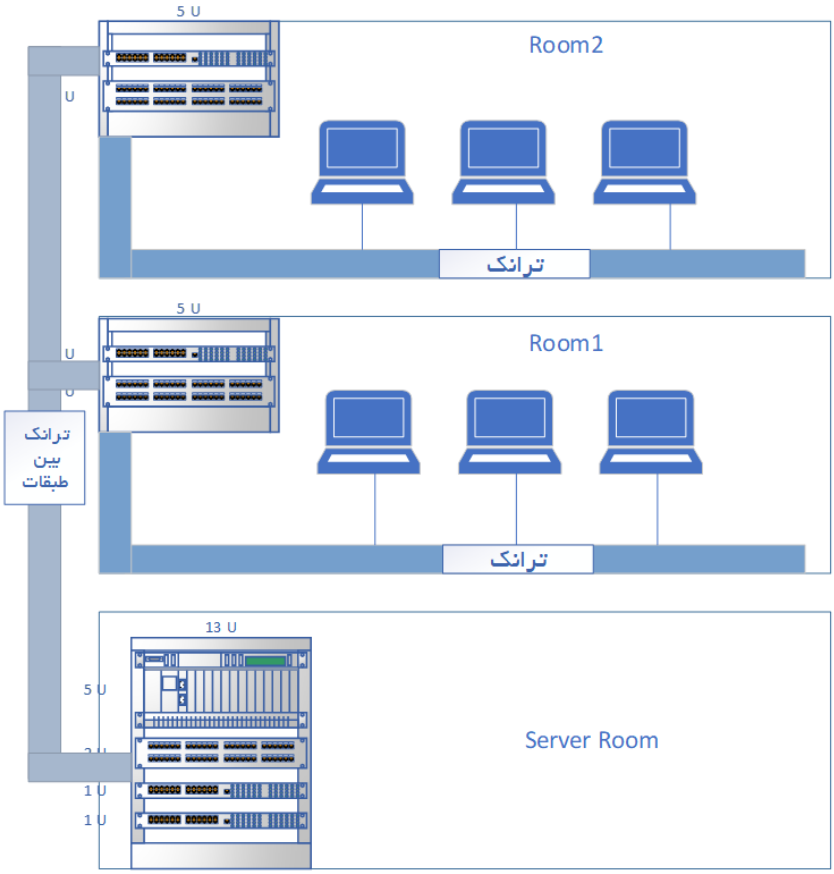
بعد از اینکه داکت و رک را نصب کردید، باید کابل‌کشی ساختمان را انجام دهید، نحوه‌ی انتخاب کابل به هزینه‌ای که می‌خواهید پرداخت کنید ربط دارد، اصولاً برای کابل‌کشی از کابل‌های SFTP استفاده می‌شود، البته هزینه‌ی بالایی دارد ولی کیفیت آن بسیار بالا خواهد بود و دچار مشکلات نویز نخواهد شد، در زیر یک ترانک را مشاهده می‌کنید که از آن کابل شبکه و کابل برق عبور کرده است.



شکل ۴- ۴۷ کابل‌کشی ساختمان

بعد از اینکه مراحل بالا را انجام دادید، یک دید کلی از پسیو شبکه بدست می‌آید که اگر بخواهیم به صورت کلی بیان کنیم، در شکل ٤-٤٨، سه طبقه از یک ساختمان را مشاهده می‌کنید که بین طبقات برای عبور کابل از ترانک استفاده شده است که البته می‌توانید از داکت هم استفاده کنید چون نیازی به متصل کردن پریز برق و سوکت نیست، در داخل طبقات هم از ترانک استفاده کردیم و سوکت‌های مشخص شده را نصب کردیم، کابل‌ها در اتاق سرور به پچ پنل متصل می‌شوند و بعد از انتقال به طبقات دیگر در رک دیواری تعبیه شده به پچ پنل داخل رک دیواری متصل می‌شوند و بعد از آن به سوئیچ متصل می‌شوند تا به کلاینت‌های داخل اتاق سرویس دهد.

www.takbook.com



شکل ۴- ۴۸ نمای کلی ساختمان

www.takbook.com

www.takbook.com

فصل پنجم

بررسی IPv4 و IPv6

بعد از اینکه در فصل‌های قبلی به طور کلی شبکه و دستگاه‌های آن را بررسی کردیم، در این فصل می‌خواهیم یاد بگیریم که آدرس‌های IP به چه صورت کار می‌کنند و از آنها چگونه باید استفاده کنیم، هر دو ورژن IPv4 و IPv6 را به طور کامل بررسی خواهیم کرد.

۵-۱ بررسی IPv4

IPV4 یا همان Internet Protocol version 4 در سال ۱۹۸۱ توسط گروه IETF؛ که به گروه ویژه مهندسی اینترنت معروف هستند ایجاد شده است و شماره‌ی جهانی آن RFC 791 است که البته قبل آن RFC 760 بوده است.

هر آدرس IPv4 شامل ۳۲ بیت است که از ٤ بخش ۸ بیتی تشکیل شده‌است. در نتیجه فضای نشانی آن ۲ به توان ۳۲ نشانی است که تعداد آن ٤,۲۹٤,۹٦۷,۲۹٦ است.

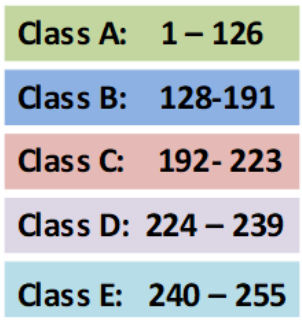
یک سری از این آدرس‌ها برای مقاصد خاصی مانند شبکه‌های خصوصی (تقریباً ۱۸ میلیون نشانی) و (چند پخشی تقریباً ۲۷۰ میلیون نشانی) رزرو شده‌است که البته به نسبت سیستم‌هایی که هم اکنون وجود دارد تعداد آن زیاد نیست و در حال حاضر هم این نوع آدرس در حال اتمام است.

همان‌طور که گفتیم، IPv4 از چهار قسمت تشکیل شده است که هر بخش، ۸ بیت است و اگر ۸ ضربدر ٤ کنیم، می‌شود 32 بیت، به آدرس زیر توجه کنید.

192.168.1.1

به هر یک از این قسمت‌ها، یک هشت‌تایی یا همان octet می‌گویند. مثلاً در IP بالا به شماره‌ی 192 یک octet می‌گویند.

IPv4 به پنج کلاس تقسیم می‌شوند که در شکل ۵-۱ آنها را مشاهده می‌کنید.



شکل ۵- ۱ کلاس IP

www.takbook.com

مثال

192.168.1.1 که عدد اول آن ۱۹۲ است، این IP در رنج کلاس c قرار دارد. به همین صورت اگر Octed اول در یکی از رنج‌های مشخص‌شده‌ی شکل قرار داشته باشد، می‌گوییم که در این کلاس قرار دارد. مثلاً، 10.10.10.1 یک IP در کلاس A است، چون 10 عدد قسمت اول آن است و بین شماره 1-126 قرار دارد.

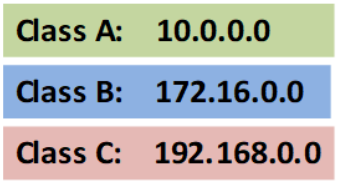
تذکر: رنج IP کلاس A از 126 - 1 است و شماره‌ی 127 برای تست کارت شبکه به کار می‌رود که همان 127.0.0.1 است و به آدرس loopback معروف است، پس برای استفاده از کلاس A می‌توان از شماره‌ی 1 – 126 استفاده کرد.

توجه داشته باشید که کلاس D برای Multicasting به کار می‌رود، این IPها روی هاست یا همان سیستم تنظیم نمی‌شوند و IPهای کلاس E برای تحقیقات به کار می‌رود و قابل‌استفاده نیست، پس فقط از IPهای کلاس‌های A,B,C برای شبکه خود استفاده می‌کنیم.

IPها به دو دسته تقسیم می‌شوند:

۲-۵ آدرس‌های خصوصی (Private IP)

این دسته از IP، فقط و فقط در شبکه‌های داخلی به کار می‌روند و در دنیای اینترنت اعتباری ندارند. این نوع از IP ها در هر کلاس وجود دارند که در شکل ۵-۲ مشخص شده‌اند.



شکل ۵- ۲ کلاس IP

IPهایی که با این اعداد شروع می‌شوند، مربوط به شبکه‌ی داخلی هستند و اعتباری در اینترنت ندارند. در جدول ۵-۱، لیستی از آدرس‌ها را مشاهده می‌کنید که برای مقاصد خاص طراحی شده‌اند.

جدول ۵- ۱ آدرس‌های IPv4

بلوک آدرس	توضیح	شماره RFC
0.0.0.0	آدرس شبکه جاری، تنها به عنوان نشانی مبدأ معتبر است.	RFC 1700
10.0.0.0	شبکه خصوصی (استفاده در شبکه‌های داخلی)	RFC 1918
127.0.0.0	آدرس بازگشت(Loopback) ، برای تست و ارتباطات داخلی سیستم استفاده می‌شود.	RFC 5735

www.takbook.com

169.254.0.0	آدرس خودکار برای کارت شبکه در صورتی که DHCP در دسترس نباشد.	RFC 3927
172.16.0.0	شبکه خصوصی (استفاده در شبکه‌های داخلی)	RFC 1918
192.0.0.0	آدرس پیکربندی خودکار برای لایه پیوند.(IANA)	RFC 5735
192.0.2.0	آدرس برای مستندسازی و نمونه کد.(TEST-NET-1)	RFC 5735
192.88.99.0	آدرس رله IPv6 به IPv4 برای ترجمه آدرس‌ها.	RFC 3068
192.168.0.0	شبکه خصوصی (استفاده در شبکه‌های داخلی).	RFC 1918
192.18.0.0	آدرس برای آزمایش‌های محک زدن شبکه.	RFC 2544
198.51.100.0	آدرس برای مستندسازی و مثال‌ها.(TEST-NET-2)	RFC 5737
203.0.113.0	آدرس برای مستندسازی و مثال‌ها.(TEST-NET-3)	RFC 5737
224.0.0.0	شبکه کلاسD ، برای آدرس‌های گروهی (Multicast) استفاده می‌شود.	RFC 3171
240.0.0.0	شبکه کلاسE ، برای کاربردهای آزمایشی و رزرو شده.	RFC 1700
255.255.255.255	آدرس پخش گسترده(Broadcast) ، برای ارسال بسته‌ها به تمامی دستگاه‌ها در شبکه.	RFC 919

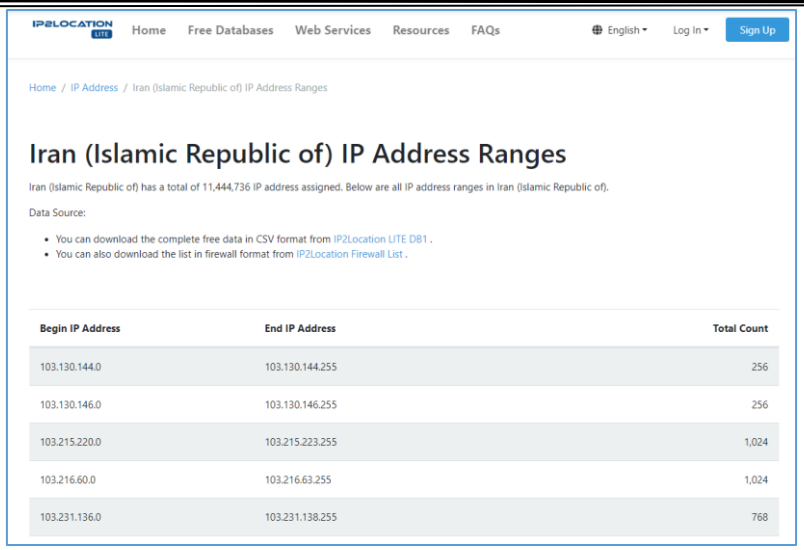
۳-۵ آدرس‌های عمومی (Public IP)

این دسته از IPها توسط سازمانی به نام IANA رجیستر می‌شوند و بعد از این کار در اینترنت قابل شناسایی هستند و دارای اعتبار. این دسته شامل تمام IPهای کلاس‌های A,B,C است، به غیر از آدرس‌های Private که در قسمت قبل باهم بررسی کردیم، به این نکته توجه کنید که هر کشور دارای آدرس‌های Public مشخص است، مثلاً وقتی وارد یک سایت مانند بانک می‌شود اگر از فیلترشکن استفاده کنید و آدرس IP شما برای یک کشور دیگر باشد به شما اجازه ورود به این سایت داده نمی‌شود چون سایت مورد نظر می‌داند که رنج IP ایران چند است و اگر آدرس شما در آن رنج نباشد سایت باز نخواهد شد. برای اینکه متوجه شوید رنج آدرس IP کشورهای مختلف به چه صورت است باید از سایت زیر استفاده کنید.

https://lite.ip2location.com/ip-address-ranges-by-country?lang=en_US

همان‌طور که در شکل ۵-۳، مشاهده می‌کنید رنج آدرس‌های کشور ایران را مشخص کرده است و شرکت‌های مختلف از این رنج یک لیست درست می‌کنند و اگر آدرس کاربر در این رنج باشد اجازه ورود به سایت را می‌دهند.

www.takbook.com



شکل ۵- ۳ رنج آدرس ایران

یک IPv4 از دو بخش اصلی تشکیل شده است

- Network address
- Host address

Network Address، به تعداد شبکه‌های موجود گفته می‌شود و Host address، به تعداد میزبان‌های موجود اشاره دارد.

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

Subnet Mask

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

جدول ۵- ۲ آدرس‌های Subnet

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

همان‌طور که در جدول ۵-۲، مشاهده می‌کنید برای هر IP در کلاس مشخص، یک Subnet Mask تعریف شده است که نشان‌دهنده‌ی تعداد شبکه و هاست است.

www.takbook.com

اگر به جدول توجه کنید در قسمت Subnet Mask اعداد ۲۵۵ مربوط به Network Address و اعداد 0 مربوط به Host address می‌باشند.

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

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

مثلاً آدرس IP زیر را با Subnet آن در نظر بگیرید، طبق جدول ۵-۳ آدرس‌هایی که به آن تعلق می‌گیرد مشخص شده است.

IP : 172.16.0.0
Subnet Mask: 255.255.0.0

جدول ۵- ۳ لیست ادرس‌های ۱۷۲.۱۶.۰.۰

Subnet	IP Address	Broadcast Address
172.16.0.0	172.16.0.1 – 172.16.0.254	172.16.0.255
172.16.1.0	172.16.1.1 – 172.16.1.254	172.16.1.255
172.16.2.0	172.16.2.1 – 172.16.2.254	172.16.2.255
172.16.3.0	172.16.3.1 – 172.16.3.254	172.16.3.255
172.16.4.0	172.16.4.1 – 172.16.4.254	172.16.4.255
تا . . .	تا . . .	تا . . .
172.16.254.0	172.16.254.1 – 172.16.254.254	172.16.254.255
172.16.255.0	172.16.255.1 – 172.16.255.254	172.16.255.255

تذکر:

همان‌طور که قبلاً گفتیم آدرس‌های Broadcast به آدرس‌هایی گفته می‌شود که برای ارسال گروهی پیام مورد استفاده قرار می‌گیرند و در این کتاب هم از آنها استفاده خواهیم کرد.

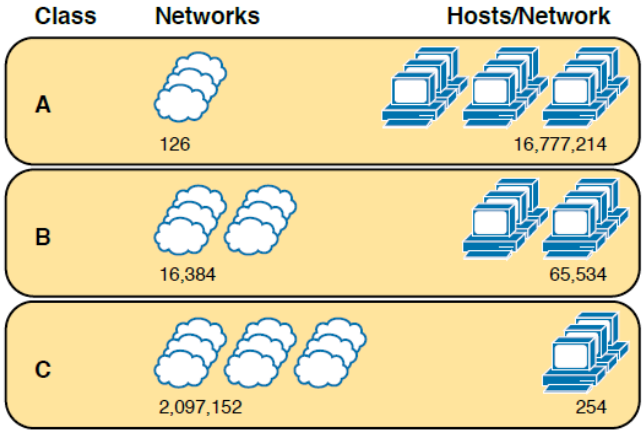
در جدول ۵-٤، اطلاعات کاملتری از سه کلاس A,B,C را مشاهده می‌کنید:

www.takbook.com

جدول ۵- ۴ کلاس A,B,C

	Class A	Class B	Class C
First octet range	1–126	128–191	192–223
Valid network numbers	1.0.0.0–126.0.0.0	128.0.0.0–191.255.0.0	192.0.0.0–223.255.255.0
Total networks	$2^7 - 2 = 126$	$2^{14} = 16,384$	$2^{21} = 2,097,152$
Hosts per network	$2^{24} - 2$	$2^{16} - 2$	$2^8 - 2$
Octets (bits) in network part	1 (8)	2 (16)	3 (24)
Octets (bits) in host part	3 (24)	2 (16)	1 (8)
Default mask	255.0.0.0	255.255.0.0	255.255.255.0

در جدول ٥–٤، می‌توانید در سطر اول رنج شبکه‌ها را مشاهده کنید، در سطر دوم رنج آدرس IP را، در سطر سوم به تعداد کل شبکه‌های موجود اشاره دارد، در سطر چهارم به تعداد کل Hostهایی که پشتیبانی می‌کند اشاره دارد که در شکل ٥–٤، دقیق مشخص شده است که مثلاً در کلاس A تعداد ١٢٦ شبکه داریم که در آن می‌تواند تا ١٦ میلیون و ٧٧٧ هزار ٢١٤ هاست را پشتیبانی کند که این عدد بسیار بزرگ است. هر چقدر تعداد شبکه بیشتر باشد از آن طرف تعداد هاست آن کمتر خواهد شد که این موضوع را در کلاس C مشاهده می‌کنید.



شکل ۵- ۴ کلاس A,B,C

برای اینکه بیشتر با Network و HOST کار کنید می‌توانید نگاهی به جدول ٥–٥، بندازید، در این جدول نام کلاس، تعداد شبکه و هاست و در آخر آدرس Network ID و Network Broadcast را مشاهده می‌کنید.

www.takbook.com

جدول ۵- ۵ جزئیات کلاس IPv4

	IP Address	Class	Network Octets	Host Octets	Network ID	Network Broadcast
1	1.1.1.1	A	1	3	1.0.0.0	1.255.255.255
2	128.1.6.5	B	2	2	128.1.0.0	128.1.255.255
3	200.1.2.3	C	3	1	200.1.2.0	200.1.2.255
4	192.192.1.1	C	3	1	192.192.1.0	192.192.1.255
5	126.5.4.3	A	1	3	126.0.0.0	126.255.255.255
6	200.1.9.8	C	3	1	200.1.9.0	200.1.9.255
7	192.0.0.1	C	3	1	192.0.0.0	192.0.0.255
8	191.255.1.47	B	2	2	191.255.0.0	191.255.255.255
9	223.223.0.1	C	3	1	223.223.0.0	223.223.0.255

همان‌طور که گفتیم الگوهایی که در بالا معرفی کردیم یک الگوی استاندارد بوده و تابع قوانین خاص خودش هست، اما الگوی غیر استاندارد هم وجود دارد که با هم آن را بررسی می‌کنیم.

٤-٥ الگوهای غیراستاندارد

همان‌طور که گفتیم، به مانند شکل ٥-٥، هر قسمت IP (octet) از هشت عدد تشکیل شده است که می‌تواند صفر یا یک باشد.

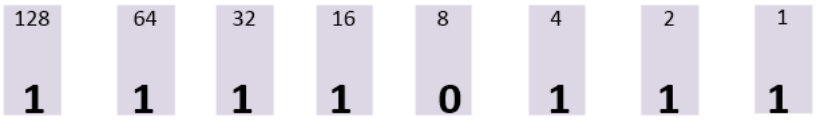


شکل ۵- ۵ Octed IP

هرکدام از این شماره‌ها در هر بخش دارای یک شماره اختصاصی هستند که به‌صورت شکل ٥-٦ است.

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

اولین قسمت از سمت چپ را در شکل ٥-٦ مشاهده می‌کنید، به نحوه‌ی قرار گرفتن اعداد توجه کنید.



شکل ۵- ۶ Octed IP

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

www.takbook.com

مثلاً اگر بخواهید شماره‌ی 192 را از بین شماره‌های 1 2 4 8 16 32 64 128 به دست بیاوریم، همیشه از سمت چپ شروع می‌کنیم، می‌گوییم ۱۲۸ از ۱۹۲ کوچک‌تر است، پس زیر ۱۲۸ را ۱ قرار می‌دهیم، در ادامه اگر ٦٤ را با ۱۲۸ که قبلاً به دست آوردیم جمع کنید می‌شود ۱۹۲ !!! چه جالب ۱۹۲ شد پس زیر ٦٤ هم ۱ قرار می‌دهیم؛ با این حساب، توانستیم شماره‌ی ۱۹۲ را پیدا کنیم، وقتی به شماره‌ی مورد نظر رسیدیم، زیر بقیه‌ی شماره‌ها صفر قرار می‌دهیم. طبق جدول ٥-٦.

جدول ٥- ٦ آدرس باینری IPV4

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

پس شماره‌ی باینری به‌دست‌آمده، 11000000 است. بقیه‌ی اعداد هم به‌صورت زیر در جدول ٥-٧ مشخص است.

جدول ٥- ٧ آدرس باینری IPV4

192	168	1	1
11000000	10101000	00000001	00000001

اگر به جدول ٥-٨، توجه کنید، دقیقاً عدد باینری به همراه عدد Decimal آن مشخص شده است که می‌تواند به شما کمک کند.

جدول ٥- ٨ آدرس باینری IPV4

Binary Mask Octet	Decimal Equivalent	Number of Binary 1s
00000000	0	0
10000000	128	1
11000000	192	2
11100000	224	3
11110000	240	4
11111000	248	5
11111100	252	6
11111110	254	7
11111111	255	8

برای اینکه با اعداد Binary و Decimal بیشتر کار کنیم، به جدول ٥-٩، توجه کنید در این جدول و در ستون Binary اعداد باینری، هر قسمت از IP را مشاهده می‌کنید، مثلاً در سطر اول اعداد 11111111 نشان دهنده‌ی عدد 255 است و عدد 11000000 برابر عدد 192 است.

www.takbook.com

جدول ۵- ۹ آدرس باینری IPV4

Binary Mask	Logic	Decimal Mask
11111111 11111111 11000000 00000000	11111111 maps to 255 11000000 maps to 192 00000000 maps to 0	255.255.192.0
11111111 11111111 11111111 11110000	11111111 maps to 255 11110000 maps to 240	255.255.255.240
11111111 11111000 00000000 00000000	11111111 maps to 255 11111000 maps to 248 00000000 maps to 0	255.248.0.0

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

IP : 192.168.1.1

Sbnet Mask :255.255.255.0

همان‌طور که آموختیم، عدد 255 به این نکته اشاره می‌کند که IP، 192.168.1 ثابت است یعنی همان Network و فقط octet آخر آن قابل تغییر از 0 تا 255 است، یعنی همان Host.

همان‌طور که می‌دانید دو IP در هر رنج مانند این IP قابل‌استفاده نیستند. به جدول ۵-۱۰، توجه کنید:

جدول ۵- ۱۰ آدرس Network در IPV4

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

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

تذکر:

www.takbook.com

نام دیگر Network address، Net ID است.

مثال: در IP زیر، Net ID و Broadcast ID را به دست آورید:

IP: 172.16.1.1

Subnetmask: 255.255.0.0

در این مثال،IP از رنج کلاس B است. همان‌طور که مشاهده می‌کنید، Subnet mask از دو تا 255 تشکیل شده است پس 2 قسمت اول IP، ثابت(172.16) و دو قسمت بعد قابل‌تغییرند، به این صورت نتیجه می‌دهد که:

Net ID: 172.16.0.0

Broadcast ID: 172.16.255.255

۱-٤-٥ اختصاص دادن رنج IP به شبکه سازمان

شما در یک شرکت کار می‌کنید که از ۳ اتاق حسابداری، فروش و طراحی تشکیل شده است؛ در این اتاق‌ها، چندین کامپیوتر به مانند شکل ۵-۷، وجود دارد.



شکل ۵- ۷ Octed IP

IP در رنج زیر می‌باشد.

192.168.1.0

255.255.255.0

سریع این IP را در ذهن خود تحلیل کنید، حداکثر IP قابل‌استفاده، ۲۵۵ عدد است. اگر متوجه شده باشید Subnet mask از سه قسمت ثابت تشکیل شده است که فقط گزینه‌ی آخر قابل‌تغییر از ۰ تا ۲۵۵ است.

www.takbook.com

برای اختصاص دادن IP به این اتاق‌ها، اول از همه، اتاقی را انتخاب می‌کنیم که بیشترین کامپیوتر را دارد که در این مثال، اتاق فروش از ٦٠ کلاینت برخوردار است.
همان‌طور که قبلاً گفتیم در هر قسمت از IP، اعدادی استاندارد و ثابتی وجود دارد.

128 64 32 16 8 4 2 1

همیشه این اعداد را در ذهن خود نگه داشته باشید، کل IP به همین اعداد خلاصه می‌شود و در ادامه، خیلی به آنها نیاز داریم.
شما اول باید ببینید عدد ٦٠ بین کدام یک از اعداد بالا قرار دارد. با کمی دقت متوجه می‌شوید که بین ٣٢ و ٦٤ قرار دارد، چون ما احتیاج به ٦٠ تا IP داریم، پس عدد ٦٤ انتخاب می‌شود.
پس رنج IP به صورت زیر می‌شود:

192.168.1.0 To 192.168.1.63

همان‌طور که گفتیم، دو آدرس از این رنج برای Net ID و Broadcast ID است، یعنی رنج زیر:

Net ID: 192.168.1.0
Broadcast ID: 192.168.1.63

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

192.168.1.1 – 192.168.1.62

رنج IP را به دست آوردیم؛ ولی Subnet mask مربوط به این IP را به دست نیاوردیم؛ برای این کار همان عدد ٦٤ را که درون شماره‌ها به دست آوردیم منهای ٢٥٦ می‌کنیم (٢٥٦ عددی است که از اعداد ٠ تا ٢٥٥ به دست می‌آید).

256 - 64 = 192

پس Subnet mask برای این IP می‌شود:

255.255.255.192

www.takbook.com

که ۱۹۲ نشان‌دهنده‌ی 64، IP برای این شبکه است.

اتاق بعدی‌ای که انتخاب می‌شود، اتاق حسابداری است که شامل ۵۰ کامپیوتر است. برای به دست آوردن رنج IP برای این اتاق، از IPهایی که استفاده نشده است، استفاده می‌کنیم.

IPهایی که در اختیارداریم به‌صورت زیر است:

192.168.1.64

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

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

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

192.168.1.64 – 192.168.1.127

255.255.255.192

که آدرس Net ID و Broadcast ID به صورت زیر خواهد بود:

Network Address: 192.168.1.64
Broadcast Address: 192.168.1.127

و رنج IP اصلی و قابل استفاده برای Host به صورت زیر است:

192.168.1.65 TO 192.168.1.126

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

192.168.1.128 To 192.168.1.143

255.255.255.240

که آدرس Net ID و Broadcast ID به صورت زیر خواهد بود:

Network Address: 192.168.1.128
Broadcast Address: 192.168.1.143

و رنج IP اصلی و قابل استفاده برای Host به صورت زیر است:

192.168.1.129 TO 192.168.1.142

باید متوجه شده باشید که ما احتیاج به 16، IP داریم، پس برای به دست آوردن Subnet mask باید ۱٦ را از ۲۵٦ کم کنیم تا عدد آخر که ۲٤۰ است به دست بیاید.

با این حساب، جدول IPها نهایی به‌صورت جدول ۵-۱۱، است:

www.takbook.com

جدول ۵- ۱۱ رنج مشخص شده برای هر اتاق

طراحی	حسابداری	فروش
192.168.1.128~143	192.168.1.64~127	192.168.1.0~63
255.255.255.240	255.255.255.192	255.255.255.192
16	64	64

در این رنج‌ها، حداقل هدر رفت IP را داشتیم.

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

نوع دیگری از IPها وجود داردند که به عنوان Class Less شناخته می‌شوند و دارای قوانین ثابتی مانند Class Full نیستند که در ادامه آن را بررسی می‌کنیم.

۲-٤-۵ بررسی CIDR

CIDR یا **Classless Inter-Domain Routing**، یک روش برای تخصیص و مدیریت آدرس‌های IP است که به‌جای استفاده از کلاس‌های سنتی آدرس‌دهی یعنی کلاسA ، B، وC از یک سیستم انعطاف‌پذیرتر استفاده می‌کند. این روش به‌ویژه در بهینه‌سازی استفاده از آدرس‌های IP و کاهش اندازه جدول‌های مسیریابی در اینترنت مؤثر است.

اصول CIDR

- **آدرس‌دهی غیرکلاسی**: CIDR به جای تقسیم‌بندی آدرس‌ها به کلاس‌های مشخص، از ماسک‌های subnet برای تعیین اندازه شبکه استفاده می‌کند.
- **علامت‌گذاری CIDR** : آدرس‌های CIDR به شکل آدرس/ ماسک نمایش داده می‌شوند. به عنوان مثال، 192.168.0.0/24 به این معنی است که ۲٤ بیت از آدرس برای شناسایی شبکه و باقی‌مانده برای شناسایی میزبان‌ها استفاده می‌شود.
- **بهینه‌سازی منابع** : با استفاده از CIDR، می‌توان آدرس‌های IP را به‌طور مؤثرتری تخصیص داد و به شبکه‌ها اجازه داد که به‌صورت جزئی‌تری تقسیم‌بندی شوند، به این معنی که می‌توان شبکه‌های کوچکتر یا بزرگتر ایجاد کرد.

www.takbook.com

- **کاهش اندازه جدول‌های مسیریابی** CIDR :اجازه می‌دهد تا چندین شبکه را در یک ورودی واحد برای مسیریابی تجمیع کرد، که این به کاهش بار بر روی روترها و افزایش کارایی شبکه کمک می‌کند.

IPهایی که به‌عنوان Class Less شناخته می‌شوند، به‌صورت زیر می‌باشند:

172.16.1.1/16

یک‌چیز جدید در این IP مشاهده می‌کنید و آن هم، یک slash به همراه یک شماره ۱٦ است که نشان‌دهنده‌ی تعداد شبکه یا همان Net ID است.

بعد از Slash، عددی بین ۱ تا ۳۲ قرار می‌گیرد. این همان عددی است که در ابتدای کار اشاره کردیم، یعنی هر IP از چهار قسمت هشت‌تایی تشکیل‌شده که می‌شود ۳۲ تا، توجه داشته باشید که حداکثر عددی که پشت slash قرار می‌گیرد ۳۰ است، چون ۲ بیت برای host Bite است.

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

192.168.1.1/24

سریع‌ترین روش برای به دست آوردن جواب به‌صورت زیر است:

هر قسمت از IP از هشت بیت تشکیل شده است که به صورت زیر است:



شکل ۵- ۸ بررسی IP و Subnet Mask

در مثالی که زدیم 24/ است که اگر به شکل ۵-۸، نگاه کنید 3 تا octet اول را باهم جمع کنیم ۲٤ می‌شود، پس می‌توان IP و Subnet mask را به این صورت نوشت:

192.168.1.0
255.255.255.0

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

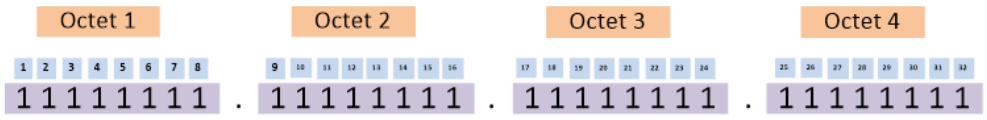
مثال دیگر :

172.16.1.1/17

اگر به مثال شکل ۵-۹ توجه کنید 16 عدد اول را داریم، پس ۲تا عدد اول IP ثابت است که در یک‌گوشه می‌نویسیم 172.16 بعد عدد 17 در octet سوم قرار دارد؛ پس، فقط با octet سوم کار می‌کنیم.

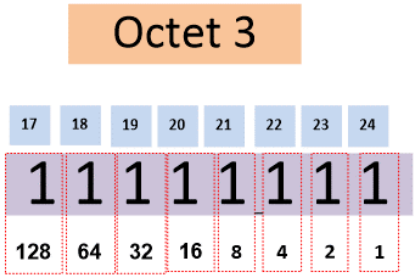
www.takbook.com

سریع اعداد ۱ ۲ ٤ ۸ ۱٦ ۳۲ ٦٤ ۱۲۸ یادداشت می‌کنیم و بعد از آن، این اعداد را بالای عدد ۱۷ تا ۲٤ از سمت چپ به راست قرار می‌دهیم تا عدد ۱۷ را پیدا کنیم. به شکل ۸-٤، توجه کنید:



شکل ۵- ۹ بررسی Octed

در شکل ۵-۱۰، به راحتی می‌توانید درک کنید که 17/ یعنی چه، ببینید سؤال از ما 17/ را می‌خواهد، پس طبق شکل ۵-۱۰، ما با octed شماره‌ی 3 کار داریم و دو octet اول را به‌صورت ثابت می‌نویسیم، چون تمام اعداد آن ۱ است، پس برای به دست آوردن عدد ۱۷، باید اعداد ۱ ۲ ٤ ۸ ۱٦ ۳۲ ٦٤ ۱۲۸ را یادداشت کرده و از سمت چپ، اعداد ۱۷ تا ۲٤ را به آن‌ها اختصاص دهیم، یعنی عدد اولی که ۱۲۸ باشد، به عنوان عدد ۱۷ است و عدد دوم که عدد ٦٤ باشد، به عنوان عدد ۱۸ است. به شکل ۵-۱۰، توجه کنید:

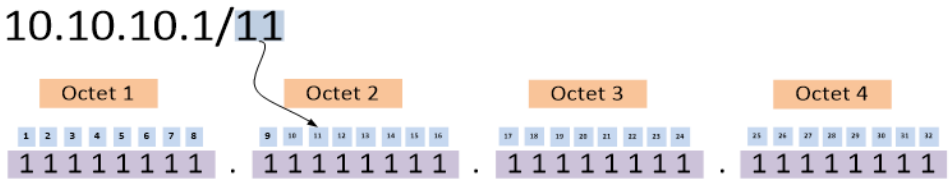


شکل ۵- ۱۰ بررسی Octed

پس ۱۷ همان عدد ۱۲۸ است. این عدد را از ۲۵٦ کم می‌کنیم و Subnet mask ما به دست می‌آید.

172.16.0~127.0
255.255.128.0

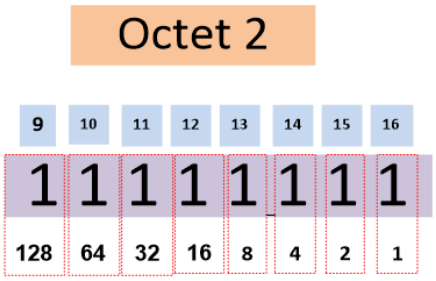
مثال آخر:



شکل ۵- ۱۱ بررسی Octed

www.takbook.com

همان‌طور که در شکل ۵-۱۱، مشاهده می‌کنید 11/ از octed اول رد شده است، پس با octed دوم کار داریم این قسمت از عدد ۹ شروع شده و به ۱۶ ختم می‌شود. عددی که در مثال گفته 11/ است، پس از ۹ و ۱۰ باید بگذریم تا به عدد ۱۱ برسیم. برای این منظور اعداد ۱ ۲ ٤ ۸ ۱٦ ۳۲ ٦٤ ۱۲۸ و از سمت چپ اعداد را با شماره ۹ و بعد ۱۰ و بعد ۱۱ شماره‌گذاری می‌کنیم، مانند شکل ۵-۱۲، عدد زیر ۱۱ که عدد ۳۲ است را از ۲۵٦ کم می‌کنیم که ۲۲٤ به دست می‌آید.

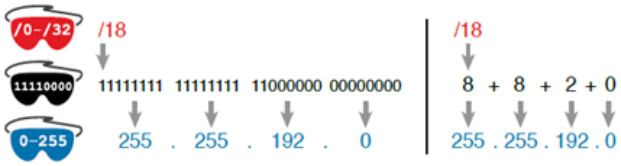


شکل ۵- ۱۲ بررسی Octed

10.0~31.0.0
255.224.0.0

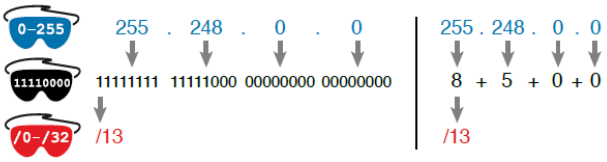
برای اینکه بیشتر با مباحث این بخش آشنا شویم روش‌های دیگری را هم با هم بررسی می‌کنیم.

در شکل ۵-۱۳، عدد 18/ را مشاهده می‌کنید که مشخص شده است این عدد از بین اعداد ۰ تا ۳۲ انتخاب شده است، یعنی اینکه دو قسمت اول Subnet Mask که ۱٦ بیت است ثابت نوشته می‌شود (255.255) و بعد از آن ۲ بیت نیاز است که می‌شود 192 .



شکل ۵- ۱۳ بررسی 18/ در IPV4

در شکل ۵-۱٤، جزئیات عدد 13/ را مشاهده می‌کنید.



شکل ۵- ۱۴ بررسی 13/ در IPV4

www.takbook.com

جدول ۵-۱۲ را برای شما به عنوان تمرین آماده کردیم که باید اطلاعات آن را تکمیل کنید، در این جدول در قسمت Prefix باید اعداد CIDR را وارد کنید، مثلاً در سطر اول عدد Prefix می‌شود 18/ و قسمت Decimal می‌شود 255.255.192.0 و به همین ترتیب به عنوان تمرین بقیه جاهای خالی را پر کنید.

جدول ۵- ۱۲ تمرین CIDR

Prefix	Binary Mask	Decimal
/18	11111111 11111111 11000000 00000000	255.255.192.0
		255.255.255.252
/25		
/16		
		255.0.0.0
	11111111 11111111 11111100 00000000	
		255.254.0.0
/27		

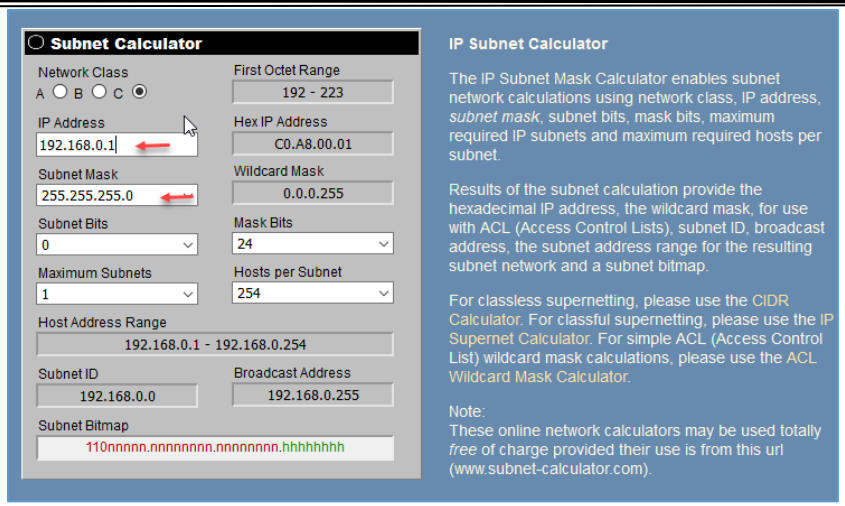
اگر جدول ۵-۱۲، را تکمیل کردید می‌توانید پاسخ آن را در جدول ۵-۱۳، مشاهده کنید:

جدول ۵- ۱۳ جواب تمرین CIDR

Prefix	Binary Mask	Decimal
/18	11111111 11111111 11000000 00000000	255.255.192.0
/30	11111111 11111111 11111111 11111100	255.255.255.252
/25	11111111 11111111 11111111 10000000	255.255.255.128
/16	11111111 11111111 00000000 00000000	255.255.0.0
/8	11111111 00000000 00000000 00000000	255.0.0.0
/22	11111111 11111111 11111100 00000000	255.255.252.0
/15	11111111 11111110 00000000 00000000	255.254.0.0
/27	11111111 11111111 11111111 11100000	255.255.255.224

برای اینکه بیشتر با بحث IP ها آشنا شوید، بهتر است سایت‌هایی که برای این منظور طراحی شده است را مشاهده کنید، سایت http://www.subnet-calculator.com یکی از سایت‌های بسیار خوب در این زمینه است که با ورود به آن با صفحه شکل ۵-۱۵ مواجه خواهید شد.

www.takbook.com



شکل ۵- ۱۵ بررسی سایت subnet-calculator

در شکل ۵-۱۵، در قسمت IP Address می‌توانید IP دلخواه خود را وارد کنید و در قسمت Subnet Mask هم باید Subnet مربوط به IP خود را انتخاب کنید، با این کار اطلاعات کاملی از رنج IP و دیگر جزئیات را دریافت خواهید کرد.

کلمه Wildcard Mask همان Subnet Mask است اما برعکس آن نوشته می‌شود مثلاً اگر Subten Mask عدد 255.255.0.0 باشد برعکس آن می‌شود 0.0.255.255 از این نوع در ادامه کار و در بحث Ruting استفاده خواهیم کرد.

۵-۵ بررسی پروتکل IPV6

شبکه‌هایی که با آن‌ها در حال حاضر کار می‌کنیم، بیشتر آن‌ها از IPv4 استفاده می‌کنند، به دلیل تولید بسیار زیاد ادوات الکترونیکی و استفاده‌ی آن‌ها از اینترنت این آدرس‌ها به اتمام رسیده، که همین امر باعث شد که محققان سازمان Internet Engineering Task Force (IETF) مدل جدید آن را با عنوان IPv6 معرفی کنند که بسیار بیشتر از IPv4 آدرس در اختیار جامعه قرار داده است، البته IPv5 هم وجود داشت که به خاطر مشکلاتی که در سر راه قرار داشت، گسترش نیافت و به فراموشی سپرده شد.

ویژگی‌های IPv6

فضای آدرس‌دهی بسیار بزرگ

همان‌طور که می‌دانید، IPv4 از ۳۲ بیت تشکیل شده است، اما IPv6 از ۱۲۸بیت تشکیل شده است که به صورت زیر بیان می‌شود:

www.takbook.com

2^128 = 340,282,366,920,938,463,374,607,431,770,000,000

این تعداد ipهایی است که این پروتکل پشتیبانی می‌کند که واقعاً زیاد است، یعنی در هر مترمربع کره‌ی زمین، چندین هزار آدرس IP اختصاص داده می‌شود.

استفاده نشدن از NAT

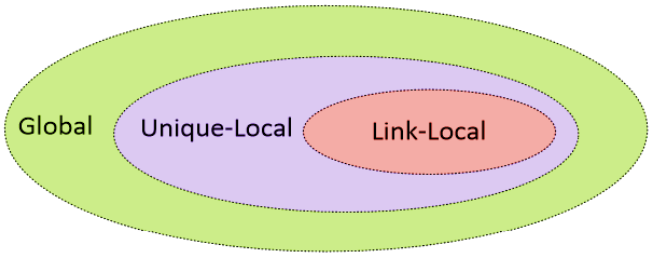
همان‌طور که می‌دانید، IPv4 برای خارج شدن از شبکه‌ی داخلی و ورود به اینترنت باید تبدیل به IPهای VALID می‌شد که این کار را با ترجمه‌ی آدرس‌های Invalid به Valid انجام می‌دادیم که به آن NAT می‌گفتند، اما در مورد IPv6 این چنین نیست و روش دیگری برای این موضوع مورد استفاده قرار می‌گیرد.

حذف شدن آدرس‌های Broadcast

در این پروتکل، به علت افزایش تعداد آدرس‌های Multicast دیگر خبری از Broadcast نیست و آدرس‌ها به صورت Unicast و Multicast و Anycast هستند.

:Unicast

به آدرس‌هایی گفته می‌شود که برای ارتباط بین یک مبدأ و مقصد استفاده می‌شوند، در شکل ۱۶-۵، ساختار آدرس‌های Unicast را مشاهده می‌کنید:



شکل ۵- ۱۶ ساختار آدرس‌های Unicast

Global unicast address

به مفهوم، آدرس‌های unicast قابل انتقال در اینترنت است (قابلیت آدرس‌دهی در اینترنت را دارد) و شبیه به نوع متناظر آن در IPv4 می‌باشد، به این نوع آدرس‌ها Aggregatable Address نیز می‌گویند، که به مانند جدول ۵-۱۴، Subnet آن از سه قسمت 3,45,16 بیت تشکیل شده است که جمعاً ۶۴ بیت و قسمت Interface آن هم از ۶۴ بیت تشکیل شده است.

جدول ۵- ۱۴ Global unicast address

3 bits	45 bits	16 bits	64 bits
001	Global Routing Prefix	Subnet ID	Interface ID

این ساختار از قسمت‌های زیر تشکیل شده است:

www.takbook.com

Unique local address

این آدرس‌ها را با نام Site-Local unicast هم می‌شناسند که قابلیت انتقال در اینترنت را نداشته و عملکرد این نوع آدرس‌ها دقیقاً شبیه به آدرس‌های local یا Private در IPv4 است. به مانند جدول ۵–۱۵، این آدرس‌ها با ۸ بیت ثابت (FD) شروع می‌شوند و به دنبال آن ٤٠ بیت صفر و سپس 16 بیت مربوط به Subnet ID است که معمولاً آن را هم صفر در نظر می‌گیرند.٦٤ بیت پایانی هم که Interface ID است که برای هر کامپیوتر منحصربه‌فرد است.

جدول ۵- ۱۵ *Unique local address*

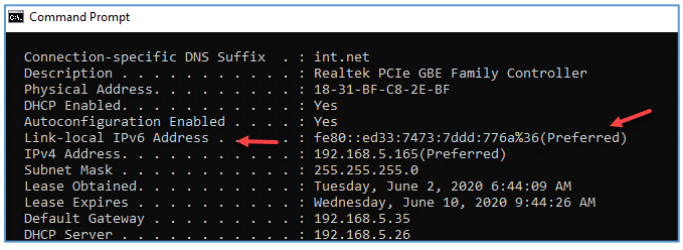
8 bits	40 bits	16 bits	64 bits
FD	Global ID	Subnet ID	Interface ID

Link local address

شبیه به آدرس‌های Private یا خصوصی در IPv4 بوده و قابل انتقال در اینترنت نیستند. این آدرس‌ها را می‌توان به اعضای یک شبکه LAN و یا چند LAN مختلف که قصد برقراری ارتباط با یکدیگر دارند، تخصیص داد.

این آدرس‌ها که در غیاب DHCP Server ایجاد می‌شوند، در IPv6 معادل Fe80::/64 هستند. به بیانی دیگر اگر در هنگام تنظیم IP آدرس، در کادر محاوره‌ای Properties کارت شبکه گزینه‌ی obtain IPv6 address automatically را انتخاب کنیم، سیستم عامل به طور خودکار بر اساس تلفیقی از MAC Address مربوط به کارت شبکه با آدرس Link-Local یک آدرس IPv6 به کارت شبکه اختصاص می‌دهد، این آدرس‌ها اصولاً برای رسیدن به گره‌های متصل شده به همان دستگاه مورد استفاده قرار می‌گیرن.

مثلاً در شکل ۵–۱۷، یک آدرس Link-Local را مشاهده می‌کنید که به یک کارت شبکه تخصیص داده شده است:



شکل ۵- ۱۷آدرس *Link Local*

یکی از نکات مهم در این نوع آدرس‌ها این است که روترها بسته‌هایی که دارای آدرس Link Local باشند به Interfaceهای دیگر انتقال نمی‌دهند، توجه داشته باشید که تمام Interfaceها دارای آدرس link-local هستند.

www.takbook.com

Multicast

برای ارتباط یک مبدأ با چند مقصد مشخص‌شده استفاده می‌شود که این مقصد در یک گروه قرار دارند؛ این آدرس جایگزین Broadcast در ipv4 شده است. در ادامه، جدول کامل این آدرس‌ها قرار گرفته شده است.

Anycast

در این آدرس‌دهی برای مثال روتر شما برای رسیدن به یک سرور چند مسیر را در پیش رو دارد، روتر مسیری را انتخاب می‌کند که کمترین Cost را داشته باشد، پس آدرس Anycast آدرسی است، برای انتخاب بهترین مسیر، تا رسیدن به یک سرور و یا انتخاب یک سرور بین چند سرور یکسان که هزینه‌ی کمتری دارد.

در جدول ٥-١٦، تفاوت اصلی بین IPV4 و IPV6 را مشاهده می‌کنید:

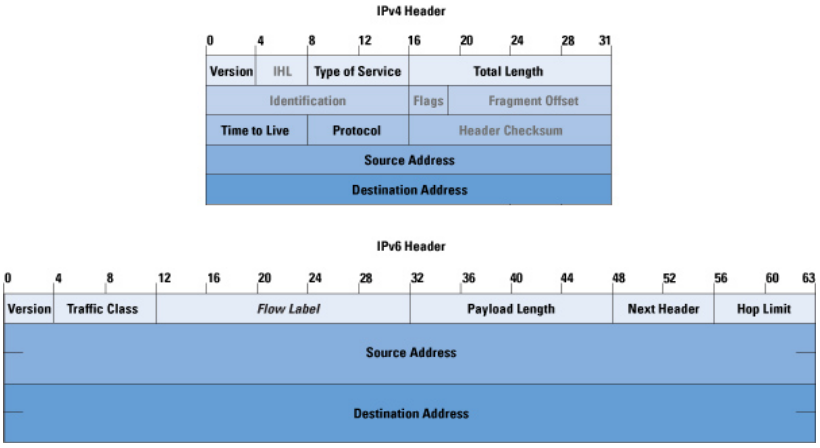
جدول ۵- ۱۶ تفاوت بین IPv4 و IPv6

IPv4	IPv6
پشتیبانی از ۲ به توان ۳۲ آدرس IP که برابر ٤,٢٩٤,٩٦٧,٢٩٦ آدرس است	پشتیبانی از ۲ به توان ۱۲۸ آدرس که بسیار بسیار زیاد است و می‌شود گفت پایانی ندارد
به خاطر محدودیت فضا باید از پروتکل NAT استفاده کرد.	به علت داشتن تعداد بالای آدرس از NAT به صورت پیش‌فرض استفاده نمی‌شود.
برای اختصاص دادن آدرس به میزبان‌ها باید از سرویس DHCP استفاده کنند و یا اینکه به صورت دستی وارد کنند.	در این ورژن میزبان‌ها دارای آدرس اختصاصی هستند که می‌توانند از آنها استفاده کنند، البته از سرویس DHCP هم می‌توانید در این پروتکل استفاده کنید.
در این پروتکل از IPSEC پشتیبانی می‌شود ولی یک گزینه‌ی اختیاری است که می‌توان از آن استفاده کرد تا محافظت از بسته‌های IP از طریق رمزگذاری، اعتبارسنجی و .. انجام شود.	در این پروتکل به صورت پیش‌فرض IPSEC پشتیبانی می‌شود و فعال است و نیازی به تنظیم آن نیست.
استفاده از broadcasts که در پروتکل ARP استفاده می‌شود.	از broadcasts و ARP به هیچ عنوان استفاده نمی‌کند ولی به جای آن از Multicast و Neighbor Discovery Protocol یا همان NDP استفاده می‌کند، ND جایگزین ARP می‌شود.
از پروتکل لایه ٤ پشتیبانی می‌کند، TCP , UDP	از پروتکل لایه ٤ پشتیبانی می‌کند، TCP , UDP
ار پروتکل‌های FTP, HTTP پشتیبانی می‌کنند.	ار پروتکل‌های FTP, HTTP پشتیبانی می‌کنند.

تفاوت Headerهای ipv4 و ipv6

www.takbook.com

با توجه به شکل ۵-۱۸، اگر به IPv4 دقیق نگاه کنید، متوجه‌ی پیچیده‌تر بودن آن نسبت به IPv6 می‌شوید، در واقع IPv6 خیلی ساده‌تر از IPv4 است.



شکل ۵- ۱۸ تفاوت Headerهای ipv4 و ipv6

هر یک از گزینه‌های موجود در این Header ها را باهم مورد بررسی قرار می‌دهیم:

Version: این فیلد ٤ بیتی بوده و نشان‌دهنده‌ی نسخه‌ی IP موجود است.

Traffic Class: برای مشخص کردن کلاس‌های مختلف و مشخص کردن اولویت پکت‌ها در IPv6 استفاده می‌شود و طول آن 8 بیت است.

Flow Label: طول این فیلد 20 بیت است. یکی از ویژگی‌های آن پشتیبانی از QOS است که یکی از ویژگی‌های جدید در IPv6 است و توانایی مسیریابی ترافیک مشخص را در شبکه می‌دهد و در این کتاب مفصل در مورد آن صحبت می‌کنیم.

Payload Length: طول این بخش 20 بیت است که شامل طول بخش بسته‌ی IPv6 است.

NextHeader: طول این فیلد 8 بیت است که نشان‌دهنده‌ی نوع Header در IPv6 است.

Hop Limit: طول این فیلد ۸ بیت است که برای مشخص کردن تعداد روترهایی است که بسته‌ی اطلاعاتی از آن رد می‌شود، یعنی زمانی‌که این بسته از یک روتر در سر راه رد می‌شود یک شماره از این زمان کم می‌شود و تا زمانی که این شماره به پایان برسد و بسته مورد نظر حذف شود.

Source Address: نشان‌دهنده‌ی آدرس مبدأ است.

Destination Address: نشان‌دهنده‌ی آدرس مقصد است.

www.takbook.com

٦-٥ روش آدرس‌دهی در IPv6

IPv6 از ۱۲۸ بیت تشکیل شده است یعنی از ۸ قسمت ۱٦ بایتی تشکیل شده است که هر قسمت آن به صورت hexadecimal است یعنی از ۰ تا F و توسط (:) هر قسمت از قسمت دیگر جدا می‌شود، در جدول ۱۷-۵، تبدیل اعداد به Hexadecimal را که مربوط به IPv6 است را مشاهده می‌کنید.

جدول ۵- ۱۷ تبدیلات اعداد

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

در زیر یک نمونه از آدرس IPv6 را مشاهده می‌کنید که دارای ۸ بخش است، البته کمی کیج کننده!

2001:0DA8:E800:0000:0260:3EFF:FE47:0001

روش‌هایی را برای کوتاه کردن آن وجود دارد که در این قسمت بررسی می‌کنیم.

روش اول – حذف صفرهای ابتدایی

در این روش هر چه صفر قبل از یک عدد وجود دارد را حذف می‌کنیم:

2001:0DA8:E800:0000:0260:3EFF:FE47
:0001
2001: DA8:E800:0: 260:3EFF:FE47: 1

روش **دوم – حذف صفرهای پشت سر هم**

www.takbook.com

در این روش اگر بین یک کلون " : " چندین صفر وجود داشت، می‌توانید صفرها را حذف کرده و فقط کلون را قرار دهیم. به روش زیر توجه کنید:

2001:0000:0000:2260:3EFF:FE47:0001

2001:: 2260:3EFF:FE47:1

همان‌طور که مشاهده می‌کنید به جای صفرهایی که در قسمت ۲ و ۳ قرار داشتند، فقط :: قرار دادیم که همین کار باعث کوتاه شدن این IP شده است.

تذکر: دو بار استفاده از کلون یا :: در یک IP امکان‌پذیر نیست و مشکل ایجاد می‌شود.

در آدرس‌دهی IPv4 اگر یادتان باشد ما از آدرس IP به همراه SubnetMask استفاده می‌کردیم که چنین موضوعی در IPv6 وجود ندارد و به جای آن از Subnet Prefix استفاده می‌کنیم.

در IPv6 چیزی به نام NETMASK وجود ندارد و جایگزین آن Prefix است، در واقع Prefix جداکننده‌ی NET ID از HOST ID است.

Net ID Host ID

2014:2015:0000:0000:BC02:0000:0001:0002/64

در مثال بالا ٦٤/ به این معناست که از سمت چپ ٦٤ بیت به جلو برویم و بعد از ٦٤ بیت قسمت HOST ID شروع می‌شود و قبل از آن مربوط به NET ID می‌شود. هر عدد در اینجا معادل ٤ بیت است.

۵-۷ انواع آدرس‌های IPv6

آدرس های Unicast به سه دسته تقسیم می‌شوند، که در زیر آنها را بررسی می‌کنیم.

فرم کلی Global Unicast

به آدرس‌های Public در IPv6 گفته می‌شود که در IPv4 هم این آدرس‌ها را داشتیم و در دنیای اینترنت اعتبار داشتند، در جدول ۵-۱۸، هدر کلی این آدرس را مشاهده می‌کنید که همه‌ی گزینه‌های آن را بررسی می‌کنیم.

از چپ به راست

جدول ۵- ۱۸ Global Unicast

INTERFACEID	SLA-ID	NLA-ID	RES	TLA-ID	FP
64 بیت	16 بیت	24 بیت	8 بیت	13 بیت	3 بیت

FP (Format Prefix):

www.takbook.com

نشان‌دهنده نوع IPv6 است و Public IPv6 آدرس‌ها در حالت باینری با ۰۰۱ شروع می‌شوند.

TLA-ID (Top Level Aggregator Identifier):

این بخش از آدرس IPv6 برای دسته‌بندی IPهایی است که به مناطق بزرگ مانند قاره‌ها اختصاص داده می‌شوند.

RES (Reserved):

بخشی از آدرس که رزرو شده است و در آدرس‌دهی فعلی استفاده نمی‌شود.

NLA-ID (Next Level Aggregator Identifier):

این بخش از آدرس به مناطق بزرگ‌تر مانند کشورها اختصاص داده می‌شود.

SLA-ID (Site Level Aggregator Identifier):

این بخش برای اختصاص آدرس‌های منحصربه‌فرد به مناطقی مانند شهرها یا سازمان‌های بزرگ استفاده می‌شود.

Ipهای خاصی در IPV6 وجود دارند که به شرح زیر می‌باشند:

::/128 (Unspecified Address)

این آدرس برای مشخص کردن یک آدرس نامشخص استفاده می‌شود. معمولاً در ابتدای فرآیند تنظیمات آدرس‌دهی Link-Local کاربرد دارد.

::/0 (Default Route)

معادل با آدرس **0.0.0.0 در** IPv4 است و برای مسیریابی پیش‌فرض (Default Routing) به‌صورت دستی مورد استفاده قرار می‌گیرد.

1::/128 (Loopback Address)

معادل آدرس Loopback در (127.0.0.1) IPv4 است و برای تست کارت شبکه و پروتکل TCP/IP استفاده می‌شود.

FE80::/10 (Link-Local Unicast Address)

این آدرس برای ارتباطات محلی (Local) در یک شبکه خاص مورد استفاده قرار می‌گیرد و معادل با آدرس IPv4 169.254.x.x است.

FF00::/8 (Multicast Address)

این محدوده به آدرس‌های Multicast اختصاص دارد که برای ارسال بسته‌ها به چندین دستگاه به‌طور همزمان مورد استفاده قرار می‌گیرند.

آدرس‌های Multicast

این آدرس‌ها جایگزین Broadcast در IPv4 شده‌اند و برای کارهای زیر استفاده می‌شوند:

- برای استفاده در سرویس DHCP.
- اعلام مسیرها در روترها که قبلاً به صورت Broadcast در IPv4 آموختیم.

www.takbook.com

- برای تقاضاهای روتر.
- و...
- این آدرس‌ها از ۸ بیت پسوند Prefix استفاده می‌کنند که به صورت FF00::/8 است، Default Gateway برای کلاینت‌ها وجود ندارد.

در جدول ۵-۱۹، انواع ipهای multicast برای پروتکل‌ها و سرورها و ... را مشاهده می‌کنید:

جدول ۵- ۱۹ تبدیلات اعداد

Address	توضیحات
ff02::1	همه‌ی گره‌ها در بخش شبکه‌های محلی
ff02::2	تمام روترها در بخش شبکه‌های محلی
ff02::5	برای الگوریتم spf مربوط به OSPFV3
ff02::6	مربوط به همه‌ی روترهای DR در پروتکل OSPF
ff02::8	مربوط به پروتکل IS-IS
ff02::9	مربوط به پروتکل RIP
ff02::a	مربوط به پروتکلEIGRP
ff02::d	مربوط به روترهای Protocol Independent Multicast (PIM)
ff02::16	گزارش مربوط به MLDv2 تعریف‌شده در RFC 3810
ff02::1:2	همه‌ی سرورهای DHCP و Real Agentها در شبکه‌ی محلی
ff02::1:3	تمام میزبان‌های LLMNR (Link Local Multicast Name Resolution) در شبکه‌ی محلی
ff05::1:3	همه‌ی سرورهای DHCP در سایت شبکه‌ی محلی
ff0x::c	مربوط به Service Discovery Protocol
ff0x::fb	مربوط به(Multicast Domain Name System (DNS
ff0x::101	مربوط به Network Time Protocol

در آدرس زیر می‌توانید تمام اطلاعات مربوط به آدرس‌های Multicast را مشاهده کنید:
https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

IPv6 می‌تواند به صورت خودکار توسط روش‌های زیر تنظیم شود:

Stateful Autoconfiguration
Stateless Autoconfiguration
EUI – 64

Stateful Autoconfiguration

www.takbook.com

در این روش که سرویس DHCP از آن استفاده می‌کند یک آدرس با طول ۱۲۸ بیت به کلاینت‌ها از طریق سرور واگذار می‌شود، توجه داشته باشید آدرس‌های Stateful و Stateless مکمل همدیگر هستند، مثلاً یک کلاینت می‌تواند از آدرس Stateless استفاده کند ولی برای بدست آوردن دیگر اطلاعت شبکه نیاز به آدرس Stateful دارد.

Stateless Autoconfiguration:

در این روش یک IPv6 که ۱۲۸ بیت است را نصف می‌کند و ٦٤ بین از آن را استفاده و ٦٤ بیت دوم را بعداً استفاده می‌کند، یعنی اینکه ٦٤ بین از یک آدرس واگذار می‌شود و ٦٤ بیت در یک زمان دیگر استفاده می‌شود.

EUI – 64:

در این روش روتر برای اختصاص دادن IP به کلاینت مورد نظر از آدرس Mac کلاینت در IPv6 استفاده می‌کند، به این صورت که ٦٤ بین اول به صورت دستی وارد می‌شود و ٦٤ بیت دوم از طریق Mac address دستگاه مورد نظر استخراج می‌شود، اما آدرس Mac، ٤٨ بیتی است. برای حل این مشکل از مقدار FFFE در وسط آدرس Mac استفاده می‌کنند و به‌این‌ترتیب آدرس مورد نظر به دستگاه مورد نظر داده می‌شود.

www.takbook.com

www.takbook.com

فصل ششم

مجازی‌سازی

۶-۱ مبانی اولیه

مجازی‌سازی شبکه (Network Virtualization) فناوری‌ای است که با استفاده از نرم‌افزار، منابع فیزیکی شبکه مانند سوئیچ‌ها، روترها و فایروال‌ها را به‌صورت منطقی و جدا از سخت‌افزار مدیریت و کنترل می‌کند. این روش مشابه مجازی‌سازی سرورها است که منابع فیزیکی یک سرور را به چندین ماشین مجازی تقسیم می‌کند. مجازی‌سازی شبکه به سازمان‌ها امکان می‌دهد تا شبکه‌های خود را با انعطاف‌پذیری بیشتر و بهره‌وری بالاتر مدیریت کنند.

اهداف و مزایای مجازی‌سازی شبکه:

- افزایش انعطاف‌پذیری: با مجازی‌سازی، می‌توانید شبکه‌ها را به سرعت و بدون نیاز به تغییرات فیزیکی تنظیم کنید. این امر به ویژه در محیط‌های پویا و مراکز داده بسیار اهمیت دارد.
- کاهش هزینه‌ها: با استفاده از مجازی‌سازی، نیازی به خرید و نگهداری سخت‌افزارهای متعدد و جداگانه نیست. این امر می‌تواند هزینه‌های مربوط به سخت‌افزار و زیرساخت شبکه را به شدت کاهش دهد.
- استفاده بهینه از منابع: مجازی‌سازی امکان استفاده بهینه از منابع فیزیکی را فراهم می‌کند. می‌توانید از یک سخت‌افزار فیزیکی برای پشتیبانی از چندین شبکه مجازی استفاده کنید و از ظرفیت‌های آن به طور کامل بهره‌برداری کنید.
- افزایش سرعت در ایجاد و پیکربندی شبکه‌ها: ساخت و پیکربندی شبکه‌های جدید با استفاده از نرم‌افزارهای مجازی‌سازی بسیار سریع‌تر از شبکه‌های فیزیکی است.
- جداسازی شبکه‌ها: با مجازی‌سازی می‌توان شبکه‌های مختلف را از هم جدا کرد، بدون اینکه نیازی به استفاده از تجهیزات فیزیکی مجزا باشد. این امر می‌تواند به افزایش امنیت و مدیریت بهتر شبکه‌ها کمک کند.

اجزای اصلی مجازی‌سازی شبکه:

- شبکه‌های مجازی (Virtual Networks): با استفاده از نرم‌افزارها می‌توان چندین شبکه مجازی ایجاد کرد که به صورت منطقی از هم جدا هستند، اما ممکن است روی یک زیرساخت فیزیکی مشترک اجرا شوند.

www.takbook.com

- سوئیچ‌های مجازی (Virtual Switches): سوئیچ‌های مجازی وظیفه اتصال دستگاه‌های مجازی در یک شبکه مجازی را دارند. این سوئیچ‌ها مانند سوئیچ‌های فیزیکی عمل می‌کنند، اما به صورت نرم‌افزاری پیاده‌سازی شده‌اند.
- روترهای مجازی (Virtual Routers): مانند روترهای فیزیکی عمل می‌کنند، اما در نرم‌افزار پیاده‌سازی شده‌اند و وظیفه مسیریابی بین شبکه‌های مجازی مختلف را بر عهده دارند.
- فایروال‌های مجازی (Virtual Firewalls): این فایروال‌ها به جای اینکه به صورت سخت‌افزاری در شبکه نصب شوند، به صورت نرم‌افزاری ترافیک شبکه‌های مجازی را کنترل و نظارت می‌کنند.

تکنولوژی‌ها و پروتکل‌های مرتبط با مجازی‌سازی شبکه:

- SDN (Software-Defined Networking): SDN یکی از مهم‌ترین مفاهیم مرتبط با مجازی‌سازی شبکه است. SDN با جدا کردن کنترل شبکه از سخت‌افزار فیزیکی و متمرکز کردن مدیریت شبکه‌ها از طریق یک کنترلر مرکزی، امکان مدیریت انعطاف‌پذیر و پویای شبکه‌ها را فراهم می‌کند.
- NFV (Network Functions Virtualization): این تکنولوژی، عملکردهای شبکه‌ای مانند فایروال، مسیریابی، و کنترل دسترسی را به جای اینکه روی سخت‌افزارهای خاص پیاده‌سازی کند، به صورت نرم‌افزاری و مجازی‌سازی شده پیاده‌سازی می‌کند. NFV به شرکت‌ها اجازه می‌دهد تا عملکردهای شبکه‌ای خود را بدون نیاز به سخت‌افزارهای گران‌قیمت مدیریت کنند.
- VXLAN (Virtual Extensible LAN): پروتکلی برای ایجاد شبکه‌های مجازی بر روی زیرساخت‌های فیزیکی، که امکان ایجاد تعداد بیشتری شبکه مجازی (VLAN) را نسبت به روش‌های سنتی فراهم می‌کند.
- OpenFlow: یکی از پروتکل‌های کلیدی در SDN که به کنترلر اجازه می‌دهد به طور مستقیم جریان‌های داده‌ای روی روترها و سوئیچ‌ها را مدیریت کند.

کاربردهای مجازی‌سازی شبکه:

- مراکز داده (Data Centers): مجازی‌سازی شبکه در مراکز داده به شدت استفاده می‌شود تا منابع شبکه‌ای به طور انعطاف‌پذیری مدیریت شوند و امکان مقیاس‌پذیری و تغییرات سریع در زیرساخت‌ها فراهم شود.
- ارائه‌دهندگان خدمات ابری (Cloud Providers): شرکت‌هایی که خدمات ابری ارائه می‌دهند از مجازی‌سازی شبکه استفاده می‌کنند تا منابع خود را به طور مؤثرتری به مشتریان مختلف اختصاص دهند.

www.takbook.com

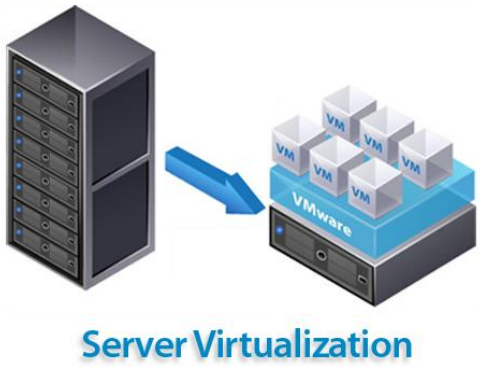
- شبکه‌های سازمانی: مجازی‌سازی شبکه در سازمان‌ها برای کاهش هزینه‌های مربوط به زیرساخت‌ها، افزایش امنیت و انعطاف‌پذیری، و مدیریت بهتر شبکه‌ها به کار می‌رود.
- ارائه‌دهندگان خدمات اینترنتی (ISPs): این شرکت‌ها با استفاده از مجازی‌سازی شبکه می‌توانند سرویس‌های متنوع و انعطاف‌پذیرتری به مشتریان خود ارائه دهند.

به طور کلی، مجازی‌سازی شبکه به سازمان‌ها کمک می‌کند تا با کاهش وابستگی به سخت‌افزار فیزیکی، به سرعت به تغییرات نیازهای شبکه پاسخ دهند و هزینه‌ها و پیچیدگی‌های مدیریتی را کاهش دهند.

۱-۱-۶ انواع مجازی‌سازی‌ها در شبکه

اگر فکر می‌کنید که مجازی‌سازی فقط و فقط برای ماشین مجازی است سخت در اشتباه هستید، بلکه در نوع‌های دیگری هم استفاده می‌شود که در زیر لیست آنها را مشاهده می کنید.

۱-۱-۱-۶ مجازی سازی سرور (Server Virtualization)

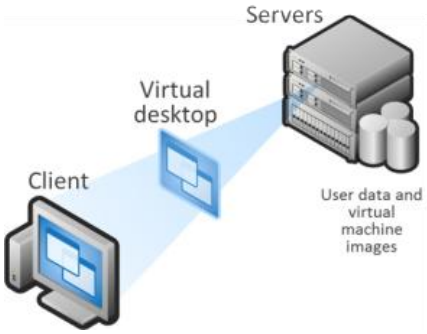


شکل ۶- ۱ Server Virtualization

به جای خرید چندین سرور فقط یک سرور قدرتمند خریداری می‌شود و سیستم‌عامل‌های مجازی‌سازی یا در اصطلاح hypervisor بر روی آنها نصب می‌شود و بسته به قدرت سخت‌افزاری سرور مورد نظر، می‌توانید چندین سرور مجازی را بر روی آن ایجاد و برای کارهای گوناگون استفاده کنید، با انجام این کار هزینه‌ها کاهش می‌یابد، امنیت اطلاعات افزایش پیدا می‌کند، هزینه‌ی پشتیبانی از سرورها کاهش پیدا می‌کند و چندین کار مهم دیگر که با مجازی‌سازی انجام می‌شود.

www.takbook.com

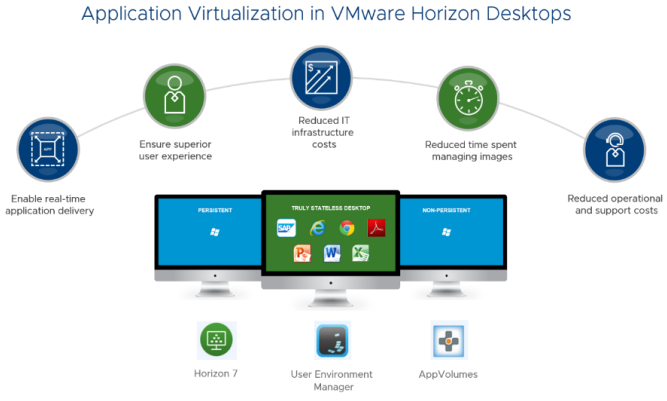
۶-۱-۱-۲ مجازی‌سازی دسکتاپ (Desktop Virtualization)



شکل ۶-۲ *Desktop Virtualization*

هر کاربر دارای یک سیستم Thin client است و این سیستم کوچک و کم هزینه از طریق کارت شبکه و آدرس IP به سرور مجازی و ماشینی که برای این کاربر ایجاد شده متصل می‌شود و به این ترتیب بدون آنکه کاربر متوجه شود وارد سیستم‌عامل خود می‌شود و با آن کار می‌کند، یک ویژگی مهم این کار این است که همه‌ی اطلاعات کاربر بر روی سرور قرار دارد و از این طریق، مدیر می‌تواند به راحتی این اطلاعات را کنترل و از آنها پشتبان تهیه کند، با انجام این روش هزینه‌های سخت‌افزاری و انسانی سازمان به شدت کاهش پیدا خواهد کرد.

۶-۱-۱-۳ مجازی‌سازی نرم‌افزار (Application Virtualization)



شکل ۶-۳ *Application Virtualization*

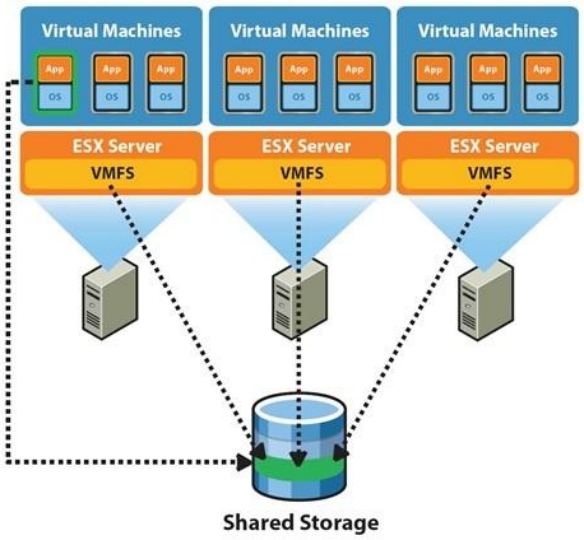
در این مدل از مجازی‌سازی‌ها، بر روی یک یا چند سرور نرم‌افزاری مورد استفاده کاربران مانند نرم‌افزارهای مالی نصب می‌شود و به صورت مجازی با کاربران به اشتراک گذاشته می‌شود، برای اجرای

www.takbook.com

این نرم‌افزارها یک نرم‌افزار Agent که مربوط به همان نرم‌افزار مجازی‌سازی است بر روی سیستم کاربر نصب می‌شود و بعد از آن کاربر با آدرس مشخص شده و از طریق وب می‌تواند به نرم‌افزارهای به اشتراک گذاشته شده دست پیدا کند، از مزایای آن می‌توان به پشتیانی دقیق از نرم‌افزار، متمرکز شدن آن، اجرای نرم‌افزار در هر سیستم با سخت‌افزار پائین و دیگر ویژگی‌هایی که انشاالله در درس‌های آینده به آن می‌رسیم.

٦-١-١-٤ مجازی‌سازی ذخیره‌سازها (Storage Virtualization)

در این قسمت می‌توانید یک هارد دیسک فیزیکی را به چندین دیسک مجازی تقسیم کنید و بر روی آن اطلاعات قرار دهید، با استفاده از این سرویس به صورت کاملاً بهبود یافته می‌توانید از اطلاعات خود استفاده کنید، پشتیبان تهیه کنید و حتی می‌توانید در SAN هم این نوع مجازی‌سازی را پیاده‌سازی کنید.



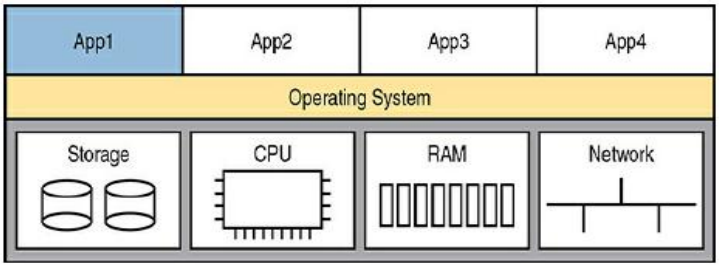
شکل ۶- ۴ Storage Virtualization

٦-١-١-٥ مجازی‌سازی شبکه (Network Virtualization)

به صورت خلاصه مجازی‌سازی شبکه را می‌توان به عنوان تکنیک‌هایی برای جداسازی منابع شبکه و محاسباتی، برای واگذاری آن‌ها به یک شبکه مجازی (منطقی)، برای همساز کردن چندین شبکه مجازی قابل برنامه‌ریزی و مستقل، دانست.

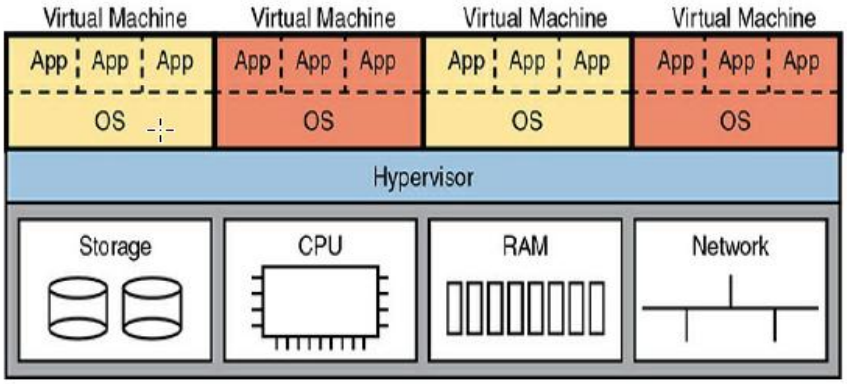
به صورت معمول فکر می‌کنید که یک سرور دارای یک سیستم‌عامل است که از کل منابع آن سرور استفاده می‌کند و بر روی آن نرم‌افزارهای مختلفی نصب شده است، که در شکل ٦-٥ این موضوع را مشاهده می‌کنید.

www.takbook.com



شکل ۶- ۵ *Virtualization*

اما در بحث مجازی‌سازی، این چنین نیست و به مانند شکل ٦-٦، یک سیستم عامل مجازی‌سازی که اصولاً به آنها Hypervisor می‌گویند بر روی سرور نصب می‌شود و بعد از آن می‌شود بر روی آن چندین ماشین مجازی با سیستم عامل‌های مختلف نصب کرد و کارهای مختلفی را بر روی آن انجام داد.



شکل ۶- ۶ *Hypervisor*

در زیر چند سیستم‌عامل مجازی‌سازی را مشاهده می‌کنید:

- VMware ESXi
- Microsoft HyperV
- Citrix XenServer
- Red Hat KVM

٦-١-١-٦ سوئیچ‌های مجازی

یک سرور را در نظر بگیرید که دارای چند پورت است که می‌تواند سیستم‌عامل مورد نظر شما را به شبکه متصل کند، اما اگر بخواهیم سیستم‌عامل مجازی بر روی سرور نصب کنید باید برای ارتباط ماشین‌های مجازی که بر روی آن نصب می‌شوند با شبکه‌ی واقعی یک سوئیچ مجازی راه‌اندازی کنیم، در این بخش

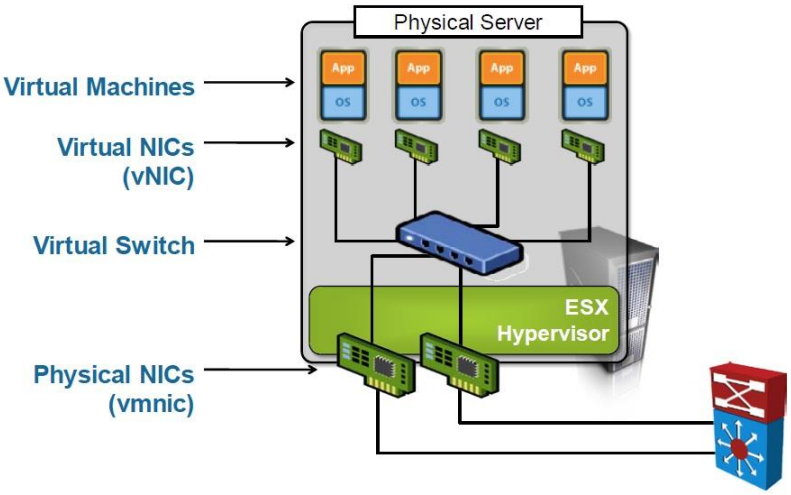
www.takbook.com

قصد نداریم که در مورد مجازی‌سازی شبکه در Hypervisior صحبت کنیم بلکه می‌خواهیم یک دید کلی از آنها بدست آوریم.

به سوئیچ‌های مجازی به اصطلاح vSwitch یا همان Virtual Switch گفته می‌شود، که به صورت نرم‌افزاری راه‌اندازی می‌شوند و می‌توانند با سوئیچ فیزیکی یا همان پورت فیزیکی سرور ارتباط برقرار کنند.

یکی از محبوب‌ترین Hyprvisior در دنیای مجازی‌سازی VMware ESXi است که در دنیای مجازی‌سازی حرف اول را می‌زند.

در شکل ٦-٧، یک Hypervisor از نوع ESXi را مشاهده می‌کنید که دارای دو کارت شبکه‌ی فیزیکی است که این دو کارت شبکه به یک سوئیچ مجازی Virtual Switch متصل شده‌اند، بعد از آن 4 تا Virtual Nics که کارت شبکه‌ی مجازی داخلی است ایجاد شده است و در آخر به ماشین‌های مجازی تخصیص داده شده است، این یک شکل کلی از سوئیچ مجازی در VMware است.



شکل ۶-۷ ESXi Hypervisor

در این فصل از کتاب به محصولات شرکت VMware پرداخته و عملکرد آنها را مورد بررسی قرار می‌دهیم، برای اینکه مطالب از ساده به سخت باشد اول از همه نرم‌افزار VMware Workstation را آموزش می‌دهیم، بعد از آن با سیستم عامل مجازی‌سازی ESXi کار می‌کنیم و در آخر با Vcenter کار خواهیم کرد، نرم‌افزارهای دیگری مانند VMware Horizon هم است که در فصلی جداگانه آموزش خواهیم داد.

٦-١-٢ بررسی نرم‌افزار VMware Workstation

نرم‌افزار مجازی‌سازی VMware Workstation را با هم بررسی کنیم تا بتوانیم بدون هزینه کردن برای سیستم‌های مختلف تمام ابزارها و سرویس‌ها را در این نرم‌افزار پیاده‌سازی کنیم.

www.takbook.com

در این فصل می‌خواهیم به صورت کامل در دسترس‌ترین نرم‌افزار مجازی‌سازی شرکت VMware را با هم بررسی کنیم، این نرم‌افزار که در سه نسخه ویندوز، لینوکس و مک موجود است، برای کاربرد شخصی ایجاد شده و بر روی سیستم‌عامل‌های مورد نظر نصب خواهد شد، با این نرم‌افزار می‌توانید ماشین‌مجازی، هارد دیسک، کارت‌شبکه و دیگر منابع سخت‌افزاری را به صورت مجازی ایجاد کنید، در این بخش این نرم‌افزار را به صورت کامل بررسی خواهیم کرد.

۱-۲-۱-٦ پردازنده

برای اینکه بتوانید این نرم‌افزار را بر روی سیستم‌عامل مورد نظر خود نصب کنید باید پردازنده آن ٦٤ بیت باشد که برند intel آن از تکنولوژی VT-x و برند AMD آن هم segment-limit support in long mode پشتیبانی کند و برای اینکه بتوانید از ویژگی مجازی‌سازی در سیستم خود استفاده کنید باید در BIOS سیستم خود تکنولوژی مجازی‌سازی که اصولاً با نام VT-x مشخص شده است را فعال کنید.

۲-۲-۱-٦ حافظه (رم)

برای اینکه یک ماشین‌مجازی را در سیستم خود راه‌اندازی کنید، باید به مقدار مورد نیاز رم برای سیستم اصلی خود در نظر بگیرید، مثلاً برای راه‌اندازی یک ماشین مجازی با ویندوز ۷ نیاز به حداقل یک گیگابایت رم دارید که به خاطر همین باید سیستم اصلی شما حداقل دو گیگابایت رم داشته باشد تا بتواند به درستی ماشین مجازی را اجرا کند، در ادامه با افزایش تعداد ماشین مجازی، نیاز به افزایش رم سیستم خود دارید.

۳-۲-۱-٦ هارد دیسک

برای نصب ماشین مجازی نیاز به هارددیسک با حجم بالا دارید، البته برای شروع کار شاید یک هارد دیسک ٥۱۲ گیگابایت برای شما کفایت کند ولی با پیشرفت کار و ایجاد ماشین‌مجازی بیشتر نیاز به فضای ذخیره‌سازی بالاتری دارید، یکی از ویژگی‌های ماشین‌مجازی این است که اگر مثلاً یک هارد دیسک ۱۰۰ گیگابایت را برای آن در نظر بگیرید در اول کار آن هارد دیسک‌مجازی پر نمی‌شود بلکه به مرور زمان و با ایجاد اطلاعت در آن، فضای آن اشغال خواهد شد.

٤-۲-۱-٦ کارت شبکه

بعد نصب VMware Workstation به صورت پیش‌فرض دو کارت شبکه Host-Only و NAT به لیست کارت شبکه‌های سیستم اصلی شما اضافه خواهد شد که در ادامه روی آنها کار خواهیم کرد، یک نوع کارت

www.takbook.com

شبکه دیگر به نام Bridged وجود دارد که به کارت شبکه فیزیکی سیستم شما متصل می‌شود و ماشین مجازی از طریق آن می‌توانند به دنیای بیرون ارتباط داشته باشند، این نوع کارت شبکه‌ها میتواند یک کارت شبکه ۱ گیگبایت باشد، البته در بعضی از سیستم‌ها بنا به نیاز ماشین‌مجازی از دو یا چند کارت شبکه فیزیکی استفاده خواهد شد.

۶-۱-۲-۵ سیستم‌عامل

شما می‌توانید نرم‌افزار VMware Workstation را بر روی سیستم‌عامل‌های لینوکس، ویندوز و مک نصب و راه‌اندازی کنید.

۶-۱-۳ نصب و راه‌اندازی نرم‌افزار VMware Workstation

برای شروع کار بهتر است نرم‌افزار VMware Workstation را بررسی کنیم، این نرم‌افزار برای ایجاد ماشین مجازی بر روی یک سیستم شخصی کاربرد دارد که برای آنهایی که می‌خواهند یک شبکه شخصی رایگان و بدون هزینه داشته باشند مناسب است.

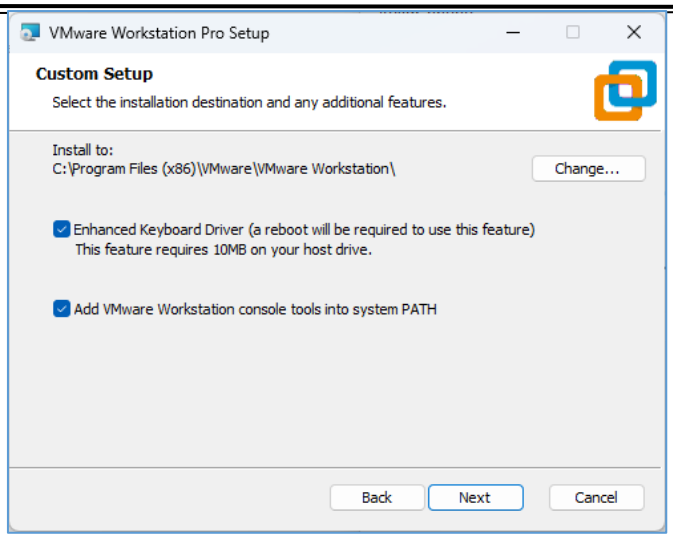
کارهایی که می‌توانید با این نرم‌افزار انجام دهید، عبارت است از:

۱. ایجاد ماشین مجازی
۲. ایجاد شبکه مجازی
۳. ایجاد هارد دیسک مجازی
۴. ایجاد امنیت بر روی ماشین‌ها
۵. ارتباط از راه دور با سرورهای VMware
۶. و...

برای نصب این نرم‌افزار بر روی ویندوز، از لینک زیر آخرین ورژن آن را از سایت اصلی دانلود کنید.
https://www.vmware.com/nordics/products/workstation-pro/workstation-pro-evaluation.html

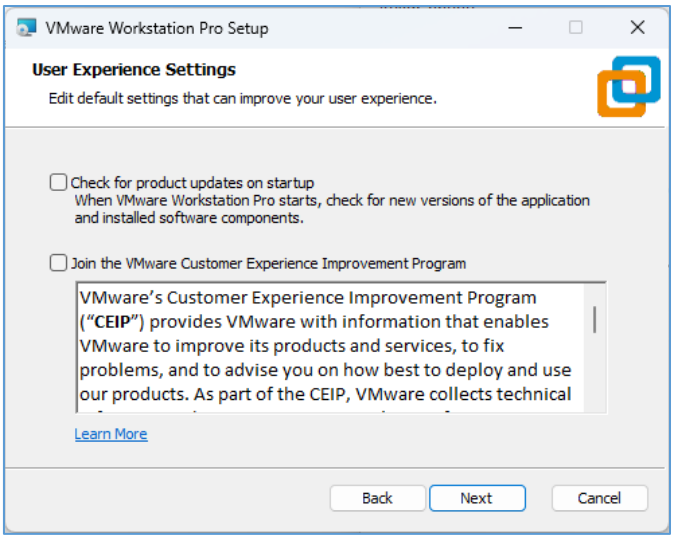
بعد از اجرا و کلیک بر روی Next به شکل ۶-۸ می‌رسید که با کلیک بر روی دکمه Change می‌توانید مسیر نصب نرم‌افزار را تغییر دهید و اگر می‌خواهید از ویژگی‌های کیبورد به صورت کامل استفاده کنید باید تیک گزینه‌ی مورد نظر را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



شکل ۶- ۸ نصب *VMware Workstation*

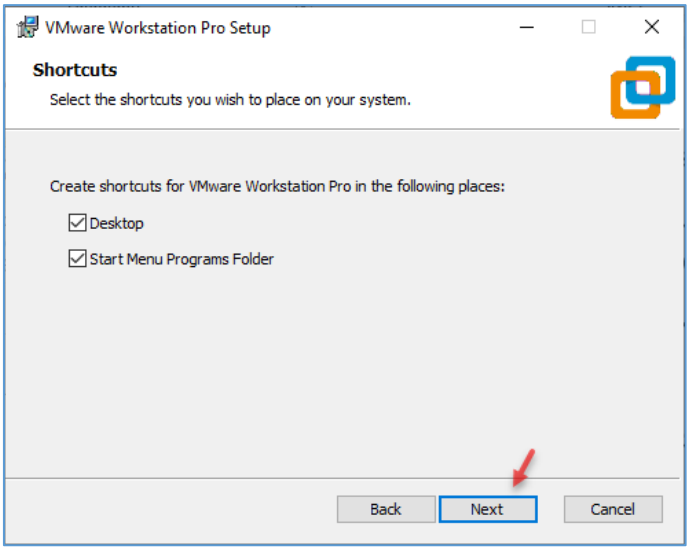
در شکل ٦-۹، اگر از ورژن اصلی و اورجینال نرم‌افزار استفاده می‌کنید بهتر است تیک‌های مورد نظر را انتخاب کنید، تیک گزینه‌ی اول برای آپدیت نرم‌افزار کاربرد دارد و تیک دوم برای متصل شدن به سیستم رفع مشکلات VMware است، ولی در صورتی که از نرم‌افزار کرک شده یا لایسنس قلابی استفاده می‌کنید تیک هر دو گزینه را بردارید.



شکل ۶- ۹ نصب *VMware Workstation*

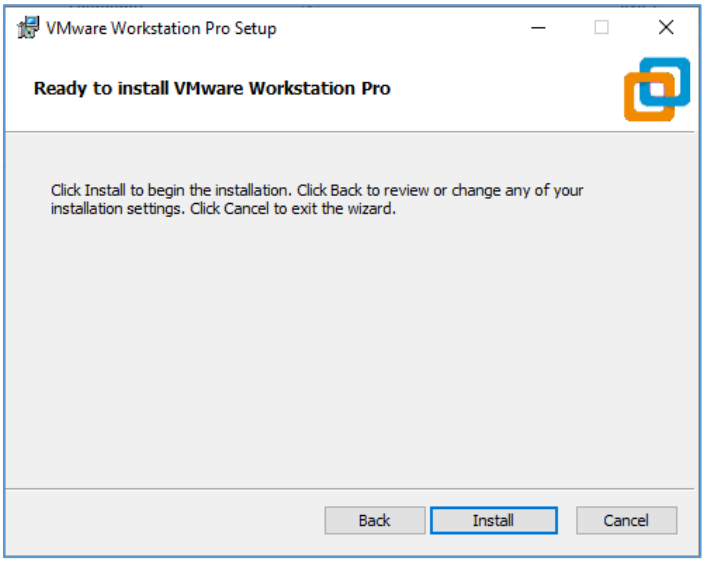
www.takbook.com

در شکل ۳-۱۰ می‌توانید برای ایجاد Shortcut بر روی Desktop و Taskbar تیک هر دو گزینه را انتخاب و بر روی Next کلیک کنید.



شکل ۶- ۱۰ نصب *VMware Workstation*

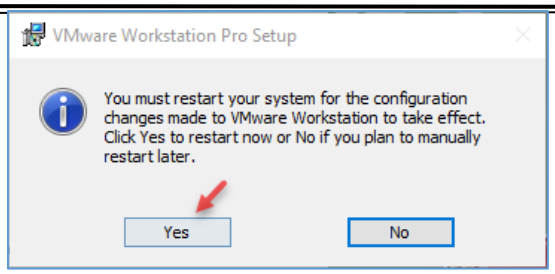
برای شروع نصب به مانند شکل ٦-۱۱ بر روی Install کلیک کنید.



شکل ۶- ۱۱ نصب *VMware Workstation*

در شکل ٦-۱۲ برای اعمال تنظیمات به صورت کامل بر روی Yes کلیک کنید تا سیستم شما Restart شود.

www.takbook.com

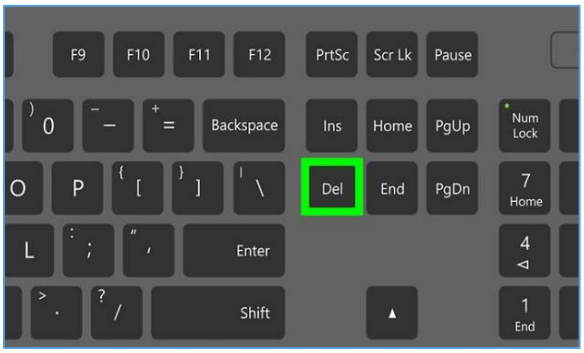


شکل ۶- ۱۲ نصب *VMware Workstation*

۱-۳-۱-۶ فعال‌سازی مجازی‌سازی در Bios

بعد از اینکه نرم‌افزار مجازی‌سازی را بر روی سیستم خود پیاده‌سازی کردید برای اینکه از قابلیت مجازی‌سازی آن استفاده کنید باید تکنولوژی مجازی‌سازی را در BIOS مادربرد سیستم خود فعال کنید. قبل از فعال‌سازی باید به این نکته اشاره کنم که در بعضی از سیستم‌ها به صورت پیش‌فرض فعال است و نیاز به انجام این مراحل نیست.

به مانند شکل ۶-۱۳ برای ورود به Bios باید از کلید Del بر روی صفحه کلید خود استفاده کنید، یعنی سیستم خود را Restart کرده و بر روی این دکمه فشار دهید تا وارد Bios شوید، البته در سیستم‌های مختلف این کلید متفاوت است و می‌تواند کلید F1, F2 یا F4 هم باشد.



شکل ۶- ۱۳ ورود به *BIOS*

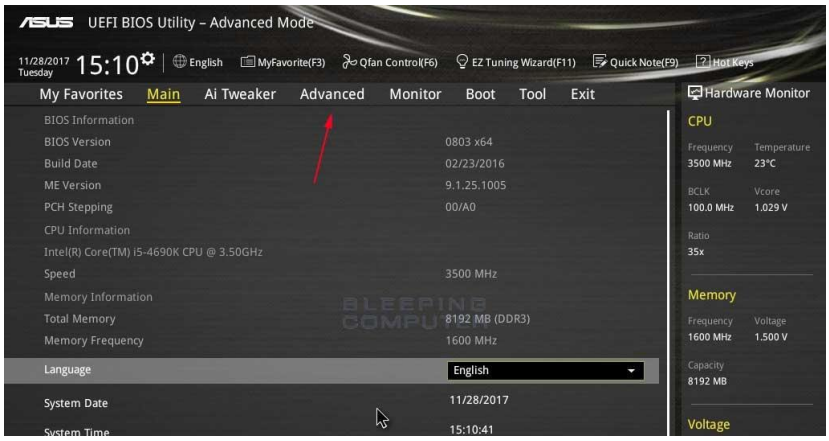
بعد از ورود به Bios به مانند شکل ۶-۱۴ اگر از مادربرد Asus استفاده می‌کنید بر روی Advanced Model یا کلید F7 فشار دهید تا وارد تنظیمات پیشرفته آن شویم، در بعضی از مادربردهای دیگر شاید به این صورت نباشد و باید وارد CPU Configuration شوید.

www.takbook.com



شکل ۶- ۱۴ تنظیمات BIOS

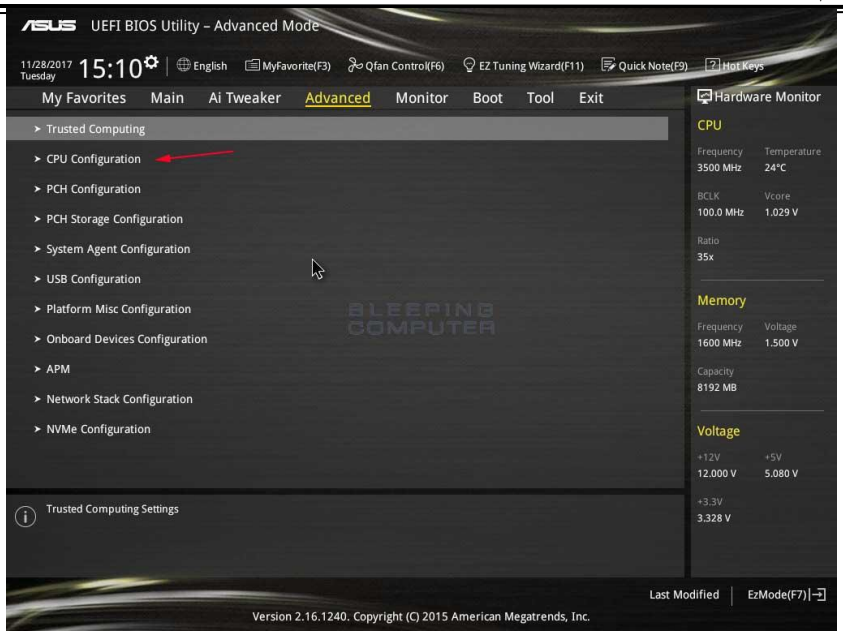
در شکل ٦-١٥ باید بر روی Advanced کلیک کنید.



شکل ۶- ۱۵ تنظیمات BIOS

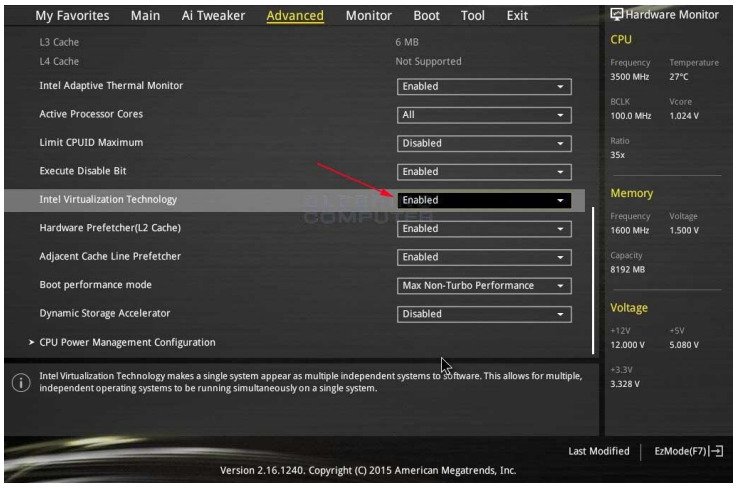
در شکل ٦-١٦ بر روی CPU Configuration کلیک کنید، توجه داشته باشید در برندهای دیگر شاید گزینه‌ی Advanced Chipset Features وجود داشته باشد که آن را باید انتخاب کنید.

www.takbook.com



شکل ۶- ۱۶ تنظیمات BIOS

در شکل ٦-۱۷ باید گزینه‌ی Intel Virtualization Technology را بر روی Enable قرار دهید.



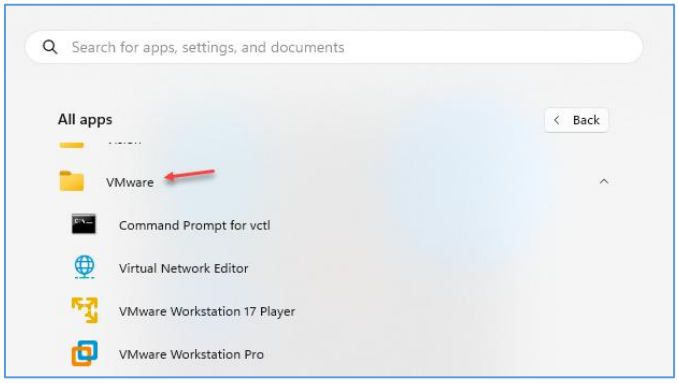
شکل ۶- ۱۷ تنظیمات BIOS

بعد از انجام این کار بر روی صفحه کلید دکمه F10 را فشار دهید و در صفحه باز شده گزینه‌ی Yes را انتخاب کنید، با این کار تنظیمات شما ذخیره و سیستم Restart خواهد شد.

بعد اجرا شدن سیستم‌عامل، به مانند شکل ٦-۱۸ اگر بر روی Start کلیک کنید، نرم‌افزار جدید برای شرکت VMware را مشاهده می‌کنید که دارای چهار گزینه است، گزینه‌ی اول Command Prompt for vctl که ابزاری

www.takbook.com

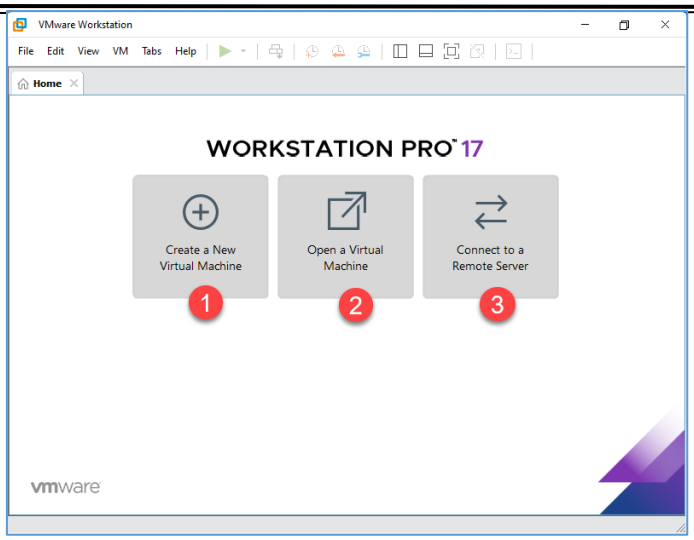
مختص شرکت VMware است و در صورت نیاز از آن استفاده خواهیم کرد، گزینه‌ی دوم Virtual Network Editor برای انجام تنظیمات بر روی کارت شبکه مجازی و فیزیکی کاربرد دارد، گزینه‌ی سوم VMware Workstation 17 Player برای ایجاد ماشین مجازی و باز کردن ماشین مجازی کاربرد دارد و یکی دیگر از کارهای جالب آن این است که از سایت https://bitnami.com می‌توانید یک سری از ماشین‌های مجازی آماده را که مربوط به نرم‌افزارهای مختلف است دانلود کنید، گزینه‌ی چهارم VMware wokstation Pro نرم‌افزار اصلی است که با این نرم‌افزار به طور کامل کار خواهیم کرد.



شکل ۶- ۱۸ *VMware Workstation*

برای شروع کار بر روی نرم‌افزار VMware Workstation Pro کلیک کنید تا شکل ٦-١٩ نمایش داده شود. در صفحه اول سه آیکون مشخص شده را مشاهده می‌کنید که گزینه‌ی اول برای ایجاد ماشین مجازی کاربرد دارد، گزینه‌ی دوم برای اجرا کردن ماشین و گزینه‌ی سوم برای متصل شدن به سرورهای دیگر مانند ESXi و... است.

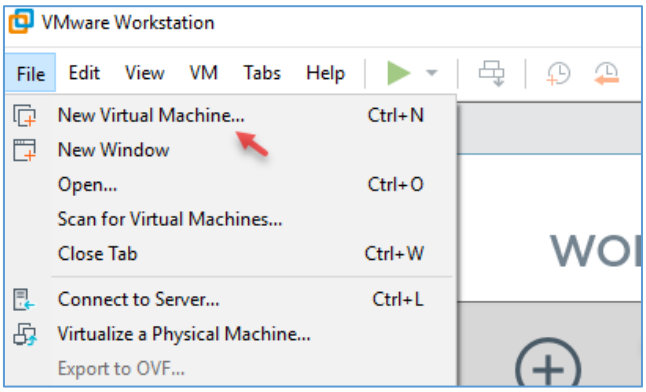
www.takbook.com



شکل ۶- ۱۹ *VMware Workstation*

۲-۳-۱-۶ ایجاد ماشین مجازی در VMware Workstation

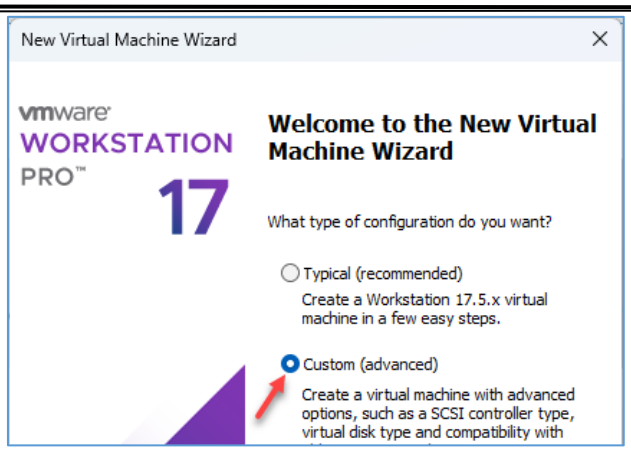
در شکل ۶-۲۰ می‌خواهیم یک ماشین مجازی بر روی این نرم‌افزار ایجاد کنیم برای این کار باید بر روی Create a New Virtual Machine که در قسمت قبل مشخص کردیم کلیک کنید و یا از منوی File بر روی New Virtual Machine کلیک کنید.



شکل ۶- ۲۰ *VMware Workstation*

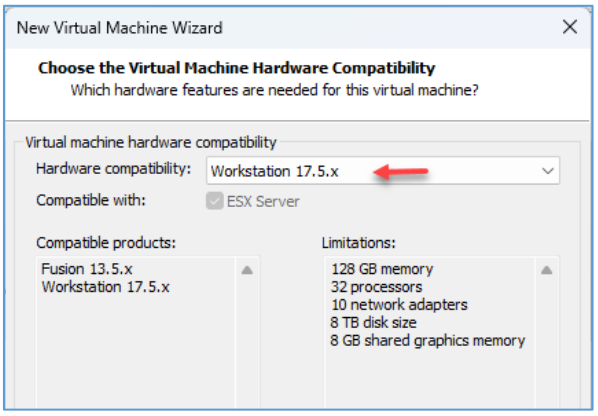
در شکل ۶-۲۱ دو گزینه را مشاهده می‌کنید، اگر گزینه‌ی Typical را انتخاب کنید یک سری از تنظیمات به صورت پیش‌فرض انجام شده و از کاربر سوال نمی‌شود ولی برای اینکه همه گزینه‌ها را بررسی کنیم گزینه‌ی Custom را انتخاب کنید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۶- ۲۱ ایجاد ماشین مجازی

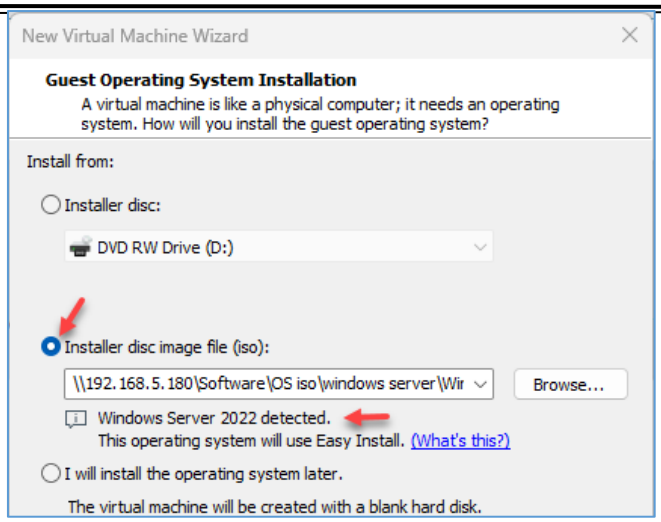
در شکل ٦-۲۲، نسخه‌های مختلف از سخت‌افزارها وجود دارد و حداکثر ظرفیت سخت‌افزاری مشخص شده که این موضوع را می‌توانید در قسمت Limitation مشاهده کنید، در قسمت Compatible products مشخص شده است که ماشین مجازی که در حال ایجاد آن هستید فقط با این نسخه‌ها به خوبی اجرا خواهد شد، در لیست گزینه‌ی Fusion هم وجود دارد که مربوط به سیستم‌عامل مک است.



شکل ۶- ۲۲ ایجاد ماشین مجازی

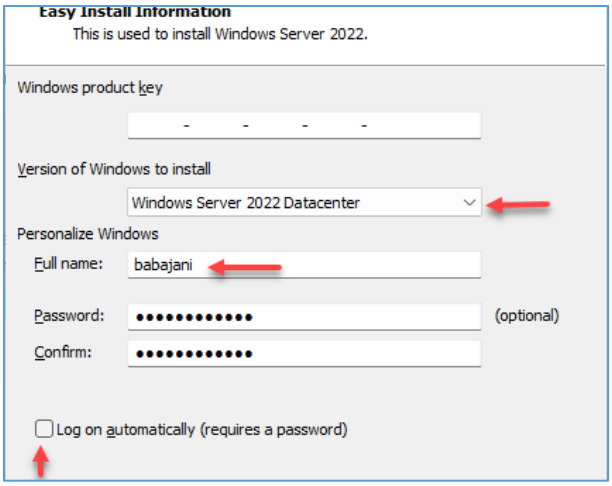
در شکل ٦-۲۳، باید یکی از دو مورد اول را برای مشخص کردن نوع ورودی فایل سیستم‌عامل انتخاب کنید که در این قسمت گزینه‌ی دوم را انتخاب می‌کنیم و فایل ویندوز سرور ۲۰۲۲ را از طریق کلیک بر روی Browse معرفی می‌کنیم. اگر در این قسمت تمایل ندارید سیستم‌عامل خود را معرفی کنید باید گزینه‌ی سوم را انتخاب کنید.

www.takbook.com



شکل ۶- ۲۳ ایجاد ماشین مجازی

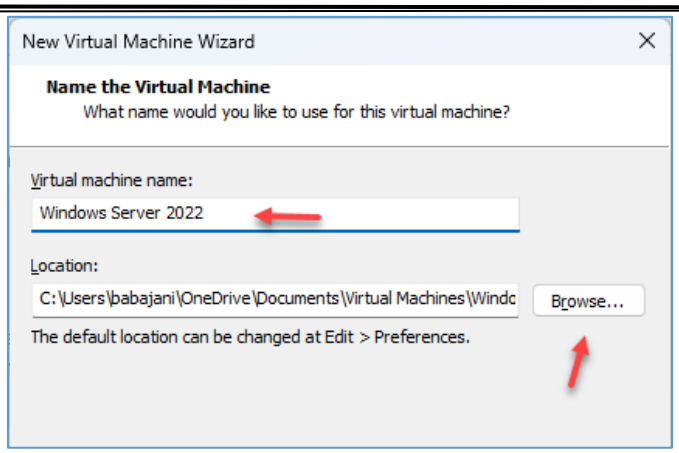
در شکل ٦-٢٤ برای اینکه نصب ویندوز به صورت اتوماتیک و سریع انجام شود، می‌توانید سریال استفاده از این محصول را وارد کنید و در قسمت Version باید ورژن ویندوز و در قسمت Full Name یک نام کاربری به همراه رمز عبور وارد کنید، توجه داشته باشید اگر تیک گزینه‌ی Log on automatically را وارد کنید بعد از نصب ویندوز بدون وارد کردن رمز عبور وارد صفحه Desktop خواهید شد.



شکل ۶- ۲۴ ایجاد ماشین مجازی

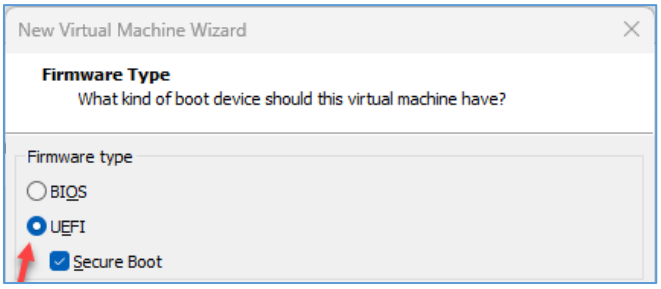
به مانند شکل ٦-٢٥، در قسمت Virtual machine name نام ماشین مجازی خود را وارد کنید و از قسمت Location باید مسیر ذخیره شدن اطلاعات ماشین مجازی را مشخص کنید، به صورت پیش‌فرض در درایوی که سیستم عامل نصب است اطلاعات ذخیره می‌شود.

www.takbook.com



شکل ۶- ۲۵ ایجاد ماشین مجازی

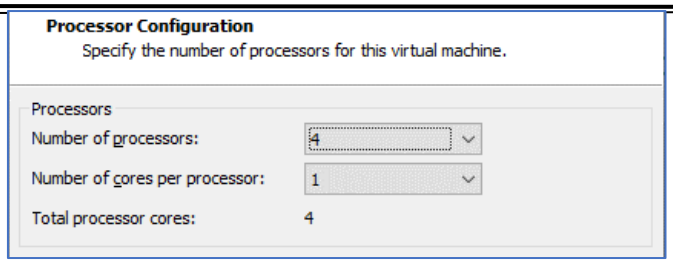
در شکل ٦-٢٦ باید نوع Firmware Type را برای این ماشین مجازی انتخاب کنید، اگر گزینه‌ی Bios را انتخاب کنید ماشین مجازی از BIOS سیستم اصلی‌تان استفاده خواهد کرد و اگر هم گزینه‌ی UEFI را انتخاب کنید، گزینه‌های پیشرفته‌تری مانند Secure Boot فعال خواهد شد که این نوع Boot به Secure Boot معروف است و هر کسی نمی‌تواند بر روی کامپیوتر شما سیستم‌عاملی به غیر از سیستم‌عامل اصلی نصب شده، نصب کند، گزینه‌ی UEFI و تیک گزینه‌ی Secure Boot را انتخاب کنید.



شکل ۶- ۲۶ ایجاد ماشین مجازی

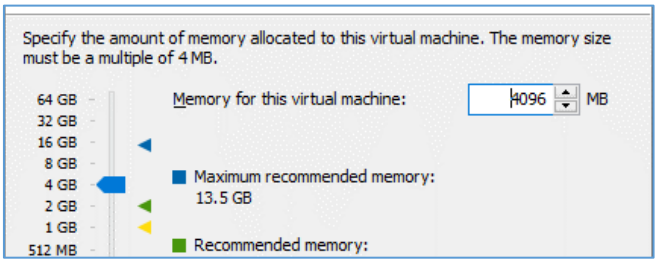
در شکل ٦-٢٧، باید تعداد هسته‌های CPU سیستم را برای این ماشین مجازی مشخص کنید، اگر چنانچه ماشین مجازی نیاز به پردازش بالا دارد، بهتر است که تعداد هسته CPU را بالا در نظر بگیرید.

www.takbook.com



شکل ۶- ۲۷ ایجاد ماشین مجازی

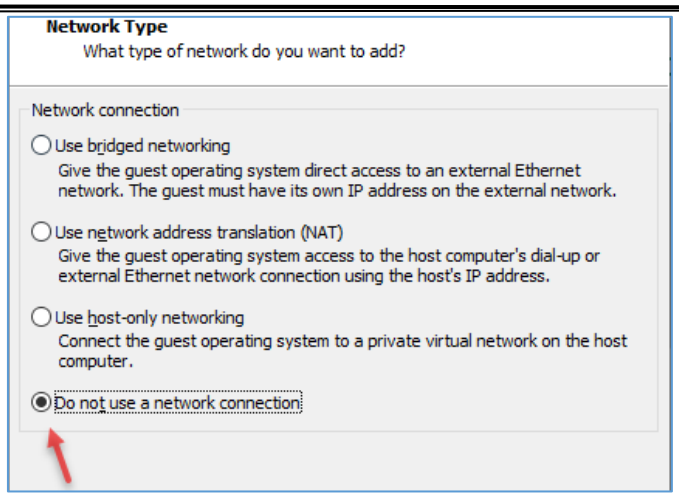
به مانند شکل ٦-۲۸ مقدار رم مورد نیاز ماشین مجازی خود را انتخاب کنید، البته در شکل، مقدار مناسب را با رنگ سبز مشخص کرده است که این مقدار فشار زیادی به سیستم اصلی شما نمی‌آورد، این سیستمی که بر روی آن ماشین مجازی در حال اجرا است 32 گیگابایت رم دارد که حداکثر می‌توانید 28 گیگابایت برای آن حافظه در نظر بگیرید که این موضوع را می‌توانید با کلیک بر روی فلش آبی مشخص کنید، برای اینکه از ویندوز سرور استفاده می‌کنیم بهتر است، برای آن ٤ گیگابایت رم در نظر بگیرید.



شکل ۶- ۲۸ ایجاد ماشین مجازی

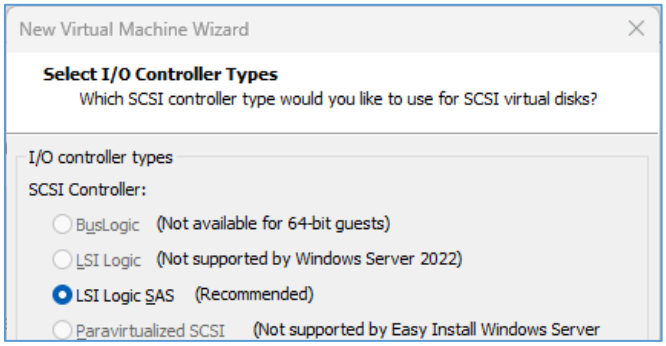
در شکل ٦-۲۹، باید نوع کارت شبکه‌ی خود را مشخص کنید، اگر گزینه‌ی اول یعنی Bridged را انتخاب کنید می‌توانید با شبکه واقعی (فیزیکی) خود ارتباط داشته باشید، اگر گزینه‌ی دوم را انتخاب کنید می‌توانید از سرویس NAT برای ارتباط با دنیای اینترنت یا شبکه دیگر استفاده کنید و یا اگر می‌خواهید یک شبکه‌ی داخلی و شخصی داشته باشید گزینه‌ی سوم را انتخاب می‌کنیم، در حال حاضر گزینه‌ی چهارم را انتخاب می‌کنیم و انشاالله در ادامه کار و بعد از بررسی شبکه مجازی یکی از این سه گزینه را انتخاب خواهیم کرد.

www.takbook.com



شکل ۶- ۲۹ ایجاد ماشین مجازی

در شکل ٦-۳۰، باید نوع کنترلر خود را مشخص کنید، دو گزینه‌ی اول به علت ٦٤ بیتی بودن سیستم و ویندوز سرور 2022 بودن آن غیر فعال شده است و فقط گزینه‌ی LSI Logic SAS فعال است و باید انتخاب کنید، توجه داشته باشید زمانی که می‌خواهیم در یک ماشین مجازی از هارد دیسک مجازی یا CD ROM و.. استفاده کنیم حتماً نیاز به یک کنترلر داریم.



شکل ۶- ۳۰ ایجاد ماشین مجازی

در شکل ٦-۳۱، نوع هارد دیسک مجازی خود را انتخاب کنید که پیشنهاد خود VMware گزینه‌ی NVMe است، در مورد هر کدام از این گزینه اگر بخواهیم توضیح مختصری بدهیم به صورت زیر خواهد بود، البته در فصل سم به طور کامل بررسی کردیم.

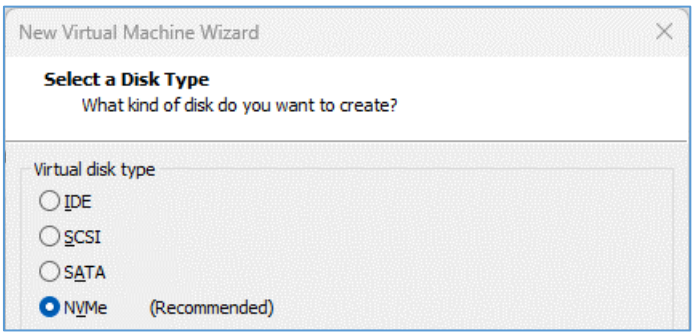
۱- SCSI (Small Computer System Interface): یکی از قدیمی‌ترین رابطها برای اتصال دستگاه‌های ذخیره‌سازی مانند هارد دیسک و نوار مغناطیسی است و برای استفاده در سرورها و محیط‌های سازمانی طراحی شده.

www.takbook.com

۲- IDE (Integrated Drive Electronics) : رابطی پرکاربرد برای کامپیوترهای شخصی که حداکثر سرعت آن در استاندارد Ultra ATA/133 برابر با ۱۳۳ MB/s بود.

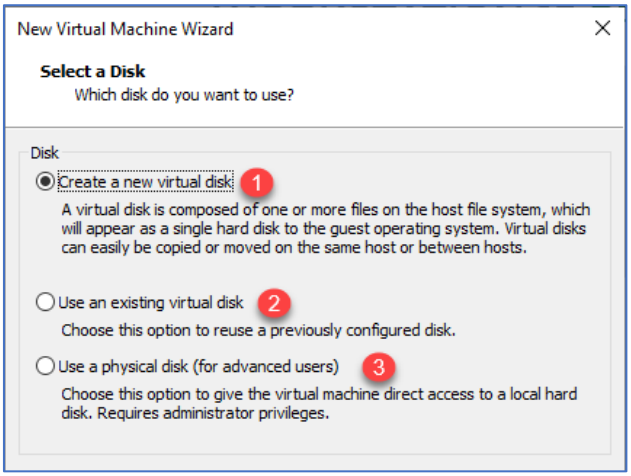
۳- SATA (Serial ATA): جایگزین IDE از اوایل دهه ۲۰۰۰ شد و کابل‌های نازک‌تر و طولانی‌تر نسبت به IDE دارد و در اکثر سیستم‌های امروزی استفاده می‌شود.

۴- NVMe (Non-Volatile Memory Express) : به‌طور چشمگیر سریع‌تر از SATA است و تا چندین گیگابایت بر ثانیه سرعت دارد.



شکل ۶- ۳۱ ایجاد ماشین مجازی

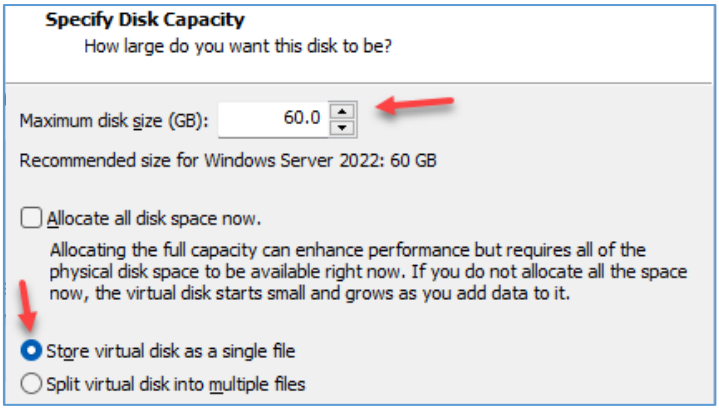
در شکل ٦-۳۲ باید هارد دیسک خود را ایجاد و یا انتخاب کنید، اگر چنانچه برای اولین بار است که می‌خواهید ماشین مجازی ایجاد کنید می‌توانید گزینه‌ی اول را انتخاب کنید و یا اگر قبلاً یک ماشین ایجاد کردید و می‌خواهید هارد دیسک مجازی آن را به این ماشین جدید ارتباط دهید گزینه‌ی دوم را انتخاب کنید و در آخر اگر بخواهید به هارد دیسک سیستم اصلی خود متصل شوید گزینه‌ی سوم را انتخاب کنید، در حال حاضر گزینه‌ی اول را انتخاب و بر روی Next کلیک کنید.



شکل ۶- ۳۲ ایجاد ماشین مجازی

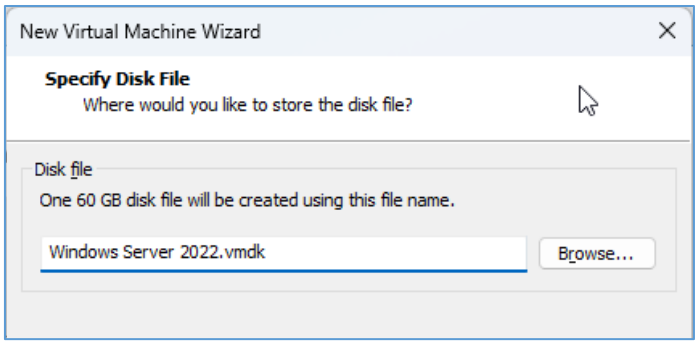
www.takbook.com

در شکل ٦-٣٣، در قسمت Maximum حداکثر اندازه هارد دیسک مجازی را مشخص کنید، اگر تیک گزینه‌ی Allocate all disk space now را انتخاب کنید همه فضایی که مشخص کردید، یکجا به این دیسک مجازی اختصاص داده خواهد شد، یعنی اینکه در هارد فیزیکی شما مثلاً ٦٠ گیگ فضا به این هارد مجازی داده خواهد شد، در پایین صفحه اگر بخواهید هارد دیسک مجازی در یک فایل مجزا ذخیره شود گزینه‌ی Store virtual disk as a single file را انتخاب کنید و یا اگر بخواهید چند هارد دیسک مجازی با حجم مشخص داشته باشید باید گزینه‌ی دوم را انتخاب کنید، توجه داشته باشید که انتخاب گزینه‌ی دوم در انتقال هارد به مکان دیگر آسان‌تر خواهد بود اما اگر سایز هارد دیسک مجازی بالا باشد در عملکرد آن با مشکل روبرو خواهد شد.



شکل ۶- ۳۳ ایجاد ماشین مجازی

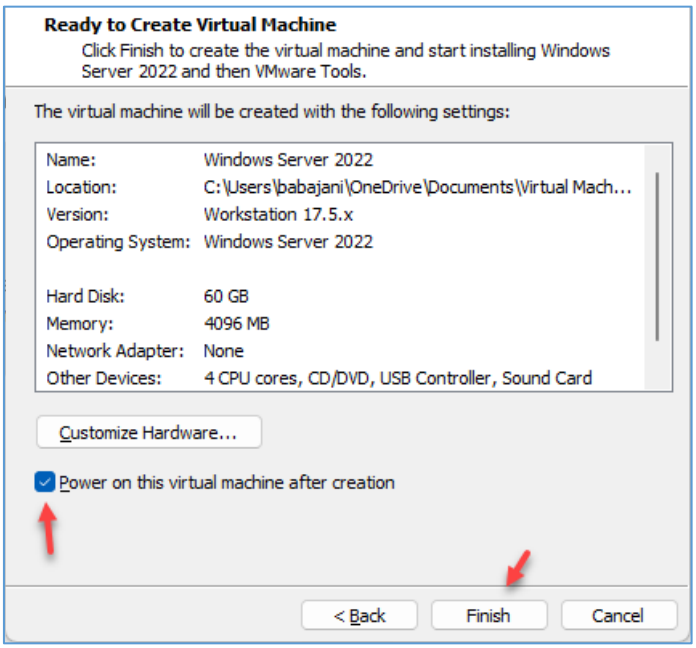
در شکل ٦-٣٤، باید مسیر ذخیره شدن دیسک مجازی را مشخص کنید که به صورت پیش‌فرض در درایوی قرار می‌گیرد که سیستم‌عامل نصب است، بهتر است این دیسک را در محلی قرار دهید که فضای آن حجم بیشتری داشته باشد تا در آینده با افزایش حجم اطلاعات ماشین مجازی، دیسک مورد نظر پر نشود.



شکل ۶- ۳۴ ایجاد ماشین مجازی

www.takbook.com

در شکل ٦-۳٥ می‌توانید تنظیماتی که برای این ماشین انجام دادید را مشاهده کنید، برای اینکه سخت‌افزارهای این ماشین مجازی را تغییر دهید باید بر روی Customize Hardware کلیک کنید که البته در ادامه این قسمت را بررسی می‌کنیم؛ برای اینکه بعد از کلیک بر روی Finish ماشین مجازی شروع به کار کند و ویندوز نصب شود تیک گزینه‌ی Power on را انتخاب کنید.



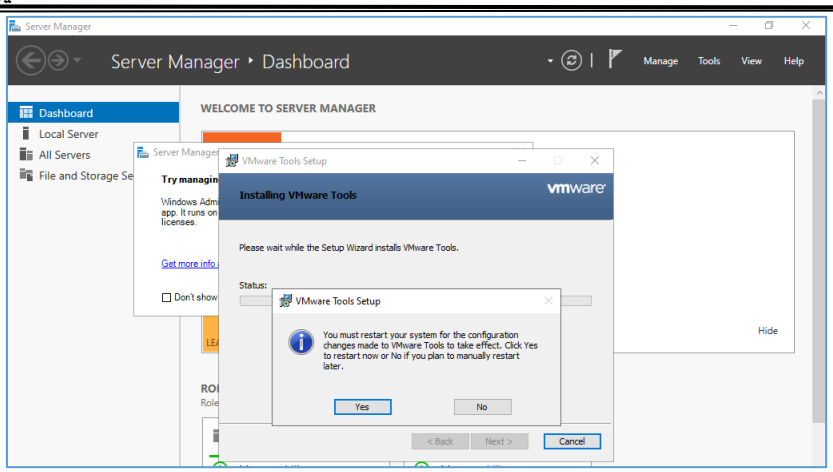
شکل ۶- ۳۵ ایجاد ماشین مجازی

بعد از نصب ویندوز و وارد شدن به محیط آن، برای اینکه سخت‌افزارهای فیزیکی بر روی ماشین مجازی اعمال شود بایدسرویس VMware Tools را نصب کنیم که البته به صورت اتوماتیک بر روی ماشین مجازی نصب خواهد شد، این یکی از ویژگی‌های مهم ارتباط ماشین مجازی با سیستم واقعی است که اگر نصب نباشد ماشین مجازی خیلی بد کار خواهد کرد و کیفیت لازم را از خود نشان نخواهد داد.

همان‌طور که در شکل٦-۳٦، مشاهده می‌کنید بعد از بالا آمدن ویندوز، سرویس VMware Tools به صورت خودکار در حال نصب می‌باشد و اگر چنانچه این سرویس به صورت خودکار اجرا نشد شما می‌توانید از منوی View گزینه‌ی Install VMware Tools را انتخاب کنید.

بعد از نصب VMware Tools ماشین را Restart کنید تا تنظیمات به طور کامل اعمال شود.

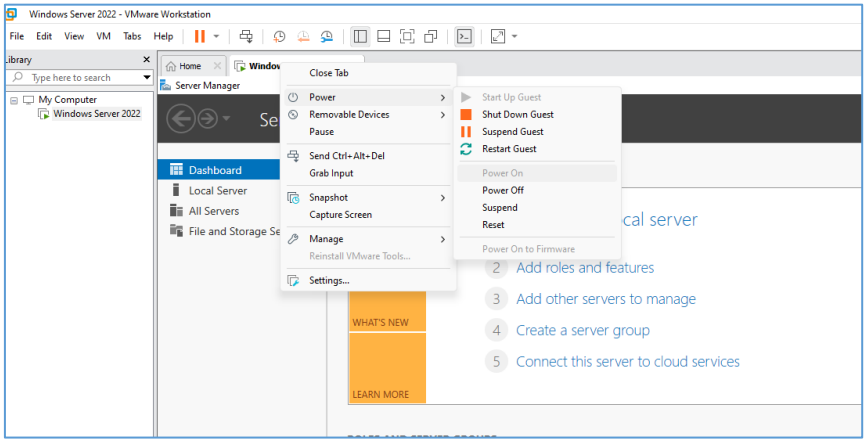
www.takbook.com



شکل ۶- ۳۶ ایجاد ماشین مجازی

۳-۳-۱-۶ کار با تنظیمات نرم‌افزار VMware Workstation

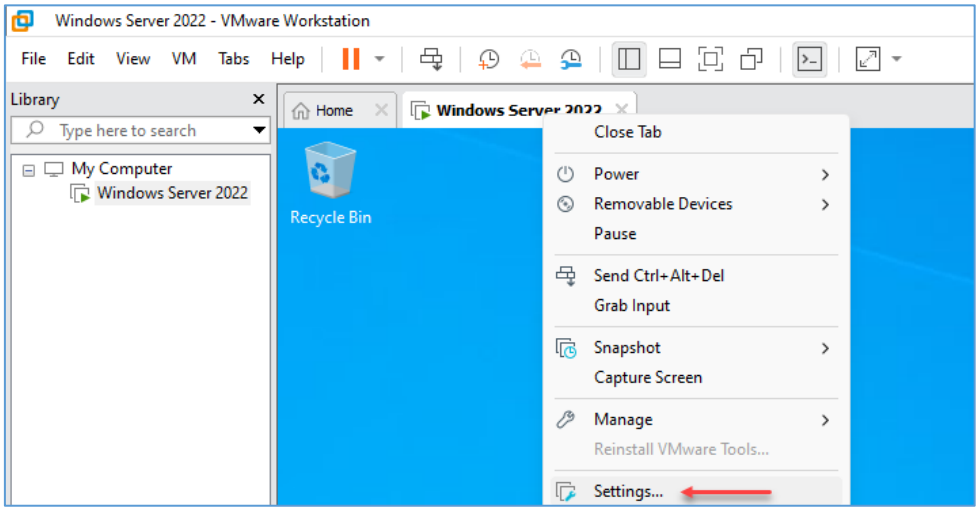
بعد از ایجاد ماشین مجازی، حالا نوبت آن است که تنظیمات نرم‌افزار را بررسی کنیم، به مانند شکل ۶-۳۷، بر روی ماشین مورد نظر کلیک راست کنید و وارد منوی Power شوید، در این منو سه قسمت وجود دارد، قسمت اول خاموش، روشن، ری‌استارت را به صورت نرم‌افزاری انجام می‌دهد یعنی اینکه مثلاً شما وارد ویندوز خود شده‌اید و سیستم خود را خاموش یا ری‌استارت کرده‌اید در آخر هر گزینه هم کلمه Guest نوشته شده است، اما در قسمت دوم به صورت سخت‌افزاری این کار انجام خواهد شد یعنی مثلاً سیستم شما روشن است و یکدفعه دکمه Restart روی کیس را فشار می‌دهید، قسمت سوم هم که مربوط به فریم و Bios می‌باشد که در حال حاضر به آن نیازی نداریم.



شکل ۶- ۳۷ اجرای ماشین مجازی

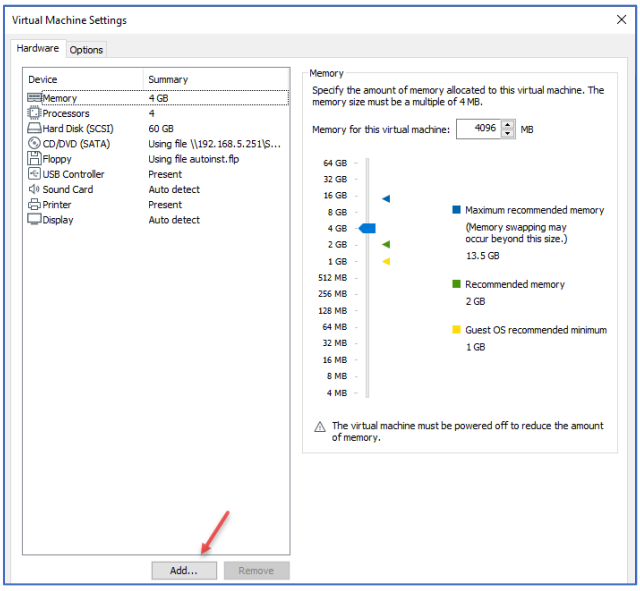
www.takbook.com

برای مشاهده تنظیمات ماشین مجازی به مانند شکل ۶-۳۸، بر روی ماشین مجازی مورد نظر کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید و یا می‌توانید از منوی VM این کار را انجام دهید.



شکل ۶- ۳۸ اجرای ماشین مجازی

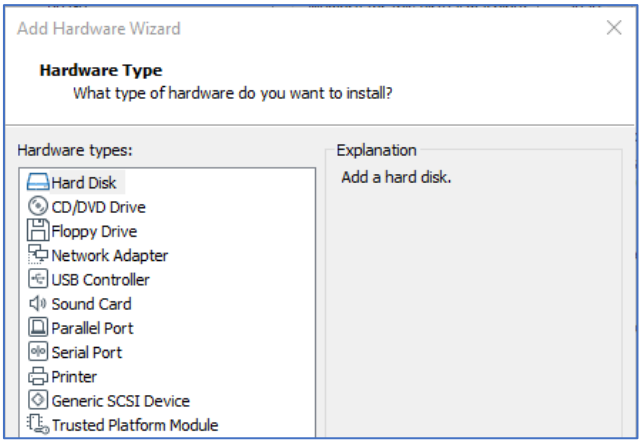
در شکل ۶-۳۹، لیستی از سخت‌افزارهایی که مربوط به این ماشین مجازی است را مشاهده می‌کنید که هر کدام قابل ویرایش و حذف هستند، برای اینکه سخت‌افزار جدید به این ماشین اضافه کنید باید بر روی Add کلیک کنید.



شکل ۶- ۳۹ تنظیمات ماشین مجازی

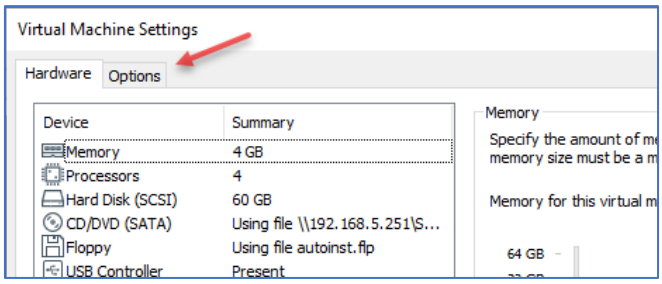
www.takbook.com

در شکل ٦-٤٠، لیست سخت‌افزارهایی که می‌توانید به این ماشین اضافه کنید را مشاهده می‌کنید، در ادامه کار و در خلال آموزش سخت‌افزار مورد نیاز را به لیست اضافه خواهیم کرد.



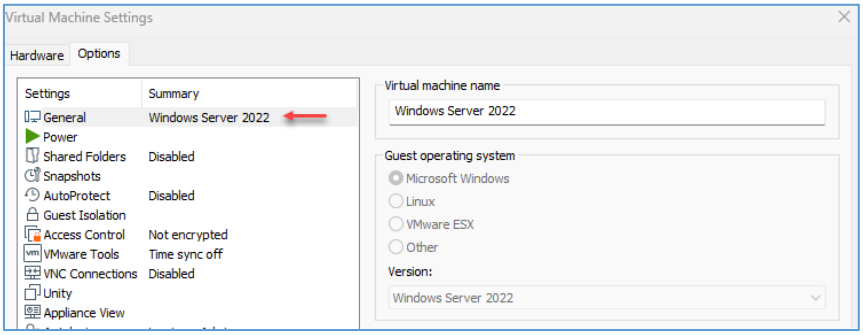
شکل ۶- ۴۰ تنظیمات ماشین مجازی

به مانند شکل ٦-٤١، وارد تب Option در پنجره‌ی Virtual Machine Settings شوید.



شکل ۶- ۴۱ تنظیمات ماشین مجازی

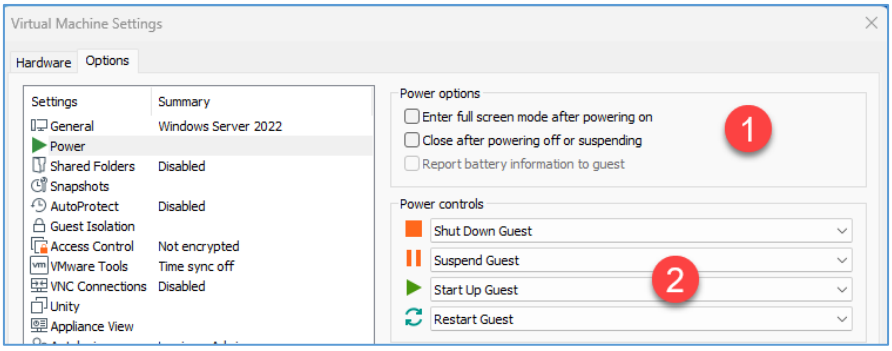
به مانند شکل ٦-٤٢، در قسمت General می‌توانید نام ماشین مجازی، نوع سیستم‌عامل، محل ذخیره‌سازی و ویژگی کیبورد را تغییر داد که البته این موارد را در هنگام ایجاد ماشین مجازی انجام دادیم.



شکل ۶- ۴۲ تنظیمات ماشین مجازی

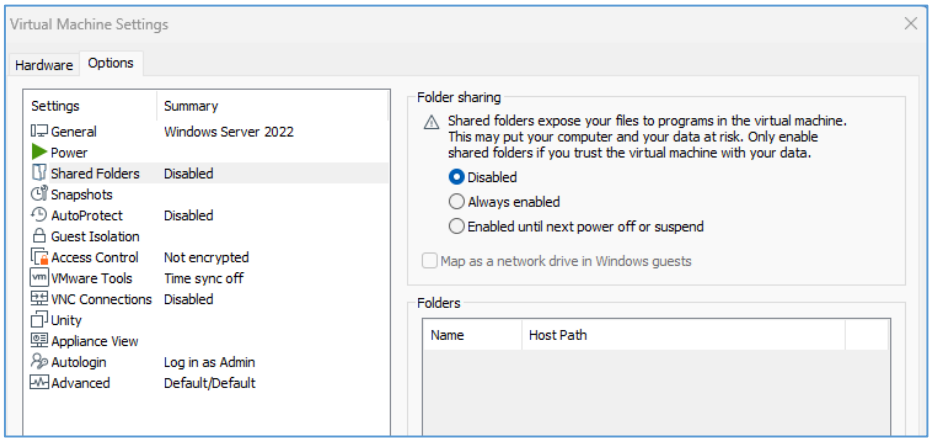
www.takbook.com

به مانند شکل ٦-٤٣، قسمت Power و در قسمت شماره‌ی یک سه گزینه را مشاهده می‌کنید، با انتخاب گزینه‌ی اول با روشن شدن ماشین مجازی صفحه‌ی آن به Full Screen تغیر حالت خواهد داد، اگر گزینه‌ی دوم انتخاب شود ماشین مجازی بعد از متوقف و خاموش شدن، بسته خواهد شد و با انتخاب گزینه‌ی سوم اگر با لپ‌تاپ کار می‌کنید اطلاعاتی از وضعیت باتری برای کاربر ارسال خواهد کرد، در قسمت شماره‌ی دو می‌توانید نوع عملکرد کلیدهای Power, Suspend, Start و Restart را از حالت نرم‌افزاری بر روی حالت سخت‌افزاری قرار دهید.



شکل ۶- ۴۳ تنظیمات ماشین مجازی

در شکل ٦-٤٤ ، در قسمت Shared Folders می‌توانید یک پوشه در سیستم اصلی خود ایجاد کنید تا بتوانید به اطلاعات ماشین مجازی دسترسی داشته باشید.

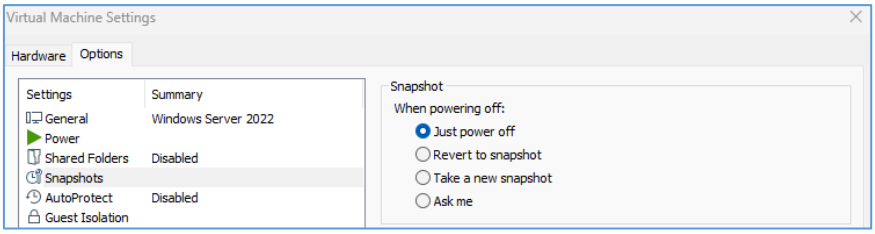


شکل ۶- ۴۴ تنظیمات ماشین مجازی

در شکل ٦-٤٥، می‌توانید مشخص کنید که زمانی که ماشین مجازی روشن می‌شود از شما در مورد گرفتن Snapshot سوال کند یا اینکه یک Snapshot جدید بگیرد و یا به آخرین Snapshot که گرفته شده است برگردد و یا اینکه فقط ماشین روشن شود، Snapshot عملکردی است که اگر آن را فعال کنید در لحظه از

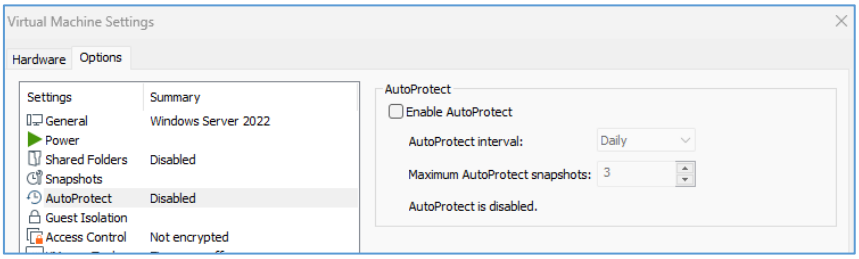
www.takbook.com

ماشین مورد نظر پشتیبان تهیه می‌کند و اگر در ادامه کار با مشکل روبرو شدید می‌توانید به تاریخی که Snapshot تهیه کردید برگردید.



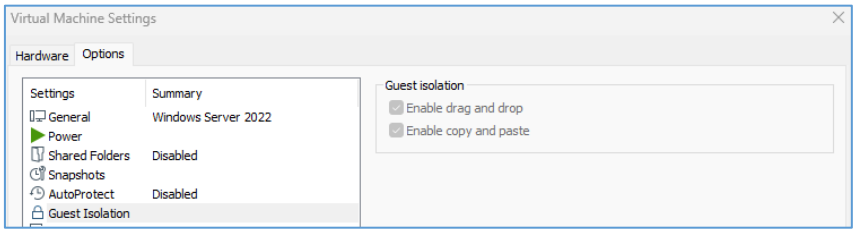
شکل ۶- ۴۵ تنظیمات ماشین مجازی

در شکل ٦-٤٦ و در قسمت AutoProtect برای ایجاد امنیت از ماشین به صورت خودکار Snapshot تهیه خواهد شد که این موضوع می‌تواند به صورت روزانه، هفتگی و یا ماهانه صورت پذیرد و حتی بسته به ظرفیت دیسک می‌تواند تعداد آن را مشخص کنید.



شکل ۶- ۴۶ تنظیمات ماشین مجازی

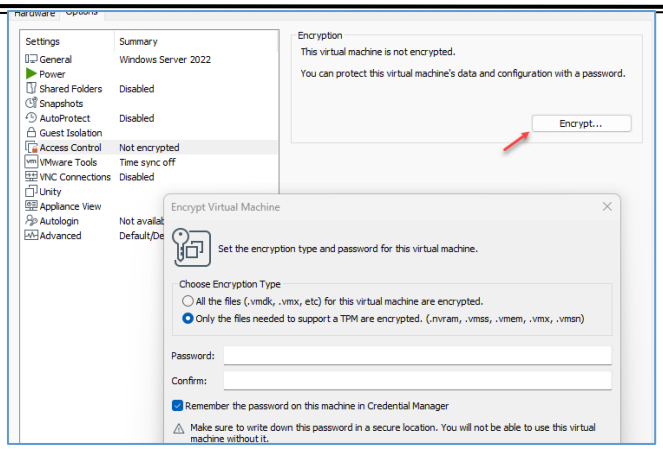
در شکل ٦-٤٧، دو گزینه وجود دارد که یکی برای Drag and drop می‌باشد و دیگری برای Copy و Past کردن است که می‌توانید آنها را غیر فعال کنید، توجه داشته باشید که این دو گزینه با نصب VMware Tools در ماشین مجازی فعال خواهند شد.



شکل ۶- ۴۷ تنظیمات ماشین مجازی

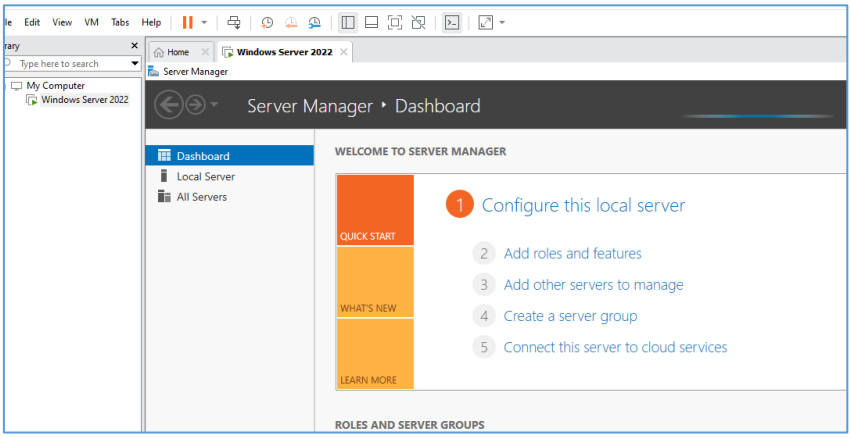
در شکل ٦-٤٨ و در قسمت Access Control می‌توانید رمز عبور برای ماشین ایجاد کنید که برای دسترسی به آن مورد نیاز است که این قسمت را در ادامه کتاب بررسی کردیم، بقیه گزینه‌ها هم در صورت نیاز بررسی خواهیم کرد.

www.takbook.com



شکل ۶- ۴۸ تنظیمات ماشین مجازی

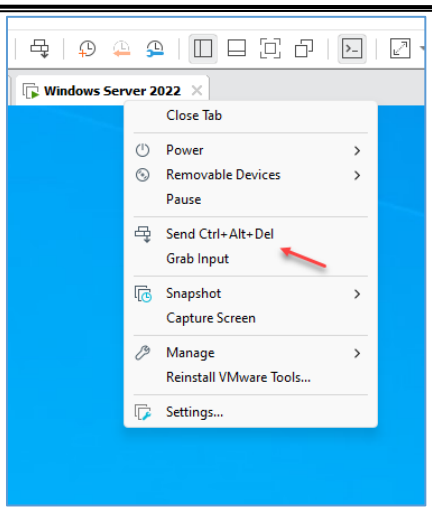
برای اینکه بتوانید صفحه ماشین مجازی را Full Screen کنید باید به مانند شکل ٦-٤٩، داخل ماشین مجازی کلیک و بعد از آن از کلید ترکیبی ALT + CTRL + Enter استفاده کنید، و برای برگشت به حالت قبل دوباره باید از همین کلیدها استفاده کنید.



شکل ۶- ۴۹ تنظیمات ماشین مجازی

برای اینکه Task Manager مربوط به ماشین مجازی را اجرا کنیم باید از کلید ترکیبی CTRL + ALT + Insert استفاده کنید، راه دیگر هم برای اجرای Task Manager این است که به مانند شکل ٦-٥٠، بر روی ماشین مجازی کلیک راست کنید و گزینه‌ی Send Ctrl+Alt+Del را انتخاب کنید.

www.takbook.com



شکل ۶- ۵۰ تنظیمات ماشین مجازی

در بعضی مواقع از سیستم عامل مانند لینوکس و... استفاده می‌کنید که با کلیک بر روی آن دیگر نمی‌توانید موس خود را از آن حالت خارج کنید، برای حل این مشکل باید از کلید ترکیبی CTRL + ALT استفاده کنید.

٤-١-٦ بررسی سیستم‌عامل ESXi

VMware ESXi (که گاهی با نام‌های vSphere Hypervisor یا VMware ESX نیز شناخته می‌شود) یک هایپروایزر نوع ۱ است که توسط شرکت VMware توسعه داده شده و برای ایجاد و مدیریت ماشین‌های مجازی (Virtual Machines) استفاده می‌شود. ESXi به صورت مستقیم روی سخت‌افزار فیزیکی (بدون نیاز به سیستم‌عامل میانی) نصب می‌شود و به کاربران اجازه می‌دهد چندین سیستم‌عامل را به طور همزمان و مستقل روی یک سرور فیزیکی اجرا کنند.

ویژگی‌های اصلی VMware ESXi:

- هایپروایزر نوع ۱: ESXi به عنوان یک هایپروایزر "Bare Metal" شناخته می‌شود که به طور مستقیم روی سخت‌افزار فیزیکی اجرا می‌شود. برخلاف هایپروایزر نوع ۲ که روی یک سیستم‌عامل میزبان نصب می‌شود، ESXi نیازی به سیستم‌عامل میانی ندارد و به همین دلیل دارای کارایی بالاتر و تأخیر کمتر است.
- اندازه کوچک و بهینه‌سازی شده: ESXi یکی از سبک‌ترین هایپروایزرها است. اندازه کوچکی دارد (حدود ۱۵۰ مگابایت) و به دلیل حذف کامپوننت‌های غیرضروری، بسیار پایدار و کارآمد است.

www.takbook.com

- مدیریت ماشین‌های مجازی: ESXi امکان ایجاد، اجرا، و مدیریت چندین ماشین مجازی روی یک سرور فیزیکی را فراهم می‌کند. هر ماشین مجازی می‌تواند یک سیستم‌عامل مستقل (مانند ویندوز، لینوکس، یا دیگر سیستم‌عامل‌ها) داشته باشد.
- ESXi: vSphere بخشی از مجموعه بزرگ‌تر VMware vSphere است که ابزارها و امکانات مدیریتی پیشرفته‌ای برای مدیریت محیط‌های مجازی‌سازی ارائه می‌دهد. با استفاده از vSphere می‌توانید از امکاناتی مثل High Availability (HA)، DRS (Distributed Resource Scheduler)، و vMotion برای مهاجرت زنده ماشین‌های مجازی بین سرورها بهره‌مند شوید.
- پشتیبانی از سخت‌افزارهای مختلف: ESXi از انواع مختلف سخت‌افزارهای سروری مانند پردازنده‌های Intel و AMD، حافظه‌ها و دیسک‌ها، کارت‌های شبکه و ذخیره‌سازی پشتیبانی می‌کند. لیست دقیق سخت‌افزارهای پشتیبانی‌شده در سایت VMware موجود است.
- امنیت بالا: ESXi دارای ویژگی‌های امنیتی پیشرفته‌ای است که از محیط‌های مجازی در برابر تهدیدات محافظت می‌کند. امکاناتی مانند مدیریت نقش‌ها و دسترسی‌ها (RBAC)، رمزنگاری، و Secure Boot از جمله ویژگی‌های امنیتی ESXi هستند.

- پشتیبانی از پروتکل‌های ذخیره‌سازی مختلف: ESXi از انواع پروتکل‌های ذخیره‌سازی مانند iSCSI، NFS، و Fibre Channel پشتیبانی می‌کند. این امکان به شما اجازه می‌دهد تا با استفاده از منابع ذخیره‌سازی مختلف، محیط مجازی خود را پیکربندی کنید.

کاربردهای VMware ESXi:

- مجازی‌سازی سرورها: ESXi برای تبدیل سرورهای فیزیکی به چندین ماشین مجازی استفاده می‌شود. این ماشین‌های مجازی می‌توانند سرویس‌های مختلفی مانند وب سرورها، دیتابیس‌ها، و سیستم‌های برنامه‌نویسی را ارائه دهند.
- کلاسترینگ و تحمل خطا (High Availability) : ESXi به همراه vSphere می‌تواند برای ایجاد کلاسترهای سرور و فراهم کردن امکان تحمل خطا (Failover) و بهبود پایداری استفاده شود. به این ترتیب اگر یکی از سرورها از دسترس خارج شود، ماشین‌های مجازی به طور خودکار به سرورهای دیگر منتقل می‌شوند.
- مراکز داده (Data Centers): ESXi در مراکز داده برای کاهش تعداد سرورهای فیزیکی و بهینه‌سازی استفاده از منابع فیزیکی به کار می‌رود. این کار منجر به کاهش هزینه‌ها و افزایش بهره‌وری منابع می‌شود.

www.takbook.com

- آزمایش و توسعه نرم‌افزار: توسعه‌دهندگان نرم‌افزار و تیم‌های تست می‌توانند از ESXi برای ایجاد ماشین‌های مجازی به منظور آزمایش نسخه‌های مختلف سیستم‌عامل‌ها و نرم‌افزارها استفاده کنند، بدون اینکه نیازی به منابع فیزیکی بیشتری داشته باشند.

تفاوت ESXi با نسخه‌های دیگر VMware (مانند VMware Workstation):

ESXi یک هایپروایزر نوع ۱ است که مستقیماً روی سخت‌افزار فیزیکی نصب می‌شود، در حالی که VMware Workstation یک هایپروایزر نوع ۲ است که روی یک سیستم‌عامل میزبان (مثلاً ویندوز یا لینوکس) اجرا می‌شود.

ESXi برای محیط‌های سروری و مراکز داده طراحی شده و دارای قابلیت‌های پیشرفته مدیریتی است، در حالی که VMware Workstation بیشتر برای آزمایش و توسعه نرم‌افزارها روی سیستم‌های دسکتاپ مورد استفاده قرار می‌گیرد.

در نهایت، VMware ESXi یکی از پرکاربردترین و محبوب‌ترین هایپروایزرها در جهان است که به دلیل قابلیت‌های پیشرفته، پایداری بالا و مدیریت آسان، در محیط‌های مختلف از جمله مراکز داده، محیط‌های توسعه و تست، و شرکت‌های بزرگ مورد استفاده قرار می‌گیرد که در ادامه به طور کامل قابلیت آن را بررسی می‌کنیم.

۱-٤-۱-٦ سخت‌افزار مورد نیاز برای نصب ESXi

برای اینکه سیستم‌عامل ESXi را بر روی سرور نصب کنید باید منابع سخت‌افزاری مورد نیاز آن را فراهم کنید، در زیر لیست سخت‌افزار مورد نیاز برای نصب آن مشخص شده است.

۱- ESXi ورژن 8 نیاز به حداقل دو هسته‌ی CPU دارد.

۲- ESXi 6.7 از پردازنده‌های X64 و X86 پشتیبانی می‌کند، پردازنده‌هایی که از سال ۲۰۰٦ به بعد تولید شدند که این پردازنده‌ها بسیار گسترده هستند و می‌توان گفت که سیستم‌عامل ESXi بر روی بیشتر پردازنده‌ها نصب خواهد شد، برای اطلاعات بیشتر در مورد پردازنده‌ها می‌توانید از لینک زیر استفاده کنید:

http://www.vmware.com/resources/compatibility

۳- برای اجرای ESXi 8 باید بیت NX/XD در Bios را فعال کنید، توجه داشته باشید بیت NX و XD بیشتر برای حافظت کاربرد دارد که NX در CPU شرکت AMD و XD در CPUهای شرکت Intel قرار دارند و باید فعال شوند.

۴- مقدار رم مورد نیاز سیستم عامل ESXi 8 برابر با ٤ گیگابایت است که برای اجرای ماشین مجازی در آن بهتر است این مقدار برابر ۸ گیگابایت باشد.

www.takbook.com

۵- برای پشتیبانی از پردازنده‌های ٦٤ بیتی باید قابلیت (Intel VT-x یا AMD RVI) در پردازنده‌ها فعال شود، که البته این کار را در قسمت قبل توضیح دادیم.

۶- به یک یا چند کارت شبکه نیاز است.

۷- نیاز به فضای ذخیره‌سازی مجزا برای ESXI است که مقدار فضای آن باید حداقل ۵ گیگابایت باشد.

۸- در این سیستم‌عامل قابلیت بوت بر روی تکنولوژی UEFI وجود دارد که با این تکنولوژی می‌توانید سیستم مورد نظر را بر روی CD-Rom، Flash و... اجرا کنید.

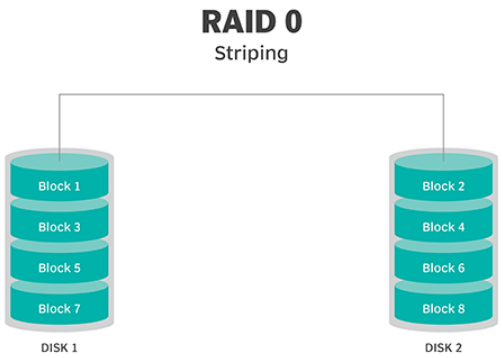
۲-٤-۱-٦ RAIDبندی هارد دیسک

قبل از تنظیم سرور HP باید بحث Raidبندی را بررسی کنیم، Raidبندی مدل‌های مختلفی دارد و کمک می‌کند تا اطلاعاتی که بر روی هاردها قرار دارد حفاظت شود و سرعت دستیابی به اطلاعات هم متغییر خواهد بود.

انواع مدل‌های Raid

۱- **Striped Volume (RAID 0)**

این نوع Raidبندی سرعت بسیار بالایی دارد و دلیل آن هم این است که از تمام فضاهای هارد دیسک استفاده می‌کند و نحوه‌ی نوشتن بر روی هارد بصورت خطی و مستقیم می‌باشد و برای فعال کردن آن حداقل به دو هارد دیسک نیاز دارید، اما نکته مهم در این نوع Raid این است که امنیت بسیار پایینی دارد به صورتی که اگر یکی از هاردها خراب شود اطلاعات به طور کامل از دست خواهد رفت، در شکل ٦-۵۱، هر دو هارد دیسک را مشاهده می‌کنید که با انتخاب نوع Raid0نحوه‌ی نوشتن اطلاعات به صورت خطی است و Blockها به ترتیب در هر هارد نوشته می‌شود.

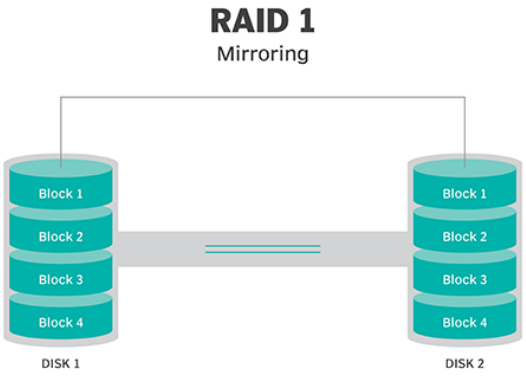


شکل ۶- ۵۱ *Striped Volume*

www.takbook.com

۲- **Disk Mirroring (RAID 1)**

در این روش که به روش آینه‌ای معروف است، حداقل به دو هارد دیسک نیاز دارید و هر چیز که در هارد اول نوشته شود در هارد دوم هم نوشته خواهد شد و این کار باعث می‌شود اطلاعات با سرعت بالا خوانده شود ولی مشکلی که دارد این است که نوشتن اطلاعات کمی آهسته خواهد بود، در این نوع Raid تحمل خطا وجود دارد و اگر یک هارد خراب شود هارد دیگر اطلاعات را در اختیار دارد، از این نوع Raid برای نصب سیستم‌عامل استفاده خواهد شد که برای نصب ESXi هم می‌توانید از این روش استفاده کنیم، در شکل ٦-٥٢ این نوع Raidبندی را مشاهده می‌کنید.

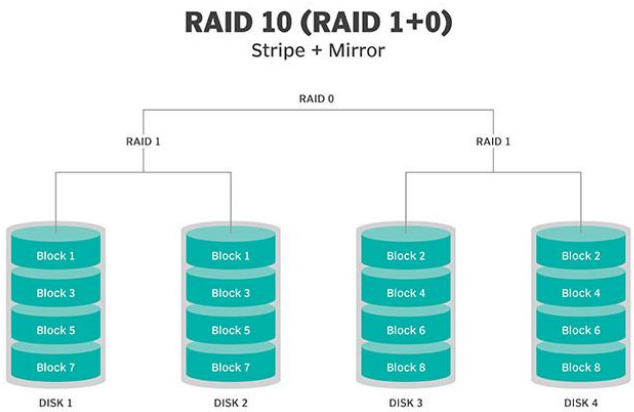


شکل ۶- ۵۲ Disk Mirroring (RAID 1)

۳- **RAID 10**

این نوع Raid ترکیبی از Raid0 و Raid 1 است، در این نوع حداقل نیاز به 4 هارد دیسک دارید، در این روش Raid اصلی Raid0 است و هر ٤ دیسک را پوشش می‌دهد و Raid داخلی Raid1 است که برای هر دو هارد دیسک طراحی شده است، در شکل ٦-٥٣، دقیقاً این موضوع مشخص شده است، مهمترین نکته این روش این است که حفظ اطلاعات بسیار بالا است و تحمل پذیری خطا خیلی بالا است و از همه روش‌ها قویتر است.

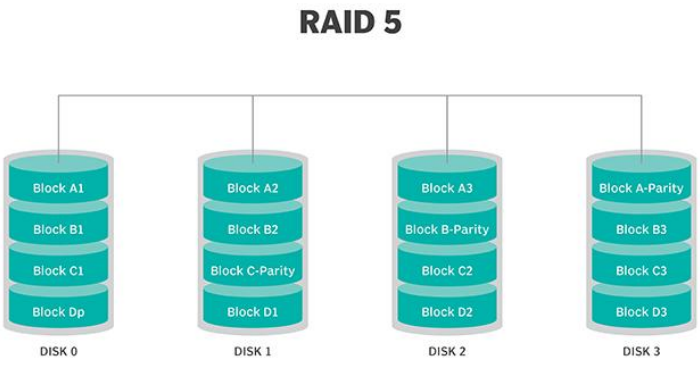
www.takbook.com



شکل ۶- ۵۳ *Disk Mirroring (RAID 1)*

۴- Raid 5

یکی از قویترین حالت‌های تقسیم‌بندی دیسک است، حداقل هارد دیسک مورد نیاز برای این حالت ۳ عدد می‌باشد که اطلاعات به طور همزمان بر روی هر سه هارد دیسک نوشته می‌شود و با از کار افتادن یک هارد، بقیه هاردها به کار خود ادامه می‌دهند ولی اگر دوتا از هاردها از کار انداخته شود هارد سوم هم از کار انداخته خواهد شد، البته اگر یکی از هاردها خراب شود باید در مدت زمان کوتاهی هارد جدید را به سرور اضافه کرد، در این روش خواندن از دیسک به صورت هم‌زمان خواهد بود از همه دیسک‌ها استفاده می‌شود، در شکل ٦-٥٤، بلاک‌بندی RAID5 را مشاهده می‌کنید، نکته‌ای که در این دیسک‌ها وجود دارد، کلمه‌ی A-Parity است که بر ایجاد تحمل پذیری خطا است و بسیار برای امنیت اطلاعات کاربرد دارد.

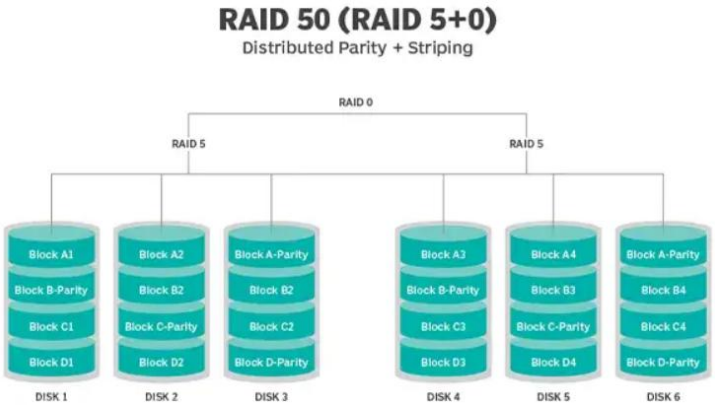


شکل ۶- ۵۴ *Raid 5*

www.takbook.com

۵- RAID 50

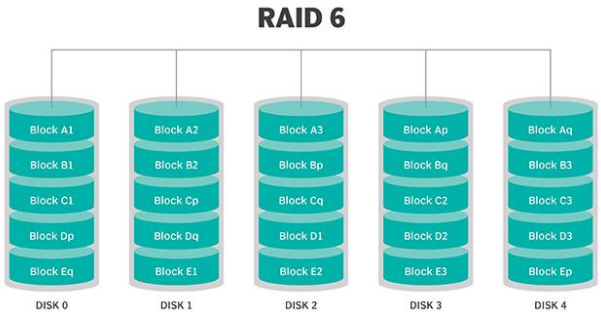
این نوع Raid ترکیبی می‌باشد و ترکیبی از RAID 0 و RAID50 است و حداقل به 6 دیسک نیاز دارد، RAID اصلی آن صفر است و RAID داخلی آن RAID5 است که در شکل ٦-٥٥، هم آن را مشاهده می‌کنید، هزینه‌ی این نوع RAID بالا است اما امنیت فوق العاده‌ای دارد.



شکل ۶- ۵۵ RAID 50

۶- RAID 6

این نوع RAID امنیت بالاتری به نسبت RAID5 دارد که اگر دو هارد دیسک خراب شود بقیه هارد دیسک‌ها به کار خود ادامه خواهند داد، در این نوع RAID از دو Parity استفاده می‌شود و به خاطر همین حجمی که ارائه می‌دهد کمتر از RAID5 است، در این نوع RAID حداقل به 4 هارد دیسک نیازمنیدم که در شکل ٦-٥٦ این موضوع مشخص شده است.

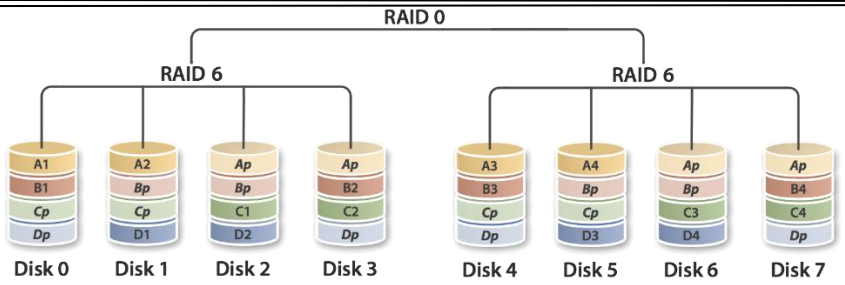


شکل ۶- ۵۶ RAID 6

۷- RAID 60

این نوع RAID ترکیبی از RAID 6 و RAID0 است که نیاز به حداقل ۸ هارد دیسک است که آن را در شکل ٦-٥٧، مشاهده می‌کنید.

www.takbook.com



شکل ۶- ۵۷ RAID 60

برای اینکه دقیق بدانیم که وقتی یک نوع RAID را انتخاب کردیم چقدر فضا در اختیار ما قرار می‌دهد باید از سایت‌های آنلاین مانند آدرس زیر استفاده کنیم.

https://www.synology.com/en-global/support/RAID_calculator

همان‌طور که در شکل ٦-٥٨، مشاهده می‌کنید، اول باید نوع و تعداد هارد را مشخص کنید که در اینجا ۸ هارد دیسک با ظرفیت ۱ ترابایت مشخص شده است، در ادامه باید نوع RAID خود را از منوی کشویی مشخص شده انتخاب کنید، در شکل مشخص است که مقدار فضایی که می‌شود استفاده کرد در RAID5 بیشتر از RAID6 است که به خاطر دلایلی است که در قسمت قبل بیان کردیم، پس این سایت بسیار می‌تواند به شما کمک کند.



شکل ۶- ۵۸ RAID_calculator

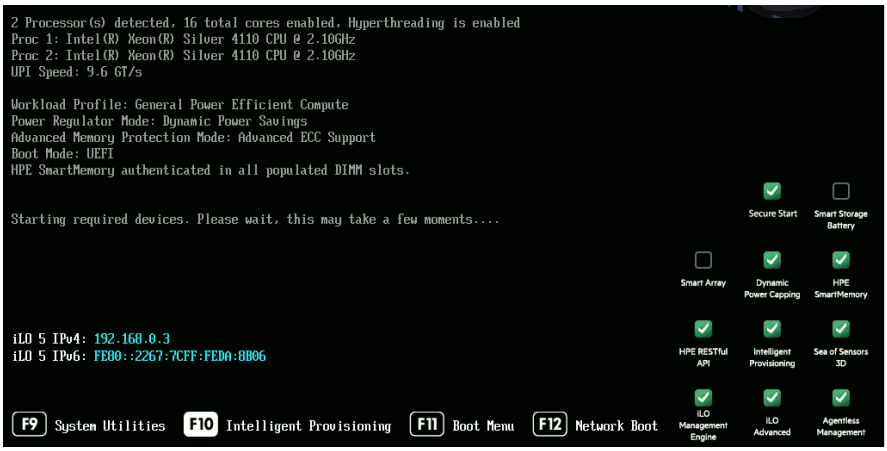
٣-٤-١-٦ تنظیمات اولیه سرور HP

برای اینکه سرورهای HP را تنظیم کنیم باید از نرم‌افزاری که در داخل خود سرور وجود دارد استفاده کنید، در سرورهای قدیمی مانند G6,G7 از نرم‌افزاری با نام Smart Start استفاده می‌شد که قبلاً در کتاب

www.takbook.com

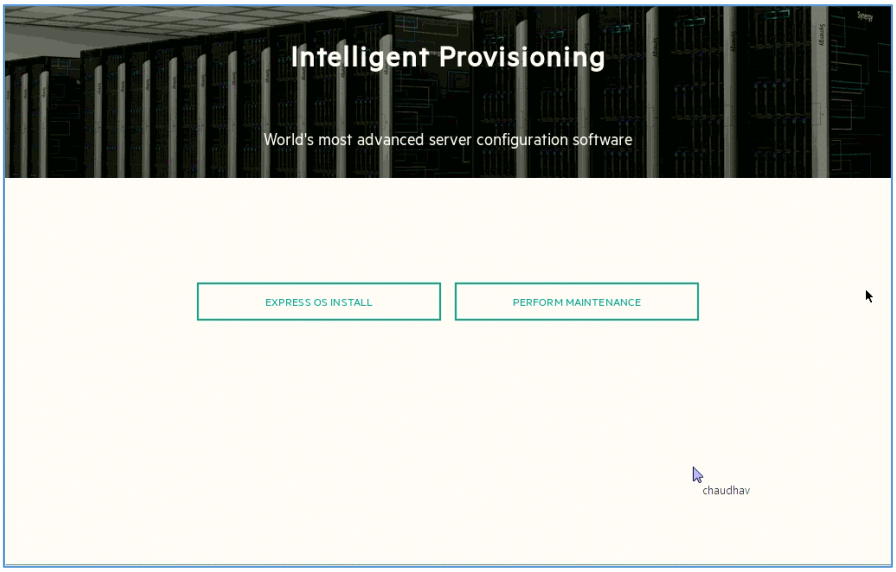
مدیر شبکه یک و کتاب VMware System توضیح دادیم. اما در سری‌های 8,9,10,11 سرور HP، این نرم‌افزار در داخل بوت قرار دارد و با فشار دادن کلید F10 در حالت Boot می‌توانید به آن دسترسی پیدا کنید.

برای انجام کار سرور را روشن می‌کنیم، و اولین صفحه‌ای که ظاهر می‌شود شکل ٦-٥٩، خواهد بود، در این صفحه باید بر روی کلید F11 فشار دهید.



شکل ۶- ۵۹ تنظیمات اولیه سرور HP

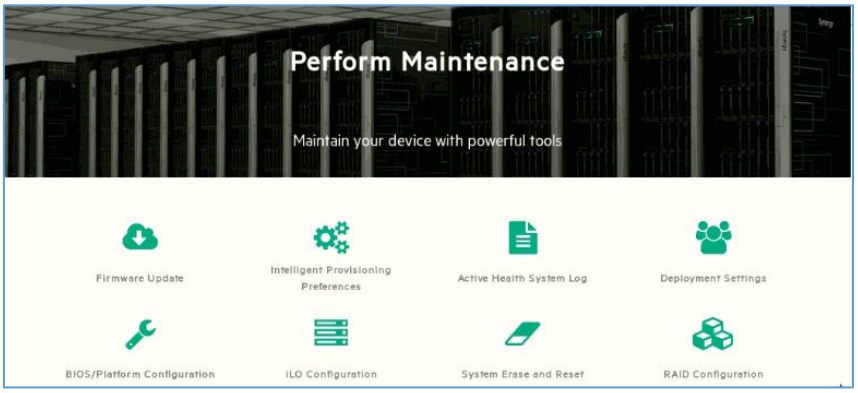
در شکل ٦-٦٠، گزینه‌ی Performance Maintenance را انتخاب کنید.



شکل ۶- ۶۰ تنظیمات اولیه سرور HP

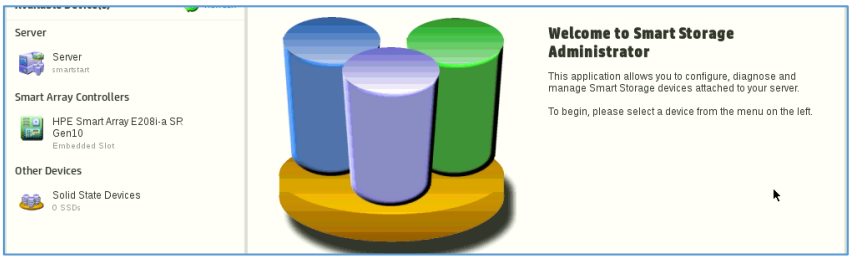
www.takbook.com

در ادامه و در صفحه‌ی زیر گزینه‌های مختلفی را مشاهده می‌کنید که اکثر گزینه‌ها را در خلال کار بررسی خواهیم کرد، در حال حاضر گزینه‌ی Raid Configuration را طبق شکل ٦-٦١، انتخاب کنید.



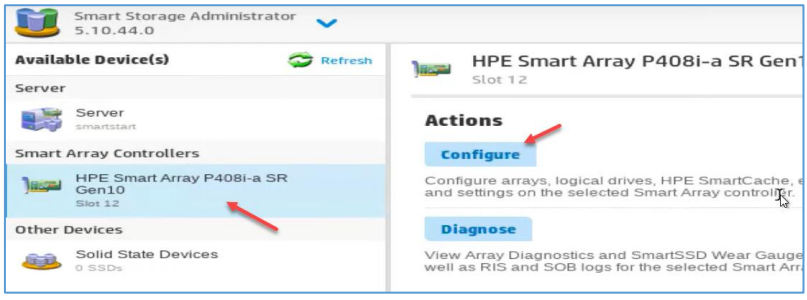
شکل ۶- ۶۱ تنظیمات اولیه سرور HP

همان‌طور که در فصل سوم سرورهای HP را بررسی کردیم، گفتیم که قطعه‌ای به نام Raid Controller وجود دارد که برای Raid بندی هارد دیسک‌ها کاربرد دارد و این صفحه دقیقاً مربوط به همان قطعه است و می‌خواهیم هاردهایی که بر روی سرور وجود دارد را Raid بندی کنیم، برای شروع بر روی HPE Smart Array کلیک کنید.



شکل ۶- ۶۲ تنظیمات اولیه سرور HP

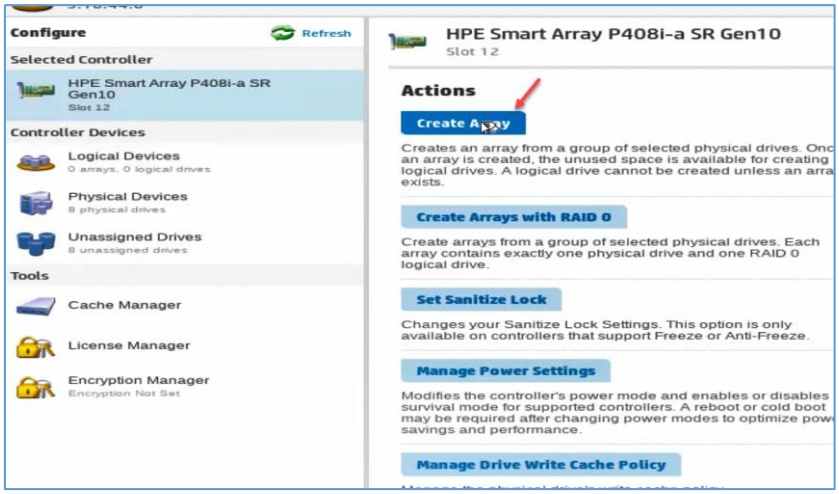
در ادامه باید به مانند شکل ٦-٦٣، بر روی Configure کلیک کنید.



شکل ۶- ۶۳ تنظیمات اولیه سرور HP

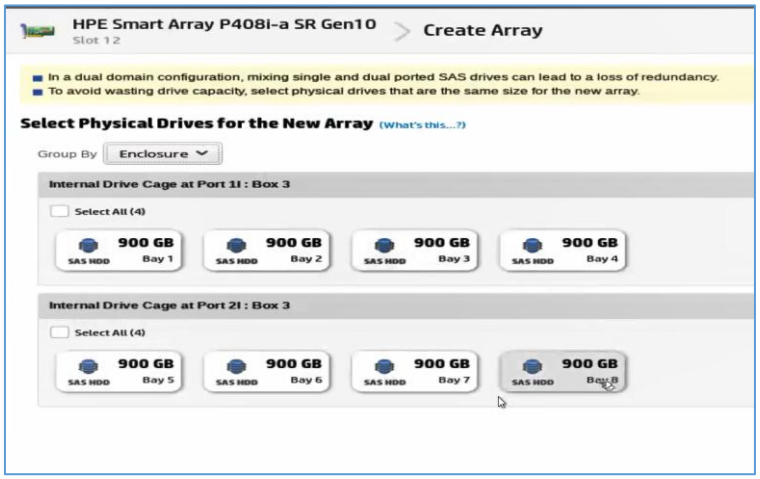
www.takbook.com

در شکل ٦-٦٤ در قسمت Physical Devices، 8 تا هارد دیسک را مشخص کرده است که بر روی سرور نصب شده است و برای اینکه آنها را Raid بندی کنیم باید بر روی Create Array کلیک کنید.



شکل ۶- ۶۴ Create Array

همان‌طور که در شکل ٦-٥٦، مشاهده می‌کنید، 8 هارد 900GB به سرور متصل و شناسایی شده است، اگر به دقت به شکل توجه کنید در زیر عدد 900 کلمه‌ی Bay نوشته شده است که این کلمه مربوط به جایگاه هارد در سرور است و مشخص می‌کند کدام هارد مربوط به کدام شیار است.



شکل ۶- ۶۵ Create Array

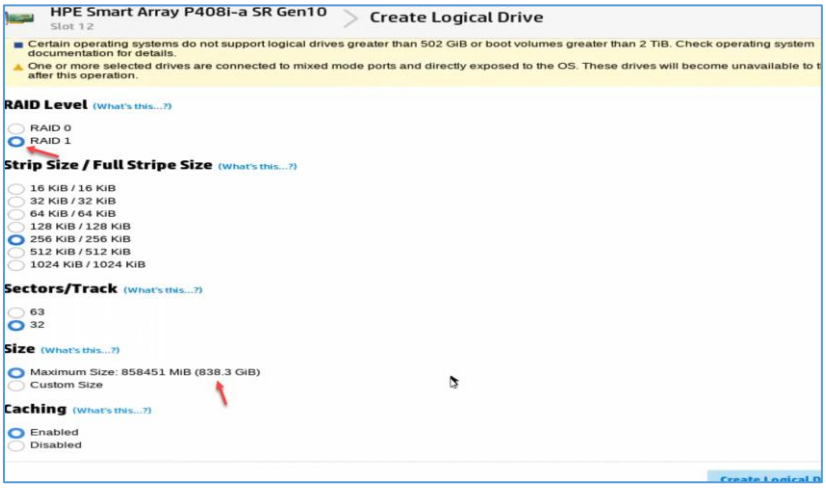
برای شروع و برای اینکه سیستم‌عامل ESXi را بر روی سرور نصب کنیم باید دوتا از هاردها را به مانند شکل ٦-٦٦، انتخاب کنیم و بر روی Create Array کلیک کنید.

www.takbook.com



شکل ۶- ۶۶ Create Array

در شکل ٦-٦٧، گزینه‌ی Raid 1 را انتخاب کنید که در قسمت Size مقدار حجم در دسترس این دو هارد را به شما نمایش می‌دهد، توجه داشته باشید چون فقط دو هارد انتخاب کردیم گزینه‌های دیگر Raid مانند Raid5 را نمایش نداده است، بر روی Create Locical Drive کلیک کنید.



شکل ۶- ۶۷ Create Array

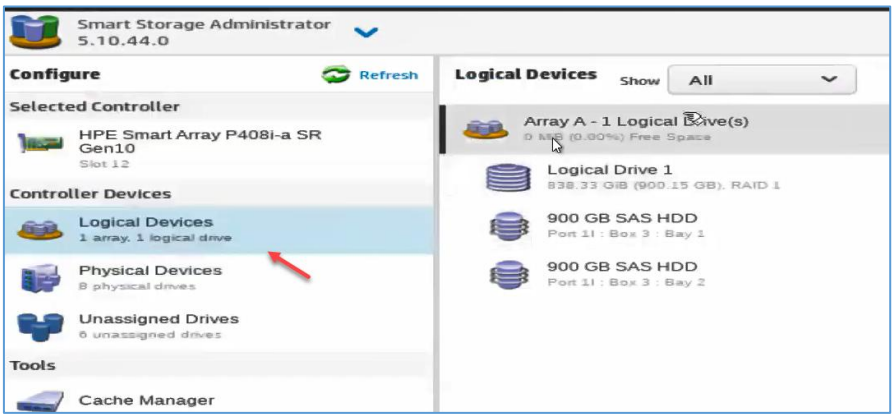
در شکل ٦-٦٨، دقیقاً مشخص کرده که کدام هاردها با Raid1 ایجاد می‌شوند و فضای کلی و فضایی که در دسترس ما قرار می‌گیرد را مشخص کرده است، بر روی Finish کلیک کنید تا Array جدید ایجاد شود.

www.takbook.com



شکل ۶- ۶۸ *Create Array*

بعد از کلیک بر روی Finish به مانند شکل ٦-٦٩، Array A ایجاد شده است که دارای دو هارد دیسک است و با نام Logical Drive 1 مشخص است.



شکل ۶- ۶۹ *Create Array*

بعد از ایجاد Raid1 می‌خواهیم بقیه‌ی هاردها را RAID5 کنیم برای این کار دوباره بر روی Create Array کلیک کنید و در شکل باز شده‌ی ٦-٧٠، همه هاردها را انتخاب کنید و بر روی Create Array کلیک کنید.

www.takbook.com



شکل ۶- ۷۰ *Create Array*

همان‌طور که در شکل ٦-۷۱، مشاهده می‌کنید، با انتخاب هر ٦ هارد گزینه‌های جدیدتری برای RAID ظاهر شده که همه آنها را در قسمت قبل توضیح دادیم، فقط RAID 60 موجود نیست که آن هم به دلیل کم بودن تعداد هارد است و مقدار آن ۸ تا نیست.

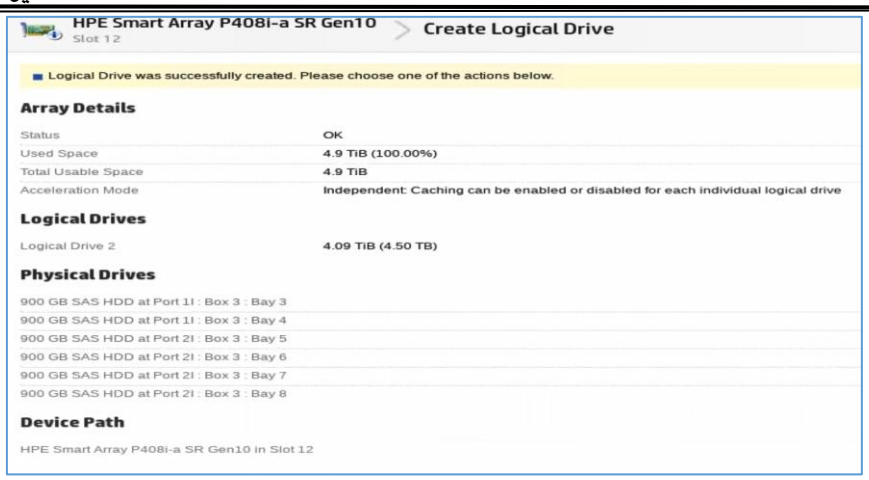
برای انجام RAID گزینه‌ی RAID5 را انتخاب کنید و بر روی Create Logical Drive کلیک کنید، فقط در قسمت شماره‌ی دوم مقدار فضایی که در دسترس قرار می‌گیرد را مشخص کرده است.



شکل ۶- ۷۱ *Create Array*

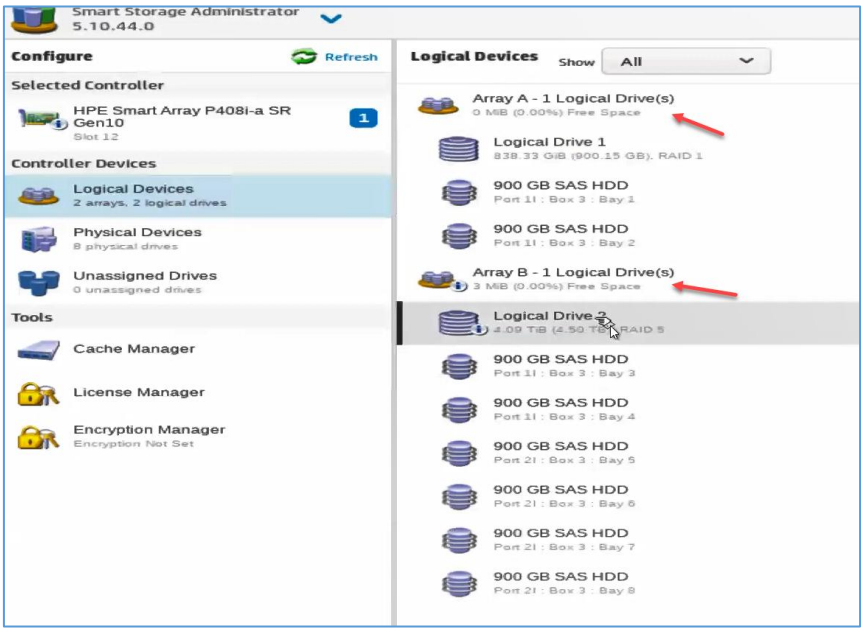
در شکل ٦-۷۲ هم بر روی Finish کلیک کنید تا کار به اتمام برسد.

www.takbook.com



شکل ۶- ۷۲ Create Array

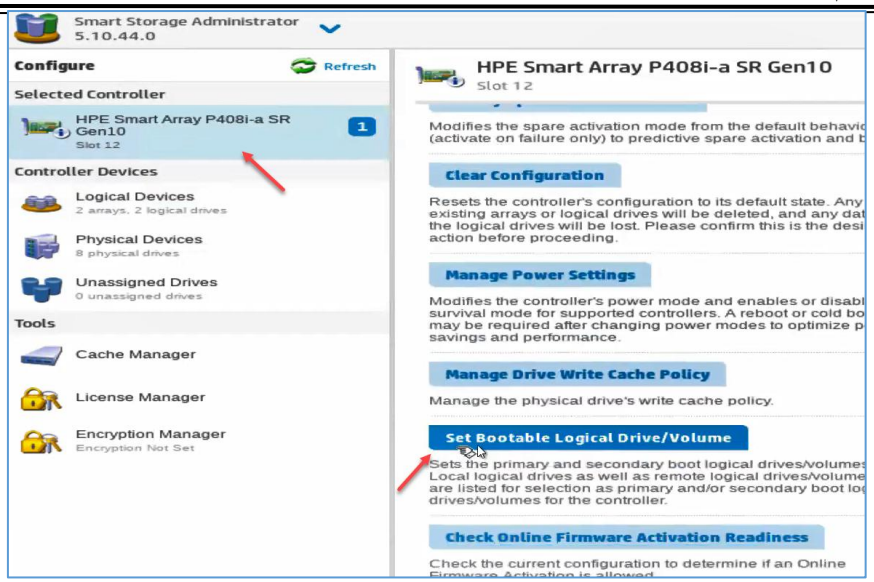
همان‌طور که در شکل ٦-۷۳، مشاهده می‌کنید دو Array ایجاد شده است که یکی با RAID1 و دیگری با RAID5 است.



شکل ۶- ۷۳ Create Array

بعد از اتمام کار شما باید مشخص کنید که کدام درایو برای Boot شدن در اولویت قرار بگیرد، برای این کار به مانند شکل ٦-۷٤، بر روی HPE Smart Array P408i کلیک کنید و صفحه را اسکرول و گزینه‌ی Set Bootable Logical Drive را انتخاب کنید.

www.takbook.com



شکل ۶- ۷۴ *Create Array*

در شکل ٦-۷۵، Logical Drive 1 را که همان دو هاردی است که روی آن RAID1 راه‌اندازی کردیم را انتخاب کنید و بر روی OK کلیک کنید و در صفحه‌ی بعد بر روی Finish کلیک کنید.



شکل ۶- ۷۵ *Create Array*

حالا همه چیز برای نصب ESXi آماده است که در مبحث بعدی آن را بررسی خواهیم کرد.

٤-٤-١-٦ نصب و راه‌اندازی ESXi

برای اینکه این آموزش به صورت جامع انجام شود ما نصب ESXi را بر روی یک سرور HP انجام می‌دهیم که در قسمت قبلی نحوه‌ی Raidبندی آن را به طور کامل بررسی کردیم، البته برای آشنایی بیشتر شما عزیزان، بر روی VMware Workstation هم می‌توانید نصب کنید.

www.takbook.com

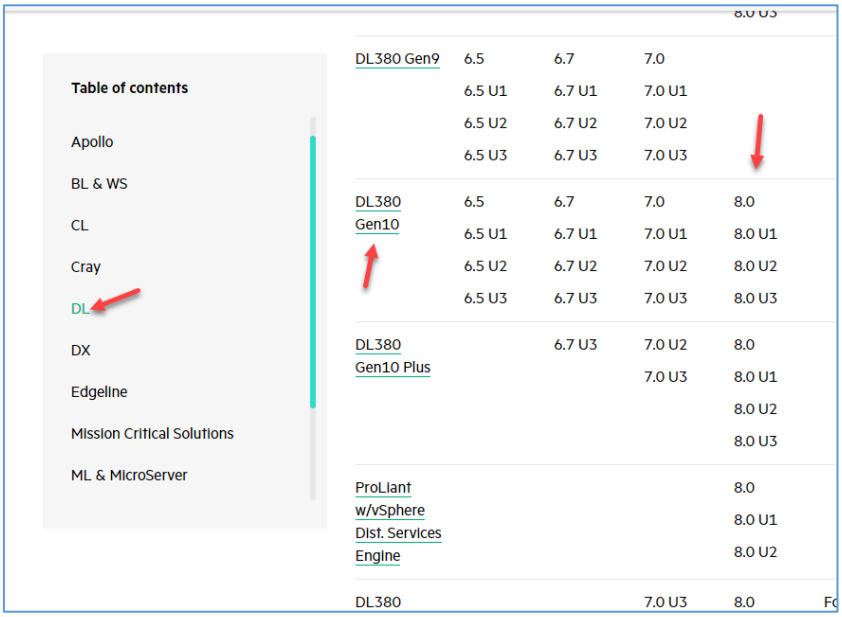
شرکت VMware برای نصب سیستم‌عامل ESXi بر روی سخت‌افزارهای مختلف ورژن‌های مختلفی از آن را ارائه داده که با هم در زیر بررسی می‌کنیم.

برای نصب ESXi بر روی سرورهای HP بهتر است که وارد سایت HP شویم و ورژن دقیق آن را مشخص کنیم، برای ورود از آدرس زیر استفاده کنید.

https://www.hpe.com/us/en/collaterals/collateral.a50010842enw.html

همان‌طور که در شکل ٦-٧٦، مشاهده می‌کنید باید مدل سرور HP خود را جستجو کنید که برای ما DL380 Gen10 است، دقیقاً در جلوی آن مشخص کرده است که پایینترین ورژن ESXi که بر روی این سرور نصب می‌شود ورژن 6.5 است و بالاترین ورژن آن هم 8.0 U3 است.

پس حتماً باید ورژنی که نیاز دارید را از سایت مورد نظر انتخاب و بر روی سرور نصب کنید، اگر ورژن برابر نباشد خطاهایی هنگام نصب به شما می‌دهد که اذیت کننده خواهد بود.



شکل ۶- ۷۶ ورژن ESXi

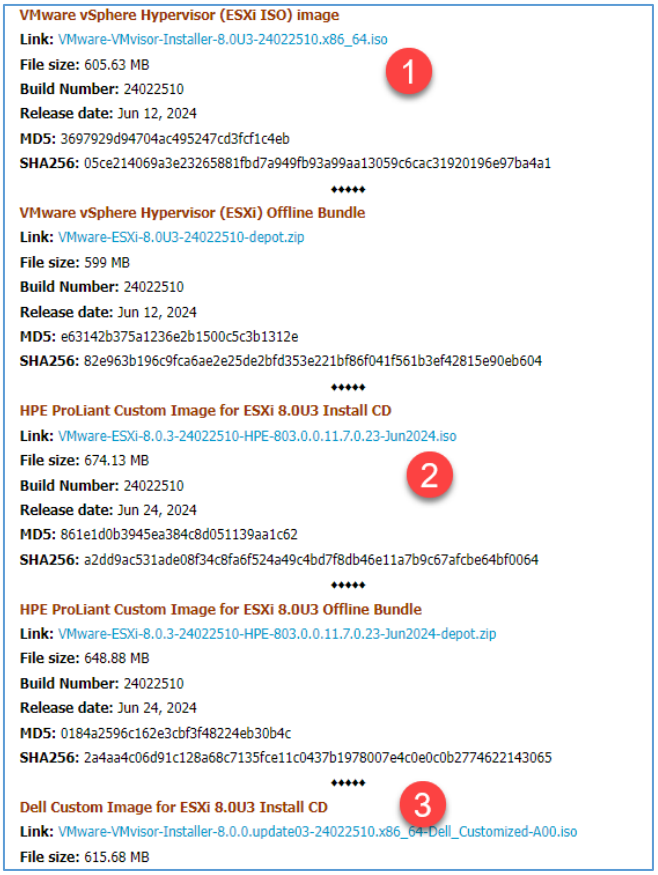
پس برای سرور HP G10 خود ESXi ورژن 8.0 U3 را انتخاب و دانلود می‌کنیم، البته برای دانلود باید وارد سایت VMware یا سایت ایرانی Digiboy.ir شوید که لینک آن را در زیر قرار می‌دهیم.

https://www.digiboy.ir/12364/vmware-vsphere-80u3/

www.takbook.com

اگر به شکل ٦-٧٧، توجه کنید، ورژن‌های مختلفی برای شما به نمایش گذاشته شده، ورژن شماره‌ی یک مربوط به کلاینت‌های خانگی و ماشین‌های مجازی است که می‌خواهید توسط نرم‌افزار VMware Workstation ایجاد کنید، در قسمت شماره‌ی دو ورژن مربوط به HP را مشاهده می‌کنید که برای HP از نام HP Proliant Custom استفاده می‌شود و در قسمت شماره‌ی سه هم ورژن مربوط به سرور Dell را مشاهده می‌کنید.

ورژن مورد نظر را دانلود کنید تا نصب آن را انجام دهیم.



شکل ۶- ۷۷ ورژن ESXi

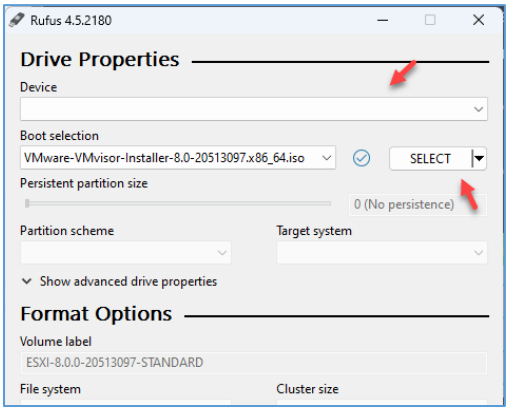
خوب تا به این مرحله ESXi را بررسی کردیم و ورژن مناسب سرور خود را انتخاب و دانلود کردیم.

برای اینکه ESXi را بر روی سرور یا هر سیستمی نصب کنید باید آن را Bootable کنید، برای این کار از نرم‌افزار Rufus استفاده کنید، برای دانلود آن می‌توانید از لینک زیر استفاده کنید.

https://rufus.ie/en/

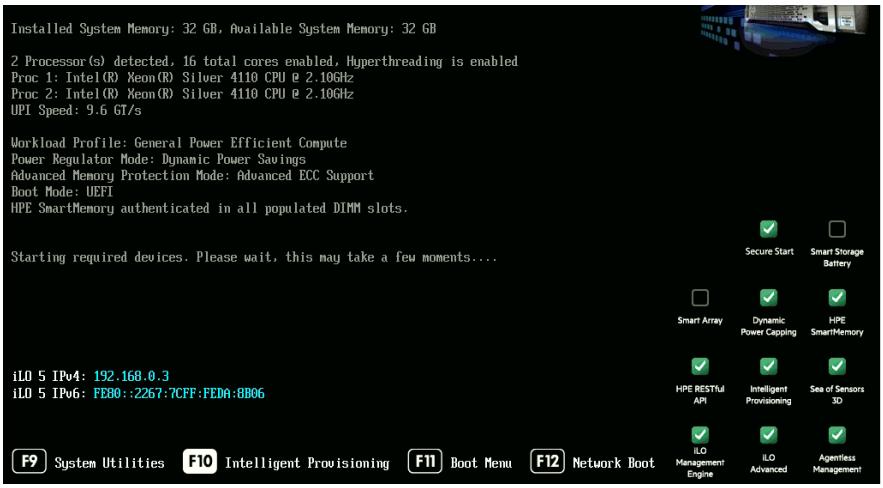
www.takbook.com

بعد از دانلود به مانند شکل ٦-٧٨، باید فلش خود را به سیستم متصل کنید، و بعد بر روی Select کلیک کنید و در آخر بر روی Start کلیک کنید تا فایل Image بر روی فلش در حالت بوت قرار بگیرد.



شکل ۶- ۷۸ نرم‌افزار *Rufus*

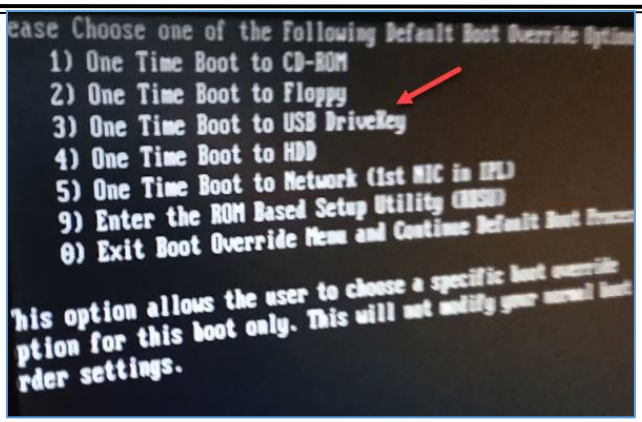
بعد از اینکه فلش را آماده کردید باید آن را به سرور HP متصل کنید و سرور را روشن کنید، به صورت پیش‌فرض فلش مورد نظر بوت خواهد شد و ESXi اجرا می‌شود، اگر چنانچه اجرا نشد باید کلید F11 را به مانند شکل ٦-٧٩، فشار دهید.



شکل ۶- ۷۹ورود به *Boot*

در ادامه کار و در صفحه‌ی شکل ٦-٨٠، باید گزینه‌ی سوم را انتخاب کنید تا فلش بوت شود.

www.takbook.com



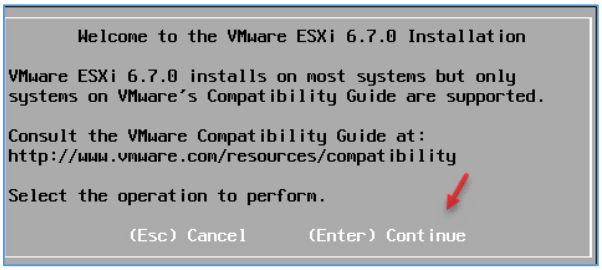
شکل ۶- ۸۰ انتخاب دستگاه Boot

بعد از بوت شدن شکل ٦-٨١، ظاهر می‌شود و فایل ESXi اجرا و برای نصب آماده می‌شود.



شکل ۶- ۸۱ اجرای فایل ESXi

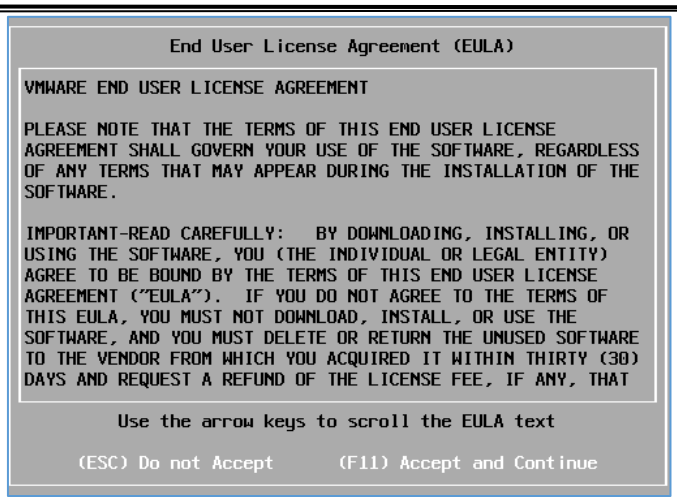
اولین صفحه‌ای که برای نصب ظاهر می‌شود به صورت شکل ٦-٨٢، است که برای ادامه باید بر روی Enter فشار دهید، توجه داشته باشید به خاطر کیفیت عکس‌ها از VMware برای نصب ESXi استفاده کردیم و نصب آن در سرور HP هم دقیقاً به همین صورت است.



شکل ۶- ۸۲ نصب ESXi

در شکل٦-٨٣، قراردادنامه استفاده از نرم‌افزار را مطالعه و در صورت تایید بر روی کلید F11 فشار دهید.

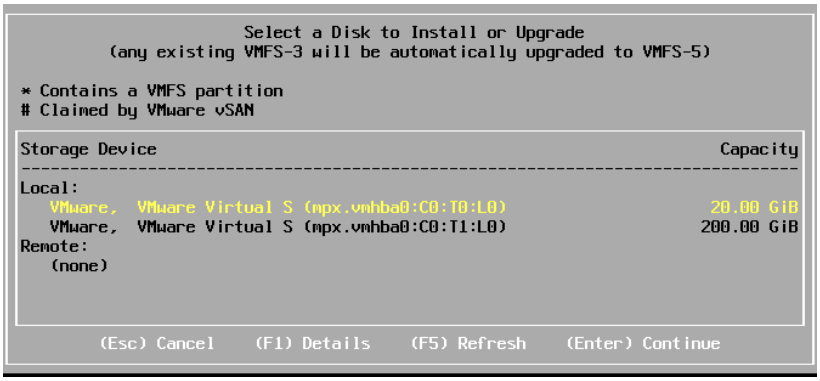
www.takbook.com



شکل ۶- ۸۳ نصب *ESXi*

در شکل ٦-٨٤، باید هارد دیسک مورد نظر را برای نصب انتخاب کنید، البته این نوع هارد دیسک از نوع مجازی و برای VMware می‌باشد.

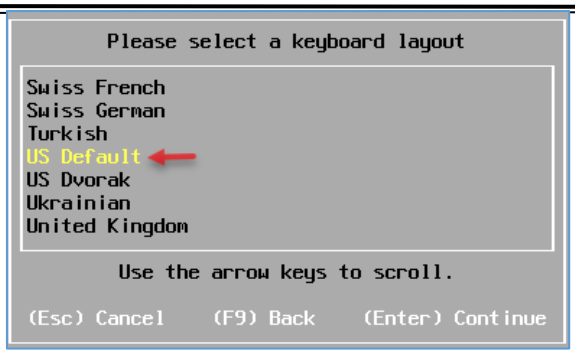
بر روی Enter فشار دهید.



شکل ۶- ۸۴ نصب *ESXi*

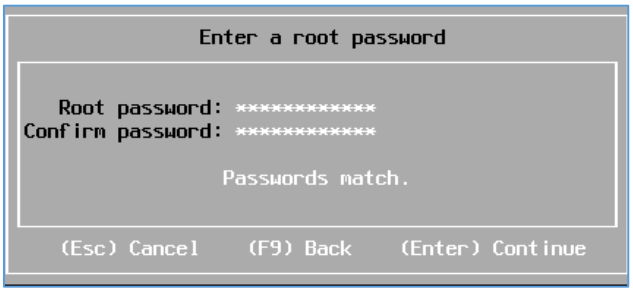
در شکل٦-٨٥ باید زبان کیبورد خود را مشخص کنید که به صورت پیش‌فرض زبان انگلیسی انتخاب شده است، بر روی Enter فشار دهید.

www.takbook.com



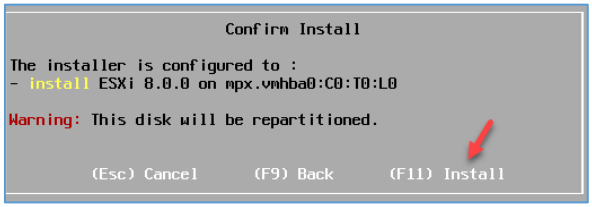
شکل ۶- ۸۵ نصب ESXi

در شکل ٦-٨٦، باید رمز عبور کاربر Root را وارد کنید که بهتر است رمز قدرتمند و پیچیده‌ای باشد. بر روی Enter فشار دهید، در صفحه بعد بر روی F11 فشار دهید تا کار نصب آغاز شود.



شکل ۶- ۸۶ نصب ESXi

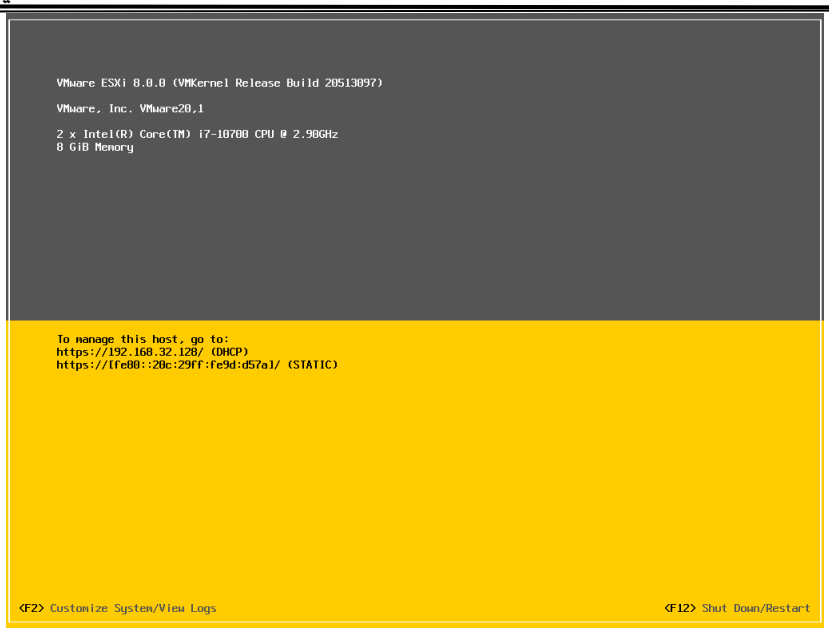
در شکل ٦-٨٧، بر روی F11 فشار دهید تا کار نصب آغاز شود.



شکل ۶- ۸۷ نصب ESXi

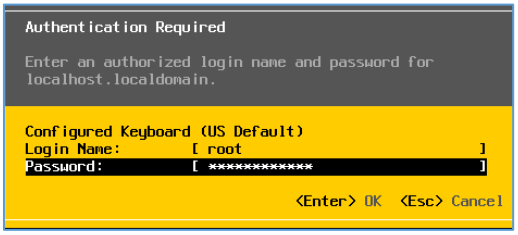
بعد از نصب و Reset شدن سرور، شکل ٦-٨٨، ظاهر می‌شود، در این قسمت ورژن ESXi که ۸ است مشخص شده است، مقدار رم و نوع CPU مشخص شده است و در وسط صفحه به آدرس IP که از طریق DHCP دریافت شده است مشخص است که البته باید آن را تغییر دهیم و برای این کار باید بر روی F2 فشار دهید.

www.takbook.com



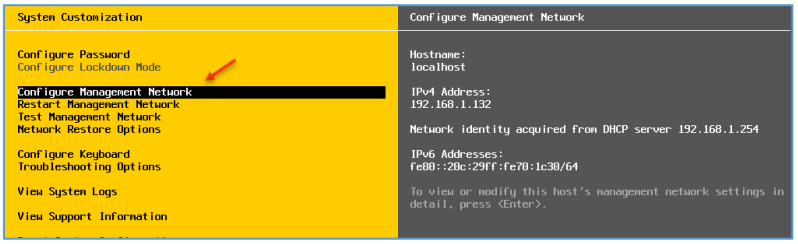
شکل ۶- ۸۸ نصب *ESXi*

در شکل ٦-۸۹، برای ورود به بخش تنظیمات باید رمز عبور کاربر Root را وارد کنید، توجه داشته باشید این رمز را در هنگام نصب وارد کردید.



شکل ۶- ۸۹ نصب *ESXi*

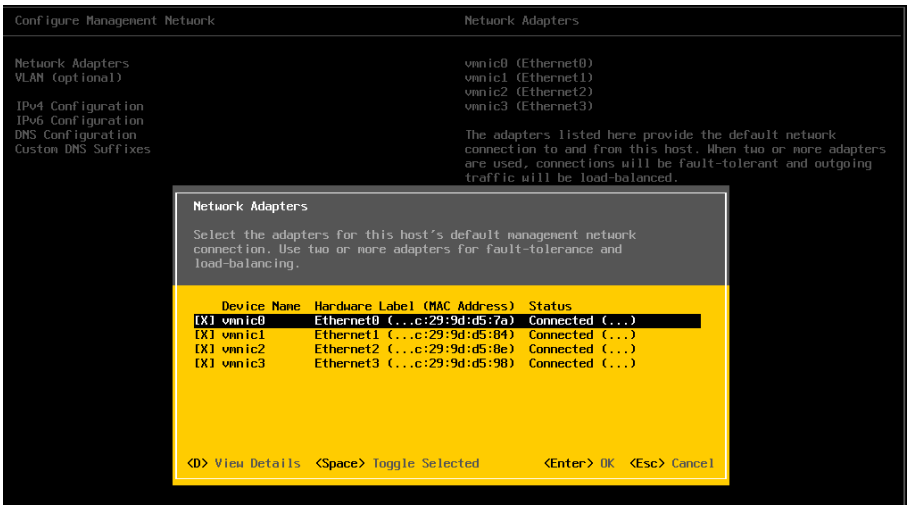
در شکل ٦-۹۰، گزینه‌ی Configure Management Network را انتخاب کنید تا کار تنظیم IP address را انجام دهیم.



شکل ۶- ۹۰ تنظیم کارت شبکه

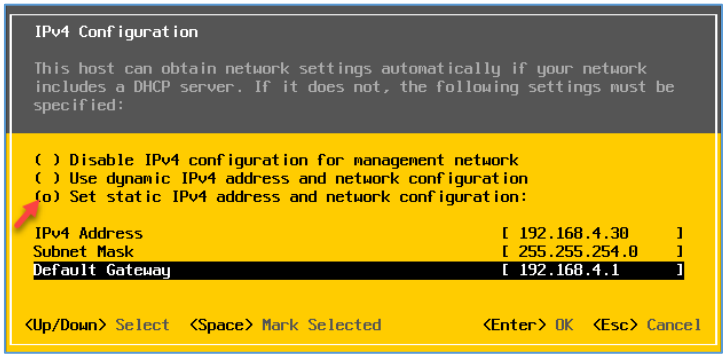
www.takbook.com

همان‌طور که از قبل بیان کردم، سرورها از چند کارت شبکه تشکیل شده‌اند، شما می‌توانید همه‌ی کارت شبکه‌های سرور را به عنوان کارت شبکه‌ی مدیریتی انتخاب کنید و اگر بر روی یکی از این کارت شبکه‌ها کابل شبکه متصل باشد صفحه‌ی مدیریتی به راحتی باز خواهد شد.



شکل ۶- ۹۱ تنظیم کارت شبکه

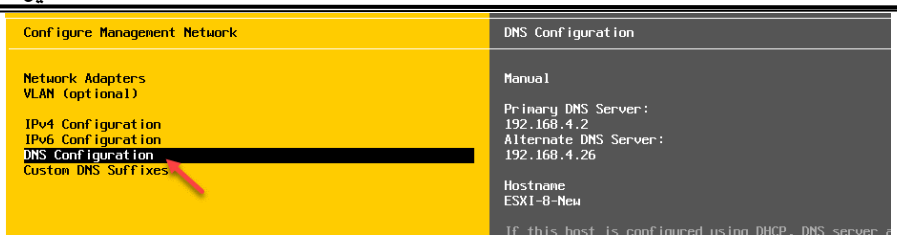
در شکل ٦-۹۲، اول گزینه‌ی...Set static IP address را با فشار دادن کلید Space انتخاب کنید و بعد، آدرس IP خود را وارد و Enter کنید.



شکل ۶- ۹۲ تنظیم کارت شبکه

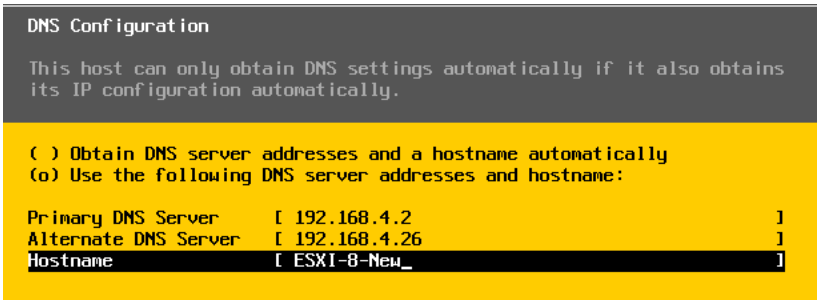
برای اینکه یک نام برای سرور ESXi خود در نظر بگیریم، وارد قسمت DNS Configuration شوید.

www.takbook.com



شکل ۶- ۹۳ تنظیم کارت شبکه

در دو قسمت اول آدرس سرورهای DNS خود را وارد کنید و در قسمت Hostname باید یک نام برای سرور خود وارد کنید و بعد بر روی Enter فشار دهید، در مورد سرویس DNS در فصل MCSE توضیحات کامل را بیان کردیم.



شکل ۶- ۹۴ تنظیم کارت شبکه

نکته مهم: برای اینکه از قابلیت DNS و اسم سرور استفاده کنید باید در سرویس DNS اصلی خود که در شبکه فعال است این نام را اضافه کنید، یعنی یک A record جدید اضافه کنید تا بتوانید از طریق نام به آن دسترسی داشته باشید.

گزینه‌های دیگری هم در صفحه تنظیمات ESXi وجود دارد، به مانند شکل ٦-٩٥، اگر بخواهید تنظیمات کارت شبکه را Reset کنید باید گزینه‌ی Restart Management Network را انتخاب کنید و یا اگر می‌خواهید Logها سرور را بررسی کنید باید گزینه‌ی View system Logs را انتخاب کنید.



شکل ۶- ۹۵ تنظیم کارت شبکه

www.takbook.com

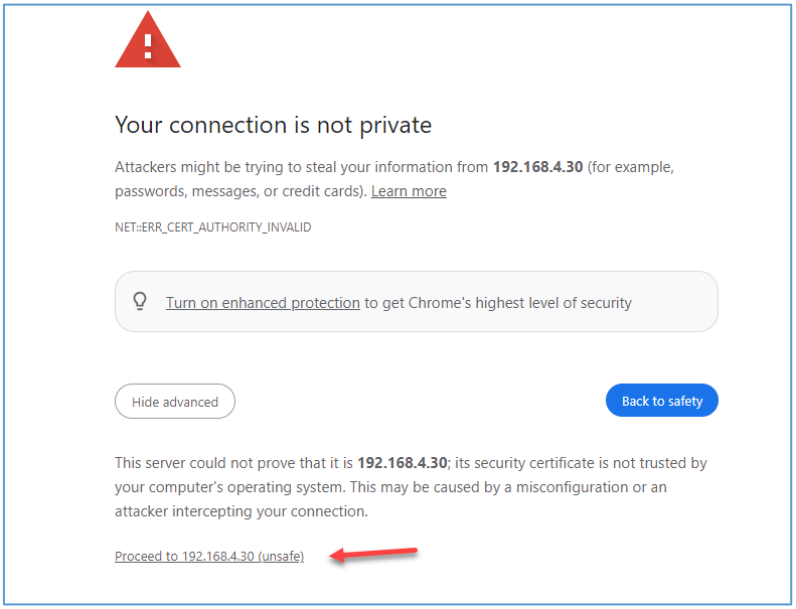
بعد از این کار، چند بار بر روی ESC فشار دهید تا به صفحه‌ی اول برگردید، بعد بر روی F12 فشار دهید و رمز عبور را دوباره وارد کنید و بعد بر روی F11 کلیک کنید تا سرور Restart شود.

نکته: در شبکه واقعی همیشه باید سرور ESXi را بر روی یک سرور فیزیکی نصب کنید و از آن استفاده کنید، و استفاده از ماشین مجازی برای این کار در شبکه واقعی کار اشتباهی است.

۵-۱-٤-٦ تنظیمات سرور ESXi

برای اینکه بتوانید سیستم عامل ESXi را تنظیم کنیم و در آن ماشین مجازی ایجاد کنیم باید به آن دسترسی پیدا کنیم که روش‌های دسترسی کاملاً تغییر کرده است.

در ورژن های قدیمی ESXi برای دسترسی به آن باید از نرم‌افزار VMware Vsphere Client استفاده می‌کردید ولی در ورژن‌های جدید دیگر نرم‌افزار کلاینتی برای آن ارئه نشده و دسترسی به آن فقط از طریق Web امکان‌پذیر است.

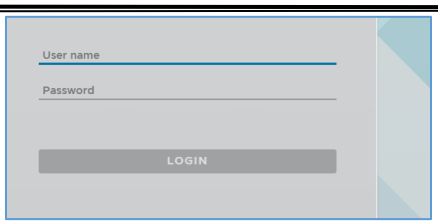


شکل ۶- ۹۶ ورود به ESXi

برای ورود به صفحه ESXi باید آدرس IP آن را در قسمت address bar وارد کنید، البته چون بر روی پروتکل HTTPs قرار دارد با خطای نامعتبر گواهینامه روبرو خواهید شد که آن را نادیده گرفته و ادامه دهید تا شکل زیر ظاهر شود.

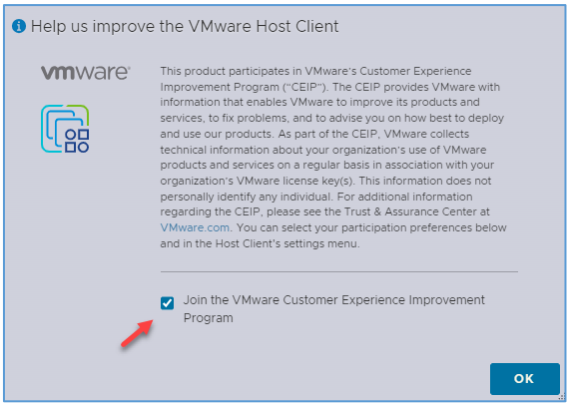
در قسمت مورد نظر باید نام کاربری root و رمز عبوری که در هنگام نصب وارد کردید را در این قسمت وارد کنید و بر روی Login کلیک کنید.

www.takbook.com



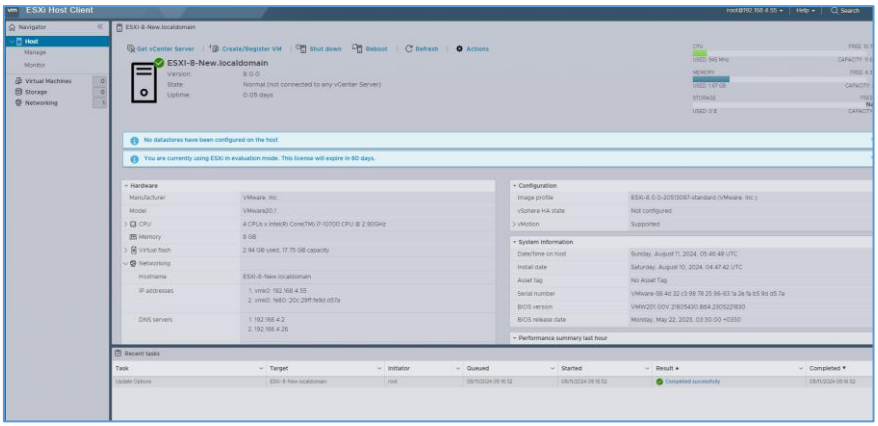
شکل ۶- ۹۷ ورود به ESXi

بعد از ورود اولین پنجره‌ای که مشاهده خواهید کرد به صورت شکل ٦-۹۸ می‌باشد، در این پیام از شما درخواست می‌شود اگر مایل بودید می‌توانید از شرکت VMware برای بهبود نرم‌افزارکمک بگیرید، در هر صورت بر روی OK کلیک کنید.



شکل ۶- ۹۸ ورود به ESXi

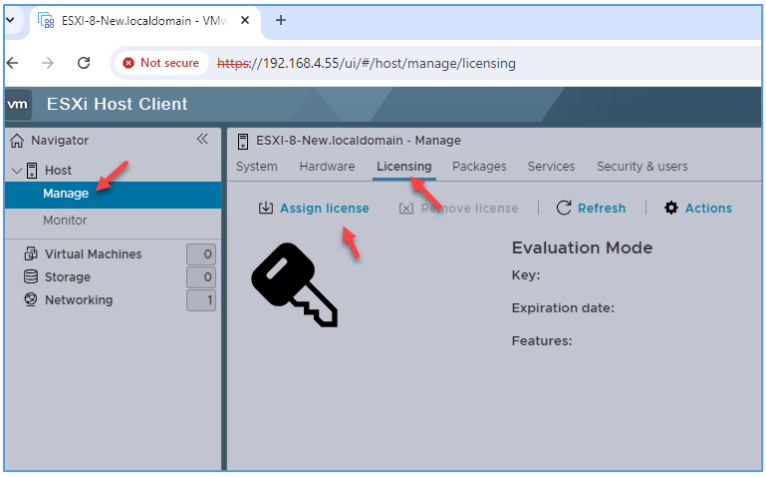
در شکل ٦-۹۹، نمای کلی از سیستم‌عامل ESXi را مشاهده می‌کنید.



شکل ۶- ۹۹ صفحه‌ی اصلی ESXi

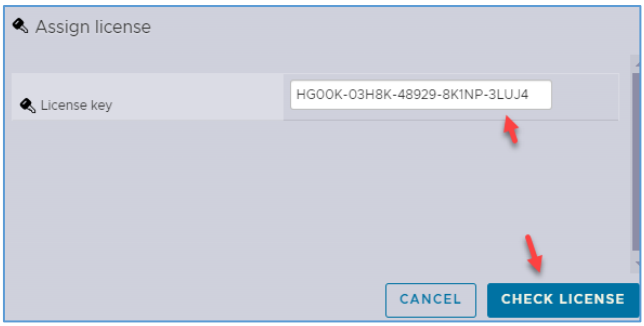
www.takbook.com

اولین کاری که باید در ESXi انجام دهید این است که لایسنس آن را وارد کنید که برای این کار از سمت چپ به مانند شکل ٦-١٠٠، بر روی Manage کلیک کنید و وارد تب Licensing شوید و بر روی Assign license کلیک کنید.



شکل ۶- ۱۰۰ لایسنس ESXi

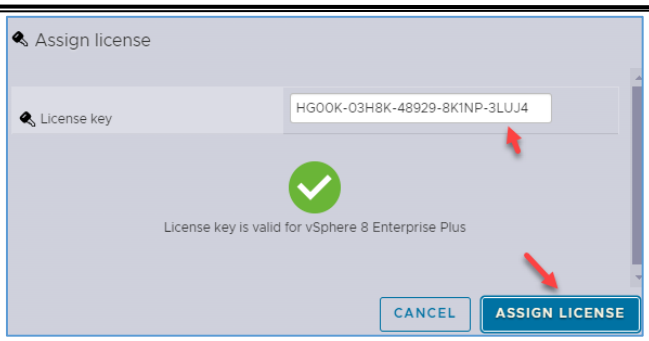
در شکل ٦-١٠١، لایسنس مورد نظر را وارد و بر روی Check license کلیک کنید.



شکل ۶- ۱۰۱ لایسنس ESXi

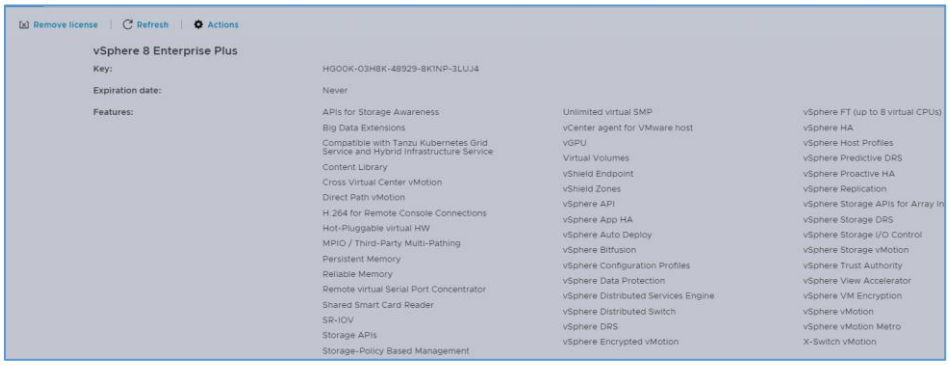
همان‌طور که در شکل ٦-١٠٢، مشاهده می‌کنید سریال مورد نظر برای VMware vSphere 8 Enterprise مورد تایید است یعنی تا این سطح دسترسی لازم را دارد، بر روی Assign license کلیک کنید.

www.takbook.com



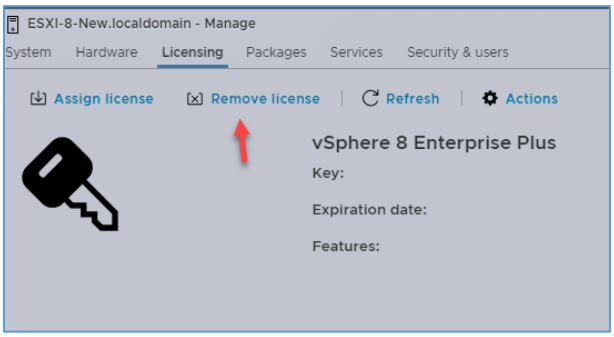
شکل ۶- ۱۰۲ لایسنس ESXi

در شکل ٦-۱۰۳، Featureهایی که برای این سریال و لایسنس در نظر گرفته شده است مشخص است، یعنی با این لایسنس ESXi می‌تواند به این منابع دسترسی پیدا کند.



شکل ۶- ۱۰۳ لایسنس ESXi

اگر با لاینس مورد نظر به مشکل خوردید می‌توانید در شکل ٦-۱۰٤، بر روی Remove license کلیک کنید و دوباره لایسنس جدید را Add کنید.

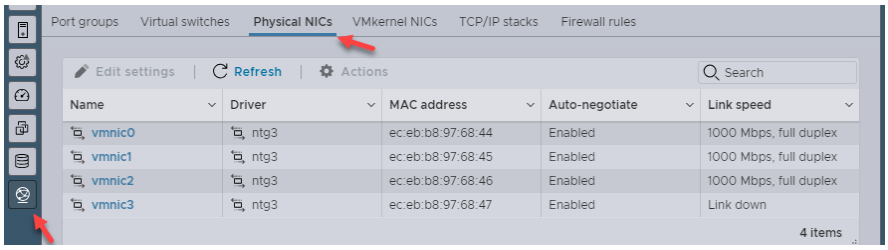


شکل ۶- ۱۰۴ لایسنس ESXi

www.takbook.com

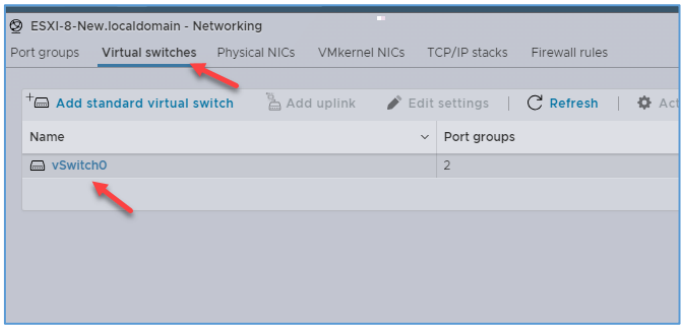
۶-۱-۴-۶ بررسی شبکه در سرور ESXi

در این قسمت می‌خواهیم به طور کامل شبکه ESXi را با هم بررسی کنیم، همان‌طور که قبلاً گفتیم سرورهای HP دارای ٤ پورت کارت شبکه هستند که از آنها می‌توانید برای ارتباط ماشین مجازی خود استفاده کنید، به مانند شکل ۶-۱۰۵، اگر از سمت چپ بر روی Networking و بعد بر روی تب Physical NICS کلیک کنید، لیست چهار کارت شبکه را مشاهده می‌کنید، در این قسمت نام Driver، آدرس MAC و سرعت کارت را مشاهده می‌کنید.



شکل ۶- ۱۰۵ بررسی شبکه در ESXi

در ادامه به مانند شکل ۶-۱۰۶، وارد تب Virtual Switches شوید، در این قسمت یک سوئیچ مجازی با عنوان vSwitch0 وجود دارد که برای بررسی بیشتر بر روی آن کلیک کنید.

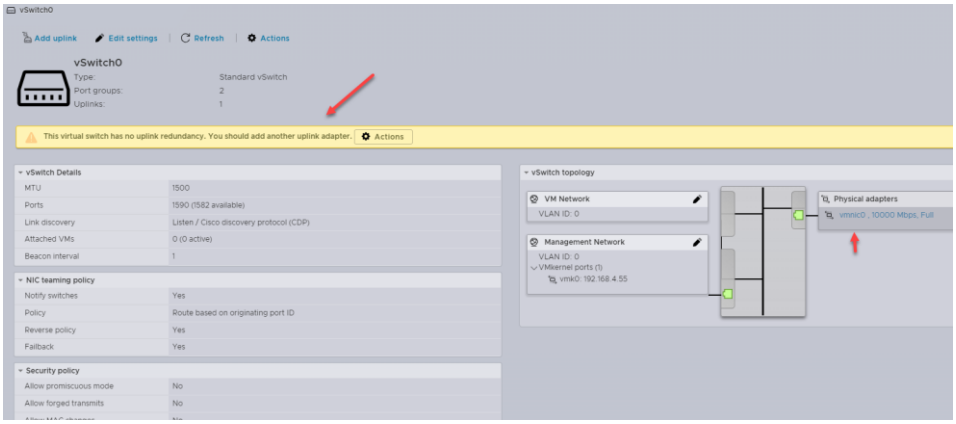


شکل ۶- ۱۰۶ بررسی شبکه در ESXi

به مانند شکل ۶-۱۰۷، در سوئیچ vSwitch0 تنظیمات مشخص شده است، اگر به سمت راست در قسمت vSwitch topology توجه کنید یک کارت شبکه با نام vmnic0 قرار دارد که به این معنی است که این سوئیچ از طریق کارت vmnic0 به شبکه متصل شده است، توجه داشته باشید قسمت Management هم از طریق این کارت با ما در ارتباط است. اگر به صفحه توجه کنید یک پیغام زرد رنگ با عنوان (This virtual switch has no uplink redundancy. You should add another uplink adapter) مشخص شده است که به این موضوع اشاره دارد که این سوئیچ تنها با یک کارت شبکه در حال کار است و برای اینکه Redundancy یا همان

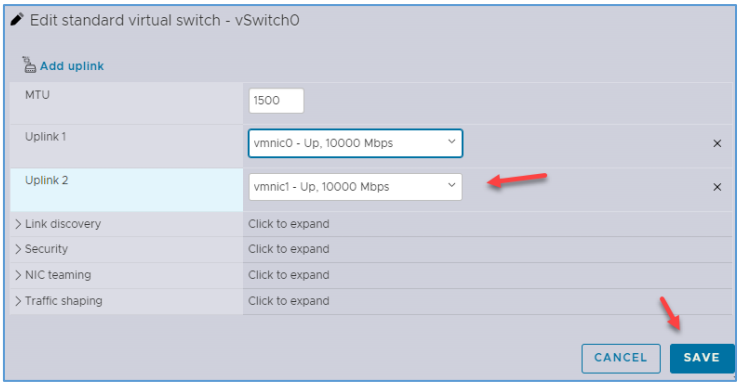
www.takbook.com

قابلیت اطمینان را افزایش دهید باید کارت شبکه دیگری را هم به این سوئیچ اضافه کنید که برای این کار در بالای صفحه بر روی Add Uplink کلیک کنید.



شکل ۶- ۱۰۷ بررسی شبکه در ESXi

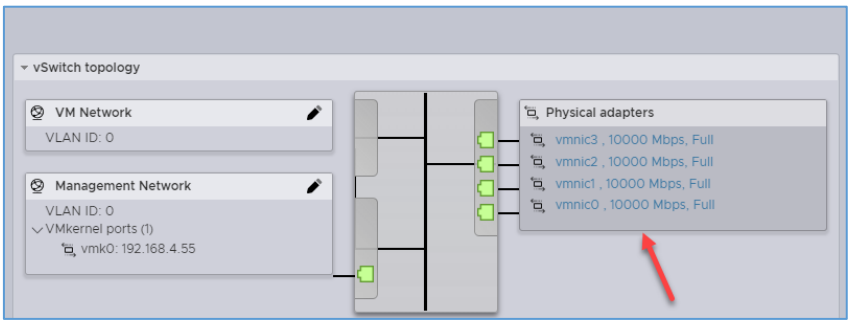
در شکل۶-۱۰۸، با هر کلیک بر روی Add Uplink می‌توانید یک کارت شبکه به لیست اضافه کنید که همان‌طور که مشخص است دو کارت شبکه به لیست اضافه شده است، با این کار اگر یک کارت شبکه از کار بیفتد یک کارت شبکه دیگر آنلاین هست و به کار خود ادامه می‌دهد و ارتباط با سرور به هیچ عنوان قطع نخواهد شد، در ادامه نحوه ارتباط ماشین مجازی با سوئیچ را شرح خواهیم داد.



شکل ۶- ۱۰۸ بررسی شبکه در ESXi

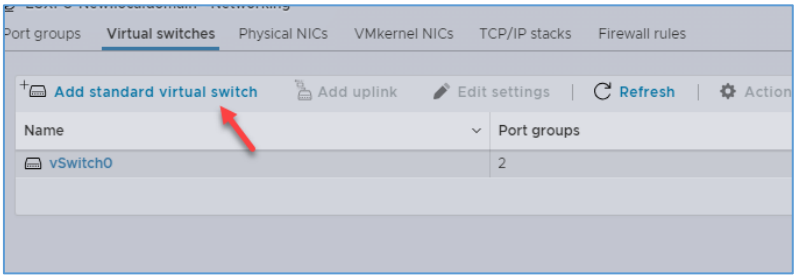
در شکل ۶-۱۰۹، هر چهار کارت شبکه به سوئیچ مورد نظر متصل شده است، توجه داشته باشید که شماره‌ی VLAN به صورت پیش‌فرض صفر در نظر گرفته شده است که در صورت که شبکه شما در VLAN خاصی قرار دارد آن را تغییر دهید.

www.takbook.com



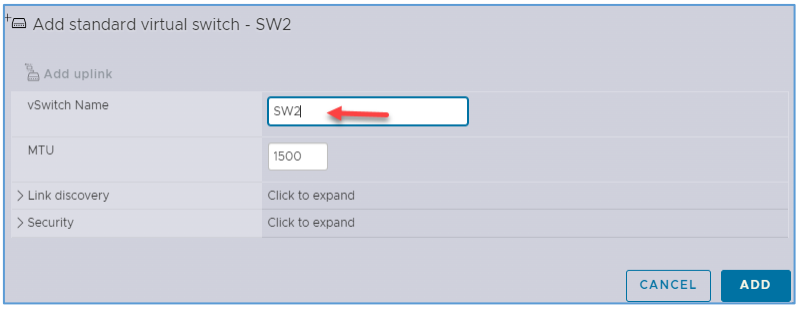
شکل ۶- ۱۰۹ بررسی شبکه در ESXi

برای اینکه یک سوئیچ مجازی جدید ایجاد کنید باید به مانند شکل ٦-۱۱۰، بر روی Add Standard Virtual switch کلیک کنید.



شکل ۶- ۱۱۰ بررسی شبکه در ESXi

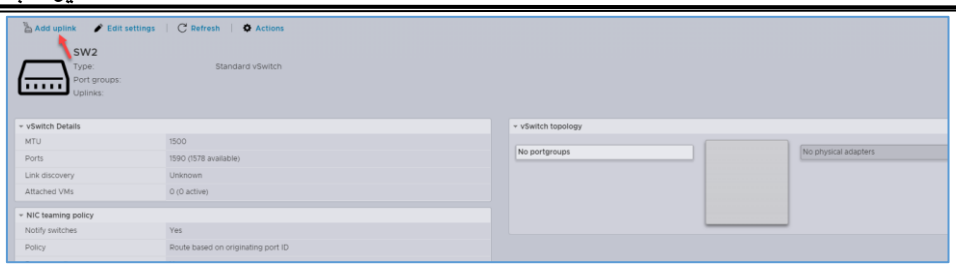
در شکل ٦-۱۱۱، نام سوئیچ خود را وارد و بر روی Add کلیک کنید، گزینه‌های دیگری برای امنیت و نوع پروتکل جستجو مانند CDP وجود دارد که در صورت نیاز آن را هم بررسی خواهیم کرد.



شکل ۶- ۱۱۱ بررسی شبکه در ESXi

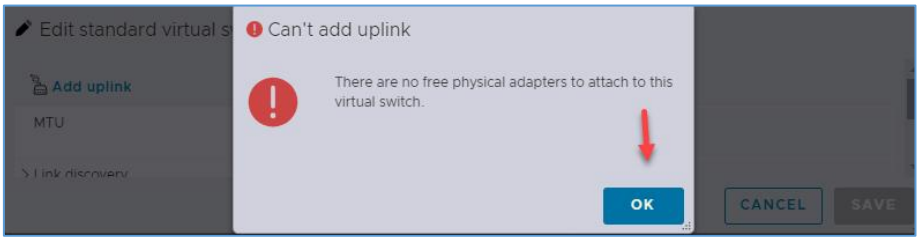
بعد از ایجاد اگر وارد سوئیچ SW2 شوید به مانند شکل ٦-۱۱۲، هیچ کارت شبکه‌ای به آن اختصاص داده نشده که برای این کار باید بر روی Add uplink کلیک کنید.

www.takbook.com



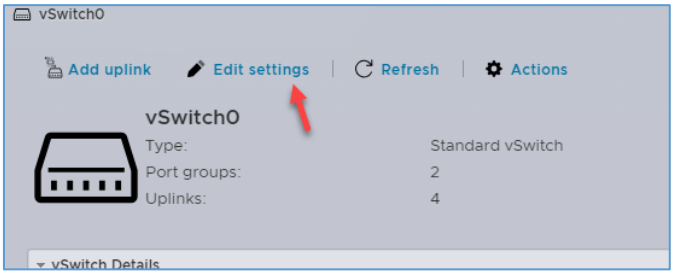
شکل ۶- ۱۱۲ بررسی شبکه در ESXi

بعد از کلیک بر روی Add با خطای شکل ٦-۱۱۳، مواجه خواهید شد که به این نکته اشاره دارد که کارت شبکه آزاد برای تخصیص دادن به این سوئیچ مجازی وجود ندارد و دلیل آن هم این است که تمام کارت شبکه‌ها را در قسمت قبلی به سوئیچ vSwitch0 تخصیص دادیم، برای آزاد کردن یک یا چند پورت باید وارد سوئیچ بشیم و پورت مورد نظر را حذف کنیم.



شکل ۶- ۱۱۳ بررسی شبکه در ESXi

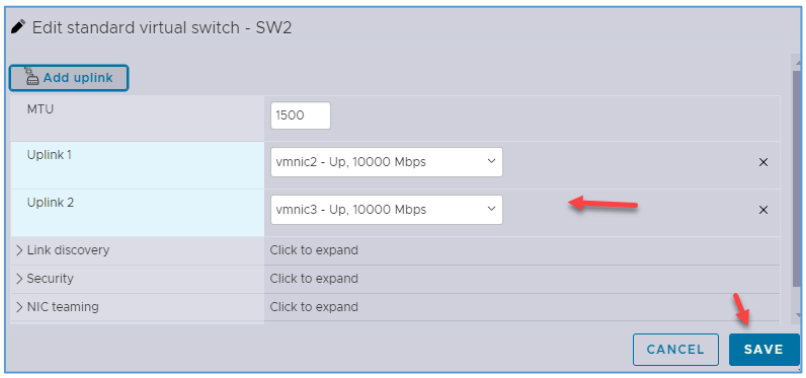
به مانند شکل ٦-۱۱٤،دوباره وارد vSwitch0 می‌شویم و بر روی Edit settings کلیک می‌کنیم و دو کارت شبکه موجود را حذف می‌کنیم.



شکل ۶- ۱۱۴ بررسی شبکه در ESXi

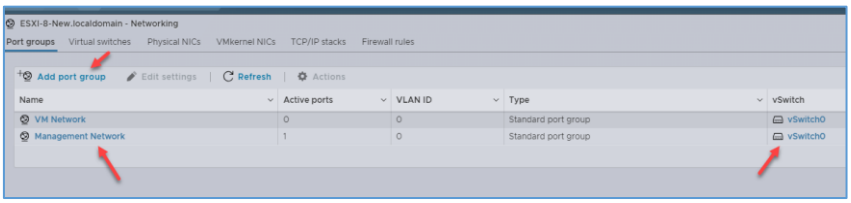
بعد از حذف کارت شبکه به مانند شکل ٦—۱۱۵، وارد سوئیچ SW2 می‌شویم و کارت شبکه‌های موجود را اضافه می‌کنیم.

www.takbook.com



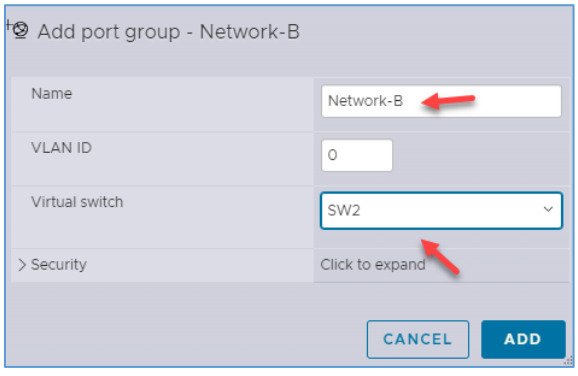
شکل ۶- ۱۱۵ بررسی شبکه در ESXi

به مانند شکل ٦-١١٦، در تب Port Group دو گروه پیش‌فرض را مشاهده می‌کنید که ماشین‌های مجازی که ایجاد می‌کنید برای ارتباط با شبکه باید به گروه VM Network متصل شوند، اگر به ستون vSwitch توجه کنید نام vSwitch0 برای آن انتخاب شده است، اگر بخواهید یک گروه جدید ایجاد کنید می‌توانید بر روی Add Port Group کلیک کنید.



شکل ۶- ۱۱۶ بررسی شبکه در ESXi

در شکل ٦-١١٧، نام گروه مورد نظر را وارد کنید و از قسمت Virtual switch می‌توانید سوئیچ مجازی جدید را انتخاب کنید.

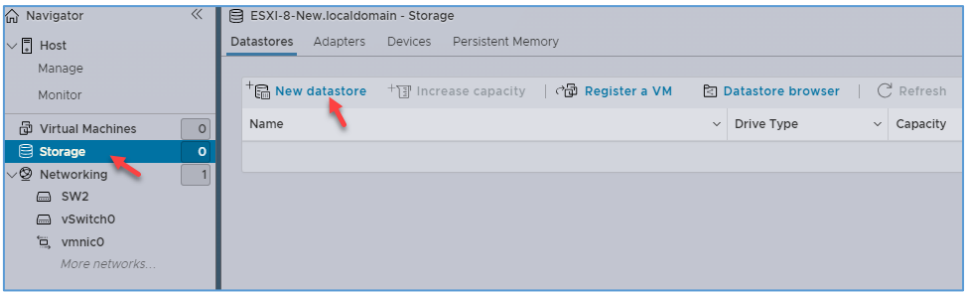


شکل ۶- ۱۱۷ بررسی شبکه در ESXi

www.takbook.com

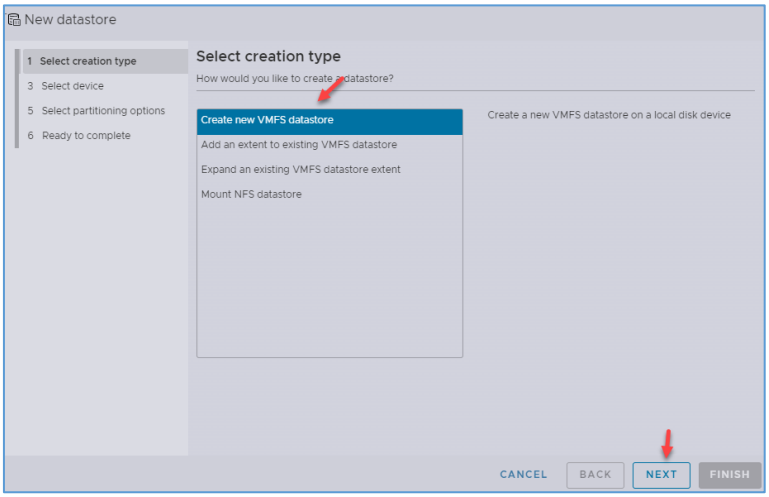
۷-٤-۱-٦ اضافه کردن هارد دیسک به سرور ESXi

همان‌طور که قبلاً گفتیم برای اضافه کردن هارد باید اول از همه هارد مورد نظر را Raid بندی کنیم که این موضوع را در قسمت‌های قبل انجام دادیم، بعد از انجام Raidبندی هارد دیسک در سرور، باید به مانند شکل ٦-۱۱۸، وارد Storage شوید و بر روی New datastore کلیک کنید.



شکل ۶- ۱۱۸ اضافه کردن هارد دیسک

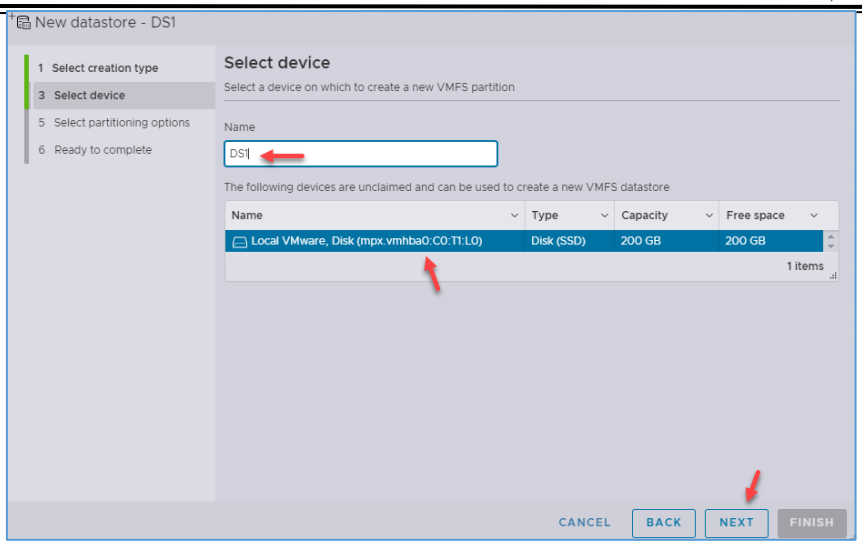
در شکل ٦-۱۱۹، چند گزینه را مشاهده می‌کنید که گزینه‌ی اول برای اضافه کردن هارد دیسک جدید، گزینه‌ی دوم و سوم برای اضافه کردن حجم هارد و گزینه‌ی آخر هم برای متصل شدن به سرور NFS است، در این قسمت گزینه‌ی اول را انتخاب و بر روی Next کلیک کنید.



شکل ۶- ۱۱۹ اضافه کردن هارد دیسک

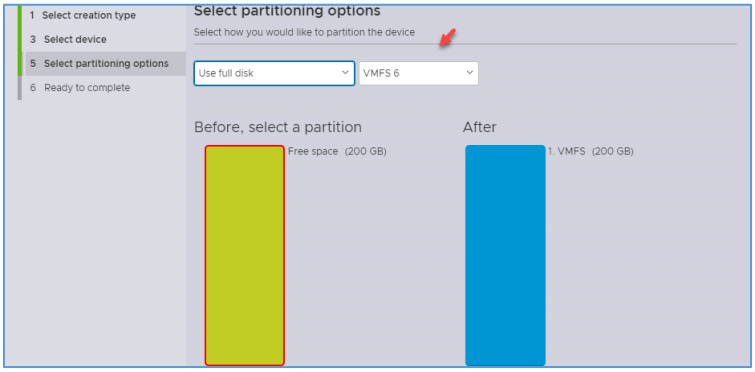
در شکل ٦-۱۲۰، نام دلخواه خود را وارد کنید، در این لیست یک هارد دیسک را مشاهده می‌کنید، آن را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



شکل ۶- ۱۲۰ اضافه کردن هارد دیسک

در شکل ٦-۱۲۱، هارد دیسک مورد نظر تبدیل به پارتیشن VMFS خواهد شد که البته در قسمت اول می‌توانید با انتخاب گزینه‌ی Custom مقدار استفاده از هارد دیسک را مشخص کنید.

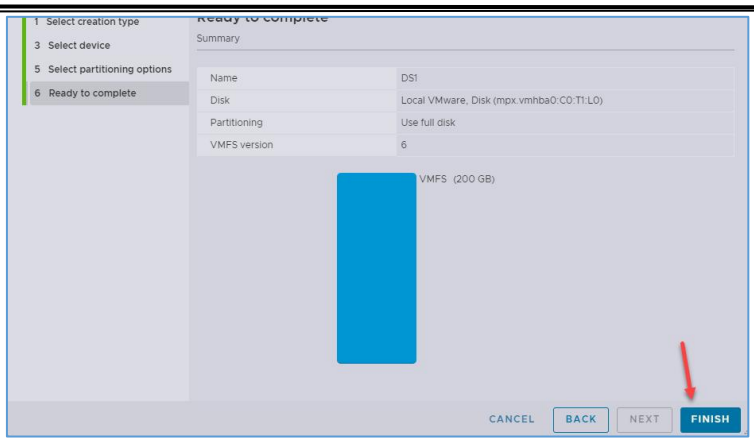


شکل ۶- ۱۲۱ اضافه کردن هارد دیسک

نکته: نوع پارتیشن VMFS6 در نظر گرفته شده که مختص شرکت VMware است و فقط بر روی ESXi 6.5 به بعد پاسخگو خواهد بود و اگر برای ESXi با ورژن دیگری بخواهید، باید ورژن آن را تغییر دهید، برای بررسی بهتر بحث VMFS اینجا را کلیک کنید.

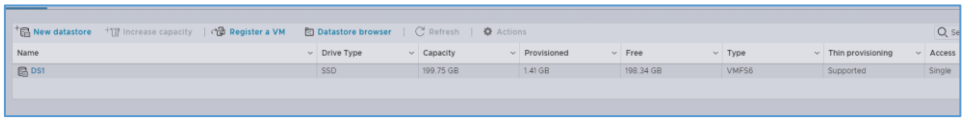
همان‌طور که در صفحهی ٦-۱۲۲، مشاهده می‌کنید که کل فضای هارد دیسک که حجمی بالغ بر ۲۰۰ گیگابایت است تبدیل به پارتیشن VMFS ورژن ٦ خواهد شد، بر روی Finish کلیک کنید.

www.takbook.com



شکل ۶- ۱۲۲ اضافه کردن هارد دیسک

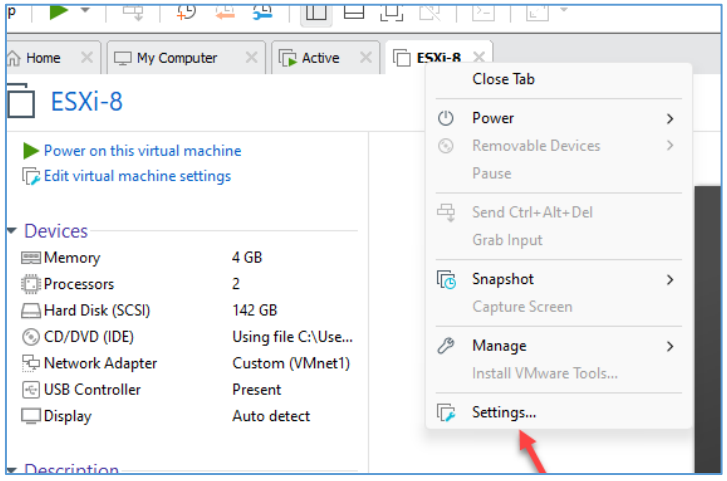
همان‌طور که در شکل ٦-۱۲۳، مشاهده می‌کنید، Data Store مورد نظر به لیست اضافه شده است و می‌توانید از آن استفاده کنید.



شکل ۶- ۱۲۳ اضافه کردن هارد دیسک

تنظیمات دیگری هم وجود دارد که در خلال کار آنها را بررسی خواهیم کرد.

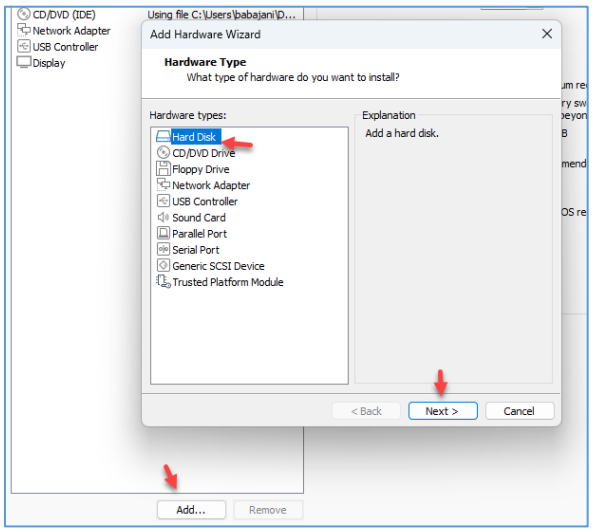
اما اگر بخواهیم در یک سرور مجازی که بر روی VMware Workstation نصب شده هارد اضافه کنیم باید به صورت شکل ٦-۱۲٤، وارد تنظیمات ماشین مورد نظر شویم.



شکل ۶- ۱۲۴ اضافه کردن هارد دیسک

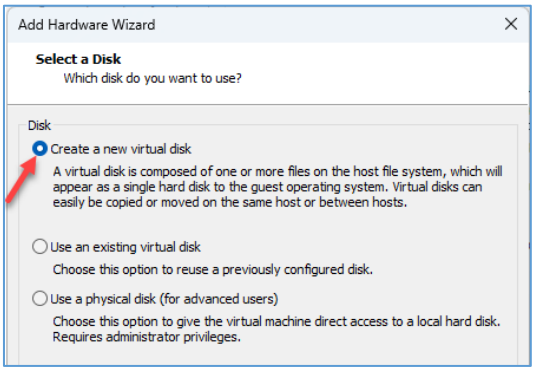
www.takbook.com

در شکل ٦-١٢٥، بر روی Add کلیک کنید و گزینه‌ی Hard Disk را انتخاب کنید.



شکل ۶- ۱۲۵ اضافه کردن هارد دیسک

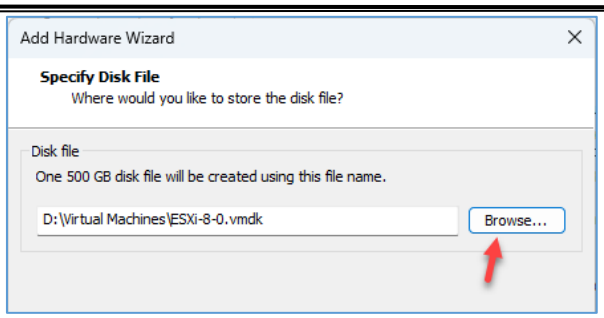
در ادامه کار به مانند شکل ٦-١٢٦ گزینه‌ی اول را برای ایجاد هارد دیسک مجازی جدید انتخاب کنید.



شکل ۶- ۱۲۶ اضافه کردن هارد دیسک

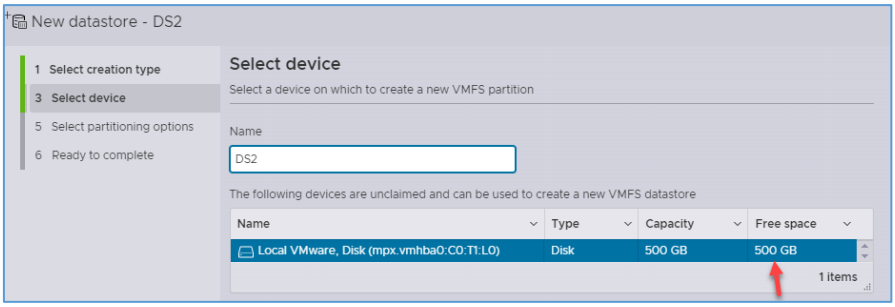
در شکل ٦-١٢٧، باید مسیر ذخیره شدن هارد دیسک را مشخص کنید.

www.takbook.com



شکل ۶- ۱۲۷ اضافه کردن هارد دیسک

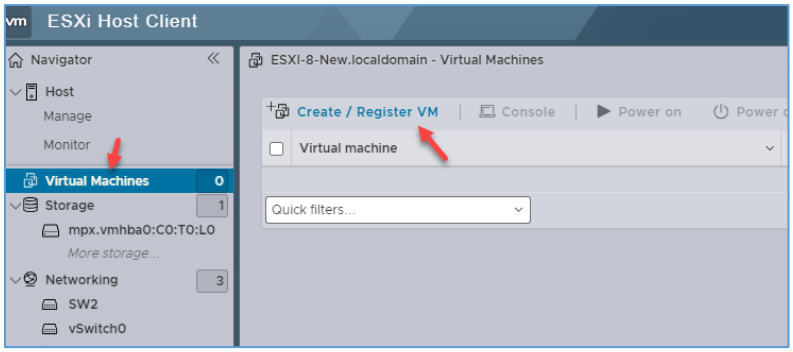
بعد از اینکه هارد را به سرور ESXi 8 معرفی کردید سرور را روشن کنید و تنظیمات اضافه کردن هارد دقیقاً به مانند قسمت قبل است و هارد را به لیست اضافه کنید که در شکل ٦-۱۲۸ این موضوع مشخص است.



شکل ۶- ۱۲۸ اضافه کردن هارد دیسک

٨-٤-١-٦ ایجاد ماشین مجازی در ESXi

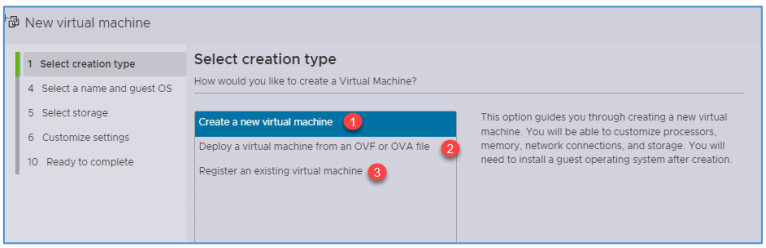
در این بخش می‌خواهیم در ESXi ماشین مجازی ایجاد و بر روی آن کار کنیم، به مانند شکل ٦-۱۲۹، از سمت چپ وارد Virtual Machines شوید و بر روی Create / Register VM کلیک کنید.



شکل ۶- ۱۲۹ ایجاد ماشین مجازی در ESXi

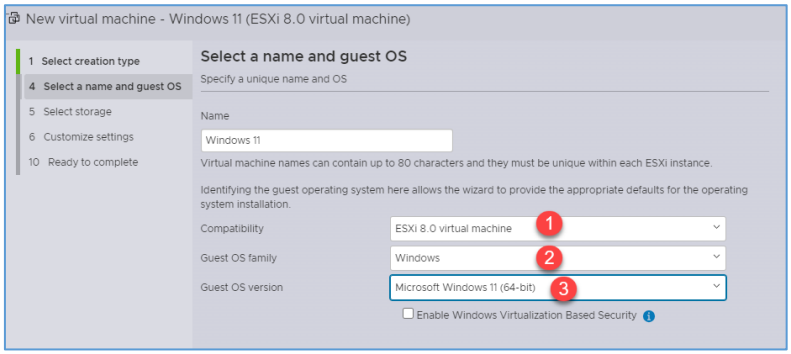
www.takbook.com

در شکل۶-۱۳۰، سه گزینه را مشاهده می‌کنید که گزینه‌ی اول برای ایجاد ماشین جدید، گزینه‌ی دوم برای ساخت فایل‌های OVF و OVA که در زمان مناسب آن را بررسی خواهیم کرد و گزینه‌ی سوم برای ایجاد ماشین مجازی که قبلاً در هارد دیسک وجود دارد استفاده می‌شود، در حال حاضر گزینه‌ی اول را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۶- ۱۳۰ ایجاد ماشین مجازی در ESXi

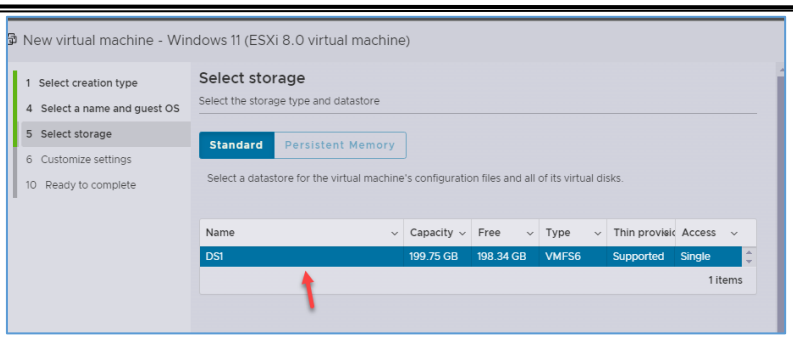
در شکل ۶-۱۳۱، نام ماشین مجازی خود را در قسمت Name وارد کنید، در قسمت شماره‌ی یک باید مشخص کنید که این ماشین مجازی با چه ورژنی از ESXi یا Workstation تعامل داشته باشد، توجه داشته باشید انتخاب ورژن‌های بالاتر باعث می‌شود این ماشین در ورژن‌های پائین‌تر ESXi یا Workstation با مشکل مواجه شود، در قسمت شماره‌ی دو نوع سیستم‌عامل را مشخص کنید و در قسمت شماره‌ی سه باید ورژن سیستم عامل را که در اینجا ویندوز ۱۱ است را انتخاب کنید، بر روی Next کلیک کنید.



شکل ۶- ۱۳۱ ایجاد ماشین مجازی در ESXi

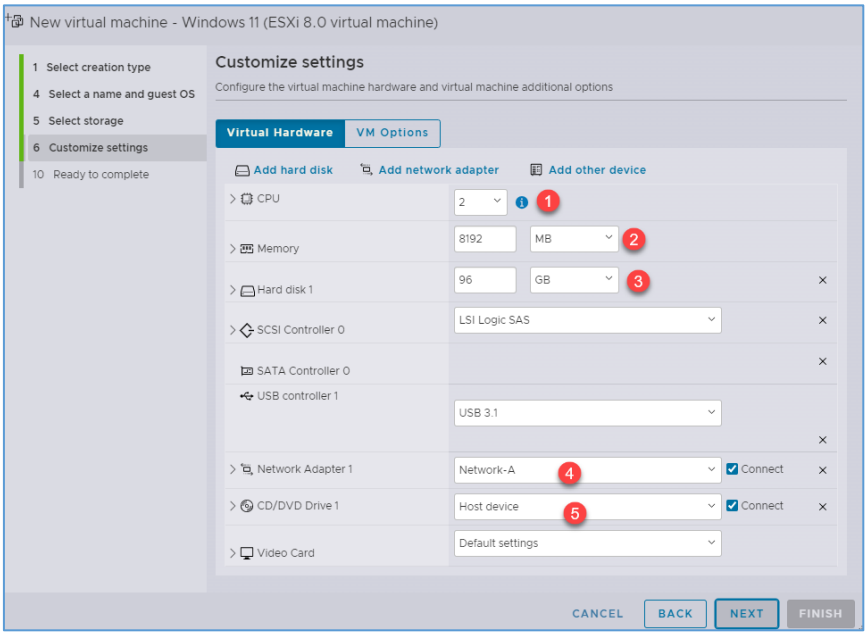
در شکل ۶-۱۳۲، باید هارد دیسک خود را که فضای مناسب برای ماشین شما داشته باشد را انتخاب کنید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۶- ۱۳۲ ایجاد ماشین مجازی در ESXi

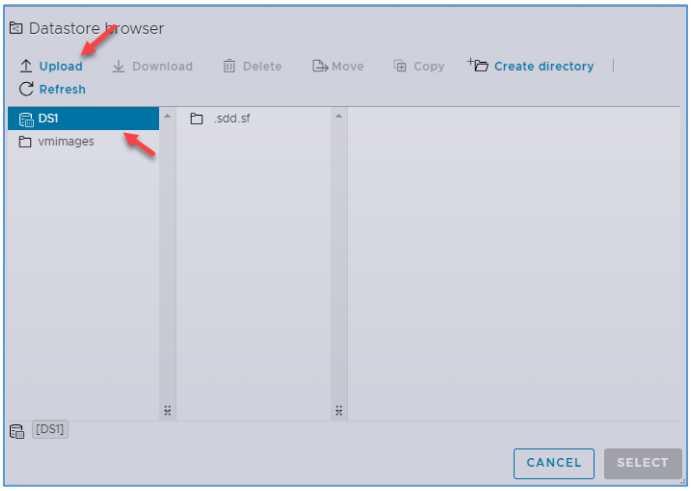
در شکل ٦-۱۳۳، باید سخت‌افزار ماشین مجازی را مشخص کنید، در قسمت شماره‌ی یک تعداد هسته CPU را مشخص کنید، در قسمت شماره‌ی دو مقدار رم آن را که بسته به نوع کارکرد ماشین دارد انتخاب کنید، در جلوی مقدار رم می‌توانید MB را به GB تغییر دهید و مقدار دلخواه را وارد کنید، در قسمت شماره‌ی سه باید مقدار فضای ماشین مجازی را مشخص کنید، که البته به صورت پیش‌فرض با انتخاب ویندوز ۱۱ مقدار ۹٦ گیگ به آن تخصیص داده شده است، در قسمت شماره‌ی چهار، کارت شبکه و در قسمت شماره‌ی پنج باید فایل سیستم‌عامل را به آن معرفی کنید که اگر بر روی سیستم‌خود از DVD/RW استفاده می‌کنید باید گزینه‌ی Host Device را انتخاب کنید و اگر هم از فایل ویندوز یک Image تهیه کردید گزینه‌ی Datastore ISO file را انتخاب کنید تا صفحه بعد ظاهر شود.



شکل ۶- ۱۳۳ ایجاد ماشین مجازی در ESXi

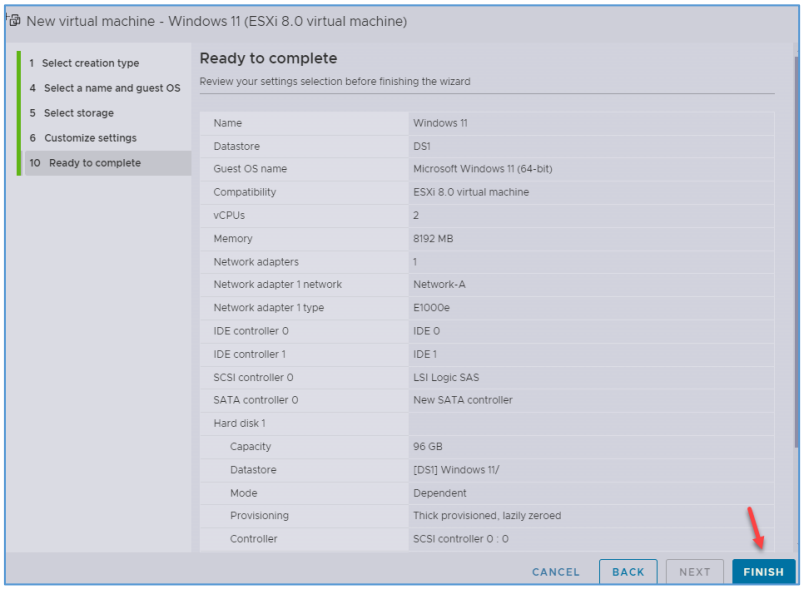
www.takbook.com

در شکل ٦-١٣٤، باید هارد دیسک مورد نظر خود را از سمت چپ انتخاب و بر روی Upload کلیک کنید و فایل Image مربوط به Windows 11 را در هارد آپلود کنید و بعد آن را انتخاب کنید.



شکل ۶- ۱۳۴ ایجاد ماشین مجازی در ESXi

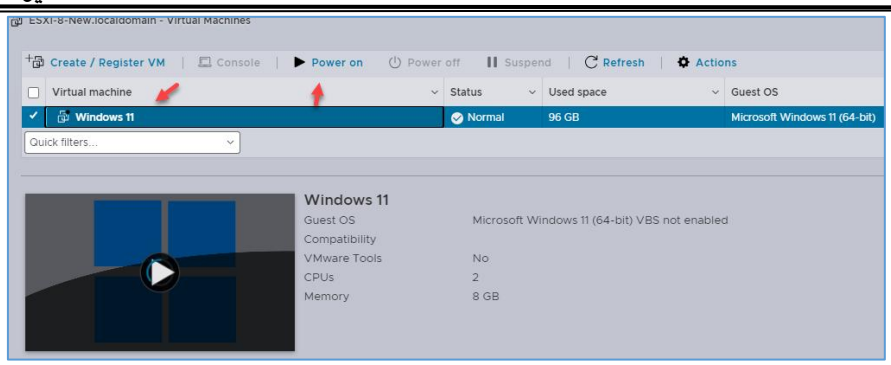
در شکل ٦-١٣٥، اگر تنظیمات نهایی ماشین مورد نظر مورد تایید است بر روی Finish کلیک کنید.



شکل ۶- ۱۳۵ ایجاد ماشین مجازی در ESXi

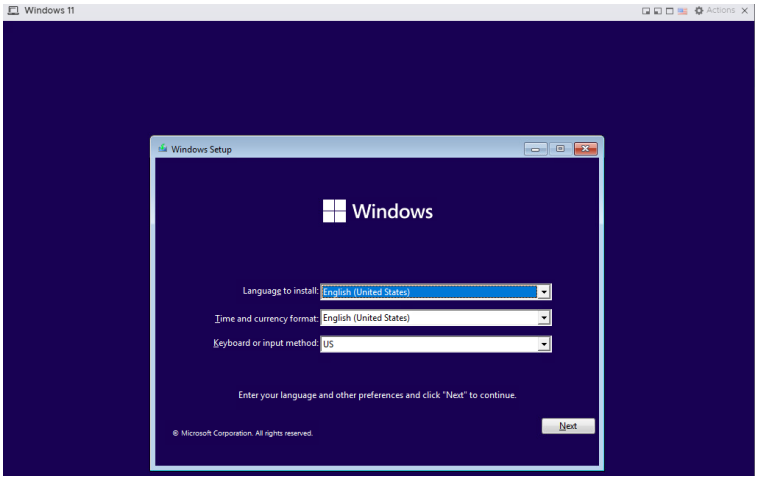
بعد از ایجاد ماشین، اگر به مانند شکل ٦-١٣٦، وارد لیست Virtual Machines شوید، ماشینی که ایجاد کردید را مشاهده می‌کنید، بر روی Power ON کلیک کنید تا ماشین مورد نظر روشن شود.

www.takbook.com



شکل ۶- ۱۳۶ ایجاد ماشین مجازی در ESXi

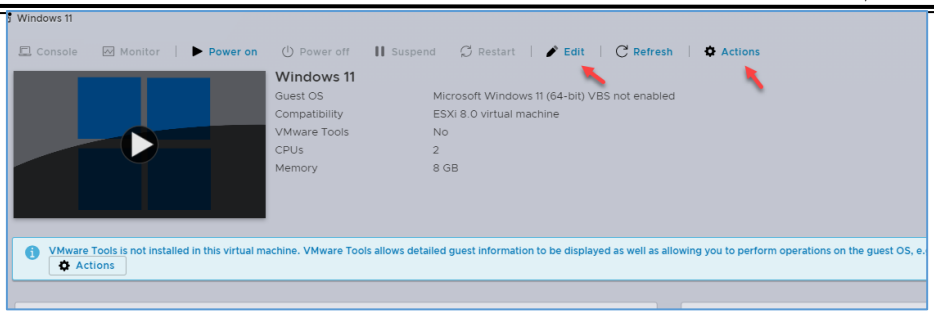
همان‌طور که در شکل ٦-۱۳۷، مشاهده می‌کنید بعد از کلیک بر روی Power on صفحه نصب ویندوز ۱۱ ظاهر شده است که می‌توانید آن را نصب و از آن استفاده کنید.



شکل ۶- ۱۳۷ ایجاد ماشین مجازی در ESXi

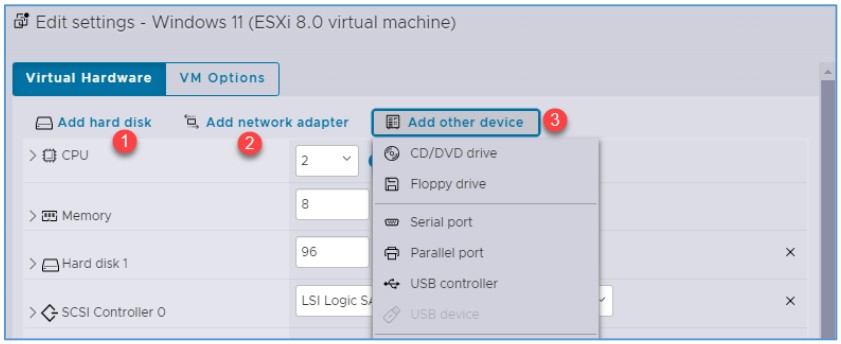
اگر در ESXi بر روی ماشین مجازی کلیک کنید، ابزارهای مختلف را به مانند شکل ٦-۱۳۸، مشاهده می‌کنید، که در صورت نیاز هر کدام از گزینه‌ها را توضیح خواهیم داد، برای ورود به تنظیمات ماشین مجازی باید بر روی گزینه‌ی Edit کلیک کنید و یا با کلیک بر روی Action و انتخاب گزینه‌ی Edit Settings این کار را انجام دهید.

www.takbook.com



شکل ۶- ۱۳۸ تنظیمات ماشین مجازی

در شکل ٦-۱۳۹، در قسمت شماره‌ی یک می‌توانید یک هارد دیسک جدید اضافه کنید، در قسمت شماره‌ی دو می‌توانید یک یا چند کارت شبکه به ماشین مورد نظر خود اضافه کنید، در قسمت شماره سه سخت‌افزارهای مخلفت دیگری هم مشاهده می‌کنید که در صورت نیاز می‌توانید از آنها استفاده کنید.



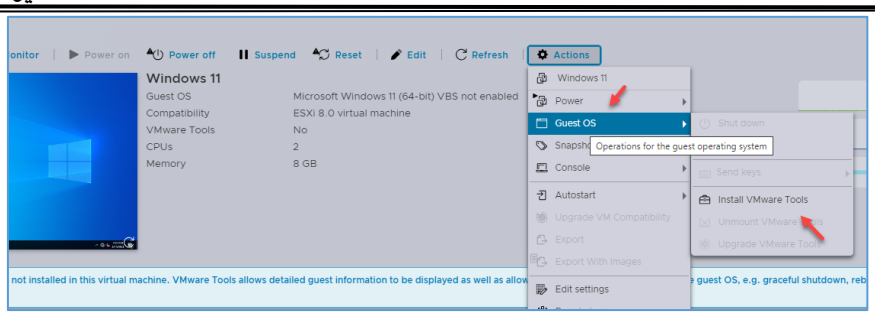
شکل ۶- ۱۳۹ اضافه کردن سخت افزار

٦-۱-٤-۹ نصب VMware Tools در ماشین مجازی

بعد از راه‌اندازی ماشین مجازی، اولین کاری که باید انجام دهید این است که سرویس VMware Tools را فعال کنید این سرویس دارای درایورهای مورد نظر VMware برای ارتباط بهتر با ماشین مورد نظر است.

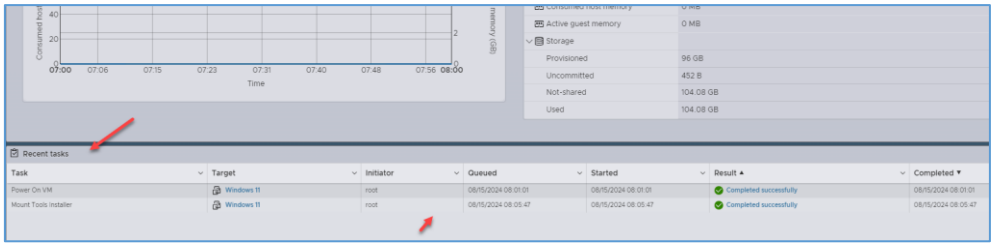
به مانند شکل ٦-۱٤۰، بر روی منوی Actions کلیک کنید و از قسمت Guest OS گزینه‌ی Install VMware Tools را انتخاب کنید، اگر به همین منو توجه کنید همه گزینه‌های آن غیر فعال است که با نصب این سرویس فعال خواهند شد.

www.takbook.com



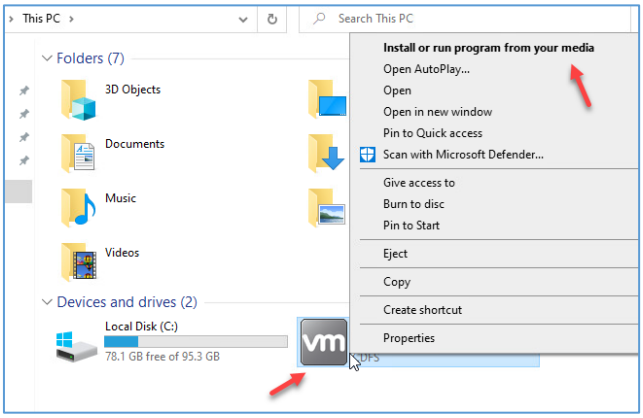
شکل ۶- ۱۴۰ نصب VMware Tools

بعد از اینکه گزینه‌ی Install VMware Tools را انتخاب کردید، اگر به شکل ٦-١٤١ دقت کنید در قسمت Recent Tasks، رویدادهای مربوط به ماشین مورد نظر ثبت می‌شود و جزئیات کار را می‌توانید متوجه شوید.



شکل ۶- ۱۴۱ نصب VMware Tools

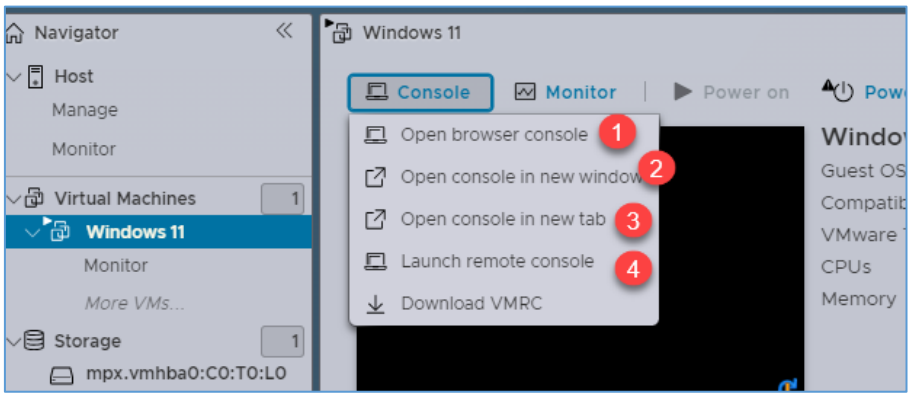
در ادامه کار اگر وارد ماشین مجازی مورد نظر شوید می‌توانید نرم‌افزار VMware Tools را مشاهده کنید، به مانند شکل ٦-١٤٢، بر روی آن کلیک راست کنید و گزینه‌ی Install or run program from your media را انتخاب کنید، بعد از این کار مراحل نصب را پیش ببرید و سرویس را فعال کنید.



شکل ۶- ۱۴۲ نصب VMware Tools

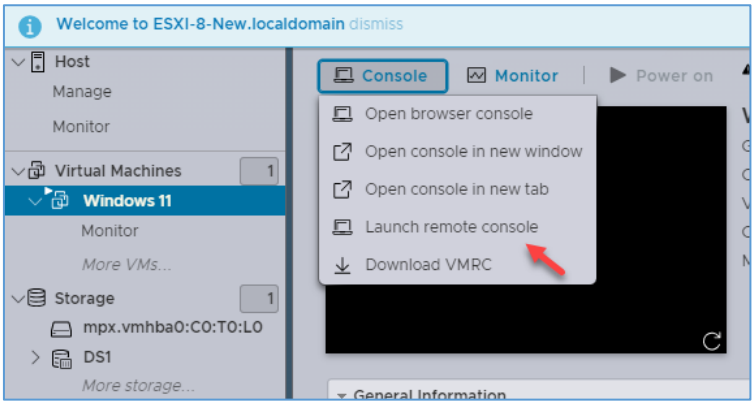
www.takbook.com

برای باز کردن ماشین مجازی باید از طریق گزینه‌ی Console اقدام کنید، به مانند شکل ٦-١٤٣، چند گزینه وجود دارد که اگر گزینه‌ی اول انتخاب شود، ماشین مورد نظر داخل محیط ESXi باز خواهد شد، با انتخاب گزینه‌ی دوم، دسترسی به ماشین داخل یک صفحه جدید باز خواهد شد که به نظرم روش خوبی است. با انتخاب گزینه‌ی سوم در یک Tab جدید باز خواهد شد و با انتخاب گزینه‌ی چهارم نرم‌افزارهایی که برای این کار طراحی شدند مانند VMware Remote Console اجرا خواهد شد و اگر این سرویس بر روی سیستم شما نصب نیست با انتخاب گزینه‌ی Download VMRC صفحه سایت VMware باز خواهد شد که بعد از باز شدن، برنامه مورد نظر را دانلود و بر روی سیستم خود نصب کنید.



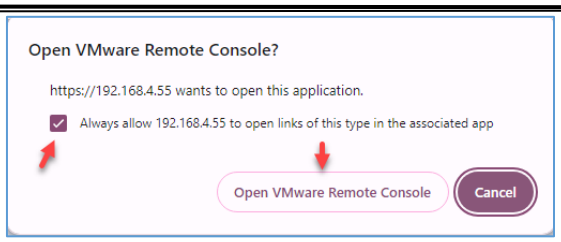
شکل ۶- ۱۴۳ نصب VMware Tools

بعد از دانلود و نصب VMware Remote Console می‌توانید به مانند شکل ٦-١٤٤، آن را اجرا کنید که این گزینه می‌تواند بسیار کمک کننده باشد.



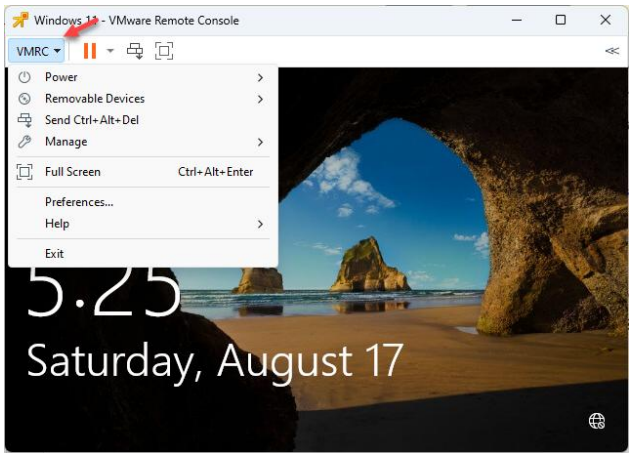
شکل ۶- ۱۴۴ VMware Remote Console

www.takbook.com



شکل ۶- ۱۴۵ VMware Remote Console

از طریق منوی VMRC می‌توانید به تنظیمات و اطلاعات ماشین مجازی دست پیدا کنید که این موضوع را در شکل ٦-١٤٦، مشاهده می‌کنید.



شکل ۶- ۱۴۶ VMware Remote Console

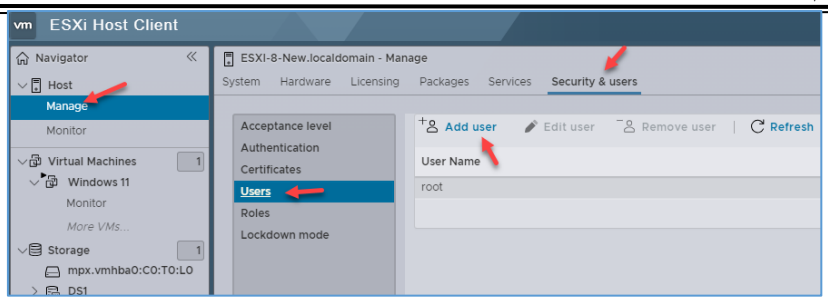
برای اینکه اندازه‌ی صفحه را تغییر دهید می‌توانید از گزینه‌ی Full Screen و یا از طریق کلید ترکیبی Ctrl+Alt+Enter استفاده کنید.

توجه داشته باشید گزینه‌هایی که در قسمت Power قرار دارند به صورت نرم‌افزاری انجام خواهد شد و مانند این است که در سیستم خود بر روی Shutdown و یا Restart کلیک کنید، گزینه‌های دیگر هم مانند CD/DVD، کارت شبکه و ... وجود دارد که می‌توانید آنها را قطع یا استفاده کنید.

۱۰-٤-۱-٦ تعریف و استفاده از کاربر در ESXI

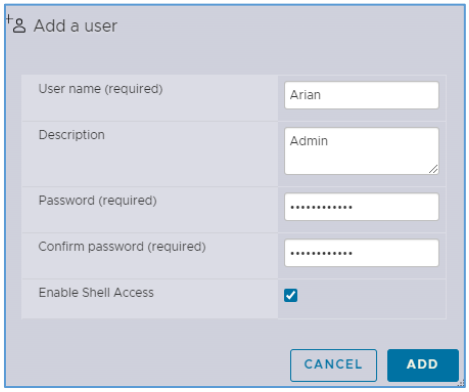
برای تعریف کاربر جدید در ESXi باید به مانند شکل ٦-١٤٧، از سمت چپ از قسمت Host وارد Manage شوید و از تب Security & users گزینه‌ی Users را انتخاب کنید، بعد از این در صفحه باز شده بر روی Add user کلیک کنید.

www.takbook.com



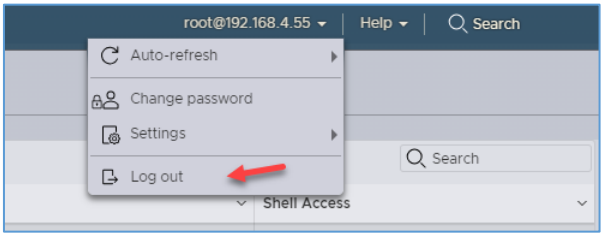
شکل ۶- ۱۴۷ کاربر در ESXI

در شکل ٦-١٤٨، نام کاربری را در قسمت User name وارد کنید و در قسمت Password هم یک رمز عبور مناسب و پیچیده وارد و بر روی Add کلیک کنید.



شکل ۶- ۱۴۸ کاربر در ESXI

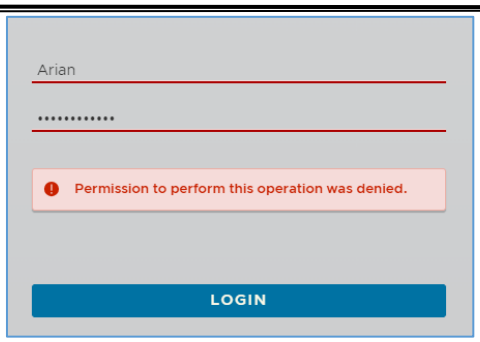
بعد از ایجاد کاربر جدید، باید از کاربر Root خارج شوید که این کار را طبق شکل ٦-١٤٩ انجام دهید.



شکل ۶- ۱۴۹ کاربر در ESXI

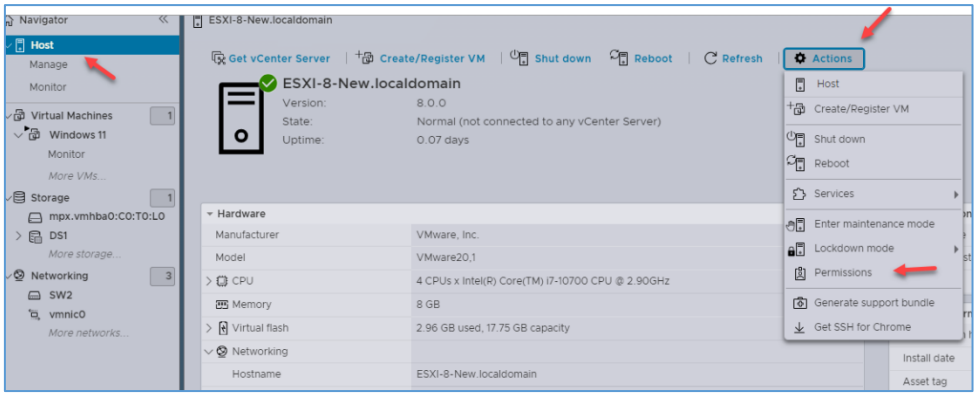
به صورت پیش‌فرض کاربر مورد نظر توانایی ورود به سرورESXi را نخواهد داشت، دلیل آن هم این است که هیچ گونه مجوزی برای آن کاربر صادر نشده است، همان‌طور که در شکل ٦-١٥٠، مشاهده می‌کنید کاربر arian توانایی ورود را ندارد.

www.takbook.com



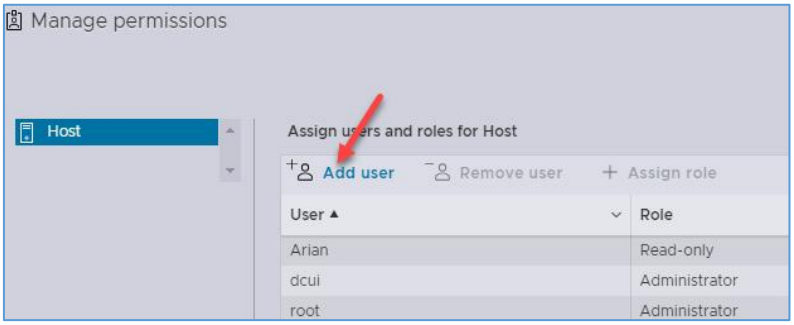
شکل ۶- ۱۵۰ کاربر در ESXI

برای اینکه مجوز به کاربر جدید بدهیم، باید با کاربر Root وارد شویم و برای تعریف دسترسی یا Permissions بر روی Host کلیک کنید و از قسمت Actions گزینه‌ی Permissions را انتخاب کنید که این موضوع را در شکل ٦-١٥١ مشاهده می‌کنید.



شکل ۶- ۱۵۱ کاربر در ESXI

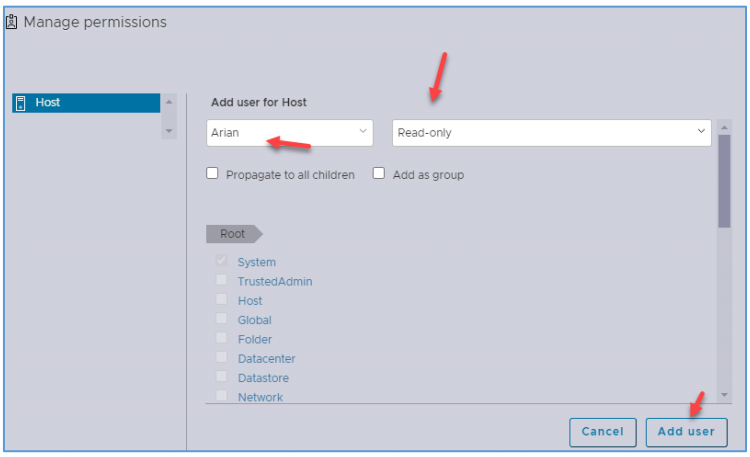
در شکل ٦-١٥٢، کاربرانی که دارای مجوز هستند را مشاهده می‌کنید، برای اضافه کردن کاربر جدید بر روی Add user کلیک کنید.



شکل ۶- ۱۵۲ کاربر در ESXI

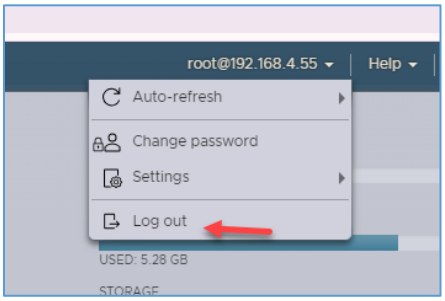
www.takbook.com

در شکل ٦-١٥٣ باید کاربر مورد نظر خود را از لیست اول انتخاب کنید و در لیست دوم حداکثر توانایی آن را مشخص کنید که در این قسمت Read-only انتخاب شده است، زمانی که Read-only را انتخاب می‌کنید در پائین صفحه دسترسی کاربر فقط برای System انتخاب می‌شود، برای تست این موضوع بر روی Add User کلیک کنید.



شکل ۶- ۱۵۳ کاربر در ESXI

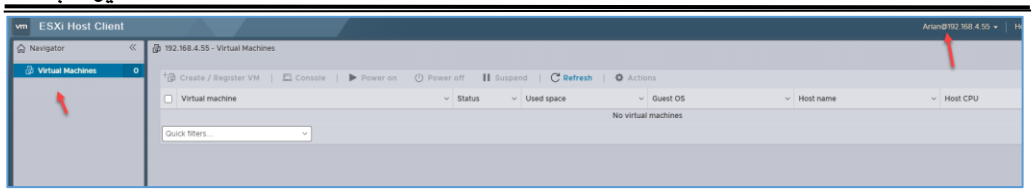
بعد از دادن دسترسی به کاربر مورد نظر برای خروج از کاربر فعلی (root) بر روی آدرس سرور در بالا و سمت راست کلیک و در منوی باز شده بر روی Log out کلیک کنید.



شکل ۶- ۱۵۴ کاربر در ESXI

همان‌طور که در شکل ٦-١٥٥، مشاهده می‌کنید کاربر Arian بسیار محدود شده است و در کل چیزی را نمی‌تواند مشاهده کند.

www.takbook.com

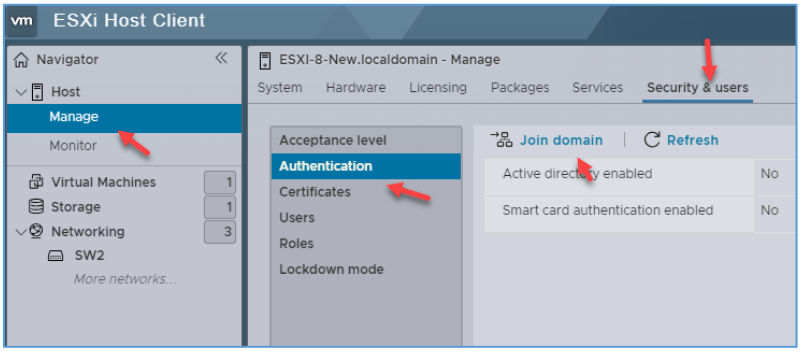


شکل ۶- ۱۵۵ کاربر در ESXI

برای تغییر دسترسی دوباره می‌توانید وارد قسمت Permissions شوید و کاربر را در گروه Administrator قرار دهید.

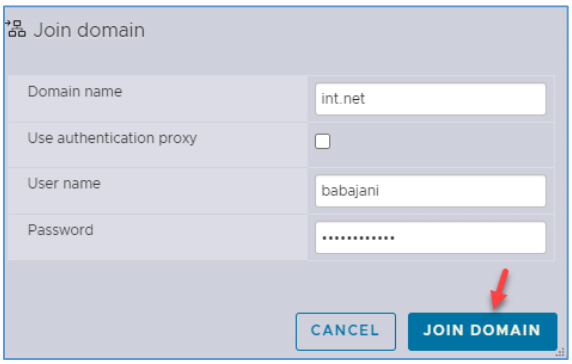
۱۱-٤-۱-٦ متصل کردن ESXi به دومین کنترلر

به مانند شکل ٦-۱٥٦، وارد تب Authentication شوید و بر روی Join domain کلیک کنید.



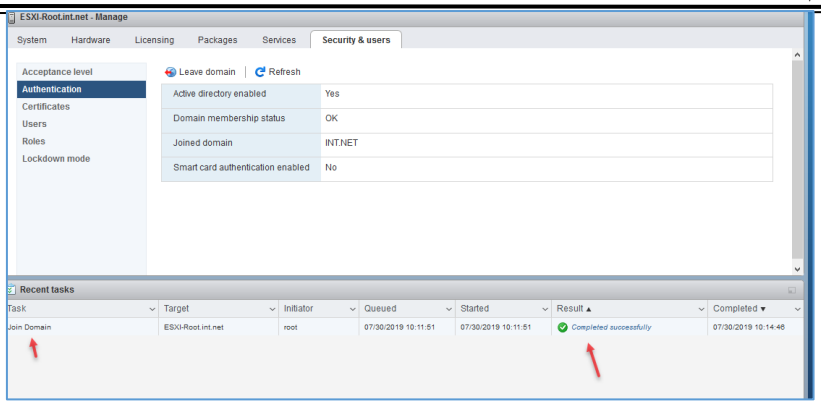
شکل ۶- ۱۵۶ متصل کردن ESXi به دومین کنترلر

در شکل ٦-۱٥۷، و در قسمت Domain name نام دومین شبکه خود را وارد کنید و در قسمت Username و Password باید اطلاعات کاربری را وارد کنید که دسترسی کامل را در شبکه داشته باشد.



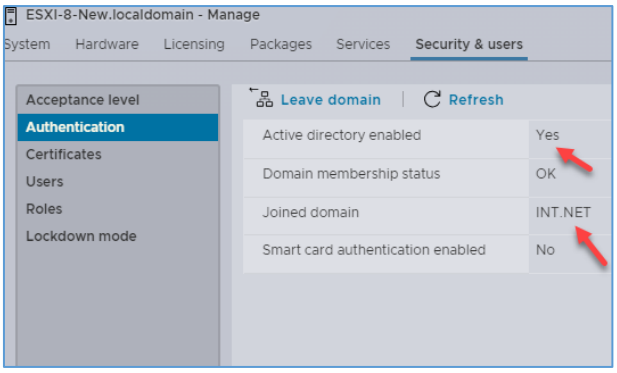
شکل ۶- ۱۵۷ متصل کردن ESXi به دومین کنترلر

www.takbook.com



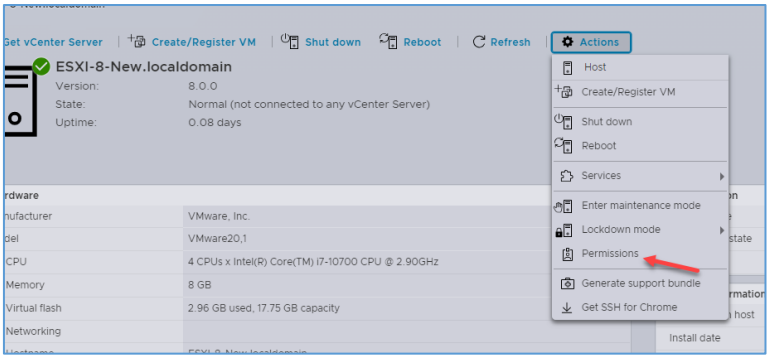
شکل ۶- ۱۵۸ متصل کردن ESXi به دومین کنترلر

بعد از کلیک بر روی Join domain به مانند شکل ٦-۱۵۹، ESXi به دومین Int.net متصل شده است.



شکل ۶- ۱۵۹ متصل کردن ESXi به دومین کنترلر

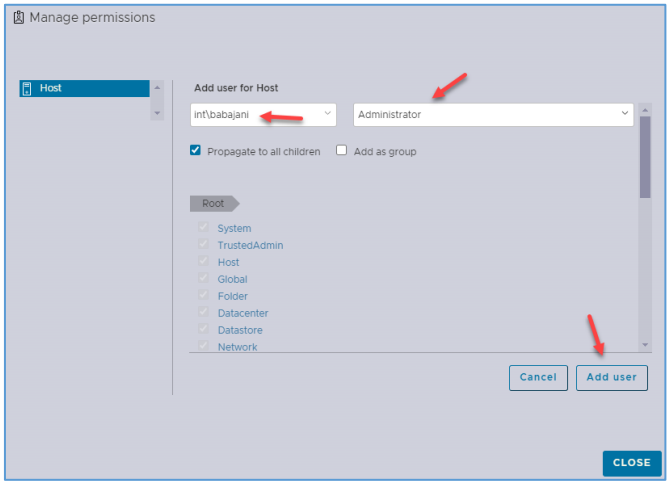
برای دسترسی به کاربر دومین دوباره به مانند شکل ٦-۱٦۰، وارد Permissions شوید.



شکل ۶- ۱۶۰ متصل کردن ESXi به دومین کنترلر

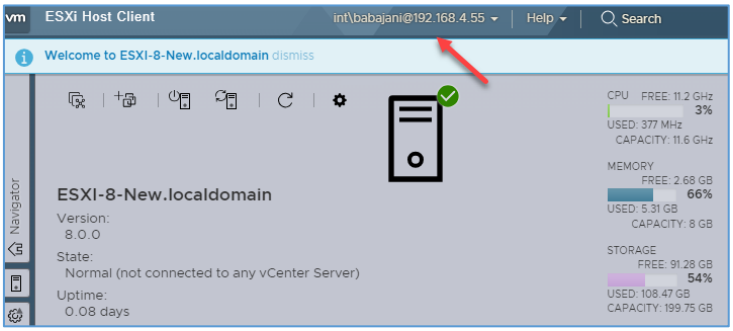
www.takbook.com

در شکل ٦-١٦١، باید نام کاربری را به همراه نام دومین خود وارد کنید که این موضوع در شکل مشخص شده است و بعد از این کار باید گروه مورد نظر را انتخاب کنید که برای این کاربر گروه Administrator در نظر گرفته شده است.



شکل ۶- ۱۶۱ متصل کردن ESXi به دومین کنترلر

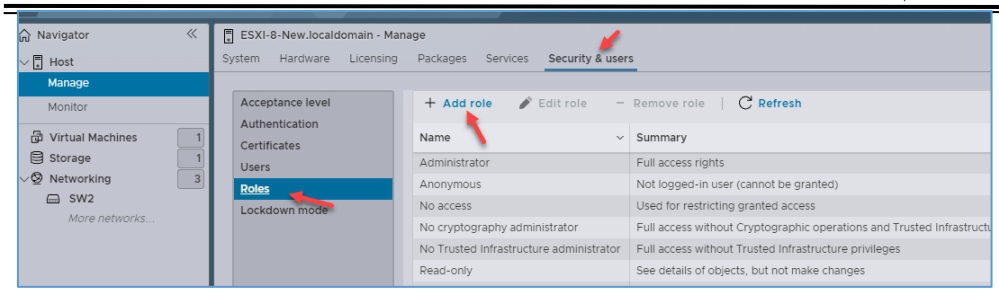
همان‌طور که در شکل ٦-١٦٢، مشاهده می‌کنید، کاربر مورد نظر که عضو دومین Int.net بوده توانسته وارد سرور ESXi شود و دسترسی لازم را داشته باشد.



شکل ۶- ۱۶۲ متصل کردن ESXi به دومین کنترلر

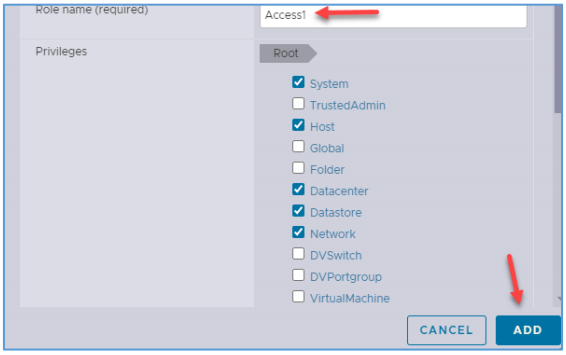
برای اینکه Role مربوط را به صورت شخصی ایجاد کنید به مانند شکل ٦-١٦٣، وارد Manage شوید و در تب Security & Users بر روی Add role کلیک کنید.

www.takbook.com



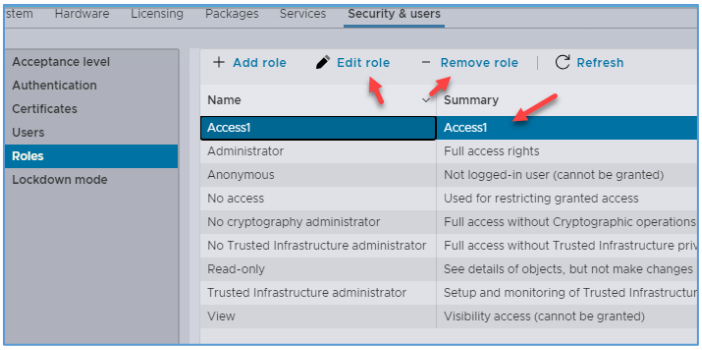
شکل ۶- ۱۶۳ متصل کردن ESXi به دومین کنترلر

به مانند شکل ٤-١٦٤، در قسمت Role name نام دلخواه خود را وارد و در قسمت Privileges باید مشخص کنید که این گروه چه دسترسی به منابع سرور ESXi داشته باشد، بعد از اتمام کار بر روی Add کلیک کنید.



شکل ۶- ۱۶۴ متصل کردن ESXi به دومین کنترلر

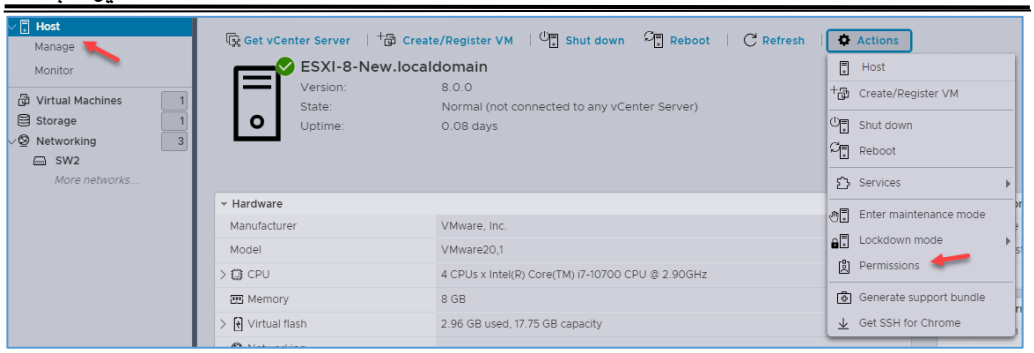
به مانند شکل ٦-١٥٦، برای حذف و یا تغییرات در Role مورد نظر باید آن را از لیست انتخاب کنید و گزینه‌های مورد نظر را انتخاب کنید، توجه داشته باشید برای اتصال کاربر به این Role باید مانند قسمت قبلی عمل کنید.



شکل ۶- ۱۶۵ متصل کردن ESXi به دومین کنترلر

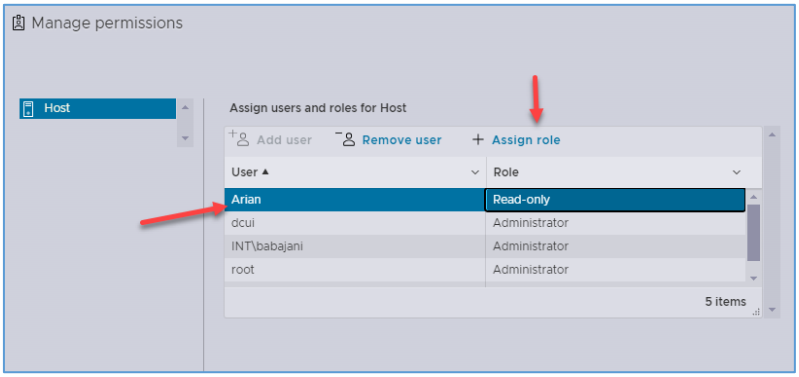
برای استفاده از Role مورد نظر به مانند شکل ٦-١٦٦ وارد Permissions شوید.

www.takbook.com



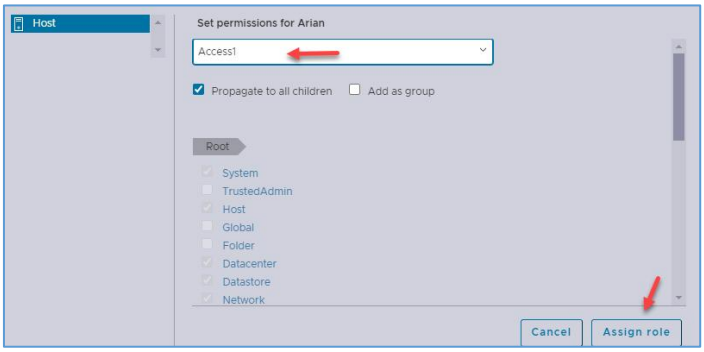
شکل ۶- ۱۶۶ متصل کردن ESXi به دومین کنترلر

به مانند شکل ٦-١٦٧، کاربر مورد نظر را انتخاب کنید و بر روی Assign role کلیک کنید.



شکل ۶- ۱۶۷ متصل کردن ESXi به دومین کنترلر

در شکل ٦-١٦٨، باید Role جدید را انتخاب کنید و بر روی Assign role کلیک کنید تا دسترسی لازم داده شود.



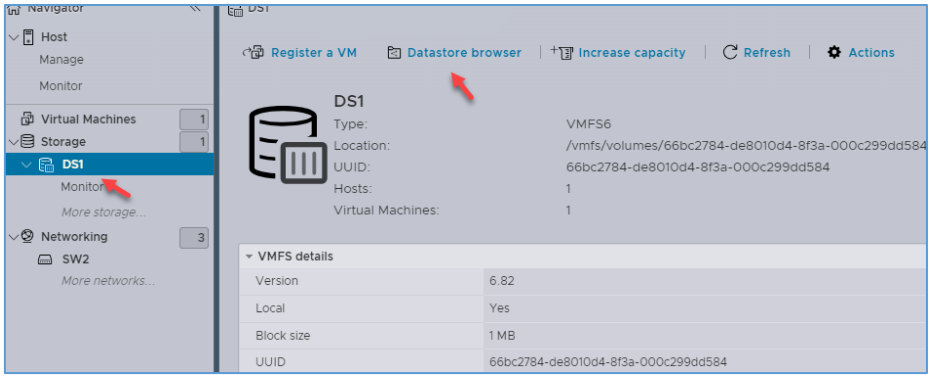
شکل ۶- ۱۶۸ متصل کردن ESXi به دومین کنترلر

www.takbook.com

۱۲-٤-۱-٦ آپلود کردن ماشین مجازی

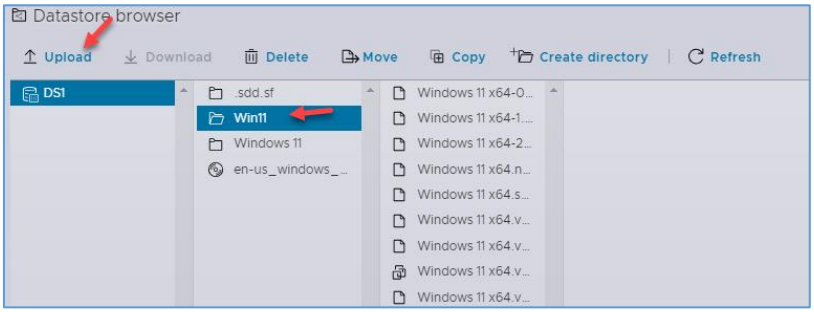
اگر چنانچه یک ماشین مجازی آماده ازجایی دیگر تهیه کردید و می‌خواهید در سرور جدید خود اجرا کنید باید به صورت زیر عمل کنید.

به مانند شکل ٦-۱٦۹، وارد Storage شوید و DataStore مورد نظر خود را انتخاب کنید و از منوی ابزار بالای آن بر روی Datastore browser کلیک کنید.



شکل ۶- ۱۶۹ آپلود کردن ماشین مجازی

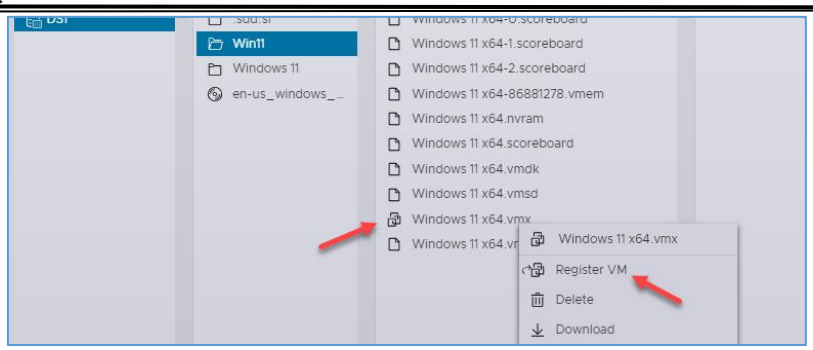
در شکل ٦-۱۷۰، باید ماشین مجازی خود را با کلیک بر روی Upload در Datastore مورد نظر قرار دهید، قبل از این کار یک پوشه برای ماشین مجازی خود ایجاد و فایل‌ها را در داخل آن بریزید، این ماشین‌مجازی را توسط نرم‌افزار VMware workstation ایجاد کردیم و حالا در ESXi می‌خواهیم اجرا کنیم.



شکل ۶- ۱۷۰ آپلود کردن ماشین مجازی

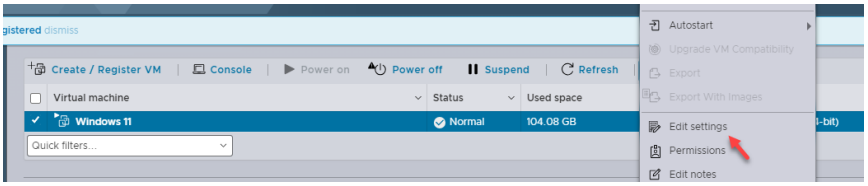
به مانند شکل ٦-۱۷۱، بعد از آپلود کردن ماشین در DataStore، برای استفاده از آن باید بر روی فایل vmx کلیک راست کنید و گزینه‌ی Register vm را انتخاب کنید.

www.takbook.com



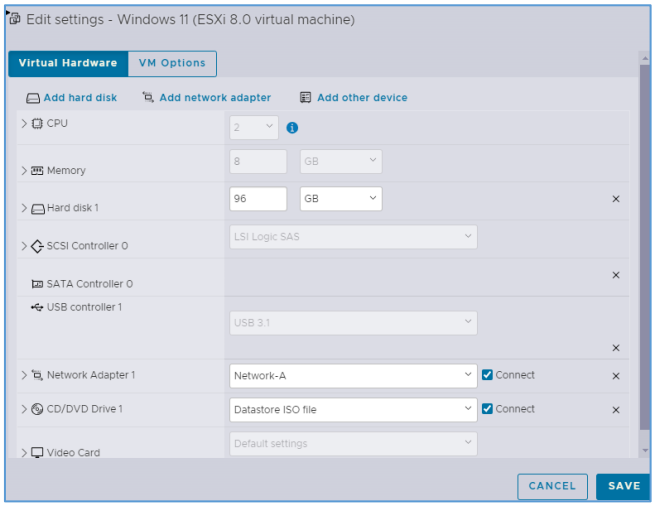
شکل ۶- ۱۷۱ آپلود کردن ماشین مجازی

اگر به شکل ٦-۱۷۲ توجه کنید، در قسمت Virtual Machines یک ماشین جدید به لیست اضافه شده است که همان ماشینی است که در قسمت قبل آپلود کردیم، برای کار با آن اول تنظیمات آن را بررسی می‌کنیم، بر روی آن کلیک راست کنید و گزینه‌ی Edit Settings را انتخاب کنید.



شکل ۶- ۱۷۲ آپلود کردن ماشین مجازی

در شکل ٦-۱۷۳، تنظیمات مربوط به ماشین مجازی را مشاهده می‌کنید که می‌توانید بر اساس نوع ماشین و منابع سخت‌افزاری سرور، آن را تغییر دهید.



شکل ۶- ۱۷۳ آپلود کردن ماشین مجازی

www.takbook.com

۱۳-٤-۱-٦ انتقال ماشین فیزیکی و مجازی به سرور ESXi

در روش قبلی انتقال ماشین مجازی به صورت دستی انجام شد و همین موضوع باعث می‌شود که تنظیمات دقیق برای سرور ESXi مبدا انجام نشود و احتمال می‌رود هارد دیسکی که در سرور آپلود کردید توانایی هماهنگ شدن و اجرا را نداشته باشد، به خاطر همین موضوع باید از روش بهتر و مطمئن‌تری برای این کار استفاده کرد.

برای انجام این‌کار شرکت VMware نرم‌افزاری را با عنوان VMware Converter آماده کرده که توانایی نصب بر روی ماشین مجازی و فیزیکی را دارد و می‌تواند به راحتی آنها را انتقال دهد، برای این کار می‌توانید از لینک زیر آخرین ورژن آن را دانلود کنید.

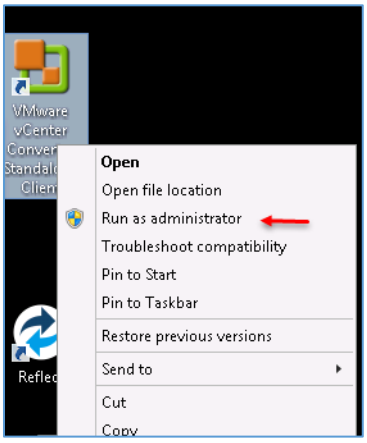
https://my.vmware.com/group/vmware/info?slug=infrastructure_operations_management/vmware_vCenter_converter_standalone/6_2_0

برای دریافت از سایت‌های ایرانی هم می‌توانید از لینک زیر هم استفاده کنید:

https://technet24.ir/vmware-vCenter-converter-standalone-3254

بعد از دانلود، آن را در سرور مورد نظر خود نصب و اجرا کنید، برای بررسی این نرم‌افزار به ادامه‌ی کار توجّه کنید.

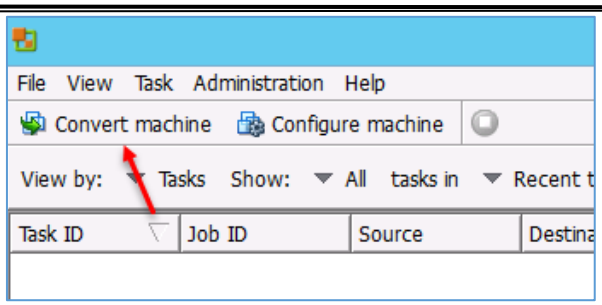
برای اجرا کردن این نرم‌افزار باید با اکانت مدیریّتی شبکهٔ خود وارد شوید، بعد از ورود بر روی آیکون آن کلیک راست کنید و گزینه‌ی Administrator Run as را انتخاب کنید تا نرم‌افزار با حداکثر مجوّز دسترسی اجرا شود.



شکل ۶- ۱۷۴ انتقال ماشین فیزیکی و مجازی

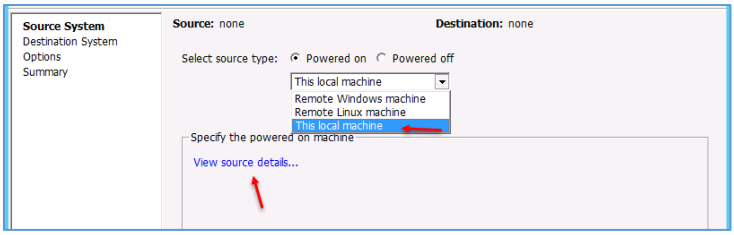
در شکل ٦-۱۷۵، بر روی Convert Machine کلیک کنید.

www.takbook.com



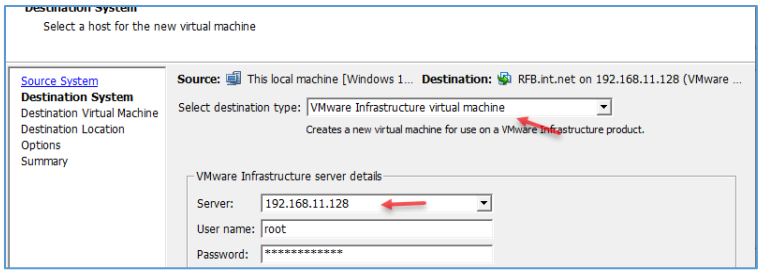
شکل ۶- ۱۷۵ انتقال ماشین فیزیکی و مجازی

در شکل ٦-١٧٦ و در قسمت Source type، گزینه‌ی Power On را انتخاب کنید تا بتوانید به سرور روشن خود متّصل شوید، سه نوع ارتباط وجود دارد؛ Windows Machine Remote برای سیستم‌های ویندوزی است که می‌توانید با وارد کردن نام یا IP سرور به آنها متّصل شد، گزینه‌ی Linux Machine برای سیستم-های لینوکسی است، گزینه‌ی Machine Local نیز برای همین سروری است که بر روی آن نصب شده است، همین گزینه را انتخاب کنید، اگر بر روی View source details کلیک کنید، اطّلاعاتی در مورد سرور به شما ارائه می‌دهد.



شکل ۶- ۱۷۶ انتقال ماشین فیزیکی و مجازی

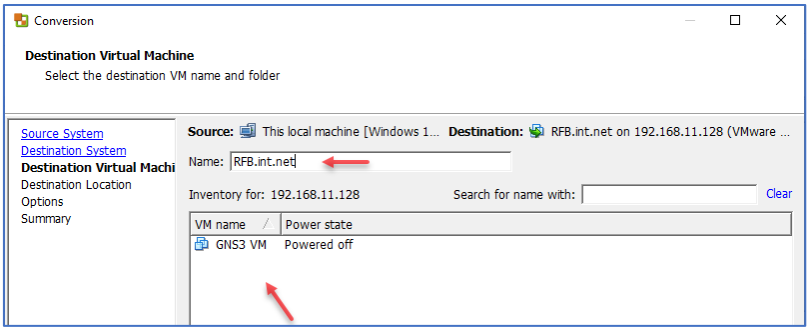
در شکل ٦-١٧٧ و در قسمت شماره‌ی یک باید نوع ماشین مجازی خود را مشخّص کنید، اگر می‌خواهید بر روی یک سرور ESXI قرار دهید باید گزینه‌ی اوّل را انتخاب کنید و یا اگر می‌خواهید یک ماشین مجازی جدا داشته باشید، گزینه‌ی دوم را انتخاب کنید، در این قسمت گزینه‌ی اول را انتخاب کنید و آدرس، نام کاربری و رمز عبور سرور ESXi را وارد کنید و بر روی Next کلیک کنید.



شکل ۶- ۱۷۷ انتقال ماشین فیزیکی و مجازی

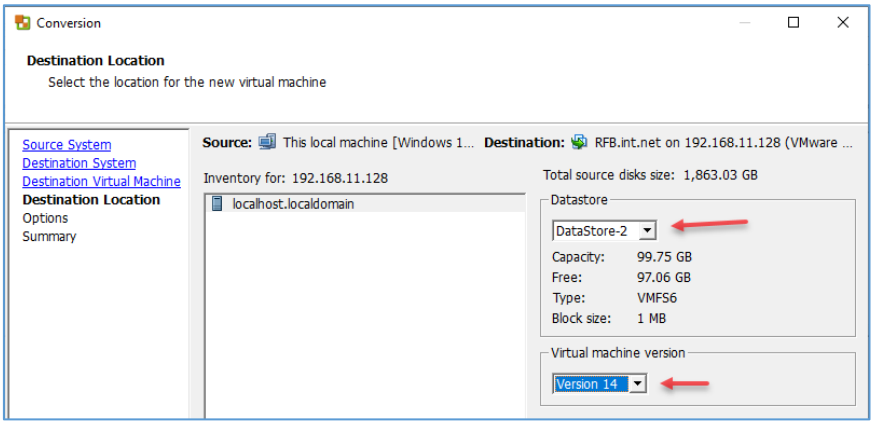
www.takbook.com

در شکل ٦-۱۷۸، نام سیستم خود را به همراه نام دومین مشاهده می‌کنید که می‌توانید آن را تعییر دهید، اگر به لیست توجه کنید ماشینی که در قسمت قبل ایجاد کردیم را مشاهده می‌کنید، بر روی Next کلیک کنید.



شکل ۶- ۱۷۸ انتقال ماشین فیزیکی و مجازی

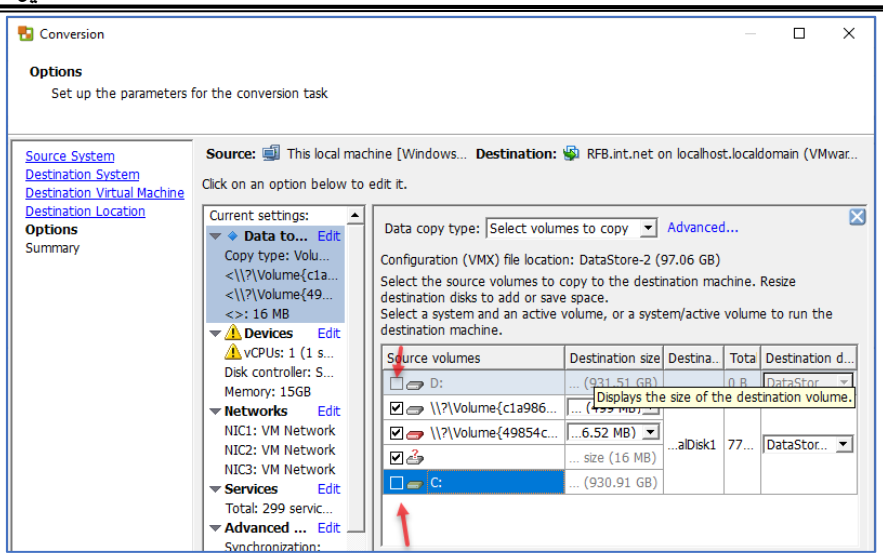
در شکل ٦-۱۷۹، باید مشخص کنید که ماشین مجازی ایجاد شده بر روی کدام DataStore در سرور ESXi قرار گیرد و بعد هم می‌توانید ورژن آن را مشخص کنید که البته بسته به آخرین ورژن این نرم‌افزار و سرور ESXi دارد.



شکل ۶- ۱۷۹ انتقال ماشین فیزیکی و مجازی

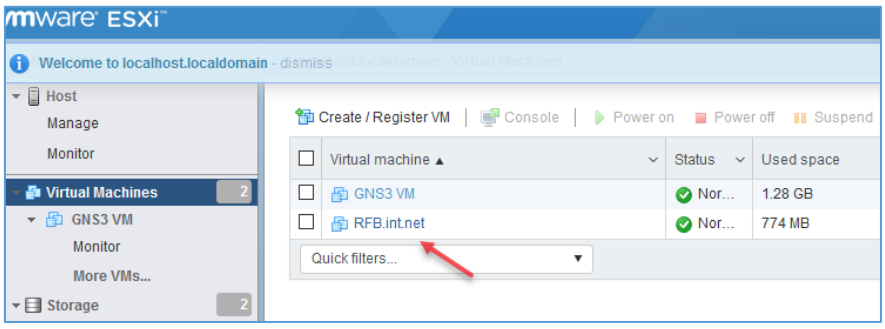
در شکل ٦-۱۸۰ می‌توانید پارتیشن‌های مورد نظر خود را برای انتقال به سرور ESXi انتخاب کنید، توجه داشته باشید برای انتقال حتماً درایوی که سیستم عامل در آن قرار دارد انتخاب شود، و به این موضوع هم توجه داشته باشید که DataStore مورد نظر در سرور ESXi باید فضای کافی داشته باشد.

www.takbook.com



شکل ۶- ۱۸۰ انتقال ماشین فیزیکی و مجازی

همان‌طور که در شکل ٦-۱۸۱، مشاهده می‌کنید با ورود به سرور ESXi ماشین مجازی جدید به لیست اضافه شده است و می‌توانید بدون هیچ مشکلی روی آن کار کنید، فقط به این موضوع توجه داشته باشید که حتماً بر روی ماشین‌ها نرم‌افزار VMware Tools را نصب کنید، تا ماشین به خوبی در سرور فعالیت کند.



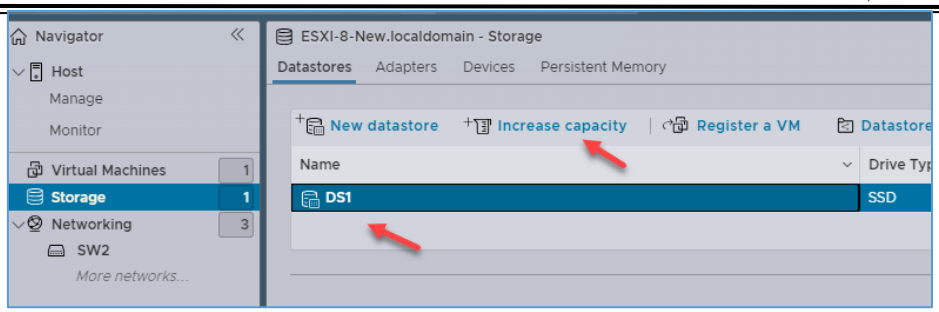
شکل ۶- ۱۸۱ انتقال ماشین فیزیکی و مجازی

١٤-٤-١-٦ افزایش حجم DataStore در ESXi

در مواردی پیش می‌آید که نیاز به افزایش حجم هارد دیسک دارید، و برای این کار نیاز است که هارد جدید به سرور اضافه کنید برای این کار به صورت زیر تنظیمات آن را انجام دهید.

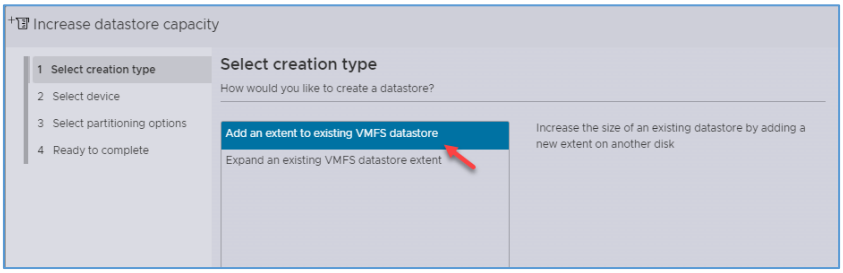
برای انجام این کار به مانند شکل ٦-۱۸۲، DataStore مورد نظر خود را انتخاب کنید و از منوی ابزار بالایی گزینه‌ی Increase capacity را انتخاب کنید.

www.takbook.com



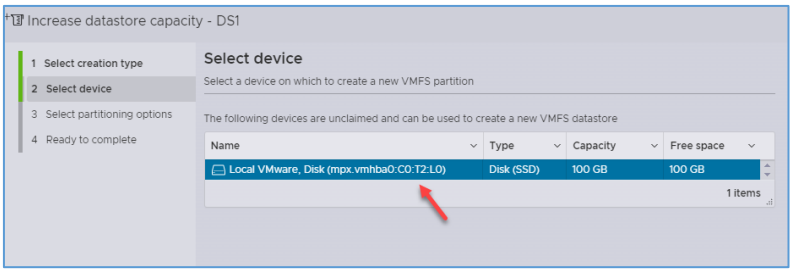
شکل ۶- ۱۸۲ افزایش حجم *DataStore*

در شکل ٦-۱۸۳، دو گزینه را مشاهده می‌کنید که گزینه‌ی اول برای اضافه کردن فضای یک هارد دیسک دیگر بر روی همین DataStore است و گزینه‌ی دوم برای استفاده از حجم باقیمانده از همان هارد قبلی است، گزینه اول را انتخاب و بر روی Next کلیک کنید.



شکل ۶- ۱۸۳ افزایش حجم *DataStore*

در شکل ٦-۱۸٤، باید هارد مورد نظر خود را انتخاب کنید، توجه داشته باشید با انتخاب این هارد، تمام فضای آن به DataStore انتخابی داده خواهد شد.



شکل ۶- ۱۸۴ افزایش حجم *DataStore*

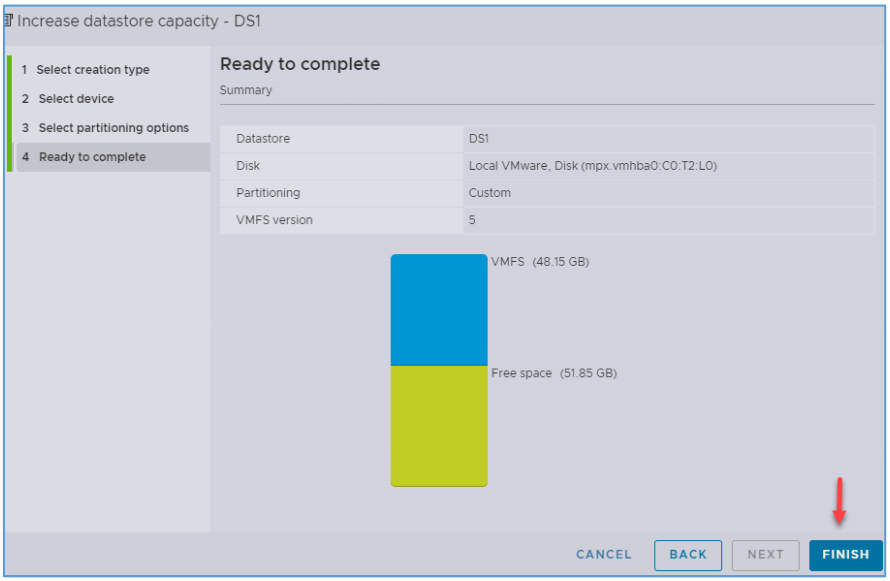
در شکل ٦-۱۸۵، می‌خواهیم نصف فضای هارد دیسک را به DataStore مورد نظر اختصاص دهیم، برای همین در قسمت اول گزینه‌ی Custom را انتخاب و مقدار فضای آن را با انتخاب قسمت سبز رنگ مشخص می‌کنیم.

www.takbook.com



شکل ۶- ۱۸۵ افزایش حجم DataStore

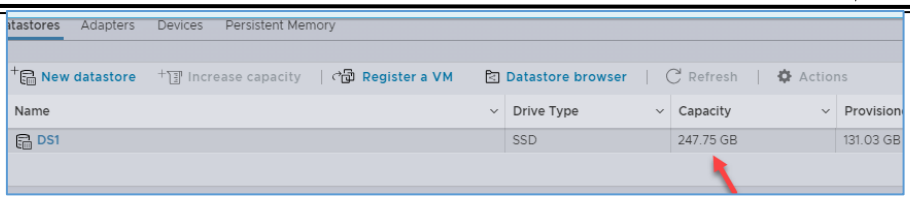
در این قسمت نصف فضای هارد به صورت آبی رنگ در آمده که مربوط به نوه VMFS است و بقیه هارد دیسک که سبز رنگ است خالی می‌باشد.



شکل ۶- ۱۸۶ افزایش حجم DataStore

به مانند شکل ٦-١٨٧، اگر به مقدار فضای هارد دیسک توجه کنید متوجه خواهید شد که ۵۰ گیگ به حجم اصلی هارد دیسک اضافه شده است، در ادامه برای نصف فضای دیگر هارد دوم می‌توانید از گزینه‌ی Expand an existing VMFS datastore extent استفاده کنید.

www.takbook.com

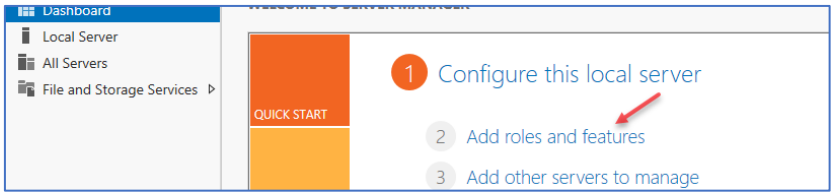


شکل ۶- ۱۸۷ افزایش حجم *DataStore*

۱۵-٤-۱-٦ اضافه کردن NFS به سرور ESXi

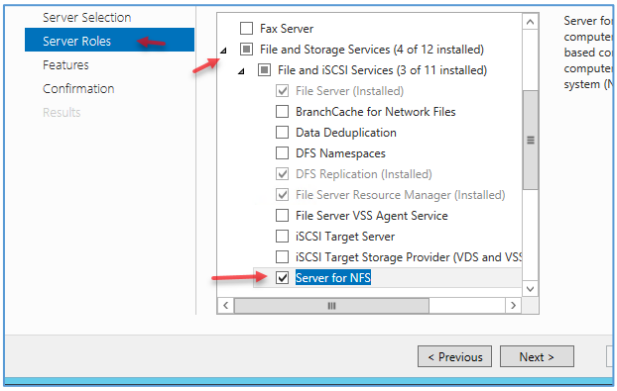
در این روش شما می‌توانید با استفاده از NFS یک هارد دیسک تحت شبکه را برای استفاده در ESXi فعال کنید، برای استفاده از این سیستم می‌توانید از سیستم‌عامل‌های مختلفی مانند لینوکس، ویندوز، مک و.... استفاده کنید، در این قسمت ما ویندوز سرور ۲۰۲۲ را برای تست انتخاب کردیم.

به مانند شکل ٦-۱۸۸، وارد ویندوز سرور شوید و Server Manager را اجرا کنید و در صفحه باز شده بر روی Add roles and Features کلیک کنید.



شکل ۶- ۱۸۸ اضافه کردن *NFS*

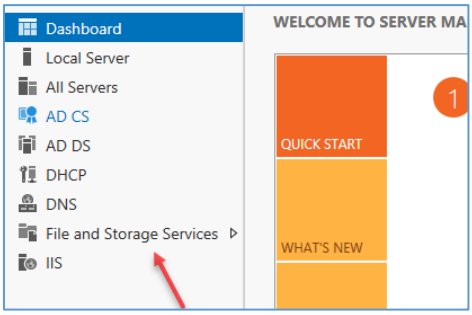
در شکل ٦-۱۸۹، از سمت چپ وارد قسمت Server Roles شوید و از قسمت File and Storage Services گزینه‌ی Server for NFS را انتخاب و بر روی Next کلیک کنید و این سرویس را نصب کنید، توجه داشته باشید بعد از نصب سرویس حتماً سرور را Restart کنید تا تنظیمات آن اعمال شود.



شکل ۶- ۱۸۹ اضافه کردن *NFS*

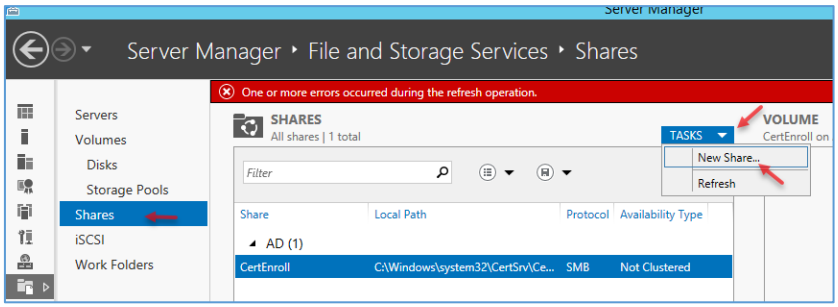
www.takbook.com

بعد از نصب سرویس در Server Manager به مانند شکل ٦-۱۹۰، بر روی File and Storage Services کلیک کنید.



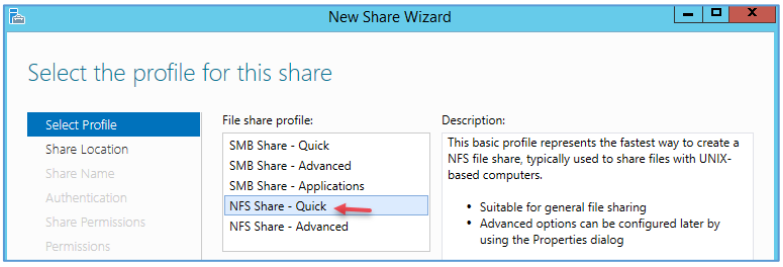
شکل ۶- ۱۹۰ اضافه کردن NFS

در شکل ٦-۱۹۱، گزینه‌ی Shares را انتخاب و بعد از منوی TASKS گزینه‌ی New Share را انتخاب کنید.



شکل ۶- ۱۹۱ اضافه کردن NFS

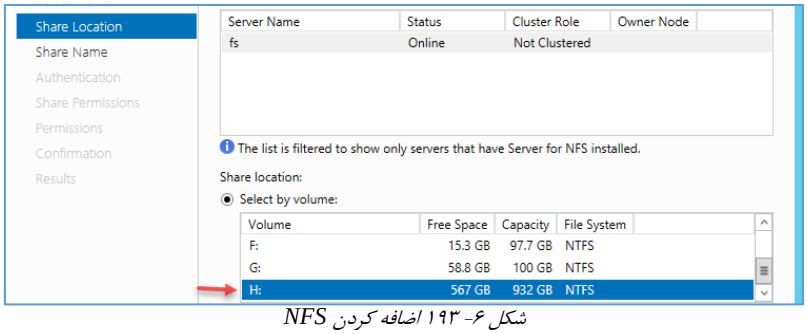
در شکل ٦-۱۹۲، گزینه‌های مختلفی را مشاهده می‌کنید، اگر توجه کنید دو گزینه مربوط به NFS را مشاهده می‌کنید که برای شروع کار گزینه‌ی Quick را انتخاب کنید، توجه داشته باشید که اگر بخواهید گزینه‌ی Advanced را انتخاب کنید، همزمان باید سرویس File Server Resource Manager باید نصب باشد.



شکل ۶- ۱۹۲ اضافه کردن NFS

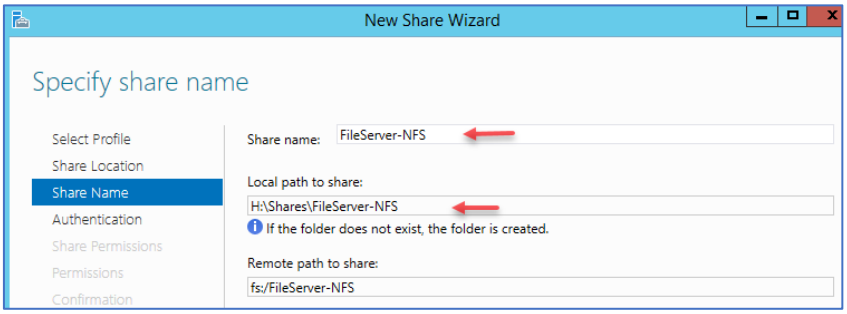
www.takbook.com

در شکل ٦-۱۹۳، باید یکی از هاردهای سرور را که فضای کافی هم دارد را انتخاب کنید و بر روی Next کلیک کنید، البته در پائین صفحه می‌توانستید فولدر مورد نظر خود را در آن درایو ایجاد و آدرس آن را در قسمت مورد نظر وارد کنید.



شکل ۶- ۱۹۳ اضافه کردن NFS

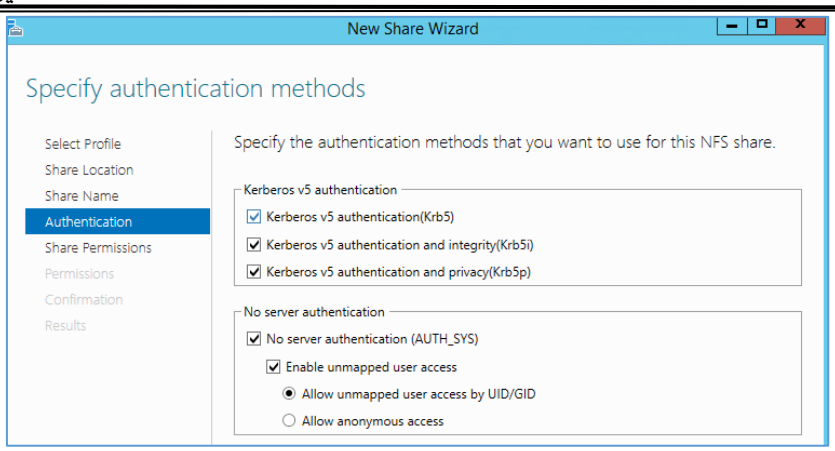
در شکل ٦-۱۹٤، در قسمت Sharename یک نام به دلخواه وارد کنید، بعد از این کار در قسمت دوم یک آدرس برای نامی که نوشتید ایجاد می‌شود و در آخر هم آدرس دسترسی در شبکه برای آن مشخص می‌شود.



شکل ۶- ۱۹۴ اضافه کردن NFS

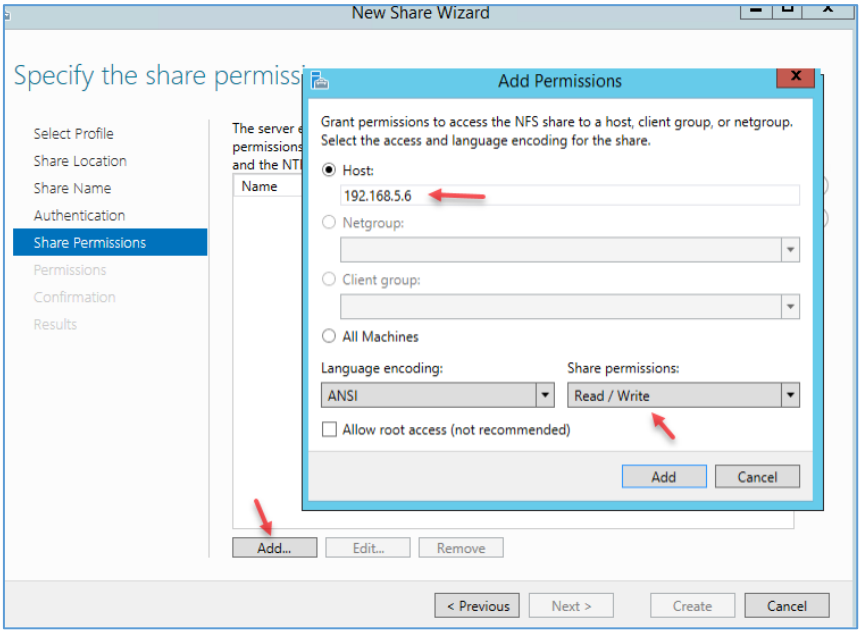
در شکل ٦-۱۹٥، باید نوع رمزنگاری را مشخص کنید، گزینه‌های مشخص شده را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



شکل ۶- ۱۹۵ اضافه کردن NFS

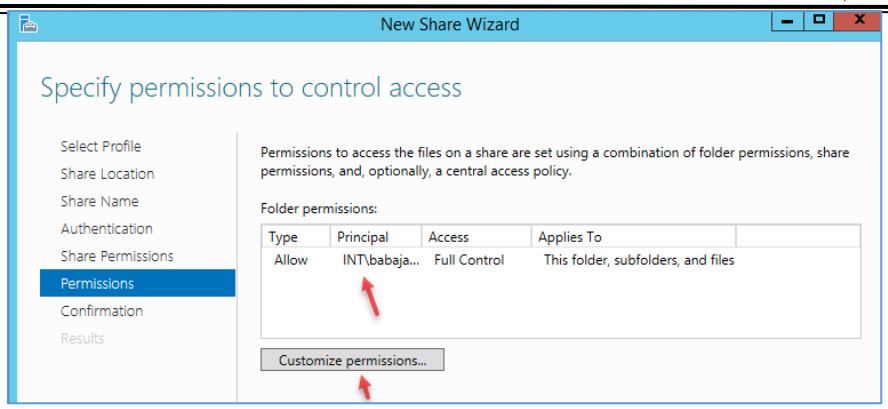
در شکل ٦-١٩٦، بر روی Add کلیک کنید و در پنجره باز شده و در قسمت Host باید آدرس سرور ESXi را وارد کنید و در پائین آن گزینه‌ی Read/write را انتخاب کنید تا سرور ESXi قادر به نوشتن در این فولدر باشد، بعد از اضافه کردن سرور بر روی Next کلیک کنید.



شکل ۶- ۱۹۶ اضافه کردن NFS

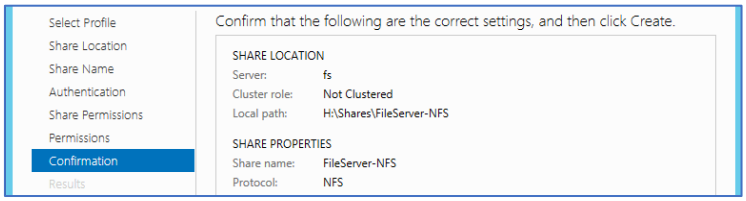
در شکل ٦-١٩٧، باید مشخص کنید که چه کاربری توانایی دسترسی به این فولدر را داشته باشد، البته می‌توانید گروه Everyone را هم به این لیست اضافه کنید تا همگی به این فولدر دسترسی داشته باشند.

www.takbook.com



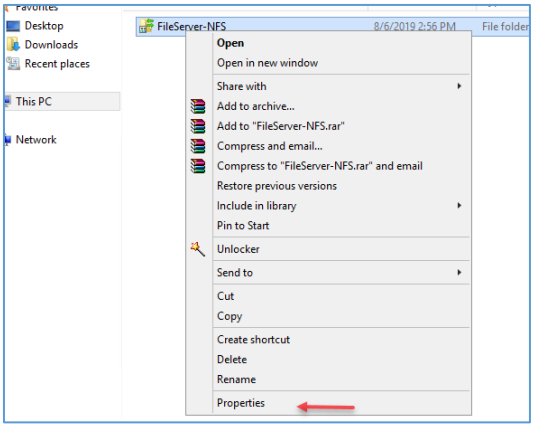
شکل ۶- ۱۹۷ اضافه کردن NFS

در شکل۶-۱۹۸، اگر تنظیمات مورد تایید است بر روی Create کلیک کنید تا تنظیمات بر روی فولدر مورد نظر اعمال شود.



شکل ۶- ۱۹۸ اضافه کردن NFS

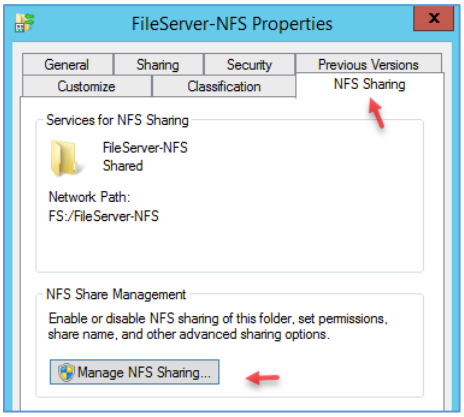
همان‌طور که در شکل ۶-۱۹۹، مشاهده می‌کنید، در آدرس مشخص شده یک پوشه با نامی که وارد کردید ایجاد شده است که آیکون آن هم تغییر کرده است، برای بررسی جزئیات بیشتر بر روی آن کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۶- ۱۹۹ اضافه کردنNFS

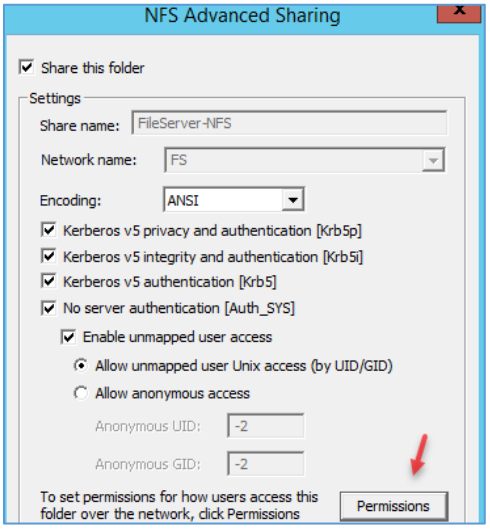
www.takbook.com

در شکل ٦-۲۰۰، وارد تب جدید NFS Sharing شوید که بعد از نصب سرویس مورد نظر ایجاد شده است، بعد از آن بر روی Manage NFS Sharing کلیک کنید.



شکل ۶- ۲۰۰ اضافه کردن NFS

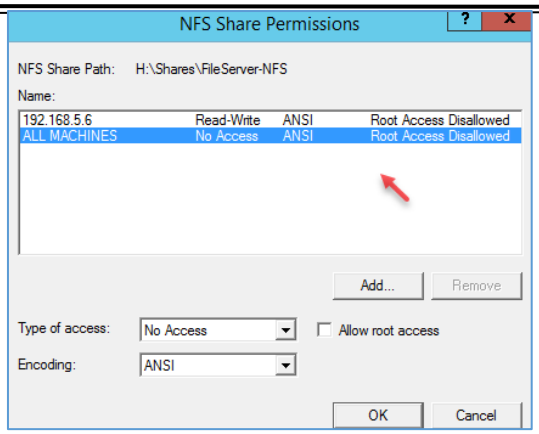
همان‌طور که در شکل ٦-۲۰۱، مشاهده می‌کنید، تنظیماتی که در قسمت قبل انجام دادیم مشخص شده است که می‌توانید آن را تغییر دهید، بر روی Permissions کلیک کنید.



شکل ۶- ۲۰۱ اضافه کردن NFS

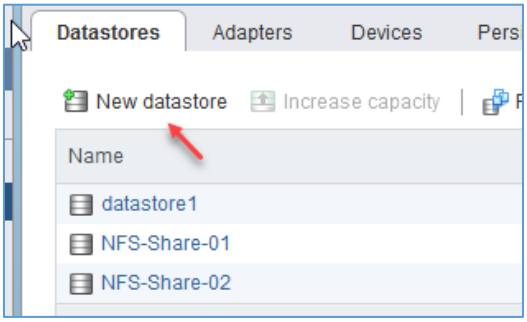
به مانند شکل ٦-۲۰۲ و در قسمت Permissions هم سرور 192.168.5.6 که مربوط به ESXi است در لیست مشخص شده است و شما هر چنتا سرور که نیاز دارید تا به این پوشه دسترسی داشته باشد را می‌توانید به لیست اضافه کنید.(اگر سرور مورد نظر را به لیست اضافه نکنید این نوع هارد دیسک به لیست اضافه نمی‌شود)

www.takbook.com



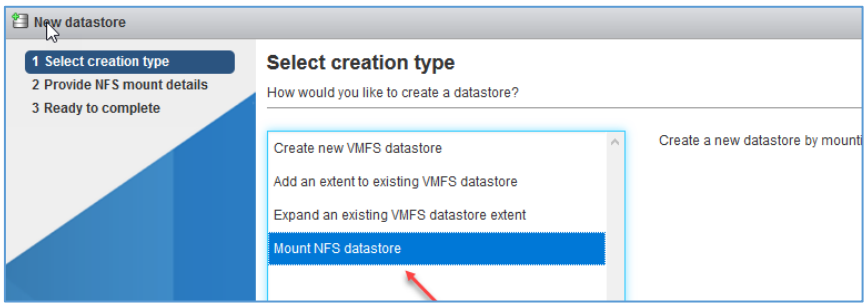
شکل ۶- ۲۰۲ اضافه کردن NFS

به مانند شکل ٦-۲۰۳، برای اضافه کردن DataStore از نوع NFS وارد ESXi شوید و بر روی New datastore کلیک کنید.



شکل ۶- ۲۰۳ اضافه کردن NFS

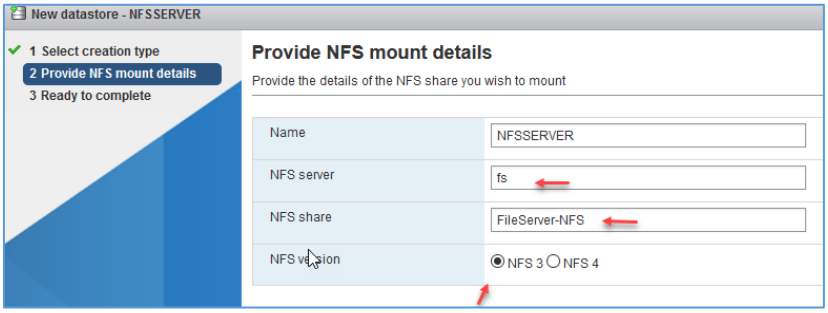
در شکل ٦-۲۰٤، باید گزینه‌ی Mount NFS datastore را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۶- ۲۰۴ اضافه کردن NFS

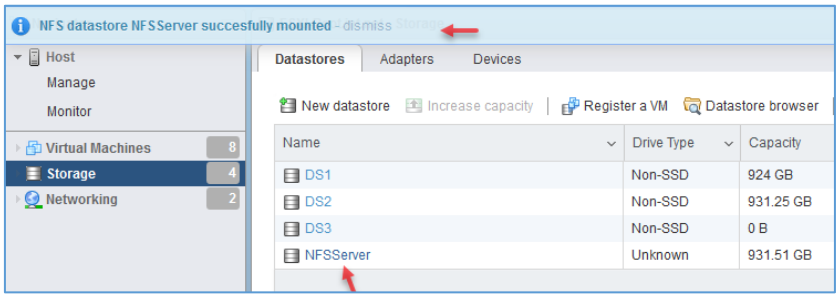
www.takbook.com

در شکل ٦-۲۰۵، یک نام به دلخواه وارد کنید و در قسمت NFS server باید نام سروری که بر روی آن NFS را فعال کردید را وارد کنید و در ادامه در قسمت NFS share باید نام فولدر Share شده را وارد کنید، گزینه‌ی آخر برای ایجاد امنیت است که NFS4 برای ایجاد امنیت بیشتر است.



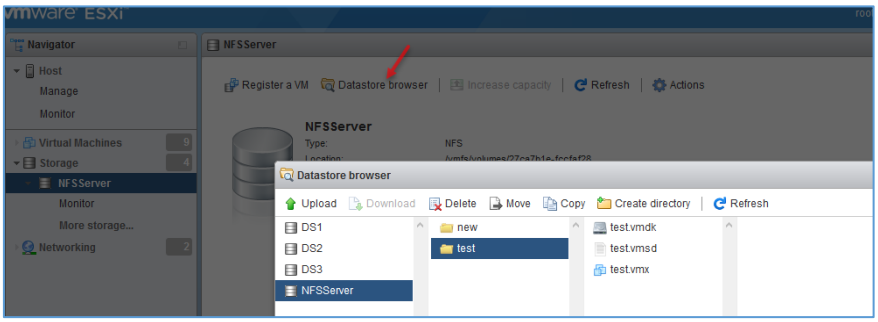
شکل ۶- ۲۰۵ اضافه کردن NFS

به مانند شکل ٦-۲۰٦، اگر به قسمت Storage توجه کنید DataStore از نوع NFS به لیست اضافه شده است.



شکل ۶- ۲۰۶ اضافه کردن NFS

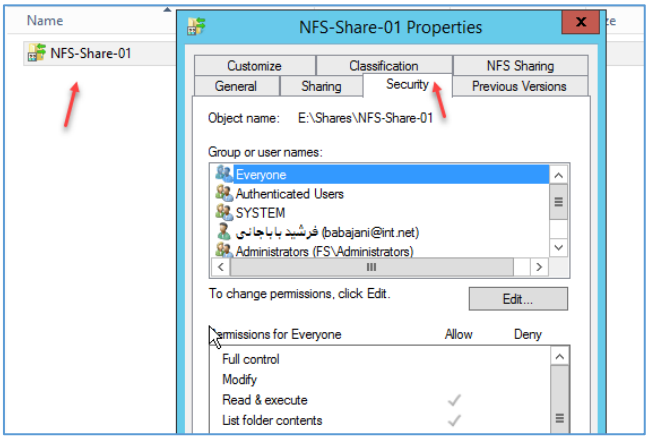
همان‌طور که در شکل ٦-۲۰۷ مشاهده می‌کنید، با ورود به DataStore جدید توانستیم فولدر و ماشین مجازی بر روی آن قرار دهیم.



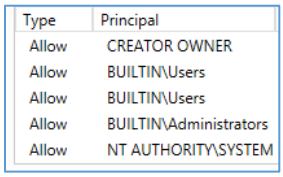
شکل ۶- ۲۰۷ اضافه کردن NFS

www.takbook.com

اگر برای ایجاد فایل در DataStore از نوع NFS با مشکل روبرو شدید و دسترسی ندارید باید به مانند شکل ۲۰۸-۶، وارد تنظیمات شوید و بعد در تب Security دسترسی لازم را اعمال کنید.



شکل ۶- ۲۰۸ تنظیم Security

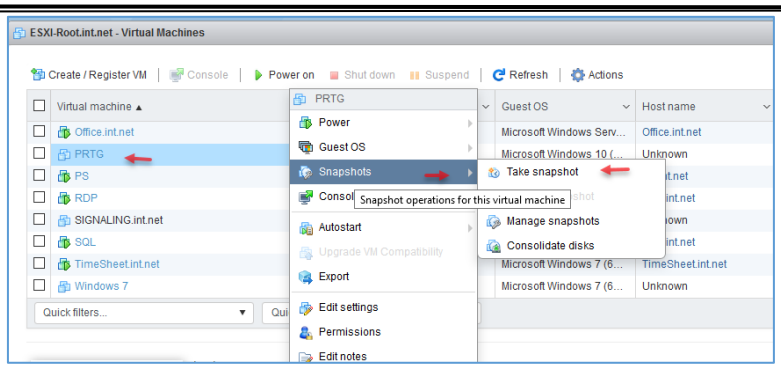


شکل ۶- ۲۰۹ اضافه کردن NFS

۶-۱-۴-۱۶ ایجاد SnapShot از ماشین‌های ESXi

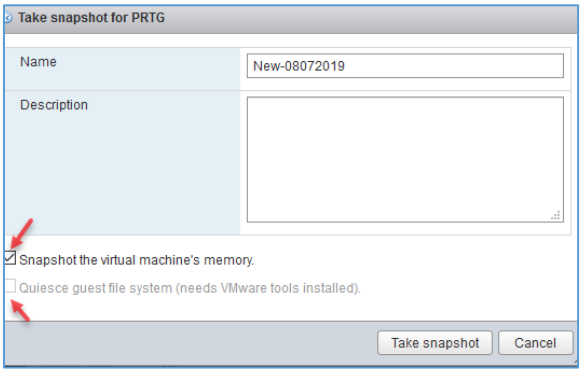
یکی از مهمترین‌کارهایی که در مجازی‌سازی می‌توان انجام داد ایجاد یک فایل SnapShot از ماشین‌هایی مجازی است تا اگر در مواردی ماشین مورد نظر با مشکل مواجه شد بتوانیم به حالت ایده‌ال برگردانیم. در مورد SnapShot و فایل‌هایی که بعد از فعال شدن آن در دایرکتوری ایجاد می‌شود را در اوایل فصل توضیح دادیم و در این قسمت نحوه‌ی فعال‌سازی آن را بررسی می‌کنیم، برای این کار به مانند شکل ۶-۲۱۰، بر روی ماشین مجازی خود کلیک راست کنید و از قسمت Snapshots گزینه‌ی Take snapshot را انتخاب کنید.

www.takbook.com



شکل ۶- ۲۱۰ SnapShot

در شکل ٦-۲۱۱، در قسمت Name یک نام به دلخواه وارد کنید که پیشنهاد می‌شود به صورت تاریخ و ساعت وارد کنید تا بررسی آن راحت تر باشد، در قسمت پائین همین صفحه دو گزینه وجود دارد که اگر گزینه‌ی Snapshot the virtual machine's memory را انتخاب کنید در صورت روشن بودن ماشین، هر گونه اطلاعاتی را که در رم قرار دارد یعنی اینکه هر نرم‌افزار یا فایلی باز باشد به همان صورت اول آن را به هارد دیسک انتقال می‌دهد و بعد از روی آن Snapshot تهیه می‌کند، توجه داشته باشد اگر نیاز به برگشت Snapshot باشد همه‌ی فایل‌های باز دقیقاً به همان صورت برگشت داده خواهد شد، اما اگر گزینه‌ی Quiesce guest file system (needs VMware tools installed) را انتخاب کنید، باعث می‌شود که نوشتن در آن زمان در هارد دیسک متوقف شود و Snapshot گرفته شود، البته به این نکته مهم باید دقت کنید که حتماً باید بر روی ماشین مجازی VMware Tools نصب شده باشد، این پشتیبان‌گیری بیشتر برای نرم‌افزارهای Veeam و امثال آنها کاربرد دارد، برای فعال کردن آن باید تیک گزینه‌ی اول را بردارید ولی اگر گزینه‌ی اول فعال باشد انتخاب خوبی برای ماشین شما خواهد بود.

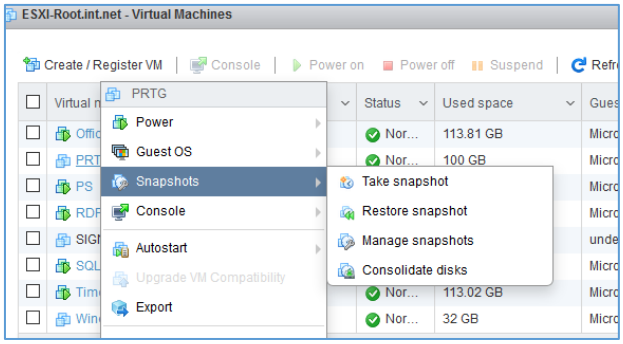


شکل ۶- ۲۱۱ / ایجاد SnapShot

www.takbook.com

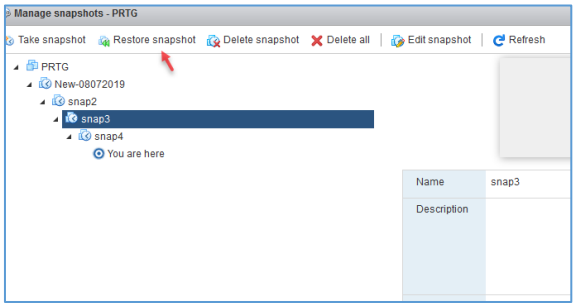
نکته مهم اینکه اگر هر دو تیک این دو گزینه را بردارید، و بعد از ماشین مورد نظر پشتیبان تهیه شود در زمان بازگشت، ماشین مورد نظر خاموش خواهد بود، که به این حالت Crash-consistent هم می‌گویند.

بعد از انجام کار اگر به مانند شکل ٦-۲۱۲، دوباره به قسمت Snapshots مراجعه کنید، گزینه‌های دیگر را می‌بینید که فعال شده‌اند، گزینه‌ی Restore snapshot برای برگشت دادن اطلاعات ماشین به آخرین Snapshot است که تهیه شده است، گزینه‌ی Manage snapshots برای مدیریت و انتخاب تاریخ مناسب برای برگشت است و گزینه‌ی Consolidate disks زمانی به کار می‌آید که از ماشین مورد نظر چندین snapshot ایجاد کرده باشید و برای اینکه این snapshotها با هم ادغام شوند و دیسک‌های زائدی که بعد از فعال کردن به وجود می‌آید حذف شوند کاربرد دارد، سعی کنید هر چند وقت یک بار این عملکرد را فعال کنید تا عملکرد ماشین‌مجازی بهبود پیدا کند که البته بر روی عملکرد ESXi هم بسیار موثر است.



شکل ۶- ۲۱۲ / ایجاد SnapShot

به مانند شکل ٦-۲۱۳، اگر وارد Manage Snapshots شوید، تمام مرحله‌هایی که از ماشین خود Snapshot تهیه کردید را مشاهده خواهید کرد، برای برگشت به تاریخ مشخص شده گزینه مورد نظر را انتخاب کنید و از نوار بالایی بر روی Restore snapshot کلیک کنید، توجه داشته باشید جمله You are here نشان دهنده مکان شما در آن Snapshot است که در شکل ٦-۲۱۳، نشان داده شده که ماشین مورد نظر روی Snap4 فعال است.

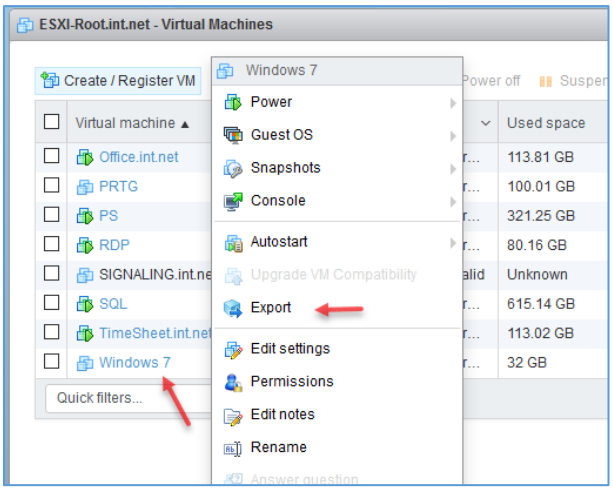


شکل ۶- ۲۱۳ / ایجاد SnapShot

www.takbook.com

۱۷-٤-۱-٦ ایجاد فایل Export از ماشین مجازی در ESXi

در این قسمت می‌خواهیم از ماشین مجازی خود یک فایل Export تهیه کنیم، که برای این‌کار به مانند شکل ٦-۲۱٤، اول از همه باید ماشین مورد نظر خود را خاموش کنید، و بعد از آن بر روی آن کلیک راست کنید و گزینه‌ی Export را انتخاب کنید.



شکل ۶- ۲۱۴ فایل *Export*

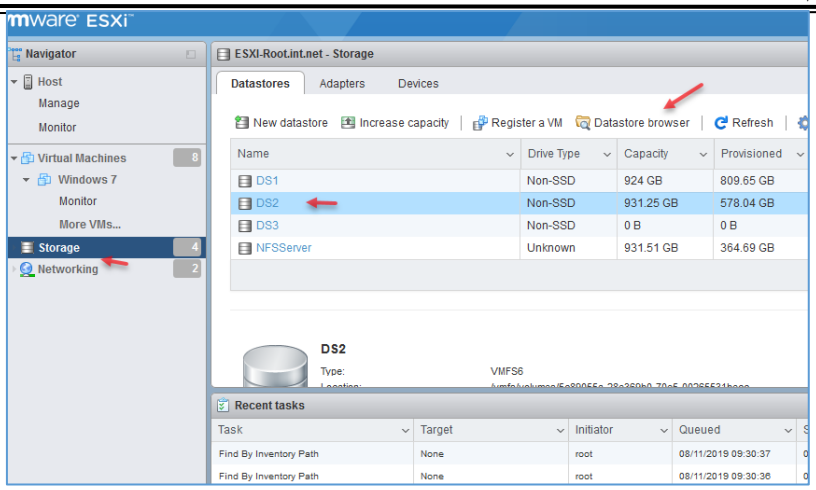
بعد از این کار یک فایل با پسوند ovf به همراه تعداد هارد دیسک‌هایی که در آن ماشین قرار دارد دانلود خواهد شد که البته مقدار زمان آن طولانی است، بعد از دانلود با کلیک بر روی فایل ovf نرم‌افزار VMware workstation اجرا شده و ماشین را می‌توانید بر روی آن Import کنید.



شکل ۶- ۲۱۵ فایل *Export*

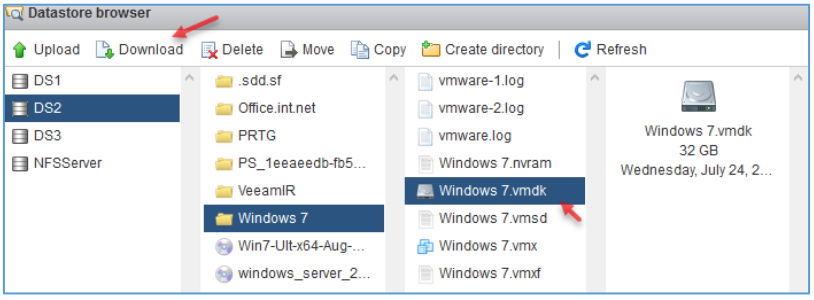
روش دیگر برای خروجی گرفتن از ماشین مجازی این است که به مانند شکل ٦-۲۱٦ وارد Storage شوید و بعد از انتخاب DataStore بر روی Datastore browser کلیک کنید.

www.takbook.com



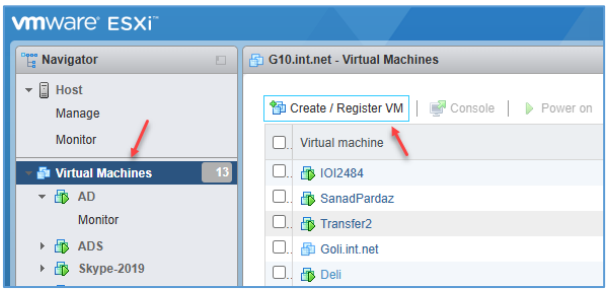
شکل ۶- ۲۱۶ فایل *Export*

در شکل ٦-۲۱۷، می‌توانید فولدر مربوط به ماشن مجازی خود را انتخاب و فایل‌های آن را به مانند شکل دانلود و در یک محل مشخص ذخیره کنید.



شکل ۶- ۲۱۷ فایل *Export*

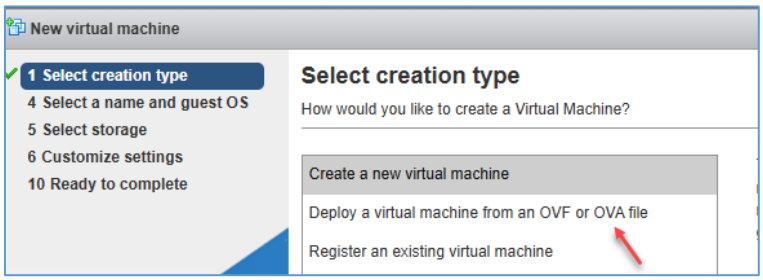
توجه داشته باشید برای اینکه فایل OVF را وارد ESXi کنیم می‌توانید به مانند شکل ٦-۲۱۸ بر روی Cerate کلیک کنید.



شکل ۶- ۲۱۸ *Import* کردن *OVF*

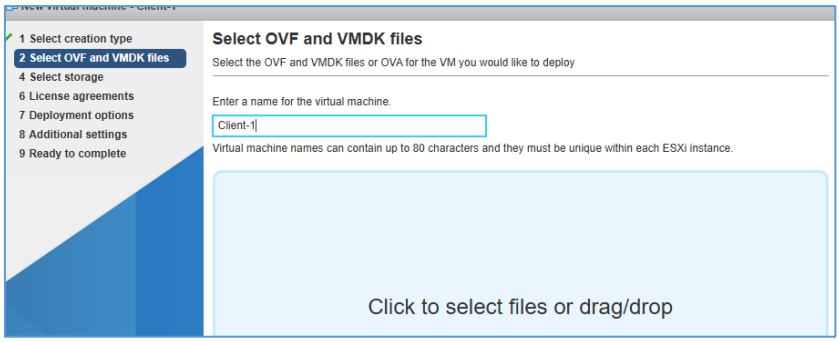
www.takbook.com

در شکل ٦-٢١٩ باید گزینه‌ی دوم را انتخاب کنید.



شکل ۶- ۲۱۹ Import کردن OVF

در شکل ٦-٢٢٠ باید فایل OVF خود را کشیده و در قسمت مشخص شده رها کنید و در ادامه ماشین مورد نظر را به لیست اضافه کنید.

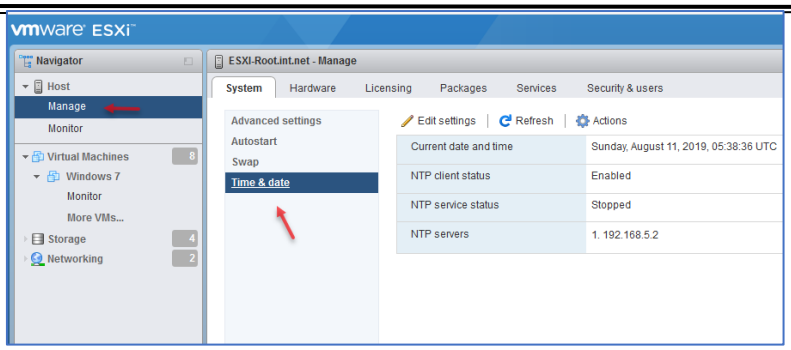


شکل ۶- ۲۲۰ Import کردن OVF

۱۸-٤-۱-٦ تنظیم زمان و تاریخ سرور

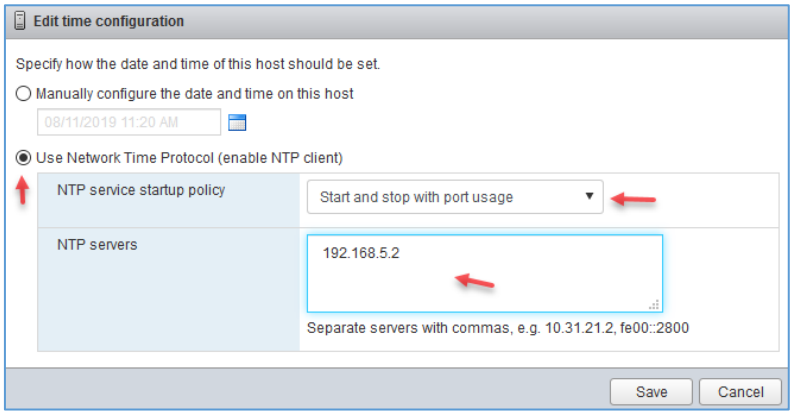
برای تنظیم تاریخ به مانند شکل ٦-٢٢١، از سمت چپ وارد Manage شوید و از تب System بر روی Time & data کلیک کنید، در این قسمت تاریخ و ساعت مشخص شده است که برای تنظیم آن باید بر روی Edit Settings کلیک کنید.

www.takbook.com



شکل ۶- ۲۲۱ تنظیم زمان و تاریخ

در شکل ٦-۲۲۲ می‌توانید به صورت دستی زمان را تنظیم کنید، که پیشنهاد خوبی نخواهد بود و بهتر است سرویس NTP یا همان Network Time Protocol را در شبکه فعال کنید و ESXi را به آن متصل کنید. برای اینکه سرور از یک سرویس NTP برای دریافت زمان و تاریخ استفاده کند باید به مانند شکل ٦-۲۲۲، گزینه‌ی Use Network Time Protocol را انتخاب کنید و در صفحه باز شده آدرس سرور NTP خود را وارد کنید، اصولاً سرویس NTP بر روی سرور دومین راه‌اندازی می‌شود تا سیستم‌ها به صورت خودکار زمان خود را با آن تنظیم کنند.



شکل ۶- ۲۲۲ تنظیم زمان و تاریخ

نکته مهم : هیچ وقت سرور NTP نباید به عنوان یک سرور مجازی در درون خود ESXi فعال باشد و بهتر است یک سرور فیزیکی دیگر به صورت جداگانه باشد، در غیر این صورت ساعت و تاریخ سرور ESXi بر روی ماشین‌ها تاثیر خواهد داشت و ماشین‌ها از سرور ESXi خود اطلاعات دریافت می‌کنند و این می‌تواند برای شبکه شما مشکل‌ساز باشد.

در شکل ٦-۲۲۲، سه گزینه برای فعال کردن سرویس NTP وجود دارد که توضیح آن به صورت زیر می‌باشد:

www.takbook.com

Start and stop with port usage

این گزینه بستگی به تنظیمات امنیتی که در شبکه یا همان فایروال خود انجام داده اید فعال یا غیرفعال خواهد شد.

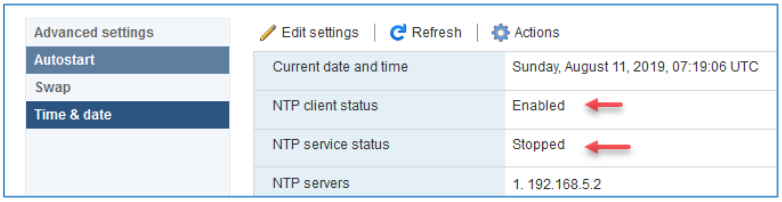
Start and stop with host

این قسمت به ماشین مجازی مربوط می‌شود و هر موقع که ماشین مجازی شما فعال شود سرویس NTP هم فعال خواهد شد.

Start and stop manually

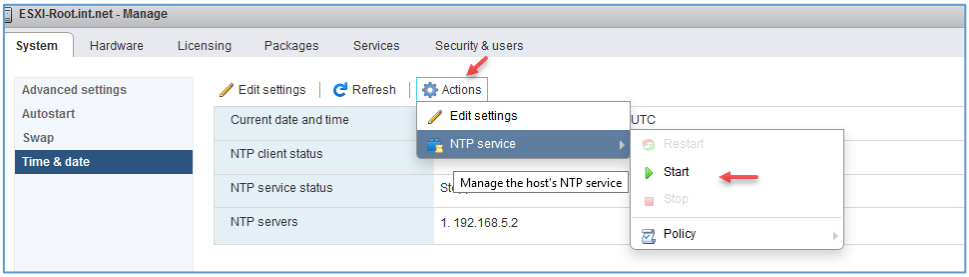
به صورت دستی سرویس را فعال و غیر فعال می‌کنیم.

توجه داشته باشید، سرویس NTP به دو صورت کلاینت و سرور است که سرویس کلاینت برای دریافت اطلاعات زمان و تاریخ از دیگر سرورها است و سرور هم برای فعال‌سازی خود ESXi به عنوان سرور NTP می‌باشد که با این کار تمام ماشین‌های زیر مجموعه آن از ESXi دستور می‌گیرند.



شکل ۶- ۲۲۳ تنظیم زمان و تاریخ

به مانند شکل ٦-٢٢٤، برای فعال کردن NTP Server باد بر روی منوی Action کلیک کنید و از قسمت NTP Service گزینه‌ی Start را انتخاب کنید، برای مشخص کردن حالت فعال بودن سرویس می‌توانید از قسمت Policy سه گزینه‌ی مورد نظر را که در بالا بررسی کردیم را انتخاب کنید.



شکل ۶- ۲۲۴ تنظیم زمان و تاریخ

۱۹-٤-۱-٦ روشن و خاموش شدن ماشین مجازی به صورت اتوماتیک

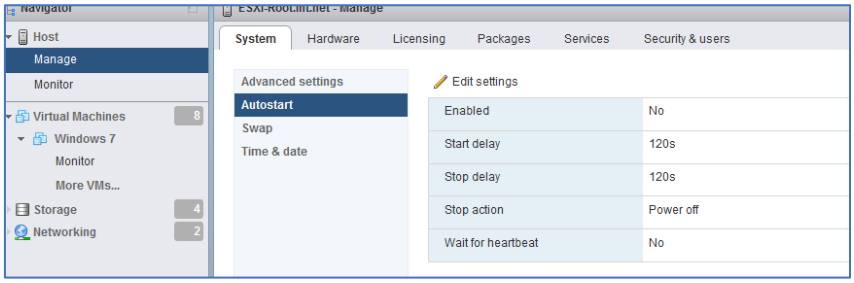
یکی از ویژگی‌های خوب ESXi و سیستم‌عامل‌هایی از این دست این است که بعد از روشن شدن سرور تنظیمی دارند که می‌توانید ماشین مجازی‌های داخل آن را به صورت اتوماتیک روشن کنید و به همین صورت در زمان خاموش شدن به ترتیب ماشین‌های مجازی خاموش می‌شوند، یعنی اگر در اتاق سرور

www.takbook.com

هستید و به صورت فیزیکی به سرور دسترسی دارید، اگر بر روی دکمه Power که بر روی سرور قرار دارد فشار دهید ESXi اول و به ترتیبی که ما مشخص می‌کنیم ماشین‌ها را خاموش می‌کند و بعد خود هسته ESXi خاموش می‌شود، که این که از صدمه دیدن به ماشین و DataStore آن جلوگیری می‌کند.

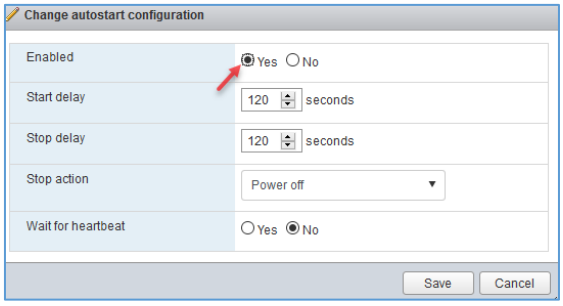
نکته: در اتاق سرور حتماً از دستگاه UPS برای فعال نگه داشتن سرور در موقع قطعی برق استفاده کنید تا صدمه‌ای به سرویس‌ها و فایل‌های شما وارد نشود، سیستم عامل ESXi به قطعی برق حساس است و در موارد پیش آمده که کل اطلاعات از دست رفته است.

به مانند شکل ٦-٢٢٥، برای ورود از سمت چپ وارد Manage شوید و در صفحه باز شده گزینه‌ی Autostart را از تب System انتخاب کنید.



شکل ۶- ۲۲۵ روشن و خاموش کردن ماشین مجازی

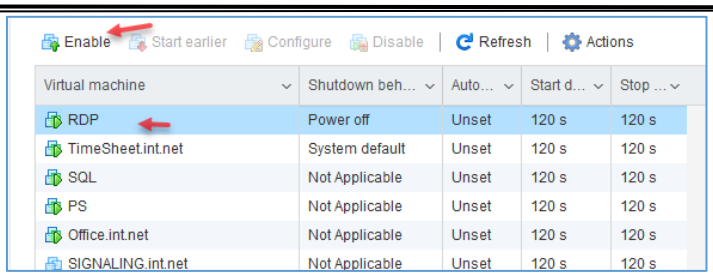
توجه داشته باشید برای فعال کردن این سرویس در شکل ٦-٢٢٦، بر روی Edit Settings کلیک کنید و در صفحه باز شده در قسمت Enabled گزینه‌ی Yes را انتخاب کنید و بر روی Save کلیک کنید.



شکل ۶- ۲۲۶ روشن و خاموش کردن ماشین مجازی

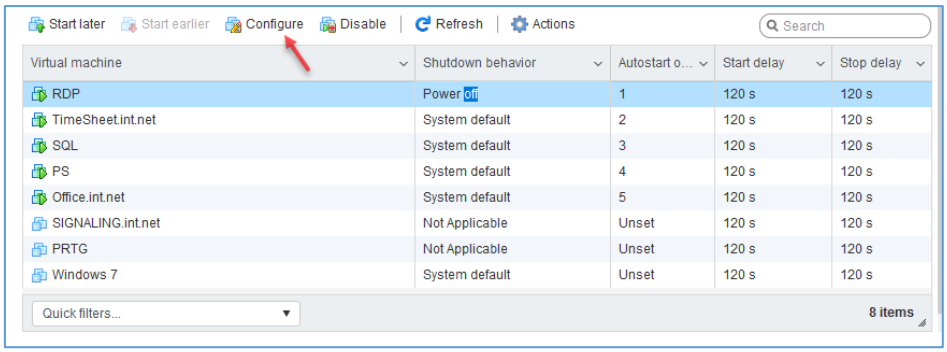
لیست تمام ماشین‌هایی که در ESXi موجود است در شکل ٦-٢٢٧ لیست شده است و برای اینکه ماشین‌های به صورت اتوماتیک خاموش و روشن شوند باید آنها را انتخاب و بر روی گزینه‌ی Enable کلیک کنید.

www.takbook.com



شکل ۶- ۲۲۷ روشن و خاموش کردن ماشین مجازی

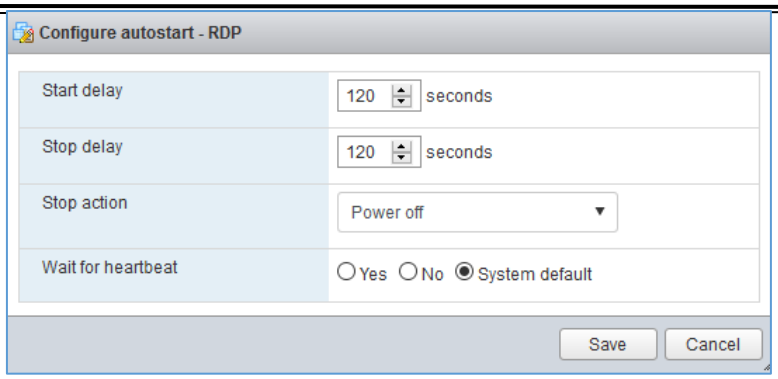
توجه داشته باشید به صورت پیش‌فرض مقدار ۱۲۰ ثانیه برای اجرای هر ماشین زمان مشخص شده است یعنی اینکه طبق اولویتی که در شکل ٦-۲۲۸، از ۱ تا ۵ مشخص شده است، ماشین‌ها روشن و یا خاموش می‌شوند، برای تنظیم این مورد باید ماشین مورد نظر را انتخاب و بر روی Configure کلیک کنید.



شکل ۶- ۲۲۸ روشن و خاموش کردن ماشین مجازی

در شکل ٦-۲۲۹، می‌توانید مقدار زمان روشن و خاموش شدن ماشین را مشخص کنید که همان‌طور که اشاره کردم مقدار آن ۱۲۰ در نظر گرفته شده است که می‌توانید آن را کمتر یا بیشتر کنید، در قسمت Stop action می‌توانید مشخص کنید که در زمان متوقف شدن ماشین چه عملیاتی روی آن انجام شود، مانند Power off, suspend, shutdown، در قسمت آخر گزینه‌ی Wait for heartbeat وجود دارد که معنی آن ضربان قلب است، این گزینه اگر فعال باشد ماشین تا زمانی که ماشین اول به وضع ایده‌ال نرسیده ماشین دوم شروع به کار نمی‌کند، ماشین اول بعد از اجرای کامل از طریق این گزینه به ماشین دوم خبر می‌دهد و آن اجرا می‌شود.

www.takbook.com



شکل ۶- ۲۲۹ روشن و خاموش کردن ماشین مجازی

نکته: همه سرورهایی که برای اتاق سرور طراحی می‌شوند به صورت اتوماتیک با وصل شدن برق اجرا می‌شوند و ماشین هم طبق روالی که تعریف کردیم به صورت اتوماتیک اجرا خواهد شد، اگر چنانچه از یک کیس معمولی استفاده می‌کنید، این سیستم‌ها بعد از خاموش شدن اجرا نخواهد شد و باید تنظیمات آن را در Bios تغییر دهیم، بیشتر Bios های امروزی گزینه‌ی با نام Power Management Setup دارد که در آن گزینه‌ی AC BACK Function را باید فعال و اطلاعات را ذخیره کنید، با این کار سیستم بعد از متصل شدن برق روشن خواهد شد.

توجه داشته باشید اگر بر روی ESXi ماشین مجازی مربوط به Active Directory قرار دارد و کاربران از این سرور اطلاعات خود را دریافت می‌کنند بهتر است که در لیست بالاتر از همه سرورها قرار داشته باشند و اول از همه روشن شوند تا کاربران به مشکل روبرو نشوند.

۲۰-٤-۱-٦ بررسی Swap در ESXi

با افزایش استفاده از مجازی‌سازی، تقاضاها برای استفاده از منابع سخت‌افزاری مورد نظر افزایش می‌یابد و در این بین باید سیستمی باشد تا بتواند این تقاضاها را مدیریت کند.

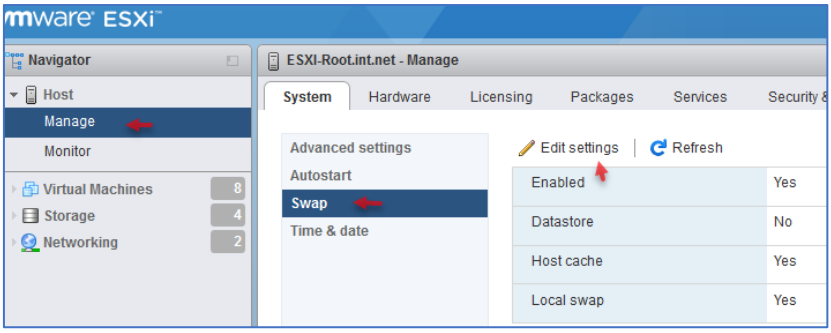
سیستم‌عامل ESXi یکی از کارآمدترین و پایدارترین سیستم‌عامل‌ها در حفظ پایداری ماشین‌های مجازی می‌باشد و سعی می‌کند به صورت درست منابع را بین ماشین‌ها تقسیسم کند، در این بین حافظه رم بیشترین درگیری را بین ماشین‌های مجازی دارد و طبق تخصیصی که به ماشین مورد نظر دادید آن ماشین به همان اندازه از منابع استفاده می‌کند البته اگر ماشینی به حافظه بیشتر نیاز داشته باشد و چنانچه حافظه کلی خالی باشد آن حافظه به عنوان مهمان به ماشین تخصیص داده می‌شود.

حال اگر کل فضای رم مصرف شده باشد و ماشین‌ها باز نیاز به حافظه رم بیشتری داشته باشند چه باید کرد؟

www.takbook.com

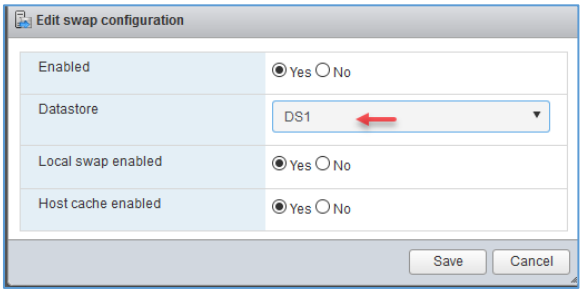
برای حل این مشکل باید از تکنولوژی Swap بین رم و هارد استفاده کرد، در این سیستم اگر نیاز به حافظه برای اجرای ماشین مجازی باشد، با تنظیمی که انجام می‌دهیم اطلاعات ماشین مجازی بر روی هارد دیسک انتقال یا به اصطلاح Swap می‌شوند و ماشین به کار خود ادامه می‌دهد ولی مشکلی که در این بین وجود دارد این است که سرعت هارد دیسک و رم کاملاً با هم متفاوت است و همین امر باعث کاسته شدن سرعت ماشین مجازی خواهد شد که برای حل درصد کمی از این مشکل باید از هارددیسک‌های SSD که از سرعت خوبی برخوردار هستند استفاده کرد.

به مانند شکل ٦-٢٣٠، برای فعال‌سازی Swap باید وارد Manage شوید و گزینه‌ی Swap را از تب System انتخاب کنید، این گزینه به صورت پیش‌فرض فعال است و برای تنظیم آن بر روی Edit settings کلیک کنید.



شکل ۶- ۲۳۰ روشن و خاموش کردن ماشین مجازی

در شکل ٦-٢٣١، در قسمت Datastore می‌توانید مشخص کنید که کدام Datastore به عنوان حافظه دوم انتخاب شود، توجه داشته باشید اگر Data Store هم پر شود از فضای ماشین مجازی مورد نظر استفاده خواهد شد.



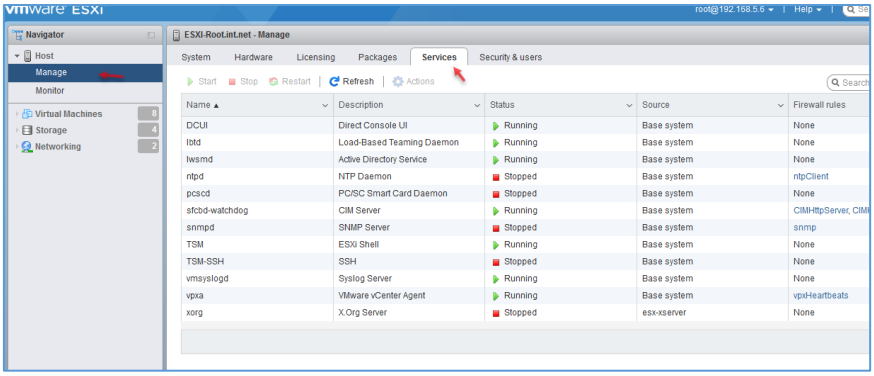
شکل ۶- ۲۳۱ روشن و خاموش کردن ماشین مجازی

٢١-٤-١-٦ فعال‌سازی سرویس‌ها در ESXi 8

سیستم عامل ESXi دارای سرویس‌های مختلفی است که برای کاربردهای مختلفی طراحی شدند که در این قسمت آنها را فعال و یا غیر فعال می‌کنیم.

www.takbook.com

به مانند شکل ٦-۲۳۲، از قسمت Manage وارد تب Services شوید، در این قسمت سرویس‌های مختلفی وجود دارند که به صورت پیش‌فرض فعال و غیرفعال شده‌اند، که در جدول ٦-۱ توضیحات آنها را مشاهده می‌کنید.



شکل ۶- ۲۳۲ روشن و خاموش کردن ماشین مجازی

جدول ۶- ۱ سرویس‌های ESxi

نام سرویس	توضیحات	پیش‌فرض
DCUI	برای ارتباط به ESXi از طریق کنسول‌های دیگر مانند Vmware Workstation و...	Running
lbtd	این سرویس مربوط به Load-Based Teaming است که در صورت نیاز فعال خواهد شد.	Running
lwsmd	هنگامی که Active Directory را به ESXi متصل می‌کنید این سرویس به صورت اتوماتیک فعال می‌شود.	Running
ntpd	مربوط به سرویس Network Time است که به صورت پیش‌فرض غیر فعال است.	Stopped
pcscd	این سرویس مربوط به کارت‌های هوشمند است که اگر نیاز به فعال‌سازی کارت هوشمند باشد فعال خواهد شد.	Stopped
sfcbd-watchdog	سرویسی است برای نرم‌افزارهای خدمات عمومی که مخفف CIM است.	Running

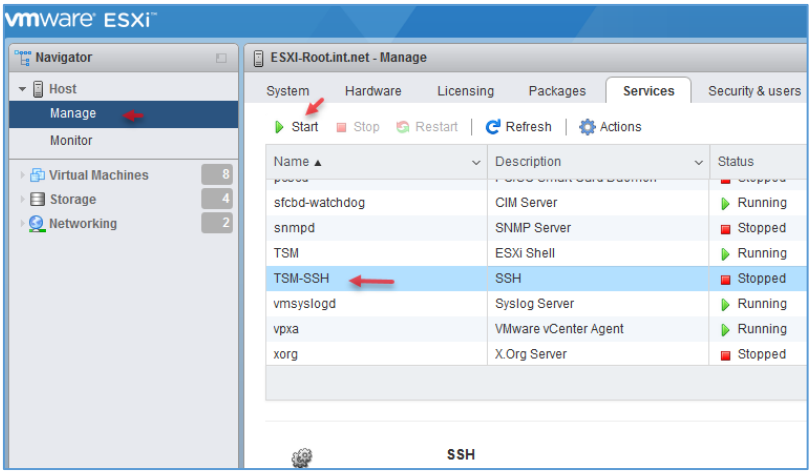
www.takbook.com

snmpd	مربوط به سرویس SNMP برای مانیتور کردن کامل ESXi می‌باشد.	Stopped
TSM	شامل یک سری از دستورات برای ESXi است که می‌توانید آنها را از طریق رابط محلی استفاده کنید.	Stopped
TSM-SSH	این سرویس هم برای ارتباط از راه دور با سرویس SSH است و دستورات را می‌توانید در آن اجرا کنید.	Stopped
vmsyslogd	برای متصل شدن به سرویس دهنده‌های Syslog سرور است تا تمام رویدادهای مربوط به ESXi در آن ثبت شود.	Running
vpxa	به VMware VCenter اجازه می‌دهد تا به ESXi از راه دور متصل شود.	Running
xorg	سرویس برای گرافیک‌های سه بعدی در داخل ماشین‌های مجازی مورد استفاده قرار می‌گیرد.	Stopped

۲۲-٤-۱-٦ فعال‌سازی ارتباط از راه دور از طریق SSH

در مواردی نیاز است که بتوانید از طریق SSH به کنسول ESXi متصل شوید و تنظیماتی را روی آن اعمال کنید، مثلاً برای آپدیت ESXi باید از طریق SSH اقدام کنید.

برای فعال‌سازی سرویس SSH به مانند شکل ٦-۲۳۳، وارد Services شوید و از لیست موجود گزینه‌ی TSM-SSH را انتخاب کنید و از نوار ابزار بالای آن بر روی Start کلیک کنید.

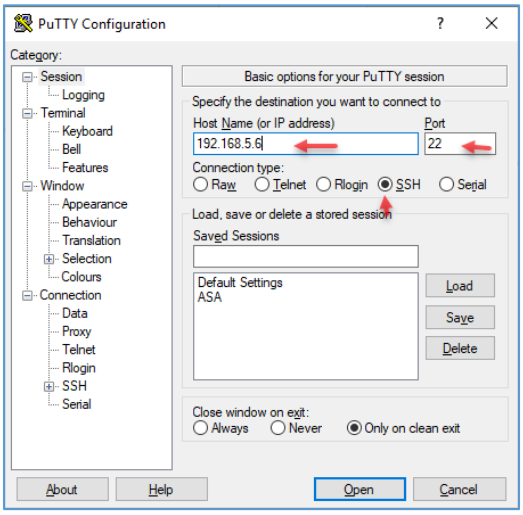


شکل ۶- ۲۳۳ فعال‌سازی SSH

www.takbook.com

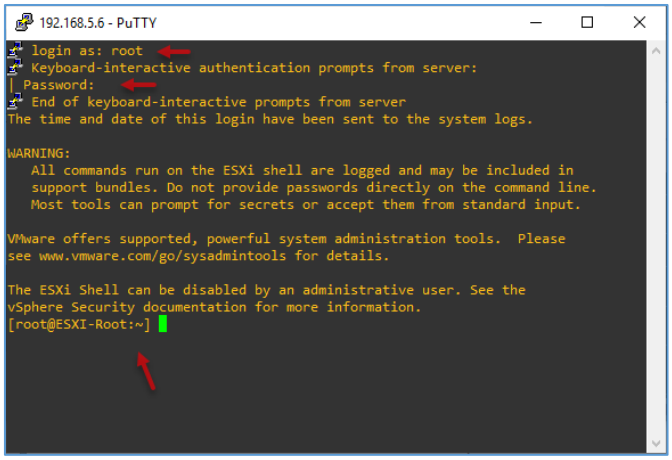
برای ارتباط از طریق SSH نرم‌افزارهای زیادی وجود دارد که می‌توان به Putty و یا Secure CRT اشاره کرد، در این قسمت نرم‌افزار Putty را انتخاب و دانلود می‌کنیم.

در شکل ٦-٢٣٤، گزینه‌ی SSH را انتخاب و آدرس سرور ESXi را وارد کنید، توجه داشته باشید پورت ارتباطی SSH به صورت پیش‌فرض ۲۲ است که در این نرم‌افزار هم مشاهده می‌کنید، بر روی Open کلیک کنید.



شکل ۶- ۲۳۴ فعال‌سازی SSH

بعد از باز شدن صفحه شکل ٦-٢٣٥، باید نام کاربری و رمز عبور مربوط به ESXi را وارد کنید و به Shell دسترسی پیدا کنید.

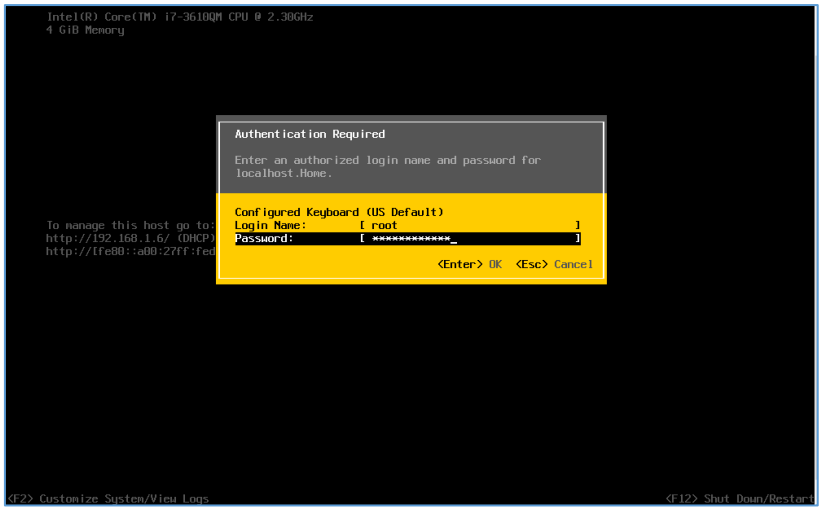


شکل ۶- ۲۳۵ فعال‌سازی SSH

www.takbook.com

در ادامه در جاهایی که نیاز به دستورات Shell است از این قسمت استفاده خواهیم کرد.

راه دیگری هم برای فعال سازی SSH وجود دارد و آن هم این است که از طریق کنسول اصلی ESXi اقدام کنیم، به همین منظور اگر از سرور فیزیکی استفاده می‌کنید باید پشت سیستم قرار بگیرید و یا اگر از سیستم مجازی استفاده می‌کنید باید وارد آن شوید و به مانند شکل ٦-٢٣٦، کلید F2 را فشار دهید و برای ورود به تنظیمات باید نام کاربری و رمز عبور را وارد کنید.



شکل ۶- ۲۳۶ فعال‌سازی SSH

در شکل ٦-٢٣٧، باید وارد قسمت Troubleshooting Options شوید.



شکل ۶- ۲۳۷ فعال‌سازی SSH

www.takbook.com

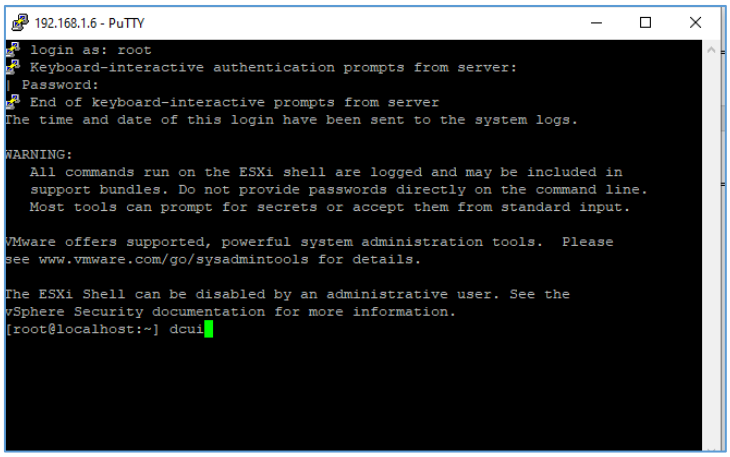
در شکل ٦-۲۳۸، باید Enable SSH با فشار Enter تبدیل به Disabled SSH شود تا این سرویس بر روی ESXi فعال شود. این هم یک روش دیگر برای فعال‌سازی سرویس SSH بود که می‌تواند در مواردی کمک کننده باشد.



شکل ۶- ۲۳۶ فعال‌سازی SSH

نکته: در صورتی که فقط نیاز به این سرویس دارید آن را فعال کنید و در غیر این صورت آن را غیرفعال کنید.

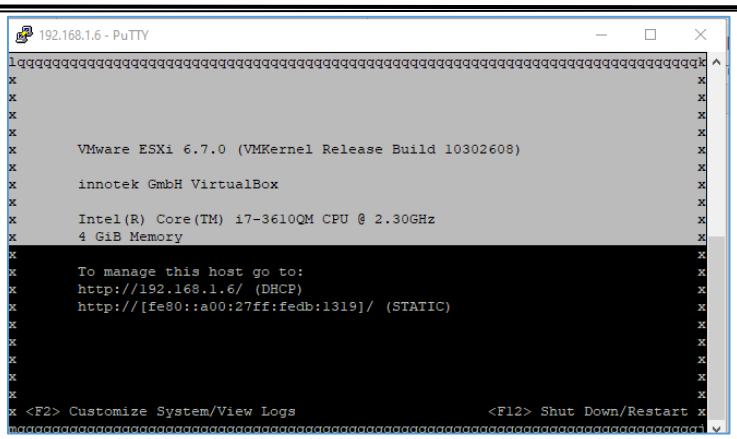
برای اینکه بتوانید به صفحه اصلی ESXi متصل شوید و تنظیمات کلی آن را مشاهده کنید باید به مانند شکل ٦-۲۳۹، از طریق SSH به سرور متصل شوید و از دستور dcui برای این منظور استفاده کنید.



شکل ۶- ۲۳۷ فعال‌سازی SSH

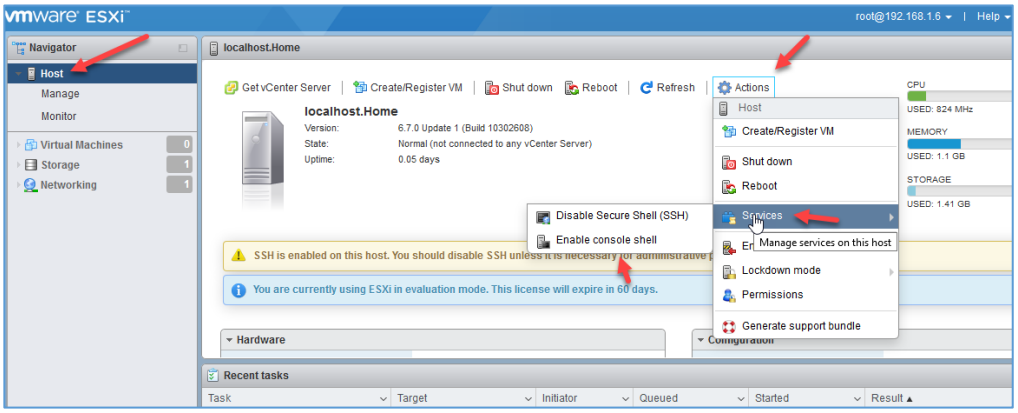
همان‌طور که در شکل ٦-۲٤۰، مشاهده می‌کنید، صفحه کنسول مورد نظر از طریق SSH باز شده است و دیگر نیاز نیست که پشت سیستم قرار بگیرید.

www.takbook.com



شکل ۶- ۲۳۸ فعال‌سازی SSH

روش دیگری هم برای فعال یا غیرفعال کردن سرویس SSH وجود دارد که باید به مانند شکل ٦-٢٤١ از قسمت Action این کار را انجام دهید.



شکل ۶- ۲۳۹ فعال‌سازی SSH

٦-١-٤-٢٣ آپدیت کردن ESXi

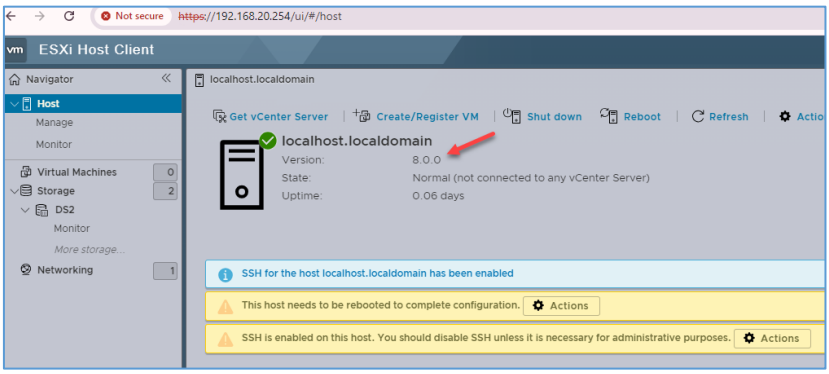
در مدت زمان مشخصی شرکت‌های ارائه دهنده نرم‌افزار به خاطر ارتقاء نرم‌افزار خود و رفع ایراداتی که از آن گرفته می‌شود تصمیم به ارائه آپدیت نرم‌افزار یا ارائه نسخه جدید آن می‌کنند که می‌تواند با سیستم شما هم‌خوای بهتر و کارایی خوبی داشته باشد و ایرادات فنی و امنیتی آن را برطرف کند.

تذکر مهم: قبل از اینکه سیستم‌عامل ESXi را آپدیت کنید بهتر است از همه ماشین‌های مجازی یک پشتیبان تهیه کنید، که بهترین نرم‌افزار پشتیبانی هم Veeam می‌باشد که در همین کتاب و در فصل سیزدهم توضیح داده شده است.

www.takbook.com

برای انجام آپدیت می‌توانید به صورت مستقیم از خود سایت VMware عملیات دانلود را انجام دهید و یا از سایت‌های ایرانی مانند digiboy.ir استفاده کنید.

اگر به شکل ٦-٢٤٢ توجه کنید ورژن این ESXi برابر است با 8.0 است که می‌خواهیم به ورژن بالاتر آپدیت کنیم.

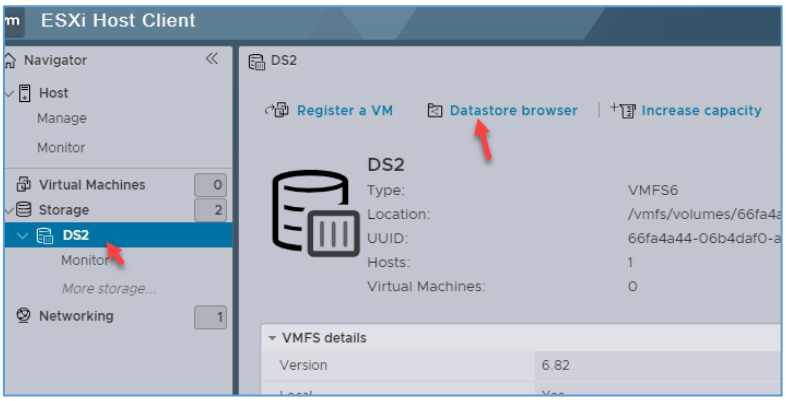


شکل ۶- ۲۴۰ آپدیت کردن ESXi

برای دانلود آخرین آپدیت در این تاریخ که ورژن 8.0 U3 آن است، می‌توانید از لینک زیر استفاده کنید:
https://fdn.digiboy.ir/dlir-s3/VMware-ESXi-8.0U3-24022510-depot.zip

توجه داشته باشید فایل آپدیت باید با نسخه نصب شده بر روی سرور فیزیکی یا مجازی یکی باشد تا با مشکلی روبرو نشوید مثلاً برای سرورهای HP باید نسخه مربوط به آن را دانلود کنید.

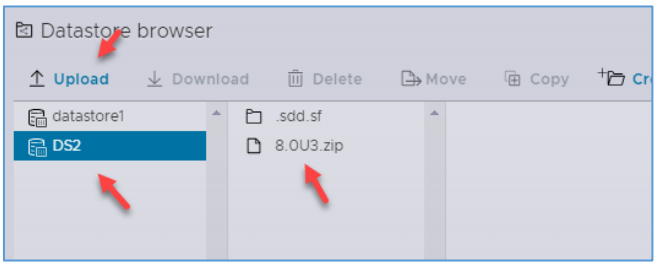
بعد از دانلود فایل مورد نظر باید آن را در ESXi خود آپلود کنید تا بتوانیم در ادامه از فایل آپدیت استفاده کنیم، برای این کار به مانند شکل ٦-٢٤٣ بر روی Datastore Browser کلیک کنید.



شکل ۶- ۲۴۱ آپدیت کردن ESXi

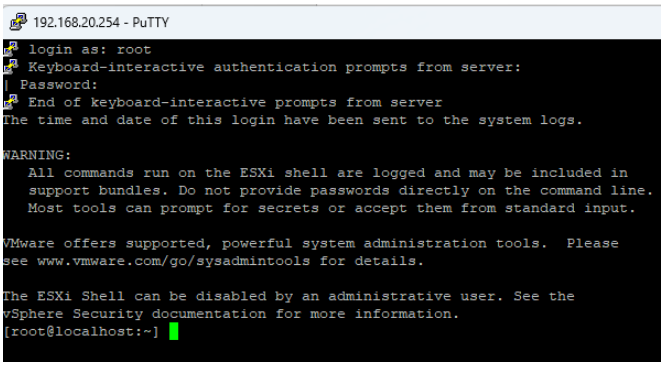
www.takbook.com

در شکل ٦-٢٤٤ بر روی Upload کلیک کنید و فایل مورد نظر را در Datastore آپلود کنید.



شکل ۶- ۲۴۲ آپدیت کردن ESXi

بعد از آپلود فایل باید از طریق SSH به سرور ESXi متصل شد که همان‌طور در قسمت قبل بررسی کردیم این کار را از طریق نرم‌افزار Putty انجام می‌دهیم.

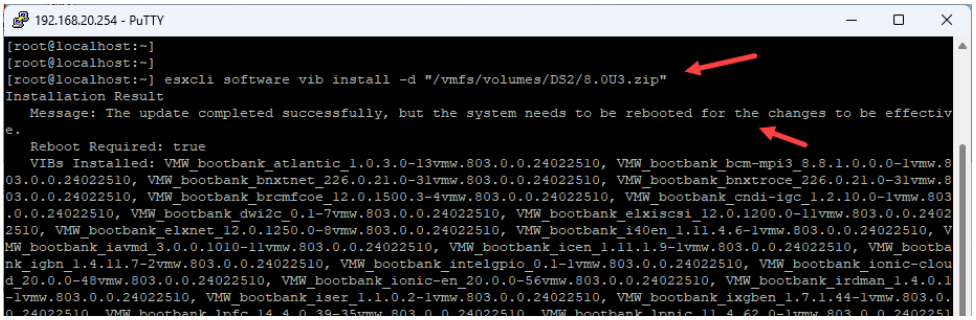


شکل ۶- ۲۴۳ آپدیت کردن ESXi

بعد از متصل شدن از طریق Putty دستور زیر را در آن اجرا کنید.

esxcli software vib install -d "/vmfs/volumes/DS2/8.0U3.zip"

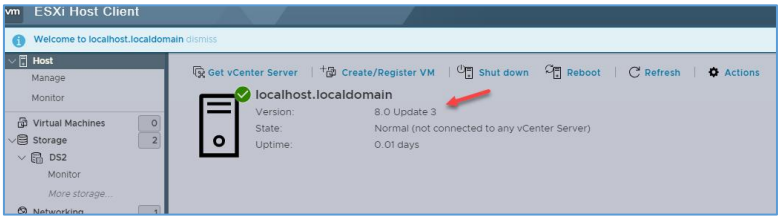
در دستور بالا باید به جای datastore1 نام DataStore خود را که فایل آپدیت را در آن کپی کردید بنویسید و در قسمت قرمز رنگ باید نام فایل خود را وارد کنید و دستور را به مانند شکل ٦-٢٤٦ اجرا کنید.



شکل ۶- ۲۴۴ آپدیت کردن ESXi۱

www.takbook.com

بعد از اجرای کامل دستور، سرور ESXi را یک بار Restart کنید تا آپدیت جدید بر روی آن اعمال شود. همان‌طور که در شکل ٦-٢٤٧مشاهده می‌کنید ESXi به ورژن 8.0U3 آپدیت شده است.



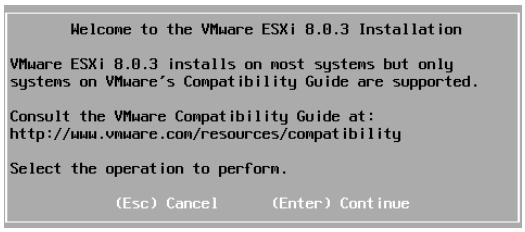
شکل ۶- ۲۴۵ آپدیت کردن ESXi

روش دیگری هم برای آپگرید کردن ESXi وجود دارد و آن هم استفاده از فایل اصلی که همان ISO است و بوت کردن آن فایل در ESXi.

برای دانلود فایل ISO می‌توانید از لینک زیر استفاده کنید:

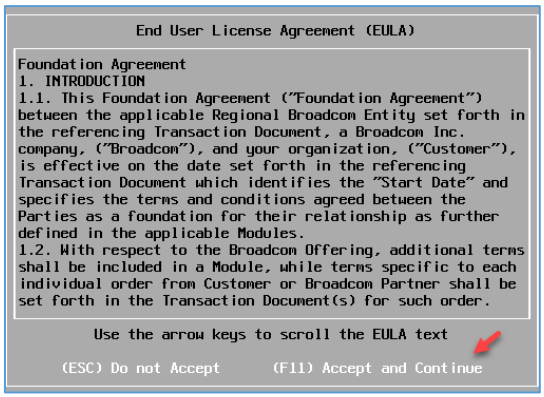
https://fdn.digiboy.ir/dlir-s3/VMware-VMvisor-Installer-8.0U3-24022510.x86_64.iso

بعد از دانلود، آن را بر روی DVD یا فلش به صورت بوت قرار دهید و از روی سرور Boot کنید، توجه داشته باشید این کار را باید بر روی سروری که ESXi 8.0 نصب است انجام دهید، در شکل ٦-٢٤٨ بر روی Enter فشار دهید.



شکل ۶- ۲۴۶ آپدیت کردن ESXi

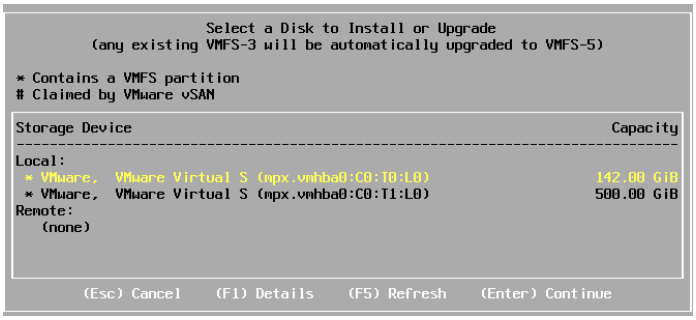
در شکل ٦-٢٤٩ بر روی F11 فشار دهید.



شکل ۶- ۲۴۷ آپدیت کردن ESXi

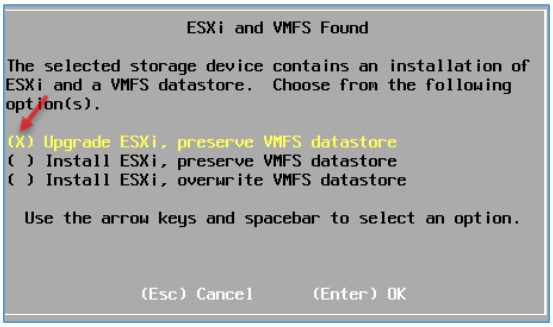
www.takbook.com

در شکل ٦-۲۵۰، هارد دیسکی را انتخاب کنید که نسخه قبلی ESXi بر روی آن قرار دارد و بعد بر روی Enter فشار دهید.



شکل ۶- ۲۴۸ آپدیت کردن ESXi

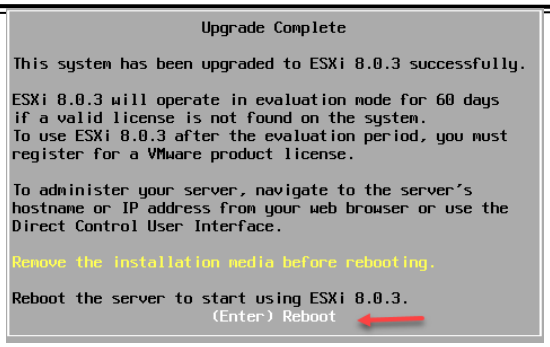
در شکل ٦-۲۵۱، سه گزینه به شما نمایش داده می‌شود که گزینه‌ی اول برای آپگرید کردن ESXi قدیمی به ورژن جدید است، گزینه‌ی دوم برای حذف ESXi قبلی و نصب ESXi جدید با این تفاوت که اطلاعات Datastore قبلی حذف نمی‌شود و به ESXi جدید انتقال داده خواهند شد، گزینه‌ی سوم هم برای حذف کامل ESXi قبلی به همراه تمام اطلاعاتی که در DataStore آن قرار داشت، توجه داشته باشید گزینه‌ی سوم مهم است و باید احتیاط کنید، چون با انتخاب آن هر چیزی که در Datastore قرار داشته باشد پاک خواهد شد. بعد از انتخاب گزینه‌ی اول باید بر روی F11 برای آپگرد شدن فشار دهید.



شکل ۶- ۲۴۹ آپدیت کردن ESXi

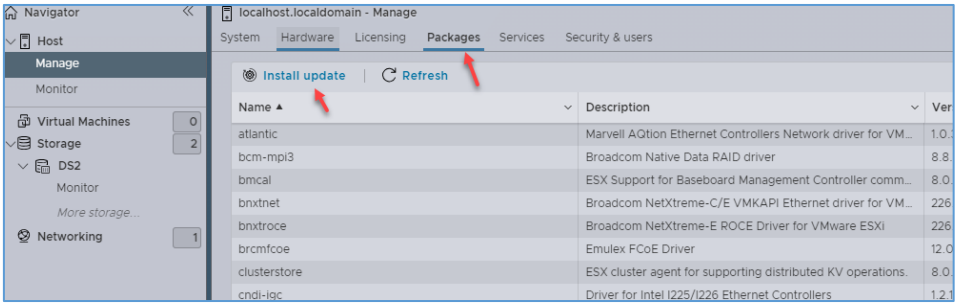
همان‌طور که در شکل ٦-۲۵۲، مشاهده می‌کنید نسخه 8.0.3 آپدیت شده و باید سرور را Restart کنید تا تنظیمات اعمال شود.

www.takbook.com



شکل ۶- ۲۵۰ آپدیت کردن ESXi

روش دیگری برای آپدیت بسته‌های ESXi وجود دارد و آن هم این است که به مانند شکل ٦-۲۵۳، باید وارد Manage شوید و از تب Packages بر روی Install update کلیک کنید، توجه داشته باشید که پسوند این نوع فایل VIB و باید از طریق یک آدرس اینترنتی صدا زده شود، در صورت نیاز این موضوع را هم بررسی خواهیم کرد.



شکل ۶- ۲۵۱ آپدیت کردن ESXi

پس در این بخش یاد گرفتیم که چگونه ESXi خود را به ورژن بالاتر آپدیت کنیم، همان‌طور که گفتیم قبل از هر کاری باید یک پشتبان از کل اطلاعات هارد دیسک موجود در سرور ESXi تهیه کنید تا مشکلی بعد از آپگرید کردن پیش نیاید.

٦-۱-٤-۲٤ کار با ISCSI در ESXi

ISCSI مخفف کلمه Internet Small Computer Systems Interface است که یک استاندارد شبکه ذخیره‌سازی بر مبنای IP است که برای ارتباط با data storage یا همان ذخیره‌سازها است. ISCSI برای تسهیل در انتقال داده‌ها در محیط اینترانت مورد استفاده قرار می‌گیرد و می‌توان در مسافت‌های طولانی هم از آن استفاده کرد، استاندارد ISCSI دارای دو بخش کلی است که در زیر آن را بررسی می‌کنیم:

Initiator

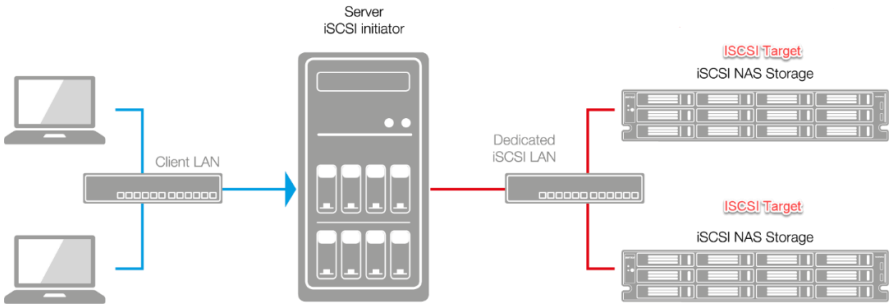
www.takbook.com

به سیستم سخت‌افزاری یا نرم‌افزاری گفته می‌شود که نقش واسط میان کاربران (کلاینت‌ها) و ذخیره‌سازهای سازمان را ایفا می‌کند. این سیستم دستورات iSCSI را از طریق پروتکل IP و معمولاً از طریق کابل منتقل می‌کند.اصولاً این سیستم را می‌توان بر روی یک سرور که بر روی آن نرم‌افزار ISCSI وجود دارد راه‌اندازی کرد مانند ویندوز سرور که در این بخش به آن خواهیم پرداخت.

Target

به سرورهای ذخیره‌ساز مانند NAS و SAN Storage اشاره دارد که Initiator برای ارائه فضای ذخیره‌سازی از آن استفاده خواهد کرد که در شکل ٦-٢٥٤ این دو موضوع را مشاهده می‌کنید.

یکی از ویژگی‌های مهم سیستم‌های ISCSI استفاده از Authentication برای احراز هویت است که امنیت اطلاعات را بسیار افزایش خواهد داد، در ادامه نحوه راه‌اندازی آن را با هم بررسی خواهیم کرد.



شکل ۶- ۲۵۲ ISCSI در ESXi

برای شروع کار باید به صورت زیر مراحل کار را پیش ببریم تا به عملکرد بهتری دست پیدا کنیم.

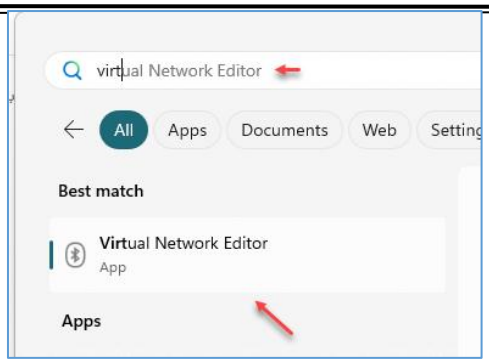
توجه داشته باشید برای راه‌اندازی این سرویس یک ویندوز سرور ۲۰۲۲ داریم که هم نقش Initiator و هم نقش Target را بازی می‌کند که این دو سرویس به یک سرور ESXi متصل می‌شود که نحوه‌ی تنظیم آنها را در ادامه با هم بررسی می‌کنیم.

تنظیم کارت شبکه در ESXi

برای اینکه سرور ISCSI را به سرور ESXi متصل کنیم نیاز به یک کارت شبکه مجزا داریم تا اطلاعات بدون ایجاد ترافیک در شبکه اصلی سرور بتواند ردوبدل شود.

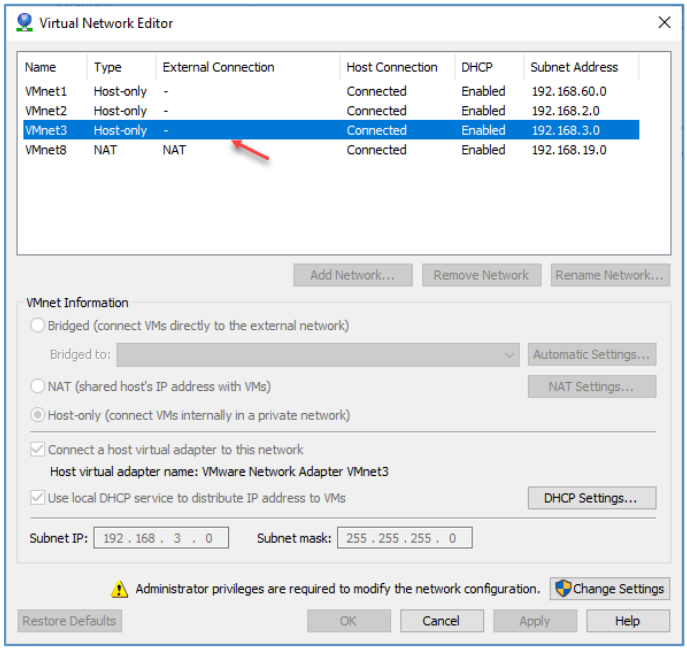
چون سرور ESXi به صورت مجازی در VMware Workstation ایجاد شده به مانند شکل ٦-٢٥٥ وارد Virtual Network Editor در ویندوز خود شوید.

www.takbook.com



شکل ۶- ۲۵۳ ISCSI در ESXi

در شکل۶-۲۵۶، باید بر روی Add Network کلیک کنید و یک کارت شبکه مجازی به لیست اضافه کنید، توجه داشته باشید برای فعال کردن گزینه‌ها باید بر روی Change Settings کلیک کنید.

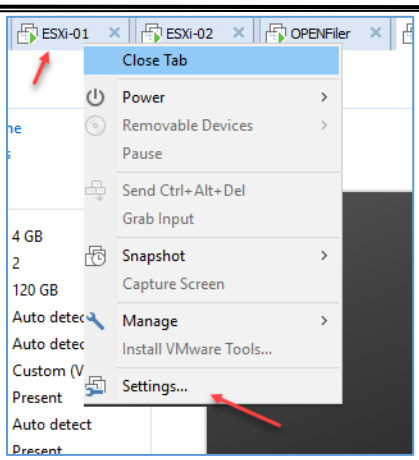


شکل ۶- ۲۵۴ ISCSI در ESXi

نکته: این کارت شبکه هم باید به سرور ESXi متصل شود و هم به سرور ویندوز ۲۰۲۲ تا بتوانیم بین آنها یک ارتباط ایجاد کنیم.

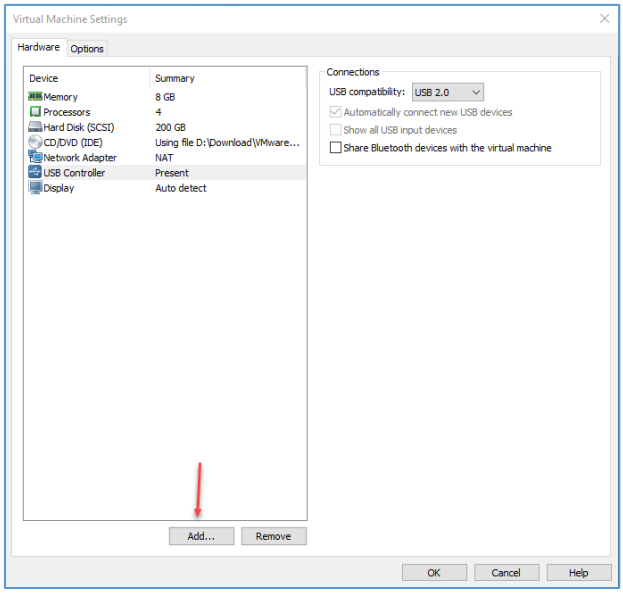
در ادامه به مانند شکل ۶-۲۵۷، بر روی سرور ESXi خود کلیک راست کنید و گزینه‌ی Setting را انتخاب کنید تا کارت شبکه جدید را به لیست اضافه کنیم.

www.takbook.com



شکل ۶- ۲۵۵ ISCSI در ESXi

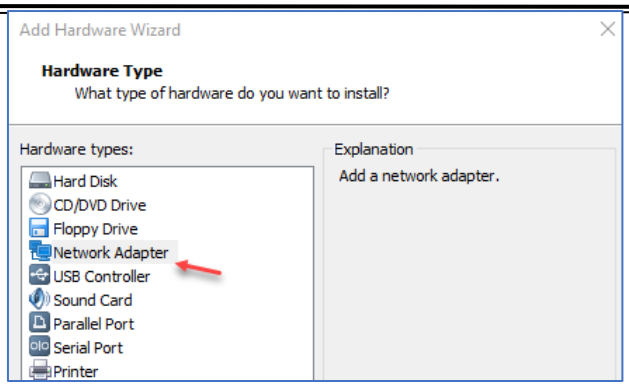
در شکل ٦-۲۵۸ باید بر روی Add کلیک کنید.



شکل ۶- ۲۵۶ ISCSI در ESXi

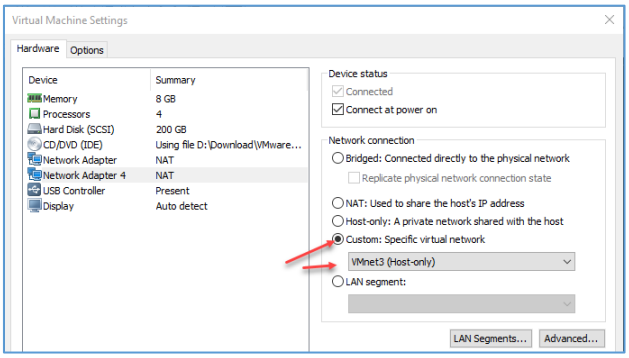
در شکل ٦-۲۵۹، Network Adapter را انتخاب و بر روی Finish کلیک کنید.

www.takbook.com



شکل ۶- ۲۵۷ ISCSI در ESXi

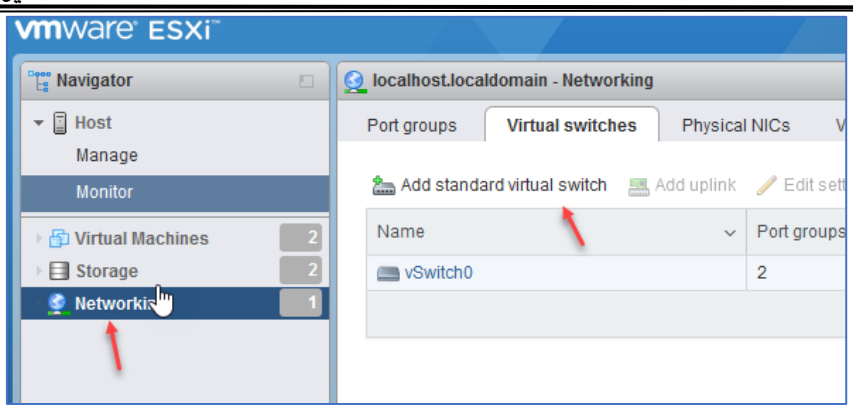
در شکل ٦-٢٦٠، باید کارت شبکه VMnet3 را که در قسمت قبل ایجاد کردیم را انتخاب و بر روی OK کلیک کنید.



شکل ۶- ۲۵۸ ISCSI در ESXi

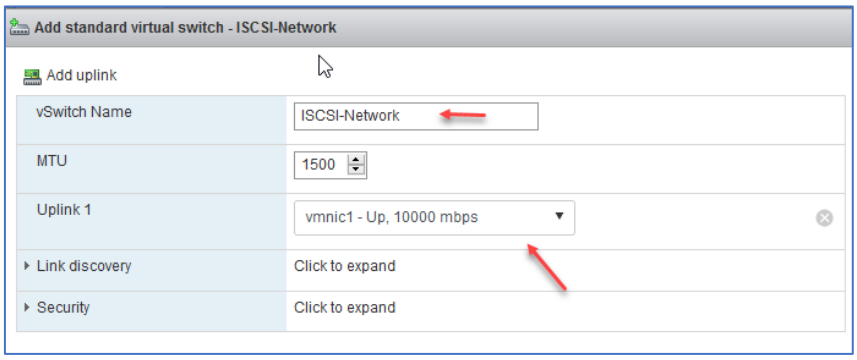
وارد ESXi شوید و به مانند شکل ٦-٢٦١، از سمت چپ گزینه‌ی Networking را انتخاب کنید و در صفحه‌ی باز شده وارد تب Virtual switches شوید و بر روی Add کلیک کنید.

www.takbook.com



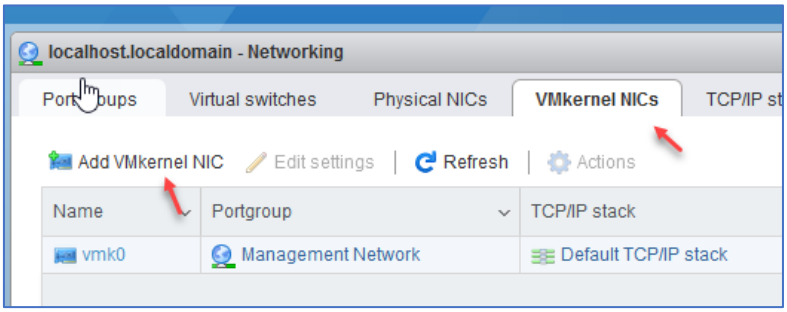
شکل ۶- ۲۵۹ ISCSI در ESXi

در شکل ٦-٢٦٢، نام مورد نظر خود را برای این سوئیچ وارد کنید و از قسمت Uplink1 باید کارت شبکه جدید که اضافه کردید را انتخاب و بر روی Add کلیک کنید.



شکل ۶- ۲۶۰ ISCSI در ESXi

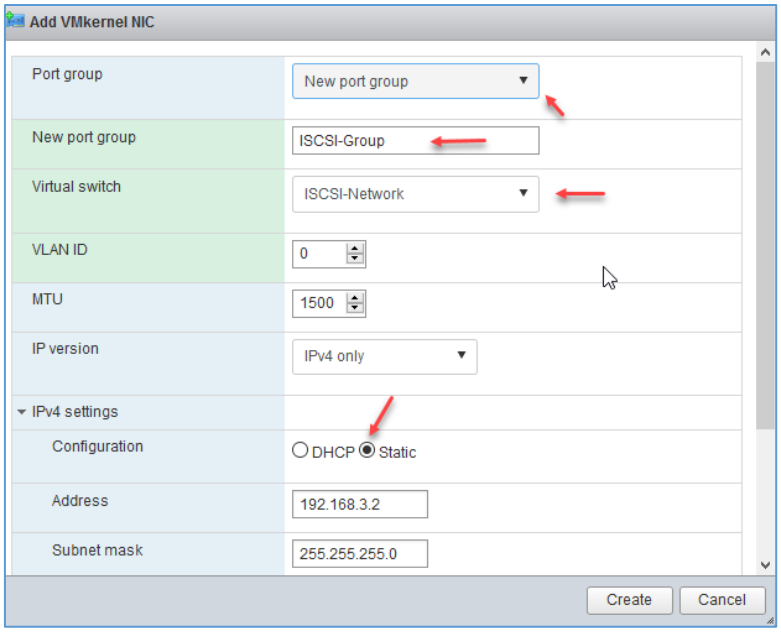
درشکل ٦-٢٦٣، وارد تب VMkernel NICs شوید و بر روی Add VMkernel NIC کلیک کنید.



شکل ۶- ۲۶۱ ISCSI در ESXi

www.takbook.com

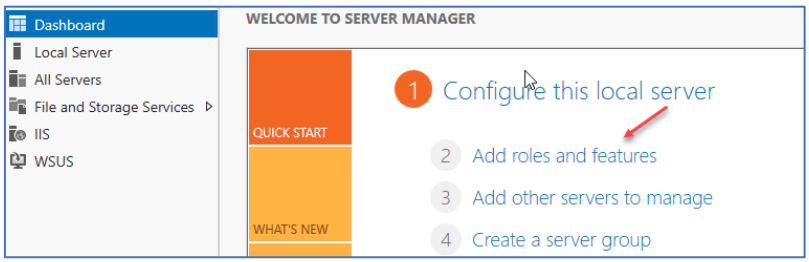
در شکل ٦-٢٦٤، در قسمت اول New Port Group را انتخاب کنید و نام گروه خود را در قسمت دوم وارد کنید، از قسمت Virtual switch باید سوئیچ مجازی که در قسمت قبل ایجاد کردیم را انتخاب کنید و در آخر باید یک آدرس IP به صورت دستی وارد و بر روی Create کلیک کنید.



شکل ۶- ۲۶۲ ISCSI در ESXi

در مرحله بعد باید ویندوز سرور ۲۰۲۲ را برای فعال‌سازی سرویس ISCSI آماده کنیم، همان‌طور که گفتیم باید همین کارت شبکه که با هم تنظیم کردیم را به ویندوز سرور متصل کنید تا با سرور ESXi در ارتباط باشد.

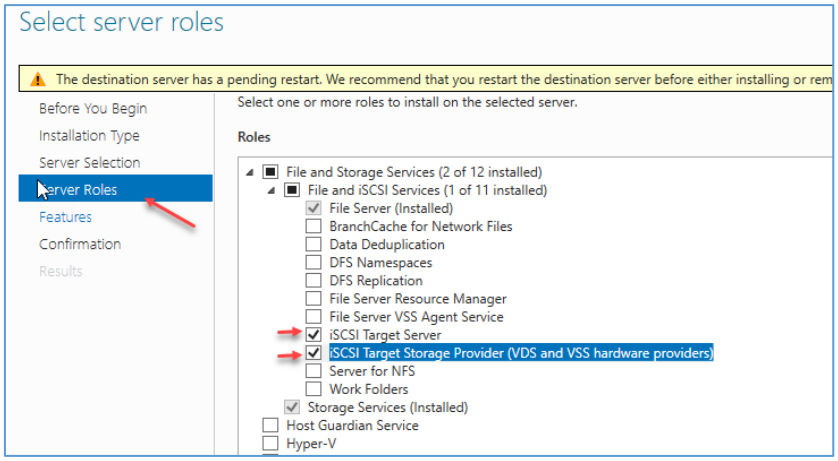
به مانند شکل ٦-٢٦٥، وارد ویندوز سرور شوید و Server Manager را اجرا کنید و در شکل باز شده بر روی Add roles and feature کلیک کنید.



شکل ۶- ۲۶۳ ISCSI در ESXi

www.takbook.com

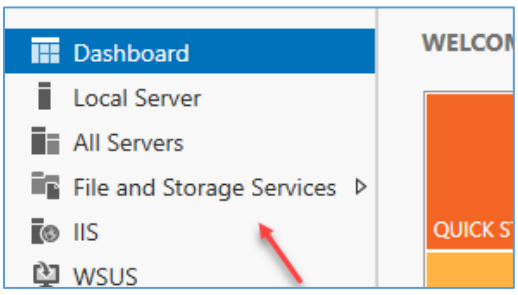
به مانند شکل ٦-٢٦٦، وارد قسمت Server Roles شوید و از زیر مجموعه File and iSCSI سرویس تیک دو گزینه‌ی مورد نظر را انتخاب کنید و سرویس را نصب کنید.



شکل ۶- ۲۶۴ ISCSI در ESXi

نکته: سیستم بعد از نصب حتماً Restart شود.

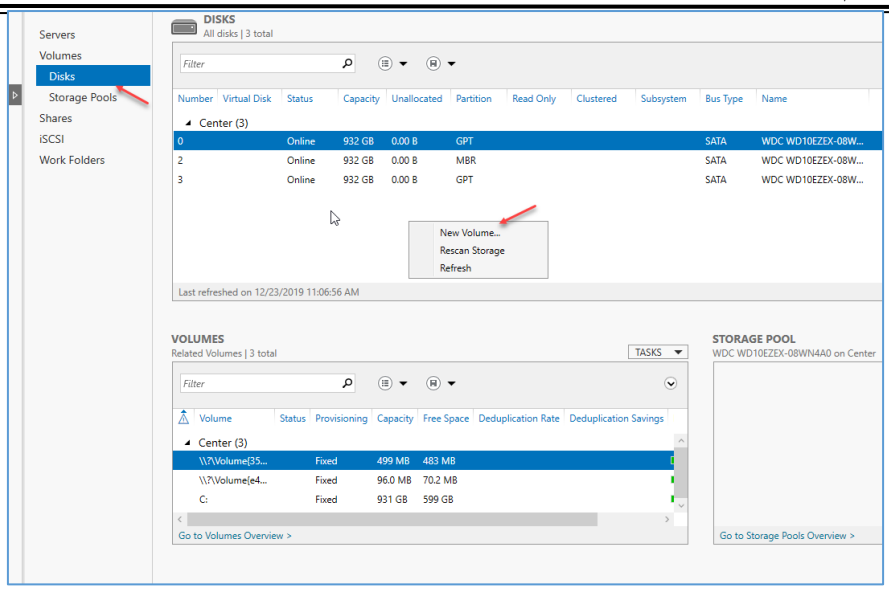
بعد از نصب سرویس در شکل ٦-٢٦٧ از قسمت چپ Server Manager بر روی گزینه‌ی File and Storage Services کلیک کنید.



شکل ۶- ۲۶۵ ISCSI در ESXi

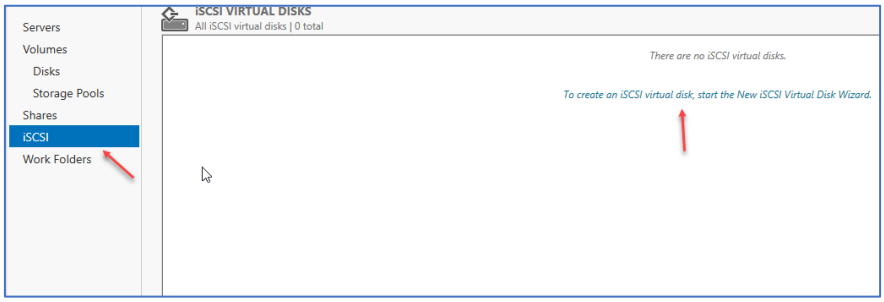
در شکل ٦-٢٦٨ و از قسمت Disks می‌توانید هارد دیسک‌هایی که بر روی این سیستم قرار دارد را مشاهده کنید، اگر بخواهید هارد دیسک جدیدی را به لیست اضافه کنید باید بر روی صفحه مورد نظر کلیک راست کنید و گزینه‌ی New Volume را انتخاب کنید، که فعلاً نیاز نیست.

www.takbook.com



شکل ۶- ۲۶۶ ISCSI در ESXi

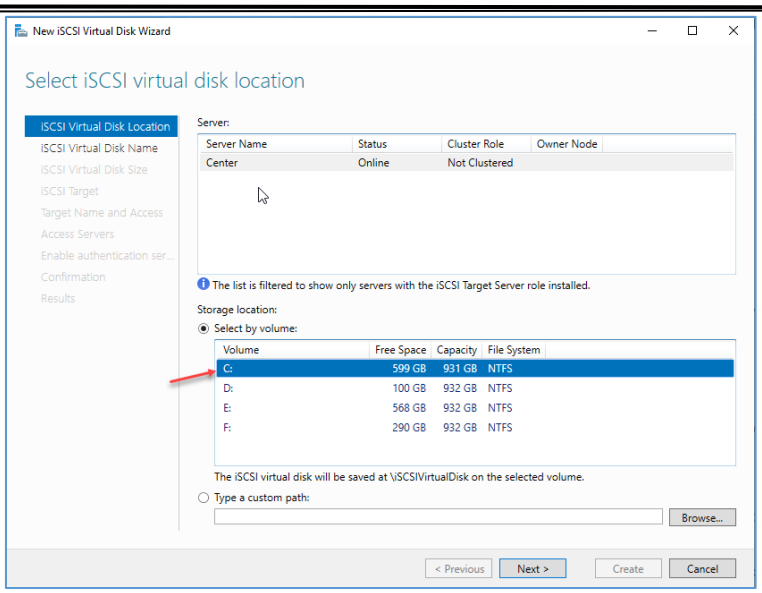
به مانند شکل ٦-٢٦٩، وارد قسمت iSCSI شوید و در صفحه‌ی باز شده بر روی گزینه‌ی مورد نظر کلیک کنید.



شکل ۶- ۲۶۷ ISCSI در ESXi

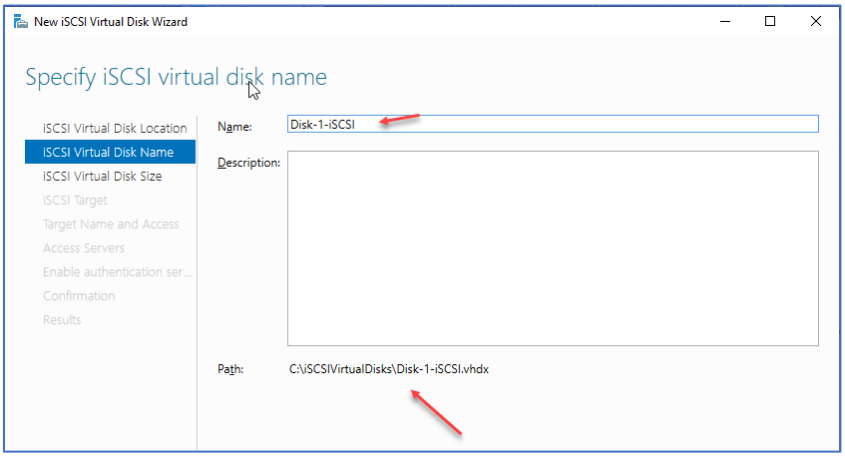
در شکل ٦-٢٧٠، باید یک پارتیشن را انتخاب کنید تا بر روی آن هارد دیسک مجازی را ایجاد کنیم، بر روی Next کلیک کنید.

www.takbook.com



شکل ۶- ۲۶۸ ISCSI در ESXi

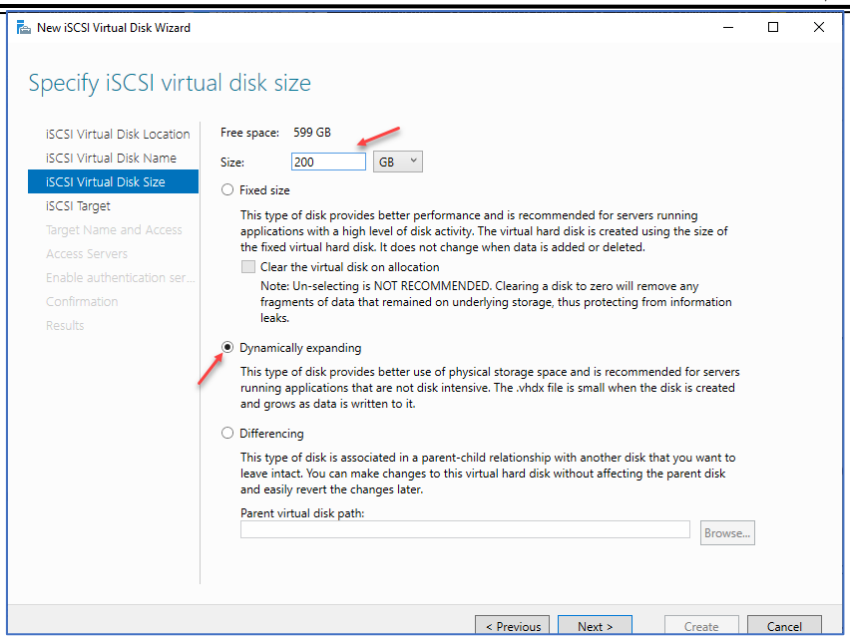
در شکل ٦-۲۷۱، باید برای هارد دیسک مجازی خود یک نام در نظر بگیرید، در قسمت Path هم مسیر ذخیره‌سازی هارد دیسک مجازی با نامی که وارد کردید را مشاهده می‌کنید، بر روی Next کلیک کنید.



شکل ۶- ۲۶۹ ISCSI در ESXi

در شکل ٦-۲۷۲، باید مشخص کنید که هارد دیسک مجازی چقدر فضا داشته باشد، برای راندمان بهتر گزینه‌ی Dynamically expanding را انتخاب و بر روی Next کلیک کنید.

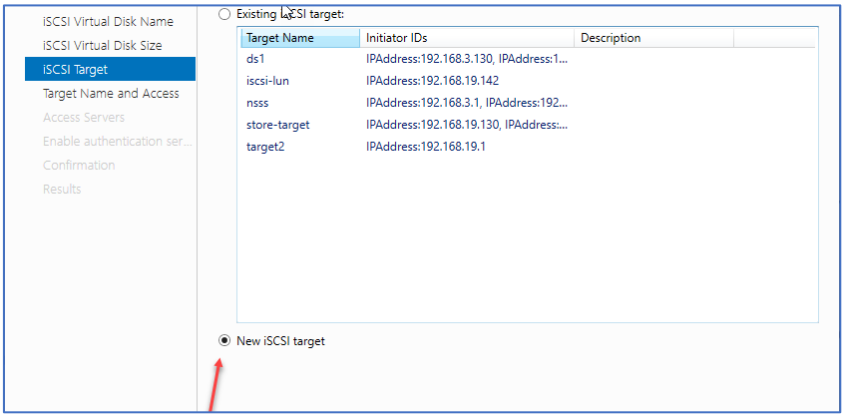
www.takbook.com



شکل ۶- ۲۷۰ ISCSI در ESXi

در شکل ٦-۲۷۳، گزینه‌ی new iSCSI target را انتخاب کنید و بر روی Next کلیک کنید.

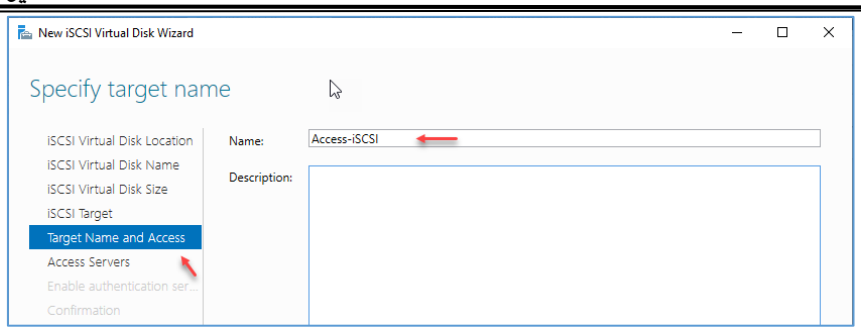
نکته: همان‌طور که در اول این بخش بیان کردیم سرور ۲۰۲۲ هم به عنوان Initiator و هم به عنوان Target عمل خواهد کرد، چون هم سرویس و هم فضای ذخیره‌سازی در این سرور وجود دارد.



شکل ۶- ۲۷۱ ISCSI در ESXi

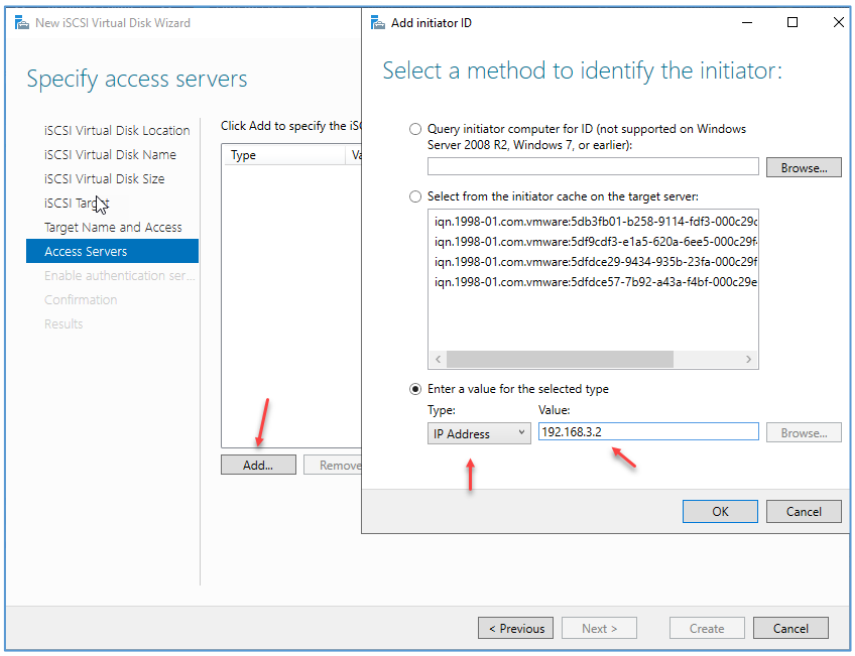
در شکل ٦-۲۷٤، یک نام برای Target خود وارد کنید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۶- ۲۷۲ ISCSI در ESXi

در شکل ٦-۲۷۵، باید بر روی Add کلیک کنید و در صفحه باز شده در پائین آن گزینه‌ی IP Address را انتخاب کنید و آدرس کارت شبکه‌ای که در قسمت قبل تنظیم کردیم را وارد و بر روی Add کلیک کنید.



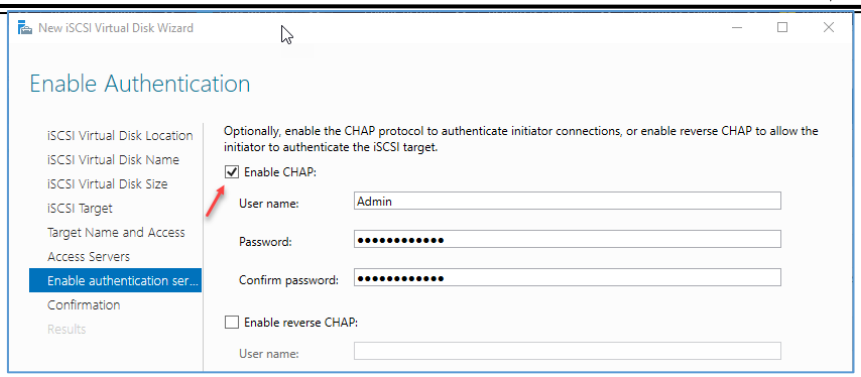
شکل ۶- ۲۷۳ ISCSI در ESXi

در شکل ٦-۲۷٦، باید امنیت ارتباط بین iSCSI و سرور ESXi را برقرار کنیم، برای این کار تیک گزینه‌ی اول را انتخاب کنید و یک نام کاربری و رمز عبور را برای آن در نظر بگیرید.

نکته: رمز عبور را به صورت پیچیده وارد کنید.

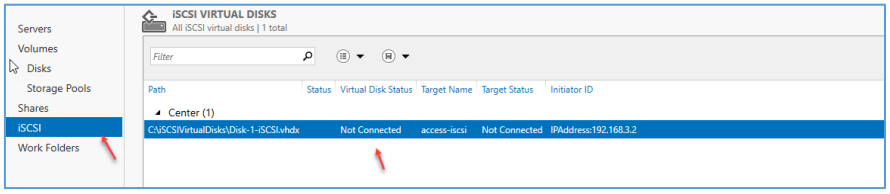
در صفحه آخر هم بر روی Create کلیک کنید تا تنظیمات اعمال شود.

www.takbook.com



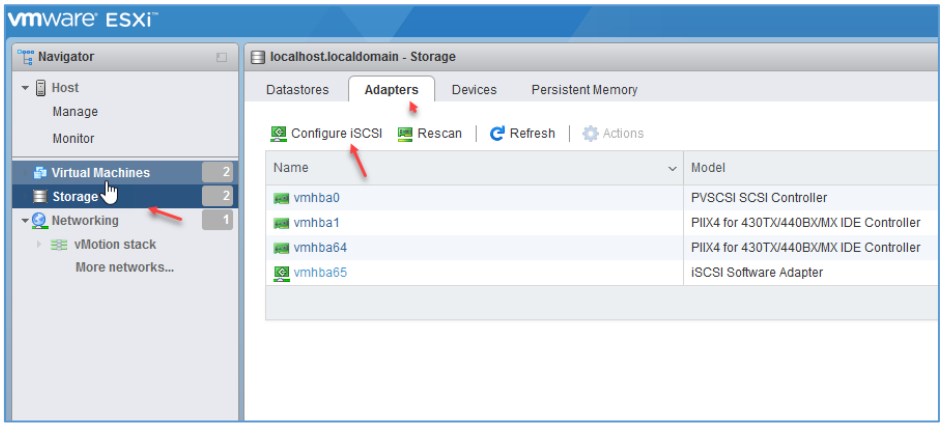
شکل ۶- ۲۷۴ ISCSI در ESXi

همان‌طور که در شکل ٦-۲۷۷ مشاهده می‌کنید هارد دیسک مجازی با تنظیمات مربوطه ایجاد شده ولی هنوز فعال نشده است و باید در سرور ESXi تنظیمات آن را کامل کنیم.



شکل ۶- ۲۷۵ ISCSI در ESXi

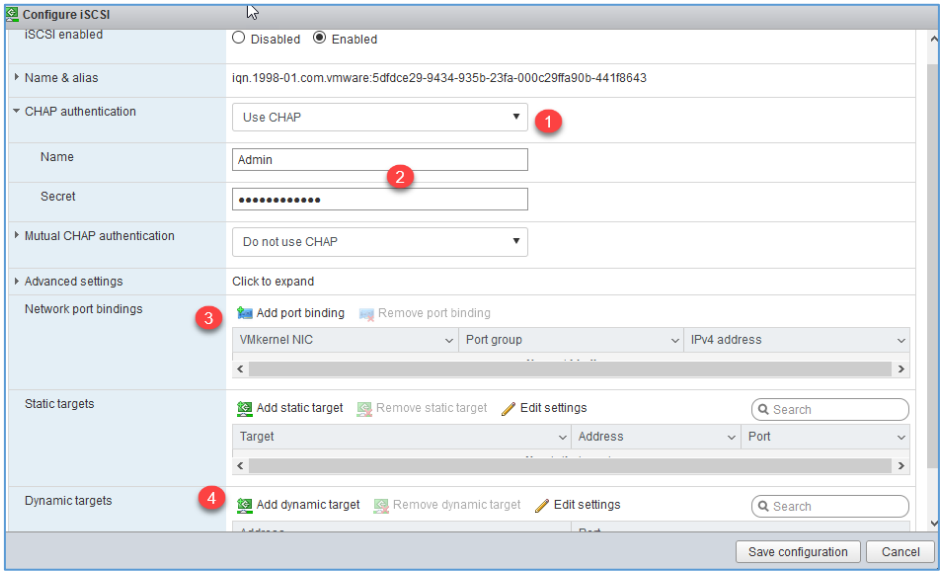
در ادامه به مانند شکل ٦-۲۷۸، وارد ESXi شوید و از قسمت Storage وارد تب Adapters شوید و بر روی Configure iSCSI کلیک کنید.



شکل ۶- ۲۷۶ ISCSI در ESXi

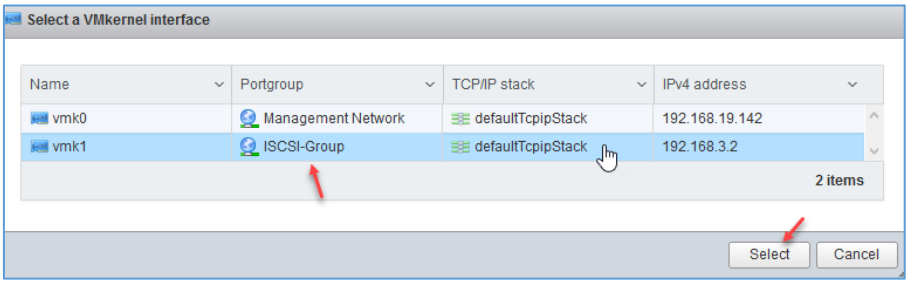
www.takbook.com

در شکل ۶-۲۷۹، باید تنظیمات مربوط به iSCSI را انجام دهید، در قسمت شماره‌ی یک باید گزینه‌ی Use CHAP را انتخاب کنید و در قسمت شماره‌ی دو باید نام کاربری و رمز عبور مورد نظر را که در سرور ۲۰۲۲ تنظیم کردید وارد کنید.



شکل ۶- ۲۷۷ ISCSI در ESXi

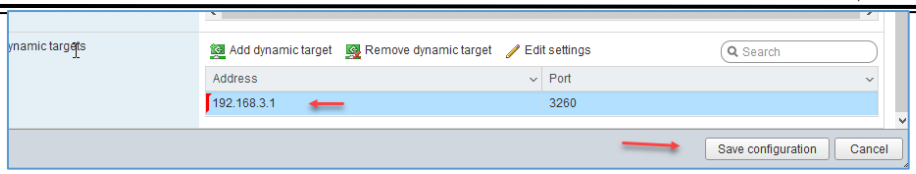
در قسمت شماره‌ی سه باید بر روی Add port binding کلیک کنید تا شکل ۶-۲۸۰، ظاهر شود و در این قسمت کارت شبکه‌ای که برای این کار آماده کردیم را انتخاب کنید.



شکل ۶- ۲۷۸ ISCSI در ESXi

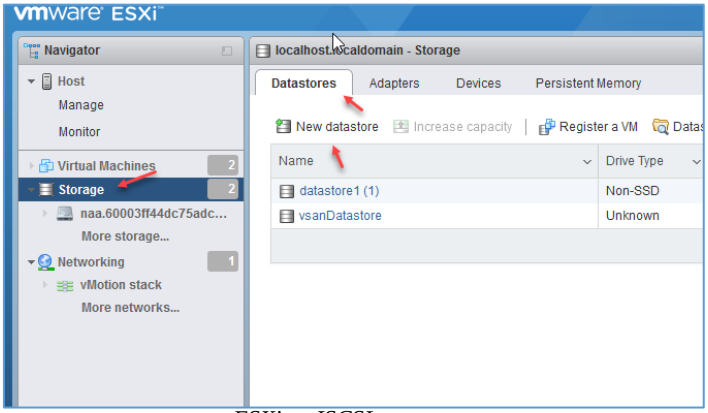
در قسمت شماره‌ی چهار بر روی Add dynamic target کلیک کنید و به مانند شکل ۶-۲۸۱، آدرس IP سرور ۲۰۲۲ را که بر روی آن سرویس iSCSI را راه‌اندازی کردیم وارد کنید و در آخر بر روی Save configuration کلیک کنید.

www.takbook.com



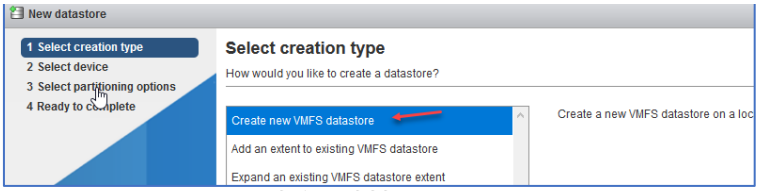
شکل ۶- ۲۷۹ ISCSI در ESXi

در ادامه کار به مانند شکل ٦-۲۸۲، باید هارد دیسک iSCSI را به ESXi اضافه کنیم برای همین کار وارد Storage شوید و در تب Datastores بر روی New datastore کلیک کنید.



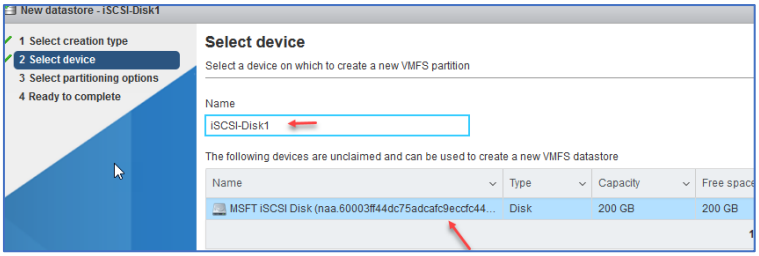
شکل ۶- ۲۸۰ ISCSI در ESXi

در شکل ٦-۲۸۳، گزینه‌ی اول را انتخاب و بر روی Next کلیک کنید.



شکل ۶- ۲۸۱ ISCSI در ESXi

در شکل ٦-۲۸٤، هارد دیسک مجازی که با هم ایجاد کردیم را مشاهده می‌کنید و می‌توانید برای آن یک نام در نظر بگیرید و از آن استفاده کنید.



شکل ۶- ۲۸۲ ISCSI در ESXi

www.takbook.com

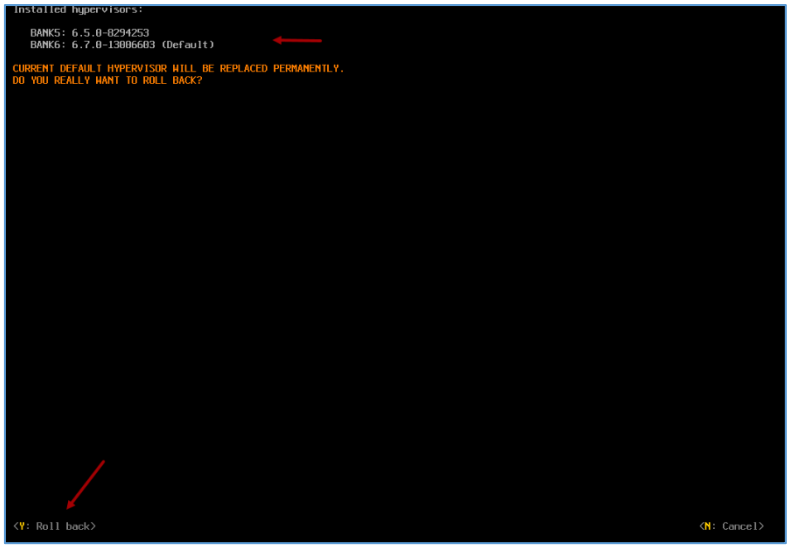
۲۵-٤-۱-٦ نحوه Downgrade کردن در ESXi

زمانی که نسخه ESXi را به ورژن بالاتر ارتقاء می‌دهید شاید با مشکلاتی روبرو شوید که مایل باشید دوباره به همان ورژن قبلی برگردید، برای این کار باید ESXi را Restart کنید و در هنگام بالا آمدن ESXi که در شکل ٦-۲۸۵، هم مشخص است باید روی کلید ترکیبی Shift + R فشار دهید تا وارد حالت Recovery شویم.



شکل ۶- ۲۸۳ Downgrade کردن در ESXi

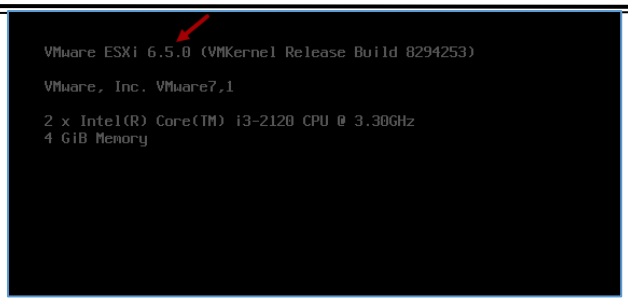
در شکل ٦-۲۸٦، دو نسخه به شما نمایش داده خواهد شد که نسخه اولیه آن ٦.٥ و نسخه‌ای که آپدیت شده است ٦.٧ است، اگر به کلمه Default توجه کنید مشخص است که نسخی فعلی که بر روی ESXi فعال است ٦.٧ می‌باشد، برای برگشت به نسخه ٦.٥ باید کلمه Y را بر روی صفحه کلید فشار دهید.



شکل ۶- ۲۸۴ Downgrade کردن در ESXi

همان‌طور که در شکل ٦-۲۸۷ مشاهده می‌کنید ESXi به ورژن ٦.٥ برگشت کرده است.

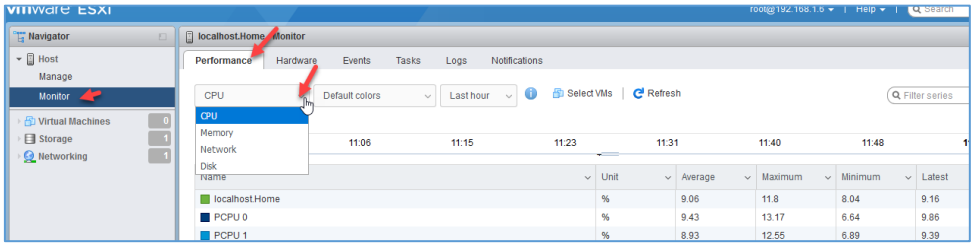
www.takbook.com



شکل ۶- ۲۸۵ Downgrade کردن در ESXi

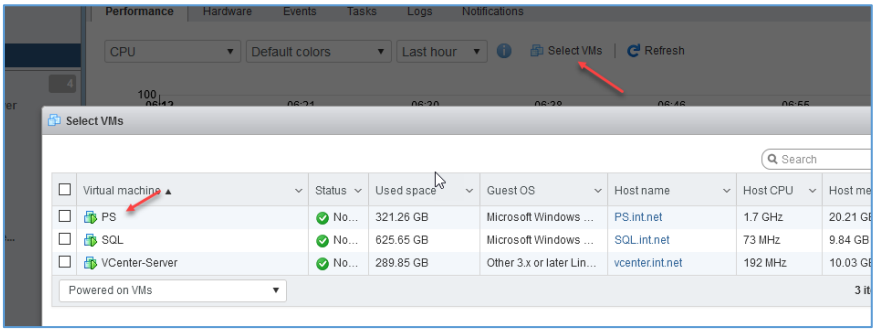
٦-۱-٤-۲٦ بررسی قسمت Monitor در ESXi

هر نرم‌افزاری برای مدیریت بهتر کارها سرویس‌های مانیتوریگ را ارائه می‌دهند که می‌تواند کمک خوبی برای مدیریت بهتر آن باشد، در قسمت Performance مقدار مصرف و درگیر بودن CPU, Memory, Network و DISK را می‌توانید در شکل ٦-۲۸۸مشاهده کنید.



شکل ۶- ۲۸۶ Monitor در ESXi

طبق شکل ٦-۲۸۹، می‌توانید با کلیک بر روی Select VMs مشخص کنید کدام ماشین بیشترین مصرف را طی ساعات گذشته داشته است.

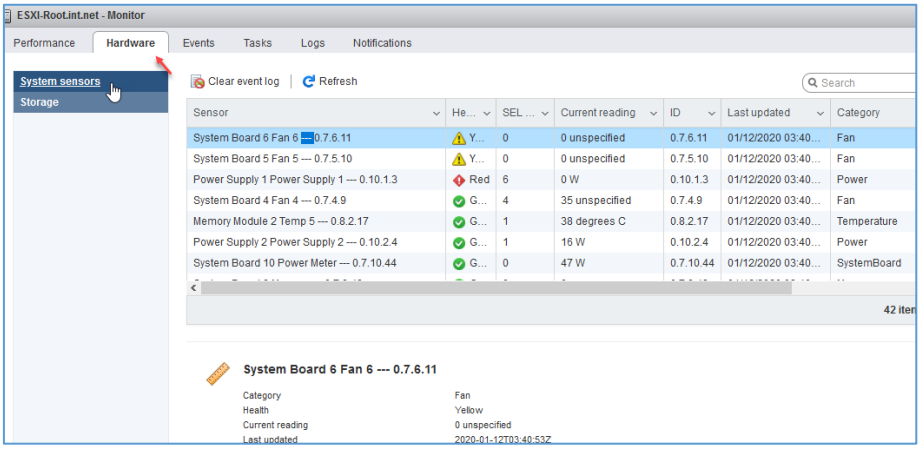


شکل ۶- ۲۸۷ Monitor در ESXi

به مانند شکل ٦-۲۹۰، در تب Hardware هم می‌توانید مشاهده کنید که سخت‌افزارهای داخل سرور در چه وضعیتی قرار دارند، مثلاً در شکل ٦-۲۹۰ و در خط اول اخطاری مبنی بر مشکل در Fan سرور به شما

www.takbook.com

می‌دهد که باید آنها را بررسی و مشکل را برطرف کنید،در تب‌های دیگر هم می‌توانید رویدادها، وظیفه‌ها و اعلان را مشاهده کنید، در کل داشتن دانشی مناسب درباره مانیتورینگ بسیار می‌تواند شما را در سالم نگه داشتن سرور و داده‌ها کمک کند.



شکل ۶- ۲۸۸ Monitor در ESXi

www.takbook.com

www.takbook.com

فصل هفتم

میکروتیک

شرکت MikroTik یک شرکت تولید کننده تجهیزات شبکه و ارائه‌دهنده راهکارهای شبکه‌ای است که در سال ۱۹۹۶ در لتونی (Latvia) تأسیس شد. این شرکت بیشتر به دلیل سیستم‌عامل RouterOS و تجهیزات شبکه‌ای به ویژه روترها و سوییچ‌ها شناخته می‌شود. MikroTik راه‌حل‌های مناسبی برای کاربران خانگی، کسب و کارهای کوچک و متوسط و حتی شبکه‌های بزرگ سازمانی ارائه می‌دهد.

۷-۱ تاریخچه و رشد MikroTik

MikroTik در ابتدا با هدف توسعه و ارائه نرم‌افزارهای شبکه‌ای تاسیس شد، اما بعداً به دلیل نیاز بازار، به تولید سخت‌افزارهایی مانند روترها و سوییچ‌ها نیز روی آورد. این شرکت با توسعه RouterOS، یک سیستم‌عامل قدرتمند مبتنی بر لینوکس، به یکی از پیشگامان در صنعت شبکه تبدیل شد.

۷-۳ ویژگی‌های متمایز MikroTik:

- قیمت مناسب: تجهیزات MikroTik نسبت به بسیاری از رقبا از قیمت پایین‌تری برخوردارند، اما قابلیت‌های پیشرفته‌ای دارند که می‌توانند با محصولات گران‌تر رقابت کنند.
- قابلیت‌های پیشرفته در RouterOS: RouterOS امکاناتی نظیر مسیریابی (Routing)، فایروال (Firewall)، مدیریت پهنای باند (Bandwidth Management)، VPN، Hotspot و موارد دیگر را در اختیار کاربران قرار می‌دهد.
- انعطاف‌پذیری بالا: سیستم‌عامل RouterOS به گونه‌ای طراحی شده که بسیار انعطاف‌پذیر است و می‌توان آن را به سادگی برای نیازهای مختلف شبکه پیکربندی کرد.
- پشتیبانی از پروتکل‌های متعدد: MikroTik از پروتکل‌های مختلفی مانند OSPF، BGP، MPLS، IPv6 و دیگر پروتکل‌های استاندارد شبکه پشتیبانی می‌کند.
- کاربرد گسترده: محصولات MikroTik در سراسر جهان برای ایجاد شبکه‌های کوچک تا شبکه‌های بزرگ ISP (ارائه‌دهنده خدمات اینترنت) مورد استفاده قرار می‌گیرند.

www.takbook.com

٤-۷ انواع روتر میکروتیک

قبل از شروع به کار باید روترهای میکروتیک را بررسی کنیم، روترهای میکروتیک در انواع و اقسام مختلف از نظر قدرت وجود دارند که به ترتیب بعضی از مدل‌های مهم آن را بررسی می‌کنیم.

روتر hAP ac lite

این روتر بسیار کوچک و ارزان قیمت است، دارای ٥ پروت Ethernet با سرعت 10/100 است و برای مصارف خانگی کاربرد دارد که در شکل ۷-۱ این روتر را مشاهده می‌کنید.



شکل ۷- ۱ روتر hAP ac lite

روتر hAP lite TC

اکسس پوینت (hAP lite) یک دستگاه کوچک ایده آل برای آپارتمان، خانه یا محل کار شما است.

hAP lite مجهز به پردازنده قدرتمند ٦٥٠ مگاهرتز، ۳۲ مگابایت رم dual chain، بی‌سیم ۲.٤ گیگاهرتز، چهار پورت اترنت سریع و دارای لایسنس RouterOS L4 است. منبع تغذیه به صورت USB طراحی شده است.



شکل ۷- ۲ روتر hAP lite TC

روتر hAP ac lite TC

اکسس پوینت روتر میکروتیک hAP ac lite TC با نام فنی RB952Ui-5ac2nD-TC یکی از محصولات بسیار عالی با قیمت بسیار مناسب میکروتیک است. اکسس پوینت روتر میکروتیک hAP ac lite TC دارای ٥ پورت

www.takbook.com

اترنت ۱۰۰/۱۰ بوده که برای پورت ٥ این دستگاه قابلیت POE OUT تعریف شده است و می تواند به میزان ولتاژ ورودی، خروجی نیز بدهد که توان ٥۰۰ میلی‌آمپر را نیز در بر داشته باشید. دارا بودن پورت USB جهت استفاده 3G / 4G و قابلیت وایرلس Dual Band و کارکرد به صورت همزمان در دو فرکانس ۲.٤ و 5.8 GHZ از دیگر امکانات این روتر می‌باشد . در طراحی Mikrotik hAP ac lite TC باکس به صورت خوابیده و ایستاده قابل استفاده می‌باشد .



شکل ۷- ۳ روتر *hAP ac lite TC*

روتر hAP ax lite

روتر وایرلس میکروتیک hAP ax lite با نام فنی L41G-2axD، hAP ax lite راه‌حل بسیار کوچکی است که باعث می‌شود هزینه‌ها را کاهش دهید جدیدترین تراشه بی‌سیم Gen6 AX میکروتیک به شما امکان می‌دهد تا طیف بی‌سیم ۲.٤ گیگاهرتز را مانند یک لیمو فشرده کنید! بسته به تنظیمات کلی شما، می‌توانید انتظار افزایش سرعت تا ۹۰٪ را داشته باشید! روتر وایرلس میکروتیک hAP ax lite دارای ٤ پورت اترنت ۱۰۰۰/۱۰۰/۱۰ می‌باشد . hAP ax lite قابلیت کارکرد در فرکانس ۲.٤ را دارا می‌باشد و نکته‌ی بسیار مهمی که در آن به قابل بیان است، استفاده از ax۸۰۲.۱۱ با پشتیبانی Wave2 که بدان معناست تا ٤۰٪ سرعت بالاتر در طیف ۲.٤ گیگاهرتز. CPU دو هسته‌ای مدرن که با فرکانس ۸۰۰ مگاهرتز کار می‌کند همراه با MB۲٥٦ رم ، هنگام انجام عملیات‌های سنگین مانند قوانین پیچیده فایروال، رمزگذاری سخت‌افزار IPsec، استفاده از رشته‌های بیشتر یا آزمایش با پیشرفته‌ترین ویژگی‌های RouterOS، عملکرد بسیار خوبی دارد.

www.takbook.com



شکل ۷- ۴ روتر hAP ax lite

روتر RB951Ui-2HnD

محصول RB951Ui-2HnD از تجهیزات میکروتیک یک دستگاه وایرلس با قابلیت Access Point برای مراکز اداری کوچک است که از نسل جدید پردازنده Atheros با قدرت بیشتر طراحی شده است. این روتر اکسس پوینت ۵ پورت اترنت و کارت وایرلس با توان خروجی ۱۰۰۰mW که از استاندارد ۸۰۲.۱۱b/g/n پشتیبانی می کند را دارا می‌باشد. همچنین این دستگاه دارای یک پورت USB می‌باشد. شایان به ذکر است که سرعت پردازنده این دستگاه ۶۰۰MHz و ۱۲۸MB حافظه رم و یک خروجی PoE برروی پورت شماره ۵ است که می‌توان دستگاه های دیگر را با استفاده از آن روشن کرد. حداکثر جریان بار برروی این پورت ۵۰۰mA می‌باشد.



شکل ۷- ۵ روتر RB951Ui-2HnD

روتر میکروتیک مدل CRS125-24G-1S-IN

www.takbook.com

یک روتر در سطح Enterprise که دارای قدرت بالایی است و برای یک سازمانی بزرگ طراحی شده است و یک روتر سوئیچ است و در لایه‌ی سوم شبکه به خوبی کار می‌کند، خودم در شرکت از این مدل استفاده می‌کنم، این روتر دارای ۱۲۸ مگابایت رم به همراه 600 مگاهرتز CPU است و دارای 24 پورت 10/100/1000 است و همچنین یک پورت فیبر نوری هم بر روی آن نصب می‌شود.



شکل ۷- ۶ روتر میکروتیک مدل CRS125-24G-1S-IN

۷-۲ محصولات اصلی MikroTik

- RouterOS: سیستم‌عامل اختصاصی MikroTik که امکانات زیادی برای مدیریت و کنترل شبکه دارد. این سیستم‌عامل به کاربران اجازه می‌دهد تا روترهای ساده را به دستگاه‌های پیشرفته‌ای برای مسیریابی، فایروال، VPN، QoS، Hotspot و موارد دیگر تبدیل کنند.
- RouterBOARD: سخت‌افزار اختصاصی MikroTik که با RouterOS یکپارچه شده و امکان مدیریت پیشرفته شبکه‌ها را فراهم می‌کند. RouterBOARD شامل انواع مختلفی از روترها، اکسس پوینت‌ها و سوییچ‌ها می‌شود.
- Cloud Core Router (CCR): یک سری از روترهای قدرتمند که برای شبکه‌های بزرگ و ترافیک سنگین طراحی شده است. این دستگاه‌ها از پردازنده‌های چند هسته‌ای بهره می‌برند و توانایی پردازش داده‌ها با سرعت بسیار بالا را دارند.
- Switches: میکروتیک انواع مختلف سوییچ‌ها را نیز تولید می‌کند که برای مدیریت و تقسیم‌بندی شبکه‌ها استفاده می‌شود.
- Wireless: میکروتیک محصولاتی برای شبکه‌های بی‌سیم (Wireless) نیز ارائه می‌دهد که شامل آنتن‌ها، اکسس پوینت‌ها، و تجهیزات شبکه‌های بی‌سیم در فواصل طولانی است.
- CAPsMAN: یک راهکار متمرکز برای مدیریت نقاط دسترسی بی‌سیم (WiFi)، که امکان مدیریت متمرکز شبکه‌های بی‌سیم را به مدیران شبکه می‌دهد.

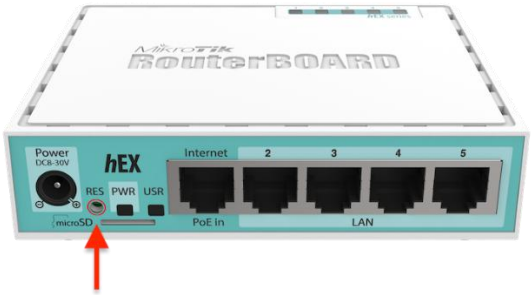
www.takbook.com

۷-۵ ریست کردن روتر میکروتیک

توجه داشته باشید ما در این کتاب از نسخه‌ی مجازی روتر میکروتیک استفاده می‌کنیم، ولی برای اینکه از یک دستگاه فیزیکی استفاده کنیم باید قبل از هر کاری آن دستگاه را ریست کنیم و بعد تنظیمات خود را بر روی آن انجام دهیم.

دو روش برای ریست کردن وجود دارد، یکی اینکه به صورت نرم‌افزاری به روتر متصل شویم و ریسیت را انجام دهیم و دیگری به صورت سخت‌افزاری، برای اینکه به صورت سخت‌افزاری انجام دهیم باید به صورت زیر عمل کنید.

طبق شکل ۷-۷ یک قسمت با عنوان RES یا همان RESET وجود دارد که شما باید دکمه را فشار دهید تا ریست انجام شود، اما روترهای میکروتیک کمی متفاوت هستند و قبل از اینکه برق را متصل کنیم باید دکمه مورد نظر را فشار دهید و وقتی دکمه را در حال فشار دادن هستید باید برق را متصل کنید و بعد از ۱۰ ثانیه می‌توانید دست خود را از دکمه ریست بردارید تا ریسیت انجام شود.



شکل ۷-۷ ریست کردن روتر میکروتیک

۷-۶ نصب و راه‌اندازی اولیه

در این کتاب که جنبه آموزشی دارد میکروتیک را به صورت نرم‌افزاری نصب و کار با آن را یاد میگیریم. برای شروع باید از لینک زیر آخرین ورژن آن را دانلود کنید:

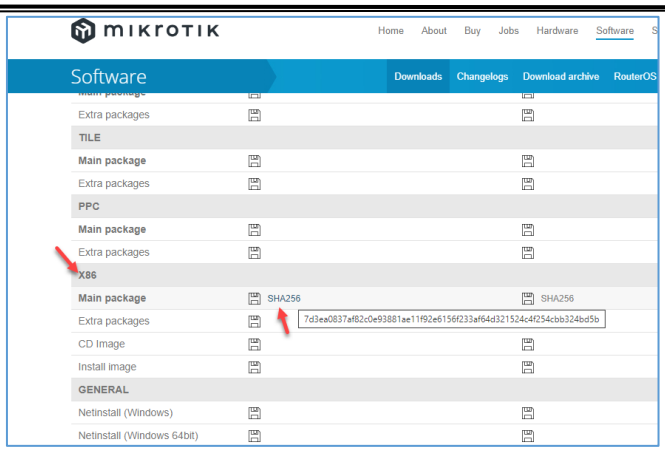
https://soft98.ir/internet/network/1163-mikrotik-routeros.html

البته تو سایت میکروتیک هم به آدرس زیر میتوانید این سیستم عامل را دانلود کنید که البته لایسنس ندارد و باید خریداری کنید:

https://mikrotik.com/download

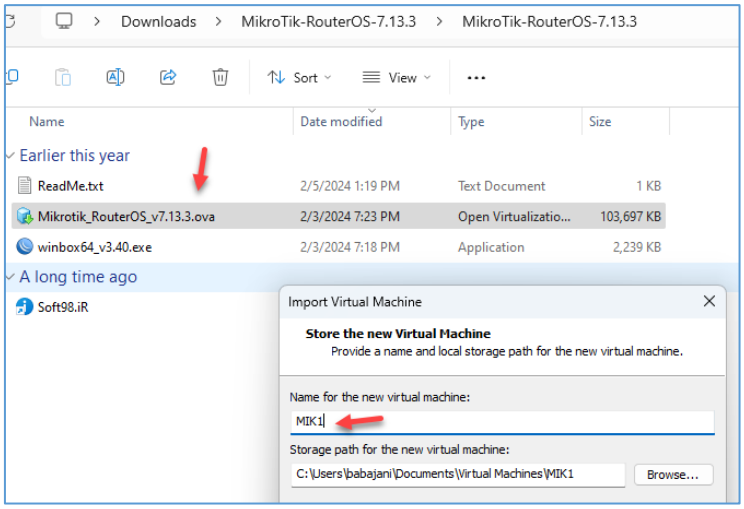
در شکل ۷-۸، برای دانلود باید در قسمت X86 فایل اصلی را دانلود کنید که در شکل ۷-۸، این موضوع مشخص شده است.

www.takbook.com



شکل ۷- ۸ دانلود روتر میکروتیک

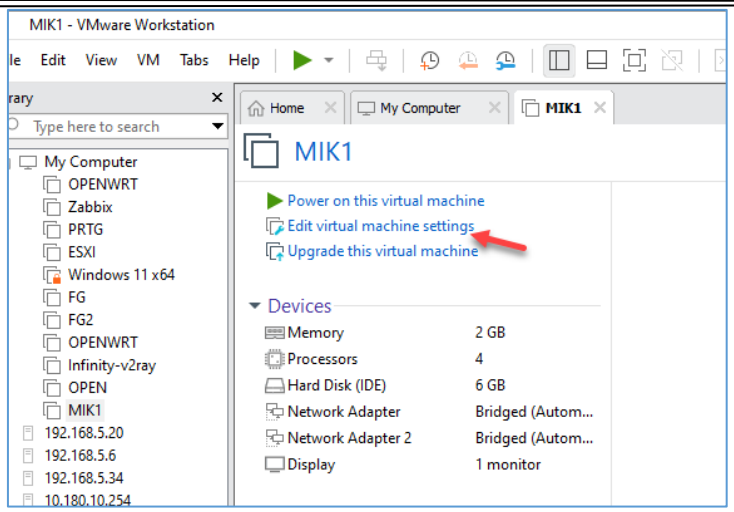
در شکل ۷-۹، لینک اول دانلود کردیم و به مانند شکل ۷-۹ اگر بر روی سیستم خود دوبار کلیک کنید فایل OVA بر روی VMware اجرا می‌شود، البته می‌توانستید این فایل را در ESXi هم اجرا کنید که انجام این کار را در فصل قبلی بررسی کردیم.



شکل ۷- ۹ اجرای روتر روی VMware

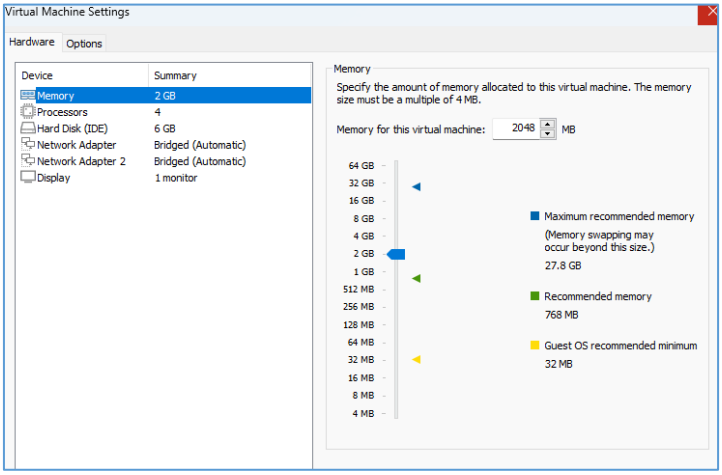
در ادامه کار، بعد از باز شدن ماشین مجازی در VMware Workstation به مانند شکل ۷-۱۰، بر روی Edit virtual… کلیک کنید.

www.takbook.com



شکل ۷- ۱۰ تنظیم سخت افزار

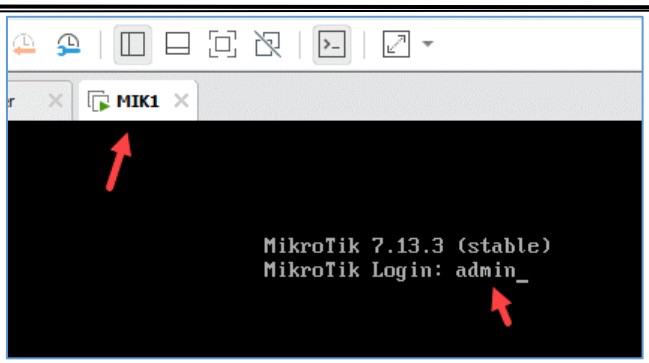
در ادامه به مانند شکل ۷-۱۱، می‌توانید تنظیمات سخت‌افزاری ماشین مجازی را تغییر دهید، توجه داشته باشید کارت شبکه باید حتماً فعال باشد تا بتوانیم به میکروتیک متصل شویم.



شکل ۷- ۱۱ تغییر سخت افزار

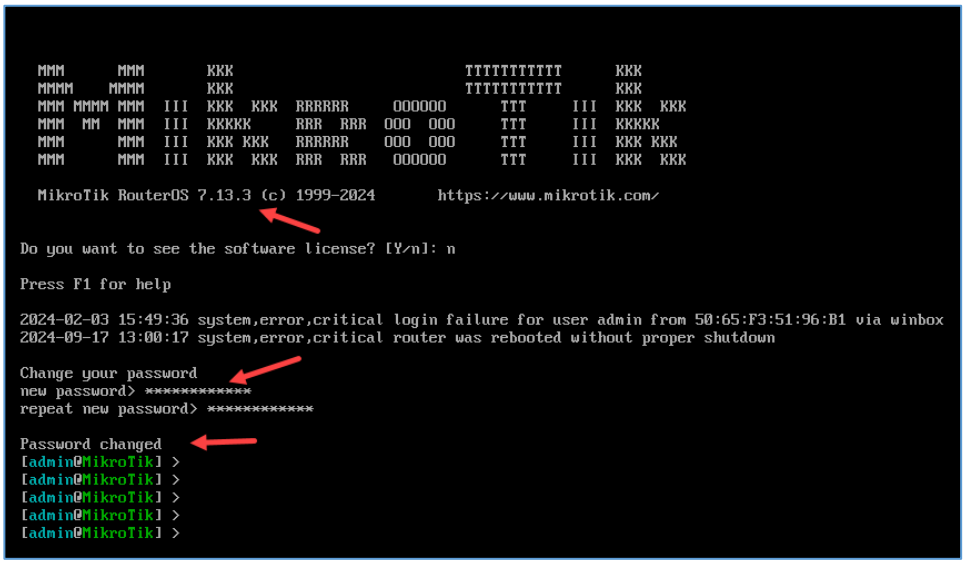
ماشین مورد نظر را روشن کنید، که شکل ۷-۱۲ را مشاهده می‌کنید ، با استفاده از نام کاربری Admin و بدون رمز می‌توانید وارد میکروتیک شوید.

www.takbook.com



شکل ۷- ۱۲ راه‌اندازی روتر میکروتیک

همان‌طور که در شکل ۷-۱۳، مشاهده می‌کنید وارد روتر میکروتیک شدیم و ورژن آن را مشاهده می‌کنید، اولین کاری که انجام می‌دهید باید رمز عبور جدید خود را به مانند شکل دو بار وارد کنید تا رمز تغییر کند که بعد از آن خط فرمان روتر در دسترس است، برای اینکه روتر میکروتیک را تنظیم کنیم بهتر است از نرم افزار Winbox استفاده کنیم.



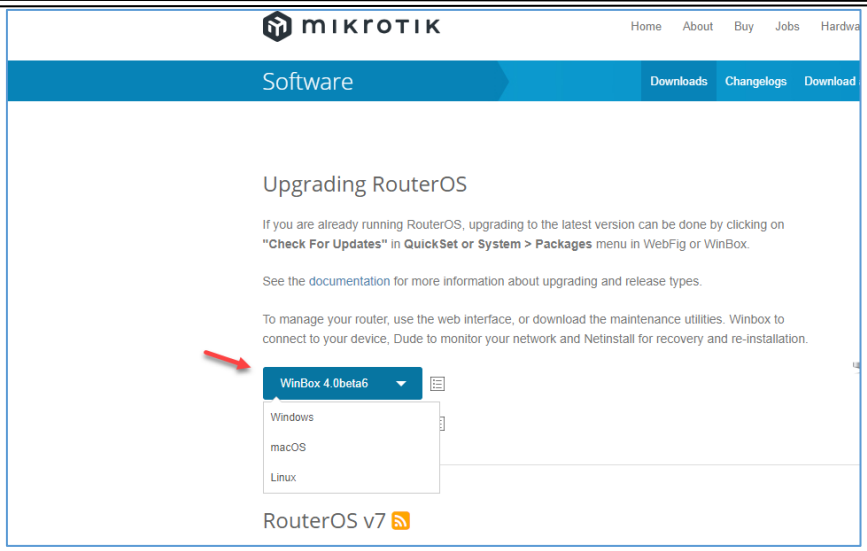
شکل ۷- ۱۳ تغییر رمز عبور

برای دانلود نرم‌افزار Winbox می‌توانید از لینک زیر استفاده کنید،

https://mikrotik.com/download

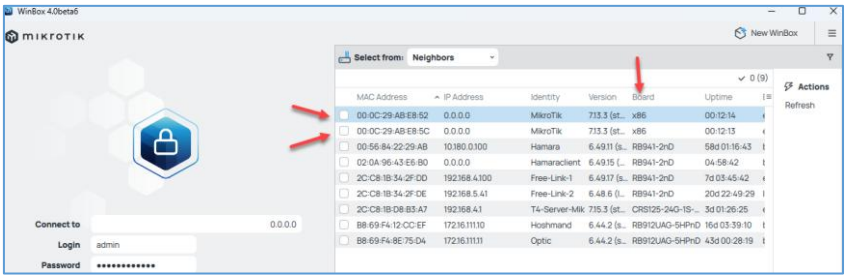
بعد از ورود به لینک مورد نظر به مانند شکل ۷-۱۴ بر روی Winbox 4 کلیک کنید.

www.takbook.com



شکل ۷- ۱۴ دانلود Winbox

بعد از دانلود، نرم‌افزار را به مانند شکل ۷-۱۵، اجرا کنید، همان‌طور که در شکل ۷-۱۵ مشاهده می‌کنید تعداد زیادی روتر میکروتیک را در قسمت Neighbors به صورت اتوماتیک پیدا کرده است که اگر به قسمت Board دقت کنید یک از آنها با برد x86 نشان داده است که منظور از آن این است که این سیستم‌عامل بر روی یک کلاینت یا سرور به صورت مجازی اجرا شده است و همان سرور ما هستش، اما چون دو کارت شبکه به آن اختصاص دادیم دو تا MAC آدرس پیدا کرده که شما کافی است با کلیک بر روی یکی از MACها و وارد کردن نام کاربری و رمز عبوری که تغییر دادید وارد روتر شوید و از تنظیمات گرافیکی جدید لذت ببرید، توجه داشته باشید نام کاربر پیش‌فرض admin و رمز عبور ندارد.



شکل ۷- ۱۵ ورود به میکروتیک

همان‌طور که در شکل ۷-۱۶ مشاهده می‌کنید، گزینه‌های زیادی قرار دارد که باید با اکثر آنها کار کنیم، طبق شماره‌ای که بر روی عکس قرار دادیم، در قسمت شماره‌ی یک سرویس‌های مختلف و تنظیمات را مشاهده می‌کنید که در ادامه باید با آنها کار کنیم، در قسمت شماره‌ی دو اطلاعات سخت‌افزاری که سیستم

www.takbook.com

عامل میکروتیک بر روی آن اجرا شده است را نشان داده است، در قسمت شماره‌ی سه می‌توانید تنظیمات خود را در Workspaceهای مختلف قرار دهید که این کار برای منظم کردن آن است، در قسمت شماره‌ی چهار هم گزینه‌های دیگری وجود دارد که اگر بر روی New Winbox کلیک کنید یک Winbox جدید باز خواهد شد، گزینه‌ای با نام Safe Mode وجود دارد که با فعال کردن آن اگر تنظیمی در روتر انجام شود با قطع ارتباط شما با روتر آن تنظیمات به حالت اولیه بر می‌گردد و ذخیره نخواهد شد.

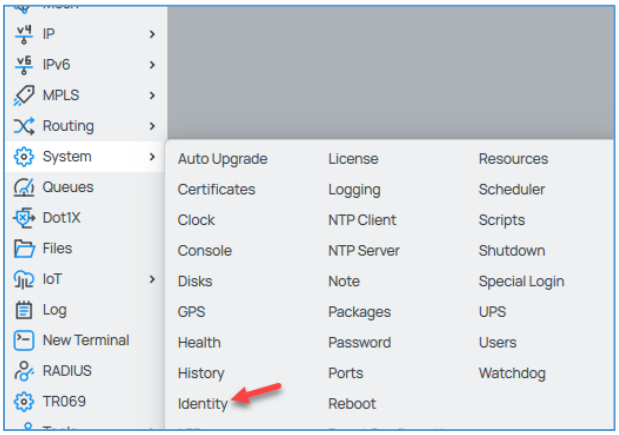


شکل ۷- ۱۶ صفحه اول Winbox

بعد از اینکه سیستم‌عامل میکروتیک را فعال کردیم باید کارهای اولیه را بر روی آن انجام دهیم.

۷-۷ تغییر نام روتر میکروتیک

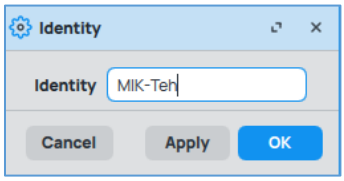
اولین قدیم این است که کارهای خود را به صورت منظم پیش ببرید، برای شروع به مانند شکل ۷-۱۷ از قسمت IP گزینه‌ی identity را انتخاب کنید تا بتوانیم نام روتر را تغییر دهیم.



شکل ۷- ۱۷ تغییر نام میکروتیک

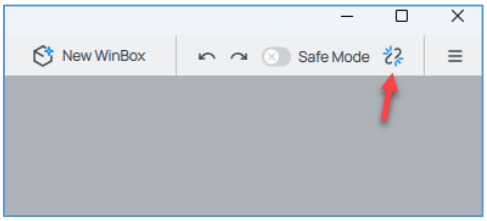
www.takbook.com

به مانند شکل ۷-۱۸ نام روتر خود را وارد کنید.



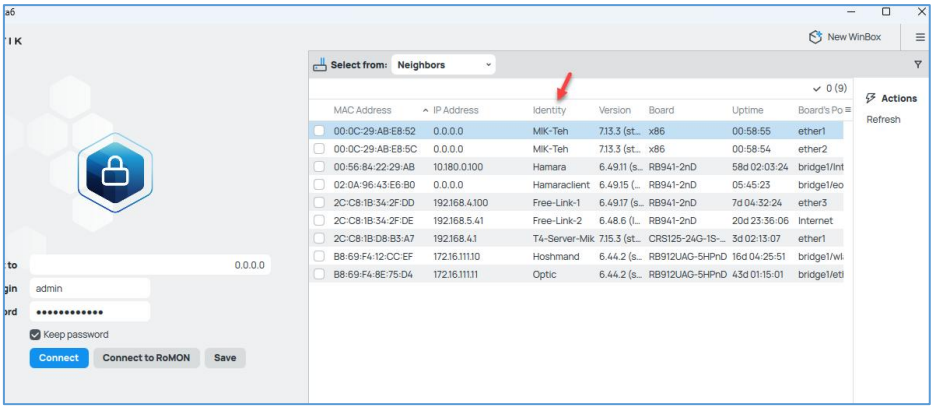
شکل ۷- ۱۸ تغییر نام میکروتیک

به مانند شکل ۷-۱۹در گوشه و سمت راست روتر بر روی آیکون قطع ارتباط کلیک کنید.



شکل ۷- ۱۹ قطع ارتباط میکروتیک

حالا اگر به مانند شکل ۷-۲۰ به قسمت identity نگاه کنید نام روتر شما مشخص است و به راحتی می‌توانید روتر خود را تشخیص دهید.



شکل ۷- ۲۰ ورود به میکروتیک

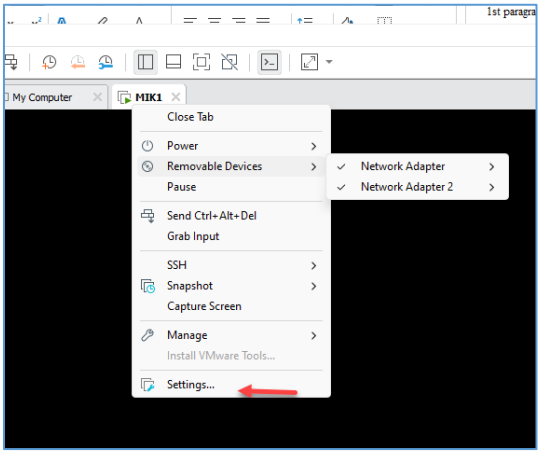
۷-۸ تنظیم نام پورت های ورودی و خروجی

اولین کاری که انجام می‌دهیم، مشخص کردن پورت ورودی و خروجی به میکروتیک است، همان‌طور که قبلاً توضیح دادیم دو پورت برای روتر میکروتیک در نظر گرفتیم؛ یکی برای ورود اینترنت به داخل میکروتیک و دیگری انتقال اینترنت به شبکه‌ی داخلی و فعال کردن سرویس‌های مختلف.

www.takbook.com

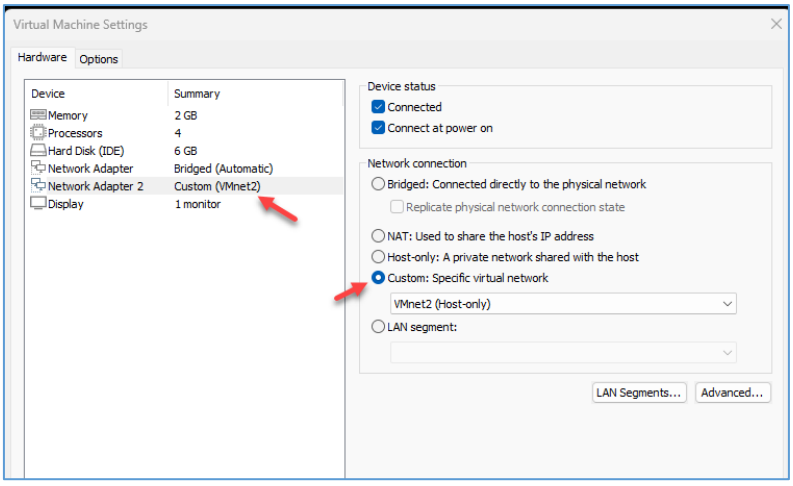
برای شروع باید وارد VMware Workstation شویم و یکی از کارت‌ها را به صورت Host Only در نظر بگیریم و دیگری را به صورت Bridge که به شبکه‌ی اینترنت متصل شود.

طبق شکل ۷-۲۱ بر روی ماشین مورد نظر خود کلیک راست کنید و گزینه‌ی Propeties را انتخاب کنید.



شکل ۷- ۲۱ تنظیم نام کارت شبکه

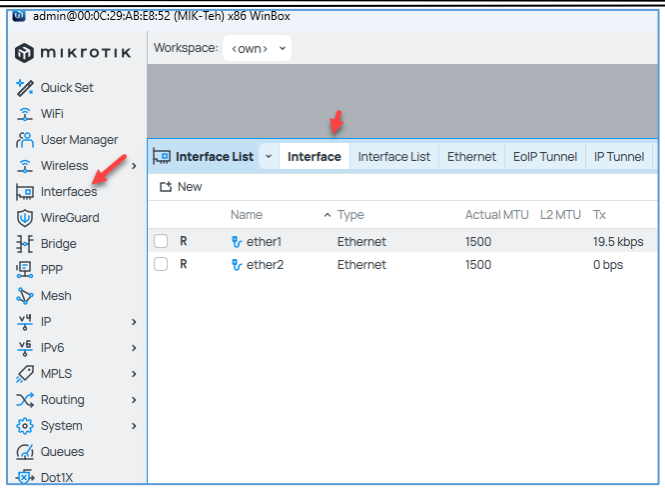
در ادامه کار و طبق شکل ۷-۲۲، کارت شبکه‌ی دوم را در حالت Host Only قرار می‌دهیم، تا به شبکه‌ی داخلی ما متصل شود، توجه داشته باشید که کلاینت‌ها برای اینکه از میکروتیک سرویس بگیرند باید به این شبکه متصل شوند.



شکل ۷- ۲۲ تنظیم کارت شبکه

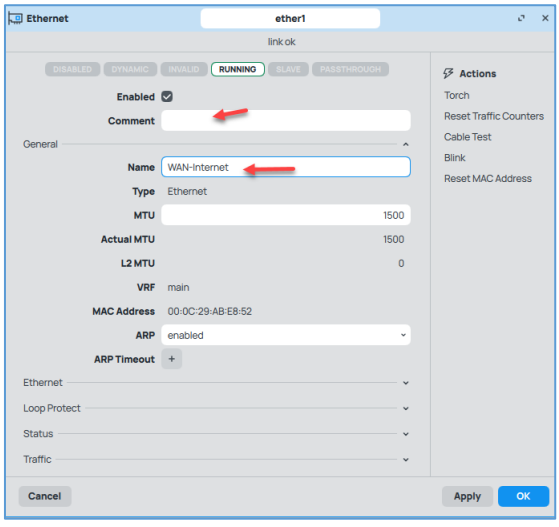
در ادامه و طبق شکل ۷-۲۳، وارد میکروتیک شوید و از سمت چپ، بر روی Interface کلیک کنید ، بر روی هر کدام از این کارت شبکه‌ها کلیک کنید و نام آنها را تغییر دهید.

www.takbook.com



شکل ۷- ۲۳ تنظیم کارت شبکه

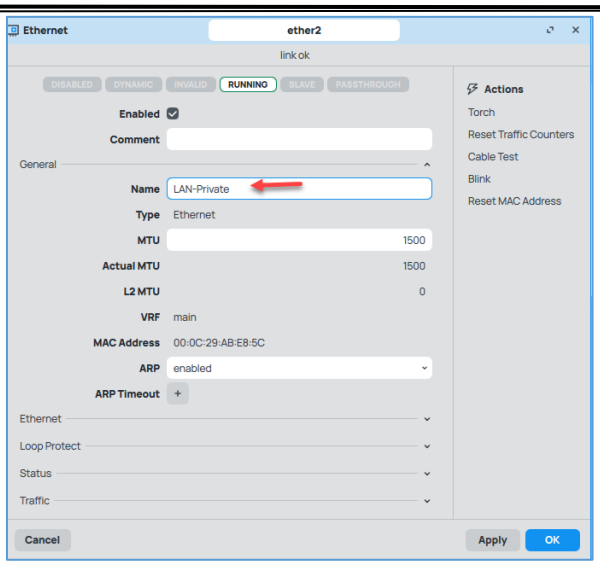
در شکل ۷-۲٤، نام کارت شبکه‌ی Internet را مشخص می‌کنیم، توجه داشته باشید در قسمت Comment می‌توانید توضیحات اضافه در مورد آن کارت شبکه بنویسید تا مدیریت آن راحت‌تر باشد و کار نظم داشته باشد.



شکل ۷- ۲۴ تنظیم شبکه اینترنت

همان‌طور که در شکل ۷-۲۵، مشاهده می‌کنید نام هر دو کارت شبکه تغییر کرده یکی داخلی و دیگری خارجی.

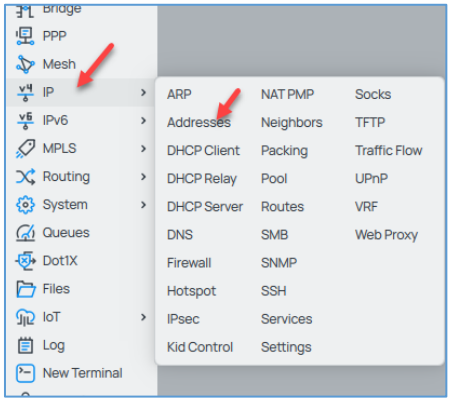
www.takbook.com



شکل ۷- ۲۵ تنظیم شبکه‌ی داخلی

۷-۹ آدرس شبکه‌ی داخلی

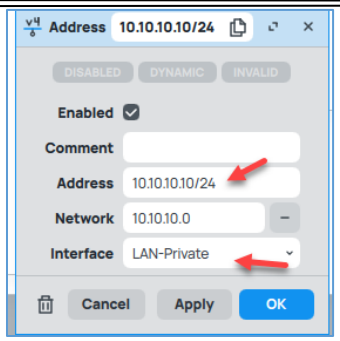
برای اینکه به شبکه‌ی داخلی خود آدرس دهیم باید به صورت شکل ۷-۲۶، وارد قسمت IP Address شویم.



شکل ۷- ۲۶ آدرس برای کارت شبکه

در ادامه طبق شکل ۷-۲۷، با کلیک بر روی New آدرس مورد نظر داخلی خود را وارد کنید، توجه داشته باشید در قسمت Interface باید نام کارت شبکه‌ی داخلی را انتخاب کنید.

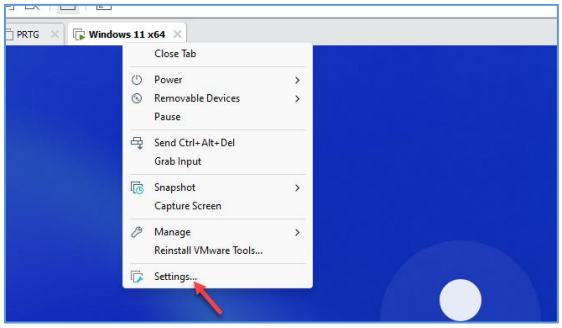
www.takbook.com



شکل ۷- ۲۷ آدرس شبکه‌ی داخلی

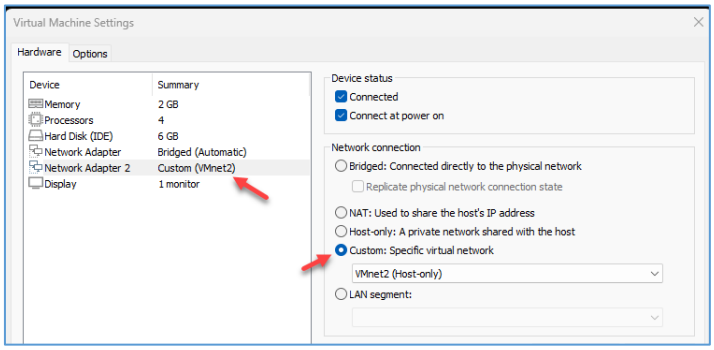
بعد از اینکه به کارت شبکه داخلی آدرس دادیم می‌توانیم وارد یکی از کلاینت‌های خود شویم و ارتباط میکروتیک را با آن تست بگیریم.

برای این کار یک ماشین مجازی فعال کردیم و بر روی آن ویندوز 11 نصب کردیم و برای اینکه کارت شبکه‌ی آن را به مانند کارت شبکه داخلی میکروتیک قرار دهیم باید طبق شکل ۷-۲۸، وارد Setting شویم.



شکل ۷- ۲۸ ورود به تنظیمات ویندوز

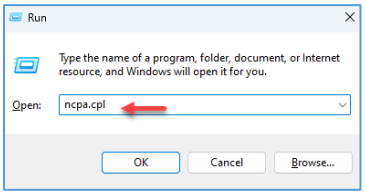
در شکل زیر کارت شبکه‌ی این ماشین را بر روی VMnet2 قرار دهید، در قسمت قبل کارت شبکه‌ی میکروتیک را بر روی VMnet2 قرار دادیم.



شکل ۷- ۲۹ تنظیم کارت شبکه

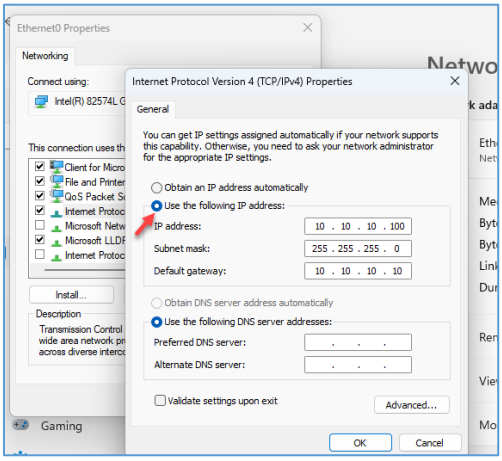
www.takbook.com

در کلاینت مورد نظر برای تست، یک آدرس در رنج همان میکروتیک قرار می‌دهیم، برای تنظیم کارت شبکه به مانند شکل ۷-۳۰ در Run دستور ncpa.cpl را اجرا کنید.



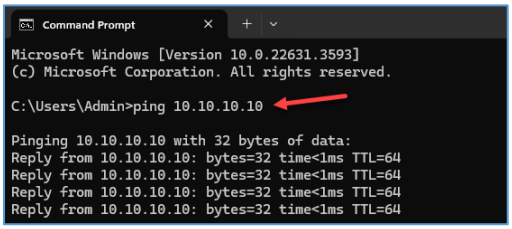
شکل ۷- ۳۰ ورود به تنظیمات کارت شبکه

بعد از باز شدن صفحه‌ی مورد نظر به مانند شکل ۷-۳۱، بر روی کارت شبکه خود کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید و آدرس در رنج شبکه میکروتیک قرار دهید.



شکل ۷- ۳۱ تغییر آدرس IP به صورت دستی

حالا اگر آدرس روتر میکروتیک را Ping کنید به مانند شکل ۷-۳۲، مشاهده خواهید کرد که با موفقیت انجام می‌شود.



شکل ۷- ۳۲ بررسی ارتباط با شبکه

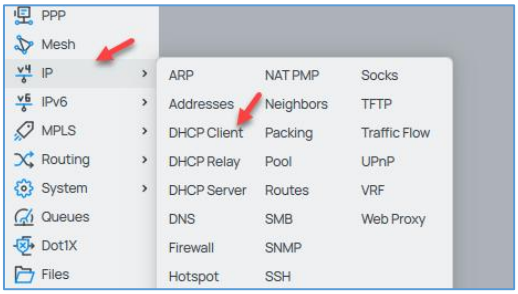
www.takbook.com

۷-۱۰ فعال‌سازی اینترنت در میکروتیک

برای اینکه میکروتیک دارای اینترنت شود شما باید از سرویس دهنده‌های اینترنت، سرویس تهیه کنید، چند حالت وجود دارد که سرویس تهیه کنید:

۱- سرویس ADSL
۲- سرویس LTE
۳- سرویس رادیویی
۴- سرویس فیبر نوری

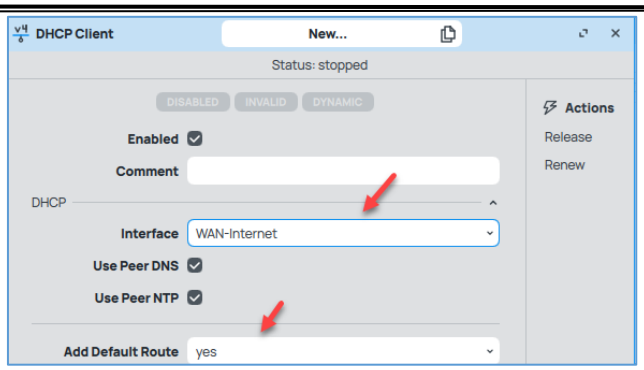
بعد از اینکه سرویس را خریداری کردید باید از طریق مودم یک کابل به پورت WAN میکروتیک که در قسمت‌های قبلی مشخص کردیم بزنید، در این حالت برای اینکه با شرکت سرویس دهنده ارتباط برقرار کنیم یا باید ارتباط مستقیم بگیریم و از کانکشن PPoE استفاده کنیم و یا اینکه مودم اینترنت را Bridge کنیم و داخل میکروتیک به آن آدرس دهیم که هر کدام از این روش‌ها بنا به نیاز خودتان انجام می‌دهیم. در این قسمت ما برای اینکه به میکروتیک اینترنت دهیم و از مودم اطلاعات بگیریم از سرویس DHCP Client استفاده می‌کنیم برای این کار به مانند شکل ۷-۳۳ وارد DHCP-Client شوید.



شکل ۷- ۳۳ تنظیم DHCP Client

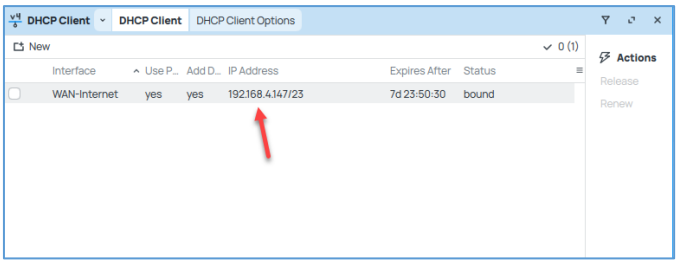
در ادامه کار بر روی New کلیک کنید و به مانند شکل باز شده‌ی ۷-۳۴، در قسمت Interface نام کارت شبکه‌ی خارجی را انتخاب کنید تا بتوانیم از آن آدرس دریافت کنیم، توجه داشته باشید برای اینکه به صورت اتوماتیک این کارت شبکه در قسمت روتینگ قرار بگیرد باید گزینه‌ی Add Default Route را بر روی Yes قرا دهید با این کار روتر اگر به دنبال آدرسی بگردد که در شبکه‌ی داخلی وجود ندارد آن را به کارت شبکه‌ی WAN ارسال می‌کند که همان اینترنت است.

www.takbook.com



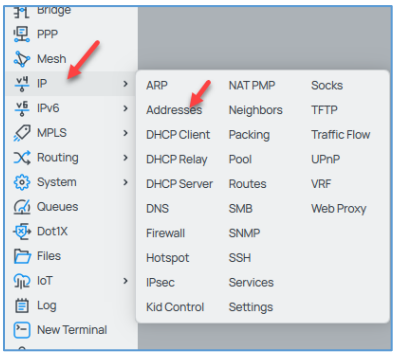
شکل ۷- ۳۴ مشخص کردن کارت شبکه اینترنت

همان‌طور که در شکل ۷-۳۵، مشاهده می‌کنید یک آدرس جدید دریافت شده که این آدرس از طریق سرویس DHCP که در مودم قرار دارد و تنظیم شده است ارسال شده است که DHCP-Client آن را دریافت کرده است.



شکل ۷- ۳۵ دریافت آدرس IP

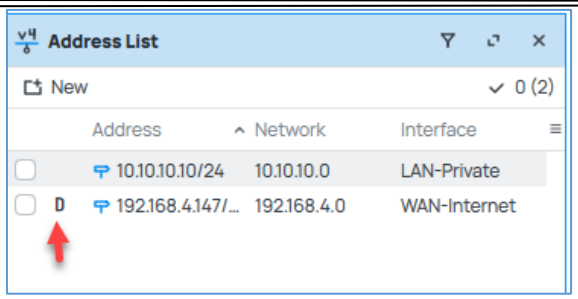
حالا اگر طبق شکل ۷-۳۶، وارد IP Address شوید این آدرسی که دریافت کرده را مشاهده می‌کنید.



شکل ۷- ۳۶ تخصیص آدرس برای کارت شبکه

توجه داشته باشید که طبق شکل ۷-۳۷، علامت D در کنار آدرس نشان دهنده‌ی Dynamic بودن آدرس است که به صورت اتوماتیک دریافت شده است.

www.takbook.com



شکل ۷- ۳۷ آدرس‌های کارت شبکه

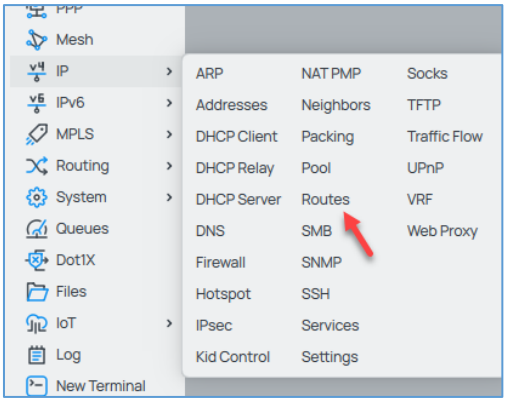
۷-۱۱ فعال‌سازی دسترسی کاربران به اینترنت

برای اینکه کلاینت ما دارای اینترنت شود، باید آدرس‌های داخلی شبکه را با استفاده از NAT به دنیای اینترنت ارسال کنیم، برای انجام آن دو کار باید انجام داد:

۱- روت کردن به سمت اینترنت

۲- ترجمه کردن آدرس در اینترنت

برای اینکه یک روت بنویسیم کافی است به مانند شکل ۷-۳۸، از قسمت IP وارد Route شوید.



شکل ۷- ۳۸ تنظیم Route در میکروتیک

در شکل ۷-۳۹، چند آدرس را مشاهده می‌کنید، اولین آدرس شبکه‌ی داخلی است (10.10.10.0/24) که بعد از اینکه در قسمت IP address این آدرس را وارد کردیم به صورت اتوماتیک در این قسمت قرار گرفته است، سه شبکه دیگر هم مشاهده می‌کنید که شبکه 192.168.4.0/23 همان آدرسی است که از طریق DHCP دریافت کردیم و دو آدرس دیگر (192.168.4.1-192.168.5.1) مربوط به آدرس مودمی است که از آن اینترنت دریافت می‌کنید و از طریق DHCP دریافت شده، شاید برای شما یک آدرس IP وجود داشته باشد.

در پشت هر روت چند حرف مشاهده می‌کنید که عبارت‌اند از:

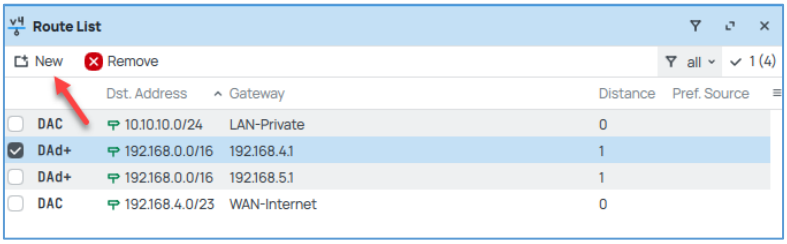
www.takbook.com

D : به معنی Dynamic بودن آن روت است و این روت توسط خود سیستم به صورت اتوماتیک ایجاد شده است و نمی‌توانید تغییراتی در آن ایجاد کنید.

A : به معنی فعال بودن روت مورد نظر است.

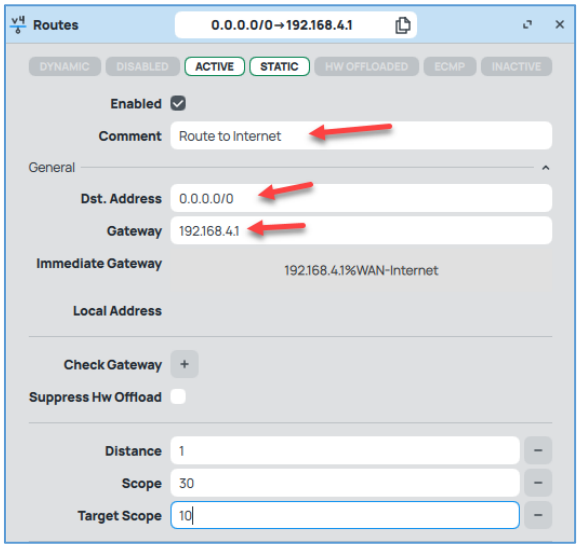
C : به این معنی است که آن روت روی یکی از کارت‌های های شبکه تنظیم شده است و فعال است.

در زیر مثلاً علامت DAd+ به این معنی است نوع شبکه از نوع Dynamic است که فعال است و علامت d کوچک به این معنی است که این روت از روی DHCP دریافت شده است.



شکل ۷- ۳۹ تنظیم Route در میکروتیک

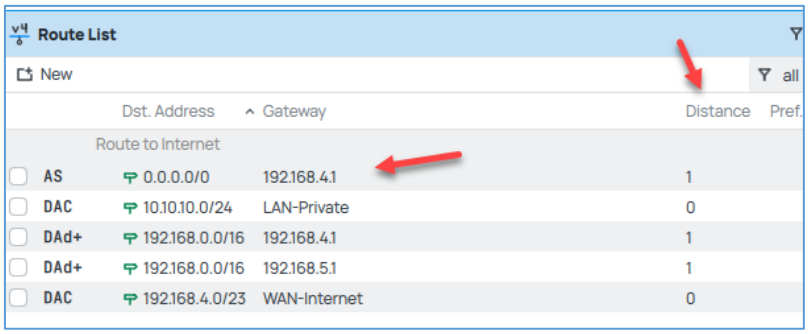
در ادامه برای اینکه یک Route به صورت دستی ایجاد کنیم باید بر روی New کلیک کنید و به مانند شکل ۷-۴۰ آدرس 0.0.0.0/0 را در قسمت Dst.Address وارد کنید، این چهار صفر به این معنی است که هر شبکه‌ای که ناشناخته بود و در روتر پیدا نشد بفرست به شبکه‌ای که در قسمت Gateway مشخص کردیم که همان اینترنت است، در اینجا با نوشتن آدرس 192.168.4.1 که به سمت اینترنت می‌رود تمام ترافیک را به آن سمت ارسال می‌کنیم.



شکل ۷- ۴۰ مشخص کردن Gateway

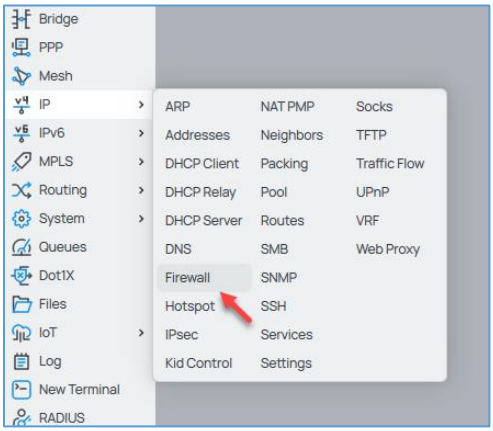
www.takbook.com

همان‌طور که در شکل ۷-٤۱ مشاهده می‌کنید در قسمت Route آدرس مورد نظر اضافه شده است، علامتی که به آن اختصاص داده شده AS است که به معنی A(Active) و S(Static) است، در قسمت Distance هم اولویت یک مسیر مشخص می‌شود که هر چقدر این عدد پایین‌تر باشد اولویت بالاتر است.



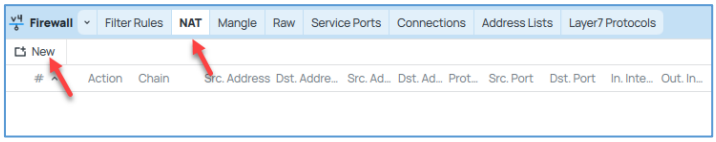
شکل ۷- ۴۱ بررسی مقدار Distance

بعد از اینکه روت را تعریف کردیم حالا باید آدرس‌های داخل شبکه را به اینترنت ترجمه کنیم یا همان NAT کنیم، برای این کار طبق شکل ۷-٤۲، از قسمت IP گزینه‌ی فایروال را انتخاب کنید.



شکل ۷- ۴۲ ورود به فایروال

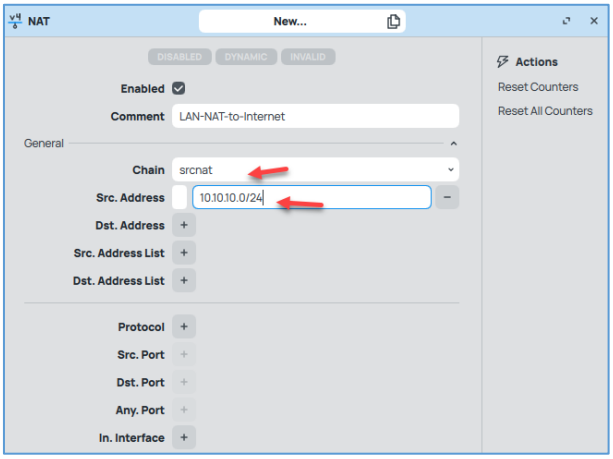
در شکل ۷-٤۳، تب‌های مختلفی را مشاهده می‌کنید که در ادامه روی آنها کار خواهیم کرد، در حال حاضر وارد تب NAT شوید و بر روی New کلیک کنید.



شکل ۷- ۴۳ ایجاد NAT در فایروال

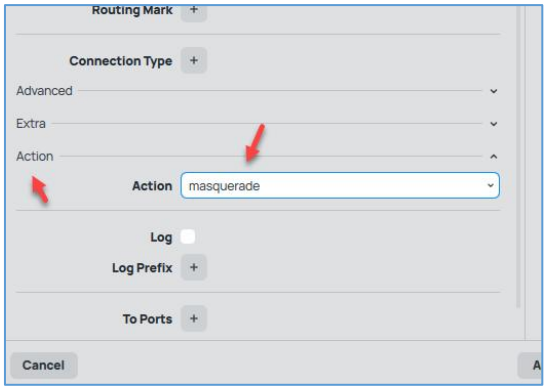
www.takbook.com

در شکل ۷-٤٤ و در قسمت Src.Address باید مشخص کنید که آدرس شبکه‌ی داخلی شما چیست، منظور از Src.Address آدرس Source یا همان مبدا است و منظور از Dst.Address آدرس مقصد است که ما چون می‌خواهیم آدرس شبکه‌ی داخلی یعنی مبدا را به اینترنت ارسال کنیم باید Src.Address را انتخاب کنیم.



شکل ۷- ۴۴ ایجاد NAT در فایروال

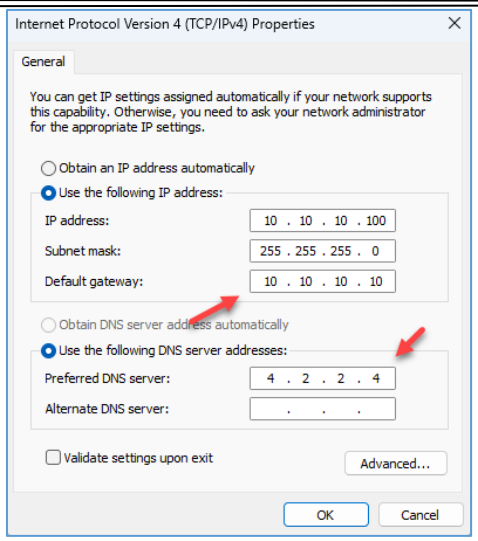
در ادامه طبق شکل ۷-٤٥، وارد قسمت Action شوید و گزینه‌ی masquerade را انتخاب کنید، این گزینه برای ترجمه کردن آدرس به خارج از شبکه است، بعد از این کار بر روی OK کلیک کنید و حالا باید وارد کلاینت شویم و ارتباط با اینترنت را چک کنیم.



شکل ۷- ۴۵ ایجاد NAT در فایروال

طبق شکل ۷-٤٦، وارد کلاینت مورد نظر شوید، توجه داشته باشید اگر آدرس را به صورت دستی وارد می‌کنید باید در قسمت Gateway آدرس داخلی روتر را وارد کنید که در شکل۷-٤٦، مشخص است و برای DNS هم یک آدرس عمومی مانند 4.2.2.4 یا 1.1.1.1 مشخص کنید.

www.takbook.com



شکل ۷- ۴۶ مشخص کردن *Gateway*

حالا اگر مرورگر خود را باز کنید مشاهده خواهید کرد به اینترنت متصل شدید که طبق شکل ۷-۴۷ این موضوع مشخص است.



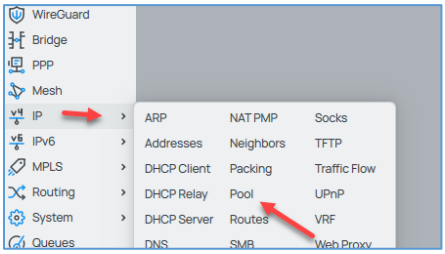
شکل ۷- ۴۷ بررسی صفحه وب

۷-۱۲ تنظیم DHCP در میکروتیک

برای اینکه بتوانیم کلاینت‌های خود را مدیریت کنیم و به صورت اتوماتیک به آنها آدرس اختصاص دهیم باید از سرویس DHCP استفاده کنیم، البته در بعضی از سازمان‌ها DHCP را در سرور ویندوز فعال می‌کنند ولی ما می‌خواهیم در میکروتیک فعال کنیم.

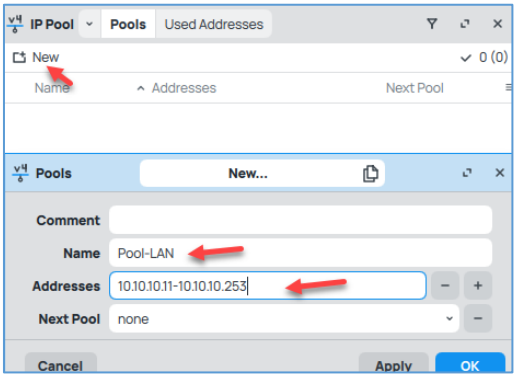
www.takbook.com

اولین کاری که باید انجام دهیم باید یک Pool از آدرس‌های شبکه داخلی ایجاد کنیم، برای این کار طبق شکل ۷–٤۸، از قسمت IP گزینه‌ی Pool را انتخاب کنید.



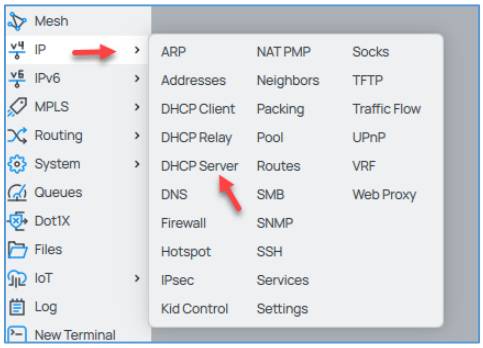
شکل ۷- ۴۸ تنظیم DHCP در میکروتیک

در شکل ۷–٤۹ بر روی New کلیک کنید و یک نام برای Pool خود در نظر بگیرید که بعداً از این نام استفاده خواهیم کرد.



شکل ۷- ۴۹ ایجاد Pool

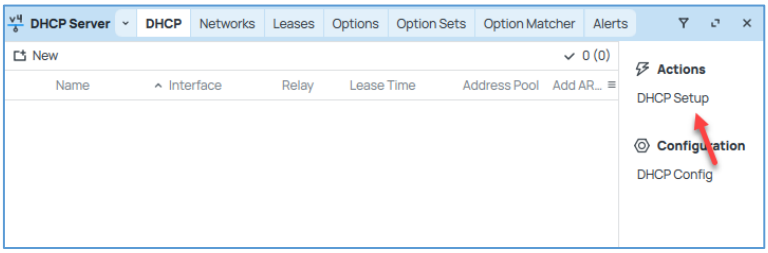
در ادامه طبق شکل ۷–۵۰، باید وارد سرویس DHCP شویم و تنظیمات آن را انجام دهیم، برای این کار از قسمت IP گزینه‌ی DHCP Server را انتخاب کنید.



شکل ۷- ۵۰ تنظیم DHCP Server

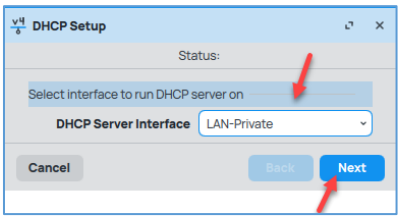
www.takbook.com

در شکل ۷-۵۱، بر روی DHCP Config کلیک کنید.



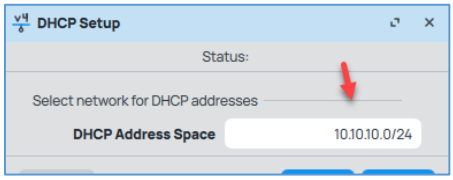
شکل ۷-۵۱ تنظیم DHCP Server

در ادامه کار باید کارت شبکه داخلی را که قرار است به کلاینت ها آدرس اختصاص دهیم را انتخاب کنید که این کار را طبق شکل ۷-۵۲ انجام دهید.



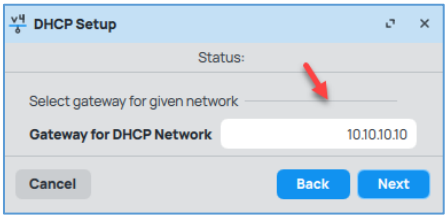
شکل ۷-۵۲ تنظیم DHCP Server

در شکل ۷-۵۳، باید آدرس شبکه‌ی خود را وارد کنید که البته به صورت اتوماتیک با انتخاب کارت شبکه‌ی داخلی نوشته می‌شود.



شکل ۷-۵۳ تنظیم DHCP Server

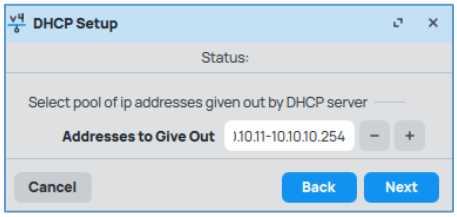
در شکل ۷-۵۴، باید آدرس Gateway که همان آدرس روتر میکروتیک است را وارد کنید.



شکل ۷-۵۴ تنظیم DHCP Server

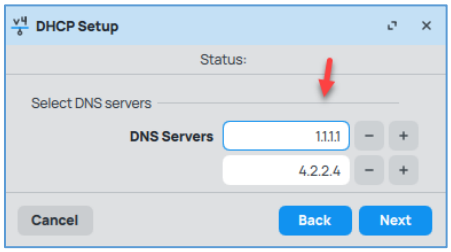
www.takbook.com

در شکل ۷-۵۵، باید در قسمت Give Out باید رنج آدرسی وارد کنید (10.10.10.11-10.10.10.254) تا به کلاینت‌خا اختصاص داده شود، توجه داشته باشید می‌توانید بر روی دکمه منفی کلیک کنید تا حذف شود و در ادامه از آن Pool که مشخص کردیم استفاده کنیم.



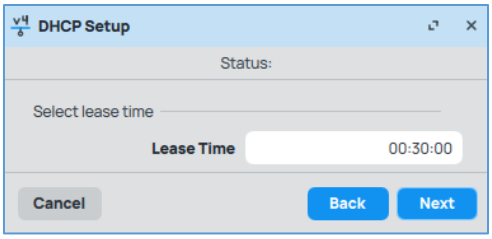
شکل ۷- ۵۵ تنظیم DHCP Server

در شکل ۷-۵۶، باید آدرس DNS را وارد کنید، توجه داشته باشید تمام این مواردی که مشخص می‌کنید به کلاینت داده خواهد شد.



شکل ۷- ۵۶ تنظیم DHCP Server

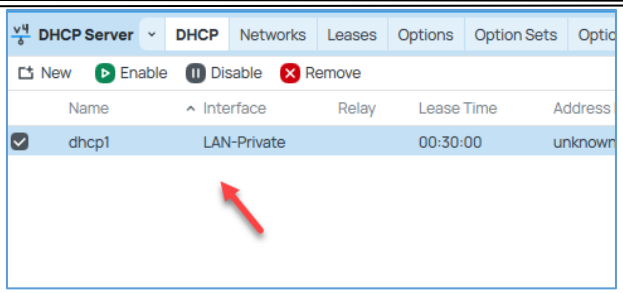
در شکل ۷-۵۷، مشخص کنید تا چه زمانی آدرس از کلاینت پگس گرفته شود، یعنی اگر کلاینت مورد نظر آنلاین نبود آن آدرس از آن پس گرفته شده و به کلاینت دیگر داده خواهد شد.



شکل ۷- ۵۷ تنظیم DHCP Server

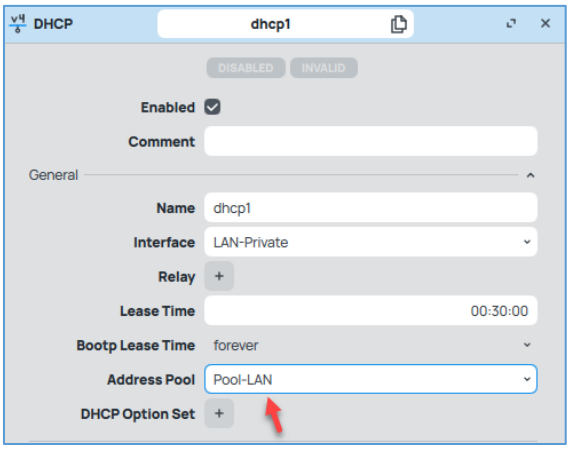
بعد از ایجاد به مانند شکل ۷-۵۸، بر روی DHCP دوبار کلیک کنید.

www.takbook.com



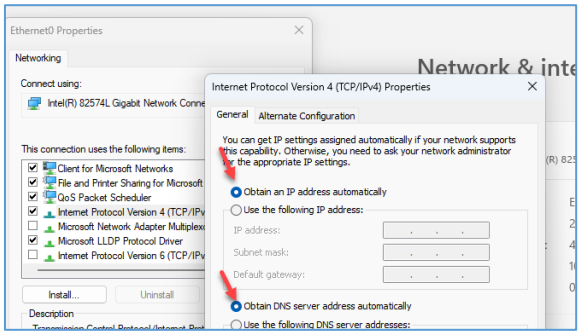
شکل ۷- ۵۸ تنظیم DHCP Server

در شکل ۷–۵۹، و از قسمت Address Pool باید Pool مورد نظر خود را انتخاب کنیم.



شکل ۷- ۵۹ تنظیم DHCP Server

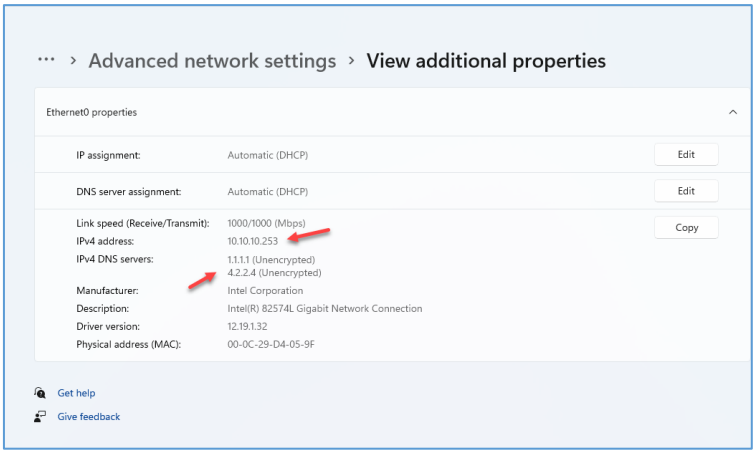
حالا همه چیز حاضر است تا به کلاینت آدرس تخصیص داده شود، برای تست این موضوع طبق شکل ۷–۶۰، وارد کلاینت شوید و کارت شبکه را بر روی حالت اتوماتیک قرار دهید تا آدرس جدید از طریق سرویس DHCP مربوط به میکروتیک دریافت شود.



شکل ۷- ۶۰ تنظیم DHCP Server

www.takbook.com

همان‌طور که در شکل ۷-۶۱، مشاهده می‌کنید، کلاینت مورد نظر آدرس مشخص شده را دریافت کرده است و دارای اینترنت هم شده است.

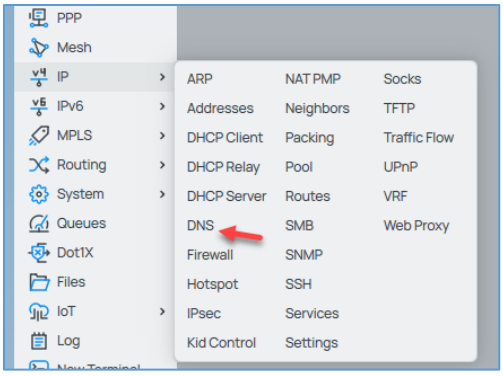


شکل ۷- ۶۱ تنظیم *DHCP Server*

اگر وارد سرویس DHCP شوید و از تب Leases مشاهده کنید کلاینت مورد نظر در لیست قرار گرفته است و نام آن به همراه آدرس IP، MAC و زمان اختصاص داده شدن IP مشخص است.

۷-۱۳ تنظیم DNS در میکروتیک

سرویس DNS یکی از محبوب ترین سرویس‌ها هستش و کار آن تبدیل آدرس IP به نام و بلعکس است، در میکروتیک هم قسمی وجود دارد که می‌توانیم تنظیمات DNS را انجام دهید، به مانند شکل ۷-۶۲، از قسمت IP بر روی DNS کلیک کنید.



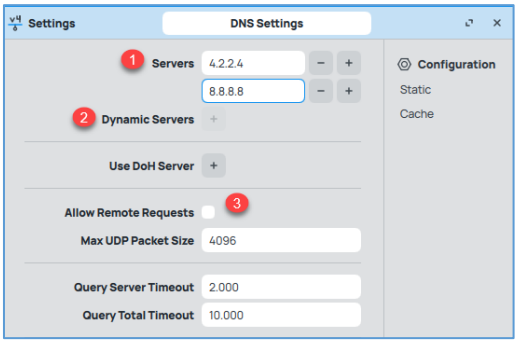
شکل ۷- ۶۲ تنظیم *DNS*

در شکل ۷-۶۳، در قسمت شماره‌ی یک می‌توانید بر روی آیکون+ کلیک کنید و چند آدرس DNS را به صورت دستی وارد کنید، در قسمت شماره‌ی دو آدرس DNS به صورت اتوماتیک ثبت می‌شود این آدرس

www.takbook.com

مثلاً از طریق DHCP دریافت و در این قسمت نمایش داده خواهد شد، در قسمت شماره‌ی سه اگر تیک گزینه‌ی Allow Remote Requests را کلیک کنید به درخواست‌هایی که از طرف کاربران به سرور میکروتیک می‌رسد پاسخ داده خواهد شد و باید این تیک خرده باشد.

احتیاط: توجه داشته باشید اگر تیک Allow Remote Requests را انتخاب کنید مورد حمله قرار خواهید گرفت که باید در فایروال پورت 53 را محدود به شبکه‌ی داخلی کنید.



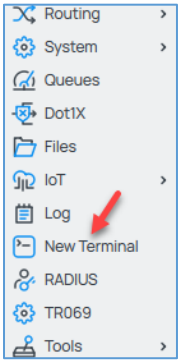
شکل ۷- ۶۳ تنظیم DNS

در خلال کتاب بر روی تمام این سرویس‌ها بیشتر کار خواهیم کرد و با ویژگی های خاص آنها آشنا خواهیم شد.

۷-۱۴ کار با ترمینال در میکروتیک

یکی از ابزارهای خوب میکروتیک استفاده از خط فرمان آن است که می‌توانید تمام کارهایی را که به صورت گرافیکی انجام می‌دهید را به صورت دستور انجام دهید، یکی از ویژگی‌های این روش در اجرای اسکریپت‌ها، لیست‌های طولانی است که در خلال کار بررسی خواهیم کرد.

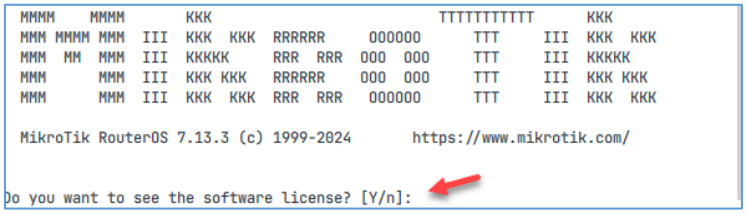
برای بررسی این سرویس به مانند شکل ۷-٦٤، بر روی New Terminal کلیک کنید.



شکل ۷- ۶۴ ترمینال در میکروتیک

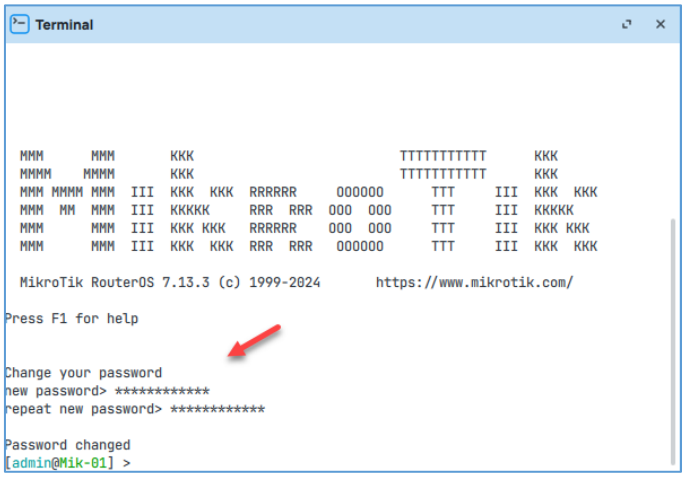
www.takbook.com

در شکل ۷-۶۸، ورژن میکروتیک مورد نظر خود را مشاهده می‌کنید که 7.13.3 است و در قسمت پایین آن از شما سوال می‌شود که آیا می‌خواهید لایسنس استفاده از این سیستم عامل را بررسی کنید که در صورت نیاز باید حرف Y را وارد کنید و در غیر این صورت باید N وارد کنید.



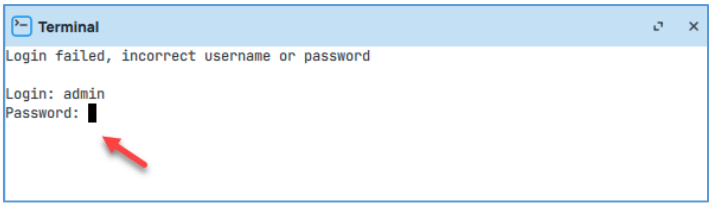
شکل ۷- ۶۵ ترمینال در میکروتیک

در ادامه کار اولین درخواستی که از شما می‌شود این است که رمز عبور جدید را وارد کنید که سعی کنید یک رمز عبور پیچیده باشد و طبق شکل ۷-۶۶ انجام دهید.



شکل ۷- ۶۶ ترمینال در میکروتیک

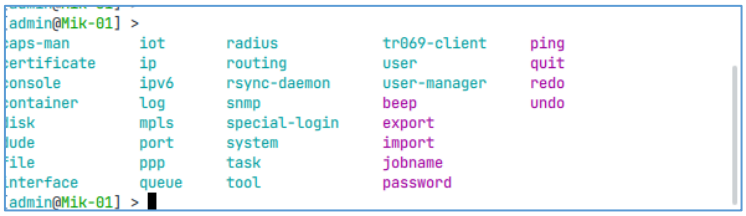
حالا اگر به مانند شکل ۷-۶۷، ترمینال را ببندید و دوباره اجرا کنید از شما نام کاربری و رمز عبور درخواست می‌شود.



شکل ۷- ۶۷ ترمینال در میکروتیک

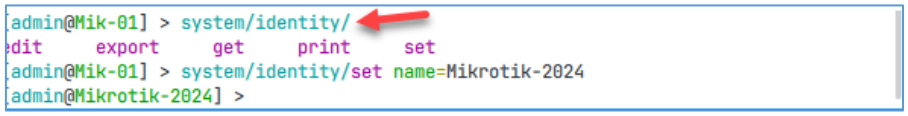
www.takbook.com

کار با دستورات میکروتیک بسیار آسان است و برای شروع بهتر است به مانند شکل ٦-٦٨، از کلید TAB استفاده کنید، با زدن کلید TAB لیست دستوراتی که باید در اول خط وارد کنید را مشاهده می‌کنید، اگر به شکل گرافیکی Winbox دقت کنید این دستورات همان قسمت‌های اولیه هستند که در Winbox وجود دارد.



شکل ۷- ۶۸ ترمینال در میکروتیک

مثلاً برای اینکه نام روتر میکروتیک خود را تغییر دهیم باید به صورت شکل ۷-٦۹، اول وارد System شوید و بعد وارد identity و در ادامه با زدن دکمه TAB ویژگی‌های آن دستور نمایش داده می‌شود که با وارد کردن دستور Set و بعد از آن زدن دکمه TAB و وارد کردن اسم جدید می‌توانید نام روتر را تغییر دهید. پس با این دستور نتیجه می‌گیریم که برای نمایش جزئیات دیگر یک دستور باید از دستور TAB استفاده کنید.



شکل ۷- ۶۹ ترمینال در میکروتیک

مثلاً می‌توانید طبق شکل ۷-۷۰، با استفاده از دستور Ping سایت مورد نظر خود را Ping بگیرید که البته این دستور متوقف نخواهد شد و باید با کلید CTRL + C این کار را انجام دهید.



شکل ۷- ۷۰ ترمینال در میکروتیک

یکی دیگر از دستورات مهم در ترمینال دستور Print است که باید به صورت شکل۷-۷۱، اجرا کنید، مثلاً وارد قسمت Nat شوید و دستور Print را اجرا کنید، همان‌طور که در شکل ۷-۷۱، مشاهده می‌کنید، تنظیمی

www.takbook.com

که قبلاً در این قسمت انجام دادیم برای ما نمایش داده است و این می‌تواند بسیار کمک کننده باشد، توجه به این نکته مهم است که با علامت / شما می‌توانید به اول خط فرمان برگردید.

```
[admin@Mikrotik-2024] > ip/firewall/nat
[admin@Mikrotik-2024] /ip/firewall/nat> print
Flags: X - disabled, I - invalid; D - dynamic
 0    ;;; LAN-NAT-to-Internet
      chain=srcnat action=masquerade src-address=10.10.10.0/24 log=no
      log-prefix=""
```

شکل ۷- ۷۱ ترمینال در میکروتیک

دستور Print را می‌توان برای نمایش Interfaceهای یک روتر میکروتیک استفاده کرد، مثلاً در شکل ۷-۷۲، با دستور interface print لیست Interfaceها به همراه Mac آدرس آنها نمایش داده شده است.

```
[admin@Mikrotik-2024] > /interface print
Flags: R - RUNNING
Columns: NAME, TYPE, ACTUAL-MTU, MAC-ADDRESS
#   NAME          TYPE   ACTUAL-MTU  MAC-ADDRESS
0 R LAN-Private   ether        1500  00:0C:29:08:5A:00
1 R WAN-Internet  ether        1500  00:0C:29:08:5A:F6
[admin@Mikrotik-2024] >
```

شکل ۷- ۷۲ ترمینال در میکروتیک

در موقعیتی شاید شما نتوانید از طریق Winbox به روتر میکروتیک خود متصل شوید و باید به نحوی متوجه آدرس IP روتر شوید برای این کار طبق شکل ۷-۷۳، باید از دستور /ip address print استفاده کنید.

```
[admin@Mikrotik-2024] >
[admin@Mikrotik-2024] > /ip address print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
#   ADDRESS            NETWORK      INTERFACE
0   10.10.10.10/24     10.10.10.0   LAN-Private
1 D 192.168.4.147/23   192.168.4.0  WAN-Internet
[admin@Mikrotik-2024] >
```

شکل ۷- ۷۳ ترمینال در میکروتیک

اگر بخواهیم بر روی یک Interface آدرس IP قرار دهیم باید به صورت زیر دستور را وارد کنیم:

/ip address add address=192.168.1.1/24 interface=LAN-Private

همان‌طور که در شکل ۷-۷٤، مشاهده می‌کنید با استفاده از این دستور و مشخص کردن نام Interface یک آدرس جدید به آن تخصیص داده شد.

www.takbook.com

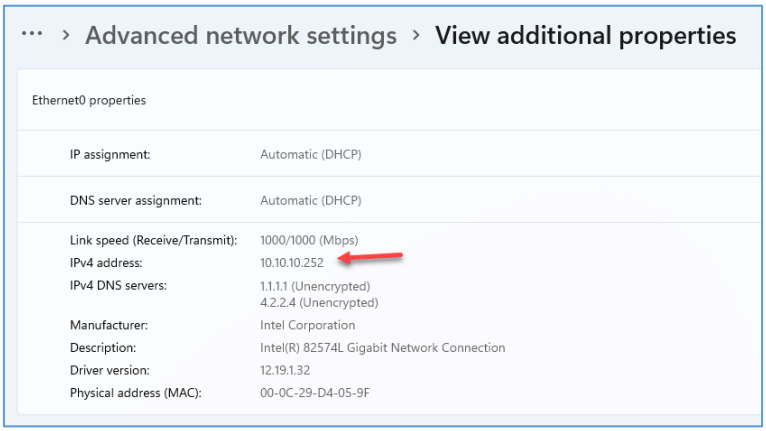

```
[admin@Mikrotik-2024] >
[admin@Mikrotik-2024] > /ip address add address=192.168.1.1/24 interface=LAN-Private
[admin@Mikrotik-2024] >
[admin@Mikrotik-2024] >
[admin@Mikrotik-2024] >
[admin@Mikrotik-2024] > /ip address print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
#   ADDRESS            NETWORK       INTERFACE
0   10.10.10.10/24     10.10.10.0    LAN-Private
1 D 192.168.4.147/23   192.168.4.0   WAN-Internet
2   192.168.1.1/24     192.168.1.0   LAN-Private
[admin@Mikrotik-2024] >
```

شکل ۷- ۷۴ ترمینال در میکروتیک

۷-۱۵ مدیریت پهنای باند کاربران

بعد از اینکه در مراحل قبلی، اینترنت را وارد روتر کردیم و کاربران توانستند از طریق سرویس DHCP آدرس IP و اینترنت دریافت کنند، حالا باید کاری کنیم که کاربران به اندازه‌ای که ما تعیین می‌کنیم، به اینترنت دسترسی داشته باشند؛ در این بحث از سرویس Queues برای محدود کردن کابران استفاده می‌کنیم.

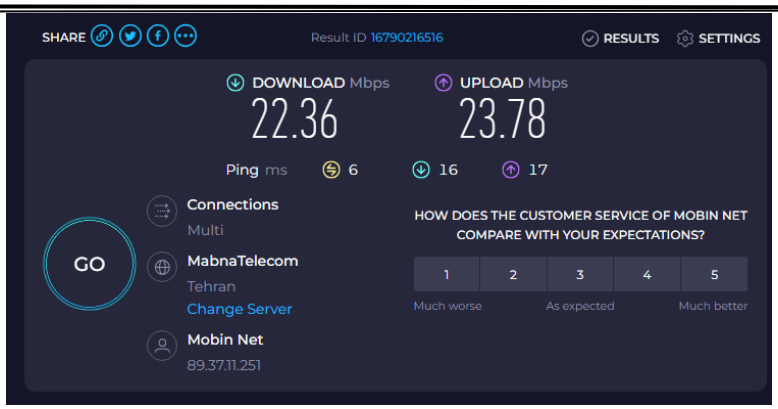
قبل از اینکه این سرویس را بررسی کنیم اول باید بررسی کنیم کلاینت ما چه آدرسی دریافت کرده است، برای بررسی این موضوع اول باید ببینیم آدرس کلاینت مورد نظر چند هست که در شکل ۷-۷۵، این موضوع مشخص شده است.



شکل ۷- ۷۵ مدیریت پهنای باند کاربران

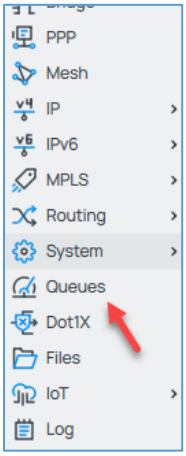
و بعد از آن باید ببینیم که پهنای باند این کلاینت در اینترنت چقدر است که باید طبق شکل ۷-۷۶، وارد سایت speedtest.net شوید و تست سرعت را به صورت زیر انجام دهید که سرعت دانلود و آپلود مشخص شده است.

www.takbook.com



شکل ۷- ۷۶ مدیریت پهنای باند کاربران

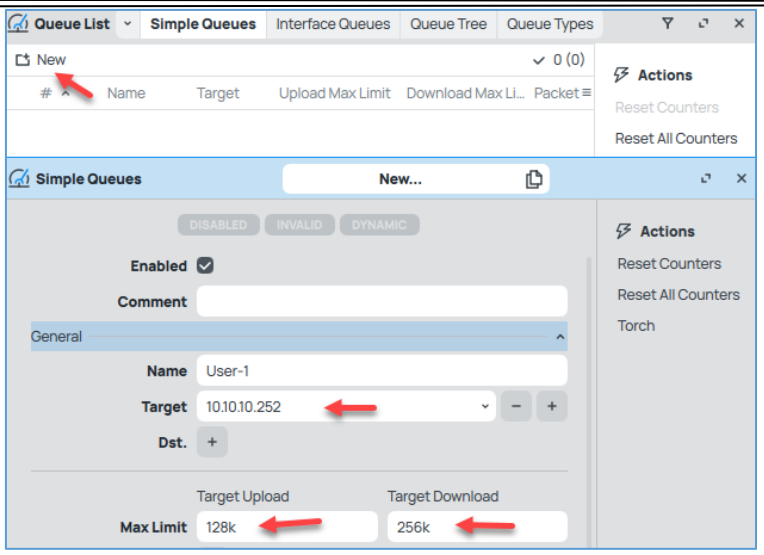
در ادامه کار طبق شکل ۷-۷۷، وارد روتر میکروتیک شوید و از سمت چپ بر روی Queues کلیک کنید.



شکل ۷- ۷۷ مدیریت پهنای باند کاربران

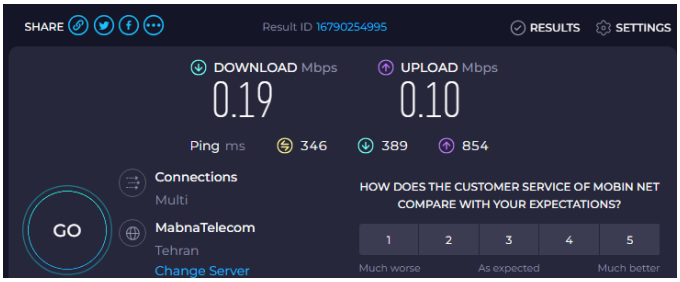
در شکل ۷-۷۸، کاربر ما دارای آدرس 10.10.10.252 است که می‌توانیم برای آن یک Rule تعریف کنیم که حداکثر سرعت دسترسی به اینترنت آن kb۱۲۸ باشد، یا اینکه برای سرعت دانلود و آپلود سرعت جداگانه‌ای در نظر بگیریم. وارد تب Simple Queues شوید و بر روی New کلیک کنید و در قسمت Target آدرس IP کلاینت مورد نظر را وارد کنید و در قسمت Upload و Download باید مقدار مشخص را برای کاربر خود وارد کنید که برای دانلود ۲۵۶ کیلوبایت و برای آپلود ۱۲۸ کیلوبایت در نظر گرفتیم، منظور از K همان کیلوبایت است.

www.takbook.com



شکل ۷- ۷۸ مدیریت پهنای باند کاربران

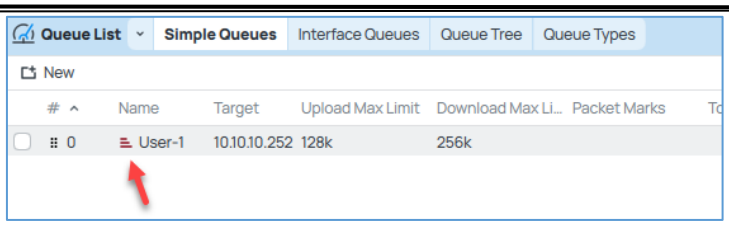
حالا اگر به مانند شکل ۷-۷۹، وارد کلاینت شوید و دوباره سایت بررسی آپلود و دانلود را چک کنید به مانند شکل زیر مقدار دانلود و آپلود به مقداری که وارد کردید تغییر می‌کند.



شکل ۷- ۷۹ مدیریت پهنای باند کاربران

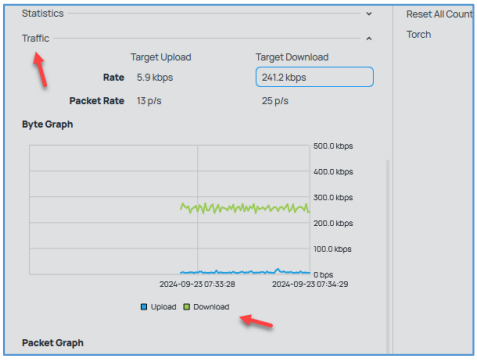
همان‌طور که در شکل ۷-۸۰، مشاهده می‌کنید Rule مورد نظر برای کاربر با آدرس 10.10.10.252، ایجاد شده است که رنگ آیکون آن قرمز شده است، این رنگ به این دلیل است که کاربر مورد نظر در حال استفاده از حداکثر ظرفیت خود است، این آیکون به سه رنگ سبز، زرد و قرمز تغییر حالت می‌دهد که نشان دهنده‌ی استفاده‌ی کاربر از اینترنت است.

www.takbook.com



شکل ۷- ۸۰ مدیریت پهنای باند کاربران

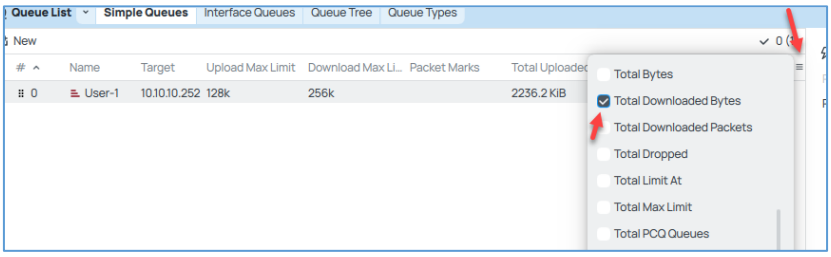
اگر به مانند شکل ۷-۸۱ ، وارد تب Traffic شوید، مقدار مصرف کاربر از اینترنت را مشاهده خواهید کرد.



شکل ۷- ۸۱ مدیریت پهنای باند کاربران

حالا چگونه باید بفهمیم که یک کاربر چه مقدار از اینترنت را مصرف کرده است، برای این کار به شکل ۷-۸۲، توجه کنید.

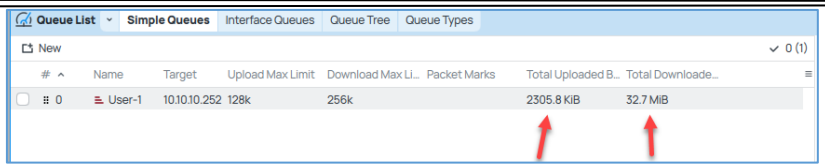
برای مشخص کردن مقدار مصرف اینترنت چند راه وجود دارد؛ یکی اینکه روی آیکون مشخص شده در شکل، کلیک کنید و تیک دو گزینه‌ی Total Uploaded Bytes و Total Download Bytes را انتخاب کنید که در شکل ۷-۸۳، نتیجه‌ی کار را مشاهده می‌کنید.



شکل ۷- ۸۲ مدیریت پهنای باند کاربران

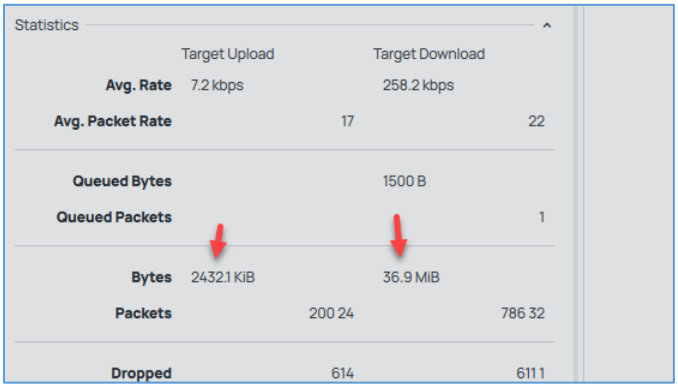
همان‌طور که در شکل ۷-۸۳، مشاهده می‌کنید مقدار مصرف مشخص شده است و مقدار آپلود و دانلود این کلاینت مشخص است.

www.takbook.com



شکل ۷- ۸۳ مدیریت پهنای باند کاربران

راه دیگر برای نمایش مقدار مصرف کاربر از اینترنت، استفاده از تب Statistics می‌باشد که در قسمت‌های مشخص شده مقدار مصرف را مشخص می‌کند، طبق شکل ۷-۸٤، در سمت چپ، مقدار آپلود و در سمت راست، مقدار دانلود را مشخص کرده است. گزینه‌های دیگری هم، مانند مقدار ارسال و دریافت پکت و... وجود دارد.

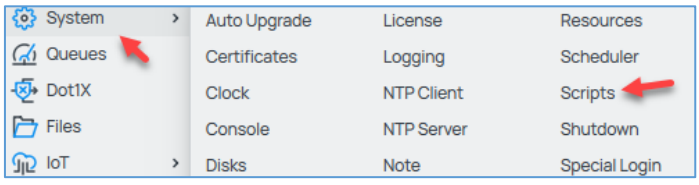


شکل ۷- ۸۴ مدیریت پهنای باند کاربران

۷-۱٦ کار با Script در میکروتیک

در قسمت قبلی یک کلاینت را به صورت دستی در لیست Queues قرار دادیم و سرعت آن را محدود کردیم، حالا اگر تعداد کلاینت‌های ما خیلی زیاد باشد و بخواهیم برای همه‌ی آنها به صورت دستی محدودیت ایجاد کنیم به خاطر همین باید از اسکریپت استفاده کنیم و به صورت اتوماتیک این محدودیت را برای همه کاربران ایجاد کنیم.

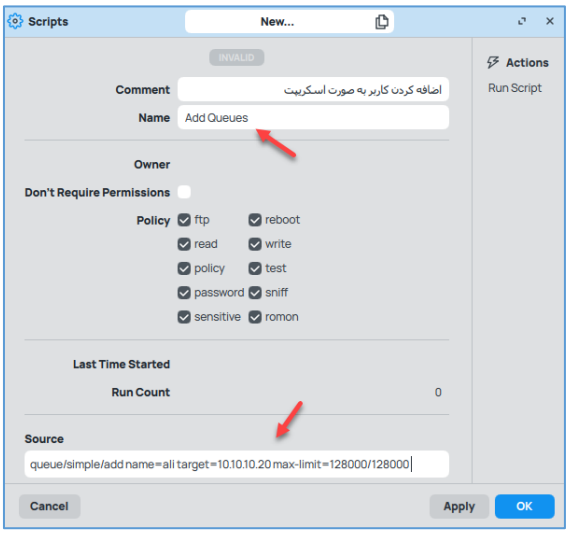
برای شروع به مانند شکل ۷-۸۵، باید وارد System شوید و بعد Scripts را انتخاب کنید.



شکل ۷- ۸۵ Script در میکروتیک

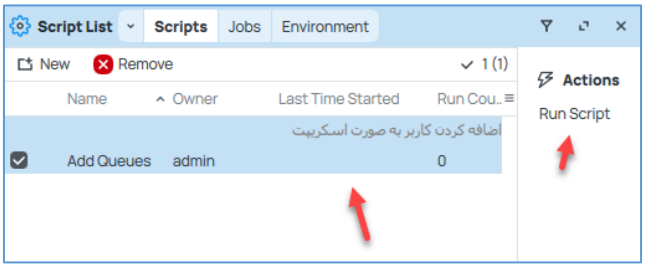
www.takbook.com

در شکل ۷-۸۶، در قسمت Name باید نام اسکریپت خود را وارد کنید و در قسمت Source هم باید دستورات خود را وارد کنید و بر روی Apply کلیک کنید، توجه داشته باشید این دستور یک Queue جدید با نام Ali ایجاد می‌کند و آدرس 10.10.10.20 به همراه سرعت مشخص شده را به آن تخصیص می‌دهد، برای اجرا باید بر روی Run Script کلیک کنید.



شکل ۷-۸۶ Script در میکروتیک

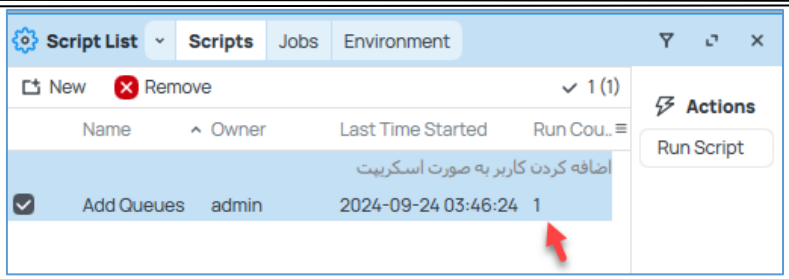
بعد از Save کردن اسکریپت مورد نظر می‌توانید به مانند شکل ۷-۸۷، بر روی Run Script کلیک کنید.



شکل ۷-۸۷ Script در میکروتیک

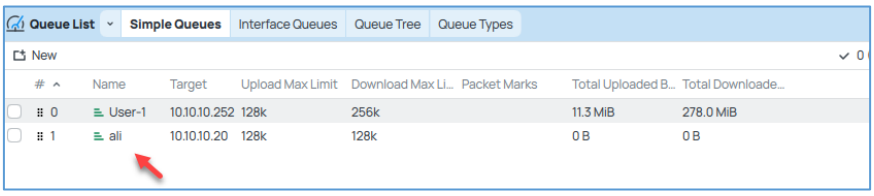
بعد از اجرا طبق شکل ۷-۸۸، مقدار Counter آن برابر یک قرار گرفته است.

www.takbook.com



شکل ۷- ۸۸ Script در میکروتیک

اگر طبق شکل ۷-۸۹، وارد Queues شوید نام کاربر Ali را مشاهده می‌کنید که با استفاده از Script ایجاد شده است.



شکل ۷- ۸۹ Script در میکروتیک

حالا در این قسمت می‌خواهیم کمی دستورات را سخت‌تر کنیم، برای اینکه بتوانیم چندین کاربر را به صورت اتوماتیک ایجاد کنیم باید از حلقه استفاده کنیم.

حلقه زیر را در نظر بگیرید، در این حلقه یک متغییر با حرف e تعریف شده است که از عدد 11 تا 254 متغییر است و در داخل آن با دستور queue simple add این حلقه با حرف e صدا زده شده و کاربرانی با نام User11,User12,User13… ایجاد می‌کند و مقدار آدرس آنها هم به صورت متغییر 10.10.10.11,10.10.10.12,10.10.10.13 ایجاد می‌شود و مقدار سرعت دانلود و آپلود همه کاربران به ۱۲۸ کیلوبایت تغییر می‌کند.

```
:for e from=11 to=254 do={
 /queue simple add name="User $e"  target="10.10.10.$e" max-limit=128000/128000
{
```

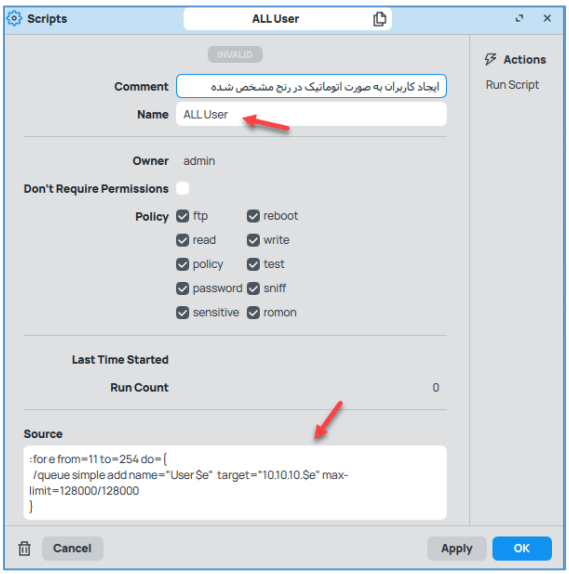
نکات مهم:

محدودیت پهنای باند: در اینجا برای هر کاربر سرعت دانلود ۱۲۸kbps و سرعت آپلود ۱۲۸kbps تنظیم شده است. شما می‌توانید مقادیر max-limit را برای نیازهای خاص خود تغییر دهید.

دسترسی به IPها: این اسکریپت فرض می‌کند که رنج IPهای 10.10.10.11 تا 10.10.10.254 متعلق به کاربران شما است و به هر کدام یک صف مستقل با پهنای باند مشخص اختصاص داده می‌شود.

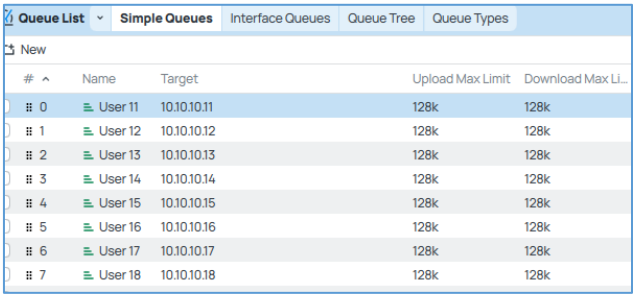
www.takbook.com

حالا طبق شکل ۷-۹۰، وارد Scripts شوید و کد مورد نظر را در آن وارد کنید و آن را اجرا کنید.



شکل ۷- ۹۰ Script در میکروتیک

با اجرای اسکریپت شکل ۷-۹۰، از آدرس 10.10.10.11 تا ادرس 10.10.10.254 در قسمت Queue برای تمام کاربران یک رول جدید ایجاد شده است که در شکل ۷-۹۱، مشخص است حالا اگر هر کاربری با هر آدرس وارد شبکه شود محدودیت کلی برای آن در نظر گرفته شده است.



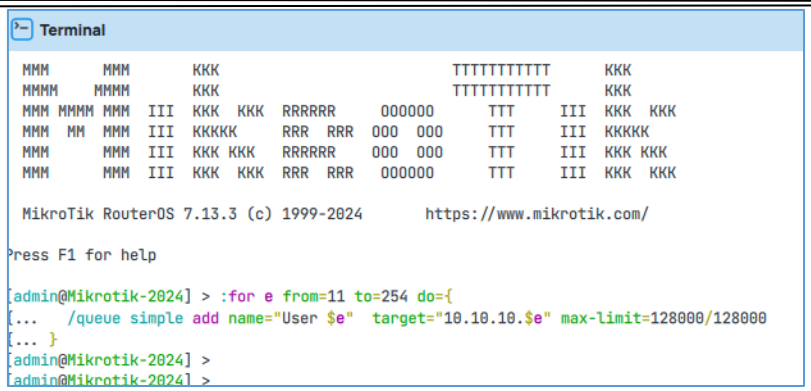
شکل ۷- ۹۱ Script در میکروتیک

نکته مهم:

در بعضی مواقع کدی که وارد می‌کنید اجرا نمی‌شود و برای عیب‌یابی کد مورد نظر باید کل آن را کپی بگیرید و در خط فرمان اجرا کنید.

در شکل ۷-۹۲، دستور قبلی که در اسکریپت اجرا کردیم را به صورت کامل در خط قفرمان Past کردیم که با موفقیت اجرا شده است.

www.takbook.com



شکل ۷- ۹۲ *Script* در میکروتیک

۷-۱۷ مدیریت دانلود و آپلود کاربران

بعد از اینکه در Queue کاربران خود را به صورت کامل ایجاد کردید، حالا نوبت آن است که مدیریتی بر روی مصرف اینترنت آنها داشته باشیم، مثلاً می‌توانیم برای هر کاربر یک سقف مشخص تنظیم کنیم و کدی بنویسیم که اگر کاربر از مرز مورد نظر عبور کرد، سرعت اینترنت آن به شدت کاهش و یا قطع شود؛ برای انجام این کار با ما همراه شوید.

برای شروع باید وارد Script شویم و یک کد را ایجاد کنیم، برای این کار از سمت چپ، وارد System می‌شویم و گزینه‌ی Script را انتخاب می‌کنیم.

دستورات زیر را در آن وارد می‌کنیم:

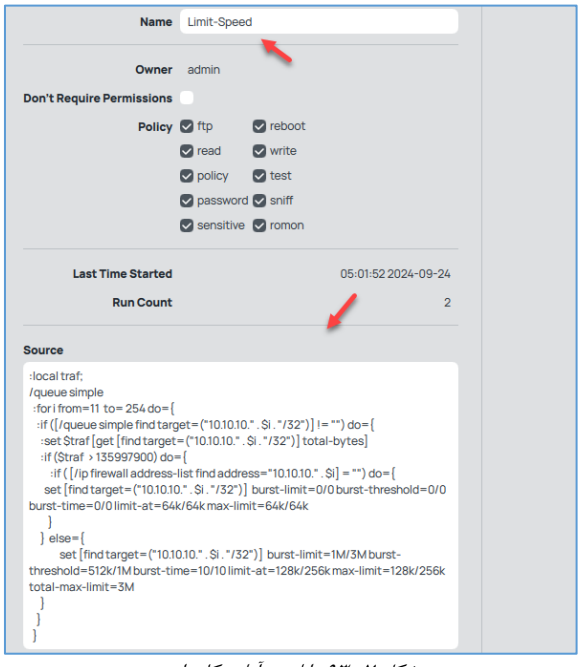
```
:local traf;
/queue simple
: for i from=11 to= 254 do}=
: if ([/queue simple find target=("10.10.10." . $i . "/32")] != "") do}=
: set $traf [get [find target=("10.10.10." . $i . "/32")] total-bytes]
: if ($traf > 135997900) do}=
: if ( [/ip firewall address-list find address="10.10.10." . $i] = "") do}=
set [find target=("10.10.10." . $i . "/32")] burst-limit=0/0 burst-threshold=0/0 burst-time=0/0 limit-at=64k/64k max-limit=64k/64k
{
{ else}=
set [find target=("10.10.10." . $i . "/32")] burst-limit=1M/3M burst-threshold=512k/1M burst-time=10/10 limit-at=128k/256k max-limit=128k/256k total-max-limit=3M
{
```

www.takbook.com


```
{
}
```

در کد بالا، اول از همه، یک حلقه‌ی For ایجاد می‌کنیم که یک محدوده را مثلاً از ۱۱ تا ۲۵٤ تحت پوشش قرار دهد، بعد از این کار یک دستور IF می‌نویسیم و می‌گوییم که از طریق جستجو، کاربرانی که آدرس IP آنها با 10.10.10 شروع می‌شود را پیدا کن و بعد با نوشتن do که با خط به یک عدد متصل است، می‌گوییم که اگر کاربر مورد نظر مقدار دانلود و آپلود آن از مقدار مشخص شده که برابر ۱۳۰ مگابایت است، عبور کند، دستوراتی که IF سوم هستند اجرا می‌شوند، یعنی اینکه سرعت دانلود و آپلود آنها به ٦٤ کیلوبایت تغییر کند، اما اگر اینچنین نبود و کاربر مورد نظر از حد مجاز عبور نکرد، ادامه‌ی کار از خط Else پیگیری می‌شود و همان تنظیمات اولیه برای کاربر مورد نظر ثبت می‌شود. زمانی که حلقه‌ی For اجرا می‌شود، تک تک کاربران به صورت پشت سر هم بررسی می‌شوند که در صورت عبور کردن از مقدار مصرف روزانه، اسکریپت روی آن اجرا می‌شود.

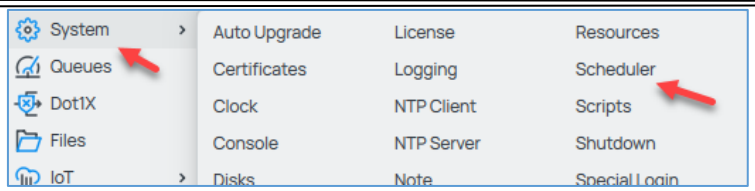
وارد Scripts شوید و دستورات را به صورت شکل ۷-۹۳، وارد کنید و اسکریپت مورد نظر را Save کنید.



شکل ۷- ۹۳ دانلود و آپلود کاربران

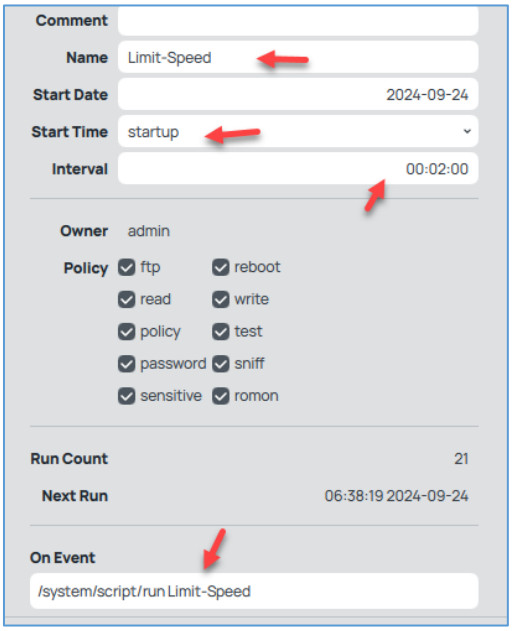
در ادامه باید به روتر بگوییم که برای چک کردن وضعیت مصرفی کاربران این اسکریپت را هر چند دقیقه یک بار اجرا کند، برای اجرای خودکار باید به مانند شکل ۷-۹٤، از سرویس Scheduler استفاده کنیم تا در تاریخ و زمان مشخص این اسکریپت اجرا شود.

www.takbook.com



شکل ۷- ۹۴ دانلود و آپلود کاربران

در شکل ۷-۹۵، بر روی New کلیک کنید و در پنجره باز شده باید نام مورد نظر خود را وارد کنید و در قسمت Interval باید مقدار زمان را بر روی دو دقیقه تنظیم کنید البته شما می‌توانید هر زمان دیگیری را وارد کنید، در قسمت Start Time هم گزینه‌ی Startup را انتخاب کنید تا بعد از ایجاد شروع به کار کند. در قسمت On Event باید کد اجرای Script را وارد کنید که این کد را می‌توانید به راحتی در ترمینال اجرا کنید و اگر اوکی بود در این قسمت کپی کنید.



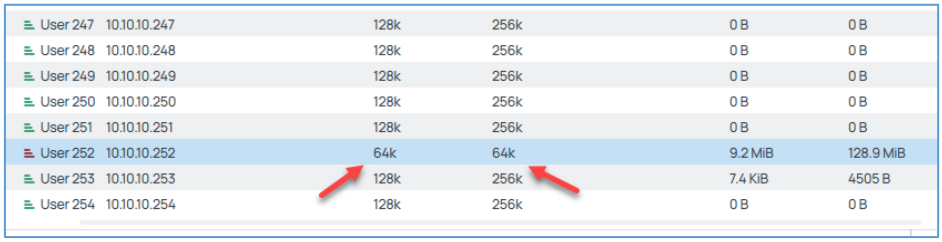
شکل ۷- ۹۵ دانلود و آپلود کاربران

بعد از انجام مراحل بالا، اسکریپت کنترل پهنای باند از طریق سرویس Schedule، هر دو دقیقه یک بار کل کاربران را بررسی می‌کند و اگر کاربری از حد مجاز خود عبور کند، سرعت آن را به ٦٤ کیلوبایت تغییر می‌دهد.

برای تست این موضوع با کلاینتی که آدرس 10.10.10.252 دارد یک دانلود بالای ۱۳۰ مگابایت انجام می‌دهیم که باید سرعت آن به ٦٤ کیلوبایت تغییر کند.

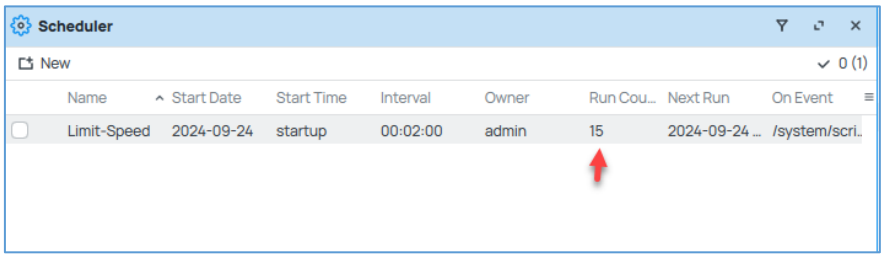
www.takbook.com

همان‌طور که در شکل ۷-۹۶، مشاهده می‌کنید بعد از دانلود حدوداً ۱۳۰ مگابایت مقدار سرعت کاربر مورد نظر به ٦٤ کیلوبایت تغییر کرده است و این نشان دهنده‌ی این است که اسکریپت ما به درستی اجرا شده است.



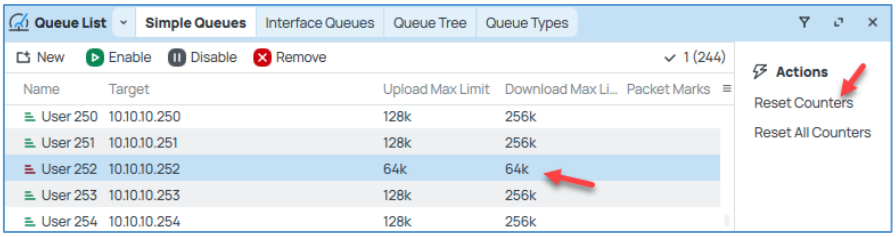
شکل ۷- ۹۶ دانلود و آپلود کاربران

حالا اگر طبق شکل ۷-۹۷، وارد قسمت Scheduler شوید مشاهده خواهید کرد که 15 بار اسکریپت مورد نظر اجرا شده است.



شکل ۷- ۹۷ دانلود و آپلود کاربران

نکته: اگر کاربری حجم خود را به اتمام رسانده باشد و شما بخواهید کاربر مورد نظر را Reset کنید، باید به این صورت عمل کنید طبق شکل ۷-۹۸، که کاربر مورد نظر خود را در لیست پیدا کنید و بعد، از قسمت بالای صفحه بر روی Reset Counters کلیک کنید، با این کار شماره‌های دانلود و آپلود کاربر مورد نظر صفر می‌شود و بعد از دو دقیقه که کل کاربران از نظر حجم مصرفی بررسی می‌شوند، سرعت این کاربر هم به صورت قبلی کاربران پیش‌فرض تغییر خواهد کرد.



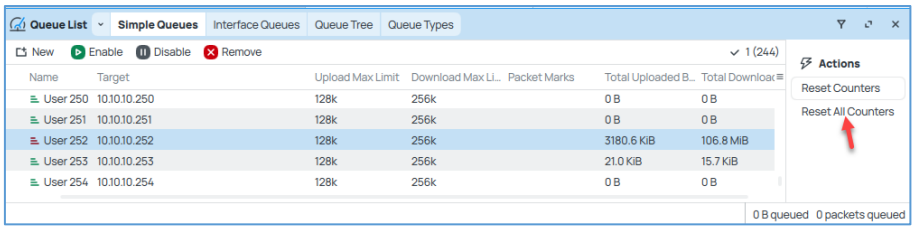
شکل ۷- ۹۸ دانلود و آپلود کاربران

www.takbook.com

حالا طی ٢٤ ساعت، کاربران از اینترنت استفاده کردند و سرعت آنها به ٦٤ تغییر کرد، اگر شما فردای آن روز در محل حضور نداشته باشید، باز هم کاربرانی که دیروز سرعت آنها به ٦٤ کیلوبایت تغییر کرد، از همان سرعت دیروز استفاده می‌کنند، چون مدیر شبکه حضور نداشته که Account آنها را Reset کند؛ برای حل این مشکل باید از همان سرویس Schedule کمک بگیرید و به این سرویس دستور دهید که در ساعت مثلاً ۱ بامداد و بعد از زمان ٢٤ ساعت، کل Account های موجود را ریست کن تا کاربرانی که سرعت آنها افت کرد، در روز بعد با سرعت خوبی کار خود را شروع کنند؛ برای انجام این کار به ادامه کار توجه کنید.

۷–۱۸ ریست کردن Counter کاربران در مدت زمان مشخص

با توجه به توضیحات قبلی برای اینکه مقدار مصرف همه‌ی کاربران را Reset کنیم، باید به مانند شکل ۷–۹۹، از سمت چپ بر روی Queues کلیک کنیم و از بالا بر روی Reset All Counters کلیک کنیم، بعد از این کار همه‌ی شمارنده‌های کاربران Reset می‌شود.

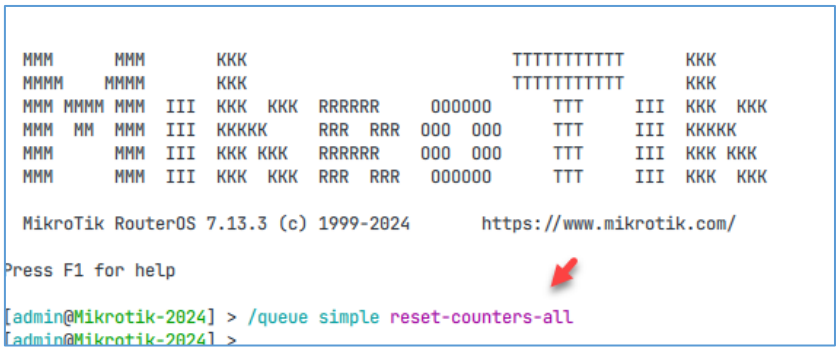


شکل ۷- ۹۹ ریست کردن Counter

اما برای استفاده در سرویس اسکریپت باید این کار را به صورت دستور در بیاوریم، برای انجام این کار به مانند شکل ۷–۱۰۰، New Terminal را در Winbox اجرا می‌کنیم.

بعد از اجرای New Terminal باید دستور زیر را وارد کنیم:

```
/queue simple reset-counters-all
```



شکل ۷- ۱۰۰ ریست کردن Counter

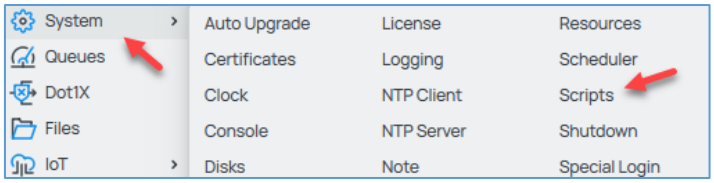
www.takbook.com

اگر خط به خط این دستور را بررسی کنیم، اول وارد قسمت Queue شدیم، بعد از آن وارد تب Simple شدیم و بعد، reset-counters-all را انتخاب کردیم تا همه‌ی شمارنده‌های کاربران Reset شود؛ اگر توجه کنید، نوشتن دستورات دقیقاً مانند این است که شما با استفاده از مأوس دستور را با کلیک بر روی reset all counter اجرا کنید.

بعد از اینکه دستور مورد نظر را بدست آوردیم، باید آن را به صورت یک فایل اسکریپت درآوریم و از طریق سرویس Schedule این فایل را در زمان مشخص اجرا کنیم.

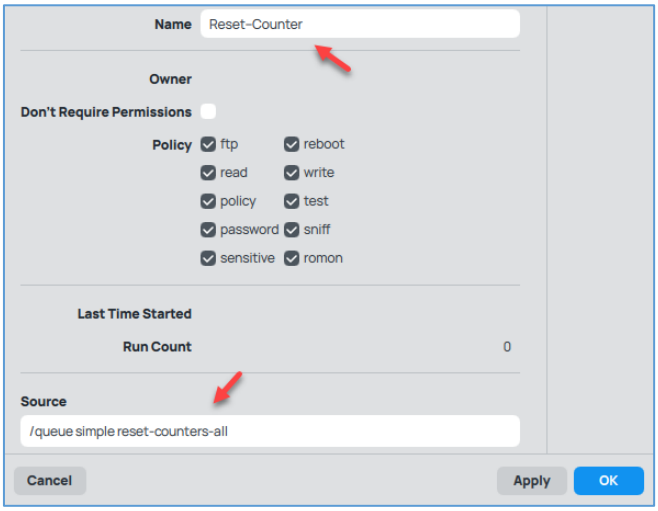
البته خود سرویس Schedule به تنهایی می‌تواند این کار را بدون فایل اسکریپت هم انجام دهد.

به مانند شکل ۷-۱۰۱، سرویس Script را به مانند قبل از طریق منوی System >> Script اجرا کنید.



شکل ۷- ۱۰۱ ریست کردن Counter

به مانند شکل ۷-۱۰۲، در تب Script بر روی آیکون New کلیک کنید تا صفحه‌ی New Script اجرا شود، بعد از آن نام مورد نظر خود را وارد کنید و در قسمت Source، همان دستور را که با هم برای ریسیت کردن کلی کانترها بدست آوردیم را وارد کنید و بر روی OK کلیک کنید.



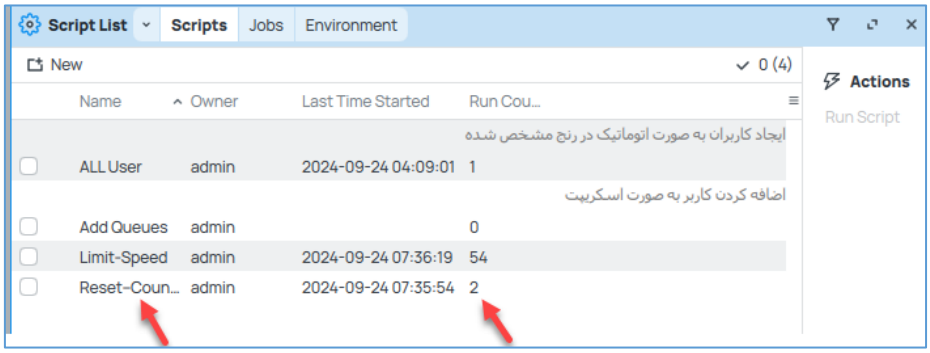
شکل ۷- ۱۰۲ ریست کردن Counter

www.takbook.com

برای اینکه در سرویس Schedule یک Rule ایجاد کنیم تا این اسکریپت را اجرا کند، نیاز به دستور داریم که همان‌طور که گفتیم، باید از طریق New Terminal به آن دست پیدا کنیم؛ به مانند شکل ۷–۱۰۳، دستور زیر را اجرا می‌کنیم:

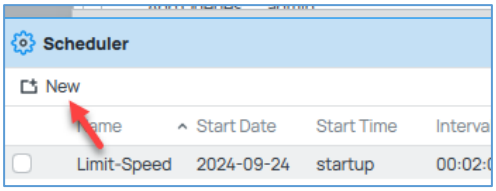
```
/system script run Reset--Counter
```

بعد از وارد کردن دستور بر روی Enter فشار دهید، همان‌طور که در شکل ۷–۱۰۳، مشاهده می‌کنید در قسمت Script List مقدار Run Count به ۲ تغییر کرده است که این عدد در هر بار اجرای اسکریپت مورد نظر تغییر می‌کند.



شکل ۷–۱۰۳ ریست کردن *Counter*

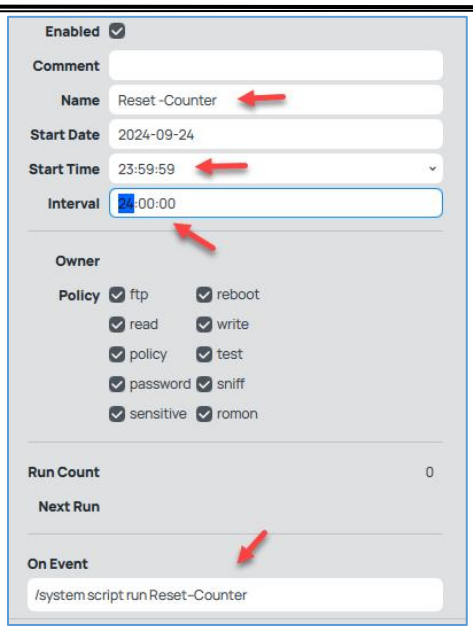
بعد از بدست آوردن دستور مورد نظر، طبق شکل ۷–۱۰۴، وارد آدرس System >> Schedule شوید و بر روی آیکون New کلیک کنید.



شکل ۷–۱۰۴ ریست کردن *Counter*

به مانند شکل ۷–۱۰۵، در صفحه‌ی باز شده در قسمت Name، نام مورد نظر خود را وارد کنید و در قسمت Start Time باید زمان اجرای آن را مشخص کنید، مثلاً ۱۲ شب و در قسمت Interval، مقدار ۱ روز یا همان ۲۴ ساعت را برای آن مشخص کنید و در قسمت On Event هم دستور مورد نظر را کپی کنید و بر روی OK کلیک کنید تا Schedule مورد نظر ایجاد شود و در زمان مشخص شده اجرا شود (به جای این دستور، می‌توانید از نام اسکریپت استفاده کنید).

www.takbook.com



شکل ۷- ۱۰۵ ریست کردن *Counter*

شما می‌توانید به جای اجرای اسکریپت مورد نظر خود دستور را به صورت مستقیم در سرویس Schedule وارد کنید و آن را تنظیم کنید تا در زمان مشخص اجرا شود.

نکته‌ی مهم: حتماً باید ساعت روتر را از قبل تنظیم کنید تا سر ساعت مشخص، تنظیماتی که انجام می‌دهید، اجرا شود.

۷-۱۹ قطع کردن اینترنت شبکه

شما می‌توانید با استفاده از اسکریپت و زمانبندی اینترنت کاربران را در زمان مشخصی غیرفعال و درزمان دیگر فعال کنید، برای این کار راه‌های مختلفی وجود دارد ولی بهترین را از نظر من این است که رولی که در قسمت NAT نوشتیم و برای ترجمه آدرس‌های داخلی به بیرونی به کار می‌رود را غیر فعال کنیم، برای این کار باید به صورت زیر عمل کنید.

به مانند شکل ۷-۱۰۶، وارد ترمینال شوید و در قسمت Firewall /Nat دستور Print را وارد کنید تا رول‌هایی که در قسمت Nat وجود دارد را مشاهده کنید، همان‌طور که مشاهده می‌کنید یک رول NAT وجود دارد که عملیات ترجمه یا همان Masquerade را بازی می‌کند.

www.takbook.com


```
[admin@Mikrotik-2024] >
[admin@Mikrotik-2024] >
[admin@Mikrotik-2024] > ip/firewall/nat/print
Flags: X - disabled, I - invalid; D - dynamic
 0    ;;; LAN-NAT-to-Internet
      chain=srcnat action=masquerade src-address=10.10.10.0/24 log=no log-prefix=""
```

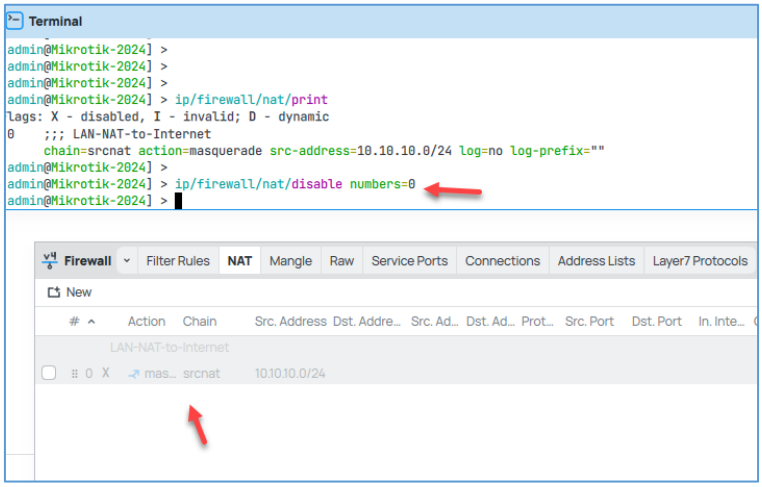
شکل ۷- ۱۰۶ قطع کردن اینترنت شبکه

شماره‌ی این NAT برابر صفر است و باید در ادامه از آن استفاده کنیم.

با استفاده از دستور زیر می‌توانید NAT مورد نظر را غیر فعال کنید.

Ip/firewall/nat/disable numbers=0

همان‌طور که در شکل ۷-۱۰۷، مشاهده می‌کنید با اجرای دستور بالا NAT مورد نظر غیر فعال شد.



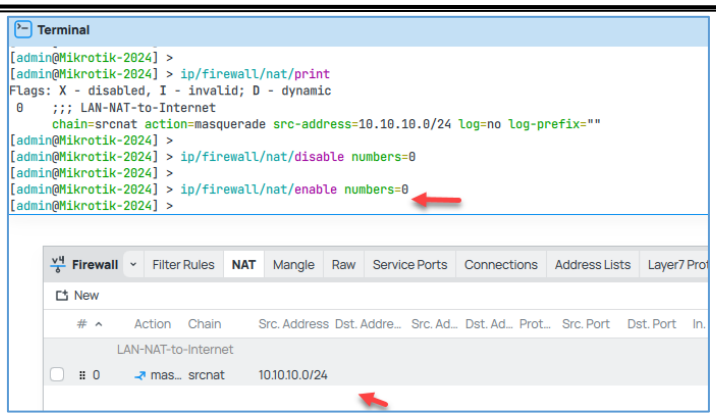
شکل ۷- ۱۰۷ قطع کردن اینترنت شبکه

با استفاده دستور زیر هم NAT مورد نظر فعال خواهد شد:

ip/firewall/nat/enable numbers=0

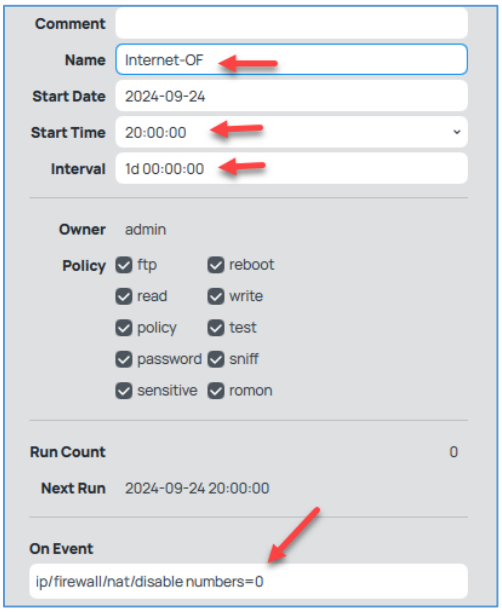
در شکل ۷-۱۰۸، این موضوع مشخص شده است:

www.takbook.com



شکل ۷- ۱۰۸ قطع کردن اینترنت شبکه

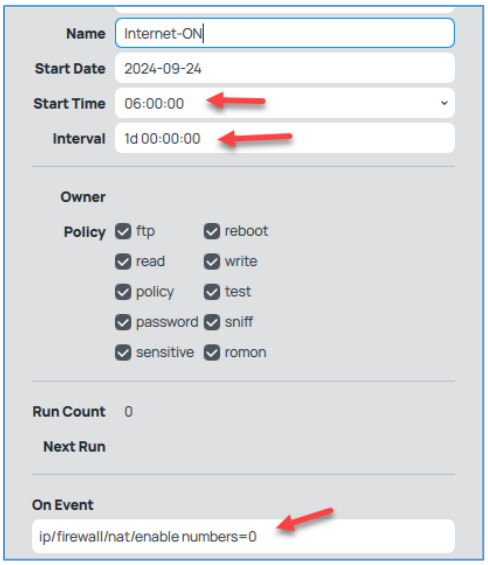
حالا همین دستورات را می‌توانیم مستقیم در Scheduler استفاده کنیم و زمان را برای آن مشخص کنیم، وارد Scheduler شوید و به مانند شکل ۷-۱۰۹، یک رول جدید ایجاد کنید و زمان اجرای آن را باید آخر ساعت کاری مثلاً ساعت 20 قرار دهید و مقدار زمان اجرای بعدی را بر روی یک روز یا همان 24 ساعت قرار دهید، در قسمت On Event هم باید دستور غیرفعال‌سازی NAT را که مشخص کردیم وارد کنید.



شکل ۷- ۱۰۹ قطع کردن اینترنت شبکه

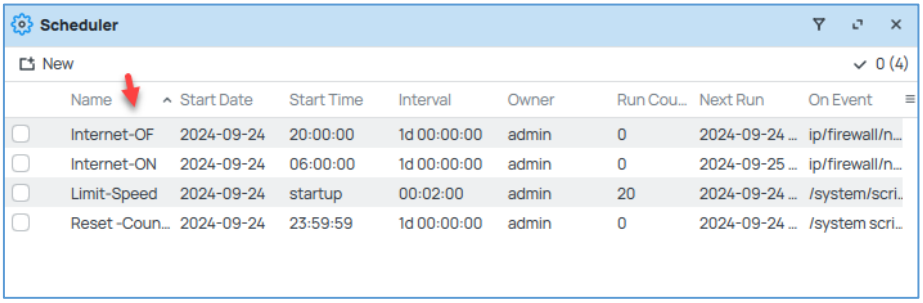
www.takbook.com

برای اینکه فردای آن روز دوباره NAT مورد نظر فعال شود باید یک رول جدید ایجاد کنید و به صورت شکل ۷-۱۱۰، دستور را وارد کنید، توجه داشته باشید زمان اجرا را باید صبح آن روز قرار دهید، مثلاً ساعت ٦ صبح و زمان اجرای بعدی را باید بر روی یک روز قرا دهید.



شکل ۷- ۱۱۰ قطع کردن اینترنت شبکه

به مانند شکل ۷-۱۱۱، همان‌طور که در لیست زمان‌بندی مشاهده می‌کنید دو رول جدید اضافه شده است و در زمان مشخص اینترنت کاربران قطع خواهد شد.



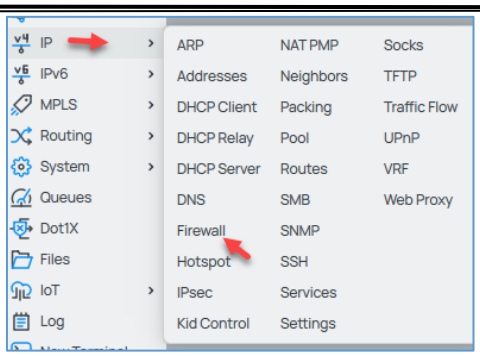
شکل ۷- ۱۱ قطع کردن اینترنت شبکه

۷-۲۰ بستن سایت‌ها در میکروتیک

در میکروتیک شما این امکان را دارید که سایت‌هایی که نیاز است ببندید را مشخص کنید، برای این کار باید از قابلیت فایروال استفاده کنیم.

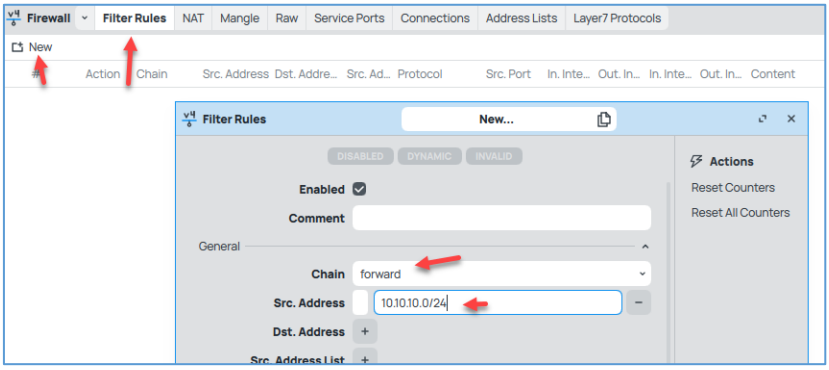
به مانند شکل ۷-۱۱۲، وارد میکروتیک شوید و از قسمت IP گزینه‌ی Firewall را انتخاب کنید.

www.takbook.com



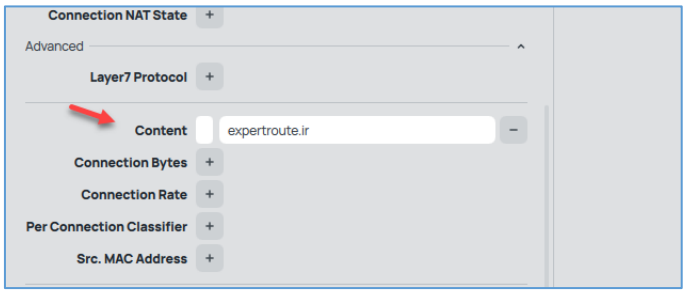
شکل ۷- ۱۱۲ بستن سایت‌ها در میکروتیک

در ادامه طبق شکل ۷-۱۱۳، وارد تب Filter شوید و بر روی New کلیک کنید و در پنجره باز شده باید در قسمت Chain گزینه‌ی Forward را انتخاب کنید، منظور از Forward این است که به پکت‌هایی اشاره می‌کند که مبدا و مقصد آن میکروتیک نیست ولی از آن عبور می‌کنند، در قسمت Src.Address باید کل آدرس‌های شبکه را وارد کنید که به صورت 10.10.10.0/24 می‌شود.



شکل ۷- ۱۱۳ بستن سایت‌ها در میکروتیک

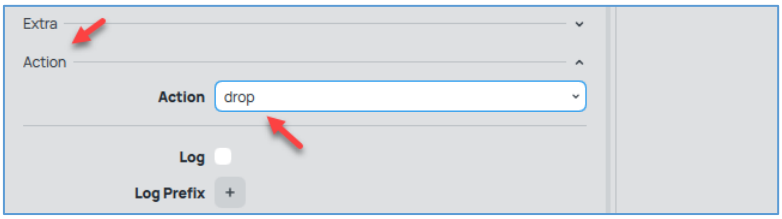
در شکل ۷-۱۱۴، وارد قسمت Advanced شوید و در قسمت Content باید آدرس سایتی که قرار است فیلتر شود را وارد کنید.



شکل ۷- ۱۱۴ بستن سایت‌ها در میکروتیک

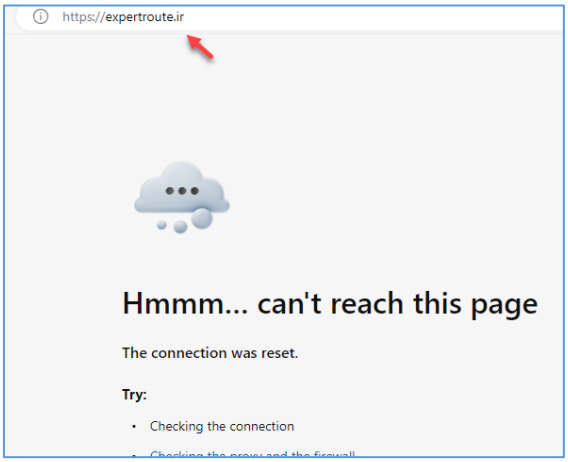
www.takbook.com

در ادامه کار طبق شکل ۷-۱۱۵، وارد قسمت Action شوید و برای بستن سایت مورد نظر باید گزینه‌ی Drop را انتخاب کنید، اگر می‌خواهید ببینید که چه اطلاعاتی با این رول بررسی می‌شود باید گزینه‌ی Log را انتخاب کنید.



شکل ۷- ۱۱۵ بستن سایت‌ها در میکروتیک

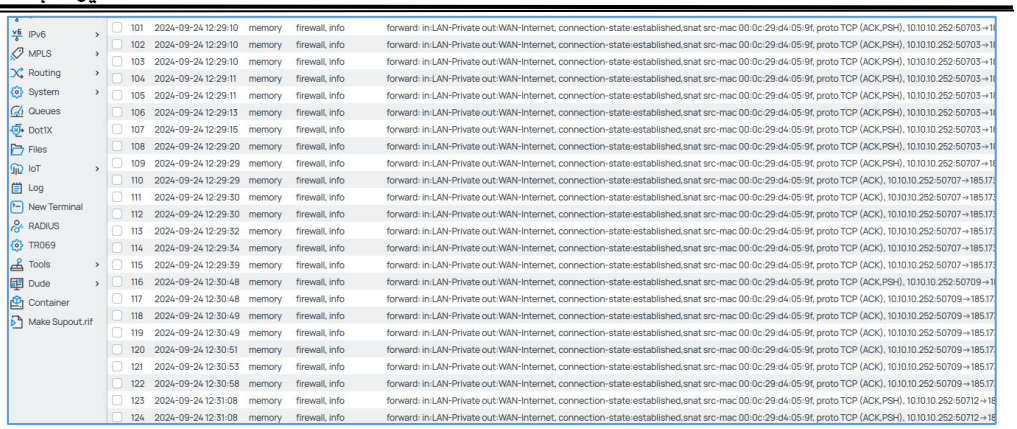
حالا برای تست این موضوع به مانند شکل ۷-۱۱۶، وارد یکی از کلاینت‌ها می‌شویم و سایت Expertroute.ir را باز می‌کنیم که مشاهده می‌کنید سایت مورد نظر باز نمی‌شود



شکل ۷- ۱۱۶ بستن سایت‌ها در میکروتیک

اگر به مانند شکل ۷-۱۱۷، وارد Log در میکروتیک شوید، تمام Packet هایی که از رول مورد نظر عبور می‌کند را برای شما نمایش می‌دهد و مشخص است کار به درستی انجام شده است و تمام پکت هایی که حاوی سایت Expertroute.ir است Drop شده است.

www.takbook.com

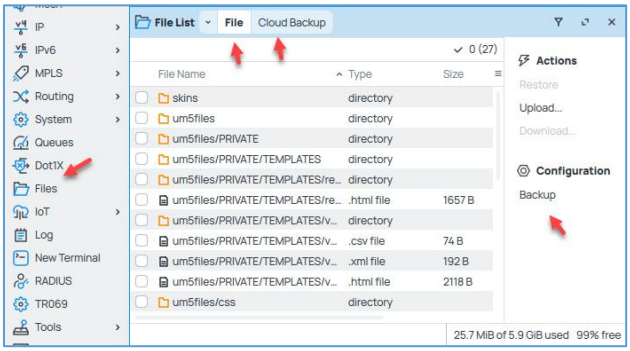


شکل ۷- ۱۱۷ بستن سایت‌ها در میکروتیک

۷-۲۱ انجام Backup و Restore در میکروتیک

برای اینکه از اطلاعات خود پشتیبان تهیه کنیم باید به صورت زیر وارد Files شوید و به مانند شکل ۷-۱۱۸، برای اینکه یک پشتیبان از تنظیمات خود تهیه کنیم دو روش وجود دارد، یکی اینکه به صورت محلی این کار را انجام دهیم و دیگری اینکه به صورت Cloud بر روی سرورهای میکروتیک انجام دهیم.

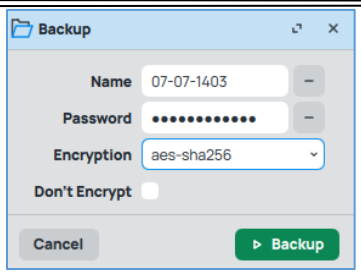
برای انجام پشتبان محلی که در خود روتر شما ذخیره می‌شود باید در شکل ۷-۱۱۸، بر روی Backup کلیک کنید.



شکل ۷- ۱۱۸ انجام Backup و Restore

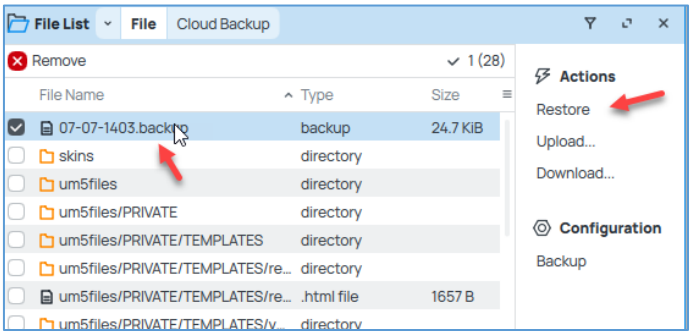
در شکل ۷-۱۱۹، باید در قسمت NAME نام مورد نظر خود را وارد کنید و در قسمت Password هم باید رمز عبوری برای فایل خود قرار دهید که در قسمت Encryption هم باید نوع رمزگذاری را مشخص کنید، توجه داشته باشید اگر بخواهید Backup شما بدون رمز ذخیره شود باید تیک گزینه‌ی don't Encrypt را انتخاب کنید.

www.takbook.com



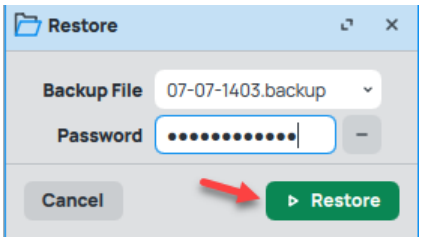
شکل ۷- ۱۱۹ انجام Backup و Restore

همان‌طور که در شکل ۷-۱۲۰، مشاهده می‌کنید Backup مورد نظر ایجاد شده است و اگر بخواهید آن را برگردانید باید آن را انتخاب کنید و گزینه‌ی Restore را کلیک کنید.



شکل ۷- ۱۲۰ انجام Backup و Restore

به مانند شکل ۷-۱۲۱، باید رمز عبور مورد نظر را وارد کنید و بر روی Restore کلیک کنید، توجه داشته باشید که بعد از Restore کردن روتر ریست خواهد شد و به همان تنظیماتی که قبلاً Backup گرفتید بر می‌گردد.



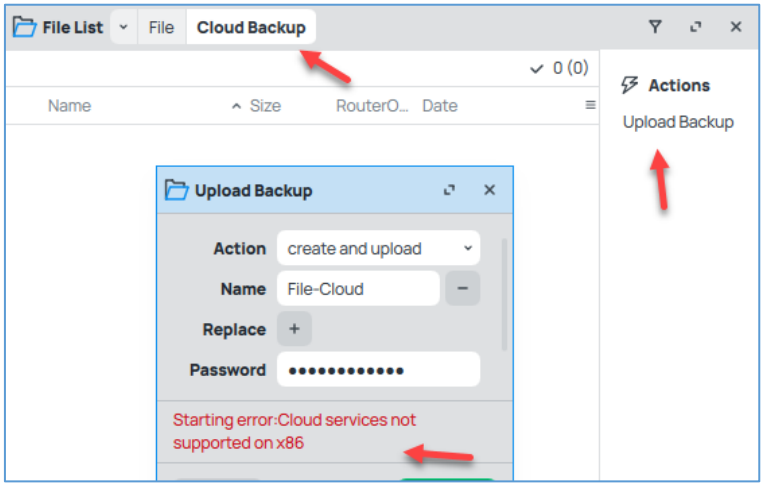
شکل ۷- ۱۲۱ انجام Backup و Restore

توجه داشته باشید که می‌توانید با کلیک بر روی گزینه‌ی Download فایل مورد نظر را در سیستم خودتان ذخیره کنید.

www.takbook.com

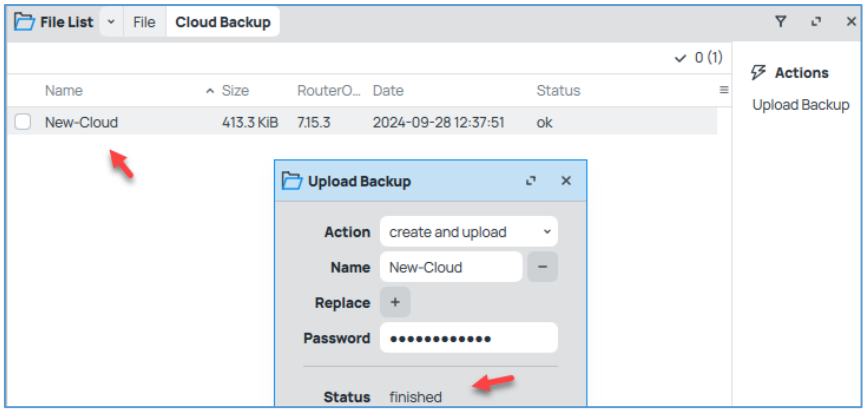
راهی دیگر برای Backup گرفتن وجود دارد و آن هم این است که آن را به صورت Cloud یا همان ابری در سرورهای میکروتیک ذخیره کنید، برای این کار به مانند شکل ۷-۱۲۲، باید وارد تب Cloud Backup شوید و بر روی Upload Backup کلیک کنید.

در قسمت Name نام دلخواه خود را وارد کنید و در قسمت Password هم یک رمز عبور برای خود وارد کنید، بعد از کلیک بر روی Start اگر چنانچه روتر میکروتیک شما از نوع مجازی و بر روی یک سیستم اجرا شده باشد این کار با خطا روبرو خواهد شد که در شکل ۷-۱۲۲، شان داده شده است.



شکل ۷-۱۲۲ انجام Backup و Restore

برای اینکه متوجه شویم که این کار عملی است یا نه طبق شکل ۷-۱۲۳، وارد میکروتیک سخت‌افزاری می‌شویم که مدل CRS-125 است و همان‌طور که مشاهده می‌کنید این کار با موفقیت انجام شده است.



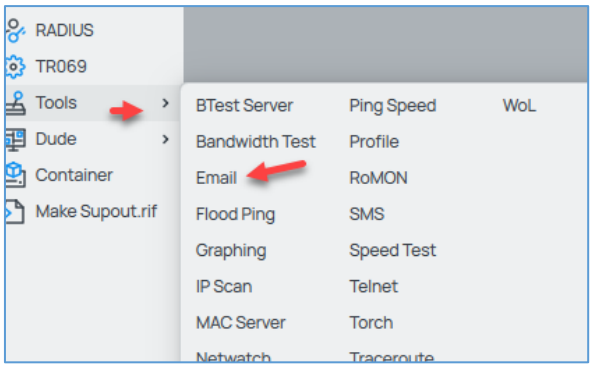
شکل ۷-۱۲۳ انجام Backup و Restore

www.takbook.com

۷-۲۲ ایجاد Backup به صورت اتوماتیک و ارسال آن به ایمیل

در قسمت قبل به صورت دستی از تنظیمات روتر Backup ایجاد کردیم که این کار در دراز مدت، کار وقت‌گیری خواهد بود، برای همین می‌توانیم با ایجاد تنظیماتی این کار را به صورت اتوماتیک انجام دهیم. اولین کاری که باید انجام دهیم، تنظیم ایمیل در میکروتیک است که زمانی که Backup تهیه می‌شود، این Backup به آدرس ایمیل ارسال شود.

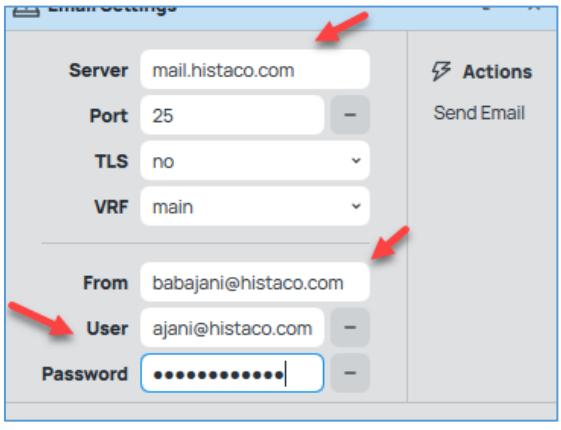
وارد میکروتیک شوید و طبق شکل ۷-۱۲٤، از قسمت IP، گزینه‌ی Email را انتخاب کنید.



شکل ۷- ۱۲۴ ایجاد Backup به صورت اتوماتیک

در ادامه کار به مانند شکل ۷-۱۲۵، باید آدرس سرور ایمیل به همراه آدرس ایمیل خود و رمز عبور آن را وارد کنید، توجه داشته باشید برای اینکه از سرورهای Gmail و Yahoo استفاده کنید باید از سایت خودشان تنظیمات را دریافت کنید مانند لینک زیر که برای Gmail است.

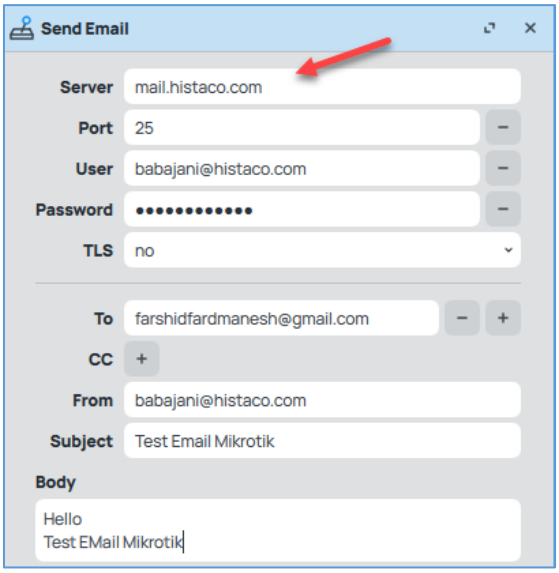
https://support.google.com/mail/answer/7104828?hl=en



شکل ۷- ۱۲۵ ایجاد Backup به صورت اتوماتیک

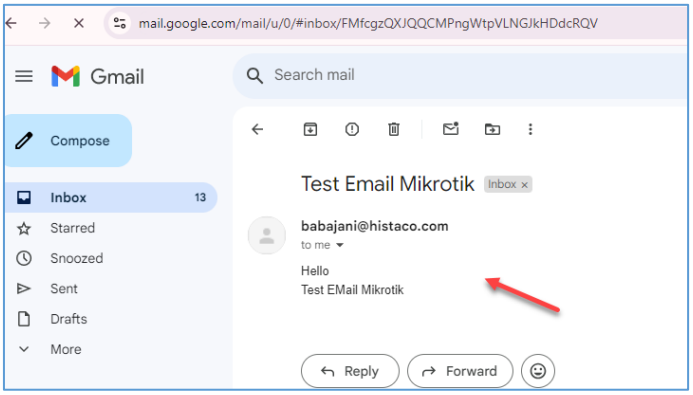
www.takbook.com

با استفاده از گزینه‌ی Send Email می‌توانید تست بگیرید که ایمیل ارسال می‌شود یا خیر، به مانند شکل ۷-۱۲۶، اطلاعات را وارد کنید و بر روی Send Email کلیک کنید.



شکل ۷- ۱۲۶ ایجاد Backup به صورت اتوماتیک

بعد از ارسال اگر وارد سرور ایمیل خود شویم مشاهده می‌کنیم که ایمیل مورد نظر به مقصد رسیده است که در شکل ۷-۱۲۷، همین موضوع مشخص شده است.



شکل ۷- ۱۲۷ ایجاد Backup به صورت اتوماتیک

بعد از اینکه ایمیل را تنظیم کردیم حالا باید کاری کنیم که به صورت اتوماتیک Backup گرفته شود و به ایمیل ارسال شود، برای این کار باید از اسکریپت استفاده کنیم.

وارد Scripts شوید و دستور زیر را در آن وارد کنید.

#####Script-Backup-Mikrotik-Expertroute#####

www.takbook.com


```
/system backup save dont-encrypt=yes name=Mikrotik-Bakup;
:delay delay-time=2
/tool/e-mail/send server=mail.histaco.com tls=no port=25 user=babajani@histaco.com password=pass
to=farshidfardmanesh@gmail.com from=babajani@histaco.com subject=Test-Final;
:delay delay-time=20
/file remove Mikrotik-Bakup.backup
/
```

این اسکریپت در خط اول به علت وجود / از هر قسمت روتر به خط اول برمی‌گردد، بعد از آن وارد System Backup می‌شود و یک فایل Backup با نام Mikrotik-Bakup ایجاد می‌کند و بعد از آن، با دستور dont-encrypt=yes این فایل رمزنگاری نمی‌شود.

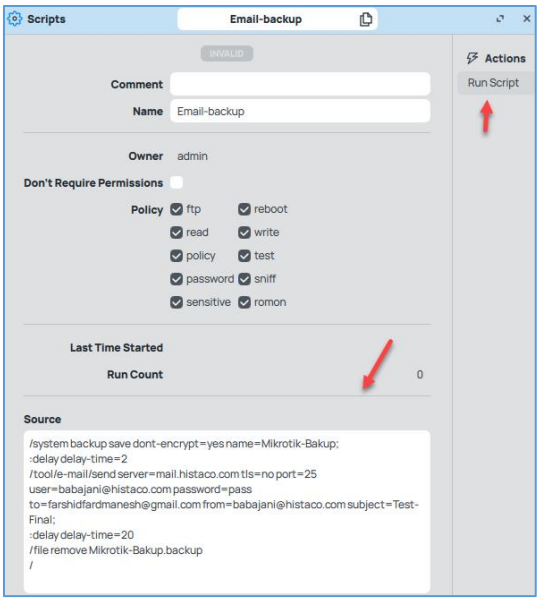
در خط دوم، یک زمان ۲ ثانیه‌ای در نظر گرفته‌ایم تا به خط سوم انتقال داده شود.

در خط سوم که مهمترین خط می‌باشد، برای فرستادن ایمیل Backup باید تنظیمات مشخص شده‌ی خود را اعمال کنید، در جایی که با رنگ قرمز مشخص شده باید اطلاعات خود را وارد کنید، در آخر خط سوم، دستور file=Mikrotik-Bakup.backup نوشته شده که به این نکته اشاره دارد که در زمان ارسال ایمیل به پیوست ایمیل این فایل را هم که در خط اول ایجاد کردیم، بفرست.

در خط چهارم یک زمان ۲۰ ثانیه‌ای در نظر گرفتیم که ایمیل در این زمان به همراه فایل ارسال شود.

در خط پنجم با دستور مورد نظر وارد File شدیم و Backup با نام Mikrotik-Bakup.backup را حذف کردیم.

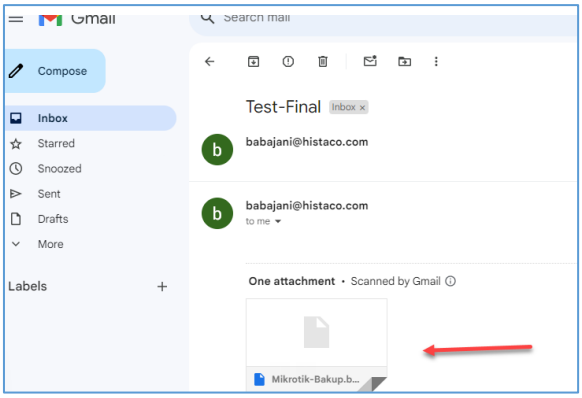
دستورات بالا را در یک فایل اسکریپت کپی می‌کنیم و آن را به صورت شکل ۷-۱۲۸ اجرا می‌کنیم.



شکل ۷- ۱۲۸ ایجاد Backup به صورت اتوماتیک

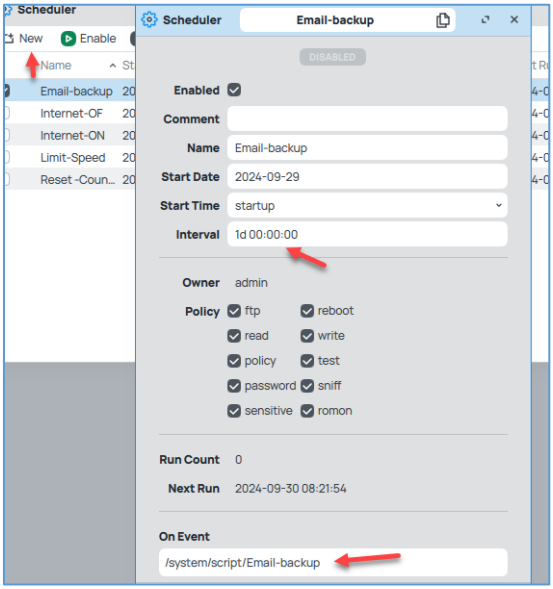
www.takbook.com

همان‌طور که در شکل ۷-۱۲۹، مشاهده می‌کنید ایمیل مورد نظر به Gmail ارسال شده است.که فایل پیوست هم همراه آن است.



شکل ۷- ۱۲۹ ایجاد Backup به صورت اتوماتیک

بعد از اینکه فایل Scripts را ایجاد کردید باید آن را توسط Schenduler در زمان‌های مشخص اجرا کنیم. به مانند شکل ۷-۱۳۰، وارد Schenduler شوید و در قسمت Interval باید مقدار زمان اجرا را مشخص کنید که یک روز در نظر گرفته شده است، در قسمت ON Event باید آدرس فایل اسکریپت را وارد کنید، بعد از ذخیره کردن آن به صورت روزانه از اطلاعات میکروتیک پشتیبان گرفته خواهد شد و به ایمیل ارسال می‌شود و از بابت داشتن پشتیبان خیالمان راحت می‌شود.



شکل ۷- ۱۳۰ ایجاد Backup به صورت اتوماتیک

www.takbook.com

۷-۲۳ راه‌اندازی Hotspot در میکروتیک

در میکروتیک، Hotspot یک ویژگی قدرتمند است که امکان کنترل دسترسی کاربران به اینترنت را فراهم می‌کند. به طور کلی، Hotspot یک صفحه ورود (Login Page) به کاربر ارائه می‌دهد تا با وارد کردن نام کاربری و رمز عبور، به شبکه اینترنت دسترسی پیدا کنند. این قابلیت برای مکان‌هایی مثل کافی‌شاپ‌ها، هتل‌ها، فرودگاه‌ها و سایر مکان‌های عمومی بسیار مفید است.

ویژگی‌های اصلی Hotspot در میکروتیک:

- کنترل دسترسی: کاربران قبل از اتصال به اینترنت باید اعتبارسنجی شوند. این اعتبارسنجی می‌تواند از طریق یوزرهای داخلی میکروتیک یا با استفاده از سرورهای خارجی مثل RADIUS انجام شود.
- صفحه ورود (Login Page): هنگام اتصال به شبکه، کاربران به صورت خودکار به صفحه ورود هدایت می‌شوند. این صفحه قابل شخصی‌سازی است تا با ظاهر و برند تجاری مکان سازگار باشد.
- مدیریت کاربران: شما می‌توانید محدودیت‌هایی مانند پهنای باند، زمان استفاده، تعداد دستگاه‌های مجاز برای اتصال و غیره برای کاربران تعریف کنید.
- پشتیبانی از روش‌های مختلف احراز هویت:

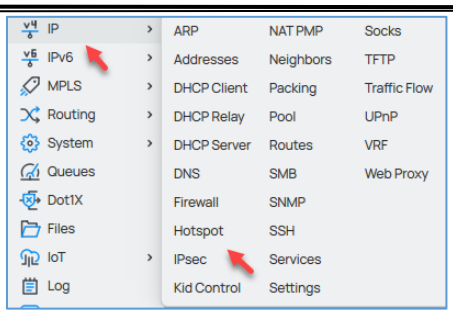
  نام کاربری و رمز عبور

  احراز هویت مبتنی بر MAC Address

  دسترسی بدون رمز عبور (Trial Mode)
- گزارش‌گیری و نظارت: میکروتیک می‌تواند گزارش‌های دقیقی از استفاده کاربران از اینترنت و پهنای باند مصرفی ارائه دهد.
- افزودن تبلیغات یا پیام‌های دلخواه: از طریق صفحه ورود، می‌توان تبلیغات یا پیام‌های سفارشی به کاربران نمایش داد.

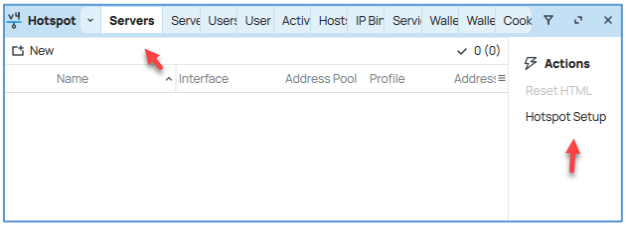
برای شروع کار طبق شکل ۷-۱۳۱، وارد IP شوید و گزینه‌ی Hotspot را انتخاب کنید.

www.takbook.com



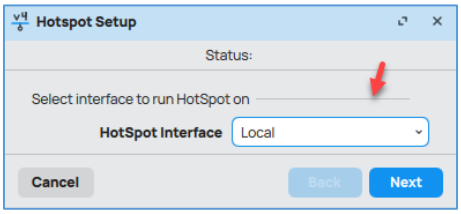
شکل ۷- ۱۳۱ راه‌اندازی Hotspot

در شکل ۷-۱۳۲، برای شروع تنظیمات Hotspot از تب Server بر روی Hotspot Setup کلیک کنید.



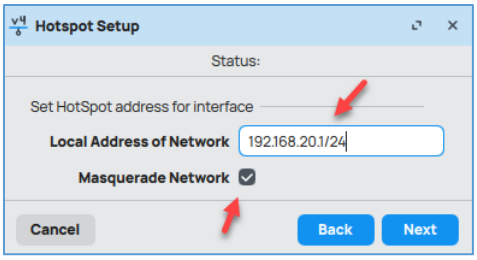
شکل ۷- ۱۳۲ راه‌اندازی Hotspot

در شکل ۷-۱۳۳، باید مشخص کنید که این سرویس بر روی کدام کارت شبکه فعال شود که برای این کار باید کارت شبکه داخلی خود را انتخاب کنید.



شکل ۷- ۱۳۳ راه‌اندازی Hotspot

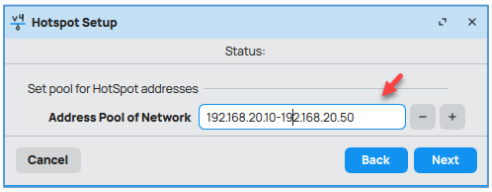
در شکل ۷-۱۳۴، باید آدرس شبکه‌ی خود را وارد و تیک گزینه‌ی مورد نظر را برای انجام عملیات NAT انتخاب کنید.



شکل ۷- ۱۳۴ راه‌اندازی Hotspot

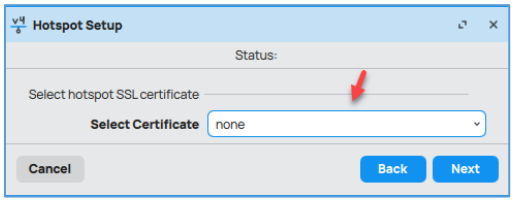
www.takbook.com

در شکل۷-۱۳۵، یک رنج آدرس برای تخصیص دادن به کاربران وارد کنید.



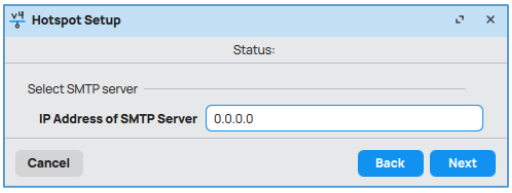
شکل ۷- ۱۳۵ راه‌اندازی Hotspot

شکل ۷-۱۳۶، مربوط به انتخاب گواهینامه برای سرویس Hotspot است که نیاز نیست انتخاب کنید و گزینه‌ی None را انتخاب کنید.



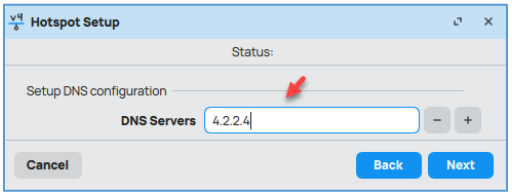
شکل ۷- ۱۳۶ راه‌اندازی Hotspot

در شکل ۷-۱۳۷، اگر در شبکه سرور ایمیل دارید می‌توانید آدرس آن را وارد کنید.



شکل ۷- ۱۳۷ راه‌اندازی Hotspot

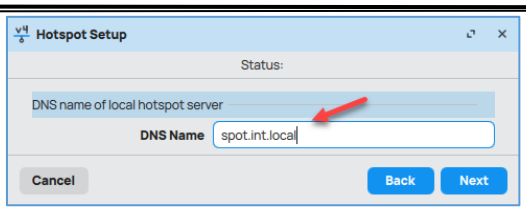
در شکل ۷-۱۳۸، اگر از DNS داخلی استفاده می‌کنید باید اول DNS داخلی و در ادامه باید DNS عمومی را وارد کنید.



شکل ۷- ۱۳۸ راه‌اندازی Hotspot

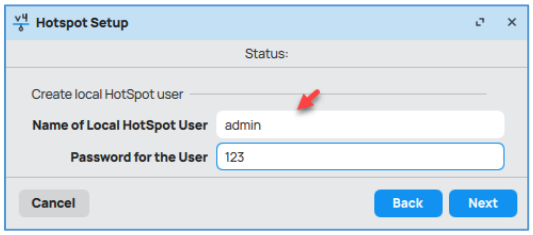
در شکل ۷-۱۳۹، باید یک نام برای Hotspot خود در نظر بگیرید و آن را در DNS سرور خود تعریف کنید، البته برای این لحظه نیازی به نام نداریم و نیازی نیست این قسمت را تکمیل کنید.

www.takbook.com



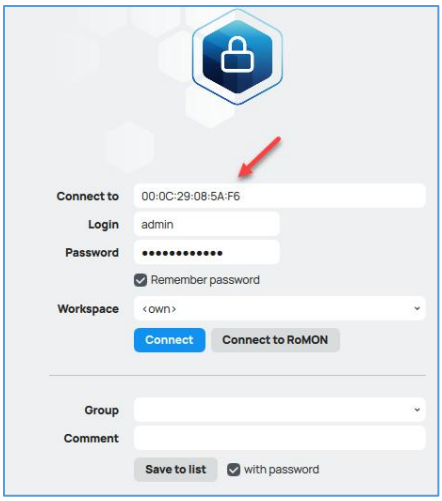
شکل ۷- ۱۳۹ راه‌اندازی Hotspot

به مانند شکل ۷-۱۴۰، می‌توانید یک کاربر برای ورود به سرویس Hotspot تعریف کنید، بعد از کلیک بر روی Next ارتباط شما با روتر قطع خواهد شد.



شکل ۷- ۱۴۰ راه‌اندازی Hotspot

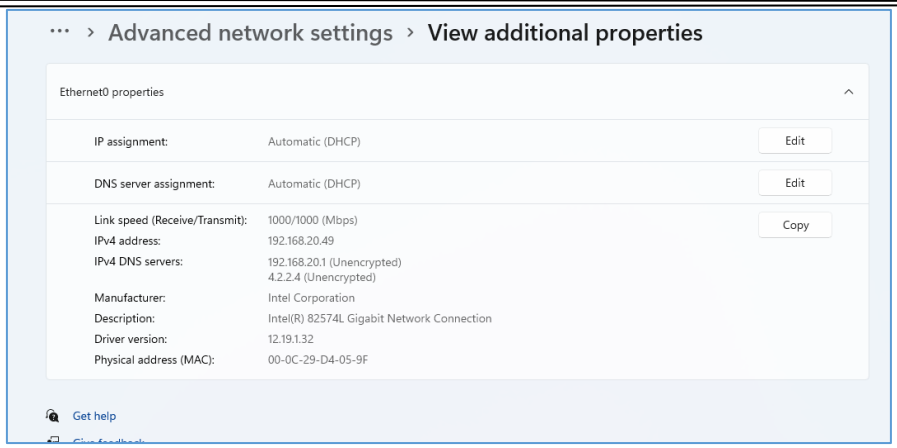
برای اینکه بتوانید از طریق Winbox به روتر متصل شوید باید از Mac address به صورت شکل ۷-۱۴۱ استفاده کنید.



شکل ۷- ۱۴۱ راه‌اندازی Hotspot

برای اینکه سرویس Hotspot را تست بگیریم، به مانند شکل ۷-۱۴۲، وارد یک کلاینت ویندوز می‌شویم و چون شبکه این کلاینت به میکروتیک متصل است روتر میکروتیک از طریق DHCP به آن آدرس تخصیص می‌دهد که در شکل ۷-۱۴۲، این موضوع را مشاهده می‌کنید.

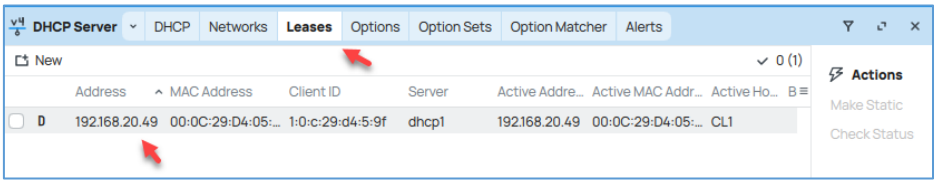
www.takbook.com



شکل ۷- ۱۴۲ راه‌اندازی *Hotspot*

همان‌طور که بیان کردیم وقتی Hotspot را راه‌اندازی می‌کنید به همراه آن سرویس DHCP هم فعال می‌شود و به خاطر همین هست که وقتی Hotspot فعال می‌شود کلاینت‌ها به صورت اتوماتیک آدرس دریافت می‌کنند.

اگر به مانند شکل ۷-۱۴۳، وارد DHCP Server در میکروتیک شوید و به تب Leases مراجعه کنید، یک آدرس جدید را مشاهده می‌کنید که به کلاینت مورد نظر تخصیص داده شده است.

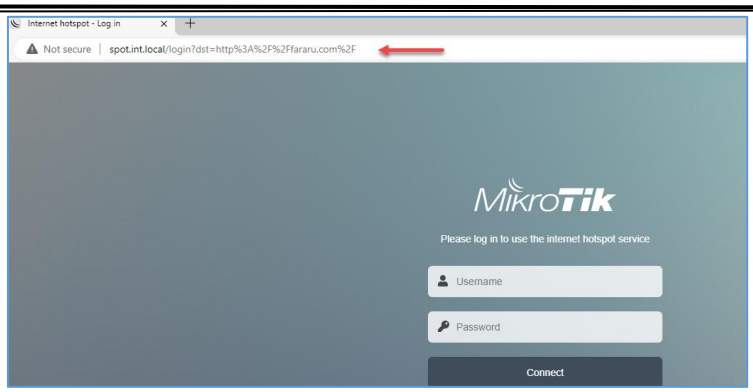


شکل ۷- ۱۴۳ راه‌اندازی *Hotspot*

برای تست کارایی Hotspot طبق شکل ۷-۱۴۴، در کلاینت مرورگر خود را باز کنید و یک سایت را باز کنید، بعد از اجرای سایت مورد نظر به صورت اتوماتیک به صفحه‌ی Hotspot ری دایرکت خواهید شد. اگر به آدرس توجه کنید همان آدرسی است که در هنگام راه‌اندازی Hotspot تنظیم کردیم، شما اگر از آدرس استفاده نکرده باشید آدرس IP روتر میکروتیک را مشاهده خواهید کرد.

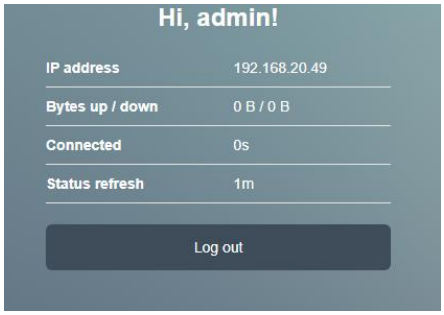
نکته مهم : بعضی از سایت‌ها HTTPS اگر اجرا کنید عملیات ری دایرکت انجام نمی‌شود که می‌توانید به صورت دستی آدرس روتر میکروتیک را وارد کنید تا صفحه Login برای شما باز شود، با کاربری که در هنگام تنظیم وارد کردیم وارد Hotspot می‌شویم.

www.takbook.com



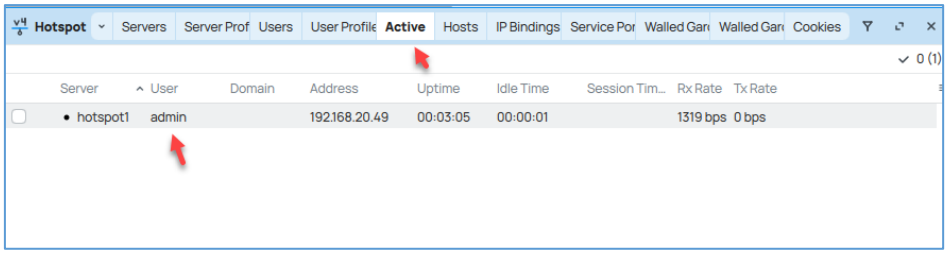
شکل ۷- ۱۴۴ راه‌اندازی Hotspot

همان‌طور که در شکل ۷-۱۴۵، مشاهده می‌کنید بعد از وارد کردن کاربر Admin صفحه‌ی Status را مشاهده می‌کنید که اطلاعاتی مانند آدرس IP، مقدار مصرف، زمان متصل شدن را نشان می‌دهد.



شکل ۷- ۱۴۵ راه‌اندازی Hotspot

اگر به مانند شکل ۷-۱۴۶، در میکروتیک وارد تب Active در سرویس Hotspot شوید مشاهده خواهید کرد که چه کاربرانی آنلاین هستند.

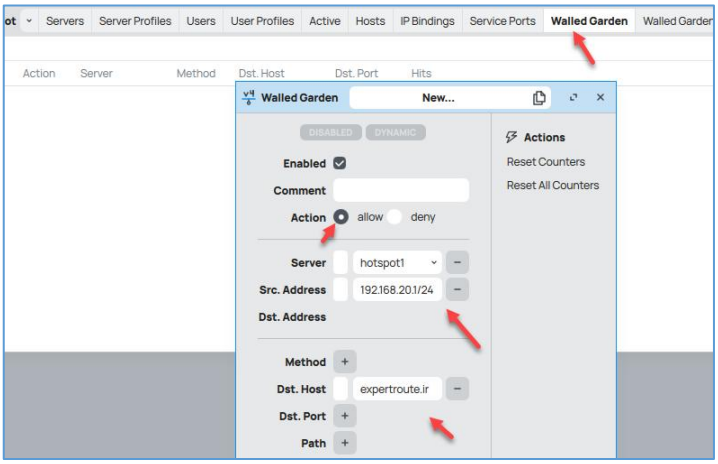


شکل ۷- ۱۴۶ راه‌اندازی Hotspot

شما می‌توانید بعضی از سایت‌ها را برای کاربران خود باز کنید، یعنی اینکه کاربر بدون ورود به Hotspot بتوانند سایت مورد نظر را باز کنند، برای انجام این کار باید طبق شکل ۷-۱۴۷، وارد Walled Garden شوید و بر روی New کلیک کنید. در قسمت Action گزینه‌ی allow را انتخاب کنید، در قسمت Server هم Hotspot

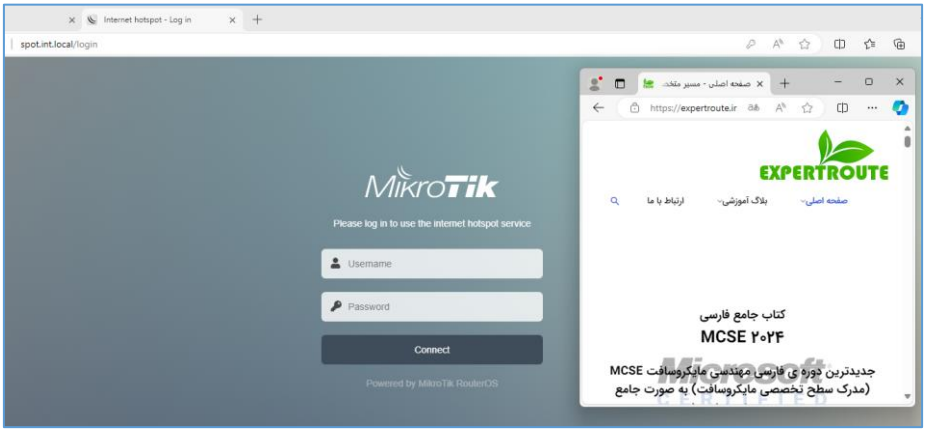
www.takbook.com

را انتخاب و آدرس شبکه‌ی داخلی خود را هم در قسمت Src.address وارد کنید. در مهم‌ترین قسمت، یعنی قسمت Dst. Host می‌توانید نام سایت مورد نظر خود را وارد و بر روی Ok کلیک کنید؛ با این کار کاربران بدون ورود به Hotspot می‌توانند از منابع سایت مورد نظر استفاده کنند، این سایت‌ها می‌تواند سایت‌های داخلی سازمان باشد.



شکل ۷- ۱۴۷ راه‌اندازی Hotspot

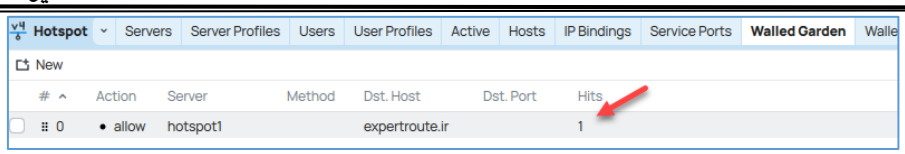
همان‌طور که در شکل ۷-۱۴۸، مشخص است سایت مورد نظر باز شده ولی هنوز کاربر به Hotspot ورود نکرده است.



شکل ۷- ۱۴۸ راه‌اندازی Hotspot

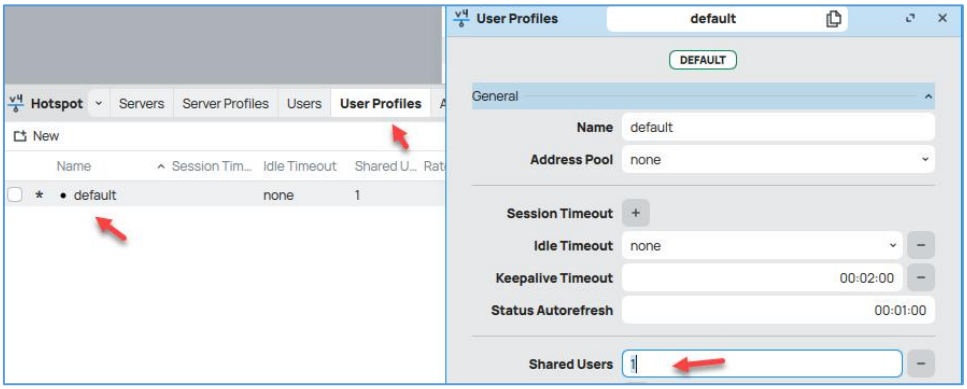
زمانی که کاربر سایت مورد نظر را اجرا کند، بطبق شکل ۷-۱۴۹، در قسمت Hits یک شمارنده وجود دارد که تعداد دفعات درخواست سایت توسط کاربران را ثبت می‌کند.

www.takbook.com



شکل ۷- ۱۴۹ راه‌اندازی *Hotspot*

توجه داشته باشد، زمانی که برای کاربر رمز عبور تعریف می‌کنید، این رمز عبور را یک نفر به طور همزمان می‌توانند مصرف کند؛ برای تغییر این مقدار به مانند شکل ۷-۱۵۰، باید وارد تب User Profiles شوید و بر روی پروفایلی که ایجاد کردید، دو بار کلیک کنید. در صفحه‌ی باز شده در قسمت Shared Users هر عددی قرار دارد، آن را به عدد مورد نظر خود تغییر دهید، اگر مثلاً سه وارد کنید، همزمان سه نفر می‌توانند با همان نام کاربری وارد سرویس شوند و از منابع استفاده کنند.

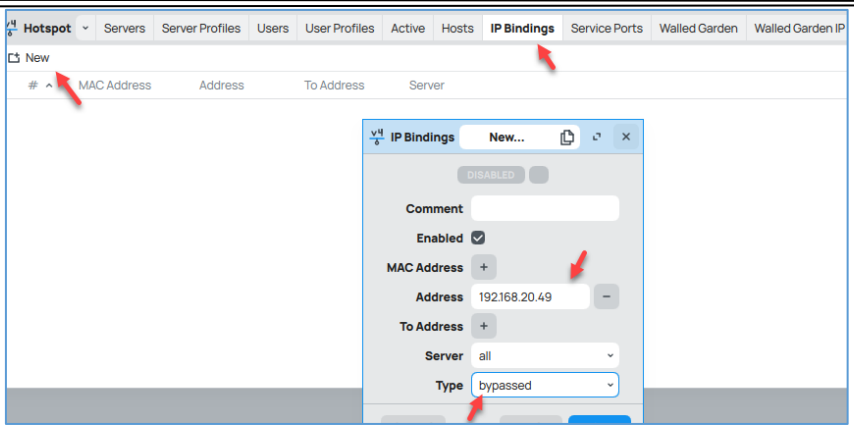


شکل ۷- ۱۵۰ راه‌اندازی *Hotspot*

یک مشکلی که مدیران شبکه با این سرویس دارند این است که کل شبکه درگیر این سرویس خواهد شد و شاید دوست نداشته باشید بعضی از اشخاص یا یک سری سرور خاص زیر مجموعه این سرویس باشند و محدود شوند، برای حل این مشکل باید از IP Bindings استفاده کنیم.

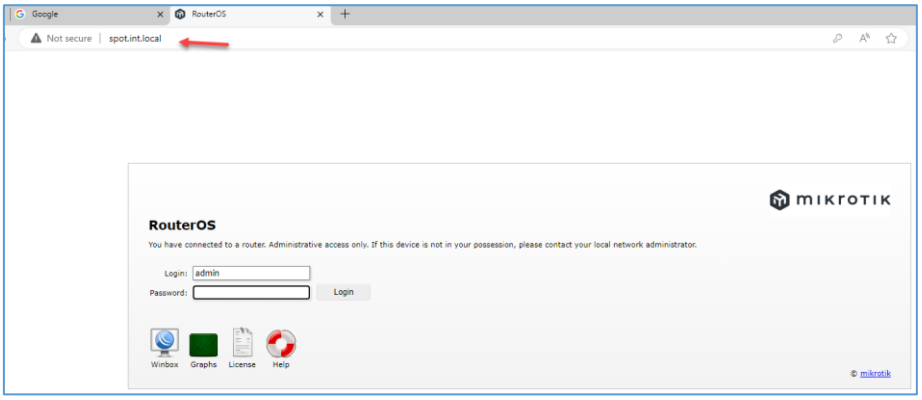
به مانند شکل ۷-۱۵۱، بر روی New کلیک کنید و آدرس کلاینت یا سرور مورد نظر را وارد کنید و در قسمت Type باید گزینه‌ی bypassed را انتخاب کنید.

www.takbook.com



شکل ۷- ۱۵۱ راه‌اندازی *Hotspot*

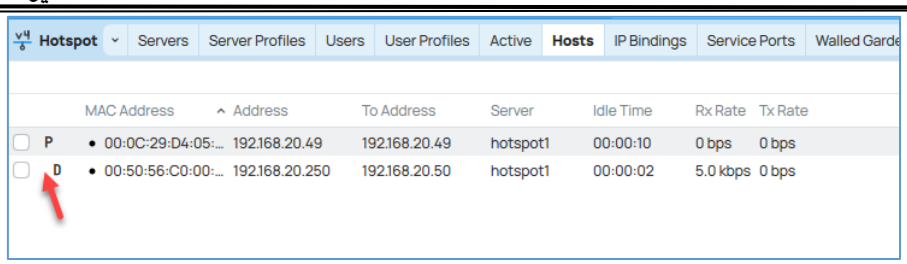
همان‌طور که در شکل ۷-۱۵۲، مشاهده می‌کنید، بعد از اینکه آدرس روتر میکروتیک را در مرورگر وارد کردیم دیگر خبری از صفحه‌ی Hotspot نیست و مستقیم صفحه میکروتیک باز می‌شود و هر سایتی را اجرا کنید باز خواهد شد.



شکل ۷- ۱۵۲ راه‌اندازی *Hotspot*

اگر به مانند شکل ۷-۱۵۳، وارد تب Host شوید، تمام سیستم‌هایی که به آنها اجازه‌ی دسترسی داده شده است، نمایش داده می‌شوند، توجه داشته باشید حرف P نشانگر سیستم‌هایی هستند که در قسمت IP Binding تعریف شده‌اند، اگر به غیر این باشد و کاربر با نام کاربری وارد شود به صورت حروف AD نشان داده خواهد شد.

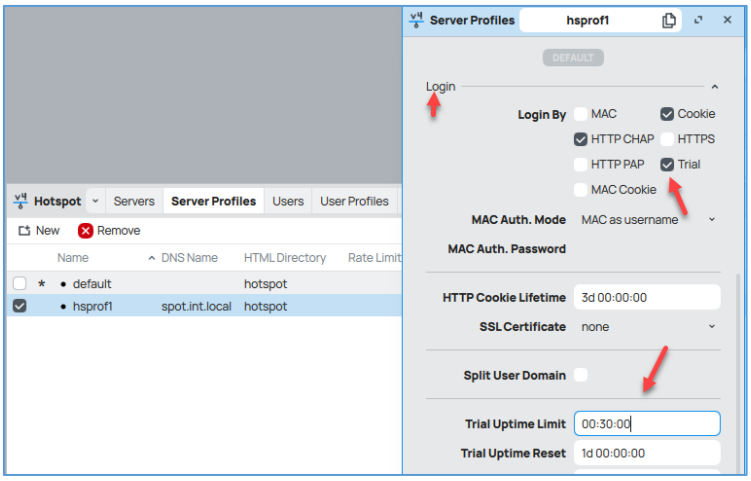
www.takbook.com



شکل ۷- ۱۵۳ راه‌اندازی Hotspot

۷-۲۸ فعال کردن ورود آزمایشی

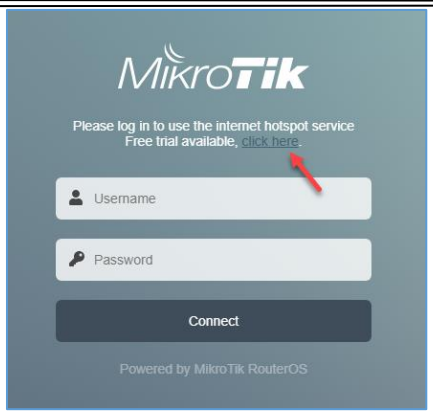
در سرویس Hotspot، گزینه‌ای با نام Trial وجود دارد که به کاربرانی که نام کاربری و رمز عبور ندارند، اجازه‌ی دسترسی به اینترنت در مدت‌زمان مشخص می‌دهد. برای فعال کردن این قابلیت به مانند شکل۷-۱۵٤، وارد تب Server Profiles شوید و بر روی پروفایل موجود در لیست دو بار کلیک کنید، در صفحه‌ی باز شده، وارد تب Login شوید و تیک گزینه‌ی Trial را انتخاب کنید. در قسمت پایین آن می‌توانید مقدار زمان دسترسی به شبکه را در قسمت Trial Uptime Limit مشخص کنید که در اینجا به صورت پیش‌فرض ۳۰ دقیقه وارد شده است که بعد از این زمان دیگر کاربر نمی‌تواند از منابع شبکه استفاده کند، اما اگر در قسمت Trial Uptime Reset، زمان را ۲٤ ساعت، یعنی یک روز قرار دهید کاربر برای روز بعد دوباره می‌تواند از سرویس آزمایشی استفاده کند. این مدل از سرویس‌ها در سازمان‌ها و نهادهای عمومی بیشتر دیده می‌شود.



شکل ۷- ۱۵۴ راه‌اندازی Hotspot

حالا اگر به مانند شکل ۷-۱۵۵، وارد صفحه‌ی Login شوید گزینه‌ی Trial را مشاهده می‌کنید که فعال شده است با کلیک بر روی آن وارد سرویس خواهید شد و اینترنت در دسترس خواهد بود.

www.takbook.com



شکل ۷- ۱۵۵ راه‌اندازی Hotspot



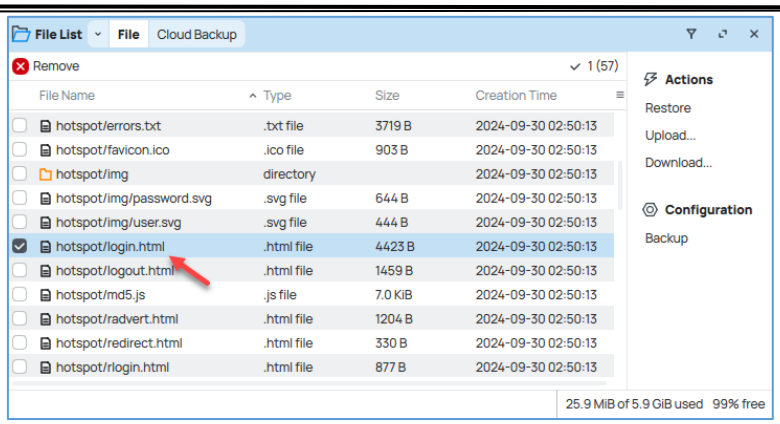
شکل ۷- ۱۵۶ راه‌اندازی Hotspot

۷-۲۹ شخصی‌سازی صفحه‌ی ورود در HotSpot

یکی از ویژگی‌های سرویس HotSpot این است که می‌توانیم صفحه‌ی ورود و اجزای مربوط به آن را شخصی‌سازی کنیم و به هر نحو که دوست داریم آن را طراحی کنیم.

برای انجام این کار به مانند شکل ۷-۱۵۷، باید از سمت چپ بر روی Files کلیک کنید تا صفحه‌ی مورد نظر ظاهر شود، همان‌طور که در لیست مورد نظر مشاهده می‌کنید، صفحات HTML مربوط به سرویس HotSpot مشخص شده است؛ برای اینکه آنها را سفارشی‌سازی کنید، آنها را بر روی کامپیوتر خود بکشید و با نرم افزارهای طراحی سایت می‌توانید این تغییرات را اعمال کنید.

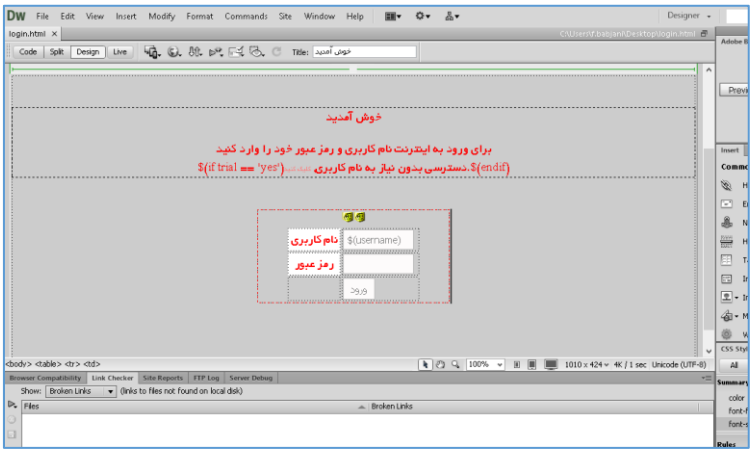
www.takbook.com



شکل ۷- ۱۵۷ صفحه‌ی ورود در HotSpot

توجه : با کوچک‌ترین تغییر اشتباه در صفحه‌ی ورود، به هیچ عنوان صفحه‌ی مورد نظر کار نخواهد کرد، پس سعی کنید یک Backup از صفحه‌ی مورد نظر داشته باشید.

همان‌طور که در شکل ۷–۱۵۸، مشاهده می‌کنید، صفحه‌ی مورد نظر توسط نرم افزار Dreamweaver، سفارشی‌سازی شده است. با همان اسم، اطلاعات را ذخیره می‌کنیم و دوباره بر روی روتر قرار می‌دهیم.

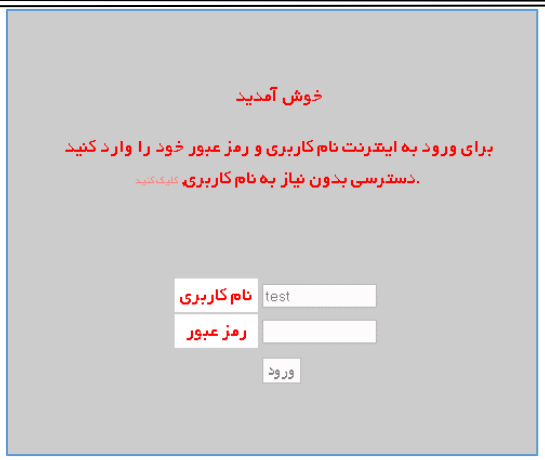


شکل ۷- ۱۵۸ صفحه‌ی ورود در HotSpot

سعی کنید اول، صفحه‌ای قدیمی را از روی روتر میکروتیک حذف کنید و بعد، این صفحه را در جای صفحه‌ی قبلی قرار دهید.

همان‌طور که در شکل ۷–۱۵۹، مشاهده می‌کنید، صفحه‌ی ورود به صورت کامل تغییر کرده است، توجه داشته باشید شما می‌توانید تمام صفحات مربوط به سرویس HotSpot را تغییر دهید.

www.takbook.com

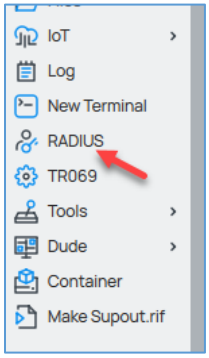


شکل ۷- ۱۵۹ صفحه‌ی ورود در HotSpot

۷-۳۰ راه‌اندازی Radius Server و ارتباط آن با Hotspot

برای اینکه کاربران خود را بهتر مدیریت کنیم و سیاست‌های درست را راه‌اندازی کنیم، بهتر است این کاربران را از طریق سرویس Radius به Active Directory یا Usermanager خود میکروتیک متصل کنید.

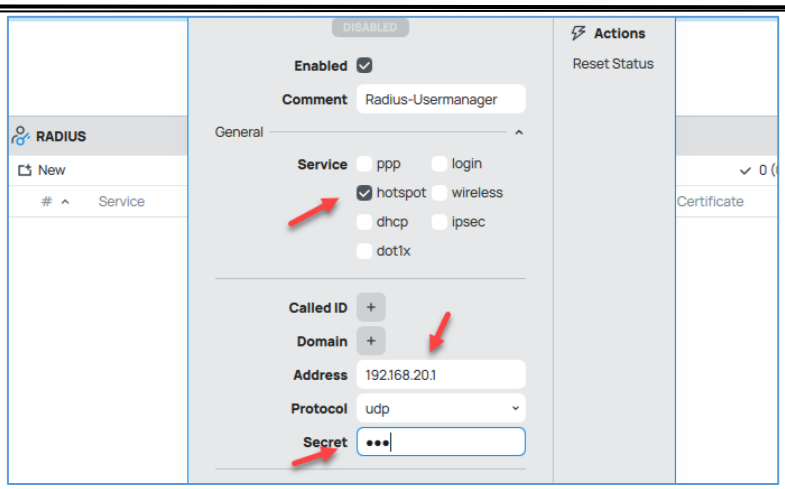
برای این کار به مانند شکل ۷-۱۶۰، وارد Radius شوید.



شکل ۷- ۱۶۰ راه‌اندازی Radius Server

در شکل ۷-۱۶۱، باید در قسمت سرویس گزینه‌ی Hotspot را انتخاب کنید و در قسمت Address، آدرس خود روتر را وارد کنید چون می‌خواهیم از Usermanager خود روتر استفاده کنیم، یک رمز هم در قسمت Secret وارد کنید و این رمز را به خاطر داشته باشید.

www.takbook.com

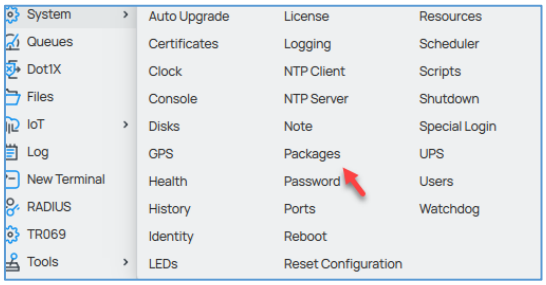


شکل ۷- ۱۶۱ راه‌اندازی Radius Server

وقتی که سرویس را فعال کردید در همان صفحه‌ی اصلی بر روی Incoming کلیک کنید و تیک گزینه‌ی Accept را انتخاب کنید.

در ادامه کار باید سرویس User manager را بر روی روتر نصب کنیم، روتر مجازی که من از آن استفاده می‌کنم این سرویس را دارد ولی برای اینکه سرویس User manager را بر روی روتر نصب کنید باید وارد سایت میکروتیک شوید و پکیج کامل مربوط به ورژن روتر خود را دانلود کنید.

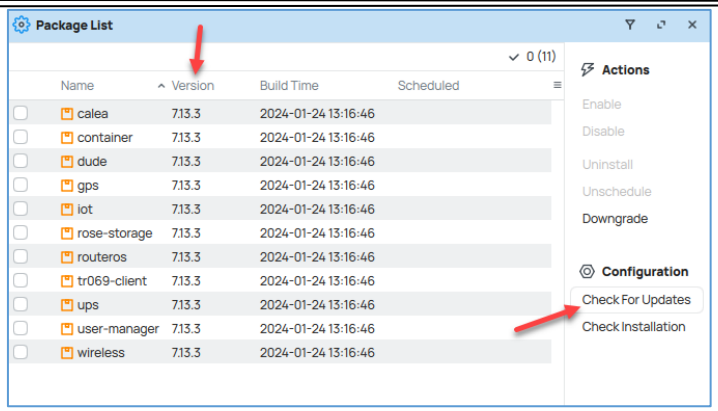
قبل از دانلود پکیج طبق شکل ۷-۱۶۲، وارد قسمت system و بعد Packages شوید و ورژن سیستم عامل روتر میکروتیک را چک کنید.



شکل ۷- ۱۶۲ راه‌اندازی Radius Server

همان‌طور که در شکل ۷-۱۶۳، مشاهده می‌کنید ورژن روتر 7.13.3 نوشته شده است و برای اینکه آخرین ورژن را داشته باشیم بهتر است بر روی Check For Updates کلیک کنید.

www.takbook.com

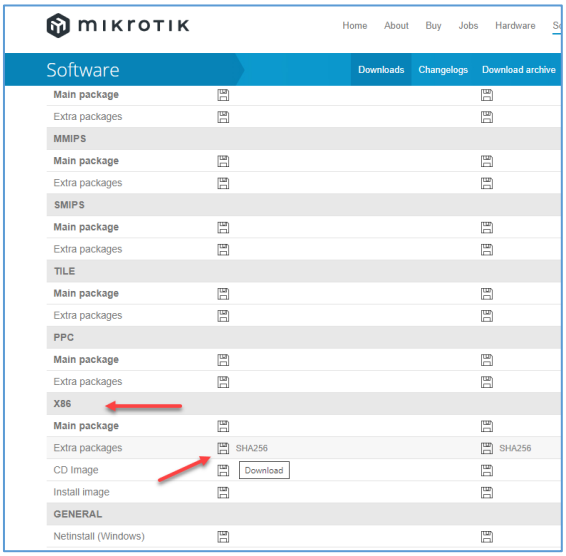


شکل ۷- ۱۶۳ راه‌اندازی Radius Server

ورژن جدید آن یعنی 7.16 در دسترس است که می‌توانید بر روی Download &install کلیک کنید، بعد از آپدیت به ورژن 7.16 باید به آدرس زیر مراجعه کنید.

https://mikrotik.com/download

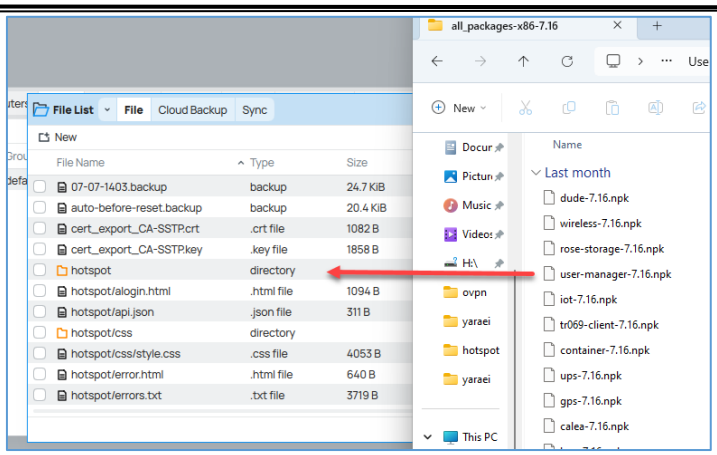
طبق شکل ۷-١٦٤مدل روتر خود را بدانید که در اینجا ورژن x86 را نصب کرده بودیم و باید در همان قسمت بر روی Extera Packages کلیک کنید.



شکل ۷-۱۶۴ راه‌اندازی Radius Server

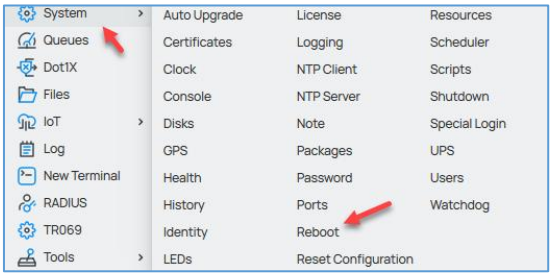
بعد از دانلود فایل آن را از حالت فشرده خارج کنید و به مانند شکل ۷-١٦٥، چندین ابزار مختلف را مشاهده می‌کنید که باید ابزار user-manager-7.16.npk را بکشید و در قسمت Files روتر میکروتیک رها کنید.

www.takbook.com



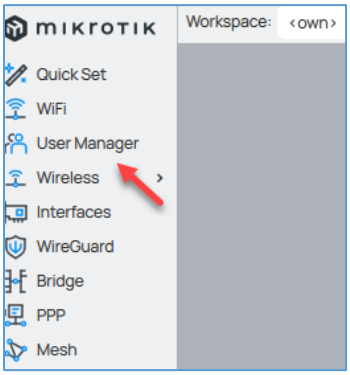
شکل ۷- ۱۶۵ راه‌اندازی *Radius Server*

بعد از کپی کردن فایل به مانند شکل ۷-۱۶۶، باید روتر را Reboot کنید تا سرویس و ابزار مورد نظر نصب شود.



شکل ۷- ۱۶۶ راه‌اندازی *Radius Server*

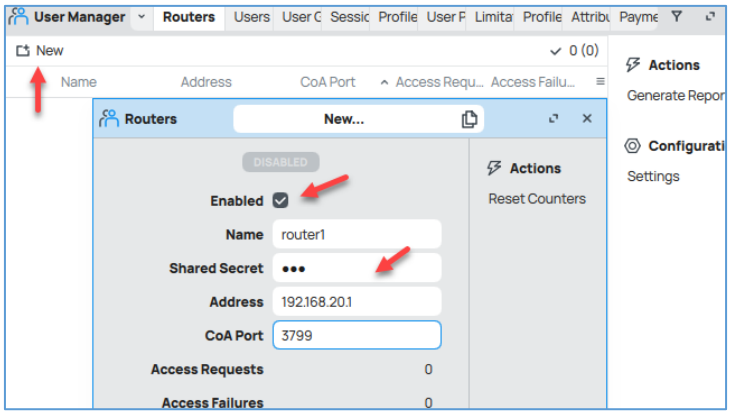
همان‌طور که در شکل ۷-۱۶۷، مشاهده می‌کنید ابزار مورد نظر نصب شده است و باید ادامه کار را با این ابزار پیش ببریم.



شکل ۷-۱۶۷ راه‌اندازی *Radius Server*

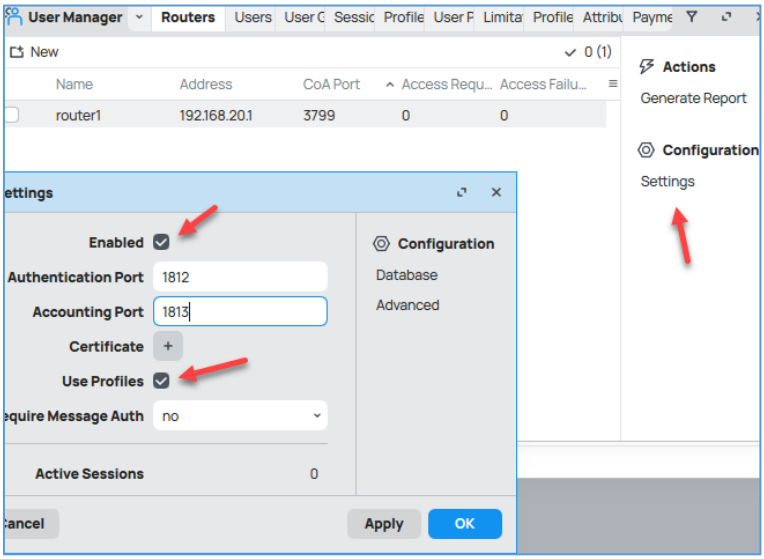
www.takbook.com

در شکل ۷–۱۶۸، در تب Routers بر روی New کلیک کنید و یک نام وارد کنید و در قسمت Shared Secret رمز عبوری که در قسمت Radius وارد کردیم را اینجا وارد کنید. و بعد آدرس سرور را باید وارد کنید و بر روی OK کلیک کنید.



شکل ۷- ۱۶۸ راه‌اندازی *Radius Server*

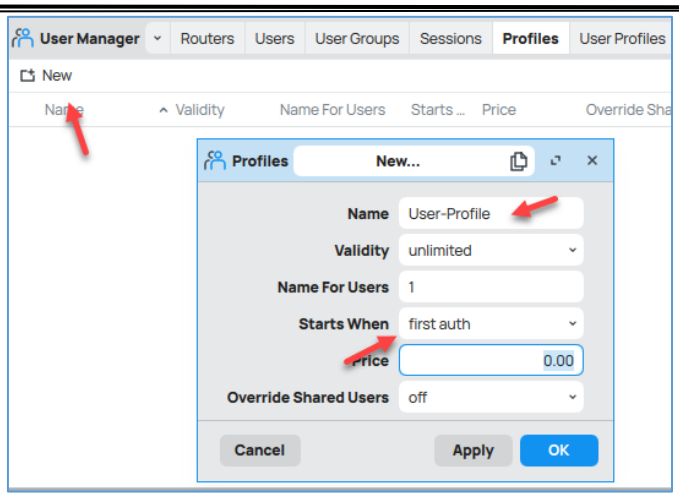
به مانند شکل ۷–۱۶۹، در همان صفحه و همان تب Routers بر روی Settings کلیک کنید و تیک Enable را انتخاب کنید و در پایین آن تیک گزینه‌ی Use Profiles را انتخاب و بر روی OK کلیک کنید.



شکل ۷- ۱۶۹ راه‌اندازی *Radius Server*

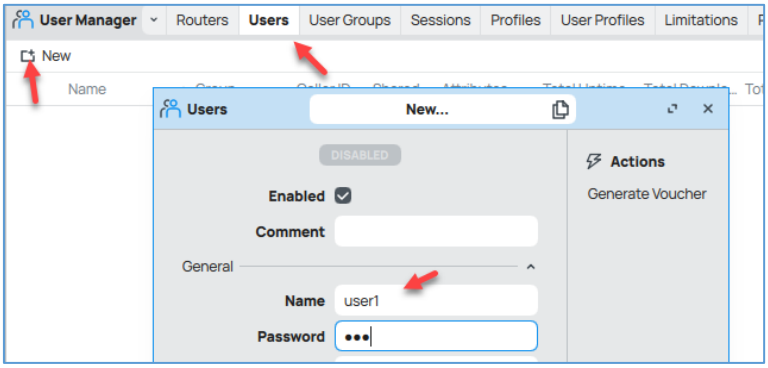
در ادامه کار طبق شکل ۷–۱۷۰، وارد تب Profiles شوید و یک نام برای آن تعریف کنید و در قسمت Starts When گزینه‌ی first auth را انتخاب کنید.

www.takbook.com



شکل ۷- ۱۷۰ راه‌اندازی *Radius Server*

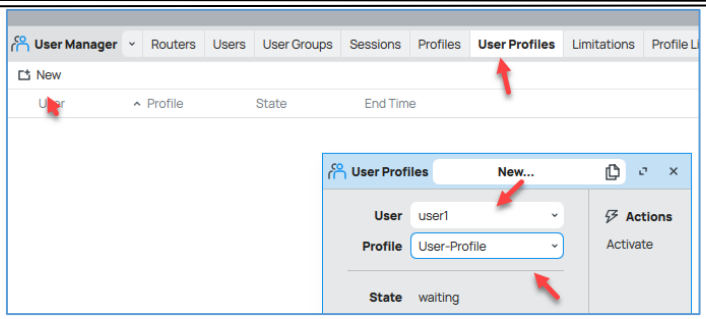
در شکل ۷-۱۷۱، وارد تب Users شوید و یک کاربر جدید تعریف کنید.



شکل ۷- ۱۶۴ راه‌اندازی *Radius Server*

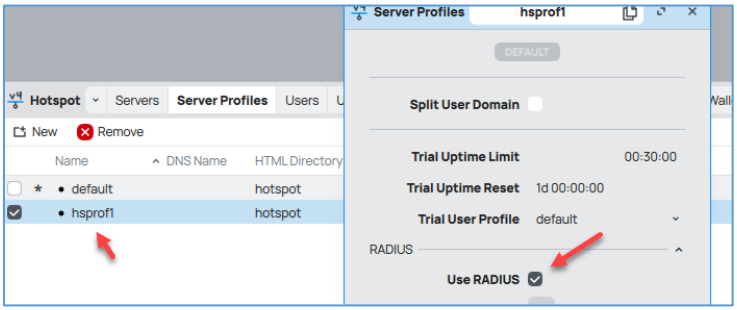
بعد از تعریف کاربر و در شکل ۷-۱۷۲، وارد تب User Profile شوید و یک پروفایل ایجاد کنید و به کاربر مورد نظر متصل کنید.

www.takbook.com



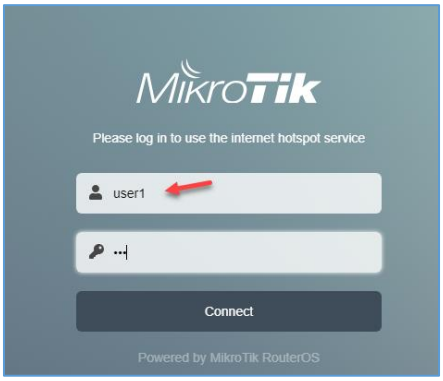
شکل ۷- ۱۶۵ راه‌اندازی *Radius Server*

بعد از اتمام کار طبق شکل ۷-۱۷۳، وارد Hotspot شوید و در تب Server Profiles بر روی پروفایل خود دو بار کلیک کنید و به ماند شکل در قسمت Radius تیک Use RADIUS را انتخاب کنید.



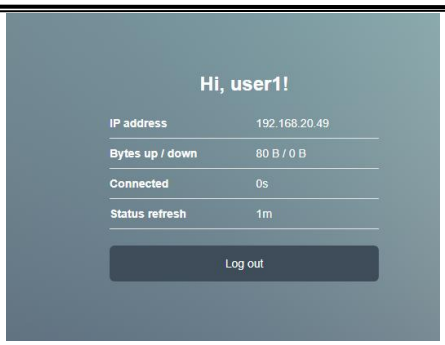
شکل ۷- ۱۶۶ راه‌اندازی *Radius Server*

بعد از اتمام کار طبق شکل ۷-۱۷٤و ۷-۱۷۵، می‌توانید با کاربرانی که در سرویس User Manager تعریف کردید وارد روتر شوید و به اینترنت دسترسی داشته باشید.



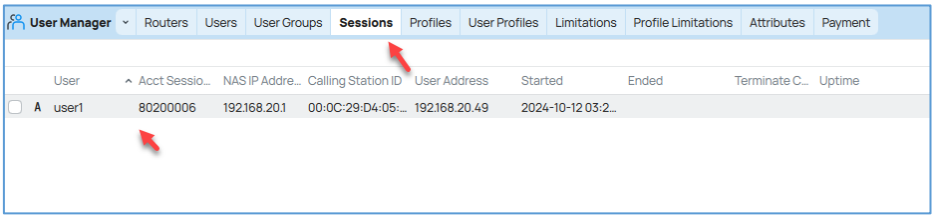
شکل ۷- ۱۶۷ راه‌اندازی *Radius Server*

www.takbook.com



شکل ۷- ۱۶۸ راه‌اندازی Radius Server

اگر بفه مانند شکل ۷-۱۷۶، به سرویس User Manager مراجعه کنید در تب Sessions کاربرانی که به سرویس متصل شده‌اند را قابل مشاهده هستند.



شکل ۷- ۱۶۹ راه‌اندازی Radius Server

توجه داشته باشید در تب Limitations و Profile Limitations می‌توانید محدودیت دانلود و آپلود ایجاد کنید.

۷-۳۱ راه‌اندازی پروتکل L2TP

L2TP (Layer 2 Tunneling Protocol) یک پروتکل تونل‌سازی در لایه ۲ مدل OSI است که برای ایجاد اتصالات امن بین شبکه‌ها استفاده می‌شود. این پروتکل به‌طور گسترده برای ایجاد شبکه‌های خصوصی مجازی (VPN) کاربرد دارد. L2TP به‌تنهایی قابلیت رمزنگاری داده‌ها را ندارد، اما معمولاً در ترکیب با IPsec (Internet Protocol Security) برای رمزنگاری و حفظ امنیت داده‌ها استفاده می‌شود.

ویژگی‌های L2TP:

- تونل‌سازی در لایه ۲: L2TP در لایه پیوند داده (Layer 2) عمل می‌کند و بسته‌های داده را تونل می‌کند تا از طریق شبکه عمومی (مانند اینترنت) انتقال یابند.
- بدون رمزنگاری: خود L2TP از رمزنگاری داده‌ها پشتیبانی نمی‌کند؛ به همین دلیل، به‌طور معمول از IPsec برای رمزنگاری استفاده می‌شود.

www.takbook.com

- انعطاف‌پذیری: L2TP می‌تواند با پروتکل‌های دیگری مانند PPP (Point-to-Point Protocol) ادغام شود تا از مزایای احراز هویت و مدیریت بسته‌های داده بهره ببرد.
- استفاده در VPNها: بیشترین کاربرد L2TP در شبکه‌های خصوصی مجازی (VPN) است که امنیت و حفظ حریم خصوصی را در انتقال داده‌ها فراهم می‌کنند.

چگونگی عملکرد:

داده‌های کاربر با استفاده از PPP فشرده و کپسوله می‌شوند.

L2TP یک تونل ایجاد می‌کند که داده‌های PPP را از طریق اینترنت یا هر شبکه‌ی دیگری انتقال می‌دهد.

برای امنیت بیشتر، اغلب L2TP با IPsec جفت می‌شود، که این ترکیب به نام L2TP/IPsec شناخته می‌شود.

کاربردها:

- اتصال امن بین شعب مختلف یک سازمان.
- دسترسی امن کاربران به منابع شبکه از راه دور.
- ایجاد ارتباطات امن بین شبکه‌های خصوصی در بستر اینترنت.

با توجه به اینکه L2TP به خودی خود رمزنگاری انجام نمی‌دهد، استفاده از آن به همراه IPsec بسیار رایج است تا امنیت در ارتباطات حفظ شود.

برای راه اندازی این پروتکل باید چند کار در میکروتیک انجام دهیم، اولین کاری که باید انجام دهیم این است که طبق شکل ۷-۱۷۷، پورت‌های مورد نیاز این پروتکل را در فایروال میکروتیک باز کنیم، برای این کار باید دستورات زیر را در Terminal وارد کنید.

```
/ip firewall filter
add action=accept chain=input  protocol=ipsec-esp\
   comment="allow L2TP VPN (ipsec-esp)"
add action=accept chain=input dst-port=1701  protocol=udp\
   comment="allow L2TP VPN (1701/udp)"
add action=accept chain=input dst-port=4500  protocol=udp\
   comment="allow L2TP VPN (4500/udp)"
add action=accept chain=input dst-port=500  protocol=udp\
  comment="allow L2TP VPN (500/udp)"
```

همان‌طور که مشاهده می‌کنید دستورات مورد نظر با موفقیت اجرا شده است.

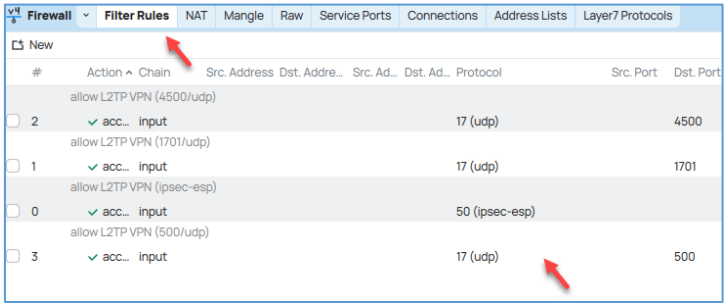
www.takbook.com


```
Press F1 for help

[admin@Mik-Teh] > /ip firewall filter
[admin@Mik-Teh] /ip/firewall/filter> add action=accept chain=input  protocol=ipsec-esp \
\...      comment="allow L2TP VPN (ipsec-esp)"
[admin@Mik-Teh] /ip/firewall/filter> add action=accept chain=input dst-port=1701  protocol=udp \
\...      comment="allow L2TP VPN (1701/udp)"
[admin@Mik-Teh] /ip/firewall/filter> add action=accept chain=input dst-port=4500  protocol=udp \
\...      comment="allow L2TP VPN (4500/udp)"
[admin@Mik-Teh] /ip/firewall/filter> add action=accept chain=input dst-port=500  protocol=udp \
\...      comment="allow L2TP VPN (500/udp)"
[admin@Mik-Teh] /ip/firewall/filter>
[admin@Mik-Teh] /ip/firewall/filter>
```

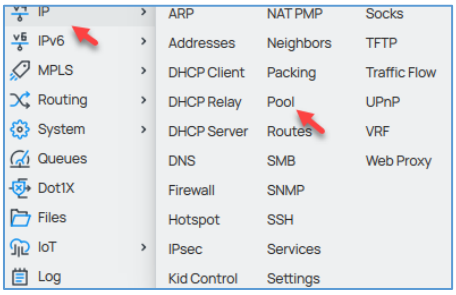
شکل ۷- ۱۷۶ پروتکل L2TP

اگر به مانند شکل ۷–۱۷۸، به قسمت Firewall و تب Filter مراجعه کنید این سه Rule را مشاهده می‌کنید که ایجاد شده است.



شکل ۷- ۱۷۸ پروتکل L2TP

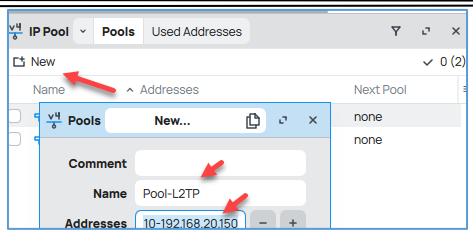
در ادامه کار باید یک Pool برای این پروتکل ایجاد کنیم و به کاربران تخصیص دهیم، برای این کار همانند شکل ۷–۱۷۹، وارد IP و بعد Pool شوید.



شکل ۷- ۱۷۹ پروتکل L2TP

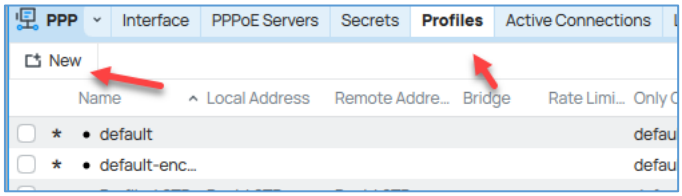
در شکل ۷–۱۸۰، یک رنج آدرس را برای کاربرانی که می‌خواهند از پروتکل L2TP استفاده کنند وارد کنید که در اینجا رنج 192.168.20.110 تا 192.168.20.150 را وارد می‌کنیم و یک نام برای آن در نظر می‌گیریم.

www.takbook.com



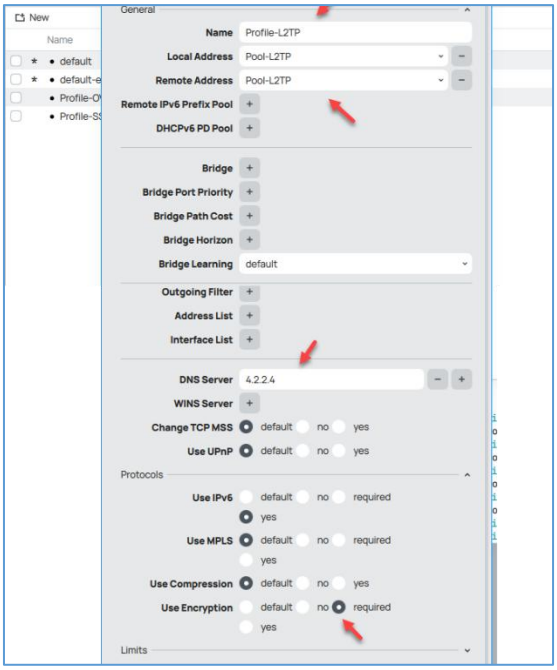
شکل ۷- ۱۸۰ پروتکل L2TP

در ادامه کار همانند شکل ۷-۱۸۱، وارد PPP شوید و بعد وارد تب Profile شوید و بر روی New کلیک کنید.



شکل ۷- ۱۸۱ پروتکل L2TP

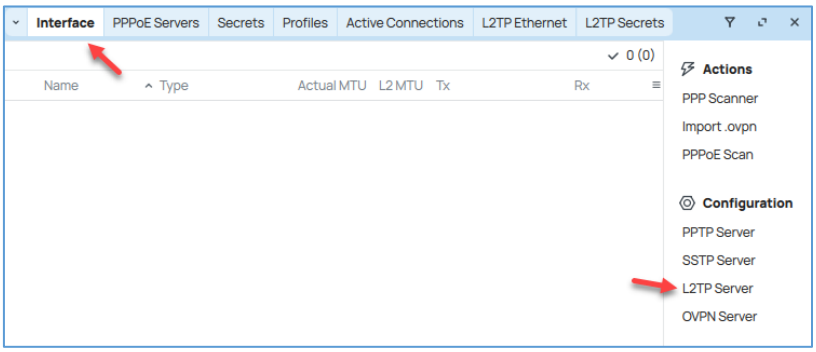
در شکل ۷-۱۸۲، باید در قسمت Local و Remote همان Pool که در قسمت قبل ایجاد کردیم را انتخاب کنید، DNS را هم در قسمت مورد نظر وارد کنید و در آخر صفحه هم گزینه‌ی Required را انتخاب کنید.



شکل ۷- ۱۸۲ پروتکل L2TP

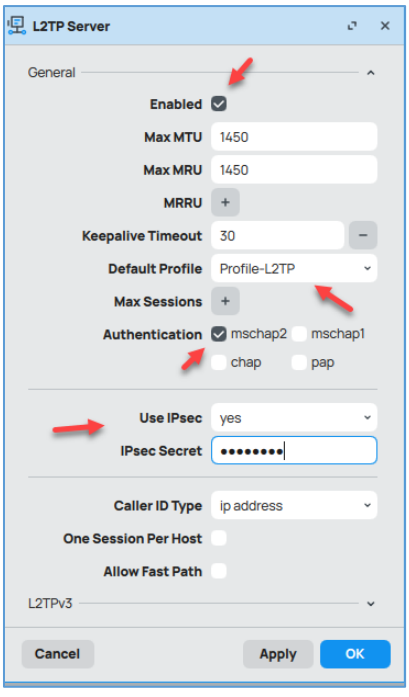
www.takbook.com

به مانند شکل ۷-۱۸۳، وارد تب Interface در PPP شوید و بر روی L2TP Server کلیک کنید.



شکل ۷- ۱۸۳ پروتکل L2TP

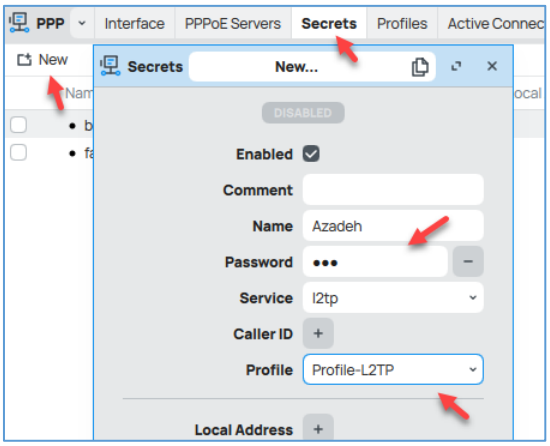
در شکل ۷-۱۸٤، گزینه‌ی Enable را انتخاب کنید و در قسمت Profile باید همان Profile که با هم ایجاد کردیم را انتخاب کنید و در قسمت Authentication هم فقط تیک گزینه‌ی mschap2 را برای امنیت بیشتر انتخاب کنید، گزینه‌ی دیگری که باعث ایجاد امنیت در پروتکل L2TP می‌شود این است که باید از Pre Share Key یا کلید عمومی استفاده کنیم که این گزینه را بر روی Yes قرار دهید و یک رمز وارد کنید، توجه داشته باشید این رمز، ربطی به نام کاربری و رمز عبور کاربر ندارد و جدا از آن است.



شکل ۷- ۱۸۴ پروتکل L2TP

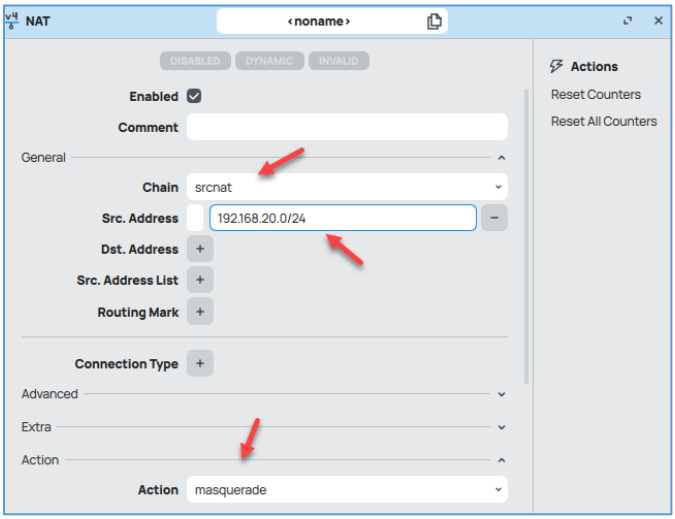
www.takbook.com

بعد از فعال‌سازی سرویس L2TP باید یک کاربر تعریف کنیم و با آن به روتر متصل شویم برای این کار به مانند شکل ۷-۱۸۵، وارد تب Secret در PPP شوید و یک کاربر انتخاب و نوع سرویس آن را بر روی L2TP قرار دهید و Profile مورد نظر را انتخاب کنید.



شکل ۷- ۱۸۵ پروتکل L2TP

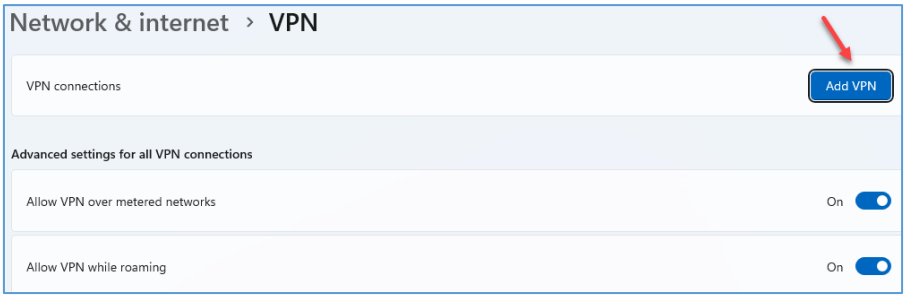
بعد از انجام مراحل بالا باید برای کاربرانی که می‌خواهند از رنج IP که در Pool مورد نظر تعریف شده استفاده کنند، آدرس داخلی آنها را به سمت اینترنت NAT کنیم تا بتوانند به اینترنت دسترسی داشته باشند، برای این کار به مانند شکل ۷-۱۸۶، وارد Firewall شوید و در تب NAT بر روی New کلیک کنید و به رنج آدرس شبکه‌ی داخلی را در قسمت SRC.Address وارد کنید و در قسمت Action گزینه‌ی Masquerade را انتخاب کنید تا آدرس‌های مورد نظر به سمت اینترنت ترجمه شوند.



شکل ۷- ۱۸۶ پروتکل L2TP

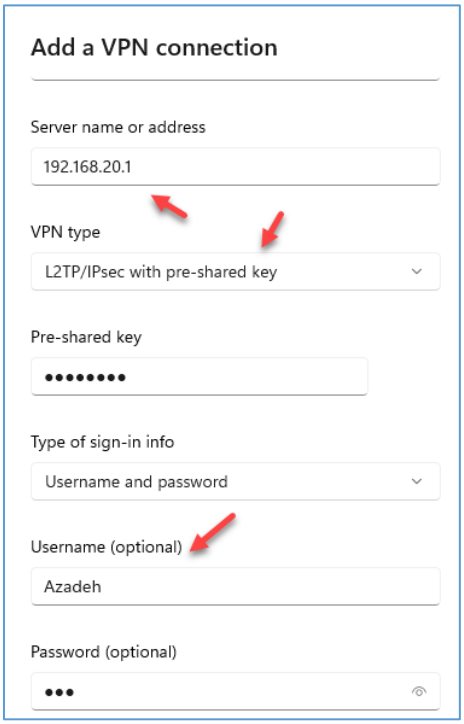
www.takbook.com

حالا می‌توانید با استفاده از کلاینت خود به روتر از طریق پروتکل L2TP متصل شوید، برای تست این موضوع به مانند شکل ۷-۱۸۷ وارد VPN مربوط به ویندوز می‌شویم و بر روی Add VPN کلیک کنید.



شکل ۷-۱۸۷ پروتکل L2TP

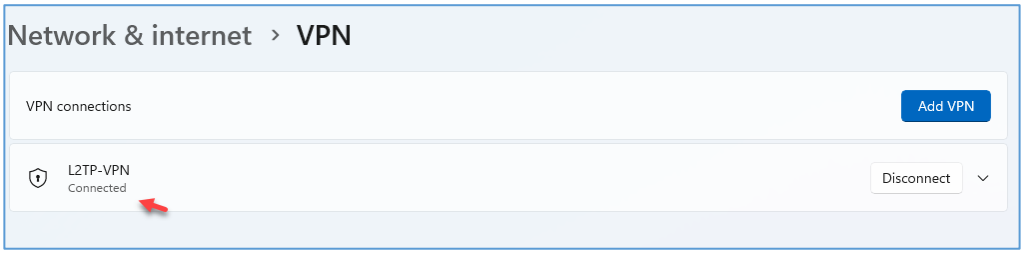
در شکل ۷-۱۸۸، باید یک نام برای VPN خود وارد کنید و در قسمت Address باید آدرس روتر میکروتیک خود را وارد کنید، نوع پروتکل را L2TP در نظر بگیرید و نام کاربری و رمز عبور را وارد کنید، در قسمت Preshare Key هم باید رمز عبور عمومی خود را وارد کنید که در قسمت قبل توضیح دادیم.



شکل ۷-۱۸۸ پروتکل L2TP

www.takbook.com

همان‌طور که در شکل ۷-۱۸۹، مشاهده می‌کنید بعد از کلیک بر روی Connect با موفقیت به روتر میکروتیک از طریق L2TP متصل شدیم.



شکل ۷- ۱۸۹ متصل شدن کلاینت

۷-۳۲ راه‌اندازی پروتکل OVPN

یکی از بهترین راه‌های ایجاد سرویس VPN امن استفاده از پروتکل قدرتمند OVPN است که در این قسمت آن را راه‌اندازی می‌کنیم.

پروتکل OVPN (OpenVPN) یک نرم‌افزار و پروتکل محبوب و متن‌باز (Open Source) برای ایجاد شبکه‌های خصوصی مجازی (VPN) است که ارتباطات ایمن و رمزگذاری شده‌ای را بین کلاینت و سرور یا بین شبکه‌های مختلف برقرار می‌کند. OpenVPN به دلیل امنیت بالا، انعطاف‌پذیری و سازگاری با انواع سیستم‌عامل‌ها و دستگاه‌ها به‌عنوان یکی از پروتکل‌های پرکاربرد در راه‌اندازی VPN شناخته می‌شود.

ویژگی‌های کلیدی پروتکل OpenVPN

- رمزگذاری قوی: OpenVPN از پروتکل‌های رمزنگاری پیشرفته‌ای مانند SSL/TLS برای احرازهویت و رمزگذاری ترافیک استفاده می‌کند. از الگوریتم‌های قوی مثل AES-256 و پروتکل‌های رمزنگاری متعدد (مانند SHA، HMAC) پشتیبانی می‌کند که امنیت بالایی را برای داده‌های شما فراهم می‌سازد.
- انعطاف‌پذیری در پیکربندی: OpenVPN می‌تواند بر روی پروتکل‌های UDP یا TCP اجرا شود، به این معنا که شما می‌توانید آن را با توجه به نیازها و محیط شبکه خود تنظیم کنید. این انعطاف‌پذیری باعث می‌شود OpenVPN به‌راحتی از فایروال‌ها و NAT عبور کند.
- استفاده از پورت‌های مختلف: یکی از مزیت‌های OpenVPN این است که می‌تواند از پورت‌های مختلف (به‌طور پیش‌فرض از پورت ۱۱۹۴ UDP) استفاده کند، اما شما می‌توانید آن را بر روی هر پورتی که می‌خواهید تنظیم کنید، حتی پورت‌های استاندارد مانند ۴۴۳ (HTTPS) که در اکثر شبکه‌ها باز است و باعث می‌شود شناسایی و مسدودسازی OpenVPN بسیار سخت‌تر شود.
- پشتیبانی از احراز هویت دو طرفه (Two-way Authentication): OpenVPN امکان استفاده از گواهی‌های دیجیتالی (SSL Certificates) برای احراز هویت را فراهم می‌کند، که امنیت بالاتری

www.takbook.com

نسبت به تنها استفاده از رمز عبور دارد. این بدان معناست که سرور و کلاینت هر دو باید گواهی‌های معتبری داشته باشند تا بتوانند به یکدیگر متصل شوند.

- Cross-platform بودن: OpenVPN برای انواع سیستم‌عامل‌ها (ویندوز، لینوکس، macOS، iOS، اندروید و حتی روترها و دستگاه‌های IoT) موجود است و این باعث می‌شود که کاربران بتوانند به راحتی از آن در هر محیطی استفاده کنند.
- مقابله با Deep Packet Inspection (DPI): یکی از قابلیت‌های کلیدی OpenVPN این است که می‌تواند به راحتی از فیلترهای Deep Packet Inspection (DPI) عبور کند. این ویژگی به OpenVPN اجازه می‌دهد تا در محیط‌هایی که تلاش برای مسدودسازی VPNها صورت می‌گیرد (مانند برخی کشورها یا شبکه‌های شرکتی) همچنان بتواند ارتباطات ایمن را فراهم کند.
- نصب و راه‌اندازی آسان: OpenVPN با وجود انعطاف‌پذیری بالا، دارای راه‌اندازی نسبتاً آسانی است. با استفاده از ابزارهای GUI (مانند OpenVPN GUI برای ویندوز) یا نصب روی روترها و سرورهای لینوکس، می‌توان آن را به‌راحتی پیکربندی کرد.

مزایای OpenVPN

- امنیت بالا به‌خاطر استفاده از استانداردهای پیشرفته رمزنگاری.
- پشتیبانی گسترده از پلتفرم‌های مختلف.
- انعطاف‌پذیری بالا در پیکربندی و استفاده از پورت‌های مختلف.
- امکان پیکربندی Site-to-Site VPN یا Client-to-Site VPN.
- عبور از فایروال‌ها و NAT به‌خاطر امکان استفاده از پورت‌های مختلف (مانند پورت ۴۴۳).

معایب OpenVPN

- کمی پیچیدگی در پیکربندی برای کاربران غیرتخصصی.
- نیاز به گواهی‌های دیجیتال و پیکربندی درست برای بهره‌مندی از احراز هویت دو طرفه.
- عملکرد نسبتاً کندتر نسبت به پروتکل‌های ساده‌تر مانند PPTP یا L2TP به دلیل استفاده از رمزنگاری قوی.

موارد استفاده از OpenVPN

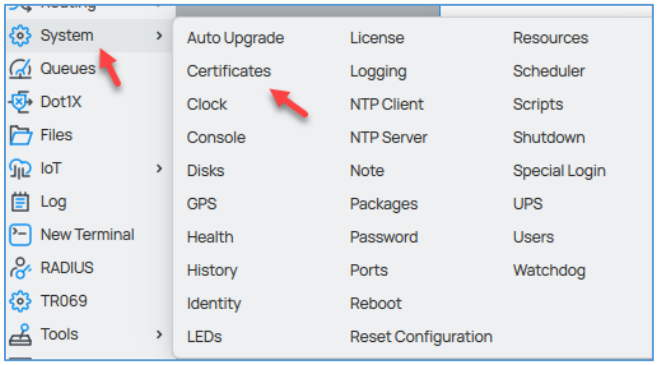
- اتصال از راه دور امن به شبکه شرکتی (کاربران می‌توانند از طریق یک تونل امن به شبکه سازمانی متصل شوند).
- اتصال بین دو یا چند شبکه از طریق اینترنت با استفاده از Site-to-Site VPN.
- استفاده از VPN برای دور زدن فیلترینگ اینترنت و حفظ حریم خصوصی.

www.takbook.com

- محافظت از داده‌های حساس در حین انتقال بر روی اینترنت یا شبکه‌های عمومی Wi-Fi.

به‌طور کلی، OpenVPN به دلیل امنیت، انعطاف‌پذیری و پشتیبانی از انواع پلتفرم‌ها و شبکه‌ها، یکی از محبوب‌ترین و قدرتمندترین پروتکل‌های VPN موجود است.

برای اینکه سرویس Open VPN را در میکروتیک فعال کنیم، باید به مانند شکل ۷-۱۹۰، اول وارد System /Certificate شوید.



شکل ۷- ۱۹۰ پروتکل OVPN

برای شروع ما باید سه تا گواهینامه ایجاد کنیم، توجه داشته باشید برای اینکه این کار به صورت سریع و بدون مشکل انجام دهیم بهتر است دستورات زیر را در Terminal وارد کنیم، در دستوارت زیر جاهایی که مشخص کردیم می‌توانید یک نام دلخواه وارد کنید.

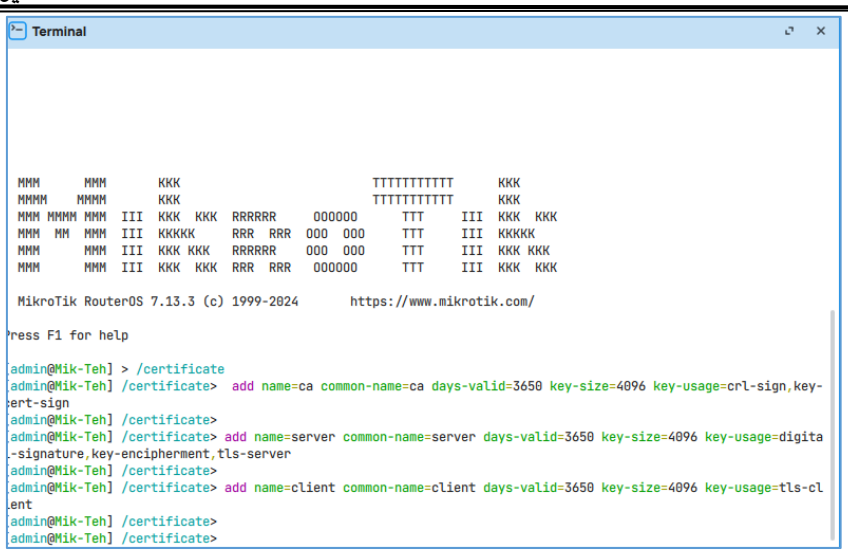
```
/certificate
 add name=ca common-name=ca days-valid=3650 key-size=4096 key-usage=crl-sign,key-cert-sign

add name=server common-name=server days-valid=3650 key-size=4096 key-usage=digital-
signature,key-encipherment,tls-server

add name=client common-name=client days-valid=3650 key-size=4096 key-usage=tls-client
```

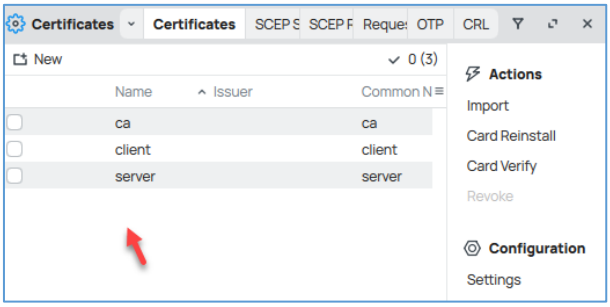
به مانند شکل ۷-۱۹۱، دستورات را وارد کردیم و خروجی آن را می‌توانید در قسمت Certificate مشاهده کنید.

www.takbook.com



شکل ۷- ۱۹۱ پروتکل OVPN

همان‌طور که در شکل ۷-۱۹۲، مشاهده می‌کنید سه تا گواهینامه با نام‌های مشخص شده ایجاد شده است.



شکل ۷- ۱۹۲ پروتکل OVPN

در ادامه کار باید این سه گواهینامه را فعال کنیم یا همان Sign کردن آنها، برای این کار باید دستورات زیر را در Terminal وارد کنید.

نکته مهم در اجرای این دستورات این است که چون لود CPU بالا می‌رود باید تک تک اجرا کنید و بعد از اتمام بعدی را اجرا کنید.

/certificate

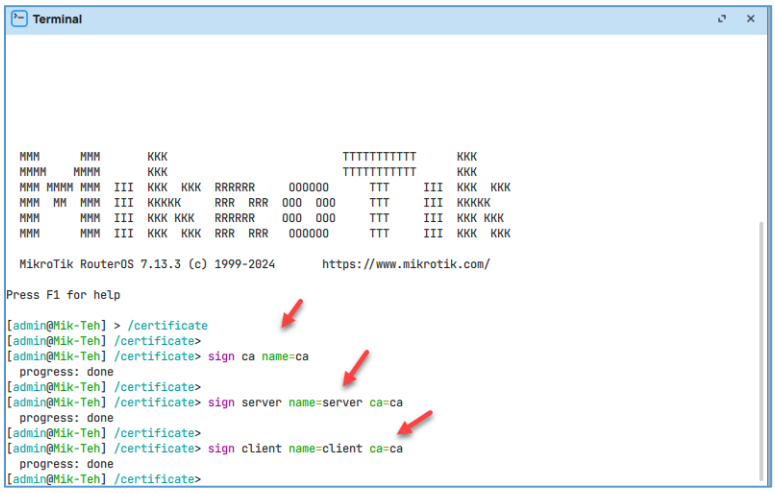
sign ca name=ca

sign server name=server ca=ca

www.takbook.com

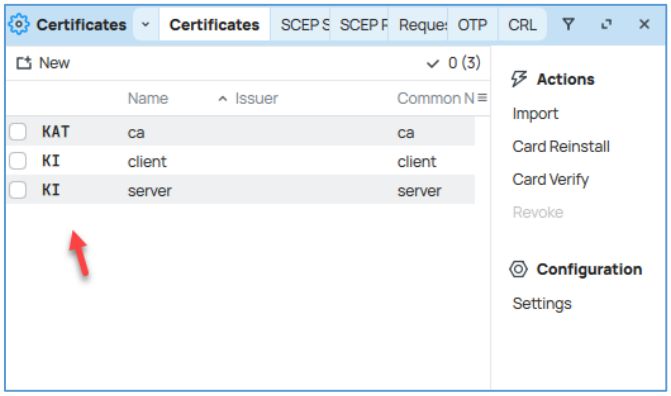
sign client name=client ca=ca

همان‌طور که در شکل ۷-۱۹۳، مشاهده می‌کنید دستورات با موفقیت اجرا شده است.



شکل ۷- ۱۹۳ پروتکل OVPN

اگر به شکل ۷-۱۹٤ و قسمت Certificate توجه کنید علامت‌هایی را مشاهده می‌کنید که قبل از Certificate ایجاد شده‌اند که مربوط به سرویس‌هایی است که بر روی این گواهینامه‌ها فعال شده است.



شکل ۷- ۱۹۴ پروتکل OVPN

در ادامه کار باید از گواهینامه‌های CA و Client یک خروجی تهیه کنیم که این کار را هم با دستور زیر انجام می‌دهیم، توجه داشته باشید برای گواهینامه‌ی کلاینت حتماً باید یک رمز ایجاد کنیم تا در هنگام متصل شدن به سرور از این رمز استفاده کنیم.

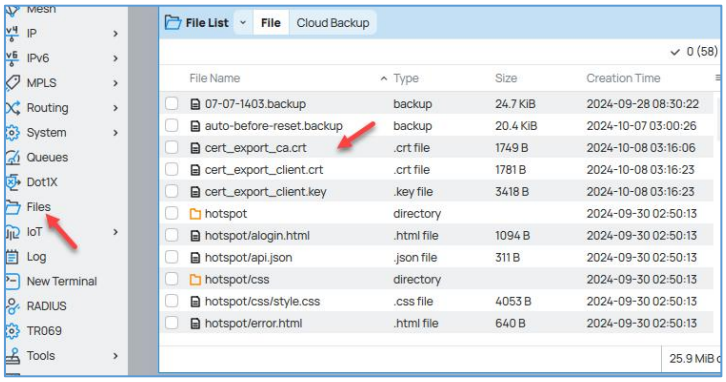
/certificate

export-certificate ca export-passphrase=""

www.takbook.com

export-certificate client export-passphrase=12345678

همان‌طور که در شکل ۷-۱۹۵، مشاهده می‌کنید دستورات مورد نظر به درستی اجرا شده است و فایل‌های مورد نظر در قسمت Files ایجاد شده‌اند، هر سه فایل را انتخاب و بر روی Download کلیک کنید و آنها را در یک جای مشخص ذخیره کنید.



شکل ۷- ۱۹۵ پروتکل OVPN

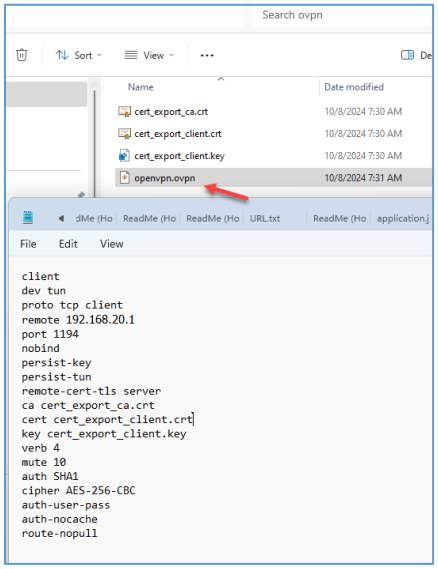
در ادامه کار باید یک فایل Config مربوط به OVPN را به این سه گواهینامه اضافه کنیم و ویرایش آن را طبق نام این گواهینامه‌ها انجام دهیم، برای این کار اطلاعات زیر را در نظر بگیرید، در تنظیمات زیر باید به جای 192.168.20.1 آدرس روتر میکروتیک را وارد کنید، البته اگر از بیرون میخواهید به روتر متصل شوید باید آدرس استاتیک خریداری شده را وارد کنید، در قسمت Port هم باید پورت پیش‌فرض 1194 را اگر از قبل تغییر نداده باشید وارد کنید، در سه قسمت وسط باید نام دقیق گواهینامه خود را وارد کنید.

```
client
dev tun
proto tcp client
remote 192.168.20.1
port 1194
nobind
persist-key
persist-tun
remote-cert-tls server
ca cert_export_ca.crt
cert cert_export_client.crt
key cert_export_client.key
verb 4
mute 10
auth SHA1
cipher AES-256-CBC
auth-user-pass
```

www.takbook.com

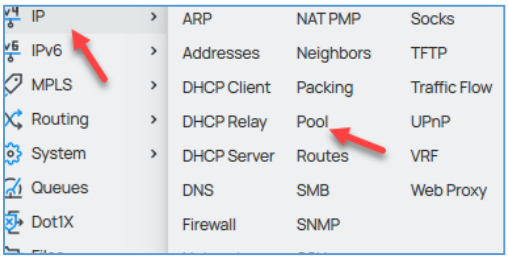
auth-nocache
route-nopull

بعد از انجام مراحل بالا فایل را با پسوند ovpn ذخیره کنید که شکل ۷-۱۹۶ به صورت زیر خواهد بود.



شکل ۷- ۱۹۶ پروتکل OVPN

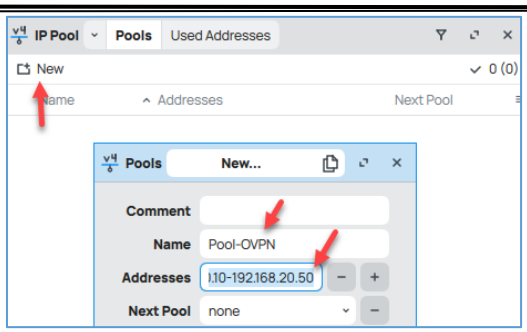
بعد از انجام مراحل بالا و آماده شدن فایل باید وارد میکروتیک شویم و چند کار دیگر را انجام دهیم، اولین کاری که انجام می‌دهیم ایجاد Pool برای کاربرانی است که از طریق Ovpn می‌خواهند به شبکه وصل شوند و وقتی می‌خواهند وصل شوند باید یک IP دریافت کنند، برای این کار طبق شکل ۷-۱۹۷، وارد IP و بعد Pool شوید.



شکل ۷- ۱۹۷ پروتکل OVPN

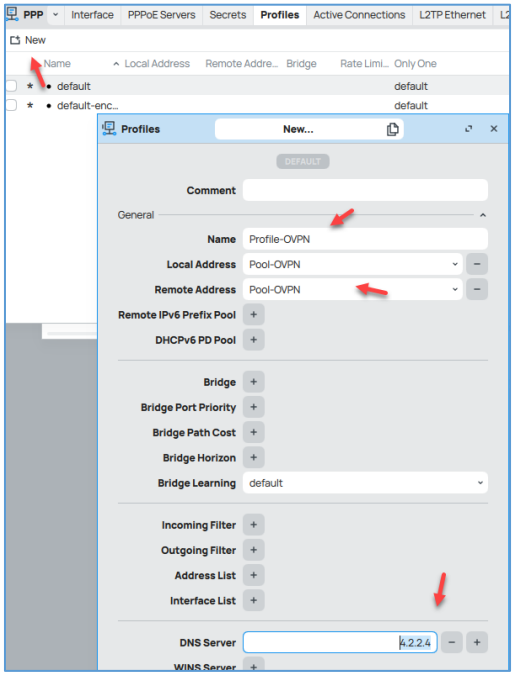
در شکل ۷-۱۹۸، یک رنج برای Pool خود وارد کنید و در قسمت Name یک نام دلخواه وارد کنید و در قسمت Address باید یک رنج آدرس وارد کنید، بهتر است که یک رنج در آدرس شبکه‌ی داخلی خود وارد کنید مثلاً 192.168.20.10 تا 192.168.20.50 و بر روی OK کلیک کنید.

www.takbook.com



شکل ۷- ۱۹۸ پروتکل OVPN

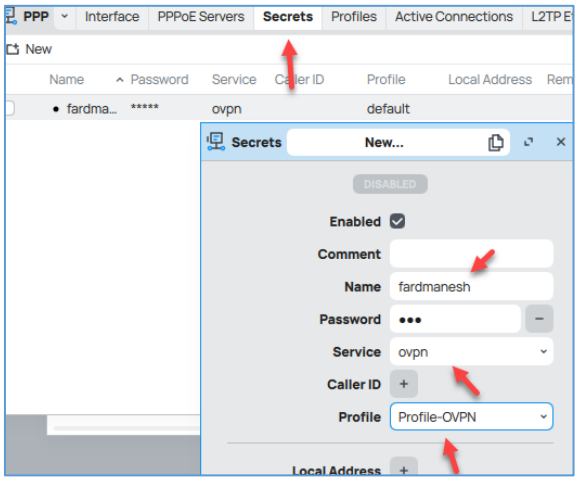
در ادامه کار باید یک Profile ایجاد کنیم و Pool بالا را به آن متصل کنیم، برای این کار به مانند شکل ۷-۱۹۹، بر روی PPP کلیک کنید و در صفحه‌ی باز شده بر روی New کلیک کنید در پنجره باز شده طبق شکل ۷-۱۹۹، باید یک نام به دلخواه وارد کنید و در قسمت آدرس هر دو را همان Pool که با هم ایجاد کردیم انتخاب کنید، توجه داشته باشید آدرس Local را می‌توانید یک آدرس ثابت بنویسید و آدرس Remote که مهم است را بر روی Pool قرار دهید، در قسمت DNS اگر نیاز دارید کاربران به شبکه داخلی مانند پرتال داخلی دسترسی داشته باشند باید آدرس DNS داخلی سازمان خود را وارد کنید و اگر این چنین نیست می‌توانید آدرس DNS عمومی را وارد کنید.



شکل ۷- ۱۹۹ پروتکل OVPN

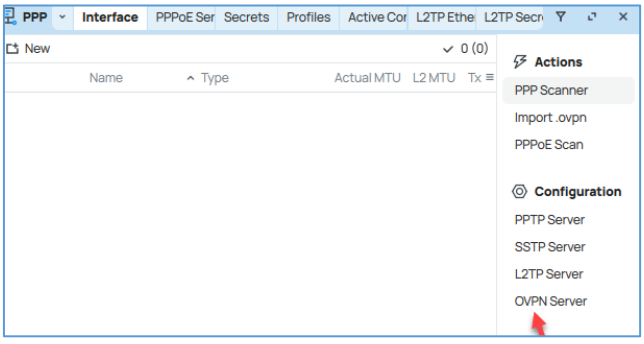
www.takbook.com

بعد از ایجاد Profile باید نام کاربری و رمزی برای سرویس OVPN ایجاد کنیم و به این Profile متصل کنیم، برای اینکار طبق شکل ۷-۲۰۰، در همان صفحه‌ی PPP گزینه‌ی Secrets را انتخاب کنید و بر روی New کلیک کنید، و در قسمت Name نام کاربری خود را وارد و در قسمت Password هم رمز عبور خود را وارد کنید، در قسمت Service هم باید سرویس OVPN را انتخاب کنید و در قسمت Profile هم گزینه‌ی Profile-OVPN که با هم ایجاد کردیم را انتخاب کنید و بر روی OK کلیک کنید.



شکل ۷- ۲۰۰ پروتکل OVPN

در آخر هم باید سرویس OVPN را فعال کنیم، برای این کار طبق شکل ۷-۲۰۱، در PPP وارد تب Interface شوید و بر روی OVPN Server کلیک کنید.

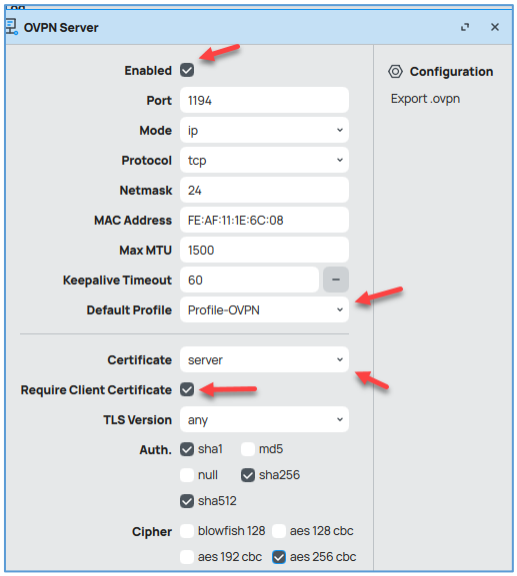


شکل ۷- ۲۰۱ پروتکل OVPN

در شکل ۷-۲۰۲، باید تیک گزینه‌ی Enable را انتخاب کنید تا سرویس فعال شود، در قسمت Profile هم باید همان Profile را انتخاب کنیم، در قسمت Certificate باید گواهینامه Server را انتخاب کنید و تیک زیری

www.takbook.com

آن را هم بزنید تا گواهینامه حتماً از کاربر درخواست شود، در قسمت Auth و Chiper دقیقاً به مانند تصویر عمل کنید تا ارتباط با مشکل روبرو نشود.

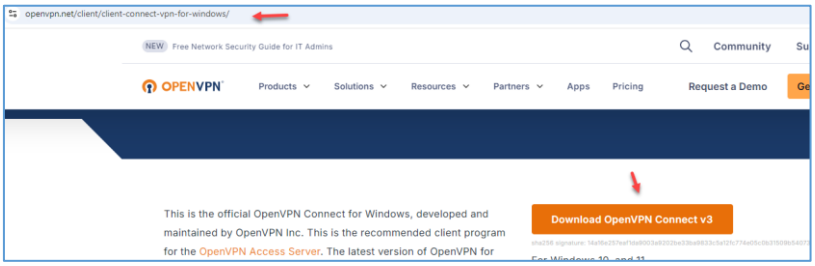


شکل ۷- ۲۰۲ پروتکل OVPN

بعد از این کار همه چیز برای ارتباط با OVPN فراهم است و فقط باید نسخه‌ی کلاینت آن را دانلود و بر روی سیستم عامل خود نصب کنید، همان‌طور گفتیم برای سیتم عاملا های مختلف نسخه OVPN وجود دارد که در این قسمت نسخه‌ی ویندوز را از لینک زیر دانلود می‌کنیم:

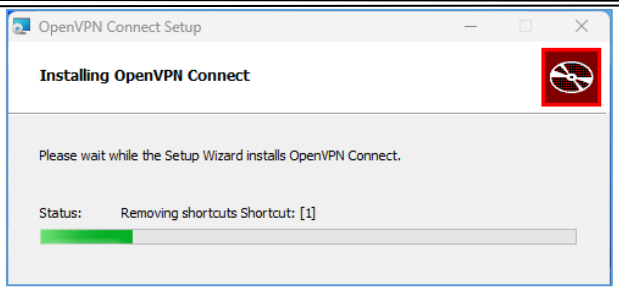
https://openvpn.net/client/client-connect-vpn-for-windows/

در شکل ۷-۲۰۲، بر روی Download کلیک کنید و فایل مورد نظر را دانلود کنید.



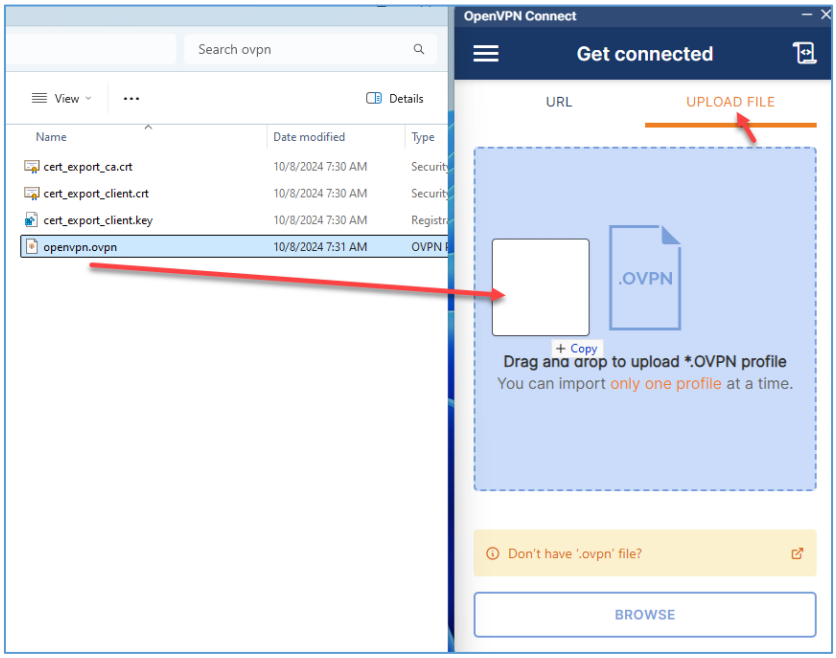
شکل ۷- ۲۰۲ پروتکل OVPN

www.takbook.com



شکل ۷- ۲۰۳ پروتکل OVPN

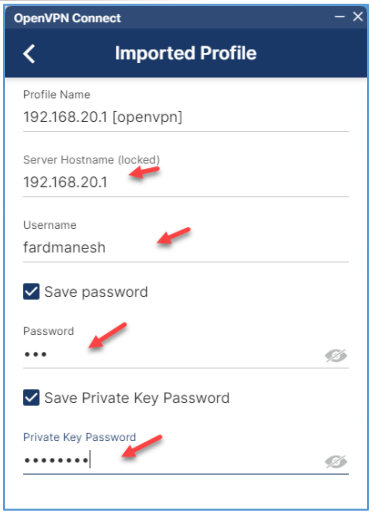
بعد از نصب فایل مورد نظر را اجرا کنید و به مانند شکل ۷-۲۰٤، به تب Upload File بروید و فایل با پسوند ovpn را بکشید و در قسمت مورد نظر رها کنید، یا اینکه فایل را در مسیر مشخص باز کنید.



شکل ۷- ۲۰۴ پروتکل OVPN

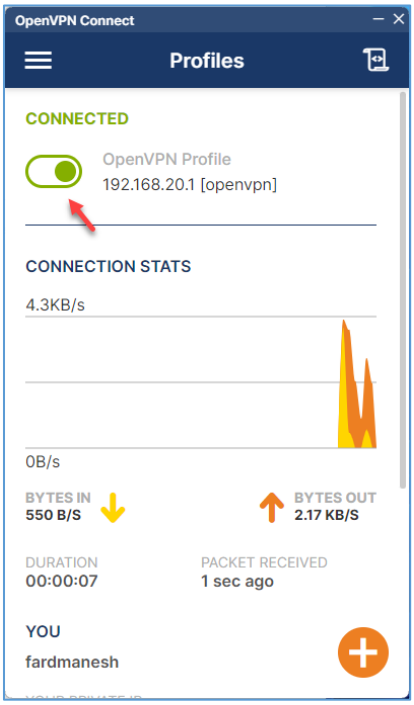
همان‌طور که در شکل ۷-۲۰۵ مشاهده می‌کنید، آدرس سرور به همراه نام کاربری مشخص شده است با کلیک بر روی Save password در هر دو قسمت باید رمز عبور کاربر را وارد کنید و در قسمت Private Key باید همان رمزی که در هنگام ایجاد کلید از گواهینامه (12345678) وارد کردیم در این قسمت وارد کنیم، بر روی Connect کلیک کنیم.

www.takbook.com



شکل ۷- ۲۰۵ پروتکل OVPN

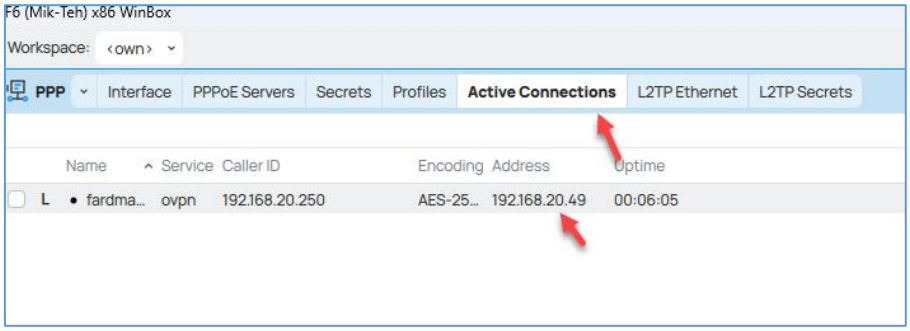
همان‌طور که در شکل ۷-۲۰۶، مشاهده می‌کنید با موفقیت توانستیم از طریق پروتکل OVPN به روتر میکروتیک متصل شویم.



شکل ۷- ۲۰۶ پروتکل OVPN

www.takbook.com

اگر به مانند شکل ۷–۲۰۷، وارد PPP و تب Active Connections شوید مشاهده خواهید کرد که کاربر مورد نظر به روتر متصل شده است و آدرسی که دریافت کرده را هم در همان رنجی است که تعریف کردیم.



شکل ۷- ۲۰۷ پروتکل OVPN

توجه داشته باشید اگر می‌خواهید از کاربر مورد نظر نام کاربری و رمز عبور دریافت نشود باید این خط را در فایل Config پاک کنید، که در شکل ۷–۲۰۸، این موضوع را مشاهده می‌کنید.

```
client
dev tun
proto tcp client
remote 192.168.20.1
port 1194
nobind
persist-key
persist-tun
remote-cert-tls server
ca cert_export_ca.crt
cert cert_export_client.crt
key cert_export_client.key
verb 4
mute 10
auth SHA1
cipher AES-256-CBC
auth-user-pass
auth-nocache
route-nopull
```

شکل ۷- ۲۰۸ پروتکل OVPN

۷–۳۳ راه‌اندازی SSTP در میکروتیک

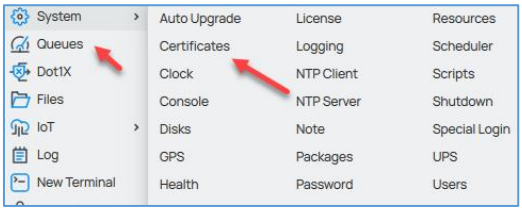
SSTP (Secure Socket Tunneling Protocol) یک پروتکل VPN است که توسط مایکروسافت توسعه داده شده است. SSTP ارتباطات امنی را برای انتقال داده‌ها بر بستر شبکه‌های عمومی فراهم می‌کند. این پروتکل از SSL/TLS برای ایجاد یک کانال امن استفاده می‌کند، که آن را به یک گزینه محبوب برای ایجاد اتصالات VPN امن تبدیل کرده است.

ویژگی‌ها و مزایای اصلی SSTP عبارتند از:

www.takbook.com

- امنیت بالا: SSTP از رمزگذاری SSL/TLS (پروتکل‌های مورد استفاده در HTTPS) استفاده می‌کند، که امنیت بسیار بالایی را فراهم می‌کند. این پروتکل به دلیل استفاده از گواهینامه‌های دیجیتال و رمزگذاری قوی، بسیار امن محسوب می‌شود.
- سازگاری با فایروال‌ها: SSTP به راحتی می‌تواند فایروال‌ها و NAT (Network Address Translation) را دور بزند. از آنجایی که ترافیک SSTP از پورت استاندارد ٤٤٣ (همان پورت HTTPS) استفاده می‌کند، فایروال‌ها به راحتی آن را مسدود نمی‌کنند.
- یکپارچگی با ویندوز: SSTP توسط مایکروسافت توسعه یافته است و به طور پیش‌فرض در سیستم‌عامل‌های ویندوز (از ویندوز ویستا به بعد) پشتیبانی می‌شود. این یکپارچگی استفاده از SSTP را برای کاربران ویندوز بسیار آسان می‌کند.
- پشتیبانی از احراز هویت قوی: SSTP می‌تواند از احراز هویت قوی مبتنی بر گواهینامه استفاده کند و به این ترتیب از حملات فیشینگ و دیگر حملات مشابه جلوگیری می‌کند.
- کاربرد در شبکه‌های محدود: از آنجایی که SSTP از پورت ٤٤٣ استفاده می‌کند، که معمولاً برای HTTPS باز است، می‌تواند در شبکه‌هایی که دسترسی به سایر پورت‌ها محدود است، مفید باشد.

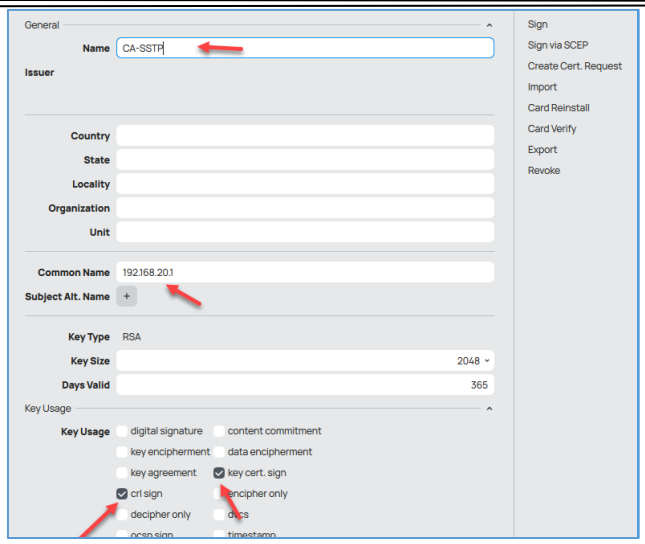
همان‌طور که گفتیم پروتکل SSTP روی پورت 443 یعنی SSL کار می‌کند و به خاطر همین باید یک گواهینامه برای آن ایجاد کنیم در کل به دو گواهینامه نیاز داریم، یکی CA و دیگری Server که با هم آنها را ایجاد می‌کنیم، برای شروع به مانند شکل وارد میکروتیک شوید و از قسمت System گزینه‌ی Certificate را انتخاب کنید



شکل ۷-۲۰۹ پروتکل SSTP

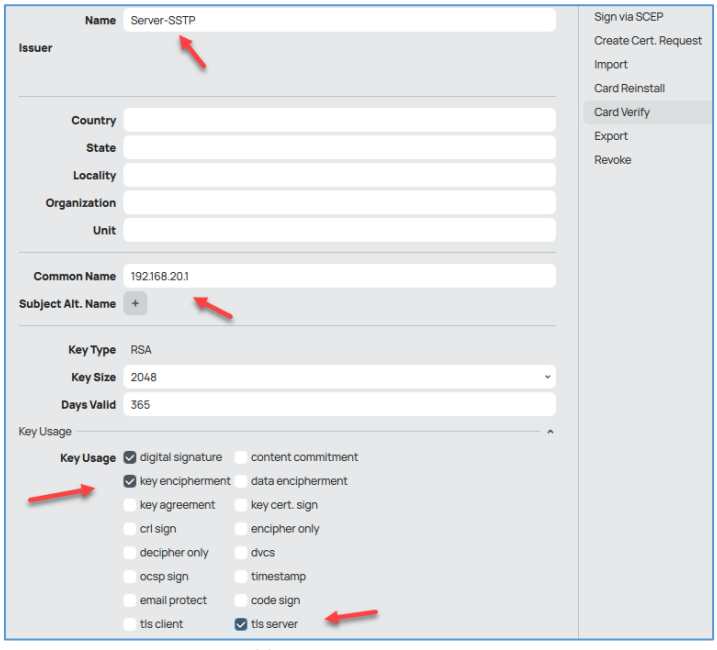
در ادامه کار طبق شکل ۷-۲۱۰، بر روی New کلیک کنید و در صفحه‌ی باز شده زیر در قسمت Name نام مورد نظر را وارد کنید که CA-SSTP وارد می‌کنیم، در قسمت Common Name که مهم است یا باید آدرس IP روتر میکروتیک را وارد کنید یا یک نام FQDN که به این آدرس اشاره می‌کند مانند sstp.expertroute.local، در قسمت Key Usage باید دو گزینه‌ی مورد نظر را انتخاب کنید و بر روی OK کلیک کنید.

www.takbook.com



شکل ۷- ۲۱۰ پروتکل SSTP

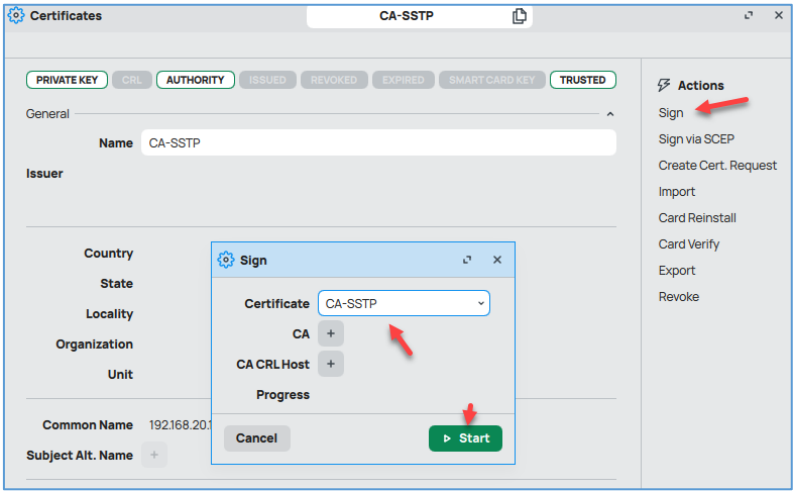
در ادامه به مانند شکل ۷-۲۱۱، یک گواهینامه دیگر برای قسمت Server ایجاد می‌کنیم که در شکل ۷-۲۱۱ این موضوع را مشاهده می‌کنید، فقط باید در قسمت Key Usage گزینه‌های مشخص شده را انتخاب کنید و بر روی OK کلیک کنید.



شکل ۷- ۲۱۱ پروتکل SSTP

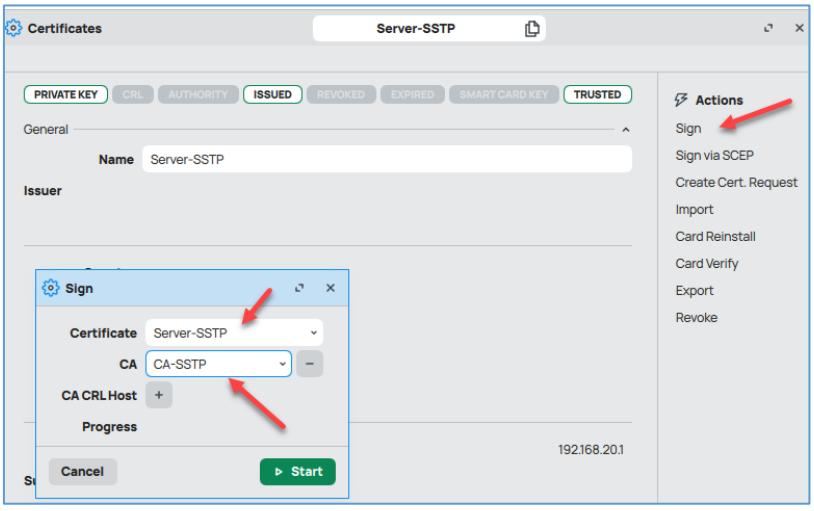
www.takbook.com

بعد از ایجاد دو گواهینامه مورد نظر باید دوباره آنها را باز کنیم و Sign کنیم تا در روتر فعال شوند، برای این کار به مانند شکل ۷-۲۱۲، اول از همه گواهینامه CA-SSTP را انتخاب کنید و بر روی sign کلیک کنید و در شکل باز شده بر روی Start کلیک کنید.



شکل ۷- ۲۱۲ پروتکل SSTP

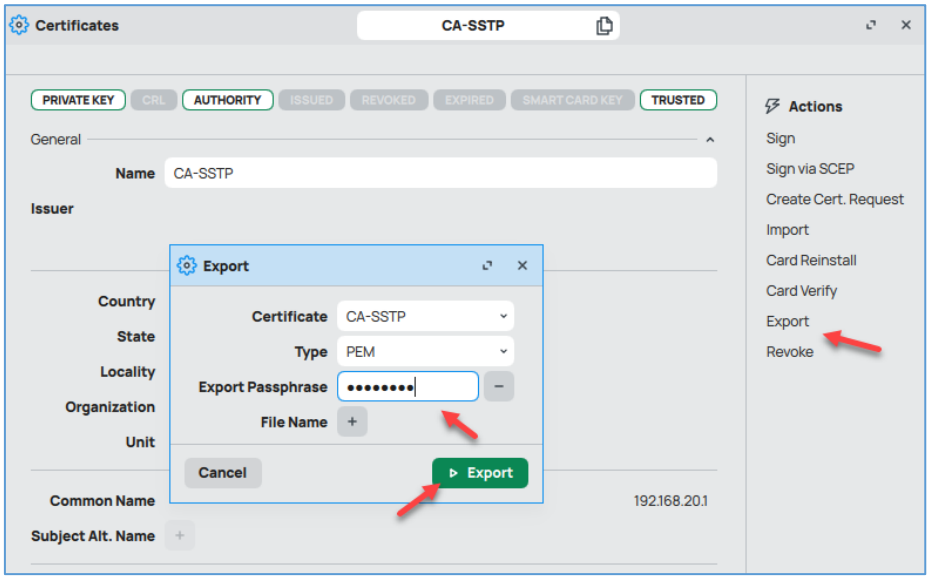
به مانند شکل ۷-۲۱۳ گواهینامه دوم را باز کنید و در قسمت CA باید CA-SSTP را که با هم ایجاد کردیم را انتخاب کنید و بر روی start کلیک کنید.



شکل ۷- ۲۱۳ پروتکل SSTP

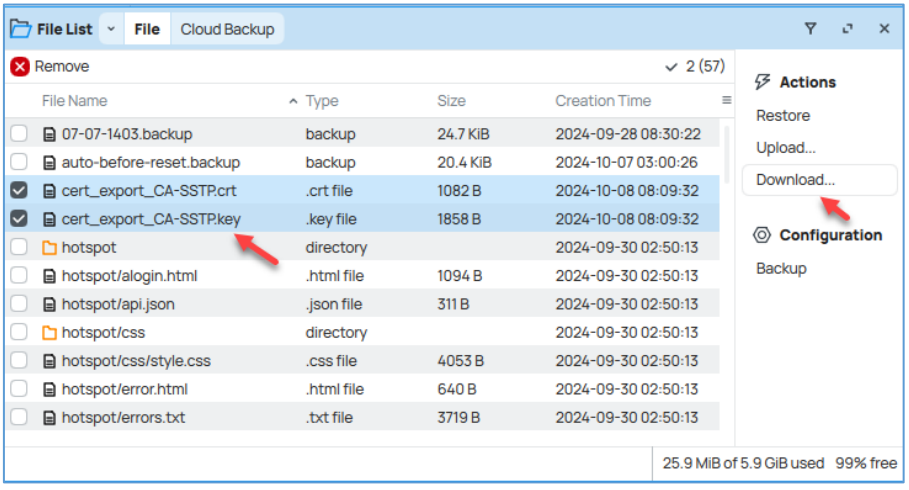
www.takbook.com

بعد از ایجاد گواهینامه باید از گواهینامه CA-SSTP یک خروجی بگیریم که به مانند شکل ۷-۲۱٤ بر روی Export کلیک کنید و در صفحه‌ی باز شده یک رمز عبور برای آن تعریف کنید که باید ۸ کاراکتر باشد.



شکل ۷- ۲۱۴ پروتکل SSTP

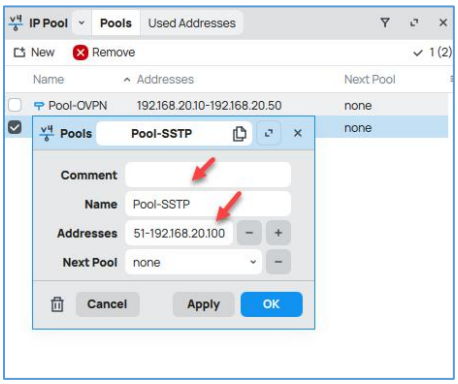
بعد از خروجی گرفتن وارد Files شوید و به مانند شکل ۷-۲۱۵، هر دو گزینه که یکی گواهینامه اصلی و دیگری فایل Key است را انتخاب کنید و بر روی Download کلیک کنید و در جای مناسب ذخیره کنید تا در ادامه از آنها استفاده کنیم.



شکل ۷- ۲۱۵، پروتکل SSTP

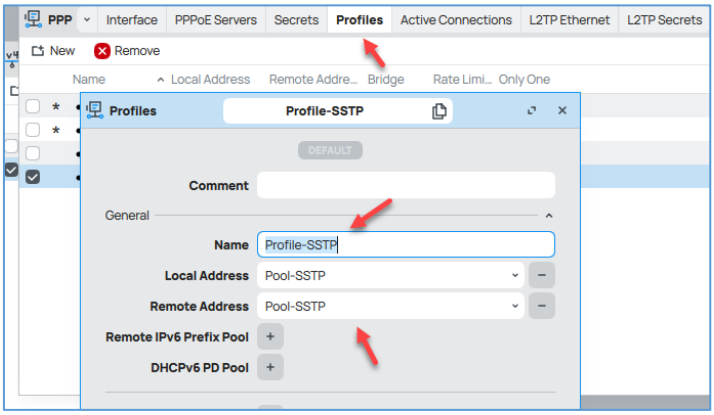
www.takbook.com

در ادامه دوباره وارد میکروتیک می‌شویم و به مانند شکل ۷-۲۱۶، یک Pool برای سرویس SSTP تعریف می‌کنیم تا کاربرانی که به روتر متصل می‌شوند یک رنج مشخص دریافت کنند، طبق شکل ۷-۲۱۵ بر روی New کلیک کنید و یک نام مشخص برای آن در نظر بگیرید و یک رنج IP برای آن مشخص کنید که در اینجا رنج 192.168.20.51 تا 192.168.20.100 در نظر می‌گیریم.



شکل ۷- ۲۱۶ پروتکل SSTP

در ادامه یک Profile ایجاد می‌کنیم و این Pool را به آن متصل می‌کنیم، طبق شکل ۷-۲۱۷، وارد PPP شوید و در تب Profile بر روی New کلیک کنید که در شکل زیر باید یک نام برای Profile خود وارد و در قسمت Local address و Remote Address هم Pool مورد نظر خود را وارد کنید، در قسمت DNS هم باید یک DNS عمومی یا داخلی وارد کنید که در اینجا 4.2.2.4 وارد می‌کنیم.

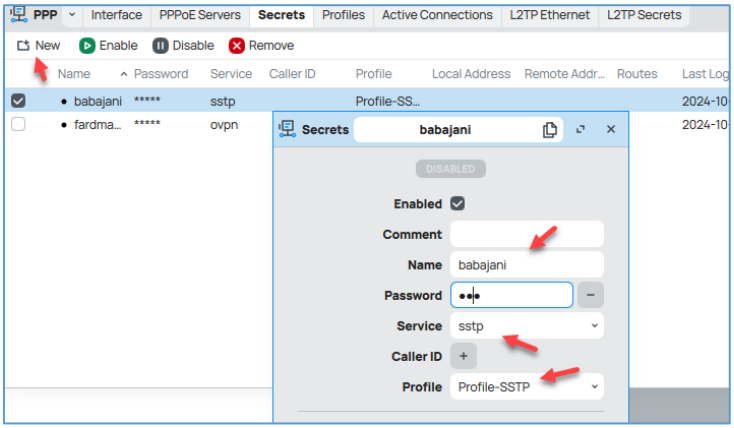


شکل ۷- ۲۱۷ پروتکل SSTP

در ادامه کار باید یک کاربر تعریف کنیم و این کاربر را به Profile مورد نظر متصل کنیم، برای این کار به مانند شکل ۷-۲۱۸، وارد تب Secret شوید و نام کاربری و رمز عبور کاربر مورد نظر خود را وارد کنید

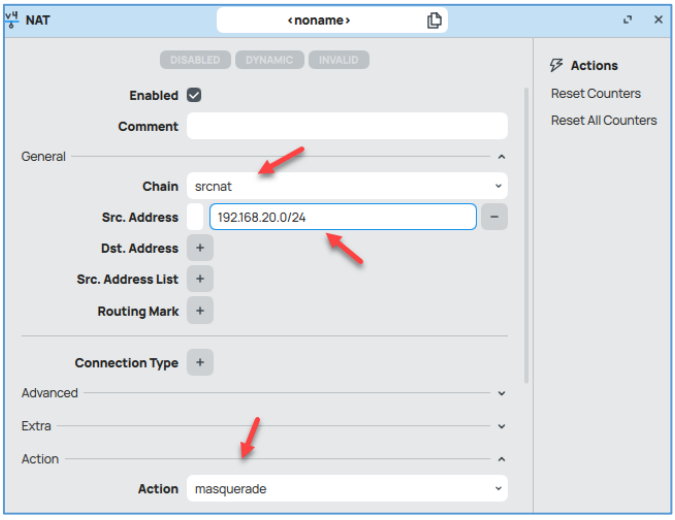
www.takbook.com

و در قسمت Service هم باید نام سرویس را SSTP در نظر بگیرید و در قسمت Profile هم باید Profile مربوط به SSTP را انتخاب کنید.



شکل ۷- ۲۱۸ پروتکل SSTP

بعد از انجام مراحل بالا باید برای کاربرانی که می‌خواهند از رنج IP که در Pool مورد نظر تعریف شده استفاده کنند، آدرس داخلی آنها را به سمت اینترنت NAT کنیم تا بتوانند به اینترنت دسترسی داشته باشند، برای این کار به مانند شکل ۷-۲۱۹، وارد Firewall شوید و در تب NAT بر روی New کلیک کنید و به صورت شکل ۷-۲۱۹، رنج آدرس شبکه‌ی داخلی را در قسمت SRC.Address وارد کنید و در قسمت Action گزینه‌ی Masquerade را انتخاب کنید تا آدرس‌های مورد نظر به سمت اینترنت ترجمه شوند.

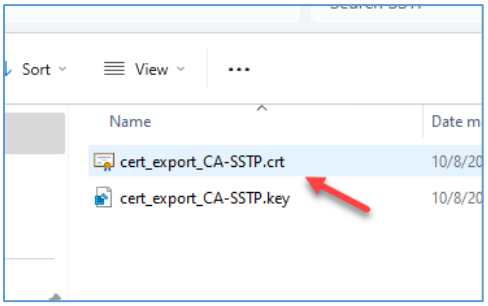


شکل ۷- ۲۱۹ پروتکل SSTP

www.takbook.com

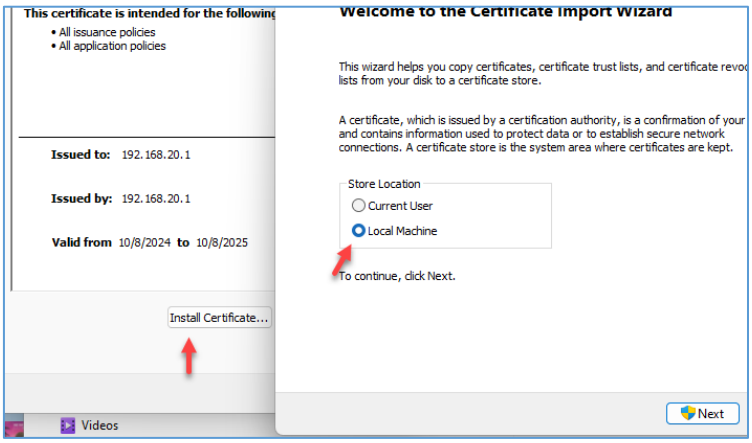
حالا کار ما با روتر میکروتیک تموم شده و باید وارد ویندوز شویم و SSTP Client را فعال کنیم و به روتر متصل شویم.

اولین کاری که باید انجام دهیم این است که گواهینامه‌ای که در روتر درست کردیم و از آن خروجی گرفتیم را در ویندوز اجرا می‌کنیم و آن را در ویندوز نصب می‌کنیم، به مانند شکل ۷-۲۲۰، بر روی گواهینامه مورد نظر دو بار کلیک کنید.



شکل ۷- ۲۲۰ پروتکل SSTP

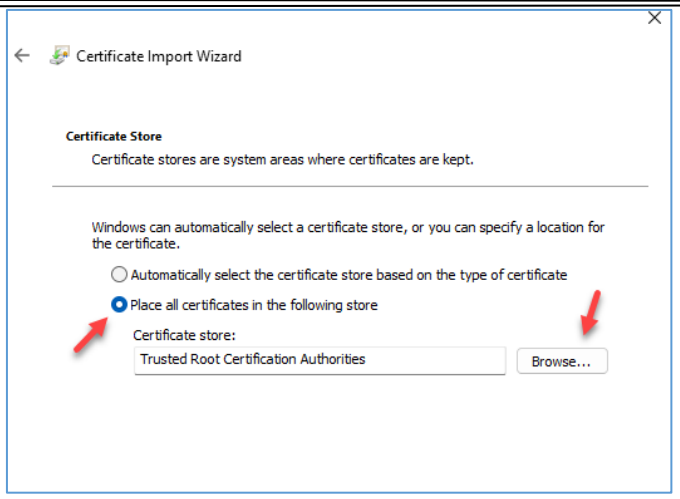
در شکل ۷-۲۲۱، بر روی Install Certificate کلیک کنید و در شکل باز شده گزینه‌ی Local Machine را انتخاب و Next کنید.



شکل ۷- ۲۲۱ پروتکل SSTP

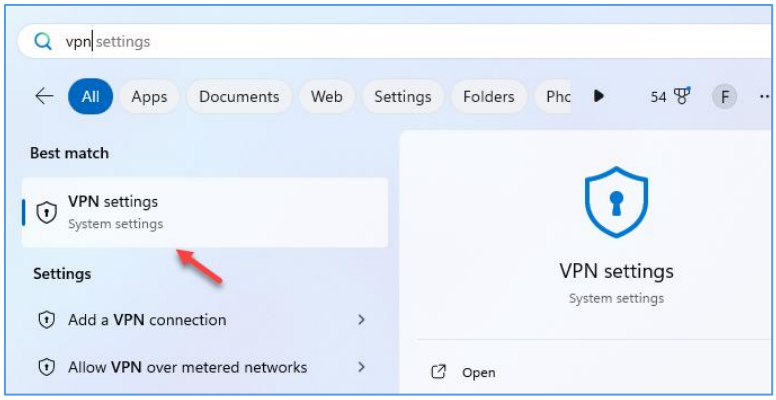
در شکل ۷-۲۲۲، گزینه‌ی Browse را انتخاب و گروه Trust Root Certification Authoriries را انتخاب کنید و Next و Finish کنید تا گواهینامه بر روی ویندوز نصب وشد.

www.takbook.com



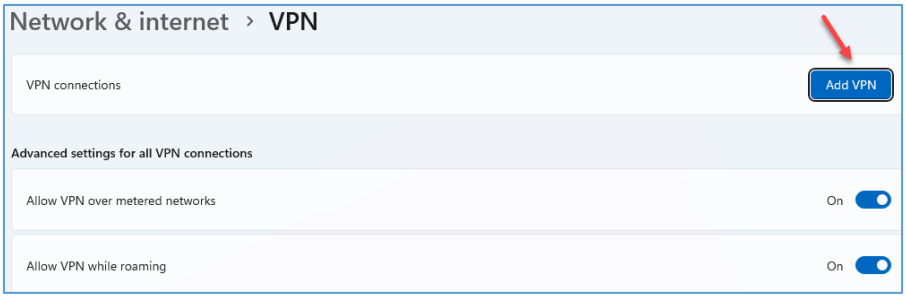
شکل ۷- ۲۲۲ پروتکل SSTP

به مانند شکل ۷–۲۲۳، در ویندوز 11 وارد تنظیمات VPN می‌شویم.



شکل ۷- ۲۲۳ پروتکل SSTP

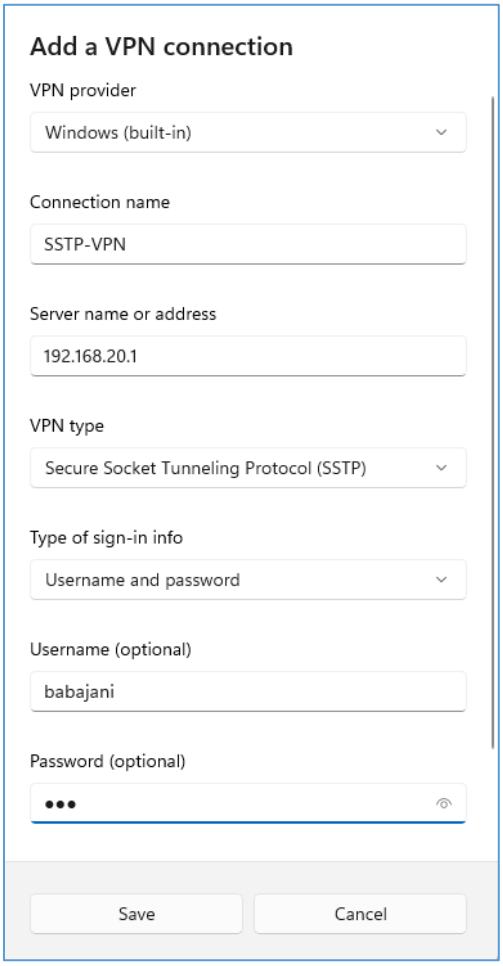
در ادامه کار طبق شکل ۷–۲۲٤، بر روی Add VPN کلیک کنید



شکل ۷- ۲۲۴ پروتکل SSTP

www.takbook.com

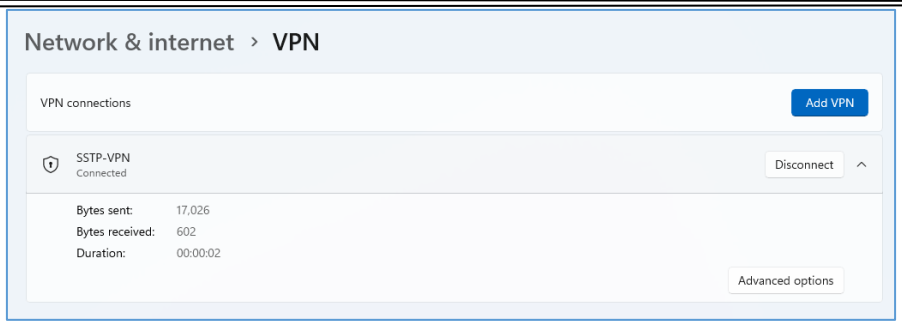
در شکل ۷-۲۲۵، باید یک نام برای VPN خود وارد کنید و در قسمت Address باید آدرس روتر میکروتیک خود که در گواهینامه هم وارد کردین اینجا وارد کنید، نوع پروتکل را SSTP در نظر بگیرید و نام کاربری و رمز عبور را وارد کنید.



شکل ۷- ۲۲۵ پروتکل SSTP

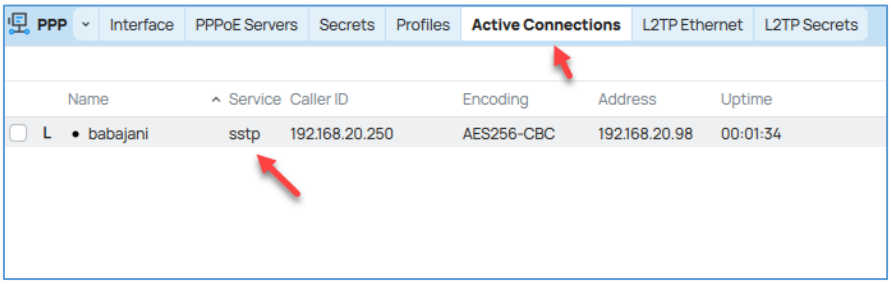
همان‌طور که در شکل ۷-۲۲٦، مشاهده می‌کنید کاربر مورد نظر توانست به درستی به سرور میکروتیک از طریق پروتکل SSTP متصل شود.

www.takbook.com



شکل ۷- ۲۲۶ پروتکل SSTP

اگر به میکروتیک هم نگاهی بیندازیم متوجه خواهید شد طبق شکل ۷-۲۲۷، کاربر مورد نظر با پروتکل SSTP متصل شده است.



شکل ۷- ۲۲۷ پروتکل SSTP

۷-۳٤ راه‌اندازی تانل 6to4

6to4 یکی از روش‌های رایج برای انتقال ترافیک IPv6 از طریق شبکه‌های مبتنی بر IPv4 است. این روش زمانی کاربرد دارد که شما هنوز از شبکه‌ای مبتنی بر IPv4 استفاده می‌کنید اما نیاز دارید که ترافیک IPv6 را از طریق این شبکه منتقل کنید. میکروتیک به عنوان یکی از تجهیزات محبوب در شبکه، از تونل 6to4 پشتیبانی می‌کند که به شما امکان می‌دهد به راحتی این انتقال را انجام دهید. مراحلی که باید برای این کار انجام دهید به صورت زیر لیست شده است.

۱- دریافت IP استاتیک
۲- ایجاد تانل 6to4
۳- ایجاد آدرس داخلی IPv6
۴- ایجاد IPv6 route
۵- ایجاد تانل GRE یا IPIPv6
۶- IPv4 برای تانل IPIPv6

www.takbook.com

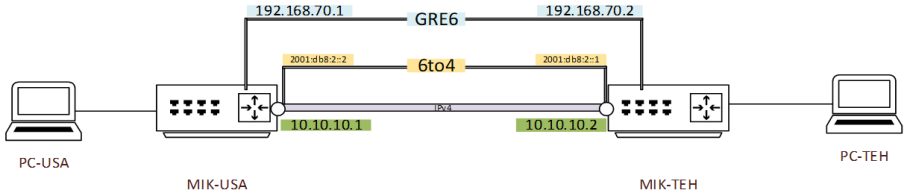
۷- روت IPv6 به سمت آدرس IPv6 تانل

۸- ایجاد منگل

۹- روت منکل به سمت تانل GRE6

به تصویر ۷-۲۲۷، توجه کنید، دو میکروتیک در دو نقطه‌ی مختلف داریم که می‌خواهیم بین آنها با استفاده از پروتکل 6to4 تانل بزنیم، آدرس‌های 10.10.10.0 به عنوان آدرس Static که در دنیای اینترنت اعتبار دارند برای شما در این مثال بررسی می‌کنیم که شما هم باید از سرویس دهنده‌ی خودتان این آدرس‌ها را درخواست کنید.

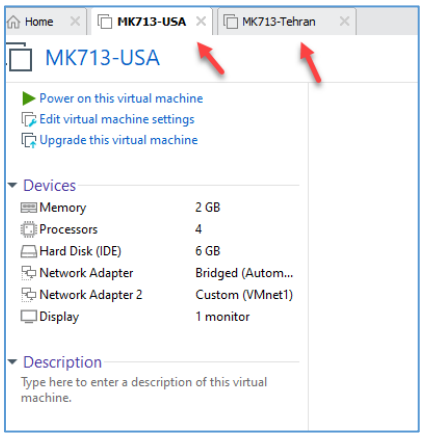
آدرس IPv6 که به صورت زرد رنگ هست خودمان می‌توانیم به دلخواه تعریف کنیم و همچنین آدرس آبی رنگ یعنی 192.168.70.0 را هم خودمان تعریف می‌کنیم که بر روی پروتکل GRE فعال می‌شود.



شکل ۷- ۲۲۷ تانل 6to4

تنظیم روتر MIK-Teh

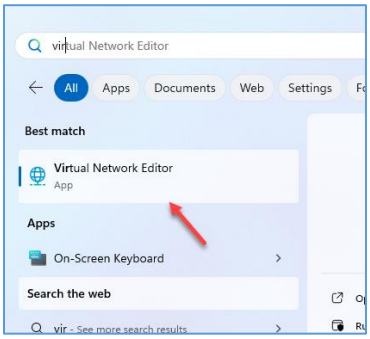
برای اینکه بر روی یک محیط آزمایشگاهی این کار را انجام دهیم، بر روی VMware Workstation دو تا میکروتیک ورژن ۷ را راه‌اندازی کردیم که شکل ۷-۲۲۸، نشان دهنده‌ی این دو میکروتیک است.



شکل ۷- ۲۲۸ تانل 6to4

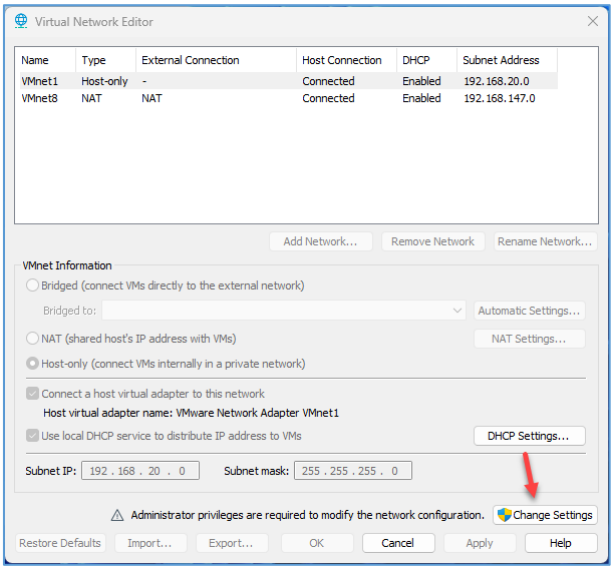
www.takbook.com

قبل از هر کاری باید کارت شبکه‌ی آنها را آماده کنیم، برای این کار وارد سرویس Virtual Network Editor شوید که شکل آن را در شماره ۷-۲۲۹ مشاهده می‌کنید.



شکل ۷- ۲۲۹ تانل 6to4

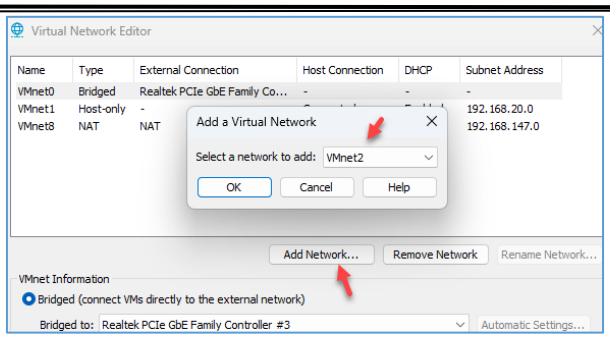
در شکل ۷-۲۳۰، بر روی Change Serrings کلیک کنید.



شکل ۷- ۲۳۰ تانل 6to4

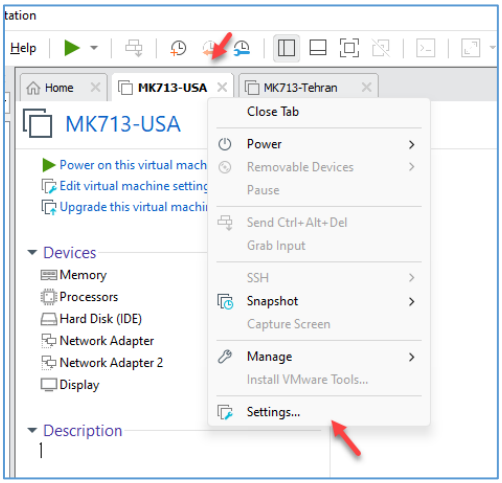
در شکل ۷-۲۳۱، دو کارت شبکه‌ی VMnet2 و VMnet3 را به لیست اضافه کنید، توجه داشته باشید این دو کارت شبکه باید از نوع Host Only باشند.

www.takbook.com



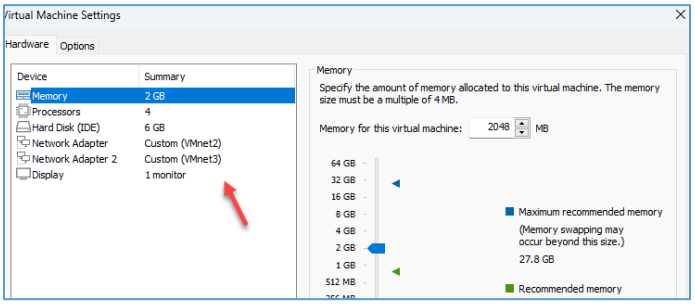
شکل ۷- ۲۳۱ تانل 6to4

در ادامه کار به مانند شکل ۷-۲۳۲، بر روی هر کدام از میکروتیک‌ها کلیک راست می‌کنیم و وارد Settings می‌شویم.



شکل ۷- ۲۳۲ تانل 6to4

به مانند شکل ۷-۲۳۳، با کلیک بر روی Add هر دو کارت شبکه را به لیست اضافه می‌کنیم، دقیقاً همین کار را برای میکروتیک دیگر (MIK-USA) انجام دهید.



شکل ۷- ۲۳۳ تانل 6to4

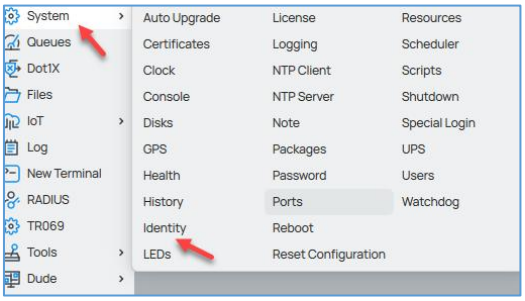
www.takbook.com

بعد از تنظیم کارت شبکه اول روتر میکروتیک MIK-THE را روشن می‌کنیم و از طریق WINBOX به آن متصل می‌شویم.

تنظیم روتر MIK-THE

۷-۳٤-۱ تغییر نام میکروتیک

برای شروع کار بهتر است برای هر کدام از میکروتیک‌های یک نام اختصاصی در نظر بگیریم که برای این کار به مانند شکل ۷-۲۳٤، باید وارد System/identity شوید.



شکل ۷- ۲۳۴ تانل 6to4

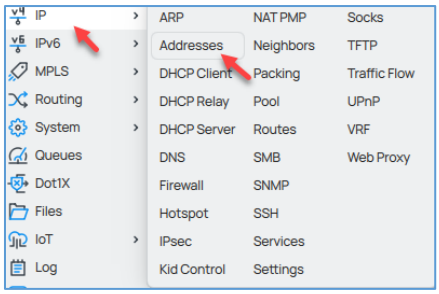
و نام روتر میکروتیک را به مانند شکل ۷-۲۳۵، تغییر دهید.



شکل ۷- ۲۳۵ تانل 6to4

۷-۳٤-۲ تنظیم آدرس IPv4 و IPv6

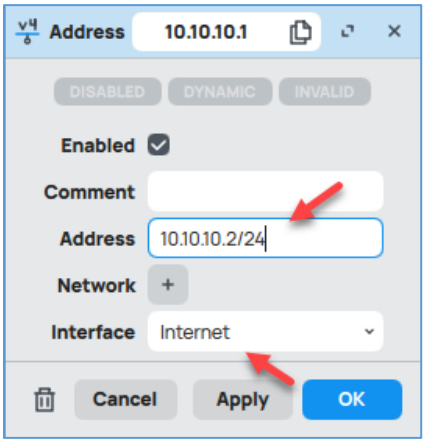
در ادامه کار باید آدرس IPv4 مربوط به شبکه‌ی داخلی و شبکه‌ی اینترنت را تعریف کنیم، برای انجام این کار به مانند شکل ۷-۲۳٦، باید وارد IP و بعد Address شوید.



شکل ۷- ۲۳۶ تانل 6to4

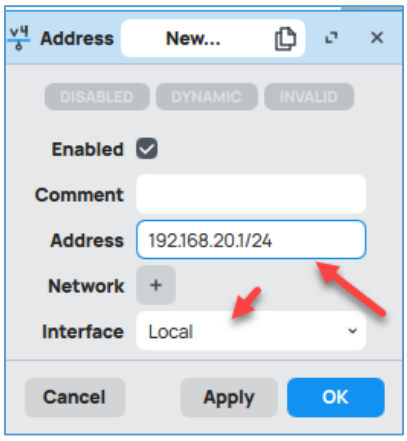
www.takbook.com

در شکل ۷-۲۳۷، باید آدرس هر کدام از کارت شبکه‌ها را وارد کنید، که در اینجا برای کارت شبکه‌ی اینترنت طبق سناریو آدرس 10.10.10.2 را در نظر می‌گیریم.



شکل ۷- ۲۳۷ تانل 6to4

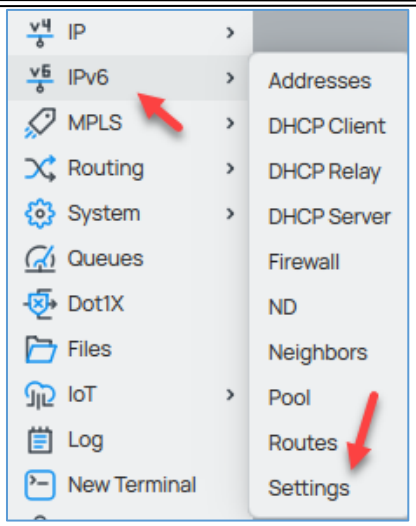
برای شبکه داخلی هم آدرس 192.168.20.1/24 را در نظر می‌گیریم.



شکل ۷- ۲۳۸ تانل 6to4

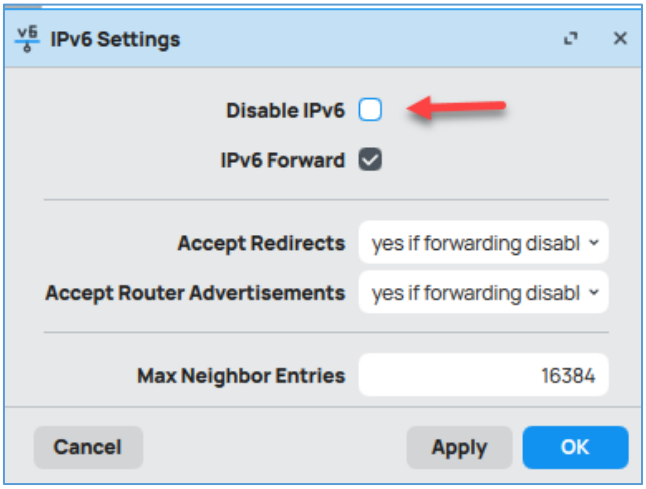
در ادامه‌ی کار باید آدرس IPv6 را فعال کنیم که به صورت پیش‌فرض این پروتکل غیر فعال است، برای انجام این کار به مانند شکل ۷-۲۳۹، از قسمت IPv6 گزینه‌ی Settings را انتخاب کنید.

www.takbook.com



شکل ۷- ۲۳۹ تانل 6to4

در شکل ۷-۲۴۰، باید تیک گزینه‌ی Disable IPv6 را بردارید تا این پروتکل بر روی روتر میکروتیک فعال شود در ادامه هم بعد از فعال کردن تانل 6to4 باید آدرس IPv6 را وارد کنیم.

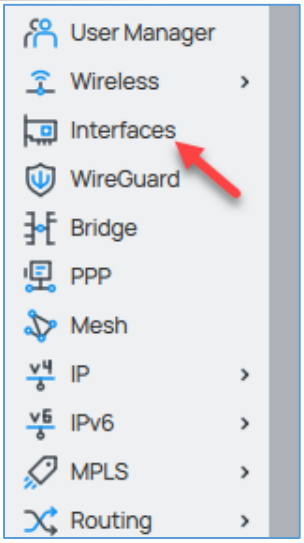


شکل ۷- ۲۴۰ تانل 6to4

۷-۳۴-۳ تانل 6to4

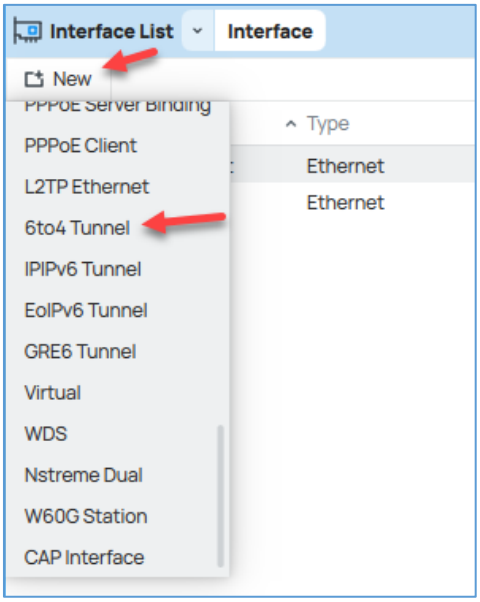
در ادامه باید تانل 6to4 را فعال کنیم، برای این کار طبق شکل ۷-۲۴۱، وارد Interface شوید.

www.takbook.com



شکل ۷- ۲۴۱ تانل 6to4

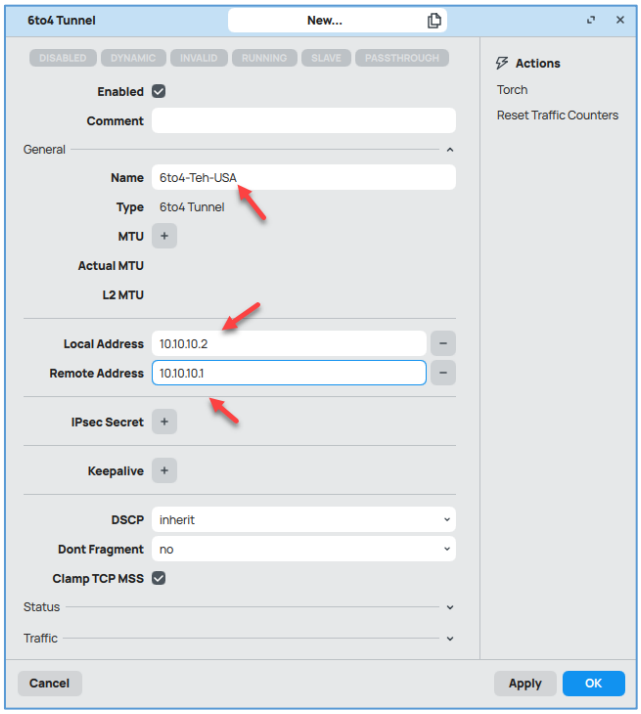
در شکل ۷-۲٤۲، بر روی New کلیک کنید و گزینه‌ی 6to4 را انتخاب کنید.



شکل ۷- ۲۴۲ تانل 6to4

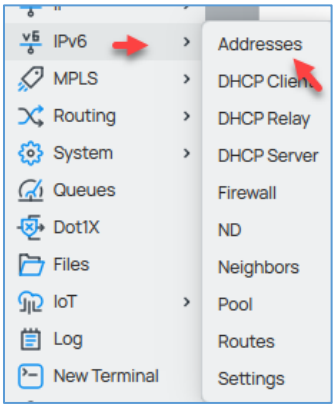
در شکل ۷-۲٤۳، باید نام مورد نظر خود را وارد کنید و در قسمت Local Address باید آدرس IP استاتیک یا معتبر خود را وارد کنید که در این سناریو 10.10.10.2 است و در قسمت Remote Address باید آدرس روتر میکروتیک که در جایی دیگر قرار دارد را وارد کنید که البته در این سناریو 10.10.10.1 است.

www.takbook.com



شکل ۷- ۲۴۳ تانل 6to4

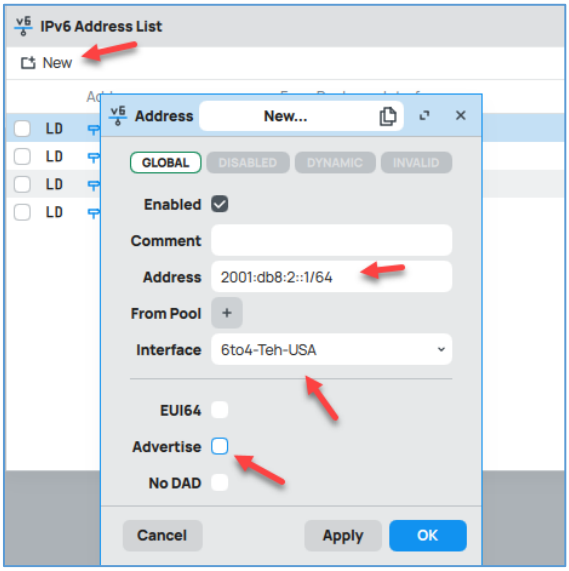
در ادامه کار بعد از فعال کردن تانل 6to4 باید آدرس IPv6 بر روی این تانل تعریف کنیم، برای این کار طبق شکل ۷-۲٤٤، از قسمت IPv6 گزینه‌ی Address را انتخاب کنید.



شکل ۷- ۲۴۴ تانل 6to4

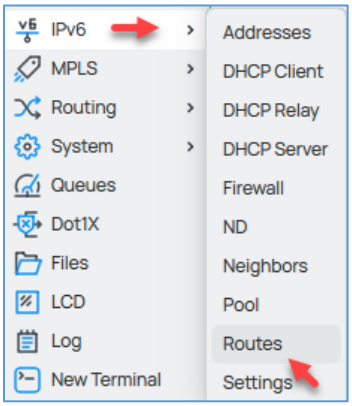
www.takbook.com

در شکل ۷-۲٤٥، در قسمت Address باید آدرس از نوع IPv6 وارد کنید که در اینجا آدرس 2001:db8:2::1/64 را وارد کردیم و در قسمت Interface هم باید تانل 6to4 را که راه‌اندازی کردیم را انتخاب کنید، تیک گزینه‌ی advertise را هم بردارید تا آدرس‌ها به درستی به مقصد ارسال شوند.



شکل ۷- ۲۴۵ تانل 6to4

در ادامه باید یک روت بنویسیم که تمام مقصدهای ناشناس IPv6 را به سمت تانل 6to4 ارسال کند، برای این کار به مانند شکل ۷-۲٤٦، از قسمت IPv6 گزینه‌ی Routes را انتخاب کنید.

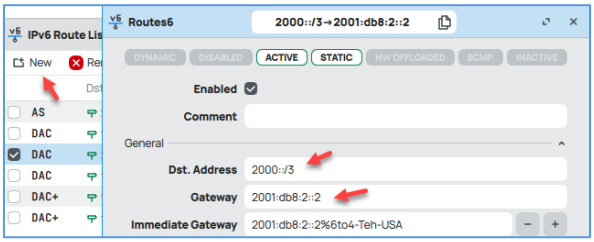


شکل ۷- ۲۴۶ تعریف Routes در IPv6

در شکل ۷-۲٤۷، و در قسمت Dst.Address باید آدرس2000::/3 که معادل 0.0.0.0 در IPv4 است را وارد کنید و در قسمت Gateway باید آدرس IPv6 روتر روبرو را وارد کنید، بعد از وارد کردن اطلاعات اگر بر

www.takbook.com

روی Apply کلیک کنید به صورت اتوماتیک تانل مورد نظر در قسمت Immediate Gateway مشخص می‌شود.

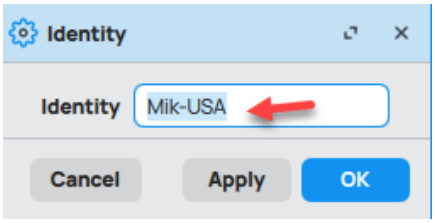


شکل ۷- ۲۴۷ تعریف Routes در IPv6

٤-٣٤-٧ تنظیم روتر MIK-USA

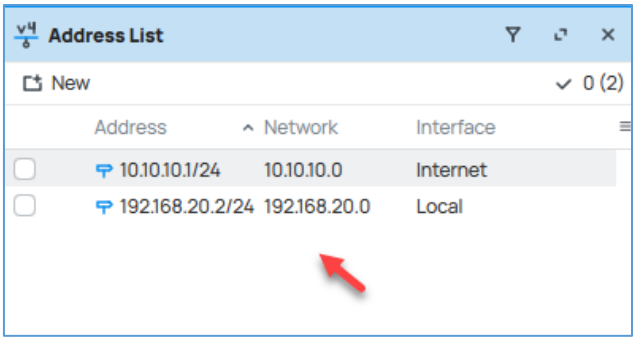
در ادامه کار باید روتر دوم خود را هم تنظیم کنیم، باید دقیقاً همان کارهایی را که برای روتر قبلی انجام دادیم در این قسمت هم انجام دهیم، برای سرعت بخشیدن به کار فقط عکس‌های مورد نیاز را در ادامه قرار می‌دهم.

تغییر نام روتر به MIK-USA به صورت شکل ۷-۲٤۸، است:



شکل ۷- ۲۴۸ تانل 6to4

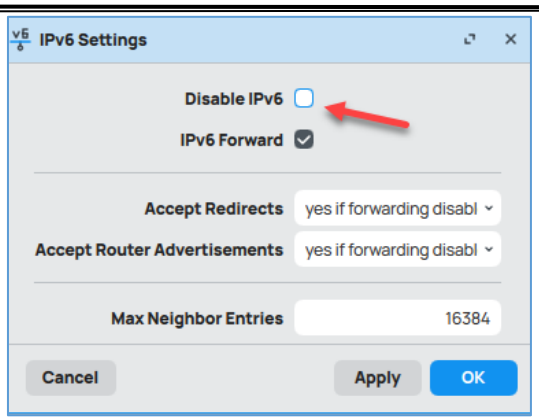
آدرس IPv4 را به مانند شکل ۷-۲٤۹، برای هر دو Interface وارد کنید:



شکل ۷- ۲۴۹ تانل 6to4

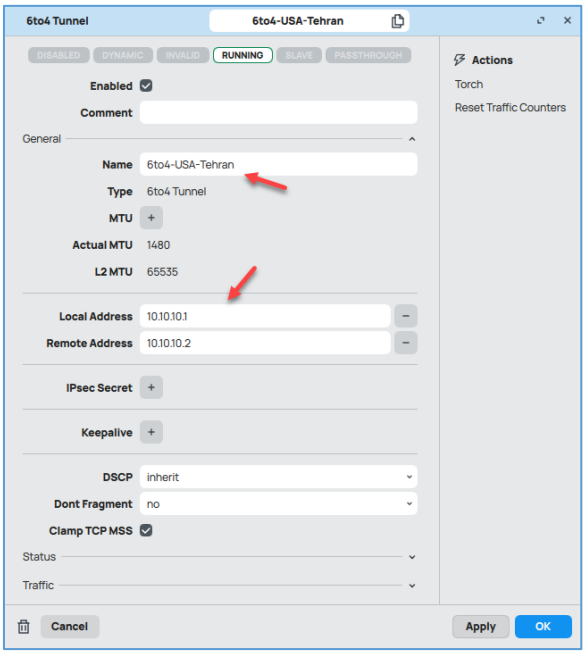
فعال کردن سرویس IPv6 به صورت شکل ۷-۲۵۰:

www.takbook.com



شکل ۷- ۲۵۰ تانل 6to4

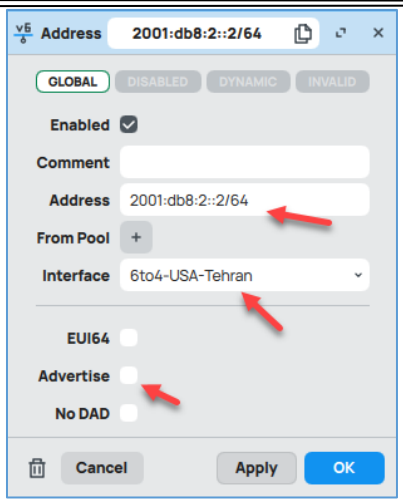
در ادامه هم به مانند شکل ۷-۲۵۱، باید تانل 6to4 را فعال کنیم، توجه داشته باشید در قسمت Local address باید آدرس همین روتر را وارد کنید و در قسمت Remote Address باید آدرس روتر Tehran را وارد کنید تا این دو همدیگر را ببینند.



شکل ۷- ۲۵۱ تانل 6to4

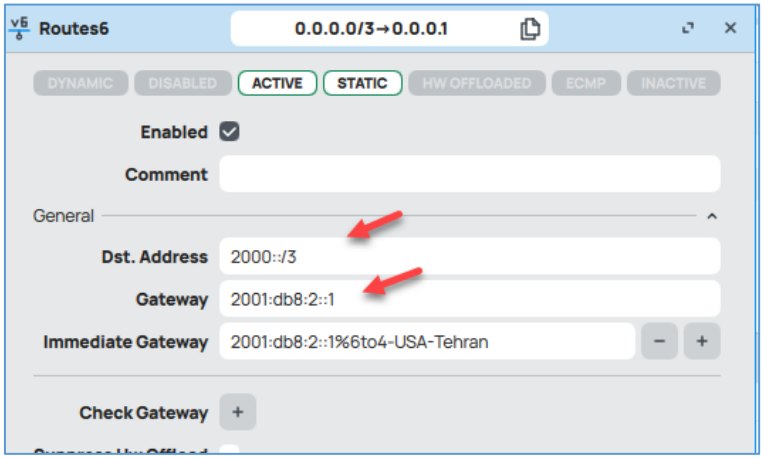
بعد از فعال کردن تونل باید آدرس IPv6 را بر روی این تونل تعریف کنیم که طبق شکل ۷-۲۵۲، این کار را انجام دهید.

www.takbook.com



شکل ۷- ۲۵۲ تانل 6to4

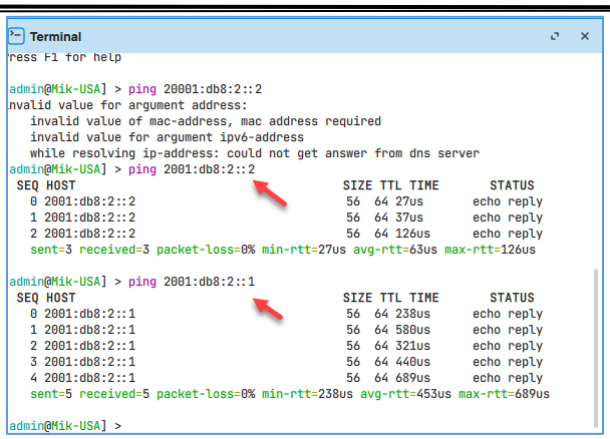
در ادامه باید یک روت به سمت این تانل ایجاد کنیم که برای این کار باید اطلاعات شکل ۷-۲۵۳ را وارد کنید.



شکل ۷- ۲۵۳ تانل 6to4

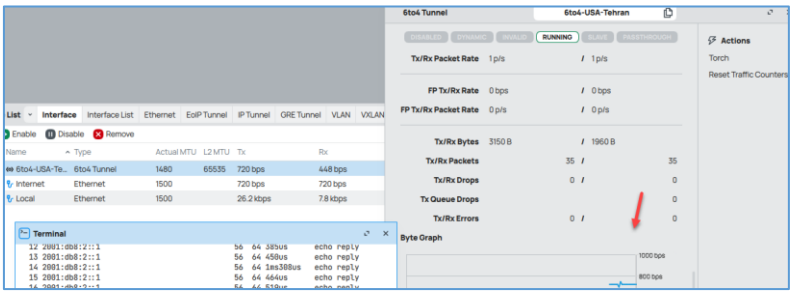
بعد از اتمام کار در هر دو روتر، می‌توانیم ارتباط بین دو روتر را از طریق تانل 6to4 تست بگیریم، برای این کار کافی است در یکی از روترها آدرس IPv6 روتر روبرو که در تانل قرار دارد را Ping بگیرید که در شکل ۷-۲۵٤، مشاهده می‌کنید که این عمل با موفقیت انجام شده است.

www.takbook.com



شکل ۷- ۲۵۴ تانل 6to4

اگر به مانند شکل ۷-۲۵۵، وارد خود تانل شوید مشاهده می‌کنید که پکت‌ها در حال عبور هستند و دریافت می‌شوند.

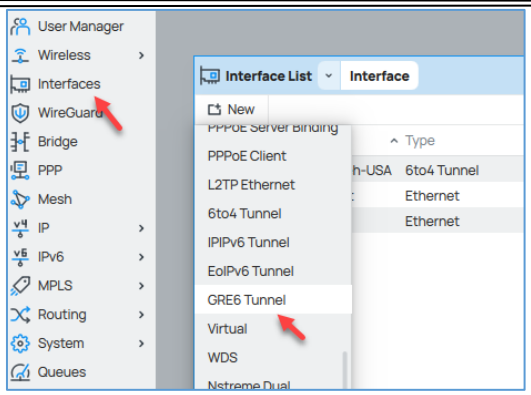


شکل ۷- ۲۵۵ تانل 6to4

۷-۳٤-۵ فعال‌سازی GRE6

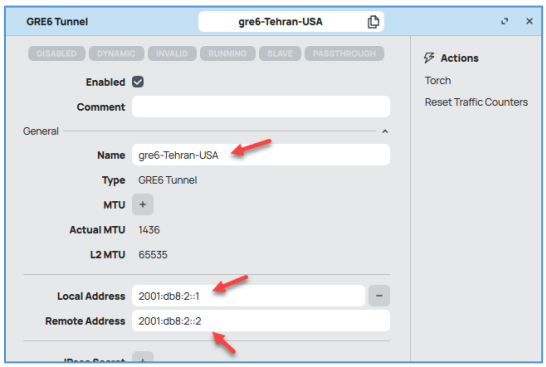
بعد از اینکه تانل 6to4 را راه‌اندازی کردیم می‌توانیم پروتکل GRE را از این تانل عبور دهیم و روی آن از آدرس IPv4 استفاده کنیم از این روش برای ایجاد تانل برای عبور ترافیک اینترنت به خارج از کشور استفاده می‌شود، یعنی اگر سرورتان خارج از ایران باشد می‌توانید ترافیک خود را به سمت سرور خارج ارسال کنید، برای تست این موضوع با هم این کار را انجام می‌دهیم، به مانند شکل ۷-۲۵۶، وارد Interfaces شوید و بر روی New کلیک کنید و گزینه‌ی GRE6 Tunnel را انتخاب کنید.

www.takbook.com



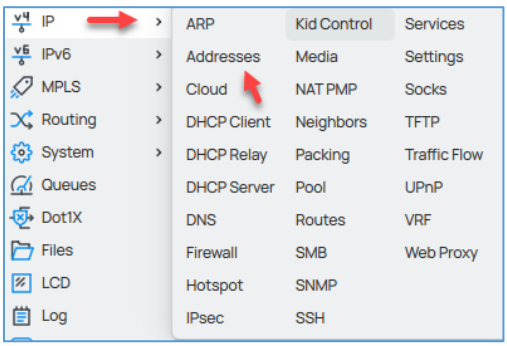
شکل ۷- ۲۵۶ فعال‌سازی GRE6

در شکل ۷–۲۵۷، یک نام به دلخواه خود وارد کنید و در قسمت Local Address باید آدرس IPv6 مربوط به همین روتر را وارد کنید و در قسمت Remote address هم آدرس IPv6 روتر روبرو را وارد کنید.



شکل ۷- ۲۵۷ فعال‌سازی GRE6

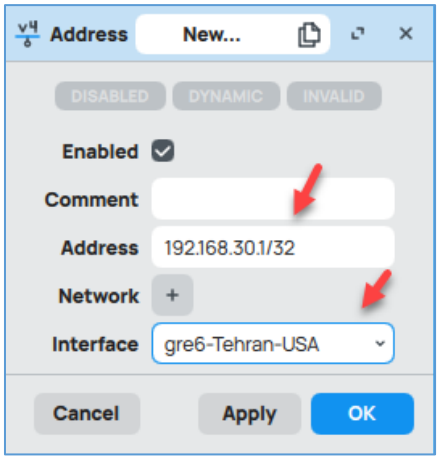
بعد از این کار باید یک آدرس IPv4 بر روی این تانل قرار دهیم تا بتوانیم از طریق IPv4 هم، با هم در ارتباط باشیم، برای این کار به مانند شکل ۷–۲۵۸، وارد IP Address شوید.



شکل ۷- ۲۵۸ فعال‌سازی GRE6

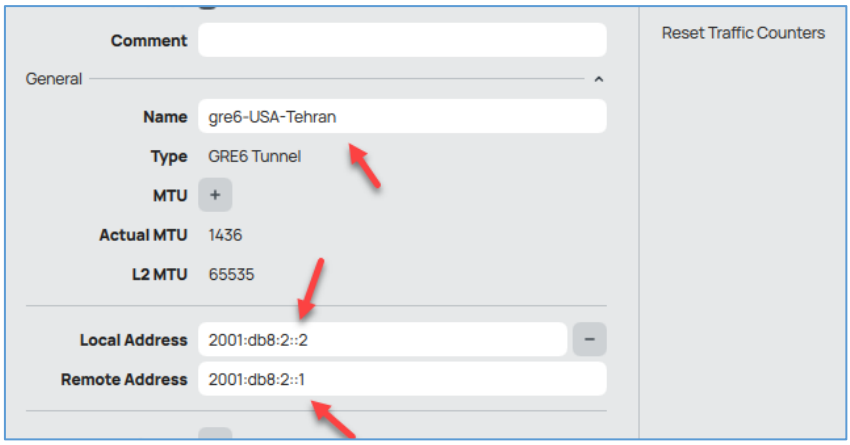
www.takbook.com

و بعد یک آدرس به صورت شکل ۷-۲۵۹ وارد کنید، فقط در قسمت Interface باید تانل GRE را انتخاب کنید تا آدرس IPv4 بتواند از آن رد شود.



شکل ۷- ۲۵۹ فعال‌سازی GRE6

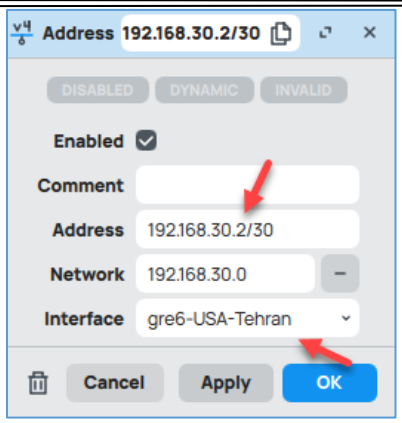
در ادامه کار باید وارد روتر دوم یعنی Mik-USA شویم و همین تنظیمات را در آن انجام دهیم، برای شروع به مانند شکل ۷-۲۶۰، وارد Interface شوید و تانل GRE6 را فعال کنید و اطلاعات را وارد کنید، در قسمت Local Address باید آدرس IPv6 روتر Mik-USA را وارد کنید و در قسمت Remote Address باید آدرس Mik-Teh را وارد کنید یعنی روتر روبرو.



شکل ۷- ۲۶۰ فعال‌سازی GRE6

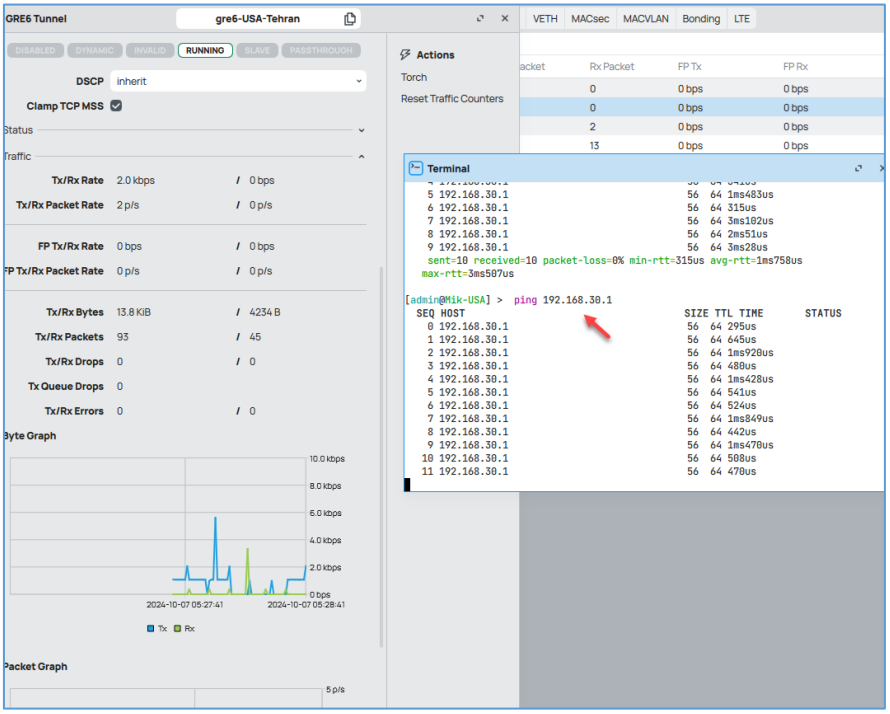
بعد از انجام کار قبلی باید یک آدرس بر روی این تانل تعریف کنیم که به صورت زیر وارد Ip address می‌شویم و به مانند شکل ۷-۲۶۱، آدرس 192.168.30.2 را در قسمت Interface وارد می‌کنیم.

www.takbook.com



شکل ۷- ۲۶۱ فعال‌سازی GRE6

در نهایت اگر روتر روبرو را پینگ بگیرید مشاهده می‌کنید اطلاعات IPv6 از طریق GRE ورژن 6 عبور می‌کند که شکل آن را در ۷-۲٦۲ مشاهده می‌کنید.

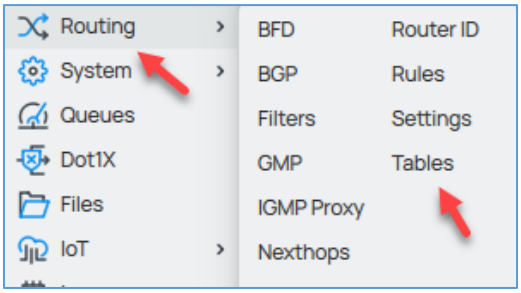


شکل ۷- ۲۶۲ فعال‌سازی GRE6

اگر بخواهید ترافیک آدرس‌های داخلی شبکه را از این تانل عبور دهید باید از منگل استفاده کنید، یعنی اینکه پکت‌ها را برچسب بزنیم و این پکت‌هایی که برچسب خورده‌اند را از یک مسیر مشخص خارج کنیم،

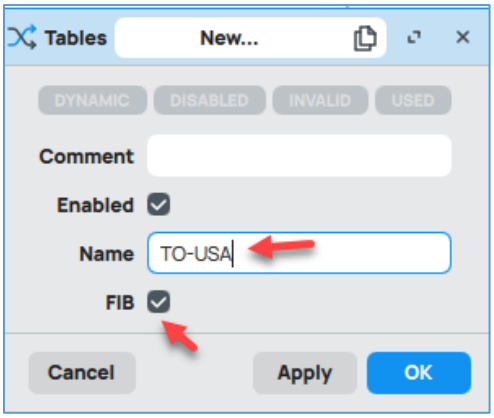
www.takbook.com

برای شروع نیاز داریم تا یک Routing Table برای آن ایجاد کنیم، به مانند شکل ۷-۲٦۳، وارد Routing و بعد Table شوید.



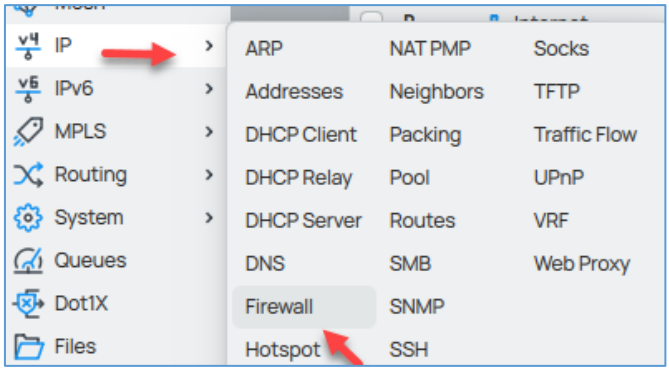
شکل ۷- ۲۶۳ فعال‌سازی GRE6

در شکل ۷-۲٦٤، یک نام وارد کنید و تیک گزینه مورد نظر را انتخاب کنید.



شکل ۷- ۲۶۴ فعال‌سازی GRE6

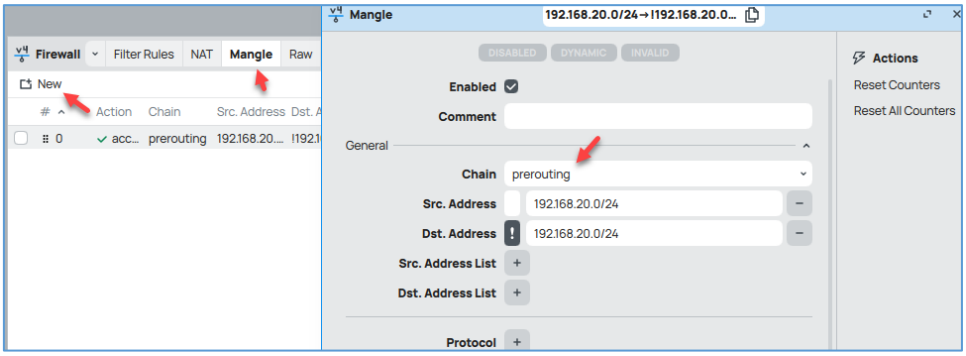
در ادامه برای فعال کردن Mangel باید به مانند شکل ۷-۲٦٥، وارد Firewall شوید.



شکل ۷- ۲۶۵ فعال‌سازی GRE6

www.takbook.com

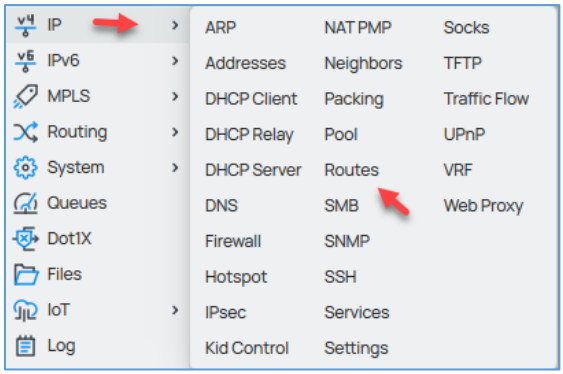
در ادامه کار طبق شکل ۷-۲۶۶، وارد تب Mangle شوید و بر روی New کلیک کنید و در صفحه‌ی باز شده در قسمت Chain گزینه‌ی Prerouting را انتخاب کنید و در قسمت Src.Address باید آدرس شبکه‌ی داخلی خود را وارد کنید تا تمام پکت‌های آنها برچسب گذاری شود و برای اینکه دوباره همین پکت‌ها به سمت شبکه داخلی برنگردد در قسمت Dst.Address باید دوباره همین شبکه را وارد کنید و علامت تعجب را بزنید تا صرف نظر کند.



شکل ۷- ۲۶۶ فعال‌سازی GRE6

در شکل ۷-۲۶۶، وارد قسمت Action شوید و در قسمت Action گزینه‌ی Markrouting را انتخاب کنید و در قسمت New هم همان Routing table را که با هم ایجاد کردیم را انتخاب کنید.

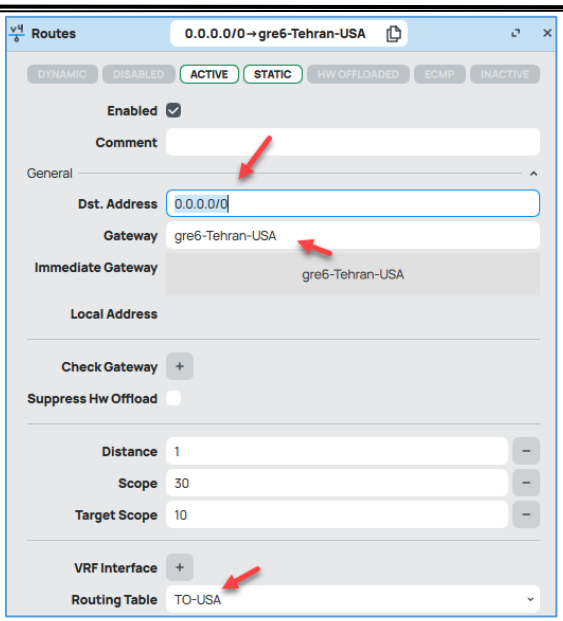
بعد از اینکه پکت‌ها را مارک کردیم باید آنها را به سمت تانل GRE روت کنیم، برای این کار طبق شکل ۷-۲۶۷، وارد Ip و بعد Routes شوید.



شکل ۷- ۲۶۷ GRE6

در شکل ۷-۲۶۸ و در قسمت Dst.Address باید آدرس 0.0.0.0/0 را وارد کنید و در قسمت Gateway باید نام دقیق تانل GRE را وارد کنید و در قسمت Routing Table حتما باید Table ایجاد کرده را انتخاب کنید و بر روی OK کلیک کنید، با این کار اطلاعات کاربران از این تانل عبور می‌کند.

www.takbook.com



شکل ۷- ۲۶۸ فعال‌سازی GRE6

۷-۳۵ راه‌اندازی پروتکل EOIP

پروتکل EOIP (مخفف Ethernet over IP) یکی از پروتکل‌های تونل‌زنی اختصاصی شرکت میکروتیک است که برای انتقال ترافیک لایه دوم (Ethernet) از طریق بستر IP طراحی شده است. این پروتکل به شما امکان می‌دهد شبکه‌های محلی (LAN) خود را از طریق شبکه‌های گسترده‌تری مانند اینترنت به یکدیگر متصل کنید، به گونه‌ای که دستگاه‌های موجود در این شبکه‌ها همانند یک شبکه محلی یکپارچه عمل کنند.

ویژگی‌های کلیدی پروتکل EOIP

- تونل‌سازی لایه دوم: EOIP به شما اجازه می‌دهد بسته‌های اترنت (Ethernet frames) را از طریق بستر IP (مثلاً اینترنت) انتقال دهید. این ویژگی برای مواردی که نیاز به گسترش یک شبکه LAN بین چندین مکان جغرافیایی وجود دارد بسیار مفید است.
- مجازی‌سازی شبکه‌ها: با استفاده از EOIP، می‌توانید به سادگی چندین شبکه فیزیکی را از طریق تونل‌های EOIP به یک شبکه مجازی واحد تبدیل کنید، به طوری که دستگاه‌های مختلف در مکان‌های مختلف انگار در یک شبکه محلی واحد قرار دارند.
- پشتیبانی از پروتکل‌های پیشرفته: این پروتکل می‌تواند به همراه تکنولوژی‌هایی نظیر VLAN و MPLS کار کند، و امکان ایجاد توپولوژی‌های پیچیده و بهینه‌سازی ترافیک شبکه را فراهم می‌کند.

www.takbook.com

- کاربردهای گسترده: EOIP برای ایجاد VPN، ارتباط بین دفاتر مختلف یک سازمان، اتصال بین شعب و حتی برای استفاده در سناریوهای افزونه‌ای (redundancy) در شبکه‌ها استفاده می‌شود.

نحوه عملکرد EOIP

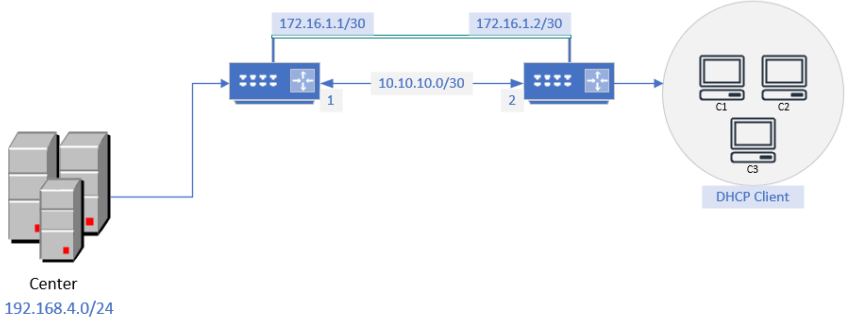
پروتکل EOIP با ایجاد یک تونل بین دو روتر میکروتیک کار می‌کند که این تونل بر بستر IP قرار دارد. بسته‌های اترنت از یک روتر وارد تونل EOIP شده و به روتر مقصد منتقل می‌شوند. در نتیجه، روترها می‌توانند بدون توجه به فاصله جغرافیایی، همانند شبکه‌ای یکپارچه و محلی به یکدیگر متصل شوند.

سناریوی کاربردی

فرض کنید سازمانی دارای دو دفتر در دو شهر مختلف است و قصد دارد این دو دفتر را به گونه‌ای به هم متصل کند که دستگاه‌های هر دو دفتر در یک شبکه محلی مشترک قرار بگیرند. با استفاده از EOIP، می‌توانید بین روترهای هر دو دفتر یک تونل EOIP ایجاد کنید و شبکه‌های LAN آنها را به هم متصل نمایید. در این حالت، همه دستگاه‌ها در هر دو دفتر انگار در یک شبکه فیزیکی واحد قرار دارند و می‌توانند به راحتی با یکدیگر ارتباط برقرار کنند.

برای شروع کار نیاز به دو روتر میکروتیک داریم که این دو روتر باید داری یک IP ثابت باشند تا بتوانیم در اینترنت به آنها دسترسی داشته باشیم، در پشت این روترها شبکه‌ی ما قرار دارید، یعنی به این صورت که در شعبه مرکزی شبکه اصلی قرار دارد و در شعبه های دیگر سیستم‌ها از طریق پروتکل EOIP به شبکه اصلی متصل می‌شوند و به راحتی می‌توانند مثلاً عضو دومین شبکه ما شوند.

فرض کنید یک شبکه در سازمان خود دارید که می‌خواهید یک شعبه دیگر در شهر دیگری راه‌اندازی کنید ولی آن شعبه از آدرس IP شما استفاده کند و تمام کلاینت‌های آن عضو دومین ما باشند و بدون مشکل کار کنند، در سناریو شکل۷-۲۶۹، دو شبکه مرکزی و یک شعبه داریم که بین آنها دو روتر میکروتیک وجود دارد که از طریق پروتکل تانل EOIP در لایه‌ی دوم و سوم به هم متصل می‌شوند و کلاینت‌هایی که در شعبه وجود دارند از طریق DHCP آدرس IP شبکه مرکزی را دریافت می‌کنند.

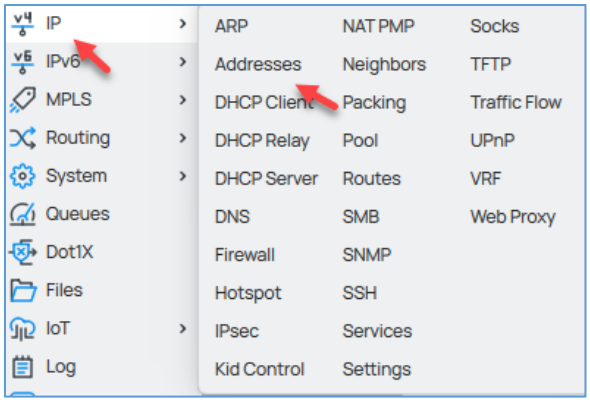


شکل ۷- ۲۶۹ پروتکل EOIP

www.takbook.com

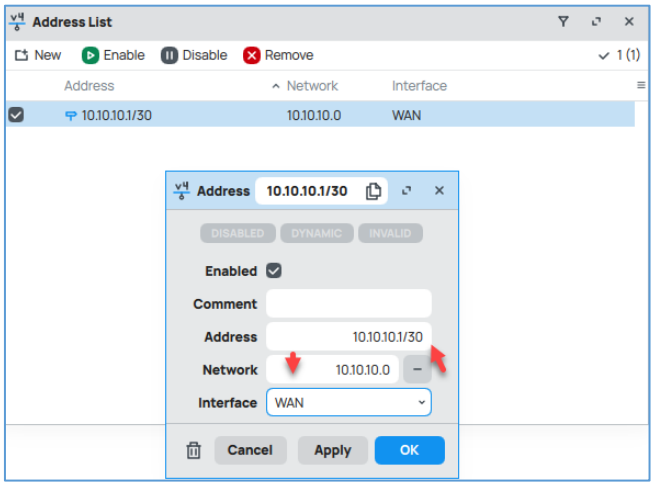
۷-۳۵-۱ تنظیم روتر مرکزی

بر روی روتر مرکزی دو کارت شبکه داریم که یکی به شبکه داخلی متصل می‌شود و دیگری هم از طریق اینترنت به شعبه متصل می‌شود، برای شروع طبق شکل ۷-۲۷۰، وارد IP و بعد Address شوید.



شکل ۷- ۲۷۰ پروتکل EOIP

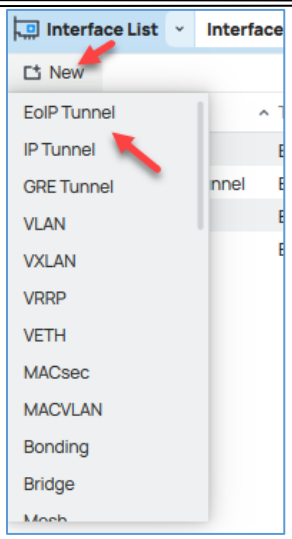
به مانند شکل ۷-۲۷۱، آدرس شبکه‌ی اینترنت را وارد می‌کنیم، توجه داشته باشید به جای این آدرس در دنیای واقعی باید از آدرس Public استفاده کنید.



شکل ۷- ۲۷۱ پروتکل EOIP

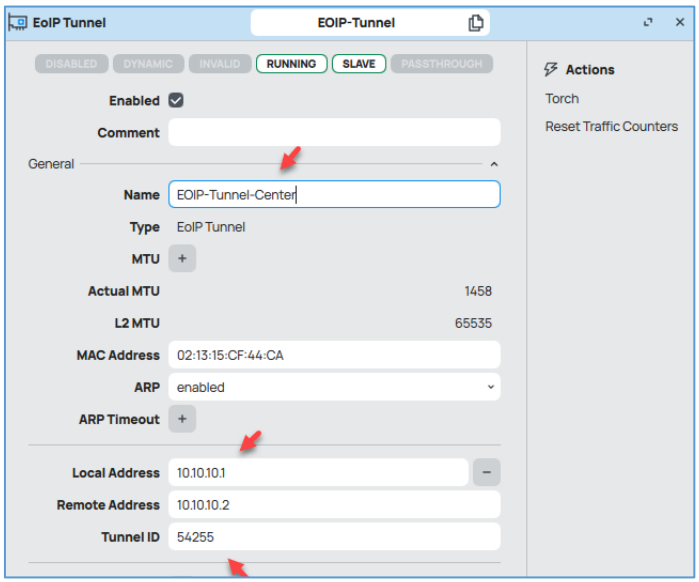
بعد از تعریف IP اینترنت باید وارد Interface شویم و تانل EOIP را فعال کنیم، به مانند شکل ۷-۲۷۲، بر روی New کلیک کنید و تانل EOIP را انتخاب کنید.

www.takbook.com



شکل ۷- ۲۷۲ پروتکل EOIP

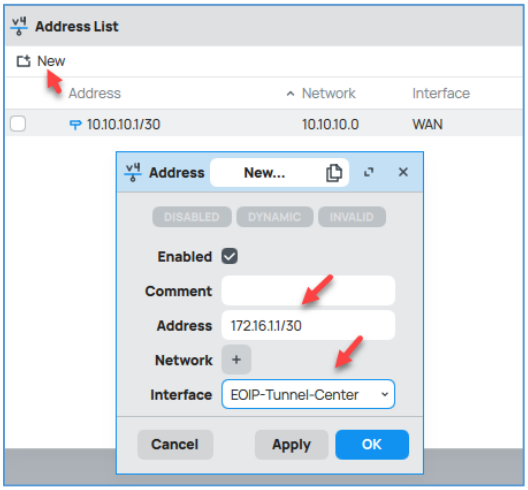
در شکل ۷-۲۷۳ یک نام برای تانل خود در نظر بگیرید و در قسمت Local Address باید آدرس Public روتر خود را وارد کنید و در قسمت Remote Address باید آدرس Public روتر شعبه‌ی خود را وارد کنید، در قسمت Tunnel ID اگر عدد می‌خواهید وارد کنید باید دقیقاً همین عدد را در Tunnel روبرو وارد کنید، توجه داشته باشید برای ایجاد امنیت بیشتر می‌توانید از IPSEC استفاده کنید که در قسمت IPsec Secret یک رمز عبور پیچیده قرار دهید.



شکل ۷- ۲۷۳ پروتکل EOIP

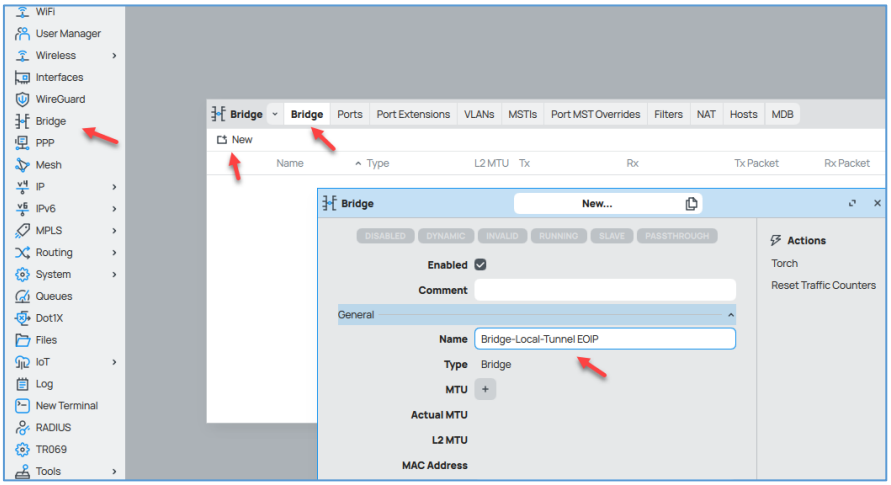
www.takbook.com

بعد از تعریف تانل EOIP باید یک آدرس IPv4 بر روی آنها تعریف کنیم تا پکت‌های IPv4 بر روی این تانل انتقال داده شود، این آدرس می‌تواند هر آدرسی به دلخواه شما باشد، طبق سناریو به مانند شکل ۷-۲۷٤، وارد IP و بعد Address می‌شویم و آدرس زیر را به تانل مورد نظر تخصیص می‌دهیم.



شکل ۷- ۲۷۴ پروتکل EOIP

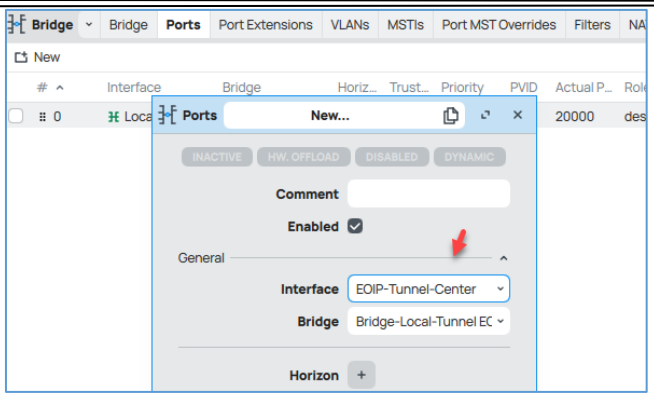
در ادامه کار وارد Bridge شوید و به مانند شکل ۷-۲۷۵ در تب Bridge بر روی New کلیک کنید و یک نام وارد کنید و بر روی OK کلیک کنید.



شکل ۷- ۲۷۵ پروتکل EOIP

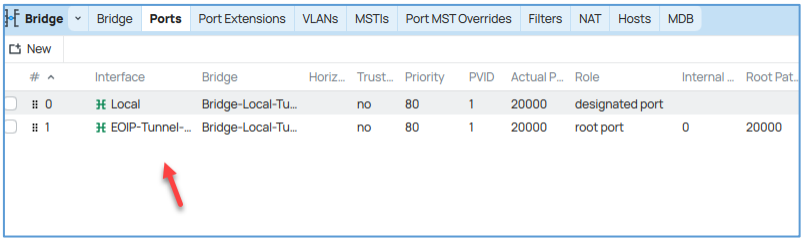
در ادامه به مانند شکل ۷-۲۷٦، وارد تب Ports شوید و بر روی New کلیک کنید و هر دو پورت را به لیست اضافه کنید.

www.takbook.com



شکل ۷- ۲۷۶ پروتکل EOIP

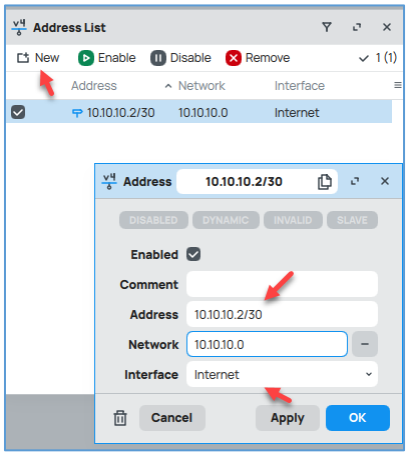
همان‌طور که مشاهده می‌کنید در شکل ۷–۲۷۷، هر دو پورت مورد نظر را به Bridge اضافه کردیم.



شکل ۷- ۲۷۷ پروتکل EOIP

۷–۳۵–۲ تنظیم روتر شعبه

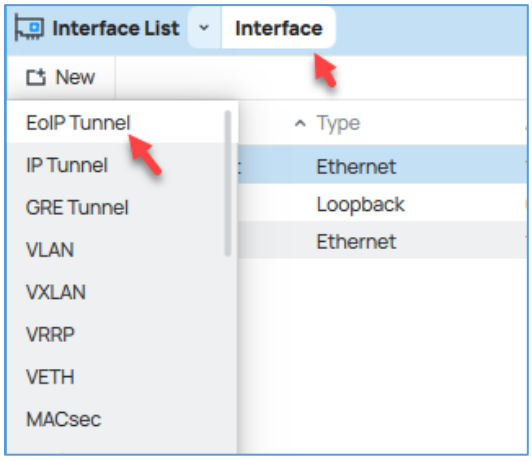
در ادامه کار باید وارد روتر شعبه شویم و تنظیمات آن را انجام دهیم، برای شروع به مانند شکل ۷–۲۷۸، وارد IP و بعد Address شوید و آدرس اینترنتی را تعریف کنید.



شکل ۷- ۲۷۸ پروتکل EOIP

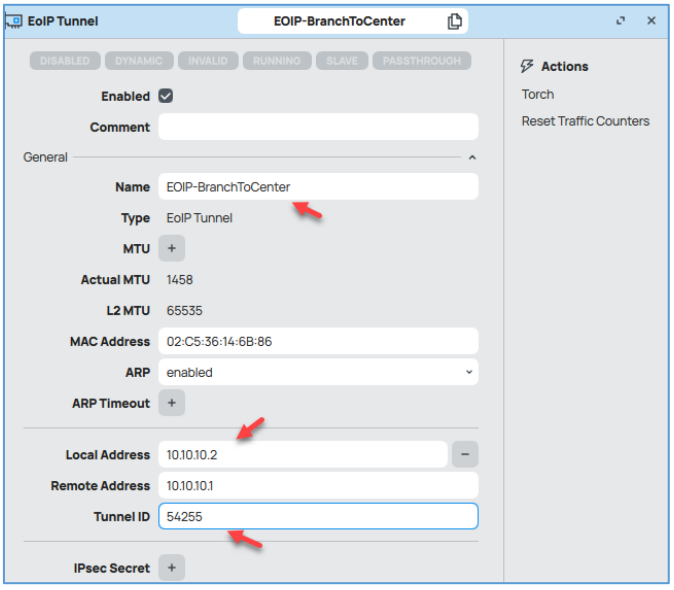
www.takbook.com

بعد از این کار باید تانل EOIP را ایجاد کنیم، طبق شکل ۷-۲۷۹، وارد Interface شوید و بر روی New کلیک کنید و گزینه‌ی EOIP Tunnel را انتخاب کنید.



شکل ۷- ۲۷۹ پروتکل EOIP

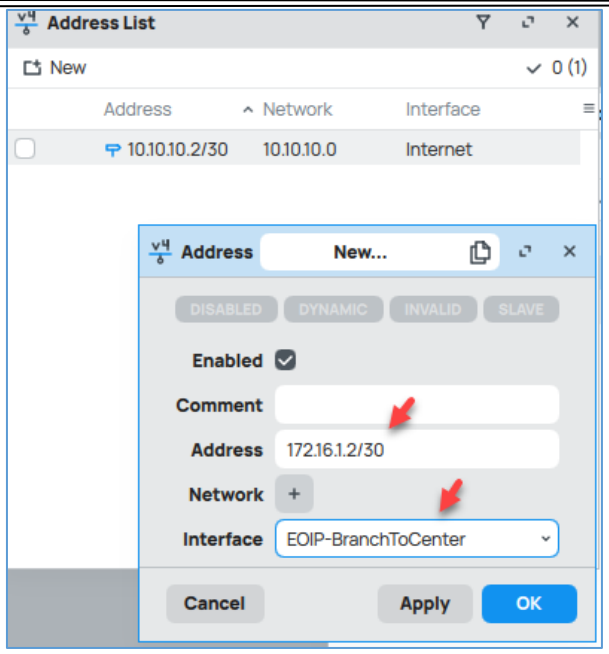
به مانند شکل ۷-۲۸۰، یک نام برای تانل خود در نظر بگیرید و آدرس Local و Remote را وارد کنید، به Tunnel ID توجه کنید که در هر دو روتر این عدد باید یکی باشد وگرنه ارتباط برقرار نخواهد شد.



شکل ۷- ۲۸۰

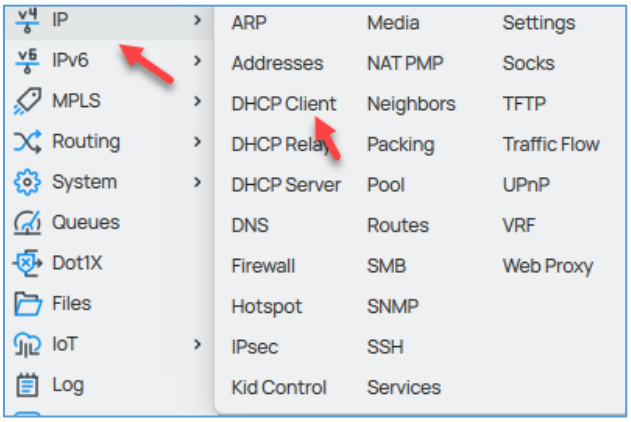
بعد از ایجاد تانل باید یک IPv4 بر روی این تانل به مانند قبل ایجاد کنیم،طبق شکل ۷-۲۸۱ وارد IP و بعد Address شوید و طبق سناریو یک آدرس IPv4 به آن تخصیص دهید.

www.takbook.com



شکل ۷- ۲۸۱ پروتکل *EOIP*

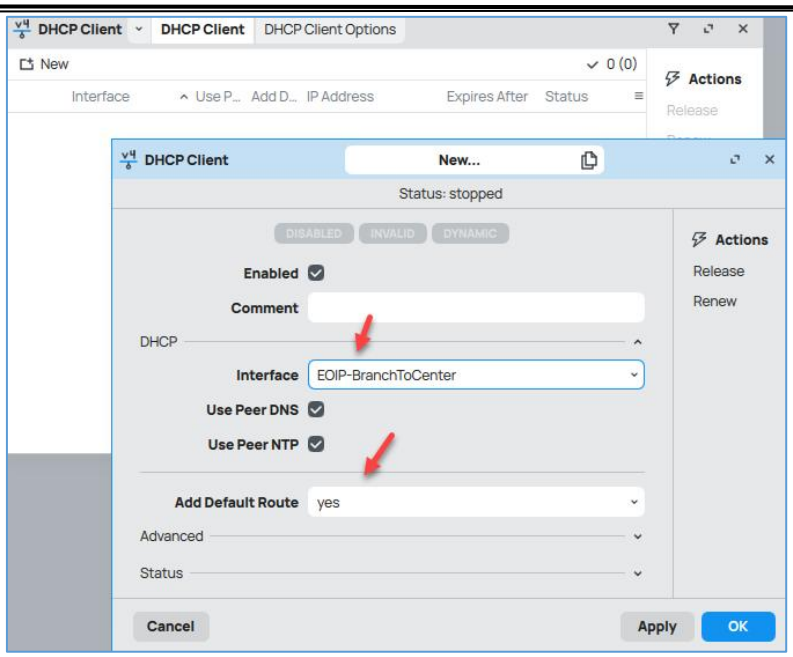
در ادامه دیگر نیازی نیست در روتر شعبه Bridge درست کنیم، فقط کافی است از DHCP Client استفاده کنیم، برای این کار طبق شکل ۷-۲۸۲، وارد IP و بعد DCHP Clients را انتخاب کنید.



شکل ۷- ۲۸۲ پروتکل *EOIP*

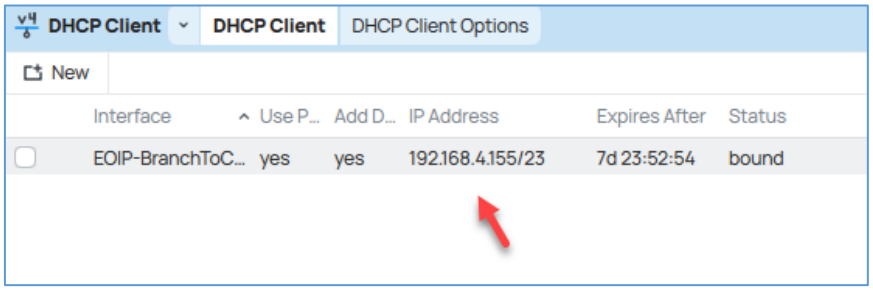
در شکل ۷-۲۸۳ باید تانل مورد نظر خود را انتخاب کنید و اگر می‌خواهید ترافیک روت به سمت این تانل ارسال شوید گزینه‌ی Yes را انتخاب کنید.

www.takbook.com



شکل ۷-۲۸۳ پروتکل *EOIP*

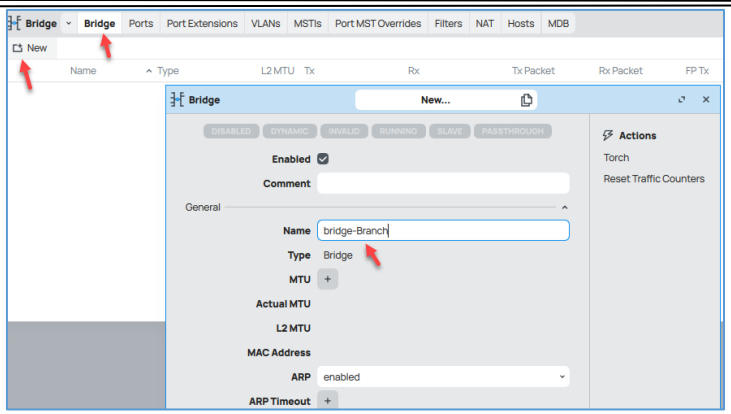
همان‌طور که در شکل ۷-۲۸٤، مشاهده می‌کنید آدرس مورد نظر از طریق سرویس DHCP دریافت شده است.



شکل ۷-۲۸۴ پروتکل *EOIP*

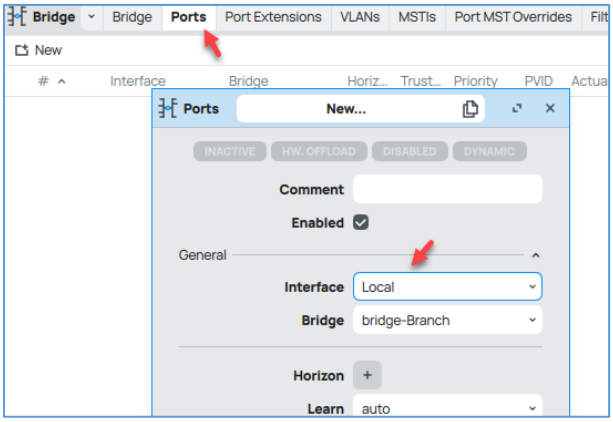
حالا برای اینکه کلاینت‌های داخل شبکه شعبه بتوانند از آدرس DHCP استفاده کنند باید تانل مورد نظر را با کارت شبکه‌ی داخلی در یک Bridge قرار دهیم، به مانند شکل ۷-۲۸۵، یک Bridge ایجاد کنید.

www.takbook.com



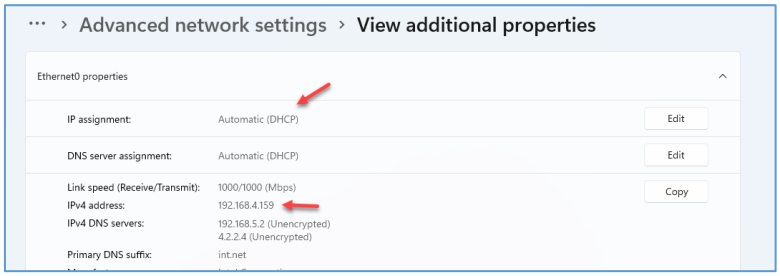
شکل ۷- ۲۸۵ پروتکل EOIP

به مانند شکل ۷-۲۸۶، وارد Port شوید و دو پورت شبکه‌ی داخلی و تانل EOIP را در لیست قرار دهید.



شکل ۷- ۲۸۶ پروتکل EOIP

بعد از اینکه دو پورت را در یک Bridge قرار دادید وارد کلاینت خود می‌شویم و این موضوع را تست می‌گیریم، همان‌طور که در شکل ۷-۲۸۷، مشاهده می‌کنیم کلاینت مورد نظر با موفقیت توانست آدرس IP را از شبکه مرکزی دریافت کنید، با این کار این کلاینت عضوی از شبکه ما است.



شکل ۷- ۲۸۷ پروتکل EOIP

www.takbook.com

فصل هشتم

مهندسی مایکروسافت

مدرک **MCSE (Microsoft Certified Solutions Expert)** یکی از معتبرترین گواهینامه‌های فنی در زمینه فناوری اطلاعات است که توسط مایکروسافت ارائه می‌شود. این مدرک به متخصصانی اعطا می‌شود که دانش و مهارت‌های لازم برای طراحی، پیاده‌سازی، مدیریت و نگهداری زیرساخت‌های **IT** مبتنی بر محصولات و سرویس‌های مایکروسافت را کسب کرده‌اند.

دوره **MCSE** به خصوص برای افرادی که در حوزه مدیریت شبکه‌ها، امنیت اطلاعات و زیرساخت‌های ابری (**Cloud**) فعالیت می‌کنند، اهمیت ویژه‌ای دارد. با کسب این مدرک، فرد توانایی خود را در زمینه راه‌حل‌های پیچیده فناوری اطلاعات و استفاده از تکنولوژی‌های پیشرفته مایکروسافت مانند **Windows Server, Azure** و **Office 365** ثابت می‌کند.

این گواهینامه نه تنها مهارت‌های فنی افراد را بهبود می‌بخشد، بلکه باعث ارتقای جایگاه شغلی و افزایش فرصت‌های شغلی در بازار کار فناوری اطلاعات نیز می‌شود.

۸-۱ تاریخچه ویندوز سرور

همان‌طور که از نام این ویندوز پیداست، با دستگاه‌های شبکه سروکار دارد و یک ویندوز کاملاً حرفه‌ای و با امکانات کامل است.

"ویندوز سرور" یک نام تجاری برای سیستم‌عامل‌های سرور منتشر شده توسط شرکت مایکروسافت است. این ویندوز امکاناتی را برای مدیریت سرورها فراهم می‌کند و بر روی سرورها نصب می‌شود. این نام تجاری شامل همه سیستم عامل‌های ویندوز با نام تجاری «ویندوز سرور» است، ولی سایر محصولات مایکروسافت را شامل نمی‌شود. اولین ویرایش ویندوز سرور منتشر شده با این نام تجاری، ویندوز سرور 2003 بود. با این وجود، اولین ویرایش سرور ویندوز، Windows NT 3.1 Server Advanced بود که بعد از آن Windows NT 3. 5 Server Windows NT 4 Server و ویندوز 2000 سرور ارائه شدند. ویندوز 2000 سرور اولین نسخه ویندوز سرور بود که به طور رسمی به عنوان ویندوز سرور معرفی شد.

ویندوز سرور 2003

ویندوز سرور 2003، نسخه تکمیل شده ویندوز 2000 سرور است و سازگاری و سایر ویژگی‌های ویندوز XP را در خود دارد. برخلاف ویندوز 2000 سرور، در نصب پیش‌فرض ویندوز سرور 2003، به منظور کاهش سطح حمله (attack surface)، هیچ‌کدام از اجزای سرور فعال نیستند. ویندوز سرور 2003 دارای

www.takbook.com

«حالت سازگاری» می‌باشد، که این قابلیت به نرم‌افزارهای قدیمی‌تر اجازه می‌دهد که با پایداری بیشتری اجرا شوند و همچنین سازگاری آن با شبکه‌های دامین ویندوز NT 4.0 بیشتر است. ویندوز سرور 2003 دارای سازگاری بهتر با اکتیو دایرکتوری بوده و پشتیبانی توسعه بهتری ارائه می‌دهد و این امر گذار از ویندوز NT 4.0 به ویندوز سرور 2003 و ویندوز XP پرو را آسان کرد.

ویندوز سرور 2003 R2

ویندوز سرور 2003 R2 نام یک محصول مکمل از شرکت مایکروسافت است. این محصول شامل یک کپی از ویندوز سرور 2003 SP1 بر روی یک CD و دسته‌ای از ویژگی‌ها با قابلیت نصب انتخابی (یادآور مایکروسافت پلاس)، بر روی CD دیگر می‌باشد. این محصول در تاریخ 6 دسامبر 2005، برای پلتفرم‌های IA-32 و x64 ارائه شد ولی شامل پلتفرم IA-64 نمی‌شد. پس از این محصول، ویندوز سرور ۲۰۰۸ معرفی شد.

ویندوز سرور 2008

ویندوز سرور 2008، دومین عضو مهم از خانواده ویندوز سرور برای کامپیوترهای سرور است. ویندوز سرور 2008 در 4 فوریه 2008 برای تولیدکنندگان و در 27 فوریه 2008 برای عموم عرضه شد. این سیستم عامل، جانشینی قدرتمند برای ویندوز سرور 2003 بود.

این ویندوز سرور در ابتدا با اسم کد "Longhorn" شناخته می‌شد و نام رسمی آن یعنی ویندوز سرور 2008، توسط بیل گیتس به عنوان رئیس مایکروسافت، در طی کنفرانس مهندسی سخت‌افزار ویندوز (WinHEC) در 16 می 2007 به آن داده شد.

کدهای مبنای مورد استفاده در ساخت ویندوز سرور 2008 مشابه کدهای ویندوز ویستا بود بنابراین معماری و عملکرد این دو ویندوز بسیار مشابه بودند. از آن جا که کدهای مبنای ویندوز سرور 2008 و ویندوز ویستا مشترک هستند، اکثر ویژگی‌های تکنیکی، امنیتی، مدیریتی و اجرایی جدید در ویندوز ویستا در ویندوز سرور ۲۰۰۸ نیز وجود دارد. از جمله این ویژگی‌های جدید می‌توان از بازنویسی شبکه (IPv6 ، شبکه بی‌سیم ، بهبود سرعت و امنیت)، بهبود نصب گرافیکی، توسعه پذیری و بازیابی، تشخیص خطای بهبود یافته، مانیتورینگ، ابزار ثبت و گزارش رخدادها، ویژگی‌های امنیتی جدید مانند BitLocker و (ASLR Address space layout randomization)، بهبود Windows Firewall با ساختار امنیتی پیش‌فرض، تکنولوژی‌های دات نت فریم ورک 3.0مخصوص زیرساخت ارتباطی ویندوز، Microsoft Message Queuing, Windows Workflow Foundation، هسته درونی، حافظه و بهبود در فایل سیستم، نام برد. پردازنده‌ها و حافظه‌ها به شکل Plug & Play (یعنی بعد از اولین اتصال به کامپیوتر به‌طور خودکار شناسایی می‌شوند) طراحی شده‌اند و به این ترتیب امکان اتصال گرم (Hot-plugging) برای این وسایل فراهم شد (اتصال گرم به این معناست که برای اتصال این وسایل به کامپیوتر نیاز به خاموش کردن کامپیوتر نیست). این موضوع

www.takbook.com

به منابع سیستم اجازه می‌دهد که با استفاده از «پارتیشن‌بندی سخت‌افزاری داینامیک» (Dynamic Hardware Partitioning) به شکل داینامیک و پویا پارتیشن‌بندی شوند به نحوی که هر پارتیشن دارای حافظه، پردازنده و دستگاه‌های هاست بریج ورودی/خروجی مختص به خود و مستقل از پارتیشن‌های دیگر است.

ویندوز سرور 2008 R2

ویندوز سرور ۲۰۰۸ R2 در 22 ژوئیه 2009 به تولیدکنندگان عرضه شد و در 22 اکتبر 2009 در دسترس عموم قرار گرفت. بر طبق نوشته وبلاگ ویندوز سرور، این ویندوز سرور در 14 سپتامبر 2009 برای فروش عرضه شد.

هسته ویندوز سرور 2008 R2 مشابه هسته ویندوز 7 (برای کلاینت‌ها)، می‌باشد. این ویندوز سرور 2008 R2، اولین سیستم عاملی است که توسط مایکروسافت انحصاراً ٦٤ بیتی عرضه شده‌است. ویژگی‌های بهبود یافته در این ویندوز شامل قابلیت‌های جدید برای اکتیو دایرکتوری، ویژگی‌های مدیریتی و مجازی‌سازی جدید، ورژن 7.5 سرویس‌های اطلاعات اینترنت (IIS)، وب سرور و پشتیبانی از حداکثر 256 پردازنده منطقی می‌باشند.

ویندوز سرور 2008 R2 دارای هفت ویرایش Foundation, Standard, Enterprise, Datacenter, Web, HPC Server, Itanium و ویندوز 2008 R2 نسخه Storage Server است.

ویندوز سرور 2012

ویندوز سرور ۲۰۱۲، با اسم کد "ویندوز سرور 8 "، ششمین نسخه از ویندوز سرور است. این ویندوز، نسخه سرور از ویندوز 8 بوده و در ادامه ویندوز سرور 2008 R2 عرضه شده‌است. در طی توسعه این ویندوز سرور، دو نسخه ارائه شد؛ نسخه پیش‌نمایش توسعه دهنده و دیگری نسخه بتا از این ویندوز سرور. این نرم‌افزار در تاریخ 4 سپتامبر 2012 به‌طور عمومی در دسترس مشتریان قرار گرفت.

بر خلاف نسخه‌های پیشین خود، ویندوز سرور 2012 کامپیوترهای مبتنی بر Itanium را پشتیبانی نمی‌کند و دارای چهار ویرایش می‌باشد. برخی ویژگی‌ها در ویندوز سرور 2012 وجود دارند که در ویندوز سرور ۲۰۰۸ R2 موجود نبودند و همچنین برخی از ویژگی‌های آن نیز نسبت به ویندوز سرور ۲۰۰۸ R2 بهبود یافته‌اند (بخصوص در رابطه با رایانش ابری). از جمله این ویژگی‌ها می‌توان نسخه به‌روزرسانی شده Hyper-V، نقش مدیریت IP آدرس (IPAM)، نسخه جدید Task Manager ویندوز و ReFS که یک فایل سیستم جدید است، را نام برد.

ویندوز سرور 2012، به رغم داشتن رابط کاربری مشابه با ویندوز 8، که مبتنی بر Metro و بسیار بحث‌برانگیز بوده، نظرات مثبتی را به سمت خود جلب نمود.

www.takbook.com

ویندوز سرور 2012 R2

ویندوز سرور 2012 R2 در ادامه ویندوز سرور ۲۰۱۲ و همزمان با ویندوز 8.1 در 18 اکتبر 2013 ارائه شد. این ویندوز برای اولین بار در 3 ژوئن 2013 در کنفرانس TechEd آمریکای شمالی رونمایی شد. بر طبق برگه اطلاعات ویندوز سرور 2012 R2 (منتشر شده در تاریخ 31 می 2013)، چهار ویرایش از این سیستم عامل وجود دارد: Foundation, Essentials, Standard و Datacenter. همان‌طور که در مورد ویندوز سرور 2012 صادق است، ویرایش‌های Datacenter و Standard از لحاظ مشخصات شبیه هستند و فقط از نظر لایسنس (بخصوص لایسنس مربوط به نمونه‌های مجازی) متفاوت می‌باشند. ویژگی‌های ویرایش Essentials، با در نظر گرفتن یک سری محدودیت‌ها، مشابه با Datacenter و Standard می‌باشد.

به روز رسانی ویندوز سرور 2012 R2 در آوریل سال 2014 ارائه شد که مجموعه ای از به روز رسانی‌های امنیتی و به روز رسانی‌های بسیار مهم را شامل می‌شد.

ویندوز سرور 2016

ویندوز سرور 2016 یک سیستم عامل سرور می‌باشد که به عنوان عضوی از خانواده ویندوزهای NT ، توسط مایکروسافت و به‌طور همزمان با ویندوز 10، توسعه داده شد. اولین نسخه پیش‌نمایش آن (Technical Preview)، به‌طور همزمان با اولین پیش‌نمایش تکنیکال سیستم سنتر، در 1 اکتبر 2014 در دسترس قرار گرفت. ویندوز سرور 2016، در 26 سپتامبر 2016 در کنفرانس Ignite مایکروسافت ارائه شد و در تاریخ 12 اکتبر 2016 در دسترس عموم قرار گرفت.

ویندوز سرور 2019

ویندوز سرور 2019 در 20 مارس 2018 به‌طور رسمی اعلام شد و اولین پیش نمایش windowsinsider در همان تاریخ ارائه شد. ویندوز سرور 2019 در 2 اکتبر 2018 منتشرشد.

ویندوز سرور 2022

Windows Server 2022 دهمین نسخه از ویندوز سرور است که منتشر شده، سیستم عامل ویندوز سرور شرکت مایکروسافت، به عنوان بخشی از خانواده سیستم عامل‌های Windows NT است. این ورژن از ویندوز سرور در 18 آگوست 2021 منتشر شد، تقریباً 3 سال پس از ویندوز سرور 2019 و چند ماه قبل از سیستم عامل ویندوز 11 منتشر شد.

مانند نسخه قبلی خود (2019)، ویندوز سرور 2025، به پردازنده‌های x64 نیاز دارد.

ویندوز سرور 2025

ویندوز سرور ۲۰۲۵، نسخه‌ای پیشرفته و بهبود یافته از سیستم‌عامل سرور مایکروسافت است که در نوامبر ۲۰۲٤ منتشر شد. این نسخه امکانات جدیدی در حوزه امنیت، مجازی‌سازی، ذخیره‌سازی، و شبکه ارائه می‌دهد و به طور خاص برای پشتیبانی از فناوری‌های مدرن همچون هوش مصنوعی، یادگیری ماشین، و مدیریت هیبریدی با Azure طراحی شده است. برخی از ویژگی‌های مهم آن عبارتند از:

www.takbook.com

امنیت پیشرفته

Credential Guard به صورت پیش‌فرض فعال شده است، که داده‌های حساس را در محیط‌های ایزوله محافظت می‌کند و حملاتی مانند "Pass-the-Hash" را کاهش می‌دهد.

SMB Security Enhancements شامل جلوگیری از حملات brute force، امضای اجباری SMB، و قابلیت محدود کردن تعداد تلاش‌های احراز هویت است.

LAPS جدید برای مدیریت رمزهای عبور ادمین محلی با قابلیت‌های جدیدی همچون مدیریت خودکار و تشخیص بازگردانی تصویر.

پیشرفت در ذخیره‌سازی

پشتیبانی از NVMe over Fabrics و بهینه‌سازی عملکرد درایوهای SSD.

بهبود در سیستم فایل ReFS، شامل قابلیت‌های جدید مثل Block Cloning.

Storage Spaces Direct (S2D) با عملکرد بهتر و امکان ذخیره‌سازی تعریف‌شده توسط نرم‌افزار.

قابلیت‌های اکتیو دایرکتوری (AD)

امکان تعمیر اشیاء آسیب‌دیده در AD و اندازه صفحه k۳۲ برای افزایش مقیاس‌پذیری.

ویژگی‌های جدید امنیتی برای رمزهای عبور ماشین‌های پیش‌فرض.

شبکه و مجازی‌سازی

Accelerated Networking با کاهش تأخیر و مصرف CPU در ماشین‌های مجازی.

بهبود در تقسیم GPU برای اشتراک منابع گرافیکی بین ماشین‌های مجازی.

یکپارچگی بیشتر با Azure Arc برای مدیریت هیبریدی.

سایر امکانات

Hotpatching برای کاهش زمان از کار افتادگی.

Virtualization-based security (VBS) برای ایجاد محیط‌های ایزوله امن برای داده‌های حساس.

ابزار DTrace برای ردیابی و عیب‌یابی سیستم به صورت لحظه‌ای.

۸-۲ نیازمندی‌های سخت‌افزاری

نیازمندی‌های سخت‌افزاری که در شکل ۸-۱، مشاهده می‌کنید حداقل نیازمندی است و برای ارائه سرویس بهتر پیشنهاد می‌شود مقدار آنها را افزایش دهید، مثلاً ۱۶ گیگ رم به همراه ۱ ترابایت هارد دیسک.

www.takbook.com

پردازنده	حداقل پردازنده باید **1.4** گیگاهرتز سرعت داشته باشد و ٦٤ بیت باشد.
رم	حداقل رم برای نسخه **Core** برابر ٥١٢ مگابایت است ولی برای نسخه **Desktop** باید ٢ گیگابایت باشد که بهتر است ٨ گگابایت در نظر بگیرید[٣]
هارد دیسک	حداقل فضای هارد مورد نیاز ٣٢ گیگ است[٣]
شبکه	یک کارت شبکه با حداقل سرعت ١ گیگابایت[٣]

شکل ٨- ١ سخت‌افزار و نرم‌افزار مورد نیاز

٨-٣ نصب و راه‌اندازی ویندوز سرور ٢٠٢٥

برای شروع به نصب می‌توانید نسخه نهایی ویندوز سرور ٢٠٢٥ را از طریق سایت مایکروسافت دانلود کنید، برای این کار می‌توانید از طریق لینک زیر اقدام کنید.

https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2025

بعد از ورود به لینک باید به مانند شکل ٨-٢ گزینه‌ی ISO را انتخاب کنید، و بعد از تکمیل اطلاعات، ویندوز مورد نظر را دانلود کنید، توجه داشته باشید در سایت‌های ایرانی این نسخه وجود دارد و می‌توانید آن را دریافت کنید.



شکل ٨- ٢ دانلود ویندز سرور٢٠٢٥

بعد از اینکه فایل ISO را دانلود کردید می‌توانید به روش‌های مختلف ویندوز سرور را بر روی سیستم‌های فیزیکی و مجازی خود نصب کنید، اگر سیستم فیزیکی دارید و می‌خواهید ویندوز را بر روی آن نصب

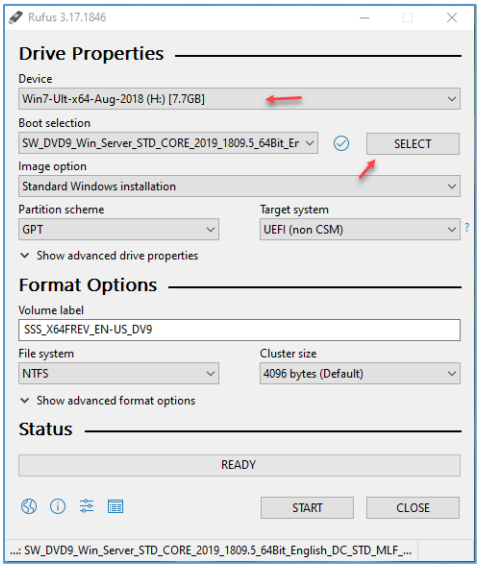
www.takbook.com

کنید باید فایل ISO را بر روی DVD رایت کنید و یا اینکه بر روی فلش بریزید، اگر بخواهید بر روی فلش قرار دهید باید از نرم‌افزار Rufus استفاده کنید.

برای دانلود نرم‌افزار می‌توانید از لینک زیر استفاده کنید:

https://github.com/pbatard/rufus/releases/download/v4.6/rufus-4.6.exe

همان‌طور که در شکل ۸-۳ مشاهده می‌کنید نرم‌افزار Rufus دانلود و اجرا شده است و از قسمت Device باید فلش دیسک مورد نظر خود را انتخاب کنید و از قسمت Select فایل ISO را انتخاب و بر روی Start کلیک کنید، بعد از اتمام کار باید فلش مورد نظر را به سیستم فیزیکی خود متصل و آن را اجرا کنید.



شکل ۸- ۳ ویندز سرور۲۰۲۵

توجه داشته باشید بعد از اینکه فلش را بر روی سیستم خود قرار دادید، باید سیستم (فیزیکی یا مجازی) خود را Restart کنید و کلید Boot Menu را روی کیبورد خود فشار دهید، در جدول ۸-۱ نام برند مادربرد به همراه کلید Boot آن را قرار دادیم، بعد از انتخاب فلش به عنوان Boot ویندوز برای نصب آماده است و می‌توانید نصب را آغاز کنید.

جدول ۸- ۱ Boot Menu

برند مادربرد	نوع	مدل	Boot Menu	Boot Once	صفحه Bios یا Setup	تغییر اولویت
ACER			Esc, F12, F9		Del, F2	
ACER	netbook	AspireOne, Aspire Timeline	F12		F2	

www.takbook.com

	F2	The "F12 Boot Menu" must be enabled in BIOS. It is disabled by default.	F12	Aspire v3, v5, v7	netbook	**ACER**
			Option	After 2006		**APPLE**
	F9		F8		desktop	**ASUS**
	F9		Esc		laptop	**ASUS**
	DEL		F8	R503C	laptop	**ASUS**
Boot Tab, Boot Device Priority, 1st Boot Device, Removable Device, F10	F2		Esc	Eee PC 1025c	netbook	**ASUS**
BIOS "Advanced Tab", Boot Order	F10		Esc, F9	Presario		**COMPAQ**
	F2	Select "USB Flash Drive"	F12	Dimension, Inspiron, Latitude	desktop	**DELL**
	F2	Select "USB Flash Drive"	F12	Inspiron One 2020, 2305, 2320, 2330 All-In-One	desktop	**DELL**
Settings->General->Boot Sequence->"USB Storage Device", then up arrow, [Apply]--[Exit]	F2	Select "USB Storage Device"	F12	Inspiron	laptop	**DELL**
	F12	Select "USB Storage Device" from boot menu	F12	Precision	laptop	**DELL**
	Tab, Del		F12			**EMACHINES**
	Esc, F10, F1		Esc, F9		generic	**HP**
BIOS "Advanced" tab, Boot Order, Move "USB Device" before "Hard Drive"	F10		Esc	Media Center	desktop	**HP**
BIOS "Advanced" tab, Boot Order, Move "USB Device" before "Hard	F10	Select boot media from the menu	Esc	Pavilion 23 All In One	desktop	**HP**

www.takbook.com

Drive". For non-UEFI media, disable secure boot and enable legacy support						
BIOS "Advanced" tab, Boot Order, Move "USB Device" before "Hard Drive"	F10		Esc	Pavilion g6 and g7	desktop	**HP**
Storage tab, Boot Order, Legacy Boot Sources	Esc F10	Then F9 for "Boot Menu"	Esc	Pavilion HPE PC, h8-1287c	desktop	**HP**
Storage tab, Boot Order, Legacy Boot Sources	Esc F10	Then F9 for "Boot Menu"	Esc	Pavilion PC, p6 2317c	desktop	**HP**
Storage tab, Boot Order, Legacy Boot Sources	Esc F10	Then F9 for "Boot Menu"	Esc	Pavilion PC, p7 1297cb	desktop	**HP**
Storage tab, Boot Order, Legacy Boot Sources	Esc F10	Then F9 for "Boot Menu"	Esc	TouchSmart 520 PC	desktop	**HP**
	Esc	Select "Patriot Memory" on the Boot Option Menu	Esc	2000	laptop	**HP**
BIOS "Advanced" tab, Boot Order, Move "USB Device" before "Hard Drive"	F10		Esc	Pavilion	notebook	**HP**
F10 Storage tab, Boot Order, Legacy Boot Sources	Esc	Then F9 for "Boot Menu"	Esc	ENVY dv6 and dv7 PC	notebook	**HP**
			F10			**INTEL**
	F1, F2		F12, F8, F10		desktop	**LENOVO**
	F1, F2		F12		laptop	**LENOVO**
	F2		F12 or Fn + F11	IdeaPad P500	laptop	**LENOVO**
	F2		F5			**NEC**

www.takbook.com

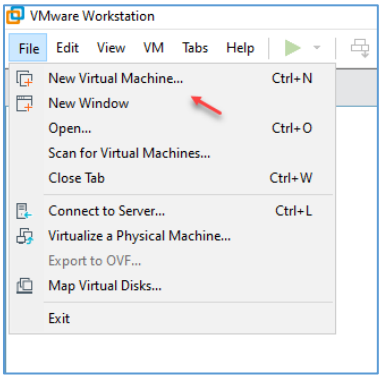
	F1, Del		F8			**PACKARD BELL**
			F12, Esc			**SAMSUNG**
Boot Tab, Select "Boot Device Priority", Press Return, Up/Down to Highlight, F6/F5 to change priority	F2		Esc	NC10	netbook	**SAMSUNG**
Boot Tab, Select "Boot Device Priority", Press Return, Up/Down to Highlight, F6/F5 to change priority	F2		Esc	Series 5 Ultra and Series 7 Chronos	ultrabook	**SAMSUNG**
	F2					**SHARP**
	F1, F2, F3		F11	VAIO, PCG, VGN		**SONY**
BIOS "BOOT" section, "External Device Boot" enabled	F2		F10	VGN Esc		**SONY**
	F1, Esc		F12	Protege, Satellite, Tecra		**TOSHIBA**
	F12		F12	Equium F12		**TOSHIBA**

نکته مهم در هنگام نصب ویندوز در سیستم‌های جدید مخصوصاً در لپ‌تاپ این است که سیستم‌های جدید از هارد SSD استفاده می‌کنند و برای نصب ویندوز نیاز به یک درایو دارند تا هارد مورد نظر در لیست هاردها ظاهر شود و برای حل این مشکل باید درایور آن را دانلود کنید.

روشی که در این کتاب بررسی می‌کنیم استفاده از ماشین مجازی برای نصب ویندوز سرور است، برای انجام این کار نرم‌افزار VMware Workstation را که در فصل ششم بررسی کردیم اجرا کنید.

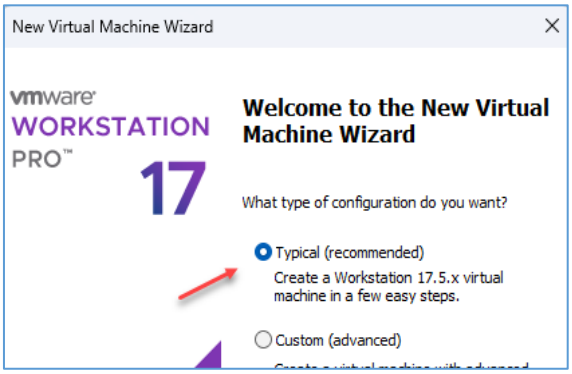
برای اینکه این ماشین مجازی را در VMware Workstation ایجاد کنید از منوی File گزینه‌ی New Virtual Machine را انتخاب کنید که در شکل ۸-٤- مشخص شده است.

www.takbook.com



شکل ۸- ۴ ایجاد ماشین مجازی

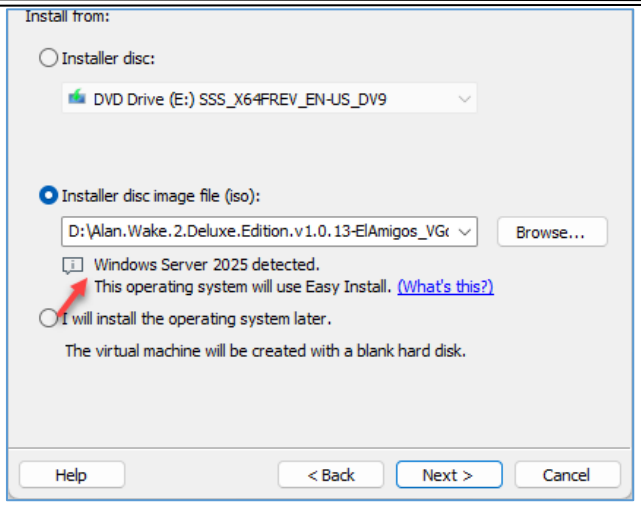
در شکل ۸-۵ گزینه‌ی Typical را انتخاب کنید.



شکل ۸- ۵ ایجاد ماشین مجازی

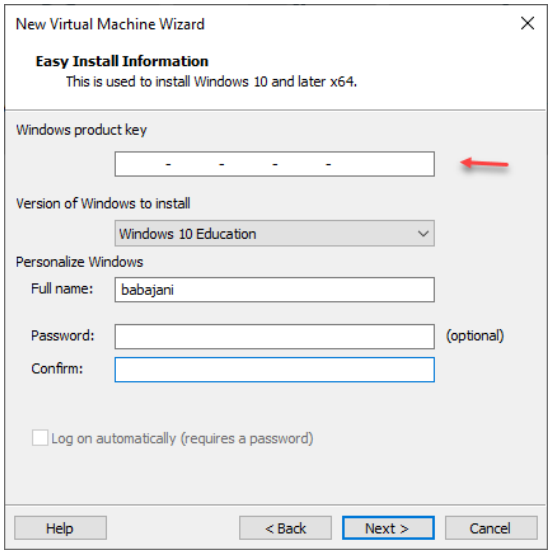
در ادامه کار به مانند شکل ۸-۶ باید گزینه‌ی Installer disc image file را انتخاب و فایل ISO مورد نظر مربوط به ویندوز سرور ۲۰۲۵ را انتخاب کنید، توجه داشته باشید که خود VMware نسخه سیستم عامل را زیر فایل به صورت اتوماتیک می‌نویسد که در اینجا ویندوز سرور ۲۰۲۵ نوشته شده است، اگر چنانچه نوع ویندوز مشخص نشود در صفحه بعد باید ورژن آن را انتخاب کنید، بر روی Next کلیک کنید.

www.takbook.com



شکل ۸- ۶ ایجاد ماشین مجازی

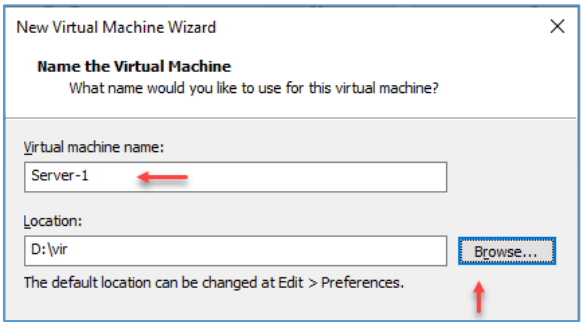
در شکل ۸-۷، می‌توانید برای راحتی کار، سریال ویندوز را به همراه نوع ورژن و نام کاربری و رمز عبور را مشخص کنید، ولی در حال حاضر نیازی به این کار نیست و فقط بر روی Next کلیک کنید.



شکل ۸- ۷ ایجاد ماشین مجازی

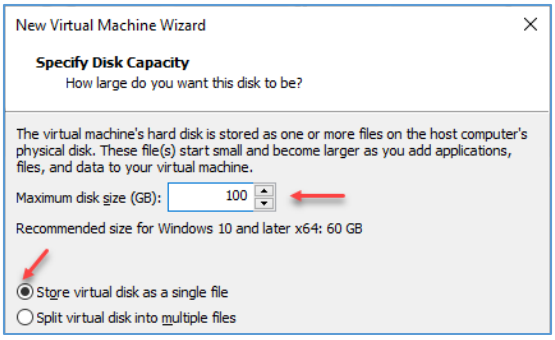
در شکل ۸-۸، باید نام ماشین مجازی خود را به همراه محل ذخیره‌سازی مشخص کنید، سعی کنید محلی را که برای ایجاد ماشین انتخاب می‌کنید فضای کافی داشته باشد.

www.takbook.com



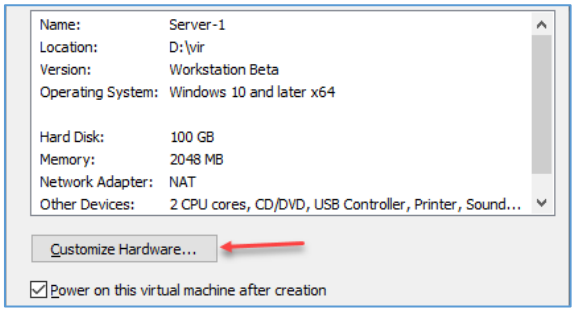
شکل ۸- ۸ ایجاد ماشین مجازی

در شکل ۸-۹، باید مقدار فضای هارد دیسک را برای این ماشین انتخاب و نوع فایل ذخیره شده را Single در نظر بگیرید.



شکل ۸- ۹ ایجاد ماشین مجازی

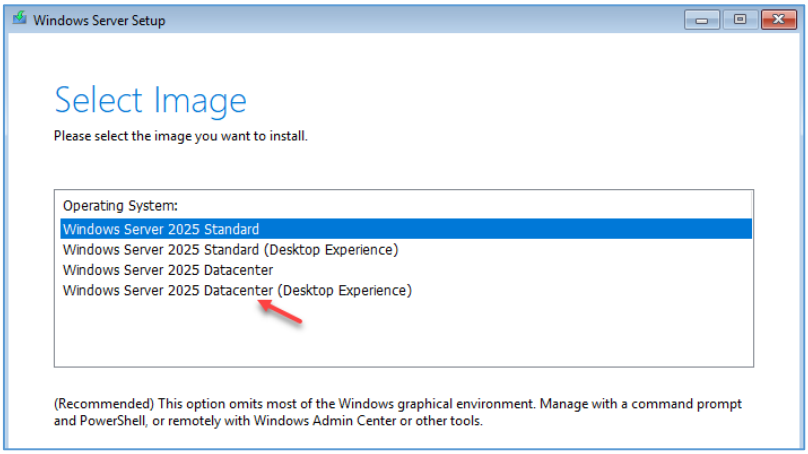
قبل از اینکه بر روی Finish در شکل ۸-۱۰، کلیک کنید بهتر است نگاهی به سخت‌افزار این ماشین بیندازیم، برای این کار می‌توانید بر روی Customize Hardware کلیک کنید و یا اینکه برای اتمام کار و روشن شدن ماشین بعد از ایجاد آن تیک گزینه‌ی Power on را انتخاب و بر روی Finish کلیک کنید.



شکل ۸- ۱۰

www.takbook.com

بعد از اجرا شدن ماشین مورد نظر اولین صفحه‌ای که مشاهده خواهید کرد شکل ۸-۱۱ است که باید یکی از نسخه‌های ویندوز سرور را انتخاب کنید که در اینجا نسخه‌ی Datacenter که نسخه‌ی کامل است را انتخاب می‌کنیم.



شکل ۸- ۱۱ نصب ویندوز سرور ۲۰۲۵

اگر به شکل ۸- ۱۱ توجه کرده باشید دو نوع ویندوز سرور را می‌توانید نصب کنید:

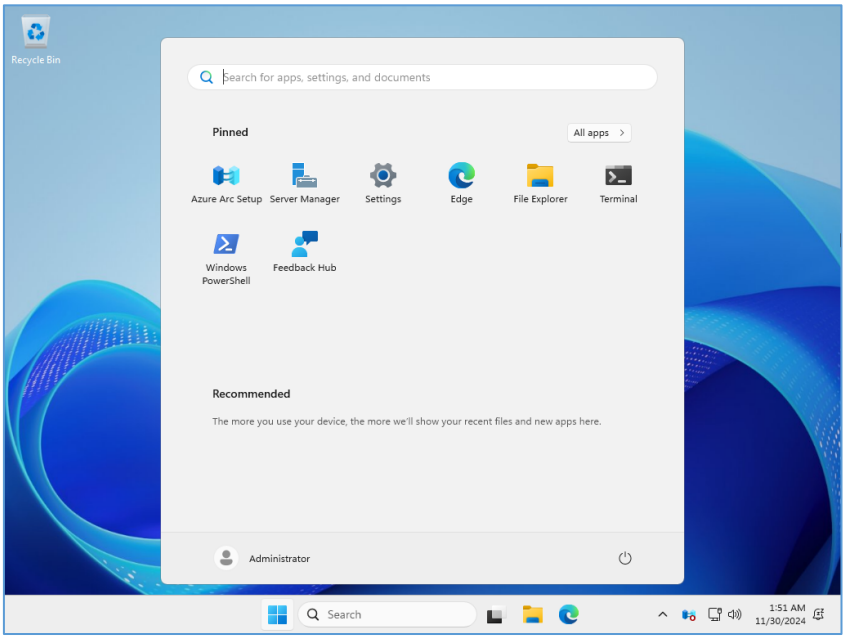
۱- Server Core : این نوع سرور یک ویندوز بدون گرافیک هست و هسته اصلی ویندوز را شامل می‌شود و نسخه کوچک شده ویندوز سرور است و تمام دستورات آن از طریق PowerShell اجرا می‌شود، این نوع سرورها اصولاً در مراکز ارائه دهنده‌ی سرویس‌های تحت وب و دیگر سرویس‌ها، کاربرد بسزایی دارد.

۲- Server with Desktop Experience: این نسخه یک بسته کامل و به صورت گرافیکی است و اکثر کاربران هم این نسخه را استفاده می‌کنند، کار با این نسخه آسان‌تر است و نیازی به اجرای کد نیست، هر چند اجرای کد در این نسخه هم می‌شود انجام داد.

ما برای شروع از نسخه‌ی Desktop استفاده می‌کنیم تا بتوانیم راحت‌تر این آموزش‌ها را فرا بگیرید و در ادامه نسخه‌ی Core آن را هم نصب خواهیم کرد.

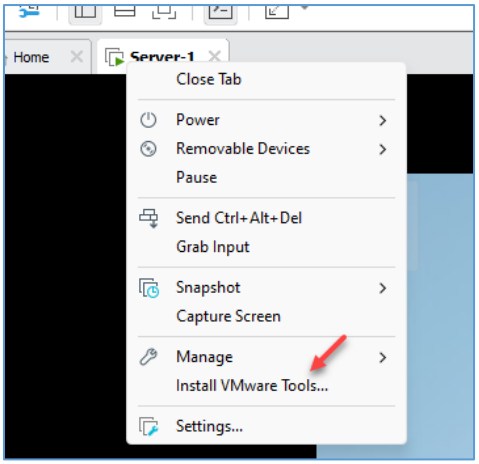
همان‌طور که در شکل ۸-۱۲ مشاهده می‌کنید ویندوز مورد نظر به صورت مجازی نصب و اجرا شده است.

www.takbook.com



شکل ۸- ۱۲ نصب ویندوز سرور ۲۰۲۵

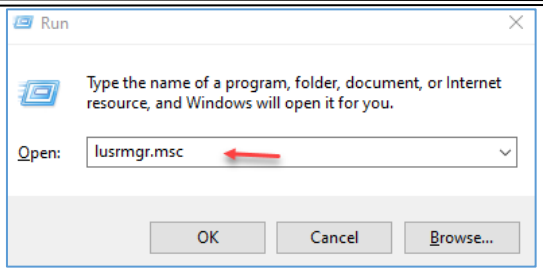
اولین کاری که انجام می‌دهیم نصب VMware Wools است که برای این کار بر روی ماشین مورد نظر کلیک راست کنید و گزینه‌ی VMware Tools را به مانند شکل ۸-۱۳، انتخاب کنید.



شکل ۸- ۱۳ نصب ویندوز سرور ۲۰۲۵

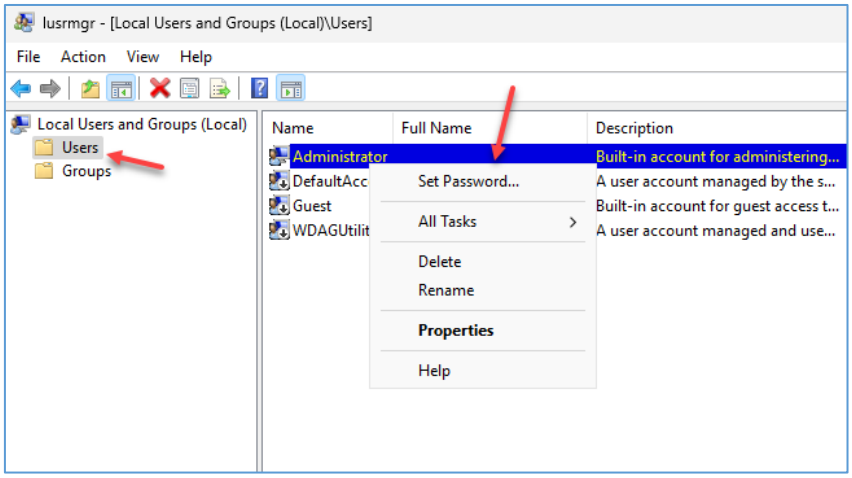
بعد از نصب VMware Tools، برای شروع کار بهتر است یک رمز عبور برای کاربر administrator در نظر بگیریم، برای این کار وارد ویندوز سرور شوید و با کلید ترکیبی WIN + R سرویس Run را اجرا کنید. به مانند شکل ۸-۱۴ باید دستور lusrmgr.msc را اجرا کنید.

www.takbook.com



شکل ۸- ۱۴ نصب ویندوز سرور ۲۰۲۵

در شکل ۸-۱۵ وارد قسمت Users شوید و بر روی کاربر Administrator کلیک راست کنید و گزینه‌ی Set Password را انتخاب کنید و یک رمز عبور پیچیده برای آن در نظر بگیرید.(مانند EP@$*2025)



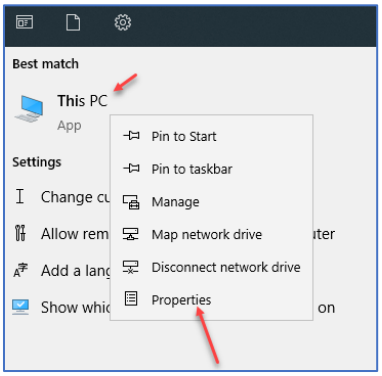
شکل ۸- ۱۵ رمز کاربر *Administrator*

در ادامه برای اینکه با کاربر Administrator وارد شویم باید از کاربر قبلی Sign out کنید و با کاربر Administrator وارد شوید.

۸-۳-۱ تغییر نام ویندوز سرور

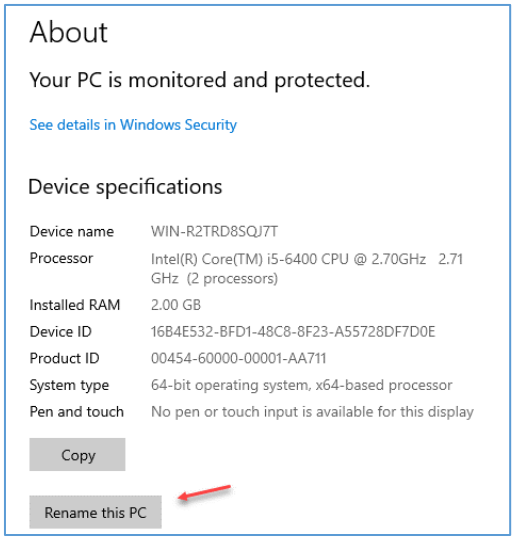
بعد از نصب ویندوز و ورود با کاربر Administrator چند کار باید انجام دهیم اول از همه نام سرور خود را تغییر می‌دهیم، سعی کنید نام‌هایی که برای سرور انتخاب می‌کنید کاملاً با همان سرور همخوانی و ساده باشد تا مدیریت آن آسان‌تر شود البته برای امنیت بیشتر پیشنهاد می‌شود که نام سرورهای یک شبکه از یک استاندارد پیروی کند تا فهمیدن اینکه نام سرور مورد نظر چه عملکردی دارد سخت‌تر شود. برای این کار به مانند شکل ۸-۱۶ بر روی آیکون کامپیوتر کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید، البته برای اینکه وارد صفحه Properties شوید می‌توانید از کلید ترکیبی Windows + Pause استفاده کنید.

www.takbook.com



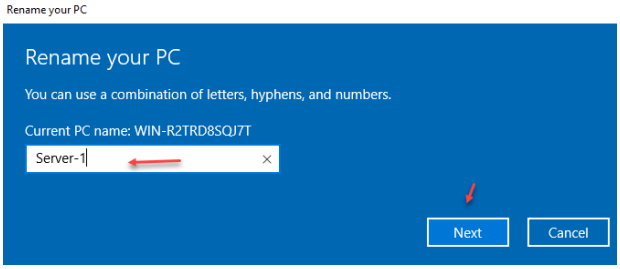
شکل ۸- ۱۶ تغییر نام ویندوز

در شکل ۸-۱۷ نام سرور را در قسمت Device name مشاهده می‌کنید که برای تغییر بر روی Rename کلیک کنید.



شکل ۸- ۱۷ تغییر نام ویندوز

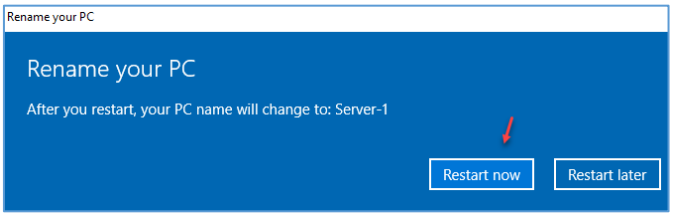
در ادامه و در شکل ۸-۱۸ باید نام سرور خود را وارد و بر روی Next کلیک کنید.



شکل ۸- ۱۸ تغییر نام ویندوز

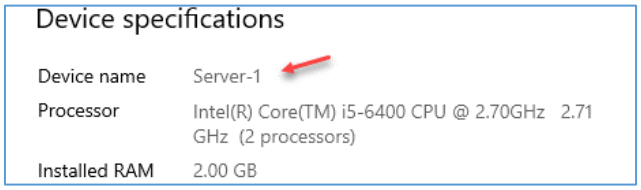
www.takbook.com

در شکل ۸- ۱۹ برای اعمال تغییرات بر روی Restart now کلیک کنید، تا سرور بعد از Restart نامش تغییر کند.



شکل ۸- ۱۹ تغییر نام ویندوز

همان‌طور که در شکل ۸-۲۰ مشاهده می‌کنید نام سرور تغییر کرده است.



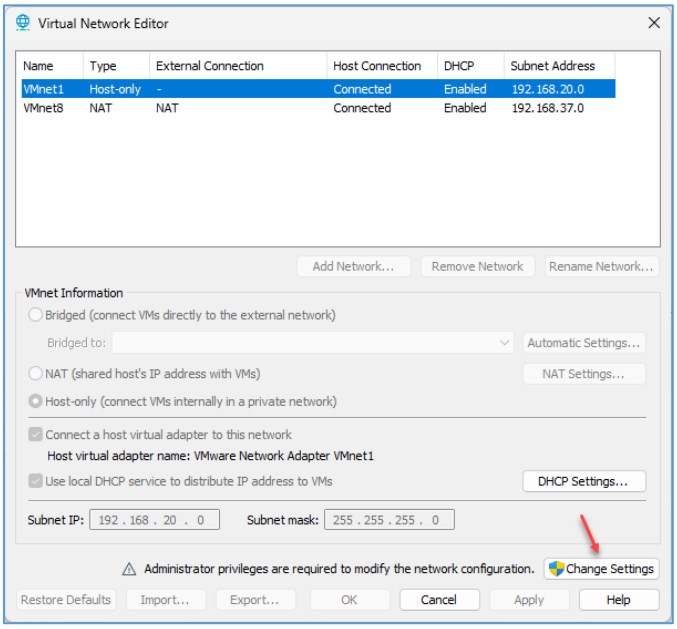
شکل ۸- ۲۰ تغییر نام ویندوز

۸-۳-۲ تخصیص آدرس IP

برای اینکه سرور خود را در شبکه شناسایی کنیم بهتر است برای آن یک آدرس IP در نظر بگیریم، از دو روش می‌شود به سرور IP داد، یکی از طریق سرویس DHCP که در ادامه کتاب در مورد آن به صورت کامل توضیح خواهیم داد و یکی به صورت دستی؛ توجه داشته باشید که همیشه باید برای سرورها به صورت دستی IP وارد کنید تا امنیت کار افزایش پیدا کند و کسی قادر به تغییر آن آدرس نباشد، هر چند می‌توانید از طریق سرویس DHCP آدرس سرور را رزرو کنید ولی در بعضی مواقع نیاز ضروری هست که آدرس را به صورت دستی وارد کنیم.

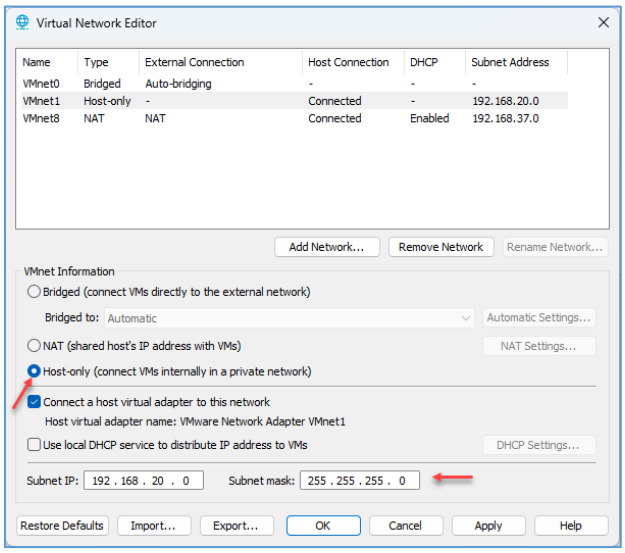
برای اینکه از طریق VMware Workstation به سرور خود کارت شبکه تخصیص دهیم باید سرویس Virtual Network Editor را در سیستم اصلی (فیزیکی) خود اجرا کنید و به مانند شکل ۸-۲۱ برای ایجاد تغییرات در آن بر روی Change Settings کلیک کنید.

www.takbook.com



شکل ۸- ۲۱ / اختصاص کارت شبکه

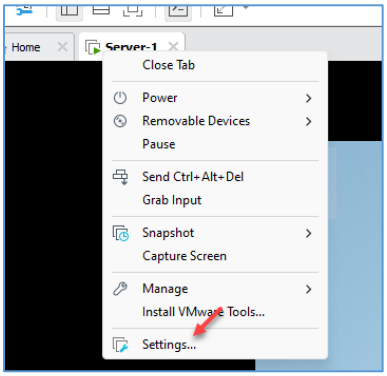
برای اینکه سیستم‌های خود را شبکه کنیم از کارت شبکه‌ی Host-only استفاده می‌کنیم، به مانند شکل ۸-۲۲ کارت شبکه‌ی مجازی VMnet1 را انتخاب کنید و در پایین صفحه IP و Subnet آن را مشخص و بر روی OK کلیک کنید، بعد از این کار تیک گزینه‌ی Use local DHCP… را بردارید تا به صورت اتوماتیک به سیستم‌های شما IP اختصاص ندهد.



شکل ۸- ۲۲ / اختصاص کارت شبکه

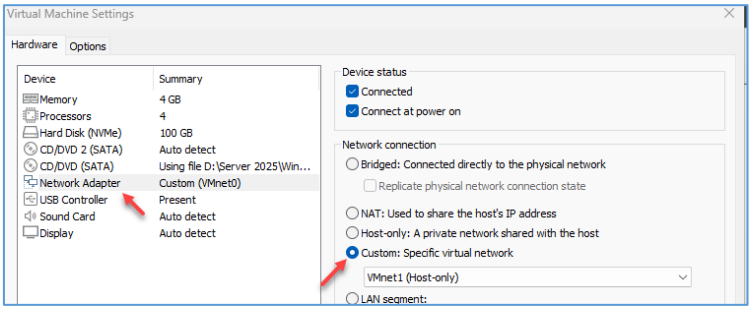
www.takbook.com

رنج IP را برای این کارت شبکه 192.168.20.0 در نظر گرفتیم که ماشین‌هایی که به این کارت متصل می‌شوند باید در این رنج باشند، در ادامه کار به مانند شکل ۸–۲۳ بر روی ماشین مورد نظر کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید.



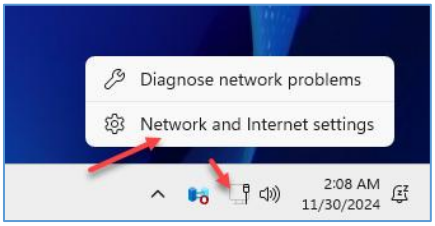
شکل ۸- ۲۳ / اختصاص کارت شبکه

به مانند شکل ۸–۲۴ کارت شبکه را انتخاب کنید و از قسمت Custom کارت شبکه‌ی مجازی VMnet1 را انتخاب و بر روی OK کلیک کنید.



شکل ۸- ۲۴ / اختصاص کارت شبکه

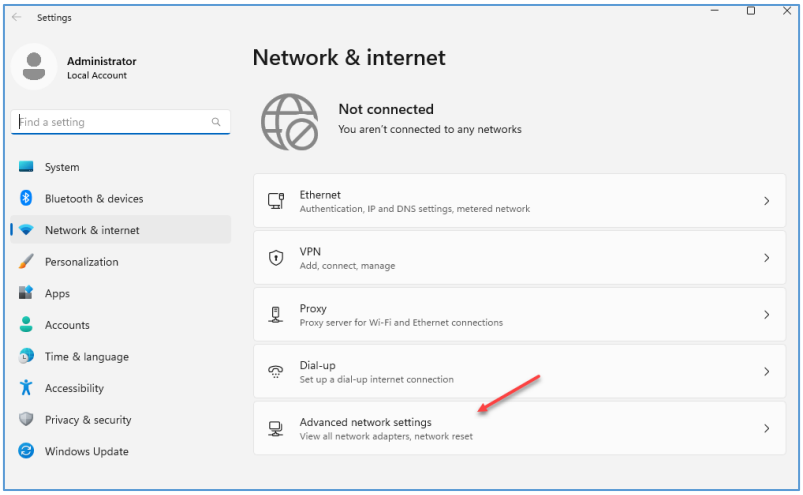
بعد از انتخاب کارت شبکه وارد ماشین مجازی خود شوید و برای اینکه به کارت شبکه IP دهیم به مانند شکل ۸–۲۵، بر روی آیکون کارت شبکه کلیک راست کنید و گزنیه‌ی Network and Internet settings را انتخاب کنید.



شکل ۸- ۲۵ تخصیص IP

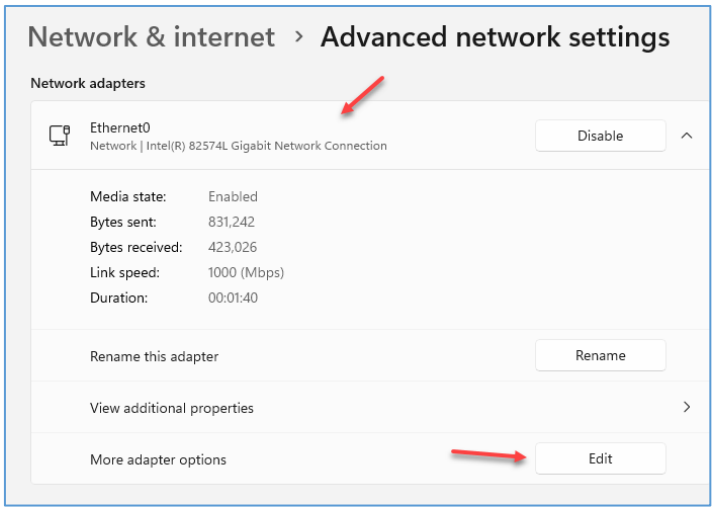
www.takbook.com

در شکل ۸–۲۶ بر روی Advanced network settings کلیک کنید تا لیست کارت شبکه را مشاهده کنید.



شکل ۸– ۲۶ تخصیص IP

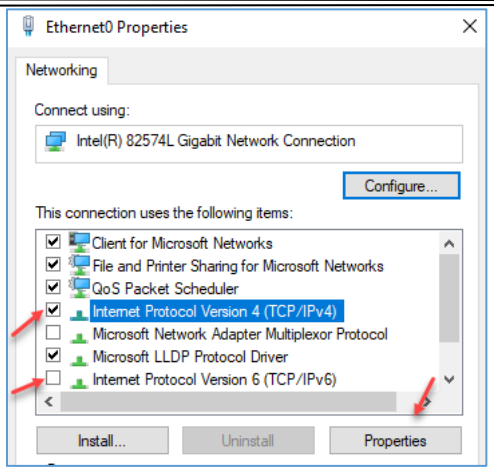
در شکل ۸–۲۷ بر روی کارت شبکه مورد نظر کلیک کنید و در منوی باز شده گزینه‌ی Edit را کلیک کنید.



شکل ۸– ۲۷ تخصیص IP

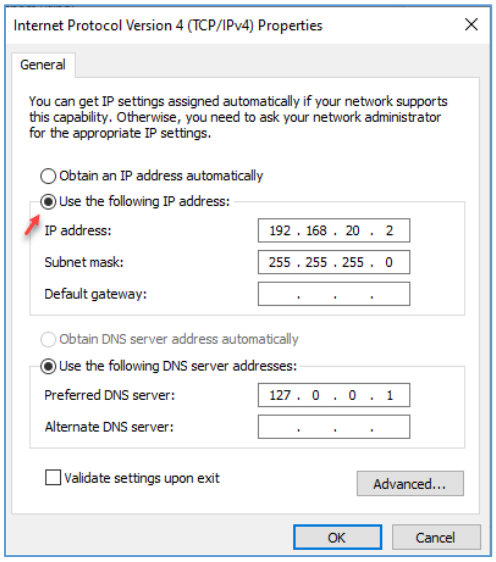
در شکل ۸–۲۸ گزینه‌های مختلفی را مشاهده می‌کنید، مثلاً می‌توانید IPv4 و یا IPv6 را مشخص کنید که در حال حاضر با IPv4 کار می‌کنیم، گزینه‌ی مورد نظر را انتخاب و بر روی Properties کلیک کنید.

www.takbook.com



شکل ۸- ۲۸ تخصیص IP

درشکل ۸-۲۹ باید آدرس IP شبکه خود را وارد کنید، رنج IP که در این شبکه استفاده می‌شود 192.168.2.0 است با Subnet، 255.255.255.0 و آدرس این سرور را 192.168.20.2 در نظر می‌گیریم و آدرس DNS آن را 127.0.0.1 (یعنی خودش) در نظر می‌گیریم، در مورد سرویس DNS در ادامه کتاب صحبت خواهیم کرد و نحوه‌ی کارکرد آن را با هم بررسی می‌کنیم.



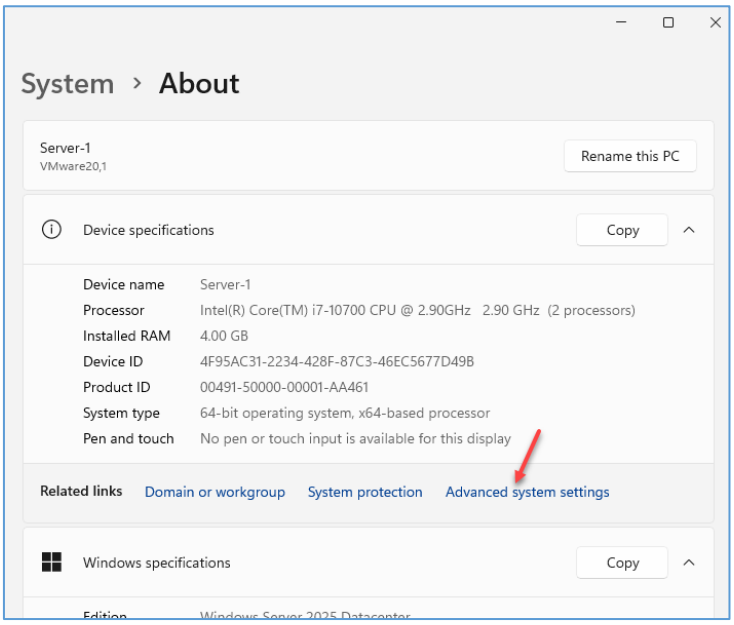
شکل ۸- ۲۹ تخصیص IP

www.takbook.com

۳-۳-۸ فعال‌سازی Remote Desktop

برای اینکه بتوانید به راحتی به سرورهای خود (سرورهای مجازی) در شبکه متصل شوید یک راه آسان آن، استفاده از Remote Desktop است .

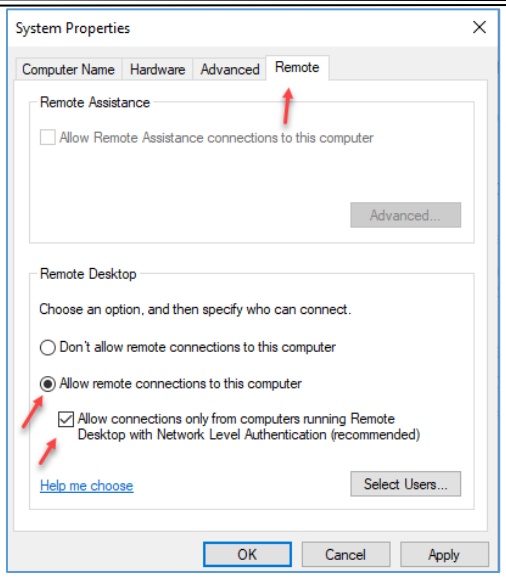
برای فعال‌سازی این سرویس به مانند شکل ۸-۳۰، از منوی Start وارد System شوید و بر روی Advanced system settings کلیک کنید.



شکل ۸- ۳۰ فعال‌سازی Remote Desktop

در شکل ۸-۳۱، وارد تب Remote شوید، اگر بخواهید قابلیت Remote را فعال کنید باید گزینه‌ی Allow remote connection to this computer را انتخاب کنید، توجه داشته باشید که اگر تیک گزینه‌ی Allow connections only… را انتخاب کنید، فقط به کاربران و سیستم‌هایی دسترسی داده خواهد شد که در یک دومین یا گروه مشخص قرار گرفته باشد، به بیان ساده‌تر یعنی اینکه کسی نمی‌تواند بیرون از شبکه دومین به سرور ما Remote بزند، در قسمت Select Users هم می‌توانید به کاربر مورد نظر خود برای انجام Remote دسترسی دهید، توجه داشته باشید که در حال حاضر فقط کاربران Local را می‌توانید انتخاب کنید و فعلاً کاربران تحت دومین که در ادامه بررسی می‌کنیم تعریف نشده است.

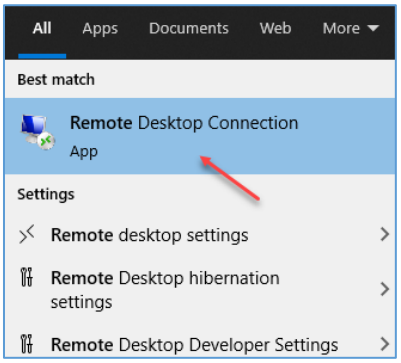
www.takbook.com



شکل ۸- ۳۱ فعال‌سازی Remote Desktop

بعد از اینکه سرویس Remote Desktop را برای ویندوز سرور مورد نظر فعال کردید، می‌توانید از طریق نرم‌افزار Remote Desktop به آن ماشین مجازی متصل شوید.

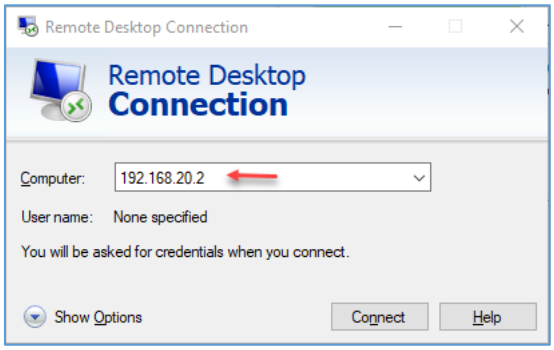
برای اجرا این نرم‌افزار وارد سیستم اصلی خود شوید و به مانند شکل ۸-۳۲ از طریق Start بر روی Remote Desktop Connection کلیک کنید و بعد از اجرا IP سیستم مجازی که به اسم Server-1 بوده را وارد کنید.



شکل ۸- ۳۲ فعال‌سازی Remote Desktop

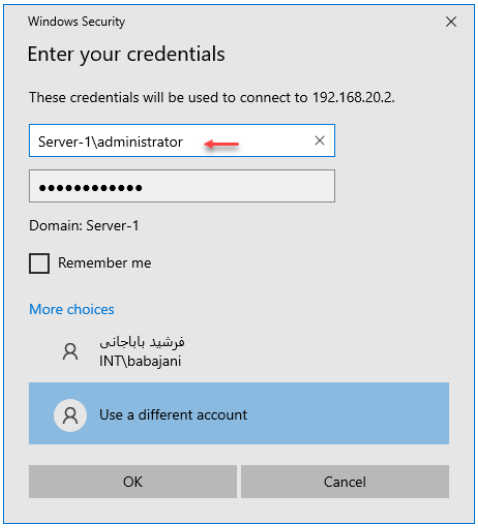
در شکل ۸-۳۳ باید آدرس IP سرور مجازی را وارد کنید و بر روی Connect کلیک کنید تا به سرور متصل شویم.

www.takbook.com



شکل ۸- ۳۳ فعال‌سازی *Remote Desktop*

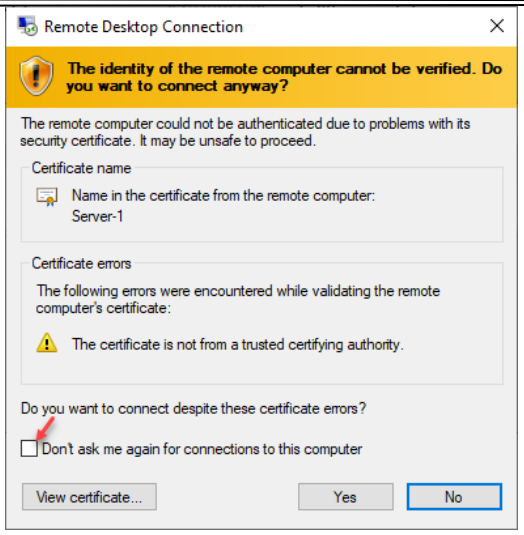
در شکل ۸-۳٤ باید نام کاربری و رمز عبور را وارد کنید، توجه داشته باشید که چون در شبکه Workgroup قرار داریم باید اول نام سرور را وارد و بعد نام کاربری را به همراه رمز وارد کنیم، توجه داشته باشید که اگر سیستم در دومین قرار داشت دیگر نیاز به وارد کردن نام سیستم نبود و فقط باید نام دومین به همراه نام کاربری و رمز عبور را وارد می‌کردید.



شکل ۸- ۳۴ فعال‌سازی *Remote Desktop*

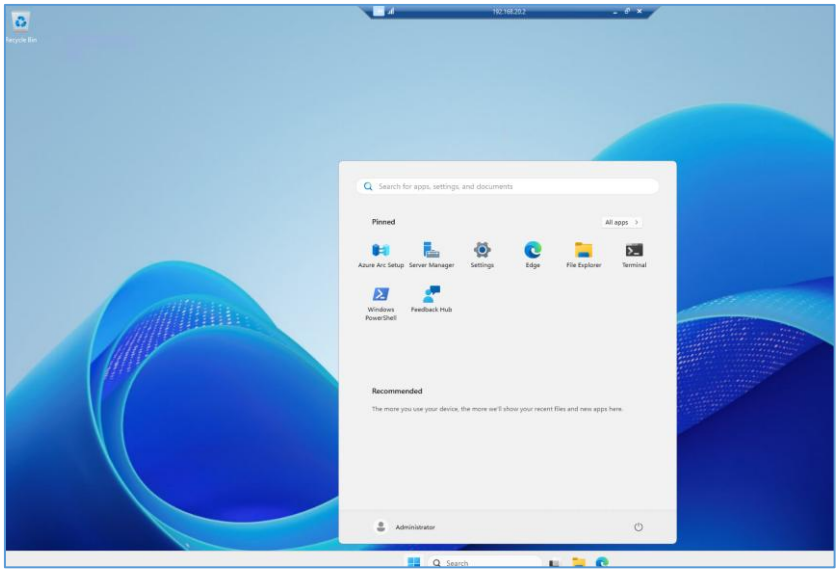
همان‌طور که در شکل ۸-۳۵ مشاهده می‌کنید، به این نکته اشاره شده است که Certificate (گواهی‌نامه امنیتی) مورد نظر مورد تایید نیست که در حال حاضر نیاز نیست که آن را بررسی کنیم بهتر است تیک گزینه‌ی مورد نظر را انتخاب کنید و بر روی Yes کلیک کنید تا دیگر این صفحه ظاهر نشود.

www.takbook.com



شکل ۸- ۳۵ فعال‌سازی *Remote Desktop*

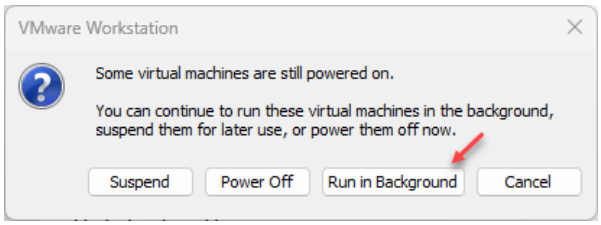
همان‌طور که در شکل ۸-۳۶ مشاهده می‌کنید با موفقیت توانستیم به سرور مجازی Server-1 متصل شویم، به این نکته اشاره کنم که این سرویس امنیت کافی در شبکه نخواهد داشت و انشاالله در فصل امنیت سرویس‌های مایکروسافت روش‌های امن‌سازی آن را بررسی خواهیم کرد.



شکل ۸- ۳۶ *Remote Desktop*

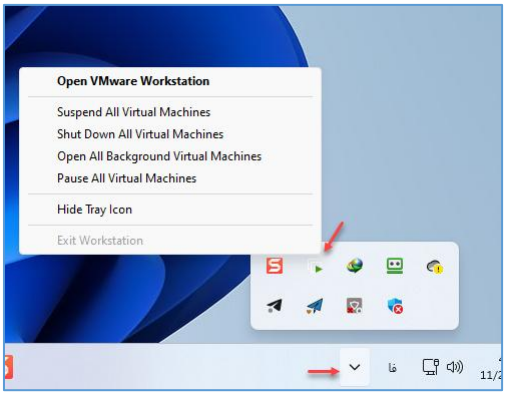
www.takbook.com

توجه داشته باشید بعد از اینکه به ماشین جدید خود Remote زدیم برای اینکه نرم‌افزار Vmware Workstation را مخفی کنیم می‌توانیم به مانند شکل ۸-۳۷، بر روی علامت Close کلیک کنیم و در صفحه باز شده‌ی زیر گزینه‌ی Run in background را انتخاب کنید تا در کنار ساعت قرار بگیرد.



شکل ۸- ۳۷ Remote Desktop

اگر به مانند شکل ۸-۳۸، بر روی آیکون مورد نظر کلیک راست کنید گزینه‌های در دسترس قرار دارد که می‌توانید بر روی ماشین مورد نظر خود اعمال کنید



شکل ۸- ۳۸ Remote Desktop

۸-۳-٤ بررسی Firewall در ویندوز سرور

فایروال ویندوز (Windows Firewall) یک ابزار امنیتی داخلی در سیستم‌عامل ویندوز است که وظیفه‌ی کنترل و مدیریت ترافیک ورودی و خروجی شبکه را بر عهده دارد. این ابزار به شما کمک می‌کند تا ارتباطات ناخواسته یا خطرناک را مسدود کنید و امنیت سیستم خود را افزایش دهید.

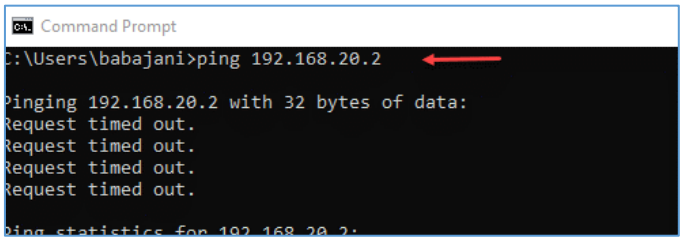
قبل از اینکه سرویس فایروال را بررسی کنیم، نرم‌افزار CMD را اجرا کنید و دستور زیر را در آن وارد کنید.

```
Ping 192.168.20.2
```

اگر به شکل ۸-۳۹ توجه کنید دستور Ping به سرور مجازی با پیام Request Timout روبرو شده است، یعنی اینکه پروتکل ICMP بر روی سرور توسط فایروال بسته شده است، اما نکته مهم این است که توانستین به سرور Remote بزنید و این به خاطر این است که زمانی که سرویس Remote Desktop را فعال

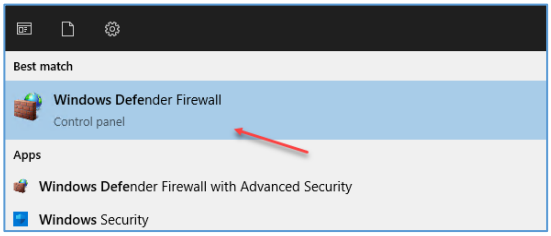
www.takbook.com

می‌کنید، تنظیمات مشخص در فایروال به صورت اتوماتیک ایجاد می‌شود، البته می‌توانید تنظیمات را به طریقی انجام دهید که پروتکل ICMP هم برای دستور Ping فعال شود.



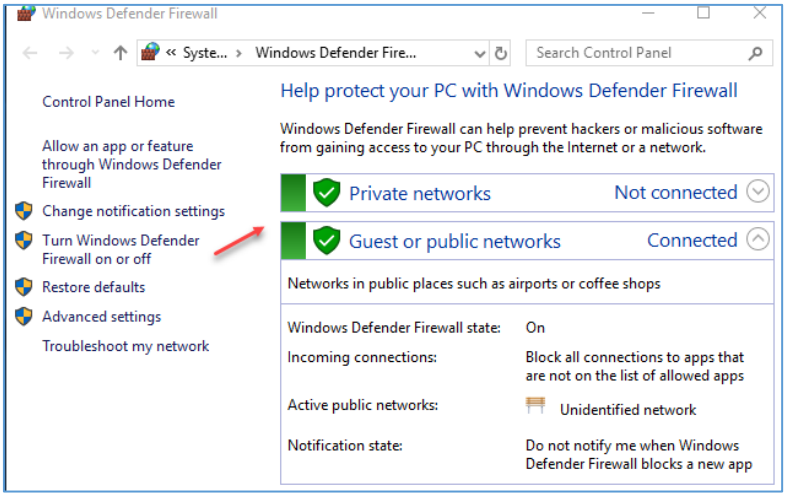
شکل ۸- ۳۹ دستور *Ping*

در ویندوز سرور ۲۰۲۵ به مانند شکل ۸–۴۰، بر روی Start کلیک کنید و سرویس Firewall را اجرا کنید.



شکل ۸- ۴۰اجرای فایروال

طبق شکل ۸–۴۱، اصولاً فایروال از سه قسمت Private، Guest و Domain تشکیل شده است که قسمت Domain زمانی که سرویس Active Directory را راه‌اندازی کردیم و سیستم‌ها را عضو دومین کردیم در این قسمت ظاهر خواهد شد.



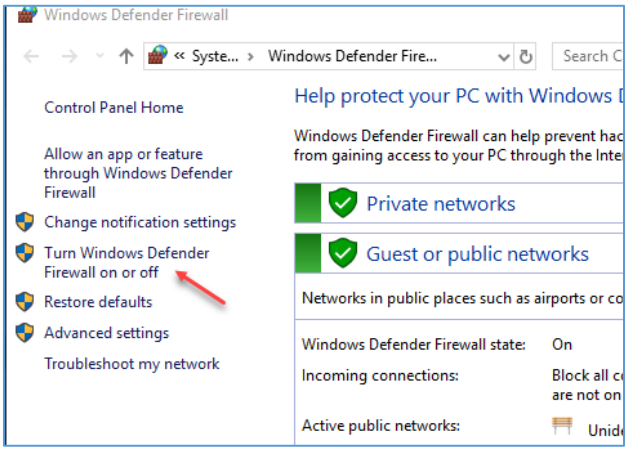
شکل ۸- ۴۱ فایروال ویندوز

قبل از بررسی سرویس فایروال بهتر است سه پروفایل Private,Guest,Domain را توضیح دهیم:

www.takbook.com

- **Domain Profile** (پروفایل دامین): این پروفایل زمانی فعال می‌شود که دستگاه عضو یک دامین باشد و به شبکه‌ای متصل شود که به عنوان دامین شناخته شده است و بیشتر برای شبکه‌های کاری یا سازمانی طراحی شده است که به دامین کنترلر دسترسی دارند و همچنین امنیت معمولاً پایین‌تر است، زیرا فرض می‌شود که شبکه قابل اعتماد است.
- **Private Profile** (پروفایل خصوصی): این پروفایل برای شبکه‌هایی طراحی شده که کاربر آن‌ها را خصوصی مشخص می‌کند، مثل شبکه خانگی یا شبکه دفاتر کوچک و باید به این نکته توجه کنید که امنیت متوسط دارد و به برخی از ارتباطات ورودی (مانند دستگاه‌های پرینتر یا فایل شیرینگ) اجازه می‌دهد، فرض بر این است که شبکه نسبتاً ایمن است، اما نه به اندازه شبکه دامین.
- **Public Profile** (پروفایل عمومی): این پروفایل برای شبکه‌های عمومی، مانند کافی‌شاپ‌ها، فرودگاه‌ها یا شبکه‌های عمومی Wi-Fi طراحی شده است، امنیت در این پروفایل بالا است و اکثر ارتباطات ورودی مسدود می‌شوند و فرض بر این است که شبکه غیرقابل اعتماد است.

اکثر مدیران و دوستان IT برای اینکه خیال خود را در شبکه راحت کنند فایروال را به طور کل خاموش می‌کنند که کار بسیار اشتباهی است. اگر بخواهید این کار را انجام دهید به مانند شکل ۸-۴۲ بر روی Turn Windows Defender Firewall on or off کلیک کنید.

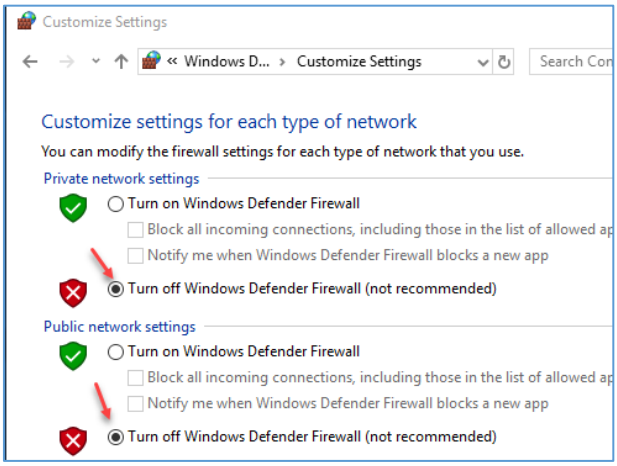


شکل ۸- ۴۲ فایروال ویندوز

درشکل ۸-۴۳ می‌توانید با انتخاب گزینه‌های مشخص شده فایروال را به صورت کامل خاموش کنید که با این کار همه‌ی راه‌های ارتباطی با ویندوز سرور باز خواهد شد، هر چند این موضوع کار شما را آسوده خواهد کرد ولی راهی را برای ورود افراد غیرمجاز باز می‌کند و بهتر است که فایروال را خاموش نکنید

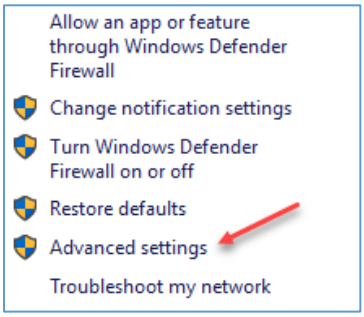
www.takbook.com

و آن را به درستی تنظیم کنید، هر چند فایروال مایکروسافت به نسبت دیگر فایروال‌های موجود در بازار خیلی ضعیف‌تر است ولی به قول معروف لنگه کفشی در بیابان نعمت است.



شکل ۸- ۴۳ فایروال ویندوز

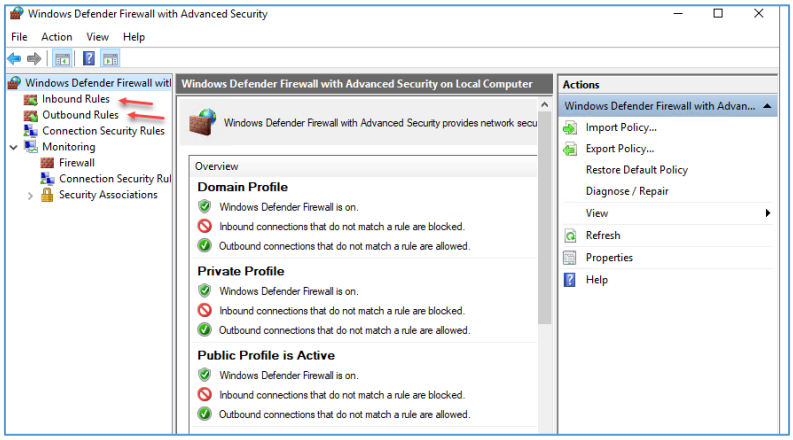
اما اگر بخواهید بیشتر روی فایروال تمرکز کنیم به مانند شکل ۸-٤٤ بر روی Advanced Settings کلیک کنید.



شکل ۸- ۴۴ فایروال ویندوز

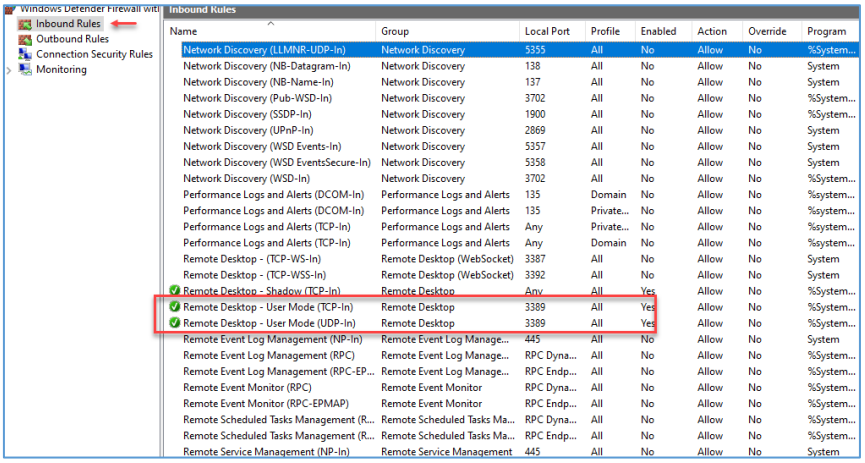
در ۸-٤٥ اطلاعات کاملتری از Firewall را مشاهده می‌کنید، همیشه این موضوع را در نظر داشته باشید که فایروال دارای یک ورودی (Inbound) و یک خروجی (outbound) است که شما می‌توانید با استفاده از Rule به ارتباطات خاص دسترسی Deny و Permit دهید.

www.takbook.com



شکل ۸- ۴۵ فایروال ویندوز

اگربه شکل ۸-٤٦ دقت کنید وارد قسمت Inbound Rules شدیم و در این قسمت گزینه‌ی Remote Desktop را مشاهده می‌کنید که بعد از اینکه سرویس را فعال کردیم در این قسمت به صورت اتوماتیک، Rule مورد نظر آن ایجاد شده است، به همین صورت شما هم می‌توانید دسترسی‌های لازم را برای دیگر سرویس‌ها و پورت‌ها فعال کنید.



شکل ۸- ۴۶ فایروال ویندوز

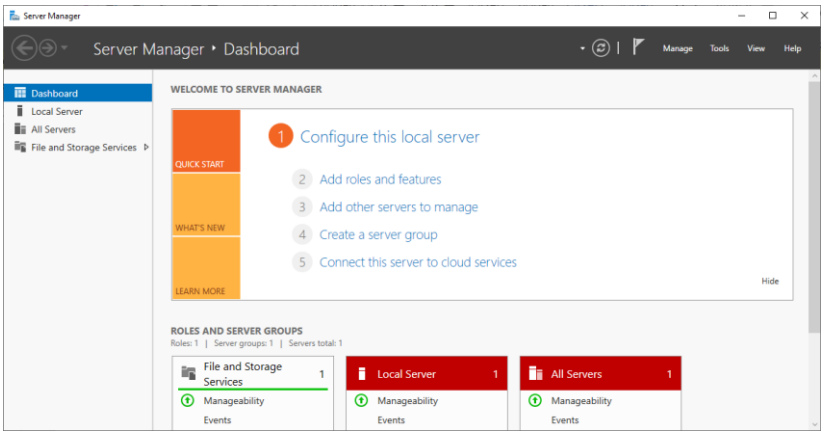
۸-۳-۵ بررسی سرویس‌های ویندوز سرور 2025

ویندوز سرور ۲۰۲۵ شامل مجموعه‌ای از سرویس‌ها و ابزارها است که برای مدیریت شبکه، ذخیره‌سازی، امنیت، و مجازی‌سازی طراحی شده‌اند. در ادامه، سرویس‌ها و ابزارهای کلیدی معرفی می‌شوند.

بعد از نصب ویندوز و وارد شدن به آن اولین چیزی که اجرا می‌شود Server Manager است که در این سرویس تمام امکانات ویندوز سرور وجود دارد و می‌توانید به راحتی آنها را پیاده‌سازی کنید.

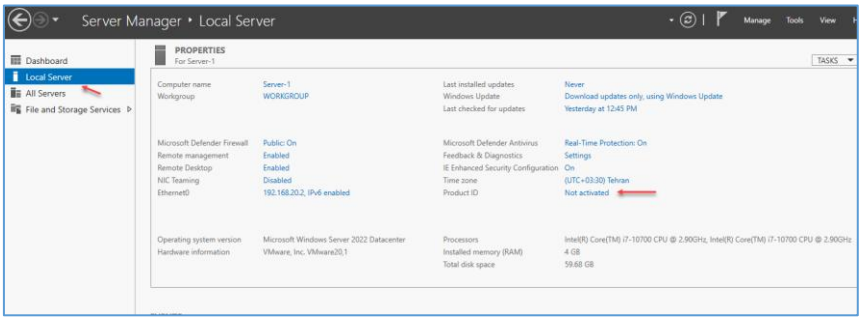
www.takbook.com

همان‌طور که در شکل ۸–۴۷، مشاهده می‌کنید، Server Manager اجرا شده است، و می‌توانید با کلیک بر روی Add Roles and Features سرویس یا نقش مورد نظر خود را فعال کنید.



شکل ۸– ۴۷ *Server Manager*

اگر به مانند شکل ۸–۴۸ وارد قسمت Local Server شوید یک نمای کلی از وضعیت سرور را مشاهده می‌کنید، مثلاً در قسمت Product ID گزینه‌ی Not activated نوشته شده است که باید لایسنس ویندوز سرور را فعال کنید.

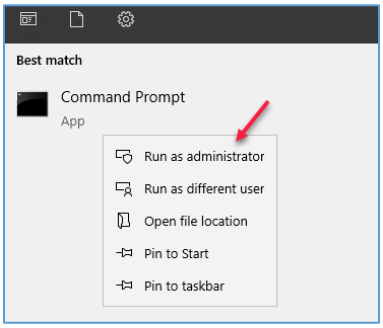


شکل ۸– ۴۸ *Server Manager*

بهترین روش فعال‌سازی ویندوز سرور در ایران برای ویندوزهای مختلف این است که از دوستانمان در سایت Digiboy.ir کمک بگیریم.

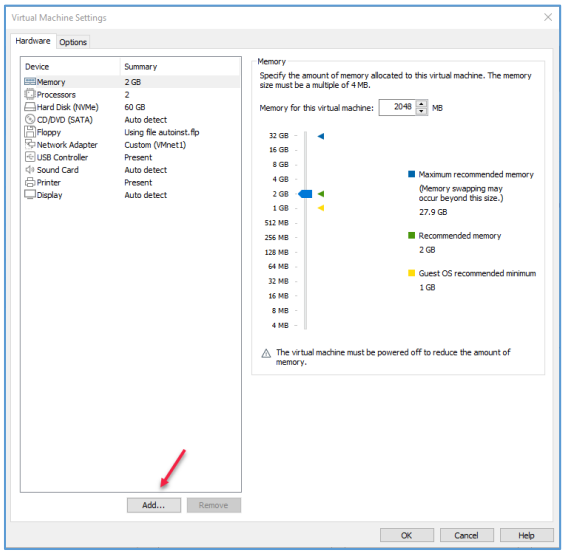
برای انجام این کار وارد Start شوید و نرم‌افزار CMD را با حداکثر دسترسی (Run as administrator) اجرا کنید که در شکل ۸–۴۹ مشخص شده است.

www.takbook.com



شکل ۸- ۴۹ *Server Manager*

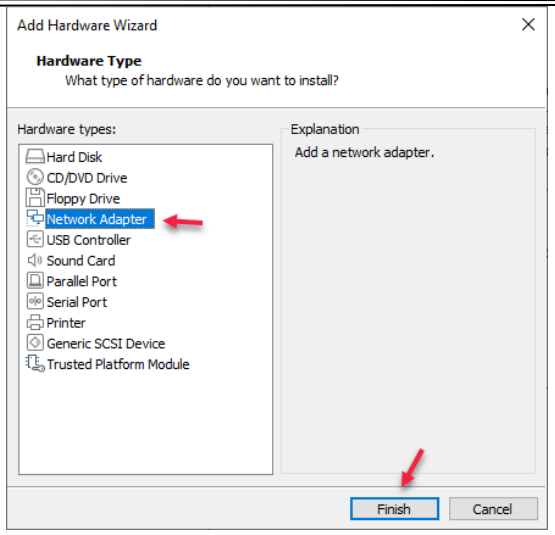
به این نکته توجه کنید که سرور شما باید دارای اینترنت باشد و برای این کار وارد نرم‌فزار VMware Workstation شوید و بر روی ماشین مجازی خود کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید. به مانند شکل ۸-۵۰ بر روی Add کلیک کنید.



شکل ۸- ۵۰ تنظیمات *Virtual Machine*

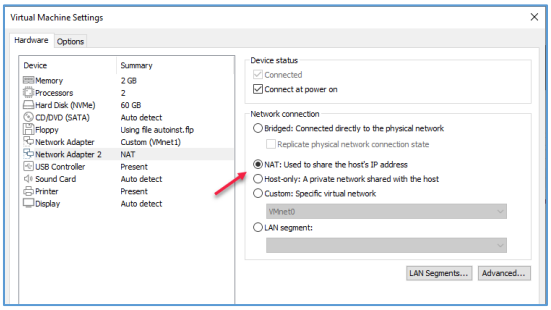
در ادامه چون ما یک کارت شبکه از قبل داشتیم و بر روی آن آدرس IP قرار دادیم بهتر است یک کارت شبکه‌ی دیگر با نوع NAT اضافه کنیم تا اینترنت بر روی سرور فعال شود، پس به مانند شکل ۸-۵۱ Network Adapter را انتخاب و بر روی Finish کلیک کنید.

www.takbook.com



شکل ۸- ۵۱ تنظیمات *Virtual Machine*

در شکل ۸-۵۲ گزینه‌ی NAT را انتخاب و بر روی OK کلیک کنید.



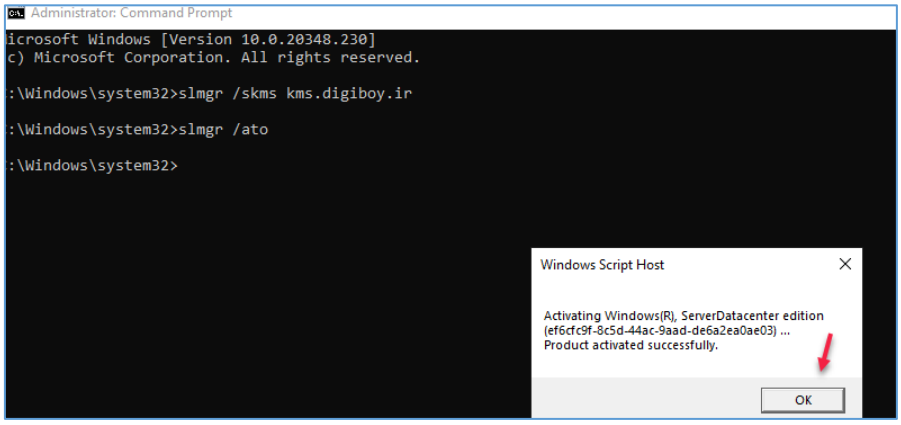
شکل ۸- ۵۲ تنظیمات *Virtual Machine*

بعد از انجام مراحل حالا اینترنت از سیستم اصلی شما وارد سرور مجازی (Server-1) شده است که باید دو دستور زیر را پشت سر هم اجرا کنید:

```
slmgr /skms kms.digiboy.ir
slmgr /ato
```

بعد از اجرای دومین دستور کمی صبر کنید تا شکل ۸-۵۳، ظاهر شود، با دیدن این شکل متوجه خواهید شد که سرور را به درستی اکتیو شده است.

www.takbook.com

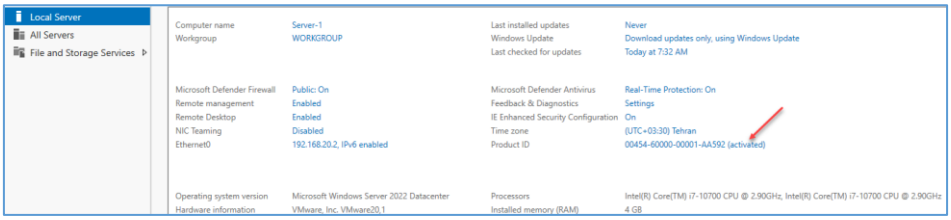


شکل ۸- ۵۳ فعال‌سازی ویندوز

نکته مهم: در آخر کار دوباره وارد تنظیمات ماشین مجازی مورد نظر شوید و آن کارت شبکه جدید که اضافه کرده بودید را حذف کنید.

راه دیگری هم برای اکتیو کردن وجود دارد و آن هم استفاده از نرم‌افزارهای Active که در سایت‌ها ایرانی موجود و به راحتی سرور را بدون نیاز به اینترنت اکتیو می‌کند اما روشی که در اینجا گفتیم کیفیت بهتری خواهد داشت.

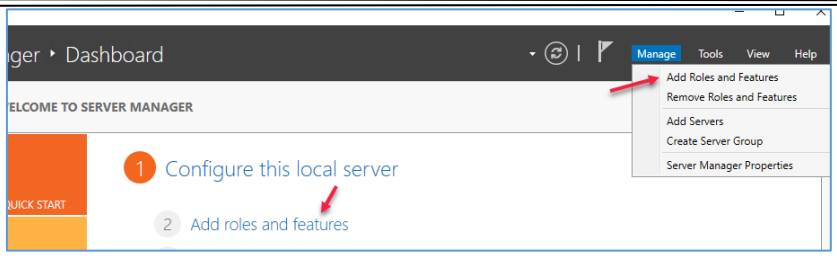
بعد از اینکه Active انجام شد دوباره وارد Server Manager شوید و به مانند شکل ۸-٥٤ و در قسمت Product-ID فعال بودن ویندوز سرور را مشاهده خواهید کرد.



شکل ۸- ۵۴ فعال‌سازی ویندوز

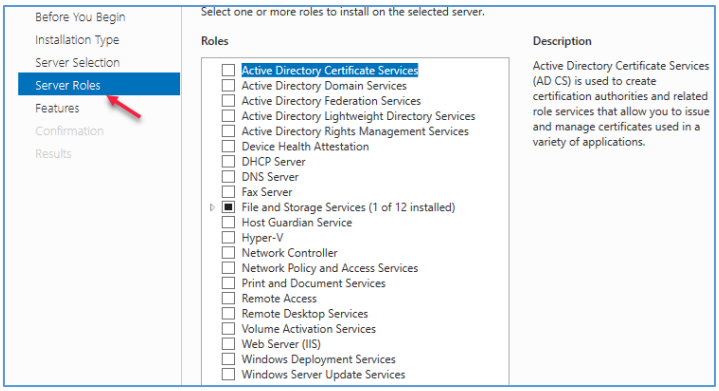
در ادامه کار می‌خواهیم سرویس‌هایی که در ویندوز سرور ارائه می‌شوند را با هم یک بررسی کلی داشته باشیم، برای این کار به مانند شکل ۸-۵۵ از قسمت Dashboard بر روی Add roles and features کلیک کنید.

www.takbook.com



شکل ۸- ۵۵ بررسی سرویس‌ها

در شکل ۸-۵۶ لیست کامل سرویس‌های اصلی ویندوز سرور ۲۰۲۵ را مشاهده می‌کنید که انشاالله در این کتاب به طور کامل آنها را بررسی خواهیم کرد.



شکل ۸- ۵۶ سرویس های ویندوز سرور ۲۰۲۵

برای اینکه به صورت منظم این سرویس‌ها را بسته به نیاز خود بررسی کنیم بهتر است طبق کتاب پیش بروید.

در زیر لیستی از سرویس‌هایی که در این کتاب بررسی خواهیم کرد را معرفی می‌کنیم که البته شاید سرویس‌های اضافه‌تری را هم توضیح دهیم.

- Active Directory (AD)

  این سرویس برای مدیریت کاربران، گروه‌ها و دستگاه‌ها در شبکه به کار می‌رود.
- DNS Server

  مدیریت نام‌های دامنه در شبکه و ترجمه نام‌ها به آدرس‌های IP.
- DHCP Server

  تخصیص خودکار آدرس‌های IP به دستگاه‌ها در شبکه.
- File and Storage Services

  مدیریت ذخیره‌سازی فایل‌ها و داده‌ها با پشتیبانی از سیستم فایل مقاوم (ReFS) و قابلیت حذف فایل‌های تکراری.
- Hyper-V

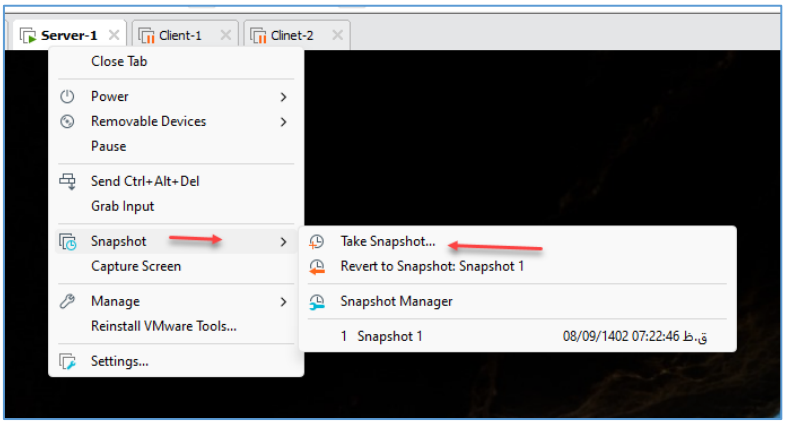
www.takbook.com

مجازی‌سازی سرورها و امکان اجرای ماشین‌های مجازی با بهبودهای جدید در مدیریت GPU و پردازنده‌ها.

- Remote Desktop Services (RDS)
  فراهم‌کردن دسترسی از راه دور به دسکتاپ‌ها و برنامه‌های ویندوز.
- Web Server (IIS)
  میزبانی برنامه‌های وب و سایت‌های اینترنتی.
- Windows Deployment Services (WDS)
  نصب و توزیع سیستم‌عامل ویندوز روی دستگاه‌های شبکه.
- Print and Document Services
  مدیریت چاپگرها و سرورهای چاپ.
- Network Policy and Access Services (NPAS)
  مدیریت دسترسی به شبکه و نظارت بر سیاست‌های شبکه.
- Failover Clustering
  پشتیبانی از دسترسی بالا و بازیابی سریع در صورت خرابی سیستم.
- Windows Admin Center
  ابزار مدیریت گرافیکی برای نظارت و مدیریت سرور.

اولین سرویسی که باید در شبکه با آن مواجه شویم سرویس کاربردی DNS است که شما در حالت عادی وقتی در اینترنت وبگردی می‌کنید بسیار زیاد از آن استفاده می‌کنید که البته چیزی از این سرویس را حس نمی‌کنید.

نکته مهم: قبل اینکه سرویس DNS را توضیح دهیم و نصب کنیم، بهتر است یک SnapShot از ماشین مورد نظر خود بگیرید، برای این کار به مانند شکل ۸–۵۷، بر روی ماشین مورد نظر کلیک راست کنید و از قسمت Snapshot بر روی Take Snapshot کلیک کنید تا یک نسخه از ویندوز را قبل از هر کاری داشته باشید و در موقع نیاز به همین تاریخ بر می‌گردیم.

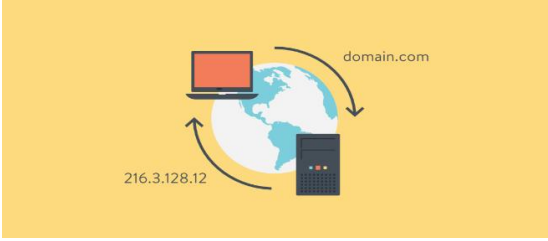


شکل ۸–۵۷ Snapshot

www.takbook.com

۸-۳-۶ سرویس DNS

DNS(Domain Name System)، 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.



شکل ۸- ۵۸ سرویس DNS

سرویس DNS (Domain Name System) یکی از اجزای اساسی اینترنت است که وظیفه‌اش تبدیل نام‌های دامنه (مثل www.example.com) به آدرس‌های IP (مثل 192.0.2.1) است. این فرآیند به ما کمک می‌کند تا به راحتی و با استفاده از نام‌های قابل فهم به وب‌سایت‌ها و سرورها دسترسی پیدا کنیم.

اصول کار DNS:

- پرس و جو: وقتی شما یک آدرس وب را در مرورگر وارد می‌کنید، دستگاه شما به یک سرور DNS درخواست می‌فرستد.
- پاسخ: سرور DNS بررسی می‌کند که آیا آدرس IP مربوط به آن دامنه را در حافظه‌اش دارد یا نه. اگر ندارد، درخواست را به سرورهای دیگر DNS ارسال می‌کند.
- دریافت آدرس IP: در نهایت، آدرس IP به دستگاه شما بازگردانده می‌شود و مرورگر شما می‌تواند به وب‌سایت مورد نظر متصل شود.

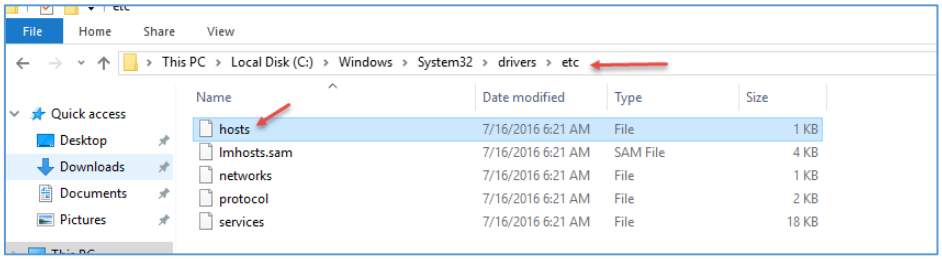
مزایای DNS:

- دسترس‌پذیری: نام‌های دامنه به یادآوری آسان‌تر از آدرس‌های عددی هستند.
- مدیریت: امکان تغییر آدرس IP یک دامنه بدون تغییر نام آن.
- توزیع بار: با استفاده از DNS، می‌توان ترافیک را به چند سرور مختلف تقسیم کرد.

۸-۳-۶-۱ بررسی فایل HOSTS در ویندوز

فایلی با نام Hosts 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.

www.takbook.com



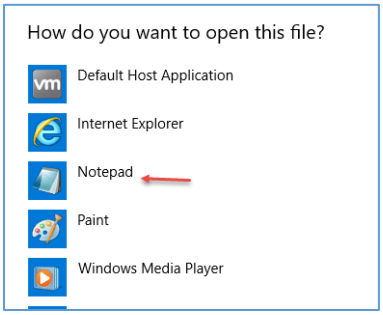
شکل ۸- ۵۹ فایل Hosts

به مانند شکل ۸-۵۹ 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 دو بار کلیک کنید تا شکل ۸-۶۰ ظاهر شود و توسط Notepad، فایل مورد نظر را باز کنید تا بتوانید فایل را ویرایش کنید.



شکل ۸- ۶۰ فایل Hosts

در شکل ۸-۶۱، اطّلاعات درون فایل hosts را مشاهده می‌کنید که برای اینکه به شما کمک کند، مثالی از آدرس‌های DNS را به شما معرّفی کرده است.

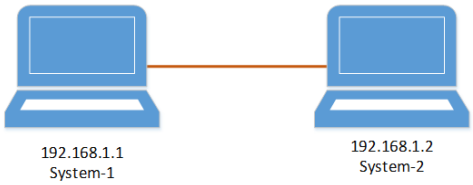
```
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

شکل ۸- ۶۱ فایل Hosts

www.takbook.com

در شکل ۸–۶۲، یک مثال را بررسی می‌کنیم و عملکرد آن را مشاهده می‌کنیم.



شکل ۸- ۶۲ بررسی DNS داخلی

در شکل ۸–۶۲، دو سیستم را مشاهده می‌کنید که هر دو با هم، شبکه شده‌اند، به صورت پیش‌فرض، این دو سیستم می‌توانند همدیگر را از 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 شکل ۸–۶۱، 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 ۸–۶۳، 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.

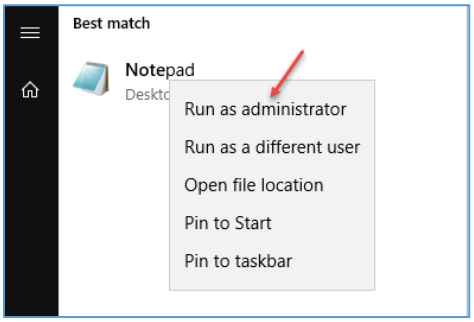
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
192.168.1.2         system-2
```

شکل ۸- ۶۳ بررسی فایل hosts

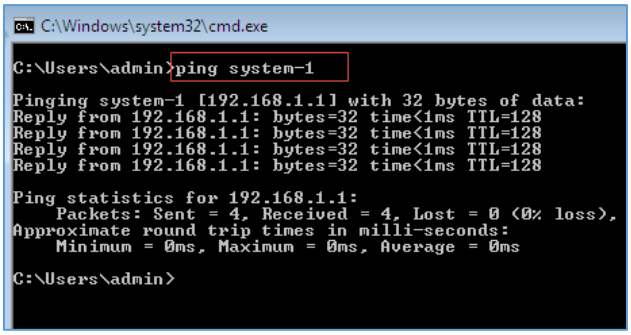
www.takbook.com

نکته‌ی مهم: در بعضی از سیستم‌ها به علّت اینکه دسترسی‌ها محدودتر هستند، نمی‌توانید به طور مستقیم اطلاعات 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 شکل ۸-٦٤، 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، یا اینکه می‌توانید فایل را بر روی Desktop کپی کنید و بعد از اینکه ویرایش مورد نظر را انجام دادید آن را در محل اصلی قرار دهید.



شکل ۸- ۶۴ بررسی فایل hosts

همان‌طور که در شکل ۸-٦٥ مشاهده می‌کنید، با این کار توانستید دو سیستم در یک شبکه workgroup را با استفاده از نام به هم متّصل کنید.



شکل ۸- ۶۵ بررسی فایل hosts

به مانند شکل ۸-٦٦، system-1 با دستور Ping بررسی شده که این کار با موفّقیّت انجام شده است.

به این نکته توجه کنید که وقتی سیستم عامل ویندوز را نصب می‌کنید، تمام سیستم ها به صورت پیش‌فرض عضو شبکه‌ی Workgroup هستند، اگر بخواهیم یک تعریف کلی از شبکه‌های Workgroup داشته باشیم باید گفت که این شبکه‌ها از مجموعه‌ای سیستم تشکیل شده‌اند که دارای سیستم عامل ویندوز هستند و از طریق شبکه می‌توانند اطلاعات را بین هم انتقال دهند ولی هر سیستم در این نوع شبکه مستقل

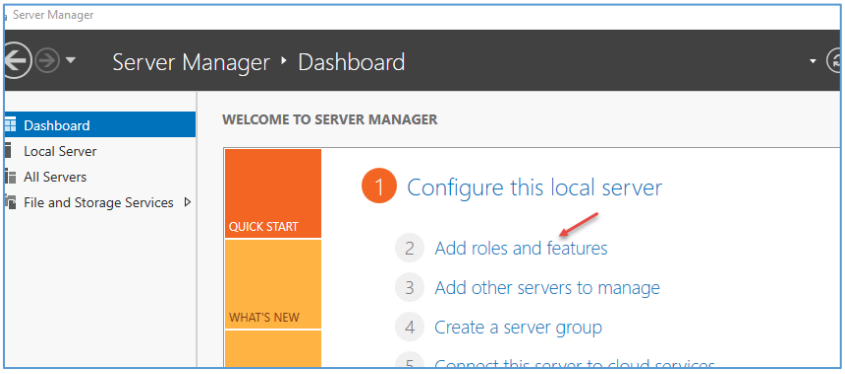
www.takbook.com

عمل می‌کند و هر کاری که نیاز باشد انجام می‌دهد و قابل کنترل نیستند که انشاالله در ادامه با معرفی Active Diectory این مشکل حل خواهد شد.

۸-۳-۶-۲ نصب و راه‌اندازی سرویس DNS

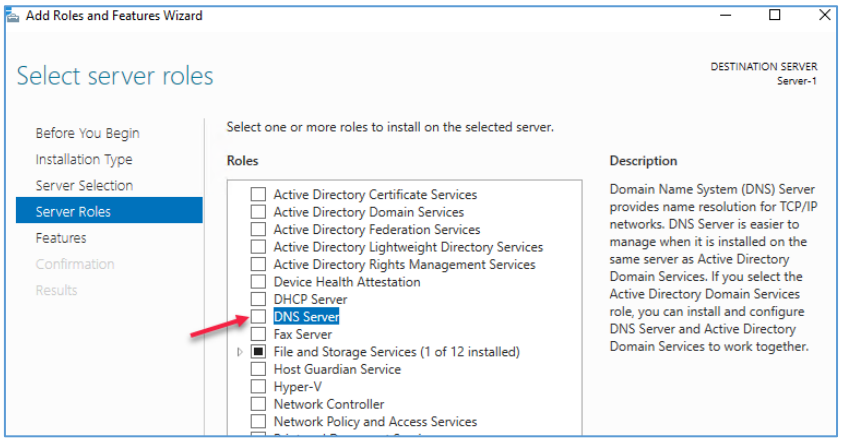
قبل از نصب این سرویس باید به این نکته اشاره کنم که در این بخش سرویس DNS نصب و امکانات آن مورد بررسی قرار می‌گیرد و بعد از اینکه آموزش به پایان رسید باید سرور را به حالت اول که Snapshot تهیه کردید برگردانید و یا اینکه سرویس DNS را پاک کنید، تا در ادامه با مشکل روبرو نشویم.

برای نصب سرویس DNS وارد ویندوز سرور شوید و Server Manager را اجرا کنید و در شکل ۸-۶۶ بر روی Add roles and features کلیک کنید.



شکل ۸- ۶۶ *Add roles and features*

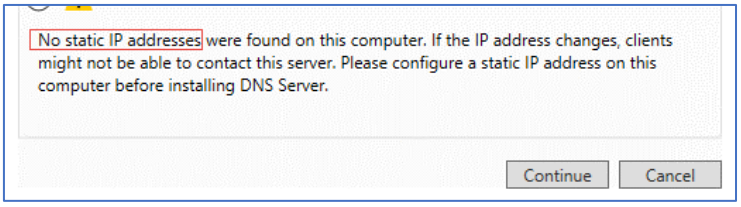
بر روی Next کلیک کنید تا به قسمت Server Roles برسید، به مانند شکل ۸-۶۷، بر روی DNS Servers کلیک کنید و در پنجره‌ی باز شده بر روی Add Features کلیک کنید.



شکل ۸- ۶۷ *Add roles and features*

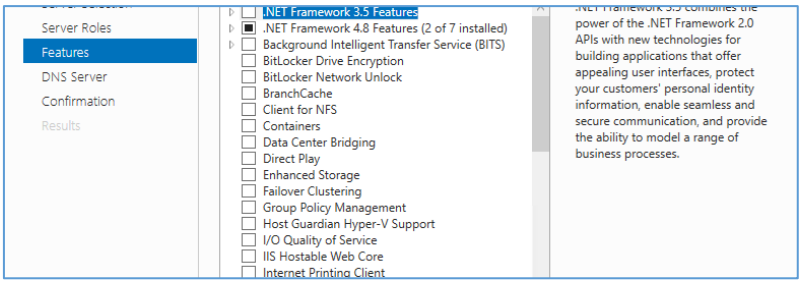
www.takbook.com

نکته: اگر بعد از کلیک بر روی Add Features با پیغام اخطار شکل ۸-۶۸، مواجه شدید، 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 که البته اگر طبق کتاب پیش رفته باشید این کار را در اوایل فصل انجام دادیم.



شکل ۸- ۶۸ آدرس‌دهی دستی

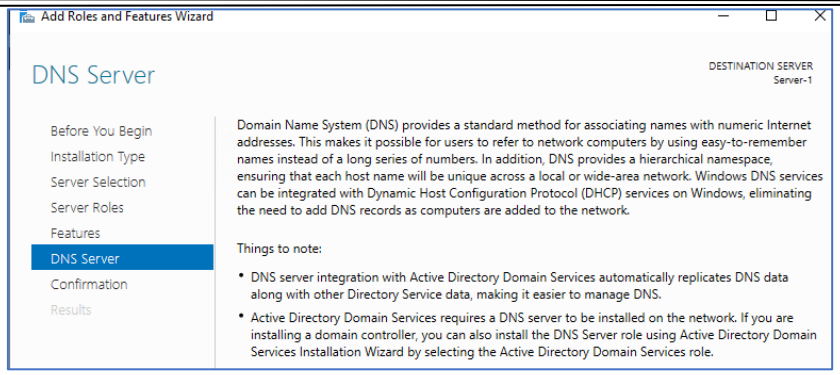
در ادامه کار به مانند شکل ۸-۶۹، فقط بر روی Next کلیک کنید.



شکل ۸- ۶۹ نصب سرویس *Active*

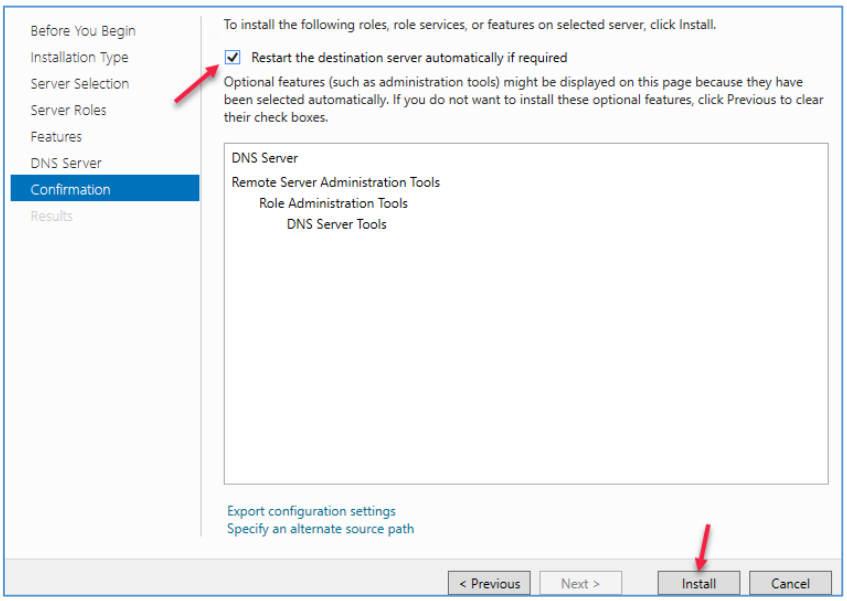
در شکل ۸-۷۰، توضیحاتی در مورد سرویس DNS داده شده است که به این موضوع اشاره دارد که سرویس DNS با سرویس‌های دیگر ویندوز مانند DHCP ، ActiveDirectory یکپارچه خواهد شد، مثلا اگر سیستمی به شبکه متصل شود به صورت اتوماتیک سرویس DHCP که در ادامه توضیح خواهیم داد به سیستم مورد نظر یک IP تخصیص خواهد داد و در همین مرحله نام و آدرس IP در سرویس DNS هم به صورت اتوماتیک ثبت خواهد شد.

www.takbook.com



شکل ۸- ۷۰ بررسی سرویس DNS

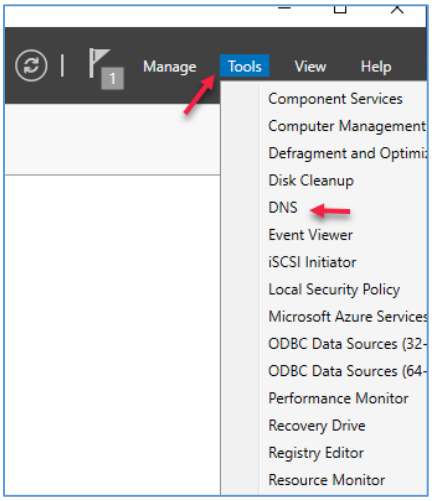
در شکل ۸–۷۱، باید تیک گزینه‌ی ...Restart را انتخاب و بر روی Install کلیک کنید.



شکل ۸- ۷۱ نصب سرویس DNS

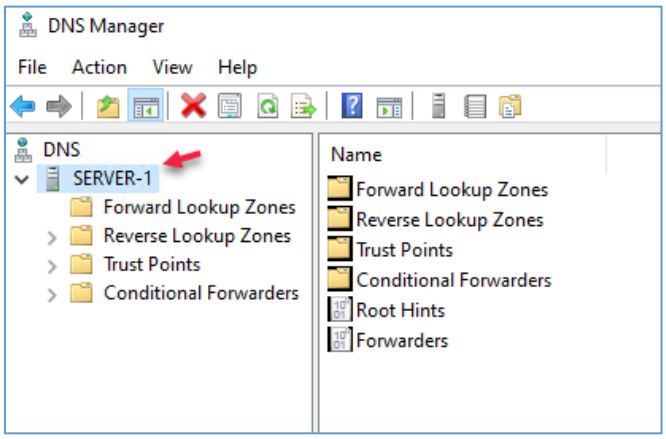
بعد از نصب در صورت نیاز سیستم Restart خواهد شد وگرنه می‌توانید بر روی Close کلیک کنید و طبق شکل ۸–۷۲، سرویس DNS را از طریق منوی Tools در Server Manager اجرا کنید و یا اینکه کلمه DNS را جستجو کنید.

www.takbook.com



شکل ۸- ۷۲ سروس DNS

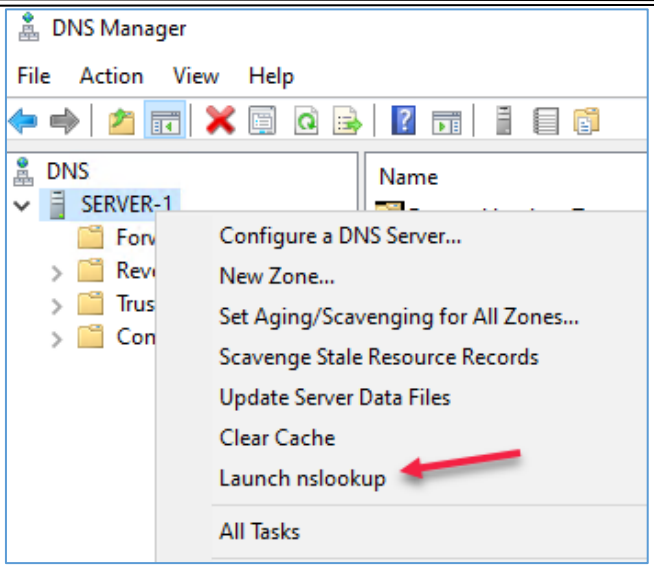
در شکل ۸-۷۳، سرویس DNS را مشاهده می‌کنید، این سرویس از قسمت‌های مختلفی تشکیل شده است.



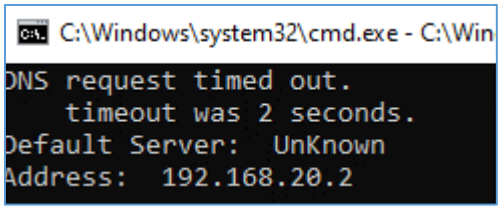
شکل ۸- ۷۳ سروس DNS

اگر به مانند شکل ۸-۷٤، بر روی نام سرور خود کلیک راست کنید و فرمان nslookup را اجرا کنید باید خروجی شما شبیه به شکل ۸-۷۵ باشد.

www.takbook.com



شکل ۸- ۷۴ سرویس DNS



شکل ۸- ۷۵ سرویس DNS

دستور nslookup برای مشخص کردن نام و آدرس IP سروری که درون آن هستیم به کار می‌رود به همراه سرور DNS اصلی است که در شکل ۸-۷۵، با خطا روبرو شده و این به خاطر تنظیم نبودن سرویس DNS است.

برای انجام تنظیمات در DNS دو گزینه‌ی مهم وجود دارد که در زیر آنها را بررسی می‌کنیم.

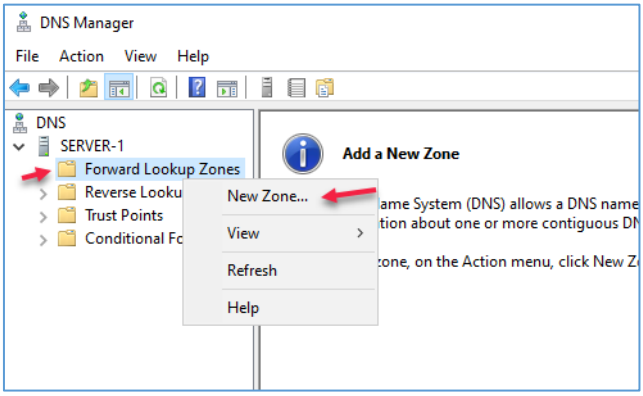
۸-۳-۶-۳ Forward Lookup Zones

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.

www.takbook.com

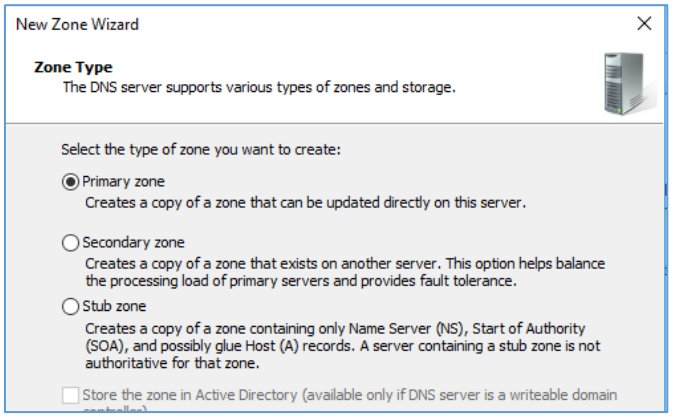
بر روی Forward Lookup Zones کلیک راست کنید و گزینه‌ی New Zone را به مانند شکل ۸-۷۶ انتخاب کنید.



شکل ۸-۷۶ *Forward Lookup Zones*

در شکل ۸-۷۷، سه گزینه را مشاهده می‌کنید، گزینه‌ی Primary zone، یک دیتابیس کلّی از همه‌ی اطّلاعات یک سرور است که 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.

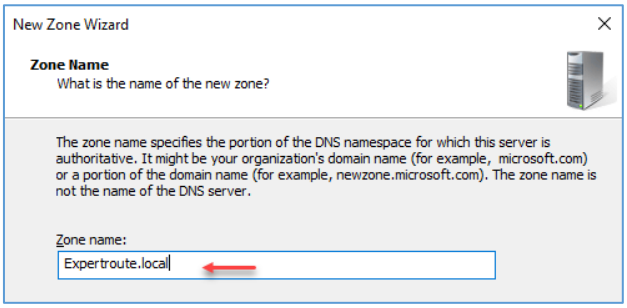


شکل ۸-۷۷ *Forward Lookup Zones*

www.takbook.com

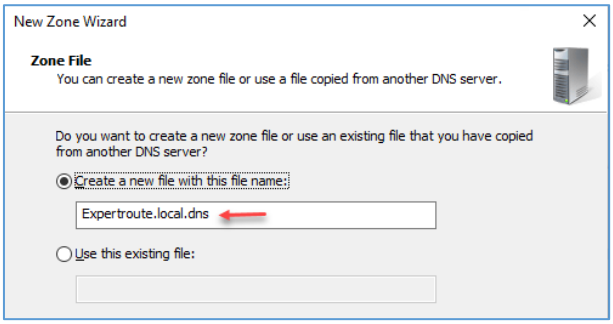
گزینه‌ی آخر، یعنی Stub zone، دقیقاً همان دیتابیس Secondary Zone است، با این تفاوت که هیچ تغییری نمی‌توانید در آن ایجاد کنید.

بعد از انتخاب گزینه‌ی Primary zone باید نام دومین خود را وارد کنید که در شکل ۸-۷۸، نام Expertroute.local را وارد کنید، شما می‌توانید هر اسم دیگری، مانند Google.com یا MSN.com وارد کنید، البتّه این دومین‌ها، تنها در شبکه‌ی داخلی اعتبار دارند؛ و اگر بخواهید در آینده به شبکه‌ی اینترنت متصل شوید با مشکل بزرگی روبرو خواهید شد. بر روی Next کلیک کنید.



شکل ۸-۷۸ *Forward Lookup Zones*

در شکل ۸-۷۹، 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 و از آن استفاده کنید.



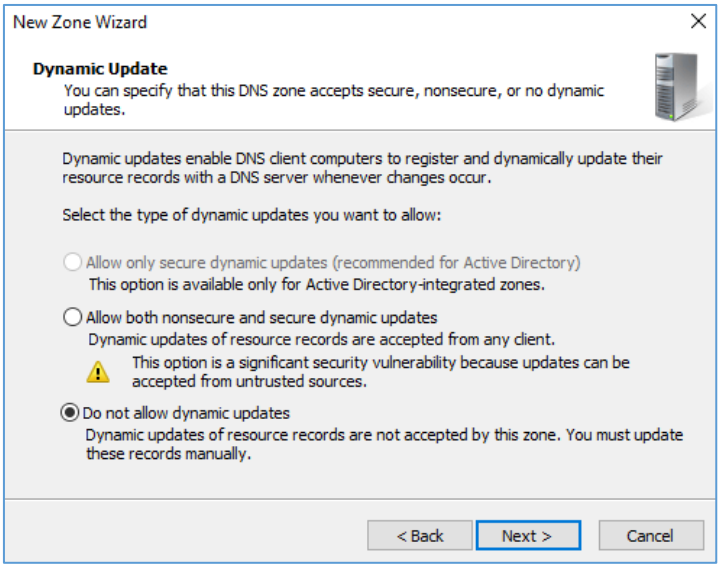
شکل ۸-۷۹ *Forward Lookup Zones*

در شکل ۸-۸۰، 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.

www.takbook.com

گزینه‌ی آخر را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۸۰ *Forward Lookup Zones*

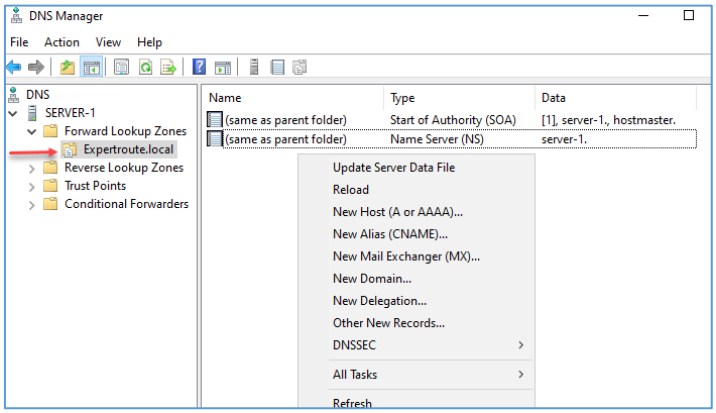
در صفحه‌ی آخر نیز بر روی Finish کلیک کنید تا دومین مورد نظر شما یا همان، Zone جدید ایجاد شود. به مانند شکل ۸-۸۱، اگر وارد Zone جدید خود با نام Expertroute.local شوید و در صفحه‌ی خالی کلیک راست کنید، چندین گزینه را مشاهده می‌کنید، گزینه‌ی New Host یا AAAA که در اصطلاح به آن A record نیزمی‌گویند، برای 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 Server-1 با استفاده از A Record ایجاد کردید و می‌خواهید یک نام دیگر نیز به سرور Server-1 اختصاص دهید، می‌توانید از این گزینه استفاده کنید. بهترین مورد استفاده از این گزینه را می‌توان در نرم‌افزار Skype For Business 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.

www.takbook.com

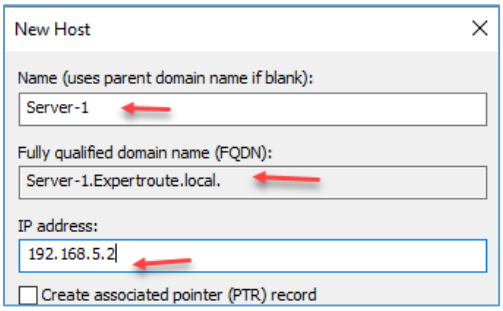
گزینه‌ی New domain نیز برای ایجاد یک Sub domain یا دومین زیرین دومین اصلی کاربرد دارد، مثلاً اگر نام دومین شما Expertroute.local باشد، با انتخاب این گزینه می‌توانید یک نام، مثلاً software به صورت Software.test.local ایجاد کنید و بعد از ایجاد آن می‌توانید نام سرورهای زیر مجموعه‌ی آن را وارد کنید. گزینه‌ی Other New Records، خود دارای چندین گزینه است که برای کارهای خاصّی ایجاد شده است که این مورد را در فصل پانزدهم بررسی خواهیم کرد.



شکل ۸-۸۱ *Forward Lookup Zones*

برای شروع کار می‌خواهیم نام سرور اصلی خود را اضافه کنیم برای این کار به مانند شکل ۸-۸۱، گزینه‌ی New Host (A) را انتخاب می‌کنیم.

به مانند شکل ۸-۸۲، در قسمت Name نام سرور (Server-1) را وارد کنید که در قسمت FQDN نام کامل سرور را به همراه نام دومینی که ایجاد کردیم مشاهده می‌کنید و در قسمت IP Address هم آدرس سرور را وارد می‌کنیم بعد از آن بر روی Add Host کلیک کنید تا رکورد مورد نظر ایجاد شود.



شکل ۸-۸۲ *Forward Lookup Zones*

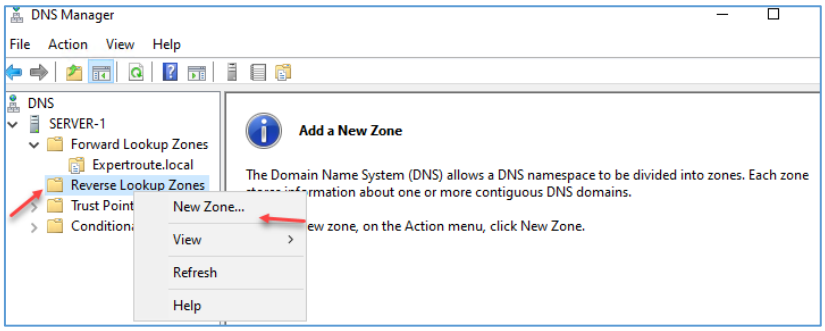
تا به اینجا، گزینه‌ی Forward Loolup Zones را بررسی کردیم که برای ایجاد Zone یا همان دومین شما کاربرد دارد و کار اصلی آن نیز تبدیل یک نام به آدرس IP است، یعنی اگر این سرویس فعّال نباشد و ما بخواهیم یک نام را در شبکه، Ping کنیم با مشکل مواجه خواهیم شد و این کار عملی نیست، اگر عملکرد

www.takbook.com

سرویس را فرا نگرفتید، نگران نباشید، چون در ادامه به صورت یک سناریوی واقعی بر روی آن بحث خواهیم کرد.

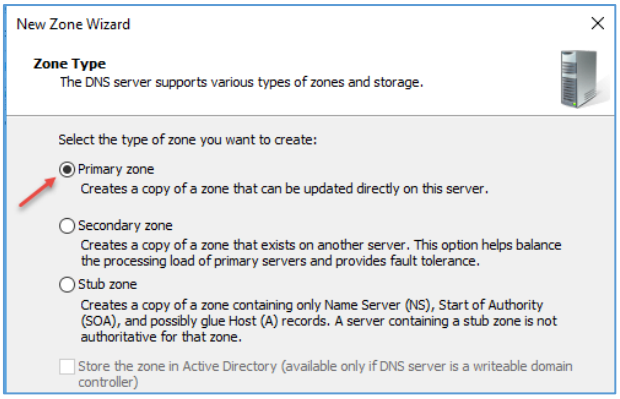
۸-۳-۶-٤ Revers Lookup zones

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 طبق شکل ۸-۸۳، بر روی Revers Lookup zones کلیک راست کنید و گزینه‌ی New Zone را انتخاب کنید.



شکل ۸-۸۳ *Revers Lookup zones*

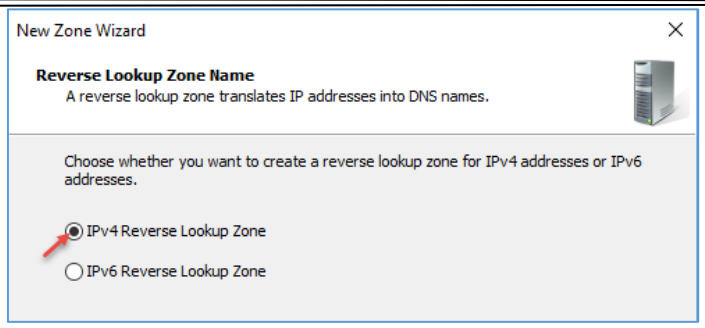
در شکل ۸-۸٤، که قبلاً توضیحات آن را بیان کردیم، گزینه‌ی Primary Zone را انتخاب و بر روی Next کلیک کنید.



شکل ۸-۸۴ *Revers Lookup zones*

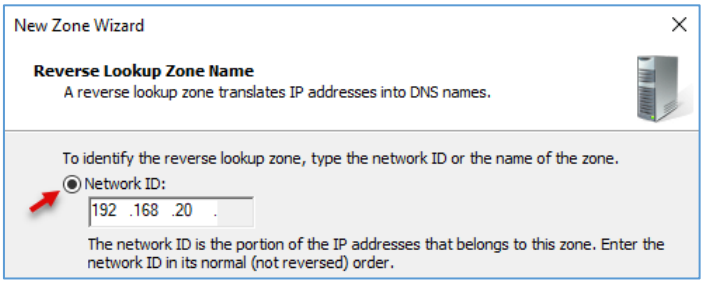
در شکل ۸-۸٤، باید ورژن IP مورد استفاده در شبکه‌ی خود را انتخاب کنید، در این قسمت IPv4 را انتخاب کنید.

www.takbook.com



شکل ۸- ۸۵ *Revers Lookup zones*

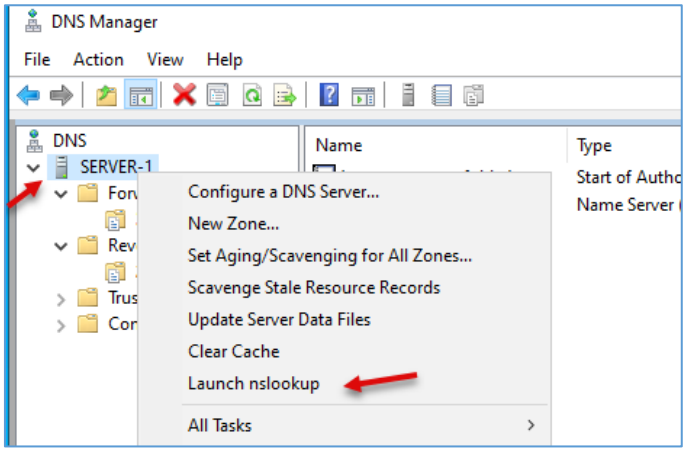
در شکل ۸-۸۶، باید Network ID خود را وارد کنید (192.168.20)، بر روی Next کلیک کنید.



شکل ۸- ۸۶ *Revers Lookup zones*

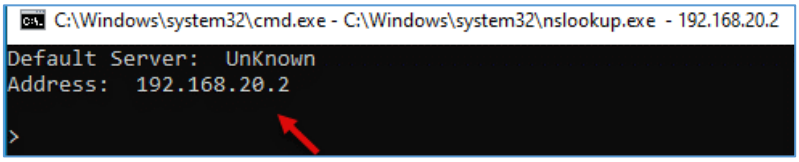
در صفحات بعد نیز بر روی Next کلیک کنید و در صفحه‌ی آخر بر روی Finish کلیک کنید.

اگر به مانند شکل ۸-۸۷، بر روی نام سرور کلیک راست کنید و گزینه‌ی Lunch Nslookup را انتخاب کنید، طبق شکل ۸-۸۸، خواهید شد که آدرس IP مورد نظر سرور بدون هیچ اسمی مشخص شده است و این بدان معنا است که تبدیل اسم به IP انجام نشده است.



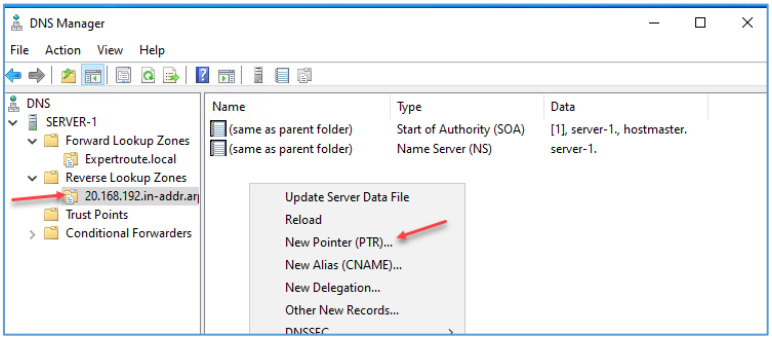
شکل ۸- ۸۷ *Revers Lookup zones*

www.takbook.com



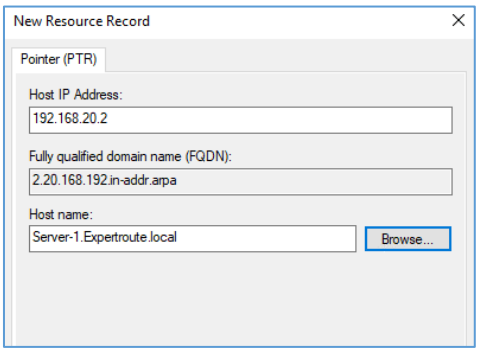
شکل ۸- ۸۸ *Revers Lookup zones*

برای حل این مشکل بعد از ایجاد Zone مربوط به Revers Lookup zones باید به مانند شکل ۸-۸۹، وارد Zone جدید در Reverse Lookup Zones شوید و با کلیک راست در جای مشخّص شده، گزینه‌ی New Pointer را انتخاب کنید.



شکل ۸- ۸۹ *Revers Lookup zones*

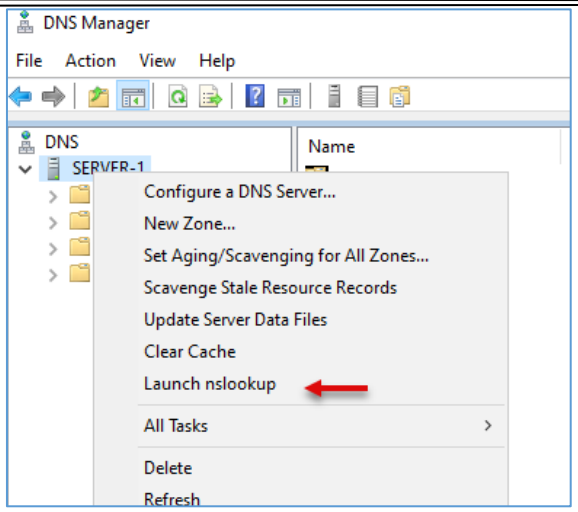
در شکل ۸-۹۰ باید بر روی Browse کلیک کنید و سرور مورد نظر را از قسمت Forward انتخاب کنید.



شکل ۸- ۹۰ *Revers Lookup zones*

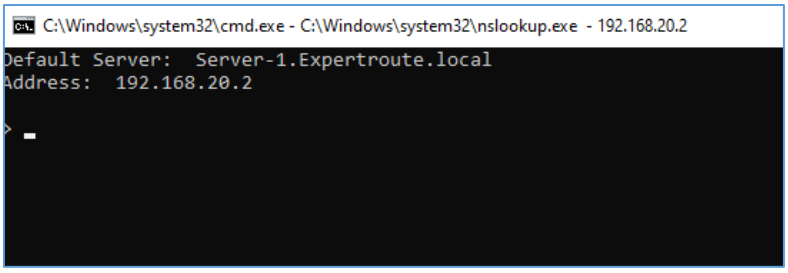
بعد از ایجاد PTR یا همان، New Pointer مانند شکل ۸-۹۱، بر روی سرور کلیک راست و گزینه‌ی Launch nslookup را انتخاب کنید.

www.takbook.com



شکل ۸- ۹۱ *Revers Lookup zones*

همان‌طور که در شکل ۸-۹۲، مشاهده می‌کنید نام سرور به همراه آدرس آن به درستی مشخص شده است.



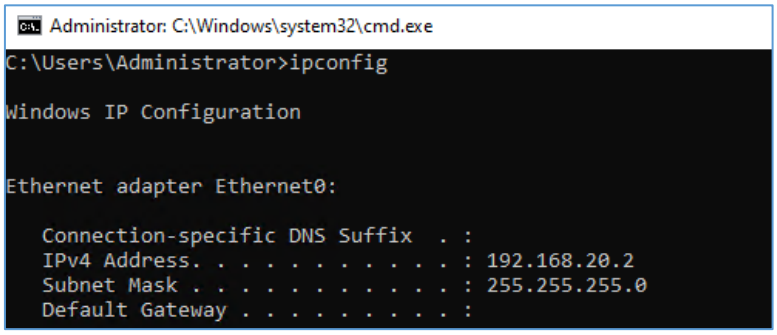
شکل ۸- ۹۲ *Revers Lookup zones*

توجه داشته باشید شما می‌توانید از دستور nslookup در CMD به صورت مجزا استفاده کنید.

دستورات دیگری برای بررسی آدرس IP وجود دارد که با هم در این قسمت بررسی می‌کنیم.

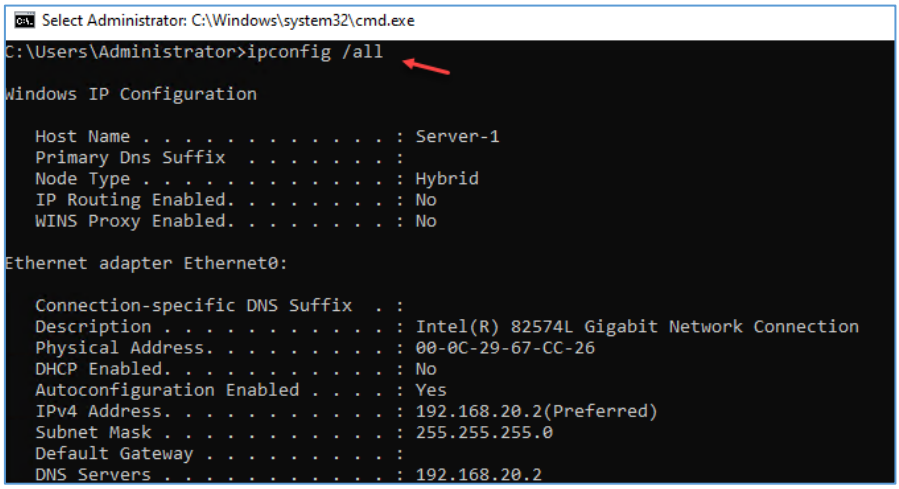
برای اینکه بتوانید مشخّصات کامل کارت شبکه را مشاهده کنید باید از دستور ipconfig استفاده کنید؛ در شکل ۸-۹۳، دستور ipconfig به تنهایی اجرا شده است و اطّلاعاتی از نام کارت شبکه که Ethernet0 است و آدرس IP، Subnet mask و Default Gateway برای شما مشخّص کرده است.

www.takbook.com



شکل ۸- ۹۳ *Revers Lookup zones*

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 ۸-۹٤، 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 در ادامه می‌توانید سرور DNS و... را ببینید، توجه داشته باشید آدرس DNS برای سرور اصلی DNS بر روی 127.0.0.1 قرار گرفته است.



شکل ۸- ۹۴ *Revers Lookup zones*

دستور ipconfig از سوئیچ‌های دیگری نیز برخوردار است، برای اینکه همه‌ی سوئیچ‌های مربوط به دستور ipconfig را بررسی کنیم، تنها کافی است از دستور ipconfig ? استفاده کنید؛ همان‌طور که در شکل ۸-۹۵ 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 بیشتر کار خواهیم کرد و برای شما به عنوان مدیر شبکه، کارآمد خواهد بود.

www.takbook.com


```
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.
```

شکل ۸- ۹۵ *Revers Lookup zones*

به عنوان مثال، اگر از دستور ipconfig /displaydns به مانند شکل ۸-۹۶ 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 با DNS داخلی است که در آدرس زیر قرار دارد:

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

```
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
```

شکل ۸- ۹۶ دستور *Ipconfig*

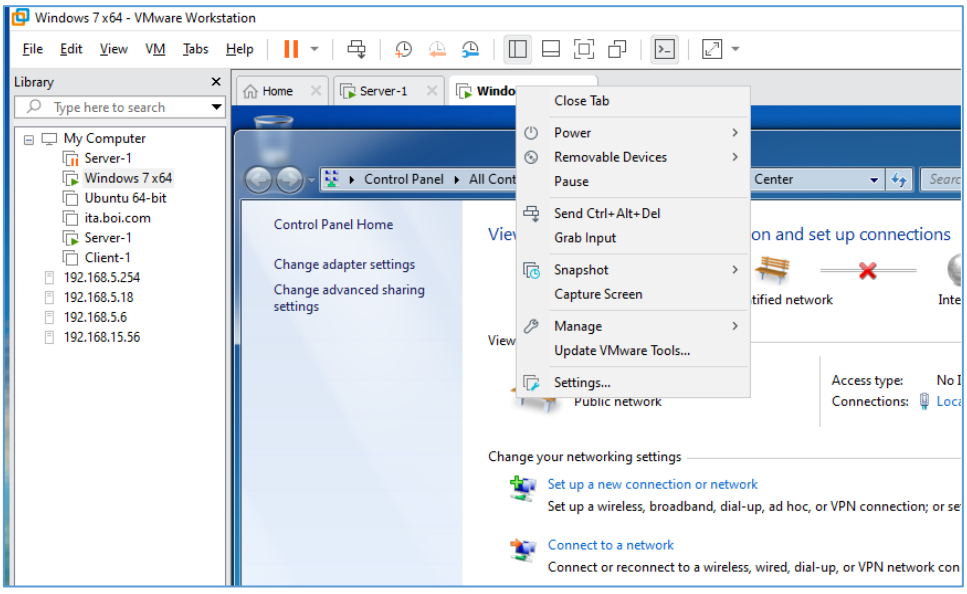
www.takbook.com

تا به اینجا، ویندوز سرور ۲۰۲۵ 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 می‌کنید با مشکل مواجه نشویم.

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 اطلاعات را دریافت کند.

برای اینکه با DNS بهتر کار کنیم می‌خواهیم یک کلاینت با ویندوز 7 را ایجاد کنیم و از طریق آن DNS سرور اصلی خود را بررسی کنیم.

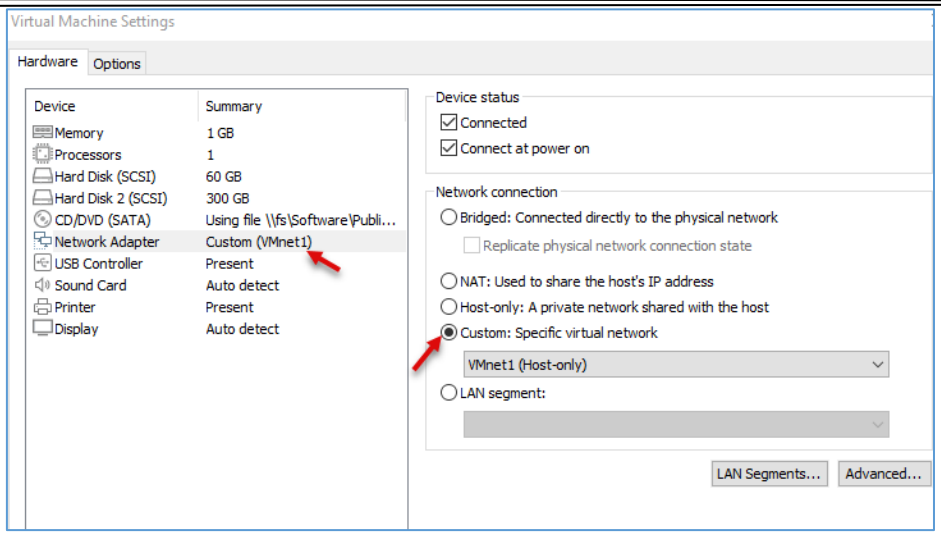
پس وارد نرم‌افزار VMware Workstation شوید و یک ماشین مجازی با ویندوز ۷ ایجاد و کارت شبکه‌ی مجازی آن را هم بر روی VMnet1 قرار دهید تا بتوانیم سرور خود را ببینیم، همان‌طور که در شکل ۸-۹۷ مشاهده می‌کنید ماشین مورد نظر ایجاد شده است و بعد از نصب و ورود به ویندوز باید آدرس IP آن را در رنج سرور اصلی قرار دهید که باید وارد تنظیمات کارت شبکه آن شوید، بر روی ماشین مجازی مورد نظر کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید.



شکل ۸-۹۷ ایجاد ماشین مجازی

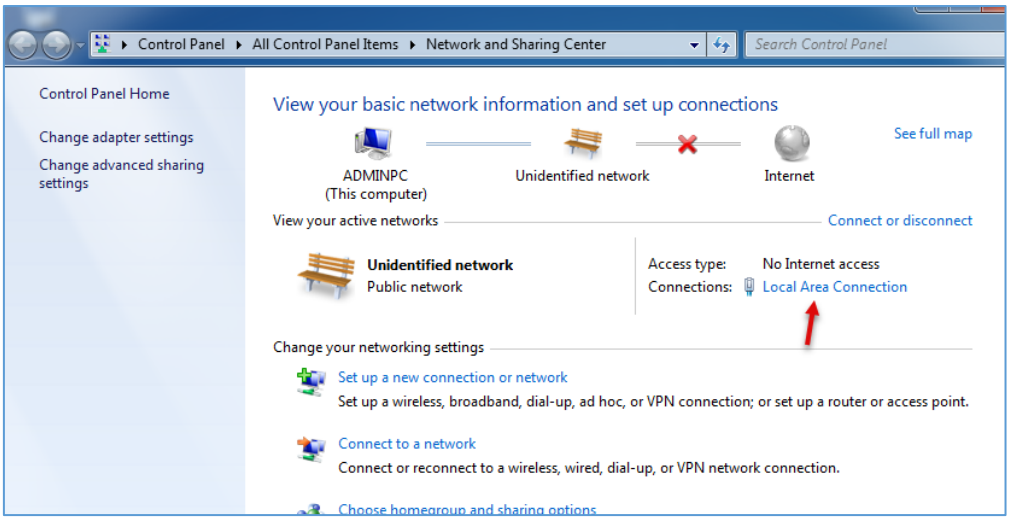
طبق شکل ۸-۹۸، کارت شبکه این ماشین را بر روی VMnet1 قرار دهید تا بتواند با سرور (Server-1) ارتباط برقرار کند.

www.takbook.com



شکل ۸- ۹۸ تنظیم کارت شبکه

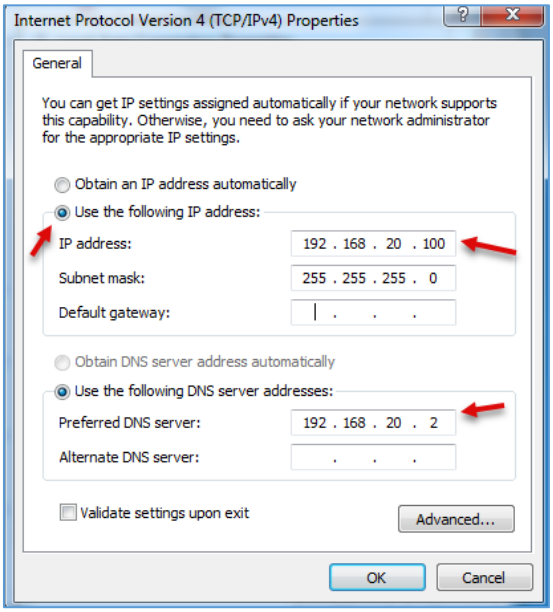
در ادامه بعد از ورود به ویندوز به مانند شکل ۸-۹۹، وارد تنظیمات کارت شبکه شوید و آدرس IP را در رنج شبکه سرور قرار دهید.



شکل ۸- ۹۹ تنظیم کارت شبکه

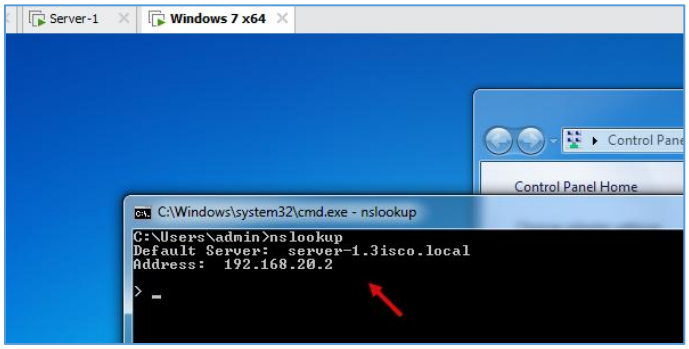
همان‌طور که در شکل ۸-۱۰۰، مشاهده می‌کنید، آدرس 192.168.20.100 به ماشین مورد نظر تخصیص داده شده است و از همه مهمتر در قسمت DNS آدرس سرور Server-1 داده شده است که DNS اصلی ما است.

www.takbook.com



شکل ۸- ۱۰۰ تنظیم کارت شبکه

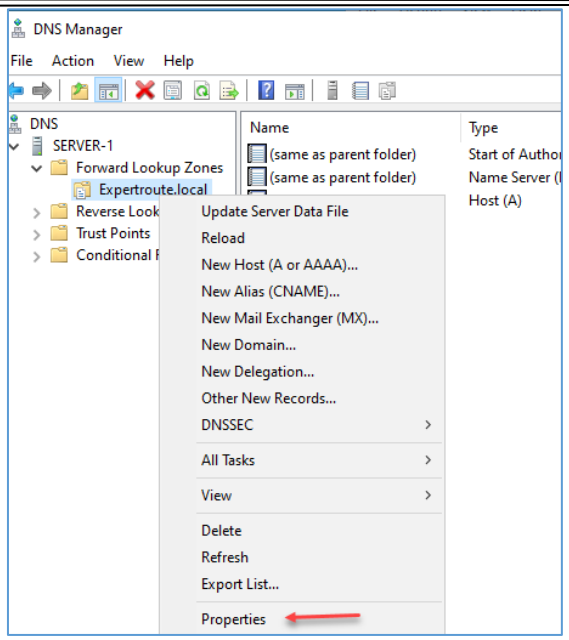
اگر به مانند شکل ۸-۱۰۱، وارد ویندوز ۷ مجازی شوید و دستور nslookup را اجرا کنید به شما اعلام می‌کند که سرور DNS برای این ماشین برابر است با server-1.Expertroute.local و به این صورت هر تنظیمی که در سرور DNS انجام شود کلاینت مجبور به انجام آن است، در ادامه با موضوعات و تست‌های بیشتری این سرویس کاربردی را بررسی خواهیم کرد.



شکل ۸- ۱۰۱ سرویس DNS

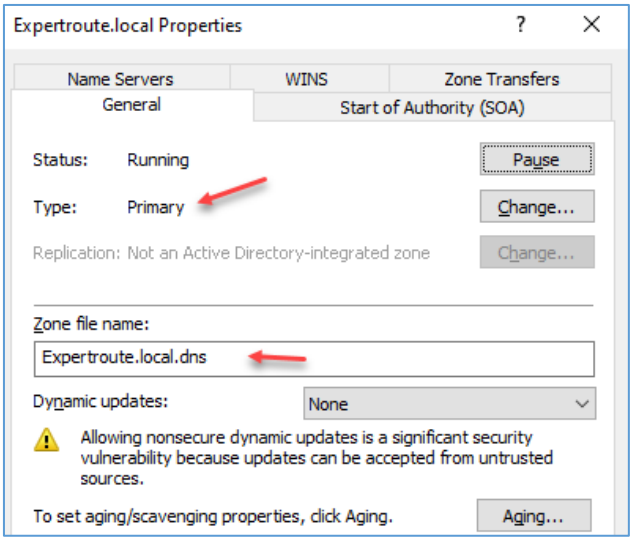
در ادامه طبق شکل ۸-۱۰۲، برای بررسی جزئیّات کار بر روی دومین کلیک راست و گزینه‌ی Properties را انتخاب کنید.

www.takbook.com



شکل ۸-۱۰۲ سرویس DNS

در شکل ۸-۱۰۳، در تب General، اگر دکمه‌ی Pause را جلوی Status کلیک کنید، این Zone غیرفعّال خواهد شد و توانایی ارائه دادن سرویس را نخواهد داشت، در قسمت Type نیز می‌توانید، نوع Zone خود را از Primary به Zoneهای دیگر تغییر دهید و در قسمت Zone File Name، نام Zone خود را مشاهده کنید.

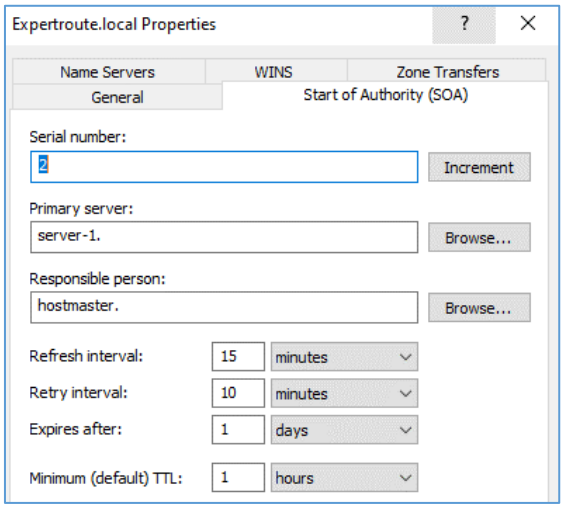


شکل ۸-۱۰۳ سرویس DNS

به مانند شکل ۸-۱۰۴ تب SOA، گزینه‌های مختلفی وجود دارد که با هم بررسی می‌کنیم.

www.takbook.com

- 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، Server-1 است.
- Responsible Person (RNAME): 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.



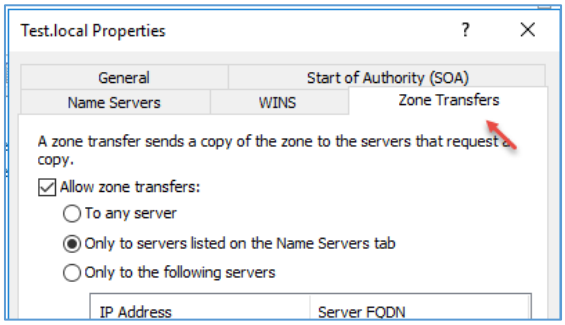
شکل ۸- ۱۰۴ سرویس DNS

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

www.takbook.com

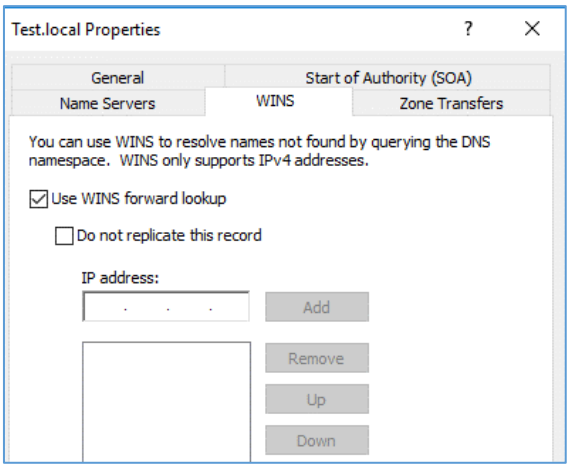
مشاهده است، برای اینکه سرور DNS مشخّصی را به لیست اضافه کنید باید بر روی Add کلیک کنید و نام سرور خود را وارد کنید.

طبق شکل ۸–۱۰۵، در قسمت Zone Transfer، می‌توانید مشخّص کنید که فایل دیتابیس شما به چه سرورهایی فرستاده شود؛ طبق شکل ۸–۱۰۵، 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.



شکل ۸- ۱۰۵ سرویس DNS

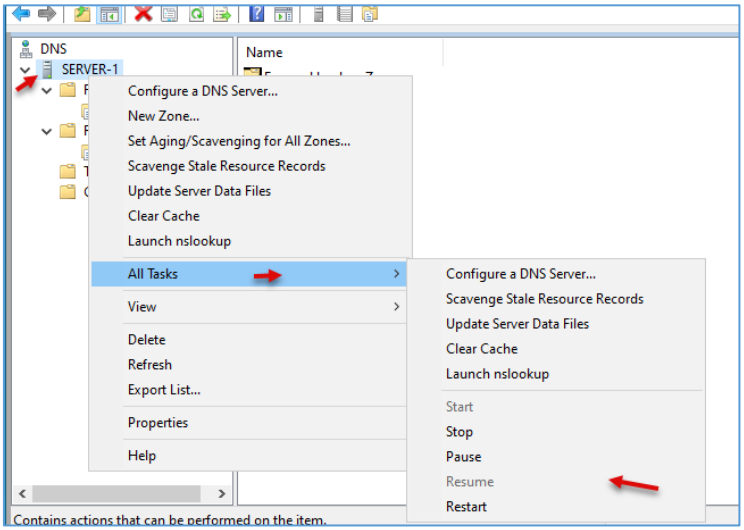
طبق شکل ۸–۱۰۶، در تب WINS می‌توانید سرور WINS خود را در لیست مورد نظر وارد کنید؛ سرویس WINS، یک سرویس قدیمی برای تبدیل IP به اسم است که فعلاً کاری با آن نداریم.



شکل ۸- ۱۰۶ سرویس DNS

تنظیمات دیگری در سرویس DNS وجود دارد، مثلاً اگر بخواهید سرویس DNS را Stop,Start و یا Restart کنید می‌توانید به مانند شکل ۸–۱۰۷، بر روی نام سرور کلیک راست کنید و از قسمت All Tasks گزینه‌ی مورد نظر خود را انتخاب کنید.

www.takbook.com



شکل ۸-۱۰۷ سرویس DNS

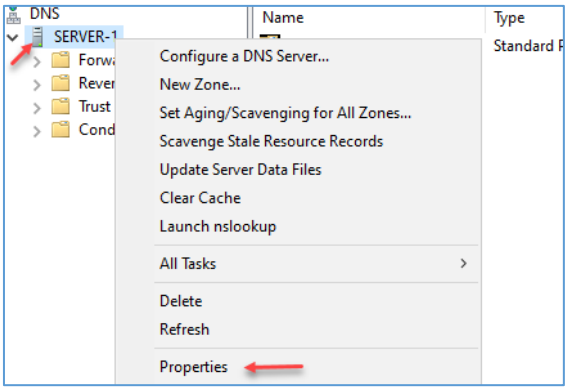
انشاالله در ادامه کار سرور DNS دیگری را هم راه‌اندازی می‌کنیم و نحوه ارتباط آنها را چک خواهیم کرد.

۸-۳-۶-۵ بررسی DNS Forwarders

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

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

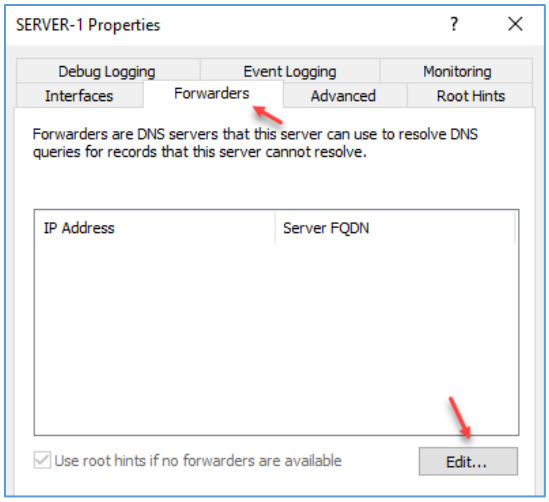
بر روی نام سرور در سرویس DNS Server کلیک راست کنید و گزینه Properties را انتخاب کنید تا شکل ۸-۱۰۸، ظاهر شود.



شکل ۸-۱۰۸ DNS Forwarders

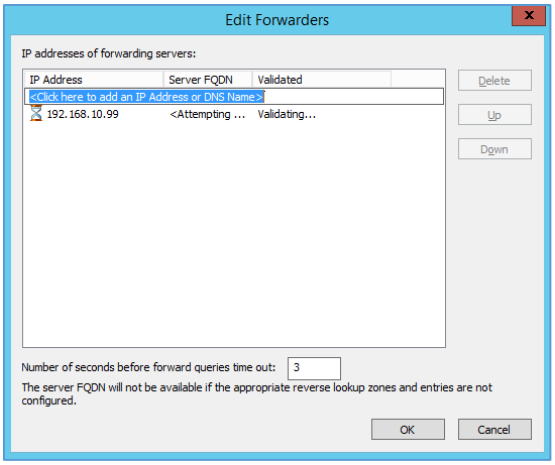
www.takbook.com

در شکل ۸-۱۰۹، وارد تب Forwarders شوید و برای معرفی DNS Server خود بر روی Edit کلیک کنید.



شکل ۸-۱۰۹ *DNS Forwarders*

در شکل ۸-۱۱۰، می‌توانید سرورهای قبلی را انتخاب و بر روی Delete کلیک کنید تا حذف شوند و بعد سرور جدید خود را وارد کنید که بعد از این کار سرویس به دنبال سرور موردنظر می‌گردد، اگر در سروری که آدرس آن را وارد کردید سرویس DNS فعال باشد به شما تایید می‌دهد، بعد از این کار بر روی ok کلیک کنید تا کار به اتمام برسد.



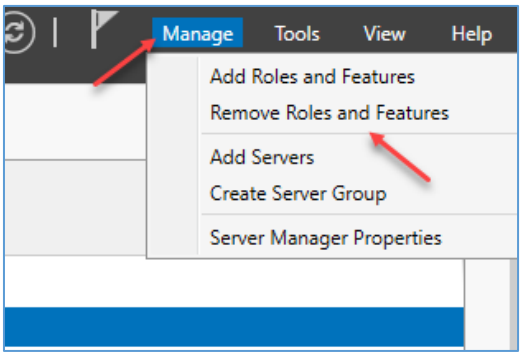
شکل ۸-۱۱۰ *DNS Forwarders*

www.takbook.com

۸-۳-۶-۶ حذف سرویس DNS

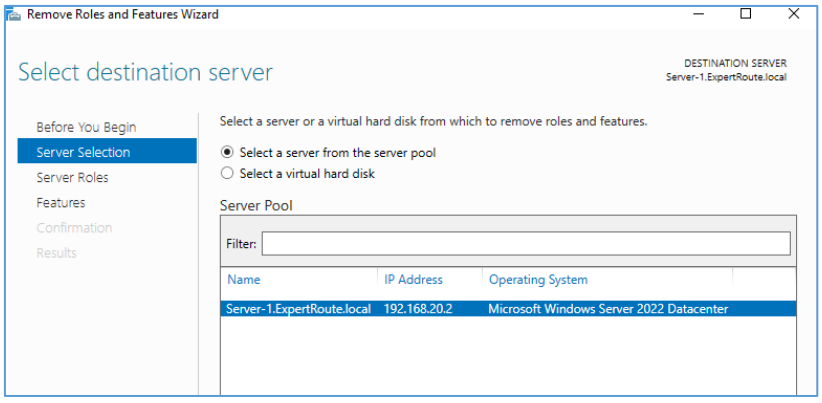
نکته مهم در این قسمت این است که، برای اینکه در مرحله بعد سرویس Active Directory را نصب کنیم بهتر است که سرویس DNS که با هم فعال کردیم را حذف کنیم و بعد اقدام به نصب سرویس Active Directory کنیم، تا تنظیمات به درستی انجام شود.

به مانند شکل ۸-۱۱۱، وارد Server Manager شوید و از قسمت Manage گزینه‌ی Remove Roles را انتخاب کنید.



شکل ۸- ۱۱۱ حذف سرویس DNS

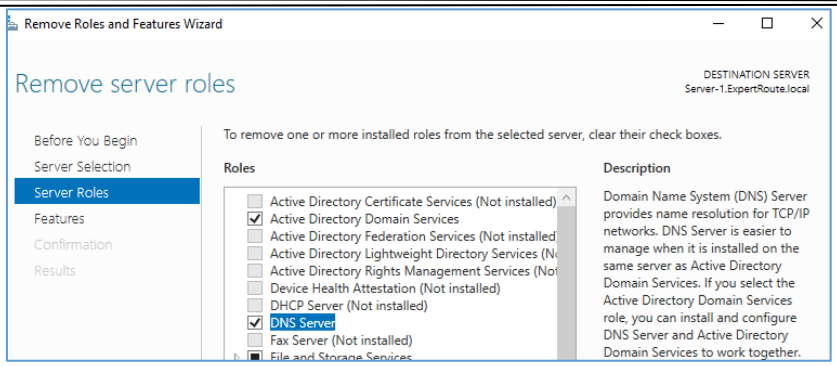
در شکل ۸-۱۱۲، بر روی Next کلیک کنید.



شکل ۸- ۱۱۲ حذف سرویس DNS

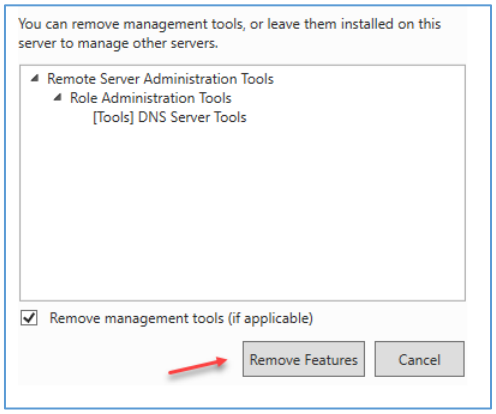
در شکل ۸-۱۱۳، گزینه‌ی DNS Server را انتخاب کنید.

www.takbook.com



شکل ۸- ۱۱۳ حذف سرویس DNS

در شکل ۸-۱۱٤، بر روی Remove Features کلیک کنید.



شکل ۸- ۱۱۴ حذف سرویس DNS

۸-۳-۷ سرویس Active Directory

سرویس Active Directory یکی از حیاتی‌ترین سرویس‌ها در سرورهای مایکروسافت است که به مدیریت جامع و متمرکز یک شبکه کمک می‌کند. این سرویس امکان تعریف کاربران، تخصیص سیاست‌ها، مدیریت دسترسی‌ها، ایجاد گروه‌ها، و بسیاری وظایف دیگر را به مدیران شبکه ارائه می‌دهد.

مدیریت شبکه به‌صورت متمرکز

سرویس Active Directory (AD) ابزار اصلی مدیریت شبکه‌های مبتنی بر ویندوز است که به سازمان‌ها این امکان را می‌دهد که کاربران، دستگاه‌ها، و منابع شبکه را به‌صورت متمرکز مدیریت کنند. این سرویس به‌خصوص برای شبکه‌های بزرگ که نیاز به کنترل و هماهنگی دقیق دارند، طراحی شده است.

نقش دامین کنترلر (Domain Controller)

سروری که Active Directory روی آن نصب شده است، به عنوان Domain Controller (DC) شناخته می‌شود. این سرور مسئولیت‌های زیر را بر عهده دارد:

www.takbook.com

- احراز هویت (Authentication):

بررسی اطلاعات ورود کاربران (مانند نام کاربری و رمز عبور) هنگام لاگین و تضمین امنیت دسترسی کاربران به منابع شبکه.

- مدیریت سطوح دسترسی (Authorization)

تعیین می‌کند که هر کاربر به چه منابعی دسترسی دارد و چه اقداماتی می‌تواند انجام دهد.

به‌عنوان مثال، وقتی کاربری به یک دستگاه متصل به دامنه (Domain) وارد می‌شود، DC تعیین می‌کند چه نرم‌افزارهایی در دسترس او باشد.

پروتکل‌ها و فناوری‌های مورد استفاده در Active Directory

- LDAP (Lightweight Directory Access Protocol)

برای دسترسی و مدیریت اطلاعات در ساختار دایرکتوری Active Directory استفاده می‌شود.

از نسخه‌های ۲ و ۳ این پروتکل پشتیبانی می‌شود.

- Kerberos

پروتکلی برای احراز هویت امن که اطمینان می‌دهد ارتباطات کاربر با سیستم بدون افشای رمز عبور امن می‌ماند.

۱-۷-۳-۸ دومین (Domain)

دومین (Domain) در ویندوز سرور، ساختاری است که برای مدیریت شبکه‌های کامپیوتری با استفاده از یک سیستم متمرکز ایجاد می‌شود. با استفاده از دامین، ادمین‌های شبکه می‌توانند دسترسی کاربران، منابع و امنیت شبکه را از طریق یک نقطه متمرکز به نام "کنترل‌کننده دامین" (Domain Controller) مدیریت کنند. این قابلیت به خصوص در سازمان‌ها و شرکت‌های بزرگ با تعداد کاربران و دستگاه‌های زیاد مفید است، زیرا باعث ساده‌سازی و تقویت امنیت و مدیریت شبکه می‌شود.

اجزای اصلی دامین در ویندوز سرور

- کنترل‌کننده دامین (Domain Controller): این کامپیوتر سرور است که خدمات احراز هویت و مدیریت دامین را انجام می‌دهد. کنترل‌کننده دامین، اطلاعات کاربران، گروه‌ها، و دستگاه‌ها را در دیتابیسی به نام Active Directory ذخیره و مدیریت می‌کند.
- Active Directory: این سرویس توسط مایکروسافت برای مدیریت اطلاعات شبکه و فراهم کردن احراز هویت و مجوزها در محیط دامین استفاده می‌شود. Active Directory، کاربران، کامپیوترها، پرینترها و سایر منابع شبکه را به صورت متمرکز مدیریت می‌کند.
- DNS (سیستم نام دامنه): DNS در دامین برای تبدیل نام‌های دامنه به آدرس‌های IP استفاده می‌شود. این سرویس به ارتباط بین دستگاه‌ها و خدمات در شبکه کمک می‌کند.

www.takbook.com

- Trusts (روابط اعتماد): ویندوز سرور به دامین‌های مختلف اجازه می‌دهد تا بین یکدیگر اعتماد ایجاد کنند. این ویژگی برای سازمان‌هایی که چند دامین دارند و نیاز به تعامل بین آن‌ها دارند، مفید است.

۸-۳-۷-۲ درختان (Trees)

در Active Directory، درخت (Tree) به مجموعه‌ای از دامین‌ها گفته می‌شود که با یکدیگر در ارتباط بوده و دارای یک فضای نام (Namespace) مشترک هستند. این ساختار سلسله مراتبی به سازمان‌ها امکان می‌دهد تا چندین دامین مرتبط با یکدیگر داشته باشند و از طریق آن، منابع و سیاست‌ها را بین دامین‌های مختلف به اشتراک بگذارند.

به زمان تولدت فکر کن وقتی پدر و مادرم نام من را فرشید گذاشتند، نام خانوادگی پدر و مادرم را انتخاب کردم. بنابراین، من فرشید فردمنش شدم. دامنه‌ها در یک درخت به همین ترتیب کار می‌کنند. هنگامی که یک دامنه فرزند ایجاد می‌کنید، نام والد را به خود اختصاص می‌دهد.

در دنیای واقعی سازمان‌ها اصولاً نام Child Domain را برای شعبه‌های خود انتخاب می‌کنند و سعی می‌کنند اسم همان شعبه را برای آن در نظر بگیرند.

توجه داشته باشید می‌توانیم چندین دامنه داشته باشیم مثلاً ExpertRoute.ir و 3isco.ir که اگر بخواهیم برای آنها دامنه‌ی فرزند تعریف کنیم، آن دامنه‌ی فرزند فقط زیر مجموعه دامنه اصلی خود کار خواهد کرد.

۸-۳-۷-۳ جنگل‌ها (Forests)

در Active Directory، جنگل (Forest) سطح بالاترین ساختار و مجموعه‌ای از یک یا چند درخت است که هر درخت می‌تواند شامل یک یا چند دامین باشد. جنگل‌ها امکان ایجاد چندین درخت و دامین‌های مختلف با فضاهای نام مستقل را فراهم می‌کنند و اغلب در سازمان‌های بزرگ و پیچیده با نیازهای متنوع امنیتی و مدیریتی استفاده می‌شوند.

نقطه ضعف این است که جنگل‌ها به طور پیش‌فرض با هم کار نمی‌کنند. اکثر شرکت‌ها جنگل مخصوص به خود را دارند و شما نمی‌خواهید شبکه شما به طور خودکار با شبکه شخص دیگری کار کند.

البته می‌توانید این جنگل‌ها را طبق قوانینی به هم متصل کنید که در صورت نیاز در این کتاب بررسی خواهیم کرد.

۸-۳-۷-۴ بررسی Domain Function Level

ویژگی وجود دارد با نام Domain Function Level که زمانیکه می‌خواهیم یک سرویس Active Directory را نصب کنیم باید انتخاب کنیم که سرورهای دیگری که می‌خواهند به عنوان یک دومین فعالیت کننده چه

www.takbook.com

نسخه‌ای باشند، در زیر ویندوز سرورهایی که پشتیبانی می‌شود مشخص شده است، در هنگام نصب Active Directory باید یکی از ورژن ها را انتخاب کنید.

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

مثلاً اگر طبق لیست بالا Windows Server 2016 را انتخاب کنید، ویندوز سرورهایی که قرار است نقش دومین را بازی کنند و به دومین اصلی ما متصل شوند باید از ورژن 2016 به بالا باشند و قبل از آن دیگر قابل قبول نیست و باید به این قسمت حتماً توجه کنید.

اجزای اصلی Active Directory:

- Domain: واحد بنیادی AD که شامل مجموعه‌ای از کاربران، گروه‌ها و دستگاه‌ها است. هر دامنه دارای یک نام منحصربه‌فرد است.
- Forest: مجموعه‌ای از یک یا چند دامنه که با هم مرتبط هستند و دارای یک ساختار دایرکتوری مشترک می‌باشند.
- Organizational Units (OUs): ساختارهایی که به سازمان‌دهی منابع درون یک دامنه کمک می‌کنند. می‌توانند شامل کاربران، گروه‌ها و کامپیوترها باشند.
- Group Policy: قابلیتی برای مدیریت و پیکربندی تنظیمات مختلف بر روی کاربران و کامپیوترها. از این طریق می‌توان سیاست‌های امنیتی و سایر تنظیمات را در سطح دامنه یا OUها اعمال کرد.

ویژگی‌ها و مزایای Active Directory:

- احراز هویت متمرکز: کاربران می‌توانند با یک نام کاربری و رمز عبور به تمامی منابع شبکه دسترسی پیدا کنند.
- مدیریت کاربر و گروه: امکان ایجاد، حذف و مدیریت کاربران و گروه‌ها به آسانی فراهم می‌شود.
- کنترل دسترسی: با استفاده از مجوزهای خاص، می‌توان دسترسی به منابع مختلف را مدیریت کرد.
- توزیع بار و افزونگی: در صورت ایجاد چندین سرور Domain Controller، می‌توان بار ترافیکی را توزیع کرد و در صورت بروز مشکل، دسترسی به منابع ادامه یابد.
- گزارش‌گیری و نظارت: قابلیت‌های گزارش‌گیری برای پیگیری فعالیت‌های کاربری و امنیتی.

موارد استفاده:

- سازمان‌ها و شرکت‌ها: برای مدیریت کاربران، گروه‌ها، و منابع شبکه.

www.takbook.com

- مدارس و دانشگاه‌ها: برای مدیریت دانش‌آموزان و کارکنان.
- شرکت‌های بزرگ: برای پشتیبانی از زیرساخت‌های IT پیچیده و توزیع‌شده.

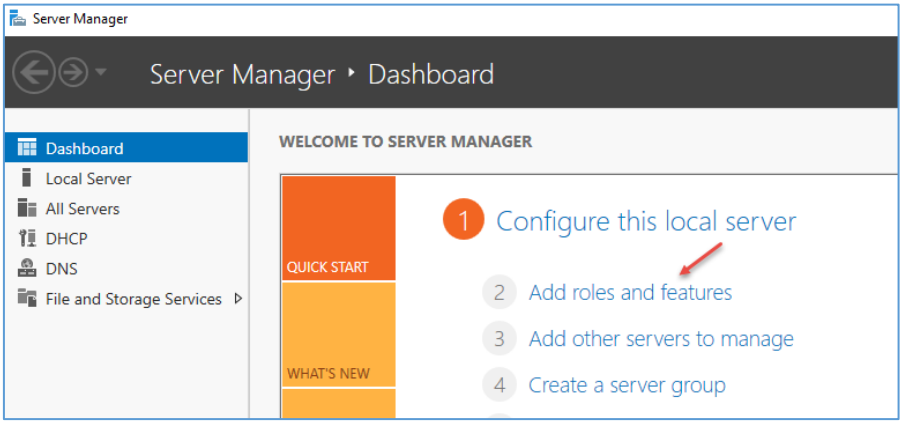
ایجاد یک دامین در ویندوز سرور نیازمند برنامه‌ریزی و توجه به چندین نکته مهم است تا شبکه به بهترین شکل عمل کند و امنیت و مدیریت آن ساده‌تر باشد. در ادامه به برخی از نکاتی که باید در فرآیند ایجاد دامین در نظر بگیرید، اشاره می‌کنم:

انتخاب نام مناسب برای دامین

- نام معنادار: نام دامین باید به‌گونه‌ای انتخاب شود که مرتبط با سازمان یا بخشی از سازمان باشد.
- اجتناب از نام‌های رایج: از استفاده از نام‌های عمومی مانند "local" یا "domain" اجتناب کنید، زیرا ممکن است باعث تداخل با دامنه‌های خارجی شود.
- ساختار DNS: نام دامین باید با ساختار DNS سازگار باشد، مانند company.com یا example.local.

۸-۳-۸ نصب و راه‌اندازی سرویس Active Directory

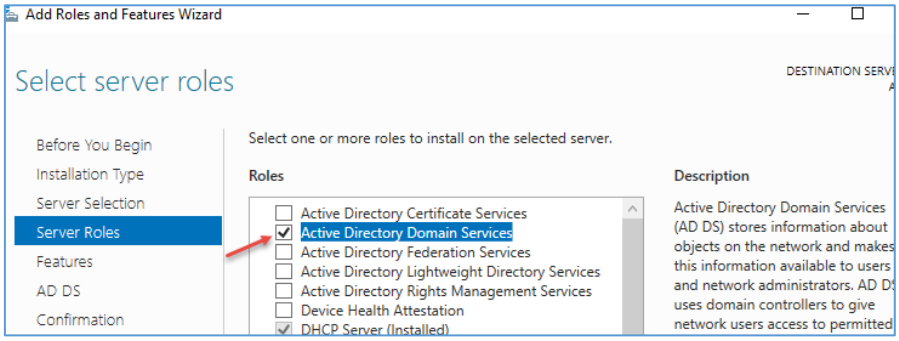
برای شروع به کار و نصب سرویس Active Directory به مانند شکل ۸-۱۱۵، وارد Server Manager شوید و بر روی Add roles and features کلیک کنید.



شکل ۸- ۱۱۵ سرویس *Active Directory*

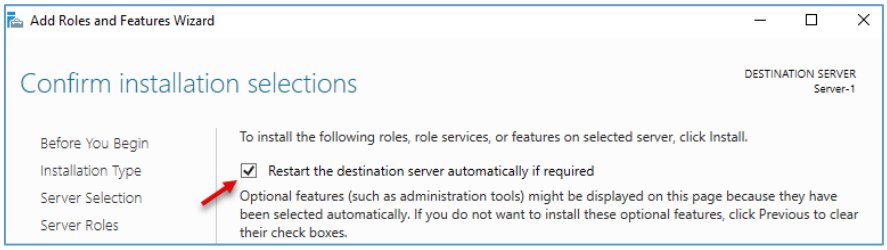
طبق شکل ۸-۱۱۶، در قسمت Server Roles، سرویس Active Directory Domain Services را انتخاب و در صفحه‌ی باز شده بر روی Add Features کلیک کنید و بعد بر روی Next کلیک کنید.

www.takbook.com



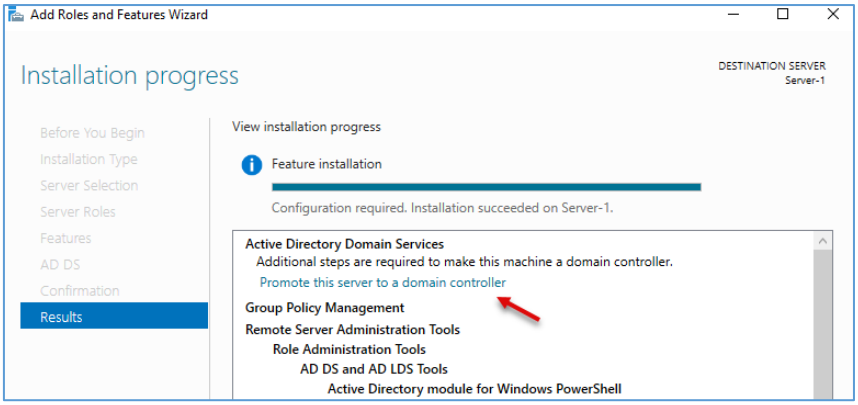
شکل ۸- ۱۱۶ سرویس *Active Directory*

طبق شکل ۸–۱۱۷، و در قسمت Confirmations، تیک گزینه‌ی Restart را انتخاب و بر روی Install کلیک کنید.



شکل ۸- ۱۱۷ سرویس *Active Directory*

بعد از نصب اولّیه‌ی سرویس، شکل ۸–۱۱۸، 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.

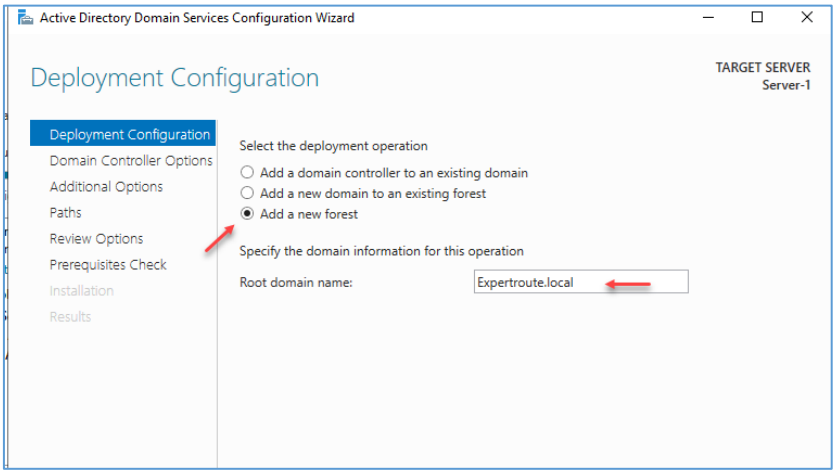


شکل ۸- ۱۱۸ سرویس *Active Directory*

در شکل ۸–۱۱۹، چند گزینه وجود دارد که برای شروع کار و راه‌اندازی دومین کنترلر باید گزینه‌ی Add a new forest را انتخاب و نام دومین خود را وارد کنید که در اینجا، Expertroute.local نوشته شده است،

www.takbook.com

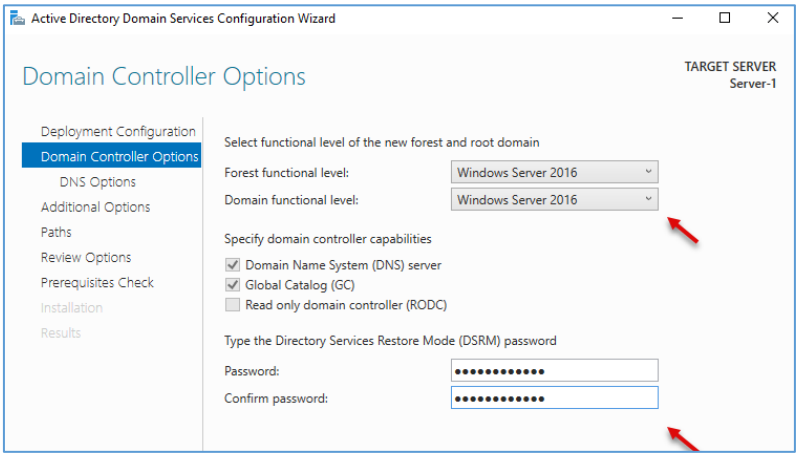
توجّه داشته باشید که اگر این نام دومین در اینترنت نیز اعتبار داشته باشد، احتمال دارد با متّصل کردن سرور به اینترنت با مشکل مواجه شوید، این نام همان نام دومین یا Zone است که در قسمت DNS وارد کرده بودیم، توجه داشته باشید اگر قبل از اینکه DNS را تنظیم کنید اقدام به نصب Active Directory کنید به صورت خودکار همزمان با نصب Active Directory سرویس DNS نصب و نام دومین در آن ایجاد خواهد شد.



شکل ۸- ۱۱۹ سرویس Active Directory

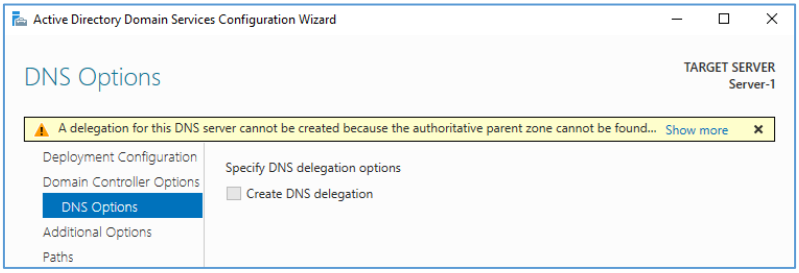
در شکل ۸-۱۲۰، در قسمت اوّل می‌توانید مشخّص کنید که سرور دومین شما با چه ورژنی از ویندوز سرور در ارتباط باشد تا بتواند اطّلاعات دومین را به آن انتقال دهد، یعنی اینکه اگر زمانی بخواهید یک دومین دیگر به شبکه‌ی خود اضافه کنید آن دومین باید دارای حداقل ویندوز سرور ۲۰۱۶ باشد، البته در سرور ۲۰۲۵ می‌توانید خود ورژن ۲۰۲۵ را انتخاب کنید تا ارتباط فقط با ویندوز سرور ۲۰۲۵ انجام شود، در قسمت پایین صفحه نیز یک رمز عبور پیچیده، مانند ExpertRoute@2012 برای مد ریکاوری DSRM وارد کنید، مد DSRM زمانی به کار می‌رود که سرویس Active directory دچار مشکل شود و مدیران شبکه با داشتن این رمز می‌توانند وارد حالت Safe Mode شوند و سرویس Active Directory را تعمیر و بازیابی کنند.

www.takbook.com



شکل ۸- ۱۲۰ سرویس *Active Directory*

در شکل ۸-۱۲۱، پیغامی ظاهر می‌شود و به این موضوع اشاره می‌کند که دومینی که انتخاب می‌کنید هم زمان باید در سرویس DNS هم ایجاد و تعریف شود و به خاطر اینکه سرویس DNS وجود ندارد این پیغام ظاهر می‌شود اما در هنگام نصب Active Directory سرویس DNS به صورت خودکار نصب و دومین Expertroute.local در آن تعریف خواهد شد.

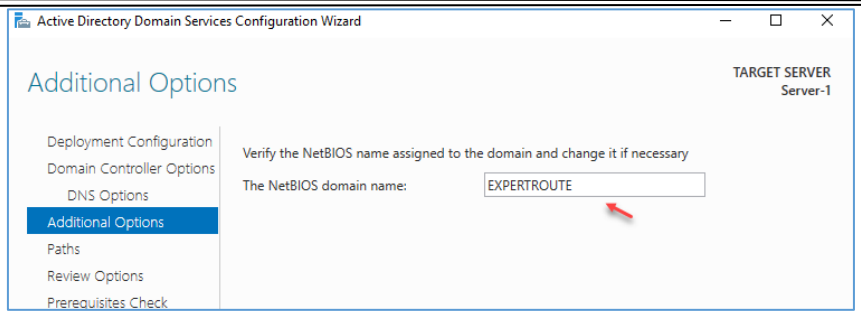


شکل ۸- ۱۲۱ سرویس *Active Directory*

در شکل ۸-۱۲۲، نام دومین در صورت موجود نبودن در شبکه و اینترنت تأیید خواهد شد؛ بر روی Next کلیک کنید.

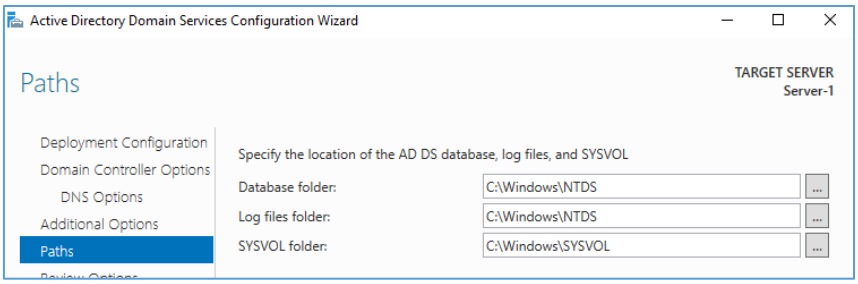
تذکّر: اگر سرور شما به اینترنت متّصل باشد و شما یک دومین، مانند ExpertRoute.ir را وارد کرده باشید در این قسمت با خطا مواجه خواهید شد، پس این نکته را مدّ نظر داشته باشید و دومینی را انتخاب کنید که در آینده با مشکل روبرو نشوید.

www.takbook.com



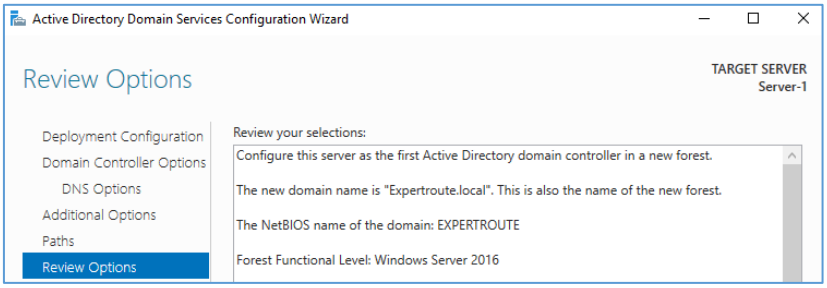
شکل ۸- ۱۲۲ تایید نام دومین

در شکل ۸–۱۲۳، می‌توانید آدرس ذخیره شدن دیتابیس و دیگر اجزای Active Directory را مشخّص کنید که به صورت پیش‌فرض، آدرس به آن داده شده است.



شکل ۸- ۱۲۳ سرویس Active Directory

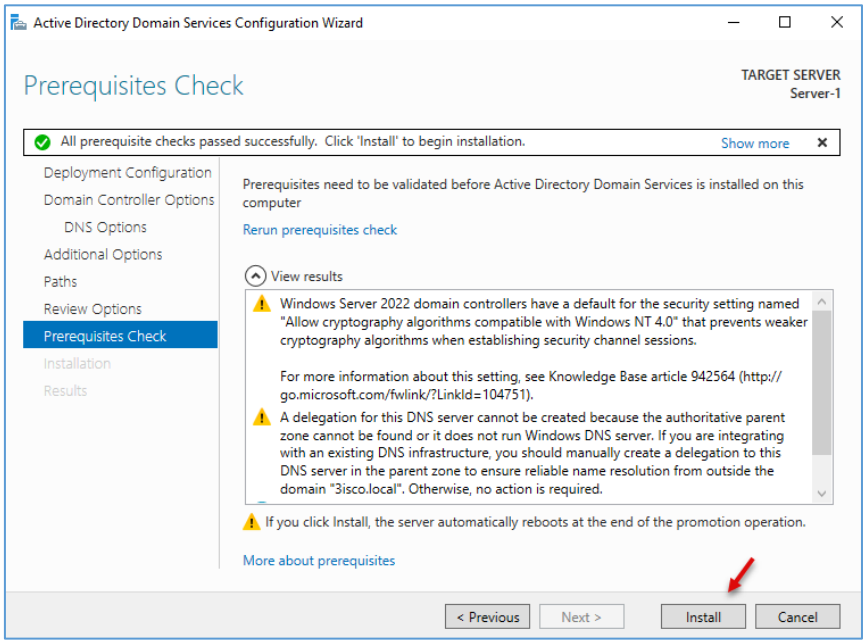
در شکل ۸–۱۲٤، اگر اطّلاعات مورد تأیید است بر روی Next کلیک کنید.



شکل ۸- ۱۲۴ سرویس Active Directory

در شکل ۸–۱۲۵، تنظیمات و پیش‌نیازهای نصب مورد تأیید است؛ بر روی Install کلیک کنید که بعد از نصب سرور Restart خواهد شد.

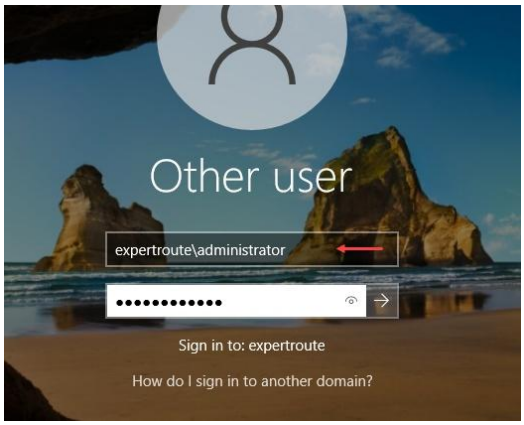
www.takbook.com



شکل ۸- ۱۲۵ سرویس *Active Directory*

نکته: در شکل ۸–۱۲۵، اگر رمز عبور پیچیده‌ای برای کاربر Administrator ایجاد نکرده باشید با خطا روبرو خواهید شد.

بعد از اجرا شدن سرور به مانند شکل ۸–۱۲۶، رمز عبور مربوط به کاربر Administrator را وارد کنید.

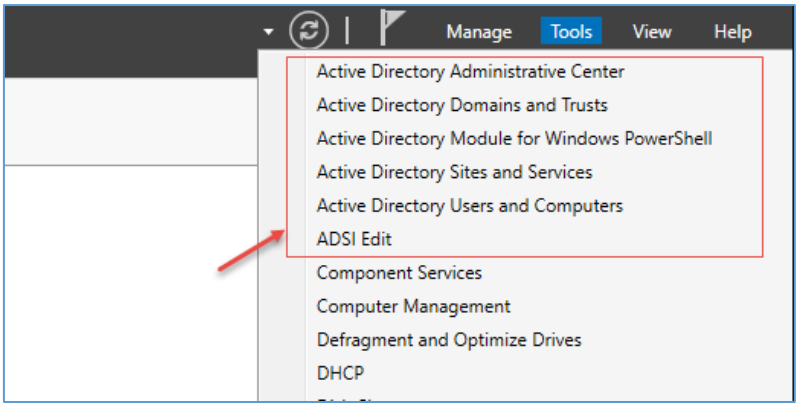


شکل ۸- ۱۲۶ ورود به ویندوز

www.takbook.com

۹-۳-۸ بررسی سرویس‌های Active directory

به مانند شکل ۸-۱۲۷، 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.



شکل ۸-۱۲۷ سرویس‌های Active Directory

Active Directory Administrator Center

Active Directory Administrative Center یک ابزار گرافیکی قدرتمند در ویندوز سرور ۲۰۲۵ است که برای مدیریت آسان‌تر و مؤثرتر Active Directory طراحی شده است. این ابزار از طریق کنسول مدیریتی (MMC) ارائه می‌شود و بسیاری از عملیات مرتبط با دامین کنترلرها و اشیای دایرکتوری مانند کاربران، گروه‌ها، واحدهای سازمانی (OU) و غیره را تسهیل می‌کند.

ویژگی‌ها:

- رابط گرافیکی مدرن: برخلاف Active Directory Users and Computers (ADUC)، این ابزار از رابط کاربری مبتنی بر Windows Presentation Foundation (WPF) استفاده می‌کند که رابط کاربرپسندتر و پیشرفته‌تری ارائه می‌دهد.
- PowerShell History: تمام اقداماتی که از طریق ADAC انجام می‌شوند، دستورات PowerShell معادل آن‌ها در History Pane نمایش داده می‌شود، که برای یادگیری و استفاده از PowerShell مفید است.
- مدیریت Fine-Grained Password Policies (FGPP): ADAC به شما اجازه می‌دهد تا به‌راحتی سیاست‌های کلمه عبور دقیق برای گروه‌ها یا کاربران خاص ایجاد و مدیریت کنید.

www.takbook.com

Dynamic Access Control (DAC): امکان پیکربندی Dynamic Access Control برای مدیریت پیشرفته دسترسی به منابع.

Recycle Bin Management: مدیریت Recycle Bin برای بازیابی اشیای حذف‌شده در Active Directory به‌صورت ساده و گرافیکی.

Active Directory Domain and Trust

Active Directory Domains and Trusts یک ابزار مدیریتی در ویندوز سرور است که برای مدیریت دامنه‌ها و تنظیمات اعتماد (Trust) در Active Directory استفاده می‌شود. این ابزار به مدیران شبکه کمک می‌کند تا ارتباطات بین دامنه‌های مختلف و سیاست‌های مرتبط را پیکربندی و مدیریت کنند.

ویژگی این سرویس:

- مدیریت Trusts: ایجاد و مدیریت ارتباطات اعتماد (Trusts) بین دامنه‌های Active Directory در یک Forest یا بین Forestهای مختلف و پشتیبانی از انواع Trustها مانند External Trust، Forest Trust، و Shortcut Trust.

Active directory Module for windows PowerShell

یک ماژول قدرتمند است که مجموعه‌ای از cmdletهای PowerShell را برای مدیریت و اتوماسیون Active Directory فراهم می‌کند. این ماژول به مدیران شبکه امکان انجام وظایف مختلف مرتبط با Active Directory را به‌صورت خط فرمان و اسکریپت می‌دهد.

Active directory Site and service

Active Directory Sites and Services یکی از ابزارهای مدیریتی در ویندوز سرور است که برای مدیریت توپولوژی فیزیکی شبکه در Active Directory طراحی شده است. این ابزار به مدیران شبکه کمک می‌کند تا ساختار منطقی (Logical) و فیزیکی Active Directory (Physical) را هماهنگ کرده و کارایی و امنیت ارتباطات بین دامین کنترلرها را بهینه‌سازی کنند.

Active Directory Users and Computers

Active Directory Users and Computers (ADUC) یکی از ابزارهای اصلی در ویندوز سرور است که برای مدیریت اشیای مختلف در Active Directory، مانند کاربران، گروه‌ها، کامپیوترها، Organizational Units (OU)، و دیگر اشیای دایرکتوری استفاده می‌شود. این ابزار رابط کاربری گرافیکی ساده‌ای دارد که به مدیران شبکه امکان مدیریت منابع Active Directory را به‌صورت مؤثر می‌دهد.

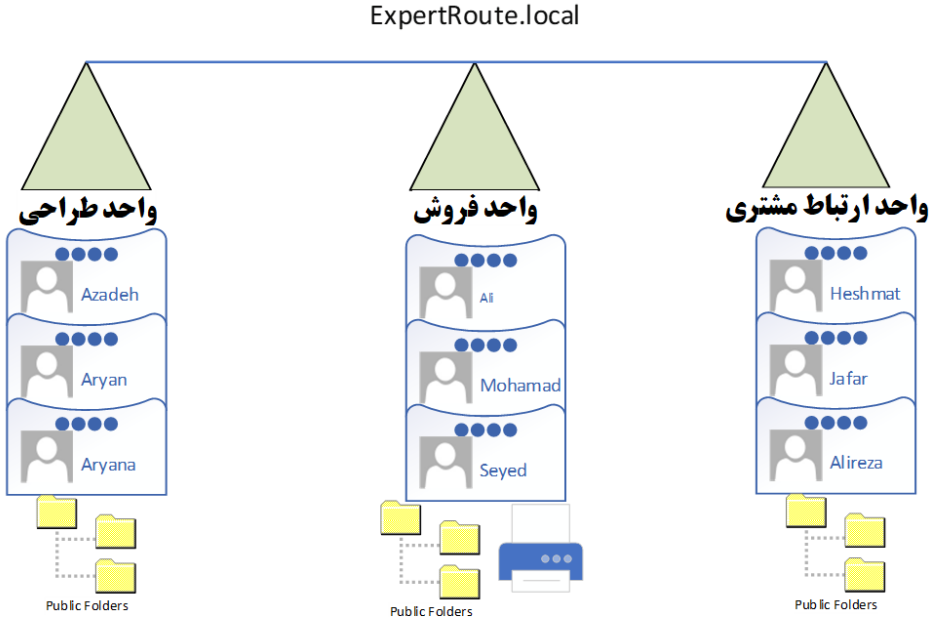
ADSI

www.takbook.com

Active Directory Service Interfaces (ADSI) یک مجموعه از رابط‌های برنامه‌نویسی کاربردی (APIs) است که به برنامه‌نویسان و مدیران شبکه این امکان را می‌دهد تا به‌صورت برنامه‌نویسی‌شده با Active Directory تعامل داشته باشند. ADSI به شما این امکان را می‌دهد که به داده‌ها و اشیای موجود در Active Directory دسترسی پیدا کرده، آنها را جستجو، ایجاد، و یا ویرایش کنید. این رابط به‌ویژه برای توسعه‌دهندگانی که می‌خواهند ابزارهای سفارشی برای مدیریت Active Directory بنویسند، مفید است.

۸-۳-۱۰ 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 ۸-۱۲۸.

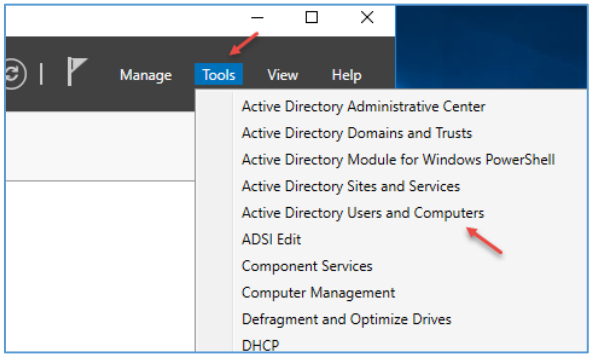


شکل ۸- ۱۲۸ *Active Directory Users and Computers*

به طور مثال، اگر تصوّر کنیم که شما در سازمان خود، دارای سه بخش کلیدی به مانند شکل ۸-۱۲۸ 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.

www.takbook.com

برای شروع کار به مانند شکل ۸-۱۲۹، وارد Server Manager شوید و از منوی Tools، گزینه‌ی Active Directory Users and Computers را انتخاب کنید.

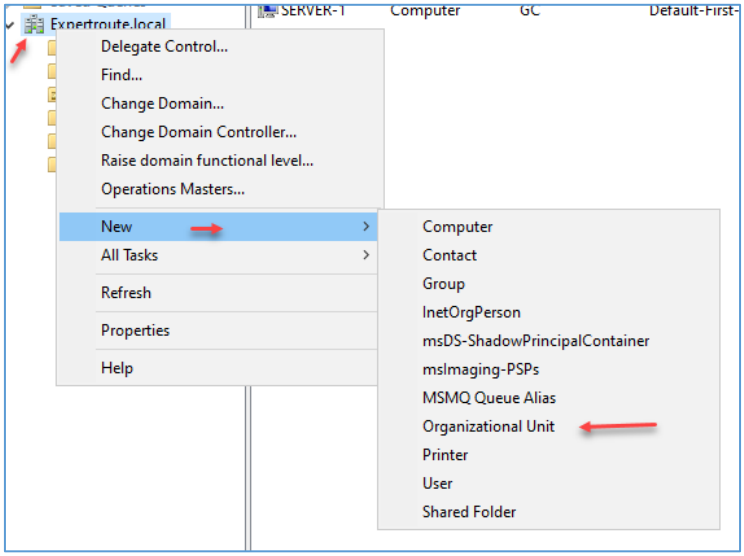


شکل ۸- ۱۲۹ *Active Directory Users and Computers*

۸-۳-۱۰-۱ تعریف Organization Unit

Organizational Unit (OU) یک واحد سازمانی در Active Directory است که برای گروه‌بندی و سازماندهی اشیای مختلف Active Directory مانند کاربران، گروه‌ها، کامپیوترها و دیگر منابع استفاده می‌شود. OU به مدیران شبکه این امکان را می‌دهد که منابع را به‌طور منطقی و بر اساس نیازهای سازمانی سازماندهی کنند، به طوری که مدیریت منابع ساده‌تر و موثرتر شود.

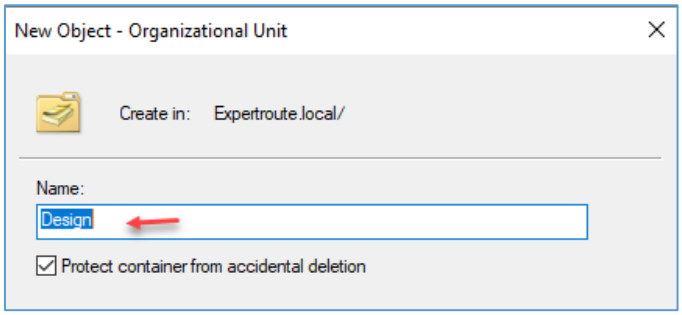
به مانند شکل ۸-۱۳۰، برای ایجاد Organization Unit یا واحد سازمانی بر روی نام دومین کلیک راست کنید و از قسمت New، گزینه‌ی Organization Unit را انتخاب کنید.



شکل ۸- ۱۳۰ *Active Directory Users and Computers*

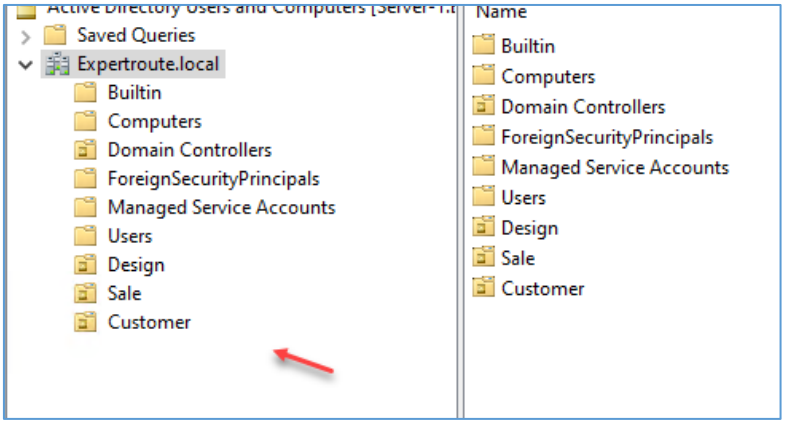
www.takbook.com

در شکل ۸-۱۳۱، 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.



شکل ۸- ۱۳۱ایجاد OU

همان‌طور که در شکل ۸-۱۳۲، 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.



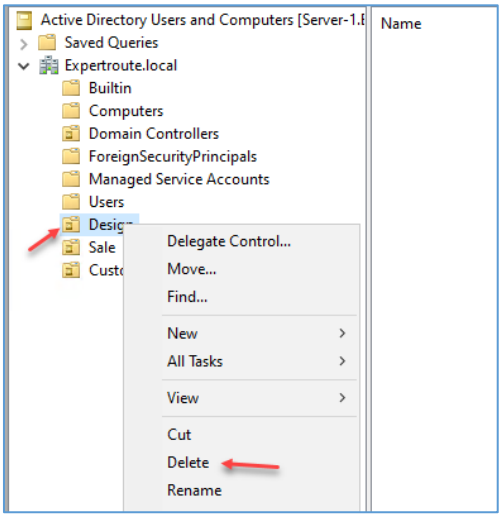
شکل ۸- ۱۳۲ایجاد OU

بعد از ایجاد واحد سازمانی می‌توانیم کاربرانی را که ایجاد می‌کنیم را در این گروه‌ها قرار دهیم و دسترسی‌های آنها را به صورت منظم بررسی کنیم.

۸-۳-۱۰-۲ چگونه واحدهای سازمانی را حذف کنیم؟

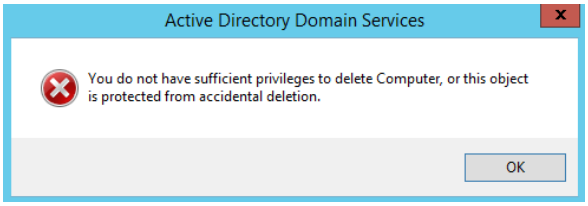
برای حذف واحد سازمانی، به مانند شکل ۸-۱۳۳، روی آن کلیک راست کنید و گزینه‌ی Delete ر انتخاب کنید و یا از نوار ابزار بر روی آیکون ضربدر کلیک کنید و در شکل باز شده، بر روی Yes کلیک کنید.

www.takbook.com



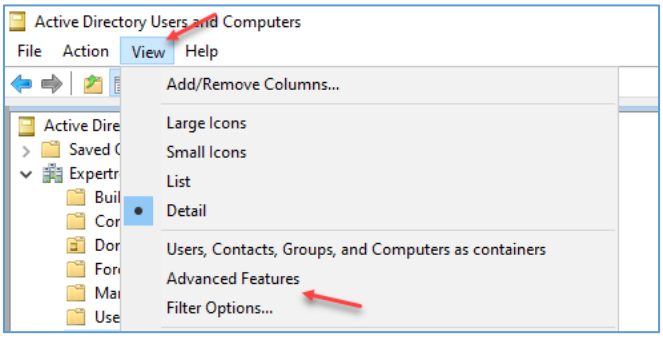
شکل ۸- ۱۳۳ حذف واحدهای سازمانی

همان‌طور که مشاهده می‌کنید با خطای شکل ۸-۱۳٤، مواجه شدیم. این Error به این نکته اشاره دارد که شما مجوز لازم برای حذف Object موردنظر را ندارید. به خاطر اینکه در موقع ایجاد OU تیک مربوط به گزینه‌ی Protect Container form accidental deletion را زده بودیم، برای حذف آن به صورت زیر عمل کنید:



شکل ۸- ۱۳۴ حذف واحدهای سازمانی

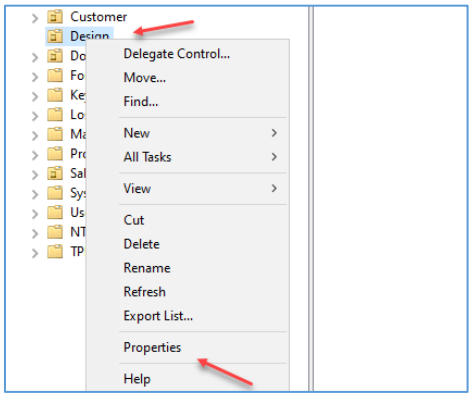
به مانند شکل ۸-۱۳۵، بر روی منوی View کلیک کنید و گزینه‌ی Advanced Features را انتخاب کنید.



شکل ۸- ۱۳۵ حذف واحدهای سازمانی

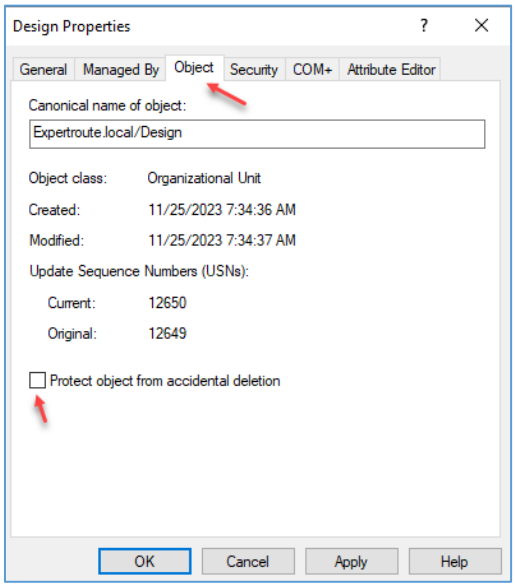
www.takbook.com

بعد از انجام کار قبلی، به مانند شکل ۸-۱۳۶، بر روی واحد سازمانی موردنظر کلیک راست می‌کنیم و گزینه‌ی Properties را انتخاب می‌کنیم تا شکل ۸-۱۳۷، ظاهر شود.



شکل ۸- ۱۳۶ حذف واحدهای سازمانی

در شکل ۸-۱۳۷، وارد تب Object شوید و تیک گزینه ی Protect Container form accidental deletion را بردارید و بر رو OK کلیک کنید.



شکل ۸- ۱۳۷ حذف واحدهای سازمانی

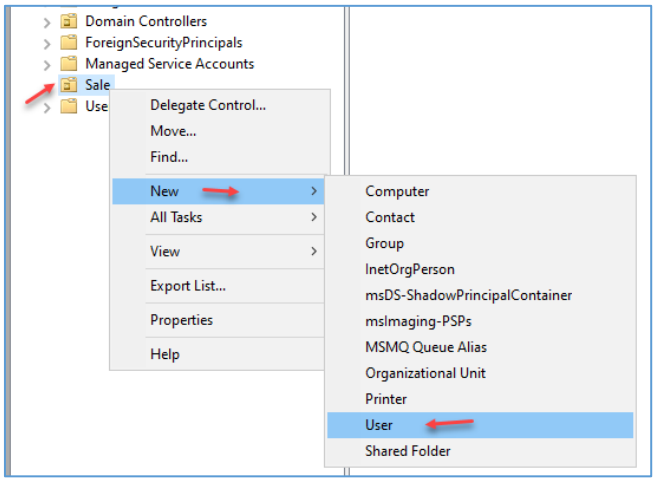
نکته مهم: زمانی که می‌خواهید یک واحد سازمانی را حذف کنید، توجه کنید که واحد سازمانی دیگری به صورت محافظت شده، زیر مجموعه‌ی واحد سازمانی در حال حذف نباشد؛ چون OU یا همان واحد سازمانی موردنظر حذف نخواهد شد؛ چون یک واحد سازمانی دیگر به صورت محافظت شده در زیر مجموعه آن قرار دارد.

www.takbook.com

۳-۱۰-۳-۸ 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.

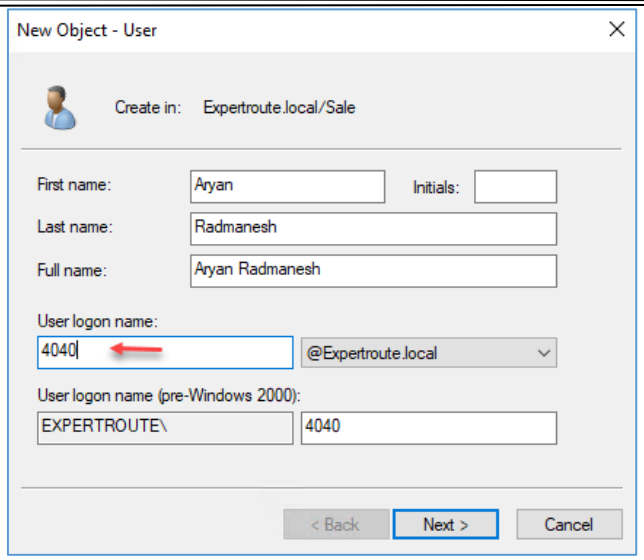
برای تعریف کاربر باید به مانند شکل ۸-۱۳۸، بر روی واحد مورد نظر خود (Sale) کلیک راست کنید و از قسمت New، گزینه‌ی User را انتخاب کنید.



شکل ۸- ۱۳۸ تعریف کاربر در Active directory

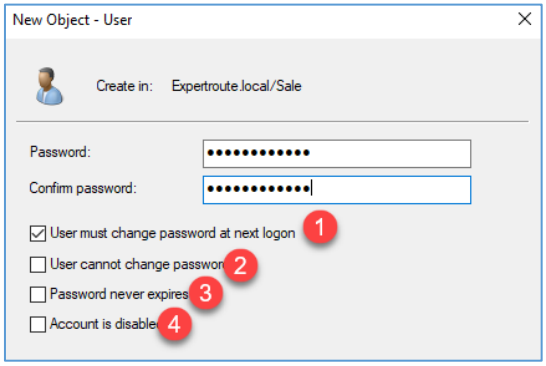
در شکل ۸-۱۳۹، در قسمت First Name، نام کاربر خود را وارد کنید و اگر این کاربر، اسم مستعار دارد، می‌توانید در قسمت Initials وارد کنید، در قسمت Last Name نیز نام خانوادگی کاربر مورد نظر را وارد کنید که بعد از ورود اطّلاعات در قسمت Full Name، نام کامل کاربر که در کلّ شبکه به نمایش در خواهد آمد را می‌بینید؛ 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 ۱۰۰ می‌تواند وارد شبکه شود، اصولاً استفاده از شماره برای نام کاربری بهترین راه حل برای مدیریت درست و آسان‌تر کاربران است.

www.takbook.com



شکل ۸- ۱۳۹ تعریف کاربر در *Active directory*

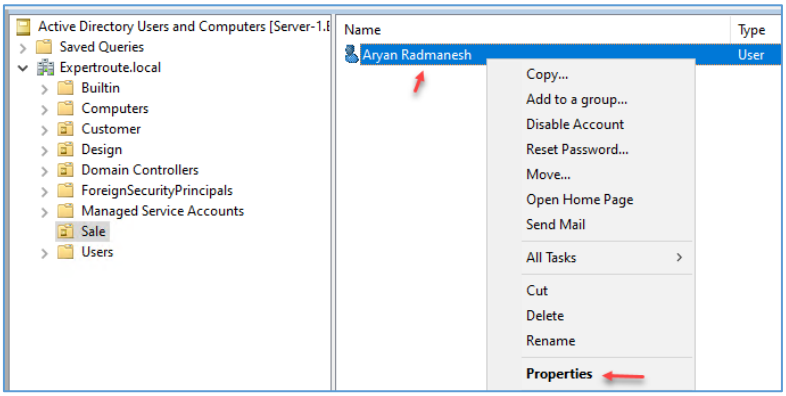
در شکل ۸-۱٤۰، باید برای کاربر مورد نظر، یک رمز عبور پیچیده، مانند ExpertRoute@2025 وارد کنید که البتّه می‌شود این پیچیدگی در رمز عبور را در سرویس Group Policy حذف کنید، گزینه‌های مختلفی نیز برای انتخاب وجود دارد که با انتخاب گزینه‌ی یک، کاربر مورد نظر با رمزی که وارد کردید، وارد سیستم می‌شود، امّا بعد از آورود به سیستم، از او درخواست تغییر رمز داده می‌شود که باید رمز جدید خود را وارد کند، 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 انقضاء نمی‌شود. شما به عنوان مدیر شبکه می‌توانید یک مدّت مشخّص را برای تغییر رمز عبور برای کاربران در سرویسGroup 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.



شکل ۸- ۱۴۰ تعریف کاربر در *Active directory*

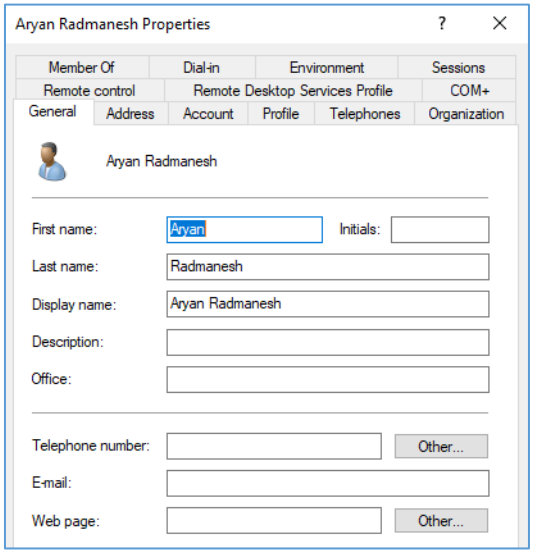
www.takbook.com

بعد از اینکه کاربر مورد نظر را ایجاد کردید این کاربر (100) به مانند شکل ۸-۱۴۱، در واحد سازمانی Sale قرار گرفته است، برای اینکه جزئیاتی از کاربر را بررسی کنیم بر روی آن کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۱۴۱ تعریف کاربر در *Active directory*

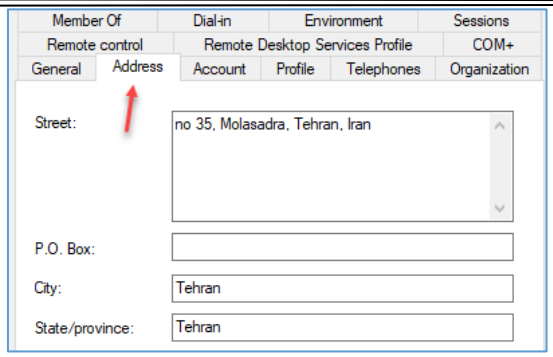
به مانند شکل ۸-۱۴۲، در تب General، اطلاعاتی را در مورد کاربر موردنظر مانند آدرس ایمیل، سایت و شماره‌ی تلفن و توضیحات مربوط به آن را مشاهده می‌کنید که بهتر است اطلاعات کاربران را به صورت کامل در این قسمت وارد کنید تا مدیریت آنها آسان‌تر باشد.



شکل ۸- ۱۴۲ تعریف کاربر در *Active directory*

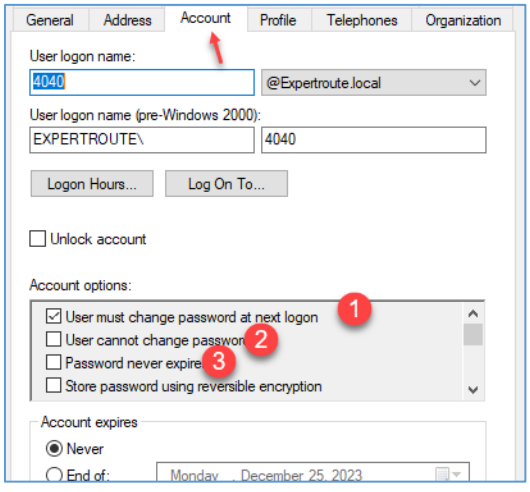
طبق شکل ۸-۱۴۳، در تب Address، می‌توانید آدرس محل کار یا سکونت کاربر مورد نظر را به صورت کامل وارد کنید.

www.takbook.com



شکل ۸- ۱۴۳ تعریف کاربر در *Active directory*

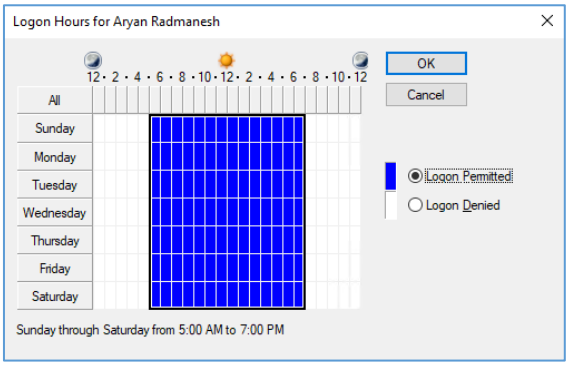
به مانند شکل ۸-۱٤٤، در تب Account، می‌توانید نام کاربری و تنظیمات آن را تغییر دهید؛ برای این کار در قسمت User logon name می‌توانید نام یا شماره کاربری را تغییر دهید. همان‌طور که گفتیم این نام برای ورود به ویندوز کاربرد دارد، در قسمت Account Options گزینه‌های مختلفی را مشاهده می‌کنید گزینه‌ی اول، برای این منظور به کار می‌رود که کاربر موردنظر بعد از ورود به ویندوز، باید رمز عبور خود را حتماً تغییر دهد. گزینه‌ی دوم، این توانایی را به مدیر شبکه می‌دهد تا از تغییر رمز عبور توسط کاربر جلوگیری کند، گزینه‌ی سوم را اگر انتخاب کنید، این رمز عبور به هیچ عنوان انقضاء نمی‌شود، درباره‌ی این موضوعات، در قسمت Group Policy بحث خواهیم کرد. اگر گزینه‌ی Account is disabled فعال باشد کاربر موردنظر غیرفعال خواهد شد و امکان ورود به ویندوز را نخواهد داشت، البته گزینه‌های دیگری هم در این قسمت وجود دارد که برای رمزنگاری و امنیت است که در وقت مناسب به آن خواهیم پرداخت. شما می‌توانید برای کاربران خود زمان ورود به ویندوز را مشخص کنید؛ برای این کار بر روی Logon Hours کلیک کنید تا شکل ۸-۱٤٤، ظاهر شود.



شکل ۸- ۱۴۴ تعریف کاربر در *Active directory*

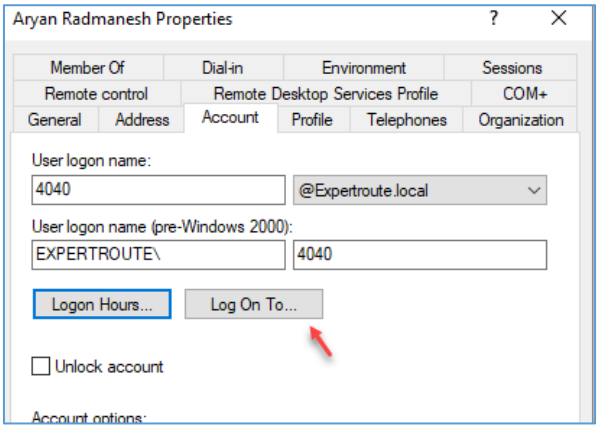
www.takbook.com

در شکل ۳-۹۹، می‌توانید زمان فعال بودن کاربر را مشخص کنید، مثلاً در این شکل کاربر فقط می‌تواند از روز یکشنبه تا پنج‌شنبه و از ساعت ٦ صبح تا ٦ بعد از ظهر وارد سیستم خود شود و به غیر از این زمان توانایی ورود نخواهد داشت.



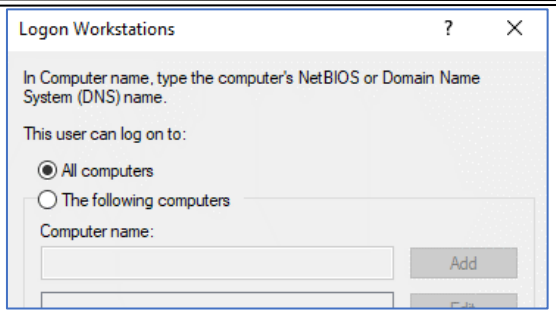
شکل ۸- ۱۴۵ تعریف کاربر در *Active directory*

در شکل ۸-۱٤٦، گزینه‌ای دیگر با نام Log On To وجود دارد که می‌توانید مشخص کنید که کاربر موردنظر از طریق چه سیستمی، توانایی ورود داشته باشد که در شکل ۸-۱٤۷، این موضوع مشخص شده است و به طور پیش‌فرض همه‌ی کاربران بر روی All Computers قرار دارند و برای اینکه آنها را به یک سیستم خاص محدود کنیم باید گزینه‌ی زیری آن را انتخاب و نام سیستم مورد نظر را به لیست وارد کنیم.



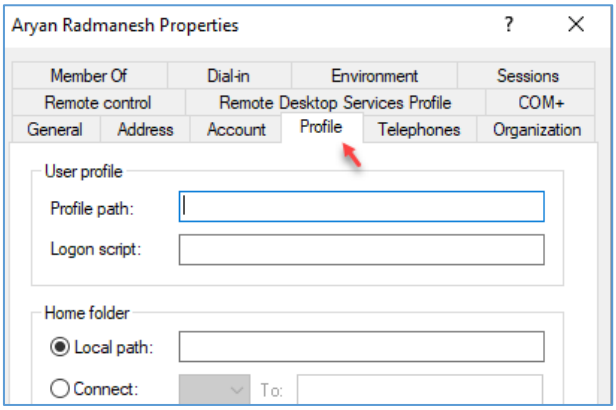
شکل ۸- ۱۴۶ تعریف کاربر در *Active directory*

www.takbook.com



شکل ۸- ۱۴۷ تعریف کاربر در *Active directory*

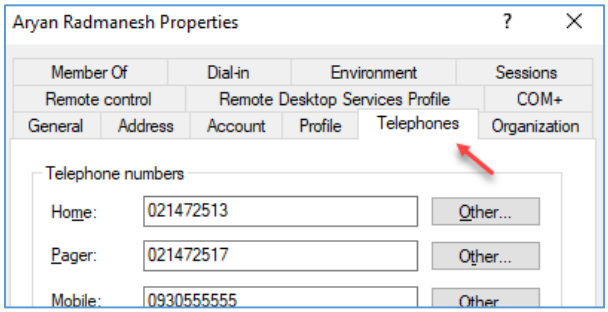
برای ادامه کار به مانند شکل ۸-۱۴۸، بر روی تب Profile کلیک کنید، تب Profile یکی از سودمندترین و پرکاربردترین تب‌ها می‌باشد. در این تب، شما می‌توانید برای تمام کاربران خود در قسمت User Profile یک محل مناسب برای Profile آن‌ها ایجاد کنید؛ یعنی Profile تمام کاربران در آدرسی درون سرور اصلی ایجاد شود و در قسمت Home Folder هم می‌توانید برای کاربران خود یک درایو مجازی ایجاد کنید که تمام اطلاعات خود را درون همان درایو قرار دهند؛ این درایو، پوشه‌ای درون سرور اصلی می‌باشد که برای بقیه‌ی کاربران Share شده است. توجه داشته باشید در درس‌های بعد کاملاً به این موضوع خواهیم پرداخت.



شکل ۸- ۱۴۸ تعریف کاربر در *Active directory*

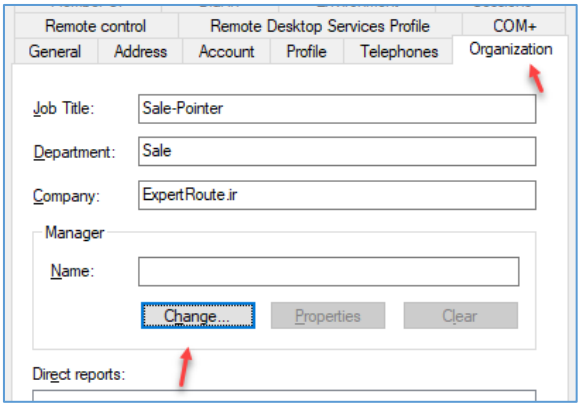
طبق شکل ۸-۱۴۹، در تب Telephones، اطلاعات تماس کاربر موردنظر را می‌توانید وارد یا مشاهده کنید.

www.takbook.com



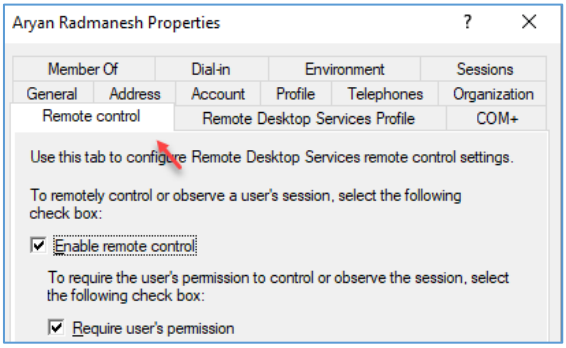
شکل ۸- ۱۴۹ تعریف کاربر در *Active directory*

طبق شکل ۸-۱۵۰، در تب Organization یا واحد سازمانی، می‌توانید نوع کار، واحد کاری، نام شرکت و مدیر کاربر موردنظر را مشخص کنید.



شکل ۸- ۱۵۰ تعریف کاربر در *Active directory*

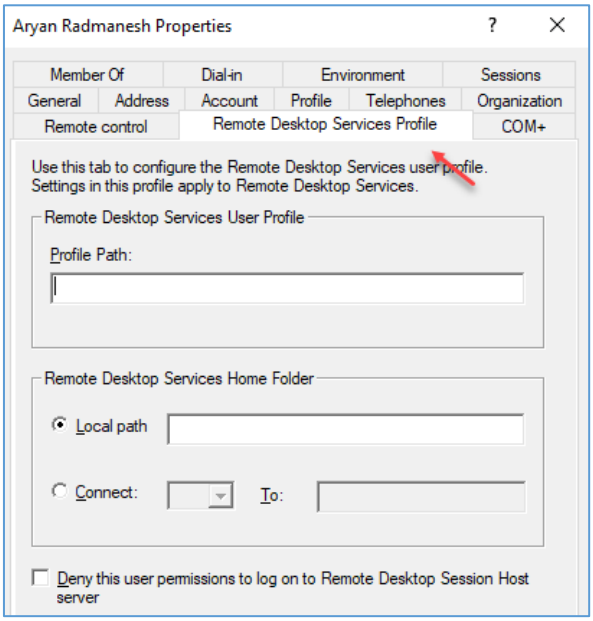
طبق شکل ۸-۱۵۱، در تب Remote Control، می‌توانیم به کاربر موردنظر این اجازه را بدهیم که در شبکه‌ی موردنظر توانایی Remote یا ارتباط از راه دور به سیستم دیگر را داشته باشد.



شکل ۸- ۱۵۱ تعریف کاربر در *Active directory*

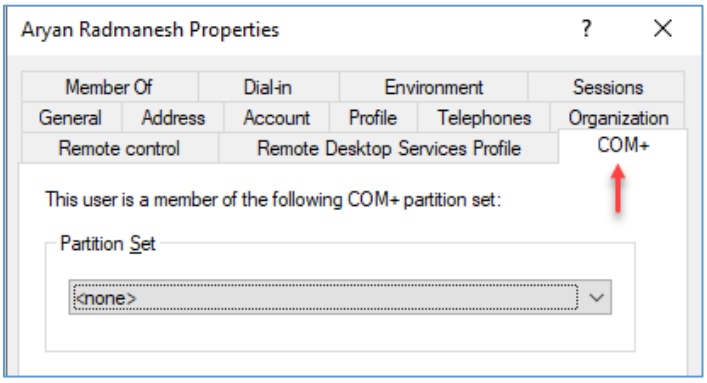
www.takbook.com

به مانند شکل ۸-۱۵۲، در تب Remote Desktop Service Profile، به مانند تب Profile، شما می‌توانید برای کاربران خود که به صورت Remote، وارد سیستم دیگری می‌شوند، Profile مشخص و هارد دیسک مجازی روی سرور اصلی ایجاد کنید تا تمام اطلاعات آن‌ها ثبت و در دسترس باشد.



شکل ۸- ۱۵۲ تعریف کاربر در *Active directory*

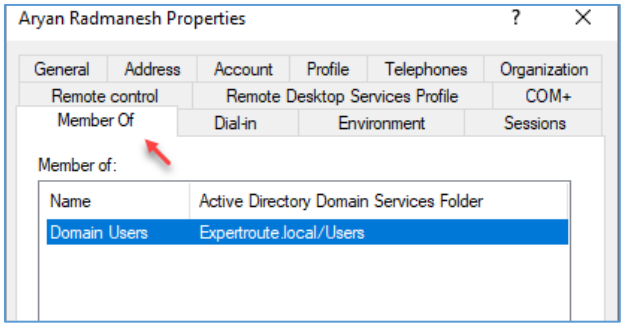
طبق شکل ۸-۱۵۳، در تب COM+ برای ایجاد Partitionهای خاص برای کاربران می‌باشد تا برنامه‌های COM خود را اجرا کنند. COM+ یک معماری برنامه نویسی شیءگرا است که توسط مایکروسافت ارائه شده تا بتواند با سیستم‌های تجزیه‌ی اطلاعات اوراکل و IBM رقابت کند.



شکل ۸- ۱۵۳ تعریف کاربر در *Active directory*

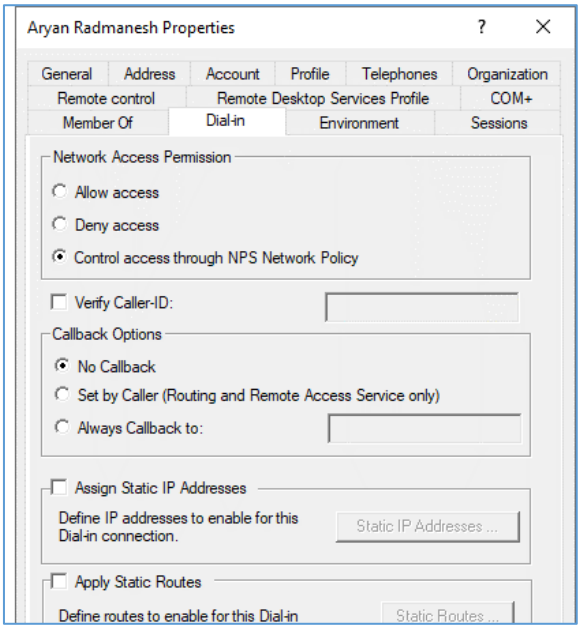
www.takbook.com

طبق شکل ۸-۱۵٤، در تب Member Of، این توانایی را داریم تا کاربر موردنظر را عضو گروه خاصی کنید یکی از ویژگی‌های این تب این است که شما می‌توانید یک گروه ایجاد کنید و مجوزهای خاصی را به آن بدهید و بقیه ی کاربران را عضو آن گروه کنید و دیگر لازم نیست به تک تک کاربران مجوز دسترسی بدهید.



شکل ۸- ۱۵۴ تعریف کاربر در Active directory

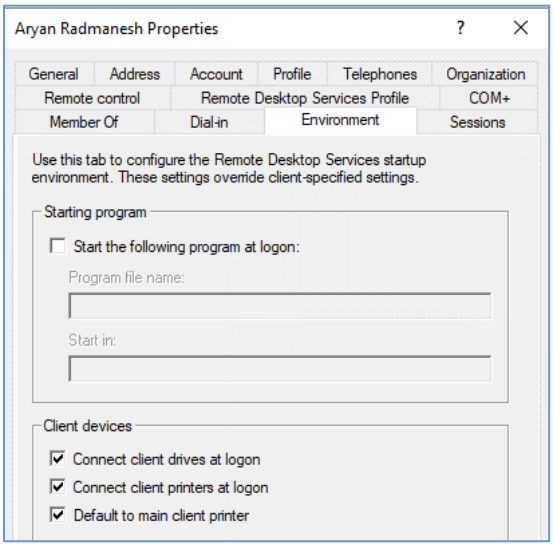
طبق شکل ۸-۱۵۵، در تب Dial-in، این توانایی را به کاربر می‌دهید تا بتوانند بیرون از شبکه‌ی سازمانی به شبکه داخلی سازمان متصل شوند، در این قسمت، می‌توانیم برای کاربر موردنظر IP Address را به صورت دستی وارد کنید و کارهای مختلف انجام دهیم.



شکل ۸- ۱۵۵ تعریف کاربر در Active directory

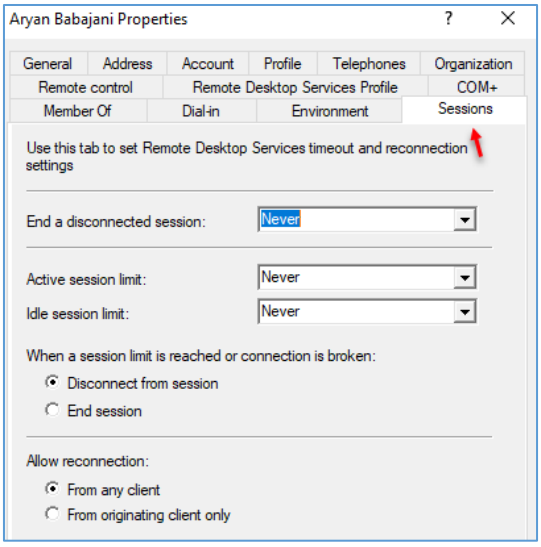
www.takbook.com

طبق شکل ۸-۱۵۶، در تب Environment، می‌توانید مشخص کنید که زمانی که کاربر وارد سیستم می‌شود، چه نرم‌افزاری برای وی توانایی اجرا شدن داشته باشد.



شکل ۸- ۱۵۶ تعریف کاربر در Active directory

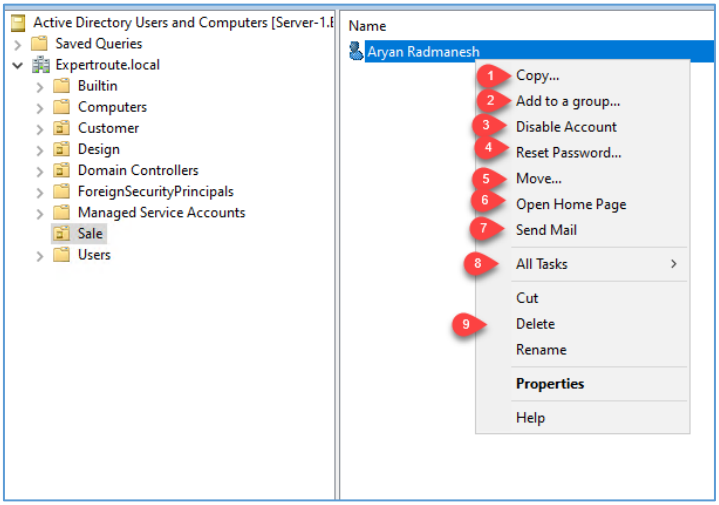
طبق شکل ۸-۱۵۷، در تب Sessions شما به عنوان مدیر شبکه این توانایی را دارید تا مشخص کنید که کاربر موردنظر تا چه زمانی در یک سیستم قرار داشته باشد و یا می‌توانید مشخص کنید که زمانی که کاربر بر روی سیستم قرار ندارد و سیستم بیکار است تا چه زمانی از ویندوز خارج شود.



شکل ۸- ۱۵۷ تعریف کاربر در Active directory

www.takbook.com

بعد از بررسی تب‌های مربوط به کاربر مورد نظر به مانند شکل ۸-۱۵۸، دوباره بر روی کاربر مورد نظر کلیک راست کنید.



شکل ۸- ۱۵۸ تعریف کاربر در Active directory

با انتخاب گزینه‌ی اول یعنی Copy توانایی این را دارید که ویژگی‌های یک کاربر را برای کاربر مورد نظر که قرار است ایجاد کنید قرار دهید، یعنی اگر در تب‌های آدرس یک کاربر اطلاعات کپی کرده باشید، همان اطلاعات برای کاربر جدید هم در نظر گرفته خواهد شد.

در قسمت شماره‌ی دوم یعنی Add to Group می‌توانید کاربر مورد نظر عضو گروه خاص کنید، در قسمت شماره‌ی سوم یعنی Disable Account می‌توانید کاربر مورد نظر را غیرفعال کنید، در قسمت شماره‌ی چهار یعنی Reset Password می‌توانید رمز کاربر را به راحتی ریست کنید حتی اگر رمز اولیه کاربر را نداشته باشید، در قسمت شماره‌ی پنج یعنی Move می‌توانید کاربر مورد نظر را از یک واحد سازمانی به واحد سازمانی دیگر انتقال دهید و یا اینکه کاربر را بکشید و رها کنید، در قسمت شماره‌ی شش یعنی Open Home Page اگر چنانچه در تب General آدرس وب مربوط به کاربر مورد نظر را وارد کرده بودید صفحه مربوط به آن باز خواهد شد، در قسمت شماره‌ی هفت می‌توانید طبق ایمیلی که برای کاربر مشخص کردید برای کاربر مورد نظر ایمیل ارسال کنید، در قسمت شماره‌ی هشت هم می‌توانید کارهای گفته شده‌ی قبل را انجام دهید و در قسمت شماره‌ی نه هم می‌توانید کاربر را حذف، برش و تغییر نام دهید.

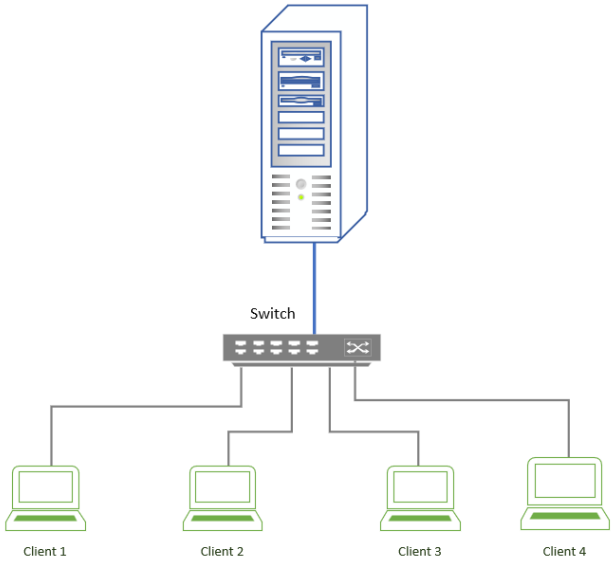
٤-١٠-٣-٨ عضو کردن کلاینت در دومین

برای اینکه کاربری که ایجاد کردیم را بررسی و تست کنیم باید با آن کاربر وارد شبکه شویم و کارهایی که قرار است در شبکه انجام دهد را با هم انجام دهیم، به خاطر این موضوع یک ماشین مجازی که قبلاً با ویندوز ۷ ایجاد کردیم را عضو شبکه‌ی دومین (Expertroute.local) می‌کنیم و کارهای مورد نظر خود را

www.takbook.com

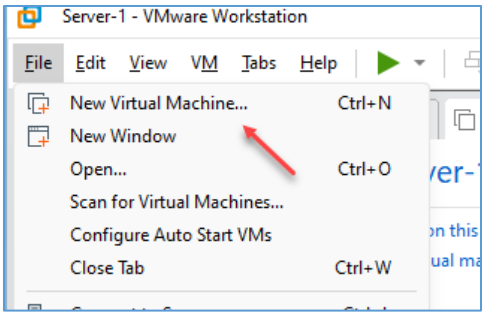
انجام می‌دهیم، توجه داشته باشید اگر یک کلاینت عضو شبکه نباشد، مدیریّت آن به شدّت سخت خواهد شد، برای اینکه مدیریّت کلاینت‌ها و کاربران آسان‌تر شود، بهتر است آنها را عضو دومین کنید تا مدیریّت آنها متمرکز شود.

در شکل ۸-۱۵۹، نقشه‌ی کلّی از یک شبکه‌ی کوچک را مشاهده می‌کنید، اگر این کلاینت‌ها عضو شبکه‌ی Expertroute.local 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 تا خیال خودتان را راحت کنید.



شکل ۸- ۱۵۹ عضو کردن کلاینت در دومین

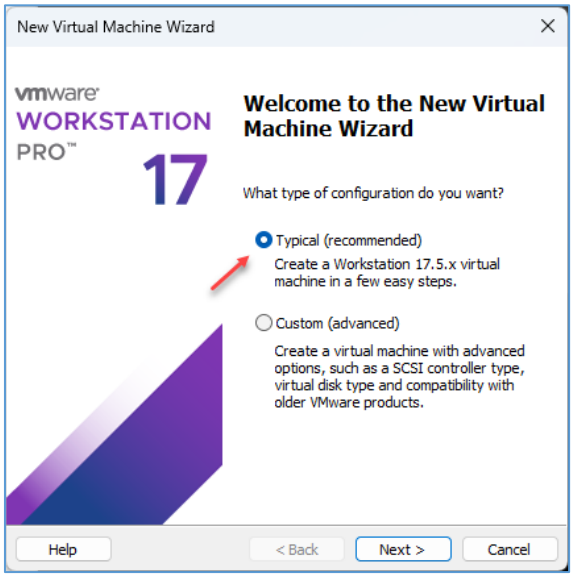
برای شروع کار یک ماشین مجازی با ویندوز ۱۱ ایجاد و شبکه آن را به سرور متصل می‌کنیم، به مانند شکل ۸-۱۶۰، ماشین مجازی ایجاد می‌کنیم.



شکل ۸- ۱۶۰ عضو کردن کلاینت در دومین

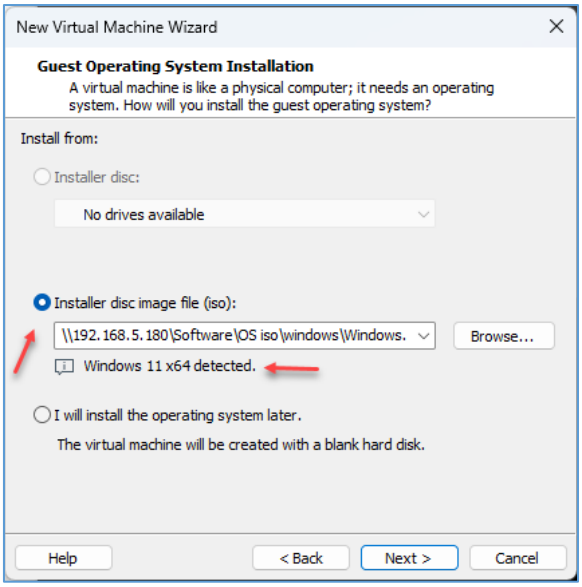
در شکل ۸-۱۶۱، گزینه‌ی Typical را انتخاب کنید.

www.takbook.com



شکل ۸- ۱۶۱ عضو کردن کلاینت در دومین

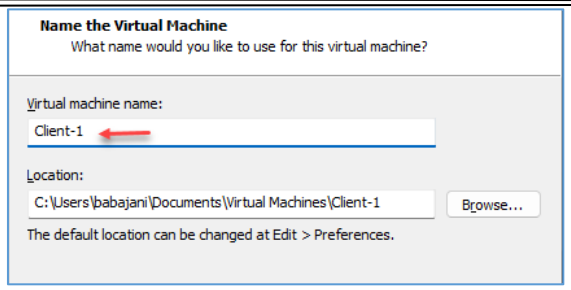
در شکل ۸-۱۶۲، باید فایل مربوط به ویندوز ۱۱را به نرم‌افزار معرفی کنید که اگر توجه کنید ورژن ویندوز به صورت اتوماتیک شناسایی می‌شود.



شکل ۸- ۱۶۲ راه‌اندازی ماشین مجازی

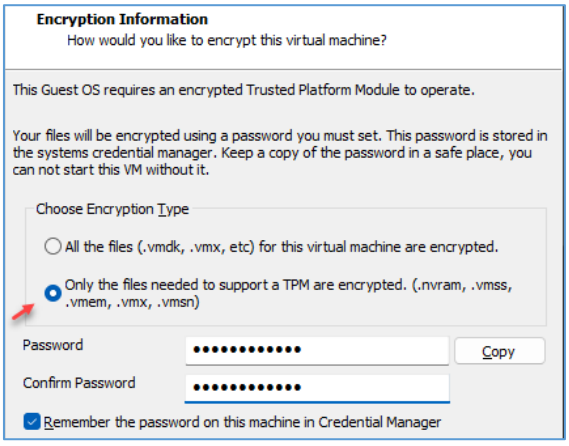
در شکل ۸-۱۶۳، نام ماشین را وارد کنید و مسیر ذخیره آن را مشخص کنید.

www.takbook.com



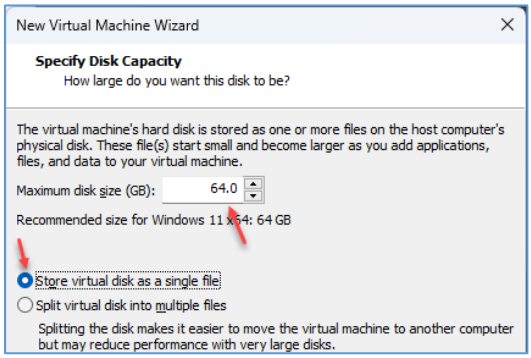
شکل ۸- ۱۶۳ راه‌اندازی ماشین مجازی

در شکل ۸-۱٦٤، می‌توانید برای امنیت بیشتر بر روی فایل‌های ماشین مجازی خود رمز عبور تخصیص دهید و در موقع اجرا باید رمز را وارد کنید.



شکل ۸- ۱۶۴ راه‌اندازی ماشین مجازی

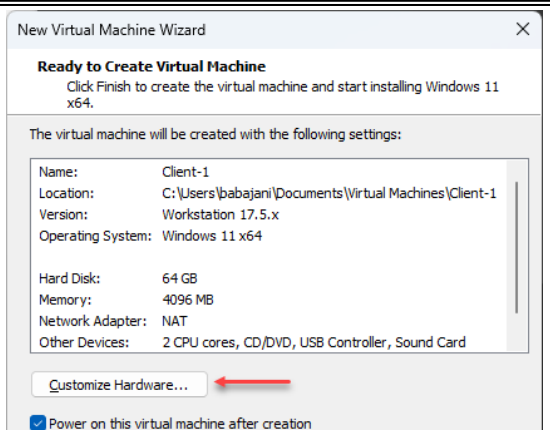
در شکل ۸-۱٦٥، مقدار فضای هارد دیسک و تک فایلی بودن آن را انتخاب کنید.



شکل ۸- ۱۶۵ راه‌اندازی ماشین مجازی

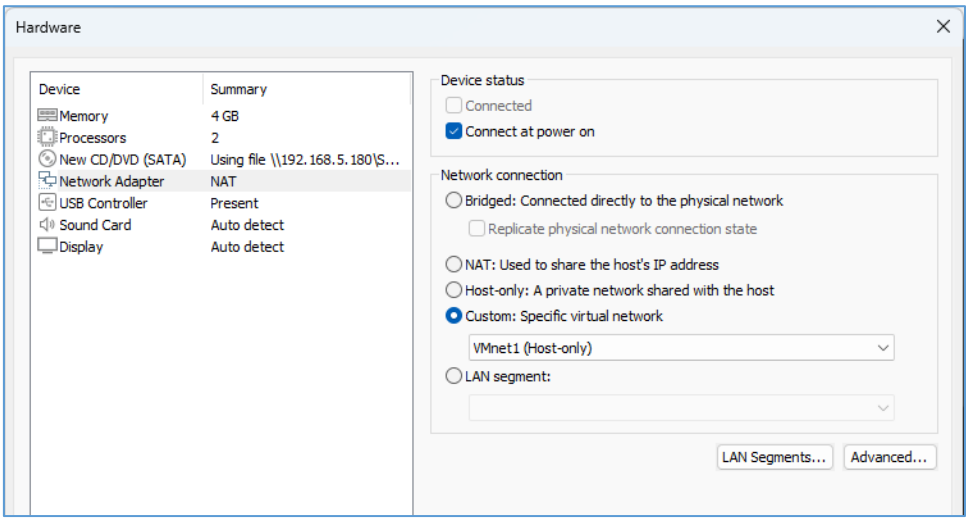
در شکل ۸-۱٦٦، بر روی Customize کلیک کنید تا کارت شبکه ماشین مورد نظر را تنظیم کنیم.

www.takbook.com



شکل ۸- ۱۶۶ راه‌اندازی ماشین مجازی

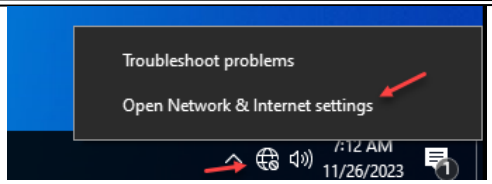
در شکل ۸-۱۶۷، باید کارت شبکه‌ی ماشین مجازی را بر روی VMnet1 قرار دهید تا بتواند با سرور اصلی ما ارتباط برقرار کند.



شکل ۸- ۱۶۷ راه‌اندازی ماشین مجازی

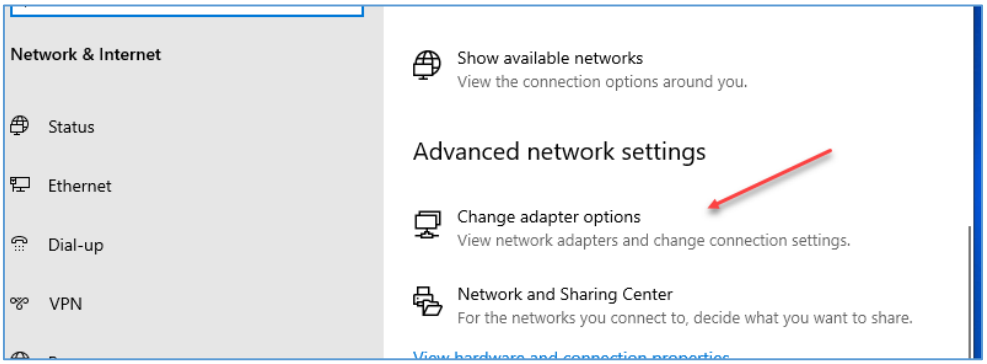
بعد از اینکه ماشین مجازی با ویندوز ۱۱راه‌اندازی کردید باید به مانند شکل ۸-۱۶۸، یک آدرس IP به صورت دستی در رنج شبکه اصلی وارد کنید، برای این کار بر روی آیکون شبکه کلیک راست کنید و گزینه‌ی Open Network & internet settings را انتخاب کنید.

www.takbook.com



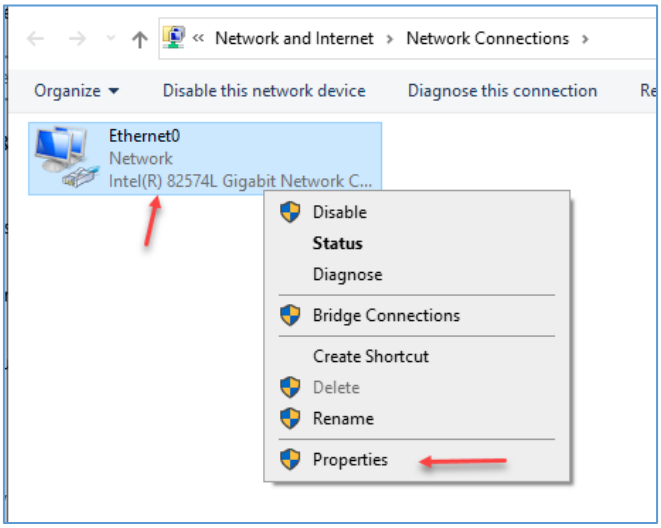
شکل ۸- ۱۶۸ تنظیم کارت شبکه

در شکل ۸-۱۶۹، بر روی Change adaptor options کلیک کنید.



شکل ۸- ۱۶۹ تنظیم کارت شبکه

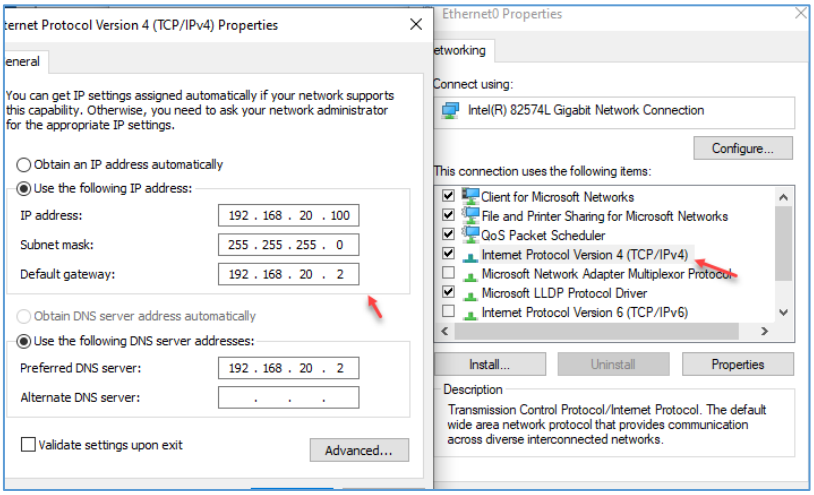
در شکل ۸-۱۷۰، بر روی کارت شبکه‌ی مورد نظر کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۱۷۰ تنظیم کارت شبکه

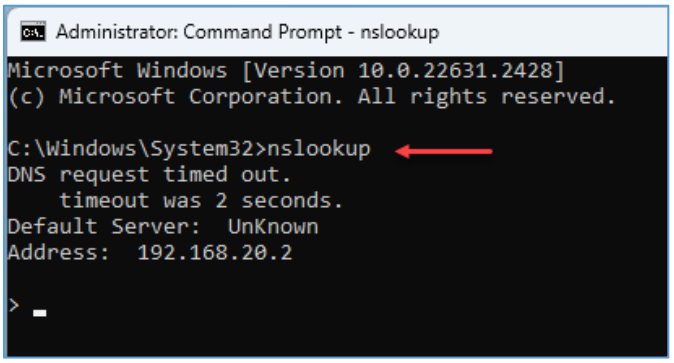
در شکل ۸-۱۷۱، بر روی IPv4 دو بار کلیک کنید و آدرس 192.168.20.100 را به همراه آدرس DNS که همان سرور اصلی ما است وارد کنید و بر روی OK کلیک کنید.

www.takbook.com



شکل ۸- ۱۷۱ تنظیم کارت شبکه

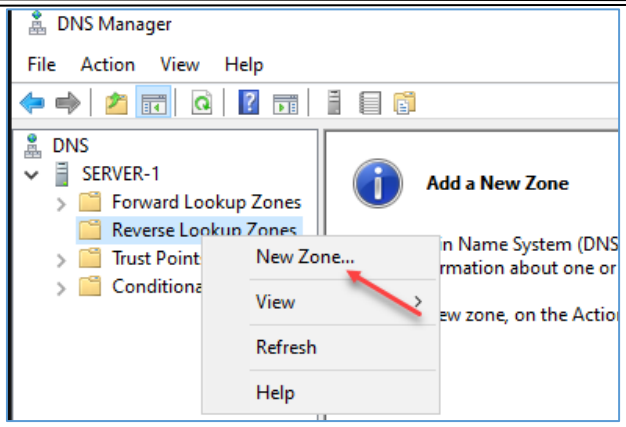
برای اینکه متوجه شویم سیستم به درستی به شبکه ما متصل است از دستور Nslookup استفاده می‌کنیم که این کار را در شکل ۸-۱۷۲، مشاهده می‌کنید که کلاینت مورد نظر با آدرس DNS که براش قرار داده بودیم توانست سرور اصلی ما را پیدا کند و این یعنی اینکه کلاینت آماده برای Join شدن با سرور دومین ما است، توجه داشته باشید اگر به مانند شکل ۸-۱۷۲، نام سرور DNS و آدرس IP آن را مشاهده نکنید نمی‌توانید کلاینت را عضو دومین مورد نظر خود کنید.



شکل ۸- ۱۷۲ دستور nslookup

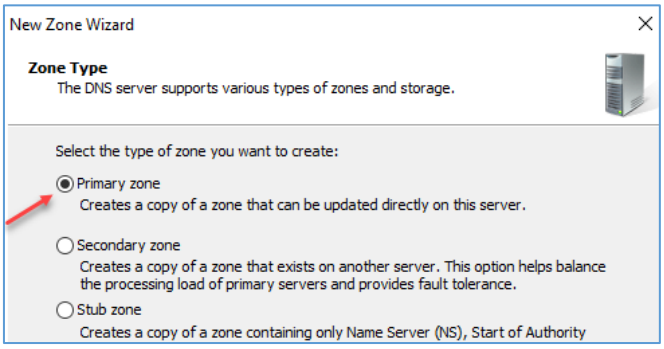
برای حل این مشکل به مانند شکل ۸-۱۷۳، وارد DNS شوید و بر روی Reverse Lookup Zones کلیک راست کنید و گزینه‌ی New Zones را انتخاب کنید، همان‌طور که گفتیم این قسمت برای تبدیل IP به اسم است که در قسمت DNS به صورت کامل بررسی کردیم ولی یک بار دیگر به صورت عملی آن را انجام می‌دهیم.

www.takbook.com



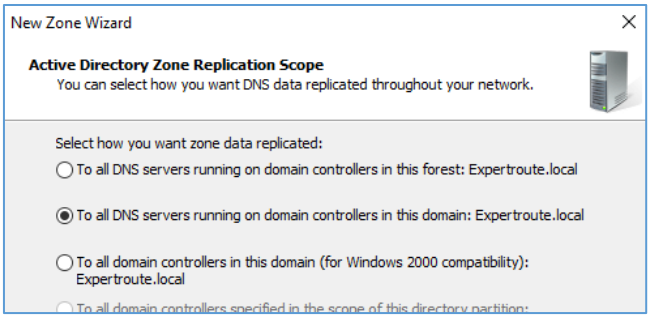
شکل ۸- ۱۷۳ تنظیم *DNS*

در شکل ۸-۱۷٤، گزینه‌ی Primary Zone را انتخاب کنید.



شکل ۸- ۱۷۴ تنظیم *DNS*

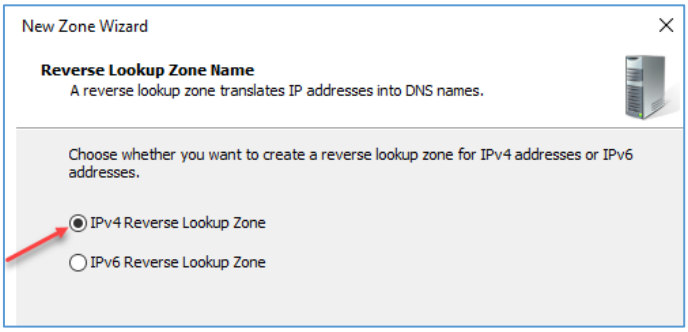
در شکل ۸-۱۷۵، گزینه‌ی دوم را انتخاب کنید، این موارد را قبلاً در بخش سرویس DNS توضیح دادیم که می‌توانید به همان بخش مراجعه کنید.



شکل ۸- ۱۷۵ تنظیم *DNS*

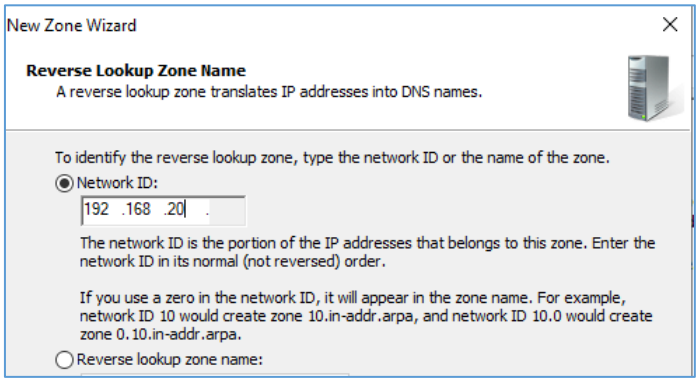
در شکل ۸-۱۷٦، گزینه‌ی IPv4 را انتخاب کنید و بر روی Next کلیک کنید.

www.takbook.com



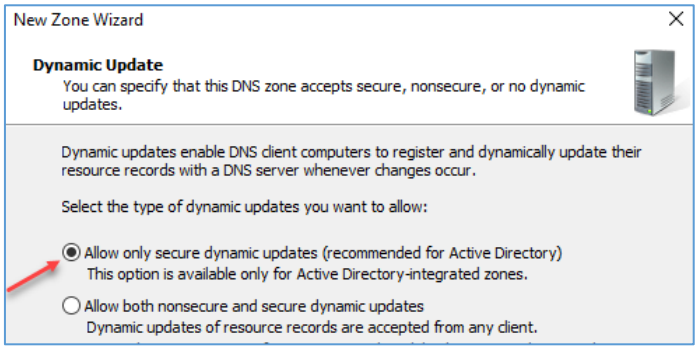
شکل ۸- ۱۷۶ تنظیم *DNS*

در شکل ۸-۱۷۷، شبکه‌ی خود را وارد کنید و بر روی Next کلیک کنید.



شکل ۸- ۱۷۷ تنظیم *DNS*

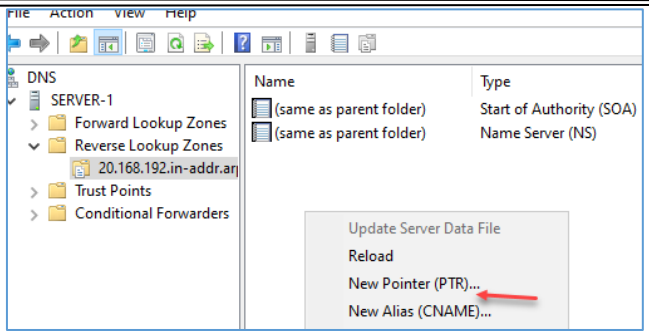
در شکل ۸-۱۷۸، باید گزینه‌ی اول را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۱۷۸ تنظیم *DNS*

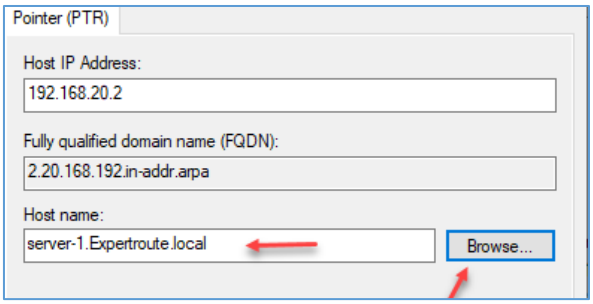
در شکل ۸-۱۷۹، بعد از ایجاد Zone مورد نظر بر روی صفحه مشخص شده کلیک راست کنید و گزینه‌ی PTR را انتخاب کنید.

www.takbook.com



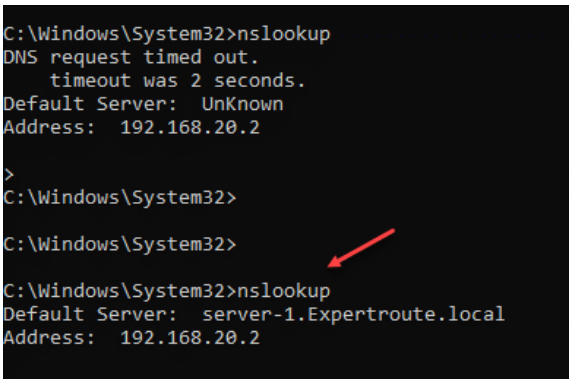
شکل ۸- ۱۷۹ تنظیم DNS

در شکل ۸-۱۸۰، در قسمت Host IP Address باید آدرس سرور DNS اصلی را وارد کنید و در قسمت Host name باید نام سرور را از طریق دکمه Browse انتخاب کنید و بر روی OK کلیک کنید.



شکل ۸- ۱۸۰ تنظیم DNS

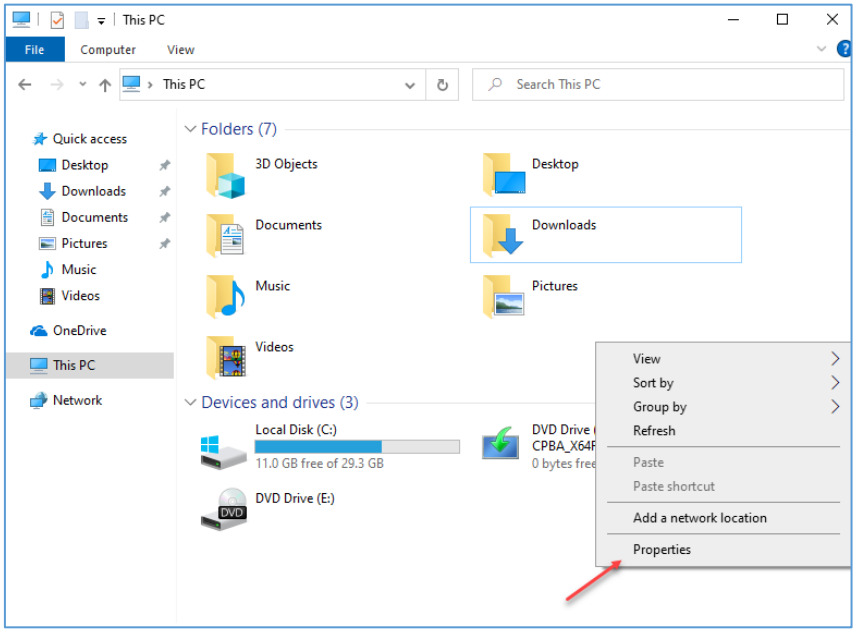
در شکل ۸-۱۸۱، اگر دستور Nslookup را اجرا می‌کنید سرور DNS که همان سرور Active Directory است با موفقیت در دسترس قرار گرفته است و حالا همه چیز برای Join کردن ماشین در دومین فعال است.



شکل ۸- ۱۸۱ تنظیم DNS

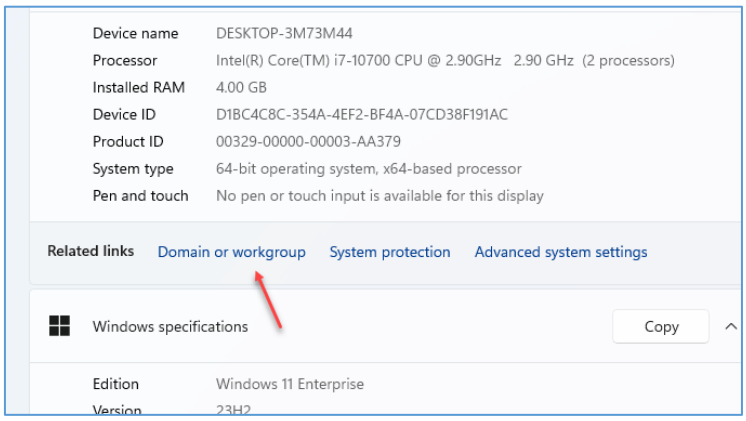
www.takbook.com

به مانند شکل ۸-۱۸۲، وارد کلاینت شوید و در My Computer کلیک راست کنید گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۱۸۲ عضو کردن دومین

به مانند شکل ۸-۱۸۳، بر روی Domain or Workgroup کلیک کنید تا شکل ۸-۱۸٤، ظاهر شود.

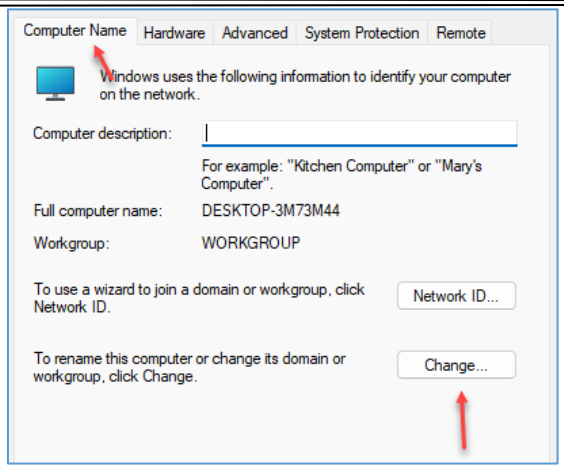


شکل ۸- ۱۸۳ عضو کردن دومین

در شکل ۸-۱۸٤، بر روی Change کلیک کنید.

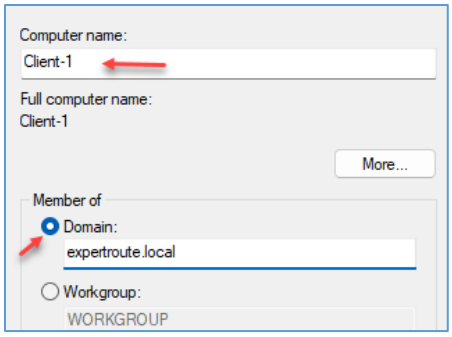
نکته: برای باز کردن صفحه‌ی شکل ۸-۱۸٤، می‌توانید از دستور sysdm.cpl در Run استفاده کنید تا دقیقاً همین صفحه باز شود.

www.takbook.com



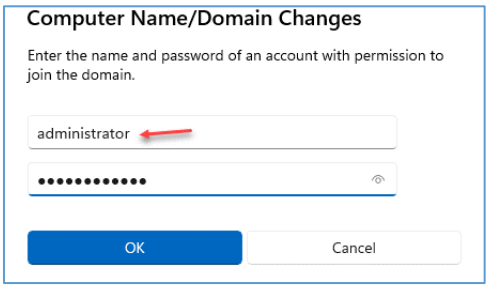
شکل ۸- ۱۸۴ عضو کردن دومین

در ادامه و در شکل ۸–۱۸۵، در قسمت Computer Name باید نام کلاینت را وارد کنید و در قسمت Member of گزینه‌ی Domain را انتخاب کنید و نام دومین را وارد و بر روی OK کلیک کنید.



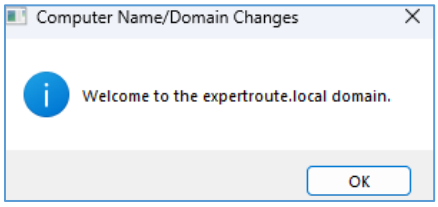
شکل ۸- ۱۸۵ عضو کردن دومین

در شکل ۸–۱۸۶، باید نام کاربری و رمز عبور کاربر Administrator را وارد کنید و بر روی OK کلیک کنید که بعد از کمی زمان شکل ۸–۱۸۷ ظاهر خواهد شد و نشان دهنده‌ی این است که کلاینت مورد نظر عضو دومین شده است.



شکل ۸- ۱۸۶ عضو کردن دومین

www.takbook.com

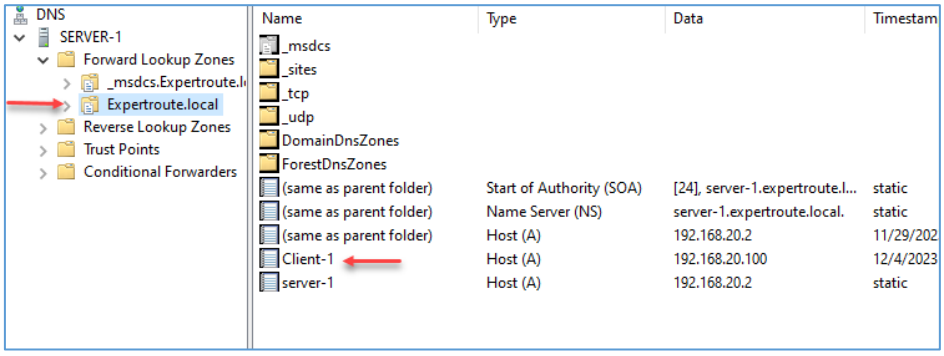


شکل ۸- ۱۸۷ عضو کردن دومین

بعد از انجام این کار کلاینت مورد نظر عضو دومین خواهد شد و نام آن در سرویس DNS و نیز Active Directory ثبت خواهد شد.

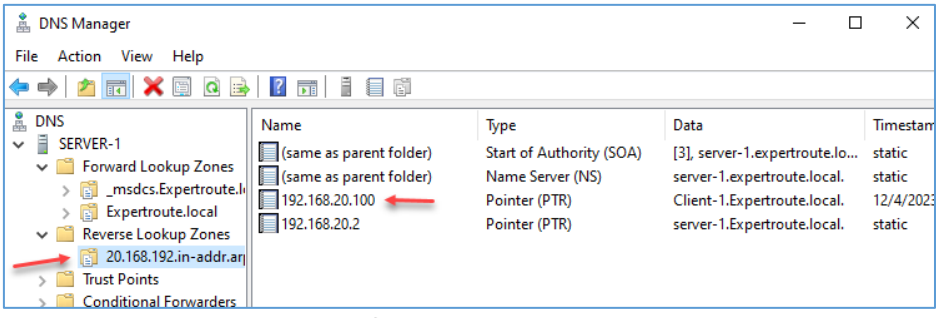
بعد از اینکه کلاینت عضو دومین شد، کلاینت را Restart کنید.

به مانند شکل ۸-۱۸۸، سرویس DNS و در Zone مربوطه، نام کلاینت Clinet-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 به صورت اتوماتیک در سرویس DNS ثبت شده است.



شکل ۸- ۱۸۸ بررسی سرویس DNS

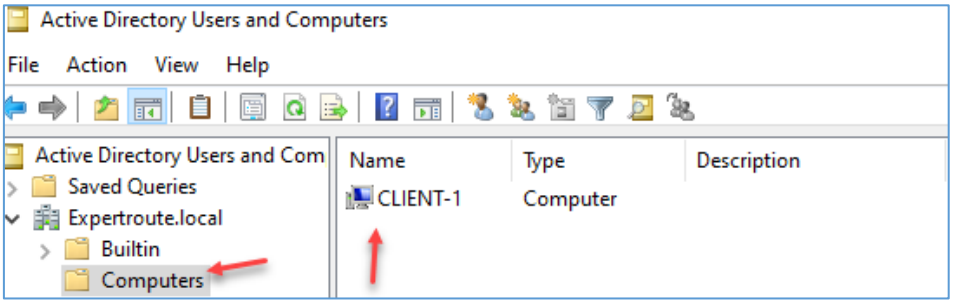
به مانند شکل ۸-۱۸۹، اگر وارد قسمت Reverse Zone شوید، مشاهده خواهید کرد که رکورد PTR مربوط به Clinet-1 نیز به صورت اتوماتیک ایجاد شده است.



شکل ۸- ۱۸۹ بررسی سرویس DNS

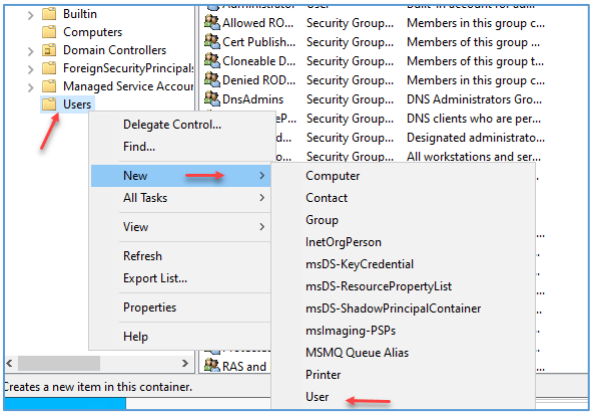
www.takbook.com

به مانند شکل ۸-۱۹۰، اگر در سرویس Active Directory وارد پوشه‌ی Computers شوید، نام کلاینت CLINET-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.



شکل ۸- ۱۹۰ بررسی سرویس Active

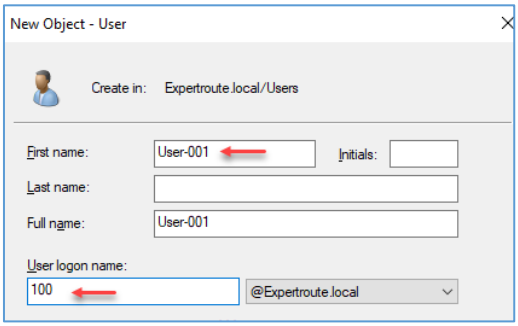
برای اینکه وارد کلاینت شویم نیاز به کاربر جدید داریم که با هم این کاربر را در Active Directory ایجاد می‌کنیم، در شکل ۸-۱۹۱، بر روی Users کلیک راست کنید واز قسمت New گزینه‌ی User را انتخاب کنید.



شکل ۸- ۱۹۱ بررسی سرویس Active

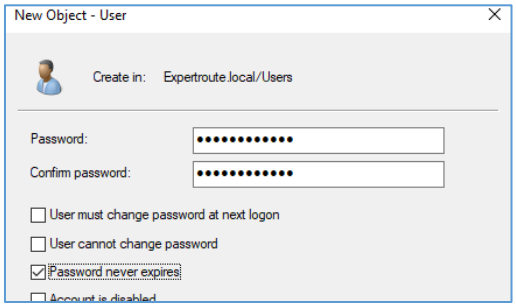
در شکل ۸-۱۹۲، اطلاعات کاربر را وارد کنید و نام کاربری را برای آن 100 در نظر می‌گیریم.

www.takbook.com



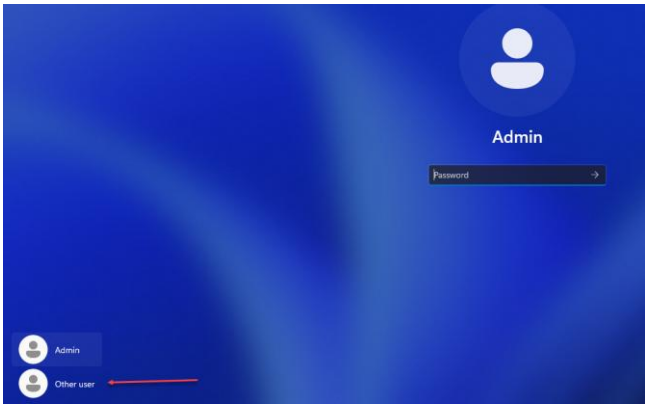
شکل ۸- ۱۹۲ بررسی سرویس *Active*

در شکل ۸-۱۹۳ رمز عبور پیچیده برای کاربر مورد نظر وارد و بر روی Next کلیک کنید.



شکل ۸- ۱۹۳ بررسی سرویس *Active*

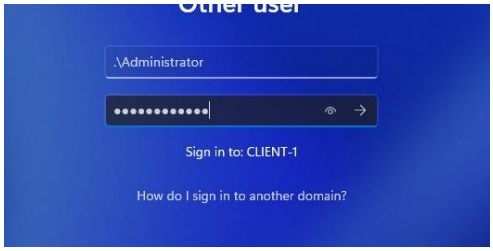
اگر به شکل ۸-۱۹٤، توجه کنید، نام Admin نوشته شده است که این کاربر، مربوط به کاربر Local خود کلاینت CLINET-1 است که اگر رمز آن را وارد کنید وارد کلاینت می‌شوید، امّا به صورت Local؛ اگر بخواهید وارد دومین شوید باید بر روی Other User کلیک کنید.



شکل ۸- ۱۹۴ ورود به کلاینت

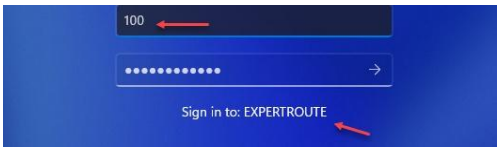
www.takbook.com

نکته: اگر چنانچه بخواهید با کاربر Local وارد کلاینتی شوید که نام آن را به خاطر نمی‌آورید، بهترین راه این است که به مانند شکل ۸–۱۹۵، از علامت "\." استفاده کنید، مثلاً اگر کاربر شما Adminitrator باشد، برای ورود به Local باید .\administrator را وارد کنید، همان‌طور که مشاهده می‌کنید، نام کلاینت در جلوی Sign in to نوشته شده است.



شکل ۸– ۱۹۵ ورود به کلاینت

برای ورود به دومین، طبق شکل ۸–۱۹۶، تنها کافی است که نام کاربری (100) که در دومین ایجاد کردید را وارد کنید و رمز عبور مربوط به آن را نیز بنویسید؛ به قسمت Sign in to توجّه کنید، نام دومین نوشته شده است، زمانی که نام دومین شما نوشته باشد یعنی کاربر مورد نظر باید در Active وجود داشته باشد تا بتواند وارد کلاینت شود.



شکل ۸– ۱۹۶ ورود به کلاینت

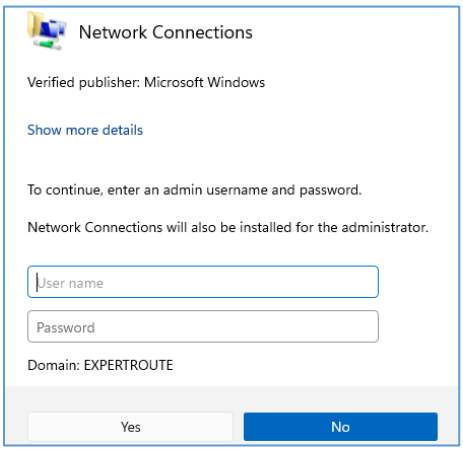
نکته مهم، زمانی که بخواهید از کاربر Administrator مربوط به دامین استفاده کنید به صورت شکل ۸–۱۹۷ دچار مشکل خواهید شد، دلیل آن هم این است که چون کاربر Administator در لیست کاربران Local کلاینت وجود دارد در قسمت Sign in to نام کلاینت نوشته می‌شود، برای حل این مشکل باید قبل از کاربر Administrator نام دومین را هم وارد کنید یعنی به صورت "expertroute\administrator" تا با کاربر Administrator دومین وارد کلاینت شوید و دسترسی کامل به منابع داشته باشید.



شکل ۸– ۱۹۷ ورود به کلاینت

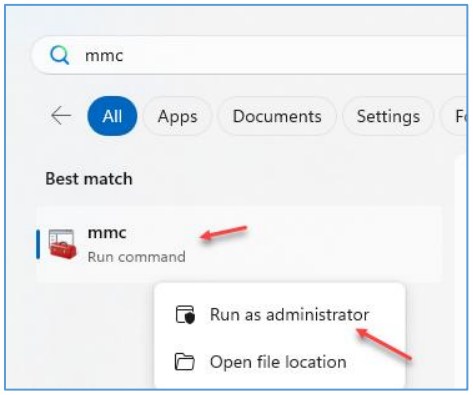
www.takbook.com

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 ۸-۱۹۸ آن را مشاهده می‌کنید. توصیه‌ی ما این است که این روند درخواست رمز عبور را حفظ کنید تا امنیّت شبکه افزایش پیدا کند.



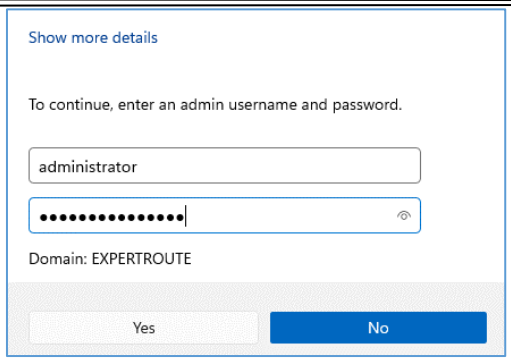
شکل ۸- ۱۹۸ درخواست رمز ادمین

امّا اگر بخواهید کاربر خاصّی را در سیستم خودش 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 ۸-۱۹۹، سرویس MMC را با اولویّت کاربر Administrator اجرا کنید و در پنجره‌ی باز شده شکل ۸-۲۰۰، نام کاربری ادمین را وارد کنید.



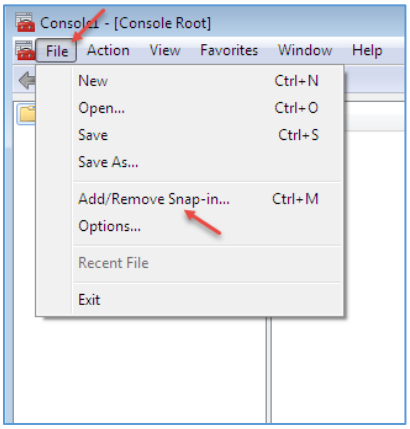
شکل ۸- ۱۹۹ ادمین کردن کاربر

www.takbook.com



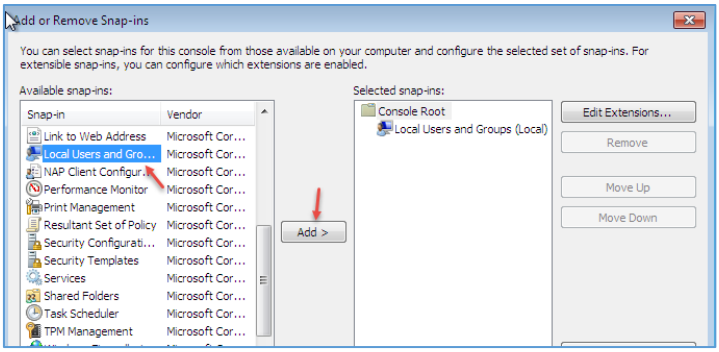
شکل ۸- ۲۰۰ ادمین کردن کاربر

به مانند شکل ۸-۲۰۱، وارد منوی File شوید و گزینه‌ی Add/Remove Snap-in... را انتخاب کنید.



شکل ۸- ۲۰۱ ادمین کردن کاربر

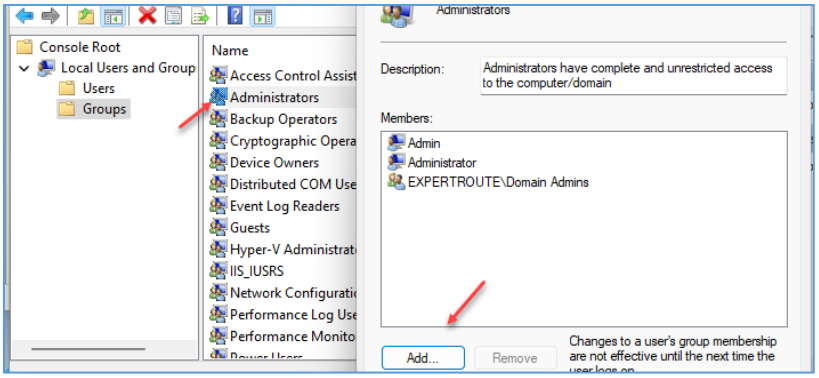
در شکل ۸-۲۰۲، از لیست مورد نظر، گزینه‌ی Local Users and Groups را با کلیک بر روی Add به لیست اضافه و بر روی OK کلیک کنید.



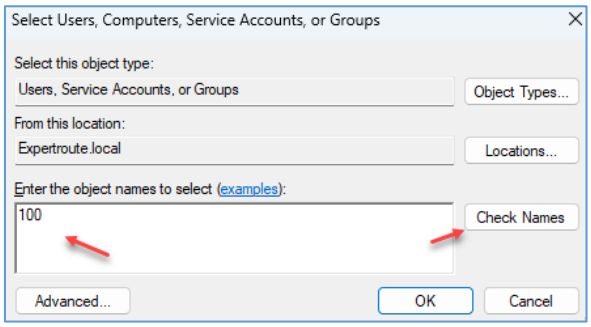
شکل ۸- ۲۰۲ ادمین کردن کاربر

www.takbook.com

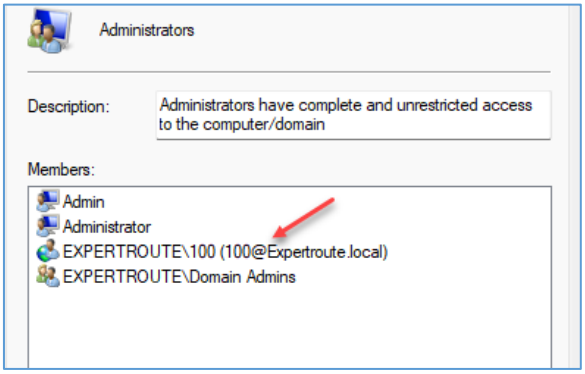
شکل ۸-۲۰۳، در این قسمت وارد پوشه‌ی Groups شوید و بر روی گروه Administrators، دو بار کلیک کنید و در پنجره‌ی باز شده بر روی Add کلیک کنید و کاربر مورد نظر دومین را به مانند شکل ۸-۲۰٤، به لیست اضافه کنید، بعد، کلاینت را Restart کنید، بعد از این کار، کاربر مورد نظر می‌تواند تنها در آن کلاینت دسترسی کامل داشته باشد.



شکل ۸- ۲۰۳ ادمین کردن کاربر



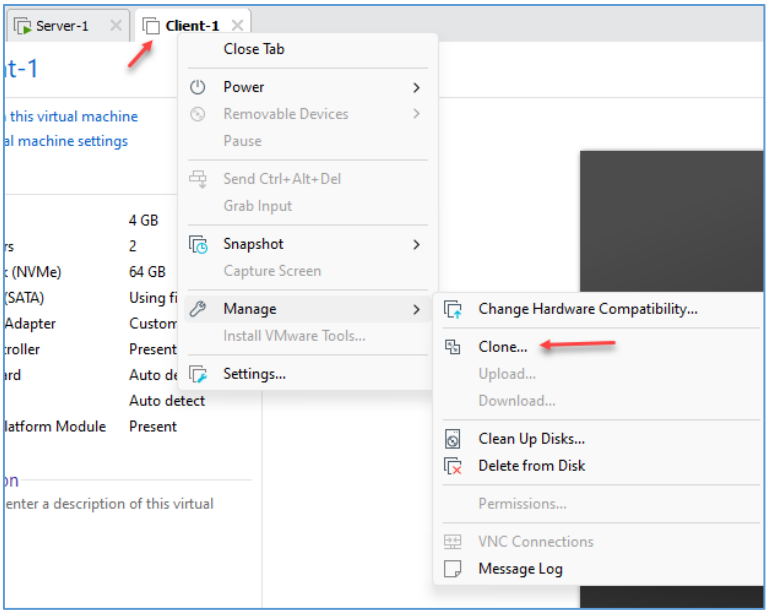
شکل ۸- ۲۰۴ ادمین کردن کاربر



شکل ۸- ۲۰۵ ادمین کردن کاربر

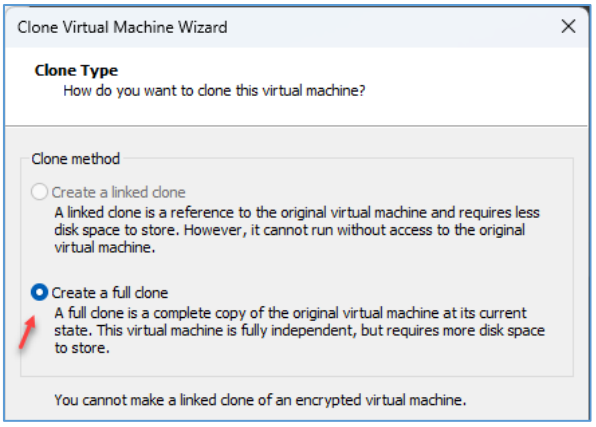
www.takbook.com

برای اینکه تنظیمات بیشتری را در Active Directory بررسی کنیم، از کلاینتی که در VMware Workstation ایجاد کردیم یک کپی (Clone) تهیه می‌کنیم و آن را با نام Clinet-2 عضو دومین می‌کنیم قبل از هر کاری ماشین مورد نظر (Client-1) را خاموش کنید و در ادامه به مانند شکل ۸–۲۰۶، بر روی ماشین مورد نظر کلیک راست کنید و گزینه‌ی Clone را انتخاب کنید.



شکل ۸– ۲۰۶ انجام Clone

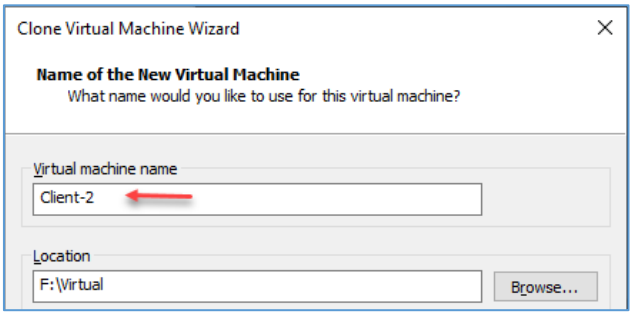
در شکل ۸–۲۰۷، گزینه‌ی دوم را انتخاب کنید تا یک کپی کامل از ماشین مورد نظر گرفته شود.



شکل ۸– ۲۰۷ انجام Clone

در شکل ۸–۲۰۸، باید نام ماشین و محل ذخیره‌سازی آن را مشخص کنید.

www.takbook.com



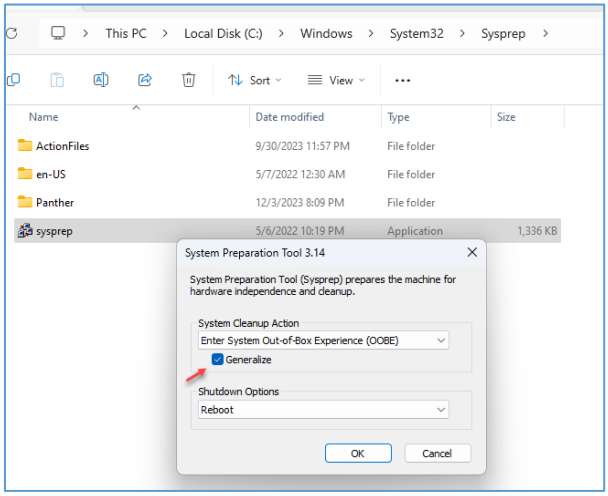
شکل ۸- ۲۰۸ انجام *Clone*

به عنوان تمرین وقتی که ماشین مورد نظر را روشن کردین آدرس IP آن را به 192.168.20.110 و نام آن را هم به Clinet-2 تغییر دهید.

یک مشکلی که در زمان Clone گرفتن از سرورها و کلاینت‌ها وجود دارد این است که هر کلاینتی که عضو دومین می‌شود دارای SSID مشخص و منحصر به فرد است و به خاطر همین موضوع زمانی که شما از کلاینت یا سرور مورد نظر Clone تهیه می‌کنید این SSID هم کپی می‌شود و وقتی ماشین کپی گرفته روشن شود ارتباط کلاینت قبلی را با دومین بر هم می‌زند، برای حل این مشکل سرویس به نام Sysprep در ریشه‌ی ویندوز وجود دارد که با فعال کردن آن سیستم‌عامل مورد نظر دوباره به تنظیمات اولیه باز می‌گردد و انگار یک سیستم‌عامل جدید نصب کردید.

برای انجام این کار وارد آدرس زیر شوید و به مانند شکل ۸-۲۰۹، فایل Sysprep را با دسترسی Administrator اجرا کنید، تیک گزینه‌ی Generalize را انتخاب و بر روی OK کلیک کنید.

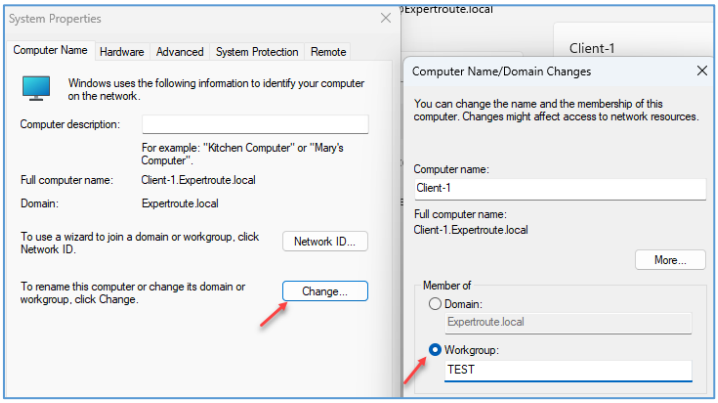
C:\Windows\System32\Sysprep



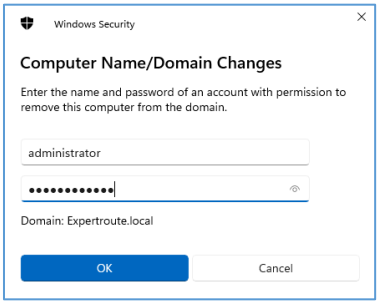
شکل ۸- ۲۰۹ اجرای *Sysprep*

www.takbook.com

بعد از اینکه سیستم کلاینت مورد نظر Restart و اجرا شد باید به مانند شکل ۸–۲۱۰، بر روی Change کلیک کنید، اول از همه باید کلاینت را از حالت دومین به حالت WorkGroup ببریم که برای این کار باید یک نام وارد و بر روی OK کلیک کنید و بعد در شکل ۸–۲۱۰، رمز عبور دومین را وارد و سیستم را Restart کنید.

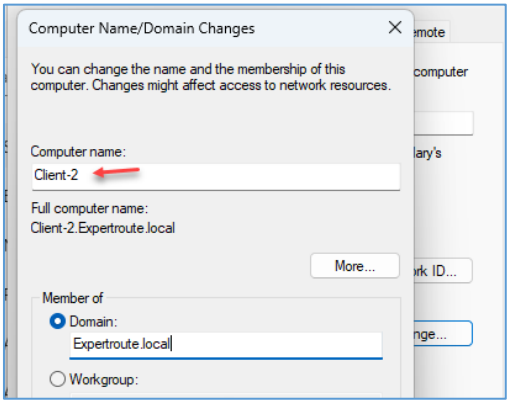


شکل ۸- ۲۱۰ تغییر حالت دومین



شکل ۸- ۲۱۱ تغییر حالت دومین

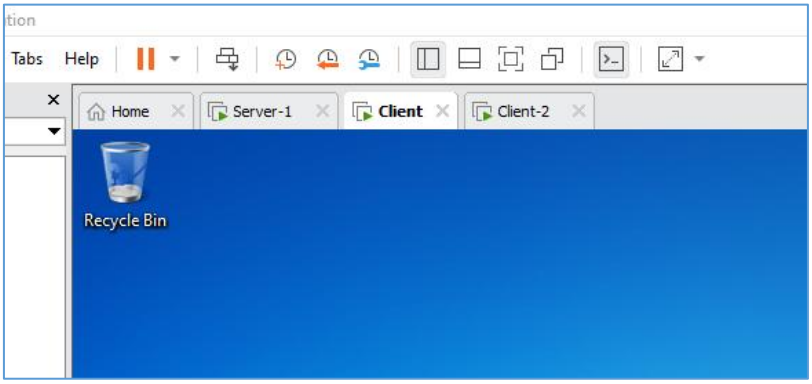
با کاربر Local وارد شوید و دوباره به مانند شکل ۸–۲۱۲، نام دومین را وارد و نام کلاینت را تغییر دهید.



شکل ۸- ۲۱۲ تغییر حالت دومین

www.takbook.com

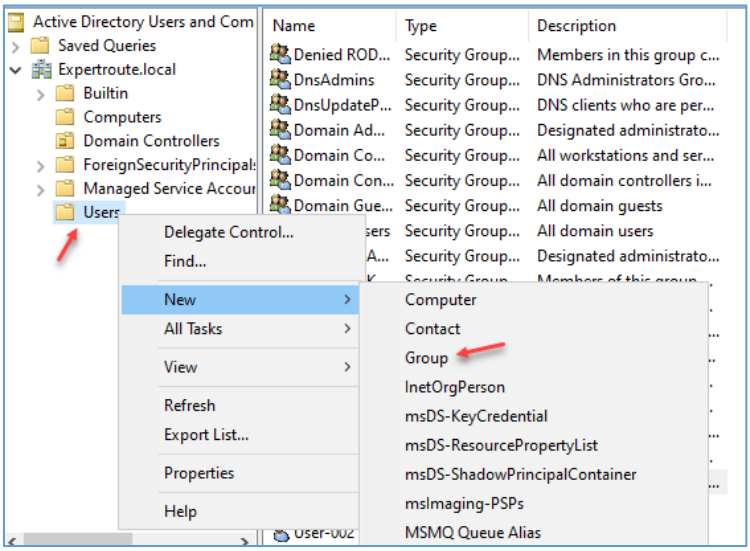
همان‌طور که در شکل ۸-۲۱۳، مشاهده می‌کنید دو ماشین Client و Client2 ایجاد شده است و هر دوی آنها عضو دومین شده‌اند و برای کار آماده هستند.



شکل ۸- ۲۱۳ ایجاد ماشین مجازی

۸-۳-۱۰-۵ ایجاد گروه در Active directory

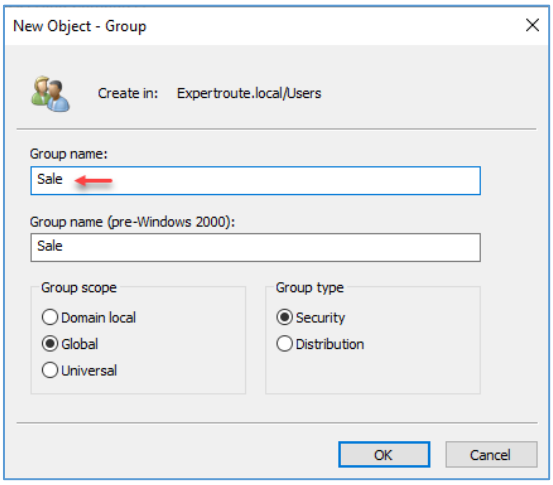
گروه‌ها در Active Directory، بیشترین نقش را ایفا می‌کنند و در بیشتر اوقات از آن‌ها برای مدیریت بهتر در کار استفاده می‌کنیم؛ برای ایجاد گروه، وارد سرویس Active Directory Users and Computers می‌شویم و از سمت چپ، به مانند شکل ۸-۲۱۴، بر روی Users کلیک راست می‌کنیم و از قسمت New، گزینه‌ی Group را انتخاب و یا از نوار ابزار بالایی بر روی آیکون مورد نظر کلیک می‌کنیم.



شکل ۸- ۲۱۴ ایجاد گروه در Active directory

www.takbook.com

در شکل ۸-۲۱۵، 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.



شکل ۸- ۲۱۵ ایجاد گروه در Active directory

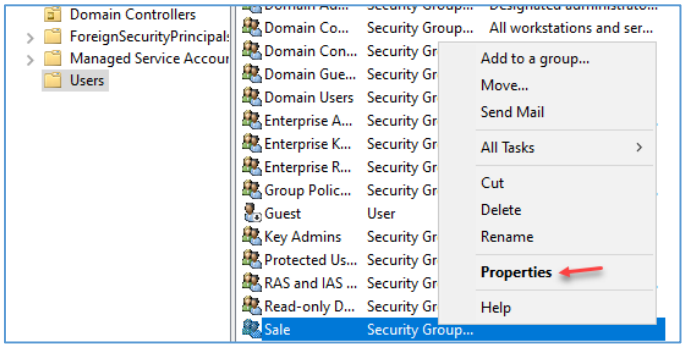
در قسمت Group Scope، سه گزینه وجود دارد؛ گزینه‌ی Domain Local که با انتخاب این گزینه، گروه مورد نظر توانایی عضوگیری کاربران از داخل دومین خود و دومین‌های Forest که به دومین اصلی، Trust می‌باشند را دارد، امّا گزینه‌ی Global که توانایی عضوگیری، تنها از دومین خود و زیرمجموعه‌ی خود را دارد، توانایی دسترسی از تمام Forestها 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.

درباره‌ی Trust کردن دومین‌ها، به صورت مفصّل در ادامه‌ی 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 گزینه‌ی 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 شروع کار، گزینه‌ی Global و Security را انتخاب و بر روی OK کلیک کنید.

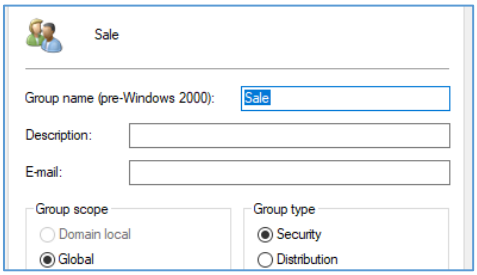
بعد از ایجاد گروه موردنظر، به مانند شکل ۸-۲۱۶، بر روی آن کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.

www.takbook.com



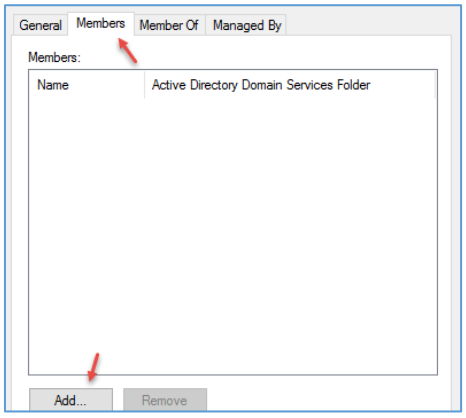
شکل ۸- ۲۱۶ ایجاد گروه در *Active directory*

در شکل ۸-۲۱۷، 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.



شکل ۸- ۲۱۷ایجاد گروه در *Active directory*

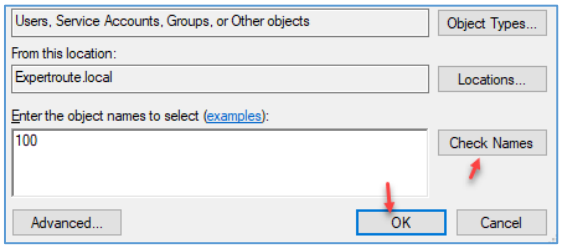
به مانند شکل ۸-۲۱۸، در تب Members، می‌توانید هر کاربری که عضو دومین باشد را زیر مجموعه‌ی این گروه قرار دهید؛ برای این کار، بر روی Add کلیک و کاربر مورد نظر را جستجو کنید.



شکل ۸- ۲۱۸ ایجاد گروه در *Active directory*

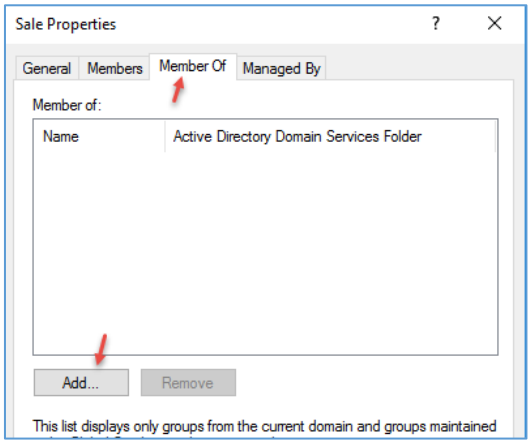
www.takbook.com

در شکل ۸-۲۱۹، نام کاربری را وارد و بر روی Check Names کلیک کنید، با این کار نام کاربر نمایش داده خواهد شد و بر روی OK کلیک کنید.



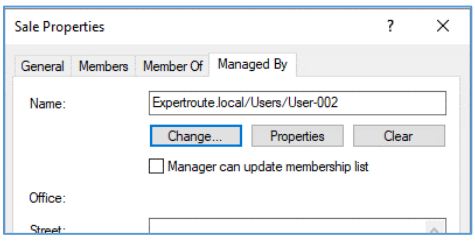
شکل ۸- ۲۱۹ ایجاد گروه در Active directory

در شکل ۸-۲۲۰، 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 به لیست اضافه کنید.



شکل ۸- ۲۲۰ ایجاد گروه در Active directory

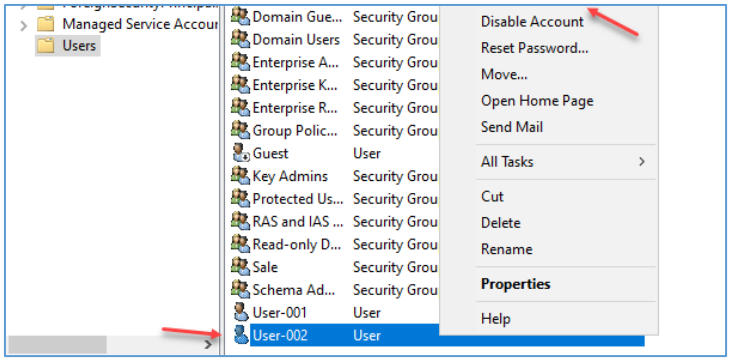
به مانند شکل ۸-۲۲۱، در تب Managed By، می‌توانید مشخّص کنید که چه کاربر و گروهی، رئیس گروه مورد نظر باشد، یعنی با انتخاب آن، تنها همان گروه یا کاربر موردنظر می‌تواند، کاربران دیگر را عضو این گروه کند.



شکل ۸- ۲۲۱ ایجاد گروه در Active directory

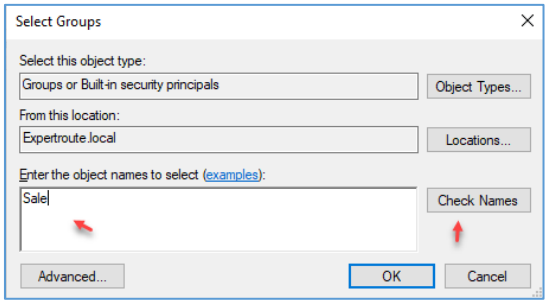
www.takbook.com

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 ۸-۲۲۲، عضو گروه مورد نظر کنید، بر روی کاربر مورد نظر کلیک راست کنید و گزینه‌ی Add to a Group را انتخاب کنید.



شکل ۸- ۲۲۲/ایجاد گروه در *Active directory*

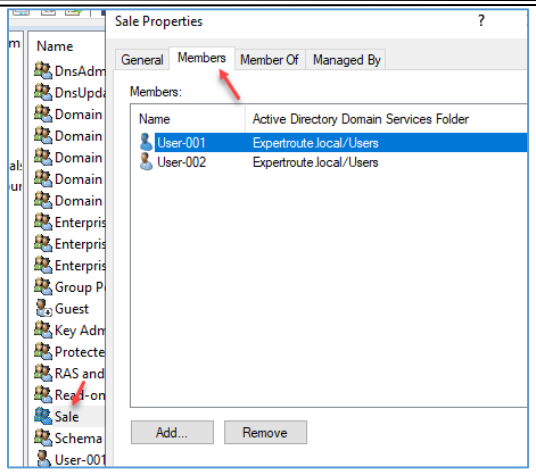
در شکل ۸-۲۲۳، در قسمت From this location دو گزینه وجود دارد، یکی نام دومین است و دیگری نام خود کلاینت، گزینه‌ی مورد نظر باید بر روی دومین قرار داشته باشد تا بتوانیم در داخل دومین جستجو انجام دهیم و اگر نام گروه یا چند کلمه‌ی اوّل گروه را می‌دانید در جای مشخّص شده وارد کنید و بر روی Check Names کلیک کنید.



شکل ۸- ۲۲۳/ایجاد گروه در *Active directory*

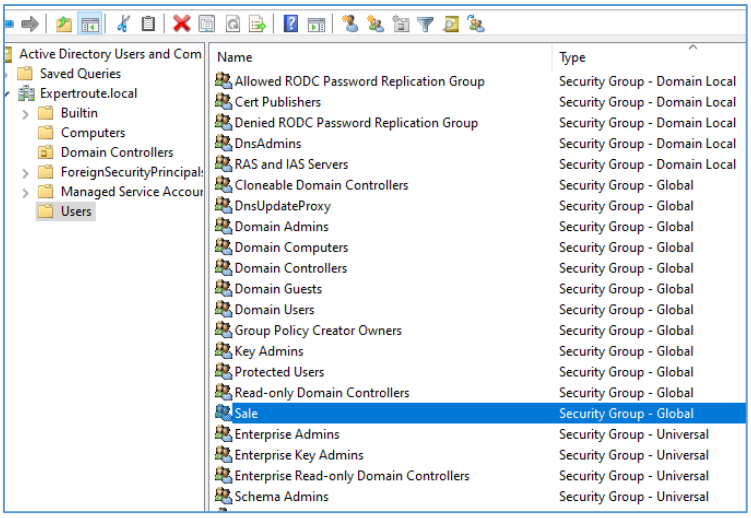
در شکل ۸-۲۲٤، در قسمت Members مربوط به گروه Sale، کاربر Aryan Rezaei به لیست اضافه شده است، اکنون شما می‌توانید این گروه را به فایل‌های به اشتراک‌گذاری شده دسترسی دهید.

www.takbook.com



شکل ۸- ۲۲۴/ایجاد گروه در *Active directory*

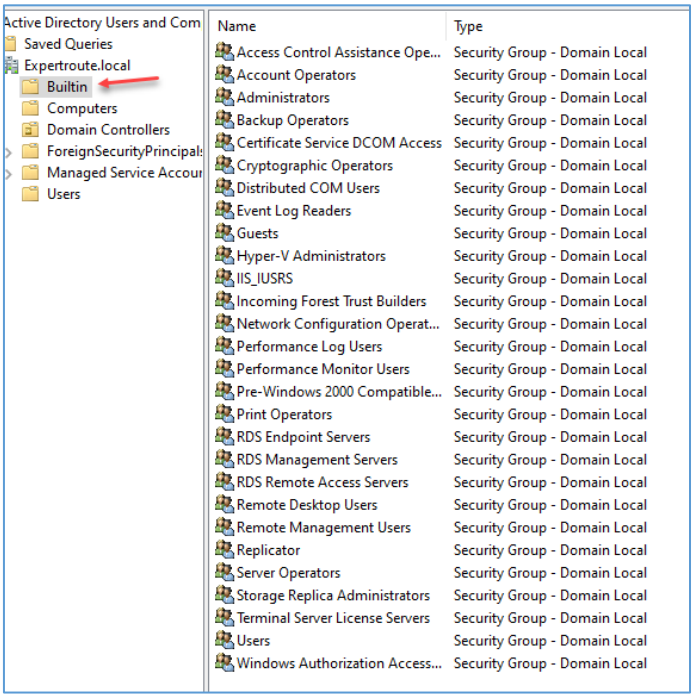
یک‌سری گروه‌ها در قسمت Users وجود دارند که این گروه‌ها با نصب و حذف سرویس‌ها، به صورت خودکار کم و زیاد می‌شوند، در شکل ۸-۲۲۵، تعدادی از این گروه‌ها را مشاهده می‌کنید.



شکل ۸- ۲۲۵/ایجاد گروه در *Active directory*

به مانند شکل ۸-۲۲۶، در قسمت Builtin نیز یک‌سری گروه تعریف شده است که دارای ویژگی خاصی هستند که بعضی از آنها را بررسی خواهیم کرد.

www.takbook.com



شکل ۸- ۲۲۶/ایجاد گروه در Active directory

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.

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.

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.

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.

Backup Operators

www.takbook.com

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.

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.

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.

Cryptographic Operators

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

Denied RODC Password Replication Group

اعضای این گروه نمی‌توانند رمز عبور RODC را تغییر دهند.

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.

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.

DnsAdmins

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

Domain Admins

www.takbook.com

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.

Domain Computers

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

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.

Domain Guests

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

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.

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.

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.

Hyper-V Administrators

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

Schema admin

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

www.takbook.com

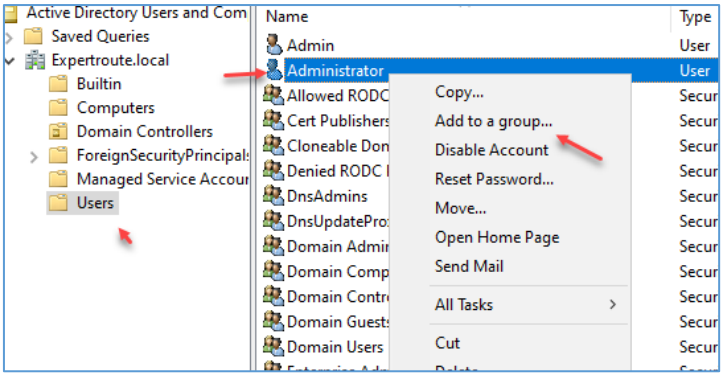
تا به اینجا، گروه‌های مهم در شبکه را بررسی کردیم که به صورت خواه، ناخواه با آنها کار خواهیم کرد، گروه‌های دیگری نیز هستند که در صورت امکان، نحوه‌ی عملکرد آنها را نیز بررسی خواهیم کرد.

عضویّت مدیران در گروه‌های اصلی

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

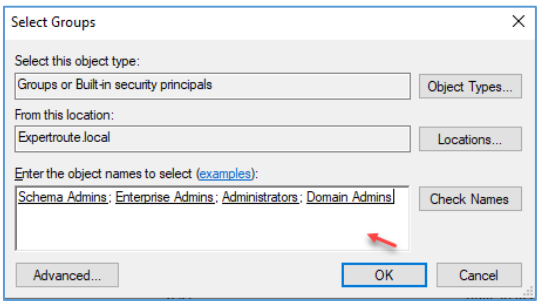
- Administrator
- Schema Admins
- Domain Admins
- Enterprise Admins

به مانند شکل ۸–۲۲۷، بر روی کاربری که می‌خواهید عضو گروه‌های بالا شوند کلیک راست کنید و گزینه‌ی Add to Group را انتخاب کنید.



شکل ۸- ۲۲۷ دسترسی ادمین در Active

در شکل ۸–۲۲۸، هر چهار گروه در لیست وارد شده‌اند و با کلیک بر روی OK کاربر مورد نظر عضو این گروه‌ها خواهد شد.



شکل ۸- ۲۲۸ دسترسی ادمین در Active

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

www.takbook.com

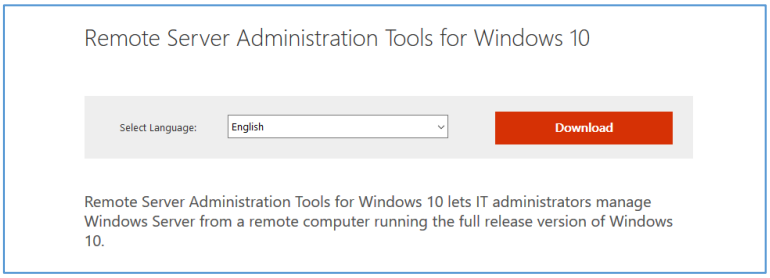
۶-۱۰-۳-۸ ارتباط از راه دور با سرویس Active Directory

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 سیستم خودش در دسترس باشد.

برای اینکه سرویس Active Directory را در یک ویندوز معمولی، مانند ویندوز ۷، ۸، ۸.۱ یا ۱۰ در دسترس باشد باید سرویس Administrative Tools را نصب کنید که باید برای هر ویندوز جدا دانلود کنید، که لینک آن را در زیر قرار دادیم:

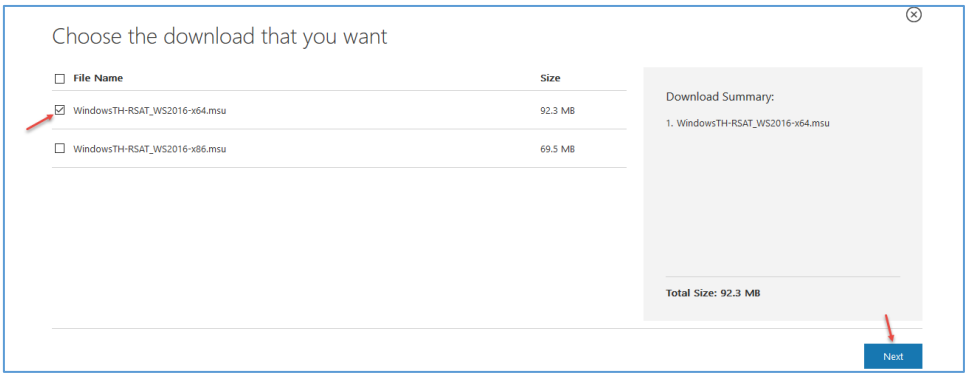
- ویندوز ۷
- ویندوز ۸
- ویندوز ۸.۱
- ویندوز ۱۰

مثلاً برای نصب در ویندوز ۱۰ فایل نصبی آن را طبق شکل ۸-۲۲۹، دانلود کنید:



شکل ۸- ۲۲۹ نصب ابزار RSAT

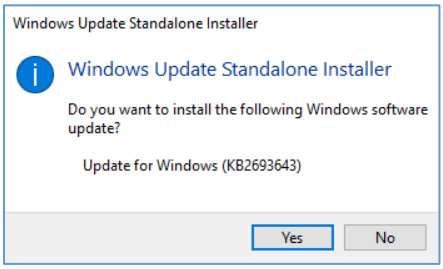
به مانند شکل ۸-۲۳۰، نوع ویندوز خود که ٦٤ یا ۳۲ بیتی است را انتخاب و بر روی Next کلیک کنید تا فایل دانلود شود.



شکل ۸- ۲۳۰ نصب ابزار RSAT

www.takbook.com

توجّه داشته باشید، سرویس Update باید قبل از اجرای فایل فعّال شده باشد، اگر فعّال نباشد با خطا مواجه خواهید شد، به مانند شکل ۸–۲۳۱، بر روی Yes کلیک کنید تا آپدیت مورد نظر بر روی کلاینت ویندوز ۱۰ اعمال شود.



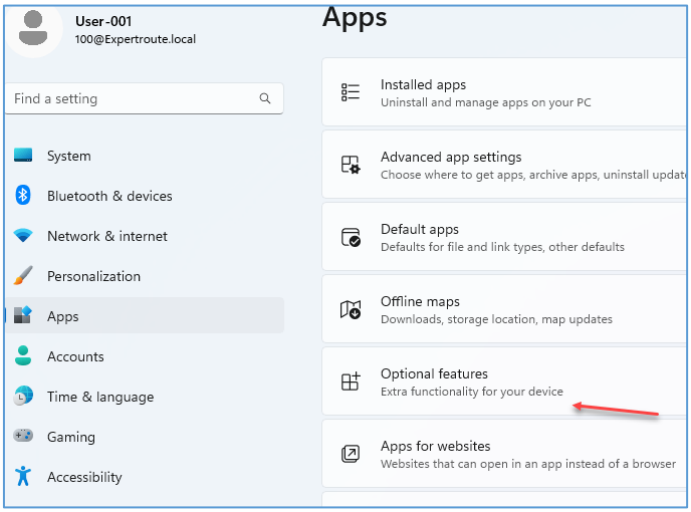
شکل ۸- ۲۳۱ نصب ابزار RSAT

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 اگر Active را جستجو کنید مشاهده خواهید کرد که سرویس‌های مورد نظر به لیست اضافه شده است.

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

برای ویندوز ۱۱ هم باید وارد Seeting شوید و از قسمت Apps باید گزینه Optional features را انتخاب کنید که این موضوع را در شکل ۸–۲۳۲، مشاهده می‌کنید.



شکل ۸- ۲۳۲ نصب ابزار RSAT

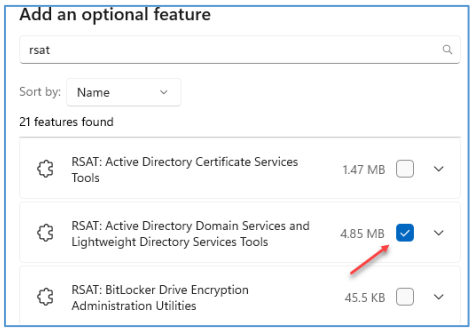
در شکل ۸–۲۳۳، بر روی View features کلیک کنید.

www.takbook.com



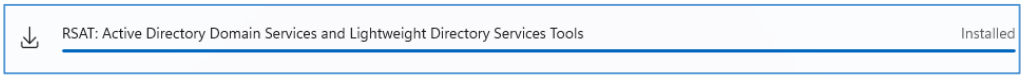
شکل ۸- ۲۳۳ نصب ابزار RSAT

با جستجوی کلمه‌ی rsat به مانند شکل ۸-۲۳٤، می‌توانید ابزار Active Directory را تیک بزنید و بر روی Install کلیک کنید تا این ابزار نصب شود، توجه داشته باشید که این ابزار برای نصب نیاز به اینترنت دارد.



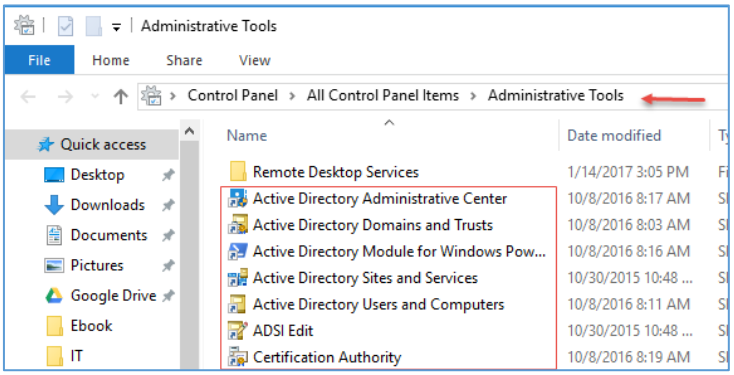
شکل ۸- ۲۳۴ نصب ابزار RSAT

همان‌طور که در شکل ۸-۲۳۵، مشاهده می‌کنید سرویس مورد نظر با موفقیت نصب شده است.



شکل ۸- ۲۳۵ نصب ابزار RSAT

همان‌طور که در شکل ۸-۲۳٦ مشاهده می‌کنید ابزارهای مربوط به Active Directory را در پوشه Administrative Tools مشاهده می‌کنید.



شکل ۸- ۲۳۶ نصب ابزار RSAT

www.takbook.com

۸-۳-۱۱ 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 مدیر شبکه باشد.

برای حل این مسائل، سرویسی با عنوان Dynamic Host Configuration Protocol یا به اختصار، DHCP ایجاد شده است تا کار مدیران شبکه را راحت کند، این سرویس با گرفتن رنج IP به تمام دستگاه‌های شبکه، یک IP مشخّص را در اختیار آنها قرار می‌دهد که این IP می‌تواند دارای مدّت انقضاء 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 (Subnet) 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 زیرشبکه (Subnet) است، کاربر DHCP نیز می‌تواند آخرین IP 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،

www.takbook.com

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.

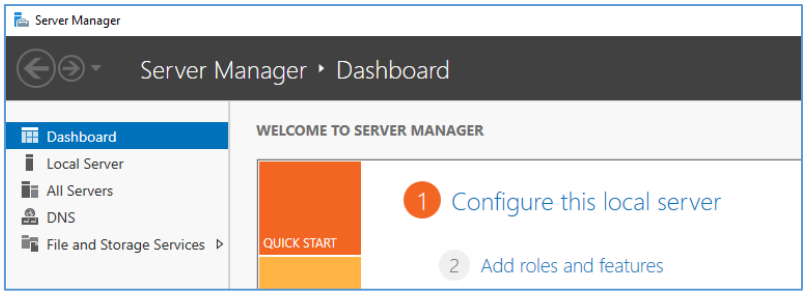
تصدیق Acknowledgement (DHCP)

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 کار شما خواهد بود یا نه.
۳. تعداد سرورهای خود را مشخّص کنید تا در صورت تمایل در لیست رزرو قرار داده شوند.

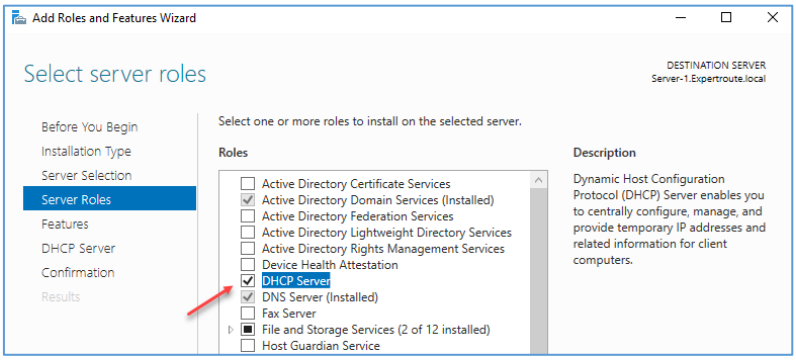
به مانند شکل ۸–۲۳۷، وارد Server Manager شوید و بر روی Add roles and feature کلیک کنید تا اقدام به نصب سرویس DHCP کنیم.



شکل ۸- ۲۳۷ سرویس DHCP

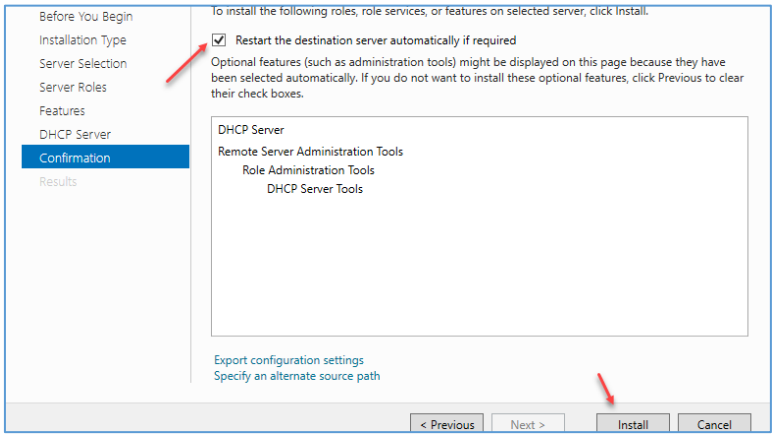
www.takbook.com

در شکل ۸–۲۳۸، 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.



شکل ۸- ۲۳۸ سرویس DHCP

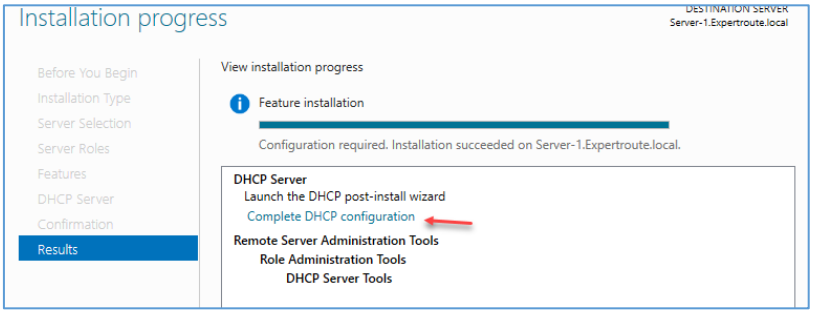
در شکل ۸–۲۳۹، بر روی Install کلیک کنید تا کار نصب سرویس DHCP آغاز شود.



شکل ۸- ۲۳۹ سرویس DHCP

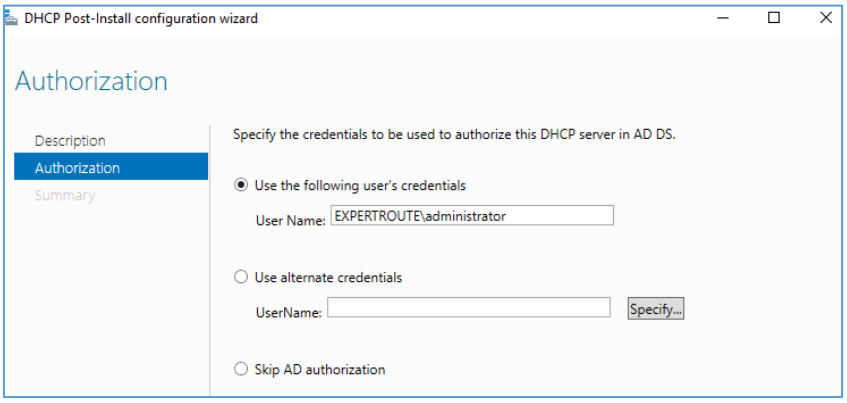
بعد از نصب سرویس DHCP، شکل ۸–۲۴۰، ظاهر می‌شود که باید بر روی Complete DHCP configuration کلیک کنید.

www.takbook.com



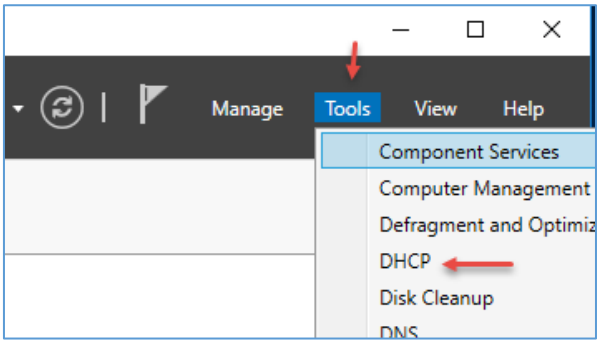
شکل ۸- ۲۴۰ سرویس *DHCP*

در شکل ۸-۲۴۱، برای کامل شدن مراحل نصب DHCP بر روی Commit کلیک کنید، بعد از این کار، دو گروهDHCP Administrators و DHCP Users ایجاد می‌شود و کار نصب سرویس DHCP به اتمام می‌رسد. و در آخر کار، سرور را Restart کنید.



شکل ۸- ۲۴۱ سرویس *DHCP*

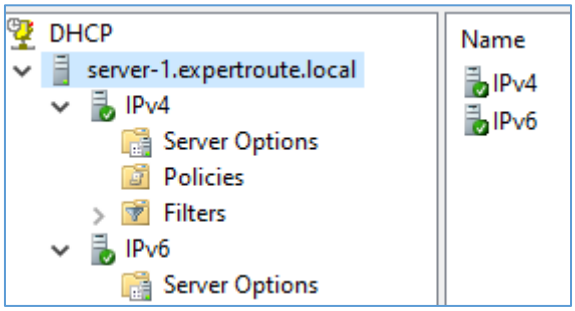
بعد از اجرا شدن سرور به مانند شکل ۸-۲۴۲، وارد Server Manager شوید و از منوی Tools، سرویس DHCP را اجرا کنید، از طریق منوی Start نیز می‌توانید با جستجوی DHCP، آن را اجرا کنید.



شکل ۸- ۲۴۲ سرویس *DHCP*

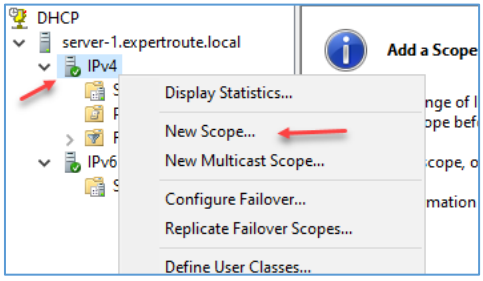
www.takbook.com

همان‌طور که در شکل ۸-۲۴۳، 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 ما در این سرویس با ورژن IPv4 است که شامل گزینه‌های مختلف است.



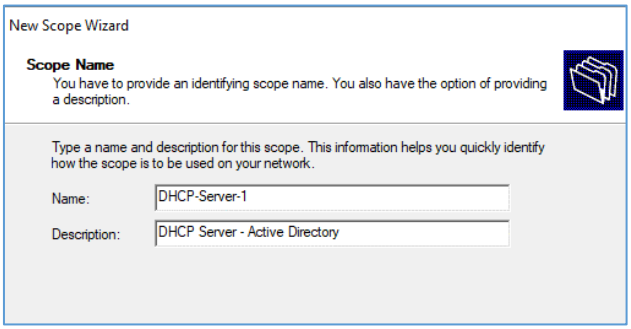
شکل ۸- ۲۴۳ سرویس DHCP

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 به مانند شکل ۸-۲۴۴، بر روی ورژن IPv4 کلیک راست کنید و گزینه‌ی Scope را انتخاب کنید.



شکل ۸- ۲۴۴ سرویس DHCP

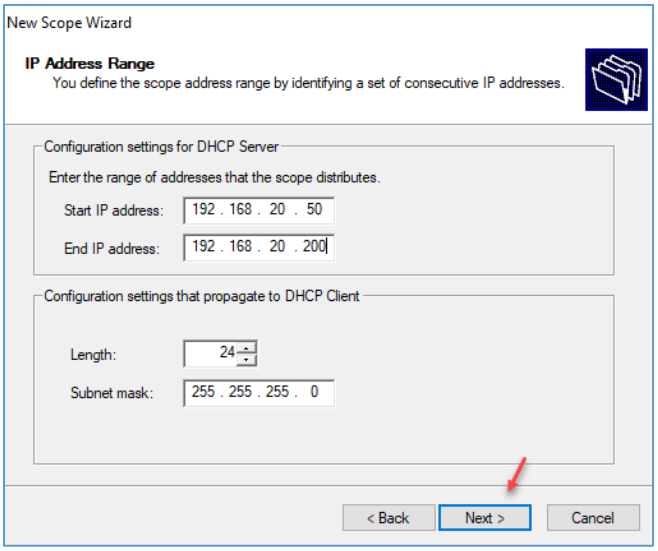
در شکل ۸-۲۴۵، نام و توضیحات مربوط به Scope خود را وارد و بر روی Next کلیک کنید.



شکل ۸- ۲۴۵ سرویس DHCP

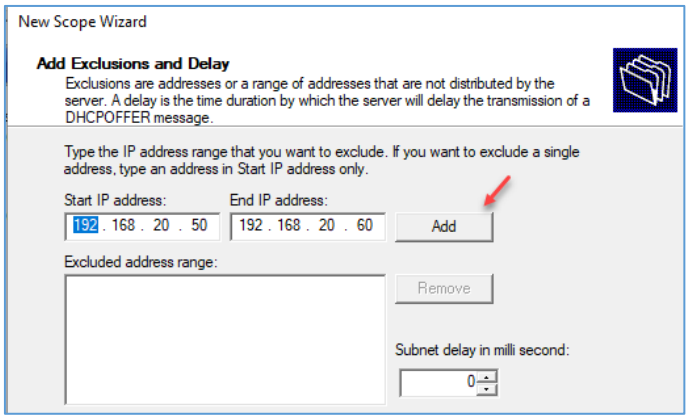
www.takbook.com

در شکل ۸-۲۴۶، 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 ۲۵۴ است، بهتر است به جای ۲۴ در قسمت Length، عدد پایین‌تر را در نظر بگیرید تا رنج شبکه‌ی شما افزایش پیدا کند؛ به مانند شکل ۸-۲۴۶، اطّلاعات را وارد و بر روی Next کلیک کنید.



شکل ۸- ۲۴۶ سرویس DHCP

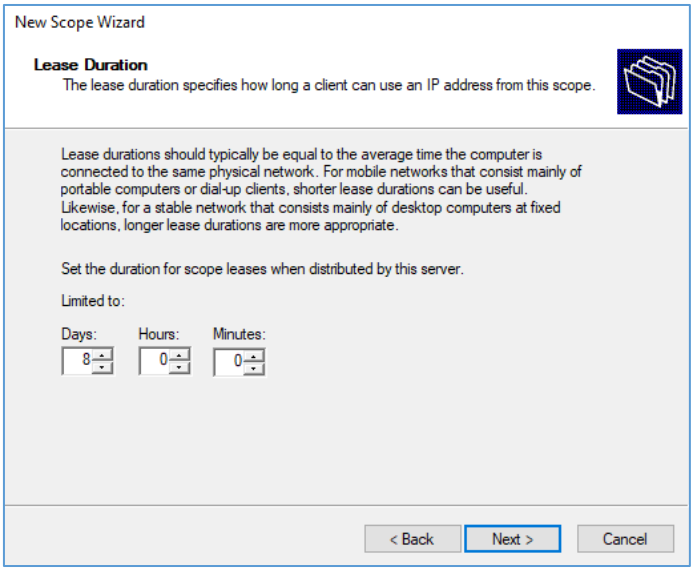
در شکل ۸-۲۴۷، می‌توانید یک رنج مشخّص از داخل رنج قبلی برای تخصیص دادن به سرورها و سیستم‌های خاص و مهمّ خود انتخاب کنید، با این کار اگر یک کلاینت معمولی، درخواست IP دهد، آدرسی که به آن تعلّق خواهد گرفت از 192.168.20.61 به بعد خواهد بود و در این رنج آدرس داده نخواهد شد. این نکته را با مثال ذکر خواهیم کرد.



شکل ۸- ۲۴۷ سرویس DHCP

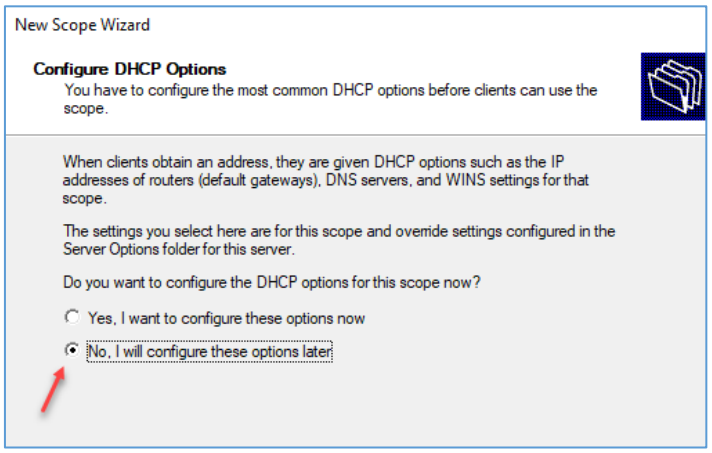
www.takbook.com

در شکل ۸-۲٤۸، 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 ۸-۲٤۸، ۸ روز در نظر گرفته شده که شما می‌توانید این زمان را تغییر دهید، اگر در این ۸ روز، دستگاه مورد نظر، خود را به سرویس DHCP معرّفی نکند، آدرس تخصیص داده شده از آن پس گرفته خواهد شد.



شکل ۸- ۲۴۸ سرویس DHCP

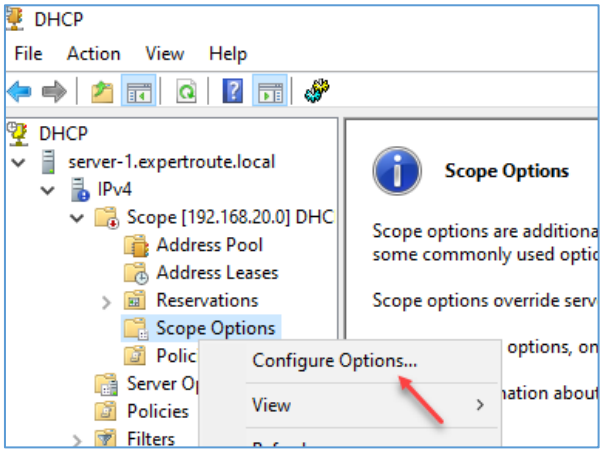
در شکل ۸-۲٤۹، شما می‌توانید با انتخاب گزینه‌ی اوّل، تنظیماتی، مانند آدرس روتر، نام دومین و آدرس Wins Server را انجام دهید که فعلاً این کار را انجام نمی‌دهیم و در ادامه انجام خواهیم داد؛ گزینه‌ی No را انتخاب و بر روی Next کلیک کنید، در صفحه‌ی بعد نیز بر روی Finish کلیک کنید.



شکل ۸- ۲۴۹ سرویس DHCP

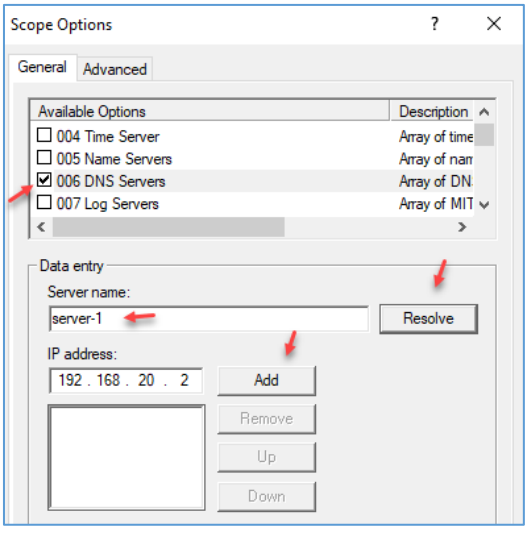
www.takbook.com

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 ۸-۲۵۰، وارد Scope مورد نظر شوید و بر روی Scope Options کلیک راست و گزینه‌ی Configurations Options را انتخاب کنید.



شکل ۸- ۲۵۰ سرویس DHCP

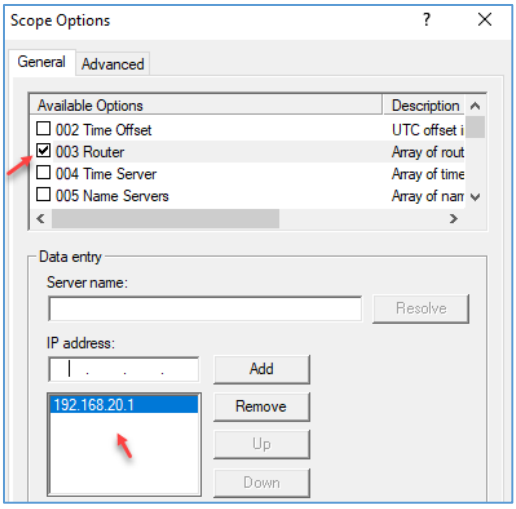
در شکل ۸-۲۵۱، باید از لیست، گزینه‌ی مورد نظر خود را انتخاب کنید، مثلاً برای اضافه کردن DNS سرور به Scope باید از لیست مورد نظر، تیک گزینه‌ی DNS Server را انتخاب کنید و در قسمت Server Name می‌توانید نام سروری که DNS بر روی آن اجرا شده است را وارد کنید که این کار را در سرور AD انجام دادیم، با وارد کردن نام سرور و کلیک بر روی Resolve، آدرس IP مشخّص می‌شود و با کلیک بر روی Add، آدرس سرور را به لیست اضافه کنید.



شکل ۸- ۲۵۱ سرویس DHCP

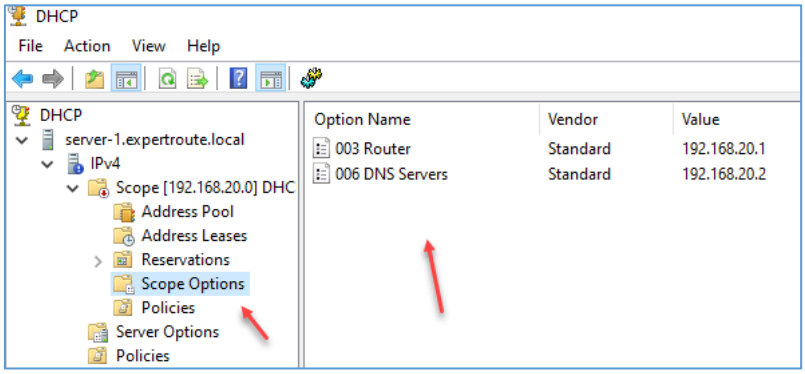
www.takbook.com

گزینه‌ی دیگر، Router است که اگر در شبکه‌ی خود از روتر (اینترنت) استفاده می‌کنید، می‌توانید آدرس آن را به مانند شکل ۸-۲۵۲، به لیست اضافه کنید، آدرس روتر در این کتاب، 192.168.20.1 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.



شکل ۸- ۲۵۲ سرویس *DHCP*

همان‌طور که در شکل ۸-۲۵۳، 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.

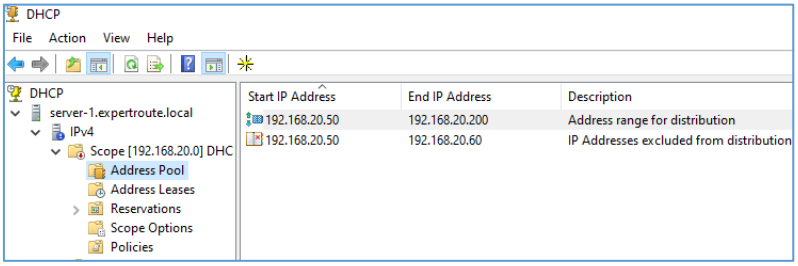


شکل ۸- ۲۵۳ سرویس *DHCP*

به مانند شکل ۸-۲۵٤، در قسمت Address Pool، رنج آدرس آن مشخّص شده است که از 192.168.20.50 تا 192.168.20.200 است و یک رنج Excluded مشخّص شده است، همان‌طور که گفتیم رنجی که به عنوان

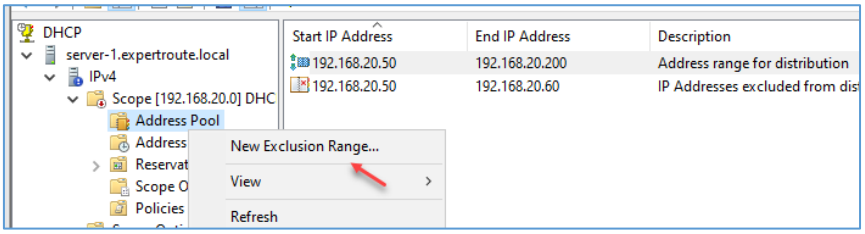
www.takbook.com

Excluded انتخاب می‌کنید به کلاینت‌ها داده نخواهد شد و از این رنج می‌توانید به سرورهای خاص خود اختصاص دهید.



شکل ۸- ۲۵۴ سرویس DHCP

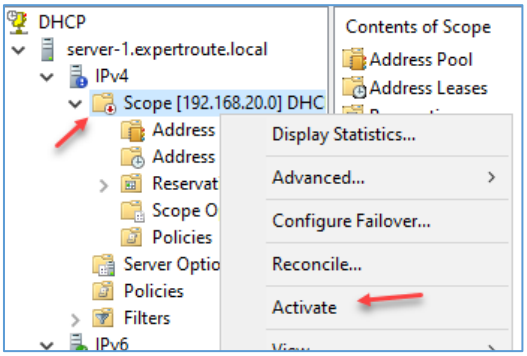
اگر چنانچه رنج Excluded را ایجاد نکردید می‌توانید به مانند شکل ۸–۲۵۵، با کلیک راست بر روی Address Pool گزینه‌ی مورد نظر را انتخاب و رنج را مشخص کنید تا به لیست اضافه شود.



شکل ۸- ۲۵۵ سرویس DHCP

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 ۸–۲۵۶، بر روی آن کلیک راست کنید و گزینه‌ی Activate را انتخاب کنید تا سرویس DNS به صورت کامل اجرا شود.

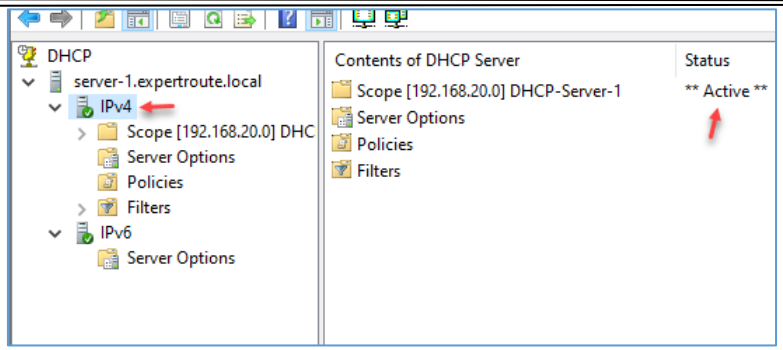
بعد از فعّال کردن سرویس، یک کلاینت را برای تست، اجرا و به شبکه‌ی خود متّصل کنید.



شکل ۸- ۲۵۶ سرویس DHCP

همان‌طور که در شکل ۸–۲۵۷، مشاهده می‌کنید، Scope مورد نظر فعّال شده است.

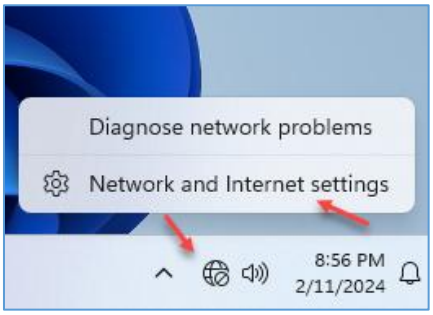
www.takbook.com



شکل ۸- ۲۵۷ سرویس DHCP

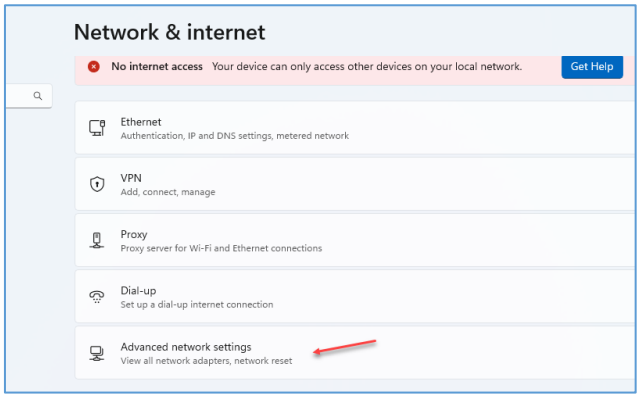
برای تست کارایی سرویس DHCP، یک کلاینت با ویندوز ۱۱ را به سرور متّصل کنید تا ببینید چه آدرسی را از سرویس DHCP دریافت می‌کند.

بعد از اینکه کلاینت را به شبکه‌ی ویندوز سرور متّصل کردید، به مانند شکل ۸–۲۵۸، وارد ویندوز ۱۱ شوید و بر روی کارت شبکه کلیک راست کنید و گزینه‌ی Network and internet Settings را انتخاب کنید.



شکل ۸- ۲۵۸ سرویس DHCP

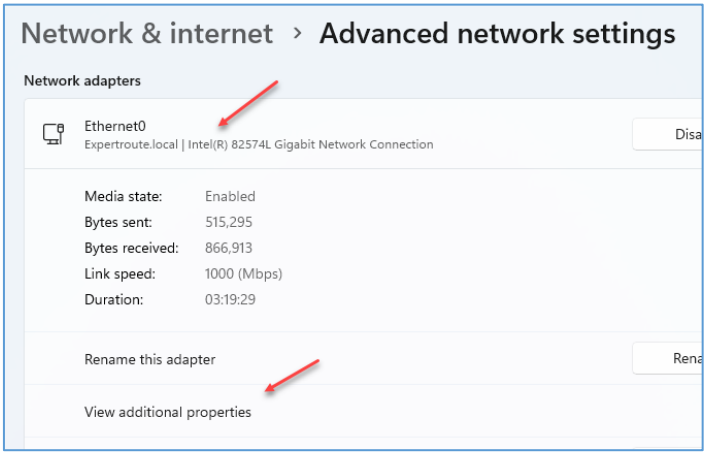
در شکل ۸–۲۵۹، گزینه‌ی Advanced network settings انتخاب کنید.



شکل ۸- ۲۵۹ سرویس DHCP

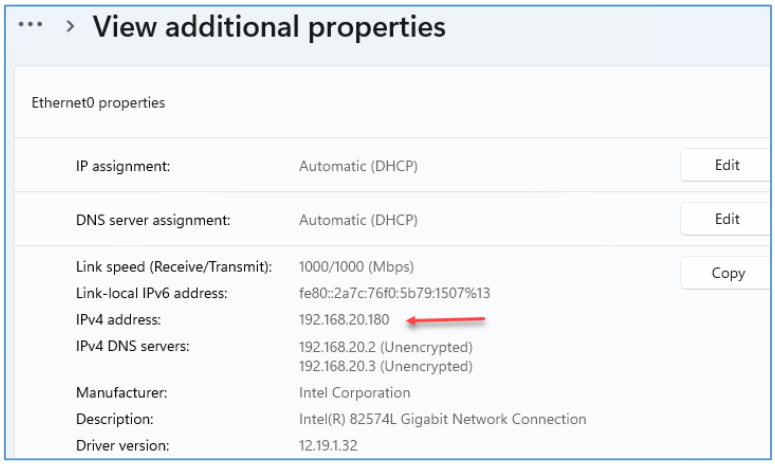
www.takbook.com

در ادامه کار به مانند شکل ۸-۲۶۰، با کلیک بر روی کارت شبکه مورد نظر گزینه‌ی View additional properties را انتخاب کنید.



شکل ۸- ۲۶۰ سرویس DHCP

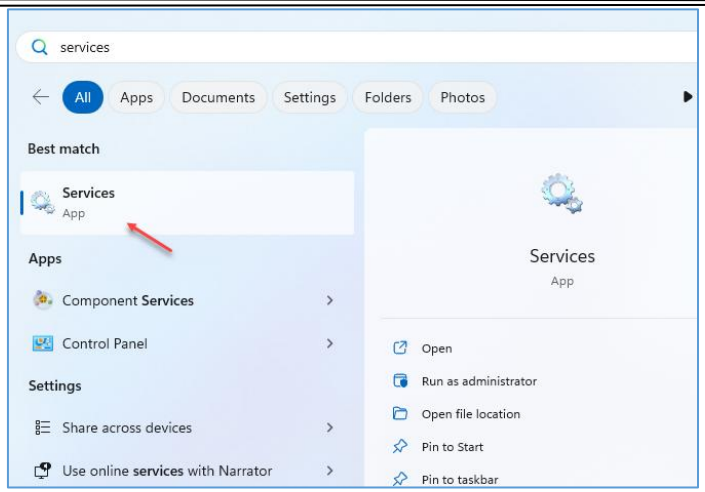
در شکل ۸-۲۶۰، اطّلاعات کارت شبکه نمایش داده شده است، همان‌طور که مشاهده می‌کنید بر روی DHCPقرار داریم، یعنی اگر در شبکه سرویس DHCP باشد، درخواست IP را به آن می‌فرستد و یک آدرس جدید دریافت می‌کند، اگر به آدرس IP توجّه کنید، 192.168.20.180 است، یعنی همان رنجی که در سرویس DHCP ایجاد کردیم، بقیّه‌ی گزینه‌ها را نیز مشاهده می‌کنید، آدرس DNS نیز مشخّص شده است.



شکل ۸- ۲۶۱ سرویس DHCP

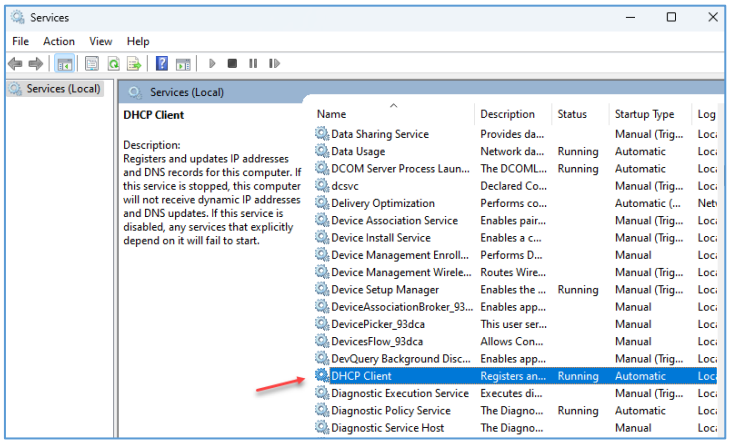
برای اینکه یک کلاینت بتواند از سرویس DHCP، آدرس جدید به صورت اتوماتیک دریافت کند باید سرویس آن فعّال باشد، برای بررسی این موضوع به مانند شکل ۸-۲۶۲، در کلاینت وارد Start شوید و Service را اجرا کنید.

www.takbook.com



شکل ۸- ۲۶۲ سرویس DHCP

همان‌طور که در شکل ۸-۲۶۳، 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.

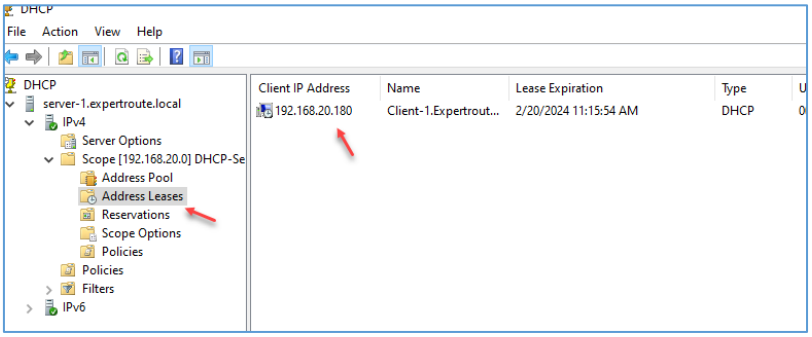


شکل ۸- ۲۶۳ سرویس DHCP

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 قبلاً بررسی کردیم.

اگر به مانند شکل ۸-۲۶۴، 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.

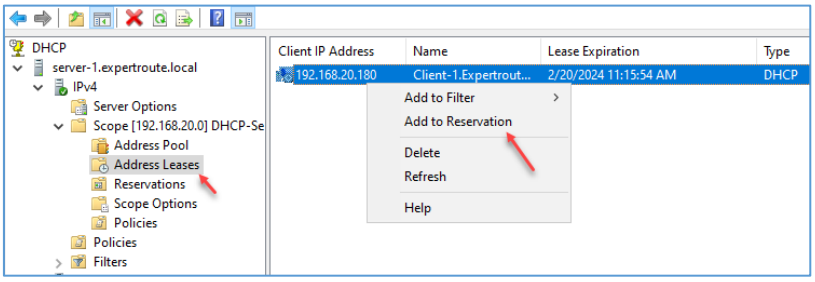
www.takbook.com



شکل ۸- ۲۶۴ سرویس DHCP

۸-۳-۱۱-۱ انجام Reservation در DHCP

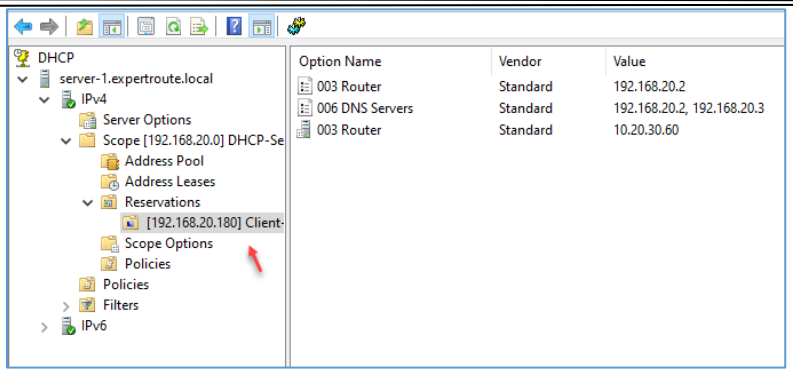
اگر بخواهید یک آدرس را برای همیشه به یک دستگاه تخصیص دهید باید به مانند شکل ۸-۲۶۵، در Address Leases بر روی آدرس مربوط به دستگاه مورد نظر کلیک راست کنید و گزینه‌ی Add to reservation را انتخاب کنید، با این کار این آدرس وارد لیست Reservation خواهد شد و دیگر آدرس آن تغییر نخواهد کرد.



شکل ۸- ۲۶۵ انجام Reservation در DHCP

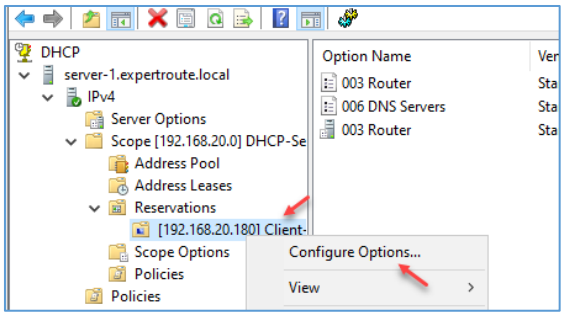
همان‌طور که در شکل ۸-۲۶۶، مشاهده می‌کنید در قسمت Reservations، آدرس دستگاه مورد نظر به لیست اضافه شده است، در این لیست شما می‌توانید تنظیمات جدیدتری را انجام دهید، یعنی اینکه می‌توانید در صورت نیاز، آدرس Router یا DNS و یا هر تنظیم خاصّ دیگری را فقط و فقط برای همین دستگاه انجام دهید.

www.takbook.com



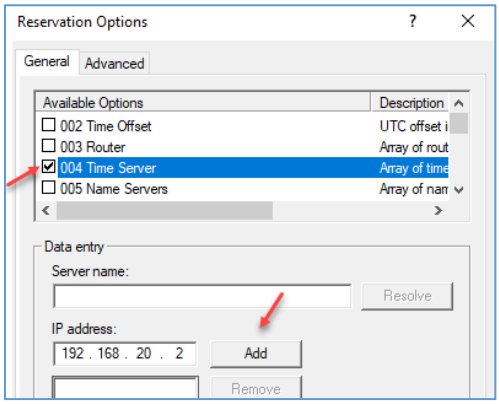
شکل ۸- ۲۶۶ انجام Reservation در DHCP

به طور مثال، اگر بخواهید آدرس Router را برای این دستگاه تغییر دهید باید به مانند شکل ۸-۲۶۷، بر روی آن کلیک راست و گزینه‌ی Configure Options را انتخاب کنید.



شکل ۸- ۲۶۷ انجام Reservation در DHCP

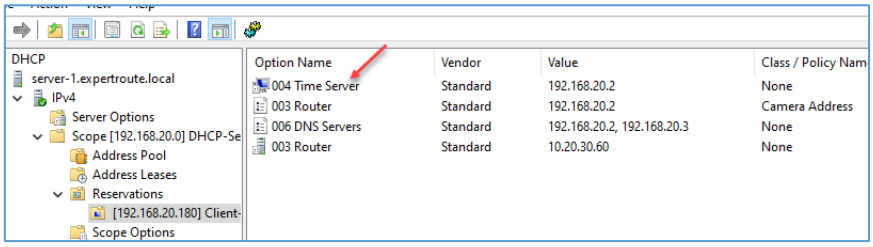
طبق شکل ۸-۲۶۸، در لیست زیر باید گزینه‌ی Time Server که برای زمان است را انتخاب و آدرس آن را در قسمت مورد نظر وارد و بر روی Add کلیک کنید؛ گزینه‌های دیگری را نیز می‌توانید برای این دستگاه تغییر دهید.



شکل ۸- ۲۶۸ انجام Reservation در DHCP

www.takbook.com

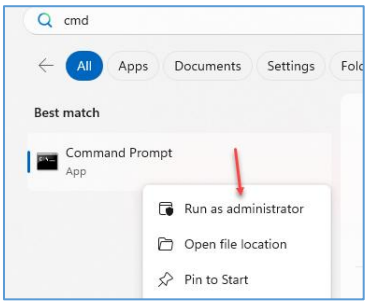
بعد از کلیک بر روی OK در شکل ۸-۲۶۹، این تغییر را مشاهده می‌کنید، برای اینکه کلاینت مورد نظر این تغییرات را دریافت کند می‌توانید از دستور Ipconfig /Renew استفاده کنید تا تنظیمات جدید دریافت شود، البته می‌توانید اول از دستور ipconfig /release و بعد از دستور Renew استفاده کنید.



شکل ۸- ۲۶۹ انجام Reservation در DHCP

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.

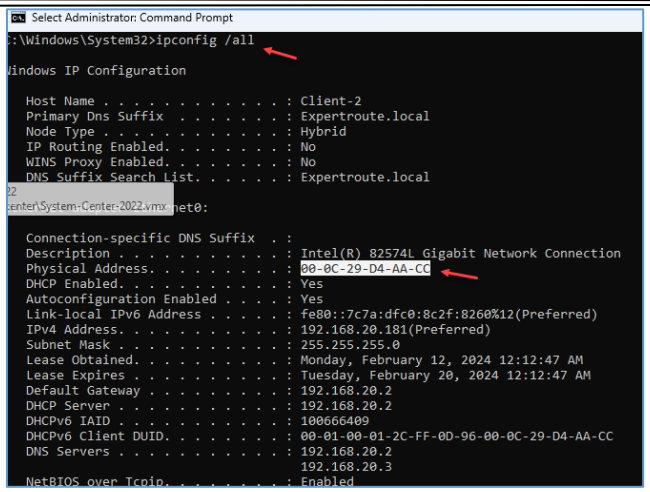
برای شروع کار کلاینت دوم خود را روشن می‌کنیم، و CMD را با دسترسی Admnistrator به مانند شکل ۸-۲۷۰، اجرا می‌کنیم.



شکل ۸- ۲۷۰ انجام Reservation در DHCP

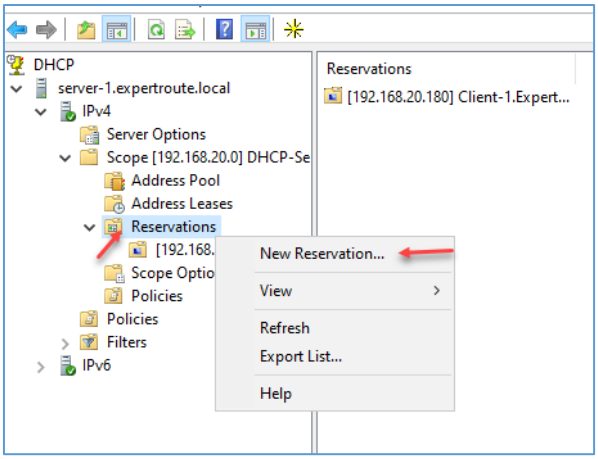
همان‌طور که در شکل ۸-۲۷۱، مشاهده می‌کنید، با دستور ipconfig /all تمام اطلاعات شبکه‌ی مربوط به کلاینت نمایش داده شده که آدرس MAC آن را مشخص کردیم، آدرس آن را کپی کنید.

www.takbook.com



شکل ۸- ۲۷۱ انجام Reservation در DHCP

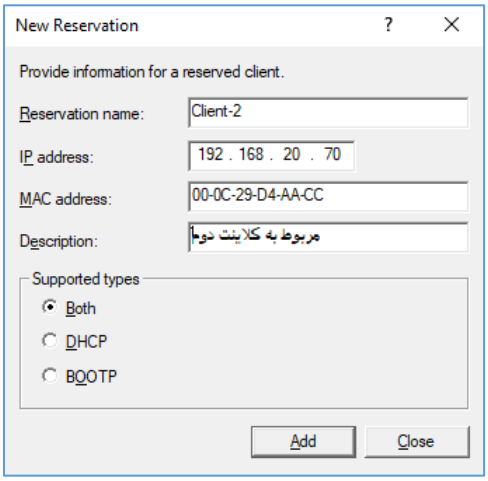
بعد از اینکه آدرس MAC را کپی کردید به مانند شکل ۸-۲۷۲، وارد سرویس DHCP شوید و برای انجام این کار بر روی Reservation کلیک راست و گزینه‌ی New Reservation را انتخاب کنید.



شکل ۸- ۲۷۲ انجام Reservation در DHCP

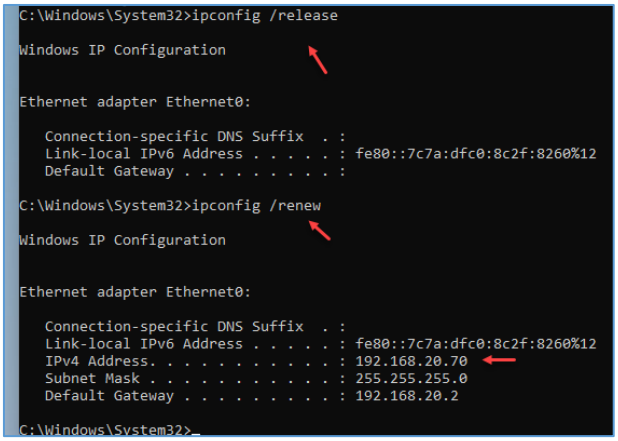
در شکل ۸-۲۷۳، باید اطّلاعات مورد نظر را وارد کنید؛ آدرس مورد نظر خود را در قسمت Ip address وارد کنید و در قسمت MAC address نیز آدرس Mac را وارد کنید که برای به دست آوردن آدرس Mac می‌توانید از دستور ipconfig /all در کلاینت مورد نظر استفاده کنید که این دستور را قبلاً بررسی کردیم. در قسمت Supported types، 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.

www.takbook.com



شکل ۸- ۲۷۳ انجام Reservation در DHCP

بعد از اینکه عملیّات Reservation را انجام دادید وارد کلاینت قبلی شوید و برای اینکه کلاینت آدرس جدید را از سرور DHCP دریافت کند، به مانند شکل ۸-۲۷٤، CMD را اجرا کنید و بعد از آن، دستور Ipconfig /Release را اجرا کنید؛ با این دستور، کلاینت آدرس قبلی خود را که 192.168.20.181 بود را از دست خواهد داد، برای دریافت آدرس جدید باید از دستور ipconfig /renew استفاده کنید که همان‌طور که در شکل ۸-۲۷٤، مشاهده می‌کنید، آدرس جدید که به صورت رزرو شده وارد کردید به کلاینت تخصیص داده شد.



شکل ۸- ۲۷۴ انجام Reservation در DHCP

۸-۳-۱۱-۲ فعّال کردن Mac Filtering در سرویس DHCP

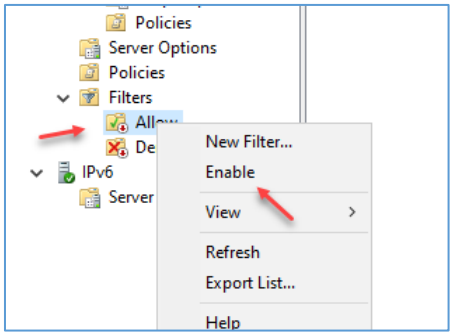
برای افزایش امنیّت شبکه‌ی خود می‌توانید از ویژگی MAC Filtering در شبکه‌ی خود استفاده کنید، با استفاده از این روش، شما می‌توانید لیستی از MAC آدرس‌های کلاینت‌ها و دستگاه‌های شبکه‌ی خود را جمع‌آوری و به سرویس DHCP اعلام کنید که تنها این سیستم‌ها اجازه دارند از شبکه، آدرس IP دریافت

www.takbook.com

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.

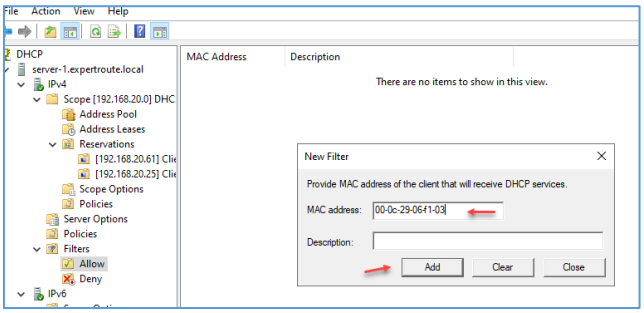
به مانند شکل ۸–۲۷۵، وارد قسمت Filter شوید؛ در این قسمت، دو گزینه‌ی Allow و Deny را مشاهده می‌کنید که به صورت پیش‌فرض غیر فعّال هستند و برای فعّال کردن این ویژگی باید بر روی هر دوی آنها کلیک راست کنید و گزینه‌ی Enable را انتخاب کنید.

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.



شکل ۸- ۲۷۵ *Mac Filtering*

با کلیک راست بر روی Allow و انتخاب گزینه‌ی New Filter، پنجره‌ی مربوط به آن در طبق شکل ۸–۲۷۶، 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.



شکل ۸- ۲۷۶ *Mac Filtering*

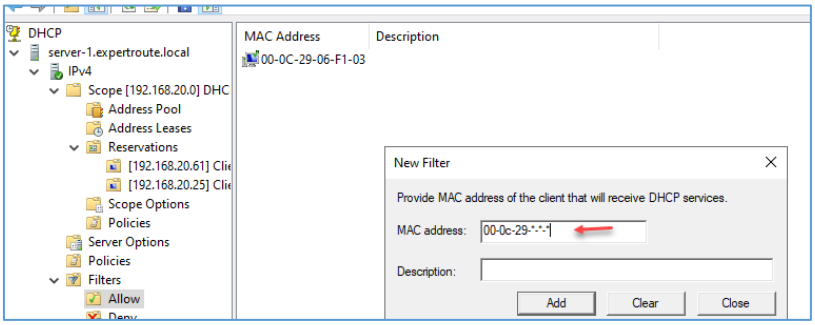
روش‌های دیگری نیز برای دادن آدرس وجود دارد، شاید شما کارت شبکه‌ی تمام سیستم‌های داخل سازمان خود را از یک شرکت خاص خریداری کرده باشید و اگر اینطور باشد، شما می‌توانید آدرس MAC را به مانند شکل ۸–۲۷۷، به صورت کلّی در این قسمت وارد کنید.

www.takbook.com

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 زیر چند آدرس اوّل را وارد و بقیّه را با علامت ستاره (*) پر کنید:

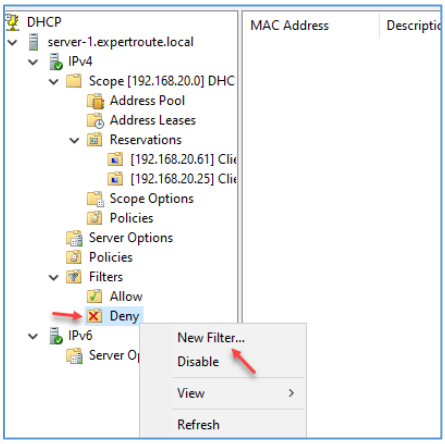
00-0c-29-*-*-*

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



شکل ۸- ۲۷۷ *Mac Filtering*

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 ۸-۲۷۸، 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.

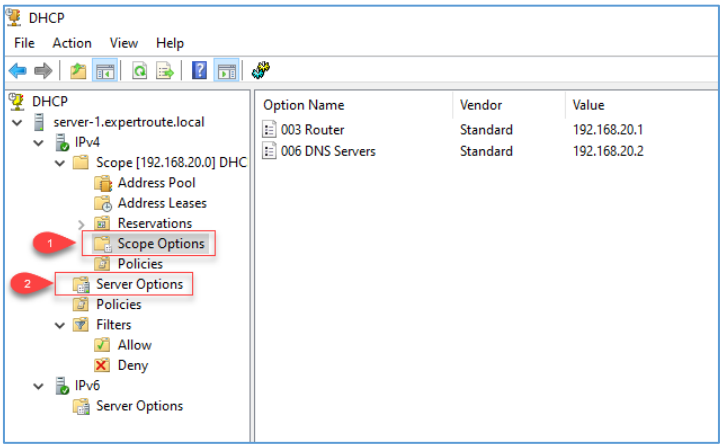


شکل ۸- ۲۷۸ *Mac Filtering*

اگر به مانند شکل ۸-۲۷۹، 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.

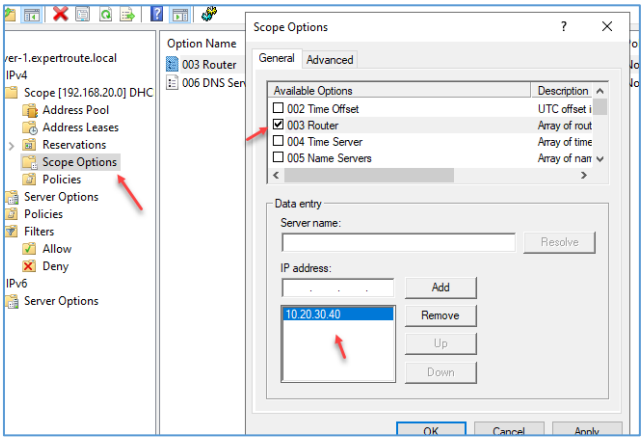
www.takbook.com

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



شکل ۸- ۲۷۹ *Mac Filtering*

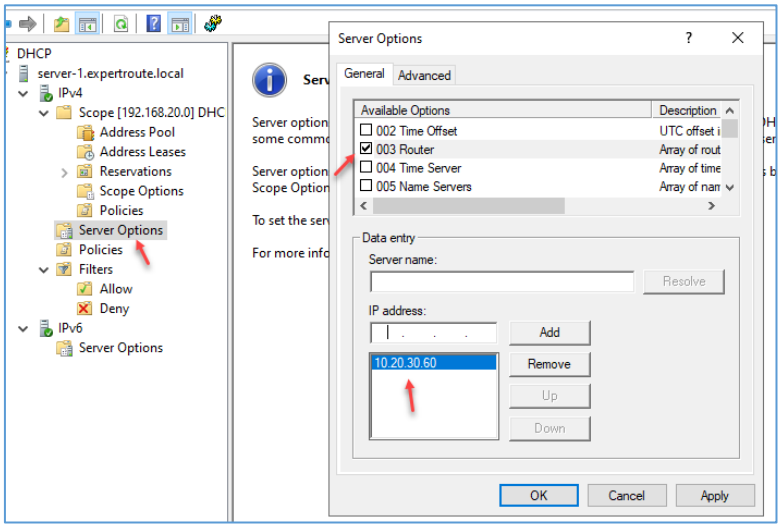
برای تست این موضوع به مانند شکل ۸-۲۸۰، در Scope Option، یک Router با آدرس 10.20.30.40 به لیست اضافه کنید.



شکل ۸- ۲۸۰ *Mac Filtering*

به مانند شکل ۸-۲۸۱، 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 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.

www.takbook.com



شکل ۸- ۲۸۱ *Mac Filtering*

به مانند شکل ۸-۲۸۲، 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.

```
C:\Users\100>ipconfig /release

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2a7c:76f0:5b79:1507%12
   Default Gateway . . . . . :

C:\Users\100>ipconfig /renew

Windows IP Configuration

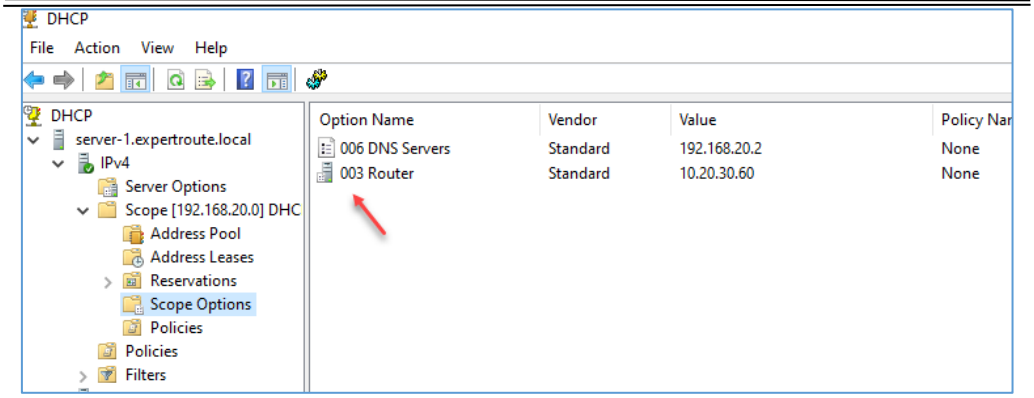

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2a7c:76f0:5b79:1507%12
   IPv4 Address. . . . . . . . . . . : 192.168.20.25
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.20.30.40
```

شکل ۸- ۲۸۲ *Mac Filtering*

اگر تنظیمات Server Options را فعّال کنید و چیزی در Scope Options وارد نکنید، به مانند شکل ۸-۲۸۳، از تنظیمات Server در scope استفاده می‌کند، از طریق شکل آیکون نیز می‌توانید به این تنظیمات پی ببرید.

www.takbook.com



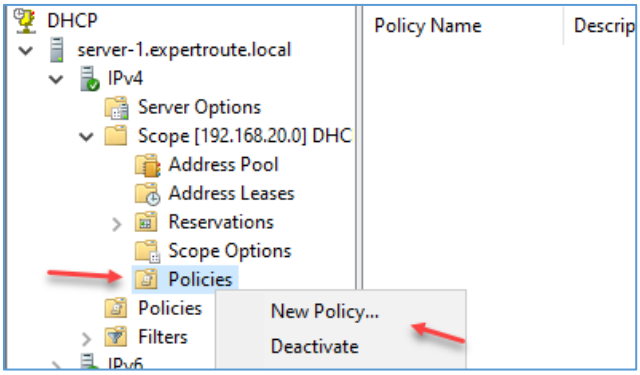
شکل ۸- ۲۸۳ *Mac Filtering*

۸-۳-۱۱-۳ تخصیص دادن آدرس مشخّص به دستگاه‌های مشخّص

برای اینکه در شبکه نظم را حفظ کنیم، 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.

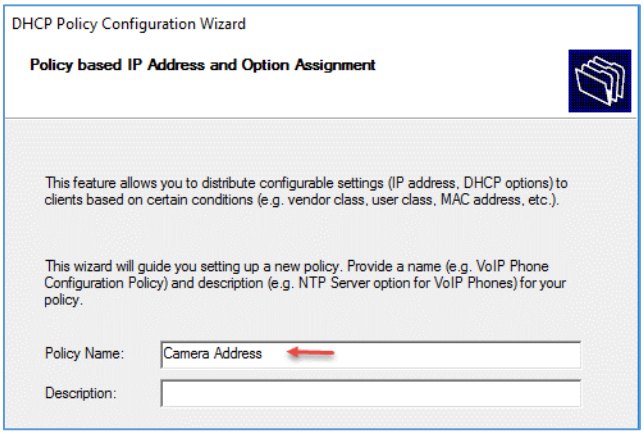
به مانند شکل ۸-۲۸٤، در داخل Scope بر روی Policies کلیک راست کنید و گزینه‌ی New Policy را انتخاب کنید.



شکل ۸- ۲۸۴ تخصیص آدرس *IP*

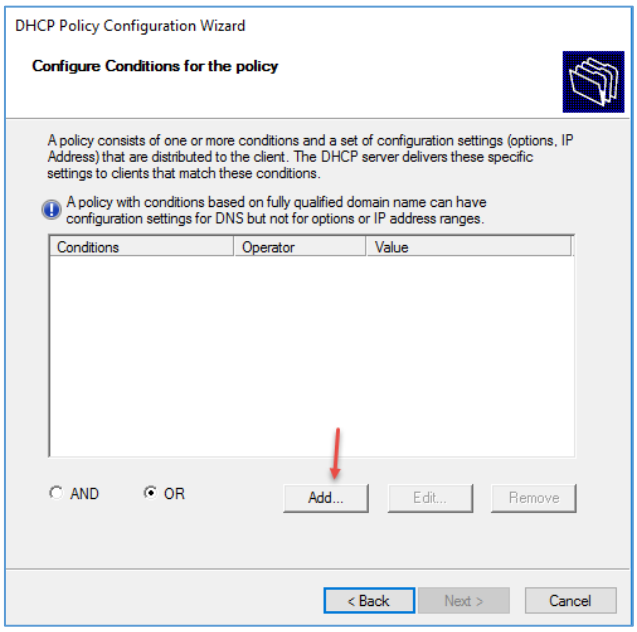
در شکل ۸-۲۸۵، یک نام به دلخواه خود وارد و بر روی Next کلیک کنید.

www.takbook.com



شکل ۸- ۲۸۵ تخصیص آدرس IP

در شکل ۸-۲۸۶ ، دو گزینه‌ی And و OR وجود دارد که باید آنها را بسته به شرط خود انتخاب کنید، مثلاً می‌خواهید یک MAC 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.

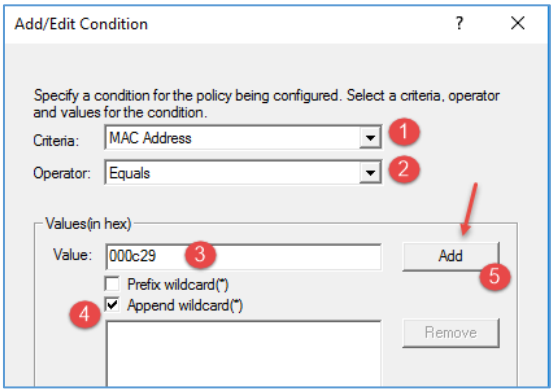


شکل ۸- ۲۸۶ تخصیص آدرس IP

در شکل ۸-۲۸۷، در قسمت شماره‌ی یک، Mac address را انتخاب کنید و در قسمت شماره‌ی دو، Equals را انتخاب کنید، در قسمت شماره‌ی سه 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

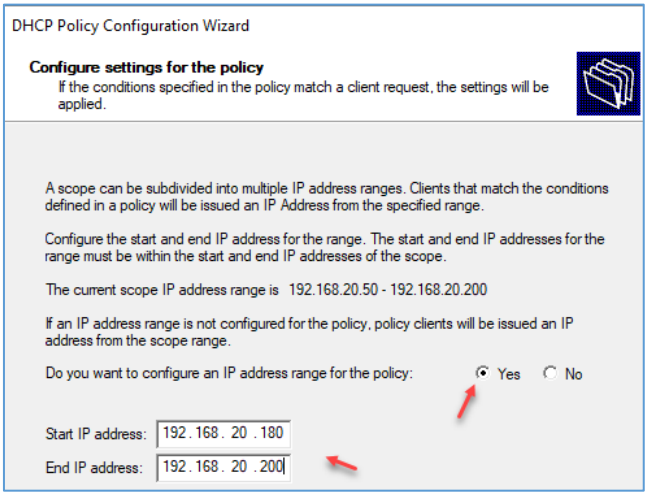
www.takbook.com

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.



شکل ۸- ۲۸۷ تخصیص دادن آدرس IP

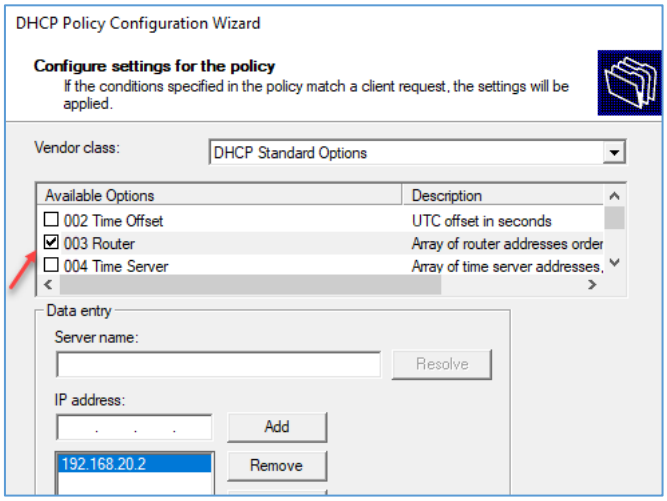
در شکل ۸-۲۸۸، می‌توانید برای دستگاه‌های خود یک رنج آدرس مشخّص کنید، مثلاً اگر این سری از مک آدرس‌ها بودند، این رنج آدرس به آنها تعلّق پیدا کند، البتّه با این کار می‌توانید نظم در کار ایجاد کنید. رنج مورد نظر خود را وارد و بر روی Next کلیک کنید.



شکل ۸- ۲۸۸ تخصیص دادن آدرس IP

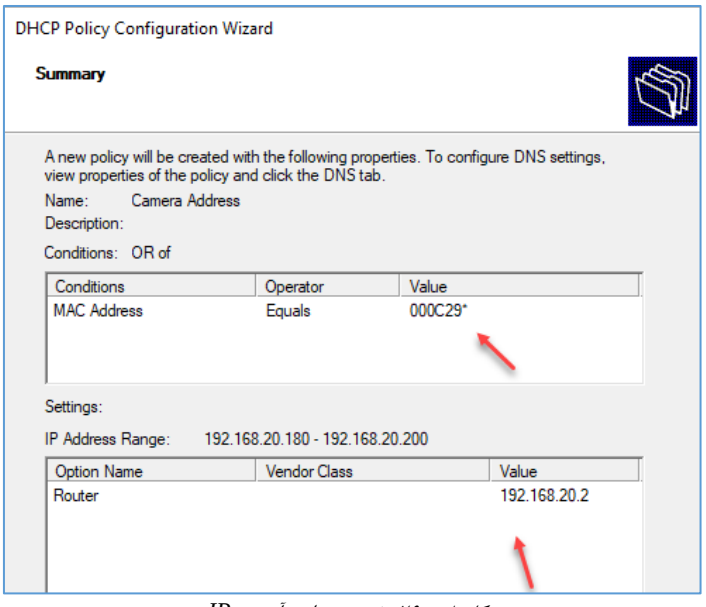
در شکل ۸-۲۸۹، می‌توانید برای رنج آدرس خود، تنظیمات مشخّص نیز انجام دهید، مثلاً می‌توانید DNS آنها را تغییر دهید و یا آدرس روتر آنها را مشخّص کنید.

www.takbook.com



شکل ۸- ۲۸۹ تخصیص دادن آدرس IP

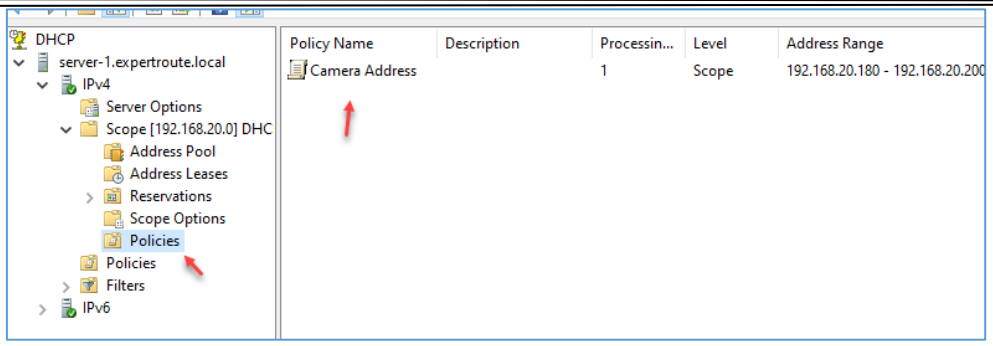
در شکل ۸-۲۹۰، می‌توانید اطّلاعات کلّی خود را مشاهده کنید، در صورت اشتباه می‌توانید به عقب برگردید و آنها را تکمیل کنید.



شکل ۸- ۲۹۰ تخصیص دادن آدرس IP

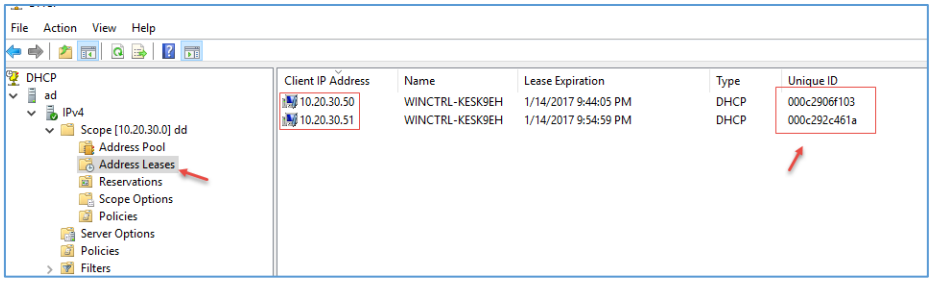
همان‌طور که در شکل ۸-۲۹۱، مشاهده می‌کنید، Policy مورد نظر به لیست اضافه شده است، در حال حاضر اگر دستگاه‌ها را به شبکه متّصل کنید، این Policy روی آنها Set خواهد شد.

www.takbook.com



شکل ۸- ۲۹۱ تخصیص دادن آدرس IP

همان‌طور که در شکل ۸-۲۹۲، مشاهده می‌کنید، دو کلاینت به لیست اضافه شده‌اند که آدرس آنها در رنج مشخّص شده است و آدرس MAC آنها نیزمشخّص است.



شکل ۸- ۲۹۲ تخصیص دادن آدرس IP

۸-۳-۱۲ بررسی IPv6 در DHCP

بعد از اینکه IPv4 طراحی شد کسی فکر آن را نکرد که وسایل الکترونیکی، آن‌قدر زیاد شوند که تعداد IP برای تخصیص به آنها با محدودیت روبرو شود، بعد از اینکه این مشکل پیش آمد، محققان سازمان Internet Engineering Task Force (IETF) مدل جدید آن را با عنوان IPv6 معرفی کردند که بسیار بیشتر از IPv4 آدرس در اختیار قرار می‌داد.

در فصل پنجم به طور کامل در مورد IPv6 صحبت کردیم و شما می‌توانید آن مثل را دقیق مطالعه و دوباره به این فصل بازگردید.

Stateful Autoconfiguration

در این روش که سرویس DHCP از آن استفاده می‌کند یک آدرس با طول ۱۲۸ بیت به کلاینت‌ها واگذار می‌شود، توجه داشته باشید آدرس‌های Stateful و Stateless مکمل همدیگر هستند، مثلاً یک کلاینت می‌تواند از آدرس Stateless استفاده کند؛ ولی برای به‌دست‌آوردن دیگر اطلاعات شبکه نیاز به آدرس Stateful دارد که در ادامه آن را بررسی خواهیم کرد.

www.takbook.com

همان‌طور که بررسی کردیم، در روش Stateful به طور کامل از سرویس DHCPv6 استفاده می‌شود که سرویس DHCPv6 به‌مانند سرویس DHCP در IPv4 عمل می‌کند و برای ارتباط از پیام‌های چهارمرحله‌ای زیر استفاده می‌کند:

مرحله اول: SOLICIT

کلاینت برای دریافت اطلاعات از سرور DHCP یک پیام با آدرس FF02::1:2 که یک پیام Multicast است ارسال می‌کند.

مرحله دوم: ADVERTISE

سرورها با استفاده از پیام ADVERTISE به پیام SOLICIT دریافتی از کلاینت پاسخ می‌دهند، توجه کنید این یک پیام Unicast است، در این پیام اطلاعات آدرس‌دهی به مشتری داده می‌شود.

مرحله سوم: REQUEST

کلاینت با تأیید آدرس دریافتی به سرور DHCP پاسخ می‌دهد.

مرحله چهارم: REPLY

در آخر کار سرور با ارسال این پیام کار را به اتمام می‌رساند.

در جدول ۸-۲، لیست جامعی از پیام‌های DHCPv6 را مشاهده می‌کنید که ممکن است در هنگام عیب‌یابی با آنها برخورد کنید:

جدول ۸- ۲ بررسی پیام‌های DHCPv6

پیام DHCP	توضیحات
SOLICIT	کلاینت برای دریافت اطلاعات از سرور DHCPv6 این پیام را ارسال می‌کند.
ADVERTISE	سرور در جواب پیام SOLICIT کلاینت، اطلاعات آدرس‌دهی را برای آن ارسال می‌کند.
REQUEST	این پیام درخواستی برای پارامترهای پیکربندی IP است که از کلاینت به یک سرور خاص DHCPv6 ارسال می‌شود.
CONFIRM	یک کلاینت این پیام را به سرور می‌فرستد تا مشخص کند آیا آدرسی که برای آن تعیین شده، مناسب است.

www.takbook.com

RENEW	کلاینت این پیام را به سروری که آدرس را از آن دریافت کرده است می‌فرستد تا طول عمر آدرس‌های اختصاص‌داده‌شده خود را افزایش دهد.
REBIND	زمانی که کلاینت پیام RENEW را ارسال کرد و پاسخی از سمت سرور دریافت نکرد، پیام REBIND را برای افزایش طول عمر آدرس خود ارسال می‌کند.
REPLY	یک سرور این پیام را در پاسخ به پیام SOLICIT، REQUEST، RENEW یا REBIND که از کلاینت دریافت کرده ارسال می‌کند که حاوی آدرس و پارامترهای پیکربندی اختصاص‌یافته است.
RELEASE	کلاینت این پیام را به سرور می‌فرستد تا به سرور اطلاع دهد که به آدرس اختصاص‌داده‌شده دیگر نیاز ندارد.
DECLINE	کلاینت این پیام را به سرور می‌فرستد تا به سرور اطلاع دهد که آدرس اختصاص‌داده‌شده در حال استفاده است.
RECONFIGURE	زمانی که سرور اطلاعات جدید و به‌روز شده‌ای دارد، سرور این پیام را به کلاینت ارسال می‌کند.
INFORMATIONREQUEST	هنگامی که کلاینت فقط نیاز به اطلاعات پیکربندی اضافی دارد و نیاز به آدرس IP ندارد، این پیام را به سرور می‌فرستد.
RELAY-FORW	یک relay agent از این پیام برای ارسال اطلاعات به سرور DHCPv6 استفاده می‌کند.
RELAY-REPL	سرور DHCPv6 هم از این پیام در پاسخ به پیام RELAY-FORW استفاده می‌کند.

همان‌طور که گفتیم DHCPv6 از دو روش برای پیکربندی پشتیبانی می‌کنید:

- Stateful configuration
- Stateless configuration (SLAAC)

نسخه‌ی Stateful تقریباً مشابه نسخه IPv4 است، در کل سرورهای DHCPv6 آدرس‌های IPv6 را به همهٔ سرویس‌گیرنده‌های DHCPv6 اختصاص می‌دهند، سرورهای DHCPv6 می‌دانند که چه آدرس‌هایی به چه کلاینت‌هایی تخصیص‌داده‌شده است.

نسخه‌ی Stateless کمی متفاوت است، در این حالت سرور DHCPv6 آدرس IPv6 را به گیرندگان اختصاص نمی‌دهد، بلکه این کار از طریق تنظیمات خودکار در خود کلاینت انجام می‌شود که قبلاً در این مورد صحبت کردیم.

www.takbook.com

تفاوتی که می‌توان بین این دو حالت پیدا کرد در تعداد پیام‌هایی است که سرور DHCPv6 استفاده می‌کند که به‌صورت زیر است:

در حالت نرمال ٤ پیام ارسال می‌شود که شامل solicit, advertise, request, reply است.

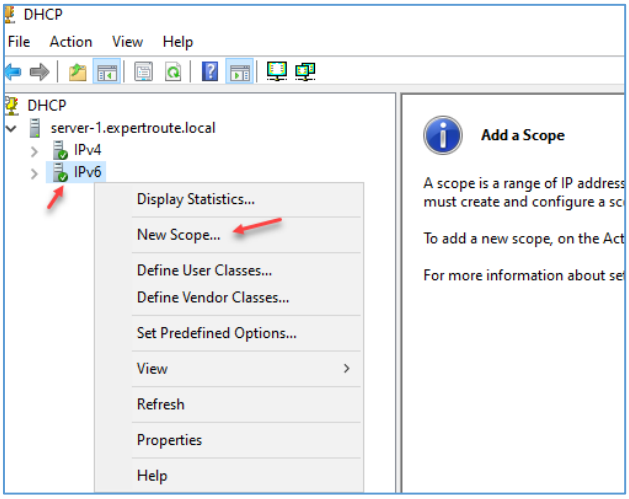
در حالت سریع (Rapid) ۲ پیام ارسال می‌شود که شامل solicit و reply است.

به طور پیش‌فرض از حالت نرمال استفاده می‌شود، ولی اگر نیاز به حالت سریع باشد باید آن را هم در سرور DHCPv6 و هم در کلاینت فعال کنید، اصولاً زمانی از حالت سریع استفاده می‌شود که شبکه‌ی شما یک شبکه‌ی تحرک بالا یا high mobility باشد و کاربران در حال رفت‌وآمد باشند.

در شبکه‌هایی که از چندین سرور DHCPv6 استفاده می‌کنید. یعنی در اصطلاح (redundancy) هستند باید از حالت نرمال یعنی از ٤ پیام استفاده کنید.

برای اینکه بهتر این سرویس را درک کنید با هم آن را در سرور DHCP فعال می‌کنیم و به کلاینت‌های خود اختصاص می‌دهیم:

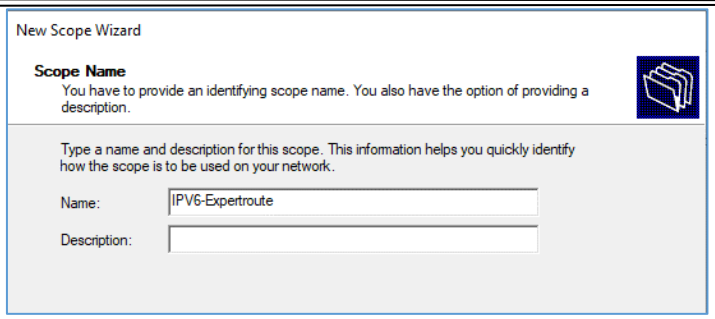
به مانند شکل ۸-۲۹۳، در سرویس DHCP بر روی IPv6 کلیک راست کنید و گزینه‌ی New Scope را انتخاب کنید.



شکل ۸- ۲۹۳ استفاده از IPv6 در DHCP

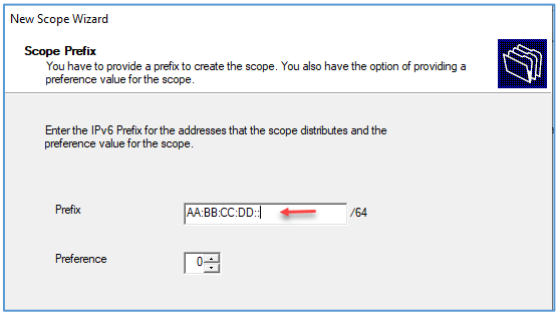
در شکل ۸-۲۹٤، نام و توضیحات دلخواه خود را وارد و بر روی Next کلیک کنید.

www.takbook.com



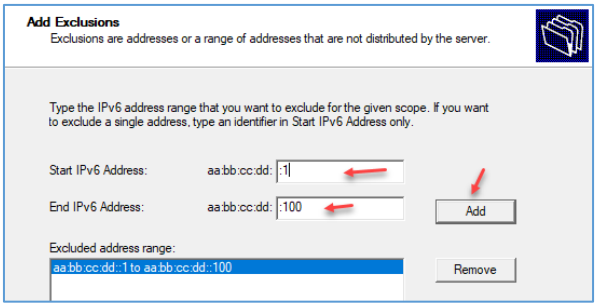
شکل ۸- ۲۹۴ استفاده از IPv6 در DHCP

در شکل ۸-۲۹۵، آدرس AA:BB:CC:DD::1 را وارد و در قسمت Prefrence هم می‌توانید یک عدد وارد کنید هر چقدر این عدد بزرگتر باشد یعنی این Scope در اولویت قرار دارد، این عدد زمانی به کار می‌آید که چندین Scope داشته باشید.



شکل ۸- ۲۹۵ استفاده از IPv6 در DHCP

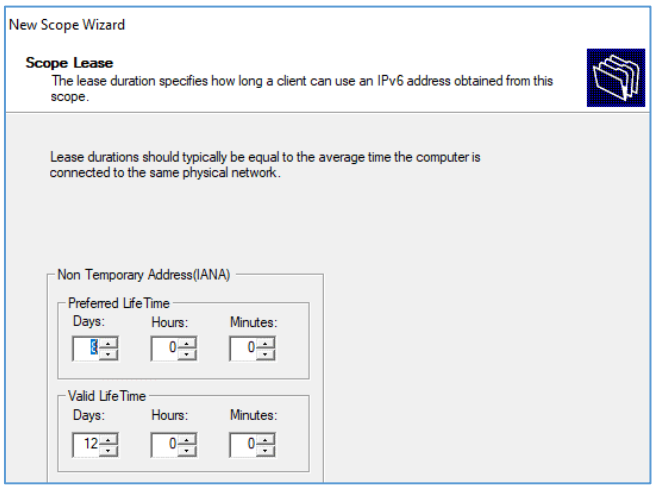
در ادامه کار طبق شکل ۸-۲۹۶، باید به مانند IPv4 یک رنج Exclusions انتخاب کنید که در اینجا از شماره‌ی 1 تا 100 انتخاب شده است، این رنج یعنی اینکه به کلاینت‌ها داده نخواهد شد و مختص مدیر شبکه است تا به سیستم‌های مشخص شده تخصیص دهد.



شکل ۸- ۲۹۶ استفاده از IPv6 در DHCP

www.takbook.com

در شکل ۸-۲۹۷، باید مقدار زمان تخصیص دادن آدرس به کلاینت‌ها را مشخص کنید که زمان ۸ روز و ۱۲ روز به صورت پیش‌فرض انتخاب شده است، توجه داشته باشید Tempoary Address به آدرس‌هایی گفته می‌شود که توسط خود کلاینت به صورت اتوماتیک ایجاد می‌شوند که در بخش‌های قبلی آن را بررسی کردیم و در این قسمت Non Temporary Address نوشته شده است یعنی آدرس‌هایی که خود سرویس DHCP تخصیص می‌دهد.

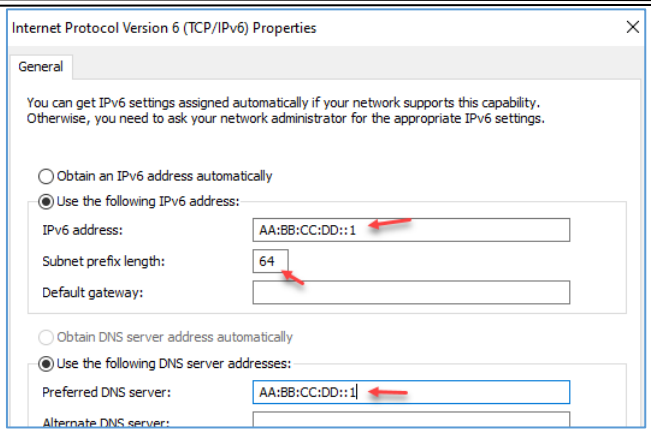


شکل ۸- ۲۹۷ استفاده از IPv6 در DHCP

در صفحه‌ی آخر هم با انتخاب گزینه‌ی Active می‌توانید Scope مورد نظر را فعال کنید.

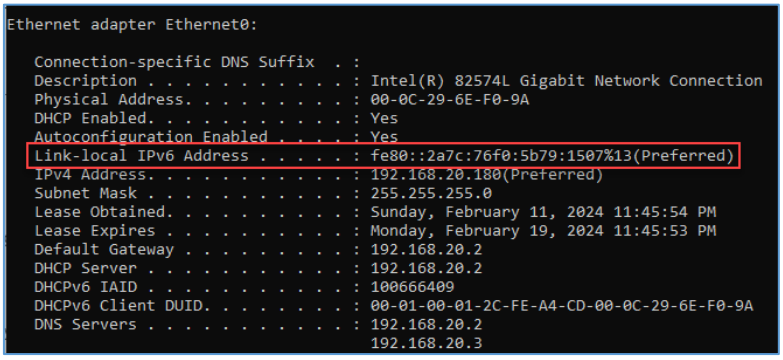
در ادامه کار شما باید به سرور اصلی DHCP به صورت دستی IPv6 اختصاص دهید تا عملیات دادن آدرس به کلاینت‌ها به درستی انجام شود، برای این کار وارد کارت شبکه‌ی سرور شوید و بر روی IPv6 دو بار کلیک کنید تا شکل ۸-۲۹۸، ظاهر شود، در قسمت IPv6 address باید آدرس این سرور را که در رنج همان Scope ایجاد شده قرار دارد وارد کنید و مقدار ٦٤ را برای Length در نظر بگیرید و در آخر مقدار DNS را برابر با همان آدرس IPv6 قرار دهید و بر روی OK کلیک کنید.

www.takbook.com



شکل ۸- ۲۹۸ استفاده از IPv6 در DHCP

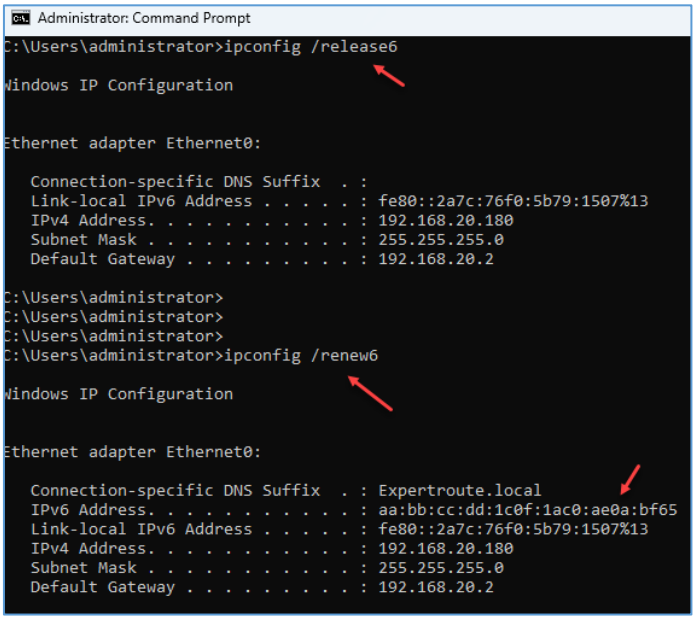
حالا وارد یکی از کلاینت‌ها شوید و CMD را اجرا کنید، همان‌طور که در شکل ۸-۲۹۹، مشاهده می‌کنید در حال حاضر کلاینت از آدرس IPv6 Local که مختص خود کلاینت است و خودش ایجاد کرده است استفاده می‌کند و هنوز هیچ آدرسی از سرور DHCPv6 دریافت نکرده است.



شکل ۸- ۲۹۹ استفاده از IPv6 در DHCP

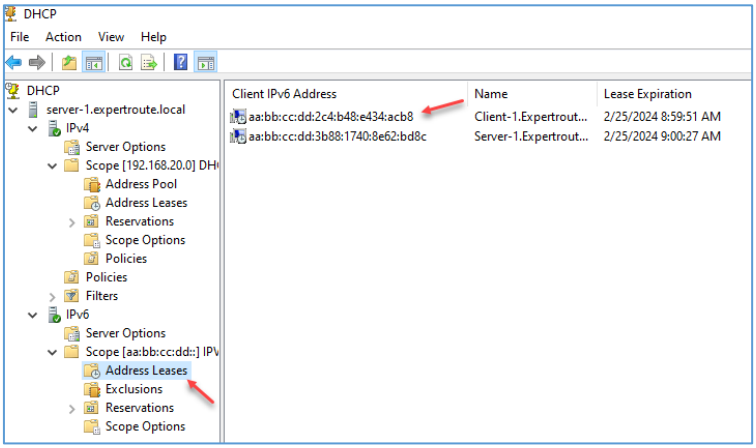
به مانند شکل ۸-۳۰۰، در CMD دستور Ipconfig /release6 را برای از دست دادن آدرس IPv6 وارد کنید و بعد از آن دستور Ipconfig /renew6 را اجرا کنید تا آدرس جدید از سرور DHCPv6 دریافت کند، اگر به خروجی دقت کنید آدرس aa:bb:cc:dd:1c0f:1ac0:ae0a:bf65 از سرور DHCPv6 دریافت شده است.

www.takbook.com



شکل ۸- ۳۰۰ استفاده از IPv6 در DHCP

به مانند شکل ۸-۳۰۱، اگر وارد سرویس DHCP شوید و در قسمت IPv6 بر روی Address Leases کلیک کنید آدرس تخصیص داده شده به کلاینت مورد نظر را مشاهده می‌کنید و همینطور آدرسی که به خود همین سرور DHCP تخصیص داده شده مشخص شده است.

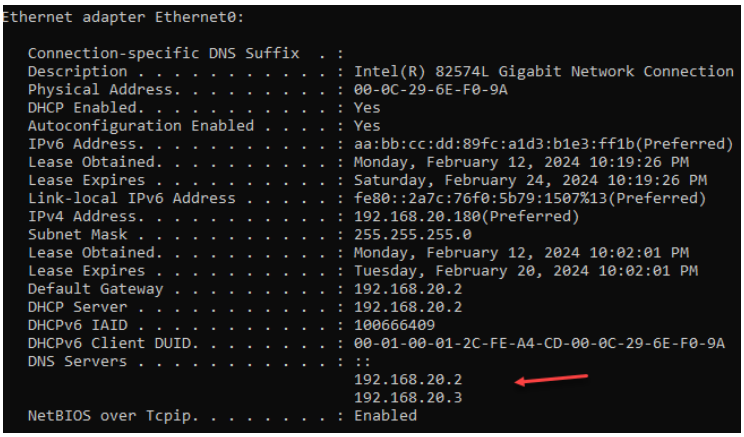


شکل ۸- ۳۰۱ استفاده از IPv6 در DHCP

نکته‌ای که می‌توان در اینجا بیان کرد این است که هر دو ورژن IP فعال است و همزمان در حال کار است.

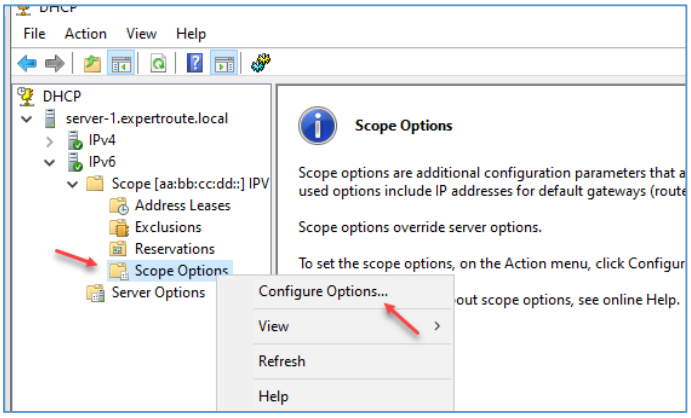
www.takbook.com

دوباره وارد کلاینت شوید و به مانند شکل ۸–۳۰۲، دستور Ipconfig /all را وارد کنید، اگر به قسمت DNS توجه کنید هیچ سروری برای Ipv6 تعریف نشده است.



شکل ۸– ۳۰۲ استفاده از IPv6 در DHCP

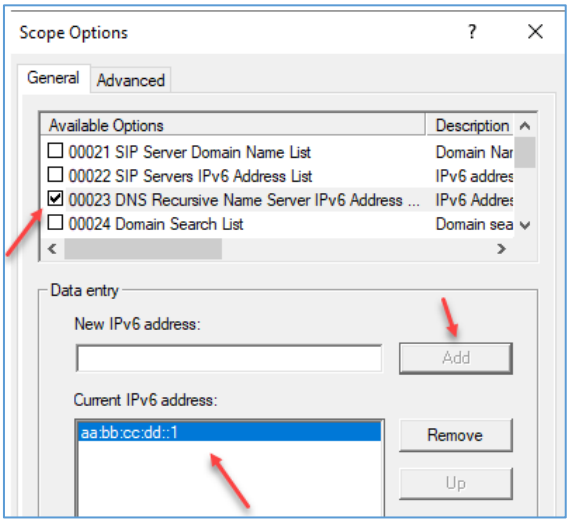
برای حل این مشکل باید به مانند شکل ۸–۳۰۳، وارد سرویس DHCP شوید و در قسمت IPv6 و از زیرمجموعه‌ی Scope Options گزینه‌ی Configure Options را انتخاب کنید.



شکل ۸– ۳۰۳ استفاده از IPv6 در DHCP

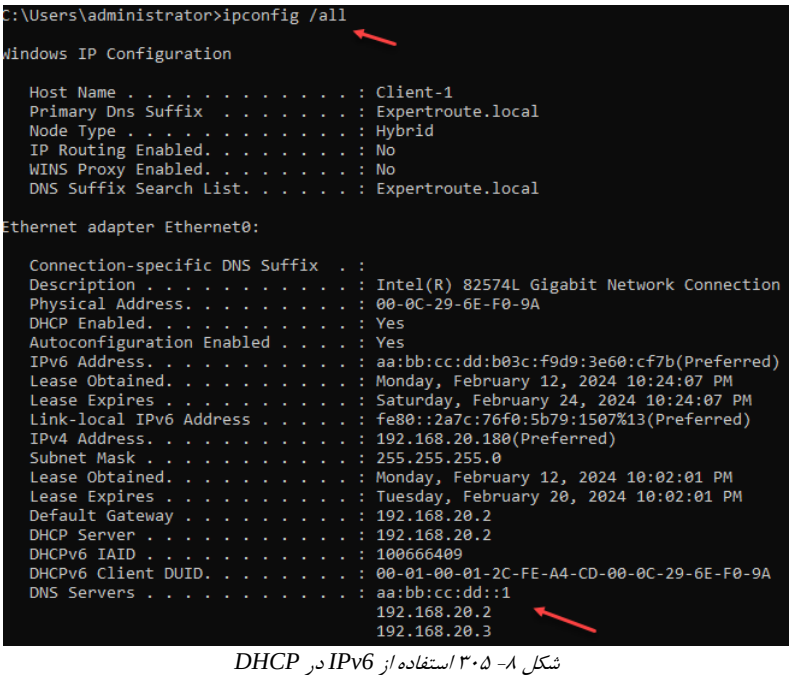
در شکل ۸–۳۰٤، گزینه‌ی DNS Recursive… را انتخاب و آدرس سرور DNS را که مشخص کردیم وارد و بر روی Add کلیک کنید و در آخر و بر روی هم OK کلیک کنید.

www.takbook.com



شکل ۸- ۳۰۴ استفاده از IPv6 در DHCP

حالا وارد کلاینت مورد نظر شوید و دستور ipconfig /release6 و در ادامه دستور ipconfig /renew6 را وارد کنید تا اطلاعات جدید از سرور DHCP دریافت شود و بعد از این دستورات باید دستور Ipconfig /all را به مانند شکل ۸-۳۰۵، وارد کنید، همان‌طور که در خروجی مشاهده می‌کنید آدرس DNS در کلاینت ثبت شده است.

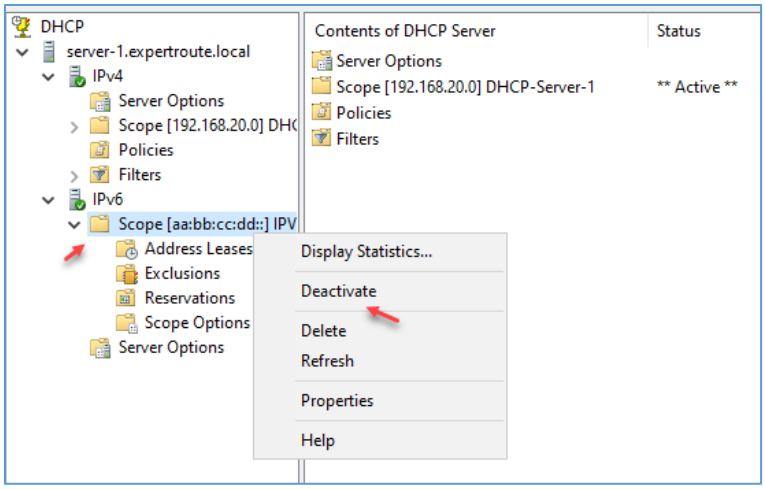


شکل ۸- ۳۰۵ استفاده از IPv6 در DHCP

www.takbook.com

توجه داشته باشید بقیه داستان‌های IPv6 هم دقیقاً شبیه به IPv4 است و طبق مراحل قبلی می‌توانید آن را انجام دهید.

اگر می‌خواهید یک Scope را چه برای IPv4 و چه برای IPv6 غیرفعال کنید باید به مانند شکل ۸-۳۰٦، بر روی Scope مورد نظر کلیک راست کنید و گزینه‌ی Deactivate را انتخاب کنید.



شکل ۸- ۳۰۶ استفاده از IPv6 در DHCP

۸-۳-۱۳ سرویس Active Directory Administrative Center

Active Directory Administrative Center (ADAC) یک ابزار گرافیکی است که توسط مایکروسافت برای مدیریت Active Directory ارائه شده است. این ابزار به مدیران شبکه کمک می‌کند تا منابع و کاربران را به راحتی مدیریت کنند و امکاناتی را برای تسهیل وظایف مدیریتی فراهم می‌آورد.

ویژگی‌ها و قابلیت‌های Active Directory Administrative Center:

- مدیریت کاربران و گروه‌ها: ADAC امکان ایجاد، ویرایش و حذف کاربران و گروه‌ها را فراهم می‌کند. همچنین می‌توانید مجوزهای دسترسی را برای هر کاربر یا گروه تعیین کنید.
- Organizational Units (OUs): مدیران می‌توانند OUs را ایجاد و مدیریت کنند. OUs به سازمان‌دهی کاربران و منابع کمک می‌کند و می‌توانند سیاست‌های گروهی خاصی را بر روی آن‌ها اعمال کرد.
- Group Policy Management: ADAC این امکان را فراهم می‌کند که سیاست‌های گروهی (Group Policies) را مدیریت کنید و تنظیمات خاصی را برای کاربران و کامپیوترها در شبکه اعمال کنید.
- فعالیت‌های گزارش‌گیری: ابزار گزارش‌گیری به مدیران اجازه می‌دهد که فعالیت‌های مختلف در Active Directory را رصد و نظارت کنند.

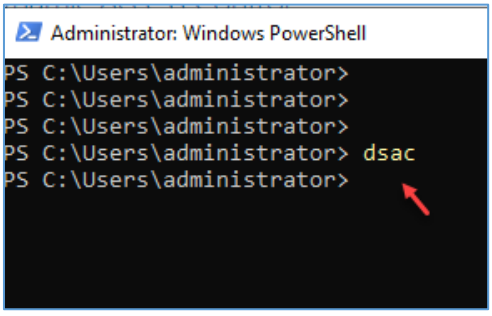
www.takbook.com

- مرورگر دایرکتوری: ADAC به مدیران این امکان را می‌دهد که به راحتی در ساختار دایرکتوری جستجو کنند و منابع مختلف را پیدا کنند.
- پشتیبانی از PowerShell: ADAC به مدیران این امکان را می‌دهد که اسکریپت‌های PowerShell را برای خودکارسازی وظایف مختلف اجرا کنند. این قابلیت به مدیران کمک می‌کند تا عملیات پیچیده را به راحتی و با سرعت بیشتری انجام دهند.

مزایای Active Directory Administrative Center:

- رابط کاربری ساده: ADAC دارای یک رابط کاربری گرافیکی است که کار با آن را برای مدیران آسان‌تر می‌کند.
- مدیریت متمرکز: مدیران می‌توانند همه منابع و کاربران را از یک نقطه مدیریت کنند.
- کاهش خطا: با استفاده از ابزارهای گرافیکی، احتمال بروز خطا در پیکربندی‌ها کاهش می‌یابد.

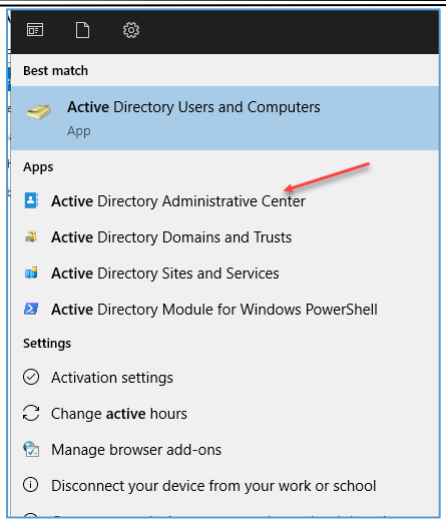
برای اجرای این سرویس می‌توانید از دو روش استفاده کنید، یکی اینکه دستور DSAC را در PowerShell به صورت شکل ۸-۳۰۷، اجرا کنید.



شکل ۸- ۳۰۷ بررسی Administrative Center

روش دیگر اینکه به مانند شکل ۸-۳۰۸، وارد Search ویندوز شوید و کلمه‌ی Active را وارد کنید و در گزینه‌های موجود، گزینه Active Directory Administrative Center را انتخاب کنید تا شکل ۸-۳۰۹، ظاهر شود.

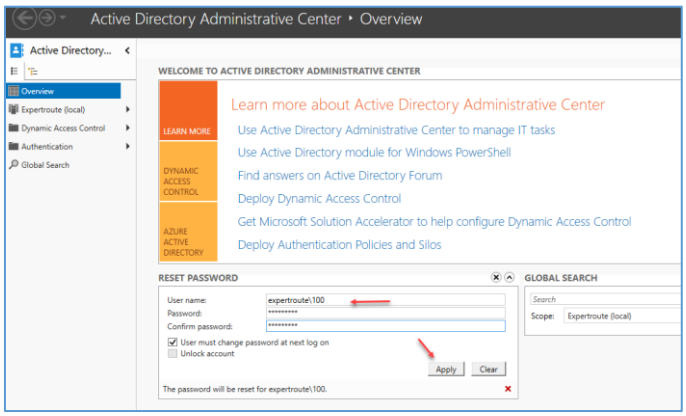
www.takbook.com



شکل ۸- ۳۰۸ بررسی *Administrative Center*

همان‌طور که در شکل ۸-۳۰۹، مشاهده می‌کنید، سرویس موردنظر اجرا شده است، در صفحه‌ی اول یعنی، Overview بیشترین چیزی که به چشم می‌خورد، لینک‌های راهنمایی قرار دارد. شما می‌توانید با متصل شدن به اینترنت و کلیک بر روی هر یک از لینک‌ها، اطلاعاتی خوبی را دریافت کنید.

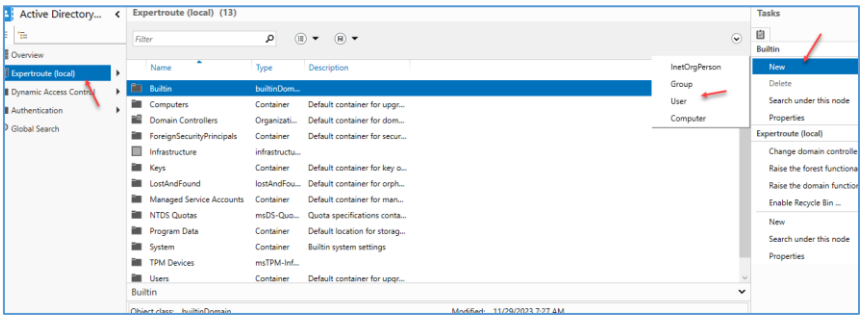
در قسمت پائین، صفحه Reset Password وجود دارد که شما می‌توانید با وارد کردن اطلاعات کاربر موردنظر به مانند شکل و وارد کردن رمز جدید، رمز کاربر موردنظر را به راحتی تغییر دهید. قسمت بعدی مربوط به Global Search می‌باشد که می‌توانید کاربران و گروه‌های موردنظر خود را جستجو کنید.



شکل ۸- ۳۰۹ بررسی *Administrative Center*

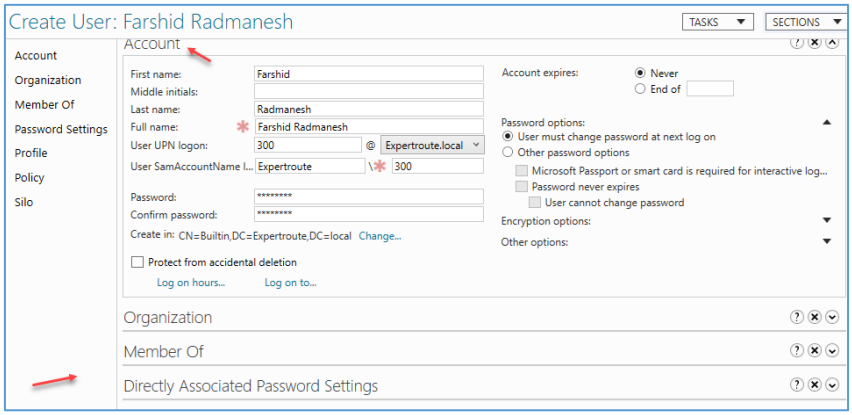
www.takbook.com

در قسمت بعد، به مانند شکل ۸-۳۱۰، بر روی نام سرور (SRV-1) کلیک کنید تا لیست کامل اطلاعات برای شما نمایش داده شود. برای ایجاد کاربر جدید از سمت راست بر روی New کلیک کنید و در منوی باز شده بر روی User کلیک کنید.



شکل ۸- ۳۱۰ بررسی *Administrative Center*

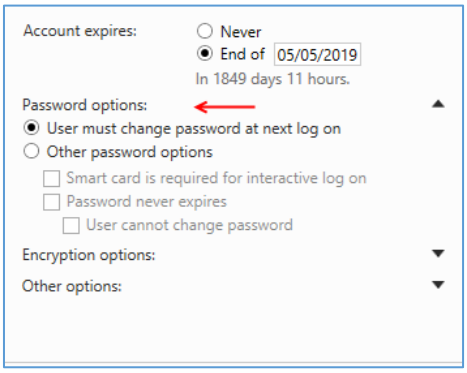
در شکل ۸-۳۱۱، هر یک از قسمت‌ها را با هم بررسی می‌کنیم. در قسمت Account، باید نام کاربر را در قسمت First name وارد کنید. نام فامیل آن را در قسمت Last Name وارد کنید که در قسمت Full name، نام کامل به صورت خودکار درج می‌شود. در قسمت User UPN logon که مهم‌ترین بخش می‌باشد، شما باید نام کاربری مربوط به کاربر موردنظر را وارد کنید که در اینجا user2 وارد شده است. این نام با نام‌هایی که در بالا وارد کرده‌اید تفاوت دارد و شما باید با این نام وارد سیستم شوید. در قسمت Password، یک رمز عبور به صورت پیچیده وارد کنید؛ یعنی به صورت Test@123456 که ترکیبی از حروف و ارقام و علائم می‌باشد؛ البته در درس‌های بعدی نحوه‌ی غیرفعال کردن پیچیدگی رمز عبور را با هم بررسی خواهیم کرد.



شکل ۸- ۳۱۱ بررسی *Administrative Center*

www.takbook.com

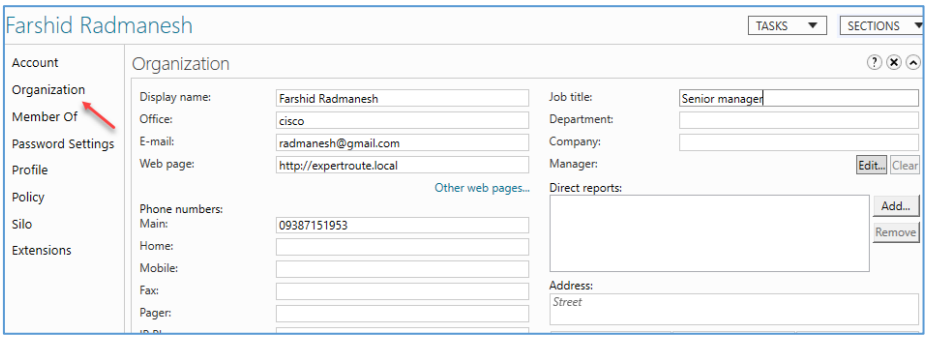
به مانند شکل ۸-۳۱۲، در قسمت Account Expire، تاریخ انقضای رمز عبور را برای کاربر موردنظر تعیین کنید و یا این قابلیت را با انتخاب گزینه‌ی Never، غیرفعال کنید. در قسمت Password options، گزینه‌ی User Must… به صورت پیش‌فرض انتخاب شده است که باعث می‌شود که کاربر در هنگام ورود، رمز دلخواه خود را وارد کند. اگر گزینه‌ی Other Password Options را انتخاب کنید، ۲ گزینه، زیرمجموعه‌ی آن می‌باشند که با انتخاب گزینه‌ی Smart card…، کاربر باید در هنگام ورود از کارت الکترونیکی خود برای ورود استفاده کند و اگر گزینه‌ی Password Never Expire را انتخاب کنید رمز عبور به هیچ وجه انقضاء نخواهد شد و اگر گزینه‌ی User Cannot Change Password را انتخاب کنید، کاربر توانایی تغییر رمز عبور را نخواهد داشت و همان رمزی که شما برای آن قرار دادید، ثابت خواهد ماند.



شکل ۸- ۳۱۲ بررسی *Administrative Center*

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

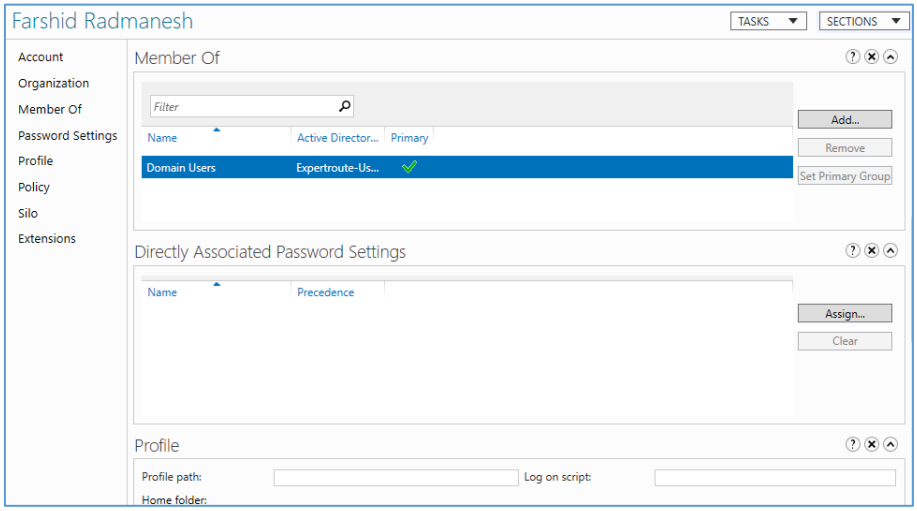
به مانند شکل ۸-۳۱۳، در قسمت Organization یا همان واحد سازمانی می‌توانید مشخصات کاملی از محل کار، آدرس، شماره تماس، وب سایت و ... را وارد کنید. سعی کنید این کار را برای هر کاربر انجام دهید تا اطلاعات کاملی از آن‌ها در اختیار شما باشد.



شکل ۸- ۳۱۳ بررسی *Administrative Center*

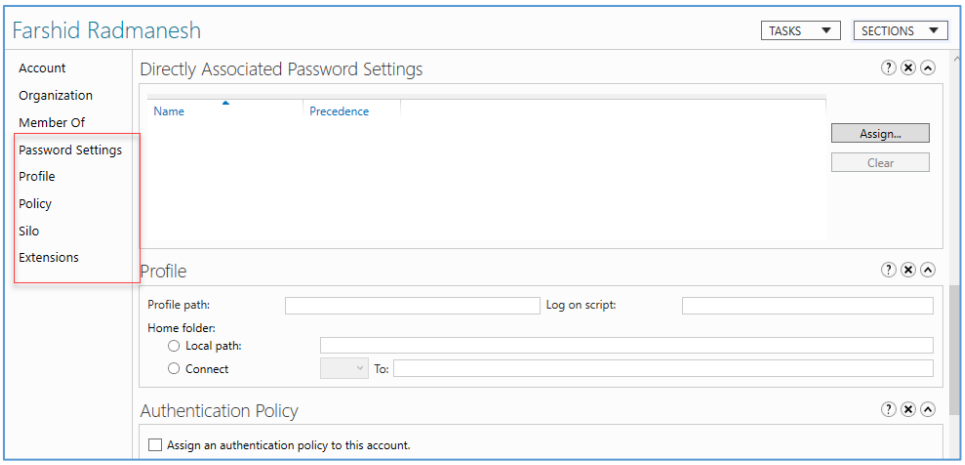
www.takbook.com

به مانند شکل ۸-۳۱٤، در قسمت Member Of، می‌توانید کاربر خود را عضو گروه خاصی کنید. برای این کار کافی است بر روی Add کلیک کنید و گروه موردنظر را مشخص کنید.



شکل ۸- ۳۱۴ بررسی *Administrative Center*

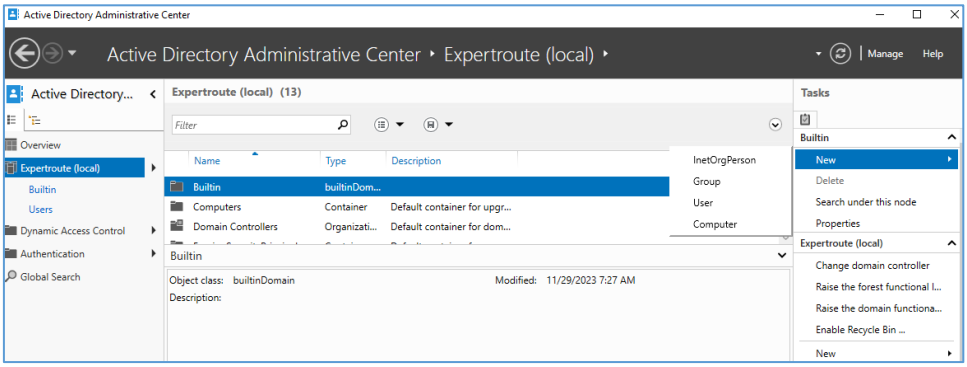
به مانند شکل ۸-۳۱۵، در قسمت Password Settings، باید یک Object برای Password ایجاد کنیم و به این قسمت متصل کنیم. Password Object، مشخص کننده‌ی حداکثر و حداقل رمز عبور و... می‌باشد. در مورد این موضوع، به صورت کامل و مفصل بحث خواهیم کرد. در قسمت Profile به مانند قبل می‌توانیم برای کاربران Profile و درایو مشخص ایجاد کنیم. قسمت‌های Policy و Silo برای تعریف احراز هویت و یا همان authentication برای کاربران می‌باشد که باید قبل از آن Policies مربوطه تعریف شود تا بتوان از این موضوع استفاده کرد.



شکل ۸- ۳۱۵ بررسی *Administrative Center*

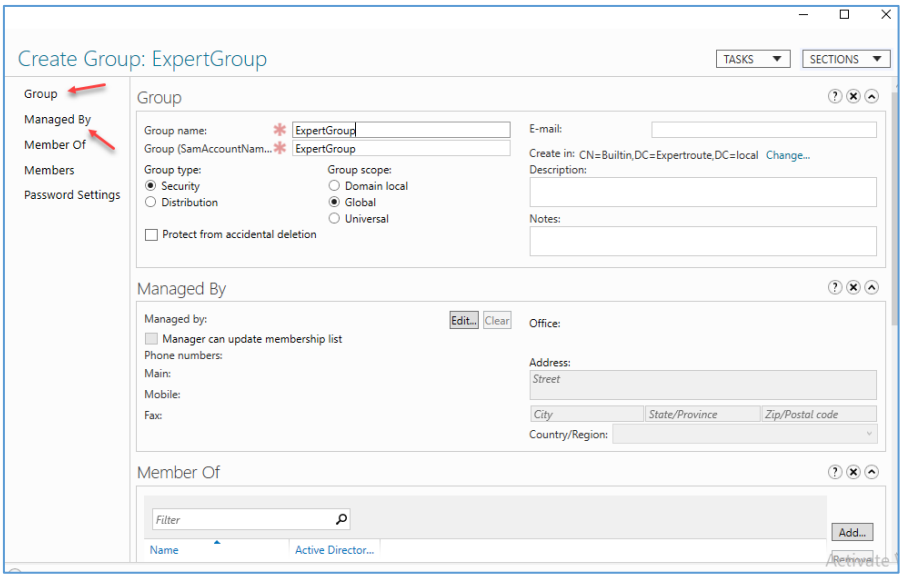
www.takbook.com

بعد از ایجاد کاربر، نوبت به این می‌رسد که یک گروه جدید ایجاد کنیم؛ برای این کار مانند شکل ۸-۳۱۶، از سمت چپ بر روی نام دومین کلیک کنید و در صفحه‌ی باز شده از قسمت New گزینه‌ی Group را انتخاب کنید.



شکل ۸- ۳۱۶ بررسی *Administrative Center*

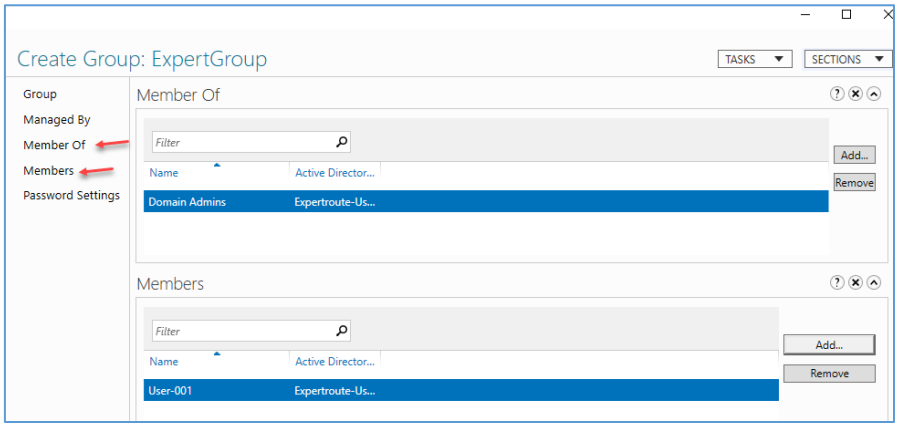
در شکل ۸-۳۱۷، در قسمت Group، باید نام گروه را در قسمت Group Name وارد کنید و در قسمت Group Type و GroupScope، نوع گروه و حوزه‌ی فعالیت آن را مشخص کنید که درباره‌ی این موضوعات قبلاً بحث کردیم. در قسمت Managed By می‌توانید یک کاربر را به عنوان مدیر این گروه مشخص کنید که با انتخاب گزینه‌ی Edit... می‌توانید کاربر موردنظر را انتخاب کنید و با انتخاب تیک گزینه‌ی Manager Can.... به کاربر موردنظر توانایی بیشتری را در مدیریت گروه موردنظر دهید.



شکل ۸- ۳۱۷ بررسی *Administrative Center*

www.takbook.com

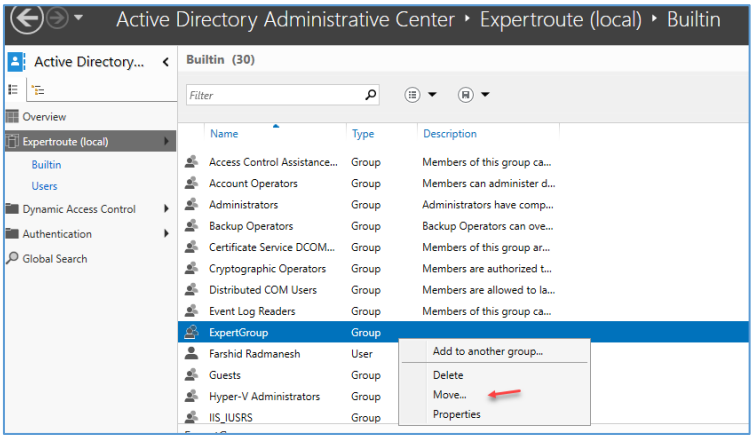
به مانند شکل ۸-۳۱۸، در قسمت Member Of، می‌توانیم این گروه را عضو گروه مشخص کنیم که این کار با کلیک بر روی Add امکان‌پذیر است و در قسمت Members می‌توانیم عضوهای این گروه را مشخص کنیم.



شکل ۸- ۳۱۸ بررسی *Administrative Center*

بر روی ok کلیک کنید تا کاربر موردنظر ایجاد شود.

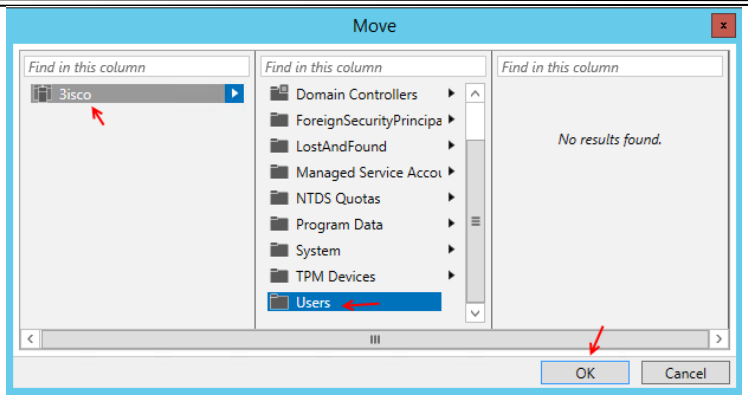
همان‌طور که در شکل ۸-۳۱۹، مشاهده می‌کنید گروه موردنظر ایجاد شده است. برای اینکه کاربران و گروه های موردنظر خود را به جای دیگر انتقال دهید بر روی آن کلیک راست کنید و گزینه‌ی Move را انتخاب کنید.



شکل ۸- ۳۱۹ بررسی *Administrative Center*

در شکل ۸-۳۲۰، باید لیست موردنظر و یا واحد سازمانی خود را انتخاب کنید تا گروه و یا کاربر موردنظر به قسمت موردنظر انتقال داده شود.

www.takbook.com



شکل ۸- ۳۲۰ بررسی *Administrative Center*

۸-۳-۱۴ سرویس Hyper-V

Hyper-V یک تکنولوژی مجازی‌سازی است که توسط مایکروسافت توسعه یافته و به کاربران و سازمان‌ها این امکان را می‌دهد که چندین ماشین مجازی (VM) را بر روی یک سرور فیزیکی اجرا کنند. این سرویس به مدیران IT کمک می‌کند تا منابع سخت‌افزاری را به‌طور بهینه‌تری مدیریت کنند و از طریق جداسازی محیط‌های مختلف، تست و توسعه نرم‌افزار را تسهیل کنند.

ویژگی‌ها و قابلیت‌های Hyper-V:

- مجازی‌سازی سرور: Hyper-V به شما این امکان را می‌دهد که چندین سیستم‌عامل مختلف را بر روی یک سرور فیزیکی اجرا کنید. این به معنای کاهش هزینه‌های سخت‌افزاری و افزایش استفاده بهینه از منابع است.
- مدیریت منابع: Hyper-V به مدیران اجازه می‌دهد منابع سخت‌افزاری مانند CPU، حافظه، و فضای دیسک را بین ماشین‌های مجازی به‌طور دینامیک تخصیص دهند.
- Isolation و امنیت: ماشین‌های مجازی به‌صورت جداگانه از یکدیگر عمل می‌کنند، که به این معنی است که مشکلات یا حملات در یک VM بر دیگر VMs تأثیر نمی‌گذارد.
- Snapshot و Checkpoint: امکان ایجاد Snapshot یا Checkpoint از ماشین‌های مجازی را فراهم می‌کند. این قابلیت به مدیران این امکان را می‌دهد که در هر زمان از وضعیت VM پشتیبان‌گیری کنند و در صورت بروز مشکل، به وضعیت قبلی برگردند.
- مقیاس‌پذیری: Hyper-V قابلیت پشتیبانی از تعداد زیادی VM و مقیاس‌پذیری برای پاسخ به نیازهای کسب‌وکار را دارد. این امکان وجود دارد که با افزایش بار، منابع بیشتری به VMها تخصیص دهید.

www.takbook.com

- Integration Services: Hyper-V از سرویس‌های ادغام (Integration Services) برای بهبود عملکرد و قابلیت‌های ماشین‌های مجازی پشتیبانی می‌کند. این سرویس‌ها شامل درایورهای بهینه‌سازی و ابزارهای مدیریت هستند.
- شبکه‌های مجازی: Hyper-V امکان ایجاد و مدیریت شبکه‌های مجازی را فراهم می‌کند، که به VMها اجازه می‌دهد به یکدیگر و به منابع خارجی متصل شوند.

مزایای Hyper-V:

- کاهش هزینه‌ها: با مجازی‌سازی، سازمان‌ها می‌توانند هزینه‌های سخت‌افزاری را کاهش دهند و از سرورهای موجود بهینه‌تر استفاده کنند.
- مدیریت آسان: ابزارهای مدیریتی مانند Hyper-V Manager و System Center Virtual Machine Manager به مدیران این امکان را می‌دهند که VMs را به‌راحتی مدیریت کنند.
- انعطاف‌پذیری: امکان تغییر منابع و تنظیمات ماشین‌های مجازی به‌راحتی و به‌طور دینامیک وجود دارد.

موارد استفاده:

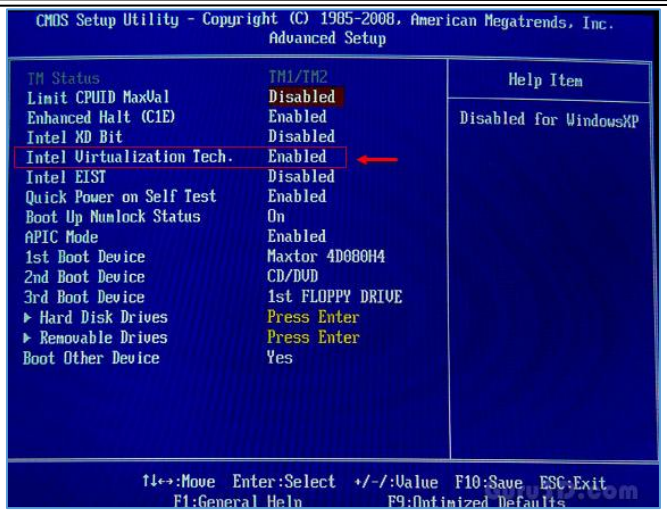
- توسعه و تست نرم‌افزار: توسعه‌دهندگان می‌توانند از Hyper-V برای ایجاد محیط‌های آزمایشی و تست استفاده کنند.
- پشتیبان‌گیری و بازیابی: سازمان‌ها می‌توانند از Hyper-V برای پشتیبان‌گیری و بازیابی سریع اطلاعات استفاده کنند.
- اجرا و مدیریت سرورهای مجازی: Hyper-V به عنوان یک پلتفرم برای راه‌اندازی سرورهای مجازی در زیرساخت‌های IT سازمان‌ها به کار می‌رود.

۱-۱۴-۳-۸ نصب سرویس Hyper-v

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، انجام این کار متفاوت خواهد بود، امّا گزینه‌های آن، به مانند شکل ۸-۳۲۱، ثابت است.

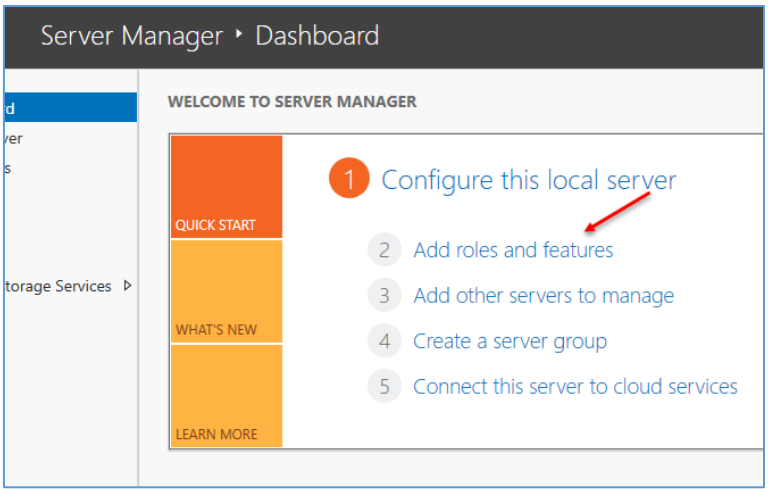
www.takbook.com



شکل ۸- ۳۲۱ سرویس Hyper-V

از نظر سخت‌افزاری، سروری که بر روی آن، سرویس Hyper-V فعال 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.

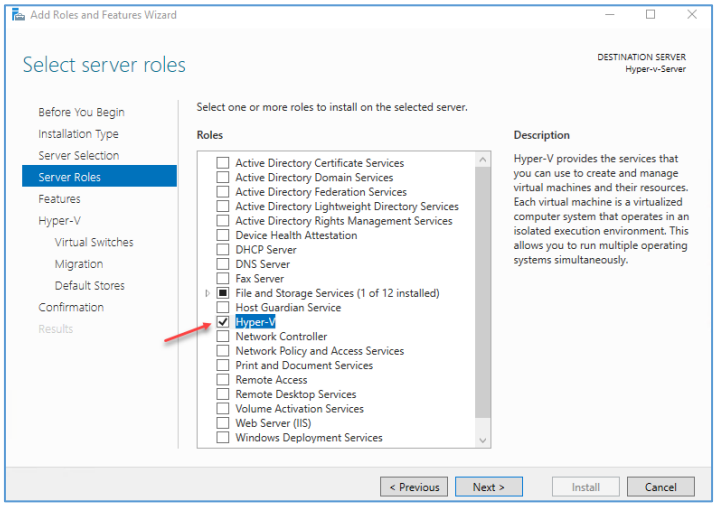
برای راه‌اندازی سرویس Hyper-V وارد ویندوز سرور ۲۰۲۵ شوید به مانند شکل ۸–۳۲۲، Server Manager را اجرا کنید و در صفحه‌ی باز شده بر روی Add roles and features کلیک کنید.



شکل ۸- ۳۲۲ سرویس Hyper-V

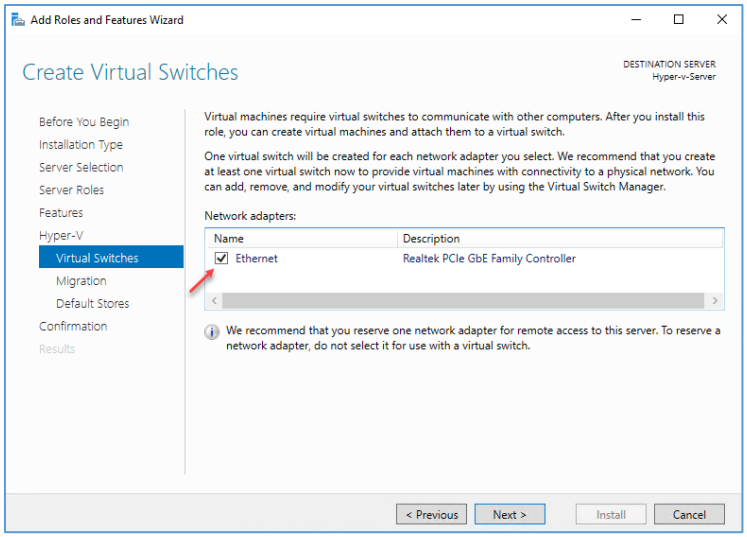
در شکل ۸–۳۲۳، گزینه‌ی Hyper-v را انتخاب و بر روی Next کلیک کنید و در آخر بر روی Install کلیک کنید تا سرویس مورد نظر نصب شود.

www.takbook.com



شکل ۸- ۳۲۳ سرویس Hyper-V

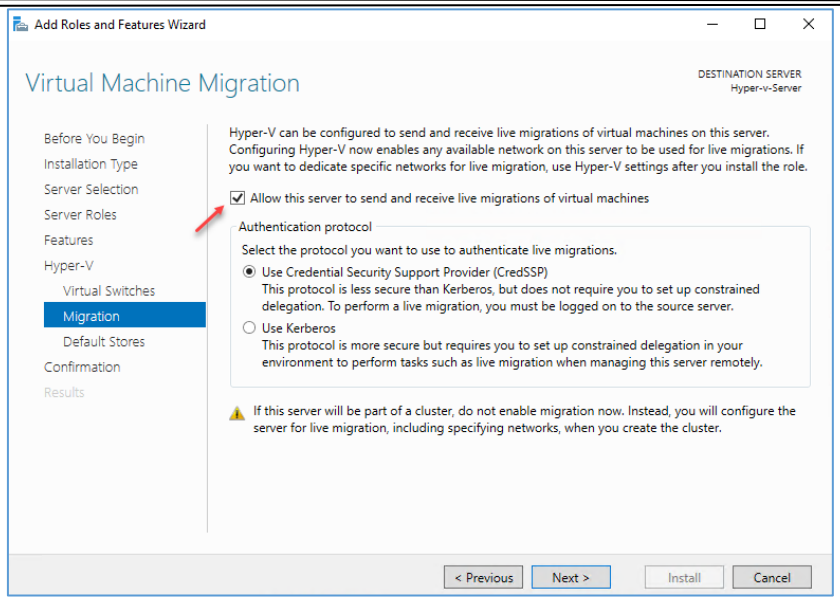
در شکل ۸-۳۲٤، باید کارت شبکه‌ی اصلی سیستم خود را انتخاب کنید تا عملیّات سوئیچینگ روی آن انجام شود.



شکل ۸- ۳۲۴ سرویس Hyper-V

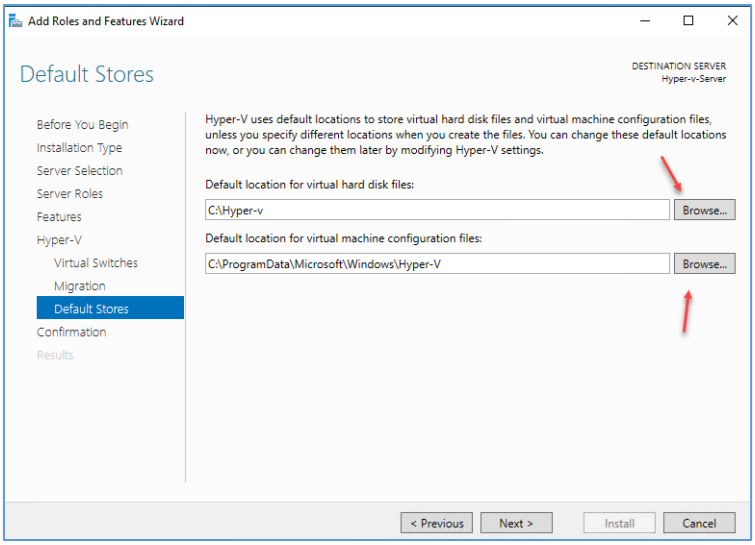
در شکل ۸-۳۲۵، تیک گزینه‌ی مورد نظر را انتخاب کنید که با این کار به این سرور و این سرویس، اجازه‌ی ارتباط با سرور و سرویس دیگر در محلّ دیگر را می‌دهید که در ادامه، در مورد این موضوع بحث خواهیم کرد، بر روی Next کلیک کنید.

www.takbook.com



شکل ۸- ۳۲۵ سرویس Hyper-V

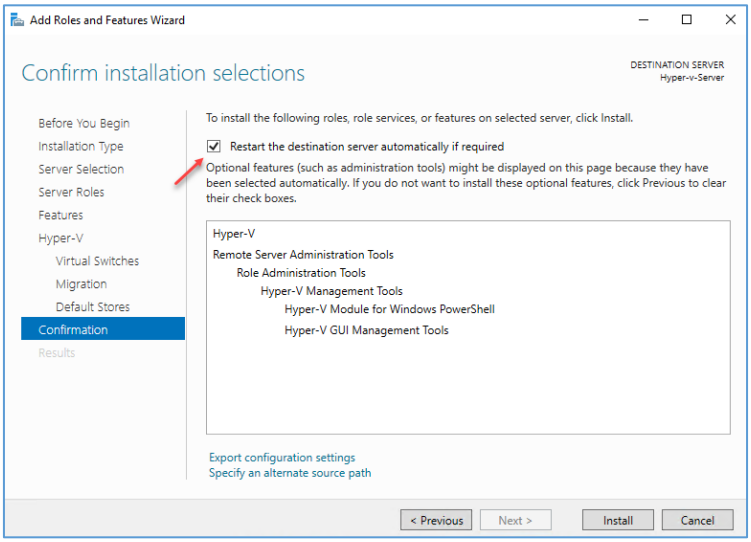
در شکل ۸-۳۲٦، باید محلّ ذخیره‌سازی اطّلاعات هارد دیسک و تنظیمات ماشین مجازی را وارد کنید، سعی کنید محلّ مورد نظر دارای حجم باشد.



شکل ۸- ۳۲۶ سرویس Hyper-V

در شکل ۸-۳۲۷، تیک گزینه‌ی Restart را انتخاب و بر روی Install کلیک کنید.

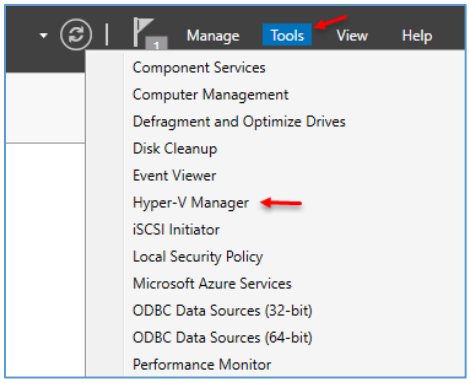
www.takbook.com



شکل ۸- ۳۲۷ سرویس *Hyper-V*

بعد از نصب سرویس اگر وارد آدرس Control Panel\Network and Internet\Network Connections شوید کارت شبکه‌ی جدید با عنوان vEthernet (Realtek PCIe GbE Family Controller - Virtual Switch) را مشاهده می‌کنید که یک کارت شبکه‌ی مجازی است و به کارت شبکه‌ی اصلی متصل شده است.

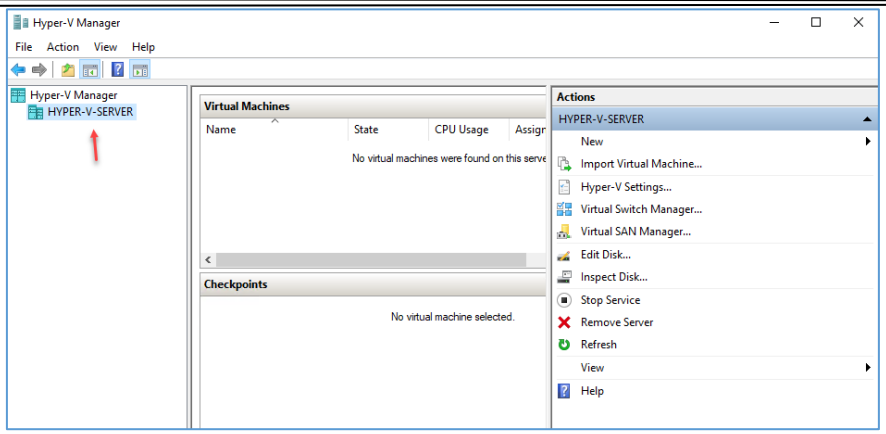
برای اجرای سرویس Hyper-V می‌توانید درجستجو سرویس مورد نظر را پیدا کنید و به مانند شکل ۸-۳۲۸، از طریق Server Manager و از طریق منوی Toools آن را اجرا کنید:



شکل ۸- ۳۲۸ سرویس *Hyper-V*

در شکل ۸-۳۲۹، سرویس Hyper-V را مشاهده می‌کنید که نسبت به ورژن 2019، 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.

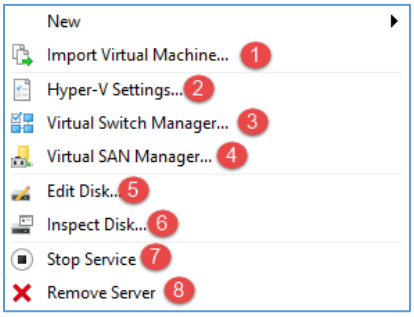
www.takbook.com



شکل ۸- ۳۲۹ سرویس Hyper-V

به مانند شکل ۸-۳۳۰، 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 و تنظیم آن 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.

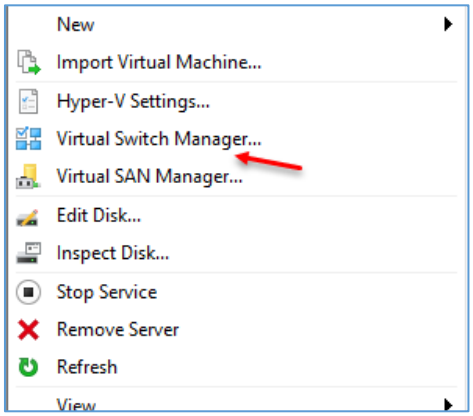
گزینه‌ی شماره‌ی پنج برای مدیریّت هارد دیسک‌های مجازی است که آنها را موقع ایجاد ماشین مجازی و یا از جایی دیگر، ایجاد می‌کنید، شماره‌ی شش، یعنی Inspect disk برای نمایش جزئیّات یک هارد دیسک مجازی است که می‌توانید اطّلاعاتی از حجم، زمان ایجاد و... را دریافت کنید، گزینه‌ی هفت برای غیر فعّال کردن سرویس Hyper-V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



شکل ۸- ۳۳۰ سرویس Hyper-V

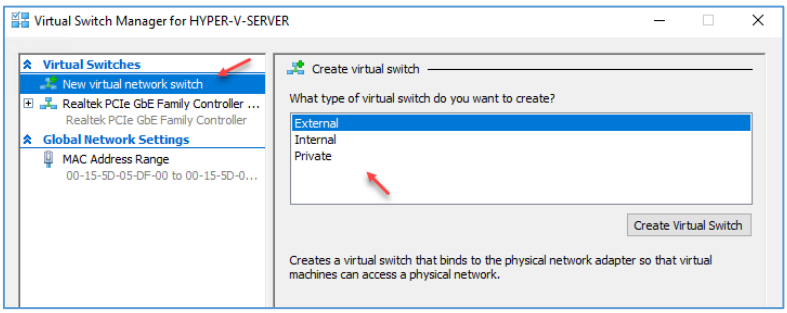
برای شروع کار به مانند شکل ۸-۳۳۱، باید کارت شبکه‌ی مربوط به سرویس Hyper-V را تنظیم کنید، برای این کار از سمت راست بر روی Virtual Switch Manager کلیک کنید.

www.takbook.com



شکل ۸- ۳۳۱ سرویس Hyper-V

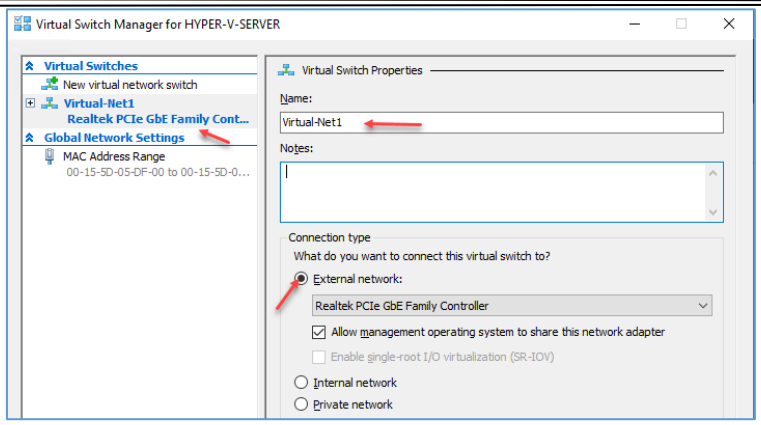
در شکل ۸-۳۳۲، از سمت چپ بر روی New Virtual Network Switch کلیک کنید، سه گزینه برای شما به نمایش در خواهد آمد که اگر External را انتخاب کنید، می‌توانید یک کارت شبکه‌ی مجازی ایجاد کنید که توانایی ارتباط با کارت شبکه‌ی اصلی را داشته باشد، به صورت پیش‌فرض، یک کارت شبکه از نوع External ایجاد شده است و به مانند شکل ۸-۲۳۲، 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.



شکل ۸- ۳۳۲ سرویس Hyper-V

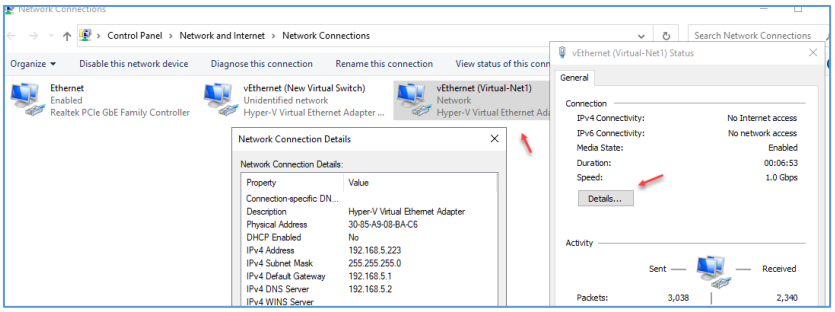
در شکل ۸-۳۳۳ در قسمت Name می‌توانید نام کارت شبکه را تغییر دهید و همینطور در قسمت External Network می‌توانید کارت شبکه‌ی اصلی خود را انتخاب کنید، توجه داشته باشید تفاوت بین کارت شبکه‌ی Internal و Private در این است که می‌توانید با استفاده از گزینه‌ی Private فقط بین ماشین مجازی ارتباط برقرار کنید ولی اگر گزینه‌ی Internal را انتخاب کنید علاوه بر ماشین مجازی می‌توانید سیستم فیزیکی خود هم در ارتباط باشید.

www.takbook.com



شکل ۸- ۳۳۳ سرویس Hyper-V

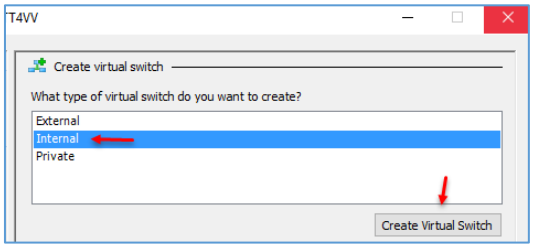
اگر وارد Network Connections شوید، به مانند شکل ۸–۲۳٤، سه کارت شبکه را مشاهده خواهید کرد که Ethernet، همان کارت شبکه‌ی اصلی ما است و در قسمت اطّلاعات IP، هیچ اطلاعاتی ندارد، امّا کارت شبکه vEthernet(Virtual-Net1)، همان کارت شبکه‌ی مجازی است که با هم ایجاد کرده بودیم و اطّلاعات IP آن نیز مشخّص شده است، کارت شبکه‌ی vEthernet(New Virtual Switch) هم همان کارت شبکه‌ی Internal است که در ادامه کارکرد آن را بررسی خواهیم کرد.



شکل ۸- ۳۳۴ سرویس Hyper-V

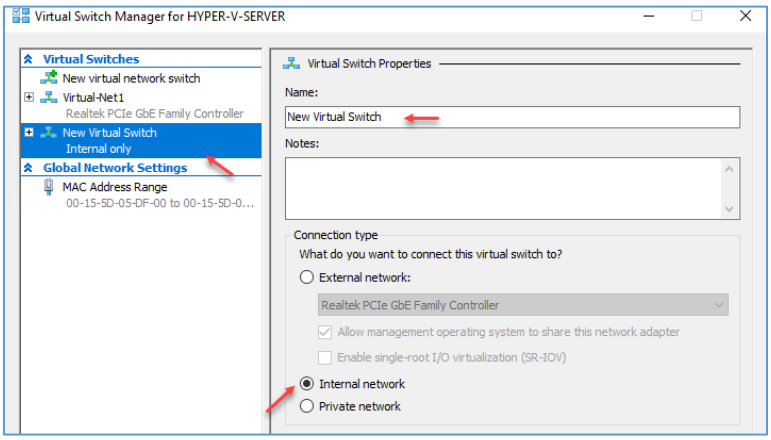
به مانند شکل ۸–۳۳۵، کارت شبکه‌ی دیگری که در لیست وجود دارد، Internal است که مختصّ ارتباط ماشین مجازی با ماشین مجازی دیگر است و توانایی ارتباط با کارت شبکه‌ی خارجی یا همان اصلی را دارد، امّا اگر گزینه‌ی Private را انتخاب کنید، می‌توانید یک ارتباط داخلی بین ماشین مجازی با ماشین مجازی دیگر ایجاد کنید و دیگر نمی‌توانید با سیستم‌های اصلی یا فیزیکی ارتباط برقرار کنید.

www.takbook.com



شکل ۸- ۳۳۵ سرویس *Hyper-V*

برای شروع کار به مانند شکل ۸-۲۳٦، با کلیک بر روی Create Virtual Switch، یک کارت Internal ایجاد کنید. می‌توانید، نام کارت شبکه‌ی خود را در قسمت Name وارد کنید و گزینه‌ی Internal Network را انتخاب و بر روی OK کلیک کنید.



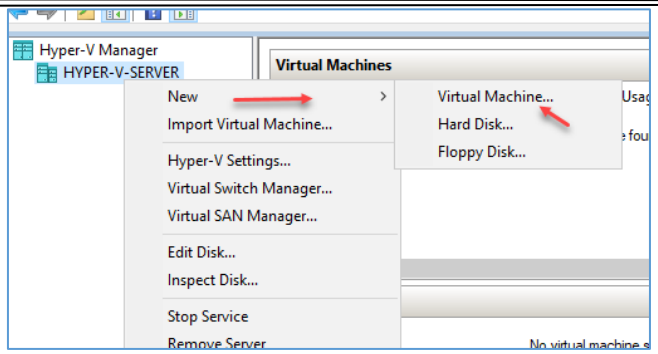
شکل ۸- ۳۳۶ سرویس *Hyper-V*

در ادامه کار ماشین مجازی با هم ایجاد و نحوه‌ی کارکرد کارت شبکه‌ها را با هم بررسی می‌کنیم.

۲-۱٤-۳-۸ ایجاد ماشین مجازی

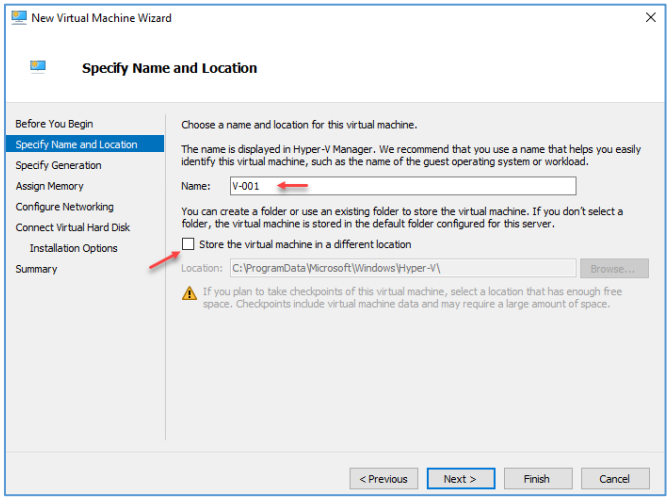
بعد از تنظیم کارت شبکه می‌توانید ماشین مجازی خود را ایجاد کنید، برای ایجاد ماشین مجازی به مانند شکل ۸-۳۳۷، وارد سرویس Hyper-V شوید و بر روی نام سرور خود کلیک راست کنید و از قسمت New، گزینه‌ی Virtual Machine انتخاب کنید.

www.takbook.com



شکل ۸- ۳۳۷ سرویس Hyper-V

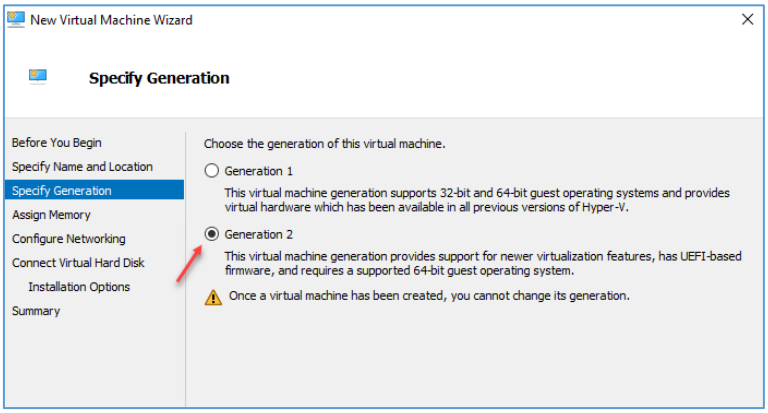
در شکل ۸-۳۳۸، باید نام ماشین مجازی خود را در قسمت Name وارد کنید و اگر بخواهید محلّ ذخیره‌سازی ماشین مجازی را تغییر دهید باید تیک گزینه‌ی Store the virtual... را انتخاب و بر روی Browse کلیک کنید و مسیر را مشخّص کنید.



شکل ۸- ۳۳۸ سرویس Hyper-V

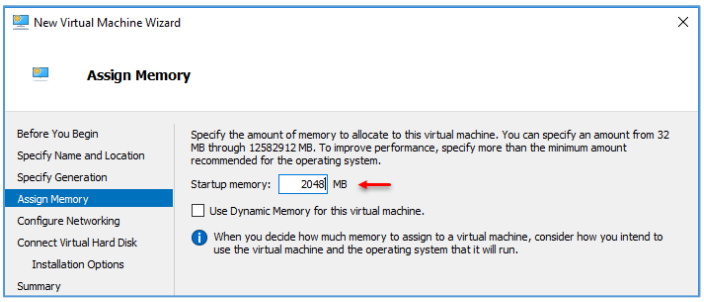
در شکل ۸-۳۳۹، دو گزینه وجود دارد که گزینه‌ی اوّل برای سیستم‌هایی که ورژن 32 bit و ٦٤bit را پشتیبانی می‌کنند و قدیمی هستند طراحی شده است و گزینه‌ی دوّم برای سخت‌افزارهای جدید که 64 bit را پشتیبانی می‌کنند و اینکه دارای UEFI می‌باشد، گزینه‌ی اوّل یا دوم را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



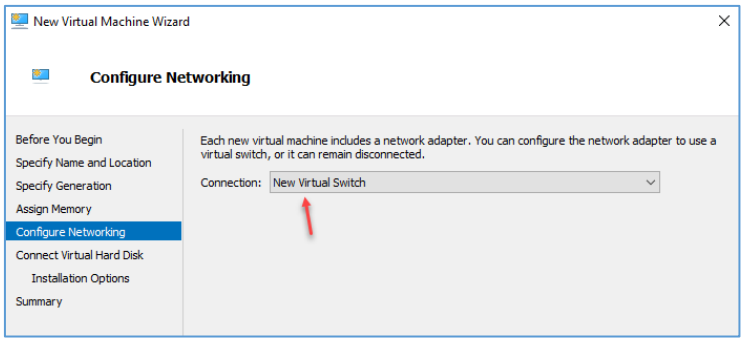
شکل ۸- ۳۳۹ سرویس Hyper-V

در شکل ۸-۳٤۰، و 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.



شکل ۸- ۳۴۰ سرویس Hyper-V

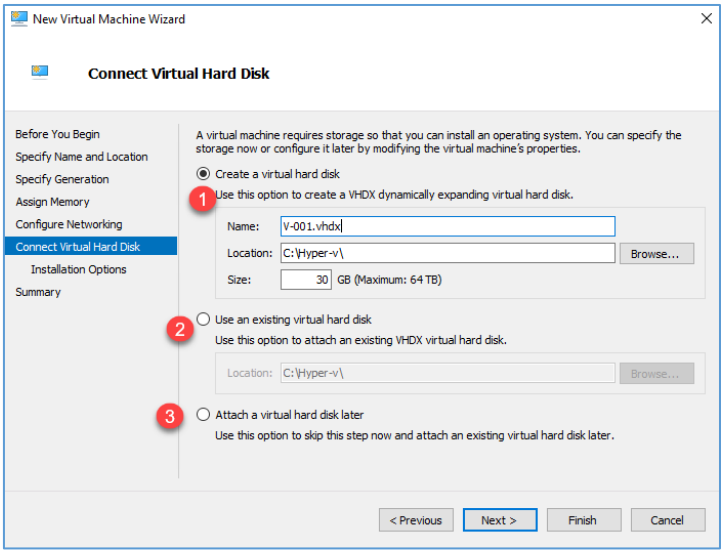
به مانند شکل ۸-۳٤۱، باید کارت شبکه‌ای که با هم ایجاد کردیم را انتخاب کنید، کارت شبکه‌ی داخلی را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۳۴۱ سرویس Hyper-V

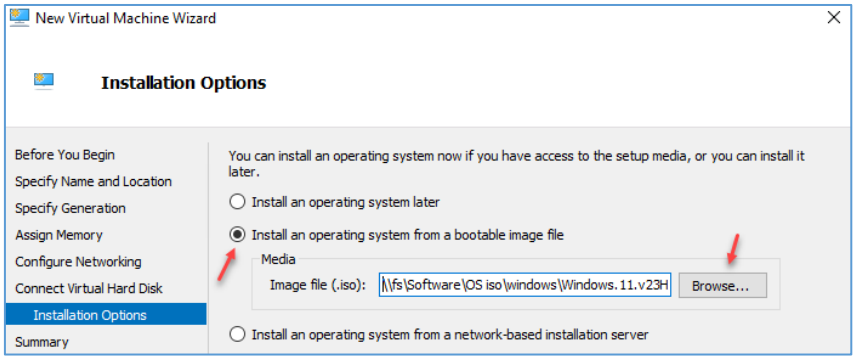
www.takbook.com

به مانند شکل ۸-۳٤۲، 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.



شکل ۸- ۳۴۲ سرویس Hyper-V

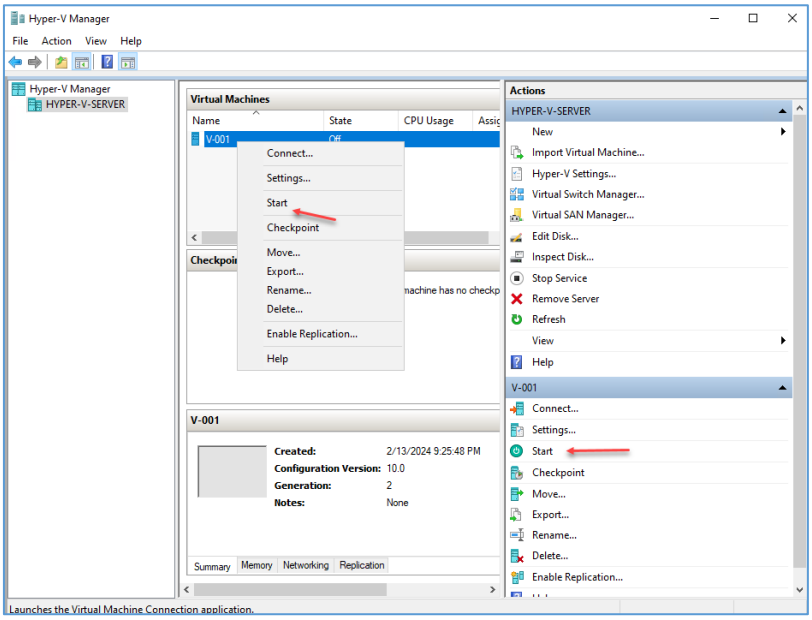
در شکل ۸-۳٤۳، باید DVD مربوط به ویندوز مورد نظر خود را در سیستم قرار دهید و گزینه‌ی Physical DVD/CD را انتخاب کنید و یا اگر از ویندوز، Image تهیّه کردید، می‌توانید در قسمت File Image بر روی Browse کلیک کنید و فایلImage مورد نظر را معرّفی کنید، بعد از انجام این کار بر روی Next کلیک کنید.



شکل ۸- ۳۴۳ سرویس Hyper-V

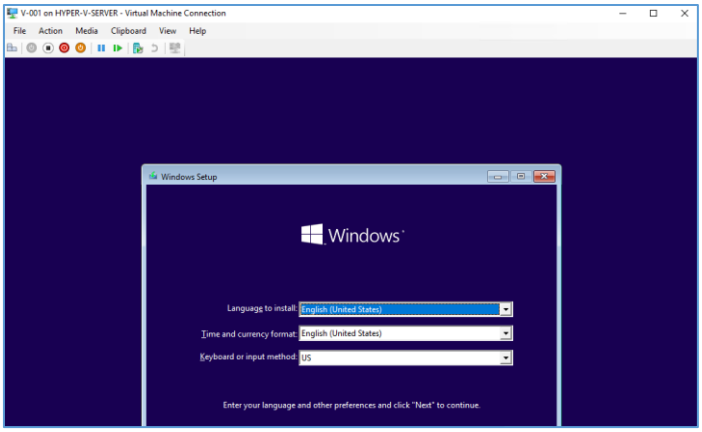
www.takbook.com

بعد از ایجاد ماشین مجازی، به مانند شکل ۸-۳٤٤، 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، بعد از روشن کردن ماشین بر روی آن دو بار کلیک کنید.



شکل ۸- ۳۴۴ سرویس Hyper-V

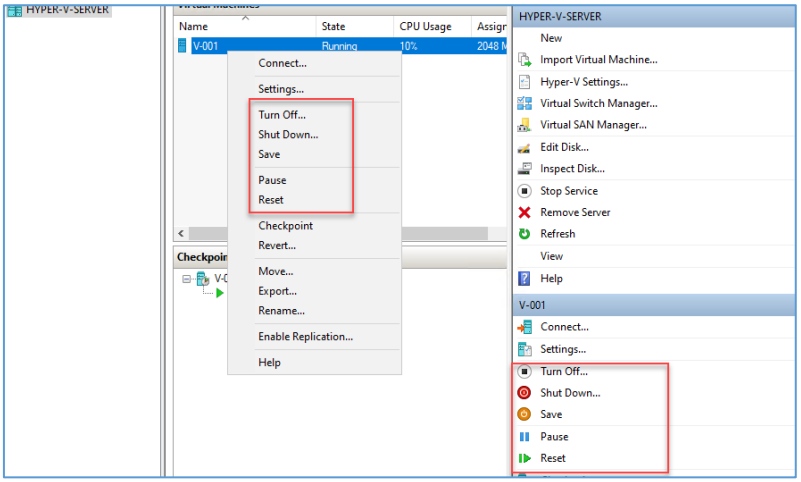
همان‌طور که در شکل ۸-۳٤٥، مشاهده می‌کنید، ماشین مورد نظر روشن شده است و ویندوز ۱۰ برای نصب آماده است، ویندوز را نصب کنید تا در ادامه از آن استفاده کنید.



شکل ۸- ۳۴۵ نصب ویندوز

www.takbook.com

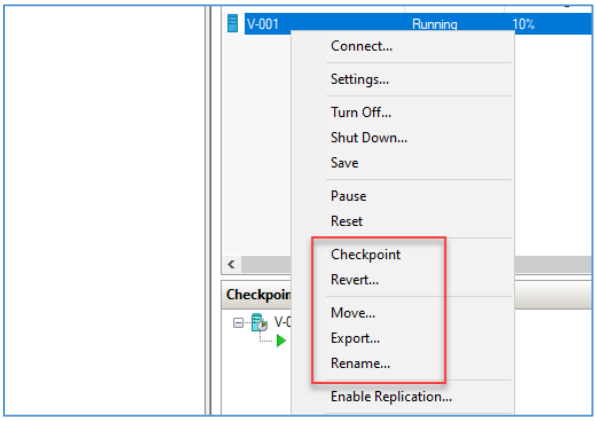
به مانند شکل ۸-۳٤٦، گزینه‌هایی دیگری نیز بعد از روشن کردن ماشین مجازی فعّال می‌شوند، مانند Turn off که برای خاموش کردن سریع ماشین مجازی می‌باشد، مانند این است که برق یک سیستم را قطع کنید. گزینه‌ی Shutdown برای خاموش کردن نرم‌افزاری سرور است، مانند اینکه داخل ویندوز بر روی Shutdown کلیک کنید، گزینه‌ی Save در هر حالتی که ماشین مجازی قرار دارد، اطّلاعات را ذخیره و ماشین را غیرفعّال 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، رم زیادی را استفاده کرده باشد و بخواهید آن را برای دقایقی متوقّف کنید، گزینه‌ی Reset نیز برای Restart کردن سریع ماشین کاربرد دارد.



شکل ۸- ۳۴۶ سرویس Hyper-V

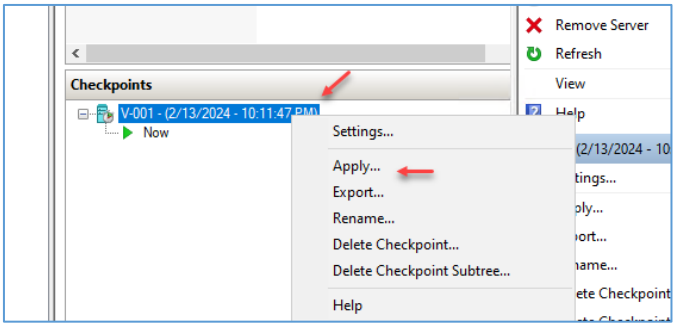
به مانند شکل ۸-۳٤۷، گزینه‌های دیگری نیز وجود دارد، گزینه‌ی Checkpoint برای ایجاد یک کپی از ماشین مورد نظر تا آن تاریخ است که اگر بعد از آن تاریخ، ماشین شما دچار مشکل شد، می‌توانید وضعیّت ماشین را به همان تاریخی برگردانید که Checkpoint را روی آن فعّال کردید، اگر توجّه کنید در وسط صفحه، وضعیّت Checkpoint 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.

www.takbook.com



شکل ۸- ۳۴۷ سرویس Hyper-V

زمانی که شما از ابزار Checkpoints استفاده می‌کنید، به مانند شکل ۸-۳٤۸، 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.

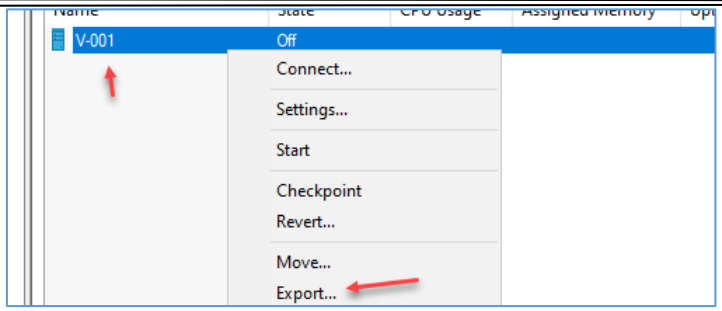


شکل ۸- ۳۴۸ سرویس Hyper-V

۳-۱٤-۳-۸ ایجاد ماشین جدید از ماشین قبلی

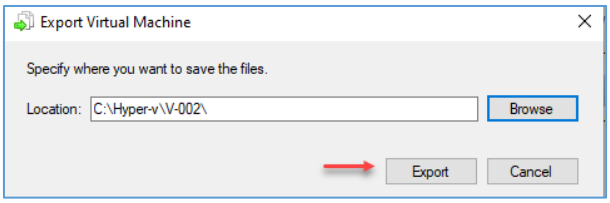
برای اینکه یک ماشین جدید ایجاد کنید دیگر نیاز نیست که دوباره همه کارها را از اول انجام دهید، فقط کافی است از ماشین قبلی یک Export تهیه کنیم و دوباره آن را به لیست اضافه کنیم، برای این کار بر به مانند شکل ۸-۳٤۹، روی ماشین مورد نظر خود کلیک راست کنید و گزینه‌ی Export را انتخاب کنید.

www.takbook.com



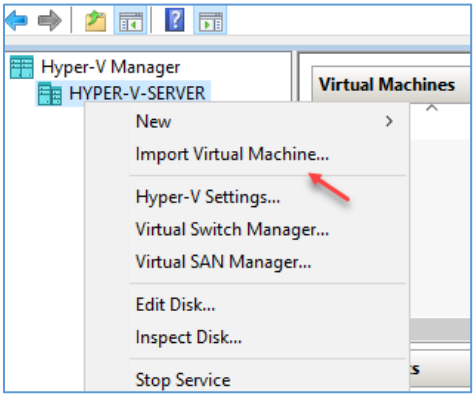
شکل ۸- ۳۴۹ سرویس Hyper-V

در شکل ۸-۳۵۰، مسیر ذخیره شدن فایل را انتخاب کنید تا تمام اطلاعات ماشین مورد نظر در جای جدید کپی شود.



شکل ۸- ۳۵۰ سرویس Hyper-V

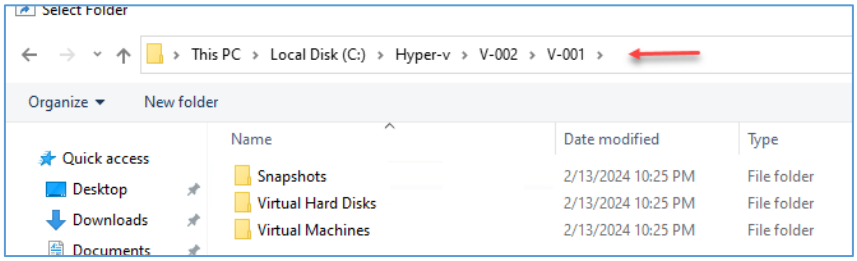
بعد از انجام Export به مانند شکل ۸-۳۵۱، روی نام سرور کلیک راست کنید و گزینه‌ی Import Virtual Machine را انتخاب کنید.



شکل ۸- ۳۵۱ سرویس Hyper-V

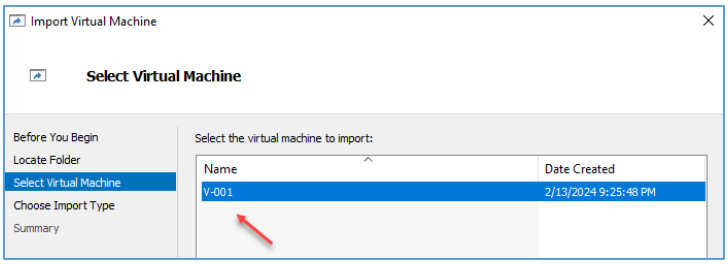
در ادامه به مانند شکل ۸-۳۵۲، آدرس جدید که ماشین مورد نظر را کپی کردید انتخاب کنید، توجه داشته باشید که این سه پوشه باید قابل مشاهده باشد.

www.takbook.com



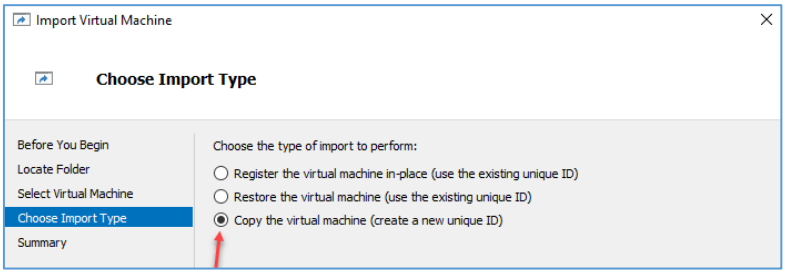
شکل ۸- ۳۵۲ سرویس Hyper-V

همان‌طور که در شکل ۸-۳۵۳، مشاهده می‌کنید نام ماشین مورد نظر در لیست موجود است و باید آن را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۳۵۳ سرویس Hyper-V

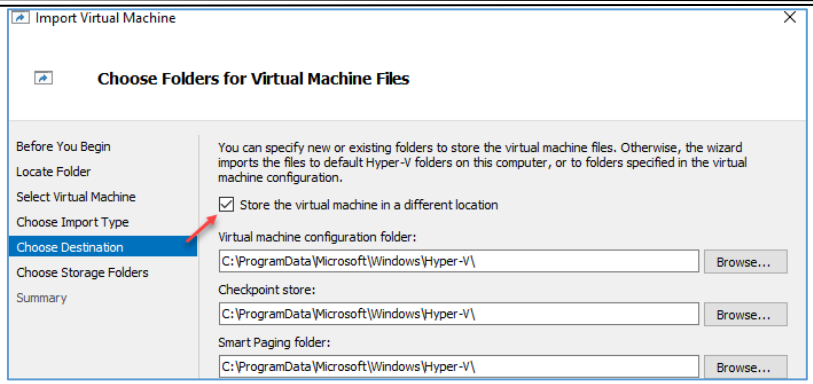
در شکل ۸-۳۵٤، سه گزینه وجود دارد اگر گزینه‌ی اول را انتخاب کنید در همان مکان اطلاعات جدید ذخیره شده و مهمتر از همه از همان Unique ID ویندوز قبلی استفاده خواهد کرد، گزینه‌ی دوم برای برگرداندن ماشین مجازی در جای جدید به همراه Unique ID همان ویندوز قبلی است و اگر گزینه‌ی سوم را انتخاب کنید می‌توانید ماشین مورد نظر را در جای جدید کپی کنید و از Unique ID جدید برای آن استفاده کنید، توجه داشته باشید که Unique ID در زمانی که می‌خواهید یک ماشین را عضو دومین کنید به کار می‌آید و اگر دو ماشین با یک Unique ID وجود داشته باشد با مشکل مواجه خواهید شد.



شکل ۸- ۳۵۴ سرویس Hyper-V

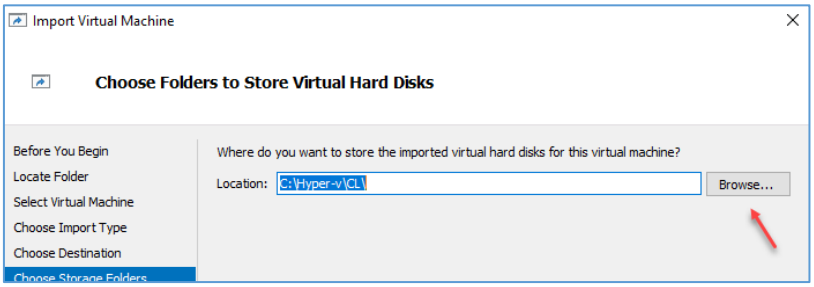
در شکل ۸-۳۵۵، می‌توانید مسیر جدید برای ذخیره شدن اطلاعات ماشین جدید را انتخاب کنید.

www.takbook.com



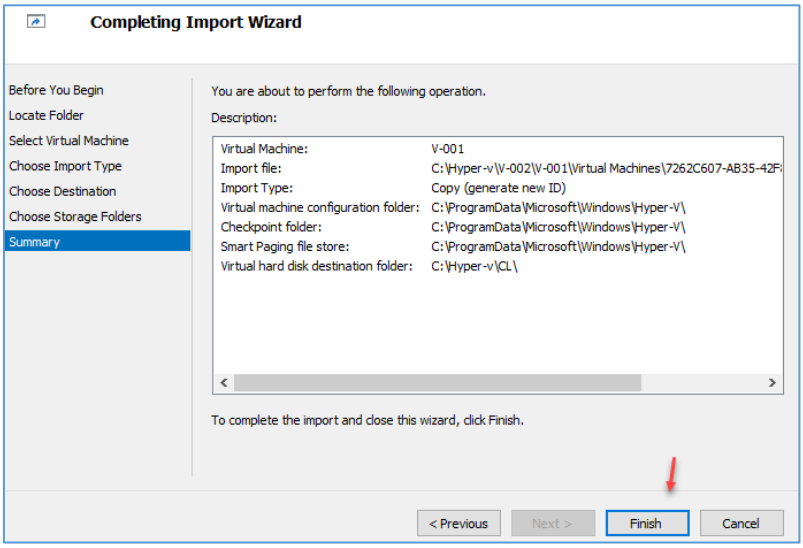
شکل ۸- ۳۵۵ سرویس Hyper-V

در شکل ۸-۳۵۶، می‌توانید محل ذخیره شدن هارد دیسک مجازی برای این ماشین را انتخاب کنید.



شکل ۸- ۳۵۶ سرویس Hyper-V

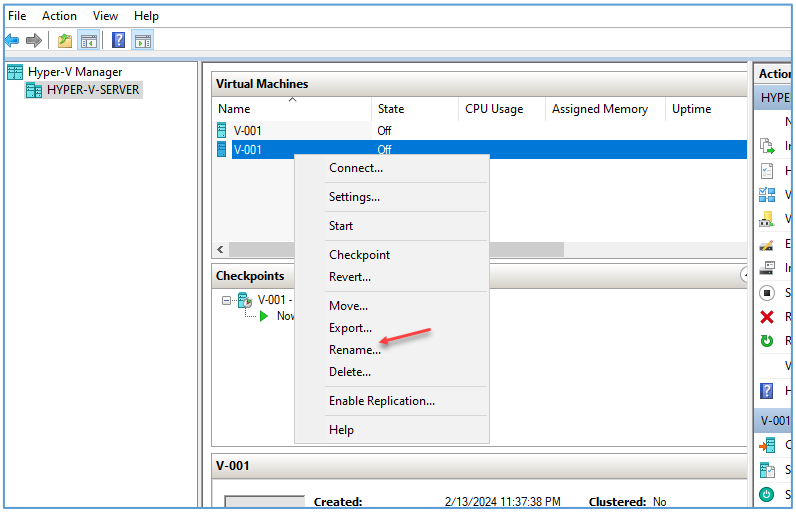
در شکل ۸-۳۵۷، اگر اطلاعات مورد تایید است بر روی Finish کلیک کنید.



شکل ۸- ۳۵۷ سرویس Hyper-V

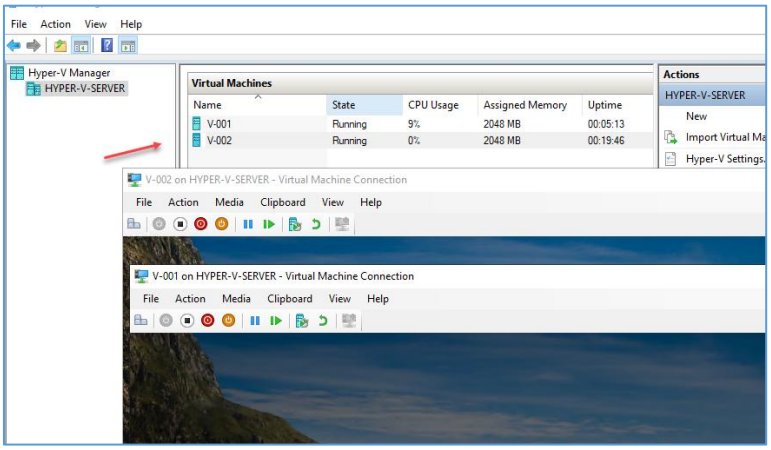
www.takbook.com

در شکل ۸-۳۵۸، ماشین مورد نظر ایجاد شده است و بر روی آن کلیک راست کنید و نام جدید خود را وارد کنید و بعد ماشین را روشن کنید.



شکل ۸- ۳۵۸ سرویس Hyper-V

همان‌طور که در شکل ۸-۳۵۹، مشاهده می‌کنید دو ماشین مجازی ایجاد و با موفقیت روشن شده است.

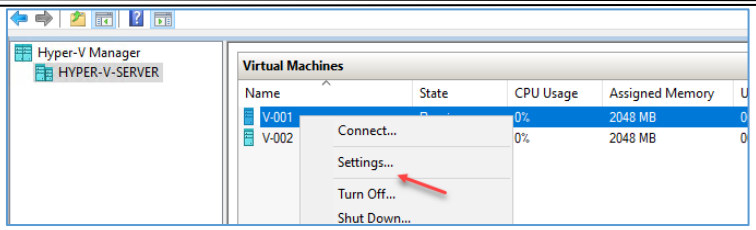


شکل ۸- ۳۵۹ سرویس Hyper-V

۸-۳-۱۴-۴ شبکه کردن ماشین مجازی

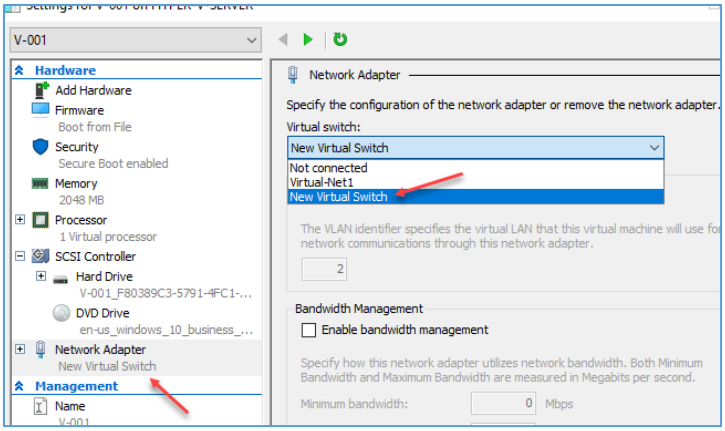
بعد از اینکه با کارت شبکه‌ی مجازی کار کردیم و نحوه‌ی ایجاد آن را بررسی کردیم می‌خواهیم دو ماشینی را که در قسمت قبلی ایجاد کردیم به هم متصل کنیم، برای این کار باید کارت شبکه‌ی داخلی را برای هر دو ویندوز در نظر می‌گیریم، به مانند شکل ۸-۳۶۰، بر روی هر دو ماشین کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید.

www.takbook.com



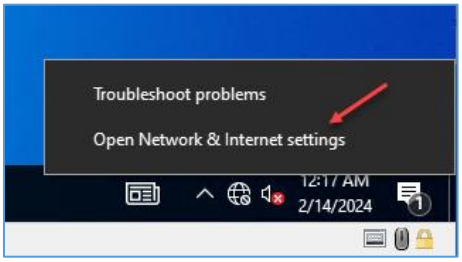
شکل ۸- ۳۶۰ شبکه کردن ماشین مجازی

به مانند شکل ۸-۳۶۱، باید کارت شبکه را انتخاب و از لیست مورد نظر کارت شبکه‌ی داخلی را که قبلاً ایجاد کردیم انتخاب کنید، دقیقاً همین کار را برای ماشین دوم هم انجام دهید.



شکل ۸- ۳۶۱ شبکه کردن ماشین مجازی

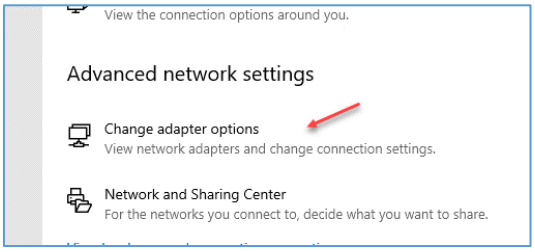
طبق شکل ۸-۳۶۲، وارد ماشین مجازی شوید و بر روی آیکون شبکه کلیک راست کنید و گزینه‌ی Open Network & internet settings را انتخاب کنید.



شکل ۸- ۳۶۲ شبکه کردن ماشین مجازی

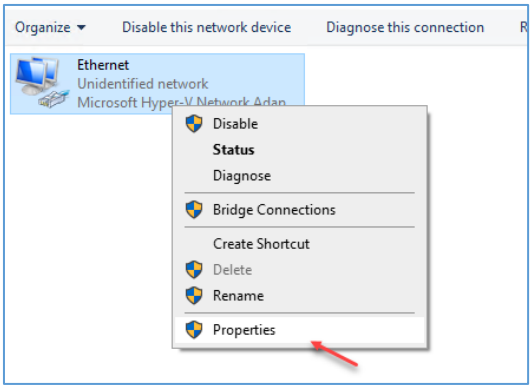
در شکل ۸-۳۶۳، گزینه‌ی Change adaptor options را انتخاب کنید.

www.takbook.com



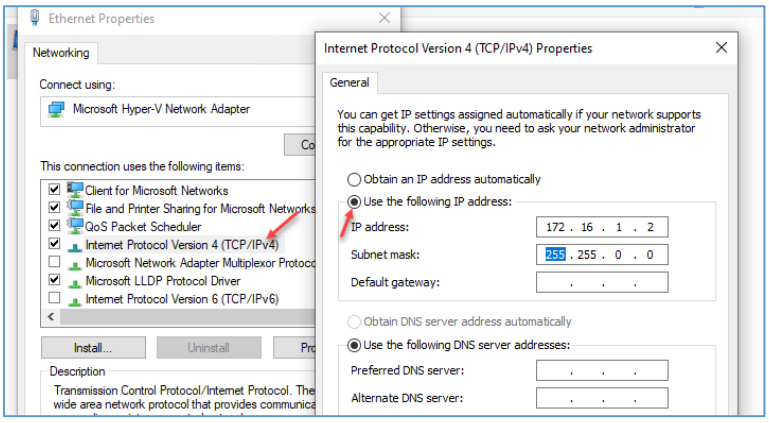
شکل ۸- ۳۶۳ شبکه کردن ماشین مجازی

به مانند شکل ۸-۳٦٤، بر روی کارت شبکه‌ی مورد نظر کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید:



شکل ۸- ۳۶۴ شبکه کردن ماشین مجازی

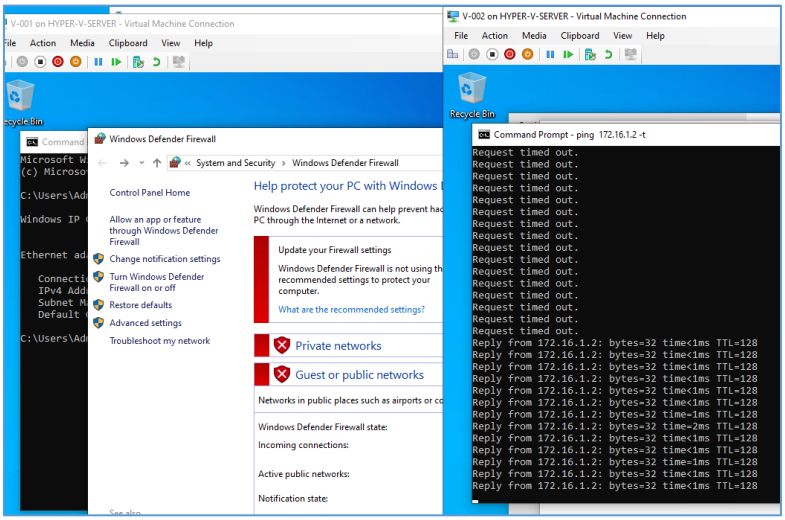
به مانند شکل ۸-۳٦٥، بر روی IPv4 دوبار کلیک کنید و آدرس 172.16.1.2 را به همراه Subnet، 255.255.0.0 وارد کنید و بر روی OK کلیک کنیدف توجه داشته باشید دقیقاً همین کار را برای ماشین دوم (V-002)انجام دهید و آدرس آن را 172.16.1.3 در نظر بگیرید.



شکل ۸- ۳۶۵ شبکه کردن ماشین مجازی

www.takbook.com

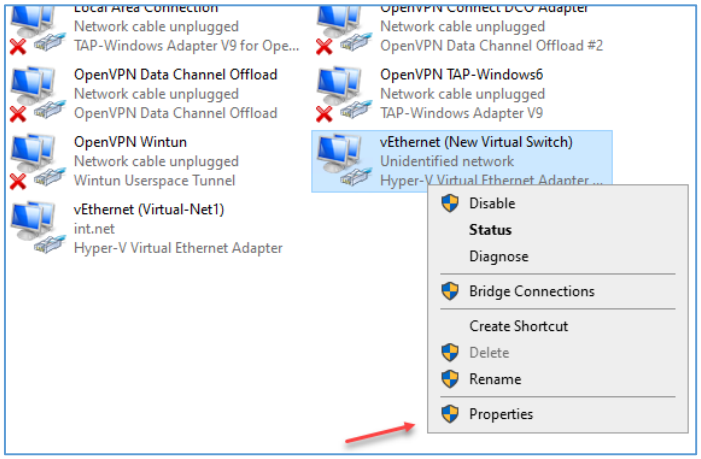
به مانند شکل ۸–۳٦٦، بعد از اینکه آدرس IP را تنظیم کردید می‌توانیم با دستور PING ارتباط را بررسی کنید اما چون فایروال روشن است ارتباط قطع خواهد بود یا باید فایروال را طبق آموزش‌های قبلی برای پروتکل ICMP تنظیم کنید و یا اینکه فایروال را خاموش کنید، همان‌طور که در شکل ۸–۳٦٦، مشاهده می‌کنید در کلاینت V-001 فایروال خاموش شده و ارتباط کلاینت V-002 با کلاینت V-001 برقرار شده است.



شکل ۸- ۳۶۶ شبکه کردن ماشین مجازی

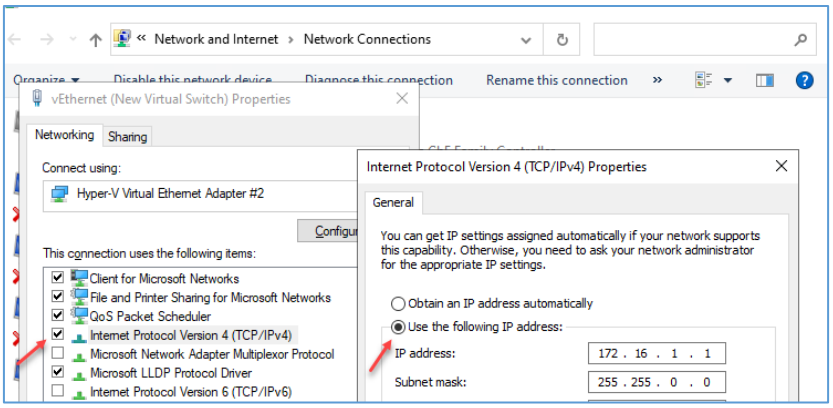
به این نکته توجه کنید که در زمان ایجاد کارت شبکه بیان کردیم که کارت شبکه بر سه نوع است که یکی External است و با کارت شبکه‌ی فیزیکی ارتباط برقرار می‌کند، اما دو کارت شبکه‌ی دیگر برای ارتباط داخلی بین ماشین‌های مجازی بود یکی Internal و دیگری Private، کارت شبکه‌ای که برای این دو ماشین فعال کردیم از نوع Internal بوده، یعنی اینکه هم می‌تواند بین ماشین مجازی ارتباط برقرار کند و هم می‌تواند با سیستم فیزیکی ارتباط شبکه داشته باشد، برای تست این موضوع به مانند شکل ۸–۳٦۷، در سیستم فیزیکی خود در قسمت Network Connection بر روی کارت شبکه‌ی Internal که نام آن New Virtual Switch کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.

www.takbook.com



شکل ۸- ۳۶۷ شبکه کردن ماشین مجازی

به مانند شکل ۸-۳۶۸، باید یک آدرس در رنج ماشین مجازی خود وارد کنید تا ارتباط با ماشین‌ها برقرار شود.

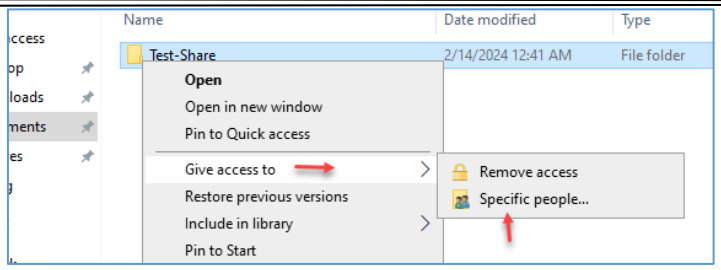


شکل ۸- ۳۶۸ شبکه کردن ماشین مجازی

مثلاً برای اینکه ارتباط بین سیستم فیزیکی و ماشین مجازی را تست بگیریم یک فایل را در سیستم فیزیکی برای ماشین مجازی Share می‌کنیم.

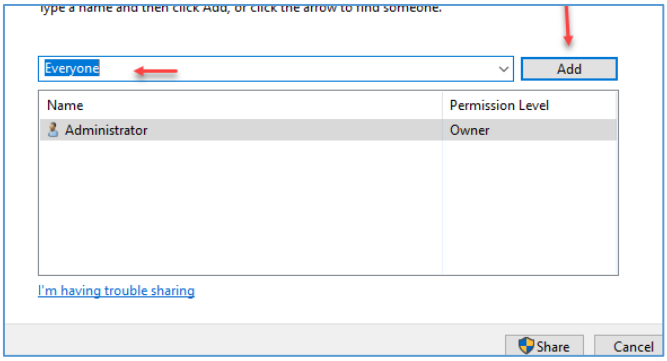
به مانند شکل ۸-۳۶۹، یک فولدر در سیستم فیزیکی ایجاد و بر روی آن کلیک راست و از قسمت Give access to گزینه‌ی Specific people را انتخاب کنید.

www.takbook.com



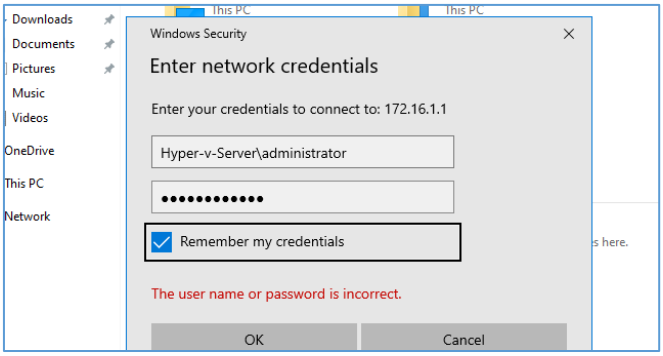
شکل ۸- ۳۶۹ شبکه کردن ماشین مجازی

در شکل ۸-۳۷۰، گروه Everyone را انتخاب و به لیست اضافه اضافه کنید و در آخر بر روی Share کلیک کنید.



شکل ۸- ۳۷۰ شبکه کردن ماشین مجازی

وارد یکی از ماشین‌های مجازی شوید و آدرس 172.16.1.1 که مربوط به سیستم فیزیکی است را وارد کنید، یعنی به صورت \\172.16.1.1 وارد کنید که شکل ۸-۳۷۱، ظاهر خواهد شد و باید نام کاربری و رمز عبور مربوط به سیستم فیزیکی خود را وارد کنید، چنانچه سیستم‌ها عضو یک دومین یا Workgroup نباشند باید حتماً قبلاً از نام کاربری، نام سیستم مورد نظر را وارد کنید.



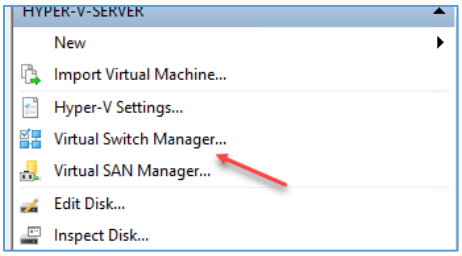
شکل ۸- ۳۷۱ شبکه کردن ماشین مجازی

www.takbook.com

۸-۳-۱۴-۵ ایجاد کارت شبکه‌ی Private

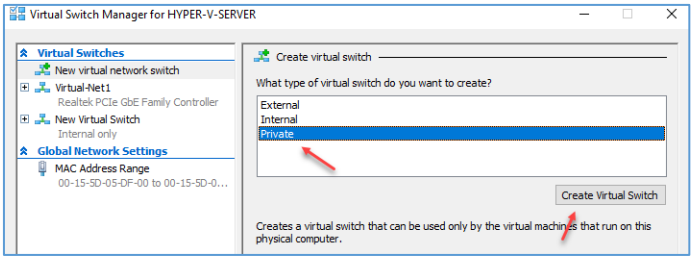
همان‌طور که در قسمت قبلی مشاهده کردید دو ماشین مجازی ایجاد کردیم که بین آنها یک کارت شبکه‌ی Internal فعال کردیم که می‌توانست با سیستم فیزیکی هم در ارتباط باشد.

اما برای اینکه یک شبکه فقط بین ماشین مجازی ارتباط برقرار کند و با جایی دیگر ارتباط نداشته باشد باید یک کارت شبکه‌ی Private ایجاد کنیم، برای این‌کار به مانند شکل ۸-۳۷۲، بر روی Virtual Switch Manager کلیک کنید.



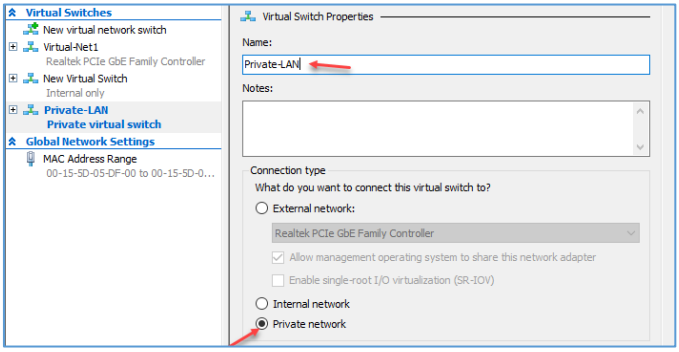
شکل ۸- ۳۷۲ ایجاد کارت شبکه‌ی Private

طبق شکل ۸-۳۷۳، گزینه‌ی Private را انتخاب و بر روی Create Virtual Switch کلیک کنید.



شکل ۸- ۳۷۳ ایجاد کارت شبکه‌ی Private

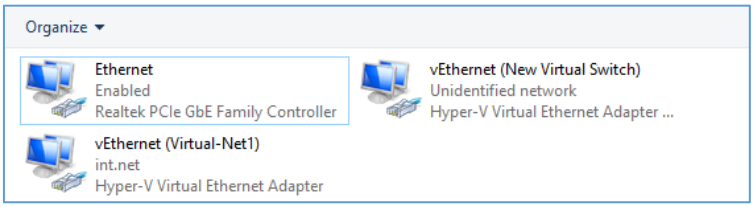
در شکل ۸-۳۷۴، نام کارت شبکه‌ی خود را وارد و کنید و بر روی OK کلیک کنید تا کارت شبکه‌ی مورد نظر ایجاد شود.



شکل ۸- ۳۷۴ ایجاد کارت شبکه‌ی Private

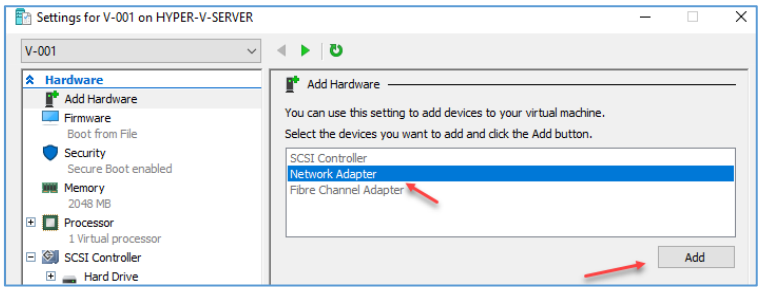
www.takbook.com

بعد از ایجاد کارت شبکه‌ی Private در سیستم فیزیکی خود وارد Network Connections شوید، همان‌طور که در شکل ۸–۳۷۵، مشاهده می‌کنید خبری از کارت شبکه‌ی Private نیست.



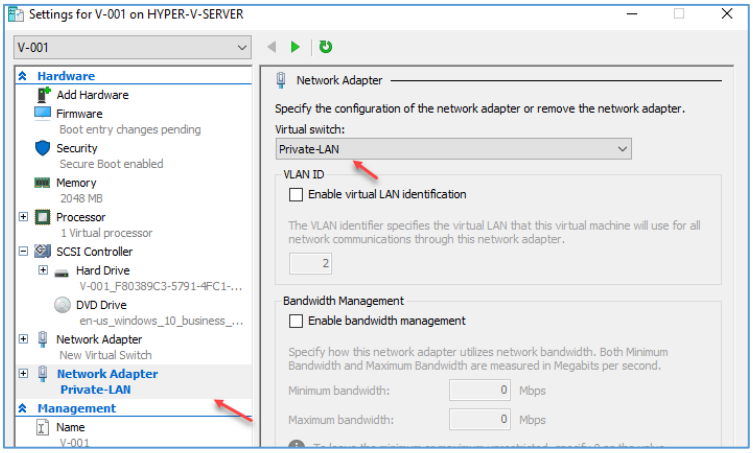
شکل ۸- ۳۷۵ ایجاد کارت شبکه‌ی *Private*

به مانند شکل ۸–۳۷۶، وارد تظیمات هر دو ماشین مجازی شوید و کارت شبکه‌ی Private را به لیست اضافه کنید، گزینه‌ی Network Adaptor را انتخاب و بر روی Add کلیک کنید.



شکل ۸- ۳۷۶ ایجاد کارت شبکه‌ی *Private*

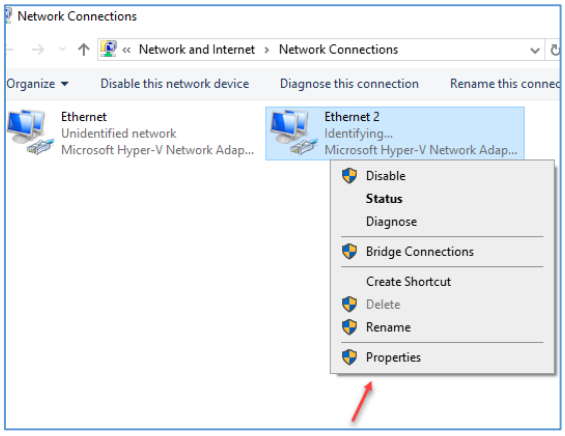
در شکل ۸–۳۷۷، کارت شبکه‌ی مورد نظر را انتخاب کنید و بر روی Ok کلیک کنید، دقیقاً همین کار را برای ماشین دوم هم انجام دهید.



شکل ۸- ۳۷۷ ایجاد کارت شبکه‌ی *Private*

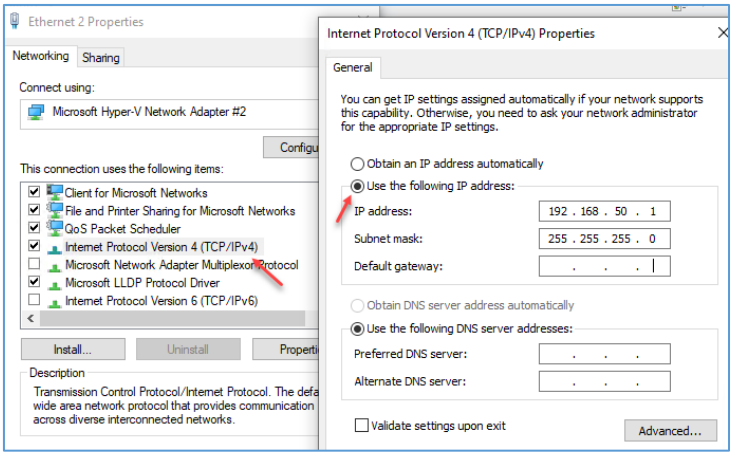
www.takbook.com

اگر وارد لیست کارت شبکه‌ها در ماشین مجازی شوید به مانند شکل ۸–۳۷۸، دو کارت شبکه را مشاهده می‌کنید، یکی که همان کارت شبکه‌ی Internal است و دیگری کارت شبکه‌ی Private است که بر روی آن کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۳۷۸ ایجاد کارت شبکه‌ی Private

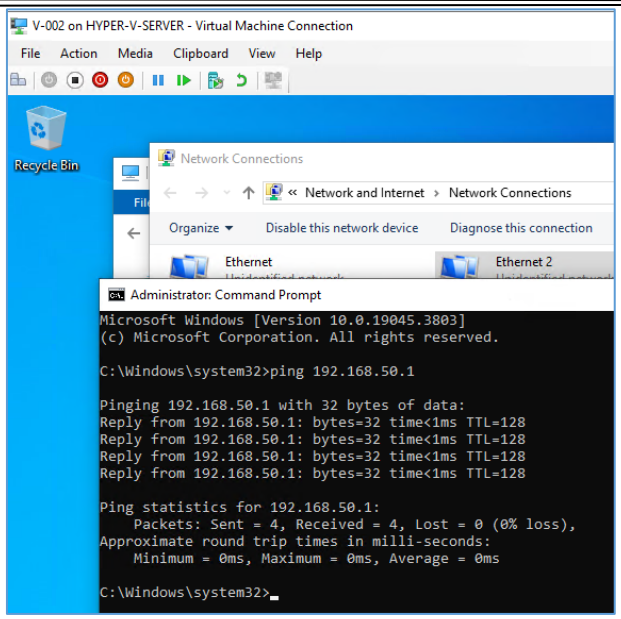
به مانند شکل ۸–۳۷۹، آدرس 192.168.50.1 را برای این ماشین مجازی در نظر بگیرید و برای ماشین دوم هم آدرس 192.168.50.2 را تخصیص دهید.



شکل ۸- ۳۷۹ ایجاد کارت شبکه‌ی Private

همان‌طور که در شکل ۸–۳۸۰، مشاهده می‌کنید ارتباط دو ماشین مجازی با استفاده از کارت شبکه‌ی Private برقرار شده است.

www.takbook.com

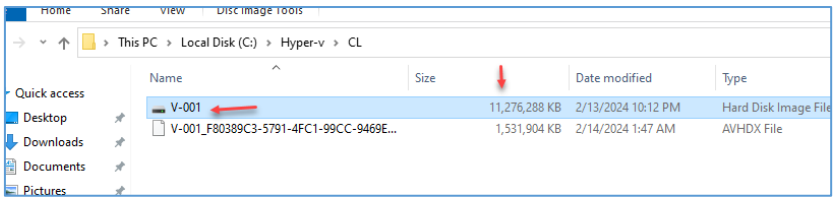


شکل ۸- ۳۸۰ ایجاد کارت شبکه‌ی Private

۸-۳-۱۴-۶ کار با هاردهای مجازی VHDX

زمانی که یک ماشین مجازی ایجاد می‌کنیم به همراه آن یک هارد دیسک مجازی با پسوند VHDX ایجاد می‌شود که پسوند VHDX تا ۶۴ ترابایت را پشتیبانی می‌کند، البته قبلاً پسوند VHD استفاده می‌شد که به نسبت پسوند جدید VHDX ضعیف‌تر بود.

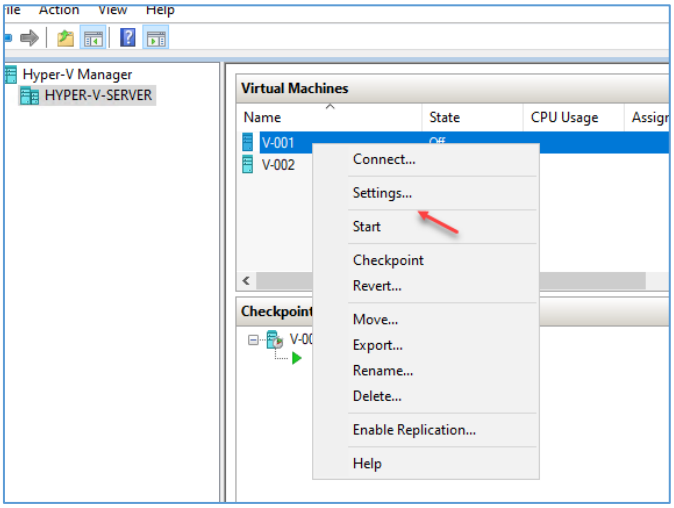
اگر وارد مسیری که ماشین مجازی ایجاد کردید شوید، منظور مسیری است که هارد مجازی را کپی کردید، به مانند شکل ۸-۳۸۱، یک هارد مجازی از نوع VHDX وجود دارد که دارای حجم تقریبی ۱۱ گیگ است.



شکل ۸- ۳۸۱ هاردهای مجازی VHDX

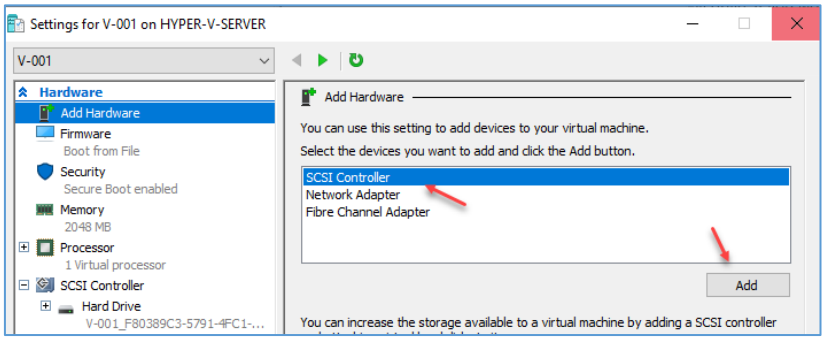
برای اینکه نحوه‌ی ایجاد یک هارد دیسک مجازی را یاد بگیریم به مانند شکل ۸-۳۸۲، بر روی یکی از ماشین‌های مجازی کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید، در ضمن ماشین مورد نظر باید خاموش باشد.

www.takbook.com



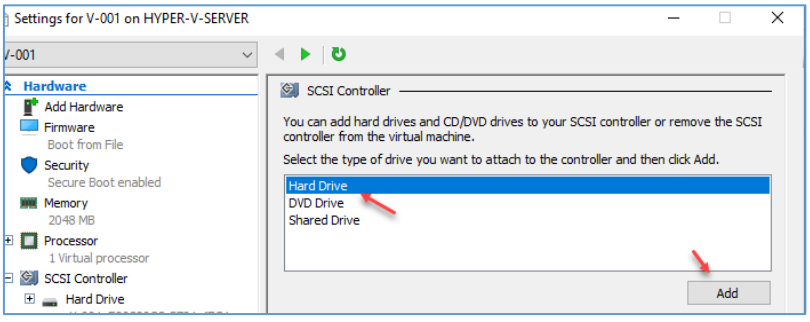
شکل ۸- ۳۸۲ هاردهای مجازی VHDX

در شکل ۸-۳۸۳، گزینه‌ی SCSI Controller را انتخاب و بر روی Add کلیک کنید.



شکل ۸- ۳۸۳ هاردهای مجازی VHDX

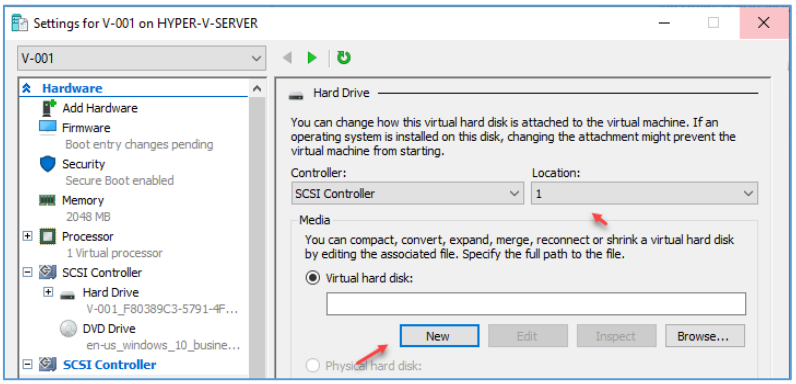
در شکل ۸-۳۸٤، گزینه‌ی Hard Drive را انتخاب کنید.



شکل ۸- ۳۸۴ هاردهای مجازی VHDX

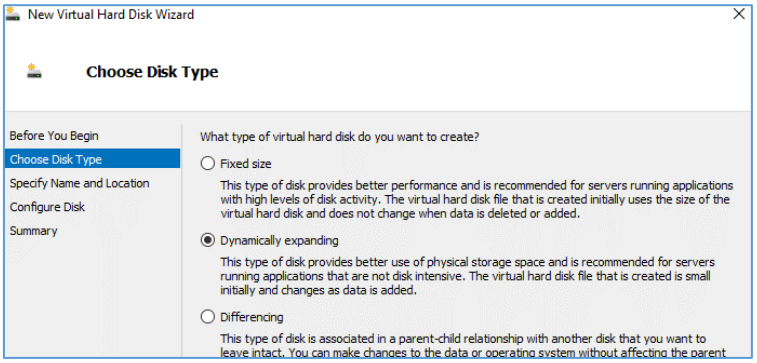
www.takbook.com

در شکل ۸–۳۸۵، در قسمت Location باید عددی را انتخاب کنید که کلمه‌ی In use نداشته باشد، در قسمت Virtual hard disk بر روی New کلیک کنید.



شکل ۸- ۳۸۵ هاردهای مجازی VHDX

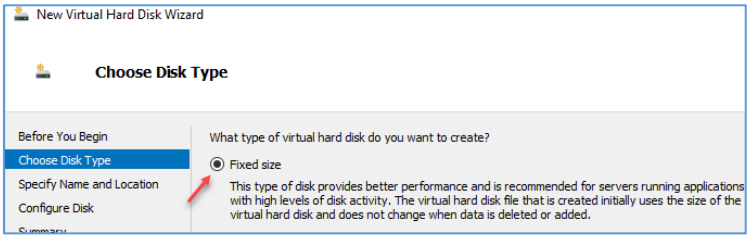
در شکل ۸–۳۸۶، باید یکی از این سه مورد را انتخاب کنیم، اگر گزینه‌ی اول را انتخاب کنید، Fixed Size تمام حجمی که برای یک هارد مجازی در نظر گرفتید برای آن تخصیص داده خواهد شد، یعنی اگر یک هارد را ۱۰ گیگ در نظر بگیرید یک هارد مجازی با حجم ۱۰ گیگ ایجاد خواهد شد، اگر گزینه‌ی دوم (Dynamically) را انتخاب کنید، مقدار فضایی که اشغال می‌شود با توجه به اطلاعاتی است که در آن قرار می‌گیرد، مثلاً یک هارد دیسک ۱۰ گیگابایتی ایجاد می‌کنید ولی در داخل آن یک فایل ۲ گیگاباتی وارد می‌کنید، اگر حجم هارد دیسک را نگاه کنید متوجه خواهید شد که ۲ گیگ فضا اشغال کرده است، در آخر اگر گزینه‌ی سوم (Differencing) را انتخاب کنید یک هارد به عنوان هارد اصلی انتخاب می‌شود و دیگر هاردهایی که ایجاد می‌کنید از این هارد استفاده خواهد کرد.



شکل ۸- ۳۸۶ هاردهای مجازی VHDX

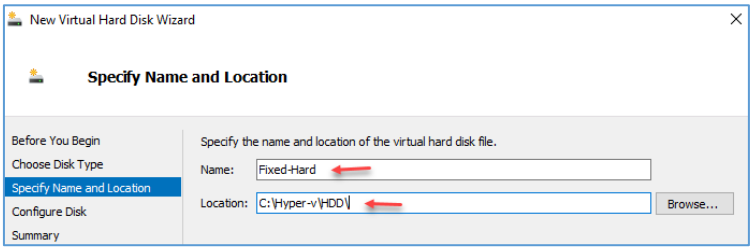
برای شروع گزینه‌ی اول یعنی Fixed را انتخاب می‌کنیم که این موضوع را در شکل ۸–۳۸۷، مشاهده می‌کنید.

www.takbook.com



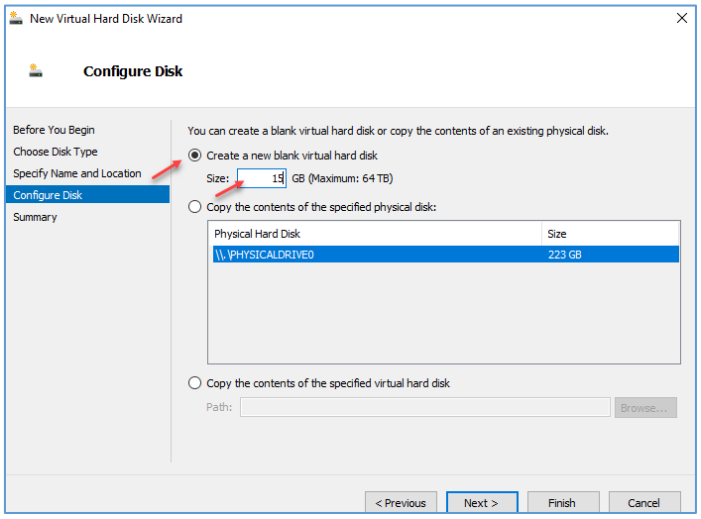
شکل ۸- ۳۸۷ هاردهای مجازی VHDX

در شکل ۸-۳۸۸، باید نام و مسیر هارد دیسک را وارد کنید.



شکل ۸- ۳۸۸ هاردهای مجازی VHDX

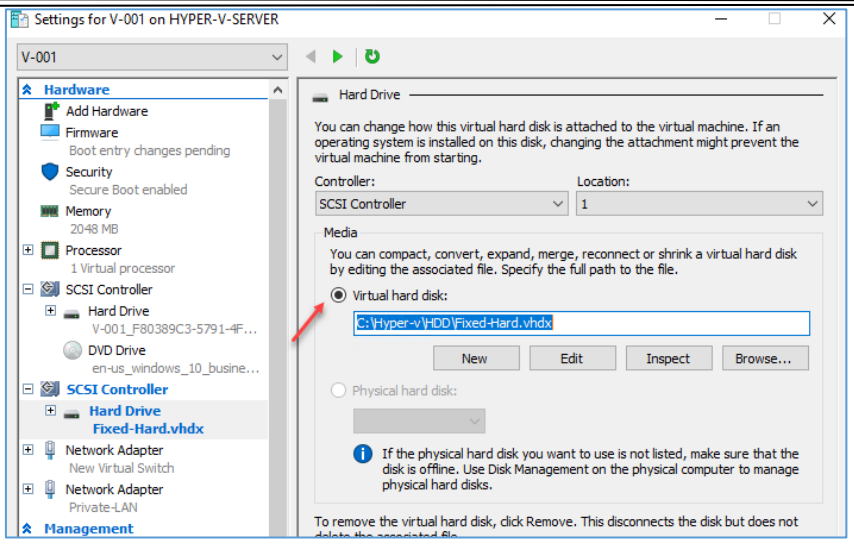
در شکل ۸-۳۸۹، باید مقدار حجم هارد دیسک مجازی را وارد کنید، البته می‌توانید هارد فیزیکی را برای ماشین مجازی در نظر بگیرید و یا اینکه در گزینه‌ی آخر اگر قبلاً هارد مجازی ایجاد کردید می‌توانید به این ماشین مجازی اختصاص دهید.



شکل ۸- ۳۸۹ هاردهای مجازی VHDX

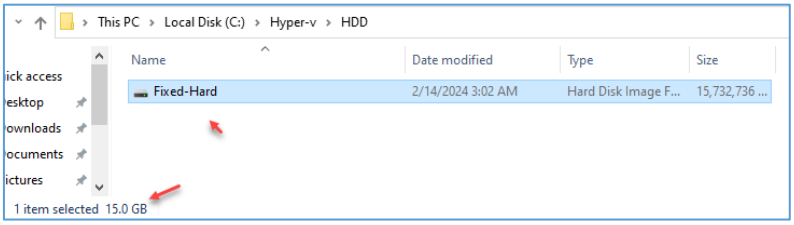
به مانند شکل ۸-۳۹۰، بعد از ایجاد هارد دیسک بر روی ok کلیک کنید تا هارد به ماشین مورد نظر اضافه شود.

www.takbook.com



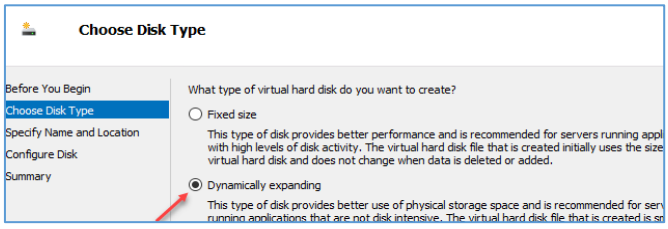
شکل ۸- ۳۹۰ هاردهای مجازی VHDX

بعد از ایجاد هارد دیسک اگر وارد مسیری که هارد را قرار دادید شوید طبق شکل ۸-۳۹۱، مشاهده خواهید کرد که مقدار فضایی که برای آن در نظر گرفته شده است دقیقاً ۱۵ گیگ است و کل فضا را اشغال کرده است و این مورد از نظر Performance بهینه نخواهد بود.



شکل ۸- ۳۹۱ هاردهای مجازی VHDX

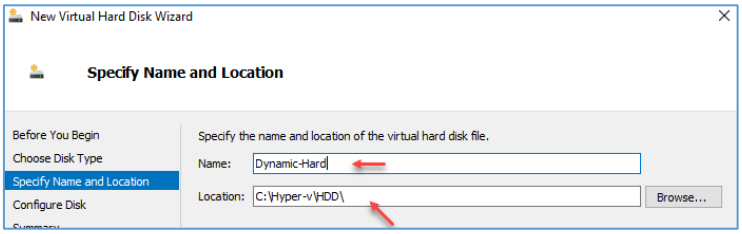
اما برای اینکه یک هارد با Performance خوب ایجاد کنیم باید گزینه‌ی Dynamic را به مانند شکل ۸-۳۹۲، انتخاب کنید.



شکل ۸- ۳۹۲ هاردهای مجازی VHDX

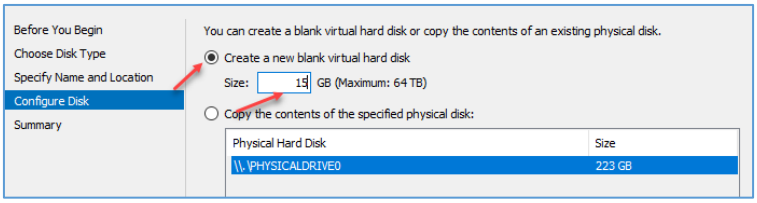
طبق شکل ۸-۳۹۳، نام و مسیر ذخیره‌سازی هارد را مشخص می‌کنیم:

www.takbook.com



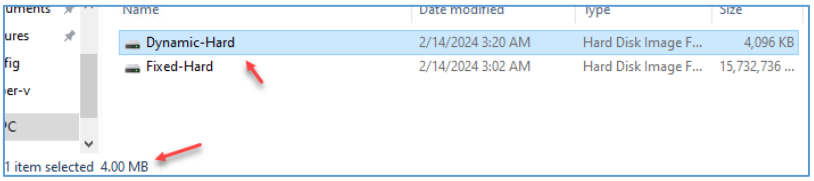
شکل ۸- ۳۹۳ هاردهای مجازی VHDX

به مانند شکل ۸-۳۹٤، برای این هارد دیسک هم ۱۵ گیگ فضا در نظر می‌گیریم تا تفاوت آن را با هارد Fixed مشاهده کنیم.



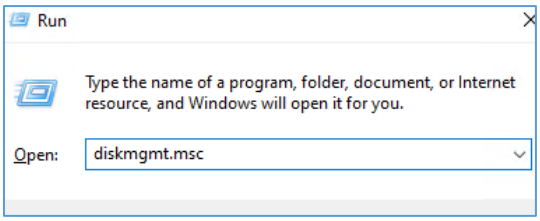
شکل ۸- ۳۹۴ هاردهای مجازی VHDX

بعد از ایجاد هارد مورد نظر اگر به مانند شکل ۸-۳۹۵، وارد مسیری که هارد قرار دارد شوید مشاهده خواهید کرد که بعد از ایجاد هارد مورد نظر اگر وارد مسیری که هارد قرار دارد شوید مشاهده خواهید کرد که مقدار فضای ٤ مگابایت فقط برای آن در نظر گرفته شده است و دیگر خبری از ۱۵ گیگ نیست و هر چقدر اطلاعات در آن کپی کنید به نسبت حجم آن اطلاعات مقدار فضای آن هم تغییر خواهد کرد.



شکل ۸- ۳۹۵ هاردهای مجازی VHDX

حالا اگر ماشین مجازی را روشن کنیم این دو هارد را می‌توانیم از طریق سرویس Disk Management مشاهده کنیم، برای اجرای سرویس مورد نظر طبق شکل ۸-۳۹٦، در Run دستور Diskmgmt.msc را اجرا کنید.



شکل ۸- ۳۹۶ هاردهای مجازی VHDX

www.takbook.com

همان‌طور که در شکل ۸-۳۹۷، مشاهده می‌کنید دو هارد دیسک انتخاب شده است و با کلیک بر روی OK هر دو هارد را فعال کنید، در مورد MBR و GPT باید گفتن که نوع پارتیشن‌بندی را مشخص می‌کنند که در نوع GPT می‌توانید پارتیشن بالای ۲ ترابایت ایجاد کنید.

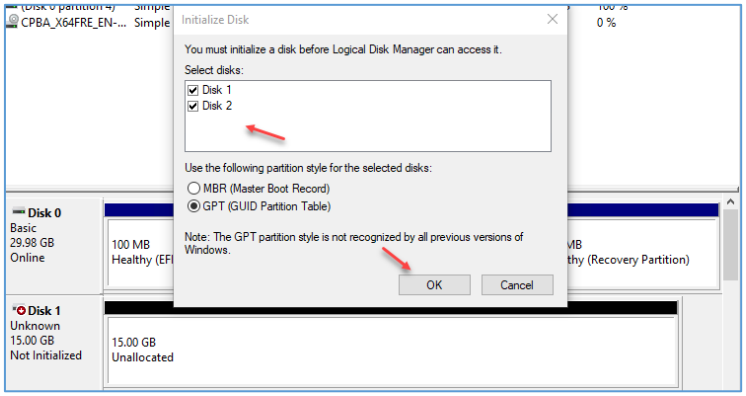
اگر بخواهیم در مورد نوع MBR و GPT توضیح دهیم می‌توانیم بگوییم:

MBR (Master Boot Record):

یک ساختار قدیمی برای پارتیشن‌بندی دیسک است که حداکثر از ۲ ترابایت فضای دیسک و ٤ پارتیشن اصلی پشتیبانی می‌کند. در دیسک‌های MBR، اطلاعات پارتیشن و بوت‌لودر در اولین سکتور ذخیره می‌شود. برای سیستم‌ها و دیسک‌های قدیمی مناسب است.

GPT (GUID Partition Table):

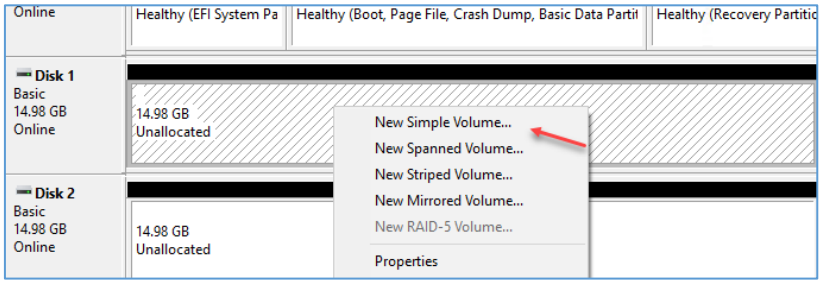
یک ساختار مدرن برای پارتیشن‌بندی دیسک است که از دیسک‌های بزرگ‌تر از ۲ ترابایت و تعداد پارتیشن‌های بیشتر (۱۲۸ در ویندوز) پشتیبانی می‌کند. GPT بخشی از استاندارد UEFI بوده و اطلاعات پارتیشن را به صورت پیشرفته‌تر و با نسخه پشتیبان ذخیره می‌کند. مناسب برای سیستم‌های جدید و دیسک‌های حجیم است.



شکل ۸- ۳۹۷ هاردهای مجازی VHDX

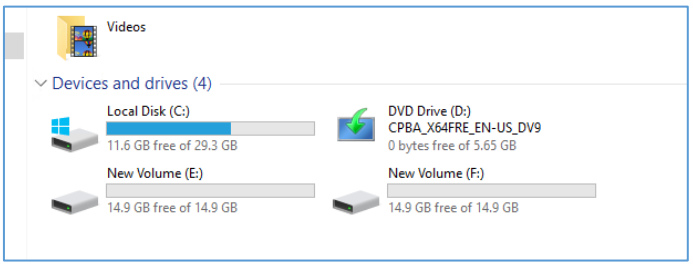
به مانند شکل ۸-۳۹۸، بر روی هر دو هارد کلیک راست کنید و گزینه‌ی New Simple Volume را انتخاب کنید و بر روی Next کلیک کنید تا پارتیشن فعال شود، توجه داشته باشید در مورد هارد دیسک و سرویس‌های آن در ادامه صحبت خواهیم کرد.

www.takbook.com



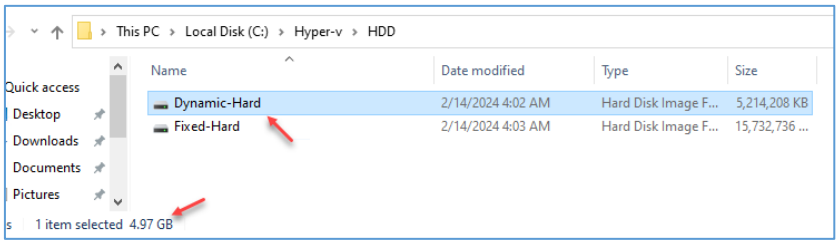
شکل ۸- ۳۹۸ هاردهای مجازی VHDX

همان‌طور که در شکل ۸-۳۹۹، مشاهده می کنید دو هارد دیسک ایجاد شده و حجم هر دو هارد برابر است، حالا می‌خواهیم در هارد دیسک Dynamic اطلاعات بریزیم و ببینیم حجم آن در سیستم فیزیکی چه تغییری می‌کند.



شکل ۸- ۳۹۹ هاردهای مجازی VHDX

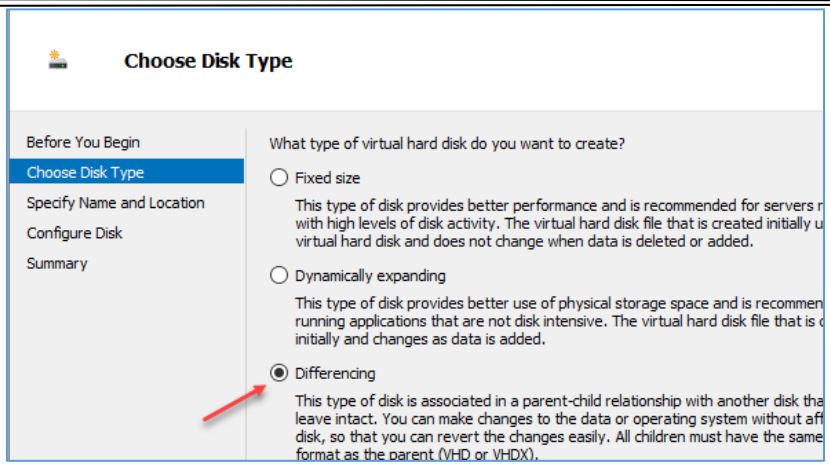
یک فایل 4.75 گیگ در هر دو هارد کپی کردیم و حالا اگر به مانند شکل ۸-۴۰۰، وارد سیستم فیزیکی شوید و مسیر هارد را بررسی کنید متوجه می‌شوید که حجم هارد Fixed تغییری نکرده ولی حجم هارد Dynamic از ٤ مگابایت به 4.97 گیگ تغییر کرده واین همان موضوعی است که تفاوت این دو هارد را بیان می‌کند.



شکل ۸- ۴۰۰ هاردهای مجازی VHDX

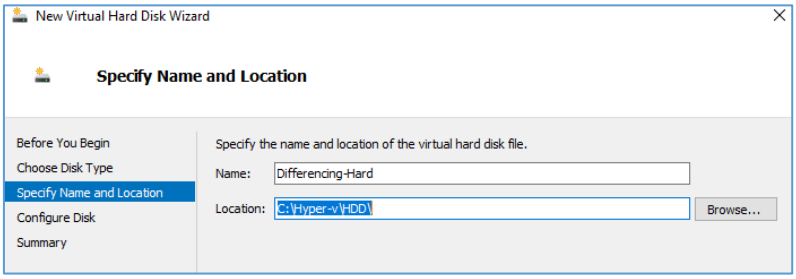
گزینه‌ی دیگر از نوع هارد وجود داشت با نام Differencing که به مانند شکل ۸-٤۰۱، انتخاب کنید.

www.takbook.com



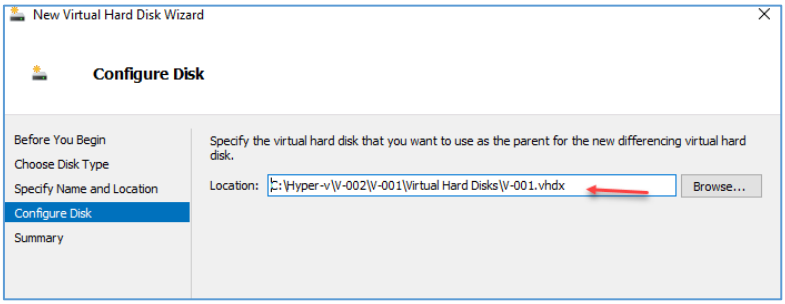
شکل ۸- ۴۰۱ هاردهای مجازی VHDX

در شکل ۸-۴۰۲، نام و مسیر هارد دیسک را مشخص کنید.



شکل ۸- ۴۰۲ هاردهای مجازی VHDX

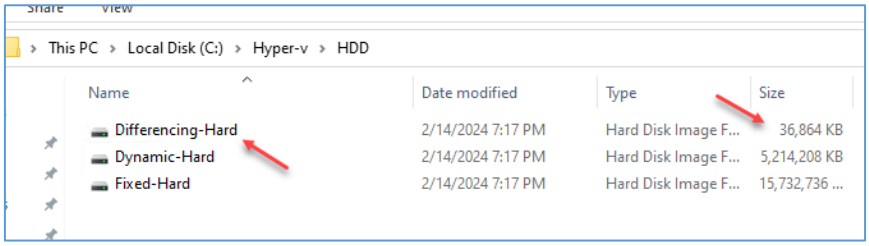
در شکل ۸-۴۰۳، باید یک هارد اصلی را که قبلاً ایجاد کردید به آن معرفی کنید، این هارد مربوط به ماشین مجازی ما هستش که بر روی آن ویندوز ۱۰ نصب شده است و هارد Differencing از این منبع استفاده خواهد کرد.



شکل ۸- ۴۰۳ هاردهای مجازی VHDX

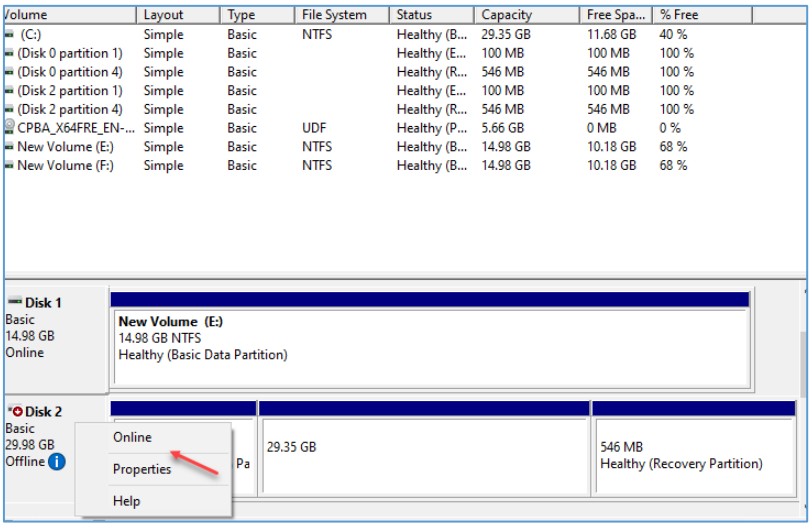
www.takbook.com

بعد از ایجاد هارد مورد نظر اگر وارد مسیری در سیستم فیزیکی خود شوید که هارد وجود دارد به مانند شکل ۸-۴۰۴، مشاهده خواهید کرد که هارد Differencing ایجاد شده اما حجم خاصی ندارد و فقط به هارد منبعی که به آن معرفی کردیم لینک شده است.



شکل ۸- ۴۰۴ هاردهای مجازی VHDX

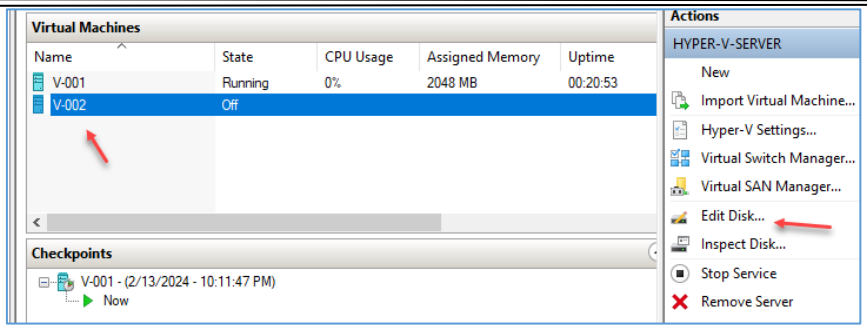
حالا اگر ماشین مجازی را روشن کنیم و سرویس Disk Management را بررسی کنیم، اگر به مانند شکل ۸-۴۰۵، به لیست توجه کنید هارد مورد نظر به لیست اضافه شده است و اگر به اطلاعات آن توجه کنید، دقیقاً اطلاعات هارد دیسک ماشین مجازی در آن قرار دارد، یعنی این هارد فقط به هارد اصلی لینک شده است، توجه داشته باشید با استفاده از این هارد می‌توانید خیلی سریع ماشین‌های مجازی مختلف ایجاد کنید و دیگر نیازی به نصب سیستم عامل نیست.



شکل ۸- ۴۰۵ هاردهای مجازی VHDX

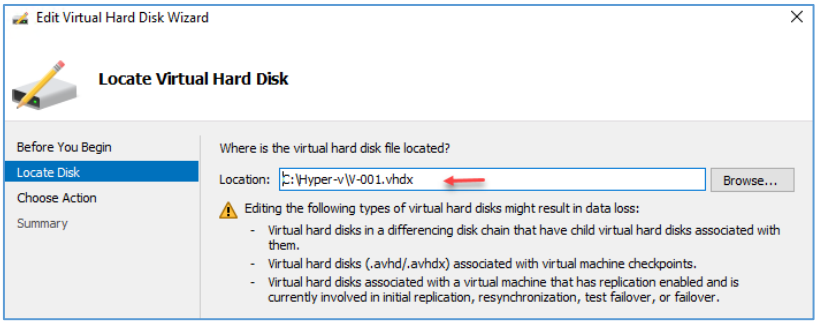
گزینه‌ی دیگری که در مورد هاردها وجود دارد این است که هارد ماشین مجازی را می‌توانید ویرایش کنید یعنی می‌توانید حجم آن را کاهش دهید و یا در صورت نیاز زیاد کنید، برای انجام این کار به مانند شکل ۸-۴۰۶، ماشین مجازی خود را انتخاب کنید و بر روی Edit Disk کلیک کنید.

www.takbook.com



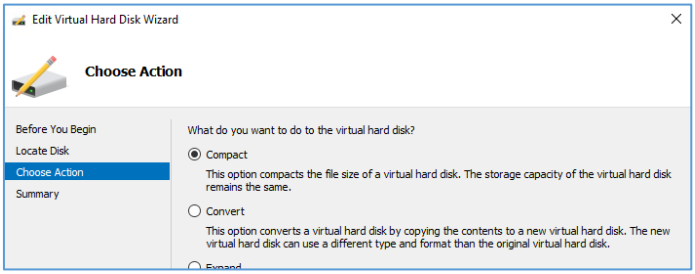
شکل ۸- ۴۰۶ هاردهای مجازی VHDX

به مانند شکل ۸–۴۰۷، یک هارد دیسک را انتخاب کنید، توجه داشته باشید که دیسک مورد نظر توسط ماشین مجازی در حال استفاده نباشد.



شکل ۸- ۴۰۷ هاردهای مجازی VHDX

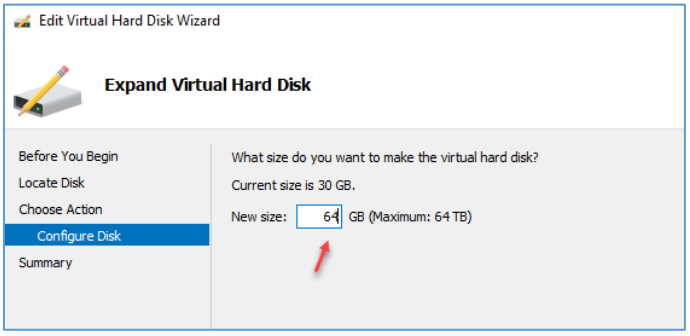
در شکل ۸–۴۰۸، سه گزینه را مشاهده می‌کنید که گزینه‌ی Compact برای فشرده‌سازی هارد مجازی به کار می‌رود، یعنی اینکه مقدار حجم هارد دیسک مجازی را بر روی هارد فیزیکی کاهش می‌دهد، گزینه‌ی Convert برای تبدیل هارد از نوع VHDX به VHD یا بلعکس است که نوع VHD قدیمی بوده و فقط پارتیشن‌های تا حجم ۲ ترابایت را قبول می‌کند، توجه داشته باشید که نوع VHDX از ویندوز ۲۰۱۲ به بعد ارائه شده است، گزینه‌ی سوم یعنی Expand برای افزایش حجم هارد دیسک استفاده می‌شود.



شکل ۸- ۴۰۸ هاردهای مجازی VHDX

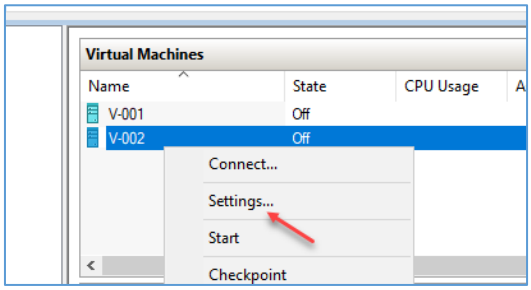
www.takbook.com

مثلاً برای اینکه حجم یک هارد دیسک را افزایش دهیم گزینه‌ی Expand را انتخاب کنید و به مانند شکل ۸-۴۰۹، مقدار فضای هارد را تغییر دهید، در مثال زیر حجم ۳۰ گیگ به ٦٤ گیگ تغییر کرده است.



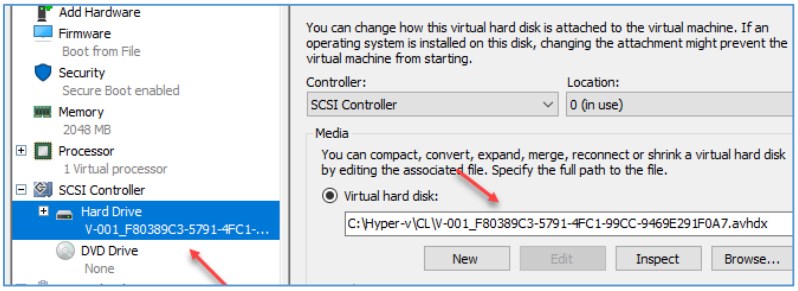
شکل ۸- ۴۰۹ هاردهای مجازی VHDX

حالا اگر بخواهیم هارد دیسک مربوط به ماشین مجازی را افزایش دهیم باید به صورت شکل ۸-۴۱۰، عمل کنید، بر روی ماشین مجازی کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید.



شکل ۸- ۴۱۰ هاردهای مجازی VHDX

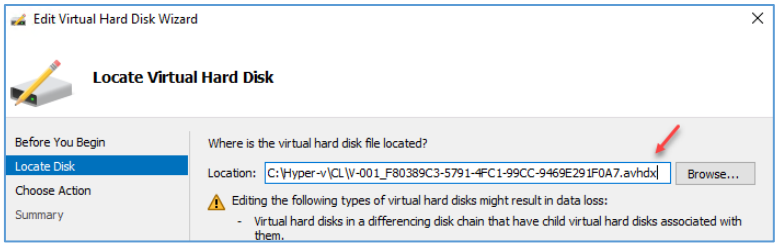
به مانند شکل ۸-۴۱۱، اگر هارد دیسک را انتخاب کنید مسیر ذخیره شدن آن را مشاهده می‌کنید، شما باید آدرس هارد را به خاطر داشته باشید و در مرحله‌ی Expand آن را معرفی کنید تا بتوانید حجم آن را افزایش دهید، اما در تصویر ۸-۴۱۱، پسوند هارد دیسک از نوع AVHDX است که این نوع فایل به این دلیل ایجاد می‌شود که از قابلیت checkpoint بر روی ماشین مجازی استفاده کرده باشید.



شکل ۸- ۴۱۱ هاردهای مجازی VHDX

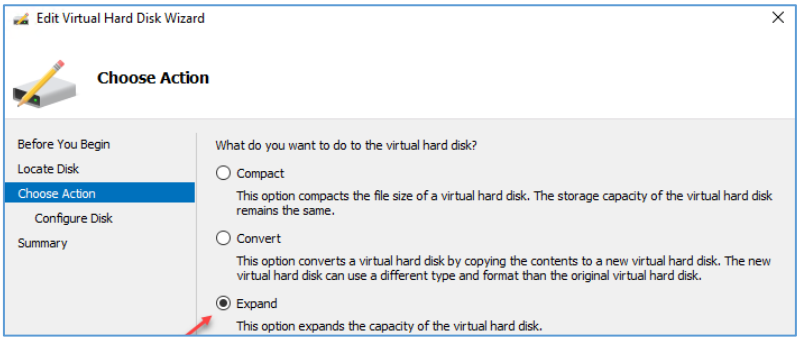
www.takbook.com

به مانند شکل ۸-۴۱۲، آدرس هارد دیسک را وارد و بر روی Next کلیک کنید.



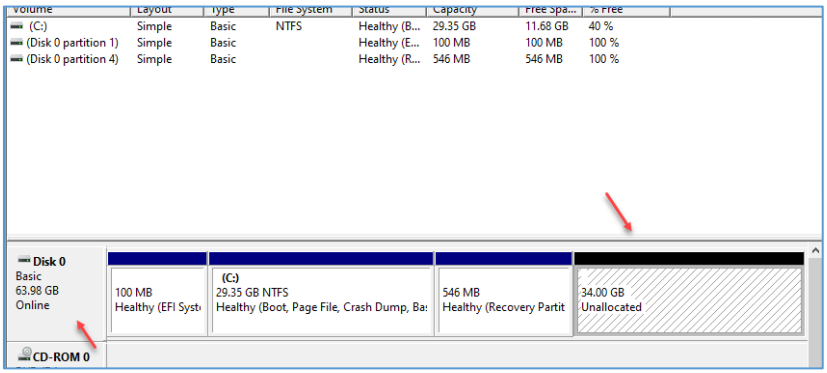
شکل ۸- ۴۱۲ هاردهای مجازی VHDX

اگر به تصویر ۸-۴۱۳، دقت کنید، دو گزینه‌ی دیگر یعنی Merge و Shrink ظاهر شده است و آن هم به دلیل این است که هارد دیسک ما از نوع Checkpoint است، گزینه‌ی Expand را انتخاب کنید و مقدار فضای هارد دیسک را به ٦٤ گیگ تغییر دهید.



شکل ۸- ۴۱۳

بعد از تغییر مقدار به مانند شکل ۸-٤١٤، وارد ماشین مجازی شوید و سرویس Disk Managemnt را باز کنید، همان‌طور که مشاهده می‌کنید، حجم جدید به هارد دیسک اضافه شده است و می‌توانید از آن استفاده کنید.

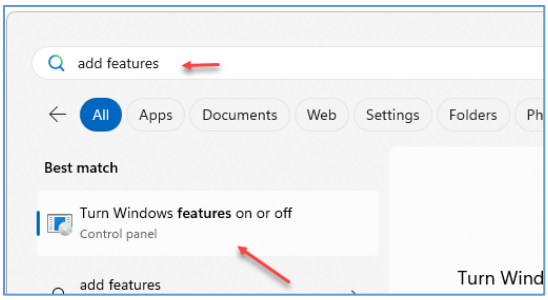


شکل ۸- ۴۱۴ هاردهای مجازی VHDX

www.takbook.com

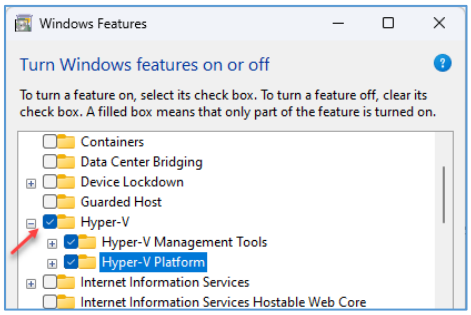
۷-۱۴-۳-۸ فعال‌سازی Hyper-v در ویندوز ۱۱

شما می‌توانید به راحتی سرویس Hyper-V را در ویندوز ۱۱ فعال کنید، برای این کار وارد start شوید و Trun windows features on or off را انتخاب کنید.



شکل ۸- ۴۱۵ Hyper-v در ویندوز ۱۱

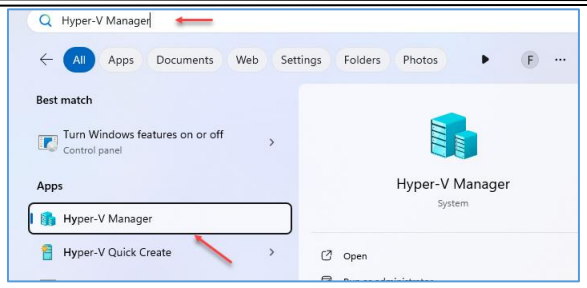
در شکل ۸-۴۱۶، تیک گزینه‌ی Hyper-v را انتخاب کنید که دو زیر مجموعه دارد، اگر می‌خواهید از طریق ویندوز ۱۱ به یک سرور Hyper-V دیگر متصل شوید فقط کافی است تیک گزینه‌ی Hyper-v Managemnt Tools را انتخاب کنید ولی اگر می‌خواهید ویندوز ۱۱ به عنوان یک سرور Hyper-V عمل کند باید تیک گزینه‌ی Hyper-v Platform را انتخاب و بر روی OK کلیک کنید.



شکل ۸- ۴۱۶ Hyper-v در ویندوز ۱۱

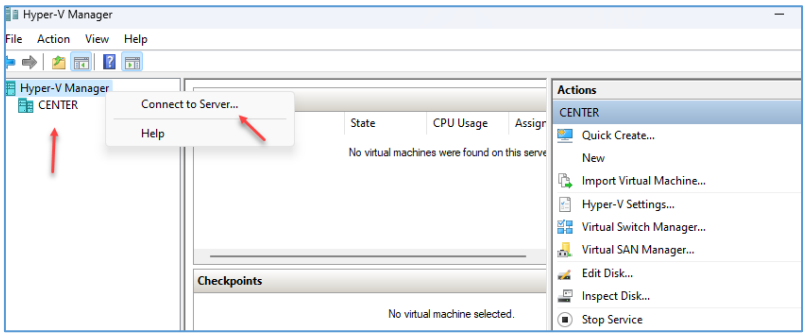
بعد از نصب Features مورد نظر وارد جستجو شوید و Hyper-v Manager را به مانند شکل ۸-۴۱۷، اجرا کنید.

www.takbook.com



شکل ۸- ۴۱۷ Hyper-v در ویندوز ۱۱

همان‌طور که در شکل ۸–٤۱۸، مشاهده می‌کنید، سرویس Hyper-v اجرا شده و می‌توانید دقیقاً همان کارهایی که در ویندوز سرور انجام می‌دادید در این قسمت هم انجام دهید، توجه داشته باشید که برای متصل شدن به یک سرور Hyper-v دیگر باید به مانند شکل ۸–٤۱۸، گزینه‌ی Connect to Server را انتخاب کنید.



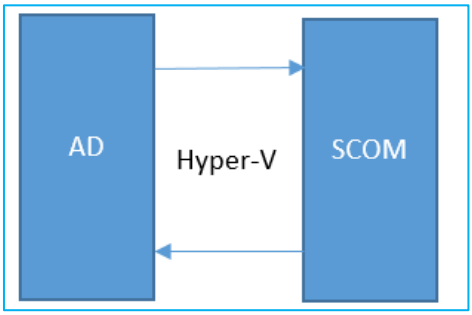
شکل ۸- ۴۱۸ Hyper-v در ویندوز ۱۱

۸–۳–۱٤–۸ 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 ۸–٤۱۹، دو سرور در نظر گرفتیم که هر کدام دارای ویندوز سرور ۲۰۲۵ هستند و بر روی هر دوی آنها، سرویس Hyper-V فعّال شده است.

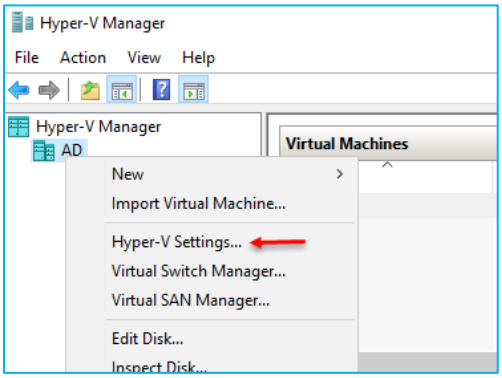
www.takbook.com



شکل ۸- ۴۱۹ ابزار *Replication*

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

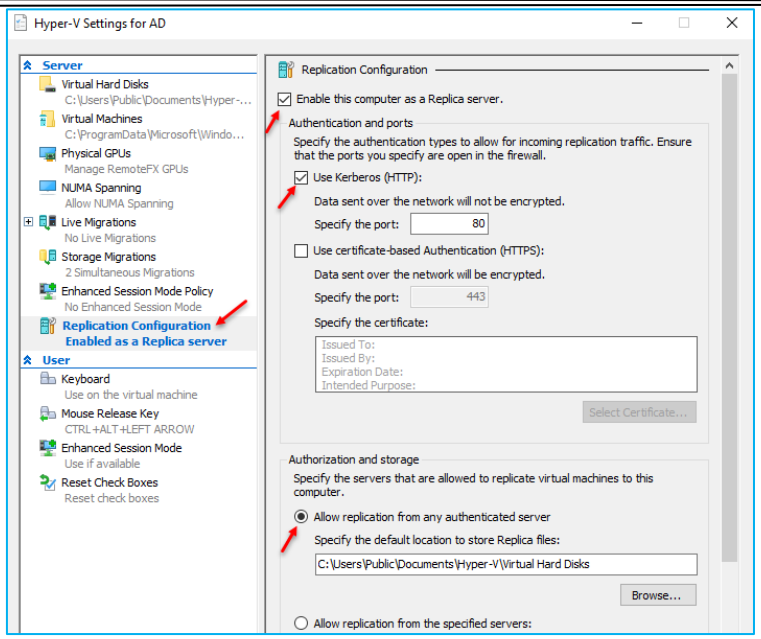
برای شروع وارد سرور AD شوید و سرویس Hyper-V را فعّال کنید، به مانند شکل ۸-٤۲۰، بر روی نام سرور، کلیک راست کنید و گزینه‌ی Hyper-V Settings را انتخاب کنید.



شکل ۸- ۴۲۰ ابزار *Replication*

در شکل ۸-٤۲۱، از سمت چپ وارد 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.

www.takbook.com



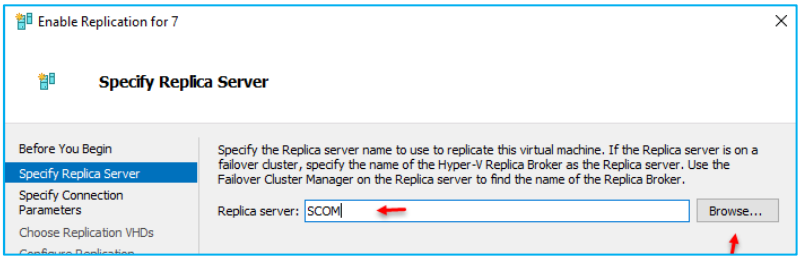
شکل ۸- ۴۲۱ ابزار *Replication*

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.

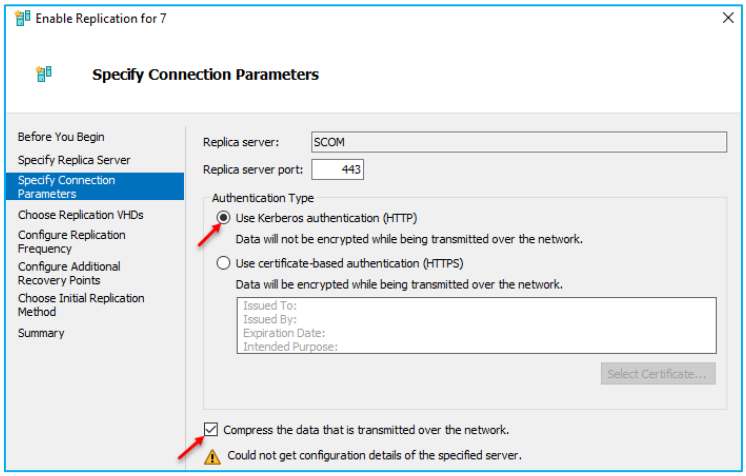
در شکل ۸-۴۲۲، باید نام سرور روبرو برای انجام Replicate را وارد کنید، نام سرور را SCOM وارد کنید، یک بار دیگر بیان می‌کنیم که در سرور روبرو، سرویس Hyper-V فعّال شده است.



شکل ۸- ۴۲۲ ابزار *Replication*

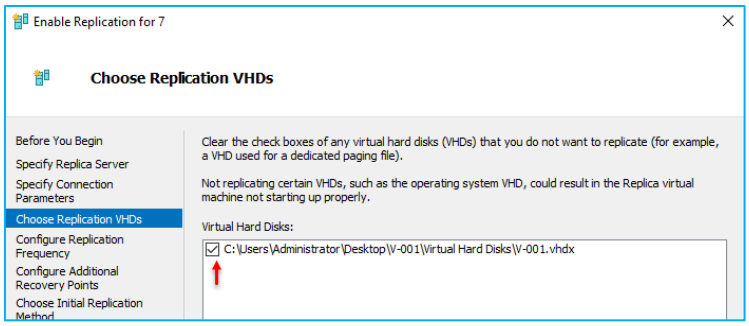
در شکل ۸-۴۲۳، بعد از تأیید سرور SCOM باید نوع ارتباط امنیّتی را مشخّص کنید، برای ادامه‌ی کار، گزینه‌ی Use Kerberos authentication (HTTP) را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



شکل ۸- ۴۲۳ ابزار Replication

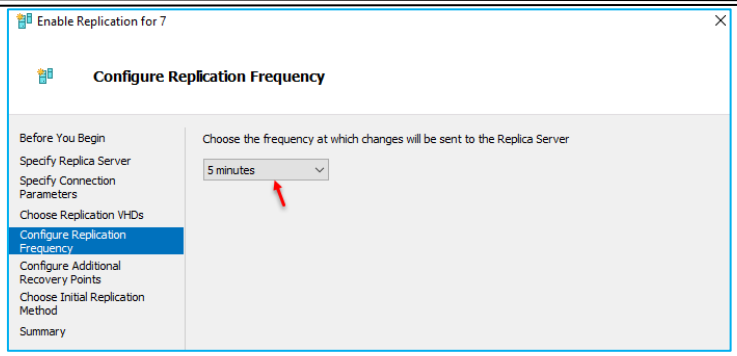
در شکل ۸-٤۲٤، باید هارد دیسک مربوط به ماشین انتخابی مورد نظر را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۴۲۴ ابزار Replication

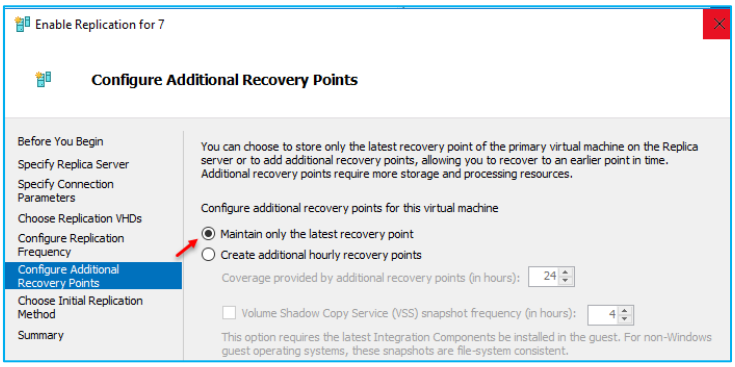
در شکل ۸-٤۲٥، می‌توانید، زمانی را برای ارتباط دو سرور برای انتقال اطّلاعات مشخّص کنید، سعی کنید این زمان، نه زیاد و نه خیلی کم باشد.

www.takbook.com



شکل ۸- ۴۲۵ ابزار *Replication*

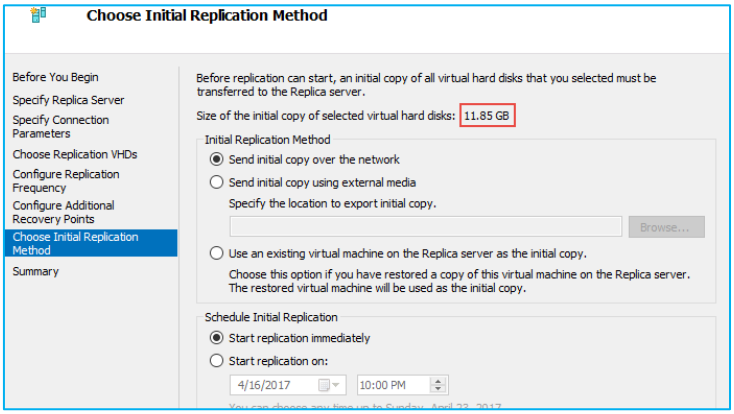
شکل ۸-۴۲۶، مربوط به ایجاد Recovery Point است تا در صورت بروز خطا بتوانید ماشین را به یک حالت پایدار برگردانید که اگر گزینه‌ی اوّل را انتخاب کنید، یک Recovery Point از ماشین مورد نظر ایجاد می‌کند، گزینه‌ی آخر برای انجامRecovery Point در ساعت‌های مختلف است که تعداد این کار را افزایش می‌دهد؛ بر روی Next کلیک کنید.



شکل ۸- ۴۲۶ ابزار *Replication*

در شکل ۸-۴۲۷، 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.

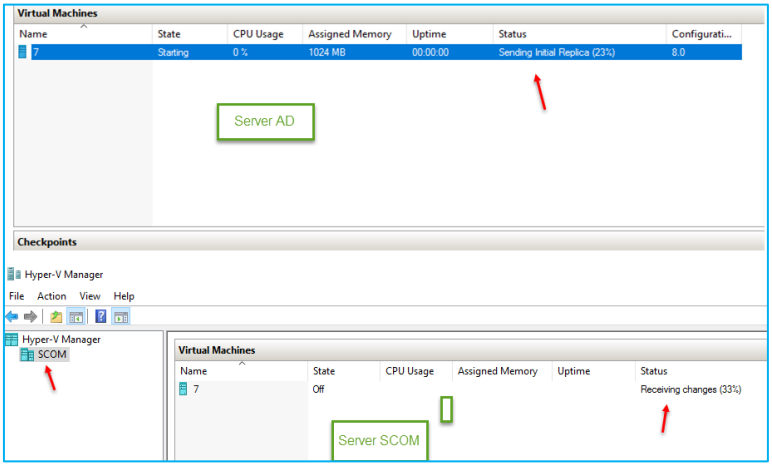
www.takbook.com



شکل ۸- ۴۲۷ ابزار *Replication*

در شکل ۸-۴۲۸، 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.

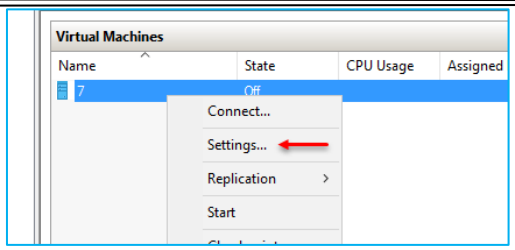
بعد از چند دقیقه، ماشین مورد نظر به صورت کامل به سرور SCOM انتقال داده می‌شود و اگر بعد از این، تغییری در سرور اوّل، یعنی AD بر روی ماشین 7 انجام شود، در سرور دوّم نیز بعد از زمان مشخّص‌شده اعمال می‌شود.



شکل ۸- ۴۲۸ ابزار *Replication*

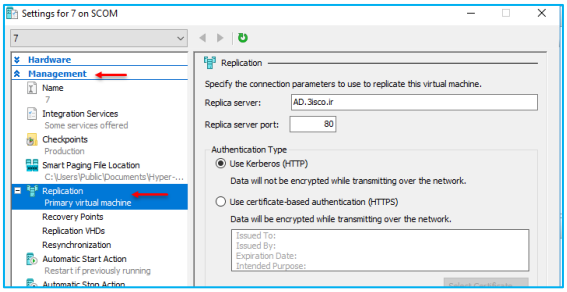
اگر بخواهید دوباره به تنظیمات Replica خود، سری بزنید باید به مانند شکل ۸-۴۲۹، بر روی ماشین مورد نظر کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید.

www.takbook.com



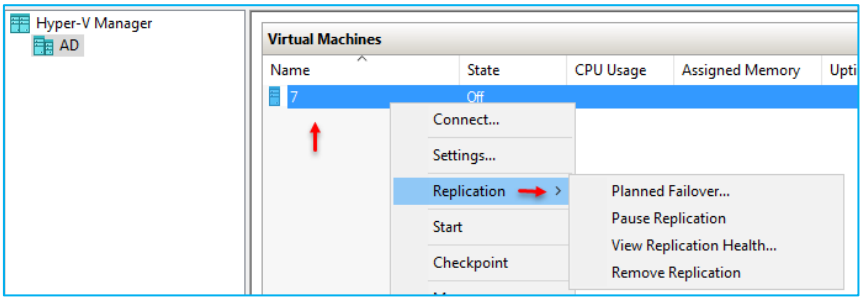
شکل ۸- ۴۲۹ ابزار *Replication*

در شکل ۸-۴۳۰، از سمت چپ وارد قسمت Management شوید و گزینه‌ی Replication را انتخاب کنید، در این صفحه می‌توانید تنظیمات مورد نظر را تغییر دهید.



شکل ۸- ۴۳۰ ابزار *Replication*

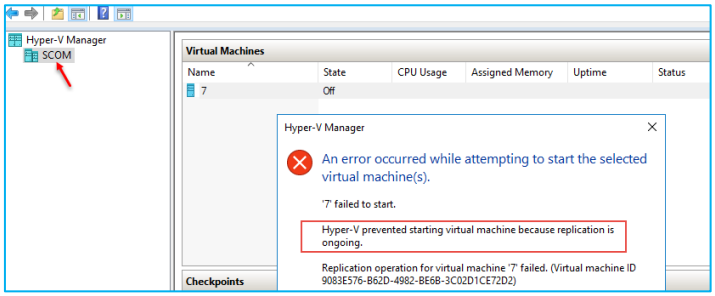
اگر بعد از انجام عملیّات Replica، به مانند شکل ۸-۴۳۱، بر روی ماشین مورد نظر کلیک راست کنید، یک گزینه‌ی جدید با نام Replication ایجاد شده است که دارای چهار گزینه است؛ گزینه‌ی اوّل برای انتقال سرور اجرا کننده‌ی ماشین به سرور دوّم است، گزینه‌ی دوّم، Pause Replication برای متوقّف کردن عملیّات Replicate بین 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.



شکل ۸- ۴۳۱ ابزار *Replication*

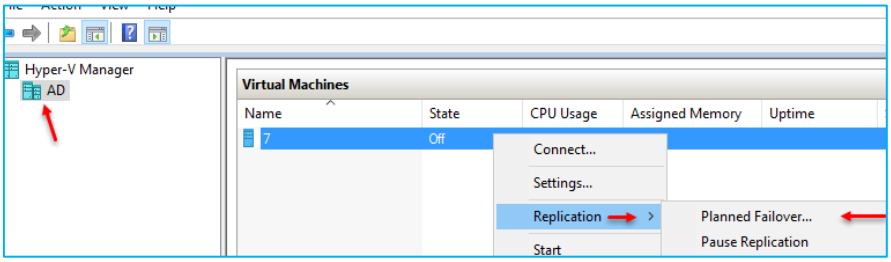
www.takbook.com

اگر چنانچه بخواهید در سرور دوّم که ماشین به آن انتقال داده شده است، ماشین را روشن کنید با خطای شکل ۸-۴۳۲، 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.



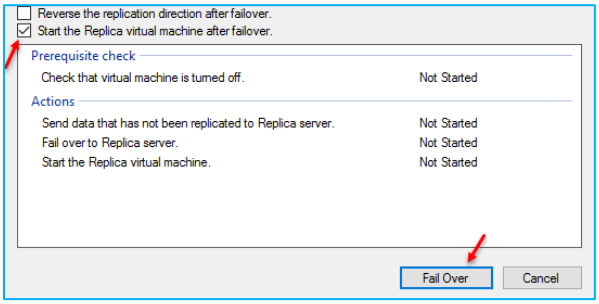
شکل ۸- ۴۳۲ ابزار Replication

حال اگر بخواهید، سرور دوّم را به عنوان سرور اصلی برای سرویس Replicate در نظر بگیرید باید به مانند شکل ۸-۴۳۳، در سرور اصلی AD بر روی ماشین مورد نظر کلیک راست و از قسمت Replication، گزینه‌ی Planned Failover را انتخاب کنید.



شکل ۸- ۴۳۳ ابزار Replication

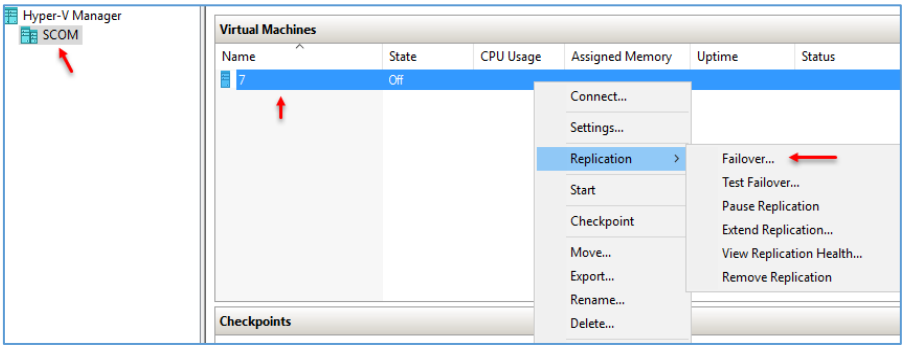
در شکل ۸-۴۳۴، برای انتقال، تیک گزینه‌ی مورد نظر را انتخاب و بر روی Fail Over کلیک کنید تا عملیّات انتقال انجام شود.



شکل ۸- ۴۳۴ ابزار Replication

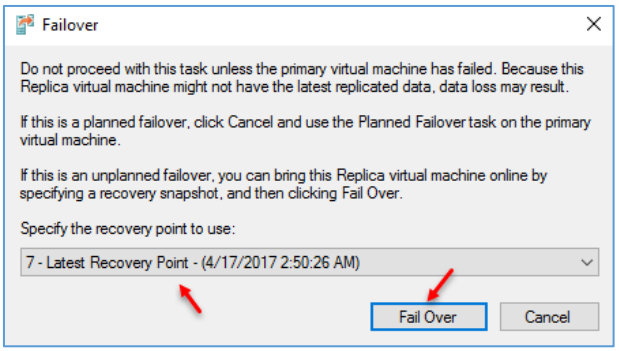
www.takbook.com

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 به مانند شکل ۸–۴۳۵، بر روی ماشین مجازی مورد نظر کلیک راست کنید و از قسمت Replication، گزینه‌ی Failover را انتخاب کنید.



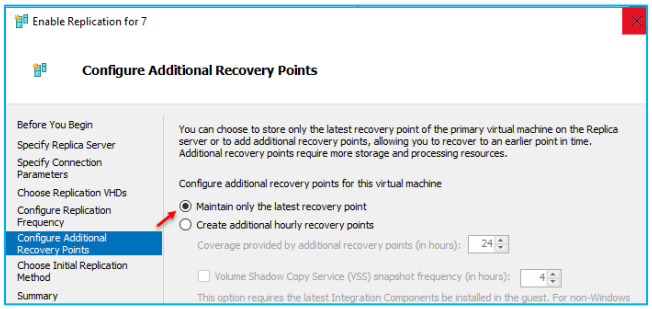
شکل ۸– ۴۳۵ ابزار *Replication*

در شکل ۸–۴۳۶، 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.



شکل ۸– ۴۳۶ ابزار *Replication*

توجّه کنید، اگر در زمان فعّال کردن Replicate، در شکل ۸–۴۳۷، گزینه‌ی دوّم را انتخاب می‌کردید، حالا در شکل ۸–۴۳۶، دارای چندین زمان مختلف برایLatset Recovery بودید.

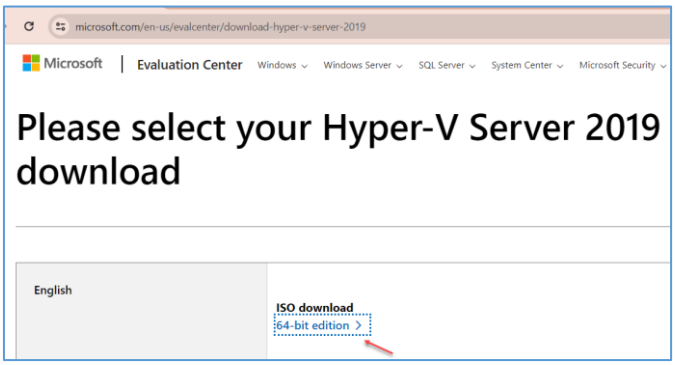


شکل ۸– ۴۳۷ ابزار *Replication*

www.takbook.com

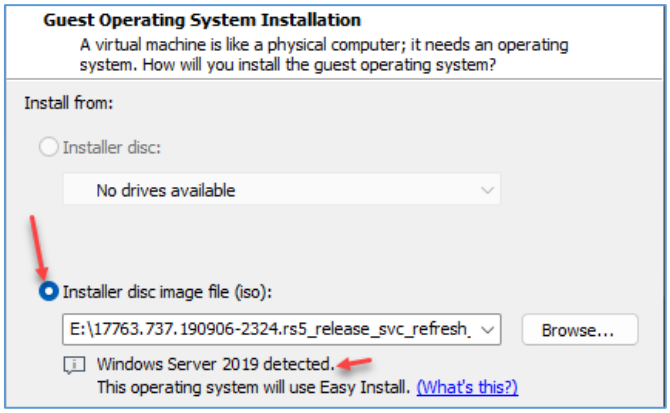
۹-۱٤-۳-۸ نصب Hyper-v سرور

بعد از اینکه در قسمت قبلی سرویس Hype-V را بر روی ویندوز سرور فعال کردید، حالا در این قسمت می‌خواهیم Hyper-V سرور را نصب کنیم، در این ویژگی یک فایل ویندوز دانلود می‌کنید که روی آن فقط ورژن Hyper-V فعال شده است و باید به این نکته اشاره کرد که این سرویس در حال حاضر این کتاب رو دارم می‌نویسم برای ورژن ۲۰۱۹ فعال شده است که از طریق لینک زیر می‌توانید دانلود کنید:
https://www.microsoft.com/en-us/evalcenter/download-hyper-v-server-2019
طبق شکل ۸-٤۳۸، بر روی لینک کلیک کنید تا فایل ISO دانلود شود.



شکل ۸- ۴۳۸ نصب Hyper-v سرور

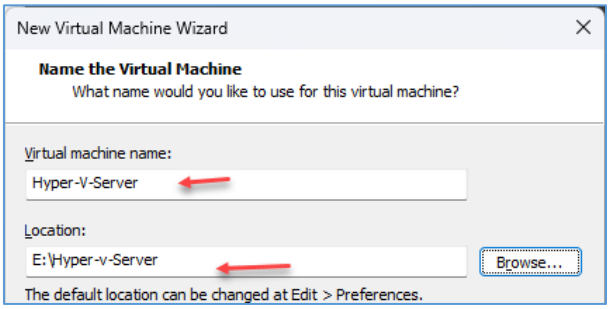
بعد از دانلود فایل مورد نظر بهتر است یک سیستم فیزیکی را آماده و این ویندوز را بر روی آن نصب کنید و یا اینکه از یک ماشین مجازی استفاده کنید، برای انجام این کار در این بخش از ماشین مجازی استفاده می‌کنیم، وارد نرم‌افزار VMware Workstation شوید و ماشین جدید را ایجاد کنید، زمانی که مانند شکل ۸-٤۳۹، فایل مورد نظر را انتخاب می‌کنید فایل مورد نظر به عنوان ویندوز سرور ۲۰۱۹ تشخیص داده می‌شود.



شکل ۸- ۴۳۹ نصب Hyper-v سرور

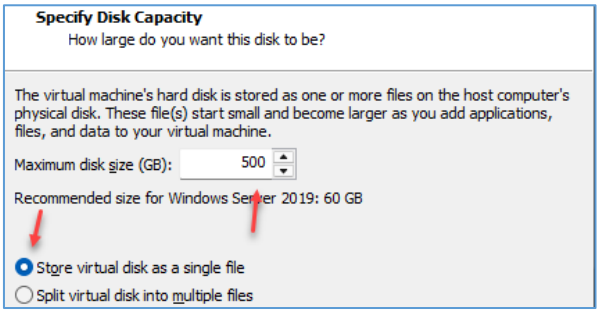
www.takbook.com

به مانند شکل ۸-٤٤۰، یک نام و مسیر ذخیره‌سازی را برای آن مشخص کنید، توجه داشته باشید باید این مسیر دارای فضای زیادی باشد که در ادامه وقتی ماشین مجازی ایجاد می‌کنیم با کمبود حافظه روبرو نشویم.



شکل ۸- ۴۴۰ نصب Hyper-v سرور

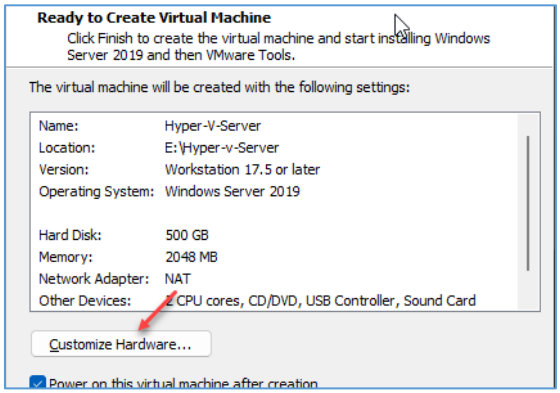
طبق شکل ۸-٤٤۱، مقدار هارد را برای این ماشین ۵۰۰ گیگابایت در نظر می‌گیریم.



شکل ۸- ۴۴۱ نصب Hyper-v سرور

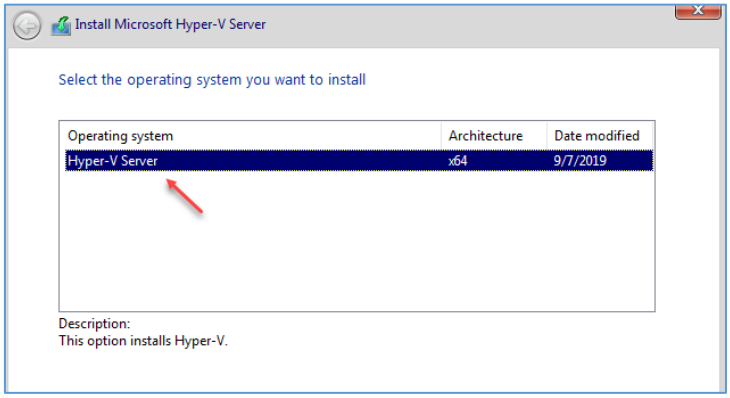
در شکل ۸-٤٤۲، باید بر روی Customize Hardware کلیک کنید و مقدار رم و مقدار CPU را برای این ماشین تغییر دهید که در این قسمت ۳۲ گیگ رم برای آن در نظر گرفتیم به همراه 8 core CPU تا قدرت مناسبی داشته باشد.

www.takbook.com



شکل ۸- ۴۴۲ نصب Hyper-v سرور

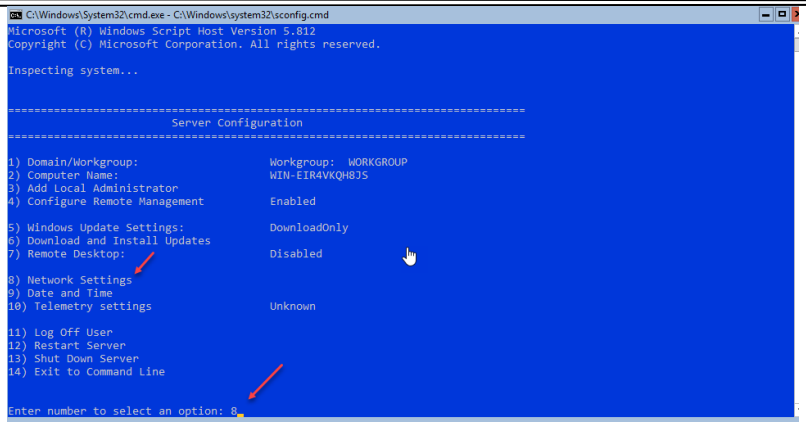
بعد از ایجاد ماشین مورد نظر آن را روشن کنید که صفحه‌ی اولی که مشاهده خواهید کرد به مانند شکل ۸-٤٤٣، خواهد بود که Hyper-v Server نوشته شده است، آن را انتخاب و بر روی Next کلیک کنید تا نصب آغاز شود.



شکل ۸- ۴۴۳ نصب Hyper-v سرور

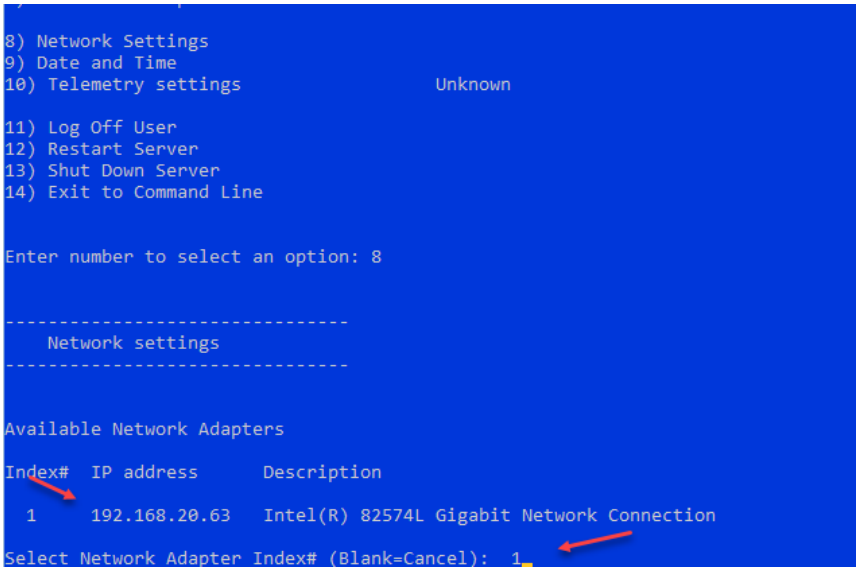
بعد از نصب اولین صفحه‌ای که مشاهده می‌کنید شکل ۸-٤٤٤،ح است که دارای گزینه‌های مختلفی است و دیگر خبر یاز گرافیک نیست، برای اینکه کار را آغاز کنیم اول باید آدرس IP سرور را مشخص کنیم، برای اینکار گزینه‌ی 8 را انتخاب می‌کنیم.

www.takbook.com



شکل ۸- ۴۴۴ نصب Hyper-v سرور

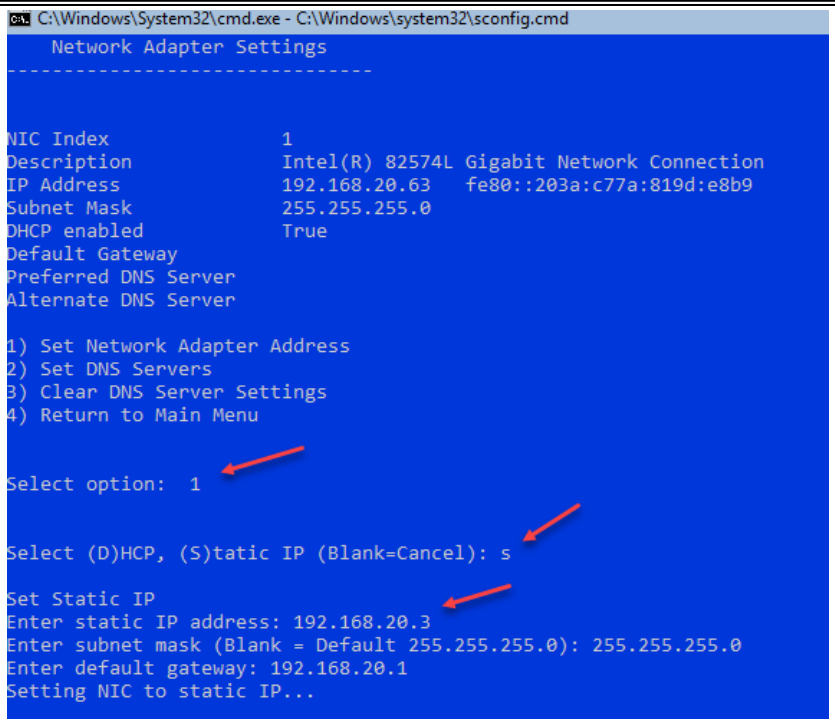
همان‌طور که در شکل ۸-٤٤٥، مشاهده می‌کنید یک آدرس IP به صورت اتوماتیک به این سرور داده شده است و ما می‌خواهیم به صورت دستی برای این سرور آدرس مشخص کنیم، برای این کار گزینه‌ی یک را وارد کنید.



شکل ۸- ۴۴۵ نصب Hyper-v سرور

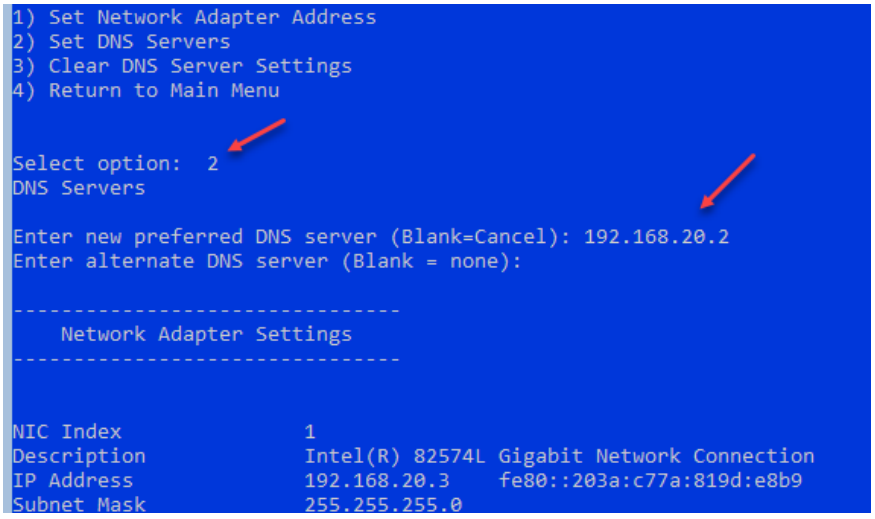
بعد از انتخاب کارت شبکه مورد نظر باید به مانند شکل ۸-٤٤٦، گزینه‌ی یک یعنی Set Network Adpator Address را انتخاب کنید، و بعد کلمه‌ی S یعنی Static را وارد کنید و آدرس را به صورت دستی وارد کنید.

www.takbook.com



شکل ۸- ۴۴۶ نصب Hyper-v سرور

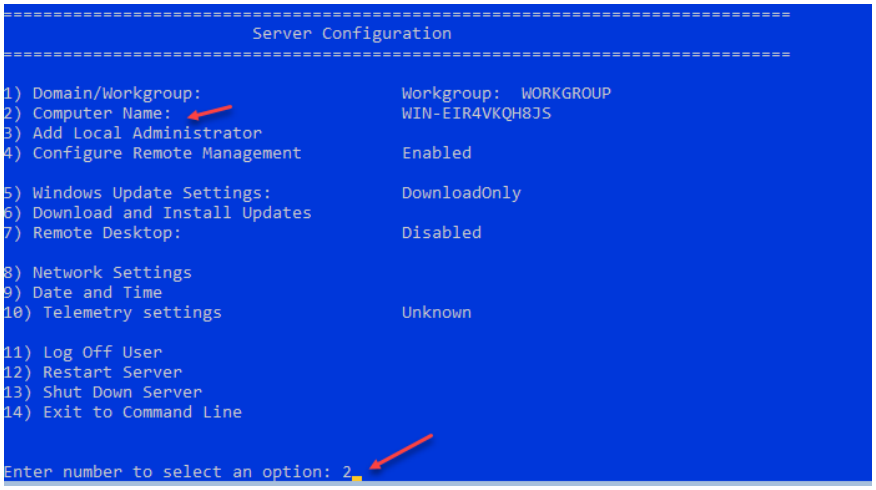
بعد از ست کردن آدرس IP به صورت دستی باید به مانند شکل ۸-٤٤٧، گزینه‌ی دوم یعنی Set DNS Servers را انتخاب و DNS سرور شبکه را ست کنید، بعد از این کار با انتخاب عدد 4 به صفحه اصلی برگردید.



شکل ۸- ۴۴۷ نصب Hyper-v سرور

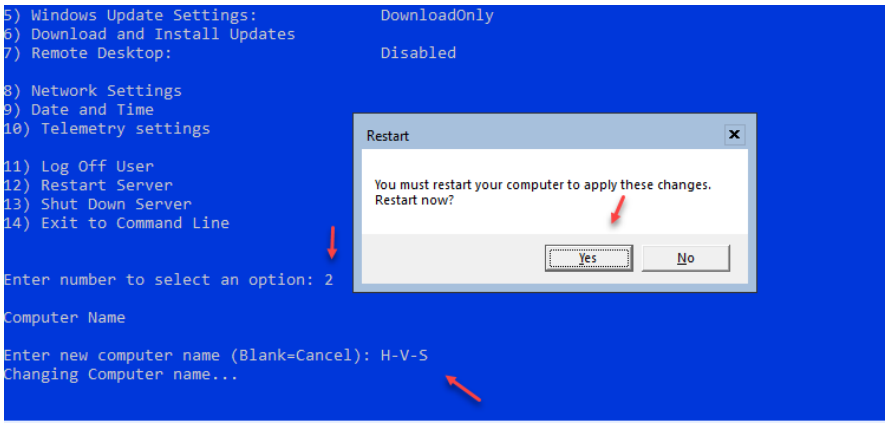
www.takbook.com

در ادامه کار نام سرور را باید تغییر دهیم که به مانند شکل ۸–٤٤۸، باید گزینه‌ی دوم را انتخاب کنید.



شکل ۸- ۴۴۸ نصب Hyper-v سرور

به مانند شکل ۸–٤٤۹، با وارد کردن نام سرور پیغامی ظاهر می‌شود که باید سرور مورد نظر Restart شود که باید بر روی Yes کلیک کنید.

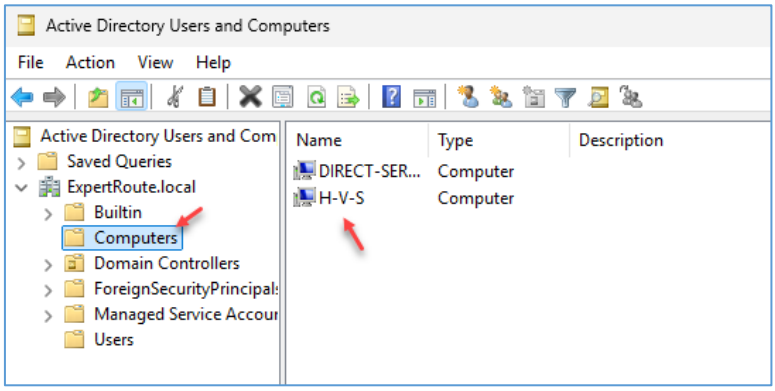


شکل ۸- ۴۴۹ نصب Hyper-v سرور

در ادامه کار برای اینکه سرور مورد نظر را عضو دومین کنیم باید گزینه‌ی یک را انتخاب و بعد کلمه D یعنی Domain را وارد و نام دومین خود را وارد کنیم و بعد باید نام دومین به همراه نام کاربری را وارد کنیم و بعد از Enter صفحه درخواست رمز ظاهر می‌شود که بعد از تایید رمز، سرور مورد نظر عضو دومین خواهد شد.

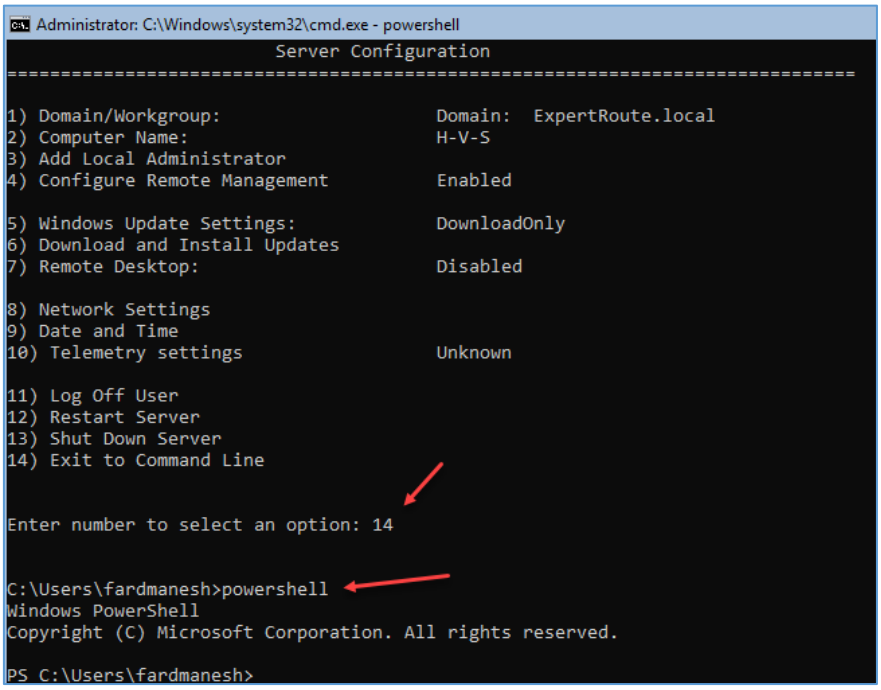
اگر به مانند شکل ۸–٤٥۰، وارد Active Directory شوید این سرور را در قسمت Computers مشاهده می‌کنید.

www.takbook.com



شکل ۸- ۴۵۰ نصب Hyper-v سرور

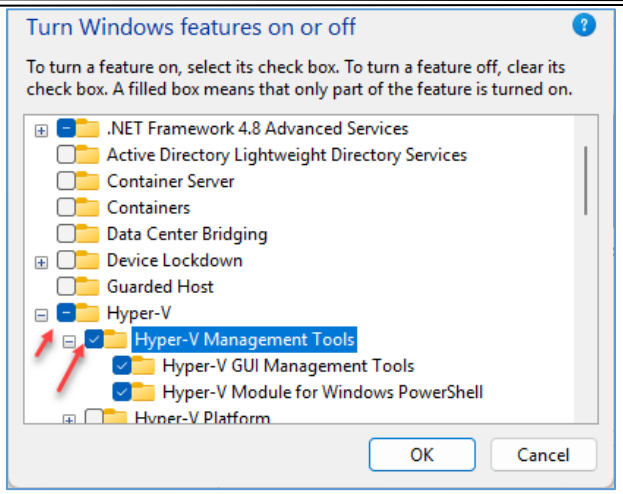
بعد از انجام مراحل قبل حالا باید تنظیماتی برای متصل شدن به سرور Hyper-v انجام دهیم، برای این کار به مانند شکل ۸-۴۵۱، با وارد کردن عدد 14 از منو خارج شوید و در خط فرمان دستور PowerShell را وارد کنید تا وارد خط فرمان PowerShell شویم.



شکل ۸- ۴۵۱ نصب Hyper-v سرور

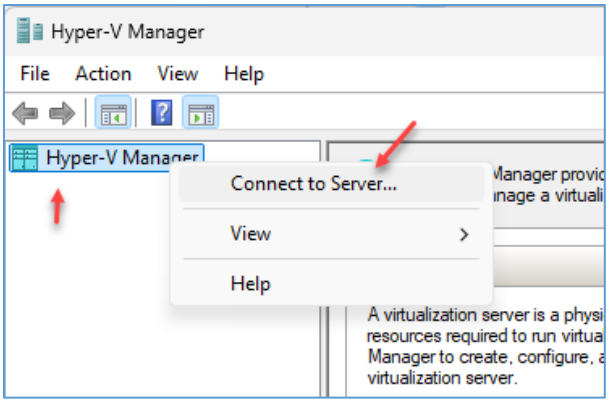
حالا برای اینکه بتوانیم به سرویس Hyper-v متصل شویم به مانند شکل ۸-۴۵۲، باید سرویس Hyper-v Management را بر روی یکی از کلاینت ها و سرورهای خود نصب کنید و بتوانیم از آن طریق به سرور متصل شویم.

www.takbook.com



شکل ۸- ۴۵۲ نصب Hyper-v سرور

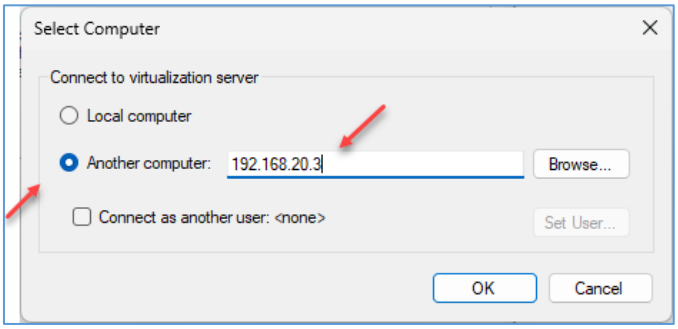
در ادامه به مانند شکل ۸-٤٥٣، سرویس مورد نظر را باز می‌کنیم و بر روی نام سرور کلیک راست می‌کنیم و گزینه‌ی Connect to Server را انتخاب می‌کنیم.



شکل ۸- ۴۵۳ نصب Hyper-v سرور

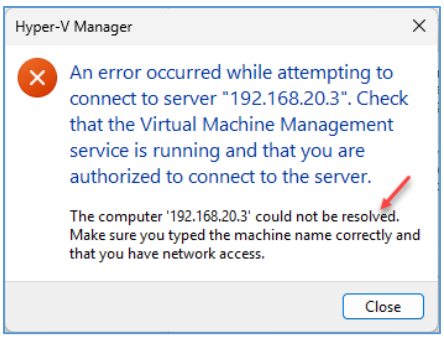
در شکل ۸-٤٥٤، باید آدرس سرور Hyper-v خود را وارد کنیم و بر روی OK کلیک کنیم.

www.takbook.com



شکل ۸- ۴۵۴ نصب Hyper-v سرور

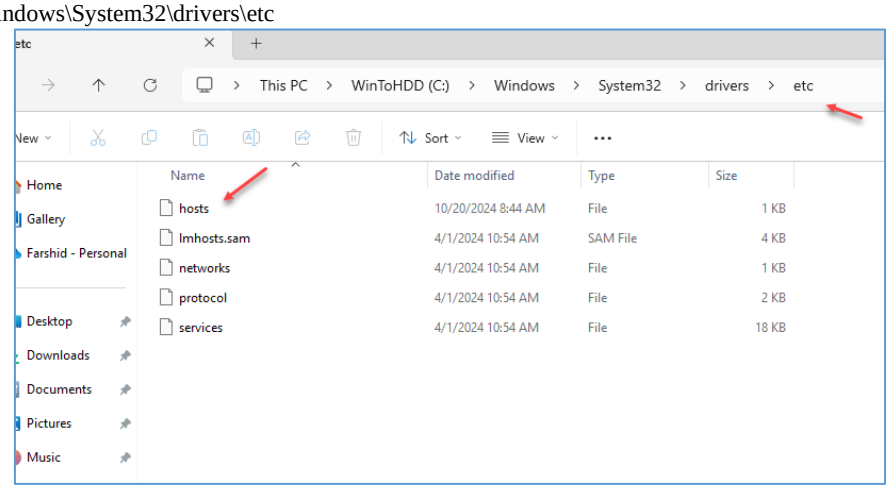
که در زمان اتصال با خطای شکل ۸-٤٥٥، روبرو می‌شوید که این خطا مربوط به Resolved نکردن نام و آدرس IP است که باید به صورت دستی این موضوع را اصلاح کنیم.



شکل ۸- ۴۵۵ نصب Hyper-v سرور

برای حل این مشکل در کلاینت خود وارد آدرس شکل ۸-٤٥٦، شوید و فایل hosts را باز کنید.

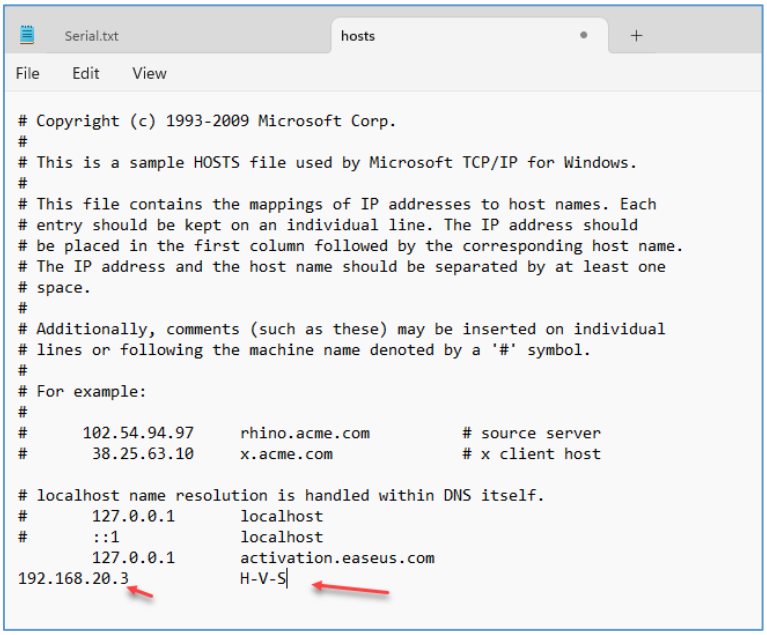
C:\Windows\System32\drivers\etc



شکل ۸- ۴۵۶ نصب Hyper-v سرور

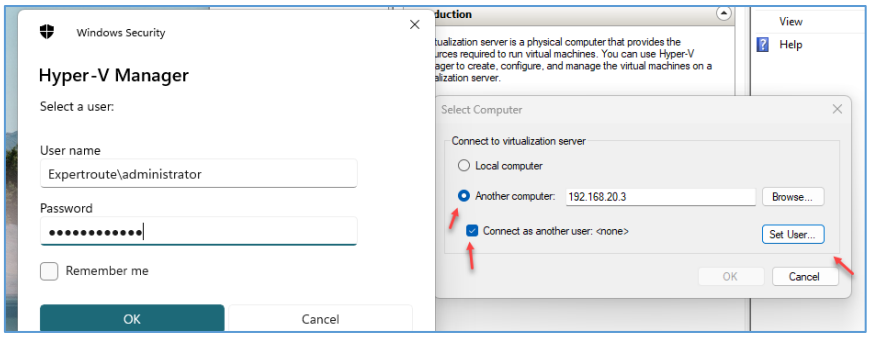
www.takbook.com

آدرس IP را به همراه نام سرور به مانند شکل ۸–۴۵۷، وارد کنید و فایل را Save کنید، اگر فایل مورد نظر Save نمی‌شود اول آن را در دسکتاپ کپی کنید تغییرات را اعمال و ذخیره کنید و بعد به جای قبلی برگردانید.



شکل ۸- ۴۵۷ نصب Hyper-V سرور

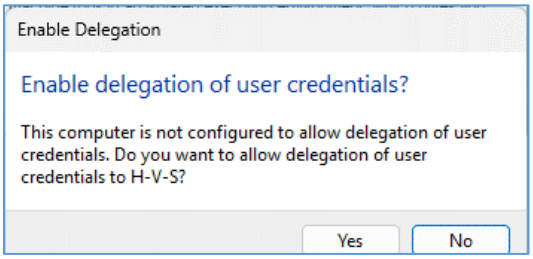
دوباره به مانند شکل ۸–۴۵۸، آدرس IP سرور را وارد و تیک User را انتخاب و بر روی Set User کلیک کنید و نام دومین را به همراه نام کاربر مورد نظر وارد و ذخیره کنید و بر روی OK کلیک کنید.



شکل ۸- ۴۵۸ نصب Hyper-V سرور

همان‌طور که در شکل ۸–۴۵۹، مشاهده می‌کنید پیغام قبلی حل شده و پیغام جدیدی ظاهر شده است.

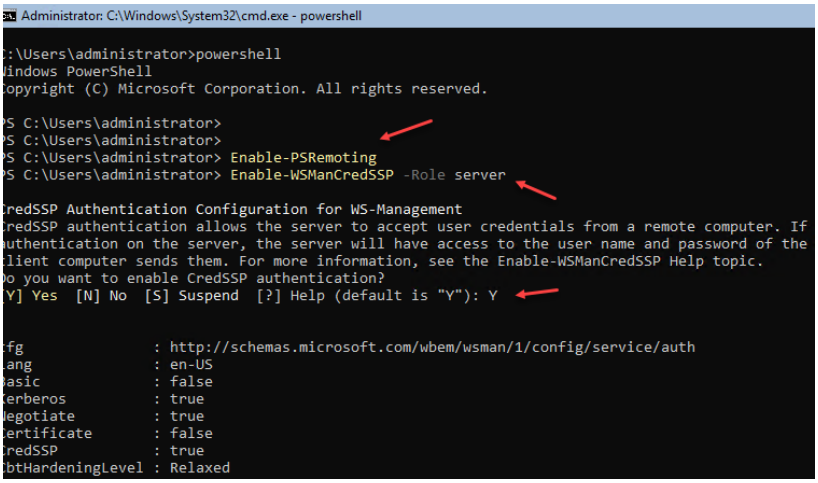
www.takbook.com



شکل ۸- ۴۵۹ نصب Hyper-v سرور

برای حل این پیغام باید وارد سرور Hyper-v شوید و دستورات زیر را در PowerShell وارد کنید.

Enable-PSRemoting
Enable-WSManCredSSP -Role server



شکل ۸- ۴۶۰ نصب Hyper-v سرور

بعد از این کار باید وارد کلاینت خود شوید و PowerShell را به مانند شکل ۸-٤٦١، اجرا کنید و دستورات زیر را به ترتیب فعال کنید.

start-service -name winrm
set-item wsman:\localhost\client\trustedhosts -value H-V-S

stop-service -name winrm
Get-Item WSMan:\localhost\Client\TrustedHosts

www.takbook.com


```
PS C:\Windows\system32> start-service -name winrm
PS C:\Windows\system32> set-item wsman:\localhost\client\trustedhosts -value H-V-S

WinRM Security Configuration.
This command modifies the TrustedHosts list for the WinRM client. The computers in the Truste
authenticated. The client might send credential information to these computers. Are you sure
this list?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
PS C:\Windows\system32> stop-service -name winrm
PS C:\Windows\system32> Get-Item WSMan:\localhost\Client\TrustedHosts

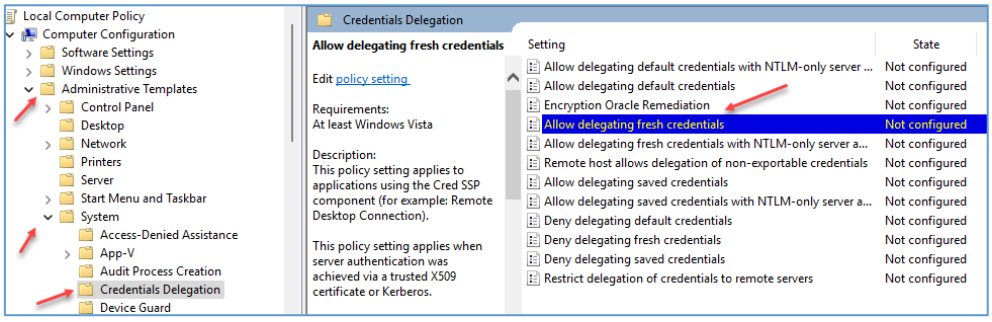
Start WinRM Service
WinRM service is not started currently. Running this command will start the WinRM service.

Do you want to continue?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

شکل ۸- ۴۶۱ نصب Hyper-V سرور

بعد از اجرای مراحل بالا، برای اینکه کار را به اتمام برسانیم باید وارد Group Policy در کلاینت مورد نظر شویم و سرویس CredSSP را تنظیم کنیم، CredSSP (Credential Security Support Provider) یک پروتکل احراز هویت است که به سیستم‌ها امکان می‌دهد اعتبارنامه‌های کاربر را از طریق شبکه به صورت امن ارسال کنند. در Hyper-V، CredSSP معمولاً برای احراز هویت در ارتباطات RDP (Remote Desktop Protocol) یا هنگام اتصال به ماشین‌های مجازی از راه دور استفاده می‌شود.

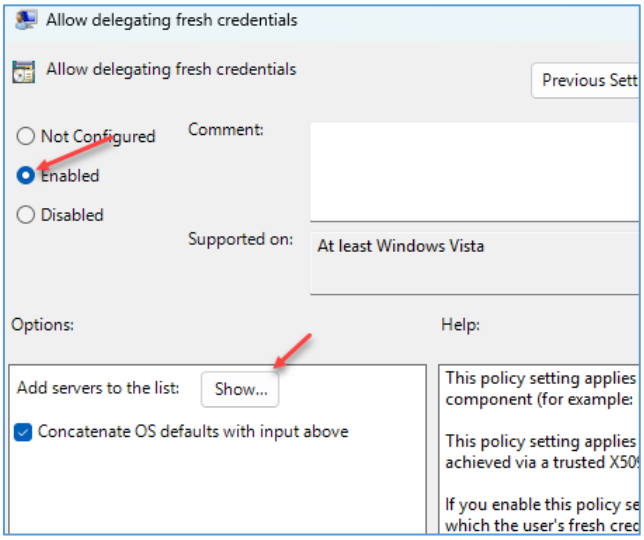
وارد سرویس Group Policy می‌شویم و به مانند شکل ۸-٤٦۲، وارد آدرس مشخص شده می‌شویم و بر روی Allow Deligation… دو بار کلیک می‌کنیم.



شکل ۸- ۴۶۲ نصب Hyper-V سرور

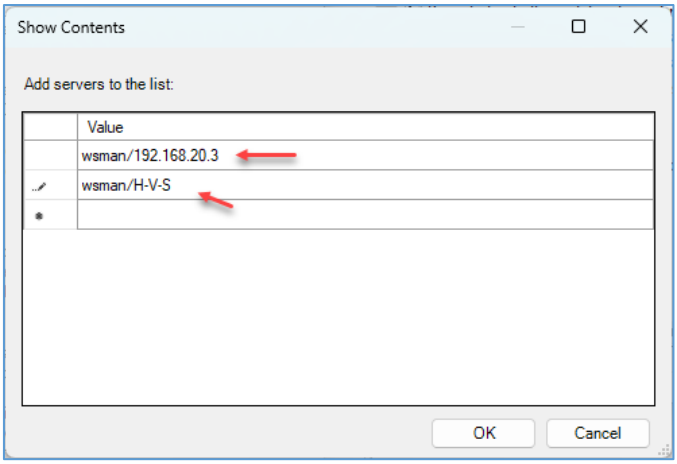
گزینه‌ی Enable را به مانند شکل ۸-٤٦۳ انتخاب و بر روی Show کلیک می‌کنیم.

www.takbook.com



شکل ۸- ۴۶۳ نصب Hyper-v سرور

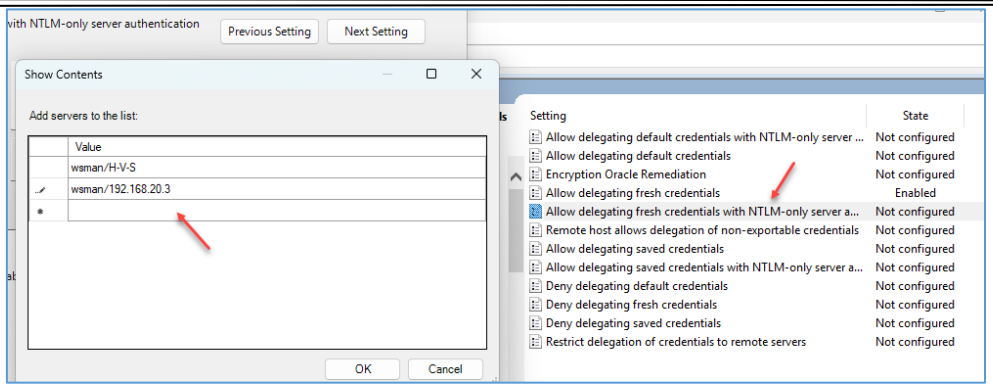
به مانند شکل ۸-٤٦٤، در این پنجره باید دو دستور زیر را در دو قسمت مشخص شده وارد کنیم، فقط به جای نام و آدرس، باید نام و آدرس سرور خود را وارد کنید.



شکل ۸- ۴۶۴ نصب Hyper-v سرور

دقیقاً همین کار را باید برای گزینه‌ی NTLM به مانند شکل ۸-٤٦٥ انجام دهید.

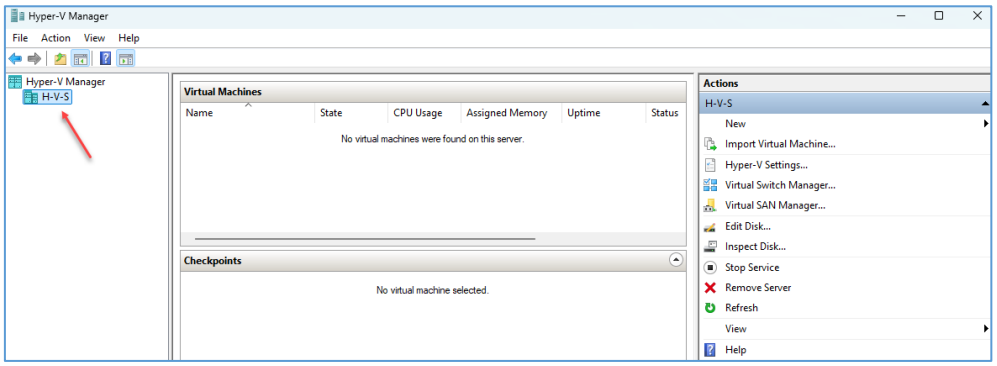
www.takbook.com



شکل ۸- ۴۶۵ نصب Hyper-v سرور

بعد از انجام مراحل بالا یک بار سرور Hyper-v و یک بار کلاینت خود را Restart کنید تا تنظیمات به صورت کامل اعمال شود.

بعد از اجرا شدن سرور به مانند شکل ۸-٤٦٦، به راحتی می‌توانید وارد سرور شوید و کارهای خود را انجام دهید.



شکل ۸- ۴۶۶ نصب Hyper-v سرور

حالا می‌توانید ماشین مجازی در این سرور ایجاد و با آن کار کنید، آموزش ایجاد ماشین مجازی را در قسمت قبل به صورت کامل توضیح دادیم که می‌توانید از آن آموزش استفاده کنید.

۸-۳-۱۵ سرویس NIC Teaming

NIC Teaming، که به عنوان "Ethernet Teaming" یا "Load Balancing and Failover (LBFO)" نیز شناخته می‌شود، یک فناوری است که به شما این امکان را می‌دهد تا چندین کارت شبکه (NIC) را به یک گروه ترکیب کنید. این کار باعث افزایش پهنای باند و افزونگی در ارتباطات شبکه می‌شود. NIC Teaming به ویژه در محیط‌های سروری و مجازی‌سازی مفید است.

www.takbook.com

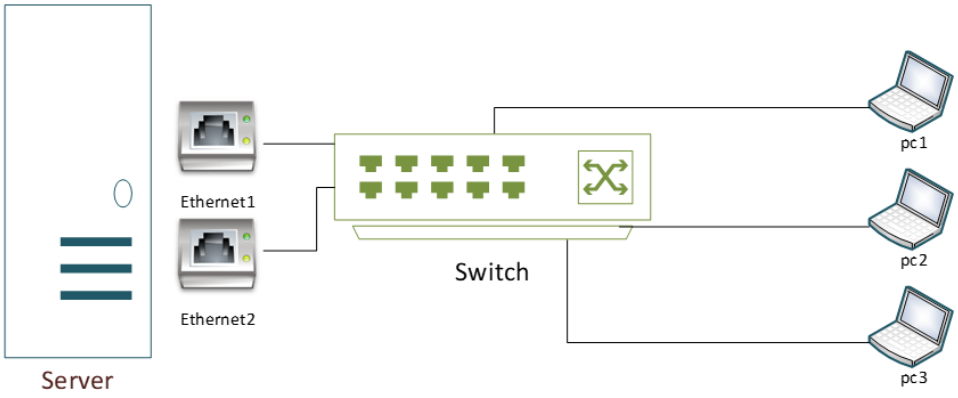
مثلاً اگر در شبکه‌ی خود از File Server و یا هر سرور ذخیره‌ساز دیگری استفاده می‌کنید و اصلاً دوست ندارید، حتّی برای چند لحظه، دسترسی به آن را از دست دهید باید از این سرویس استفاده کنید؛ تا زمانی که یک خطّ شبکه قطع شد، خطّ دیگری شروع به کار کند و جای خطّ قبلی را بگیرد.

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.

ویژگی‌ها و مزایای NIC Teaming:

- افزایش پهنای باند: با ترکیب چند NIC، می‌توانید پهنای باند بیشتری نسبت به استفاده از یک NIC منفرد داشته باشید. این به ویژه در محیط‌های با ترافیک بالا کاربرد دارد.
- افزونگی و قابلیت اطمینان: در صورتی که یکی از کارت‌های شبکه دچار مشکل شود، تیم NIC به طور خودکار ترافیک را به سایر کارت‌ها منتقل می‌کند. این کار به افزایش قابلیت اطمینان شبکه کمک می‌کند.
- بهبود عملکرد: در برخی از پیکربندی‌ها، بار ترافیکی بین NICها توزیع می‌شود که می‌تواند عملکرد کلی شبکه را بهبود بخشد.
- مدیریت ساده: با استفاده از NIC Teaming، می‌توانید چندین NIC را به عنوان یک واحد واحد مدیریت کنید، که کار مدیریت شبکه را آسان‌تر می‌کند.

برای شروع کار به شکل ۸-٤٦٧، توجّه کنید.



شکل ۸- ۴۶۷ سرویس NIC Teaming

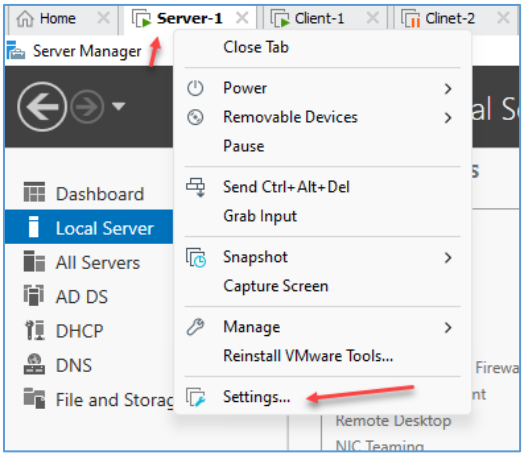
در شکل ۸-٤٦٧، یک سرور قرار دارد که دارای دو کارت شبکه است و این دو کارت شبکه از طریق کابلی به سوئیچ در شبکه متّصل شده‌اند و کلاینت‌ها و یا همان، PCها از طریق سوئیچ و بعد از طریق این دو

www.takbook.com

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.

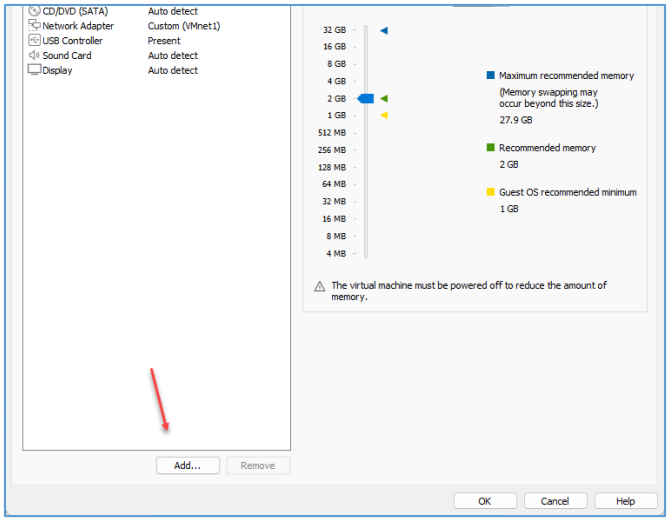
برای شروع کار به سرور خود، دو کارت شبکه اضافه می‌کنیم، در اینجا از سرور Server-1 استفاده می‌کنیم که آدرس IP آن، 192.168.20.2 بوده است.

بر روی سرور مورد نظر به مانند شکل ۸–٤٦٨، کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید.



شکل ۸- ۴۶۸ سرویس NIC Teaming

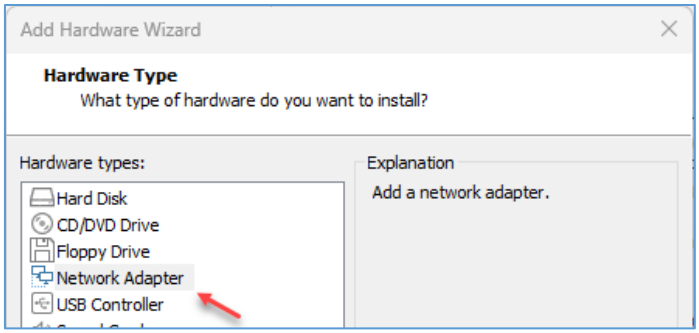
در شکل ۸–٤٦٩، بر روی Add کلیک کنید.



شکل ۸- ۴۶۹ سرویس NIC Teaming

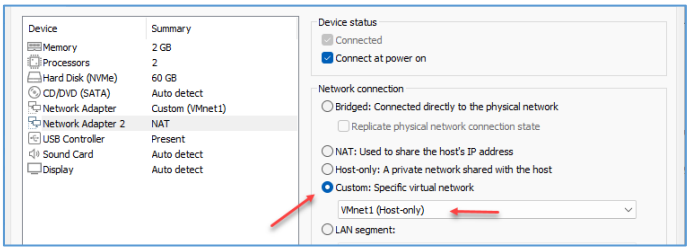
www.takbook.com

در شکل ۸-۴۷۰، هم Network Adaptor را انتخاب و بر روی Finish کلیک کنید.



شکل ۸- ۴۷۰ سرویس NIC Teaming

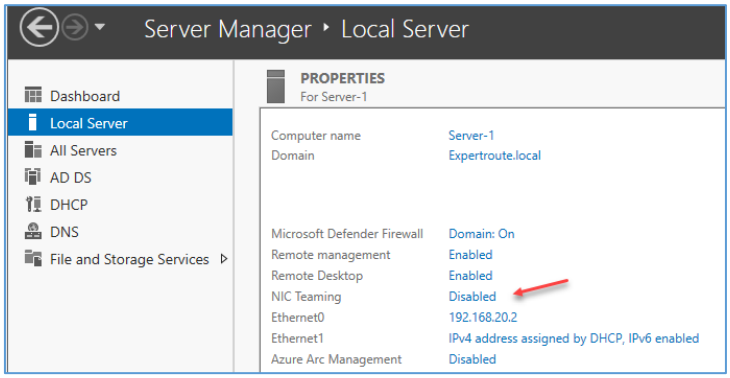
در شکل ۸-۴۷۱، گزینه‌ی Custom را انتخاب کنید و کارت شبکه‌ی VMnet1 را انتخاب و به لیست اضافه کنید.



شکل ۸- ۴۷۱ سرویس NIC Teaming

پس در حال حاضر، سرور Server-1 دارای دو کارت شبکه است، امّا هنوز تنظیماتی روی آن اعمال نشده است.

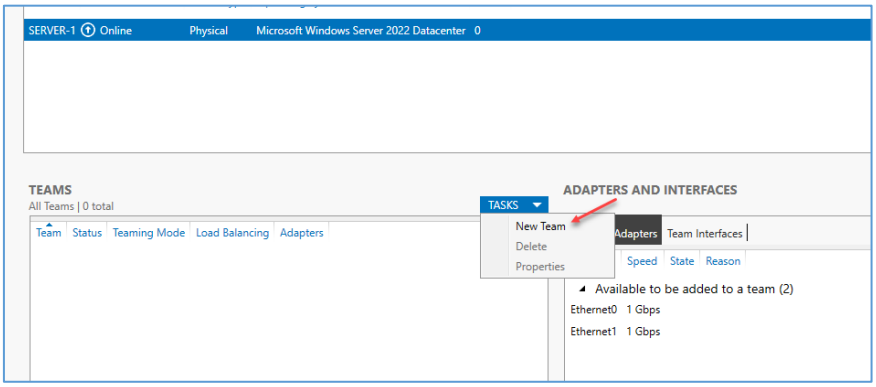
برای شروع به مانند شکل ۸-۴۷۲، واردServer Manager شوید و از سمت چپ بر رویLocal Server کلیک کنید و در صفحه‌ی باز شده، مقابل جلوی گزینه‌یNIC Teaming، بر روی Disabled کلیک کنید تا صفحه‌ی مورد نظر ظاهر شود.



شکل ۸- ۴۷۲ سرویس NIC Teaming

www.takbook.com

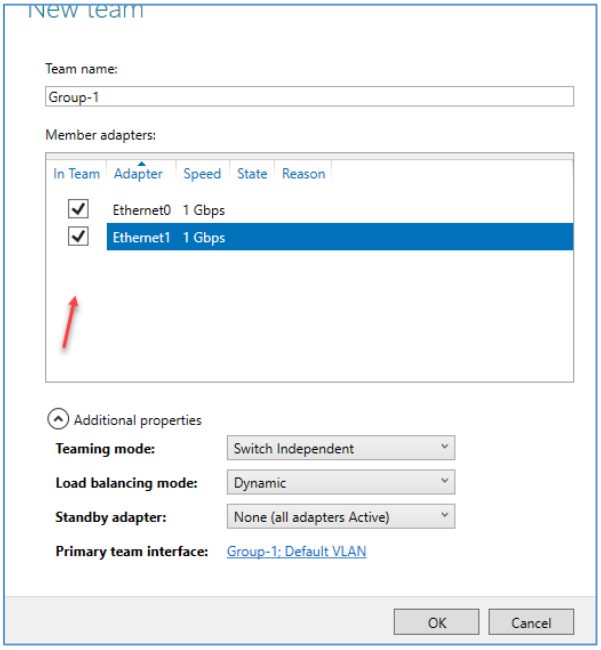
در شکل ۸-۴۷۳، دو کارت شبکه که بر روی سرور قرار گرفته شده، مشخّص است، برای شروع کار از قسمت TASKS، گزینه‌ی New Team را انتخاب کنید.



شکل ۸- ۴۷۳ سرویس NIC Teaming

به مانند شکل ۸-۴۷۴، 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.

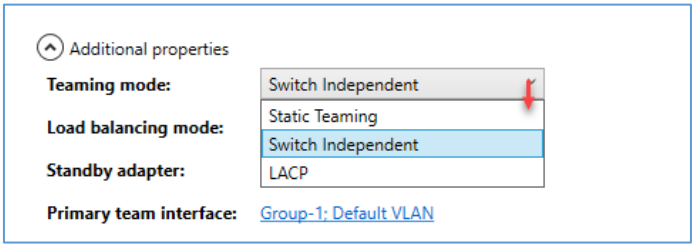
در قسمت Additional Properties، تنظیمات مربوط به Switch وجود دارد که هر کدام را با هم بررسی می‌کنیم.



شکل ۸- ۴۷۴ سرویس NIC Teaming

www.takbook.com

در قسمت Teaming Mode، سه گزینه وجود دارد که در شکل ۸-۴۷۵، آن را مشاهده می‌کنید، در ادامه هر کدام از آنها را توضیح خواهیم داد



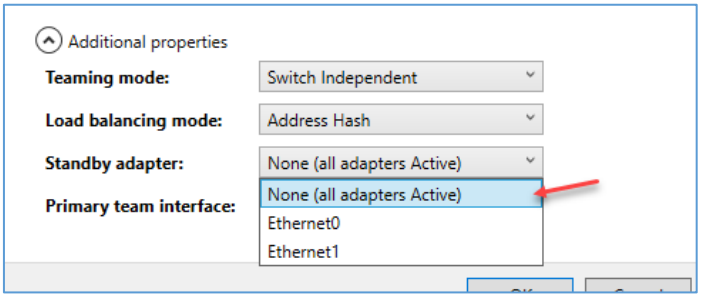
شکل ۸- ۴۷۵ سرویس NIC Teaming

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 ۸-۴۷۶، اگر Switch independent را انتخاب کنید، قسمت Standby adapter فعّال خواهد شد و در قسمت Standby adapter اگر گزینه‌ی اوّل ((None (all adapters Active) را انتخاب کنید، یعنی اینکه هر دو کارت شبکه به طور همزمان فعّال خواهد بود که این کار باعث ایجاد Load Balancing خواهد شد،



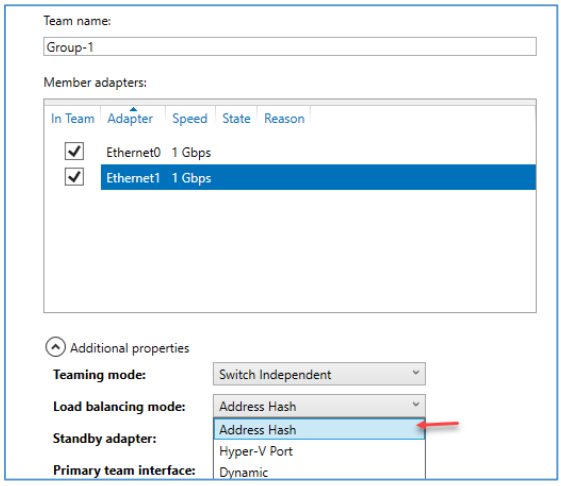
شکل ۸- ۴۷۶ سرویس NIC Teaming

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 دیگری 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 ۸-۴۷۷، انجام دهید و بر روی OK کلیک کنید.

www.takbook.com

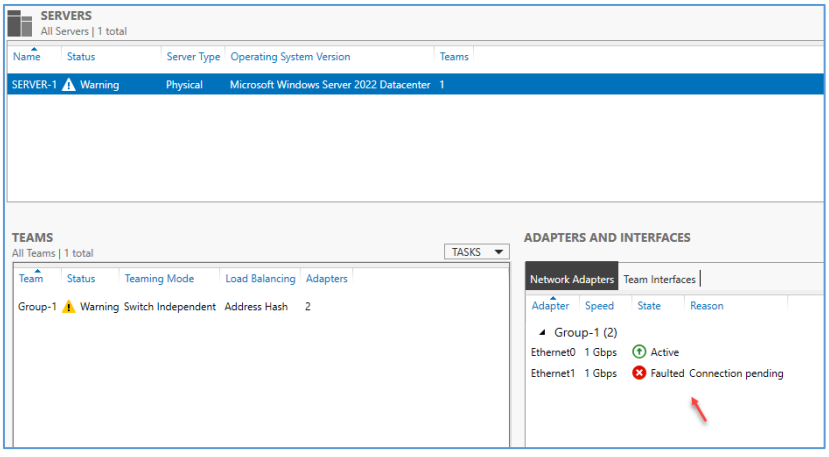
نکته مهم: اگر از ماشین مجازی استفاده می‌کنید، انتخاب دوحالت دیگر به غیر از Address Hash باعث ایجاد خطا می‌شود و شما باید در قسمت Load Balancing mode، فقط گزینه‌ی Address Hash را انتخاب کنید.



شکل ۸- ۴۷۷ سرویس NIC Teaming

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

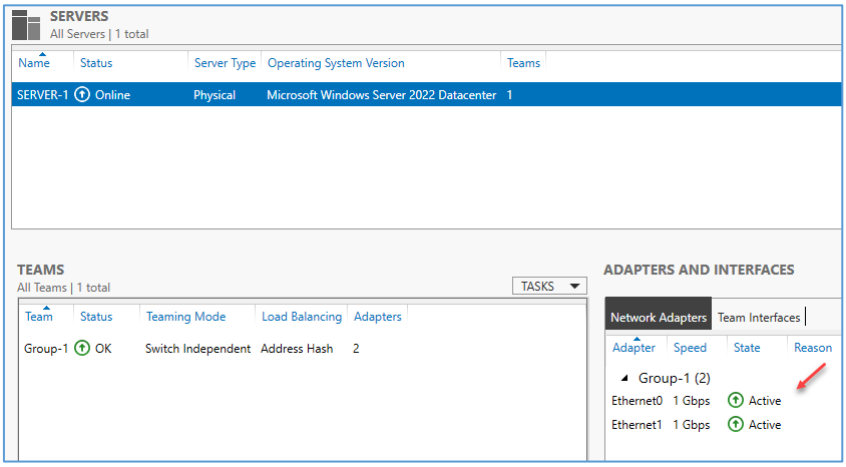
بعد از اینکه بر روی OK کلیک کردید، عملیّات انجام خواهد شد و شکل ۸-۴۷۸، برای شما به نمایش در خواهد آمد؛ در چند ثانیه‌ی اوّل، شاید یکی از کارت‌های شبکه شما با خطا Faulted… روبرو شود که بعد از چند ثانیه به حالت پایدار بر خواهد گشت و سرویس با قدرت، شروع به کار خواهد کرد که در شکل ۸-۴۷۹، مشاهده می‌کنید.



شکل ۸- ۴۷۸ سرویس NIC Teaming

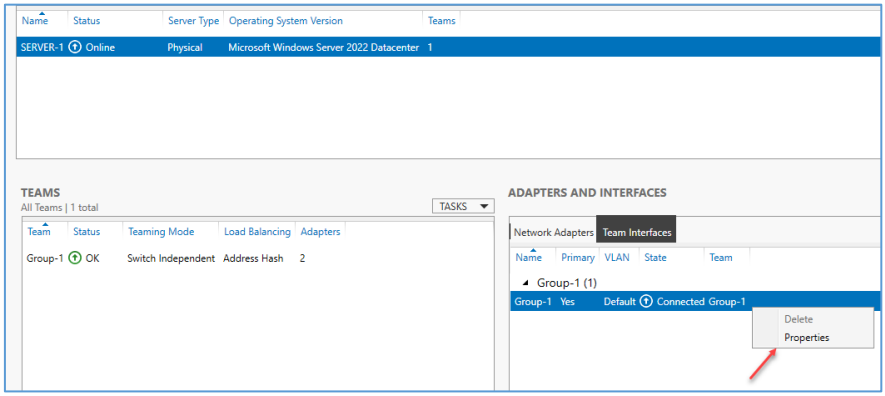
همان‌طور که در شکل ۸-۴۷۹، مشاهده می‌کنید دو کارت شبکه فعال شدند و در حال کار هستند.

www.takbook.com



شکل ۸- ۴۷۹ سرویس *NIC Teaming*

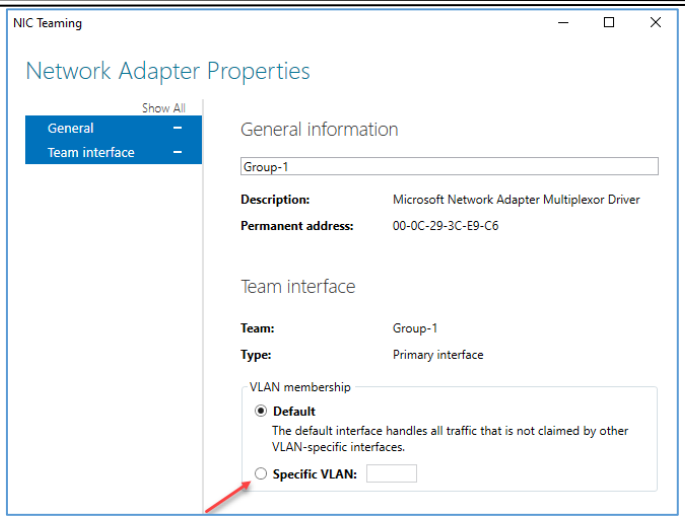
اگر در سوئیچ اصلی خود در شبکه از شماره‌ی VLAN خاصّی استفاده می‌کنید، می‌توانید وارد Team Interface شوید و به مانند شکل ۸-۴۸۰، بر روی نام مورد نظر خود که ایجاد کردید، کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۴۸۰ سرویس *NIC Teaming*

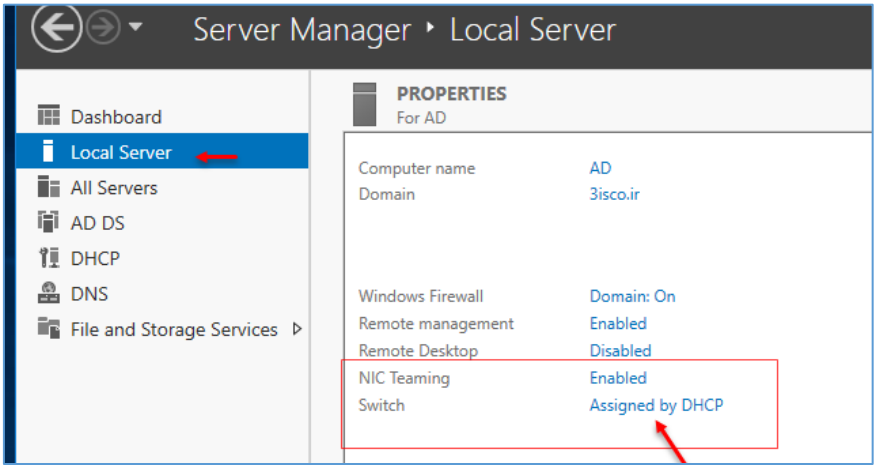
به مانند شکل ۸-۴۷۱، اگر شماره‌ی Vlan خاصّی تعریف کردید، می‌توانند گزینه‌ی Specific VLAN را انتخاب و نام شماره‌ی Vlan را وارد کنید تا سرور با سوئیچ ارتباط برقرار کند و دچار مشکل نشود.

www.takbook.com



شکل ۸- ۴۸۱ سرویس *NIC Teaming*

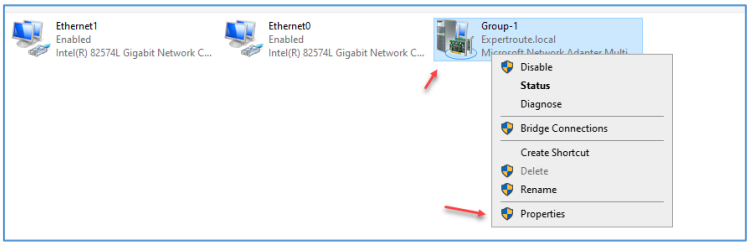
بعد از انجام عملیّات بالا، به مانند شکل ۸-٤۸۲، دوباره وارد Local Server شوید و اگر به قسمت NiC Teaming توجّه کنید،وضعیت آن به Enabled تغییر کرده است و برای اینکه آدرس IP سرور را ست کنید باید بر رویAssigned by DHCP کلیک کنید.



شکل ۸- ۴۸۲ سرویس *NIC Teaming*

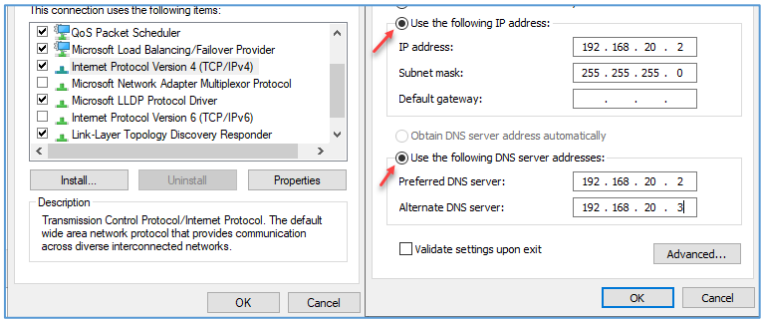
در شکل ۸-٤۸۳، دو کارت شبکه را مشاهده می‌کنید، به همراه نام Switch که با هم ایجاد کردیم را مشاهده می‌کنید، برای اینکه آدرس IP سرور را Set کنید باید بر روی Switch کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.

www.takbook.com



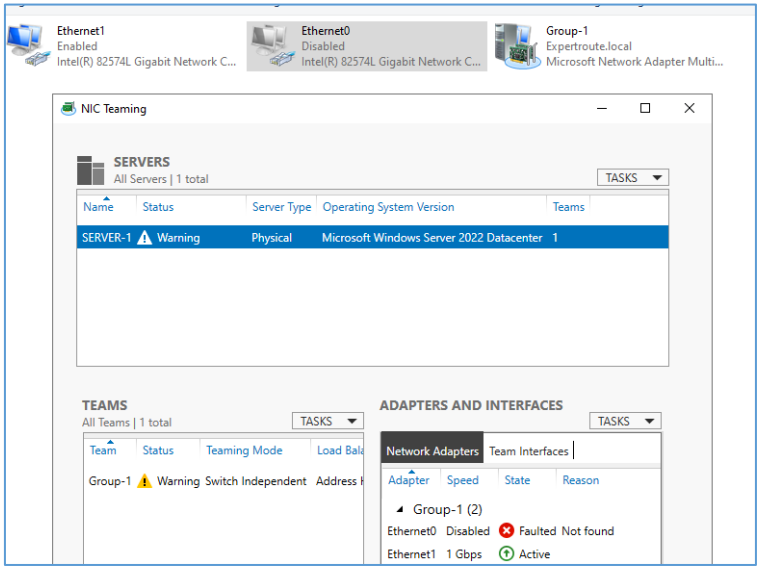
شکل ۸- ۴۸۳ سرویس NIC Teaming

به مانند شکل ۸-٤٨٤، آدرس سرور را وارد و بر روی OK کلیک کنید.



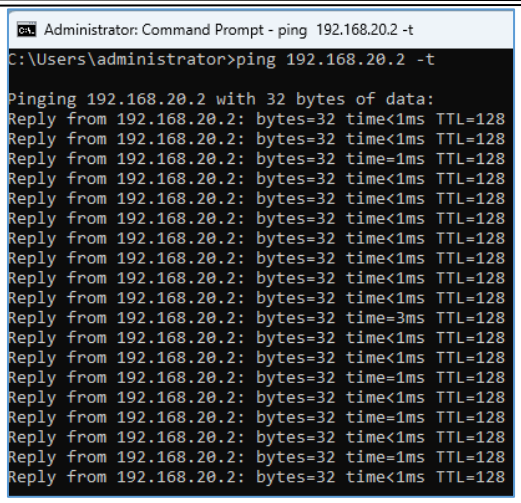
شکل ۸- ۴۸۴ سرویس NIC Teaming

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 ۸-٤٨٥ و شکل ۸-٤٨٦، Ping سرور مورد نظر، یعنی سرور Server-1 را مشاهده می‌کنید که هیچگونه Time out مشاهده نشده است.



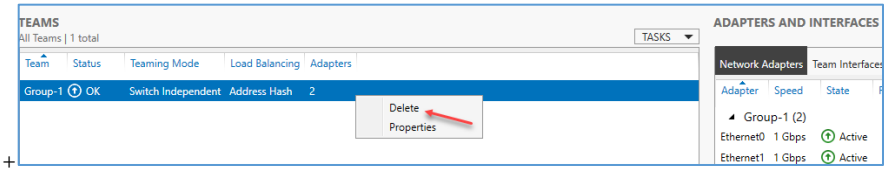
شکل ۸- ۴۸۵ سرویس NIC Teaming

www.takbook.com



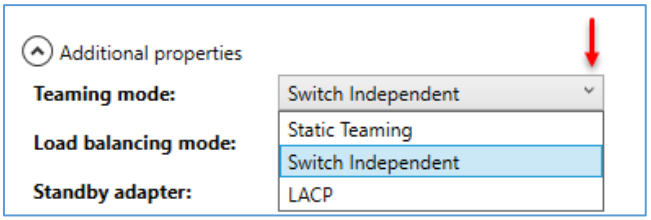
شکل ۸- ۴۸۶ سرویس NIC Teaming

تا اینجا، کار این سرویس را فرا گرفتیم و حال می‌خواهیم این سرویس را غیر فعّال کنیم که برای این کار باید به مانند شکل ۸–۴۸۷، در قسمت TEAMS بر روی Team مورد نظر خود کلیک راست کنیم و گزینه‌ی Delete را انتخاب کنیم.



شکل ۸- ۴۸۷ سرویس NIC Teaming

روش‌های دیگری به مانند شکل ۸–۴۸۸، مانند Static Teaming و LACP وجود دارد که این روش‌ها اگر انتخاب شوند باید سوئیچ‌هایی مربوط به آنها نیز در این حالت تنظیم شوند تا بتوانند با هم ارتباط برقرار کنند.



شکل ۸- ۴۸۸ سرویس NIC Teaming

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

www.takbook.com

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.

۱۶-۳-۸ سرویس Web Server (IIS)

یک ابزار قابل نصب بر روی ویندوز سرور که از طریق آن می‌توانیم سایت‌های خود را برای کاربران به اشتراک بگذاریم، در بعضی از سرویس‌هایی که با هم کار می‌کنیم، سرویس IIS به صورت اتوماتیک نصب می‌شود و وب سایت مورد نظر بر روی آن فعال می‌شود، اصولاً این سرویس بر روی ویندوز سرور اجرا می‌شود اما می‌توان با ابزاری به نام Mono آن را در لینوکس هم اجرا کرد.

توجه داشته باشید که وب‌سایت‌های که بر روی این سرویس پیاده‌سازی می‌شوند باید با زبان برنامه‌نویسی ASP نوشته شده باشند.

Internet Information Services (IIS) یک سرویس وب سرور است که توسط مایکروسافت توسعه یافته و به عنوان بخشی از سیستم‌عامل ویندوز سرور ارائه می‌شود. IIS به کاربران این امکان را می‌دهد که وب‌سایت‌ها و برنامه‌های وب را میزبانی کنند و به آن‌ها خدمات ارائه دهند.

ویژگی‌ها و قابلیت‌های IIS:

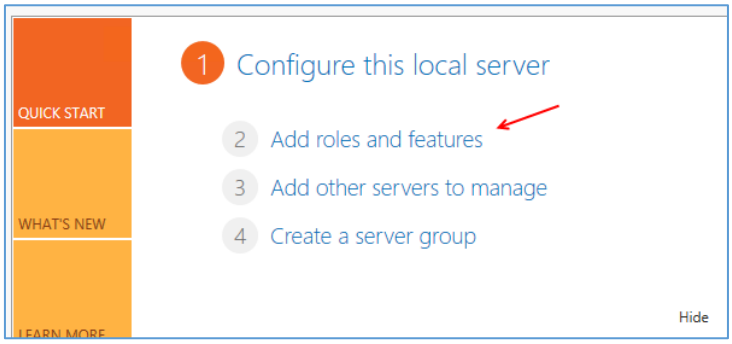
- پشتیبانی از پروتکل‌های مختلف: IIS از پروتکل‌های مختلفی مانند HTTP، HTTPS، FTP و FTPS پشتیبانی می‌کند، که این امکان را به مدیران می‌دهد که انواع مختلف خدمات را ارائه دهند.
- مدیریت آسان: IIS دارای یک رابط کاربری گرافیکی (GUI) است که به مدیران این امکان را می‌دهد تا وب‌سایت‌ها و تنظیمات سرور را به راحتی مدیریت کنند. همچنین می‌توان از PowerShell برای مدیریت و خودکارسازی وظایف استفاده کرد.
- امنیت: IIS از مکانیزم‌های امنیتی متعددی مانند احراز هویت، کنترل دسترسی، و SSL/TLS برای محافظت از وب‌سایت‌ها و داده‌ها استفاده می‌کند.
- مقیاس‌پذیری: IIS به راحتی می‌تواند با افزایش ترافیک وب‌سایت‌ها مقیاس‌پذیر شود و به مدیران این امکان را می‌دهد که منابع را بر اساس نیازها تنظیم کنند.
- پشتیبانی از برنامه‌های وب: IIS می‌تواند برنامه‌های تحت وب نوشته شده در زبان‌های مختلف (مانند ASP.NET، PHP، و غیره) را میزبانی کند. این ویژگی به توسعه‌دهندگان این امکان را می‌دهد که برنامه‌های وب خود را به راحتی در IIS مستقر کنند.
- تجزیه و تحلیل و گزارش‌گیری: IIS امکاناتی برای تجزیه و تحلیل ترافیک وب و گزارش‌گیری فراهم می‌کند که به مدیران این امکان را می‌دهد که عملکرد وب‌سایت‌ها را نظارت کنند.

در این بخش می‌خواهیم وب سرور (IIS) را روی ویندوز سرور راه اندازی کنیم تا بتوانیم وب سایت‌های خود را روی سرور ۲۰۲۵ اجرا کنیم، البته با نصب سرویس‌هایی قبلی که با هم بررسی کردیم سرویس

www.takbook.com

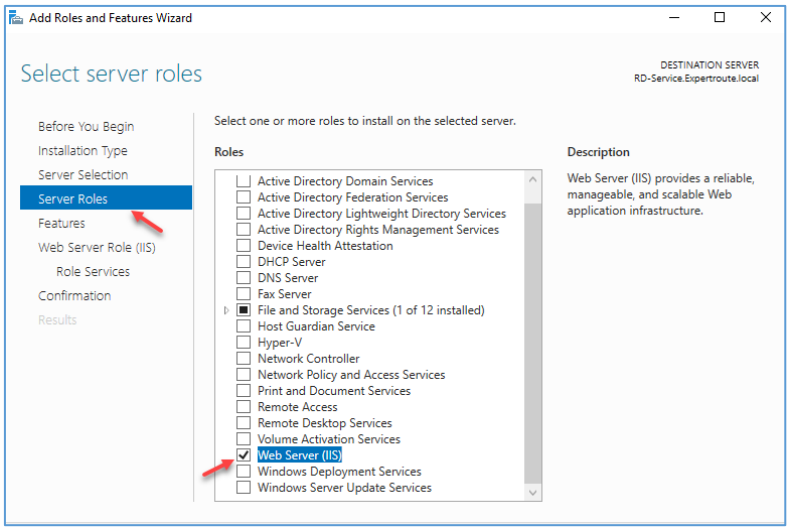
iiS به صورت خودکار روی سرور نصب شده است، ولی در این قسمت از اول این سرویس را بررسی خواهیم کرد و از نصب سرویس IIS و یا همان Web Server آغاز خواهیم کرد. توجه داشته باشید به همراه این سرویس سرویس DNS که قبلاً بررسی کرده‌ایم در این قسمت بررسی خواهد شد، چون این سرویس کاملاً با سرویس DNS در ارتباط است.

برای شروع کار به مانند شکل ۸–۴۸۹، وارد Server Manager شوید و بر روی Add roles and features کلیک کنید.



شکل ۸– ۴۸۹ *Web Server (IIS)*

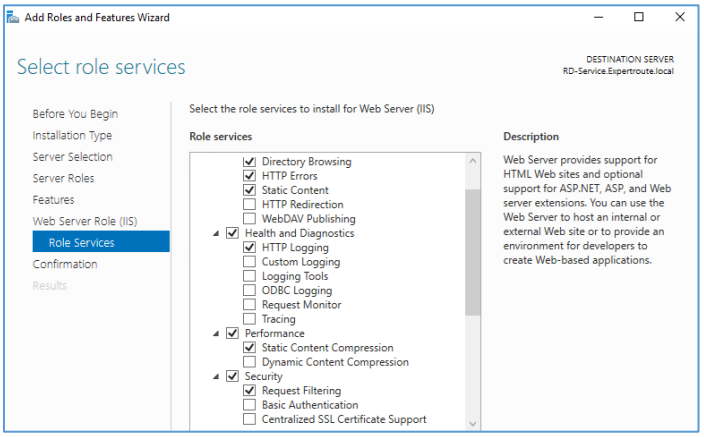
به مانند شکل ۸–۴۹۰، در قسمت Server Roles، گزینه Web Servers (IIS) را انتخاب کنید و در پنجره باز شده بر روی Add Features کلیک کنید.



شکل ۸– ۴۹۰ *Web Server (IIS)*

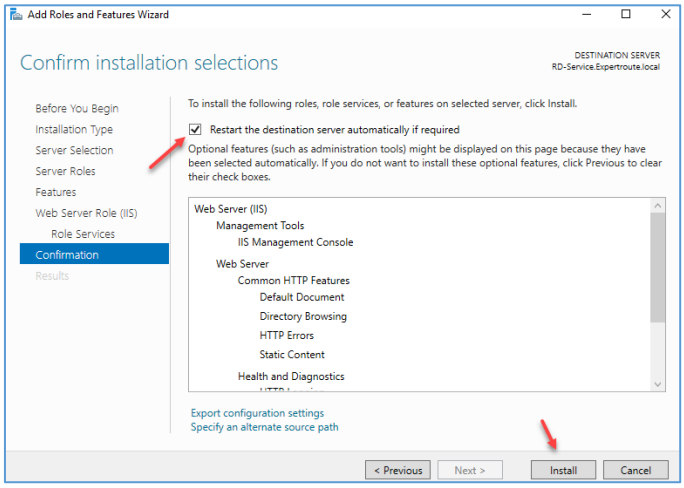
به مانند شکل ۸–۴۹۱، در قسمت Role Services تمام زیر مجموعه‌ی سرویس IIS را مشاهده می‌کنید که در حال حاضر به گزینه‌ای دست نزنید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۸- ۴۹۱ *Web Server (IIS)*

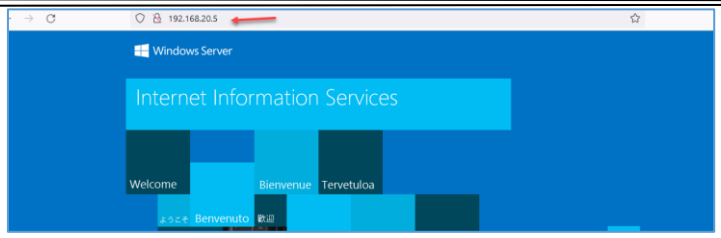
طبق شکل ۸-۴۹۲، تیک گزینه موردنظر را انتخاب و بر روی Install کلیک کنید.



شکل ۸- ۴۹۲ *Web Server (IIS)*

بعد از این که سرویس iiS را نصب کردید، باید تست کنیم که سرویس به درستی کار می‌کند و قابل اجرا است، برای این کار به مانند شکل ۸-۴۹۳، آدرس سرور را وارد کنید و یا اینکه از آدرس localhost در درون سرور استفاده کنید.

www.takbook.com

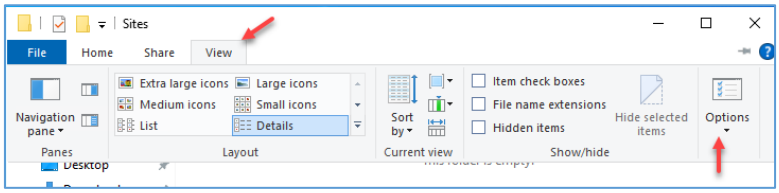


شکل ۸- ۴۹۳ *Web Server (IIS)*

همان‌طور که در شکل ۸-۴۹۳، مشاهده می‌کنید با اجرای آدرس بالا مشخص‌شده است که سرویس IIS به درستی در حال کار می‌باشد.

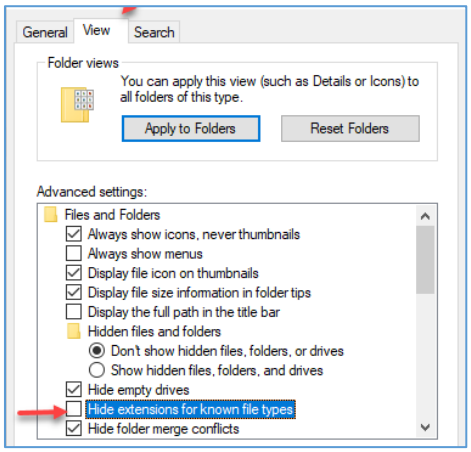
۸-۳-۱۶-۱ ایجاد وب سایت در IIS

برای شروع باید یک پوشه در یکی از درایوهای خود ایجاد و فایل‌های مربوط به وب سایت خود را در آن قرار دهیم، برای شروع فعلاً یک فایل HTML با نام Index.html را در پوشه‌ای با نام Sites در درایو C ایجاد می‌کنیم، توجه داشته باشید که برای اینکه پسوند یک فایل را مشاهده کنیم باید به مانند شکل ۸-۴۹۴، از قسمت View بر روی Options کلیک کنید.



شکل ۸- ۴۹۴ *ایجاد وب سایت در IIS*

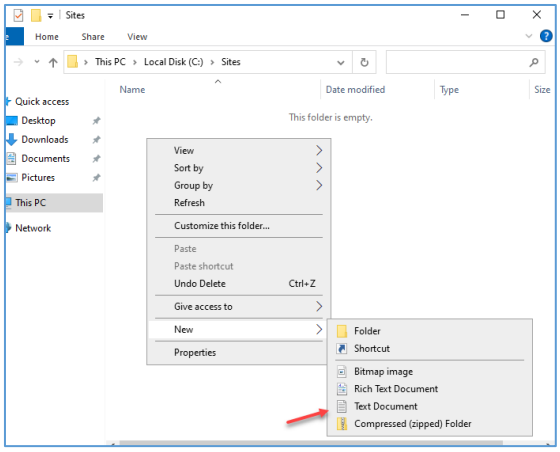
و به مانند شکل ۸-۴۹۵، از تب View تیک گزینه‌ی Hide extensions for known file types را بردارد.



شکل ۸- ۴۹۵ *ایجاد وب سایت در IIS*

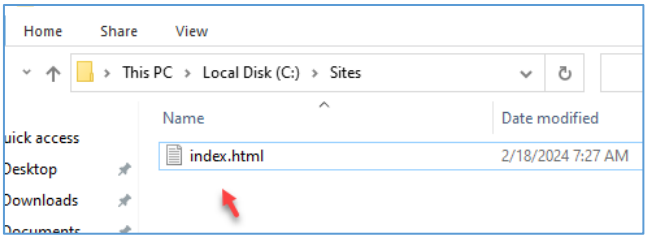
www.takbook.com

بعد از این کار به مانند شکل ۸-۴۹۶، یک فایل TXT ایجاد می‌کنیم و اسم ان را Index.html در نظر می‌گیریم.



شکل ۸- ۴۹۶ ایجاد وب سایت در IIS

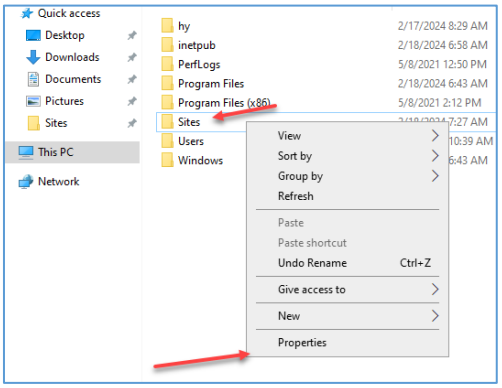
همان‌طور که در شکل ۸-۴۹۷، مشاهده می‌کنید فایل مورد نظر ایجاد شده است:



شکل ۸- ۴۹۷ ایجاد وب سایت در IIS

در ادامه باید به پوشه مورد نظر دسترسی بدهیم تا سرویس IIS بتواند به آن دسترسی داشته باشد.

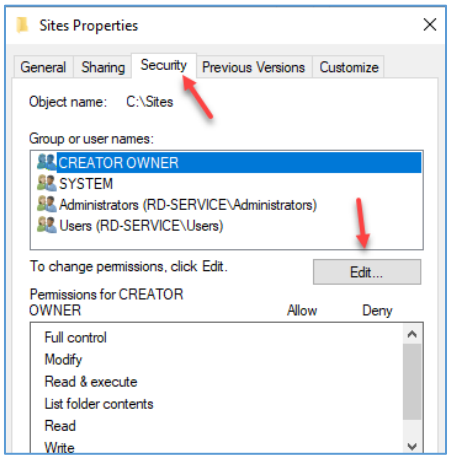
به مانند شکل ۸-۴۹۷، بر روی پوشه‌ی مورد نظر کلیک راست کنید و وارد Properties شوید.



شکل ۸- ۴۹۸ ایجاد وب سایت در IIS

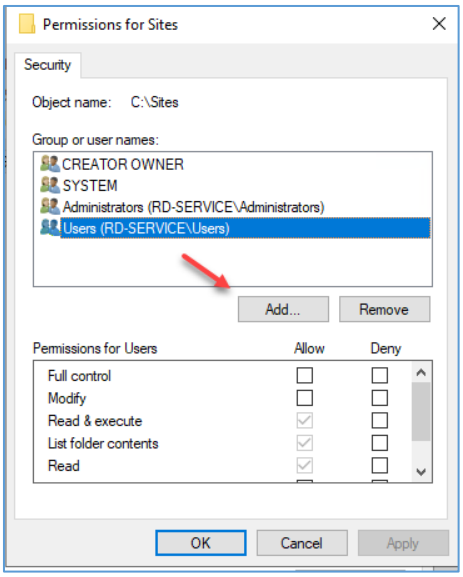
www.takbook.com

در شکل ۸-۴۹۹، وارد تب Security شوید و برای شروع کار بر روی Edit کلیک کنید تا شکل بعد ظاهر شود.



شکل ۸- ۴۹۹ ایجاد وب سایت در IIS

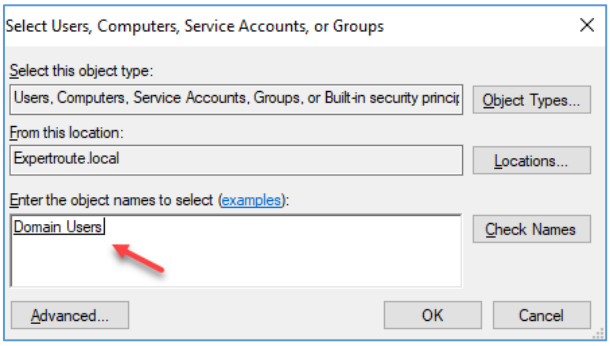
به مانند شکل ۸-۵۰۰، در این قسمت برای دسترسی همه کاربران عضو دومین به وب‌سایت موردنظر، به گروه Domain users، مجوز دسترسی به پوشه موردنظر را بدهیم، چون تمام کاربران به صورت پیش-فرض عضو این گروه می‌باشند برای انجام این کار بر روی Add کلیک کنید.



شکل ۸- ۵۰۰ ایجاد وب سایت در IIS

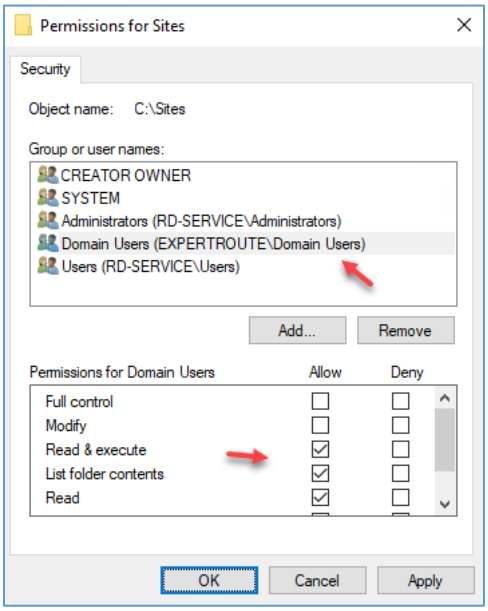
www.takbook.com

به مانند شکل ۸-۵۰۱، در این قسمت اگر کلمه domain use را وارد کنید و بعد بر روی Check Names کلیک کنید گروه Domain users به صورت خودکار به لیست اضافه می‌شود، بعد از این کار بر روی Ok کلیک کنید.



شکل ۸- ۵۰۱ ایجاد وب سایت در IIS

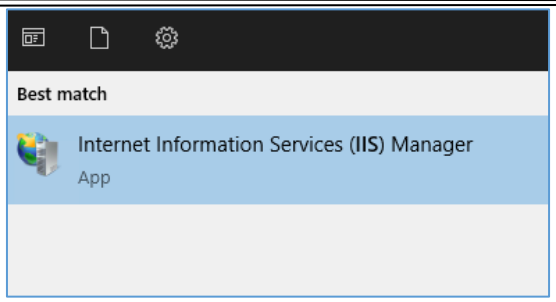
بعد از اضافه شدن گروه موردنظر در لیست، به مانند شکل ۸-۵۰۲، بر روی آن کلیک کنید تا مجوزهای آن مشخص شود، در مجوزهای موردنظر فقط گزینه Read را انتخاب کنید تا کاربران فقط بتوانند سایت موردنظر را اجرا کنند.



شکل ۸- ۵۰۲ ایجاد وب سایت در IIS

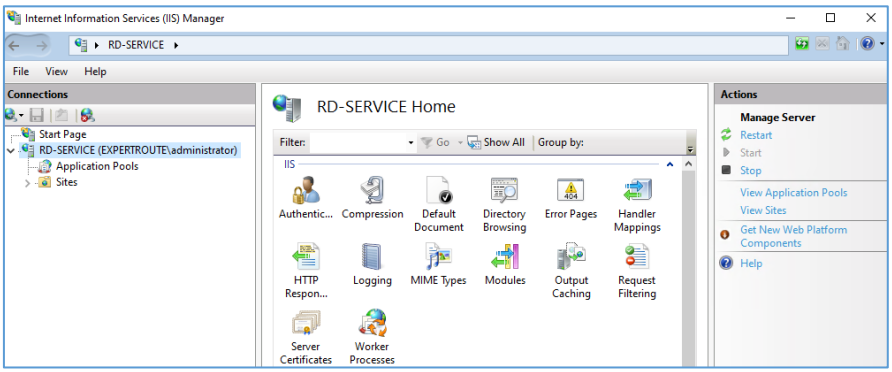
بعد از انجام عملیات قبلبه مانند شکل ۸-۵۰۳، وارد Search شوید و کلمه IIS را وارد کنید و در گزینه‌های موجود بر روی Internet Information Services کلیک کنید.

www.takbook.com



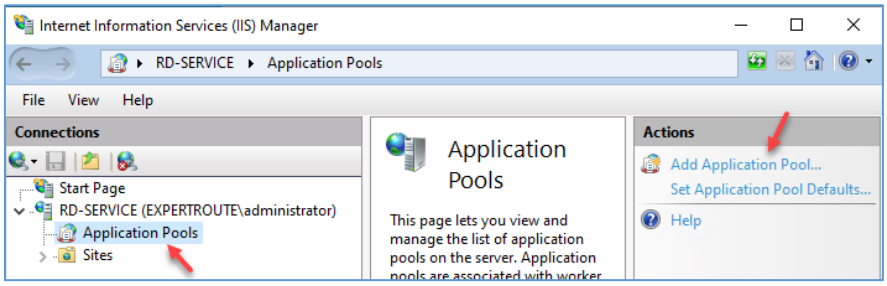
شکل ۸-۵۰۳ ایجاد وب سایت در IIS

همان‌طور که در شکل ۸-۵۰٤، مشاهده می‌کنید، سرویس IIS به صورت کامل اجرا شده است.



شکل ۸-۵۰۴ ایجاد وب سایت در IIS

برای شروع کار باید یک Application Pool ایجاد کنیم، Application Pool به یک محوطه‌ای گفته می‌شود که چندین سایت در آن قرار دارند و در کنار هم کار می‌کنند، اگر دو سایت در دو Pool مختلف قرار داشته باشند، هیچ ارتباطی با هم نخواهند داشت و نمی‌توانند با هم ارتباط برقرار کنند، برای شروع به مانند شکل ۸-۵۰۵، از سمت چپ بر روی Application Pools کلیک کنید و گزینه Add Application Pool را انتخاب کنید.

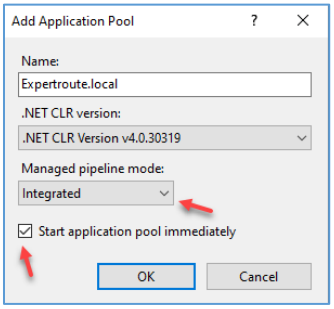


شکل ۸-۵۰۵ ایجاد وب سایت در IIS

در شکل ۸-۵۰٦، در قسمت Name نام دلخواه خود را وارد کنید و در قسمت Managed Pipeline Mode که مهمترین بخش می‌باشد گزینه Integrated را انتخاب کنید توجه داشته باشید که گزینه‌ی Integrated با

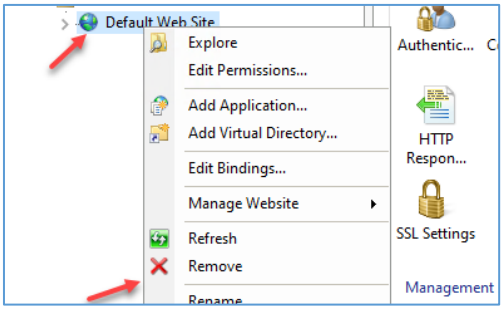
www.takbook.com

ASP.net هماهنگی کامل دارد و به خوبی کار می‌کند. و اگر تیک گزینه آخر را انتخاب کنید این Pool بعد از ایجاد شروع به کار می‌کنید و Start می‌شود.



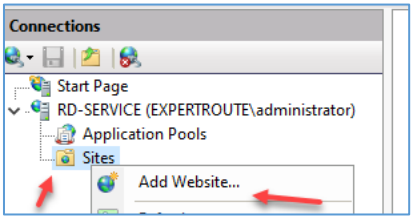
شکل ۸- ۵۰۶ ایجاد وب سایت در IIS

بعد از ایجاد Application Pool وارد بخش Site می‌شویم و به مانند شکل ۸-۵۰۷، وب سایت پیش‌فرض با نام Default Web Site وجود دارد که در این قسمت آن را حذف می‌کنیم، بر روی آن کلیک راست کنید و گزینه Remove را انتخاب و بر روی Yes کلیک کنید.



شکل ۸- ۵۰۷ ایجاد وب سایت در IIS

بعد از حذف سایت پیش‌فرض به مانند شکل ۸-۵۰۸، بر روی Site مجدداً کلیک راست کنید و بر روی Add Website کلیک کنید تا شکل ۸-۵۰۹، ظاهر شود.



شکل ۸- ۵۰۸ ایجاد وب سایت در IIS

در شکل ۸-۵۰۹، به ترتیب شماره‌های مشخص‌شده قسمت‌های مختلف را بررسی می‌کنیم:

در قسمت شماره‌ی یک باید نام دلخواه وب سایت خود را وارد کنید.

www.takbook.com

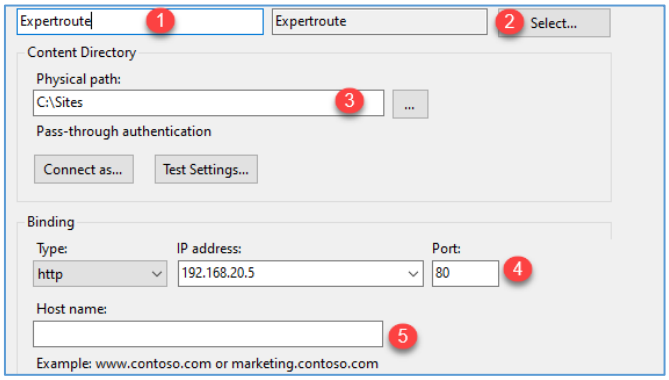
در قسمت Application Pool که بسیار مهم می‌باشد، قسمت شماره‌ی دو، باید Application Pool که قبلاً با نام Expertroute.local ایجاد کردیم را با کلیک بر روی Select انتخاب کنید.

در قسمت شماره‌ی سه، Physical Path، باید آدرس وب سایت خود را در شبکه و یا درایو موردنظر خودتون مشخص کنید، این آدرس را قبلاً ایجاد کردیم و دسترسی‌های مشخص را به آن تخصیص دادیم.

در قسمت شماره چهار شما باید نوع پروتکل و آدرس سرور را انتخاب کنید و شماره پورت را بر روی ۸۰ قرار دهید که این شماره پیش‌فرض برای سرویس IIS می‌باشد، یعنی تمام وب‌سایت‌هایی که شما در اینترنت باز میکنید به صورت پیش فرض بر روی پورت 80(HTTP) و 443 (HTTPS) هستند.

در قسمت شماره‌ی پنج، Host Name، باید آدرس وب سایت خود را مشخص کنیم که فعلاً کاری با این قسمت نداریم و در قسمت بعدی این موضوع را بررسی می‌کنیم.

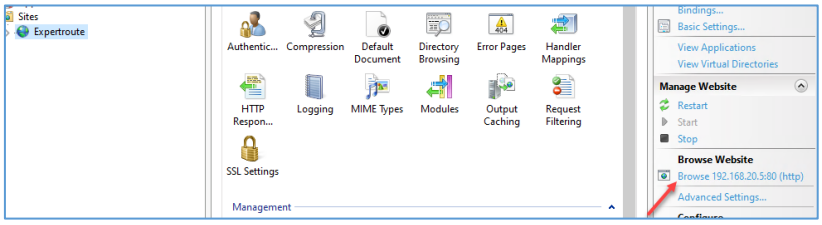
در پایین صفحه تیک گزینه‌ی Start Website Immediately را انتخاب کنید تا سایت مورد نظر شروع به کار کند.



شکل ۸- ۵۰۹ایجاد وب سایت در IIS

بعد از انجام عملیات بالا بر روی Ok کلیک کنید تا وب سایت موردنظر ایجاد شود.

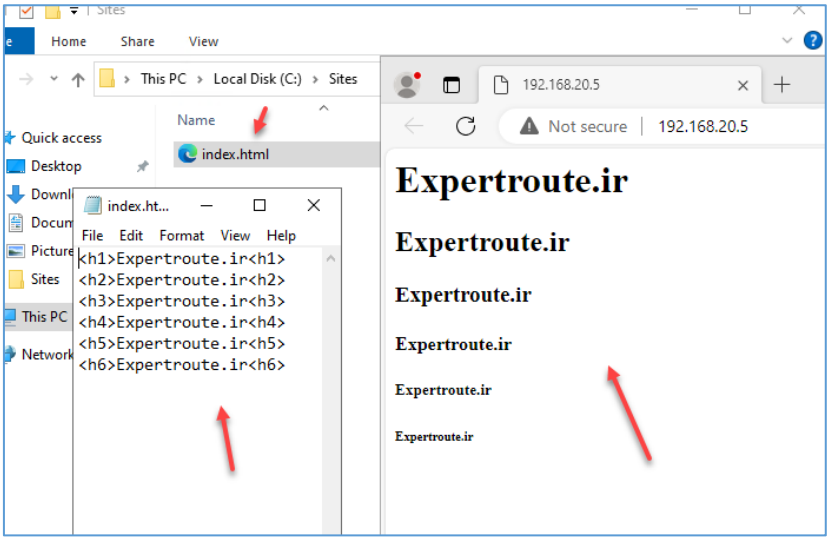
همان‌طور که درشکل ۸-۵۱۰، مشاهده می‌کنید، وب سایت موردنظر به درستی ایجاد شده است، برای اجرای آن از سمت راست بر روی Browse 192.168.20.5:80 کلیک کنید و یا وارد Internet Explorer شوید و آدرس را در Address bar وارد کنید.



شکل ۸- ۵۱۰ایجاد وب سایت در IIS

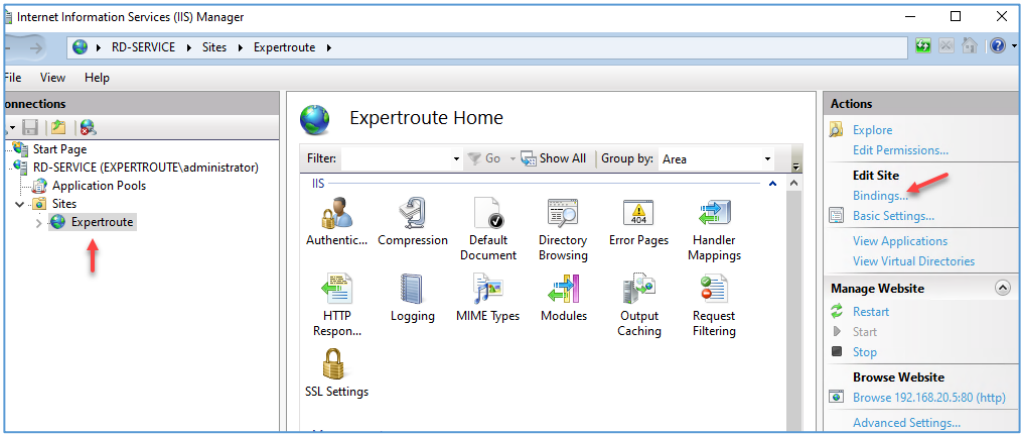
www.takbook.com

همان‌طور که در شکل ۸-۵۱۱ مشاهده می‌کنید وب سایت موردنظر به درستی اجرا شده است، توجه داشته باشید که در فایل Index.html چند کد html وارد کردیم که سایت مورد نظر را به این شکل نشان دهد.



شکل ۸- ۵۱۱ایجاد وب سایت در IIS

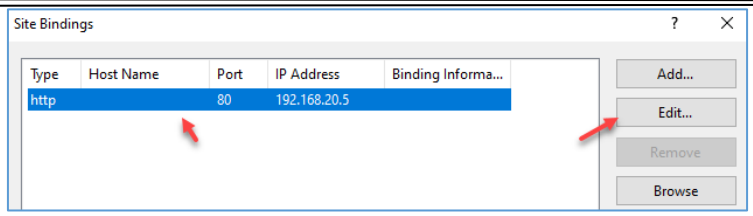
حالا می‌خواهیم از طریق آدرس، وب سایت مورد نظر را اجرا کنیم، مثلاً با وارد کردن آدرس www.expertroute.ir وب سایت موردنظر باز شود، برای انجام این کار سایت مورد نظر را طبق شکل ۸-۵۱۲، انتخاب کنید و بر روی Bindings کلیک کنید.



شکل ۸- ۵۱۲ایجاد وب سایت در IIS

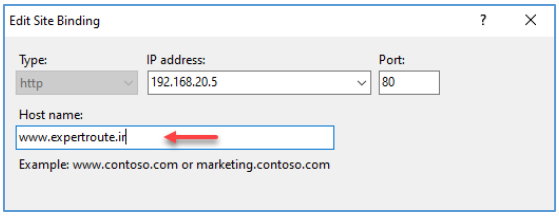
در شکل ۸-۵۱۳، آدرس مورد نظر را انتخاب کنید و بر روی Edit کلیک کنید.

www.takbook.com



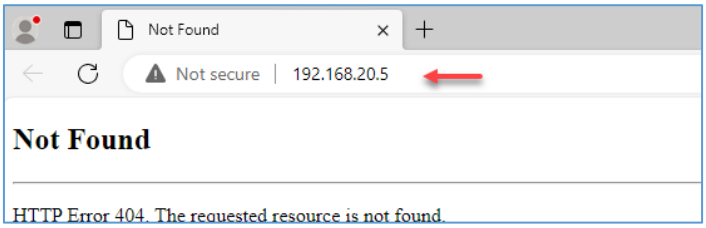
شکل ۸-۵۱۳ ایجاد وب سایت در IIS

در شکل ۸-۵۱٤، در قسمت Host name نام وب سایت خود را وارد کنید که در این قسمت آدرس www.3isco.ir وارد شده است، بعد از وارد کردن اطلاعات موردنظر بر روی ok کلیک کنید.



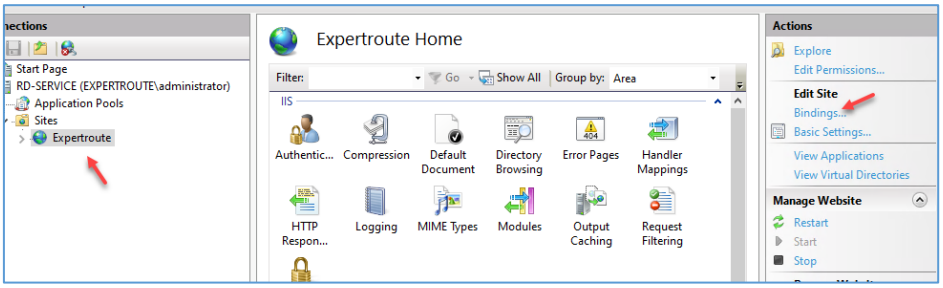
شکل ۸-۵۱۴ ایجاد وب سایت در IIS

نکته: بعد از این کار دیگر نمی‌توانید از طریق آدرس IP به وب سایت موردنظر دسترسی داشته باشید، همان‌طور که در شکل ۸-۵۱۵، مشاهده می‌کنید، با اجرای IP موردنظر هیچ صفحه‌ای برای نمایش ظاهر نشد.



شکل ۸-۵۱۵ ایجاد وب سایت در IIS

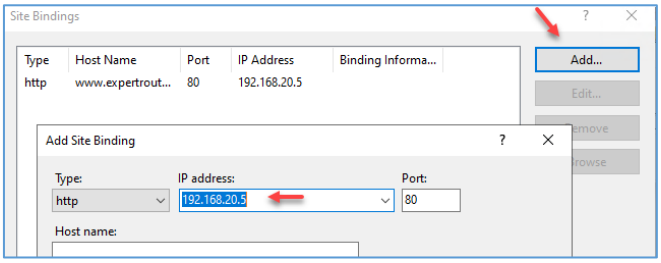
برای حل این مشکل به مانند شکل ۸-۵۱٦، دوباره به قسمت Bindings مراجعه می‌کنیم.



شکل ۸-۵۱۶ ایجاد وب سایت در IIS

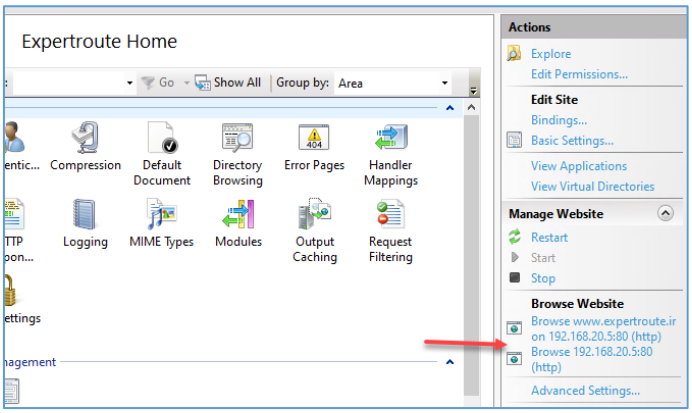
www.takbook.com

به مانند شکل ۸-۵۱۷، بر روی ADD کلیک کنید و در پنجره باز شده در قسمت Ip address باید آدرس سرور را انتخاب کنید و بر روی ok کلیک کنید، توجه کنید پورت را تغییر ندهید، بعد از این کار با آدرس IP هم می‌توانید سایت خود را اجرا کنید.



شکل ۸-۵۱۷ ایجاد وب سایت در IIS

به مانند شکل ۸-۵۱۸، اگر به قسمت Browse Website هم توجه کنید دو گزینه ایجاد شده است.

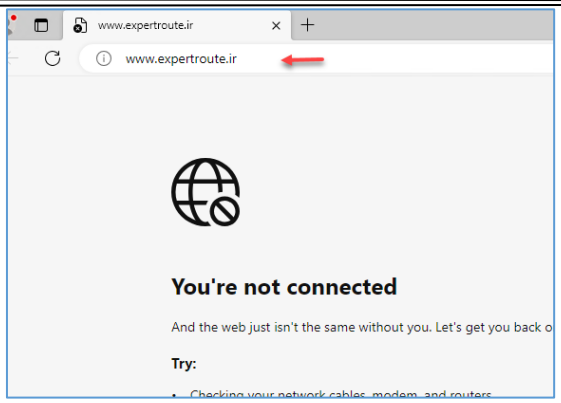


شکل ۸-۵۱۸ ایجاد وب سایت در IIS

خوب حالا می‌خواهیم وب سایت را با آدرس www.3isco.ir اجرا کنیم، وارد Browser می‌شویم آدرس موردنظر را اجرا می‌کنیم.

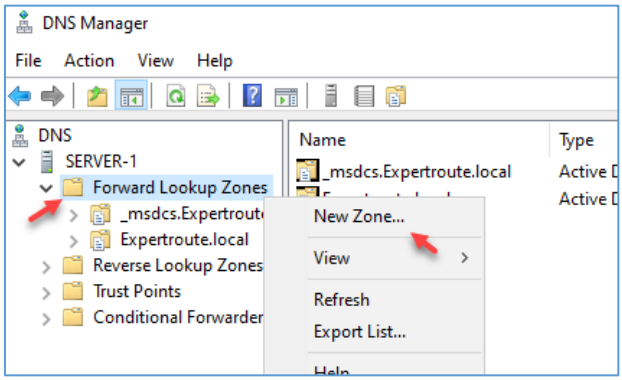
همان‌طور که در شکل ۸-۵۱۹ مشاهده می‌کنید با اجرای آدرس موردنظر با پیغام خطای This page can't… مواجه شدیم که این مشکل به خاطر این است که سرور آدرس www.expertroute.ir را نمی‌شناسد، همان‌طور که قبلاً گفتیم سرویس DNS کار بررسی آدرس و IP را انجام می‌دهد و باید در این سرویس تعریف شود.

www.takbook.com



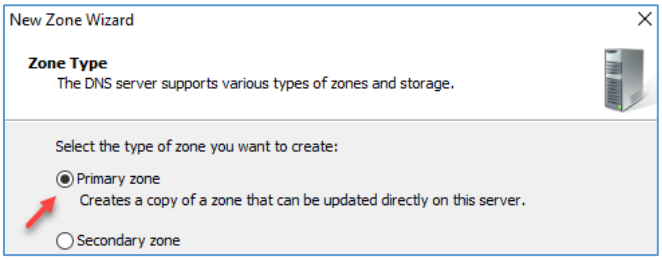
شکل ۸- ۵۱۹/ایجاد وب سایت در IIS

برای اینکه این مشکل را حل کنیم باید به مانند شکل ۸-۵۲۰، وارد سرویس DNS شویم و یک Zone جدید برای دومین Expertroute.ir ایجاد کنیم، برای این کار بر روی Forward Lookup Zones کلیک راست کنید و گزینه‌ی New Zone را انتخاب کنید.



شکل ۸- ۵۲۰/ایجاد وب سایت در IIS

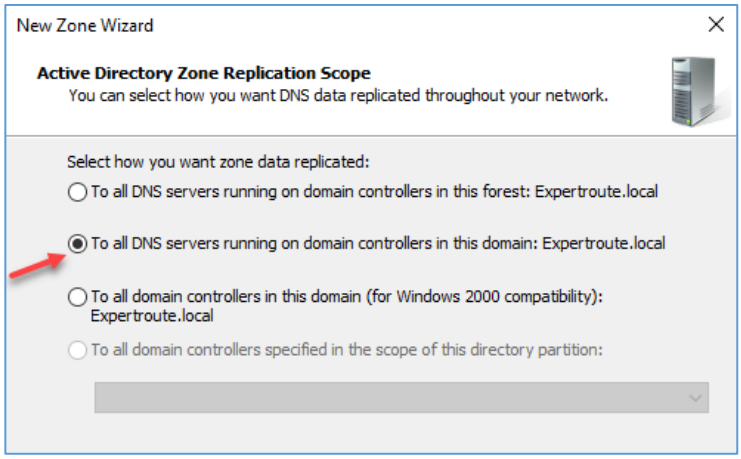
در شکل ۸-۵۲۱، گزینه‌ی Primary Zone را انتخاب کنید، توجه داشته باشید تمام این مراحل را در قسمت DNS Server توضیح دادیم.



شکل ۸- ۵۲۱/ایجاد وب سایت در IIS

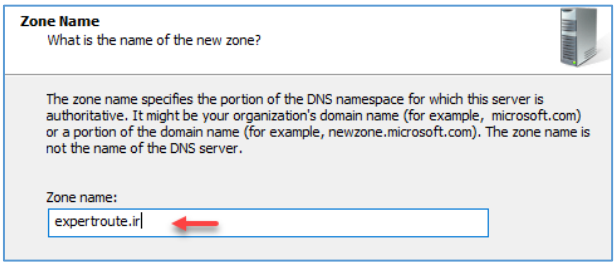
www.takbook.com

در شکل ۸-۵۲۲، گزینه‌ی مورد نظر را انتخاب و بر روی Next کلیک کنید.



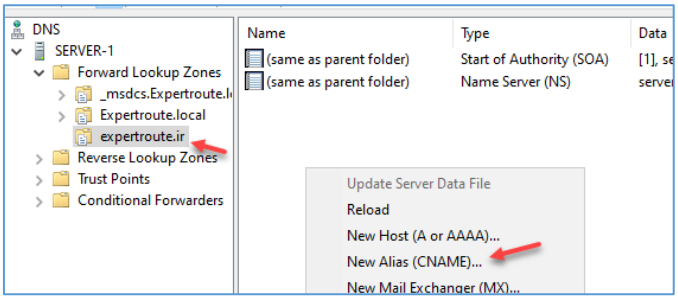
شکل ۸-۵۲۲ ایجاد وب سایت در IIS

در شکل ۸-۵۲۳، نام Zone خود را وارد و بر روی Next کلیک کنید، در صفحه‌ی بعد هم بر روی Next کلیک کنید و در آخر بر روی Finish کلیک کنید.



شکل ۸-۵۲۳ ایجاد وب سایت در IIS

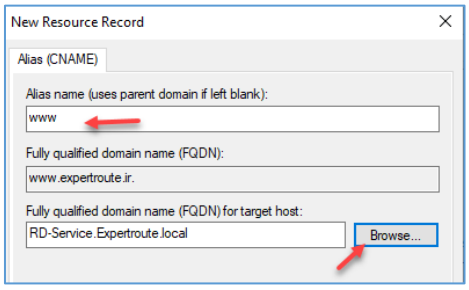
در شکل ۸-۵۲٤، وارد Zone مورد نظر شوید و در جای خالی کلیک راست کنید و گزینه‌ی CNAME را ایجاد کنید.



شکل ۸-۵۲۴ ایجاد وب سایت در IIS

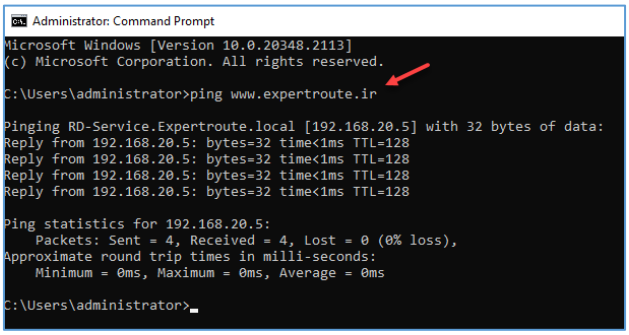
www.takbook.com

در این صفحه و در قسمت Alias Name کلمه www را وارد کنید که همزمان در قسمت Fully Qualified آدرس www.expertroute.ir به صورت خودکار درج می‌شود، در قسمت Host بر روی Browse کلیک کنید و در صفحه باز شده وارد دومین Expertroute.local که قبلاً ایجاد کردیم شوید و کامپیوتر سرور که بر روی آن سرویس IIS فعال است را انتخاب کنید این کار به این منظور است که کاربر بعد از اجرای آدرس www.expertroute.ir به کدام کامپیوتر هدایت شود. بر روی ok کلیک کنید.



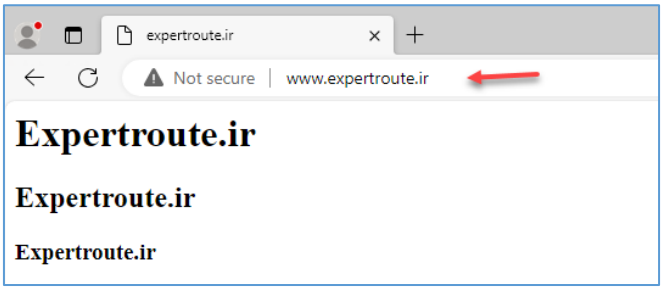
شکل ۸- ۵۲۵ ایجاد وب سایت در IIS

اگر به مانند شکل ۸–۵۲۶، وارد CMD شوید و آدرس سایت را Ping کنید نتیجه درست را نشان می‌دهد.



شکل ۸- ۵۲۶ ایجاد وب سایت در IIS

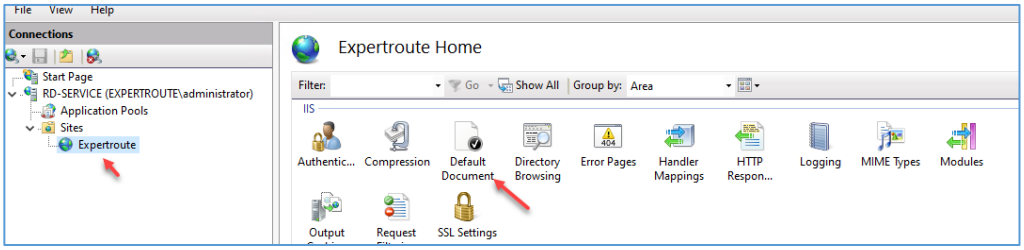
همان‌طور که در شکل ۸–۵۲۷، مشاهده می‌کنید، بعد از انجام تنظیمات موردنظر در سرویس DNS سایت موردنظر از طریق سرویس DNS اجرا شده است.



شکل ۸- ۵۲۷ ایجاد وب سایت در IIS

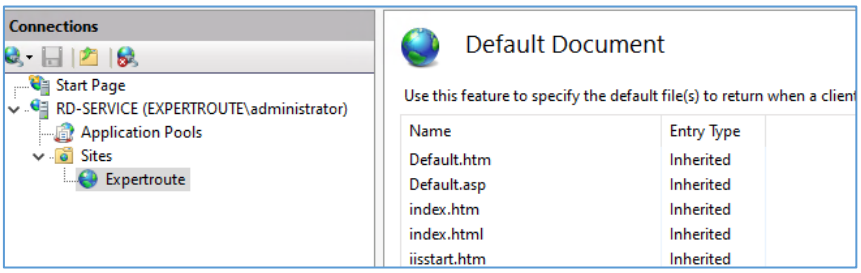
www.takbook.com

تا این قسمت سرویس IIS را فعال و توانستیم سایت خود را راه‌اندازی و از طریق IP و آدرس اجرا کنیم. یکی سری ابزارها در IIS وجود دارد که با هم نگاهی به آنها می‌اندازیم، اگر به مانند شکل ۸-۵۲۸، بر روی سایت خود کلیک کنید، ابزارهایی برای نمایش داده خواهد شد که هر کدام یک کار بخصوص را انجام می‌دهند، برای شروع وارد Default Document شوید.



شکل ۸- ۵۲۸ ایجاد وب سایت در IIS

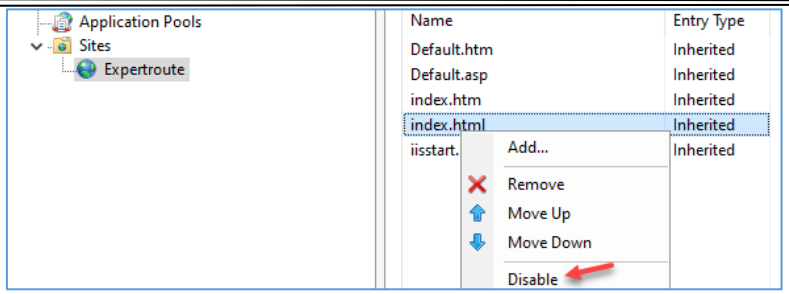
اگر به شکل ۸-۵۲۹، توجه کنید، چندین فایل را مشاده می‌کنید که این فایل‌ها اگر در Root سایت شما قرار داشته باشن به صورت پیش‌فرض این فایل‌ها باز می‌شوند، مثلاً سایت ما با آدرس www.expertroute.ir به صورت www.expertroute.ir/index.html باز می‌شود ولی شما آدرس index.html را مشاهده نمی‌کنید چون اسم آن در لیست زیر وجود دارد. که اگر یادتان باشد ما یک فایل index.html در پوشه‌ی سایت خود ایجاد کرده بودیم.



شکل ۸- ۵۲۹ ایجاد وب سایت در IIS

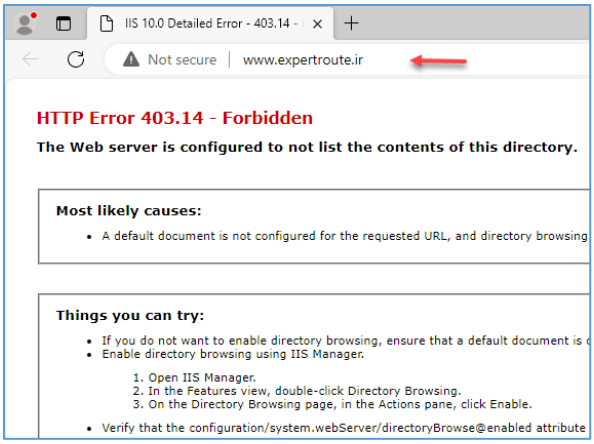
اگر به مانند شکل ۸-۵۳۰، بر روی Index.html کلیک راست کنید و گزینه‌ی Disable را انتخاب کنید سایت شما اجرا نخواهد شد.

www.takbook.com



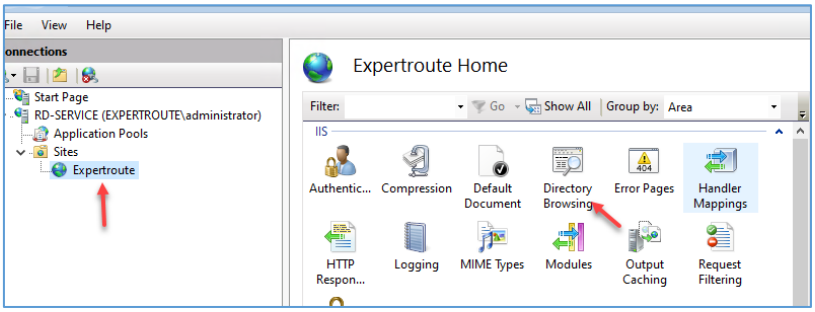
شکل ۸- ۵۳۰ایجاد وب سایت در IIS

برای چک کردن این موضوع سایت را اجرا می‌کنیم، که در شکل ۸-۵۳۱، مشاهده می‌کنید سایت از دسترس خارج شده است و دسترسی محدود شده است، اگر دوباره فعال کنید سایت مورد نظر اجرا خواهد شد.



شکل ۸- ۵۳۱ایجاد وب سایت در IIS

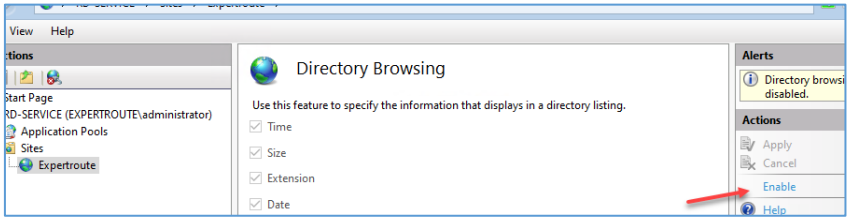
به مانند شکل ۸-۵۳۲، ابزار دیگری وجود دارد به نام به نام Directory Browsing که می‌توانید با فعال کردن آن اطلاعات سایت خود را به صورت لیست شده نشان دهید که اصولاً این مورد در ریشه‌ی اصلی سایت پیشنهاد نمی‌شود چون یک ضعف امنیتی بزرگ است.



شکل ۸- ۵۳۲ایجاد وب سایت در IIS

www.takbook.com

به مانند شکل ۸-۵۳۳، وارد Directory Browsing شوید و بر روی Enable کلیک کنید تا این ویژگی فعال شود.



شکل ۸-۵۳۳ ایجاد وب سایت در IIS

بعد از فعال کردن آن اگر سایت را باز کنید اطلاعات به صورت شکل ۸-۵۳٤، نمایش داده خواهد شد و لیست فایلهایی که در پوشه سایت قرار دادیم را مشاهده می‌کنید، اگر به فایل index توجه کنید یک عدد ۱ هم برای آن قرار دادیم تا سایت به صورت لیست نمایش داده شود، منظورمان همان index.hdml است که در قسمت قبل توضیح دادیم.



شکل ۸-۵۳۴ ایجاد وب سایت در IIS

۸-۳-۱۷ سرویس FTP

File Transfer Protocol یا به اختصار FTP یک پروتکل برای انتقال فایل در شبکه است هر چند در حال حاضر از پروتکل قدرتمن‌تر SFTP استفاده می‌شود ولی هستند جاهایی که از این پروتکل استفاده می‌کنند و در این قسمت می‌خواهیم نحوه‌ی راه‌اندازی را با هم بررسی کنیم.

اجزای اصلی FTP

- سرور FTP: سیستمی است که فایل‌ها را ذخیره کرده و امکان دسترسی کاربران به آن‌ها را فراهم می‌کند.
- کلاینت FTP: برنامه‌ای است که کاربران از طریق آن به سرور FTP متصل می‌شوند و عملیات انتقال فایل‌ها را انجام می‌دهند.

www.takbook.com

نحوه عملکرد

سرویس FTP از دو نوع ارتباط استفاده می‌کند:

- ارتباط کنترلی (Control Connection): این ارتباط برای ارسال دستورات بین کلاینت و سرور استفاده می‌شود.
- ارتباط داده‌ای (Data Connection): این ارتباط برای انتقال فایل‌های واقعی بین کلاینت و سرور استفاده می‌شود.

انواع حالت‌های اتصال FTP

- Anonymous FTP: در این حالت، کاربر می‌تواند بدون نیاز به وارد کردن نام کاربری و رمز عبور خاص، به فایل‌های عمومی دسترسی داشته باشد.
- Authenticated FTP: در این حالت، کاربران باید با استفاده از نام کاربری و رمز عبور مشخص به سرور متصل شوند.

مزایا و معایب FTP

مزایا:

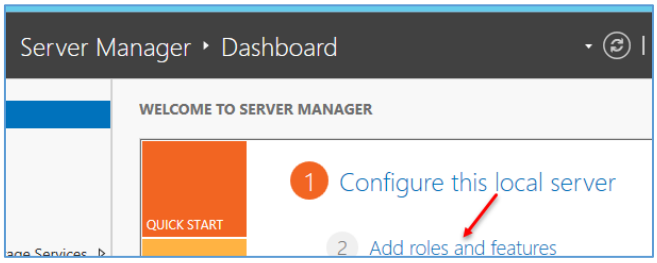
- سادگی و کارایی: برای انتقال فایل‌های بزرگ و همچنین دسترسی همزمان به چندین کاربر کارآمد است.
- قابلیت بازگشت در صورت خطا: در صورت بروز خطا در حین انتقال فایل، پروتکل FTP می‌تواند مجدداً از نقطه‌ای که انتقال متوقف شده، ادامه دهد.

معایب:

- امنیت پایین: FTP در حالت استاندارد از رمزگذاری استفاده نمی‌کند و اطلاعات (از جمله نام کاربری و رمز عبور) به صورت متنی ارسال می‌شوند، که ممکن است به سرقت اطلاعات منجر شود.
- پشتیبانی ضعیف از فایروال‌ها: به دلیل نیاز به باز کردن پورت‌های اضافی برای اتصال داده، ممکن است مشکلاتی در عبور از فایروال‌ها ایجاد کند.

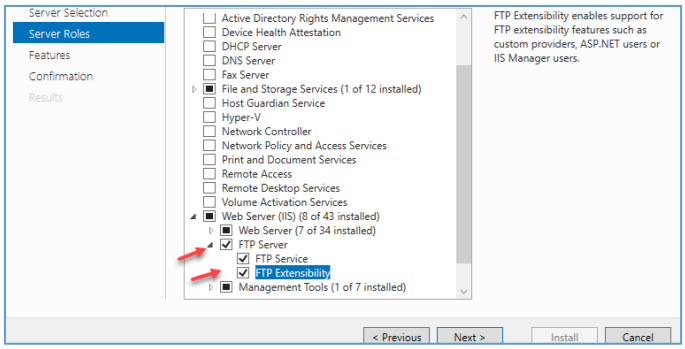
برای شروع کار وارد ویندوز سرور ۲۰۲۵ شوید و به مانند شکل ۸-۵۳۵، ابزار Server Manager را اجرا کنید و بر روی Add roles and features کلیک کنید.

www.takbook.com



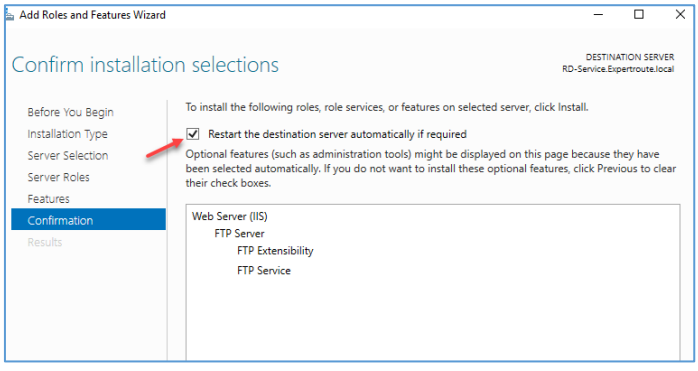
شکل ۸- ۵۳۵ سرویس FTP

در شکل ۸-۵۳۶، باید سرویس FTP را که زیر مجموعه‌ی سرویس IIS است انتخاب کنید، بعد از انتخاب بر روی Next کلیک کنید.



شکل ۸- ۵۳۶ سرویس FTP

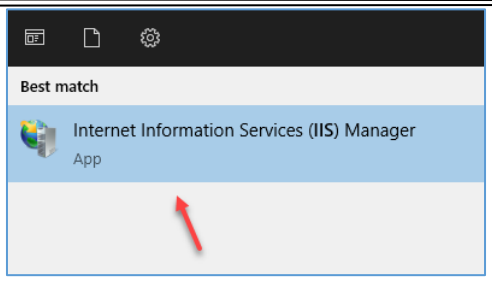
در شکل ۸-۵۳۷، تیک گزینه‌ی ...Restart the را انتخاب کنید و بر روی Install کلیک کنید، توجه داشته باشید که زمانی که گزینه‌ی ..Restart را انتخاب می‌کنید در صورت تشخیص، سرور مورد نظر به صورت اتوماتیک Restart خواهد شد وگرنه این کار انجام نمی‌گیرد.



شکل ۸- ۵۳۷ سرویس FTP

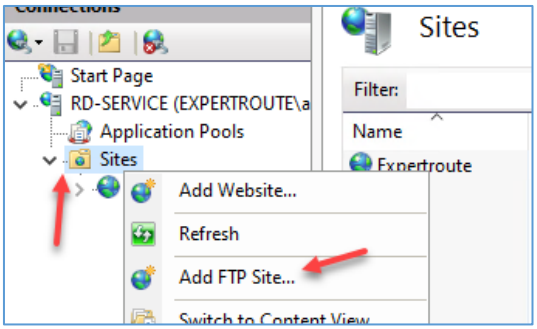
بعد از نصب سرویس به مانند شکل ۸-۵۳۸، وارد Search شوید و سرویس IIS را اجرا کنید.

www.takbook.com



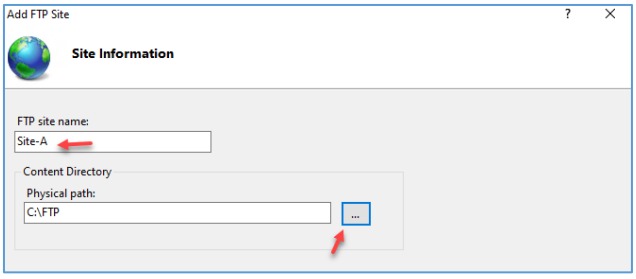
شکل ۸- ۵۳۸ سرویس FTP

همان‌طور که در شکل ۸-۵۳۹، مشاهده می‌کنید سرویس مورد نظر اجرا شده است، به مانند شکل برروی Sites کلیک راست کنید و گزینه‌ی Add FTP Site را انتخاب کنید.



شکل ۸- ۵۳۹ سرویس FTP

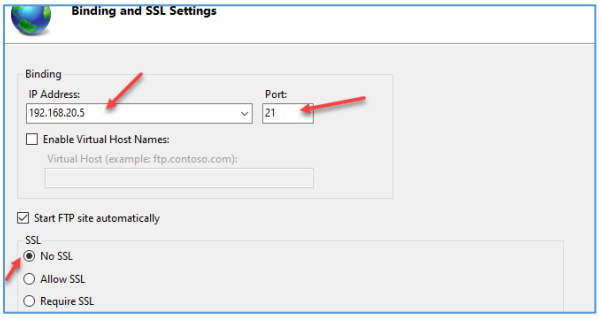
در شکل ۸-۵۴۰، نام FTP را به دلخواه وارد کنید و یک مسیر مناسب برای آن ایجاد و انتخاب کنید.



شکل ۸- ۵۴۰ سرویس FTP

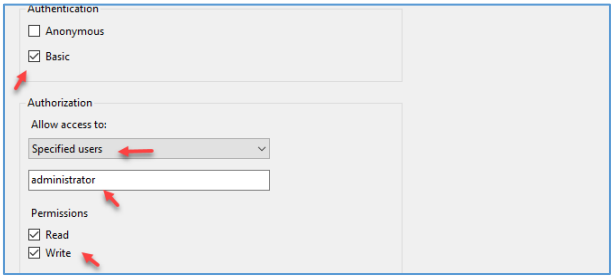
در شکل ۸-۵۴۱، پورت مربوط به سرویس FTP را مشاهده می‌کنید که می‌توانید آن را تغییر دهید ولی پورت پیش‌فرض آن ۲۱ است، در قسمت SSL می‌توانید پروتکل SSL را برای ارتباطFTP فعال کنید تا ارتباط به صورت امن انجام شود، در مورد ایجاد گواهینامه‌های SSL در قسمت Active Directory Certificate Service توضیحات ارائه شده است، در حال حاضر گزینه‌ی No SSL را انتخاب کنید و بر روی Next کلیک کنید.

www.takbook.com



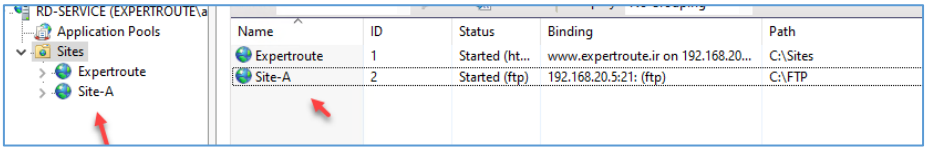
شکل ۸- ۵۴۱ سرویس FTP

در شکل ۸-۵٤۲، که مربوط به تایید هویت است گزینه‌ی Basic را انتخاب کنید و در قسمت Autorization گزینه‌ی Specified Users را انتخاب کنید و یک کاربر که برای دسترسی به FTP نیاز دارید را وارد کنید و تیک گزینه‌ی Read و Write را انتخاب کنید و بر روی Finish کلیک کنید.



شکل ۸- ۵۴۲ سرویس FTP

همان‌طور که در شکل ۸-۵٤۳، مشاهده می‌کنید FTP مورد نظر ایجاد شده است و حالا می‌توانیم به آن دسترسی داشته باشیم.



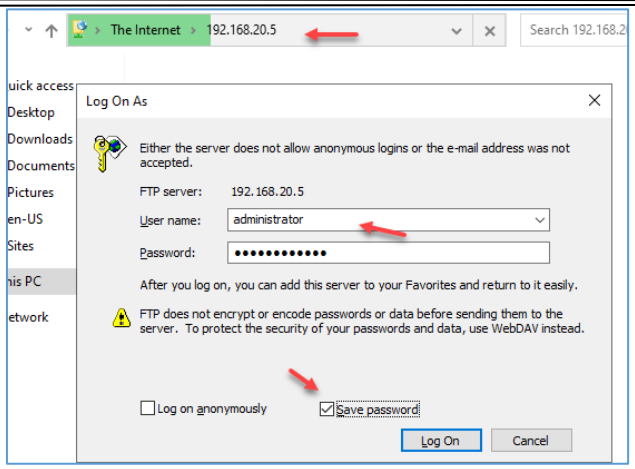
شکل ۸- ۵۴۳ سرویس FTP

برای تست این موضوع آدرس زیر را در یک فولدر اجرا کنید:

ftp://192.168.20.5/

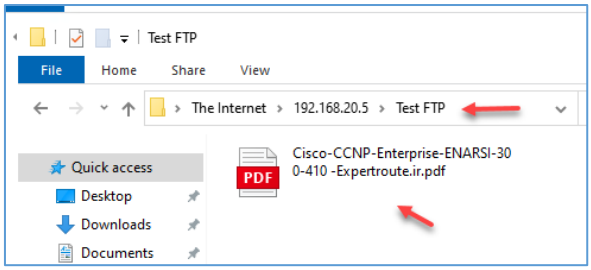
با اجرای این آدرس به مانند شکل ۸-۵٤٤، از شما نام کاربری و رمز عبور دریافت می‌شود که نام کاربری Administartor را برای آن در نظر گرفتیم و رمز عبور آن را هم وارد می‌کنیم، توجه داشته باشید که این نام کاربری نام کاربری Local مربوط به خود سرور است و ربطی به دامین ندارد.

www.takbook.com



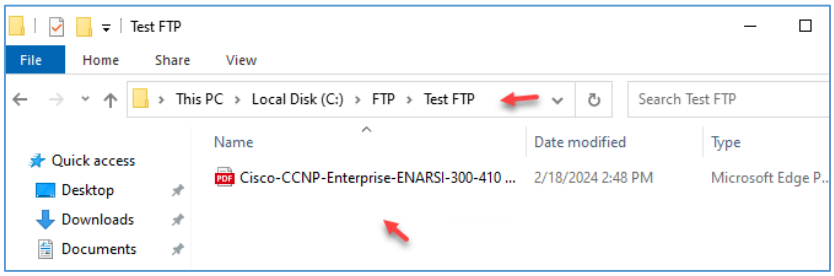
شکل ۸- ۵۴۴ سرویس FTP

بعد از باز شدن آدرس مورد نظر به راحتی می‌توانید فایل مورد نظر خود را به آدرس مشخص شده انتقال دهید، در شکل ۸-۵٤۵، یک پوشه با نام Test FTP ایجاد و فایل خود را در آن انتقال دادیم.



شکل ۸- ۵۴۵ سرویس FTP

به مانند شکل ۸-٥٤٦، اگر وارد پوشه مورد نظر در درایو C شوید این پوشه و فایل را مشاهده خواهید کرد.



شکل ۸- ۵۴۶ سرویس FTP

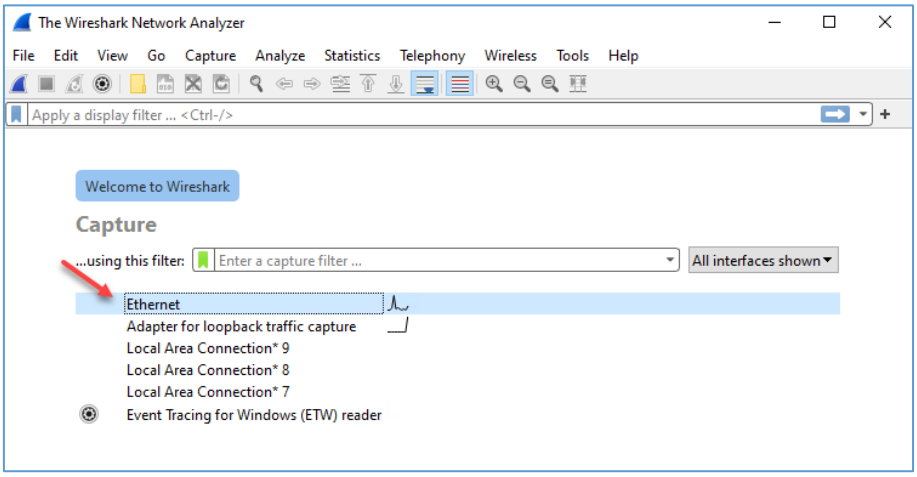
www.takbook.com

یک نکته مهم در استفاده از این سرویس وجود دارد و آن هم این است که این سرویس واقعاً ناامن است و برای اینکه این موضوع را درک کنید یک نرم‌افزار sniffing بر روی سرور نصب می‌کنیم و ارتباط پروتکل FTP را بررسی می‌کنیم.

می‌خواهیم از طریق نرم‌افزار Wireshark ارتباط بین سیستم‌ها را چک کنیم برای این کار از طریق لینک زیر بسته به نوع سیستم عامل نرم‌افزار را دانلود کنید:

https://www.wireshark.org/download.html

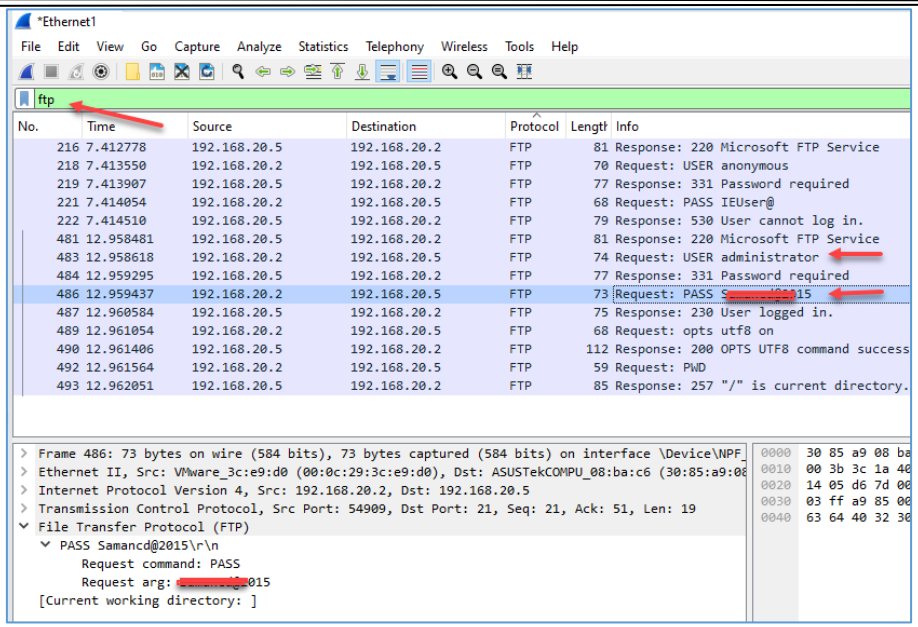
بعد از نصب نرم‌افزار آن را اجرا کنید و به مانند شکل ۸-۵۴۸، کارت شبکه‌ی اصلی سیستم خود را که بر روی آن آدرس IP مورد نظر را ست کردید انتخاب کنید.



شکل ۸- ۵۴۷ سرویس FTP

به مانند شکل ۸-۵۴۸، اگر در قسمت فیلتر کلمه‌ی FTP را وارد کنید، دقیقاً تمام ارتباطات مشخص شده است و اگر به خروجی شکل ۸-۵۴۸، توجه کنید دقیقاً نام کاربری Administrator به همراه رمز عبور مشخص شده است و به همین خاطر می‌گویند که ارتباط FTP بسیار ناامن است.

www.takbook.com



شکل ۸- ۵۴۸ سرویس *FTP*

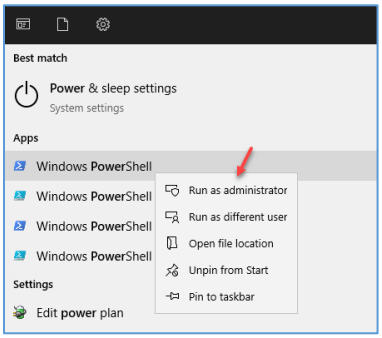
۸-۳-۱۸ سرویس SFTP

همان‌طور که در قسمت قبلی مشاهده کردید سرویس FTP از امنیت خوبی برخوردار نبود و به راحتی با یک نرم‌افزار Sniffing می‌شود نام کاربری و رمز عبور را پیدا کرد، برای اینکه این مشکلات امنیتی حل شود باید سرویس SFTP را راه‌اندازی کنیم، این سرویس از Open-SSH استفاده می‌کند و امنیت بسیار بالایی دارد و به راحتی نمی‌توان به آن نفوذ کرد.

سرویسی که در این قسمت می‌خواهیم بررسی کنیم سرویس (SFTP(SSH File Transfer Protocol است، با استفاده از این پروتکل تمام اطلاعات به صورت امن انتقال داده خواهند شد و دیگر هیچ دسترسی به اطلاعات آن توسط مهاجم وجود نخواهد داشت، توجه داشته باشید که این پروتکل از پروتکل SSH قدرت گرفته است و برای قابلیت انتقال فایل به صورت امن طراحی شده است.

برای اینکه این پروتکل را فعال کنیم باید به صورت زیر عمل کنیم، اول از همه سرویس Powersheel را با استفاده از کاربر Administrator به مانند شکل ۸-۵۴۹، اجرا کنید:

www.takbook.com

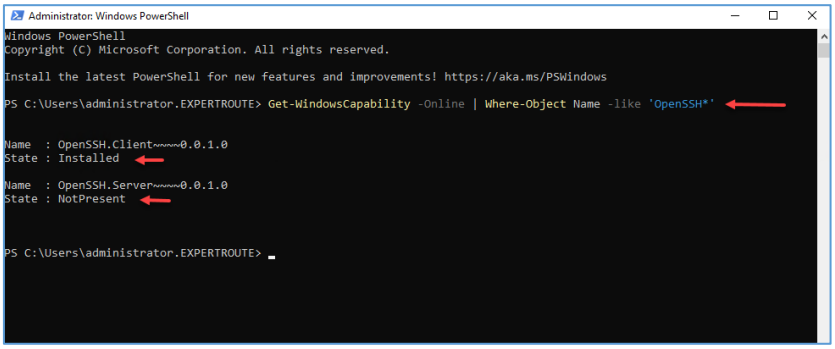


شکل ۸- ۵۴۹ سرویس SFTP

می‌خواهیم با استفاده از دستورات PowerShell این سرویس را نصب کنیم، برای این کار اول بررسی می‌کنیم که آیا سرویس OpenSSH بر روی ویندوز سرور نصب شده است یا نه که باید دستور زیر را وارد کنید:

```
Get-WindowsCapability -Online | Where-Object Name -like 'OpenSSH*'
```

همان‌طور که در شکل ۸-۵۵۰، مشاهده می‌کنید OpenSSH Client بر روی ویندوز سرور ۲۰۲۵ نصب شده است اما OpenSSH Server نصب نشده است.



شکل ۸- ۵۵۰ سرویس SFTP

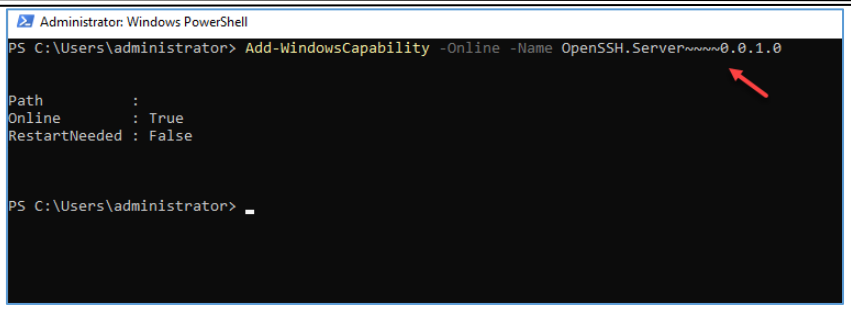
برای نصب سرویس OpenSSH Server باید سرور خود را به اینترنت متصل کنید و دستور زیر را در PowerShell اجرا کنید:

```
Add-WindowsCapability -Online -Name OPenSSH.Server~~~~0.0.1.0
```

که به مانند شکل ۸-۵۵۱، در خروجی مشخص است سرویس مورد نظر به درستی نصب نشده است.

نکته: چنانچه سرور را به اینترنت متصل نکنید با خطای 0x8024402c روبرو خواهید شد.

www.takbook.com



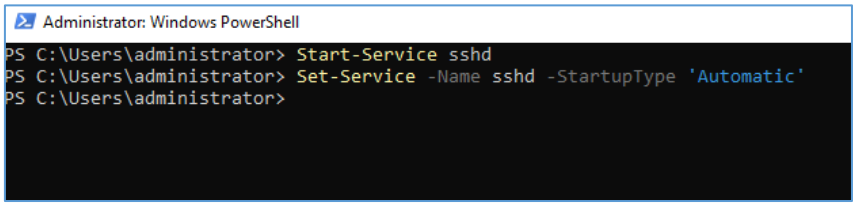
شکل ۸- ۵۵۱ سرویس *SFTP*

بعد از نصب باید سرویس آن را فعال کنیم و حالت آن را بر روی Automatic قرار دهیم، برای این کار از دو دستور زیر استفاده کنید:

```
Start-Service sshd

Set-Service -Name sshd -StartupType 'Automatic'
```

همان‌طور که در شکل ۸-۵۵۲، مشاهده می‌کنید دو دستور مورد نظر با موفقیت اجرا شده است.

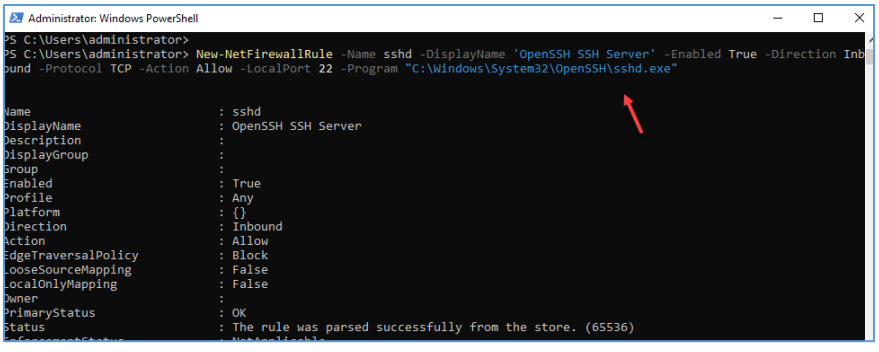


شکل ۸- ۵۵۲ سرویس *SFTP*

اگر می‌خواهید در فایروال برای این سرویس دسترسی ایجاد کنید می‌توانید دستور زیر را در PowerShell اجرا کنید:

```
New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH SSH Server' -
Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort
22 -Program "C:\Windows\System32\OpenSSH\sshd.exe"
```

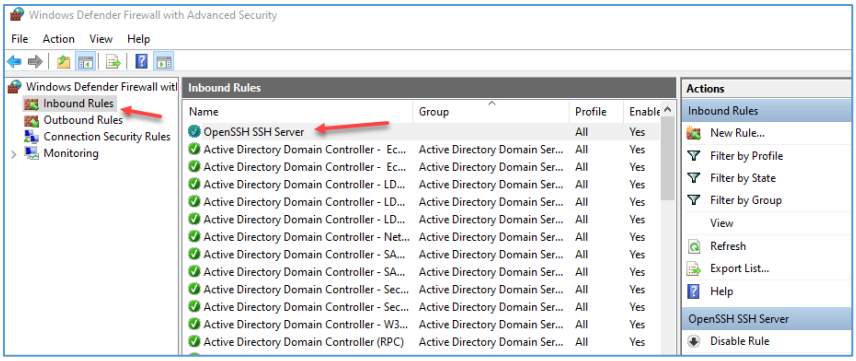
همان‌طور که در شکل ۸-۵۵۳، مشاهده می‌کنید Rule مورد نظر ایجاد شده است.



شکل ۸- ۵۵۳ سرویس *SFTP*

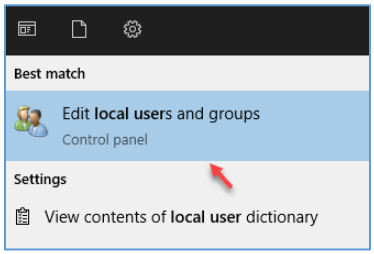
www.takbook.com

اگر وارد سرویس Firewall شویدبه مانند شکل ۸-۵۵٤، این Rule را مشاهده می‌کنید:



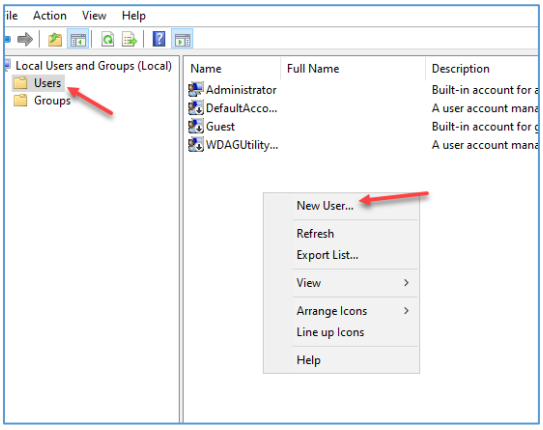
شکل ۸- ۵۵۴ سرویس SFTP

در ادامه کار نیاز به کاربر داریم تا به سرویس SFTP دسترسی داشته باشد، برای این کار یک کاربر جدید در Local Users and groups ایجاد می‌کنیم، سرویس Local Users and groups را به مانند شکل ۸-۵۵۵، اجرا کنید.



شکل ۸- ۵۵۵ سرویس SFTP

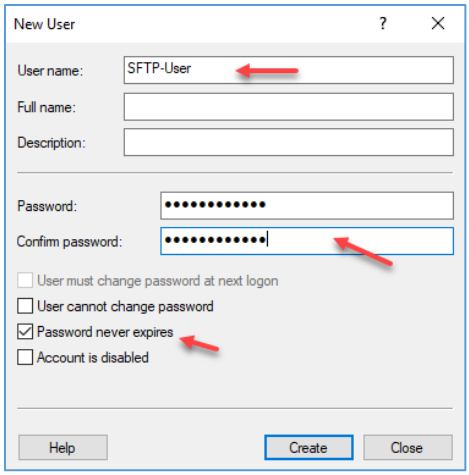
در شکل ۸-۵۵٦، بر روی Users کلیک کنید و گزینه‌ی New User را انتخاب کنید.



شکل ۸- ۵۵۶ سرویس SFTP

www.takbook.com

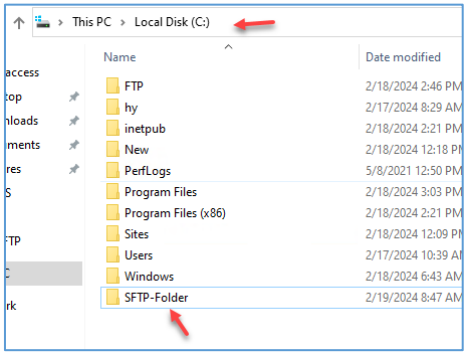
در شکل ۸–۵۵۷، نام کاربر خود را به همراه رمز عبور وارد و بر روی Create کلیک کنید:



شکل ۸- ۵۵۷ سرویس SFTP

شما از طریق دومین هم می‌توانید برای این سرویس کاربر تعریف کنید و از آن استفاده کنید در هر دو حالت این موضوع امکان پذیر است.

بعد از ایجاد کاربر مورد نظر چه در دومین و چه به صورت Local باید یک پوشه در درایو مورد نظر خود ایجاد کنید تا بتوانیم اطلاعات را از طریق پروتکل SFTP انتقال دهیم برای این کار به مانند شکل ۸–۵۵۸، یک پوشه با نام SFTP-Folder در درایو C ایجاد کردیم.



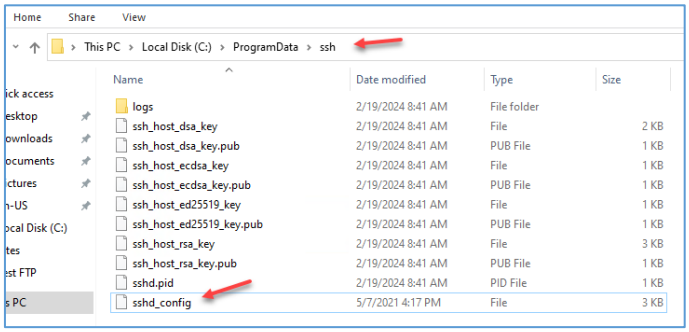
شکل ۸- ۵۵۸ سرویس SFTP

در ادامه کار باید وارد فایل Config شوید و آدرس این فولدر را مشخص کنید.

C:\ProgramData\ssh

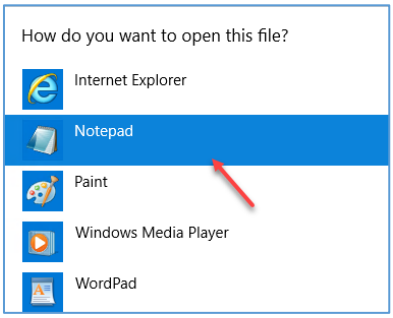
در آدرس شکل ۸–۵۵۹، بر روی فایل SSH_config دو بار کلیک کنید.

www.takbook.com



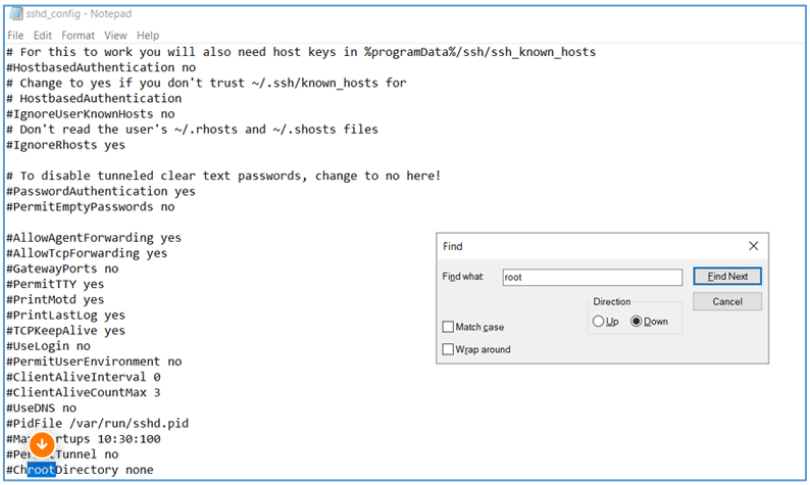
شکل ۸- ۵۵۹ سرویس SFTP

در شکل ۸-۵۶۰، نرم‌افزار Notepad را انتخاب کنید.



شکل ۸- ۵۶۰ سرویس SFTP

بعد از باز کردن فایل مورد نظر، به مانند شکل ۸-۵۶۱، باید آدرس فولدری که ایجاد کردیم را وارد کنید، توجه داشته باشید که علامت # را از پشت کلمه‌ی ChrootDirectory بردارید و به جای کلمه‌ی none آدرس فولدر را وارد کنید.

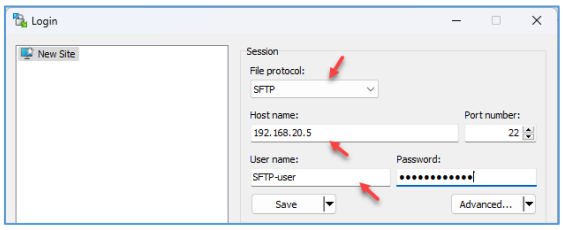


شکل ۸- ۵۶۱ سرویس SFTP

www.takbook.com

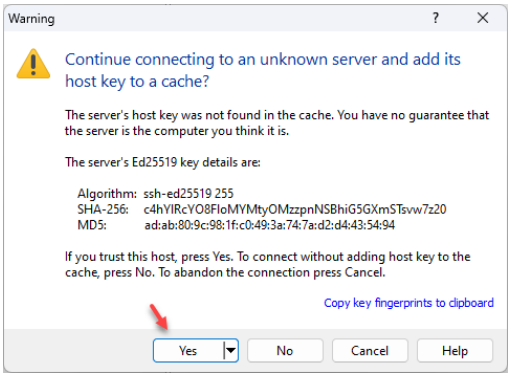
حالا می‌خواهیم از طریق پروتکل SFTP به سرور متصل شویم، برای این کار راه‌های زیادی وجود دارد ولی بهترین کار استفاده از نرم‌افزار WinSCP است که می‌توانید آن را از لینک زیر دانلود کنید:
https://winscp.net/eng/download.php

بعد از نصب و فعال‌سازی نرم‌افزار شکل ۸-۵۶۲، را مشاهده می‌کنید که در قسمت File Protocol باید پروتکل SFTP را انتخاب کنید و در قسمت Host name هم آدرس سروری که بر روی SFTP راه‌اندازی کردید را وارد کنید و نام کاربری و رمز عبور که با هم ایجاد کردیم را وارد کنید و در آخر بر روی Login کلیک کنید.



شکل ۸- ۵۶۲ سرویس SFTP

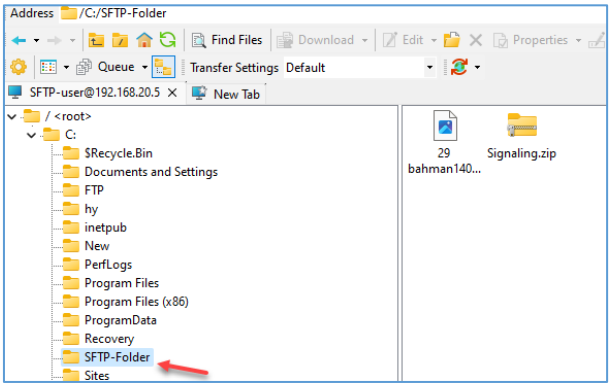
در ادامه دسته کلید بررسی می‌شود و برای تایید باید به مانند شکل ۸-۵۶۳، بر روی Yes کلیک کنید.



شکل ۸- ۵۶۳ سرویس SFTP

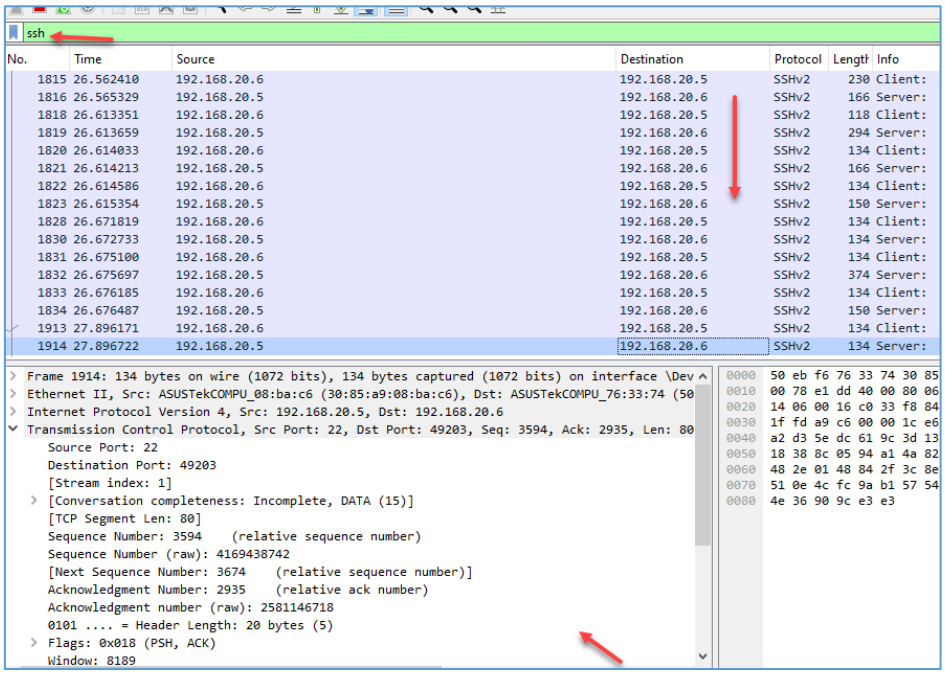
همان‌طور که در شکل ۸-۵۶۴، مشاهده می‌کنید ارتباط با موفقیت برقرار شد و فولدر مورد نظر در دسترس است، و چند فایل را هم به آن انتقال دادیم، برای انتقال فایل می‌توانید فایل را از روی سیستم خود بکشید و در فولدر مورد نظر رها کنید.

www.takbook.com



شکل ۸- ۵۶۴ سرویس SFTP

همان‌طور که در شکل ۸-۵۶۵، گفتیم، وقتی که پروتکل SFTP را فعال می‌کنید امنیت کامل انتقال فایل برقرار خواهد شد که برای بررسی این موضوع دوباره نرم‌افزار WireShark را اجرا کنید و در قسمت فیلتر کلمه‌ی SS را وارد کنید، که در شکل ۸-۵۶۵، مشاهده می‌کنید که ارتباط با SFTP از طریق پورت SSH یعنی ۲۲ برقرار شده اما خبری از نام کاربری و رمز عبور نیست و امنیت کامل برقرار است.



شکل ۸- ۵۶۵ سرویس SFTP

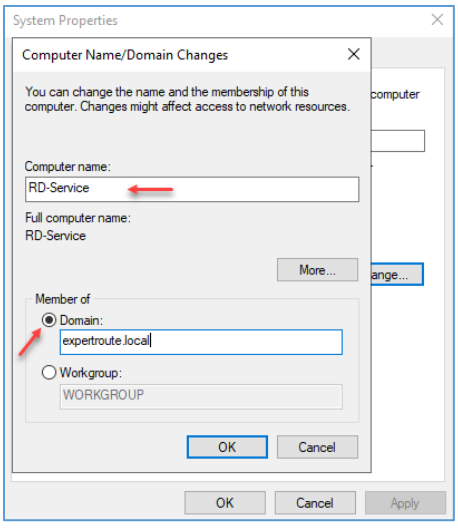
www.takbook.com

۸-۳-۱۹ 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 کار نیاز به یک سیستم دارید که به صورت فیزیکی باشد و یا اینکه اگر می‌خواهید از ماشین مجازی استفاده کنید حتماً از Hyper-V استفاده کنید، اگر بخواهید از نرم‌افزار VMware Workstation استفاده کنید سرویس Hyper-V که مربوط به سرویس Remote Desktop است نصب نخواهد شد و با مشکل روبرو می‌شوید.

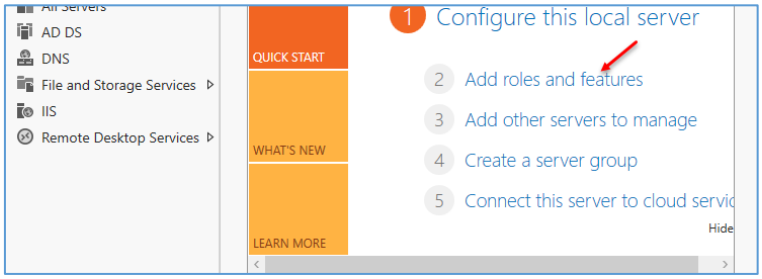
بعد از فعال‌سازی ویندوز سرور یک آدرس IP استاتیک (192.168.20.5) برای آن در نظر بگیرید و آن را عضو دومین Expertroute.local کنید، به مانند شکل ۸-۵۶۶، نام سرور را به RD-Service تغییر دادیم و آن را عضو دومین Expertroute.local کردیم.



شکل ۸- ۵۶۶ سرویس Remote Desktop

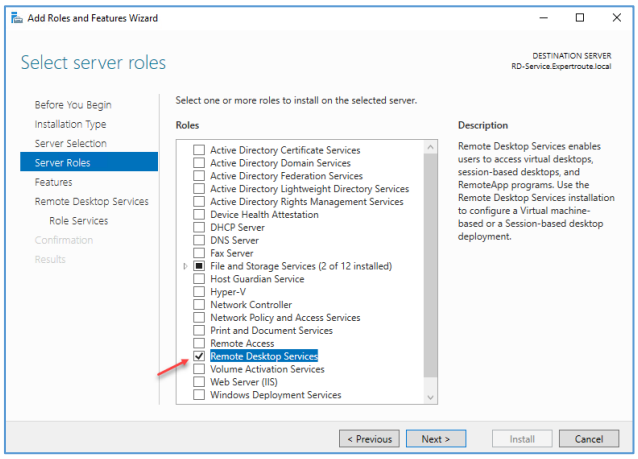
بعد از آماده‌سازی سرور به مانند شکل ۸-۵۶۷، وارد Server Manager شوید و بر روی گزینه‌ی Add roles and features کلیک کنید.

www.takbook.com



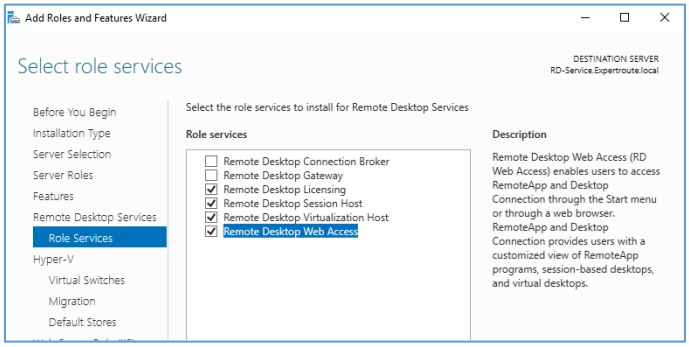
شکل ۸- ۵۶۷ سرویس *Remote Desktop*

در شکل ۸-۵۶۸، سرویسRemote Desktop Services را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۵۶۸ سرویس *Remote Desktop*

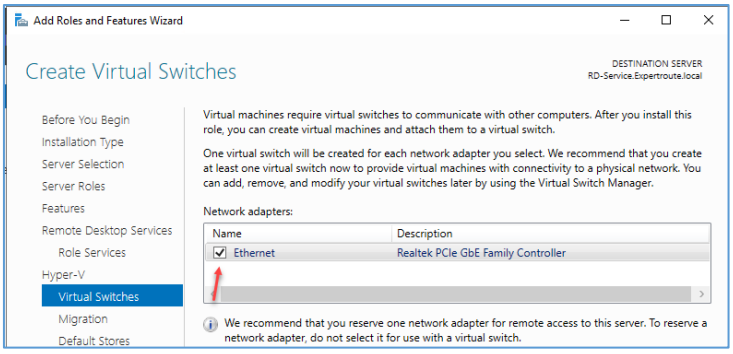
به مانند شکل ۸-۵۶۹، در قسمت Role Services، هر چهار گزینه‌ی مورد نظر را انتخاب و بر روی Next کلیک کنید، توجه داشته باشید که اگر گزینه‌ی Remote Desktop Vitulization Host را انتخاب کنید سرویس Hyper-V نصب خواهد شد و اگر ماشین شما مجازی باشد با خطا روبرو خواهید شد.



شکل ۸- ۵۶۹ سرویس *Remote Desktop*

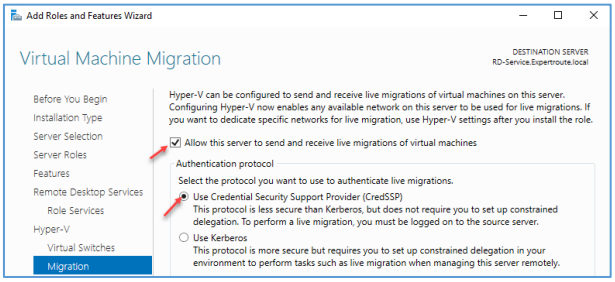
www.takbook.com

در شکل ۸–۵۷۰، کارت شبکه‌ی فیزیکی خود را انتخاب کنید تا سرویس Hyper-V بر روی آن فعال شود.



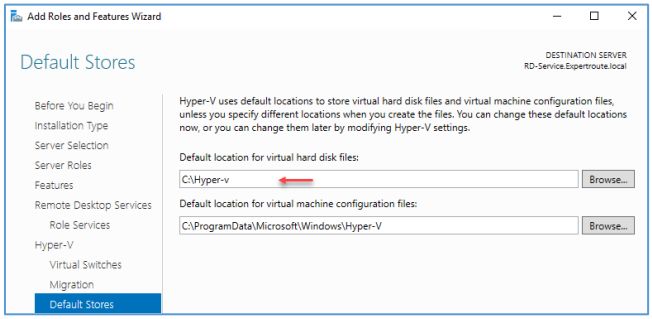
شکل ۸- ۵۷۰ سرویس *Remote Desktop*

در ادامه به مانند شکل ۸–۵۷۱، تیک گزینه‌ی Allow this server to send.. را انتخاب کنید و گزینه‌ی Use Credential… را انتخاب کنید، البته این موارد را در فصل Hyper-V بررسی کردیم.



شکل ۸- ۵۷۱ سرویس *Remote Desktop*

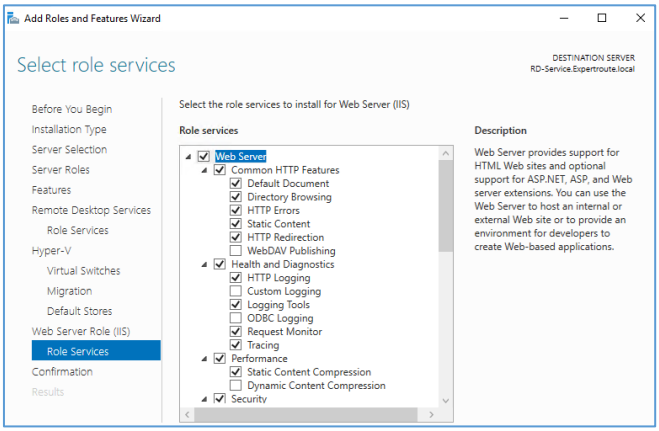
در شکل ۸–۵۸۲، یک مسیر برای ذخیره کردن اطلاعات سرویس Hyper-V انتخاب کنید.



شکل ۸- ۵۷۲ سرویس *Remote Desktop*

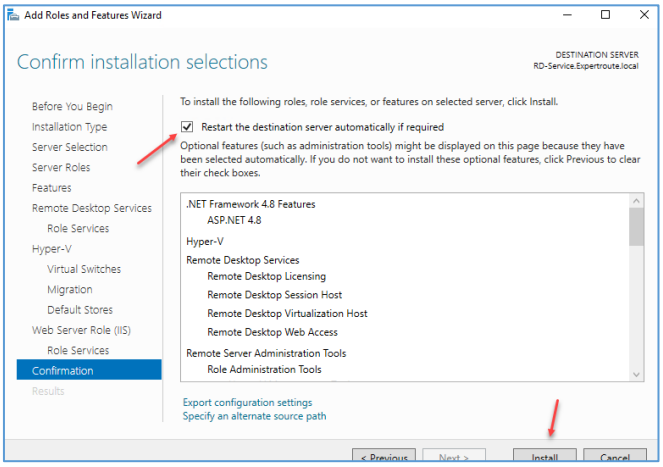
در شکل ۸–۵۷۳، برای نصب سرویس IIS است بر روی Next کلیک کنید.

www.takbook.com



شکل ۸- ۵۷۳ سرویس *Remote Desktop*

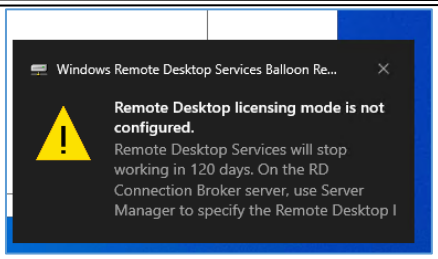
به مانند شکل ۸-۵۷٤، تیک گزینه‌ی Restart را انتخاب کنید و بر روی Install کلیک کنید.



شکل ۸- ۵۷۴ سرویس *Remote Desktop*

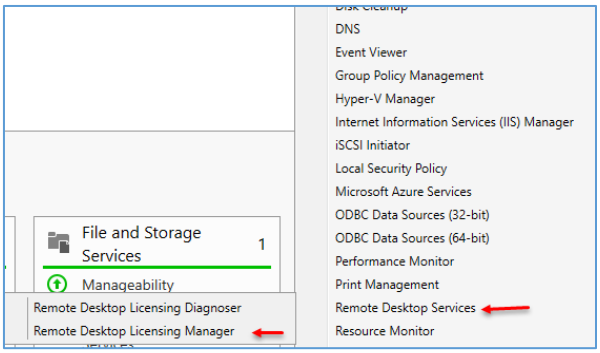
بعد از نصب سرویس و Restart شدن سرور اولین پیامی که مشاهده می‌کنید شکل ۸-۵۷۵، خواهد بود و به این نکته اشاره دارد که لایسنس هنوز تنظیم نشده و لایسنس پیش‌فرضی که وجود دارد یک لایسنس ۱۲۰ روزه است.

www.takbook.com



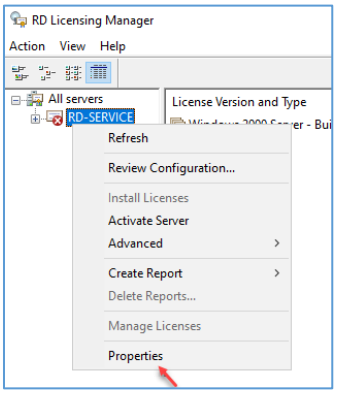
شکل ۸- ۵۷۵ سرویس *Remote Desktop*

در ادامه به مانند شکل ۸–۵۷٦، وارد Server Manager شوید و از قسمت Tools، گزینه‌ی Remote Desktop Licensing Manager را انتخاب کنید.



شکل ۸- ۵۷۶ سرویس *Remote Desktop*

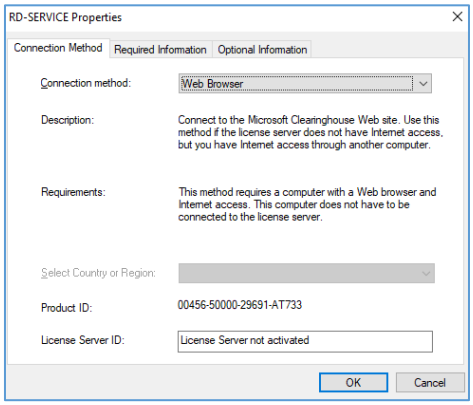
بعد از باز شدن سرویسRemote Desktop Licensing Manager، به مانند شکل ۸–۵۷۷، بر روی نام سرور کلیک راست و بر روی Properties کلیک کنید.



شکل ۸- ۵۷۷ سرویس *Remote Desktop*

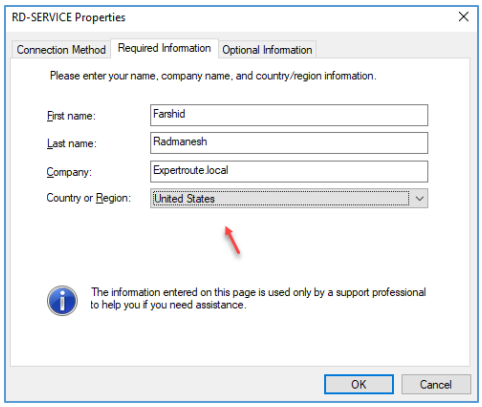
در شکل ۸–۵۷۸، از قسمت Connection method، گزینه‌ی Web Brwser را انتخاب کنید و در ادامه، وارد تب Required information شوید.

www.takbook.com



شکل ۸- ۵۷۸ سرویس *Remote Desktop*

در شکل ۸-۵۷۹، باید اطّلاعات خود را وارد کنید و در قسمت Country نیز نام کشور آمریکا را انتخاب و بر روی OK کلیک کنید.

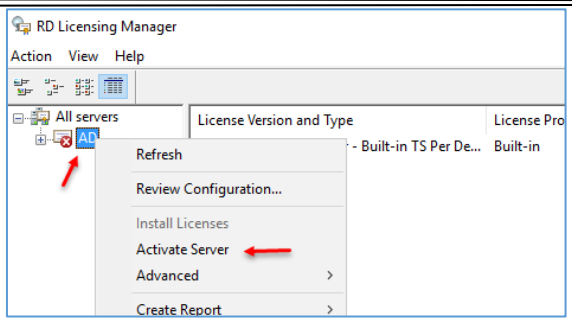


شکل ۸- ۵۷۹ سرویس *Remote Desktop*

بعد از انجام مراحل بالا به مانند شکل ۸-۵۸۰، دوباره بر روی نام سرور کلیک راست کنید و گزینه‌ی Activate Server را انتخاب کنید.

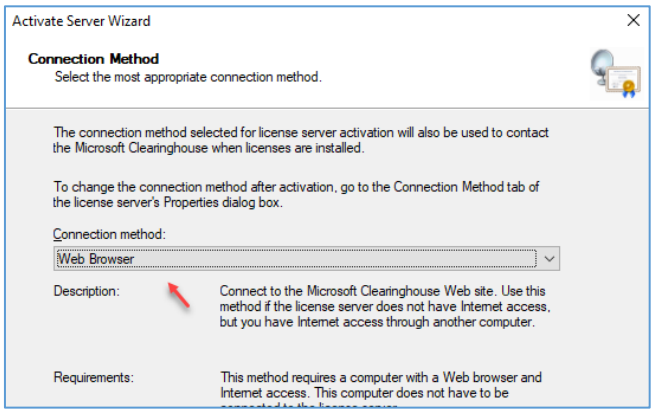
نکته: در ادامه کار، سرور باید به اینترنت متّصل شود.

www.takbook.com



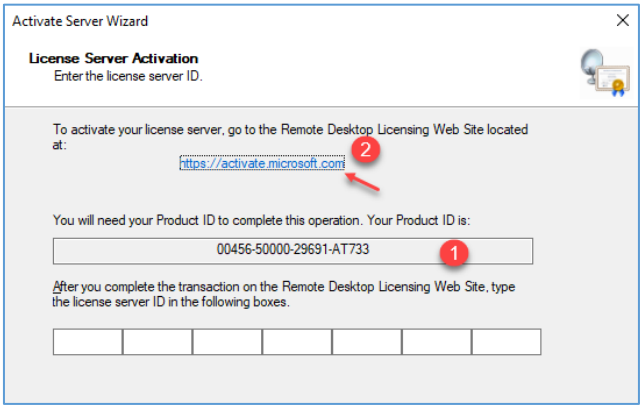
شکل ۸- ۵۸۰ سرویس *Remote Desktop*

در شکل ۸-۵۸۱، گزینه‌ی Web Browser را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸- ۵۸۱ سرویس *Remote Desktop*

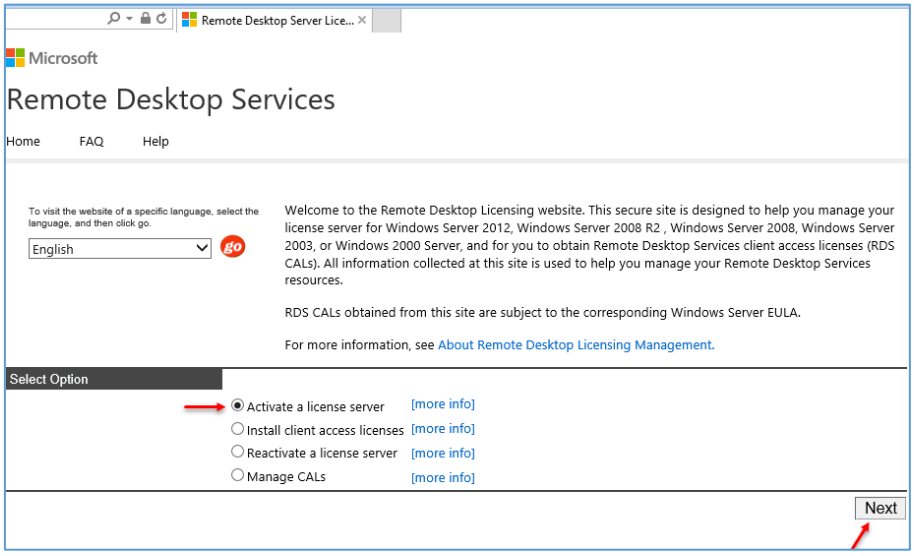
در شکل ۸-۵۸۲، در قسمت شماره‌ی یک، برای سرور شما یک Product ID مشخّص شده است، قبل از هر چیز، این شماره را در یک جای مناسب ذخیره کنید تا در ادامه از آن استفاده کنید، در ادامه بر روی لینک شماره‌ی دو در صفحه کلیک کنید.



شکل ۸- ۵۸۲ سرویس *Remote Desktop*

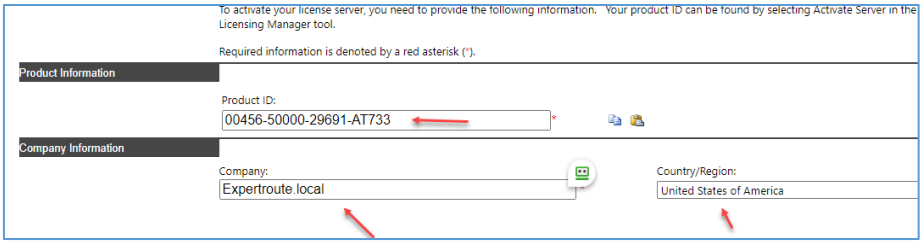
www.takbook.com

در شکل ۸-۵۸۳، صفحه‌ی مربوط به Active ظاهر می‌شود، گزینه‌ی Activate a license Server را انتخاب و بر روی Next کلیک کنید.



شکل ۸-۵۸۳ سرویس *Remote Desktop*

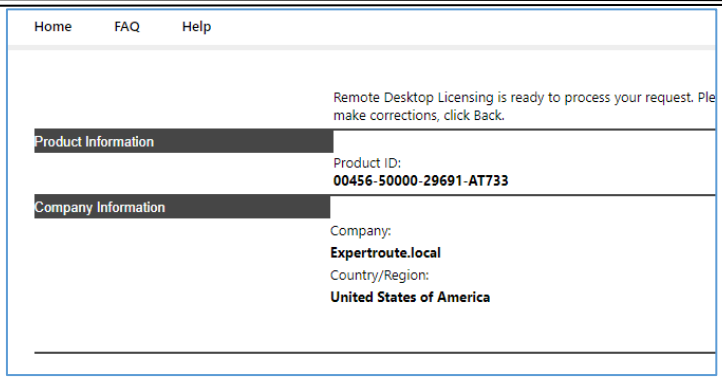
در شکل ۸-۵۸٤، در قسمت Product ID، شماره‌ای که در اوّل کار در یک فایل Copy کردید را وارد کنید، بعد در قسمت Company، نام شرکتی که در قسمت قبل وارد کردید را وارد و نام کشور را آمریکا انتخاب و بر روی Next کلیک کنید.



شکل ۸-۵۸۴ سرویس *Remote Desktop*

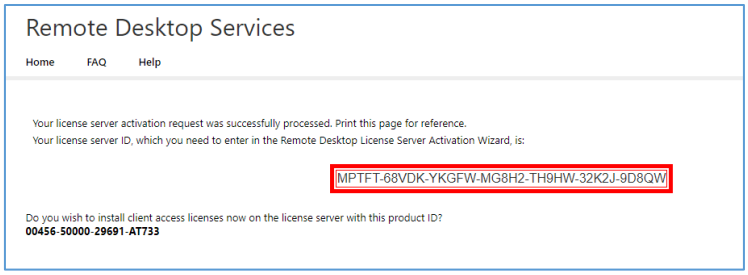
در شکل ۸-۵۸۵، اگر اطّلاعات شما مورد تأیید است، بر روی Next کلیک کنید.

www.takbook.com



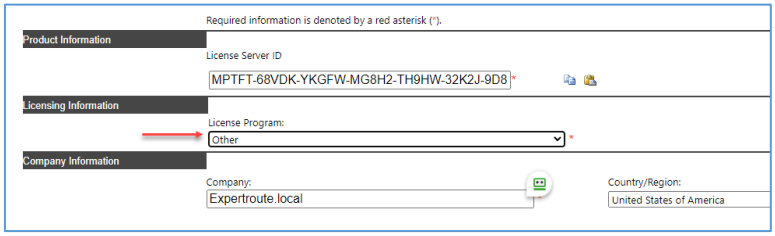
شکل ۸- ۵۸۵ سرویس *Remote Desktop*

در شکل ۸–۵۸۶، یک شماره‌ی دوّم به شما داده می‌شود که این شماره را نیز کپی کنید و در کنار همان شماره‌ای قرار دهید تا در ادامه از آن استفاده کنید؛ بر روی Yes کلیک کنید.



شکل ۸- ۵۸۶ سرویس *Remote Desktop*

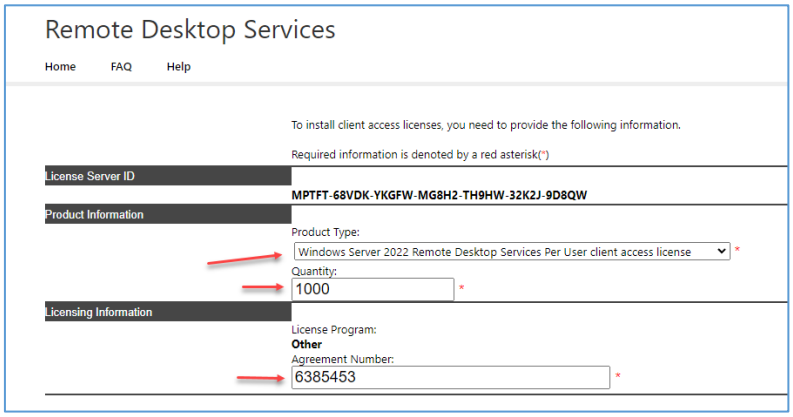
در شکل ۸–۵۸۷، برای ایجاد لایسنس در قسمت License Program، گزینه‌ی Other را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۵۸۷ سرویس *Remote Desktop*

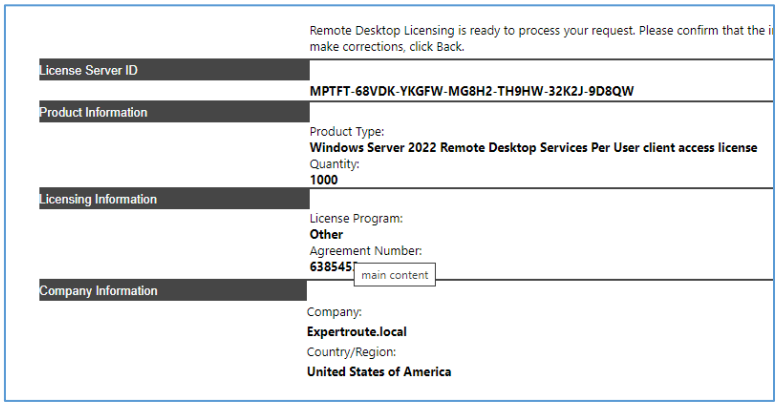
در شکل ۸–۵۸۸، در قسمت Product Type، سرویس Windows Server 2025 Remote Desktop Services per… را انتخاب کنید، در قسمت Quantity، عدد 1000 را وارد و در قسمت آخر نیز عدد 6385453 را وارد و بر روی Next کلیک کنید.

www.takbook.com



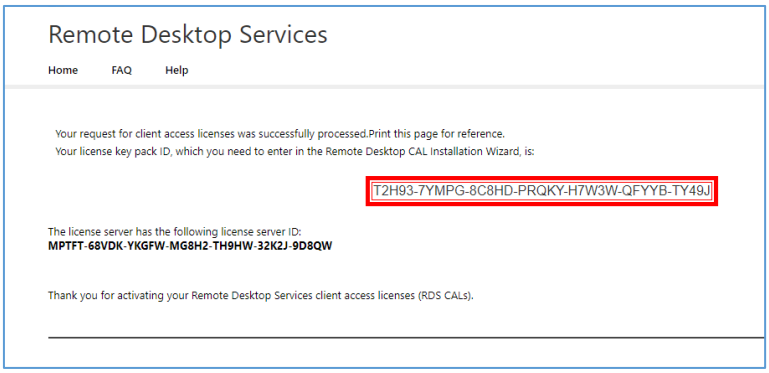
شکل ۸- ۵۸۸ سرویس *Remote Desktop*

اگر در شکل ۸-۵۸۹، اطّلاعات مورد تأیید است، بر روی Next کلیک کنید.



شکل ۸- ۵۸۹ سرویس *Remote Desktop*

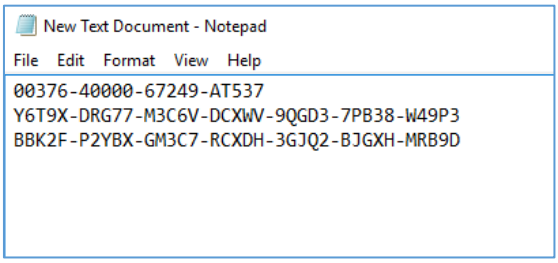
در شکل ۸-۵۹۰، یک سریال نهایی به شما داده خواهد شد که این شماره را نیز کنار همان شماره‌ها قرار دهید و بر روی Finish کلیک کنید.



شکل ۸- ۵۹۰ سرویس *Remote Desktop*

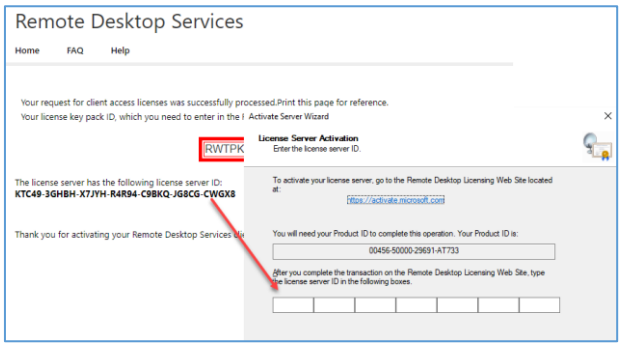
www.takbook.com

همان‌طور که در شکل ۸-۵۹۱، مشاهده می‌کنید، هر سه سریال در کنار هم قرار داده شده است، در ادامه برای اجرای نهایی سرویس از دو سریال پایینی استفاده می‌کنیم.



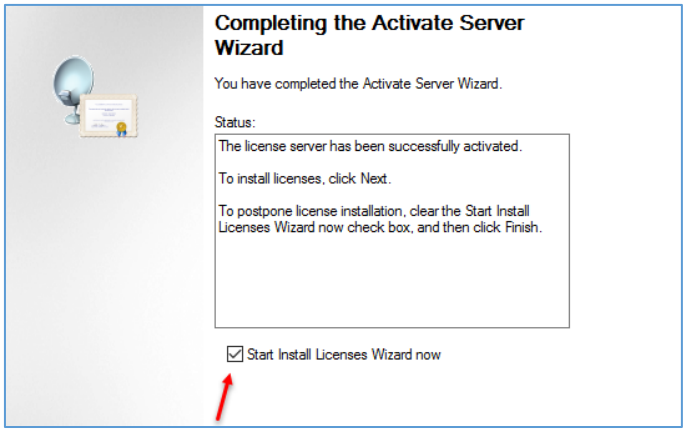
شکل ۸- ۵۹۱ سرویس *Remote Desktop*

در شکل ۸-۵۹۲، شماره‌ی سریال دوّم را در قسمت مورد نظر وارد و بر روی Next کلیک کنید تا سرور، Active شود.



شکل ۸- ۵۹۲ سرویس *Remote Desktop*

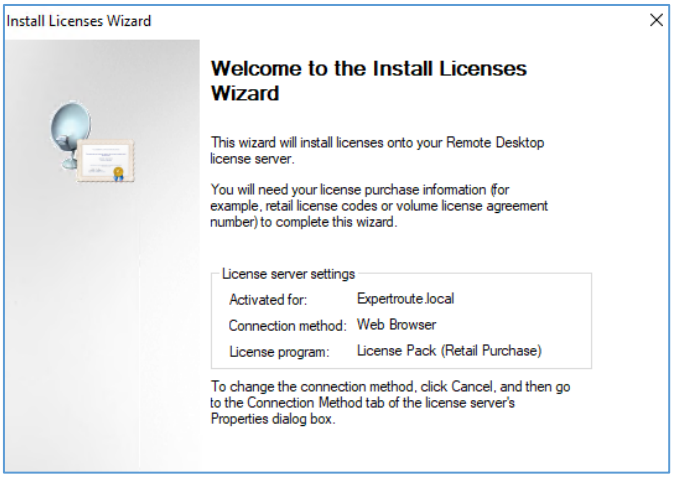
در ادامه و بعد از تأیید نهایی سرور باید لایسنس آن را نیز فعّال کنید، به مانند شکل ۸-۵۹۳، تیک گزینه‌ی Start Install Licenses Wizard now را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۵۹۳ سرویس *Remote Desktop*

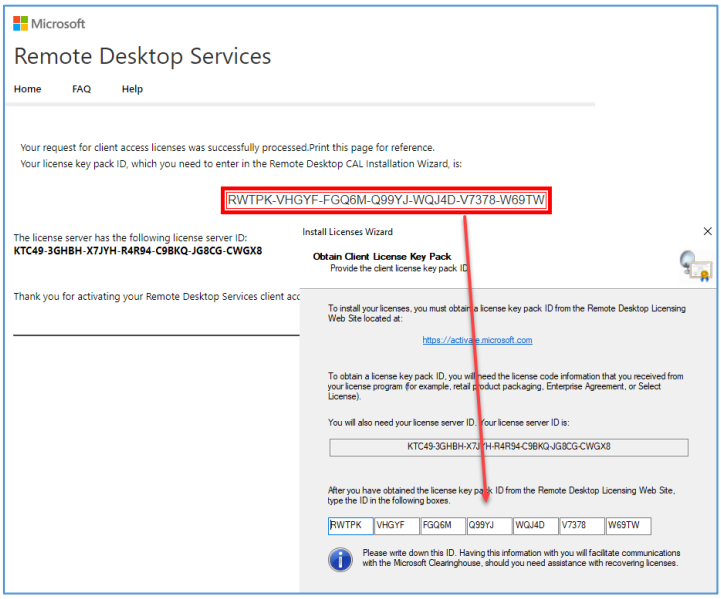
www.takbook.com

به مانند شکل ۸-۵۹٤، صفحه‌ی Welcome ظاهر می‌شود، بر روی Next کلیک کنید.



شکل ۸- ۵۹۴ سرویس *Remote Desktop*

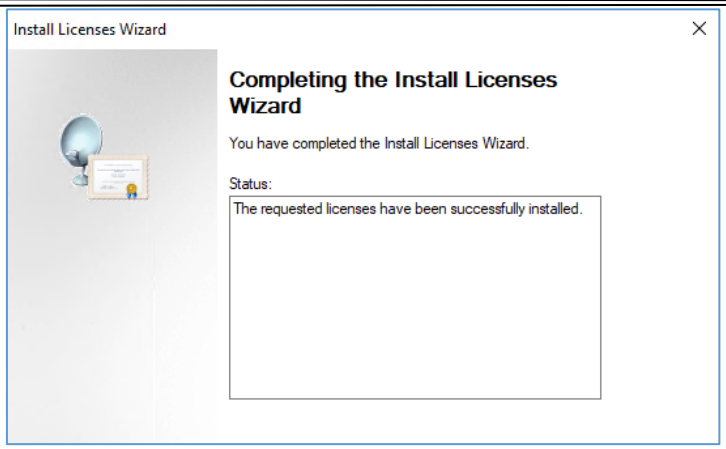
در شکل ۸-۵۹۵، باید سریال اصلی را در قسمت مورد نظر کپی و بر روی Next کلیک کنید تا سرور به صورت کامل فعّال شود.



شکل ۸- ۵۹۵ سرویس *Remote Desktop*

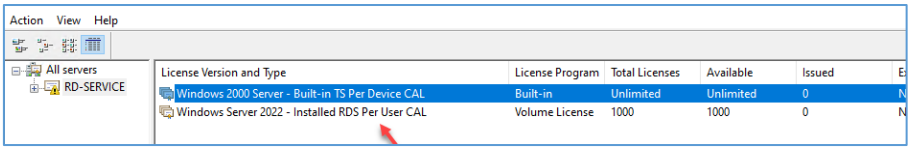
در شکل ۸-۵۹٦، بر روی Finish کلیک کنید.

www.takbook.com



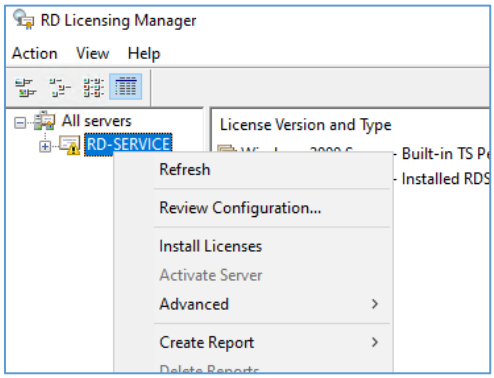
شکل ۸- ۵۹۶ سرویس *Remote Desktop*

همان‌طور که در شکل ۸–۵۹۷، مشاهده می‌کنید لایسنس مورد نظر به لیست اضافه شده است و همه چیز برای ادامه کار آماده است.



شکل ۸- ۵۹۷ سرویس *Remote Desktop*

در ادامه کار به مانند شکل ۸–۵۹۸، بر روی نام سرور کلیک راست کنید و گزینه‌ی Review Configuration را انتخاب کنید.

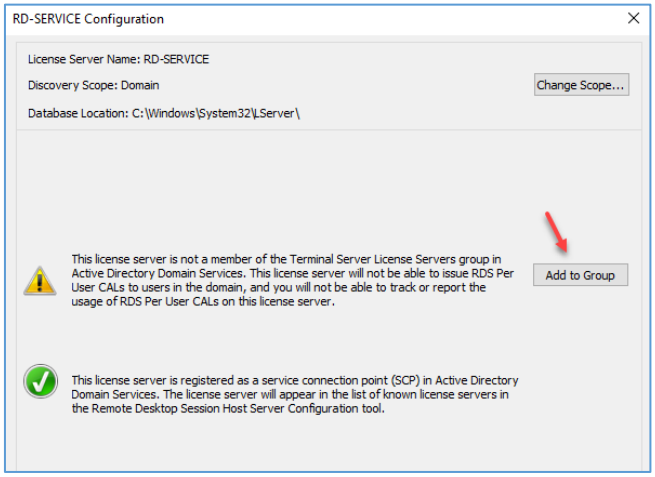


شکل ۸- ۵۹۸ سرویس *Remote Desktop*

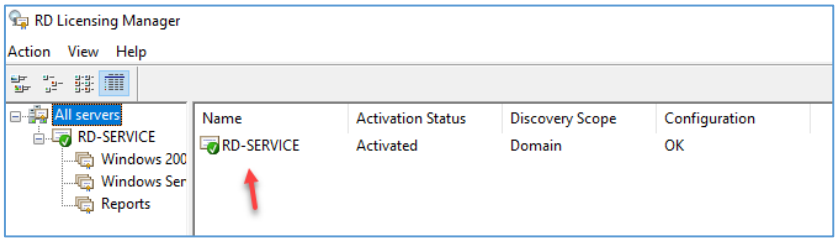
در شکل ۸–۵۹۹، یک پیغام برای شما ظاهر می‌شود که به شما این پیام را می‌دهد که اکانت Network Service، عضو گروه‌های گفته‌شده نیست که در ادامه باید این کار انجام شود، برای حلّ مشکل بر روی

www.takbook.com

Add to Group کلیک کنید و در صفحات باز شده بر روی OK کلیک کنید و حتماً بعد از آن سرور را Restart کنید، همان‌طور که در شکل ۸-۶۰۰، مشاهده می‌کنید سرویس مورد نظر به درستی فعال شده است.



شکل ۸- ۵۹۹ سرویس *Remote Desktop*



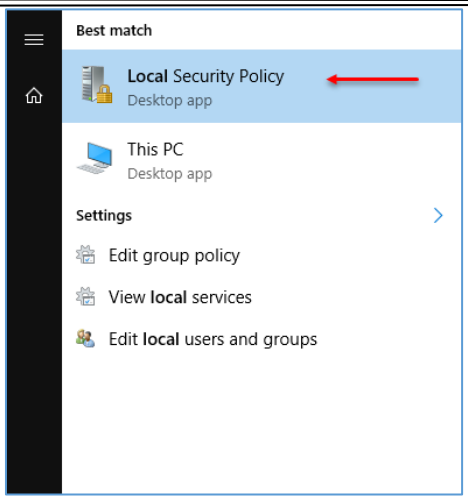
شکل ۸- ۶۰۰ سرویس *Remote Desktop*

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.

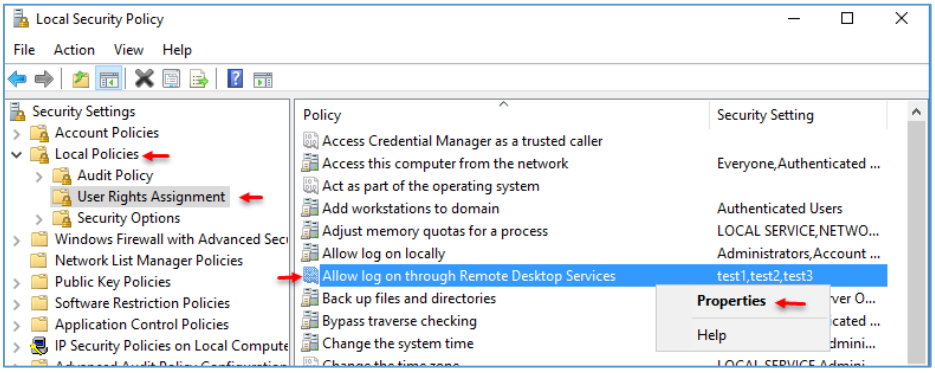
وارد سرور اصلی که در اینجا همان، RD-Service است شوید و به مانند شکل ۸-۶۰۱، در Start، سرویس Local Security Policy را اجرا کنید تا تنظیمات مورد نیاز برای Remote را انجام دهید.

www.takbook.com



شکل ۸- ۶۰۱ سرویس *Remote Desktop*

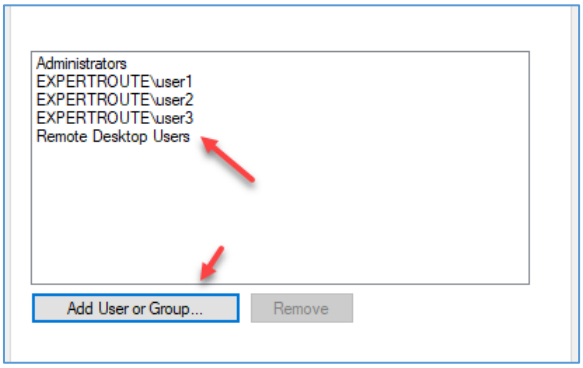
در شکل ۸-۶۰۲، از سمت چپ از قسمت Local Policies وارد قسمت User Rights assignment شوید و در لیست بازشده بر روی گزینه‌ی Allow log on through Remote Desktop کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۶۰۲ سرویس *Remote Desktop*

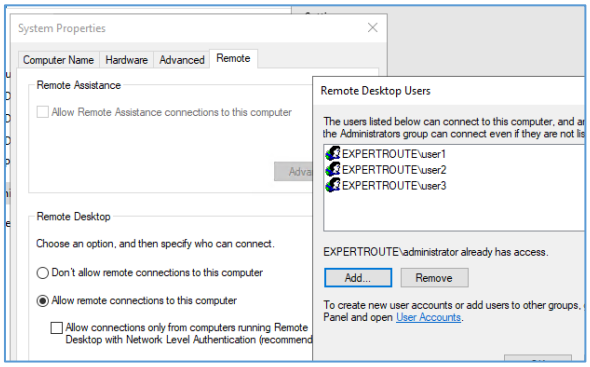
در شکل ۸-۶۰۳، باید کاربرانی که می‌خواهند به این سرور دسترسی داشته باشند را با کلیک بر روی Add User or Group به لیست اضافه کنید، همان‌طور که مشاهده می‌کنید، سه کاربر با نام‌های Test1, Test2, Test3 به لیست اضافه شده است.

www.takbook.com



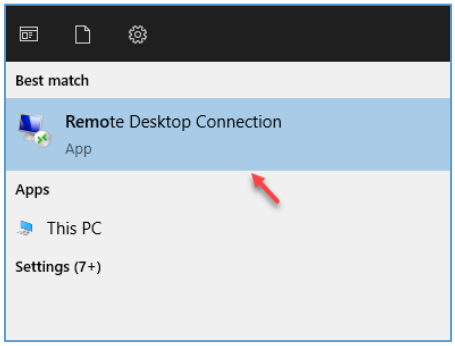
شکل ۸- ۶۰۳ سرویس *Remote Desktop*

در سرویس Remote Desktop هم طبق شکل ۸-٦٠٤، کاربران را اضافه کنید



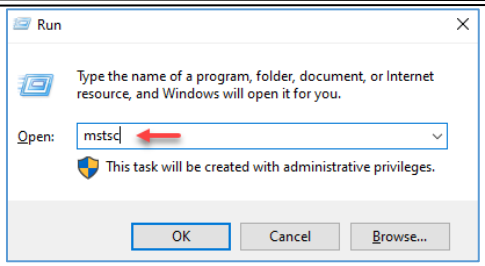
شکل ۸- ۶۰۴ سرویس *Remote Desktop*

برای تست از یک کلاینت که دارای ویندوز 11 است و عضو شبکه‌ی شده است، استفاده می‌کنیم، برای شروع به مانند شکل ۸-٦٠٥، وارد start شوید و سرویس Remote Desktop را اجرا کنید، یا اینکه وارد Run شوید و دستور MSTSC را اجرا کنید.



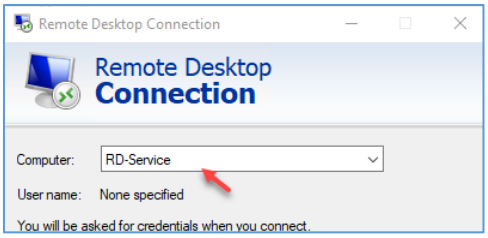
شکل ۸- ۶۰۵ سرویس *Remote Desktop*

www.takbook.com



شکل ۸- ۶۰۶ سرویس *Remote Desktop*

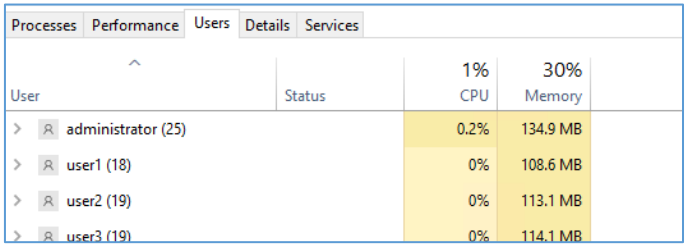
در شکل ۸-۶۰۷، باید نام سرور خود را که سرویسRemote Dekstop را بر روی آن فعّال کردید را وارد و بر روی Connect کلیک کنید و بعد از آن برای ورود، نام کاربری مورد نظر خود را وارد کنید.



شکل ۸- ۶۰۷ سرویس *Remote Desktop*

بعد از اینکه با کاربرهای مورد نظر (هر سه کاربر) به سرور RD-Service ریموت زدید، وارد آن شوید و سرویس Task Manager را اجرا کنید.

در شکل ۸-۶۰۸، 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 کاربرانTest1, Test2, Test3 از طریق ریموت وارد سیستم شده‌اند که چندین کاربر دیگر نیز می‌توانند به صورت همزمان وارد شوند.

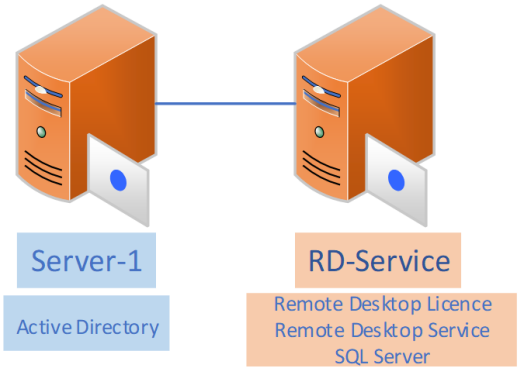


شکل ۸- ۶۰۸ سرویس *Remote Desktop*

۸-۳-۱۹-۱ 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 وب‌سایت به نرم‌افزارها و ماشین‌های مجازی خود از طریق Remote دسترسی داشته باشید که این خود می‌تواند کمک زیادی به شما کند.

www.takbook.com

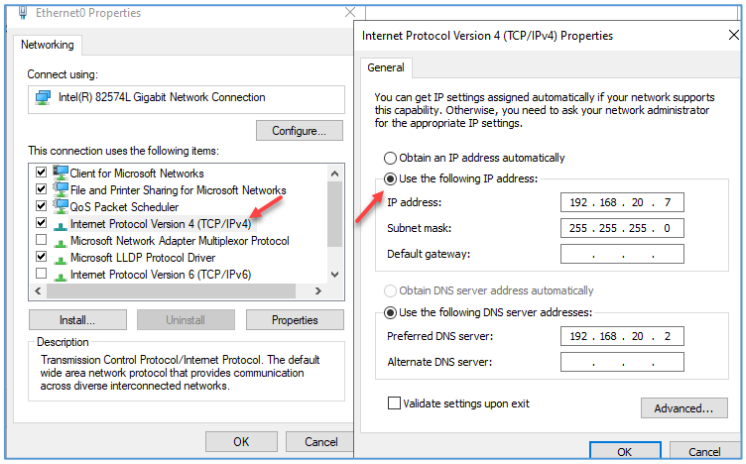


شکل ۸- ۶۰۹ Remote Desktop از طریق Web

برای راه‌اندازی این سرویس در حالت Quick (سریع)، نیاز به دو سرور داریم که یکی از سرورها نقش Active Directory را بازی می‌کند و سرور دوم نقش Remote Dektop Licence،SQL و سرویس Remote Desktop را بازی می‌کند.

طبق سناریو قبلی میخواهیم سرور جدیدی راه‌اندازی کنیم که بر روی آن سرویس Remote Desktop را فعال و دسترسی از طریق وب را بررسی می‌کنیم.

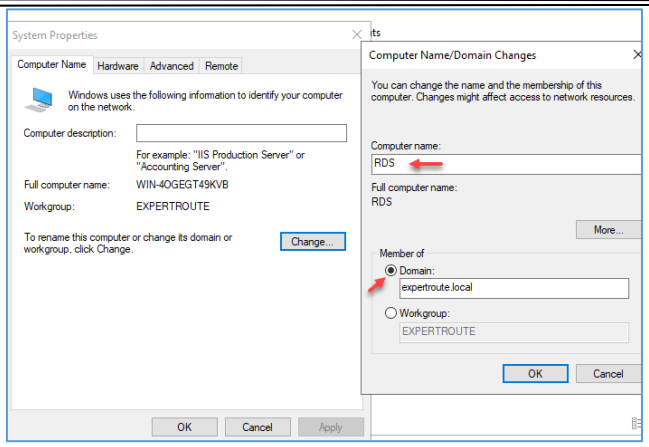
بر روی سرور RDS ویندوز سرور ۲۰۲۵ نصب کنید و طبق شکل ۸-۶۱۰، آدرس IP آن را به صورت دستی وارد کنید.



شکل ۸- ۶۱۰ Remote Desktop از طریق Web

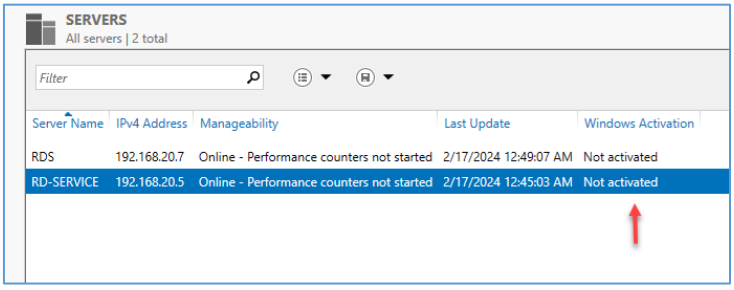
در شکل ۸-۶۱۱، نام سرور را وارد و آن را عضو دومین کنید.

www.takbook.com



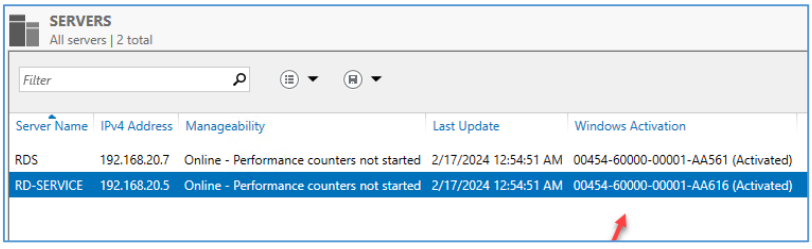
شکل ۸- ۶۱۱ Remote Desktop از طریق Web

در شکل ۸-۶۱۲، هر دو سرور را مشاهده می‌کنید، در ادامه، همه‌ی کارها را در سرور RD-Service انجام خواهیم داد، اگر به شکل توجه کنید هر دو سرور Not activated هستند که باید هر دوی آنها را با روشی که در فصل دوم گفتم فعال کنید.



شکل ۸- ۶۱۲ Remote Desktop از طریق Web

همان‌طور که در شکل ۸-۶۱۳، مشاهده می‌کنید هر دو سرور فعال شده‌اند و حالا می‌توانیم ادامه کار را با خیال آسوده انجام دهیم.

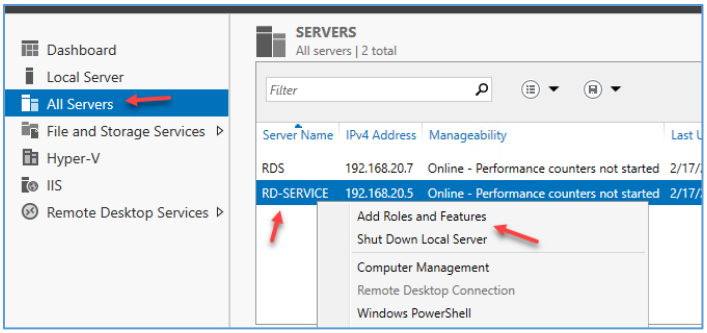


شکل ۸- ۶۱۳ Remote Desktop از طریق Web

برای شروع کار به مانند شکل ۸-۶۱۴، بر روی نام سرور RD-Service کلیک راست کنید و گزینه‌ی Add Role and Features را انتخاب کنید.

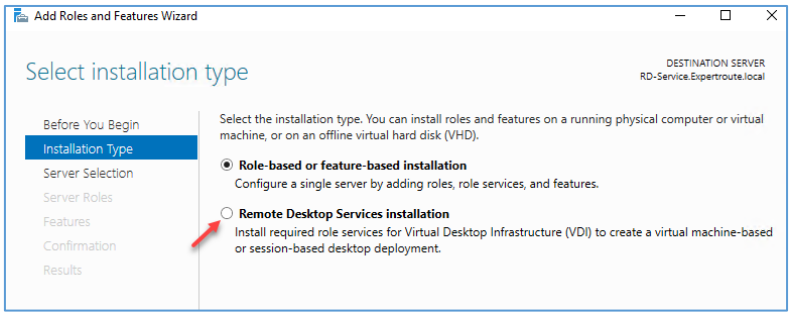
www.takbook.com

تذکّر: همه‌ی عملیّات در سرور RD-Service انجام می‌شود.



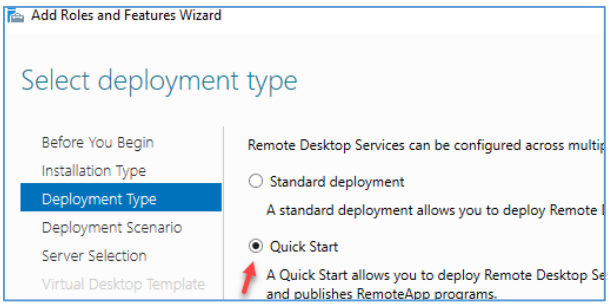
شکل ۸- ۶۱۴ Remote Desktop از طریق Web

در شکل ۸-۶۱۵، گزینه‌ی Remote Desktop Services Installation را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۶۱۵ Remote Desktop از طریق Web

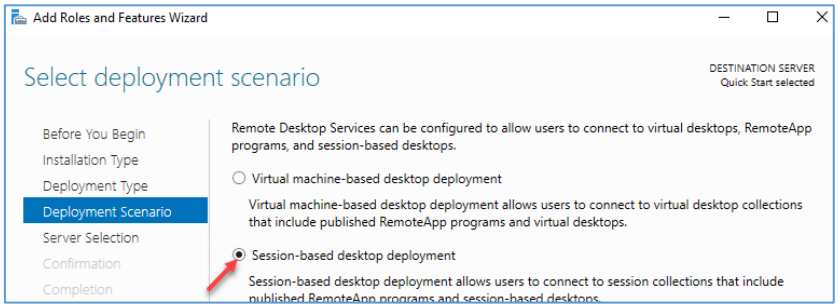
برای تنظیم این سرویس دو روش وجود دارد که روش اول Quick Start است و خیلی سریع نصب انجام می‌شود، ولی اگر روش Standard را انتخاب کنید تنظیم آن زمان‌بر و پیچیده‌تر خواهد بود که در قسمت قبلی این روش را به صورت کامل توضیح دادیم، گزینه‌ی Quick Start را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸- ۶۱۶ Remote Desktop از طریق Web

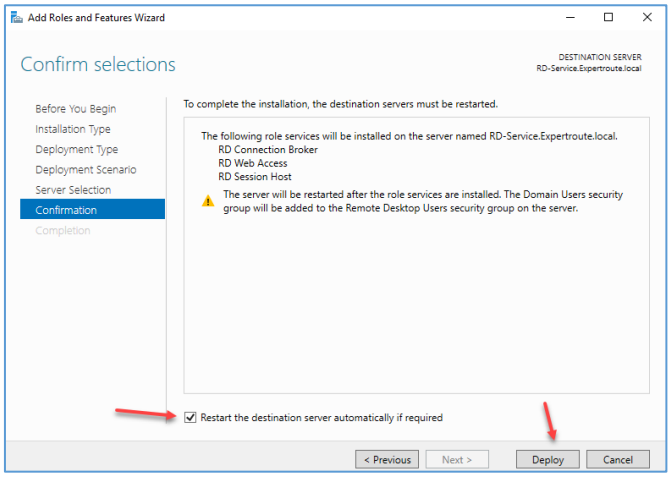
www.takbook.com

در شکل ۸–۶۱۷، دو گزینه وجود دارد، اگر بخواهیم ماشین مجازی را برای کاربران خود به اشتراک بگذاریم باید گزینه‌ی Virtual machine-based desktop deployment را انتخاب کنید و اگر بخواهید نرم‌افزار را برای کاربران به اشتراک بگذارید باید گزینه‌ی Seesion-based desktop deployment را انتخاب کنید.



شکل ۸- ۶۱۷ *Remote Desktop از طریق Web*

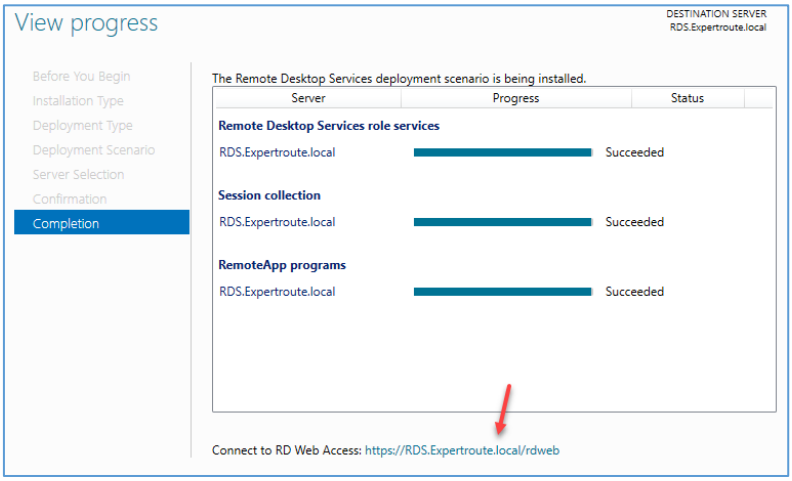
بعد از انتخاب در شکل ۸–۶۱۸، بر روی Deploy کلیک کنید تا سرویس مورد نظر نصب شود.



شکل ۸- ۶۱۸ *Remote Desktop از طریق Web*

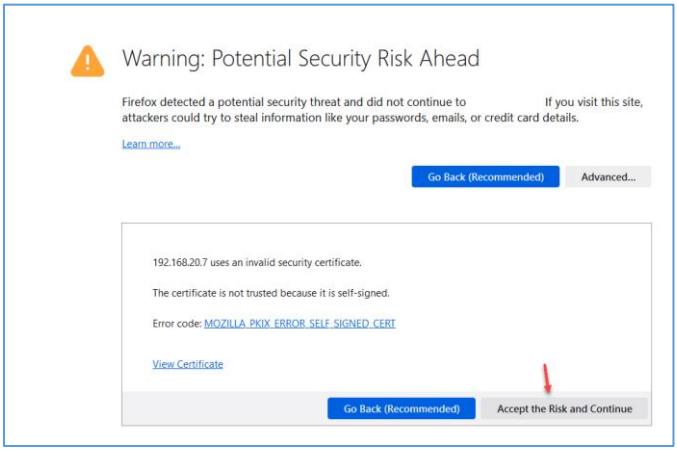
همان‌طور که در شکل ۸–۶۱۹، مشاهده می‌کنید سه سرویس بر روی سرور RDS نصب شده است و در آخر صفحه آدرس دسترسی به آن را مشاهده می‌کنید، قبل از اینکه به آدرس مورد نظر متصل شویم بهتر است به این نکته توجه کنید که زمانی که حالت Quick Start را انتخاب می‌کنید یک لایسنس ۱۲۰ روزه برای شما در نظر گرفته خواهد شد و سرویس شما طبق این لایسنس کار خواهد کرد و همچنین بعد از این مدت زمات سرویس از کار خواهد افتاد که البته روش‌های برای حل آن وجود دارد و جای نگرانی نخواهد بود.

www.takbook.com



شکل ۸- ۶۱۹ *Remote Desktop از طریق Web*

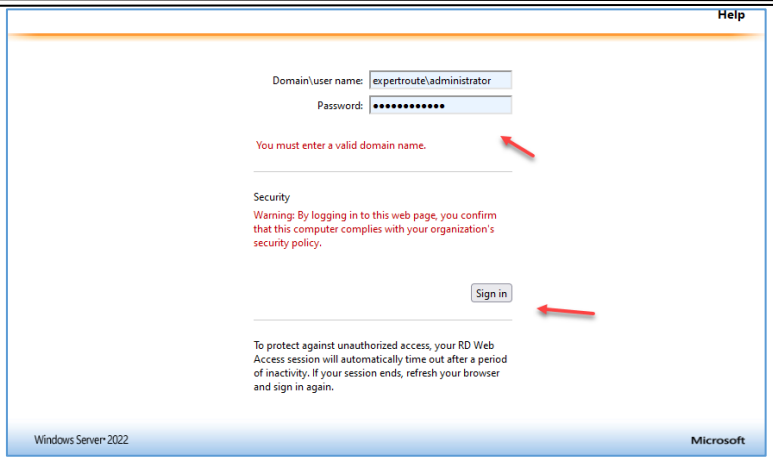
بعد از کلیک بر روی آدرس مورد نظر شکل ۸-۶۲۰، ظاهر خواهد شد، توجه داشته باشید که چون گواهینامه‌ی سرور قابل اعتماد نیست شکل ۸-۶۲۰، را مشاهده خواهید کرد که باید بر روی Accept the risk and continue کلیک کنید.



شکل ۸- ۶۲۰ *Remote Desktop از طریق Web*

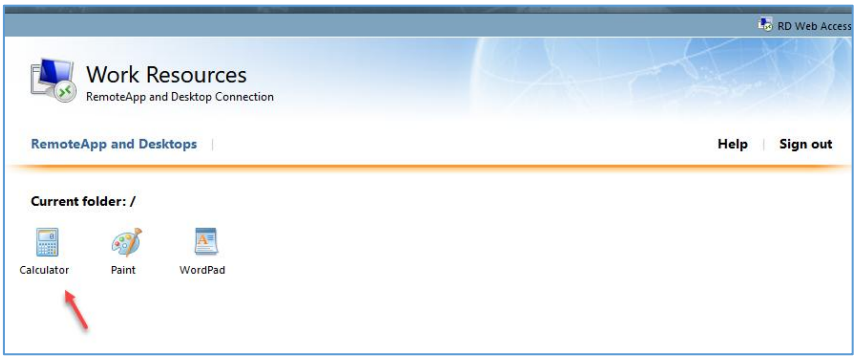
نکته مهم: چنانچه آدرس RDweb را در مرورگر Edge اجرا کنید، شاید با خطا شکل ۸-۶۲۱، مواجه شوید و صفحه‌ی مورد نظر اجرا نشود، که برای حل این مشکل بهتر است از مرورگر Firefox استفاده کنید.
همان‌طور که در شکل ۸-۶۲۱، مشاهده می‌کنید، صفحه‌ی ورود ظاهر شده است و باید نام دومین را به همراه نام کاربر مورد نظر وارد کنید.

www.takbook.com



شکل ۸- ۶۲۱ Remote Desktop از طریق Web

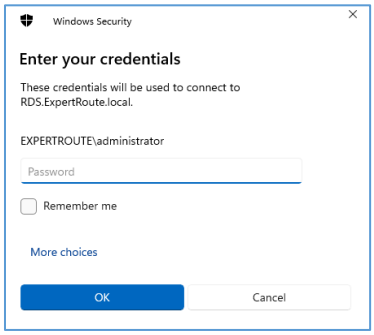
بعد از ورود به مانند شکل ۸-۶۲۲، سه آیکون نرم‌افزار ویندوز را مشاهده می‌کنید که به صورت پیش‌فرض در دسترس قرار گرفته است و شما می‌توانید با کلیک بر روی آن، آنها را اجرا کنید، توجه داشته باشید این نرم‌افزارها از طریق سرور اجرا می‌شوند و ارتباطی با کلاینت شما ندارند.



شکل ۸- ۶۲۲ Remote Desktop از طریق Web

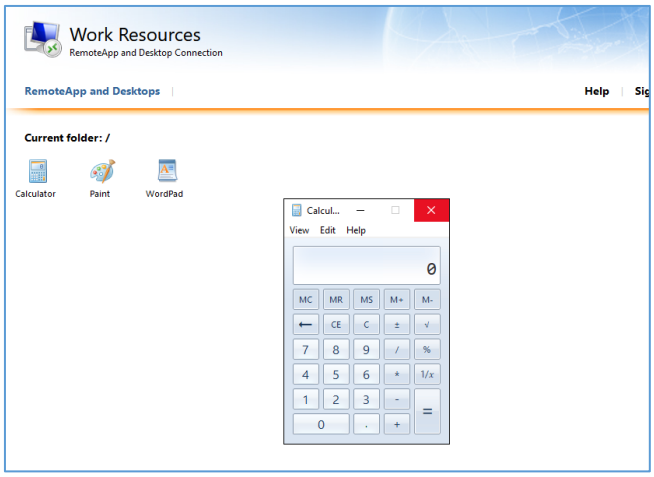
بعد از کلیک بر روی آیکون مورد نظر یک فایل دانلود شده که باید بر روی آن کلیک کنید تا عملیات اتصال با سرور انجام شود، بعد از کلیک به مانند شکل ۸-۶۲۳، باید نام کاربری و رمز عبور برای دسترسی را وارد کنید، توجه داشته باشید به طور پیش‌فرض کاربری که با آن سرویس را نصب کردید دسترسی دارد و بهتر است نام کاربری آن را وارد کنیم.

www.takbook.com



شکل ۸- ۶۲۳ Remote Desktop از طریق Web

همان‌طور که در شکل ۸-٦٢٤، مشاهده می‌کنید، نرم افزار مورد نظر با موفقیت اجرا شده است و این نرم افزار هیچ ارتباطی با سیستم کلاینت شما ندارد و از طریق سرور اجرا شده است.

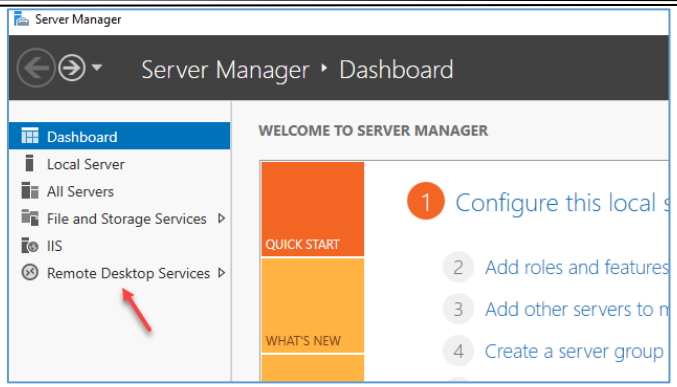


شکل ۸- ۶۲۴ Remote Desktop از طریق Web

۸-۳-۱۹-۲ اجرای نرم‌افزار از طریق سرویس Remote Desktop

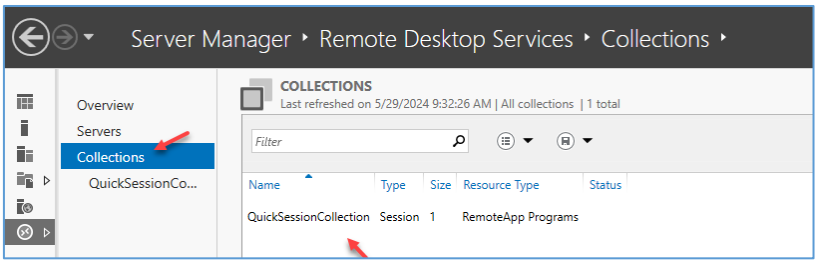
همان‌طور که در قسمت قبل مشاهده کردید سه نرم افزار به صورت پیش‌فرض فعال شده بوند که ما آنها را اجرا کردیم، اما حالا می‌خواهیم بررسی کنیم که چطوری می‌توانیم نرم‌افزار دلخواه خود را بارگذاری و اجرا کنیم، برای این کار به مانند شکل ۸-٦٢٥، وارد سرور RDS شوید و سرویس Server Manager را اجرا کنید و در شکل باز شده بر روی Remote Desktop Service کلیک کنید.

www.takbook.com



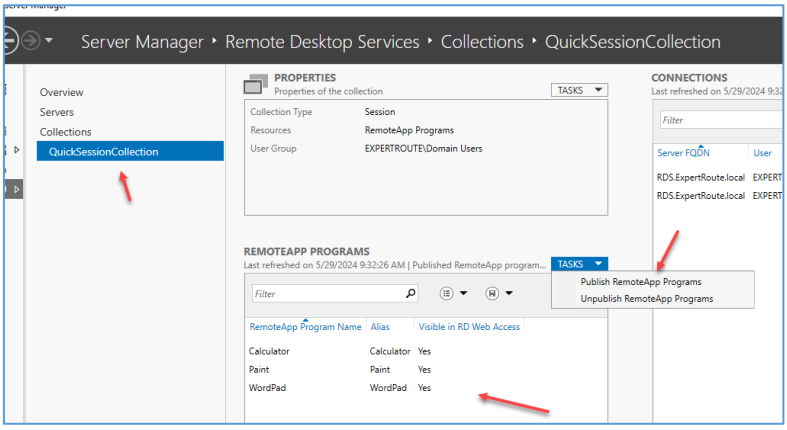
شکل ۸- ۶۲۵ اجرای نرم‌افزار از طریق سرویس *Remote Desktop*

اگر به مانند شکل ۸-٦۲٦، وارد قسمت Collections شوید، از قبل یک Collection با نام QuickSessionCollection ایجاد شده است که برای بررسی آن وارد شوید.



شکل ۸- ۶۲۶ اجرای نرم‌افزار از طریق سرویس *Remote Desktop*

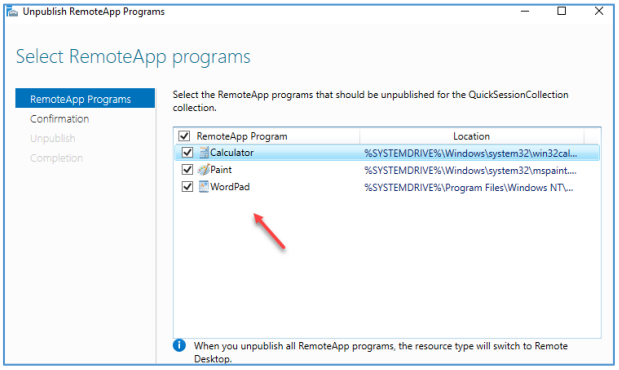
در شکل ۸-٦۲۷، همان سه نرم افزاری که در قسمت قبل با هم مشاهده و اجرا کردیم را می‌بینید، زمانی که حالت Quick Start را در هنگام نصب سرویس انتخاب می‌کنید این سه نرم‌افزار به صورت پیش‌فرض Publish می‌شود.



شکل ۸- ۶۲۷ اجرای نرم‌افزار از طریق سرویس *Remote Desktop*

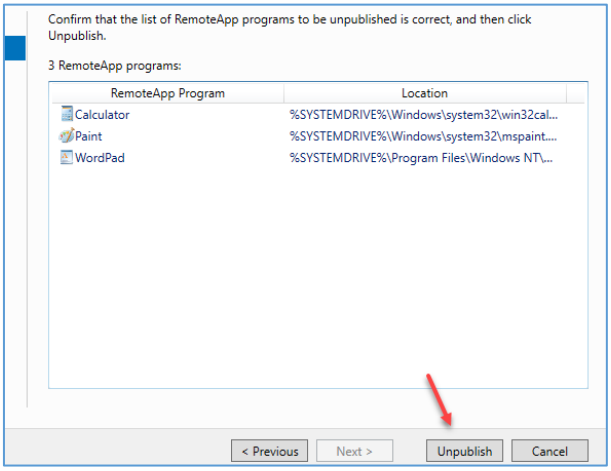
www.takbook.com

اگر می‌خواهید نرم افزارهای مورد نظر را حذف کنید می‌توانید بر روی Unpublish کلیک کنید تا شکل ۸-۶۲۸، ظاهر شود، بعد نرم افزار را انتخاب و Next کنید.



شکل ۸- ۶۲۸ اجرای نرم‌افزار از طریق سرویس Remote Desktop

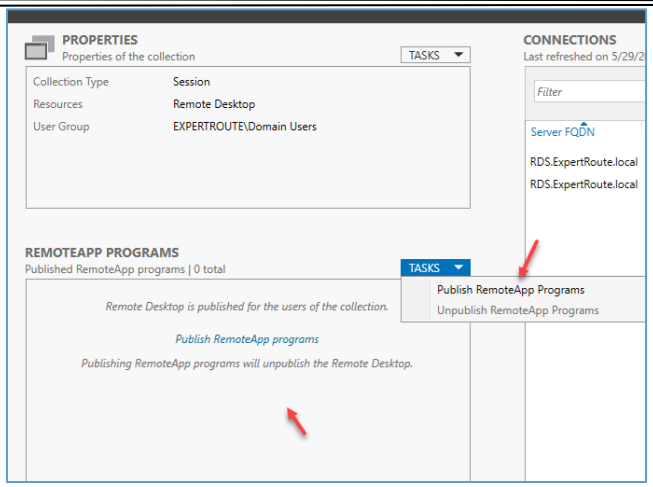
در شکل ۸-۶۲۹، بر روی Unpublish کلیک کنید تا نرم افزارها از لیست حذف شوند.



شکل ۸- ۶۲۹ اجرای نرم‌افزار از طریق سرویس Remote Desktop

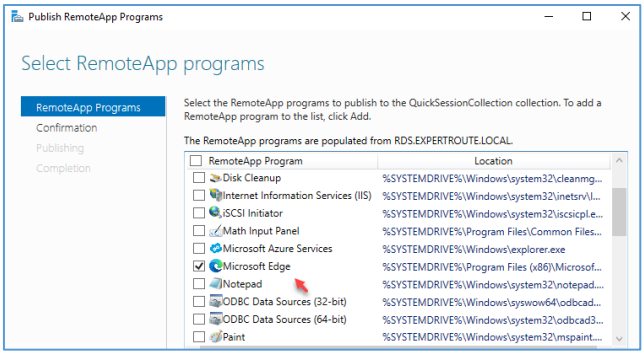
همان‌طور که در شکل ۸-۶۳۰، مشاهده می‌کنید نرم افزارهای مورد نظر پاک شده و برای ایجاد یک نرم‌افزار دلخواه از قسمت TASKS گزینه‌ی Publish… را انتخاب کنید.

www.takbook.com



شکل ۸- ۶۳۰ اجرای نرم‌افزار از طریق سرویس *Remote Desktop*

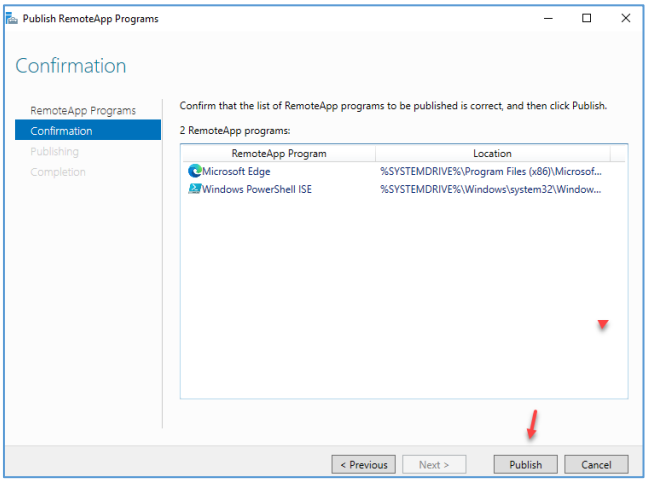
در شکل ۸-۶۳۱، شما می‌توانید از لیست مورد نظر نرم‌افزارهای مشخص شده را انتخاب کنید و یا اینکه بر روی Add کلیک کنید و یک نرم‌افزار خاص که در یک مسیر خاص قرار دارد را انتخاب کنید.



شکل ۸- ۶۳۱ اجرای نرم‌افزار از طریق سرویس *Remote Desktop*

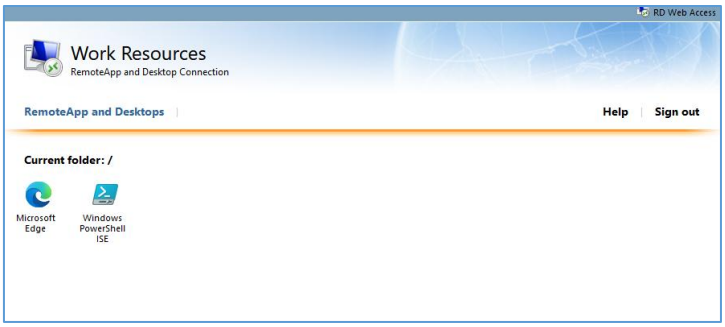
در شکل ۸-۶۳۲، دو نرم‌افزار انتخاب شده و باید بر روی Publish کلیک کنید.

www.takbook.com



شکل ۸- ۶۳۲ اجرای نرم‌افزار از طریق سرویس *Remote Desktop*

بعد از Publish اگر صفحه‌ی وب را بررسی کنیم این دو نرم افزار را به صورت شکل ۸-٦۳۳، مشاهده خواهید کرد، با کلیک بر روی هر کدام، نرم افزارها اجرا خواهند شد.

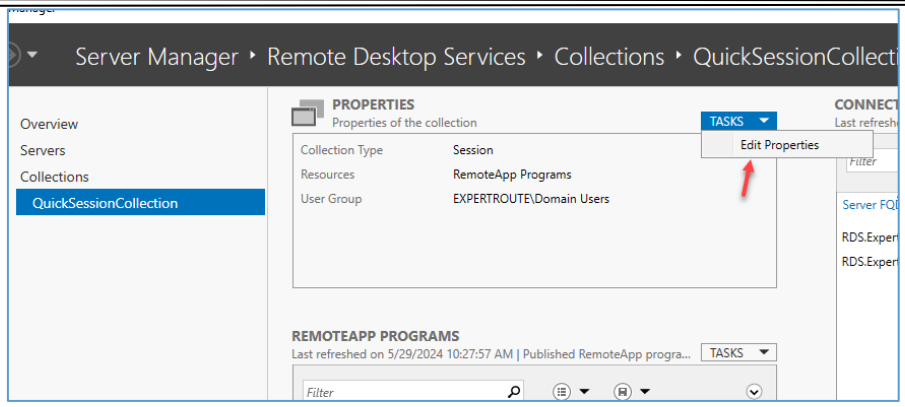


شکل ۸- ۶۳۳ اجرای نرم‌افزار از طریق سرویس *Remote Desktop*

۸-۳-۱۹-۳ بررسی تنظیمات Session Collection

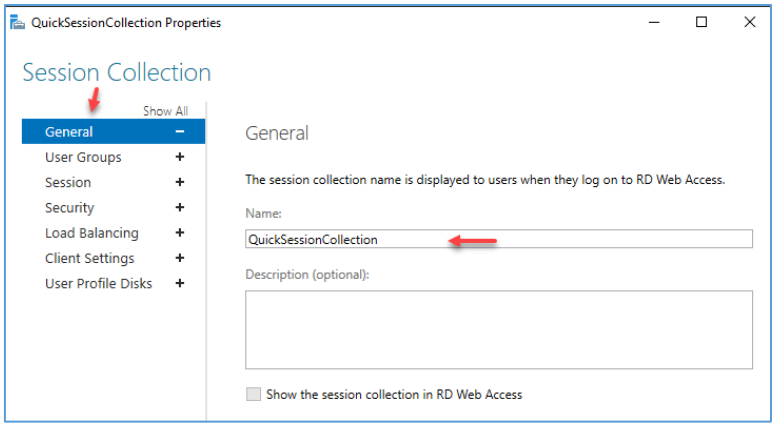
برای اینکه بعضی از تنظیمات مهم Collection خود را بررسی کنیم درServer Manager و در قسمت Properties به مانند شکل ۸-٦۳٤، بر روی Tasks کلیک کنید و گزینه‌ی Edit Properties را انتخاب کنید.

www.takbook.com



شکل ۸- ۶۳۴ تنظیمات *Session Collection*

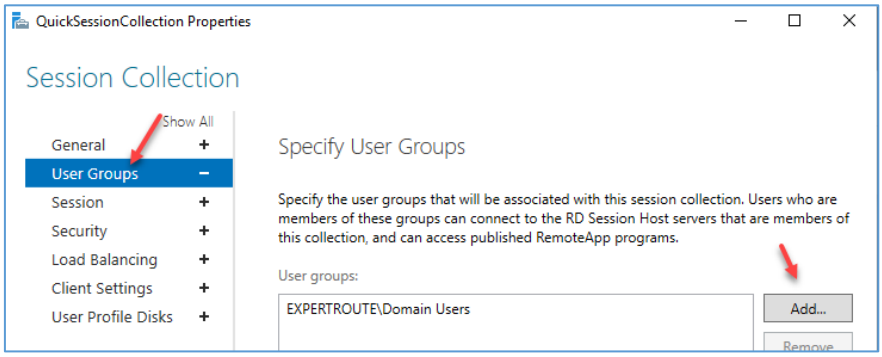
در شکل ۸-۶۳۵، در تب General می‌توانید نام Collection خود را تغییر دهید و توضیحات مربوط به آن را وارد کنید.



شکل ۸- ۶۳۵ تنظیمات *Session Collection*

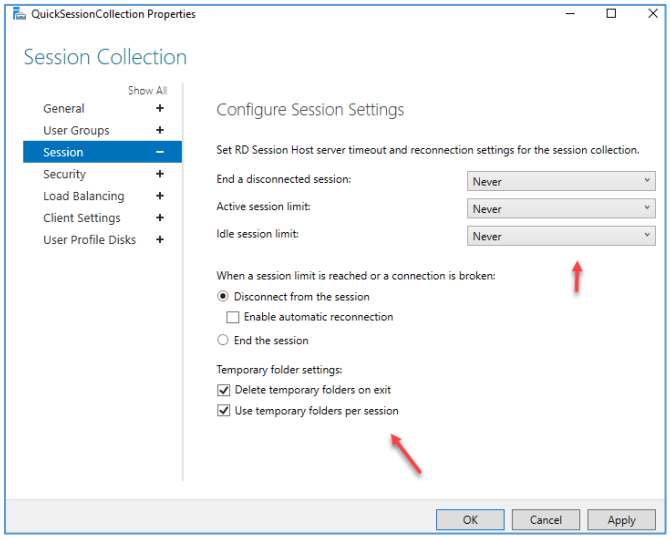
به مانند شکل ۸-۶۳۶، در قسمت User Groups یک گروه با عنوان Domain Users را مشاهده می‌کنید و این گروه همان گروهی است که تمام کاربران دومین به صورت پیش‌فرض عضو آن هستند، اگر بخواهید به کاربران خاصی دسترسی دهید باید این گروه را از لیست پاک کنید و بعد از آن بر روی Add کلیک کنید و کاربران خاص را وارد لیست کنید تا فقط همان کاربران دسترسی لازم برای اجرا داشته باشند.

www.takbook.com



شکل ۸- ۶۳۶ تنظیمات *Session Collection*

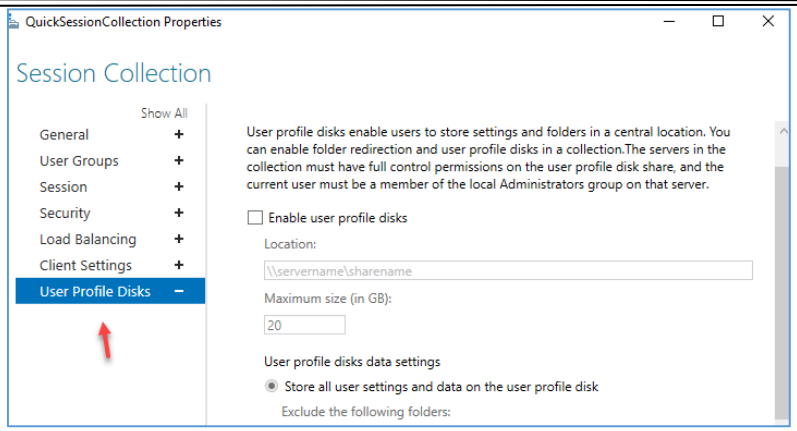
قسمت بعدی Session است که به مانند شکل ۸-۶۳۷، می‌توانید مشخص کنید که زمانی که یک کاربر به سرور متصل شد چقدر زمان ارتباط پایدار باشد که در شکل ۸-۶۳۷ریال بر روی Never قرار دارد و این یعنی اینکه تا زمانی که کابر خودش نخواهد ارتباط آن قطع نخواهد شد، اگر به قسمت پایین صفحه توجه کنید که مشخص کرده بعد از خروج کاربر از ارتباط مورد نظر تمام فایل‌های موقتی که ایجاد کرده از سرور پاک می‌شود.



شکل ۸- ۶۳۷ تنظیمات *Session Collection*

قسمت‌های دیگر نیاز به توضیحی در حال حاضر ندارند ولی اگر به مانند شکل ۸-۶۳۸، به قسمت User Profile Disks نگاه کنید، در این قسمت می‌توانید مسیر پیش‌فرض ایجاد Profile برای کاربران را به یکی سرور دیگر انتقال دهید، اگر این کار را نکنید تمام پروفایل‌ها در خود سرور RDS ایجاد خواهند شد.

www.takbook.com

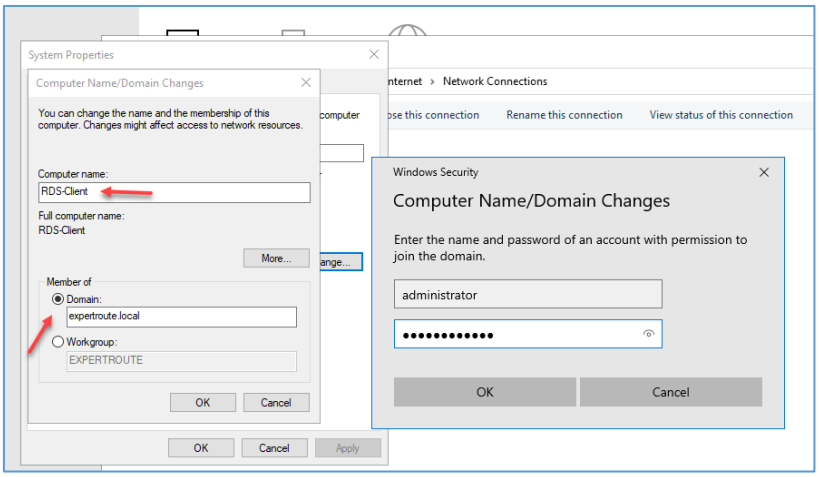


شکل ۸- ۶۳۸ تنظیمات *Session Collection*

نکته مهم : برای اینکه به صورت پیشرفته با این سرویس کار کنید باید از نرم‌افزار قدرتمند VMware Horizon استفاده کنید که یک پلتفرم مخصوص همین کار است و با این سرویس هماهنگ است، در مورد این نرم‌افزار در فصل شانزدهم به طور کامل صحبت کردیم.

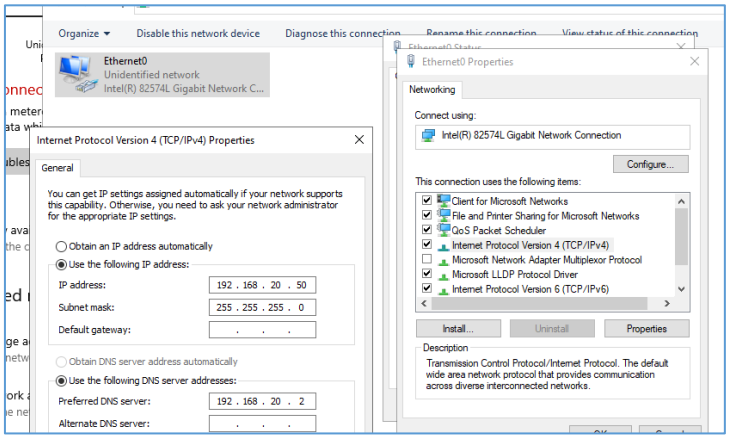
٨-٣-١٩-٤ فعال کردن Remote Desktop Clients

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. یک سرور جدید با نام RDS-Client ایجاد می‌کنیم و به صورت شکل ۸-۶۳۹ و شکل ۸-٦٤٠، نام و آدرس IP آن را مشخص می‌کنیم:



شکل ۸- ۶۳۹ فعال کردن *Remote Desktop Clients*

www.takbook.com

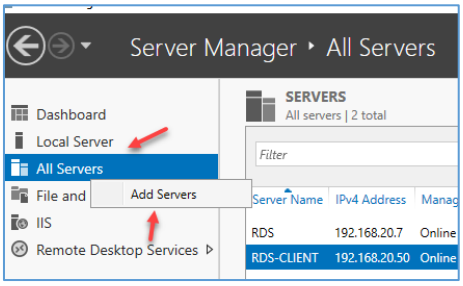


شکل ۸- ۶۴۰ فعال کردن *Remote Desktop Clients*

بعد از اینکه سرور مورد نظر را ایجاد و آن را عضو دومین کردید دیگر با سرور مورد نظر کاری نداریم و ادامه کار را در سرور RDS انجام می‌دهیم.

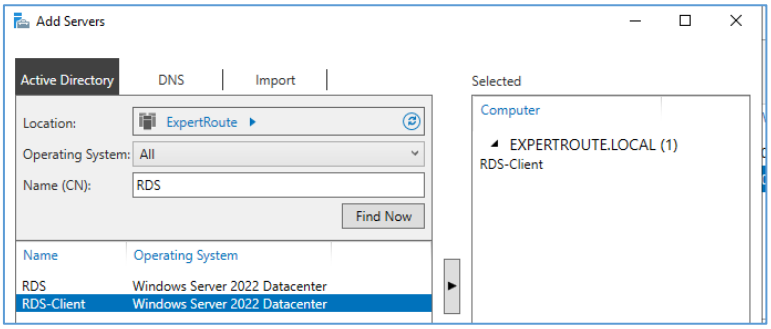
وارد سرور RDS شوید و Server Manager را اجرا کنید.

به مانند شکل ۸-٦٤١، در قسمت All Servers کلیک راست کنید و گزینه‌ی Add Servers را انتخاب کنید.



شکل ۸- ۶۴۱ فعال کردن *Remote Desktop Clients*

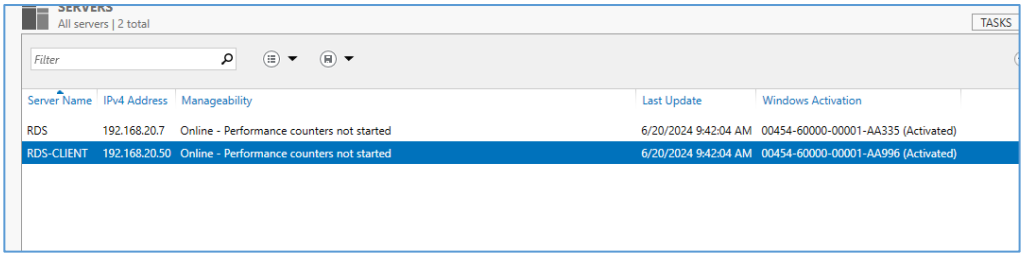
در شکل ۸-٦٤٢، نام سرور جدید را جستجو و به لیست اضافه کنید.



شکل ۸- ۶۴۲ فعال کردن *Remote Desktop Clients*

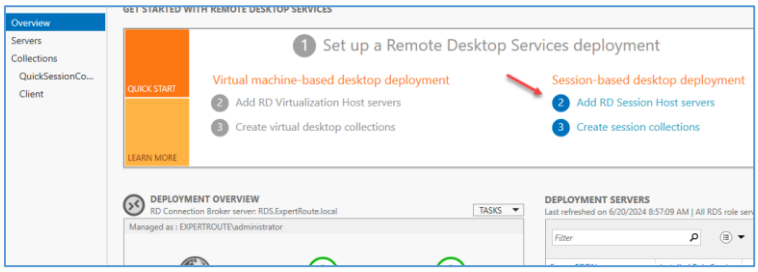
www.takbook.com

همان‌طور که در شکل ۸–٦٤٣، مشاهده می‌کنید سرور جدید به لیست اضافه شده است.



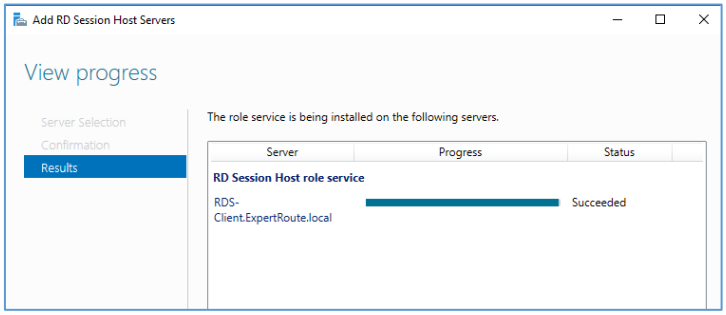
شکل ۸- ۶۴۳ فعال کردن *Remote Desktop Clients*

چون از قبل سرویس Remote Desktop را بر روی سرور RDS نصب کردیم دیگر نیازی به نصب دوباره آن نیست و فقط به مانند شکل ۸–٦٤٤، وارد سرویس Remote Desktop در Server Manager شوید و بر روی Add RD Seesion Host servers کلیک کنید.



شکل ۸- ۶۴۴ فعال کردن *Remote Desktop Clients*

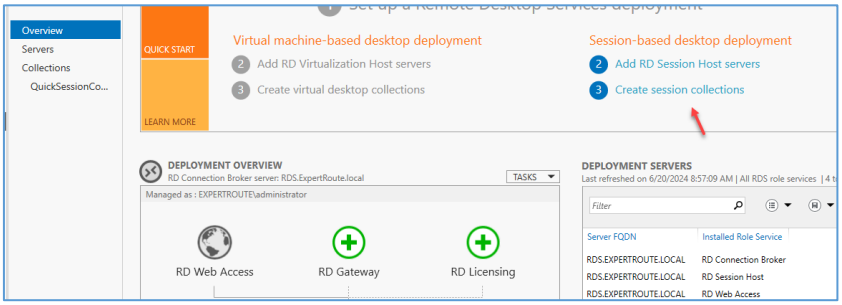
به مانند شکل ۸–٦٤٥، سرور RDS-Client را به لیست اضافه کنید و بر روی Next کلیک کنید تا تنظیمات لازم بر روی سرور RDS-Client انجام شود، توجه داشته باشید در موقع نصب سرویس سرور RDS-Client ری استارت خواهد شد.



شکل ۸- ۶۴۵ فعال کردن *Remote Desktop Clients*

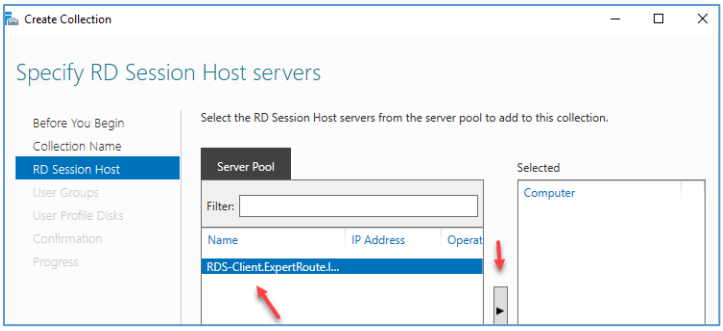
بعد از نصب سرویس بر روی سرور جدید، دوباره وارد سرور RDS شوید و به مانند شکل ۸–٦٤٦، از قسمت Remote Desktop گزینه‌ی Create session collections را انتخاب کنید.

www.takbook.com



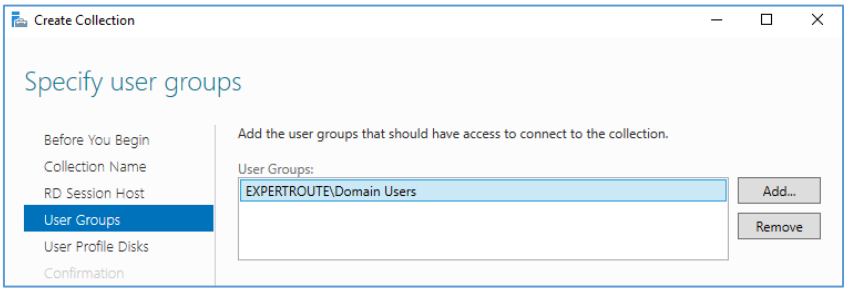
شکل ۸- ۶۴۶ فعال کردن *Remote Desktop Clients*

در ادامه و در صفحه‌ی اول یک نام به دلخواه وارد کنید و در ادامه و در شکل ۸-٦٤٧، سرور RDS-Client را با جهت نما مشخص شده به لیست اضافه کنید و بر روی Next کلیک کنید.



شکل ۸- ۶۴۷ فعال کردن *Remote Desktop Clients*

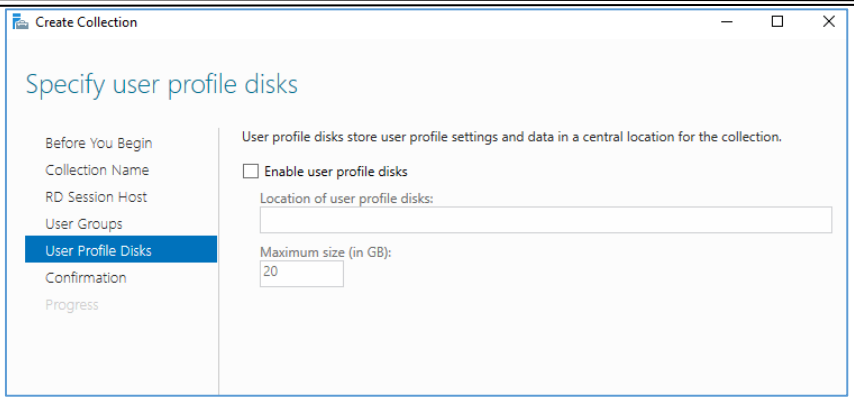
در صفحه ۸-٦٤٨، باید مشخص کنید چه کسانی می‌توانند به سرور مورد نظر Remote بزنند که به صورت پیش‌فرض گروه Domain Users انتخاب شده است.



شکل ۸- ۶۴۸ فعال کردن *Remote Desktop Clients*

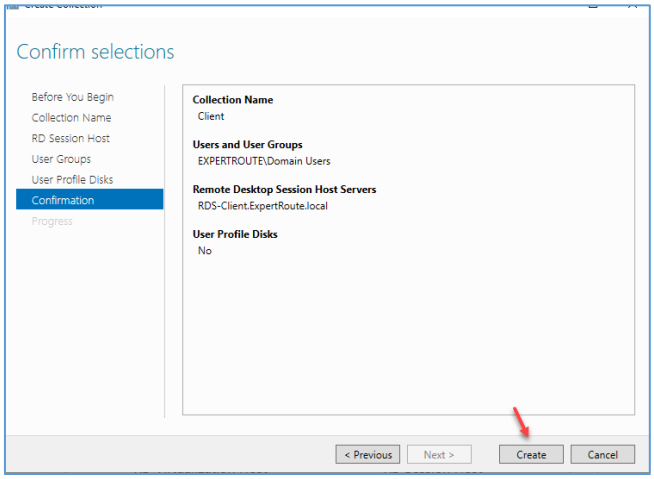
در شکل ۸-٦٤٩، می‌توانید مشخص کنید که Profile کاربران در کدام آدرس ذخیره شود که این آدرس را باید به صورت Share شده وارد کنید، اگر تیک گزینه‌ی مورد نظر را بردارید در همان سرور اطلاعات ذخیره خواهد شد.

www.takbook.com



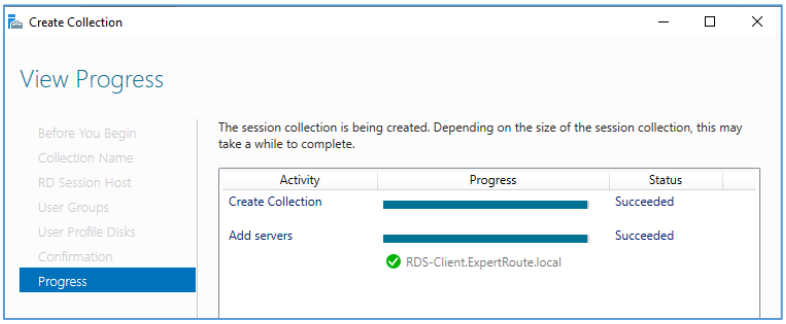
شکل ۸- ۶۴۹ فعال کردن *Remote Desktop Clients*

در شکل ۸-٦٥٠، بر روی Create کلیک کنید تا تنظیمات مورد نظر انجام شود.



شکل ۸- ۶۵۰ فعال کردن *Remote Desktop Clients*

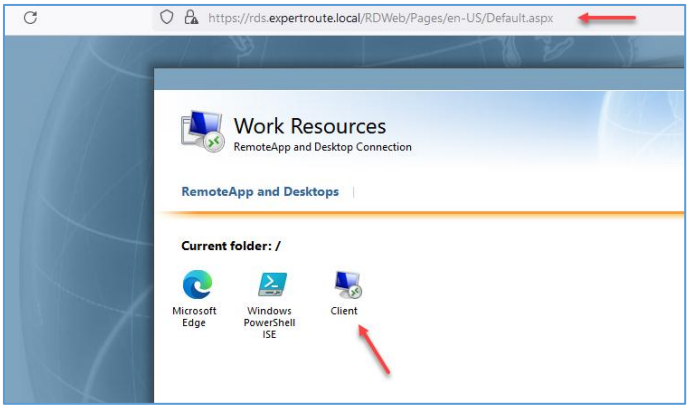
همان‌طور که شکل ۸-٦٥١، مشاهده می‌کنید سرویس مورد نظر به درستی تنظیم شده است.



شکل ۸- ۶۵۱ فعال کردن *Remote Desktop Clients*

www.takbook.com

بعد از انجام تنظیمات بالا اگر وارد یک کلاینت شوید و آدرس RDweb را به مانند شکل ۸-۶۵۲ اجرا کنید، همان‌طور که مشاهده می‌کنید آیکون Remote Desktop ظاهر شده است و نام Collection خود را که Client وارد کرده بودیم را مشاهده می‌کنید، بر روی آن کلیک کنید و در ادامه به صورت اتوماتیک وارد سرور خواهید شد.



شکل ۸- ۶۵۲ فعال کردن *Remote Desktop Clients*

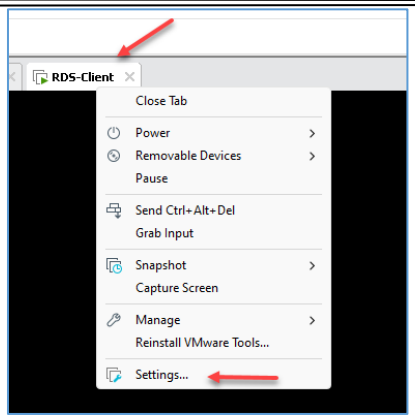
۸-۳-۱۹-۵ راه‌اندازی Virtual Host Server

در این قسمت می‌خواهیم از طریق سرویس Remote desktop یک ماشین مجازی در Hyper-v ایجاد کنیم و آن را به صورت Template در Remote Dekstop تنظیم کنیم و به کاربران اختصاص دهیم، اصولاً به این روش VDI گفته می‌شود.

اولین کاری که باید انجام دهید این است که سرویس Hyper-V را بر روی سرور فعال کنید، قبل از انجام این کار باید به این نکته توجه کنید که اگر از سرور فیزیکی استفاده می‌کنید مشکلی در تنظیمات پیدا نخواهید کرد، اما اگر از سرور مجازی که بر روی VMware اجرا شده است، استفاده می‌کنید باید یک تنظیم کوچک را انجام دهید تا سرویس Hyper-V بر روی ماشین مجازی نصب شود.

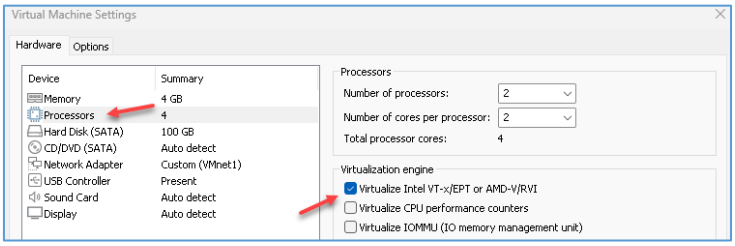
سروری که در قسمت قبل برای شما راه‌اندازی کردیم با نام RDS-Client بود که در این قسمت هم از آن استفاده می‌کنیم، برای تنظیم ماشین مجازی به مانند شکل ۸-۶۵۳، در نرم‌افزار VMware Workstation بر روی ماشین مجازی مورد نظر کلیک راست کنید و وارد Settings شوید.

www.takbook.com



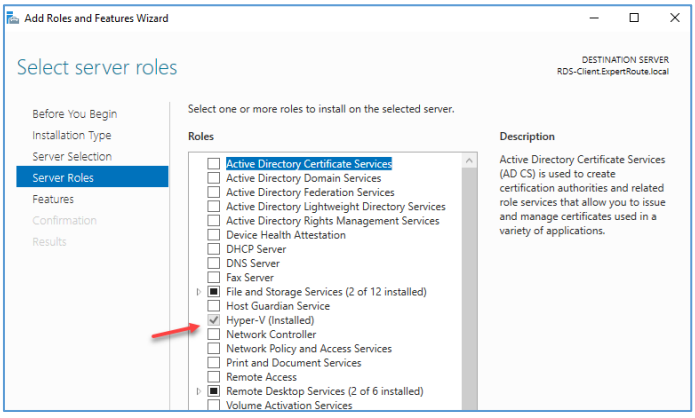
شکل ۸- ۶۵۳ راه‌اندازی *Virtual Host Server*

در ادامه و به مانند شکل ۸-٦٥٤، وارد قسمت Processors شوید و تیک گزینه‌ی Virtulize intel vt-x... را انتخاب و بر روی OK کلیک کنید، با این کار می‌توانید سرویس Hyper-V را بر روی سرور مجازی نصب کرد.



شکل ۸- ۶۵۴ راه‌اندازی *Virtual Host Server*

برای نصب سرویس Hyper-V وارد سرور RDS-Client شوید و و در Server Manager سرویس Hyper-V را به مانند شکل ۸-٦٥٥، انتخاب و نصب کنید.

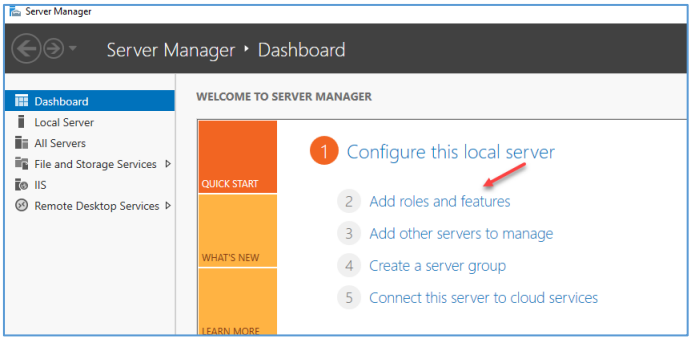


شکل ۸- ۶۵۵ راه‌اندازی *Virtual Host Server*

www.takbook.com

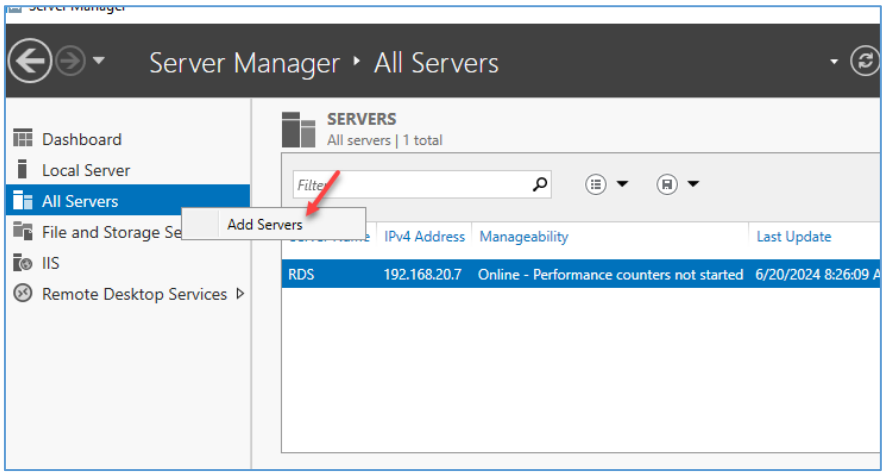
بعد از اینکه سرویس Hyper-V به درستی نصب شد باید وارد سرور RDS شویم و قابلیت Virtual Host Server را فعال کنیم و سرور RDS-Clinet را به آن معرفی کنیم.

به مانند شکل ۸-٦٥٦، در سرور RDS وارد Server Manager شوید و بر روی Add Roles and Features کلیک کنید.



شکل ۸- ۶۵۶ راه‌اندازی *Virtual Host Server*

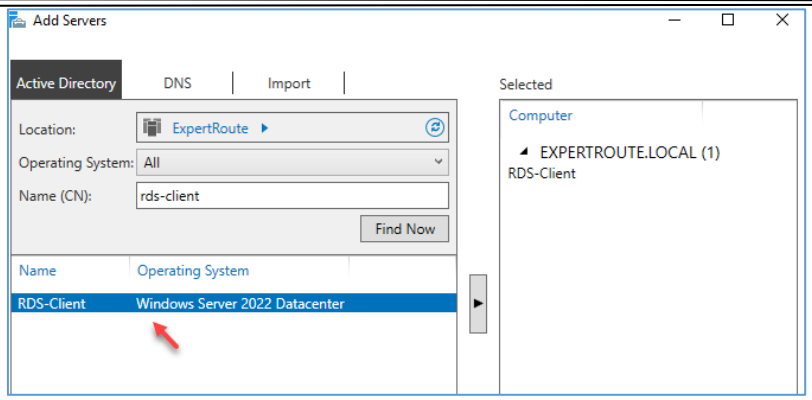
برای اینکه بتوانیم قابلیت Virtual Host Server را فعال کنیم، باید سرور RDS-Client را به سرور RDS اضافه کنیم، برای این کار به مانند شکل ۸-٦٥٧، در Server Manager بر روی All Servers کلیک راست کنید و گزینه‌ی Add Servers را انتخاب کنید.



شکل ۸- ۶۵۷ راه‌اندازی *Virtual Host Server*

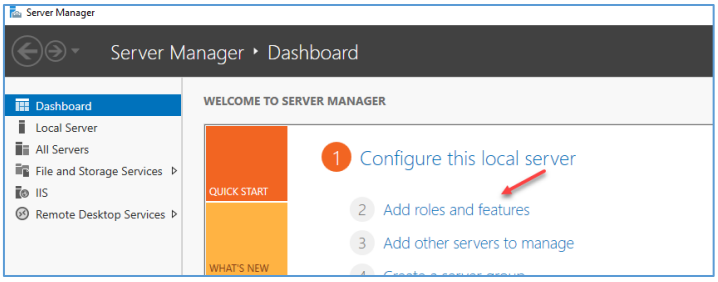
به مانند شکل ۸-٦٥٨، نام سرور مورد نظر را جستجو کنید و آن را به استفاده از جهت‌نما به لیست اضافه کنید، با این کار در سرور RDS می‌توانیم تنظیمات RDS-Client را انجام دهیم.

www.takbook.com



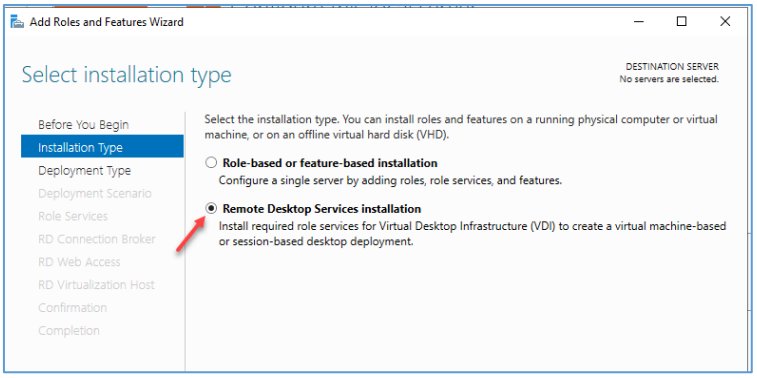
شکل ۸- ۶۵۸ راه‌اندازی *Virtual Host Server*

بعد از اینکه سرور را به لیست اضافه کردیم باید به مانند شکل ۸-۶۵۹، بر روی Add Role and Features کلیک کنید.



شکل ۸- ۶۵۹ راه‌اندازی *Virtual Host Server*

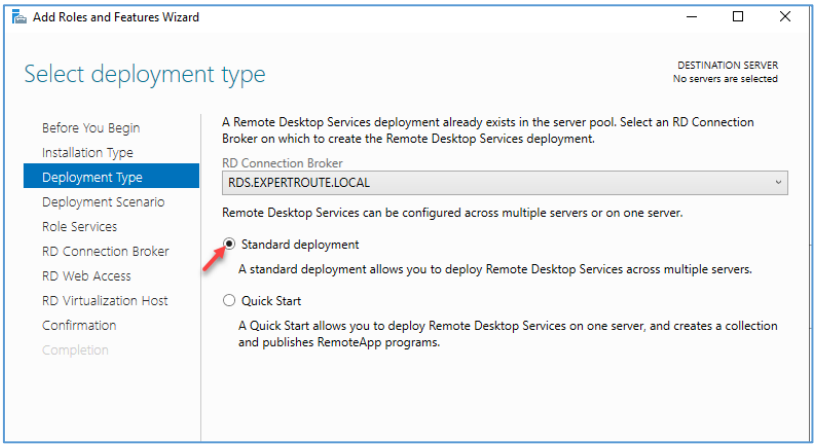
در شکل ۸-۶۶۰، گزینه‌ی Remote Desktop Services installation را انتخاب کنید.



شکل ۸- ۶۶۰ راه‌اندازی *Virtual Host Server*

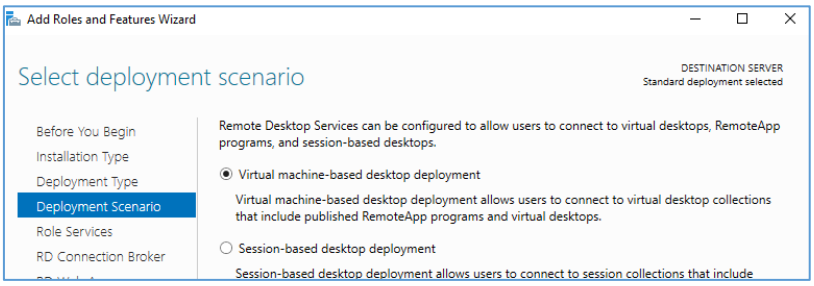
در شکل ۸-۶۶۱، گزینه‌ی Standard Deployment را انتخاب کنید.

www.takbook.com



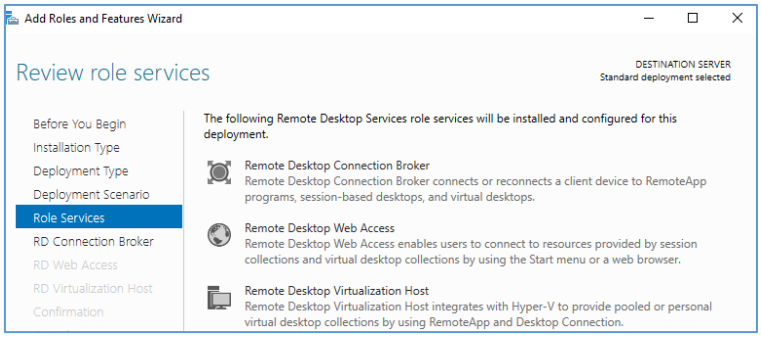
شکل ۸- ۶۶۱ راه‌اندازی *Virtual Host Server*

در شکل ۸-٦٦٢، گزینه‌ی Virtual machine-based desktopdeployment را انتخاب کنید.



شکل ۸- ۶۶۲ راه‌اندازی *Virtual Host Server*

در شکل ۸-٦٦٣، یک ویژگی را مشاهده می‌کنید که باید آنها را در ادامه فعال کنید، البته قبلاً دو ویژگی اول را برای سرور RDS فعال کردیم.

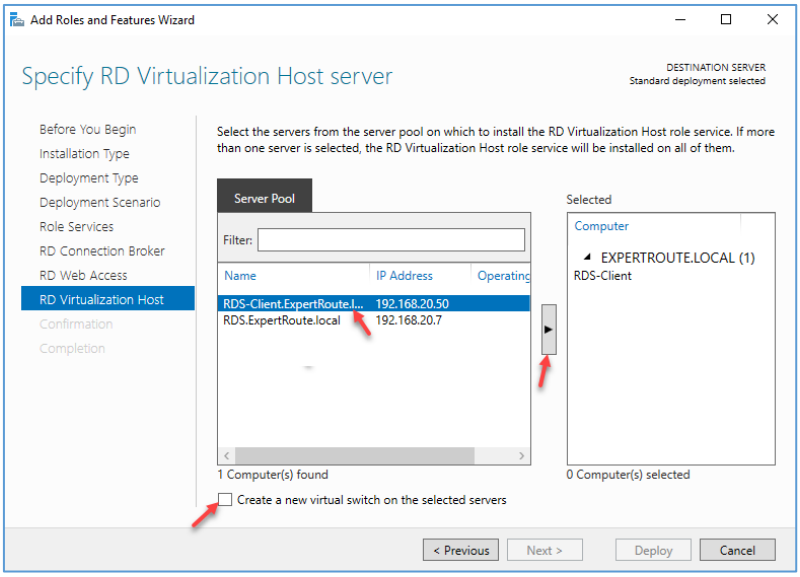


شکل ۸- ۶۶۳ راه‌اندازی *Virtual Host Server*

همان‌طور که بیان کردیم دو قسمت RD Web Access و RD Connection Broker مربوط به سرور RDS است که قبلاً فعال شده است اگر برای شما فعال نیست سرور RDS را به لیست اضافه کنید و در شکل

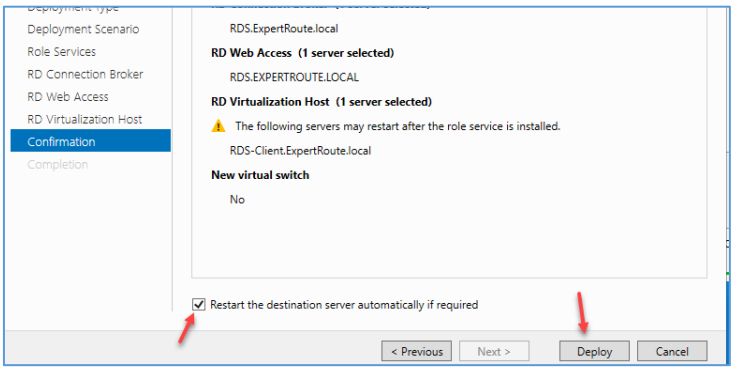
www.takbook.com

۸-٦٦٤، در قسمت RD Virtualization Host سرور RDS-Client را به لیست اضافه کنید، به این نکته مهم توجه کنید که برای اینکه ارتباط بین دو سرور برقرار باشد باید تیک گزینه‌ی Create a new virtual Switch را انتخاب کنید تا یک کارت شبکه مجازی بین این دو سرور ایجاد شود تا در زمان ایجاد ماشین مجازی بتوانیم از این کارت استفاده کنیم.



شکل ۸- ۶۶۴ راه‌اندازی *Virtual Host Server*

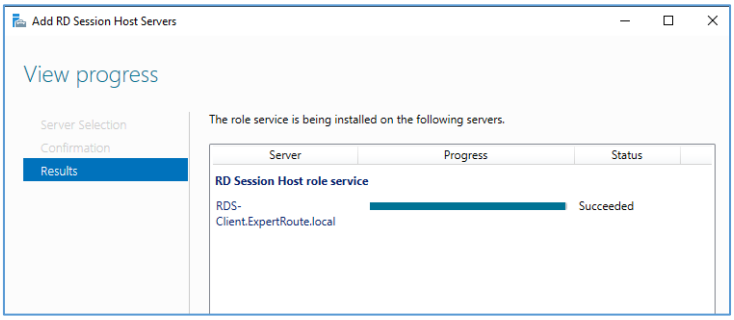
در شکل ۸-٦٦٥، تیک گزینه‌ی ... Restart را انتخاب کنید و بر روی Deploy کلیک کنید، بعد از انجام این کار سرویس مورد نظر بر روی سرور RDS-Client فعال خواهد شد و سرور مورد نظر Restart می‌شود.



شکل ۸- ۶۶۵ راه‌اندازی *Virtual Host Server*

همان‌طور که در شکل ۸-٦٦٦، مشاهده می‌کنید، سرویس مورد نظر بر روی RDS-Client نصب شد.

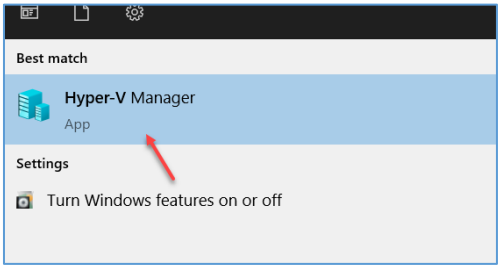
www.takbook.com



شکل ۸- ۶۶۶ راه‌اندازی *Virtual Host Server*

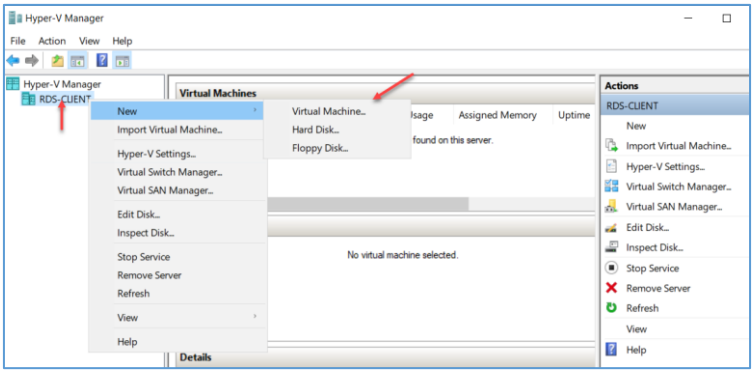
قبل از اینکه ادامه کار را در سرور RDS انجام دهیم باید وارد سرور RDS-Client شویم و یک ماشین مجازی ایجاد کنیم.

سرویس Hyper-V در سرور RDS-Client به مانند شکل ۸-٦٦٧، اجرا کنید.



شکل ۸- ۶۶۷ راه‌اندازی *Virtual Host Server*

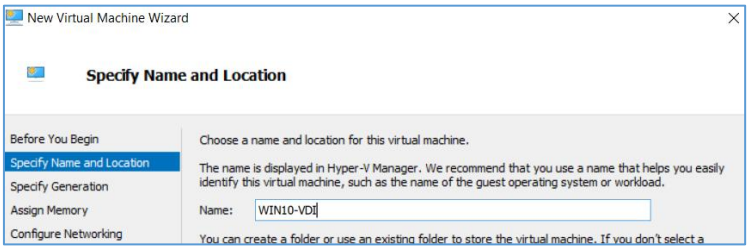
بعد از اجرای سرویس Hyper-V بایدبه مانند شکل ۸-٦٦٨، یک ماشین مجازی ایجاد کنیم و بر روی آن ویندوز مثلاً 10 را نصب کنیم تا بتوانیم در ادامه کار از آن یک Template ایجاد کنیم و به کاربران خود اختصاص دهیم..



شکل ۸- ۶۶۸ راه‌اندازی *Virtual Host Server*

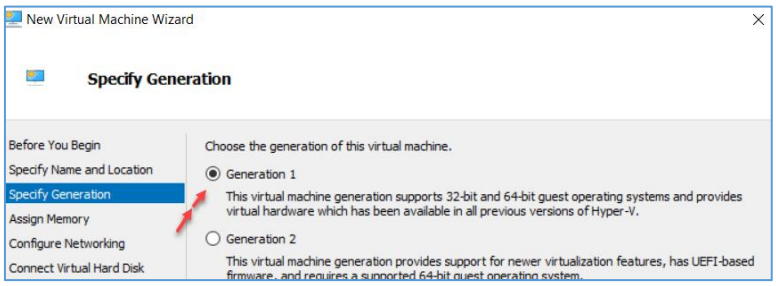
www.takbook.com

در شکل ۸-٦٦٩، یک نام برای ماشین مجازی خود وارد کنید و می‌توانید با انتخاب تیک گزینه‌ی Store... مسیر ماشین مجازی خود را تغییر دهید.



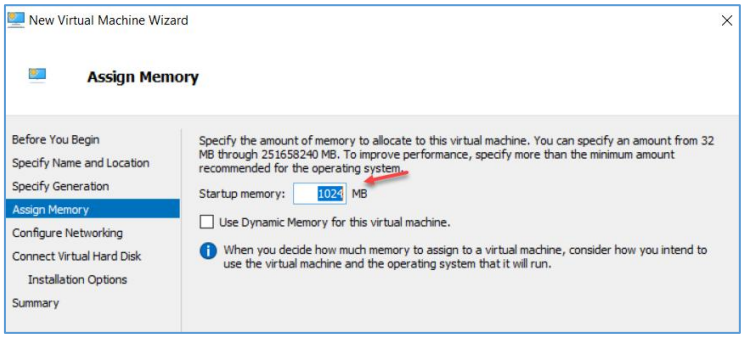
شکل ۸- ۶۶۹ راه‌اندازی *Virtual Host Server*

در شکل ۸-٦٧٠، دو گزینه وجود دارد که گزینه‌ی اوّل برای سیستم‌هایی که ورژن 32 bit و ٦٤bit را پشتیبانی می‌کنند و قدیمی هستند طراحی شده است و گزینه‌ی دوّم برای سخت‌افزارهای جدید که 64 bit را پشتیبانی می‌کنند و اینکه دارای UEFI می‌باشد، گزینه‌ی اوّل یا دوم را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۶۷۰ راه‌اندازی *Virtual Host Server*

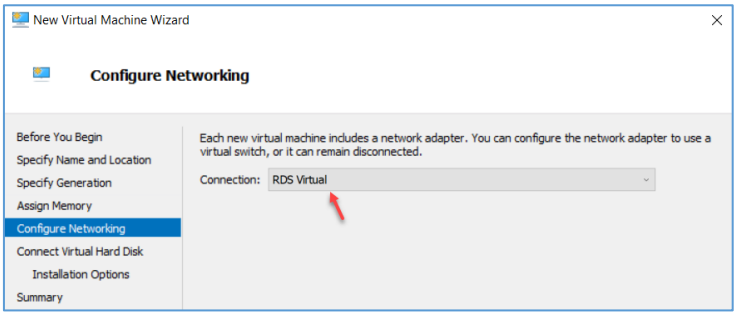
در شکل ۸-٦٧١، باید مقدار رم ماشین مورد نظر را وارد کنید که برای این ماشین 1 گیگابایت در نظر گرفتیم.



شکل ۸- ۶۷۱ راه‌اندازی *Virtual Host Server*

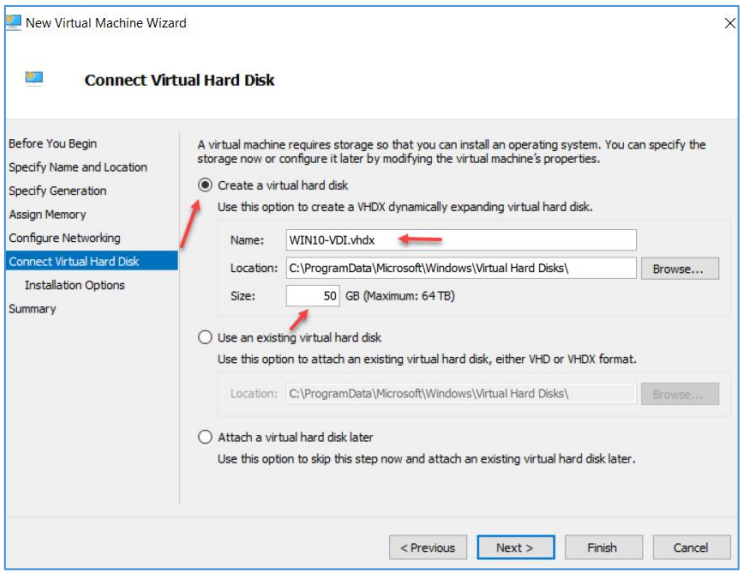
www.takbook.com

در شکل ۸-۶۷۲، کارت شبکه‌ی مورد نظر که بین دو سرور RDS و RDS-Client به صورت اتوماتیک ایجاد شده را انتخاب کنید، این کارت شبکه را در سرور RDS توضیح دادیم که باید تیک آن را انتخاب می‌کردید تا تنظیم آن انجام می‌شد.



شکل ۸- ۶۷۲ راه‌اندازی *Virtual Host Server*

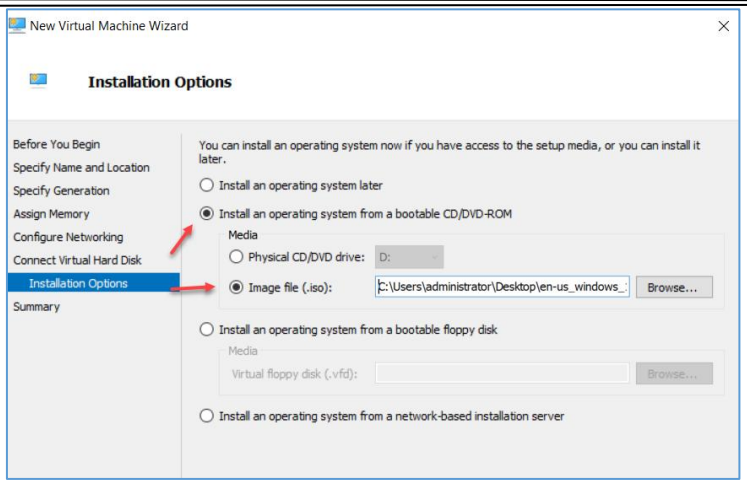
در شکل ۸-۶۷۳، باید هارد مجازی را ایجاد کنید، برای این کار گزینه‌ی اول را انتخاب کنید و مسیر و مقدار آن را مشخص کنید.



شکل ۸- ۶۷۳ راه‌اندازی *Virtual Host Server*

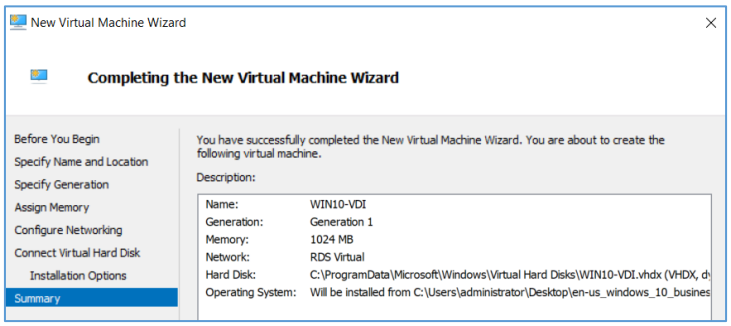
در شکل ۸-۶۷۴، باید image مربوط به ویندوز مورد نظر خود را معرفی کنید تا بتوانیم ویندوز را نصب کنیم.

www.takbook.com



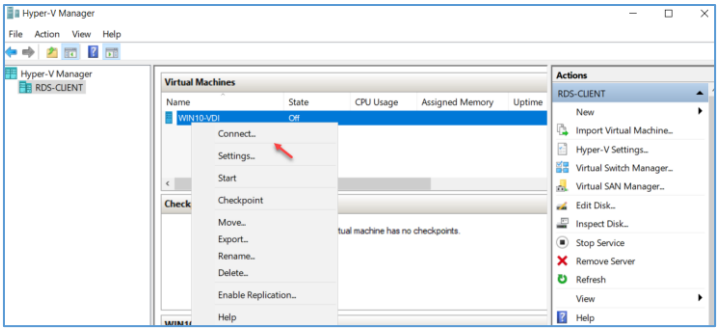
شکل ۸- ۶۷۴ راه‌اندازی *Virtual Host Server*

به مانند شکل ۸-۶۷۵، بر روی Finish کلیک کنید تا ماشین مورد نظر ایجاد شود.



شکل ۸- ۶۷۵ راه‌اندازی *Virtual Host Server*

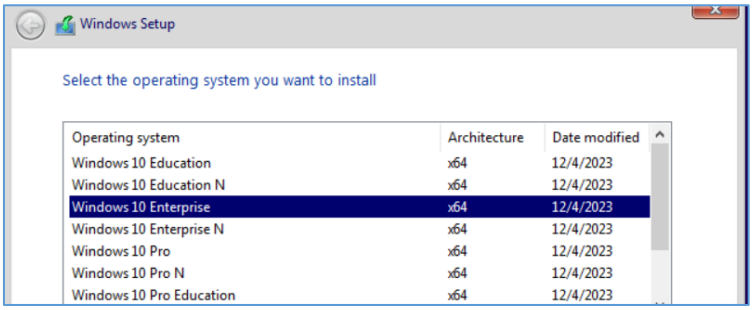
بعد از ایجاد ماشین مورد نظر به مانند شکل ۸-۶۷۶، بر روی Start کلیک کنید و نصب ویندوز را انجام دهید.



شکل ۸- ۶۷۶ راه‌اندازی *Virtual Host Server*

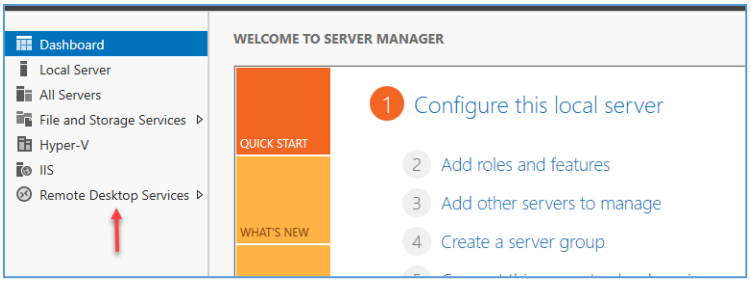
www.takbook.com

در هنگام نصب ویندوز باید به این نکته توجه کنید که ویندوز مورد نظر باید لایسنس VDI را داشته باشد، مثلاً اگر ورژن Enterprise را انتخاب کنید این ویژگی را پشتیبانی خواهد کرد که این موضوع را در شکل ۸-۶۷۷ مشاهده می‌کنید.



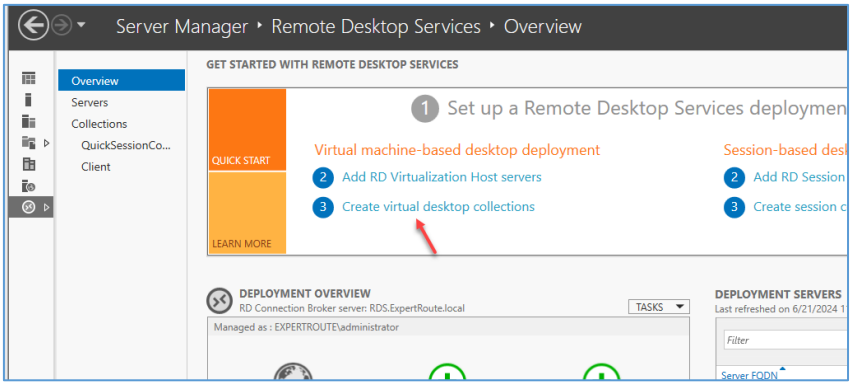
شکل ۸- ۶۷۷ راه‌اندازی Virtual Host Server

بعد از نصب ویندوز در Hyper-V و ایجاد ماشین مجازی باید دوباره به سرور RDS برگردیم و وارد Server Manager شوید و به مانند شکل ۸-۶۷۸، بر روی Remote Desktop Services کلیک کنید.



شکل ۸- ۶۷۸ راه‌اندازی Virtual Host Server

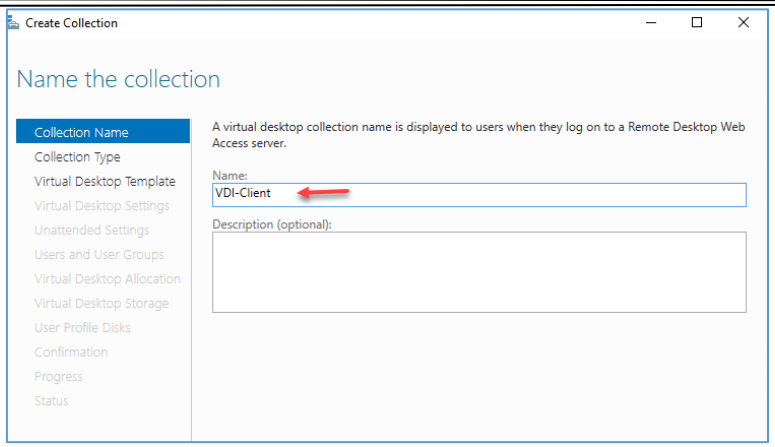
در شکل ۸-۶۷۹، بر روی Create virtual desktop collections کلیک کنید.



شکل ۸- ۶۷۹ راه‌اندازی Virtual Host Server

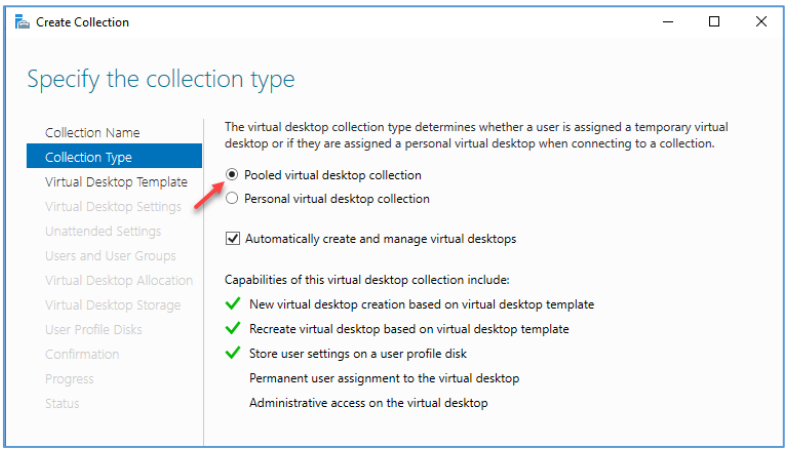
در شکل ۸-۶۸۰، یک نام برای Collection خود انتخاب کنید.

www.takbook.com



شکل ۸- ۶۸۰ راه‌اندازی *Virtual Host Server*

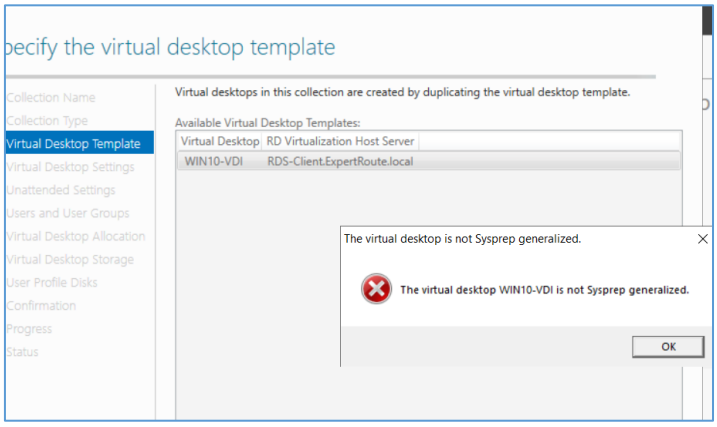
در شکل ۸-۶۸۱، دو گزینه را مشاهده می‌کنید که گزینه‌ی اول (Pooled) برای ایجاد و مدیریت جمی Remote dektop است و گزینه‌ی Personal برای ایجاد Remote Dekstop تکی برای کاربران است، بهترین گزینه را می‌توان Pooled نامید چون به صورت دست‌جمعی بر روی ماشین‌های ایجاد شده مدیریت می‌کند، مثلاً می‌توان آخرین آپدیت‌های امنیتی را روی آنها پیاده‌سازی کرد.



شکل ۸- ۶۸۱ راه‌اندازی *Virtual Host Server*

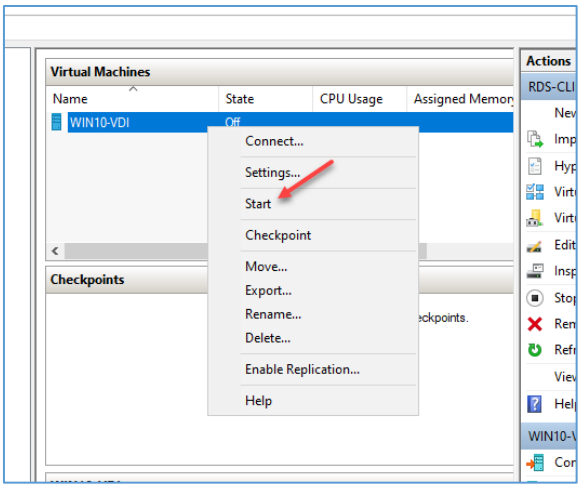
در شکل ۸-۶۸۲، سرور مجازی که در Hyper-V ایجاد کردیم را در لیست مشاهده می‌کنید، بر روی Next کلیک کنید که دو حالت دارد یا از این مرحله عبور خواهید کرد و یا اینکه با خطای زیر مواجه خواهید شد، این خطا مربوط به سرویس Sysprep است که در همین کتاب هم آن را بررسی کردیم، این سرویس برای ایجاد یک ID جدید برای ویندوز و تنظیم دوباره آن کاربرد دارد، برای حل این مشکل باید دستوری را در ماشین مجازی Hyper-v وارد کنید.

www.takbook.com



شکل ۸- ۶۸۲ راه‌اندازی *Virtual Host Server*

پس تا اینجا Stop کنید و به مانند شکل ۸-۶۸۳، وارد سرور RDS-Client شوید و سرویس Hyper-V را اجرا و وارد ماشین مجازی مورد نظر شوید.

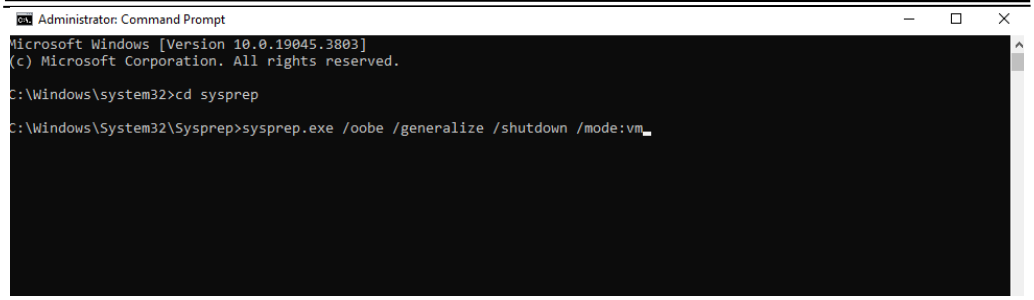


شکل ۸- ۶۸۳ راه‌اندازی *Virtual Host Server*

با استفاده از دستورات زیر و طبق شکل ۸-۶۸۴، Sysprep را اجرا و مد آن را به حالت VM تغییر می‌دهیم:

```
Cd sysprep
Sysprep.exe /oobe /generalize /shutdown /mode:vm
```

www.takbook.com

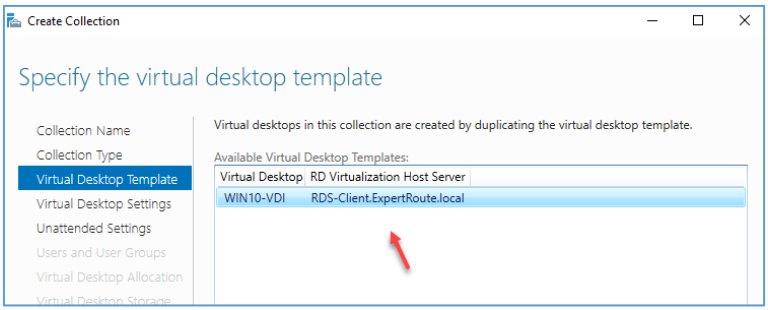


شکل ۸- ۶۸۴ راه‌اندازی *Virtual Host Server*

بعد از اجرا، Sysprep فعال شده و تنظیمات ویندوز را به حالت اولیه نصب بر می‌گرداند و شما می‌توانید آن را خاموش کنید و به سرور RDS برگردید و ادامه نصب را پیگیری کنیم.

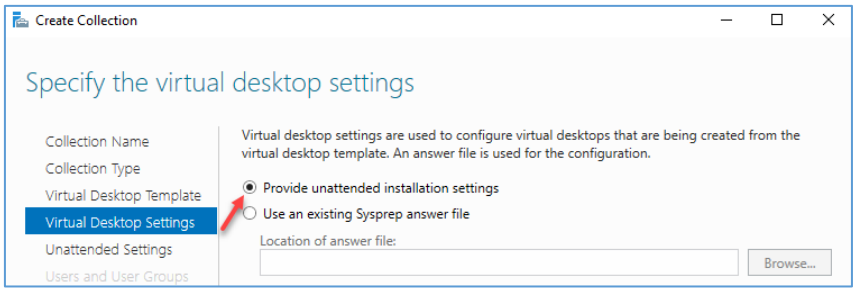
**** یک نکته بسیار مهم قبل از ادامه کار باید اشاره کنیم این است که برای اینکه سرویس ما به درستی کار کند باید در شبکه سرویس DHCP داشته باشیم، برای این کار باید وارد سرور Active Directory شوید و سرویس DHCP را نصب و راه‌اندازی کنید، برای راه‌اندازی این سرویس در همین فصل می‌توانید آموزش آن را مشاهده کنید.

در ادامه و در شکل ۸-۶۸۵، مرحله‌ی ساخت Collection که در این قسمت که خطا داشتیم می‌توانیم بر روی Next کلیک کنیم تا مرحله بعدی اجرا شود.



شکل ۸- ۶۸۵ راه‌اندازی *Virtual Host Server*

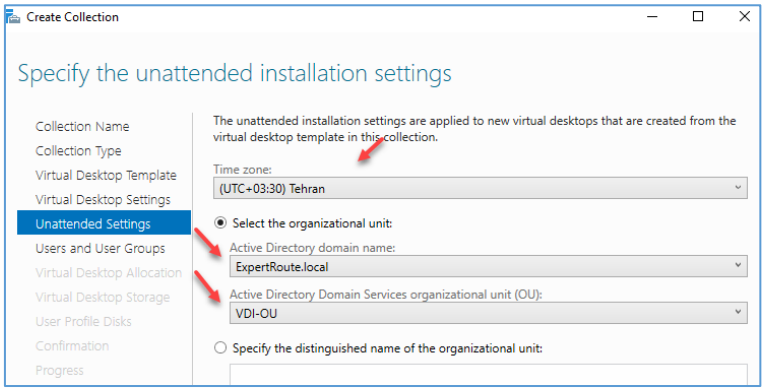
در شکل ۸-۶۸۶، گزینه‌ی اول را انتخاب کنید.



شکل ۸- ۶۸۶ راه‌اندازی *Virtual Host Server*

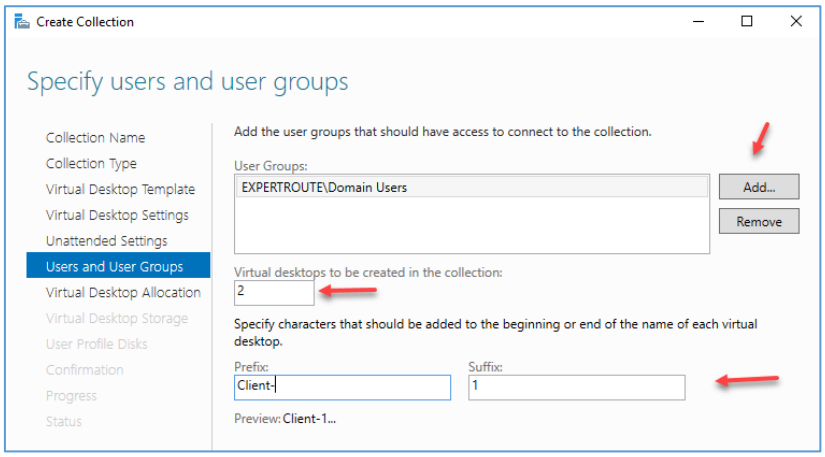
www.takbook.com

در شکل ۸-۶۸۷، باید منطقه زمانی را انتخاب کنید که +3:30 مربوط به تهران است و در ادامه برای اینکه مدیریت بهتری بر روی کارکرد این سرویس داشته باشید باید یک OU در Active Directory ایجاد کنید، البته این کار را در اوایل کتاب انجام دادیم، پس نام دومین و OU مورد نظر را انتخاب کنید.



شکل ۸- ۶۸۷ راه‌اندازی *Virtual Host Server*

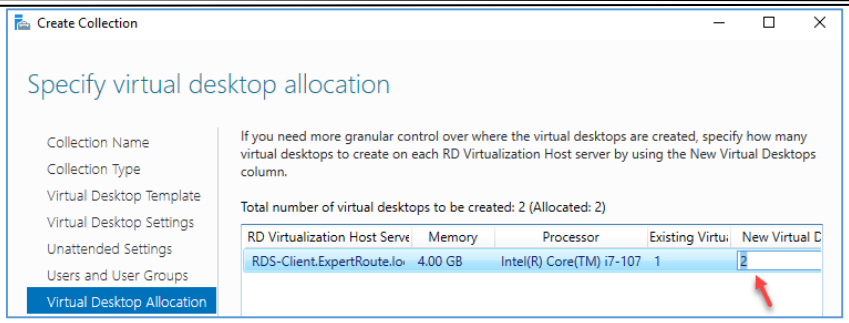
در شکل ۸-۶۸۸، باید مشخص کنید که چه کاربرانی توانایی متصل شدن به این Collection را داشته باشند، در قسمت دوم که عدد 2 نوشته شده است یعنی اینکه تعداد ماشین‌هایی که ایجاد می‌شود دو عدد است و در قسمت آخر هم می‌توانید مشخص کنید که نام ماشین‌ها به چه صورت باشد، ما در اینجا Client-1 را وارد کردیم که عدد یک تغییر خواهد کرد یعنی برای ماشین دوم می‌شود Client-2.



شکل ۸- ۶۸۸ راه‌اندازی *Virtual Host Server*

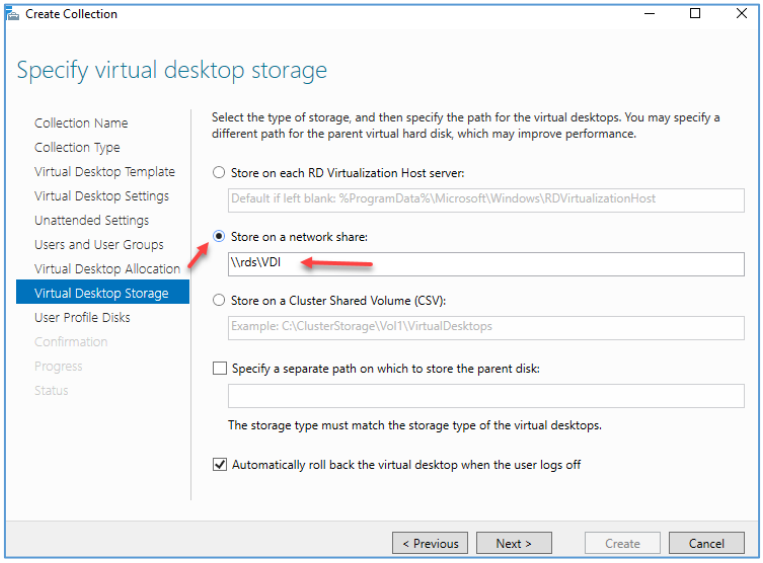
در شکل ۸-۶۸۹، سخت‌افزار سرور RDS را مشخص کرده است که باید تعداد ماشین مجازی را برای ایجاد مشخص کنید که عدد 2 نوشته شده است.

www.takbook.com



شکل ۸- ۶۸۹ راه‌اندازی *Virtual Host Server*

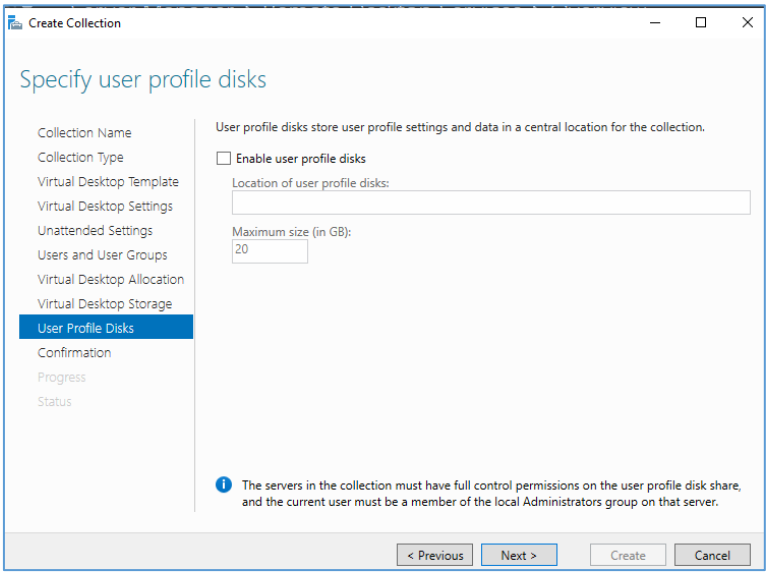
در ادامه کار و در شکل ۸-۶۹۰، باید مسیری را مشخص کنید که اطلاعات ماشین مجازی جدید در آن کپی شود، اگر بخواهید اطلاعات در همان سرور RDS-Client کپی شود می‌توانید از گزینه‌ی اول انتخاب کنید حالا اگر سرور RDS-Client مقدار فضای کافی نداشته باشد می‌توانیم از طریق گزینه‌ی دوم یک مسیر Share شده را وارد کنیم، که در این شکل یک پوشه با نام VDI در سرور RDS ایجاد شده که این پوشه در یک هارد 300 گیگابایتی است، و این مسیر را Share کردیم، توجه داشته باشید که در موقع Share سرور RDS-client$ باید دسترسی Read-Write به پوشه مورد نظر داشته باشد.



شکل ۸- ۶۹۰ راه‌اندازی *Virtual Host Server*

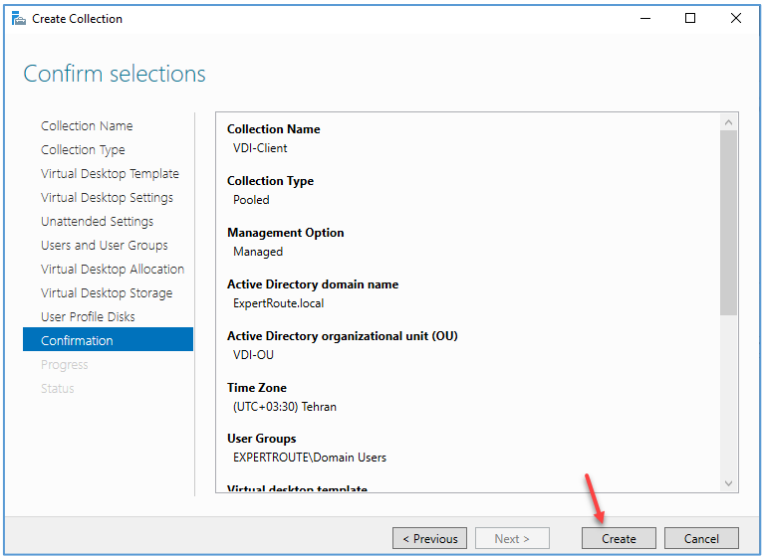
در شکل ۸-۶۹۱، می‌توانید مشخص کنید که اطلاعات User Profile کاربران در چه مسیری ذخیره شود که باید یک مسیر Share شده به آن معرفی کنید، اگر تیک گزینه‌ی مورد نظر را بردارید در همان مسیری که هارد دیسک ایجاد می‌شود ذخیره خواهد شد یعنی مسیری که Share کردیم، آدرس \\RDS\VDI.

www.takbook.com



شکل ۸- ۶۹۱ راه‌اندازی *Virtual Host Server*

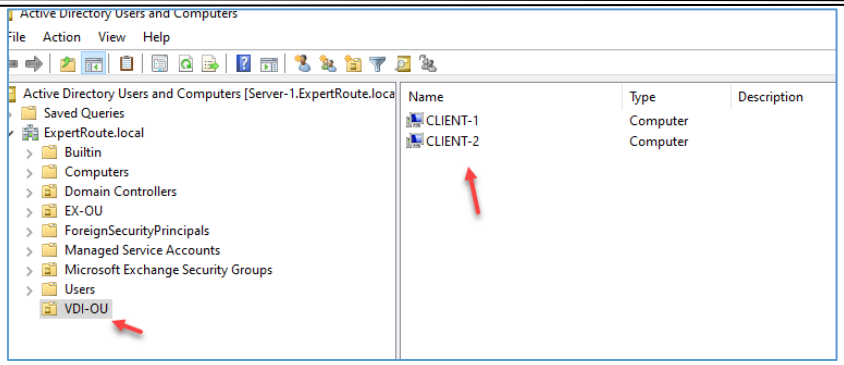
در نهایت و در شکل ۸-۶۹۲، اگر تنظیمات مورد نظر قابل قبول است بر روی Create کلیک کنید تا ماشین‌های مورد نظر ایجاد شود، توجه داشته باشید بسته به سرعت سیستم زمان‌بر خواهد بود.



شکل ۸- ۶۹۲ راه‌اندازی *Virtual Host Server*

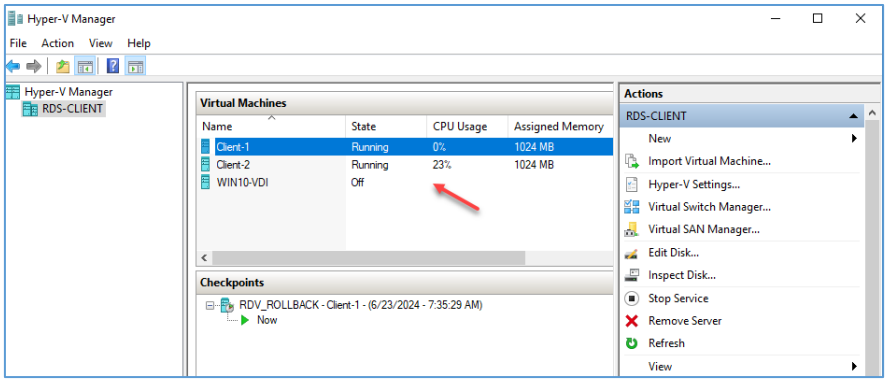
بعد از ایجاد Collection مورد نظر اگر به مانند شکل ۸-۶۹۳، وارد Active Directory شوید و OU مورد نظر که انتخاب کرده بودیم را مشاهده کنید کامپیوتری با نام Client1 و Client2 ایجاد شده است.

www.takbook.com



شکل ۸- ۶۹۳ راه‌اندازی *Virtual Host Server*

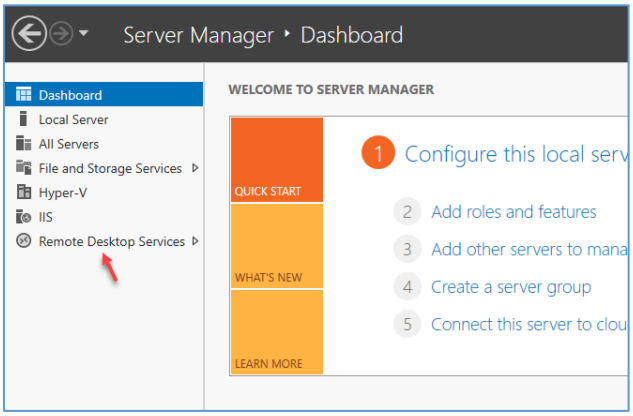
در سرویس Hyper-V هم Client-1 و Client-2 ایجاد و فعال شده است که این موضوع را در شکل ۸-٦٩٤، مشاهده می‌کنید.



شکل ۸- ۶۹۴ راه‌اندازی *Virtual Host Server*

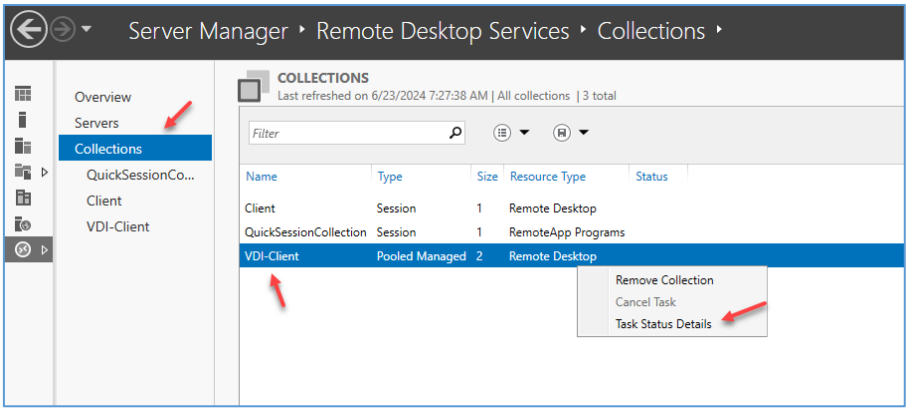
اگر خطایی در هنگام نصب رخ دهد، برای اینکه آن خطا را مشاهده کنید باید وارد سرور RDS شوید و Server Manager را اجرا کنید و به مانند شکل ۸-٦٩٥، بر روی Remote Dektop Services کلیک کنید.

www.takbook.com



شکل ۸- ۶۹۵ راه‌اندازی *Virtual Host Server*

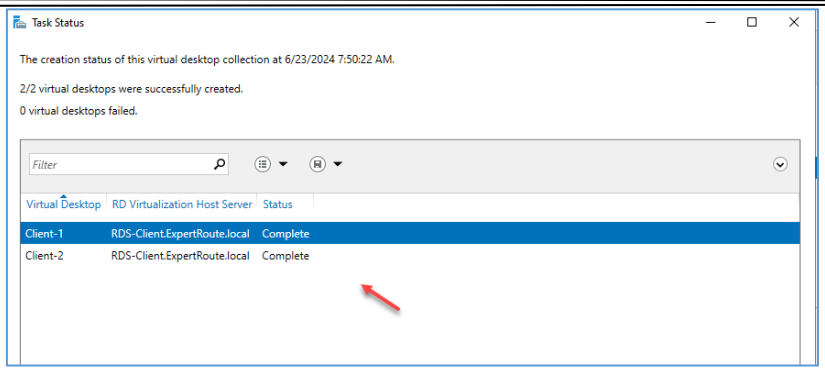
در شکل ۸-٦٩٦، باید بر روی Collections کلیک کنید و در قسمت مورد نظر بر روی VDI-Client که نام Collection ما بود کلیک راست کنید و گزینه‌ی Task Status Details را انتخاب کنید.



شکل ۸- ۶۹۶ راه‌اندازی *Virtual Host Server*

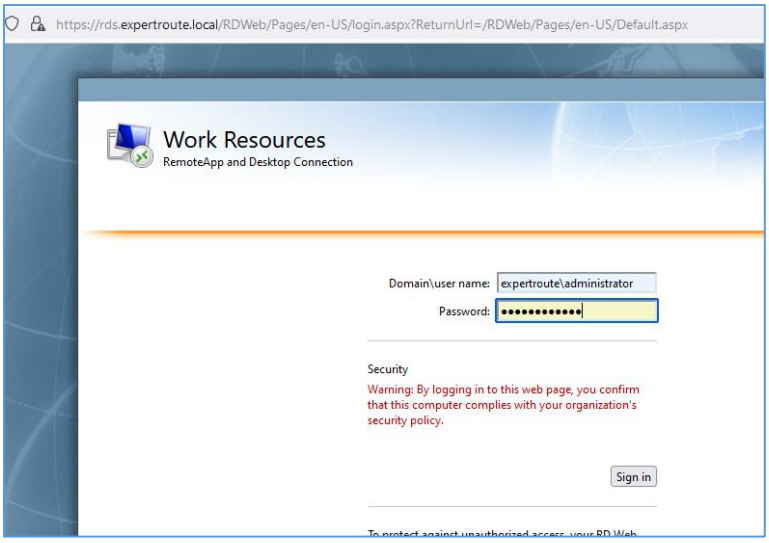
اگر به شکل ۸-٦٩٧، توجه کنید هر دو کلاینت با موفقیت ایجاد شده و خطایی رخ نداده است، مهمترین خطایی که در این قسمت رخ می‌دهد خطایی است که مربوط به سرویس DHCP است که اگر در شبکه این سرویس فعال نباشد، در زمان این ماشین‌های مجازی نمی‌توان به آنها به صورت اتوماتیک IP داد و به همین خاطر با مشکل روبرو خواهند شد سرویس Hyper-V به سرور RDS پاسخگو نخواهد بود.

www.takbook.com



شکل ۸- ۶۹۷ راه‌اندازی *Virtual Host Server*

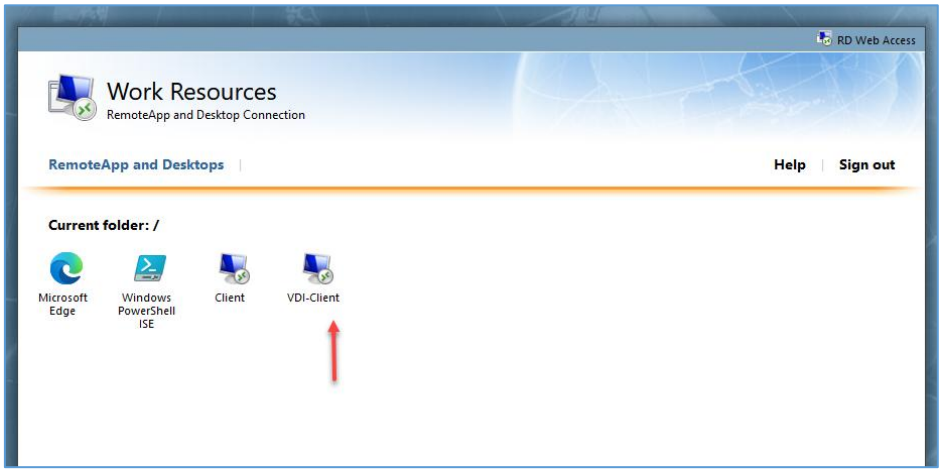
بعد از اتمام کار وارد کلاینت شوید و آدرس RDWEB را به مانند شکل ۸-٦۹۸، اجرا کنید و با نام کاربری Administrator وارد سایت شوید.



شکل ۸- ۶۹۸ راه‌اندازی *Virtual Host Server*

همان‌طور که در شکل ۸-٦۹۹، مشاهده می‌کنید، Collection جدیدی که ایجاد کردیم در لیست قرار گرفته است و می‌توانید با کلیک بر روی آن وارد سرور شوید.

www.takbook.com

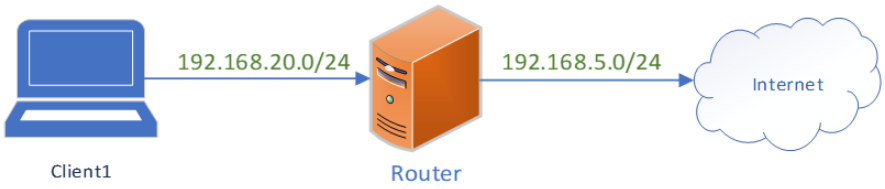


شکل ۸- ۶۹۹ راه‌اندازی *Virtual Host Server*

به این نکته توجه کنید که شما دو ماشین مجازی به صورت اتوماتیک ایجاد کردید وقتی کاربر می‌خواهد به این Collection که با نام VDI-Client ایجاد کردید متصل شود، یکی از این دو ماشین به انتخاب خود سرور RDS به کاربر تخصیص داده خواهد شد و User Profile هر کاربر هم در همه ماشین ها به صورت اشتراکی وجود دارد و فرقی ندارد که کاربر وارد کدام سرور مجازی شود.

۸-۳-۲۰ 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.



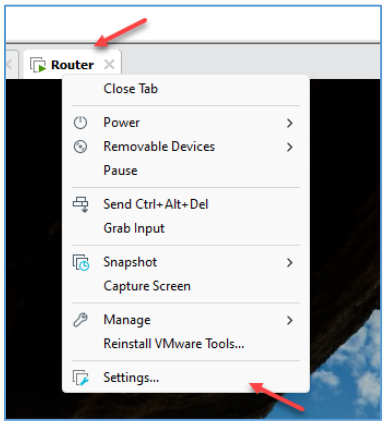
شکل ۸- ۷۰۰ سرویس *Remote Access*

در شکل ۸-۷۰۰، یک سرور با نام Router وجود دارد که کلاینت‌های شبکه از طریق آن می‌توانند به اینترنت متّصل شوند، برای این کار باید در سرور Router تنظیمات لازم را انجام دهید.

برای شروع یک ماشین مجازی با نام Router ایجاد کردیم و ویندوز سرور ۲۰۲۵ را بر روی آن نصب کردیم و آن را عضو دومین کردیم.

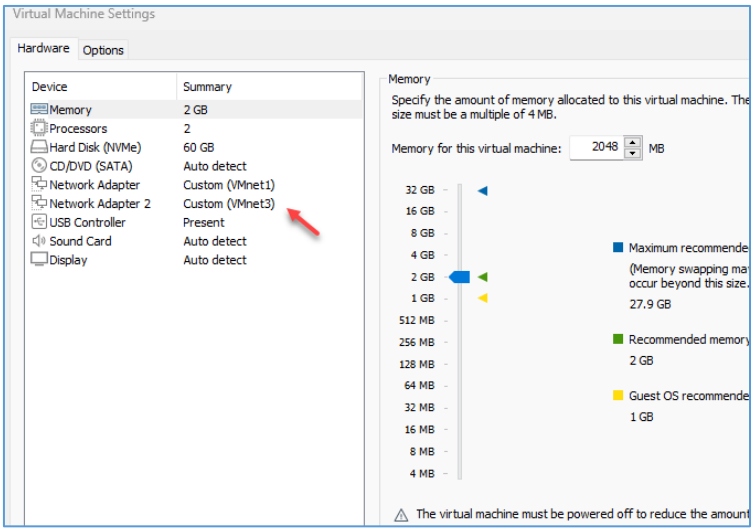
www.takbook.com

برای اینکه تنظیمات آن را بررسی کنیم به مانند شکل ۸-۷۰۱، بر روی ماشین مجازی مورد نظر کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید.



شکل ۸- ۷۰۱ سرویس *Remote Access*

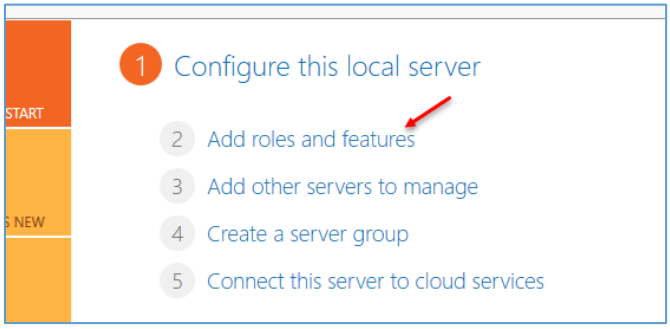
سرور Router باید دارای دو کارت شبکه باشد که در شکل ۸-۷۰۲، دو کارت شبکه را مشاهده می‌کنید، که یکی از کارت شبکه‌ها (VMnet1) با شبکه‌ی داخلی و دیگری (VMnet3) با شبکه‌ی خارجی (اینترنت) ارتباط داشته باشد که در این قسمت نیز کارت شبکه‌ی VMnet3 با شبکه‌ی خارجی (اینترنت) با رنج 192.168.5.0 ارتباط دارد و کارت شبکه‌ی VMnet1 با شبکه‌ی داخلی با رنج 192.168.20.0 ارتباط دارد که کلاینت‌ها نیز برای ارتباط از طریق کانکشن VPN با آدرس سرور 192.168.20.54 که مربوط به سرور Router است، ارتباط برقرار می‌کنند و از این طریق به اینترنت دست پیدا خواهند کرد.



شکل ۸- ۷۰۲ سرویس *Remote Access*

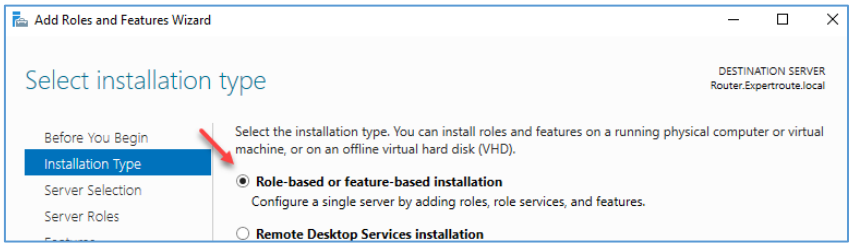
www.takbook.com

برای شروع کار به مانند شکل ۸-۷۰۳، وارد Server Manager مربوط به سرور Router یا همان، VPN شوید و بر روی Add roles and features کلیک کنید.



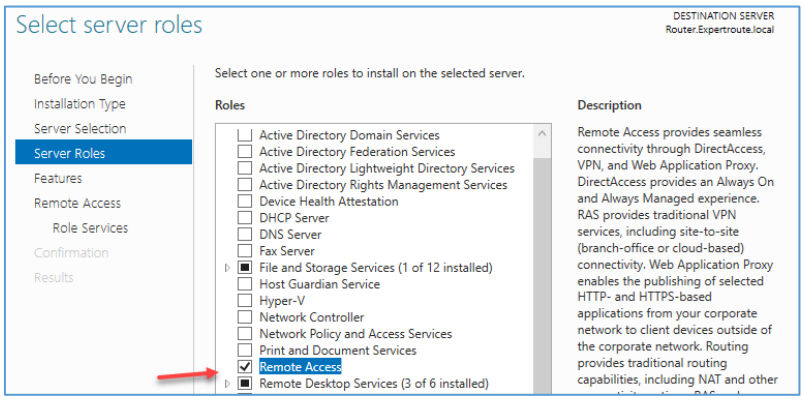
شکل ۸- ۷۰۳ سرویس *Remote Access*

گزینه‌ی اوّل را به مانند شکل ۸-۷۰۴، انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۷۰۴ سرویس *Remote Access*

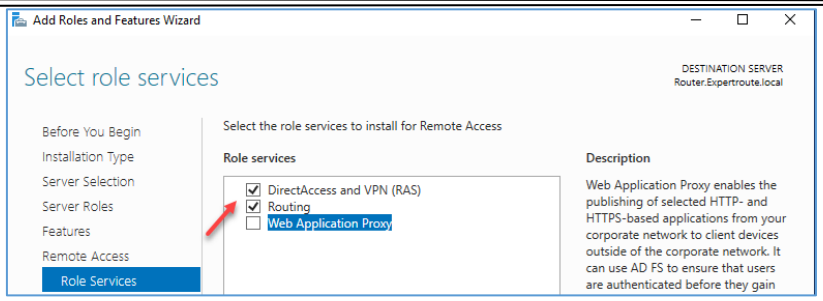
در شکل ۸-۷۰۵، گزینه‌ی Remote Access را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۷۰۵ سرویس *Remote Access*

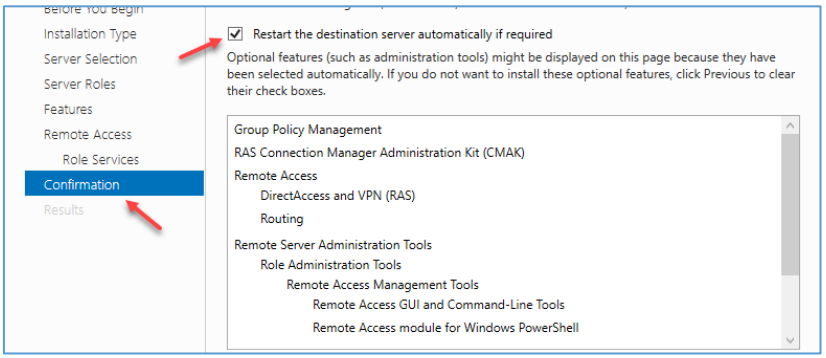
در شکل ۸-۷۰۶، دو گزینه‌ی DirectAccess and VPN (RAS) و Routing را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



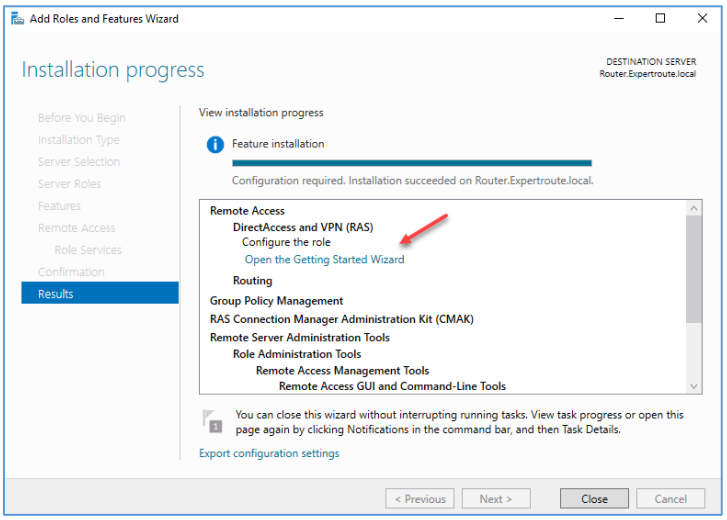
شکل ۸- ۷۰۶ سرویس *Remote Access*

در شکل ۸–۷۰۷، تیک گزینه‌ی Restart را انتخاب و بر روی Install کلیک کنید.



شکل ۸- ۷۰۷ سرویس *Remote Access*

در شکل ۸–۷۰۸، بعد از نصب، بر روی Open the Getting started Wizard کلیک کنید.



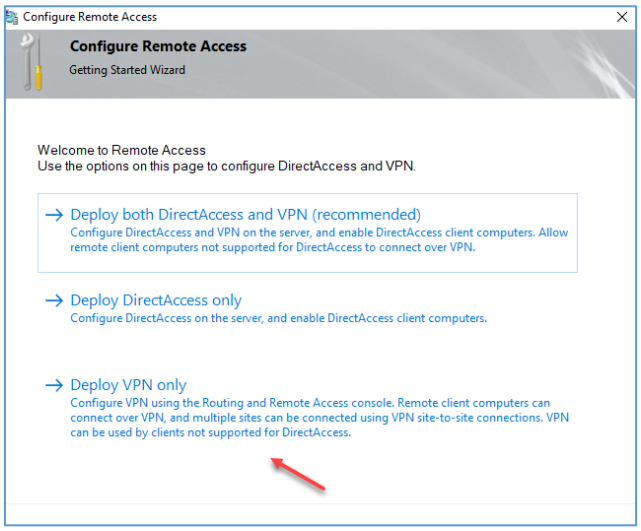
شکل ۸- ۷۰۸ سرویس *Remote Access*

www.takbook.com

در شکل ۸-۷۰۹، سه گزینه را مشاهده می‌کنید که برای شروع باید گزینه‌ی Deploy VPN only را انتخاب کنید.

۸-۳-۲۰-۱ فعال‌سازی سرویس PPTP

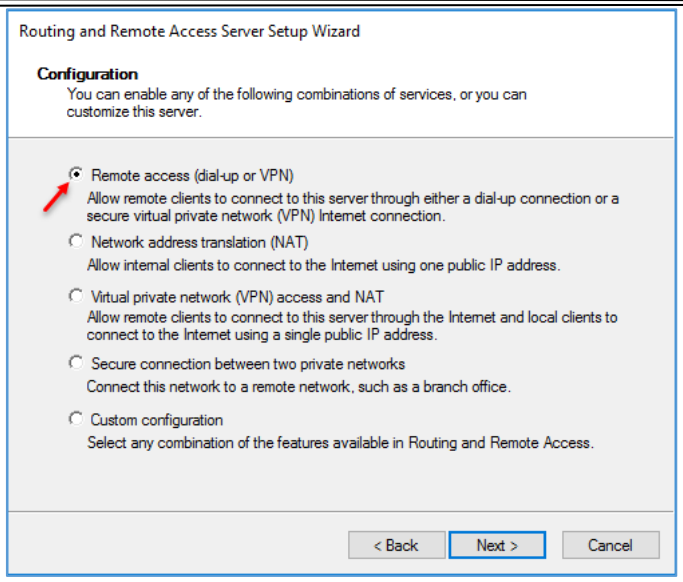
سرویس PPTP که مخفف Point-to-Point Tunneling Protocol است، یکی از پروتکل‌های قدیمی برای ایجاد شبکه‌های خصوصی مجازی (VPN) به شمار می‌رود. این پروتکل به کاربران امکان می‌دهد که از طریق اینترنت به شبکه‌های خصوصی، به صورت ایمن و رمزگذاری شده، متصل شوند.



شکل ۸- ۷۰۹ سرویس Remote Access

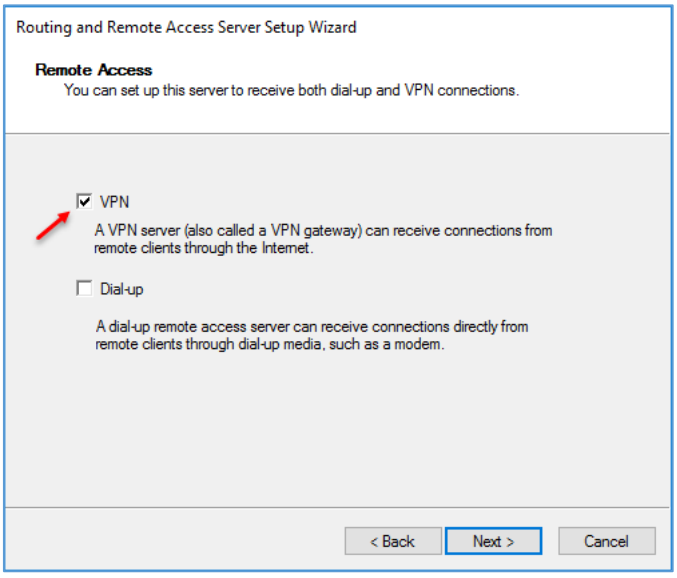
در شکل ۸-۷۱۰، گزینه‌ی Remote Access را انتخاب کنید تا بتوانید VPN را بر روی این سرور راه‌اندازی کنید.

www.takbook.com



شکل ۸- ۷۱۰ سرویس *Remote Access*

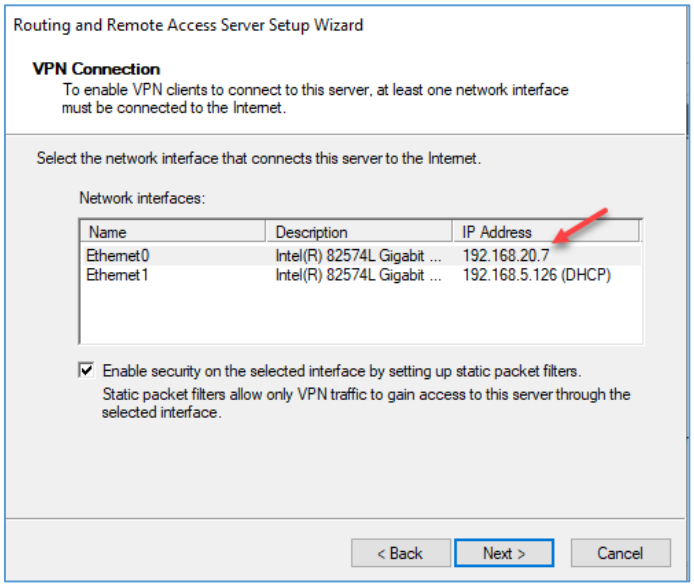
در شکل ۸-۷۱۱، تیک گزینه‌ی VPN را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۷۱۱ سرویس *Remote Access*

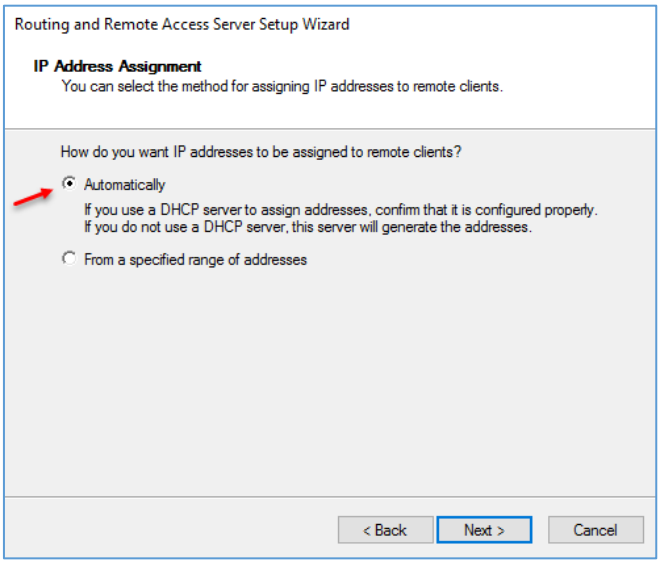
در شکل ۸-۷۱۲، دو کارت شبکه را مشاهده می‌کنید که برای ارتباط کاربران باید کارت شبکه‌ای را انتخاب کنید که داخلی باشد و آدرس شبکه‌ی داخلی بر روی آن تعریف شده باشد.

www.takbook.com



شکل ۸-۷۱۲ سرویس *Remote Access*

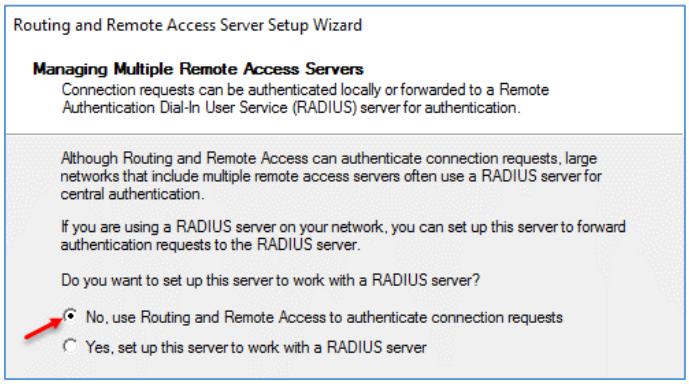
در شکل ۸-۷۱۳، می‌توانید برای کاربرانی که از طریق VPN به سرور متّصل می‌شوند با انتخاب گزینه‌ی From a specified...، یک رنج IP خاص به آنها اختصاص دهید یا گزینه‌ی Automatically را انتخاب کنید تا از طریق سرویس DHCP به آنها IP داده شود.



شکل ۸-۷۱۳ سرویس *Remote Access*

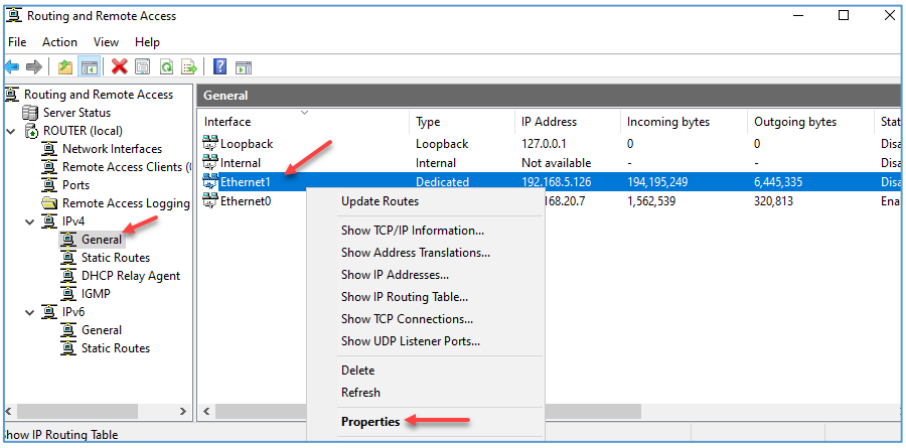
www.takbook.com

به مانند شکل ۸–۷۱٤، اگر 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.



شکل ۸- ۷۱۴ سرویس *Remote Access*

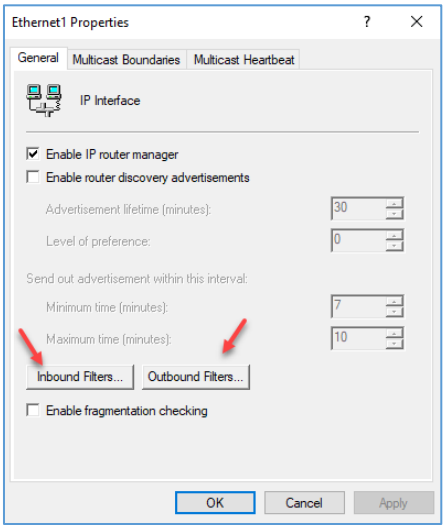
بعد از فعّال کردن سرویس، برای اینکه به درخواست‌های ورودی و خروجی اجازه عبور دهید باید به مانند شکل ۸–۷۱۵، بر حسب IP، آدرس شبکه‌ی خود را وارد کنید و به قسمت General بروید و بر روی کارت شبکه‌ای که به اینترنت متّصل است که در اینجا، Ethernet1 است، کلیک راست و گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۷۱۵ سرویس *Remote Access*

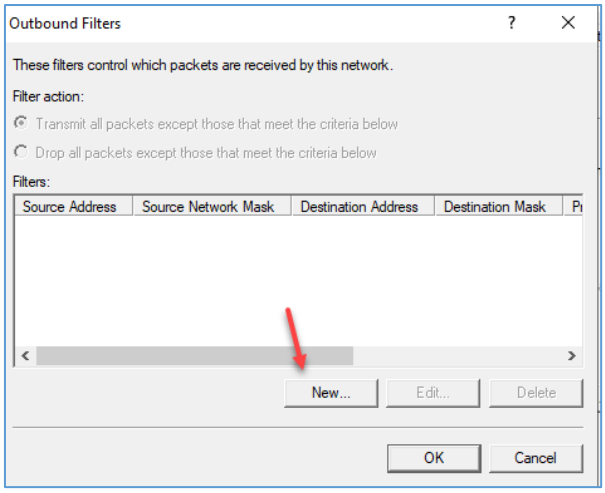
در شکل ۸–۷۱٦، دو گزینه‌ی Inboound Filters وOutbound Filters را مشاهده می‌کنید، برای اینکه همین سرور به اینترنت دسترسی داشته باشد باید بر روی گزینه‌ی Outbound Filters کلیک کنید.

www.takbook.com



شکل ۸- ۷۱۶ سرویس *Remote Access*

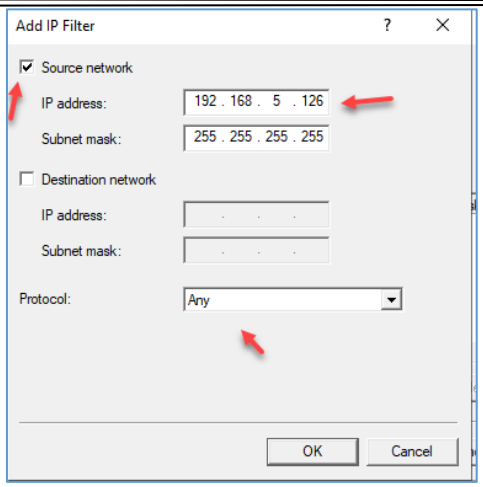
در شکل ۸-۷۱۷، برای اینکه اجازه‌ی عبور به ترافیک دهید، باید آدرس سرور را وارد کنید، برای این کار بر روی New کلیک کنید.



شکل ۸- ۷۱۷ سرویس *Remote Access*

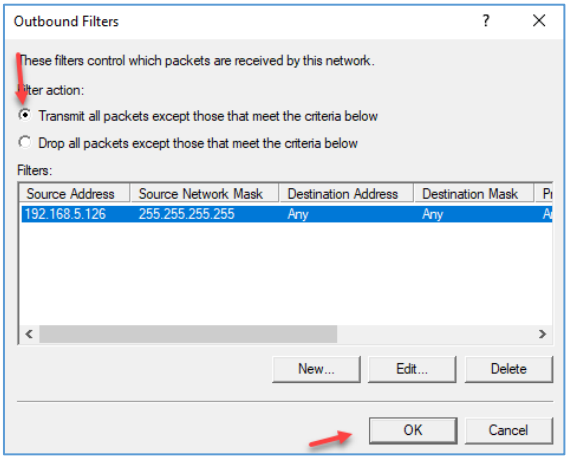
در شکل ۸-۷۱۸، آدرس سرور مورد نظر را وارد و در قسمت Protocol گزینه‌ی Any را انتخاب کنید.

www.takbook.com



شکل ۸- ۷۱۸ سرویس *Remote Access*

بعد از اضافه کردن آدرس مورد نظر باید به مانند شکل ۸-۷۱۹، 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 192.168.5.126 دارا خواهد بود.

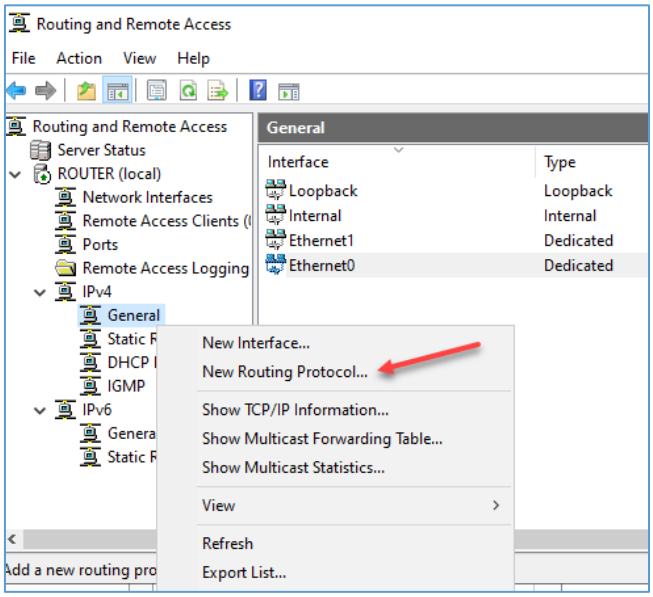


شکل ۸- ۷۱۹ سرویس *Remote Access*

بعد از این که سرور Router 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.

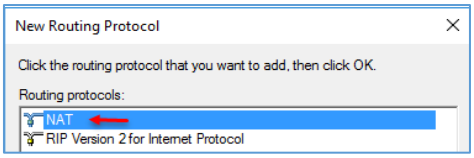
برای انجام این کار به مانند شکل ۸-۷۲۰، بر روی General کلیک راست کنید و گزینه‌ی New routing Protocol را انتخاب کنید، البتّه بستگی به این دارد که پروتکل شبکه‌ی شما، IPv4 یا IPv6 باشد.

www.takbook.com



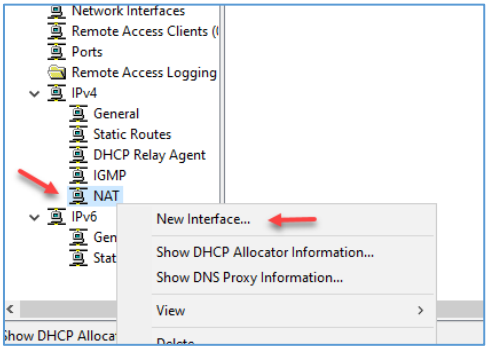
شکل ۸- ۷۲۰ سرویس *Remote Access*

در شکل ۸-۷۲۱، پروتکل NAT را انتخاب کنید تا آدرس‌های شبکه‌ی داخلی به آدرس‌های قابل فهم در شبکه‌ی اینترنت تبدیل شود.



شکل ۸- ۷۲۱ سرویس *Remote Access*

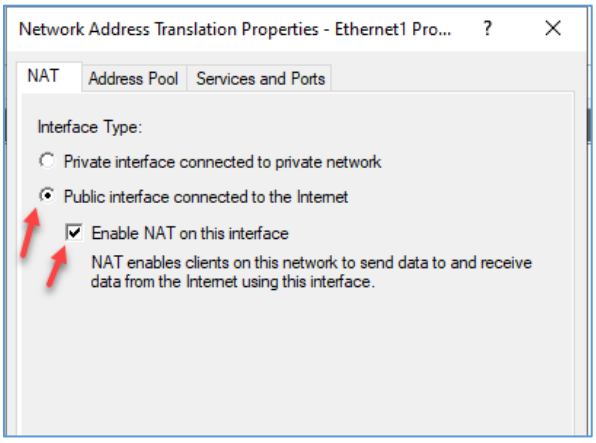
در شکل ۸-۷۲۲، گزینه‌ی NAT به لیست اضافه شده است، بر روی آن کلیک راست کنید و گزینه‌ی New Interface را انتخاب کنید.



شکل ۸- ۷۲۲ سرویس *Remote Access*

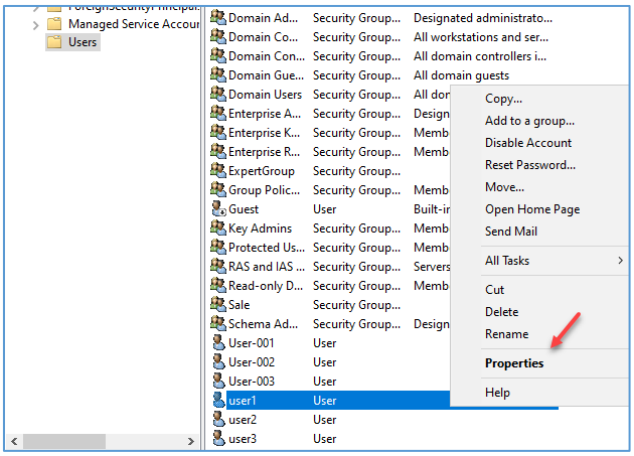
www.takbook.com

در شکل ۸–۷۲۳، 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.



شکل ۸- ۷۲۳ سرویس *Remote Access*

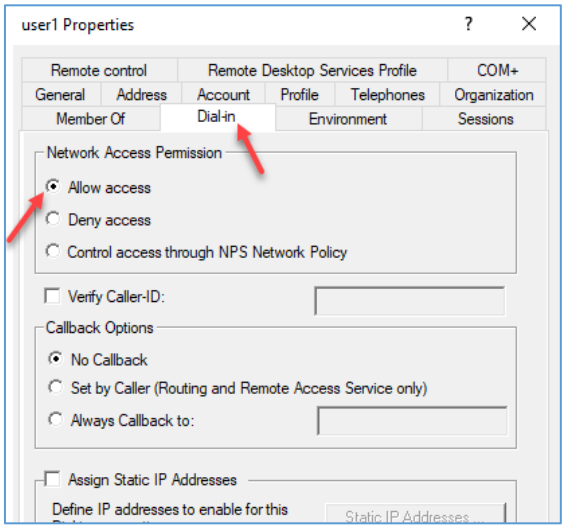
بعد از اینکه سرویس را آماده کردید باید به کاربران خود در شبکه دسترسی دهید تا بتوانند به سرور Router، یک کانکشن VPN بزنند، برای این کار به مانند شکل ۸–۷۲٤، وارد Active Directory Users and Computers شوید و بر روی نام کاربر خود کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۷۲۴ سرویس *Remote Access*

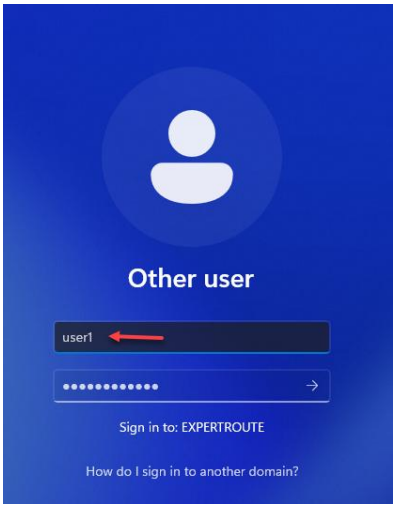
در شکل ۸–۷۲۵، وارد تب Dial-in شوید و تیک گزینه‌ی Allow Access را انتخاب و بر روی OK کلیک کنید.

www.takbook.com



شکل ۸- ۷۲۵ سرویس *Remote Access*

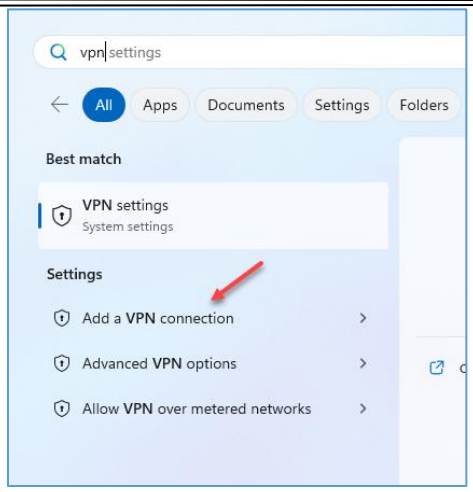
برای تست موضوع به مانند شکل ۸-۷۲۶، با کاربر User1 وارد یکی از کلاینت‌های شبکه که ویندوز 11 نیز بر روی آن نصب شده است می‌شویم.



شکل ۸- ۷۲۶ سرویس *Remote Access*

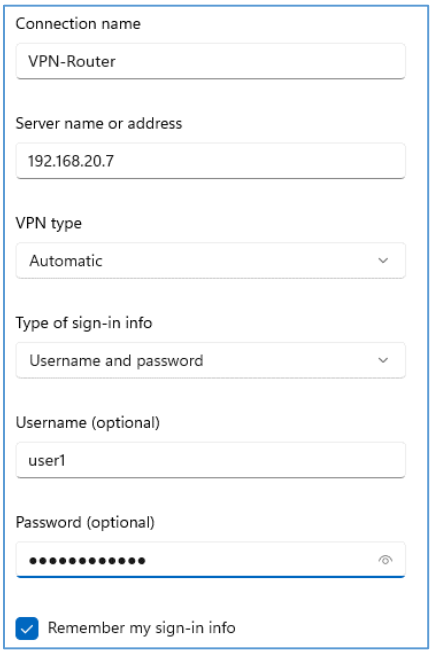
در ادامه کار به مانند شکل ۸-۷۲۷، وارد جستجو شوید و کلمه‌ی VPN را وارد کنید و در گزینه‌های مورد نظر بر روی Add a VPN کلیک کنید.

www.takbook.com



شکل ۸- ۷۲۷ سرویس *Remote Access*

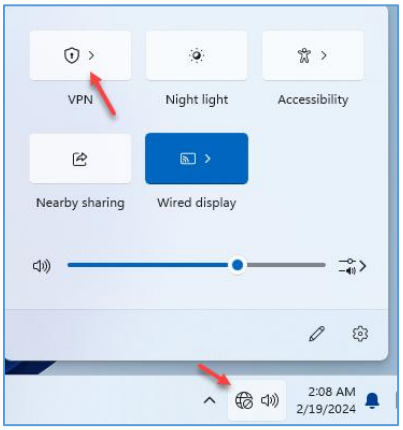
در شکل ۸–۷۲۸، نام VPN خود را به دلخواه وارد کنید و در قسمت Server name or address باید آدرس سرور VPN که در قسمت قبل مشخص کردیم را وارد کنید و نوع ارتباط را بر روی Automatic قرار دهید، البته می‌توانید ارتباط PPTP را انتخاب کنید.



شکل ۸- ۷۲۸ سرویس *Remote Access*

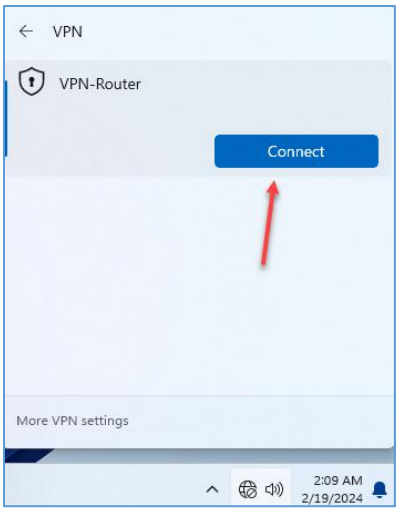
بعد از ایجاد کانکشن به مانند شکل ۸–۷۲۹، بر روی کارت شبکه کلیک کنید و وارد قسمت VPN شوید.

www.takbook.com



شکل ۸- ۷۲۹ سرویس *Remote Access*

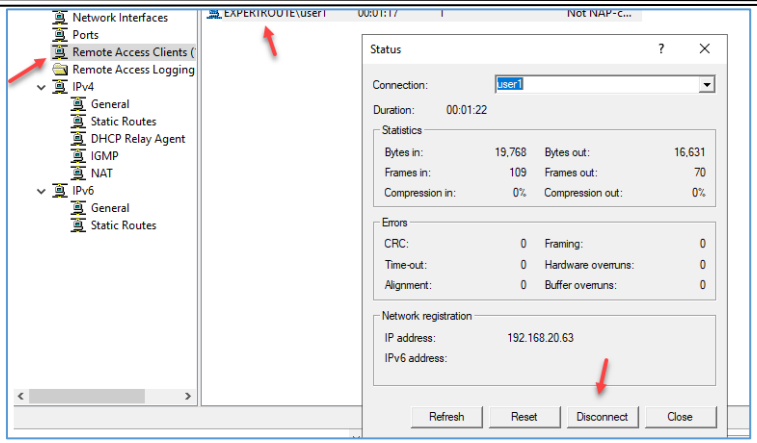
همان‌طور که در شکل ۸-۷۳۰، مشاهده می‌کنید کانکشن مورد نظر ایجاد و می‌توانید بر روی Connect کلیک کنید تا ارتباط VPN وصل شود.



شکل ۸- ۷۳۰ سرویس *Remote Access*

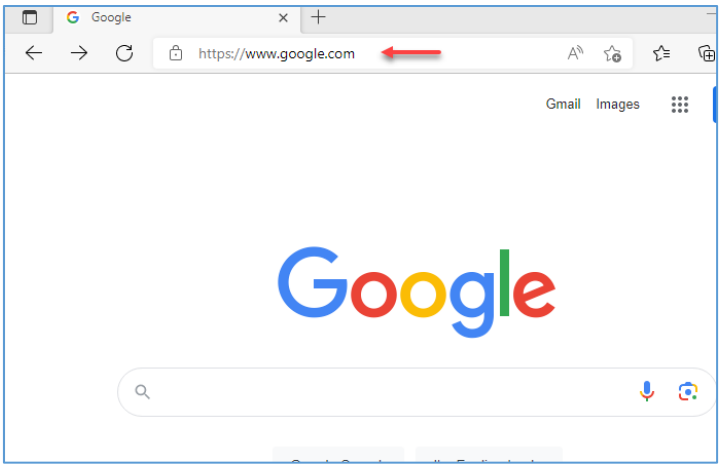
بعد از ارتباط، اگر وارد سرویس Routing شوید و بر روی Remote Access Client کلیک کنید، مشاهده می‌کنید که یک کاربر به لیست اضافه شده است و زمان ارتباط آن را مشاهده می‌کنید، برای اینکه وضعیّت آن را بهتر مشاهده کنید باید بر روی آن کلیک راست کنید و گزینه‌ی Status را انتخاب کنید که شکل ۸-۷۳۱ را مشاهده می‌کنید و اگر بخواهید آن را قطع کنید باید گزینه‌ی Disconnect را انتخاب کنید.

www.takbook.com



شکل ۸- ۷۳۱ سرویس *Remote Access*

حالا اگر وارد کلاینت شویم و یک صفحه‌ی وب را باز کنید متوجه خواهید شد که این کار به درستی انجام شده است که این موضوع را در شکل ۸-۷۳۲، مشاهده می‌کنید.



شکل ۸- ۷۳۲ سرویس *Remote Access*

نکته مهم: اگر چنانچه صفحات سایت برای شما باز نشد باید به DNS خود رجوع کنید، یعنی زمانی که با VPN از طریق کلاینت به سرور متصل می‌شوید باید دستور ipconfig /all را در CMD به صورت زیر شکل ۸-۷۳۳، وارد کنید، بعد از اجرا، اطلاعاتی از کانکشن مورد نظر را به مشا نشان می‌دهد، که در خروجی زیر مشخص است که DNS فقط شبکه‌ی داخلی است و خبری از DNS خارجی مانند 8.8.8.8 و ... نیست.

www.takbook.com

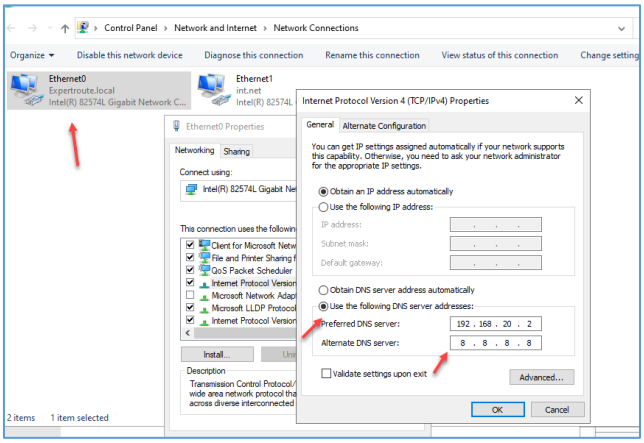

```
PPP adapter VPN-Router:

   Connection-specific DNS Suffix  . : Expertroute.local
   Description . . . . . . . . . . . : VPN-Router
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.20.59(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
   DNS Servers . . . . . . . . . . . : 192.168.20.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\user1>
```

شکل ۸- ۷۳۳ سرویس *Remote Access*

برای حل این مشکل باید به مانند شکل ۸-۷۳٤، وارد سرور Router شوید و یک DNS خارجی هم برای آن ست کنید تا کلاینتها بتوانند صفحات وب را ببینند.



شکل ۸- ۷۳۴ سرویس *Remote Access*

بعد از ست کردن آدرس DNS اگر دوباره دستور ipconfig /all را به مانند شکل ۸-۷۳۵، اجرا کنید DNS مورد نظر را مشاهده خواهید کرد.

```
PPP adapter VPN-Router:

   Connection-specific DNS Suffix  . : Expertroute.local
   Description . . . . . . . . . . . : VPN-Router
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.20.58(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
   DNS Servers . . . . . . . . . . . : 192.168.20.2
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

شکل ۸- ۷۳۵ سرویس *Remote Access*

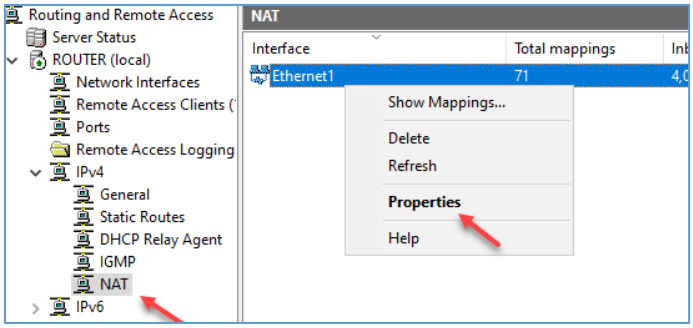
www.takbook.com

تا با اینجا سرویس Remote access را نصب و از طریق کلاینت به آن متصل شدیم و کلاینت هم دارای اینترنت شد، اما مشکل بزرگی که وجود دارد این است که پروتکلی که با آن به سرویس Remote Access متصل شدید PPTP بود و همان‌طور که می‌دانید پروتکل PPTP امنیت ندارد و برای اینکه این مشکل را حل کنیم باید از پروتکل‌های قویتر استفاده کنیم.

در ادامه می‌خواهیم پروتکل L2TP را که مخفف کلمه‌ی Layer 2 Tunneling Protocol استفاده کنیم، این پروتکل علاوه بر استفاده از نام کاربری و رمز عبور، از یک کلید اشتراکی استفاده می‌کند که باید در کلاینت و سرور یکی باشد.

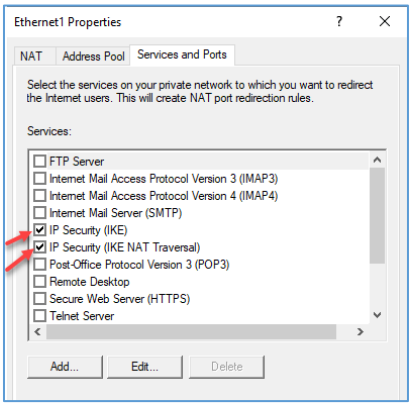
۸-۳-۲۰-۲ فعال‌سازی سرویس L2TP

برای انجام این کار به مانند شکل ۸-۷۳۶، وارد سرویس Remote Access شوید و از قسمت NAT بر روی کارت شبکه‌ای که به سمت اینترنت است کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۷۳۶ فعال‌سازی سرویس L2TP

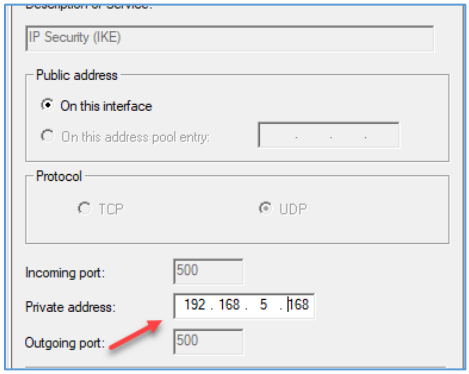
در شکل ۸-۷۳۷، وارد تب Services and Ports شوید و تیک دو گزینه‌ی مورد نظر را انتخاب کنید، زمانی که تیک مورد نظر را کلیک می‌کنید صفحه بعدی باز می‌شود.



شکل ۸- ۷۳۷ فعال‌سازی سرویس L2TP

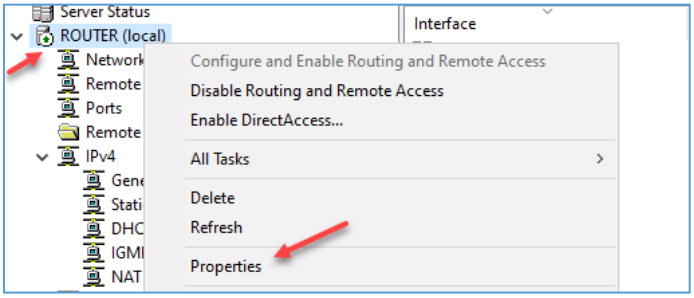
www.takbook.com

در شکل ۸-۷۳۸، باید در قسمت Private Address باید آدرس IP مربوط به کارت شبکه‌ی اینترنت را وارد کنید.



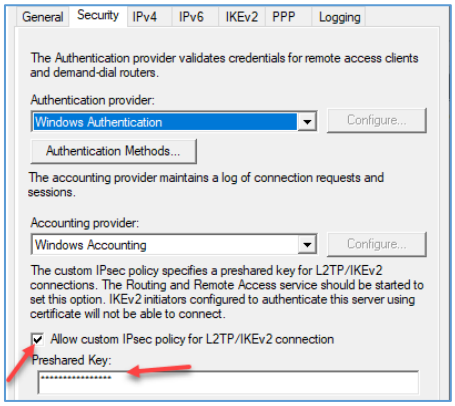
شکل ۸- ۷۳۸ فعال‌سازی سرویس L2TP

در ادامه به مانند شکل ۸-۷۳۹، بر روی نام سرور کلیک راست کنید و Properties را انتخاب کنید.



شکل ۸- ۷۳۹ فعال‌سازی سرویس L2TP

در شکل ۸-۷۴۰، تیک گزینه‌ی Allow custom certificate... را انتخاب کنید و باید یک رمز عبور مناسب برای کلید اشتراکی وارد کنید تا در ادامه از آن استفاده کنیم.



شکل ۸- ۷۴۰ فعال‌سازی سرویس L2TP

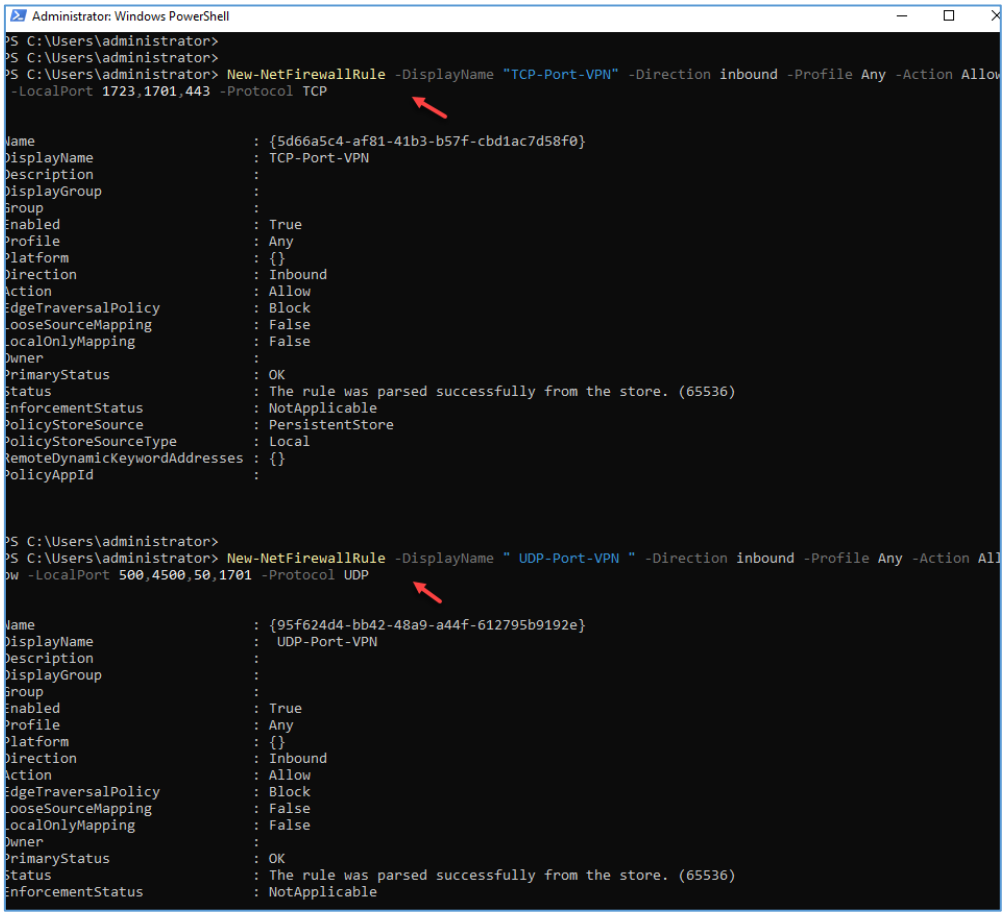
www.takbook.com

اگر در سرور خود از Firewall ویندوز استفاده می‌کنید باید به پورت‌های L2TP دسترسی دهید، برای انجام این کار به مانند شکل ۸–۷٤۱، از دستورات PowerShell استفاده می‌کنیم:

```
New-NetFirewallRule -DisplayName "TCP-Port-VPN" -Direction inbound -Profile Any -Action Allow -LocalPort 1723,1701,443 -Protocol TCP

New-NetFirewallRule -DisplayName " UDP-Port-VPN " -Direction inbound -Profile Any -Action Allow -LocalPort 500,4500,50,1701 -Protocol UDP

New-NetFirewallRule -DisplayName "GRE-Port" -Direction inbound -Protocol 47 -Profile Any -Action Allow
```



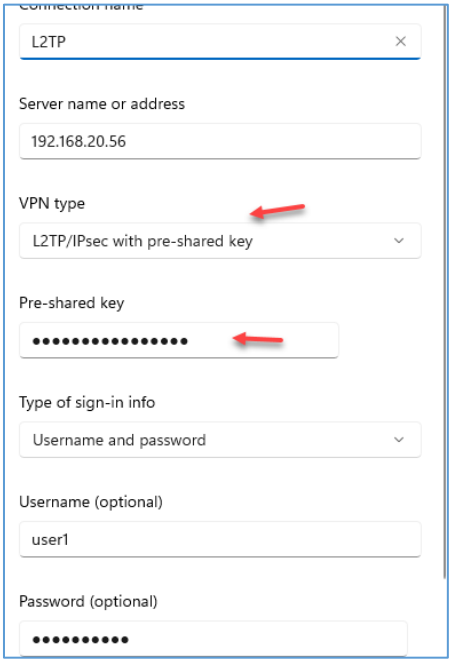
شکل ۸– ۷۴۱ فعال‌سازی سرویس L2TP

بعد از این کار حتماً سرور را Restart کنید.

در ادامه وارد کلاینت مورد نظر شوید و به مانند قبل یک VPN جدید ایجاد کنید و به مانند شکل ۸–۷٤۲، نام آن را مشخص کنید، در قسمت VPN Type باید نوع L2TP/IPSec with pre-shared key را انتخاب کنید و

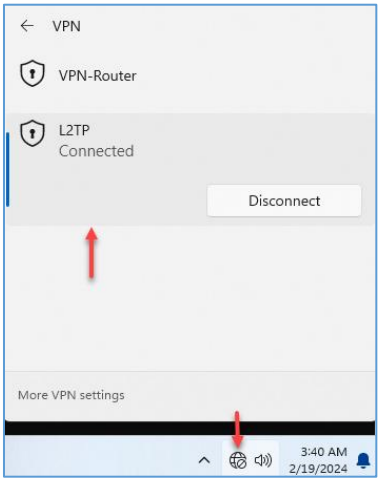
www.takbook.com

بعد از آن باید در قسمت Pre-shared Key رمز عبور اشتراکی را وارد کنید و در آخر هم نام کاربری و رمز عبور کاربری که در قسمت‌های قبلی VPN آن را فعال کردیم را وارد و OK کنید.



شکل ۸- ۷۴۲ فعال‌سازی سرویس L2TP

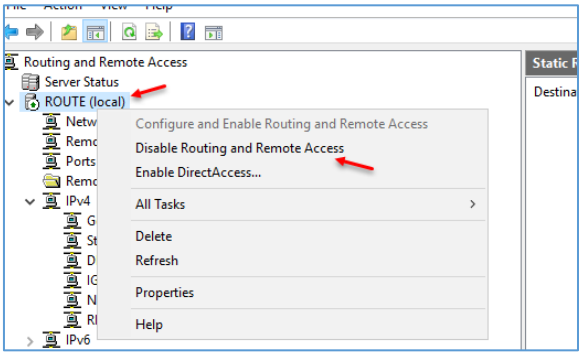
همان‌طور که در شکل ۸-۷۴۳، مشاهده می‌کنید پروتکل L2TP با موفقیت متصل شده است.



شکل ۸- ۷۴۳ فعال‌سازی سرویس L2TP

www.takbook.com

برای غیر فعال کردن تنظیمات انجام داده شده در سرویس Routing and Remote access باید به مانند شکل ۸-۷٤٤، بر روی نام سرور کلیک راست کنید و گزینه‌ی Disable Routing and Remote Access را انتخاب کنید.



شکل ۸- ۷۴۴ فعال‌سازی سرویس L2TP

۸-۳-۲۱ سرویس Active Directory Certificate

Active Directory Certificate Services (AD CS) یکی از سرویس‌های موجود در Windows Server است که به سازمان‌ها امکان مدیریت و پیاده‌سازی زیرساخت کلید عمومی (PKI) و صدور گواهی‌های دیجیتال را می‌دهد. این سرویس ابزاری برای صدور، مدیریت، و اعتبارسنجی گواهینامه‌های دیجیتال فراهم می‌کند که در تأمین امنیت شبکه‌ها، احراز هویت کاربران، دستگاه‌ها و سرویس‌ها و همچنین رمزنگاری داده‌ها استفاده می‌شود.

کاربردهای اصلی AD CS:

- صدور گواهینامه‌های دیجیتال: AD CS برای صدور گواهینامه‌هایی که برای احراز هویت کاربران، دستگاه‌ها یا سرویس‌ها در شبکه‌های مایکروسافت استفاده می‌شود، طراحی شده است.
- رمزنگاری و احراز هویت: با استفاده از گواهینامه‌ها، داده‌ها می‌توانند رمزنگاری شوند و همچنین هویت کاربران و دستگاه‌ها به صورت امن تأیید شود. این موضوع برای ایجاد اتصال‌های امن (مانند VPN و SSL) حیاتی است.
- مدیریتPKI : AD CS به سازمان‌ها اجازه می‌دهد تا یک زیرساخت کلید عمومی (Public Key Infrastructure - PKI) را راه‌اندازی کنند و به‌طور کامل آن را مدیریت نمایند. این شامل ایجاد و مدیریت Certificate Authorities (CA) (مرجع‌های صدور گواهینامه)، صدور و بازپس‌گیری گواهینامه‌ها، و تنظیم خط‌مشی‌های امنیتی مرتبط با آن‌ها است.

www.takbook.com

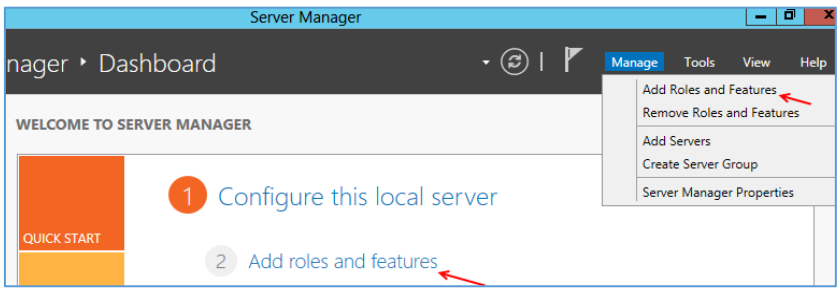
- امضای دیجیتال و رمزنگاری ایمیل: AD CS امکان صدور گواهینامه‌هایی را فراهم می‌کند که برای امضای دیجیتال ایمیل‌ها و اسناد، رمزنگاری ارتباطات و داده‌ها به کار می‌روند.

اجزای اصلی AD CS:

- Certificate Authority (CA): قلب AD CS است و مسئول صدور، مدیریت و اعتبارسنجی گواهینامه‌های دیجیتال است. CA می‌تواند Root CA یا Subordinate CA باشد. Root CA یک CA اصلی است که بالاترین سطح اعتماد را در یک PKI دارد.
- Certificate Enrollment: فرایند درخواست و دریافت گواهینامه‌های دیجیتال توسط کاربران، دستگاه‌ها یا سرویس‌ها.
- Certificate Revocation List (CRL): لیستی از گواهینامه‌هایی که قبل از انقضای آن‌ها لغو شده‌اند. این لیست برای اعتبارسنجی گواهینامه‌ها مورد استفاده قرار می‌گیرد.
- Online Responder: یک سرویس که به صورت بلادرنگ وضعیت گواهینامه‌ها را تأیید می‌کند. این سرویس از پروتکل OCSP (Online Certificate Status Protocol) استفاده می‌کند تا ببیند آیا یک گواهینامه معتبر است یا لغو شده.
- Certificate Templates: قالب‌های پیش‌تعریف شده برای صدور گواهینامه‌های مختلف. این قالب‌ها تعیین می‌کنند که گواهینامه برای چه نوع کاربران، سرویس‌ها یا دستگاه‌هایی صادر می‌شود و چه سطح دسترسی‌ها و کاربردهایی دارد.

به طور مثال شما زمانی که به سایت فیسبوک متصل می‌شوید این گواهینامه برای دسترسی به سایت از طریق پروتکل HTTPS فعال می‌شود، اگر زمان و تاریخ سیستم شما دقیق نباشد با مشکلات امنیتی مواجع می‌شوید و دسترسی به سایت به صورت کامل امکانپذیر نخواهد بود. شاید زمانی برای شما پیش آمده باشد که سایت فیسبوک را باز می‌کنید، همه چیز درهم است و شکل و قالب سایت تغییر کرده است که این به خاطر تنظیم نبودن ساعت و تاریخ سیستم است.

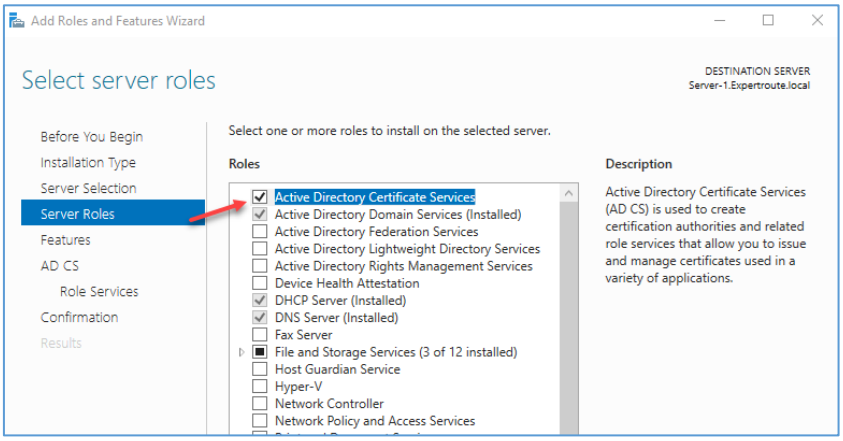
برای نصب این سرویس وارد سرور شوید و به مانند شکل ۸-۷۴۵، از قسمت ServerManager بر روی Add Roles and Features کلیک می‌کنیم.



شکل ۸- ۷۴۵ نصب *Certificate Service*

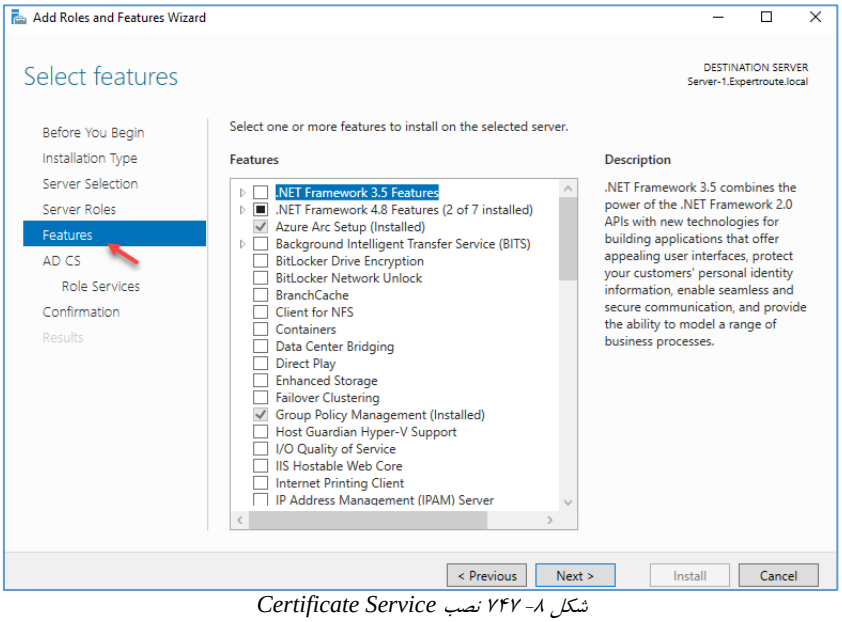
www.takbook.com

بر روی Next کلیک کنید تا به قسمت Server Roles برسید، در این قسمت به مانند شکل ۸–۷٤٦، از میان Roleهای موجود گزینه Active Directory Certificate Service را انتخاب و بر روی Add Features کلیک کنید و بعد بر روی Next کلیک کنید.



شکل ۸- ۷۴۶ نصب *Certificate Service*

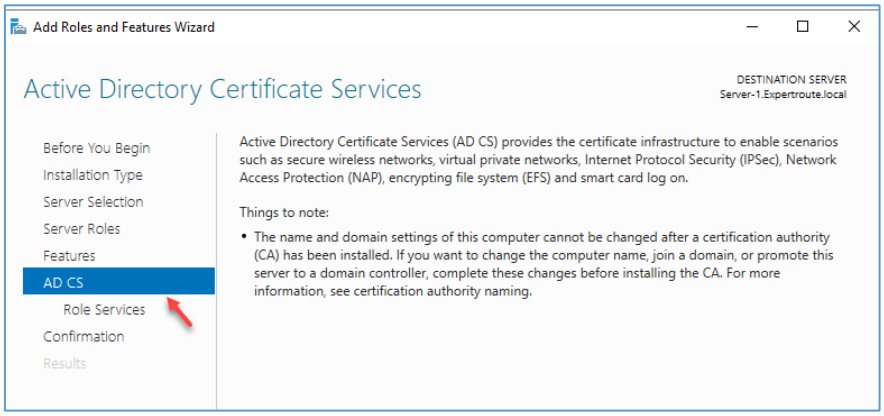
در شکل ۸–۷٤۷، به گزینه‌ای دست نزنید و بر روی Next کلیک کنید.



شکل ۸- ۷۴۷ نصب *Certificate Service*

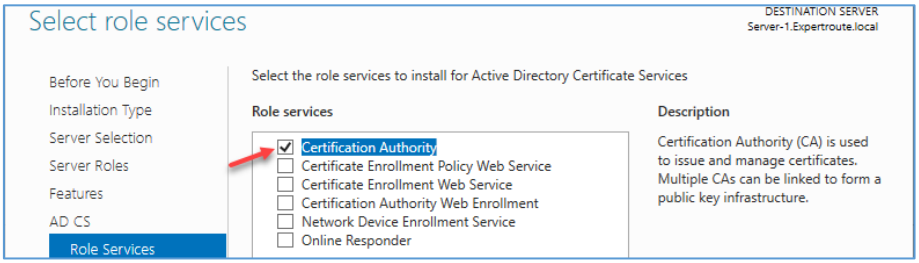
در شکل ۸–۷٤۸، توضیحاتی در مورد سرویس انتخاب شده است که بعد از مطالعه بر روی Next کلیک کنید.

www.takbook.com



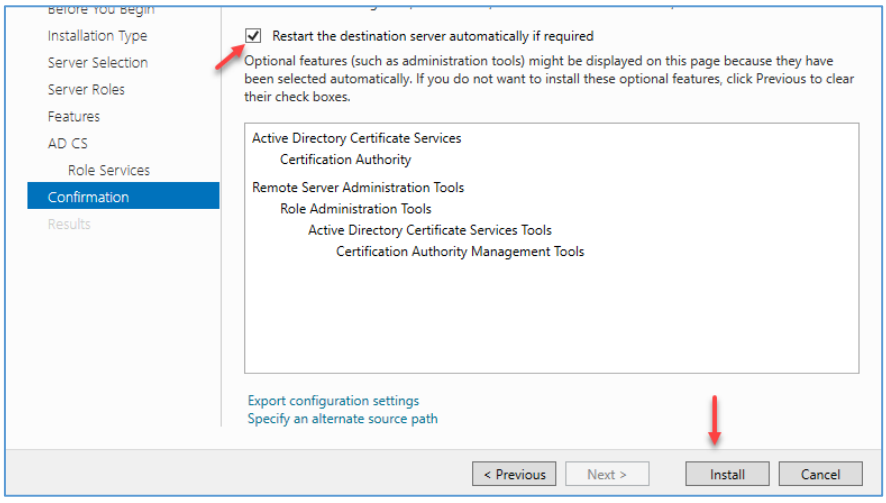
شکل ۸- ۷۴۸ نصب *Certificate Service*

در شکل ۸-۷۴۹، گزینه Certification Authority را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۷۴۹ نصب *Certificate Service*

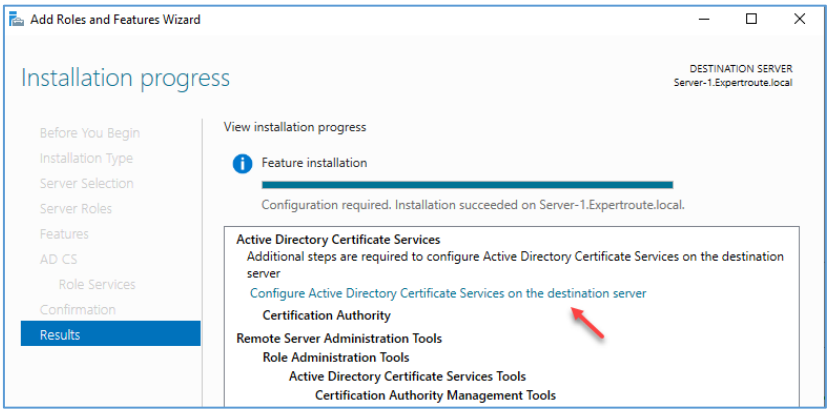
برای نصب سرویس در شکل ۸-۷۵۰، بر روی install کلیک کنید.



شکل ۸- ۷۵۰ نصب *Certificate Service*

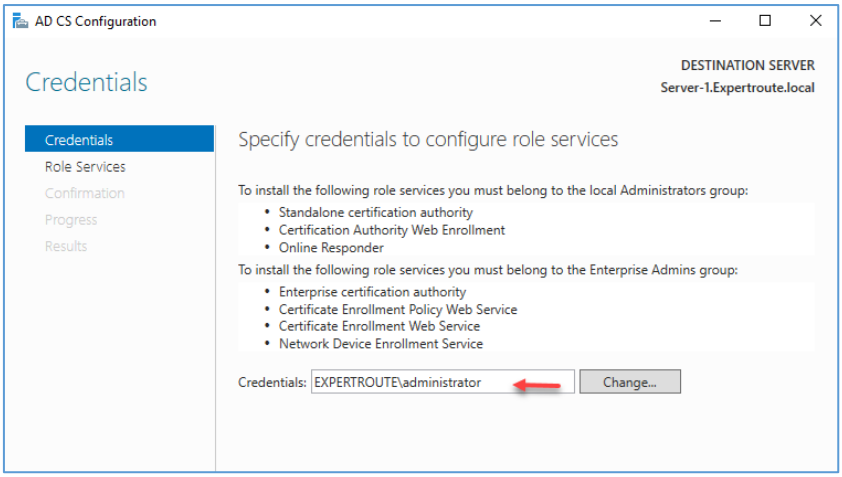
www.takbook.com

در شکل ۸–۷۵۱، بعد از نصب سرویس باید بر روی Configuration Active… کلیک کنید تا سرویس را تنظیم و فعال کنیم.



شکل ۸- ۷۵۱ نصب *Certificate Service*

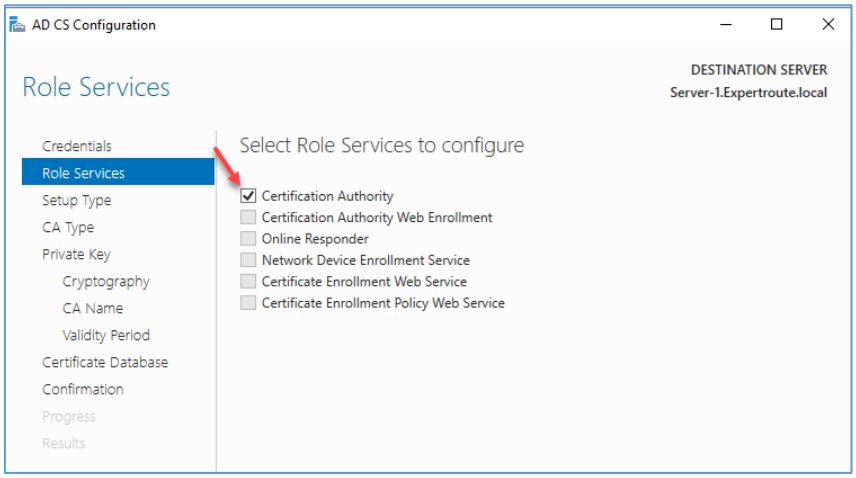
در شکل ۸–۷۵۲، در قسمت Credentials باید یک کاربر با اولویت بالا که معمولاً Administrator است را وارد کنید. البته به طور پیش فرض این کاربر تعریف می‌شود، بر روی Next کلیک کنید.



شکل ۸- ۷۵۲ نصب *Certificate Service*

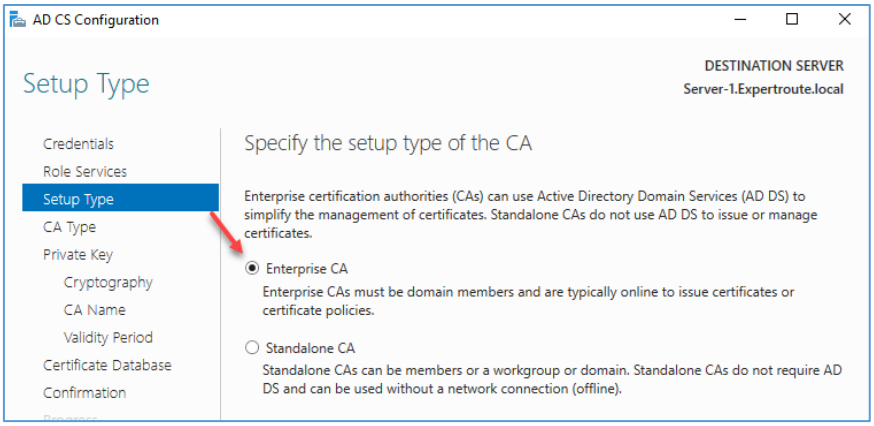
در شکل ۸–۷۵۳، گزینه Certification Authority را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



شکل ۸- ۷۵۳ نصب *Certificate Service*

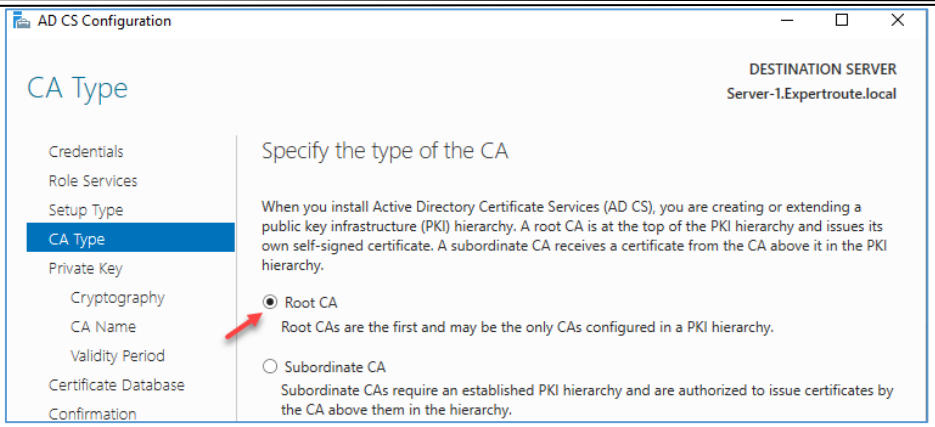
در شکل ۸–۷۵٤، گزینه Enterprise CA را انتخاب کنید، توجه داشته باشید زمانی این گزینه فعال می‌شود که سرویس Active Directory Domain فعال شده باشد، وگرنه باید گزینه Standalone CA را انتخاب کنید.



شکل ۸- ۷۵۴ نصب *Certificate Service*

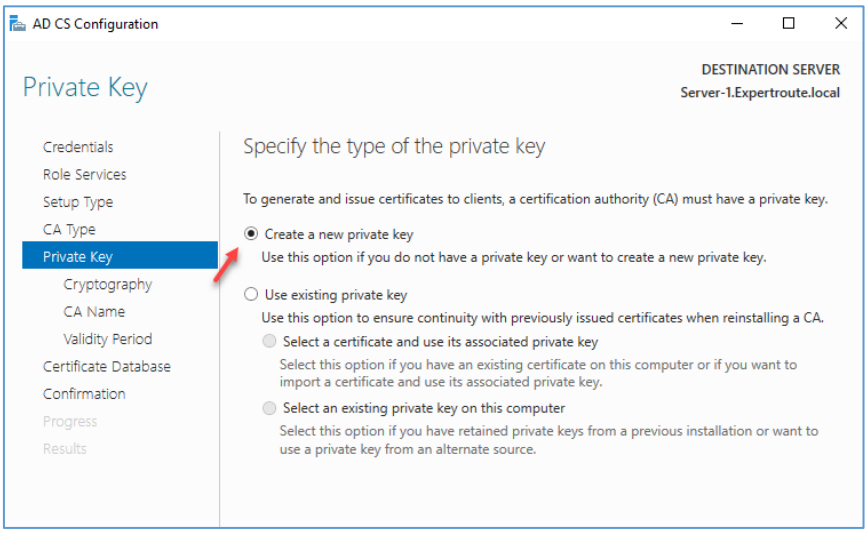
در شکل ۸–۷۵۵، گزینه Root CA را انتخاب کنید چون این سرور زیر مجموعه سرور دیگری یا سرویس Certificate دیگری نیست و برای اولین بار این سرویس نصب می‌شود به خاطر همین باید به عنوان Root در نظر گرفته شود. بر روی Next کلیک کنید.

www.takbook.com



شکل ۸- ۷۵۵ نصب *Certificate Service*

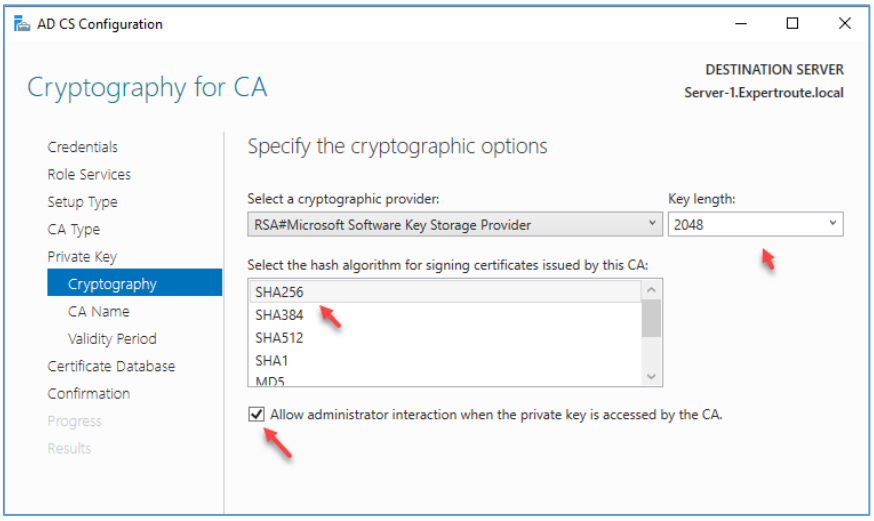
در شکل ۸–۷۵۶، باید یک دسته کلید ایجاد کنیم، اگر برای اولین بار است باید گزینه اول را انتخاب کنید و یا اگر از قبل ایجاد کرده‌اید گزینه دوم را انتخاب کنید.



شکل ۸- ۷۵۶ نصب *Certificate Service*

در شکل ۸–۷۵۷، باید الگوریتم رمزنگاری را برای این سرویس انتخاب کنید، توجه داشته باشید که الگوریتم SHA256 بهترین انتخاب می‌باشد و به صورت پیش‌فرض انتخاب شده است و طول کلید هم ۲۰۴۸ انتخاب شده است که انتخاب خوبی است، بر روی Next کلیک کنید.

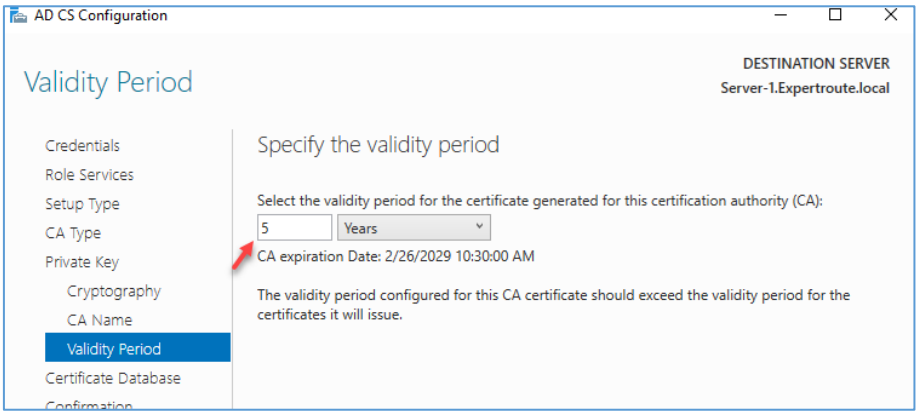
www.takbook.com



شکل ۸- ۷۵۷ نصب *Certificate Service*

در شکل ۸-۷۵۸، سعی کنید نوشته قسمت Common name for this CA را به خاطر داشته باشید، شاید در آینده به کار شما بیاید.

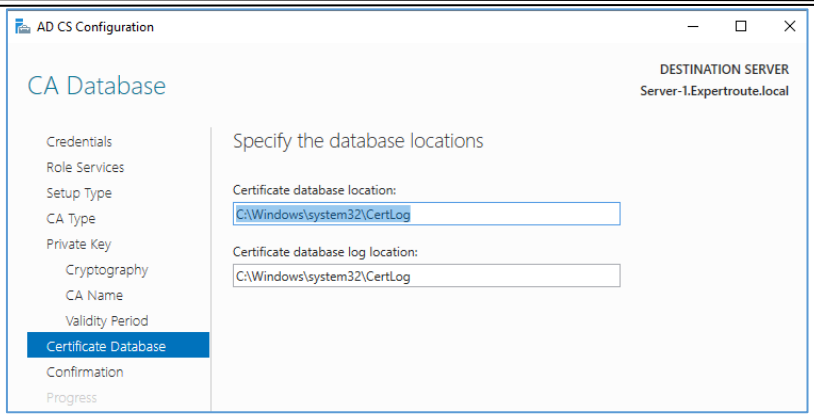
در این قسمت، باید مدت اعتبار گواهینامه خود را وارد کنید که می‌تواند بر طبق روز، هفته، ماه، سال باشد که در این قسمت ۵ سال وارد شده است.



شکل ۸- ۷۵۸ نصب *Certificate Service*

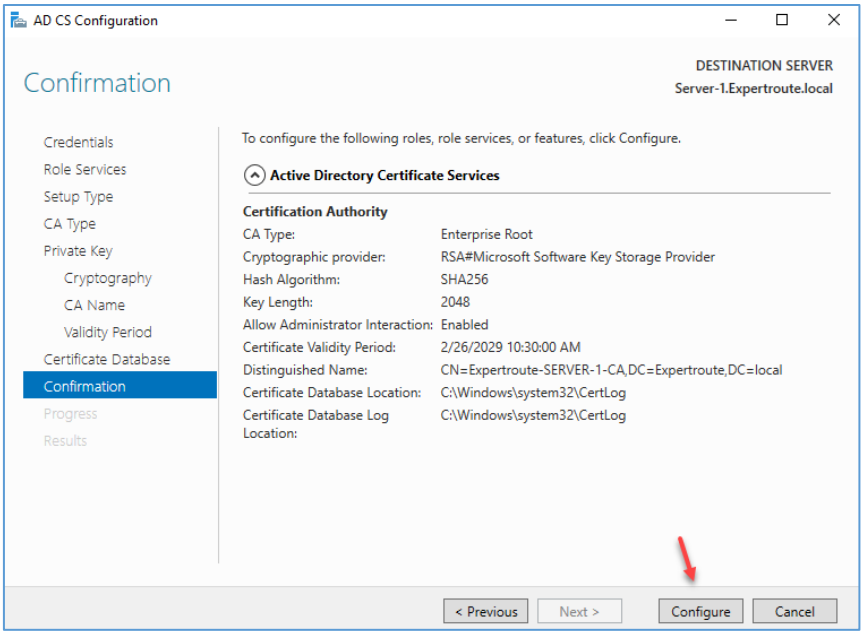
در شکل ۸-۷۵۹، باید محل ذخیره‌سازی دیتابیس این سرویس را وارد کنید که سعی کنید بر روی پیش فرض قرار دهید.

www.takbook.com



شکل ۸- ۷۵۹ نصب *Certificate Service*

در شکل ۸-۷٦۰، اگر اطلاعات لیست شده را قبول دارید بر روی configure کلیک کنید تا تنظیمات اعمال شود.

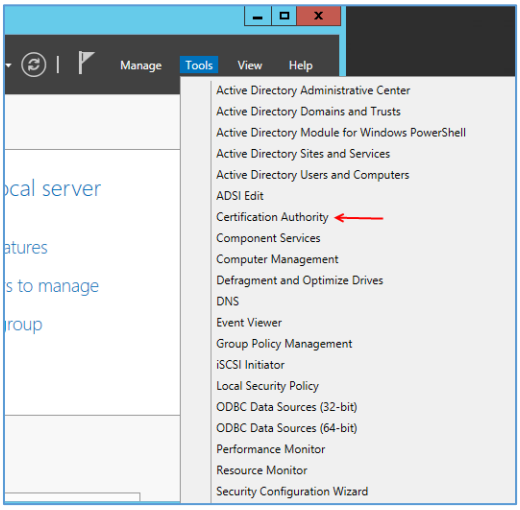


شکل ۸- ۷۶۰ نصب *Certificate Service*

در آخر بر روی Close کلیک کنید و سیستم را Restart کنید.

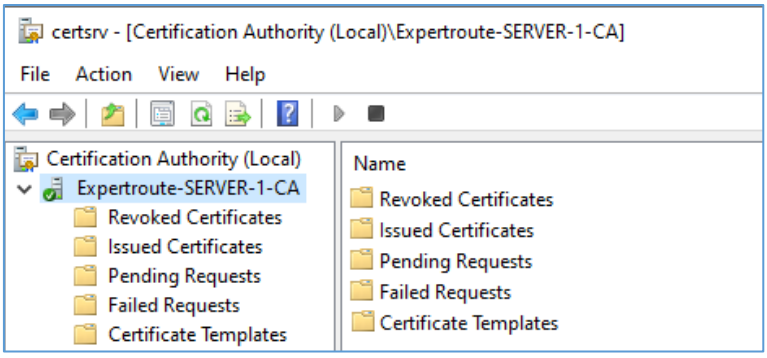
بعد از اجرا شدن سرویس، می‌توانید به مانند شکل ۸-۷٦۱، وارد Search شوید و سرویس موردنظر را اجرا کنید و یا می‌توانید از طریق Server Manager و از منوی Tools بر روی Certification Authority کلیک کنید.

www.takbook.com



شکل ۸- ۷۶۱ نصب *Certificate Service*

همان‌طور که در شکل ۸-۷٦۲، مشاهده می‌کنید سرویس مورد نظر اجرا شده است و دارای پنج پوشه است.



شکل ۸- ۷۶۲ نصب *Certificate Service*

اگر بخواهیم در مورد پوشه‌های شکل ۸-۷٦۲، توضیح دهیم باید بگوییم که:

۱- Revoked Certificates (گواهی‌نامه‌های لغو شده) : این پوشه شامل گواهی‌نامه‌هایی است که به دلیل نقض امنیتی، از دست رفتن کلید خصوصی، یا هر دلیل دیگری توسط مدیر CA لغو شده‌اند. این اطلاعات برای اطمینان از اینکه گواهی‌نامه‌های لغو شده دیگر معتبر نیستند، ضروری هستند.

۲- Issued Certificates (گواهی‌نامه‌های صادر شده): این پوشه شامل تمامی گواهی‌نامه‌هایی است که توسط سرویس گواهی‌نامه صادر شده‌اند و به کاربران یا دستگاه‌ها تخصیص داده شده‌اند. می‌توانید جزئیات هر گواهی‌نامه مانند تاریخ صدور، تاریخ انقضا، صادرکننده و گیرنده را مشاهده کنید.

www.takbook.com

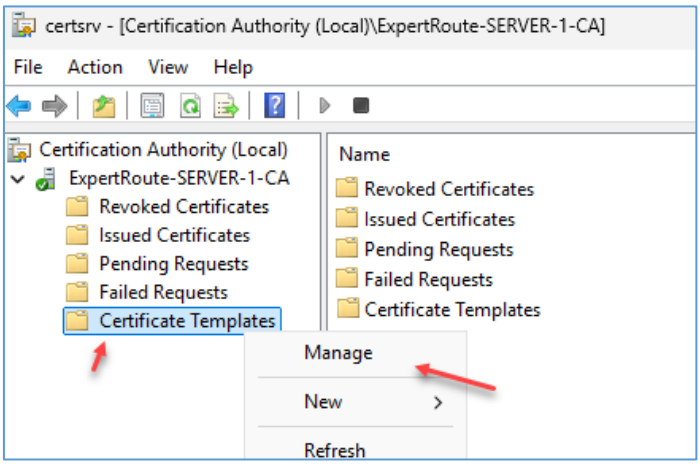
۳- Pending Requests (درخواست‌های در انتظار): در این قسمت، درخواست‌های گواهی‌نامه‌ای که توسط کاربران یا دستگاه‌ها ارسال شده‌اند اما هنوز توسط مدیر CA تأیید یا صادر نشده‌اند، ذخیره می‌شوند. مدیر می‌تواند این درخواست‌ها را بررسی و در صورت تأیید، گواهی‌نامه مربوطه را صادر کند.

۴- Failed Requests در کنسول مدیریت سرویس Certificate Authority (CA) مربوط به درخواست‌های گواهی‌نامه‌ای است که به دلایلی با شکست مواجه شده و نتوانسته‌اند به طور موفقیت‌آمیز پردازش یا صادر شوند.

۵- Certificate Templates (الگوهای گواهی‌نامه): الگوهای گواهی‌نامه‌ها تعیین‌کننده نوع و ویژگی‌های گواهی‌نامه‌های صادر شده هستند. این بخش به مدیر امکان می‌دهد الگوهای موجود را مشاهده، ایجاد یا ویرایش کند تا مطمئن شود که گواهی‌نامه‌های صادر شده با نیازهای سازمان مطابقت دارند.

برای تست این سرویس می‌خواهیم یک وب‌سایت که در سرویس IIS ایجاد کردیم را به صورت HTTPS اجرا کنیم و زمانی که می‌خواهیم از HTTPS استفاده کنیم باید یک گواهینامه معتبر داشته باشیم، برای این کار از سرویس Certificate استفاده می‌کنیم.

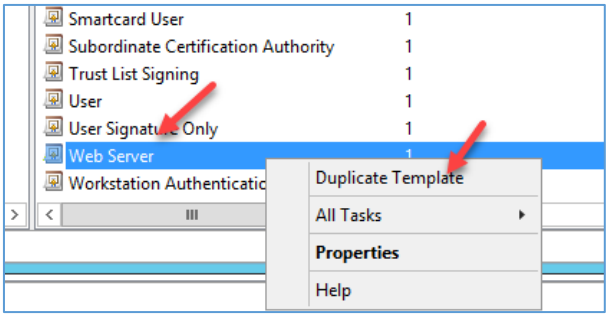
برای اینکه به وب سایت خود یک گواهینامه تخصیص دهیم باید از Templateهای آماده استفاده کنیم که به مانند شکل ۸-۷۶۳، وارد Certificate Template شوید، این قسمت یک سری گواهینامه‌های امنیتی آماده را برای قسمت‌های مختلف ویندوز از قبل آماده کرده است، در این قسمت می‌خواهیم یک قالب برای کاربران خود ایجاد کنیم، برای همین کار بر روی Certificate Templates کلیک راست کنید و گزینه Manage را انتخاب کنید.



شکل ۸- ۷۶۳ نصب *Certificate Service*

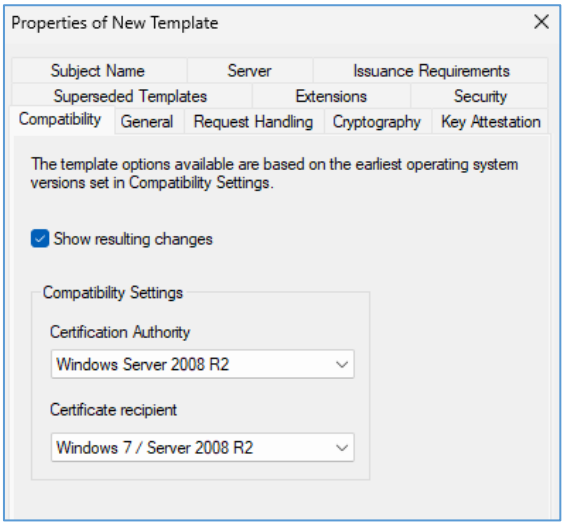
www.takbook.com

در شکل ۸-۷٦٤، انواع قالب‌های مختلف در زمینه‌های مختلف را مشاهده می‌کنید، از بین آن‌ها بر روی Web Server کلیک راست کنید و گزینه Dublicate Template را انتخاب کنید. توجه داشته باشید این قالب‌ها یک سری تنظیماتی هستند که از قبل انجام‌شده است، که مثلاً برای استفاده وب‌سایت از قالب Web Server استفاده می‌کنیم.



شکل ۸- ۷۶۴ نصب *Certificate Service*

در شکل ۸-۷٦٥، در تب Compatibility گزینه‌های برای انتخاب حداقل ویندوزهایی که می‌خواهند از این گواهینامه امنیتی استفاده کنند وجود دارد که می‌توانید بسته به سازمان خود که از چه ویندوزهایی استفاده می‌کند، گزینه موردنظر را انتخاب کنید که البته نیازی به تغییر نیست.



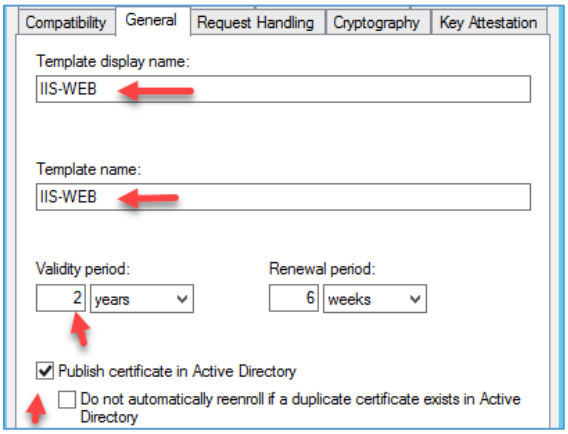
شکل ۸- ۷۶۵ راه‌اندازی *Certificate Service*

به مانند شکل ۸-۷٦٦، در تب General باید در قسمت Template Display Name نام موردنظر خود را وارد کنید، با واردکردن آن در قسمت Template name به‌صورت خودکار این اسم نوشته می‌شود.

www.takbook.com

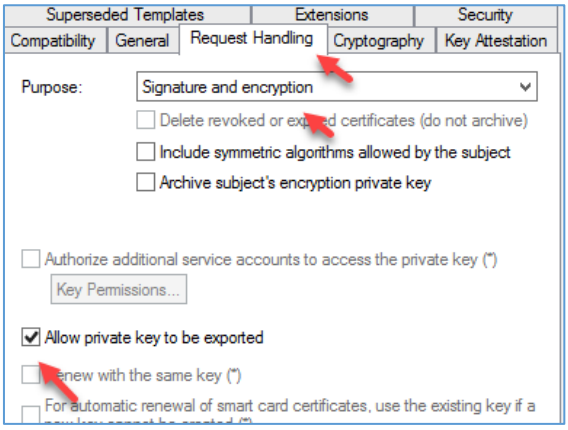
در قسمت Validity Period باید حداکثر اعتبار این گواهینامه را مشخص کنید که در این قسمت ۱ سال انتخاب‌شده است و در قسمت Renewal Period باید مقدار زمان هشدار تا رسیدن به‌اندازه Validity Period را مشخص کنید که در اینجا ٦ هفته مشخص‌شده است.

یکی از مهمترین گزینه‌ها تیک گزینه‌ی Publish certificate in active Directory را انتخاب کنید تا این گواهینامه در Active قرار بگیرد تا کاربران به صورت اتوماتیک به آن دسترسی داشته باشند.



شکل ۸- ۷۶۶ راه‌اندازی *Certificate Service*

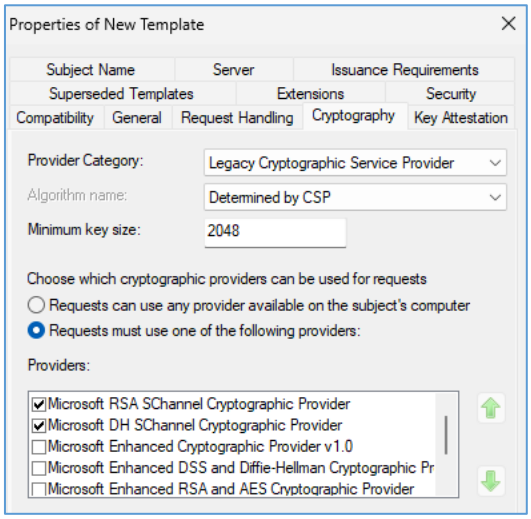
به مانند شکل ۸-۷٦۷، در تب Request Handling می‌توانید در قسمت Purpose نوع گواهینامه خود را مشخص کنید، مثلاً اگر در سازمان خود از کارت‌های هوشمند استفاده می‌کنید گزینه Smart Card را انتخاب کنید و یا گزینه دیگر را برای سازمان خود انتخاب کنید البته در حالت پیش‌فرض گزینه رمزنگاری و امضاء دیجیتال انتخاب‌شده است که باید همین گزینه باشد و حتماً تیک گزینه‌ی Allow private Key to exported را انتخاب کنید تا قابلیت Export برای این Template فعال شود.



شکل ۸- ۷۶۷ راه‌اندازی *Certificate Service*

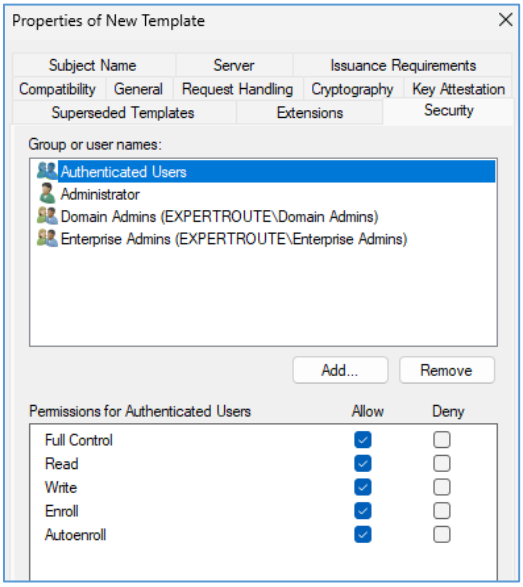
www.takbook.com

به مانند شکل ۸-۷۶۸، در تب Cryptography می‌توانید، نوع Provider گواهینامه موردنظر را تغییر دهید و طول کلید را تغییر دهید، هر چه طول کلید بیشتر باشد، امنیت کار افزایش پیدا می‌کند، هرچند عدد ۲۰۴۸ هم‌عددی بزرگی است.



شکل ۸- ۷۶۸ راه‌اندازی *Certificate Service*

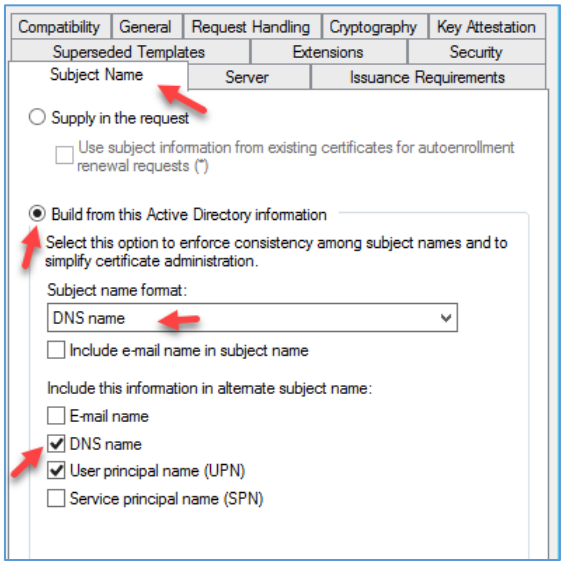
به مانند شکل ۸-۷۶۹، در تب Security از لیست موردنظر گروه Authenticated Users را انتخاب کنید و در قسمت Permissions گزینه‌های Read و Enroll را انتخاب کنید که البته در سرور جدید همه گزینه‌ها به صورت پیش فرض انتخاب شده است.



شکل ۸- ۷۶۹ راه‌اندازی *Certificate Service*

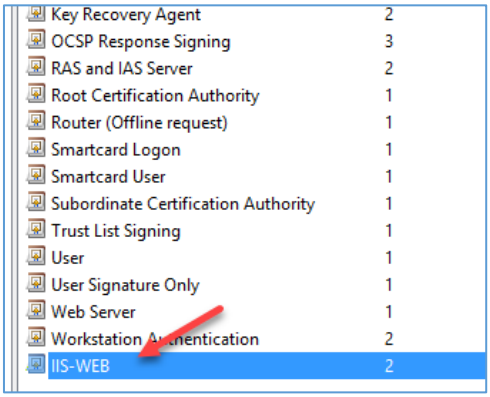
www.takbook.com

به مانند شکل ۸–۷۷۰، در تب Subject Name گزینه‌ی Build from this Active Directory را انتخاب کنید و از منوی کشویی گزینه‌ی DNS name را انتخاب کنید و تیک گزینه‌ی DNS name را انتخاب کنید و بر روی OK کلیک کنید تا Template مورد نظر ایجاد شود.



شکل ۸- ۷۷۰ راه‌اندازی *Certificate Service*

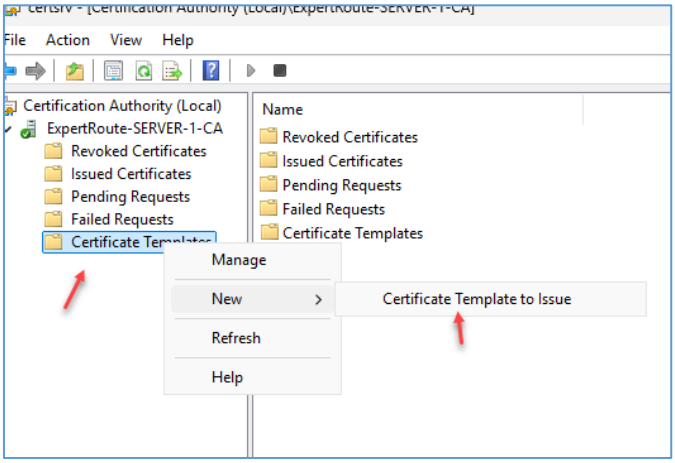
همان‌طور که در شکل ۸–۷۷۱، مشاهده می‌کنید Template مورد نظر ایجاد شده است.



شکل ۸- ۷۷۱ راه‌اندازی *Certificate Service*

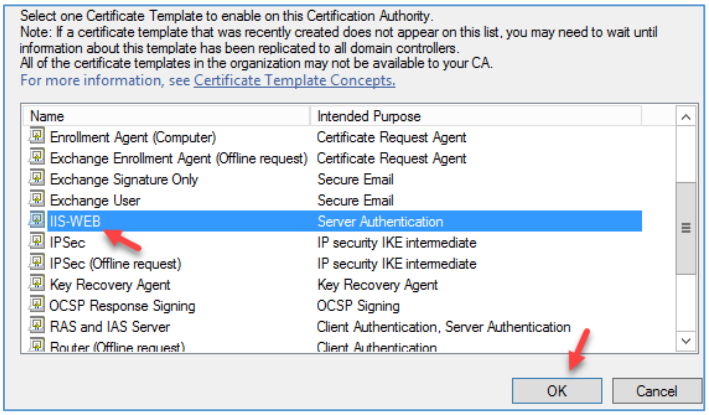
وارد سرویس شوید و به مانند شکل ۸–۷۷۲، بر روی Certificate Templates کلیک راست کنید و از قسمت New گزینه Certificate Template to issue را انتخاب کنید.

www.takbook.com



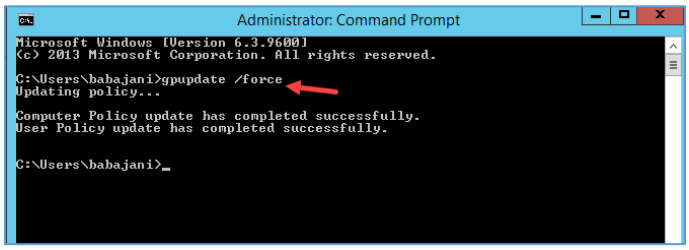
شکل ۸- ۷۷۲ راه‌اندازی *Certificate Service*

در شکل ۸-۷۷۳، Template مورد نظر که با هم ایجاد کردیم را انتخاب و بر روی OK کلیک کنید.



شکل ۸- ۷۷۳ راه‌اندازی *Certificate Service*

بعد از این کار به مانند شکل ۸-۷۷٤، با دستور gpupdate /force یک بار Group Policy را آپدیت کنید.



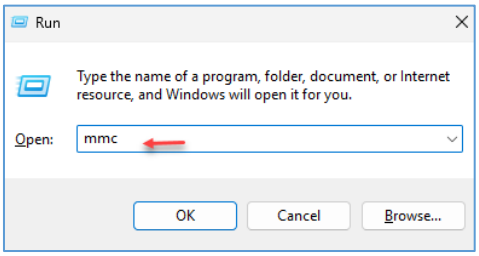
شکل ۸- ۷۷۴ راه‌اندازی *Certificate Service*

www.takbook.com

بعد از ایجاد Template مورد نظر همه چی برای ایجاد یک گواهینامه برای سرورهایی که سایت‌های IIS بر روی آنها فعال شده است فراهم شده است.

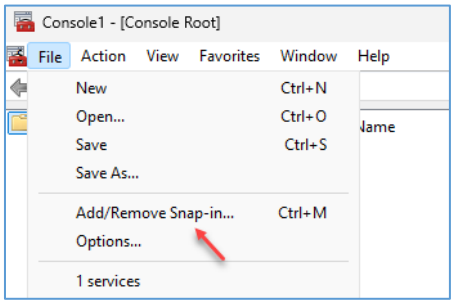
برای انجام و تست این کار یک سرور با نام sql.expertroute.local داریم و می‌خواهیم سایت آن را با این Template فعال کنیم تا دارای گواهینامه معتبر شود.

برای شروع وارد سرور SQL می‌شویم و سرویس MMC را به مانند شکل ۸–۷۷۵، در Run اجرا می‌کنیم.



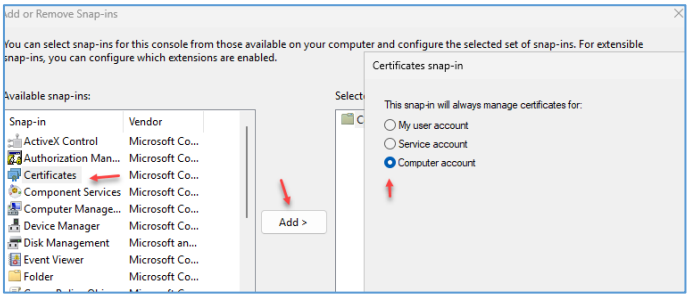
شکل ۸– ۷۷۵ اجرای mmc

به مانند شکل ۸–۷۷۶، وارد منوی File شوید و بر روی Add/Remove Snap-in کلیک کنید.



شکل ۸– ۷۷۶ اجرای mmc

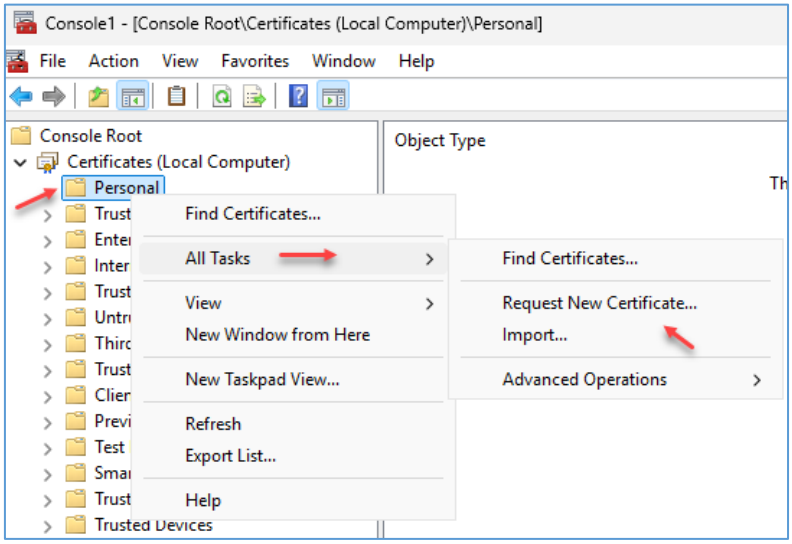
در شکل ۸–۷۷۷، گزینه‌ی Certificate را انتخاب کنید و بر روی Add کلیک کنید و در پنجره باز شده گزینه‌ی Computer Account را انتخاب کنید.



شکل ۸– ۷۷۷اجرای mmc

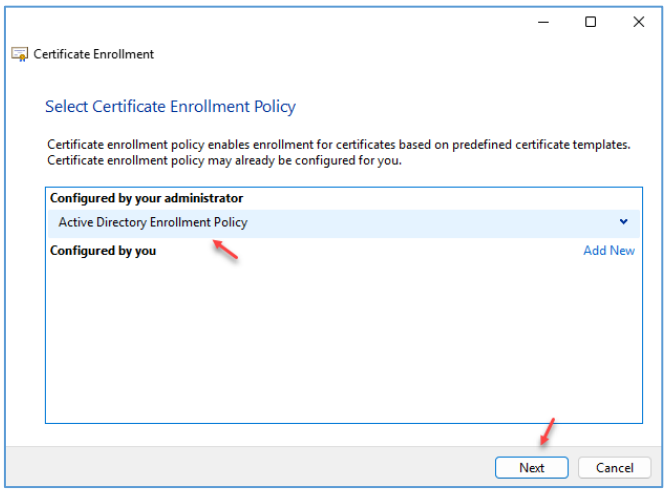
www.takbook.com

در شکل ۸–۷۷۸، از قسمت Personal وارد All Tasks شوید و گزینه‌ی Request New Certificate را اجرا کنید.



شکل ۸- ۷۷۸ درخواست گواهینامه برای سایت

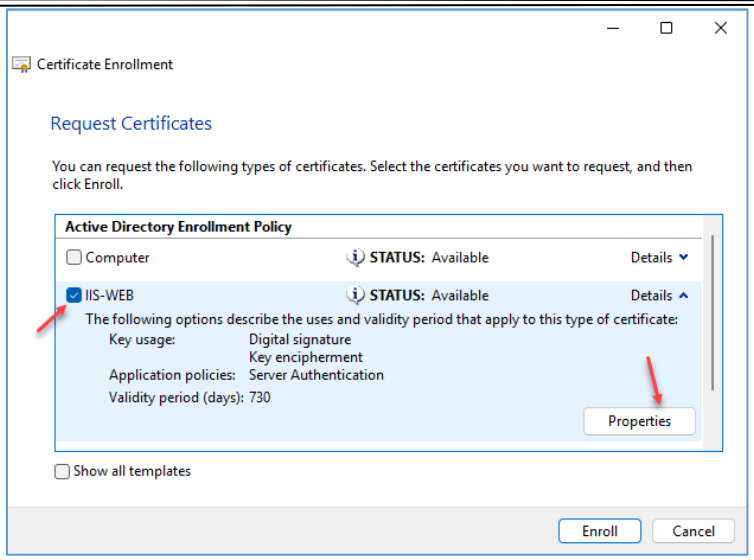
در ادامه کار و در شکل ۸–۷۷۹، گزینه‌ی Active Directory را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸- ۷۷۹ درخواست گواهینامه برای سایت

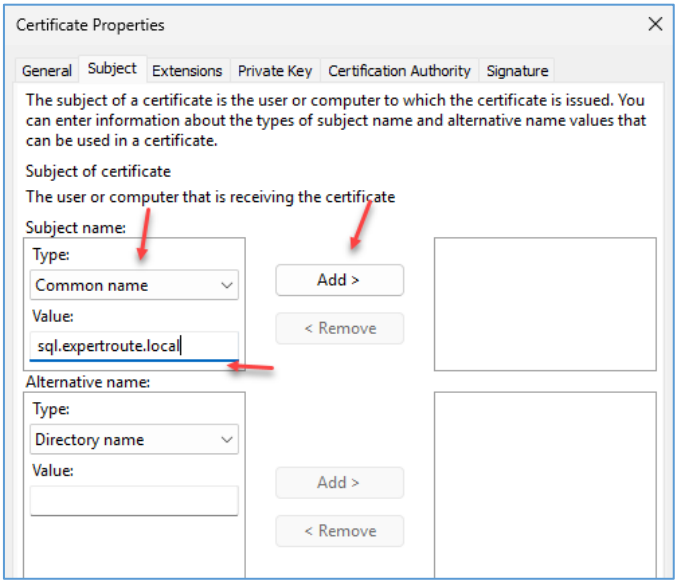
در شکل ۸–۷۸۰، همان Template که با هم ایجاد کرده بودیم را مشاهده می‌کنید، آن را انتخاب و بر روی گزینه‌ی Properties کلیک کنید.

www.takbook.com



شکل ۸- ۷۸۰ درخواست گواهینامه برای سایت

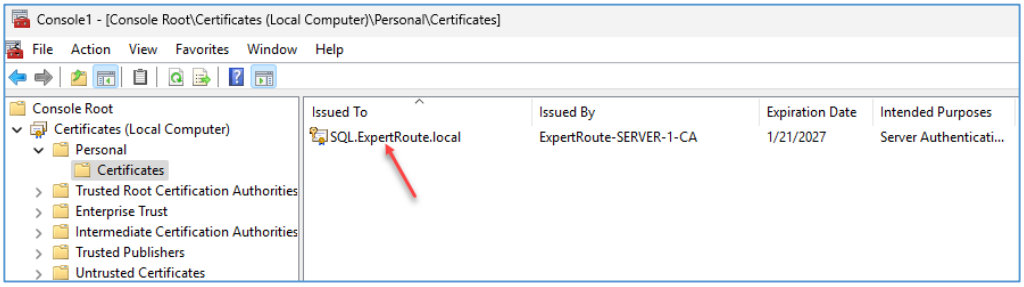
به مانند شکل ۸-۷۸۱، وارد تب Subject شوید و گزینه‌ی Common name را انتخاب و آدرس سایت خود را وارد کنید و بعد بر روی Add کلیک کنید تا به لیست اضافه شود، بعد از کلیک بر روی OK بر روی Enroll کلیک کنید.



شکل ۸- ۷۸۱ درخواست گواهینامه برای سایت

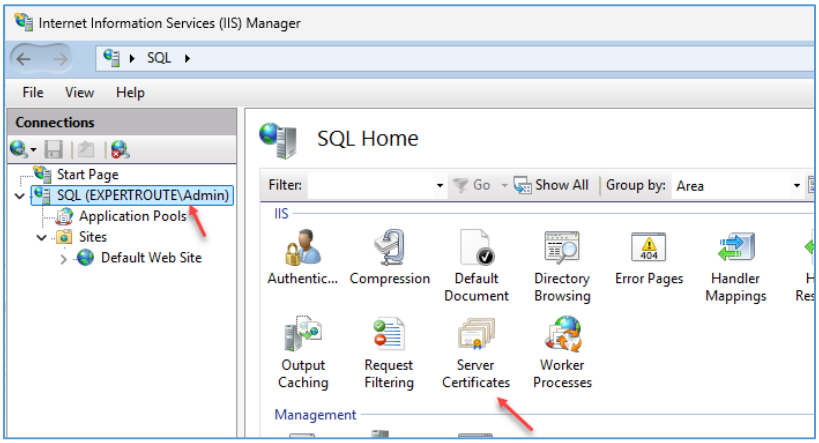
www.takbook.com

همان‌طور که در شکل ۸-۷۸۲، گواهینامه مورد نظر به لیست اضافه شده است و همه چیز آماده است که سایت خود را بر روی این گواهینامه بالا بیاریم.



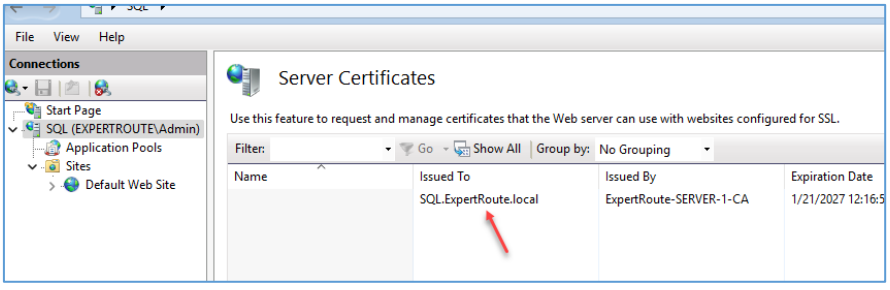
شکل ۸- ۷۸۲ درخواست گواهینامه برای سایت

به مانند شکل ۸-۷۸۳، بر روی نام سرور کلیک کنید و در صفحه‌ی باز شده بر روی Server Certificate کلیک کنید.



شکل ۸- ۷۸۳ درخواست گواهینامه برای سایت

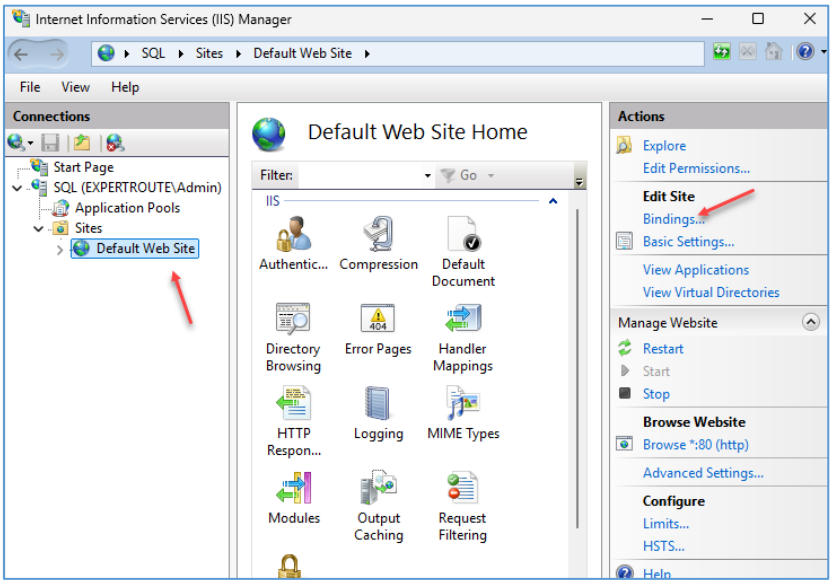
همان‌طور که در شکل ۸-۷۸٤، مشاهده می‌کنید گواهینامه جدید در سرویس IIS هم در دسترس است و می‌توانیم سایت را بر روی آن فعال کنیم.



شکل ۸- ۷۸۴ درخواست گواهینامه برای سایت

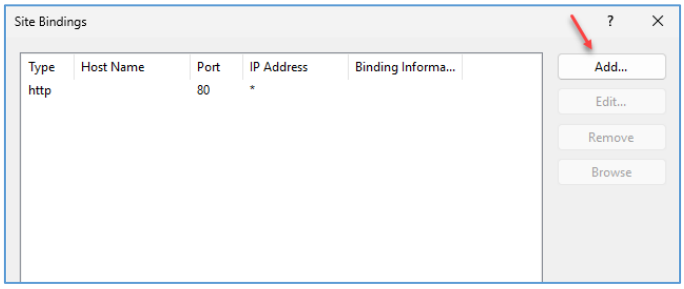
www.takbook.com

به مانند شکل ۸-۷۸۵، برای اینکه SSL را بر روی سایت خود فعال کنیم، باید سایت مورد نظر خود را انتخاب کنیم و بر روی Bindings کلیک کنید.



شکل ۸- ۷۸۵ فعال کردن SSL

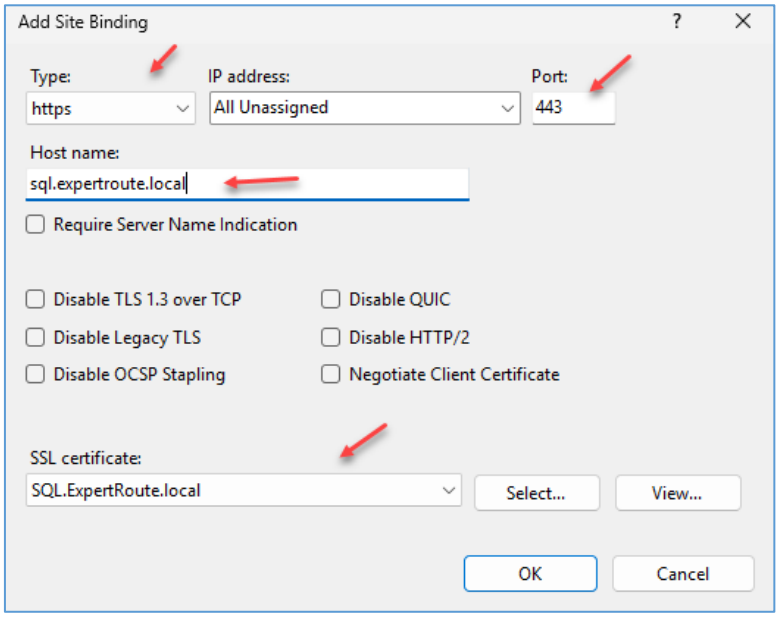
در شکل ۸-۷۸۶، یک پورت 80 برای پروتکل http را مشاهده می‌کنید که به صورت پیش‌فرض وجود دارد، برای اینکه SSL را اضافه کنیم بر روی Add کلیک کنید.



شکل ۸- ۷۸۶ فعال کردن SSL

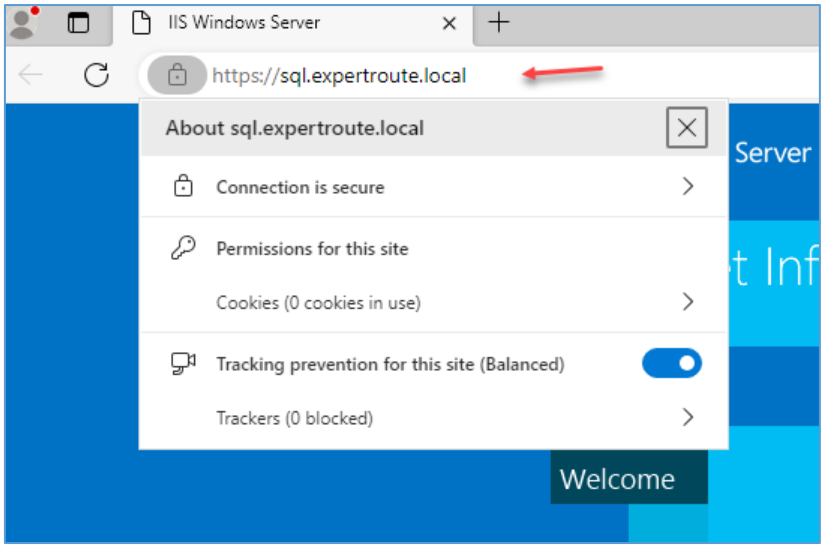
در شکل ۸-۷۸۷، گزینه‌ی https را انتخاب کنید و پورت آن را برابر با 443 قرار دهید و در قسمت Host name باید آدرس سایت را وارد کنید و در قسمت SSL certificate باید گواهینامه‌ای که با هم ایجاد کردیم را انتخاب کنید.

www.takbook.com



شکل ۸- ۷۸۷ فعال کردن SSL

بعد از انجام مراحل بالا باید سایت مورد نظر را تست بگیریم، که همان‌طور در شکل ۸-۷۸۸، مشاهده می‌کنید سایت با گواهینامه‌ای که ایجاد کرده‌ایم، فعال شده است.



شکل ۸- ۷۸۸ فعال کردن SSL

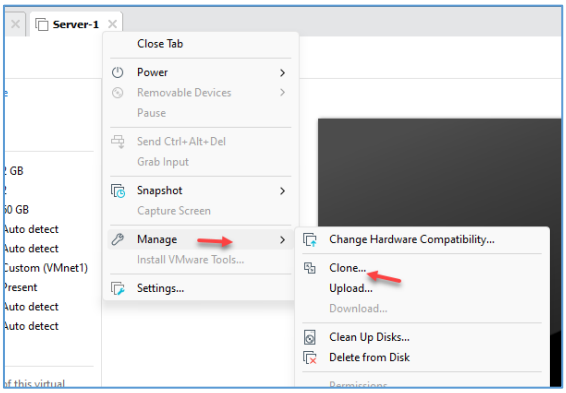
www.takbook.com

۸-۳-۲۲ سرویس Windows Server update Service (WSUS)

فرض کنید شما در شبکه خود ۲۰۰ کلاینت داشته باشید و همه آنها به اینترنت متصل باشند، اگر همه این کلاینت‌ها در یک زمان بخواهند آپدیت شوند چه اتفاقی برای پهنای باند شبکه می‌افتد؟ خوب مسلماً حجم بالایی از پهنای باند مصرف می‌شود و کل شبکه کند می‌شود و از همه مهم‌تر هزینه افزایش پیدا می‌کند.

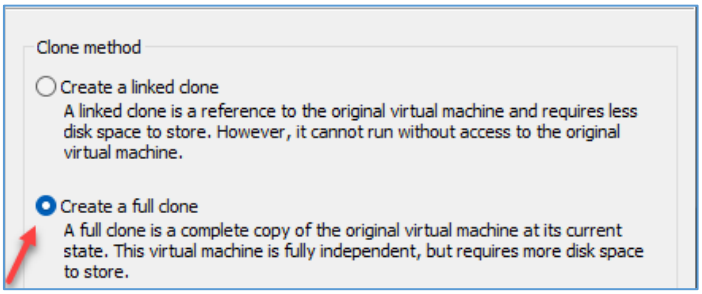
برای حل این مشکل تیم مایکروسافت سرویس WSUS یا همان Windows Server Update Service را معرفی کرد، این سرویس بر روی ویندوز سرور نصب می‌شود و تمام آپدیت‌ها را از سایت مایکروسافت برای تمام محصولات آن دریافت می‌کند و کلاینت‌های موجود در شبکه می‌توانند از طریق این سرویس اطلاعات خود را آپدیت کنند که نحوه تنظیم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

برای فعال‌سازی این سرویس بهتر است یک سرور مجزا برای آن در نظر بگیرید، همان‌طور که در شکل ۸-۷۸۹، مشاهده می‌کنید بر روی سرور قبلی خود که در VMware Workstation ایجاد کردیم کلیک راست می‌کنیم و یک Clone از آن ایجاد می‌کنیم.



شکل ۸- ۷۸۹ گرفتن Clone از ماشین مجازی

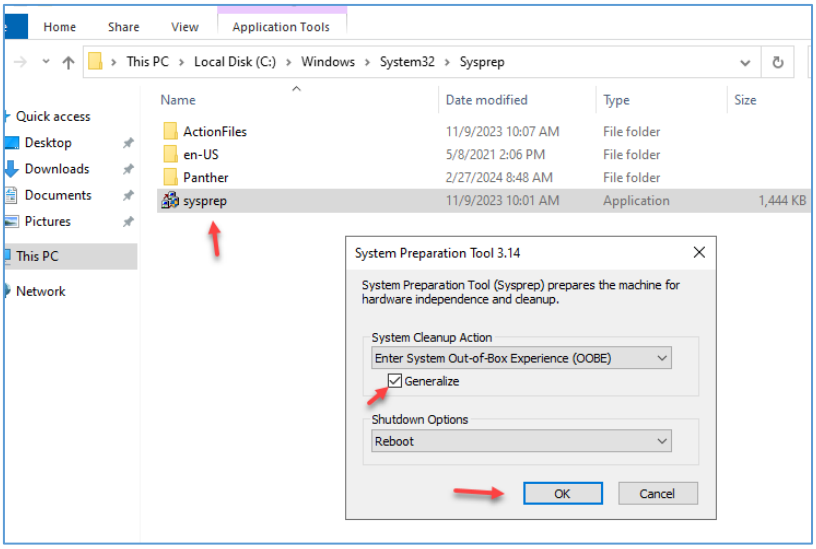
در شکل ۸-۷۹۰، گزینه‌ی Create a full Clone را انتخاب کنید تا یک کپی کامل از ماشین قبلی ایجاد شود.



شکل ۸- ۷۹۰ گرفتن Clone از ماشین مجازی

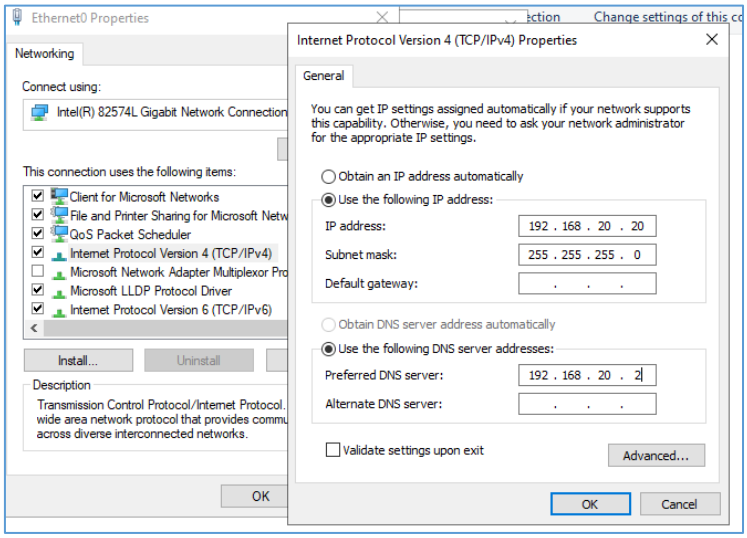
www.takbook.com

بعد از ایجاد کپی از ماشین مورد نظر به مانند قبل اولین کاری که انجام می‌دهید ورود به آدرس مشخص شده در شکل ۸-۷۹۱، است و اجرای فایل sysprep برای ایجاد یک شناسه‌ی جدید برای این ماشین تا در موقع متصل شدن به Active Directory با مشکل مواجه نشود، تیک گزینه‌ی Generalize را انتخاب و بر روی OK کلیک کنید.



شکل ۸- ۷۹۱ ریست تنظیمات ویندوز سرور

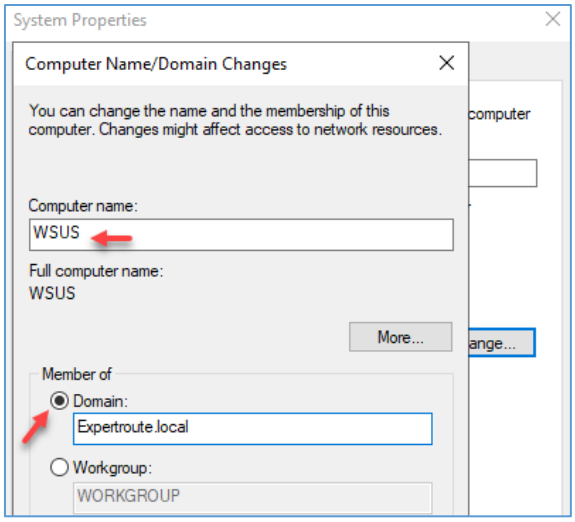
در ادامه و بعد از ورود به ویندوز سرور جدید باید آدرس IP آن را به مانند شکل ۸-۷۹۲، به صورت دستی وارد کنید.



شکل ۸- ۷۹۲ تغییر آدرس IP

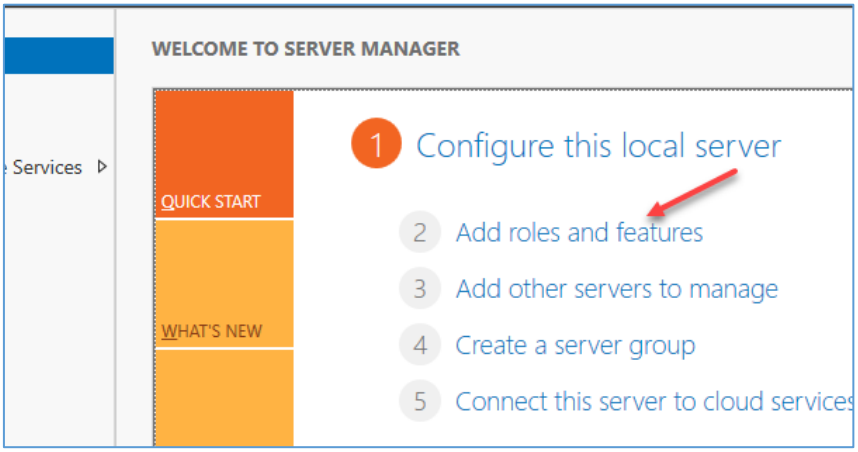
www.takbook.com

در ادامه کار باید نام سرور را تغییر و آن را به مانند شکل ۸-۷۹۳، عضو دومین مورد نظر خود کنید.



شکل ۸- ۷۹۳ عضو کردن در دومین

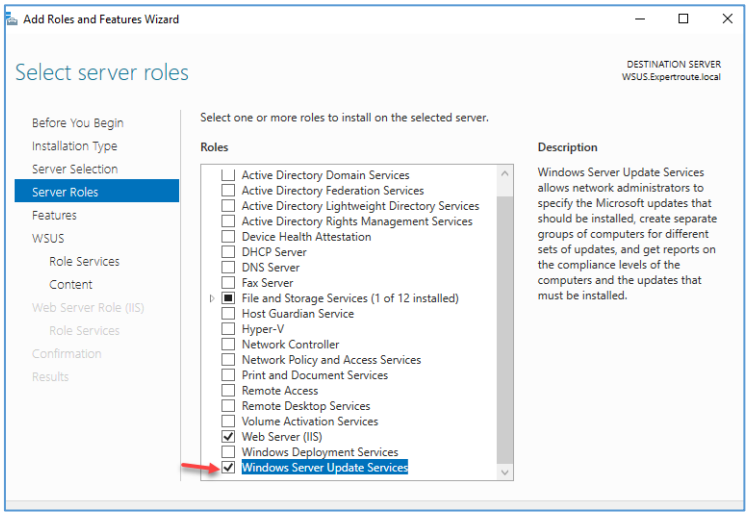
برای نصب سرویس WSUS باید وارد Server Manager شوید و به مانند شکل ۸-۷۹٤، بر روی Add Roles and Feature کلیک کنید.



شکل ۸- ۷۹۴ نصب و راه‌اندازی سرویس WSUS

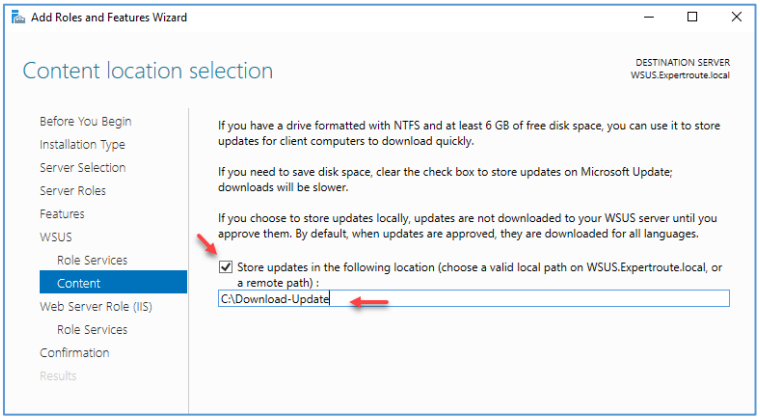
به مانند شکل ۸-۷۹۵، بر روی Next کلیک کنید تا به قسمت Server Roles برسید، در این قسمت از لیست Roleهای موجود گزینه Windows Server Update Services را انتخاب کنید و در پنجره باز شده بر روی Add Feature کلیک کنید زمانی که این سرویس را انتخاب می‌کنید به صورت اتوماتیک سرویس IIS هم انتخاب می‌شود.

www.takbook.com



شکل ۸- ۷۹۵ نصب و راه‌اندازی سرویس WSUS

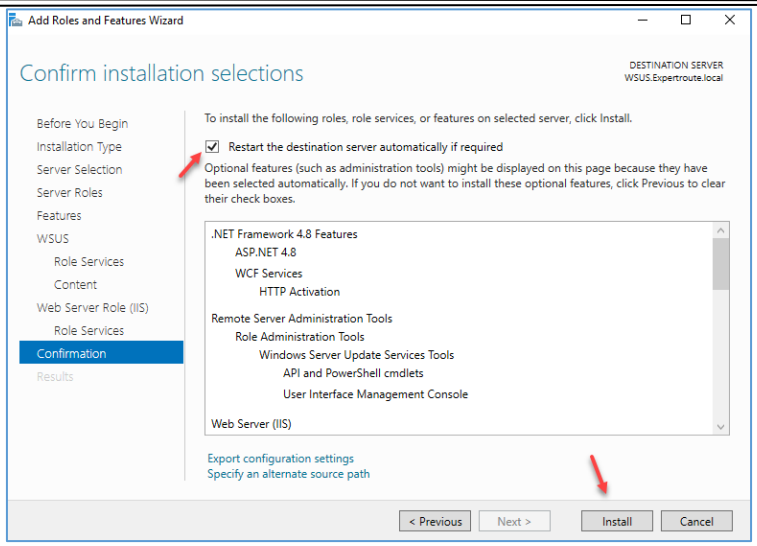
به مانند شکل ۸-۷۹۶، بر روی Next کلیک کنید تا به قسمت Content برسید، در این قسمت باید آدرس مناسبی را وارد کنید که درایو آن بیشتر از ٦ گیگابات فضا داشته باشد تا فایل‌های آپدیت زمانی که دانلود می‌شوند در این آدرس قرار بگیرد.



شکل ۸- ۷۹۶ نصب و راه‌اندازی سرویس WSUS

در شکل ۸-۷۹۷، بر روی Install کلیک کنید تا نصب سرویس آغاز شود.

www.takbook.com



شکل ۸- ۷۹۷ نصب و راه‌اندازی سرویس WSUS

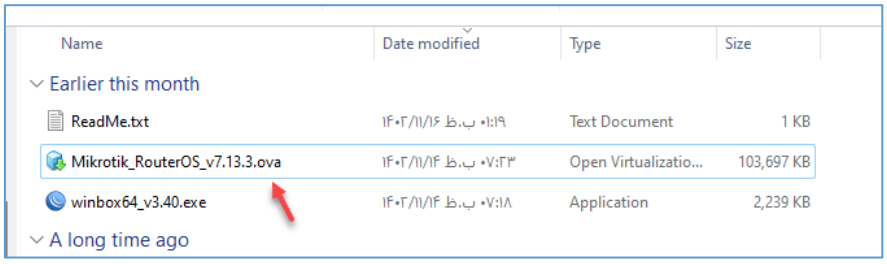
بعد از نصب سرویس WSUS و قبل از اجرای آن حتماً سرور را به اینترنت متصل کنید تا تنظیمات به درستی انجام شود، اگر اینترنت فعال نباشد این کار امکان پذیر نیست.

برای اینکه از اینترنت استفاده کنیم می‌توانیم از میکروتیک برای این کار استفاده کنیم، که در فصل فهتم به صورت کامل میکروتیک را بررسی کردیم، برای انجام این کار یک ماشین مجازی میکروتیک دانلود و تظیمات خود را روی آن انجام می‌دهیم و زمانی که میکروتیک اینترنت‌دار شد در قسمت Gateway آدرس میکروتیک را برای سرورها وارد می‌کنیم تا اینترنت برای آنها فعال شود.

برای شروع از لینک زیر روتر میکروتیک را دانلود کنید:

https://soft98.ir/internet/network/1163-mikrotik-routeros.html

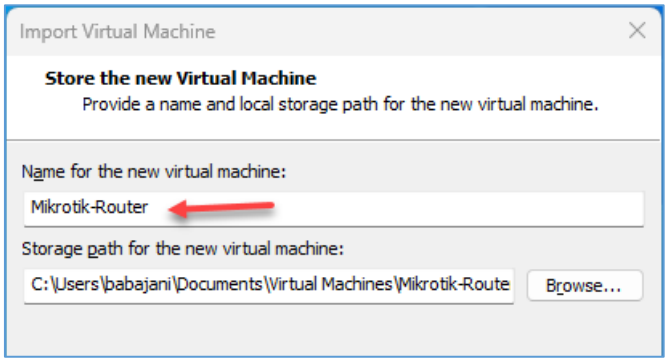
بعد از دانلود و اکسترکت کردن فایل به مانند شکل ۸-۷۹۸، بر روی فایل ova دو بار کلیک کنید تا از طریق نرم‌افزار VMware اجرا شود.



شکل ۸- ۷۹۸ نصب و راه‌اندازی میکروتیک

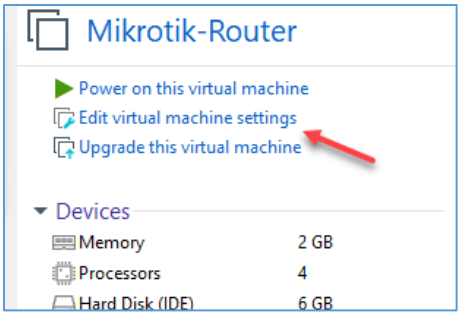
در ادامه و در شکل ۸-۷۹۹، نام سیستم را وارد کنید و بر روی Import کلیک کنید.

www.takbook.com



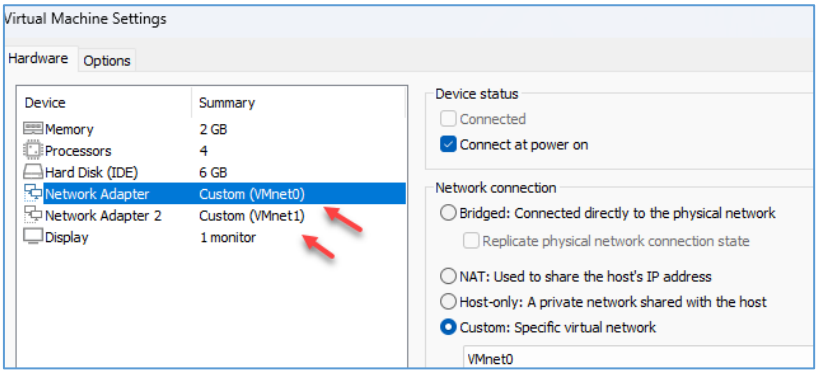
شکل ۸- ۷۹۹ نصب و راه‌اندازی میکروتیک

بعد از ایجاد ماشین مورد نظر به مانند شکل ۸-۸۰۰، بر روی Edit virtual machine settings کلیک کنید تا تنظیمات کارت شبکه را انجام دهیم.



شکل ۸- ۸۰۰ نصب و راه‌اندازی میکروتیک

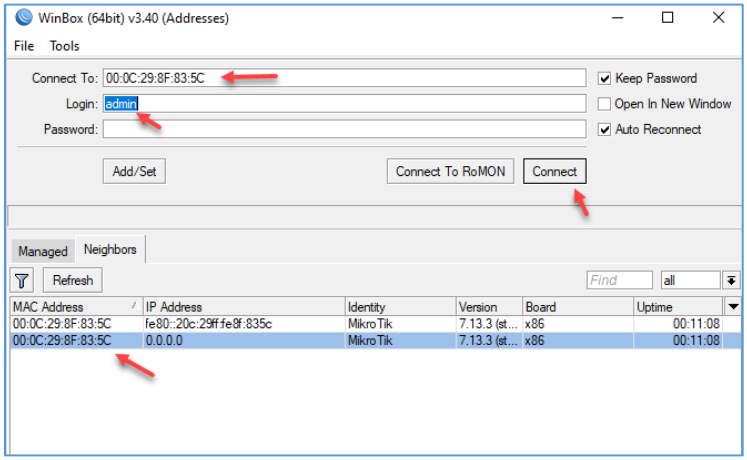
در شکل ۸-۸۰۱، باید یک کارت شبکه را به اینترنت متصل کنید و کارت شبکه‌ی دیگر را به کارت شبکه‌ی داخلی سرورها متصل کنید که کارت شبکه‌ی VMnet0 مربوط به اینترنت و کارت شبکه‌ی VMnet1 مربوط به شبکه‌ی داخلی است.



شکل ۸- ۸۰۱ نصب و راه‌اندازی میکروتیک

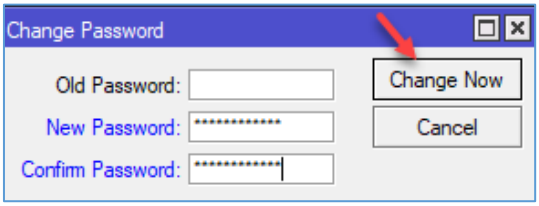
www.takbook.com

بعد از انجام مراحل بالا ماشین مورد نظر را روشن کنید، توجه داشته باشید برای متصل شدن به میکروتیک می‌توانید از نرم‌افزار گرافیکی آن با نام Winbox که در پوشه‌ی دانلود قرار داشت استفاده کنید، اگر در نرم‌افزار مورد نظر وارد تب Neighbors شوید و اگر به شکل ۸-۸۰۲، توجه کنید به صورت اتومانیک میکروتیک را پیدا کرده است که بر روی آدرس MAC آن دو بار کلیک کنید و با استفاده از نام کاربری Admin و بدون پسورود بر روی Connect کلیک کنید و وارد آن شوید.



شکل ۸- ۸۰۲ نصب و راه‌اندازی میکروتیک

بعد از ورود به مانند شکل ۸-۸۰۳، رمز عبور جدید را وارد کنید:



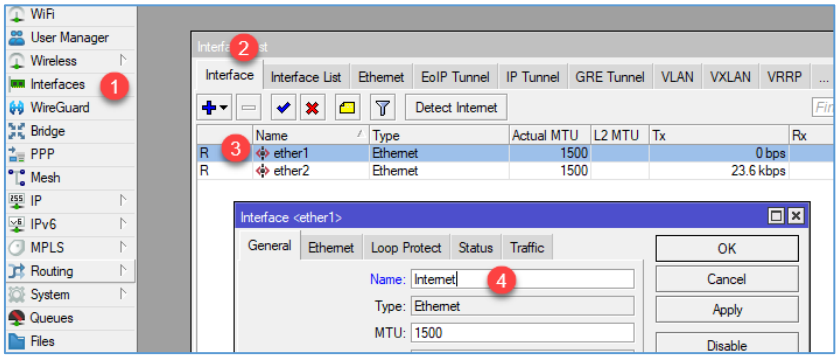
شکل ۸- ۸۰۳ نصب و راه‌اندازی میکروتیک

توجه داشته باشید این فصل، مربوط به آموزش سیستم‌های مایکروسافت است و ربطی به میکروتیک ندارد و برای اینکه در این قسمت از روتر میکروتیک استفاده کنیم خیلی سریع آموزش آن را در این قسمت قرار می‌دهیم ولی برای یادگیری کامل میکروتیک باید فصل هفتم این کتاب را مطاله بفرمایید.

به مانند شکل ۸-۸۰٤، اولین کاری که انجام می‌دهیم دو کارت شبکه‌ای که به میکروتیک اختصاص دادیم را مشخص می‌کنیم که کدام برای اینترنت و کدام برای شبکه‌ی داخلی است.

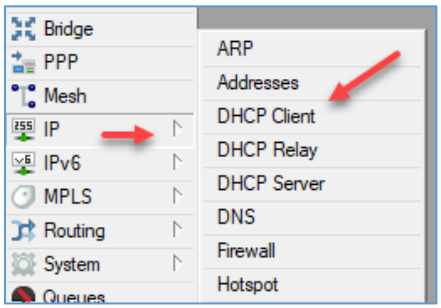
به مانند شکل ۸-۸۰٤، بر روی Interfaces کلیک کنید و در شکل باز شده در تب Interface دو کارت شبکه‌ی مورد نظر خود را مشاهده می‌کنید که اولی را به Internet و دومی را به Local تغییر می‌دهیم.

www.takbook.com



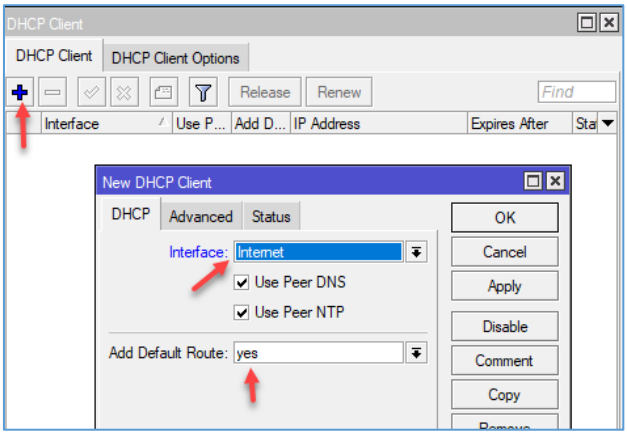
شکل ۸- ۸۰۴ نصب و راه‌اندازی میکروتیک

به مانند شکل ۸-۸۰۵، وارد منوی IP شده و گزینه‌ی DHCP Client را انتخاب می‌کنیم.



شکل ۸- ۸۰۵ نصب و راه‌اندازی میکروتیک

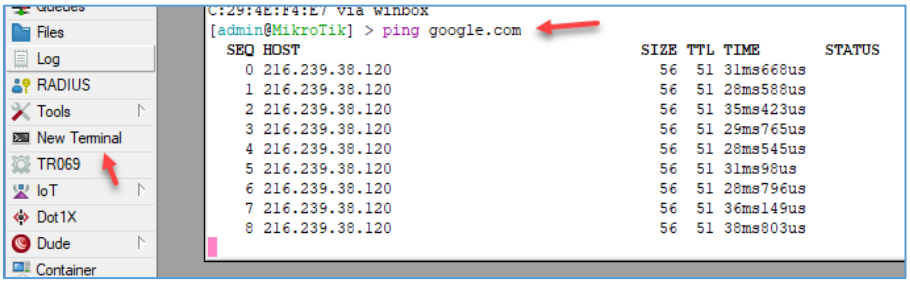
در ادامه کار می‌خواهیم از طریق DHCP که در شبکه‌ی Internet وجود دارد آدرس را دریافت کنیم، برای این کار به مانند شکل ۸-۸۰۶، در تب DHCP Client بر روی علامت + کلیک کنید و در شکل باز شده کارت شبکه‌ی Internet را انتخاب کنید و حتماً گزینه‌ی Add Default Route را بر روی Yes قرار دهید تا تمام ترافیک به سمت اینترنت Route شود.



شکل ۸- ۸۰۶ نصب و راه‌اندازی میکروتیک

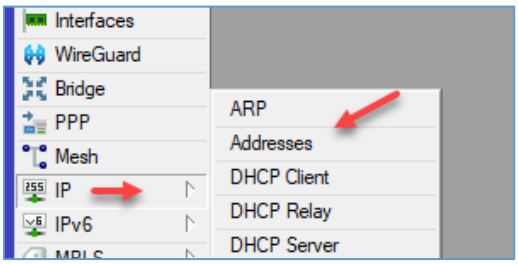
www.takbook.com

بعد از این کار به مانند شکل ۸-۸۰۷، اگر وارد Terminal شوید و Ping Google.com را اجرا کنید متوجه خواهید شد که میکروتیک به راحتی به اینترنت متصل شده است، حالا باید شبکه‌ی داخلی را درست کنیم.



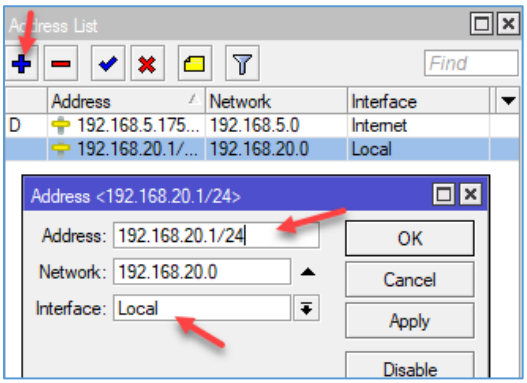
شکل ۸- ۸۰۷ نصب و راه‌اندازی میکروتیک

در ادامه کار به مانند شکل ۸-۸۰۸، وارد منوی IP شوید و گزینه‌ی Adresses را انتخاب کنید.



شکل ۸- ۸۰۸ نصب و راه‌اندازی میکروتیک

در شکل ۸-۸۰۹، بر روی آیکون + کلیک کنید و آدرس 192.168.20.1/24 را وارد کنید و نام Interface را هم بر روی Local قرار دهید و بر روی OK کلیک کنید.

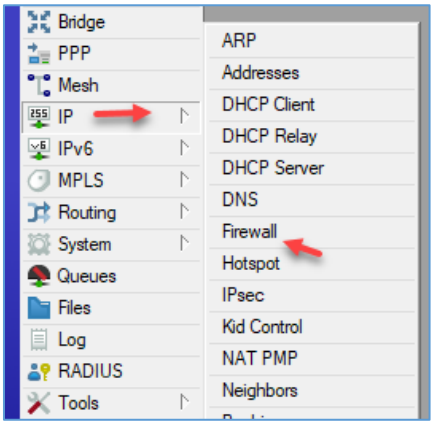


شکل ۸- ۸۰۹ نصب و راه‌اندازی میکروتیک

حالا اگر شبکه‌ی داخلی را هم Ping بگیریم این موضوع به صورت صحیح انجام می‌شود.

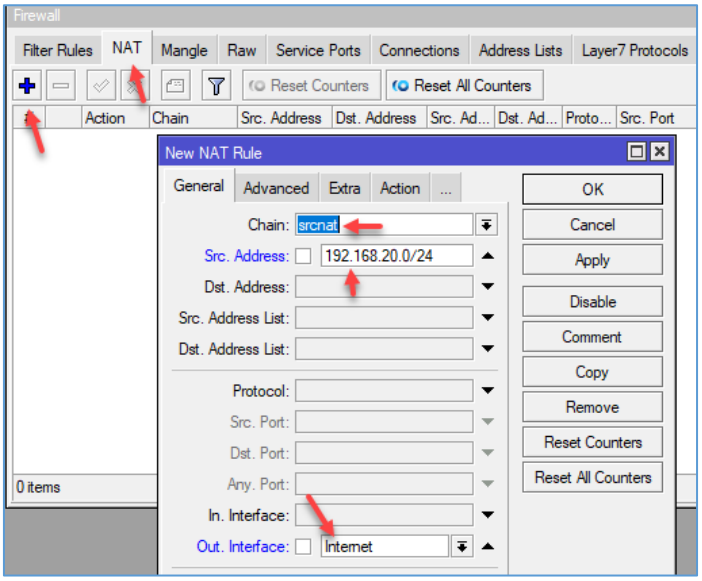
www.takbook.com

بعد از اینکه دو شبکه را آماده کردیم باید به مانند شکل ۸-۸۱۰، وارد Firewall و قسمت NAT شویم و آدرس‌های داخلی را به سمت اینترنت NAT کنیم تا کاربران و سیستم‌ها بتوانند به اینترنت دسترسی داشته باشند.



شکل ۸- ۸۱۰ نصب و راه‌اندازی میکروتیک

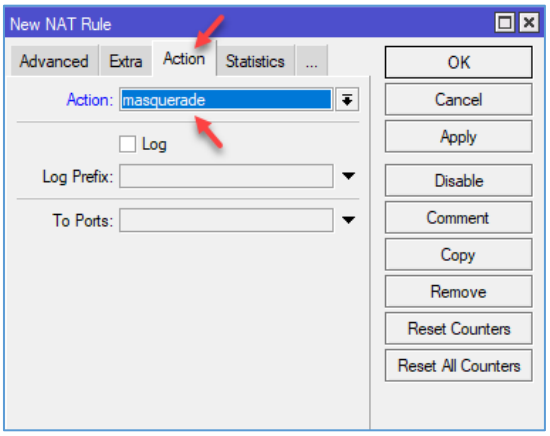
به مانند شکل ۸-۸۱۱، وارد تب NAT شوید و بر روی + کلیک کنید و در قسمت Chain گزینه‌ی srcnat را انتخاب کنید و در قسمت Src. Address باید آدرس شبکه‌ی داخلی خود را وارد کنید که در اینجا 192.168.20.0/24 وارد می‌کنیم و در قسمت Out. Interface باید کارت شبکه‌ی اینترنت را انتخاب کنید بعد از این کار وارد تب Action شوید.



شکل ۸- ۸۱۱ نصب و راه‌اندازی میکروتیک

www.takbook.com

به مانند شکل ۸-۸۱۲، در تب Action و برای اینکه آدرس‌های داخلی در اینترنت معتبر باشند گزینه‌ی masquerade را انتخاب کنید و بر روی OK کلیک کنید.



شکل ۸- ۸۱۲ نصب و راه‌اندازی میکروتیک

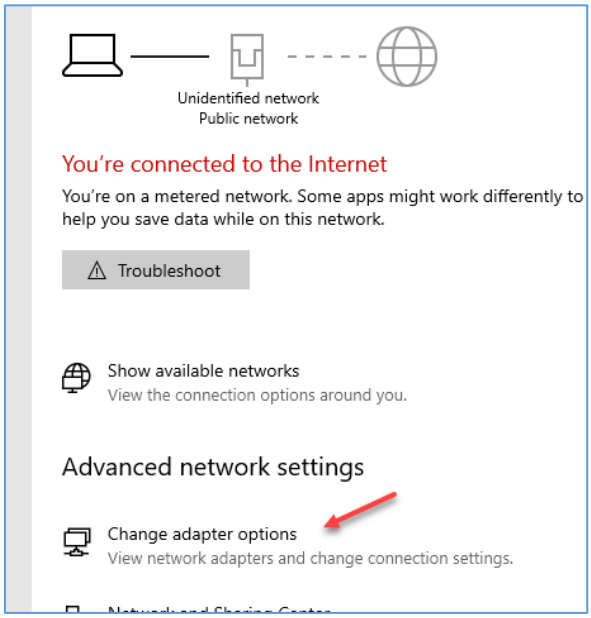
حالا روتر میکروتیک آماده است و کلاینت‌ها و سرورها می‌توانند به آن متصل شوند، برای این کار وارد سرور WSUS شوید و کلید ترکیبی WIN + X را فشار دهید تا شکل ۸-۸۱۳، ظاهر شود و در این شکل بر روی Network Connections کلیک کنید.



شکل ۸- ۸۱۳ تنظیم کارت شبکه

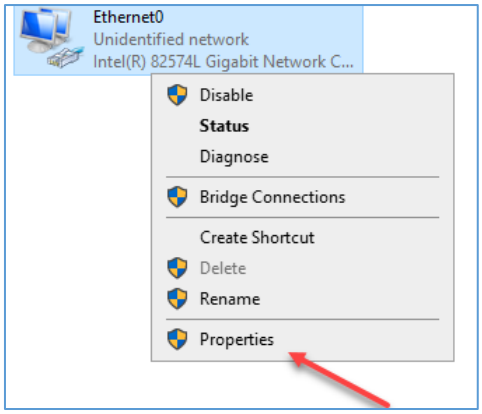
در شکل ۸-۸۱٤، بر روی Change adaptor options کلیک کنید.

www.takbook.com



شکل ۸- ۸۱۴ نصب و راه‌اندازی میکروتیک

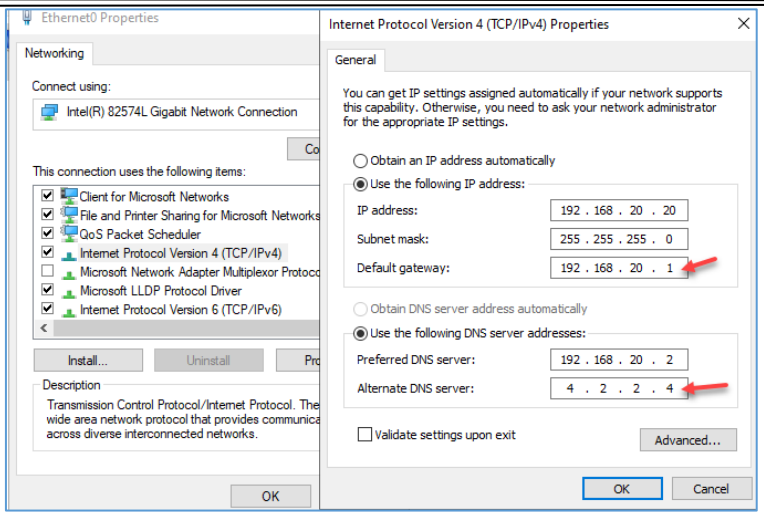
بر روی کارت شبکه‌ی مورد نظر کلیک راست کنید و به مانند شکل ۸-۸۱۵، گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۸۱۵ تنظیم کارت شبکه

در شکل ۸-۸۱۶، در قسمت default gateway باید آدرس روتر میکروتیک را وارد کنید، یعنی آدرس شبکه‌ی داخلی میکروتیک که 192.168.20.1 است و در قسمت DNS هم آدرس 4.2.2.4 را وارد کنید که DNS گوگل برای اینترنت است.

www.takbook.com



شکل ۸- ۸۱۶ تنظیم کارت شبکه

حالا اگر مرورگر را باز کنید اینترنت متصل خواهد بود که این موضوع را در شکل ۸-۸۱۷ مشاهده می‌کنید.



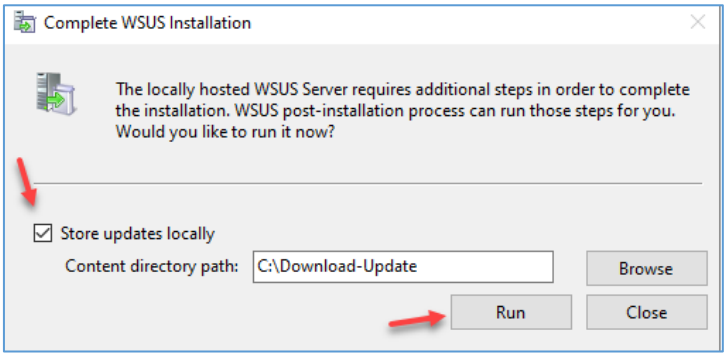
شکل ۸- ۸۱۷ تنظیم کارت شبکه

تا به اینجای کار سرویس WSUS نصب شده است و برای اینترنت داشتن آن یک روتر میکروتیک مجازی راه‌اندازی کردیم و سرور WSUS را به اینترنت متصل کردیم.

برای اجرای سرویس WSUS وارد Serach شوید و کلمه wsus را وارد کنید و در گزینه‌های موجود بر روی Windows Server Update Service کلیک کنید.

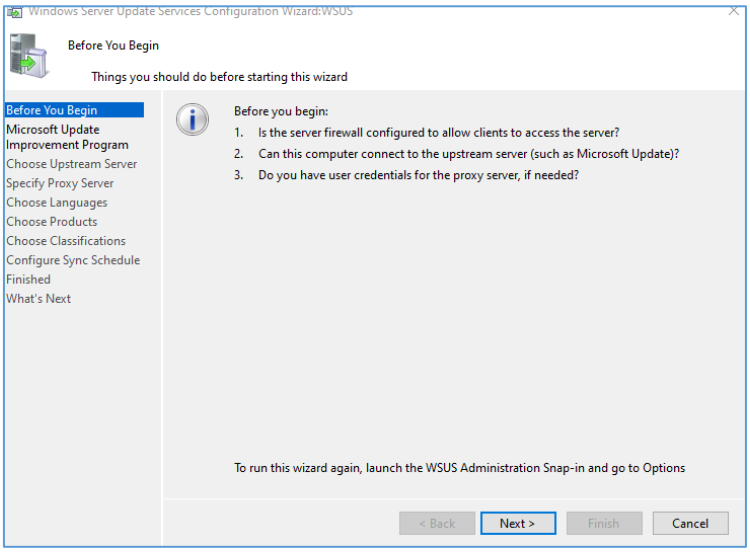
www.takbook.com

در شکل ۸-۸۱۸، آدرسی که قبلاً در هنگام نصب سرویس وارد کرده‌ایم را مشاهده می‌کنید که می‌توانید آدرس موردنظر را تغییر بدهید، بر روی Run کلیک کنید و بعد از ایجاد دیتابیس مورد نظر در آدرس مشخص شده شکل بعدی ظاهر خواهد شد.



شکل ۸- ۸۱۸ راه‌اندازی سرویس wsus

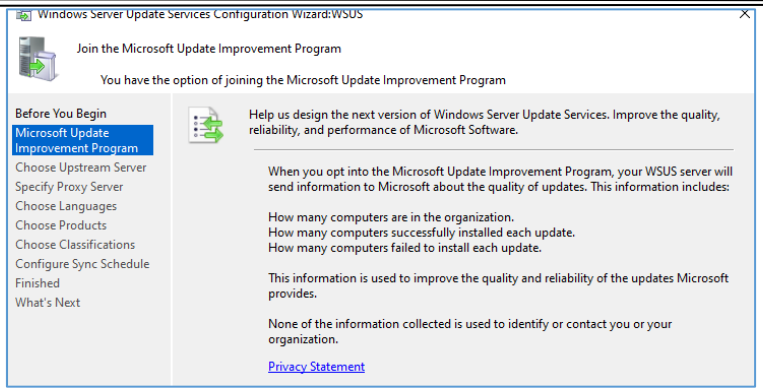
پنجره شکل ۸-۸۱۹، برای شما باز می‌شود که برای تنظیم سرویس بر روی Next کلیک کنید.



شکل ۸- ۸۱۹ راه‌اندازی سرویس wsus

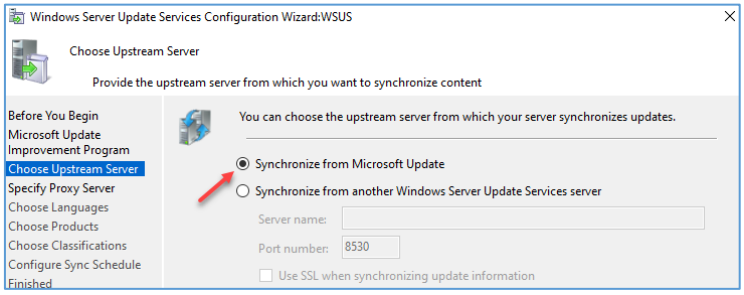
در شکل ۸-۸۲۰، توضیحاتی در مورد نحوه‌ی آپدیت شدن به شما می‌دهد که آن را مطالعه و بر روی Next کلیک کنید.

www.takbook.com



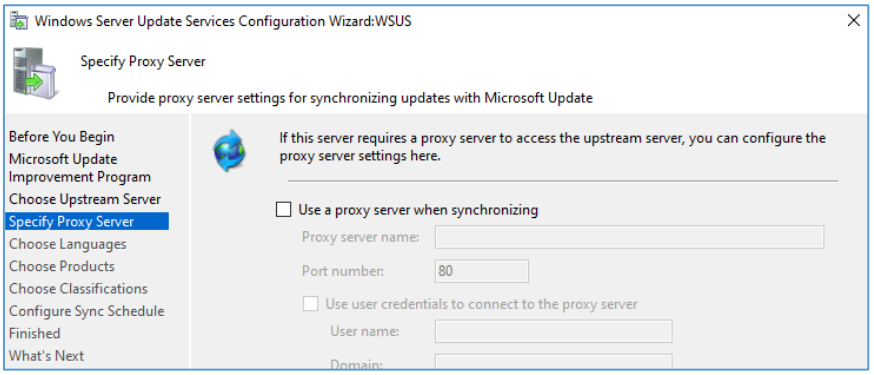
شکل ۸- ۸۲۰ راه‌اندازی سرویس wsus

در شکل ۸-۸۲۱، با انتخاب گزینه اول سرور شما به صورت مستقیم از طریق اینترنت با سرور مایکروسافت Syn و یا هماهنگ می‌شود، ولی اگر سرور دیگری دارید که می‌خواهید به آن متصل شوید باید گزینه دوم را فعال و آدرس سرور موردنظر را به همراه پورت آن وارد کنید.



شکل ۸- ۸۲۱ راه‌اندازی سرویس wsus

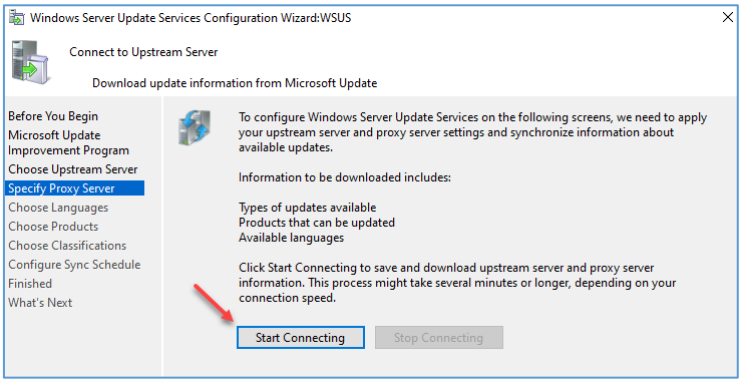
در شکل ۸-۸۲۲، اگر از سرور Proxy خاصی استفاده می‌کنید می‌توانید آدرس آن را با فعال کردن گزینه Use a Proxy… وارد کنید.



شکل ۸- ۸۲۲ راه‌اندازی سرویس wsus

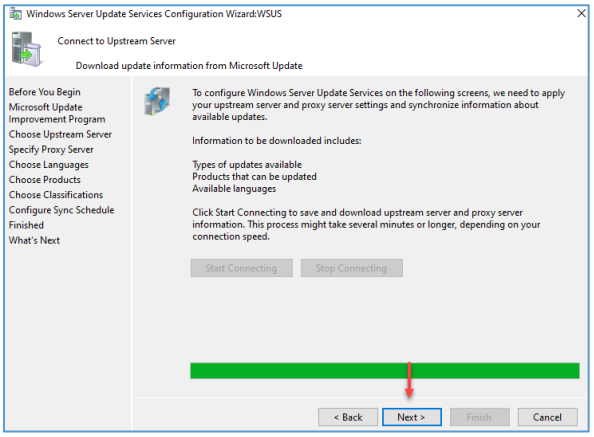
www.takbook.com

در شکل ۸-۸۲۳، برای اینکه به سرور Upstream مایکروسافت متصل بشویم حتماً باید به اینترنت متصل باشیم وگرنه اجازه ادامه کار را به شما نمی‌دهد. بر روی Start Connecting کلیک کنید تا عملیات آغاز شود.



شکل ۸- ۸۲۳ راه‌اندازی سرویس wsus

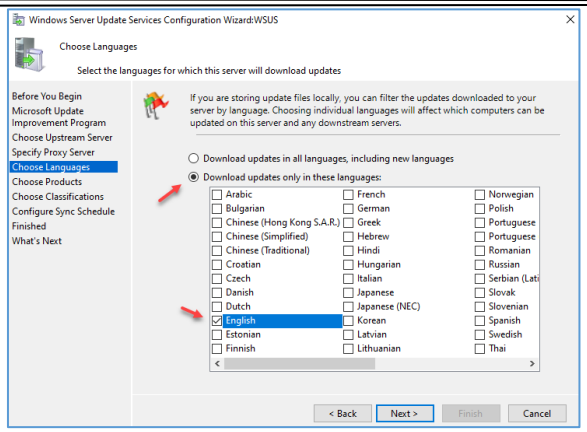
در شکل ۸-۸۲٤، با موفقیت به سرور مایکروسافت متصل شده‌ایم، برای ادامه کار بر روی Next کلیک کنید.



شکل ۸- ۸۲۴ راه‌اندازی سرویس wsus

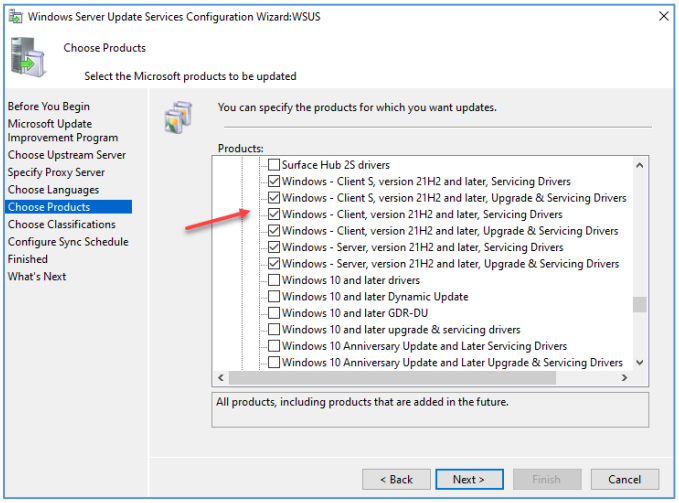
مطابق شکل ۸-۸۲۵، زبان موردنظر خود را انتخاب کنید تا آپدیت‌های موردنظر به زبان موردنظر دریافت شود.

www.takbook.com



شکل ۸- ۸۲۵ راه‌اندازی سرویس wsus

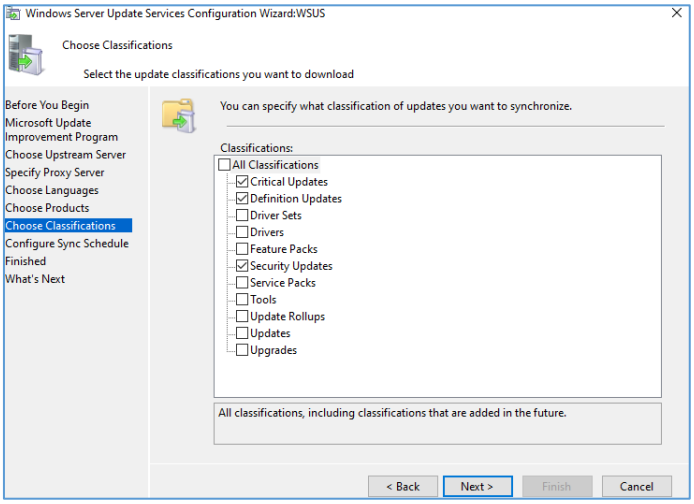
به این قسمت توجه کنید، شما باید بسته به نیاز سازمان خود محصولات موردنظر خود را از لیست انتخاب کنید، مثلاً اگر کلاینت های شبکه شما از ویندوز 8 بهره می‌برند، باید در این قسمت تیک ویندوز 8 را انتخاب کنید و یا مثلاً تیک ویندوز ۷ را انتخاب کنید.



شکل ۸- ۸۲۶ راه‌اندازی سرویس wsus

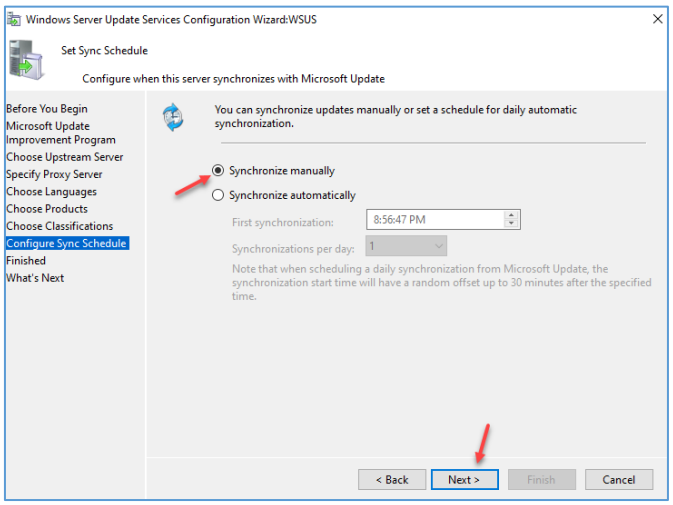
درشکل ۸-۸۲۷، نوع آپدیت خود را انتخاب کنید مثلاً اگر می‌خواهید درایورهای ویندور خود را آپدیت کنید گزینه Drivers را انتخاب کنید.

www.takbook.com



شکل ۸- ۸۲۷ راه‌اندازی سرویس wsus

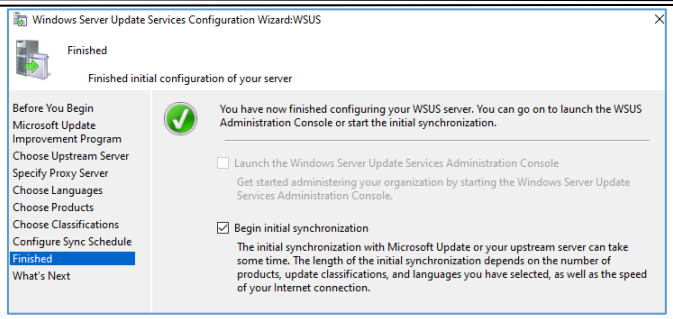
در شکل ۸-۸۲۸، باید مشخص کنید که آیا می‌خواهید همسان‌سازی یا Synchronize به صورت دستی انجام شود که با انتخاب گزینه اول این کارامکان‌پذیر است و یا با انتخاب گزینه دوم به صورت اتوماتیک در زمان مشخص‌شده انجام شود. گزینه اول را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۸۲۸ راه‌اندازی سرویس wsus

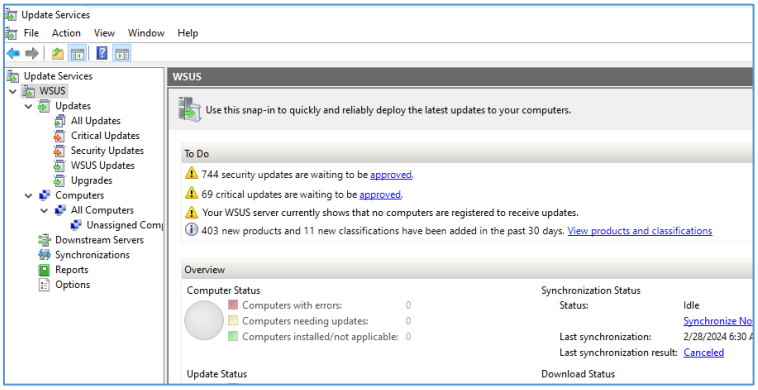
در شکل ۸-۸۲۹، با انتخاب گزینه Begin initial Synchronize کار همسان‌سازی سرور اصلی با سرور مایکروسافت برای دریافت آپدیت بعد از بستن این پنجره آغاز خواهد شد.

www.takbook.com



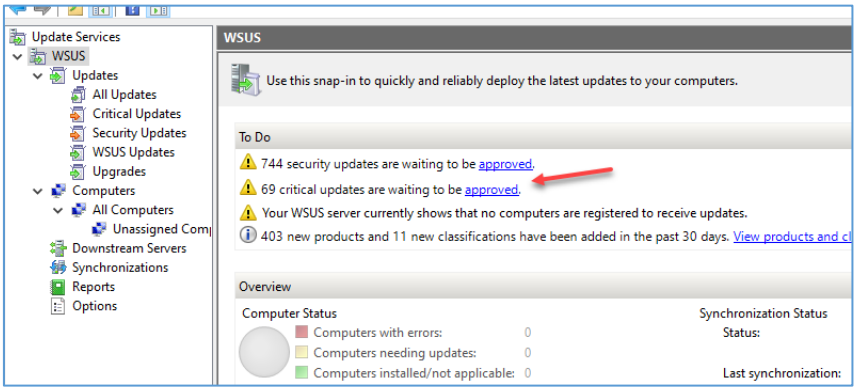
شکل ۸- ۸۲۹ راه‌اندازی سرویس wsus

در شکل ۸-۸۳۰، سرویس wsus اجرا شده است و اگر به وسط صفحه نگاه کنید کارSynchronize به صورت اتوماتیک آغاز شده است و در بالای آن تعداد ۷٤٤ Security Update و ٦۹ تا Certical Updates دریافت کرده است.



شکل ۸- ۸۳۰ راه‌اندازی سرویس wsus

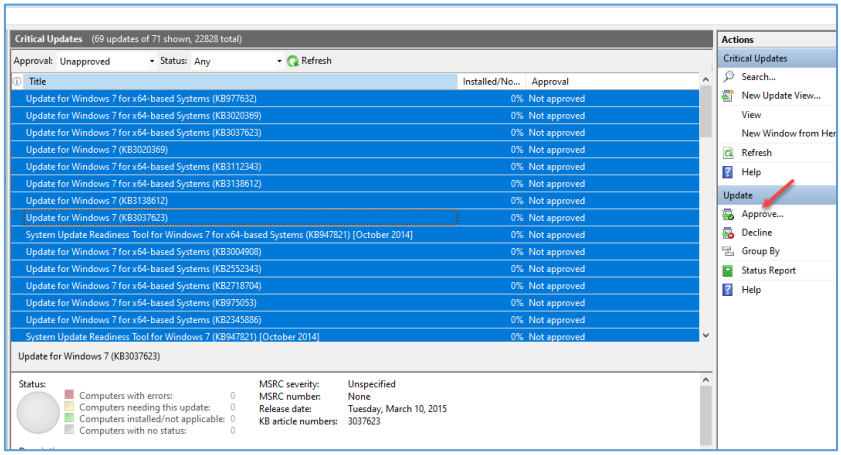
به مانند شکل ۸-۸۳۱، بعد از اتمام Synchronize برروی Approved مربوط به Certical Updates کلیک کنید.



شکل ۸- ۸۳۱ راه‌اندازی سرویس wsus

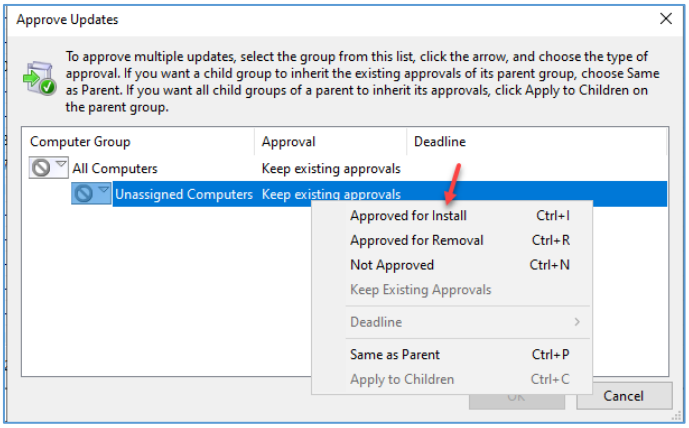
www.takbook.com

در شکل ۸-۸۳۲، آپدیت‌ها مربوط به قسمت Certical Updates را مشاهده می‌کنید، برای این که این آپدیت‌ها دانلود شوند، همه آنها را انتخاب کنید و از سمت راست بر روی Approve کلیک کنید.



شکل ۸- ۸۳۲ راه‌اندازی سرویس wsus

در شکل ۸-۸۳۳، باید بر روی هر یک از گزینه‌ها کلیک کنید تا منوی موردنظر باز شود و بعد گزینه Approved for install را انتخاب کنید. توجه داشته باشید قبل از این کار باید تنظیمات مربوط به کلاینت‌ها برای دریافت آپدیت را انجام دهیم.

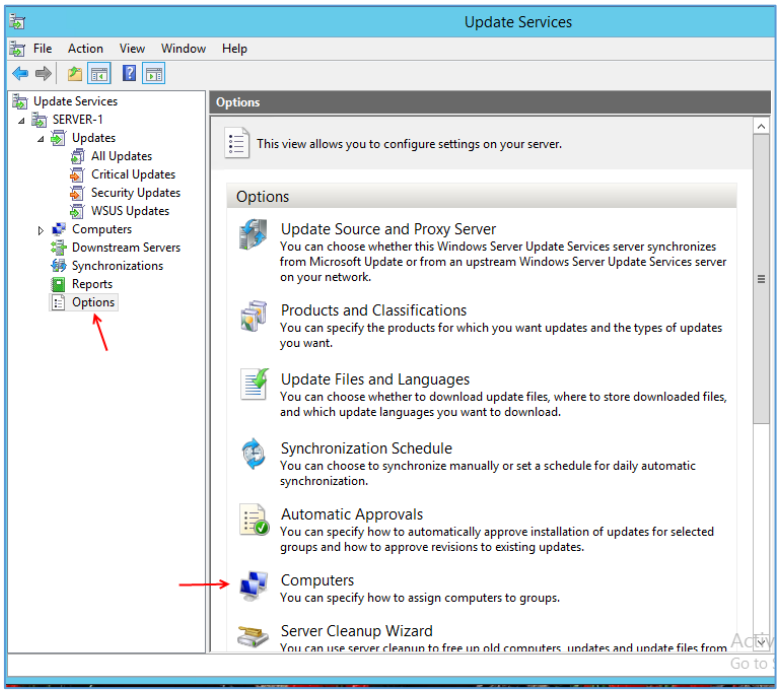


شکل ۸- ۸۳۳ راه‌اندازی سرویس wsus

برای اینکه تمام کلاینت‌ها بتوانند آپدیت را دریافت کنند لازم نیست وارد هر کلاینت بشویم و تنظیمات مربوط به آن را جداگانه انجام دهیم، فقط کافی است که وارد سرور اصلی شویم و از طریق سرویس wsus و Group Policy تنظیمات مربوط به آن را انجام دهیم تا تمام کلاینت‌های عضو شبکه موردنظر از آپدیت موردنظر استفاده کنند.

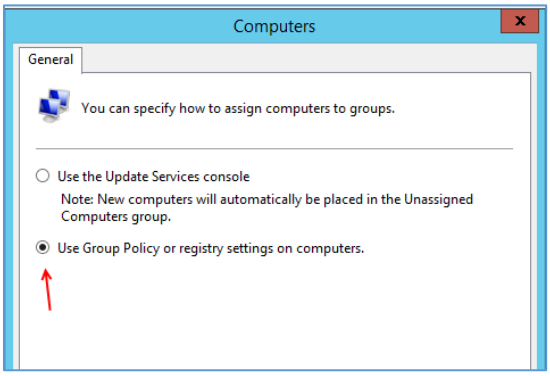
www.takbook.com

برای شروع کار به مانند شکل ۸-۸۳٤، در سرویس wsus از سمت چپ بر روی Options کلیک کنید و در صفحه باز شده بر روی Computers کلیک کنید تاصفحه‌ی مورد نظر ظاهر شود.



شکل ۸- ۸۳۴ راه‌اندازی سرویس wsus

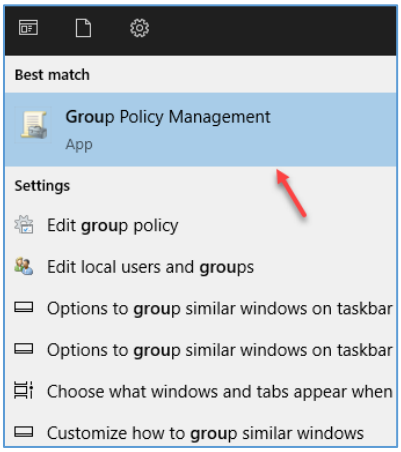
در شکل ۸-۸۳۵، گزینه Use Group Policy or registry settistry on computers را انتخاب کنید و بر روی ok کلیک کنید.



شکل ۸- ۸۳۵ راه‌اندازی سرویس wsus

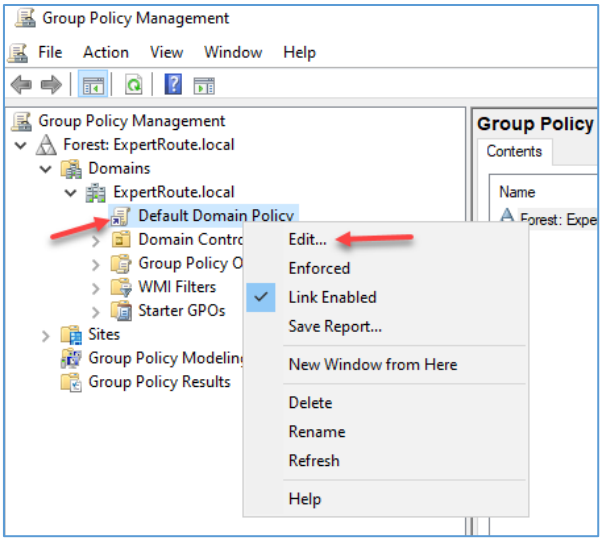
بعد از انجام کار قبل وارد سرور Active directory شوید و به مانند شکل ۸-۸۳٦، سرویس Group Policy Management را اجرا کنید.

www.takbook.com



شکل ۸- ۸۳۶ راه‌اندازی سرویس wsus

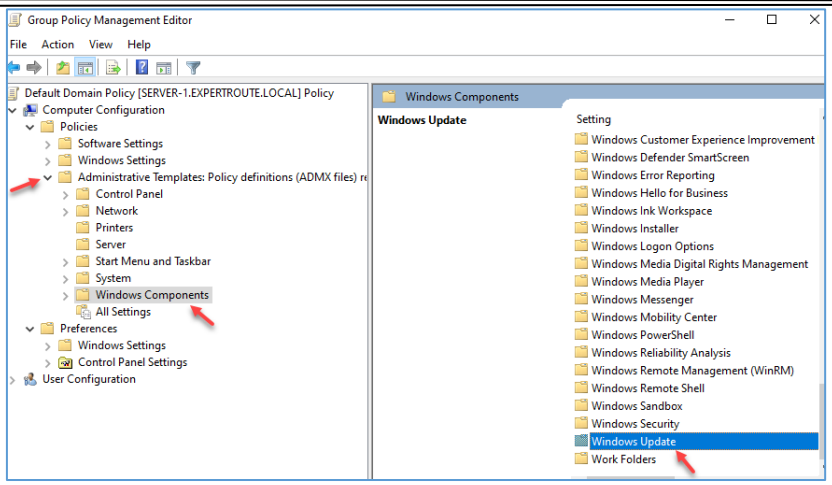
در شکل ۸-۸۳۷، از سمت چپ بر روی Default Domain Policy کلیک راست کنید و گزینه Edit را انتخاب کنید.



شکل ۸- ۸۳۷ راه‌اندازی سرویس wsus

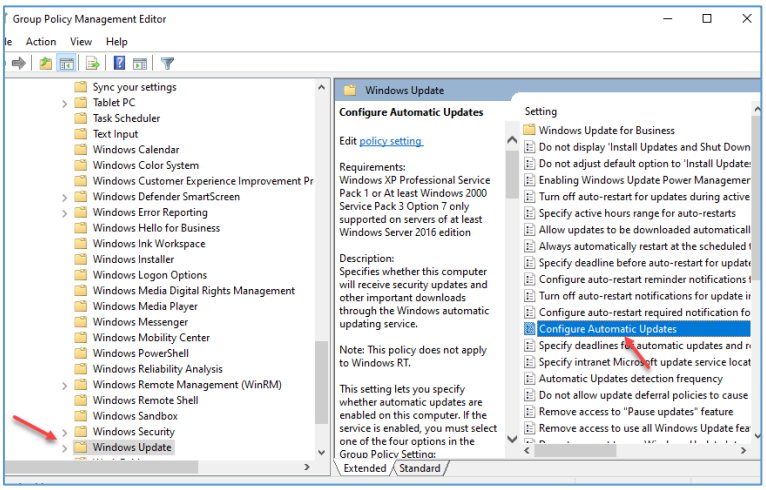
در شکل ۸-۸۳۸، از سمت چپ اول ..Administrative Templates را انتخاب و بعد Windows Components را انتخاب کنید و در لیست باز شده وارد Windows Update شوید.

www.takbook.com



شکل ۸- ۸۳۸ راه‌اندازی سرویس wsus

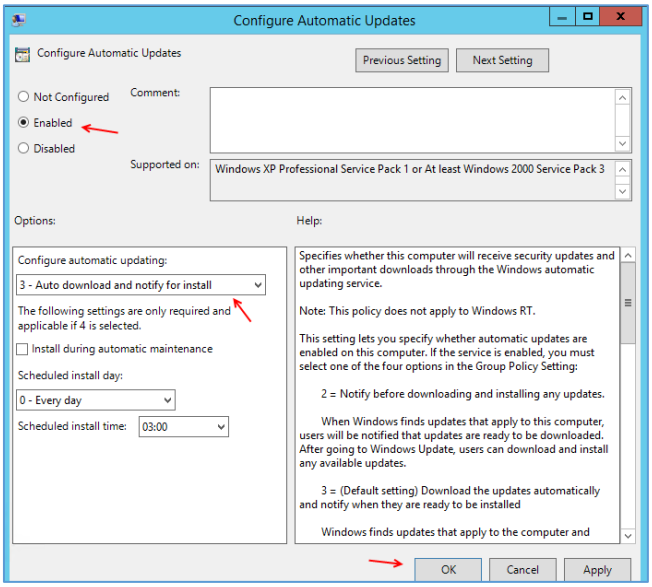
در شکل ۸-۸۳۹، بر روی گزینه Configure Automatic Update دو بار کلیک کنید تا شکل بعد ظاهر شود.



شکل ۸- ۸۳۹ راه‌اندازی سرویس wsus

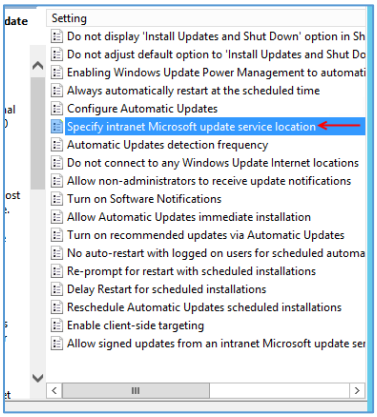
در شکل ۸-۸٤۰، گزینه‌ی Enabled را انتخاب کنید و در قسمت Configure automatic updating گزینه سوم را انتخاب کنید تا آپدیت به صورت اتوماتیک دانلود و نصب شود البته می‌توانید با انتخاب گزینه دوم برای آن زمان بندی هم تعریف کنید.

www.takbook.com



شکل ۸- ۸۴۰ راه‌اندازی سرویس wsus

بعد انجام کار قبل دوباره در صفحه‌ی شکل ۸-۸۴۱، بر روی Specifies intranet Microsoft… دو بار کلیک کنید.



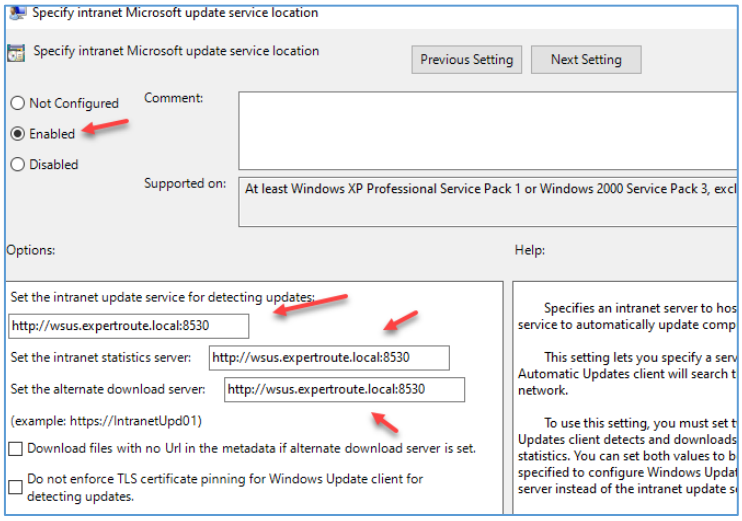
شکل ۸- ۸۴۱ راه‌اندازی سرویس wsus

در شکل ۸-۸۴۲، باید آدرس سرور داخلی خود را به کلاینت‌ها اعلام کنیم تا کلاینت ها بتوانند از طریق این آدرس آپدیت خود را دریافت کنند، برای این کار بر روی Enable کلیک کنید و در دو قسمت مشخص‌شده آدرس زیر را وارد کنید:

http://server-1.srv-1.com:8530

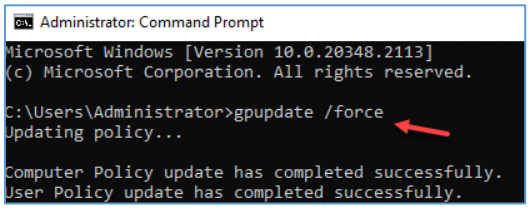
www.takbook.com

در این آدرس باید به جای Server-1 نام سرور خود را وارد کنید و به جای Srv-1.com نام دومین خود را وارد کنید و پورت 8530 هم برای سرویس WSUS ثابت می‌باشد. بعد از این کار بر روی ok کلیک کنید.



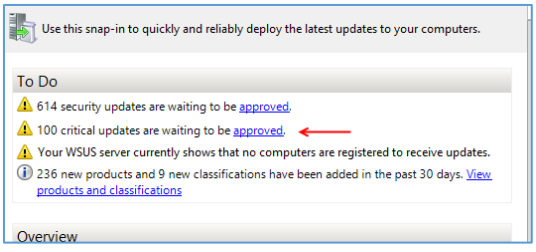
شکل ۸- ۸۴۲ راه‌اندازی سرویس wsus

بعد از اتمام کار به مانند شکل ۸-۸۴۳، وارد CMD شوید و دستور gpupdate /force را اجرا کنید تا Group Policy بدون نیاز به Restart آپدیت شود.



شکل ۸- ۸۴۳ راه‌اندازی سرویس wsus

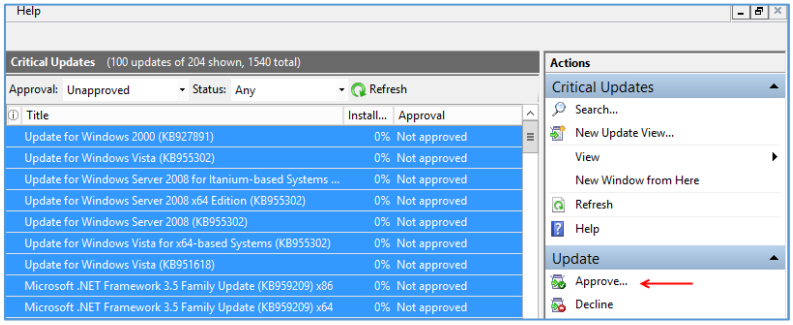
بعد از انجام عملیات قبل باید به مانند شکل ۸-۸۴۴، وارد سرویس WSUS شویم و از قسمت To do یکی از آپدیت‌ها را انتخاب کنید



شکل ۸- ۸۴۴ راه‌اندازی سرویس wsus

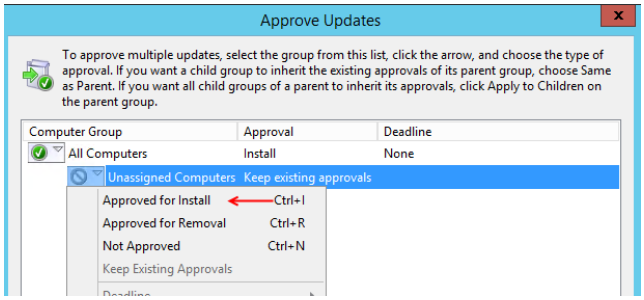
www.takbook.com

در شکل ۸-۸٤٥، به مانند قبل باید آپدیت‌هایی که از سایت مایکروسافت دریافت شده را انتخاب کنید و بعد بر روی Approve کلیک کنید.



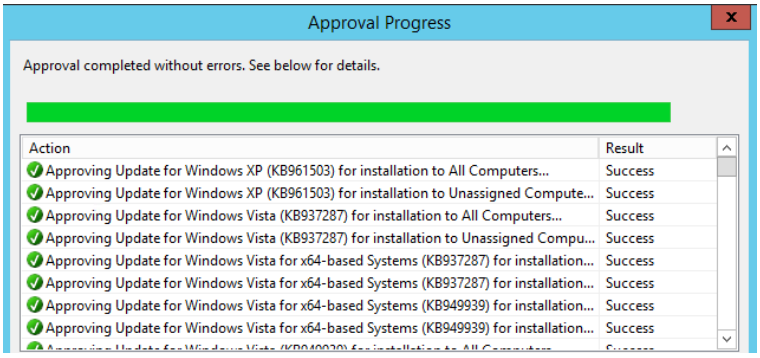
شکل ۸- ۸۴۵ راه‌اندازی سرویس wsus

در این قسمت به مانند شکل ۸-۸٤٦، بر روی هر یک از قسمت‌ها کلیک کنید تا منوی موردنظر باز شود، در این منو گزینه Approved For install را انتخاب کنید.



شکل ۸- ۸۴۶ راه‌اندازی سرویس wsus

همان‌طور که در شکل ۸-۸٤۷، مشاهده می‌کنید آپدیت‌های موردنظر از سرور مایکروسافت دانلود شده و درون کامپیوتر سرور قرار گرفته و کلاینت‌ها با استفاده از آدرس سرور می‌توانند این آپدیت‌ها را دریافت کنند.



شکل ۸- ۸۴۷ راه‌اندازی سرویس wsus

www.takbook.com

۸-۳-۲۳ سرویس Windows Deployment

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

ویژگی‌های کلیدی WDS

پیاده‌سازی از راه دور (Remote Installation): دستگاه‌ها می‌توانند سیستم‌عامل را مستقیماً از سرور WDS دریافت کنند.

پشتیبانی از بوت PXE: دستگاه‌ها با استفاده از شبکه و قابلیت Preboot Execution Environment (PXE) می‌توانند به سرور WDS متصل شوند.

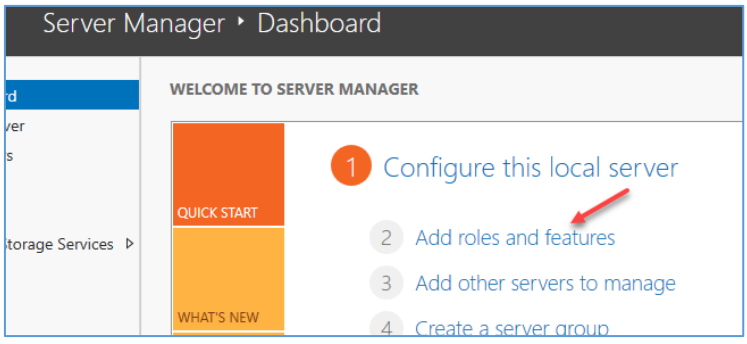
ایجاد و مدیریت تصاویر (Images): امکان ساخت و مدیریت انواع تصاویر سیستم‌عامل ویندوز (Boot و Install Images) وجود دارد.

سفارشی‌سازی: شما می‌توانید Images سیستم‌عامل را با نرم‌افزارها، تنظیمات و درایورهای خاص سفارشی‌سازی کنید.

ادغام با Active Directory: در صورت وجود دامین، می‌توانید WDS را با Active Directory برای کنترل بهتر دستگاه‌ها ادغام کنید.

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

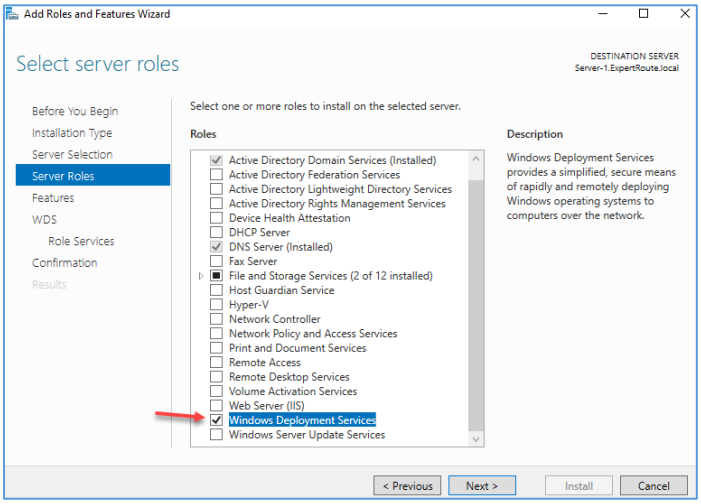
برای انجام این کار نیاز به یک سرور با ویندوز سرور ۲۰۲۵ دارید که باید عضو دومین باشد، بعد از اینکه سرور مورد نظر را عضو دومین کردید برای شروع به مانند شکل ۸-۸٤۸، وارد Server Manager شوید و بر روی Add Roles and Feature کلیک کنید.



شکل ۸- ۸۴۸ نصب و راه‌اندازی سرویس wds

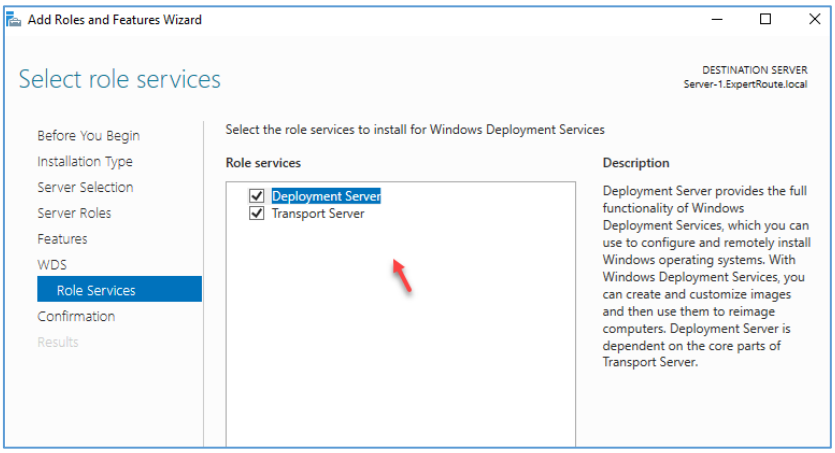
به مانند شکل ۸-۸٤۹، از سمت چپ بر روی Server Roles کلیک کنید و از لیست Roles گزینه Windows Deployment Services را انتخاب کنید و آن را نصب کنید.

www.takbook.com



شکل ۸- ۸۴۹ نصب و راه‌اندازی سرویس wds

در شکل ۸-۸۵۰، فقط بر روی Next کلیک کنید.

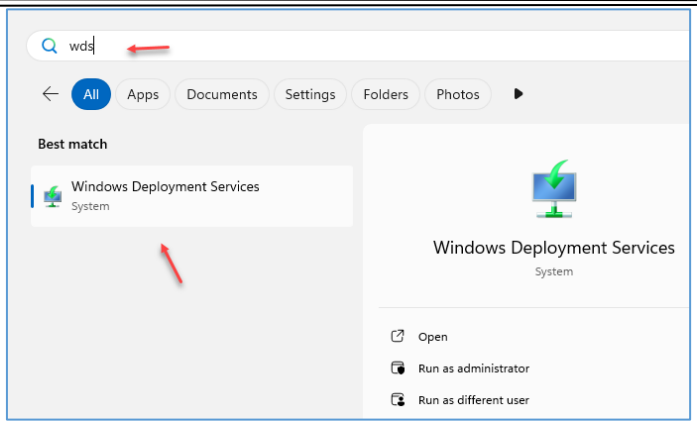


شکل ۸- ۸۵۰ نصب و راه‌اندازی سرویس wds

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

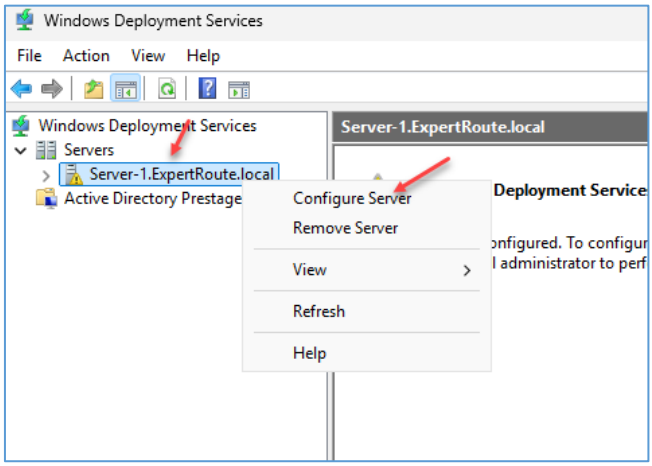
بعد از نصب به مانند شکل ۸-۸۵۱، وارد Search شوید و کلمه wds را وارد و بعد سرویس موردنظر را اجرا کنید، سعی کنید با کلیک راست کردن روی سرویس موردنظر آن را وارد Start و یا وارد Taskbar کنید.

www.takbook.com



شکل ۸- ۸۵۱

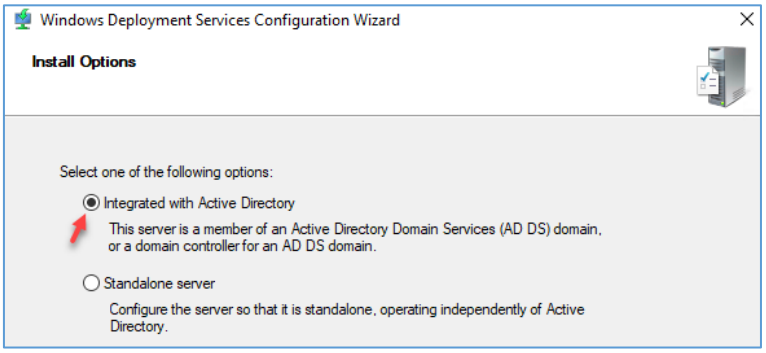
بعد از ورود به سرویس موردنظر به مانند شکل ۸-۸۵۲، وارد قسمت Servers شوید و بر روی نام سرور خود کلیک راست کنید و گزینه Configure Server را انتخاب کنید تا تنظیمات مربوط به این سرویس را انجام دهیم.



شکل ۸- ۸۵۲ نصب و راه‌اندازی سرویس wds

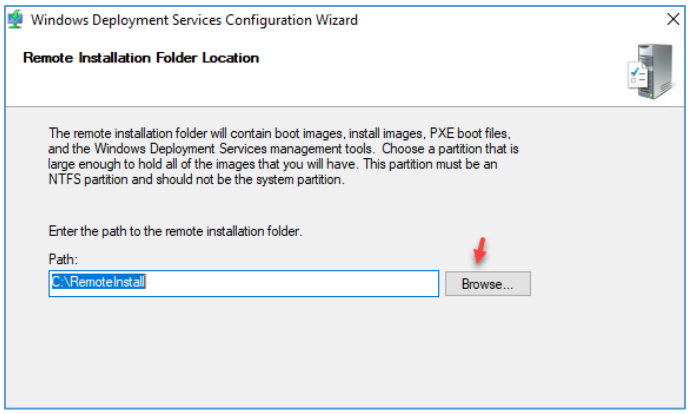
در شکل ۸-۸۵۳، گزینه Integrated with Active Directory را انتخاب کنید تا سرویس موردنظر با Active خود را هماهنگ کند.

www.takbook.com



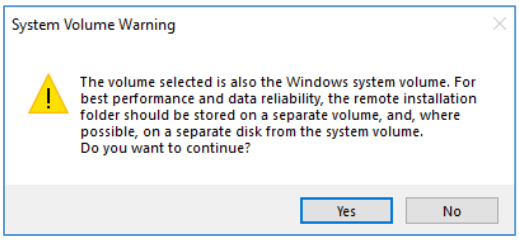
شکل ۸- ۸۵۳ نصب و راه‌اندازی سرویس wds

در شکل ۸-۸۵٤، باید آدرسی را وارد کنید تا فایل‌های مربوط به سیستم‌عامل در آدرس موردنظر کپی شود تا کلاینت‌ها بتوانند از این آدرس استفاده کنند، البته این آدرس Share خواهد شد.



شکل ۸- ۸۵۴ نصب و راه‌اندازی سرویس wds

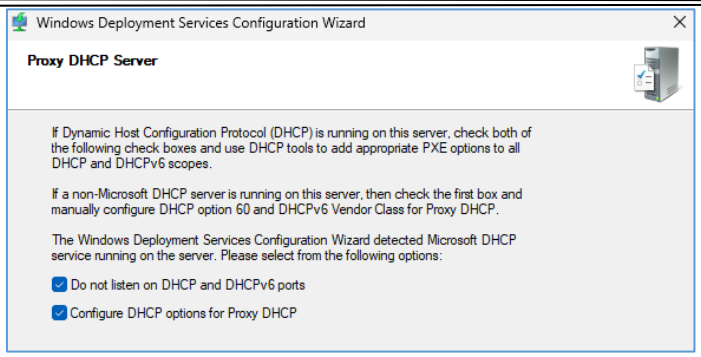
بعد از کلیک بر روی Next پنجره‌ای شکل ۸-۸۵۵، باز می‌شود که به این نکته اشاره دارد که درایوی که انتخاب کردید درایو System می‌باشد یعنی ویندوز شما روی آن نصب شده است، بهتر است درایو دیگری را انتخاب کنید تا امنیت اطلاعات و کیفیت افزایش پیدا کند.



شکل ۸- ۸۵۵ نصب و راه‌اندازی سرویس wds

در شکل ۸-۸۵٦، بر روی Next کلیک کنید تا اطلاعات و تنظیمات مورد نظر اعمال شود.

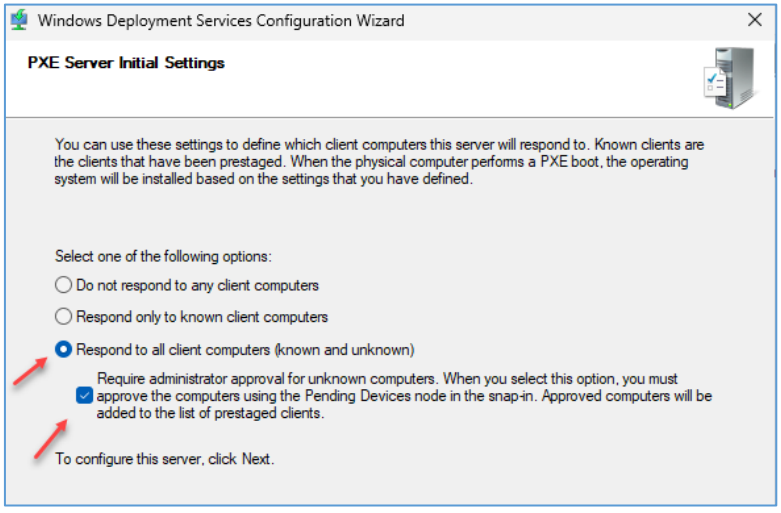
www.takbook.com



شکل ۸- ۸۵۶ نصب و راه‌اندازی سرویس wds

در شکل ۸-۸۵۷، سه گزینه را مشاهده می‌کنید که گزینه‌ی Do not respond to any client computers، در این حالت، سرور WDS به هیچ درخواستی از کلاینت‌ها پاسخ نمی‌دهد،گزینه‌ی Respond only to known client computers ، سرور WDS فقط به کلاینت‌هایی که قبلاً در Active Directory ثبت شده‌اند (Managed Devices) پاسخ می‌دهد و کلاینت‌هایی که شناخته‌شده نیستند، نادیده گرفته می‌شوند

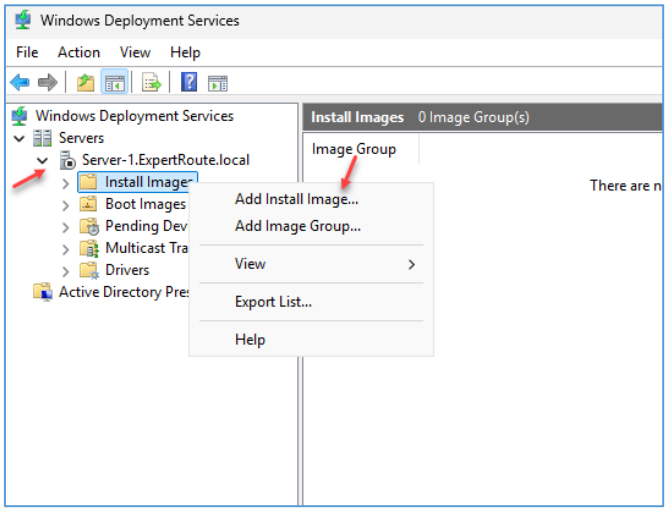
Respond to all client computers، سرور WDS به همه کلاینت‌ها (شناخته‌شده و ناشناخته) پاسخ می‌دهد که شما هم باید همین گزینه را انتخاب کنید، توجه داشته باشید اگر تیک گزینه‌ی For unknown clients, require administrator approval، را انتخاب کنید، زمانی که این گزینه فعال است، کلاینت‌های ناشناخته ابتدا باید توسط مدیر در Pending Devices تأیید شوند، مدیر می‌تواند در کنسول WDS درخواست‌های این کلاینت‌ها را مشاهده کند و تصمیم بگیرد که به آنها اجازه بوت داده شود یا خیر.



شکل ۸- ۸۵۷ نصب و راه‌اندازی سرویس wds

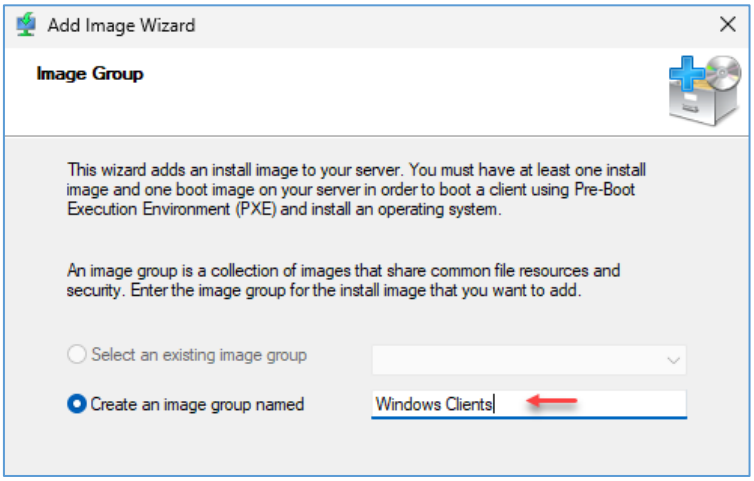
www.takbook.com

در ادامه کار شکل ۸-۸۵۸، را مشاهده می‌کنید که هنوز سرویس WDS فعال نشده است و بهتر است قبل از فعال شدن تنظیمات دیگر آن را تکمیل کنیم، برای شروع بر روی Install image کلیک راست کنیدو گزینه‌ی Add install Image را انتخاب کنید.



شکل ۸- ۸۵۸ نصب و راه‌اندازی سرویس wds

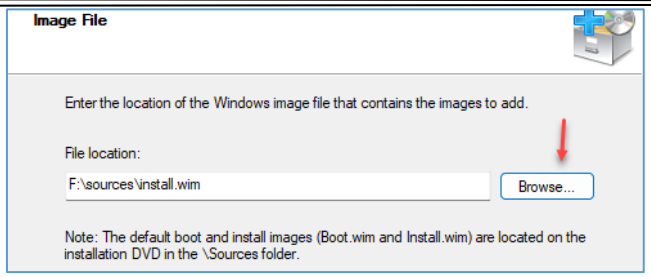
در شکل ۸-۸۵۹، باید برای شروع یک گروه ایجاد کنید، پس یک نام به دلخواه خود وارد کنید.



شکل ۸- ۸۵۹ نصب و راه‌اندازی سرویس wds

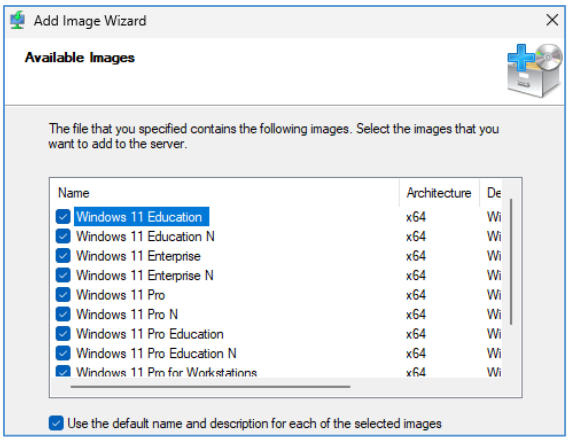
اگر به نوشته‌ی شکل ۸-۸۶۰، دقت کنید به این موضوع اشاره کرده که باید دو فایل Install.wim و Boot.wim را به آن معرفی کنید، برای این کار بر روی Browse کلیک کنید و فایل مربوطه را انتخاب کنید.

www.takbook.com



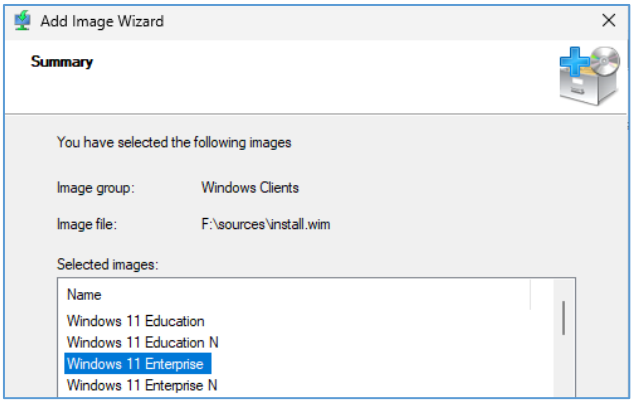
شکل ۸- ۸۶۰ نصب و راه‌اندازی سرویس wds

در شکل ۸-۸۶۱، باید ورژن‌های موجود در این Image که مربوط به ویندوز 11 است را انتخاب کنید که ما همهی گزینه‌ها را انتخاب می‌کنیم.



شکل ۸- ۸۶۱ نصب و راه‌اندازی سرویس wds

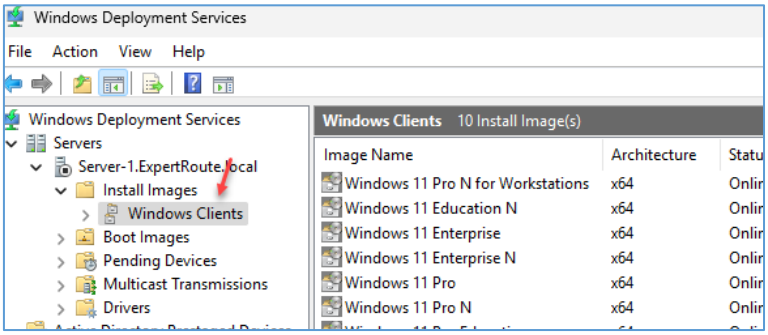
در شکل ۸-۸۶۲، بر روی Next کلیک کنید.



شکل ۸- ۸۶۲ نصب و راه‌اندازی سرویس wds

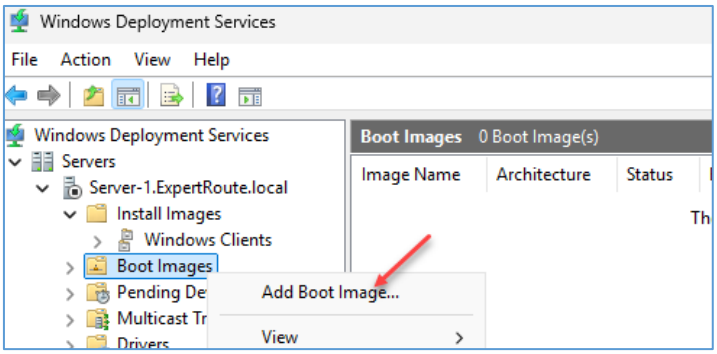
همان‌طور که در شکل ۸-۸۶۳، مشاهده می‌کنید گروه مورد نظر ایجاد شده است.

www.takbook.com



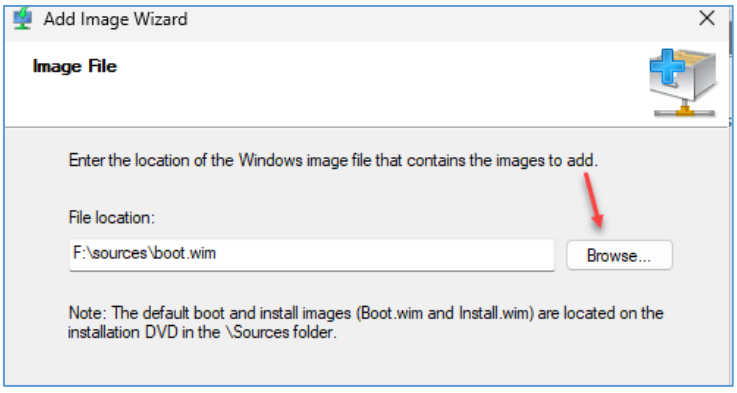
شکل ۸- ۸۶۳ نصب و راه‌اندازی سرویس wds

در ادامه کار به مانند شکل ۸-۸٦٤، باید فایل Boot را هم به سرویس معرفی کنیم برا این کار بر روی Boot Images کلیک راست کنید و گزینه‌ی Add Boot Image را انتخاب کنید.



شکل ۸- ۸۶۴ نصب و راه‌اندازی سرویس wds

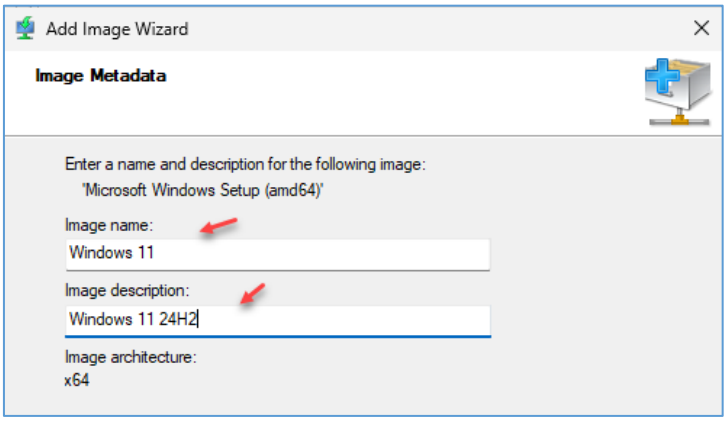
در شکل ۸-۸٦٥، باید فایل Boot را به سرویس معرفی کنید.



شکل ۸- ۸۶۵ نصب و راه‌اندازی سرویس wds

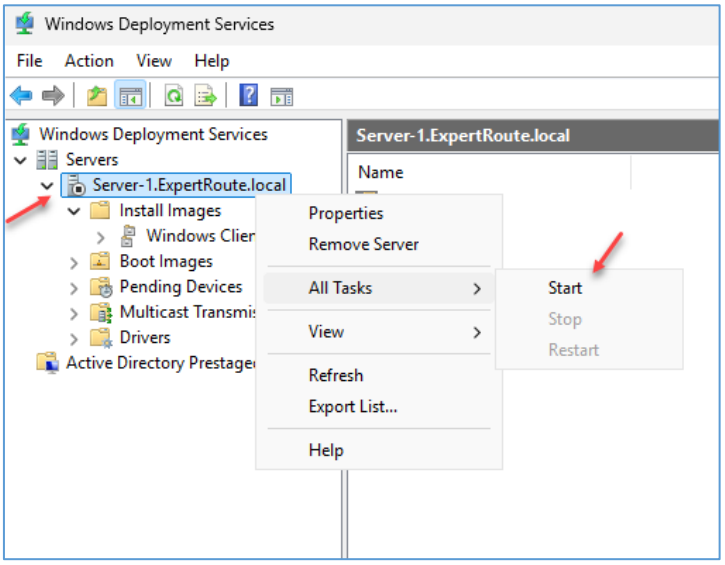
www.takbook.com

در شکل ۸-۸۶۶، نام و توضیحات مربوط به فایل Boot خود را وارد کنید، بر روی Next کلیک کنید تا فایل مورد نظر به سرویس اضافه شود.



شکل ۸- ۸۶۶ نصب و راه‌اندازی سرویس wds

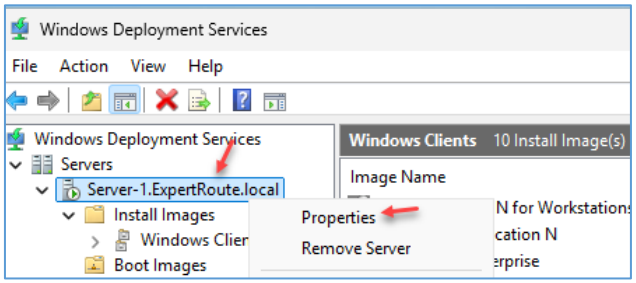
بعد از ایجاد هر دو Image موردنظر به مانند شکل ۸-۸۶۷، بر روی سرور اصلی کلیک راست کنید و از قسمت All Tasks گزینه Start را انتخاب کنید تا سرویس موردنظر فعال شود.



شکل ۸- ۸۶۷ نصب و راه‌اندازی سرویس wds

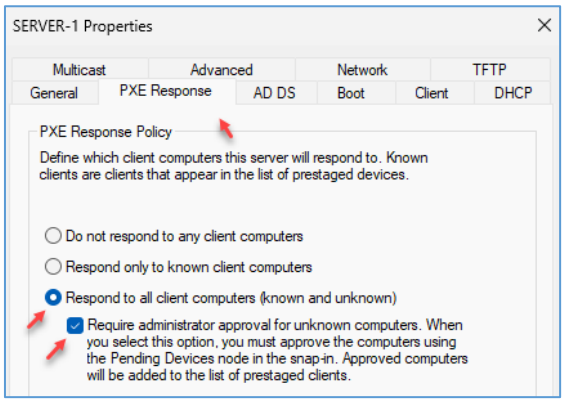
بعد از اینکه سرویس را Start کردیم به مانند شکل ۸-۸۶۸، بر روی نام سرور کلیک راست می‌کنیم و گزینه Properties را انتخاب می‌کنیم.

www.takbook.com



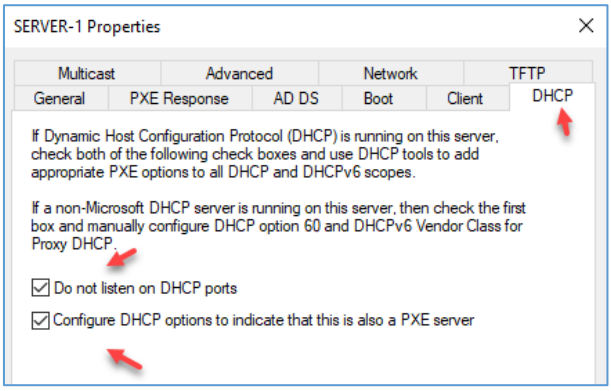
شکل ۸- ۸۶۸ نصب و راه‌اندازی سرویس wds

در شکل ۸-۸۶۹، وارد تب PXE Response شوید و گزینه Respond to all Client Computer را انتخاب کنید تا کلاینت‌ها زمانی که روشن می‌شوند از طریق سرویس DHCP بتوانند به سرویس Deployment متصل شوند و ویندوز را اجرا کنند، توجه داشته باشید برای اینکه جلوی افراد مهاجم را بگیریم بهتر است تیک گزینه‌ی Require administrator… را انتخاب کنید تا با تایید مدیر کار نصب انجام شود.



شکل ۸- ۸۶۹ نصب و راه‌اندازی سرویس wds

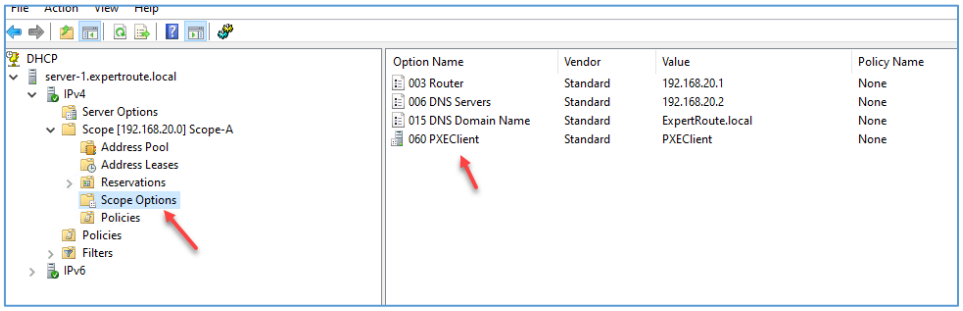
در ادامه کار به مانند شکل ۸-۸۷۰، وارد تب DHCP شوید و تیک دو گزینه‌ی مورد نظر را انتخاب کنید:



شکل ۸- ۸۷۰ نصب و راه‌اندازی سرویس wds

www.takbook.com

بعد از اتمام کار به سرویس DHCP نگاهی می‌اندازیم، به مانند شکل ۸-۸۷۱، اگر به قسمت Scope Options مراجعه کنید، گزینه‌ای را با نام PXEClient ایجاد شده است که مربوط به سرویس Deployment می‌باشد.

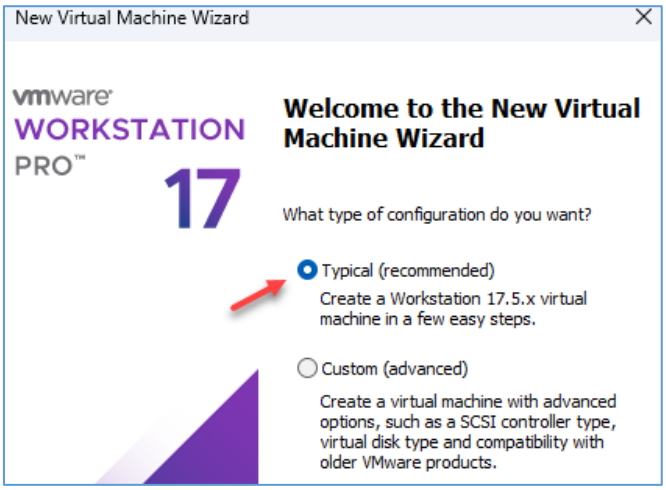


شکل ۸- ۸۷۱ نصب و راه‌اندازی سرویس wds

نکته مهم: برای استفاده از قابلیت سرویس Deployment حتماً باید سرویس DHCP، Active Directory و DNS را قبل از آن نصب کنید.

برای اینکه از این سرویس استفاده کنیم باید قابلیت Boot تحت شبکه را فعال کنید، در سیستم های واقعی برای متصل شدن به سرویس DHCP باید وارد منوی Boot شوید و Network را انتخاب کنید تا بتوانید به شبکه متصل شوید.

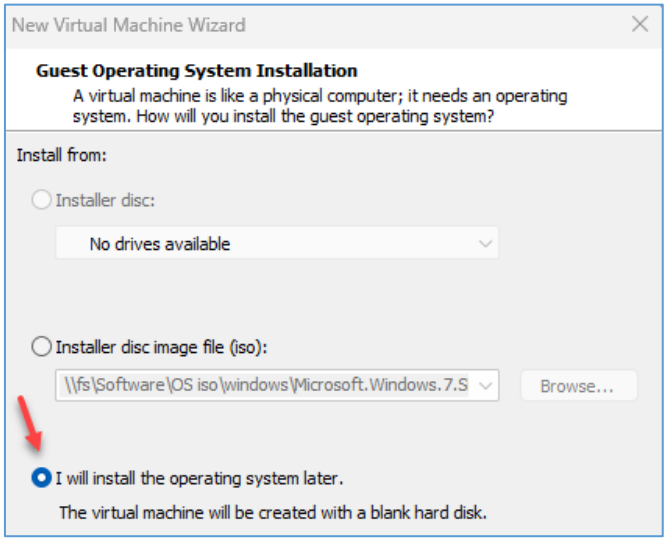
اما در این قسمت می‌خواهیم از یک ماشین مجازی استفاده کنیم، برای استفاده از ماشین مجازی وارد Vmware شوید و یک ماشین مجازی جدید ایجاد کنید به مانند شکل ۸-۸۷۲، گزینه‌ی Typical را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸- ۸۷۲ راه‌اندازی ماشین مجازی برای wds

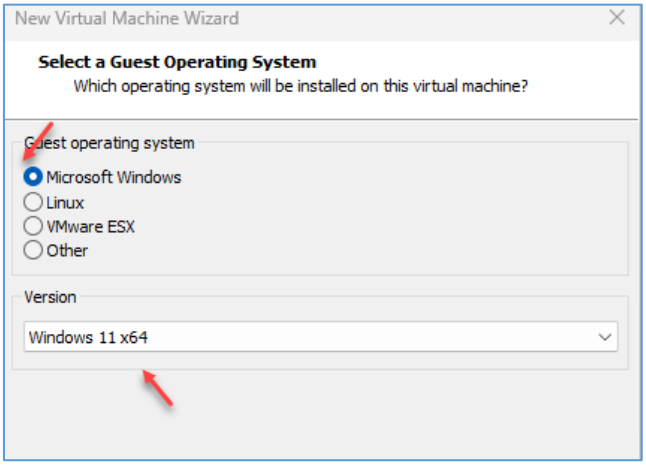
www.takbook.com

در شکل ۸-۸۷۳، برای انتخاب DVD مربوط به سیستم‌عامل نیازی به انتخاب نیست و گزینه‌ی آخر را انتخاب کنید.



شکل ۸- ۸۷۳ راه‌اندازی ماشین مجازی برای wds

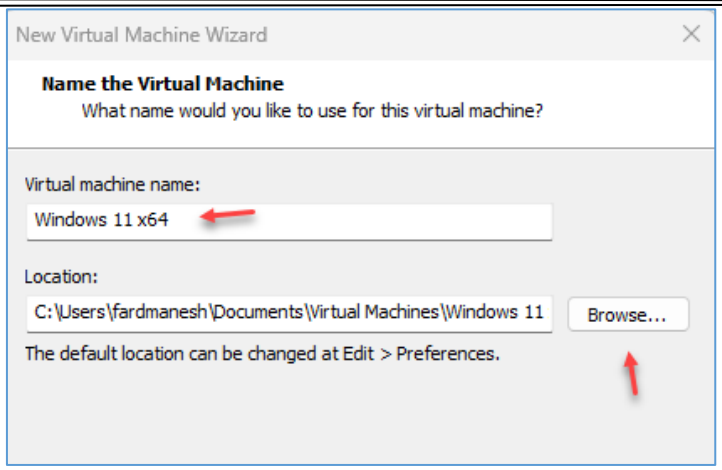
در شکل ۸-۸۷۴، باید ورژن ویندوز خود را انتخاب کنید.



شکل ۸- ۸۷۴ راه‌اندازی ماشین مجازی برای wds

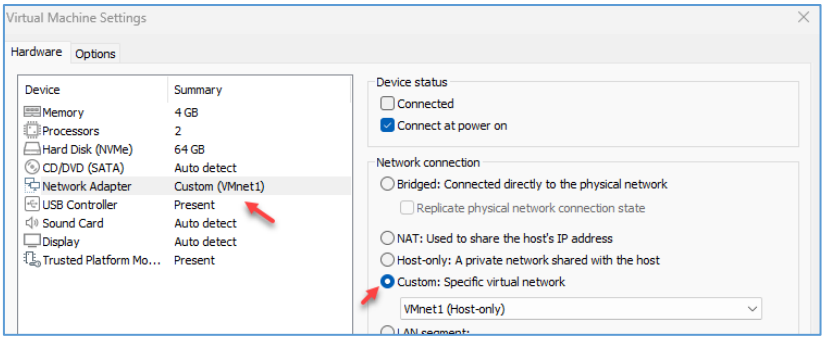
به مانند شکل ۸-۸۷۵، یک اسم برای آن انتخاب و مسیر را مشخص کنید.

www.takbook.com



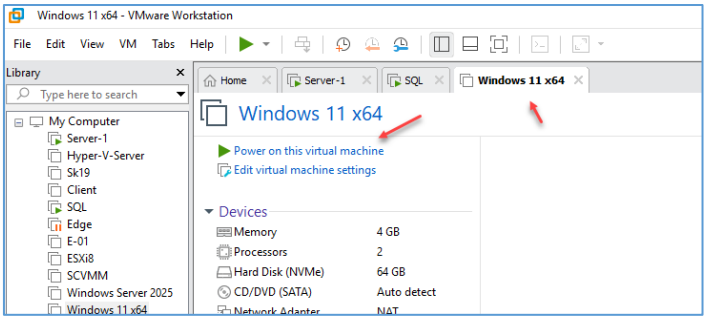
شکل ۸- ۸۷۵ راه‌اندازی ماشین مجازی برای wds

مهمترین چیز بعد از ایجاد ماشین مجازی این است که کارت شبکه‌ی آن را به درستی انتخاب کنید تا به کارت شبکه‌ی سرور متصل باشد که این موضوع را در شکل ۸-۸۷۷، مشاهده می‌کنید.



شکل ۸- ۸۷۶ راه‌اندازی ماشین مجازی برای wds

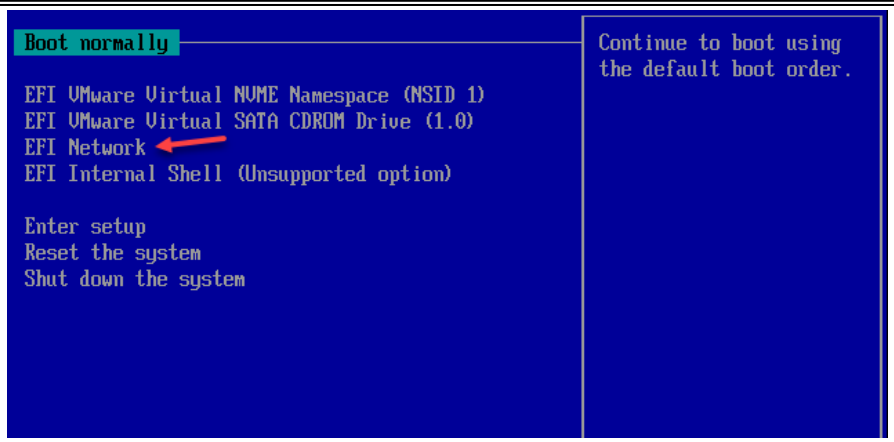
به مانند شکل ۸-۸۷۷، بعد از ایجاد ماشین مجازی آن را روشن کنید.



شکل ۸- ۸۷۷ راه‌اندازی ماشین مجازی برای wds

بعد از روشن کردن ماشین مورد نظر به مانند شکل ۸-۸۷۸، باید گزینه‌ی EFI Network را انتخاب کنید.

www.takbook.com



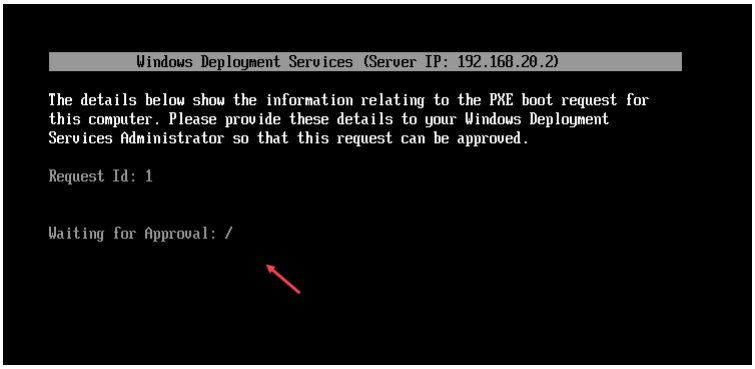
شکل ۸- ۸۷۸ راه‌اندازی ماشین مجازی برای wds

همان‌طور که در شکل ۸-۸۷۹، مشاهده می‌کنید فایل سرور مورد نظر پیدا شده است یکی از IPها مربوط به همین کلاینت است و آدرس دیگر مربوط به سرور است که برای ورود به آن باید Enter را فشار دهید.



شکل ۸- ۸۷۹ راه‌اندازی ماشین مجازی برای wds

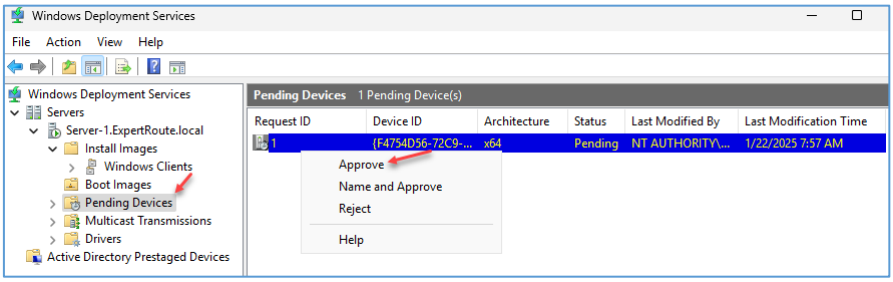
اگر به شکل ۸-۸۸۰، دقت کنید بعد از اینکه کلاینت به سرور متصل شد، درخواست تایید برای مدیر سیستم ارسال می‌شود و تا تایید کردن مدیر، کلاینت کاری نمی‌تواند انجام دهد.



شکل ۸- ۸۸۰ راه‌اندازی ماشین مجازی برای wds

www.takbook.com

برای اینکه درخواست کلاینت را تایید کنیم باید به مانند شکل ۸-۸۸۱، بر روی Pending Devices کلیک کنید که یک درخواست را مشاهده میکنید باید بر روی آن کلیک راست کنید و گزینه‌ی Approve را انتخاب کنید.



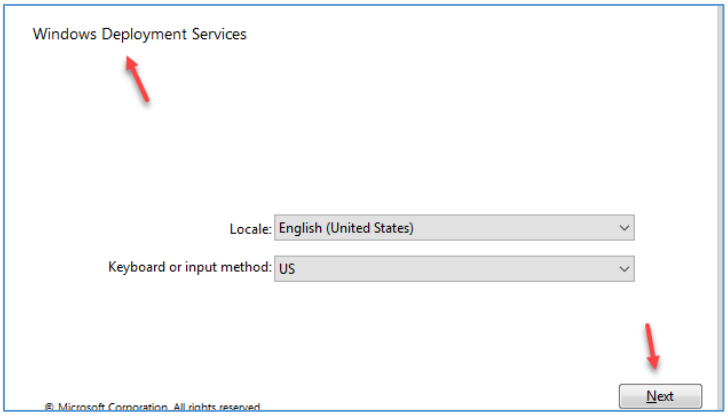
شکل ۸- ۸۸۱ راه‌اندازی ماشین مجازی برای wds

همان‌طور که در شکل ۸-۸۸۲، مشاهده می‌کنید فایل مورد نظر از طریق شبکه و از سروری که روی آن سرویس Deployment را فعال کردیم در حال لود شدن است.



شکل ۸- ۸۸۲ راه‌اندازی ماشین مجازی برای wds

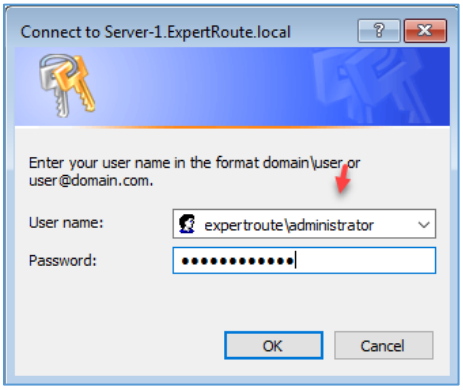
همان‌طور که شکل ۸-۸۸۳، مشاهده می‌کنید پنجره نصب ویندوز ظاهر شده است که نشان می‌دهد این ویندوز ازطریق Windows Deployment Services فعال شده است برای ادامه بر روی Next کلیک کنید.



شکل ۸- ۸۸۳ راه‌اندازی ماشین مجازی برای wds

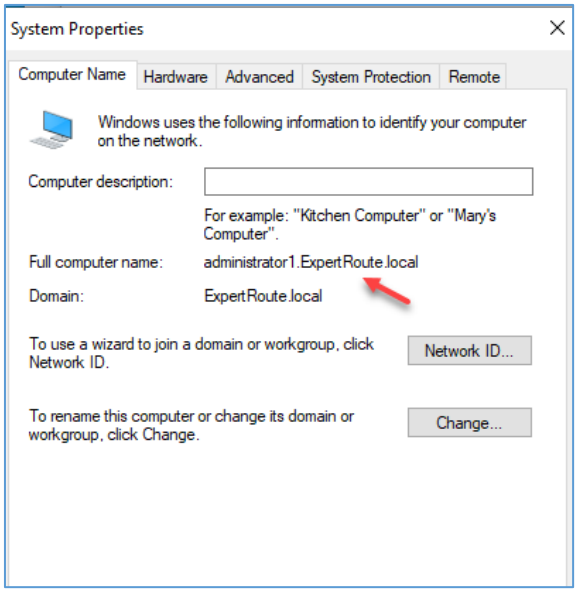
www.takbook.com

در شکل ۸-۸۸٤، باید نام کاربری و رمز عبور مدیر شبکه را وارد کنیم، یعنی مدیر سرور اصلی و بعد بر روی ok کلیک کنید و بعد از آن ورژن ویندوز را انتخاب و کار نصب را انجام دهید.



شکل ۸- ۸۸۴ راه‌اندازی ماشین مجازی برای wds

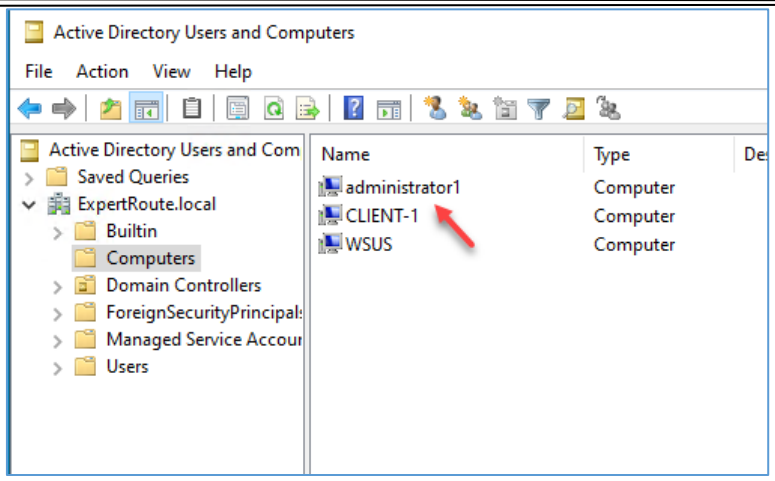
نکته: تمام کلاینت‌هایی که به این صورت ویندوز روی آنها نصب می‌شود به صورت خودکار عضو دومین موردنظر می‌شوند و دیگر لازم نیست به خودتان زحمت بدید و بر روی تک تک کلاینت‌ها عملیات Join به دومین را انجام دهید، این موضوع را در شکل ۸-۸۸۵، مشاهده می‌کنید.



شکل ۸- ۸۸۵ راه‌اندازی ماشین مجازی برای wds

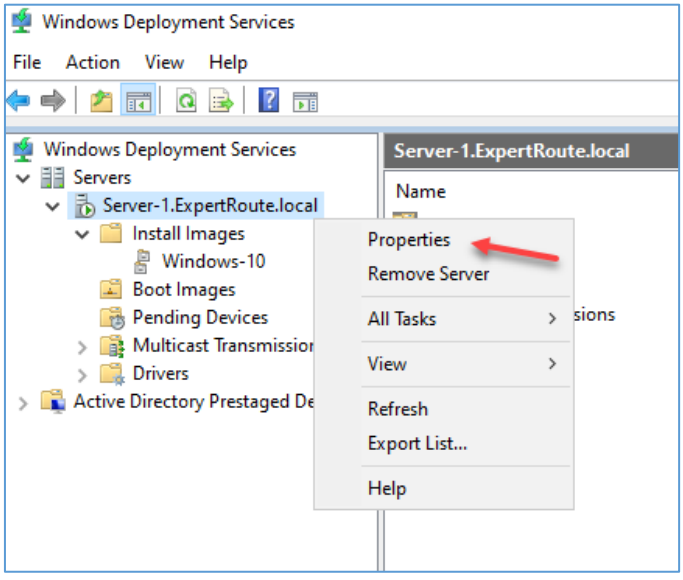
به مانند شکل ۸-۸۸٦، اگر وارد Active directory هم شوید در قسمت Computers می‌توانید نام کلاینت جدید که عضو دومین شده است را مشاهده کنید.

www.takbook.com



شکل ۸- ۸۸۶ بررسی سرویس Active

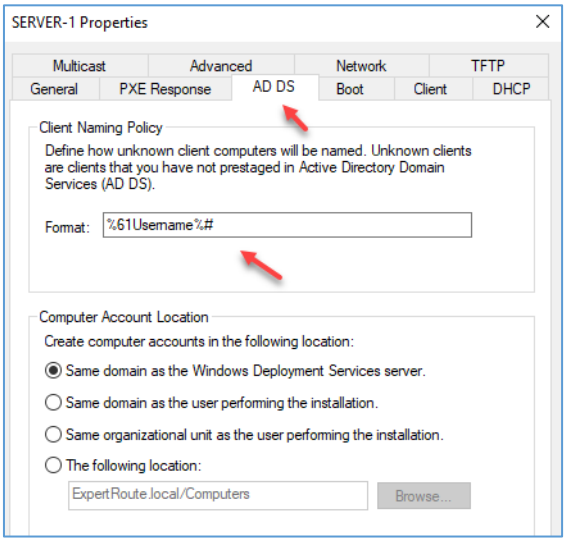
اگر به شکل ۸-۸۸۶، توجه کنید نام کامپیوتر Administrator1 در نظر گرفته شده است که این اسم از یک قالب پیروی می‌کند برای اینکه این قالب را مشاهده کنید به مانند شکل ۸-۸۸۷، بر روی نام سرور کلیک راست و وارد Properties شوید.



شکل ۸- ۸۸۷ تغییر قالب اسمی

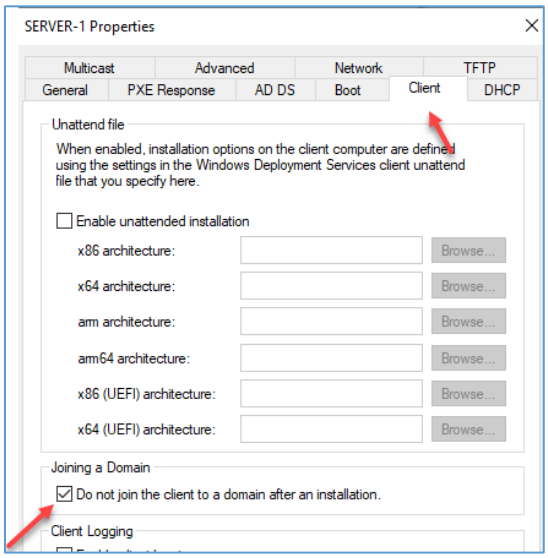
در ادامه به مانند شکل ۸-۸۸۸، وارد تب AD DS شوید، همان‌طور که مشاهده می‌کنید فرمت نوشته شده است و یک عدد هم به نام کاربری مورد نظر اضافه خواهد شد یعنی هر بار این عدد تغییر خواهد کرد یعنی از یک تا ۹۹۹ قابل تغییر است.

www.takbook.com



شکل ۸- ۸۸۸ تغییرات در سرویس wds

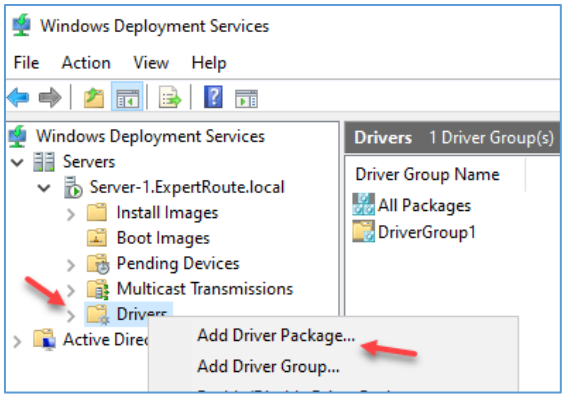
همان‌طور که گفتیم تمام کلاینت‌هایی که از این طریق ویندوز بر روی آنها نصب می‌شوند به صورت اتوماتیک عضو دومین می‌شوند و برای اینکه این موضوع اتفاق نیفتد باید به مانند شکل ۸-۸۸۹، وارد تب Client شوید و تیک گزینه‌ی Do not join the client to a domain after an installation را به مانند شکل فعال کنید.



شکل ۸- ۸۸۹ تغییرات در سرویس wds

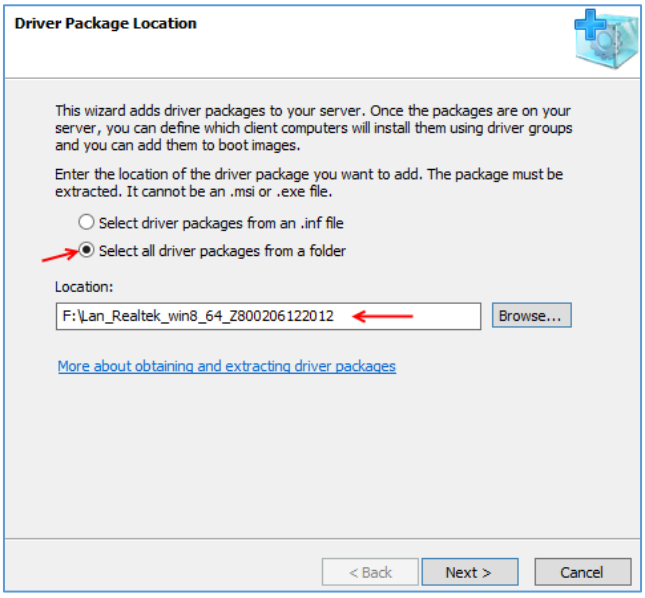
www.takbook.com

بعد از نصب ویندوز از طریق شبکه شاید شما نیاز داشته باشید که درایورهای مربوط به کلاینت‌ها هم به صورت خودکار از طریق این سرویس نصب شود، برای انجام این کار سرویس Deployment را اجرا کنید و به مانند شکل ۸-۸۹۰، از سمت چپ بر روی Drivers کلیک راست کنید و بر روی Add Driver Package کلیک کنید.



شکل ۸- ۸۹۰ اضافه کردن درایور در سرویس wds

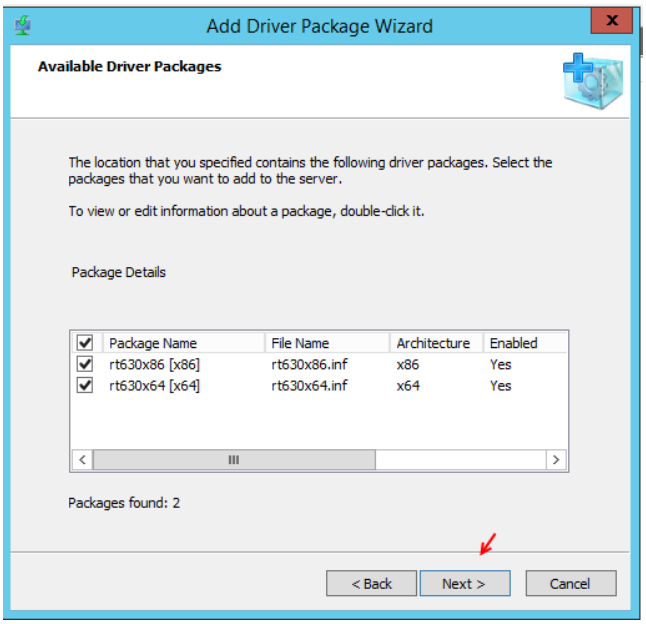
به مانند شکل ۸-۸۹۱، در این قسمت دو روش برای معرفی درایور موردنظر وجود دارد که با انتخاب گزینه اول می‌توانید فایل INF مربوط به درایور موردنظر را به آن معرفی کنید و یا با انتخاب گزینه دوم پوشه مربوط به درایو موردنظر را به مانند شکل معرفی کنید.



شکل ۸- ۸۹۱ اضافه کردن درایور در سرویس wds

www.takbook.com

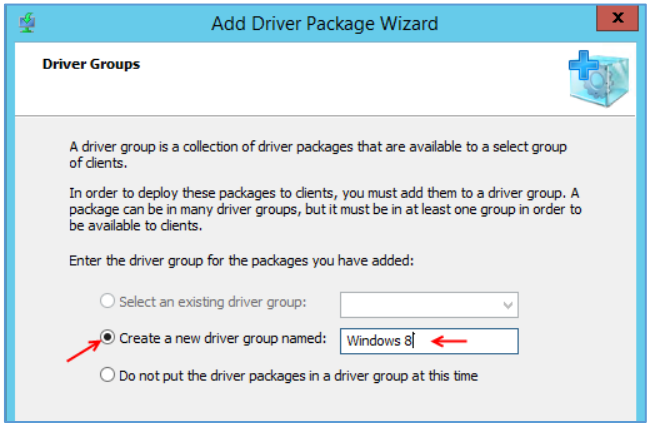
بعد از بررسی انجام شده در شکل ۸-۸۹۲، دو ورژن برای این درایو پیدا شده است که می‌توانید هر دو و یا یکی از آنها را انتخاب کنید.



شکل ۸- ۸۹۲ اضافه کردن درایور در سرویس wds

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

در شکل ۸-۸۹۳، می‌توانید برای درایو موردنظر خود یک گروه ایجاد کنید، مثلاً اگر درایو مربوط به ویندوز 8 می‌باشد یک گروه با نام Windows 8 ایجاد کنید.



شکل ۸- ۸۹۳

www.takbook.com

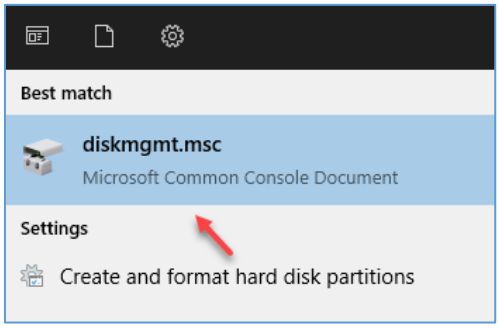
با این کار درایور آماده نصب می‌باشد و زمانی یک کلاینت اقدام به نصب ویندوز کند این درایور در صورت نیاز بر روی آن به صورت خودکار نصب خواهد شد.

بررسی دیسک‌ها و ابزارها

در این بخش در مورد دیسک‌ها و ذخیره‌سازها صحبت می‌کنیم و نحوه‌ی مدیریت آنها را بررسی خواهیم کرد و در کنار آن یاد می‌گیریم چگونه امنیت آنها را حفظ کنیم و یک پشتیبان کامل از اطلاعات آنها تهیه کنیم.

۸-۳-۲٤ بررسی سرویس Disk Management

این سرویس ساده که در ویندوز قرار دارد، برای مدیریت هارد دیسک‌ها و درایورها می‌باشد که می‌تواند عملیات سودمندی را برای بهره‌وری بالاتر سرورها انجام دهد، این سرویس بصورت پیش‌فرض بر روی ویندوز سرور نصب شده است و برای اجرای آن کافی است به مانند شکل ۸-۸۹٤، در Run کلمه‌ی Diskmgmt.msc را وارد و Enter کنید و یا از طریق Search به آن دست پیدا کنید.



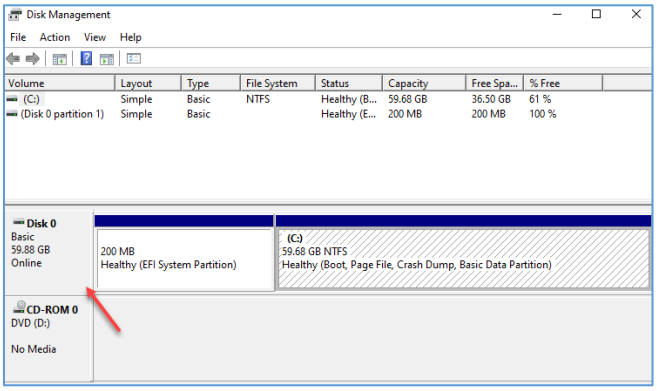
شکل ۸-۸۹۴ بررسی سرویس Disk Management

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

به مانند شکل ۸-۸۹۵، در این سرویس یک هارد دیسک با نام Disk 0 را مشاهده می‌کنید که دارای ۵۹.۸۸ گیگابایت فضا است، نوع دیسک در این قسمت Basic در نظر گرفته شده است. که می‌توان آن را به Dynamic تغییر داد ک در ادامه این موضوع را بررسی خواهیم کرد.

یک DVD Rom هم در کنار هارد دیسک مشاهده می‌کنید که در این قسمت لیست شده است.

www.takbook.com

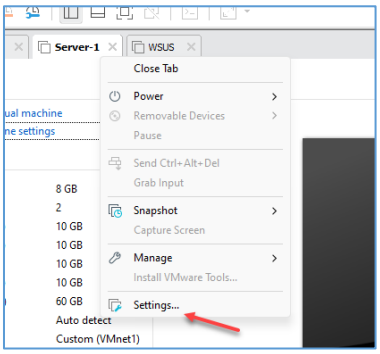


شکل ۸- ۸۹۵ بررسی سرویس Disk Management

ابزارها مختلفی برای هارد دیسک مورد نظر وجود دارد که در این قسمت آنها را بررسی می‌کنیم.

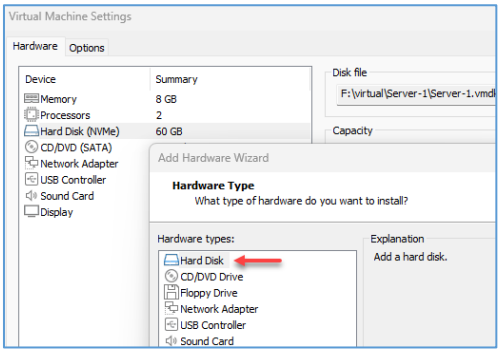
قبل از اینکه عملیات مورد نظر را انجام دهیم ٤ هارد دیسک مجازی را از طریق VMware Workstation به ماشین مورد نظر خود اضافه می‌کنیم و روی آنها کار خواهیم کرد.

به مانند شکل ۸-۸۹٦، بر روی ماشین مورد نظر کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید.



شکل ۸- ۸۹۶ بررسی سرویس Disk Management

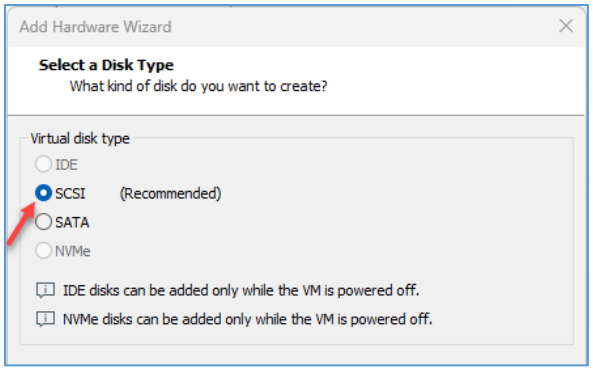
به مانند شکل ۸-۸۹۷، بر روی Add کلیک کنید و Hard Disk را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸- ۸۹۷ بررسی سرویس Disk Management

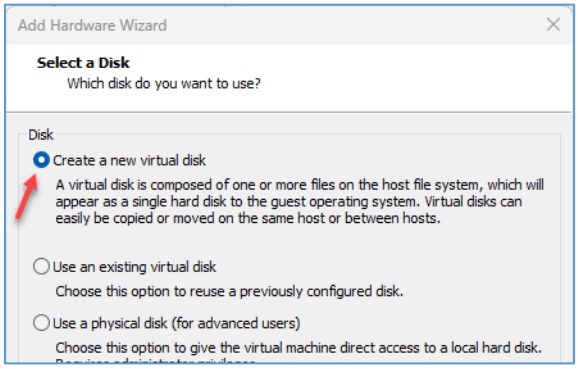
www.takbook.com

به مانند شکل ۸–۸۹۸، گزینه‌ی SCSI یا SATA را انتخاب و بر روی Next کلیک کنید.



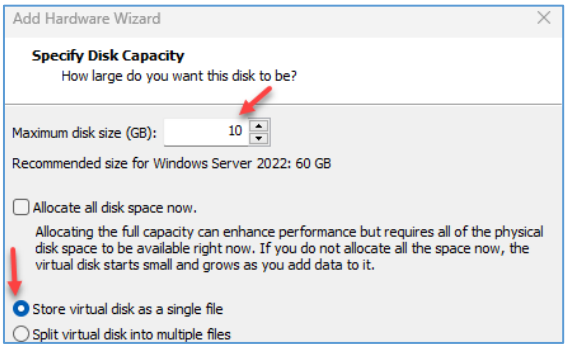
شکل ۸– ۸۹۸ بررسی سرویس *Disk Management*

به مانند شکل ۸–۸۹۹، برای ایجاد هارد دیسک جدید گزینه‌ی اول را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸– ۸۹۹ بررسی سرویس *Disk Management*

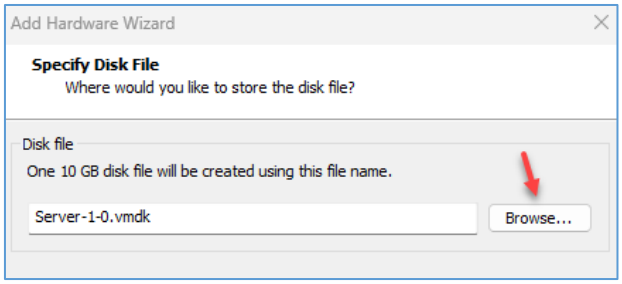
حجم ۱۰ گیگ را طبق شکل ۸–۹۰۰، برای هر کدام از هارد دیسک‌ها وارد کنید.



شکل ۸– ۹۰۰ بررسی سرویس *Disk Management*

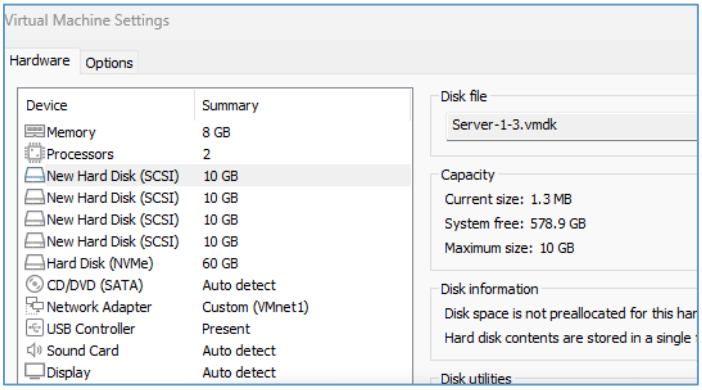
www.takbook.com

در شکل ۸-۹۰۱، می‌توانید مسیر ذخیره‌سازی هارد دیسک مورد نظر را تغییر دهید.



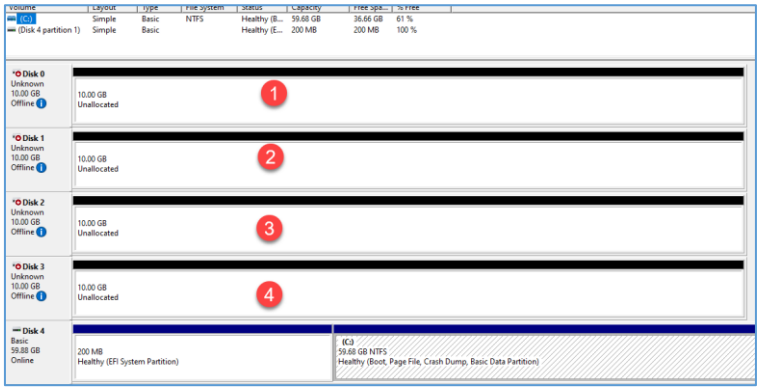
شکل ۸- ۹۰۱ بررسی سرویس *Disk Management*

همان‌طور که در شکل ۸-۹۰۲، مشاهده می‌کنید هارد دیسک‌های مورد نظر به ماشین مورد نظر اضافه شده است و برای ادامه کار وارد ماشین مورد نظر می‌شویم و سرویس Disk Management را اجرا می‌کنیم.



شکل ۸- ۹۰۲ بررسی سرویس *Disk Management*

به مانند شکل ۸-۹۰۳، همان‌طور که در سرویس Disk Management مشاهده می‌کنید، هر چهار دیسک مورد نظر به لیست اضافه شده است و می‌توانیم عملیات خود را بر روی آن انجام دهیم.



شکل ۸- ۹۰۳ بررسی سرویس *Disk Management*

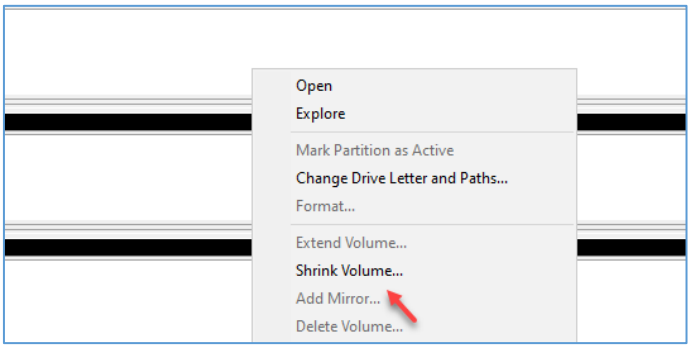
www.takbook.com

۱-۲٤-۳-۸ Shrink کردن

Shrink کردن یک دیسک به این صورت است که از مقدار فضای خالی موجود بر روی یک درایو یک درایو جدید از آن به وجود می‌آید به طور مثال اگر یک درایو C داشته باشید و مقدار ۲۰ گیگابایت فضا خالی داشته باشد می‌توانید از این مقدار فضای خالی یک پارتیشن از نوع shrink ایجاد کنید.

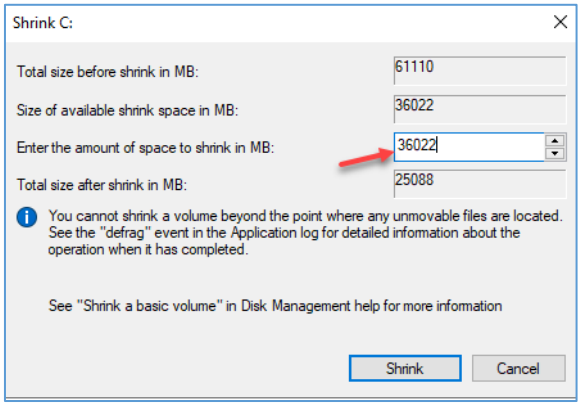
توجه داشته باشید این نوع پارتیشن مجازی، تابع درایو اصلی خود است و اگر درایو اصلی را حذف کنید این پارتیشن نیز حذف خواهد شد.

به مانند شکل ۸-۹۰٤، بر روی نام درایو و یا به مانند شکل در قسمت Disk 0 بر روی درایو C کلیک راست کنید و گزینه Shrink Volume را انتخاب کنید.



شکل ۸- ۹۰۴ بررسی سرویس Disk Management

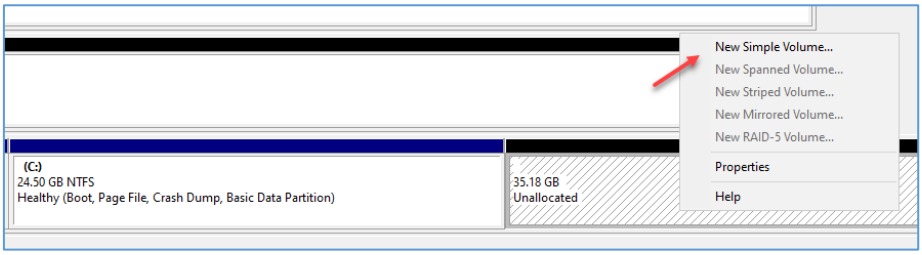
در شکل ۸-۹۰۵، در قسمت Total Size Before Shrink in MB مقدار فضای کل درایو موردنظر نوشته شده است، در قسمت Size of… مقدار فضای در دسترس نوشته شده است که باید در قسمت سوم مقدار فضایی را که برای ایجاد پارتیشن نیاز دارید را وارد کنید و بر روی Shrink کلیک کنید، در این شکل ۳٦ گیگ از فضای ٦۱ گیگ درایو C بعد از Shrink به درایو جدید اختصاص داده خواهد شد.



شکل ۸- ۹۰۵ بررسی سرویس Disk Management

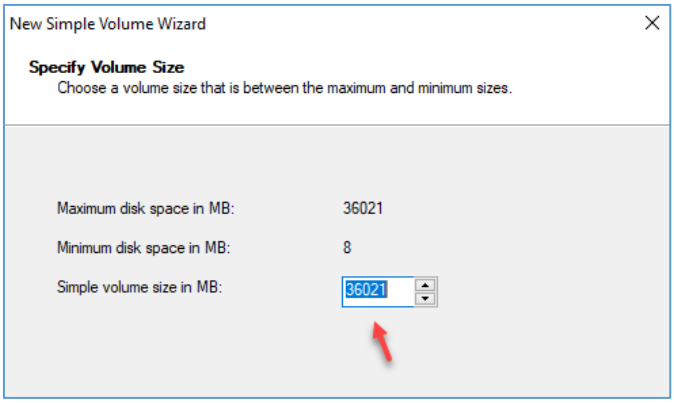
www.takbook.com

بعد از ایجاد پارتیشن موردنظر به مانند شکل ۸-۹۰۶، بر روی آن کلیک راست می‌کنیم و گزینه New Simple Volume را انتخاب می‌کنیم، البته در این قسمت گزینه‌های غیر فعال دیگر وجود دارد که با هم در ادامه آنها را بررسی می‌کنیم.



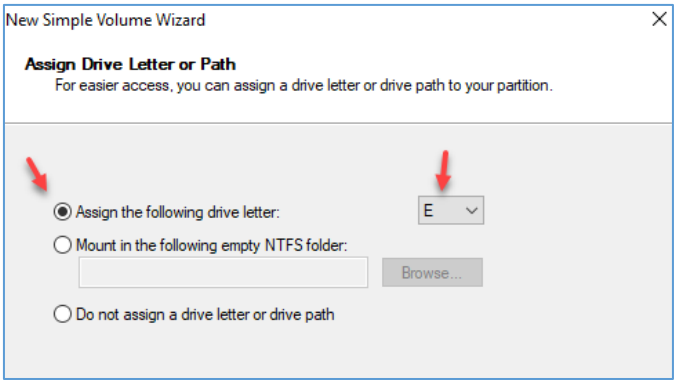
شکل ۸- ۹۰۶ بررسی سرویس *Disk Management*

در شکل ۸-۹۰۷، مقدار فضای مورد نیاز خود را برای ایجاد درایو جدید وارد کنید و بر روی Next کلیک کنید.



شکل ۸- ۹۰۷ بررسی سرویس *Disk Management*

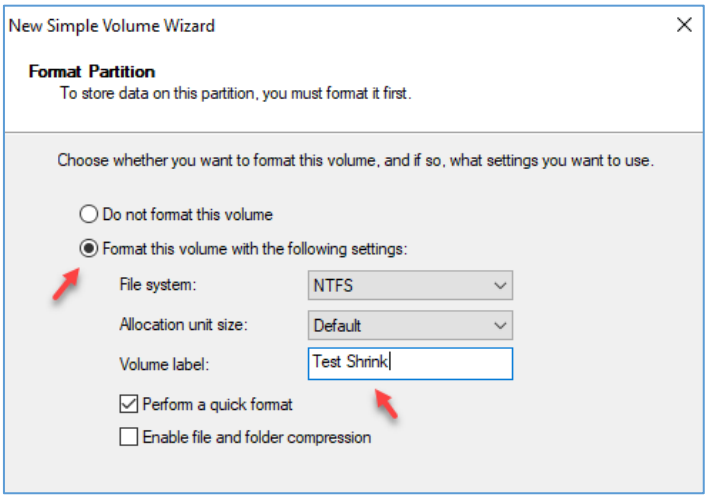
در شکل ۸-۹۰۸، نام درایو موردنظر خود را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸- ۹۰۸ بررسی سرویس *Disk Management*

www.takbook.com

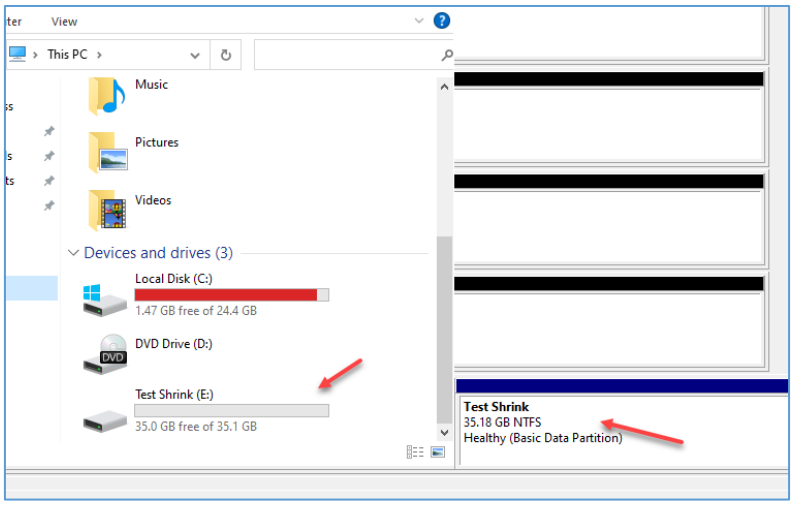
در شکل ۸-۹۰۹، اگر می‌خواهید درایو موردنظر شما بعد از ایجاد فرمت شود، گزینه Format this... را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸- ۹۰۹ بررسی سرویس *Disk Management*

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

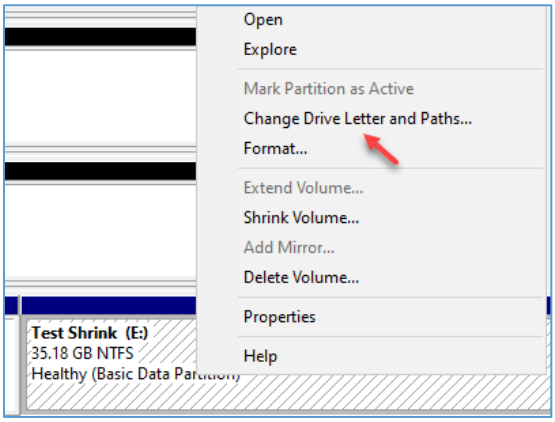
همان‌طور که در شکل ۸-۹۱۰، مشاهده می‌کنید، درایو Shrink با موفّقیت ایجاد شده است و می‌توانید از آن مانند یک درایو استفاده کنید.



شکل ۸- ۹۱۰ بررسی سرویس *Disk Management*

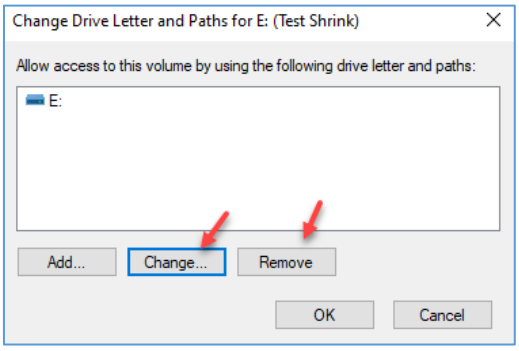
www.takbook.com

اگر به شکل ۸-۹۱۰، توجه کنید حرف E برای درایو مورد نظر در نظر گرفته شده است و برای اینکه این حرف را تغییر دهید می‌توانید بر روی درایو مورد نظر کلیک راست کنید و به مانند شکل ۸-۹۱۱، گزینه‌ی Change Drive Letter and Paths را انتخاب کنید.



شکل ۸- ۹۱۱ بررسی سرویس *Disk Management*

با استفاده از شکل ۸-۹۱۲، با کلیک بر روی Change می‌توانید نام درایو را تغییر دهید و اگر چنانچه بر روی Remove کلیک کنید فقط نام درایو مورد نظر حذف می‌شود و پارتیشن اصلی آن حذف نخواهد شد و با این کار باعث می‌شوید درایو مورد نظر در My computers نمایش داده نشود.



شکل ۸- ۹۱۲ بررسی سرویس *Disk Management*

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

۸-۳-۲٤-۲ تقسیم‌بندی در سرویس Disk Management

همان‌طور که می‌دانیم اطلاعات برای هر سازمانی بسیار مهم است و تمام تلاش خود را می‌کنند تا این اطلاعات را حفظ کنند، سرویس Disk Management امکاناتی را در اختیار شما قرار می‌دهد تا با استفاده از

www.takbook.com

چندین هارد دیسک از اطلاعات خود نسخه پشتیبان تهیه کنید، به این صورت نیست که پشتیبان‌گیری به صورت دستی انجام شود بلکه زمانی که در یک هارد دیسک اطلاعاتی را وارد می‌کنید در هارد دیسک دیگر این اطلاعات به صورت خودکار کپی می‌شود و همین کار باعث می‌شود که زمانی که یک هار دیسک از کار افتاد هارد دیسک دیگر شروع به فعالیت کند و یا از اطلاعات آن استفاده کنید.

تقسیم‌بندی به چهار صورت زیر انجام می‌شود:

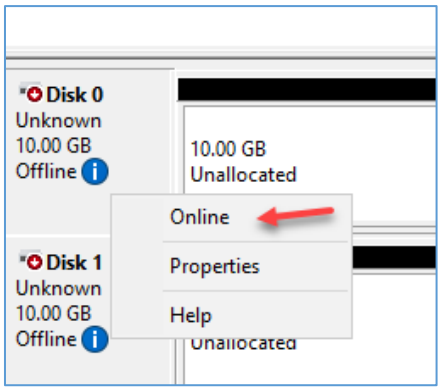
- ✓ Spanned Volume
- ✓ Striped Volume
- ✓ Mirrored Volume
- ✓ RAID – 5

این تقسیم بندی‌ها را با هم بررسی می‌کنیم و نتیجه کار را مشاهده می‌کنیم.

بررسی Spanned Volume

تقسیم‌بندی Spanned به این صورت است که می‌توانیم از ۲ هارد دیسک تا ۳۲ هارد دیسک در این تقسیم‌بندی استفاده کنیم، Spanned به این صورت عمل می‌کند که اطلاعات موردنظر خود را هم زمان در چندین دیسک وارد می‌کند و اگر یکی از دیسک‌ها از کار افتاد کل اطلاعات از بین خواهد رفت، با هم این موضوع را بررسی می‌کنیم تا متوجه شویم این تقسیم‌بندی زیاد هم جالب نخواهد بود.

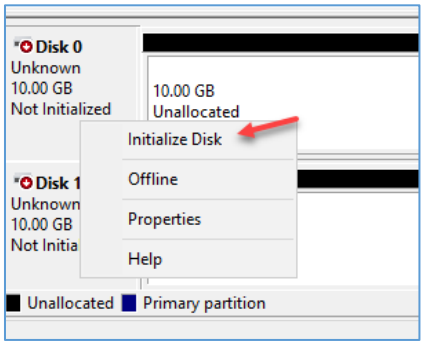
به مانند شکل ۸–۹۱۳، اگر به دیسک‌های جدید دقت کنید همه آنها در وضعیت آفلاین قرار دارند و باید بر روی آنها کلیک راست کنید و گزینه‌ی Online را انتخاب کنید.



شکل ۸- ۹۱۳ بررسی *Spanned Volume*

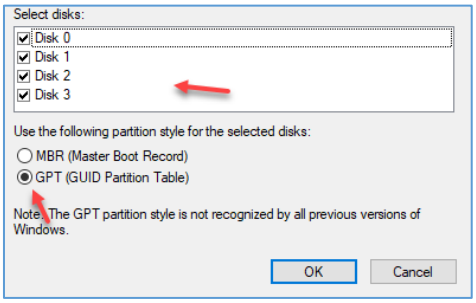
در ادامه به مانند شکل ۸–۹۱٤، باید بر روی هارد دیسک دوباره کلیک راست کنید و گزینه‌ی Initialize Disk را انتخاب کنید.

www.takbook.com



شکل ۸- ۹۱۴ بررسی *Spanned Volume*

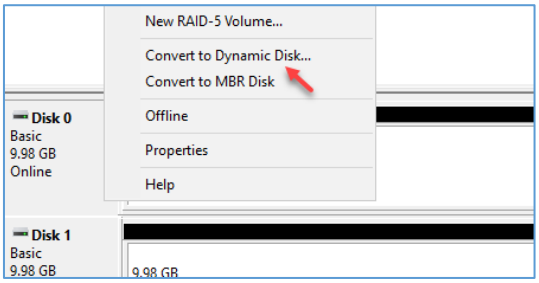
همان‌طور که در شکل ۸-۹۱۵، مشاهده می‌کنید همه دیسک‌های جدید در لیست موجود است و همه آنها را انتخاب کنید و برای نوع پارتیشن هم گزینه‌ی جدید GPT که بالای ۲ ترابایت را هم ساپورت می‌کند را انتخاب کنید.



شکل ۸- ۹۱۵ بررسی *Spanned Volume*

حالا همه چیز برای ایجاد تقسیم‌بندی آماده است و با هم این کار را انجام می‌دهیم.

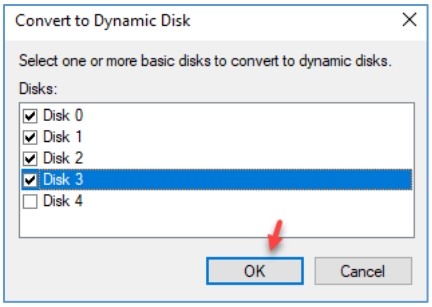
با دقت به شکل ۸-۹۱۶، توجه کنید، ٤ دیسکی که به لیست اضافه شده است از نوع Basic می‌باشد که برای استفاده از عملیات تقسیم‌بندی باید به حالت Dynamic تغییر حالت دهد، برای تغییر حالت به Dynamic بر روی یکی از چهار هارد موردنظر کلیک راست کنید و گزینه Convert to Dynamic Disk… را انتخاب کنید تا شکل بعد ظاهر شود.



شکل ۸- ۹۱۶ بررسی *Spanned Volume*

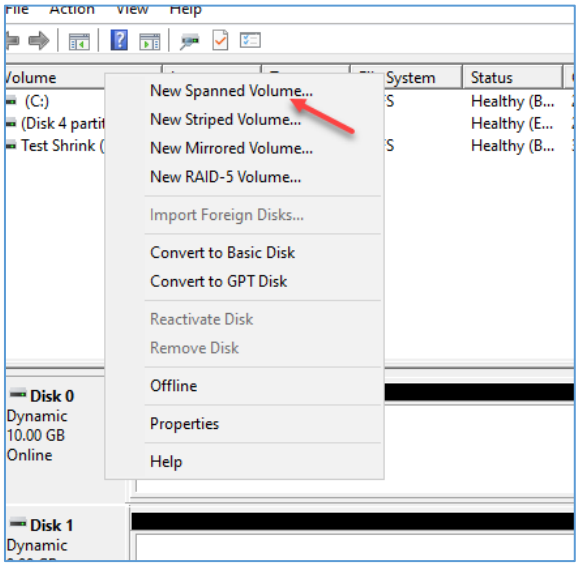
www.takbook.com

هر چهار هارد جدید را به مانند شکل ۸–۹۱۷، انتخاب کنید و بر روی OK کلیک کنید.



شکل ۸– ۹۱۷ بررسی *Spanned Volume*

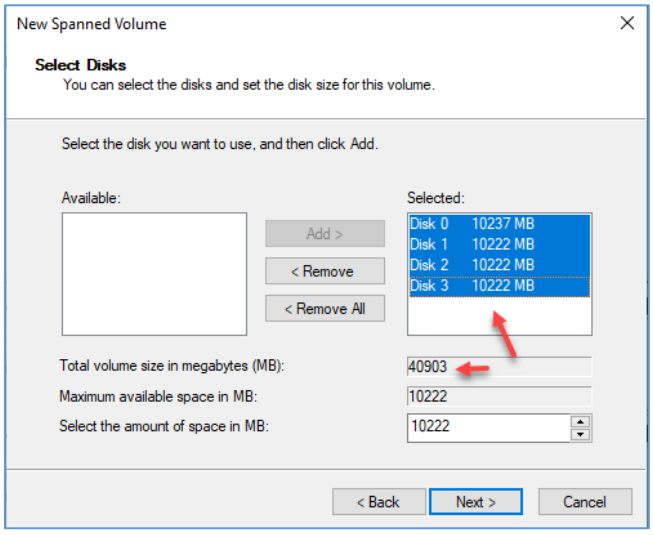
بعد از تبدل به حالت Dynamic به مانند شکل ۸–۹۱۸، بر روی هارد دیسک کلیک راست کنید و گزینه New Spanned Volume را انتخاب کنید، در صفحه باز شده بر روی Next کلیک کنید تا شکل بعد ظاهر شود.



شکل ۸– ۹۱۸ بررسی *Spanned Volume*

در شکل ۸–۹۱۹، ٤ هارد دیسک موردنظر انتخاب شده است، اگر به قسمت Total Volume size in Megabytes توجه کنید، کل فضای ٤ هارد دیسک را نوشته است، بر روی Next کلیک کنید.

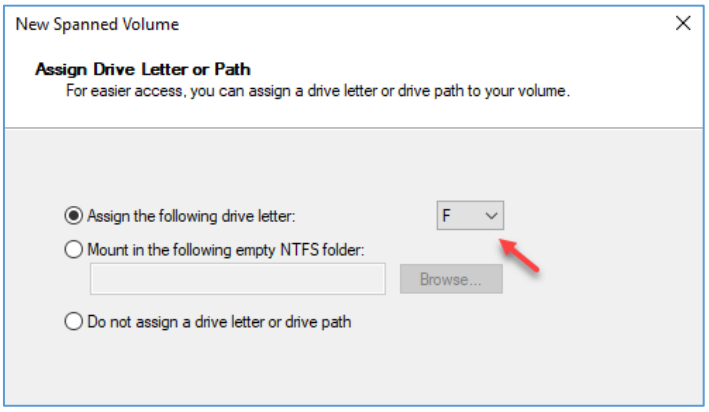
www.takbook.com



شکل ۸- ۹۱۹ بررسی *Spanned Volume*

در شکل ۸-۹۲۰، گزینه اول را انتخاب و نام درایو موردنظر خود را انتخاب کنید و بر روی Next کلیک کنید.

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

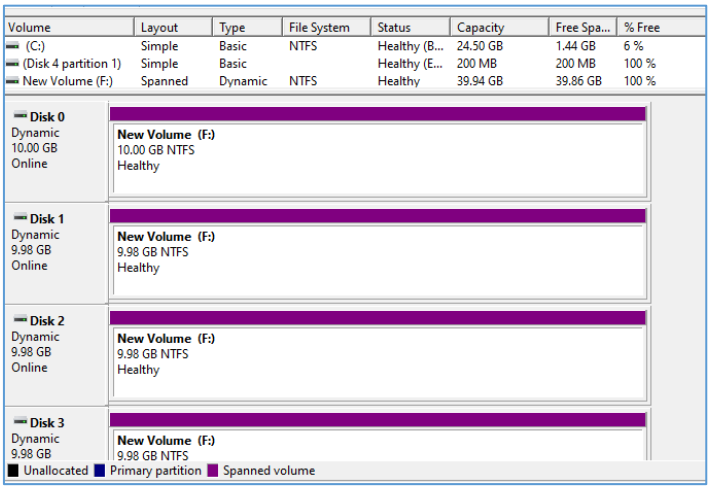


شکل ۸- ۹۲۰ بررسی *Spanned Volume*

بعد از انجام کارهای بالا هر 4 هارد دیسک به صورت هم زمان Format می‌شوند، همان‌طور که در شکل ۸-۹۲۱، مشاهده می‌کنید، هارد دیسک‌های موردنظر، به صورت یک هارد با نوع Spanned تبدیل شده است، اگر به درایو G در بالا نگاه کنید نوع آن Spanned و مقدار حافظه آن را ۳۹.۹٤ در نظر گرفته است که این فضای کل هر ۳ هارد دیسک می‌باشد و در قسمت Free عدد 100% نوشته شده است، یعنی اینکه این نوع

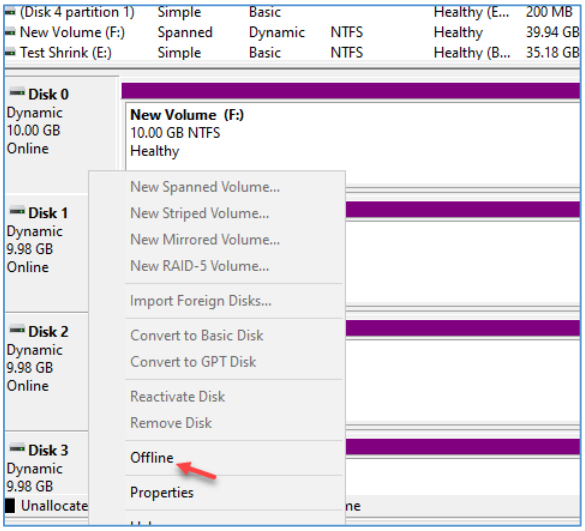
www.takbook.com

هار دیسک هیچ گونه امنیتی ندارد و با خراب شدن یک هارد تمام اطلاعات از بین خواهد رفت، با هم این موضوع را تست می‌کنیم.



شکل ۸- ۹۲۱ بررسی *Spanned Volume*

به مانند شکل ۸-۹۲۲، بر روی یکی از هارد دیسک‌ها کلیک راست کنید و گزینه Offline را انتخاب کنید تا هارد دیسک انتخاب شده از کار انداخته شود.



شکل ۸- ۹۲۲ بررسی *Spanned Volume*

در شکل ۸-۹۲۳، مشاهده می‌کنید که هر ۳ هارد دیسک از رده خارج شدند و این همان موضوعی است که استفاده از این نوع هارد دیسک‌ها با تقسیم‌بندی Spanned زیاد امنیت ندارد، خوبی این روش فقط استفاده از کل فضای هاردها به عنوان یک هارد است.

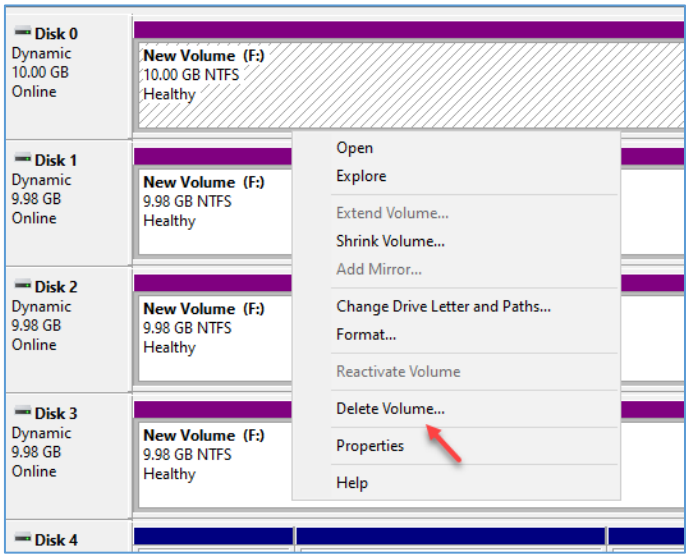
www.takbook.com



شکل ۸- ۹۲۳ بررسی *Spanned Volume*

بررسی Striped Volume

قبل از اینکه از این تقسیم‌بندی استفاده کنیم، برای استفاده از هارد دیسک‌های قبلی در این قسمت به مانند شکل ۸-۹۲٤، بر روی یکی از هارد دیسک‌ها کلیک راست کنید و گزینه Delete Volume را انتخاب کنید تا عملیات قبلی بر روی این سه هارد دیسک حذف شود.



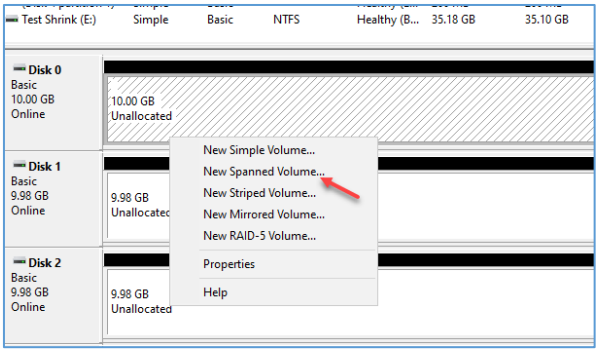
شکل ۸- ۹۲۴ بررسی *Striped Volume*

تقسیم‌بندی Striped به این صورت می‌باشد که در این تقسیم‌بندی به مانند قبل از ۲ تا ۳۲ هارد دیسک می‌توانید استفاده کنید، تقسیم‌بندی Striped به این صورت عمل می‌کند که به مانند قبل اگر ۳ هار دیسک

www.takbook.com

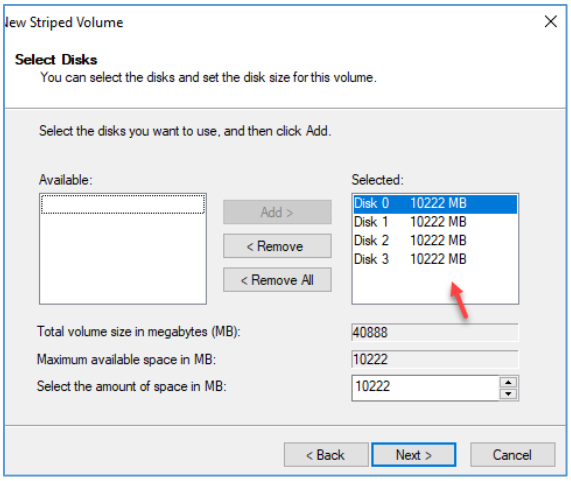
داشته باشیم ظرفیت همه آنها را با هم جمع می‌کند و به عنوان یک هارد دیسک در اختیار ما قرار می‌دهد که با از رده خارج شدن یکی از آنها بقیه آنها هم از کار خواهند افتاد.

وارد سرویس موردنظر شوید و به مانند شکل ۸–۹۲۵، بر روی یکی از درایوها کلیک راست کنید و گزینه New Striped Volume را انتخاب کنید.



شکل ۸- ۹۲۵ بررسی *Striped Volume*

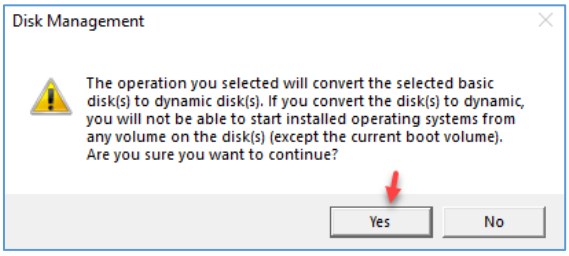
طبق شکل ۸–۹۲۶، هر چهار هارد را انتخاب و بر روی Next کلیک کنید تا دیسک مورد نظر ایجاد شود.



شکل ۸- ۹۲۶ بررسی *Striped Volume*

توجه داشته باشید نوع دیسک Basic می‌باشد که بعد از ایجاد New Striped Volume به مانند شکل ۸–۹۲۷، از شما سوأل خواهد شد که برای استفاده از این قابلیت باید دیسک تبدیل به نوع Dynamic شود، البته می‌توانید بر روی هارد دیسک‌های موردنظر کلیک راست کنید و گزینه Convert To Dynamic Disk را انتخاب کنید.

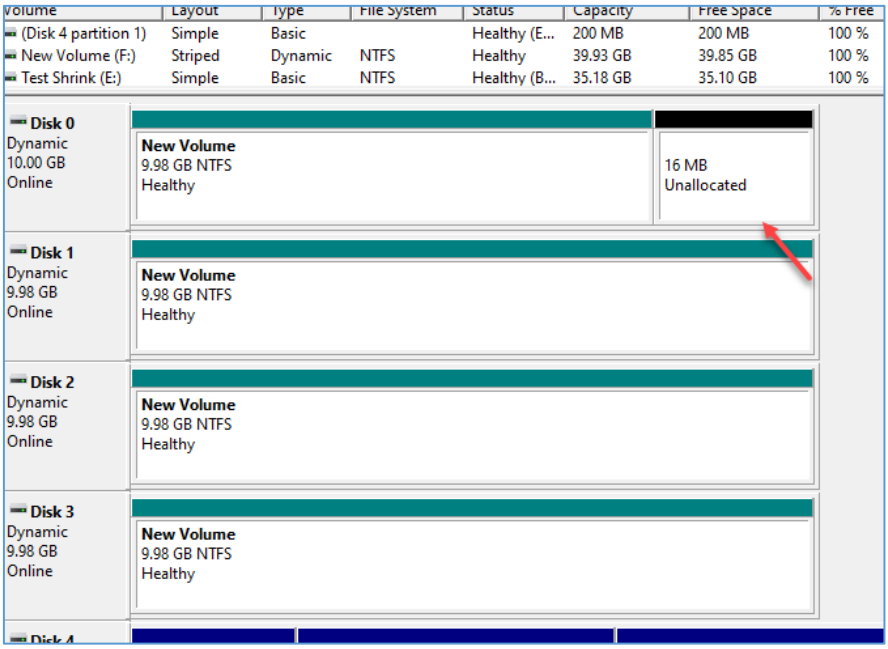
www.takbook.com



شکل ۸- ۹۲۷ بررسی *Striped Volume*

یک نکته اساسی در این قسمت وجود دارد و آن این است که در هاردهای موجود اگر یکی از هاردها مثلاً ۸ گیگ باشد و بقه‌ی هاردها ۱۰ گیگ باشند در زمان ایجاد این نوع تمام هاردها با همان هارد ۸ گیگ یکسان می‌شوند و از بقیه فضای موجود هاردها استفاده نخواهد شد که باید به این نکته توجه کنید که همه هاردها باید با یک حجم باشند.

همان‌طور که در شکل ۸-۹۲۸، مشاهده می‌کنید هارد دیسک موردنظر از نوع Striped ایجاد شده است، اگر به مقدار فضای آنها نگاهی بیندازید، متوجه خواهید شد یک هارد دیسک فضای خود را با هارد دیسکی که از بقیه فضای کمتر داشت برابر کردند و به خاطر همین مقدار ۱۶ مگابایت فضا بدون استفاده رها شده است.



شکل ۸- ۹۲۸ بررسی *Striped Volume*

www.takbook.com

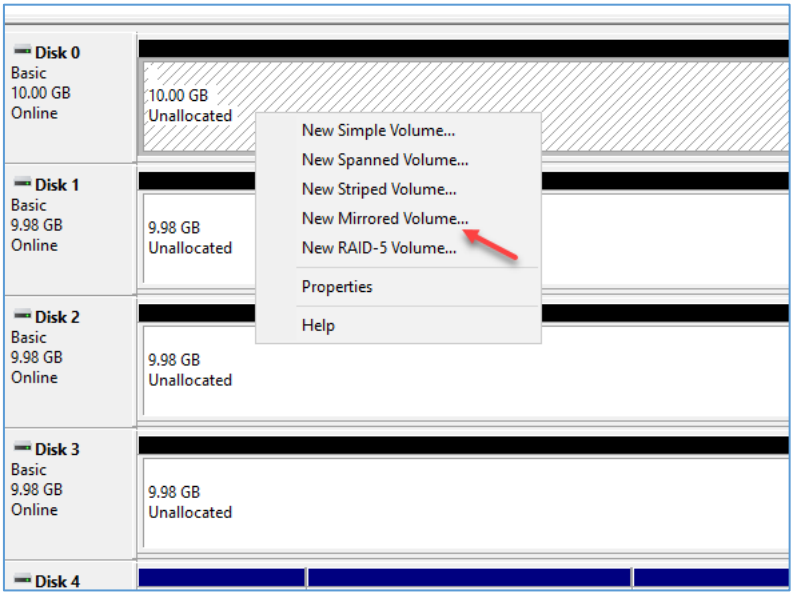
این نوع تقسیم‌بندی به مانند تقسیم‌بندی قبلی بدون امنیت می‌باشد و با خرابی یک هارد دیسک بقیه آنها از کار خواهند افتاد.

بررسی Mirroring Volume

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

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

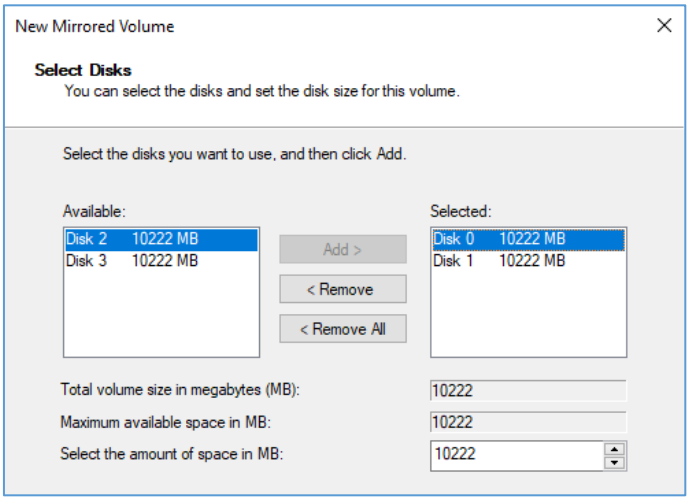
در شکل ۸–۹۲۹، بر روی یکی از هارد دیسک‌ها کلیک راست کنید و گزینه New Mirrored Volume را انتخاب کنید و در شکل باز شده بر روی Next کلیک کنید تا شکل بعد ظاهر شود.



شکل ۸– ۹۲۹ بررسی Mirroring Volume

در شکل ۸–۹۳۰، فقط دو هارد دیسک می‌تواند به لیست اضافه شود و هارد دیسک دیگری نمی‌تواند به لیست اضافه کنید، اگر به مقدار فضای کل هارد دیسک نگاهی بیندازید متوجه خواهید شد که فقط از فضای یک هارد دیسک استفاده می‌شود.

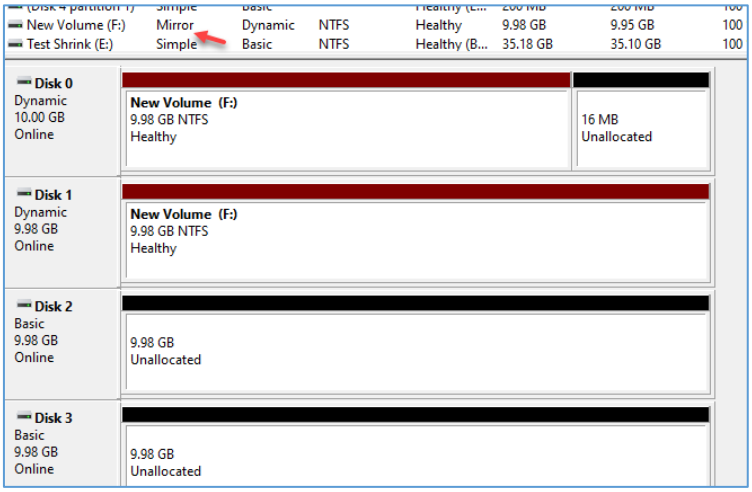
www.takbook.com



شکل ۸– ۹۳۰ بررسی Mirroring Volume

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

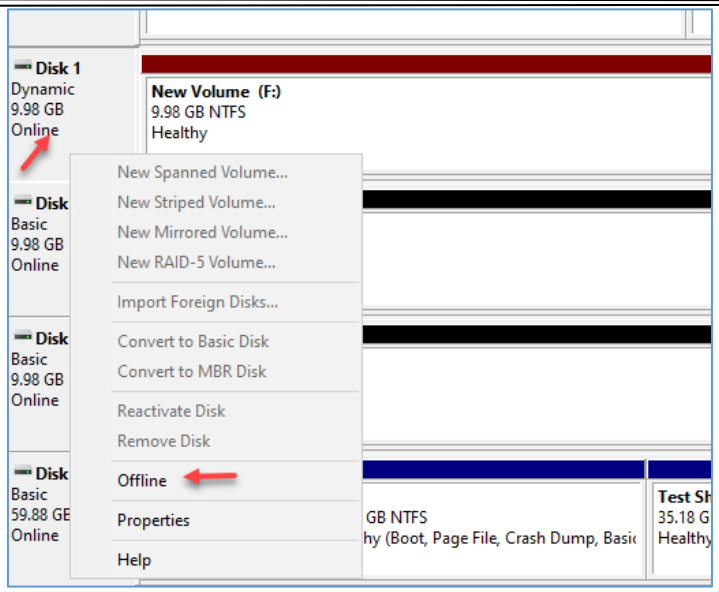
در شکل ۸–۹۳۱، هارد دیسک موردنظر با قالب Mirror ایجاد شده است که امنیت اطلاعات در این نوع تقسیم بندی‌ها ۱۰۰ می‌باشد، برای درک بهتر این موضوع در صفحه بعد یکی از هارد دیسک‌ها را از رده خارج می‌کنیم.



شکل ۸- ۹۳۱ بررسی *Mirroring Volume*

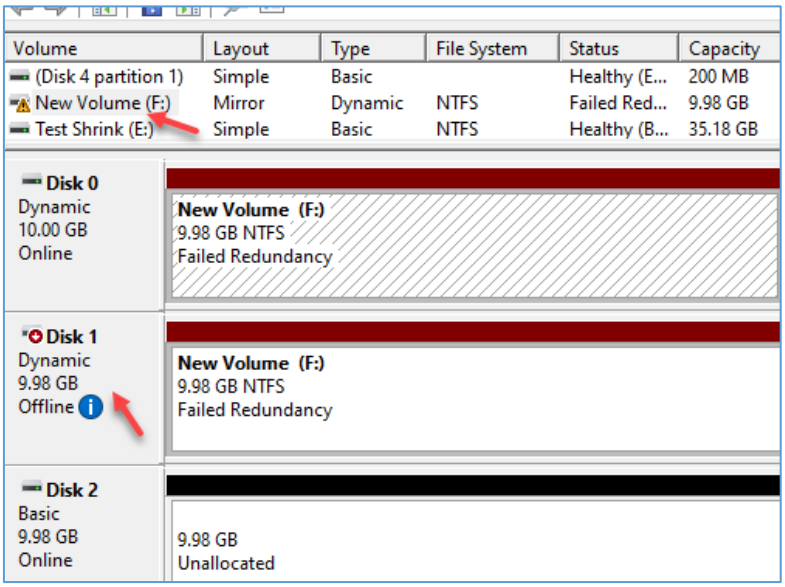
به مانند شکل ۸–۹۳۲، بر روی یکی از هارد دیسک‌ها که عملیات Mirror روی آن انجام شده کلیک راست کنید و گزینه Offline را انتخاب کنید تا هارد موردنظر از کار انداخته شود.

www.takbook.com



شکل ۸- ۹۳۲ بررسی *Mirroring Volume*

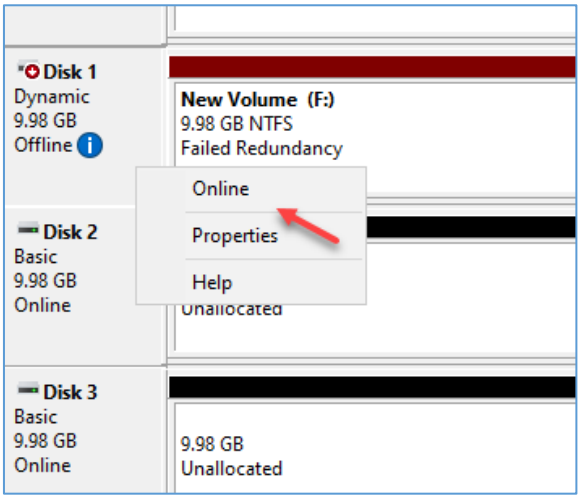
همان‌طور که در شکل ۸-۹۳۳، مشاهده می‌کنید، هارد دیسک شماره ۱ از کار افتاده، بعد از این عمل علامت اخطار روی درایو نمایان شده است و در قسمت پائین نوشته Failed Redundancy ظاهر شده است که نشان دهنده این است که یکی از هارد دیسک‌ها از کار افتاده و هارد دوم در حال کار می‌باشد و باید هارد اول را تعویض کنید.



شکل ۸- ۹۳۳ بررسی *Mirroring Volume*

www.takbook.com

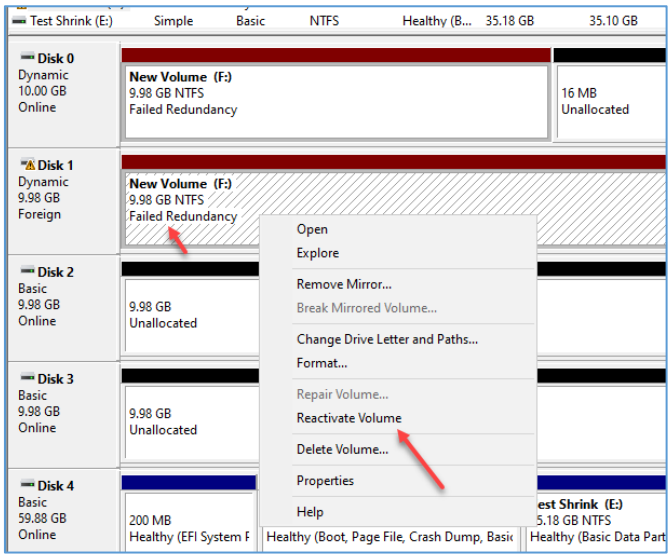
برای حل این مشکل به مانند شکل ۸-۹۳٤، بر روی هارد دیسکی که با مشکل مواجه شده کلیک راست می‌کنیم و گزینه Online را انتخاب می‌کنیم، البته در واقعیت باید هارد را تعمیر یا تعویض کنید و بعد این کار را انجام دهید.



شکل ۸- ۹۳۴ بررسی *Mirroring Volume*

به شکل ۸-۹۳۵، توجه کنید که بعد از اینکه هارد دیسک را فعال کردیم، هنوز در حالت Failed Redundancy قرار دارد که برای حل این مشکل به شکل ۸-۹۳۵، توجه کنید.

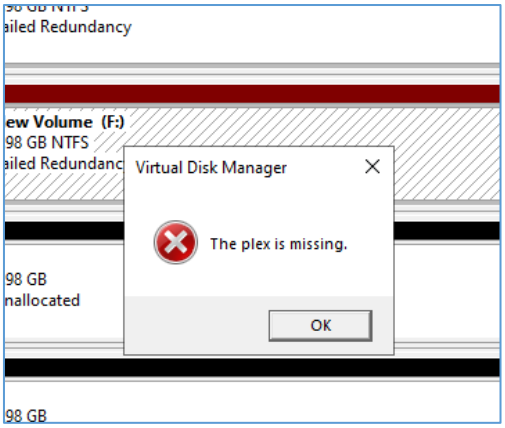
بر روی هارد دیسک دارای مشکل کلیک راست کنید و گزینه Reactivate Disk را انتخاب کنید تا همسان‌سازی بین دو دیسک انجام شود، کمی باید صبر کنید تا عملیات انجام شود.



شکل ۸- ۹۳۵ بررسی *Mirroring Volume*

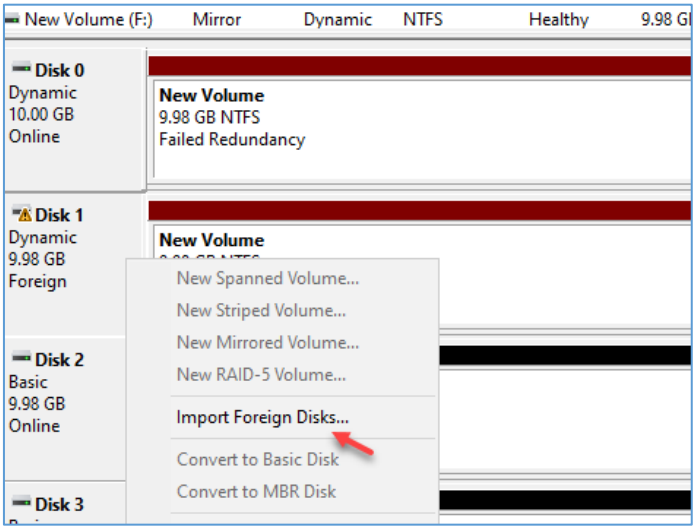
www.takbook.com

بعد از اینکه Reactive را فعال کردید با خطای شکل ۸–۹۳٦، روبرو خواهید شد



شکل ۸- ۹۳۶ بررسی *Mirroring Volume*

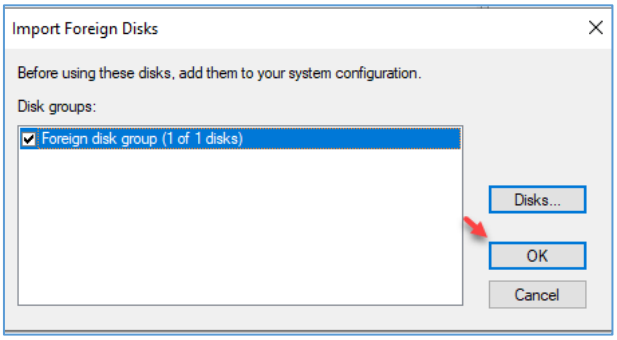
برای حل این مشکل باید به مانند شکل ۸–۹۳۷، بر روی هارد دیسک دارای مشکل کلیک راست کنید و گزینه‌ی Import Foreign Disks را انتخاب کنید.



شکل ۸- ۹۳۷ بررسی *Mirroring Volume*

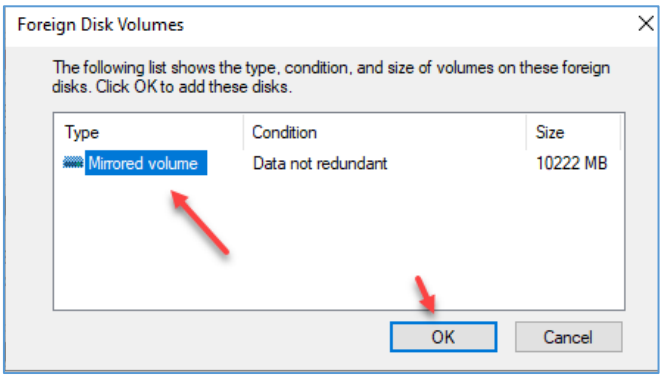
در شکل ۸–۹۳۸، تیک گزینه‌ی مورد نظر را انتخاب کنید و بر روی OK کلیک کنید.

www.takbook.com



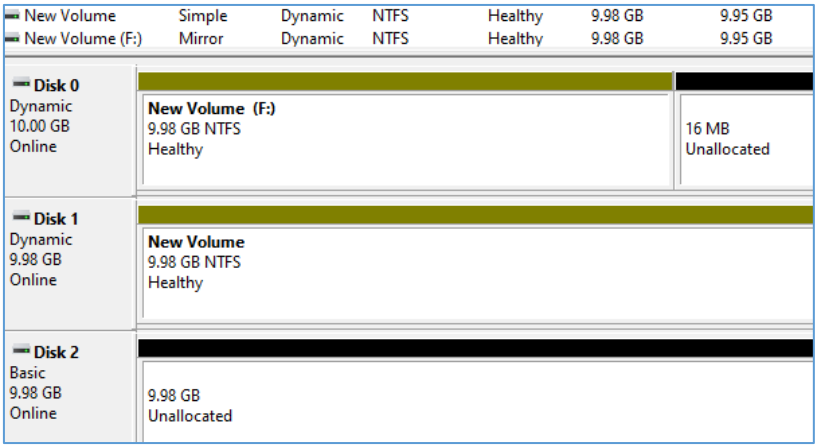
شکل ۸- ۹۳۸ بررسی *Mirroring Volume*

در شکل ۸-۹۳۹، بر روی OK کلیک کنید.



شکل ۸- ۹۳۹ بررسی *Mirroring Volume*

همان‌طور که در شکل ۸-۹٤۰، مشاهده می‌کنید دو هارد دیسک در حالت استیبل قرار گرفته است و در حال کار هستند.



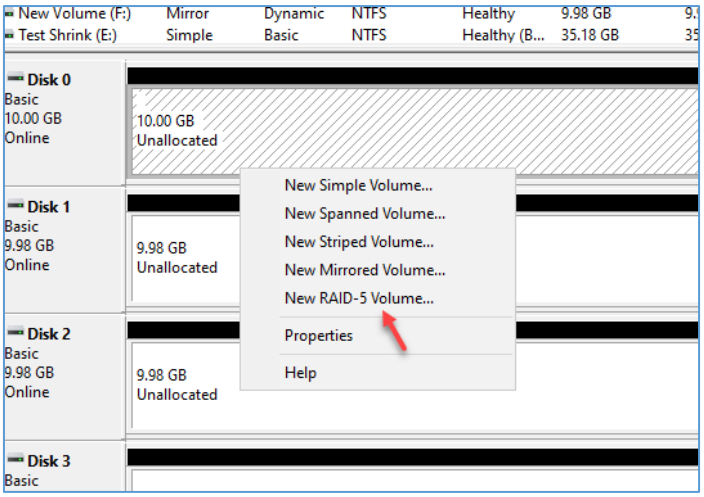
شکل ۸- ۹۴۰ بررسی *Mirroring Volume*

www.takbook.com

بررسی RAID–5

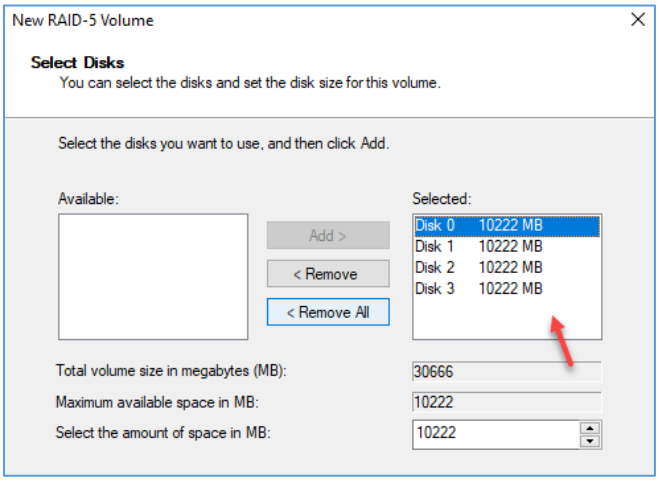
یکی از قویترین حالت‌های تقسیم بندی دیسک (البته در ویندوز سرور) با امنیت بسیار بالا که حداقل هارد دیسک مورد نیاز برای این حالت ۳ عدد می‌باشد که اطلاعات به طور همزمان بر روی هر سه هارد دیسک نوشته می‌شود و با از کار افتادن یک هارد، بقیه هاردها به کار خود ادامه می‌دهند ولی اگر دوتا از هاردها از کار انداخته شود هارد سوم هم از کار انداخته خواهد شد.

به مانند شکل ۸–۹٤۱، بر روی یکی از هاردهای زیر کلیک راست کنید و گزینه New RAID-5 را انتخاب کنید.



شکل ۸– ۹٤۱ بررسی RAID–5

در شکل ۸–۹٤۲، هر چهار هارد دیسک را به لیست اضافه کنید و بر روی Next کلیک کنید.

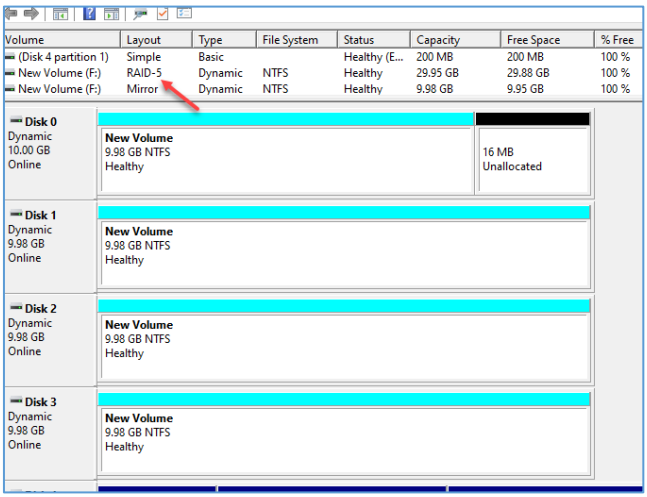


شکل ۸– ۹۴۲ بررسی RAID–5

www.takbook.com

در دو صفحه بعدی بر روی Next کلیک کنید و در صفحه آخر بر روی Finish کلیک کنید تا کار ایجاد هارد با قالب RAID-5 ایجاد شود.

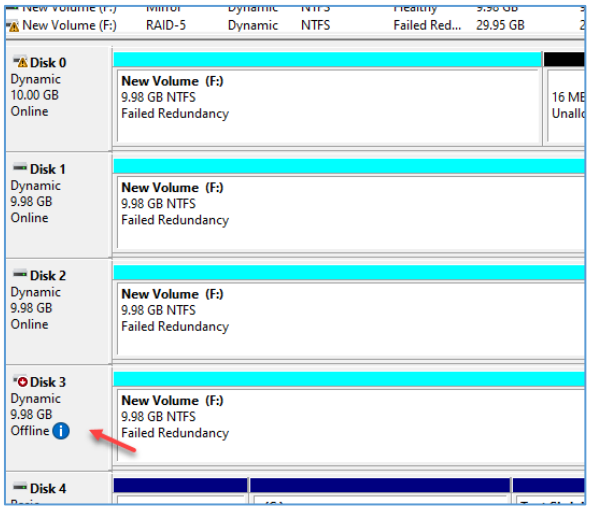
همان‌طور که در شکل ۸-۹۴۳، مشاهده می‌کنید، هارد دیسک‌ها با قالب RAID-5 ایجاد شده‌اند، به این نکته توجه کنید که مقدار فضای کل هارد برابر با 33% از هر هارد می‌باشد و بقیه برای پشتیبان‌گیری و امنیت مورد استفاده قرار می‌گیرند.



شکل ۸- ۹۴۳ بررسی RAID–5

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

در شکل ۸-۹۴۴، هارد شماره یک غیر فعال شده ولی بقیه هاردها به کارخود ادامه می‌دهند.

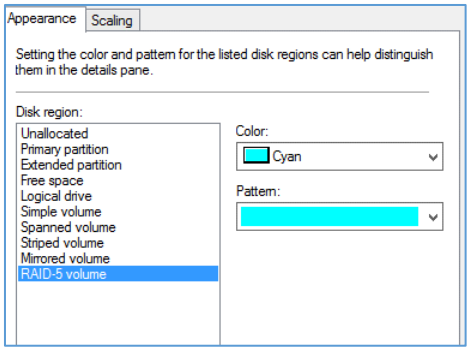


شکل ۸- ۹۴۴ بررسی RAID–5

www.takbook.com

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

در شکل ۸-۹٤٥، شما می‌توانید گزینه موردنظر خود را انتخاب و رنگ آن را به دلخواه خود تغییر دهید.

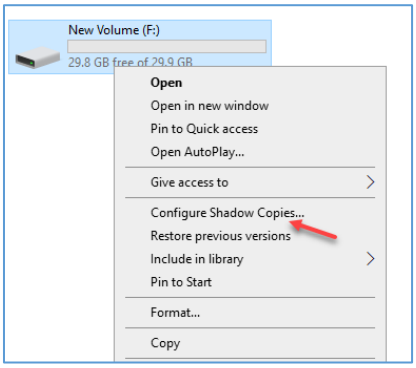


شکل ۸- ۹۴۵ بررسی RAID-5

۸-۳-۲٤-۳ کار با قابلیت Shadow Copy در درایوها

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

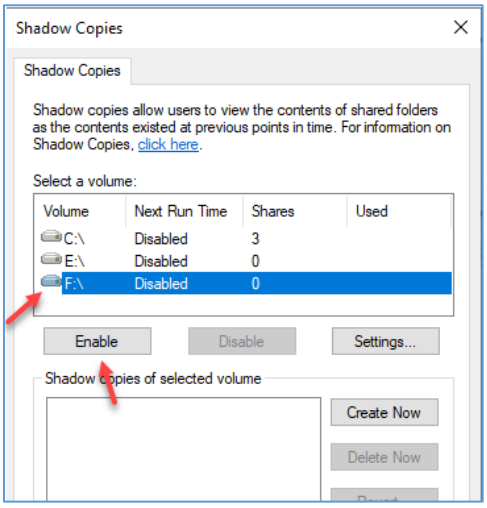
به دو طریق می‌توانید وارد تنظیمات Shadow Copy شوید، به مانند شکل ۸-۹٤٦، روی درایو موردنظر کلیک راست کنید و گزینه Properties را انتخاب کنید و به تب Shadow Copy مراجعه کنید یا به صورت شکل بر روی درایو موردنظر کلیک راست کنید و گزینه Configure Shadow Copies را انتخاب کنید.



شکل ۸- ۹۴۶ Shadow Copy در درایوها

www.takbook.com

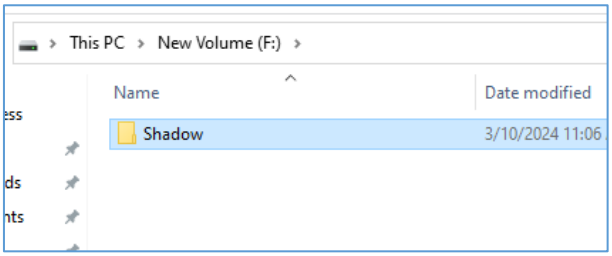
در شکل ۸-۹۴۷، اول باید نام درایو مورد نظر را انتخاب کنید و بعد برای فعال‌سازی این قابلیت بر روی Enable کلیک کنید و در صفحه باز شده بر روی Yes کلیک کنید تا قابلیت Shadow روی درایو مشخص‌شده فعال شود.



شکل ۸- ۹۴۷ *Shadow Copy در درایوها*

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

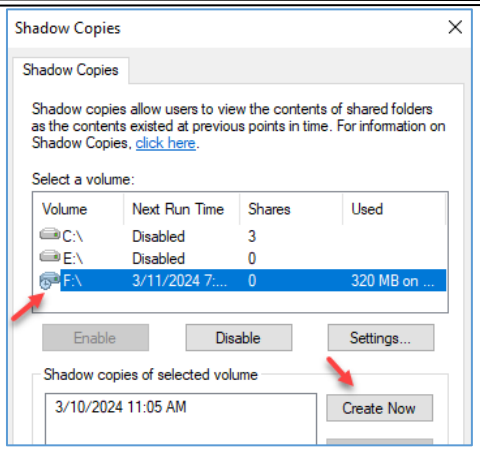
در شکل ۸-۹۴۸، پوشه موردنظر در درایو موردنظر ایجاد می‌کنیم، بعد از آن دوباره به قسمت shadow Copies مربوط به درایو موردنظر مراجعه می‌کنیم و یک Shadow از اطلاعات داخل درایو ایجاد می‌کنیم.



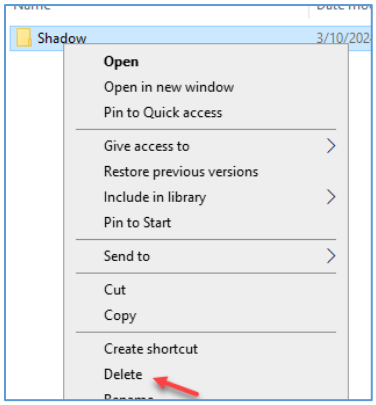
شکل ۸- ۹۴۸ *Shadow Copy در درایوها*

به مانند شکل ۸-۹۴۹، وارد تب Shadow Copies می‌شویم و نام درایو را از لیست انتخاب می‌کنیم و بر روی Create Now کلیک می‌کنیم تا عملیات Shadow انجام شود، بعد از آن بر روی ok کلیک کنید و پوشه ایجاد شده قبلی را به مانند شکل ۸-۹۵۰، حذف کنید.

www.takbook.com

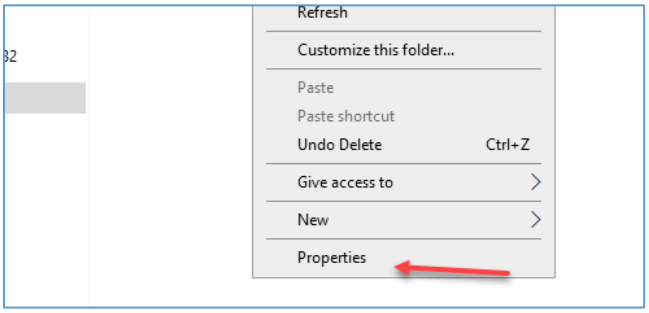


شکل ۸- ۹۴۹ *Shadow Copy* در درایوها



شکل ۸- ۹۵۰ *Shadow Copy* در درایوها

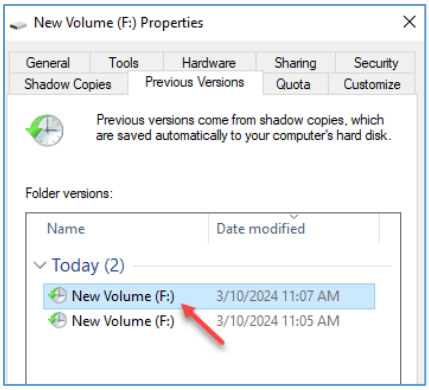
در شکل ۸-۹۵۱، پوشه ایجاد شده با نام Shadow حذف شده است و می‌خواهیم با استفاده از قابلیت Shadow اطلاعات از دست داده را برگردانیم، برای این کار در قسمت خالی صفحه کلیک راست می‌کنیم و گزینه Properties را انتخاب می‌کنیم.



شکل ۸- ۹۵۱ *Shadow Copy* در درایوها

www.takbook.com

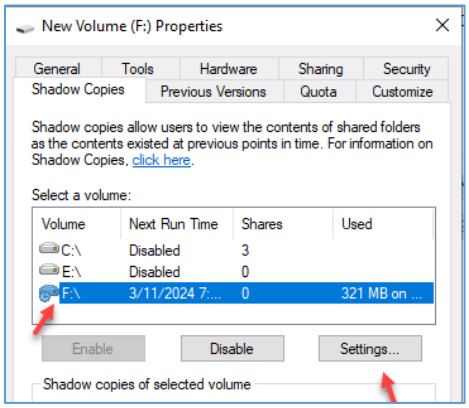
به مانند شکل ۸-۹۵۲، وارد تب Previous Versions می‌شویم و همان‌طور که مشاهده می‌کنید یک نسخه از درایو موردنظر در زمان و تاریخ مشخص‌شده ایجاد شده است، اگر بر روی Open کلیک کنید پوشه قبلی را مشاهده خواهید کرد، برای برگشت اطلاعات به حالت مشخص‌شده قبل بر روی Restore کلیک کنید و در صفحه باز شده بر روی Restore کلیک کنید.



شکل ۸- ۹۵۲ *Shadow Copy* در درایوها

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

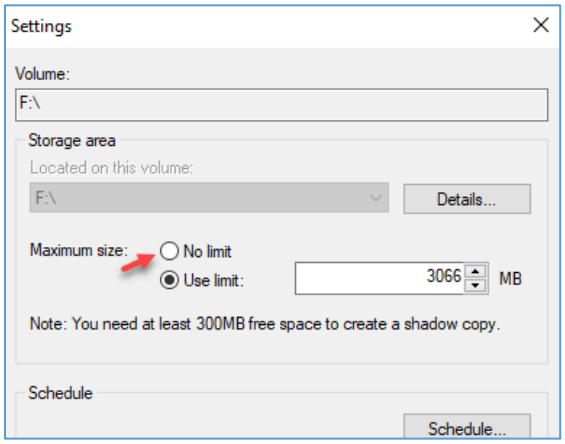
تا به اینجای کار نحوه‌ی فعال‌سازی و کارکرد قابلیت Shadow Copies را فرا گرفتیم و در این قسمت می‌خواهیم زمان‌بندی را برای اجرای عملیات Shadow ایجاد کنیم، برای ایجاد زمان‌بندی به مانند شکل ۸-۹۵۳، بر روی درایو موردنظر کلیک راست کنید و گزینه Configure Shadow Copy را انتخاب کنید و در تب Shadow Copies بر روی نام درایو کلیک کنید و بعد بر روی Settings کلیک کنید.



شکل ۸- ۹۵۳ *Shadow Copy* در درایوها

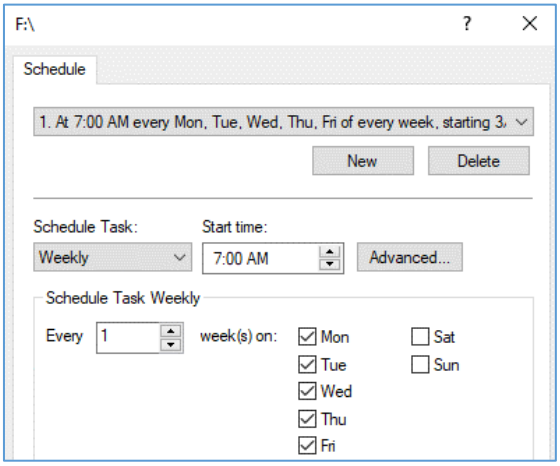
www.takbook.com

در شکل ۸-۹۵٤، می‌توانید در قسمت Maximum Size مشخص کنید که مقدار فضا برای عملیات Shadow چقدر باشد و یا با انتخاب گزینه No Limit مقدار نامحدود را به آن بدهید، برای ایجاد زمان‌بندی بر روی Schedule… کلیک کنید تا شکل ۸-۹۵۵، ظاهر شود.



شکل ۸- ۹۵۴ Shadow Copy در درایوها

همان‌طور که در شکل ۸-۹۵۵، مشاهده می‌کنید، به صورت پیش‌فرض مقدار اولیه به برنامه داده شده است و در روزهای مشخص‌شده روزی یک بار این کار را در ساعت ۷ صبح انجام می‌دهد که شما می‌توانید این زمان و روزها را تغییر دهید.



شکل ۸- ۹۵۵ Shadow Copy در درایوها

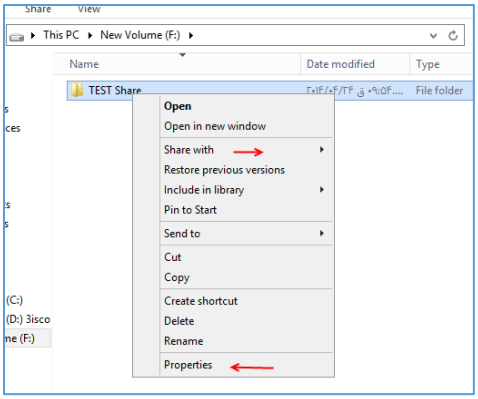
بر روی ok کلیک کنید تا تنظیمات موردنظر ذخیره شود.

www.takbook.com

۲۵-۳-۸ به اشتراک گذاری فایل‌ها

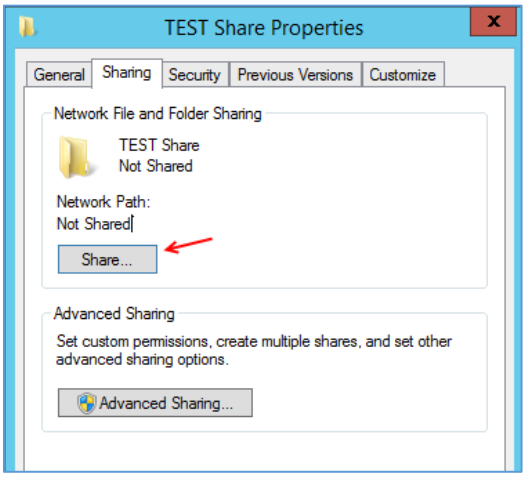
به اشتراک گذاری یا همان Share کردن فایل‌ها یکی از قابلیت‌های ابتدایی هر سیستم‌عامل در حال حاضر می‌باشد که توانسته کمک خوبی برای اشتراک‌گذاری فایل‌ها در شبکه باشد. در این قسمت یک پوشه را با هم Share می‌کنیم و نحوه ایجاد امنیت در به اشتراک‌گذاری فایل‌ها را بررسی می‌کنیم.

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



شکل ۸- ۹۵۶ به اشتراک گذاری فایل‌ها

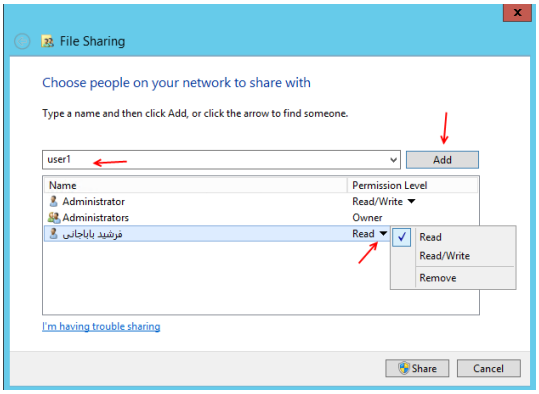
در شکل ۸-۹۵۷، به دو طریق می‌توان فایل موردنظر را برای کاربر موردنظر با مجوز خاص share کرد که فعلاً در این قسمت گزینه Share... را انتخاب می‌کنیم.



شکل ۸- ۹۵۷ به اشتراک گذاری فایل‌ها

www.takbook.com

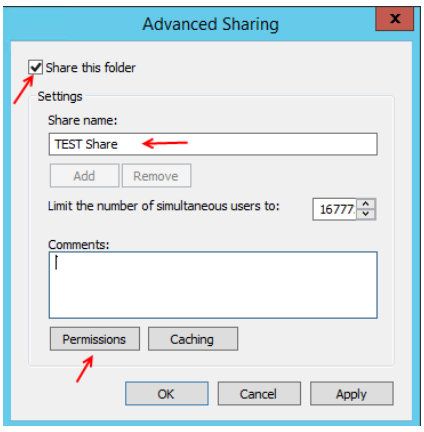
در شکل ۸–۹۵۸، باید نام کاربر موردنظر را در قسمت مشخص‌شده که User1 نوشته شده وارد کنید و بعد بر روی Add کلیک کنید تا به لیست اضافه شود و یا می‌توانید بر روی منوی کشویی که User1 وارد شده کلیک کنید و بعد بر روی Find People کلیک کنید.



شکل ۸– ۹۵۸ به اشتراک گذاری فایل‌ها

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

روش پیشرفته‌تری هم وجود دارد که می‌توانیم فایل یا پوشه خود را برای دیگران Share کنیم، برای این کار زمانی که وارد تب Sharing فایل موردنظر می‌شویم، بر روی Advanced Sharing کلیک کنید تا شکل ۸–۹۵۹، ظاهر شود.

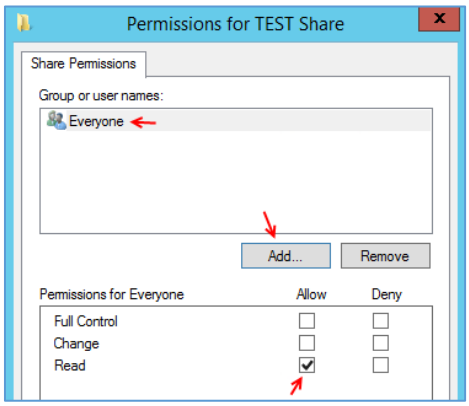


شکل ۸– ۹۵۹ به اشتراک گذاری فایل‌ها

www.takbook.com

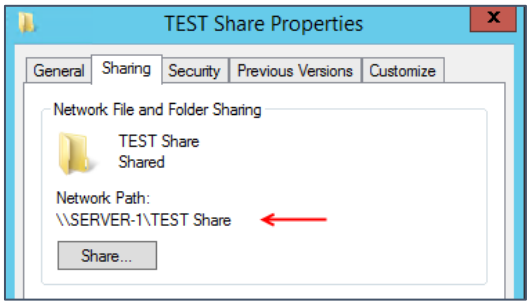
در شکل ۸-۹۵۹، تیک گزینه Share this folder را انتخاب کنید و در قسمت Share Name نام فایلی که می‌خواهید Share شود را وارد کنید، توجه داشته باشید که هر چیز که در این قسمت وارد کنید همان هم در قسمت Share برای دیگران نمایش داده می‌شود. در قسمت Limit the number… تعداد کاربران استفاده از این فایل را مشخص کنید که به صورت پیش فرض ۱۶۷۷۷ وارد شده است، اگر بر روی Apply کلیک کنید فایل موردنظر Share خواهد شد ولی اگر بخواهید این فایل را فقط برای کاربر خاصی Share کنید باید بر روی Permissions کلیک کنید.

به مانند شکل ۸-۹۶۰، اگر به لیست کاربران و گروه‌ها توجه کنید، فقط گروه Everyone قرار دارد که نشان دهنده این است که این پوشه برای تمام کاربران با دسترسی Read اشتراک گذاشته شده، اگر می‌خواهید این پوشه را برای کاربر خاصی Share کنید، گروه Everyone را انتخاب و بر روی Remove کلیک کنید تا گروه موردنظر از لیست حذف شود، بعد برای اضافه کردن کاربر موردنظر بر روی Add کلیک کنید و کاربر موردنظر را به لیست اضافه کنید.



شکل ۸- ۹۶۰ به اشتراک گذاری فایل‌ها

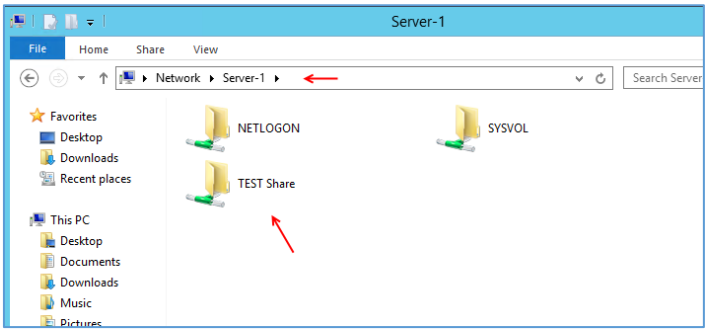
بعد از اینکه فایل را Share کردین به مانند شکل ۸-۹۶۱، در قسمت Network Path مسیر فایل در شبکه مشخص می‌شود یعنی با وارد کردن آدرس موردنظر در Address bar می‌توانید به فایل موردنظر دسترسی پیدا کنید.



www.takbook.com

برای ورود به قسمت Share باید از آدرس \\ServerName استفاده کنید که به جای ServerName باید نام سرور خود و یا آدرس IP آن را وارد کنید. به مانند شکل ۸-۹۶۱، عمل کنید.

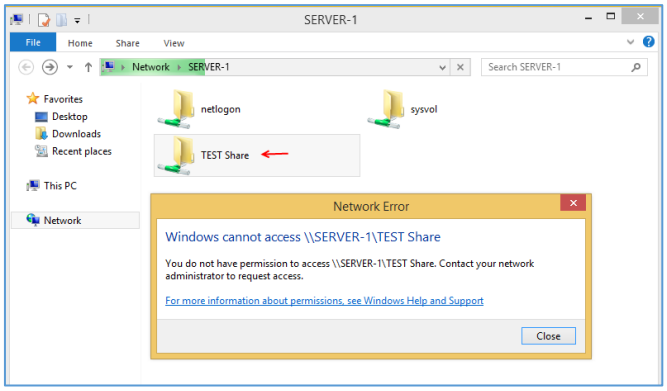
\\Server-1\



شکل ۸- ۹۶۱ به اشتراک گذاری فایل‌ها

زمانی که یک پوشه را برای یک کاربر خاصی Share کنید و به بقیه کاربران دسترسی ندهید، کاربران دیگر به جزء کاربران موجود در لیست نمی‌توانند به فایل موردنظر دسترسی داشته باشند. در شکل ۸-۹۶۱، پوشه Test Share فقط برای کاربر Administrator اشتراک گذاشته شده است و کاربران دیگر مجوز دسترسی به این فایل را ندارند، برای تست این موضوع با کاربر User1 که قبلاً ایجاد کرده بودیم وارد ویندوز می‌شویم که قبلاً آن را به شبکه متصل کرده بودیم.

در شکل ۸-۹۶۲، وارد آدرس \\Server-1 شده‌ایم که فایل‌های Share شده ویندوز سرور را برای ما لیست کرده است که با دابل کلیک بر روی پوشه Test Share با پیغام مواجه شده‌ایم در این پیغام به شما خسته نباشید گفته و به این موضوع اشاره دارد که این پوشه توسط صاحب آن برای شما Share نشده است و مجوز دسترسی به شما داده نشده است. پس اگر در جایی دیگر با این پیغام مواجه شدید بدانید که فایل موردنظر برای شما Share نشده است.



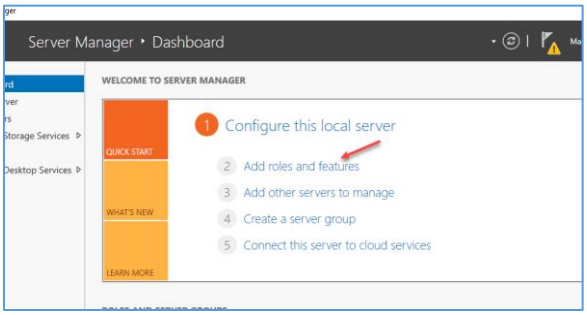
شکل ۸- ۹۶۲ به اشتراک گذاری فایل‌ها

www.takbook.com

۸-۳-۲۶ کار با Bitlocker

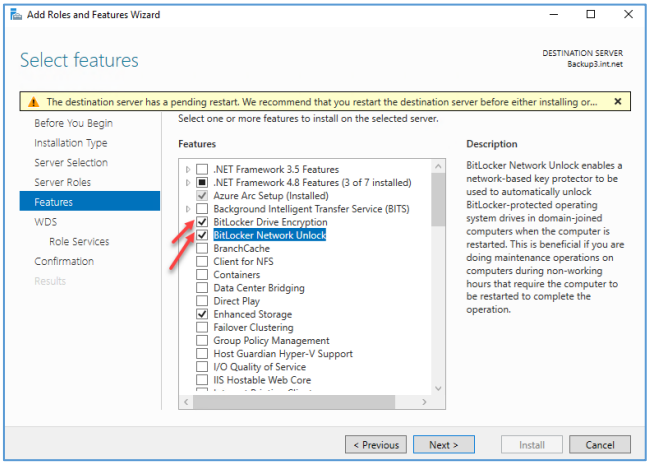
BitLocker یک ابزار رمزنگاری ارائه شده توسط مایکروسافت است که برای رمزنگاری درایوها و محافظت از اطلاعات حساس استفاده می‌شود. این ابزار به صورت پیش‌فرض در نسخه‌های حرفه‌ای (Pro)، تجاری (Enterprise)، و آموزشی (Education) سیستم‌عامل ویندوز (از ویندوز ۷ به بعد) در دسترس است. در ادامه، مراحل کلی کار با BitLocker و نکات مهم آن توضیح داده شده‌اند.

برای استفاده از این سرویس می‌توانیم وارد ویندوز سرور شویم و این سرویس را فعال کنیم، وارد یکی از سرورهای خود شوید و Server Manager را اجرا کنید و در شکل ۸-۹۶۳، بر روی Add Features کلیک کنید.



شکل ۸- ۹۶۳ فعال‌سازی سرویس Bitlocker

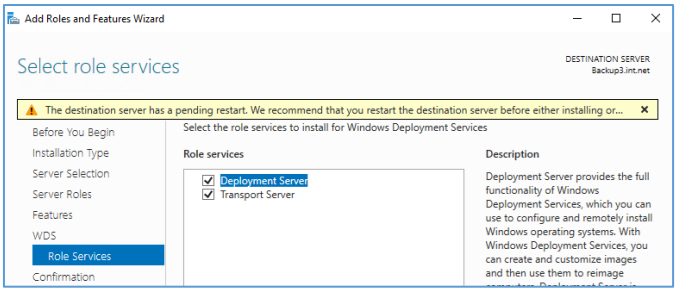
بر روی Next کلیک کنید و به مانند شکل ۸-۹۶۴، وارد قسمت Features شوید و در این قسمت تیک هر دو گزینه‌ی را انتخاب کنید و بر روی Next کلیک کنید، توجه داشته باشید که گزینه Bitlocker Network Unlock برای ایجاد یک گواهینامه در شبکه است تا کاربران مشخص بتوانند بدون هیچ تنظیمی درایو مورد نظر را مدیریت کنند.



شکل ۸- ۹۶۴ فعال‌سازی سرویس Bitlocker

www.takbook.com

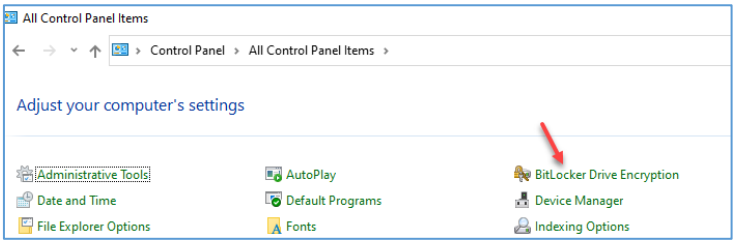
در شکل زیر تیک هر دو گزینه را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸- ۹۶۵ فعال‌سازی سرویس Bitlocker

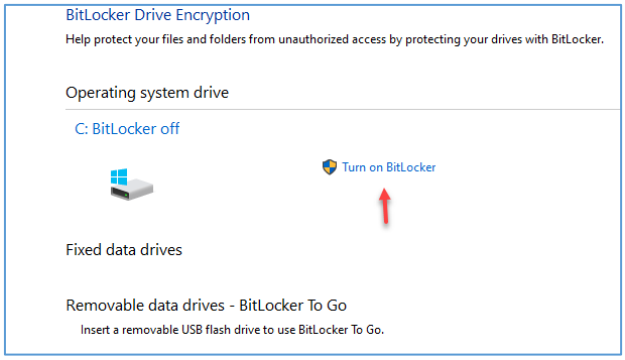
همان‌طور که در شکل ۸-۹٦٦، مشاهده می‌کنید سرویس مورد نظر به درستی نصب شده است، بهتر است سرور را Restart کنید تا تنظیمات به صورت کامل اعمال شود.

بعد از نصب وارد Control Panel شوید و بر روی BitLocker Drive Encryption کلیک کنید.



شکل ۸- ۹۶۶ فعال‌سازی سرویس Bitlocker

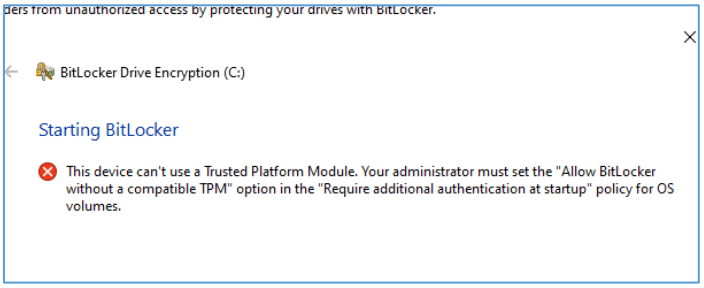
در شکل ۸-۹٦٧، درایو C برای شما نمایش داده شده و برای اینکه قابلیت BitLocker را روی آن فعال کنیم باید بر روی Turn on BitLocker کلیک کنید.



شکل ۸- ۹۶۷ فعال‌سازی سرویس Bitlocker

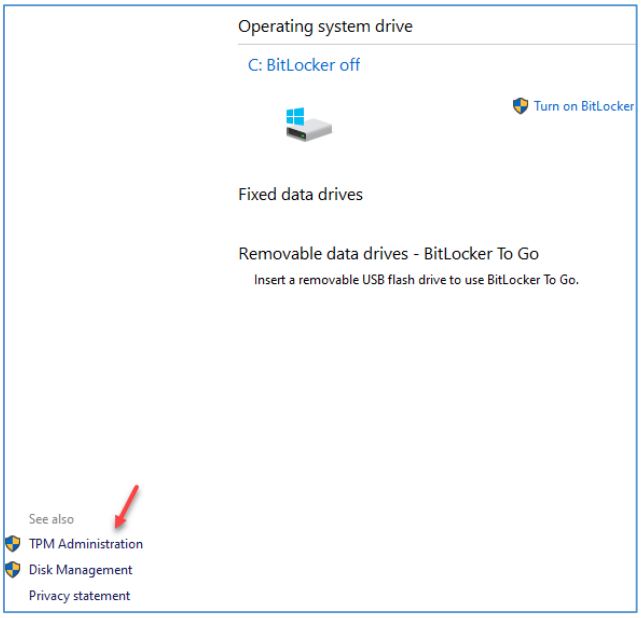
بعد از کلیک بر روی گزینه‌ی مورد نظر با خطای شکل ۸-۹٦٨، روبرو می‌شویم که به این نکته اشاره دارد که باید سرویس TPM بر روی سرور فعال شود.

www.takbook.com



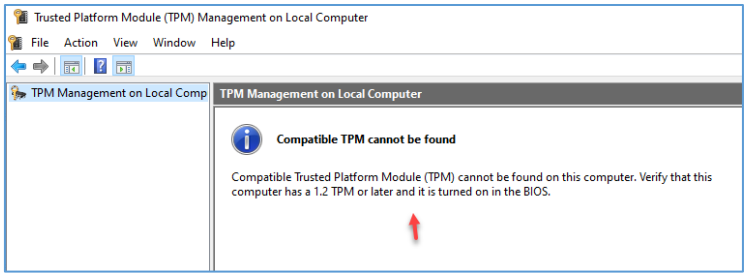
شکل ۸- ۹۶۸ فعال‌سازی سرویس Bitlocker

در شکل ۸-۹۶۹، در Control Panel بر روی TPM Administration کلیک کنید.



شکل ۸- ۹۶۹ فعال‌سازی سرویس Bitlocker

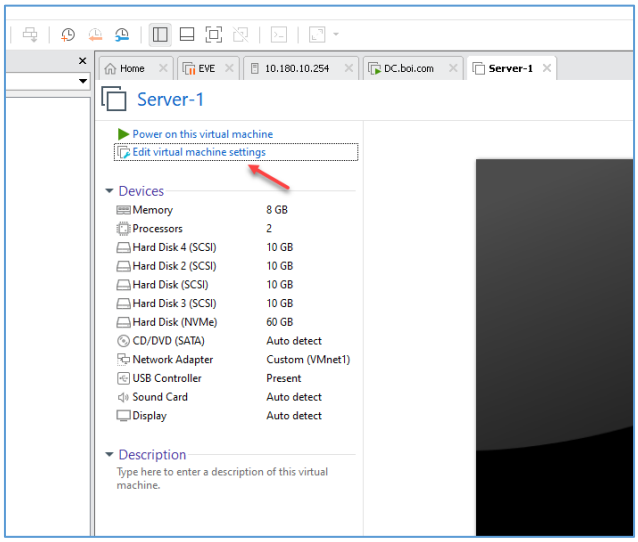
همان‌طور که در شکل ۸-۹۷۰، مشاهده می‌کنید سرویس TPM فعال نیست و باید آن را در سرور و در Bios آن فعال کنید.



شکل ۸- ۹۷۰ فعال‌سازی سرویس Bitlocker

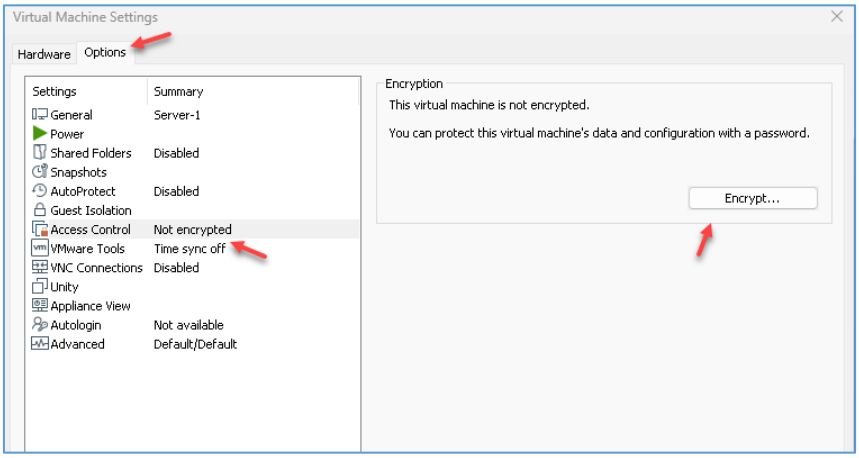
www.takbook.com

اگر از VMware Workstation استفاده می‌کنید باید ماشین مورد نظر را خاموش کنید، و به مانند شکل ۸-۹۷۱، وارد تنظیمات آن شوید.



شکل ۸- ۹۷۱ فعال‌سازی سرویس *Bitlocker*

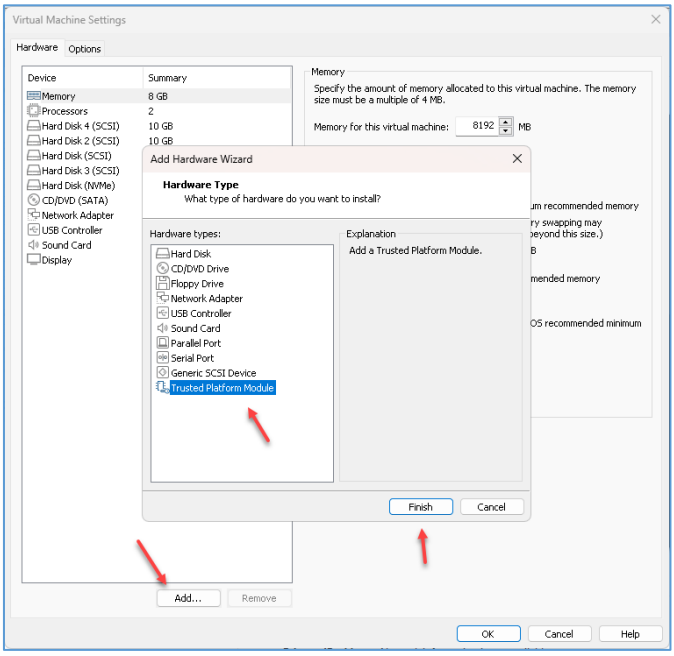
در شکل ۸-۹۷۲، وارد Options شوید و بر روی Encrypt کلیک کنید، تا فایل‌های ماشین مجازی رمزنگاری شوند.



شکل ۸- ۹۷۲ فعال‌سازی سرویس *Bitlocker*

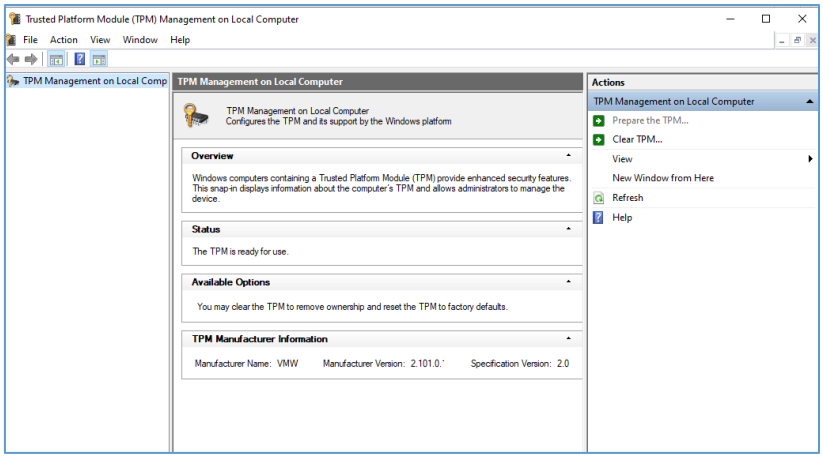
در شکل ۸-۹۷۳، وارد Hardware شوید و بر روی Add کلیک کنید و در صفحه‌ی باز شده گزینه‌ی Trusted Platform Module را انتخاب و بر روی Finish کلیک کنید.

www.takbook.com



شکل ۸- ۹۷۳ فعال‌سازی سرویس Bitlocker

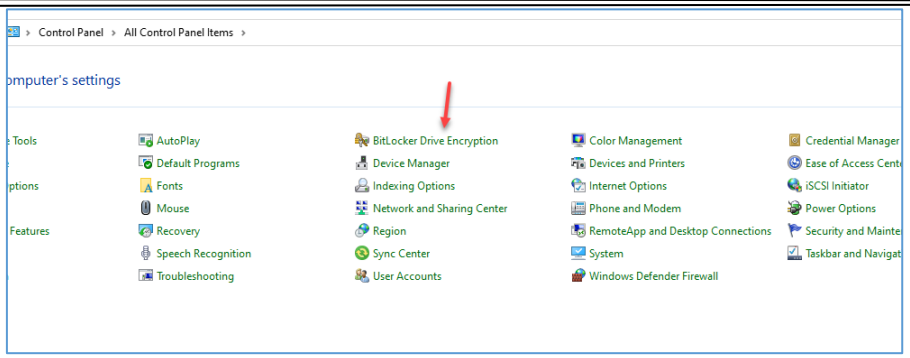
حالا وارد سرور شوید و به مانند شکل ۸-۹۷٤، سرویس TPM Administrator را اجرا کنید و همان‌طور که در شکل مشاهده می‌کنید سرویس مورد نظر به درستی فعال شده است.



شکل ۸- ۹۷۴ فعال‌سازی سرویس Bitlocker

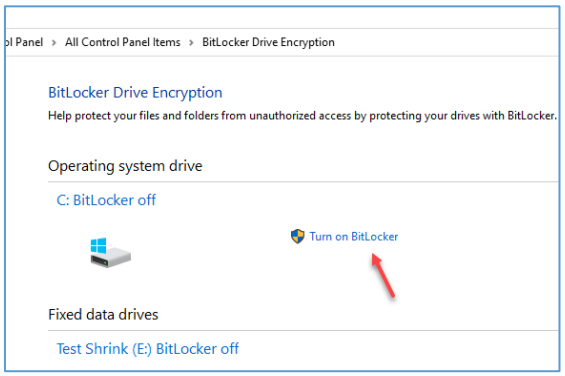
حالا دوباره وارد Control Panel می‌شویم و به مانند شکل ۸-۹۷۵، بر روی BitLocker کلیک می‌کنیم.

www.takbook.com



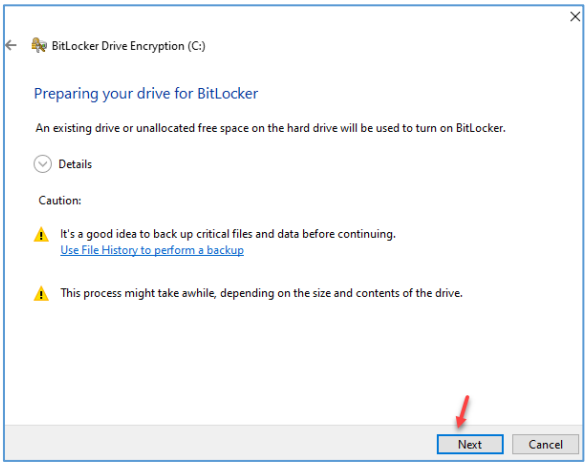
شکل ۸- ۹۷۵ فعال‌سازی سرویس *Bitlocker*

در شکل ۸-۹۷۶، بر روی Turn on BitLocker کلیک کنید.



شکل ۸- ۹۷۶ فعال‌سازی سرویس *Bitlocker*

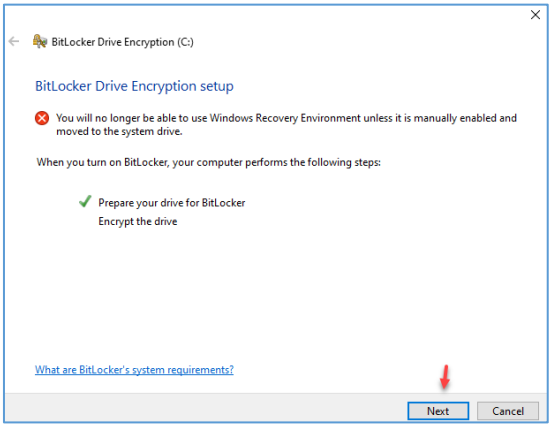
در شکل ۸-۹۷۷، بر روی Next کلیک کنید تا کار آغاز شود.



شکل ۸- ۹۷۷ فعال‌سازی سرویس *Bitlocker*

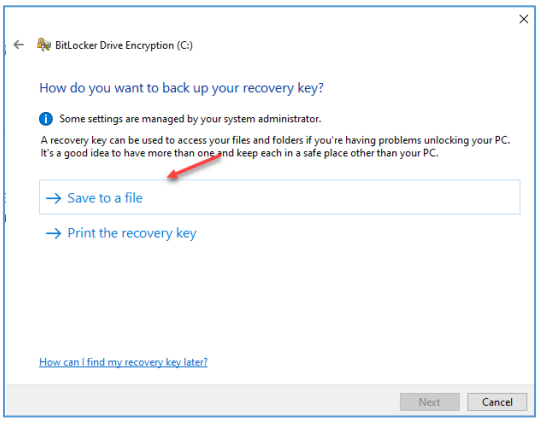
www.takbook.com

شکل ۸–۹۷۸، به این نکته اشاره دارد که باید کد ریکاوری که این سرویس به شما می‌دهد باید به صورت دستی در جای مناسب ذخیره کنید.



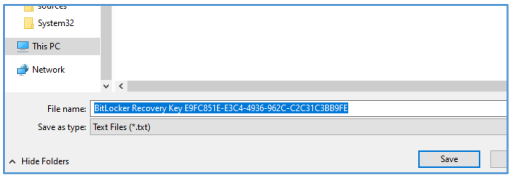
شکل ۸– ۹۷۸ فعال‌سازی سرویس Bitlocker

در شکل ۸–۹۷۹، می‌توانید فایل را Print بگیرید و یا اینکه بر روی Save to a file کلیک کنید و فایل را ذخیره کنید.



شکل ۸– ۹۷۹ فعال‌سازی سرویس Bitlocker

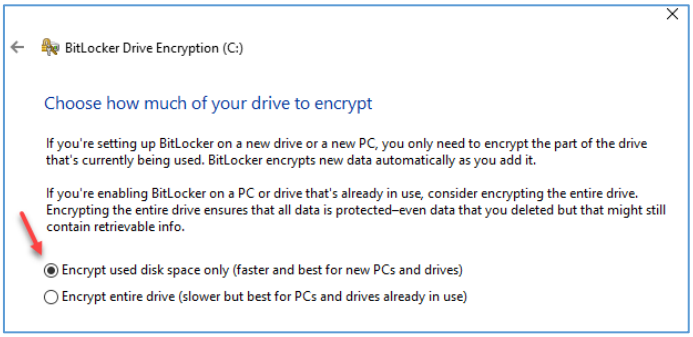
در شکل ۸–۹۸۰، باید یک پوشه در یک درایوی به غیر از C ایجاد و فایل را ذخیره کنید، توجه داشته باشید این فایل ریکاوری است و باید از آن خوب مراقبت کنید.



شکل ۸– ۹۸۰ فعال‌سازی سرویس Bitlocker

www.takbook.com

در شکل ۸-۹۸۱، گزینه‌ی اول را انتخاب کنید و طبق فضای خالی موجود عملیات Encryption در سریعترین زمان انجام خواهد شد، اگر بخواهیم کل فضای دیسک را Encrypt کنیم باید گزینه‌ی دوم را انتخاب کنیم که این کار بسیار زمان بر خواهد بود.



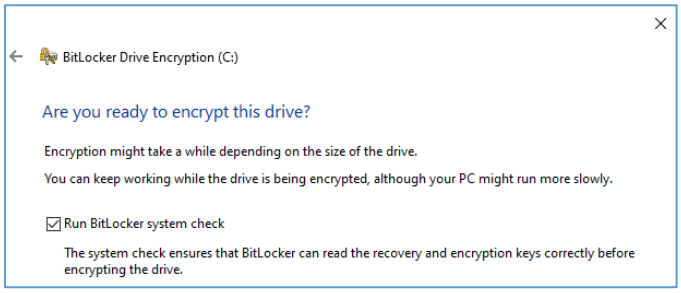
شکل ۸- ۹۸۱ فعال‌سازی سرویس Bitlocker

در شکل ۸-۹۸۲، گزینه‌ی اول را انتخاب کنید.



شکل ۸- ۹۸۲ فعال‌سازی سرویس Bitlocker

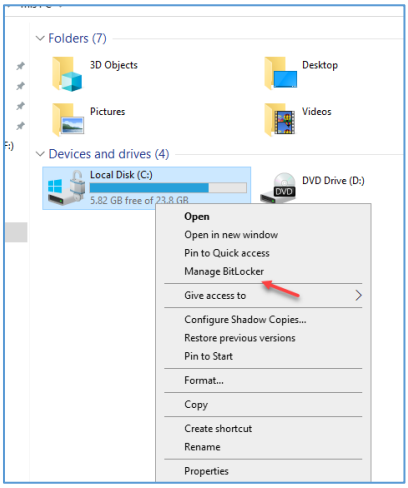
به مانند شکل ۸-۹۸۳، بر روی Contonue کلیک کنید تا کار آغاز شود.



شکل ۸- ۹۸۳ فعال‌سازی سرویس Bitlocker

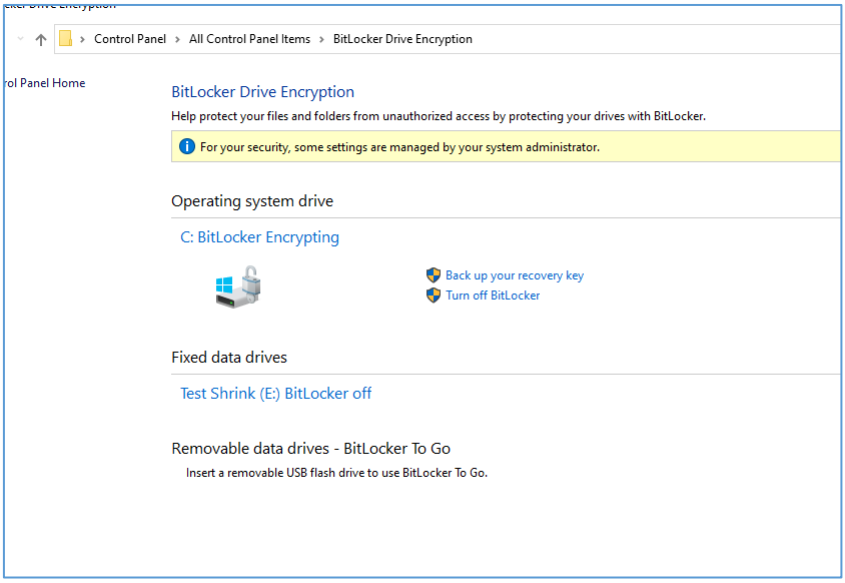
www.takbook.com

بعد از کلیک بر روی Continue سرور را باید Restart کنید، بعد از ورود به سرور به مانند شکل ۸-۹۸٤، وارد My Computer شوید که در این قسمت یک قفل در کنار آیکون درایو C مشاهده می‌کنید که نشان دهنده‌ی فعال بودن BitLocker است.



شکل ۸- ۹۸۴ فعال‌سازی سرویس Bitlocker

همان‌طور که در شکل ۸-۹۸۵، مشاهده می‌کنید دو گزینه وجود دارد یکی برای پشتیبانگیری از فایل Key و دیگری برای خاموش کردن BitLocker وجود دارد که می‌توانید از آنها استفاده کنید.



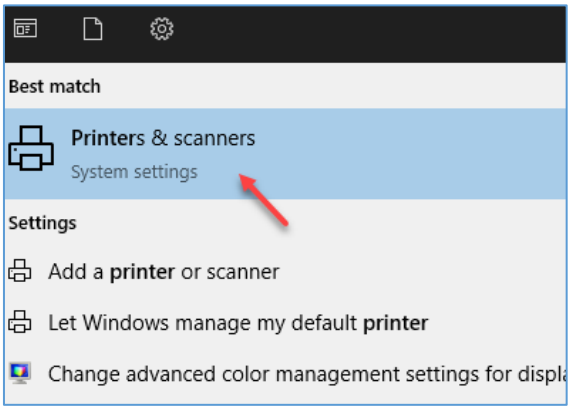
شکل ۸- ۹۸۵ فعال‌سازی سرویس Bitlocker

www.takbook.com

۸-۳-۲۷ نصب وراه اندازی Print Server

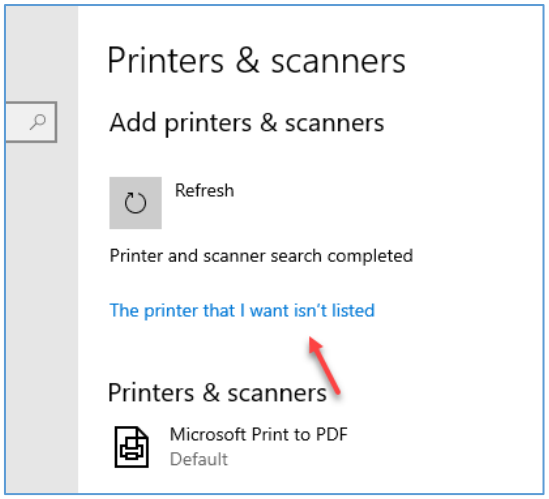
استفاده از Printer در شبکه ها یکی از مقدماتی ترین کارها در سازمان‌ها می‌باشد که استفاده گسترده‌ای از آن می‌شود، در این بخش در اول کار یک پرینتر را نصب و نحوه Share کردن آن برای دسترسی در کل شبکه را بررسی می‌کنیم.

به مانند شکل ۸-۹۸٦، وارد ویندوز سرور شوید و در قسمت Search کلمه Printers را وارد کنید و در نتیجه جستجو بر روی Device and Printers کلیک کنید.



شکل ۸- ۹۸۶ نصب وراه اندازی *Print Server*

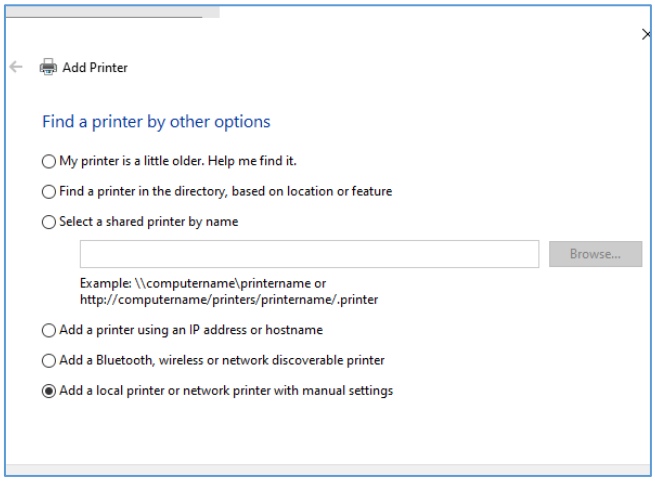
در شکل ۸-۹۸۷، باید پرینتر خود را به لیست اضافه کنیم، برای این کار بر روی Add a Printer کلیک کنید و بعد از زمانی انتظار بر روی The Printer that I want isn't listed کلیک کنید.



شکل ۸- ۹۸۷ نصب وراه اندازی *Print Server*

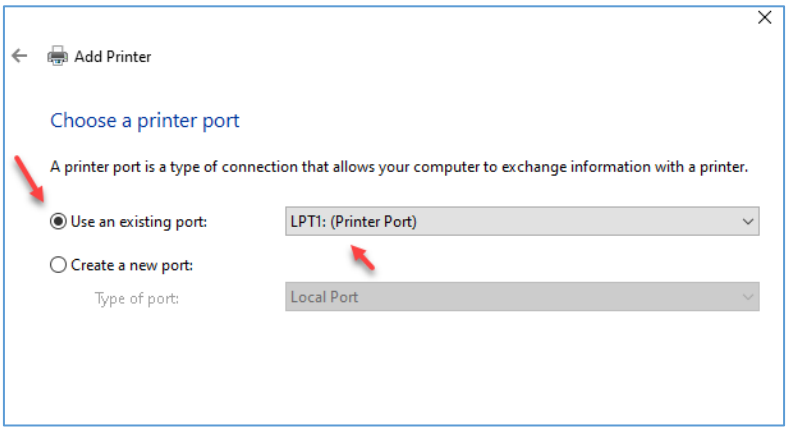
www.takbook.com

در شکل ۸-۹۸۸، گزینه‌های مختلفی برای، انتخاب Printer موردنظر قرار دارد که همه آنها را بررسی خواهیم کرد، در حال حاضر گزینه آخر را انتخاب کنید تا بتوانید یک پرینتر به صورت پیش‌فرض تعریف کنیم.



شکل ۸- ۹۸۸ نصب وراه اندازی *Print Server*

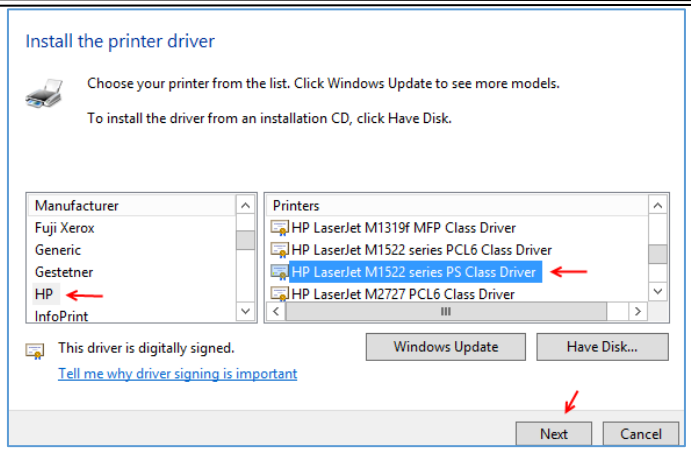
در شکل ۸-۹۸۹، گزینه اول را انتخاب و پورت LPT1 را انتخاب کنید، وبعد بر روی Next کلیک کنید.



شکل ۸- ۹۸۹ نصب وراه اندازی *Print Server*

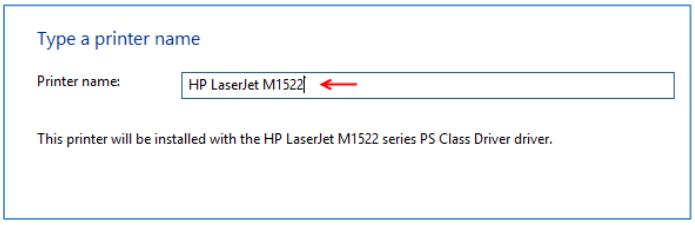
در شکل ۸-۹۹۰، نام کارخانه سازنده و مدل پرینتر را انتخاب و برروی Next کلیک کنید.

www.takbook.com



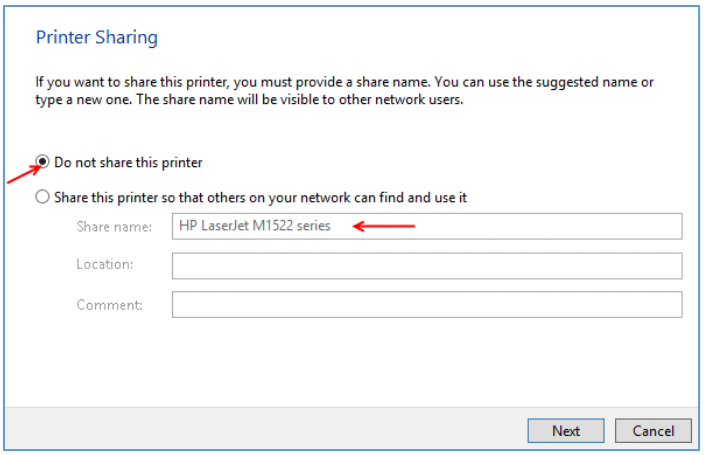
شکل ۸- ۹۹۰ نصب وراه اندازی *Print Server*

در شکل ۸-۹۹۱، نام پرینتر خود را وارد کنید و بر روی Next کلیک کنید.



شکل ۸- ۹۹۱ نصب وراه اندازی *Print Server*

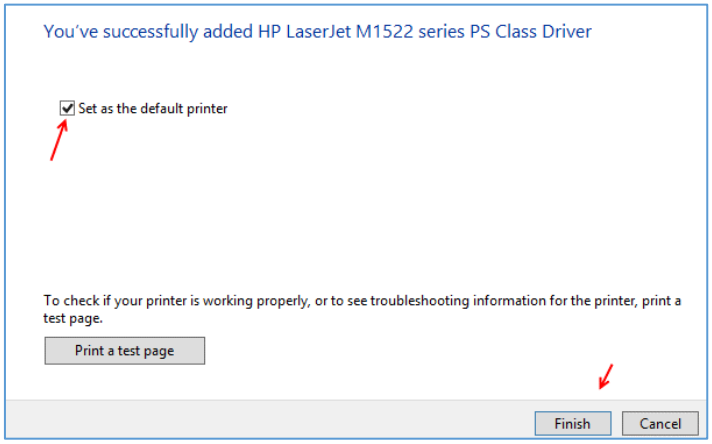
در شکل ۸-۹۹۲، که مربوط به share کردن Printer می‌باشد در حال حاضر گزینه اول را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۹۹۲ نصب وراه اندازی *Print Server*

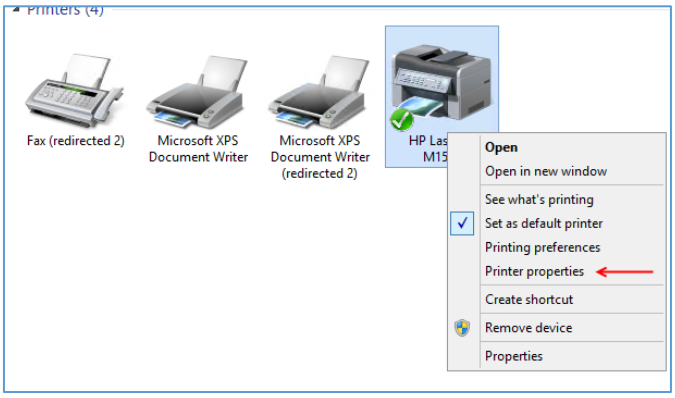
www.takbook.com

در شکل ۸-۹۹۳، تیک گزینه Set as the default printer را انتخاب تا به عنوان Printer پیش‌فرض انتخاب شود. بر روی Finish کلیک کنید تا Printer موردنظر ایجاد شود.



شکل ۸- ۹۹۳ نصب وراه اندازی *Print Server*

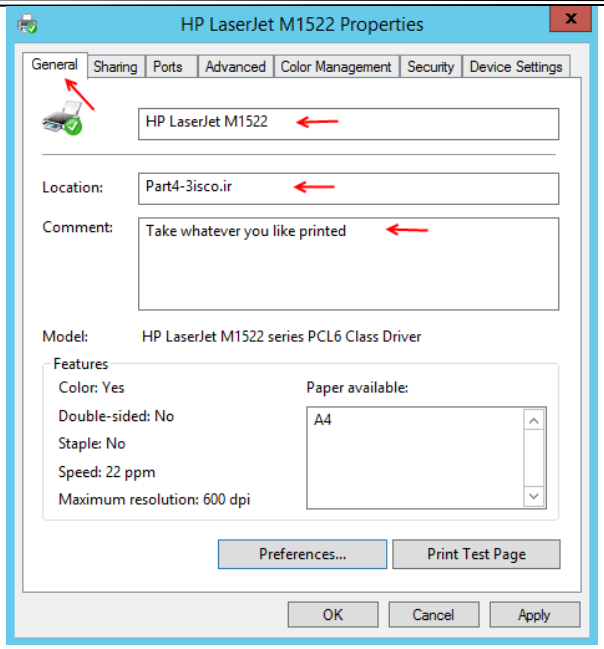
بعد از ایجاد Printer موردنظر به مانند شکل ۸-۹۹٤، بر روی آن کلیک راست کنید و گزینه‌ی Printing Properties را انتخاب کنید.



شکل ۸- ۹۹۴ نصب وراه اندازی *Print Server*

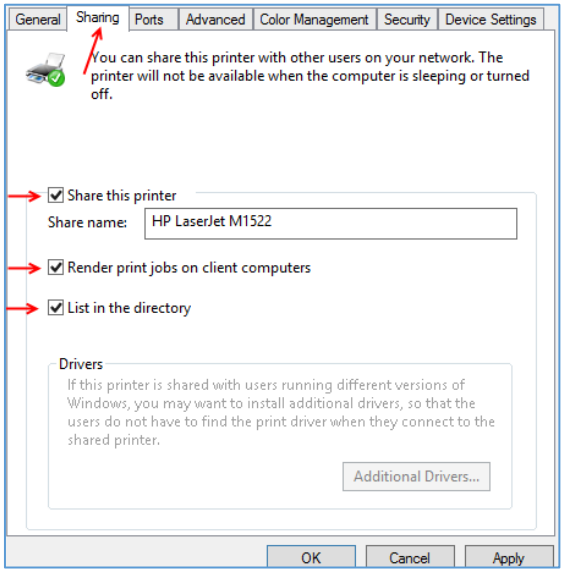
در شکل ۸-۹۹۵، وارد تب General می‌شویم، در این تب در قسمت اول می‌توانید نام Printer خود را تغییر دهید، در قسمت Location منطقه قرارگیری Printer را مشخص کنید، در قسمت Comment پیغامی را قرار دهید. در قسمت پائین صفحه با انتخاب Preferences می‌توانید اندازه کاغذ، نوع کاغذ، سیاه و سفید بودن و یا رنگی بودن و..... را می توانید مشخص کنید.

www.takbook.com



شکل ۸- ۹۹۵ نصب و راه اندازی *Print Server*

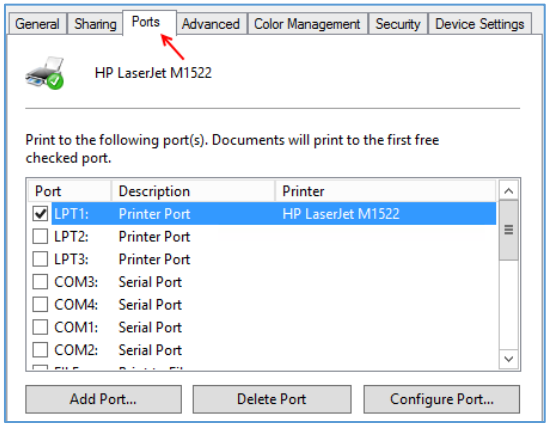
به مانند شکل ۸-۹۹۶، در تب Sharing می‌توانید Printer موردنظر خود را برای کاربران دیگر Share کنید، تیک گزینه Share this printer را انتخاب کنید و نام پرینتر خود را وارد کنید و دو گزینه دیگر درقسمت زیری آن را هم انتخاب کنید.



شکل ۸- ۹۹۶ نصب وراه اندازی *Print Server*

www.takbook.com

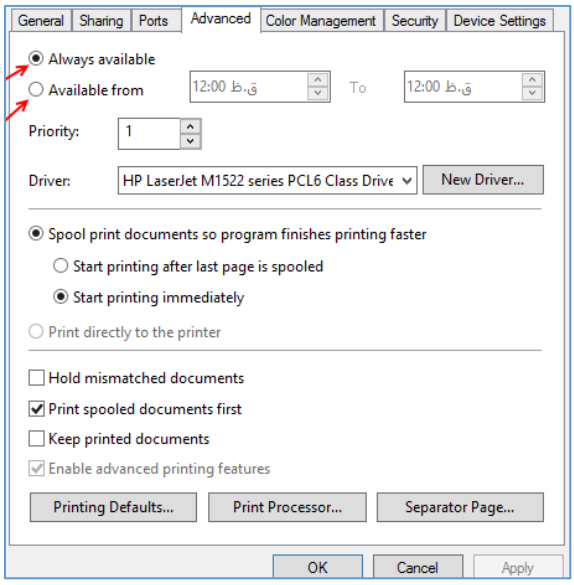
به مانند شکل ۸-۹۹۷، در تب Ports می‌توانید نوع پورت موردنظر Printer خود را تغییر دهید و یا پورت جدید تعریف کنید که زیاد هم به کار شما نخواهد آمد مگر در شرایط خاص.



شکل ۸- ۹۹۷ نصب وراه اندازی *Print Server*

به مانند شکل ۸-۹۹۸، در تب Advanced می‌توانید بر کارکرد Printer خود مدیریت داشته باشید، مثلاً اگر گزینه Always Available را انتخاب کنید دستگاه Printer در تمام ساعت آماده به کار می‌باشد. ولی اگر گزینه Available from را انتخاب کنید می‌توانید ساعت کار موردنظر خود را وارد کنید تا کاربران فقط در ساعت خاص بتوانند از این دستگاه استفاده کنند.

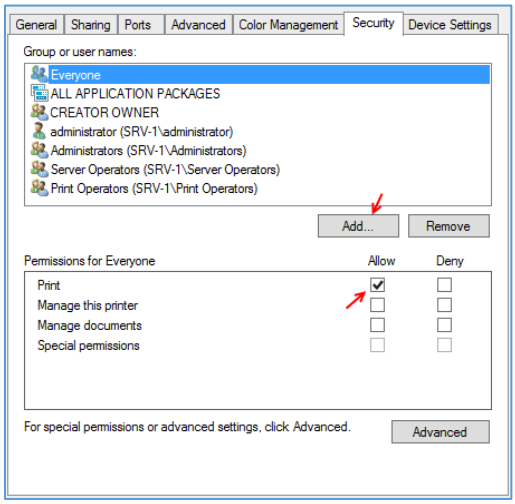
تب Color Management مربوط به تنظیمات رنگبندی دستگاه موردنظر می‌باشد که بسته به هر دستگاه متفاوت است.



شکل ۸- ۹۹۸ نصب وراه اندازی *Print Server*

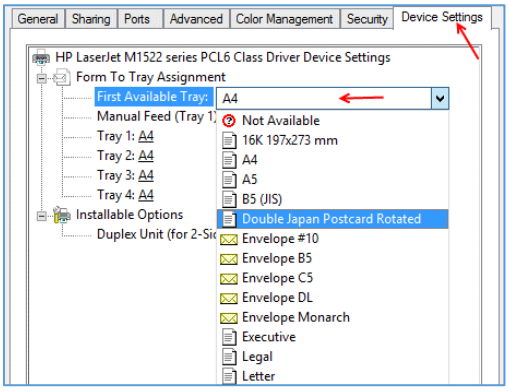
www.takbook.com

در تب Security که مهمترین قسمت می‌باشد شما می‌توانید مشخص کنید که چه کاربر و گروهی می‌تواند به Printer دسترسی داشته باشد و می‌تواند چه کاری انجام دهد، مثلاً در شکل ۸-۹۹، گروه Everyone فقط مجوز Print را دریافت کرده است و کار دیگه‌ای را نمی‌تواند انجام دهد، به این موضوع توجه کنید که تمام کاربرانی که ایجاد می‌کنید به صورت پیش‌فرض عضو گروه Everyone هستند و توانایی Print را خواهد داشت، اگر این موضوع برای شما جالب نیست و فقط می‌خواهید که کاربری را که در لیست بالا وارد می‌کنید توانایی Print داشته باشد باید گروه Everyone را از لیست حذف کنید. در لیست بالا گروهی با نام Print Operations وجود دارد که مدیریت کاملی بر روی Printer دارد و مجوز دسترسی آن Full می‌باشد و اگر یک کاربر را عضو این گروه کنید توانایی بالایی در مدیریت Printer خواهد داشت.



شکل ۸- ۹۹۹ نصب وراه اندازی *Print Server*

در تب آخر یعنی Device Settings می‌توانید اندازی کاغذ Printer را برای چاپ به مانند شکل ۸-۱۰۰۰، انتخاب کنید.

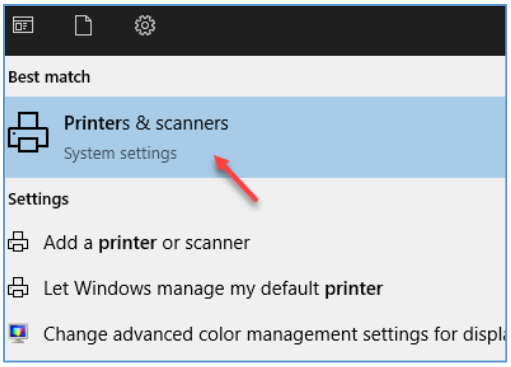


شکل ۸- ۱۰۰۰ نصب وراه اندازی *Print Server*

www.takbook.com

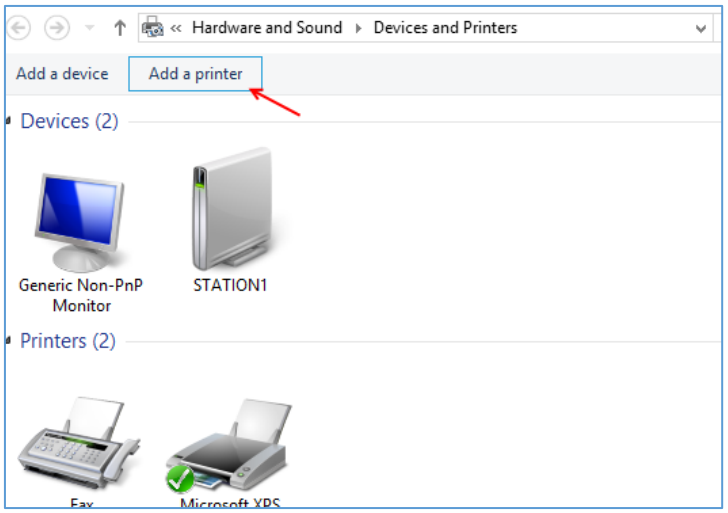
تا به اینجا Printer را نصب کردیم و با تنظیمات آن آشنا شدیم و Printer را در شبکه به اشتراک گذاشتیم، حالا می‌خواهیم از طریق کلاینت به Printer به اشتراک گذاشته شده دسترسی پیدا کنیم.

به مانند شکل ۸-۱۰۰۱، وارد Search شوید و کلمه Printers را وارد کنید و در نتایج جستجو بر روی Device and Printers کلیک کنید.



شکل ۸- ۱۰۰۱ نصب وراه اندازی *Print Server*

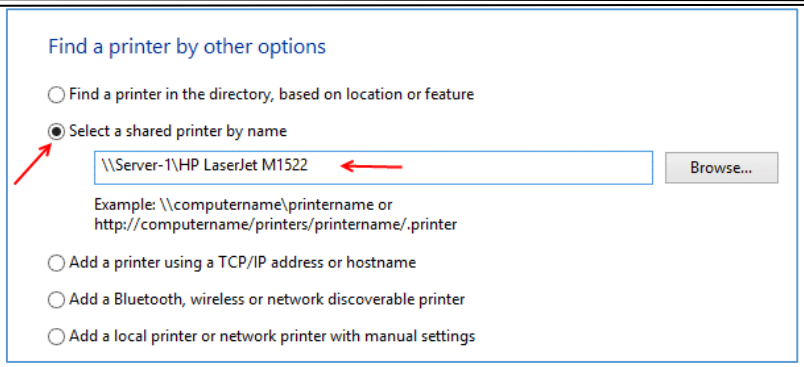
در شکل ۸-۱۰۰۲، برای اضافه کردن Printer موردنظر بر رو Add a Printer کلیک کنید.



شکل ۸- ۱۰۰۲ نصب وراه اندازی *Print Server*

در شکل ۸-۱۰۰۳، گزینه Select a shared Printer by name را انتخاب کنید و آدرس Printer موردنظر را به صورت مشخص‌شده وارد کنید، شما باید به جای Server-1 نام و یا IP سروری را وارد کنید که Printer روی آن نصب است و اگر بعد از وارد کردن اسم از بک اسلش استفاده کنید نام Printer به صورت خودکار نمایان می‌شود. برروی Next کلیک کنید.

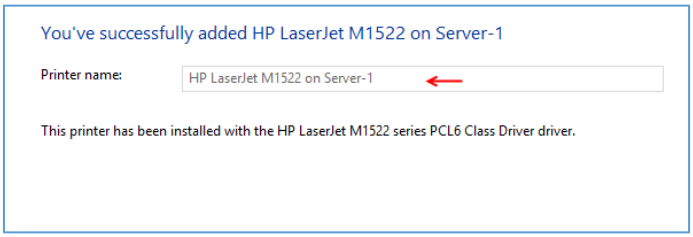
www.takbook.com



شکل ۸- ۱۰۰۳ نصب وراه اندازی *Print Server*

همان‌طور که در شکل ۸–۱۰۰٤، مشاهده می‌کنید، Printer موردنظر با موفقیت نصب شده است، بر روی Next کلیک کنید.

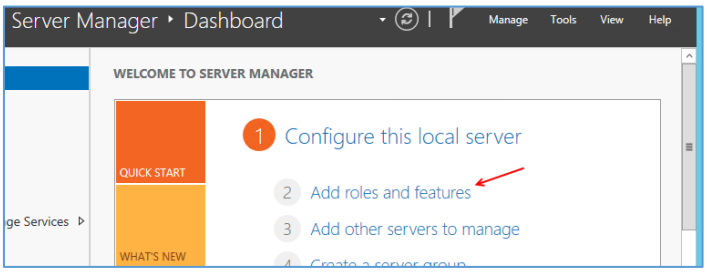
در صفحه بعد بر روی Finish کلیک کنید تا Printer موردنظر به لیست اضافه شود.



شکل ۸- ۱۰۰۴ نصب وراه اندازی *Print Server*

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

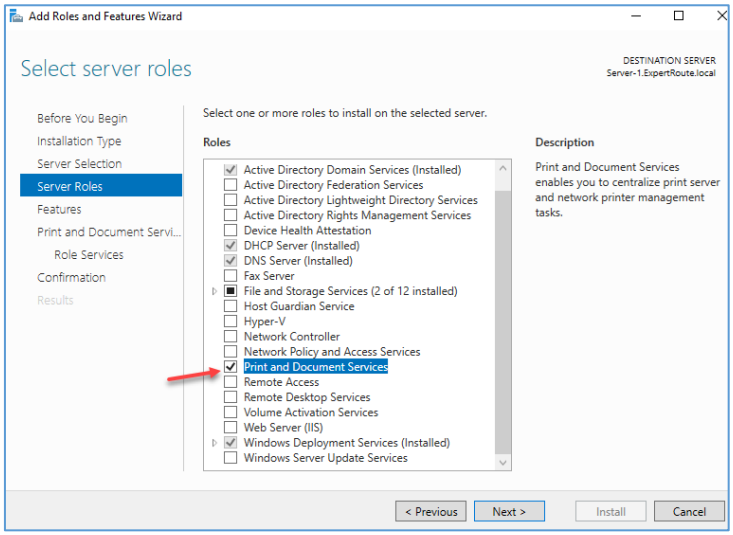
وارد ویندوز سرور شوید و Server Manager را اجرا کنید و در صفحه باز شده به مانند شکل ۸–۱۰۰۵، بر روی Add rolesand features کلیک کنید.



شکل ۸- ۱۰۰۵ نصب و راه اندازی *Print Server*

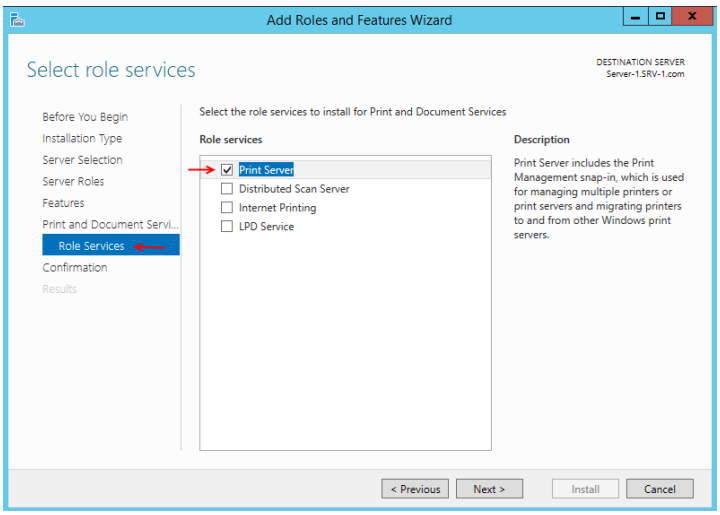
www.takbook.com

برای رسیدن به صفحه‌ی شکل۸-۱۰۰۶، باید بر روی Next کلیک کنید تا به قسمت Server Roles برسید و از لیست Roleها گزینه‌ی Print and document Services را انتخاب کند و در پنجره‌ای که باز می‌شود بر روی Add Feature کلیک کنید.



شکل ۸- ۱۰۰۶ نصب و راه اندازی Print Server

تمام قسمت‌ها را رد کنید تا به قسمت Role Service برسید که در این قسمت به مانند شکل ۸-۱۰۰۷، تیک هر دو گزینه‌ی Print Server و Internet Printing را انتخاب کنید و بر روی Next کلیک کنید، در صفحه آخر بر روی Install کلیک کنید تا سرویس موردنظر نصب شود.

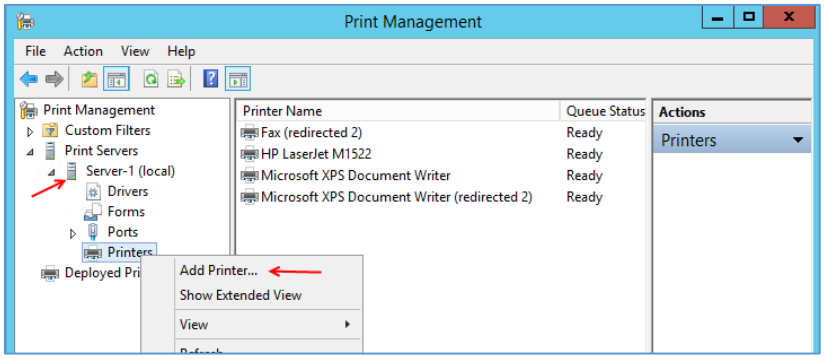


شکل ۸- ۱۰۰۷ نصب و راه اندازی Print Server

www.takbook.com

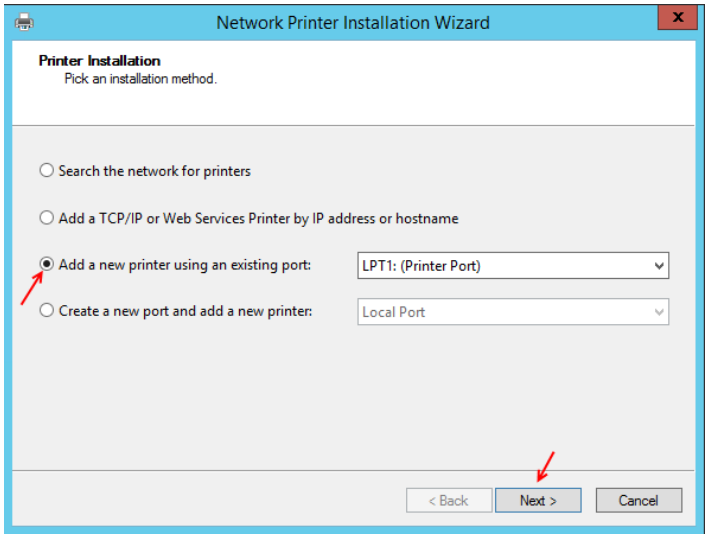
بعد ار نصب سرویس موردنظر وارد Search شوید و کلمه Print را وارد کنید و در نتایج جستجو گزینه Print Management را انتخاب کنید.

همان‌طور که در شکل ۸–۱۰۰۸، مشاهده می‌کنید سرویس موردنظر به درستی اجرا شده است و اگر از سمت چپ نام سرور خود را که در اینجا Server-1 می‌باشد انتخاب کنید و در لیست باز شده بر روی Printers کلیک کنید، باید به مانند شکل لیست Printerهای نصب شده روی سرور را مشاهده کنید. برای اضافه کردن یک Printer به لیست باید روی Priners کلیک راست کنید و گزینه Add Printer را انتخاب کنید.



شکل ۸– ۱۰۰۸ نصب و راه اندازی *Print Server*

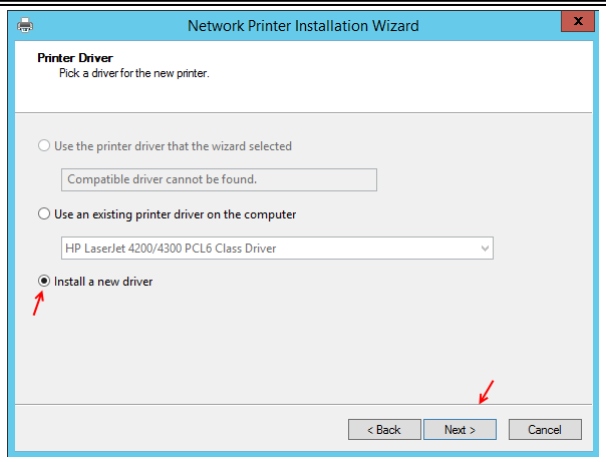
تا شکل ۸–۱۰۰۹، ظاهر شود، در این شکل به مانند قبل می‌توانید از روش‌های مختلف، پرینتر موردنظر خود را به لیست اضافه کنید، در این قسمت گزینه سوم را انتخاب و بر روی Next کلیک کنید.



شکل ۸– ۱۰۰۹ نصب و راه اندازی *Print Server*

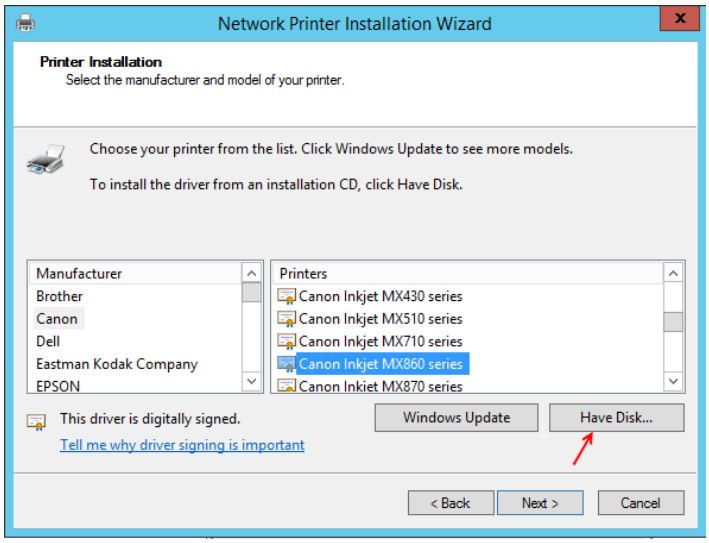
در شکل ۸–۱۰۱۰، گزینه سوم یعنی Install a new driver را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



شکل ۸- ۱۰۱۰ نصب و راه اندازی *Print Server*

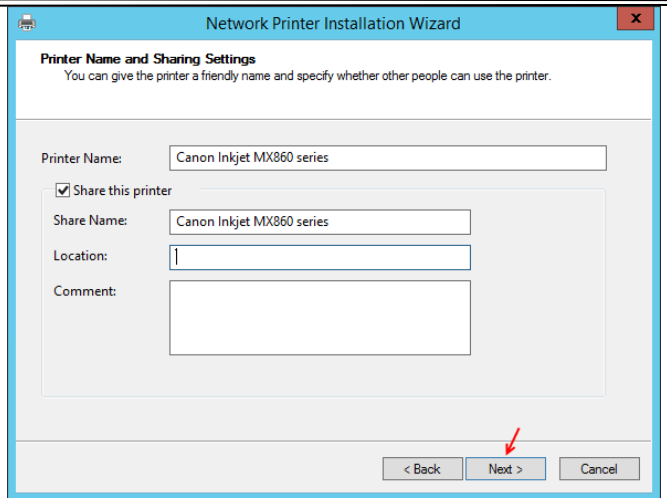
در شکل ۸-۱۰۱۱، می‌توانید نام کارخانه سازنده به همراه مدل Printer را در صورت موجود بودن انتخاب کنید و یا اگر CD یا DVD مربوط به پرینتر موردنظر را در اختیار دارید، بر روی Have Disk کلیک کنید و درایور موردنظر را به برنامه معرفی کنید.



شکل ۸- ۱۰۱۱ نصب و راه اندازی *Print Server*

در شکل ۸-۱۰۱۲، می‌توانیم نام Printer خود را مشاهده و یا ویرایش کنید، اگر می‌خواهید Printer موردنظر را در شبکه Share کنید تیک گزینه Share this printer را انتخاب کنید و در قسمت Share Name نام Printer خود را زمانی که share می‌شود را وارد کنید در قسمت Location هم محل قرارگیری Printer را وارد کنید و بر روی Next کلیک کنید.

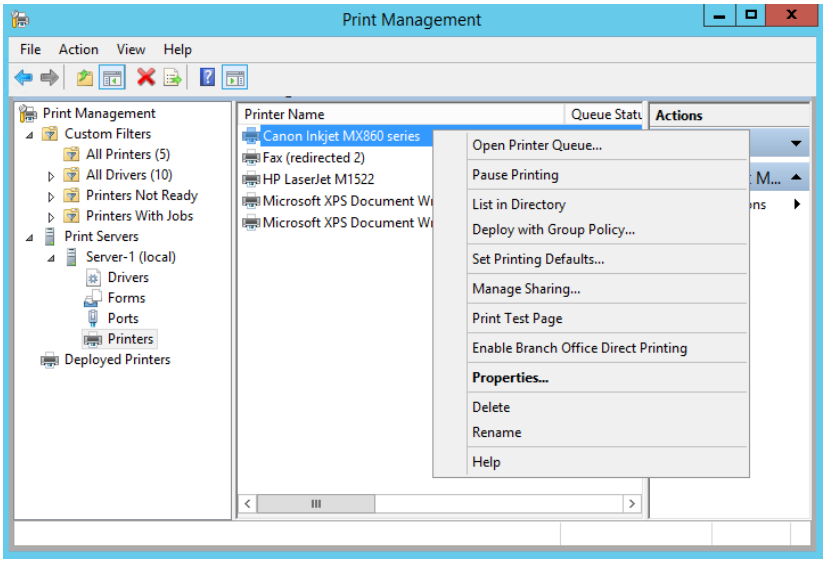
www.takbook.com



شکل ۸- ۱۰۱۲ نصب و راه اندازی *Print Server*

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

بعد از ایجاد Printer به مانند شکل ۸-۱۰۱۳، بر روی آن کلیک راست کنید، در منوی باز شده یک سری امکانات در اختیار شما قرار می‌دهد.



شکل ۸- ۱۰۱۳ نصب و راه اندازی *Print Server*

بعد از اینکه پرینتر مورد نظر ایجاد کردید می‌توانید وارد آدرس اینترنتی شوید و اطلاعات پرینترهای به اشتراک گذاشته شده را ببینید.

www.takbook.com

۲۸-۳-۸ کار با File Server Resource Manager (FSRM)

File Server Resource Manager (FSRM) یکی از ابزارهای مدیریتی قدرتمند در ویندوز سرور است که برای مدیریت، نظارت و کنترل فایل‌ها و فضای دیسک در فایل سرورها استفاده می‌شود. این ابزار به مدیران شبکه امکان می‌دهد تا فضای ذخیره‌سازی را بهینه‌سازی کرده و دسترسی به فایل‌ها را بر اساس سیاست‌های سازمانی محدود کنند.

قابلیت‌های کلیدی FSRM

- مدیریت سهمیه‌ها (Quota Management)

تنظیم محدودیت‌های فضا برای پوشه‌ها یا درایوها، ایجاد هشدار در صورت نزدیک شدن به محدودیت فضای تعیین‌شده و اعمال سیاست‌های خودکار برای جلوگیری از تجاوز از سهمیه.

- فیلترهای فایل (File Screening)

محدود کردن انواع فایل‌هایی که کاربران می‌توانند روی سرور ذخیره کنند (مانند جلوگیری از ذخیره فایل‌های MP3 یا ویدئو).

- ایجاد استثنا برای کاربران یا گروه‌ها.
- مدیریت گزارش‌ها (Storage Reports Management)

تولید گزارش‌هایی از مصرف فضا، فایل‌های قدیمی، فایل‌های بزرگ و غیره و کمک به شناسایی رفتارهای غیرعادی یا ناکارآمد در استفاده از فضای ذخیره‌سازی.

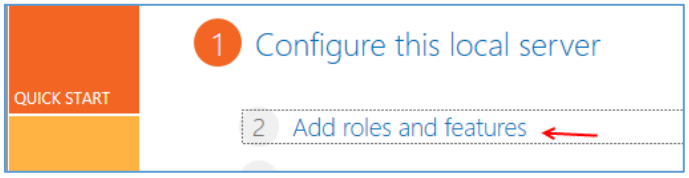
- طبقه‌بندی فایل‌ها (File Classification)

سازمان‌دهی فایل‌ها بر اساس متادیتا و ویژگی‌های تعریف‌شده، خودکارسازی فرآیند دسته‌بندی برای مدیریت بهتر اطلاعات.

- مدیریت وظایف (File Management Tasks)

خودکارسازی عملیات مختلف مانند انتقال یا حذف فایل‌ها بر اساس معیارهای خاص.

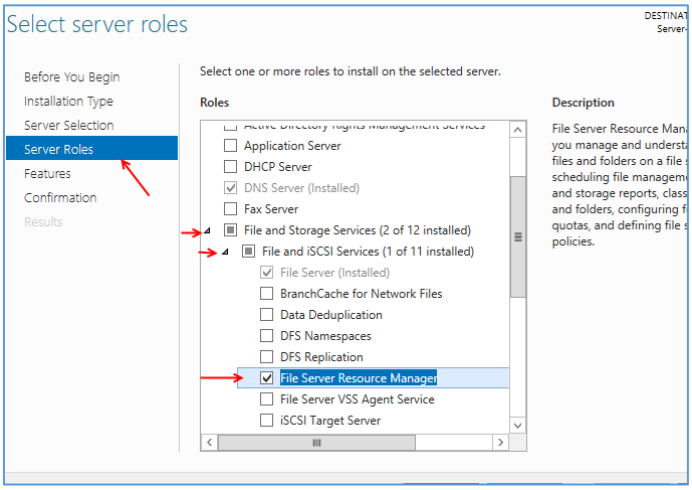
برای شروع کار به مانند شکل ۸-۱۰۱٤، Server Manager را اجرا کنید بر روی Add Roles and Features کلیک کنید.



شکل ۸-۱۰۱۴ *File Server Resource Manager (FSRM)*

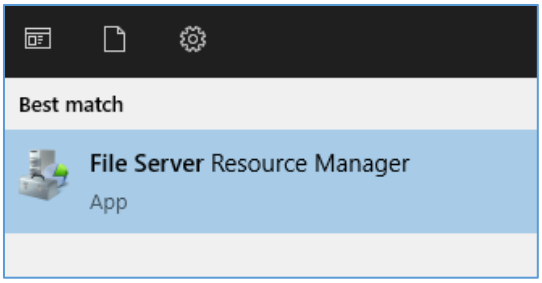
www.takbook.com

بر روی Next کلیک کنید تا به قسمت Server Roles برسید، در شکل ۸–۱۰۱۵، اول File and Storage… و بعد File and iSCSI… را انتخاب کنید و در زیر مجموعه آن گزینه File Server Resource Manager را انتخاب کنیدو بر روی Next کلیک کنید.



شکل ۸- ۱۰۱۵ File Server Resource Manager (FSRM)

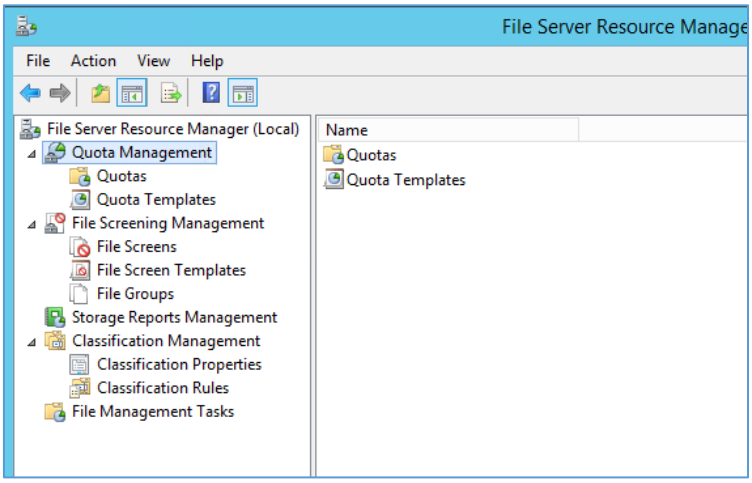
بعد از نصب سرویس به مانند شکل ۸–۱۰۱۶، وارد Search شوید و File Server Resource Manager را وارد کنید و گزینه موردنظر را انتخاب کنید.



شکل ۸- ۱۰۱۶ File Server Resource Manager (FSRM)

همان‌طور که در شکل ۸–۱۰۱۷، مشاهده می‌کنید سرویس موردنظر به درستی اجرا شده است این سرویس از قسمت‌های مختلفی مانند Quota, Screening,… تشکیل شده است که با هم این قسمت‌ها را بررسی می‌کنیم.

www.takbook.com

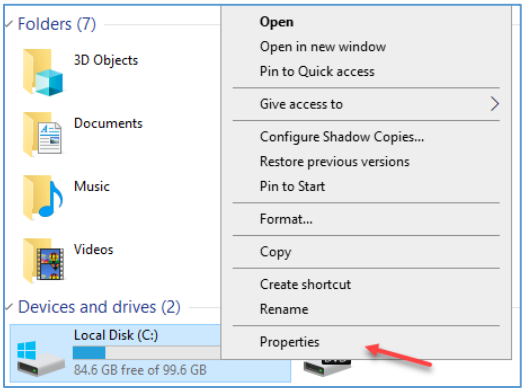


شکل ۸- ۱۰۱۷ File Server Resource Manager (FSRM)

کار با Quota Management

Quota قابلیتی در ویندوز می‌باشد که از طریق آن می‌توانید فضای هارد دیسک را برای کاربران محدود کنید تا کاربر نتواند بیشتر از آن، از فضای هارد دیسک استفاده کند، در این سرویس اگر فضای کاربر به حد موردنظر نزدیک شود، این سرویس به روش‌های مختلف به شما اخطار خواهد داد.

برای شروع به مانند شکل ۸-۱۰۱۸، وارد My Computer شوید و بر روی یکی از درایوهای خود کلیک راست کنید و گزینه Properties را انتخاب کنید.



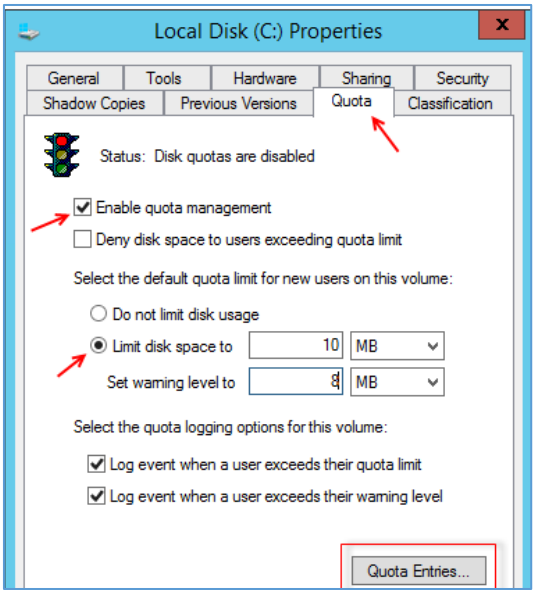
شکل ۸- ۱۰۱۸ کار با Quota Management

تذکر مهم: برای استفاده از این قابلیت، پارتیشن موردنظر حتماً باید از نوع NTFS باشد.

در شکل ۸-۱۰۱۹، وارد تب Quota شوید و برای فعال کردن این قابلیت گزینه Enable quota management انتخاب کنید. برای محدود کردن فضای دیسک باید گزینه Limit disk Space to را انتخاب کنید و حجم موردنظر خود را وارد کنید که در اینجا ۱۰ مگابایت وارد شده است یعنی اینکه کاربر می‌تواند تا همین

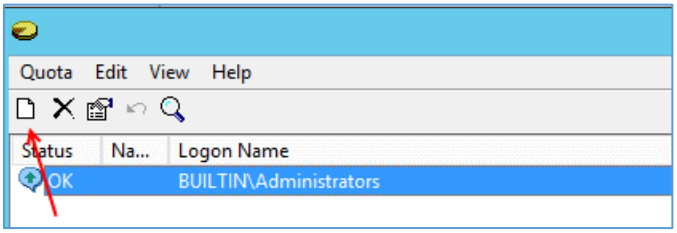
www.takbook.com

مقدار از فضای دیسک استفاده کند، در قسمت Set warning level to اگر کاربر از ۸ مگابایت فضای دیسک استفاده کرد یک اخطار برای مدیر شبکه ارسال خواهد شد. دو گزینه آخر صفحه را انتخاب کنید تا Log برای مدیر شبکه ارسال شود، حالا چگونه می‌توان این فضا را به یک کاربر خاص نسبت داد، برای این کار باید بر روی گزینه Quota Entries کلیک کنید.



شکل ۸- ۱۰۱۹ کار با *Quota Management*

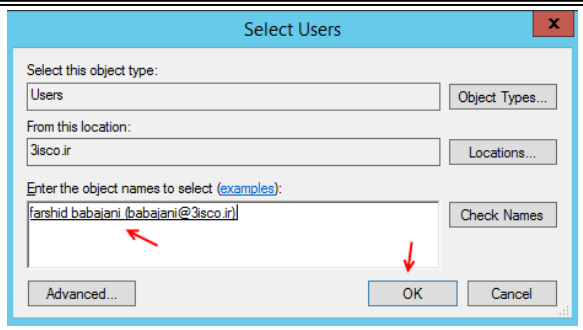
در شکل ۸–۱۰۲۰، برای اینکه مقدار فضای خود را به یک کاربر نسبت دهیم باید بر روی آیکون New Quota کلیک کنید.



شکل ۸- ۱۰۲۰ کار با *Quota Management*

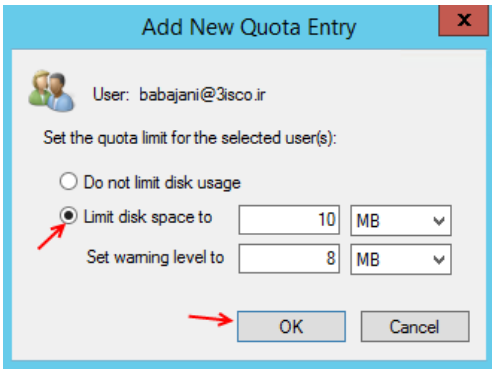
در شکل ۸–۱۰۲۱، کاربر موردنظر خود را به لیست اضافه می‌کنیم، برای این کار می‌توانید از گزینه Advanced استفاده کنید، بعد از اضافه کردن کاربر موردنظر بر روی ok کلیک کنید.

www.takbook.com



شکل ۸- ۱۰۲۱ کار با *Quota Management*

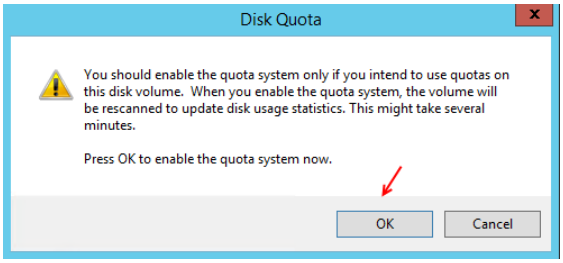
در شکل ۸-۱۰۲۲، مقدار فضای موردنظر را برای کاربر موردنظر مشخص می‌کنیم، در این قسمت کاربر نمی‌تواند بیش از 10 مگابایت از فضای هارد دیسک استفاده کند، البته اگر کاربر به مرز ۸ مگابایت رسید یک اخطار برای کاربر موردنظر ارسال می‌شود.



شکل ۸- ۱۰۲۲ کار با *Quota Management*

بر روی ok کلیک کنید تا اطلاعات ثبت شود، بعد از آن صفحه موردنظر را ببندید و در صفحه Properties بر روی ok کلیک کنید.

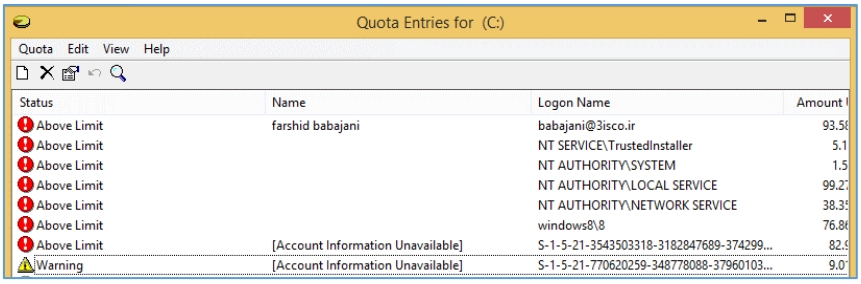
زمانی که در صفحه قبل بر روی ok کلیک کردید، شکل ۸-۱۰۲۳، ظاهر می‌شود که، به شما این اخطار را می‌دهد که سرویس Quota را روی درایو سیستمی می‌خواهید فعال کنید که این کار درستی نخواهد بود، چون بعد از اینکه بر روی ok کلیک کنید صفحه‌ای شبیه به شکل زیر را مشاهده خواهید کرد.



شکل ۸- ۱۰۲۳ کار با *Quota Management*

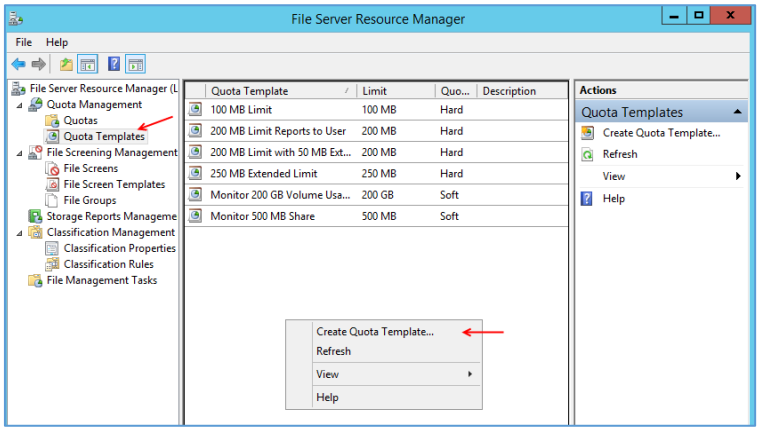
www.takbook.com

شکل ۸-۱۰۲٤، مربوط به Quota Entries می‌باشد که با هم کاربر خود را به آن اضافه کردیم، همان‌طور که مشاهده می‌کنید سرویس‌هایی که از منابع سرور استفاده می‌کردند محدود شده‌اند و این نشان دهنده‌ی این است که نباید Quota را روی درایو سیستم که اصولاً درایو C است فعال کنیم، پس این نکته را هیچ وقت فراموش نکنید.



شکل ۸- ۱۰۲۴ کار با *Quota Management*

بعد از این که سرویس Quota را روی درایو موردنظر بررسی کردیم دوباره وارد سرویس File Server Resource می‌شویم و به مانند شکل ۸-۱۰۲۵، از سمت چپ گزینه Quota Templates را انتخاب کنید و در صفحه باز شده کلیک راست کنید و گزینه Creat Quota Templates را انتخاب کنید.



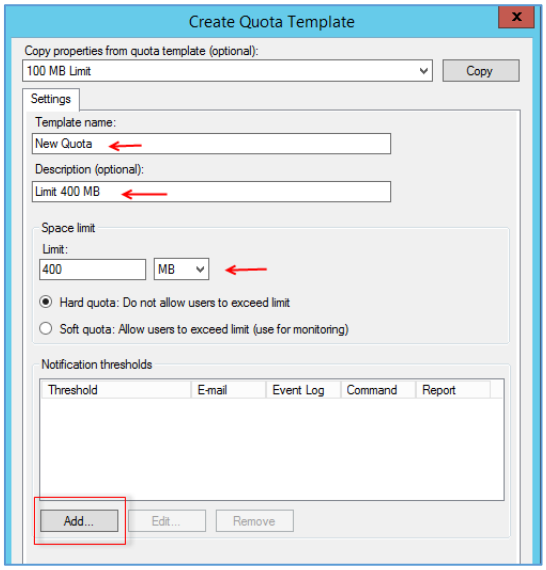
شکل ۸- ۱۰۲۵ کار با *Quota Management*

در این قسمت می‌خواهیم یک Quota Template ایجاد کنیم و یک مقدار خاص را به آن اختصاص دهیم و از طریق Quota به یک درایو و یا پوشه موردنظر اختصاص دهیم.

در شکل ۸-۱۰۲٦، در قسمت Template Name نام دلخواه خود را وارد کنید و در قسمت Description توضیحات آن را وارد کنید. در بخش Space limit باید در فیلد Limit حداکثر فضای مصرفی را وارد کنید و در جلوی آن یکی از مقادیر ....,MB,GB را انتخاب کنید که در اینجا 400 MB وارد شده است. دو گزینه Hard Quota و Soft Quota وجود دارد که در این قسمت گزینه Hard Quota را انتخاب کنید.

www.takbook.com

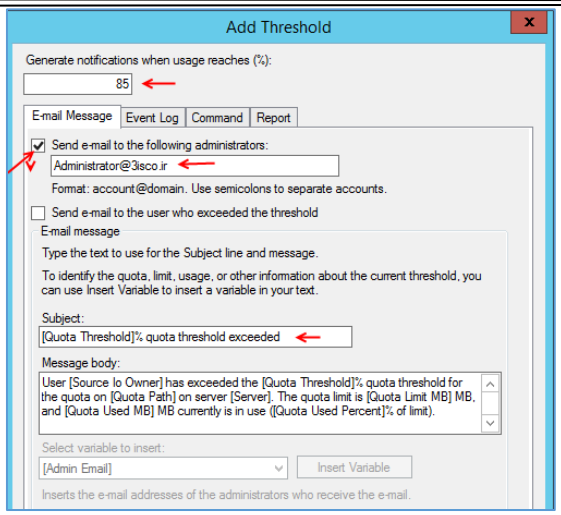
Hard Quota یعنی اینکه یک کاربر نمی‌تواند بیشتر از حجم مورد استفاده کند ولی گزینه Soft Quota به این منظور است که زمانی کاربر بیشتر از حجم موردنظر استفاده کرد، برای شما فقط اخطار ارسال می‌شود. در این قسمت Hard Quota را انتخاب کنید، در قسمت Notification Thresholds باید یک سری Log به مجموعه اضافه کنیم که مثلاً اگر حجم مصرفی به 85% رسید به مدیر شبکه ایمیل ارسال شود و یا Log ارسال شود، این روش‌ها برای Monitoring شبکه بسیار مهم می‌باشند و مدیر شبکه باید این توانایی را در اشکال‌زدایی مشکلات توسط Log داشته باشد، برای این کار بر روی Add کلیک کنید.



شکل ۸- ۱۰۲۶ کار با *Quota Management*

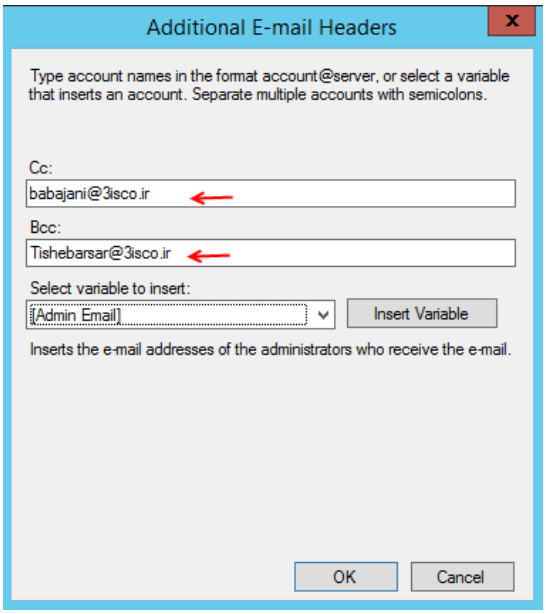
در شکل ۸-۱۰۲۷، وارد تب E-mail Message شوید، در قسمتی که 85 نوشته به این منظور است که زمانی که کاربر از 85 درصد کل فضای ٤٠٠ مگابایت استفاده کرد کارهای زیر آن انجام بگیرد یعنی اینکه تیک گزینه Send e-mail... را انتخاب کنید و ایمیل مدیر شبکه را وارد کنید، البته باید سرویس SMTP از قبل فعال شده باشد، در قسمت Subject عنوان ایمیل را وارد می‌کنید که به جای Quota Thresholds مقدار 85% قرار خواهد گرفت، در قسمت Message body هم اطلاعات مربوط به Quota قرار دارد که به همراه ایمیل ارسال خواهد شد، برای اینکه این اطلاعات به ایمیل‌های دیگر ارسال شود باید بر روی Additional E-mail Headers کلیک کنید.

www.takbook.com



شکل ۸- ۱۰۲۷ کار با *Quota Management*

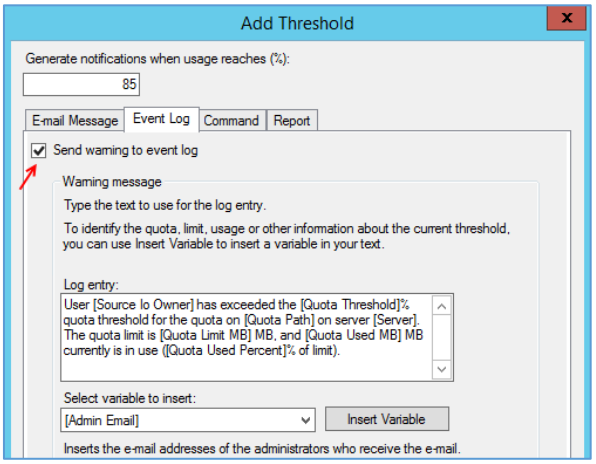
در شکل ۸–۱۰۲۸، باید ایمیل‌های دیگر خود را در قسمت CC, Bcc وارد کنید، برای اضافه کردن یک Variable جدید بر روی Insert Variable کلیک کنید، بر روی ok کلیک کنید تا اطلاعات ثبت شود.



شکل ۸- ۱۰۲۸ کار با *Quota Management*

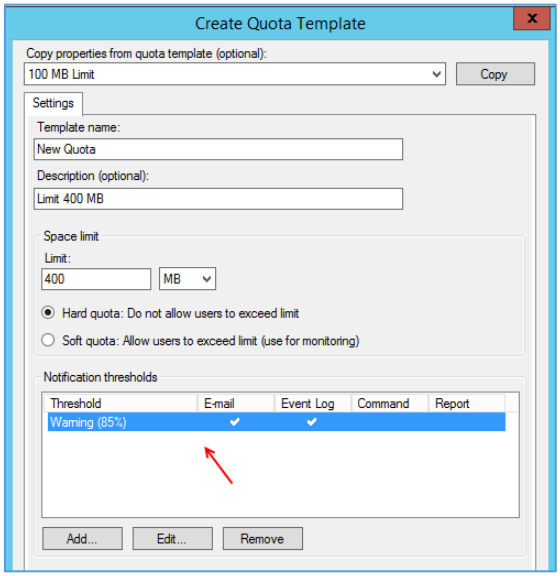
به مانند شکل ۸–۱۰۲۹، در تب Event Log با فعال کردن Send warning to event log و انتخاب Log entry مشخص برای شما Log فرستاده می‌شود، تب Command هم برای اجرای Script مشخص است و تب Report هم برای ارسال گزارش با جزئیات مشخص به ایمیل خاص است.

www.takbook.com



شکل ۸- ۱۰۲۹ کار با *Quota Management*

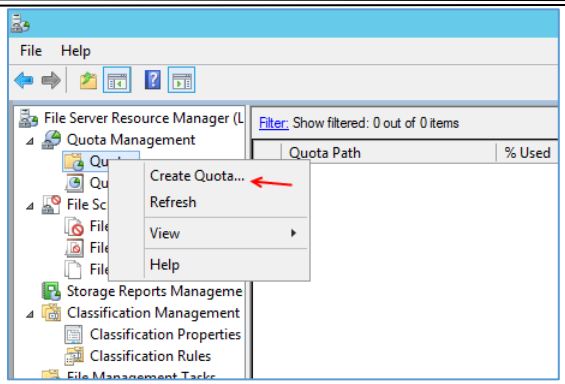
همان‌طور که در شکل ۸-۱۰۳۰، مشاهده می‌کنید Notification موردنظر به لیست اضافه شده که عدد آن 85% را نشان می‌دهد که ما از قبل این موضوع را مشخص کردیم، بر روی ok کلیک کنید تا Quota Template موردنظر ایجاد شود.



شکل ۸- ۱۰۳۰ کار با *Quota Management*

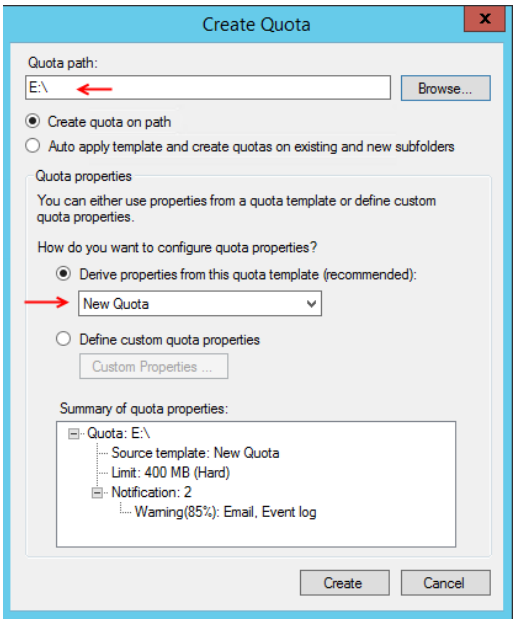
بعد از ایجاد Quota Template به مانند شکل ۸-۱۰۳۱، از سمت چپ بر روی Quota کلیک کنید و بر روی آن کلیک راست کنید و گزینه Create Quota را انتخاب کنید.

www.takbook.com



شکل ۸- ۱۰۳۱ کار با *Quota Management*

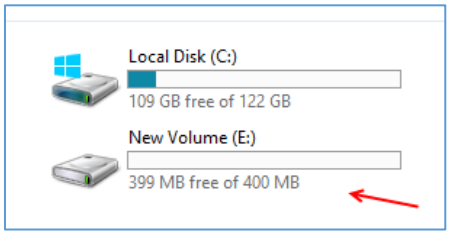
در شکل ۸-۱۰۳۲، در قسمت Quota Path باید درایو و وفولدری را که می‌خواهید Quota روی آن اجرا شود را انتخاب کنید که در اینجا درایو E انتخاب شده است، در قسمت Derive properties from this.... باید همان Quota Template را انتخاب کنید که در مرحله قبل ایجاد کرده بودیم که بعد از انتخاب New Quota اطلاعات آن در قسمت Summary of Quota نمایش داده شده است، بر روی Create کلیک کنید تا Quota موردنظر ایجاد شود و درایو موردنظر محدود شود.



شکل ۸- ۱۰۳۲ کار با *Quota Management*

همان‌طور که در شکل ۸-۱۰۳۳، مشاهده می‌کنید درایو E محدود شده است و فقط ٤٠٠ مگابایت حجم قابل استفاده دارد.

www.takbook.com

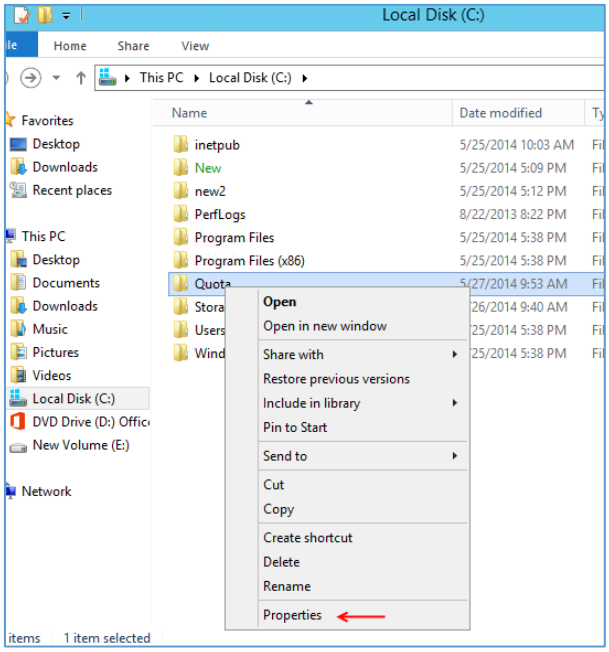


شکل ۸- ۱۰۳۳ کار با *Quota Management*

۸-۳-۲۸-۱ ایجاد درایو از طریق شبکه و محدود کردن کاربران آن

یکی از بیشترین کاربردهای استفاده از شبکه در سازمان‌های بزرگ ایجاد درایو از طریق شبکه برای تمام کاربران است، در این قسمت می‌خواهیم یک درایو شبکه‌ای ایجاد کنیم و کاربران را محدود کنیم تا فقط از حجم مشخصی استفاده کنند، برای شروع باید یک پوشه در یکی از درایوهای سرور ایجاد کنیم البته می‌توان این کار را روی یک درایو هم انجام داد.

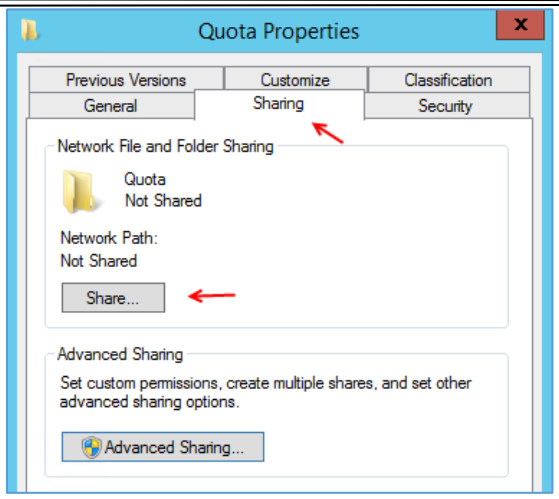
به مانند شکل ۱۰-۳٤، وارد درایو C می‌شویم و یک پوشه با نام Quota ایجاد می‌کنیم، البته شما می‌توانید با هر اسمی این پوشه را ایجاد کنید، بر روی آن کلیک راست می‌کنیم و گزینه Properties ر انتخاب می‌کنیم.



شکل ۸- ۱۰۳۴ ایجاد درایو از طریق شبکه و محدود کردن کاربران

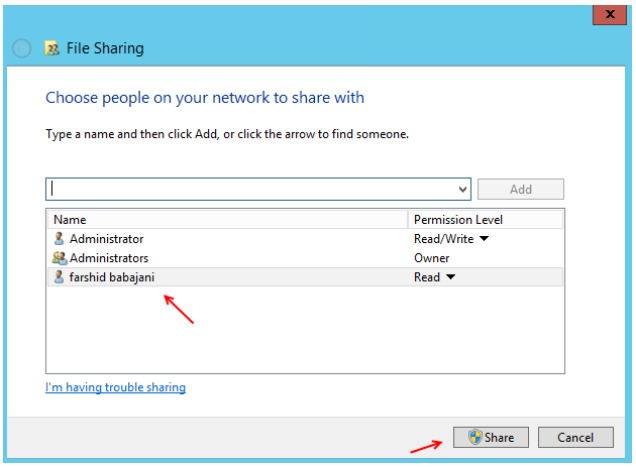
شکل ۸-۱۰۳۵، وارد تب Sharing شوید و گزینه Share را انتخاب کنیدتا شکل بعد ظاهر شود.

www.takbook.com



شکل ۸- ۱۰۳۵ ایجاد درایو از طریق شبکه و محدود کردن کاربران

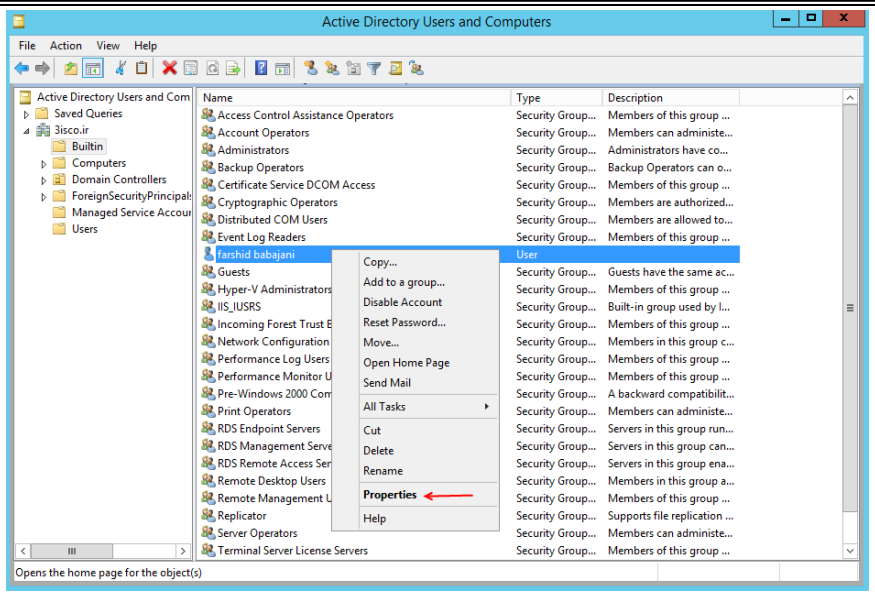
در شکل ۸-۱۰۳۶، باید کاربر خود را با کلیک بر روی Add به لیست اضافه کنید و توانایی Read را به آن بدهید و بعد بر روی Share کلیک کنید.



شکل ۸- ۱۰۳۶ ایجاد درایو از طریق شبکه و محدود کردن کاربران

بعد از انجام کارهای مشخص‌شده بالا، به مانند شکل ۸-۱۰۳۷، وارد Active Directory Users and Computer شوید و بر روی کاربر موردنظر خود کلیک راست کنید و گزینه Properties را انتخاب کنید.

www.takbook.com

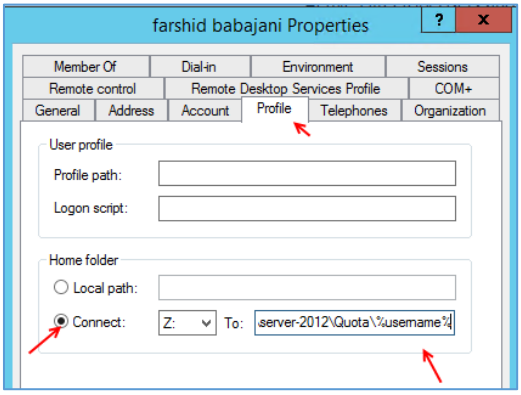


شکل ۸- ۱۰۳۷ ایجاد درایو از طریق شبکه و محدود کردن کاربران

در شکل ۸-۱۰۳۸، وارد تب Profile شوید و گزینه Connect را انتخاب کنید و یکی از نام‌های درایو را مثلاً Z را انتخاب کنید و در جلوی آن آدرس زیر را وارد کنید:

\\Server-2012\Quota\%username%

در این دستور به جای Server-2012 باید نام سرور خود را وارد کنید و به جای Qouta باید نام پوشه خودتان را وارد کنید، در قسمت آخر می‌توانید نام کاربر را وارد کنید و یا %username% وارد کنید. بر روی ok کلیک کنید تا اطلاعات ثبت شود.



شکل ۸- ۱۰۳۸ ایجاد درایو از طریق شبکه و محدود کردن کاربران

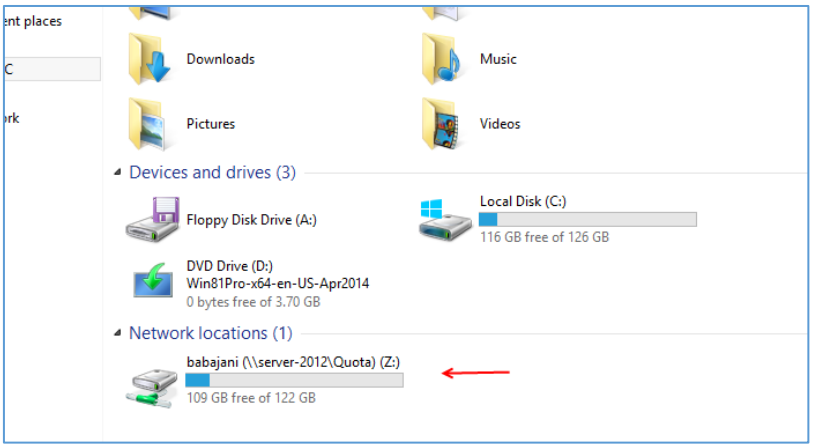
بعد از آن با کاربر موردنظر وارد یکی از کلاینت‌ها می‌شویم، این موضوع را در شکل ۸-۱۰۳۹، مشاهده می‌کنید.

www.takbook.com



شکل ۸- ۱۰۳۹ ایجاد درایو از طریق شبکه و محدود کردن کاربران

اگر به مانند شکل ۸-۱۰۴۰، وارد My Computer شویم درایو موردنظر را مشاهده می‌کنیم، حجم این درایو برابر کل درایو C در سرور اصلی می‌باشد ولی ما باید این حجم را توسط Quota محدود کنیم.

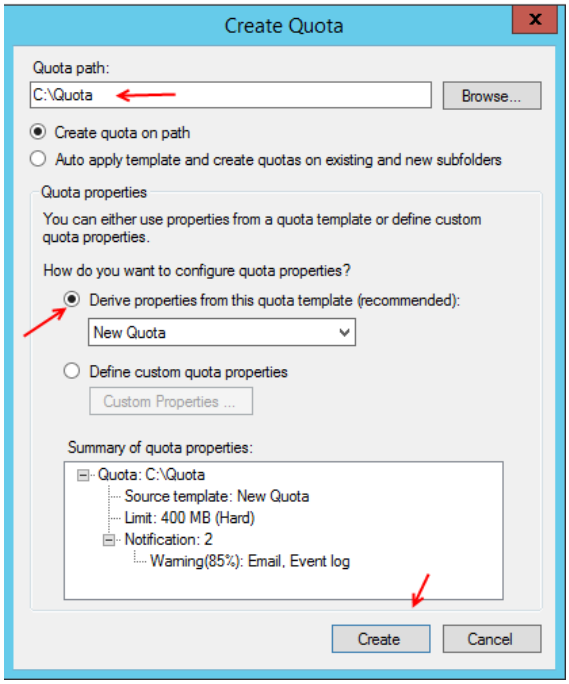


شکل ۸- ۱۰۴۰ ایجاد درایو از طریق شبکه و محدود کردن کاربران

وارد سرور اصلی شوید و سرویس File Server Resource Manager را اجرا کنید و وارد Quota شوید، بر روی Quota کلیک راست کنید و گزینه Create Quota را انتخاب کنید.

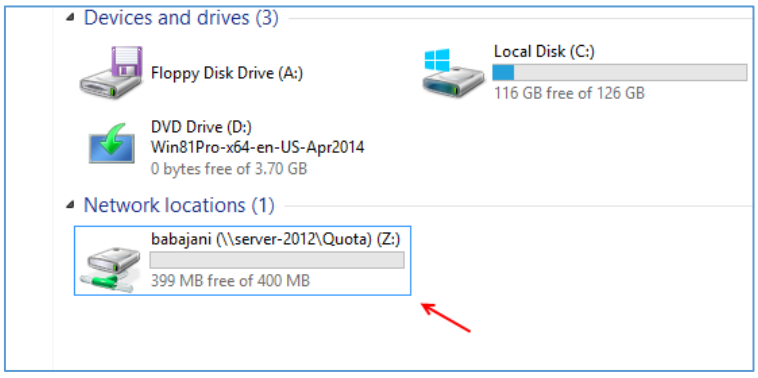
به مانند شکل ۸-۱۰۴۱، در قسمت Quota Path آدرس همان پوشه‌ای را بدهید که در قسمت قبل آن را محدود کردیم و در قسمت Derive Properties from this… همان Template که قبلاً ایجاد کردیم را انتخاب کنید تا پوشه موردنظر به ۴۰۰ مگابایت محدود شود، بر روی Create کلیک کنید تا Quota روی پوشه موردنظر فعال شود.

www.takbook.com



شکل ۸- ۱۰۴۱ ایجاد درایو از طریق شبکه و محدود کردن کاربران

بعد از ایجاد محدودیت به مانند شکل ۱۰۴۲، دوباره وارد کلاینت می‌شویم و همان‌طور که در شکل مشاهده می‌کنید Quota کار خود را انجام داده است و پوشه موردنظر محدود شده است.

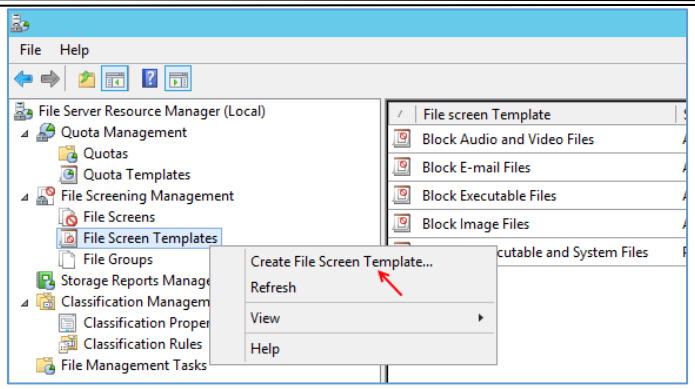


شکل ۸- ۱۰۴۲ ایجاد درایو از طریق شبکه و محدود کردن کاربران

۸-۳-۲۸-۲ جلوگیری از کپی کردن نوع خاصی از فایل برای کاربران

در این قسمت به بررسی توانایی دیگر سرویس File Server Resource Manager می‌پردازیم، این سرویس با نام File Screen می‌باشد که به مدیر شبکه این توانایی را می‌دهد تا از کپی کردن یک فایل با نوع خاص مثلاً MP3, JPEG و یا نوع دیگر جلوگیری کند که شکل ۸-۱۰۴۳، نشان دهنده‌ی این موضوع است.

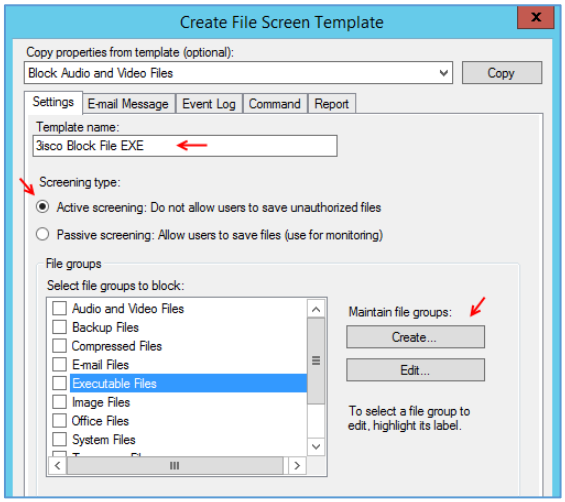
www.takbook.com



شکل ۸- ۱۰۴۳ جلوگیری از کپی کردن نوع خاصی از فایل

برای شروع وارد سرویس File Server Resource Manager شوید و از سمت چپ بر روی File Screen Template کلیک راست کنید و گزینه Create File Screen Template را انتخاب کنید.

در شکل ۸-۱۰٤٤، در قسمت Template name نام موردنظر خود را وارد کنید و در قسمت Screening type یکی از گزینه‌های Active Screening و Passive Screening را انتخاب کنید، اگر گزینه Active Screening را انتخاب کنید، از کپی شدن فایل موردنظر جلوگیری می‌کند، ولی اگر گزینه Passive Screening را انتخاب کنید، فایل موردنظر کپی خواهد شد و یک اخطار و یا ایمیل برای مدیر شبکه ارسال خواهد شد که مثلاً کاربر X از فایل با نوع MP3 استفاده کرده است و داخل پوشه کپی کرده است.



شکل ۸- ۱۰۴۴ جلوگیری از کپی کردن نوع خاصی از فایل

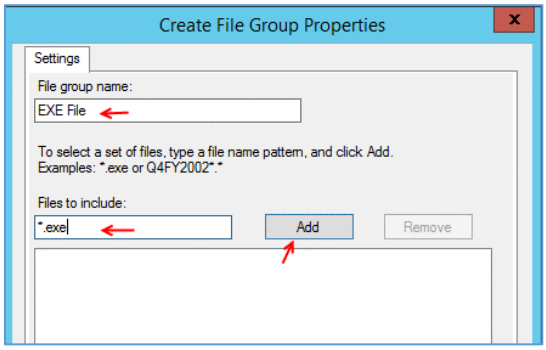
www.takbook.com

اگر به قسمت File Groups نگاه کنید، یک سری آیتم از قبل ایجاد شده است که هر کدام پسوندهای متفاوتی را شامل می‌شوند، مثلاً Executable Files شامل نوع‌های Exe,Bat,.... است، برای اینکه یک پسوند جدید خودمان ایجاد کنیم در شکل ۸-۱۰۴٤، بر روی Create کلیک کنید..

به مانند شکل ۸-۱۰٤٥، در قسمت File Group Name باید نام مشخص خود را وارد کنید و در قسمت File to include باید نوع فایل خود را که در اینجا *.exe است، وارد کنید و بعد بر روی Add کلیک کنید تا پسوند موردنظر به لیست اضافه شود.

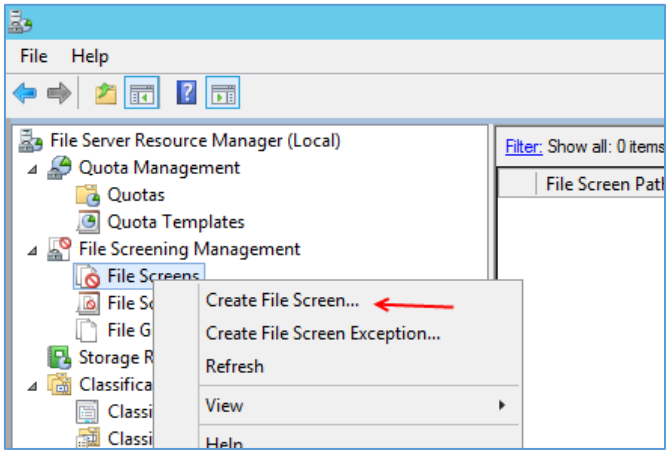
قسمت File to Exclude به این معنی است اگر پسوند فایلی را وارد کنید، یعنی اینکه با این پسوند کاری نداشته باش.

بر روی OK کلیک کنید و در صفحه بعد هم بر روی ok کلیک کنید تا Template موردنظر ایجاد شود.



شکل ۸- ۱۰۴۵ جلوگیری از کپی کردن نوع خاصی از فایل

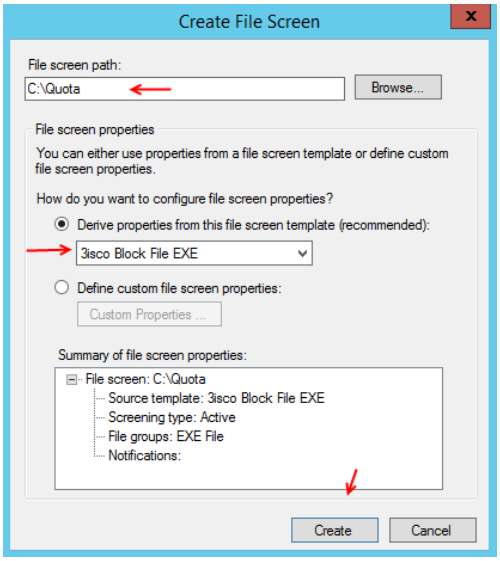
بعد از ایجاد Template به مانند شکل ۸-۱۰٤٦، بر روی File Screen کلیک راست کنید و گزینه Create File Screen انتخاب کنید تا شکل بعد ظاهر شود.



شکل ۸- ۱۰۴۶ جلوگیری از کپی کردن نوع خاصی از فایل

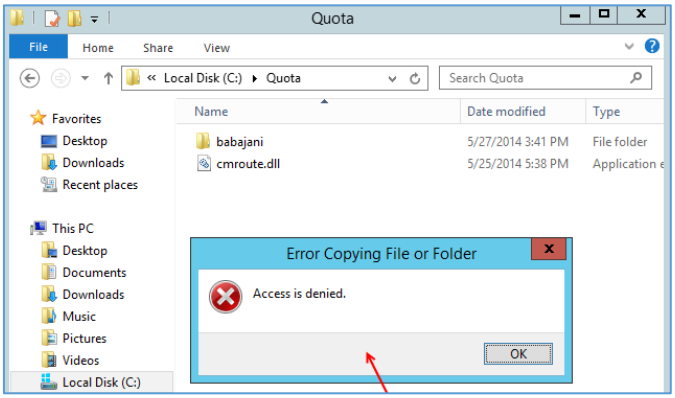
www.takbook.com

در شکل ۸–۱۰٤۷، باید با کلیک بر روی دکمه Browse مسیر پوشه یا درایوی که می‌خواهید این محدودیت روی آن اعمال شود را انتخاب کنید، بعد از آن در قسمت Derive properties from باید همان Template را انتخاب کنید که در قسمت قبل ایجاد کردیم، در پایان بر روی Create کلیک کنید تا محدودیت اعمال شود.



شکل ۸– ۱۰۴۷ جلوگیری از کپی کردن نوع خاصی از فایل

همان‌طور که در شکل ۸–۱۰٤۸، مشاهده می‌کنید، با کپی کردن فایل با پسوند EXE با Error مواجع شدیم.



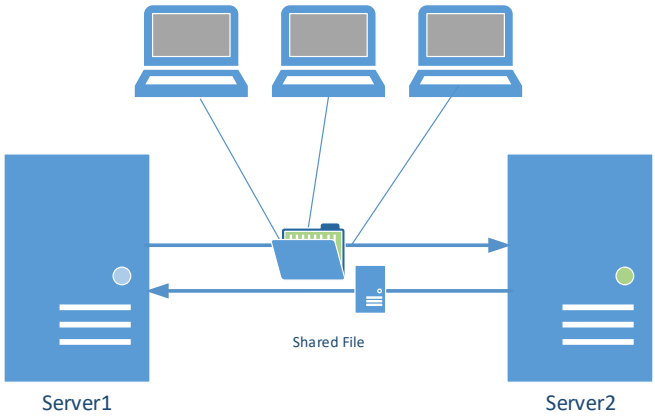
شکل ۸– ۱۰۴۸ جلوگیری از کپی کردن نوع خاصی از فایل

۸–۳–۲۹ کار با سرویس DFS یا Distributed File System

شاید در سازمانی که کار می‌کنید از چند سرور مختلف استفاده می‌کنید و روی هر کدام از آنها فایل‌های خود را Share می‌کنید و برای بدست آوردن فایل‌ها باید هر کدام از آدرس‌های سرور را جداگانه وارد کنید که همین کار باعث هدر رفت زمان خواهد شد، با استفاده از سرویس DFS شما می‌توانید فایل‌های

www.takbook.com

Share مربوط به پوشه خاص را با هم Synchroniz کنید، یعنی اینکه اگر در یک سرور پوشه‌ای با نام X را Share کردید و در سرور دیگر پوشه‌ای با نام Y را Share کردید، می‌توانید با استفاده از این سرویس این دو پوشه در دو سرور مختلف را داخل یک پوشه قرار دهید. شکل ۸-۱۰۴۹، این موضوع را نمایش می‌دهد.

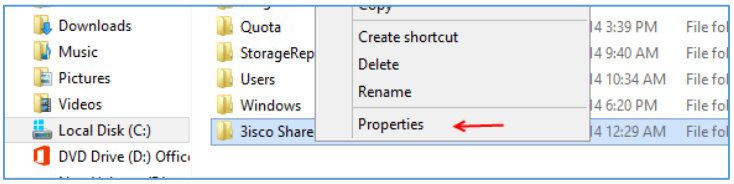


شکل ۸- ۱۰۴۹ سرویس DFS یا Distributed File System

برای شروع کار نیاز به دو سرور داریم که بر روی آنها ویندوز سرور 2025 نصب شده است، روال کار به این صورت است که اول در هر دو سرور یک پوشه را به دلخواه خود Share می‌کنیم و یک سری دسترسی‌ها را به آن می‌دهیم، بعد از آن سرویس‌های DFS را روی هر دو سرور نصب می‌کنیم و عملیات انتقال را انجام می‌دهیم.

در این سناریو یک سرور به عنوان سرور اصلی که روی آن سرویس Active Directory فعال شده است و سرور دیگر زیر مجموعه سرور اول می‌باشد، در کل تفاوتی ندارد که حتماً Active Directory نصب شده باشد، دو سرور اگر با هم شبکه شده باشند می‌توان این موضوع را انجام داد.

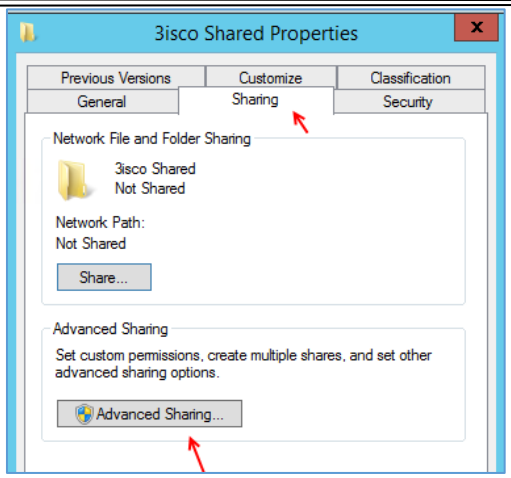
وارد سرور اول می‌شویم و به مانند شکل ۸-۱۰۵۰، یک پوشه با نام 3isco Shared ایجاد می‌کنیم و بعد بر روی آن کلیک راست می‌کنیم و گزینه Properties را انتخاب می‌کنیم.



شکل ۸- ۱۰۵۰ سرویس DFS یا Distributed File System

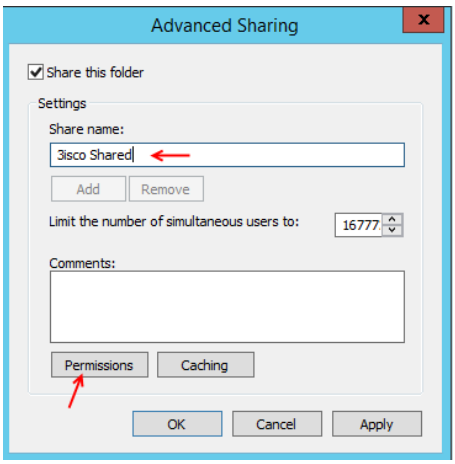
در شکل ۸-۱۰۵۱، وارد تب Sharing شوید و بر روی Advanced Sharing کلیک کنید تا شکل بعد ظاهر شود.

www.takbook.com



شکل ۸- ۱۰۵۱ سرویس DFS یا *Distributed File System*

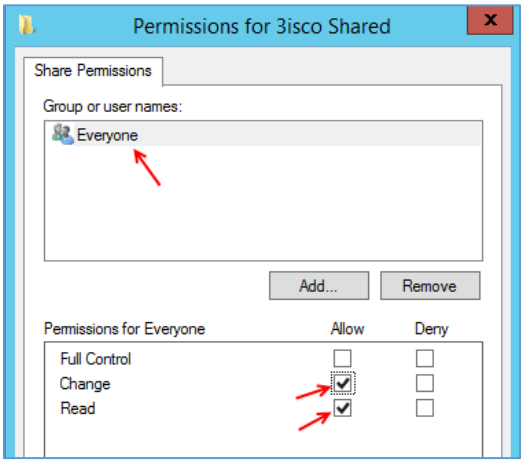
به مانند شکل ۸–۱۰۵۲، در قسمت Share name نام موردنظر خود را وارد کنید و در قسمت Comments بر روی Permissions کلیک کنید.



شکل ۸- ۱۰۵۲ سرویس DFS یا *Distributed File System*

در شکل ۸–۱۰۵۳، گروه Everyone را انتخاب کنید و مجوزهای Change و Read را برای آن فعال کنید، توجه داشته باشید تمام کاربران در شبکه عضو این گروه می‌باشند.

www.takbook.com

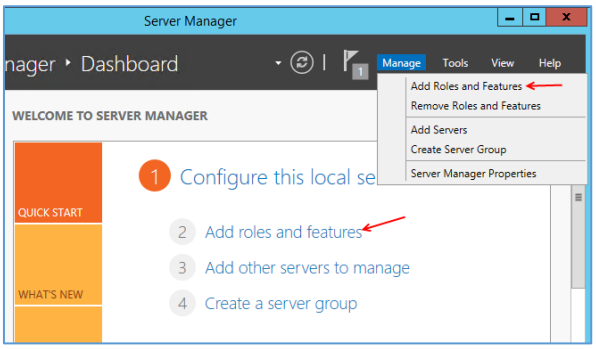


شکل ۸- ۱۰۵۳ سرویس DFS یا *Distributed File System*

بر روی ok کلیک کنید تا پوشه موردنظر Share شود، دقیقاً همین کار را در سرور دیگر انجام دهید و پوشه‌ای در درایو موردنظر خود ایجاد و آن را با مجوزهای لازم Share کنید.

بعد از share کردن فایل نوبت به نصب سرویس می‌رسد، توجه داشته باشید که نصب سرویس باید در هر دو سرور به مانند هم انجام شود.

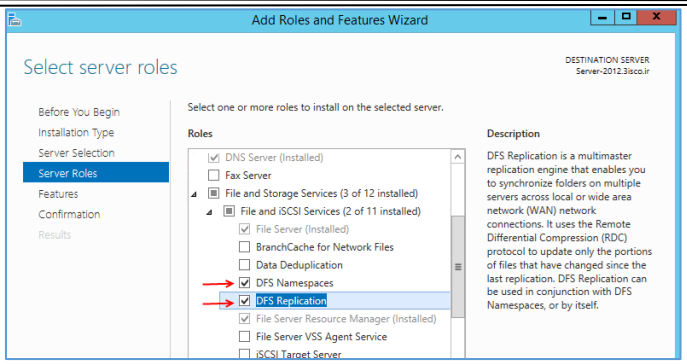
برای شروع به مانند شکل ۸-۱۰۵٤، وارد Server Manager می‌شویم و در صفحه باز شده بر روی Add Roles and Features کلیک می‌کنیم. توجه داشته باشید این کار را هم می‌توانیم از طریق منوی Manage انجام دهید.



شکل ۸- ۱۰۵۴ سرویس DFS یا *Distributed File System*

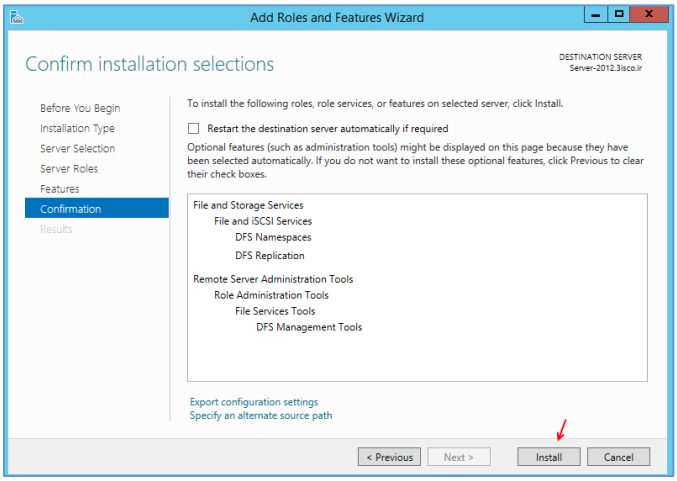
به مانند شکل ۸-۱۰۵۵، وارد قسمت Server Roles شوید و از Roleهای موجود وارد قسمت File and storage.. بعد وارد File and iSCSI… شوید و دو گزینه DFS Namespaces و DFS Replication را انتخاب و بر روی Next کلیک کنید تا به قسمت Configuration برسید.

www.takbook.com



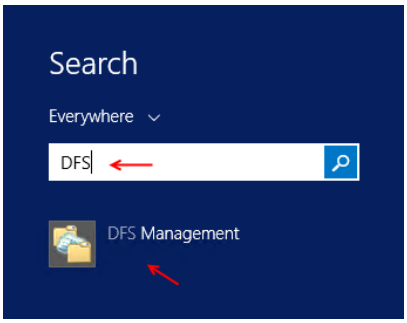
شکل ۸- ۱۰۵۵ سرویس DFS یا Distributed File System

در شکل ۸-۱۰۵۶، برای نصب سرویس موردنظر بر روی install کلیک کنید.



شکل ۸- ۱۰۵۶ سرویس DFS یا Distributed File System

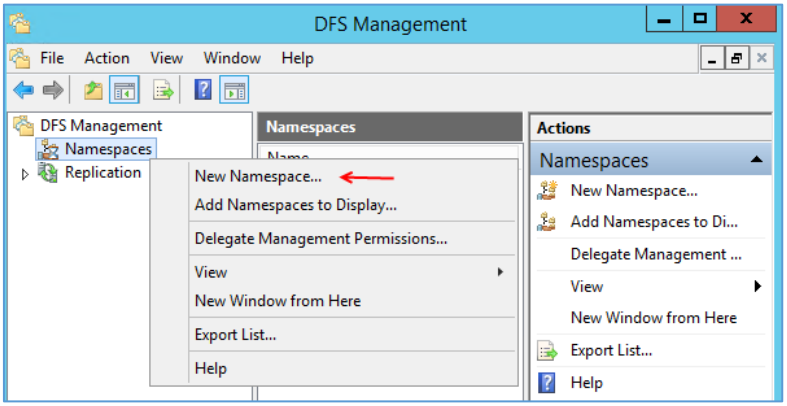
بعد از نصب سرویس از طریق Search سرویس DFS را به مانند شکل ۸-۱۰۵۷، اجرا کنید.



شکل ۸- ۱۰۵۷ سرویس DFS یا Distributed File System

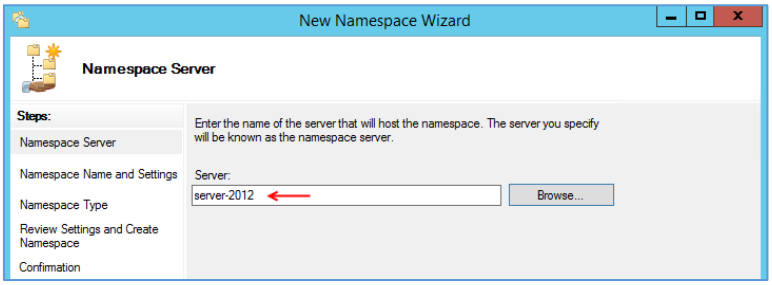
www.takbook.com

بعد از اجرای سرویس موردنظر به مانند شکل ۸-۱۰۵۸، از سمت چپ بر روی Namespace کلیک کنید و یا می‌توانید گزینه New Namespace را از سمت راست سرویس انتخاب کنید.



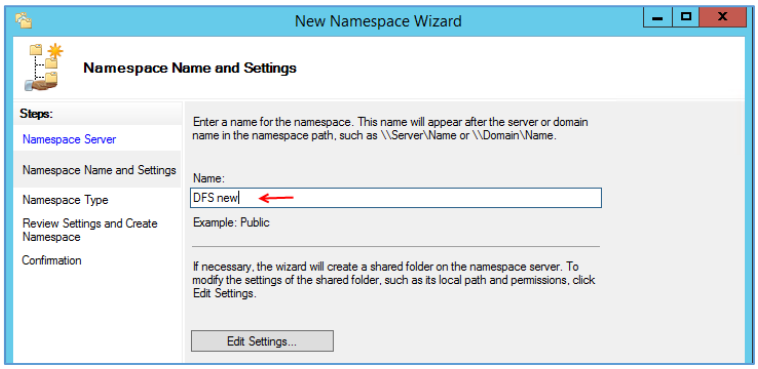
شکل ۸- ۱۰۵۸ سرویس DFS یا Distributed File System

در شکل ۸-۱۰۵۹، باید نام سرور خود را وارد کنید، اگر دقیق نمی‌دانید می‌توانید با کلیک بر روی Browse نام سرور موردنظر را پیدا کنید. برای ادامه کار بر روی Next کلیک کنید.



شکل ۸- ۱۰۵۹ سرویس DFS یا Distributed File System

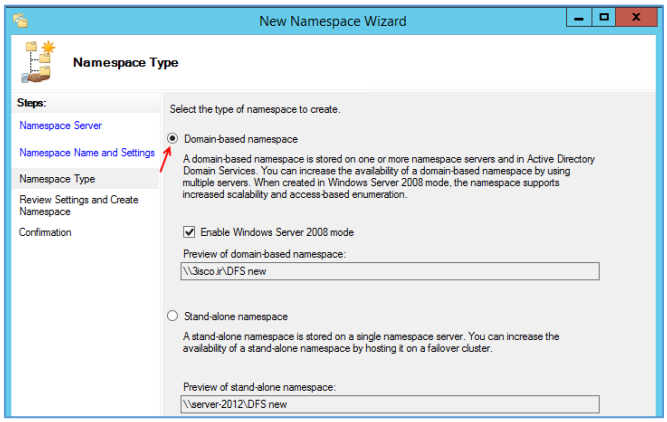
در شکل ۸-۱۰۶۰، یک اسم به دلخواه خود وارد کنید و بر روی Next کلیک کنید.



شکل ۸- ۱۰۶۰ سرویس DFS یا Distributed File System

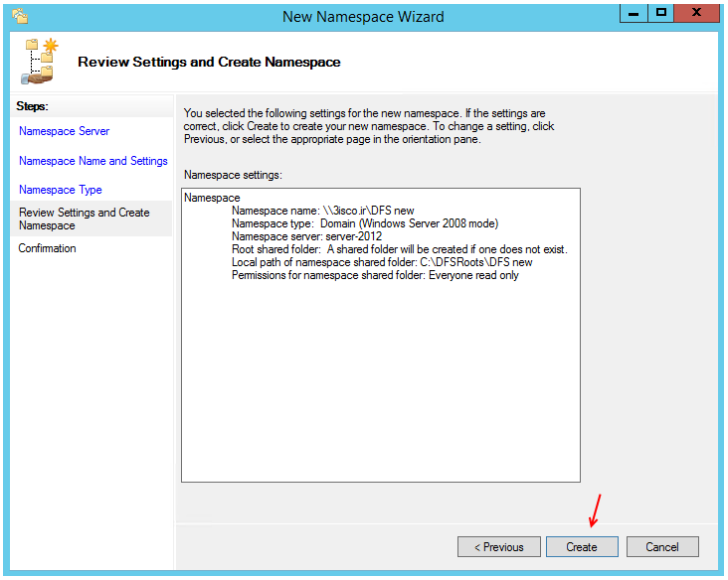
www.takbook.com

در شکل ۸–۱۰۶۱، دو گزینه وجود دارد که گزینه Domain-based namespace را انتخاب کنید، تفاوت این گزینه با گزینه Stand-alone این است که می‌تواند چندین سرور را هم زمان پشتیبانی کند.



شکل ۸- ۱۰۶۱ سرویس DFS یا Distributed File System

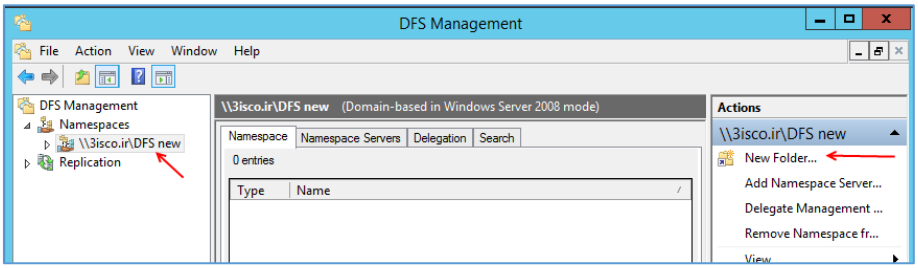
در شکل ۸–۱۰۶۲، اطلاعات کامل نمایش داده می‌شود و برای ایجاد Namespace بر روی Create کلیک کنید، بعد از ایجاد Namespace موردنظر بر روی Close کلیک کنید.



شکل ۸- ۱۰۶۲ سرویس DFS یا Distributed File System

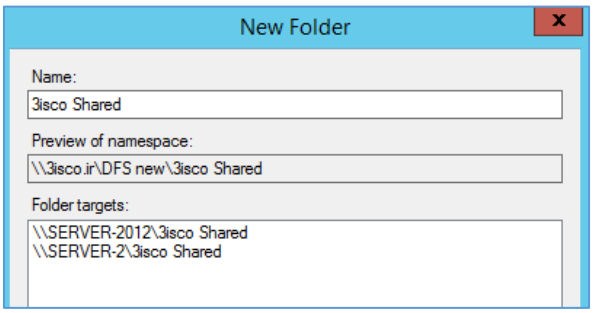
به مانند شکل ۸–۱۰۶۳، از سمت چپ Namespace جدید را انتخاب کنید و از سمت راست بر روی New Folder کلیک کنید.

www.takbook.com



شکل ۸- ۱۰۶۳ سرویس DFS یا *Distributed File System*

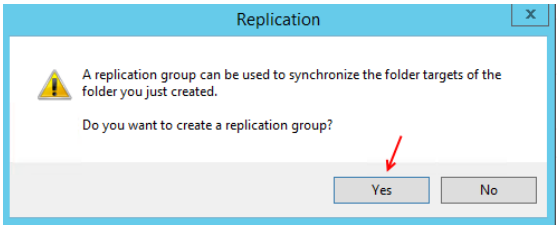
در شکل ۸-۱۰٦٤، در قسمت Name نام دلخواه خود را وارد کنید و در مهمترین بخش با کلیک بر روی Add پوشه share شده را که از قبل تنظیم کرده بودیم را انتخاب می‌کنیم و به لیست اضافه می‌کنیم. توجه داشته باشید در این قسمت باید پوشه‌های Share شده هر دو سرور به لیست اضافه شوند.



شکل ۸- ۱۰۶۴ سرویس DFS یا *Distributed File System*

بر روی ok کلیک کنید تا New Folder ایجاد شود.

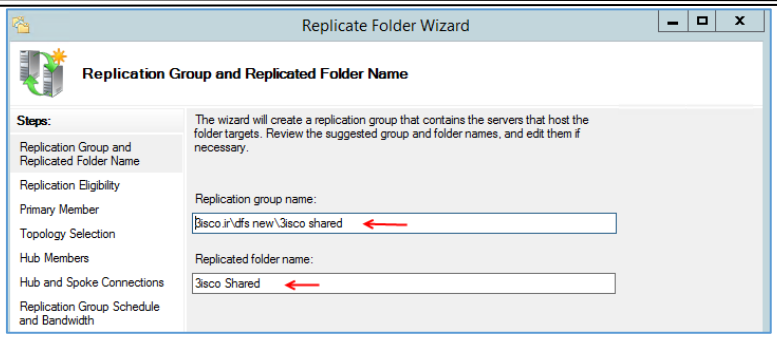
در شکل ۸-۱۰٦٥، از شما سوال می‌شود که آیا می‌خواهید دو سرور را با هم Synchronize کنید که باید بر روی Yes کلیک کنید.



شکل ۸- ۱۰۶۵ سرویس DFS یا *Distributed File System*

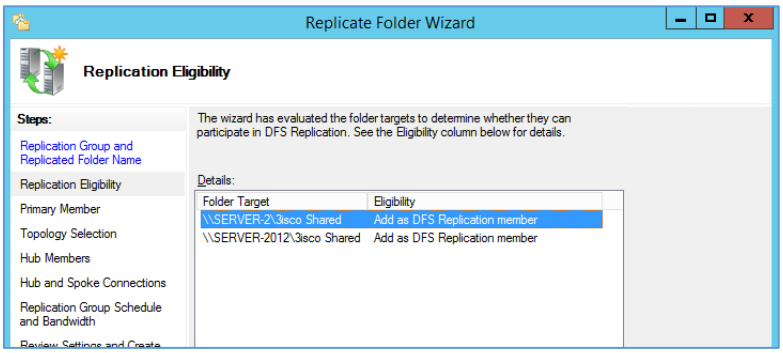
در شکل ۸-۱۰٦٦، بر روی next کلیک کنید.

www.takbook.com



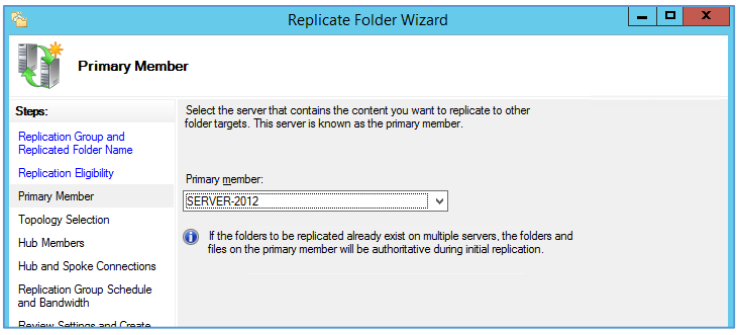
شکل ۸- ۱۰۶۶ سرویس DFS یا *Distributed File System*

در شکل ۸–۱۰٦۷، بر روی Next کلیک کنید.



شکل ۸- ۱۰۶۷ سرویس DFS یا *Distributed File System*

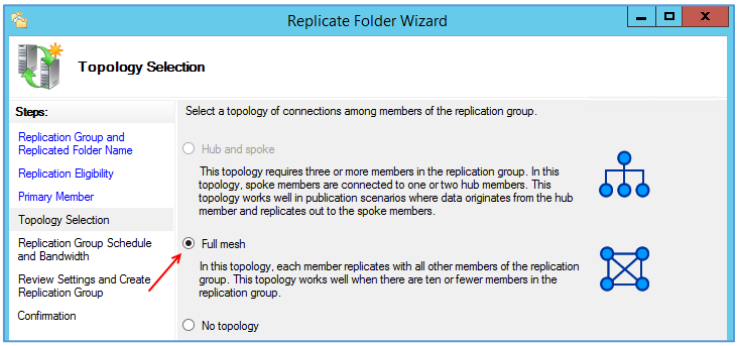
در شکل ۸–۱۰٦۸، باید از لیست کشویی سروری را انتخاب کنید که ارجحیت بیشتری نسبت به سرور دیگر دارد، در اینجا Server-2012 سرور Active Dircetory می‌باشد.



شکل ۸- ۱۰۶۸ سرویس DFS یا *Distributed File System*

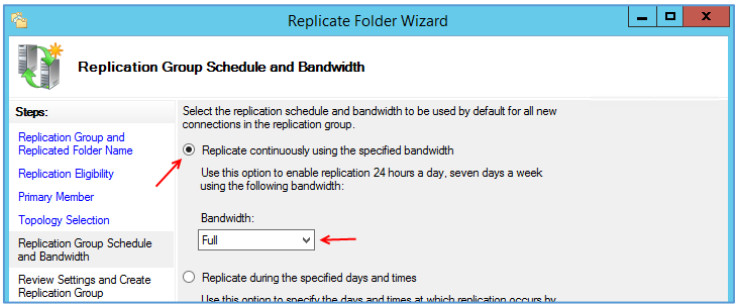
در شکل ۸–۱۰٦۹، باید توپولوژی شبکه را مشخص کنید که درباره توپولوژی در فصل اول به صورت کامل صحبت کردیم که در این قسمت گزینه Full Mesh را انتخاب و بر رویNext کلیک کنید.

www.takbook.com



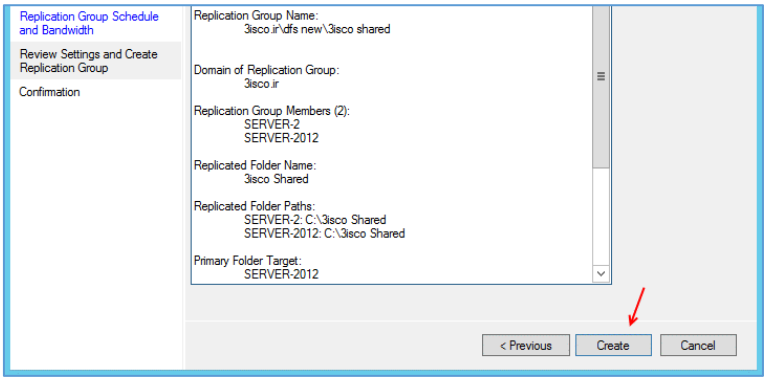
شکل ۸- ۱۰۶۹ سرویس DFS یا Distributed File System

در شکل ۸-۱۰۷۰، می‌توانید مشخص کنید زمانی که بین دو سرور اطلاعات در حال انتقال است چقدر از حجم مصرفی شبکه را مصرف کند که در این قسمت گزینه Full انتخاب شده است، ولی اگر نیاز به زمان‌بندی دارید می‌توانید گزینه Replicate during the... را انتخاب کنید و بر روی Edit Schedule کلیک کنید.



شکل ۸- ۱۰۷۰ سرویس DFS یا Distributed File System

در آخر کار به مانند شکل ۸-۱۰۷۱، بر روی Create کلیک کنید تا عملیات همسان‌سازی انجام شود.

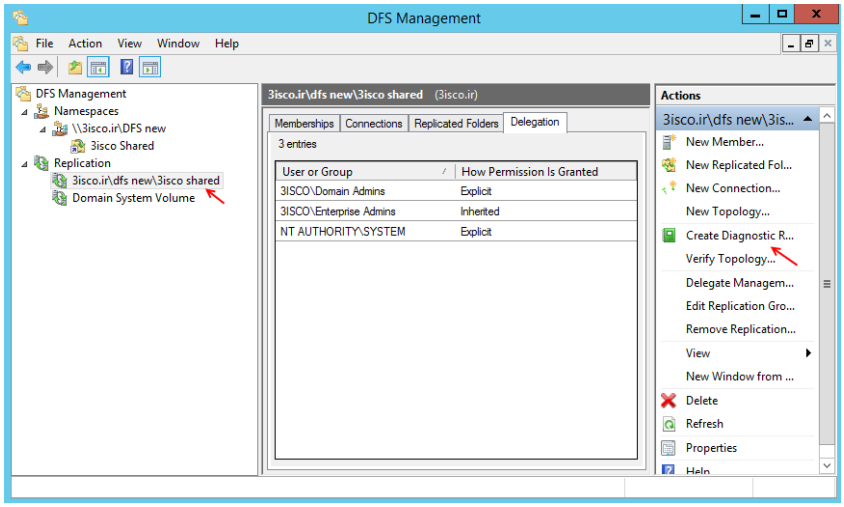


شکل ۸- ۱۰۷۱ سرویس DFS یا Distributed File System

www.takbook.com

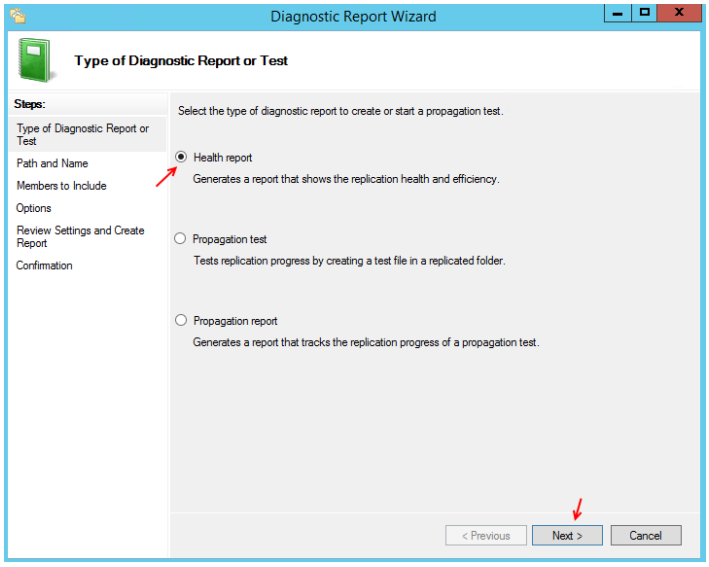
بعد ار ایجاد Replicate موردنظر از این پس در هر یک از سرورها فایلی در پوشه موردنظر قرار داده شود، این اطلاعات فقط در یک پوشه و توسط همه افراد داخل شبکه در دسترس است.

برای گزارش‌گیری از وضعیت Replication موجود به مانند شکل ۸-۱۰۷۲، از سمت چپ بر روی آن کلیک کنید و از سمت راست بر روی Creat Diagnostic Report کلیک کنید.



شکل ۸- ۱۰۷۲ سرویس DFS یا Distributed File System

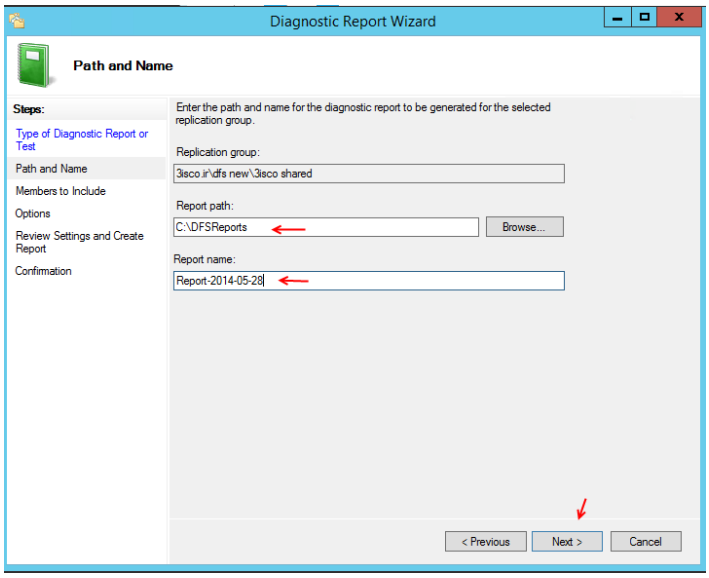
در شکل ۸-۱۰۷۳، گزینه اول را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۱۰۷۳ سرویس DFS یا Distributed File System

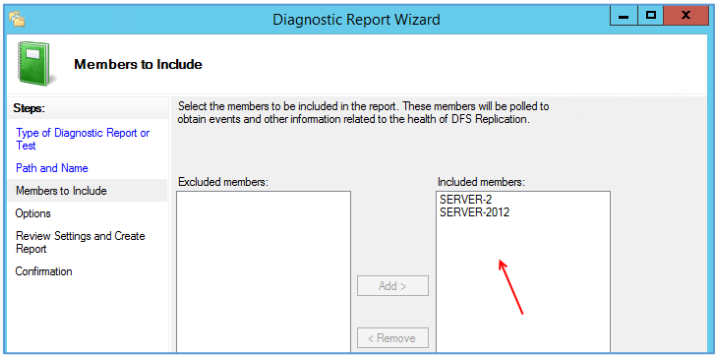
www.takbook.com

در شکل ۸-۱۰۷٤، در قسمت Report Path مسیر ذخیره‌سازی گزارشات را می‌توانید مشخص کنید و در قسمت Report Name هم نام گزارش خود را وارد کنید.



شکل ۸- ۱۰۷۴ سرویس DFS یا Distributed File System

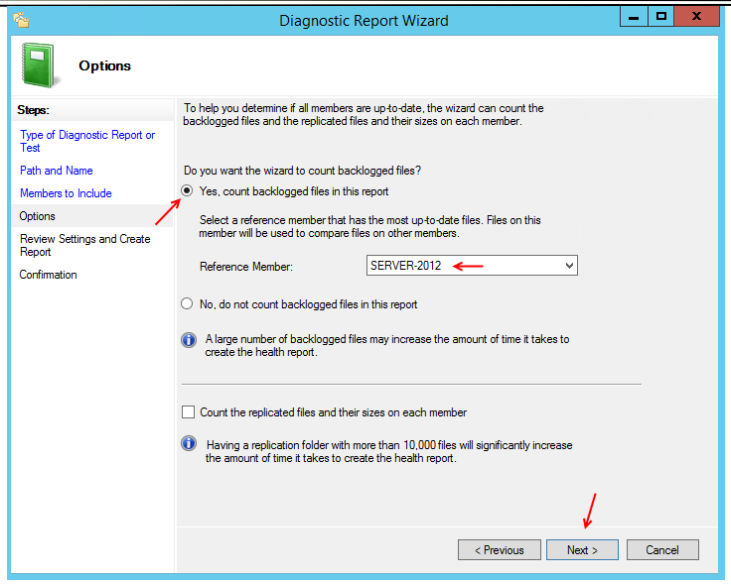
در شکل ۸-۱۰۷۵، هر دو سرور باید در قسمت Included members قرار داشته باشند، بر روی Next کلیک کنید.



شکل ۸- ۱۰۷۵ سرویس DFS یا Distributed File System

در شکل ۸-۱۰۷٦، گزینه‌ی اول را انتخاب و از لیست کشویی سرور اصلی را انتخاب و بر روی Next کلیک کنید.

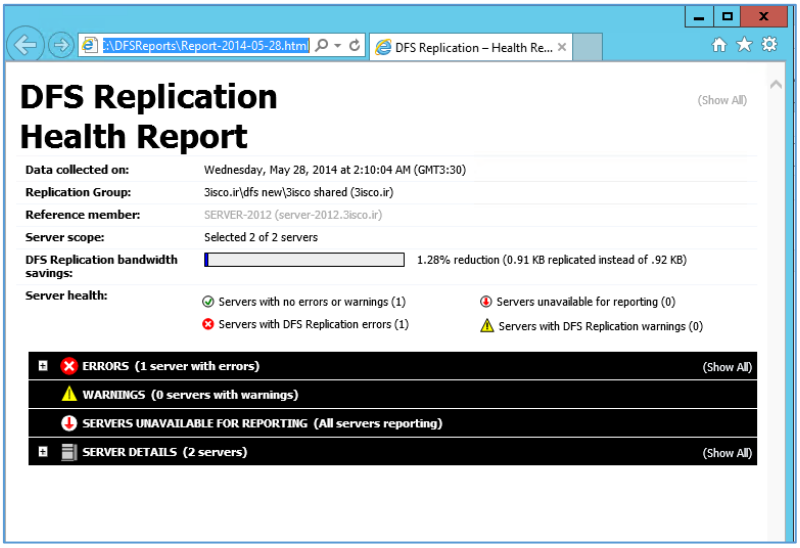
www.takbook.com



شکل ۸- ۱۰۷۶ سرویس DFS یا *Distributed File System*

در صفحه آخر هم بر روی Create کلیک کنید تا یک فایل با پسوند HTML ایجاد شود.

وارد آدرس C:\DFSReport می‌شویم و گزارش موردنظر را که با نام Report-2014-05-28 بود را روی Internet Explorer اجرا می‌کنیم. همان‌طور که در شکل ۸-۱۰۷۷، مشاهده می‌کنید گزارش موردنظر اجرا شده است و می‌توانید اطلاعات را بررسی کنید.



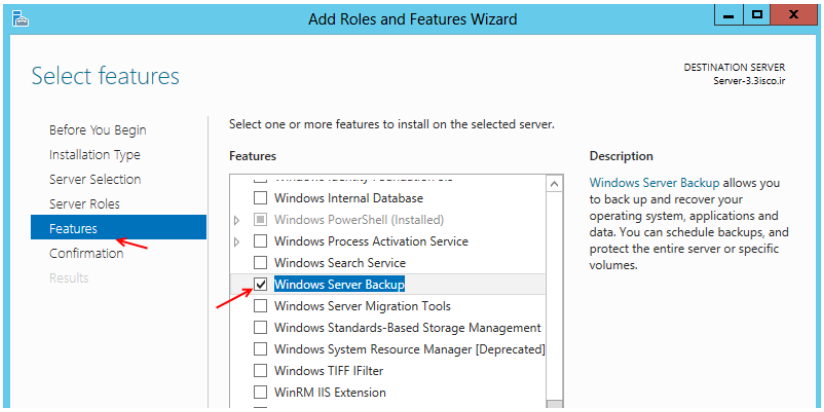
شکل ۸- ۱۰۷۷ سرویس DFS یا *Distributed File System*

www.takbook.com

۸-۳-۳۰ نحوه‌ی ایجاد Backup و Restore

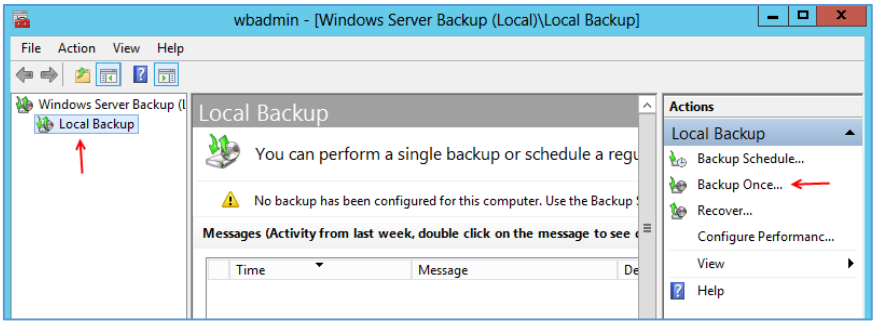
یکی از مهمترین کارهایی که در یک شبکه انجام می‌شود گرفتن Backup کامل از اطلاعات موجود بر روی سرور است این اطلاعات می‌تواند، اطلاعات Active Directory و یا اطلاعات سرویس‌های دیگر بر روی سرور باشد، برای انجام این کار به روش زیر عمل کنید، توجه داشته باشید در فصل سیزدهم به طور تخصصی مسئله Backup را بررسی کردیم.

وارد سرور شوید و Server Manager را اجرا کنید و در صفحه باز شده بر روی Add Roles and Features کلیک کنید و در صفحه باز شده بر روی Next کلیک کنید تا به قسمت Features برسید، در این قسمت به مانند شکل ۸-۱۰۷۸، گزینه Windows Server Backup را انتخاب کنید و بر روی Next کلیک کنید و در آخر بر روی Install کلیک کنید.



شکل ۸- ۱۰۷۸ نحوه‌ی ایجاد Backup و Restore

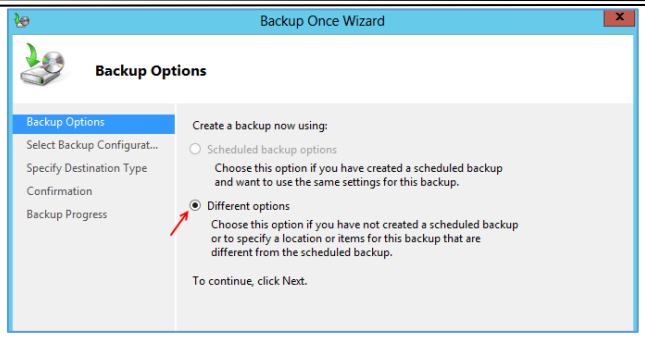
بعد از نصب سرویس به مانند شکل ۸-۱۰۷۹، وارد Serach شوید و سرویس Windows server Backup را اجرا کنید، بعد از اجرای سرویس از سمت چپ بر روی Backup Once کلیک کنید، تاشکل بعد ظاهر شود.



شکل ۸- ۱۰۷۹ نحوه‌ی ایجاد Backup و Restore

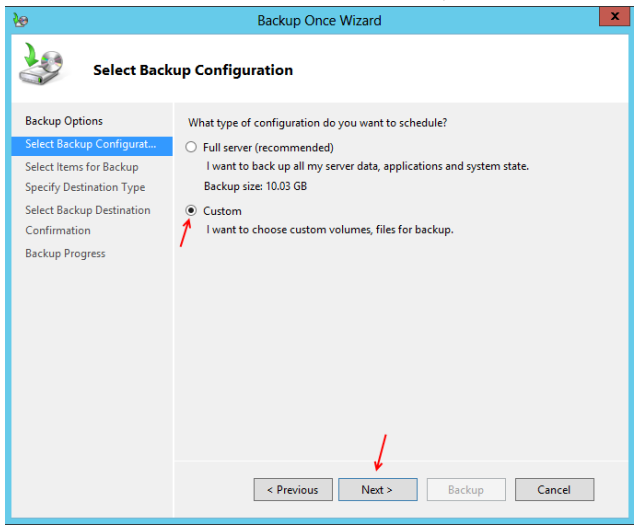
در شکل ۸-۱۰۸۰، گزینه‌ی Different options را انتخاب کنید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۸- ۱۰۸۰ نحوه‌ی ایجاد Backup و Restore

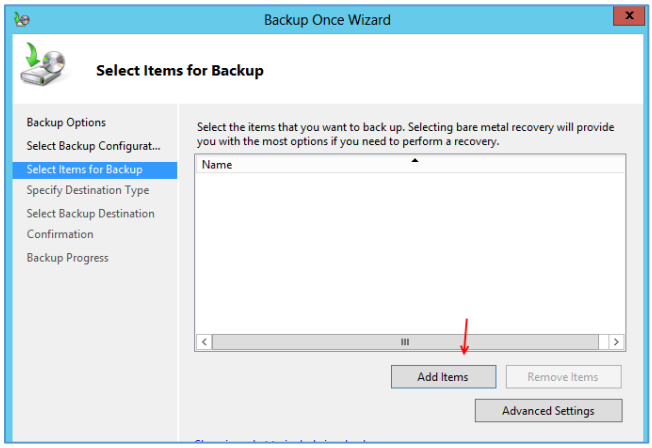
در شکل ۸-۱۰۸۱، اگر گزینه Full Server را انتخاب کنید تمام بخش‌های سرور شما، مانند فایل‌ها، اسناد، سرویس‌ها و... Backup گرفته می‌شود که حجمی حدود ۱۰ گیگابایت را برای این سرور نیاز ، برای اینکه گزینه‌های موردنظر خود را انتخاب کنیم، Custom را انتخاب و بر روی next کلیک کنید.



شکل ۸- ۱۰۸۱ نحوه‌ی ایجاد Backup و Restore

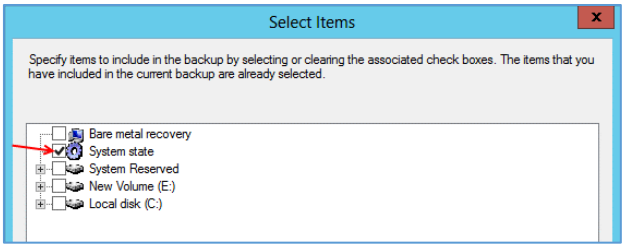
در شکل ۸-۱۰۸۲، باید قسمت موردنظر خود را برای گرفتن Backup انتخاب کنیم برای این کار بر روی Add item کلیک کنید.

www.takbook.com



شکل ۸- ۱۰۸۲ نحوه‌ی ایجاد Backup و Restore

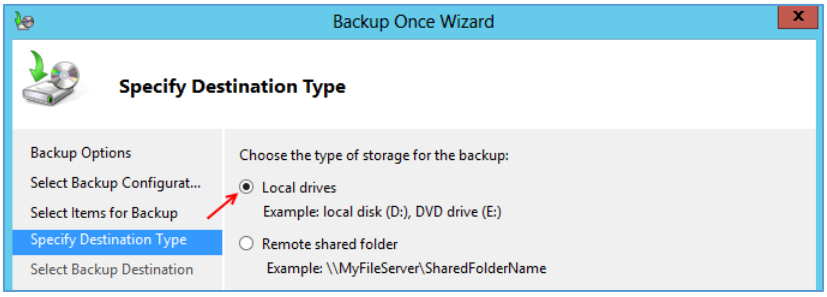
در شکل ۸-۱۰۸۳، برای اینکه از اطلاعات Active Directory یک Backup تهیه کنیم، گزینه System state را انتخاب کنید و بر روی ok کلیک کنید.



شکل ۸- ۱۰۸۳ نحوه‌ی ایجاد Backup و Restore

بعد از اضافه شدن به لیست موردنظر بر روی next کلیک کنید.

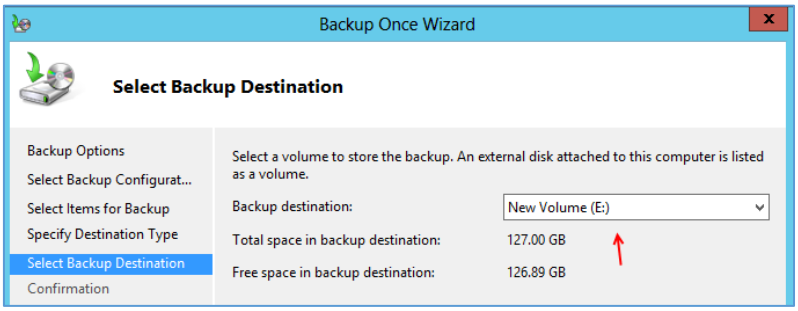
در شکل ۸-۱۰۸٤، باید محل ذخیره‌سازی Backup خود را انتخاب کنید، به این نکته توجه کنید که محل ذخیره‌سازی نمی‌تواند درایو ویندوز که به صورت پیش‌فرض درایو C است باشد، شما می‌توانید یک آدرس در شبکه را وارد کنید، در این قسمت گزینه local drives را انتخاب کنید و بر روی next کلیک کنید.



شکل ۸- ۱۰۸۴ نحوه‌ی ایجاد Backup و Restore

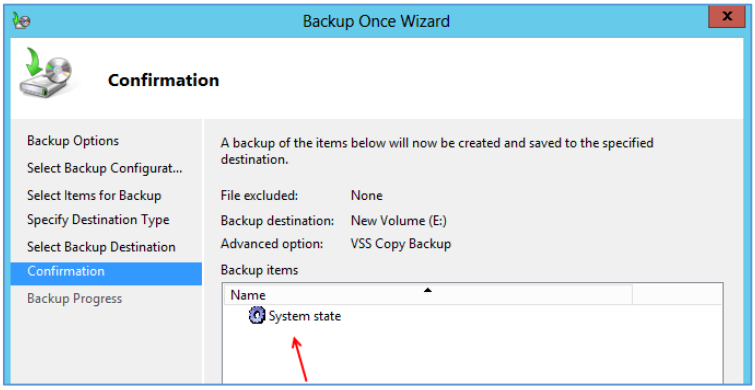
www.takbook.com

در شکل ۸–۱۰۸۵، درایو موردنظر خود را انتخاب کنید، اگرتوجه کنید در اینجا درایو E انتخاب شده است. اگر از ماشین مجازی استفاده می‌کنید، سرور را Shutdown کنید و یک هارد مجازی به آن اضافه کنید.



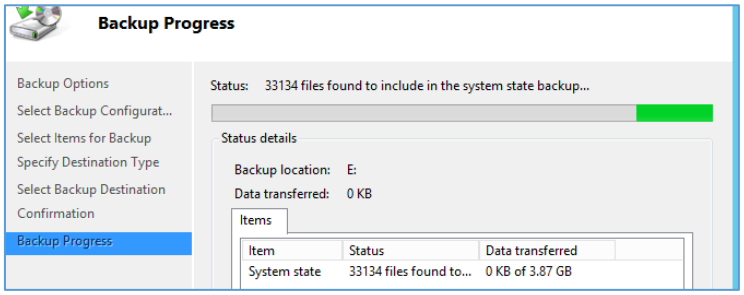
شکل ۸– ۱۰۸۵ نحوه‌ی ایجاد Backup و Restore

در شکل ۸–۱۰۸۶، بر روی Backup کلیک کنید تا Backup از قسمت System state تهیه شود.



شکل ۸– ۱۰۸۶ نحوه‌ی ایجاد Backup و Restore

همان‌طور که در شکل ۸–۱۰۸۷ مشاهده می‌کنید Backup مورد نظر در حال اجرا است، توجه داشته باشید مدت زمان این کار بسته به حجم سرور زمان بر خواهد بود.



شکل ۸– ۱۰۸۷ نحوه‌ی ایجاد Backup و Restore

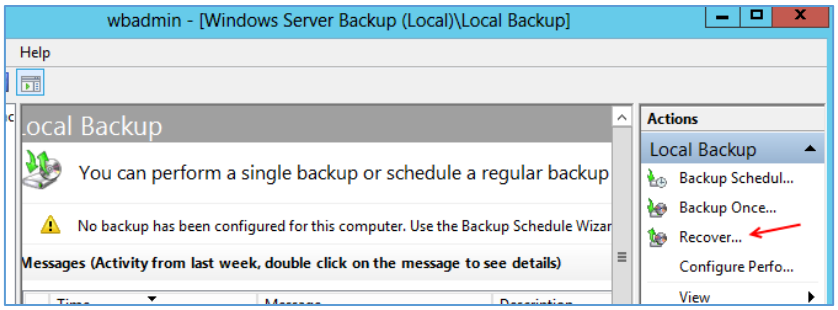
www.takbook.com

با انجام کارهای قبلی توانستیم از قسمت system state یک Backup تهیه کنیم که این Backup شامل تمام سرویس‌های فعال در سرور است خصوصاً سرویس Active Directory که از اهمیت بالایی برخوردار است.

توجه داشته باشید که شما می‌توانید یک زمانبندی مشخص انجام دهید تا از سیستم خود، هر چند وقت به صورت خودکار Backup تهیه کنید.

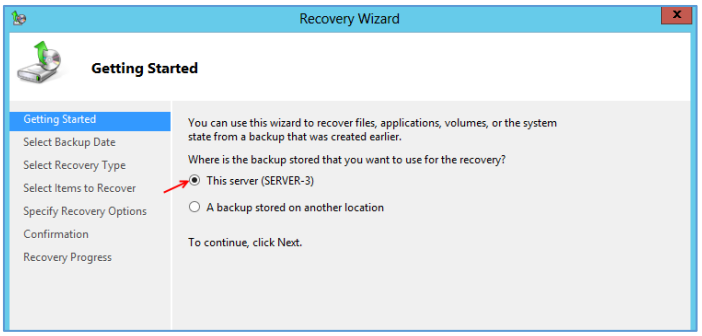
Restore کردن Backup

شاید، برای شما پیش بیاید که تمام اطلاعات موجود در سرور خود را از دست دهید، ولی دیگر نگران نیستید، چون از قبل یک Backup از کل سرویس‌ها و اطلاعات تهیه کردید و می‌توانید در این قسمت آن را به راحتی Restore کنید، برای شروع به مانند شکل ۸-۱۰۸۸، وارد سرویس Backup شوید و بر روی Recover.. کلیک کنید.



شکل ۸- ۱۰۸۸ نحوه‌ی ایجاد Backup و Restore

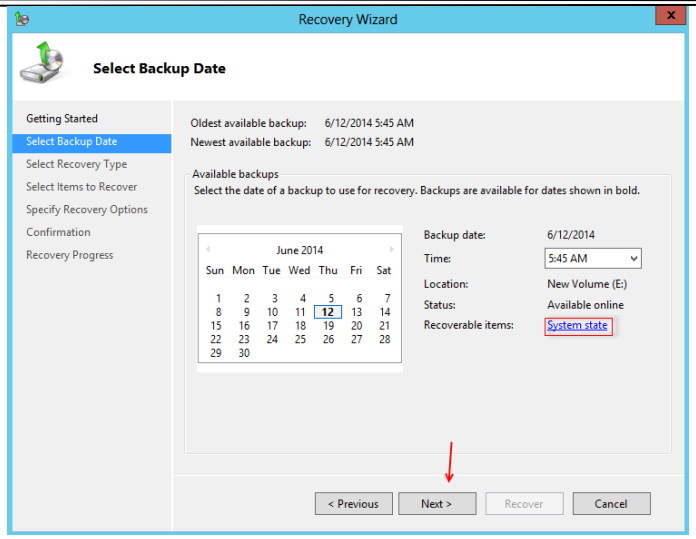
در شکل ۸-۱۰۸۹، گزینه‌ی This Server را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸- ۱۰۸۹ نحوه‌ی ایجاد Backup و Restore

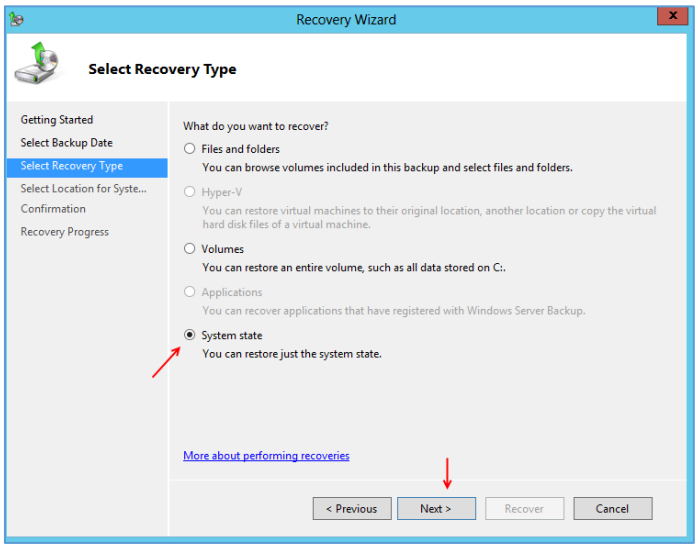
در شکل ۸-۱۰۹۰، مشخص‌شده است که کدام قسمت می‌خواهد Recover شود، اگر توجه کنید زمان آخرین Backup گرفته شده از سیستم را نشان می‌دهد، در قسمت Recoverable items نوع backup را مشخص کرده است که از کدام قسمت backup تهیه شده است.

www.takbook.com



شکل ۸- ۱۰۹۰ نحوه‌ی ایجاد Backup و Restore

در شکل ۸-۱۰۹۱، گزینه System State را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸- ۱۰۹۱ نحوه‌ی ایجاد Backup و Restore

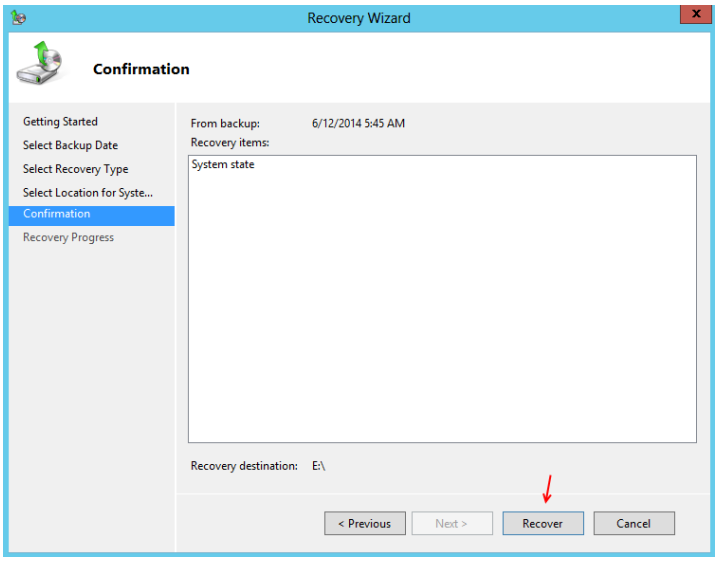
در شکل ۸-۱۰۹۲، گزینه‌ی Alternate location را انتخاب کنید و آدرس جایی که از آن Backup تهیه کردید را وارد کنید که همیشه این نکته را در نظر داشته باشید که درایوی را انتخاب کنید که درایو سیستم است و ویندوز روی آن نصب شده است. بر روی Next کلیک کنید.

www.takbook.com



شکل ۸- ۱۰۹۲ نحوه‌ی ایجاد Backup و Restore

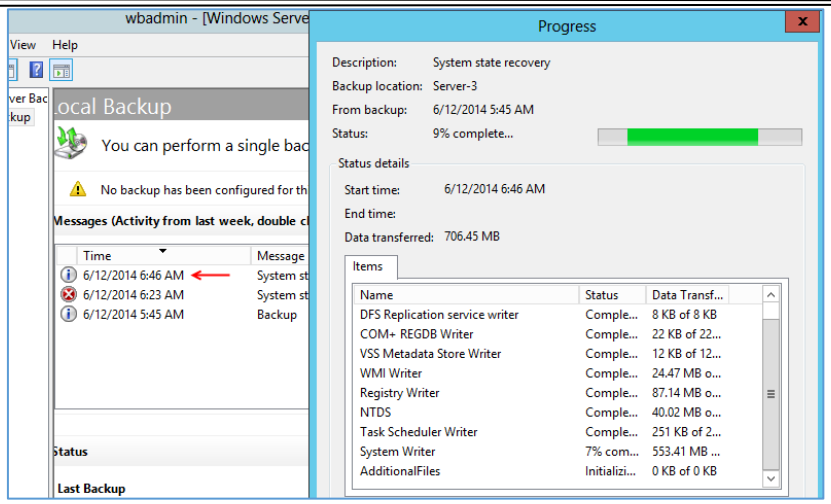
در شکل ۸-۱۰۹۳، برای انجام عملیات بر روی Recover کلیک کنید.



شکل ۸- ۱۰۹۳ نحوه‌ی ایجاد Backup و Restore

به مانند شکل ۸-۱۰۹٤، اگر از لیست موردنظر بر روی Recover دوبار کلیک کنید، قسمت Progress ظاهر می‌شود که نحوه انتقال اطلاعات را در قسمت‌های موردنظر مشخص کرده است.

www.takbook.com



شکل ۸- ۱۰۹۴ نحوه‌ی ایجاد Backup و Restore

برای اینکه زمانبندی را ایجاد کنید در سرویس موردنظر از سمت راست بر روی Backup Schedul کلیک کنید در صفحه باز شده بر روی Next کلیک کنید، در صفحه بعد custom را انتخاب و گزینه system state را به مانند قبل به لیست اضافه کنید و بر روی Next کلیک کنید، در صفحه Time باید ساعت مشخص ایجاد Backup را مشخص کنید، بر روی Next کلیک کنید. در صفحه Destination Type گزینه دوم را انتخاب و بر روی Next کلیک کنید و در صفحه بعد درایوی را برای ذخیره کردن Backup وارد کنید و در صفحه آخر بر روی Finish کلیک کنید تا در زمان مشخص‌شده این کار انجام گیرد.

۸-۳-۳۱ بررسی سرویس PowerShell

PowerShell یک محیط خط فرمان و یک زبان اسکریپت‌نویسی قدرتمند است که توسط مایکروسافت توسعه داده شده است. این ابزار برای مدیریت و خودکارسازی وظایف در سیستم‌های ویندوزی (و حتی سیستم‌های دیگر مانند لینوکس و macOS) طراحی شده است. در ادامه، توضیحات بیشتری درباره PowerShell ارائه می‌دهیم.

ویژگی‌های کلیدی PowerShell

- پشتیبانی از cmdlets

هر دستور در PowerShell یک cmdlet است، که عملیات خاصی مانند مدیریت فایل‌ها، فرایندها، سرویس‌ها، یا پیکربندی سیستم را انجام می‌دهد، ساختار cmdletها بسیار استاندارد است و معمولاً به صورت Verb-Noun (مانند Get-Help, Set-Item) تعریف می‌شوند.

- قابلیت‌های شیءمحور

www.takbook.com

برخلاف بسیاری از خطوط فرمان دیگر (مانند CMD یا Bash)، PowerShell با اشیاء (Objects) کار می‌کند. به این معنا که خروجی یک دستور، داده‌ای ساختاریافته است که می‌تواند به راحتی به دستور بعدی منتقل شود.

- قابلیت اسکریپت‌نویسی

PowerShell یک زبان اسکریپت‌نویسی کامل دارد که از حلقه‌ها (for, while)، شرط‌ها (if)، و توابع پشتیبانی می‌کند،فایل‌های اسکریپت PowerShell با پسوند .ps1 ذخیره می‌شوند.

- پشتیبانی از پلتفرم‌های مختلف

PowerShell ابتدا برای ویندوز طراحی شده بود، اما اکنون نسخه‌ای به نام PowerShell Core منتشر شده است که به صورت Cross-Platform در سیستم‌عامل‌های لینوکس، مک، و ویندوز قابل استفاده است.

- ادغام با سیستم‌های مدیریتی

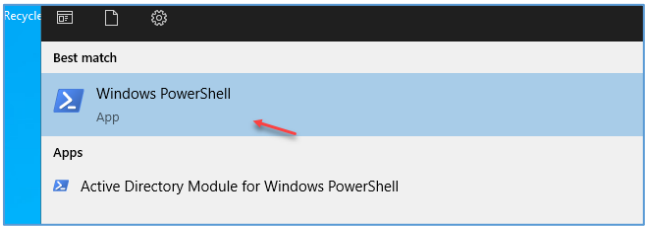
PowerShell به صورت یکپارچه با ابزارهای مدیریتی مایکروسافت مانند Active Directory، Microsoft Azure، و Office 365 کار می‌کند.

مزایای PowerShell نسبت به CMD

برخلاف CMD که فقط با متن کار می‌کند، PowerShell خروجی‌های ساختاریافته‌ای ارائه می‌دهد که پردازش آن‌ها راحت‌تر است، می‌تواند دستورات زنجیره‌ای و پیچیده‌تری را اجرا کند، و همچنین قابلیت اتصال به سیستم‌های راه دور، اجرای اسکریپت‌ها در سطح شبکه، و مدیریت منابع ابری را دارد.

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

روش اول: اجرای PowerShell به این صورت است که به مانند شکل ۸-۱۰۹۵، وارد Search ویندوز خود شویم و کلمه‌ی PowerShell را وارد کنیم و درنتیجه جستجو بر روی Windows PowerShell کلیک راست کنید و گزینه‌ی Run as administrator را انتخاب کنید تا مانند قبل، از روی کاربر Administrator اجرا شود.

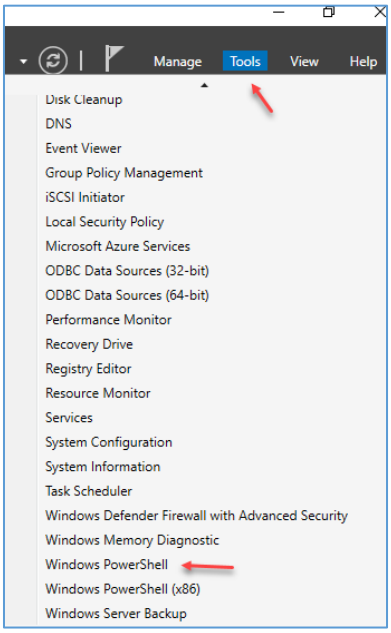


شکل ۸- ۱۰۹۵ PowerShell

روش دوم: به این صورت است که به مانند شکل ۸-۱۰۹۶، وارد Server Manager شویم و از منوی Tools گزینه‌ی Windows PowerShell را انتخاب کنیم.

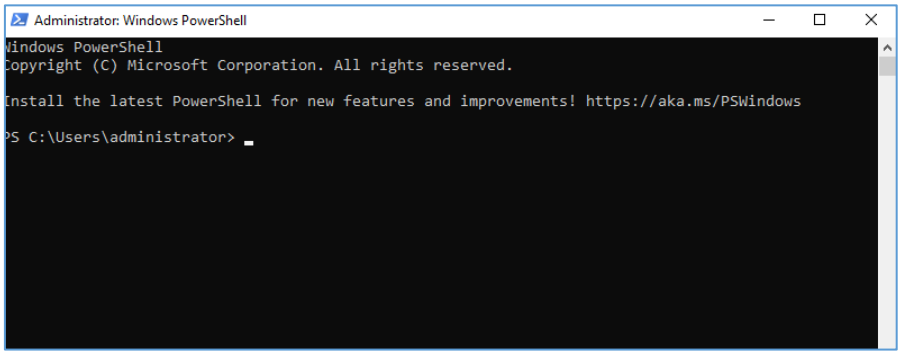
www.takbook.com

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



شکل ۸- ۱۰۹۶ *PowerShell*

بعد از اجرای PowerShell با کاربر Administrator، شکل ۸–۱۰۹۷ را مشاهده خواهید می‌کنید که کاملاً شبیه به CMD ویندوز است.



شکل ۸- ۱۰۹۷ *PowerShell*

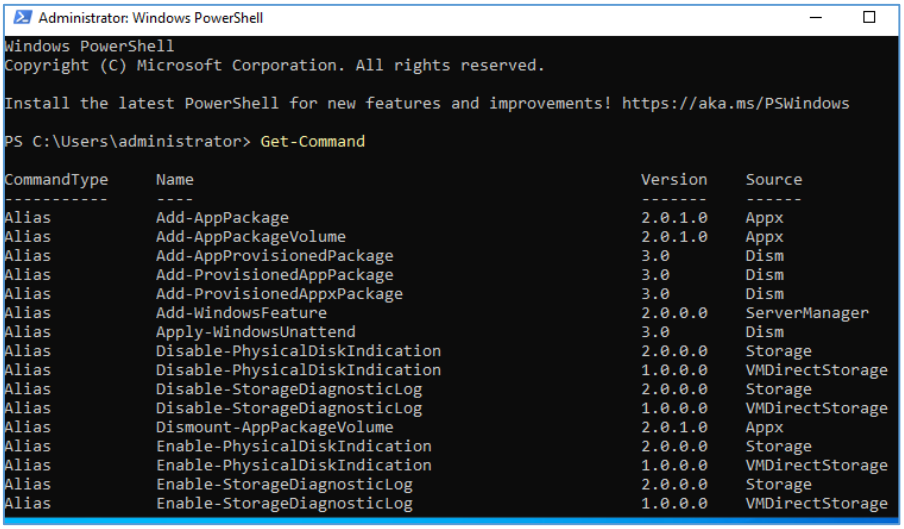
نکته: همان‌طور که عرض کردیم دستورات در PowerShell به عنوان cmdlets (که مخفف "command-lets" است) شناخته می‌شوند. هر cmdlet یک فرمان کوچک و تخصصی است که برای انجام وظایف خاصی در PowerShell استفاده می‌شود. این cmdletها معمولاً به فرم فعل–اسم (مانند Get-Process یا Set-Item) نوشته می‌شوند و بر اساس یک ساختار استاندارد طراحی شده‌اند.

www.takbook.com

فهرست کامل دستورات (cmdlets) در PowerShell بسیار گسترده است و صدها دستور مختلف وجود دارد که برای مدیریت سیستم‌ها، فایل‌ها، شبکه‌ها و موارد دیگر استفاده می‌شود. توضیح کامل همه‌ی این دستورات به صورت یکجا ممکن است زمان‌بر باشد، اما می‌توانم روش‌هایی را برای دسترسی به لیست کامل دستورات و توضیحات آن‌ها ارائه دهم و همچنین مثال‌هایی از دسته‌های پرکاربرد ارائه کنیم.

برای مشاهده تمام دستورات موجود در PowerShell، می‌توانید از دستور زیر استفاده کنید، که خروجی آن را در شکل ۸-۱۰۹۸، مشاهده می‌کنید.

Get-Command

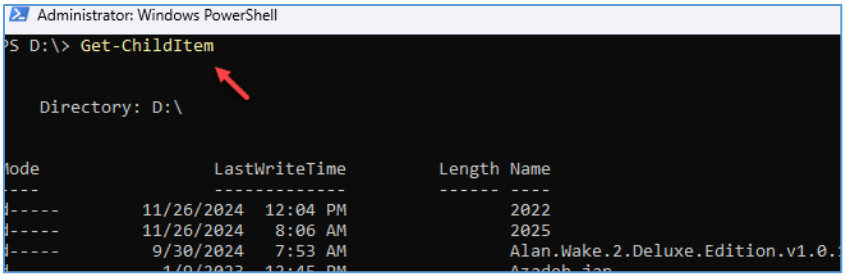


شکل ۸- ۱۰۹۸ دستورات PowerShell

در ادامه کار با دستورات مختلف و کاربری در PowerShell آشنا خواهیم شد.

دستور Get-ChildItem

با استفاده از این دستور می‌توانید تمام فایل‌ها و پوشه‌ها در دایرکتوری جاری را مشاهده کنید، در خروجی شکل ۸-۱۰۹۹، اطلاعات ریشه درایو D نمایش داده شده است.



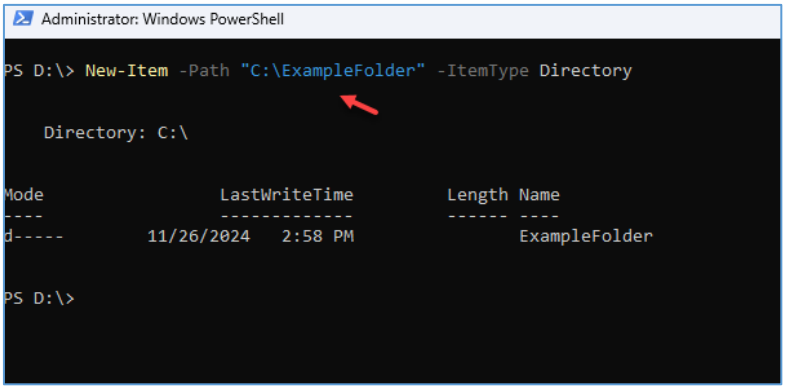
شکل ۸- ۱۰۹۹ دستورات PowerShell

دستور New-Item

www.takbook.com

با استفاده از این دستور می‌توانید File و دایرکتوری مختلفی ایجاد کنید، مثلاً دستور زیر یک پوشه ExampleFolder در ریشه‌ی درایو C ایجاد می‌کند که خروجی را در شکل ۸–۱۱۰۰، مشاهده می‌کنید.

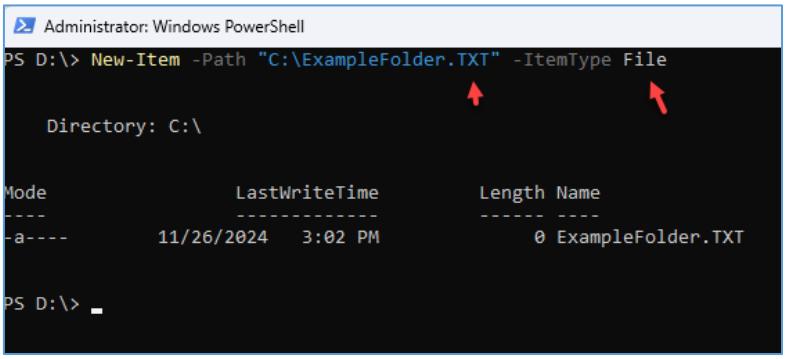
```
New-Item -Path "C:\ExampleFolder" -ItemType Directory
```



شکل ۸- ۱۱۰۰ دستور *New-Item*

مثلاً اگر بخواهیم به جای ایجاد پوشه یک فایل ایجاد کنیم به مانند شکل ۸–۱۱۰۱،باید از دستور زیر استفاده می‌کردیم که در قسمت ItemType باید گزینه‌ی File را انتخاب کنیم و نوع فایل را TXT در نظر گرفتیم.

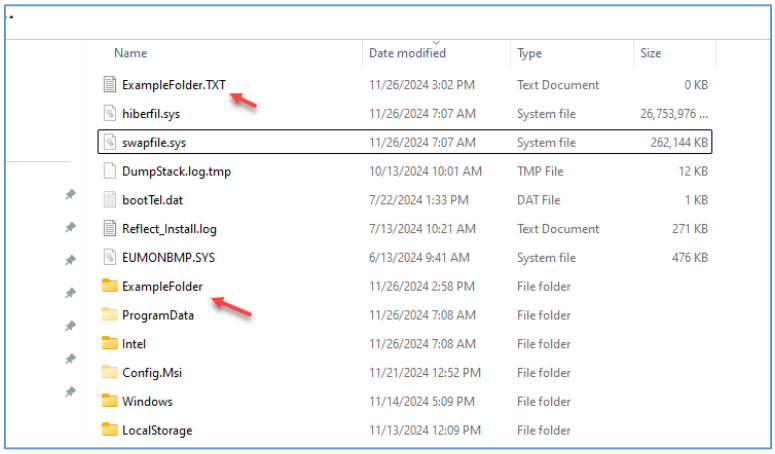
```
New-Item -Path "C:\ExampleFolder.TXT" -ItemType File
```



شکل ۸- ۱۱۰۱ دستور *New-Item*

همان‌طور که در شکل ۸–۱۱۰۲، مشاهده می‌کنید هر دو فایل مورد نظر ایجاد شده است.

www.takbook.com

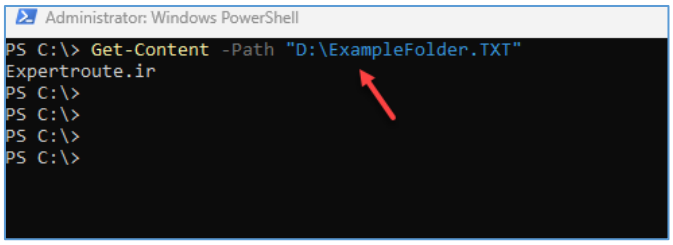


شکل ۸- ۱۱۰۲ دستور *New-Item*

دستور Get-Content

فایل TXT که با هم ایجاد کردیم را باز می‌کنیم و کلمه Expertroute.ir توش می‌نویسیم و به مانند شکل ۸-۱۱۰۳، با دستور Get-Content محتوای آن فایل را در خروجی چاپ می‌کنیم.

```
Get-Content -Path "D:\ExampleFolder.TXT"
```



شکل ۸- ۱۱۰۳ دستور *Get-Content*

به این نکته توجه کنید که اگر در درایو C فایل مورد نظر باز نشد و یا اطلاعات در آن ذخیره نشد در درایو دیگر این کار را انجام دهید.

دستور Copy-Item

برای اینکه یک فایل و یا یک پوشه را در مسیری دیگر کپی کنید می‌توانید از دستور زیر استفاده کنید، دستور زیر فایل ExampleFolder.TXT را از درایو C به درایو F کپی می‌کند.

```
Copy-Item -Path "C:\ExampleFolder.TXT" -Destination "F:\ExampleFolder.TXT"
```

همان‌طور که در شکل ۸-۱۱۰۴، مشاهده می‌کنید دستور مورد نظر اجرا شده و فایل هم به درستی کپی شده است که در دایرکتوری درایو F این موضوع را مشاهده می‌کنید.

www.takbook.com


```
PS C:\> Copy-Item -Path "C:\ExampleFolder.TXT" -Destination "F:\ExampleFolder.TXT"
PS C:\> f:
PS F:\> Get-ChildItem


    Directory: F:\

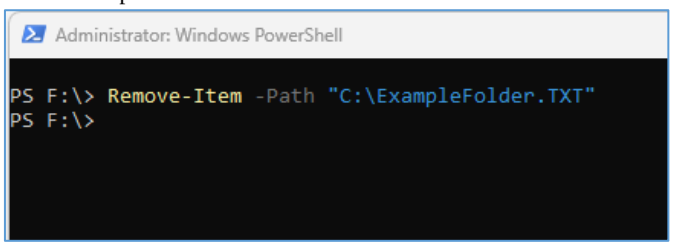

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          7/3/2024   8:19 AM                Auto.Clicker.2.3.2.8
d-----          6/1/2024  11:53 AM                cisco
d-----         3/18/2024   8:12 AM                Compressed
d-----        12/18/2023  12:28 PM                Download
d-----         4/15/2024   7:31 AM                edata
d-----         11/2/2024  11:29 AM                GNS3-VM
d-----         11/2/2024  11:28 AM                GNS3.VM.VMware.Workstation.2.2.49 (1)
d-----          1/1/2024  11:07 AM                iVMS-4200alarmPicture
d-----         4/15/2024   7:31 AM                KEYGEN
d-----         6/23/2024   8:26 AM                Logo Experroute
d-----          8/7/2024   3:36 PM                madarek
d-----         4/15/2024   7:31 AM                Microsoft.Silverlight.5.1.50918.0
d-----         9/29/2024   1:19 PM                New folder
d-----         11/5/2024  12:05 PM                New folder (2)
d-----          1/2/2024   2:33 PM                PSAutoRecover
d-----         6/24/2024   1:12 PM                RDSSS
da----         3/17/2024   6:55 AM                Shadow-Sharifi
d-----         4/15/2024   7:31 AM                Telegram Desktop
d-----         3/18/2024   8:05 AM                Video
d-----        12/11/2023   7:04 AM                VisionSalary
d-----        12/13/2023   8:36 AM                Xshell.5.0.0835
d-----        12/13/2023   8:36 AM                لاومسا
d-----         6/23/2024   8:24 AM                آرسک
-a----         11/4/2024   9:39 AM       34394877 Cisco-CCNP-Enterprise-ENARSI-300-410 - Copy2.docx
-a----        11/26/2024   3:02 PM              0 ExampleFolder.TXT
-a----         11/2/2024  11:04 AM      957067937 GNS3.VM.VMware.Workstation.2.2.49 (1).zip
```

شکل ۸- ۱۱۰۴ دستور *Copy-Item*

دستور Remove-Item

برای حذف یک فایل یا پوشه می‌توانیم از این دستور استفاده کنیم که خروجی آن را در شکل ۸–۱۱۰۵ مشاهده می‌کنید.

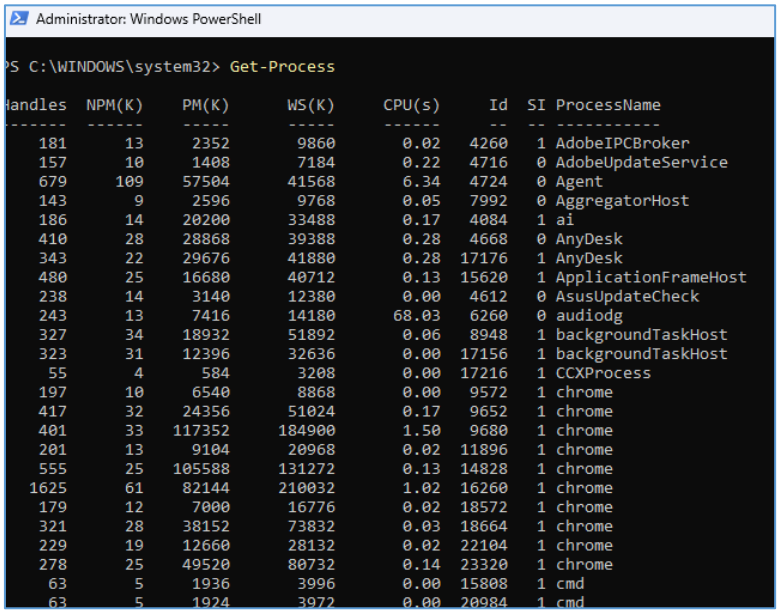
Remove-Item -Path "C:\ExampleFolder.TXT"



شکل ۸- ۱۱۰۵ دستور *Remove-Item*

دستورات بسیار زیادی وجود دارد که باید در مواقع نیاز از آنها استفاده کنیم، مثلاً برای اینکه متوجه شویم که چه Processهایی در سیستم شما در حال کار هستند می‌توانیم از دستور Get-Process استفاده کنیم که خروجی آن را در شکل ۸–۱۱۰۶، مشاهده می‌کنید.

www.takbook.com



شکل ۸- ۱۱۰۶ دستور Get-Process

مثلاً برای اینکه فرآیند AnyDesk را که در شکل ۸-۱۱۰۶، مشاهده می‌کنید ببندیم باید از دستور زیر استفاده کنیم:

Stop-Process -Name "AnyDesk”

بعد از اجرای دستور به مانند شکل ۸-۱۱۰۷، باید یکی از کلیدهای Y یا A را وارد کنید تا Process مورد نظر بسته شود.

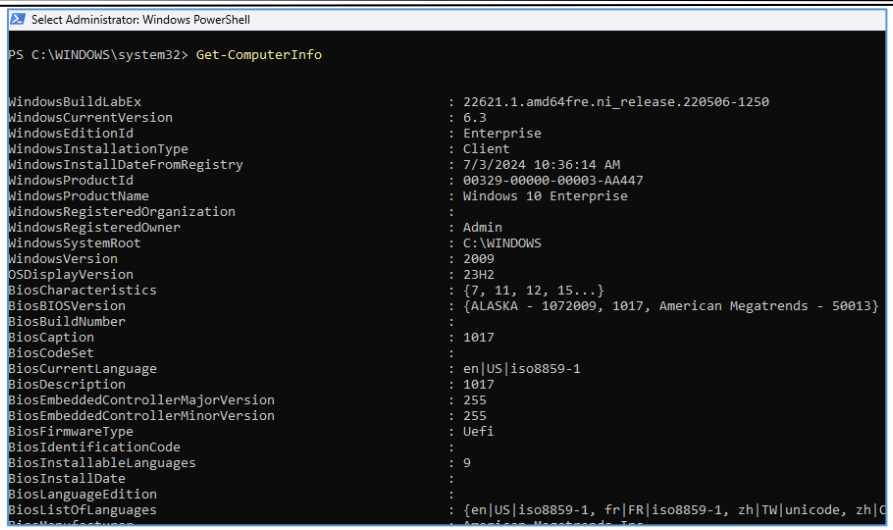
```
PS C:\WINDOWS\system32> Stop-Process -Name "AnyDesk"

Confirm
Are you sure you want to perform the Stop-Process operation on the following item: AnyDesk(4668)?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A
PS C:\WINDOWS\system32> Get-Process
```

شکل ۸- ۱۱۰۷ دستور Get-Process

برای نمایش اطلاعات سیستم خود می‌توانید از دستور Get-ComputerInfo استفاده کنید، که در خروجی شکل ۸-۱۱۰۸، این دستور مشخص شده است.

www.takbook.com

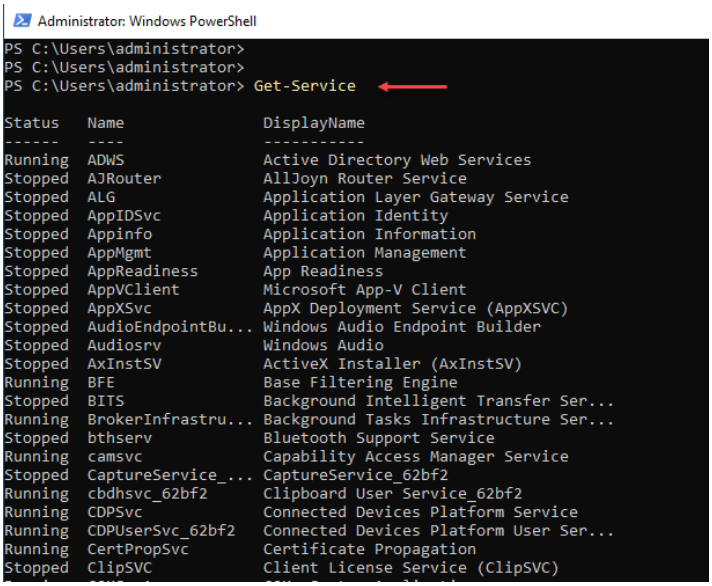


شکل ۸- ۱۱۰۸ دستور *Get-Process*

برای نمایش اینکه چه کاربری وارد سیستم شما شده می‌توانید از دستور زیر استفاده کنید:

```
Get-WmiObject -Class Win32_ComputerSystem | Select-Object -Property UserName
```

برای اینکه در PowerShell متوجه شویم که چه سرویس‌هایی در حال کار می‌باشند می‌توانیم از دستور Get-Service استفاده کنیم که این عمل را در شکل ۸–۱۱۰۹، مشاهده می‌کنید.

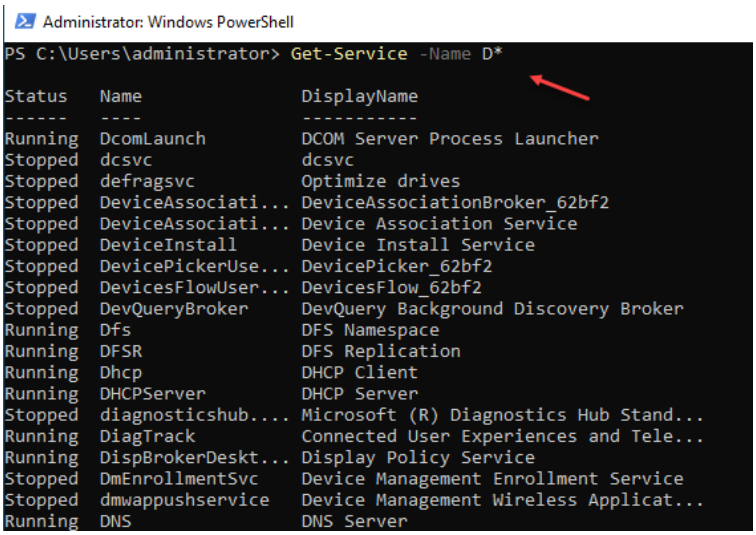


شکل ۸- ۱۱۰۹ دستور *Get-Service*

www.takbook.com

شاید در این بخش بخواهید سرویس‌هایی با نام D را از بقیه‌ی سرویس‌ها جدا کنید؛ برای این کار از دستور زیر استفاده می‌کنیم که خروجی آن را در شکل ۸-۱۱۱۰، مشاهده می‌کنید.

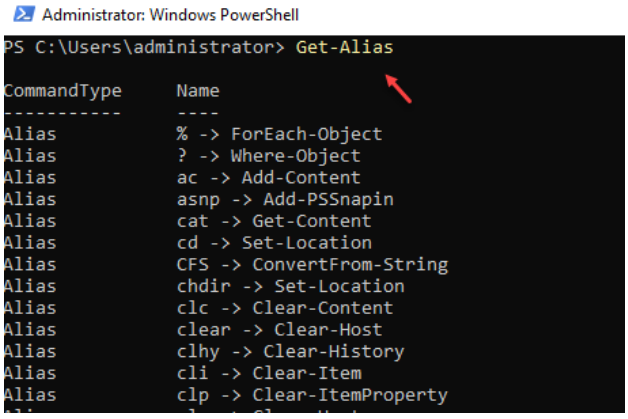
```
Get-Service -Name D*
```



شکل ۸- ۱۱۱۰ *Get-Service*

همان‌طور که در شکل ۸-۱۱۱۰، مشاهده می‌کنید با واردکردن دستور Get-Service -Name D* لیست سرویس‌هایی که با حرف D در حال کار می‌باشند را برای ما لیست کرده است.

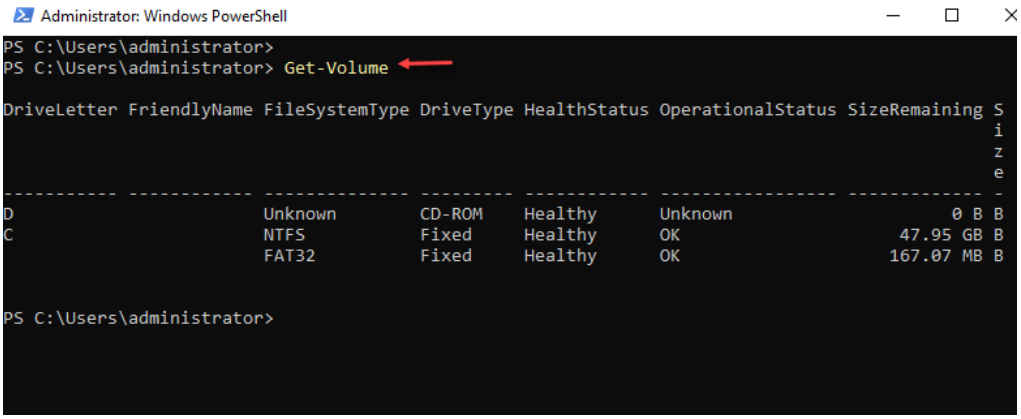
دستوری با نام Alias وجود دارد که با واردکردن Get-Alias می‌توانید لیست دستورات مخفف و کوتاه شده را مشاهده کنید، مثلاً به‌جای اینکه دستور Add-Content را وارد کنیم، از دستور کوتاه شده‌ی ac استفاده می‌کنیم که خروجی آن را در شکل ۸-۱۱۱۱، مشاهده می‌کنید.



شکل ۸- ۱۱۱۱ *Get-Alias*

www.takbook.com

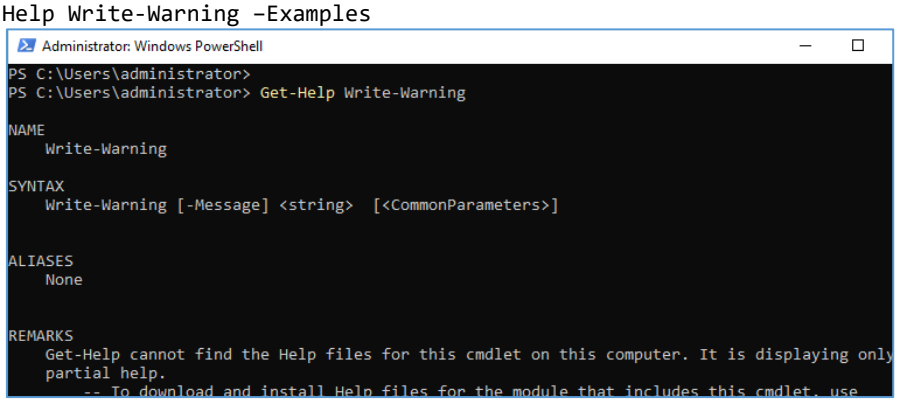
با دستور Get-Volume می‌توانید لیست درایوهای خود را به‌مانند شکل ۸-۱۱۱۲، مشاهده کنید.



شکل ۸-۱۱۱۲ *Get-Volume*

با استفاده از دستور Get-Help می‌توانیم متوجه شویم که چگونه از یک دستور داخل PowerShell استفاده کنیم، مثلاً با اجرای دستور Get-Command لیست دستورات مشخص می‌شود و بعد ازآن می‌توانیم دستور موردنظر را به‌مانند شکل ۸-۱۱۱۳، جلوی Get-Help وارد کنیم تا اطلاعات درباره‌ی آن مشخص شود و برای اینکه مثالی از دستور موردنظر را مشاهده کنید، در ادامه‌ی دستور قبلی، دستور Examples– را اضافه کنید؛ یعنی به‌صورت زیر وارد کنید.

```
Get-Help Write-Warning -Examples
```



شکل ۸-۱۱۱۳ *Get-Help*

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

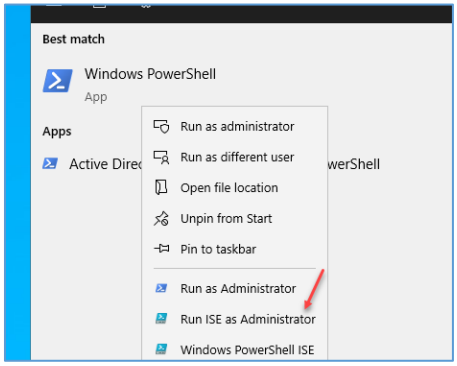
تذکر: زمانی که دستوری را در حال تایپ کردن هستید، می‌توانید با کلیک بر روی دکمه‌ی TAB دستور کامل آن را به‌صورت خودکار مشاهده کنید؛ مثلاً با واردکردن دستور Get-c و بعد فشردن کلید TAB

www.takbook.com

می‌توانید دستور کامل آن، یعنی GET-Command را مشاهده کنید، یا با واردکردن دستور -GET و فشردن کلید TAB به‌دفعات متعدد می‌توانید، تمام دستورات بعد -GET را مشاهده کنید.

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

برای اجرای این سرویس به مانند شکل ۸-۱۱۱٤، بر روی Taskbar روی آیکون PowerShell کلیک راست کنید و گزینه‌ی Run ISE as Administrator را انتخاب کنید تا شکل ۸-۱۱۱۵، ظاهر شود.

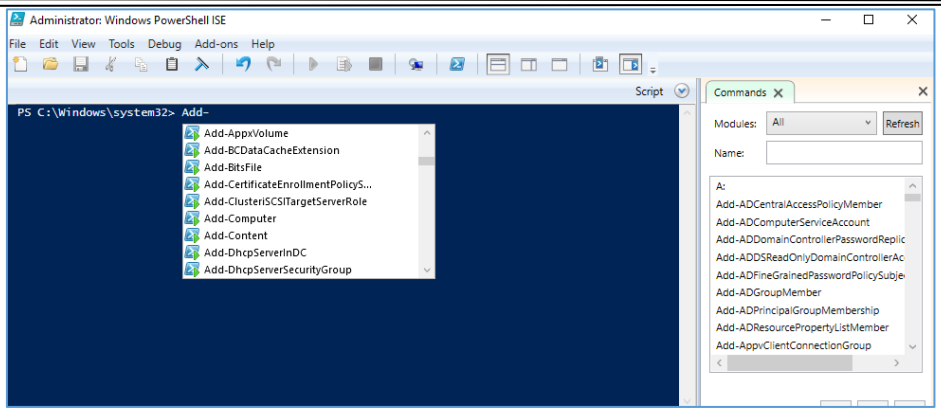


شکل ۸- ۱۱۱۴ Windows PowerShell ISE

همان‌طور که در شکل ۸-۱۱۱۵، مشاهده می‌کنید با واردکردن کلمه‌ی -Add تمام دستورات بعدازآن را به ما نمایش داده است که شما می‌توانید یکی از دستورات را انتخاب کنید.

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

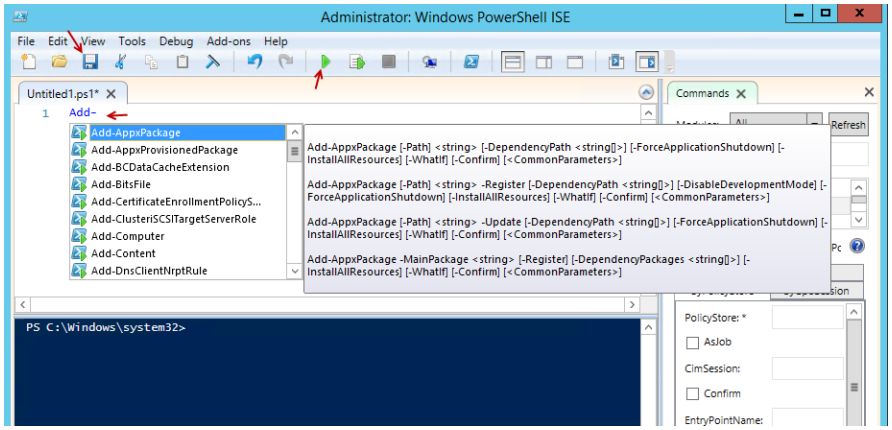
www.takbook.com



شکل ۸- ۱۱۱۵ Windows PowerShell ISE

یکی دیگر از راه‌های استفاده از دستورات PowerShell، این است که از Script استفاده کنیم؛ یعنی اینکه دستورات را داخل یک فایل قرار دهیم و از آن در موقع نیاز استفاده کنیم، برای این کار در شکل ۸–۱۱۱۵، بر روی آیکون Script که با فلش هم مشخص‌شده کلیک کنید تا شکل ۸–۱۱۱۶ ظاهر شود.

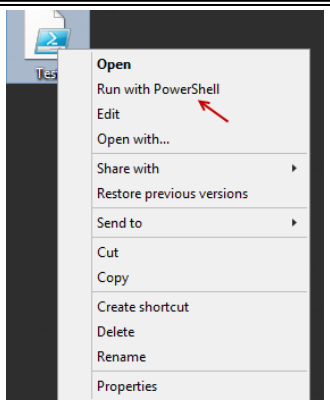
در شکل ۸–۱۱۱۶، قسمت Script فعال‌شده است و برای اینکه از این قسمت استفاده کنیم باید دستورات موردنظر را در قسمت مشخص‌شده وارد کنیم و برای اینکه از دستورات، خروجی تهیه کنیم باید بر روی آیکون Start کلیک کنیم و برای ایجاد فایل Script باید بر روی آیکون Save کلیک کنیم و فایل موردنظر را بانام مشخص، در جای مشخص ذخیره کنیم.



شکل ۸- ۱۱۱۶ Windows PowerShell ISE

همان‌طور که در شکل ۸–۱۱۱۷، مشاهده می‌کنید، Script موردنظر بانام Test در جای مناسب ذخیره‌شده است و برای اجرای آن باید روی آن کلیک راست کنیم و گزینه‌ی Run with PowerShell را انتخاب کنیم تا فایل موردنظر اجرا شود.

www.takbook.com



شکل ۸- ۱۱۱۷ *Windows PowerShell ISE*

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

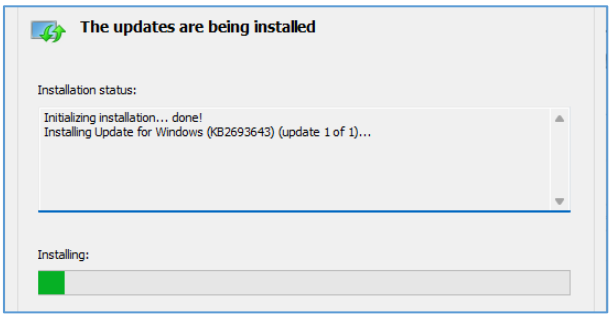
۸-۳-۳۱-۱ مدیریت Active Directory از طریق PowerShell

مدیریت Active Directory (AD) از طریق PowerShell یکی از کاربردهای اصلی این ابزار است و به مدیران سیستم اجازه می‌دهد تا وظایف مختلفی را به صورت خودکار و سریع انجام دهند. برای مدیریت Active Directory با PowerShell، ابتدا باید ماژول Active Directory نصب و در دسترس باشد.

روی ویندوز سرور اگر Active Directory نصب باشد، ماژول AD به صورت پیش‌فرض در دسترس خواهد بود، اما اگر بخواهید بر روی ویندوز عادی این ویژگی را فعال کنید باید از نرم‌افزار RSAT (Remote Server Administration Tools) استفاده کنید که می‌توانید از لینک زیر دانلود کنید:

https://www.microsoft.com/en-us/download/details.aspx?id=45520

بعد از دانلود به مانند شکل ۸-۱۱۱۸، آن را نصب کنید تا این سرویس به ویندوز شما اضافه شود.

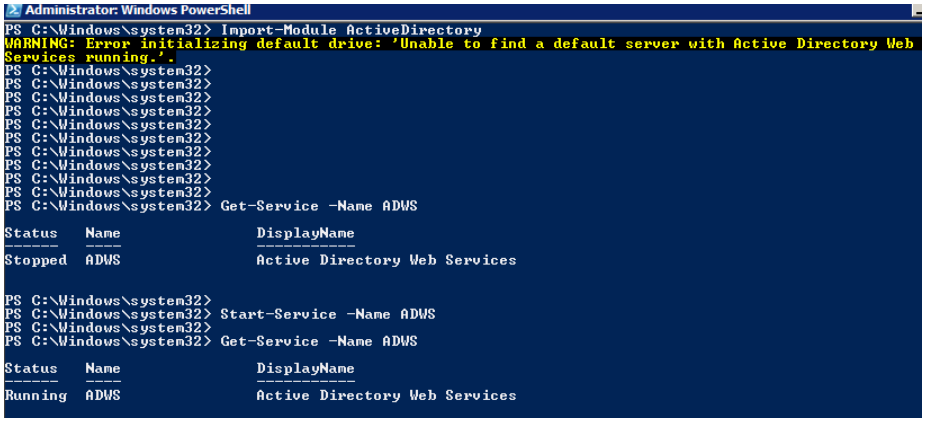


شکل ۸- ۱۱۱۸ نصب *RSAT*

بعد از فعال‌سازی سرویس مورد نظر با استفاده از دستور Import-Module ActiveDirectory باید دستورات مورد نیاز ActiveDirectory را وارد PowerShell کنید.

www.takbook.com

توجه داشته باشید در بعضی از سرورها دستورات Active Directory کار نمی‌کنند و این مشکل اصولاً به خاطر فعال نبودن سرویس ADWS است که به مانند شکل زیر ۸-۱۱۱۹، با استفاده از دستور Get-Service -Name ADWS می‌توانید وضعیت سرویس را مشاهده کنید و اگر Stop بود می‌توانید با دستور Start-Service -Name ADWS فعال کنید تا مشکل حل شود.



شکل ۸- ۱۱۱۹ نصب سرویس ADWS

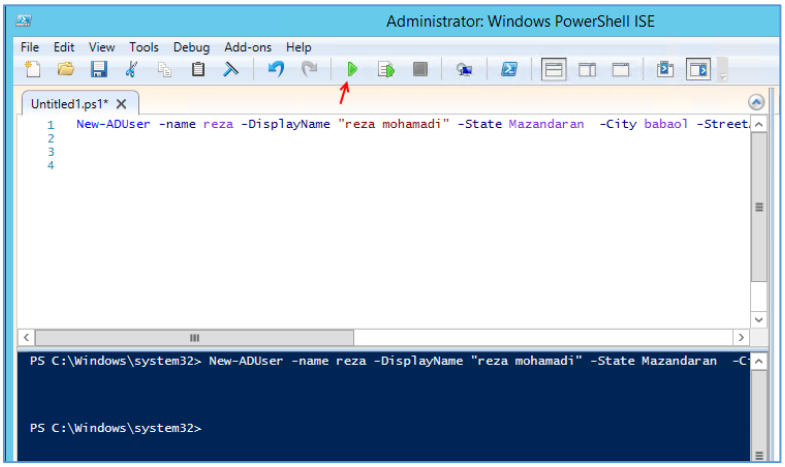
ایجاد کاربر از طریق PowerShell

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

همان‌طور که در شکل ۸-۱۱۲۰، مشاهده می‌کنید، وارد سرویس ISE شده ایم که قبلاً با این سرویس کار کرده بودیم. دستوراتی را که در شکل می‌بینید برای ایجاد یک کاربر با نام و مشخصات خاص می‌باشد که با هم آن‌ها را بررسی خواهیم کرد.

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

www.takbook.com



شکل ۸- ۱۱۲۰ ایجاد کاربر از طریق PowerShell

دستورات بالا را به‌صورت کلمه به کلمه بررسی می‌کنیم. برای ایجاد کاربر از طریق PowerShell باید از دستور New-ADUser استفاده کرد که در دستور قبلی مشاهده شد. پس از وارد کردن این دستور، باید یک Dash (تیره) قرار دهیم. با این کار، لیستی از دستورات مرتبط با New-ADUser به‌صورت منو باز می‌شود که می‌توانید بسته به نیاز خود از آن‌ها استفاده کنید. بنابراین، بعد از هر دستور باید یک تیره قرار دهید تا دستورات مربوط به دستور اصلی نمایش داده شوند.

مرحله بعدی، معرفی نام کاربر است. ابتدا باید Name – را وارد کرده و سپس نام کاربر را بنویسید. به‌عنوان مثال، در اینجا نام کاربر "Reza" است. پس از این کار، می‌توانید کد را بدون وارد کردن سایر اطلاعات اجرا کنید، زیرا اطلاعات دیگر برای تکمیل مشخصات کاربر استفاده می‌شوند. برای مثال، با استفاده از دستور DisplayName – می‌توانید نام کامل کاربر را وارد کنید.

نکته مهم در این قسمت این است که اگر نامی که وارد می‌کنید شامل چند کلمه جدا از هم باشد، باید آن را در داخل دابل کوتیشن ("") قرار دهید. به‌عنوان مثال: "Reza Mohamadi". این کار از بروز خطا (Error) جلوگیری می‌کند.

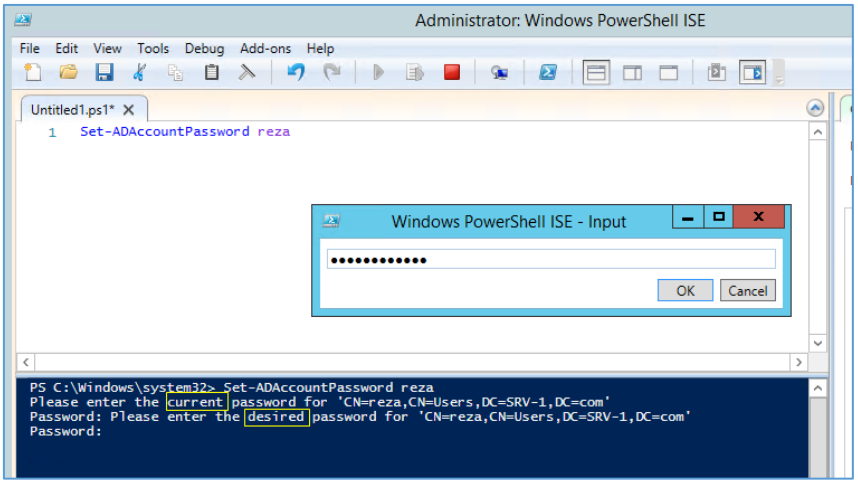
سایر دستورات مانند نام استان، شهر، خیابان و موارد مشابه را می‌توانید به‌دلخواه وارد کنید. این اطلاعات مربوط به Properties یک کاربر هستند که قبلاً بررسی کردیم. در نهایت، با کلیک بر روی آیکون Run Script، این دستورات اجرا شده و کاربر موردنظر ایجاد می‌شود.

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

```
Set-ADAccountPassword reza
```

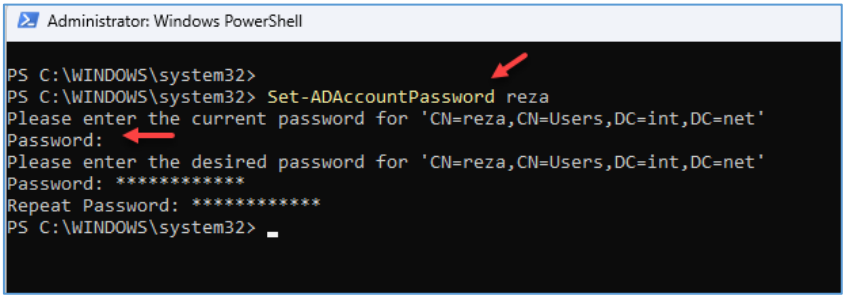
www.takbook.com

این دستور، برای قرار دادن رمز عبور بر روی کاربر موردنظر می‌باشد برای این کار به مانند شکل ۸-۱۱۲۱، باید ابتدا دستورSet-ADAccountPassword را وارد کنید و بعد از آن، باید نام کاربر را که در قسمت name– آن وارد کردید را اینجا وارد کنید تا پنجره دریافت رمز عبور برای شما ظاهر شود. اگر کاربر شما از قبل، رمز عبور بر روی آن Set شده است، باید در پنجره ی current، رمز موردنظر را وارد کنید؛ وگرنه باید بدون وارد کردن کلمه‌ای، بر روی ok کلیک کرد و بعد، باید در قسمت Desired، رمز جدید را وارد کنید و بعد بر روی ok کلیک کنید و در پنجره آخر، رمز را دوباره تکرار کنید. بر روی ok کلیک کنید تا به کاربر موردنظر، رمز عبور تعلق گیرد.



شکل ۸- ۱۱۲۱ بررسی دستور Set-ADAccountPassword

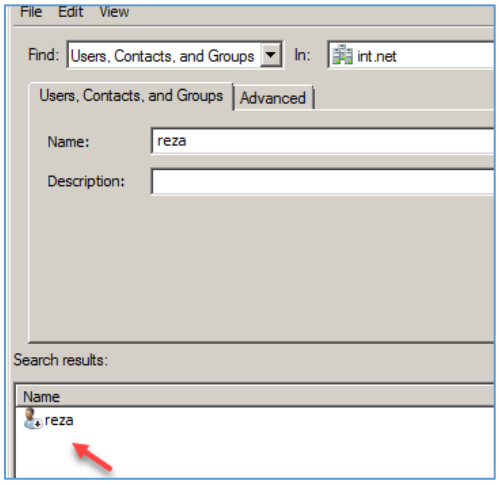
اگر همین دستور را در PowerShell عادی اجرا کنیم شکل ۸-۱۱۲۲، در قسمت اول چون کاربر رمزی ندارد نیازی نیست آن رمز را وارد کنید و در دو قسمت بعدی رمز را دو بار وارد کنید.



شکل ۸- ۱۱۲۲ بررسی دستور Set-ADAccountPassword

تا به اینجا یک کاربر با جزئیات مشخص‌شده، ایجاد و رمز عبور آن را هم مشخص کردیم؛ ولی اگر در حال حاضر، وارد سرویس Active Directory Users and Computers شوید در قسمت Users کاربر موردنظر به مانند شکل ۸-۱۱۲۳، غیرفعال خواهد بود.

www.takbook.com

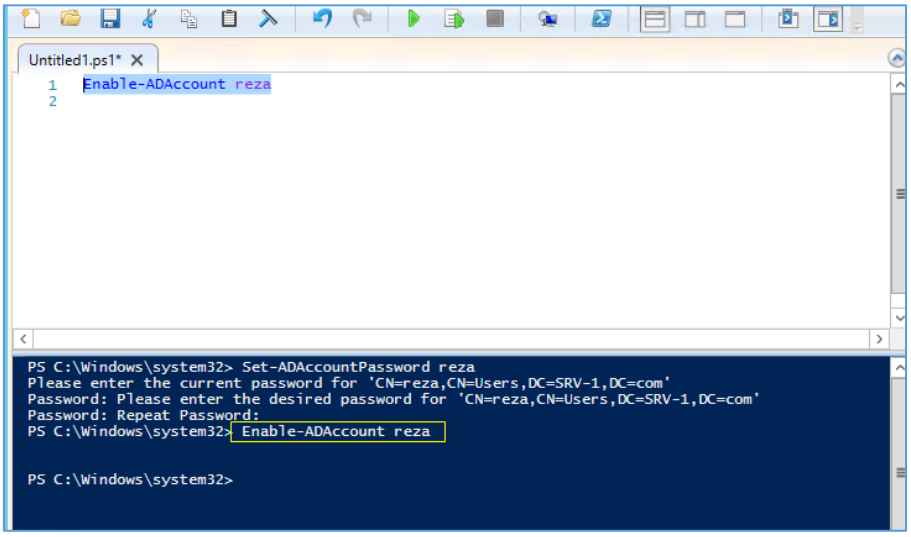


شکل ۸- ۱۱۲۳ بررسی دستور *Set-ADAccountPassword*

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

```
Enable-ADAccount reza
```

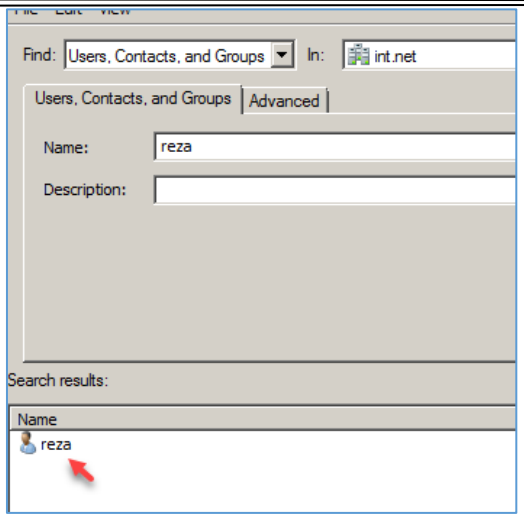
در این دستور، باید به جای Reza، نام کاربر خود را وارد کنید تا کاربر موردنظر فعال شود. همان‌طور که گفتیم برای اجرای این دستورات باید بر روی آیکون Run Script در بالای صفحه شکل ۸-۱۱۲٤، کلیک کنید.



شکل ۸- ۱۱۲۴ بررسی دستور *Set-ADAccountPassword*

همان‌طور که در شکل ۸-۱۱۲۵، مشاهده می‌کنید، کاربر Reza فعال شده است و توانایی ورود به سیستم خود را دارد.

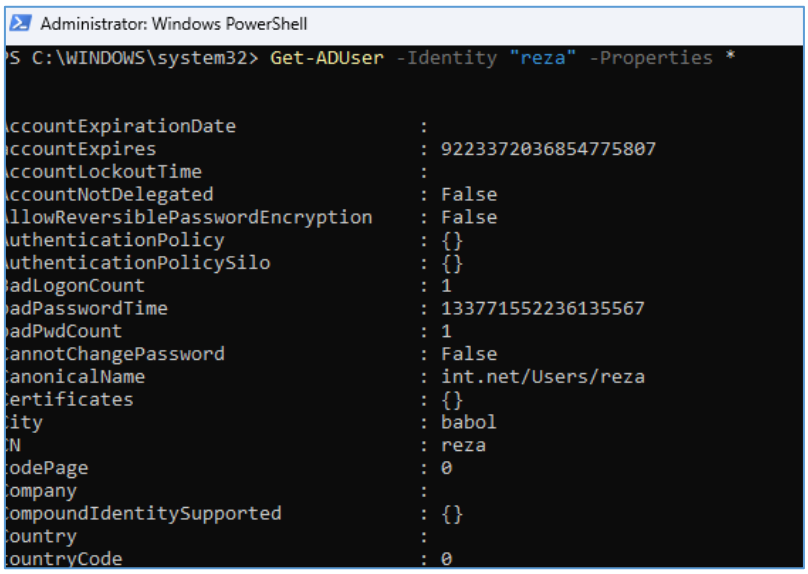
www.takbook.com



شکل ۸- ۱۱۲۵ بررسی کاربر جدید

برای اینکه اطلاعات کاملی از کاربر ایجاد شده را ببینیم می‌توانیم به مانند شکل ۸-۱۱۲٦، از دستور زیر استفاده کنیم

```
Get-ADUser -Identity "reza" -Properties *
```

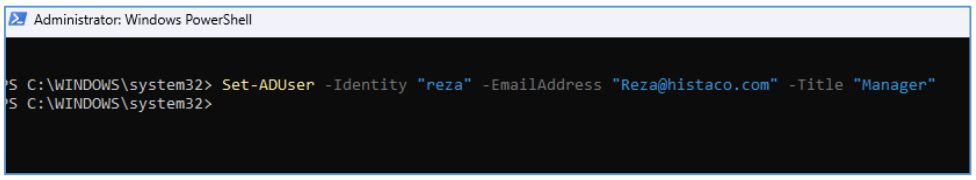


شکل ۸- ۱۱۲۶

www.takbook.com

برای اینکه بتوانید اطلاعات کاربر را ویرایش کنید می‌توانید از دستور زیر استفاده کنید، با استفاده از دستور Set-ADUser، کاربر مورد نظر انتخاب و اطلاعات آن ویرایش می‌شود که این موضوع را در شکل ۸-۱۱۲۷، مشاهده می‌کنید.

```
Set-ADUser -Identity "reza" -EmailAddress "Reza@histaco.com" -Title "Manager"
```

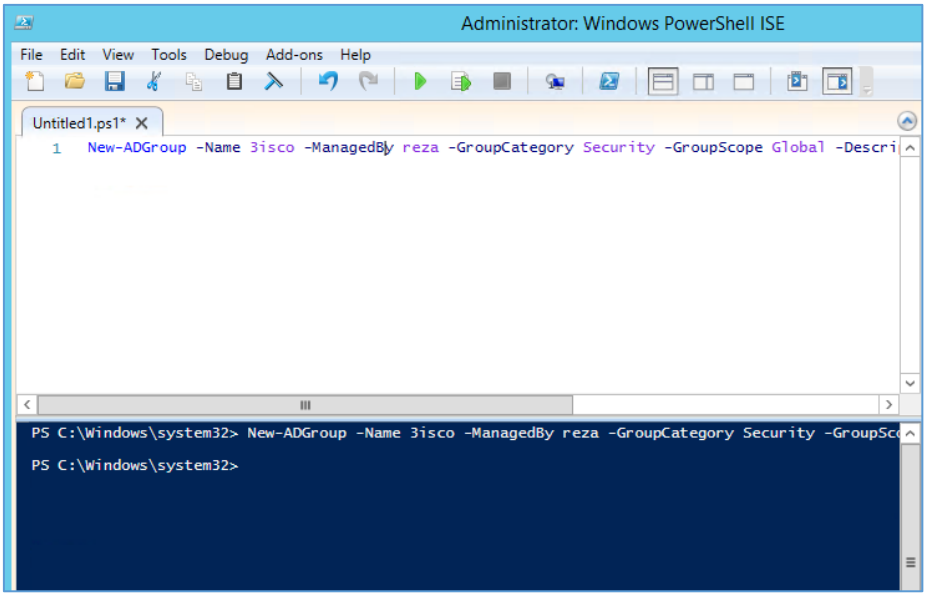


شکل ۸- ۱۱۲۷ بررسی کاربر جدید

۸-۳-۳۱-۲ ایجاد گروه از طریق PowerShell

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

در شکل ۱۱۲۸، دستورات مربوط به ایجاد گروه اجرا شده است و گروهی با نام ExpertRoute، با تنظیمات موردنظر ایجاد شده است که در زیر، آن‌ها را بررسی می‌کنیم.



شکل ۸- ۱۱۲۸ ایجاد گروه از طریق PowerShell

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

www.takbook.com

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

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

۳-۳۱-۳-۸ نحوه ی ایجاد Organization Unit از طریق PowerShell

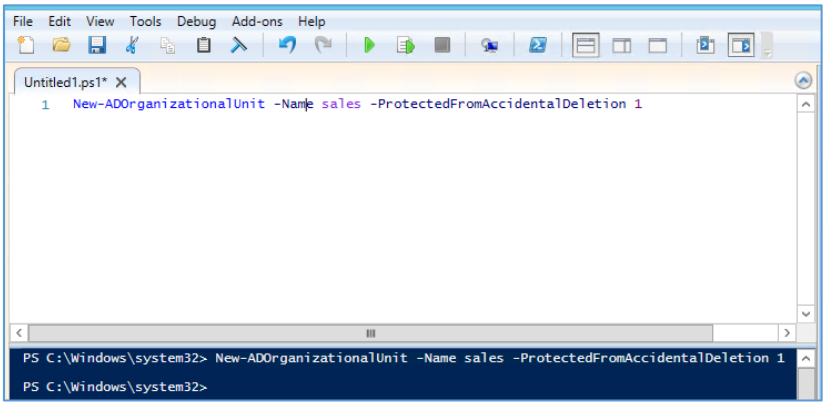
برای ایجاد واحد سازمانی، دوباره وارد Power shell ISE شوید و دستورات زیر را اجرا کنید:

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

با استفاده از دستور New-ADOrganizationalUnit، می‌توانیم یک واحد سازمانی در Active Directory خود ایجاد کنیم به این صورت که ابتدا دستور New-ADOrganizationalUnit را وارد می‌کنیم و بعد از آن با دستور Name– و نام واحد سازمانی که در اینجا Sales می‌باشد، می‌توانیم به راحتی یک واحد سازمانی ایجاد کنیم. در ادامه‌ی دستورات بالا، دستور ProtectedFromAccidentalDeletion 1– را مشاهده می‌کنید که این دستور، برای جلوگیری از حذف شدن شی و یا object موردنظر می‌باشد. زمانی که عدد جلوی آن ۱ باشد یعنی اینکه این قابلیت فعال شده است و اگر صفر باشد یعنی غیر فعال شده است. توجه داشته باشید که این قسمت را قبلاً در اوای این فصل بررسی کردیم.

همان‌طور که در شکل ۸-۱۱۲۹ مشاهده می‌کنید، گروه سازمانی مورد به درستی ایجاد شده است.

www.takbook.com



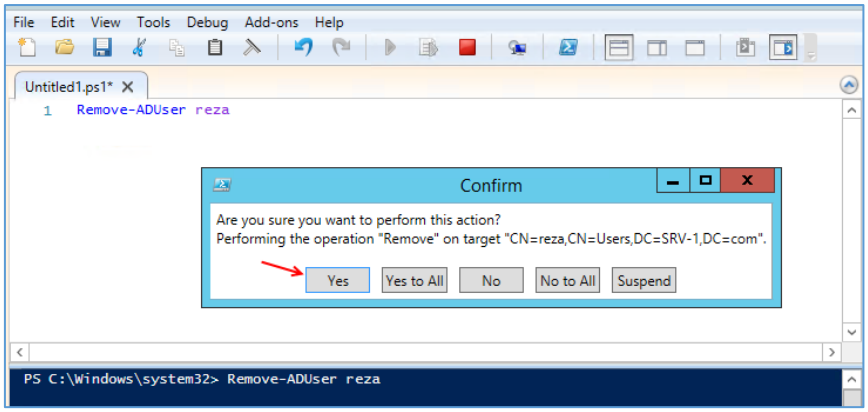
شکل ۸- ۱۱۲۹ نحوه ی ایجاد *Organization Unit*

۸-۳-۳۱-۳ حذف users،Groups و Organization Unit از طریق Power Shell

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

```
Remove-ADUser reza
```

بعد از اجرای دستور قبلی در PowerShell، شکل ۸-۱۱۳۰، ظاهر می‌شود که از شما سوأل می‌شود که آیا می‌خواهید کاربر Reza را که در قسمت Users قرار دارد، حذف کنید؟ اگر بر روی Yes و Yes to All کلیک کنید، کاربر موردنظر حذف خواهد شد.



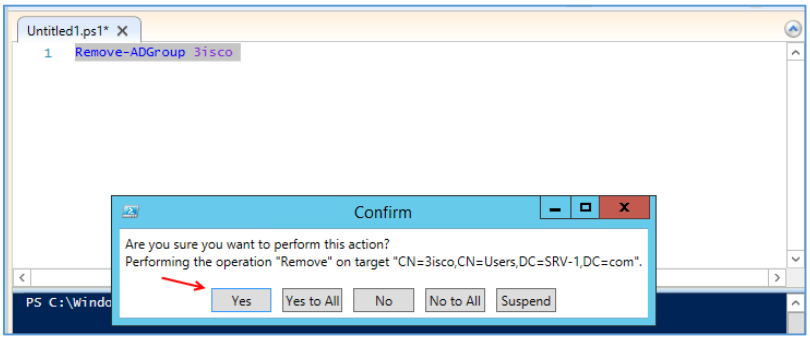
شکل ۸- ۱۱۳۰ حذف users،Groups و *Organization Unit*

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

```
Remove-ADGroup ExpertRoute
```

www.takbook.com

همان‌طور که در شکل ۸-۱۱۳۱، مشاهده می‌کنید با دستور Remove-ADGroup و بعد از آن، نام گروه موردنظر و اجرای آن از شما سوأل می‌شود که گروه موردنظر را می‌خواهید حذف کنید یا نه؟



شکل ۸- ۱۱۳۱ حذف users، Groups و Organization Unit

برای حذف واحدهای سازمانی باید از دستور زیر استفاده کنید:

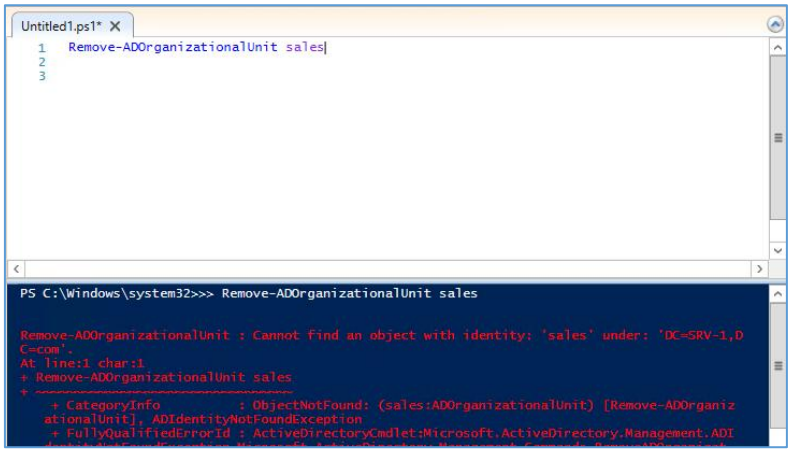
```
Remove-ADOrganizationalUnit sales
```

Sales، نام واحد سازمانی ما می‌باشد که در قسمت قبل ایجاد کرده بودیم و می‌خواهیم آن را حذف کنیم.

بعد از اینکه دستور را اجرا کنید، با Error شکل ۸-۱۱۳۲، مواجه خواهید شد.

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

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



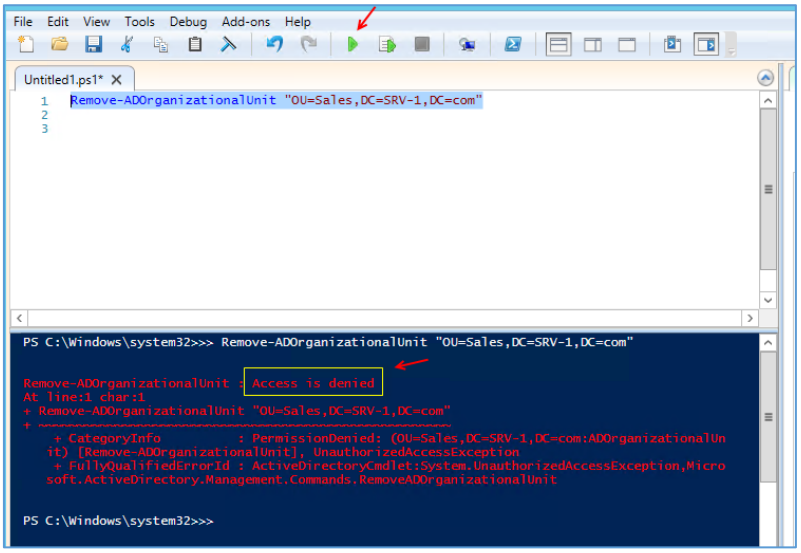
شکل ۸- ۱۱۳۲ حذف users، Groups و Organization Unit

در دستور قبلی، برای بدست آوردن شی Sales باید به این صورت عمل کنیم که داخل ۲ تا "" باید نام OU=Sales و بعد کاما قرار دهیم و بعد DC=SERV-1 که نام دومین ما می‌باشد. بعد کاما و در آخر

www.takbook.com

DC=Com را وارد می‌کنیم. این دستور به این صورت می‌باشد که باید نام واحد سازمانی و نام دومین را ذکر کنیم تا با خطا قبلی مواجه نشویم.

بعد از اجرای دستور موردنظر در PowerShell، به مانند شکل ۸-۱۱۳۳، با خطا مواجه شدیم که به این نکته اشاره دارد که دسترسی به شی موردنظر را نداریم. این مشکل به خاطر این است که در هنگام تعریف شی، آن را به صورت محافظت شده ایجاد کردیم. برای حل این مشکل، باید دستور محافظت کننده‌ی شی موردنظر را غیرفعال کنیم.



شکل ۸- ۱۱۳۳ حذف users، Groups و Organization Unit

برای این کار، ابتدا دستور زیر را اجرا می‌کنیم:

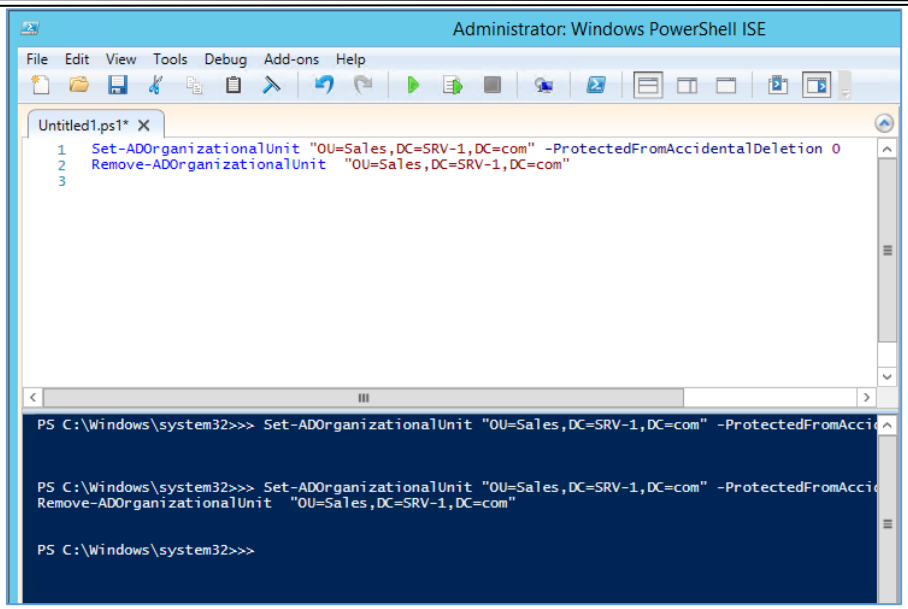
```
Set-ADOrganizationalUnit "OU=Sales,DC=SRV-1,DC=com" -
ProtectedFromAccidentalDeletion 0
```

در این دستور، شی Sales را با دستور Set-ADOrganizationalUnit انتخاب کردیم و با دستور ProtectedFromAccidentalDeletion 0، محافظت کننده‌ی آن را غیرفعال کردیم. عدد صفر به معنی غیرفعال شدن می‌باشد.

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

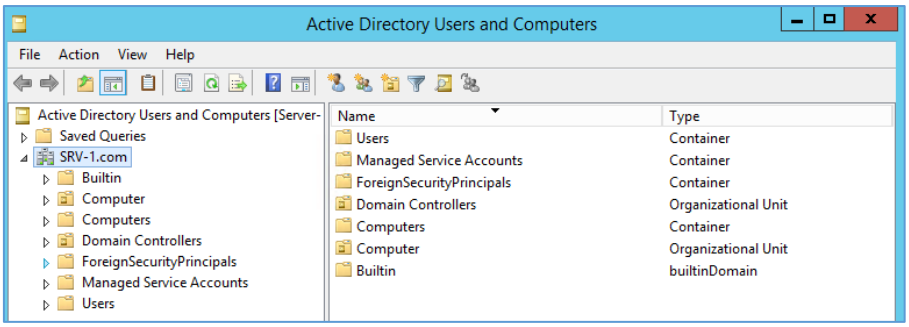
همان‌طور که در شکل ۸-۱۱۳٤، مشاهده می‌کنید، دستورات به صورت پشت سر هم، در دو خط به صورت کامل اجرا شده و شی موردنظر به صورت کامل حذف شده است.

www.takbook.com



شکل ۸- ۱۱۳۴ حذف users، Groups و Organization Unit

همان‌طور که در شکل ۸-۱۱۳۵، مشاهده می‌کنید، گروه سازمانی با Sales به صورت کامل از لیست سرویس حذف شده است.



شکل ۸- ۱۱۳۵ حذف users، Groups و Organization Unit

۸-۳-۳۱-٤ کار با DHCP از طریق دستورات PowerShell

استفاده از PowerShell برای مدیریت سرویس DHCP در ویندوز سرور یک راهکار قدرتمند و سریع برای مدیریت تنظیمات، محدوده آدرس‌ها، کلاینت‌ها و موارد دیگر است. برای این کار، از ماژول DHCPServer استفاده می‌شود که با نصب DHCP روی ویندوز سرور، به‌طور پیش‌فرض نصب و فعال می‌شود.

برای اینکه سرویس DHCP را نصب کنیم باید از دستور زیر استفاده کنیم:

```
Install-WindowsFeature -Name DHCP -IncludeManagementTools
```

www.takbook.com

بعد از نصب سرویس می‌توانید ماژول DHCP را با دستور زیر در PowerShell فراخوانی کنید:

```
Import-Module DHCPServer
```

برای اینکه وضعیت سرویس DHCP را بررسی کنیم می‌توانیم از دستور زیر استفاده کنیم:

```
Get-Service -Name DHCPServer
```

اگر سرویس درحالت Stop قرار داشته باشد می‌توانید با دستور زیر آن را فعال کنید:

```
Start-Service -Name DHCPServer
```

برای مدیریت سرویس DHCP دستور Get-DhcpServerv4Scope است که با معرفی نام سرور، تعداد Scopeهای فعال شده روی آن را نشان می‌دهد.

```
Get-DhcpServerv4Scope -ComputerName Server-1
```

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

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

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

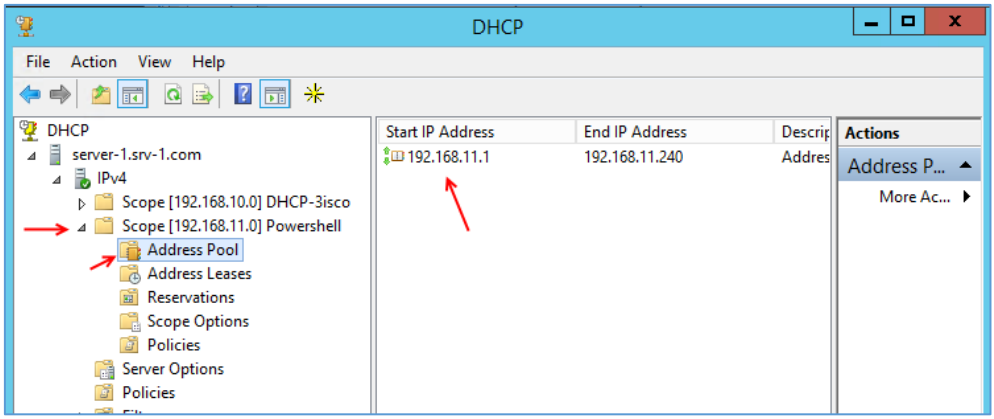
اولین دستوری که مشاهده می‌کنید، دستور Add-DhcpServerv4Scope می‌باشد که برای ایجاد Scope با IPv4 مورد استفاده قرار می‌گیرد. بعد از آن، باید تنظیمات مربوط به آن را انجام دهیم. اولین دستور بعد از آن Name PowerShell- می‌باشد که نام Scope را PowerShell در نظر می‌گیریم. شما می‌توانید هر نام دیگری به جای آن وارد کنید، فقط توجه داشته باشید که اگر در نام خود از فاصله استفاده کردید حتماً نام موردنظر را بین دو دابل کوتیشن "" قرار دهید تا با Error مواجه نشوید. دستور بعدی StartRange 192.168.11.1 می‌باشد که نشان دهنده‌ی آدرس شروع Scope موردنظر می‌باشد. دستور بعدی هم EndEange 192.168.11.240 می‌باشد که آدرس پایانی آن می‌باشد و دستور بعدی، SubnetMask 255.255.255.0 است که Subnet آن را باید مشخص کنید. همان‌طور که قبلاً بیان کردیم، برای اینکه قسمت IP را متوجه شوید به فصل پنجم کتاب، قسمت بررسی IPv4 مراجعه کنید.

www.takbook.com

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

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

همان‌طور که در شکل ۸-۱۱۳۶، در سرویس DHCP مشاهده می‌کنید، Scope با نام PowerShell و با آدرس 192.168.11.0 اضافه شده است و در Address Pool موردنظر Start IP و End IP مشخص‌شده است.



شکل ۸- ۱۱۳۶ کار با DHCP از طریق دستورات PowerShell

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

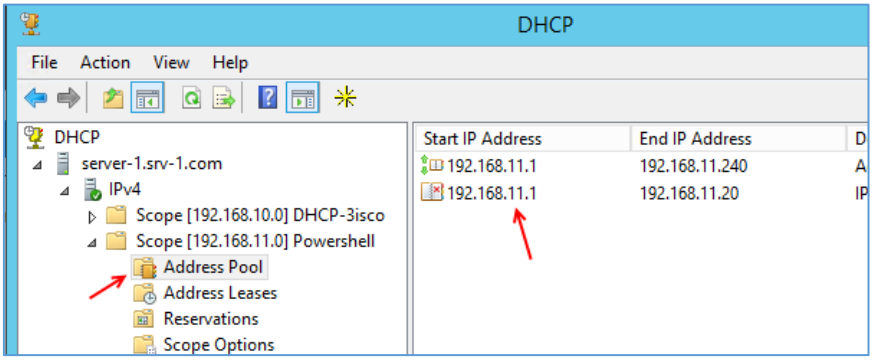
برای ایجاد IP Exclusion، وارد PowerShell می‌شویم و دستور زیر را اجرا می‌کنیم:

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

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

www.takbook.com

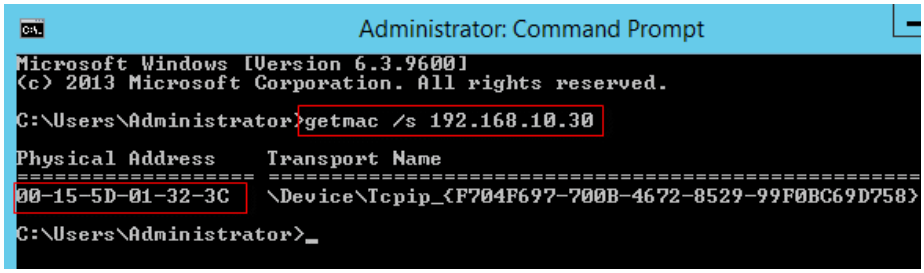
همان‌طور که در شکل ۸-۱۱۳۷، مشاهده می‌کنید، IP Exclusion به درستی وسط دستورات PowerShell ایجاد شده است.



شکل ۸- ۱۱۳۷ کار با DHCP از طریق دستورات PowerShell

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

برای ایجاد Reservations، باید Mac Address کامپیوتر موردنظر را بدست بیاورید؛ به مانند شکل ۸-۱۱۳۸، از دستور getmac /s 192.168.10.30 استفاده می‌کنیم.



شکل ۸- ۱۱۳۸ کار با DHCP از طریق دستورات PowerShell

آدرس MAC کامپیوتر موردنظر را که 00-15-5D-01-32-3C می‌باشد را بدست می‌آوریم و از آن در دستور زیر استفاده می‌کنیم:

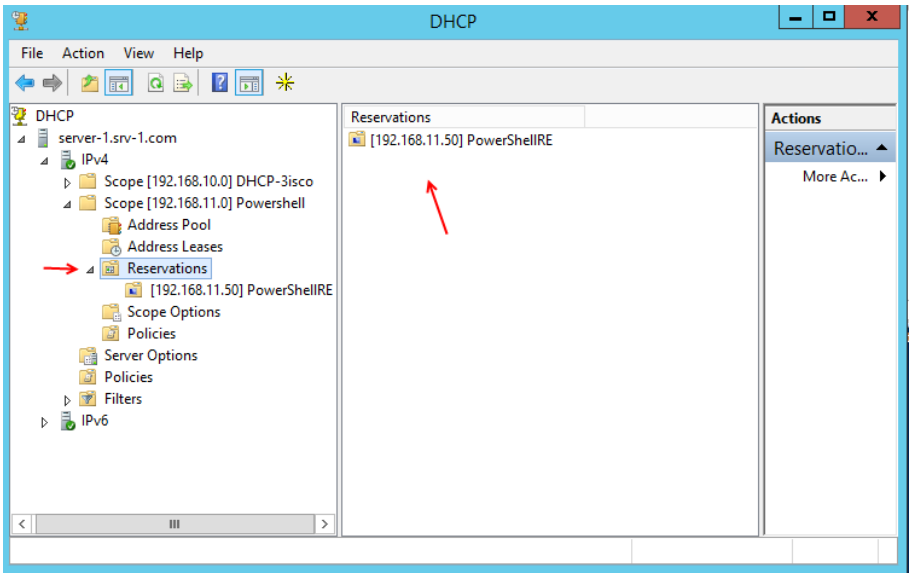
```
Add-DhcpServerv4Reservation -ScopeId 192.168.11.0 -Name PowerShellRE -
IPAddress 192.168.11.50 -Type Both -ClientId 00-15-5D-01-32-3C
```

دستور Add-DhcpServerv4Reservation برای ایجاد Reservation مورد استفاده قرار می‌گیرد. بعد از آن باید از طریق ScopeId 192.168.11.0، آدرس NetID مربوط به Scope موردنظر را وارد کنیم که به جای 192.168.11.0، باید NetID مربوط به شبکه‌ی خود را وارد کنید. بعد از آن از طریق دستور Name PowerShellRE، یک نام برای آن در نظر می‌گیریم که شما باید به جای PowerShellRE، نام دلخواه خود را وارد کنید. در ادامه IPAddress 192.168.11.50 مربوط به کلاینت یا سرور موردنظر را وارد کنید و بعد،

www.takbook.com

نوع آن را با دستور Type Both مشخص کنید. سپس در مهم‌ترین بخش که معرفی Mac address کلاینت یا سرور موردنظر است از طریق دستور ClientId 00-15-5D-01-32-3C، آدرس Mac مربوط به کلاینت موردنظر را وارد کنید و در آخر کار دستور موردنظر را اجرا کنید.

به مانند شکل ۸-۱۱۳۹، با ورود به سرویس DHCP، اگر به قسمت Reservations مراجعه کنید، مشاهده خواهید کرد که عملیات به مانند شکل با موفقیت اجرا شده است.



شکل ۸- ۱۱۳۹ کار با DHCP از طریق دستورات PowerShell

دستورات زیادی برای کار با DHCP در قسمت‌های مختلف وجود دارد که در ادامه‌ی کتاب به آن‌ها خواهیم پرداخت.

۸-۳-۳۱-۵ کار با DNS Server از طریق دستورات PowerShell

مدیریت DNS Server از طریق دستورات PowerShell به شما امکان می‌دهد تنظیمات سرور DNS را به راحتی انجام دهید، رکوردها را مدیریت کنید، و وضعیت سرویس را بررسی کنید. برای این کار، معمولاً از ماژول DNS Server استفاده می‌شود که بخشی از Windows Server است.

برای نصب سرویس DNS با استفاده از PowerShell باید از دستور زیر استفاده کنیم:

```
Install-WindowsFeature -Name DNS -IncludeManagementTools
```

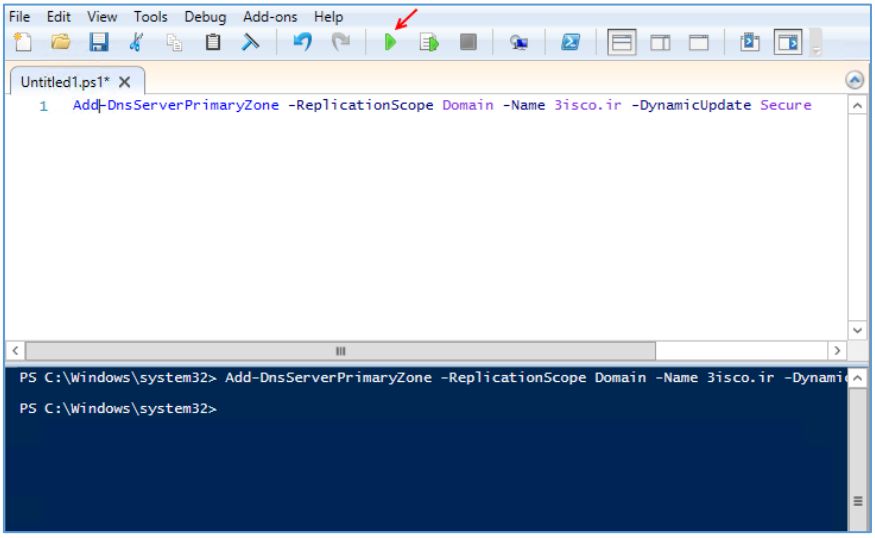
سرویس PowerShell ISE را با اولویت کاربر Administrator اجرا می‌کنیم.

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

www.takbook.com


```
Add-DnsServerPrimaryZone -ReplicationScope Domain -Name ExpertRoute.ir
-DynamicUpdate Secure
```

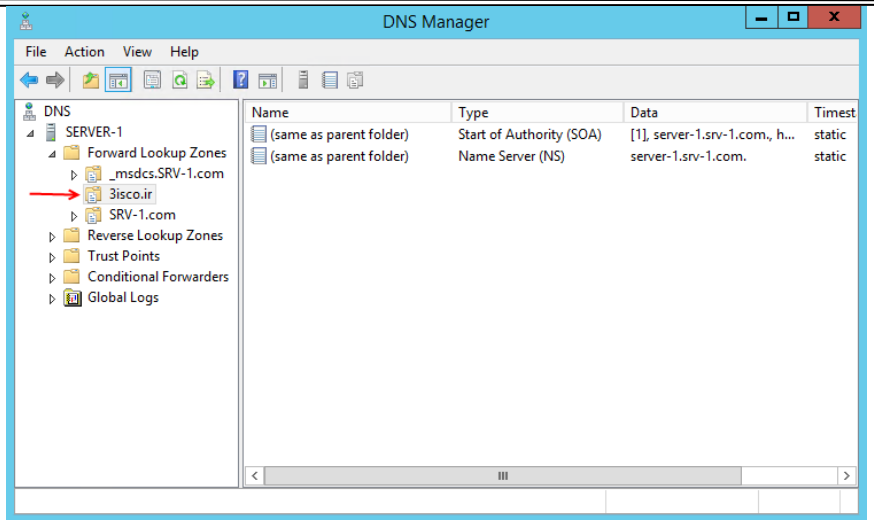
دستور Add-DnsServerPrimaryZone برای ایجاد یک Zone Primary اصلی می‌باشد. بعد از آن باید نحوه‌ی استفاده از این Zone را با استفاده از دستور ReplicationScope Domain مشخص کنید، این دستور یعنی اینکه این Zone که می‌خواهیم ایجاد کنیم یک Zone اصلی می‌باشد و زیرمجموعه یا Forest کسی دیگر نیست، بعد از این دستور باید نام Zone خود را با استفاده از دستور Name ExpertRoute.ir مشخص کنید که باید به جای ExpertRoute.ir نام موردنظر خود را وارد کنید و در قسمت آخر نحوه دریافت آپدیت را مشخص کند که به صورت امن باشد یا نه که در این قسمت DynamicUpdate Secure را وارد می‌کنیم. بعد ار وارد کردن دستور به مانند شکل ۸-۱۱۴۰، بر روی آیکون Run Script کلیک کنید.



شکل ۸- ۱۱۴۰ کار با DNS Server از طریق دستورات PowerShell

در شکل ۸-۱۱۴۱، Zone موردنظر ما با نام ExpertRoute.ir به درستی در سرویس DNS و در قسمت Forward Lookup ایجاد شده است.

www.takbook.com



شکل ۸- ۱۱۴۱ کار با DNS Server از طریق دستورات PowerShell

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

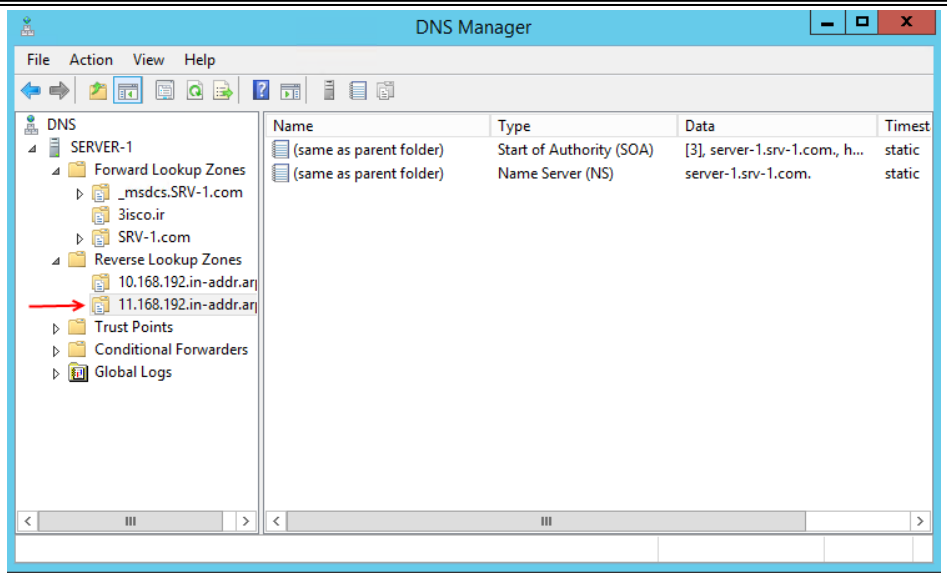
با استفاده از دستور زیر یک Reverse Lookup Zone برای آدرس 192.168.11 ایجاد می‌شود:

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

در دستورات بالا دستور Add-DnsServerPrimaryZone برای ایجاد یک Zone Primary یا اصلی می‌باشد، بعد باید آدرس شبکه موردنظر را وارد کنیم یعنی NetID آن را وارد کنیم که با استفاده از دستور NetworkId 192.168.11.0/24 تعریف می‌شود، توجه داشته باشید که به جای 192.168.11.0 آدرس موردنظر خود را وارد کنید و به جای 24/ باید مقدار موردنظر خود را وارد کنید 24/ یعنی 255.255.255.0 که این موضوعات در قسمت IPv4 به صورت کامل بررسی شده است، در دستور بعدی نوع دریافت آپدیت را مشخص می‌کنیم که به صورت امن می‌باشد DynamicUpdate Secure و بعد باید نوع دومین را مشخص کنیم که در اینجا دومین اصلی می‌باشد و باید از نام دومین به صورت ReplicationScope Domain استفاده کنیم.

بعد ازوارد کردن دستورات بالا آنها را اجرا کنید تا به صورت شکل ۸-۱۱۴۲، Zone موردنظر در قسمت Reverse Lookup Zone ایجاد شود.

www.takbook.com



شکل ۸- ۱۱۴۲ کار با DNS Server از طریق دستورات PowerShell

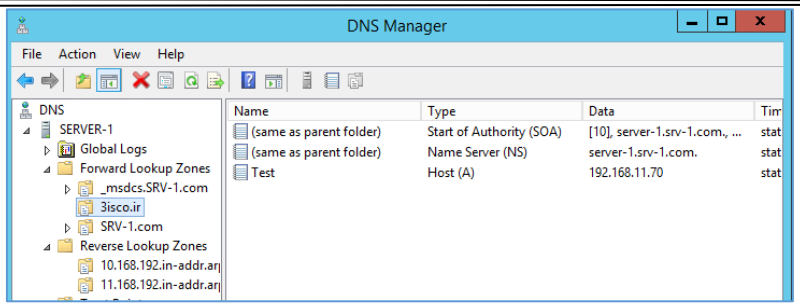
بعد از اینکه Reverse Lookup Zone را ایجاد کردیم باید در داخل ExpertRoute.ir یک Host A از طریق فرامین PowerShell ایجاد کنیم، برای این کار از دستورات زیر برای ایجاد Host A استفاده می‌کنیم:

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

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

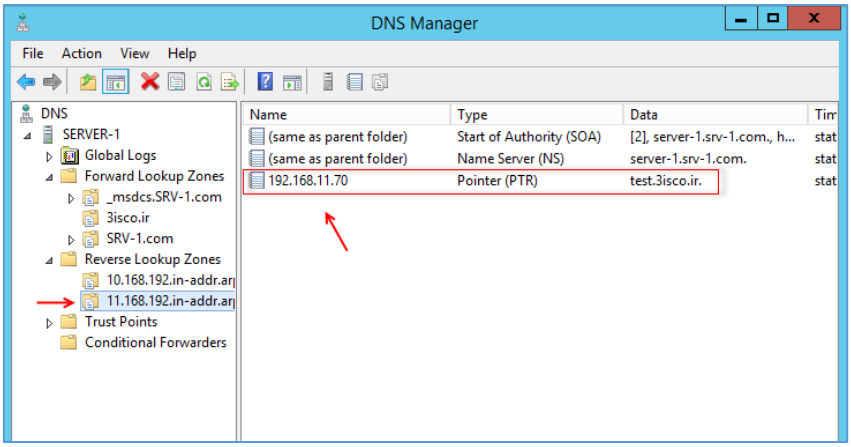
در شکل ۸-۱۱۴۳، بعد از دستور قبلی در ExpertRoute.ir یک Host A با نام Test ایجاد شده است،

www.takbook.com



شکل ۸- ۱۱۴۳ کار با *DNS Server* از طریق دستورات *PowerShell*

توجه داشته باشید، با اجرای دستور قبلی یک Record PTR هم در قسمت Reverse به صورت خودکار ایجاد شده است که شکل ۸-۱۱٤٤، نشان دهنده‌ی همین موضوع است.



شکل ۸- ۱۱۴۴ کار با *DNS Server* از طریق دستورات *PowerShell*

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

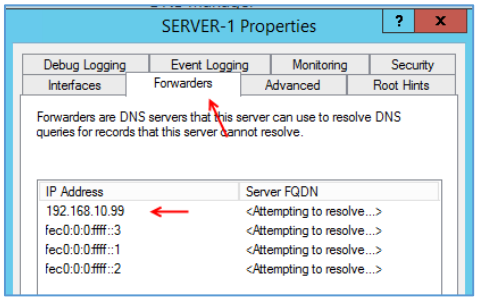
```
Add-DnsServerForwarder -IPAddress 192.168.10.99 -PassThru
```

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

بعد از اجرای دستور صفحه قبل اگر به مانند شکل ۸-۱۱٤٥، دوباره به قسمت Forwarders مراجعه کنیم متوجه می‌شویم که IP Address موردنظر به لیست اضافه شده است.

توجه داشته باشید اگر به مانند شکل ۸-۱۱٤٥، IP Address خود را در لیست مشاهده نمی‌کنید، سرویس DNS را ببندید و دوباره باز کنید.

www.takbook.com



شکل ۸- ۱۱۴۵ کار با *DNS Server* از طریق دستورات *PowerShell*

۶-۳۱-۳-۸ حذف کامپیوترهایی غیرفعال در شبکه

اگر وارد یک سازمان شوید و این سازمان بسیار بزرگ باشد باید توانایی زیادی برای حل مسائل پیچیده داشته باشید، مثلاً یک دومین دارید که دارای هزاران کامپیوتر است و برای اینکه بفهمید که کدام کامپیوتر در لیست فعال است یا خیر باید دستورات PowerShell را بلد باشید.

در این قسمت با استفاده از دستورات زیر می‌توانیم بفهمیم که چه سیستم‌هایی از ۹۰ روز قبل تا به حال با دومین مورد نظر ارتباط برقرار نکردند و بعد از شناسایی، آنها را غیرفعال و بعد از لیست حذف کنیم، برای این کار باید از کد زیر استفاده کنید.

```
Import-Module ActiveDirectory

# Set the number of days since last logon
$DaysInactive = 90
$InactiveDate = (Get-Date).Adddays(-($DaysInactive))

#--------------------------------
# FIND INACTIVE COMPUTERS
#--------------------------------
# Below are three options to find inactive computers. Select the one that is most appropriate for your requirements:

# Get AD Computers that haven't logged on in xx days
$Computers = Get-ADComputer -Filter { LastLogonDate -lt $InactiveDate -and Enabled -eq $true } -Properties LastLogonDate | Select-Object Name, LastLogonDate, DistinguishedName

# Get AD Computers that have never logged on
$Computers = Get-ADComputer -Filter { LastLogonDate -notlike "*" -and Enabled -eq $true } -Properties LastLogonDate | Select-Object Name, LastLogonDate, DistinguishedName

# Automated way (includes never logged on computers)
$Computers = Search-ADAccount -AccountInactive -DateTime $InactiveDate -ComputersOnly | Select-Object Name, LastLogonDate, Enabled, DistinguishedName
```

www.takbook.com


```
#------------------------------
# REPORTING
#------------------------------
# Export results to CSV
$Computers | Export-Csv C:\Temp\InactiveComputers.csv -NoTypeInformation


#------------------------------
# INACTIVE COMPUTER MANAGEMENT
#------------------------------
# Below are two options to manage the inactive computers that have been found. Either disable them, or
delete them. Select the option that is most appropriate for your requirements:

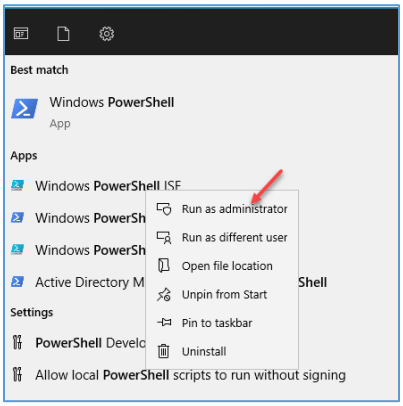

# Disable Inactive Computers
ForEach ($Item in $Computers){
  $DistName = $Item.DistinguishedName
  Set-ADComputer -Identity $DistName -Enabled $false
  Get-ADComputer -Filter { DistinguishedName -eq $DistName } | Select-Object Name, Enabled
}


# Delete Inactive Computers
ForEach ($Item in $Computers){
  Remove-ADComputer -Identity $Item.DistinguishedName -Confirm:$false
  Write-Output "$($Item.Name) - Deleted"
}
```

اگر کپی کردن کد برای شما در این قسمت سخت است می‌توانید از آدرس زیر آن را دانلود کنید:

https://expertroute.ir/code/Code-Delete-Account-computer.txt

بعد از دانلود وارد سرور Active Directory شوید و سرویس Powershell ISE را به مانند شکل ۸–۱۱۴۶، اجرا کنید.



شکل ۸- ۱۱۴۶ حذف کامپیوترهایی غیرفعال در شبکه

www.takbook.com

بعد از اجرا، کد قبلی را به مانند شکل ۸-۱۱۴۷، در آن کپی کنید، در کد زیر عدد ۹۰ را مشاهده می‌کنید که بدین معنا است سیستم‌هایی که از ۹۰ روز قبل تا به امروز با دومین ارتباط برقرار نکردن را انتخاب کند.

```
PS C:\Users\administrator> Import-Module ActiveDirectory

# Set the number of days since last logon
$DaysInactive = 90
$InactiveDate = (Get-Date).Adddays(-($DaysInactive))

#--------------------------------
# FIND INACTIVE COMPUTERS
#--------------------------------
# Below are three options to find inactive computers. Select the one that is most appropriate for your requirements:

# Get AD Computers that haven't logged on in xx days
$Computers = Get-ADComputer -Filter { LastLogonDate -lt $InactiveDate -and Enabled -eq $true } -Properties LastLogonDate | Select-Object Name, LastLogonDate, DistinguishedName

# Get AD Computers that have never logged on
$Computers = Get-ADComputer -Filter { LastLogonDate -notlike "*" -and Enabled -eq $true } -Properties LastLogonDate | Select-Object Name, LastLogonDate, DistinguishedName

# Automated way (includes never logged on computers)
$Computers = Search-ADAccount -AccountInactive -DateTime $InactiveDate -ComputersOnly | Select-Object Name, LastLogonDate, Enabled, DistinguishedName

#--------------------------------
# REPORTING
#--------------------------------
# Export results to CSV
$Computers | Export-Csv C:\Temp\InactiveComputers.csv -NoTypeInformation

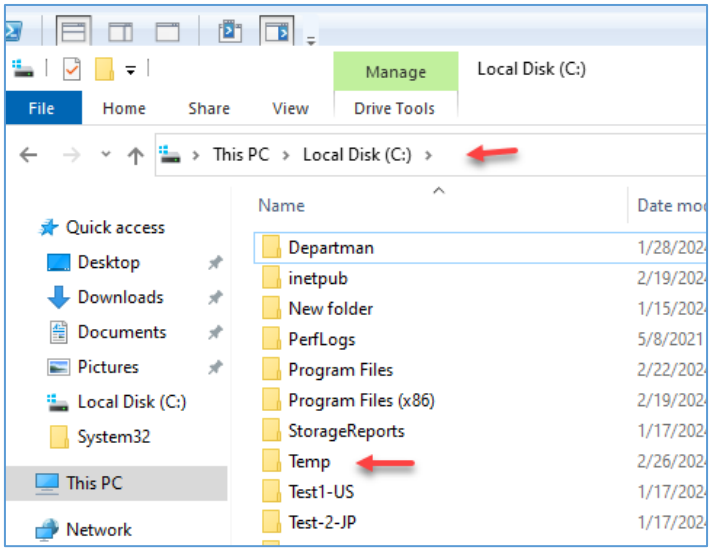
#--------------------------------
# INACTIVE COMPUTER MANAGEMENT
#--------------------------------
# Below are two options to manage the inactive computers that have been found. Either disable them, or delete them. Select the option that is most appropriate for your requirements:

# Disable Inactive Computers
ForEach ($Item in $Computers){
  $DistName = $Item.DistinguishedName
  Set-ADComputer -Identity $DistName -Enabled $false
  Get-ADComputer -Filter { DistinguishedName -eq $DistName } | Select-Object Name, Enabled
}

# Delete Inactive Computers
ForEach ($Item in $Computers){
  Remove-ADComputer -Identity $Item.DistinguishedName -Confirm:$false
  Write-Output "$($Item.Name) - Deleted"
}
```

شکل ۸- ۱۱۴۷ حذف کامپیوترهایی غیرفعال در شبکه

بعد از کپی فایل قبل از اینکه Enter را فشار دهید به مانند شکل ۸-۱۱۴۷، وارد درایو C شوید و یک فولدر با نام Temp ایجاد کنید.

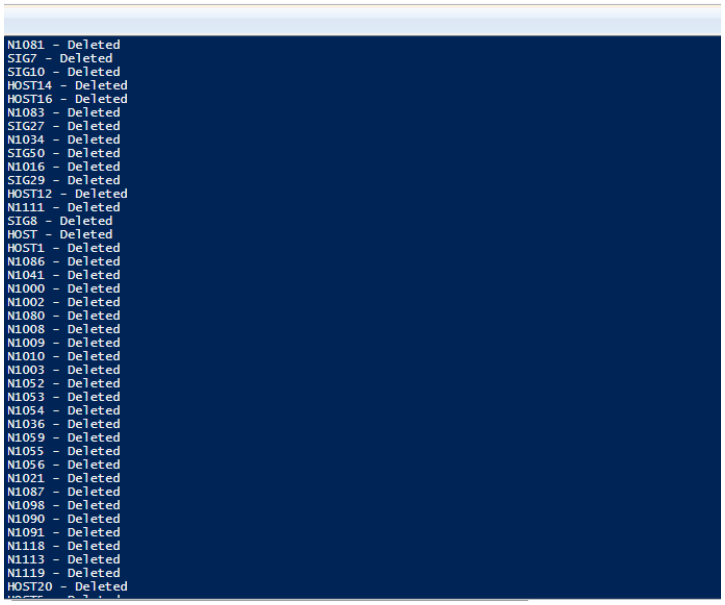


شکل ۸- ۱۱۴۸ حذف کامپیوترهایی غیرفعال در شبکه

بعد از ایجاد پوشه مورد نظر بر روی Enter فشار دهید تا کد مورد نظر اجرا شود، فقط به این نکته توجه کنید که بعد از اجرای کد، سیستم‌های شما از Active Directory حذف خواهند شد.

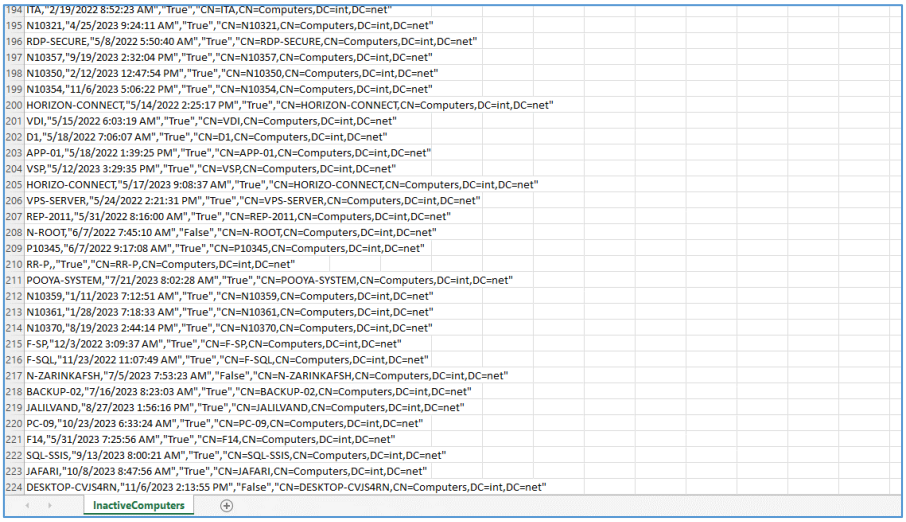
www.takbook.com

بعد از اجرای کد لیست سیستم های مورد نظر در آدرس مشخص شده در درایو C و در یک فایل اکسل کپی می‌شوند و در ادامه به مانند شکل ۸-۱۱۴۹، همه‌ی آنها حذف می‌شوند.



شکل ۸- ۱۱۴۹ حذف کامپیوترهایی غیرفعال در شبکه

اگر به فایل اکسل هم نگاهی بیندازیم متوجه خواهیم شد که ۲۲۳ کامپیوتر پیدا شده که بعد از آن حذف شده است که این موضوع را در شکل ۸-۱۱۵۰، مشاهده می‌کنید.



شکل ۸- ۱۱۵۰ حذف کامپیوترهایی غیرفعال در شبکه

www.takbook.com

۸-۳-۳۱-۷ اتوماتیک کردن کارها با PowerShell

اتوماتیک‌سازی وظایف شبکه با PowerShell به شما این امکان را می‌دهد که کارهای تکراری را ساده کنید و مدیریت شبکه را سریع‌تر و کارآمدتر انجام دهید. در زیر چند نمونه از سناریوهای اتوماتیک‌سازی با PowerShell آورده شده است:

در زیر چندین مثال را با هم بررسی می‌کنیم:

۸-۳-۳۱-۸ مدیریت تنظیمات IP

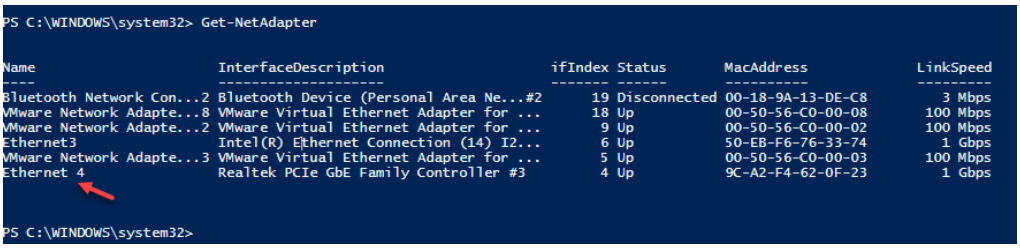
تغییر IP به حالت استاتیک

اگر بخواهید تنظیمات IP یک کارت شبکه را از DHCP به استاتیک تغییر دهید، فقط کافی است، در جاهایی که مشخص کردیم اطلاعات شبکه‌ی خود را وارد کنید و دستورات را اجرا کنید.

```
New-NetIPAddress -InterfaceAlias "Ethernet 4" -IPAddress
"192.168.4.102" -PrefixLength 23 -DefaultGateway "192.168.4.1"

Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses
"192.168.5.26", "8.8.4.4"
```

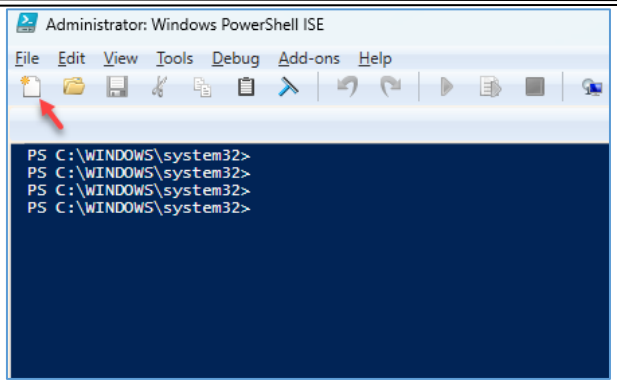
برای اینکه در دستور قبلی نام کارت شبکه خود را بدست بیاورید، باید از دستور `Get-NetAdapter` استفاده کنید که در شکل ۸-۱۱۵۱، لیست تمام کارت شبکه‌های موجود نمایش داده شده است که ما در این خروجی نیاز به تغییرات بر روی کارت شبکه با نام `Ethernet 4` داریم.



شکل ۸- ۱۱۵۱ اتوماتیک کردن کارها با PowerShell

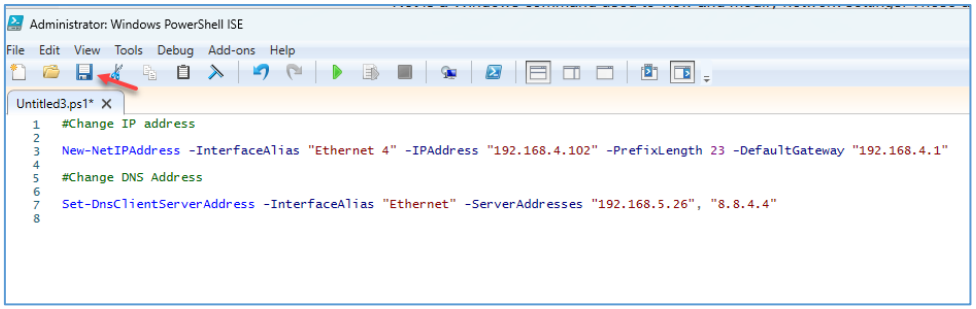
توجه داشته باشید شما می‌توانید این دستورات را در قالب یک فایل PS1 ایجاد و آن را با یک کلیک اجرا کنید، برای این کار کافی است PowerShell ISE را اجرا کنید و به مانند شکل ۸-۱۱۵۲، بر روی New کلیک کنید.

www.takbook.com



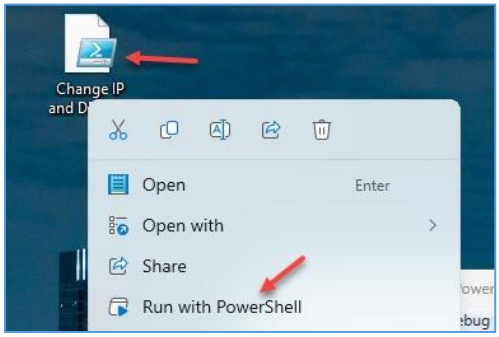
شکل ۸- ۱۱۵۲ اتوماتیک کردن کارها با PowerShell

در شکل ۸-۱۱۵۳، دستور مورد نظر خود را وارد کردیم و برای اینکه فایل مورد نظر را ذخیره کنیم باید بر روی آیکون Save کلیک کنید.



شکل ۸- ۱۱۵۳ اتوماتیک کردن کارها با PowerShell

بعد از ذخیره کردن فایل مورد نظر به مانند شکل ۸-۱۱۵٤، بر روی آن کلیک راست کنید و گزینه‌ی مورد نظر را انتخاب کنید و یا اینکه بر روی آن دو بار کلیک کنید تا اجرا شود.



شکل ۸- ۱۱۵۴ اتوماتیک کردن کارها با PowerShell

www.takbook.com

نکته مهم: در ورژن‌های جدید ویندوز یک سری محدودیت برای اجرای اسکریپت وجود دارد و باید این محدودیت را بردارید، برای این کار اول با دستور Get-ExecutionPolicy که خروجی آن در شکل ۸-۱۱۵۵، مشخص شده است بررسی می‌کنیم که بر روی کدام حالت قرار دارد.

خروجی می‌تواند یکی از موارد زیر باشد:

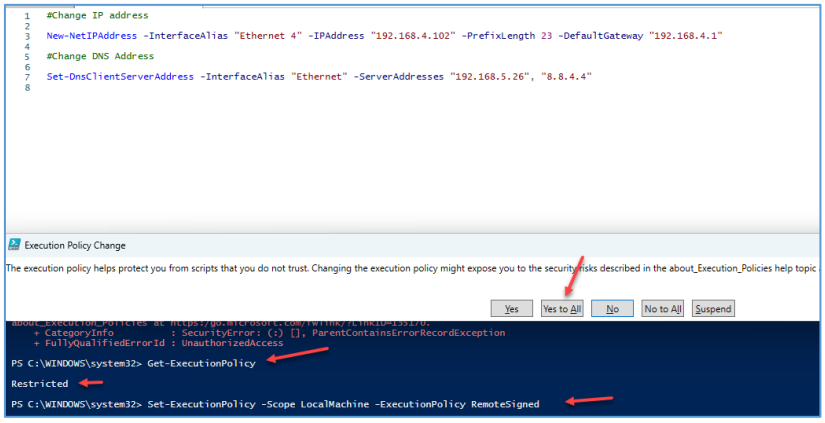
Restricted: اجرای هیچ اسکریپتی مجاز نیست.

RemoteSigned: اسکریپت‌های لوکال اجرا می‌شوند، اما اسکریپت‌های دانلود شده باید امضا داشته باشند.

Unrestricted: تمام اسکریپت‌ها اجرا می‌شوند.

Bypass: محدودیت اجرای اسکریپت غیرفعال است.

همان‌طور که در شکل ۸-۱۱۵۵،مشاهده می‌کنید بر روی حالت Restricted قرار دارد و هیچ اسکریپتی اجرا نمی‌شود که باید این محدودیت را برداریم.



شکل ۸- ۱۱۵۵ اتوماتیک کردن کارها با PowerShell

تغییر Execution Policy موقتاً (فقط برای جلسه فعلی)

برای تغییر سیاست فقط برای جلسه فعلی PowerShell:

```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned
```

این تنظیم پس از بستن PowerShell به حالت قبلی باز می‌گردد.

تغییر Execution Policy برای کاربر فعلی

برای تغییر دائمی سیاست اجرای اسکریپت برای کاربر جاری:

```
Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy RemoteSigned
```

تغییر Execution Policy برای کل سیستم

برای تغییر سیاست اجرای اسکریپت برای کل سیستم (نیاز به دسترسی Administrator):

```
Set-ExecutionPolicy -Scope LocalMachine -ExecutionPolicy RemoteSigned
```

www.takbook.com

اجرای اسکریپت بدون تغییر سیاست (Bypass)

اگر نمی‌خواهید سیاست را تغییر دهید و فقط یک اسکریپت خاص را اجرا کنید:

```
powershell -ExecutionPolicy Bypass -File
"C:\Users\babajani\Desktop\Change IP and DNS.ps1"
```

در ادامه دستوراتی که برای اتوماتیک‌سازی به کار می‌رود استفاده از دستوری است که اطلاعات کارت شبکه را بر روی حالت DHCP قرار دهد که برای این کار باید از دستور زیر استفاده کنید:

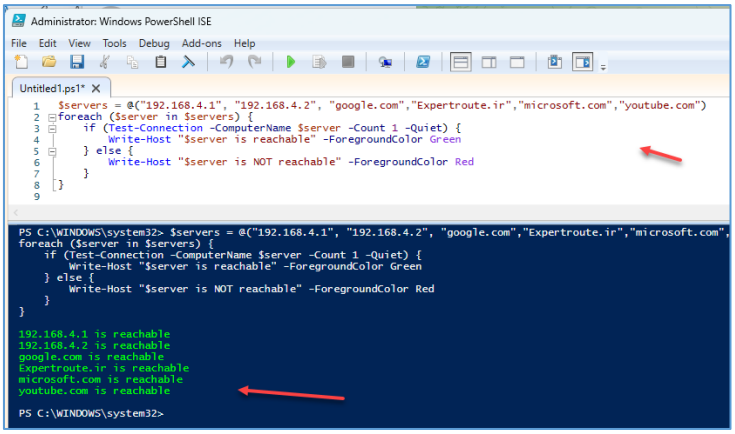
```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet 4" -
ResetServerAddresses
Set-NetIPInterface -InterfaceAlias "Ethernet 4" -Dhcp Enabled
```

۹-۳۱-۳-۸ Ping کردن هم‌زمان چند مقصد

برای اینکه بتوانیم چند مقصد را Ping کنیم می‌توانیم از کد اتوماتیک زیر استفاده کنیم، در این کد شما به جای آدرس‌های مشخص شده می‌توانید آدرس سرورهای داخلی و خارجی خود را وارد کنید، می‌توانید با این دستور آدرس IP تمام سرورهای خود را بدهید تا در صورت نیاز همه آنها را بررسی کند.

```
$servers = @("192.168.4.1", "192.168.4.2",
"google.com","Expertroute.ir","microsoft.com","youtube.com")
foreach ($server in $servers) {
    if (Test-Connection -ComputerName $server -Count 1 -Quiet) {
        Write-Host "$server is reachable" -ForegroundColor Green
    } else {
        Write-Host "$server is NOT reachable" -ForegroundColor Red
    }
}
```

همان‌طور که در خروجی شکل ۸-۱۱۵۶، مشاهده می‌کنید تمام آدرس‌ها بررسی شده و Ping آنها انجام شده است.



شکل ۸-۱۱۵۶ Ping کردن هم‌زمان چند مقصد

www.takbook.com

این مثال‌ها نمونه‌ای از اتوماتیک‌سازی در شبکه بوده که می‌توانید با یادگیری بیشتر نمونه‌های قویتری ایجاد کنید.

برای اینکه اکثر دستورات PowerShell را یاد بگیریم می‌توانید جدول ۸-۳ را بررسی کنید، در این جدول اکثر دستورات مهم بررسی شده و توضیح مناسب برای آن داده شده است.

توجه داشته باشید منظور از نام کوتاه (Alias) به این معنا است که مثلاً دستور Get-ChildItem دارای سه نام کوتاه شده‌ی dir, gci, ls است که به جای دستور اصلی می‌توانید استفاده کنید، و همچنین در قسمت نوع یا Type دستورات به دو قسمت Cmdlet که مخصوص خود PowerShell است و از قبل آماده شده است و دیگری Function که مربوط به توابعی است که کاربران می‌توانند از آنها استفاده و یا ایجاد کنند.

جدول ۸- ۳ بررسی دستورات Powershell

نام دستور	نام کوتاه	توضیحات	نوع
Get-ChildItem	dir, gci, ls	پرونده‌ها و پوشه‌ها را در یک درایو سیستم فایل بازیابی می‌کند.	Cmdlet
Invoke-Command	icm	دستورات را روی کامپیوترهای محلی و راه دور اجرا می‌کند.	Cmdlet
Import-Module	ipmo	ماژول‌ها را به جلسه جاری اضافه می‌کند.	Cmdlet
Export-Csv	epcsv	اشیاء را به یک سری از رشته‌های جدا شده با کاما (CSV) تبدیل می‌کند و این رشته‌ها را در یک فایل CSV ذخیره می‌کند.	Cmdlet
Write-Host		خروجی سفارشی را به میزبان (Host) می‌نویسد.	Cmdlet
Get-WmiObject	gwmi	نمونه‌هایی از کلاس‌های WMI یا اطلاعات مربوط به کلاس‌های موجود را بازیابی می‌کند.	Cmdlet
Get-Content	cat, gc, type	محتوای یک فایل را بازیابی می‌کند.	Cmdlet
Get-Date		تاریخ و زمان جاری را دریافت می‌کند.	Cmdlet
Invoke-WebRequest	curl, iwr, wget	محتوای یک صفحه وب از اینترنت را دریافت می‌کند.	Cmdlet
Start-Process	saps, start	یک یا چند فرآیند را روی کامپیوتر محلی شروع می‌کند.	Cmdlet
Copy-Item	copy, cp, cpi	یک مورد را از یک مکان به مکان دیگر کپی می‌کند.	Cmdlet
Set-ExecutionPolicy		ترجیحات کاربر برای سیاست اجرایی PowerShell را تغییر می‌دهد.	Cmdlet
Out-File		خروجی را به یک فایل ارسال می‌کند.	Cmdlet

www.takbook.com

Where-Object	?, where	اشیاء را از مجموعه‌ای بر اساس مقادیر ویژگی‌هایشان انتخاب می‌کند.	Cmdlet
Import-Csv	ipcsv	اشیاء سفارشی شبیه به جدول از داده‌های CSV می‌سازد.	Cmdlet
Send-MailMessage		یک پیام ایمیل ارسال می‌کند.	Cmdlet
New-Object		یک نمونه از یک شیء .NET یا COM ایجاد می‌کند.	Cmdlet
Select-String	sls	متن را در رشته‌ها و فایل‌ها پیدا می‌کند.	Cmdlet
Remove-Item	del, erase, rd, ri, rm, rmdir	فایل‌ها و پوشه‌ها را حذف می‌کند.	Cmdlet
Select-Object	select	اشیاء یا ویژگی‌های اشیاء را انتخاب می‌کند.	Cmdlet
Test-Path		بررسی می‌کند که آیا همه اجزای مسیر یک فایل یا دایرکتوری وجود دارند.	Cmdlet
Invoke-RestMethod	irm	درخواست HTTP یا HTTPS به یک وب‌سرویس RESTful ارسال می‌کند.	Cmdlet
Install-Package		یک یا چند بسته نرم‌افزاری را نصب می‌کند.	Cmdlet
ForEach-Object	%, foreach	عملیاتی را بر روی هر مورد در مجموعه‌ای از اشیاء ورودی انجام می‌دهد.	Cmdlet
Write-Output	echo, write	اشیاء مشخص‌شده را به دستور بعدی در PipeLine ارسال می‌کند.	Cmdlet
Get-Process	gps, ps	فرآیندهای در حال اجرا در کامپیوتر محلی یا راه دور را دریافت می‌کند.	Cmdlet
Get-Service	gsv	سرویس‌های موجود در کامپیوتر محلی یا راه دور را دریافت می‌کند.	Cmdlet
Format-Table	ft	خروجی را به صورت جدول فرمت می‌کند.	Cmdlet
Test-Connection		بسته‌های درخواست اکو ICMP ("پینگ") را به یک یا چند کامپیوتر ارسال می‌کند.	Cmdlet
New-Item	ni	یک مورد جدید ایجاد می‌کند.	Cmdlet
Get-EventLog		رویدادها را در یک لاگ رویداد یا فهرستی از لاگ‌های رویداد روی کامپیوترهای محلی یا راه دور دریافت می‌کند.	Cmdlet
Get-WinEvent		رویدادها را از لاگ‌های رویداد و فایل‌های لاگ ردیابی رویدادها در کامپیوترهای محلی و راه دور دریافت می‌کند.	Cmdlet

www.takbook.com

Install-Module		یک یا چند ماژول را از یک گالری آنلاین دانلود کرده و آن‌ها را روی کامپیوتر محلی نصب می‌کند.	Function
Enter-PSSession	etsn	یک جلسه تعاملی با یک کامپیوتر راه دور آغاز می‌کند.	Cmdlet
Get-Credential		یک شیء اعتبارسنجی بر اساس نام کاربری و رمز عبور دریافت می‌کند.	Cmdlet
Read-Host		یک خط ورودی از کنسول می‌خواند.	Cmdlet
Get-AppxPackage		فهرستی از بسته‌های نرم‌افزاری نصب‌شده در پروفایل کاربر را دریافت می‌کند.	Cmdlet
Get-Acl		توصیف امنیتی یک منبع (مانند فایل یا کلید رجیستری) را دریافت می‌کند.	Cmdlet
Get-Help		اطلاعاتی درباره دستورات و مفاهیم PowerShell نمایش می‌دهد.	Cmdlet
Start-Job	sajb	یک کار پس‌زمینه PowerShell را آغاز می‌کند.	Cmdlet
Add-PSSnapin		یک یا چند Snap-in PowerShell را به جلسه جاری اضافه می‌کند.	Cmdlet
New-PSSession	nsn	ارتباطی دائمی با یک کامپیوتر محلی یا راه دور برقرار می‌کند.	Cmdlet
Invoke-Expression	iex	دستورات یا عبارات را روی کامپیوتر محلی اجرا می‌کند.	Cmdlet
Add-Content	ac	محتوا، مانند کلمات یا داده‌ها، را به یک فایل اضافه می‌کند.	Cmdlet
New-PSDrive	mount, ndr	درایوهای شبکه موقت و دائمی را ایجاد می‌کند.	Cmdlet
Move-Item	mi, move, mv	یک مورد را از یک مکان به مکان دیگر منتقل می‌کند.	Cmdlet
Get-Item	gi	فایل‌ها و پوشه‌ها را دریافت می‌کند.	Cmdlet
Compare-Object	compare, diff	دو مجموعه از اشیاء را مقایسه می‌کند.	Cmdlet
Sort-Object	sort	اشیاء را بر اساس مقادیر ویژگی‌ها مرتب می‌کند.	Cmdlet
Test-NetConnection		اطلاعات تشخیصی برای یک ارتباط نمایش می‌دهد.	Function

www.takbook.com

Set-Acl		توصیف امنیتی یک مورد خاص، مانند فایل یا کلید رجیستری، را تغییر می‌دهد.	Cmdlet
Set-Content	sc	محتوای یک فایل را با محتوای مشخص‌شده جایگزین می‌کند.	Cmdlet
Start-Transcript		رکوردی از تمام یا بخشی از یک جلسه PowerShell را در یک فایل متنی ایجاد می‌کند.	Cmdlet
Get-HotFix		دریافت اصلاحات (Hotfix) اعمال‌شده به کامپیوترهای محلی و راه دور.	Cmdlet
Get-ItemProperty	gp	دریافت ویژگی‌های یک مورد مشخص.	Cmdlet
Add-Member		افزودن ویژگی‌ها و متدهای سفارشی به یک شیء PowerShell.	Cmdlet
Remove-AppxPackage		حذف یک بسته اپلیکیشن از حساب کاربری.	Cmdlet
Rename-Item	ren, rni	تغییر نام یک مورد در فضای نام ارائه‌دهنده PowerShell.	Cmdlet
Add-Type		افزودن نوع .NET Framework به جلسه PowerShell.	Cmdlet
Get-Member	gm	دریافت ویژگی‌ها و متدهای اشیاء.	Cmdlet
ConvertTo-SecureString		تبدیل رشته‌های رمزگذاری‌شده به رشته‌های امن.	Cmdlet
New-SelfSignedCertificate		ایجاد یک گواهی خودامضا برای اهداف تست.	Cmdlet
Start-Sleep	sleep	به تعویق انداختن فعالیت در یک اسکریپت یا جلسه برای مدت مشخص.	Cmdlet
Restart-Computer		سیستم عامل را در کامپیوترهای محلی و راه دور راه‌اندازی مجدد می‌کند.	Cmdlet
Out-GridView	ogv	خروجی را به صورت یک جدول تعاملی در یک پنجره جداگانه نمایش می‌دهد.	Cmdlet
Format-List	fl	خروجی را به صورت فهرستی از ویژگی‌ها قالب‌بندی می‌کند که هر ویژگی در خط جدیدی نمایش داده می‌شود.	Cmdlet
Set-ItemProperty	sp	مقدار یک ویژگی از یک مورد را ایجاد یا تغییر می‌دهد.	Cmdlet

www.takbook.com

Measure-Object	measure	ویژگی‌های عددی اشیاء و کاراکترها، کلمات و خطوط در اشیاء رشته‌ای (مانند فایل‌های متنی) را محاسبه می‌کند.	Cmdlet
Split-Path		بخشی از یک مسیر را باز می‌گرداند.	Cmdlet
Get-Counter		داده‌های شمارنده عملکرد را از کامپیوترهای محلی و راه دور دریافت می‌کند.	Cmdlet
Get-CimInstance		نمونه‌های CIM یک کلاس را از یک سرور CIM دریافت می‌کند.	Cmdlet
Add-Computer		کامپیوتر محلی را به یک دامنه یا گروه کاری اضافه می‌کند.	Cmdlet
Add-AppxPackage		یک بسته اپلیکیشن امضا شده را به حساب کاربری اضافه می‌کند.	Cmdlet
ConvertTo-Html		اشیاء .NET Framework را به HTML تبدیل می‌کند که می‌تواند در مرورگر وب نمایش داده شود.	Cmdlet
Import-StartLayout		طرح‌بندی استارت را به یک تصویر ویندوز متصل وارد می‌کند.	Cmdlet
Set-Location	cd, chdir, sl	موقعیت کاری جاری را به یک مکان مشخص تنظیم می‌کند.	Cmdlet
Get-NetAdapter		ویژگی‌های پایه‌ای آداپتور شبکه را دریافت می‌کند.	Function
Export-StartLayout		طرح‌بندی صفحه شروع را صادر می‌کند.	Cmdlet
Enable-PSRemoting		کامپیوتر را برای دریافت دستورات از راه دور پیکربندی می‌کند.	Cmdlet
Get-Command	gcm	تمام دستورات را دریافت می‌کند.	Cmdlet
Get-ExecutionPolicy		سیاست‌های اجرایی برای جلسه جاری را دریافت می‌کند.	Cmdlet
Join-Path		یک مسیر و یک مسیر فرعی را به یک مسیر واحد ترکیب می‌کند.	Cmdlet
Import-PSSession	ipsn	دستورات را از یک جلسه دیگر به جلسه جاری وارد می‌کند.	Cmdlet
Get-FileHash		مقدار هش یک فایل را با استفاده از الگوریتم هش مشخص محاسبه می‌کند.	Function
Write-Error		یک شیء را به جریان خطا می‌نویسد.	Cmdlet

www.takbook.com

Stop-Service	spsv	یک یا چند سرویس در حال اجرا را متوقف می‌کند.	Cmdlet
Stop-Process	kill, spps	یک یا چند فرآیند در حال اجرا را متوقف می‌کند.	Cmdlet
Start-Service	sasv	یک یا چند سرویس متوقف‌شده را شروع می‌کند.	Cmdlet
Unblock-File		فایل‌هایی که از اینترنت دانلود شده‌اند را باز می‌کند.	Cmdlet
Get-Disk		یک یا چند دیسک قابل مشاهده برای سیستم عامل را دریافت می‌کند.	Function
Get-Module	gmo	ماژول‌هایی که وارد شده‌اند یا می‌توانند وارد شوند را دریافت می‌کند.	Cmdlet
ConvertTo-Json		یک شیء را به رشته‌ای با فرمت JSON تبدیل می‌کند.	Cmdlet
New-WebServiceProxy		یک شیء نمایندگی وب‌سرویس ایجاد می‌کند که به شما امکان می‌دهد وب‌سرویس را در PowerShell مدیریت کنید.	Cmdlet
Reset-ComputerMachinePassword		رمز عبور حساب ماشین کامپیوتر را بازنشانی می‌کند.	Cmdlet
Get-ScheduledTask		شیء تعریف وظیفه یک وظیفه زمان‌بندی‌شده را از کامپیوتر محلی دریافت می‌کند.	Function
Write-EventLog		یک رویداد را به یک لاگ رویداد می‌نویسد.	Cmdlet
Set-Service		سرویس را شروع، متوقف و تعلیق می‌کند و ویژگی‌های آن را تغییر می‌دهد.	Cmdlet
Out-String		اشیاء را به میزبان به صورت رشته‌هایی ارسال می‌کند.	Cmdlet

دستورات زیاد دیگری هم وجود دارد که به خاطر محدودیت کتاب نتوانستیم همه آنها را بررسی کنیم.

۸-۳-۳۲ بررسی Server Core

Windows Server Core یک نصب سبک و حداقل‌شده از ویندوز سرور است که به‌طور ویژه برای کاهش اندازه نصب، افزایش امنیت، و کاهش پیچیدگی‌ها طراحی شده است. در این نوع نصب، بسیاری از اجزای گرافیکی ویندوز (مثل محیط دسکتاپ، Explorer و غیره) حذف می‌شوند و تنها امکانات ضروری برای اجرای سرور باقی می‌ماند. این نوع نصب به‌ویژه برای سناریوهای خاص مانند سرورهای وب، DNS،

www.takbook.com

DHCP، Active Directory، Hyper-V و دیگر سرویس‌های مشابه مفید است که نیازی به رابط گرافیکی ندارند.

ویژگی‌های Server Core

- حجم کمتر و عملکرد بهینه

نصب Server Core کمتر از ۵ گیگابایت به فضای دیسک نیاز دارد و به دلیل این که از بسیاری از سرویس‌ها و برنامه‌های اضافی ویندوز استفاده نمی‌کند، منابع کمتری را مصرف می‌کند، این کاهش منابع باعث عملکرد بهتر و کارایی بالاتر در محیط‌های سرور می‌شود.

- امنیت بالاتر

چون بسیاری از سرویس‌ها و ویژگی‌های گرافیکی غیرفعال هستند، حملات به سیستم سطحی‌تر و دشوارتر می‌شود، نیاز کمتری به مدیریت و پچ‌کردن نرم‌افزارهای اضافی وجود دارد.

- نیاز به مدیریت از راه دور

چون رابط کاربری گرافیکی (GUI) در Server Core وجود ندارد، مدیریت سیستم باید از طریق خط فرمان (Command Line) و ابزارهای مدیریت از راه دور مانند PowerShell, Windows Admin Center, Remote Server Administration Tools (RSAT) یا سرویس‌های مدیریت دیگری انجام شود.

- پشتیبانی از ویژگی‌های ضروری سرور

در Server Core، بسیاری از سرویس‌های مهم ویندوز سرور همچنان پشتیبانی می‌شوند مانند:

  - Active Directory Domain Services (AD DS)
  - DHCP
  - DNS
  - Hyper-V
  - File Server
  - Print Services
  - IIS (Internet Information Services)
  - Windows Defender

- پشتیبانی از نصب‌های قابل تبدیل:

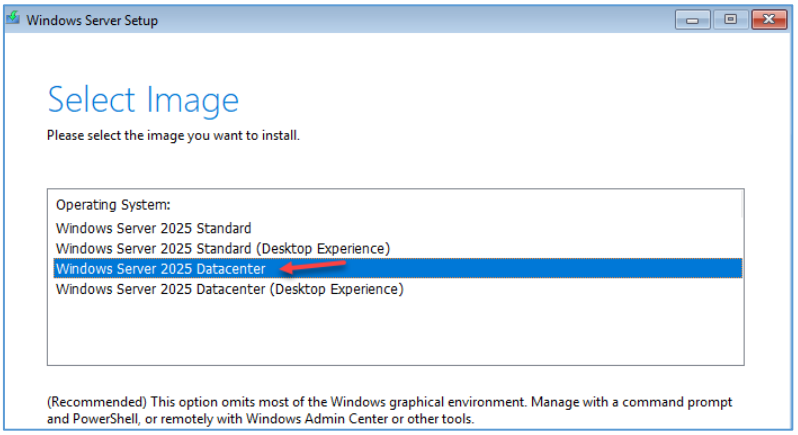
در صورتی که نیاز به رابط کاربری گرافیکی (GUI) برای مدیریت سیستم داشته باشید، می‌توانید Windows Server Core را به Server with Desktop Experience تبدیل کنید. این کار به راحتی از طریق PowerShell قابل انجام است.

- پشتیبانی از PowerShell

مدیریت اصلی و نصب ویژگی‌ها و نقش‌های سرور در Server Core عمدتاً با استفاده از PowerShell انجام می‌شود. این ابزار خط فرمان به‌ویژه برای اتوماسیون، پیکربندی و نظارت بر سرورها مفید است.

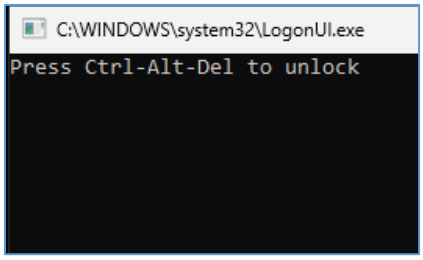
www.takbook.com

برای نصب این ویندوز فقط کافی است در زمان نصب گزینه‌ی عادی را انتخاب کنید یعنی گزینه‌ی که Desktop Experience نداشته باشد که در شکل ۸–۱۱۵۷، مشخص شده است، توجه داشته باشید برای اینکه نسخه‌ی آخر ویندوز سرور را داشته باشیم از نسخه‌ی ۲۰۲۵ استفاده کردیم.



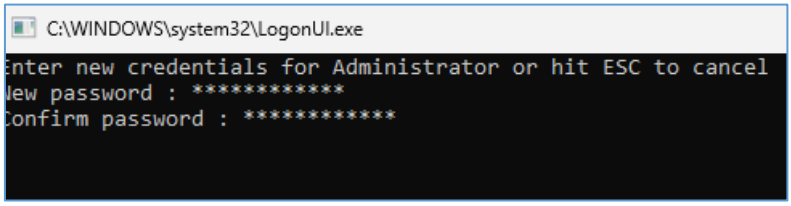
شکل ۸- ۱۱۵۷ نصب و راه‌اندازی *Server Core*

بعد از نصب، صفحه‌ی که به شما نمایش داده می‌شود به صورت شکل ۸–۱۱۵۸، خواهد بود که باید دکمه ترکیبی CTRL + ALT + DEL را فشار دهید.



شکل ۸- ۱۱۵۸ نصب و راه‌اندازی *Server Core*

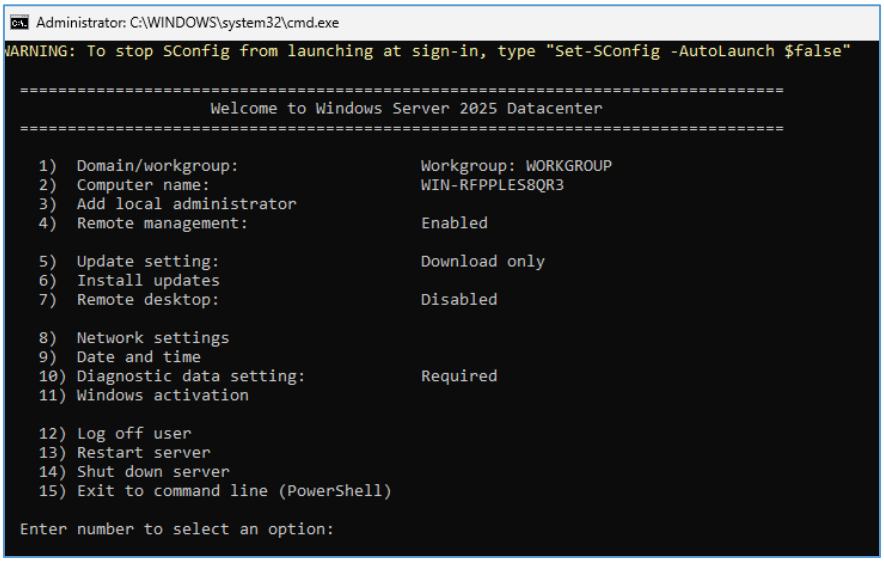
در ادامه باید به مانند شکل ۸–۱۱۵۹، بر روی OK کلیک کنید و رمز عبور جدید را برای کاربر Administrator مشخص کنید.



شکل ۸- ۱۱۵۹ نصب و راه‌اندازی *Server Core*

www.takbook.com

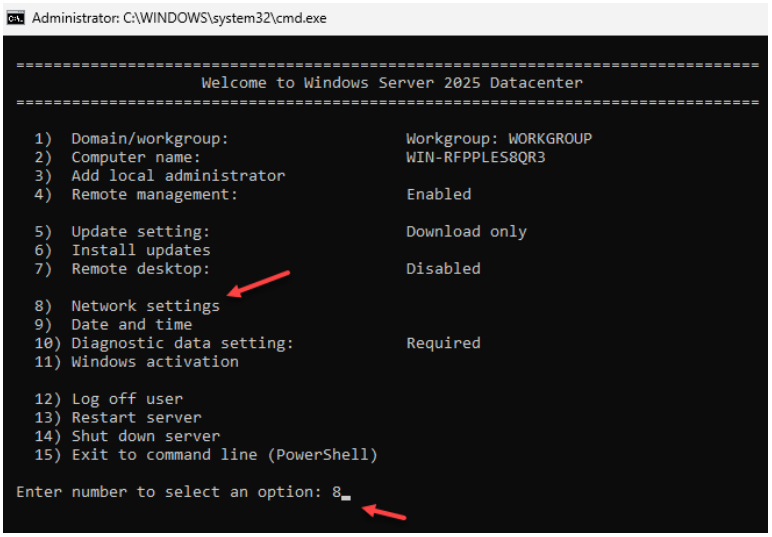
در صفحه‌ی بعد عدد یک را وارد و Enter کنید تا به صفحه‌ی اصلی و مدیریتی شکل ۸-۱۱۶۰، برسیم در این صفحه اطلاعات کلی از سیستم خود را مشاهده می‌کنید که در ادامه تنظیمات مورد نیاز خود را بر روی آن انجام می‌دهیم.



شکل ۸- ۱۱۶۰ نصب و راه‌اندازی *Server Core*

۸-۳-۳۲-۱ بررسی IP Address و عضو کردن در دومین

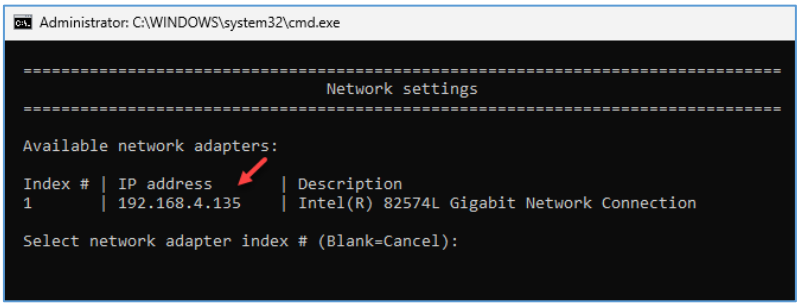
برای شروع کار اگر سرور شما به شبکه سازمان که دارای سرویس DHCP است متصل باشد باید آدرس جدید دریافت کرده باشد که در صفحه اصلی باید عدد 8 را به مانند شکل ۸-۱۱۶۱، وارد و Enter کنید.



شکل ۸- ۱۱۶۱ بررسی IP Address و عضو کردن در دومین

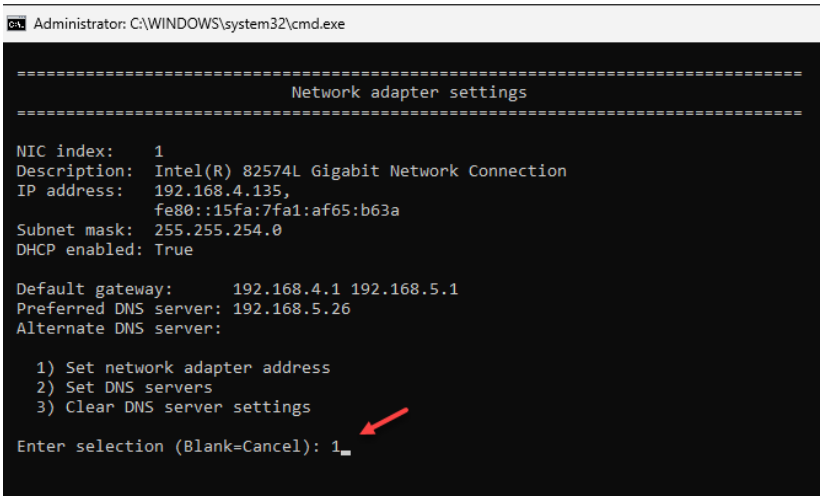
www.takbook.com

همان‌طور که در شکل ۸–۱۱۶۲، مشاهده می‌کنید آدرس IP برای این سرور 192.168.4.135 است که به صورت DHCP دریافت شده است.



شکل ۸- ۱۱۶۲ بررسی IP Address و عضو کردن در دومین

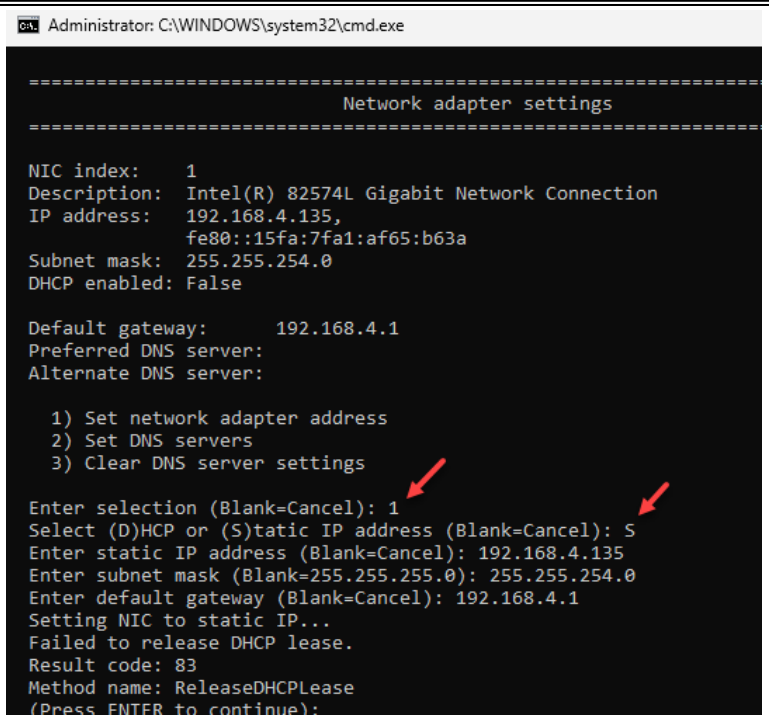
با وارد کردن عدد مربوط به کارت شبکه‌ای که آدرس دریافت کرده می‌توانید وارد جزئیات آن کارت شبکه شوید، در شکل ۸–۱۱۶۳، برای اینکه کارت شبکه را از حالت DHCP به Static تغییر دهید باید گزینه‌ی اول را انتخاب کنید.



شکل ۸- ۱۱۶۳ بررسی IP Address و عضو کردن در دومین

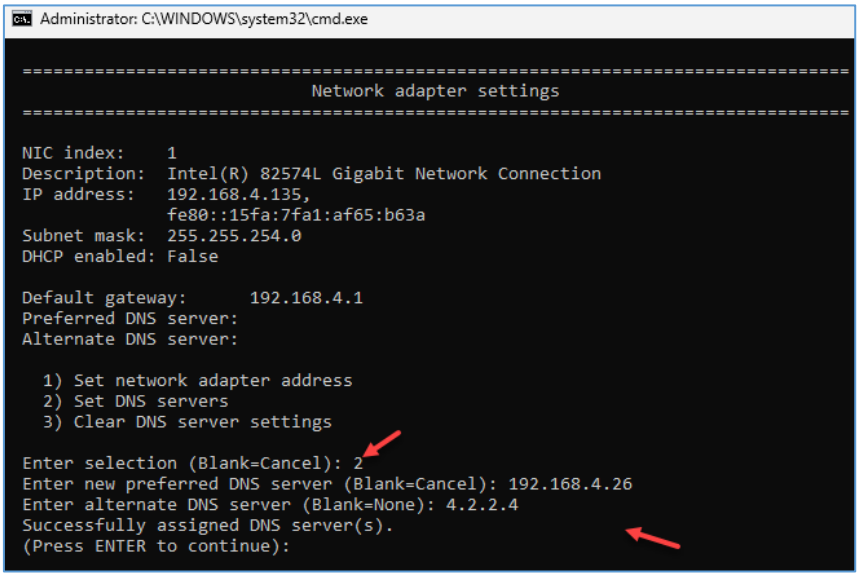
همان‌طور که در شکل ۸–۱۱۶۴، مشاهده می‌کنید بعد انتخاب کارت شبکه باید انتخاب کنید که کارت شبکه بر روی Static قرار بگیرد یا DHCP که با وارد کردن کلمه S آن را به حالت static تغییر می‌دهیم و بعد اطلاعات IP را وارد می‌کنیم.

www.takbook.com



شکل ۸- ۱۱۶۴ بررسی IP Address و عضو کردن در دومین

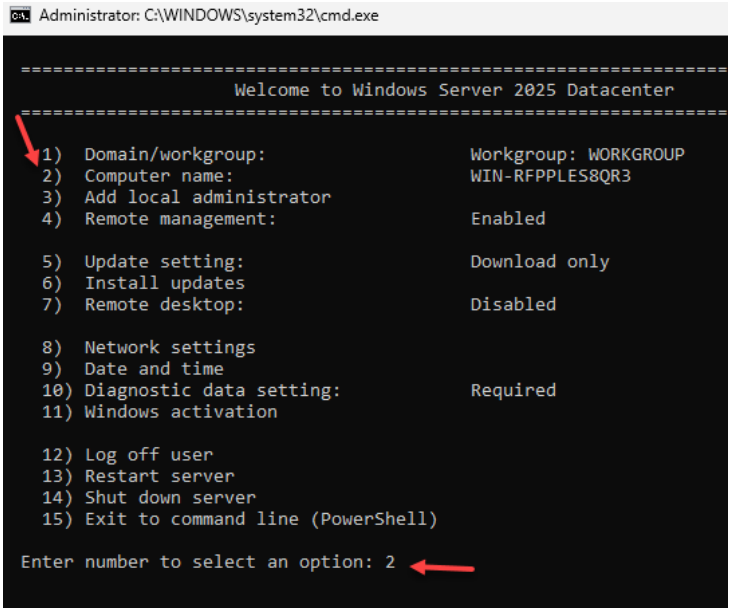
برای تغییر DNS هم باید گزینه‌ی دوم را به مانند شکل ۸-۱۱۶۵، انتخاب و اطلاعات را وارد کنید.



شکل ۸- ۱۱۶۵ بررسی IP Address و عضو کردن در دومین

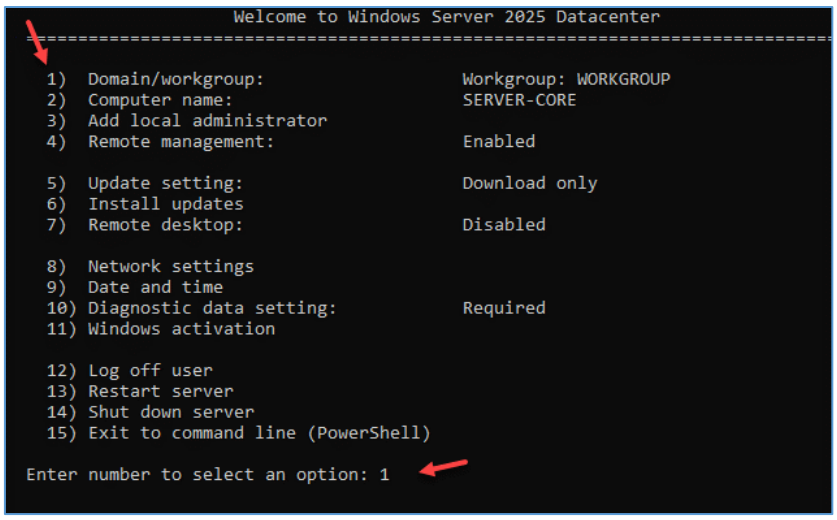
www.takbook.com

در ادامه کار می‌خواهیم نام سرور را تغییر دهیم و آن را عضو دومین کنیم، برای این کار به مانند شکل ۸-۱۱۶۶، گزینه‌ی دوم را انتخاب کنید، نام مورد نظر خود را وارد کنید و در ادامه کلمه Y را وارد تا سرور Restart شود و نام سرور تغییر کند.



شکل ۸- ۱۱۶۶ بررسی IP Address و عضو کردن در دومین

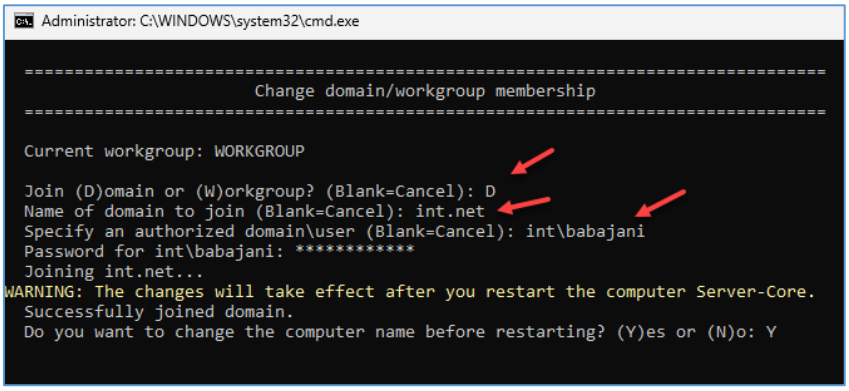
در ادامه کار باید سرور را عضو دومین کنیم، برای این کار عدد یک را به مانند شکل ۸-۱۱۶۷، وارد کنید.



شکل ۸- ۱۱۶۷ بررسی IP Address و عضو کردن در دومین

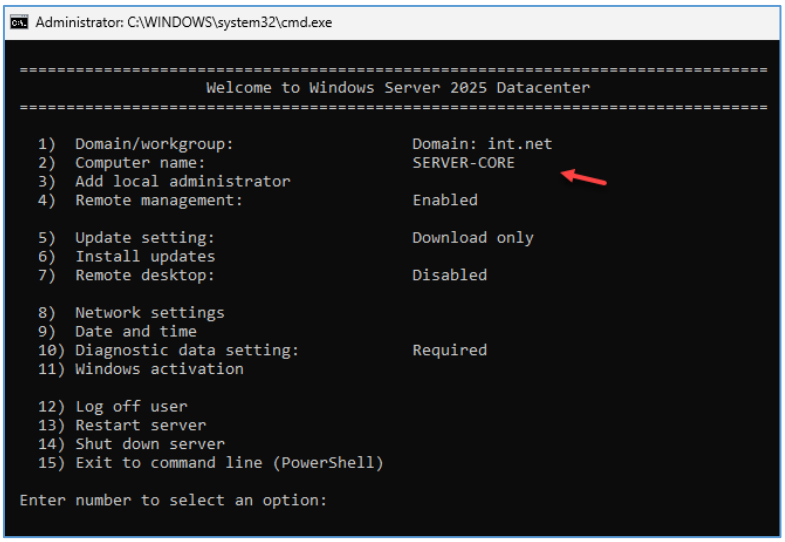
www.takbook.com

در شکل ۸-۱۱۶۸، باید کلمه‌ی D یعنی Join Domain را وارد کنید، و در ادامه باید نام دومین را وارد کنید و بعد از آن باید نام دومین را به همراه نام کاربری و رمز عبور وارد کنید و Enter کنید تا سرور عضو دومین شود.



شکل ۸- ۱۱۶۸ بررسی IP Address و عضو کردن در دومین

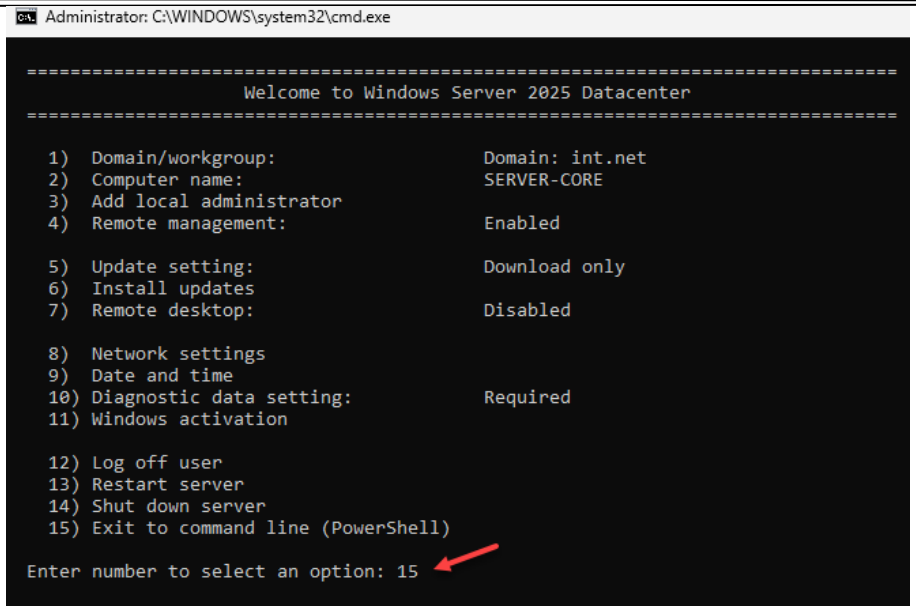
همان‌طور که در شکل ۸-۱۱۶۹، مشاهده می‌کنید سیستم مورد نظر عضو دومین شده است و نام آن هم تغییر کرده است.



شکل ۸- ۱۱۶۹ بررسی IP Address و عضو کردن در دومین

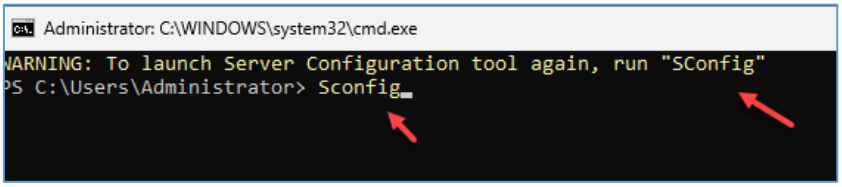
گزینه‌هایی دیگری مانند فعال‌سازی ویندوز، آپدیت و... وجود دارد که می‌توانید از آنها استفاده کنید، برای اینکه دستورات قدرتمند PowerShell را اجرا کنیم به مانند شکل ۸-۱۱۷۰، عدد 15 را وارد کنید تا از این حالت که به آن Sconfig می‌گویند خارج شویم و وارد خط فرمان PowerShell شویم.

www.takbook.com



شکل ۸- ۱۱۷۰ بررسی IP Address و عضو کردن در دومین

همان‌طور که در شکل ۸-۱۱۷۱، مشاهده می‌کنید وارد خط فرمان PowerShell شدیم و یک دستور در بالای صفحه به شما نمایش داده شده است که به این موضوع اشاره دارد که اگر از دستور Sconfig استفاده کنید دوباره به منوی اصلی برمی‌گردید.



شکل ۸- ۱۱۷۱ بررسی IP Address و عضو کردن در دومین

در ادامه کار شما می‌توانید از دستورات PowerShell برای مدیریت سرور خود استفاده کنید.

مثلاً برای نمایش IP Address باید از دستور Get-NetIPConfiguration استفاده کنید ک خروجی آن را در شکل ۸-۱۱۷۲، مشاهده می‌کنید.

www.takbook.com


```
PS C:\Users\Administrator> Get-NetIPConfiguration


InterfaceAlias       : Ethernet0
InterfaceIndex       : 6
InterfaceDescription : Intel(R) 82574L Gigabit Network Connection
NetProfile.Name      : int.net
IPv4Address          : 192.168.4.135
IPv6DefaultGateway   :
IPv4DefaultGateway   : 192.168.4.1
DNSServer            : 192.168.4.26
                       4.2.2.4
```

شکل ۸- ۱۱۷۲ بررسی IP Address و عضو کردن در دومین

بقیه دستورات را در قسمت قبلی بیان کردیم که می‌توانید برای مدیریت سرور Core استفاده کنید.

۸-۳-۳۳ نصب و راه‌اندازی NANO Server

Nano Server نسخه‌ای بسیار سبک و بهینه‌شده از Windows Server است که توسط مایکروسافت برای استفاده در محیط‌های مدرن، مانند پشتیبانی از کانتینرها و محیط‌های ابری طراحی شده است. این نسخه از ویندوز سرور به‌طور خاص برای کاهش مصرف منابع، افزایش امنیت و ساده‌سازی مدیریت سیستم‌ها در محیط‌هایی با نیاز به عملکرد بالا ایجاد شده است.

Nano Server در واقع یک نسخه حداقل‌شده از Windows Server است که تنها اجزای ضروری و پایه‌ای برای اجرای سرویس‌های خاص مانند Hyper-V, Web Server (IIS)، و DNS را در اختیار می‌گذارد.

در ابتدا، Nano Server محدود به نسخه‌های Windows Server 2016 بود، اما در نسخه‌های بعدی Windows Server 2019 و Windows Server 2025 نیز ادامه یافت. با این حال، در Windows Server 2025، مایکروسافت اعلام کرد که Nano Server به عنوان یک گزینه نصب مستقل حذف شده است و به‌جای آن، این فناوری بیشتر برای Containers (کانتینرها) و Hyper-V به‌کار گرفته می‌شود.

برای اینکه هر دو نسخه قدیم و جدید را بررسی کنیم اول نسخه‌ی ۲۰۱۶ را بررسی و راه‌اندازی می‌کنیم و بعد از آن نسخه‌ی جدید آن را بررسی خواهیم کرد.

۸-۳-۳۳-۱ نصب ورژن ۲۰۱۶

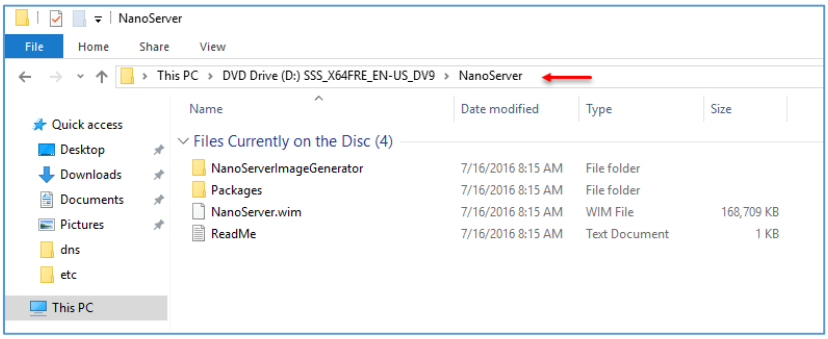
Nano Server، یک سیستم عامل بسیار کوچک و سریع از مایکروسافت است که برای ارائه‌ی سرویس‌های مختلف ایجاد شده است، این سرویس‌ها می‌تواند، سرویس IIS، DNS و... باشد که این سرویس را در زیر بررسی خواهیم کرد.

https://www.microsoft.com/en-us/download/details.aspx?id=54065

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

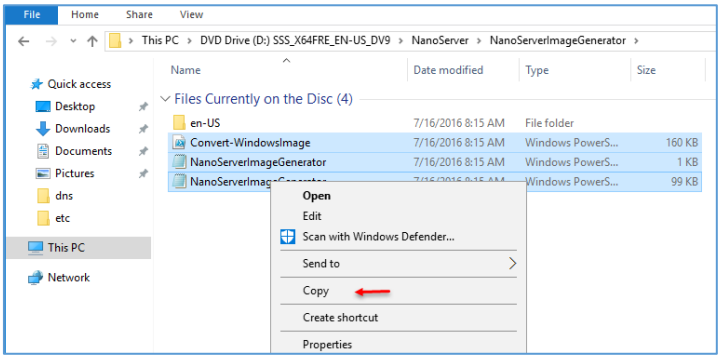
www.takbook.com

اگر وارد DVD مربوط به ویندوز سرور ۲۰۱۶ شوید، یک پوشه با عنوان NANO Server وجود دارد که اجزای آن، به مانند شکل ۸-۱۱۷۳، است.



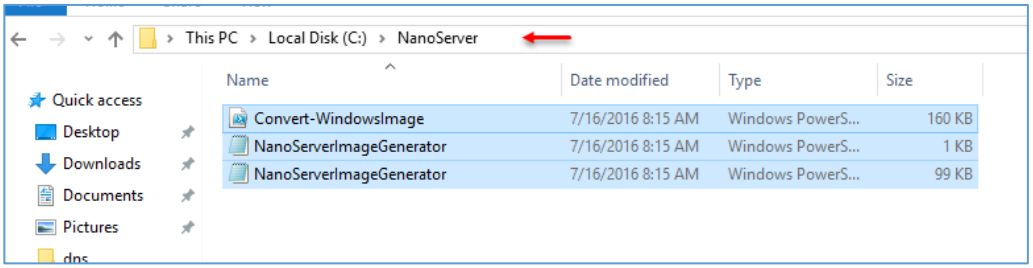
شکل ۸-۱۱۷۳ نصب و راه‌اندازی NANO Server

به مانند شکل ۸-۱۱۷۴، وارد پوشه‌ی NanoServerImageGenerator شوید و سه فایل انتخاب‌شده را Copy بگیرید و به دلخواه خود، یک پوشه در درایو C قرار دهید.



شکل ۸-۱۱۷۴ نصب و راه‌اندازی NANO Server

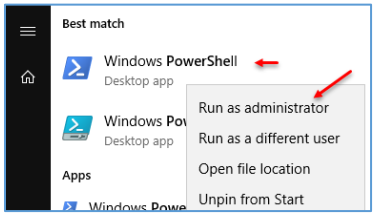
همان‌طور که در شکل ۸-۱۱۷۵، مشاهده می‌کنید، فایل‌های مورد نظر در درایو C و در پوشه‌ی NanoServer قرار گرفته‌اند.



شکل ۸-۱۱۷۵ نصب و راه‌اندازی NANO Server

www.takbook.com

به مانند شکل ۸-۱۱۷۶، وارد Start شوید و سرویس Powershell را با دسترسی کاربر Administrator، اجرا کنید.



شکل ۸- ۱۱۷۶ نصب و راه‌اندازی NANO Server

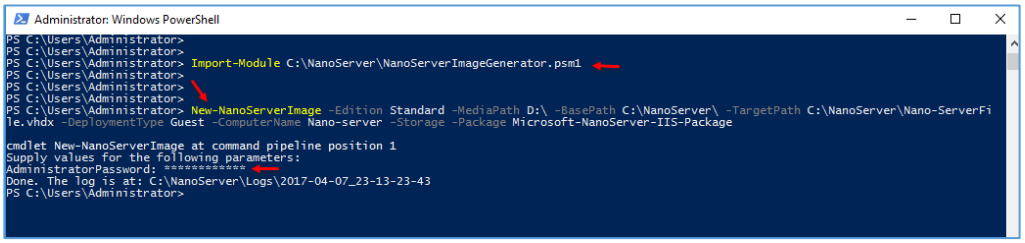
بعد از باز شدن سرویس PowerShell باید دستورات مورد نظر آن را وارد کنید که این کار را در زیر انجام دادیم:

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

با استفاده از دستور قبلی، 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
```

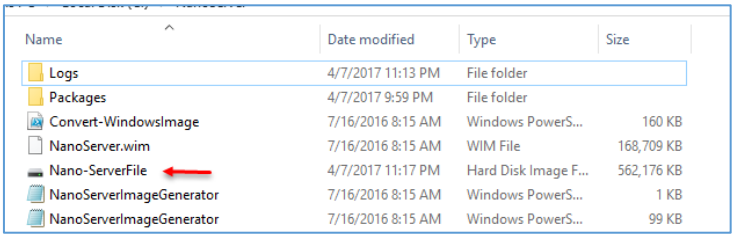
به مانند شکل ۸-۱۱۷۷، باید دستورات بالا را وارد کنید تا فایل مورد نظر خود را اجرا کنید، در دستور بالا به جای D:\ باید آدرس درایوی را وارد کنید که ویندوز سرور 2016 در آن قرار دارد، در قسمت BasePath، آبی رنگ باید آدرس محلّ فایل کپی‌شده که با هم انجام دادیم را وارد کنید و در قسمت TargetPath، سبز رنگ باید 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.



شکل ۸- ۱۱۷۷ نصب و راه‌اندازی NANO Server

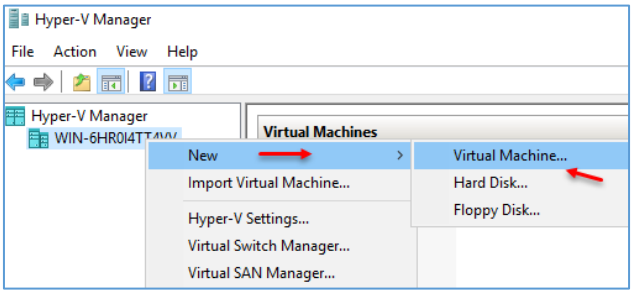
www.takbook.com

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 ۸–۱۱۷۸ ظاهر شود.



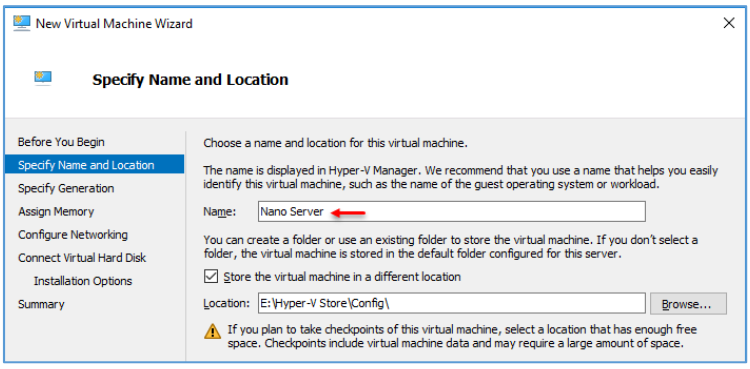
شکل ۸– ۱۱۷۸ نصب و راه‌اندازی NANO Server

بعد از ایجاد هارد دیسک مورد نظر در قسمت قبل، به مانند شکل ۸–۱۱۷۹، 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.



شکل ۸– ۱۱۷۹ نصب و راه‌اندازی NANO Server

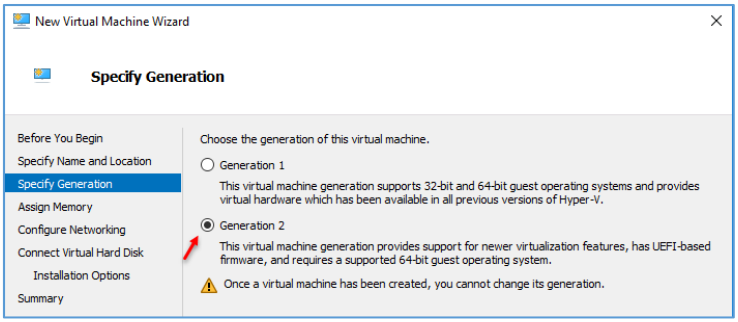
در شکل ۸–۱۱۸۰، نام سرور Nano را وارد کنید و محلّ ذخیره‌سازی این ماشین را مشخّص و بر روی Next کلیک کنید.



شکل ۸– ۱۱۸۰ نصب و راه‌اندازی NANO Server

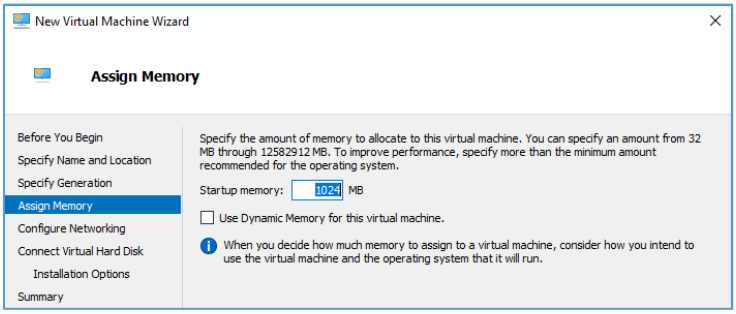
www.takbook.com

در شکل ۸-۱۱۸۱، گزینه‌ی مورد نظر را انتخاب و بر روی Next کلیک کنید.



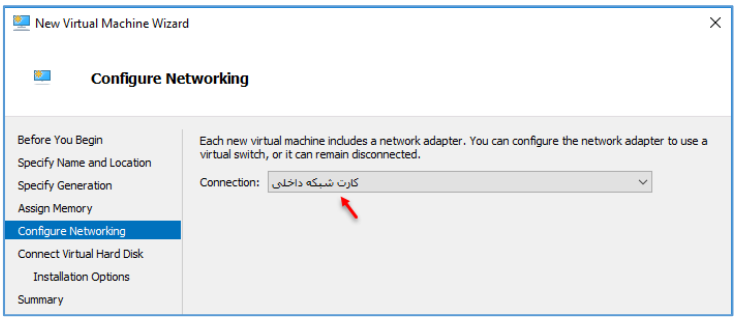
شکل ۸- ۱۱۸۱ نصب و راه‌اندازی NANO Server

در شکل ۸-۱۱۸۲، 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.



شکل ۸- ۱۱۸۲ نصب و راه‌اندازی NANO Server

در شکل ۸-۱۱۸۳، باید کارت شبکه‌ی مورد نظر خود را انتخاب کنید که فعلاً برای تست کار باید کارت شبکه‌ی داخلی را انتخاب کنید.

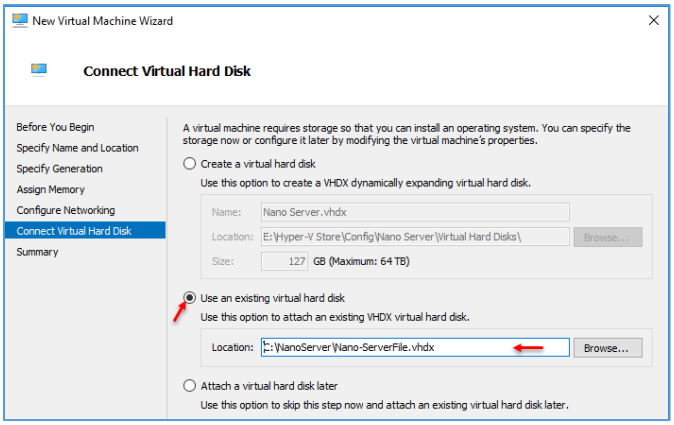


شکل ۸- ۱۱۸۳ نصب و راه‌اندازی NANO Server

در شکل ۸-۱۱۸٤، 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.

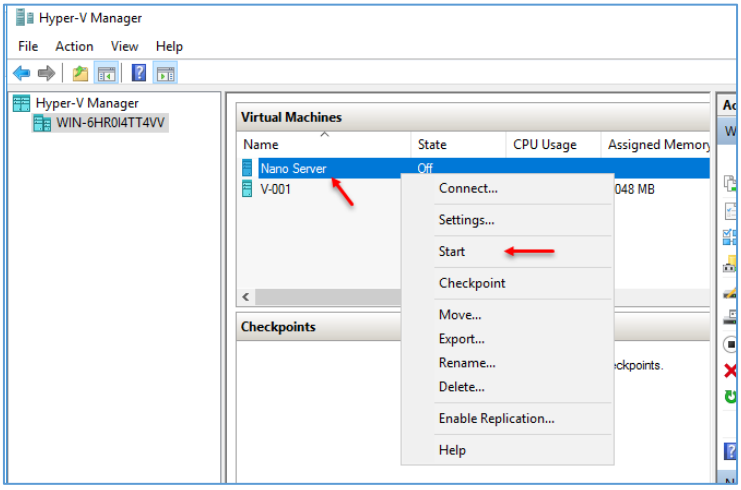
www.takbook.com

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



شکل ۸- ۱۱۸۴ نصب و راه‌اندازی NANO Server

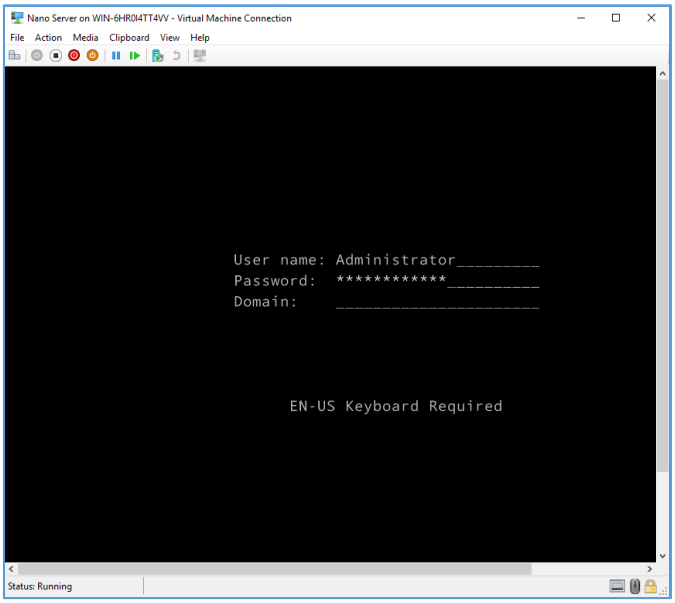
بعد از ایجاد ماشین مجازی، به مانند شکل ۸-۱۱۸۵، بر روی آن کلیک راست کنید و بعد بر روی Start کلیک کنید تا ماشین روشن شود.



شکل ۸- ۱۱۸۵ نصب و راه‌اندازی NANO Server

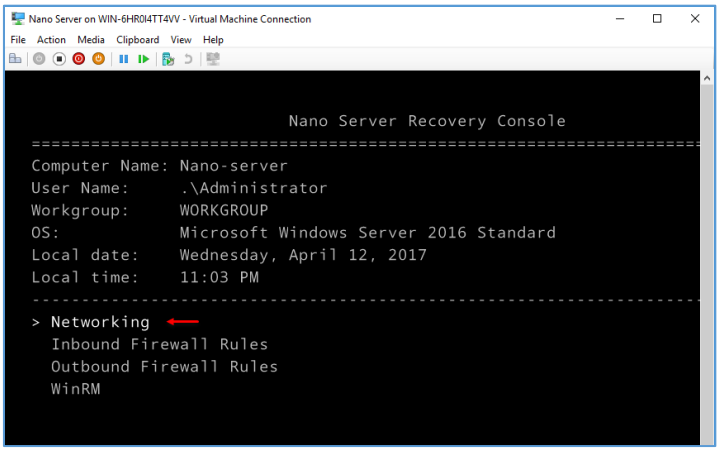
بعد از روشن شدن ماشین مجازی، شکل ۸-۱۱۸۶، ظاهر می‌شود که از شما نام کاربری، رمز عبور و نام دومین دریافت می‌شود که برای ورود باید نام کاربری Administrator را به همراه رمز عبوری که در هنگام نصب وارد کردید را دوباره در اینجا تکرار کنید و بر روی Enter فشار دهید.

www.takbook.com



شکل ۸- ۱۱۸۶ نصب و راه‌اندازی *NANO Server*

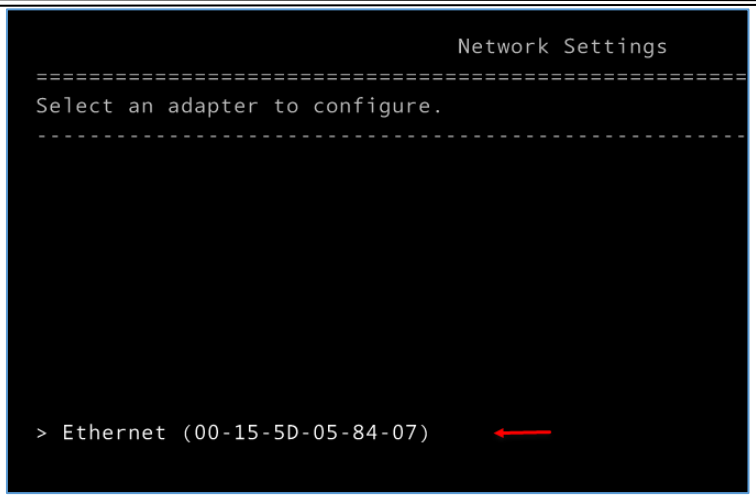
در شکل ۸-۱۱۸۷، اطّلاعاتی از سرور را مشاهده می‌کنید، مثلاً نوع سیستم عامل را ویندوز سرور 2016 استاندارد در نظر گرفته است و...، برای اینکه یک وب سرور از طریق Nano Server ایجاد کنید باید وارد قسمت Networking شوید و یک آدرس IP برای سرور تخصیص دهید.



شکل ۸- ۱۱۸۷ نصب و راه‌اندازی *NANO Server*

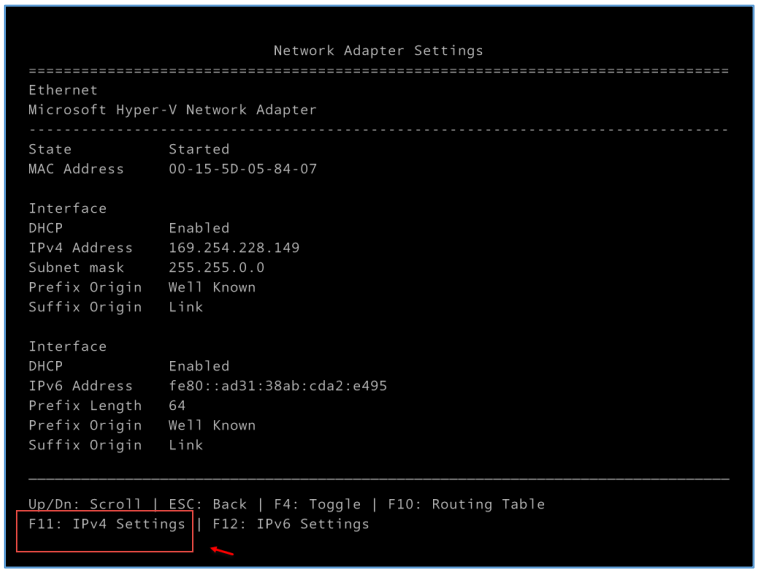
در شکل ۸-۱۱۸۸، تعداد کارت شبکه‌ی تخصیص‌داده شده به سرور مشخّص می‌شود که فعلاً یکی است، بر روی Enter فشار دهید تا وارد آن شوید و آدرس IP را وارد کنید.

www.takbook.com



شکل ۸- ۱۱۸۸ نصب و راه‌اندازی *NANO Server*

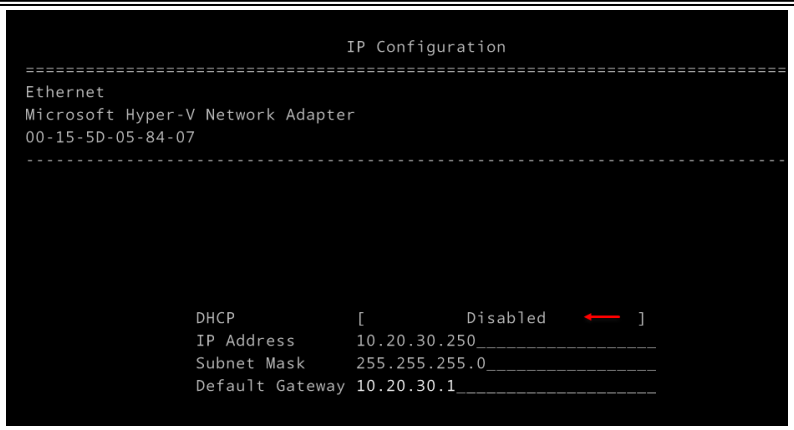
در شکل ۸-۱۱۸۹، اگر سرویس DHCP در شبکه‌ی شما فعّال باشد، سرور Nano به صورت اتوماتیک، آدرس IP دریافت می‌کند و اگر چنانچه بخواهید به صورت دستی آدرس وارد کنید باید به پایین صفحه مراجعه کنید که برای تنظیم آدرس IPv4 باید بر روی F11 کلیک کنید و برای IPv6 بر روی F12 کلیک کنید.



شکل ۸- ۱۱۸۹ نصب و راه‌اندازی *NANO Server*

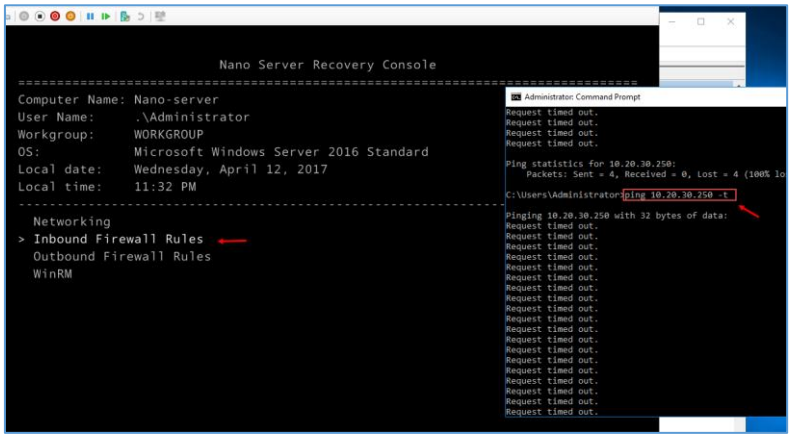
در شکل ۸-۱۱۹۰، اوّل باید با کلید بر روی F4، سرویس DHCP را غیرفعّال کنید تا از طریق سرویس DHCP، آدرس دریافت نکند، بعد از این کار با کلید بر روی TAB، آدرس IP سرور را به همراه Gateway و Subnet وارد کنید و بر روی Enter کلیک کنید تا اطّلاعات ذخیره شود.

www.takbook.com



شکل ۸- ۱۱۹۰ نصب و راه‌اندازی NANO Server

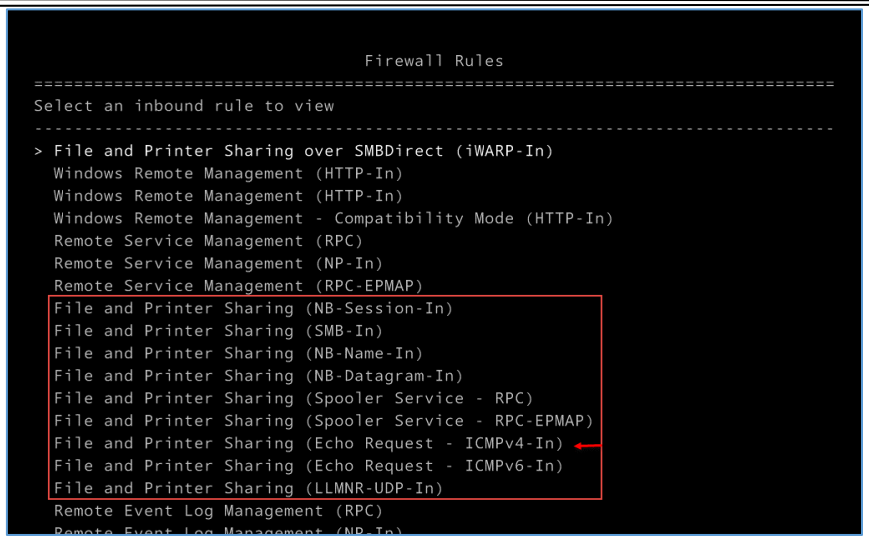
بعد از اینکه آدرس‌دهی کردید، می‌توانید با یک عملیّات Ping این موضوع را تست بگیرید، همان‌طور که در شکل ۸-۱۱۹۱، مشاهده می‌کنید از ویندوز اصلی، سرور Nano را Ping گرفتیم که با خطای Timed out روبرو شدیم، برای حلّ آن باید فایروال را دستکاری کنید، لذا ابتدا وارد Nano Server شوید و بعد از آن وارد قسمت Inpound Firewall Rules شوید.



شکل ۸- ۱۱۹۱ نصب و راه‌اندازی NANO Server

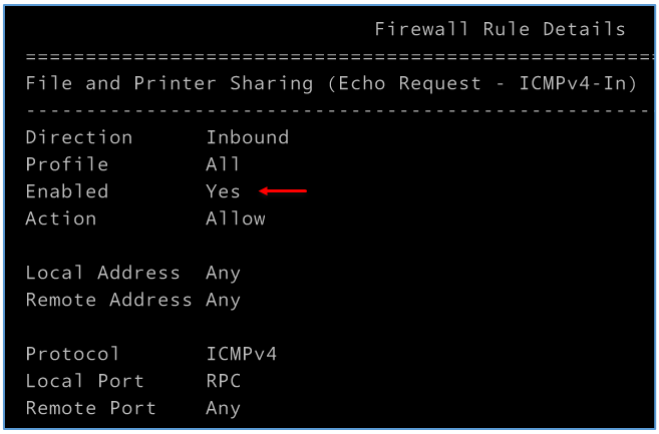
در شکل ۸-۱۱۹۲، گزینه‌های مختلفی را مشاهده می‌کنید، اگر تنها بخواهید عملیّات Ping را تکمیل کنید باید وارد گزینه‌ای که با فلش مشخّص شده است، شوید و بعد از آن، کلید F4 را فشار دهید تا فعّال شود و بعد، بر روی Esc کلید کنید، با این کار Ping فعّال خواهد شد، امّا اگر بخواهید دسترسی به کلّ سرور برای راه‌اندازی وب سرور داشته باشید باید وارد همه‌ی گزینه‌هایی که مشخّص شده است، شوید و با کلیک بر روی دکمه‌ی F4، آنها را فعّال کنید.

www.takbook.com



شکل ۸- ۱۱۹۲ نصب و راه‌اندازی *NANO Server*

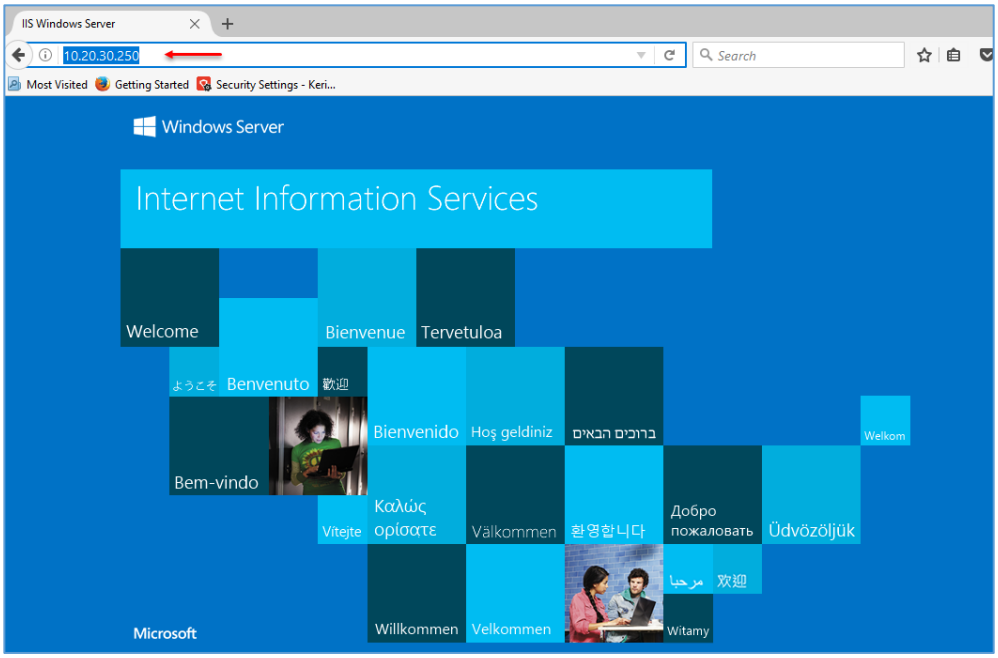
در شکل ۸-۱۱۹۳، یکی از این گزینه‌ها را مشاهده می‌کنید که با کلید بر روی F4، سرویس آن Enabled شده است.



شکل ۸- ۱۱۹۳ نصب و راه‌اندازی *NANO Server*

اگر به مانند شکل ۸-۱۱۹٤، آدرس سرور Nano را داخل مرورگر وارد کنید، سرویس IIS را مشاهده می‌کنید که فعّال شده و در دسترس است.

www.takbook.com

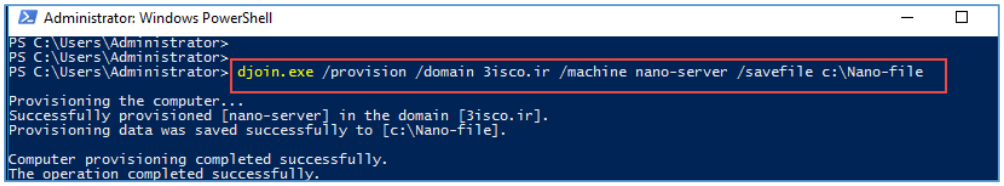


شکل ۸- ۱۱۹۴ نصب و راه‌اندازی NANO Server

عضو کردن Nano Server در 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.



شکل ۸- ۱۱۹۵ عضو کردن Nano Server در Domain

همان‌طور که در شکل ۸-۱۱۹۵، مشاهده می‌کنید، دستوری به شکل زیر وارد شده است:

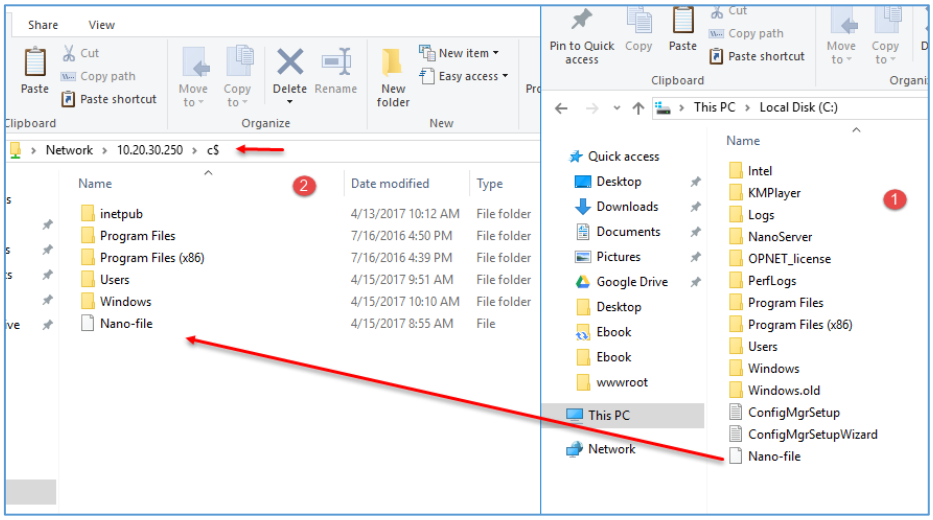
djoin.exe /provision /domain ExpertRoute.ir /machine nano-Server /savefile c: \Nano-file

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 ۸-۱۱۹۶، 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

www.takbook.com

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.



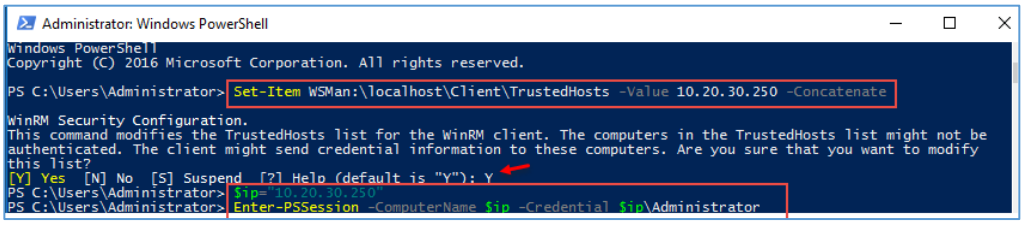
شکل ۸- ۱۱۹۶ عضو کردن Nano Server در Domain

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 که شکل ۸-۱۱۹۷ نشان دهنده این موضوع است.

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



شکل ۸- ۱۱۹۷ عضو کردن Nano Server در Domain

www.takbook.com

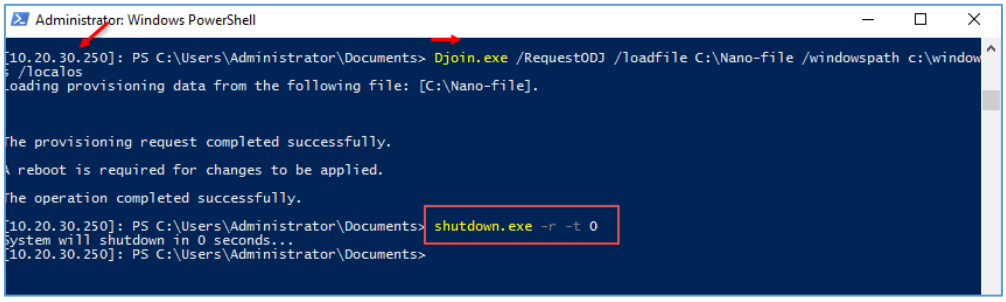
در دستورات قبلی و خط اوّل، یک متغیّر با نام IP تعریف کنید و آدرس سرور Nano را در آن قرار دهید و بر روی Enter کلید کنید.

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، این موضوع را در شکل ۸-۱۱۹۸، مشاهده می‌کنید.



شکل ۸- ۱۱۹۸ عضو کردن Nano Server در Domain

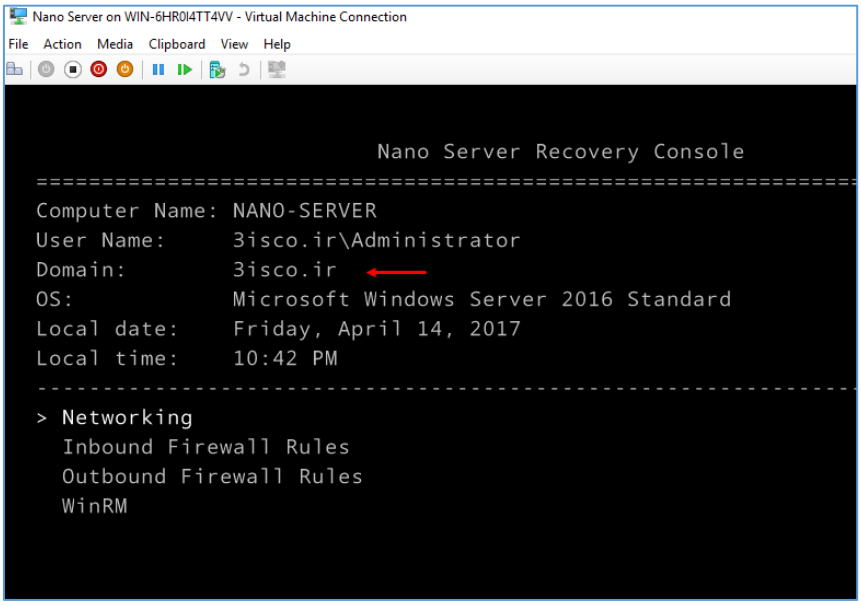
بعد از اجرا شدن سرور به مانند شکل ۸-۱۱۹۹، نام دومین را نیز در هنگام ورود وارد کنید و بر روی Enter فشار دهید.



شکل ۸- ۱۱۹۹ عضو کردن Nano Server در Domain

www.takbook.com

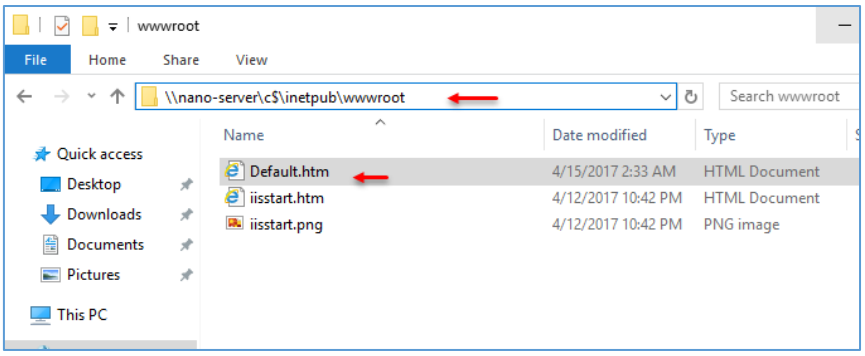
همان‌طور که در شکل ۸–۱۲۰۰، مشاهده می‌کنید، سرور مورد نظر، عضو دومین 3isco.ir شده و در شبکه مورد تأیید است.



شکل ۸- ۱۲۰۰ عضو کردن Nano Server در Domain

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

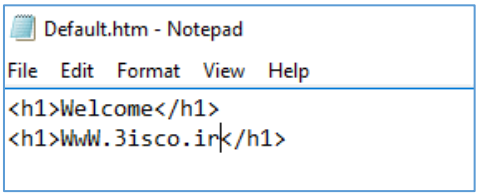
به مانند شکل ۸–۱۲۰۱، وارد آدرس مورد نظر در سرور Nano شوید و یک فایل htm با عنوان Default.htm ایجاد کنید و یک نوشته به مانند شکل ۸–۱۲۰۲، وارد کنید.



شکل ۸- ۱۲۰۱اجرای وب‌سایت در nano

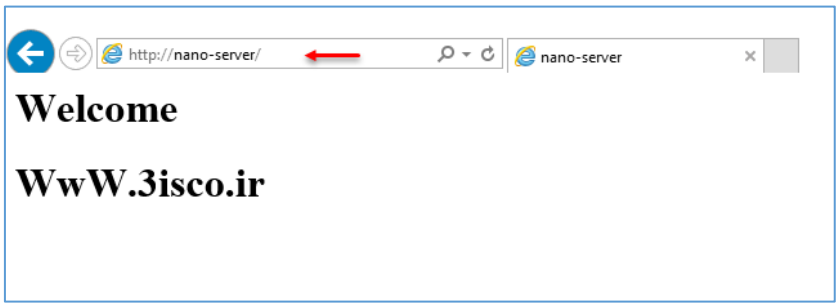
در شکل ۸–۱۲۰۲، متن HTML وارد شده است و در محلّ مورد نظر با نام مورد نظر ذخیره شده است.

www.takbook.com



شکل ۸- ۱۲۰۲ اجرای وب‌سایت در nano

بعد از انجام کارهای بالا، به مانند شکل ۸-۱۲۰۳، وارد مرورگر هر یک از سرورهای داخل شبکه شوید؛ در آدرس باید به جای Nano-server، نام سرور Nano خود را وارد کنید تا مشاهده کنید سایت مورد نظر برای شما باز خواهد شد.



شکل ۸- ۱۲۰۳ اجرای وب‌سایت در nano

۸-۳-۳۳-۲ کار با Docker در ویندوز سرور ۲۰۲۵

Docker یک پلتفرم نرم‌افزاری است که برای توسعه، ارسال و اجرای برنامه‌ها به صورت ایزوله شده و مستقل از محیط‌های مختلف استفاده می‌شود. این پلتفرم از کانتینرها (containers) برای اجرای برنامه‌ها در محیط‌های جداگانه و سبک استفاده می‌کند که به راحتی می‌توان آن‌ها را جابجا و مقیاس‌پذیر کرد.

Containers در دنیای فناوری به یک روش مجازی‌سازی اشاره دارد که به برنامه‌ها و سرویس‌ها اجازه می‌دهد در محیطی ایزوله و مستقل از سیستم‌عامل میزبان اجرا شوند. در این محیط ایزوله، هر کانتینر فقط شامل نرم‌افزار و وابستگی‌های لازم برای اجرای آن برنامه است. این ویژگی‌ها باعث می‌شود که کانتینرها سبک، سریع و به راحتی قابل انتقال بین سیستم‌ها و محیط‌ها باشند.

کاربردهای Containers

- مجازی‌سازی سبک: برخلاف ماشین‌های مجازی (VM)، که نیاز به سیستم‌عامل کامل دارند، کانتینرها تنها وابستگی‌ها و فایل‌های اجرایی لازم برای برنامه را در خود دارند، که باعث کاهش مصرف منابع می‌شود.

www.takbook.com

- قابلیت حمل و نقل: کانتینرها به شما این امکان را می‌دهند که برنامه‌ها را از یک محیط به محیط دیگر، مانند از یک سرور به سرور دیگر یا از محیط توسعه به محیط تولید، بدون نیاز به تغییرات زیاد منتقل کنید.
- مقیاس‌پذیری و توسعه سریع‌تر: از آنجا که کانتینرها می‌توانند به‌صورت جداگانه و مستقل از یکدیگر اجرا شوند، برنامه‌نویسان می‌توانند به راحتی برنامه‌های خود را مقیاس‌پذیر کنند و تغییرات را سریع‌تر اعمال کنند.
- امنیت: کانتینرها به دلیل ایزوله بودن، امنیت بیشتری نسبت به روش‌های دیگر مجازی‌سازی دارند. هر کانتینر به طور مستقل از دیگر کانتینرها عمل می‌کند.

استفاده از Containers در ویندوز

ویندوز نیز از کانتینرها پشتیبانی می‌کند و می‌توان از آن‌ها برای اجرای برنامه‌ها در محیط‌های ایزوله بهره برد. ویندوز از دو نوع کانتینر پشتیبانی می‌کند:

- Windows Containers: این کانتینرها به طور کامل بر روی ویندوز اجرا می‌شوند و از ویژگی‌های خاص ویندوز برای ایزوله‌سازی استفاده می‌کنند.
- Hyper-V Containers: این نوع کانتینرها مشابه ویندوز کانتینرها هستند، اما از تکنولوژی Hyper-V برای ایزوله‌سازی و تأمین امنیت بیشتر استفاده می‌کنند.

برای نصب Docker باید از دستور زیر استفاده کنید:

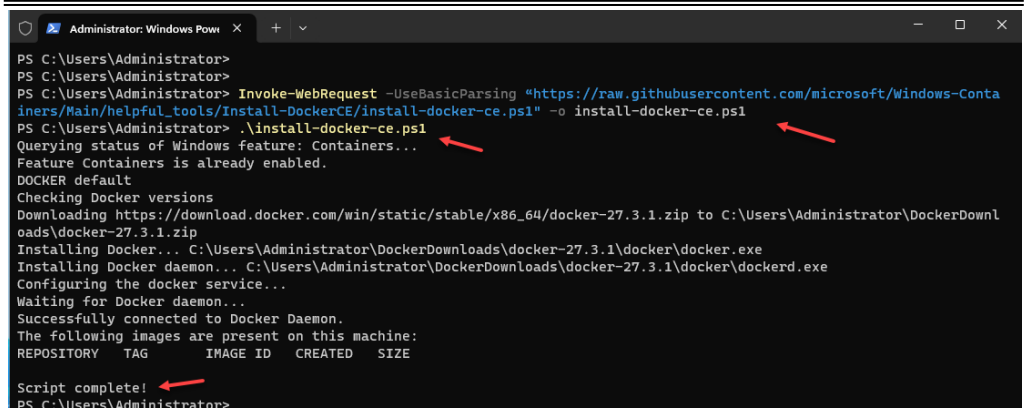
```
Invoke-WebRequest -UseBasicParsing
“https://raw.githubusercontent.com/microsoft/Windows-
Containers/Main/helpful_tools/Install-DockerCE/install-docker-ce.ps1"
-o install-docker-ce.ps1
```

بعد از دانلود Docker باید با دستور زیر آن را نصب کنید:

```
\.install-docker-ce.ps1
```

همان‌طور که در شکل۱۲۰٤-۸، مشاهده می‌کنید Docker با موفقیت بر روی ویندوز سرور 2025 نصب شده است، فقط باید به این نکته توجه کنید که در هنگام نصب Docker سرور باید به اینترنت متصل باشد.

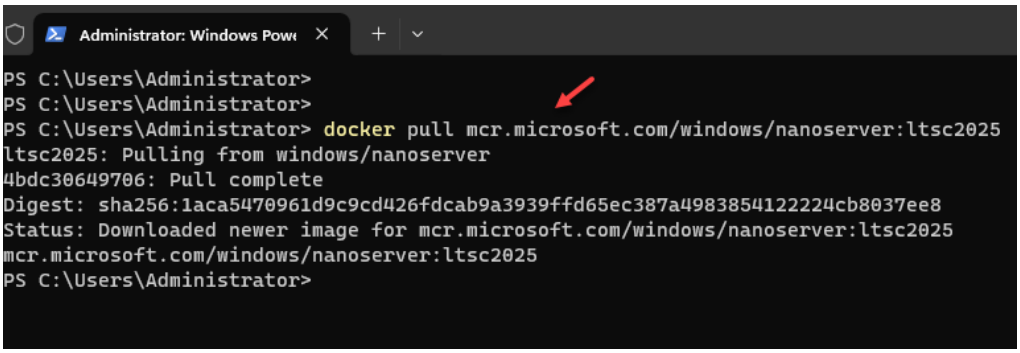
www.takbook.com



شکل ۸- ۱۲۰۴ کار با *Docker* در ویندوز سرور

بعد از نصب نرم‌افزار Docker باید با دستور زیر آخرین ورژن Nano Server را نصب کنید، بعد از اجرای این دستور آخرین ورژن این نرم افزار دانلود و نصب می‌شود که این موضوع را در شکل ۸-۱۲۰۵، مشاهده می‌کنید.

```
docker pull mcr.microsoft.com/windows/nanoserver:ltsc2025
```



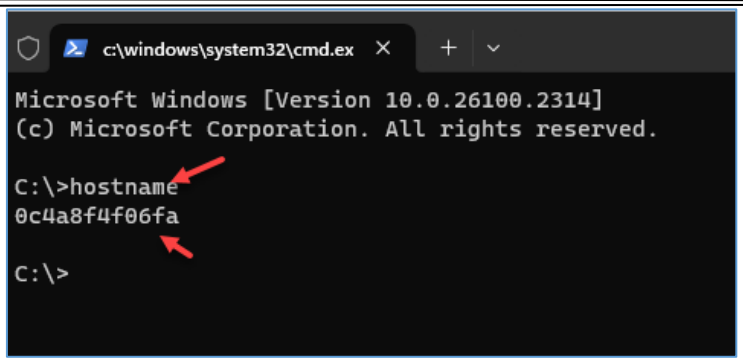
شکل ۸- ۱۲۰۵ کار با *Docker* در ویندوز سرور

بعد از نصب می‌توانید یک کانتینر از NanoServer با دستور زیر ایجاد کنید.

```
docker run -it mcr.microsoft.com/windows/nanoserver:ltsc2025
```

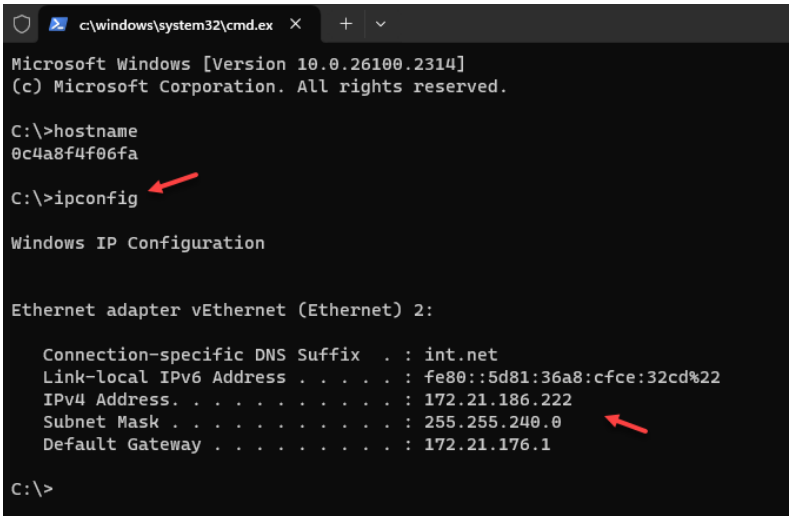
بعد از اجرا ی دستور به مانند شکل ۸-۱۲۰۶، وارد محیط CMD می‌شوید و اگر دستور hostname را وارد کنید چند حروف و عدد را مشاهده می‌کنید که نشان می‌دهد بر روی Nano Server قرار دارید.

www.takbook.com



شکل ۸- ۱۲۰۶ کار با Docker در ویندوز سرور

به مانند شکل ۸-۱۲۰۷، با استفاده از دستور ipconfig هم می‌تواند آدرس IP و اطلاعات مورد نظر که دریافت کرده را مشاهده کنید.



شکل ۸- ۱۲۰۷ کار با Docker در ویندوز سرور

۸-۳-۳۵ کار با Group Policy

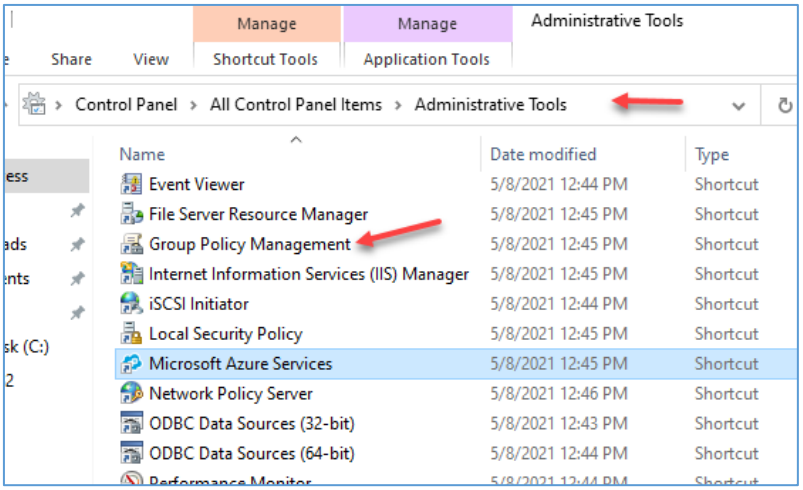
Group Policy امکانی است در ویندوز سرور که به کمک آن می‌توانید تنظیمات خاصی را در آن انجام دهید و این تنظیمات را بر روی کاربران و کلاینت‌ها اعمال کنید، همان‌طور که می‌دانید زمانی که می‌خواهیم برای یک کاربر رمز عبور تعریف کنیم، حتماً باید یک رمز پیچیده و تعداد مشخص استفاده کنیم که کنترل پیچیدگی رمز عبور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

نکته مهم: قبل از اینکه Domain Controller را روی سرور نصب کنید، Group Policy به صورت Local Group Policy در دسترس است و می‌توانید تنظیمات آن را تغییر دهید ولی اگر Domain Controller روی

www.takbook.com

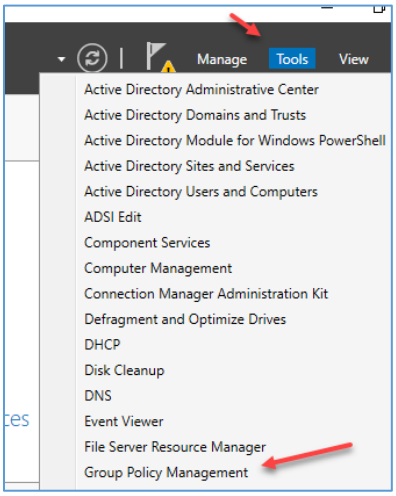
سرور شما نصب باشد دیگر Local Group policy کاربرد ندارد و گزینه‌های آن غیرفعال می‌شوند و در عوض Group Policy مربوط به Domain فعال می‌شود که در زیر بررسی خواهیم کرد.

برای اجرای سرویس Group Policy می‌توانید به آدرس شکل ۸-۱۲۰۸، مراجعه کنید و Group Policy Management را اجرا کنید.



شکل ۸- ۱۲۰۸ کار با *Group Policy*

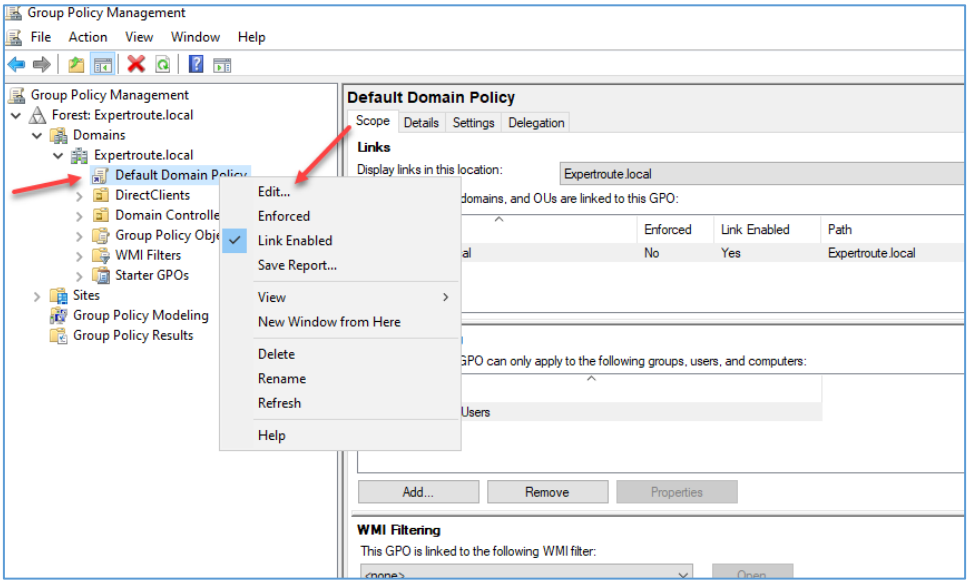
و یا به مانند شکل ۸-۱۲۰۹، وارد Server Manager شوید و از منوی Tools گزینه‌ی Group Policy Management را انتخاب کنید.



شکل ۸- ۱۲۰۹ کار با *Group Policy*

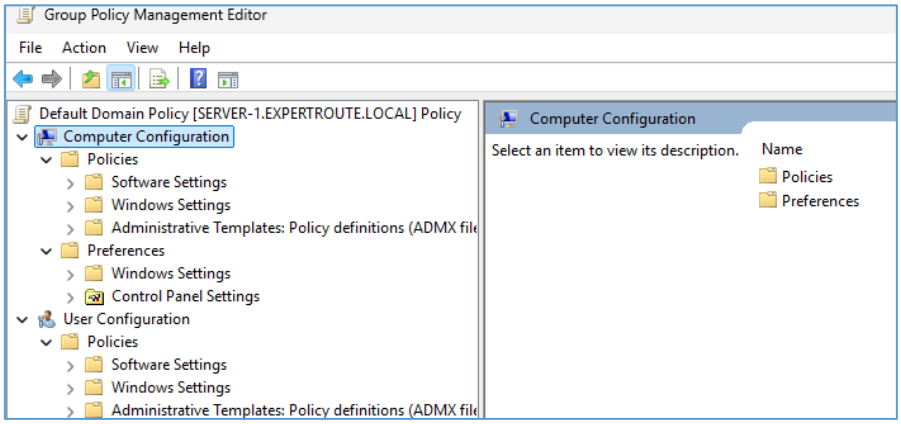
www.takbook.com

همان‌طور که در شکل ۸-۱۲۱۰، مشاهده می‌کنید وارد سرویس Group Policy شدیم، در ادامه با تمام اجزای این سرویس آشنا خواهید شد، برای شروع باید وارد قسمت ویرایش اطلاعات Group Policy شویم، برای این کار به مانند شکل بر روی Default Domain Policy کلیک راست کنید و گزینه Edit را انتخاب کنید.



شکل ۸- ۱۲۱۰ کار با Group Policy

همان‌طور که در شکل ۸-۱۲۱۱، مشاهده می‌کنید، در قسمت Edit Group Policy دو قسمت وجود دارد، یکی Computer Configuration است که مربوط به تنظیماتی است که مختص سرورها و کلاینت‌ها است و قسمت User configuration هم مختص کاربران است این بدین معنا است که در هر قسمت اگر تغییراتی ایجاد کنید این تغییرات برای کاربر یا سیستم مورد نظر اعمال می‌شود.

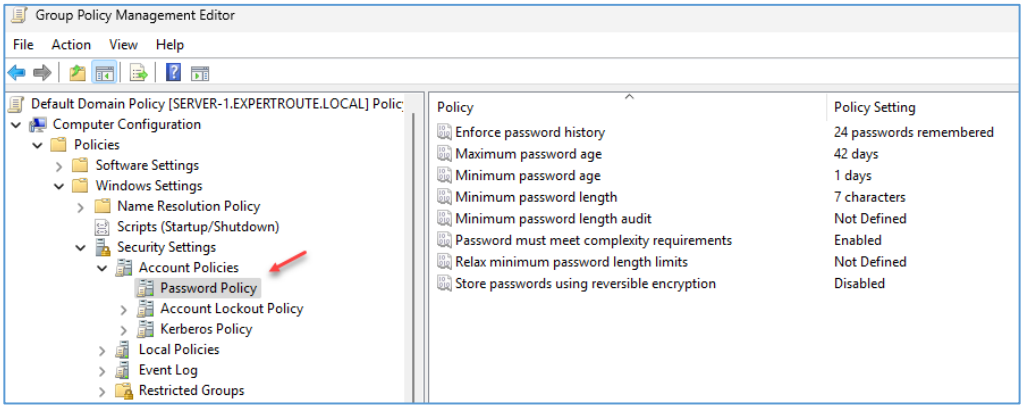


شکل ۸- ۱۲۱۱ کار با Group Policy

www.takbook.com

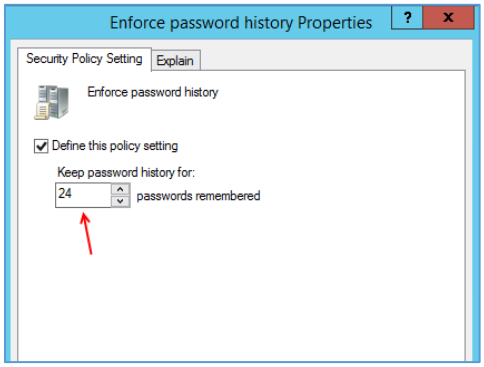
۱-۳۵-۳-۸ بررسی قسمت Account Policy

برای شروع کار قسمت Password Policy را با هم بررسی می‌کنیم، در این قسمت می‌توانیم حداقل طول یک Password را کم یا زیاد کنیم و یا پیچیدگی آن را تغییر دهیم، برای این کار به مانند شکل ۸-۱۲۱۲، وارد قسمت Password Policy می‌شویم که در این قسمت ۸ گزینه را مشاهده می‌کنید که در زیر آنها را بررسی می‌کنیم.



شکل ۸- ۱۲۱۲ کار با *Group Policy*

در قسمت Enforce Password history می‌توانید مشخص کنید که چه تعداد از رمز عبورهایی که توسط مدیر و کاربران شبکه وارد شده است در Domain ذخیره شود تا کسی دیگر نتواند رمزی شبیه به رمز دیگران ایجاد کند که در شکل ۸-۱۲۱۳، عدد ۲٤ قرار دارد که تا ۲٤ رمز عبور را در خود ذخیره می‌کند و شما می‌توانید این عدد را به راحتی تغییر دهید، بعد از تغییر بر روی ok کلیک کنید.

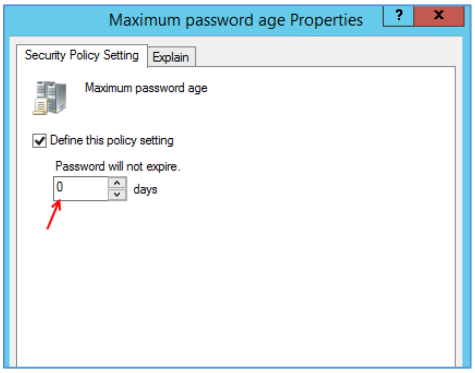


شکل ۸- ۱۲۱۳ کار با *Group Policy*

در قسمت Maximim Password age می‌توانید مشخص کنید که یک رمز عبور تا چند روز اعتبار داشته باشد، در شکل ۸-۱۲۱٤، عدد ٤۲ را به صفر تغییر دادیم و اگر به دقت به شکل توجه کنید بالای عدد صفر نوشته Password will not expire که به این معنا است که رمز به هیچ عنوان انقضاء نخواهد شد، اگر به یاد

www.takbook.com

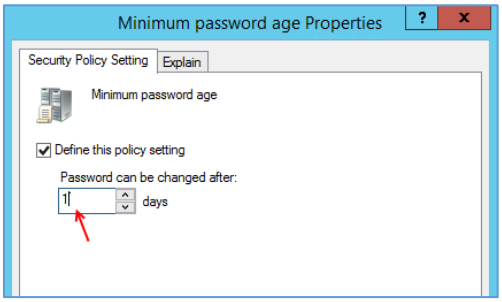
داشته باشید در زمان ایجاد کاربر گزینه‌ای با نام Password Never Expire وجود داشت که با انتخاب آن کاربر نمی‌توانست رمز عبور را تغییر دهد، در این قسمت هم با وارد کردن عدد صفر دیگر لازم نیست تیک گزینه Password Never Expire را در موقع ایجاد کاربر انتخاب کنیم.



شکل ۸- ۱۲۱۴ کار با *Group Policy*

به مانند شکل ۸-۱۲۱۵، Minimum Password age می‌توانید مشخص کنید که زمانی که یک کاربر رمز عبور خود را تغییر داد تا چه زمانی فرصت دارد که رمز عبور خود را دوباره تغییر دهد که این عدد به صورت پیش‌فرض بر روی ۱ روز قرار دارد که می‌تواند عددی بین ۱ تا ۹۹۸ باشد.

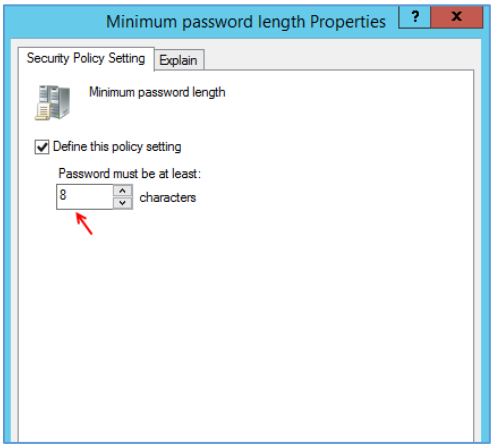
نکته مهم: زمانی که عدد قسمت Maximim Password age را به صفر تغییر دهید دیگر Minimum Password age هیچ گونه تاثیری ندارد، فقط توجه داشته باشید Minimum Password age باید کوچکتر از Maximim Password age باشد، جزءاینکه Maximim Password age به صفر تغییر کرده باشد.



شکل ۸- ۱۲۱۵ کار با *Group Policy*

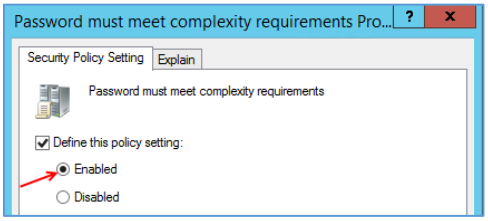
شکل ۸-۱۲۱۶، مربوط به Minimum Password length می‌باشد که طول رمز عبور را مشخص می‌کند که به صورت پیش‌فرض برای دومین ۷ می‌باشد که می‌توانید این مقدار را تغییر دهید که در این قسمت این عدد به ۸ کاراکتر تغییر کرده است، سعی کنید مقدار رمز عبور را از ۸ به بالا وارد کنید تا امنیت اطلاعات قوی‌تر شود.

www.takbook.com



شکل ۸- ۱۲۱۶ کار با Group Policy

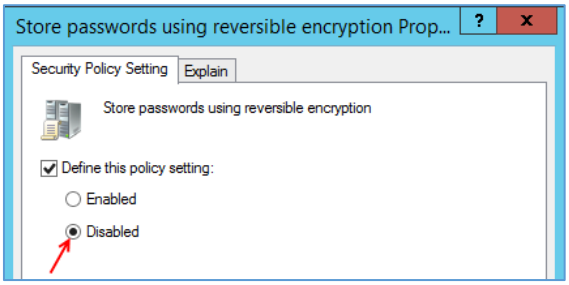
در شکل ۸-۱۲۱۷، Password must meet Complexity requirements می‌توانید مشخص کنید که آیا رمز عبور باید به صورت پیچیده وارد شود به طور مثال Test@123456 ترکیبی از حروف، اعداد و علائم باشد و یا با انتخاب گزینه Disabled نیازی به وارد کردن رمز به صورت پیچیده نیست.



شکل ۸- ۱۲۱۷ کار با Group Policy

در شکل ۸-۱۲۱۸، Store Passwords Using Reversible encryption با انتخاب Enabled رمز عبور به صورت Clear Text در شبکه فعال می‌شود و امنیت اطلاعات بسیار کاهش می‌یابد که سعی کنید در صورت نیاز آن را فعال کنید.

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

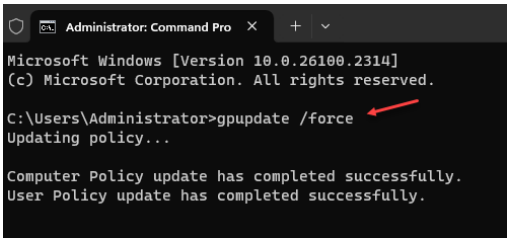


شکل ۸- ۱۲۱۸ کار با Group Policy

www.takbook.com

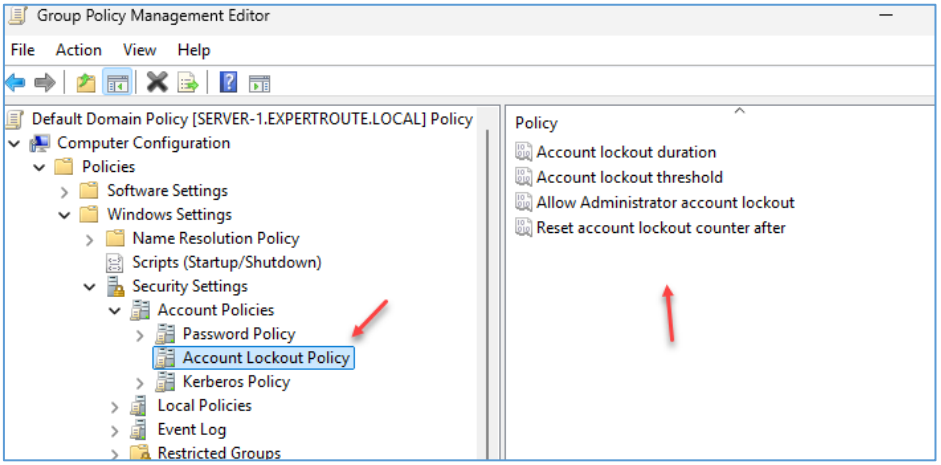
توجه داشته باشید گزینه‌ی Relax minimum password length limits اگر این گزینه فعال شود، محدودیت‌های طول حداقلی رمز عبور ممکن است کاهش یابد. در اینجا "Not Defined" است، یعنی تغییری در آن داده نشده.

نکته مهم: بعد از اینکه تنظیمات Group Policy را تغییر دادید، برای اینکه این تنظیمات روی دامین و کلاینت‌های سازمان به صورت سریع اعمال شود باید از دستور Gpupdate /Force در CMD استفاده کنید، که این دستور در شکل ۸-۱۲۱۹، اجرا شده است.



شکل ۸- ۱۲۱۹ کار با Group Policy

قسمت بعدی که با هم بررسی می‌کنیم، Account Lookout Policy می‌باشد، به مانند شکل ۸-۱۲۲۰، از سمت چپ بر روی Account Lookout Policy کلیک کنید تا صفحه مربوط به آن باز شود، در این صفحه چهار گزینه وجود دارد که با هم مورد بررسی قرار می‌دهیم.

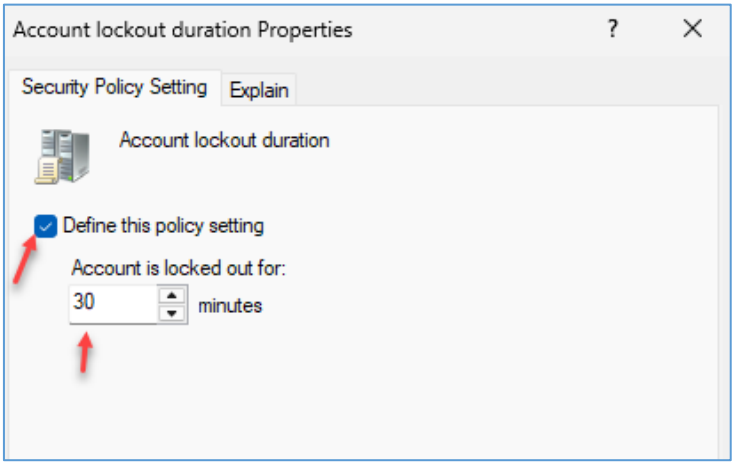


شکل ۸- ۱۲۲۰ کار با Group Policy

در قسمت Account Lockout duration می‌توانید مشخص کنید که، یک حساب زمانی که قفل شد تا چه مدت قفل بماند و بعد فعال شود، مثلاً در شکل ۸-۱۲۲۱، گزینه Define this policy setting را انتخاب کنید و یک عدد بر حسب دقیقه مثلاً ۳۰ وارد کنید این عدد به این معنا است که کاربر زمانی که به دلایل گوناگون مثلاً

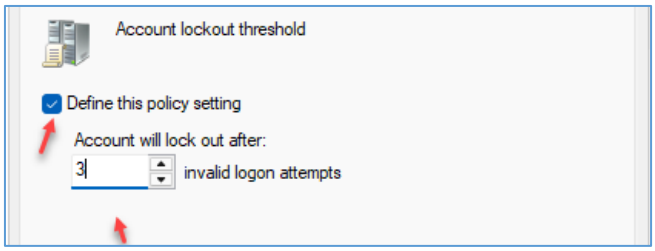
www.takbook.com

اشتباه وارد کردن رمز عبور به دفعات متعدد و یا غیرفعال کردن حساب توسط مدیر شبکه بعد از این ۳۰ دقیقه حساب موردنظر دوباره فعال می‌شود.



شکل ۸- ۱۲۲۱ کار با *Group Policy*

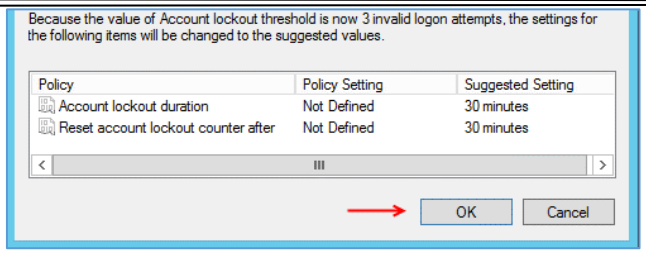
در شکل ۸-۱۲۲۲، شما می‌توانید مشخص کنید که کاربر بعد از اینکه به تعداد مشخص‌شده مثلاً ۳ بار رمز ورود را به اشتباه وارد کرد حساب آن قفل شود، البته بعد از زمان مشخص‌شده در قسمت Account Lockout duration این حساب فعال می‌شود.



شکل ۸- ۱۲۲۲ کار با *Group Policy*

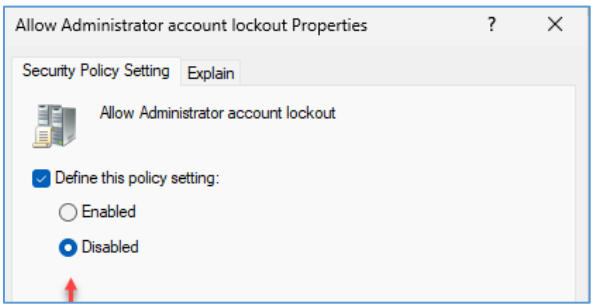
زمانی که در قسمت قبل بر روی ok کلیک کنید شکل ۸-۱۲۲۳، ظاهر می‌شود، در این قسمت این پیغام به شما داده می‌شود که اگر می‌خواهید این قسمت فعال شود باید هر دو قسمت Account Lockout duration و Reset Account تنظیم شوند که به صورت پیش‌فرض ۳۰ دقیقه می‌باشد.

www.takbook.com



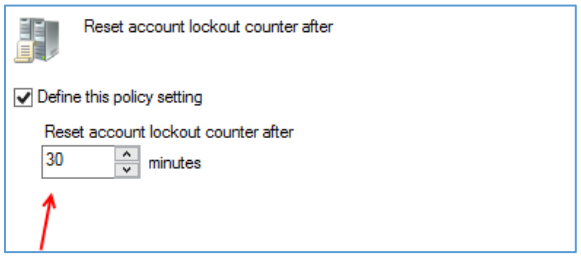
شکل ۸- ۱۲۲۳ کار با Group Policy

به مانند شکل ۸-۱۲۲٤، اگر گزینه‌ی Allow Administrator account lockout را فعال کنید، باعث می‌شود اکانت کاربر Adminitsrator هم قفل شود که باید به این موضوع خیلی دقت کنید و در صورتی که نیاز ندارید آن را فعال نکنید.



شکل ۸- ۱۲۲۴ کار با Group Policy

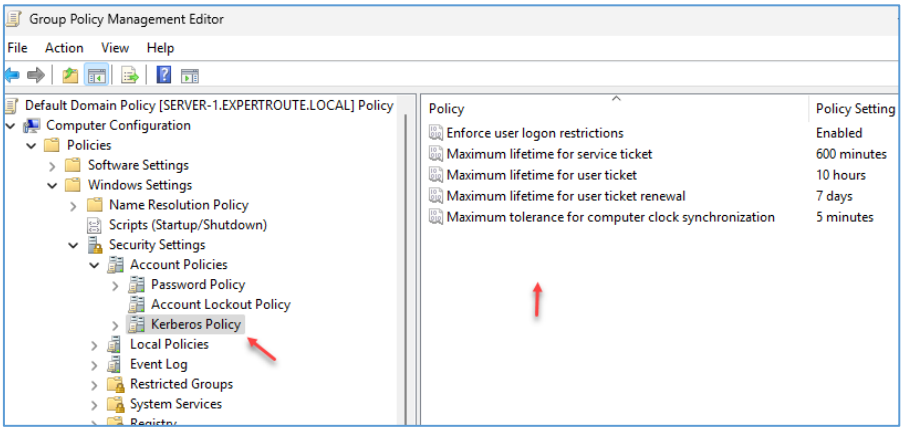
در شکل ۸-۱۲۲۵، باید عددی را مساوی یا کمتر از عدد قسمت Account Lockout duration تعریف کنید که زمانی که کاربر ورود اشتباه داشت اطلاعات ذخیره شده در داخل دایرکتوری حذف شود، یعنی اینکه مثلاً تعداد ورود کاربر ۳ بار شد این اطلاعت در اکتیو دایرکتوری به صورت یک شمارنده ثبت می‌شود که با اعمال زمان مناسب در این قسمت این شمارنده صفر خواهد شد.



شکل ۸- ۱۲۲۵ کار با Group Policy

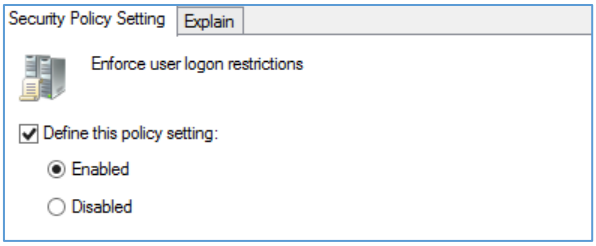
قسمت بعدی که مورد بررسی قرار می‌دهیم به مانند شکل ۸-۱۲۲٦، Kerberos Policy می‌باشد که مربوط به امنیت کاربران می‌باشد که تک تک این پنج گزینه را با هم مورد بررسی قرار می‌دهیم.

www.takbook.com



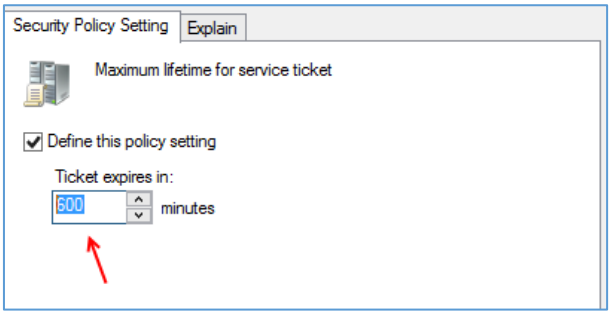
شکل ۸- ۱۲۲۶ کار با *Group Policy*

شکل ۸-۱۲۲۷، مربوط به ورود کاربران می‌باشد که به صورت پیش‌فرض فعال است و زمانی که یک کاربر وارد سیستم می‌شود یک گواهینامه امنیتی برای آن صادر می‌شود.



شکل ۸- ۱۲۲۷ کار با *Group Policy*

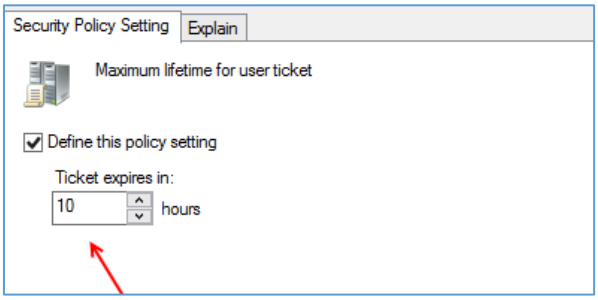
شکل ۸-۱۲۲۸، قسمت Maximum lifetime for Service ticket می‌توانید مشخص کنید که مدت زمان گواهینامه اعتباری برای یک سرویس فعال چقدر باشد. که بعد از اتمام این زمان سرویس انقضاء شده و در سرور نمی‌تواند به دیگران سرویس دهد.



شکل ۸- ۱۲۲۸ کار با *Group Policy*

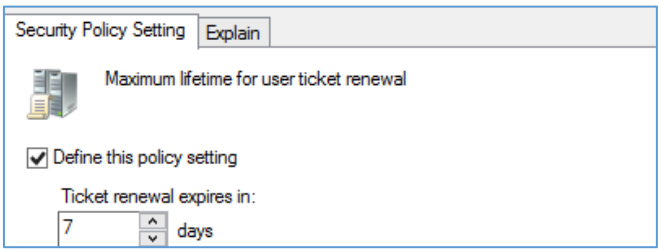
www.takbook.com

در شکل ۸-۱۲۲۹، در قسمت Maximum lifetime for user ticket می‌توانید مقدار زمانی را که یک کاربر می‌تواند از گواهینامه تخصیص داده شده به وی در زمان ورود استفاده کند مشخص کنید. که این عدد باید بین ۰ تا ۹۹۹۹ قرار گیرد که اگر صفر باشد گزینه بعدی آن هم غیر فعال می‌شود.



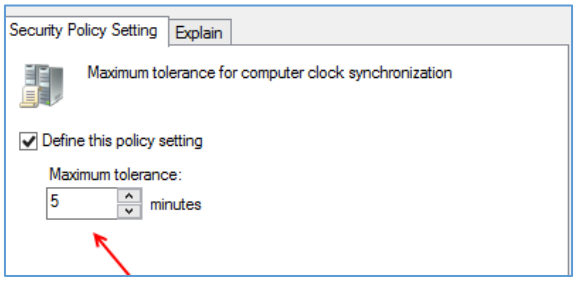
شکل ۸- ۱۲۲۹ کار با Group Policy

به مانند شکل ۸-۱۲۳۰، در قسمت Maximum lifetime for user ticket renewal تعداد روز فعال بودن گواهینامه یا بلیط داده شده به کاربر را مشخص می‌کند که بعد از آن گواهینامه یا بلیط موردنظر انقضاء می‌شود.



شکل ۸- ۱۲۳۰ کار با Group Policy

به مانند شکل ۸-۱۲۳۰، قسمت Maximum tolerance for computer clock synchronization به این منظور استفاده می‌شود که در زمان مشخص‌شده مثلاً هر ۵ دقیقه کامپیوتر سرور با کامپیوتر کلاینت تارخ و زمان خود را با هم هماهنگ‌سازی کنند چون الگوریتم Kerbros شدیداً به برابر بدون زمان بین سرور و کلاینت نیاز دارد تا گواهینامه برای سرویس کاربر موردنظر تعریف و محاسبه کند.

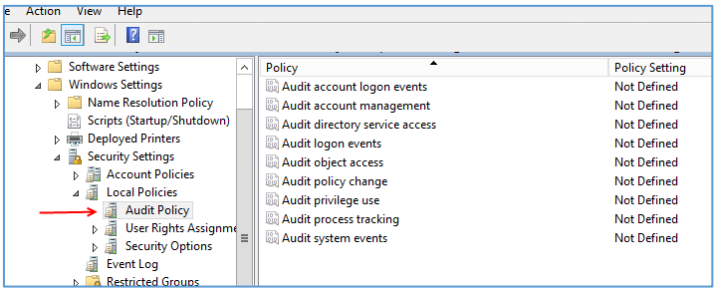


شکل ۸- ۱۲۳۱ کار با Group Policy

www.takbook.com

۲-۳۵-۳-۸ بررسی قسمت Audit Policy

قسمت Audit Policy مربوط به ثبت رویدادهای مربوط به ورود کاربران و ایجاد تغییرات و تغییر رمز عبور و ... می‌باشد که در صورت نیاز می‌توانید هر یک از قسمت‌های موجود را فعال کنید، در شکل ۸-۱۲۳۲، وارد قسمت Audit Policy می‌شویم که در این قسمت ۹ گزینه مختلف وجود دارد که هر کدام برای منظور خاصی طراحی شده‌اند که در جدول ۸-٤، همه آنها را بررسی می‌کنیم.



شکل ۸- ۱۲۳۲ کار با Group Policy

جدول ۸- ۴ بررسی قسمت Audit Policy

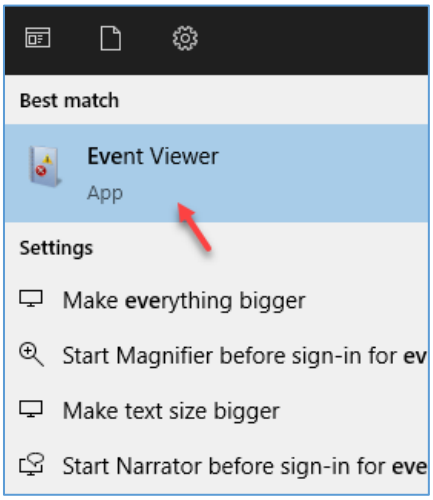
گزینه	توضیحات
Audit account logon events	این گزینه زمانی که فعال شود ورود کاربران را به سیستم ثبت می‌کند.
Audit account management	برای ثبت رویدادهایی مانند ایجاد کاربر، حذف، تغییر نام و... به کار می‌رود.
Audit directory service access	ثبت رویدادهای مربوط به دسترسی کاربران به فایل ها می‌باشد.
Audit logon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

www.takbook.com

Audit process tracking	این قسمت هم بر روی حسابرسی سیستم عامل بر روی فرایندها کاربرد دارد.
Audit system events	ثبت رویدادهایی مانند تغییر ساعت سیستم، تاریخ، برنامه های Startup و ...

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

همه رویدادهای سیستم یا همان Event یا Log در سرویس Event Viewer ثبت می‌شود، برای اجرای این سرویس به مانند شکل ۸-۱۲۳۳، وارد Search شوید و کلمه event را وارد کنید و سرویس Event Viewer را اجرا کنید.

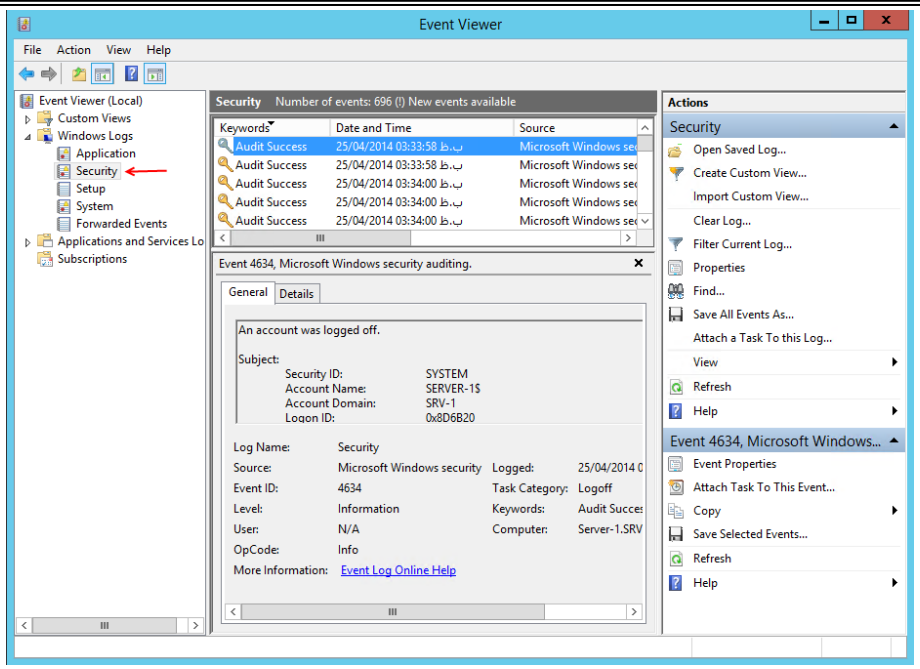


شکل ۸- ۱۲۳۳ بررسی *Event Viewer*

همان‌طور که در شکل ۸-۱۲۳٤، مشاهده می‌کنید، وارد سرویس Event Viewer شدیم، در این سرویس تمام ردپای ویندوز ثبت می‌شود، یعنی شما هیچ کاری را نمی‌توانید انجام دهید که در اینجا ثبت نشود.

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

www.takbook.com



شکل ۸- ۱۲۳۴ بررسی Event Viewer

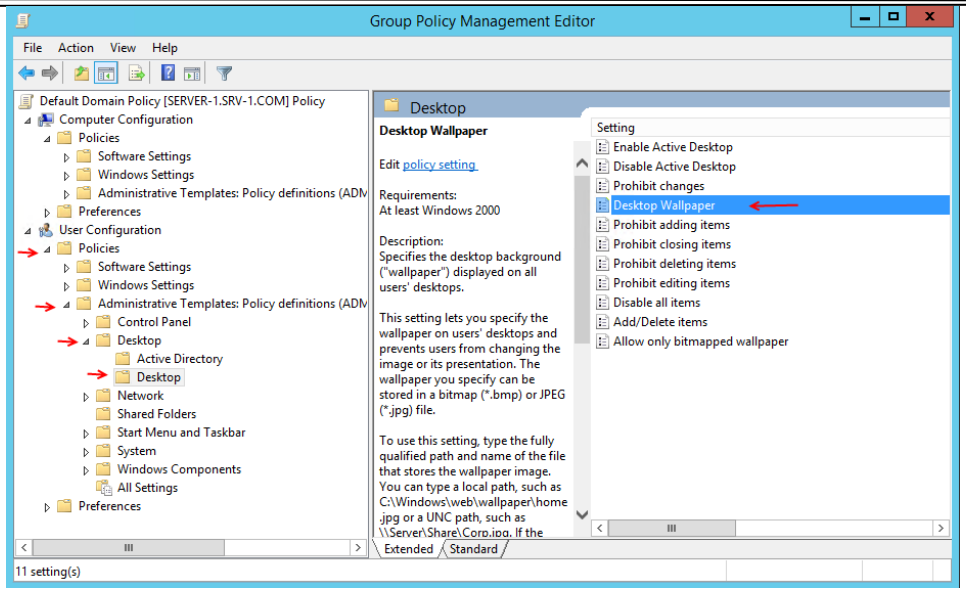
با این سرویس می‌توانید مشخص کنید که چه کاربری یا کامپیوتری در چه زمان و تاریخی وارد سیستم شده است، در کل این سرویس فقط از طریق مدیر شبکه اجرا می‌شود و از دسترس کاربران معمولی خارج است.

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

۳-۳۵-۳-۸ تغییر تصویر BackGround تمام کلاینت‌های شبکه

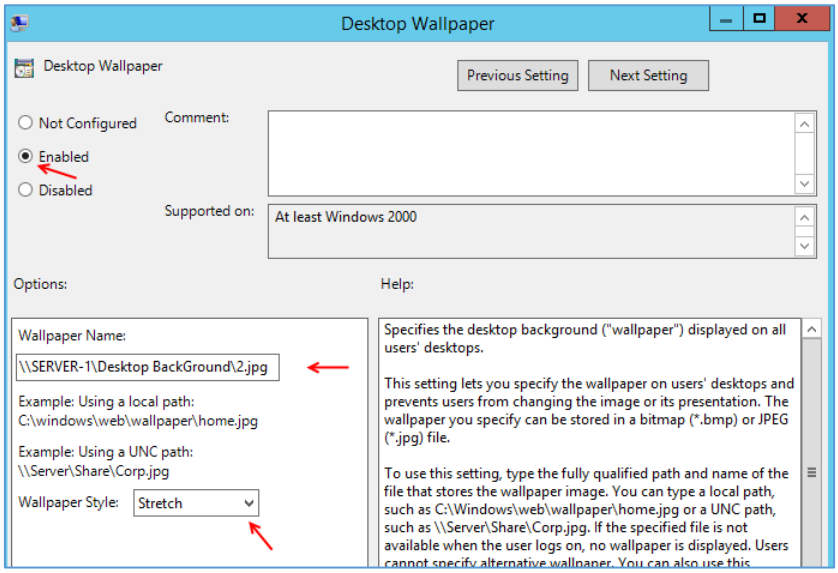
در این قسمت می‌خواهیم یک تصویر را به‌عنوان تصویر زمینه تمام کلاینت‌های متصل به شبکه دومین قرار دهیم، این کار توسط سرویس Group Policy به‌راحتی امکان‌پذیر است، برای شروع سرویس Group Policy را اجرا کنید و به مسیر مشخص‌شده در شکل ۸-۱۲۳۵، مراجعه کنید، در لیست بازشده مربوط به Desktop بر روی Desktop Wallpaper دو بار کلیک کنید.

www.takbook.com



شکل ۸- ۱۲۳۵ تغییر تصویر BackGround تمام کلاینت‌های شبکه

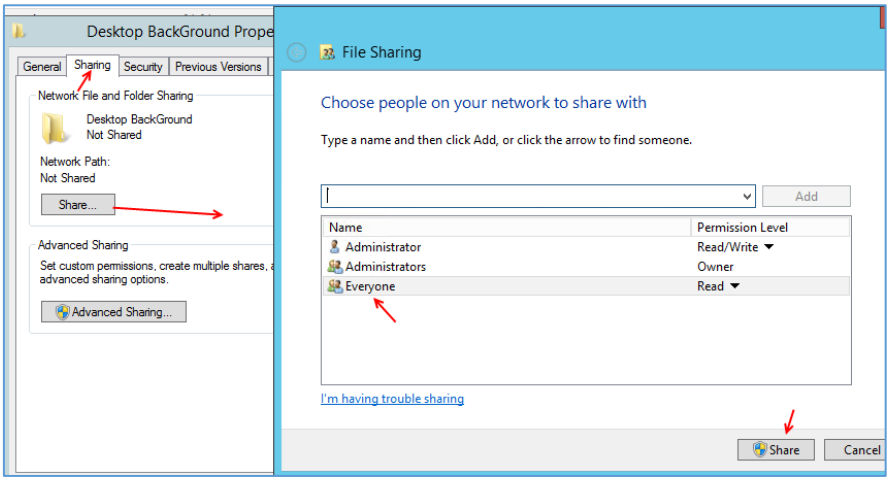
در شکل ۸-۱۲۳۶، گزینه Enable را در بالای صفحه انتخاب کنید و در قسمت Wallpaper Name که مهم‌ترین بخش است، باید آدرس عکس موردنظر خود را وارد کنید، همان‌طور که مشاهده می‌کنید آدرس موردنظر به‌صورت شبکه‌ای واردشده است، شما باید یک پوشه در سرور خود ایجاد کنید و عکس موردنظر خود را داخل آن قرار دهید و بعدازآن باید پوشه موردنظر را برای تمام کاربران Share کنید.



شکل ۸- ۱۲۳۶ تغییر تصویر BackGround تمام کلاینت‌های شبکه

www.takbook.com

در شکل ۸-۱۲۳۷، یک پوشه بانام Desktop BackGround ایجادشده است و برای گروه Everyone اشتراک گذاشته‌شده است، تمام کاربران داخل شبکه عضو گروه Everyone می‌باشند که فقط مجوز Read را به آن دادیم.

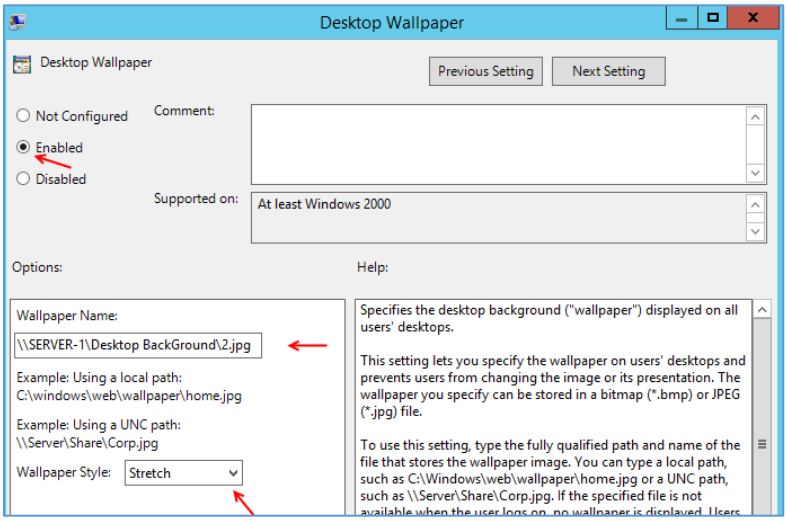


شکل ۸- ۱۲۳۷ تغییر تصویر BackGround تمام کلاینت‌های شبکه

به مانند شکل ۸-۱۲۳۶، برمی‌گردیم، در بخش Wallpaper Name آدرس شبکه عکس داخل پوشه Desktop BakGround را وارد می‌کنیم:

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

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



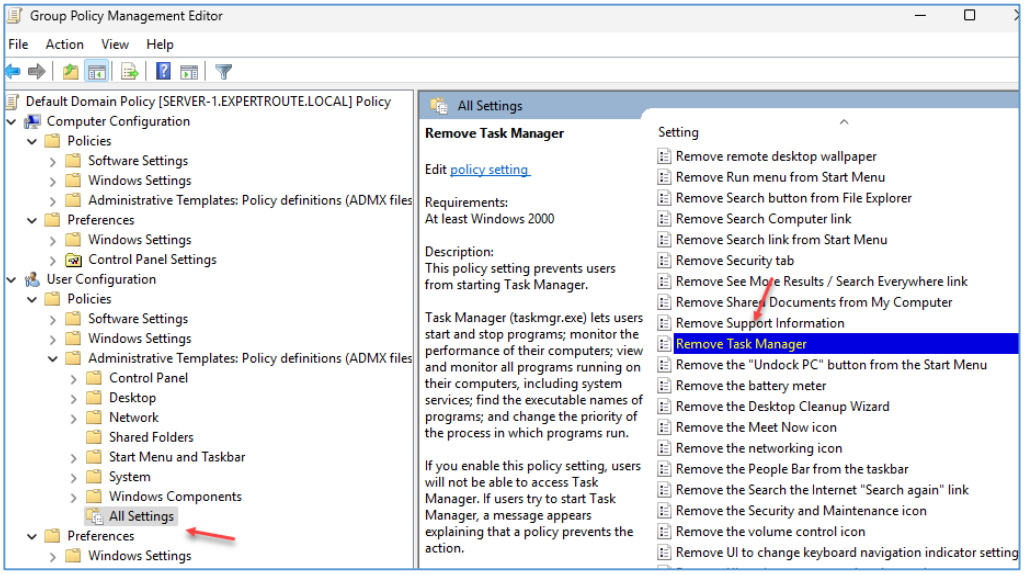
شکل ۸- ۱۲۳۸ تغییر تصویر BackGround تمام کلاینت‌های شبکه

www.takbook.com

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

٤-۳-۳۵-۸ غیرفعال کردن Task Manager برای تمام کلاینت‌ها

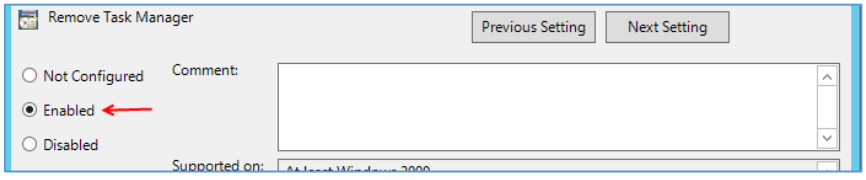
برای اینکه Task Manager را برای تمام کلاینت‌های داخل شبکه غیرفعال کنید، وارد سرویس Group Policy شوید، به مانند شکل ۸-۱۲۳۹، از سمت چپ بر روی All Settings کلیک کنید و در لیست بازشده بر روی گزینه Remove Task Manager دو بار کلیک کنید.



شکل ۸- ۱۲۳۹ غیرفعال کردن Task Manager برای تمام کلاینت‌ها

در شکل ۸-۱۲٤۰، برای فعال کردن این موضوع بر روی Enabled کلیک کنید و بعد بر روی ok کلیک کنید. با این کار هیچ کلاینتی نمی‌تواند Task Manager را اجرا کند.

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

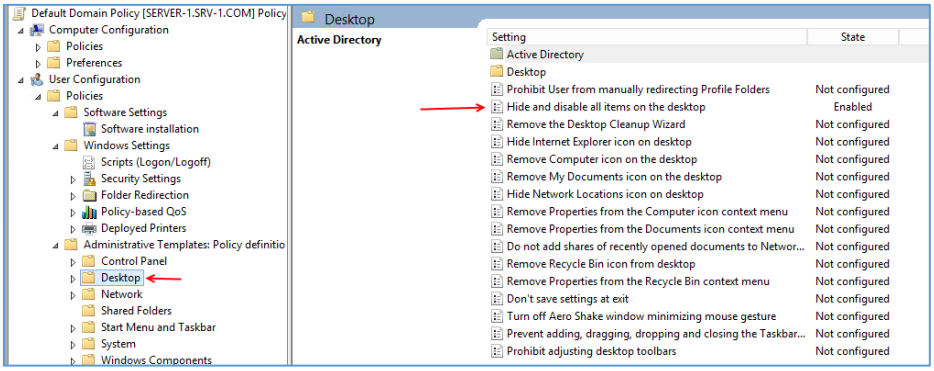


شکل ۸- ۱۲۴۰ غیرفعال کردن Task Manager برای تمام کلاینت‌ها

www.takbook.com

۸-۳-۳۵-۵ حذف کردن راست کلیک بر روی Desktop در تمام کلاینت‌ها

در این قسمت می‌خواهیم راست کلیک کردن بر روی Desktop مربوط به کلاینت‌ها را غیرفعال کنیم برای این کار برای ورود به این قسمت به مانند شکل ۸-۱۲۴۱، از قسمت Administrative Templates گزینه Desktop را انتخاب کنید و در لیست بازشده بر روی گزینه Edit and disable all items on the desktop دو بار کلیک کنید.



شکل ۸- ۱۲۴۱ حذف کردن راست کلیک بر روی Desktop

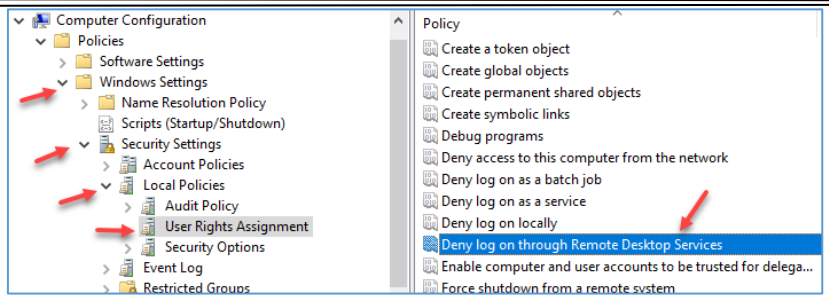
در صفحه بازشده گزینه Enable را انتخاب و بر روی ok کلیک کنید، بعد از این کار هیچ کاربری نمی‌تواند روی کلاینت خود کلیک راست کند.

در شکل ۸-۱۲۴۱، کارهایی دیگری می‌توان انجام داد مثلاً با Enable کردن گزینه Remove Computer Icon on the Desktop می‌توانید آیکون My computer را روی Desktop حذف کنیم و یا با فعال کردن گزینه Remove Properties from the computer icon context menu می‌توانید گزینه Properties مربوط به آیکون My Computer را حذف کنید.

۸-۳-۳۵-۶ غیرفعال کردن Remote Desktop بر روی کلاینت‌ها

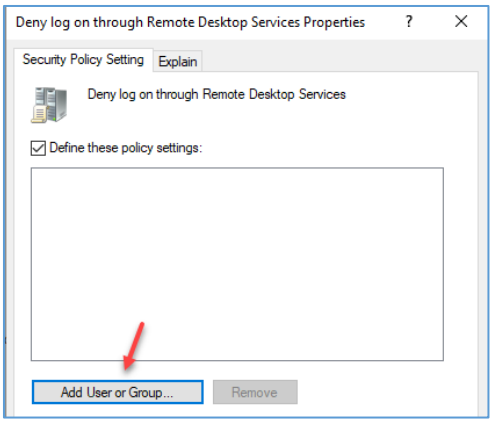
برای اینکه به کلاینت‌ها اجازه ندهیم که بتوانند از سرویس Remote Desktop استفاده کنند باید در Group Policy مسیر زیر را بررسی کنیم، به مانند شکل ۸-۱۲۴۲، در قسمت User Rights Assignment بر روی گزینه‌ی Deny log on through Remote desktop Services را دو بار کلیک کنید.

www.takbook.com



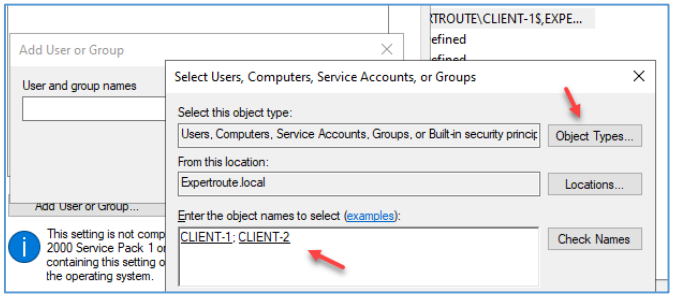
شکل ۸- ۱۲۴۲ غیرفعال کردن *Remote Desktop* بر روی کلاینت‌ها

در ادامه و در شکل ۸-۱۲۴۳، برای اینکه کلاینت و یا کاربر را به لیست اضافه کنید بر روی Add user or Group کلیک کنید.



شکل ۸- ۱۲۴۳ غیرفعال کردن *Remote Desktop* بر روی کلاینت‌ها

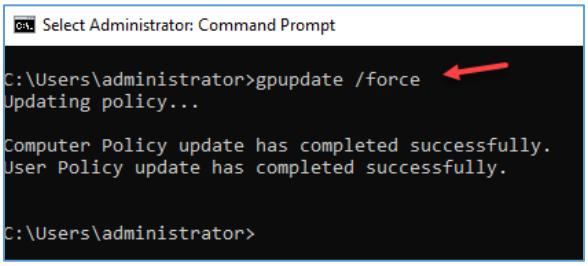
به مانند شکل ۸-۱۲۴۴، بر روی Browse کلیک کنید و از قسمت Object Types باید گزینه‌ی Computers را انتخاب کنید و نام کلاینت خود را وارد بر روی OK کلیک کنید.



شکل ۸- ۱۲۴۴ غیرفعال کردن *Remote Desktop* بر روی کلاینت‌ها

به مانند شکل ۸-۱۲۴۵، برای اینکه تنظیمات بر روی کلاینت‌ها اعمال شود باید دستور gpupdate /force را اجرا کنید.

www.takbook.com

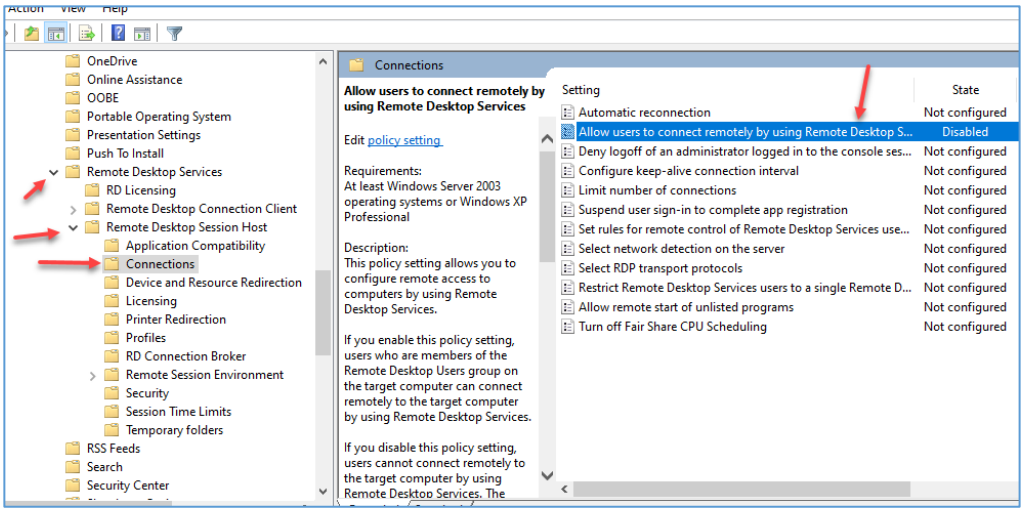


شکل ۸- ۱۲۴۵ غیرفعال کردن Remote Desktop بر روی کلاینت‌ها

حالا اگر وارد کلاینت شوید و از Remote Desktop استفاده کنید، این سرویس به هیچ عنوان کار نخواهد کرد، برای اینکه این موضوع را غیرفعال کنید باید کلاینت مورد نظر را از لیست خارج کنید.

روش دیگری هم وجود دارد که می‌توانید بر روی هر سیستم Remote Dektop را غیرفعال کنید، برای این کار Grop Policy را اجرا کنید و به مسیر زیر بروید و به مانند شکل ۸-۱۲٤٦، گزینه‌ی Allow users to connect remotely by using Remote Desktop Services را غیر فعال کنید که با این کار کسی نمی‌تواند به این سیستم ریموت بزند.

Computer Configuration – Administrative Templates – Windows Components – Remote Desktop Session Host – Connectins



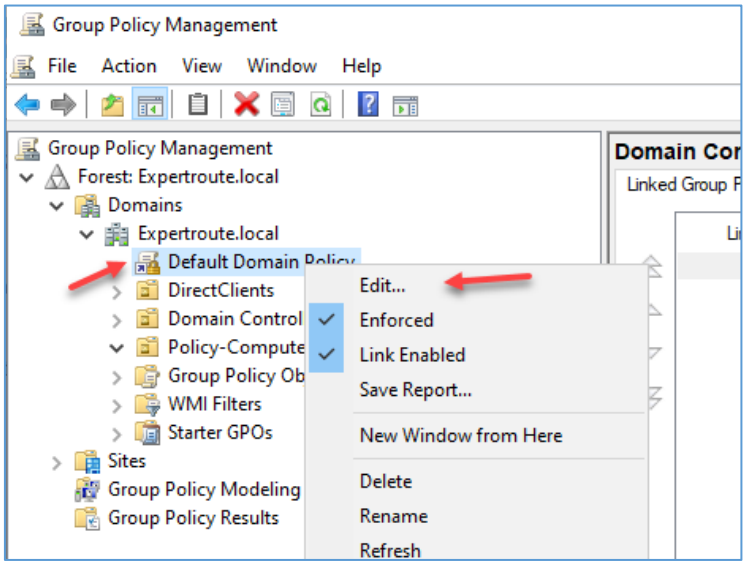
شکل ۸- ۱۲۴۶ غیرفعال کردن Remote Desktop بر روی کلاینت‌ها

www.takbook.com

۷-۳۵-۳-۸ ارسال پیام در شبکه برای کاربران

شما می‌توانید از طریق Group Policy برای کاربران خود پیام ارسال کنید، این پیام زمانی که کاربر قبل از اینکه رمز عبور خود را وارد کند بر روی صفحه نمایش داده می‌شود، برای این کار به صورت زیر عمل می‌کنیم.

به مانند شکل ۸-۱۲۴۷، وارد Group Policy Managemnt شوید و بر روی Default Domain Policy کلیک راست کنید و گزینه‌ی Edit را انتخاب کنید .



شکل ۸- ۱۲۴۷ ارسال پیام در شبکه برای کاربران

وارد آدرس زیر شوید:

Computer Configuration\Windows Settings \Security Settings\Local Policies\Security Options

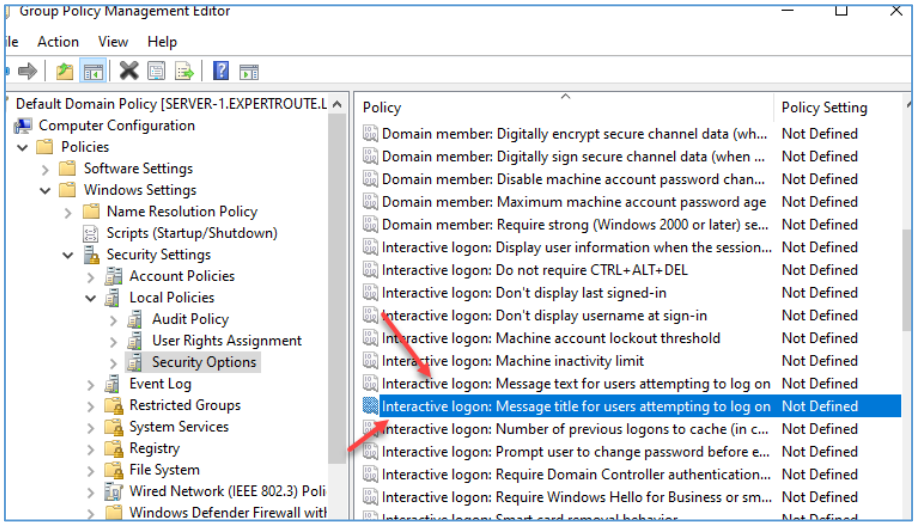
همان‌طور که در شکل ۸-۱۲۴۸، مشاهده می‌کنید دو گزینه با نام‌های زیر وجود دارد:

Interactive logon: Message title for users attempting to log on

Interactive logon: Message text for users attempting to log on

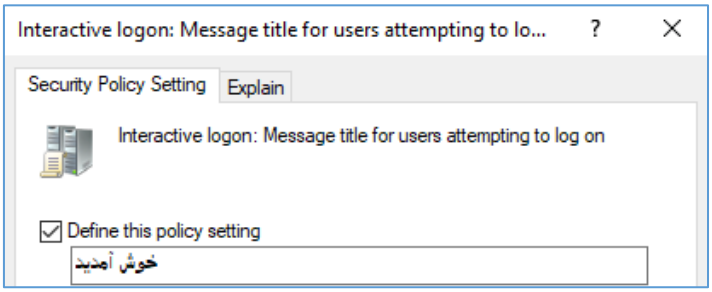
گزینه‌ی Interactive logon: Message title for users attempting to log on مربوط به عنوان پیام است و گزینه‌ی Interactive logon: Message text for users attempting to log on مربوط به متن پیام است که در زیر تغییرات آن را مشاهده می‌کنید.

www.takbook.com



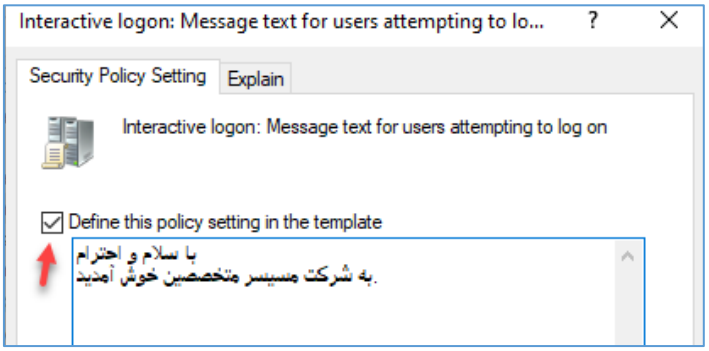
شکل ۸- ۱۲۴۸ ارسال پیام در شبکه برای کاربران

در شکل ۸-۱۲۴۹، باید تیک گزینه‌ی مورد نظر را انتخاب و عنوان خود را وارد کنید:



شکل ۸- ۱۲۴۹ ارسال پیام در شبکه برای کاربران

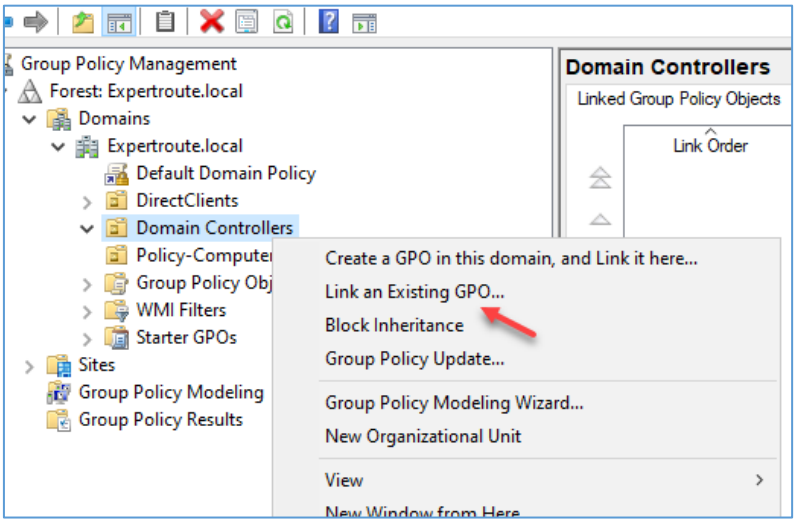
در شکل ۸-۱۲۵۰، باید تیک گزینه‌ی مورد نظر را انتخاب و متن پیام خود را وارد کنید.



شکل ۸- ۱۲۵۰ ارسال پیام در شبکه برای کاربران

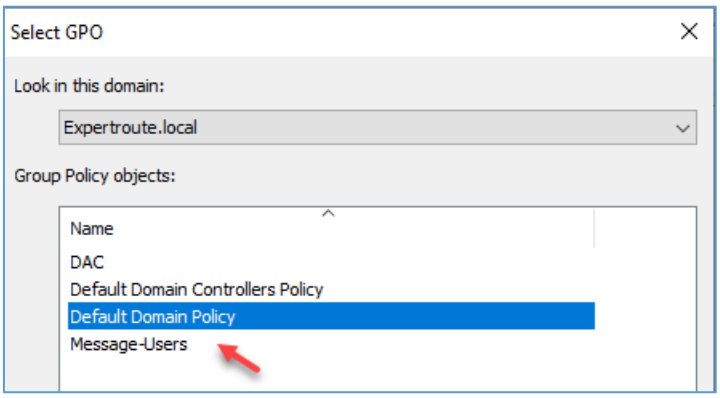
www.takbook.com

در ادامه کار باید Group Policy را برای کاربران و کلاینت‌ها آپدیت کنید برای این کار به مانند شکل ۸-۱۲۵۱، بر روی Domain Controllers کلیک راست کنید و گزینه‌ی Link an Existing GPO را انتخاب کنید.



شکل ۸- ۱۲۵۱ ارسال پیام در شبکه برای کاربران

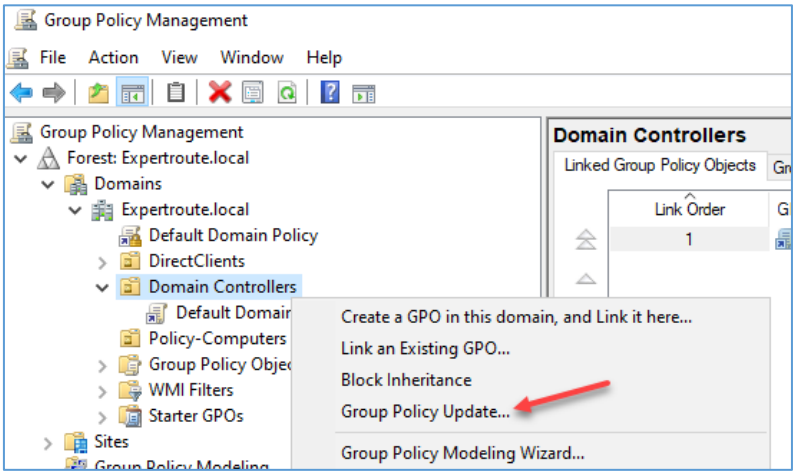
در شکل ۸-۱۲۵۲، Default Domain Policy را انتخاب کنید تا به لیست اضافه شود.



شکل ۸- ۱۲۵۲ ارسال پیام در شبکه برای کاربران

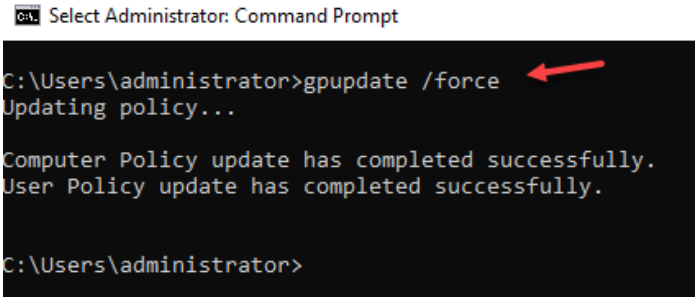
بعد از این کار باید Group Policy را برای کاربرن و کلاینت‌ها آپدیت کنید، به مانند شکل ۸-۱۲۵۳، بر روی Domain Controllers کلیک راست کنید و گزینه‌ی Group Policy Update را انتخاب کنید.

www.takbook.com



شکل ۸- ۱۲۵۳ ارسال پیام در شبکه برای کاربران

در آخر هم به مانند شکل ۸-۱۲۵٤، با دستور gpupdate /force آپدیت نهایی را انجام دهید.



شکل ۸- ۱۲۵۴ ارسال پیام در شبکه برای کاربران

برای اینکه این پیام را مشاهده کنید باید کلاینت مورد نظر خود را ری استارت کنید و قبل از اینکه رمز عبور کاربر را وارد کنید این پیغام به مانند شکل ۸-۱۲۵۵، ظاهر خواهد شد.

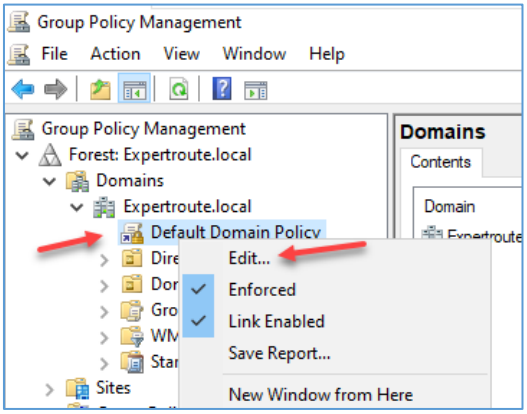


شکل ۸- ۱۲۵۵ ارسال پیام در شبکه برای کاربران

www.takbook.com

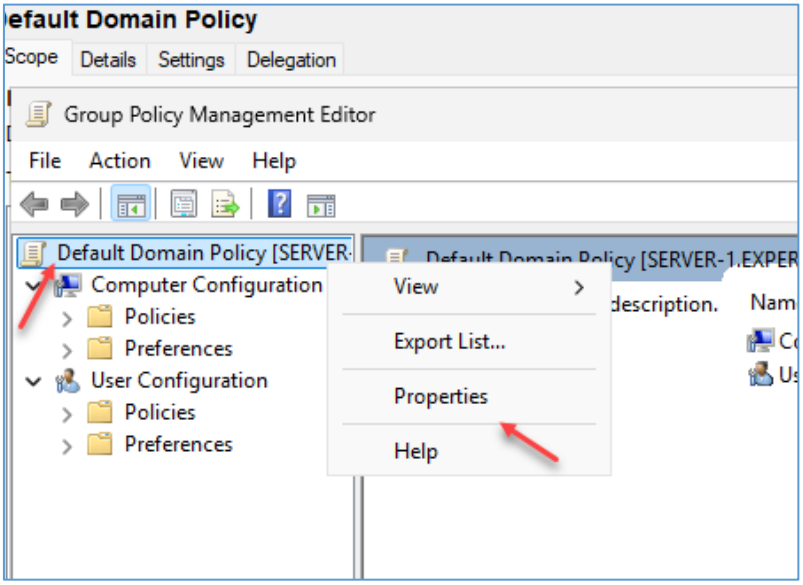
۸-۳-۳۵-۸ غیرفعال کردن تمام تنظیمات انجام شده در Group Policy

برای اینکه تمام تنظیمات اعمال شده روی Group Policy را به صورت سریع غیرفعال کنیم، به مانند شکل ۸-۱۲۵۶، بر روی Default Domain Policy کلیک راست می‌کنیم و گزینه Edit را انتخاب می‌کنیم.



شکل ۸- ۱۲۵۶ غیرفعال کردن تمام تنظیمات انجام شده در Group Policy

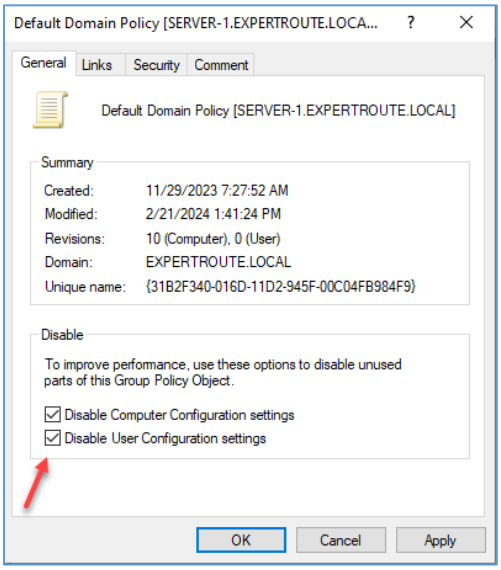
در شکل ۸-۱۲۵۷، بر روی Default Domain Policy کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۱۲۵۷ غیرفعال کردن تمام تنظیمات انجام شده در Group Policy

به مانند شکل ۸-۱۲۵۸، وارد تب General می‌شویم و تیک دو گزینه زیری آن را به مانند شکل انتخاب می‌کنیم و بعد بر روی ok کلیک می‌کنیم، با این کار تمام تنظیمات به حالت اولیه برمی‌گردد.

www.takbook.com



شکل ۸- ۱۲۵۸ *Default Domain Policy*

۹-۳۵-۳-۸ بررسی Processing Order در Group Policy

Processing Order در Group Policy تعیین‌کننده ترتیب اعمال تنظیمات سیاست‌های گروهی (GPOs) بر روی یک کامپیوتر یا کاربر است. در ویندوز، Group Policy بر اساس یک ساختار سلسله‌مراتبی عمل می‌کند و قوانین آن در یک ترتیب مشخص اجرا می‌شود. این ترتیب به شرح زیر است:

Local Group Policy

ابتدا سیاست‌های محلی (Local Group Policy) که روی کامپیوتر ذخیره شده‌اند، اعمال می‌شوند، اگر تنظیمی در این سطح تعریف شده باشد و در سطح بالاتر سیاستی خلاف آن وجود نداشته باشد، این تنظیم باقی می‌ماند.

Site Group Policy

GPOهایی که به یک سایت در Active Directory اعمال شده‌اند، پس از Local Policy اجرا می‌شوند، این سیاست‌ها برای تمام کامپیوترها و کاربران در محدوده آن سایت تأثیرگذار هستند، در صورت وجود چند GPO در این سطح، ترتیب اعمال آن‌ها توسط اولویت تعیین‌شده در کنسول مدیریت GPO مشخص می‌شود.

Domain Group Policy

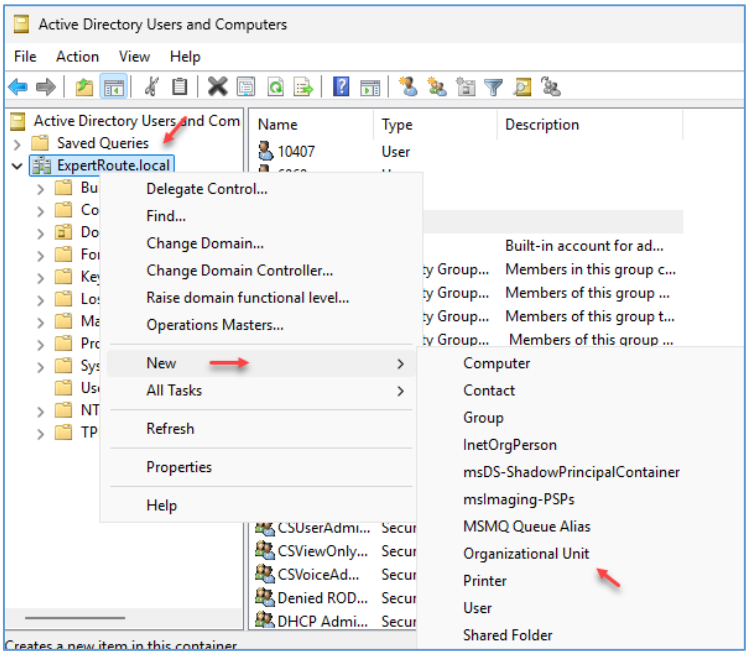
GPOهایی که به دامین اعمال شده‌اند، بعد از سیاست‌های سایت (Site Group Policy) اجرا می‌شوند، این تنظیمات برای تمام کامپیوترها و کاربران عضو دامین اعمال می‌شوند، اگر تنظیمی در این سطح با تنظیمات قبلی (Site یا Local) تناقض داشته باشد، تنظیمات دامین غالب خواهد بود.

Organizational Unit (OU) Group Policy

www.takbook.com

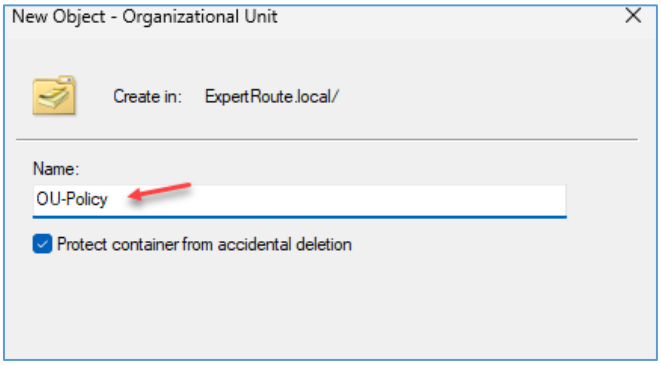
GPOهایی که به یک OU (Organizational Unit) اعمال شده‌اند، در آخرین مرحله اجرا می‌شوند، در صورت وجود چند OU در ساختار سلسله‌مراتبی (مثلاً OUهای فرزند)، GPOها از بالاترین سطح OU به پایین‌ترین سطح اعمال می‌شوند.

برای اینکه این موضوع را تست بگیریم می‌خواهیم دو عکس را برای یک کاربر با اولویت‌های مختلف در Background سیستم او قرار دهیم، برای این کار به مانند شکل ۸-۱۲۵۹، یک OU ایجاد میکنیم، برای این کار بر روی نام دومین خود کلیک راست کنید و از قسمت New گزینه‌ی OU را انتخاب کنید.



شکل ۸- ۱۲۵۹ اولویت‌بندی در Group Policy

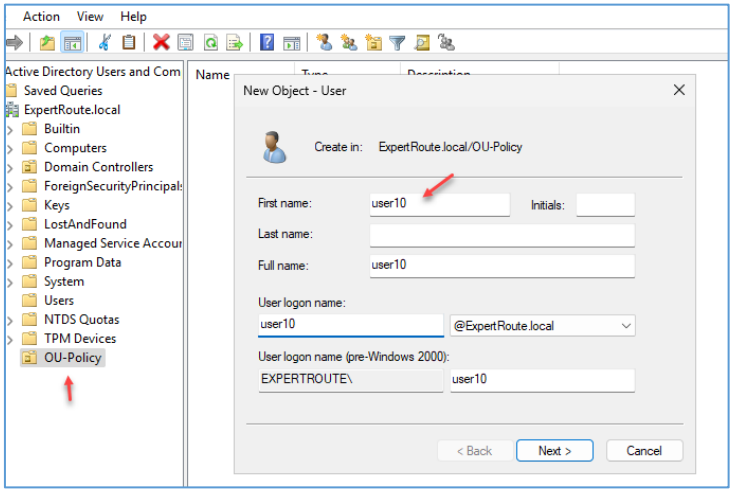
یک OU با نام OU-Policy ایجاد می‌کنیم که این موضوع را در شکل ۸-۱۲۶۰، مشاهده می‌کنید.



شکل ۸- ۱۲۶۰ اولویت‌بندی در Group Policy

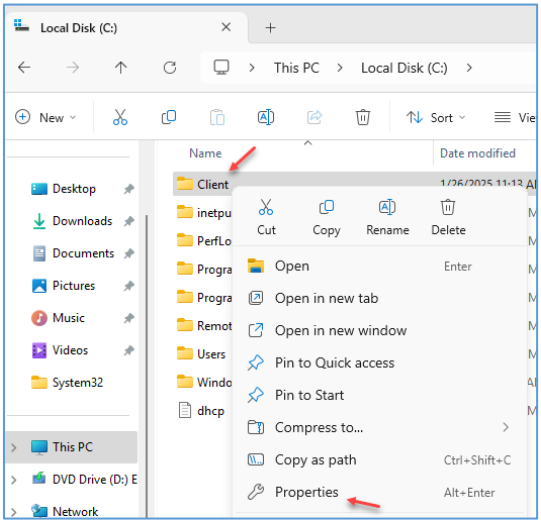
www.takbook.com

در ادامه کار به مانند شکل ۸-۱۲۶۱، یک کاربر جدید با نام user10 در زیر مجموعه‌ی OU مورد نظر ایجاد می‌کنیم.



شکل ۸- ۱۲۶۱ اولویت‌بندی در Group Policy

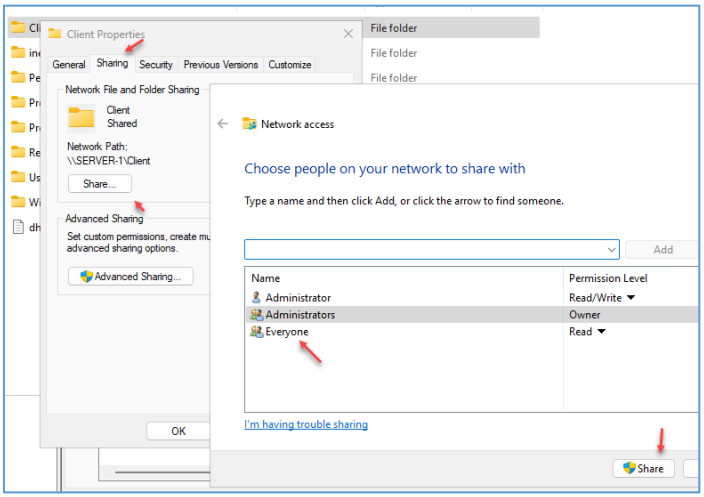
در ادامه کار دو عکس را باید آماده کنیم تا برای کاربر مورد نظر در Background سیستم او با اولویتی که مشخص می‌کنیم قرار دهیم، اول از همه یک فولدر به مانند شکل ۸-۱۲۶۲، ایجاد و بر روی آن کلیک راست می‌کنیم و وارد Properties می‌شویم.



شکل ۸- ۱۲۶۲ اولویت‌بندی در Group Policy

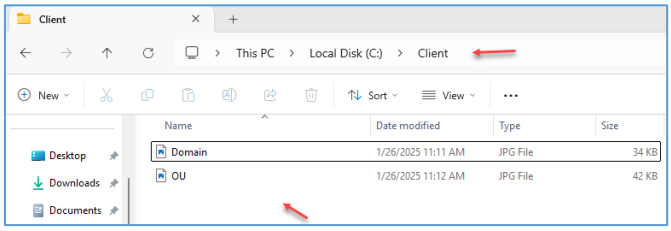
www.takbook.com

در شکل ۸-۱۲۶۳، باید وارد تب Sharing شوید و این پوشه را برای گروه Everyone به اشتراک بگذارید.



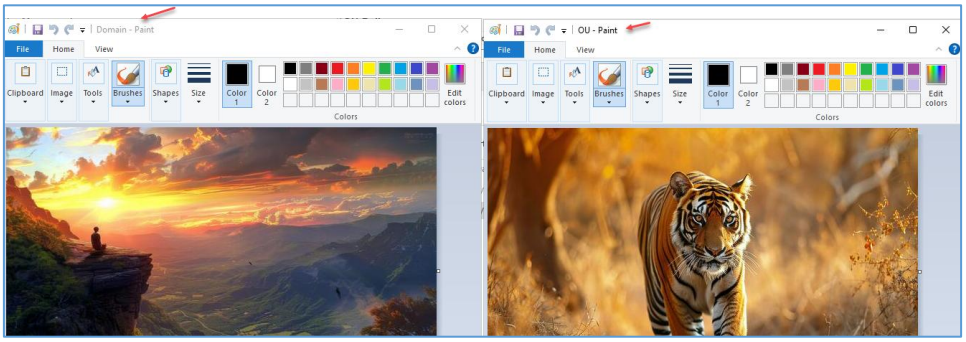
شکل ۸- ۱۲۶۳ اولویت‌بندی در Group Policy

باید دو عکس را به مانند شکل ۸-۱۲۶۴، داخل پوشه قرار دهیم تا بتوانیم به سرویس Group Policy معرفی کنیم.



شکل ۸- ۱۲۶۴ اولویت‌بندی در Group Policy

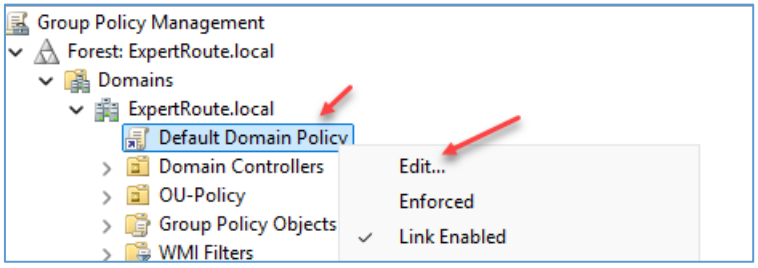
در شکل ۸-۱۲۶۵، هر دو عکس باز شده و مشخص شده است.



شکل ۸- ۱۲۶۵ اولویت‌بندی در Group Policy

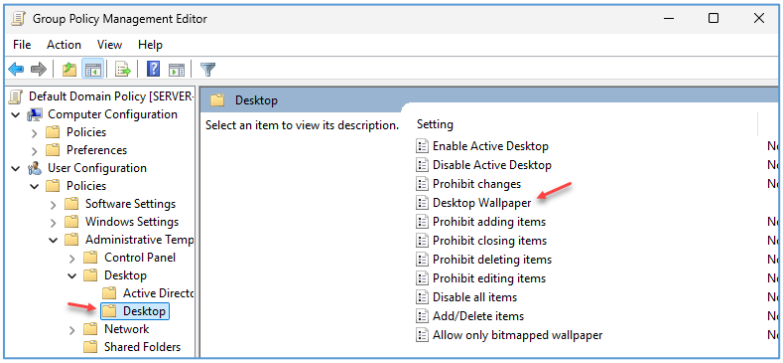
www.takbook.com

بعد از انجام مراحل بالا وارد سرویس Group Policy می‌شویم و به مانند شکل ۸–۱۲۶۶، بر روی Default Domain Policy کلیک راست کنید و بر روی Edit کلیک کنید.



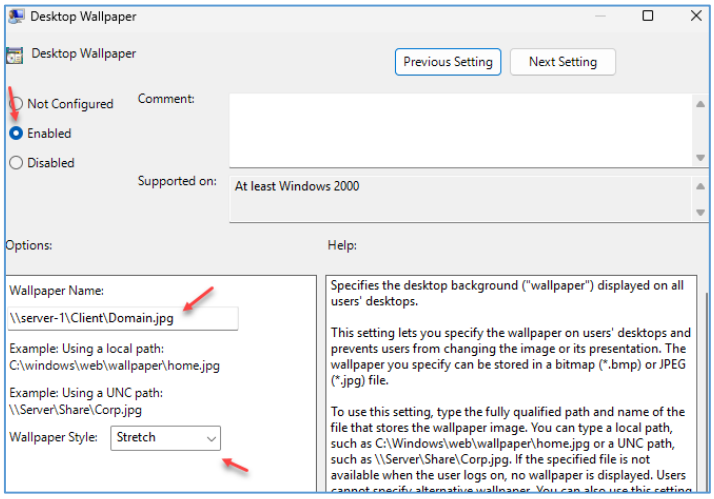
شکل ۸- ۱۲۶۶ اولویت‌بندی در Group Policy

به مانند شکل ۸–۱۲۶۷، وارد مسیر زیر شوید و بر روی Desktop Walpaper دو بار کلیک کنید.



شکل ۸- ۱۲۶۷ اولویت‌بندی در Group Policy

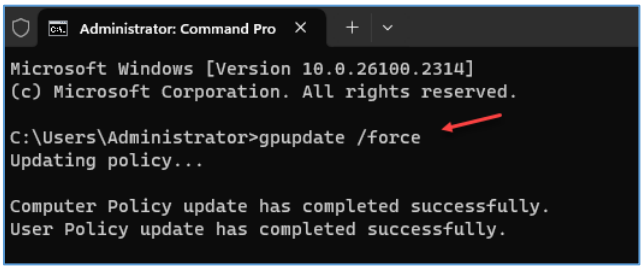
در شکل ۸–۱۲۶۸، باید گزینه‌ی Enable را انتخاب و مسیر عکس مربوط به Domain را وارد کنید.



شکل ۸- ۱۲۶۸ اولویت‌بندی در Group Policy

www.takbook.com

بعد از انجام تغییرات در Group policy به مانند شکل ۸–۱۲۶۹، با استفاده از دستور Gpupdate /force یک بار دیگر تنظیمات را برای کلاینت‌ها Update کنید.



شکل ۸- ۱۲۶۹ اولویت‌بندی در Group Policy

در ادامه به مانند شکل ۸–۱۲۷۰، با کاربر User-1 وارد یکی از کلاینت‌های می‌شویم که همان‌طور مشاهده می‌کنید Background سیستم کاربر به عکس Domain تغییر کرده است.

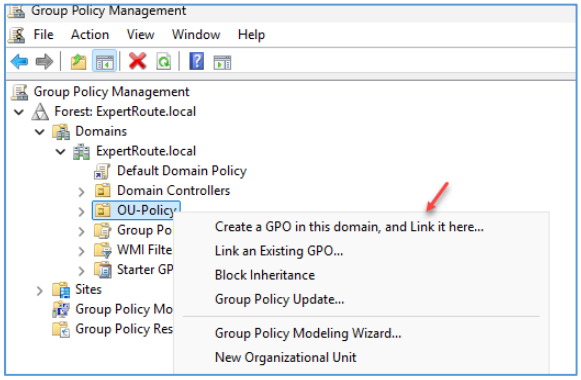


شکل ۸- ۱۲۷۰ اولویت‌بندی در Group Policy

حالا برای اینکه متوجه شویم الویت‌بندی به چه صورت کار می‌کند می‌خواهیم عکس دوم را بر روی OU که ایجاد کردیم و کاربر User-1 را در آن قرار دادیم فعال کنیم، به مانند شکل ۸–۱۲۷۱، وارد Group Policy

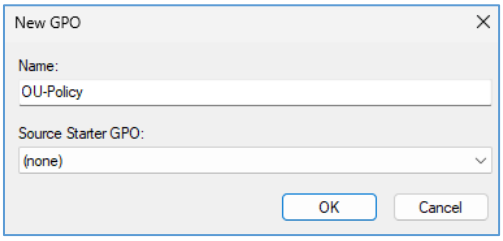
www.takbook.com

می‌شویم و بر روی OU که با هم ایجاد کرده بودیم کلیک راست می‌کنیم و گزینه‌ی Create a GPO… را انتخاب کنید تا یک object جدید برای این OU ایجاد شود.



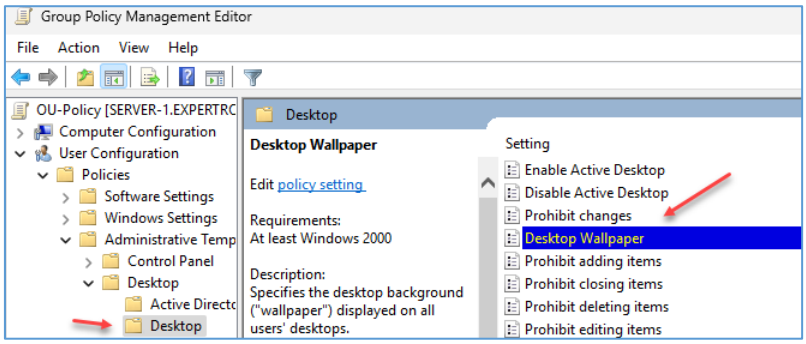
شکل ۸- ۱۲۷۱ اولویت‌بندی در *Group Policy*

به مانند شکل ۸-۱۲۷۲، یک نام برای این Object وارد کنید، با این کار OU مورد نظر به این GPO لینک شده است و هر تغییری بدهیم در زیر مجموعه‌ی OU تغییر می‌کند.



شکل ۸- ۱۲۷۲ اولویت‌بندی در *Group Policy*

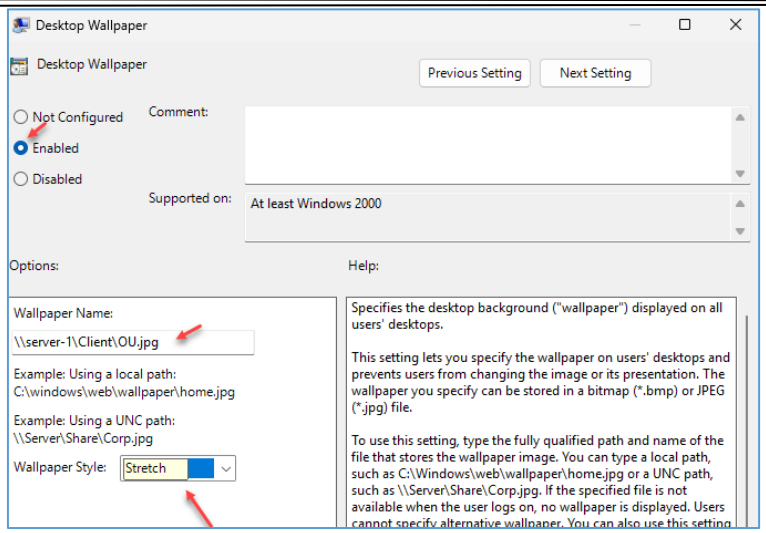
به مانند شکل ۸-۱۲۷۳، وارد مسیر مشخص شده شوید و بر روی Desktop Wallpaper دو بار کلیک کنید.



شکل ۸- ۱۲۷۳ اولویت‌بندی در *Group Policy*

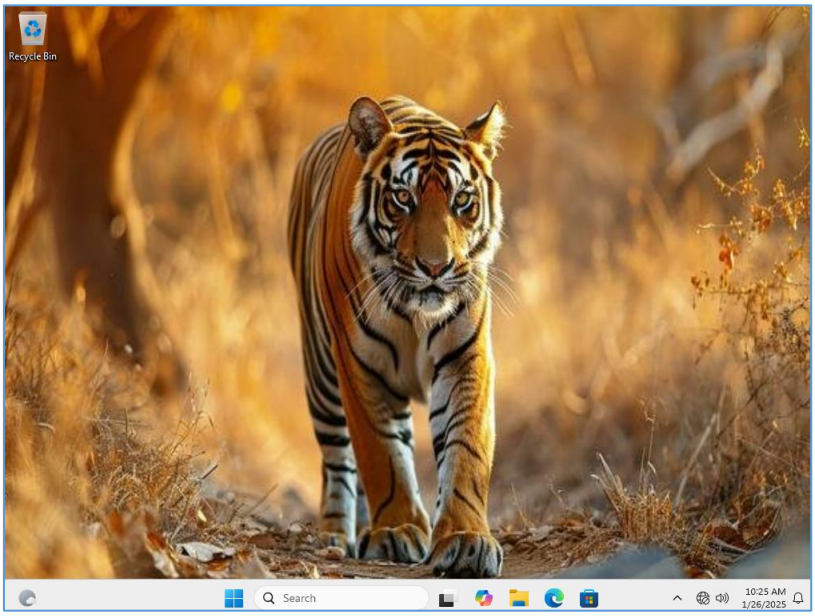
به مانند شکل ۸-۱۲۷٤، گزینه‌ی Enable را انتخاب کنید و مسیر عکس مربوط به OU را وارد کنید و گزینه‌ی Stretch را وارد کنید تا عکس بزرگ شود.

www.takbook.com



شکل ۸- ۱۲۷۴ اولویت‌بندی در Group Policy

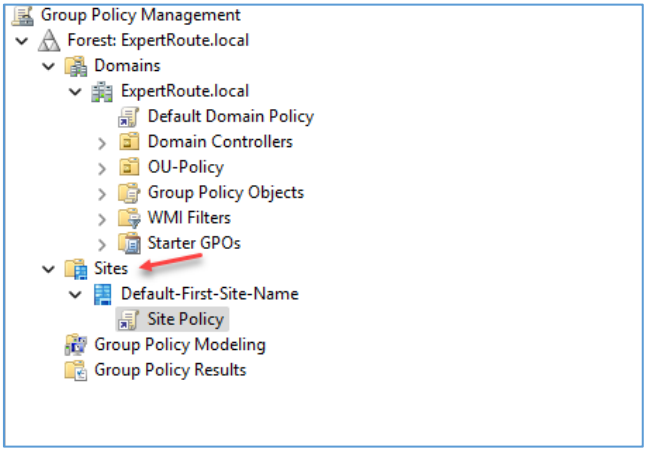
حالا اگر دوباره از کاربر قبلی خارج شویم و دوباره وارد ویندوز شویم به مانند شکل ۸-۱۲۷۵، مشاهده خواهید کرد که عکس مورد نظر تغییر کرده است و این نشان دهنده‌ی این است که اولویت OU بالاتر از دومین است و شما می‌توانید برای واحدهای محتلف خود OUهای مختلف ایجاد کنید و برای هر کدام از واحدها سیاست‌های مشخص را تنظیم کنید.



شکل ۸- ۱۲۷۵ اولویت‌بندی در Group Policy

www.takbook.com

به این نکته توجه کنید که اگر به مانند شکل ۸-۱۲۷۶، در قسمت Sites سیاست GPO را تعریف کنید روی تمام دومینها و زیر مجموعه‌ی آن تاثیرگذار است.

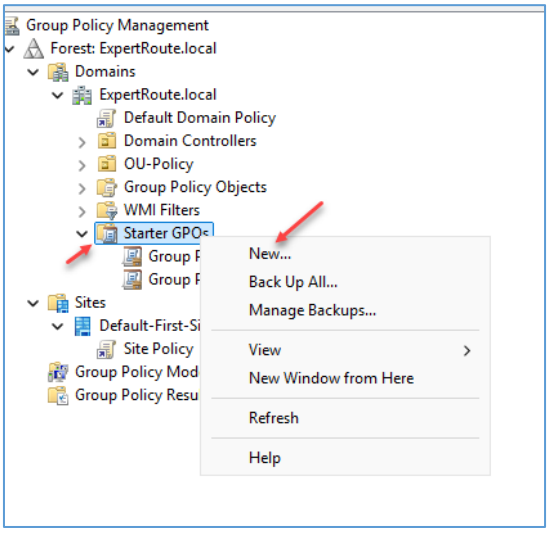


شکل ۸- ۱۲۷۶ اولویت‌بندی در Group Policy

۸-۳-۳۵-۱۰ بررسی Starter GPO

Starter GPO در Group Policy یک قالب (Template) از پیش‌تنظیم‌شده است که می‌توانید برای ایجاد GPOهای جدید از آن استفاده کنید. این ویژگی کمک می‌کند تنظیمات موردنظر خود را از قبل تعریف کرده و هنگام ایجاد GPOهای جدید، زمان کمتری صرف تنظیمات پایه کنید.

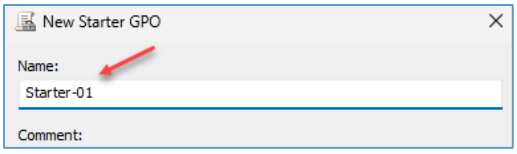
برای تست این موضوع به مانند شکل ۸-۱۲۷۷، وارد Group policy شوید و بر روی Starter GPOs کلیک راست کنید و گزینه‌ی New را انتخاب کنید.



شکل ۸- ۱۲۷۷ بررسی Starter GPO

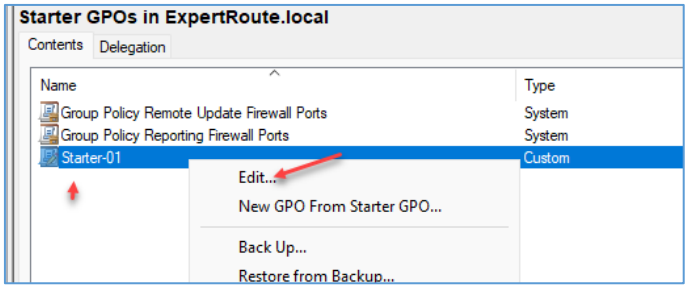
www.takbook.com

در ادامه کار به مانند شکل ۸–۱۲۷۸، یک نام به دلخواه وارد کنید.



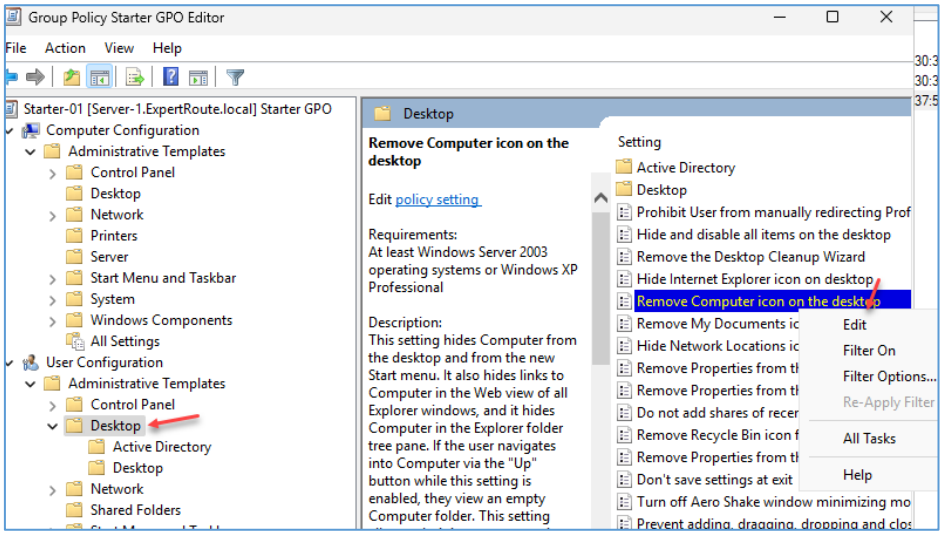
شکل ۸– ۱۲۷۸ بررسی *Starter GPO*

بعد از ایجاد به مانند شکل ۸–۱۲۷۹، بر روی آن کلیک راست کنید و گزینه‌ی Edit را انتخاب کنید.



شکل ۸– ۱۲۷۹ بررسی *Starter GPO*

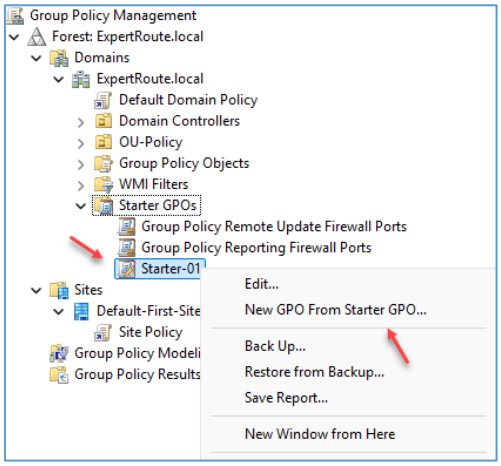
برای اینکه یک تغییری در این Starter که به عنوان Template است ایجاد کنیم به مانند شکل ۸–۱۲۸۰، وارد آدرس مورد نظر می‌شویم و بر روی گزینه‌ی Remove Computer icon on the desktop کلیک راست می‌کنیم و وارد Edit می‌شویم و در ادامه گزینه‌ی Enable را انتخاب می‌کنیم تا فعال شود.



شکل ۸– ۱۲۸۰ بررسی *Starter GPO*

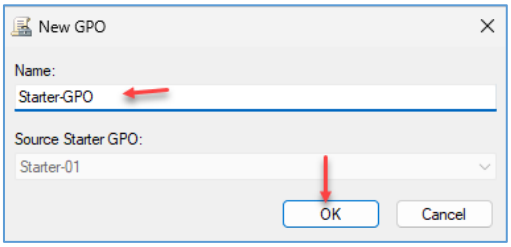
www.takbook.com

در ادامه کار برای اینکه از این Starter استفاده کنیم باید یک GPO جدید با این Template ایجاد کنیم، برای این کار به مانند شکل ۸-۱۲۸۱، بر روی Starter ایجاد شده کلیک راست کنید و گزینه‌ی New GPO... را انتخاب کنید.



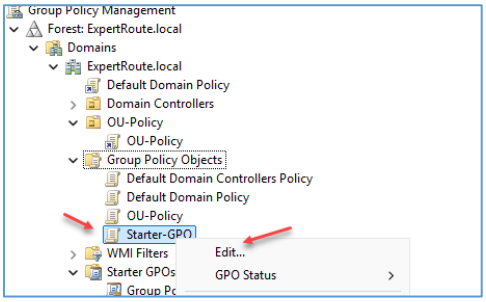
شکل ۸- ۱۲۸۱ بررسی Starter GPO

در شکل ۸-۱۲۸۲، یک نام به دلخواه وارد کنید.



شکل ۸- ۱۲۸۲ بررسی Starter GPO

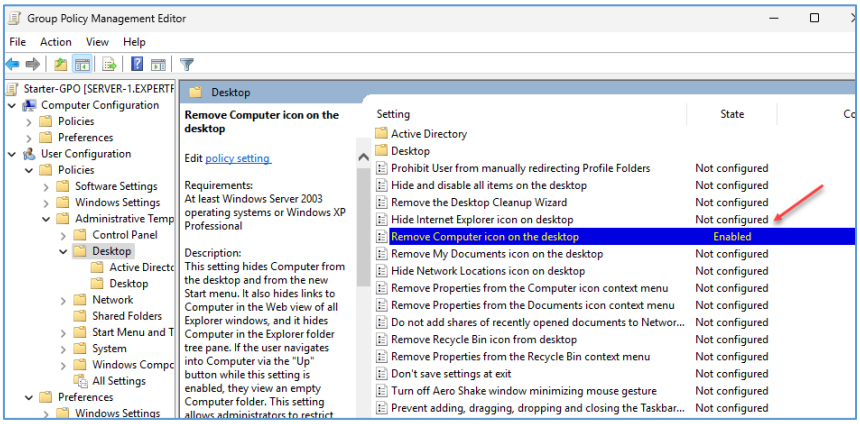
حالا به مانند شکل ۸-۱۲۸۳، باید بر روی GPO جدید کلیک راست کنید و گزینه‌ی Edit را انتخاب کنید.



شکل ۸- ۱۲۸۳ بررسی Starter GPO

www.takbook.com

همان‌طور که در شکل ۸–۱۲۸٤، مشاهده می‌کنید تغییراتی که در Starter ایجاد کردیم به این GPO منتقل شده است و به این روش می‌توانید تنظیمات متفاوت در Templateهای متفاوت انجام دهید و از آنها در GPO استفاده کنید.



شکل ۸- ۱۲۸۴ بررسی Starter GPO

۸–۳–۳۵–۱۱ بررسی و کار با WMI Filtering

WMI Filtering در Group Policy ابزاری قدرتمند است که به شما امکان می‌دهد GPOها را فقط بر اساس شرایط خاصی اعمال کنید. این شرایط با استفاده از کوئری‌های WMI (Windows Management Instrumentation) تعریف می‌شوند. برای مثال، می‌توانید سیاستی را فقط برای کامپیوترهایی با سیستم‌عامل خاص، مقدار RAM مشخص یا نام خاص اعمال کنید.

برا انجام این کار باید Query نویسی را بلد باشید، مثلاً با استفاده از Query زیر سیستم‌عامل‌هایی که ویندوز ۱۰ هستند انتخاب می‌شوند و آن سیسات بر روی آنها اعمال می‌شود.

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.%" AND ProductType = "1"
```

در دستور بالا به ما اعلام می‌کند که به دنبال سیستم‌عامل ویندوز بگرد (Win32_OperatingSystem) و ورژن آن با .10 شروع شود، یعنی سیستم‌عامل ویندوز 10 به بعد، در جدول ۸–۵، دقیقاً ورژن هر ویندوز مشخص شده است.

جدول ۸- ۵ ورژن ویندوز

سیستم‌عامل	شماره‌ی ورژن
Windows 11	10.0*
Windows 10	10.0*
Windows Server 2022	10.0*
Windows Server 2019	10.0*
Windows Server 2016	10.0*
Windows 8.1	6.3*

www.takbook.com

سیستم‌عامل	شماره‌ی ورژن
Windows Server 2012 R2	6.3*
Windows 8	6.2
Windows Server 2012	6.2
Windows 7	6.1
Windows Server 2008 R2	6.1
Windows Server 2008	6.0
Windows Vista	6.0
Windows Server 2003 R2	5.2
Windows Server 2003	5.2
Windows XP 64-Bit Edition	5.2
Windows XP	5.1
Windows 2000	5.0

در دستور قبلی ProductType هم وجود داشت که به این موضوع اشاه دارد که اگر ProductType برابر با یک باشد یعنی ویندوز کلاینتی مانند ویندوز ۷،۸،۱۰،۱۱ و اگر ProductType برابر با دو باشد یعنی ویندوز از نوع سرور است که بر روی آن دومین کنترلر نصب شده است و در آخر اگر ProductType برابر با سه باشد یعنی ویندوز از نوع سرور است.

چند مثال را با هم بررسی می‌کنیم:

دستور زیر برای ویندوزهایی است که مقدار رم آنها برابر ٤ گیگابایت است:

```
SELECT * FROM Win32_ComputerSystem WHERE TotalPhysicalMemory >= 4294967296
```

دستور زیر برای اعمال GPO فقط برای کامپیوترهای Windows Server 2019:

```
SELECT * FROM Win32_OperatingSystem WHERE Version = "10.0.17763" AND ProductType = "3"
```

دستور زیر برای اعمال GPO برای کامپیوترهای متصل به نام خاصی از دامین:

```
SELECT * FROM Win32_ComputerSystem WHERE Domain = "example.com"
```

دستور زیر برای اعمال GPO فقط برای کامپیوترهایی با پردازنده ٦٤ بیتی:

```
SELECT * FROM Win32_Processor WHERE AddressWidth = "64"
```

دستور زیر برای اعمال GPO روی کامپیوترهایی با نام خاص در دامین:

```
SELECT * FROM Win32_ComputerSystem WHERE Name LIKE "PC-%"
```

دستور زیر برای اعمال GPO فقط روی کامپیوترهایی با برند خاص (مانند Dell):

```
SELECT * FROM Win32_ComputerSystem WHERE Manufacturer = "Dell Inc."
```

دستور زیر برای اعمال GPO برای لپ‌تاپ‌ها (دارای باتری):

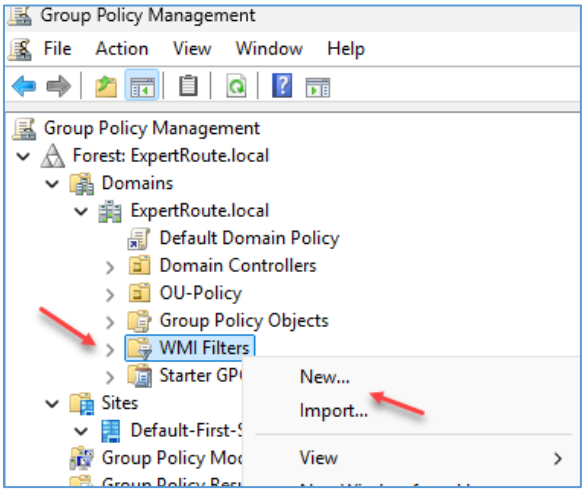
```
SELECT * FROM Win32_Battery
```

www.takbook.com

دستور برای اعمال GPO روی کامپیوترهایی با فضای دیسک بیشتر از ۱۰۰ گیگابایت:

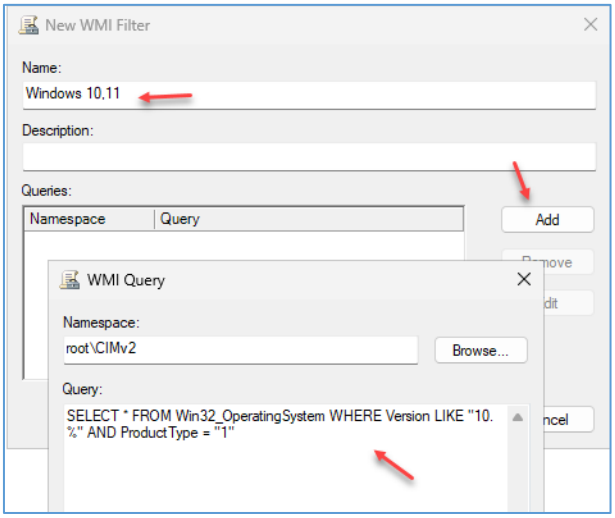
```
SELECT * FROM Win32_LogicalDisk WHERE FreeSpace >= 107374182400 AND DriveType = "3"
```

برای اینکه یک مثال را با هم بررسی کنیم، به مانند شکل ۸-۱۲۸۵، بر روی WMI Filters کلیک راست کنید و گزینه‌ی New را انتخاب کنید.



شکل ۸- ۱۲۸۵ بررسی و کار با WMI Filtering

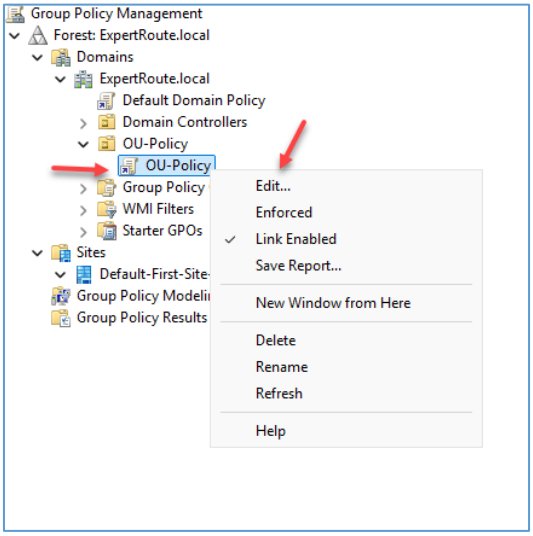
در ادامه کار به مانند شکل ۸-۱۲۸۶، بر روی Add کلیک کنید و کد مورد نظر را در آن قرار دهید، این کد کلاینت‌هایی که سیستم‌عامل آنها از ویندوز ۱۰ به بالا باشد را انتخاب می‌کند و GPO مورد نظر بر روی آنها اعمال می‌شود.



شکل ۸- ۱۲۸۶ بررسی و کار با WMI Filtering

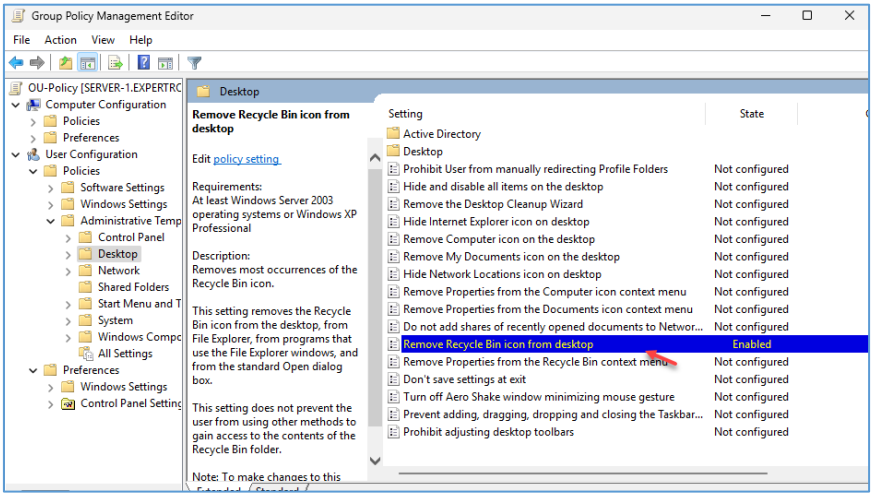
www.takbook.com

در ادامه و به مانند شکل ۸-۱۲۸۷، بر روی GPO که قبلاً برای OU خود ایجاد کرده بودیم کلیک راست می‌کنیم و گزینه‌ی Edit را انتخاب می‌کنیم.



شکل ۸- ۱۲۸۷ بررسی و کار با WMI Filtering

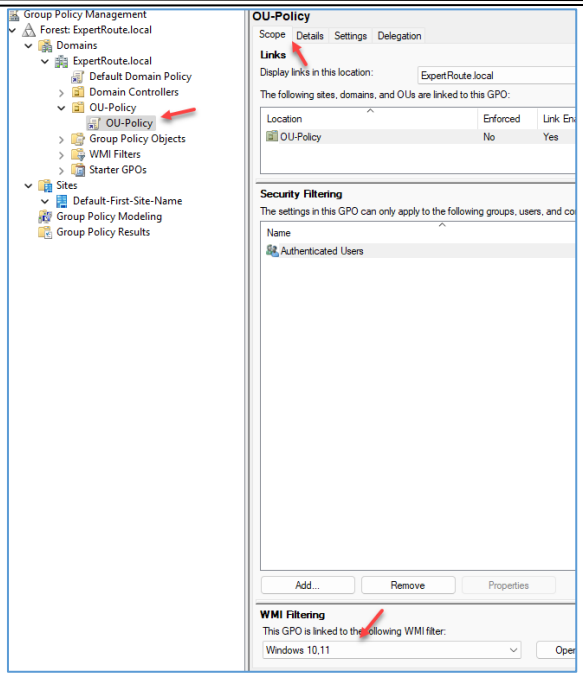
به مانند شکل ۸-۱۲۸۸، یکی از گزینه‌ها را فعال می‌کنیم.



شکل ۸- ۱۲۸۸ بررسی و کار با WMI Filtering

در نهایت به مانند شکل ۸-۱۲۸۹، بر روی OU مورد نظر کلیک کنید و از تب Scope باید همان WMI را که با هم ایجاد کردیم را انتخاب کنید و بر روی OK کلیک کنید تا تنظیمات اعمال شود و چون کلاینت ما دارای ویندوز ۱۱ است این تغییر بر روی آن اعمال خواهد شد.

www.takbook.com

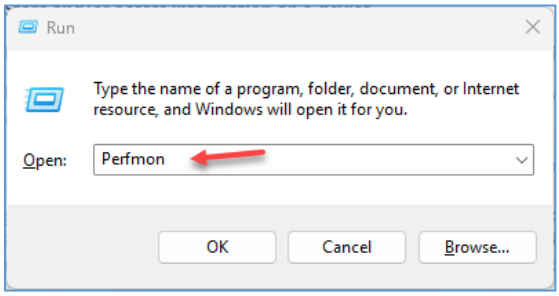


شکل ۸- ۱۲۸۹ بررسی و کار با WMI Filtering

۸-۳-۳۶ کار با سرویس‌های Monitoring

در ویندوز سرور سرویس‌ها و ابزارهایی وجود دارند که می‌توانیم بر روی تمام اجزای سرور خود از Cpu گرفته تا ارتباط اینترنت، نظارت کامل داشته باشیم، سرویس‌هایی مانند Performance Monitor و Event Viewer وجود دارد.

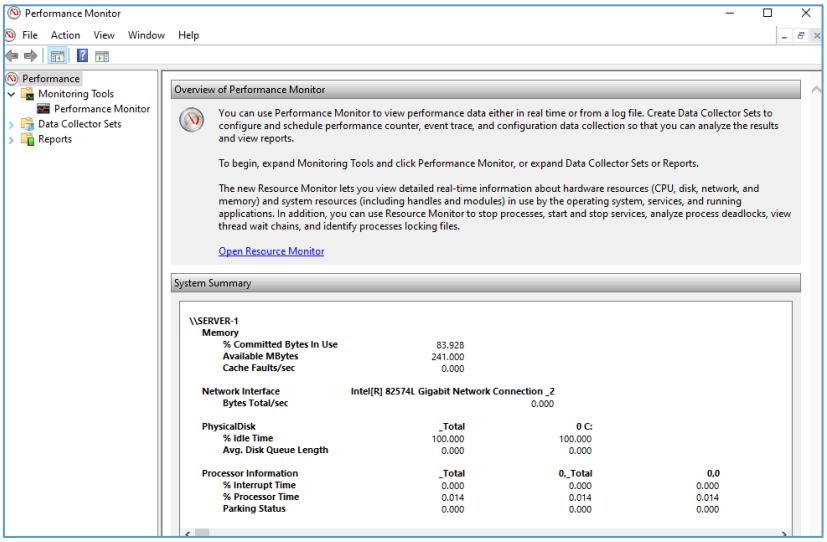
در ابتدا سرویس Performance Monitor را بررسی می‌کنیم، این سرویس به صورت پیش‌فرض بر روی ویندوز سرور نصب است و نیاز به نصب دوباره نیست، برای اجرای این سرویس به مانند شکل ۸-۱۲۹۰، وارد Run شوید و کلمه Perfmon را وارد و بعد اجرا کنید.



شکل ۸- ۱۲۹۰ کار با سرویس‌های Monitoring

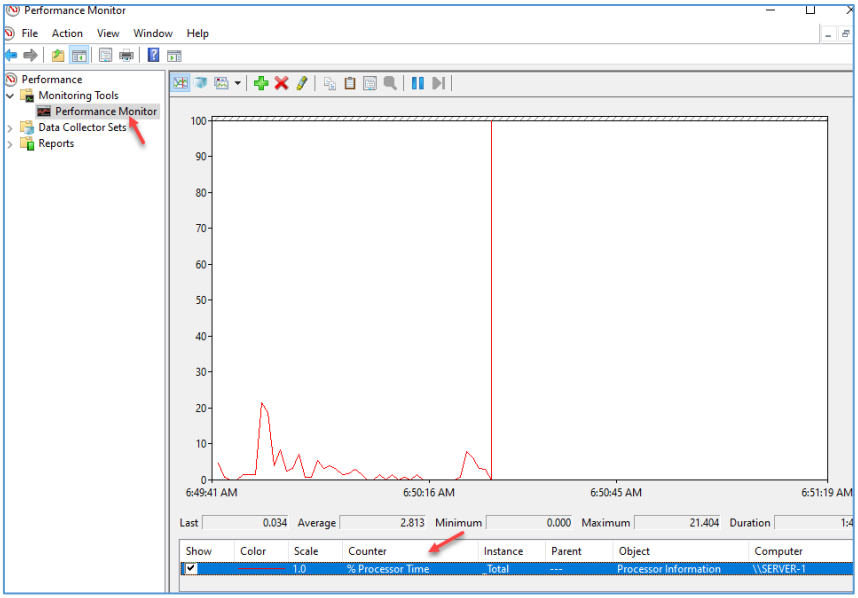
همان‌طور که در شکل ۸-۱۲۹۱، مشاهده می‌کنید سرویس Performance Monitor اجرا شده است.

www.takbook.com



شکل ۸- ۱۲۹۱ کار با سرویس‌های Monitoring

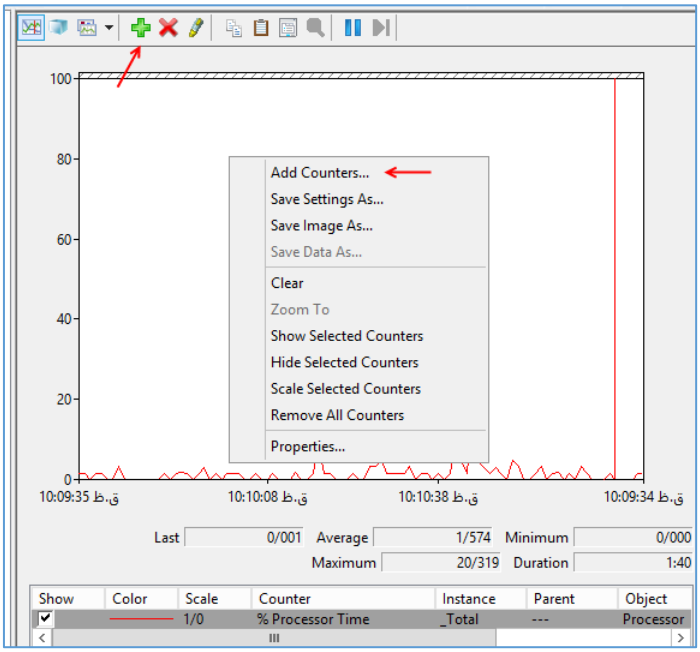
اگر از سمت چپ بر روی Performance Monitor کلیک کنید، به مانند شکل ۸-۱۲۹۲، یک شمارنده مربوط به Processor Time را مشاهده می‌کنید که نشان دهنده‌ی کارکرد CPU می‌باشد.



شکل ۸- ۱۲۹۲ کار با سرویس‌های Monitoring

www.takbook.com

در شکل ۸-۱۲۹۳، می‌خواهیم یک شمارنده جدید به لیست اضافه کنیم تا نحوه‌ی کارکرد آن را بررسی کنیم، برای این کار به مانند شکل در قسمت مشخص‌شده کلیک راست کنید و گزینه Add Counters را انتخاب کنید و یا از نوار ابزار بالا بر روی آیکون + کلیک کنید.



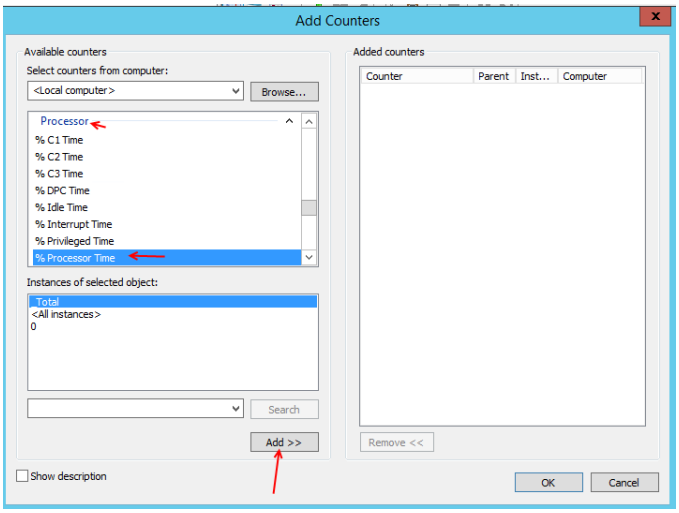
شکل ۸- ۱۲۹۳ کار با سرویس‌های Monitoring

شمارنده‌های مختلفی را می‌توانیم به این لیست اضافه کنیم، به مانند شکل ۸-۱۲۹٤، در این قسمت لیست تمام شمارنده‌های موجود رامشاهده می‌کنید.

مثلاً در این شکل شمارنده Processor خود دارای زیر مجموعه و یا ریز اطلاعات می‌باشد که می‌تواند کل مجموعه و یا یکی از آنها را انتخاب کنید.

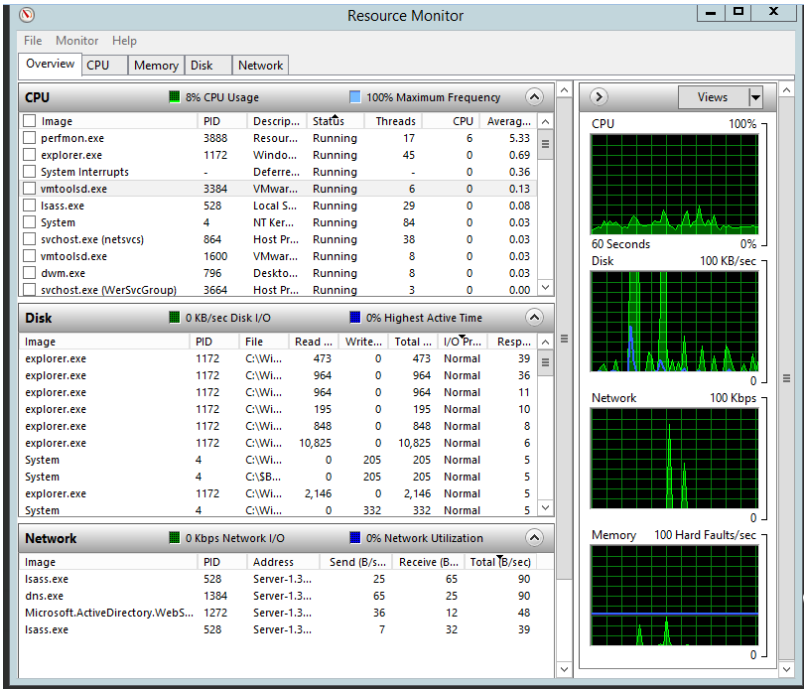
توجه داشته باشید در بالای شکل Local Computer نوشته که نشان دهنده این است که این شمارنده‌ها مربوط به این Computer می‌باشد که می‌توانید با کلیک بر روی Browse کامپیوتر دیگر را به لیست اضافه کنید و اطلاعات و شمارنده های آن را مورد بررسی قرار دهید.

www.takbook.com



شکل ۸- ۱۲۹۴ کار با سرویس‌های *Monitoring*

به مانند شکل ۸-۱۲۹۵، سرویس دیگری با نام Resource Monitor وجود دارد که می‌توانی از طریق Serach آن را اجرا کنید، این سرویس به صورت خلاصه شده کارکرد پردازنده، Ram، Hard شبکه را مانیتور می‌کند، در این سرویس تمام نرم‌افزارها و سرویس‌هایی که از منابع استفاده می‌کنند در این سرویس لیست شده است که کار مانیتورینگ سرور را آسان کرده است.



شکل ۸- ۱۲۹۵ کار با سرویس‌های *Monitoring*

www.takbook.com

۳۷-۳-۸ کار با ویژگی‌های مختلف Domain

در زیر به انواع دامین‌های موجود در اکتیو دایرکتوری مایکروسافت اشاره می‌کنیم و آنها را با یک مثال بررسی خواهیم کرد.

Writeable Domain Controller (WDC)

یک دامین کنترلر معمولی که قابلیت خواندن و نوشتن اطلاعات در دایرکتوری را دارد، و از ویژگی‌های آن می‌توان به ایجاد کاربران جدید، تغییر رمز عبور یا تغییرات Policy از طریق این دامین کنترلر اشاره کرد، معمولاً این دومین کنترلر به عنوان دامین کنترلر اصلی در محیط‌های شبکه استفاده می‌شود.

Read-Only Domain Controller (RODC)

نسخه‌ای از دامین کنترلر که فقط قابلیت خواندن اطلاعات دایرکتوری را دارد، مناسب برای محیط‌هایی با امنیت پایین یا دفاتر راه دور، توجه داشته باشید تغییرات ذخیره نمی‌شوند؛ هر گونه تغییر باید به WDC ارسال شود، اطلاعات حساس مانند رمز عبور کاربران به صورت پیش‌فرض در RODC ذخیره نمی‌شود، مگر اینکه به طور خاص مجاز شده باشد.

Child Domain

دامین‌هایی که زیرمجموعه یک دامین مادر (Parent Domain) هستند و بخشی از ساختار درختی (Tree) اکتیو دایرکتوری را تشکیل می‌دهند، می‌توانند سیاست‌ها و کاربران مستقل داشته باشند، اما همچنان بخشی از Forest دایرکتوری هستند، سازمان‌هایی که نیاز به تقسیم‌بندی بر اساس منطقه جغرافیایی یا واحد سازمانی دارند می‌توانند از این نوع دومین استفاده کنند.

Tree Domain

به دامین‌هایی که یک رابطه سلسله‌مراتبی و ساختاری بین خود دارند و در یک Forest هستند گویند، دامین‌های Tree معمولاً از یک فضای نام متفاوت (DNS Namespace) استفاده می‌کنند، مثلاً اگر دامین اصلی شما example.com باشد، یک دامین Tree می‌تواند subsidiary.com باشد.

Parent Domain

دامین اصلی در سلسله‌مراتب یک Tree که دامین‌های زیرمجموعه (Child Domains) به آن متصل هستند، تمامی Child Domains از Parent Domain ارث‌بری می‌کنند، توجه داشته باشید که کنترل و مدیریت اصلی در Parent Domain انجام می‌شود.

Forest Root Domain

www.takbook.com

اولین دامین در یک Forest که کل ساختار اکتیو دایرکتوری را مدیریت و هدایت می‌کند، تمامی تنظیمات Forest (مانند Schema) در این دامین تعریف و ذخیره می‌شود.

Domain Trusts

ارتباطات (Trusts) بین دو دامین که اجازه می‌دهد کاربران از یک دامین به منابع دامین دیگر دسترسی پیدا کنند.

One-way Trust: دسترسی یک‌طرفه.

Two-way Trust: دسترسی دوطرفه.

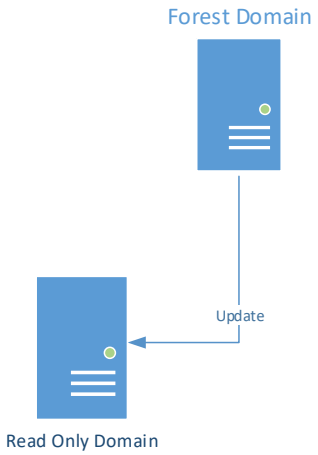
External Trust: ارتباط بین دامین‌های خارج از Forest.

Forest Trust: ارتباط بین Forestهای مختلف.

۳۸-۳-۸ کار با Read Only Domain Controller

کار با سرویس Active Directory یکی از مهمترین بخش‌ها می‌باشد که امنیت آن برای یک شرکت یا سازمان بسیار اهمیت دارد، شما باید به عنوان مدیر شبکه کارهای امنیتی لازم را برای جلوگیری از دسترسی نامعتبر انجام دهید، یکی از راه‌های ایجاد امنیت استفاده از Read Only Domain Controller یا RODC است این یعنی یک دومین کنترلر فقط خواندنی و ایجاد تغییر در آن غیر ممکن است.

دلیل آن این است که این دومین کنترلر زیر مجموعه‌ی دومین کنترلر دیگر است و فقط یک کپی از اطلاعات دومین کنترلر اصلی را در خود نگه می‌دارد و هیچ تغییر را نمی‌تواند به صورت مستقیم در دومین کنترلر اصلی انجام دهد. در کل تغییرات توسط دومین کنترلر اصلی اعمال یا Replicate می‌شود.

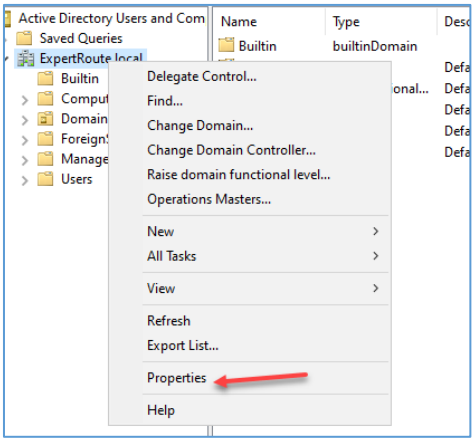


شکل ۸- ۱۲۹۶ *Read Only Domain Controller*

www.takbook.com

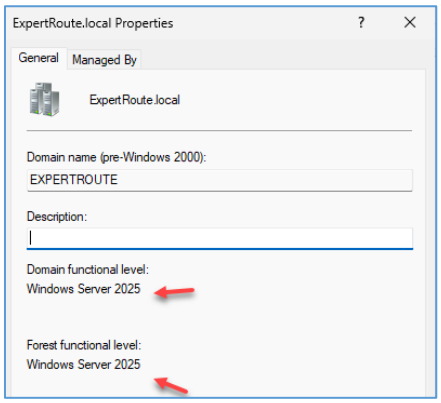
در شکل ۸–۱۲۹۶، سرور Forest سرور اصلی می‌باشد و آپدیت‌ها به صورت یک طرفه (One-way Trust) به سرور Read Only فرستاده می‌شود.

برای شروع کار ما نیاز به یک Domain Controller اصلی داریم که این دومین کنترلر از قبل نصب شده است، مهمترین چیزی که برای شروع باید بدانیم این است که دومین مورد نظر ما تا چه ورژنی از ویندوز سرور را برای این کار پشتیبانی می‌کند برای بررسی این موضوع وارد دومین اصلی خود شوید و در سرویس Active Directory Users and Computers روی سرور کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۱۲۹۷ *Read Only Domain Controller*

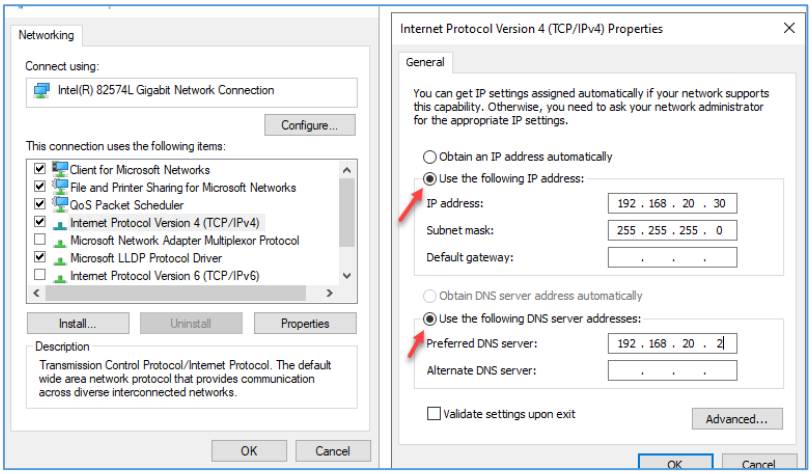
همان‌طور که در شکل ۸–۱۲۹۸، مشاهده می‌کنید پایینترین ورژن ویندوز سروری که این دومین پشتیبانی می‌کند 2025 است و ویندوز سرورهای شما باید بالای 2025 باشد که در ادامه از ویندوز سرور ۲۰۲۵ استفاده می‌کنیم.



شکل ۸- ۱۲۹۸ *Read Only Domain Controller*

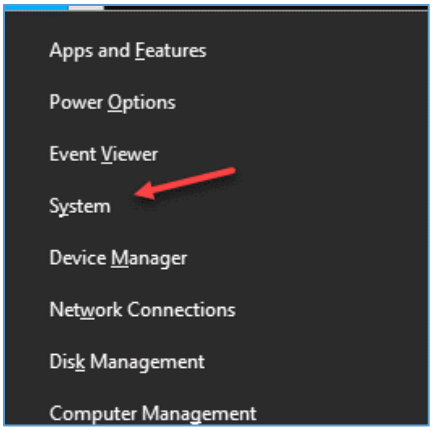
www.takbook.com

در ادامه کار یک سرور جدید فعال و روی آن ویندوز سرور 2025 نصب می‌کنیم و بعد از آن شروع به راه‌اندازی سرویس Read Only Domain Controller می‌کنیم، بعد از ایجاد سرور جدید باید آدرس IP آن را به مانند شکل ۸-۱۲۹۹، به صورت دستی وارد کنید.



شکل ۸- ۱۲۹۹تغییر آدرس IP

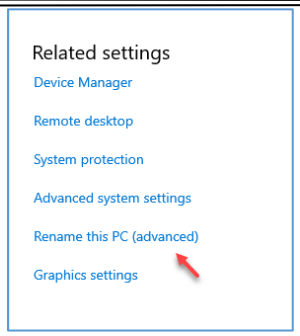
در ادامه بعد از اینکه آدرس IP را مشخص کردید کلید ترکیبی WIN+X را فشار دهید و به مانند شکل ۸-۱۳۰۰، در منوی باز شده گزینه‌ی System را انتخاب کنید.



شکل ۸- ۱۳۰۰ راه‌اندازی Read Only Domain Controller

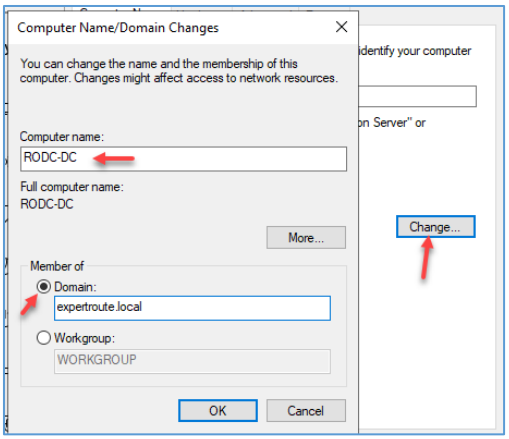
در پنجره باز شده به مانند شکل ۸-۱۳۰۱، بر روی Rename this PC کلیک کنید.

www.takbook.com



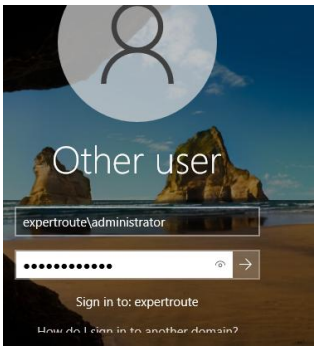
شکل ۸- ۱۳۰۱ *Read Only Domain Controller*

در شکل ۸-۱۳۰۲، بر روی Change کلیک کنید و در صفحه‌ی باز شده نام سرور را به همراه نام دومین وارد و آن را عضو دومین کنید.



شکل ۸- ۱۳۰۲ *تغییر نام سرور و عضو کردن در دومین*

بعد از اینکه عضو دومین شدید به مانند شکل ۸-۱۳۰۳، با کاربر Administrator یا کاربری که دسترسی کامل به شبکه دارد وارد سرور شوید.

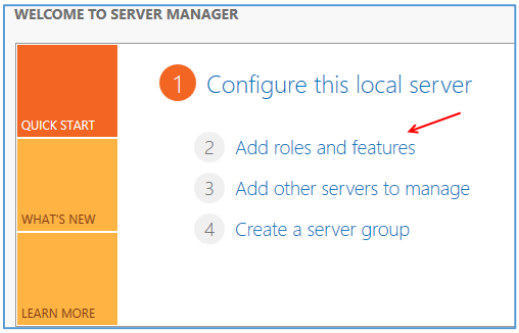


شکل ۸- ۱۳۰۳ *Read Only Domain Controller*

www.takbook.com

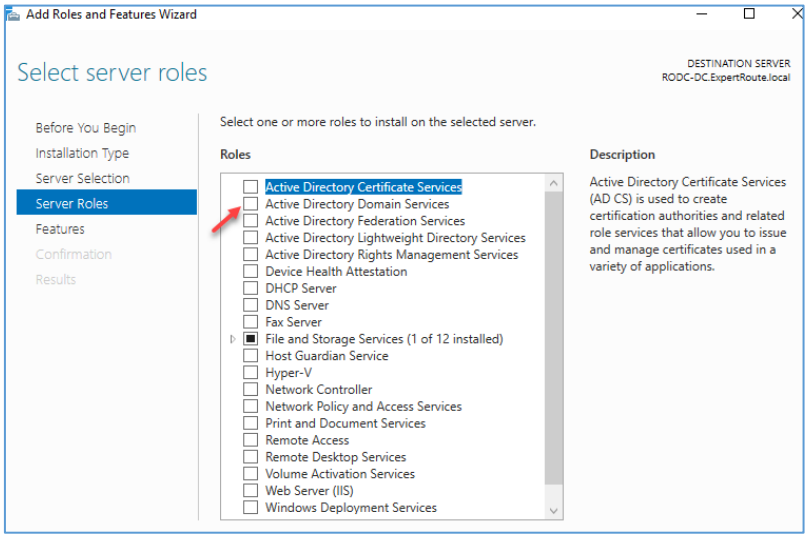
بعد از ورود Server Manager را اجرا کنید و به مانند شکل ۸-۱۳۰٤، بر روی Add roles and features کلیک کنید.

نکته: این سرور زیرمجموعه‌ی دومین اصلی می‌باشد.



شکل ۸- ۱۳۰۴ *Read Only Domain Controller*

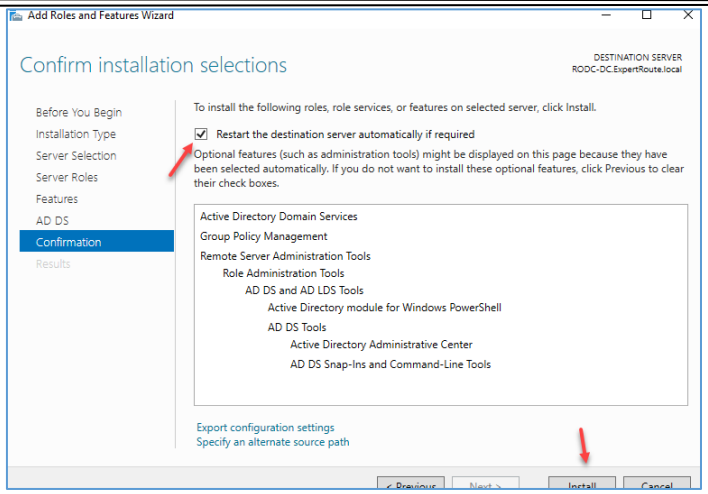
به مانند شکل ۸-۱۳۰۵، در صفحه Server Roles گزینه Active Directory Domain Services را انتخاب کنید و در شکل باز شده بر روی Add Feature کلیک کنید و بعد بر روی Next کلیک کنید تا به صفحه Confirmation برسیم.



شکل ۸- ۱۳۰۵ *Read Only Domain Controller*

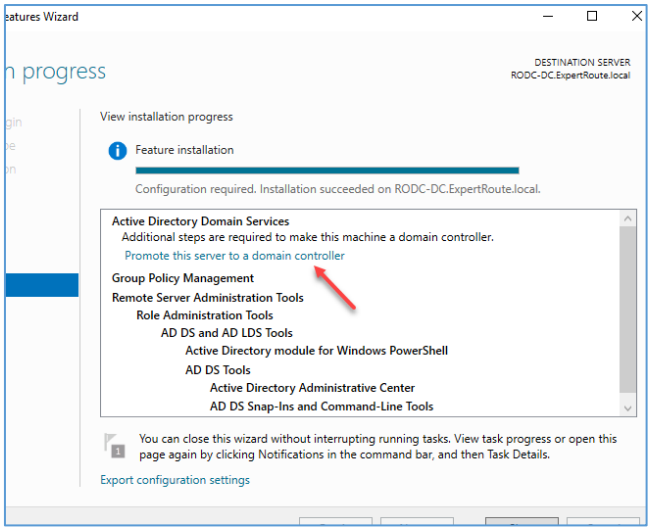
در شکل ۸-۱۳۰٦، برای نصب سرویس بر روی Install کلیک کنید.

www.takbook.com



شکل ۸-۱۳۰۶ *Read Only Domain Controller*

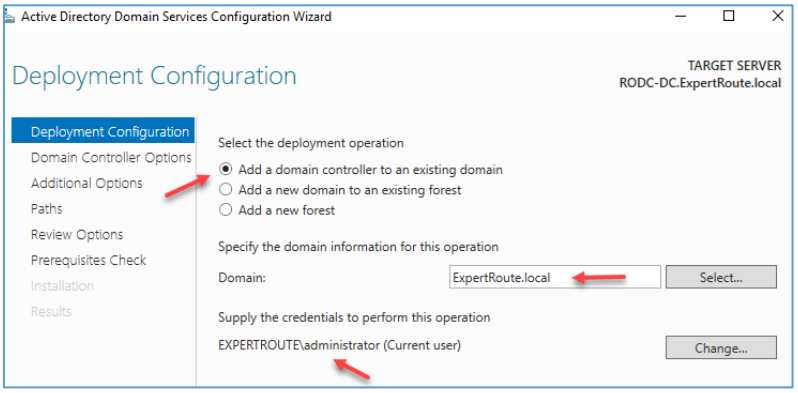
بعد از نصب سرویس، در شکل ۸–۱۳۰۷، بر روی Promote this server to a domain controller کلیک کنید تا تنظیمات RODC را انجام دهیم، RODC همان Read Only Domain Controller است.



شکل ۸-۱۳۰۷ *Read Only Domain Controller*

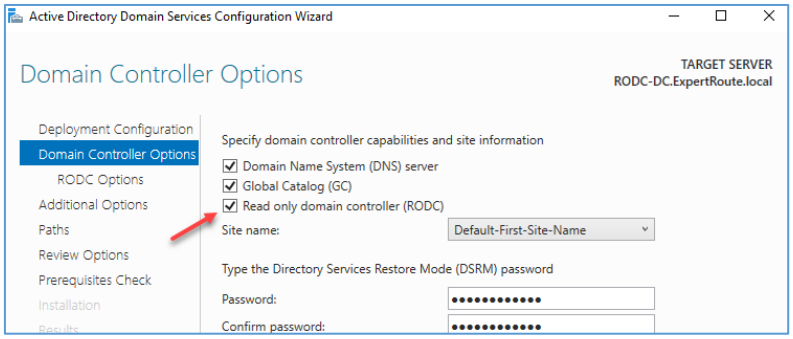
در شکل ۸–۱۳۰۸، گزینه Add a domain controller to an existing domain را انتخاب کنید، همان‌طور که مشاهده می‌کنید دومین Expertroute.local شناسایی شده است، برای ادامه کار بر روی Next کلیک کنید.

www.takbook.com



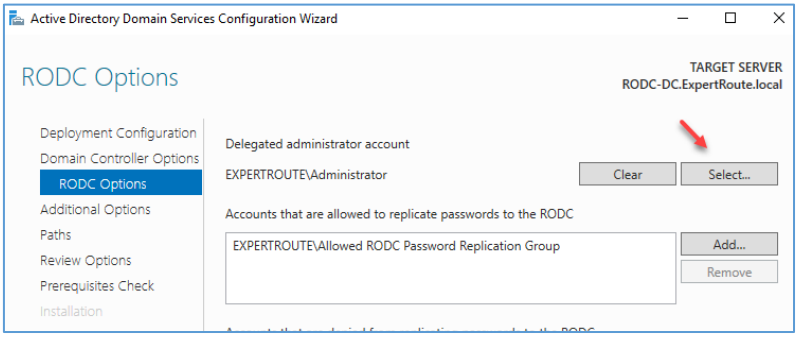
شکل ۸- ۱۳۰۸ *Read Only Domain Controller*

در شکل ۸-۱۳۰۹، مهمترین کار انتخاب گزینه Read Only domain Controller است و بعد یک رمز برای Restore Mode می‌باشد.



شکل ۸- ۱۳۰۹ *Read Only Domain Controller*

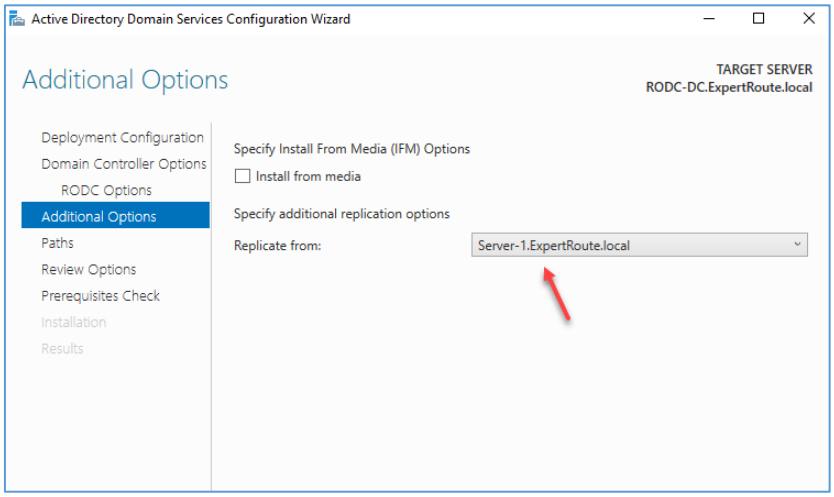
در شکل ۸-۱۳۱۰، می‌توانید با کلیک بر روی Select گروه یا کاربر مورد نظر خود را اضافه کنید تا دسترسی به این سرویس داشته باشد و بعد بر روی Next کلیک کنید.



شکل ۸- ۱۳۱۰ *Read Only Domain Controller*

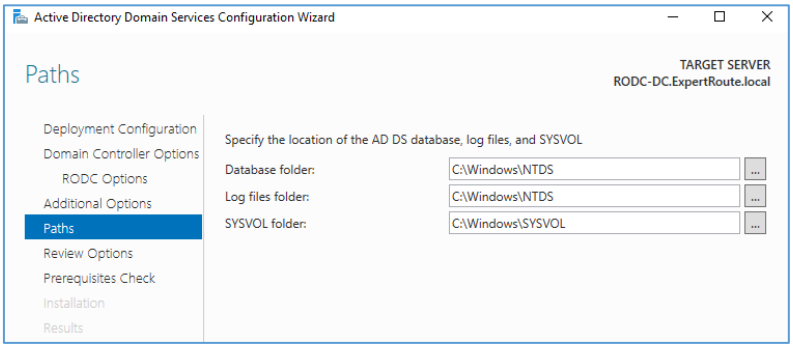
www.takbook.com

در شکل ۸-۱۳۱۱، از لیست کشویی سرور اصلی خود را که دومین کنترلر اصلی روی آن نصب است را انتخاب کنید، گزینه‌ای با نام Install from media را مشاهده می‌کنید که در قسمت بعد این گزینه را کامل توضیح خواهیم داد.



شکل ۸- ۱۳۱۱ *Read Only Domain Controller*

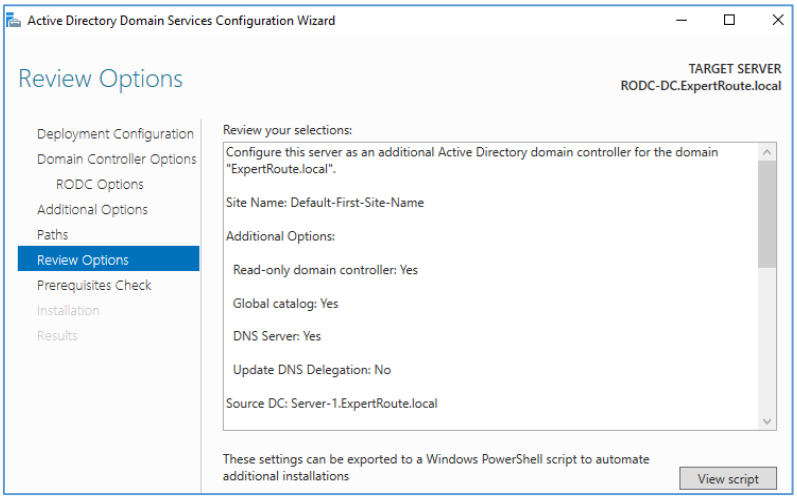
در شکل ۸-۱۳۱۲، بر روی Next کلیک کنید.



شکل ۸- ۱۳۱۲ *Read Only Domain Controller*

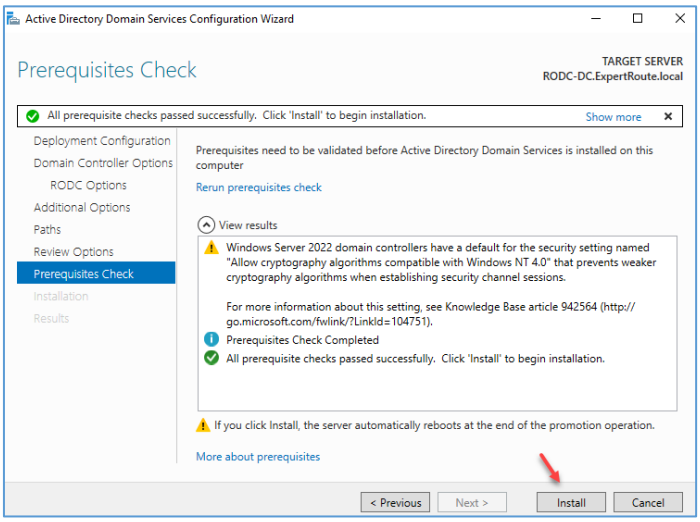
در شکل ۸-۱۳۱۳، که مربوط به اطلاعات کاملی از نصب دومین می‌باشد آن را بررسی و بر روی Next کلیک کنید

www.takbook.com



Read Only Domain Controller شکل ۸- ۱۳۱۳

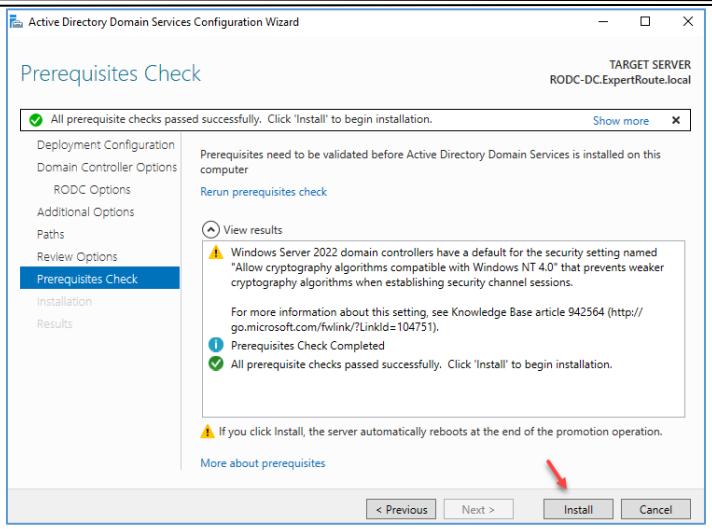
در شکل ۸-۱۳۱٤، برای نصب سرویس بر روی install کلیک کنید.



Read Only Domain Controller شکل ۸- ۱۳۱۴

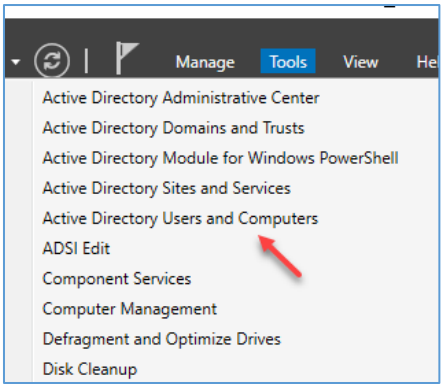
به مانند شکل ۸-۱۳۱۵، بعد از چند دقیقه سرویس موردنظر نصب می‌شود.

www.takbook.com



شکل ۸- ۱۳۱۵ *Read Only Domain Controller*

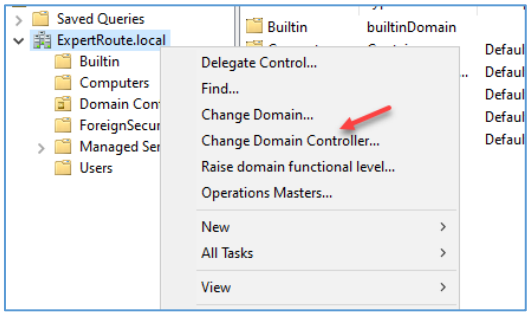
بعد از نصب سرویس به مانند شکل ۸-۱۳۱۶، Active Directory users and computers را روی سرور دوم اجرا کنید.



شکل ۸- ۱۳۱۶ *Read Only Domain Controller*

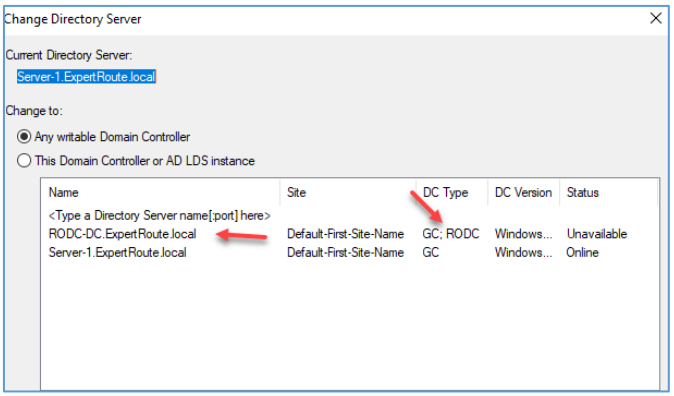
نکته‌ای که در اینجا مشاهده می‌شود این است که در حال حاضر سیستم دومین بر روی RODC قرار ندارد، برای تنظیم آن، بر روی نام سرور به مانند شکل ۸-۱۳۱۷، کلیک راست کنید و گزینه Change Domain Controller را انتخاب کنید.

www.takbook.com



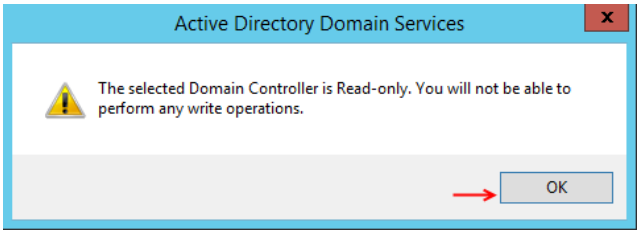
شکل ۸- ۱۳۱۷ *Read Only Domain Controller*

در شکل ۸-۱۳۱۸، گزینه The Domain Controller or AD LDS instance را انتخاب کنید و بین گزینه‌های موجود نام سروری را انتخاب کنید که به عنوان دومین فقط خواندنی (RODC) معرفی کردیم که در اینجا سرور RODC-DC به عنوان یک سرور دومین کنترلر فقط خواندنی RODC انتخاب شده است، اگر به ستون DC Type هم توجه کنید نوع دومین را از نوع RODC در نظر گرفته است، بعد از انتخاب بر روی Ok کلیک کنید.



شکل ۸- ۱۳۱۸ *Read Only Domain Controller*

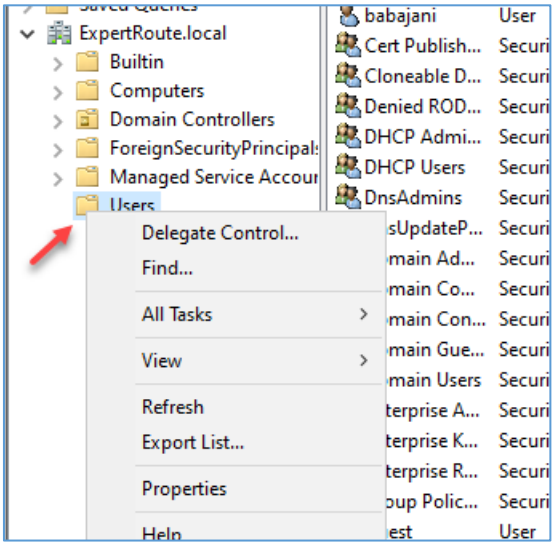
بعد از کلیک بر روی ok شکل ۸-۱۳۱۹، ظاهر می‌شود و به شما این اخطار را می‌دهد که این دومین کنترلر به فقط خواندنی تبدیل می‌شود و دیگر نمی‌توانید روی آن تغییری ایجاد کنید.



شکل ۸- ۱۳۱۹ *Read Only Domain Controller*

www.takbook.com

به مانند شکل ۸-۱۳۲۰، اگر بر روی Users کلیک راست کنید، متوجه خواهید شد هیچ کاربری را نمی‌توانید ایجاد کنید و این یعنی اینکه دومین مورد مظر فقط خواندنی است و برای نمایش اطلاعات به کار می‌رود و البته کلاینت‌ها می‌توانند از طریق این دومین وارد سیستم شوند.



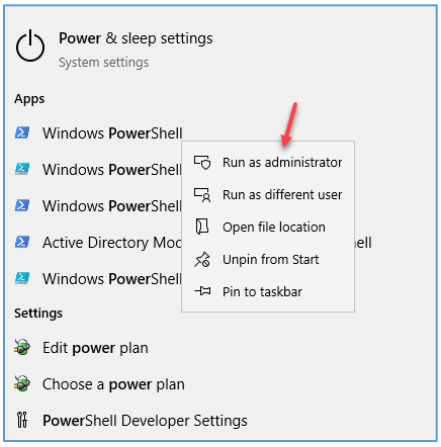
شکل ۸- ۱۳۲۰ *Read Only Domain Controller*

۸-۳-۳۹ کار با Install From Media (IFM)

همان‌طور که در قسمت قبل مشاهده کردید توانستیم یک دومین کنترلر فقط خواندنی (RODC) را نصب و بررسی کنیم، حالا باید به این نکته توجه کنید که اگر شما مدیر IT یک شرکت بسیار بزرگ باشید و حجم اطلاعات Active Directory بسیار بالا باشد و اگر بخواهیم در یک شعبه دیگر خود یک دومین کنترلر RODC فقط خواندنی راه‌اندازی کنیم برای اینکه این اطلاعات را به سرور جدید انتقال دهیم باید از خطوط ارتباطی مانند اینترنت استفاده کنیم، شاید سرعت آنچنان بالا نباشد و ساعت‌ها این انتقال طول بکشد، برای حل این مشکل مایکروسافت سرویس IFM را معرفی کرد که شما می‌توانید با چند دستور از اطلاعات Active directory اصلی خود فایل خروجی تهیه کنید و در دیگر شعبه‌ی خود آن را اجرا کنید تا زمان کوتاهی برای این انتقال انجام شود.

برای انجام این کار باید یک سرور به مانند قبل ایجاد کنید و آن را عضو دومین کنید، بعد از این کار به مانند شکل ۸-۱۳۲۱، با کاربر Administrator وارد سرور شوید و سرویس Powershell را با دسترسی کامل اجرا کنید.

www.takbook.com



شکل ۸- ۱۳۲۱ کار با *Install From Media (IFM)*

بعد از اجرای PowerShell دستور زیر را اجرا کنید:

```
Ntdsutil
```

بعد از اجرای دستور Ntdsutil دستور زیر را وارد کنید:

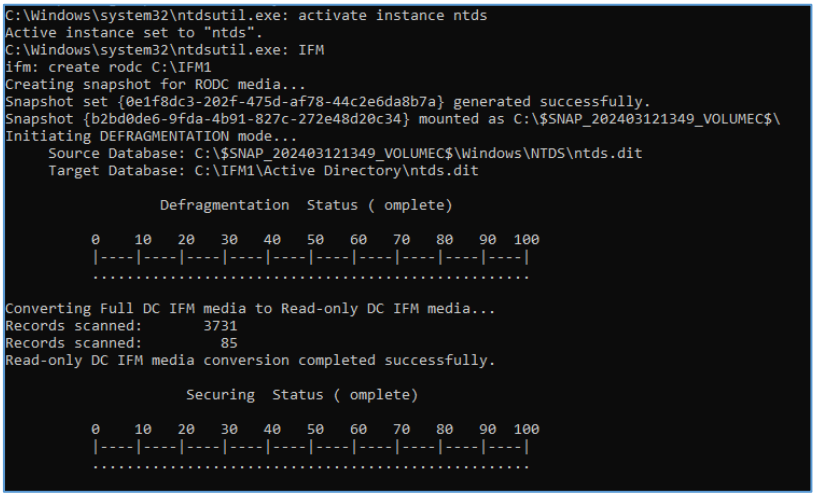
```
Activate instance ntds
```

در ادامه هم دستور IFM را وارد کنید تا برای نصب دومین فقط خواندنی آماده شود

```
IFM
```

در ادامه هم دستور دستور زیر را وارد کنید تا اطلاعات مورد نظر در پوشه‌ی مشخص شده ذخیره شود، البته اگر فقط دستور دوم یعنی دستور Create sysvol rodc C::\IFM3 را وارد کنید کافی است و نیازی به دستور اول نیست

```
Create rodc c:\IFM1
Create sysvol rodc C::\IFM3
```



شکل ۸- ۱۳۲۲ کار با *Install From Media (IFM)*

www.takbook.com


```
ifm: create sysvol rodc C:\IFM3
Creating snapshot for RODC media...
Snapshot set {7c636dfb-9ba0-40db-888e-e65b58e4a55e} generated successfully.
Snapshot {af0ec97f-d8eb-437a-a255-6474a704a207} mounted as C:\$SNAP_202403121350_VOLUMEC$\
Snapshot {af0ec97f-d8eb-437a-a255-6474a704a207} is already mounted.
Initiating DEFRAGMENTATION mode...
     Source Database: C:\$SNAP_202403121350_VOLUMEC$\Windows\NTDS\ntds.dit
     Target Database: C:\IFM3\Active Directory\ntds.dit

                Defragmentation  Status ( omplete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................

Converting Full DC IFM media to Read-only DC IFM media...
Records scanned:       3731
Records scanned:         85
Read-only DC IFM media conversion completed successfully.

                    Securing  Status ( omplete)

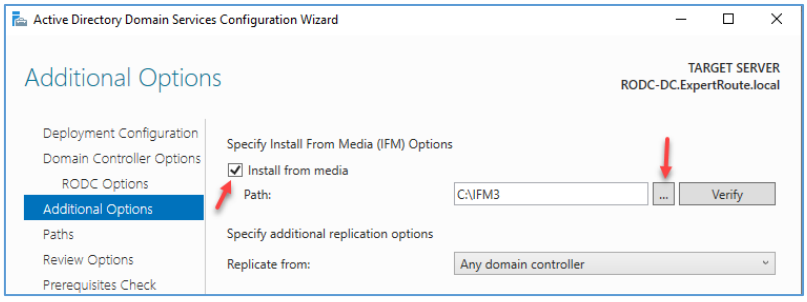
          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................

2046 pages seen
502 blank pages seen
0 unchanged pages seen
2 unused pages zeroed
1491 used pages seen
0 pages with unknown objid
66773 nodes seen
2 flag-deleted nodes zeroed
0 flag-deleted nodes not zeroed
0 version bits reset seen
0 orphaned LVs
```

شکل ۸- ۱۳۲۳ کار با *Install From Media (IFM)*

با این دو دستور دو پوشه در درایو مورد نظر ایجاد خواهد شد که در ادامه کار از آن استفاده خواهیم کرد، توجه داشته باشید این پوشه‌ها را باید از طریق سروری که می‌خواهید بر روی آن RODC فعال کنید دسترسی داشته باشید.

برای استفاده از این فایل باید مراحل نصب دومین RODC را به مانند قسمت قبلی پیش ببرید و در شکل ۸-۱۳۲٤، در قسمت Additional Options تیک گزینه‌ی Install from media را انتخاب کنید و بر روی دکمه‌ی مشخص شده کلیک کنید و پوشه‌ی IFM3 که مربوط به دستور دوم است را انتخاب کنید تا اطلاعات از آن پوشه دریافت شود و کار را ادامه دهید و در آخر بر روی Intsall کلیک کنید تا دومین RODC نصب و راه‌اندازی شود.



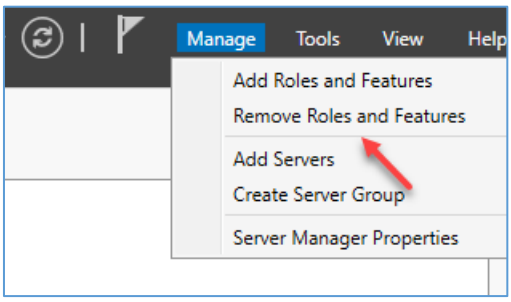
شکل ۸- ۱۳۲۴ *Install From Media (IFM)*

www.takbook.com

همان‌طور که گفتیم این روش زمانی استفاده می‌شود که حجم داده‌های شما زیاد باشد و از طریق ارتباط از راه دور زمان زیادی طول بکشد تا Sync بین سرور اصلی و دومین فرعی انجام شود.

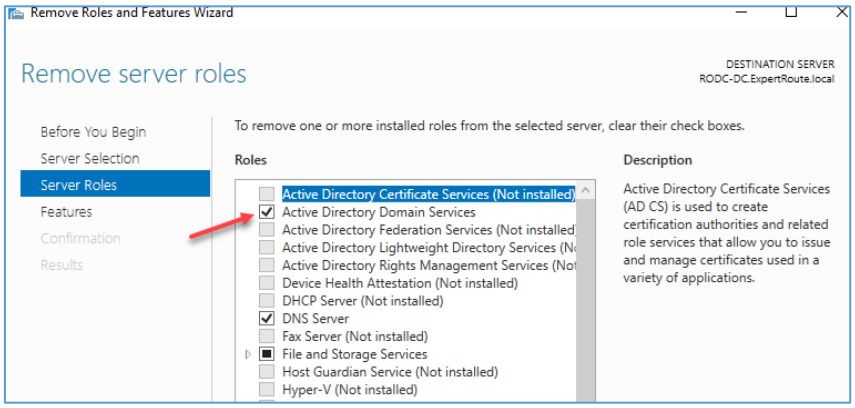
۸-۳-٤۰ حذف Read Only Domain Controller

بعد از ایجاد دومین فقط خواندنی (RODC)، می‌خواهیم ارتباط آن را با دومین قطع کنیم و به طور کامل آن را حذف کنیم، برای انجام این کار وارد سرور RODC شوید و Server Manager را اجرا کنید، به مانند شکل بعد وارد منوی Manage شوید و گزینه‌ی Remove Roles and Features را انتخاب کنید.



شکل ۸- ۱۳۲۵ حذف Read Only Domain Controller

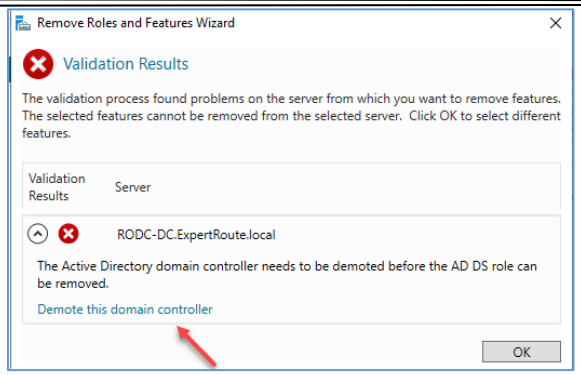
در شکل ۸-۱۳۲٦، در قسمت Server roles تیگ گزینه‌ی Active Directory Domain Services را بردارید و در شکل باز شده بر روی Remove Features کلیک کنید.



شکل ۸- ۱۳۲۶ حذف Read Only Domain Controller

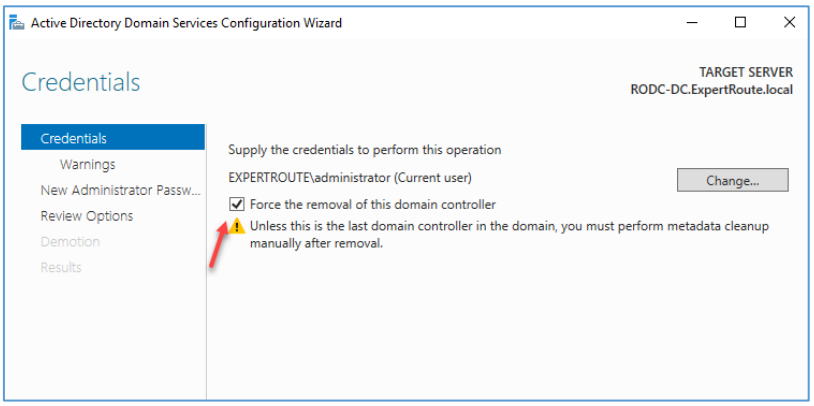
در ادامه کار شکل ۸-۱۳۲٦، ظاهر می‌شود که باید برای حذف سرویس مورد نظر بر روی Demote this domain controller کلیک کنید.

www.takbook.com



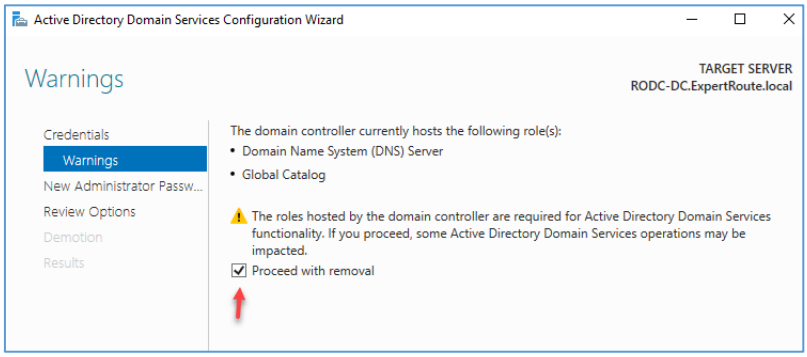
شکل ۸- ۱۳۲۷ حذف *Read Only Domain Controller*

در شکل ۸–۱۳۲۸، تکیک گزینه‌ی مورد نظر را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸- ۱۳۲۸ حذف *Read Only Domain Controller*

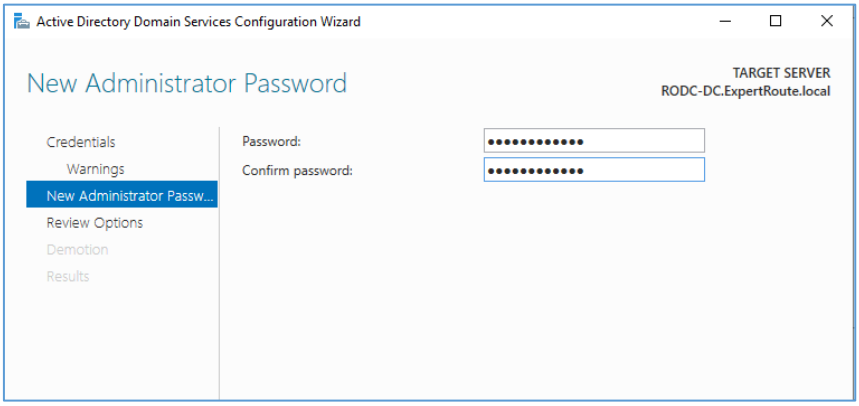
به مانند شکل ۸–۱۳۲۹، تیک گزینه‌ی مورد نظر را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۱۳۲۹ حذف *Read Only Domain Controller*

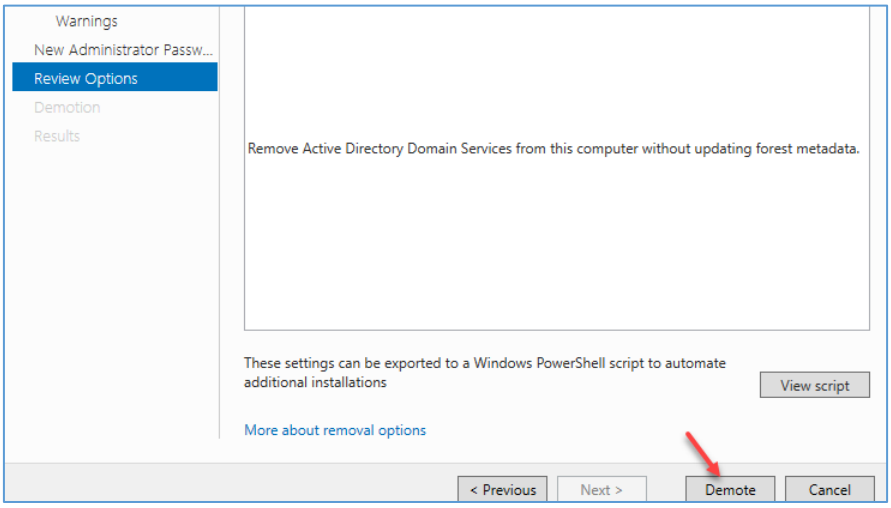
www.takbook.com

در شکل ۸-۱۳۳۰، یک رمز جدید برای کاربر Administrator وارد کنید، توجه داشته باشید بعد از حذف سرویس سرور مورد نظر از دومین خارج خواهد شد.



شکل ۸- ۱۳۳۰ حذف *Read Only Domain Controller*

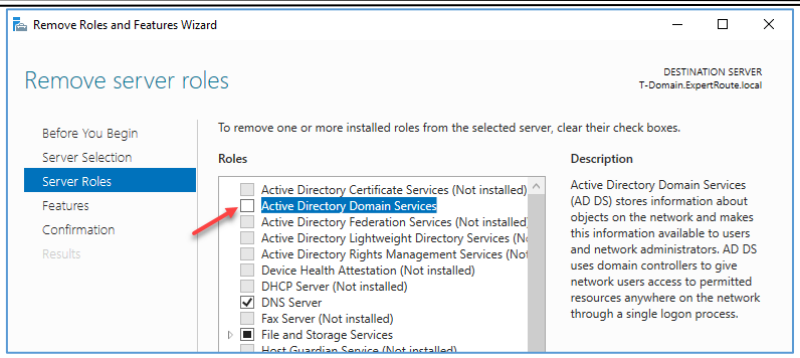
در شکل ۸-۱۳۳۱، بر روی Demote کلیک کنید تا سرویس مورد نظر حذف و سرور Restart شود.



شکل ۸- ۱۳۳۱ حذف *Read Only Domain Controller*

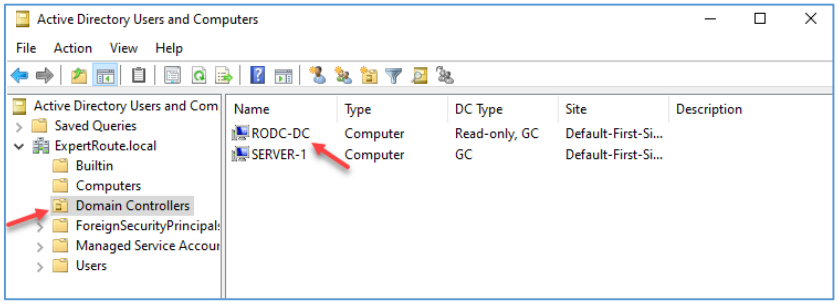
بعد از Restart شدن به مانند شکل ۸-۱۳۳۲، دوباره وارد ویندوز سرور RODC شوید و Server Manager اجرا و سرویس Active directory را به مانند شکل حذف کنید.

www.takbook.com



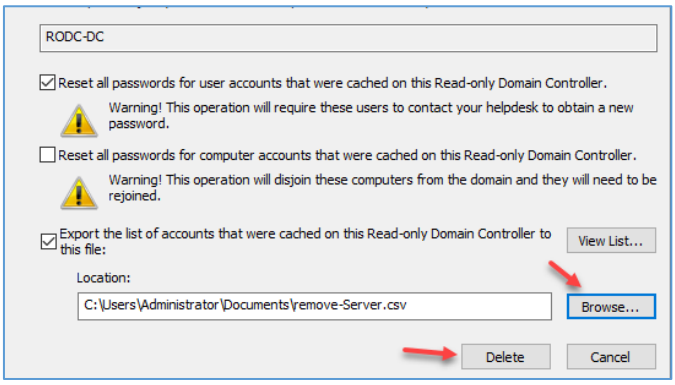
شکل ۸- ۱۳۳۲ حذف *Read Only Domain Controller*

بعد از انجام مراحل بالا فقط ارتباط از طرف سرور RODC قطع شده و برای کامل کردن حذف دومین RODC باید وارد سرور اصلی (Server-1) شوید و سرویس Active Directory Users and computers را اجرا کنید و به مانند شکل ۸–۱۳۳۳، وارد Domain Controllers شوید و سرور RODC-DC را حذف کنید.



شکل ۸- ۱۳۳۳ حذف *Read Only Domain Controller*

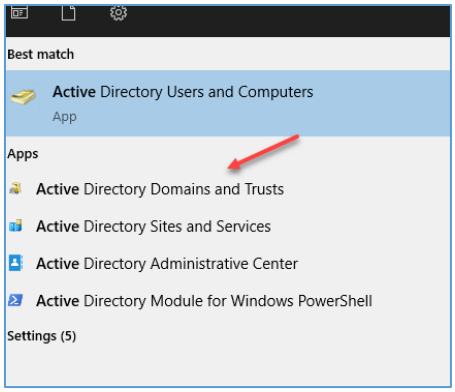
بعد از کلیک بر روی Delete در شکل ۸–۱۳۳٤، بر روی Browse کلیک کنید و یک نام بنویسید تا اطلاعات در آن ذخیره شود، بعد از انتخاب مسیر بر روی Delete کلیک کنید تا سرور مورد نظر حذف شود.



شکل ۸- ۱۳۳۴ حذف *Read Only Domain Controller*

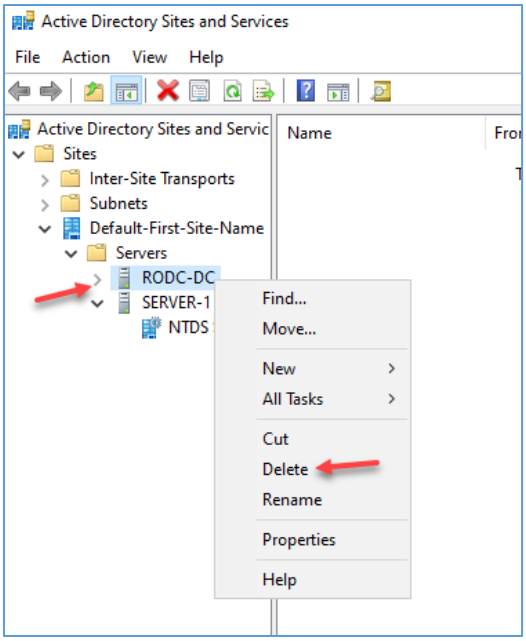
www.takbook.com

در مرحله آخر به مانند شکل سرویس Active Directory Sites and Services را اجرا کنید.



شکل ۸- ۱۳۳۵ حذف Read Only Domain Controller

و در شکل ۸-۱۳۳٦، سرور مورد نظر را حذف کنید تا کار حذف به پایان برسد.



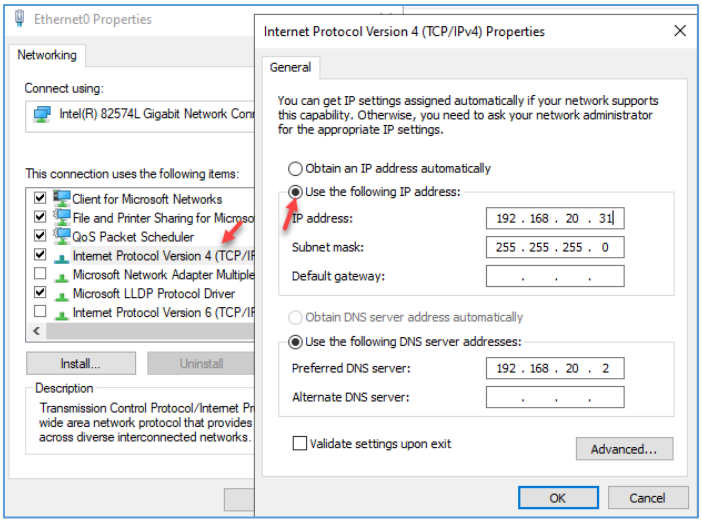
شکل ۸- ۱۳۳۶ حذف Read Only Domain Controller

۸-۳-٤۱ ایجاد Domain Tree

در این قسمت می‌خواهیم یک Domain Tree ایجاد کنیم، این نوع دومین‌ها توانایی ارتباط مستقیم با دومین اصلی را دارند یعنی اینکه Trust و یا همان اعتماد بین دو دومین برقرار است، در حالت Domain Tree می‌توانید چندین Domain ایجاد کنید که این دومین‌ها با هم به طور کامل ارتباط خواهند داشت.

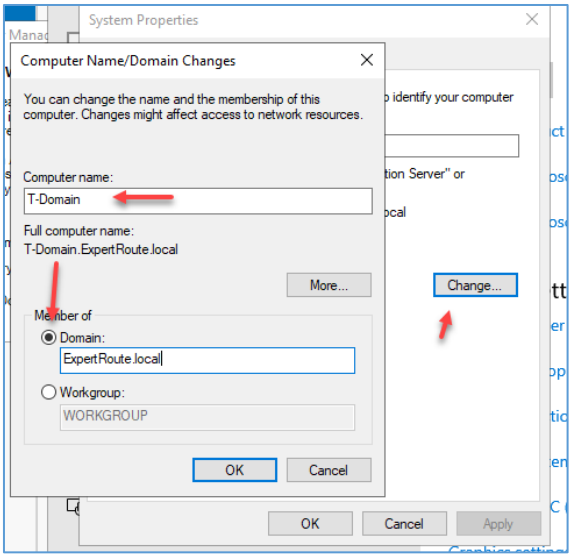
www.takbook.com

برای ایجاد Domain Tree باید از قبل یک دومین فعال (Forest) جنگل، داشته باشیم، توجه داشته باشید که سروری که روی آن Domain Tree فعال می‌شود به سرور اصلی شبکه شده است، اولین کاری که انجام می‌دهیم آدرس IP را به صورت شکل ۸–۱۳۳۷، به صورت دستی وارد می‌کنیم، توجه داشته باشید رمز عبور کاربر Administrator را باید به صورت پیچیده وارد کنید.



شکل ۸- ۱۳۳۷ تغییر آدرس IP

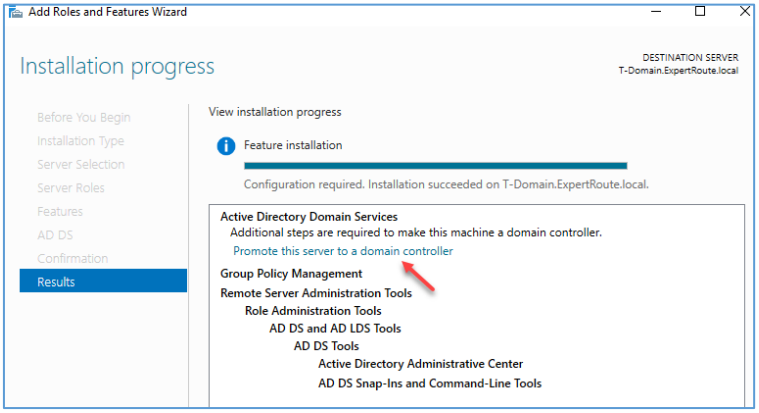
در ادامه کار به مانند شکل ۸–۱۳۳۸، یک نام برای سرور انتخاب و آن را عضو دومین کنید.



شکل ۸- ۱۳۳۸ Domain Tree

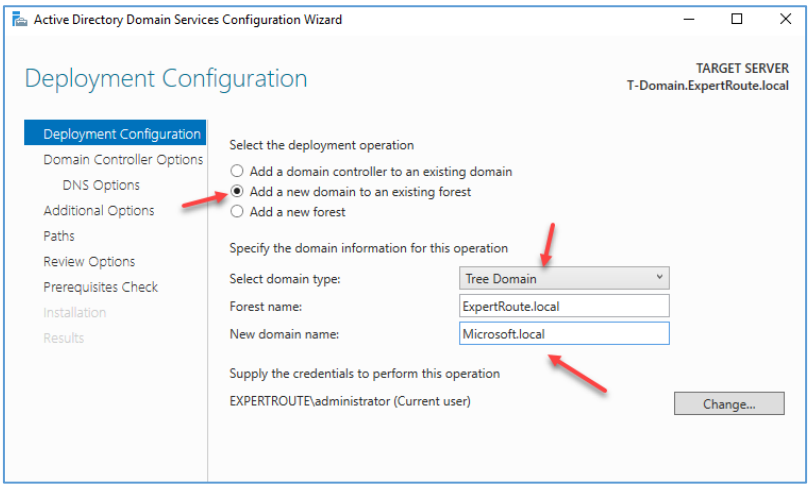
www.takbook.com

برای شروع کار سرویس Active Directory را به مانند شکل ۸-۱۳۳۹، نصب کنید و بر روی ....Promote کلیک کنید.



شکل ۸- ۱۳۳۹ Domain Tree

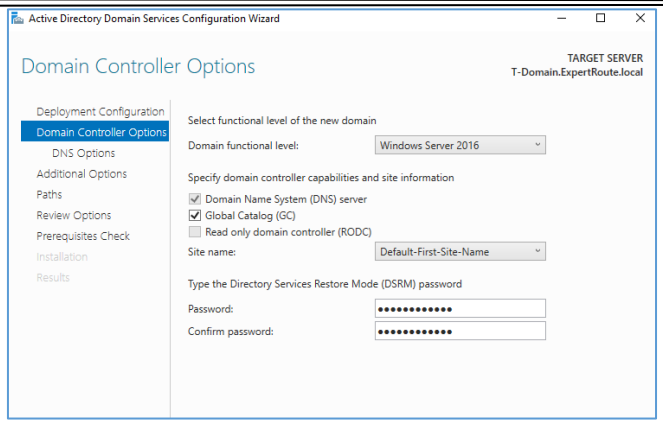
در شکل ۸-۱۳٤۰، اول گزینه Add a new domain to an existing forest را انتخاب کنید، در قسمت Select domain type گزینه Tree Domain را انتخاب کنید و در قسمت Forest name نام دومین Root خود را وارد کنید و در قسمت New Domain name نام دومین جدید خود را وارد کنید، توجه داشته باشید با کلیک بر روی Change نام کاربری را وارد کنید که در دومین اصلی (Forest) که در اینجا Expertroute.local می‌باشد اعتبار داشته باشد، برای ادامه کار بر روی Next کلیک کنید.



شکل ۸- ۱۳۴۰ Domain Tree

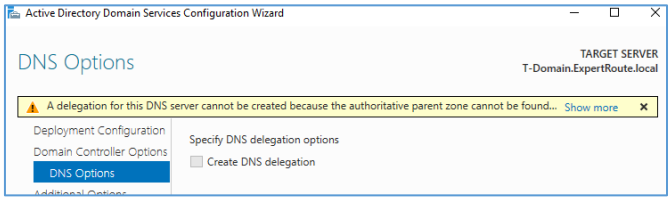
در شکل ۸-۱۳٤۱، رمز مربوط به Restore Mode را که قبلاً توضیح دادم به دلخواه خود وارد کنید و بر روی Next کلیک کنید.

www.takbook.com



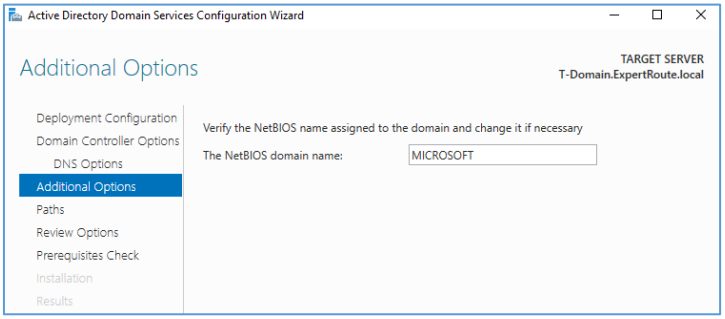
شکل ۸- ۱۳۴۱ *Domain Tree*

در شکل ۸-۱۳٤۲، بر روی Next کلیک کنید.



شکل ۸- ۱۳۴۲ *Domain Tree*

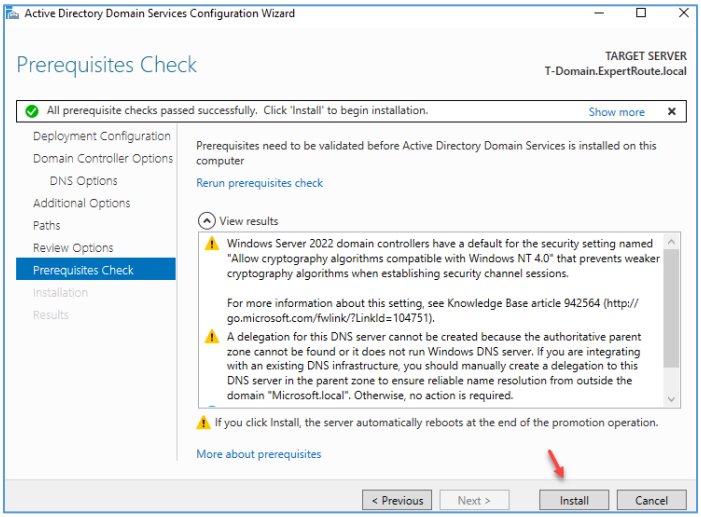
در شکل ۸-۱۳٤۳، اگر نام دومین شما از قبل وجود نداشته باشد به مانند شکل تایید می‌شود، توجه داشته باشید اگر به اینترنت متصل باشید و این نام در اینترنت وجود داشته باشد، به هیچ عنوان تایید نخواهد شد.



شکل ۸- ۱۳۴۳ *Domain Tree*

در شکل ۸-۱۳٤٤، بعد از بررسی سیستم به شما مجوز نصب داده می‌شود، برای نصب سرویس بر روی install کلیک کنید، توجه داشته باشید بیشترین مشکلی که در این قسمت شاید به وجود بیاید تنظیم نکردن IP به صورت Static می‌باشد.

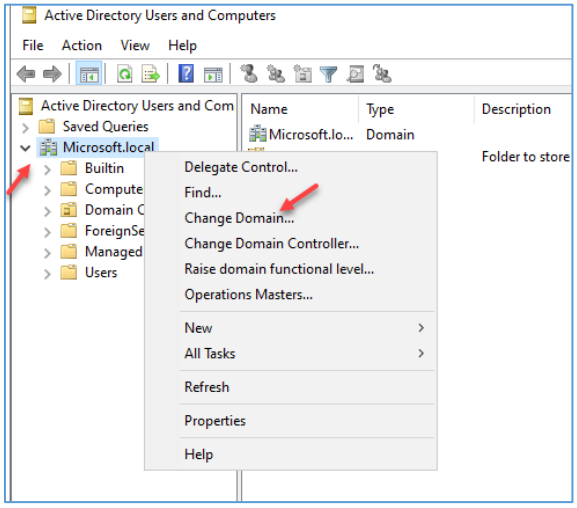
www.takbook.com



شکل ۸- ۱۳۴۴ *Domain Tree*

بعد از نصب، سرویس Active Directory Users and Computers را اجرا کنید.

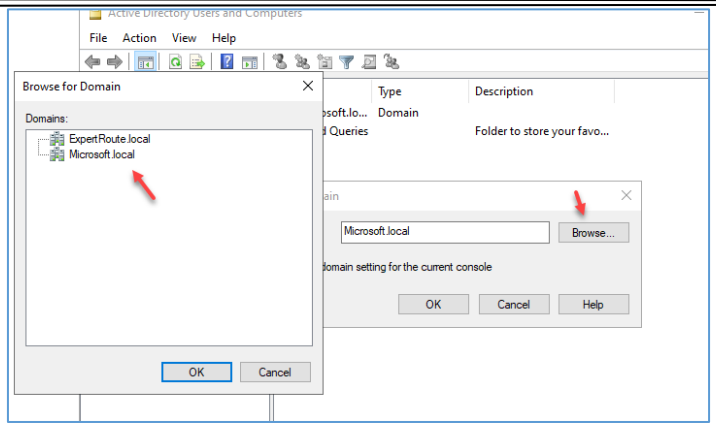
به مانند شکل ۸-۱۳٤٥، بر روی دومین مورد نظر کلیک راست کنید و گزینه Change Domain را انتخاب کنید.



شکل ۸- ۱۳۴۵ *Domain Tree*

در شکل ۸-۱۳٤٦، بر روی Browse کلیک کنید و همان‌طور که در شکل هم مشاهده می‌کنید هر دو دومین در دسترس است که در این قسمت دومین Expertroute.local را انتخاب و بر روی ok کلیک می‌کنیم.

www.takbook.com



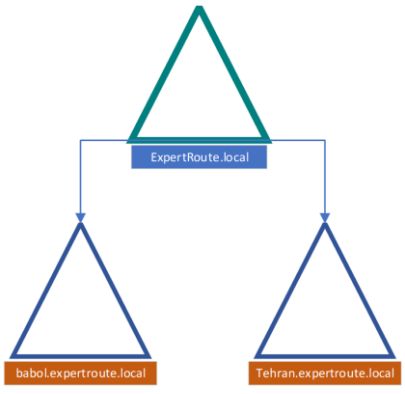
شکل ۸- ۱۳۴۶ *Domain Tree*

با این کار می‌توانید از طریق سرور دوم دومین اصلی را به راحتی مدیریت کنید، چگونگی ایجاد شدن این ارتباط از طریق سرویس Active Directory Domain and Trust انجام می‌شود.

اگر بخواهیم یک مثال در مورد Domain Tree بزنیم می‌توانیم به دومین Microsoft.com اشاره کنیم که بین دومین اصلی و Forest است و دومینی مانند Bing.com هم برای شرکت مایکروسافت است و زیر مالکیت این شرکت کنترل می‌شود و همه این دومین‌ها در یک Forest قرار دارند.

۸-۳-۴۲ نحوه ایجاد Child Domain

این نوع دومین، زیر مجموعه‌ی دومین اصلی شما خواهد شد، یعنی اینکه اگر شما یک دومین با نام Expertroute.local داشته باشید، دومین Child به صورت Child.Expertroute.local ایجاد می‌شود. بیشترین کاربرد این نوع دومین‌ها در شرکت‌های بزرگ که دارای چندین شعبه در چندین شهر مختلف می‌باشد به کار می‌رود، اگر به شکل ۸-۱۳۴۷، توجه کنید دومین اصلی مشخص شده است و دو دومین Child زیر مجموعه‌ی دومین اصلی قرار دارند.

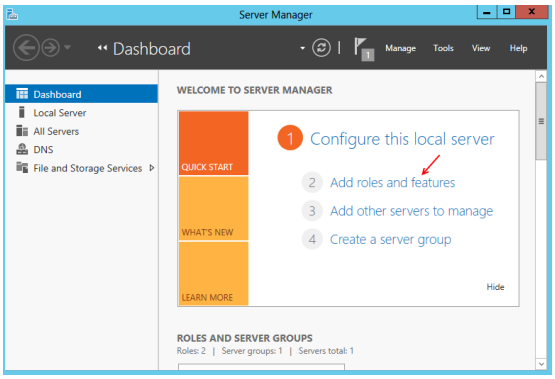


شکل ۸- ۱۳۴۷ *ایجاد Child Domain*

www.takbook.com

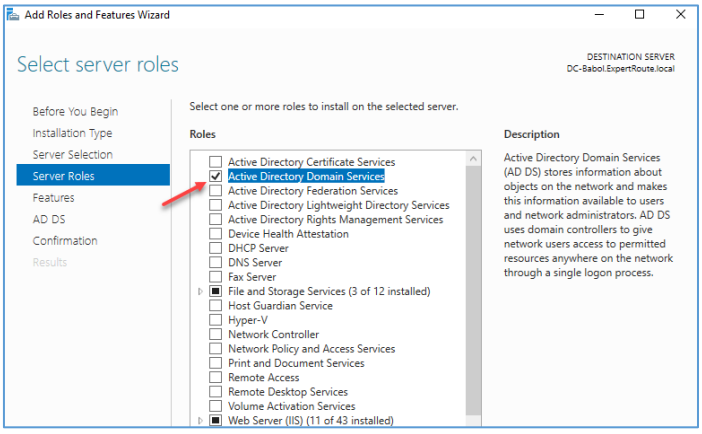
برای ایجاد Child Domain نیاز به یک دومین اصلی که در اینجا Expertroute.ir می‌باشد و یک دومین دیگر که کار Child را انجام دهد، به فرض مثال دومین Expertroute.local از قبل نصب و راه‌اندازی شده است و روی سرور دوم هم ویندوز سرور 2025 نصب شده است و آدرس IP در رنج سرور اصلی تنظیم شده است. توجه داشته باشید که این دو سرور باید همدیگر را ببینند.

برای شروع وارد سرور دوم شوید و Server Manager را اجرا کنید، و به مانند شکل ۸-۱۳۴۸، بر روی Add roles and features کلیک کنید.



شکل ۸- ۱۳۴۸ نحوه ایجاد *Child Domain*

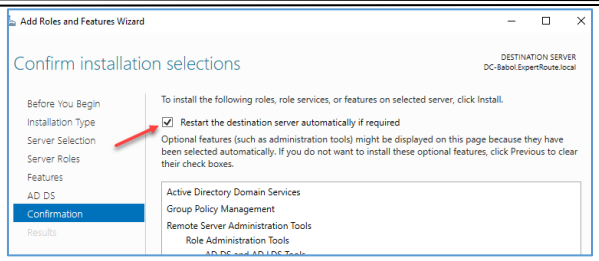
در شکل ۸-۱۳۴۹، از سمت چپ بر روی Server Roles کلیک کنید و از لیست Roles گزینه Active Directory Domain Service را انتخاب کنید و در شکل باز شده بر روی Add Features کلیک کنید و بر روی Next کلیک کنید.



شکل ۸- ۱۳۴۹ نحوه ایجاد *Child Domain*

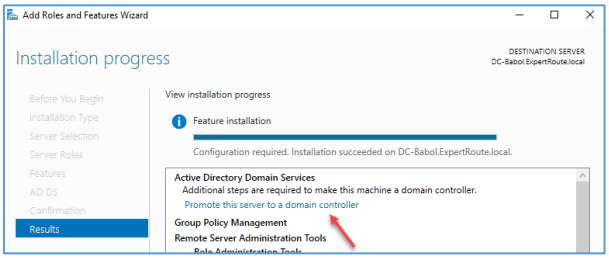
در شکل ۸-۱۳۵۰، گزینه‌ی Restart the destination را انتخاب و بر روی install کلیک کنید تا Active Directory نصب شود.

www.takbook.com



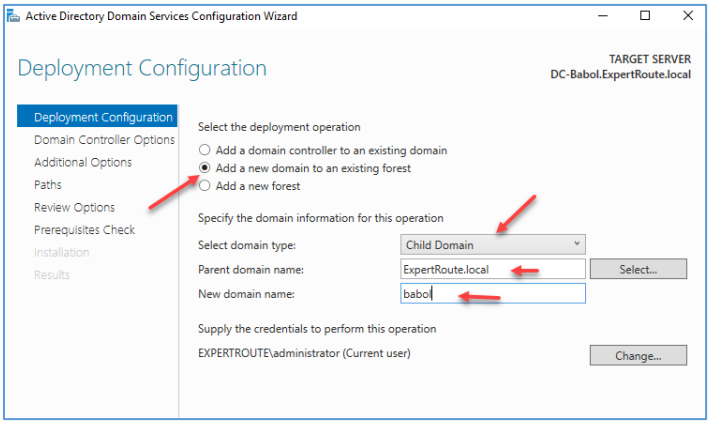
شکل ۸- ۱۳۵۰ نحوه ایجاد *Child Domain*

در شکل ۸-۱۳۵۱، بر روی Promote this server to a domain controller کلیک کنید.



شکل ۸- ۱۳۵۱ نحوه ایجاد *Child Domain*

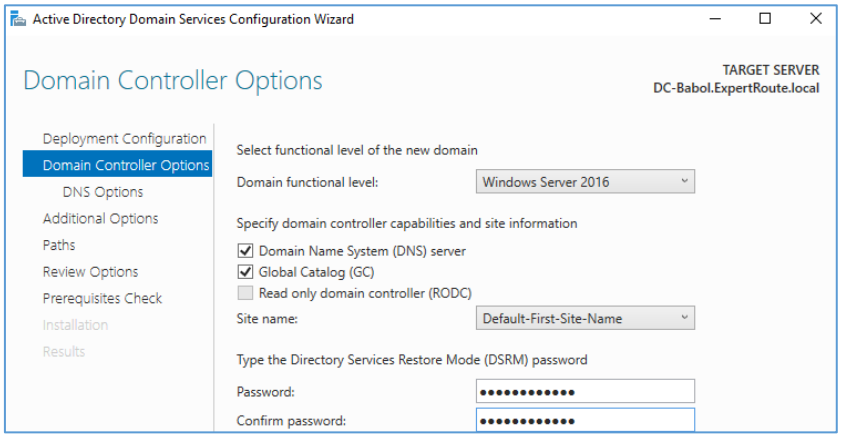
در شکل ۸-۱۳۵۲، اول گزینه Add a new domain to an existing forest را انتخاب کنید، در قسمت Select domain type گزینه‌ی Child Domain را انتخاب کنید و در قسمت Forest name نام دومین Root خود را وارد کنید و در قسمت New Domain name نام دومین جدید خود را وارد کنید، توجه داشته باشید با کلیک بر روی Change نام کاربری را وارد کنید که در دومین اصلی (Forest) که در اینجا Expertroute.local می‌باشد اعتبار داشته باشد، برای ادامه کار بر روی Next کلیک کنید.



شکل ۸- ۱۳۵۲ نحوه ایجاد *Child Domain*

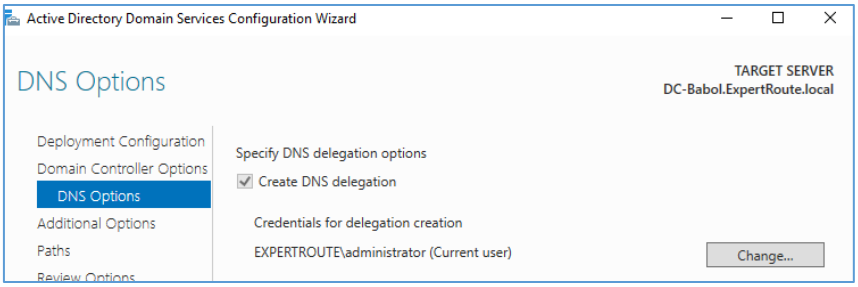
در شکل ۸-۱۳۵۳، یک رمز عبور برای Restore Mode در نظر بگیرید.

www.takbook.com



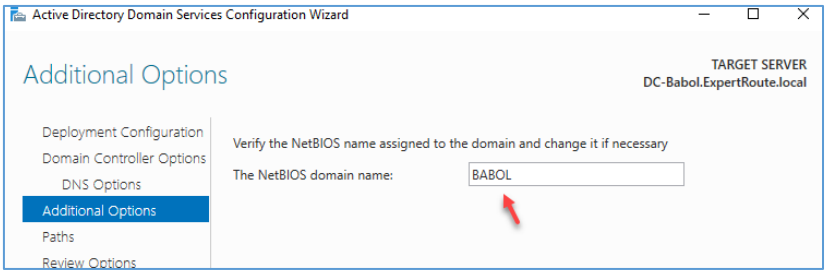
شکل ۸- ۱۳۵۳ نحوه ایجاد *Child Domain*

در شکل ۸-۱۳۵٤، می‌توانید نام کاربری را وارد کنید که اولویت بالایی در دسترسی به سرویس DNS را داشته باشد.



شکل ۸- ۱۳۵۴ نحوه ایجاد *Child Domain*

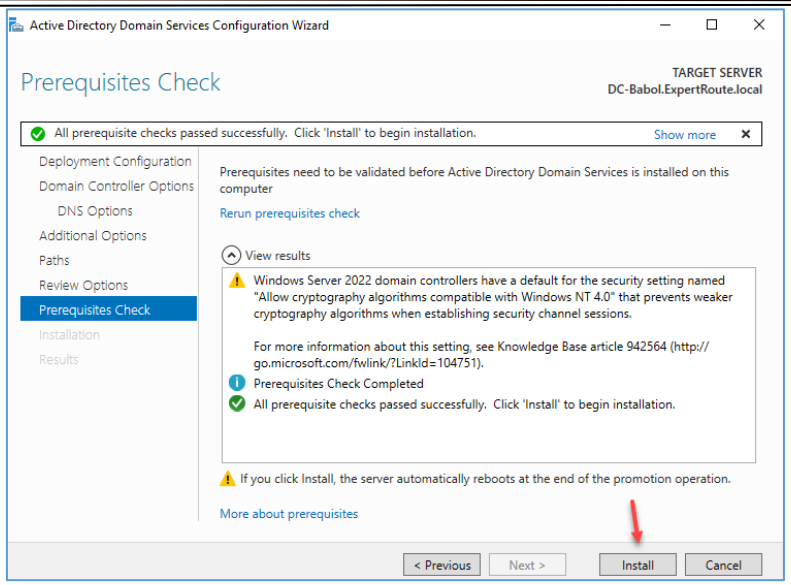
در شکل ۸-۱۳۵۵، نام Child تایید شده و می‌توانیم بر روی Next کلیک کنیم.



شکل ۸- ۱۳۵۵ نحوه ایجاد *Child Domain*

در شکل ۸-۱۳۵٦، بعد از تایید اطلاعات بر روی install کلیک کنید تا کار نصب Child domain آغاز شود. به این ترتیب Child domain به راحتی ایجاد شده است و می‌توانید از آن استفاده کنید.

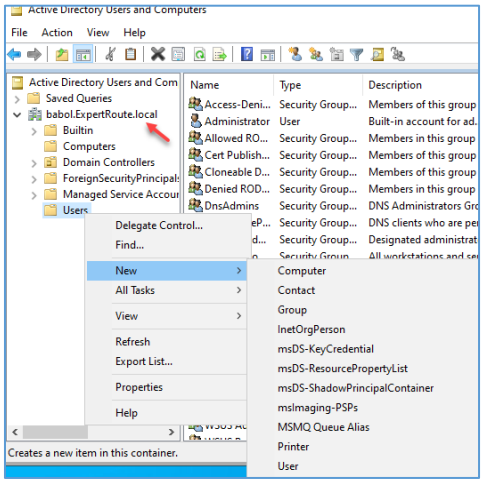
www.takbook.com



شکل ۸- ۱۳۵۶ نحوه ایجاد Child Domain

اگر وارد سرویس Active Directory Users and Computres شوید مشاهده خواهید کرد که Child Domain با موفقیت نصب شده است و آدرس Babol.ExpertRoute.local هم برای آن مشخص شده است.

شما می‌توانید در این دومین به راحتی کاربران و گروه‌های خود را ایجاد کنید و آنها را به همکاران بدهید.

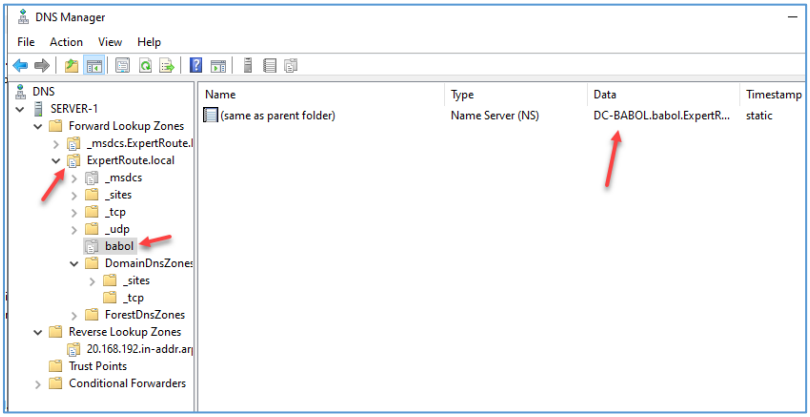


شکل ۸- ۱۳۵۷ نحوه ایجاد Child Domain

برای اینکه کلاینت‌ها بتوانند عضو این دومین شوند باید DNS را بررسی کنیم، توجه داشته باشید سرویس DNS در همان سرور Forest اصلی نصب است و اطلاعات در همان سرور اصلی قرار دارد یعنی سرور

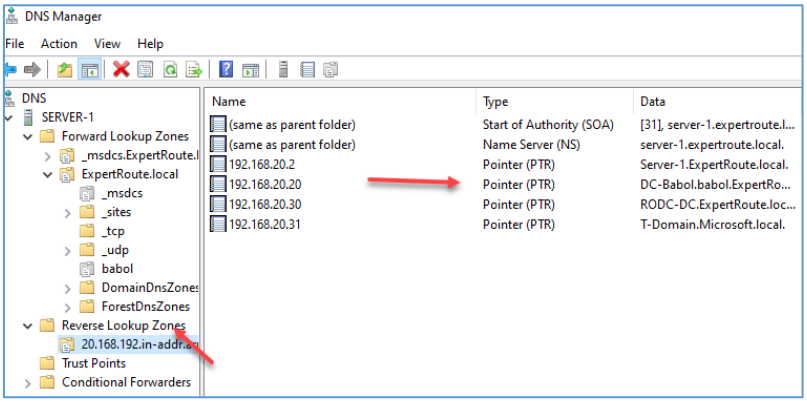
www.takbook.com

Server-1 ، برای بررسی این موضوع وارد DNS در سرور اصلی شوید، همان‌طور که در شکل ۸-۱۳۵۸، مشاهده می‌کنید یک پوشه جدید با نام Babol ایجاد شده است که این نوع فایل یک Name Server است.



شکل ۸- ۱۳۵۸ نحوه ایجاد *Child Domain*

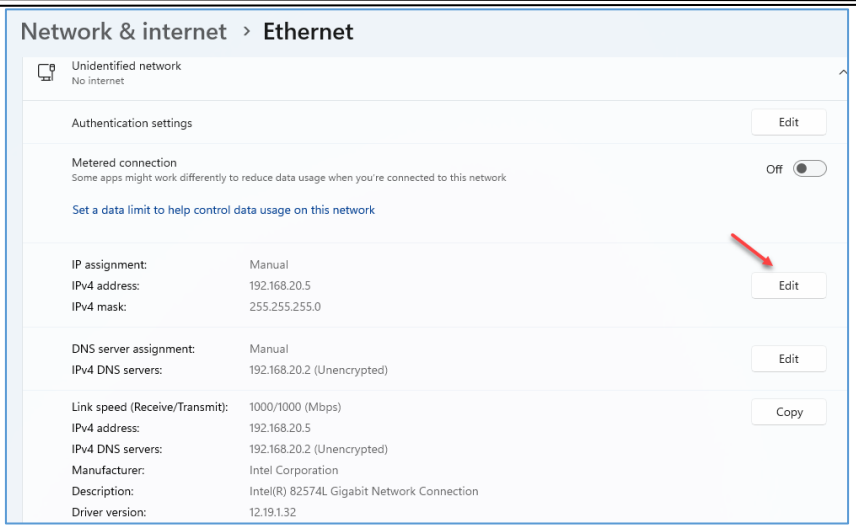
اگر وارد Reverse LooKup Zones شوید نام دومین جدید را به مانند شکل ۸-۱۳۵۹،مشاهده می‌کنید که به صورت اتوماتیک ایجاد شده است.



شکل ۸- ۱۳۵۹ نحوه ایجاد *Child Domain*

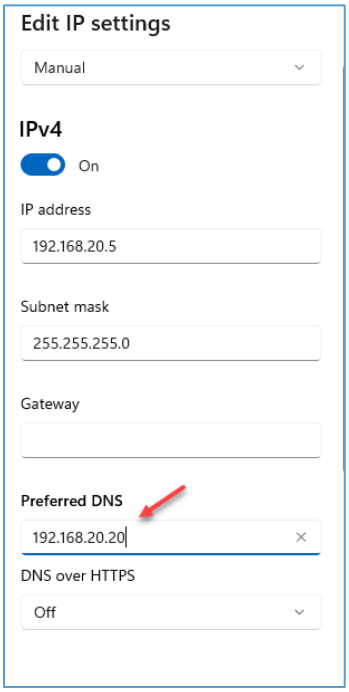
برای اینکه یک کلاینت را عضو دومین کنیم می‌توانیم آدرس DNS آن را روی سرور دومین Child تنظیم کنیم البته روی سرور اصلی هم شدنی است، برای این کار وارد Ethernet شوید و به مانند شکل ۸-۱۳٦۰ بر روی Edit کلیک کنید.

www.takbook.com



شکل ۸- ۱۳۶۰ نحوه ایجاد *Child Domain*

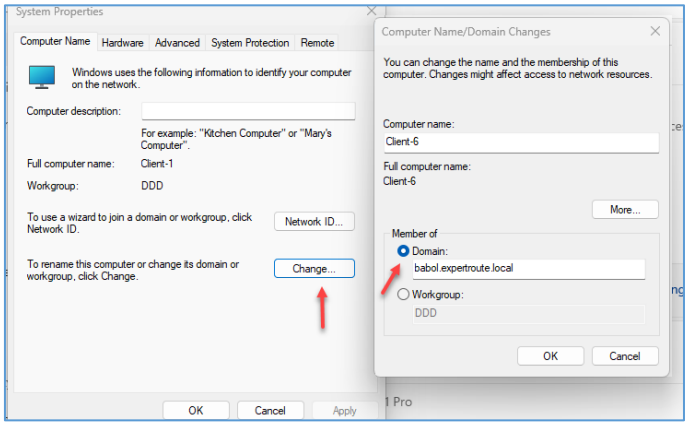
در شکل ۸-۱۳۶۱، باید در قسمت DNS آدرس دومین جدید یعنی Babol را وارد کنید



شکل ۸- ۱۳۶۱ نحوه ایجاد *Child Domain*

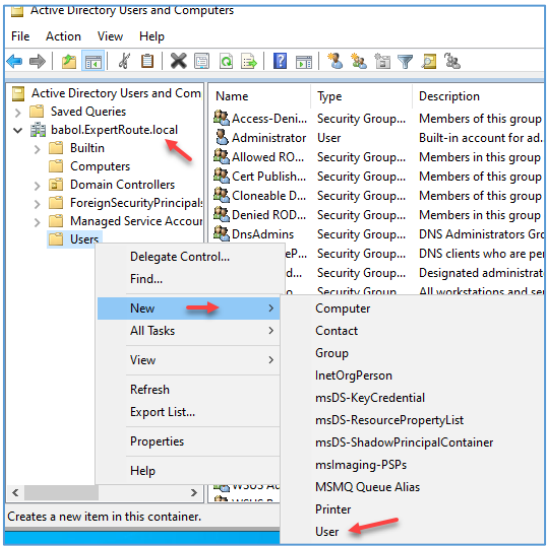
به مانند شکل ۸-۱۳۶۲، باید آدرس سرور babol.expertroute.local را در قسمت Domain وارد کنید و نام کلاینت را مشخص کنید و بعد آن را عضو دومین کنید.

www.takbook.com



شکل ۸- ۱۳۶۲ نحوه ایجاد Child Domain

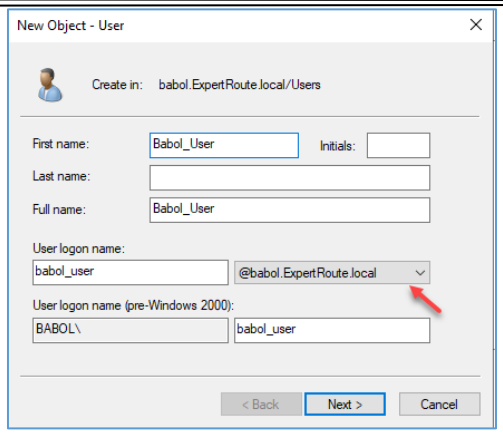
بعد از این که کلاینت را عضو دومین کردید و قبل از ورود به آن می‌خواهیم در دومین Child یک کاربر تعریف کنیم و از طریق آن کاربر وارد دومین جدید شویم، برای این کار سرویس Active Directory Users and Computers را به مانند شکل ۸-۱۳۶۳، اجرا و از قسمت Users یک کاربر جدید ایجاد کنید.



شکل ۸- ۱۳۶۳ نحوه ایجاد Child Domain

اگر به شکل ۸-۱۳۶۴، توجه کنید می‌توانید از قسمت User logon name نام دومین مورد نظر خود را انتخاب کنید، یکی دومین اصلی یا همان Forest و دیگری دومین Child است که در این قسمت Child را انتخاب می‌کنیم.

www.takbook.com



شکل ۸- ۱۳۶۴ نحوه ایجاد Child Domain

بعد از ایجاد کاربر مورد نظر از طریق کلاینتی که عضو دومین Child شده وارد شبکه خواهیم شد که نحوه‌ی ورود را در شکل ۸-۱۳٦٥، مشاهده می‌کنید:



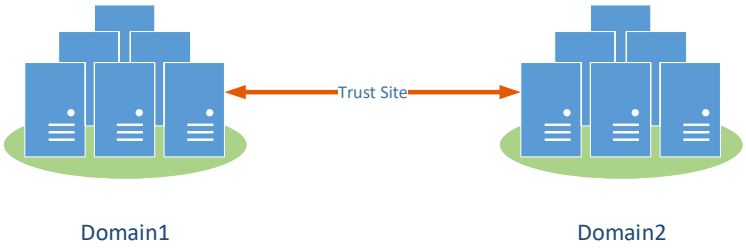
شکل ۸- ۱۳۶۵ نحوه ایجاد Child Domain

۸-۳-٤۳ ایجاد Trust بین دو دومین مختلف

ایجاد Trust (رابطه اعتماد) بین دو دامنه در اکتیو دایرکتوری به شما اجازه می‌دهد که کاربران یک دامنه به منابع دامنه دیگر دسترسی داشته باشند. این قابلیت زمانی مفید است که سازمان شما چند دامنه یا چند Forest داشته باشد.

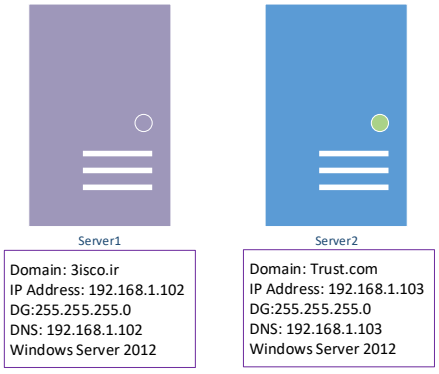
در این بخش می‌خواهیم دو دومین جدا از هم که هیچ گونه ارتباطی با هم ندارند را به هم ارتباط دهیم، این کار توسط سرویس Active Directory Domain and Trust انجام می‌شود که در این بخش با هم این سرویس را به صورت کامل بررسی می‌کنیم.

www.takbook.com



شکل ۸- ۱۳۶۶ ایجاد Trust بین دو دومین مختلف

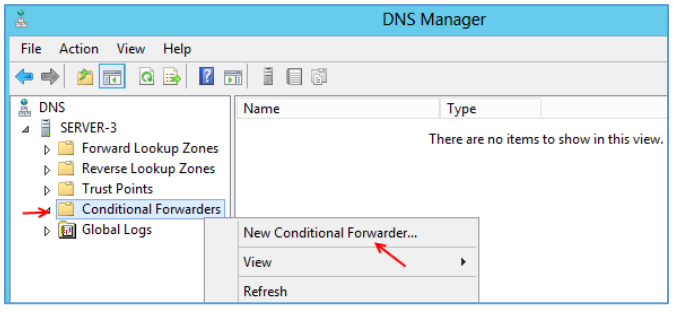
برای شروع از قبل دو دومین کنترلر آماده شده است که یکی با نام 3isco.ir و دیگری با نام Trust.com می‌باشد. توجه داشته باشید که رنج IP هر دو شبکه در یک رنج مشخص قرار دارد که این موضوع را در شکل ۸-۱۳۶۷، مشاهده می‌کنید.



شکل ۸- ۱۳۶۷ ایجاد Trust بین دو دومین مختلف

اولین کاری که باید انجام دهیم، تنظیم سرویس DNS می‌باشد، برای این‌کار اول وارد سرور 3isco می‌شویم و سرویس DNS را اجرا می‌کنیم.

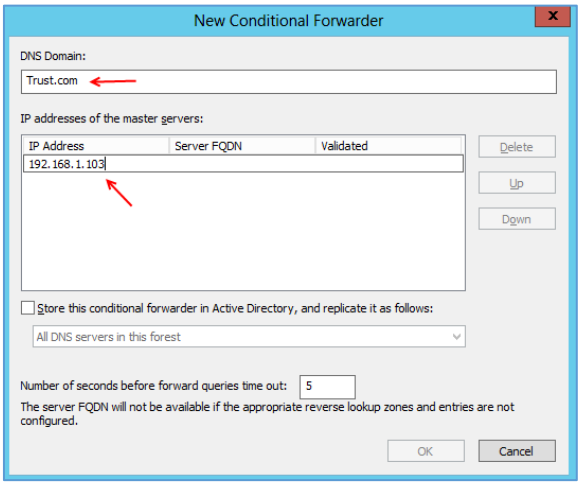
در شکل ۸-۱۳۶۸، از سمت چپ بر روی Conditional Forwarders کلیک راست کنید و گزینه New Conditional Forwarder را انتخاب کنید.



شکل ۸- ۱۳۶۸ ایجاد Trust بین دو دومین مختلف

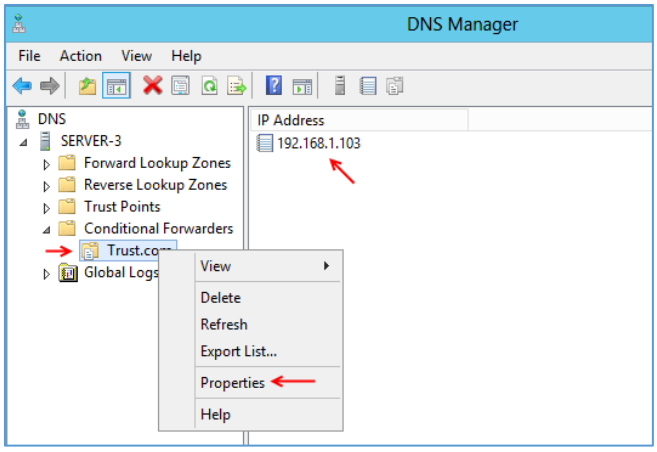
www.takbook.com

همان‌طور که گفتم در حال حاضر سروری که دومین 3isco.ir بر روی آن فعال است بررسی می‌شود. در شکل ۸-۱۳٦۹، در قسمت DNS Domain نام دومین خود را که می‌خواهید با آن Trust برقرار کنید را وارد کنید، بعد از آن در قسمت IP Address آدرس IP موردنظر شبکه Trust.com را وارد کنید، همان‌طور که گفتم این دو شبکه باید در یک رنج قرار داشته باشند، بعد از آن بر روی Enter فشار دهید و بعد OK کنید.



شکل ۸- ۱۳۶۹ ایجاد Trust بین دو دومین مختلف

بعد از ایجاد ارتباط دهنده موردنظر، برای اینکه متوجه شوید که ارتباط با سرور روبرو انجام گرفته به مانند شکل ۸-۱۳۷۰، بر روی Properties کلیک کنید و در شکل باز شده بر روی Edit کلیک کنید، اگر ارتباط برقرار باشد با آیکون سبز مشخص‌شده است.

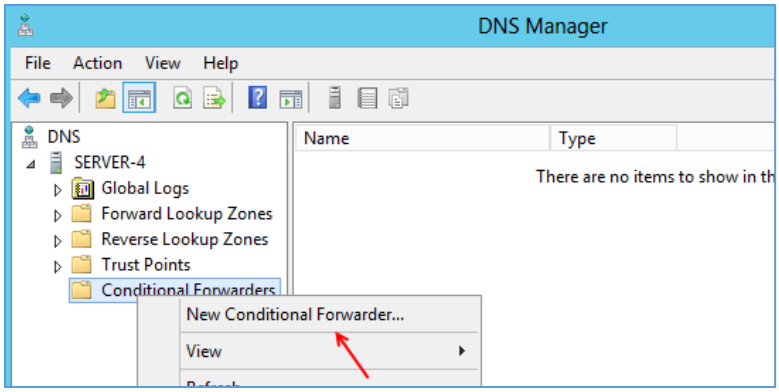


شکل ۸- ۱۳۷۰ ایجاد Trust بین دو دومین مختلف

www.takbook.com

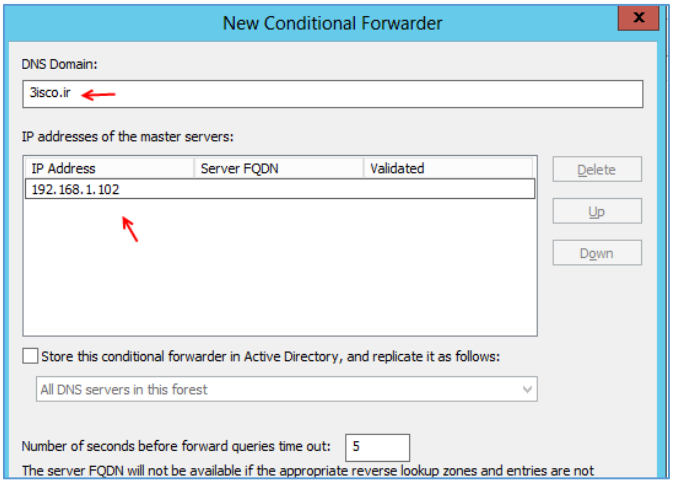
بعد از انجام کار قبلی باید وارد سرور دوم شویم و همین کار را برای سرور Trust.com برای انتقال اطلاعات به سرور 3isco.ir انجام دهیم.

به مانند شکل ۸-۱۳۷۱، وارد سرویس DNS شوید و بر روی Conditional Forwarders کلیک راست کنید و گزینه New Conditional Forwarder را انتخاب کنید.



شکل ۸- ۱۳۷۱ ایجاد Trust بین دو دومین مختلف

در شکل ۸-۱۳۷۲، در قسمت DNS Domain نام دومین روبرو خود را که می‌خواهید با آن Trust برقرار کنید را وارد کنید، بعد از آن در قسمت IP Address آدرس IP موردنظر شبکه 3isco.ir را وارد کنید، همان‌طور که گفتم این دو شبکه باید در یک رنج قرار داشته باشند، بعد از آن بر روی Enter فشار دهید و بعد OK کنید.

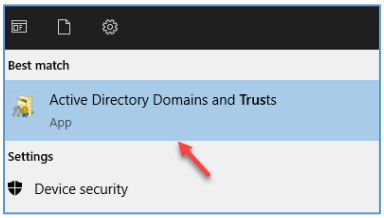


شکل ۸- ۱۳۷۲ ایجاد Trust بین دو دومین مختلف

با انجام کارهای قبلی همه اطلاعات مربوط به DNS Server به همدیگر ارسال می‌شود، یعنی اینکه اگر شما یک Host در یکی از سرویس‌های DNS ایجاد کنید، در طرف دیگر این Host ایجاد می‌شود.

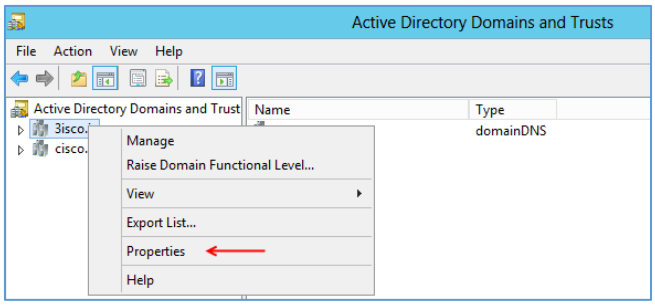
www.takbook.com

در ادامه باید سرویس Active Directory Domain and Trust را برای ارتباط دو دومین با هم تنظیم کنیم.
وارد سرور اول یعنی سروری که دومین 3isco.ir روی آن فعال است می‌شویم و به مانند شکل ۸-۱۳۷۳، سرویس Active Directory Domain and Trust را در Serach اجرا می‌کنیم.



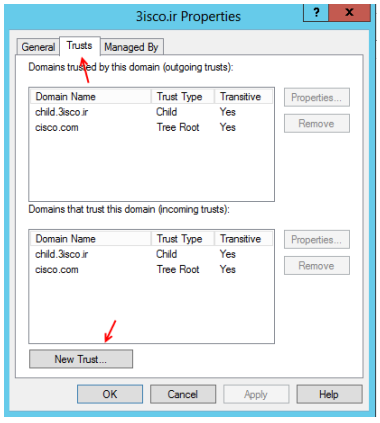
شکل ۸- ۱۳۷۳ ایجاد Trust بین دو دومین مختلف

بعد از اجرای سرویس به مانند شکل ۸-۱۳۷٤، روی نام دومین خود کلیک راست کنید و گزینه Properties را انتخاب کنید.



شکل ۸- ۱۳۷۴ ایجاد Trust بین دو دومین مختلف

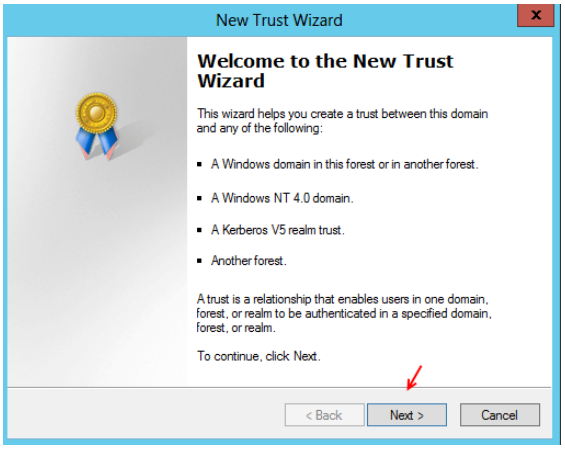
در شکل ۸-۱۳۷۵، وارد تب Trusts شوید و برای ایجاد ارتباط بین دو دومین موردنظر بر روی New Trust کلیک کنید.



شکل ۸- ۱۳۷۵ ایجاد Trust بین دو دومین مختلف

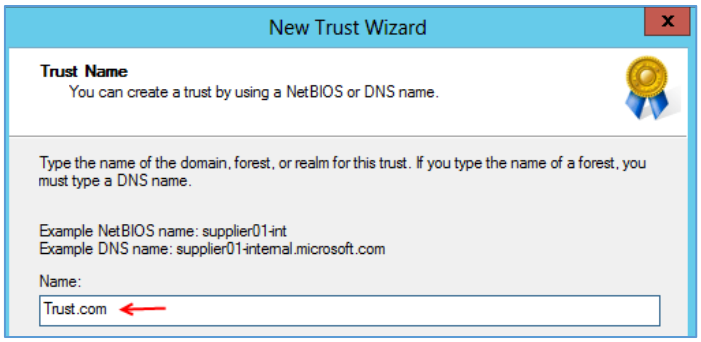
www.takbook.com

به مانند شکل ۸-۱۳۷۵، بر روی Next کلیک کنید.



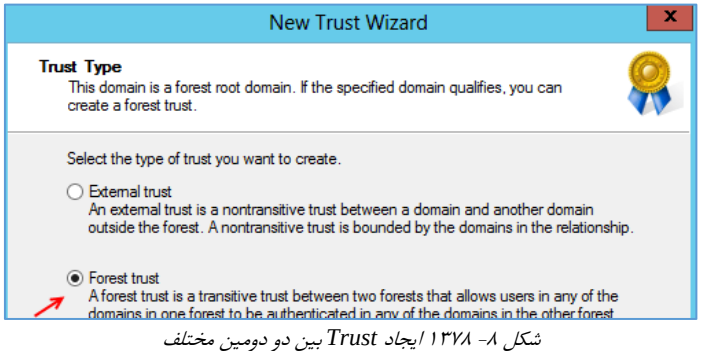
شکل ۸- ۱۳۷۶ ایجاد Trust بین دو دومین مختلف

در شکل ۸-۱۳۷۷، باید نام دومین روبرو را وارد کنید که در این قسمت Trust.com وارد شده است.



شکل ۸- ۱۳۷۷ ایجاد Trust بین دو دومین مختلف

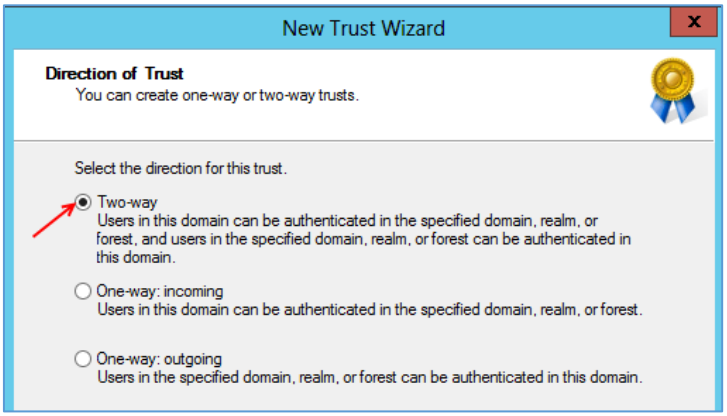
در شکل ۸-۱۳۷۸، برای انتقال اطلاعات از دومین اصلی به دومین دیگر گزینه Forest trust را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸- ۱۳۷۸ ایجاد Trust بین دو دومین مختلف

www.takbook.com

در شکل باید مشخص کنید که ارتباط بین دو دومین به چه صورت باشد، آیا می‌خواهید فقط اطلاعات ارسال شود و یا فقط دریافت شود و یا می‌خواهید هم ارسال و هم دریافت شود که باید گزینه اول یعنی Two-way را انتخاب کنید. و بر روی next کلیک کنید.



شکل ۸- ۱۳۷۹ ایجاد Trust بین دو دومین مختلف

در شکل ۸-۱۳۸۰، گزینه‌ی Both this domain… را انتخاب و بر روی next کلیک کنید.

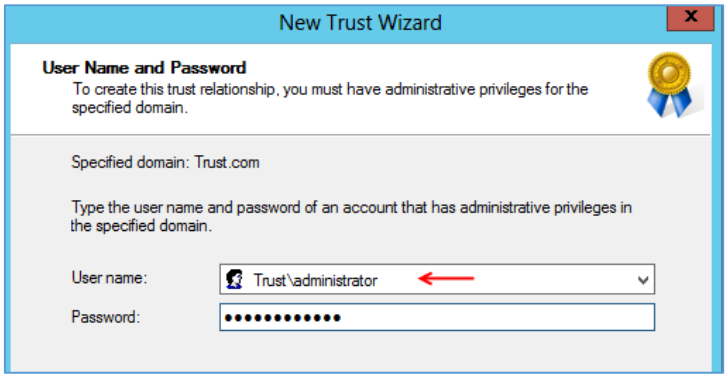


شکل ۸- ۱۳۸۰ ایجاد Trust بین دو دومین مختلف

در شکل ۸-۱۳۸۱، باید نام کاربری را وارد کنید که در دومین Trust.com یعنی دومین روبرویی اعتبار داشته باشد.

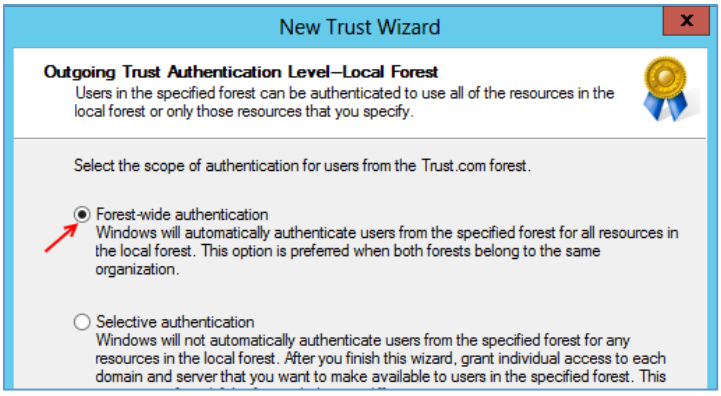
بعد از وارد کردن اطلاعات بر روی Next کلیک کنید.

www.takbook.com



شکل ۸- ۱۳۸۱ ایجاد Trust بین دو دومین مختلف

در شکل ۸-۱۱۸۲، نحوه‌ی ایجاد امنیت را می‌توانید انتخاب کنید که در این بخش گزینه اول را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۱۳۸۲ ایجاد Trust بین دو دومین مختلف

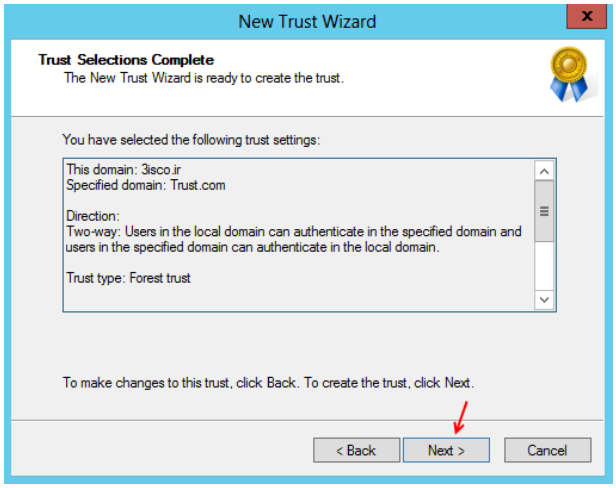
در شکل ۸-۱۳۸۲، گزینه اول را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۱۳۸۳ ایجاد Trust بین دو دومین مختلف

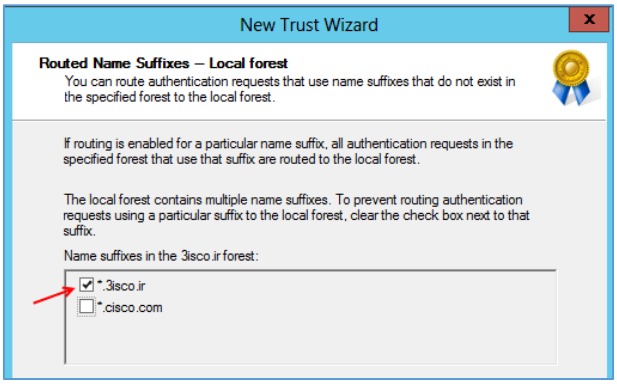
www.takbook.com

در شکل ۸-۱۳۸٤، این صفحه بر روی Next کلیک کنید....



شکل ۸- ۱۳۸۴ ایجاد Trust بین دو دومین مختلف

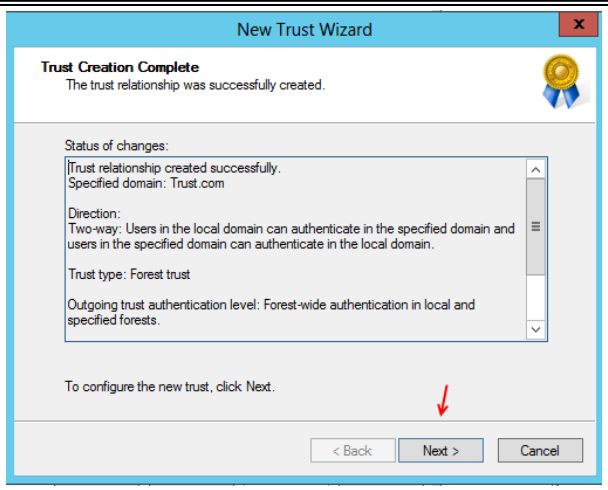
اگر در سرور خود از چندین دومین استفاده می‌کنید و یا استفاده می‌کردید به مانند شکل ۸-۱۳۸٤، در این قسمت لیست دومین‌ها را برای شما لیست می‌کنید که شما باید دومین موردنظر خود را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۱۳۸۵ ایجاد Trust بین دو دومین مختلف

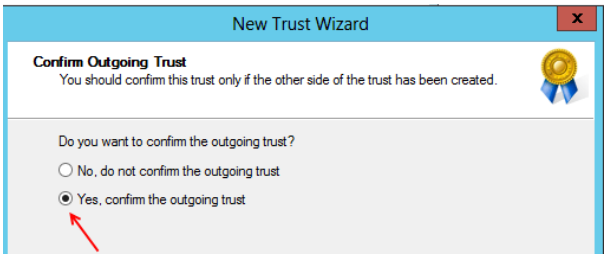
در شکل ۸-۱۳۸٦، بر روی Next کلیک کنید.

www.takbook.com



شکل ۸- ۱۳۸۶ ایجاد Trust بین دو دومین مختلف

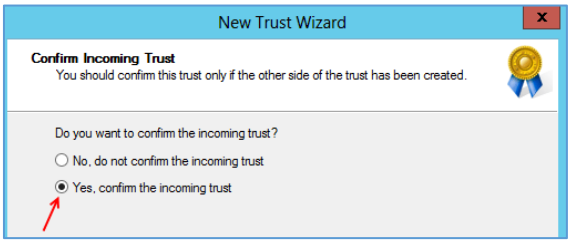
در شکل ۸-۱۳۸۷، مربوط به تنظیم Outgoing Trust می‌باشد که باید گزینه Yes را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۸- ۱۳۸۷ ایجاد Trust بین دو دومین مختلف

در شکل ۸-۱۳۸۸، گزینه‌ی ..Yes را انتخاب و بر روی next کلیک کنید.

در صفحه آخر بر روی Finish کلیک کنید.

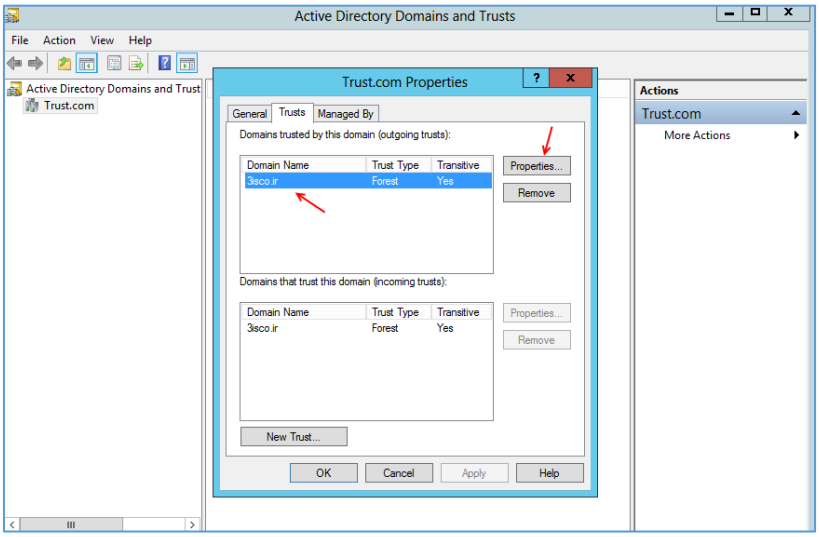


شکل ۸- ۱۳۸۸ ایجاد Trust بین دو دومین مختلف

بعد از ایجاد Trust در دومین 3isco.ir حالا باید وارد سرور دوم شویم، همان‌طور که در شکل ۸-۱۳۸۹، مشاهده می‌کنید سرور دوم یعنی دومین Trust.com به صورت خودکار تنظیمات ارتباطی را از سرور

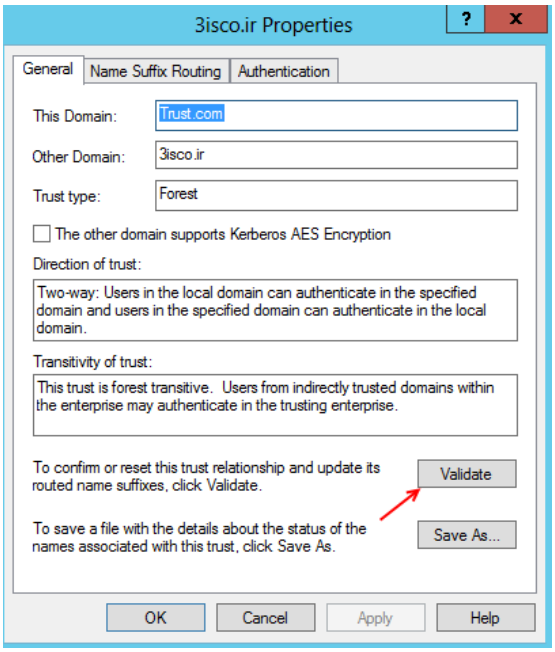
www.takbook.com

3isco.ir دریافت کرده است. برای اینکه متوجه بشویم که ارتباط با سرور زیر به صورت کامل برقرار شده است روی دومین موردنظر کلیک کنید و گزینه Properties را انتخاب کنید.



شکل ۸- ۱۳۸۹ ایجاد Trust بین دو دومین مختلف

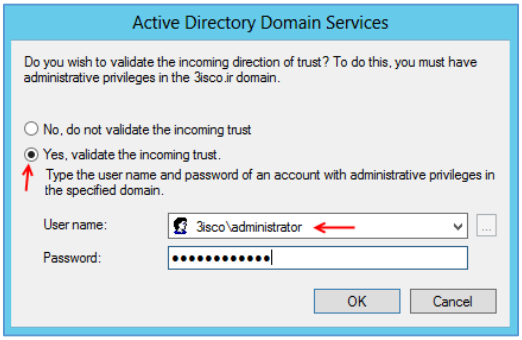
در شکل ۸–۱۳۹۰، در تب General بر روی گزینه Validate کلیک کنید تا شکل ۸–۱۳۹۱، ظاهر شود.



شکل ۸- ۱۳۹۰ ایجاد Trust بین دو دومین مختلف

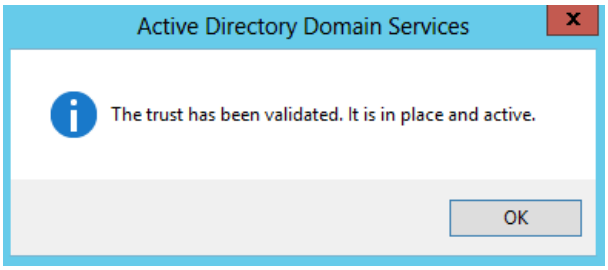
www.takbook.com

در شکل ۸-۱۳۹۱، باید نام کاربری که در دومین 3isco.ir اعتبار دارد را وارد کنید و بر روی ok کلیک کنید.



شکل ۸- ۱۳۹۱ ایجاد Trust بین دو دومین مختلف

بعد از کلیک بر روی ok شکل ۸-۱۳۹۲، این پیغام مبنی بر انجام صحیح ارتباط با دومین روبرویی ظاهر می‌شود.



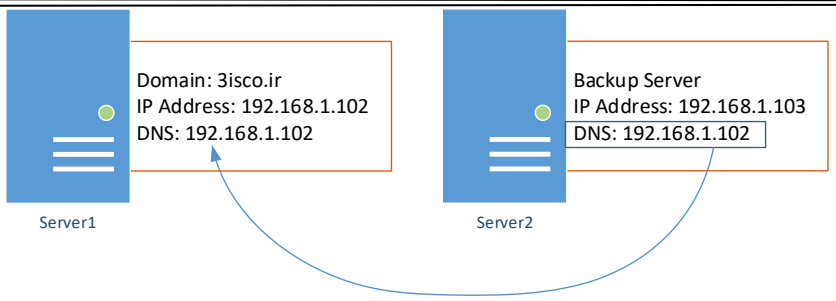
در ادامه نحوه انتقال اطاعات یک اکتیو دایرکتوری به یک اکتیو دایرکتوری دیگر را با هم بررسی می‌کنیم.

۸-۳-٤٤ انتقال اطلاعات Active Directory

اگر شما مدیر یک شبکه بزرگ یا کوچک باشید و بعد از تلاش‌های بسیار یک دومین کنترلر به همراه چندین کاربر و گروه و ... ایجاد کرده باشید، حتماً دوست ندارید با ایجاد مشکل در سرور اصلی همه اطلاعات از بین برود، برای اینکه اطلاعات خود را که بسیار مهم است، حفظ کنیم، می‌توانیم یک سرور جدید آماده کنیم و اطلاعات مربوط به دومین کنترلر خود را به صورت کامل در طی فواصل زمانی مشخص به سرور دیگر انتقال دهیم.

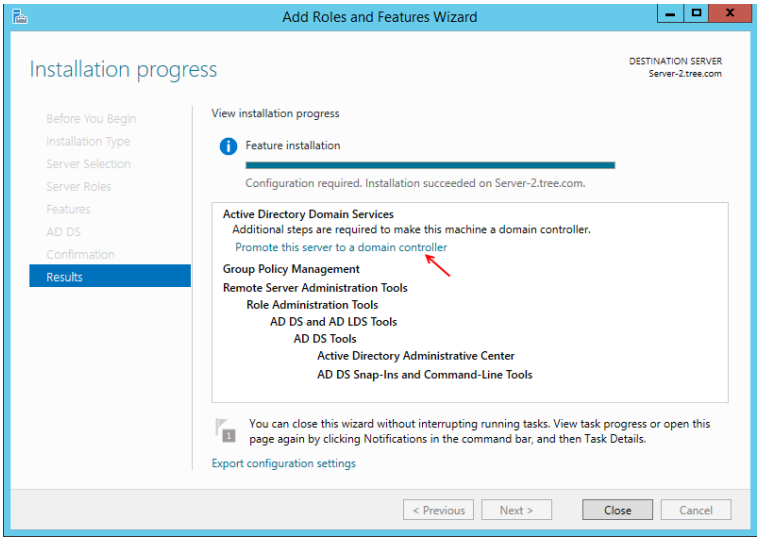
برای این کار نیاز به یک سرور اصلی داریم که اطلاعات کاربران، گروه‌ها و ... روی آن قرار دارد که در این قسمت دومین 3isco.ir این نقش را بازی می‌کند، یک سرور دیگر در کنار سرور اول قرار می‌دهیم و رنج IP آن را در رنج IP سرور اصلی قرار می‌دهیم، توجه داشته باشید آدرس DNS باید آدرس سرور اصلی باشد.

www.takbook.com



شکل ۸- ۱۳۹۲ انتقال اطلاعات *Active Directory*

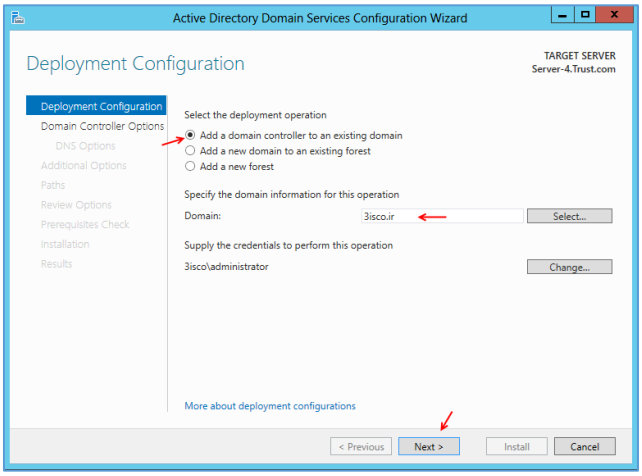
برای شروع وارد سرور دوم می‌شویم و Server Manager را اجرا می‌کنیم، بعد از اجرا بر روی Add Roles And Features کلیک کنید، در صفحه باز شده بر روی Next کلیک کنید تا به Server Roles برسید در این قسمت گزینه Active Directory Domain Services را انتخاب کنید و بر روی Next کلیک کنید و سرویس را نصب کنید. بعد از نصب به مانند شکل ۸-۱۳۹۳، بر روی Promote this server to a domain controller کلیک کنید.



شکل ۸- ۱۳۹۳ انتقال اطلاعات *Active Directory*

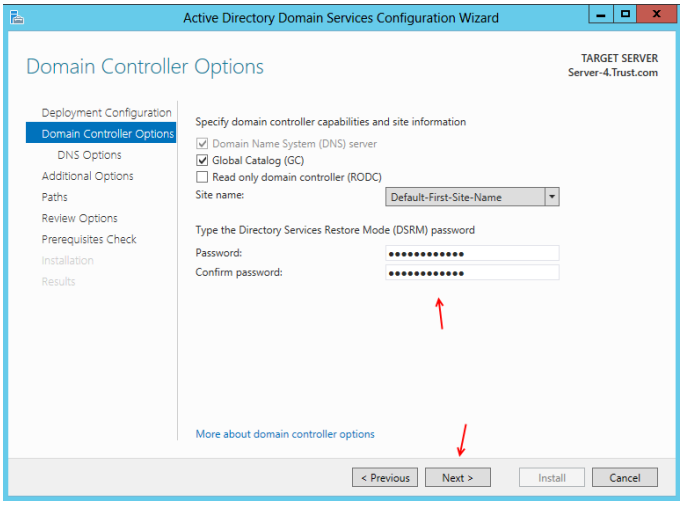
در شکل ۸-۱۳۹٤، گزینه Add a domain controller to an existing domain را انتخاب و در قسمت Domain نام دومین خود را به مانند شکل وارد کنید و در قسمت Supply the cre… یک نام کاربری که در دومین 3isco.ir اعتبار دارد را وارد کنید و بر روی Next کلیک کنید.

www.takbook.com



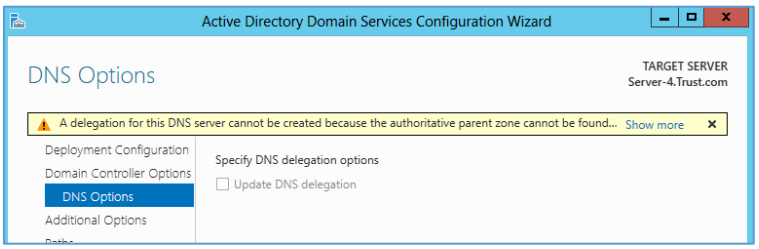
شکل ۸- ۱۳۹۴ انتقال اطلاعات *Active Directory*

در شکل ۸-۱۳۹۵، رمز عبور برای Restore Mode وارد کنید و بر روی Next کلیک کنید.



شکل ۸- ۱۳۹۵ انتقال اطلاعات *Active Directory*

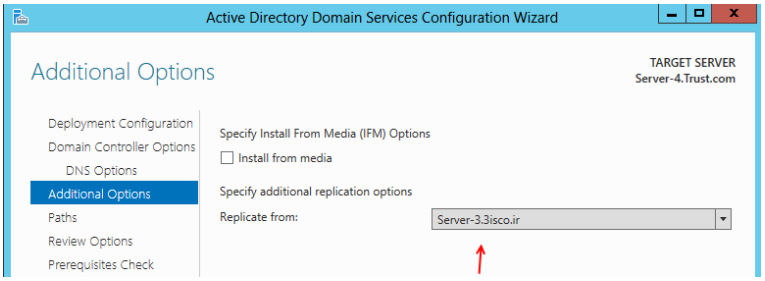
در شکل ۸-۱۳۹۶، بر روی Next کلیک کنید.



شکل ۸- ۱۳۹۶ انتقال اطلاعات *Active Directory*

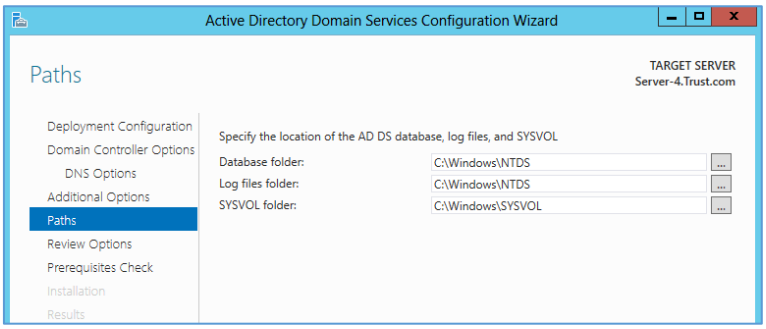
www.takbook.com

در شکل ۸–۱۳۹۷، از قسمت Replicate from از منوی کشویی سرور موردنظر خود که دومین 3isco.ir روی آن فعال است را انتخاب کنید.Server-3 نام سروری است که دومین روی آن فعال است، بر روی Next کلیک کنید.



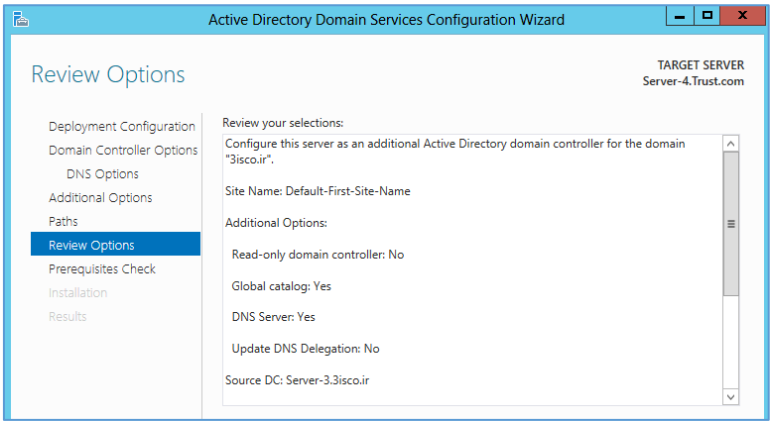
شکل ۸– ۱۳۹۷ انتقال اطلاعات Active Directory

در شکل ۸–۱۳۹۸، بر روی Next کلیک کنید.



شکل ۸– ۱۳۹۸ انتقال اطلاعات Active Directory

در شکل ۸–۱۳۹۹، بر روی next کلیک کنید.



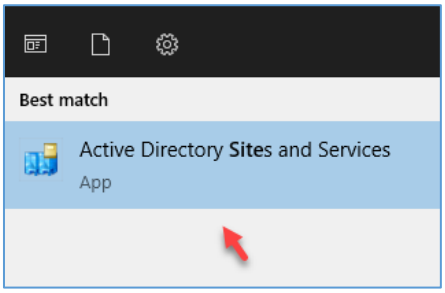
شکل ۸– ۱۳۹۹ انتقال اطلاعات Active Directory

در صفحه آخر هم بر روی Install کلیک کنید تا دومین موردنظر فعال شود.

www.takbook.com

بعد از این که تنظیمات موردنظر را انجام دادید، تمام اطلاعات از دومین اصلی یعنی3isco.ir به سرور دوم انتقال داده می‌شود، اگر هم یک کاربر ایجاد کنید چند ثانیه بعد این کاربر به سرور دوم انتقال داده می‌شود، به نظرشما کار انتقال اطلاعات Active را چه سرویسی انجام می‌دهد؟

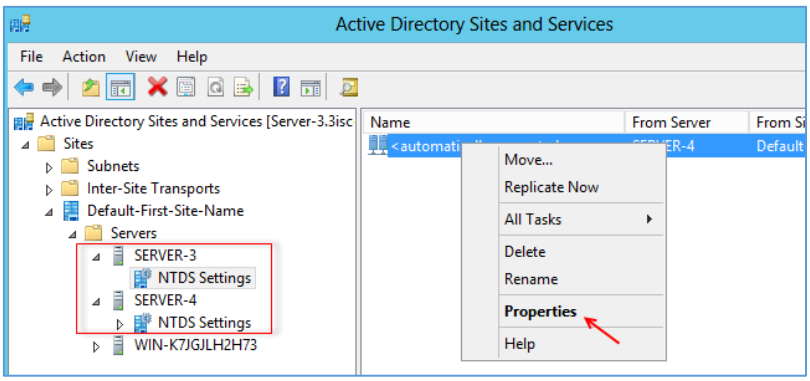
کار انتقال اطلاعات بین دو سرور توسط سرویس Site and Service انجام می‌شود که برای اجرای آن وارد سرور اصلی که دومین 3isco.ir روی آن قرار دارد شوید و در Search به مانند شکل ۸-۱۴۰۰، سرویس Site And Service را اجرا کنید.



شکل ۸- ۱۴۰۰ انتقال اطلاعات *Active Directory*

همان‌طور که در شکل ۸-۱۴۰۱، مشاهده می‌کنید سرویس موردنظر اجرا شده است، اگر از سمت چپ وارد Server شوید مشاهده می‌کنید که دو سرور با نام‌های Server-3 و Server-4 ایجاد شده است که ارتباط بین دو سرور از این طریق انجام می‌شود.

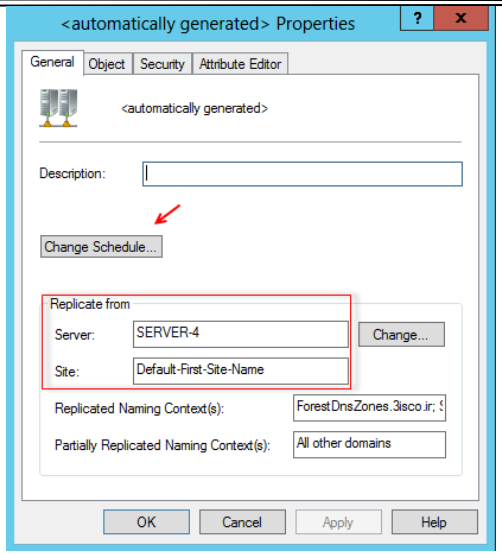
اگر برروی NTDS Settings در قسمت Server- 3 کلیک کنید در صفحه باز شده بر روی <Automatically generated> کلیک راست کنید و Propertoes را انتخاب کنید.



شکل ۸- ۱۴۰۱ انتقال اطلاعات *Active Directory*

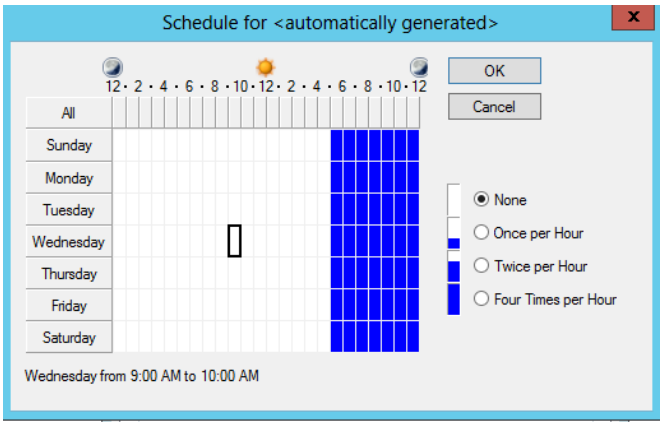
در شکل ۸-۱۴۰۲، اگر به قسمت Replicate from توجه کنید نام سرور را Server-4 می‌باشد و در قسمت Site نام Link ارتباطی به صورت پیش فرض وارد شده است. برای اینکه مشخص کنید که چه زمانی اطلاعات Active Directory بین دو سرور انتقال داده شود، بر روی Change Schedule کلیک کنید.

www.takbook.com



شکل ۸- ۱۴۰۲ انتقال اطلاعات *Active Directory*

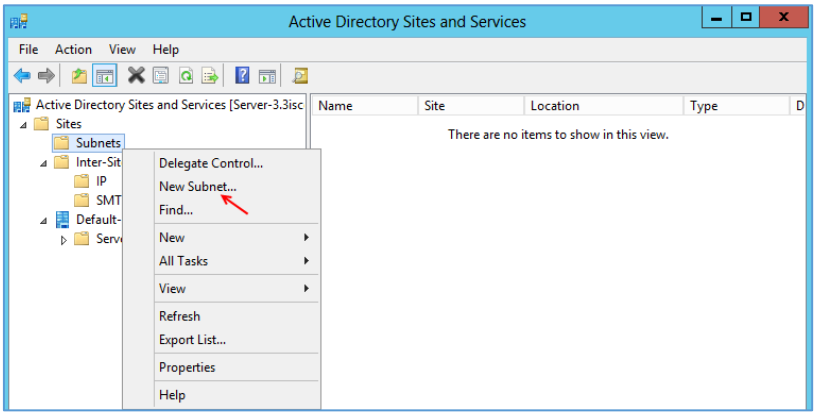
در شکل ۸-۱۴۰۳، با بررسی شرایط سازمان خود ساعات و روزهای مورد نیاز خود را برای انتقال اطلاعات بین دو سرور را انتخاب کنید، سعی کنید این کار را در ساعات کم کاری انجام دهید، اگر همه مستطیل‌های موردنظر را انتخاب کنید و بر روی None کلیک کنید همه آنها به رنگ سفید در می‌آیند.



شکل ۸- ۱۴۰۳ انتقال اطلاعات *Active Directory*

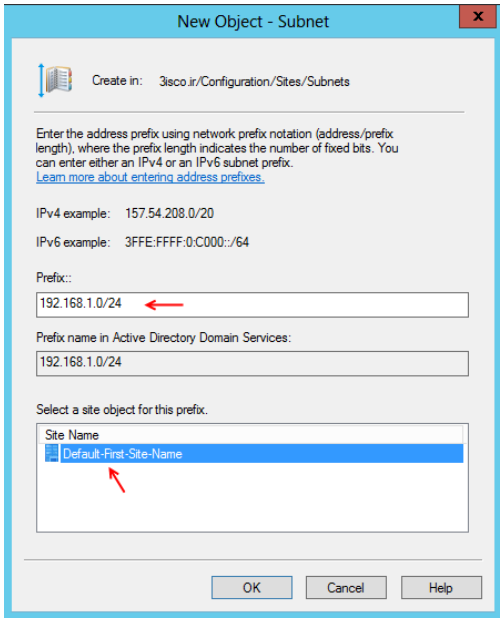
بعد از انجام عملیات بالا از سمت چپ به مانند شکل ۸-۱۴۰۴، بر روی Subnets کلیک راست کنید و گزینه‌ی New Subnet را انتخاب کنید، این قسمت برای تعریف Subnet شبکه موردنظر می‌باشد.

www.takbook.com



شکل ۸- ۱۴۰۴ انتقال اطلاعات *Active Directory*

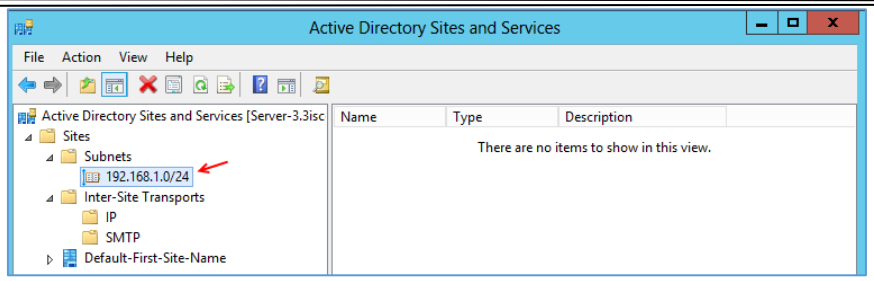
در شکل ۸–۱٤۰۵، در قسمت Prefix آدرس Net شبکه خود را وارد کنید، یعنی اگر آدرس به صورت 192.168.1.102 و subnet به صورت 255.255.255.0 بود سه تا 255 به این معنی است که سه قسمت اول IP ثابت است و چون هر قسمت ۸ بیتی است ۳ تا ۸ تا می‌شود ۲٤ بیت که آدرس به صورت 192.168.1.0/24 وارد می‌کنیم. بعد از وارد کردن اطلاعات Site Name را انتخاب و بر روی ok کلیک کنید.



شکل ۸- ۱۴۰۵ انتقال اطلاعات *Active Directory*

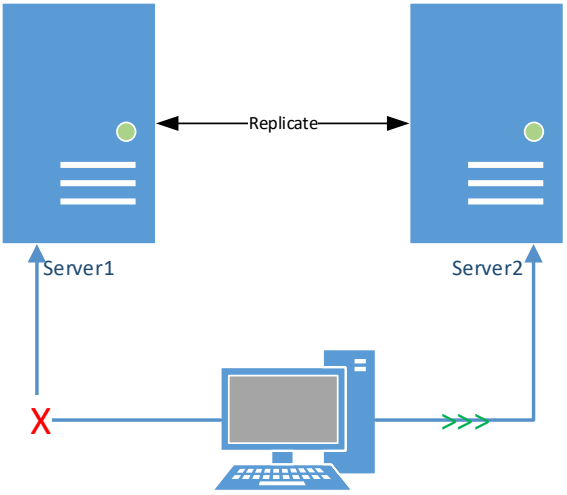
همان‌طور که در شکل ۸–۱٤۰٦، مشاهده می‌کنید Subnet موردنظر ایجاد شده است، توجه داشته باشید با ایجاد Subnet در یکی از سرورها در سرور دیگر هم این Subnet به صورت خودکار ایجاد می‌شود.

www.takbook.com



شکل ۸- ۱۴۰۶ انتقال اطلاعات *Active Directory*

بیشترین کاربرد این سرویس این است که تمام اطلاعات موجود در سرور اصلی که در اینجا Server1 می‌باشد به Server2 انتقال داده می‌شود و اگر چنانچه server1 کارایی خود را از دست بدهد، به مانند شکل ۸-۱۴۰۷، شبکه به هیچ عنوان قطع نخواهد شد و تمام کاربران به Server 2 منتقل می‌شوند.



شکل ۸- ۱۴۰۷ انتقال اطلاعات *Active Directory*

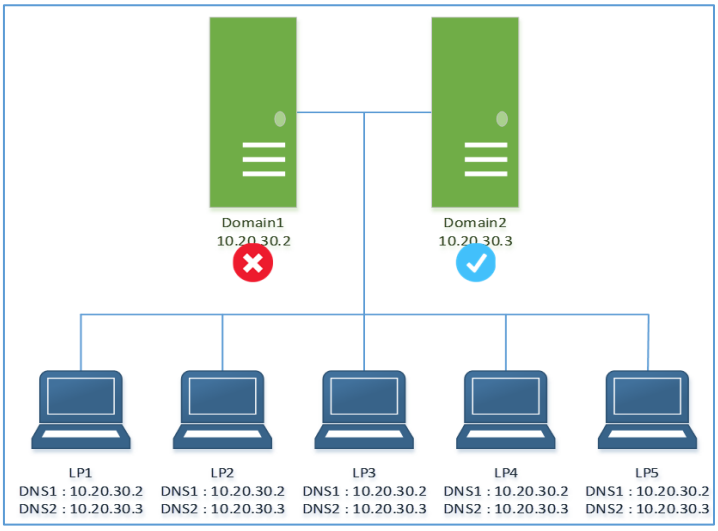
www.takbook.com

۸-۳-٤٥ ایجاد failover در Domain و DHCP

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 باشید.

Failover به معنای ایجاد یک سیستم پشتیبان یا جایگزین برای سرویس‌ها یا سرورها است تا در صورت بروز مشکل در سرور اصلی (مانند خرابی سخت‌افزاری، نرم‌افزاری یا قطع شدن ارتباط)، سرویس به‌صورت خودکار یا دستی به سرور پشتیبان منتقل شود. هدف از Failover، کاهش زمان از کارافتادگی (downtime) و افزایش دسترس‌پذیری (high availability) سیستم‌ها است.

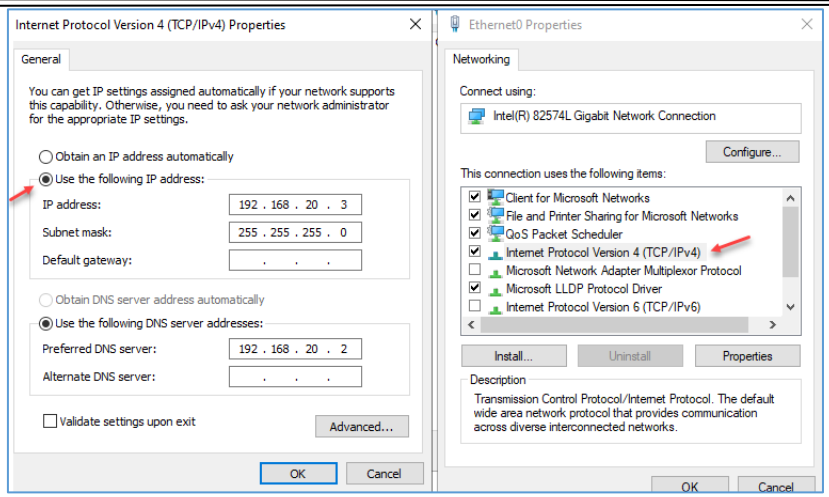
در شکل ۸-۱٤۰۸، دو سرور دومین در شبکه فعّال است و از طریق سرویس DHCP، آدرس آنها به کلاینت‌ها داده شده است، اگر چنانچه Domain1 با آدرس 10.20.30.2 ارتباطش قطع شود، Domain 2 با آدرس 10.20.30.3، شبکه را پایدار نگه می‌دارد و کاربران می‌توانند از این سرور سرویس بگیرند، این تجربه در شبکه برای بنده اتّفاق افتاده است که با این روش به راحتی توانستم مشکل را حل کنم.



شکل ۸- ۱۴۰۸ ایجاد failover در Domain و DHCP

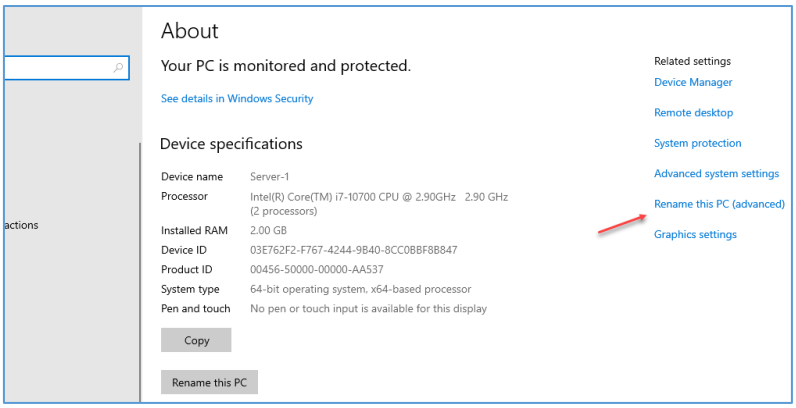
برای این کار باید از سرور اصلی یک Clone تهیه کنیم، برای این منظور، ما یک سرور دیگر با مشخّصات سرور دومین اصلی آماده کردیم و ویندوز سرور ۲۰۲۵ را بر روی آن نصب کردیم و به مانند شکل ۸-۱٤۰۹، بر روی آن، آدرس 192.168.20.3 را set کردیم، توجّه داشته باشید آدرس DNS اوّل را باید آدرس سرور DC که همان، 192.168.20.2 است وارد کنید و در قسمت دوّم باید آدرس خود سرور را وارد کنید یا می‌توانید به جای آدرس 192.168.20.3 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.

www.takbook.com



شکل ۸- ۱۴۰۹ ایجاد failover در Domain و DHCP

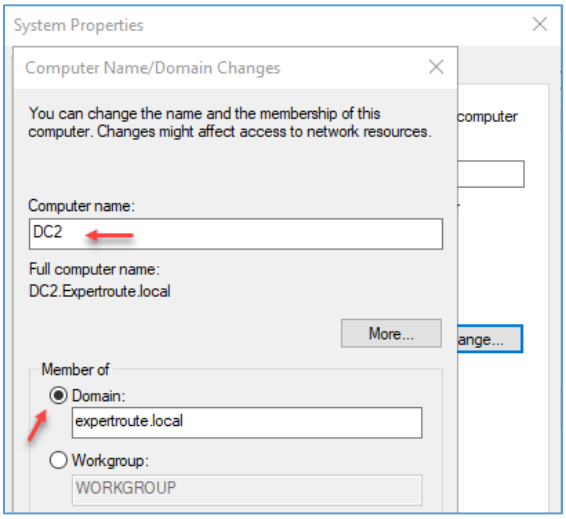
به مانند شکل ۸-۱٤۱۰، وارد صفحه About شوید و بر روی Rename this PC کلیک کنید، برای اینکه این صفحه را مشاهده کنید می‌توانید از کلید ترکیبی پنجره و Pause استفاده کنید.



شکل ۸- ۱۴۱۰ ایجاد failover در Domain و DHCP

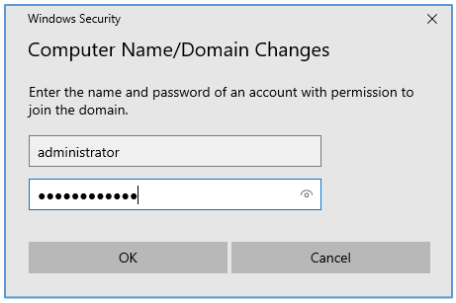
در شکل ۸-۱٤۱۱، واردComputer Name شوید و بر روی Change کلیک کنید و نام سرور را DC2 و نام دومین را، ExpertRoute.local وارد و بر روی OK کلیک کنید.

www.takbook.com



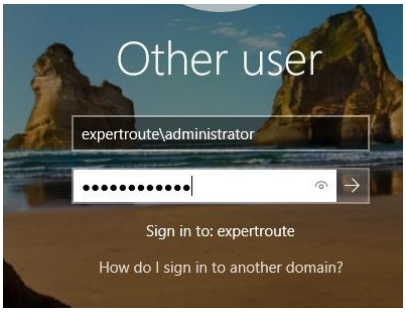
شکل ۸- ۱۴۱۱ ایجاد failover در Domain و DHCP

بعد از این کار، به مانند شکل ۸-۱٤۱۲، رمز عبور کاربر Administrator را وارد و بعد، سرور را Restart کنید.



شکل ۸- ۱۴۱۲ ایجاد failover در Domain و DHCP

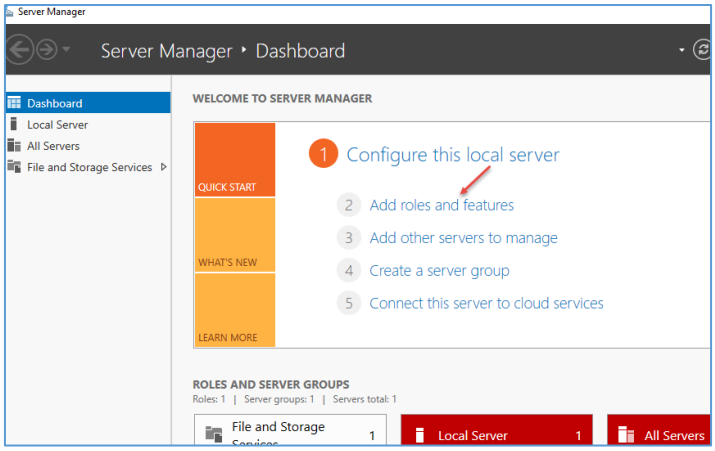
بعد از اینکه سرور را عضو دومین کردید باید سرویس Active directory را بر روی آن راه‌اندازی کنید تا به دومین اصلی متّصل شوید.



شکل ۸- ۱۴۱۳ ایجاد failover در Domain و DHCP

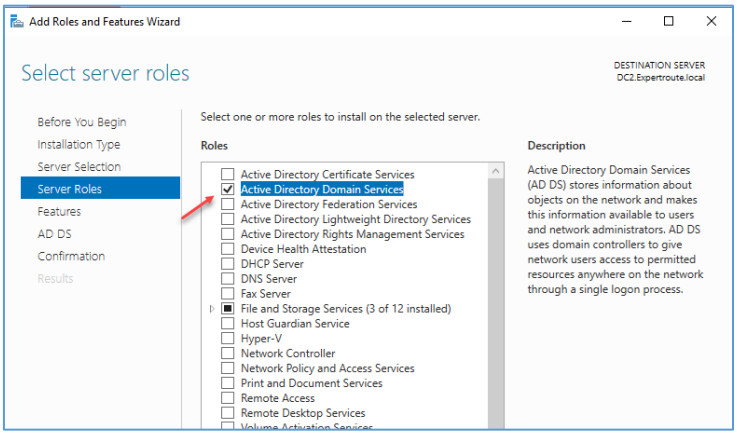
www.takbook.com

به مانند شکل ۸–۱٤۱٤، وارد Server Manager شوید و بر روی Add role and Features کلیک کنید.



شکل ۸- ۱۴۱۴ ایجاد *failover* در *Domain* و *DHCP*

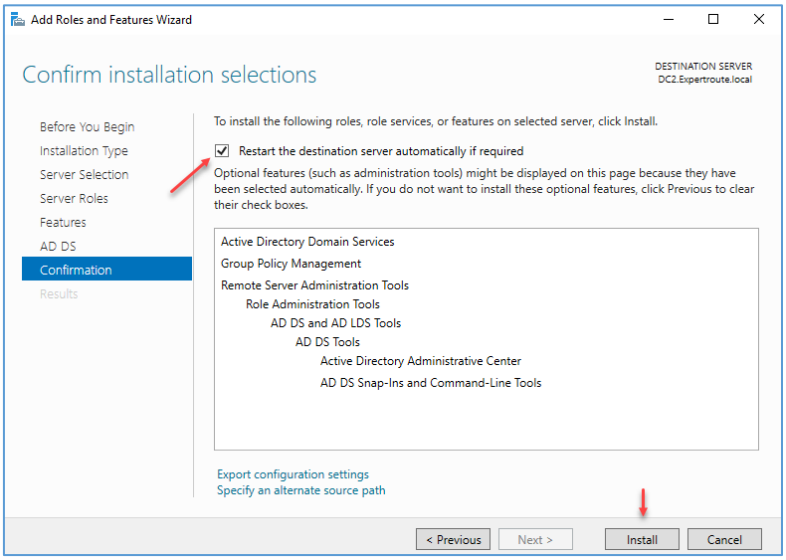
به مانند شکل ۸–۱٤۱٥، وارد Server Roles شوید و از لیست سرویس‌ها، گزینه‌ی Active directory domain and Services را انتخاب و بر روی Next کلیک کنید.



شکل ۸- ۱۴۱۵ ایجاد *failover* در *Domain* و *DHCP*

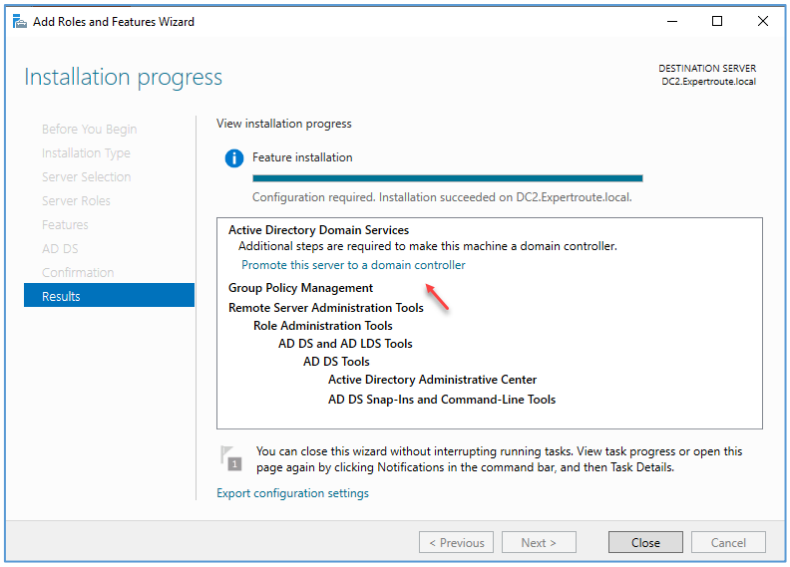
به مانند شکل ۸–۱٤۱٦، بر روی Next کلیک کنید تا به صفحه‌ی مورد نظر برسید و بر روی Install کلیک کنید تا سرویس نصب شود.

www.takbook.com



شکل ۸- ۱۴۱۶ ایجاد failover در Domain و DHCP

در شکل ۸-۱٤۱۷، بعد از نصب باید سرویس را تنظیم کنید، برای این کار بر روی Promote this server to a domain controller کلیک کنید.

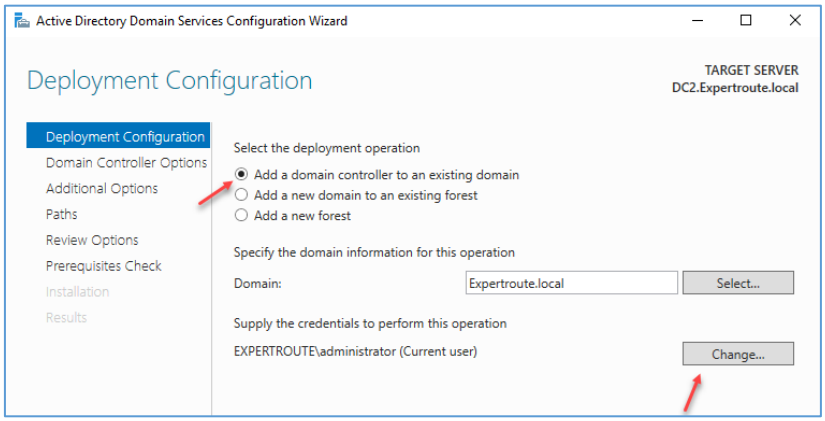


شکل ۸- ۱۴۱۷ ایجاد failover در Domain و DHCP

در شکل ۸-۱٤۱۸، چون از قبل دومین فعّال شده است باید گزینه‌ی اوّل را انتخاب کنید و در قسمت Domain باید بررسی کنید که نام دومین (ExpertRoute.ir) درست انتخاب شده است یا نه، در قسمت آخر نیز باید

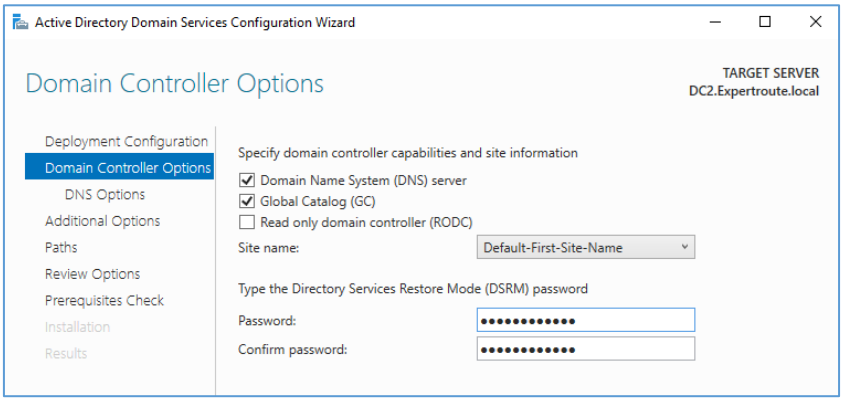
www.takbook.com

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.



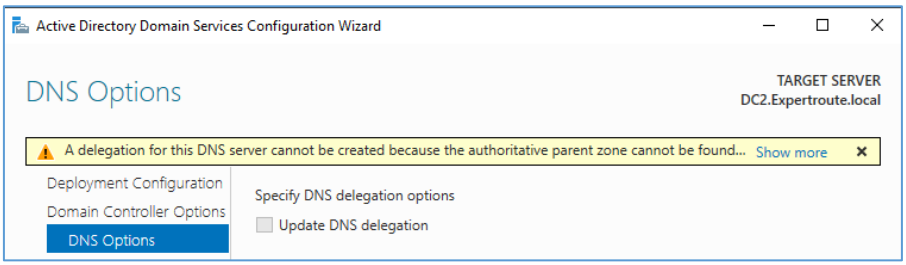
شکل ۸- ۱۴۱۸ ایجاد failover در Domain و DHCP

در شکل ۸-۱۴۱۹، 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.



شکل ۸- ۱۴۱۹ ایجاد failover در Domain و DHCP

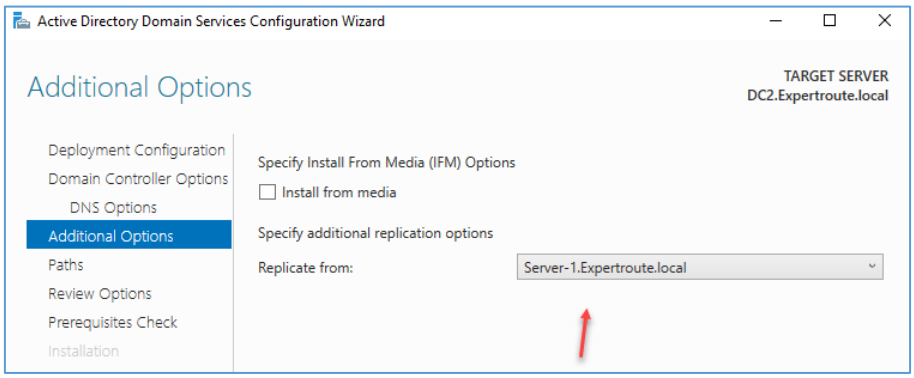
در شکل ۸-۱۴۲۰، بر روی Next کلیک کنید.



شکل ۸- ۱۴۲۰ ایجاد failover در Domain و DHCP

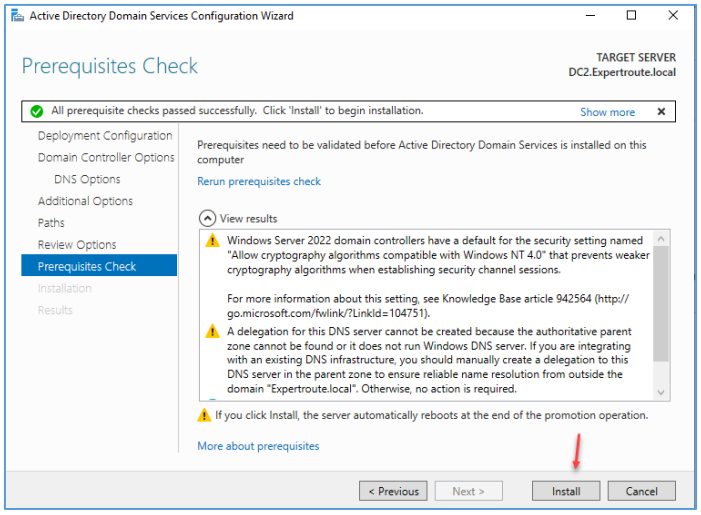
www.takbook.com

به مانند شکل ۸-۱۴۲۱، 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، این موضوع را در چند قسمت قبلی بررسی کردیم.



شکل ۸- ۱۴۲۱ ایجاد failover در Domain و DHCP

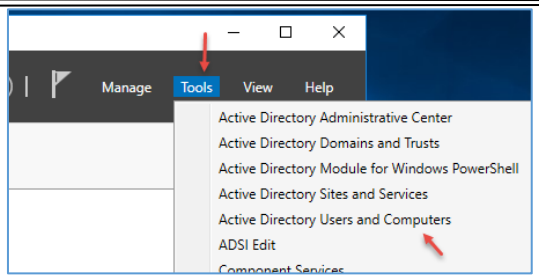
بر روی Next کلیک کنید تا به صفحه‌ی شکل ۸-۱۴۲۲ برسید، در این صفحه، پیش‌نیازها بررسی می‌شود و اگر اوکی بود، اجازه‌ی نصب سرویس صادر می‌شود؛ بر روی Install کلیک کنید تا کار آغاز شود.
بعد از نصب، سرور را Restart کنید.



شکل ۸- ۱۴۲۲ ایجاد failover در Domain و DHCP

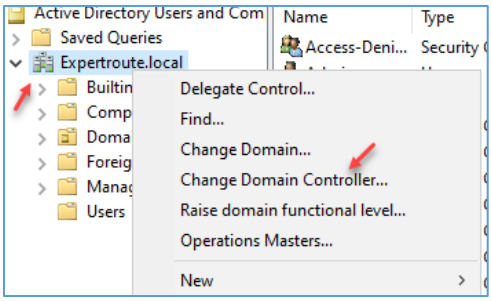
بعد ار ورود به سرور DC2 می‌توانید سرویس‌های اضافه شده به Server Manager را مشاهده کنید.
به مانند شکل ۸-۱۴۲۳، بر روی Active Directory Users and computers کلیک کنید.

www.takbook.com



شکل ۸- ۱۴۲۳ ایجاد failover در Domain و DHCP

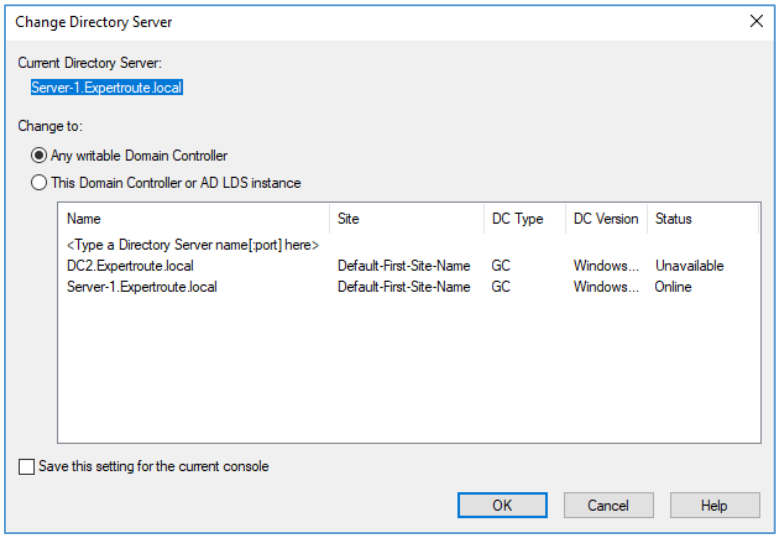
در شکل ۸–۱٤۲٤، بر روی نام دومین خود کلیک راست کنید و گزینه‌ی Change Domain Controller را انتخاب کنید.



شکل ۸- ۱۴۲۴ ایجاد failover در Domain و DHCP

به مانند شکل ۸–۱٤۲٥، 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.

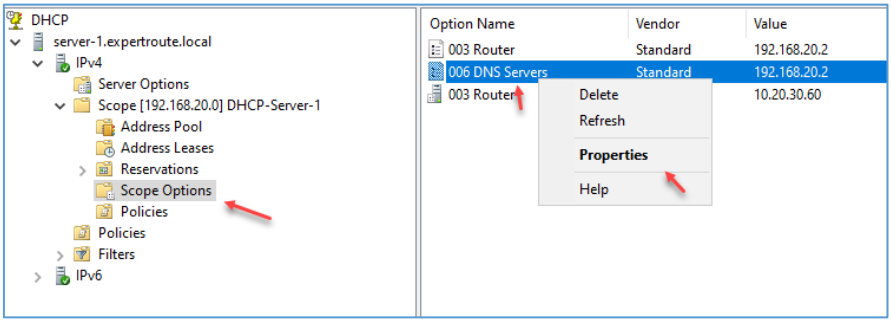
www.takbook.com



شکل ۸- ۱۴۲۵ ایجاد failover در Domain و DHCP

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 192.168.20.3 ایجاد شده است.

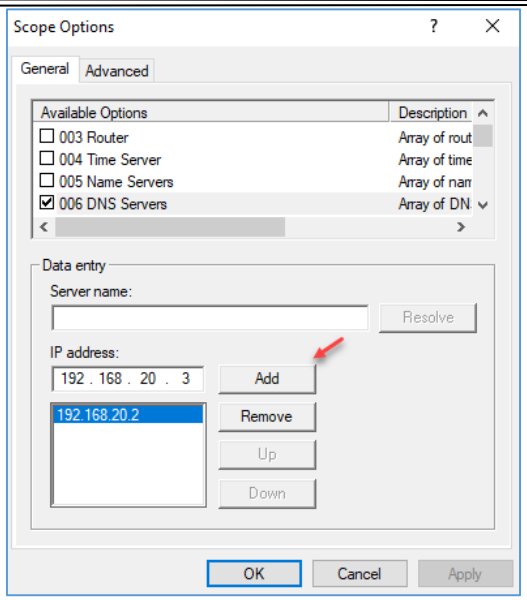
به مانند شکل ۸-۱٤۲٦، وارد سرور اوّل، AD شوید و سرویس DHCP را اجرا کنید و به مانند شکل در Scope مورد نظر بر روی Scope Options کلیک کنید و در صفحه‌ی باز شده بر روی DNS Server کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۱۴۲۶ ایجاد failover در Domain و DHCP

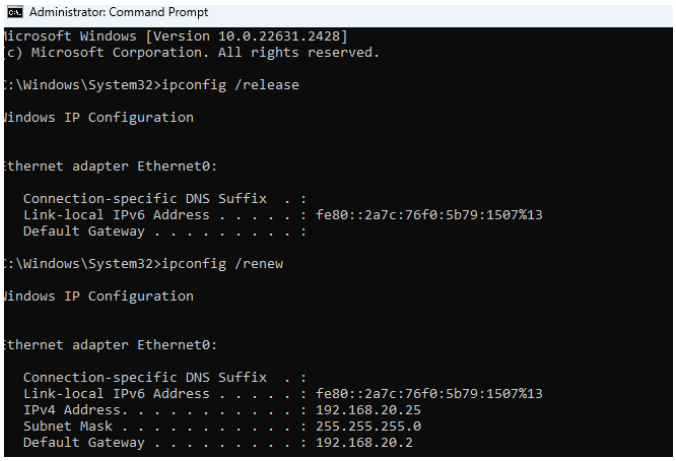
در شکل ۸-۱٤۲۷، باید آدرس سرور دومین DC2 را وارد و بر روی Add کلیک کنید، توجّه داشته باشید با کلیدهای UP و Down می‌توانید اولویّت سرورها را تغییر دهید، سعی کنید سرور اصلی، اوّل و سرور فرعی، دوّم باشد، بر روی OK کلیک کنید تا تنظیمات جدید اعمال شود.

www.takbook.com



شکل ۸- ۱۴۲۷ ایجاد *failover* در *Domain* و *DHCP*

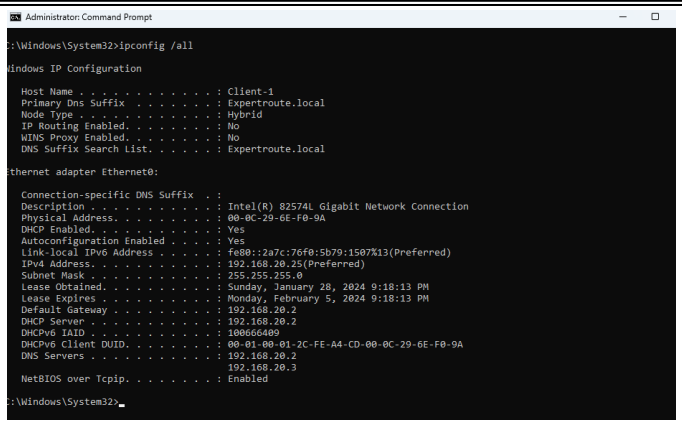
بعد از انجام کار وارد یکی از کلاینت‌ها شوید و برای اینکه آخرین تغییرات را به صورت سریع از سرویس DHCP دریافت کنید به مانند شکل ۸–۱٤۲۸، از دستور Ipconfig /release و بعد، از دستور ipconfig /Renew استفاده کنید.



شکل ۸- ۱۴۲۸ ایجاد *failover* در *Domain* و *DHCP*

همان‌طور که در شکل ۸–۱٤۲۹، 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.

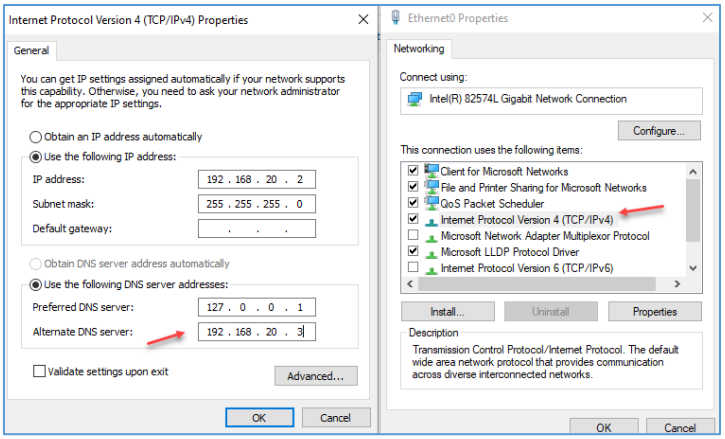
www.takbook.com



شکل ۸- ۱۴۲۹ ایجاد failover در Domain و DHCP

یک نکته‌ی مهم این است که به مانند شکل ۸-۱۴۳۰، بعد از انجام کارهای بالا در سرور اوّل، آدرس سرور دوّم را نیز وارد کنید تا همه چیز اوکی شود.

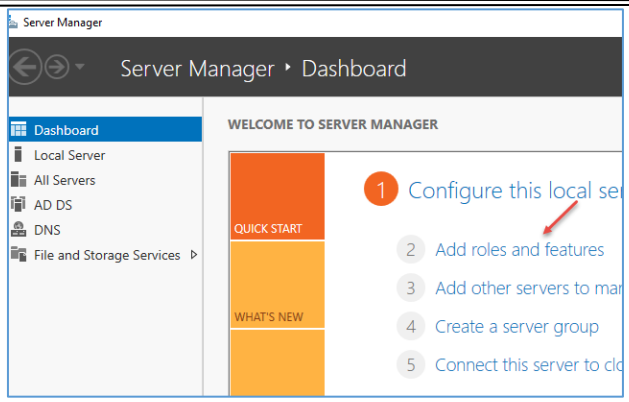
با این کار، هر دو سرور مکمّل هم خواهند بود و با قطع شدن یکی از آنها، دیگری به کاربران در شبکه سرویس خواهد داد.



شکل ۸- ۱۴۳۰ ایجاد failover در Domain و DHCP

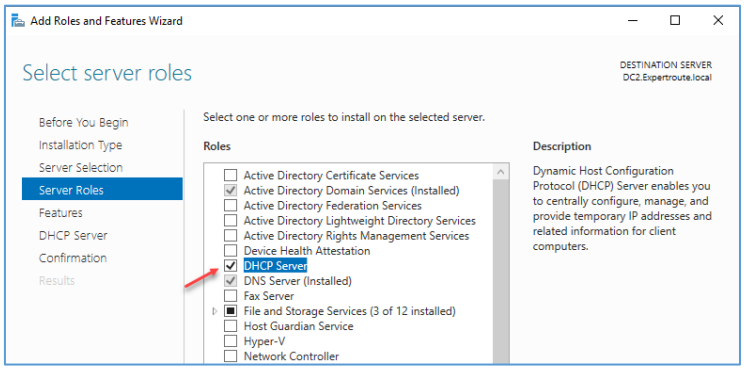
برای اینکه یک مجموعه‌ی کامل از سرویس‌ها را در هر دو سرور داشته باشید باید سرویس DHCP را روی سرور DC2 نصب کنید و آن را با سرویس DHCP سرور AD هماهنگ‌سازی کنید که در این قسمت، آن را انجام خواهیم داد؛ به مانند شکل ۸-۱۴۳۱، وارد Server Manager در سرور DC2 شوید و بر روی Add role and Features کلیک کنید.

www.takbook.com



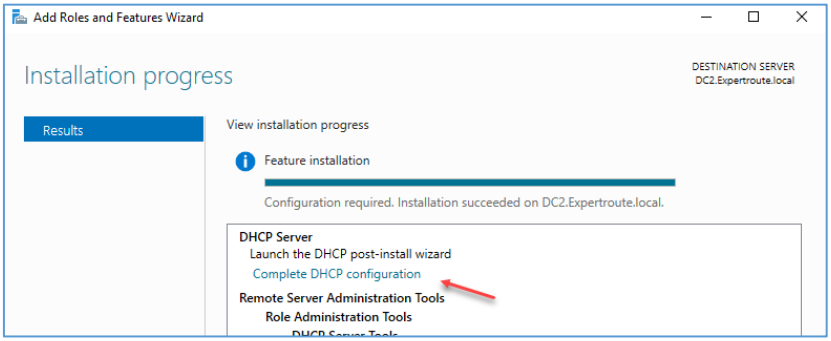
شکل ۸- ۱۴۳۱ ایجاد failover در Domain و DHCP

به مانند شکل ۸-۱٤۳۲، 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.



شکل ۸- ۱۴۳۲ ایجاد failover در Domain و DHCP

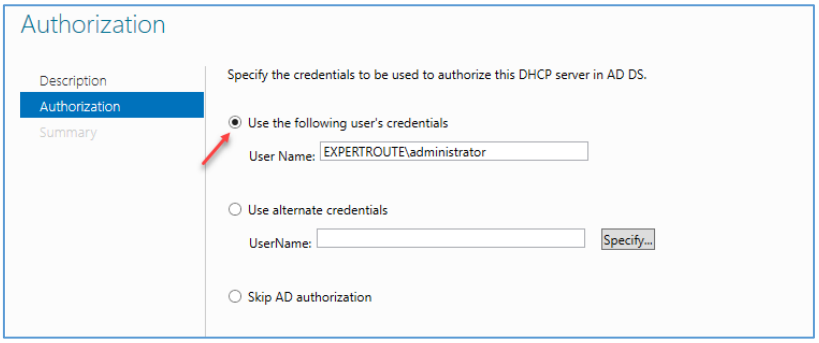
در شکل ۸-۱٤۳۳، برای کامل کردن سرویس DHCP بر روی گزینه‌ی مشخّص‌شده، کلیک کنید.



شکل ۸- ۱۴۳۳ ایجاد failover در Domain و DHCP

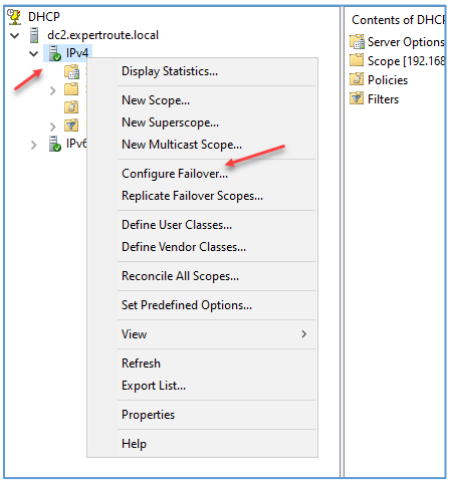
www.takbook.com

در کل ۸-۱٤۳٤، 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.



شکل ۸- ۱۴۳۴ ایجاد failover در Domain و DHCP

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 ۸-۱٤۳٥، بر روی IPv4 کلیک راست و گزینه‌ی Configure Failover را انتخاب کنید.

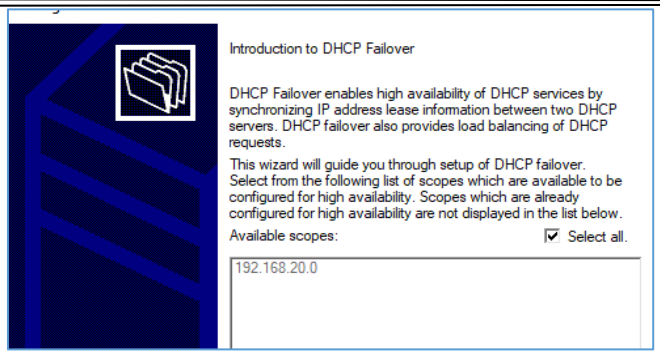


شکل ۸- ۱۴۳۵ ایجاد failover در Domain و DHCP

در شکل ۸-۱٤۳٦، Scope شما که 192.168.20.0 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.

www.takbook.com



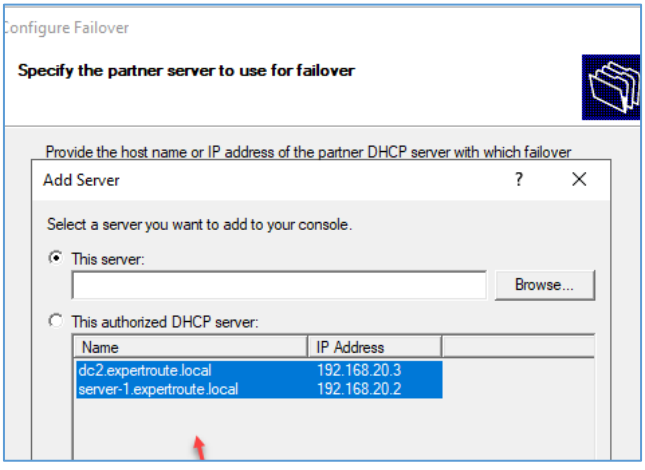
شکل ۸- ۱۴۳۶ ایجاد *failover* در *Domain* و *DHCP*

در شکل ۸-۱٤۳۷، باید سرور دوّم، یعنی DC2 که روی آن سرویس DHCP را فعّال کردید را انتخاب و بر روی Add Server کلیک کنید.



شکل ۸- ۱۴۳۷ ایجاد *failover* در *Domain* و *DHCP*

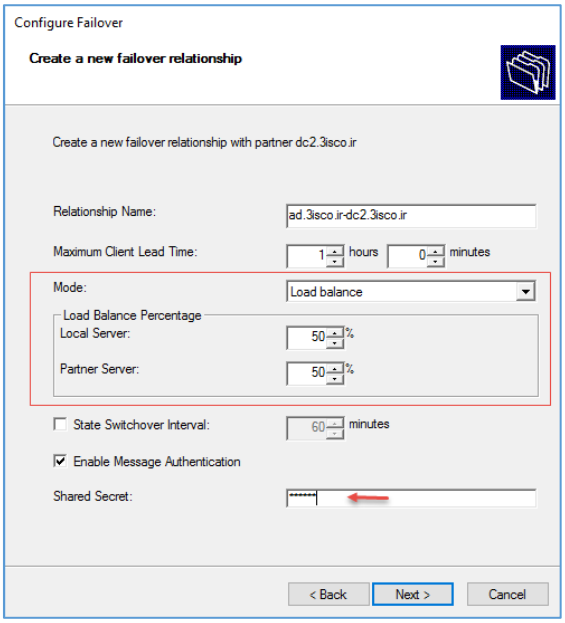
در شکل ۸-۱٤۳۸، با کلیک بر روی دکمه‌ی Browse می‌توانید سرور دوّم، DC2 را به لیست، اضافه و بر روی OK کلیک کنید و در صفحه‌ی قبل بر روی Next کلیک کنید.



شکل ۸- ۱۴۳۸ ایجاد *failover* در *Domain* و *DHCP*

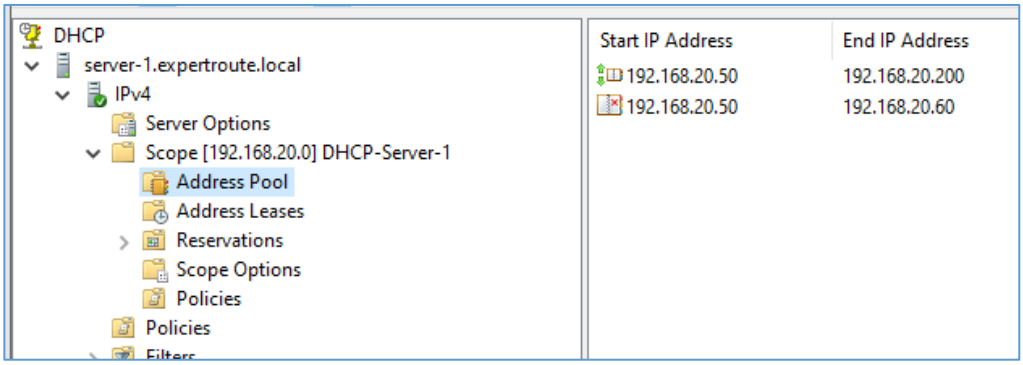
www.takbook.com

در شکل ۸-۱۴۳۹، 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.



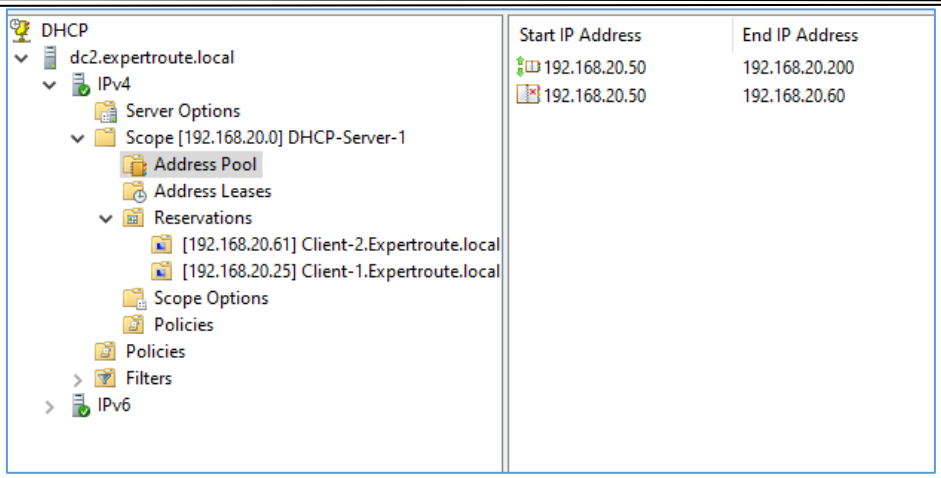
شکل ۸- ۱۴۳۹ ایجاد failover در Domain و DHCP

همان‌طور که در شکل‌های ۸-۱۴۴۰ و ۸-۱۴۴۱، مشاهده می‌کنید، در هر دو سرور، سرویس DHCP فعّال شده است و هم‌زمان به شبکه سرویس می‌دهند.



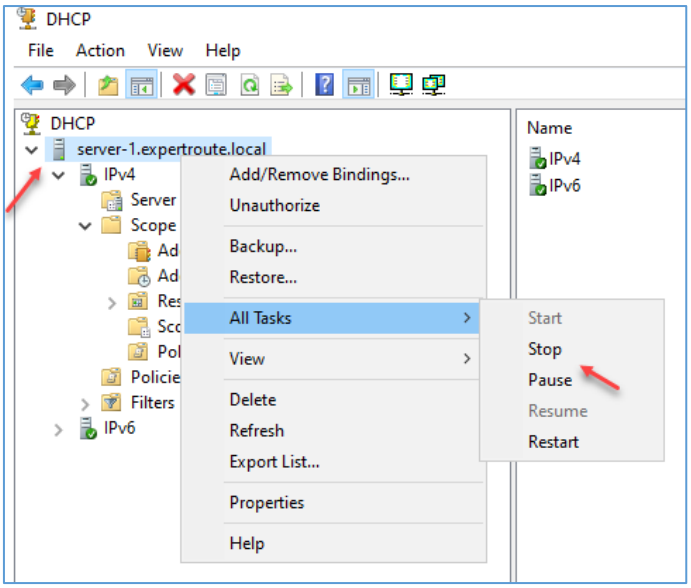
شکل ۸- ۱۴۴۰ ایجاد failover در Domain و DHCP

www.takbook.com



شکل ۸- ۱۴۴۱ ایجاد *failover* در *Domain* و *DHCP*

حال، اگر در سرور AD، سرویس DHCP را به مانند شکل ۸-۱٤٤۲، Stop کنید، سرور DC2 به کار خود ادامه خواهد داد و شبکه با مشکلی مواجه نخواهد شد.



شکل ۸- ۱۴۴۲ ایجاد *failover* در *Domain* و *DHCP*

در شکل ۸-۱٤٤۳، کلاینت با دستور ipconfig /release درخواست IP داده است که سرور اصلی، یعنی ۱۹۲.۱٦۸.۲۰.۲ 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 ۱۹۲.۱٦۸.۲۰.۳ (DC2) که در شکل ۸-۱٤٤٤، مشخّص شده است به آن IP تخصیص داده است.

www.takbook.com


```
C:\Users\101>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Client-1
   Primary Dns Suffix  . . . . . . . : Expertroute.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : Expertroute.local

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-6E-F0-9A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2a7c:76f0:5b79:1507%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.20.25(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, January 28, 2024 9:18:13 PM
   Lease Expires . . . . . . . . . . : Monday, February 5, 2024 9:18:13 PM
   Default Gateway . . . . . . . . . : 192.168.20.2
   DHCP Server . . . . . . . . . . . : 192.168.20.2
   DHCPv6 IAID . . . . . . . . . . . : 100666409
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-FE-A4-CD-00-0C-29-6E-F0-9A
   DNS Servers . . . . . . . . . . . : 192.168.20.2
                                       192.168.20.3
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\101>ipconfig /release
```

شکل ۸- ۱۴۴۳/ ایجاد failover در Domain و DHCP

```
Select Command Prompt
C:\Users\101>
C:\Users\101>ipconfig /renew

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2a7c:76f0:5b79:1507%13
   IPv4 Address. . . . . . . . . . . : 192.168.20.25
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.20.2

C:\Users\101>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Client-1
   Primary Dns Suffix  . . . . . . . : Expertroute.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : Expertroute.local

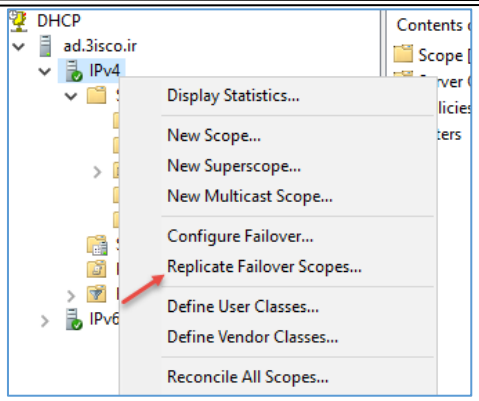
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-6E-F0-9A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2a7c:76f0:5b79:1507%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.20.25(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, January 28, 2024 10:40:59 PM
   Lease Expires . . . . . . . . . . : Monday, February 5, 2024 10:40:59 PM
   Default Gateway . . . . . . . . . : 192.168.20.2
   DHCP Server . . . . . . . . . . . : 192.168.20.3
   DHCPv6 IAID . . . . . . . . . . . : 100666409
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-FE-A4-CD-00-0C-29-6E-F0-9A
   DNS Servers . . . . . . . . . . . : 192.168.20.2
```

شکل ۸- ۱۴۴۴/ ایجاد failover در Domain و DHCP

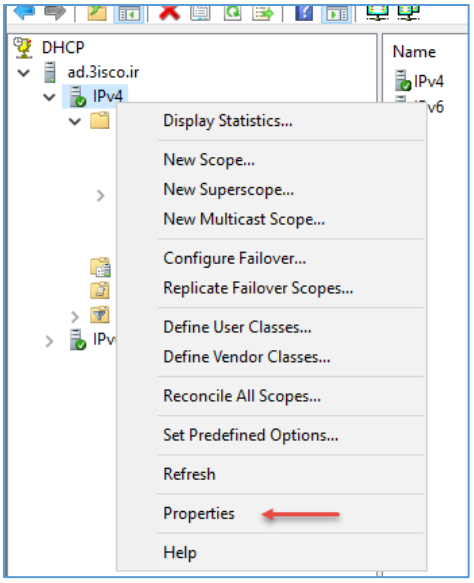
اگر بخواهید دو سرور DHCP، آخرین تغییرات را به صورت سریع به هم ارسال کنند باید بر روی IPv4 کلیک راست کنید و به مانند شکل ۸-۱٤٤٥، بر روی Replicate Failover Scopes کلیک کنید و در شکل باز شده بر روی Yes کلیک کنید تا آخرین تغییرات بین دو سرور با هم ردّ و بدل شود.

www.takbook.com



شکل ۸- ۱۴۴۵ ایجاد failover در Domain و DHCP

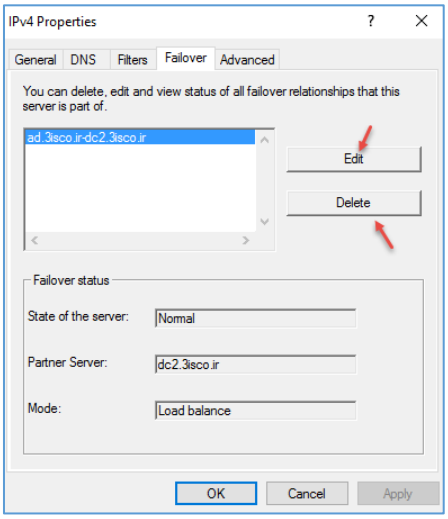
حال، اگر بخواهید تنظیمات Failover را در هر دو سرور تغییر دهید و یا اینکه آن را حذف کنید باید به مانند شکل ۸-۱٤٤٦، بر روی IPv4 کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۸- ۱۴۴۶ ایجاد failover در Domain و DHCP

در شکل ۸-۱٤٤۷، 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 غیرفعّال کنید باید بر روی Delete کلیک کنید.

www.takbook.com



شکل ۸- ۱۴۴۷/ایجاد failover در Domain و DHCP

www.takbook.com

www.takbook.com

فصل نهم

بررسی نرم‌افزار مانیتورینگ

در این بخش به طور خاص می‌خواهیم ابزارهای مانیتورینگ را بررسی کنیم و نرم‌افزار و دستگاهایی که نیاز به مانیتورینگ دارند را تنظیم و بررسی کنیم.
نرم‌افزارهای مانیتورینگ گسترده هستند و هر کدام ویژگی خاص خودشان را دارند، اما تجربه خودم از ابزارهای مانیتورینگ به این چهار نرم‌افزار ختم می‌شود.

۱- PRTG
۲- ZABBIX
۳- ManageEngine
۴- SolarWinds

هر کدام از این نرم‌افزارها داری ویژگی خاصی هستند که می‌توانیم برای کار خود انتخاب کنید، اما بیشترین نرم‌افزاری که دوستان مدیر شبکه از آن استفاده می‌کنند ZABBIX و PRTG است که در این کتاب PRTG را بررسی خواهیم کرد.

۹-۱ کار با نرم افزار PRTG

PRTG (Paessler Router Traffic Grapher) یک نرم‌افزار مانیتورینگ شبکه است که توسط شرکت Paessler توسعه یافته و برای نظارت بر زیرساخت‌های شبکه و سیستم‌های فناوری اطلاعات استفاده می‌شود. این نرم‌افزار به مدیران سیستم اجازه می‌دهد تا وضعیت سرورها، دستگاه‌های شبکه (مانند روترها، سوئیچ‌ها، و فایروال‌ها)، نرم‌افزارها، و سرویس‌های مختلف را به صورت بلادرنگ (real-time) مانیتور کنند.

ویژگی‌های کلیدی PRTG

- مانیتورینگ جامع شبکه: PRTG قادر است اجزای مختلف شبکه از جمله پهنای باند شبکه، زمان پاسخ‌دهی، مصرف CPU و RAM، استفاده از دیسک، سرویس‌های ابری و حتی سنسورهای IoT را مانیتور کند.
- نصب و پیکربندی آسان: PRTG دارای نصب سریع و رابط کاربری گرافیکی کاربرپسند است که برای کاربران با هر سطحی از دانش فنی قابل استفاده است.
- استفاده از سنسورها: PRTG بر پایه مفهوم "سنسور" کار می‌کند. هر سنسور یک پارامتر مشخص از دستگاه یا سرویس را نظارت می‌کند، مثلاً Ping، HTTP، SNMP، یا پهنای باند. هر دستگاه می‌تواند چندین سنسور داشته باشد.

www.takbook.com

- پشتیبانی از پروتکل‌های مختلف: این نرم‌افزار از پروتکل‌های مختلفی مانند SNMP (Simple Network Management Protocol)، WMI (Windows Management Instrumentation)، Flow (NetFlow, sFlow, jFlow)، و Ping پشتیبانی می‌کند.
- هشدارها و نوتیفیکیشن‌ها: PRTG در صورت بروز مشکلات (مثل قطعی شبکه، استفاده بیش از حد منابع، یا خطاهای سیستم)، هشدارهایی از طریق ایمیل، پیامک، یا اعلان‌های مختلف ارسال می‌کند.
- داشبوردهای سفارشی‌سازی‌شده: کاربران می‌توانند داشبوردهای بصری را مطابق با نیازهای خود تنظیم کنند و نمایشی کامل از شبکه و دستگاه‌هایشان داشته باشند.
- گزارش‌گیری و تحلیل: PRTG امکان ایجاد گزارش‌های جامع و دوره‌ای از عملکرد و سلامت شبکه و دستگاه‌ها را ارائه می‌دهد.

مزایا و معایب PRTG

مزایا:

- نصب و راه‌اندازی سریع و آسان.
- پشتیبانی از طیف وسیعی از دستگاه‌ها و پروتکل‌ها.
- قابلیت مانیتورینگ بلادرنگ با گراف‌های بصری و قابل فهم.
- ارائه گزارش‌ها و تحلیل‌های جامع.
- مدیریت هشدارها و نوتیفیکیشن‌های قابل تنظیم.

معایب:

- محدودیت در نسخه رایگان: نسخه رایگان PRTG به مانیتور کردن تا ۱۰۰ سنسور محدود است. برای شبکه‌های بزرگ‌تر، باید از نسخه‌های تجاری استفاده کرد.
- مصرف منابع: اگر شبکه بزرگی مانیتور شود، ممکن است PRTG از منابع سخت‌افزاری قابل توجهی استفاده کند.
- پیچیدگی برای شبکه‌های بسیار بزرگ: در شبکه‌های بسیار بزرگ و پیچیده، ممکن است پیکربندی و مدیریت PRTG زمان‌بر و چالش‌برانگیز باشد.

نسخه‌های PRTG

- نسخه رایگان: این نسخه امکان مانیتورینگ تا ۱۰۰ سنسور را به صورت رایگان فراهم می‌کند.

www.takbook.com

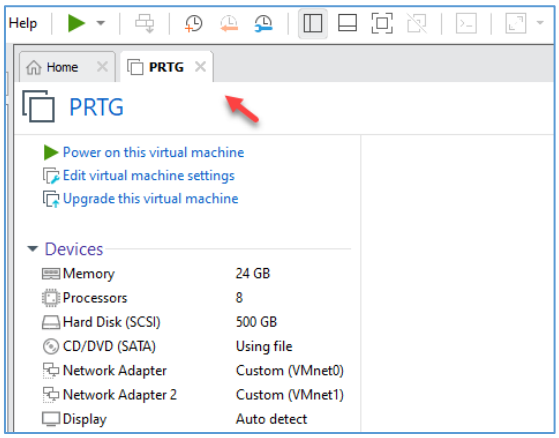
- نسخه‌های تجاری: برای شرکت‌هایی که نیاز به مانیتورینگ گسترده‌تری دارند، نسخه‌های تجاری PRTG با قابلیت مانیتور کردن هزاران سنسور موجود است. این نسخه‌ها به تناسب تعداد سنسورها قیمت‌گذاری می‌شوند.

نصب و راه‌اندازی PRTG

همان‌طور که بیان کردیم این نرم‌افزار دارای لایسنس‌های متعددی است که باید برای استفاده، آنها را تهیه کنید، ولی چون در ایران نمی‌توانیم برای آن هزینه کنیم می‌توانیم برای یادگیری از شرکت‌هایی با مانند Digiboy استفاده کنید که لینک دانلود آن را در زیر قرار دادیم، توجه داشته باشید در این لینک یک ماشین مجازی قرار داده شده که بر روی آن PRTG نصب و کرک شده است، شما می‌توانید آن را بر روی نرم‌افزار Vmware Workstaion یا ESXi اجرا کنید.

https://www.digiboy.ir/11799/prtg-network-monitor-21-0-x/

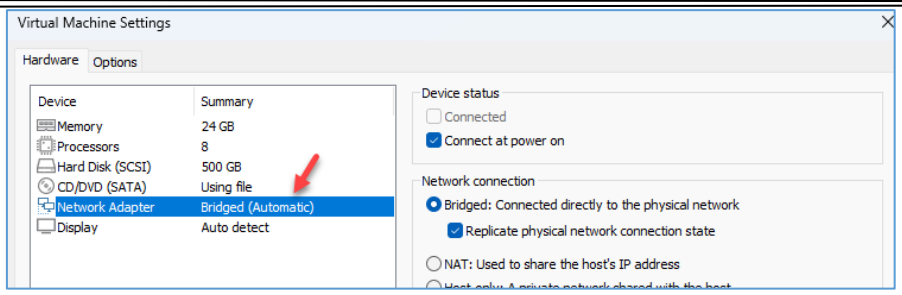
بعد از دانلود آن را اجرا کنید و در نرم‌افزار Vmware Workstation باز کنید، همان‌طور که در شکل ۹-۱، مشاهده می‌کنید ماشین مورد نظر باز شده است برای تنظیم سخت‌افزار آن بر روی Edit کلیک کنید.



شکل ۹- ۱ اجرای ماشین مجازی

به مانند شکل ۹-۲، می‌توانید مقدار RAM ، CPU را تغییر دهید و همچنین باید کارت شبکه‌ی شبکه داخلی سازمان خود را انتخاب کنید تا نرم‌افزار بتواند از به شبکه داخلی دسترسی داشته باشد و بتواند سرور ها و کلاینت ها را ببیند.

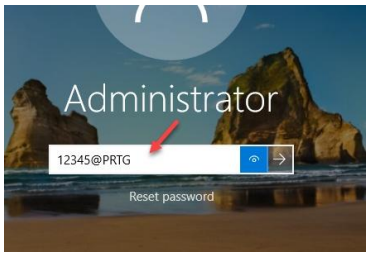
www.takbook.com



شکل ۹- ۲ تنظیم کارت شبکه

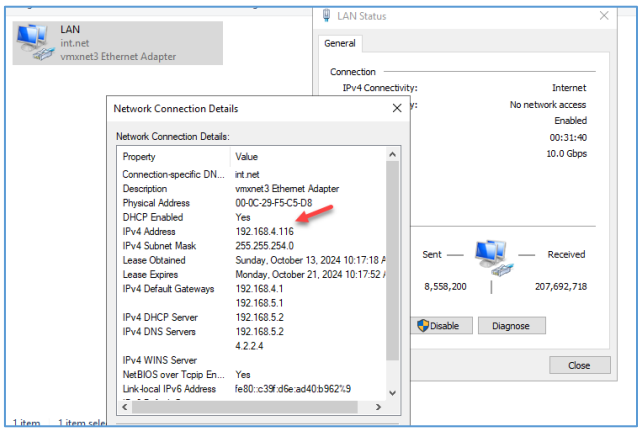
بعد از تنظیم سخت افزار مورد نظر ماشین مورد نظر را روشن کنید تا از طریق وب به صفحه مدیریتی آن دسترسی داشته باشیم.

برای ورود به ویندوز رمز پیش‌فرضی که بر روی آن قرار دارد 12345@PRTG است، طبق شکل ۹-۳، رمز عبور را وارد کنید.



شکل ۹- ۳ ورود به سرور

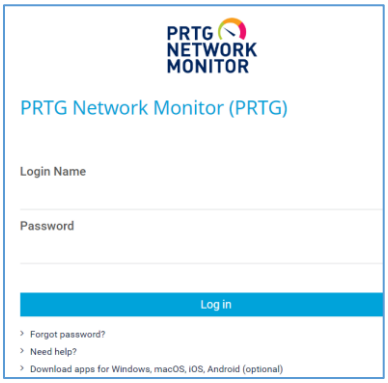
در ادامه باید ببینیم این سرور چه آدرسی دریافت کرده است که در شکل ۹-٤، مشاهده می‌کنید سرور مورد نظر آدرس 192.168.4.116 دریافت کرده است.



شکل ۹- ۴ بررسی آدرس IP

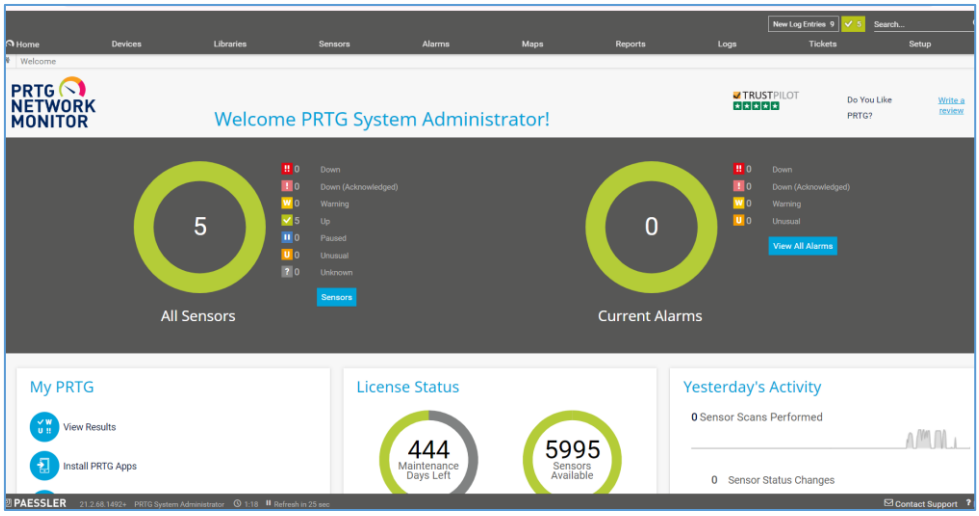
www.takbook.com

حالا می‌توانید از هر کلاینتی به صفحه‌ی وب دسترسی داشته باشید، اولین صفحه‌ای که مشاهده خواهید کرد به صورت شکل ۹-۵، می‌باشد که باید نام کاربری و رمز عبور پیش‌فرض آن را وارد کنید که هر دوی آنها prtgadmin است.



شکل ۹- ۵ ورود به PRTG

بعد از ورود شکل ۹-۶، را که نمای کلی نرم‌افزار است را مشاهده می‌کنید، عدد 5995 مربوط به تعداد سنسورهای در دسترس است که شما می‌توانید برای دستگاه‌های خودتان استفاده کنید.

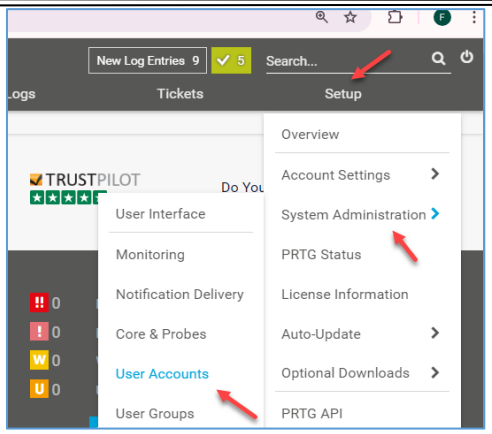


شکل ۹- ۶ صفحه اول نرم افزار PRTG

۹-۱-۱ تغییر رمز ورود

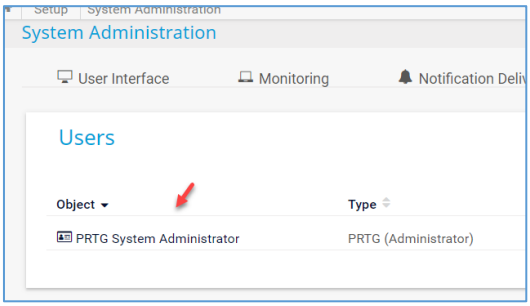
اولین کاری که انجام می‌دهید، تغییر رمز عبور نرم‌افزار است که برای این کار به مانند شکل ۹-۷، از منوی Setup و از قسمت System Administration گزینه‌ی User Accounts را انتخاب کنید.

www.takbook.com



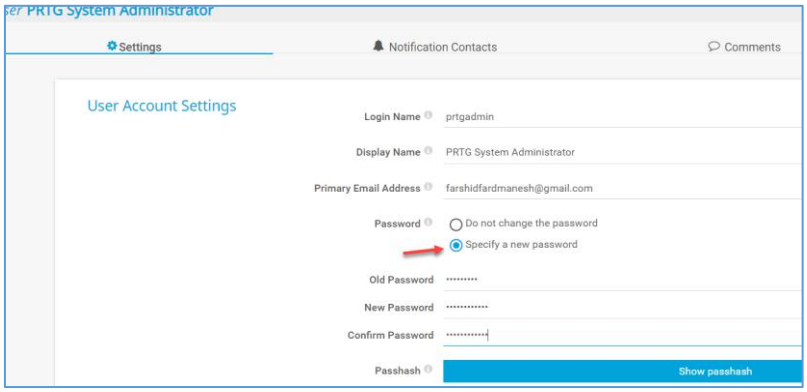
شکل ۹- ۷ تغییر رمز ورود

به مانند شکل ۹-۸، بر روی کاربر مورد نظر کلیک کنید.



شکل ۹- ۸ تغییر رمز ورود

در ادامه کار به مانند شکل ۹-۹، گزینه‌ی Specify را انتخاب کنید و رمز عبور قدیم که همان prtgadmin است را وارد و رمز عبور جدید خود را دو بار وارد و بر روی Save کلیک کنید.

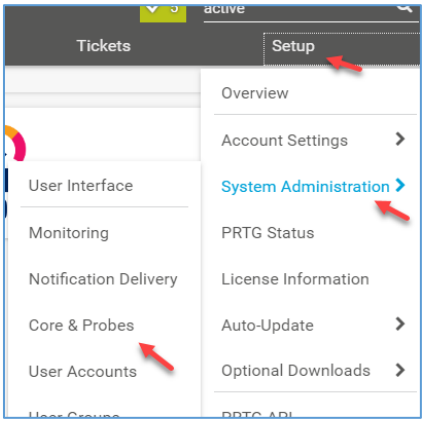


شکل ۹- ۹ تغییر رمز ورود

www.takbook.com

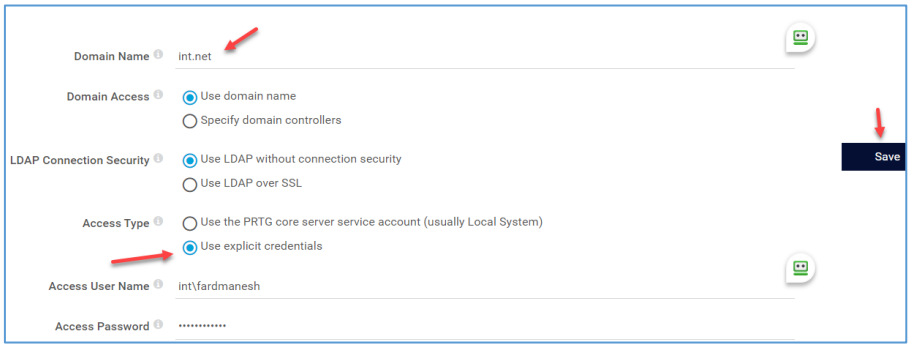
۹-۱-۲ عضو کردن در دومین

برای اینکه بتوانید از کاربران دومین برای ورود به سرور PRTG استفاده کنیم، باید PRTG را عضو دومین کنیم، برای این کار به مانند شکل ۹-۱۰، از طریق System Administration گزینه‌ی Core & Probes را انتخاب کنید.



شکل ۹- ۱۰ عضو کردن در دومین

در شکل ۹-۱۱، باید نام دومین خود را در قسمت Domain Name وارد کنید و در قسمت Access Type باید گزینه‌ی Use explicit certificates را انتخاب کنید و نام کاربری و رمز عبور ادمین دومین را وارد کنید و بر روی Save کلیک کنید، با این گروه‌های دومین در دسترس قرار خواهند گرفت.



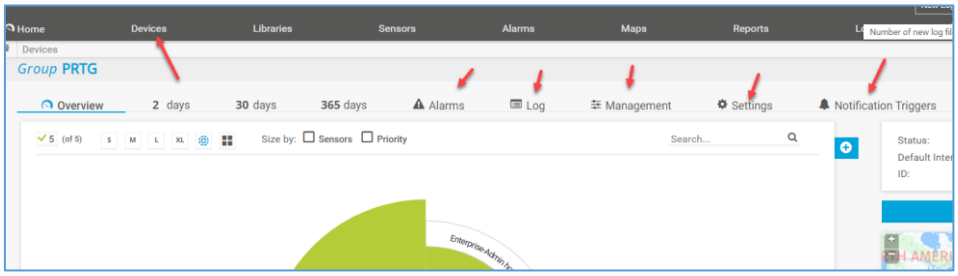
شکل ۹- ۱۱ عضو کردن در دومین

۹-۱-۳ اضافه کردن دستگاه‌ها به PRTG

برای شروع کار و برای تست نرم‌افزار می‌خوایم دستگاه‌های شبکه را به آن متصل کنیم، برای شروع وارد Device شوید، همان‌طور که در شکل ۹-۱۲، مشاهده می‌کنید چند سنسور به صورت پیش‌فرض قرار دارند که این سنسورها مربوط به خود سرور PRTG است که از وضعیت سلامتی سرور ما را با خبر

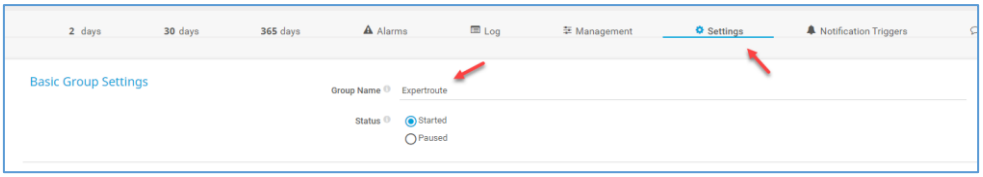
www.takbook.com

می‌کند، در قسمت بالایی صفحه هم چندین تب برای انجام تنظیمات وجود دارد که هر کدام را توضیح خواهیم داد، برای شروع وارد تب Settings شوید.



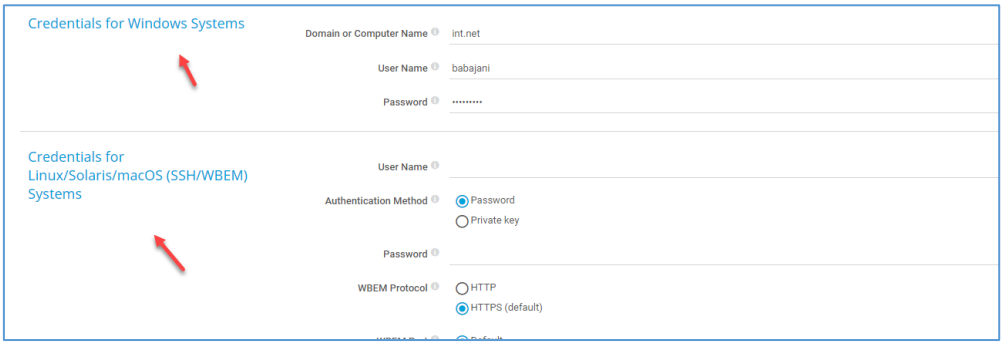
شکل ۹- ۱۲ اضافه کردن دستگاه‌ها به PRTG

در شکل ۹-۱۳، می‌توانید نام پروژه و یا سازمان خود را مشخص کنید و همچنین در قسمت Status می‌توانید پروژه را در حالت start یا Paused قرار دهید.



شکل ۹- ۱۳ اضافه کردن دستگاه‌ها به PRTG

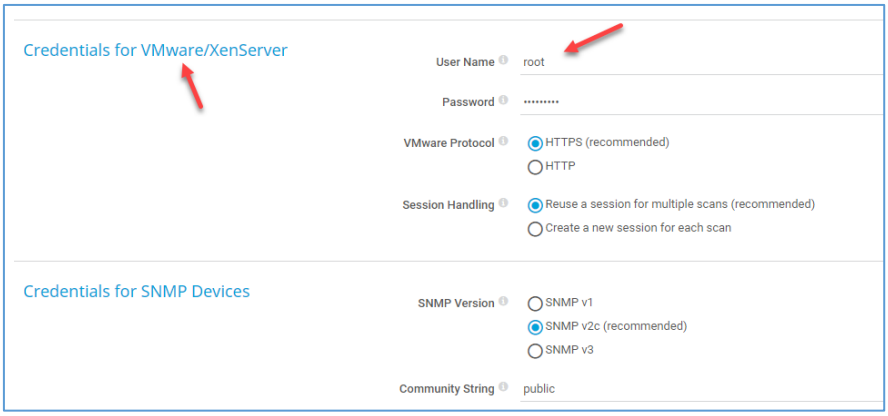
بعد از اینکه صفحه را به سمت پایین اسکرول کردید به مانند شکل ۹-۱٤، می‌توانید مشخص کنید که نرم‌افزار PRTG برای دسترسی به منابع سیستم عامل‌های مختلف از چه نام کاربری و رمز عبور استفاده کند، مثلاً در قسمت Credentials for Windows Systems نام دومین، نام کاربری و رمز عبور مربوط به Active Directory ویندوز سرور را وارد کنید تا با این نام کاربری در کل شبکه بررسی انجام شود و همه دستگاه‌ها شناسایی و به لیست اضافه شوند، در قسمت Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems اگر چنین سیستم عامل‌هایی دارید باید نام کاربری و رمز عبور را معرفی کنید.



شکل ۹- ۱۴ اضافه کردن دستگاه‌ها به PRTG

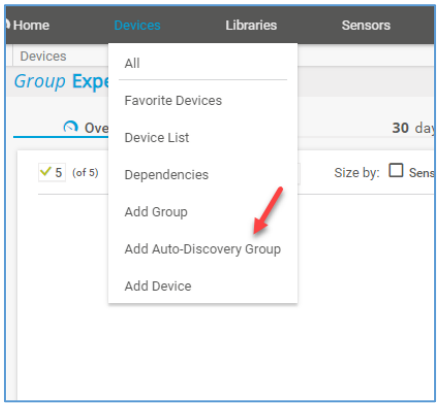
www.takbook.com

در شکل ۹-۱۵، برای اینکه به سرورهای VMware/XenServer دسترسی داشته باشیم باید نام کاربری و رمز عبور آنها را وارد کنید، مثلاً برای سرورهای ESXi که نام کاربری آنها root است را وارد کنید، گزینه‌های زیاد دیگری هم وجود دارد که در صورت لزوم آنها را بررسی می‌کنیم، در نهایت بر روی Save کلیک کنید تا اطلاعات ذخیره شود.



شکل ۹- ۱۵ اضافه کردن دستگاه‌ها به PRTG

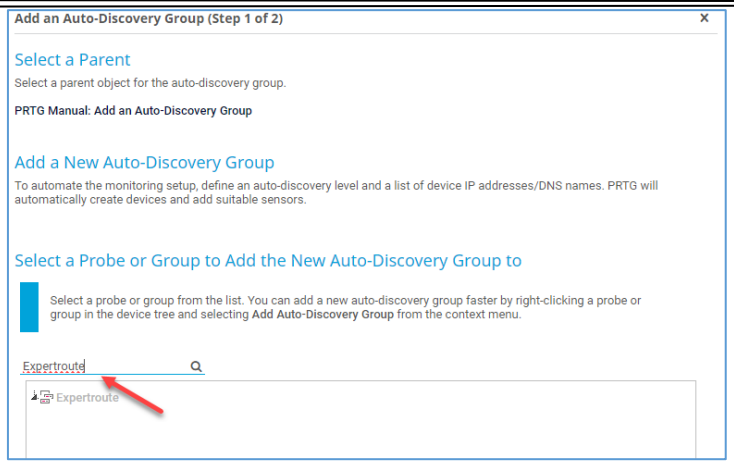
در ادامه کار می‌خواهیم کاری کنیم که نرم‌افزار PRTG خودش به صورت اتوماتیک در شبکه جستجو کند و تمام دستگاه‌های شبکه را دریافت و به لیست اضافه کند، برای این کار به مانند شکل ۹-۱۶، از منوی Devices گزینه‌ی Add Auto-Discovery Group را انتخاب کنید.



شکل ۹- ۱۶ اضافه کردن دستگاه‌ها به PRTG

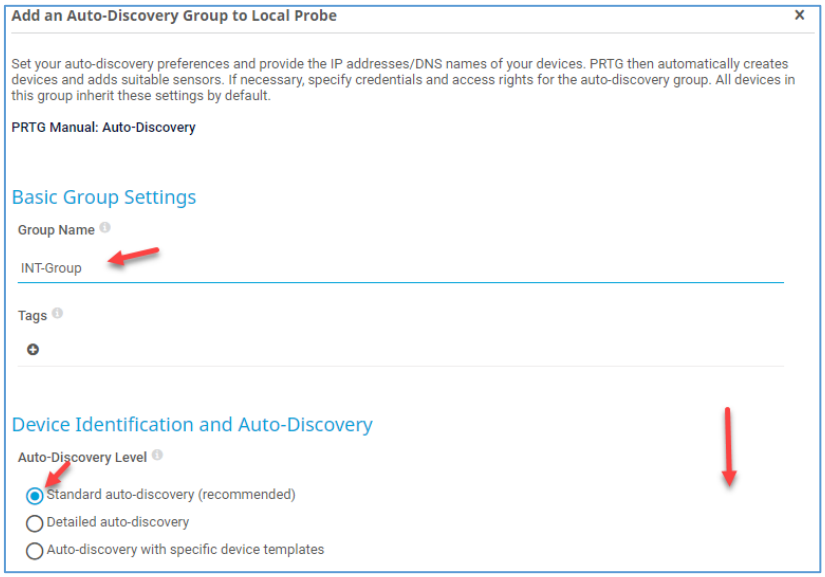
به مانند شکل ۹-۱۷، یک نام برای سر گروه خود وارد و بر روی OK کلیک کنید.

www.takbook.com



شکل ۹- ۱۷ اضافه کردن دستگاه‌ها به PRTG

در ادامه کار و در شکل ۹-۱۸، باید نام گروه خود را مشخص کنید و در قسمت Device Identification and Auto-Discovery باید گزینه‌ی Standard را انتخاب کنید و برای ادامه کار صفحه را به پایین اسکرول کنید.

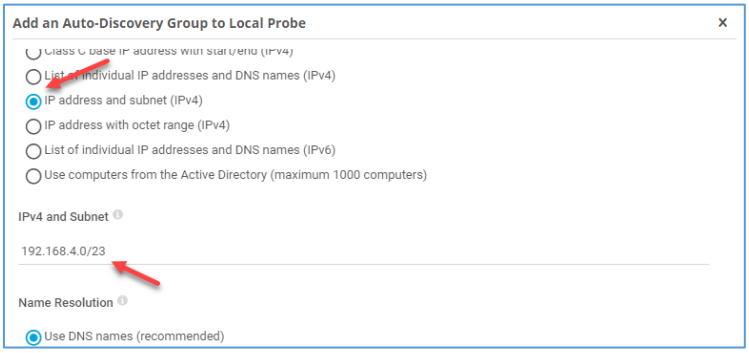


شکل ۹- ۱۸ اضافه کردن دستگاه‌ها به PRTG

در شکل ۹-۱۹، باید مشخص کند شبکه‌ی داخلی شما دارای چه رنج آدرسی است که به مانند شکل گزینه‌ی IP Address and subnet (IPv4) را انتخاب کنید و در قسمت IPv4 and Subnet باید Subnet شبکه‌ی خود را وارد کنید، در قسمت Name Resolution گزینه‌ی اول را انتخاب کنید تا کلاینت‌ها و سرورهای شما از طریق سرویس DNS شناسایی شوند، توجه داشته باشید در پایین صفحه می‌توانید نام کاربری و رمز عبور

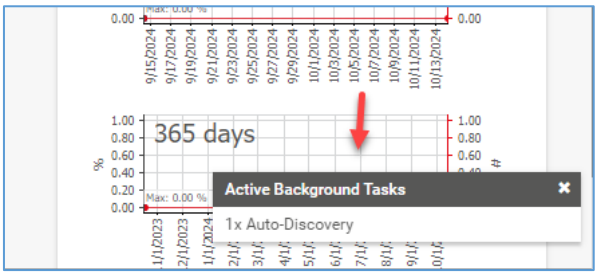
www.takbook.com

کلاینت‌های ویندوزی و لینوکسی و... را مشخص کنید ولی نیاز به این کار نیست چون در قسمت قبل این کار را انجام دادیم.



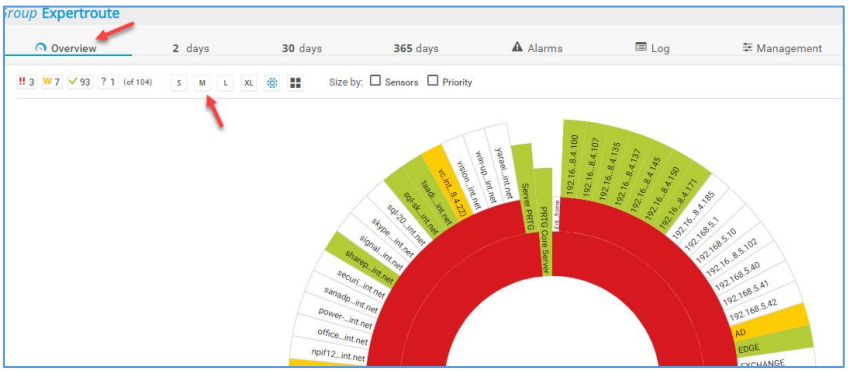
شکل ۹- ۱۹ اضافه کردن دستگاه‌ها به PRTG

بعد از کلیک بر روی OK کار آغاز می‌شود و یک پیغام در پایین و سمت راست صفحه به صورت شکل ۹-۲۰، مشاهده خواهید کرد.



شکل ۹- ۲۰ اضافه کردن دستگاه‌ها به PRTG

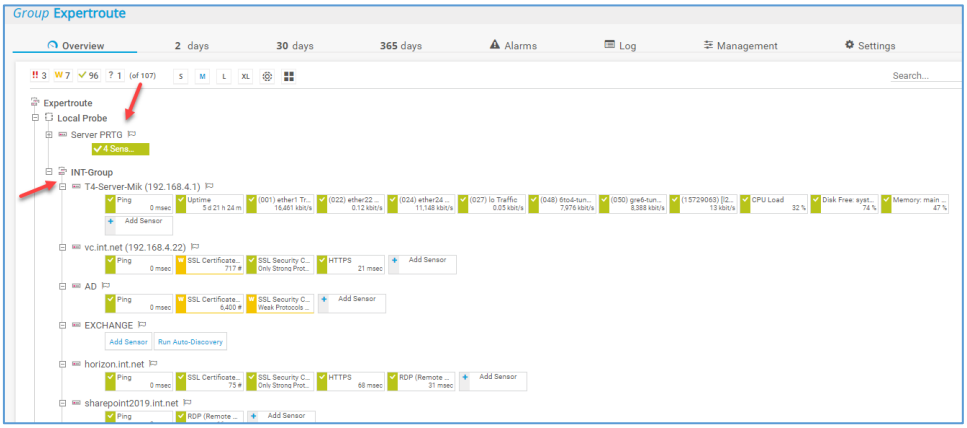
در ادامه کار اگر به طبق شکل ۹-۲۱، وارد Overview شوید یک شکل دایره را مشاهده می‌کنید که در آن چندین دستگاه مختلف را که به صورت اتوماتیک بررسی کرده نشان می‌دهد، برای اینکه لیست دستگاه‌های شناسایی شده را بهتر ببینیم بهتر است بر روی کلمه M کلیک کنید تا به صورت لیست نمایش داده شوند.



شکل ۹- ۲۱ اضافه کردن دستگاه‌ها به PRTG

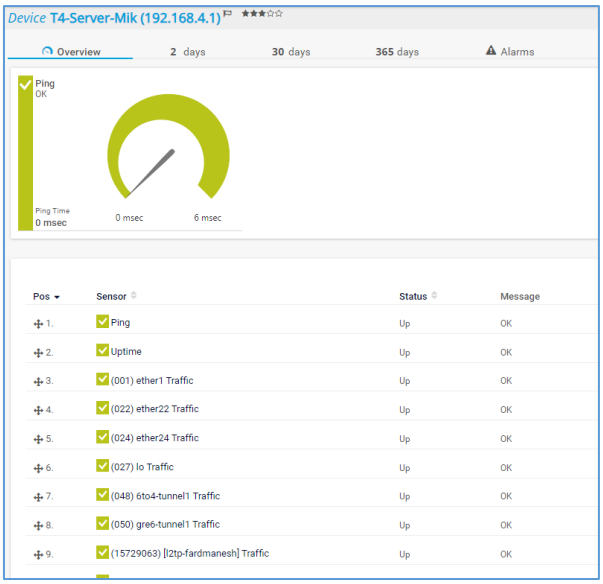
www.takbook.com

در شکل ۹-۲۲، دو گروه را مشاهده می‌کنید یکی که (Server PRTG) مربوط به خود سرور PRTG است و سنسورهایی که برای این سرور در نظر گرفته شده است و گروهی که ما با هم ایجاد کردیم و عملیات Autodiscover را اجرا کردیم دارای تعداد زیادی کلاینت و سرور است که به صورت اتوماتیک شناسایی شده است، برای بررسی بیشتر بر روی کلاینت اول یعنی T4-Server-Mik که مربوط به روتر میکروتیک است کلیک می‌کنیم.



شکل ۹- ۲۲ اضافه کردن دستگاه‌ها به PRTG

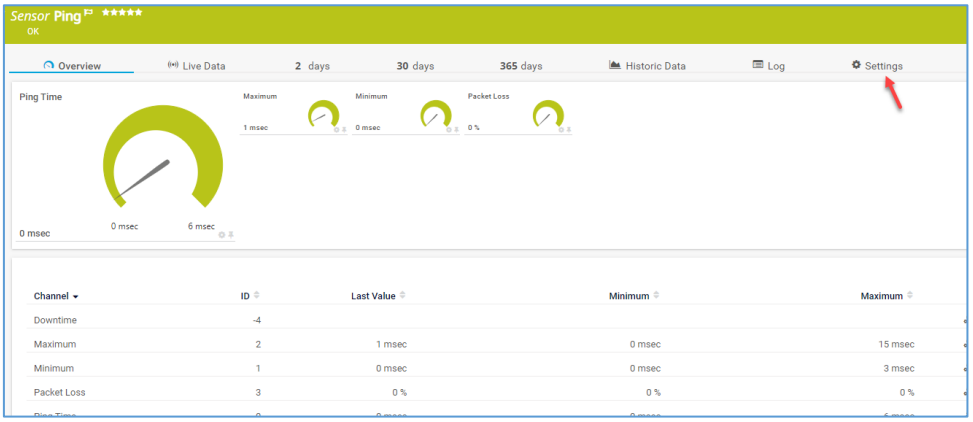
همان‌طور که در شکل ۹-۲۳، مشاهده می‌کنید، این دستگاه دارای سنسورهای مختلفی است، مثلاً سنسور اول سنسور Ping است که آنلاین بودن دستگاه را هر ۳۰ ثانیه یک بار چک می‌کند.



شکل ۹- ۲۳ اضافه کردن دستگاه‌ها به PRTG

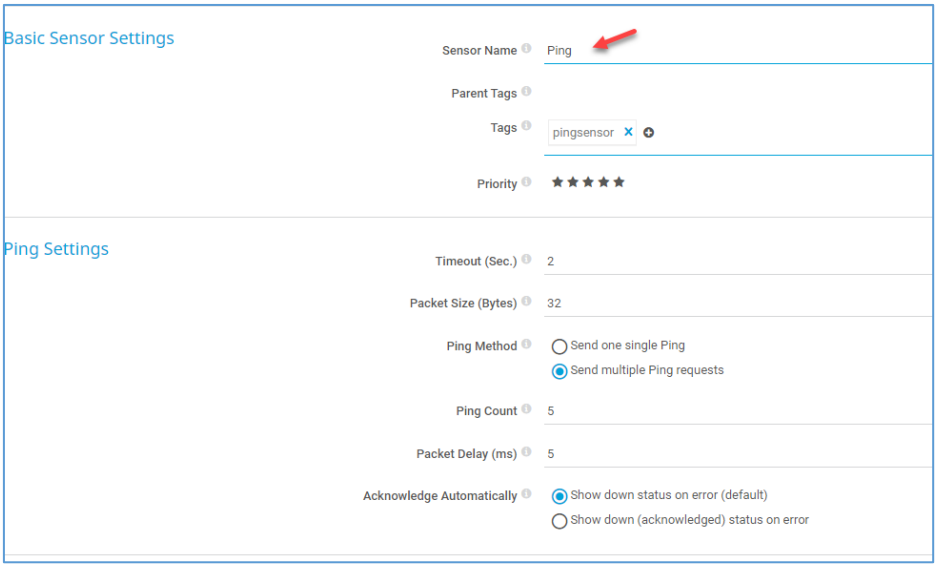
www.takbook.com

برای اینکه تنظیمات هر کدام از سنسورها را مشاهده کنید باید بر روی آن کلیک کنید، تا شکل ۹-۲۴، باز شود، در این قسمت برای اینکه تنظیمات دقیق این سنسور را مشاهده کنید باید بر روی Settings کلیک کنید.



شکل ۹- ۲۴ اضافه کردن دستگاه‌ها به PRTG

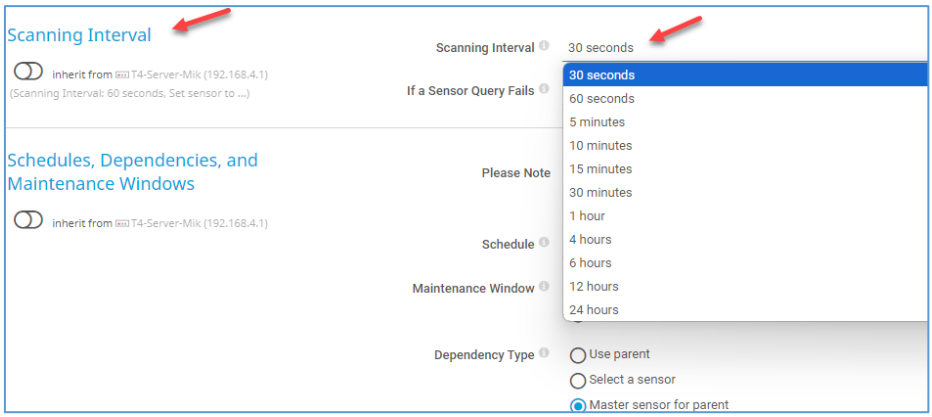
همان‌طور که در شکل ۹-۲۵، مشاهده می‌کنید تنظیمات دقیق مربوط به سنسور Ping را مشاهده می‌کنید که می‌توانید آنها را تغییر دهید.



شکل ۹- ۲۵ اضافه کردن دستگاه‌ها به PRTG

www.takbook.com

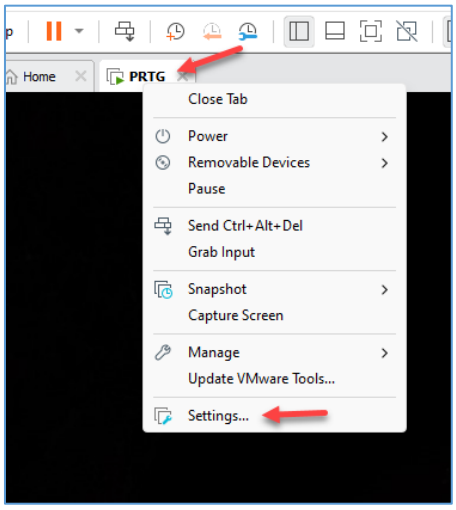
اگر بخواهیم زمان اجرای سنسور را تغییر دهیم باید صفحه را رو به پایین اسکرول کنید و به مانند شکل ۹-۲۶، از قسمت Scanning Interval بر روی زمان مورد نظر کلیک کنید و طبق شکل یکی از زمان‌ها را انتخاب کنید که به صورت پیش‌فرض ۳۰ ثانیه است.



شکل ۹- ۲۶ اضافه کردن دستگاه‌ها به PRTG

۹-۱-٤ اضافه کردن شبکه دوم به PRTG

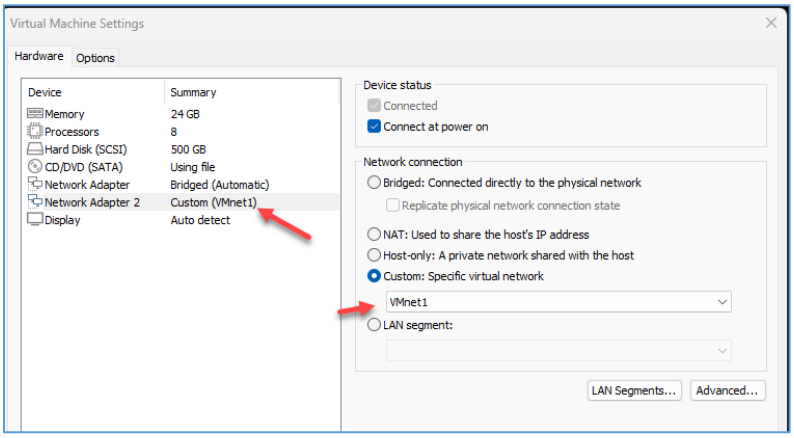
تا به اینجای کار یک شبکه را به لیست نرم‌افزار PRTG اضافه کردیم که به صورت اتوماتیک دستگاه‌های شبکه شناسایی شدند، اگر چنانچه در شبکه‌ی سازمانی خود دارای یک شبکه دوم و خصوصی هستید و می‌خواهید آن را به لیست شبکه‌های PRTG اضافه کنید، اول از همه باید کارت شبکه‌ی مورد نظر را به سرور PRTG متصل کنید که در اینجا به مانند شکل ۹-۲۷، وارد تنظیمات ماشین مورد نظر در VMware workstation می‌شویم.



شکل ۹- ۲۷ اضافه کردن شبکه دوم به PRTG

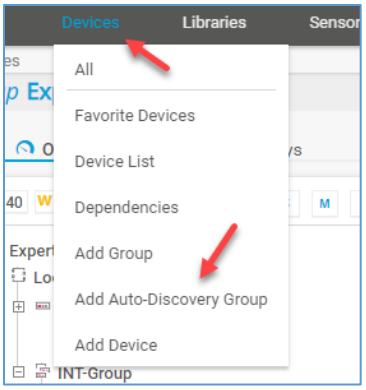
www.takbook.com

در ادامه، کارت شبکه‌ی دوم را به لیست اضافه کنید، همان‌طور که در شکل ۹-۲۸، مشاهده می‌کنید یک کارت شبکه VMnet1 به لیست اضافه کردیم که مربوط به شبکه دوم ما است و دارای کلاینت‌های زیادی است.



شکل ۹- ۲۸ اضافه کردن شبکه دوم به PRTG

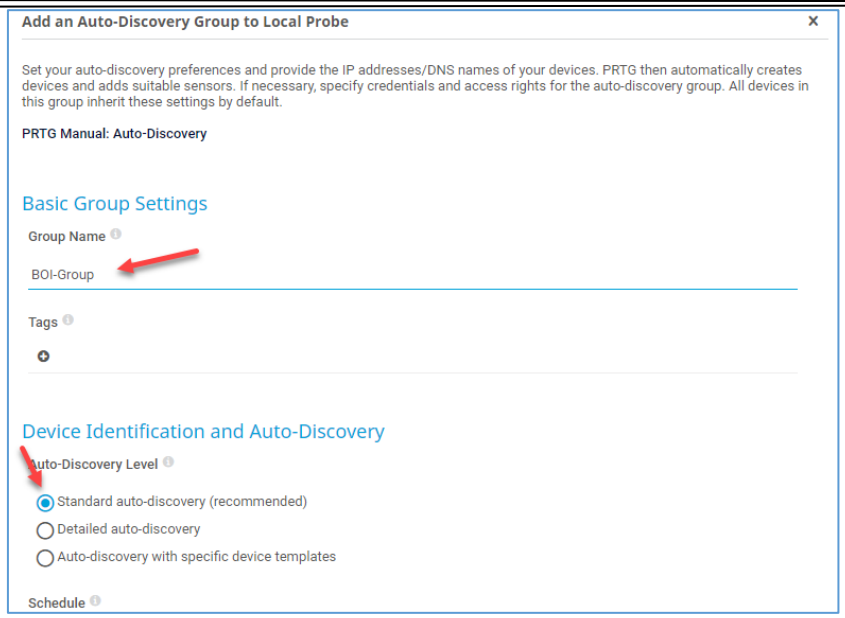
بعد از اضافه کردن شبکه‌ی مورد نظر طبق شکل ۹-۲۹، وارد PRTG شوید و دوباره از منوی Devices گزینه‌ی Add Auto-Discovery را انتخاب کنید.



شکل ۹- ۲۹ اضافه کردن شبکه دوم به PRTG

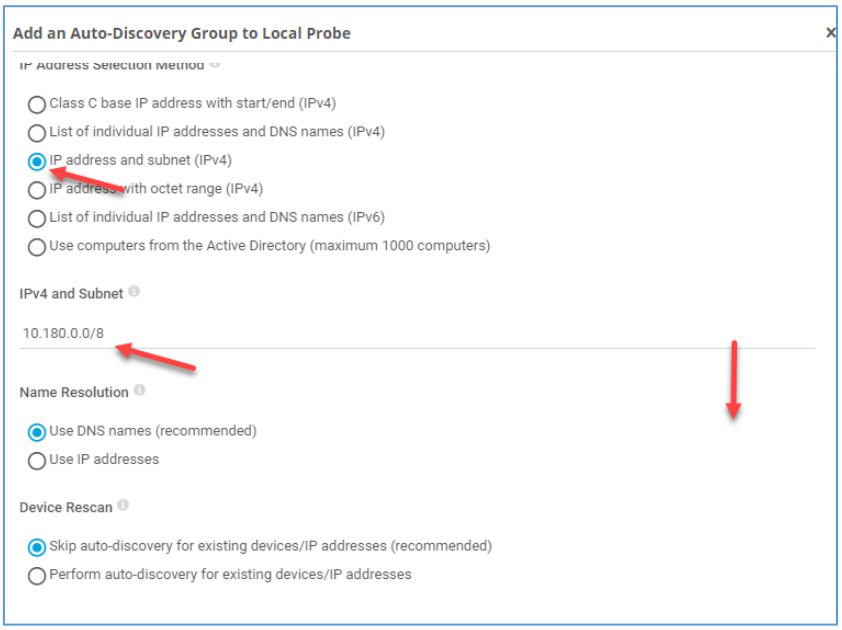
در ادامه کار به مانند قبل نام گروه خود را طبق شکل ۹-۳۰، مشخص کنید و گزینه‌ی Standard را انتخاب کنید.

www.takbook.com



شکل ۹- ۳۰ اضافه کردن شبکه دوم به PRTG

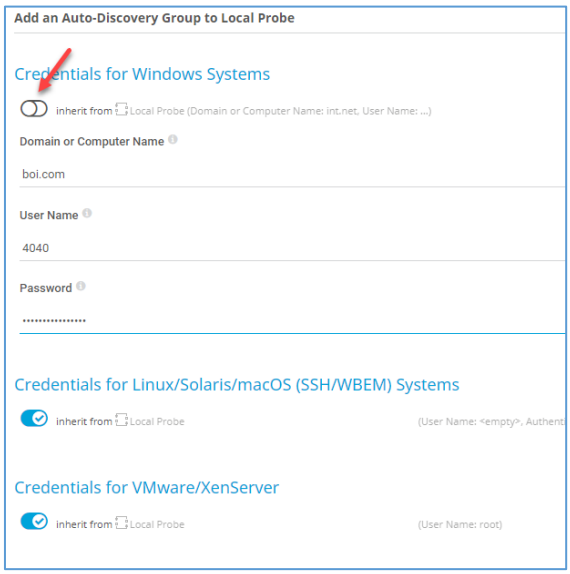
در شکل ۹-۳۱، باید Subnet شبکه‌ی دوم خود را وارد کنید تا PRTG روی این شبکه کار کند.



شکل ۹- ۳۱ اضافه کردن شبکه دوم به PRTG

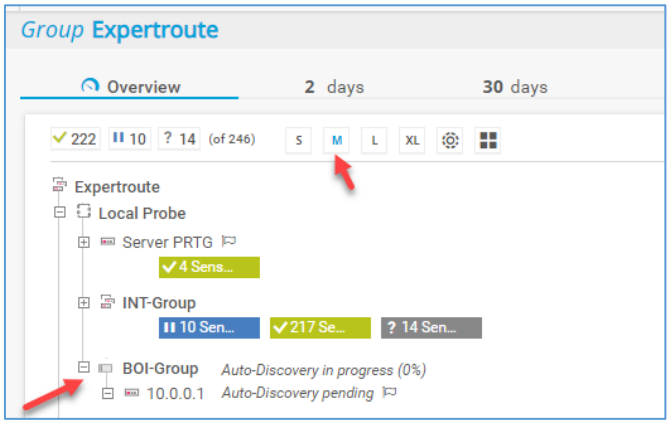
www.takbook.com

صفحه را رو به پایین اسکرول کنید، به مانند شکل ۹-۳۲، در این قسمت چون شبکه متفاوت است و نام کاربری و رمز عبور آن متفاوت است باید، به مانند شکل در قسمت Credentials for Windows Systems نام دومین و نام کاربری شبکه جدید خود را وارد کنید و اگر هم سیستم عامل‌های دیگر مانند ESXi دارید می‌توانید رمز آن را هم وارد کنید ولی در اینجا چون رمز ESXi در هر دو شبکه یکسان است نیازی به وارد کردن نبود و اگر آن را وارد نکنید از همان تنظیماتی که در اول کار انجام دادیم استفاده خواهد کرد.



شکل ۹- ۳۲ اضافه کردن شبکه دوم به PRTG

همان‌طور که در شکل ۹-۳۳، مشاهده می‌کنید عملیات Discover بر روی شبکه‌ی دوم شروع به کار کرده و دستگاه‌ها در حال شناسایی هستند.

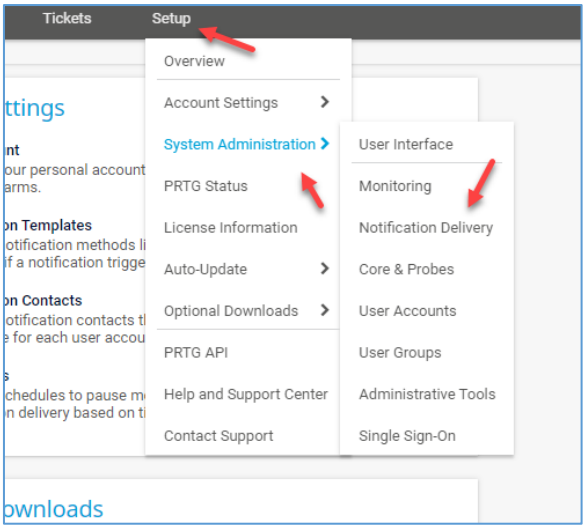


شکل ۹- ۳۳ اضافه کردن شبکه دوم به PRTG

www.takbook.com

۹-۱-۵ ارسال ایمیل در PRTG

یکی از راه‌های باخبر شدن از وضعیت سرورها و کلاینت‌ها این است که سرویس ایمیل را راه‌اندازی کنیم، برای این کار طبق شکل ۹-۳۴، از منوی Setup و از قسمت System Administration گزینه‌ی Notification Delivery را انتخاب کنید.



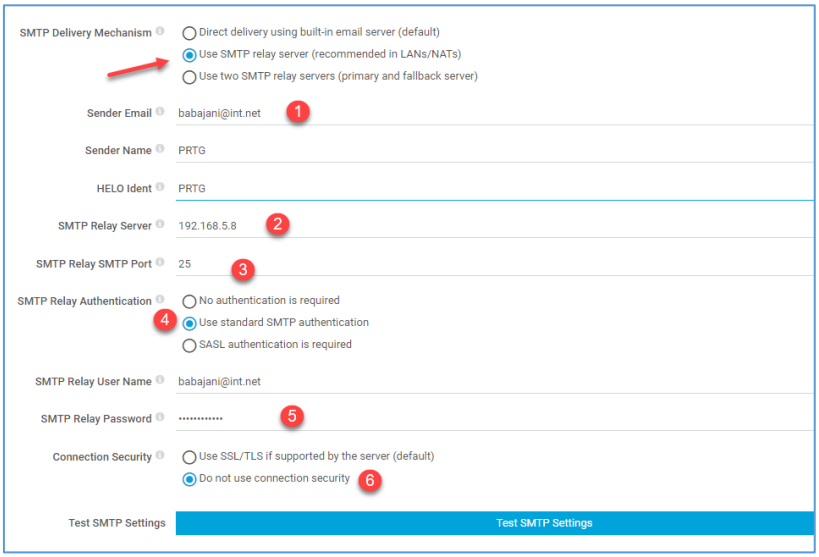
شکل ۹- ۳۴ ارسال ایمیل در PRTG

در شکل ۹-۳۵، چون می‌خواهیم PRTG را به ایمیل داخلی خود متصل کنیم گزینه‌ی Use SMTP relay server (recommended in LANs/NATs) را انتخاب کنید و در قسمت شماره‌ی یک باید آدرس ایمیل خود را وارد کنید، در قسمت شماره‌ی دو باید آدرس سرور ایمیل خود را وارد کنید که می‌تواند یک ایمیل داخلی و یا خارجی باشد که البته اگر ایمیل خارجی وارد می‌کنید سررور PRTG شما باید دارای اینترنت باشد، در قسمت شماره‌ی سه باید پورت Outgoing را مشخص می‌کنیم که به صورت پیش‌فرض 25 است و در قسمت شماره‌ی چهار برای وارد کردن نام کاربری و رمز عبور ایمیل گزینه‌ی Use standard SMTP authentication را انتخاب کنید و نام کاربری و رمز عبور ایمیل خود را وارد کنید.

توجه داشته باشید در قسمت شماره‌ی شش یعنی قسمت Connection Security اگر از پروتکل‌های امنیتی برای متصل شدن به ایمیل استفاده می‌کنید باید گزینه‌ی اول را انتخاب کنید ولی اگر از گزینه‌ی امنیتی استفاده نمی‌کنید، می‌توانید گزینه‌ی Do not use connection security را انتخاب کنید.

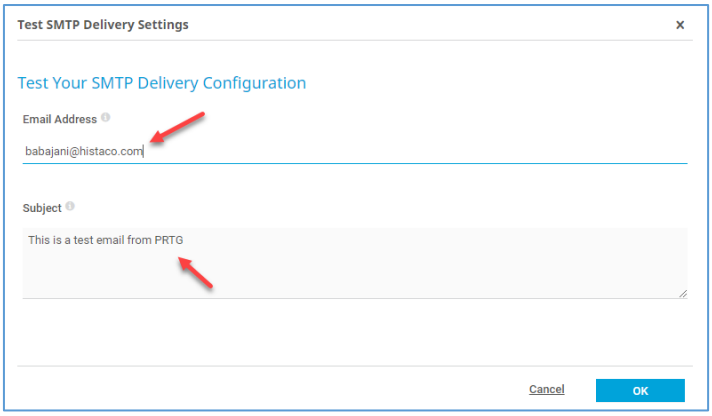
برای اینکه تنظیمات ایمیل خود را تست بگیریم باید بر روی گزینه‌ی Test SMTP Settings کلیک کنید.

www.takbook.com



شکل ۹- ۳۵ ارسال ایمیل در PRTG

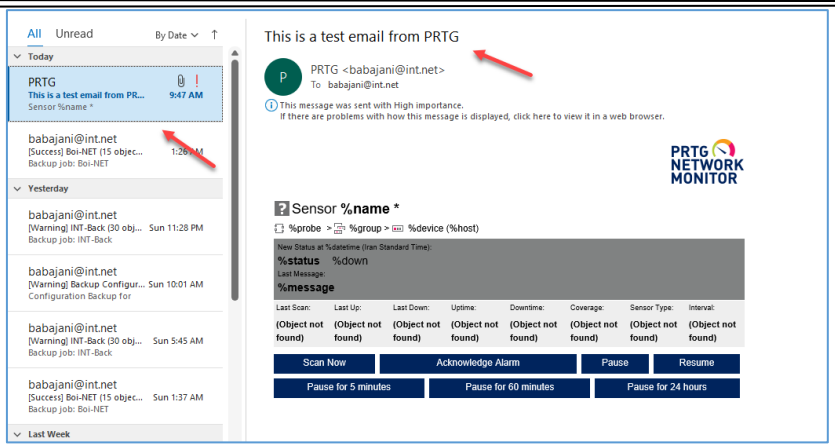
در شکل ۹-۳۶، باید مشخص کنید که ایمیل تست برای کدام یک از کاربران ارسال شود که ایمیل را نوشته و بر روی OK کلیک می‌کنیم که یک پیغام ظاهر می‌شود مبنی بر ارسال ایمیل.



شکل ۹- ۳۶ ارسال ایمیل در PRTG

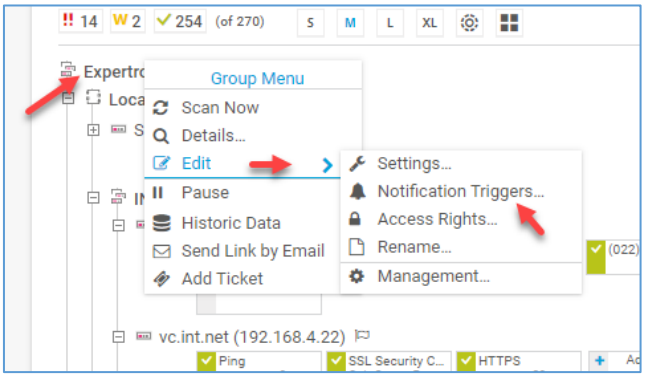
حالا اگر به مانند شکل ۹-۳۷، وارد سرور ایمیل خود شویم این ایمیل تستی که از سرور PRTG ارسال شده را خواهیم دید.

www.takbook.com



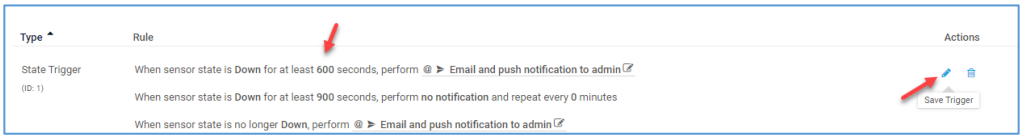
شکل ۹- ۳۷ ارسال ایمیل در PRTG

برای اینکه وضعیت کلاینت‌ها و سرورها به آدرس ایمیل ما ارسال شوند باید به مانند شکل ۹–۳۸، در قسمت Device باید بر روی نام شاخه اصلی کلیک راست کنید و از قسمت Expertroute و بعد Edit گزینه‌ی Notification Triggers را انتخاب کنید.



شکل ۹- ۳۸ ارسال ایمیل در PRTG

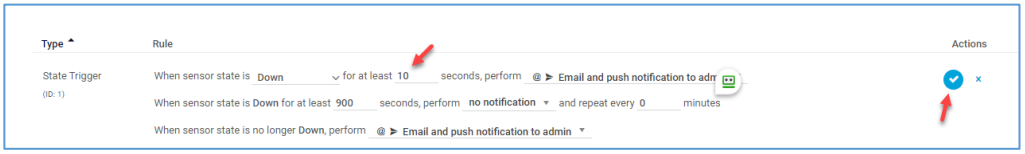
در ادامه کار و در صفحه‌ی شکل ۹–۳۹، عدد 600 را مشاهده می‌کنید که بدین معنا است که اگر یک کلاینت یا سرور و یا هر دستگاهی در شبکه خاموش شود بعد 600 ثانیه یعنی 10 دقیقه یک ایمیل به مدیر شبکه ارسال خواهد شد، برای اینکه این مقدار را تغییر دهیم و ایمیل ارسالی را مشخص کنیم بر روی آیکون مورد نظر کلیک کنید.



شکل ۹- ۳۹ ارسال ایمیل در PRTG

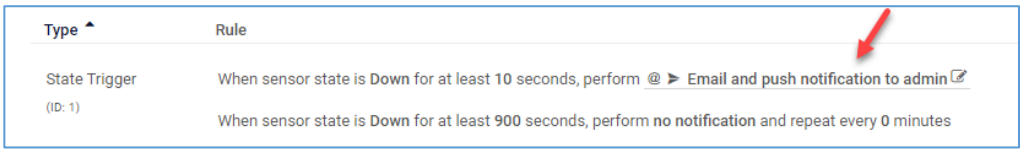
www.takbook.com

در شکل ۹-۴۰، مقدار 600 را به 10 ثانیه تغییر می‌دهیم و بر روی آیکون مورد نظر کلیک می‌کنیم تا اطلاعات ذخیره شود.



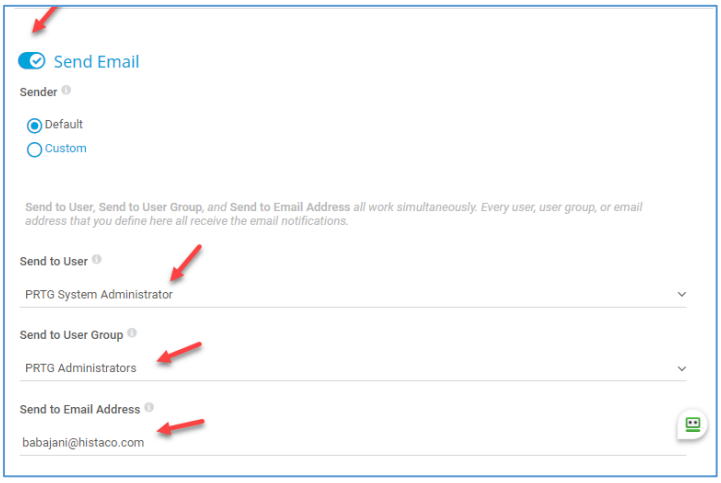
شکل ۹- ۴۰ ارسال ایمیل در PRTG

در ادامه برای اینکه مشخص کنیم اطلاعات به کدام ایمیل ارسال شود باید به مانند شکل ۹-۴۱، بر روی گزینه‌ی مورد نظر کلیک کنید.



شکل ۹- ۴۱ ارسال ایمیل در PRTG

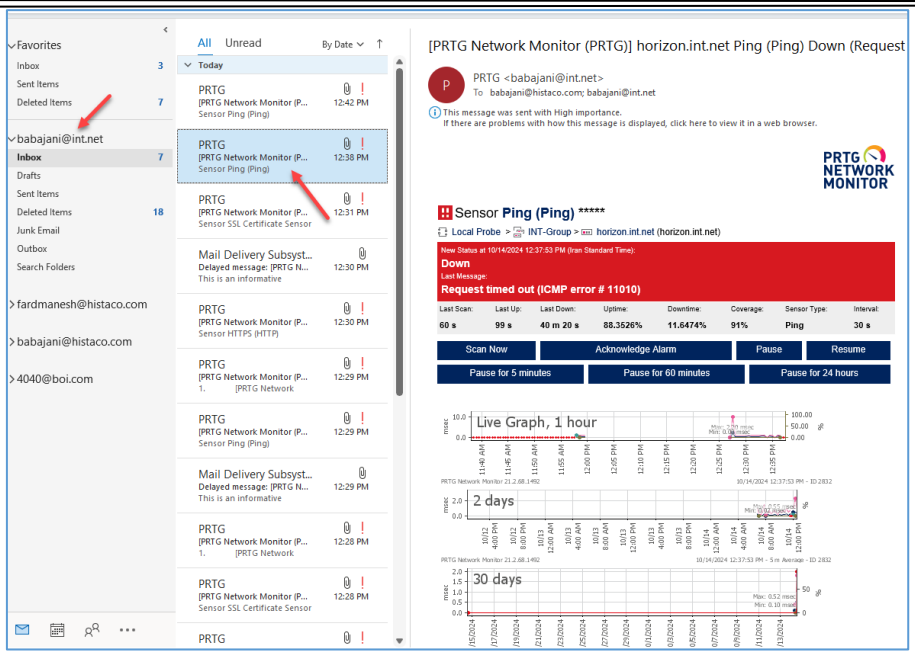
در شکل ۹-۴۲، باید گروه مورد نظر به همراه آدرس ایمیلی که قرار است اطلاعات ارسال شود را انتخاب کنید.



شکل ۹- ۴۲ ارسال ایمیل در PRTG

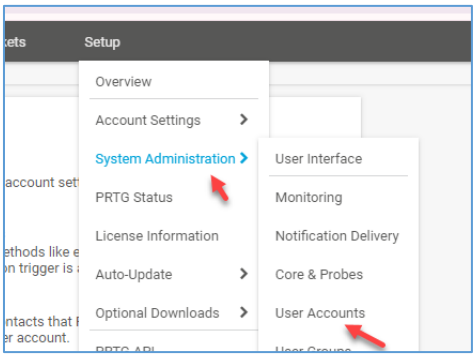
بعد از این کار حالا می‌خواهیم بررسی کنیم آیا ایمیل ارسال می‌شود یا نه که طبق شکل ۹-۴۳،وارد ایمیل می‌شویم و به مانند شکل مشخص است که ایمیل‌های اطلاع رسانی دریافت شده است.

www.takbook.com



شکل ۹- ۴۳ ارسال ایمیل در PRTG

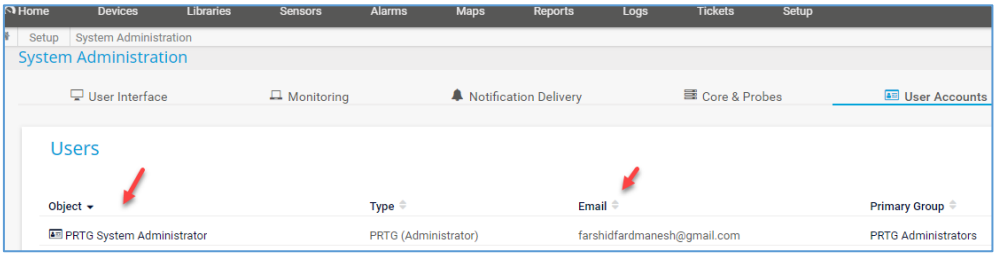
نکته مهم: اگر چنانچه ایمیل برای شما ارسال نشد، باید ببینید که بر روی کاربر مورد نظر چه ایمیلی تعریف کردید، برای این کار به مانند شکل ۹-٤٤، وارد User Accounts شوید.



شکل ۹- ۴۴ ارسال ایمیل در PRTG

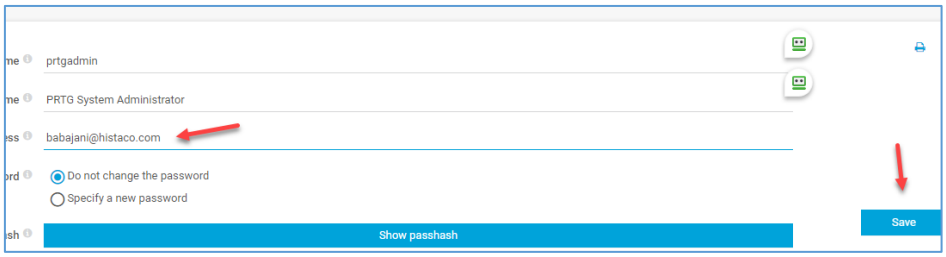
در شکل ۹-٤٥، اگر به ستون ایمیل توجه کنید یک آدرس Gmail نوشته شده است که باید بر روی کاربر مورد نظر کلیک کنید و آن را به ایمیل مورد نظر خود تغییر دهید تا ایمیل به کاربر مشخص شده ارسال شود.

www.takbook.com



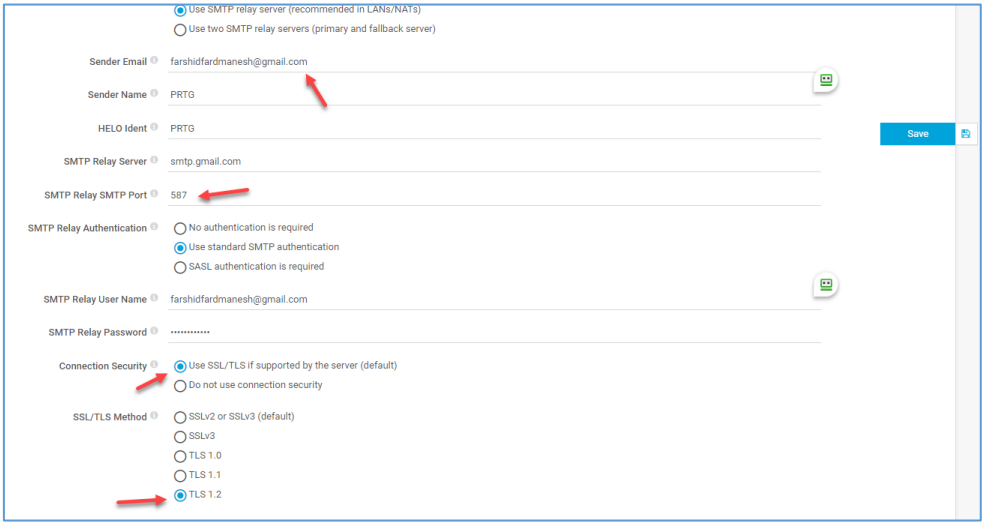
شکل ۹- ۴۵ ارسال ایمیل در PRTG

همان‌طور که در شکل ۹-٤٦، مشاهده می‌کنید ایمیل مورد نظر را تغییر دادیم و برای ذخیره کردن آن بر روی Save کلیک کنید.



شکل ۹- ۴۶ ارسال ایمیل در PRTG

توجه داشته باشید اگر می‌خواهید از آدرس Gmail خود استفاده کنید تنظیمات آن را می‌توانید طبق شکل ۹-٤٧، انجام دهید:



شکل ۹- ۴۷ ارسال ایمیل در PRTG

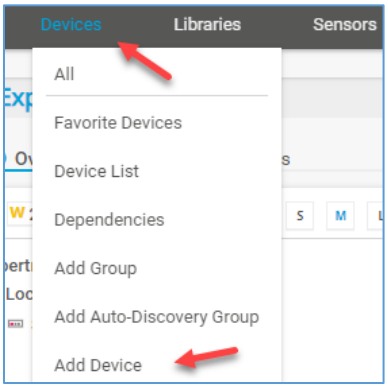
نکته مهم در مورد Gmail

www.takbook.com

از آنجا که PRTG به عنوان یک نرم‌افزار خارجی نیاز به اتصال به Gmail دارد، باید اجازه دسترسی به برنامه‌های با امنیت کمتر را بدهید، برای این کار باید قابلیت "Less Secure Apps" (برنامه‌های با امنیت کمتر) را در Gmail فعال کنید.

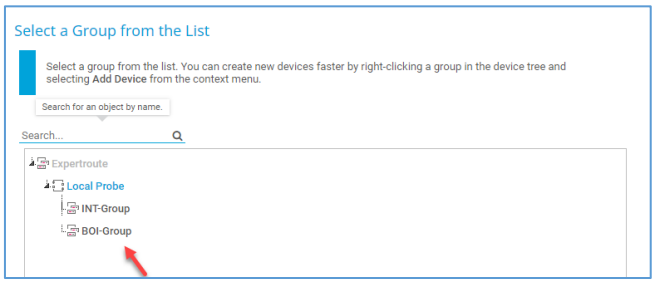
۹-۱-۶ اضافه کردن دستی دستگاه به PRTG

تا به اینجای کار همه چیز به صورت اتوماتیک اجرا شد و به لیست نرم افزار اضافه شده است، اما گاهی اوقات نیاز است که یک سرور یا کلاینت و یا هر دستگاه دیگری را به صورت اتوماتیک به لیست اضافه کنید، برای این کار به مانند شکل ۹-۴۸، از منوی Devices بر روی Add Devices کلیک کنید.



شکل ۹- ۴۸ اضافه کردن دستی دستگاه به PRTG

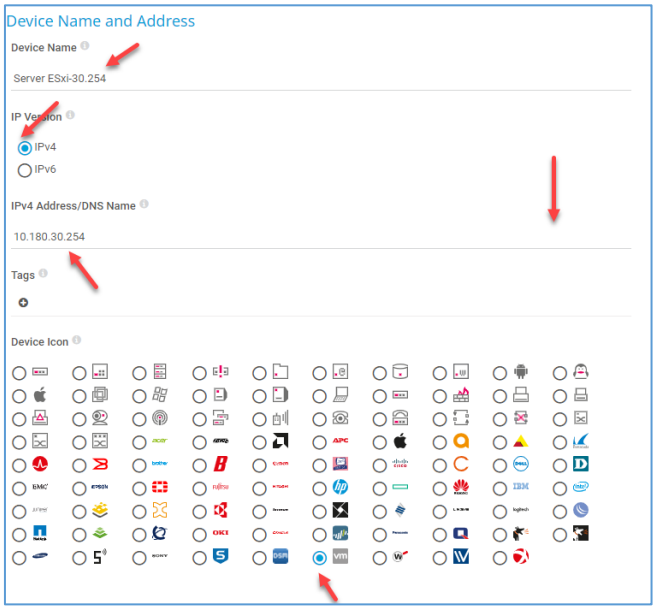
در شکل ۹-۴۹، گروه مورد نظر خود را انتخاب کنید و بر روی OK کلیک کنید.



شکل ۹- ۴۹ اضافه کردن دستی دستگاه به PRTG

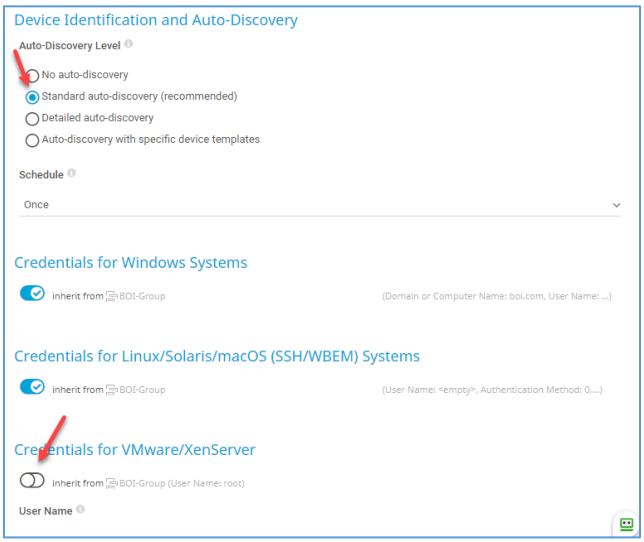
در شکل ۹-۵۰، باید نام سرور خود را وارد کنید و گزینه‌ی IPv4 را انتخاب کنید و آدرس سرور را وارد کنید، حتی می‌توانید یک آیکون به آن اختصاص دهید، در ادامه کار صفحه را رو به پایین اسکرول کنید.

www.takbook.com



شکل ۹- ۵۰ اضافه کردن دستی دستگاه به PRTG

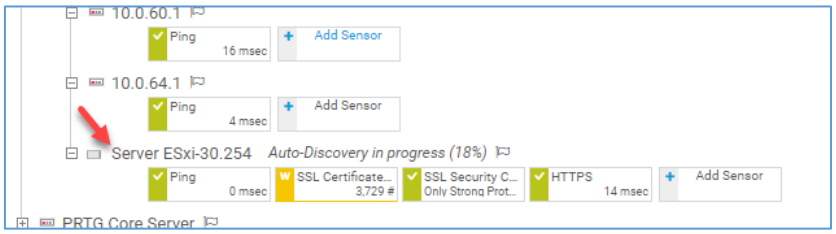
در شکل ۹-۵۱، باید برای اینکه Discovery انجام شود گزینه‌ی Standard را انتخاب کنید و در قسمت Credentials for VMware/XenServer باید نام کاربر و رمز عبور سرور ESXi خود را دقیق مشخص کنیم، البته اگر در قسمت‌های قبلی این نام کاربری و رمز را درست وارد کرده بودید دیگر نیازی نبود از این قسمت وارد کنید و به صورت سلسله مراتبی از بالا تنظیمات را دریافت می‌کرد.



شکل ۹- ۵۱ اضافه کردن دستی دستگاه به PRTG

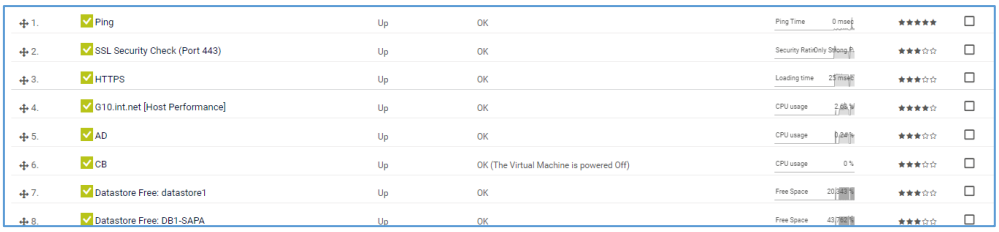
www.takbook.com

همان‌طور که در شکل ۹-۵۲، مشاهده می‌کنید سرور مورد نظر به لیست اضفه شده است و تمام سنسورهای در دسترس آن در حال یافتن و ثبت است.



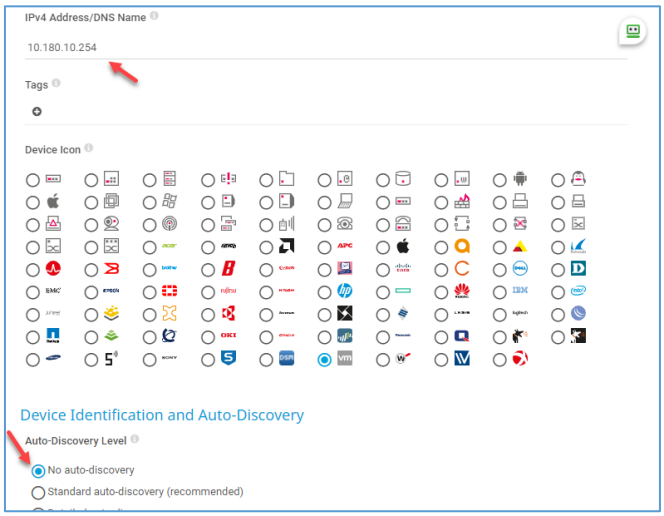
شکل ۹- ۵۲ اضافه کردن دستی دستگاه به PRTG

بعد از اینکه عملیات Discovery تمام شد اطلاعاتی که از یک سرور ESxi دریافت می‌شود در شکل ۹-۵۳، مشخص است، اطلاعاتی مانند وضعیت کارت شبکه، Datastoreها، ماشین‌ها و...



شکل ۹- ۵۳ اضافه کردن دستی دستگاه به PRTG

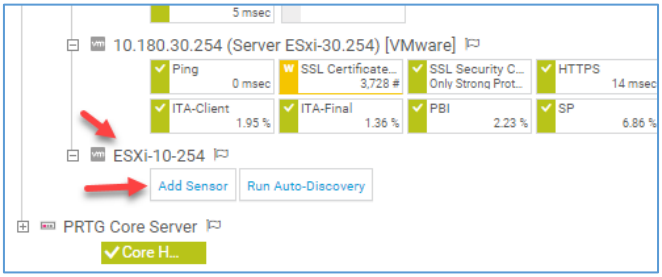
حالا اگر بخواهیم بدون عملیات Discovery سنسورها را بر روی یک سرور تعریف کنیم باید به صورت شکل ۹-۵۴، عمل کنیم، دوباره یک سرور جدید به لیست اضافه می‌کنیم با این تفاوت که قسمت Discovery آن را بر روی حالت خاموش قرار می‌دهیم.



شکل ۹- ۵۴ اضافه کردن دستی دستگاه به PRTG

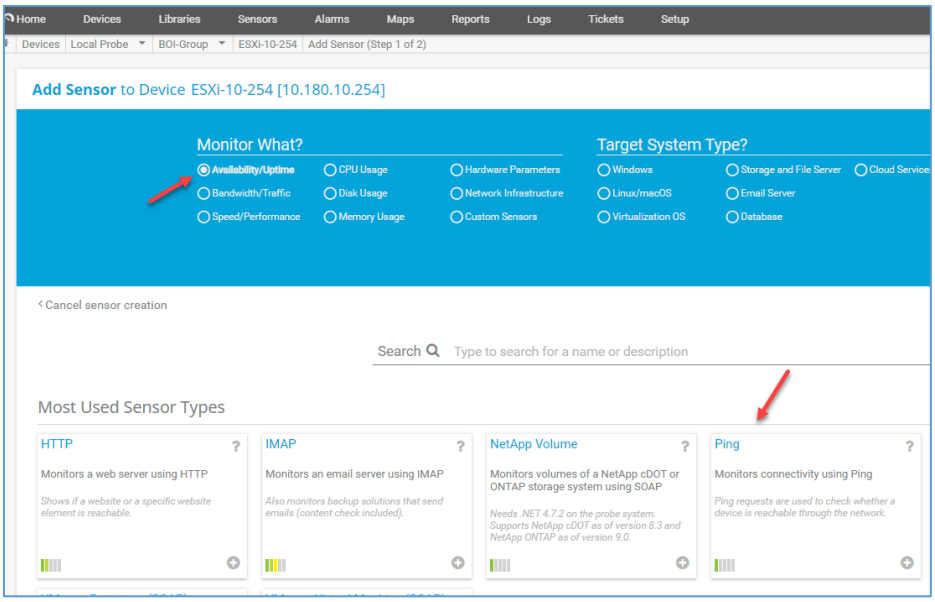
www.takbook.com

بعد از ایجاد سرور مورد نظر اگر به آن شکل ۹–۵۵، توجه کنید گزینه‌ی Add Sensor را مشاهده می‌کنید که می‌توانید بر روی آن کلیک کنید.



شکل ۹ - ۵۵ اضافه کردن دستی دستگاه به PRTG

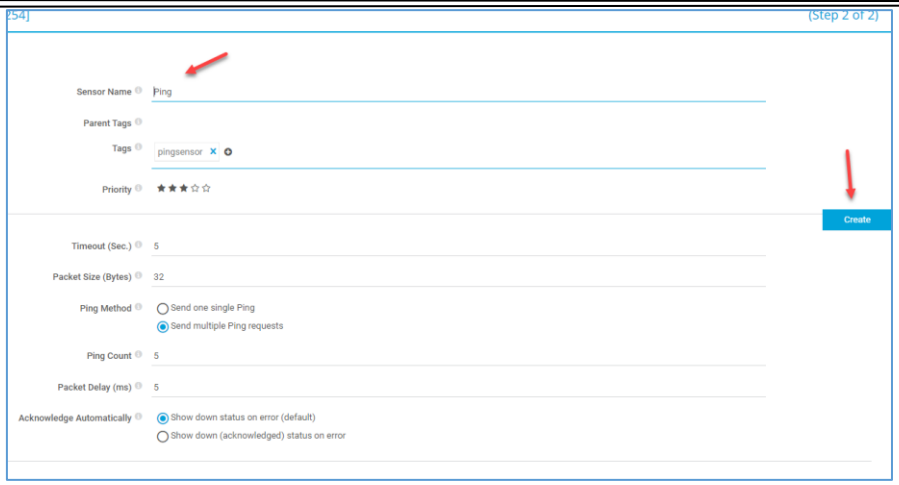
در شکل ۹–۵۶، و در قسمت بالای صفحه باید دسته‌های مورد نیاز خود را انتخاب کنید، برای مثال می‌خواهیم سنسور Ping را به سرور اضافه کنیم، برای این کار گزینه‌ی Availability/Uptime را انتخاب کنید و گزینه‌ی Ping را انتخاب کنید.



شکل ۹ - ۵۶ اضافه کردن دستی دستگاه به PRTG

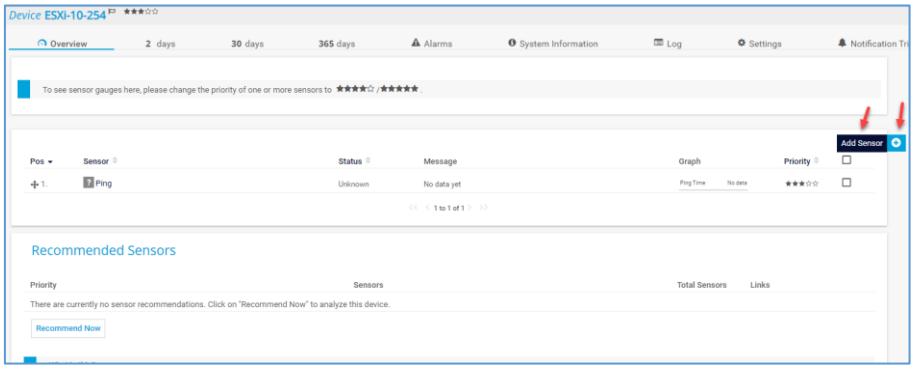
در شکل ۹–۵۷، تنظیمات مربوط به سنسور Ping را مشاهده می‌کنید که می‌توانید آنها را تغییر دهید، بر روی Create کلیک کنید.

www.takbook.com



شکل ۹- ۵۷ اضافه کردن دستی دستگاه به PRTG

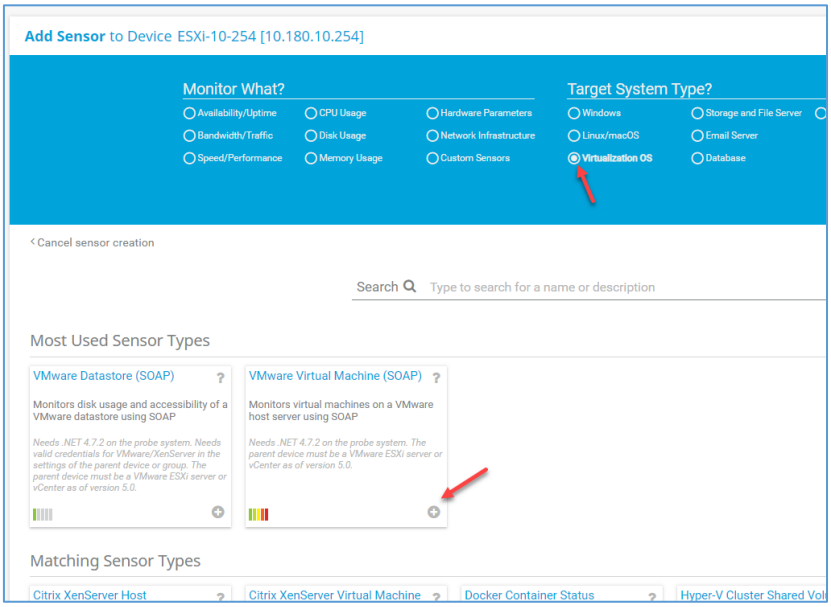
همان‌طور که در شکل ۹-۵۸، مشاهده می‌کنید سنسور مورد نظر به لیست اضافه شده است و بعد از مدت زمان مشخص آنلاین خواهد شد، در این صفحه برای اضافه کردن سنسورهای دیگر بر روی آیکون + کلیک و گزینه‌ی Add Sensor را انتخاب کنید.



شکل ۹- ۵۸ اضافه کردن دستی دستگاه به PRTG

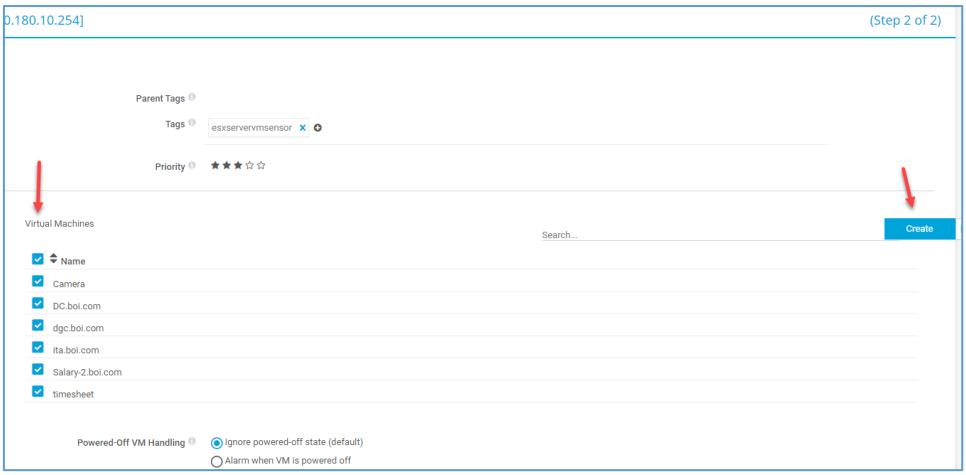
چون در حال کار بر روی ESXi هستیم، برای اینکه مشاین‌های مجازی که بر روی سرور ESxi قرار دارد را مدیریت کنیم باید دسته‌ی Virtualization OS را به مانند شکل ۹-۵۹، انتخاب کنید، در زیر آن دو دسته به شما نمایش داده می‌شود که یکی برای ماشین مجازی و دیگری برای Datastore سرور ESxi است که در حال حاضر بر روی آیکون گزینه‌ی VMware Virtual Machine (SOAP) کلیک کنید.

www.takbook.com



شکل ۹- ۵۹ اضافه کردن دستی دستگاه به PRTG

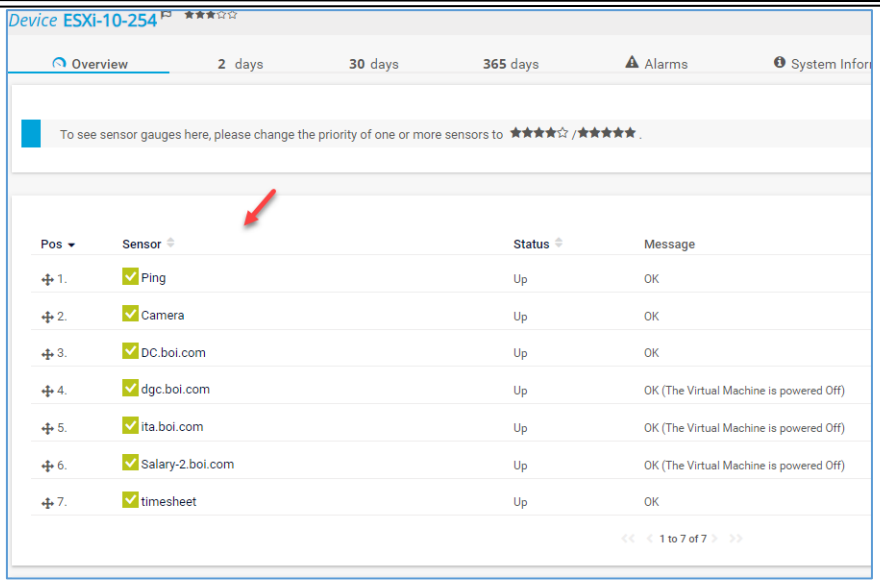
همان‌طور که در شکل ۹-۶۰، مشاهده می‌کنید، تمام ماشین‌های مجازی در دسترس قرار گرفته است و می‌توانید همه آنها را انتخاب کنید و بر روی Create کلیک کنید.



شکل ۹- ۶۰ اضافه کردن دستی دستگاه به PRTG

همان‌طور که در شکل ۹-۶۱، مشاهده می‌کنید سنسورها با موفقیت اضافه شدند و در حال کار هستند.

www.takbook.com



شکل ۹- ۶۱ اضافه کردن دستی دستگاه به PRTG

۹-۱-۷ اضافه کردن میکروتیک به PRTG

یکی از پروتکل‌هایی که در همه‌ی دستگاه‌های شبکه وجود دارد، پروتکل SNMP است.

پروتکل SNMP (Simple Network Management Protocol) یکی از مهم‌ترین و پرکاربردترین پروتکل‌ها در مدیریت شبکه است. این پروتکل به مدیران شبکه اجازه می‌دهد تا دستگاه‌های مختلف شبکه مانند روترها، سوئیچ‌ها، سرورها، پرینترها، و حتی دستگاه‌های IoT را مانیتور و مدیریت کنند.

SNMP پروتکلی است که برای نظارت و مدیریت دستگاه‌های شبکه طراحی شده است. این پروتکل در لایه‌ی کاربرد (Application Layer) مدل OSI فعالیت می‌کند و به مدیران شبکه اجازه می‌دهد تا اطلاعات مربوط به دستگاه‌های شبکه را دریافت کرده و همچنین تغییرات مدیریتی را اعمال کنند.

SNMP در چندین نسخه مختلف منتشر شده است که هر کدام ویژگی‌ها و قابلیت‌های متفاوتی دارند:

الف) SNMPv1

این نسخه اولین و ساده‌ترین نسخه SNMP است که در دهه ۱۹۸۰ معرفی شد. امنیت در این نسخه بسیار ضعیف است و تنها شامل یک مکانیسم ساده احراز هویت با استفاده از یک Community String (رشته جامعه) است.

ب) SNMPv2c

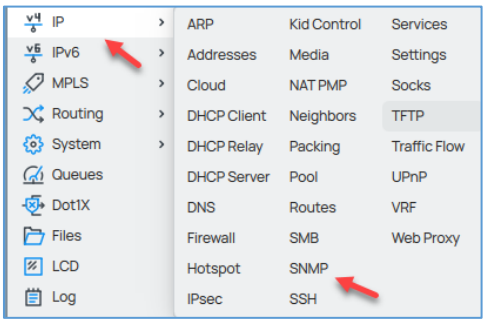
این نسخه بهبودهایی در زمینه عملکرد و قابلیت‌ها نسبت به SNMPv1 دارد، از جمله امکان انتقال تعداد بیشتری از داده‌ها در هر پیام. امنیت در SNMPv2c همچنان ساده و مبتنی بر Community String است.

ج) SNMPv3

www.takbook.com

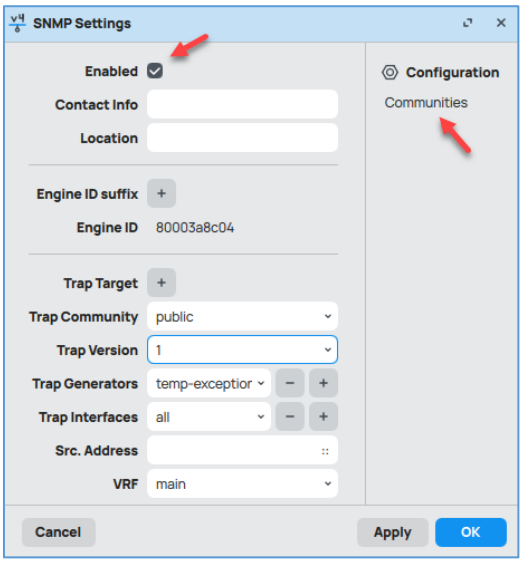
این نسخه آخرین و امن‌ترین نسخه SNMP است. در SNMPv3، قابلیت‌های امنیتی مانند رمزنگاری و احراز هویت اضافه شده است که باعث می‌شود اطلاعات ارسال‌شده بین مدیر و عامل SNMP محافظت شود. همچنین، این نسخه کنترل بیشتری بر دسترسی‌ها و اطلاعات ارائه می‌دهد.

در این بخش می‌خواهیم اطلاعات روتر میکروتیک را از طریق پروتکل SNMP به PRTG انتقال دهیم، برای این کار به مانند شکل ۹-۶۲، وارد روتر میکروتیک شوید و از قسمت IP بر روی SNMP کلیک کنید.



شکل ۹- ۶۲ اضافه کردن میکروتیک به PRTG

در شکل ۹-۶۳، تیک گزینه‌ی Enable را انتخاب کنید تا سرویس SNMP فعال شود و برای اینکه تنظیمات دقیق را انجام دهیم بر روی Communities کلیک کنید.



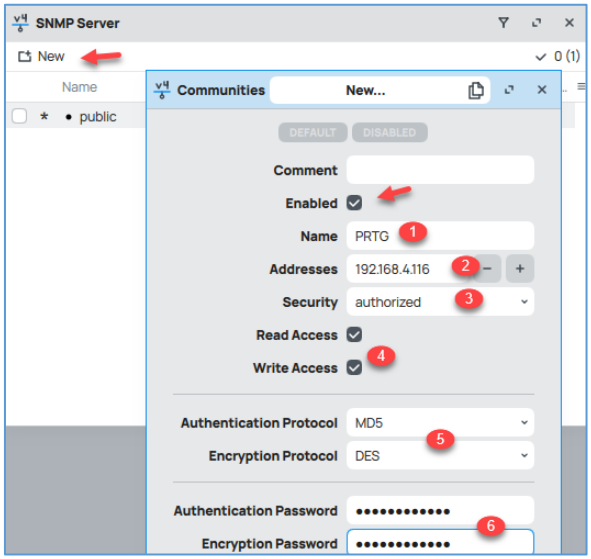
شکل ۹- ۶۳ اضافه کردن میکروتیک به PRTG

در شکل ۹-۶۴، تیک گزینه‌ی Enable را انتخاب کنید و در قسمت شماره‌ی یک باید یک نام وارد کنید توجه داشته باشید این نام همان نام کاربری است که در ادامه باید از آن استفاده کنیم، در قسمت Address باید

www.takbook.com

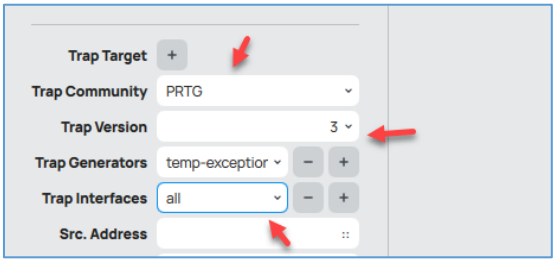
آدرس سرور PRTG را وارد کنیم، در قسمت Security که مربوط به امنیت ارتباط این پروتکل است باید گزینه‌ی Authorized را انتخاب کنید.

در قسمت شماره‌ی ٤ باید مشخص کنید که دسترسی به چه صورت باشد، برای اینکه دسترسی PRTG به کل اطلاعات روتر دسترسی داشته باشد باید هر دو گزینه را تیک بزنید، در قسمت شماره‌ی پنج باید نوع رمزنگاری و احراز هویت را مشخص کنید که دو گزینه‌ی MD5 و DES بهترین انتخاب است، در قسمت شماره‌ی شش باید یک رمز برای همان نام کاربری در قسمت Authentication وارد کنید و در قسمت Encryption باید یک رمز دوم وارد کنید که در ادامه از ان استفاده می‌کنیم، بر روی OK کلیک کنید.



شکل ۹- ۶۴ اضافه کردن میکروتیک به PRTG

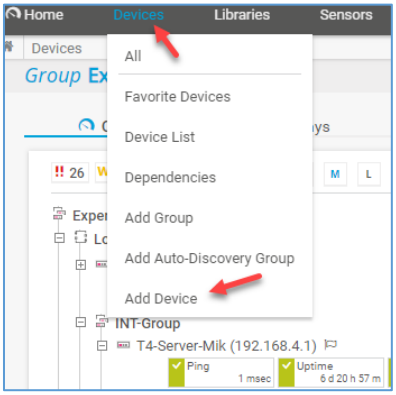
در شکل ۹-٦٥، و در قسمت TRAP Community همان نام که در قسمت قبل ایجاد کردیم را انتخاب کنید و در قسمت TRAP Version باید ورژن شماره‌ی سه را انتخاب کنید، توجه داشته باشید در قسمت TRAP Interface می‌توانید مشخص کنید که چه Interface را می‌خواهید بررسی کنید به صورت پیش‌فرض بر روی All قرار دارد و شما بر اساس نیاز خود باید Interface خود را انتخاب کنید.



شکل ۹- ۶۵ اضافه کردن میکروتیک به PRTG

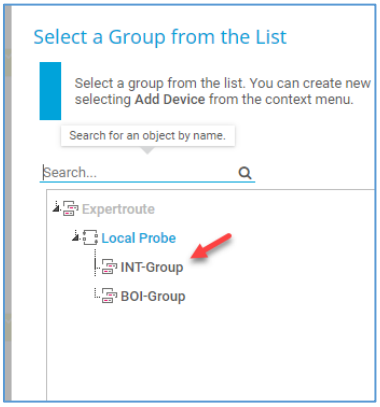
www.takbook.com

همه چیز برای اضافه کردن میکروتیک به PRTG آماده است، به مانند شکل ۹-۶۶، وارد PRTG می‌شویم و بر روی ADD Devices کلیک می‌کنیم.



شکل ۹- ۶۶ اضافه کردن میکروتیک به PRTG

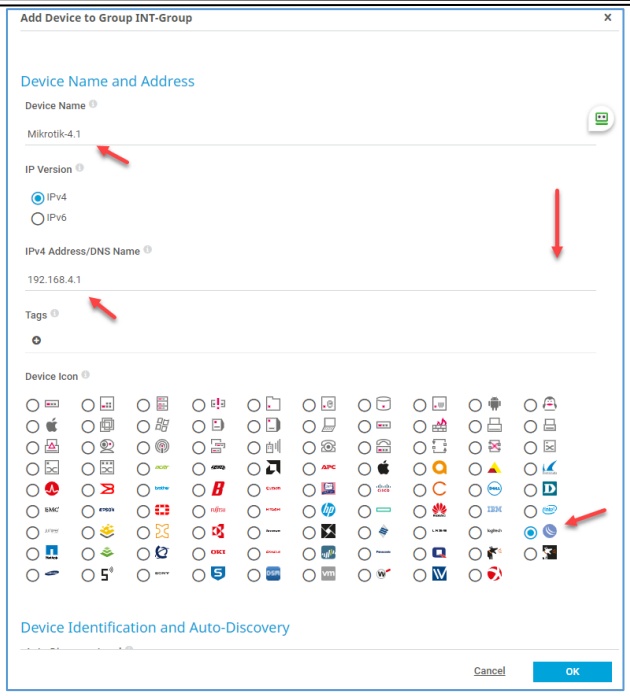
در ادامه کار به مانند شکل ۹-۶۷، گروه مورد نظر خود را انتخاب کنید.



شکل ۹- ۶۷ اضافه کردن میکروتیک به PRTG

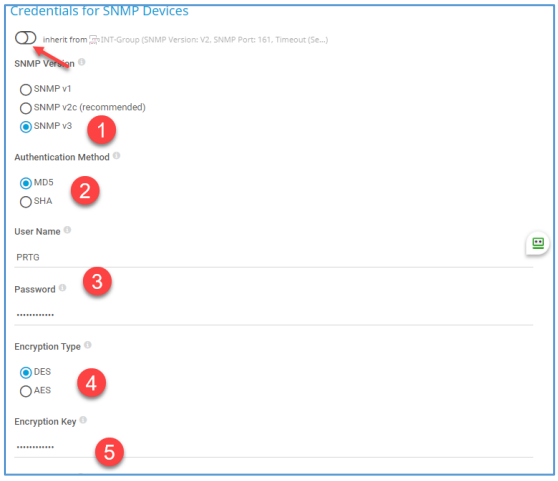
در شکل ۹-۶۸، باید یک نام برای روتر میکروتیک خود در نظر بگیرید که به دلخواه می‌باشد، در قسمت آدرس هم باید آدرس روتر میکروتیک را وارد کنید و در قسمت آیکون باید یک آیکون برای مدیریت بهتر انتخاب کنید، بعد از این کار صفحه را به سمت پایین اسکرول کنید.

www.takbook.com



شکل ۹- ۶۸ اضافه کردن میکروتیک به PRTG

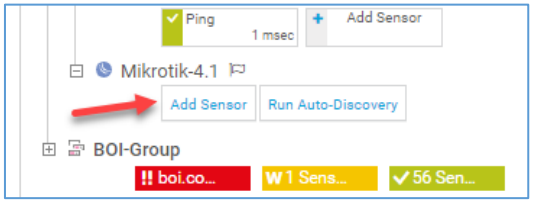
در شکل ۹-۶۹، در قسمت شماره‌ی یک باید ورژن سوم SNMP را انتخاب کنید و در قسمت شماره‌ی دو نوع احراز هویت را دقیقاً به مانند تنظیمات میکروتیک یعنی MD5 انتخاب کنید و در قسمت شماره‌ی سه باید نام کاربری و رمز عبور را که در میکروتیک تنظیم کردیم در این قسمت وارد کنید و در قسمت شماره‌ی چهار نوع رمزنگاری را DES انتخاب و رمز آن را در قسمت شماره‌ی پنج وارد کنید.



شکل ۹- ۶۹ اضافه کردن میکروتیک به PRTG

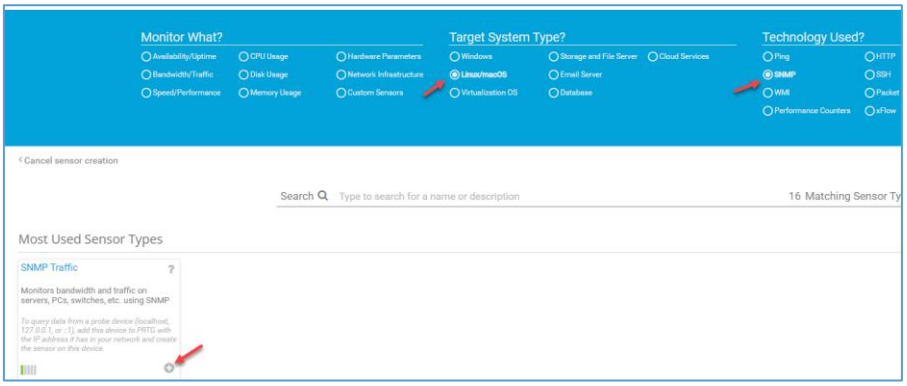
www.takbook.com

همان‌طور که در شکل ۹-۷۰، مشاهده می‌کنید میکروتیک به لیست اضافه شده است و بر روی Add Sensor کلیک کنید.



شکل ۹- ۷۰ اضافه کردن میکروتیک به PRTG

در شکل ۹-۷۱، باید پروتکل SNMP را انتخاب کنید و نوع سیستم‌عامل را لینوکس انتخاب کنید در صفحه پایینی آن بر روی آیکون + مربوط به SNMP Traffic کلیک کنید.



شکل ۹- ۷۱ اضافه کردن میکروتیک به PRTG

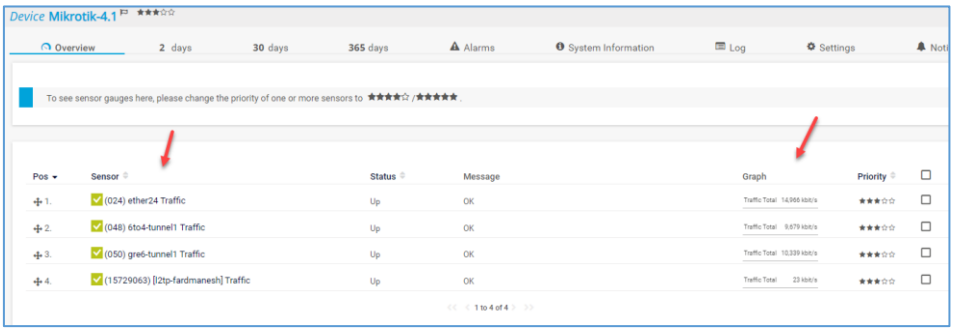
هانطور که در شکل ۹-۷۲، مشاهده می‌کنید تمام اینترفیس‌های مربوط به روتر میکروتیک در دسترس قرار گرفته است و می‌توانید همه یا هر کدام که نیاز دارید را انتخاب کنید، توجه داشته باشید اینترفیس‌هایی که با رنگ مشکی‌تر مشخص شده‌اند یعنی روی این اینترفیس‌ها تراقیک ردو بدل میشه، بعد از انتخاب بر روی Create کلیک کنید تا به لیست اضافه شود.



شکل ۹- ۷۲ اضافه کردن میکروتیک به PRTG

www.takbook.com

همان‌طور که در شکل ۹-۷۳، مشاهده می‌کنید Interfaceهای مورد نظر به لیست اضافه شده است و فعال شده‌اند.



شکل ۹- ۷۳ اضافه کردن میکروتیک به PRTG

www.takbook.com

www.takbook.com

www.takbook.com

فصل دهم

بررسی Failover Clustring

Failover Clustring ۱۰-۱

Failover Clustering یا کلاسترینگ انتقال خودکار (جابه‌جایی خودکار) یک فناوری است که به منظور افزایش قابلیت اطمینان، دسترسی‌پذیری بالا (High Availability) و تحمل خرابی (Fault Tolerance) در سیستم‌های کامپیوتری و سرورها استفاده می‌شود.

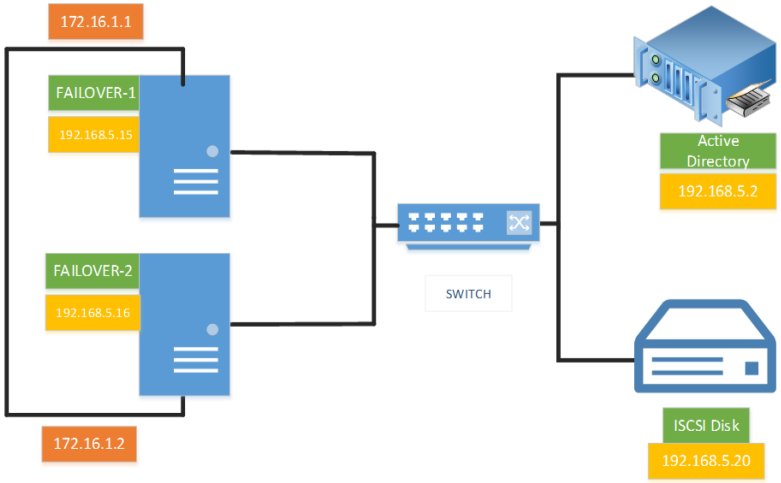
زمانی که صحبت از داده‌ها و سرورهای مهمی می‌شود خود به خود به این فکر می‌افتیم چگونه این سرورها را همیشه روشن نگه داریم یعنی اینکه دسترسی به داده‌های آن در یک لحظه هم نباید با اختلال روبرو شود، برای انجام این کار مایکروسافت سرویسی با نام Failover Clustering را معرفی کرد که در این سرویس چند سرور به‌عنوان Node در گروهی قرار دارند و چنانچه برای یکی از سرورها مشکلی ایجاد شود سرورهایی دیگری که در آن گروه قرار دارند جایگزین آن می‌شوند.

مفهوم Failover Clustering

در این فناوری، چندین سرور یا سیستم به صورت یک گروه (کلاستر) با هم کار می‌کنند. یکی از این سیستم‌ها به عنوان گره اصلی (Active Node) وظایف یا سرویس‌ها را اجرا می‌کند و بقیه به عنوان گره‌های پشتیبان (Passive Nodes) آماده هستند تا در صورت خرابی گره اصلی، به صورت خودکار یا دستی، وظایف را بر عهده بگیرند. این فرآیند را Failover می‌نامند.

برای انجام این کار نیاز به چند سرور به‌مانند شکل ۱۰-۱، داریم، در این سناریو نیاز به یک سرور Active Directory، یکی سرور ISCSI برای ایجاد دیسک ISCSI و دسترسی از طریق شبکه، و دو سرور FAILOVER که باید نقش FAILOVER را بازی کنند که البته این چند سرور از طریق چند سوئیچ به هم متصل می‌شوند و دو سرور FAILOVER باید یک کارت شبکه‌ی دیگر هم داشته باشند.

www.takbook.com

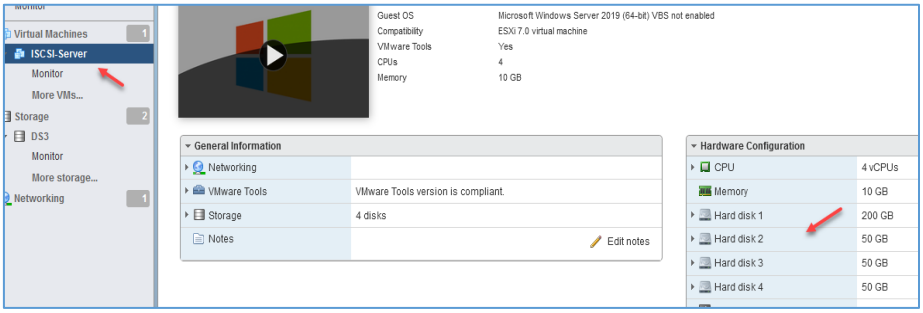


شکل ۱۰- ۱ *Failover Clustring*

۱۰-۱-۱ تنظیمات سرور iSCSI

برای شروع کار باید سرور ISCSI را آماده کنیم، برای ایجاد این سرور شما می‌توانید از نرم‌افزارهای رایگان مانند FreeNAS و... استفاده کنید و دیسک‌های تحت شبکه با پروتکل ISCSI را ایجاد کنید، ولی در این آموزش ما از یک ویندوز سرور ۲۰۲۵ استفاده می‌کنیم.

برای شروع کار و ایجاد سرور، پیشنهاد می‌شود که از سرورهای مجازی برای این کار استفاده کنید، تا نحوه ایجاد و مدیریت آن آسان باشد، برای همین ما از یک سرور ESXi استفاده کردیم و یک ماشین مجازی به مانند شکل ۱۰-۲، یک ماشین مجازی با نام ISCSI-Server ایجاد کردیم و به آن چهار هارد اضافه کردیم، برای کار Failover Clustring نیاز به چهار هارد دیسک از نوع ISCSI داریم تا بتوانیم از آن در این سناریو استفاده کنیم، بعد از ایجاد ماشین مورد نظر بر روی آن ویندوز سرور ۲۰۲۵ نصب می‌کنیم.

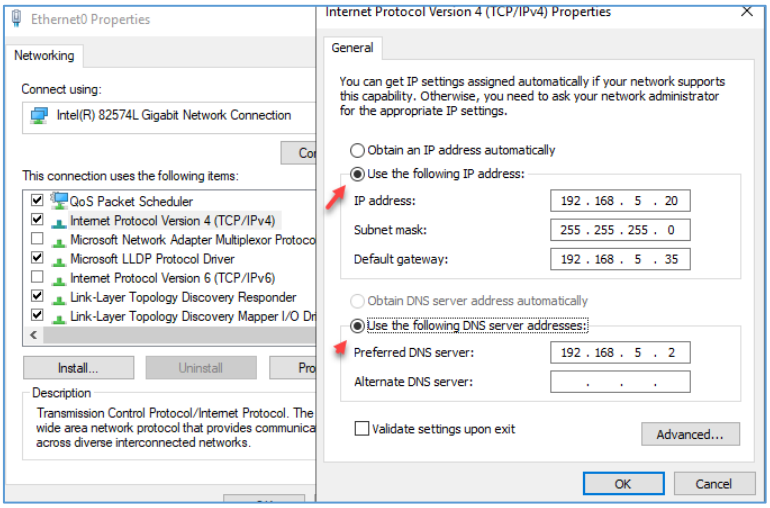


شکل ۱۰- ۲ *تنظیمات سرور iSCSI*

www.takbook.com

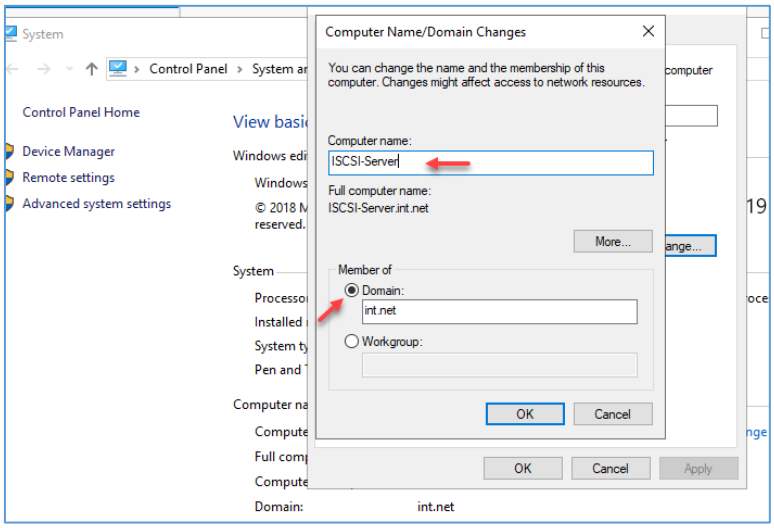
بعد از اجرا شدن ویندوز مورد نظر اولین کاری که انجام می‌دهید این است که آدرس IP را به‌صورت دستی وارد کنید و در قسمت نام سرور هم یک نام برای آن وارد و آن را عضو دومین کنید.

به‌مانند شکل ۱۰-۳، IP سرور مورد نظر را وارد و بر روی OK کلیک کنید، البته می‌توانستید از سرویس DHCP هم برای این کار استفاده کنید.



شکل ۱۰- ۳ تنظیمات آدرس

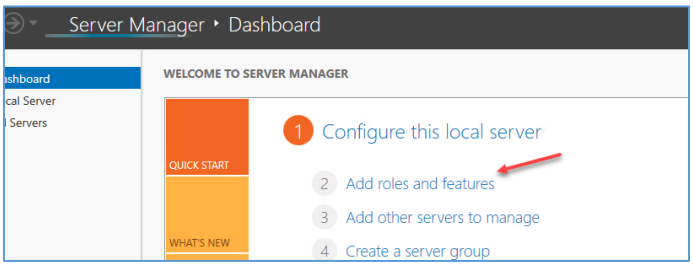
در شکل ۱۰-٤، باید نام سرور را وارد و آن را عضو دومین کنید.



شکل ۱۰- ۴ عضو کردن در دومین

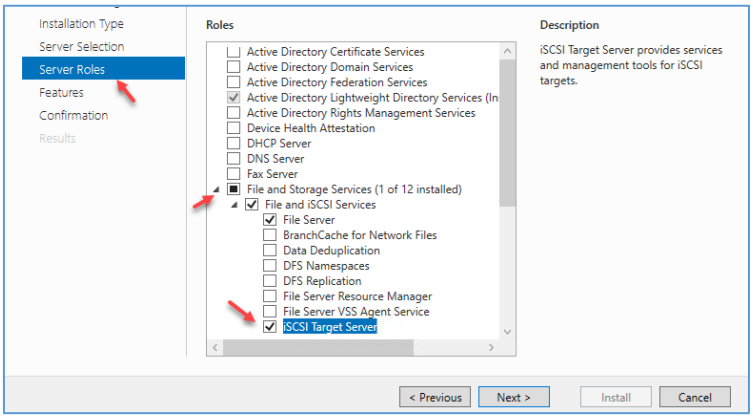
www.takbook.com

بعد از اینکه مراحل بالا را انجام دادید باید سرویس ISCSI را بر روی سرور نصب کنیم، برای این کار به‌مانند شکل ۱۰-۵، وارد Server Manager شوید و بر ری Add Roles and features کلیک کنید.



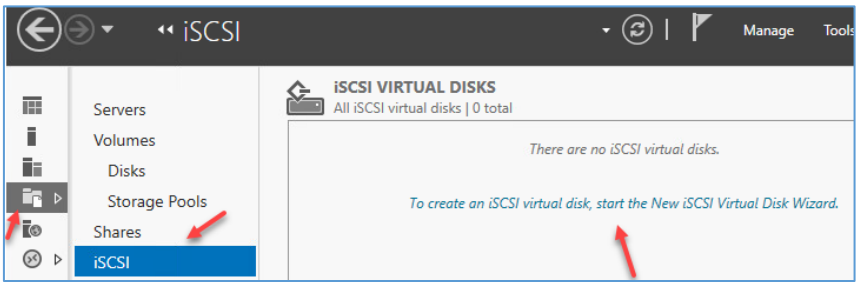
شکل ۱۰- ۵ تنظیمات سرور iSCSI

به‌مانند شکل ۱۰-٦، وارد Server Roles شوید و از زیر مجموعه‌ی File and ISCSI Services تیک گزینه‌ی ISCSI Target Server را انتخاب و بر روی Next کلیک کنید و در ادامه بر روی Install کلیک کنید، فقط توجه داشته باشید در قسمت آخر تیک گزینه‌ی Restart را انتخاب کنید تا سرویس بعد از نصب Restart شود.



شکل ۱۰- ۶ تنظیمات سرور iSCSI

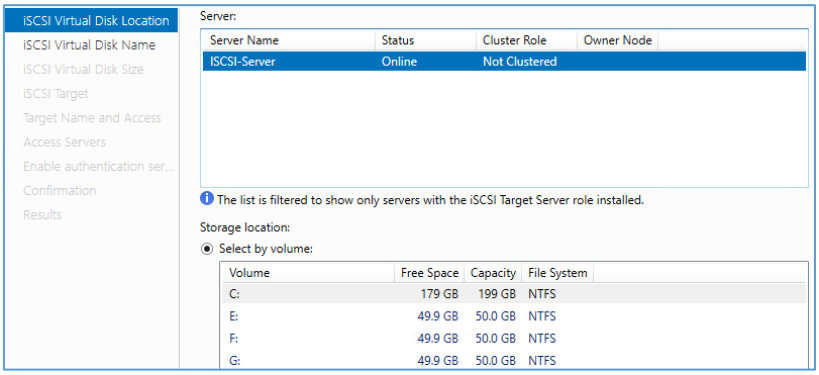
به‌مانند شکل ۱۰-۷، در قسمت File and Storage Services وارد iSCSI شوید و بر روی To Create an iSCSI virtual disk کلیک کنید.



شکل ۱۰- ۷ تنظیمات سرور iSCSI

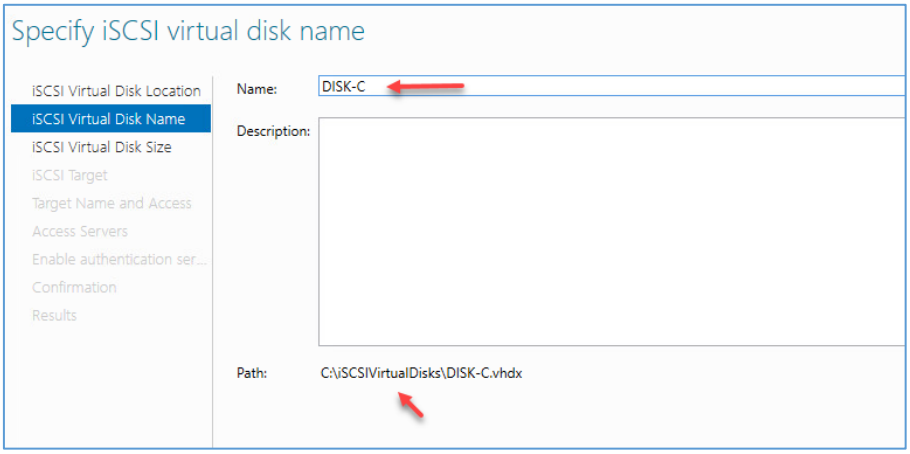
www.takbook.com

در شکل ۱۰-۸، تمام هارد دیسک‌های مجازی که به ماشین مورد نظر اضافه کردیم را مشاهده می‌کنید که در ادامه باید آن را برای سرورهای مورد نظر به اشتراک بگذاریم، یکی از هاردها را از لیست انتخاب کنید و روی Next کلیک کنید؛ توجه داشته باشید که برای هر هارد باید این کار را انجام دهید.



شکل ۱۰- ۸ تنظیمات سرور iSCSI

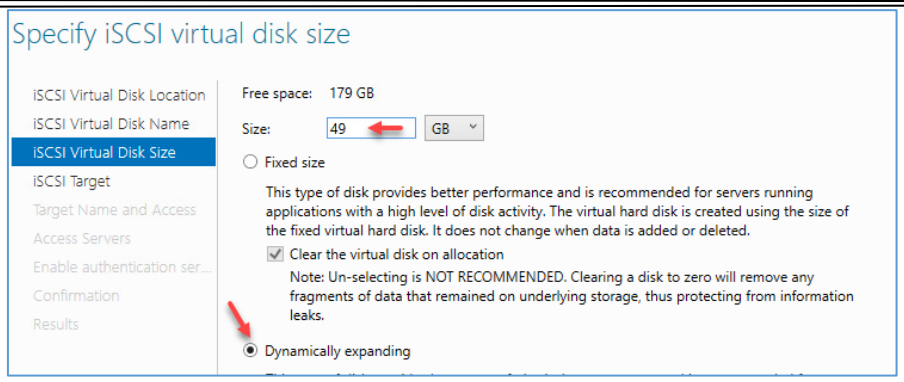
در شکل ۱۰-۹، باید یک نام برای دیسک مجازی خود انتخاب کنید که در زیر صفحه مسیر ذخیره شدن این دیسک مشخص شده است.



شکل ۱۰- ۹ تنظیمات سرور iSCSI

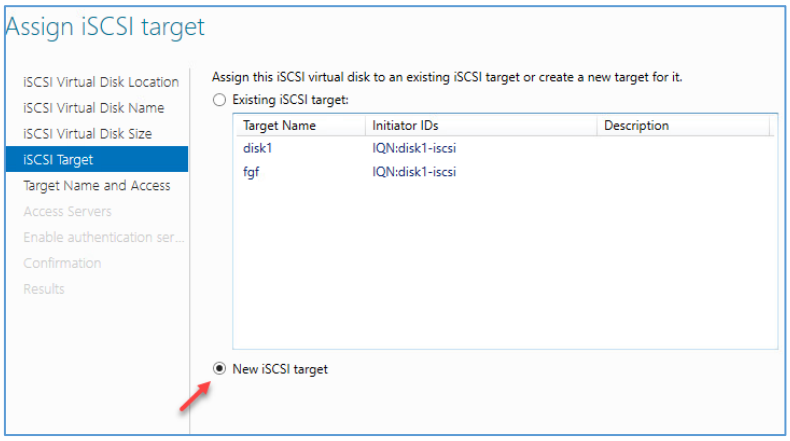
در شکل ۱۰-۱۰، باید حجم مورد نظر برای ایجاد دیسک مجازی را مشخص کنید، که در اینجا ٤٩ گیگ وارد شده است که البته بستگی به نوع کار و حجم اطلاعات شما دارد، توجه داشته باشید اگر گزینه‌ی Fixed را انتخاب کنید، کل فضا به این هارد مجازی اختصاص داده خواهد شد ولی اگر گزینه‌ی Dynamically را انتخاب کنید به مرور زمان این حجم پر خواهد شد که پیشنهاد خود مایکروسافت گزینه اول است.

www.takbook.com



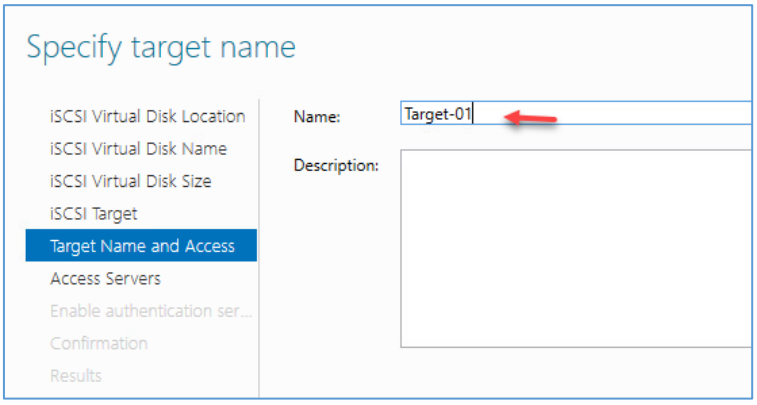
شکل ۱۰- ۱۰ تنظیمات سرور iSCSI

در شکل ۱۰-۱۱ گزینه‌ی New iSCSI target را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۰- ۱۱ تنظیمات سرور iSCSI

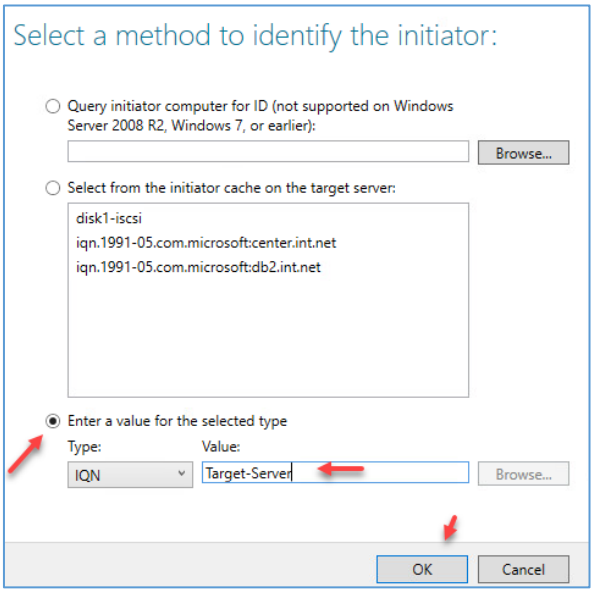
در شکل ۱۰-۱۲، باید یک نام برای target خود به دلخواه وارد و بر روی Next کلیک کنید.



شکل ۱۰- ۱۲ تنظیمات سرور iSCSI

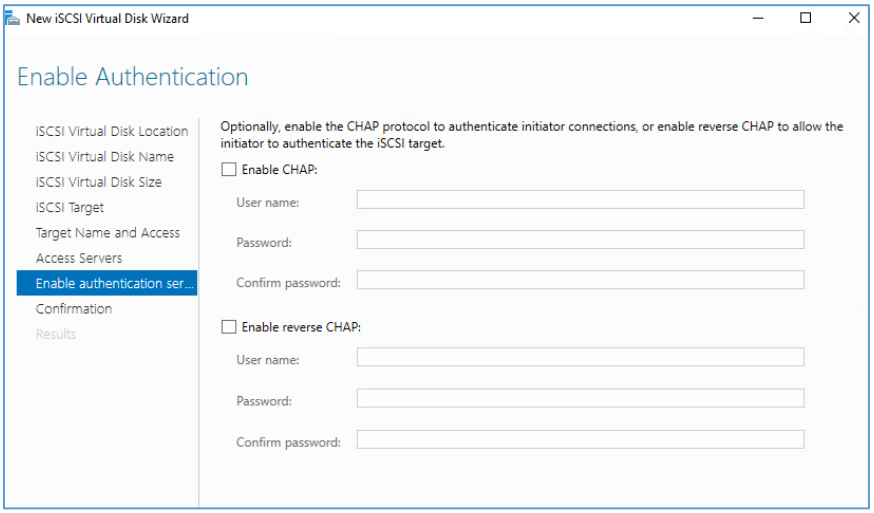
www.takbook.com

در شکل ۱۰-۱۳، گزینه‌ی Enter a value for selected type را انتخاب کنید و یک نام وارد کنید، توجه داشته باشید که این نام مهم بوده و در ادامه برای ارتباط با هارد دیسک مجازی از آن استفاده خواهد شد.



شکل ۱۰-۱۳ تنظیمات سرور iSCSI

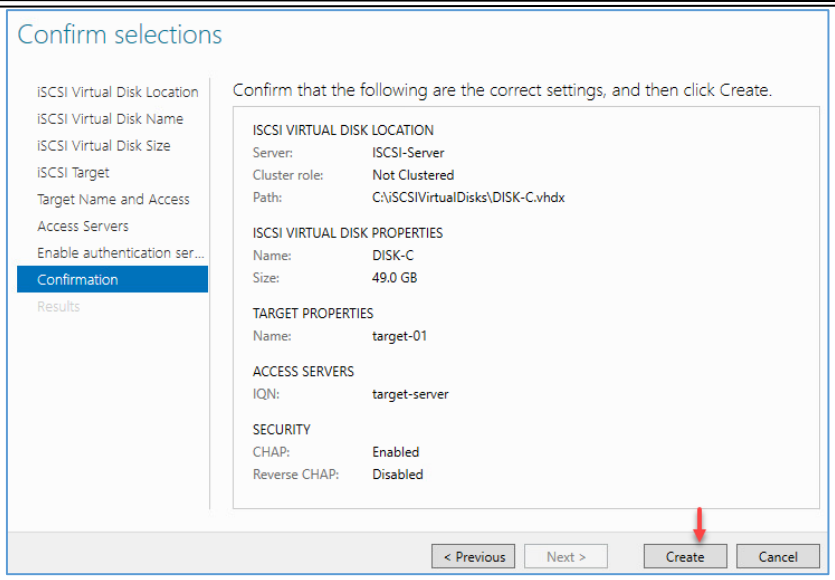
در شکل ۱۰-۱٤، می‌توانید ارتباط خود را رمزگذاری کنید، تا کسی نتواند به هارد دیسک مجازی مورد نظر دست پیدا کنید، در حال حاضر نیازی به این کار نیست و بر روی Next کلیک کنید.



شکل ۱۰-۱۴ تنظیمات سرور iSCSI

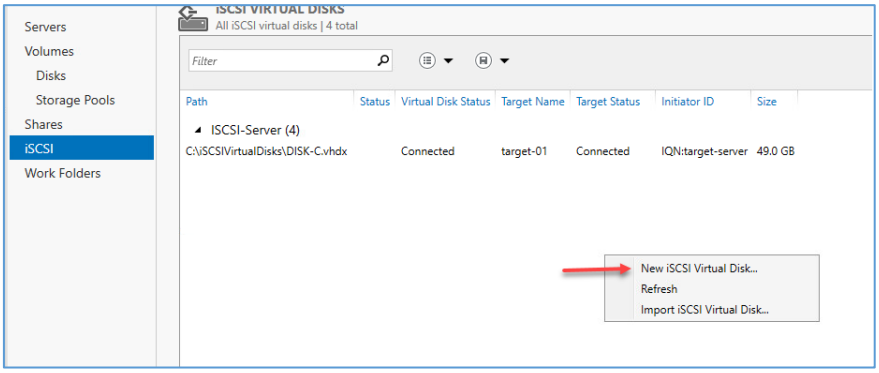
در شکل ۱۰-۱۵، بر روی Create کلیک کنید تا target مورد نظر به همراه هارد دیسک مجازی ایجاد شود.

www.takbook.com



شکل ۱۰- ۱۵ تنظیمات سرور iSCSI

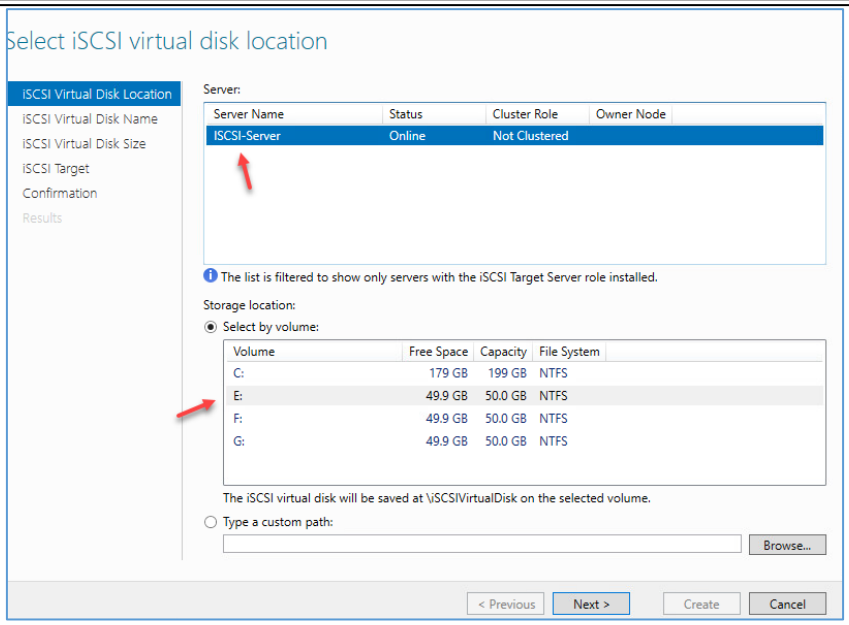
همان‌طور که در شکل ۱۰-۱۶، مشاهده می‌کنید، هارد دیسک مجازی مورد نظر داخل درایو C با حجم ۴۹ گیگابایت ایجاد شده است و در ادامه باید ۳ هارددیسک دیگر را هم به لیست اضافه کنید که برای اینکه به طور کامل متوجه شوید یکی از آنها را ایجاد می‌کنیم، بر روی صفحه‌ی مورد نظر کلیک راست کنید و گزینه‌ی New iSCSI Virtual Disk را انتخاب کنید.



شکل ۱۰- ۱۶ تنظیمات سرور iSCSI

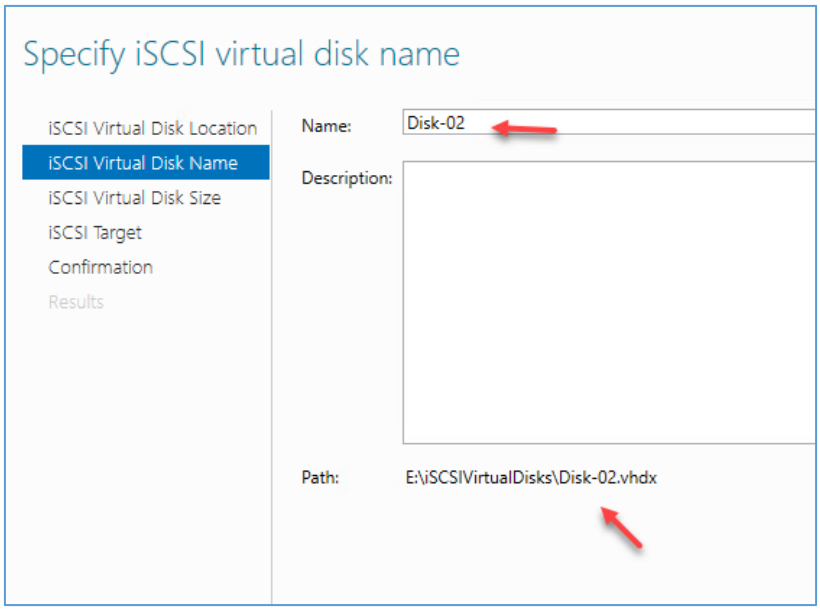
در شکل ۱۰-۱۷، که قبلاً درایو C را برای ایجاد هارد مجازی انتخاب کرده بودیم، حالا باید درایو بعدی یعنی E را انتخاب و بر روی Next کلیک کنیم.

www.takbook.com



شکل ۱۰-۱۷ تنظیمات سرور iSCSI

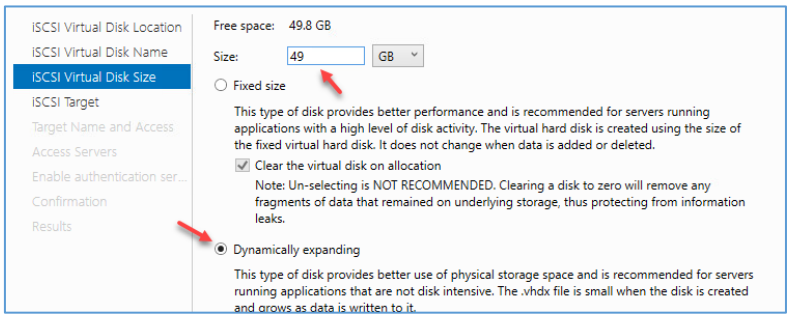
در شکل ۱۰-۱۸، باید نام دیسک را وارد کنید و در پایین صفحه محل ذخیره شدن آن را در درایو E مشاهده می‌کنید.



شکل ۱۰-۱۸ تنظیمات سرور iSCSI

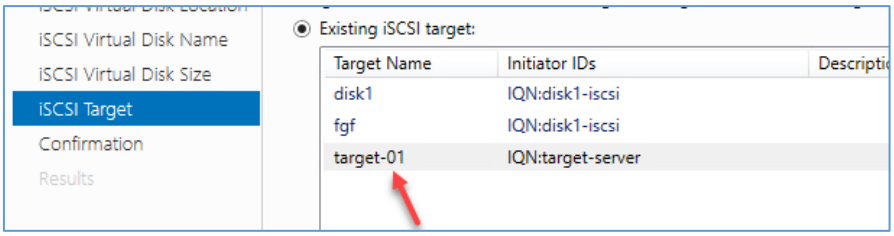
www.takbook.com

در شکل ۱۰-۱۹، باید حجم مورد نظر خود را وارد کنید که در اینجا ٤۹ گیگابایت را وارد و بر روی Next کلیک کنید.



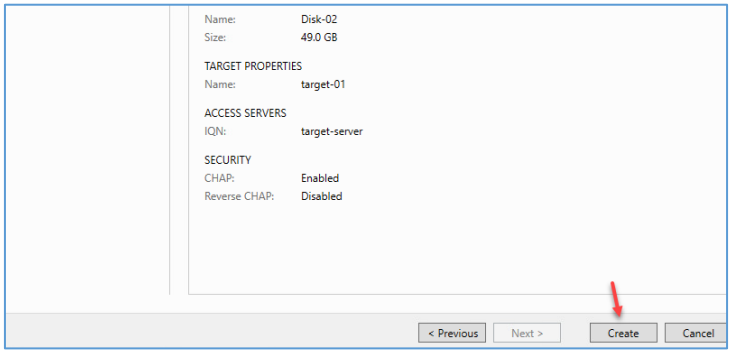
شکل ۱۰- ۱۹ تنظیمات سرور iSCSI

در شکل ۱۰-۲۰، باید در قسمت Existing همان target که در قسمت اول ایجاد کردیم را انتخاب کنید، با این کار این دیسک هم زیر مجموعه‌ی آن target خواهد شد.



شکل ۱۰- ۲۰ تنظیمات سرور iSCSI

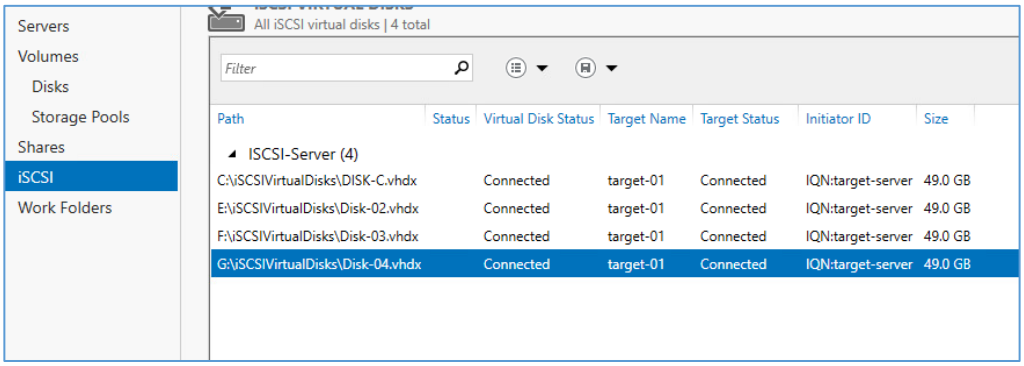
در شکل ۱۰-۲۱، باید بر روی Create کلیک کنید تا هارد دیسک مورد نظر ایجاد شود، توجه داشته باشید که دقیقاً همین مراحل را برای دو دیسک دیگر هم انجام دهید تا جمعاً ٤ دیسک به لیست اضافه شود.



شکل ۱۰- ۲۱ تنظیمات سرور iSCSI

همان‌طور که در شکل ۱۰-۲۲، مشاهده می‌کنید هر چهار دیسک مورد نظر ایجاد شده است و حالا می‌توانیم به آنها متصل شویم.

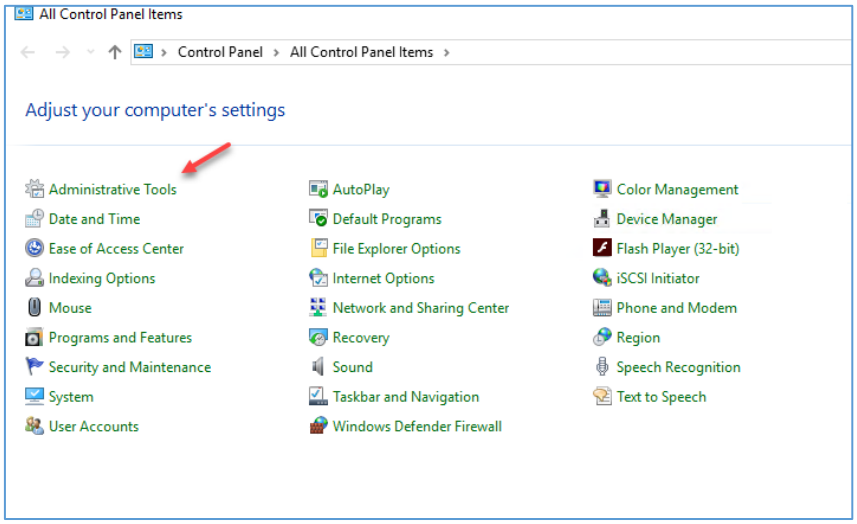
www.takbook.com



شکل ۱۰- ۲۲ تنظیمات سرور iSCSI

۱۰-۱-۲ تنظیمات سرور Failover-1

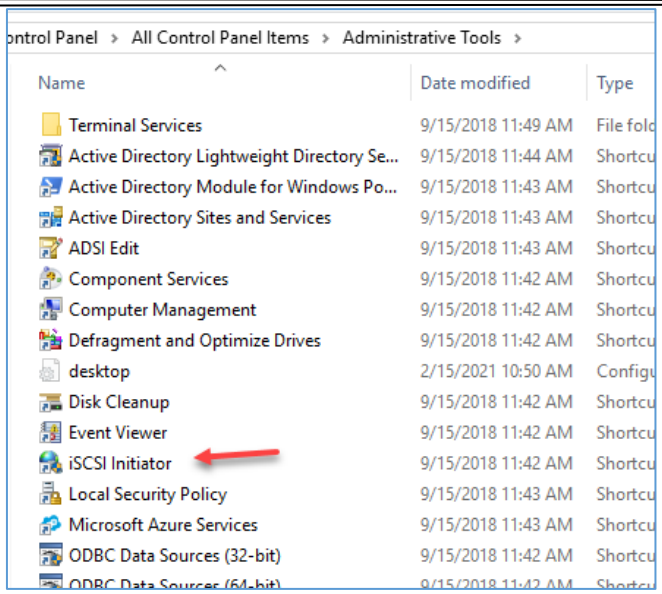
در ادامه کار باید وارد دو سرور Failover شویم و این چهار هارد را به آنها اضافه کنیم، به‌مانند شکل ۱۰-۲۳ وارد کنترل پنل هر کدام از سرورها شوید و بر روی Administrative Tools کلیک کنید.



شکل ۱۰- ۲۳ تنظیمات سرور Failover-1

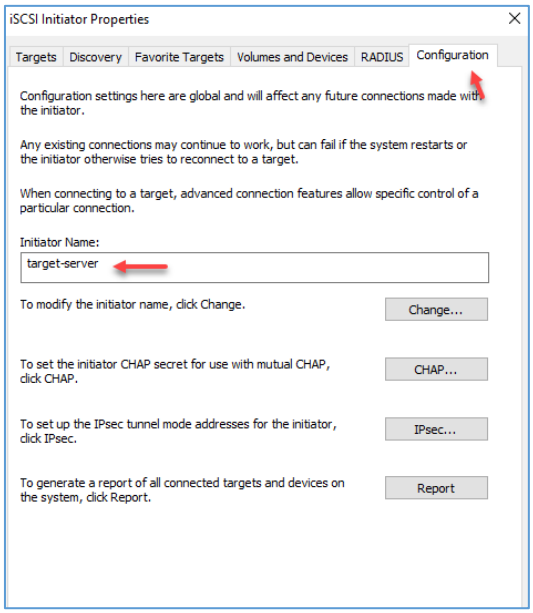
برای متصل شدن به دیسک‌های iSCSI ابزاری وجود دارد با نام iSCSI Initiator که در تمام ویندوزهای سرور موجود است و حتی می‌توانید آن را از اینترنت دانلود کنید و بر روی ویندوز مورد نظر خود نصب کنید، مانند شکل ۱۰-۲٤، بر روی iSCSI Initiator دو بار کلیک کنید.

www.takbook.com



شکل ۱۰- ۲۴ تنظیمات سرور Failover-1

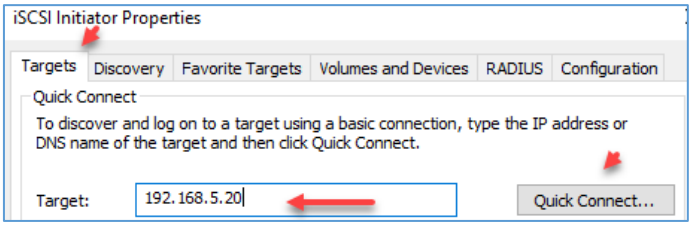
در شکل ۱۰–۲۵، در تب Configuration باید نام Initiator Name را که با نام target—server ایجاد کردیم را وارد کنید.



شکل ۱۰- ۲۵ تنظیمات سرور Failover-1

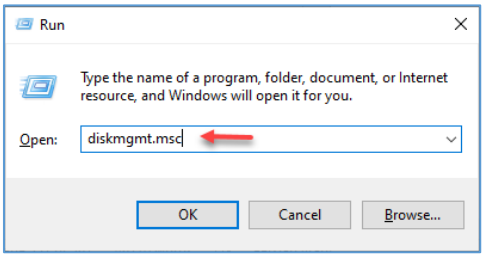
www.takbook.com

در شکل ۱۰-۲۶، در تب Targets باید آدرس IP سرور iSCSI را وارد و بر روی Connect کلیک کنید، با این کار شما توانستید هارد دیسک مورد نظر را به لیست پارتیشن‌های خود اضافه کنید که با هم آنها را آماده‌سازی می‌کنیم.



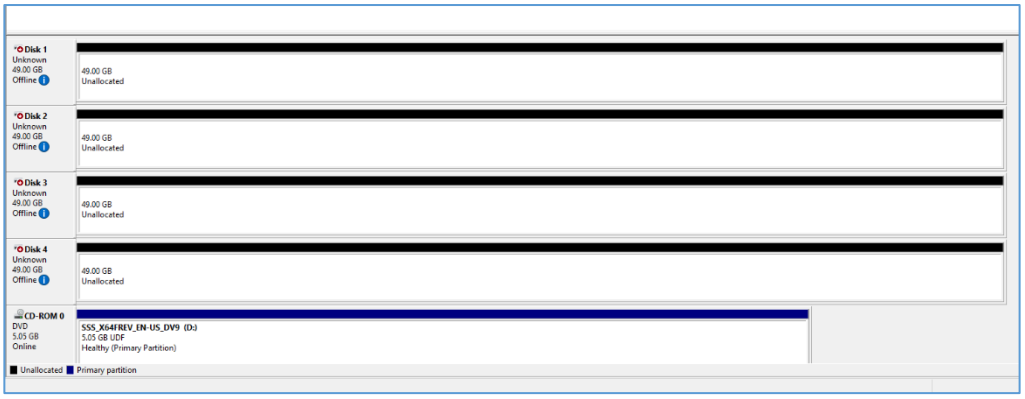
شکل ۱۰- ۲۶ تنظیمات سرور Failover-1

برای اینکه در سرور Failover-01 که عملیات بالا را در آن انجام دادیم بتوانیم هارددیسک‌های iSCSI را مشاهده کنیم باید به‌مانند شکل ۱۰-۲۷، در RUN دستور diskmgmt.msc را اجرا کنید تا سرویس Disk Management اجرا شود.



شکل ۱۰- ۲۷ تنظیمات سرور Failover-1

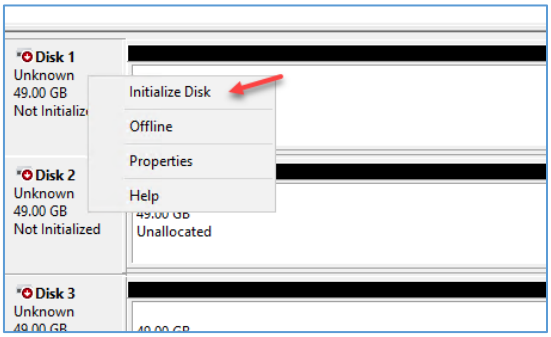
همان‌طور که در شکل ۱۰-۲۸، مشاهده می‌کنید هر چهار هارد به لیست اضافه شده است و باید تنظیمات آنها را انجام دهیم.



شکل ۱۰- ۲۸ تنظیمات سرور Failover-1

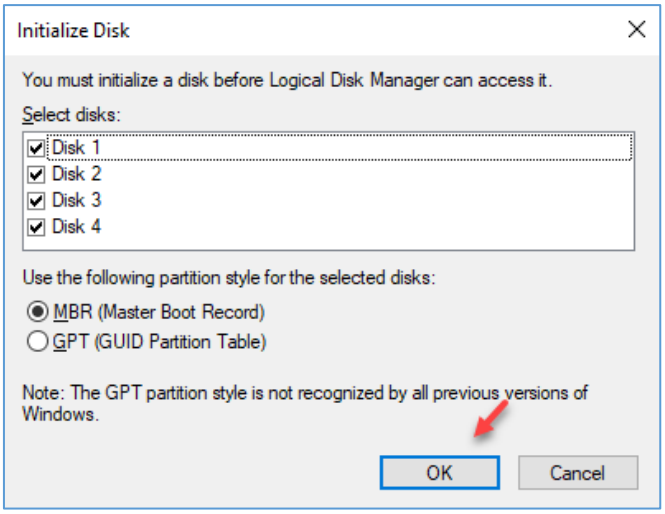
www.takbook.com

برای اینکه این هارد دیسک‌ها را تنظیم کنیم باید به‌مانند شکل ۱۰-۲۹، بر روی دیسک مورد نظر کلیک راست کنید و گزینه‌ی اول یعنی Online و بعد Initialize Disk را انتخاب کنید.



شکل ۱۰- ۲۹ تنظیمات سرور Failover-1

در شکل ۱۰-۳۰، می‌توانید MBR که برای هارد دیسک‌هایی با حداکثر ظرفیت ۲ ترابایت است و GPT برای هارد دیسک‌هایی بیشتر از ۲ ترابایت، انتخاب و بر روی OK کلیک کنید.



شکل ۱۰- ۳۰ تنظیمات سرور Failover-1

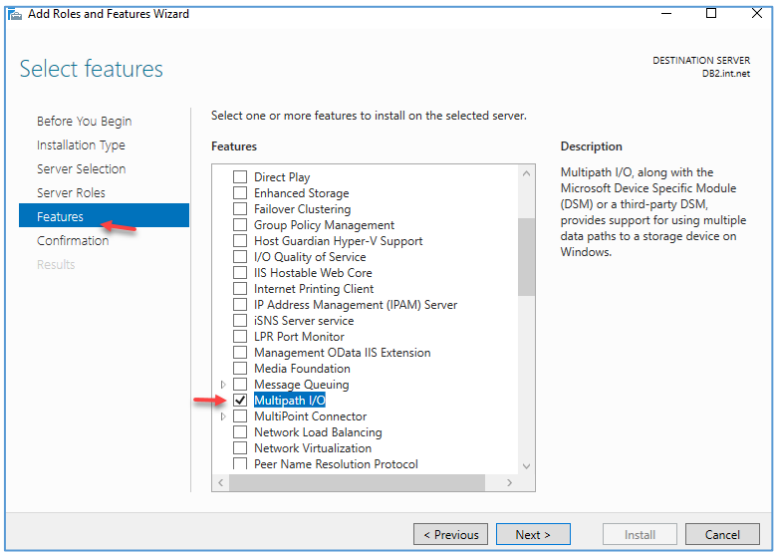
کمی کارهایی که تا این مرحله انجام دادیم را بررسی کنیم، یک سرور iSCSI ایجاد کردیم و روی آن چند هارد متصل کردیم و با سرویس iSCSI چهار هارد مجازی که برای ادامه کار طراحی شده است را ایجاد کردیم و در ادامه از طریق سرور Failover-1 توانستیم از طریق سرویس iSCSI Initiator به هاردهای iSCSI متصل شویم و بعد در سرویس Diskmgmt.msc هاردهای اضافه شده را اول Online و بعد Initialize کردیم و دیگر نباید کار انجام دهیم.

حالا باید وارد سرور Failover-2 شویم و هاردهای iSCSI را به آن هم اضافه کنیم.

www.takbook.com

۳-۱-۱۰ تنظیمات سرور Failover-2

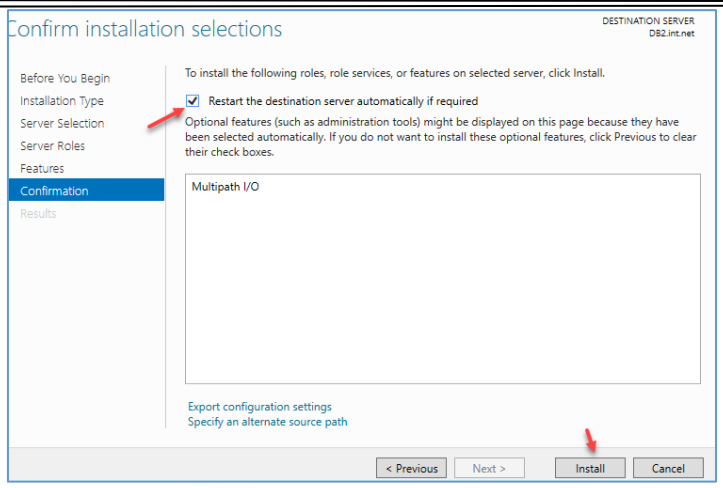
شما در این سرور هم باید آن چهار هارد iSCSI را به لیست اضافه کنید، اما یک مشکل اساسی وجود دارد و آن هم این است که شما نمی‌توانید بیشتر از یک سرور را به صورت پیش‌فرض به سرور iSCSI متصل کنید، برای این کار باید یک سرویس دیگر را بر روی سرور iSCSI نصب کنید و آن هم سرویس Multipath I/O است که به‌مانند شکل ۱۰-۳۱، باید وارد Server Manager در سرور iSCSI شوید و از قسمت Features تیک گزینه‌ی Multipath I/O را انتخاب و بر روی Next کلیک کنید.



شکل ۱۰- ۳۱ تنظیمات سرور Failover-2

در شکل ۱۰-۳۲، حتماً تیک گزینه‌ی Restart the destination… را انتخاب و بر روی Install کلیک کنید.

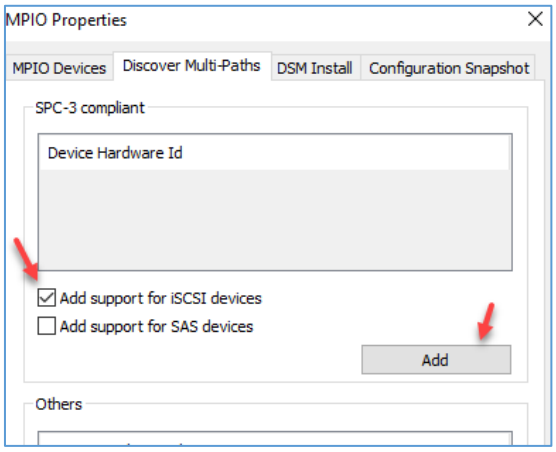
www.takbook.com



شکل ۱۰- ۳۲ تنظیمات سرور *Failover-2*

نکته مهم: این سرویس را در هر سه سرور iSCSI, Failover-1, Failover-2 حتماً باید نصب کنید و به‌صورت زیر تنظیمات آن را انجام دهید.

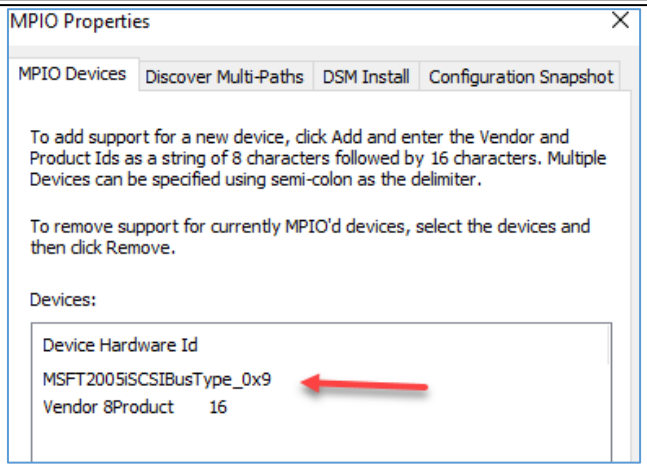
بعد از نصب سرویس وارد Administrative Tools شوید و سرویس MPIO را اجرا کنید، بعد از اجرا به‌مانند شکل ۱۰–۳۳، وارد تب Discover Multi-Paths شوید و تیک گزینه‌ی Add support را انتخاب کنید و بر روی Add کلیک کنید.



شکل ۱۰- ۳۳ تنظیمات سرور *Failover-2*

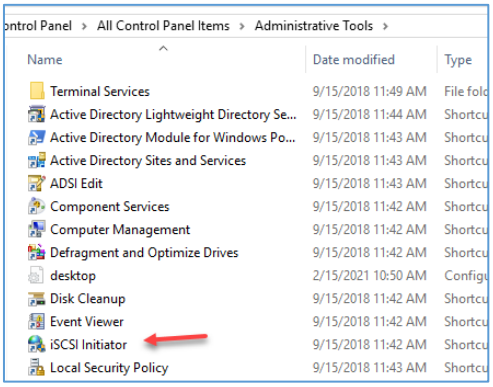
به‌مانند شکل ۱۰–۳٤، وارد تب MPIO Devices شوید و باید در لیست مورد نظر Device مورد نظر را حتماً مشاهده کنید تا عملیات موفقیت‌آمیز باشد.

www.takbook.com



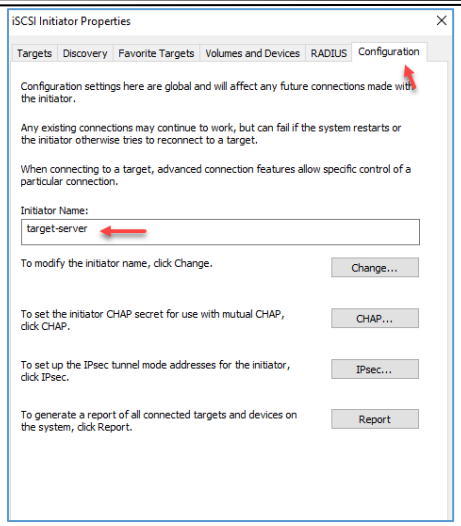
شکل ۱۰- ۳۴ تنظیمات سرور Failover-2

بعد از انجام مراحل بالا باید وارد سرور Failover-2 شوید و به‌مانند شکل ۱۰-۳۵، iSCSI Initiator را اجرا کنید و دقیقاً همان کاری که در سرور اول یعنی Failover-1 انجام دادید در این قسمت هم انجام دهید.

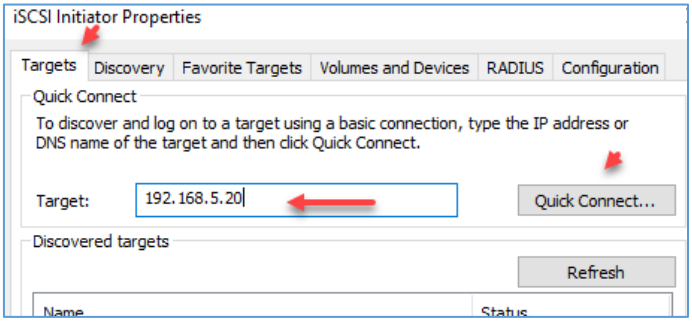


شکل ۱۰- ۳۵ تنظیمات سرور Failover-2

www.takbook.com



شکل ۱۰- ۳۶ تنظیمات سرور Failover-2



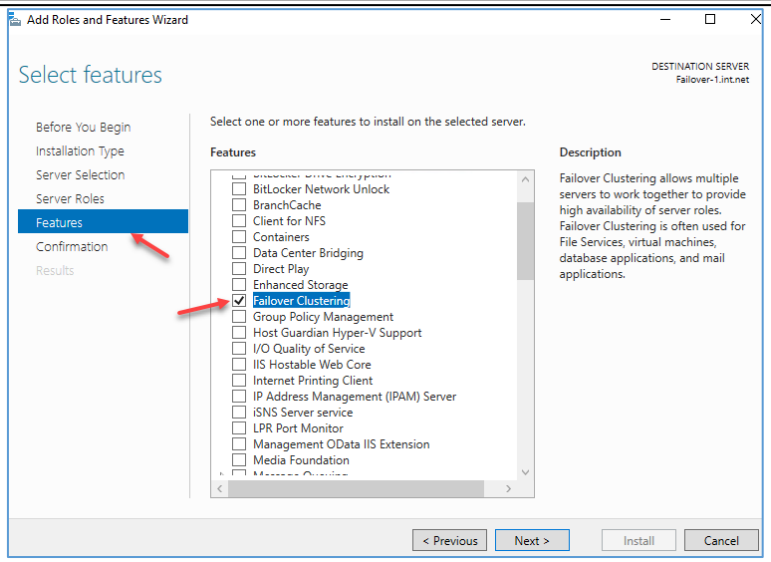
شکل ۱۰- ۳۷ تنظیمات سرور Failover-2

در ادامه هارد دیسک مورد نظر به لیست اضافه و کارهایی را که در سرور Failover-1 انجام دادیم در این سرور هم باید انجام دهیم.

بعد از اینکه هارد دیسک‌های مجازی را در هر سرور ایجاد کردیم باید سرویس‌های دیگری را هم فعال کنیم، سرویس دیگری که از گذشته وجود داشته با نام Application Server بوده که تا ویندوز سرور ۲۰۱۲ وجود داشته ولی در ویندوز سرور ۲۰۲۲ و ۲۰۲۵ این گزینه وجود ندارد ولی سرویس‌های آن به‌صورت پیش‌فرض بر روی ویندوز فعال است و مشکلی از این لحاظ نخواهید داشت.

در ادامه باید سرویس Clustring را بر روی هر دو سرور Failover-1 و Failover-2 نصب کنید، به این صورت که مانند شکل ۱۰–۳۸، وارد Server Manager شوید و تیک گزینه‌ی Failover Clustring را از قسمت Features انتخاب و نصب کنید.

www.takbook.com

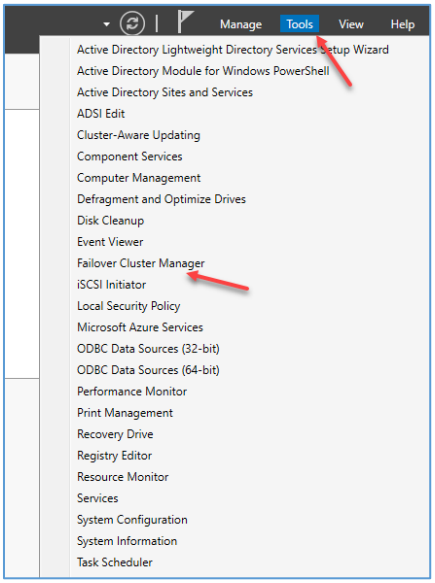


شکل ۱۰- ۳۸ تنظیمات سرور Failover-2

نصب این سرویس کمی زمان‌بر خواهد بود، توجه داشته باشید که بعد از نصب سرویس حتماً سرور باید Restart شود.

در ادامه باید کنسول مدیریتی سرویس Clustring را در هر دو سرور اجرا کنید و کارهای زیر را در هر دو سرور انجام دهید.

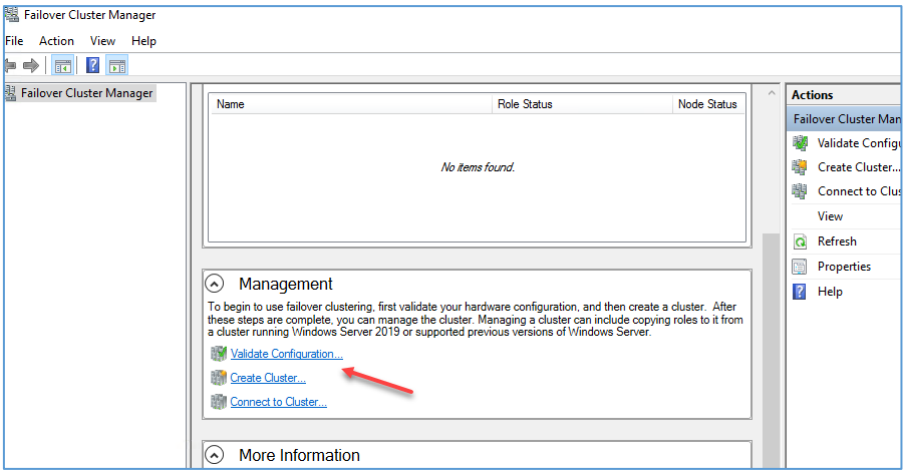
به‌مانند شکل ۱۰-۳۹، وارد Server Manager شوید و از منوی Tools سرویس Clustring را اجرا کنید.



شکل ۱۰- ۳۹ تنظیمات سرور Failover-2

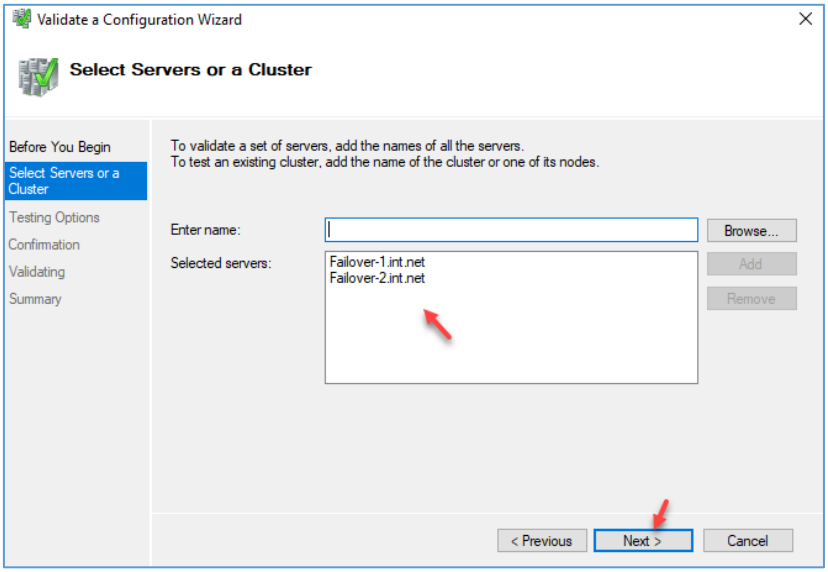
www.takbook.com

اولین کاری که در این سرویس باید انجام دهیم این است که تست می‌گیریم ببینیم ارتباط و تنظیمات انجام شده در هر دو سرور که قرار است کلاستر شوند به درستی انجام شده است یا نه، برای این کار به‌مانند شکل ۱۰-٤۰، بر روی Validate Configuartion کلیک کنید.



شکل ۱۰- ۴۰ تنظیمات سرور Failover-2

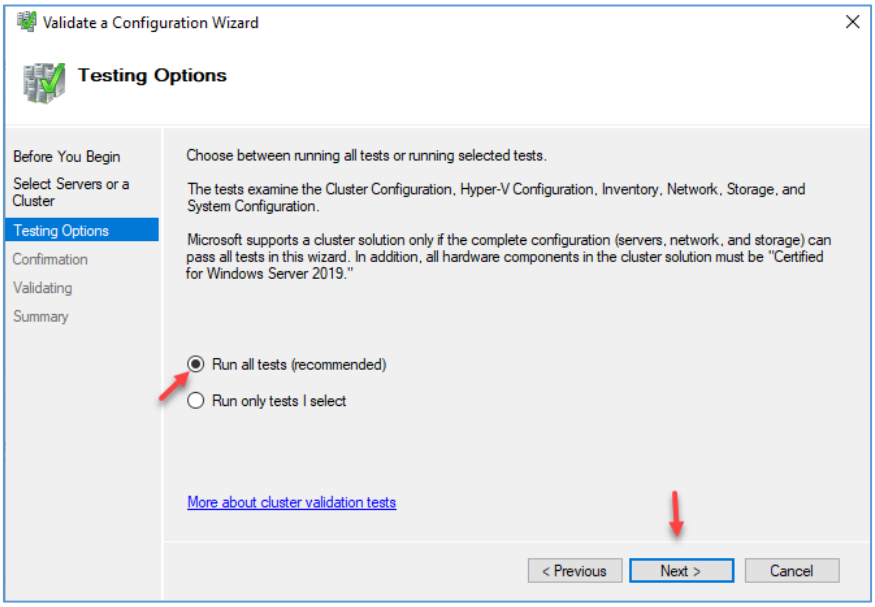
در شکل ۱۰-٤۱، باید نام سرور مورد نظر خود را وارد و بر روی Add کلیک کنید، توجه داشته باشید باید نام هر دو سرور را به لیست اضافه کنید.



شکل ۱۰- ۴۱ تنظیمات سرور Failover-2

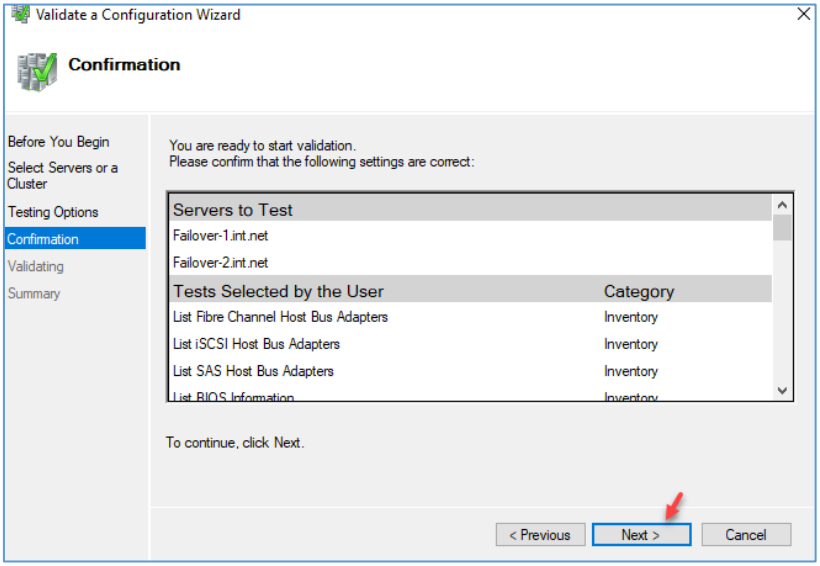
www.takbook.com

در شکل ۱۰-٤۲، باید گزینه‌ی Run all tests را انتخاب کنید تا قبل از اینکه موضوع را عملیاتی کنیم مراحل کار تست شود.



شکل ۱۰- ۴۲ تنظیمات سرور Failover-2

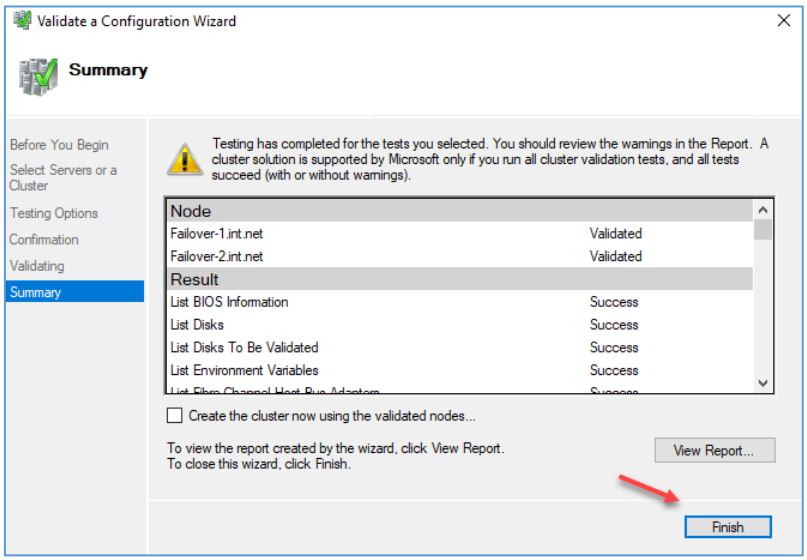
در ادامه کار و در شکل ۱۰-٤۳، بر روی Next کلیک کنید.



شکل ۱۰- ۴۳ تنظیمات سرور Failover-2

www.takbook.com

همان‌طور که در شکل ۱۰-٤٤، مشاهده می‌کنید عملیات با موفقیت انجام شده است، اما شاید برای شما با خطاهای مختلفی مواجه شده باشد که حتماً باید آن خطا ها را بررسی کنیم.



شکل ۱۰- ۴۴ تنظیمات سرور Failover-2

خطاهایی که معمولاً در این قسمت روی می‌دهد شامل موارد زیر است:

۱- کارت شبکه‌ی دوم تعریف نشده باشد.

۲- سیستم تحت دامین نباشد.

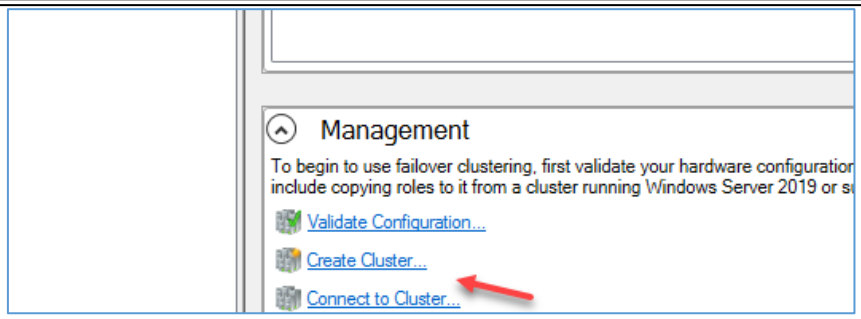
۳- هارد دیسک به درستی در هر دو سرور ایجاد نشده باشد، که این خطا یکی از متداولترین خطاها است.

۴- سرویس MPIO در هر سه سرور فعال نباشد.

اگر همه‌ی مواردهای بالا را به درستی انجام دهید دیگر با خطا مواجه نخواهید شد.

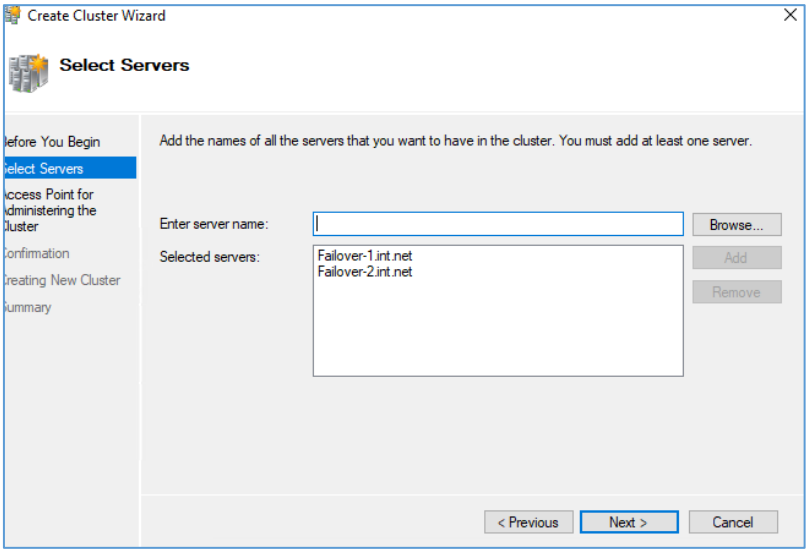
در ادامه کار و بعد از تست موفقیت‌آمیز کار باید Cluster اصلی خود را ایجاد کنیم برای این کار به‌مانند شکل ۱۰-٤٥، بر روی Create Cluster کلیک کنید.

www.takbook.com



شکل ۱۰- ۴۵ تنظیمات سرور Failover-2

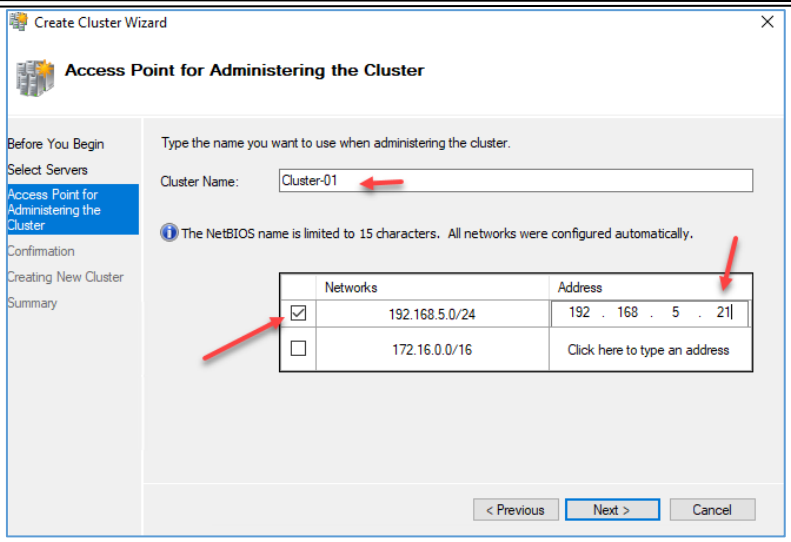
در شکل ۱۰-٤٦، هر دو سرور failover را وارد و بر روی Next کلیک کنید.



شکل ۱۰- ۴۶ تنظیمات سرور Failover-2

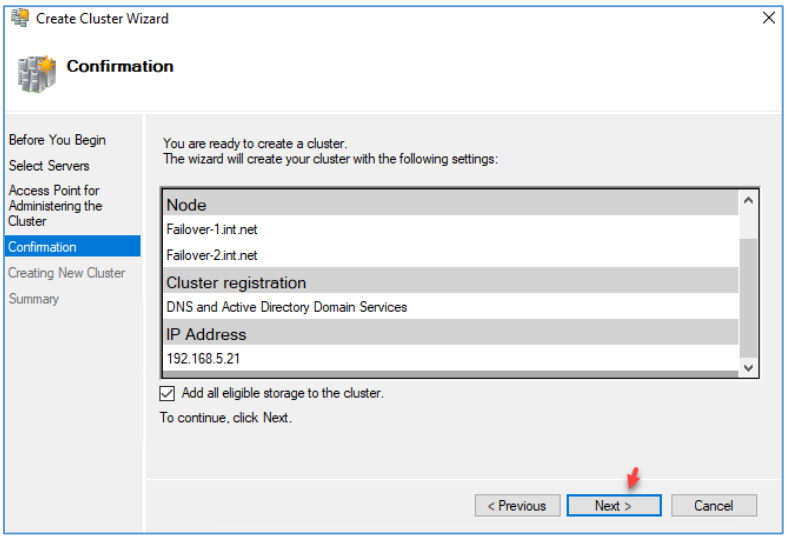
در شکل ۱۰-٤٧، باید مشخص کنید که کدام شبکه به‌عنوان شبکه‌ی Cluster باید انتخاب شود، و زمانی که شبکه‌ی Cluster را انتخاب می‌کنید باید برای آن یک آدرس IP مشخص در نظر بگیرید، که در اینجا شبکه‌ی اصلی یعنی 192.168.5 انتخاب شده و آدرس 192.168.5.21 به‌عنوان شبکه‌ی Cluster در نظر گرفته خواهد شد و بعد از اتمام کانفیگ اگر همه چیز به درستی پیش برود شما می‌توانید این IP را Ping کنید و از آن استفاده کنید.

www.takbook.com



شکل ۱۰- ۴۷ تنظیمات سرور Failover-2

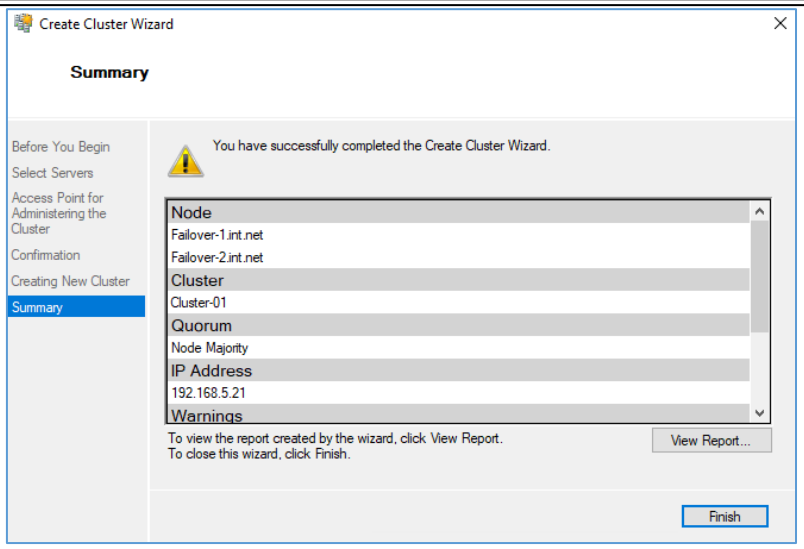
به‌مانند شکل ۱۰-٤۸، بر روی Next کلیک کنید تا کار نصب آغاز شود.



شکل ۱۰- ۴۸ تنظیمات سرور Failover-2

همان‌طور که در شکل ۱۰-٤۹، مشاهده می‌کنید عملیات Clustring به درستی انجام شده است و حالا ما بر روی آدرس 192.168.5.21 سرویس کلاستر داریم و می‌توانید در ادامه از آن استفاده کنیم.

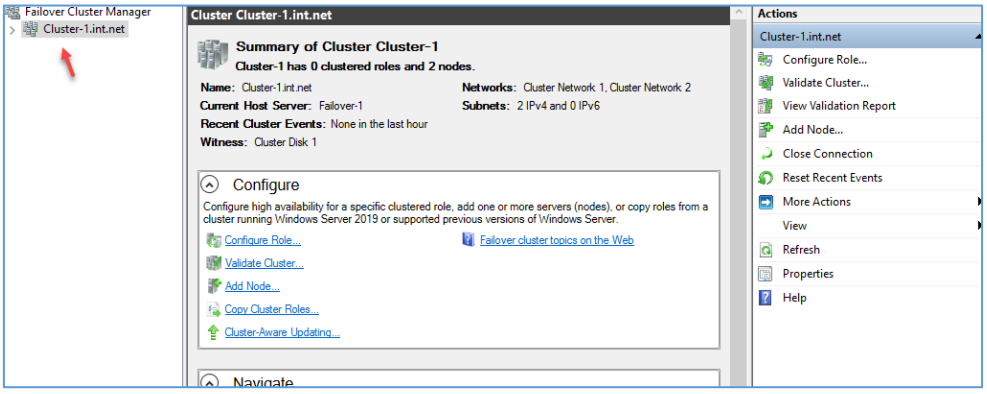
www.takbook.com



شکل ۱۰- ۴۹ تنظیمات سرور Failover-2

توجه داشته باشید که اگر در یک سرور عملیات ایجاد Clustring را انجام دهید در سرور دیگر هم همین تنظیمات انجام خواهد شد.

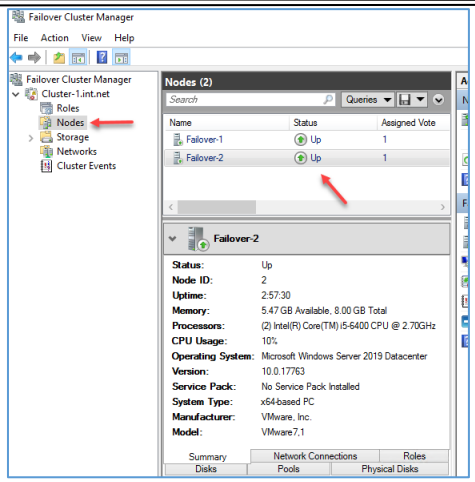
همان‌طور که در شکل ۱۰–۵۰، مشاهده می‌کنید Cluster مورد نظر با موفقیت ایجاد شده است.



شکل ۱۰- ۵۰ تنظیمات سرور Failover-2

اگر به‌مانند شکل ۱۰–۵۱، وارد قسمت Node شوید دو سرور Failover-1 و Failover-2 را مشاهده می‌کنید که هر دو در حالت روشن یعنی UP قرار دارند و می‌توانند سرویس ارائه دهند.

www.takbook.com

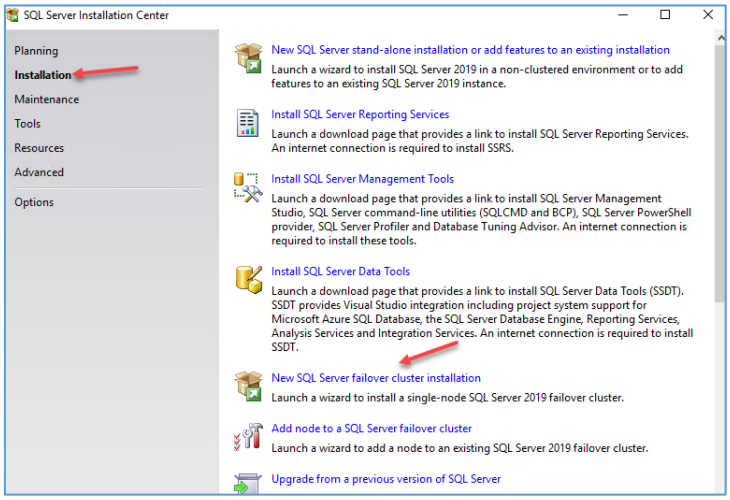


شکل ۱۰- ۵۱ تنظیمات سرور Failover-2

در ادامه کار باید نرم‌افزار SQL Server را بر روی هر دو سرور Failover-1 و Failover-2 نصب کنیم، البته روش نصب با قبل تفاوت خواهد داشت.

برای اینکه این سرورها و سرویس کلاسترینگ را تست بگیریم میخواهیم از نرم‌افزار SQL استفاده کنیم. وارد یکی از سرورها مثلاً Failover-2 می‌شویم و نرم‌افزار SQL Server را برای نصب اجرا می‌کنیم.

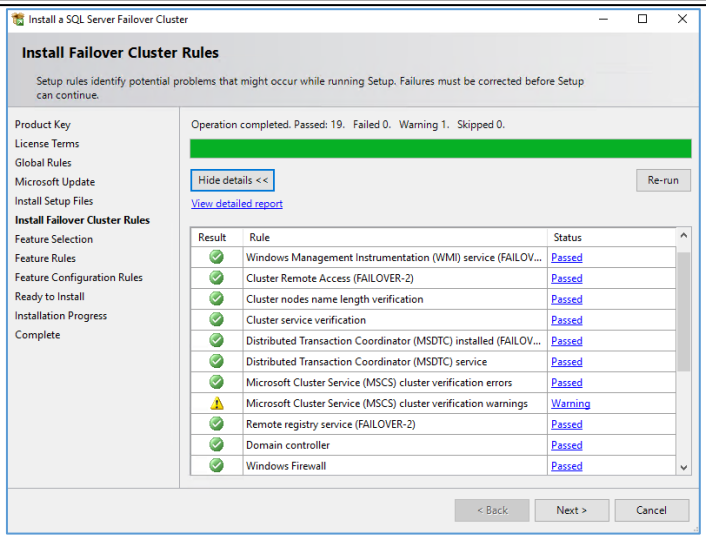
به‌مانند شکل ۱۰-۵۲، وارد Installation شوید و بر روی Installation کلیک کنید و در صفحه‌ی باز شده بر روی New SQL Server failover cluster کلیک کنید.



شکل ۱۰- ۵۲ تنظیمات سرور Failover-2

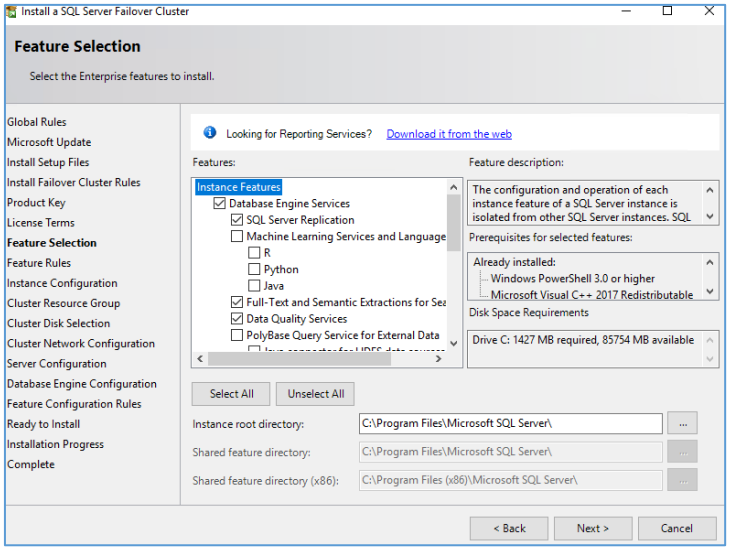
در در شکل ۱۰-۵۳، بررسی‌های اولیه انجام می‌شود که اگر از نظر Clustring مشکلی نباشد می‌توانید کار را ادامه دهید.

www.takbook.com



شکل ۱۰- ۵۳ تنظیمات سرور Failover-2

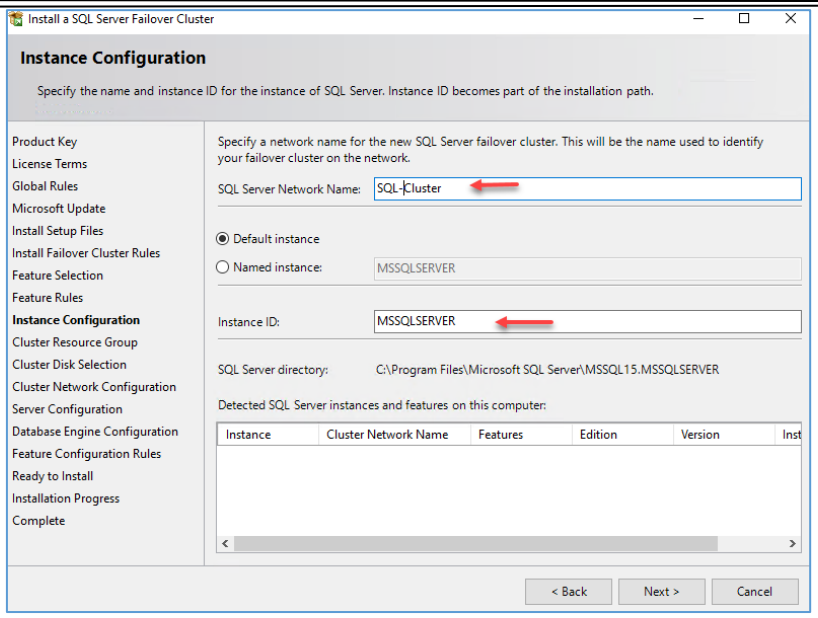
در شکل ۱۰-٥٤، تیک گزینه‌ی Database Engine Services را انتخاب و بر روی Next کلیک کنید، البته این موارد را قبلاً توضیح دادیم.



شکل ۱۰- ۵۴ تنظیمات سرور Failover-2

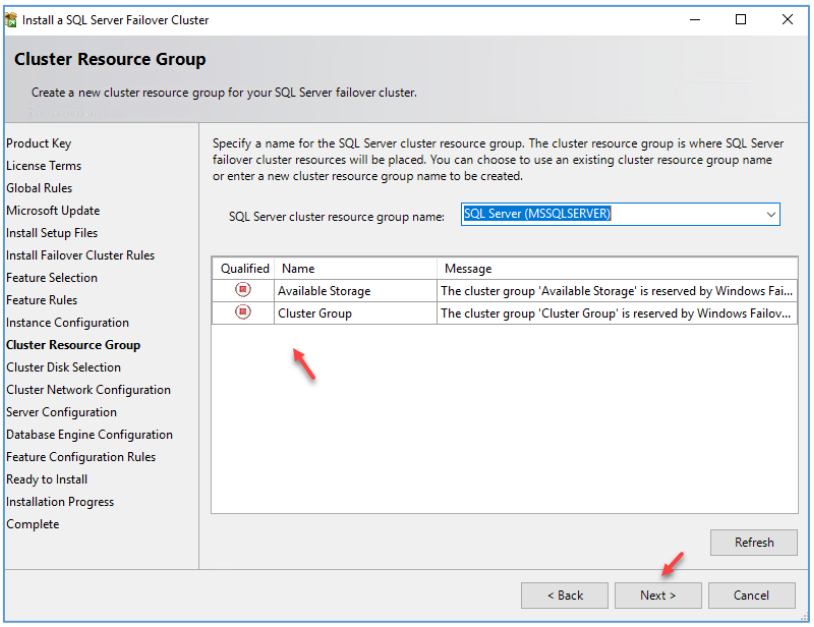
در شکل ۱۰-٥٥، باید در قسمت SQL Server Network Name یک نام به دلخواه خود وارد کنید، البته این نام مهم است و برای دسترسی به SQL باید از این نام استفاده کنیم، در قسمت بعدی هم باید نام Instance را وارد کنید.

www.takbook.com



شکل ۱۰- ۵۵ تنظیمات سرور Failover-2

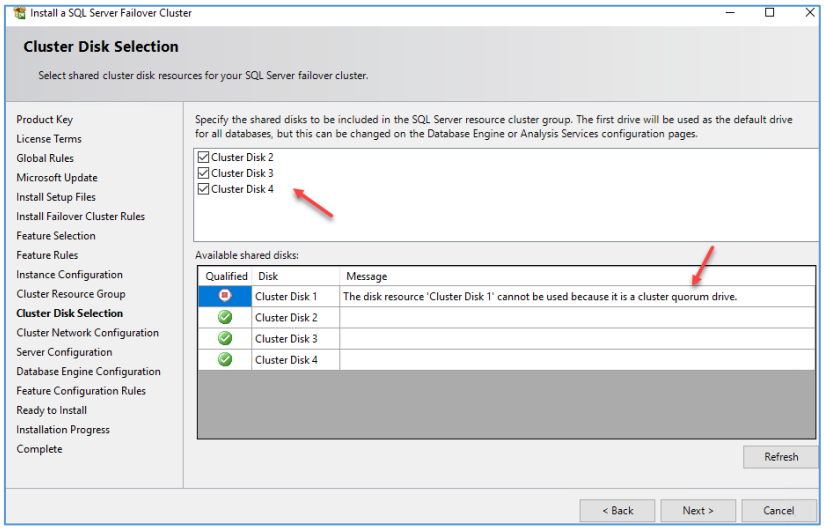
در شکل ۱۰-۵٦، دو سرویس موردنیاز برای فعال‌سازی Clustring در SQL را مشاهده می‌کنید، بر روی Next کلیک کنید.



شکل ۱۰- ۵۶ تنظیمات سرور Failover-2

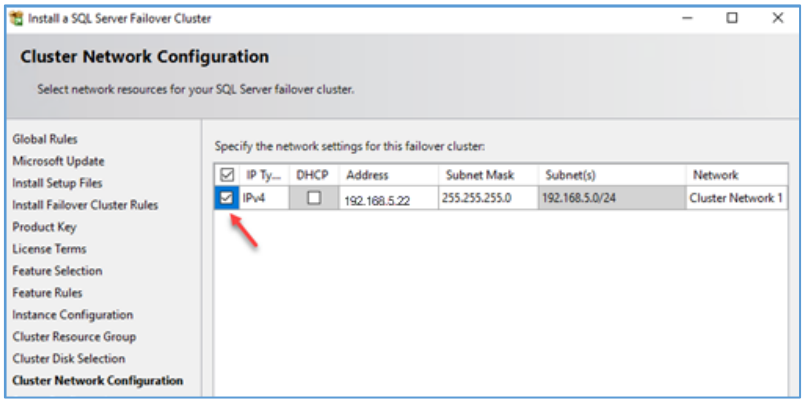
www.takbook.com

در شکل ۱۰-۵۷، باید همه‌ی دیسک‌های موجود را انتخاب کنید، فقط سه دیسک در لیست قرار دارد، اما یک دیسک دیگر که دیسک شماره‌ی یک باشد در لیست برای انتخاب وجود ندارد، دلیل آن هم این است که اصولاً زمانی که سیستم Clustring را فعال می‌کنید، دیسک اول به‌صورت پیش‌فرض به‌عنوان دیسک Quorum انتخاب می‌شود، این دیسک تشکیل‌دهنده‌ی تنظیمات اصلی Clustring است و به‌صورت خودکار تنظیم می‌شود، البته می‌توانستیم در قسمت ایجاد Clustring این دیسک را تنظیم کنیم تا خودش یک دیک را انتخاب نکند، در شکل ۱۰-۵۷، مشخص شده است که کدام دیسک به‌عنوان دیسک Quorum انتخاب شده است.



شکل ۱۰- ۵۷ تنظیمات سرور Failover-2

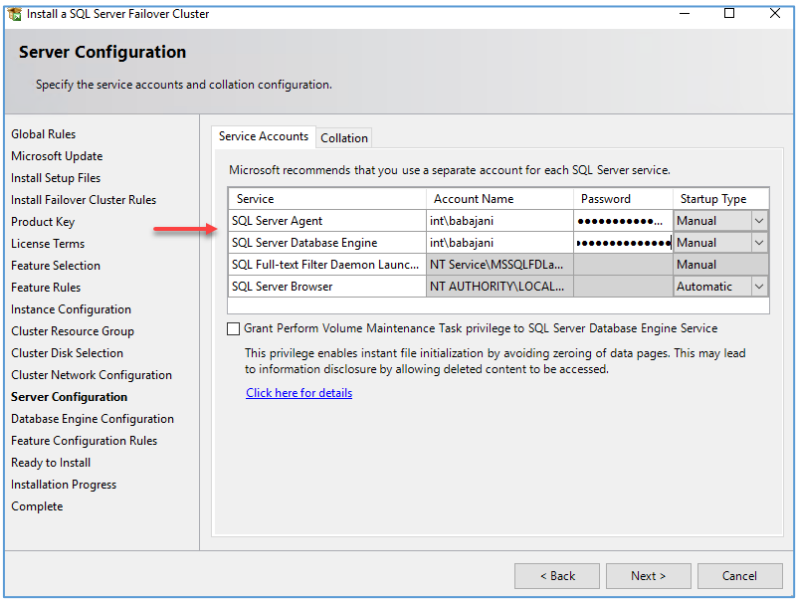
در شکل ۱۰-۵۸، باید شبکه‌ی IPv4 خود را انتخاب کنید و یک آدرس IP جدید برای SQL وارد کنید، توجه داشته باشید این IP با IP که در قسمت Clustring وارد کردیم متفاوت خواهد بود.



شکل ۱۰- ۵۸ تنظیمات سرور Failover-2

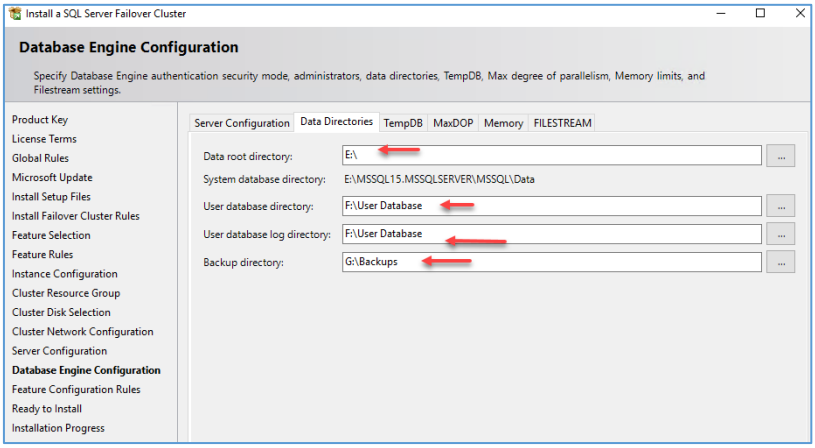
www.takbook.com

در شکل ۱۰-۵۹، باید نام کاربری که قرار است دسترسی کامل برای اجرای سرویس‌ها را داشته باشد وارد کنید و بر روی Next کلیک کنید.



شکل ۱۰- ۵۹ تنظیمات سرور Failover-2

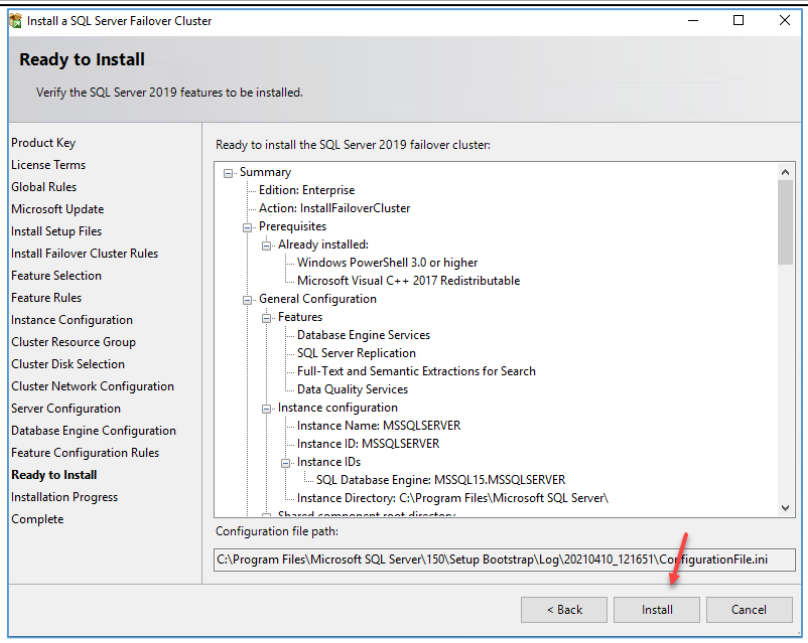
در شکل ۱۰-۶۰، و در تب Server Configuration بر روی Current User کلیک کنید و بعد در تب Data Directories باید محل ذخیره شدن دیتابیس‌ها و اطلاعات کاربران و فایل‌های پشتیبان را مشخص کنید، سعی کنید هر قسمت را در یکی از هاردهای Cluster که ایجاد کردیم وارد کنید و بر روی Next کلیک کنید.



شکل ۱۰- ۶۰ تنظیمات سرور Failover-2

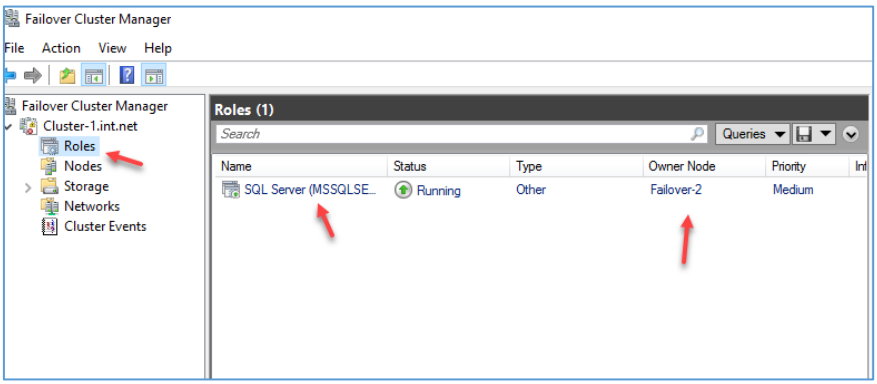
در شکل ۱۰-۶۱، بر روی Install کلیک کنید تا کار نصب آغاز شود.

www.takbook.com



شکل ۱۰- ۶۱ تنظیمات سرور Failover-2

بعد از نصب سرویس Clustring برای SQL سرور، اگر وارد سرویس Failover Cluster Manager به‌مانند شکل ۱۰-۶۲، شوید از سمت چپ بر روی Roles کلیک کنید، همان‌طور که مشاهده می‌کنید SQL Server با Instance مورد نظر توسط سرور Failover-2 ایجاد شده است.

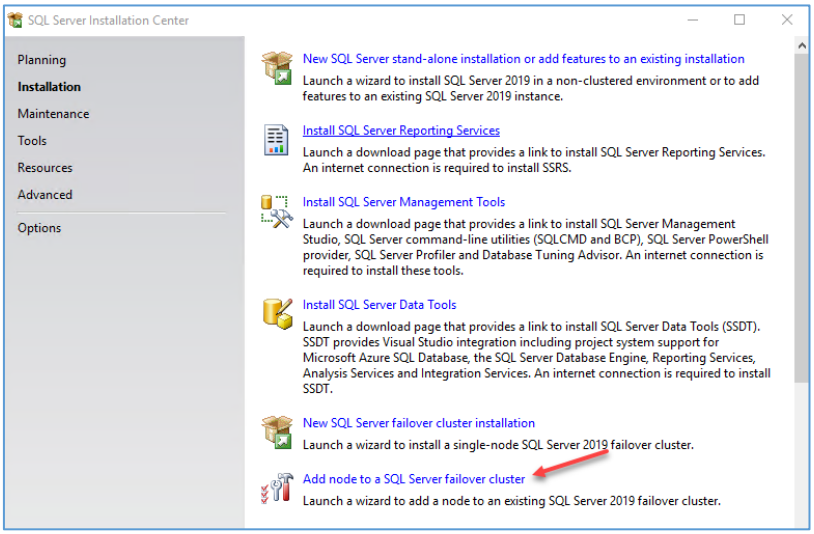


شکل ۱۰- ۶۲ تنظیمات سرور Failover-2

بعد از اینکه سرویس SQL را برای سرور Failover-2 راه‌اندازی کردیم باید حتماً در سرور Failover-1 هم این سرویس را فعال کنیم تا عملیات Clustring به‌درستی انجام شود، برای این کار باید دوباره نرم‌افزار

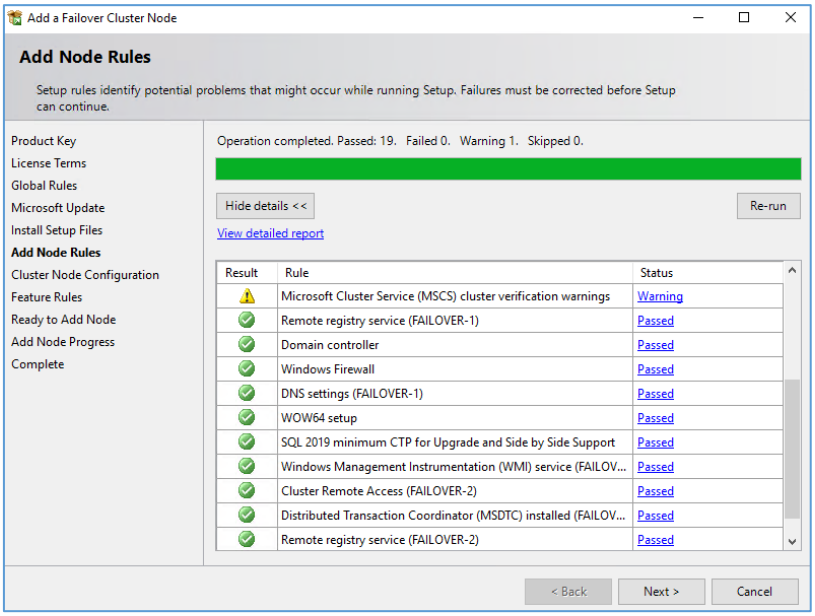
www.takbook.com

نصب SQL را اجرا کنید و به‌مانند شکل ۱۰-۶۳، بر روی Add node to a SQL Server Failover Clustring کلیک کنید.



شکل ۱۰- ۶۳ تنظیمات سرور Failover-2

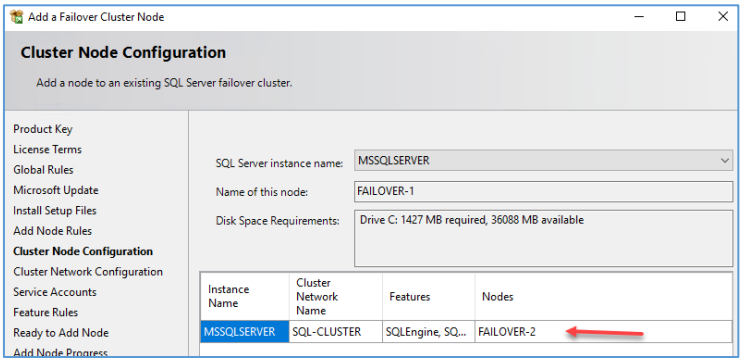
در شکل ۱۰-۶۴، بررسی‌های مربوط به Clustring انجام شده و در صورت نبود خطا بر روی Next کلیک کنید.



شکل ۱۰- ۶۴ تنظیمات سرور Failover-2

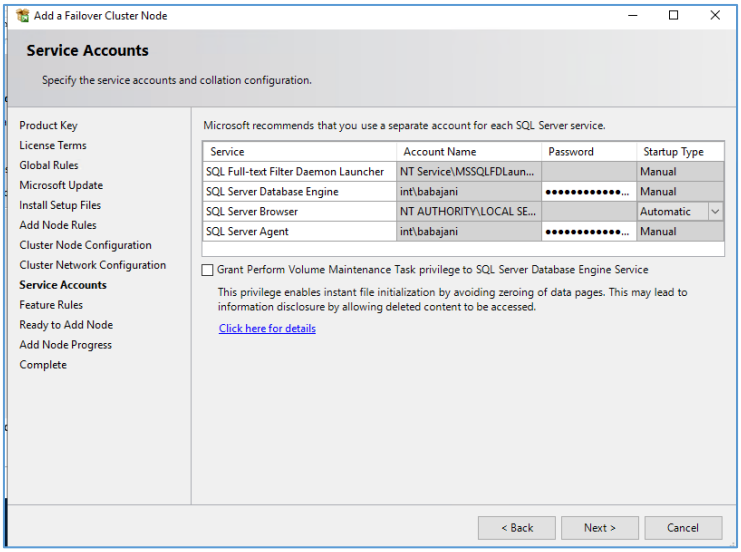
www.takbook.com

همان‌طور که در شکل ۱۰-۶۵، مشاهده می‌کنید کلاستر مورد نظر که با نام شبکه‌ی SQL-Cluster ایجاد کرده بودیم به‌صورت اتوماتیک پیدا شده که نشان می‌دهد این نام را از سرور Failover-2 گرفته است، برای ادامه کار بر روی Next کلیک کنید.



شکل ۱۰- ۶۵ تنظیمات سرور Failover-2

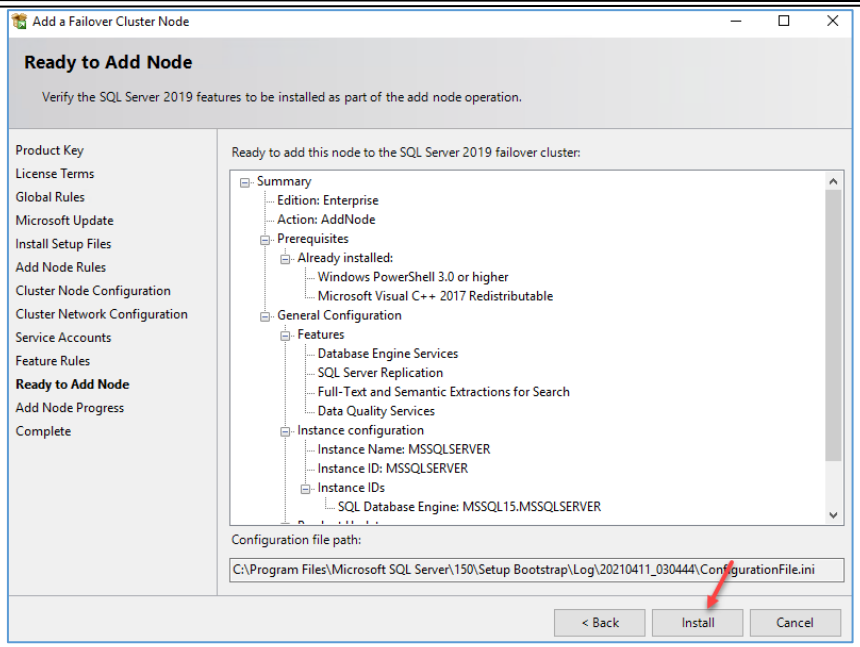
در شکل ۱۰-۶۶، باید نام کاربری که قرار است سرویس‌های مورد نظر را اجرا کنید وارد کنید، سعی کنید همان کاربری که در Failover-2 وارد کردید در این قسمت هم وارد کنید.



شکل ۱۰- ۶۶ تنظیمات سرور Failover-2

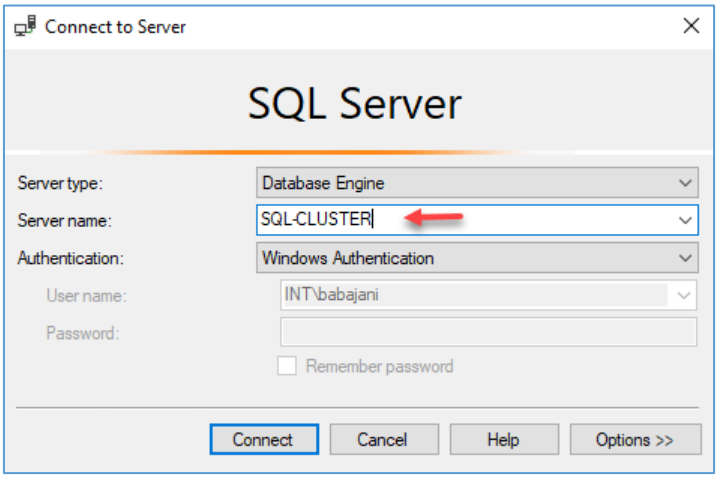
در شکل ۱۰-۶۷، بر روی Install کلیک کنید تا کار نصب آغاز شود.

www.takbook.com



شکل ۱۰- ۶۷ تنظیمات سرور Failover-2

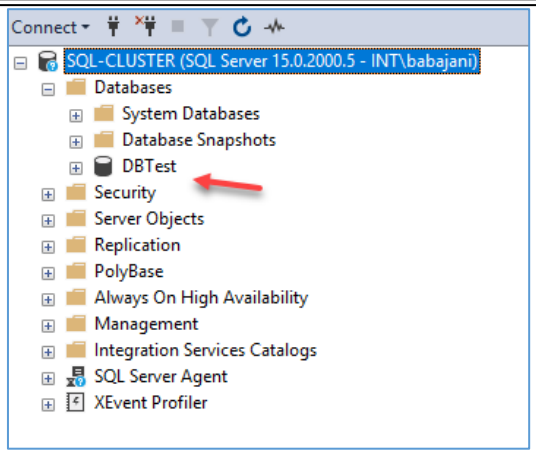
خوب برای تست عملکرد Clustring به‌مانند شکل ۱۰-٦٨، نرم‌افزار SQL Server Management Studio را اجرا کنید و در قسمت Server name باید همان نام شبکه که در مراحل راه‌اندازی SQL Clustring وارد کردید در این قسمت هم وارد کنید.



شکل ۱۰- ۶۸ تنظیمات سرور Failover-2

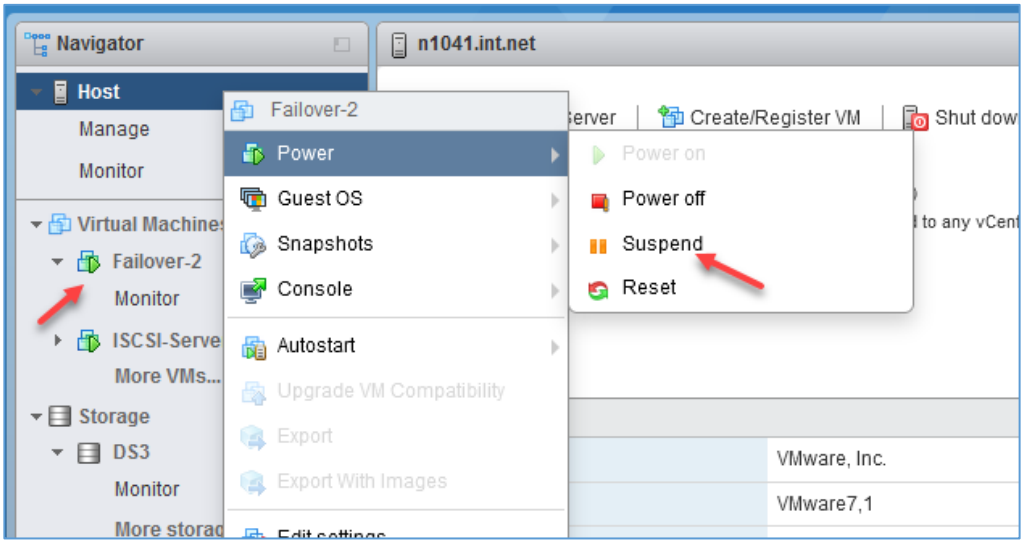
در شکل ۱۰-٦٩، به‌عنوان تست یک دیتابیس در سرور ایجاد کردیم و می‌خواهیم ببینیم زمانی که یکی از این سرورهای Failover را از دست دهیم چه اتفاقی رخ می‌دهد.

www.takbook.com



شکل ۱۰- ۶۹ تنظیمات سرور Failover-2

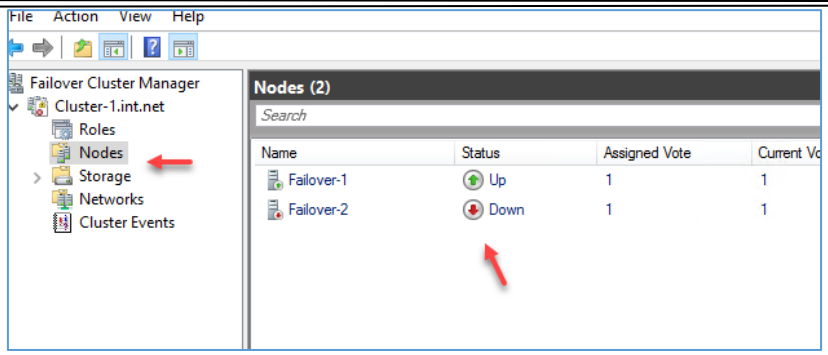
در شکل ۱۰-۷۰، سرور Failover-2 را که سرور اصلی در کلاسترینگ بوده را خاموش و یا Suspend می‌کنیم.



شکل ۱۰- ۷۰ تنظیمات سرور Failover-2

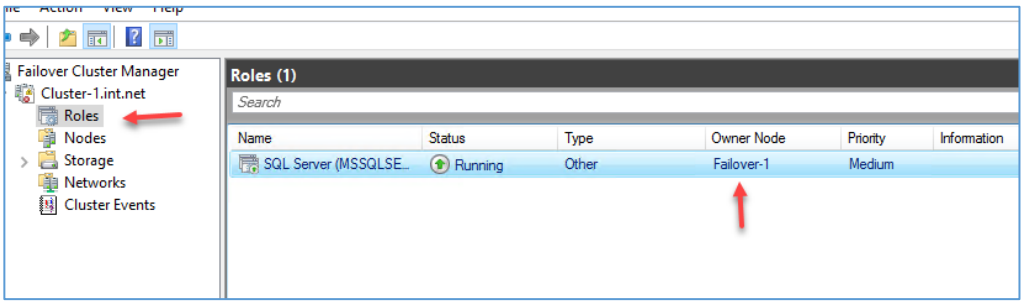
اگر به‌مانند شکل ۱۰-۷۱، وارد سرویس Clustring شوید و در قسمت Node مشاهده خواهید کرد سرور Failover-2 ازکارافتاده.

www.takbook.com



شکل ۱۰- ۷۱ تنظیمات سرور Failover-2

در شکل ۱۰-۷۲، وارد قسمت Roles شوید و همان‌طور که مشاهده می‌کنید در ستون Owner node سرور تغییر کرده و Failover-1 فعال است.



شکل ۱۰- ۷۲ تنظیمات سرور Failover-2

خوب در این فصل توانستیم با کمک چهار سرور سرویس Failover Clustring را راه‌اندازی کنیم و توانایی آن را مشاهده کنیم، این نوع سرویس‌ها در سازمان‌هایی مانند بانک که قطع شدن یکلحظه از سیستم می‌تواند خسارت جبران‌ناپذیری وارد کند خیلی حیاتی و مهم است، پس شما به‌عنوان یک DBA باید نحوه‌ی راه‌اندازی این سرویس را کاملاً مسلط باشید.

www.takbook.com

فصل یازدهم

System Center 2022

System Center 2022 یک مجموعه نرم‌افزاری مدیریت سیستم از شرکت مایکروسافت است که برای مدیریت سرورها و زیرساخت‌های IT در محیط‌های سازمانی و ترکیبی (on-premises و cloud) طراحی شده است. این نسخه جدید، قابلیت‌ها و بهبودهای بسیاری را نسبت به نسخه‌های قبلی ارائه داده است که به سازمان‌ها کمک می‌کند تا بهره‌وری خود را افزایش دهند، امنیت و دسترس‌پذیری سیستم‌ها را بهبود دهند و فرآیندهای مدیریت را ساده‌تر کنند.

در ادامه به بررسی ویژگی‌ها و قابلیت‌های جدید System Center 2022 می‌پردازیم:

۱. پشتیبانی از ویندوز سرور 2022 و پلتفرم‌های ترکیبی

System Center 2022 از Windows Server 2022 به‌طور کامل پشتیبانی می‌کند. این امکان به سازمان‌ها اجازه می‌دهد تا از قابلیت‌های جدید و بهینه‌سازی‌های امنیتی ویندوز سرور بهره‌مند شوند. همچنین System Center 2022 پشتیبانی گسترده‌ای از محیط‌های ترکیبی، شامل ادغام با Microsoft Azure، دارد و می‌تواند به مدیریت سرویس‌های ابری و منابع در محل کمک کند.

۲. بهبود در Operations Manager (SCOM)

System Center Operations Manager یا SCOM در نسخه 2022 با بهبودهایی مواجه شده است که عملکرد، مقیاس‌پذیری و قابلیت‌های نظارتی را ارتقا داده است. این بهبودها شامل موارد زیر است:

بهبود در مدیریت لاگ‌ها و خطاها: با بهینه‌سازی‌هایی که در SCOM انجام شده، شناسایی و مدیریت خطاها و هشدارها سریع‌تر و دقیق‌تر شده است.

پشتیبانی از Discovery خودکار: SCOM 2022 اکنون قابلیت شناسایی خودکار اجزای جدید اضافه شده به شبکه را دارد که مدیریت سیستم‌ها را ساده‌تر می‌کند.

نظارت و یکپارچگی با محیط‌های ترکیبی: امکان نظارت بر منابع Azure و دیگر سرویس‌های ابری از طریق SCOM فراهم شده است.

۳. Virtual Machine Manager (SCVMM) و بهینه‌سازی برای مجازی‌سازی

www.takbook.com

System Center Virtual Machine Manager 2022، یا به اختصار SCVMM، برای مدیریت ماشین‌های مجازی و زیرساخت‌های مجازی بهبود یافته است. برخی از ویژگی‌های جدید آن شامل موارد زیر می‌شود:

- پشتیبانی از VMware vSphere 7.0: امکان مدیریت و ادغام با نسخه‌های جدید VMware فراهم شده است.
- قابلیت‌های جدید در بهینه‌سازی منابع و مدیریت بار: SCVMM 2022 با بهینه‌سازی فرآیند مدیریت منابع، به مدیران کمک می‌کند تا از زیرساخت‌های مجازی خود بهره‌وری بیشتری داشته باشند.
- پشتیبانی از شبکه‌های مجازی: این نسخه امکان پیکربندی و مدیریت شبکه‌های مجازی پیشرفته را بهبود داده است.

٤. Service Manager (SCSM) و بهبود در مدیریت خدمات

System Center Service Manager یا SCSM ابزار مدیریت خدمات IT است و در نسخه 2022 بهبودهایی در زمینه تجربه کاربری، عملکرد و یکپارچگی با دیگر اجزای System Center داشته است. این بهبودها شامل:

- بهبود فرآیندهای اتوماتیک‌سازی خدمات: فرآیندهای درخواست خدمات و مدیریت تغییرات در این نسخه سریع‌تر و کارآمدتر شده‌اند.
- تجربه کاربری بهتر: رابط کاربری و کارکردهای اصلی بهینه شده‌اند تا کاربران راحت‌تر بتوانند درخواست‌های خدمات را ثبت و پیگیری کنند.

٥. Data Protection Manager (DPM) و بهبود در پشتیبان‌گیری و بازیابی

Data Protection Manager یا DPM، ابزار پشتیبان‌گیری و بازیابی اطلاعات System Center است که در نسخه ۲۰۲۵ بهبودهای زیر را تجربه کرده است:

- پشتیبان‌گیری بهینه‌تر و سریع‌تر: با بهینه‌سازی‌هایی که انجام شده، فرآیند پشتیبان‌گیری سریع‌تر و کارآمدتر شده است.
- پشتیبانی از پشتیبان‌گیری ترکیبی (on-premises و cloud): امکان پشتیبان‌گیری از منابع به Azure و بازگردانی اطلاعات به‌صورت ترکیبی فراهم شده است.
- پشتیبانی از محیط‌های ترکیبی و ابری: این نسخه قابلیت پشتیبانی از منابع مختلف از جمله SQL Server، Exchange، SharePoint و فایل‌های مختلف را فراهم می‌کند.

٦. Orchestrator و بهبود در اتوماسیون فرآیندهای IT

www.takbook.com

System Center Orchestrator ابزار اتوماسیون فرآیندهای IT است و در نسخه 2022 با بهینه‌سازی‌ها و قابلیت‌های جدیدی همراه شده است:

- پشتیبانی از اسکریپت‌های PowerShell: با ادغام و پشتیبانی از PowerShell، کاربران می‌توانند فرآیندهای پیچیده را به‌راحتی اتوماسیون کنند.
- ادغام با سرویس‌های Azure: امکان استفاده از Orchestrator برای اتوماسیون سرویس‌های Azure نیز فراهم شده است.

۷. پشتیبانی گسترده‌تر و بهبود امنیت

System Center 2022 امکاناتی برای تقویت امنیت سیستم‌های مدیریت‌شده فراهم می‌کند، از جمله:

- پشتیبانی از استانداردهای امنیتی جدید: این نسخه شامل بهبودهایی در رمزنگاری و تایید هویت برای اطمینان از امنیت بالاتر است.
- ابزارهای گزارش‌دهی امنیتی: ابزارهایی برای گزارش و مانیتورینگ امنیتی برای محافظت از زیرساخت‌ها در برابر تهدیدات بهینه‌سازی شده‌اند.

۸. قابلیت‌های گزارش‌دهی و داشبوردهای مدیریتی

System Center 2022 داشبوردهای مدیریتی پیشرفته‌تری دارد که به مدیران امکان مانیتورینگ دقیق‌تر و سریع‌تر سیستم‌ها و شبکه‌ها را می‌دهد. این داشبوردها شامل گزارش‌های سفارشی و نمودارهای تحلیلی هستند.

۱-۱۱ نصب و راه‌اندازی Microsoft.System.Center. Operations.Manager



Microsoft System Center Operations Manager یا به اختصار SCOM، یک ابزار نظارت و مدیریت زیرساخت‌های شبکه و سیستم‌ها است که به مدیران شبکه و فناوری اطلاعات امکان می‌دهد سرورها،

www.takbook.com

کامپیوترهای کلاینت، برنامه‌ها و سرویس‌های شبکه‌ای خود را به‌صورت متمرکز مانیتور کنند. این ابزار بخشی از مجموعه Microsoft System Center است و برای شناسایی و تحلیل مشکلات شبکه، بهینه‌سازی عملکرد سیستم‌ها و پیشگیری از وقوع مشکلات در زیرساخت‌های IT طراحی شده است.

ویژگی‌های اصلی SCOM:

- مانیتورینگ جامع: امکان نظارت بر سیستم‌عامل‌ها، نرم‌افزارها، سرویس‌ها و سخت‌افزارهای مختلف.
- گزارش‌دهی پیشرفته: ارائه گزارش‌های تحلیلی و داشبوردهای قابل تنظیم برای مشاهده وضعیت سلامت و عملکرد زیرساخت‌ها.
- پشتیبانی از هشدارها (Alerts): شناسایی و اطلاع‌رسانی در مورد رخدادهای غیرعادی و مشکلات احتمالی در لحظه.
- مدیریت مبتنی بر قوانین (Rule-Based Management): اعمال قوانین و تنظیمات خاص برای شناسایی و رفع خودکار مشکلات.
- یکپارچگی با سایر محصولات مایکروسافت: سازگاری با Azure، SQL Server، Active Directory و سایر سرویس‌های مایکروسافت.

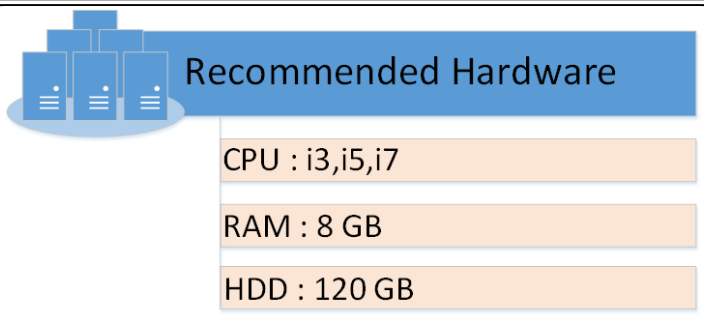
برای راه‌اندازی این نرم‌افزار در شبکه، نیاز به یک سرور با سخت‌افزار خوب داریم که در زیر، پیش‌نیازهای آن را بررسی می‌کنیم.
سخت‌افزاری که برای این سرویس در نظر گرفته شده است باید یک سیستم قدرتمند باشد تا بتواند به درستی نرم‌افزار را اجرا کند؛ پیشنهادی که در بالا ارائه شده است، می‌تواند یک پیشنهاد خوب باشد.
در ادامه با نصب این نرم‌افزار و کار با آن آشنا خواهیم شد.

برای شروع کار می‌توانید مجموعه نرم‌افزارهای System Center 2022 را از لینک زیر دریافت کنید:

https://soft98.ir/internet/network/1040-system-center-dl.html

برای نصب این نرم‌افزار نیاز به پیش‌نیازهای نرم‌افزاری دارید که در شکل ۱۱-۱، مشخص شده است.

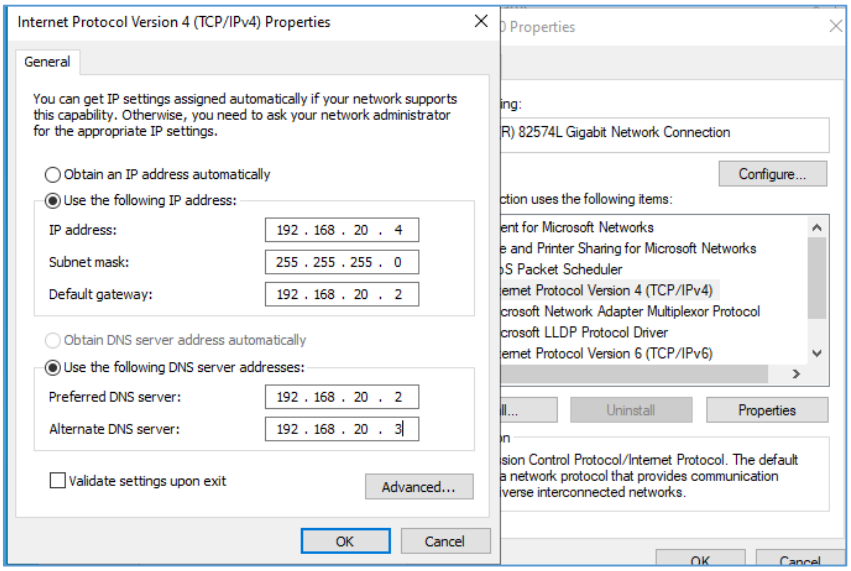
www.takbook.com



شکل ۱۱- ۱ سخت افزار مورد نیاز

برای شروع کار یک ویندوز سرور ۲۰۲۲ را با سخت‌افزاری که بیان کردیم آماده می‌کنیم و تنظیمات را به صورت زیر در آن انجام می‌دهیم.

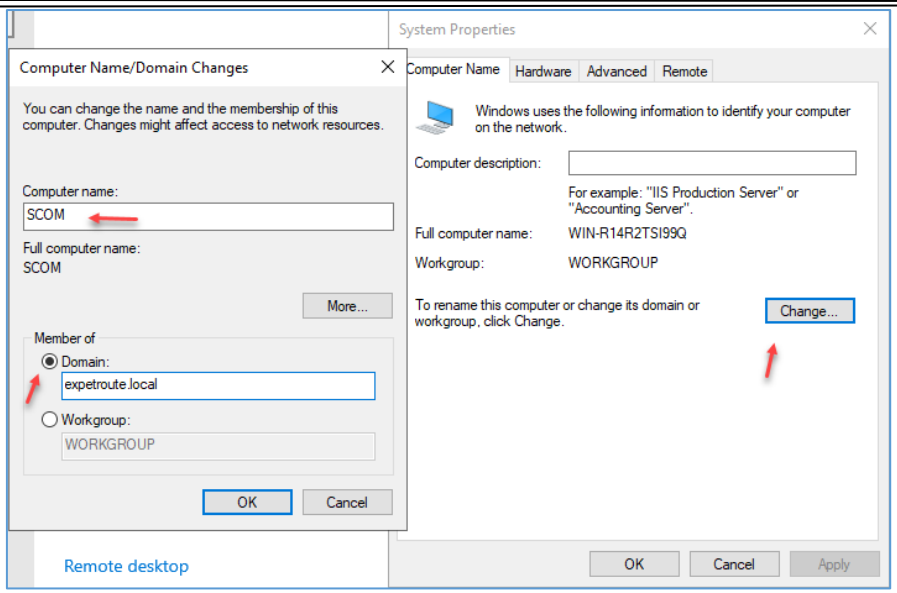
بعد از نصب ویندوز بر روی سیستم جدید باید آدرس IP آن را مشخّص کنید، برای این سرور، به مانند شکل ۱۱-۲، آدرس IP را به صورت 192.168.20.4 در نظر بگیرید و به مانند شکل اطّلاعات را وارد کنید.



شکل ۱۱- ۲ تنظیم آدرس IP

بعد از وارد کردن آدرس، به مانند شکل ۱۱-۳، نام سرور را به SCOM تغییر دهید و آن را عضو دومین Expertroute.local کنید که این عمل را در شکل مشاهده می‌کنید.

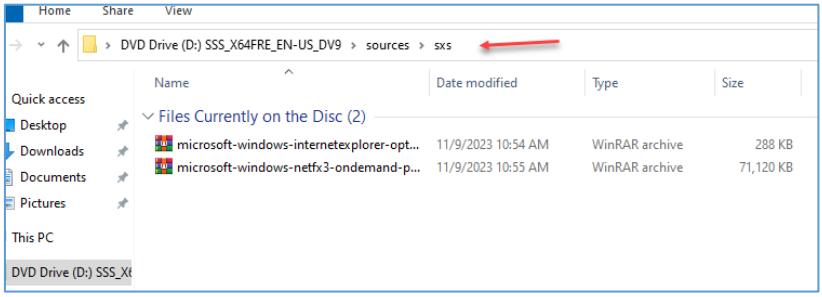
www.takbook.com



شکل ۱۱-۳ عضو کردن در دومین

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.

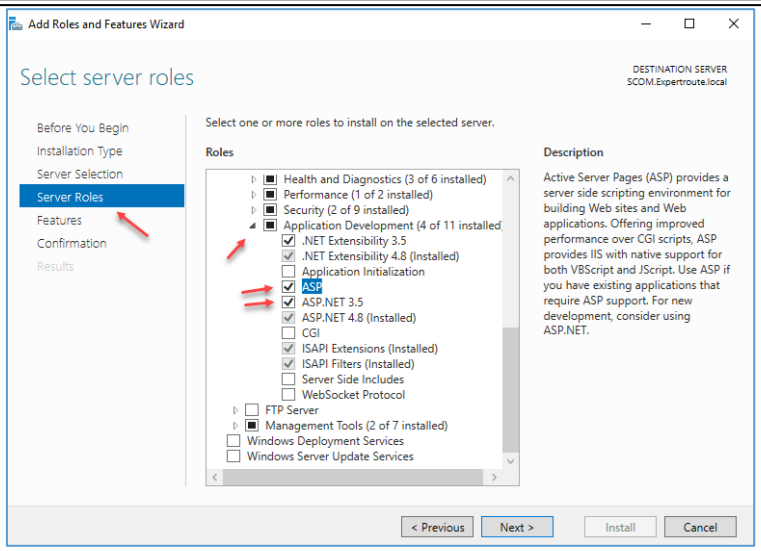
برای شروع کار اول از همه باید NetFarmwork 3.5 نصب کنید، برای نصب Net 3.5 به مانند شکل ۱۱-٤، وارد DVD مربوط به ویندوز سرور ۲۰۲۵ شوید و آدرس زیر را کپی بگیرید:



شکل ۱۱-۴ نصب *Net 3.5*

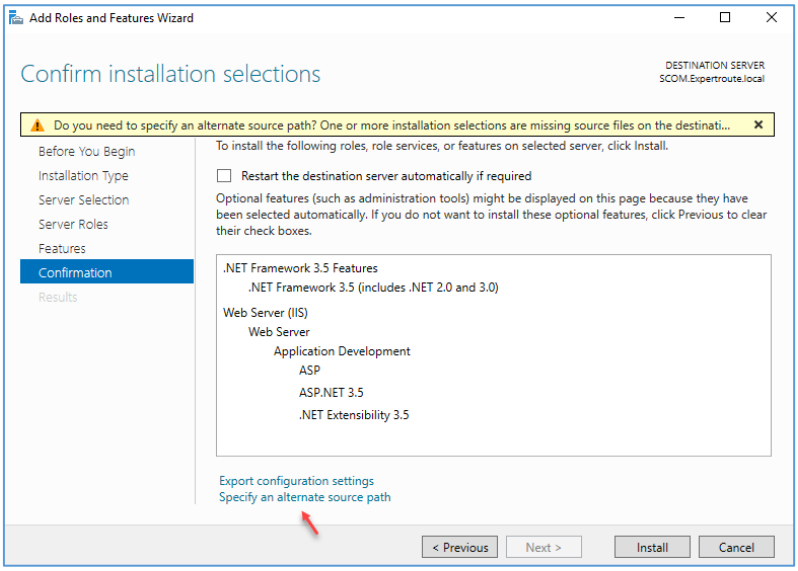
به مانند شکل ۱۱-۵، وارد Server Manager شوید و بر روی Add roles and Features کلیک کنید و در قسمت Server Roles گزینه‌های مورد نظر را تیک بزنید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۱- ۵ نصب Net 3.5

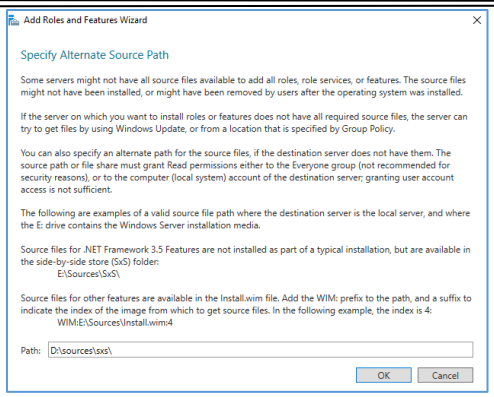
به مانند شکل ۱۱-۶، در قسمت Confirmation بر روی Specify an alternate source path کلیک کنید.



شکل ۱۱- ۶ نصب Net 3.5

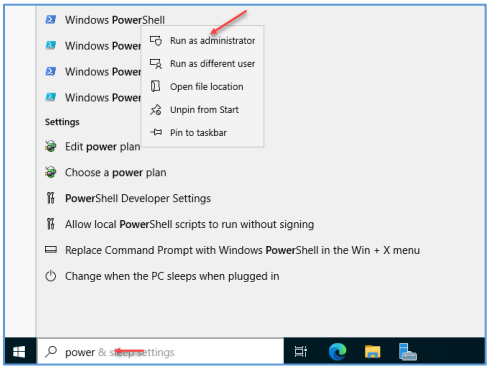
در شکل ۱۱-۷، آدرس مورد نظر را کپی کنید و بر روی ok کلیک کنید و در آخر بر روی Next کلیک کنید تا کار نصب آغاز شود.

www.takbook.com



شکل ۱۱- ۷ نصب Net 3.5

بعد از نصب NetFramwork باید پیش‌نیازهای دیگر را نصب کنیم، برای این کار به مانند شکل ۱۱-۸، عمل کنید و PowerShell را اجرا کنید:



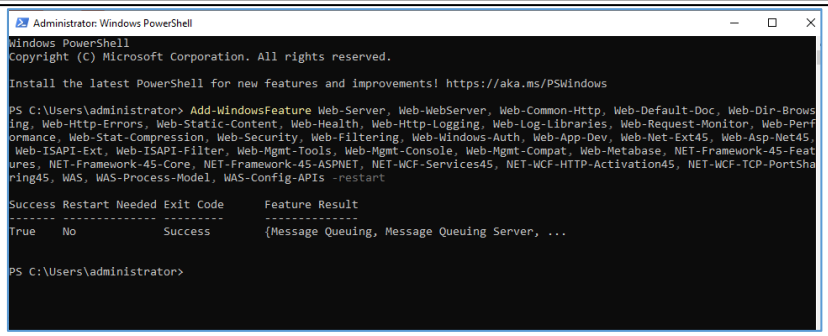
شکل ۱۱- ۸ نصب پیش نیاز ها

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 ۱۱-۹، مشاهده می‌کنید، دستورات به خوبی اجرا شده و پیش‌نیازها نصب شده است، بعد از این کار، سرور را Restart کنید.

www.takbook.com



شکل ۱۱- ۹ نصب پیش نیاز ها

بعد از انجام مراحل بالا، نیاز به نرم‌افزار SQL دارید که در این کتاب از SQL Server 2022 استفاده کردیم که آخرین ورژن این نرم‌افزار محبوب است.

۱۱-۲ نیازمندی‌های SQL Server 2025

برای اینکه سرور SQL خود را راه‌اندازی کنیم، نیاز داریم بدانیم که این سرور چقدر از منابع سخت‌افزاری ما را قرار است مصرف کند، برای همین به جدول ۱۱-۱، توجه کنید.

جدول ۱۱- ۱ نیازمندی سخت‌افزاری

سخت‌افزار	نیازمندی
هارد دیسک	نرم‌افزار SQL برای نصب اولیه نیازمند ٦ گیگابایت فضا در هارد دیسک است، اما برای یک محیط عملیاتی باید مشخص شود آن سازمان نیازمند چقدر از فضای هارد دیسک است؛ مثلاً برای محیطی که دارای ۱۰۰ کارمند است باید حداقل ۲۰۰ گیگ فضا برای آن در نظر گرفت، البته همه‌ی اینها مربوط به کاری است که انجام می‌دهید، توجه داشته باشید حتماً از RAIDبندی در سرور خود برای هارد دیسک استفاده کنید تا در صورت خرابی هاردها اطلاعات شما از دست نرود.
مانیتور	سرور SQL برای اجرا نیازمند رزولیشن Super-VGA (800x600) است.
اینترنت	برای آپدیت نرم‌افزار SQL و استفاده از بخش‌های دیگر نیازمند اینترنت هستیم، البته یک پیشنهاد است و حتماً نیازی نیست که اینترنت داشته باشید.
رم	حداقل نیازمندی یک گیگابایت است، برای عملکرد بهتر باید حداقل ٤ گیگابایت رم برای این سرور در نظر بگیرید، البته در محیط عملیاتی واقعی امروزه، حداقل ۱۰ گیگابایت یک انتخاب ایده‌ال است.

www.takbook.com

سرعت پردازنده	حداقل پردازنده X64 با سرعت 1.4 GHz است، اما برای عملکرد بهتر باید از پردازنده ۲ گیگاهرتز به بالا استفاده شود.
نوع پردازنده	پردازنده‌های امروزی از نوع Intel و AMD به خوبی پاسخگوی نیاز این نرم‌افزار هستند.

جدول ۱۱-۲ نشان می‌دهد که کدام نسخه های SQL Server 2025 با کدام نسخه‌های Windows سازگار است:

جدول ۱۱- ۲ سیستم‌عامل

پشتیبانی سیستم‌عامل					
نسخه‌های مختلف SQL >>	Enterprise	Developer	Standard	Web	Express
Windows Server 2025 Datacenter	Yes	Yes	Yes	Yes	Yes
Windows Server 2025 Standard	Yes	Yes	Yes	Yes	Yes
Windows Server 2025 Essentials	Yes	Yes	Yes	Yes	Yes
Windows Server 2016 Datacenter	Yes	Yes	Yes	Yes	Yes
Windows Server 2016 Standard	Yes	Yes	Yes	Yes	Yes
Windows Server 2016 Essentials	Yes	Yes	Yes	Yes	Yes
Windows 10 IoT Enterprise	No	Yes	Yes	No	Yes
Windows 10 Enterprise	No	Yes	Yes	No	Yes
Windows 10 Professional	No	Yes	Yes	No	Yes
Windows 10 Home					

نکته:

نصب SQL Server فقط در پردازنده‌های x64 پشتیبانی می‌شود و در پردازنده‌های x86 پشتیبانی نمی‌شود که باید به این نکته توجه کنید.

از نیازمندی‌های دیگر SQL Server می‌توان به NET Framework 3.5 اشاره کرد که باید نسخه‌ی مورد نظر آن را که در خود ویندوز ارائه می‌شود نصب کنید، البته این نرم‌افزار به‌صورت پیش‌فرض بر روی سرور نصب خواهد شد.

توجه داشته باشید در هنگام نصب SQL Server اجزای زیر بر روی سرور نصب خواهد شد:

- SQL Server Native Client
- SQL Server Setup support files

اگر بخواهید SQL را به همراه اجزای کامل آن بر روی سرور نصب کنید، هرکدام از اجزا طبق جدول ۱۱-۳ نیازمند فضای موردنیاز هستند.

توجه داشته باشید که این مورد را در موقع نصب SQL انتخاب خواهیم کرد.

www.takbook.com

جدول ۱۱-۳ اجزای SQL

ویژگی مورد نظر	مقدار فضای موردنیاز
Database Engine and data files, Replication, Full-Text Search, and Data Quality Services	1480 MB
Database Engine (as above) with R Services (In-Database)	2744 MB
Database Engine (as above) with PolyBase Query Service for External Data	4194 MB
Analysis Services and data files	698 MB
Reporting Services	967 MB
Microsoft R Server (Standalone)	280 MB
Reporting Services - SharePoint	1203 MB
Reporting Services Add-in for SharePoint Products	325 MB
Data Quality Client	121 MB
Client Tools Connectivity	328 MB
Integration Services	306 MB
Client Components (other than SQL Server Books Online components and Integration Services tools)	445 MB
Master Data Services	280 MB
SQL Server Books Online Components to view and manage help content*	27 MB
All Features	8030 MB

۳-۱۱ نصب و راه‌اندازی SQL Server 2022 در ویندوز

قبل از نصب SQL Server 2022 بهتر است یک موضوع بسیار مهم را بررسی کنیم، همان‌طور که می‌دانید دو نوع سیستم داریم:

- فیزیکی
- مجازی

به طور معمول یک سیستم فیزیکی با رم و هارد و فضای ذخیره‌سازی مناسب را برای نصب SQL Server در نظر می‌گیرید و فکر می‌کنید بهترین عملکرد را ارائه دادید، اما اگر در این بین، اطلاعات شما از دست برود و هارددیسک شما خراب شود، آن‌وقت چه کاری باید انجام دهید، آیا به نظر شما استفاده از سیستم فیزیکی برای استفاده‌ی مستقیم از SQL Server کار درستی خواهد بود؟

هرچند می‌توانید با روش‌هایی مانند Raidبندی و روش‌های دیگر جلوی ازبین‌رفتن اطلاعات را بگیرید، اما بهترین کار این است که از مجازی‌سازی استفاده کنیم و ازروی ماشینی که ایجاد می‌کنیم، پشتیبان تهیه

www.takbook.com

کنیم تا در موقع ازدست‌رفتن سرور در سریع‌ترین زمان ممکن بتوانیم آن را برگردانیم، البته روش‌های پشتیبان‌گیری در SQL یک موضوع مفصل خواهد بود که در فصل مربوط به پشتیبان‌گیری به‌صورت کامل به آن خواهیم پرداخت.

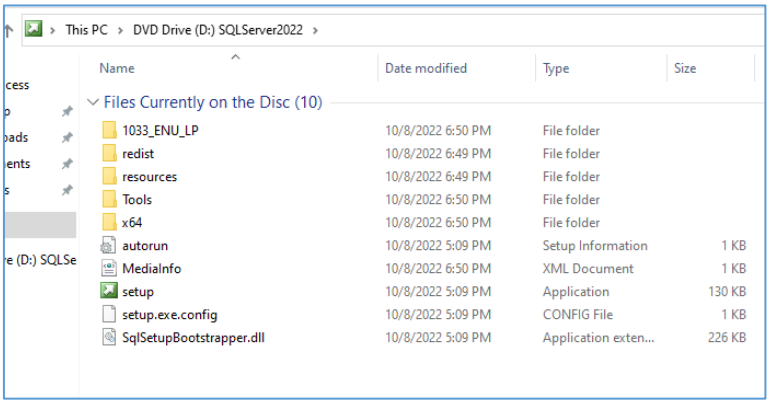
ما برای این کتاب سرور مجازی را انتخاب می‌کنیم، بهترین عملکرد در مجازی‌سازی را شرکت VMware ارائه می‌دهد و شما می‌توانید ماشین مورد نظر خود را توسط نرم‌افزار VMware Workstation و یا با سیستم‌عامل ESXi ایجاد کنید.

برای این کتاب ما از یک سرور ESXi استفاده کردیم که روی آن یک ماشین مجازی ایجاد کردیم و سخت‌افزار مناسب را برای آن در نظر گرفتیم، بعد از این کار بر روی آن ویندوز سرور ۲۰۲۵ نصب کردیم تا همه چیز برای نصب نرم‌افزار SQL آماده باشد.

برای اینکه نرم‌افزار SQL Server 2022 را دانلود کنید می‌توانید به‌صورت مستقیم از سایت مایکروسافت دانلود کنید و یا اینکه آن را از سایت‌های ایرانی مانند Soft98.ir دانلود کنید:

https://www.microsoft.com/en-us/sql-server/sql-server-downloads

بعد از دانلود فایل مورد نظر، به‌مانند شکل ۱۱-۱۰، بر روی فایل Setup.exe دو بار کلیک کنید.

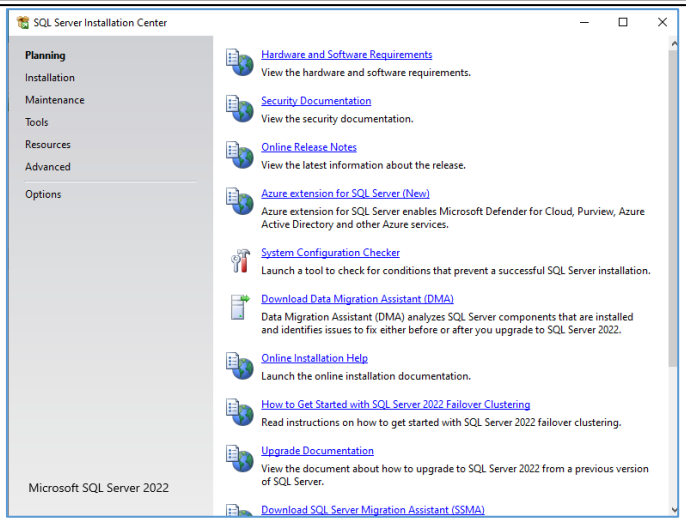


شکل ۱۱- ۱۰ فایل Setup

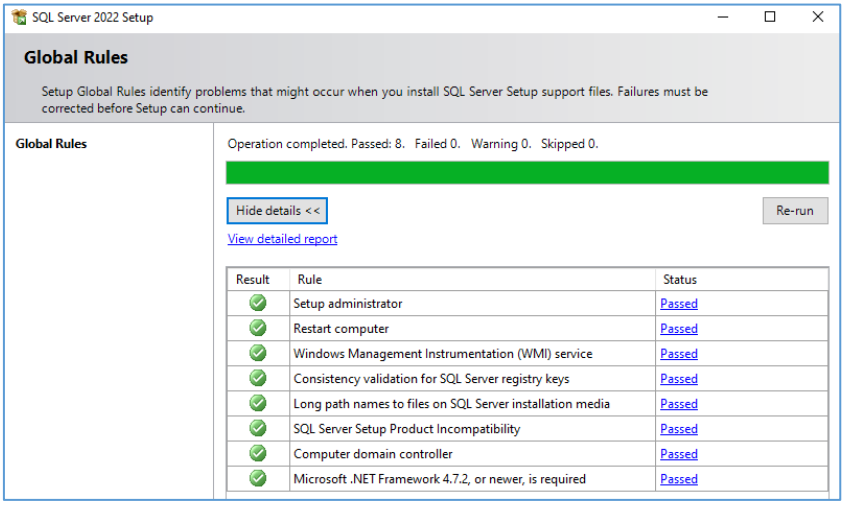
اولین صفحه‌ای که به شما نمایش داده می‌شود، شکل ۱۱-۱۱، است که گزینه‌های مختلفی را به شما ارائه می‌دهد، مثلاً در گزینه‌ی اول اطلاعاتی را در مورد سخت‌افزار و نرم‌افزار موردنیاز برای نصب SQL Server توضیح می‌دهد و همچنین در گزینه‌های دیگر می‌توانید موارد دیگر را هم بررسی کنید.

برای اینکه متوجه شویم که سیستمی که در حال نصب SQL بر روی آن هستید آیا مناسب است یا نه باید در شکل ۱۱-۱۱، بر روی لینک System Configuration Checker کلیک کنید، تا به‌مانند شکل ۱۱-۱۲، همه‌ی گزینه‌ها اوکی باشد.

www.takbook.com



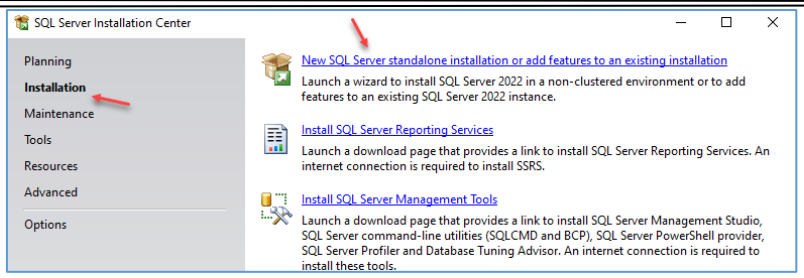
شکل ۱۱- ۱۱ نصب SQL Server 2022



شکل ۱۱- ۱۲ بررسی نصب SQL

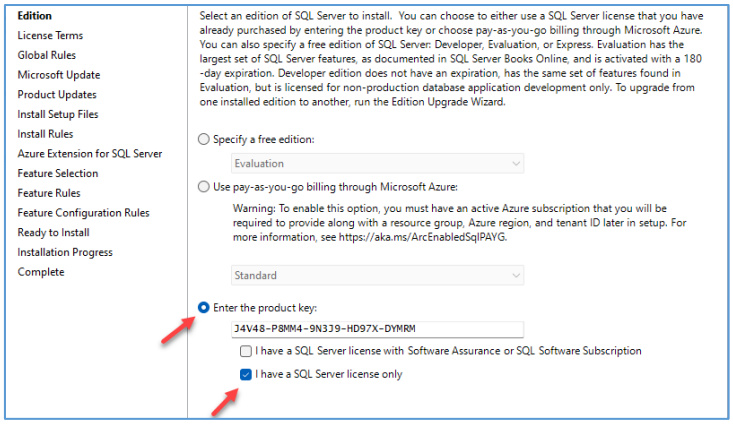
برای اینکه نصب SQL Server را آغاز کنید، باید به‌مانند شکل ۱۱-۱۳، وارد Installation شوید و بر روی New SQL Server stand-alone installation or add fearure to an existing installation کلیک کنید.

www.takbook.com



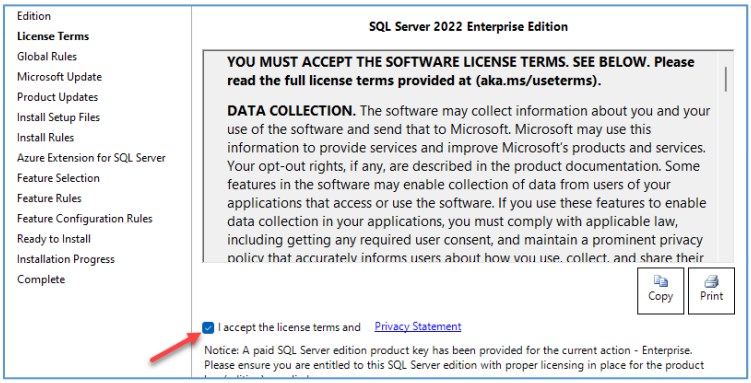
شکل ۱۱-۱۳ نصب SQL

در شکل ۱۱-۱٤، باید سریال نرم‌افزار را وارد و بر روی Next کلیک کنید.



شکل ۱۱-۱٤ وارد کردن سریال نرم‌افزار

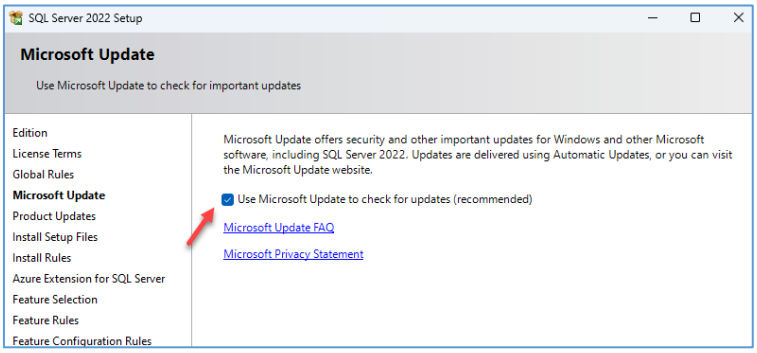
در شکل ۱۱-۱۵، باید توافقنامه‌ی استفاده از این نرم‌افزار را مطالعه و درصورتی‌که آن را قبول دارید، تیک گزینه‌ی I accept the license terms را انتخاب و بر روی Next کلیک کنید.



شکل ۱۱-۱۵ تأیید توافقنامه

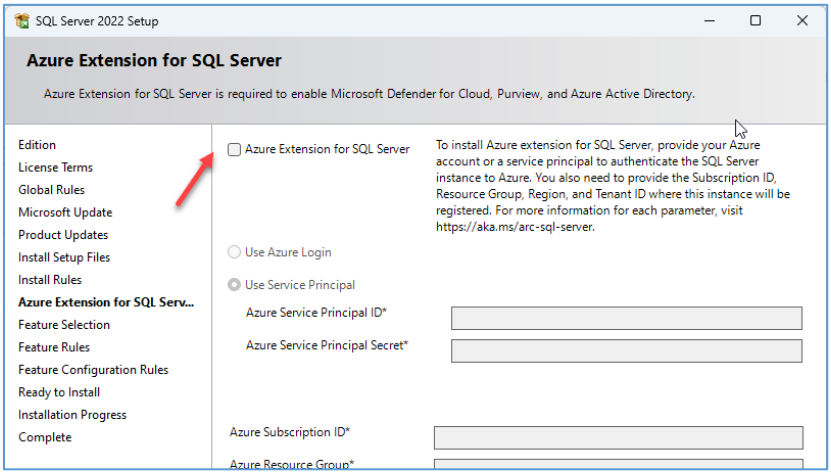
www.takbook.com

به‌مانند شکل ۱۱-۱۶، می‌توانید با انتخاب تیک گزینه‌ی Use Microsoft Updates To ... آخرین آپدیت‌های نرم‌افزار SQL را از سایت مایکروسافت دریافت کنید.



شکل ۱۱-۱۶ دریافت آپدیت

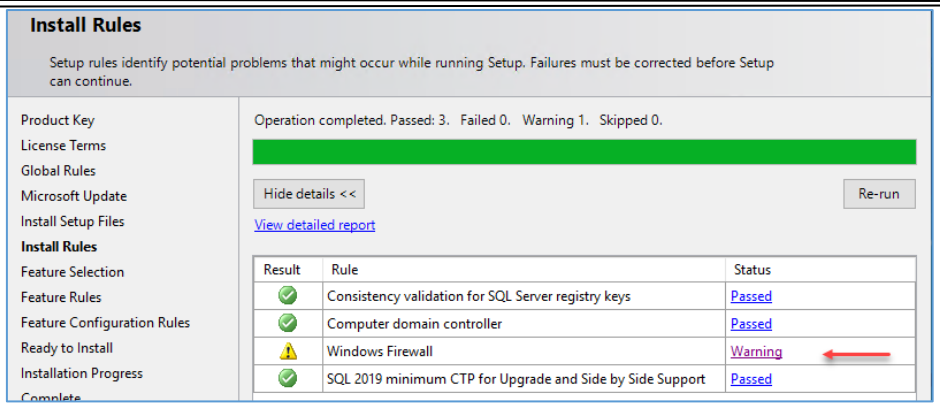
در شکل ۱۱-۱۷ نیازی به ابزار مربوط به Azure نیست، همان‌طور که می‌دانید سرویس Azure مایکروسافت یک سرویس ابری است که تمام ابزارهای مایکروسافت در آن در دسترس است و در این مرحله ما نیازی به این ابزار نداریم و تیک گزینه‌ی مورد نظر را بردارید.



شکل ۱۱-۱۷ Azure

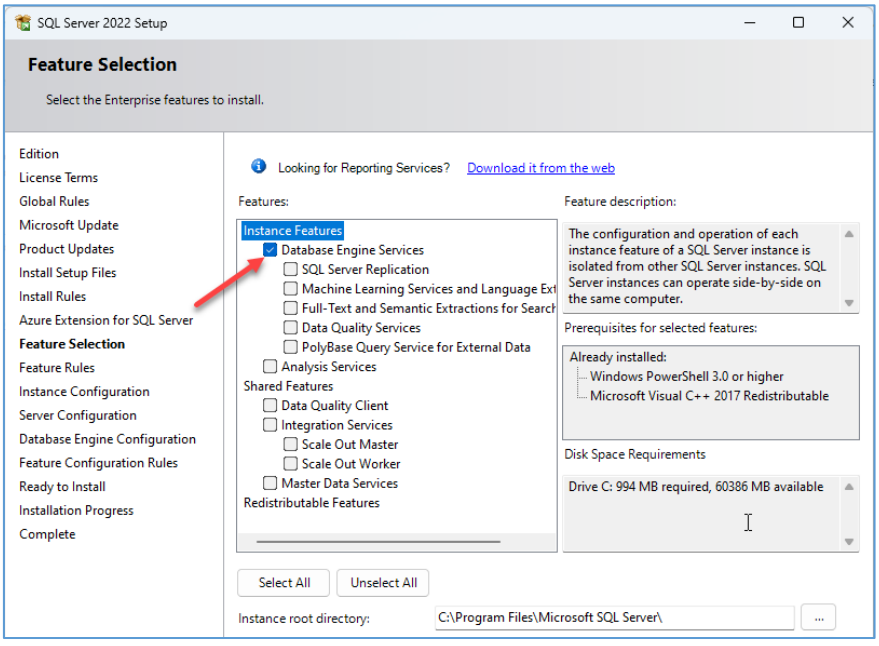
در شکل ۱۱-۱۸، بررسی اولیه انجام می‌شود و در این قسمت همه چیز باید Passed باشد، اگر به شکل ۱۱-۱۸، توجه کنید، متوجه خواهید شد که قسمت Firewall با یک اخطار روبرو شده است و به این موضوع اشاره دارد که برای استفاده از SQL در شبکه باید پورت‌های مورد نظر آن در فایروال باز باشد که ادامه این کار را انجام خواهیم داد.

www.takbook.com



شکل ۱۱- ۱۸ بررسی نیازمندی‌های اولیه

در شکل ۱۱-۱۹، باید تیک گزینه‌ی Database Engine را انتخاب کنید و همچنین می‌توانید مسیر نصب را تغییر دهید، Database Engine هسته‌ی اصلی SQL Server است و تمام اطلاعات مانند دیتابیس‌ها، جداول و... در آن قرار می‌گیرد و برای شروع باید انتخاب و نصب شود.

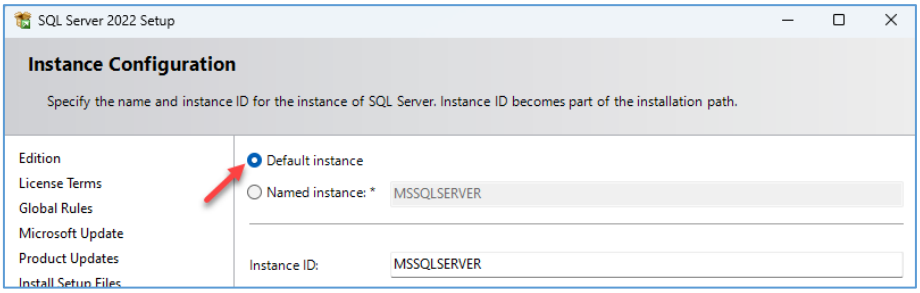


شکل ۱۱- ۱۹ انتخاب Feature

در شکل ۱۱-۲۰، باید Instance را مشخص کنید، Instance را به‌عنوان یک ظرف در نظر بگیرید که داخل آن می‌توانید دیتابیس خود را قرار دهید و نرم‌افزارهای خاص خود را داشته باشید، مثلاً اطلاعاتی که در Instance با نام DB1 قرار دارد با اطلاعاتی که در Instance با نام DB2 قرار دارد متفاوت است، اصولاً

www.takbook.com

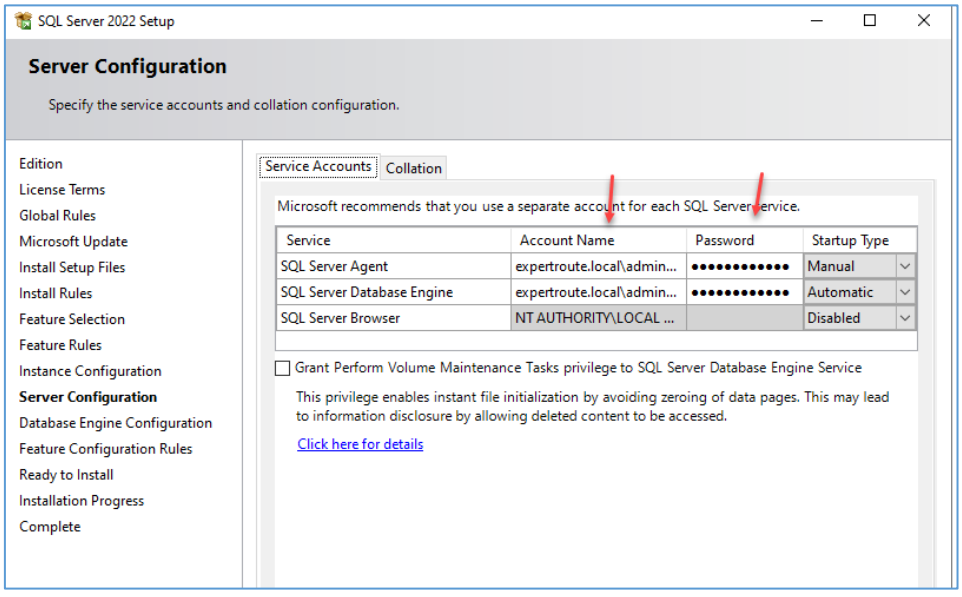
Instance را به‌عنوان یک مزرعه‌ی جدا می‌شناسند که داخل آن می‌توانید دیتابیس‌ها و سرویسهای خود را داشته باشید، در شکل ۱۱-۲۰، Instance با نام پیش‌فرض MSSQLSERVER قرار دارد که سرویس را بر روی آن فعال می‌کنیم، البته شما می‌توانید نام‌های دیگر را هم انتخاب کنید.



شکل ۱۱- ۲۰ بررسی *Instance*

در شکل ۱۱-۲۱، باید یک کاربر را برای اجرای سرویس‌های SQL در نظر بگیرید، توجه داشته باشید که آن کاربر دسترسی لازم در شبکه را داشته باشد، برای همین منظور کاربر administrator که یک کاربر تحت دومین است با دسترسی کامل به شبکه وارد شده است و با همین کاربر هم باید در ادامه وارد SQL شویم.

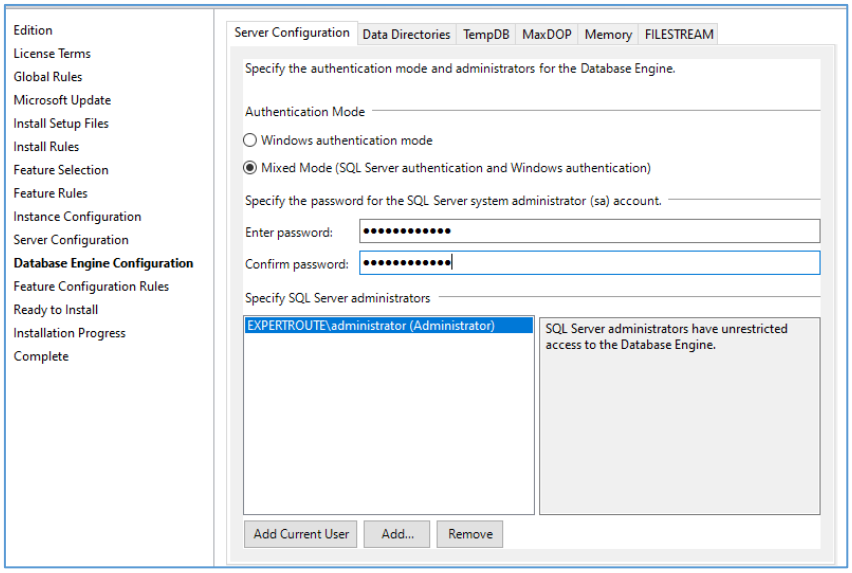
توجه داشته باشید کاربری که در این قسمت وارد می‌کنید، بهتر است کاربر مخصوص به این کار باشد تا دیگر کاری با آن نداشته باشید یعنی اینکه مثلاً رمز آن را تغییر ندهید تا سیستم دچار مشکل شود.



شکل ۱۱- ۲۱ تنظیم سرور

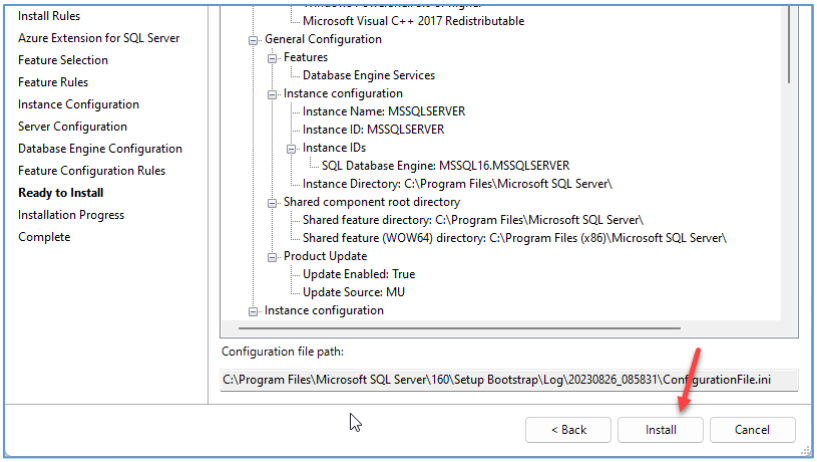
www.takbook.com

در شکل ۱۱-۲۲، باید مشخص کنید که چه کاربرانی دسترسی به Database داشته باشند که با کلیک بر روی Add Current User می‌توانید با کاربری که در حال نصب SQL هستید، آن را به لیست اضافه کنید و یا اینکه هر کاربر دیگری که مورد نظر شماست با کلیک بر روی Add آن را به لیست اضافه کنید، توجه داشته باشید دو حالت احراز هویت وجود دارد که به‌صورت پیش‌فرض Windows aythentication mode انتخاب شده است و اگر بخواهید کاربر sa که کاربر پیش‌فرض در SQL است باید در این قسمت گزینه Mixed Mode را انتخاب و یک رمز عبور برای آن در نظر بگیرید.



شکل ۱۱- ۲۲ تنظیم دسترسی به دیتابیس

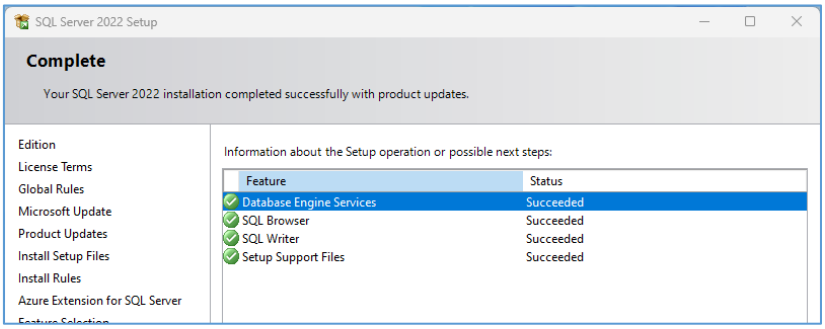
در شکل ۱۱-۲۳، بر روی Install کلیک کنید تا کار نصب آغاز شود.



شکل ۱۱- ۲۳ Install SQL

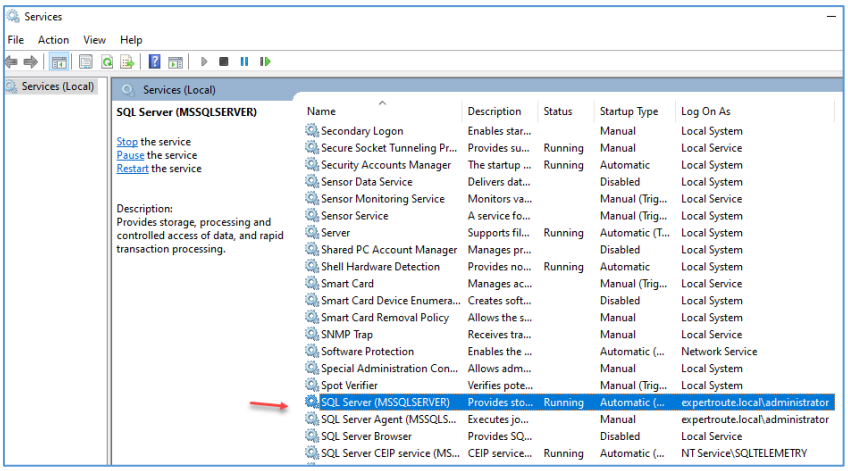
www.takbook.com

همان‌طور که در شکل ۱۱-۲۴، مشاهده می‌کنید نرم‌افزار SQL Server به‌درستی بر روی سرور نصب شده است.



شکل ۱۱-۲۴ *Finish Install*

اگر بعد از نصب به‌مانند شکل ۱۱-۲۵، وارد Services شوید، مشاهده خواهید کرد که سرویس SQL Server به‌درستی در حال اجرا است.



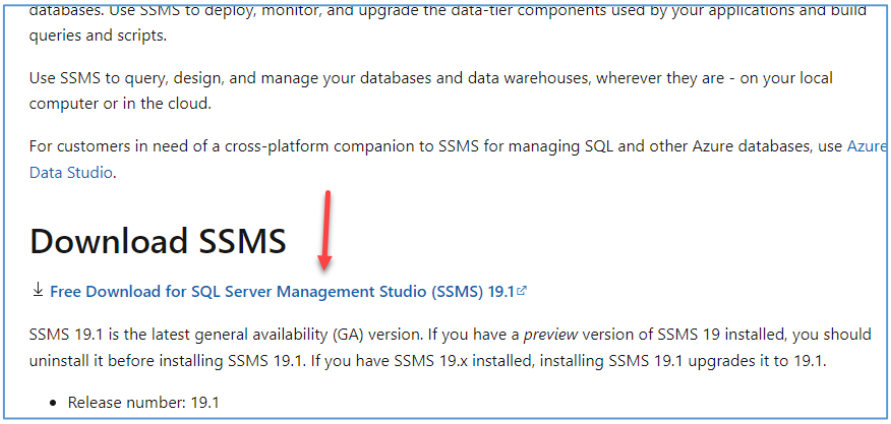
شکل ۱۱-۲۵ سرویس *SQL Server*

بعد از نصب نرم‌افزار SQL Server نیاز به یک نرم‌افزاری داریم تا بتوانیم SQL را مدیریت کنیم، یعنی کاربر جدید تعریف کنیم، دسترسی آن را مشخص کنیم، دیتابیس جدید ایجاد کنیم و موارد دیگر؛ همه‌ی این کارها توسط نرم‌افزار SQL Server Management Tools یا به‌اختصار SSMS انجام خواهد گرفت، در نسخه‌های جدید این نرم‌افزار به‌صورت جداگانه ارائه می‌شود و می‌توانید از طریق لینک زیر آن را دانلود کنید:

https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver15

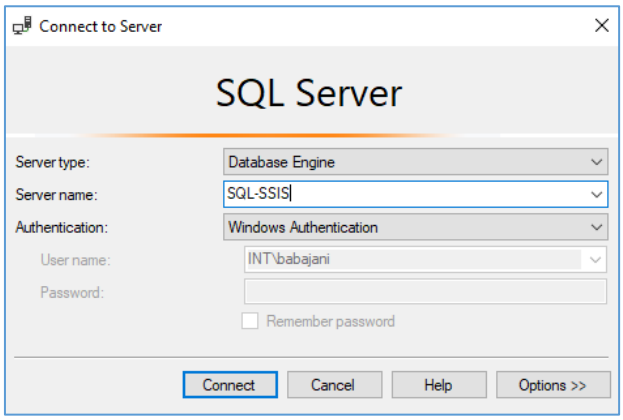
www.takbook.com

بعد از ورود به صفحه شکل ۱۱-۲۶، بر روی لینک دانلود کلیک کنید تا نرم‌افزار مورد نظر دانلود شود و بعد از دانلود آن را بر روی سرور و یا هر سیستمی که می‌خواهید نصب کنید.



شکل ۱۱- ۲۶ دانلود SSMS

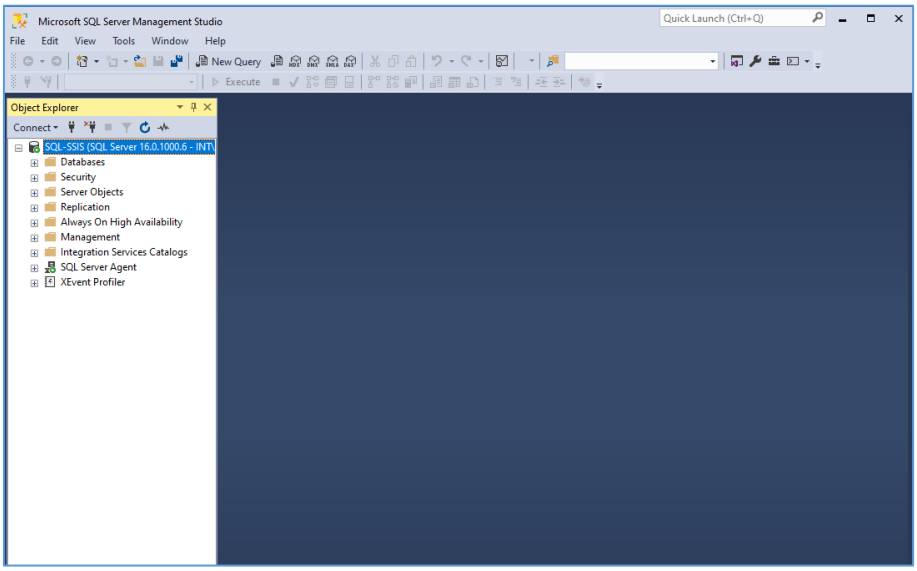
بعد از نصب و از طریق منوی Start نرم‌افزار SSMS را اجرا کنید که به‌مانند شکل ۱۱-۲۷، صفحه مورد نظر برای شما ظاهر خواهد شد. در این صفحه شما باید در قسمت Server Type، گزینه‌ی Database Engine را انتخاب کنید که شامل دیتابیس شما خواهد بود؛ در قسمت Server Name باید نام سرور SQL خود را وارد کنید، توجه داشته باشید اگر داخل سرور هستید می‌توانید از نام localhost نیز استفاده کنید، اما برای دسترسی از بیرون باید از نام سرور استفاده کنید. در قسمت Authentication نیز اگر بر روی Windows Authentication قرار دهید با همان نام کاربری که Login کردید وارد خواهد شد که مسلماً باید دسترسی لازم را داشته باشد و یا اینکه می‌توانید از SQL Server Authentication استفاده کنید.



شکل ۱۱- ۲۷ ورود به SQL Server

www.takbook.com

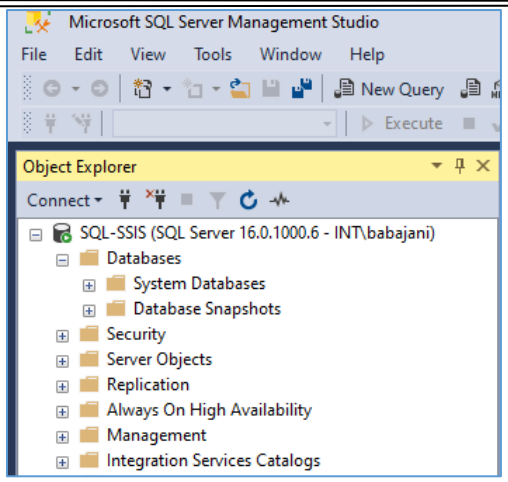
در شکل ۱۱-۲۸، یک نمای کلی از نرم‌افزار SSMS را که به Database Engine متصل شده است را مشاهده می‌کنید، در قسمت Databases می‌توانید دیتابیس‌های خود و دیتابیس‌هایی که توسط نرم‌افزارهای دیگر به‌صورت اتوماتیک ایجاد می‌شود را مشاهده کنید. در قسمت Security باید کاربران خود را معرفی و دسترسی‌های لازم برای آنها را مشخص کنید؛ در قسمت Server Objects یک سری اشیا یا همان Object وجود دارد که برای مانیتور کردن عملکرد سرور خواهد بود. در قسمت Replication نیز یک سری ابزار وجود دارد تا بتوانید دیتابیس‌ها را از یک پایگاه‌داده به یک پایگاه‌داده به‌صورت درست و امن انتقال دهید، PolyBase نیز یک ابزار برای انتقال اطلاعات از یک پایگاه‌داده متفاوت، مانند Oracle به SQL است؛ گزینه‌ی Always On High Availability برای ایجاد یک گروه از سرورها برای پایدار نگه‌داشتن دیتابیس‌ها و سرورها است که یک روش جدید در میان روش‌های دیگر است. در قسمت Managemnt یک سری ابزار وجود دارد، مانند پشتیبان‌گیری از دیتابیس‌ها، LOG گیری و موارد دیگر که در مدیریت SQL بسیار کمک‌کننده خواهد بود؛ قسمت Inetgaration Service Catalog نیز برای یکپارچه‌سازی داده‌ها در سازمان شما است که با یاری خدا همه‌ی این گزینه‌ها را در ادامه توضیح خواهیم داد و در آخر نیز سرویس SQL Agent برای انجام پشتیبان‌گیری و کارهایی دیگر موردنیاز است.



شکل ۱۱- ۲۸ شکل کلی نرم افزار

اولین قسمتی که بررسی می‌کنیم Databases است، به‌مانند شکل ۱۱-۲۹، بعد از بازکردن قسمت Databases، دو گزینه را مشاهده می‌کنید، یکی Systems و دیگری Database Snapshots است؛ در قسمت Systems، چهار دیتابیس را مشاهده می‌کنید که به‌صورت پیش‌فرض ایجاد می‌شوند، در جدول ۱۱-٤، این دیتابیس‌ها را توضیح دادیم.

www.takbook.com



شکل ۱۱- ۲۹ بررسی Database

جدول ۱۱- ۴ دیتابیس‌های سیستم

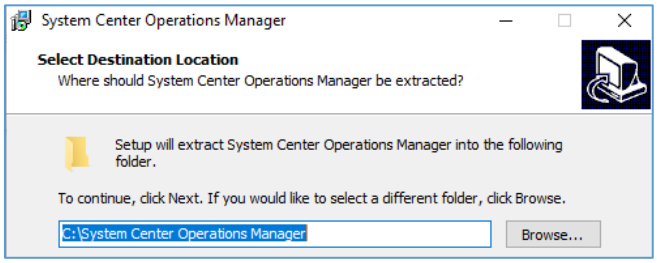
دیتابیس سیستم	توضیحات
master	پایگاه‌داده Master به‌عنوان قلب تپنده SQL است و اگر از دست برود با مشکل مواجه خواهید شد، دیتابیس Master شامل اطلاعاتی حیاتی زیر است: • زمانی که یک کاربر ایجاد می‌کنید، ID آن در این دیتابیس قرار می‌گیرد. • تمام رویدادها یا همان Logها در این دیتابیس قرار می‌گیرد. • نام و اطلاعات مربوط به پایگاه داده‌ها. • خطاهای سیستم و تمام پیام‌های موجود در سرور. • مقداردهی اولیه‌ی SQL Server . • پایگاه داده‌های محلی. • جدول‌های خاص پایگاه داده‌ها.
tempdb	همان‌طور که از اسم آن مشخص است، یک پایگاه‌داده موقت است، زمانی که شما SQL Server ۲۰۲۵ را اجرا می‌کنید، اطلاعات موقت در این پایگاه‌داده قرار می‌گیرد، مثالی که در این رابطه می‌توان زد، مانند RAM سیستم

www.takbook.com

	شما که زمانی نرم‌افزاری را اجرا می‌کنید، اطلاعات به‌صورت موقت در این حافظه قرار می‌گیرد و بعد از بستن نرم‌افزار، اطلاعات نیز از حافظه پاک می‌شوند. زمانی که یک دستور را در SQL اجرا می‌کنید، اطلاعات این دستور به‌صورت موقت در این پایگاه‌داده قرار می‌گیرد و پردازش می‌شود و طول عمر آن به کار کاربر مورد نظر برمی‌گردد.
model	این پایگاه‌داده به‌عنوان یک الگو در نظر گرفته می‌شود، یعنی اینکه یک سری استانداردهایی در آن تعریف شده است که همه‌ی پایگاه داده‌ها از آن استاندارد پیروی می‌کنند. مجموعه‌های از پیش تعیین‌شده در این پایگاه وجود دارد که برای ساخت پایگاه داده‌های دیگر به کار می‌رود، مانند حجم پایگاه داده‌ها، اندازه‌ی جدول‌ها و موارد دیگر.
Resource	یک پایگاه‌داده‌ی فقط خواندنی که اطلاعات System Object در آن نگهداری می‌شود، البته در لیست ظاهری وجود ندارد.
msdb	در این پایگاه‌داده یک سری کارهای از پیش تعیین‌شده قرار دارد این کارها می‌تواند پشتیبان‌گیری و یا بازگردانی اطلاعات باشد که این کار بدون دخالت کسی و به‌صورت خودکار انجام می‌شود.

۱۱-٤ نصب و راه‌اندازی SCOM

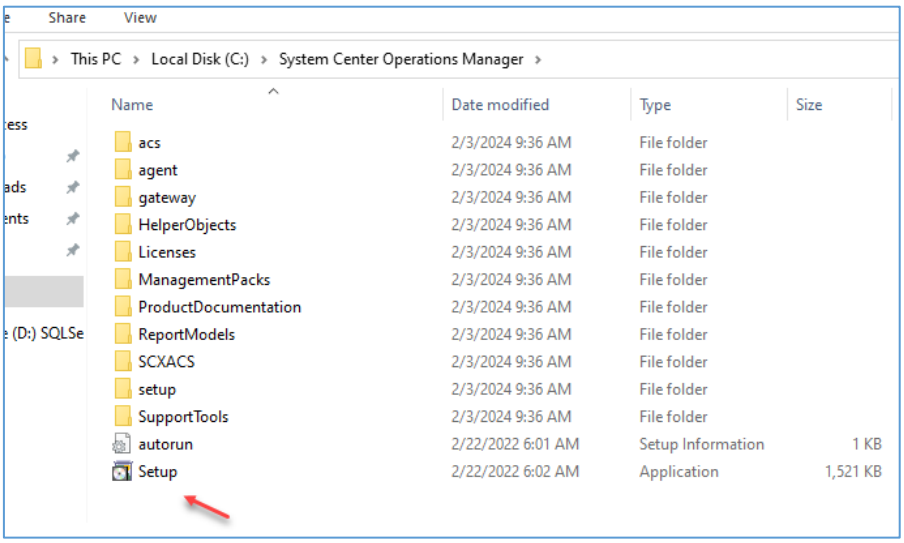
بعد از آماده‌سازی SQL Server حالا باید سرویس SCOM را بر روی سرور نصب کنیم برای انجام این کار بر روی فایل Setup کلیک کنید و برای استخراج کردن فایل‌های نرم‌افزار، به مانند شکل ۱۱-۳۱، یک مسیر را در سرور انتخاب و بر روی Next کلیک کنید تا این کار انجام شود.



شکل ۱۱- ۳۰ نصب و راه‌اندازی SCOM

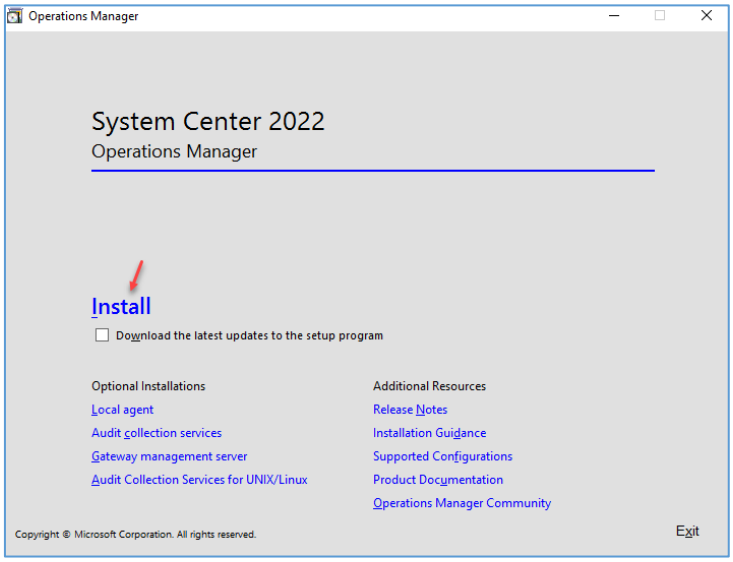
www.takbook.com

بعد از استخراج شدن فایل، به مانند شکل ۱۱-۳۲، بر روی Setup، کلیک کنید تا کار نصب را آغاز کنید.



شکل ۱۱- ۳۱ نصب و راه‌اندازی SCOM

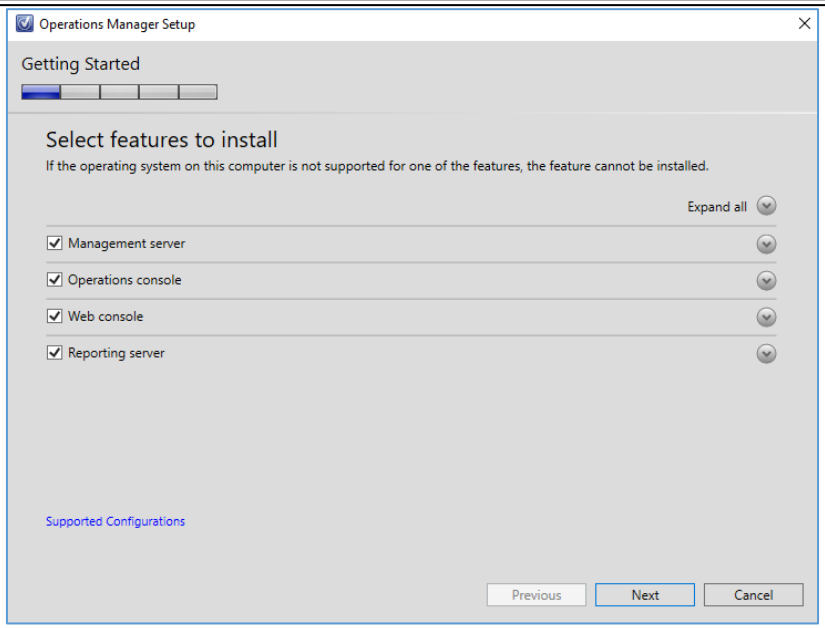
در شکل ۱۱-۳۳، صفحه‌ی اوّل Operation Manager را مشاهده می‌کنید، برای شروع کار بر روی Install کلیک کنید.



شکل ۱۱- ۳۲ نصب و راه‌اندازی SCOM

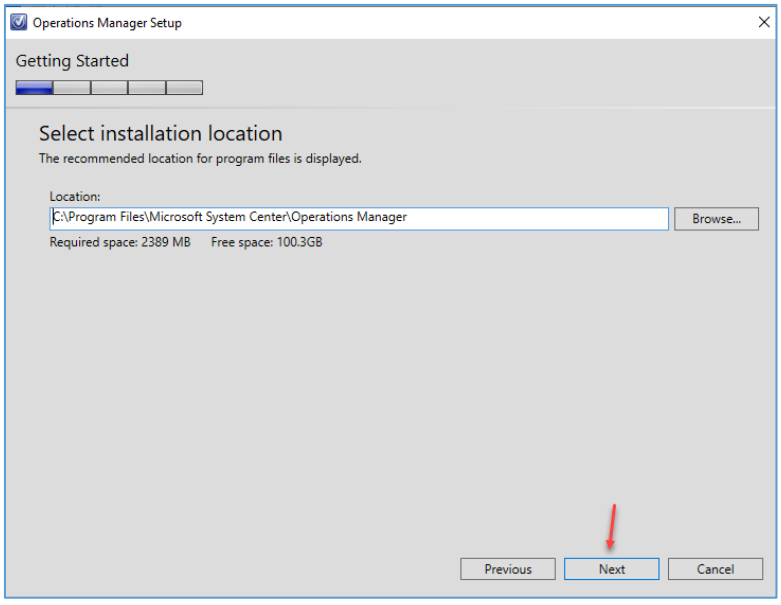
در شکل ۱۱-۳٤، تیک هر چهار گزینه را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۱- ۳۳ نصب و راه‌اندازی SCOM

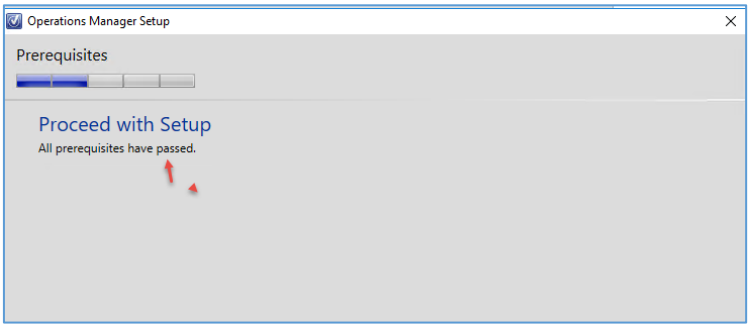
در شکل ۱۱-۳۵، آدرس محلّ نصب نرم‌افزار را مشخّص کنید، توجّه داشته باشید محلّ مورد نظر دارای ظرفیّت حداقل، ۲۳۸۹ مگابایت باشد.



شکل ۱۱- ۳۴ نصب و راه‌اندازی SCOM

www.takbook.com

همان‌طور که شکل ۱۱-۳۶، مشاهده می‌کنید، تمام پیش‌نیازها که از قبل نصب کردید، به درستی تأیید شده است، بر روی Next کلیک کنید.



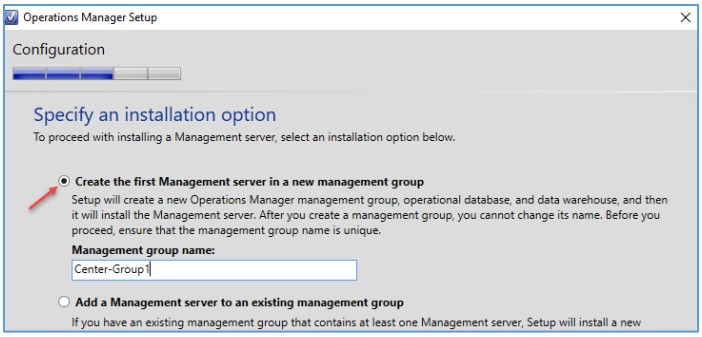
شکل ۱۱- ۳۵ نصب و راه‌اندازی SCOM

اگر در شکل ۱۱-۳۶، با خطای سرویس Asp.net روبرو شدید می‌توانید از طریق دستورات زیر این سرویس را بر روی سرور نصب کنید.

```
Import-Module ServerManager
Add-WindowsFeature Web-ASP-Net, Web-ISAPI-Filter, Web-Mgmt-Console, NET-Framework-Features, Web-Mgmt-Service, Web-Scripting-Tools, Web-ASP-Net45, Web-ISAPI-Ext -source:D:\sources\sxs
```

در شکل ۱۱-۳۷، 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.

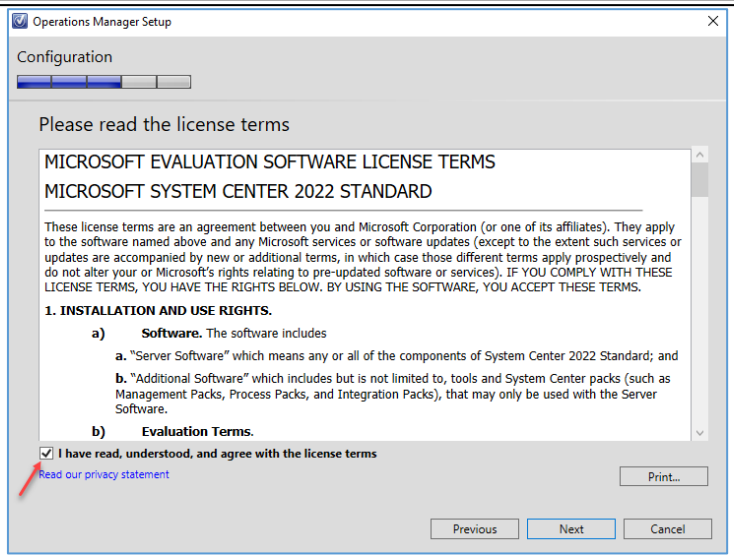
بر روی Next کلیک کنید.



شکل ۱۱- ۳۶ نصب و راه‌اندازی SCOM

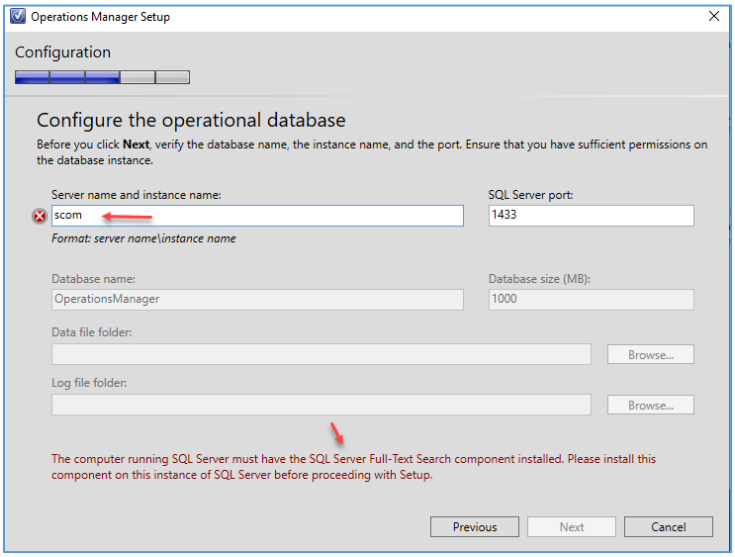
در شکل ۱۱-۳۸، اگر توافقنامه‌ی استفاده از نرم‌افزار مورد تأیید است، تیک مورد نظر را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۱- ۳۷ نصب و راه‌اندازی SCOM

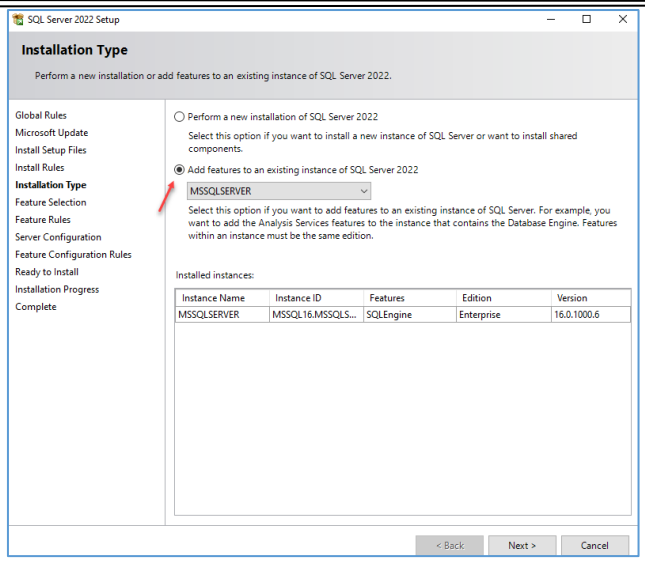
در شکل ۱۱-۳۹، باید اطلاعات را تکمیل کنید برای شروع کار در قسمت اول نام سرور را وارد کنید، بعد وارد کردن نام سرور با خطا روبرو می‌شوید که در این خطا اعلام می‌شود که ویژگی SQL Server Full-Text Search نصب نشده است که باید وارد SQL بشویم و آن را نصب کنیم.



شکل ۱۱- ۳۸ نصب و راه‌اندازی SCOM

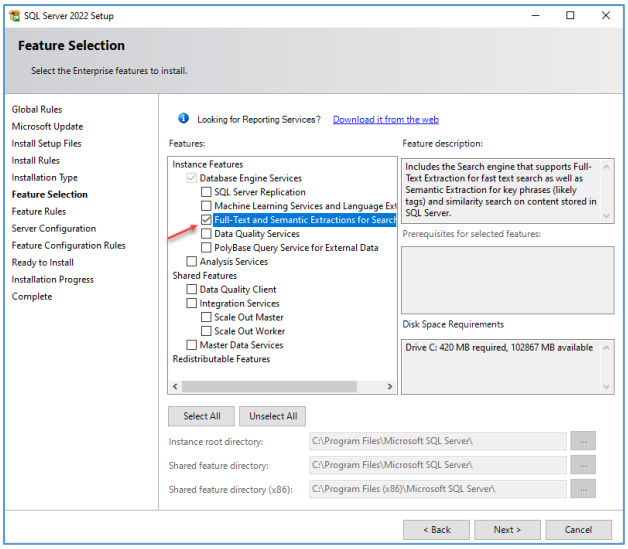
فایل Setup نرم‌افزار SQL Server 2022 اجرا کنید و به مانند شکل ۱۱-۴۰، Instance قبلی را که نصب کرده بودیم انتخاب کنید تا ویژگی مورد نظر را به آن اضافه کنیم.

www.takbook.com



شکل ۱۱- ۳۹ نصب و راه‌اندازی SCOM

در شکل ۱۱-٤۱، گزینه ...Full-Text را انتخاب کنید و آن را نصب کنید.

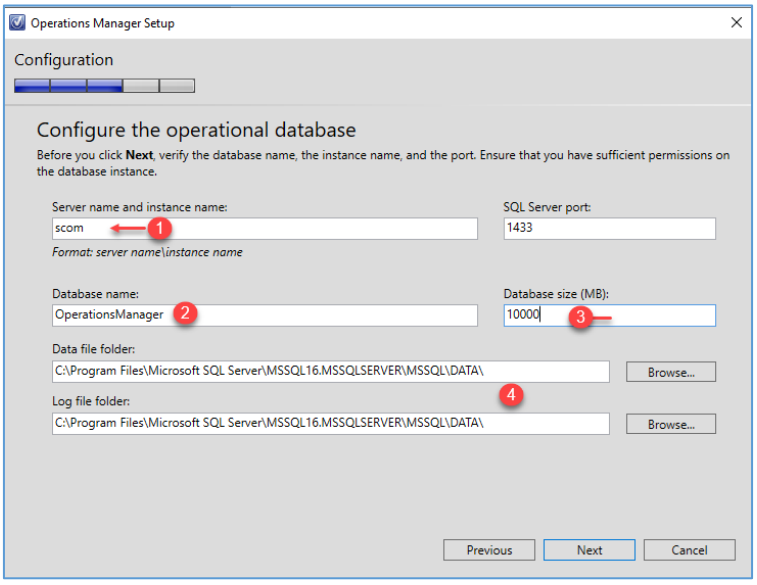


شکل ۱۱- ۴۰ نصب و راه‌اندازی SCOM

در شکل ۱۱-٤۲، 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

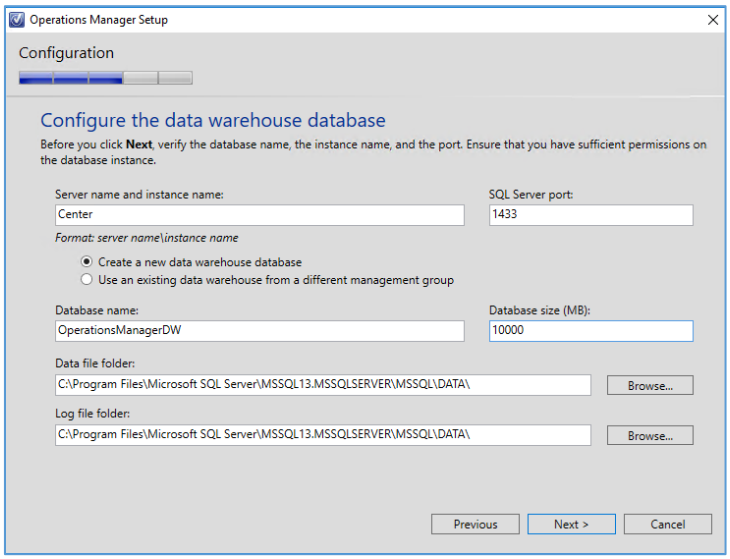
www.takbook.com

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.



شکل ۱۱- ۴۱ نصب و راه‌اندازی SCOM

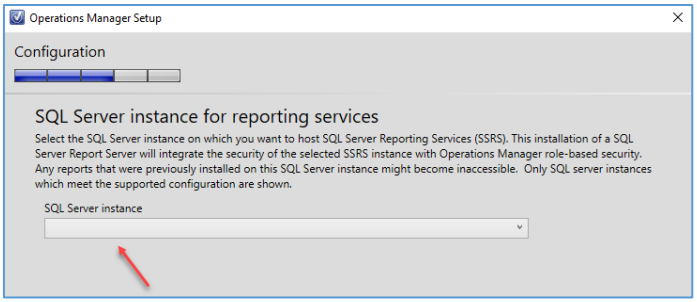
در شکل ۱۱-٤۳، نیز به مانند صفحه‌ی قبل عمل کنید و نام سرور Center را وارد کنید و حجم دیتابیس را تغییر دهید و بر روی Next کلیک کنید.



شکل ۱۱- ۴۲ نصب و راه‌اندازی SCOM

www.takbook.com

در شکل ۱۱–٤٤، باید Instance مربوط به سرویس Reporting را مشخّص کنید که این سرویس را در موقع نصب SQL باید فعّال می‌کردیم، به این دلیل Instance به صورت خودکار شناسایی نشد و باید این سرویس را بر روی SQL نصب کنیم.

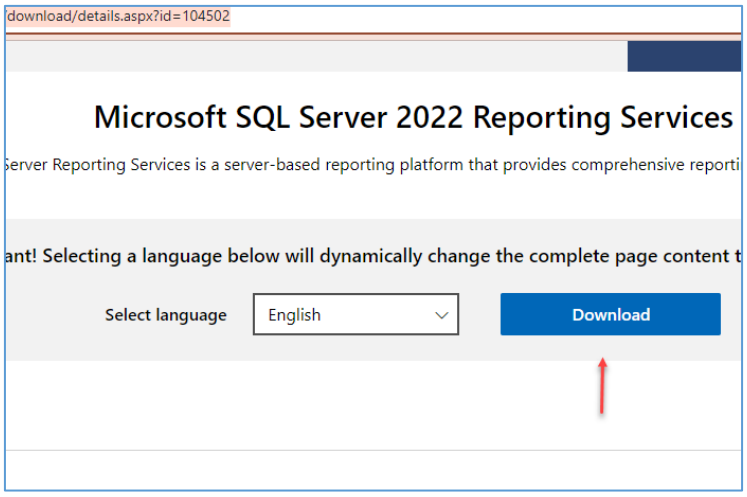


شکل ۱۱- ۴۳ نصب و راه‌اندازی SCOM

برای نصب سرویس Reporting وارد آدرس زیر شوید و نرم‌افزار SQL Server Reporting Service را دانلود کنید:

https://www.microsoft.com/en-us/download/details.aspx?id=104502

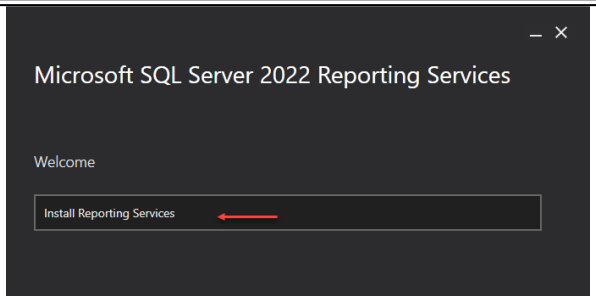
به مانند شکل ۱۱–٤٥، بر روی دانلود کلیک کنید و فایل را اجرا کنید:



شکل ۱۱- ۴۴ نصب Reporting Service

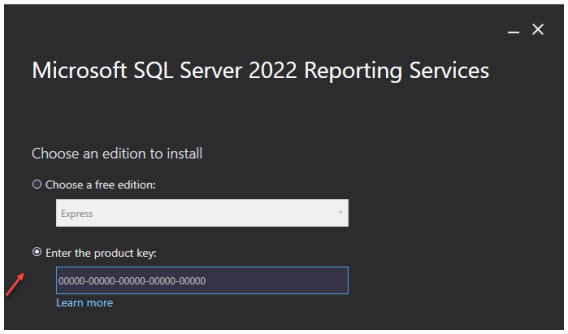
در شکل ۱۱–٤٦، بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۱- ۴۵ نصب *Reporting Service*

در شکل ۱۱-۴۷، باید لایسنس نرم‌افزار را وارد کنید، اگر لایسنس در دسترس ندارید می‌توانید صفر وارد کنید.



شکل ۱۱- ۴۶ نصب *Reporting Service*

در شکل ۱۱-۴۸، توافقنامه را تایید و بر روی Next کلیک کنید.



شکل ۱۱- ۴۷ نصب *Reporting Service*

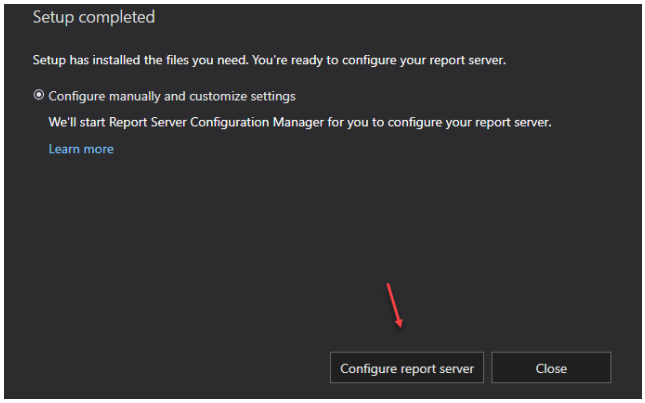
در شکل ۱۱-۴۹، بر روی Next کلیک کنید.

www.takbook.com



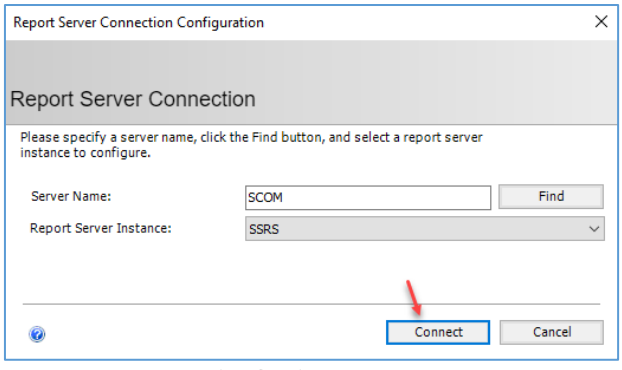
شکل ۱۱- ۴۸ نصب *Reporting Service*

بعد از نصب به مانند شکل ۱۱–۵۰، بر روی Configure report server کلیک کنید.



شکل ۱۱- ۴۹ نصب *Reporting Service*

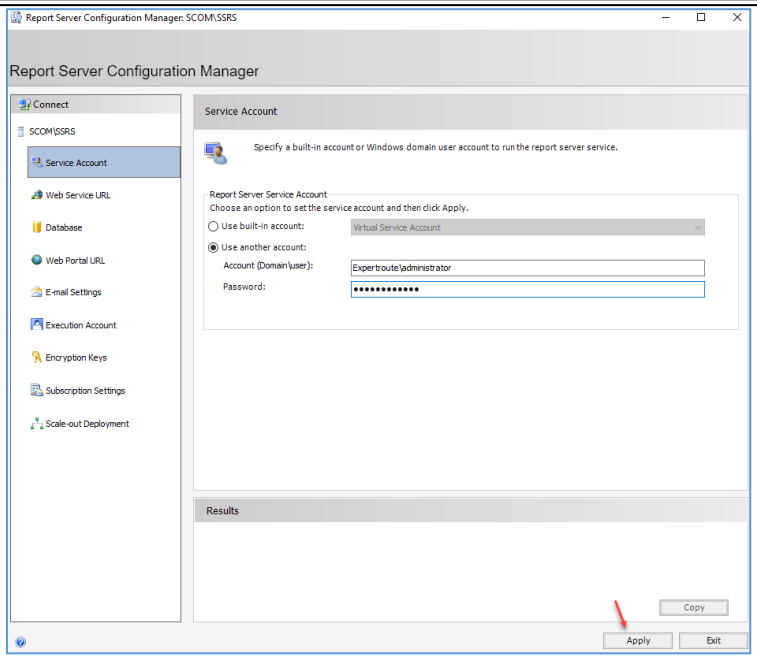
در شکل ۱۱–۵۱، بر روی Connect کلیک کنید.



شکل ۱۱- ۵۰ نصب *Reporting Service*

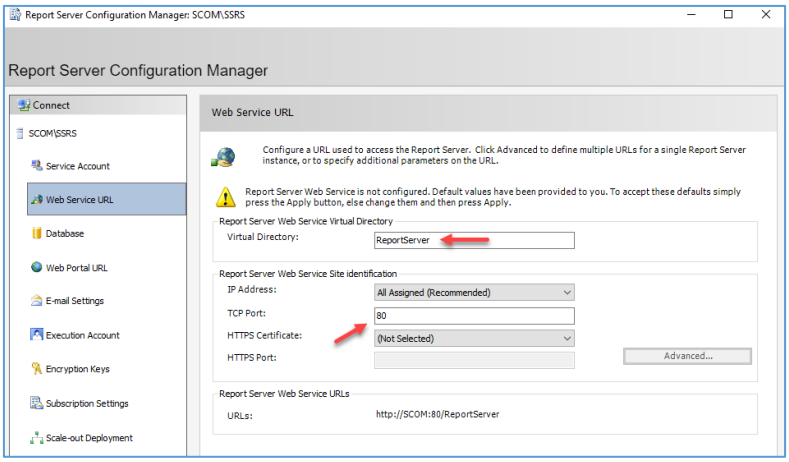
در شکل ۱۱–۵۲، باید اکانت مورد نظر خود که دسترسی کامل به شبکه دارد را وارد کنید.

www.takbook.com



شکل ۱۱- ۵۱ نصب *Reporting Service*

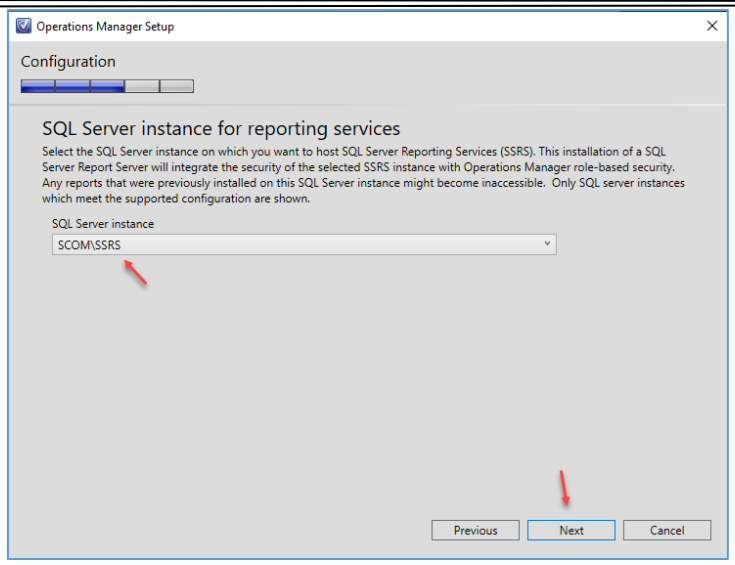
در شکل ۱۱-۵۳، باید سرویس تحت وب را فعال کنید، یک نام به دلخواه وارد کنید و آدرس مورد نظر را انتخاب کنید و در قسمت TCP Port باید پورت 443 را وارد کنید و در آخر بر روی Apply کلیک کنید.



شکل ۱۱- ۵۲ نصب *Reporting Service*

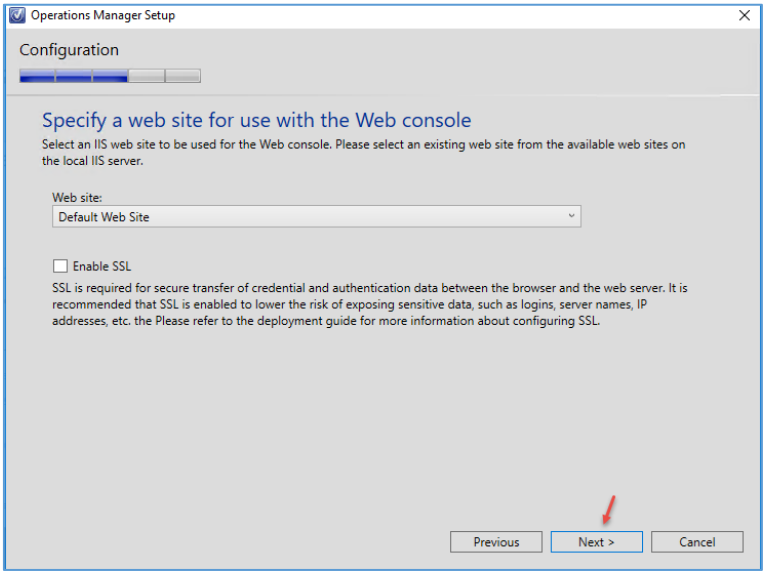
به مانند شکل ۱۱-۵۴، نصب Operation Manager همان Report Server که با هم در قسمت قبل ایجاد کردیم را انتخاب کنید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۱- ۵۳ نصب و راه‌اندازی SCOM

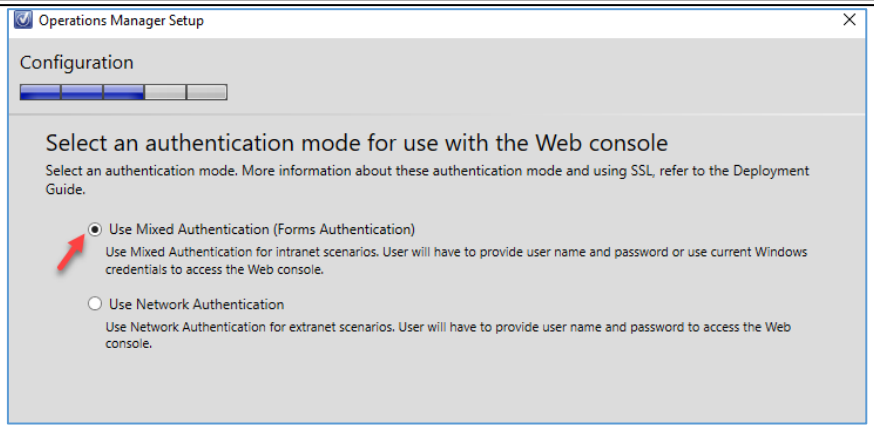
در شکل ۱۱-۵۵، یک وب سایت از سرویس IIS انتخاب می‌شود تا بر روی آن، کنسول وب این نرم‌افزار فعّال شود، بر روی Next کلیک کنید.



شکل ۱۱- ۵۴ نصب و راه‌اندازی SCOM

در شکل ۱۱-۵۶، باید روش احراز هویّت را مشخّص کنید که در حال حاضر باید گزینه‌ی اوّل را انتخاب و بر روی Next کلیک کنید.

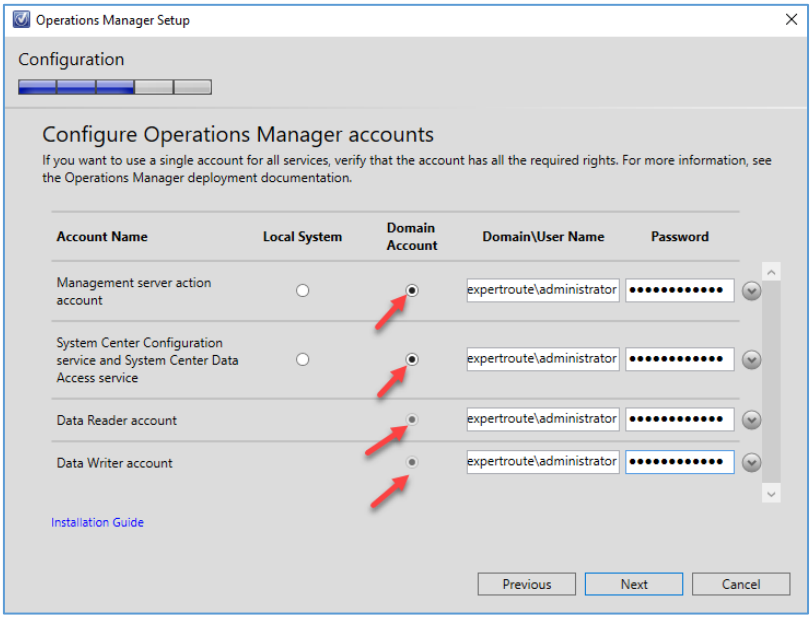
www.takbook.com



شکل ۱۱- ۵۵ نصب و راه‌اندازی SCOM

در شکل ۱۱–۵۷، Account ادمین شبکه را وارد کنید، البتّه اگر این اکانت Administrator نباشد، بهتر خواهد بود.

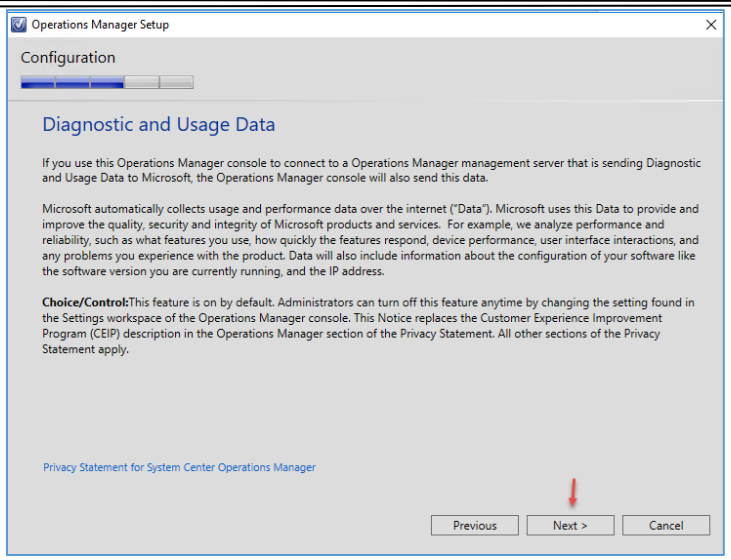
به مانند شکل ۱۱–۵۷،، نام کاربری و رمز عبور مربوط را وارد و بر روی Next کلیک کنید، توجه داشته باشید اگر کاربر Administrator را وارد کنید با اخطاری روبرو می‌شوید که به این نکته اشاره دارد که باید از نام کاربر دیگری برای این کار استفاده کنید تا مدیریت مشکلات آسان‌تر شود.



شکل ۱۱- ۵۶ نصب و راه‌اندازی SCOM

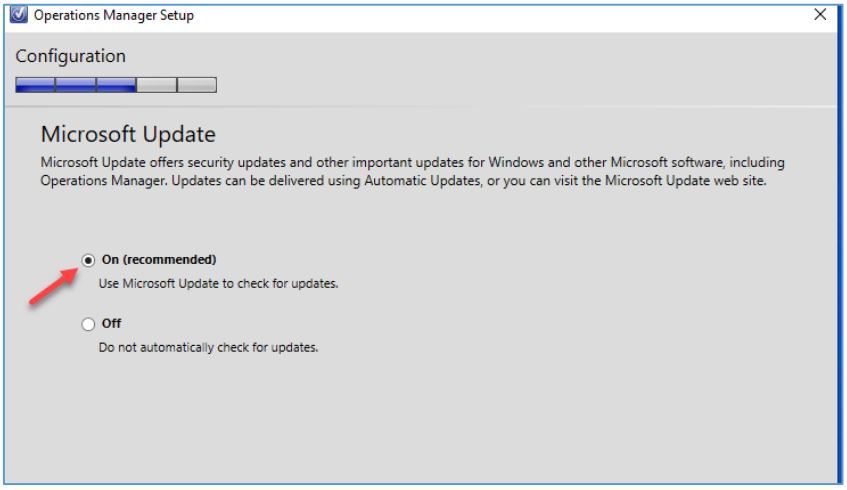
در شکل ۱۱–۵۸، بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۱- ۵۷ نصب و راه‌اندازی SCOM

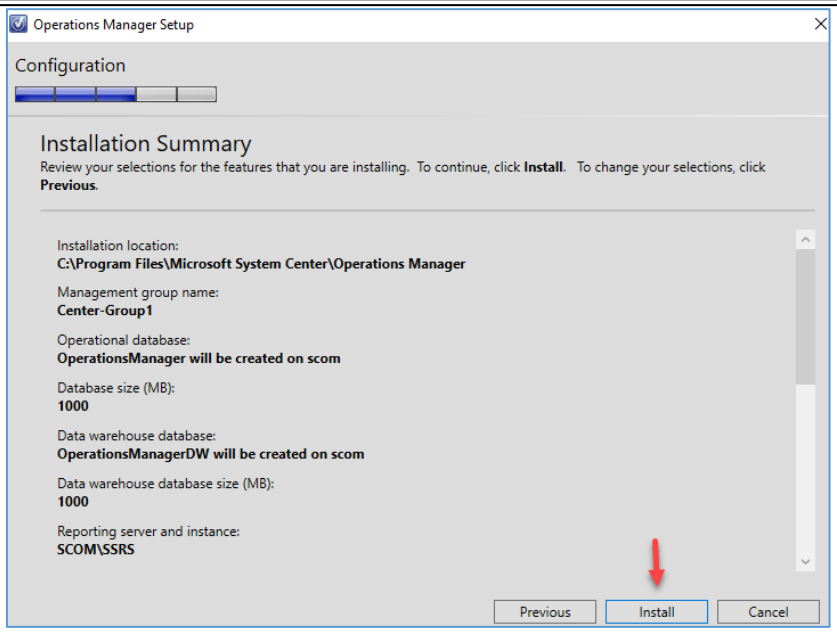
در شکل ۱۱-۵۹، اگر مایل بودید که نرم‌افزار شما آپدیت شود، گزینه‌ی On را انتخاب کنید، در غیر این صورت، گزینه‌ی Off را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۱- ۵۸ نصب و راه‌اندازی SCOM

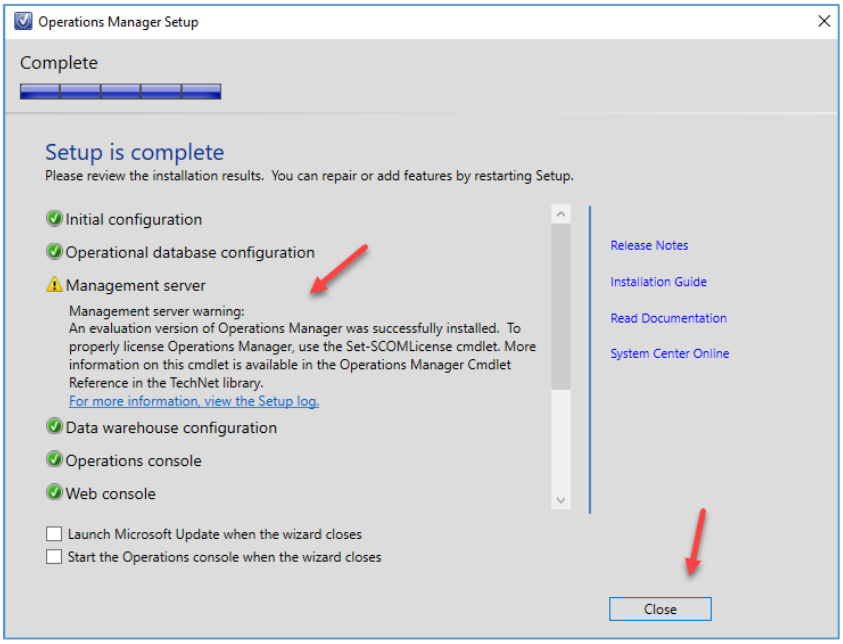
در شکل ۱۱-۶۰، اگر تنظیماتی که انجام دادید، مورد تأیید است بر روی Install کلیک کنید.

www.takbook.com



شکل ۱۱- ۵۹ نصب و راه‌اندازی SCOM

همان‌طور که در شکل ۱۱-۶۱، 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.



شکل ۱۱- ۶۰ نصب و راه‌اندازی SCOM

www.takbook.com

تیک گزینه‌ی مورد نظر را بردارید و بر روی Close کلیک کنید، حتماً سرور را Restart کنید.

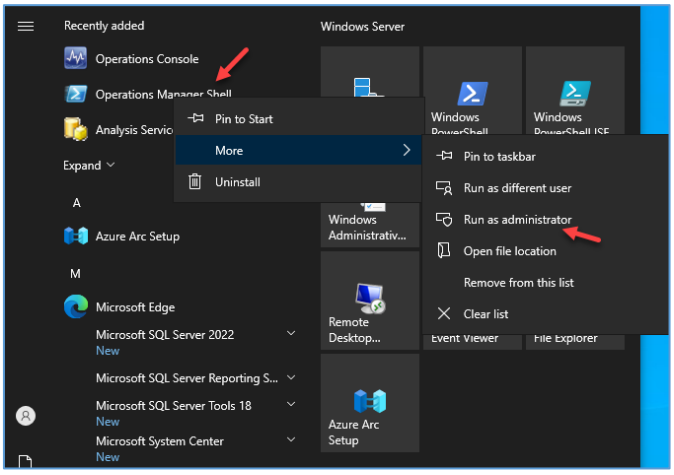
برای فعّال‌سازی لایسنس باید به صورت زیر عمل کنید:

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
```

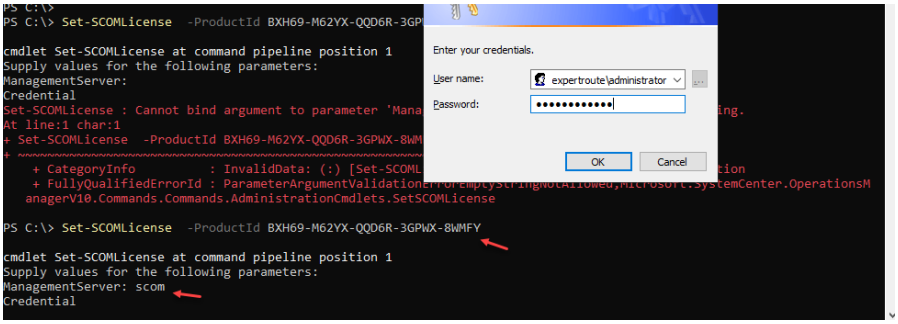
در دستور بالا، شما باید به جای X، سریال نرم‌افزار را وارد کنید.

بعد از نصب نرم‌افزار به مانند شکل ۱۱-٦۲، وارد Start شوید و پوشه‌ی مربوط به System Center 2016 را باز کنید و سرویس Operation Management Shell را اجرا کنید.



شکل ۱۱- ٦۱ نصب و راه‌اندازی SCOM

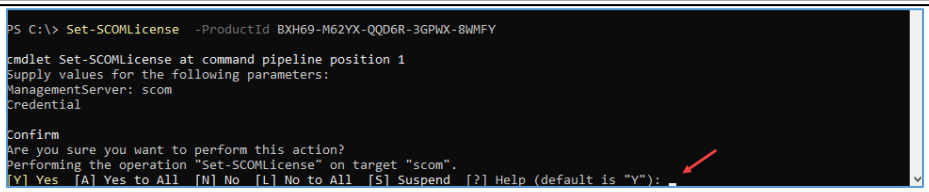
همان‌طور که در شکل ۱۱-٦۳، مشاهده می‌کنید، لایسنس مورد نظر بر روی سرور فعّال شده است.



شکل ۱۱- ٦۲ نصب و راه‌اندازی SCOM

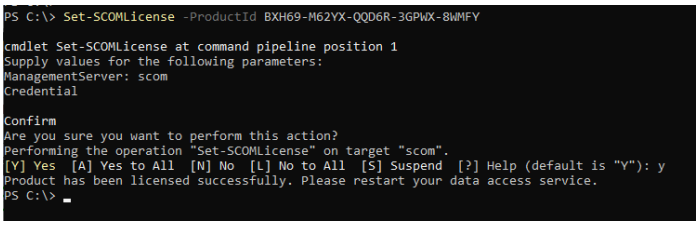
در شکل ۱۱-٦٤، باید کلمه‌ی Y را وارد کنید تا لاینس مورد نظر تایید شود.

www.takbook.com



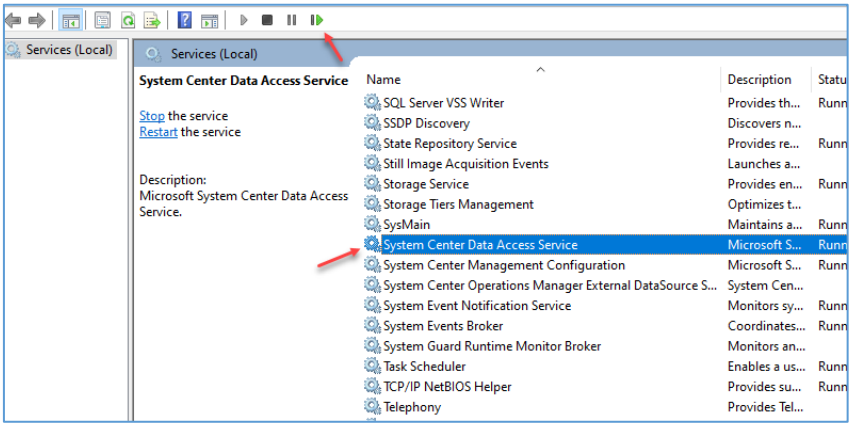
شکل ۱۱- ۶۳ نصب و راه‌اندازی SCOM

همان‌طور که در شکل ۱۱-۶۵، مشاهده می‌کنید لایسنس مورد نظر با موفقیت تایید شد.



شکل ۱۱- ۶۴ نصب و راه‌اندازی SCOM

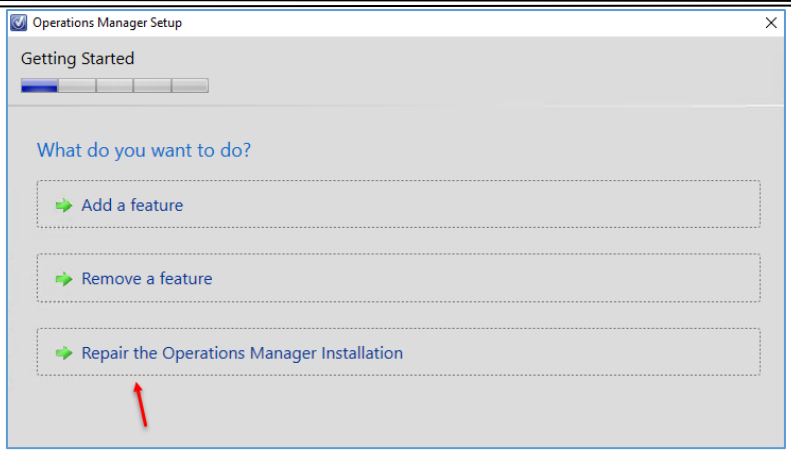
در ادامه به مانند شکل ۱۱-۶۶ وارد Services شوید و سرویس System Center Data Access Service را ری استارت کنید.



شکل ۱۱- ۶۵ نصب و راه‌اندازی SCOM

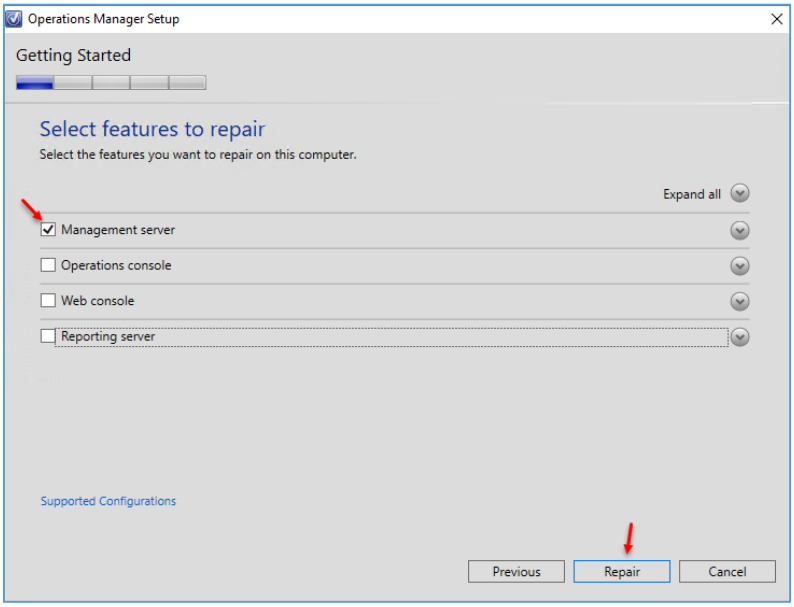
بعد از اینکه لایسنس نرم‌افزار را وارد کردید، دوباره فایل Setup مربوط به نرم‌افزار Operations Manager را اجرا کنید که شکل ۱۱-۶۷، ظاهر خواهد شد، در این قسمت بر روی Repair the Operations کلیک کنید تا بار دیگر، نرم‌افزار با لایسنس جدید نصب شود.

www.takbook.com



شکل ۱۱- ۶۶ نصب و راه‌اندازی SCOM

در شکل ۱۱–۶۸، 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.

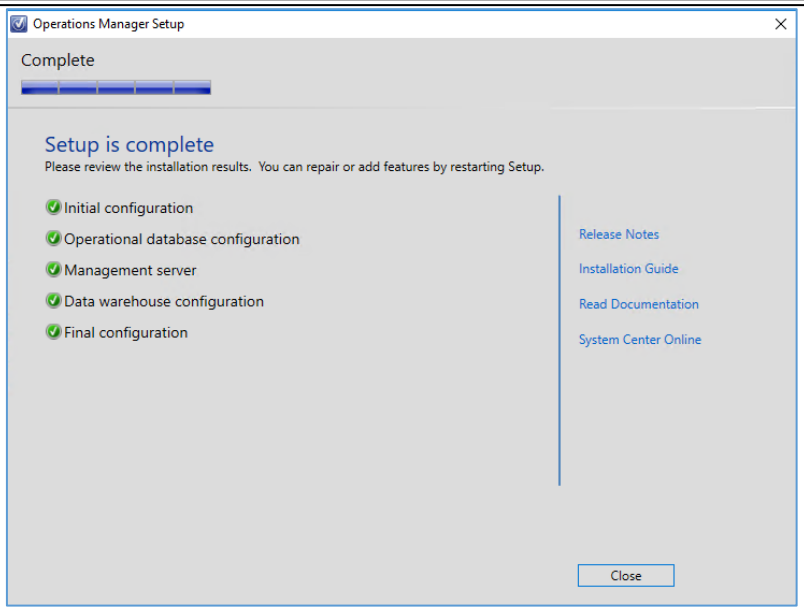


شکل ۱۱- ۶۷ نصب و راه‌اندازی SCOM

همان‌طور که در شکل ۱۱–۶۹، مشاهده می‌کنید، عملیّات به طور کامل انجام شده و سیستم، آماده‌ی کار است.

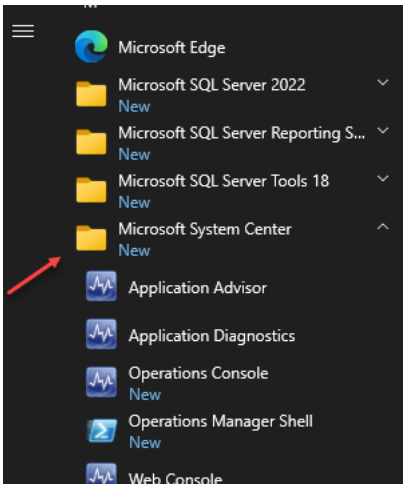
برای بار آخر، سرور را Restart کنید تا کار خود را با این نرم‌افزار آغاز کنید.

www.takbook.com



شکل ۱۱- ۶۸ نصب و راه‌اندازی SCOM

این نرم افزار، بعد از نصب دارای چندین ابزار است که در شکل ۱۱-۶۹، مشاهده می کنید، برای شروع کار بر روی Operations Console کلیک کنید.

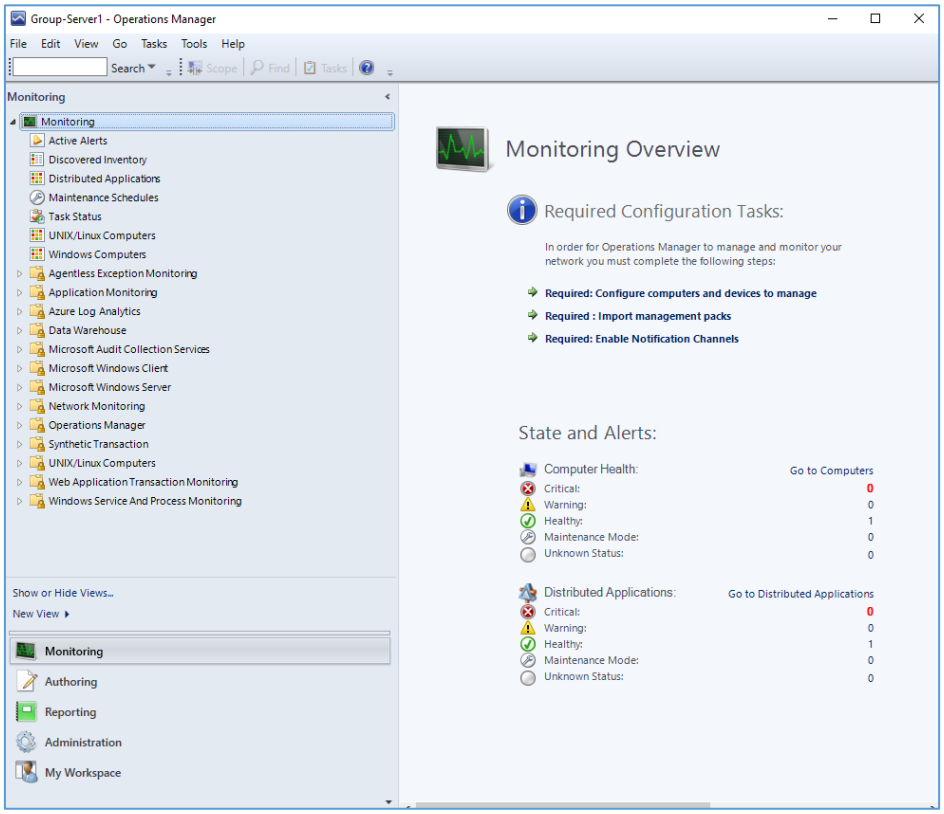


شکل ۱۱- ۶۹اجرای Operations Console

در شکل ۱۱-۷۰، صفحه‌ی مدیریّتی نرم‌افزار Operations Manager را مشاهده می‌کنید که دارای ابزارهای مختلف برای مدیریّت هر چه بهتر شبکه است، در سمت چپ، ۵ قسمت را مشاهده می‌کنید که قسمت

www.takbook.com

Monitoring، همان‌طور که از نامش پیداست، برای مانیتور کردن شبکه کاربرد دارد که این قسمت، خود از ابزارهای زیادی تشکیل شده است.



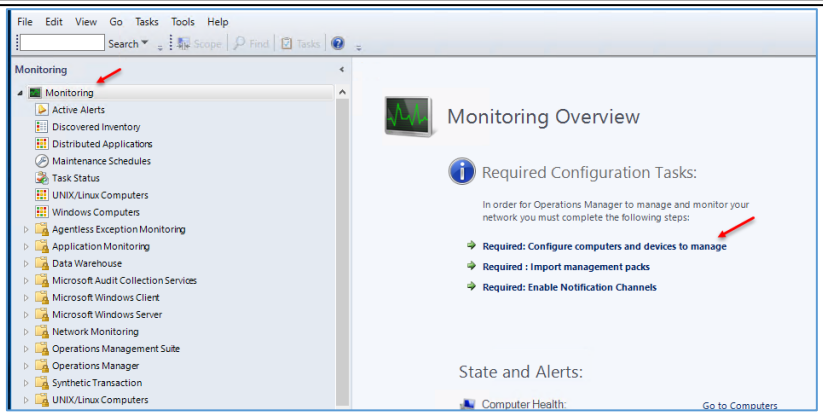
شکل ۱۱- ۷۰ نصب و راه‌اندازی SCOM

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.

۱۱-٤-۱ کار با قسمت Monitoring در System Center

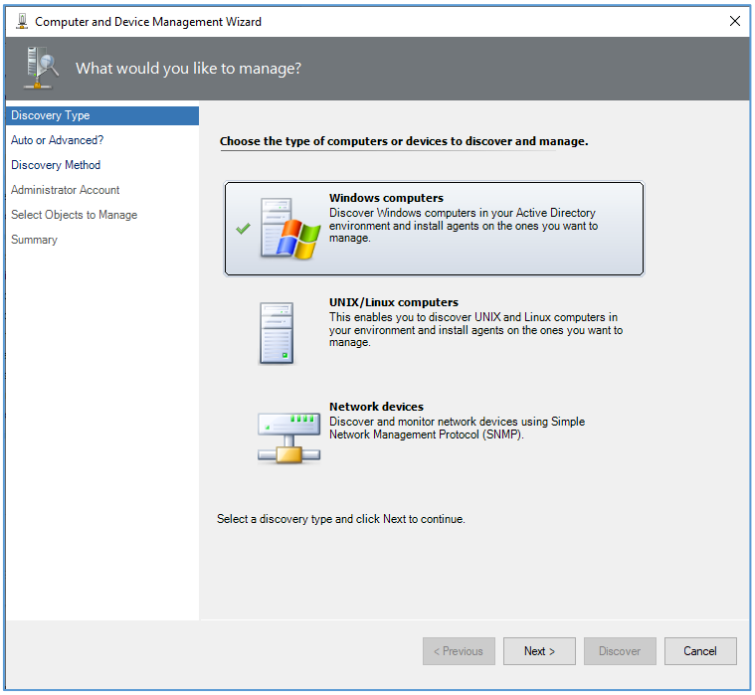
برای شروع و مانیتور کردن کلّ شبکه به مانند شکل ۱۱-۷۱، وارد قسمت Monitoring شوید و به مانند شکل Requires: Configure computers and devices to manage را انتخاب کنید.

www.takbook.com



شکل ۱۱- ۷۱ بررسی قسمت *Monitoring*

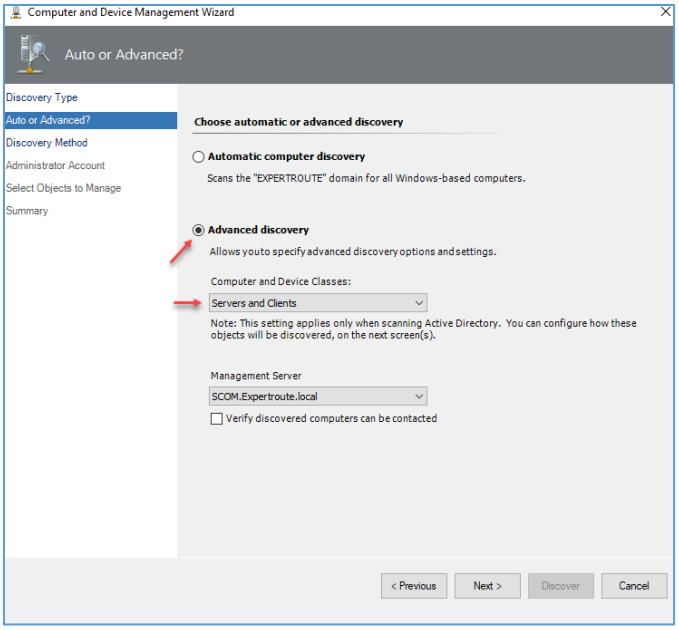
در شکل ۱۱-۷۲، سه گزینه وجود دارد؛ گزینه‌ی اوّل برای سیستم‌هایی است که با سیستم عامل ویندوز کار می‌کنند، گزینه‌ی دوّم سیستم‌هایی است که با سیستم عامل لینوکس کار می‌کنند و گزینه‌ی آخر نیز برای سیستم‌هایی است که پروتکل SNMP روی آنها فعّال شده است و می‌خواهید از آن اطّلاعات دریافت کنید، در این قسمت بر روی گزینه‌ی اوّل کلیک کنید.



شکل ۱۱- ۷۲ بررسی قسمت *Monitoring*

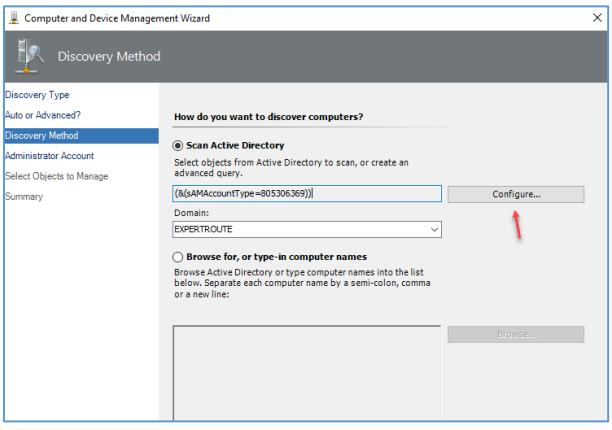
www.takbook.com

در شکل ۱۱-۷۳، 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.



شکل ۱۱- ۷۳ بررسی قسمت Monitoring

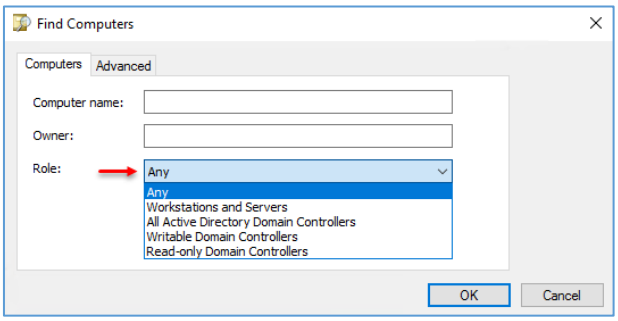
در شکل ۱۱-۷٤، اگر گزینه‌ی اوّل را انتخاب کنید، تمام سیستم‌های داخل Active Directory بررسی خواهند شد و اگر بخواهید عملیّات را تنها بر روی یک سیستم خاص انجام دهید باید گزینه‌ی دوّم را انتخاب و نام سیستم را وارد کنید.



شکل ۱۱- ۷۴ بررسی قسمت Monitoring

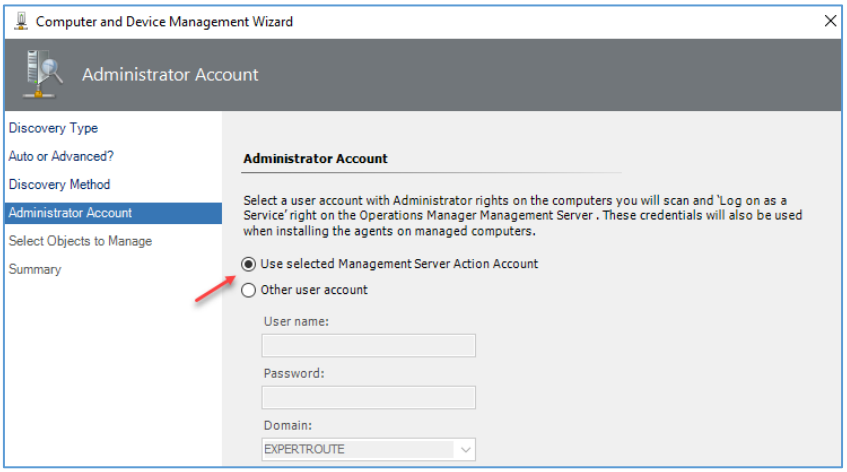
www.takbook.com

در شکل ۱۱-۷٤، گزینه‌ی اوّل را انتخاب و بر روی Configure کلیک کنید، در شکل ۱۱-۷۵، می‌توانید نوع Active Directory را مشخّص کنید که باید گزینه‌ی Any ر انتخاب کنید.



شکل ۱۱- ۷۵ بررسی قسمت Monitoring

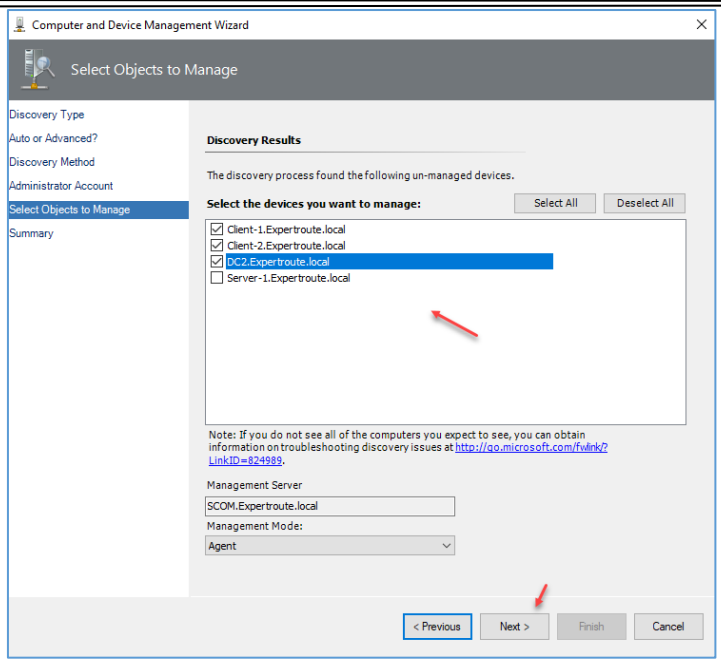
در شکل ۱۱-۷٦، باید یک اکانت با دسترسی کامل وارد کنید، می‌توانید گزینه‌ی اوّل را انتخاب کنید تا با همان اکانتی که نرم‌افزار Operation Manager را نصب کردید، کار مانیتورینگ انجام شود و یا اگر می‌خواهید اکانت دیگری را وارد کنید باید گزینه‌ی Other user account را انتخاب و اکانت مورد نظر را وارد کنید، گزینه‌ی اوّل را انتخاب کنید و بر روی Discover کلیک کنید.



شکل ۱۱- ۷۶ بررسی قسمت Monitoring

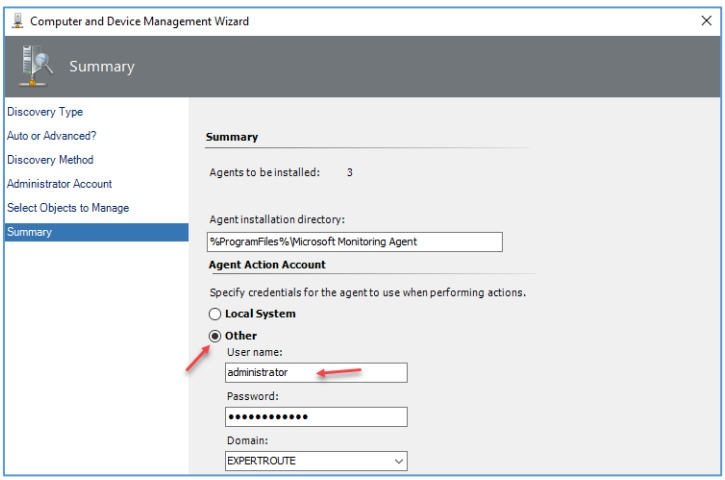
در شکل ۱۱-۷۷، بعد از بررسی شبکه، دو سیستم در دسترس بوده است و در لیست قرار گرفتند، برای اینکه عملیّات مانیتورینگ را بر روی آنها انجام دهید، آنها را انتخاب کنید تا بعد از Next، یک نرم‌افزار Agent که مربوط به این Operations Maneger است، در سیستم مقصد نصب شود تا اطّلاعات آن سیستم برای سرور ارسال شود.

www.takbook.com



شکل ۱۱- ۷۷ بررسی قسمت Monitoring

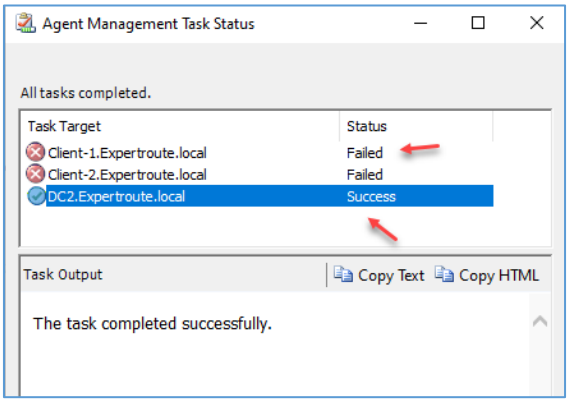
در شکل ۱۱–۷۸، مسیر نصب Agent در سیستم مقصد مشخّص شده است که در ProgramFiles انجام می‌شود، شما می‌توانید برای این نرم‌افزار یک اکانت خاص وارد کنید تا اجرا شود و یا آن را بر روی Local System قرار دهید.



شکل ۱۱- ۷۸ بررسی قسمت Monitoring

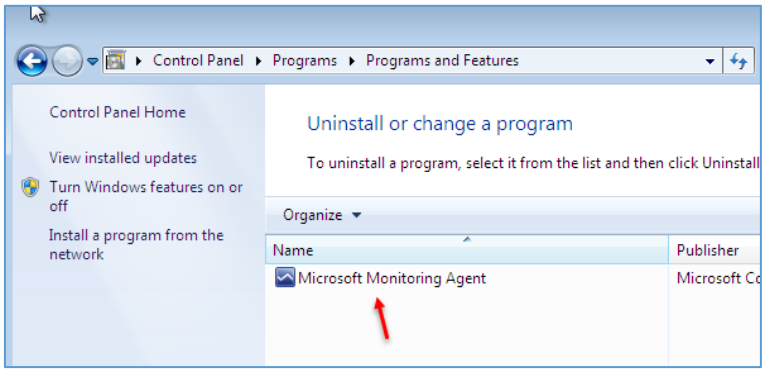
www.takbook.com

در شکل ۱۱-۷۹، Agent مورد نظر در یک سیستم نصب شده است و در دو سیستم دیگر نصب نشده است و با خطا روبرو شده است.



شکل ۱۱- ۷۹ بررسی قسمت Monitoring

اگر در یکی از سیستم‌هایی که این نرم‌افزار نصب شده است به مانند شکل ۱۱-۸۰، وارد قسمت Program and Features شوید، به مانند شکل نرم‌افزار Agent را مشاهده خواهید کرد، در دو سیستمی که خطا داده نرم‌افزار Agent را به صورت دستی نصب می‌کنیم.



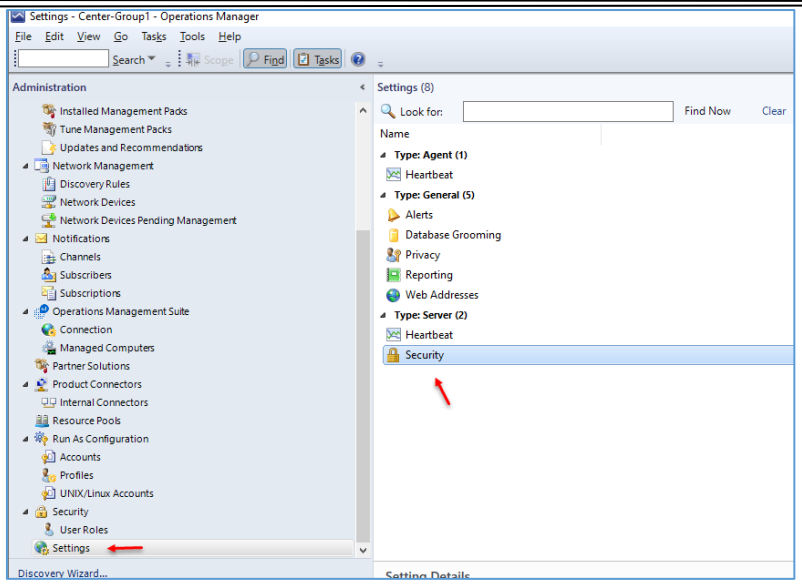
شکل ۱۱- ۸۰ بررسی قسمت Monitoring

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، نرم‌افزارOperation Manager ارسال می‌شود که اگر آن را تأیید کنید، کلاینت زیر مجموعه‌ی نرم‌افزار خواهد شد.

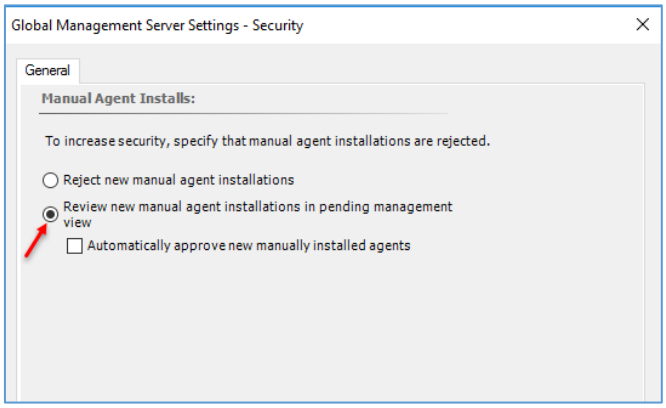
به مانند شکل ۱۱-۸۱، از سمت چپ وارد قسمت Settings شوید و بر روی گزینه‌ی Security کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.

www.takbook.com



شکل ۱۱- ۸۱ نصب *Agent* در کلاینت

در شکل ۱۱-۸۲، 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.



شکل ۱۱- ۸۲ نصب *Agent* در کلاینت

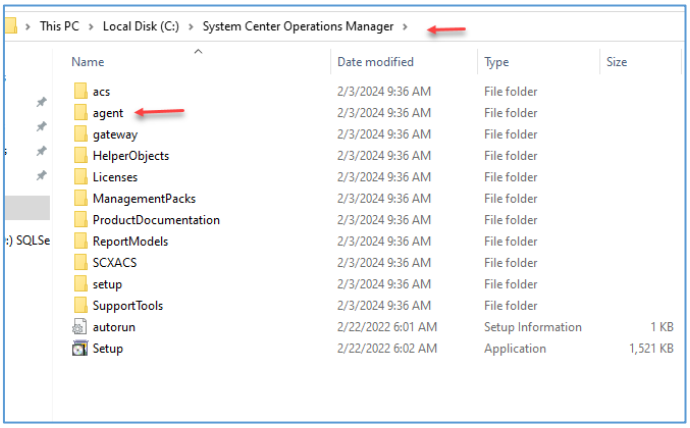
برای این که Agent را بر روی یک کلاینت نصب کنید، می‌توانید از بسته‌ی خود نرم‌افزار SCOM استفاده کنید و به مانند شکل ۱۱-۸۳، فایل Setup اصلی را اجرا کنید و بر روی Local Agent کلیک کنید تا Setup آن اجرا شود، راه دیگر این است که از خود فایل Agent استفاده کنید.

www.takbook.com



شکل ۱۱- ۸۳ نصب *Agent* در کلاینت

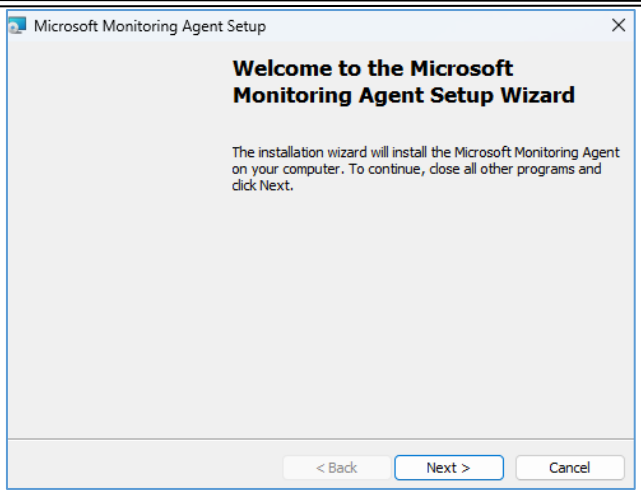
همان‌طور که در شکل ۱۱-۸٤، مشاهده می‌کنید، نرم‌افزار Agent در پوشه‌ی Agent وجود دارد که می‌توانید این پوشه را برای کاربران خود، Share کنید تا بتوانند آن را نصب کنند و یا اینکه از طریق Group Policy نرم‌افزار را برای کاربران نصب کنید، در هر صورت، این فایل را اجرا کنید و بر روی کلاینت نصب کنید.



شکل ۱۱- ۸۴ نصب *Agent* در کلاینت

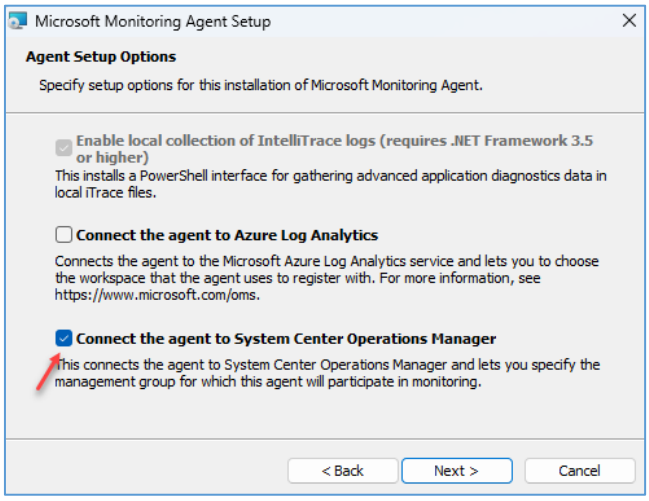
به مانند شکل ۱۱-۸۵، بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۱- ۸۵ نصب *Agent* در کلاینت

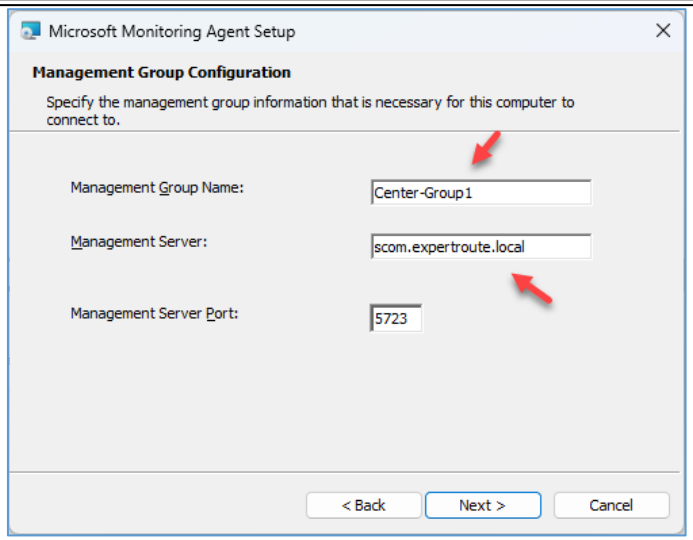
در شکل ۱۱-۸۶ برای متّصل شدن به سرور SCOM، تیک گزینه‌ی آخر را انتخاب و بر روی Next کلیک کنید.



شکل ۱۱- ۸۶ نصب *Agent* در کلاینت

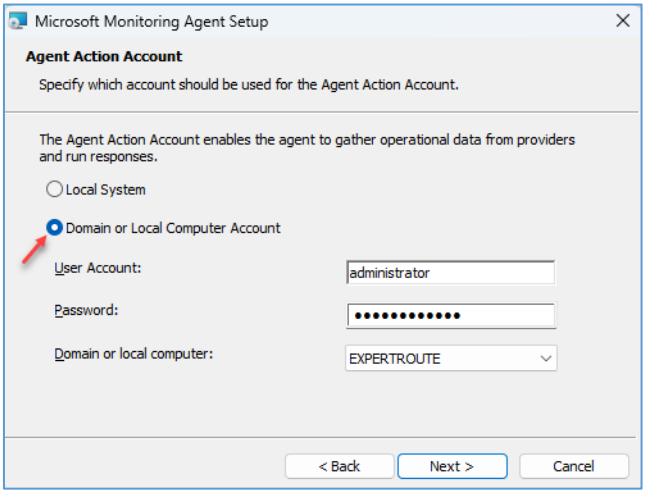
در شکل و در قسمت اوّل باید نام گروهی که در هنگام نصب وارد کردید را وارد کنید که در این کتاب، نام را Center-Group1 وارد کردیم، در قسمت دوّم باید نام سرور را وارد کنید و به پورت پیش‌فرض آن دست نزنید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۱- ۸۷ نصب *Agent* در کلاینت

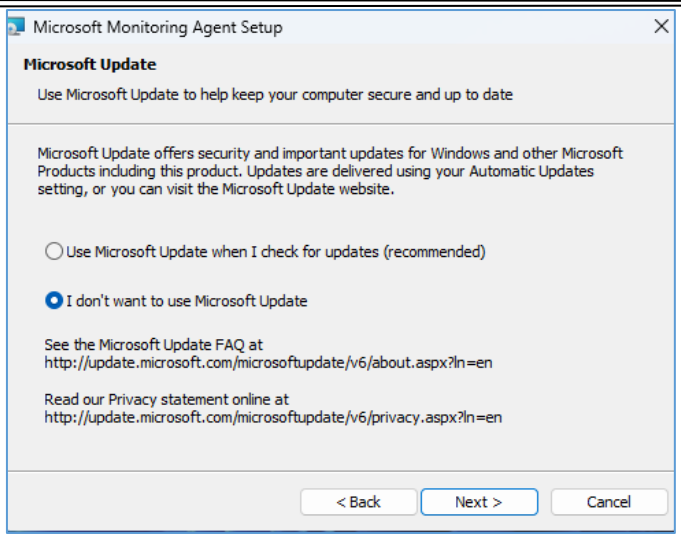
در این قسمت، Local System را انتخاب و بر روی Next کلیک کنید، اگر چنانچه می‌خواهید از یک اکانت دیگر تحت دومین که دسترسی لازم را دارد، استفاده کنید باید گزینه‌ی دوّم را انتخاب و نام اکانت مورد نظر را وارد کنید.



شکل ۱۱- ۸۸ نصب *Agent* در کلاینت

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

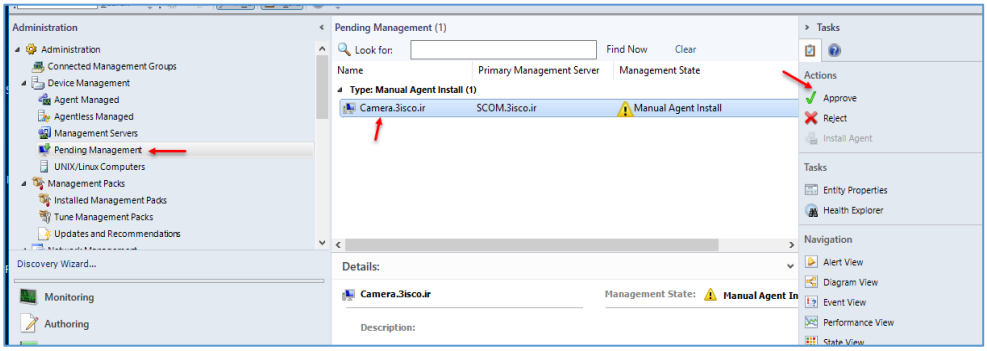
www.takbook.com



شکل ۱۱- ۸۹ نصب *Agent* در کلاینت

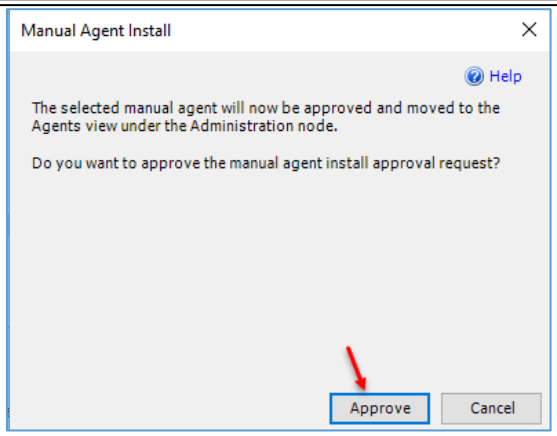
در صفحه‌ی بعد بر روی Install کلیک کنید.

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.



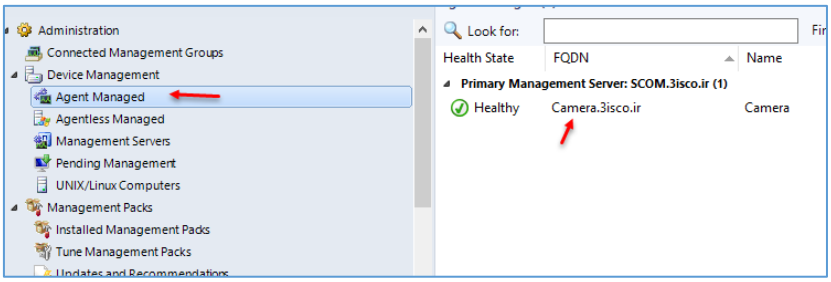
شکل ۱۱- ۹۰ نصب *Agent* در کلاینت

www.takbook.com



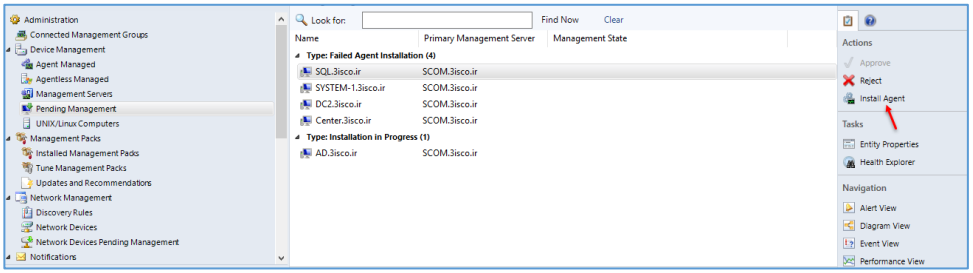
شکل ۱۱- ۹۱ نصب *Agent* در کلاینت

اگر به قسمت Agent Managed مراجعه کنید، مشاهده خواهید کرد که سیستم مورد نظر تأیید و به لیست اضافه شده است.



شکل ۱۱- ۹۲ نصب *Agent* در کلاینت

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.



شکل ۱۱- ۹۳ نصب *Agent* در کلاینت

www.takbook.com

۱۱-۵سرویس Microsoft Endpoint Configuration Manager

مایکروسافت Endpoint Configuration Manager، که قبلاً با نام System Center Configuration Manager یا SCCM شناخته می‌شد، یکی از محصولات مهم مایکروسافت برای مدیریت و کنترل شبکه‌های سازمانی است. این سرویس به ادمین‌های شبکه کمک می‌کند تا کامپیوترها، سرورها، و دستگاه‌های همراه (مانند لپ‌تاپ‌ها و تبلت‌ها) را به صورت متمرکز و یکپارچه مدیریت کنند.

ویژگی‌های کلیدی Endpoint Configuration Manager

- توزیع نرم‌افزار: این سرویس امکان نصب، به‌روزرسانی، و مدیریت نرم‌افزارها را در دستگاه‌های مختلف به صورت خودکار و از راه دور فراهم می‌کند. این قابلیت به ویژه در محیط‌های بزرگ بسیار مفید است، چرا که نیاز به نصب دستی نرم‌افزار را کاهش می‌دهد.
- مدیریت وصله‌ها و به‌روزرسانی‌ها: Configuration Manager می‌تواند به‌روزرسانی‌های امنیتی و وصله‌های جدید را به صورت خودکار به دستگاه‌ها اعمال کند. این ویژگی به امنیت شبکه کمک کرده و از بروز حملات و تهدیدهای امنیتی جلوگیری می‌کند.
- مدیریت دستگاه‌های همراه (MDM): با استفاده از این سرویس می‌توان دستگاه‌های همراه (مثل گوشی‌ها و تبلت‌ها) را نیز مدیریت کرد. این امکان به سازمان‌ها اجازه می‌دهد که دستگاه‌های کارکنان را از طریق قوانین خاص کنترل کنند، امنیت داده‌ها را حفظ کنند و حتی در صورت نیاز دستگاه‌ها را قفل یا پاک کنند.
- کنترل و نظارت بر تنظیمات سیستم‌ها: از طریق Endpoint Configuration Manager می‌توان تنظیمات مختلفی مثل پالیسی‌های امنیتی و پیکربندی شبکه را در تمامی سیستم‌ها اعمال کرد و از این طریق امنیت شبکه را تقویت کرد.
- مدیریت امنیتی و تنظیمات دسترسی: این سرویس امکان اعمال سیاست‌های امنیتی مانند مدیریت پالیسی‌های دسترسی و رمز عبور، رمزگذاری دیسک، و مدیریت سطح دسترسی کاربران را فراهم می‌آورد.
- گزارش‌دهی و تحلیل داده‌ها: Configuration Manager امکان ایجاد گزارش‌های دقیق از وضعیت دستگاه‌ها، به‌روزرسانی‌ها، و نرم‌افزارها را فراهم می‌کند. این گزارش‌ها به مدیران شبکه کمک می‌کند که به وضعیت کلی شبکه پی ببرند و مشکلات احتمالی را شناسایی کنند.

در ادامه کار می‌خواهیم نصب این سرویس را با هم بررسی کنیم و کار با آن را یاد بگیریم.

www.takbook.com

۱۱-٦ نصب نرم‌افزار Microsoft Endpoint Configuration Manager

برای نصب Microsoft Endpoint Configuration Manager به پیش‌نیازهایی در چندین حوزه نیاز است، شامل سخت‌افزار، سیستم‌عامل، پایگاه داده، و نرم‌افزارهای مرتبط. این موارد باید برای اطمینان از عملکرد صحیح و کارآمد این سرویس آماده باشند. در ادامه، نیازمندی‌های مختلف را شرح می‌دهم.

۱۱-٦-۱ نیازمندی‌های سخت‌افزاری

- پردازنده: حداقل پردازنده‌های چند هسته‌ای با قدرت پردازشی بالا (ترجیحاً Intel Xeon یا AMD EPYC برای سرورهای بزرگ).
- حافظه (RAM): حداقل ۸ گیگابایت رم توصیه می‌شود، اما برای سازمان‌های بزرگ ممکن است تا ۱٦ یا حتی ۳۲ گیگابایت رم نیاز باشد.
- فضای ذخیره‌سازی (Disk): بسته به حجم داده‌ها و تعداد دستگاه‌های تحت مدیریت، به حداقل ۲۰۰ گیگابایت فضای خالی نیاز است. در سازمان‌های بزرگ، استفاده از ذخیره‌سازی‌های سریع (مثل SSD) و حجیم توصیه می‌شود.
- کارت شبکه: نیازمند یک یا چند کارت شبکه با سرعت ۱ گیگابیت بر ثانیه یا بالاتر است.

۱۱-٦-۲ نیازمندی‌های نرم‌افزاری

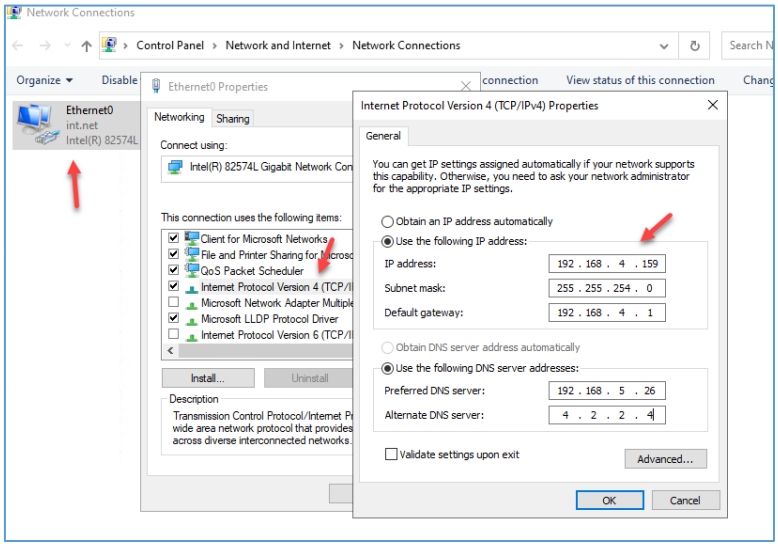
- سیستم‌عامل: ویندوز سرور ۲۰۱۹، ۲۰۲۲ یا ۲۰۲۵ برای سرور اصلی پیشنهاد می‌شود. این سیستم‌ها باید به‌روز باشند و تمام آپدیت‌های امنیتی نصب شده باشند.
- پایگاه داده: SQL Server نسخه‌های ۲۰۱۹، ۲۰۱۷ یا ۲۰۱٦ نیاز است. SQL Server Express برای محیط‌های کوچک قابل استفاده است، اما در محیط‌های بزرگ و سازمانی نسخه‌های Enterprise یا Standard توصیه می‌شوند.
- Microsoft .NET Framework: نیازمند نصب نسخه ٤.۸ یا بالاتر از .NET Framework است.
- Windows ADK: برای پیکربندی ویندوزهای کلاینت باید Windows Assessment and Deployment Kit (ADK) نصب شود. این ابزار برای عملیات دیپلوی و تصویرسازی نیاز است.
- Windows Server Update Services (WSUS): برای مدیریت به‌روزرسانی‌ها و وصله‌های امنیتی استفاده می‌شود.
- پیش‌نیازهای وابسته به IIS: نصب Internet Information Services (IIS) برای برخی از نقش‌های Configuration Manager مانند مدیریت کلاینت‌های تحت وب الزامی است.

www.takbook.com

۳-۶-۱۱ تنظیم سرور

سروری که برای این موضوع در نظر می‌گیریم یک ویندوز سرور ۲۰۲۵ روی آن نصب است که ۱۶ گیگابایت رم دارد و ۱۰۰ گیگ هارد دیسک که البته برای سازمان‌های بزرگ باید این مقدار را افزایش دهید تا در ادامه با مشکل روبرو نشوید.

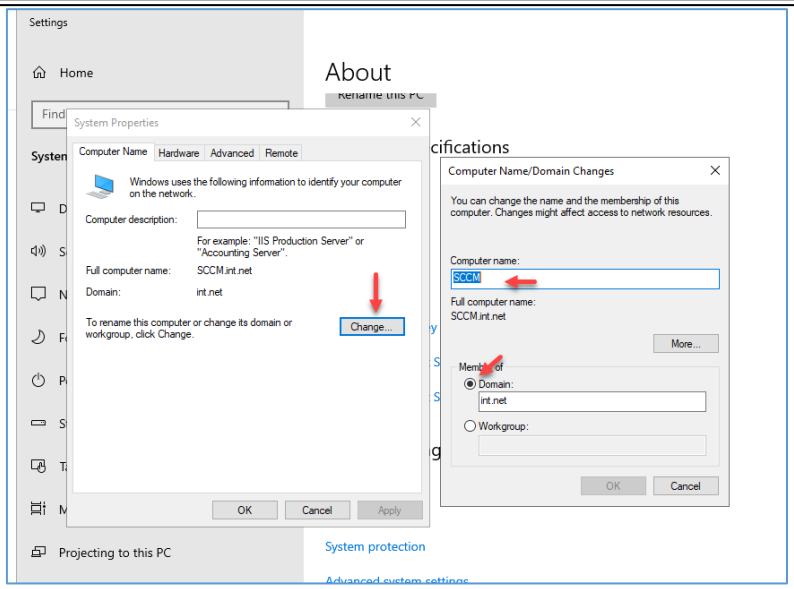
بعد از نصب ویندوز سرور وارد آن شوید و IP آدرس آن را به صورت دستی وارد کنید.



شکل ۱۱- ۹۴ تنظیم آدرس IP

در ادامه باید سرور مورد نظر عضو دومین کنید که به مانند شکل زیر این کار را انجام می‌دهیم.

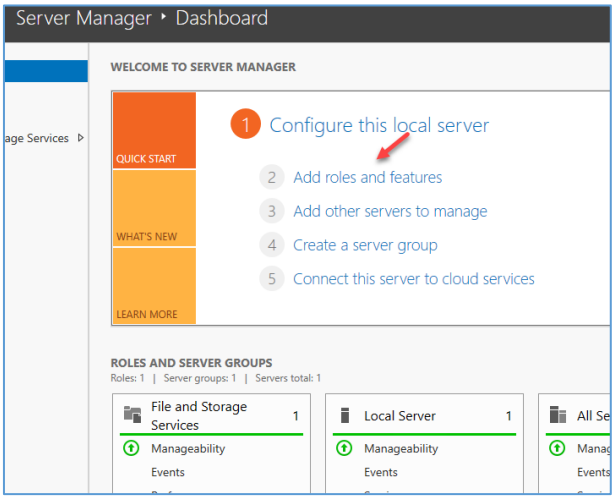
www.takbook.com



شکل ۱۱- ۹۵ تنظیم نام و عضو کردن در دومین

۱۱-٦-٤ نصب پیش‌نیازها

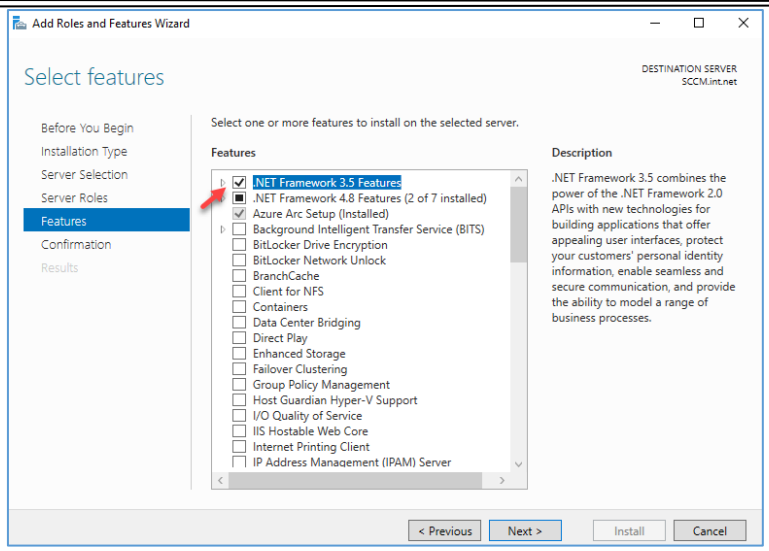
در ادامه کار باید سرویس .Net 3.5 را بر روی سرور نصب کنید، برای اینکار نیاز به DVD مربوط به ویندوز سروری دارید که بر روی سرور نصب کردید، وارد Server Manager شوید و بر روی Add roles and Features کلیک کنید.



شکل ۱۱- ۹۶ نصب پیش‌نیازها

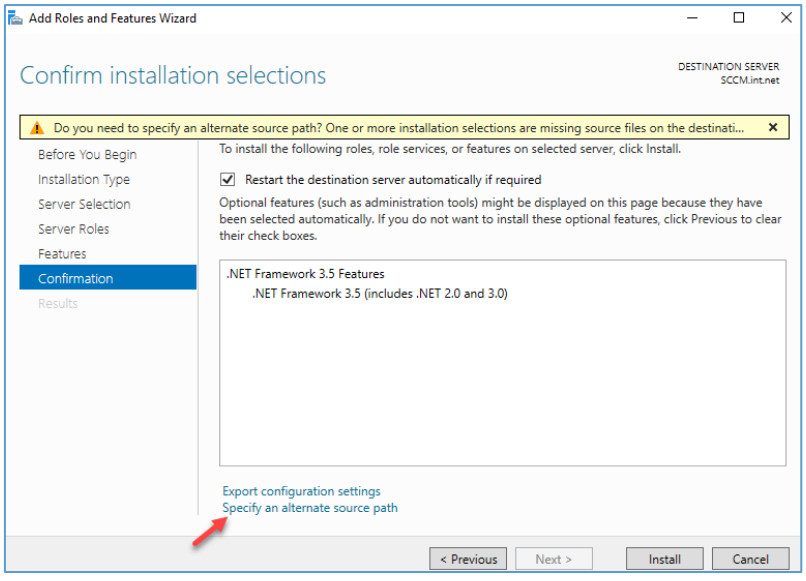
در شکل زیر از قسمت Features گزینه‌ی .NET Framework 3.5 را انتخاب کنید.

www.takbook.com



شکل ۱۱- ۹۷ نصب پیش‌نیازها

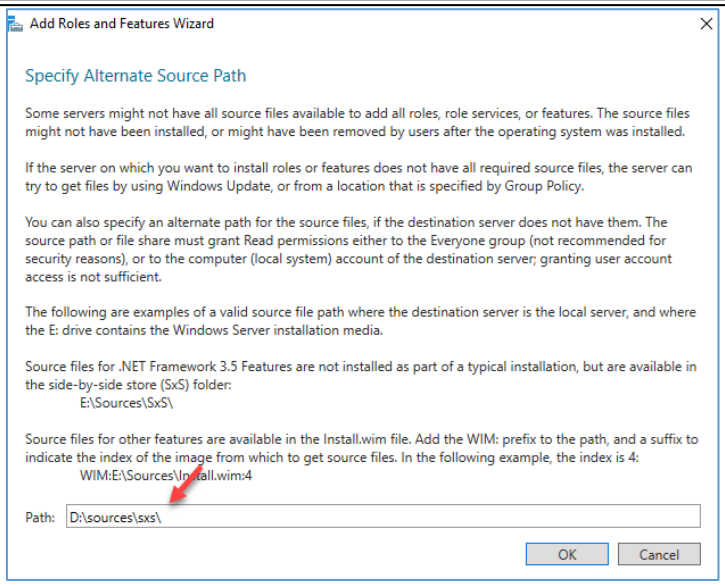
در شکل زیر بر روی Specify an alternate source path کلیک کنید.



شکل ۱۱- ۹۸ نصب پیش‌نیازها

در شکل زیر باید آدرس DVD ویندوز سرور 2025 را طبق شکل زیر وارد کنید.

www.takbook.com



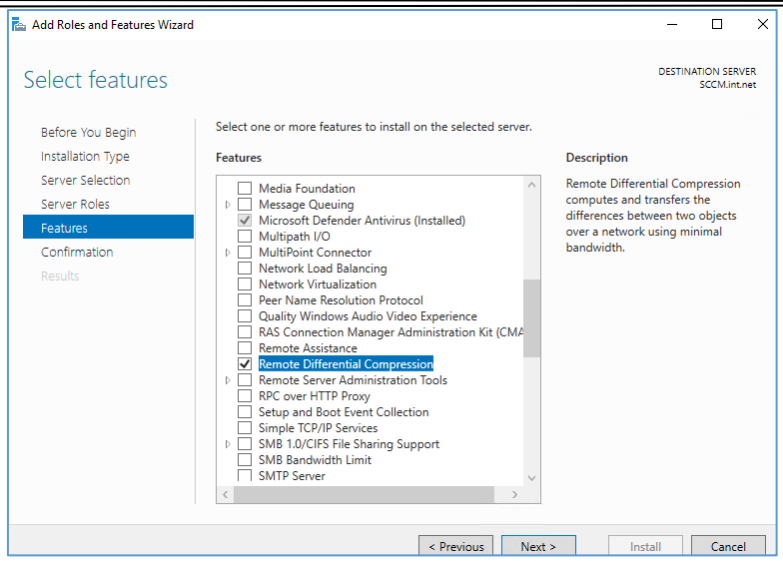
شکل ۱۱- ۹۹ نصب پیش‌نیازها

بعد از نصب .NET 3.5 باید دو پیش‌نیاز دیگر را نصب کنیم، یکی Remote Differential Compression که ویژگی Remote Differential Compression (RDC) در ویندوز سرور، یک فناوری برای بهینه‌سازی انتقال داده‌ها از طریق شبکه است. RDC این امکان را می‌دهد که فقط تغییرات اعمال‌شده بر روی فایل‌ها (به جای کل فایل) بین سیستم‌ها منتقل شوند. این فناوری برای شرایطی که پهنای باند محدود است یا فایل‌های بزرگ نیاز به همگام‌سازی دارند، بسیار مفید است.

به‌طور کلی، RDC با تجزیه فایل‌ها به بلوک‌های کوچک و محاسبه تفاوت‌های آن‌ها، فقط تغییرات مورد نیاز را منتقل می‌کند. از RDC به‌ویژه در سناریوهای همگام‌سازی فایل‌ها، پشتیبان‌گیری، و تکرار اطلاعات استفاده می‌شود، جایی که کوچک‌ترین تغییرات در داده‌ها باید به سرعت و با حداقل پهنای باند منتقل شوند.

برای نصب این ویژگی وارد Server Manager شوید و به مانند شکل زیر از قسمت Features گزینه‌ی مورد نظر را انتخاب و نصب کنید.

www.takbook.com



شکل ۱۱- ۱۰۰ نصب پیش‌نیازها

بعد از نصب باید نرم‌افزار Windows ADK را نصب کنیم، Windows ADK (Assessment and Deployment Kit) مجموعه‌ای از ابزارها و فناوری‌های مایکروسافت است که به مدیران سیستم و متخصصان IT کمک می‌کند تا سیستم‌عامل‌های ویندوز را در مقیاس بزرگ آماده‌سازی، پیکربندی و استقرار دهند.

Windows PE (Preinstallation Environment) یک محیط سبک ویندوز که به مدیران اجازه می‌دهد تا ویندوز را نصب، بازیابی یا عیب‌یابی کنند. معمولاً در مراحل اولیه نصب استفاده می‌شود.

برای دانلود باید وارد لینک زیر شوید:

https://learn.microsoft.com/en-us/windows-hardware/get-started/adk-install

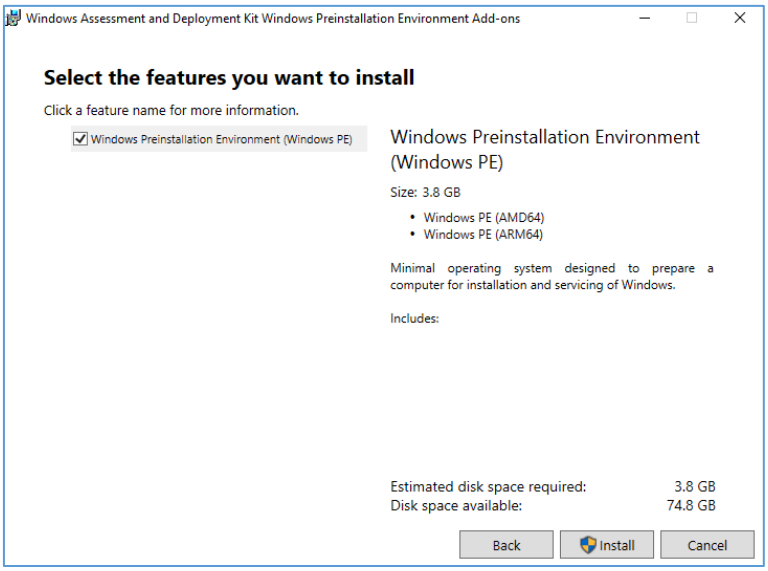
بعد از ورود به سایت به مانند شکل زیر هر دو نرم‌افزار را دانلود و نصب آن را انجام دهید، توجه داشته باشید برای نصب این نرم افزار نیاز به اینترنت در سرور دارید تا بتواند تمام ابزارهای لازم را دانولد و نصب کند.

www.takbook.com



شکل ۱۱- ۱۰۱ نصب پیش‌نیازها

همان‌طور که در شکل زیر مشاهده می‌کنید نرم‌افزار دانلود و آماده‌ی نصب است که نیاز به 3.8 گیگ فایل دارد که باید از اینترنت دانلود و بر روی سرور نصب شود.



شکل ۱۱- ۱۰۲ نصب پیش‌نیازها

۱۱-۶-۵ نصب SQL Server

برای اینکه نرم‌افزار Microsoft Endpoint را نصب کنیم نیاز به Database داریم که باید نرم‌افزار SQL Server 2025 را نصب کنیم که نیازی نیست دوباره در این قسمت نصب آن را انجام دهیم، دقیقاً به مانند قسمت قبلی این کار را انجام دهید.

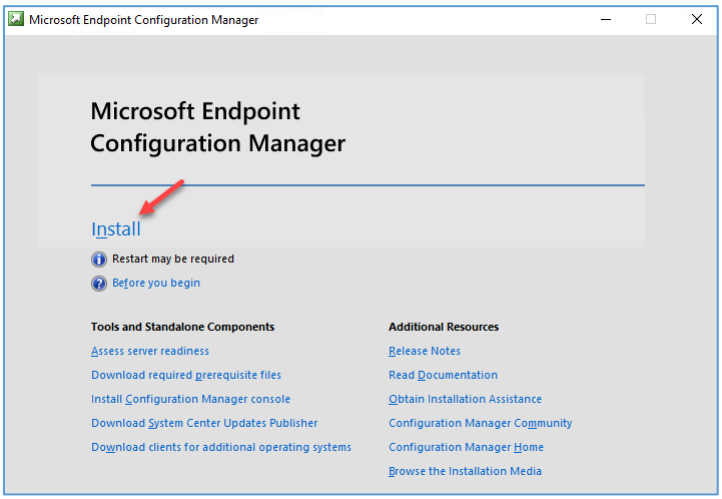
www.takbook.com

۷-۶-۱۱ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

بعد از نصب پیش‌نیازها باید نرم‌افزار اصلی را اجرا کنیم، برای دانلود نرم‌افزار Microsoft Endpoint باید به سایت مایکروسافت مراجعه کنید ولی برای راحتی کار شما یک سایت ایرانی برای این کار معرفی می‌کنم:

https://cdna.download.ir/dlir-software/Microsoft.System.Center.Configuration.Manager.2203.rar

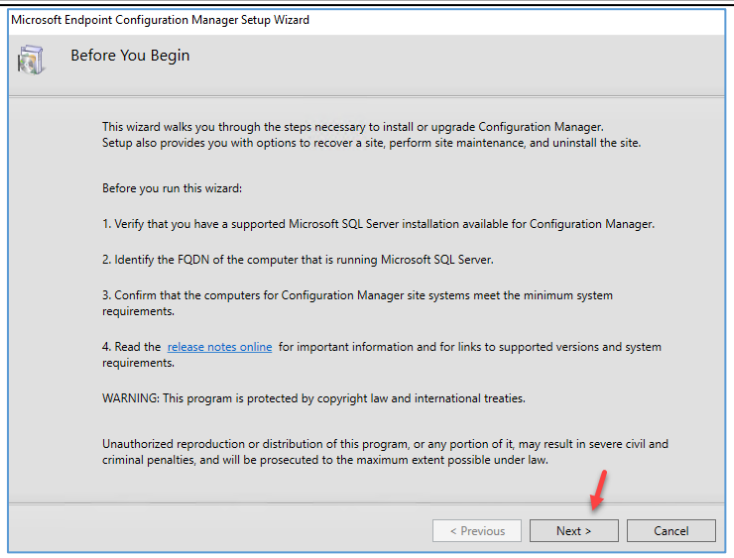
بر روی فایل Setup.exe کلیک کنید و در شکل باز شده بر روی Install کلیک کنید:



شکل ۱۱- ۱۰۳ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

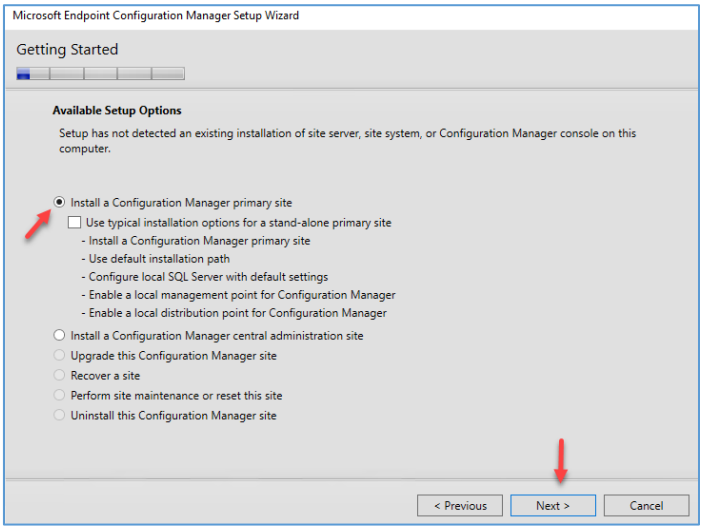
در شکل زیر پیش‌نیازهای مربوط به نرم‌افزار مشخص شده است.

www.takbook.com



شکل ۱۱- ۱۰۴ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

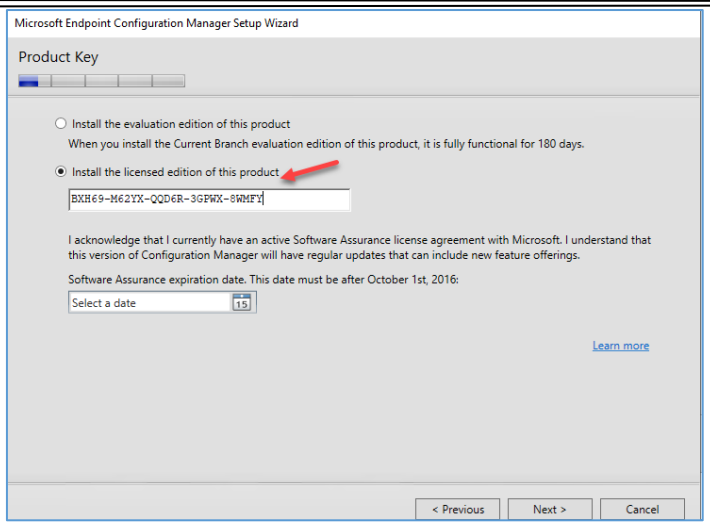
در شکل زیر برای راه‌اندازی کامل گزینه‌ی اول را انتخاب کنید.



شکل ۱۱- ۱۰۵

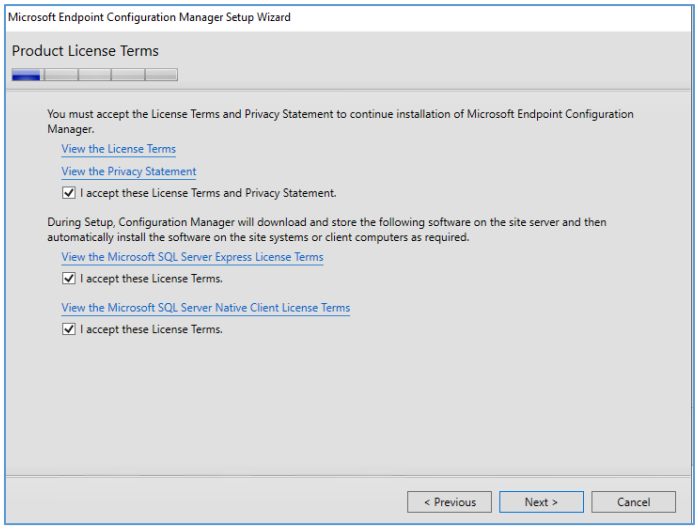
در این شکل باید لایسنس نرم‌افزار را وارد کنید.

www.takbook.com



شکل ۱۱- ۱۰۶ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

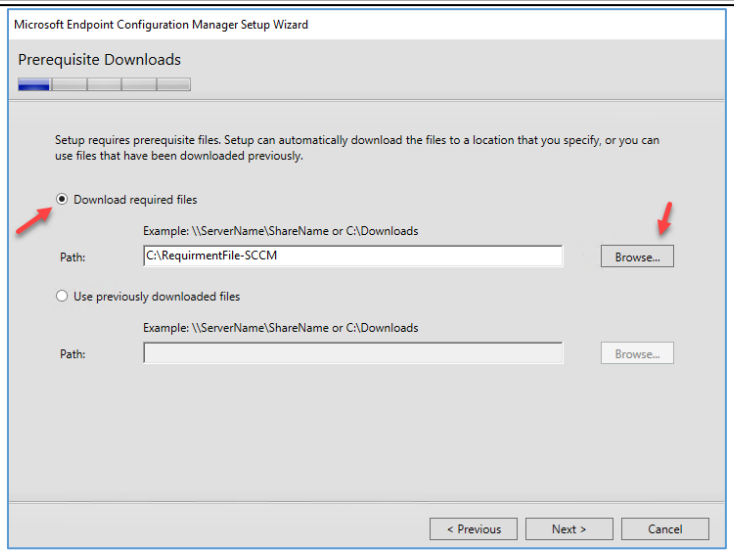
در شکل زیر توافقنامه را تایید و ادامه دهید.



شکل ۱۱- ۱۰۷ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

در شکل زیر باید یک سری فایل از اینترنت دانلود شوید که باید یک مسیر برای آن مشخص کنید که بعد از کلیک بر روی Next کار دانلود انجام می‌شود.

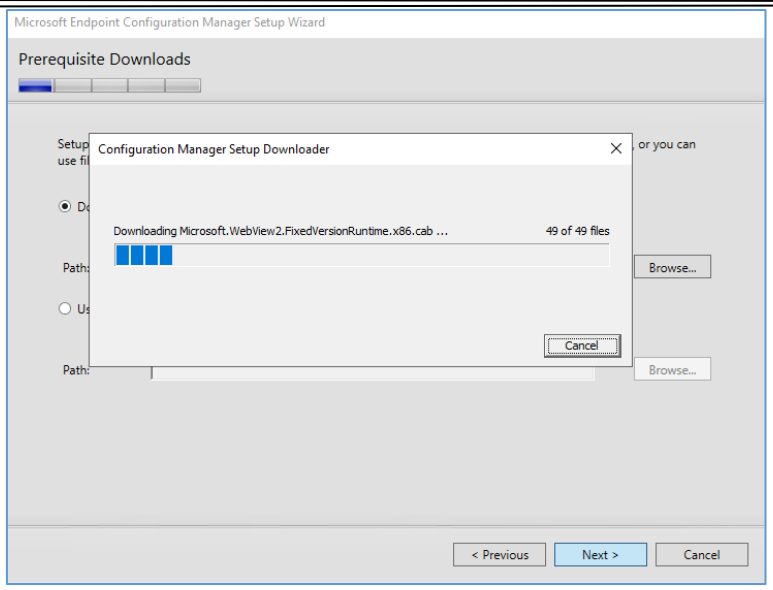
www.takbook.com



شکل ۱۱- ۱۰۸ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

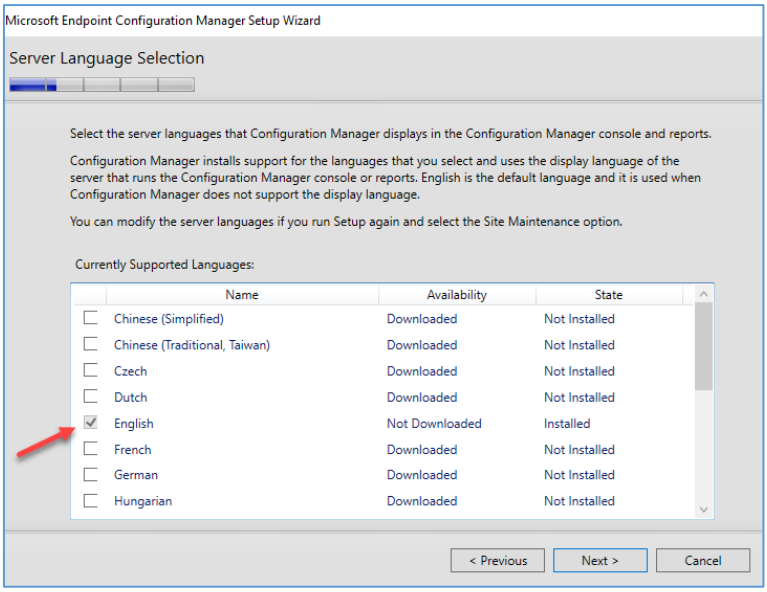
همان‌طور که مشاهده می‌کنید فایل مورد نظر دانلود و به اتمام رسیده است.

www.takbook.com



شکل ۱۱- ۱۰۹ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

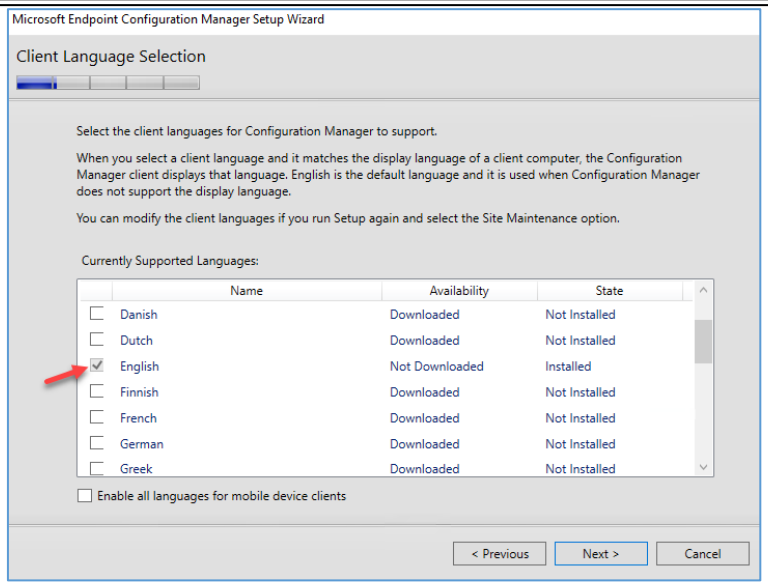
در شکل زیر باید زبان سرور را انتخاب کنید



شکل ۱۱- ۱۱۰ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

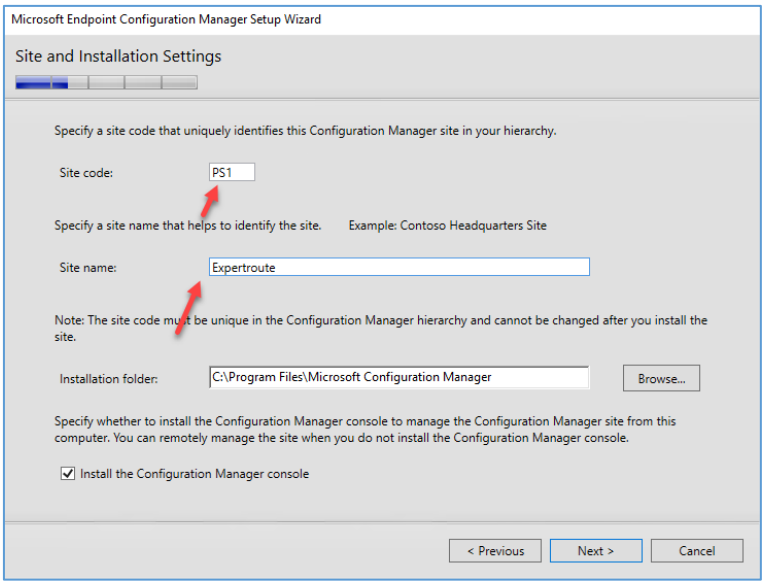
در شکل زیر باید زبان کاری کلاینت را انتخاب کنید.

www.takbook.com



شکل ۱۱- ۱۱۱ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

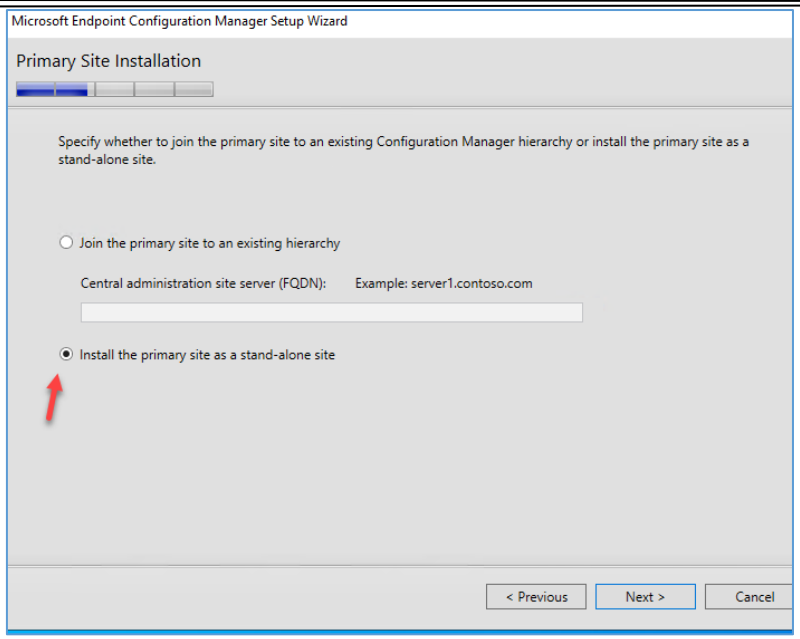
در شکل زیر باید یک کد برای سایت خود وارد کنید و در قسمت Site هم باید یک نام برای سایت خود وارد کنید و در آخر باید مسیر برای آن مشخص کنید.



شکل ۱۱- ۱۱۲ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

در این قسمت باید گزینه‌ی دوم را انتخاب کنید که تنظیمات بر روی همین سرور اعمال شود.

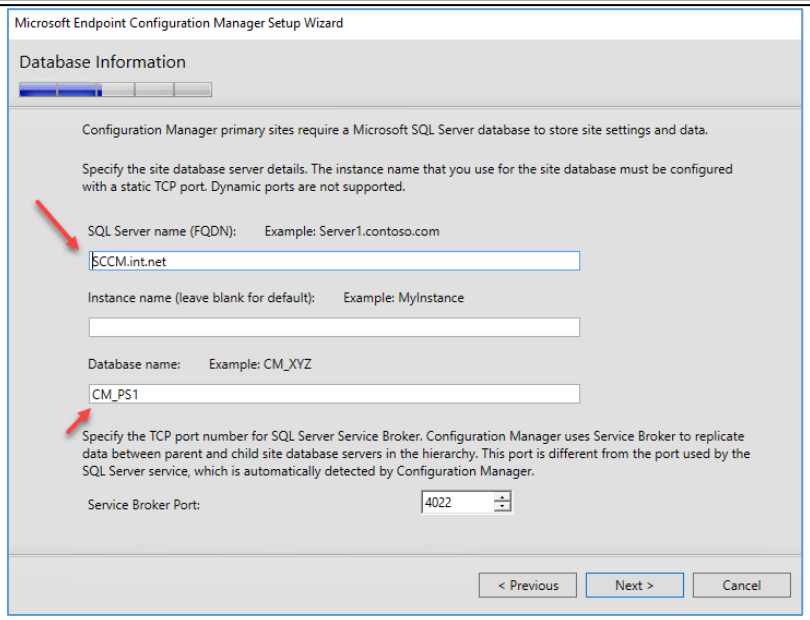
www.takbook.com



شکل ۱۱- ۱۱۳ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

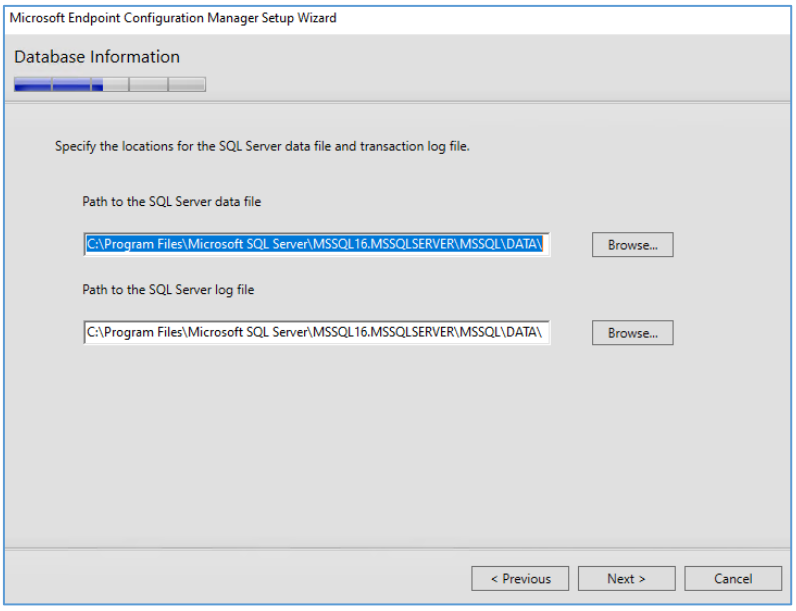
در شکل زیر باید آدرس سرور SQL که همین سرور است را وارد کنید، و نام دیتابیس را وارد کنید، توجه داشته باشید اگر از Instance استفاده کردید باید نام آن را در قسمت Instance name وارد کنید که برای این سرور چون به صورت پیش‌فرض SQL نصب شده نیازی به این کار نیست.

www.takbook.com



شکل ۱۱- ۱۱۴ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

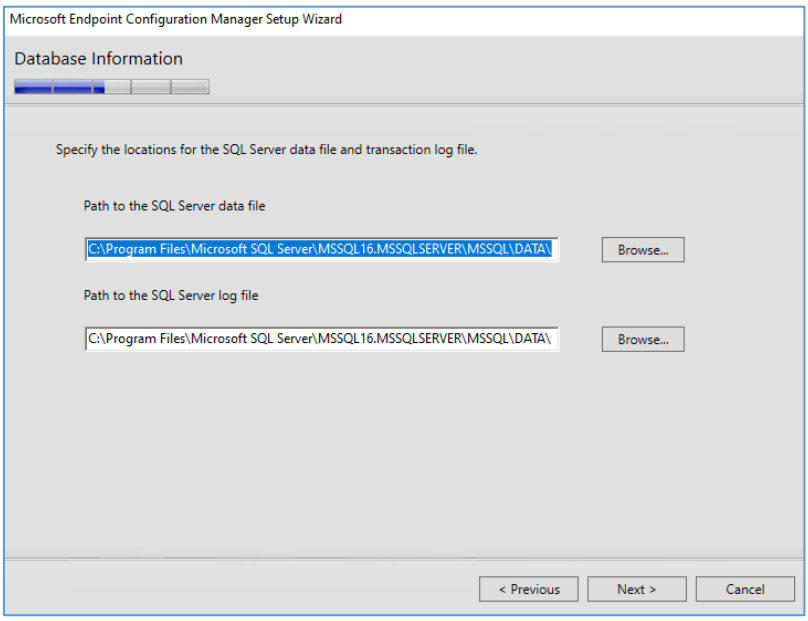
در شکل زیر باید مسیر ذخیره شدن فایل Database را مشخص کنید، یکی برای خود دیتابیس و دیگری برای Log.



شکل ۱۱- ۱۱۵ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

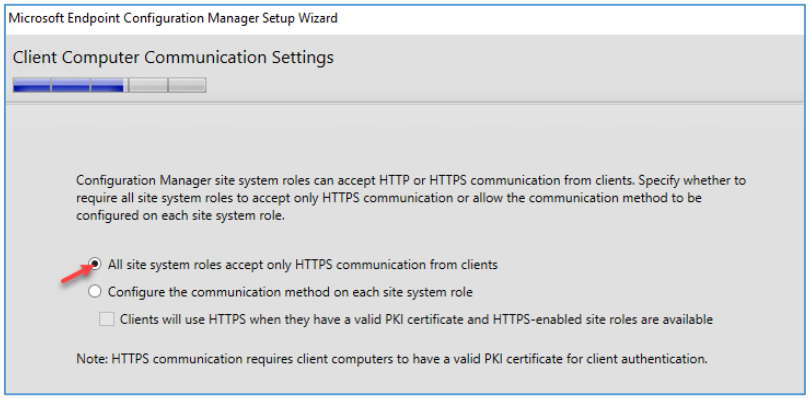
www.takbook.com

در شکل زیر نام سرور را وارد و بر روی Next کلیک کنید.



شکل ۱۱- ۱۱۶ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

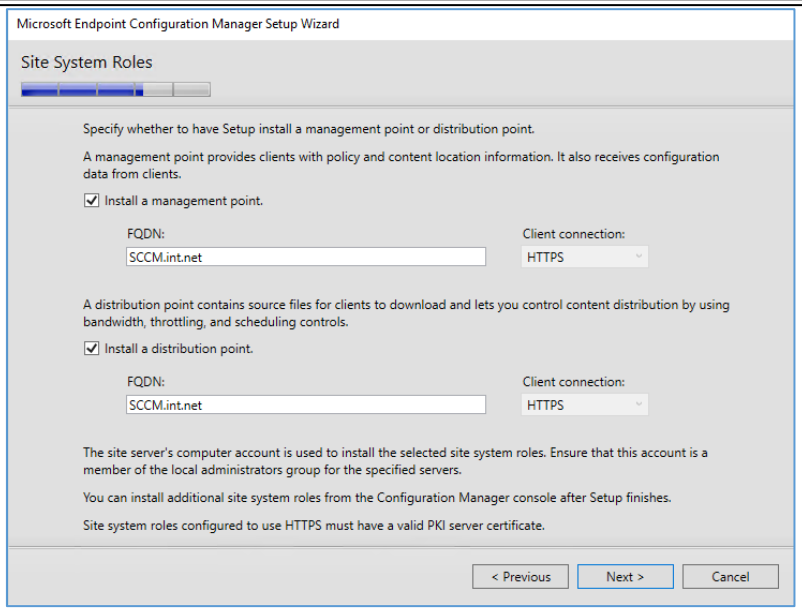
در شکل زیر باید گزینه‌ی اول را انتخاب کنید تا ارتباط به صورت HTTPS ایجاد شود.



شکل ۱۱- ۱۱۷ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

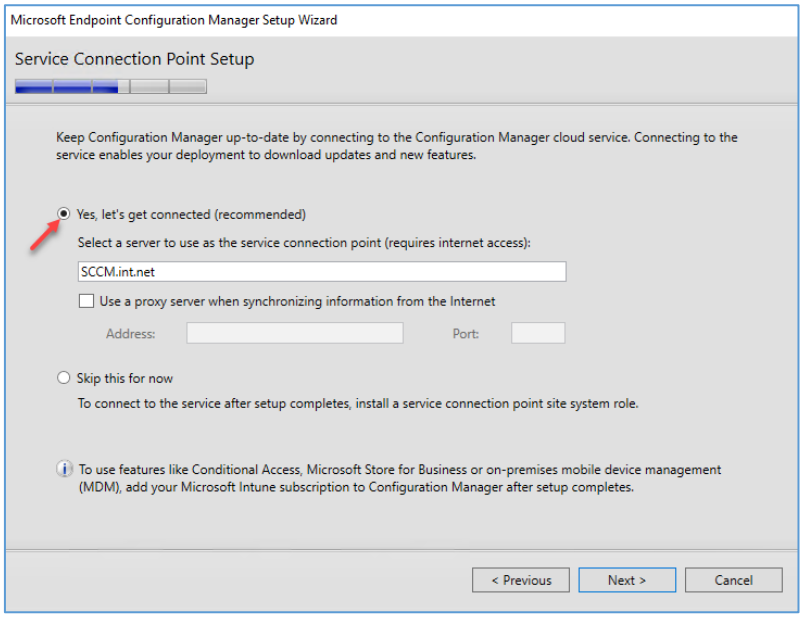
در شکل زیر بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۱- ۱۱۸ نصب و راه‌اندازی نرم‌افزار *Microsoft Endpoint*

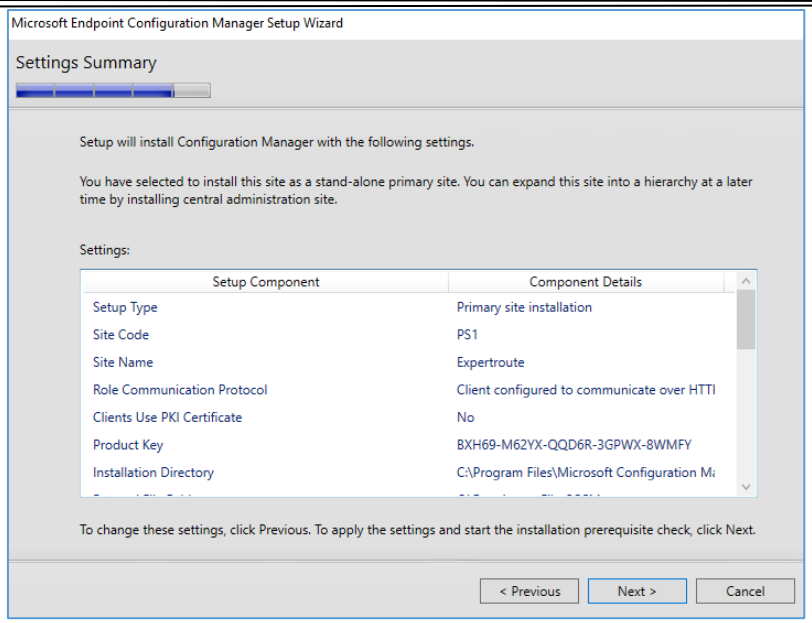
در شکل زیر بر روی Next کلیک کنید.



شکل ۱۱- ۱۱۹ نصب و راه‌اندازی نرم‌افزار *Microsoft Endpoint*

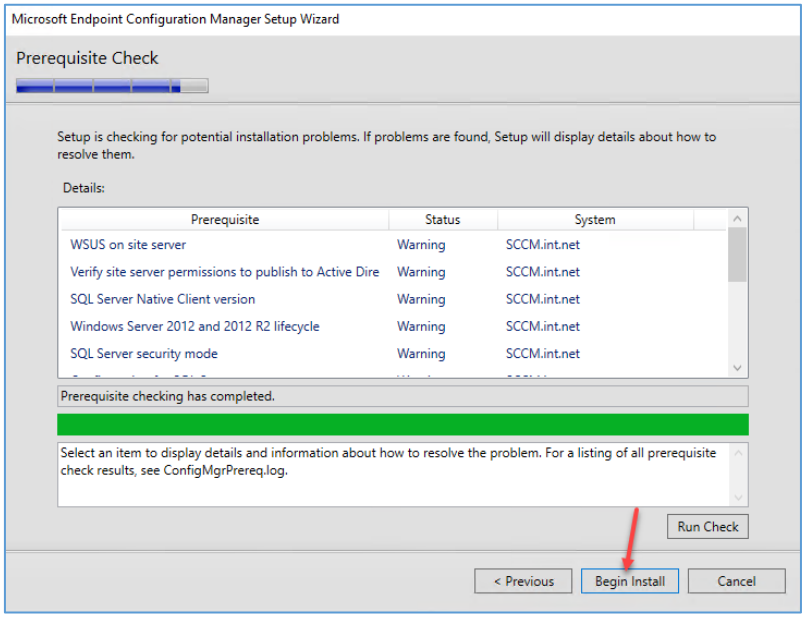
تنظیمات نهایی را در شکل زیر مشاهده می‌کنید، بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۱- ۱۲۰ نصب و راه‌اندازی نرم‌افزار *Microsoft Endpoint*

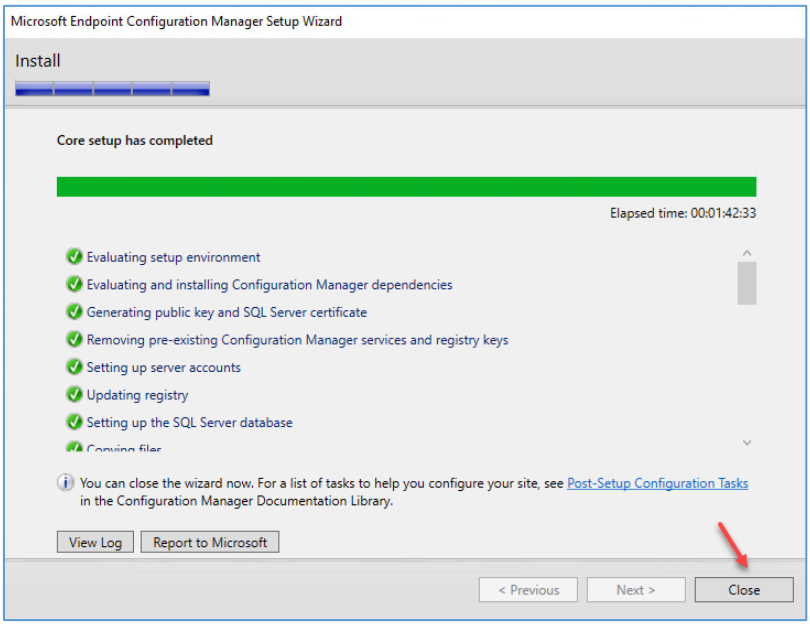
در شکل زیر تمام پیش‌نیازها بررسی شده و اگر یکی از آنها نصب نباشد نمی‌توانید کار نصب را انجام دهید، به مانند شکل زیر بر روی Begin Install کلیک کنید تا کار نصب آغاز شود.



شکل ۱۱- ۱۲۱ نصب و راه‌اندازی نرم‌افزار *Microsoft Endpoint*

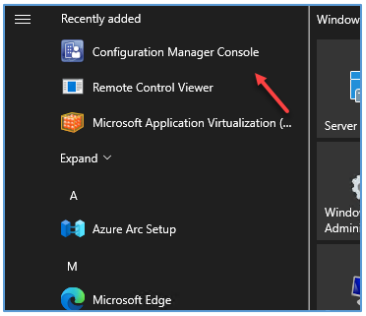
www.takbook.com

هماطور که مشاهده می‌کنید با موفقیت نصب انجام شده است.



شکل ۱۱- ۱۲۲ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

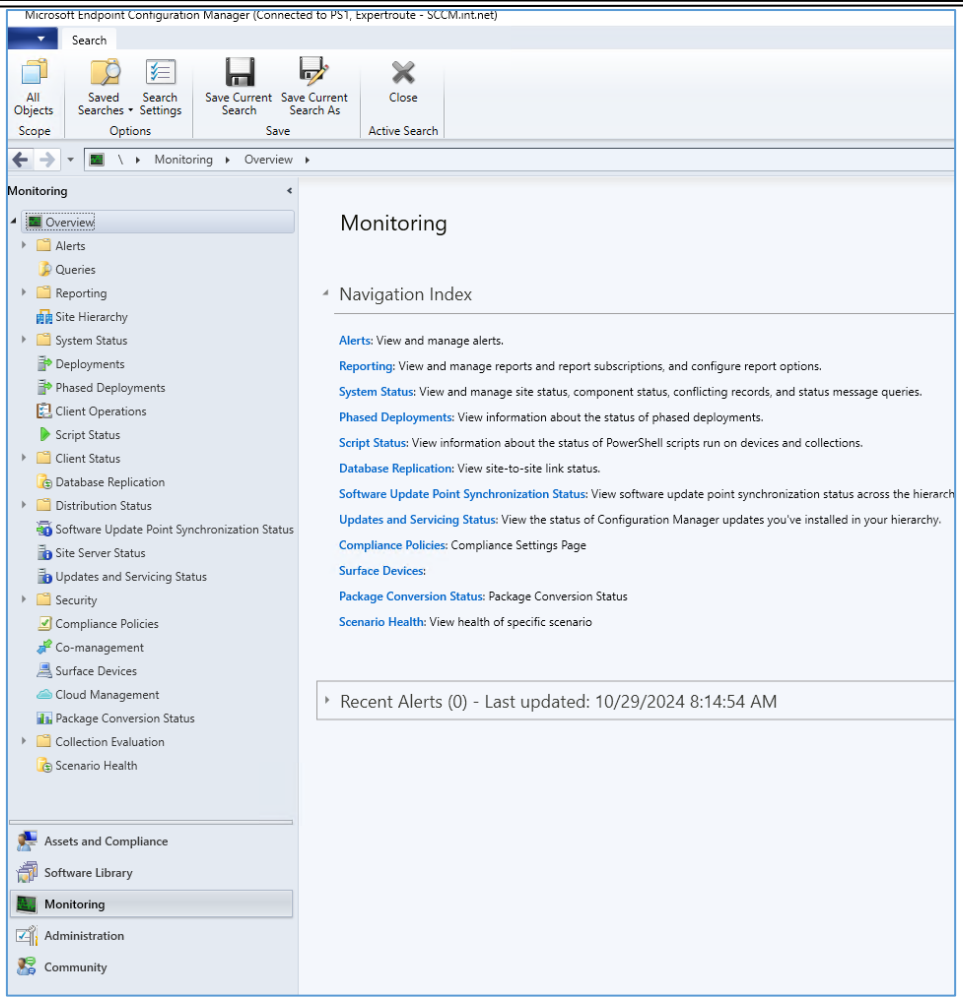
بعد از نصب بر روی Start کلیک کنید و نرم‌افزار Configuration Manager Console را اجرا کنید.



شکل ۱۱- ۱۲۳ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

همان‌طور که در شکل زیر مشاهده می‌کنید نرم‌افزار مورد نظر با موفقیت نصب شده است و اگر به سمت چپ آن دقت کنید قسمت‌های مختلفی برای کارهای مختلف را مشاهده می‌کنید که در صورت نیاز همه آنها را توضیح خواهیم داد.

www.takbook.com



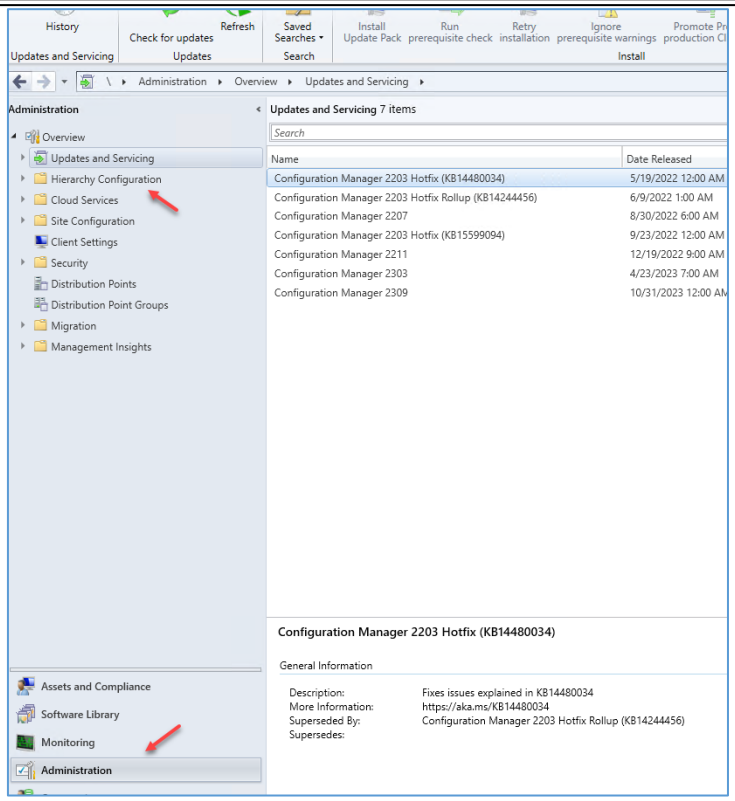
شکل ۱۱- ۱۲۴ نصب و راه‌اندازی نرم‌افزار Microsoft Endpoint

۸-۶-۱۱ بررسی روش Discovery در Endpoint

بعد از نصب موفقیت‌آمیز نرم‌افزار Endpoint حالا می‌خواهیم با استفاده از روش Discovery کاربران، سیستم‌ها، شبکه‌ها و ... را در سازمان خود بررسی کنیم و آنها را به نرم‌افزار اضافه کنیم.

برای شروع به مانند شکل زیر وارد قسمت Administation شوید و بر روی Hierarchy Configuration کلیک کنید.

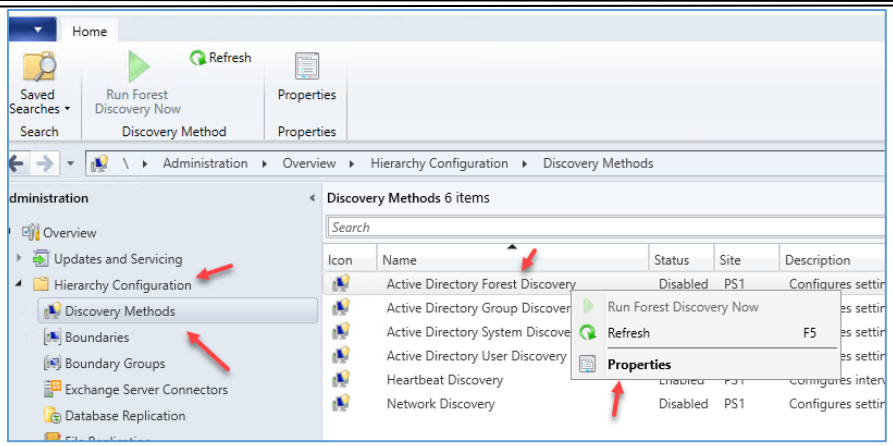
www.takbook.com



شکل ۱۱- ۱۲۵ بررسی روش Discovery

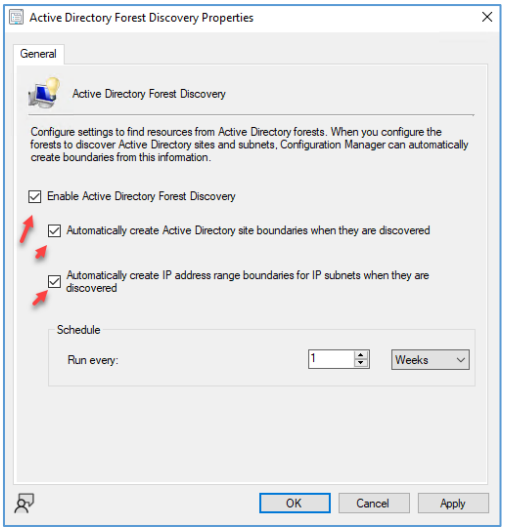
به مانند شکل زیر در زیر مجموعه‌ی Hierarchy Configuration گزینه‌ی discovery Methods را انتخاب کنید و در صفحه‌ی که باز می‌شود چند گزینه را مشاهده می‌کنید، بر روی Active Directory Forest Discovery کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.

www.takbook.com



شکل ۱۱- ۱۲۶ بررسی روش Discovery

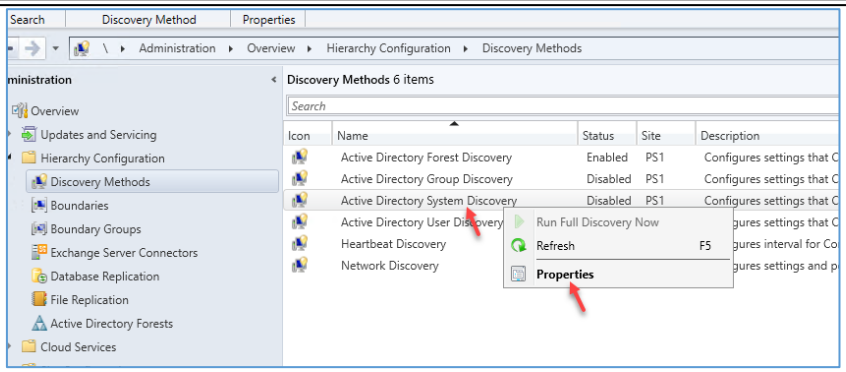
به مانند شکل زیر باید گزینه‌های مورد نظر را انتخاب کنید تا سرویس Discovery فعال شود.



شکل ۱۱- ۱۲۷ بررسی روش Discovery

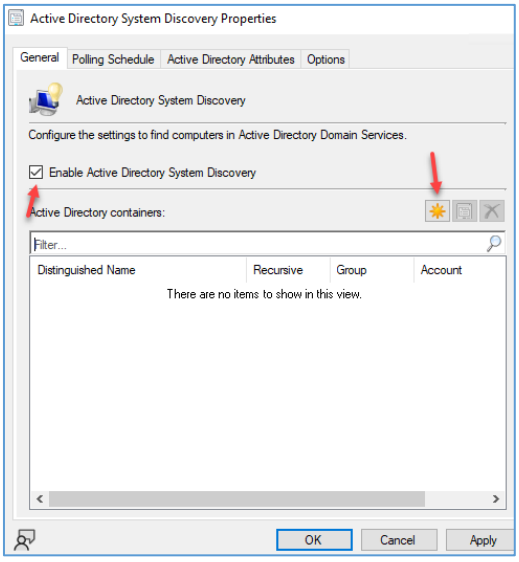
گزینه‌ی بعدی که باید فعال کنیم سیستم‌های داخل سازمان شما هستش که باید Discovery شویند، برای این کاربر روی Active Directory System Discovery کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.

www.takbook.com



شکل ۱۱- ۱۲۸ بررسی روش *Discovery*

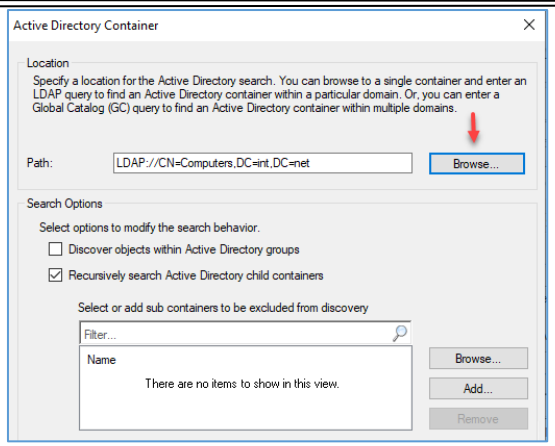
در شکل زیر تیک مورد نظر را انتخاب کنید تا سرویس فعال شود و برای اینکه دقیق مشخص کنیم که سیستم‌های در Active Dircetory در کدام OU قرار دارند بر روی آیکون ستاره کلیک کنید.



شکل ۱۱- ۱۲۹ بررسی روش *Discovery*

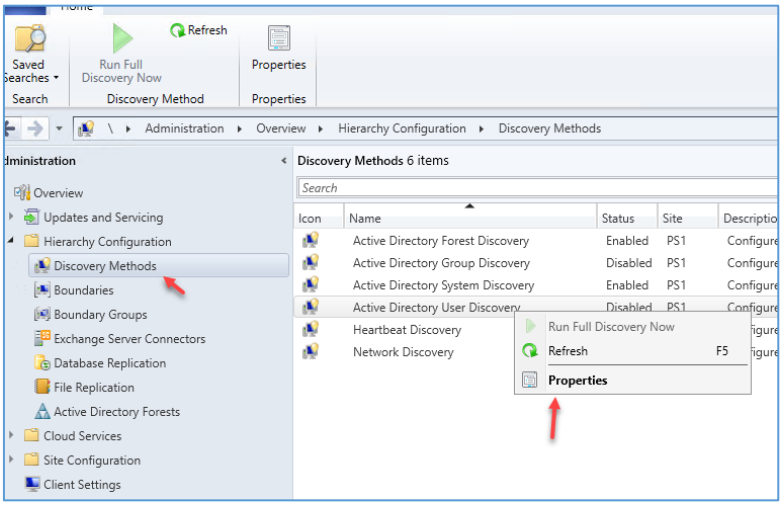
به مانند شکل زیر بر روی Browse کلیک کنید و OU مورد نظر را انتخاب کنید که به صورت پیش‌فرض باید قسمت Computers در Active Directory را انتخاب کنید.

www.takbook.com



شکل ۱۱- ۱۳۰ بررسی روش Discovery

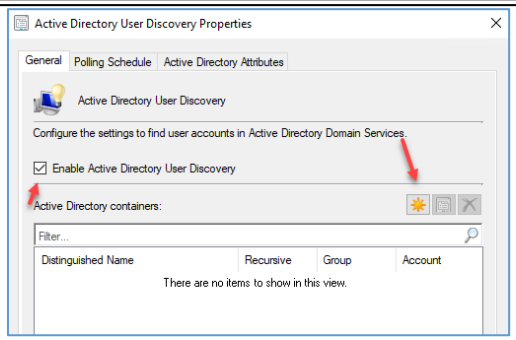
شما می‌توانید کاربران را هم در Active directory جستجو کنید که برای این کار باید به مانند شکل زیر بر روی Active Directory User Discovery کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۱۱- ۱۳۱ بررسی روش Discovery

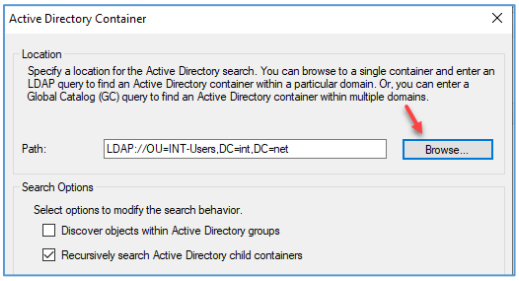
در شکل زیر تیک گزینه‌ی Enable را انتخاب کنید و بر روی ستاره کلیک کنید.

www.takbook.com



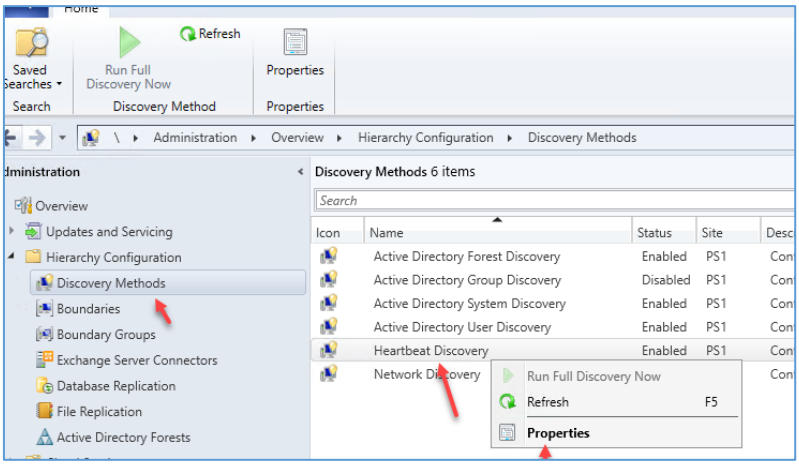
شکل ۱۱- ۱۳۲ بررسی روش Discovery

در شکل زیر بر روی Browse کلیک کنید و OU مربوط به کاربران را انتخاب کنیدو بر روی OK کلیک کنید.



شکل ۱۱- ۱۳۳ بررسی روش Discovery

گزینه‌ی دیگری با عنوان Heartbeat Discovery وجود دارد که یک روش کشف و به‌روزرسانی اطلاعات مربوط به دستگاه‌های کلاینت موجود در شبکه است. این مکانیزم به Configuration Manager کمک می‌کند تا حضور دستگاه‌های کلاینت را در پایگاه داده تأیید و اطلاعات آن‌ها را به‌روز نگه دارد، بر روی آن کلیک راست و گزینه‌ی Properties را انتخاب کنید.

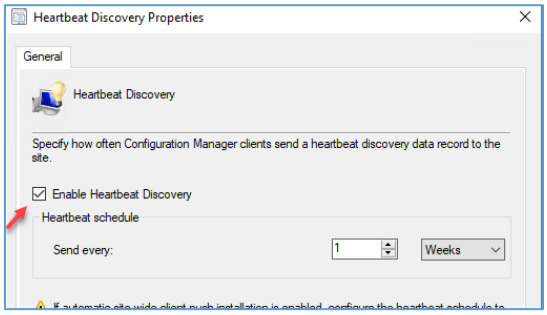


شکل ۱۱- ۱۳۴ بررسی روش Discovery

www.takbook.com

در شکل زیر تیک گزینه‌ی Enable را انتخاب کنید تا سرویس فعال شود، توجه داشته باشید زمان‌بندی سرویس Heartbeat Discovery در Microsoft Endpoint Configuration Manager به‌گونه‌ای تنظیم شده که دستگاه‌های کلاینت در فواصل منظم یک پیام Heartbeat به سرور ارسال کنند. این فاصله زمانی می‌تواند توسط مدیر شبکه تعیین شود تا متناسب با نیازهای شبکه و ترافیک سیستم تنظیم گردد.

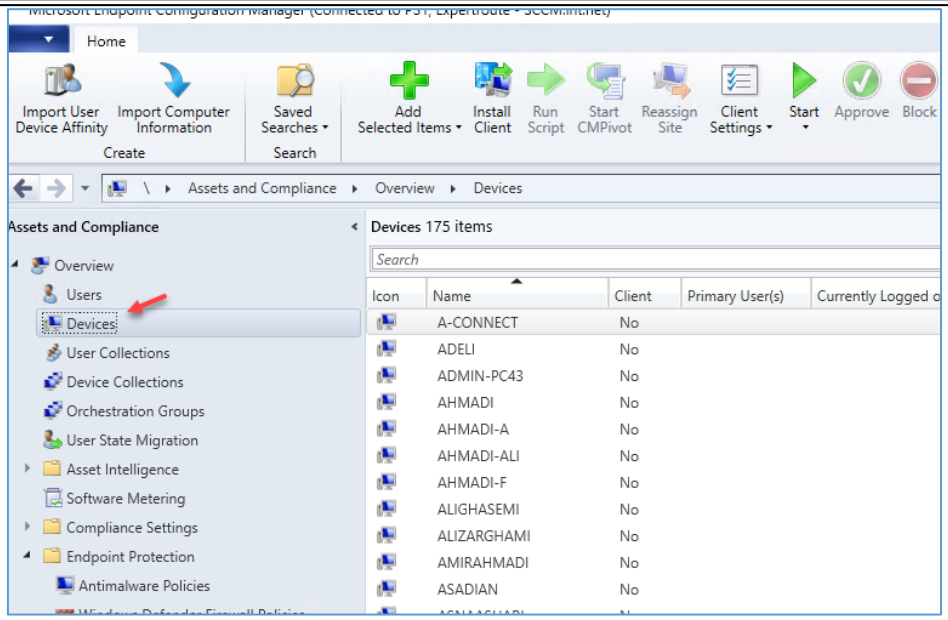
به‌طور پیش‌فرض، این زمان‌بندی هر ۷ روز است، اما مدیر می‌تواند آن را تغییر دهد تا به‌روزرسانی وضعیت کلاینت‌ها سریع‌تر یا کندتر انجام شود.
زمان‌بندی کوتاه‌تر (مثلاً روزانه) باعث می‌شود اطلاعات دستگاه‌ها سریع‌تر به‌روز شوند، اما ممکن است ترافیک شبکه را افزایش دهد.
زمان‌بندی طولانی‌تر (مثلاً دو هفته یکبار) ترافیک شبکه را کاهش می‌دهد، اما اطلاعات کمتری از وضعیت دستگاه‌های کلاینت در دسترس خواهد بود.



شکل ۱۱- ۱۳۵ بررسی روش Discovery

حالا برای اینکه ببنیم تنظیمات ما به درستی عمل کرده باید به مانند شکل زیر و از قسمت Assets and Compliance وارد Devices یا Users شوید که تمام اطلاعاتی که در Active Directory است را مشاهده خواهید کرد.

www.takbook.com



شکل ۱۱- ۱۳۶ بررسی روش Discovery

www.takbook.com

www.takbook.com

فصل دوازدهم

VMware VCenter Sever

به عنوان مدیر شبکه مدیریت کردن چندین سرور ESXi به صورت جدا از هم کار بسیار دشواری خواهد بود و همیشه باید یک مسیر درست برای مدیریت آنها پیدا کنید.
نرم‌افزاری که در این فصل می‌خواهیم مورد بررسی قرار دهیم، نرم‌افزار VMware Vcenter Server است که در دو نسخه ویندوزی و لینوکسی مورد استفاده قرار می‌گیرید، در مورد این نسخه‌ها در زیر توضیحاتی را ارائه می‌دهیم.

VMware vCenter Server یک پلتفرم مدیریت مرکزی برای محیط‌های مجازی‌سازی شده با استفاده از VMware vSphere است. این نرم‌افزار امکان مدیریت هاست‌های ESXi، ماشین‌های مجازی (VMs)، منابع و کلاسترها را به صورت متمرکز فراهم می‌کند. vCenter Server ابزارهای پیشرفته‌ای برای مدیریت، اتوماسیون، مانیتورینگ و مقیاس‌پذیری زیرساخت مجازی ارائه می‌دهد.

ویژگی‌ها و قابلیت‌های vCenter Server

۱. مدیریت متمرکز:
vCenter Server به شما امکان می‌دهد تا تعداد زیادی هاست و ماشین مجازی را از طریق یک پنل مدیریتی واحد مدیریت کنید. این امکان به مدیران کمک می‌کند تا به راحتی منابع خود را کنترل و پیکربندی کنند، ماشین‌های مجازی را مانیتور کنند و عملیات مختلف را اجرا کنند.

۲. کلاسترینگ و مدیریت منابع:
High Availability (HA): این قابلیت در vCenter Server به شما اجازه می‌دهد تا با ایجاد کلاستر، دسترس‌پذیری ماشین‌های مجازی را تضمین کنید. در صورت خرابی یک هاست، ماشین‌های مجازی به صورت خودکار بر روی هاست‌های دیگر راه‌اندازی می‌شوند.
Distributed Resource Scheduler (DRS): DRS به مدیریت خودکار منابع پردازشی (مانند CPU و RAM) در بین ماشین‌های مجازی کمک می‌کند و با توزیع بار کاری بین هاست‌های مختلف، عملکرد بهینه را تضمین می‌کند.
۳. vMotion:

www.takbook.com

vMotion یکی از قابلیت‌های کلیدی vCenter Server است که به شما امکان می‌دهد تا ماشین‌های مجازی را بدون نیاز به توقف، به هاست‌های مختلف منتقل کنید. این ویژگی کمک می‌کند که تعادل بار بهینه حفظ شود و در عین حال کاربران بدون وقفه به سرویس‌های خود دسترسی داشته باشند.

٤. Storage vMotion:

این قابلیت به شما اجازه می‌دهد که دیسک‌های ماشین مجازی را بین datastoreهای مختلف جابجا کنید بدون اینکه ماشین مجازی نیاز به خاموشی یا وقفه داشته باشد. این ویژگی برای مدیریت و بهینه‌سازی منابع ذخیره‌سازی بسیار مفید است.

٥. Snapshots و Backup:

vCenter Server به شما اجازه می‌دهد تا snapshots از ماشین‌های مجازی بگیرید، که این snapshots به عنوان نسخه‌های پشتیبان قابل استفاده هستند. همچنین می‌توان از راه‌حل‌های پشتیبانی مانند VMware vSphere Data Protection برای تهیه نسخه پشتیبان منظم استفاده کرد.

٦. مانیتورینگ و گزارش‌دهی:

vCenter Server ابزارهایی برای مانیتورینگ منابع، ماشین‌های مجازی و هاست‌ها ارائه می‌دهد. می‌توانید نمودارهای عملکرد، گزارش‌های لاگ و هشدارها را مشاهده کنید تا از سلامت زیرساخت خود مطمئن شوید و به مشکلات احتمالی پاسخ دهید.

۷. پیکربندی خودکار و اتوماسیون:

vCenter Server از طریق ابزارهایی مانند vSphere Auto Deploy و Host Profiles امکان پیکربندی خودکار و یکپارچه‌سازی هاست‌ها را فراهم می‌کند. این ابزارها به مدیران اجازه می‌دهند تا به سرعت هاست‌های جدید را به کلاستر اضافه کنند و تنظیمات استاندارد را به صورت خودکار اعمال کنند.

۸. Role-Based Access Control (RBAC):

با استفاده از RBAC در vCenter Server می‌توانید مجوزهای مختلفی به کاربران اختصاص دهید. این امکان به شما کمک می‌کند تا سطح دسترسی کاربران را بر اساس نیاز آن‌ها محدود یا گسترش دهید.

۹. Content Library:

www.takbook.com

Content Library در vCenter Server به شما اجازه می‌دهد که الگوها (templates)، فایل‌های ISO، و دیگر فایل‌های مرتبط با ماشین‌های مجازی را به صورت مرکزی مدیریت کنید و آن‌ها را بین چندین هاست یا کلاستر به اشتراک بگذارید.

۱۰. Integrated Solutions:

vCenter Server به راحتی با سایر محصولات VMware و راه‌حل‌های جانبی مانند NSX (شبکه مجازی‌سازی)، vSAN (ذخیره‌سازی مجازی‌سازی)، و vRealize Operations ادغام می‌شود. این ادغام‌ها به شما امکان می‌دهد تا مدیریت شبکه، ذخیره‌سازی و بهینه‌سازی منابع را به طور کامل و جامع انجام دهید.

معماری vCenter Server:

vCenter Server معمولاً به دو روش قابل پیاده‌سازی است:

vCenter Server Appliance (VCSA):

نسخه لینوکسی مبتنی بر Photon OS که توسط VMware توسعه یافته است. این نسخه به دلیل بهره‌وری بیشتر و کاهش پیچیدگی نسبت به نسخه ویندوزی ترجیح داده می‌شود.

vCenter Server روی Windows:

نسخه‌ای که بر روی ویندوز نصب می‌شود. این نسخه در نسخه‌های اخیر کمتر مورد استفاده قرار می‌گیرد و VMware بیشتر تمرکز خود را روی VCSA گذاشته است.

مزایای vCenter Server:

مدیریت کارآمد و متمرکز: vCenter Server امکان مدیریت چندین هاست ESXi و هزاران ماشین مجازی را از یک نقطه فراهم می‌کند.

افزایش بهره‌وری: با استفاده از قابلیت‌هایی مثل vMotion، DRS و HA، ماشین‌های مجازی به طور خودکار بهینه‌سازی می‌شوند و خرابی‌ها کاهش می‌یابند.

کاهش هزینه‌ها: با استفاده از اتوماسیون و کاهش نیاز به دخالت دستی، هزینه‌های عملیاتی کاهش پیدا می‌کند.

امنیت بالا: با استفاده از RBAC، امکان کنترل دقیق دسترسی کاربران به منابع فراهم می‌شود.

نسخه VMware Vcenter Appliance

همان‌طور که بیان کردیم این نسخه از Vcenter به صورت یک پکیج آماده لینوکسی می‌باشد و به صورت ماشین مجازی بر روی ESXi یا دیگر مجازی‌سازها نصب می‌شود.

www.takbook.com

VMware Vcenter Appliance یا VCSA ابزارهای مختلفی را برای نظارت بر روی سرورهای مختلف VMware در اختیار شما قرار می‌دهد

در جدول زیر حداکثر تعداد سرورها، ماشین‌ها و... که VCSA پستیبانی می‌کند مشخص شده است:

جدول ۱۲- ۱ پشتیبانی سخت افزار

1000	Hosts (with embedded vPostgres database)
15,000	Virtual machines (with embedded vPostgres database)
1000	Hosts (with Oracle database)
15,000	Virtual machines (with Oracle database)

در جدول بالا تعداد Hosts که در Vcenter ورژن لینوکسی یا همان Appliance پشتیبانی می‌شود تعداد ۱۰۰۰ مورد است که رقم بالایی می‌باشد و تعداد ماشین‌های مجازی هم ۱۵۰۰۰ ماشین است.
البته به این نکته توجه کنید که VCSA از دو دیتابیس برای کارهای خود استفاده می‌کند که یکی دیتابیس vPostgres و دیگری Oracle است که هر کدام از آنها اگر استفاده شوند تعداد Host و ماشین‌های مجازی آنها در لیست مشخص شده است.

مزیت VCSA یا Vcenter Appliance این است که برای جاهای بسیار بزرگ با Host های زیاد مورد استفاده قرار می‌گیرد، در این کتاب هم همین نسخه را مورد بررسی قرار می‌دهیم.
برای دانلود نسخه VMware Vcenter Appliance (VCSA) از لینک زیر استفاده کنید:

https://www.digiboy.ir/11064/vmware-vsphere-8-0/

۱۲-۱ منابع مورد نیاز برای راه‌اندازی VMware Vcenter Appliance

همان‌طور که گفتیم نسخه VCSA یا همان نسخه آماده که تحت سیستم عامل لینوکس است به صورت مجازی بر روی یک Hypervisior مانند ESXi راه‌اندازی می‌شود و مانند نسخه ویندوزی آن به صورت فیزیکی بر روی سرور نصب نخواهد شد.

مجوز استفاده از نرم‌افزار

برای استفاده از این نرم‌افزار باید سریال آن را خریداری کنید، که البته در ایران متاسفانه همه چیز کرک می‌شود، برای اینکه حداکثر کارایی VCSA را دریافت کنید، باید از دو نسخه (سریال) زیر استفاده کنید:

- vSphere Enterprise Plus
- vSphere Remote Office Branch Office (ROBO)

www.takbook.com

نسخه vSphere Enterprise Plus می‌توانند اکثر نیازهای شما را برآورده کند.

زیر ساخت مورد نیاز

برای راه‌اندازی Vcenter به منابع سخت‌افزاری زیر که البته روی یک سیستم‌عامل دیگر اجرا می‌شود نیاز است:

۱- حداقل باید یک CPU با دو هسته را برای این ماشین در نظر بگیرید تا Vcenter توانایی اجرا داشته باشند.

۲- حداقل رم مورد نیاز ۸ گیگابایت باشد تا مشکلی در اجرا پیش نیاید.

۳- حداقل هارد دیسک هم ۸۰ گیگابایت باید در نظر گرفت.

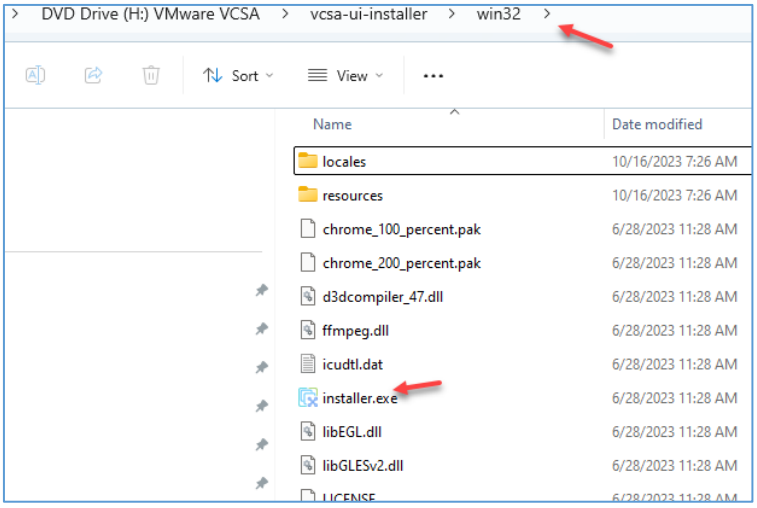
تنظیمات فایروال برای Vcenter

برای اینکه ماشین Vcenter ما در ESXi به درستی کار کند باید به پورت خروجی ۲۳۷۷ و پورت ورودی ٤٤۳ اجازه عبور داد که البته این تنظیمات در زمان ایجاد ماشین VCSA یا همان Vcenter Appliance انجام خواهد شد و نیاز به تنظیم دوباره ان نیست.

برای ارتباط Vcenter نیاز به کارت شبکه است که در موقع تنظیم آن به ماشین اختصاص داده خواهد شد.

۱۲-۲ نصب VMware Vcenter Appliance

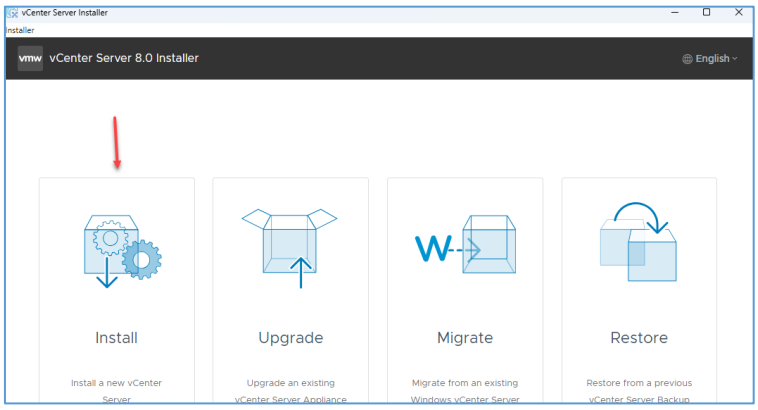
در این قسمت می‌خواهیم کار نصب VMware Vcenter Appliance را آغاز کنیم، با توجه به لینکی که در اختیار شما قرار دادیم بعد از دانلود به مانند شکل ۱۲-۱، وارد آدرس مورد نظر شوید و فایل Installer.exe را با دسترسی Admin اجرا کنید.



شکل ۱۲- ۱ نصب *VMware Vcenter Appliance*

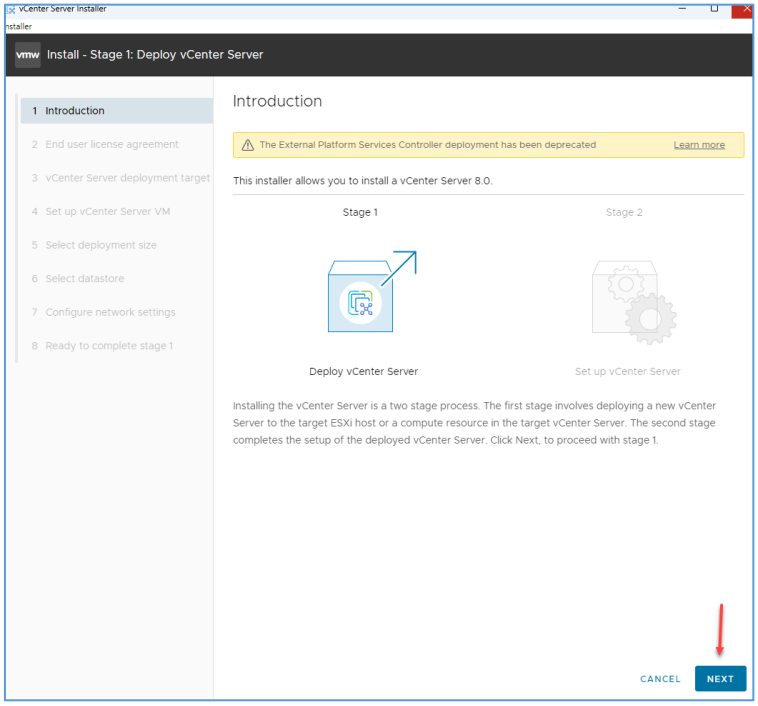
www.takbook.com

در شکل۱۲-۲، چهار گزینه را مشاهده می‌کنید که گزینه‌ی Install برای نصب اولیه مورد استفاده قرار می‌گیرد گزینه‌ی Upgrade برای ارتقاء نسخه Vcenter appliance است و Migrate هم برای تغییر نسخه لینوکسی Vcenter به ویندوزی است و در آخر گزینه‌ی Restore برای برگرداندن پشتبانی که از قبل تهیه کردید، در حال حاضر بر روی گزینه‌ی install کلیک کنید.



شکل ۱۲- ۲ نصب *VMware Vcenter Appliance*

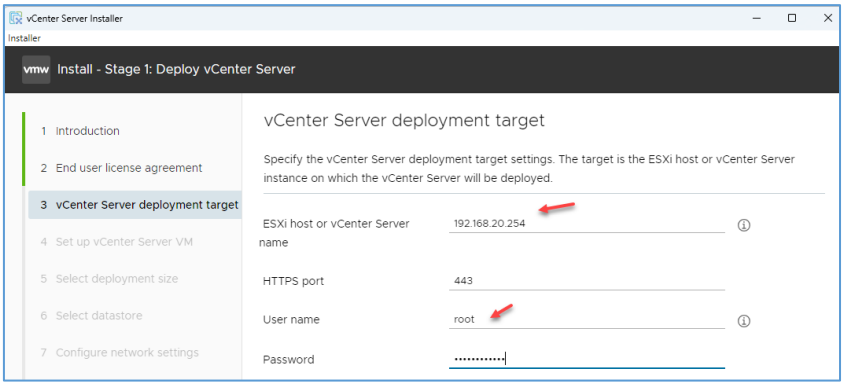
در شکل ۱۲-۳، برای آغاز ایجاد و راه‌اندازی VCSA بر روی Next کلیک کنید.



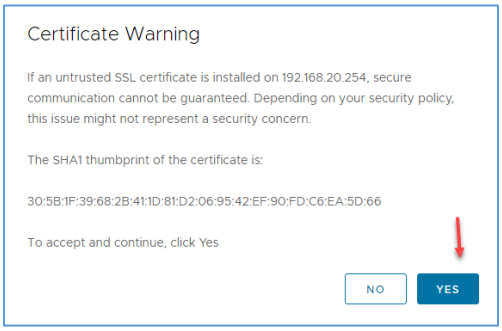
شکل ۱۲- ۳ نصب *VMware Vcenter Appliance*

www.takbook.com

در شکل ۱۲-٤، باید آدرس سرور ESXi که با هم راه‌اندازی کردیم را وارد کنید و بعد از آن پورت ارتباطی٤٤۳ را در صورت تغییر ندادن وارد و نام کاربری و رمز عبور آن را هم وارد کنید، بعد از کلیک بر روی Next به مانند شکل ۱۲-٥، صفحه Certificate ظاهر می‌شود که بر روی Yes کلیک کنید.

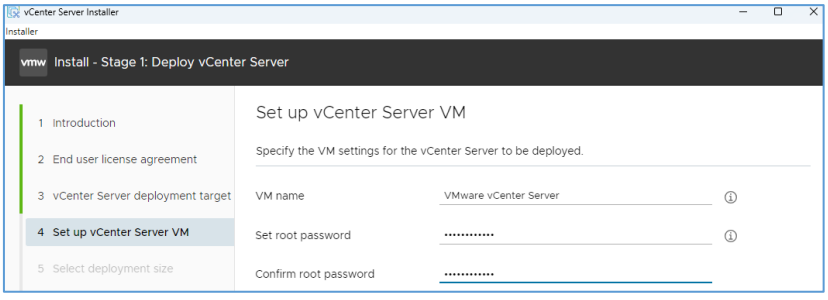


شکل ۱۲- ۴ نصب *VMware Vcenter Appliance*



شکل ۱۲- ۵ نصب *VMware Vcenter Appliance*

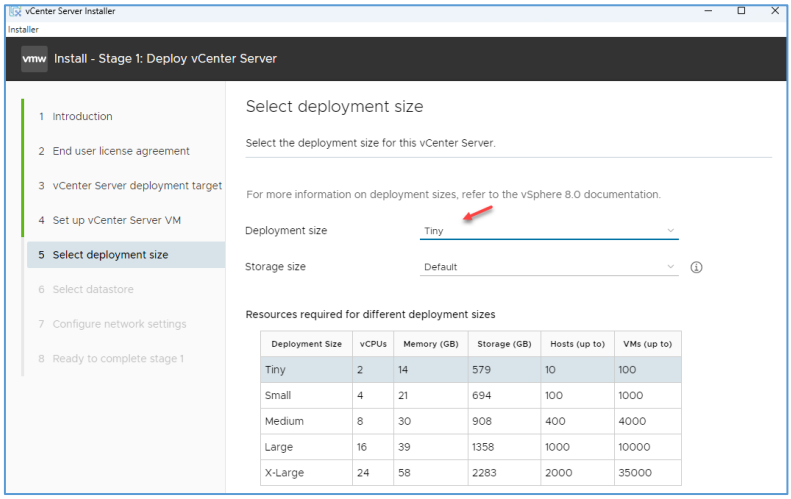
به مانند شکل ۱۲-٦، باید نام ماشین به همراه رمز عبور Root که برای ورود به Vcenter کاربرد دارد را وارد و بر روی Next کلیک کنید، سعی کنید از رمز عبور پیچیده برای حفظ امنیت سرور استفاده کنید.



شکل ۱۲- ۶ نصب *VMware Vcenter Appliance*

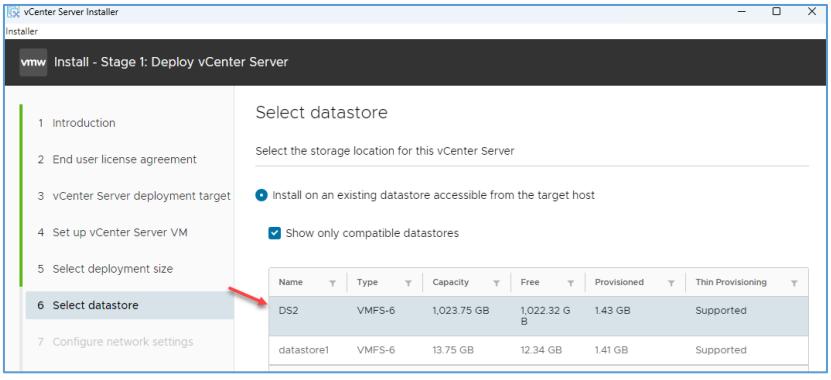
www.takbook.com

در شکل ۱۲-۷، باید به نسبت ظرفیت سازمان خود یکی از گزینه‌ها را از لیست انتخاب کنید، مثلاً اگر گزینه‌ی Tinyرا از منوی کشویی انتخاب کنید لیست زیری آن آپدیت می‌شود و مشخص می‌شود که حداقل تعداد هسته CPU باید ۲ باشد، مقدار مناسب رم باید ۱۰ گیگابایت باشد، و مقدار فضای پیشنهادی ۳۰۰ گیگابایت است، تعداد هاست و ماشین مجازی آماده به کار هم به ترتیب ۱۰ و ۱۰۰ است که می‌تواند برای سازمان‌های کوچک که تا ۱۰۰ کاربر دارند مناسب باشد.



شکل ۱۲- ۷ نصب *VMware Vcenter Appliance*

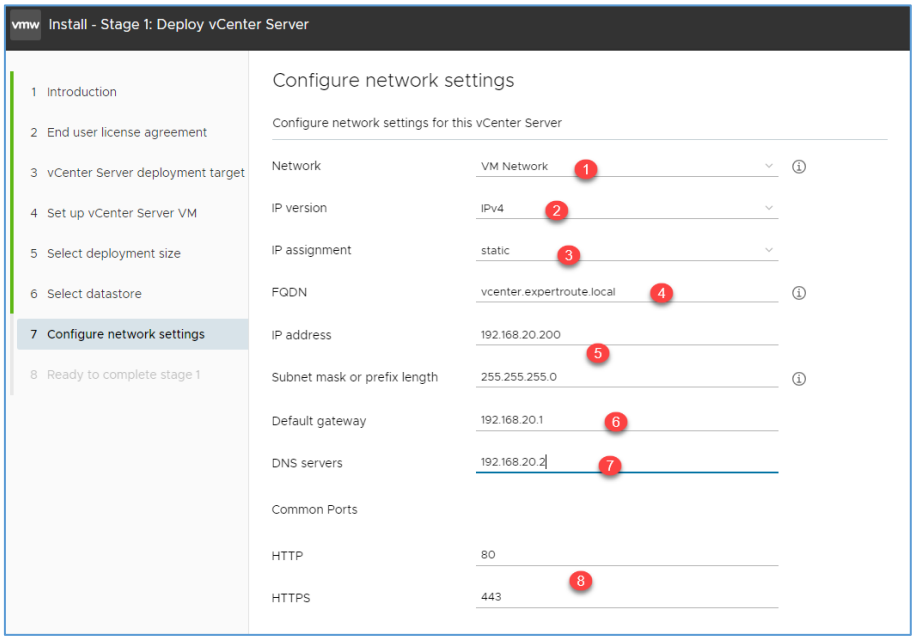
در شکل ۱۲-۸، باید DataStore مورد نظر خود را که فضای کافی دارد را انتخاب کنید، اگر هم مقدار فضا کافی نیست تیک گزینه‌ی Enable Thin Disk Mode را انتخاب کنید، با انتخاب این گزینه اگر مقدار فضای هارد دیسک کمتر از ۳۰۰ گیگابایت (طبق جدول) باشد Vcenter بر روی آن نصب خواهد شد ولی پیشنهاد این است که سعی کنید مقدار فضای مورد نیاز را برای Vcenter فراهم کنید تا در ادامه با مشکل مواجه نشوید.



شکل ۱۲- ۸ نصب *VMware Vcenter Appliance*

www.takbook.com

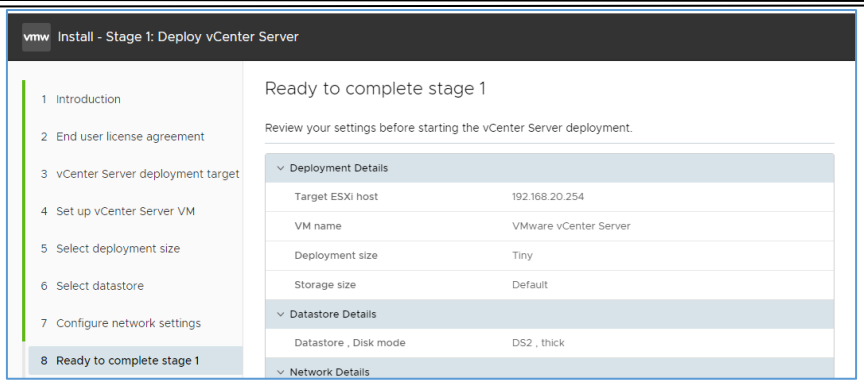
در شکل ۱۲-۹، باید تنظیمات کارت شبکه را انجام دهید، در قسمت شماره‌ی یک، کارت شبکه مورد نظر خود را انتخاب کنید، در قسمت شماره‌ی دو نوع پروتکل IP را انتخاب کنید، در قسمت شماره‌ی سه آدرس IP از نوع دستی یا اتوماتیک را انتخاب کنید، در قسمت شماره‌ی چهار، آدرس FQDN سرور یا همان نام آن را وارد کنید، توجه داشته باشید که این نام باید در سرویس DNS شبکه تعریف شود، در قسمت شماره‌ی پنج باید آدرس IP و Subnet آن را وارد کنید، در قسمت شماره‌ی شش در صورت داشتن Default Gateway مثلاً مودم اینترنت آدرس آن را وارد کنید در قسمت شماره‌ی هفت باید آدرس سرور DNS را وارد کنید و در آخر هم باید پورت‌های ارتباطی که به صورت پیش‌فرض ۸۰ و ٤٤۳ است را تنظیم کنید و بر روی Next کلیک کنید.



شکل ۱۲- ۹ نصب *VMware Vcenter Appliance*

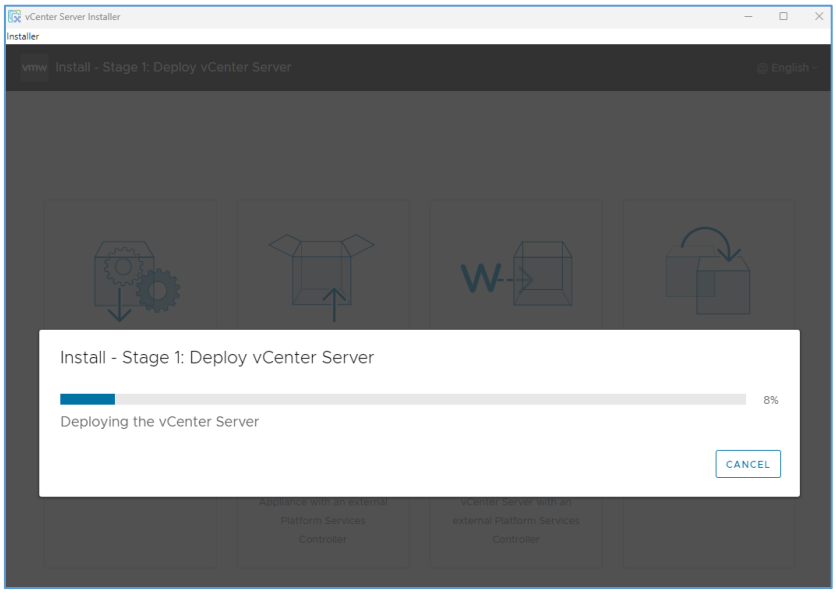
در شکل ۱۲-۱۰، تنظیماتی که انجام دادید را بررسی کنید و در صورت تایید بر روی Finish کلیک کنید تا کار Deploy کردن Vcenter Server آغاز شود.

www.takbook.com



شکل ۱۲- ۱۰ نصب *VMware Vcenter Appliance*

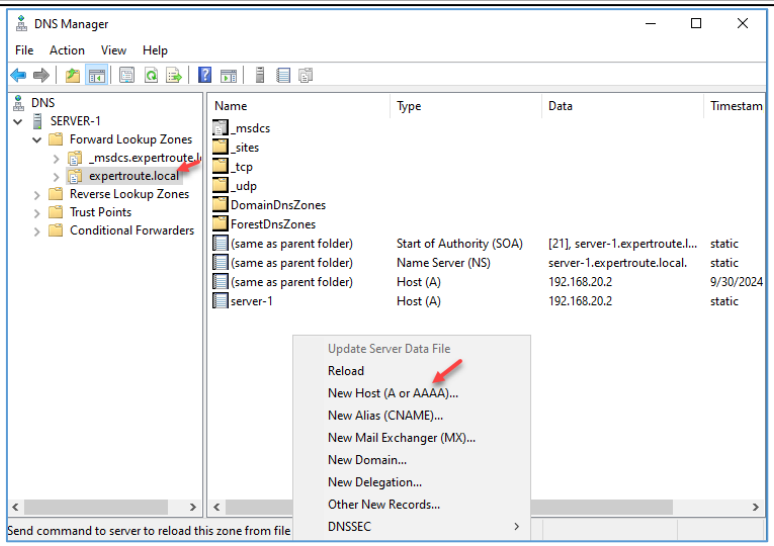
همان‌طور که در شکل ۱۲-۱۱، مشاهده می‌کنید نرم‌افزار Vcenter در حال Deploy شدن است و برای اینکه تنظیمات DNS را برای نام Vcenter آماده کنیم باید وارد سرور Active شویم.



شکل ۱۲- ۱۱ نصب *VMware Vcenter Appliance*

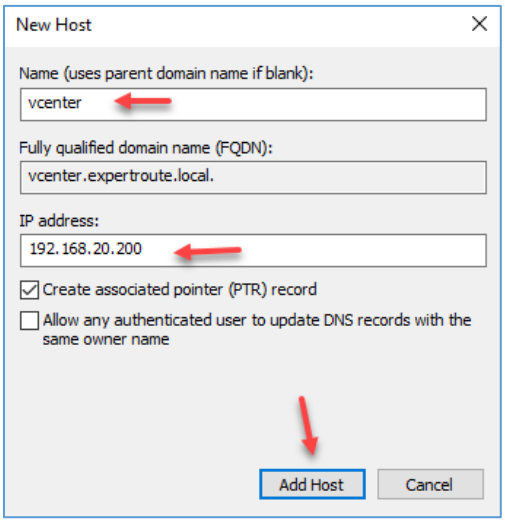
به مانند شکل ۱۲-۱۲، بعد از ورود به سرور Active باید وارد سرویس DNS شوید و برای تعریف آدرس Vcenter گزینه‌ی AAA را انتخاب کنید.

www.takbook.com



شکل ۱۲-۱۲ نصب *VMware Vcenter Appliance*

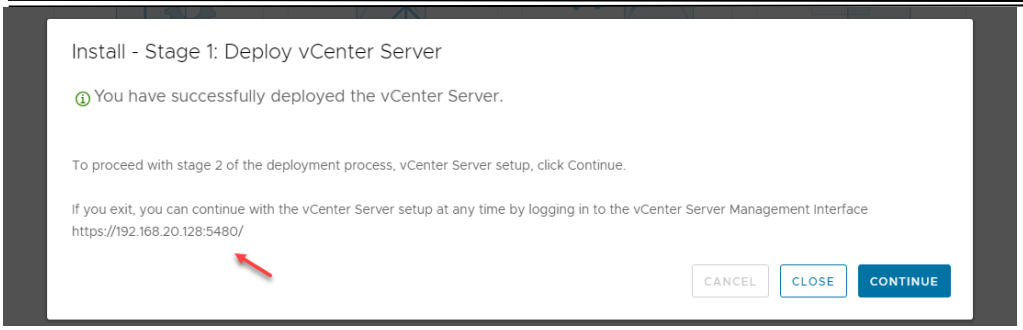
در شکل ۱۲-۱۳، باید نام سرور و آدرس آن را وارد کنید و تیک گزینه‌ی PTR را هم انتخاب کنید، با این کار سرور Vcenter از طریق نام هم در دسترس است.



شکل ۱۲-۱۳ نصب *VMware Vcenter Appliance*

در شکل ۱۲-۱۴، بعد از Deploy کردن کار Vcenter آغاز می‌شود و به شما اعلام می‌کند که کار به اتمام رسیده ولی برای تنظیم نهایی آن باید وارد آدرس مشخص شده شویم.

www.takbook.com

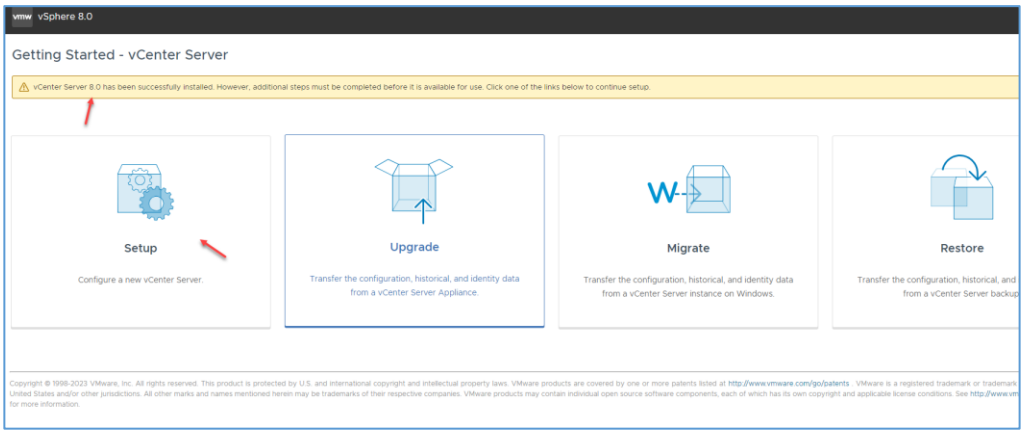


شکل ۱۲- ۱۴ نصب *VMware Vcenter Appliance*

برای ورود باید از آدرس FQDN که در قسمت قبل مشخص کردید استفاده کنید، که به صورت زیر خواهد بود:

https://vcenter.expertroute.local:5480

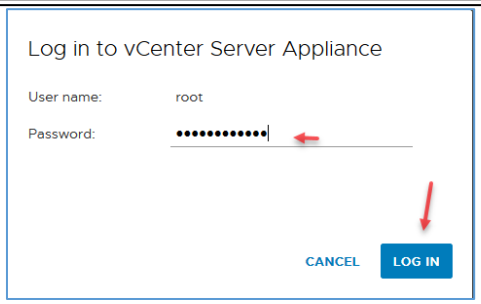
بعد از ورود به آدرس بالا شکل ۱۲-۱۵، ظاهر می‌شود، در بالای صفحه یک پیغام به شما نمایش داده شده است و به این موضوع اشاره دارد که کار Deploy سرور Vcenter بر روی هاست ESXi انجام شده است ولی برای انجام تنظیمات دیگر باید بر روی Set up در شکل کلیک کنید، در کل این آدرس در آینده برای ارتقاء نرم‌افزار و تبدیل آن به کار می‌آید و باید آدرس را با پورتی که برای آن مشخص شده است به یاد داشته باشید.



شکل ۱۲- ۱۵ نصب *VMware Vcenter Appliance*

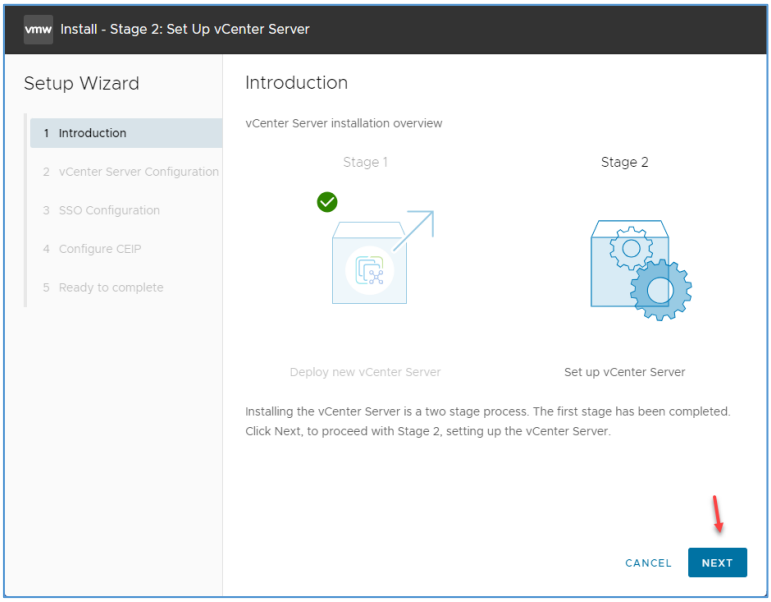
در شکل ۱۲-۱۶، برای ورود به Vcenter Server باید رمز عبور کاربر root را که در هنگام نصب مشخص کردید وارد و بر روی LOG IN کلیک کنید.

www.takbook.com



شکل ۱۲-۱۶ نصب *VMware Vcenter Appliance*

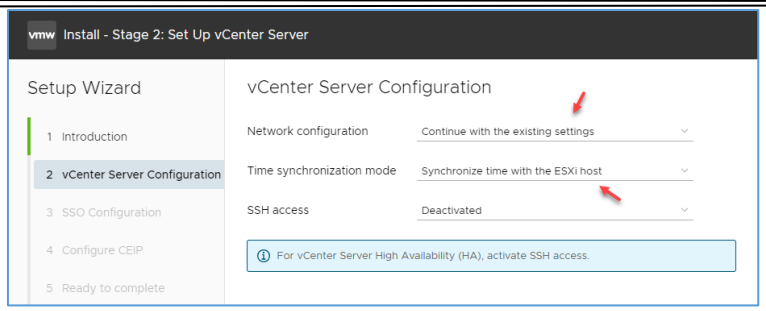
در شکل ۱۲-۱۷، مشخص شده است که کار نصب به اتمام رسیده و برای تنظیم باید بر روی NEXT کلیک کنید.



شکل ۱۲-۱۷ نصب *VMware Vcenter Appliance*

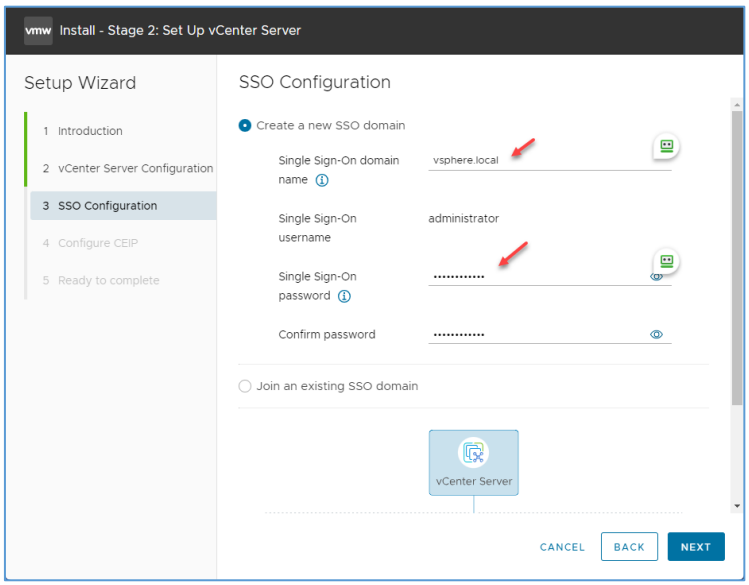
در شکل ۱۲-۱۸، در قسمت Network به گزینه‌ای دست نزنید و در قسمت Time می‌توانید مشخص کنید که ساعت و تاریخ را از چه مسیری دریافت کنید که همان ESXi اصلی را انتخاب کنید.

www.takbook.com



شکل ۱۲- ۱۸ نصب *VMware Vcenter Appliance*

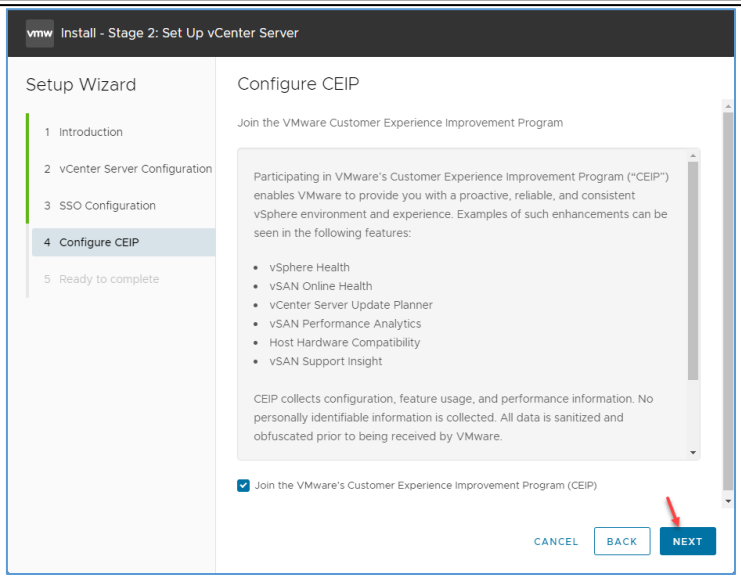
در شکل ۱۲-۱۹، باید برای SSO یا همان Single Sign-On یک نام دومین به غیر دومین اصلی شبکه خود وارد کنید و برای کاربر Administrator آن یک رمز عبور پیچیده وارد و بر روی Next کلیک کنید.



شکل ۱۲- ۱۹ نصب *VMware Vcenter Appliance*

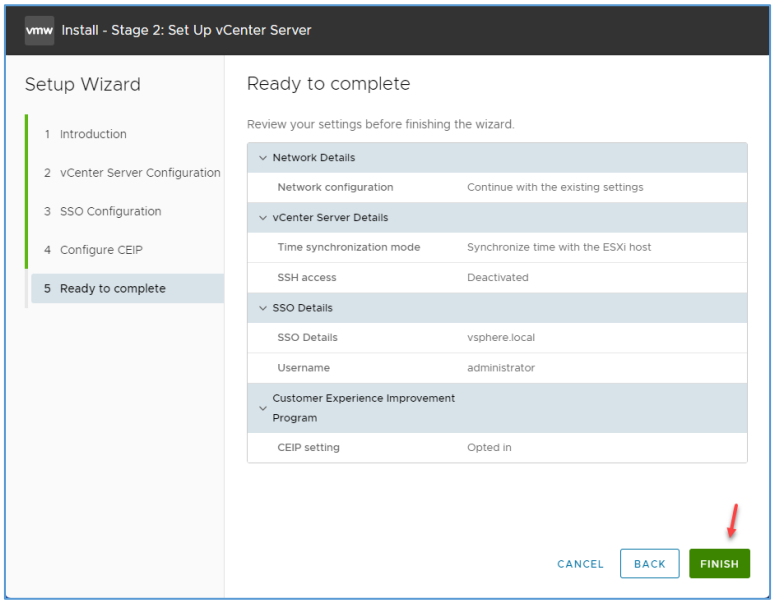
در شکل ۱۲-۲۰، اگر از لایسنس اصلی Vcenter استفاده می‌کنید و برای کمک به حل مشکلات و پاسخ با سوالات شما می‌توانید تیک گزینه‌ی CEIP را انتخاب کنید تا تیم VMware بتوانند به شما کمک کنند، توجه داشته باشید سرور مورد نظر باید به اینترنت متصل باشد.

www.takbook.com



شکل ۱۲- ۲۰ نصب *VMware Vcenter Appliance*

در شکل ۱۲-۲۱، اگر اطلاعات نهایی مورد تایید است بر روی Finish کلیک کنید.

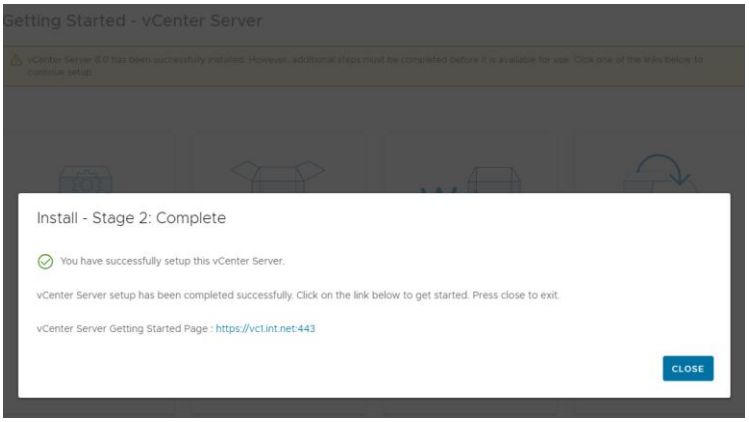


شکل ۱۲- ۲۱ نصب *VMware Vcenter Appliance*

نکته مهم: قبل از اینکه در این قسمت بر روی Finish کلیک کنید حتماً DNS سرور را برای Vcenter تنظیم کنید تا نامی که دادیم قابل شناسایی باشد، منظور ما همان نام Vcenter.expertroute.local که در صفحات

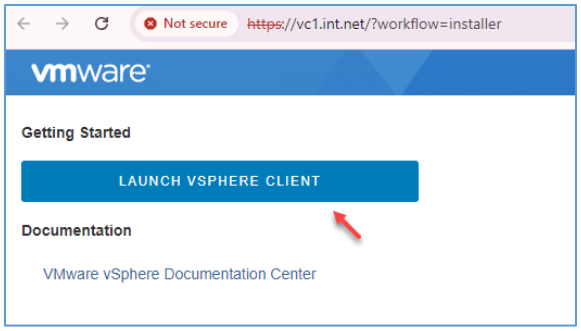
www.takbook.com

اول وارد کردیم اگر در شبکه Ping بگیریم باید IP مورد نظر یعنی ۱۹۲.۱٦۸.۲۰.۱۲۸ را شناسایی کند، در غیر این صورت بعد کلیک بر روی Finish کار با خطا مواجه می‌شود و باید همه چی را از اول شروع کنید.
بعد از تنظیم DNS و کلیک بر روی Finish سرویس‌های Vcenter شروع به فعال شدند می‌کنند که مقدار زمان آن بستگی به سرعت سروری که ESXi بر روی آن نصب شده است دارد.
در شکل ۱۲-۲۲، کار به اتمام رسیده و برای ورود باید بر روی آدرس مشخص شده در صفحه کلیک کنید که در ادامه آن را بررسی خواهیم کرد.



شکل ۱۲- ۲۲ نصب *VMware Vcenter Appliance*

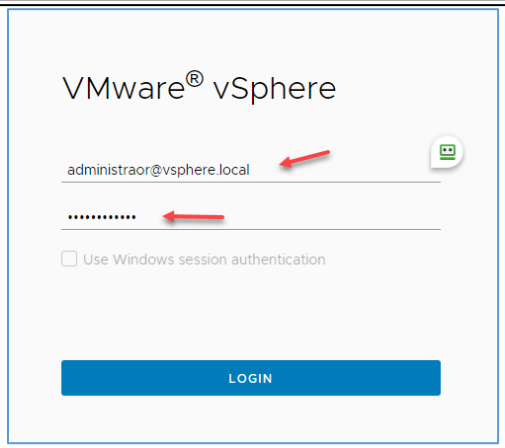
اولین صفحه‌ای که مشاهده می‌کنید شکل ۱۲-۲۳، است که باید بر روی آیکون مورد نظر کلیک کنید.



شکل ۱۲- ۲۳ نصب *VMware Vcenter Appliance*

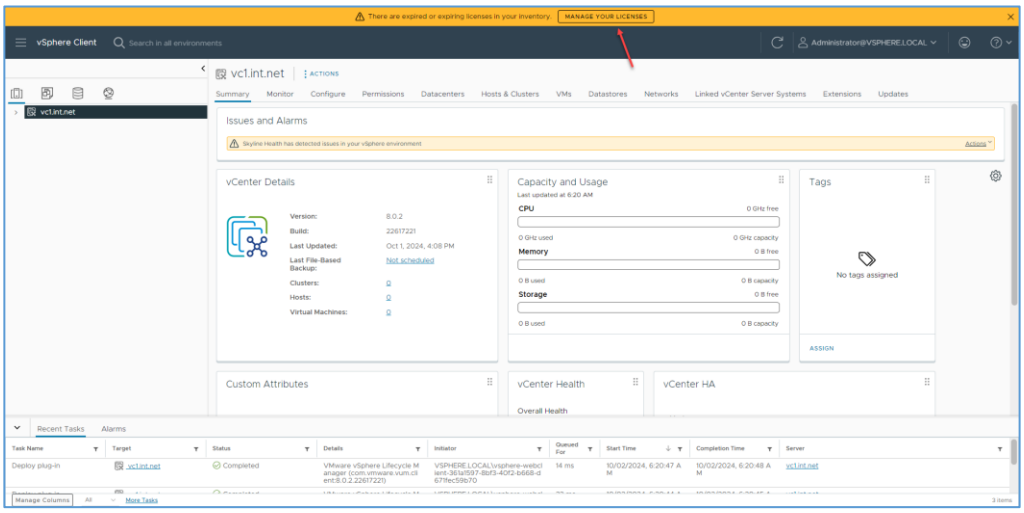
در ادامه به مانند شکل ۱۲-۲٤، باید نام کاربری را به همراه دومین داخلی که در هنگام نصب وارد کردیم را در این قسمت وارد کنیم و وارد Vcenter شویم.

www.takbook.com



شکل ۱۲- ۲۴ نصب *VMware Vcenter Appliance*

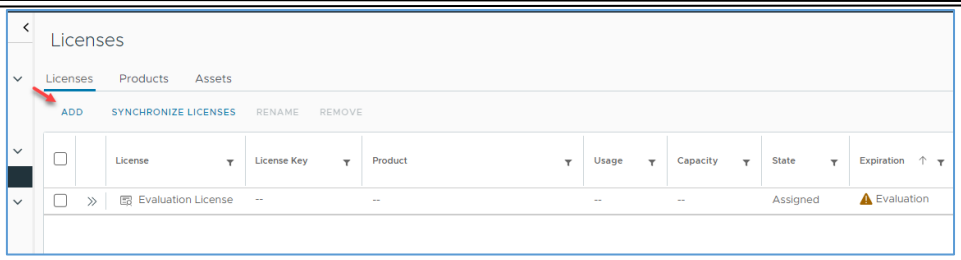
در شکل ۱۲-۲۵، صفحه اول Vcenter را مشاهده می‌کنید که بسیار زیبا و کاربر پسند طراحی شده است، اولین کاری که باید انجام دهید این است که لایسنس نرم‌افزار را بروز کنید، برای این کار باید بر روی نوار بالایی که در شکل مشخص شده است کلیک کنید.



شکل ۱۲- ۲۵ نصب *VMware Vcenter Appliance*

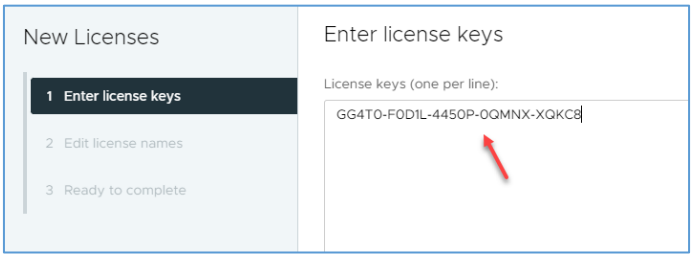
در شکل ۱۲-۲۶، وارد قسمت Licenses شدیم، همان‌طور که مشاهده می‌کنید یک لایسنس آزمایشی با نام Evaluation Lic موجود است که مجوز ۶۰ روز زمان برای استفاده از Vcenter را فراهم می‌کند، برای اینکه لایسنس جدید به نرم‌افزار معرفی کنید بر روی Add کلیک کنید.

www.takbook.com



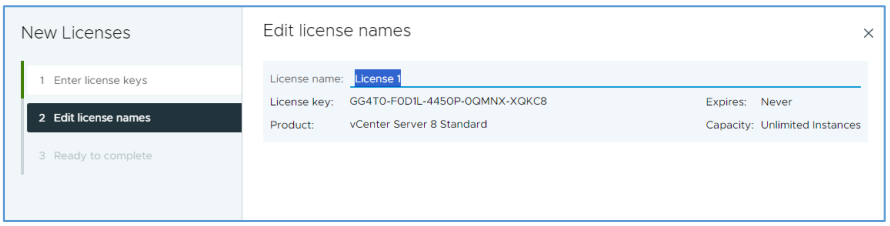
شکل ۱۲- ۲۶ نصب *VMware Vcenter Appliance*

در شکل ۱۲-۲۷، باید لایسنس مورد نظر خود را وارد کنید انتخاب لایسنس از نوع VMware Vsphere Standard انتخاب خوبی می‌تواند باشد.



شکل ۱۲- ۲۷ نصب *VMware Vcenter Appliance*

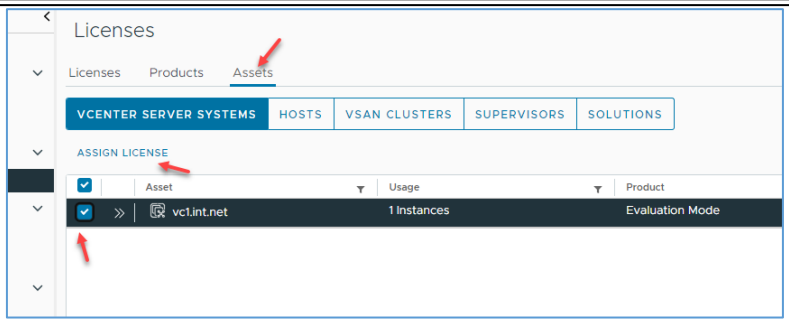
در شکل ۱۲-۲۸، نوع لایسنس مشخص شده است و در قسمت License name می‌توانید نام دلخواه برای لایسنس خود وارد کنید، بعد از این کار بر روی NEXT و در آخر بر روی FINISH کلیک کنید.



شکل ۱۲- ۲۸ نصب *VMware Vcenter Appliance*

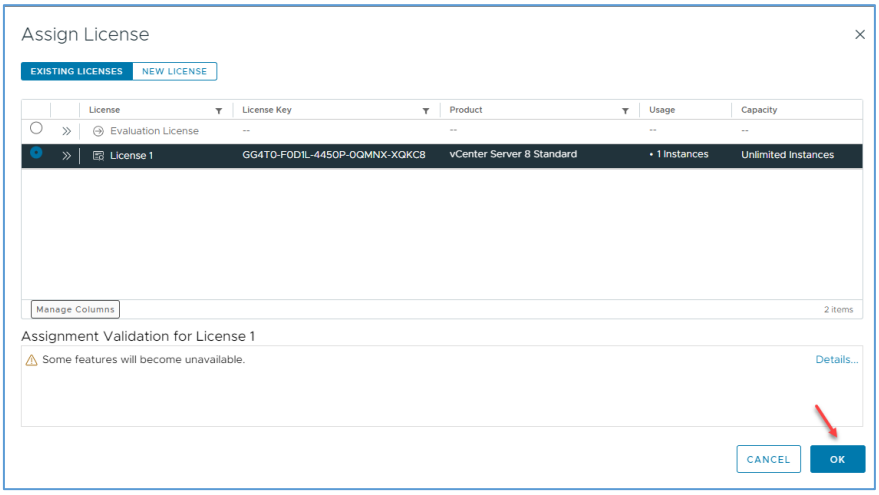
بعد از اینکه لایسنس مورد نظر را اضافه کردید باید آن را برای سرور یا سرورهای Vcenter که در شبکه دارید Assign کنید، برای این کار به مانند شکل ۱۲-۲۹، باید وارد تب Assets شوید و از لیست مورد نظر سرور Vcenter خود را انتخاب کنید و بر روی Assign License کلیک کنید.

www.takbook.com



شکل ۱۲- ۲۹ نصب *VMware Vcenter Appliance*

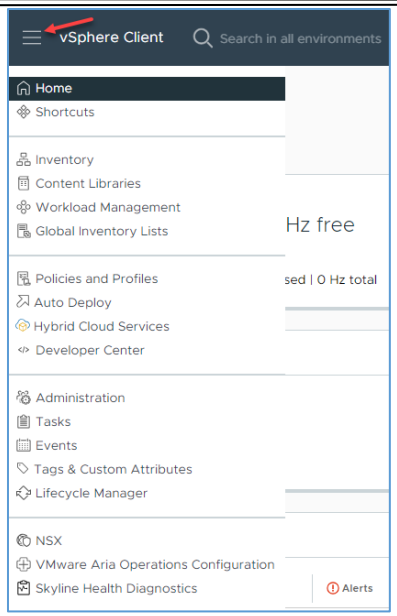
در شکل ۱۲-۳۰، باید لایسنسی که به لیست اضافه کردید را انتخاب کنید و بر روی OK کلیک کنید.



شکل ۱۲- ۳۰ نصب *VMware Vcenter Appliance*

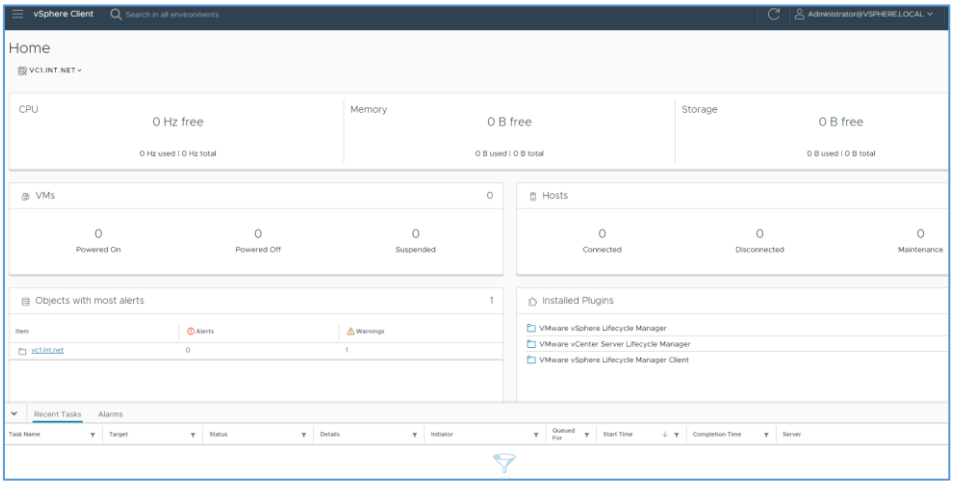
بعد از اعمال لایسنس مورد نظر به مانند شکل ۱۲-۳۱، بر روی آیکون سه نقطه کلیک کنید، در این منو گزینه‌های مختلفی وجود دارد که باید با هم همه آنها را بررسی کنیم، برای شروع بر روی Home کلیک کنید.

www.takbook.com



شکل ۱۲- ۳۱ نصب *VMware Vcenter Appliance*

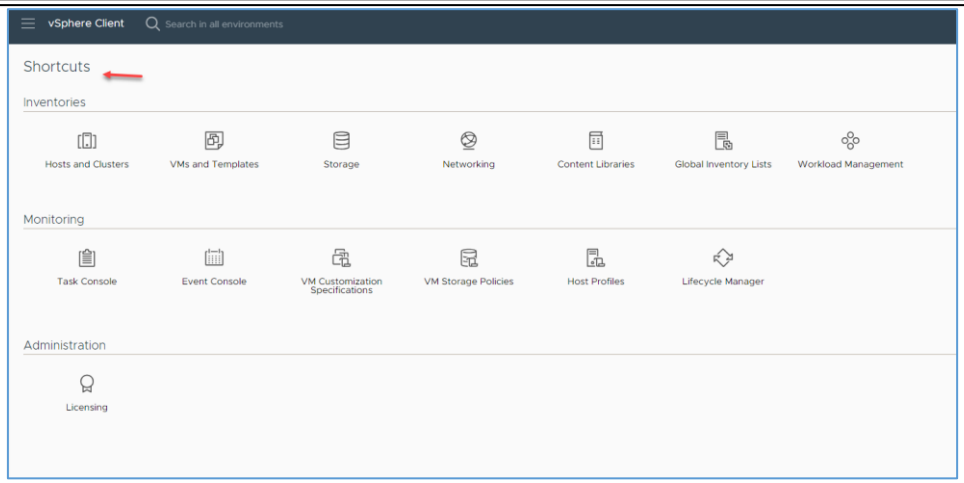
همان‌طور که در شکل ۱۲-۳۲، مشاهده می‌کنید در صفحه‌ی Home اطلاعات سخت‌افزاری، تعداد ماشین‌های مجازی به همراه تعداد سرورهای ESXi و اطلاعات مانیتورینگ از وضعیت سرور را به ما نشان می‌دهد.



شکل ۱۲- ۳۲ نصب *VMware Vcenter Appliance*

در شکل ۱۲-۳۳، قسمت Shortcutes هم که از نام آن پیداست تمام ابزارهای به صورت سریع به مانند شکل در دسترس قرار گرفتند و می‌توانیم از آنها استفاده کنیم.

www.takbook.com



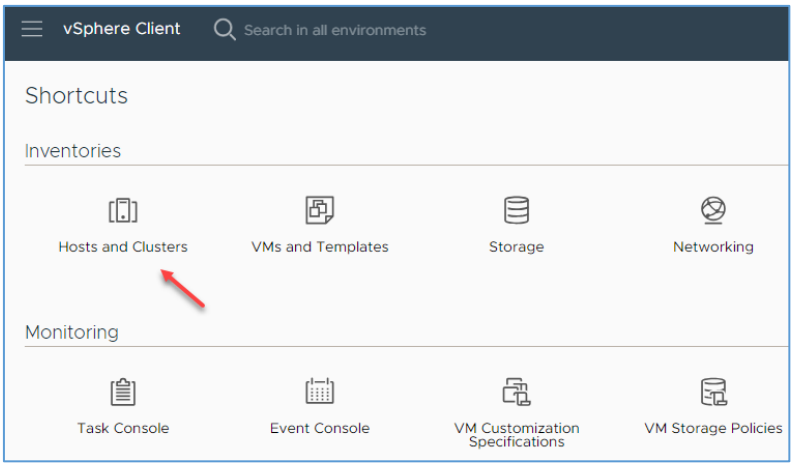
شکل ۱۲- ۳۳ نصب *VMware Vcenter Appliance*

در ادامه کار با همه ابزارها کار خواهیم کرد و برای شروع کار می‌خواهیم سرورهای ESXi که در مجموعه خود داریم به سرور Vcenter اضافه کنیم.

۱۲-۳ نحوه اضافه کردن ESXi به سرور Vcenter

برای شروع کار با Vcenter یک سرور ESXi را به لیست آن اضافه می‌کنیم و کارهای خود را روی آن انجام می‌دهیم.

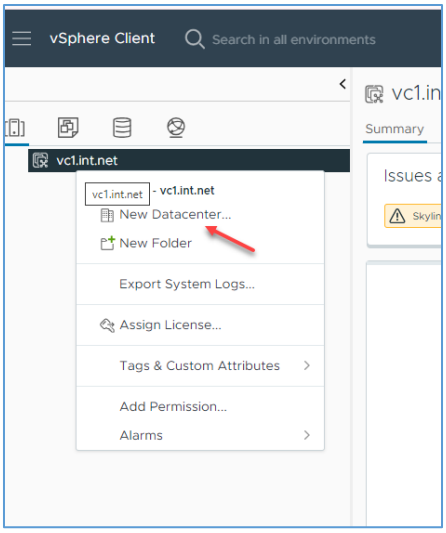
به مانند شکل ۱۲-۳٤، در صفحه Shortcuts بر روی Hosts and Clusters کلیک کنید البته از سمت چپ هم می‌توانید این کار را انجام دهید.



شکل ۱۲- ۳۴ اضافه کردن *ESXi* به سرور *Vcenter*

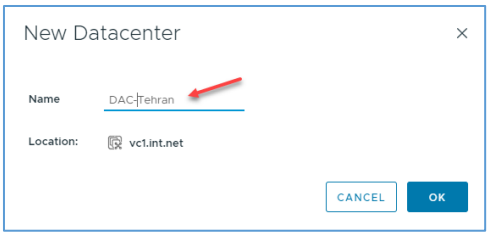
www.takbook.com

در شکل ۱۲-۳۵، سرور Vcenter مورد نظر خود را از لیست انتخاب کنید و در صفحه باز شده از قسمت ACTIONS گزینه‌ی New Datacenter را انتخاب کنید، البه روی خود نام Vcenter هم می‌توانستید کلیک راست کنید.



شکل ۱۲- ۳۵ اضافه کردن ESXi به سرور Vcenter

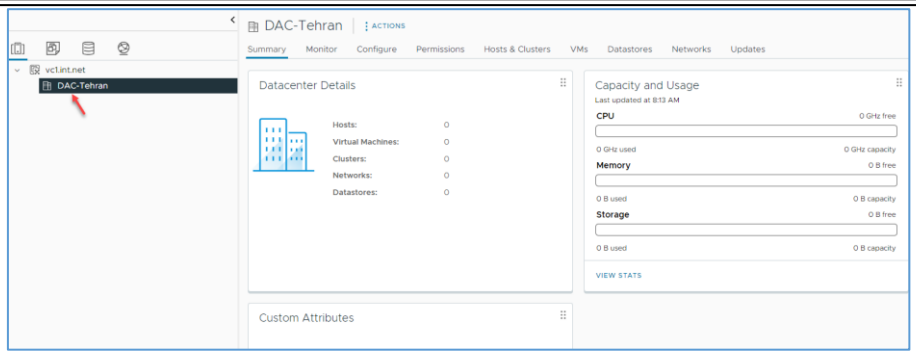
در شکل ۱۲-۳۶، یک نام به دلخواه وارد و بر روی OK کلیک کنید، در این Datacenter می‌توانید چندین هاست مانند ESXi اضافه کنید، اصولاً Datacenter برای جدا کردن بخش‌های سازمان از هم است مثلاً یک سازمان چندین شعبه در شهر دارد و می‌تواند با این کار یک برنامه‌ریزی خوب ایجاد کند، و همه چیز به صورت منظم باشد.



شکل ۱۲- ۳۶ اضافه کردن ESXi به سرور Vcenter

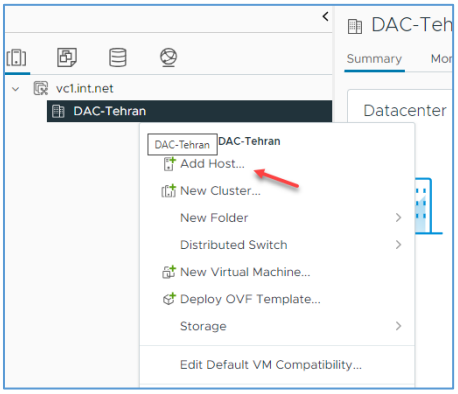
در شکل ۱۲-۳۷، بر روی Datacenter که ایجاد کردید کلیک کنید که در شکل مشخص است که هر دیتاسنتر که ایجاد می‌کنیم دارای تنظیمات خاص خودش است که در صورت نیاز باید آنها را تغییر دهیم.

www.takbook.com



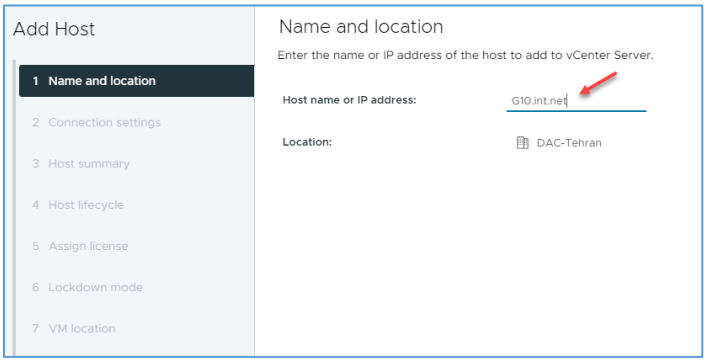
شکل ۱۲- ۳۷ اضافه کردن ESXi به سرور Vcenter

برای شروع کار و اضافه کاردن هاست ESXi به مانند شکل ۱۲-۳۸، از منوی ACTIONS گزینه‌ی Add Host را انتخاب کنید.



شکل ۱۲- ۳۸ اضافه کردن ESXi به سرور Vcenter

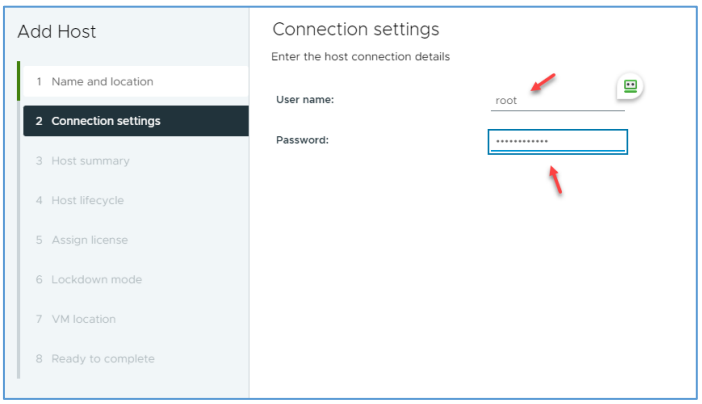
در شکل ۱۲-۳۹، باید آدرس سرور ESXi خود را وارد کنید، همان‌طور که گفتیم می‌توانید چندین ESXi را به یک Datacenter اضافه کنید.



شکل ۱۲- ۳۹ اضافه کردن ESXi به سرور Vcenter

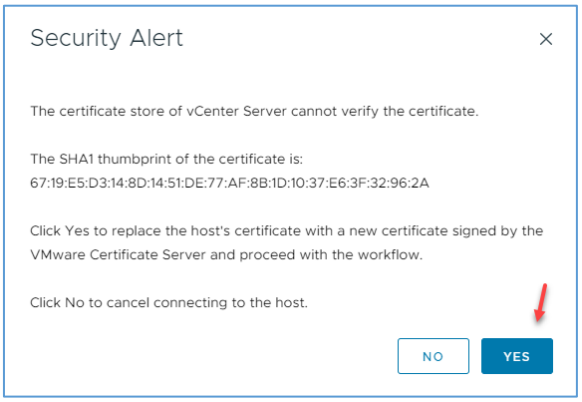
www.takbook.com

در شکل ۱۲-۴۰، نام کاربری و رمز عبور سرور ESXi را وارد و بر روی Next کلیک کنید.



شکل ۱۲- ۴۰ اضافه کردن ESXi به سرور Vcenter

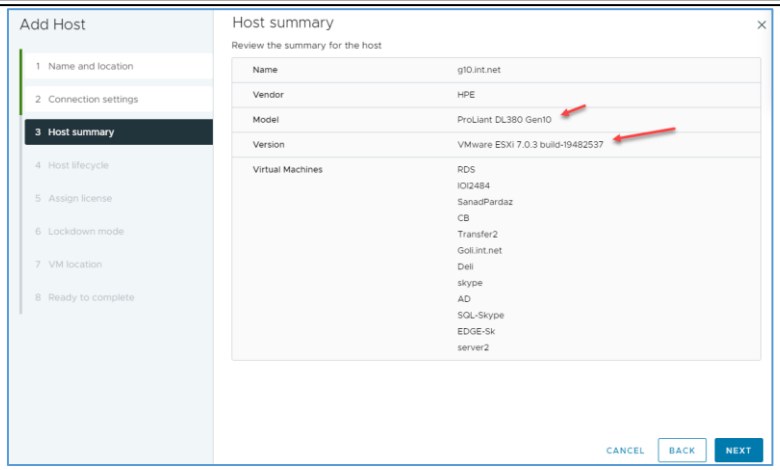
در شکل ۱۲-۴۱، باید گواهینامه یا همان Certificate سرور ESXi را تایید کنید، بر روی Yes کلیک کنید.



شکل ۱۲- ۴۱ اضافه کردن ESXi به سرور Vcenter

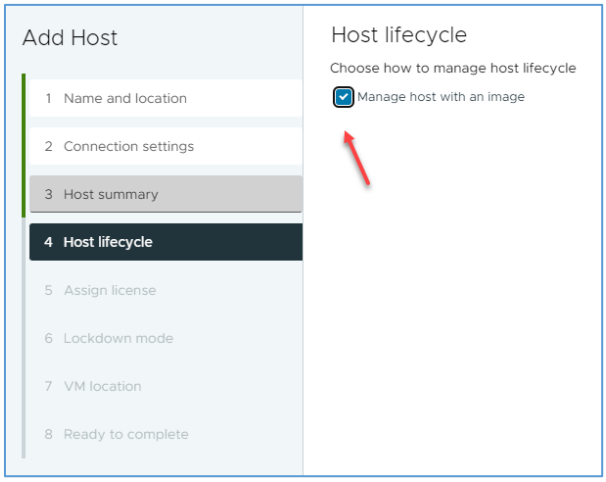
در شکل ۱۲-۴۲، اطلاعات سرور ESXi مشخص شده است و می‌توانید ماشین‌های مجازی که بر روی آن قرار دارد را مشاهده کنید.

www.takbook.com



شکل ۱۲- ۴۲ اضافه کردن ESXi به سرور Vcenter

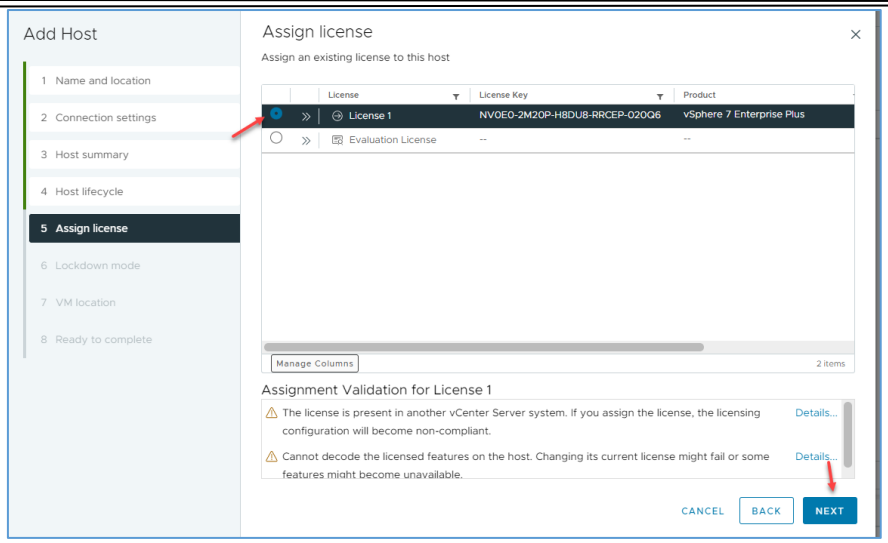
در شکل ۱۲-۴۳، باید تیک این گزینه را بردارید و بر روی Next کلیک کنید، این گزینه مربوط به قابلیت جدید Lifecycle است که در ادامه روی آن کار خواهیم کرد.



شکل ۱۲- ۴۳ اضافه کردن ESXi به سرور Vcenter

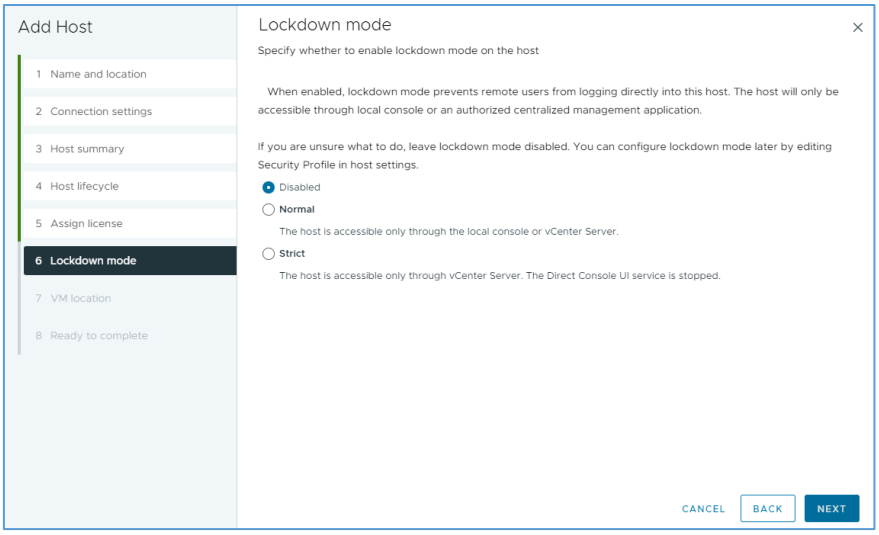
در شکل ۱۲-۴۴، یک لایسنس برای تخصیص دادن به هاست مورد نظر انتخاب کنید، این لایسنس را قبلاً و در بخش‌های قبلی به سرور اضافه کردیم.

www.takbook.com



شکل ۱۲- ۴۴ اضافه کردن ESXi به سرور Vcenter

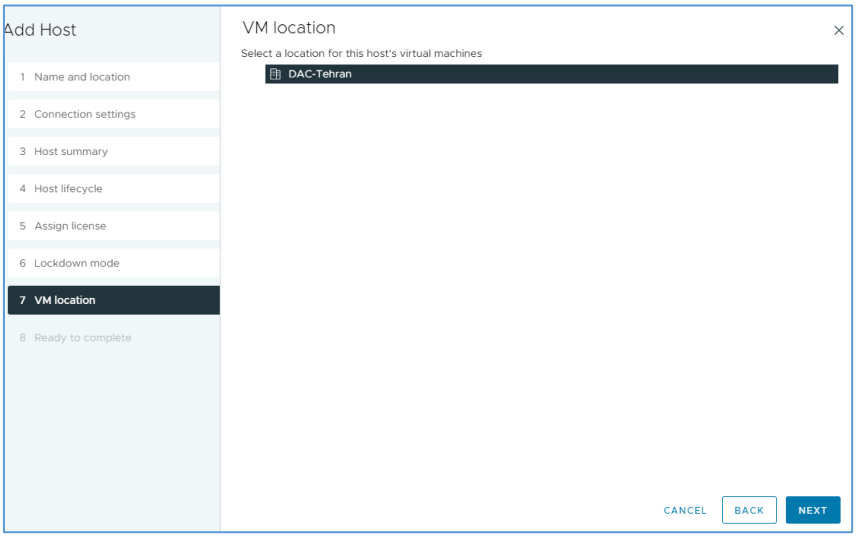
در شکل ۱۲-٤٥، گزینه‌ی Lockdown Mode را مشاهده می‌کنید که یک قابلیت بسیار مهم و امنیتی در Vcenter است، با فعال کردن این سرویس هیچ کسی به صورت مستقیم نمی‌تواند به هاست ESXi متصل شود و تنظیماتی که شما در Vcenter انجام دادید دیگر کسی نمی‌تواند آن را تغییر دهد، که این کار بسیار می‌تواند کمک کننده باشد، در حال حاضر گزینه‌ی Disabled را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۲- ۴۵ اضافه کردن ESXi به سرور Vcenter

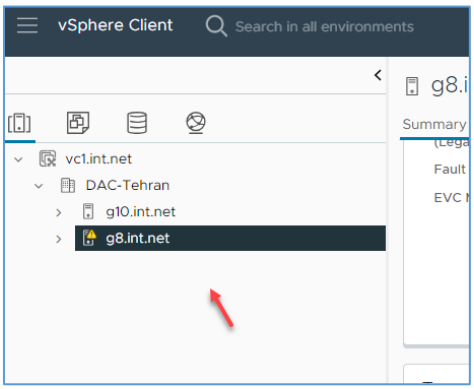
www.takbook.com

در شکل ۱۲-٤٦, باید مشخص کنید که هاست در کدام یک از دیتاسنترهایی که ایجاد کردید قرار گیرد، بر روی Next کلیک و در آخر بر روی Finish کلیک کنید تا هاست مورد نظر به لیست Vcenter اضافه شود.



شکل ۱۲- ۴۶ اضافه کردن ESXi به سرور Vcenter

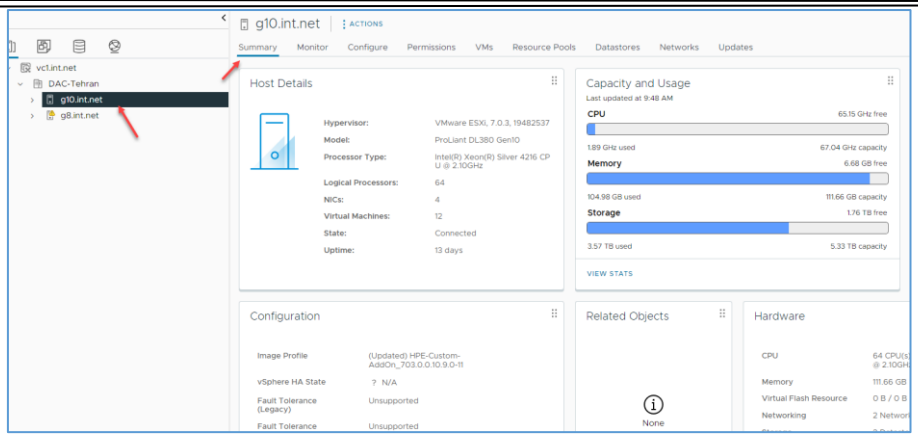
همان‌طور که در شکل ۱۲-٤۷، مشاهده می‌کنید، دو هاست به لیست اضافه کردیم.



شکل ۱۲- ۴۷ اضافه کردن ESXi به سرور Vcenter

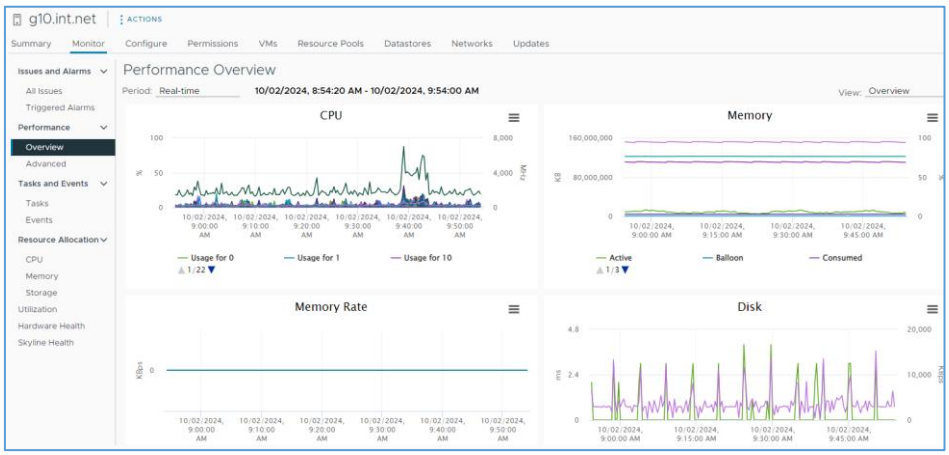
در شکل ۱۲-٤۸، با کلیک کردن بر روی هر هاست اطلاعات کاملی از سخت‌افزار و نرم‌افزار آن نمایش داده می‌شود، در تب اول یعنی Summary اطلاعات جامعی از سخت‌افزار، نرم‌افزارهای مورد نظر نمایش داده می‌شود که می‌تواند کمک کننده باشد، مثلاً در قسمت Hypervisior مدل سیستم‌عامل نصب شده بر روی هاست را ESXi 7.0.3 نشان داده است.

www.takbook.com



شکل ۱۲- ۴۸ اضافه کردن ESXi به سرور Vcenter

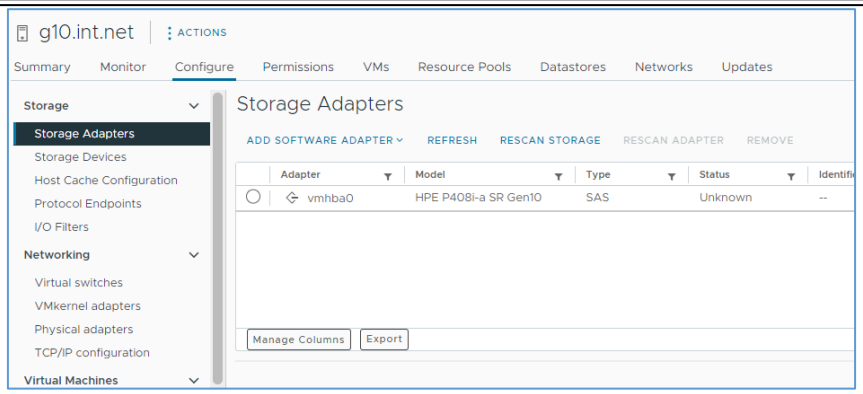
در شکل ۱۲-۴۹، در قسمت Monitor اطلاعات کاملی از رویدادهایی که در هاست مورد نظر روی می‌دهد را می‌تواند مشاهده کنید، در قسمت Overview می‌توانید مقدار مصرف CPU، RAM و ... را مشاهده می‌کنید.



شکل ۱۲- ۴۹ اضافه کردن ESXi به سرور Vcenter

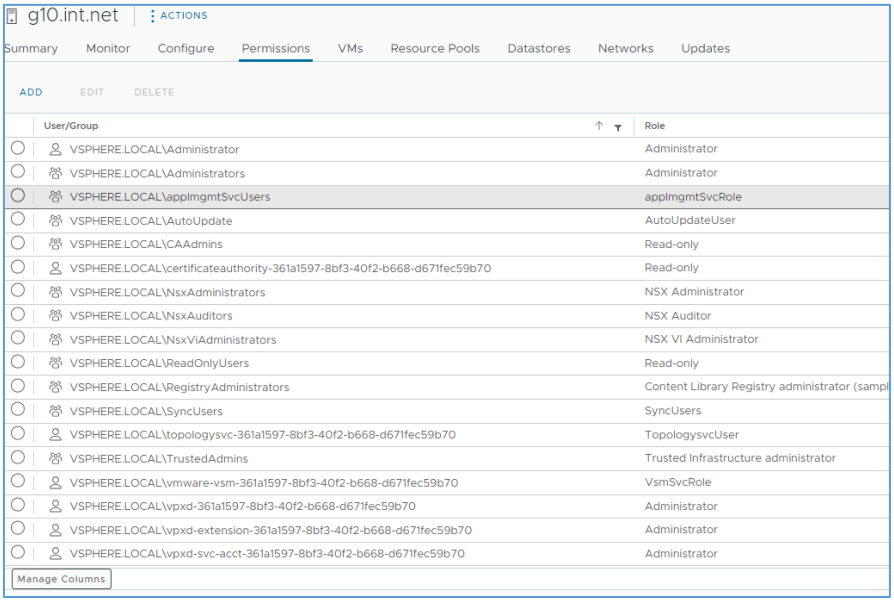
به مانند شکل ۱۲-۵۰، در قسمت Configure می‌توانید تمام تنظیمات اعمال شده به همراه جزئیات سخت‌افزاری هاست مورد نظر را مشاهده می‌کنید، در این قسمت می‌توانید بدون نیاز به متصل شدن مستقیم به ESXi تنظیمات آن را تغییر دهید.

www.takbook.com



شکل ۱۲- ۵۰ اضافه کردن ESXi به سرور Vcenter

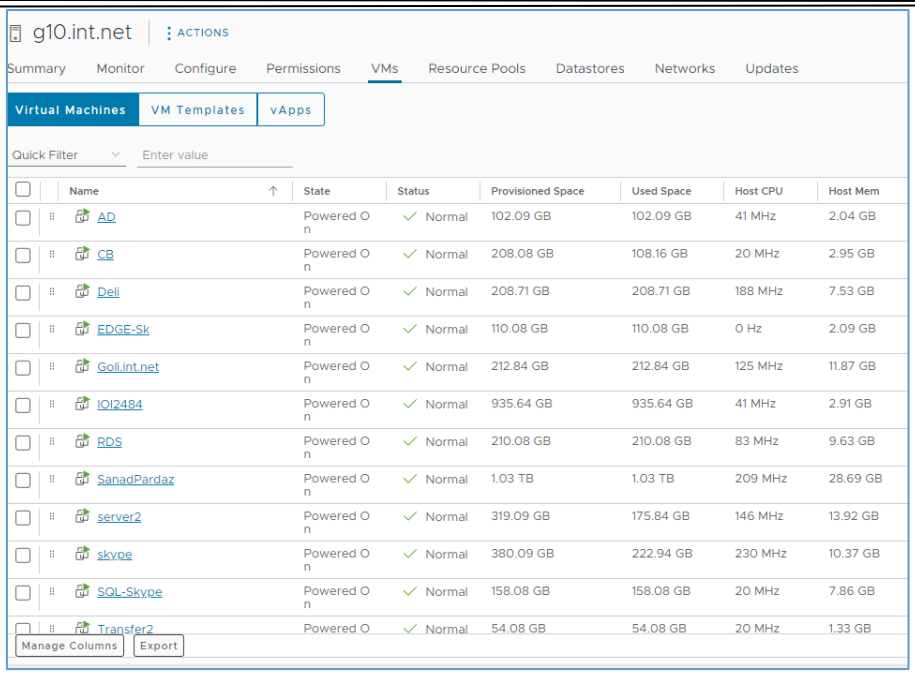
به مانند شکل ۱۲-۵۱، در تب Permissions می‌توانید دسترسی‌های مشخص شده به کاربران را مشاهده کنید و آنها را تغییر دهید.



شکل ۱۲- ۵۱ اضافه کردن ESXi به سرور Vcenter

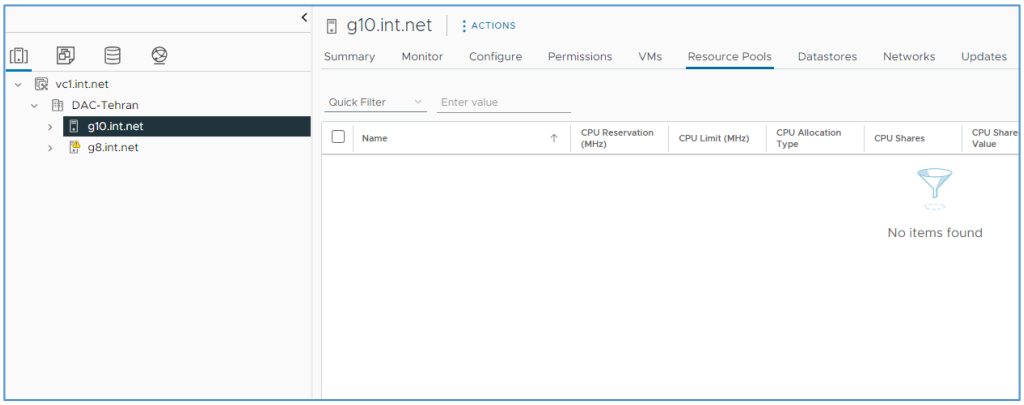
در شکل ۱۲-۵۲، در تب VMs تمام ماشین‌های مجازی مربوط به هاست مورد نظر را مشاهده می‌کنید که در ادامه عملیات خود را بر روی آنها انجام خواهیم داد.

www.takbook.com



شکل ۱۲- ۵۲ اضافه کردن ESXi به سرور Vcenter

به مانند شکل ۱۲–۵۳، در تب Resource Pools هم می‌توانید یک مجموعه ایجاد کنید و منابع سخت‌افزی که می‌خواهید به ماشین‌های مورد نظر داده شود را مشخص کنید، در تب Datastores هم می‌توانید Datastore موجود بر روی هاست و مقدار فضای آنها را مشاهده کنید.

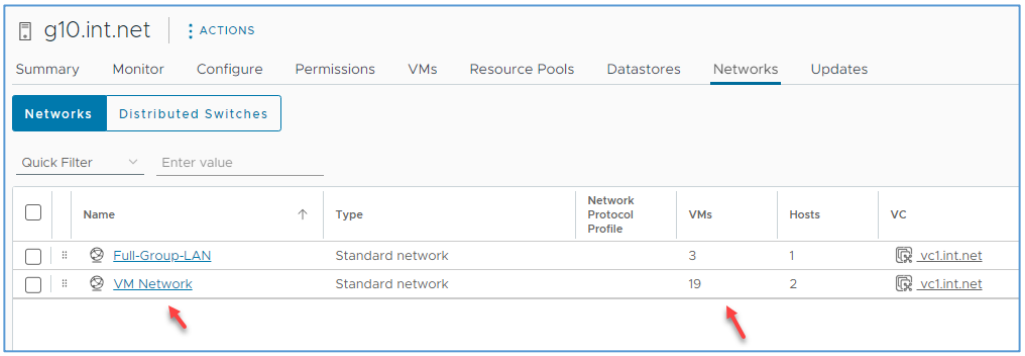


شکل ۱۲- ۵۳ بررسی Resource Pools

به مانند شکل ۱۲–٥٤، در تب شبکه کارت‌های شبکه فعال این هاست را به همراه تعداد ماشین‌هایی که به آنها اختصاص داده شده است را مشاهده می‌کنید، همان‌طور که گفتیم در Vcenter می‌توانید به صورت

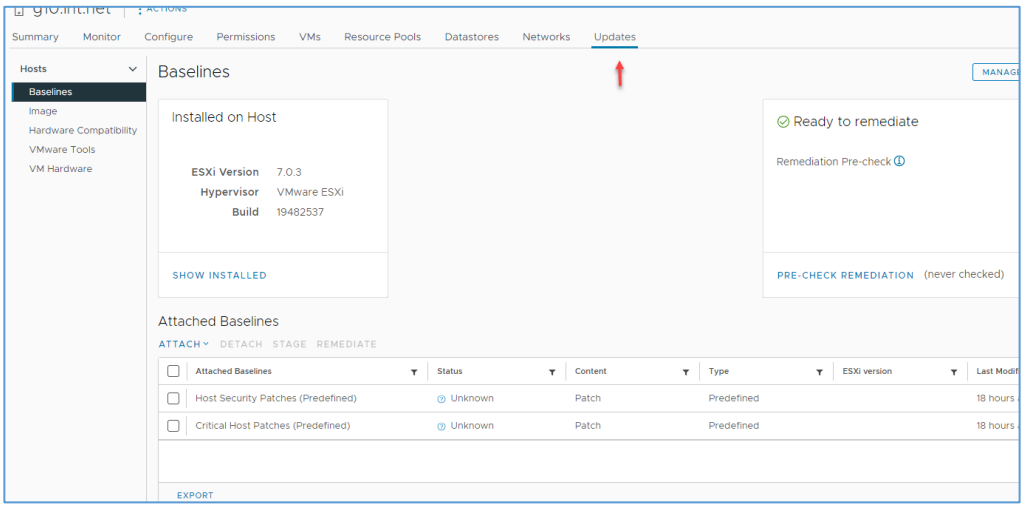
www.takbook.com

کامل به هاست ESXi دسترسی داشته باشید و تنظیمات را بدون اینکه به ESXi به صورت مستقیم متصل شوید انجام دهید.



شکل ۱۲- ۵۴ بررسی تب *Networks*

به مانند شکل ۱۲-۵۵، در تب Updates هم اطلاعاتی از ورژن نرم‌افزار و آپدیت‌های در دسترس را مشاهده خواهید کرد، حتی می‌توانید از طریق Vcenter هاست ESXi را به همراه Vmware Tools آپدیت کنید، این موارد در خلال کار توضیح داده خواهد شد.



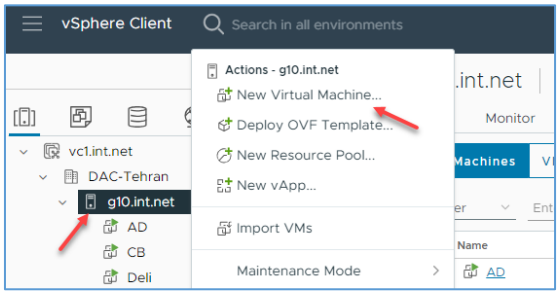
شکل ۱۲- ۵۵ بررسی تب *Updates*

۱۲-٤ ایجاد ماشین مجازی توسط VMware Vcenter

بعد از بررسی اولیه Vcenter در این بخش می‌خواهیم ماشین مجازی جدید از طریق آن ایجاد کنیم، که این کار منوط به این است که هاست ESXi خود را از قبل به Vcenter اضافه کرده باشید.

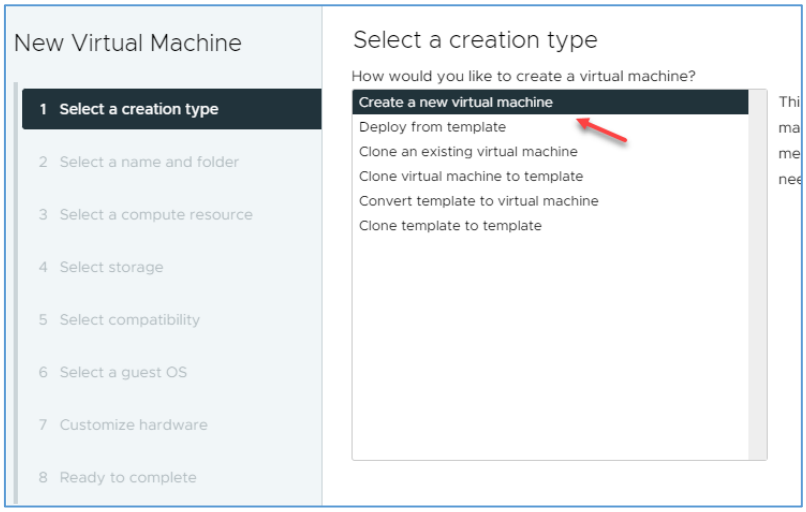
www.takbook.com

برای شروع کار به مانند شکل ۱۲–۵۶، باید از لیست مورد نظر یکی از هاست‌های خود را انتخاب کنید، و در صفحه باز شده گزینه‌ی New virtual Machine را انتخاب کنید.



شکل ۱۲ - ۵۶ اضافه کردن ماشین مجازی

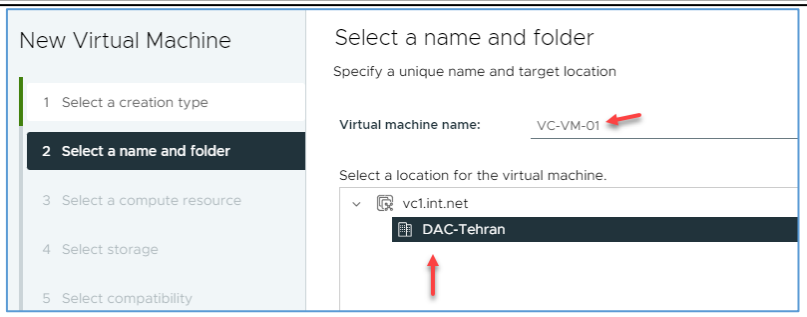
در شکل ۱۲–۵۷، باید گزینه‌ی Create a new virtual machine را انتخاب کنید.



شکل ۱۲ - ۵۷ اضافه کردن ماشین مجازی

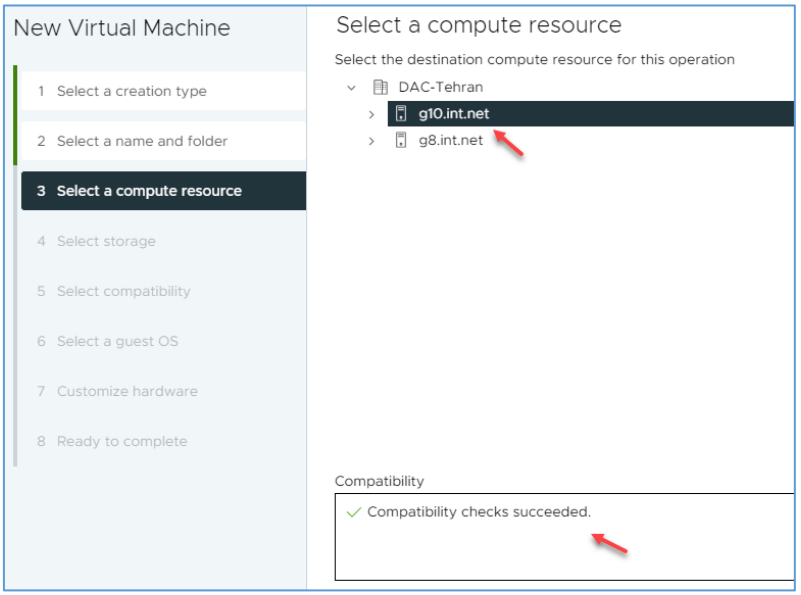
در شکل ۱۲–۵۸، نام ماشین مجازی خود را وارد کنید و از مسیر نصب آن را در زیر مشخص کنید که در مجموعه کدام DataCenter قرار بگیرد.

www.takbook.com



شکل ۱۲- ۵۸ اضافه کردن ماشین مجازی

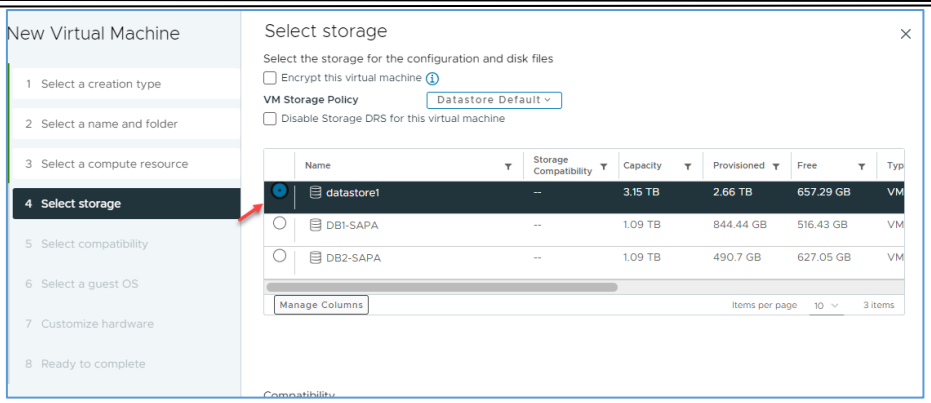
در شکل ۱۲-۵۹، باید هاست ESXi خود را انتخاب کنید که به صورت پیش‌فرض هاستی انتخاب شده است که در حال حاضر در حال انجام عملیات بر روی آن هستیم، توجه داشته باشید اگر مشکلاتی در هاست مورد نظر وجود داشته باشد در زیر شکل به شما پیغام خطا خواهد داد.



شکل ۱۲- ۵۹ اضافه کردن ماشین مجازی

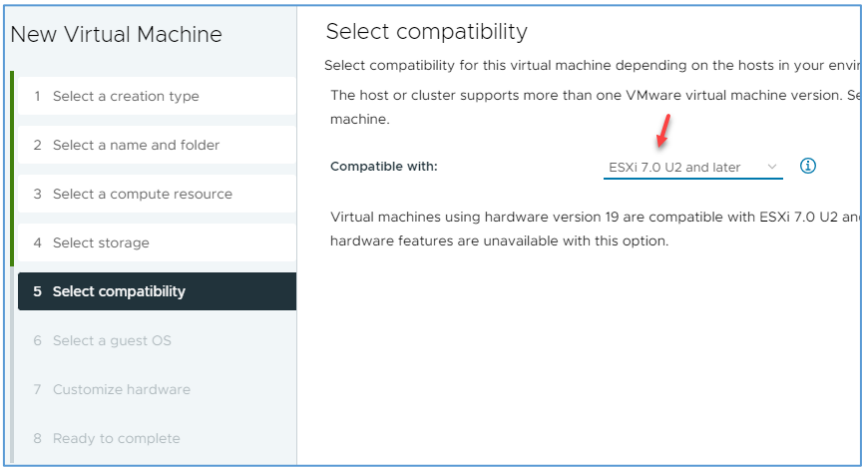
در شکل ۱۲-۶۰، باید DataStore مورد نظر خود را انتخاب کنید، توجه داشته باشید که در ستون Free فضای مناسب وجود داشته باشد.

www.takbook.com



شکل ۱۲- ۶۰ اضافه کردن ماشین مجازی

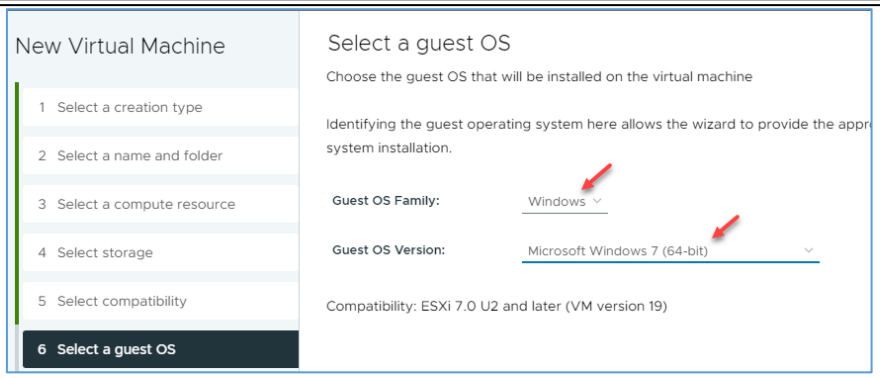
در شکل ۱۲-۶۱، می‌توانید مشخص کنید که ماشین مجازی شما با چه ورژنی از ESXi کار کند، مثلاً در این شکل ورژن ESXi 7.0.2 انتخاب شده که این بدان معنا است که این ماشین فقط با ورژن ESXi 7.0.2 و بالاتر هماهنگی خواهد داشت.



شکل ۱۲- ۶۱ اضافه کردن ماشین مجازی

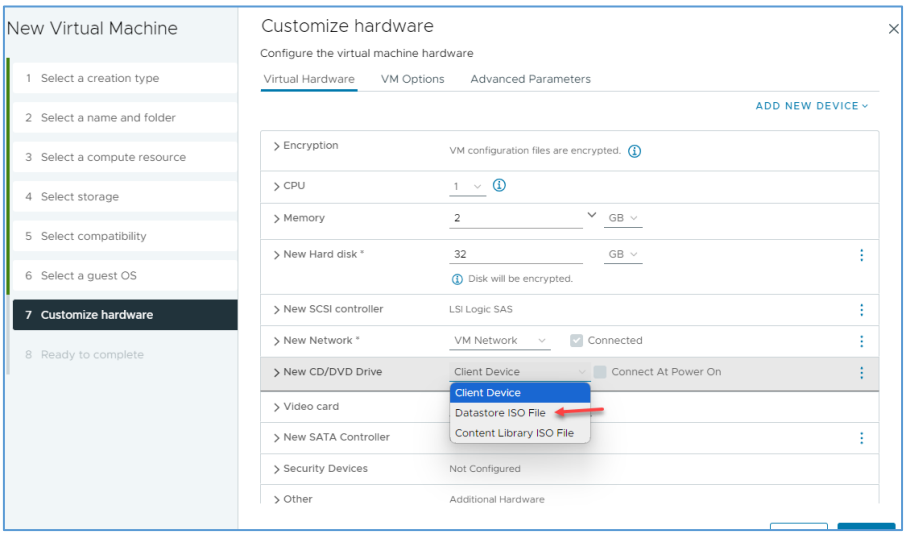
در شکل ۱۲-۶۲، باید سیستم عامل خود را از لیست انتخاب کنید و همینطور ورژن مربوط به آن را.

www.takbook.com



شکل ۱۲- ۶۲ اضافه کردن ماشین مجازی

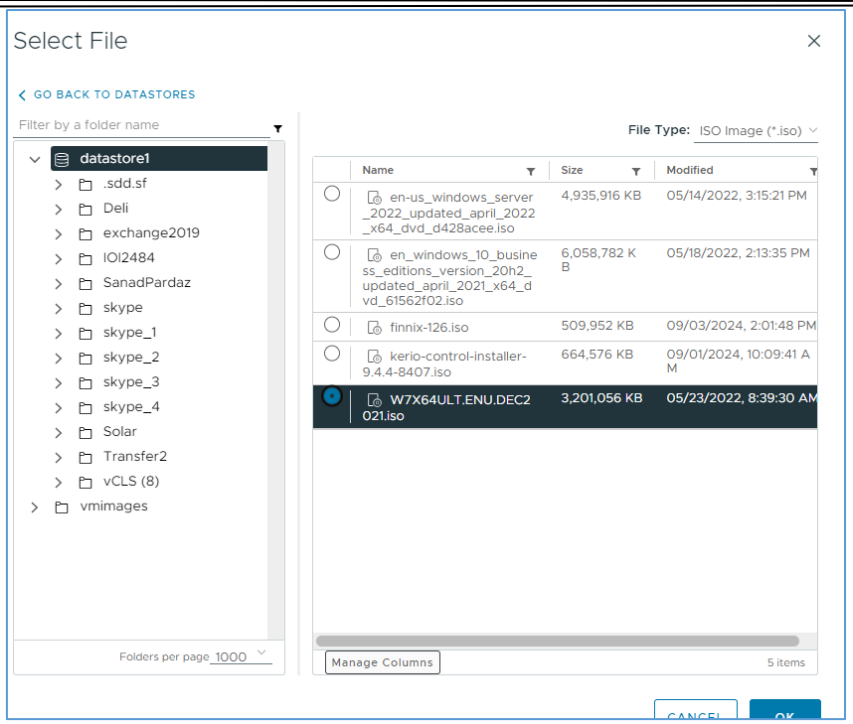
در شکل ۱۲-۶۳، باید مشخص کنید که این ماشین از چه منابع سخت‌افزاری استفاده کند، برای اینکه سیستم‌عامل را برای نصب به ماشین معرفی کنید می‌توانید از فایل ISO یا DVD در دستگاه استفاده کنید.



شکل ۱۲- ۶۳ اضافه کردن ماشین مجازی

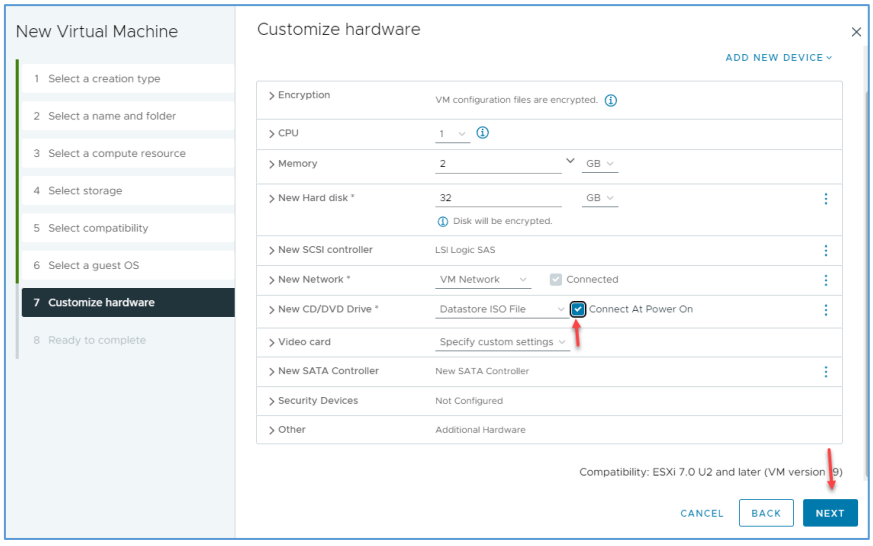
در شکل ۱۲-۶۴، باید فایل ISO مربوط به سیستم عامل مورد نظر خود را انتخاب کنید.

www.takbook.com



شکل ۱۲- ۶۴ اضافه کردن ماشین مجازی

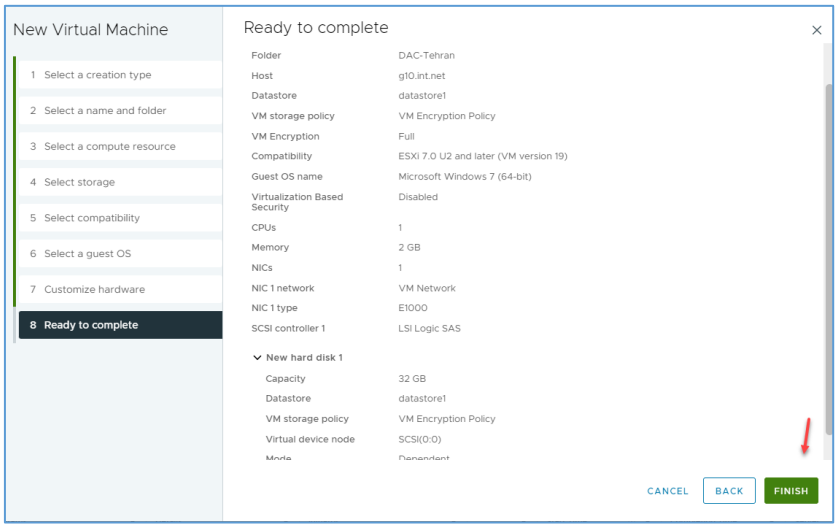
بعد از انتخاب به مانند شکل ۱۲-٦٥، تیک گزینه‌ی Connect را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۲- ۶۵ اضافه کردن ماشین مجازی

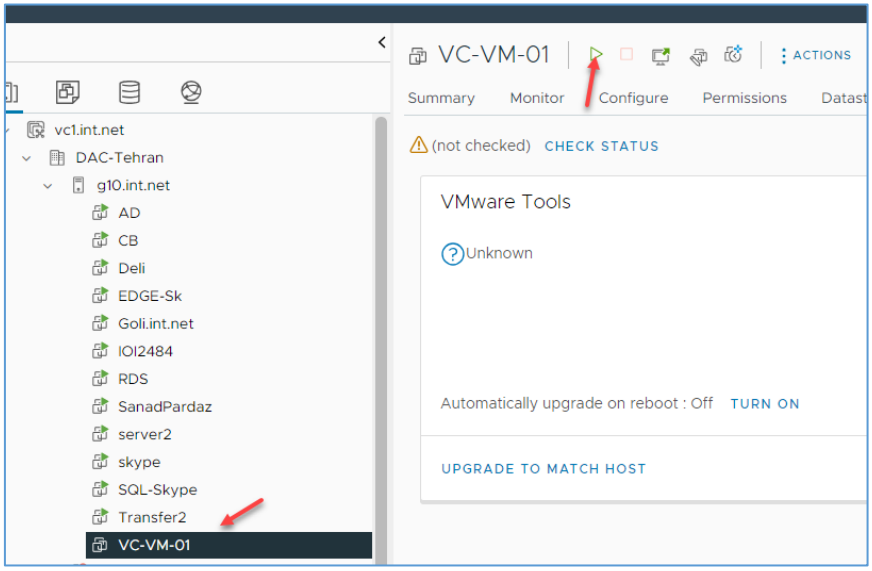
www.takbook.com

در شکل ۱۲-٦٦، اگر اطلاعات کلی مورد تایید است بر روی Finish کلیک کنید.



شکل ۱۲- ۶۶ اضافه کردن ماشین مجازی

بعد از اعمال تغییرات در ماشین مورد نظر می‌توانید به مانند شکل ۱۲-٦٧، ماشین را روشن و ویندوز را بر روی آن نصب کنید.

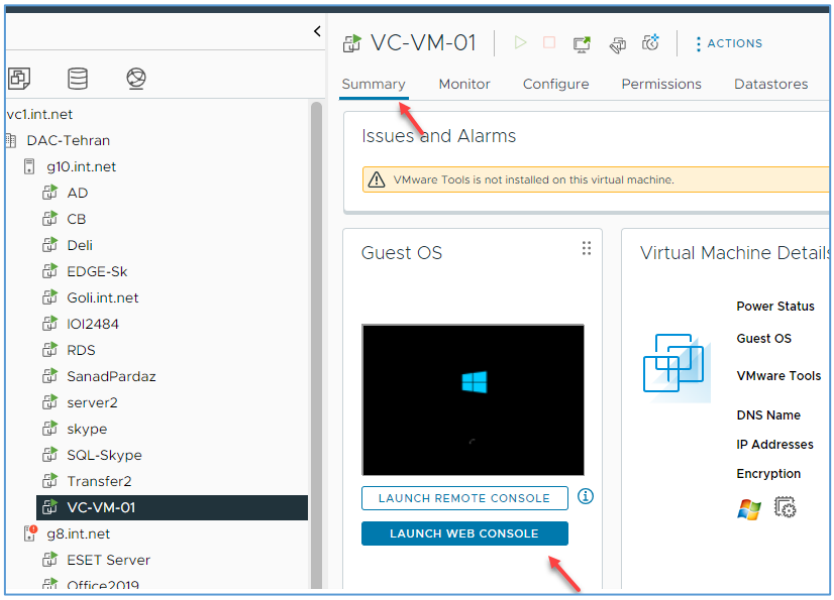


شکل ۱۲- ۶۷ روشن کردن ماشین مجازی

برای اینکه کنسول ماشین مجازی را مشاهده کنید به مانند شکل ۱۲-٦٨، بر روی ماشین مورد نظر دو بار کلیک کنید که در صفحه باز شده دو گزینه مشخص شده است اولی روی نرم‌افزار Remote Console

www.takbook.com

که در درس‌های قبلی بررسی کردیم باز خواهد شد و دومی ماشین را در یک صفحه وب جدید باز خواهد کرد ما همان گزینه‌ی دوم را انتخاب می‌کنیم.



شکل ۱۲- ۶۸ اجرای ماشین مجازی

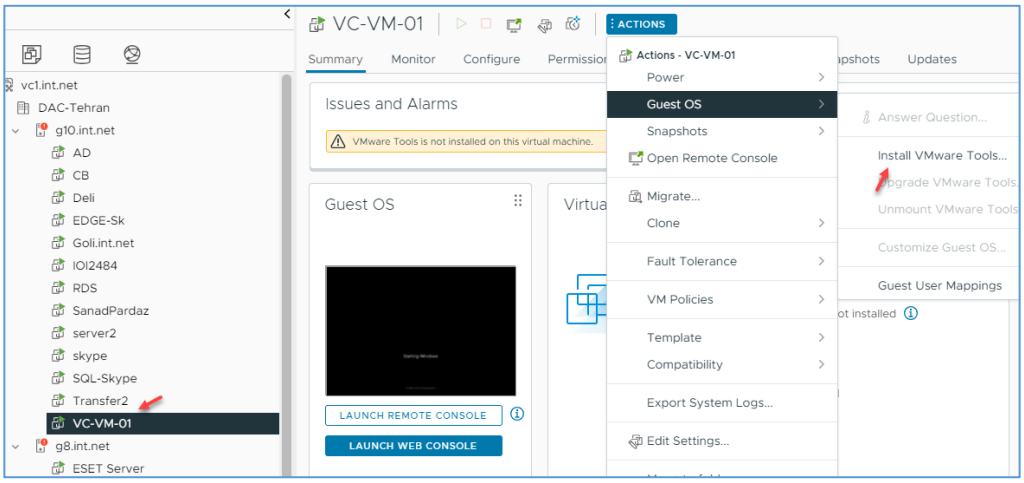
همان‌طور که در شکل ۱۲-۶۹،مشاهده می‌کنید ماشین مورد نظر در صفحه جدید اجرا شده و مراحل نصب ویندوز در حال انجام است، در سمت راست تصویر می‌توانید از کلیدهای موجود برای بزرگ کردن صفحه، استفاده از کیبورد و کلید CTRL+ALT+DEL استفاده کنید.



شکل ۱۲- ۶۹ اجرای ماشین مجازی

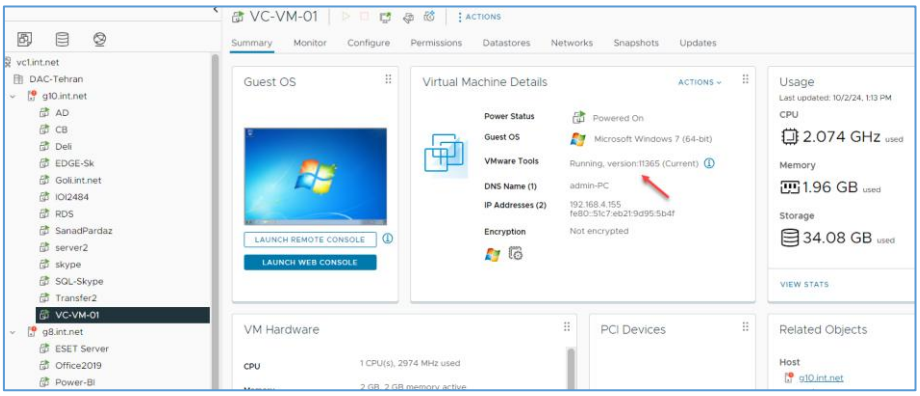
www.takbook.com

اولین کاری که بعد از نصب سیستم عامل انجام می‌دهیم نصب VMware Tools بر روی آن است که برای این کار طبق شکل ۱۲-۷۰، از منوی Actions وارد Guest OS شوید و گزینه‌ی Install VMware Tools را انتخاب کنید. با این کار یک فایل Image در درون ماشین فعال شده که باید بر روی فایل Setup آن کلیک کنید و آن را نصب کنید.



شکل ۱۲- ۷۰ نصب VMware Tools

بعد از نصب حتماً ماشین مورد نظر را Restart کنید، همان‌طور که در شکل ۱۲-۷۱،مشاهده می‌کنید بعد از نصب Vmware Tools اطلاعات ماشین مورد نظر در این شکل مشخص شده است.

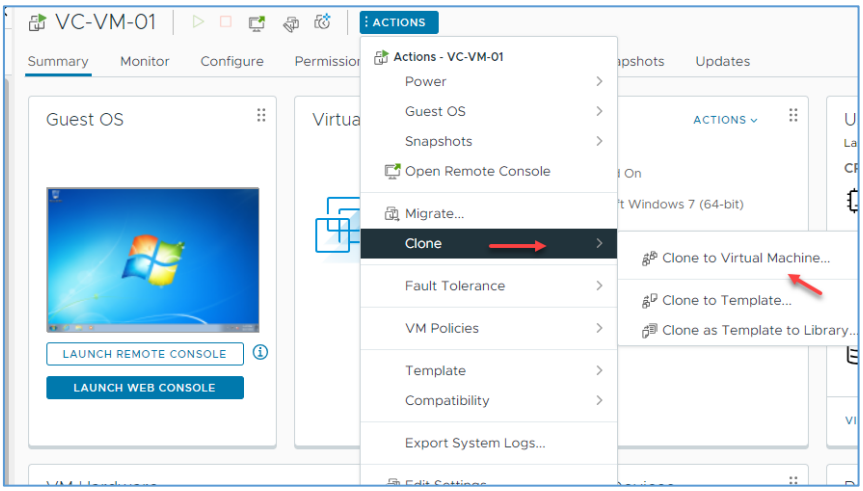


شکل ۱۲- ۷۱ نصب VMware Tools

www.takbook.com

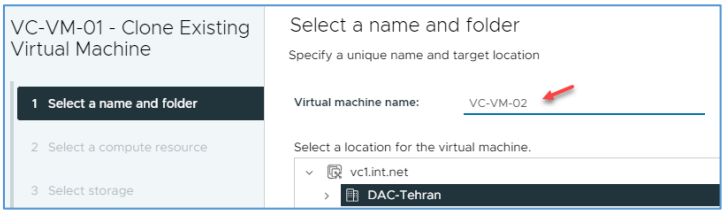
۱۲-۵ ایجاد Clone از ماشین مجازی در Vcenter

در این قسمت می‌خواهیم از ماشین‌های مجازی که ایجاد کردیم یک یا چند Clone (کپی) از آن تهیه کنیم، برای این کار بعد از انتخاب ماشین مورد نظر از لیست، به مانند شکل ۱۲-۷۲، بر روی ACTIONS کلیک کنید و از قسمت Clone گزینه‌ی Clone to Virtual machine را انتخاب کنید.



شکل ۱۲-۷۲ ایجاد Clone از ماشین مجازی

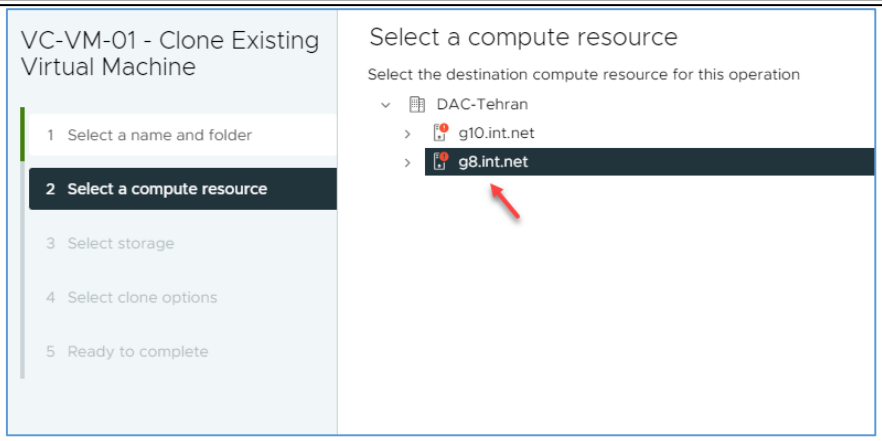
در شکل ۱۲-۷۳، نام ماشین جدید را وارد و بعد از انتخاب DataCenter بر روی Next کلیک کنید.



شکل ۱۲-۷۳ ایجاد Clone از ماشین مجازی

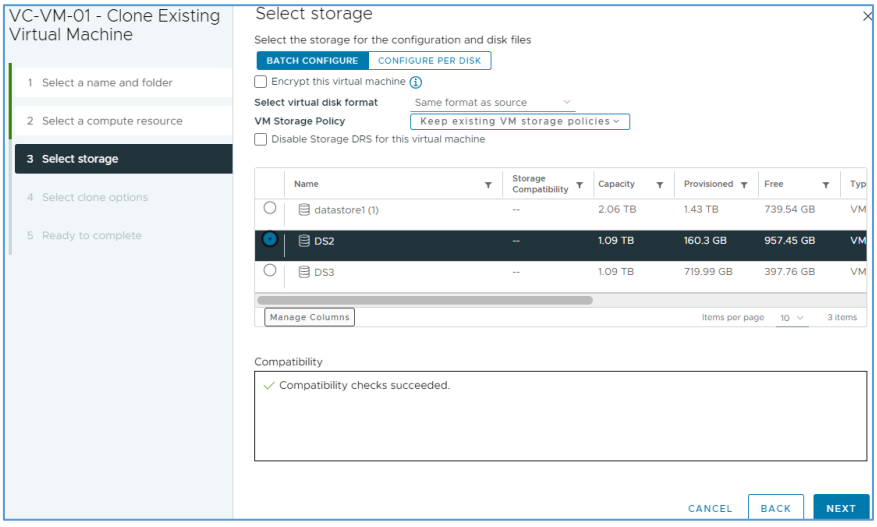
در شکل ۱۲-۷٤، باید هاست مورد نظر خود را انتخاب کنید تا Clone مورد نظر در زیرمجموعه آن قرار بگیرد، ما یک سرور جدید که ESXi ورژن ۸ دارد را انتخاب می‌کنیم.

www.takbook.com



شکل ۱۲- ۷۴ ایجاد Clone از ماشین مجازی

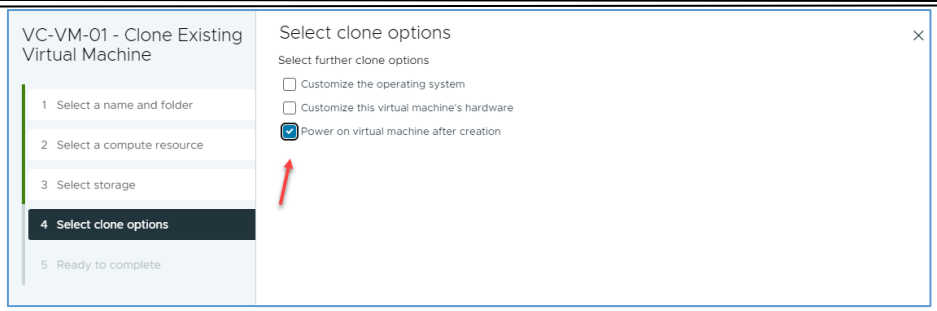
در شکل ۱۲-۷۵، DataStore را انتخاب و بر روی Next کلیک کنید.



شکل ۱۲- ۷۵ ایجاد Clone از ماشین مجازی

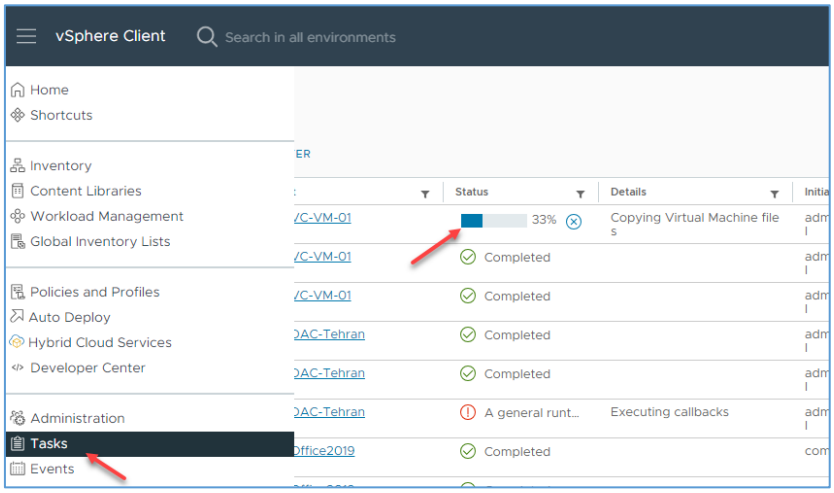
درشکل ۱۲-۷۶، اگر چنانچه می‌خواهید ورژن دیگری از ویندوز را برای Clone خود انتخاب کنید باید تیک گزینه‌ی اول را انتخاب کنید، برای تغییر تنظیمات سخت‌افزاری مانند رم و .. تیک گزینه‌ی دوم را انتخاب کنید و در آخر برای روشن کردن سیستم تیک گزینه‌ی آخر را هم انتخاب کنید، در صفحه بعد هم بر روی FINISH کلیک کنید تا Clone مورد نظر ایجاد شود.

www.takbook.com



شکل ۱۲- ۷۶ ایجاد Clone از ماشین مجازی

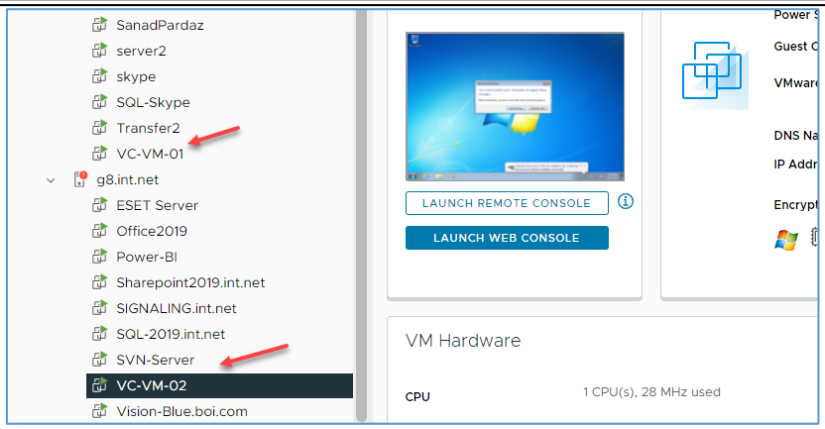
اگر به مانند شکل ۱۲-۷۷، در Vcenter وارد Task شوید تمام عملیاتی که در Vcenter انجام شده و در حال انجام است نمایش داده شده است، اگر خط اول آن توجه کنید نوشته Clone virtual که در حال Clone گرفتن از ماشین VM1 است.



شکل ۱۲- ۷۷ ایجاد Clone از ماشین مجازی

بعد از اتمام کار ماشین جدید در سرور ESXi جدید کپی شده است و می‌توانید از آن استفاده کنید که این موضوع را در شکل ۱۲-۷۸، مشاهده می‌کنید.

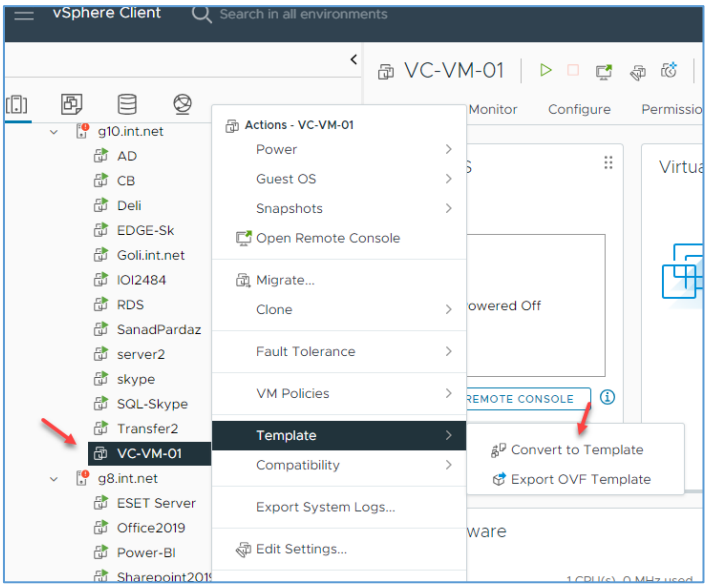
www.takbook.com



شکل ۱۲- ۷۸ ایجاد Clone از ماشین مجازی

۱۲-۶ کار با Template در Vcenter

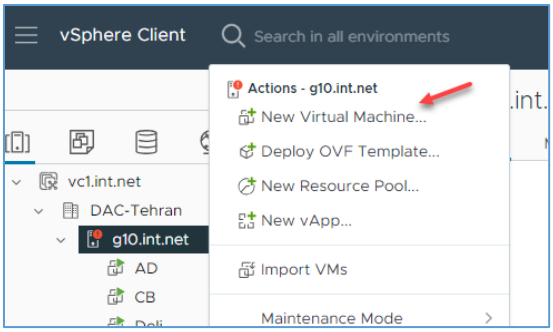
برای اینکه چندین بار نیاز نداشته باشیم که سیستم‌عامل نصب کنیم و از همان سیستم عاملی که نصب کردیم به دفعات چندین نسخه ایجاد کنیم، برای این کار ماشین مجازی مورد نظر خود را خاموش کنید و به مانند شکل ۱۲-۷۹، بر روی ماشین مجازی خود کلیک راست کنید و از قسمت Template گزینه‌ی Convert to Template را انتخاب کنید، به این نکته هم توجه کنید با انتخاب این گزینه این ماشین از لیست اصلی حذف و به لیست Template اضافه خواهد شد.



شکل ۱۲- ۷۹ ایجاد Template در vCenter

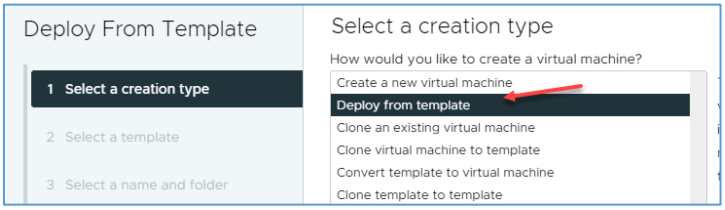
www.takbook.com

بعد از تبدیل ماشین به Template در زیر مجموعه هاست G10.int.net ماشین مورد نظر که از آن Template ایجاد کردیم حذف خواهد شد. برای اینکه بتوانیم از Template موجود یک ماشین مجازی جدید ایجاد کنیم، باید به مانند شکل ۱۲-۸۰، روی نام سرور کلیک راست کنید و گزینه‌ی New را انتخاب کنیم.



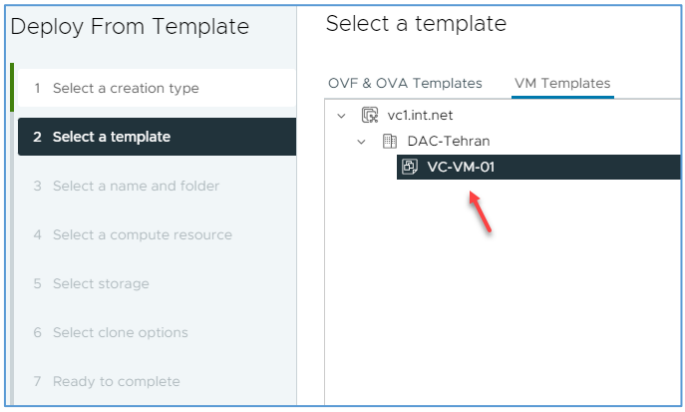
شکل ۱۲- ۸۰ ایجاد Template در vCenter

در شکل ۱۲-۸۱، برای ایجاد ماشین مجازی از روی Template گزینه‌ی Depoly from template را انتخاب کنید.



شکل ۱۲- ۸۱ ایجاد Template در vCenter

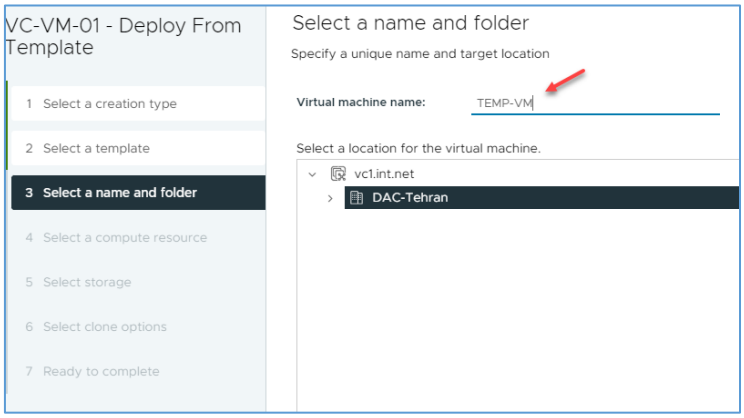
در شکل ۱۲-۸۲، وارد تب VM Templates شوید و ماشین مورد نظر را که در Data Center مورد نظر خود قرار دادید انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۲- ۸۲ ایجاد Template در vCenter

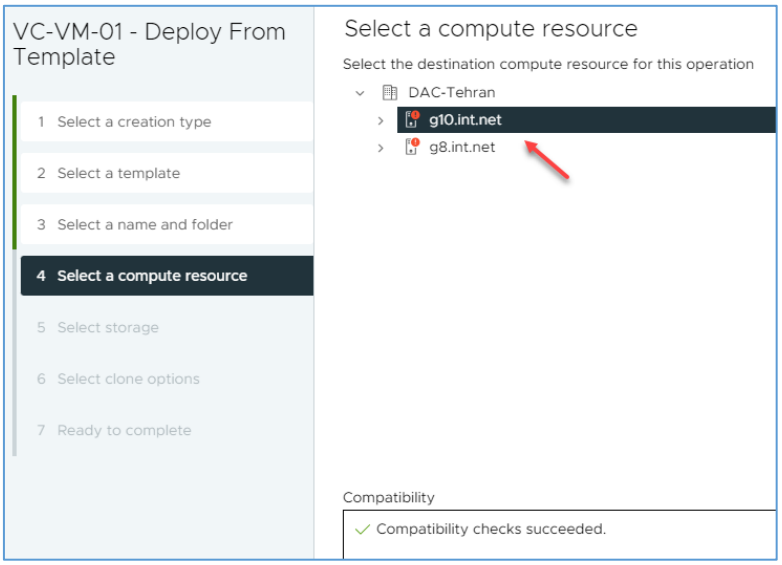
www.takbook.com

در شکل ۱۲-۸۳، نام ماشین مجازی خود را که یک ماشین جدید است انتخاب کنید و در زیر آن Data Center آن را انتخاب و بر روی Next کلیک کنید.



شکل ۱۲-۸۳ ایجاد Template در vCenter

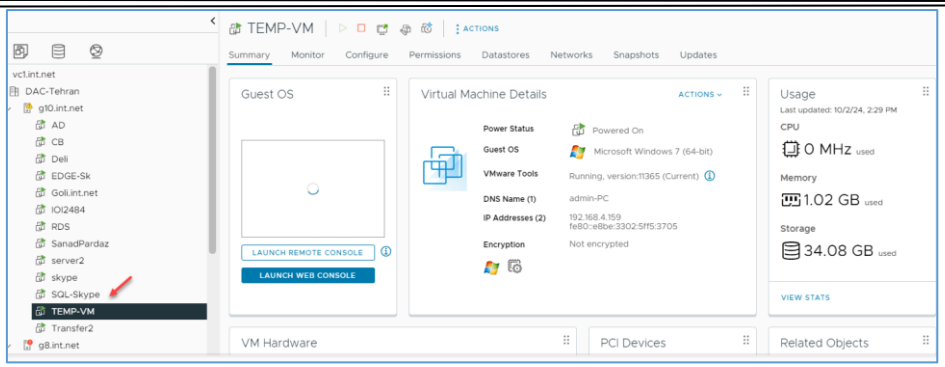
در شکل ۱۲-۸٤، باید هاست ESXi مورد نظر خود را انتخاب کنید تا ماشین بر روی آن قرار گیرد، در صفحه بعد هم DataStore مورد نظر را انتخاب کنید و در صفحه بعدی هم تنظیمات مربوط به ماشین مورد نظر را انجام دهید و در آخر بر روی Finish کلیک کنید.



شکل ۱۲-۸۴ ایجاد Template در vCenter

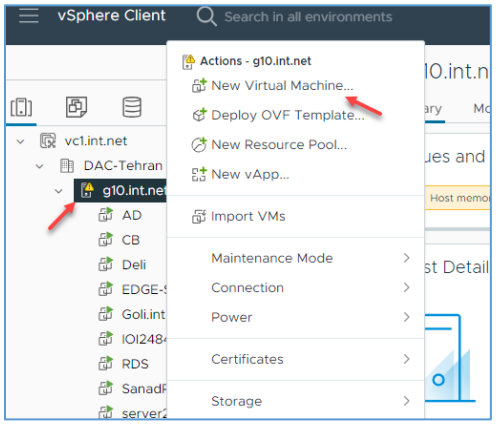
همان‌طور که در شکل ۱۲-۸۵، مشاهده می‌کنید ماشین مورد نظر از روی Template که درست کردیم ایجاد شده است و می‌توانید تنظیمات خود را بر روی آن انجام دهید.

www.takbook.com



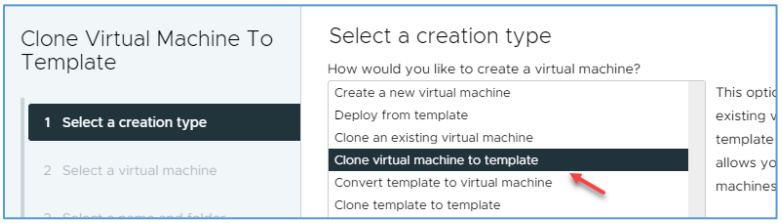
شکل ۱۲- ۸۵ ایجاد *Template* در *vCenter*

روش دیگری هم وجود دارد که بتوانید بدون تبدیل مستقیم ماشین به Template از آن یک کپی تهیه کرد و اصل ماشین را در لیست ESXi حفظ کرد، برای این کار به مانند شکل ۱۲-۸٦، بر روی New Virtual Machine کلیک کنید.



شکل ۱۲- ۸۶ ایجاد *Template* در *vCenter*

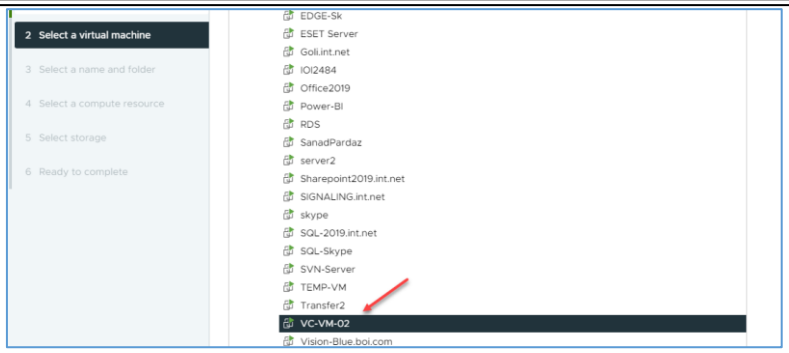
در شکل ۱۲-۸۷، گزینه‌ی Clone virtual machine to template را انتخاب کنید.



شکل ۱۲- ۸۷ ایجاد *Template* در *vCenter*

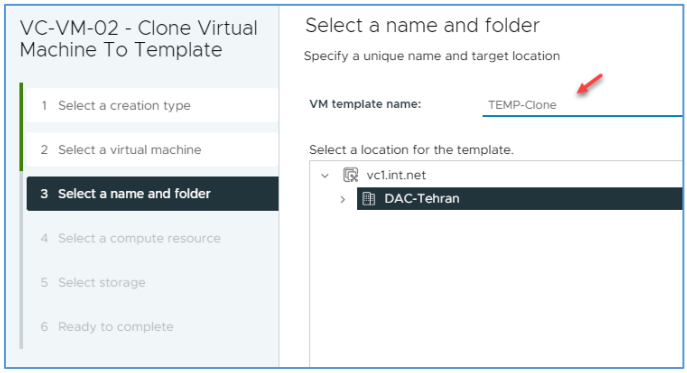
در شکل ۱۲-۸۸، ماشین مورد نظر خود را برای تبدیل شدن به Template انتخاب کنید.

www.takbook.com



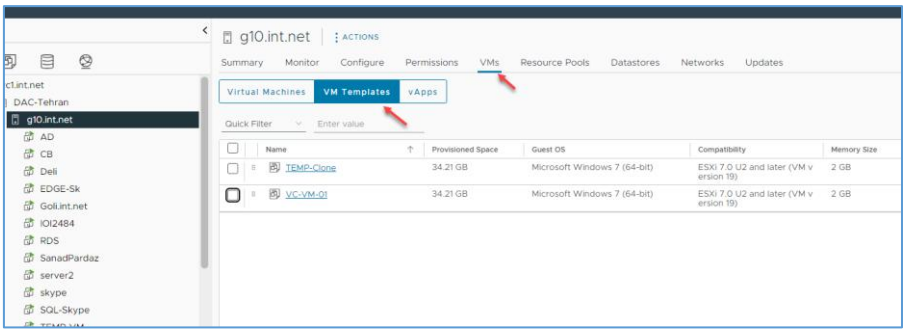
شکل ۱۲- ۸۸ ایجاد *Template* در *vCenter*

به مانند شکل ۱۲-۸۹، نام جدید را وارد و بر روی Next کلیک کنید، در صفحات بعد هم تنظیمات را به مانند قسمت‌های قبلی انجام دهید و بر روی Finish کلیک کنید.



شکل ۱۲- ۸۹ ایجاد *Template* در *vCenter*

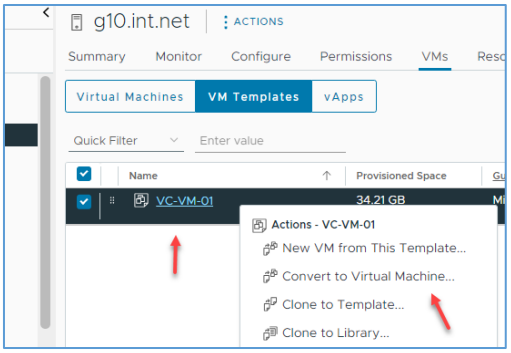
برای اینکه ماشین‌های مجازی را به همراه Template آن مشاهده کنید باید به ملنند شکل ۱۲-۹۰، وارد تب VMs شوید و دوباره تب VM Templates in Folders را انتخاب کنید، همان‌طور که مشاهده می‌کنید ماشین VC-VM-01 حذف نشده است و ماشین Temp-Clone را در لیست مشاهده می‌کنید.



شکل ۱۲- ۹۰ ایجاد *Template* در *vCenter*

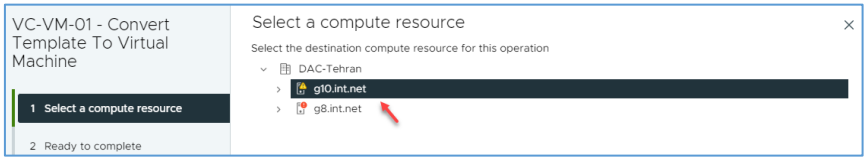
www.takbook.com

به مانند شکل ۱۲-۹۱، اگر بر روی ماشین مجازی Template در لیست مورد نظر کلیک راست کنید، گزینه‌هایی را در دسترس شما قرار می‌دهد، مثلاً برای تبدیل Template به ماشین مجازی واقعی گزینه‌ی Convert to Virtual Machine را انتخاب کنید و ماشین مورد نظر خود را ایجاد کنید.



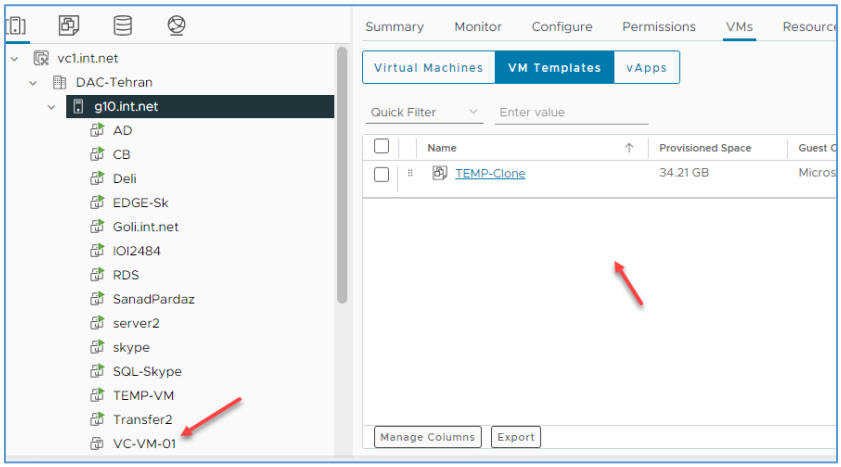
شکل ۱۲- ۹۱ ایجاد Template در vCenter

در شکل ۱۲-۹۲، باید هاست ESXi مورد نظر خود را انتخاب و بر روی Next و بعد بر روی Finish کلیک کنید.



شکل ۱۲- ۹۲ ایجاد Template در vCenter

همان‌طور که در شکل ۱۲-۹۳، مشاهده می‌کنید ماشین VC-VM-01 از لیست Template حذف شده و به لیست اصلی و به عنوان ماشین مجازی فعال شده است.



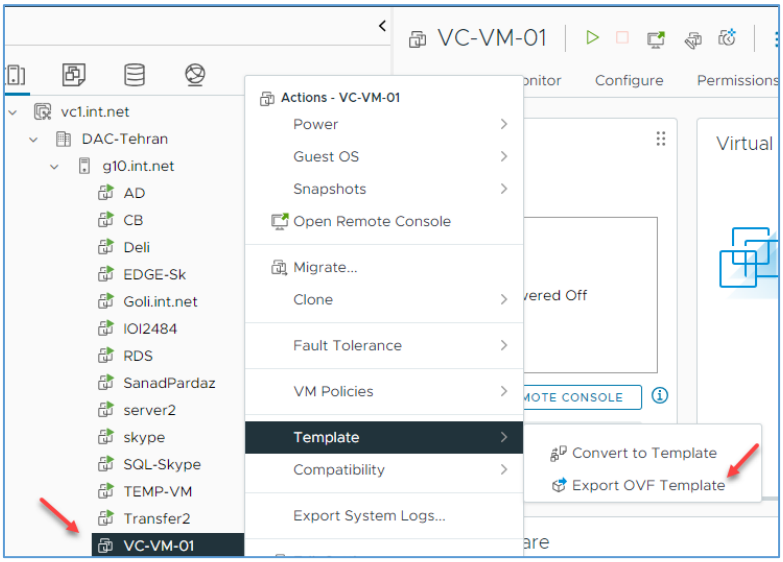
شکل ۱۲- ۹۳ ایجاد Template در vCenter

www.takbook.com

۱۲-۷ ایجاد فایل OVF از ماشین مجازی در Vcenter

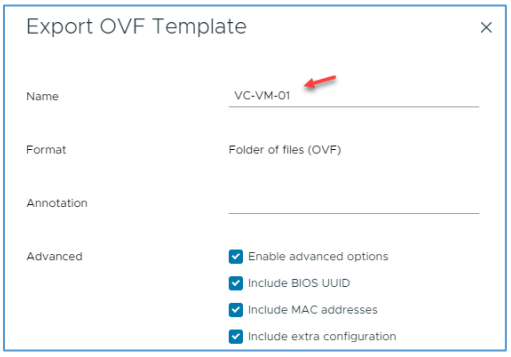
در این قسمت می‌خواهیم از ماشین‌های مجازی یک فایل OVF ایجاد کنیم و از این فایل در سرورها و نرم‌افزارهای دیگر استفاده کنیم.

برای انجام این کار به مانند شکل ۱۲-۹٤، بر روی ماشین مجازی یا Template مورد نظر کلیک راست کنید و از قسمت Template گزینه‌ی Export OVF Template را انتخاب کنید.



شکل ۱۲- ۹۴ ایجاد فایل OVF از ماشین مجازی

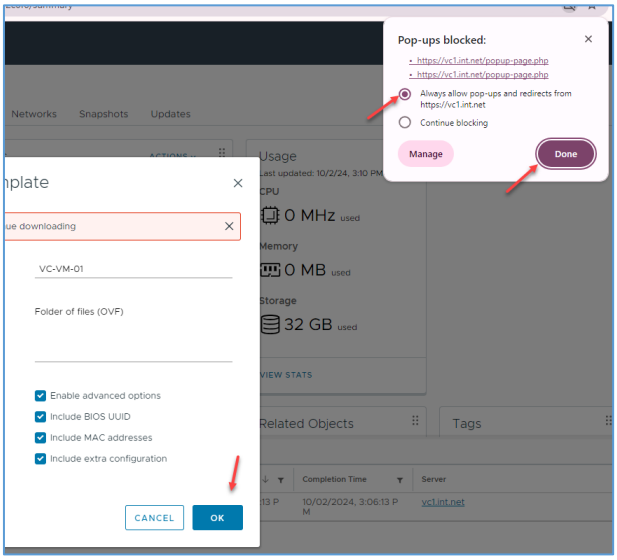
در شکل ۱۲-۹۵، می‌توانید نام ماشین مورد نظر را تغییر دهید، اگر می‌خواهید اطلاعات Bios، آدرس MAC و تنظیمات ماشینی که از آن در حال تهیه OVF هستید حفظ شود می‌توانید تیک مورد نظر آنها را انتخاب کنید.



شکل ۱۲- ۹۵ ایجاد فایل OVF از ماشین مجازی

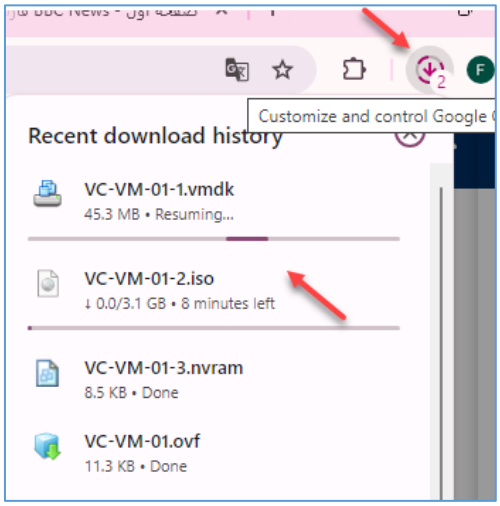
www.takbook.com

بعد از اینکه در قسمت قبل بر روی OK کلیک کردید فایل‌های مورد نظر دانلود خواهند شد و برای اینکه اجازه دانلود داده شود به مانند شکل ۱۲-۹۶، باید به پنجره‌های PopUP اجازه و دسترسی دهید.



شکل ۱۲- ۹۶ ایجاد فایل OVF از ماشین مجازی

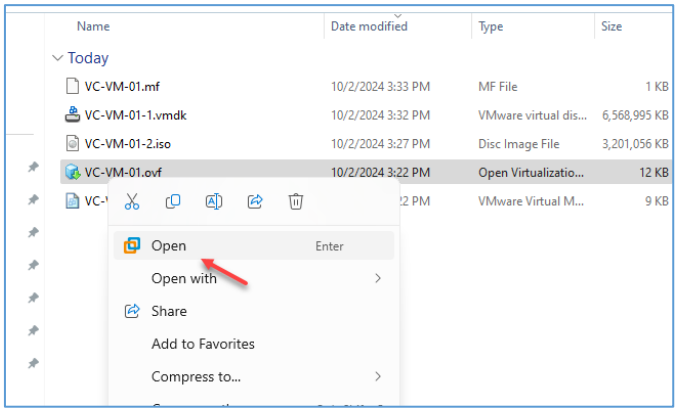
همان‌طور که در شکل ۱۲-۹۷، مشاهده می‌کنید تمام فایل‌های ماشین مجازی در حال دانلود شدن است.



شکل ۱۲- ۹۷ ایجاد فایل OVF از ماشین مجازی

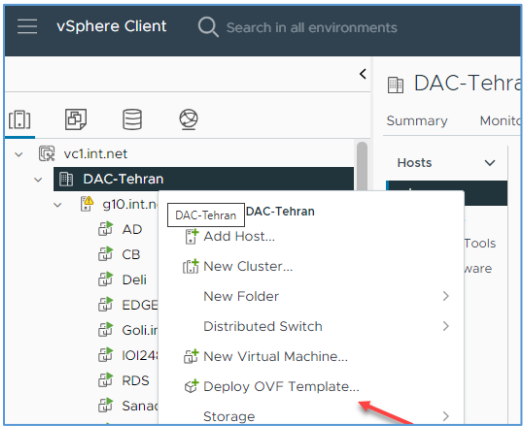
www.takbook.com

به مانند شکل ۱۲-۹۸، بعد از دانلود اگر وارد فولدر مورد نظر شوید فایل‌های مورد نظر را مشاهده می‌کنید، اگر بر روی فایل OVF کلیک راست کنید می‌توانید آن را بر روی VMware Workstation اجرا کنید، که این مبحث را در فصل ششم به صورت کامل بررسی کردیم.



شکل ۱۲- ۹۸ ایجاد فایل OVF از ماشین مجازی

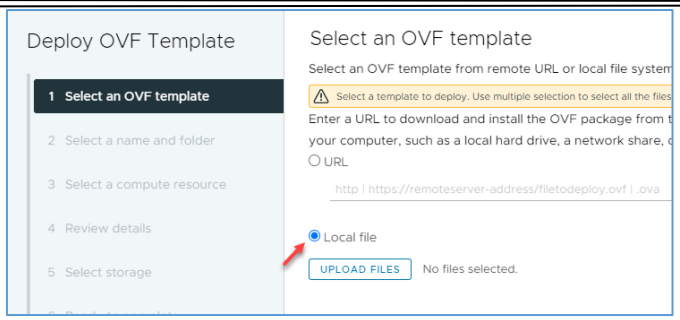
برای اینکه بتوانید فایل با پسوند OVF را در ESXi اجرا کنید باید به مانند شکل ۱۲-۹۹، در Vcenter بر روی Data Center مورد نظر کلیک راست کنید و گزینه‌ی Depoly OVF Template را انتخاب کنید.



شکل ۱۲- ۹۹ ایجاد فایل OVF از ماشین مجازی

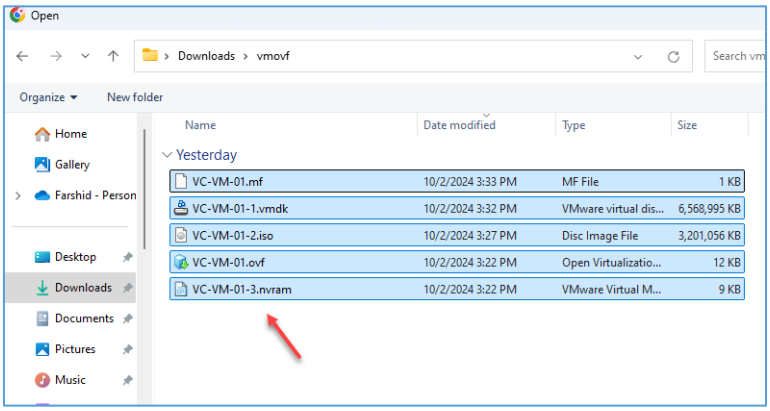
در شکل ۱۲-۱۰۰، گزینه‌ی Local file را انتخاب و بر روی Browse کلیک کنید.

www.takbook.com



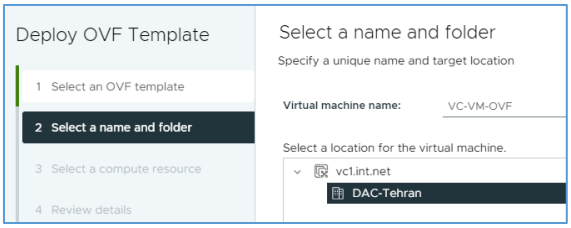
شکل ۱۲- ۱۰۰ ایجاد فایل OVF از ماشین مجازی

در شکل ۱۲-۱۰۱، باید توجه داشته باشید که همه فایل‌های موجود در پوشه را که در قسمت قبل دانلود کردیم انتخاب کنید، وگرنه با مشکل مواجه خواهید شد، بعد از انتخاب بر روی open کلیک و بعد بر روی Next کلیک کنید.



شکل ۱۲- ۱۰۱ ایجاد فایل OVF از ماشین مجازی

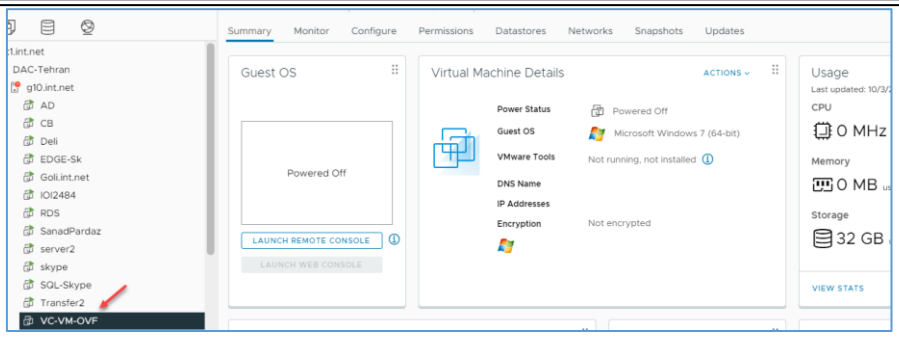
در شکل ۱۲-۱۰۲، نام مورد نظر را وارد کنید، در صفحات بعد هم بر روی Next کلیک کنید و در آخر بر روی Finish کلیک کنید تا ماشین مورد نظر ایجاد شود.



شکل ۱۲- ۱۰۲ ایجاد فایل OVF از ماشین مجازی

همان‌طور که در شکل ۱۲-۱۰۳، مشاهده می‌کنید ماشین مورد نظر Deploy شده و اگر به پایین صفحه توجه کنید ماشین مورد نظر در حال Import است.

www.takbook.com

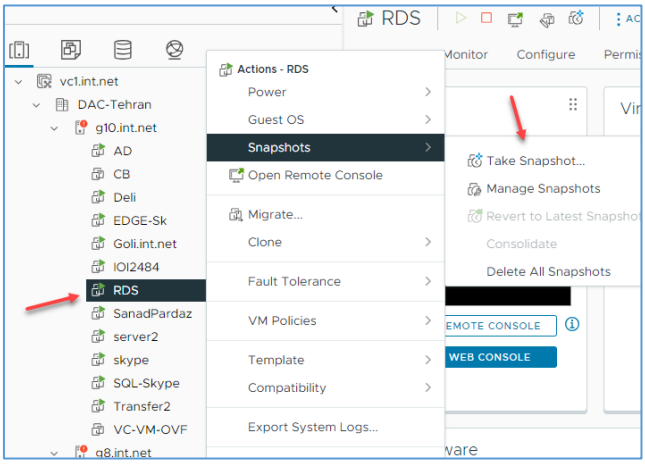


شکل ۱۲-۱۰۳ ایجاد فایل OVF از ماشین مجازی

۱۲-۸ کار با SnapShots در Vcenter

یکی از دیگر از راه‌کارهای حفظ اطلاعات ماشین‌ها، استفاده از Snapshot در فواصل زمانی مشخص است که این مبحث را در قسمت‌های قبلی بررسی کردیم.

برای شروع کار به مانند شکل ۱۲-۱۰۴، بر روی ماشین مورد نظر کلیک راست کنید و از قسمت Snapshots گزینه‌ی Take Snapshot را انتخاب کنید.

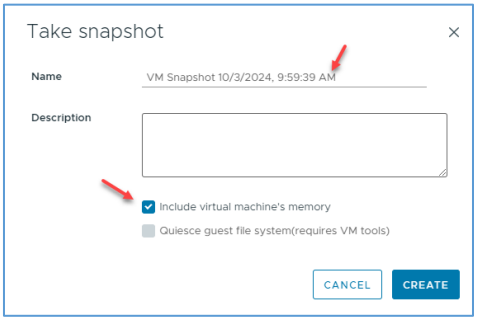


شکل ۱۲-۱۰۴ کار با SnapShots در Vcenter

در شکل ۱۲-۱۰۵، می‌توانید نام Snapshot خود را وارد کنید که به صورت پیش‌فرض یک نام به همراه تاریخ و ساعت مشخص شده است، اگر گزینه‌ی Snapshot the virtual machine's memory را انتخاب کنید در صورت روشن بودن ماشین، هر گونه اطلاعاتی را که در رم قرار دارد یعنی اینکه هر نرم‌افزار یا فایلی باز باشد به همان صورت اول آن را به هارد دیسک انتقال می‌دهد و بعد از روی آن Snap تهیه می‌کند، توجه داشته باشد اگر نیاز به برگشت Snapshot باشد همه فایل‌های باز دقیقاً به همان صورت برگشت داده خواهد شد، اما اگر گزینه‌ی Quiesce guest file system (needs VMware tools installed) را انتخاب کنید،

www.takbook.com

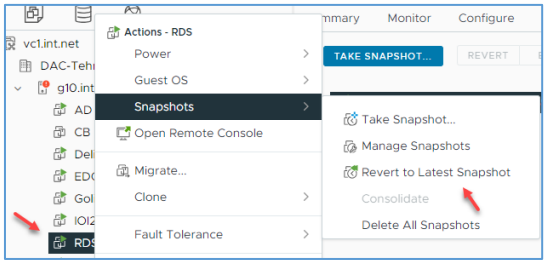
باعث می‌شود که نوشتن در آن زمان در هارد دیسک متوقف شود و Snapshot گرفته شود والبته به این نکته مهم باید دقت کنید که حتماً باید بر روی ماشین مجازی VMware Tools نصب شده باشد، این پشتیبان‌گیری بیشتر برای نرم‌افزارهای Veeam و امثال آنها کاربرد دارد، برای فعال کردن آن باید تیک گزینه‌ی اول را بردارید ولی اگر گزینه‌ی اول فعال باشد انتخاب خوبی برای ماشین شما خواهد بود.



شکل ۱۲- ۱۰۵ کار با SnapShots در Vcenter

نکته مهم اینکه اگر هر دو تیک این دو گزینه را بردارید، اگر از ماشین مورد نظر پشتیبان تهیه شود در زمان بازگشت ماشین مورد نظر خاموش خواهد بود که به این حالت Crash-consistent هم می‌گویند.

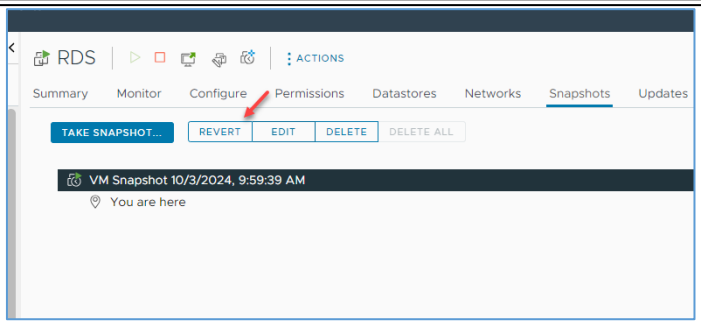
بعد از انجام Snapshot، برای اینکه ماشین مجازی خود را به همان تاریخ مورد نظر برگردانید باید به مانند شکل ۱۲-۱۰۶، بر روی Revert to Last Snapshot کلیک کنید، توجه داشته باشید این گزینه فقط آخرین Snapshot را برمی‌گرداند و برای اینکه Snapshot را در تاریخ مشخص انتخاب کنید باید بر روی Manage Snapshots کلیک کنید.



شکل ۱۲- ۱۰۶ کار با SnapShots در Vcenter

به مانند شکل ۱۲-۱۰۷، در Manage Snapshots می‌توانید Snapshot تاریخ مشخص شده را انتخاب و بر روی REVERT TO کلیک کنید، برای حذف آنها هم می‌توانید از کلید Delete استفاده کنید.

www.takbook.com



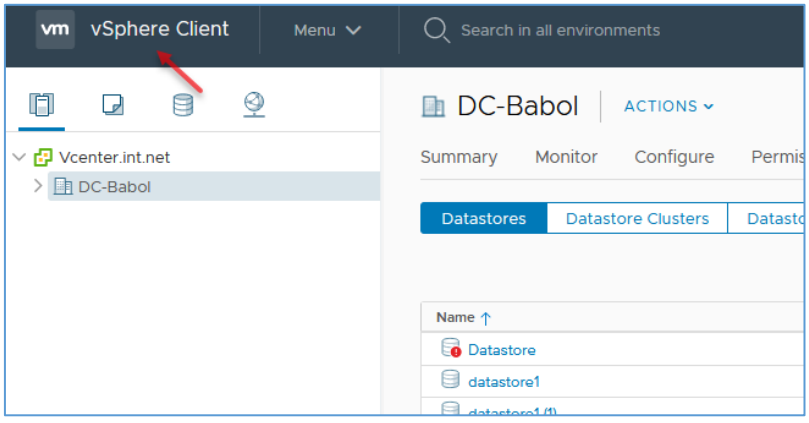
شکل ۱۲- ۱۰۷ کار با *SnapShots* در *Vcenter*

۱۲-۹ کار با Content Libraries در Vcenter

در این بخش می‌خواهیم عملکرد Content Libraries را در Vcenter بررسی کنیم، این قابلیت این امکان را به ما می‌دهد که فایل‌های ماشین‌های مجازی خود را بین یک یا چند Vcenter که می‌تواند در یک سازمان یا در شهرهای مختلف باشد انتقال دهیم، این کار می‌تواند از اتلاف وقت جلوگیری و کارها را منظم کند.

برای انجام این کار ما دو Vcenter را آماده کردیم که یکی با نام DC-Babol و دیگری با نام DC-Tehran و برای شروع کار در Vcenter مربوط به DC-Babol تنظیمات مربوط به Content Libraries را انجام می‌دهیم.

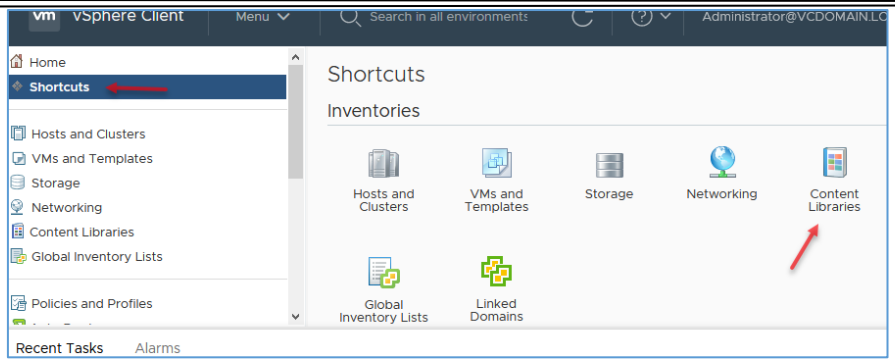
به مانند شکل ۱۲-۱۰۸، بر روی vSphere Client در بالای صفحه کلیک کنید.



شکل ۱۲- ۱۰۸ کار با *Content Libraries* در *Vcenter*

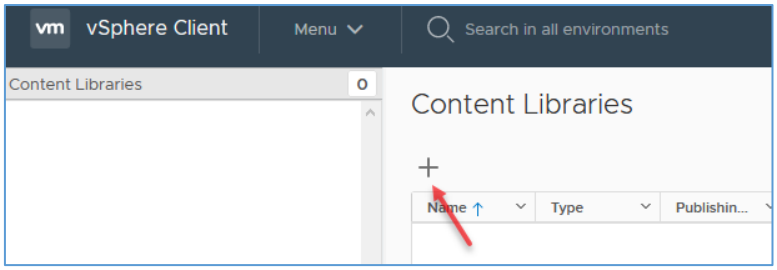
در شکل ۱۲-۱۰۹، از قسمت Shortcuts بر روی آیکون Content Libraries کلیک کنید.

www.takbook.com



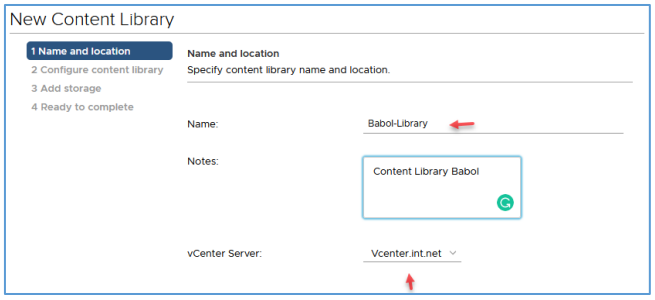
شکل ۱۲- ۱۰۹

در شکل ۱۲-۱۱۰، بر روی + کلیک کنید.



شکل ۱۲- ۱۱۰ کار با Content Libraries در Vcenter

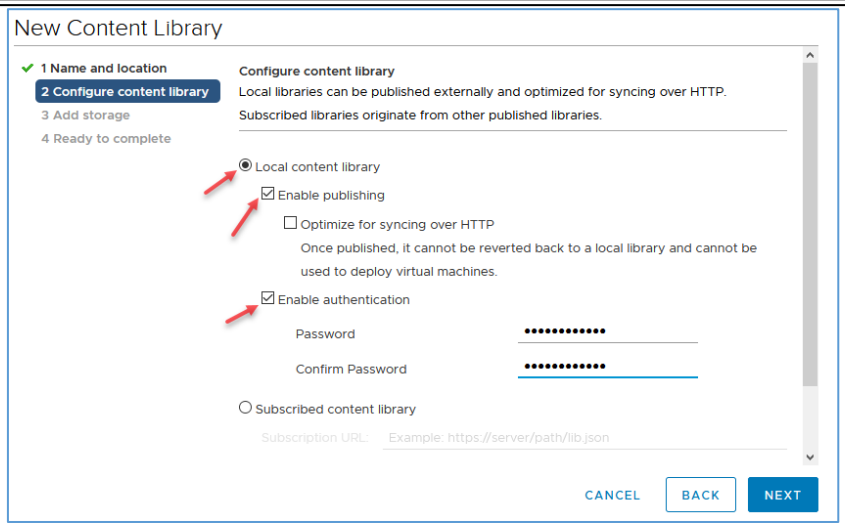
در شکل ۱۲-۱۱۱، نام مورد نظر خود را وارد کنید و بر روی Next کلیک کنید.



شکل ۱۲- ۱۱۱ کار با Content Libraries در Vcenter

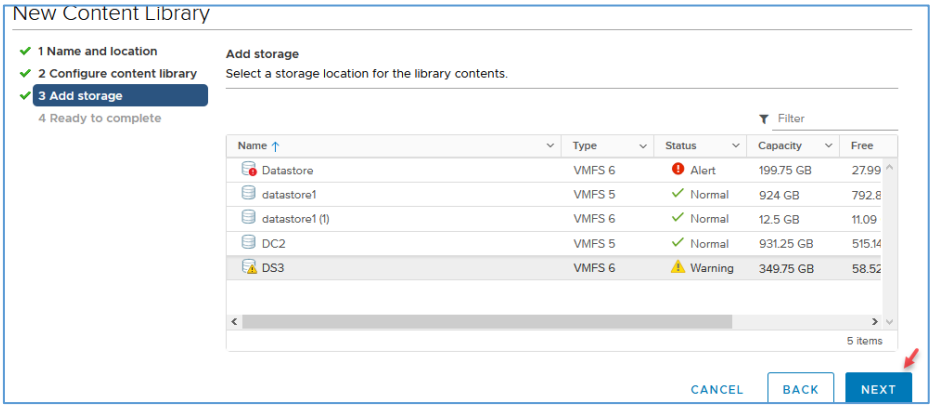
در شکل ۱۲-۱۱۲، گزینه‌ی Local content library را انتخاب کنید و تیک گزینه‌ی Enable Publishing را انتخاب کنید و برای اینکه اطلاعات بین Vcenterها با امنیت رد و بدل شود بهتر است گزینه‌ی Enable authentication را انتخاب و یک رمز پیچیده وارد کنید.

www.takbook.com



شکل ۱۲-۱۱۲ کار با Content Libraries در Vcenter

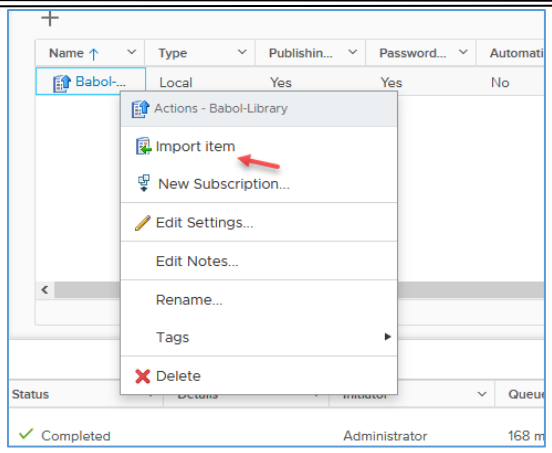
در شکل ۱۲-۱۱۳، باید یک Data Store انتخاب کنید که فضای کافی برای آپلود کردن فایل‌ها داشته باشد، بهتر است یک DataStore مجزا برای این کار قرار دهید تا با کمبود فضا مواجه نشوید، بعد از انتخاب بر روی Next کلیک و در صفحه بعد بر روی Finish کلیک کنید.



شکل ۱۲-۱۱۳ کار با Content Libraries در Vcenter

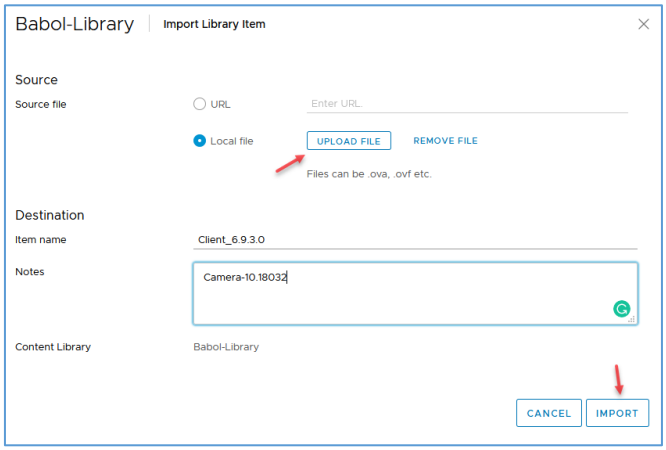
بعد از ایجاد Content Library به مانند شکل ۱۲-۱۱۴، بر روی آن کلیک راست کنید و گزینه‌ی Import item را انتخاب کنید.

www.takbook.com



شکل ۱۲- ۱۱۴ کار با Content Libraries در Vcenter

در شکل ۱۲-۱۱۵، می‌توانید آدرس فایل و یا خود فایل را از سیستم خود انتخاب کنید که این کار را باید با کلیک کردن بر روی UPLOAD FILE انجام دهید، بعد از این کار می‌توانید نام و توضیحات آن را تغییر دهید و بر روی IMPORT کلیک کنید.

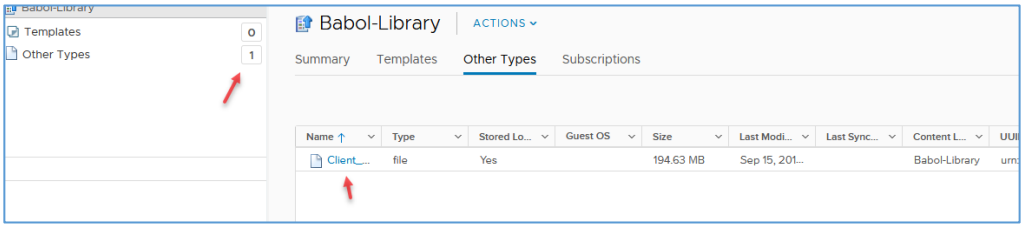


شکل ۱۲- ۱۱۵ کار با Content Libraries در Vcenter

همان‌طور که در شکل ۱۲-۱۱۶، مشاهده می‌کنید، وارد Library مورد نظر شدیم و دو قسمت Template و Other Types را مشاهده می‌کنید، قسمت اول برای Templateهای آماده ماشین‌ها می‌باشد که با پیوند OVF

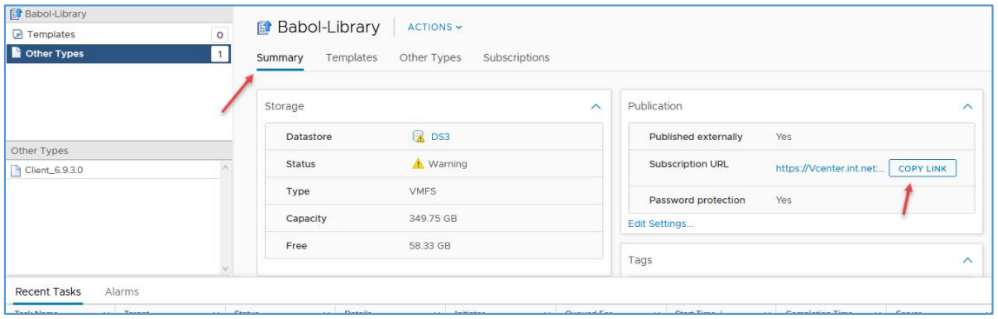
www.takbook.com

و OVA ایجاد می‌شود و قسمت دوم برای نوع‌های دیگر فایل‌ها است، که همان‌طور که مشاهده می‌کنید فایلی که آپلود کردیم چون از نوع EXE بوده در قسمت دوم قرار گرفته است.



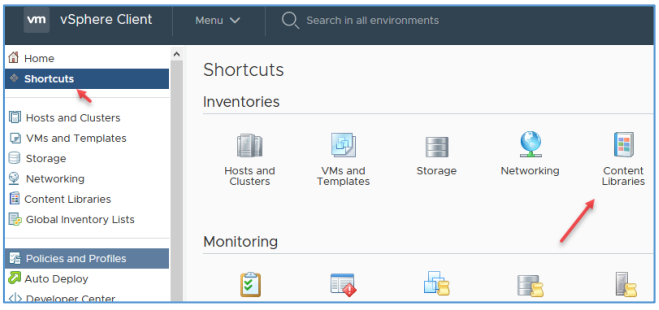
شکل ۱۲- ۱۱۶ کار با *Content Libraries* در *Vcenter*

در ادامه باید به Vcenter دوم اعلام کنیم که اطلاعات Content Library را از Vcenter مربوط به DC-Babol دریافت کنید برای این کار باید در Vcenter اولی که Content Library را در آن راه‌اندازی کردیم، یک آدرس با عنوان Subscription دریافت کنیم، برای این کار به مانند شکل ۱۲-۱۱۷، وارد تب Summary شوید و از قسمت Publication بر روی COPY LINK کلیک کنید.



شکل ۱۲- ۱۱۷ کار با *Content Libraries* در *Vcenter*

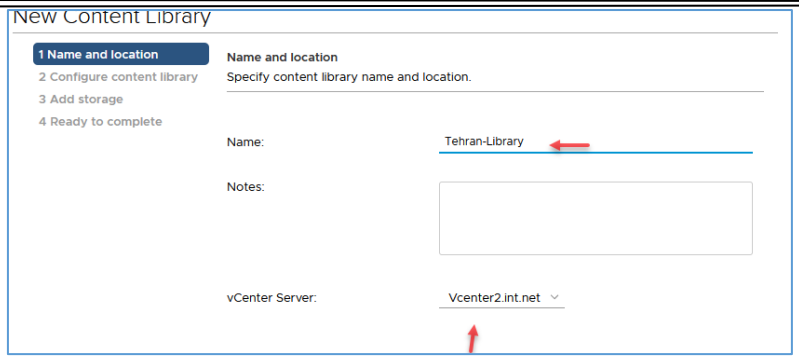
در Vcenter دوم به مانند شکل ۱۲-۱۱۸، وارد Shortcuts شوید و بر روی Content Libraries کلیک کنید.



شکل ۱۲- ۱۱۸ کار با *Content Libraries* در *Vcenter*

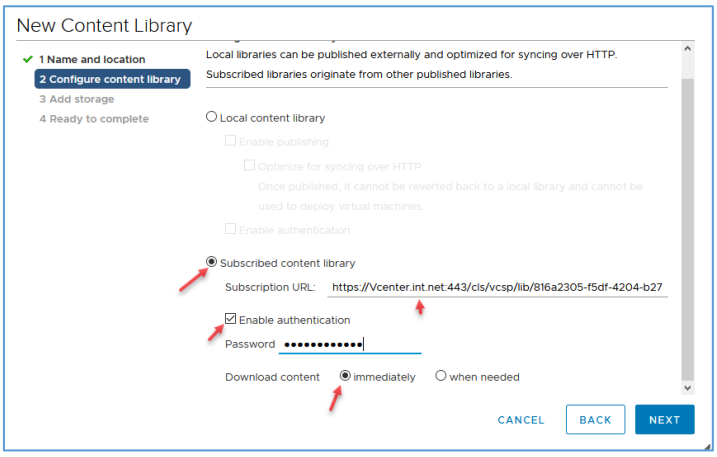
در شکل ۱۲-۱۱۹، نام مورد نظر را به دلخواه وارد کنید، همان‌طور که در قسمت Vcenter Server مشاهده می‌کنید Vcenter2 که جدیداً راه انداختیم انتخاب شده است.

www.takbook.com



شکل ۱۲- ۱۱۹ کار با *Content Libraries* در *Vcenter*

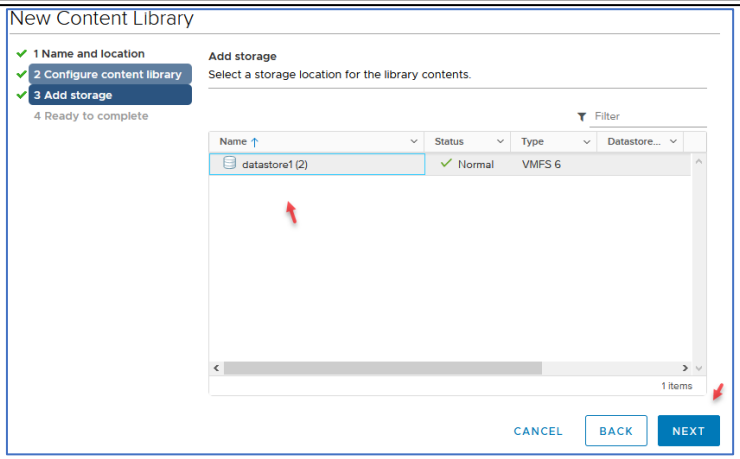
در شکل ۱۲-۱۲۰، باید گزینه‌ی Subscribed Content library را انتخاب کنید و همان آدرسی که در Vcenter قبلی کپی گرفتید در این قسمت وارد کنید، بعد از این کار باید تیک گزینه‌ی Enable authentication را انتخاب کنید و رمز عبوری که در هنگام ایجاد Content library مربوط به DC-Babol وارد کردیم را این قسمت وارد کنید، در قسمت آخر به مانند شکل ۱۲-۱۲۰، اگر گزینه‌ی immediately را انتخاب کنید تمام اطلاعاتی که در VCenter اول قرار دارد در Vcenter دوم هم کپی می‌شود ولی اگر به این صورت نیازی به دانلود اتوماتیک ندارید می‌توانید گزینه‌ی when needed را انتخاب کنید.



شکل ۱۲- ۱۲۰ کار با *Content Libraries* در *Vcenter*

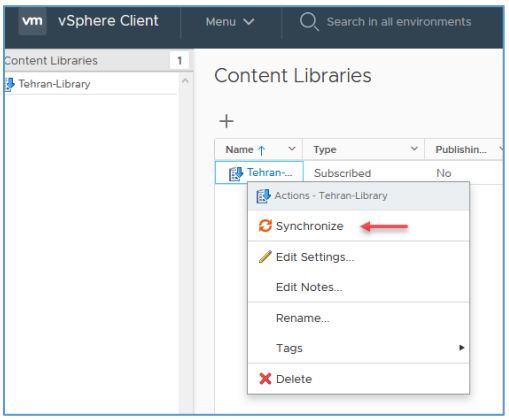
در شکل ۱۲-۱۲۱، Data Store مناسب خود را انتخاب و بر روی Next و بعد Finish کلیک کنید.

www.takbook.com



شکل ۱۲- ۱۲۱ کار با *Content Libraries* در *Vcenter*

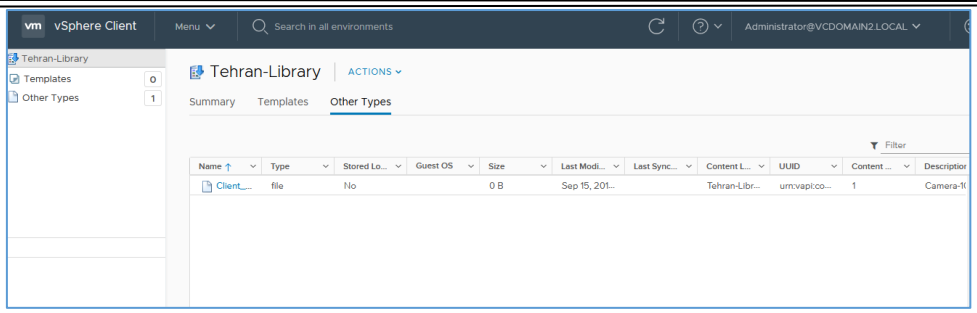
به مانند شکل ۱۲-۱۲۲، بعد از ایجاد Content Libraries اگر بر روی آن کلیک راست کنید دیگر خبری از گزینه‌ی IMPORT نیست و به جای آن گزینه‌ی Synchronize اضافه شده است که اگر بر روی آن کلیک کنید تمام اطلاعات موجود در Vcenter اول را در این Vcenter کپی خواهد کرد البته این کار در فواصل زمانی مشخص به صورت اتوماتیک انجام خواهد شد.



شکل ۱۲- ۱۲۲ کار با *Content Libraries* در *Vcenter*

همان‌طور که در شکل ۱۲-۱۲۳، مشاهده می‌کنید فایلی که در Vcenter اول آپلود کرده بودیم در این Vcenter هم قرار گرفته است.

www.takbook.com

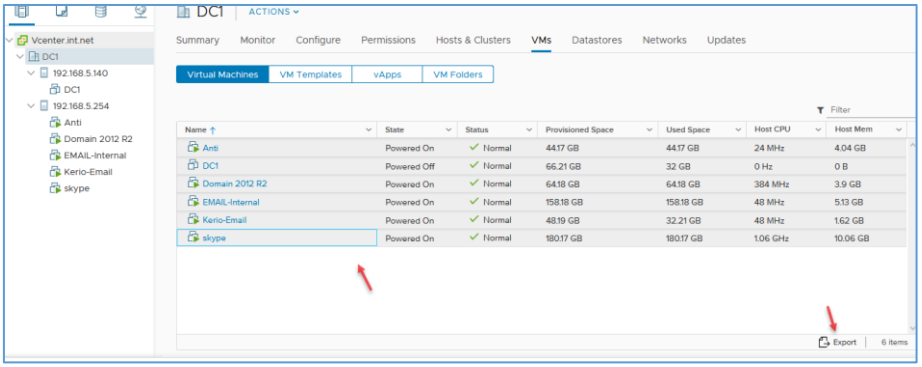


شکل ۱۲- ۱۲۳ کار با Content Libraries در Vcenter

۱۰-۱۲ ایجاد گزارش از ماشین‌های مجازی

یکی از نیازهای مدیر شبکه داشتن مشخصات کامل از سرورها و ماشین‌های مجازی است، برای همین می‌توانیم این کار را در Vcenter به راحتی انجام دهید.

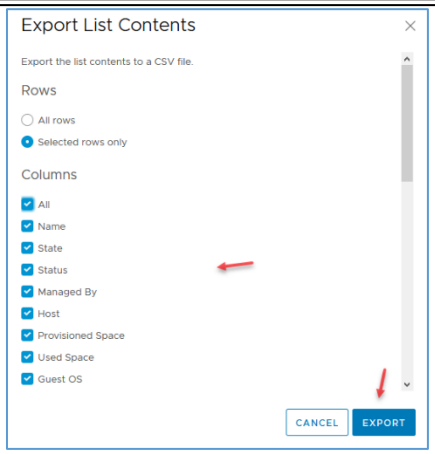
برای این کار به مانند شکل ۱۲-۱۲٤، هاست مورد نظر را انتخاب کنید و وارد تب VMs شوید و برای اینکه همه ماشین‌ها را انتخاب کنید، ماشین اول را انتخاب و کلید Shift را فشار دهید و همزمان با ماوس ماشین آخر را انتخاب کنید، بعد از انتخاب در قسمت پایین صفحه بر روی Export کلیک کنید.



شکل ۱۲- ۱۲۴ ایجاد گزارش از ماشین‌های مجازی

در شکل ۱۲-۱۲۵، می‌توانید مشخص کنید فایل خروجی اکسل دارای چه ستون‌هایی باشد که لیست آن را مشاهده می‌کنید و با انتخاب گزینه‌ی All همه آنها انتخاب خواهد شد، بعد از این کار بر روی EXPORT کلیک کنید.

www.takbook.com

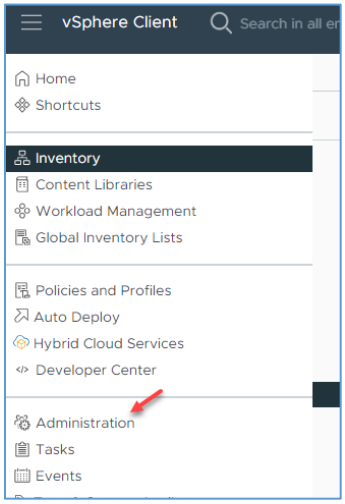


شکل ۱۲- ۱۲۵ ایجاد گزارش از ماشین‌های مجازی

بعد از این کار یک فایل اکسل با پسوند CSV دانلود خواهد شد و شامل جزئیات کاملی از سخت افزار و نرم‌افزار ماشین‌های انتخاب شده خواهد بود.

۱۲-۱۱ اتصال VCenter به Active Directory

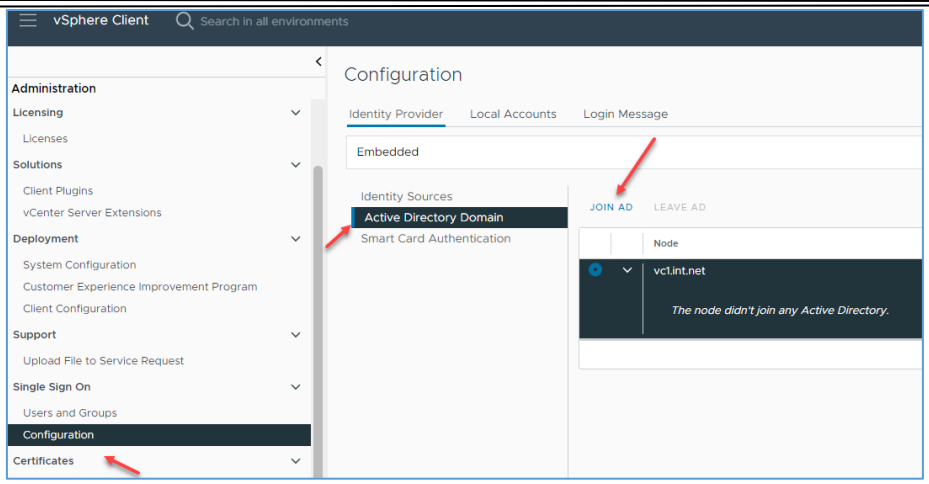
برای اتصال Vcenter به سرویس Active Directory یا همان دومین کنترلر باید به مانند شکل ۱۲-۱۲۶، وارد Administration شوید.



شکل ۱۲- ۱۲۶ اتصال VCenter به Active Directory

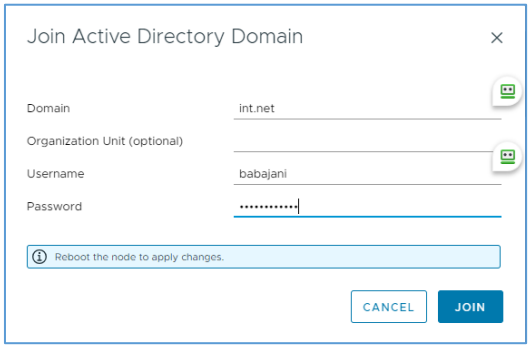
در شکل ۱۲-۱۲۷، از قسمت Single Sign On گزینه‌ی Configuration را انتخاب کنید و در صفحه باز شده گزینه‌ی Active Directory Domain را انتخاب کنید و بر روی JOIN AD کلیک کنید.

www.takbook.com



شکل ۱۲- ۱۲۷ اتصال VCenter به Active Directory

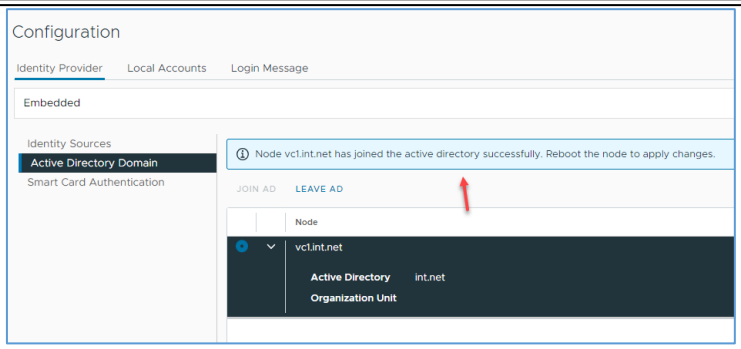
در شکل ۱۲-۱۲۸، نام دومین خود را وارد کنید و نام کاربری که دسترسی لازم را داشته باشد وارد و بر روی OK کنید.



شکل ۱۲- ۱۲۸ اتصال VCenter به Active Directory

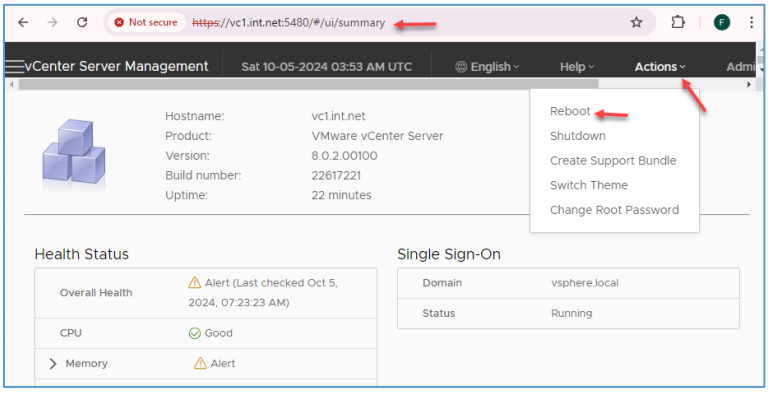
همان‌طور که در شکل ۱۲-۱۲۹، مشاهده می‌کنید سرور عضو دومین شده است و فقط نیاز دارد که آن را Restart کنید.

www.takbook.com



شکل ۱۲- ۱۲۹ اتصال VCenter به Active Directory

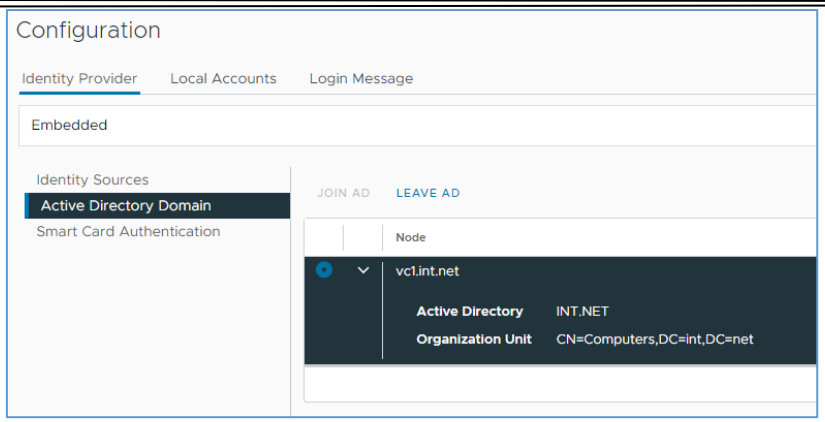
بعد از انجام این کار باید سرور Vcenter را Restart کنید که باید به مانند شکل ۱۲-۱۳۰، وارد آدرس مدیریتی شویم و از منوی Action گزینه‌ی Reboot را انتخاب کنیم.



شکل ۱۲- ۱۳۰ اتصال VCenter به Active Directory

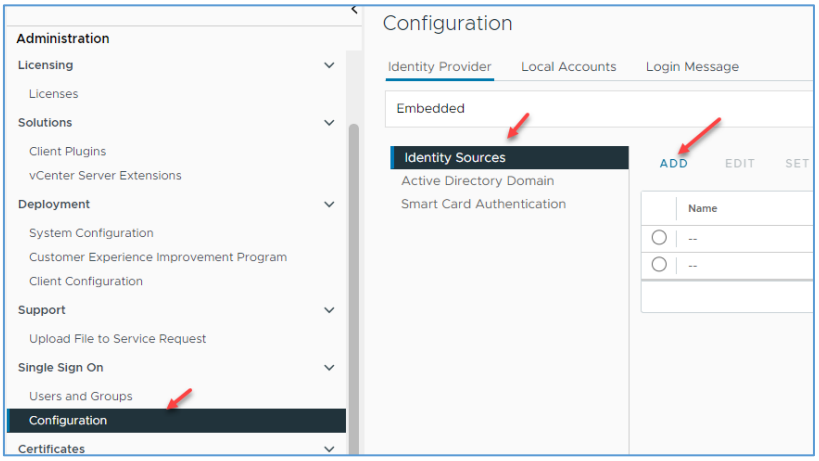
بعد از Restart کردن سرور Vcenter اگر به مانند شکل ۱۲-۱۳۱، دوباره به قسمت مشخص شده قبلی برگردید مشاهده می‌کنید که نام دومین به مانند شکل اضافه شده و دکمه Join غیرفعال شده است.

www.takbook.com



شکل ۱۲- ۱۳۱ اتصال *VCenter* به *Active Directory*

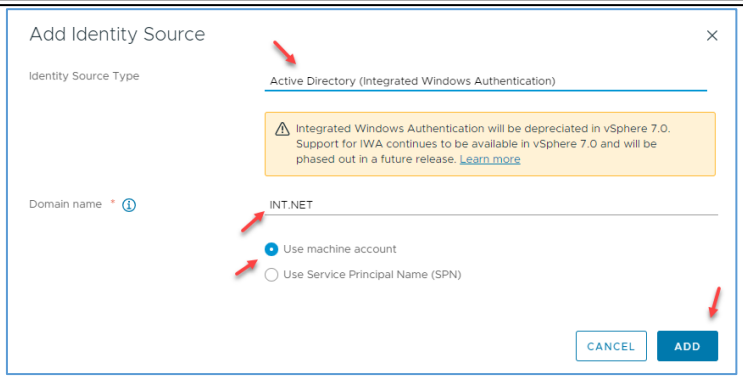
بعد از join کردن سرور Vcenter، برای اینکه نام دومین در لیست Vcenter قابل مشاهده باشد باید به مانند شکل ۱۲-۱۳۲، از سمت چپ وارد Configuration شوید و در صفحه باز شده بر روی تب Identity Source و در ادامه روی ADD کلیک کنید.



شکل ۱۲- ۱۳۲ اتصال *VCenter* به *Active Directory*

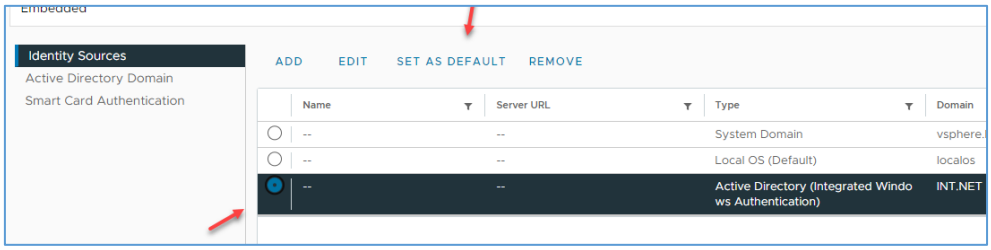
در شکل ۱۲-۱۳۳، گزینه‌ی اول را انتخاب کنید و بر روی ADD کلیک کنید، با این کار دومین مورد نظر به لیست دومین‌های در دسترس اضافه خواهد شد.

www.takbook.com



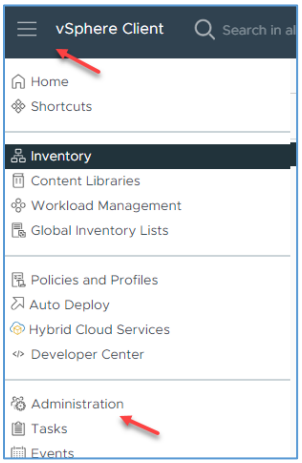
شکل ۱۲- ۱۳۳ اتصال VCenter به Active Directory

همان‌طور که در شکل ۱۲-۱۳٤، مشاهده می‌کنید دومین مورد نظر به لیست اضافه شده است و برای اینکه به عنوان دومین پیش‌فرض قرار بگیرید باید آن را انتخاب و بر روی Set As Default کلیک کنید.



شکل ۱۲- ۱۳۴ اتصال VCenter به Active Directory

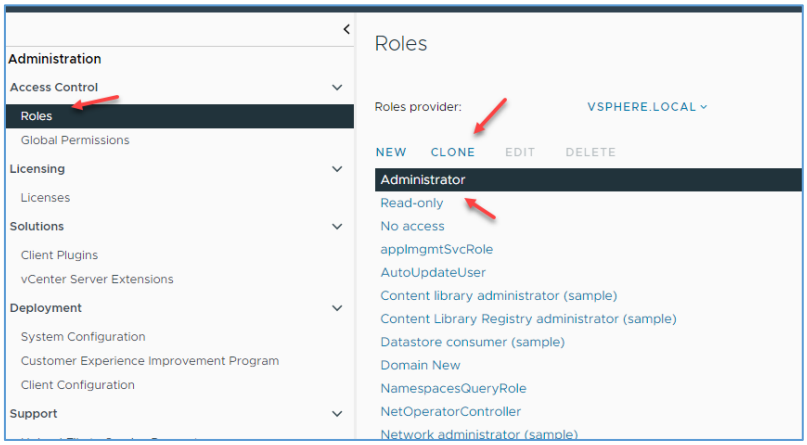
بعد از اینکه Vcenter عضو دومین شد می‌خواهیم با استفاده از نام کاربری دومین وارد Vcenter شویم، برای این کار به مانند شکل ۱۲-۱۳۵، وارد Administrator شوید.



شکل ۱۲- ۱۳۵ اتصال VCenter به Active Directory

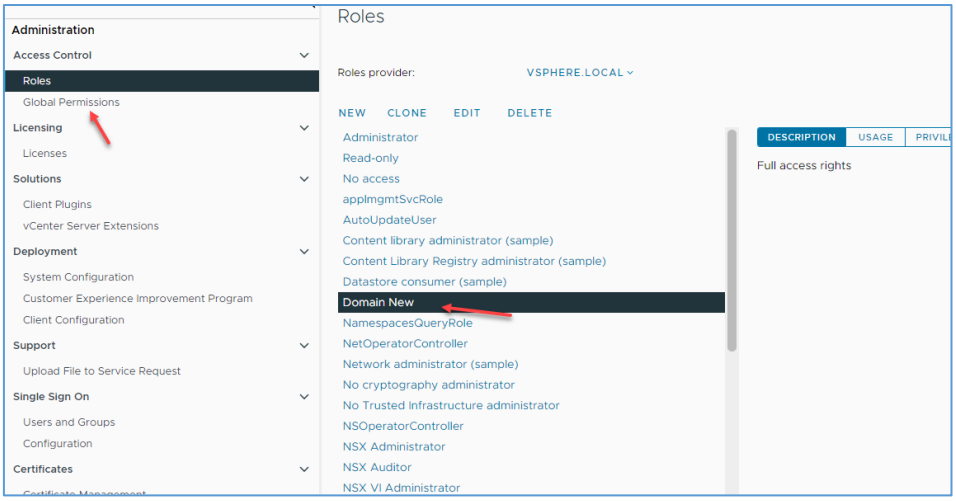
www.takbook.com

در ادامه کار به مانند شکل ۱۲-۱۳۶، وارد Role شوید و به مانند شکل Administrator را که دسترسی کامل به همه اجزای VCenter دارد انتخاب و با کلیک بر روی CLONE یک کپی از آن تهیه کنید.



شکل ۱۲- ۱۳۶ اتصال VCenter به Active Directory

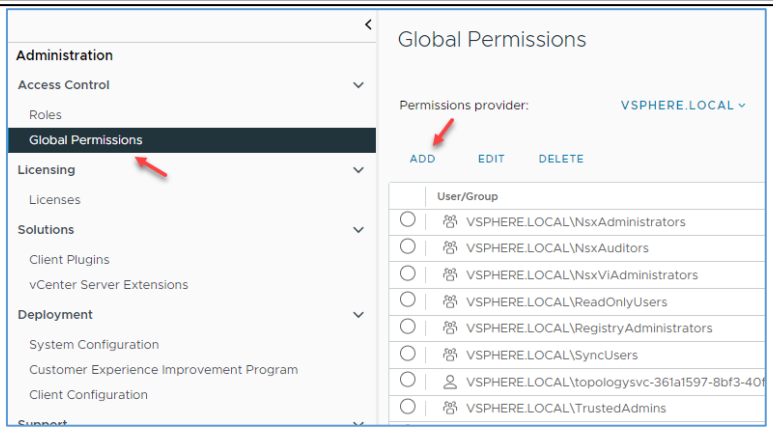
بعد از ایجاد Role جدید با نام Domain new که در شکل ۱۲-۱۳۷، مشاهده می‌کنید باید از سمت چپ وارد Global Permissions شوید.



شکل ۱۲- ۱۳۷ اتصال VCenter به Active Directory

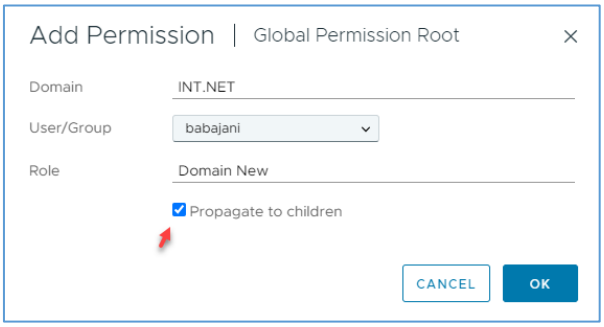
به مانند شکل ۱۲-۱۳۸، بر روی ADD کلیک کنید.

www.takbook.com



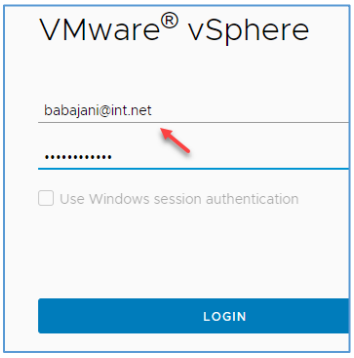
شکل ۱۲- ۱۳۸ اتصال VCenter به Active Directory

در شکل ۱۲-۱۳۹، باید از قسمت Domain نام دومین خود را انتخاب کنید و در قسمت User/Group باید نام کاربر خود را وارد و در قسمت Role هم باید همان Role جدید که با هم انتخاب کردیم را انتخاب کنید و تیک گزینه‌ی زیری آن را انتخاب کنید.



شکل ۱۲- ۱۳۹ اتصال VCenter به Active Directory

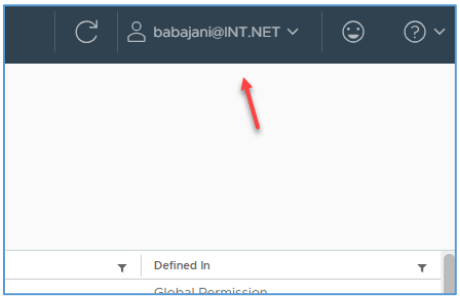
بعد از اضافه کردن کاربر دومین می‌توانید به مانند شکل ۱۲-۱۴۰، با کاربر جدید وارد Vcenter شوید.



شکل ۱۲- ۱۴۰ اتصال VCenter به Active Directory

www.takbook.com

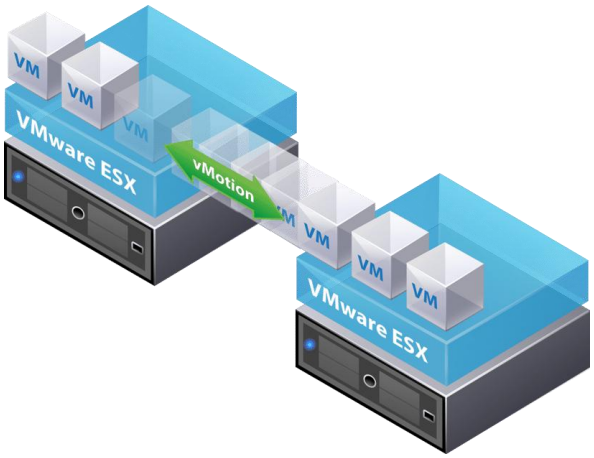
همان‌طور که در شکل ۱۲-۱٤۱، مشاهده می‌کنید توانستیم با موفقیت و با کاربر دومین وارد Vcenter شویم.



شکل ۱۲- ۱۴۱ اتصال VCenter به Active Directory

۱۲-۱۲ راه‌اندازی قابلیت Vmotion در Vcenter

یک سرور را در نظر بگیرید که بر روی آن ESXi پیاده‌سازی شده و بنا به دلایلی با مشکل مواجه شده و می‌خواهید ماشین‌های مجازی آن را به یک سرور دیگر انتقال دهید، این کار را می‌توانید با روش‌های مختلف انجام دهید، اما این نوع کار باید با امنیت و به درستی انجام شود و بهترین روش برای این کار استفاده از قابلیت Vmotion در Vcenter است، قابلیت مهم این کار این است که ماشین روشن خواهد ماند و در موقع انتقال خاموش نخواهد شد.

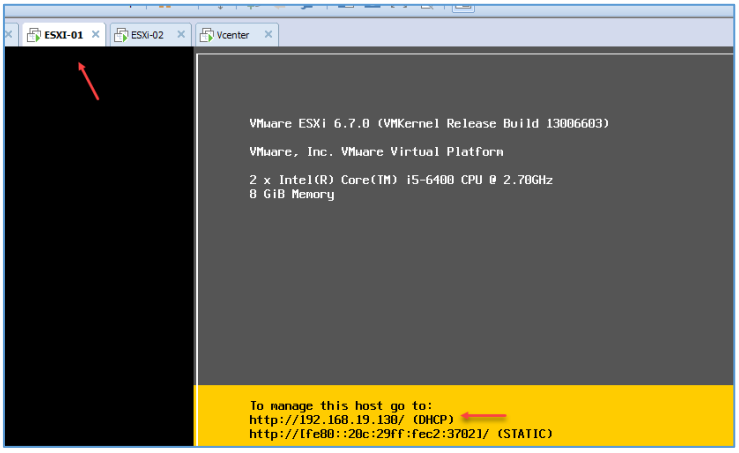


شکل ۱۲- ۱۴۲سرویس vMotion

در شکل ۱۲-۱٤۳، یک سناریو را با هم پیاده‌سازی می‌کنیم که در آن دو سرور ESXi و یک سرور Vcenter وجود دارد و ماشین با استفاده از قابلیت Vmotion و بدون اینکه خاموش شود به ESXi دوم انتقال داده خواهد شد.

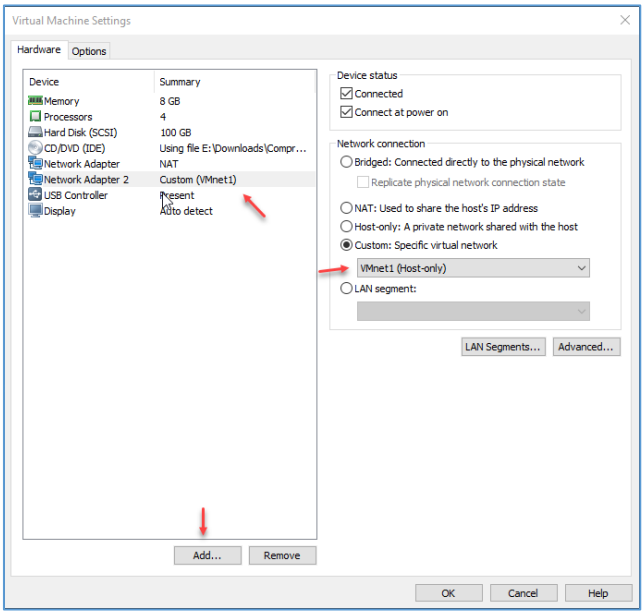
www.takbook.com

برای شروع کار باید بین دو سرور ESXi یک کارت شبکه را برای عملیات Vmotion مشخص کنیم برای همین در نرم‌افزار VMware یک کارت شبکه به هر دو سرور ESXi اضافه می‌کنیم، همان‌طور که در شکل ۱۲-۱٤۳، مشاهده می‌کنید دو ESXi و یک سرور Vcenter را مشاهده می‌کنید، بر روی ESXi-01 کلیک راست کنید و گزینه‌ی Settings را انتخاب کنید.



شکل ۱۲- ۱۴۳ راه‌اندازی قابلیت Vmotion در Vcenter

در شکل ۱۲-۱٤٤، با کلیک بر روی Add یک کارت شبکه جدید به لیست اضافه می‌کنیم و از قسمت Custom کارت شبکه‌ی VMnet1 را انتخاب می‌کنیم، شما باید همین کار را دقیقاً برای ESXi دوم هم انجام دهید.

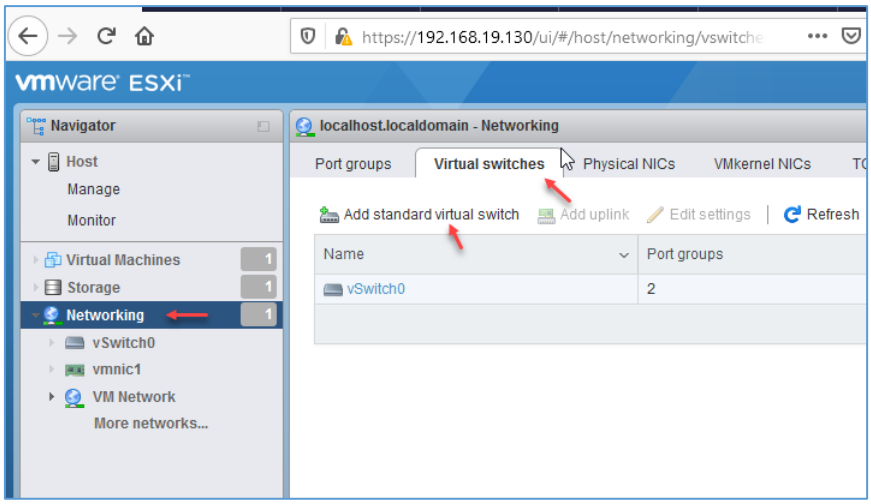


شکل ۱۲- ۱۴۴ راه‌اندازی قابلیت Vmotion در Vcenter

www.takbook.com

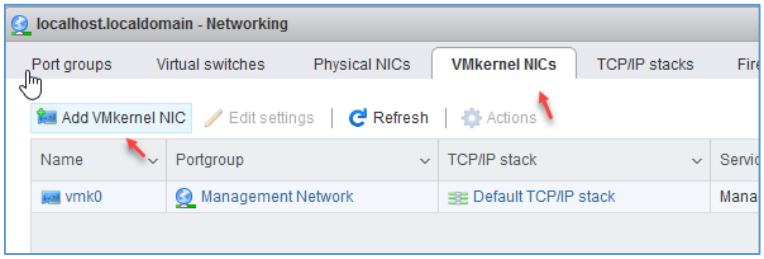
تنظیم ESXI-01

در ادامه کار به مانند شکل ۱۲-۱٤٥، وارد صفحه ESXi-01 که آدرس آن 192.168.19.130 هست شوید و بعد بر روی Networking کلیک کنید، در صفحه‌ی باز شده وارد تب virtual switches شوید و برای اینکه یک ارتباط مجزا داشته باشید باید در این قسمت بر روی Add standard virtual switch کلیک کنید، در صفحه‌ی باز شده نام سوئیچ مجازی خود را وارد و از قسمت Uplink1 کارت شبکه جدید را انتخاب و بر روی Add کلیک کنید.



شکل ۱۲- ۱۴۵ راه‌اندازی قابلیت Vmotion در Vcenter

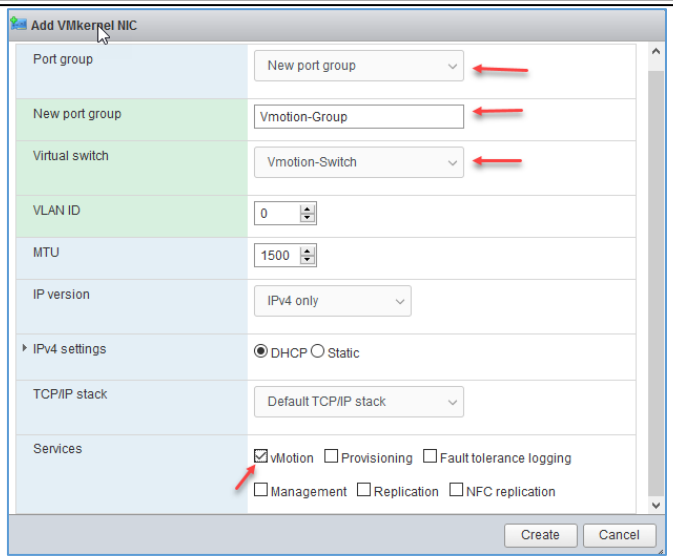
در ادامه به مانند شکل ۱۲-۱٤٦، وارد تب VMkernel NICs شوید و بر روی Add VMKernel NIC کلیک کنید.



شکل ۱۲- ۱۴۶ راه‌اندازی قابلیت Vmotion در Vcenter

در شکل ۱۲-۱٤۷، در قسمت اول New port group را انتخاب کنید، در قسمت دوم باید نام گروه خود را وارد و در قسمت سوم باید همان سوئیچ مجازی که در قسمت قبل ایجاد کردیم را انتخاب کنیم، بعد از این کار در آخر صفحه و از قسمت Services باید تیک گزینه‌ی VMotion را انتخاب کنید، تا این سرویس بر روی این سوئیچ و کارت شبکه فعال شود.

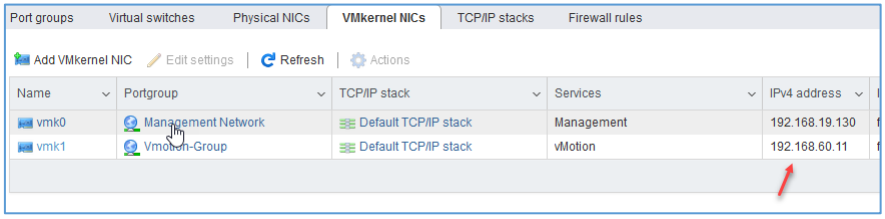
www.takbook.com



شکل ۱۲- ۱۴۷ راه‌اندازی قابلیت Vmotion در Vcenter

نکته: در قسمت IPv4 settings اگر بر روی کارت شبکه‌ی، سرویس DHCP را فعال کردید نیاز به تغییری نیست ولی اگر تعریف نکردید باید گزینه‌ی Static در شکل ۱۲-۱۴۷، را انتخاب کنید و یک آدرس برای آن در نظر بگیرید، توجه داشته باشید در ESXi دوم هم باید آدرسی که وارد می‌کنید در همین رنج باشد.

در شکل ۱۲-۱۴۸، kernel مورد نظر اضافه شده است و همان‌طور که مشاهده می‌کنید آدرس IP که برای آن در نظر گرفته شده 192.168.60.11 است.



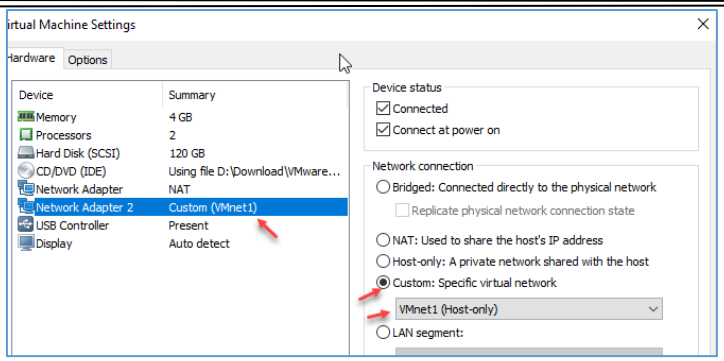
شکل ۱۲- ۱۴۸ راه‌اندازی قابلیت Vmotion در Vcenter

تنظیم ESXI-02

بعد از تنظیم سرور ESXi-01 باید در سرور دوم هم همان تنظیمات با همان کارت شبکه را انجام دهیم تا این دو سرور در یک گروه با هم در ارتباط باشند.

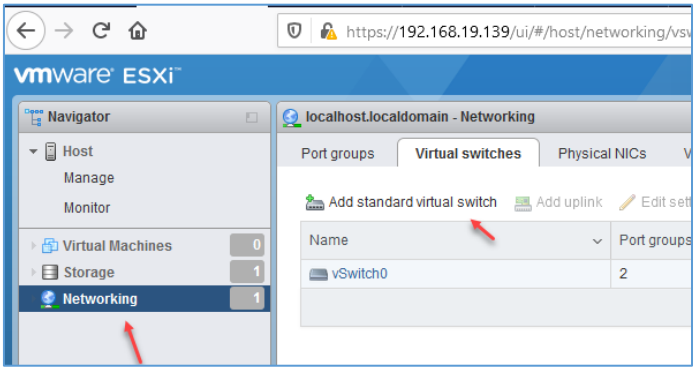
به مانند شکل ۱۲-۱۴۹، برای انجام این کار در ESXi-02 وارد Settings شوید و دقیقا همان کارهای قبلی را انجام دهید، پس نیازی به توضیح دوباره نخواهد بود، فقط با عکس مراحل را پیش‌می‌بریم، کارت شبکه را اضافه و تنظیم کنید.

www.takbook.com



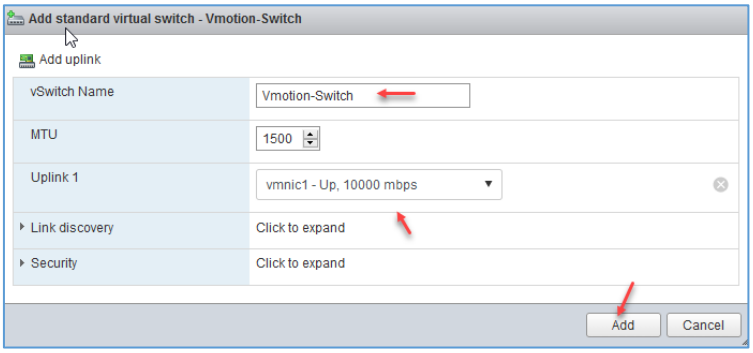
شکل ۱۲- ۱۴۹ راه‌اندازی قابلیت Vmotion در Vcenter

به مانند شکل ۱۲-۱۵۰، بر روی Networking کلیک کنید، در صفحه‌ی باز شده وارد تب virtual Switches شوید و بر روی Add standard virtual switch کلیک کنید.



شکل ۱۲- ۱۵۰ راه‌اندازی قابلیت Vmotion در Vcenter

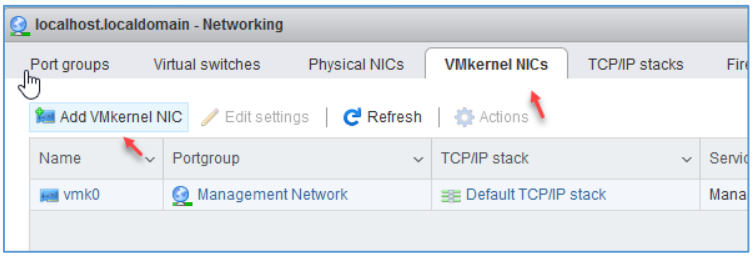
در شکل ۱۲-۱۵۱، نام سوئیچ مجازی خود را وارد و از قسمت Uplink1 کارت شبکه جدید را انتخاب و بر روی Add کلیک کنید.



شکل ۱۲- ۱۵۱ راه‌اندازی قابلیت Vmotion در Vcenter

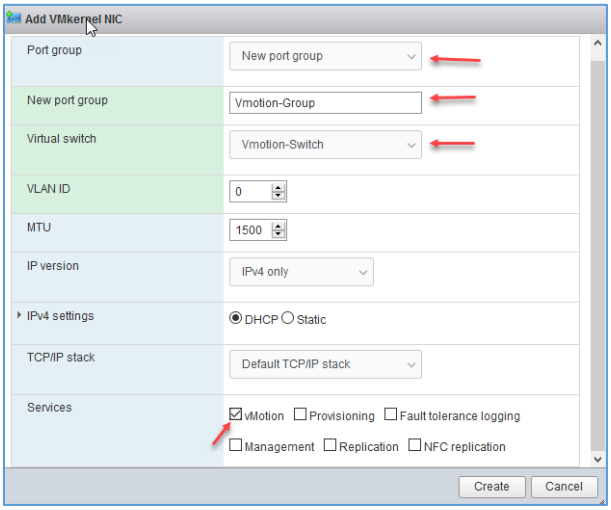
www.takbook.com

به مانند شکل ۱۲-۱۵۲، وارد تب VMkernel NICs شوید و بر روی Add VMKernel NIC کلیک کنید.



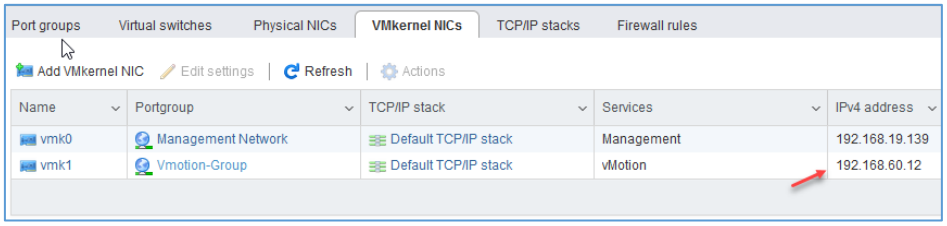
شکل ۱۲- ۱۵۲ راه‌اندازی قابلیت Vmotion در Vcenter

در شکل ۱۲-۱۵۳، به مانند قبل عمل کنید و بر روی Create کلیک کنید.



شکل ۱۲- ۱۵۳ راه‌اندازی قابلیت Vmotion در Vcenter

همان‌طور که در شکل ۱۲-۱۵۴، مشاهده می‌کنید سرور دوم هم تنظیم شده است.



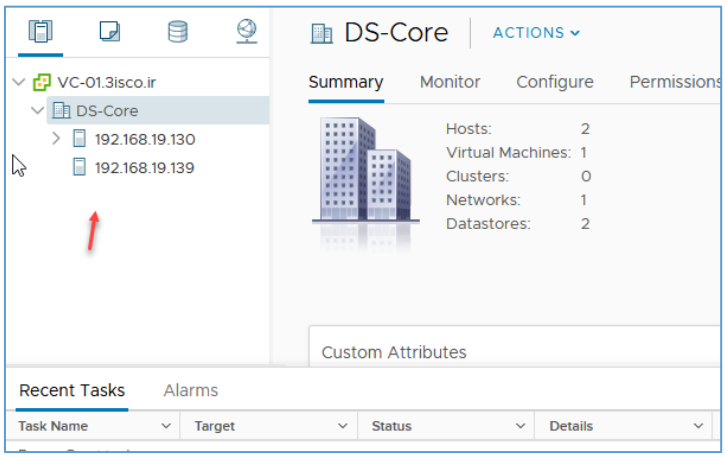
شکل ۱۲- ۱۵۴ راه‌اندازی قابلیت Vmotion در Vcenter

در مرحله بعد باید هارد دیسک از نوع iSCSI را به هر دو سرور ESXi اضافه کنید تا هر دو بتوانند از آن هارد دیسک به صورت اشتراکی استفاده کنند، با این کار ماشین مورد نظر شما بر روی آن هارد دیسک

www.takbook.com

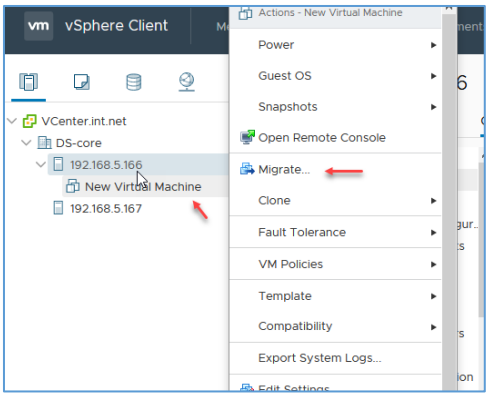
ایجاد شده و در زمان انتقال بدون هیچ قطعی به سرور دوم منتقل می‌شود، توجه داشته باشید نحوه‌ی ایجاد هارد ISCSI را در فصل دهم توضیح دادیم.

بعد از انجام مراحل قبل وارد Vcenter خود شوید و با توجه به آموزش‌های قبلی یک DataCenter با نام DS-Core به مانند شکل ۱۲-۱۵۵، ایجاد و دو سرور ESXi را به لیست اضافه کنید.



شکل ۱۲- ۱۵۵ راه‌اندازی قابلیت Vmotion در Vcenter

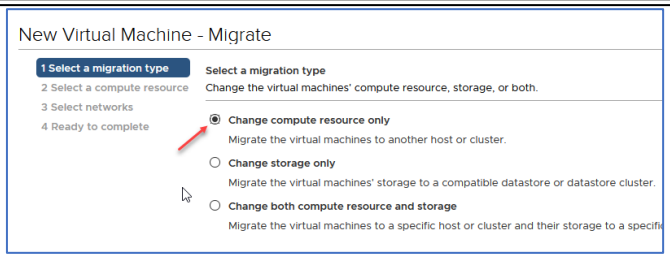
بعد از اضافه کردن دو سرور ESXi به Vcenter می‌خواهیم کاری کنیم که ماشین مجازی با نام Server-1 که روشن هم است، به سرور ESXi-02 انتقال پیدا کند، برای این کار به مانند شکل ۱۲-۱۵۶، بر روی ماشین کلیک راست کنید و گزینه‌ی Migrate را انتخاب کنید.



شکل ۱۲- ۱۵۶ راه‌اندازی قابلیت Vmotion در Vcenter

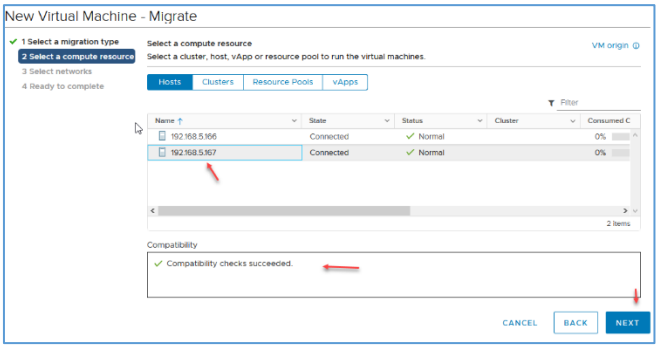
در شکل ۱۲-۱۵۷، سه گزینه را مشاهده می‌کنید اگر اولی را انتخاب کنید فقط ماشین مجازی منتقل می‌شود و گزینه‌ی دوم برای انتقال DataStore به Datastore دیگر است و گزینه‌ی سوم هر دوی این موارد را پوشش می‌دهد، پس گزینه‌ی اول را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



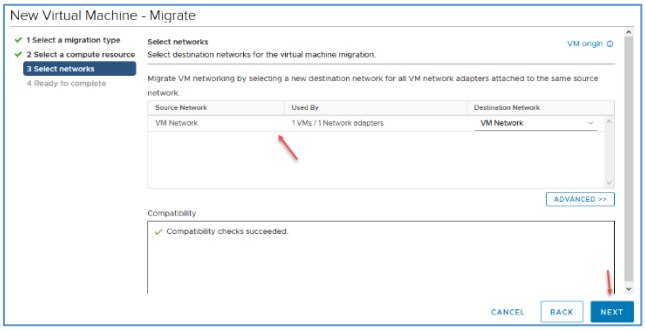
شکل ۱۲- ۱۵۷ راه‌اندازی قابلیت Vmotion در Vcenter

در شکل ۱۲-۱۵۸، باید آدرس IP سرور دوم یعنی ESXi-02 را انتخاب و بر روی Next کلیک کنید.



شکل ۱۲- ۱۵۸ راه‌اندازی قابلیت Vmotion در Vcenter

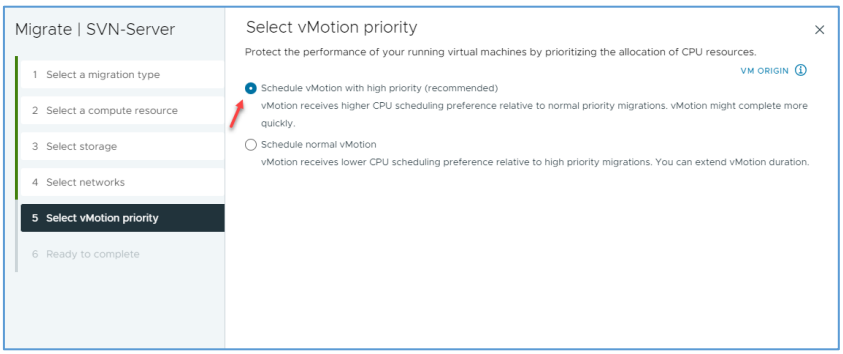
در شکل ۱۲-۱۵۹، باید کارت شبکه مورد نظر را انتخاب کنید، البته به صورت پیش‌فرض کارت شبکه خود ماشین انتخاب می‌شود.



شکل ۱۲- ۱۵۹ راه‌اندازی قابلیت Vmotion در Vcenter

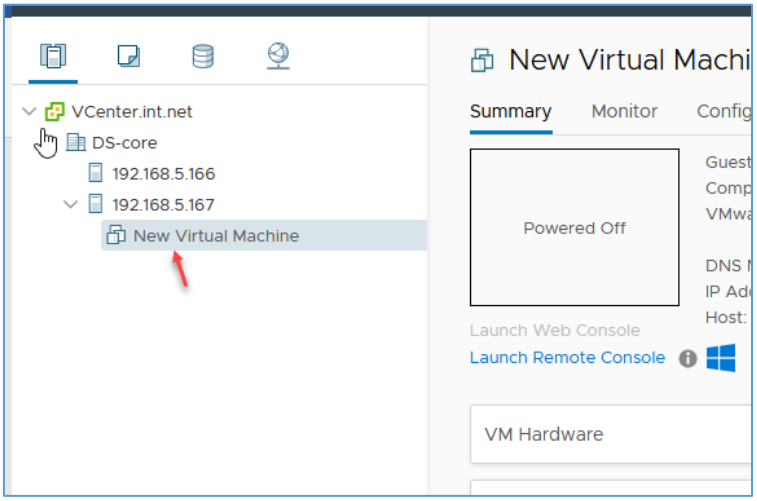
در شکل ۱۲-۱۶۰، دو گزینه مشاهده می‌کنید که گزینه‌ی اول برای این است که انجام عملیات Vmotion با توان کامل CPU انجام شود و گزینه‌ی دوم که به صورت معمولی انجام می‌شود، گزینه‌ی اول را انتخاب و بر روی Next کلیک می‌کنیم و در آخر هم بر روی Finish کلیک کنید.

www.takbook.com



شکل ۱۲- ۱۶۰ راه‌اندازی قابلیت Vmotion در Vcenter

همان‌طور که در شکل ۱۲-۱٦۱، مشاهده می‌کنید، سرور مورد نظر به ESXi-02 انتقال پیدا کرد.



شکل ۱۲- ۱۶۱ راه‌اندازی قابلیت Vmotion در Vcenter

www.takbook.com

۱۳-۱۲ بررسی DRS در VCenter

DRS (Distributed Resource Scheduler) یکی از ویژگی‌های پیشرفته در vCenter Server است که به مدیریت منابع و بهینه‌سازی عملکرد در محیط‌های مجازی‌سازی کمک می‌کند. این ویژگی در VMware vSphere برای توزیع بار کاری بین سرورها و بهبود استفاده از منابع استفاده می‌شود.

عملکرد DRS:

DRS به طور خودکار منابع CPU و RAM را در کلاستر (مجموعه‌ای از هاست‌ها) بین ماشین‌های مجازی (VMs) توزیع می‌کند و در صورت نیاز ماشین‌های مجازی را به هاست‌های مختلف منتقل می‌کند تا از عملکرد بهینه بهره‌مند شوند.

مراحل کار DRS

مانیتورینگ منابع: DRS منابع CPU و حافظه هاست‌ها را به طور مداوم مانیتور می‌کند تا مشخص کند که آیا هاست‌ها بیش از حد بارگیری شده‌اند یا منابع بیشتری دارند.

ارائه پیشنهادات یا انتقال خودکار: بسته به تنظیمات، DRS ممکن است پیشنهاد انتقال ماشین‌های مجازی بین هاست‌ها را بدهد یا به صورت خودکار ماشین‌ها را انتقال (vMotion) دهد.

تعادل بار (Load Balancing): DRS تلاش می‌کند تا منابع به صورت متعادل در هاست‌های موجود در کلاستر توزیع شوند تا هیچ یک از هاست‌ها بیش از حد بارگیری نشوند.

گروه‌های وابستگی (Affinity/Anti-Affinity Rules): DRS به شما این امکان را می‌دهد تا قوانین وابستگی تعریف کنید. به عنوان مثال، می‌توانید مشخص کنید که برخی ماشین‌های مجازی همیشه باید روی یک هاست باشند (Affinity) یا از هم جدا باشند (Anti-Affinity).

واکنش به تغییرات منابع: در صورت بروز تغییر در نیازهای منابع یا در دسترس بودن هاست‌ها، DRS می‌تواند به سرعت تغییرات را مدیریت کرده و ماشین‌های مجازی را مجدداً توزیع کند.

مزایای DRS

- تعادل خودکار بار: با مانیتورینگ و مهاجرت خودکار ماشین‌های مجازی، از کارایی و استفاده بهینه از منابع هاست‌ها اطمینان حاصل می‌شود.

www.takbook.com

- صرفه‌جویی در مصرف انرژی: در صورت کمبود بار کاری، DRS می‌تواند ماشین‌های مجازی را به هاست‌های کمتر منتقل کرده و هاست‌های بلااستفاده را خاموش کند.
- انعطاف‌پذیری بالا: DRS به شما این امکان را می‌دهد تا در محیط‌های پیچیده و بزرگ به راحتی منابع را مدیریت کنید.

قبل از فعال کردن DRS باید در مورد Clustering صحبت کنیم.

Clustering در vCenter

Clustering در vCenter Server به معنی ترکیب چندین هاست ESXi به عنوان یک واحد منطقی برای بهینه‌سازی مدیریت منابع و افزایش قابلیت اطمینان در یک محیط مجازی است. با استفاده از کلاسترها، می‌توان منابع موجود را به صورت متمرکز مدیریت کرد و از ویژگی‌های پیشرفته مثل High Availability (HA) و Distributed Resource Scheduler (DRS) بهره‌مند شد.

اهداف Clustering در vCenter

بهبود دسترس‌پذیری: کلاسترها از ویژگی‌هایی مثل HA استفاده می‌کنند تا در صورت خرابی یک هاست، ماشین‌های مجازی به سرعت بر روی هاست‌های دیگر روشن شوند.

تعادل منابع: با استفاده از DRS، کلاستر می‌تواند به طور خودکار ماشین‌های مجازی را بین هاست‌های مختلف منتقل کند تا تعادل بار حفظ شود و منابع به طور بهینه استفاده شوند.

مدیریت ساده‌تر: یک کلاستر به مدیران IT امکان می‌دهد تا هاست‌ها و منابع ماشین‌های مجازی را به صورت متمرکز مدیریت کنند.

ویژگی‌های اصلی Clustering:

High Availability (HA)

این ویژگی تضمین می‌کند که اگر یک هاست در کلاستر از کار بیفتد، ماشین‌های مجازی که روی آن هاست در حال اجرا بودند به صورت خودکار روی هاست‌های دیگر راه‌اندازی می‌شوند. HA به افزایش دسترس‌پذیری کمک می‌کند و از خرابی‌های طولانی جلوگیری می‌کند.

Fault Tolerance (FT): زیرمجموعه‌ای از HA است که نسخه‌ای دقیق و در حال اجرای ماشین مجازی بر روی هاست دیگر ایجاد می‌کند. در صورت خرابی هاست، نسخه پشتیبان به صورت فوری وارد عمل می‌شود.

Distributed Resource Scheduler (DRS)

www.takbook.com

DRS یکی از اجزای حیاتی کلاستر است که بار کاری را بین هاست‌های موجود در کلاستر توزیع می‌کند. این سیستم به صورت خودکار ماشین‌های مجازی را با استفاده از vMotion بین هاست‌ها جابجا می‌کند تا استفاده از منابع بهینه و تعادل بار حفظ شود.

Storage DRS

علاوه بر مدیریت منابع پردازشی، DRS می‌تواند توزیع ذخیره‌سازی را نیز مدیریت کند. Storage DRS بر روی ذخیره‌سازها (Datastore Clusters) اعمال می‌شود و به تعادل بار بین ذخیره‌سازهای مختلف کمک می‌کند.

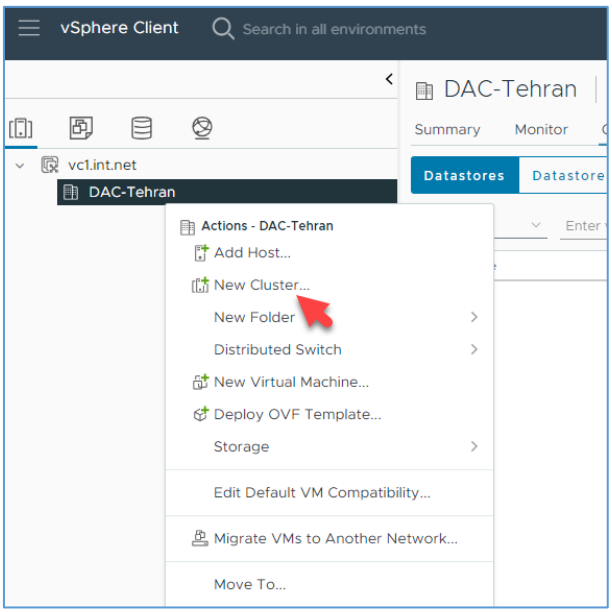
Resource Pools

در کلاسترها می‌توان Resource Poolها ایجاد کرد که به نوعی تقسیم‌بندی منابع داخل یک کلاستر هستند. این ویژگی برای تخصیص منابع به بخش‌های مختلف یک سازمان یا پروژه‌های مختلف بسیار مفید است. مدیران می‌توانند منابع مشخصی از CPU و RAM را به هر Resource Pool اختصاص دهند.

vMotion

با استفاده از vMotion در کلاستر، ماشین‌های مجازی می‌توانند به صورت زنده و بدون وقفه در سرویس‌دهی بین هاست‌های مختلف جابجا شوند. این ویژگی در ترکیب با DRS و HA به تعادل بار و کاهش خرابی کمک می‌کند.

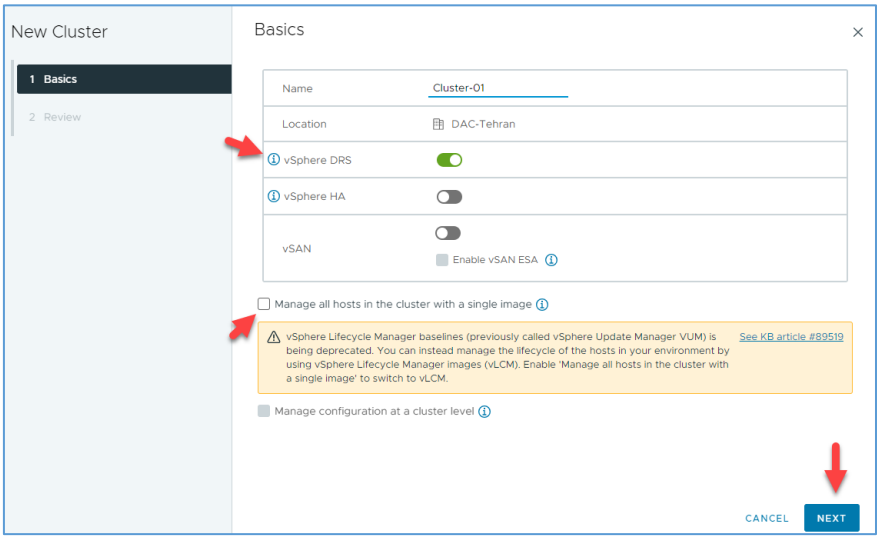
برای راه‌اندازی DRS باید به صورت شکل ۱۲-۱۶۲، عمل کنیم، قبل از هر کاری باید یک کلاستر جدید ایجاد کنیم و سرورهای ESXi خود را عضو آن کنیم، برای شروع بر روی DataCenter خود کلیک راست کنید و گزینه‌ی New Cluster را انتخاب کنید.



شکل ۱۲- ۱۶۲ بررسی DRS در VCenter

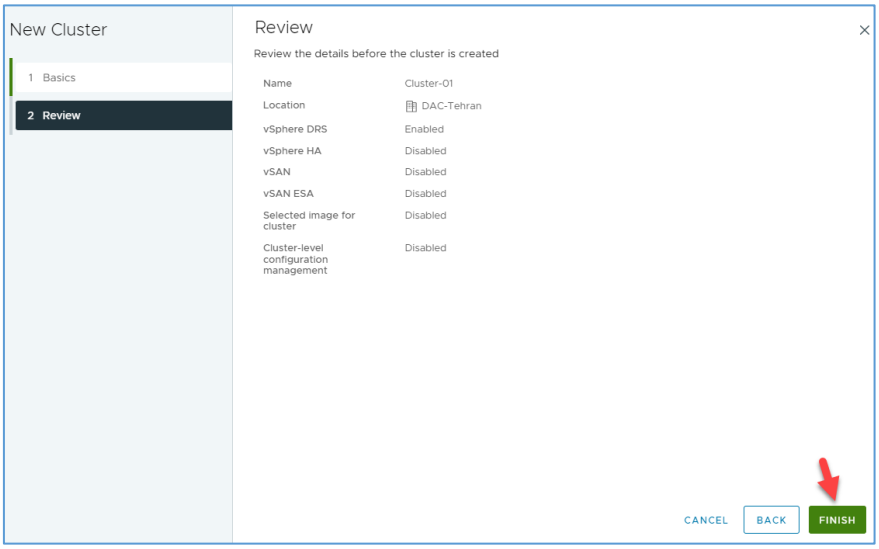
www.takbook.com

در ادامه کار و در شکل ۱۲-۱۶۳، باید نام Cluster خود را به دلخوله وارد کنید و در قسمت سرویس‌های سرویس RDS را فعال کنید و تیک گزینه‌ی مورد نظر را بردارید.



شکل ۱۲- ۱۶۳ بررسی DRS در VCenter

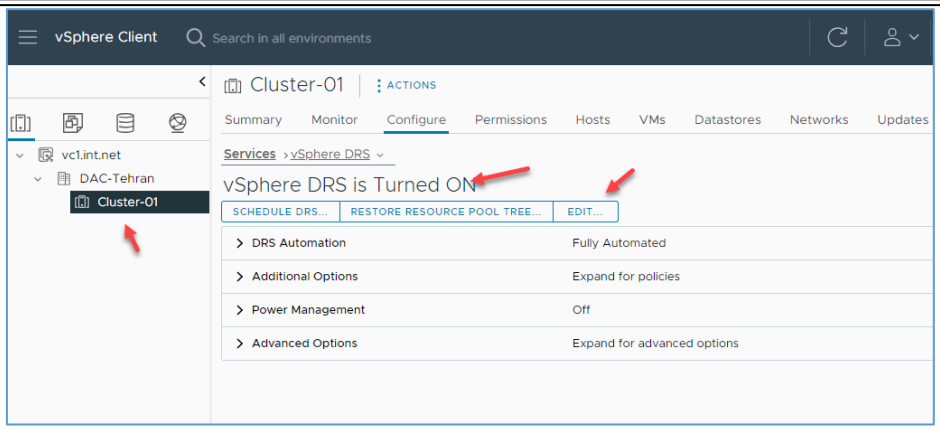
در شکل ۱۲-۱۶۳، بر روی Finish کلیک کنید.



شکل ۱۲- ۱۶۴ بررسی DRS در VCenter

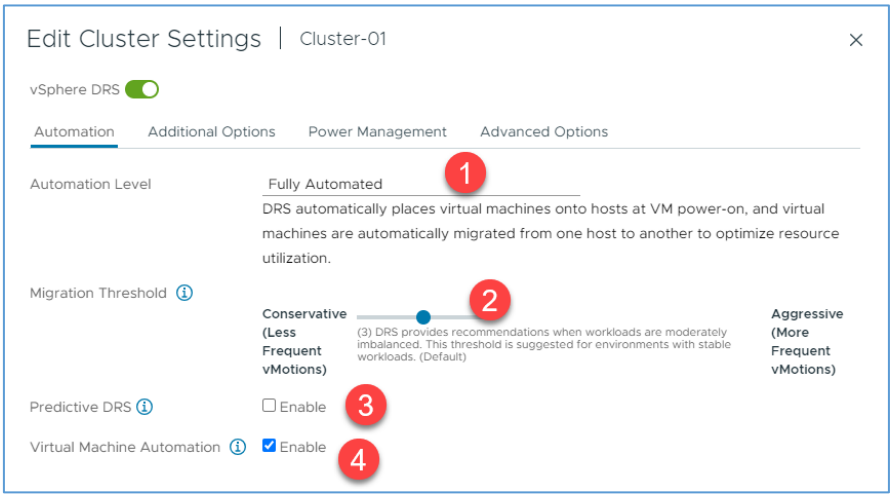
همان‌طور که در شکل ۱۲-۱۶۵، مشاهده می‌کنید سرویس DRS فعال شده است و برای بررسی بیشتر آن باید بر روی Edit کلیک کنید.

www.takbook.com



شکل ۱۲- ۱۶۵ بررسی DRS در VCenter

در شکل ۱۲-۱۶۶، گزینه‌های مختلف را مشاهده می‌کنید، در قسمت شماره‌ی یک یعنی قسمت Automation Level سه گزینه وجود دارد که گزینه‌ی Manual که همان‌طور از اسمش پیداست به صورت دستی انجام می‌شود و به صورت دستی باید یک ماشین را به یک سرور دیگر انتقال دهید، گزینه‌ی Partially Automated اگر فعال باشد در زمانی که می‌خواهیم یک ماشین مجازی ایجاد کنیم سرویس DRS تصمیم می‌گیرد که این ماشین را در کدام Host یا همان ESxi ایجاد کند در آخر کار هم اگر گزینه‌ی Fully Automated را انتخاب کنید کلیه تصمیمات توسط DRS گرفته می‌شود و همه‌ی کارها به صورت خودکار انجام می‌شود.



شکل ۱۲- ۱۶۶ بررسی DRS در VCenter

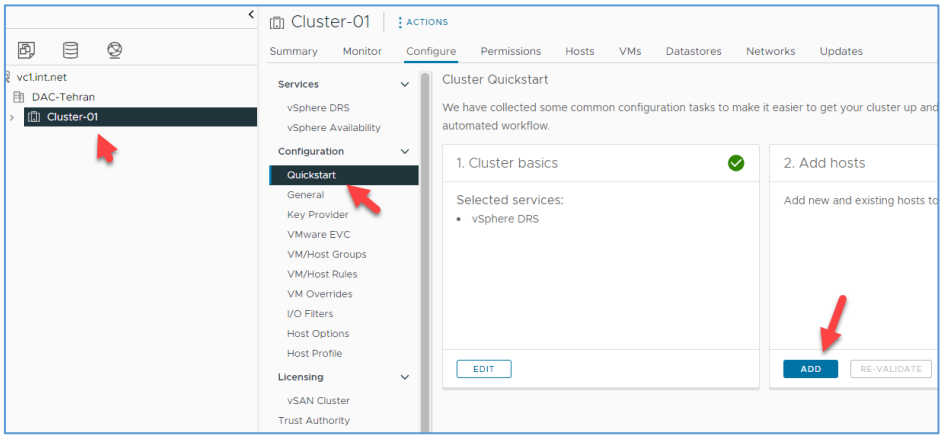
در قسمت شماره‌ی دوم یعنی Migration Threshold می‌توانیم مشخص کنیم که یک ماشین در چه زمانی به هاست دیگر منتقل شود یعنی اینکه اگر ما مقدار آستانه را به سمت Aggressive ببریم سرویس DRS خیلی حساس‌تر خواهد شد و با کوچکترین مشکلی در یک هاست ماشین مورد نظر را به هاست دیگر

www.takbook.com

انتقال می‌دهد و هر چقدر به سمت Conservative برویم تحمل‌پذیری بالا می‌رود و خیلی کمتر حساسیت وجود دارد، در قسمت شماره‌ی سه اگر از ابزار vRealize که برای مانیتورینگ است استفاده می‌کنید باید تیک گزینه‌ی Predictive DRS را انتخاب کنید، در قسمت شماره‌ی چهار اگر قصد دارید یک ماشین مجازی خاص به سرور دیگر منتقل نشود باید تیک آن را انتخاب کنید.

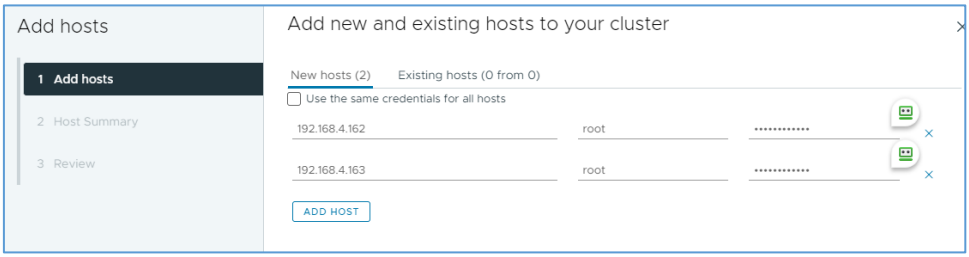
برای تست عملکرد DRS باید یک کلاسنتر ایجاد کنیم که در این کلاستر دو میزبان ESXi اضافه می‌کنیم و این سرویس را تست میگیریم.

بر روی کلاستر خود به مانند شکل ۱۲-۱۶۷، کلیک کنید و و از قسمت Quickstart بر روی Add در قسمت Hosts کلیک کنید.



شکل ۱۲- ۱۶۷ بررسی DRS در VCenter

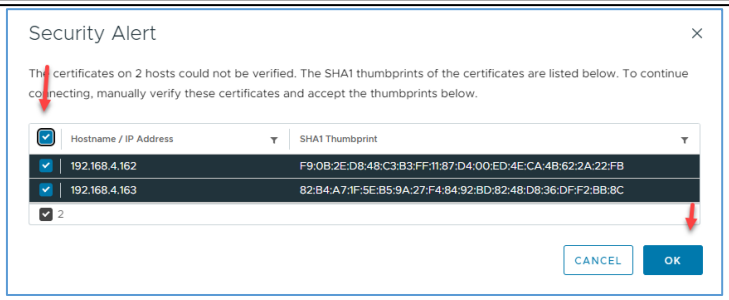
در شکل ۱۲-۱۶۸، باید اطلاعات دو یا چند سرور ESXi خود را وارد کنیم.



شکل ۱۲- ۱۶۸ بررسی DRS در VCenter

در شکل ۱۲-۱۶۹، برای تایید Certificate باید هر دو گزینه را انتخاب کنید و بر روی Next کلیک کنید.

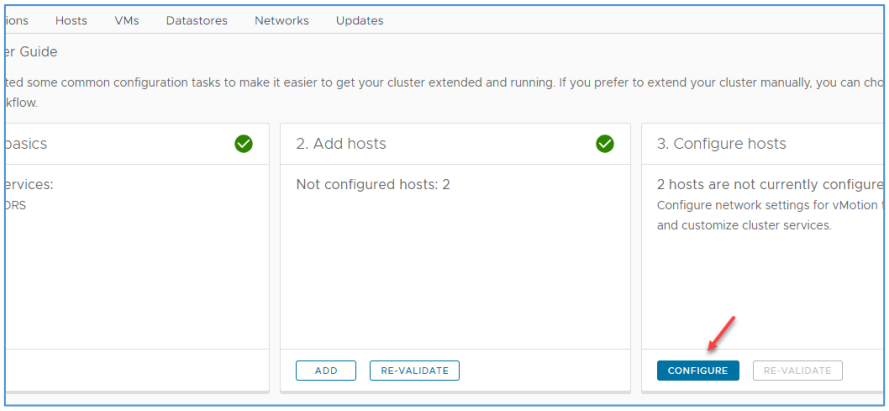
www.takbook.com



شکل ۱۲- ۱۶۹ بررسی DRS در VCenter

همان‌طور که در شکل ۱۲-۱۷۰، مشاهده می‌کنید دو سرور تایید شده است و بر روی Next کلیک کنید و در قسمت آخر بر روی Finish کلیک کنید.

بعد از چند دقیقه مرحله‌ی دوم هم اوکی می‌شود و باید مرحله‌ی سوم را بررسی کنیم که باید بر روی گزینه‌ی Configure کلیک کنید.



شکل ۱۲- ۱۷۰ بررسی DRS در VCenter

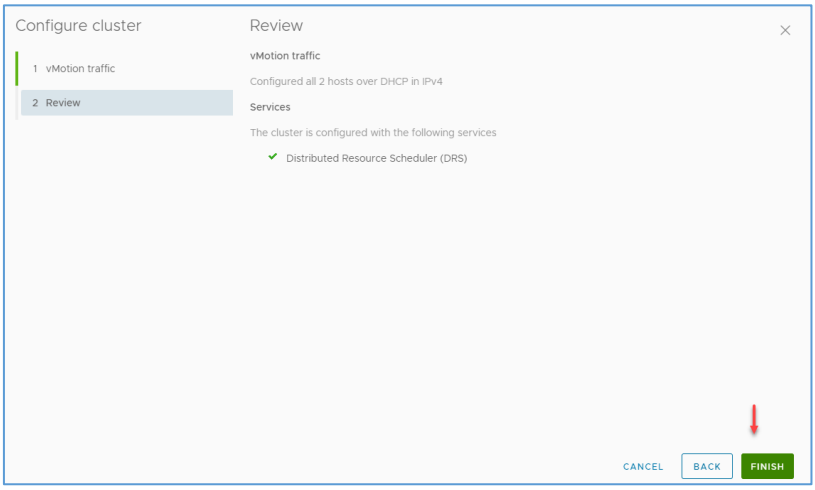
در شکل ۱۲-۱۷۱، IPv4 را انتخاب و نوع آن را DHCP در نظر بگیرید.



شکل ۱۲- ۱۷۱ بررسی DRS در VCenter

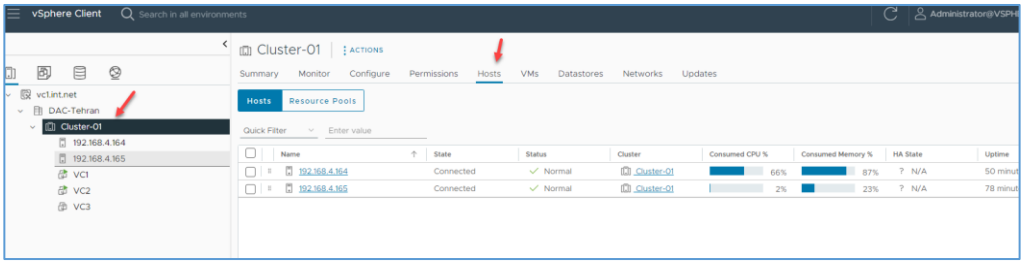
www.takbook.com

همان‌طور که در شکل ۱۲-۱۷۲، مشاهده می‌کنید سرویس DRS هم فعال است و باید بر روی Finish کلیک کنید تا تنظیمات بر روی Host های مورد نظر اعمال شود.



شکل ۱۲- ۱۷۲ بررسی DRS در VCenter

برای تست سرویس DRS به مانند شکل ۱۲-۱۷۳، در یکی از هاست‌های ESXi سه ماشین مجازی ایجاد و آنها را روشن می‌کنیم، اگر به قسمت Hosts توجه کنید چون همه ماشین‌ها بر روی Host اول یعنی 192.168.4.164 قرار دارد مقدار مصرف CPU و رم بالا رفته است و اگر از یک حدی بالاتر برود سرویس DRS به صورت اتوماتیک یک یا چند ماشین را به سرور دیگری که در کلاستر است انتقال می‌دهد که باعث تعادل در بار سرورها خواهد شد.

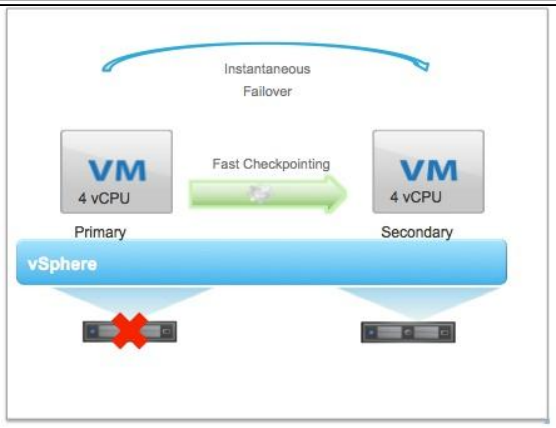


شکل ۱۲- ۱۷۳ بررسی DRS در VCenter

۱۲-۱٤ بررسی High Availability (HA) در Vcenter

یکی از ویژگی‌های مهم نرم‌افزار Vcenter این است که از سرویس High Availability (HA) پشتیبانی می‌کند، این سرویس زمانی به کار می‌آید که دو سرور ESXi داشته باشید و اگر یکی از آنها از کار بیفتد، یکی دیگر به کار ادامه خواهد داد و بدین صورت ماشین مورد نظر هیچ‌وقت خاموش نخواهد شد.

www.takbook.com



شکل ۱۲- ۱۷۴ بررسی High Availability (HA) در Vcenter

برای اینکه این سرویس را راه‌اندازی کنیم، نیاز است چند مورد را قبل از آن تنظیم کنیم:

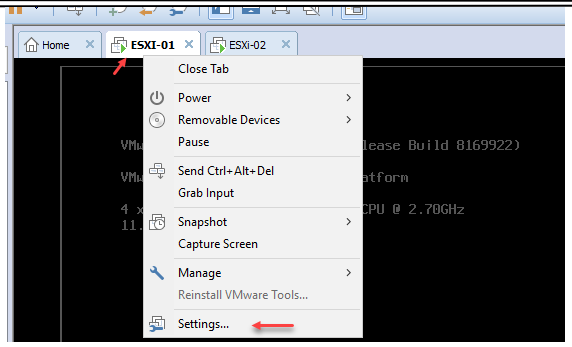
۱- حداقل نیاز به دو سرور ESXi دارید تا بتوانید این عملیات را انجام دهید.
۲- نیاز به سرور Vcenter برای فعال‌سازی و مدیریت سرویس.
۳- نیاز به کارت شبکه مجزا برای ارتباط ESXiها با هم و فعال‌سازی سرویس Fault Tlerance آن.
۴- پیاده‌سازی فضای اشتراکی مانند، iSCSI، NFS و ...

توجه داشته باشید بهترین حالت این است که سرورهای ESXi از یک ورژن باشند و سرورهای فیزیکی آنها هم دارای حداقل CPU دارای دو هسته و ۸ گیگ رم باشند که با افزایش این مقادیر به عملکرد بهتری دست پیدا خواهید کرد.

مرحله اول – تنظیم کارت شبکه

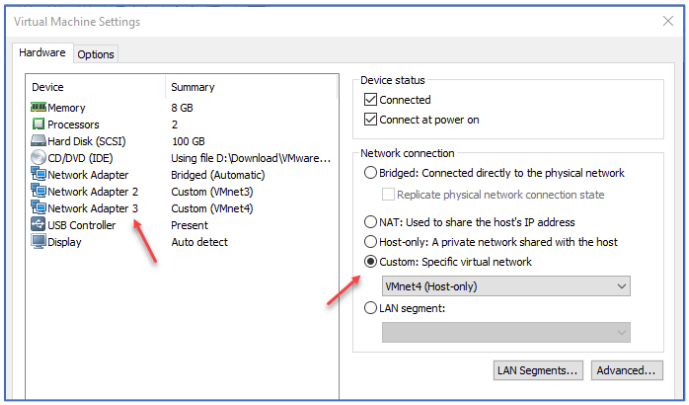
برای اجرای عملیات fault tolerance، ابتدا باید یک کارت شبکه‌ی مجزا برای این منظور در نظر گرفته شود. در سرورهای ESXi که به این عملیات اختصاص داده‌اید، باید این کارت شبکه را تنظیم و راه‌اندازی کنید. اگر قصد دارید این کار را به صورت مجازی انجام دهید، کافی است به مانند شکل ۱۲-۱۷۵، روی سرور مورد نظر کلیک راست کرده و از بخش Settings یک کارت شبکه جدید اضافه کنید.

www.takbook.com



شکل ۱۲- ۱۷۵ بررسی High Availability (HA) در Vcenter

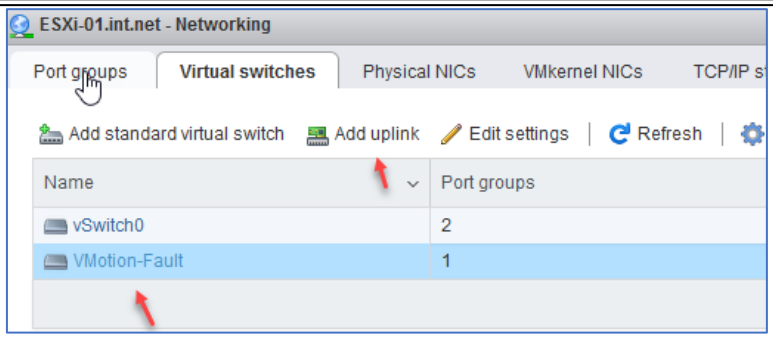
همان‌طور که در شکل ۱۲-۱۷۶، مشاهده می‌کنید، کارت شبکه‌ی VMnet4 برای این موضوع در نظر گرفته شده است که آدرس شبکه آن 192.168.110.0 است و دقیقاً همین کارت شبکه را برای ESXi دوم در نظر بگیرید.



شکل ۱۲- ۱۷۶ بررسی High Availability (HA) در Vcenter

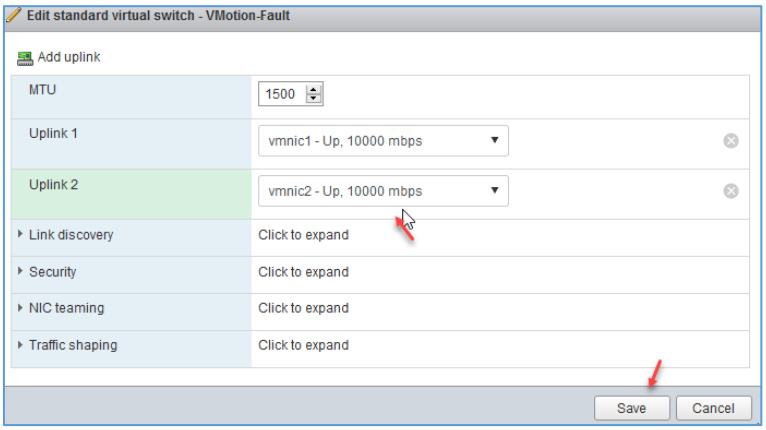
به مانند شکل ۱۲-۱۷۷، وارد هر یک از سرورهای ESXi شوید و از قسمت Networking وارد تب Virtual switches شوید، در قسمت قبلی سرویس VMotion را برای کارت شبکه VMnet3 فعال کردیم و می‌خواهیم بر روی همین سوئیچ سرویس Fault را فعال کنیم، قبل از این کار برای اینکه از کارت شبکه جدید استفاده کنیم بر روی Add uplink کلیک کنید و کارت شبکه جدید را به این سوئیچ اضافه کنید، با این کار دو خط ارتباطی بین دو سرور ESXi فعال خواهد شد و این کار باعث می‌شود در زمان قطع شدن یکی از خطها، خط دیگر ارتباط را حفظ کند.

www.takbook.com



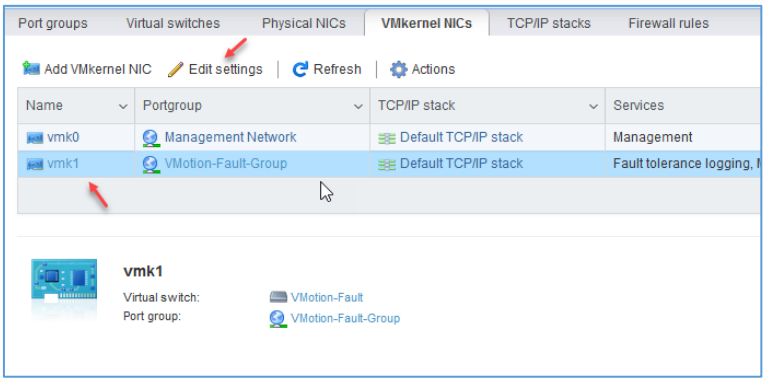
شکل ۱۲- ۱۷۷ بررسی High Availability (HA) در Vcenter

در شکل ۱۲-۱۷۸، باید کارت شبکه‌ی دوم یعنی vmnic2 را انتخاب و بر روی Save کلیک کنید.



شکل ۱۲- ۱۷۸ بررسی High Availability (HA) در Vcenter

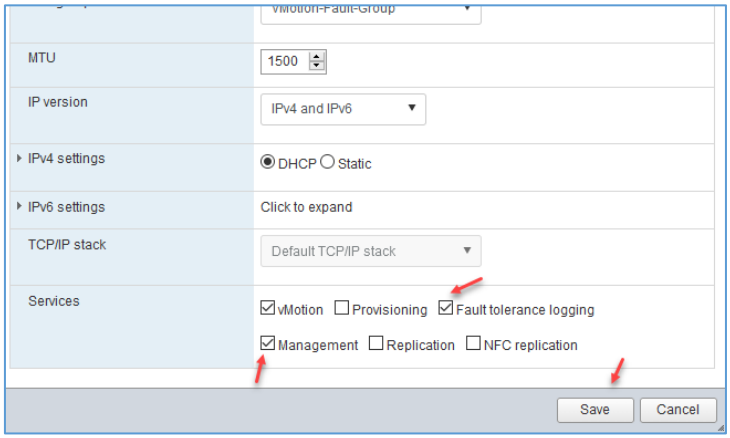
در ادامه و به مانند شکل ۱۲-۱۷۹، وارد تب VMkernel NICs شوید و گروه قبلی که در قسمت VMotion ایجاد کردید را انتخاب و بر روی Edit settings کلیک کنید.



شکل ۱۲- ۱۷۹ بررسی High Availability (HA) در Vcenter

www.takbook.com

در شکل ۱۲-۱۸۰، از قسمت Services باید سرویس Fault tolerance را انتخاب کنید، توجه داشته باشید آدرس IPv4 را در حالت DHCP انتخاب کنید و بر روی Save کلیک کنید.



شکل ۱۲- ۱۸۰ بررسی *High Availability (HA)* در *Vcenter*

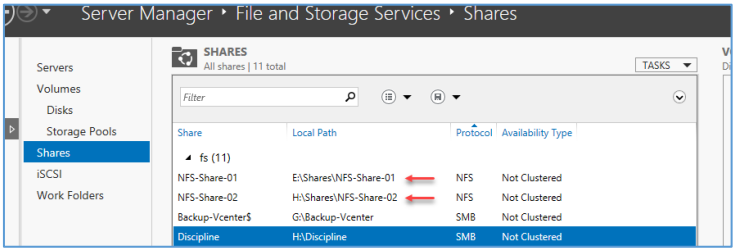
نکته: برای اینکه سرویس Management هم به صورت Load Balance کار کند بهتر است که در این قسمت تیک سرویس Management را انتخاب کنید تا از طریق هر دو کارت شبکه بتوانید به صفحه‌ی مدیریتی دسترسی داشته باشید، دقیقاً تمام این مراحل را برای سرور ESXi-02 هم انجام دهید.

مرحله دوم – اضافه کردن iSCSI یا NFS

نحوه اضافه کردن iSCSI و NFS را در درس‌های قبلی فرا گرفتید و در این قسمت فقط می‌خواهیم به صورت کلی به آن بپردازیم.

برای اینکه سرویس Fault Tolerance را راه‌اندازی کنیم، باید یک فضای ذخیره‌سازی اشتراکی داشته باشیم تا این عملیات به خوبی انجام گیرد.

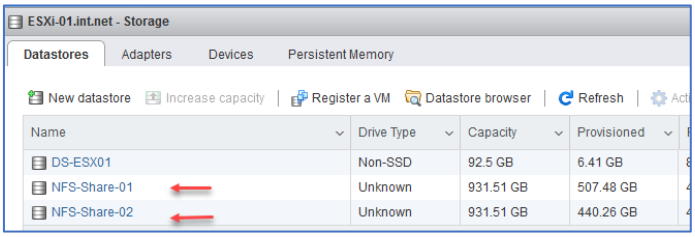
نکته: پیشنهاد می‌شود این فضا برای هر یک از سرورهای ESXi جداگانه باشد و یکی نباشد، برای همین وارد Fileserver می‌شویم و از طریق سرویس NFS دو فضای‌جداگانه برای آنها ایجاد می‌کنیم، همان‌طور که در شکل ۱۲-۱۸۱، مشاهده می‌کنید دو فضای NFS ایجاد شده که باید هر دوی آنها را به سرور ESXi تخصیص دهیم، آموزش راه‌اندازی سرویس NFS را در درس‌های قبلی آموختیم.



شکل ۱۲- ۱۸۱ بررسی *High Availability (HA)* در *Vcenter*

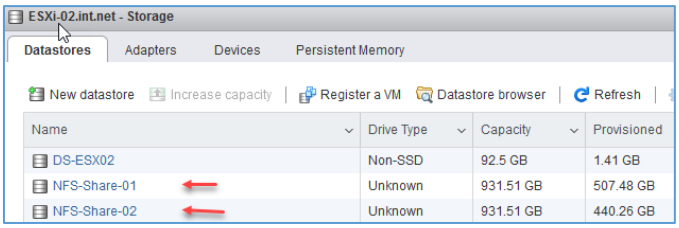
www.takbook.com

بعد از ایجاد فضای ذخیره‌سازی از نوع NFS باید به مانند شکل ۱۲-۱۸۲، وارد ESXi-01 شوید و با کلیک بر روی New datastore هر دو فضای ایجاد شده را به لیست اضافه کنید.



شکل ۱۲- ۱۸۲ بررسی High Availability (HA) در Vcenter

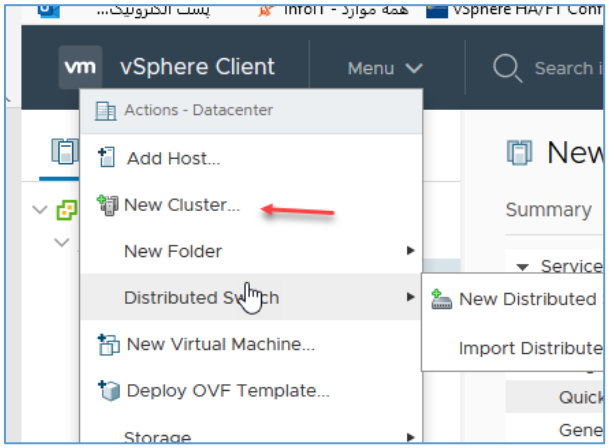
دقیقاً همین کار را برای سرور ESXi-02 هم انجام دهید که در شکل رو۱۲-۱۸۳، این موضوع را مشاهده می‌کنید.



شکل ۱۲- ۱۸۳ بررسی High Availability (HA) در Vcenter

مرحله سوم – ایجاد Clustering

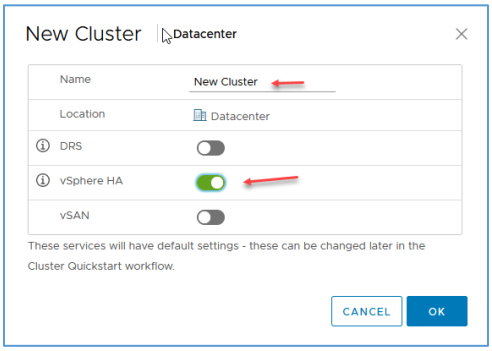
در ادامه کار همه چیز آماده است تا قابلیت Fault Tlorance را پیاده‌سازی کنیم، برای این کار نیاز است تا Clustring را در Vcenter ایجاد کنیم، برای این کار به مانند شکل ۱۲-۱۸٤، وارد Vcenter شوید و بر روی DataCenter خود کلیک راست کنید و گزینه‌ی New Cluster را انتخاب کنید.



شکل ۱۲- ۱۸۴ بررسی High Availability (HA) در Vcenter

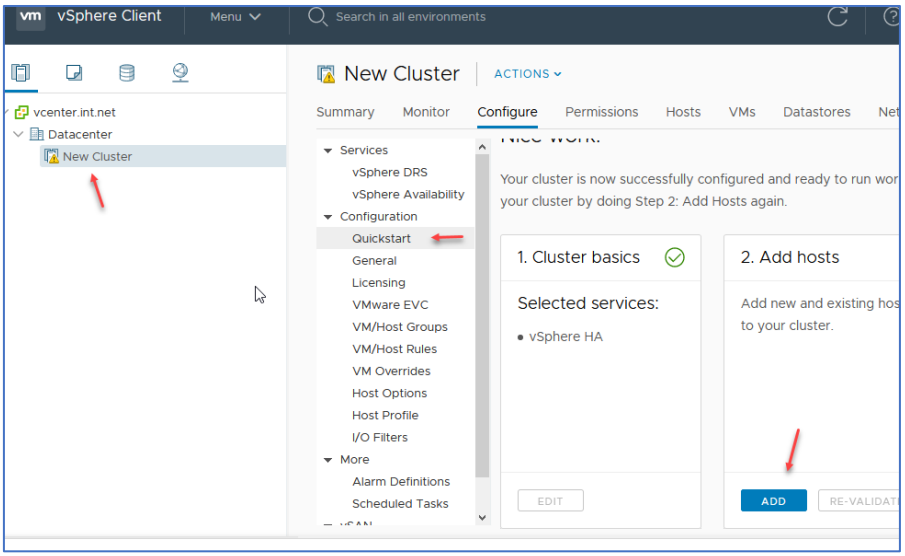
www.takbook.com

در شکل ۱۲-۱۸۵، باید نام Cluster خود را وارد و از قسمت سرویس‌های گزینه‌ی vSphere HA را فعال کنید و بر روی OK کلیک کنید.



شکل ۱۲- ۱۸۵ بررسی High Availability (HA) در Vcenter

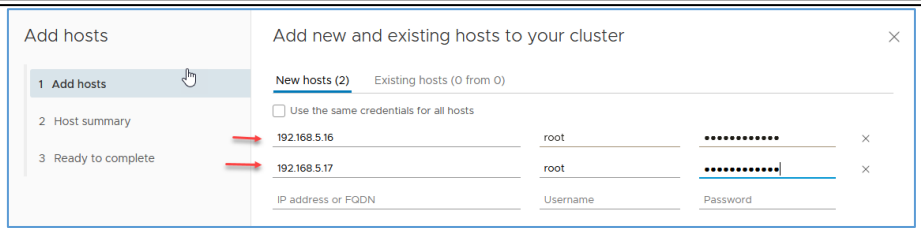
در شکل ۱۲-۱۸۶، Cluster مورد نظر ایجاد شده و باید از قسمت Configuration گزینه‌ی Quickstart را انتخاب کنید و در صفحه‌ی باز شده بر روی Add کلیک کنید.



شکل ۱۲- ۱۸۶ بررسی High Availability (HA) در Vcenter

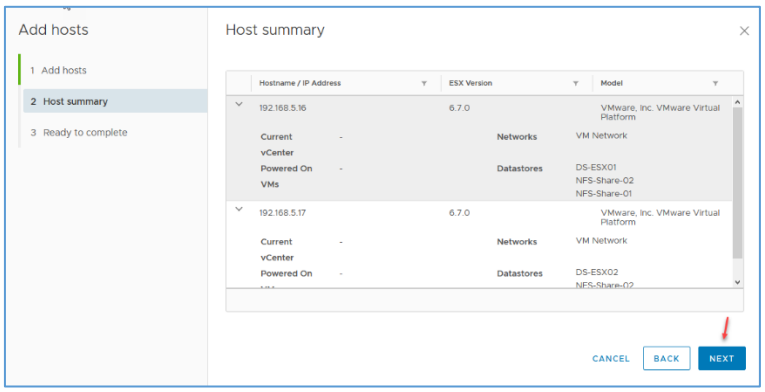
در شکل ۱۲-۱۸۷، باید آدرس هر دو سرور ESXi را به همراه نام کاربری و رمز عبور آنها وارد کنید، اگر چند سرور ESXi دارید، برای اینکه نیاز نباشد رمز عبور را چندین بار تکرار کنید باید تیک گزینه‌ی Use the same… را انتخاب کنید تا برای بقیه هم در نظر گرفته شود.

www.takbook.com



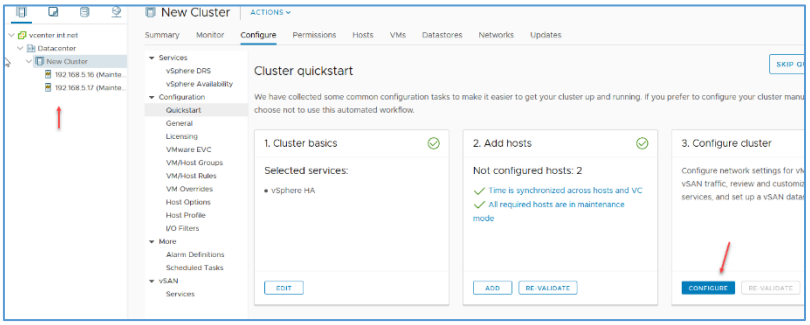
شکل ۱۲- ۱۸۷ بررسی *High Availability (HA)* در *Vcenter*

در شکل ۱۲-۱۸۸، اطلاعات هر دو سرور را مشاهده می‌کنید، بر روی Next کلیک کنید و در صفحه بعد بر روی Finish کلیک کنید.



شکل ۱۲- ۱۸۸ بررسی *High Availability (HA)* در *Vcenter*

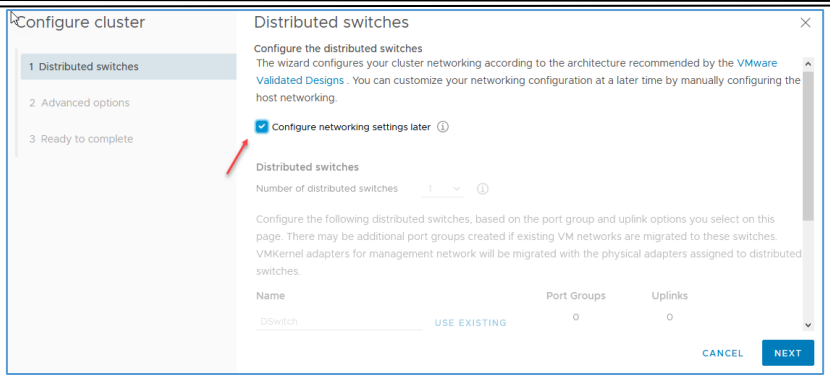
همان‌طور که در شکل ۱۲-۱۸۹، مشاهده می‌کنید، دو سرور به Cluster به درستی اضافه شده و حالا باید آن را Config کنید، برای این کار بر روی CONFIGURE کلیک کنید.



شکل ۱۲- ۱۸۹ بررسی *High Availability (HA)* در *Vcenter*

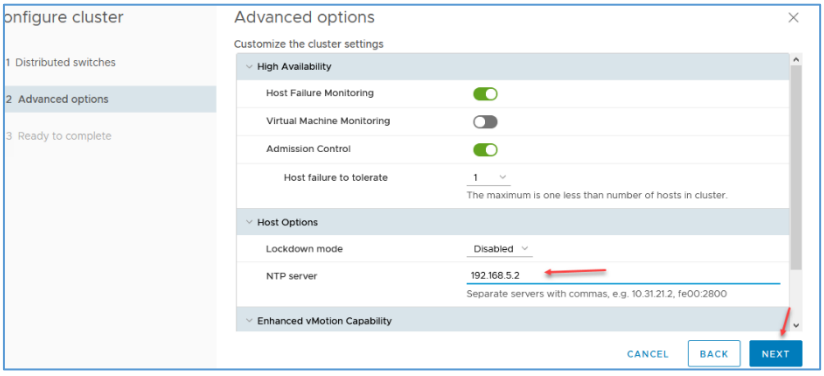
در شکل ۱۲-۱۹۰، می‌توانید برای پایداری بیشتر Distributed Switchs را فعال کنید، که فعلاً نیاز نیست و تیک آن را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



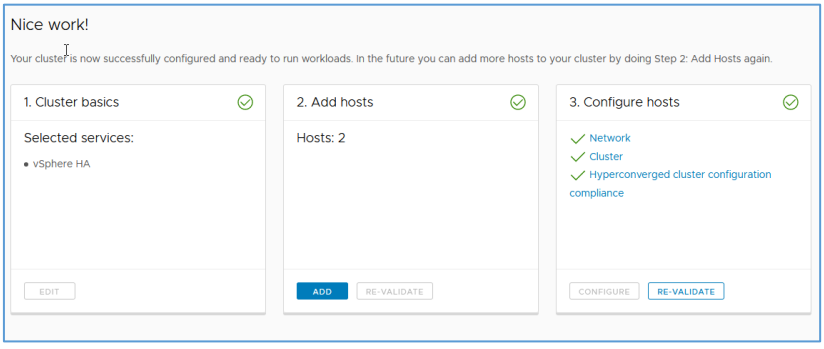
شکل ۱۲- ۱۹۰ بررسی *High Availability (HA) در Vcenter*

در شکل ۱۲–۱۹۱، برای تنظیم زمان و تاریخ باید آدرس سرور NTP خود را در قسمت NTP Server وارد کنید.



شکل ۱۲- ۱۹۱ بررسی *High Availability (HA) در Vcenter*

همان‌طور که در شکل ۱۲–۱۹۲، مشاهده می‌کنید سرویس به درستی اجرا شده است.

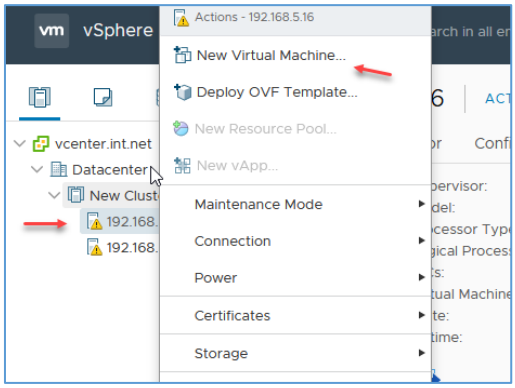


شکل ۱۲- ۱۹۲ بررسی *High Availability (HA) در Vcenter*

مرحله چهارم – ایجاد ماشین مجازی و فعال‌سازی Fault Tlorance

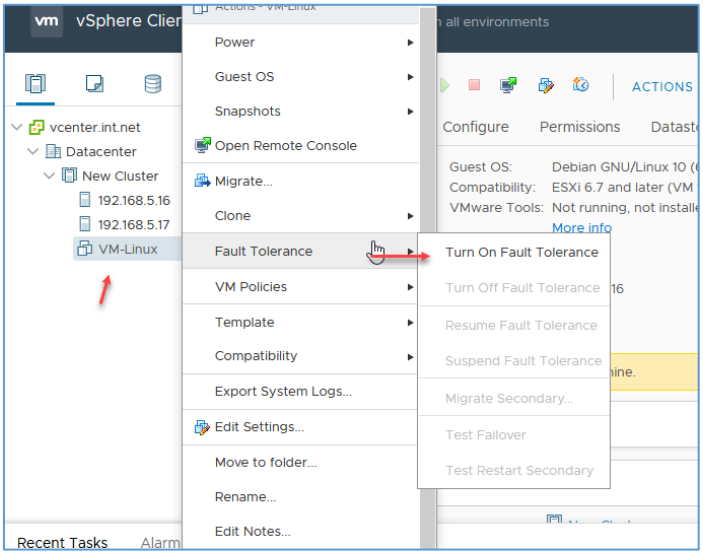
www.takbook.com

در ادامه به مانند شکل ۱۲-۱۹۳، یک ماشین مجازی ایجاد و بر روی آن یک سیستم عامل نصب می‌کنیم و بعد بر روی آن سرویس Fault Tlorance را فعال می‌کنیم، با این کار یک کپی از این ماشین به سرور دوم انتقال پیدا خواهد کرد.



شکل ۱۲- ۱۹۳ بررسی High Availability (HA) در Vcenter

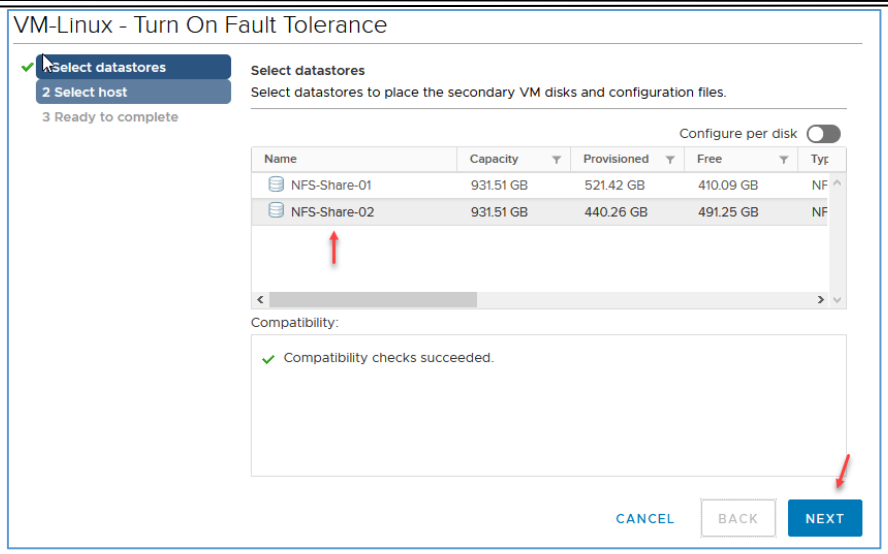
بعد ایجاد ماشین مجازی، به مانند شکل ۱۲-۱۹۴، بر روی آن کلیک راست کنید و از قسمت Fault Tolerance گزینه‌ی Turn On Fault Tolerance کلیک کنید.



شکل ۱۲- ۱۹۴ بررسی High Availability (HA) در Vcenter

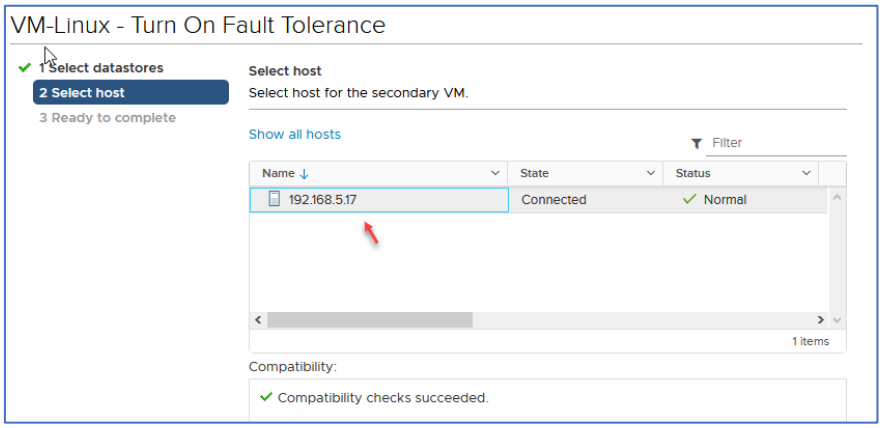
در شکل ۱۲-۱۹۵، باید هارد اشتراکی دوم را انتخاب کنید، همان‌طور که مشاهده می‌کنید در این قسمت فقط هارد اشتراکی نمایان شده و هاردهای اصلی سرورها نمایش داده نشده است.

www.takbook.com



شکل ۱۲- ۱۹۵ بررسی *High Availability (HA)* در *Vcenter*

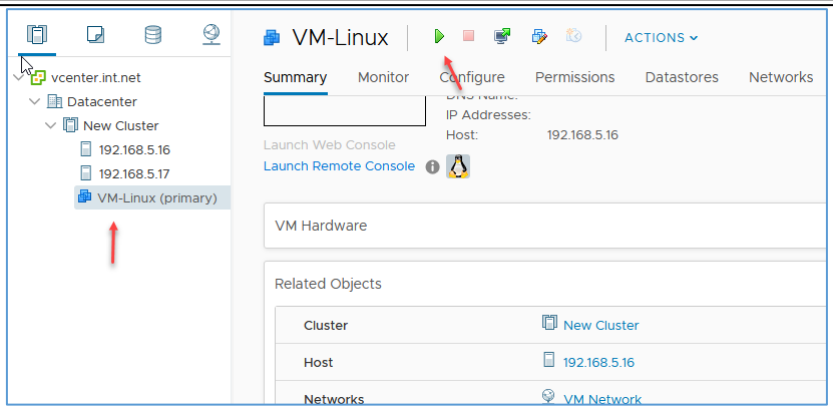
درشکل ۱۲–۱۹٦، باید سرور ESXi دوم را انتخاب کنید، توجه داشته باشید اگر کلاً از یک فضای اشتراکی استفاده می‌کردید در این قسمت با اخطاری روبرو می‌شدید.



شکل ۱۲- ۱۹۶ بررسی *High Availability (HA)* در *Vcenter*

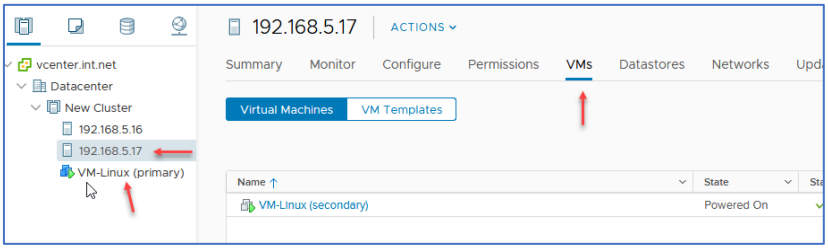
همان‌طور که در شکل ۱۲–۱۹۷، مشاهده می‌کنید، کلمه Primary بر روی ماشین مورد نظر نمایان شده و این نشان دهنده‌ی این است که سرور اصلی فعال است و سرویس Fault در حال کار است.

www.takbook.com



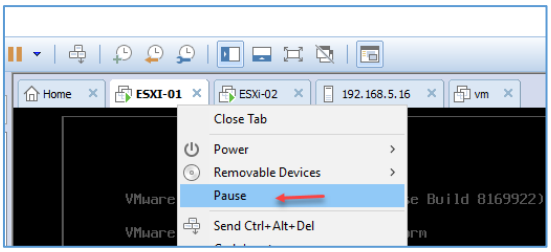
شکل ۱۲- ۱۹۷ بررسی *High Availability (HA)* در *Vcenter*

همان‌طور که در شکل ۱۲-۱۹۸، مشاهده می‌کنید ماشین مورد نظر به سرور دوم انتقال پیدا کرده و به خوبی در حال کار است.



شکل ۱۲- ۱۹۸ بررسی *High Availability (HA)* در *Vcenter*

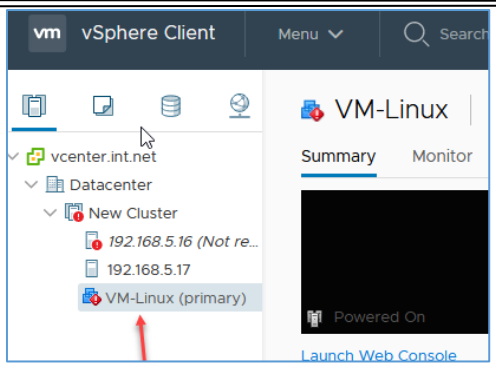
حالا اگر به مانند شکل ۱۲-۱۹۹، سرور اول ESXi را که سرور اصلی ما است غیرفعال کنیم ماشین مورد نظر بدون مشکل باید به کار خود ادامه دهد، برای همین بر روی سرور اول کلیک راست کنید و گزینه‌ی Pause را انتخاب کنید.



شکل ۱۲- ۱۹۹ بررسی *High Availability (HA)* در *Vcenter*

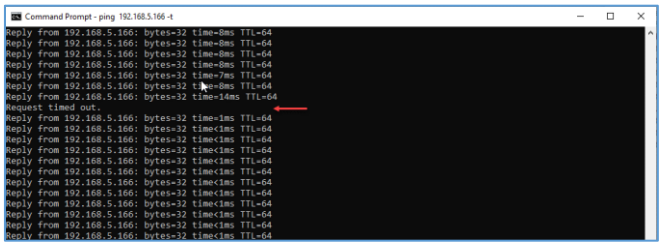
همان‌طور که در شکل ۱۲-۲۰۰، مشاهده می‌کنید سرور ESXi اول، از کار افتاده و علامت اخطار قرمز رنگ بر روی سرور و ماشین قرار گرفته است، این بدان معنا است که ماشین مورد نظر در حال کار بر روی سرور دوم است .

www.takbook.com



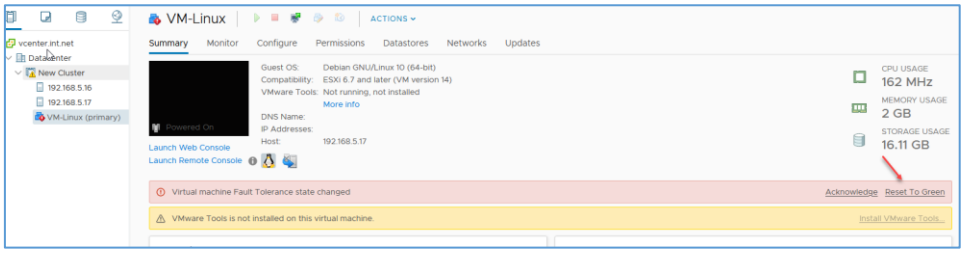
شکل ۱۲- ۲۰۰ بررسی *High Availability (HA)* در *Vcenter*

در شکل ۱۲-۲۰۱، Ping ماشین مورد نظر را مشاهده می‌کنید که فقط یک Time out در زمان قطع شدن سرور اول داده است و دوباره به کار خود بر روی سرور دوم ادامه داده است.



شکل ۱۲- ۲۰۱ بررسی *High Availability (HA)* در *Vcenter*

بعد از اینکه سرور اول را تعمیر و روشن کردید، می‌توانید صفحه مورد نظر را به مانند شکل ۱۲-۲۰۲، Refresh یا اینکه بر روی Reset to Green کلیک کنید تا ماشین به حالت اول برگردد.



شکل ۱۲- ۲۰۲ بررسی *High Availability (HA)* در *Vcenter*

با این کار توانستیم دو سرور ESXi را به یک Vcenter که بر روی آن Cluster فعال شده است را اضافه و عملیات Fault tolerance را بر روی آن پیاده‌سازی کنیم.

www.takbook.com

فصل سیزدهم

Veeam Backup & Replication

یک نرم‌افزار قدرتمند در پشتیبان‌گیری است که حداکثر اطمینان را برای شما به ارمغان می‌آورد؛ با این نرم‌افزار فوق‌العاده می‌توانید از نرم‌افزارها، فایل‌ها، سایت‌ها و... پشتیبان تهیّه کنید و کمتر از چند دقیقه آن را برگردانید. نرم‌افزار Veeam، یکی از بهترین‌ها در بازار نرم‌افزارها است و به خاطر اطمینان کامل در بازگردانی اطّلاعات، رقیبی مقابل خود نمی‌بیند.

این‌نرم افزار به مانند دیگر نرم‌افزارها دارای نیازمندی‌هایی برای نصب است که در جدول ۱۳-۱ و۱۳-۲، آنها را مورد بررسی قرار می‌دهیم.

نیازمندی سخت‌افزاری

جدول ۱۳- ۱ نیازمندی سخت‌افزاری

پردازنده	پردازنده بهتر است، حداقل دو هسته‌ای و ۲ گیگاهرتز سرعت داشته باشد، بهترین پیشنهاد پردازندهی ۸ هسته‌ای.
رم	حداقل رم باید ٤ گیگابایت باشد تا عملکرد متوسّط از سرور را داشته باشیم، بهترین پیشنهاد رم ١٦ گیگابایت است.
کارت شبکه	بهترین حالت استفاده از کارت شبکه، گیگابایت است تا حداکثر سرعت را در انتقال فایل داشته باشیم، بهترین پیشنهاد کارت شبکه‌ی 10G است.
هارد دیسک	برای نصب و راه‌اندازی، حداقل باید ٤ گیگابایت محلّ ذخیره‌سازی داشته باشیم، البتّه برای اجرای Backup و ذخیره این فایل‌ها باید هاردهایی با ظرفیّت بالا به نسبت شبکه داشته باشیم تا کلّ اطّلاعات شبکهٔ ما را پشتیبانی کند.

نیازمندی نرم‌افزاری

جدول ۱۳- ۲ نیازمندی نرم‌افزاری

سیستم عامل	از سیستم عامل ویندوز که لیست آن در زیر آمده است، می‌توان استفاده کرد: • Microsoft Windows Server 2025 • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 • Microsoft Windows Server 2008 SP2 • Microsoft Windows 10 • Microsoft Windows 8.x

www.takbook.com

• Microsoft Windows 7 SP1	
این نرم‌افزارهای اوّلیّه برای نصب Veeam مورد نیاز است: • Microsoft .NET Framework 4.5.2 • Microsoft Windows Installer 4.5 • Microsoft SQL Server Management Objects • Microsoft SQL Server System CLR Types • Microsoft Visual C++ 2010 Service Pack 1 redistributable package	نرم‌افزار

نصب نرم‌افزار Veeam Backup and Replication

برای دانلود نرم‌افزار مورد نظر به لینک زیر مراجعه کنید:

https://soft98.ir/software/backup/2098-veeam-backup.html

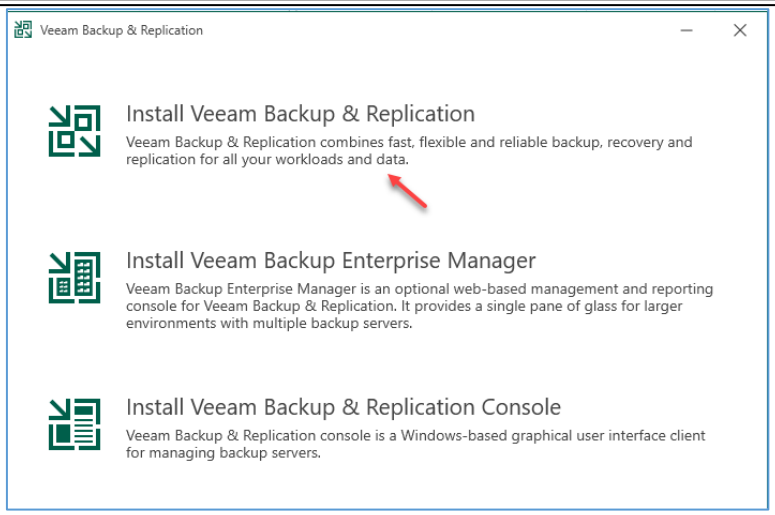
بعد از اجرای فایل Setup بر روی Install کلیک کنید، گزینه‌های دیگری نیز وجود دارد که گزینهٔ Enterprise برای مدیریّت چندین Backup & Replication Veeam کاربرد دارد و گزینهٔ Console نیز برای ارتباط از سیستم خودتان با سرورهای Veeam است که فعلاً کاری با آنها نداریم، در شکل۱۳-۱ بر روی Install کلیک کنید.



شکل ۱۳- ۱ نصب نرم‌افزار Veeam Backup and Replication

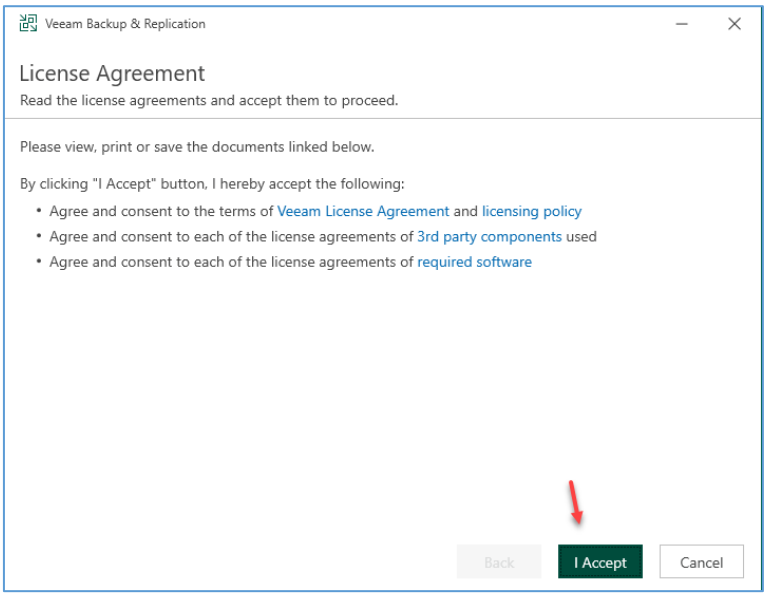
در شکل ۱۳-۲، سه گزینه را مشاهده می‌کنید، گزینه‌ی اول برای نصب و راه‌اندازی Veeam Backup and Replication است و گزینه اصلی برای این مورد است، گزینه‌ی Install Veeam Backup Enterprise Manager برای نصب ورژن تحت وب است که برای مدیریت چندین سرور Veeam کاربرد دارد، گزینه‌ی سوم فقط برای نصب کنسول مدیریتی است که بعدش باید به یک سرور Veeam متصل کنیم.

www.takbook.com



شکل ۱۳- ۲ نصب نرم‌افزار *Veeam Backup and Replication*

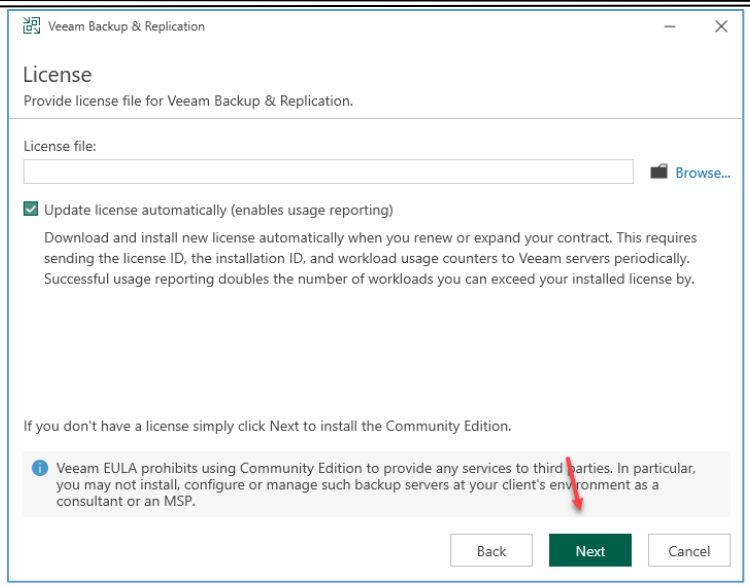
در شکل ۱۳-۳، قراردادنامه را بررسی و تأیید کنید و بر روی Next کلیک کنید.



شکل ۱۳- ۳ نصب نرم‌افزار *Veeam Backup and Replication*

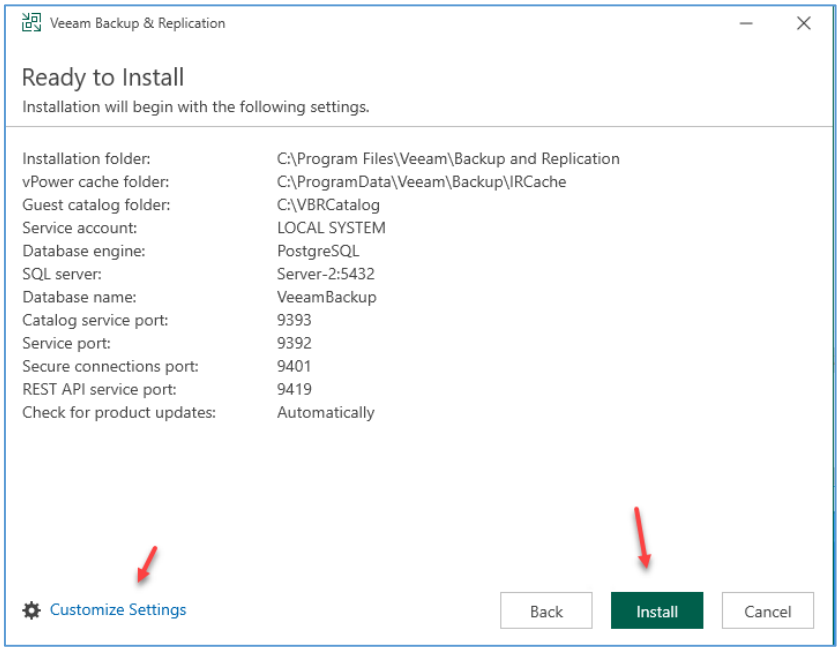
در شکل ۱۳-٤، اگر لایسنس نرم‌افزار را خریداری کردید، بر روی Browse کلیک کنید و فایل لایسنس را معرّفی کنید و اگر لایسنسی در اختیار ندارید، می‌توانید از آن صرف نظر کنید و بر روی Next کلیک کنید، توجه داشته باشید سرور به اینترنت متصل نباشد.

www.takbook.com



شکل ۱۳- ۴ نصب نرم‌افزار *Veeam Backup and Replication*

در شکل ۱۳-۵، بر روی Install کلیک کنید تا کار نصب آغاز شود و اگر می‌خواهید کاربری که نصب را انجام می‌دهد تغییر دهید و یا اینکه مسیر نصب را مشخص کنید باید بر روی Customize Settings کلیک کنید.



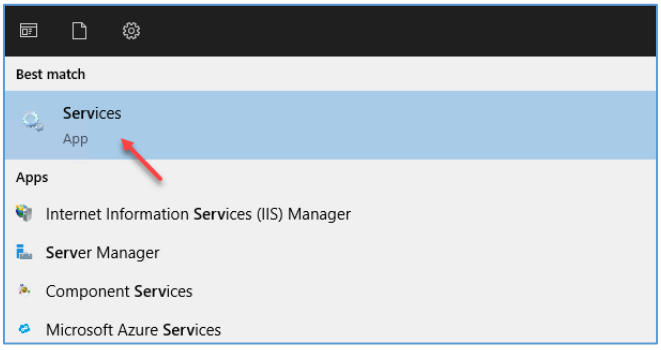
شکل ۱۳- ۵ نصب نرم‌افزار *Veeam Backup and Replication*

www.takbook.com

بسته به سرعت سیستم شما کار نصب زمان‌بر خواهد بود، نصب به صورت اتوماتیک انجام خواهد شد و نیاز به تنظیم خاصی نیست.

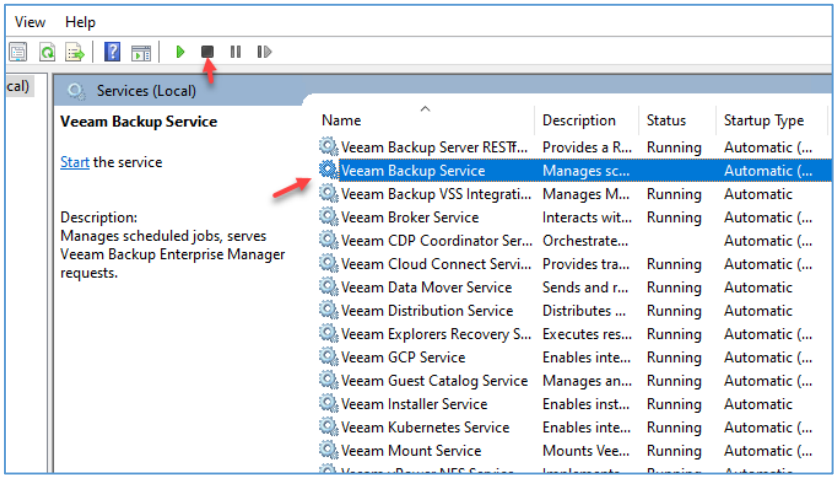
برای اینکه از امکانات کامل نرم‌افزار استفاده کنیم باید لایسنس آن را معرفی کنیم، اگر شرایط خرید آن را دارید بهتر است خریداری کنید، ولی اگر می‌خواهید آزمایشی و به صورت شخصی استفاده کنید می‌توانید از لایسنس‌های کرک شده استفاده کنید.

برای کرک کردن این نرم افزار اولین کاری که انجام می‌دهید Stop کردن سرویس Veeam است برای این کار به مانند شکل ۱۳-۶، وارد Services در سرور خود شوید.



شکل ۱۳- ۶ نصب نرم‌افزار *Veeam Backup and Replication*

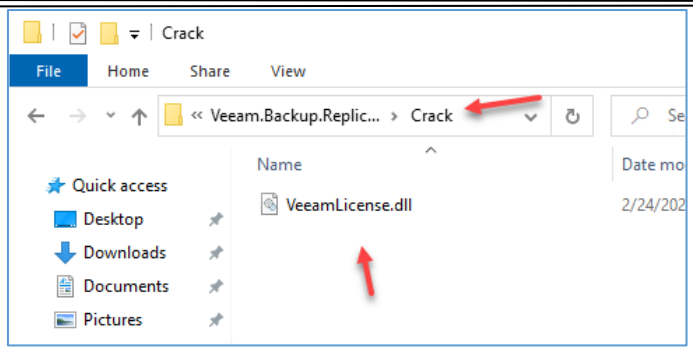
به مانند شکل ۱۳-۷، در لیست مورد نظر سرویس Veeam Backup Services را Stop کنید.



شکل ۱۳- ۷ نصب نرم‌افزار *Veeam Backup and Replication*

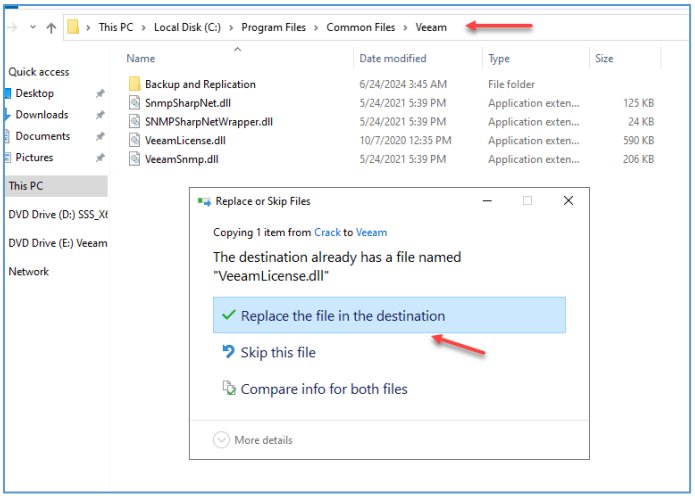
بعد از این کار به مانند شکل ۱۳-۸، وارد پوشه Crack در فایل دانلودی شوید و فایل مورد نظر را کپی کنید.

www.takbook.com



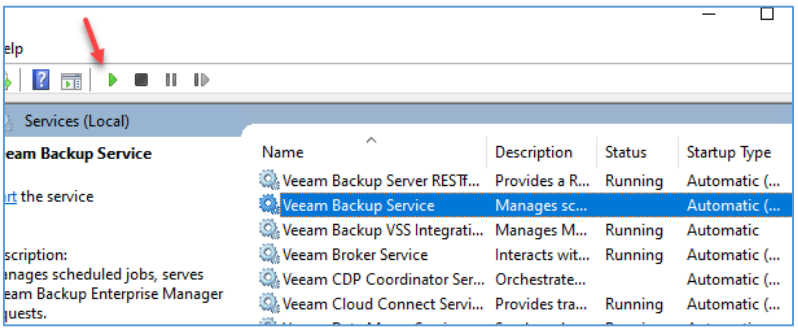
شکل ۱۳- ۸ فایل Crack

به مانند شکل ۱۳-۹، در مسیر مشخص شده فایل را جایگزین کنید.



شکل ۱۳- ۹ فایل Crack

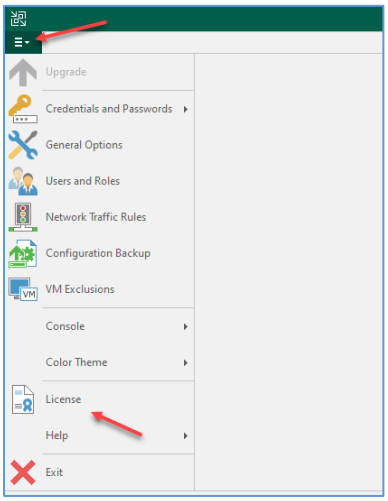
بعد از جایگزین کردن فایل مورد نظر به مانند شکل ۱۳-۱۰، وارد Services شوید و سرویس قبلی که Stop کرده بودید را روشن کنید:



شکل ۱۳- ۱۰ اجرای سرویس

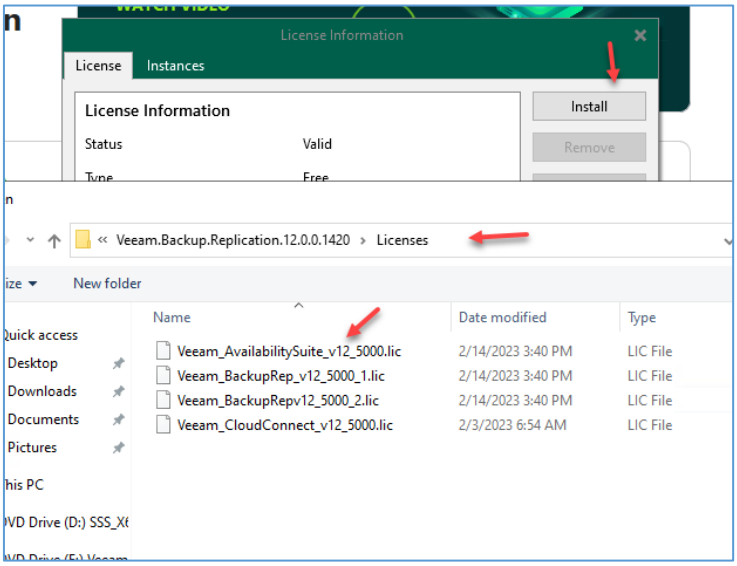
www.takbook.com

بعد از انجام مراحل بالا نرم افزار Veeam را اجرا کنید و به مانند شکل ۱۳-۱۱، وارد License شوید.



شکل ۱۳- ۱۱ بررسی لایسنس

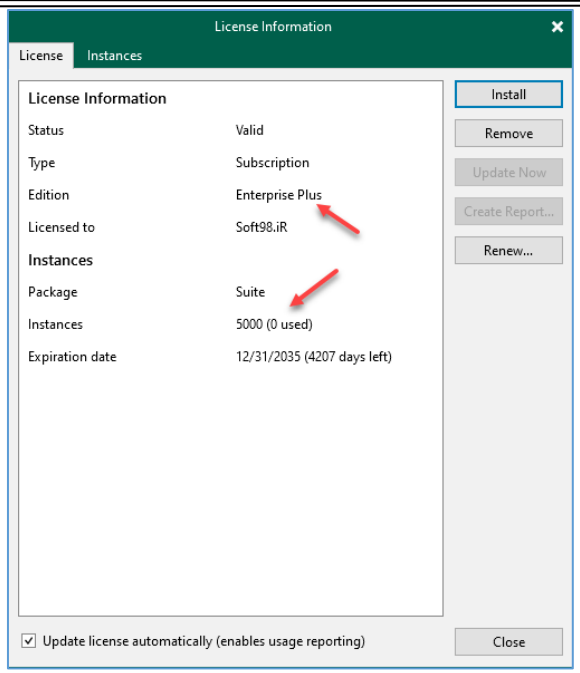
به مانند شکل ۱۳-۱۲، بر روی Install کلیک کنید، و وارد فایل دانلودی شوید و پوشه‌ی Licenses را باز کنید و لایسنس اول را انتخاب کنید.



شکل ۱۳- ۱۲ بررسی لایسنس

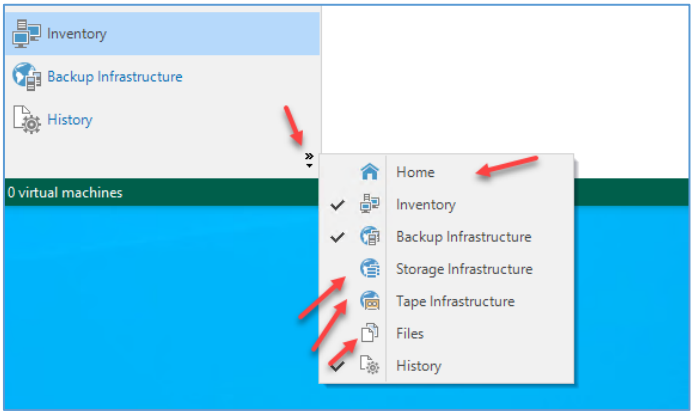
همان‌طور که در شکل ۱۳-۱۳، مشاهده می‌کنید لایسنس مورد نظر فعال شده است و حالا می‌توانید از نرم‌افزار به طور کامل استفاده کنید.

www.takbook.com



شکل ۱۳- ۱۳ بررسی لایسنس

زمانی که نرم‌افزار باز شد در پایین صفحه فلش مورد نظر را کلیک کنید و تمام ویژگی‌های آن را تیک بزنید تا در لیست ظاهر شود.

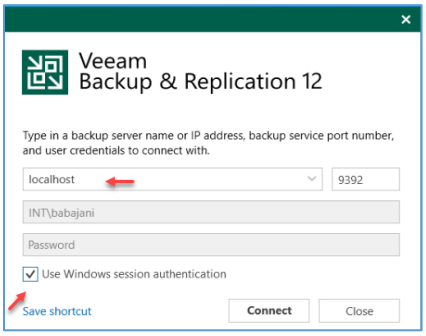


شکل ۱۳- ۱۴ بررسی گزینه‌های نرم‌افزار

بعد از نصب و فعال‌سازی، نرم‌افزار Veeam Backup را اجرا کنید، به مانند شکل ۱۳-۱۵، در قسمت اوّل، کلمهٔ Localhost نوشته شده است که اشاره می‌کند به سیستمی که در حال کار با آن هستید و نرم‌افزار بر روی آن نصب شده است، اگر نرم‌افزار بر روی سرور دیگری نصب شده باشد باید به جای Localhost،

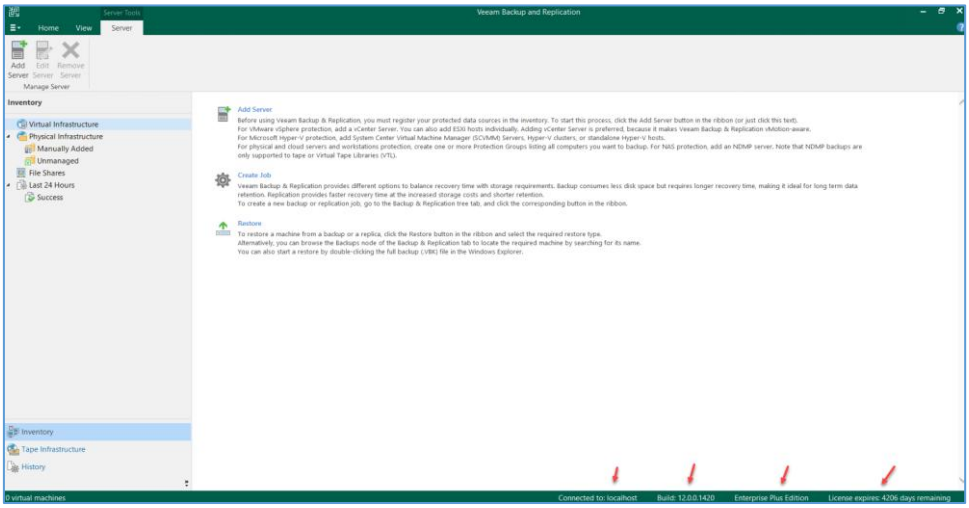
www.takbook.com

نام سرور مورد نظر را وارد کنید و شماره پورت مورد نظر که به صورت پیش‌فرض 9392 است را وارد کنید و باید توجه داشته باشید که این پورت در فایروال سرور بسته نباشد در ادامه برای ورود از همان کاربری استفاده می‌کند که با آن وارد سیستم شده‌اید؛ بر روی Connect کلیک کنید تا نرم‌افزار اجرا شود.



شکل ۱۳- ۱۵ ورود به برنامه

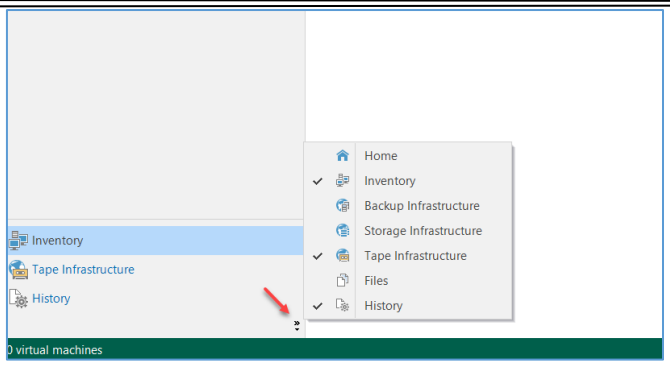
همان‌طور که در شکل ۱۳-۱۶، مشاهده می‌کنید، نرم‌افزار اجرا شده و آماده کار است، در نوار پایین آن مواردی را مشاهده می‌کنید مانند، آدرس سرور که در اینجا Localhost است، ورژن دقیق نرم‌افزار، نوع لایسنس و زمان انقضاء لایسنس مشخص شده است.



شکل ۱۳- ۱۶ بررسی نرم‌افزار

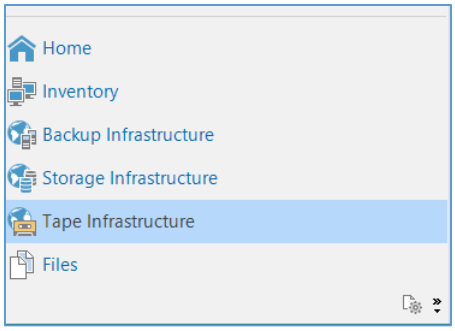
اگر به مانند شکل ۱۳-۱۷، در سمت چپ صفحه و قسمت پایین بر روی فلش مود نظر کلیک کنید گزینه‌های دیگر که دردسترس هستند را مشاهده می‌کنید که باید تیک آنها را انتخاب کنید.

www.takbook.com



شکل ۱۳- ۱۷ بررسی نرم افزار

حالا اگر بخواهیم گزینه‌ها را در شکل ۱۳-۱۸، بررسی کنیم، در قسمت Home اطلاعاتی مربوط به Jobها و نتیجه‌ها کارهایی که انجام می‌شود مشخص می‌شود، منظور از Jobها به وظایفی است که شما برای منابع خود مشخص می‌کنید، یعنی اینکه مشخص می‌کنید یک یا چند ماشین مجازی از کدام سرور انتخاب و در چه زمانی شروع به پشتیبانگیری شود و از این دست کارها که در ادامه بررسی خواهیم کرد.



شکل ۱۳- ۱۸ بررسی نرم افزارها

در قسمت Inventory منابعی که قرار است از آنها Backup تهیه شود را مشخص می‌کنیم، مانند سرورهای ESXi، سرورهای Hyper-V، Fileهای Share شده و....

در قسمت Backup Infrastructure باید محل ذخیره‌سازی Backupها را مشخص کنیم که وقتی در قسمت Job یک ماشین مجازی را انتخاب می‌کنید تا پشتیبان تهیه شود باید محل ذخیره‌سازی آن را مشخص کنید.

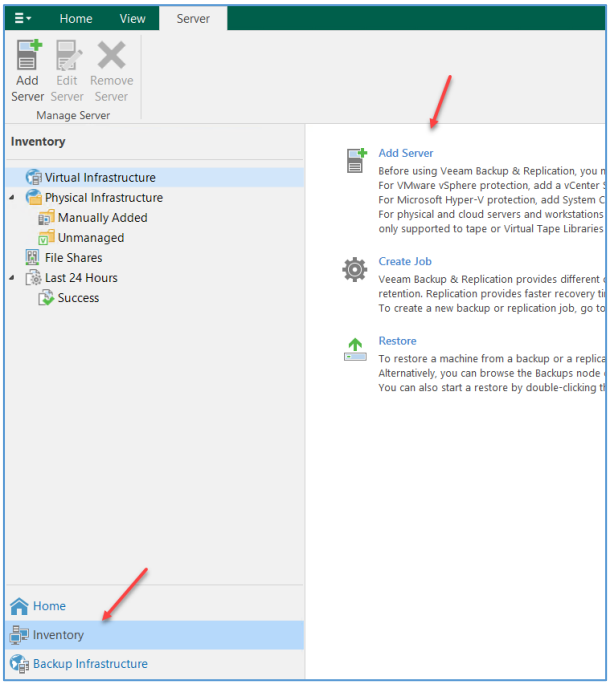
در قسمت Storage infrastructure می‌توانید سیستم‌های Storge شرکت‌های مختلف مانند Cisco و ... استفاده کنید و آن را به Veeam متصل کنید.

در قسمت Tape infrastructure می‌توانید ابزارهای ذخیره‌سازی قدیمی با نام Tape را به Veeam اضافه و استفاده کنید.

www.takbook.com

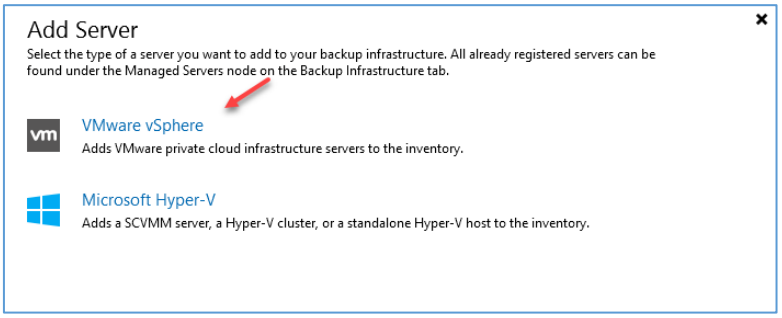
در قسمت File هم می‌توانید از File های موجود بر روی سرور Backup تهیه کنید.

برای شروع کار باید منابعی و سرورهایی که داریم را باید به نرم‌افزار Veeam Backup اضافه کنیم، برای این کار به مانند شکل ۱۳-۱۹، بر روی Add Server در قسمت Inventory کلیک کنید.



شکل ۱۳- ۱۹ اضافه کردن سرور

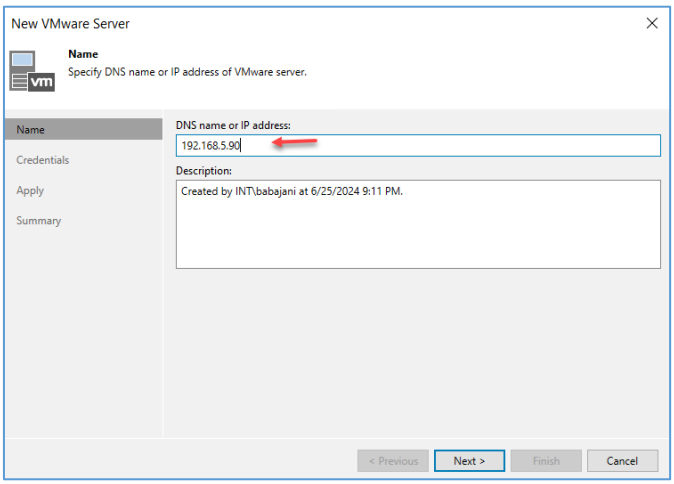
در شکل ۱۳-۲۰، دو گزینه وجود دارد، یکی برای شرکت VMware است و دیگری برای شرکت مایکروسافت، در مورد سرور Hyper-V در همین کتاب و در فصل هشتم به صورت کامل آن را بررسی و نصب آن را آموزش دادیم، اما برای اینکه با VMware هم آشنا شویم می‌خواهیم سرور ESXi آن را به لیست اضافه کنیم، برای شروع کار بر روی VMware Vsphere کلیک کنید.



شکل ۱۳- ۲۰ اضافه کردن سرور ESXi

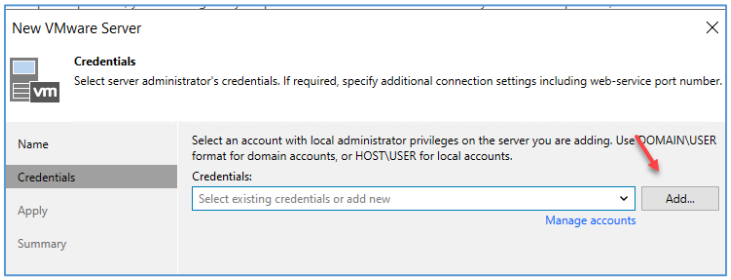
www.takbook.com

در شکل ۱۳-۲۱، باید آدرس سرور ESXI یا Vcenter خود را وارد کنید.



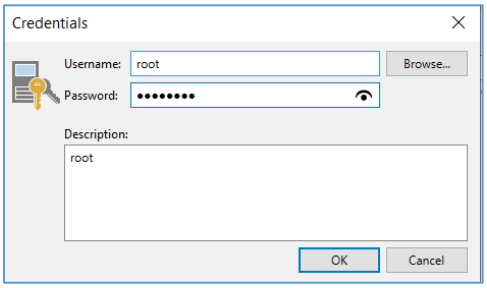
شکل ۱۳- ۲۱ اضافه کردن سرور

در شکل ۱۳-۲۲، باید نام کاربری که برای ورود به سرور استفاده می‌کنید را وارد کنید، برای این کار بر روی Add کلیک کنید.



شکل ۱۳- ۲۲ اضافه کردن سرور ESXi

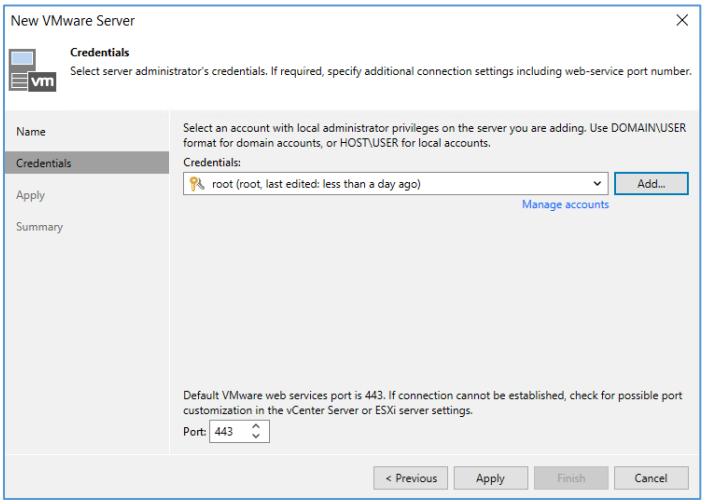
در شکل ۱۳-۲۳، نام کاربری و رمز عبور سرور را وارد کنید.



شکل ۱۳- ۲۳ اضافه کردن سرور ESXi

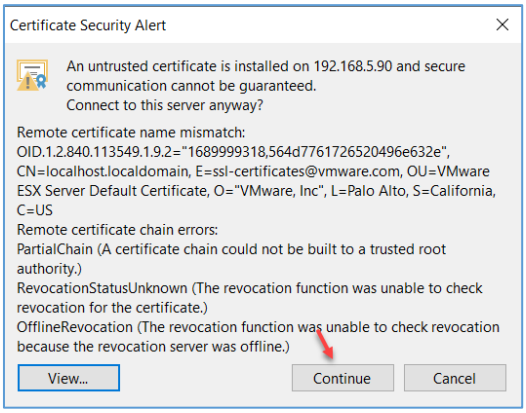
www.takbook.com

بعد از اضافه کردن نام کاربری و رمز عبور سرور مورد نظر به مانند شکل ۱۳-۲۴، بر روی Apply کلیک کنید تا به سرور متصل شویم.



شکل ۱۳- ۲۴ اضافه کردن سرور ESXi

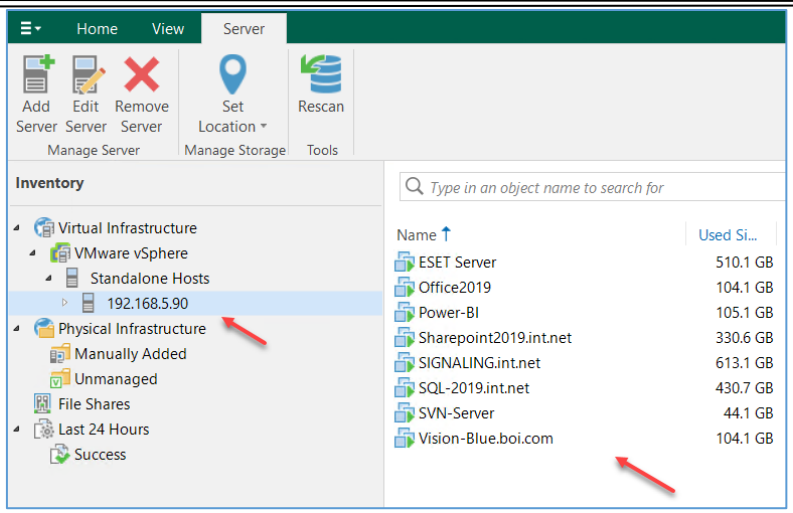
زمانی که می‌خواهید به سرور متصل شوید به مانند شکل ۱۳-۲۵، گزینه‌ی Untrusted Cerftificate را مشاهده می‌کنید که با ید بر روی Continue کلیک کنید تا سرور مورد نظر به لیست اضافه شود.



شکل ۱۳- ۲۵ اضافه کردن سرور ESXi

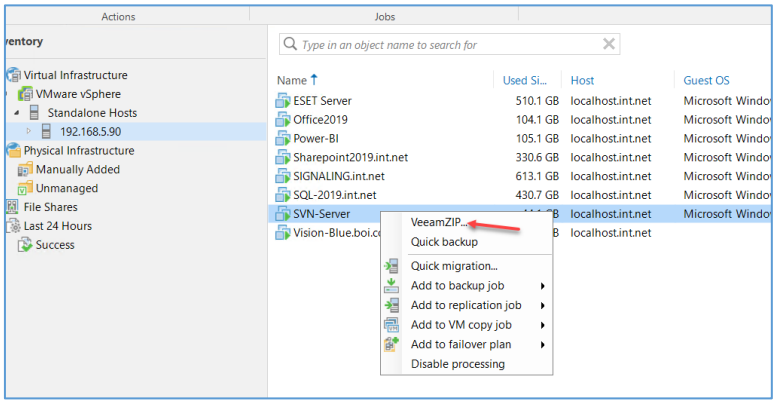
بعد از اینکه سرور را به لیست اضافه کردید می‌توانید به مانند شکل ۱۳-۲۶، بر روی آن کلیک کنید تا لیست ماشین‌های مجازی که بر روی آن قرار دارد را مشاهده کنید.

www.takbook.com



شکل ۱۳- ۲۶ بررسی ماشین‌های ESXi

در شکل ۱۳-۲۷، برای اینکه تستی از نرم‌افزار داشته باشیم، می‌توانیم بر روی ماشین مجازی خود در سرور Vmware کلیک راست کنیم و از آن پشتیبان تهیّه کنیم، همان‌طور که مشاهده می‌کنید گزینه‌های مختلفی را مشاهده می‌کنید، برای تست سریع گزینه‌ی VeeamZIP را انتخاب کنید.

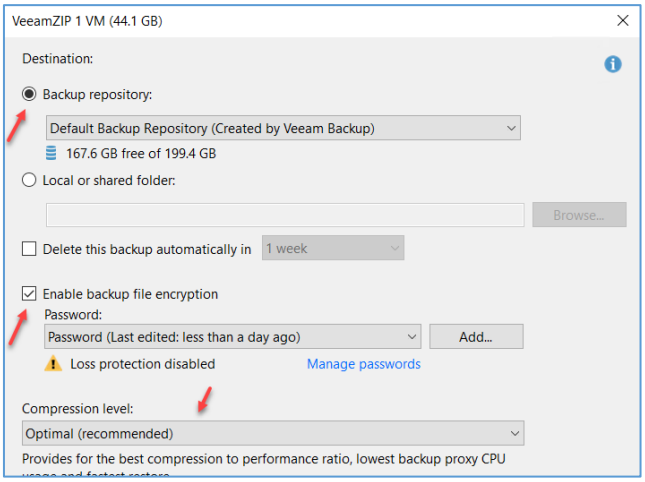


شکل ۱۳- ۲۷ بررسی ماشین‌های ESXi

در شکل ۱۳-۲۸، در قسمت Backup Repository باید مسیر ذخیره کردن فایل را انتخاب کنید که به صورت پیش‌فرض درایو اصلی سرور مشخص شده است، البته در ادامه روی این مورد کار خواهیم کرد و نحوه‌ی اضافه کردن مسیر جدید را بررسی می‌کنیم، اگر نیاز بود می‌توانید با انتخاب گزینه‌ی Local or Shared folder مسیری را برای آن مشخص کنید این مسیر می‌توانید در خود سرور باشد و یا اینکه مسیر اشتراک گذاری شده باشد.

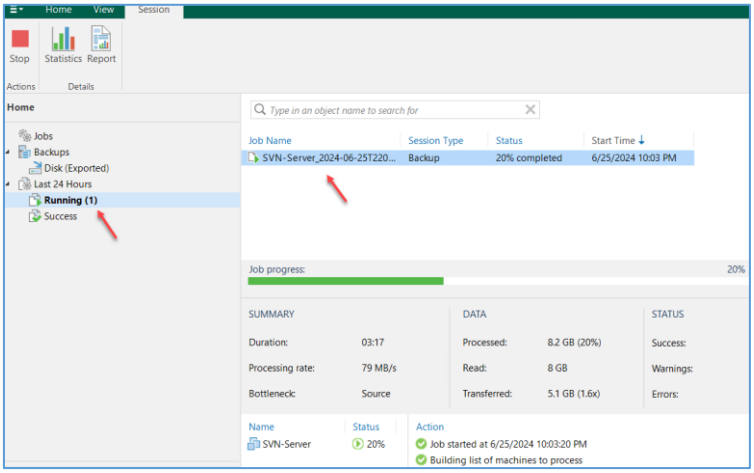
www.takbook.com

برای اینکه بر روی فایل Backup خود رمز عبور قرار دهید می‌توانید به مانند شکل ۱۳-۲۸، تیک گزینه‌ی Enable backup file encryption را انتخاب کنید و با کلیک بر روی Add یک رمز عبور برای آن مشخص کنید، در قسمت Compression level می‌توانید فشرده‌سازی فایل را تغییر دهید تا حجم آن کاهش پیدا کند.



شکل ۱۳- ۲۸ بررسی ماشین‌های ESXi

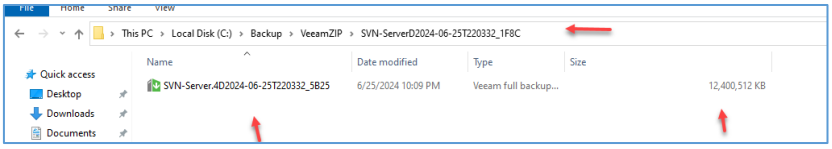
برای اینکه متوجّه شویم کاری که انجام دادیم به درستی عمل می‌کند یا نه باید به مانند شکل ۱۳-۲۹، از سمت چپ وارد Home شویم و در قسمت Last 24 Hours در قسمت Running یک Job در حال کار است که درصد پیشرفت آن را مشاهده می‌کنید، اگر بر روی آن کلیک کنید مقدار سرعت خواندن و نوشتن در مسیر جدید مشخص شده است و در قسمت Transfer هم اندازه فایل Backup گرفته شده مشخص شده است.



شکل ۱۳- ۲۹ گرفتن پشتیبان از سرور

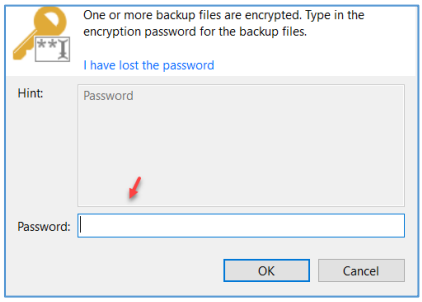
www.takbook.com

اگر بخواهیم فایل مورد نظر را مشاهده کنیم باید به مانند شکل ۱۳-۳۰، وارد مسیر زیر در درایو C شویم، همان‌طور که در شکل ۱۳-۳۰، مشاهده می‌کنید فایل مورد نظر ایجاد شده و حجم آن هم نزدیک به ۱۲ گیگابایت است.



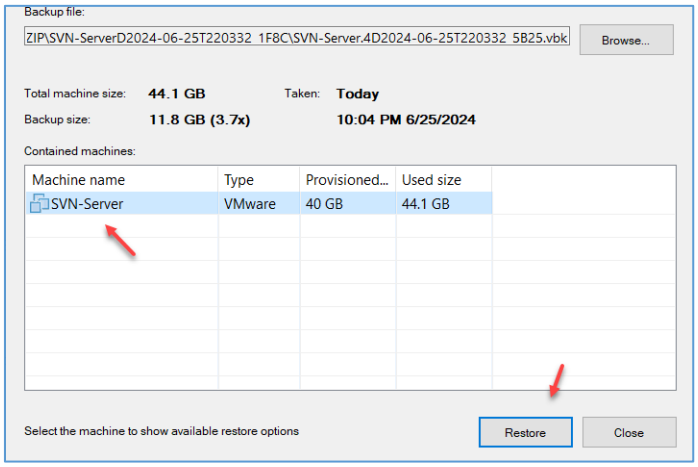
شکل ۱۳- ۳۰ فایل پشتبان سرور

اگر به مانند شکل ۱۳-۳۱، بر روی همین فایل دو بار کلیک کنید وارد Veeam Backup خواهیم شد، که در مرحله‌ی اول باید رمز عبوری را که برای آن مشخص کردید وارد کنید.



شکل ۱۳- ۳۱ اجرای فایل پشتیبان

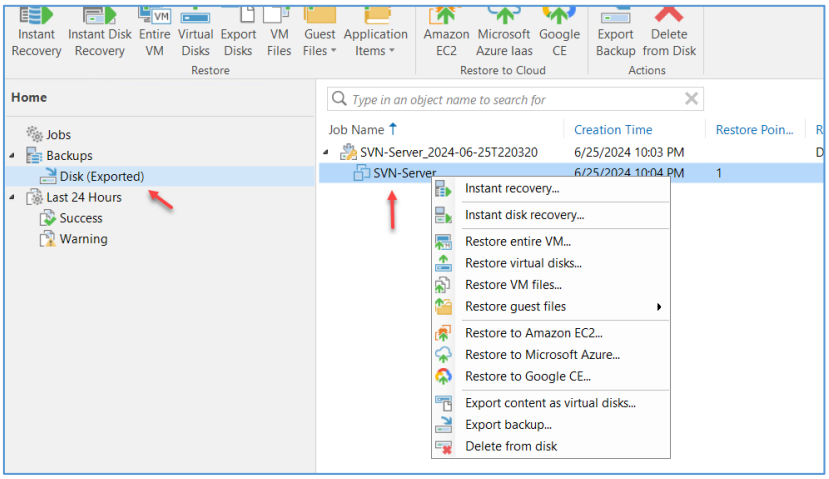
در شکل ۱۳-۳۱، اندازهٔ فایل بک آپ و تاریخ بک آپ آن مشخّص شده است که برای برگشت به آن روز باید فایل مورد نظر را از لیست، انتخاب و بر روی Restore کلیک کنید، توجه داشته باشید که نحوه‌ی Restore کردن را در ادامه بررسی خواهیم کرد.



شکل ۱۳- ۳۲ Restore کردن فایل پشتیبان

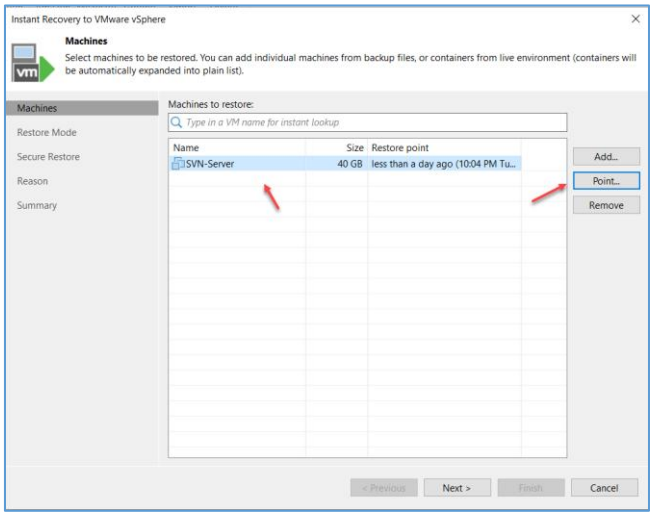
www.takbook.com

روش دیگر برای استفاده از فایل بک آپ، این است که به مانند شکل ۱۳-۳۳، از قسمت Home بر روی Disk کلیک کنید، با انتخاب این گزینه، صفحهٔ مربوط به فایل‌های پشتیبان‌گیری‌شده را مشاهده خواهید کرد، بر روی فایل مورد نظر کلیک راست کنید؛ در این منو گزینه‌های مختلف وجود دارد، با انتخاب گزینهٔ اوّل می‌توانید خیلی سریع Backup مورد نظر را برگردانید.



شکل ۱۳- ۳۳ بررسی ابزارهای فایل پشتیبان

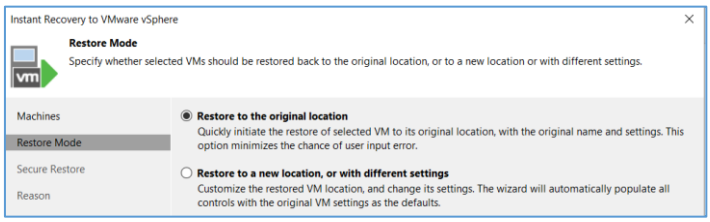
در شکل ۱۳-۳٤، آخرین بک آپ مربوط به ماشین مورد نظر را مشاهده می‌کنید که می‌توانید تاریخ مورد نظر خود را با کلیک بر روی Point انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۳- ۳۴ انتخاب Point مورد نظر

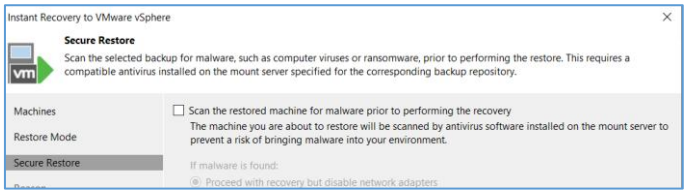
www.takbook.com

در شکل ۱۳-۳۵، دو گزینه وجود دارد که با انتخاب گزینهٔ اوّل می‌توانید فایل Backup را در همان قسمت اصلی که ماشین قرار دارد کپی کنید یعنی دقیقاً جایگزین ماشین قبلی خواهد شد، با انتخاب گزینهٔ دوّم، می‌توانید مسیر آن را در سرور دیگری تغییر دهید؛ در حال حاضر، گزینهٔ اوّل را انتخاب و بر روی Next کلیک کنید.



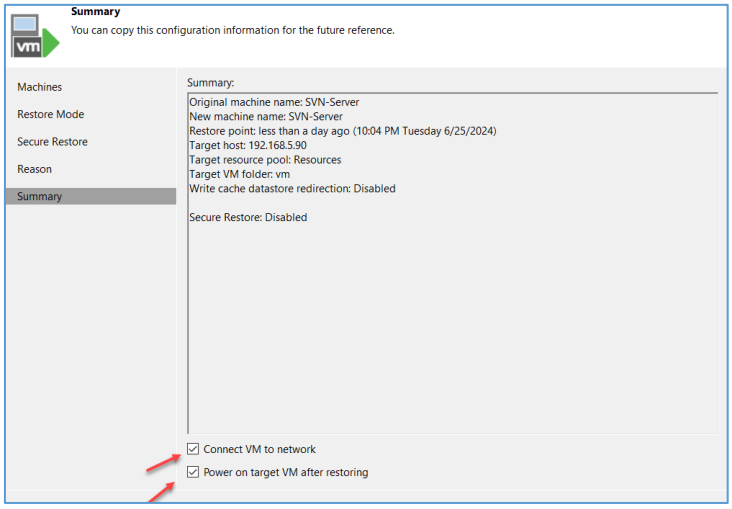
شکل ۱۳- ۳۵ Restore کردن فایل پشتیبان

در شکل ۱۳-۳۶، می‌توانید تیک گزینه‌ی مورد نظر را انتخاب کنید تا قبل از Restore، فایل‌ها از نظر ویروس بررسی شوند.



شکل ۱۳- ۳۶ Restore کردن فایل پشتیبان

در شکل ۱۳-۳۷، می‌توانید تیک گزینه‌های مورد نظر را انتخاب کنید که بعد از Restore، ماشین مورد نظر روشن و کارت شبکهٔ آن متّصل باشد.



شکل ۱۳- ۳۷ Restore کردن فایل پشتیبان

www.takbook.com

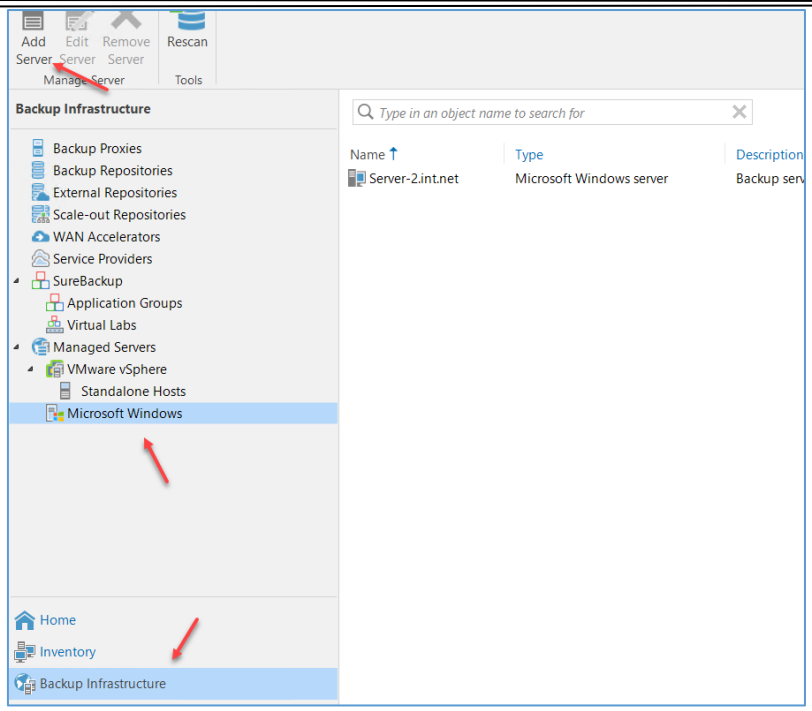
این روش‌هایی که با هم بررسی کردیم، کار ساده‌ای است که این نرم‌افزار می‌تواند به خوبی انجام دهد، در ادامه بیشتر با ویژگی‌های قدرتمند آن آشنا خواهیم شد.

۱-۱۳ اضافه‌کردن سرور Backup

در این قسمت می‌خواهیم کمی کار را با کیفیّت‌تر کنیم؛ کار اصولی و درست این است که شما یک سرور پشتیبان یا همان، Repository را به نرم‌افزار معرّفی کنید و ماشین‌ها و اطّلاعات را به آن سرور انتقال دهید، در این قسمت می‌خواهیم این کار را با هم انجام دهیم. سروری که برای این کار انتخاب می‌کنید باید از سرعت شبکهٔ خوبی برخوردار باشد، یعنی باید حداقل سرعت گیگابایت داشته باشد تا در موقع پشتیبان‌گیری با عملکرد ضعیف روبرو نشوید، در بخش دیگر باید هارد دیسک با ظرفیّت بالا برای آن در نظر بگیرید تا با کمبود فضا روبرو نشوید، اگر برای شرکت شما، هزینه ملاک نیست می‌توانید از هارد دیسک‌های SAS با سرعت بالا استفاده کنید که البتّه نیاز به سرورهایی دارد که آنها را پشتیبانی کند، برای شروع کار می‌خواهیم یک سرور معمولی را به نرم‌افزار اضافه کنیم تا در ادامهٔ کار بتوانیم به عنوان یک پشتیبان از آن استفاده کنیم.

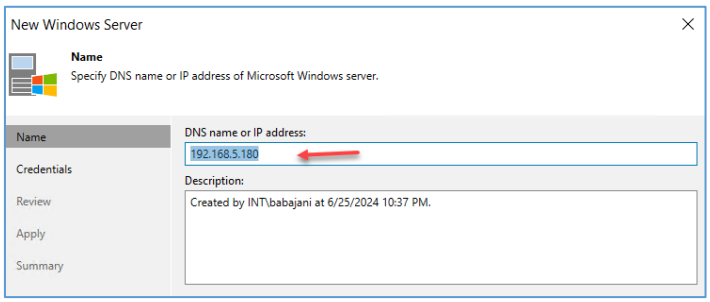
به مانند شکل ۱۳-۳۸، وارد قسمت Backup Infrastructure شوید و از سمت چپ بر روی Microsoft Windows کلیک کنید، به خاطر این موضوع این گزینه را انتخاب کردیم که سیستم عامل ما از نوع ویندوز است، بر روی Add Server کلیک کنید.

www.takbook.com



شکل ۱۳- ۳۸ اضافه‌کردن سرور Backup

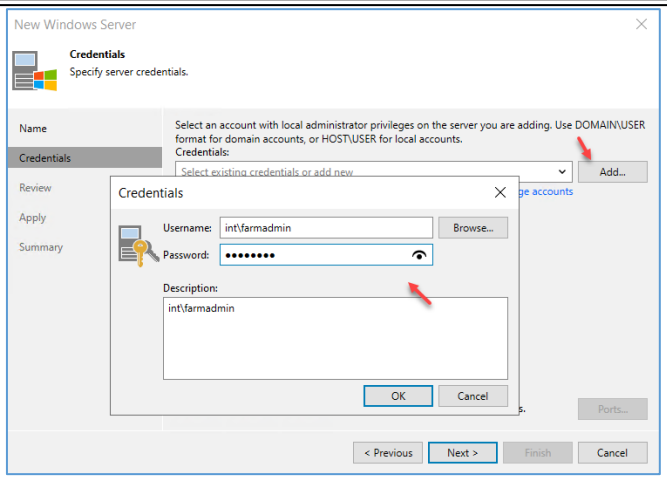
در شکل ۱۳-۳۹، باید در قسمت DNS name or IP address، نام یا آدرس IP سرور خود که قرار است نقش پشتیبان را بازی کند را وارد کنید و بر روی Next کلیک کنید.



شکل ۱۳- ۳۹ اضافه‌کردن سرور Backup

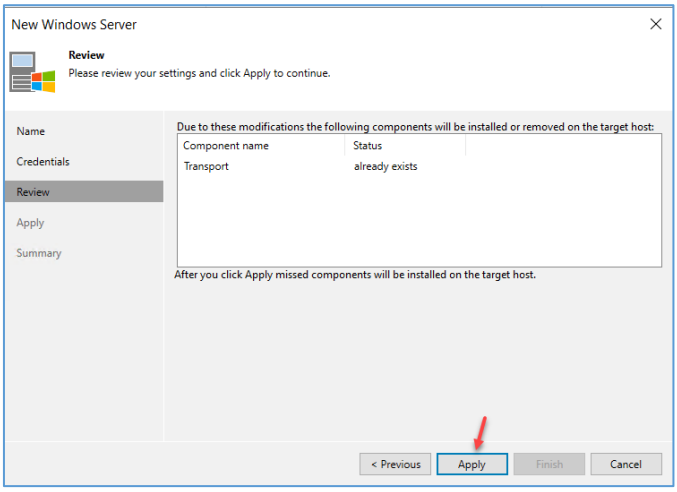
در شکل ۱۳-۴۰، با کلیک بر روی Add باید نام کاربری را وارد کنید که دسترسی کامل به شبکه داشته باشد، اگر از قبل وارد کردید، می‌توانید آن را از لیست انتخاب کنید؛ در قسمت پایین صفحه، گزینهٔ Port وجود دارد که پورت‌هایی را که نرم‌افزار نیاز دارد تا با این سرور در ارتباط باشد را مشخّص می‌کند که البتّه قابل تغییر است.

www.takbook.com



شکل ۱۳- ۴۰ اضافه‌کردن سرور Backup

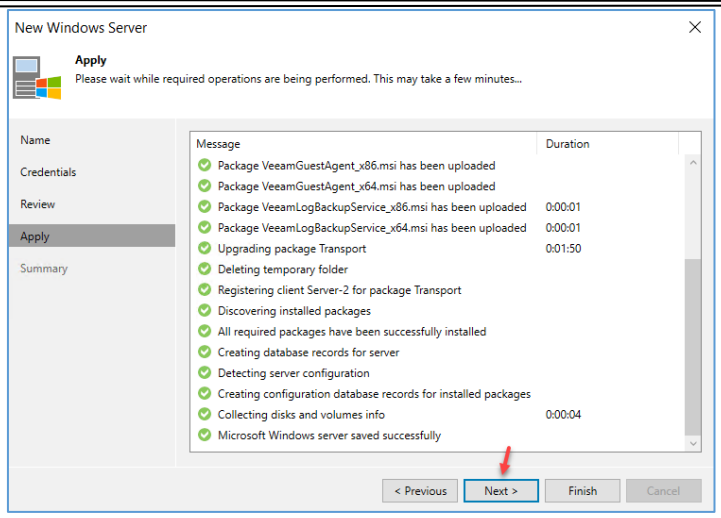
به مانند شکل ۱۳-۴۱، بر روی Apply کلیک کنید تا ارتباط با سرور پشتیبان انجام شود.



شکل ۱۳- ۴۱ اضافه‌کردن سرور Backup

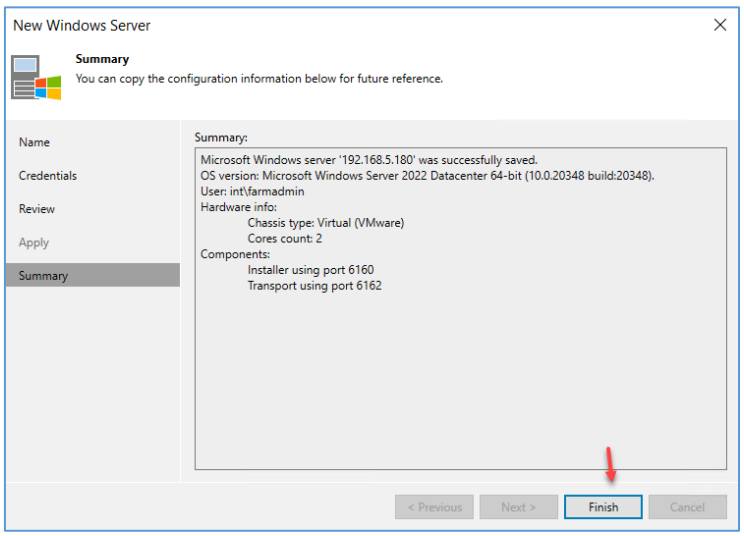
همان‌طور که در شکل ۱۳-۴۳، مشاهده می‌کنید با موفقیت این کار انجام شده است، بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۳- ۴۲ اضافه‌کردن سرور Backup

در شکل ۱۳-٤٤، توجه داشته باشید پورت‌های ارتباطی با سرور به صورت پیش‌فرض 6160 و 6162 است که این دو پورت باید در فایروال سرور باز شده باشد، به این نکته توجه کنید که یک پکیج با نام Veeam Transport به سیستم سرور انتقال داده شده و Veeam از طریق آن به سرور متصل می‌شود.

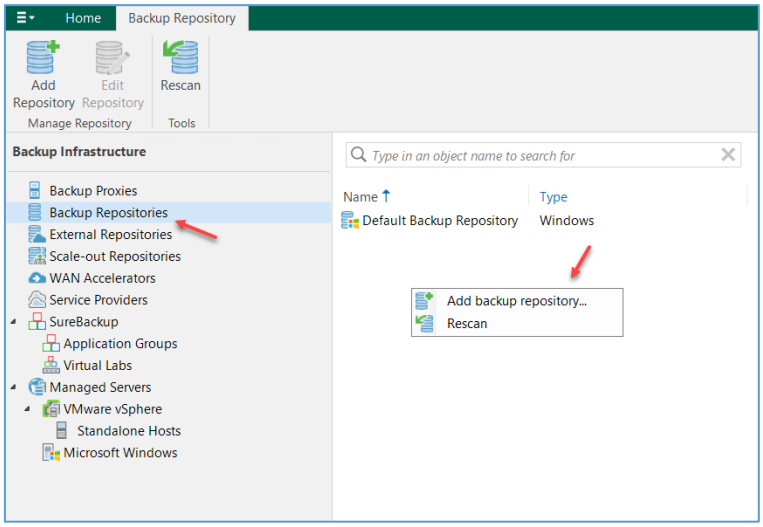


شکل ۱۳- ۴۳ اضافه‌کردن سرور Backup

در مرحلهٔ بعد باید سروری را که به عنوان پشتیبان اضافه کردید را در لیست Repositories یا همان، مخزن اضافه کنید تا بتوانید اطّلاعات را به آن انتقال دهید.

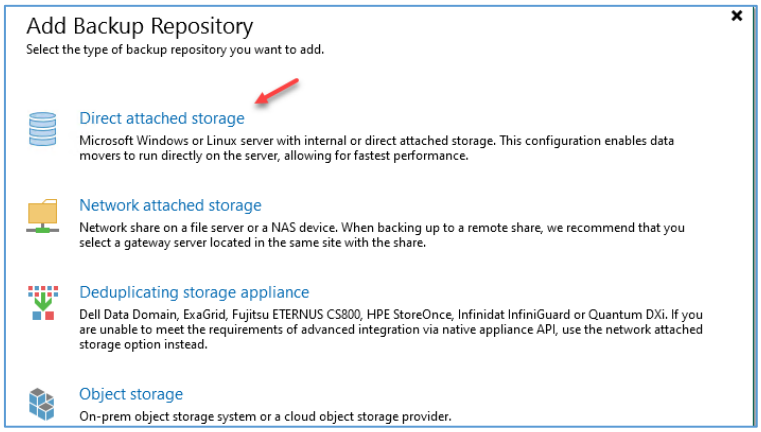
www.takbook.com

به مانند شکل ۱۳-٤٤، بر روی Backup Repositories کلیک کنید و در صفحه‌ی باز شده بر روی Add کلیک کنید، توجه داشته باشید در این قسمت می‌توانید هارد دیسک های خود سرور Veeam را هم به لیست اضافه کنید.



شکل ۱۳- ۴۴ اضافه کردید در لیست *Repositories*

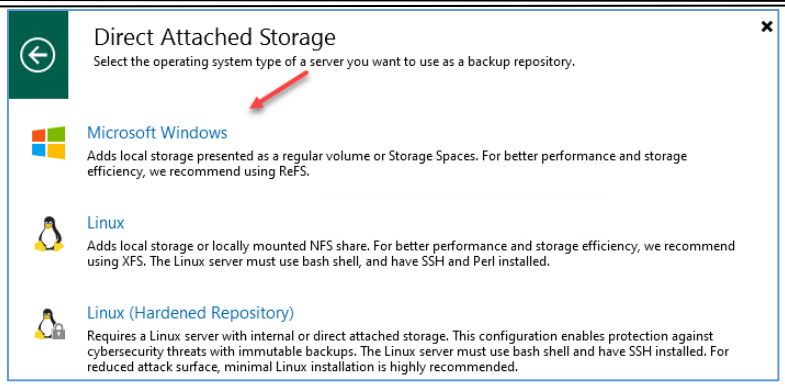
در شکل ۱۳-٤٥، گزینه‌ی Direct attached storage را انتخاب کنید، گزینه‌های دیگر را در ادامه بررسی خواهیم کرد.



شکل ۱۳- ۴۵ اضافه کردید در لیست *Repositories*

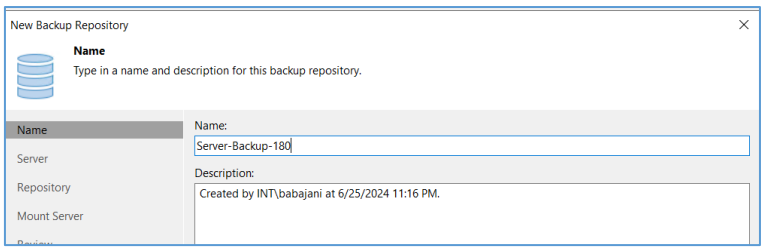
در شکل ۱۳-٤٦، سیستم عامل ویندوز را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



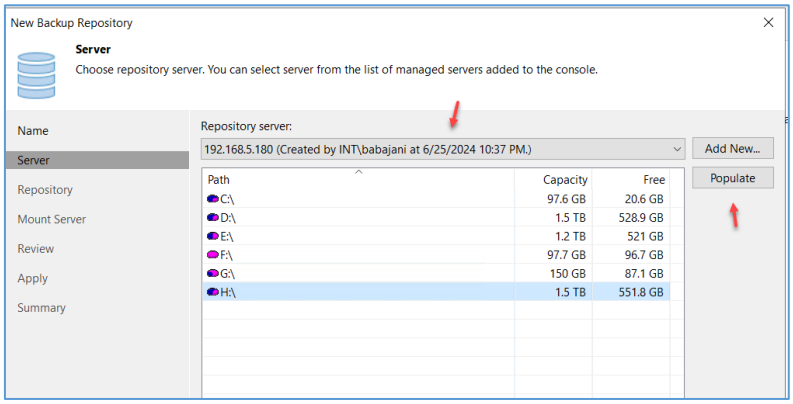
شکل ۱۳- ۴۶ اضافه کردید در لیست Repositories

در شکل ۱۳–٤۷، نام و توضیحات مربوط به سرور خود را وارد و بر روی Next کلیک کنید،



شکل ۱۳- ۴۷ اضافه کردید در لیست Repositories

در شکل ۱۳–٤۸، باید در قسمت Repository Server نام سرور جدید را انتخاب کنید و بر روی Populate کلیک کنید تا لیست تمام پارتیشن‌های موجود را به شما نمایش دهد، در شکل هر کدام از پارتیشن‌ها که فضای کافی داشتند را انتخاب کنید.

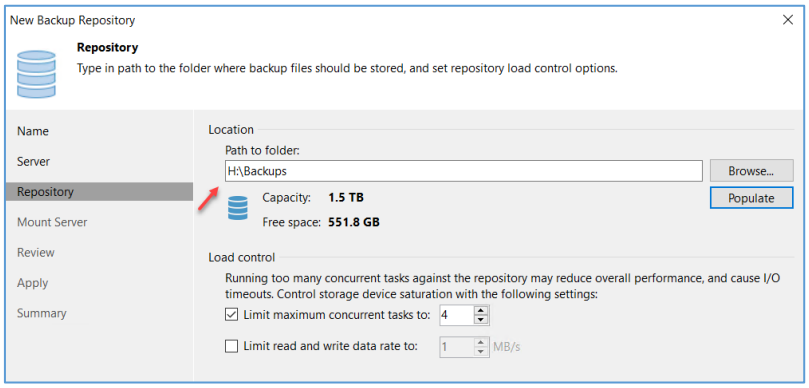


شکل ۱۳- ۴۸ اضافه کردید در لیست Repositories

www.takbook.com

در شکل ۱۳-٤۹، باید درایو مورد نظر را در سرور انتخاب کنید، اگر بر روی Populate کلیک کنید، فضای خالی آن را مشاهده خواهید کرد، در قسمت Limit maximum می‌توانید تعداد وظایف همزمان را مشخّص کنید، مثلاً در این شکل، ٤ در نظر گرفته شده است که همزمان، ٤ وظیفه می‌تواند بر روی این سیستم اجرا کرد.

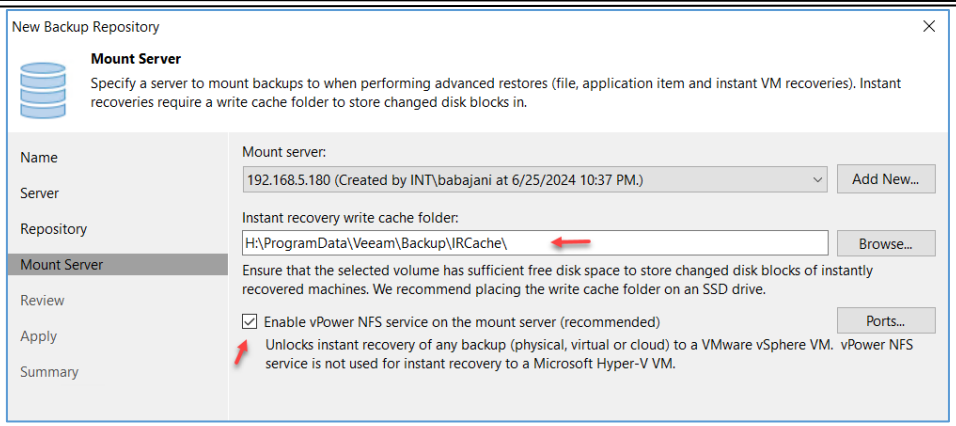
در قسمت Limit read، می‌توانید، مشخّص کنید که سرعت خواندن و نوشتن در سیستم سرور چقدر باشد، با این کار می‌توانید سرور را بهتر مدیریّت کنید و از اینکه سیستم مورد نظر از شبکه خارج شود، جلوگیری کنید.



شکل ۱۳- ۴۹ اضافه کردید در لیست Repositories

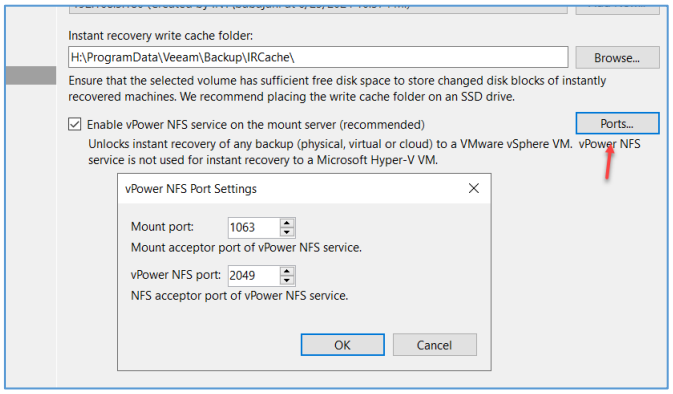
شکل ۱۳-۵۰، مربوط به Restore شدن اطّلاعات و نمایش آن است که باید Mount Server را مشخّص کنید که همان، سرور جدید است که اضافه کردیم، آن را انتخاب می‌کنیم، تیک گزینهٔ مورد نظر را انتخاب کنید تا سرویس NFS بر روی سیستم شما فعّال شود، توجّه داشته باشید، اگر از قبل بر روی سیستم شما این سرویس نصب شده باشد در این قسمت این سرویس نصب نخواهد شد و با مشکل روبرو می‌شوید، در قسمت Folder نیز می‌توانید آدرسی برای ذخیره شدن اطّلاعات مشخّص کنید.

www.takbook.com



شکل ۱۳- ۵۰ اضافه کردید در لیست Repositories

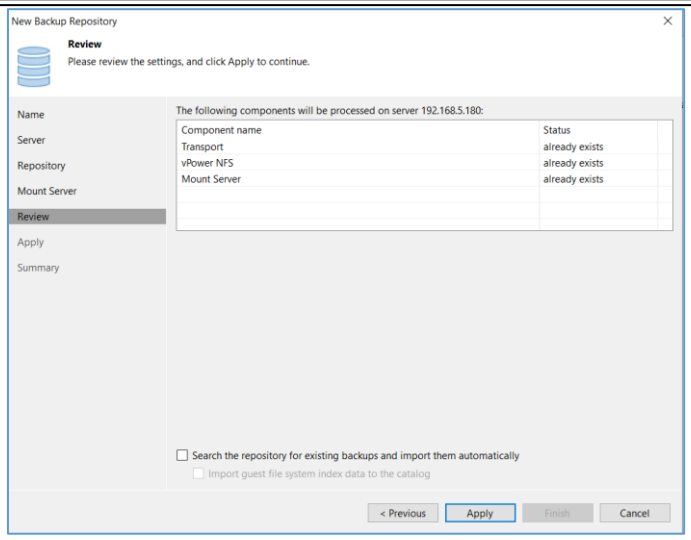
اگر در شکل ۱۳-۵۱، بر روی پورت کلیک کنید دو پورت را به مانند شکل ۱۳-۵۱، مشاهده می‌کنید که این دو پورت باید در فایروال باز باشند تا ارتباط بین سرورها برقرار باشد.



شکل ۱۳- ۵۱ اضافه کردید در لیست Repositories

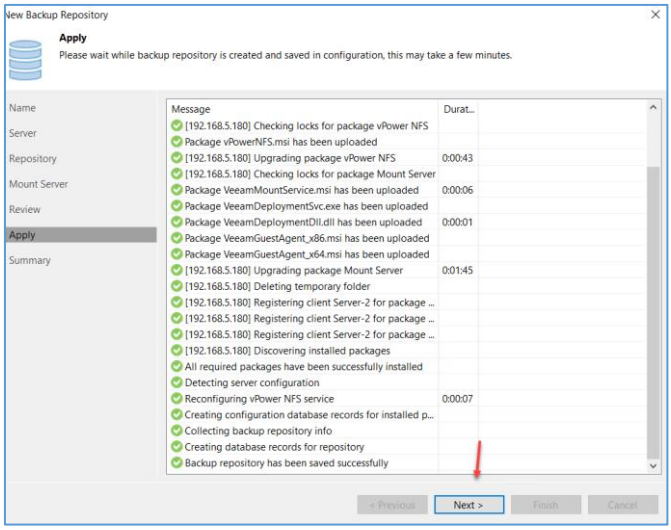
در شکل ۱۳-۵۲، بر روی Apply کلیک کنید تا تنظیمات مورد نظر انجام شود.

www.takbook.com



شکل ۱۳- ۵۲ اضافه کردید در لیست *Repositories*

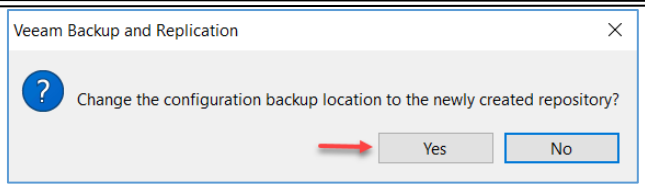
همان‌طور که در شکل ۱۳–۵۳، مشاهده می‌کنید تنظیمات مورد نظر با موفقیت انجام شده و می‌توانید بر روی Next و در انتها بر روی Finish کلیک کنید.



شکل ۱۳- ۵۳ اضافه کردید در لیست *Repositories*

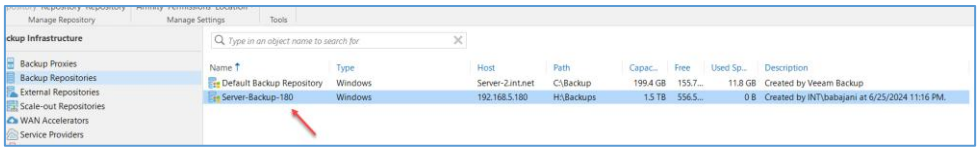
در شکل ۱۳–٥٤، سؤال می‌کند که آیا مایل هستید Repository پیش‌فرض را تغییر دهید یا نه، که باید بر روی Yes کلیک کنید.

www.takbook.com



شکل ۱۳- ۵۴ اضافه کردید در لیست Repositories

در شکل ۱۳-۵۵، مشخص شده است که Repository جدید به موفقیت به لیست اضافه شده است.

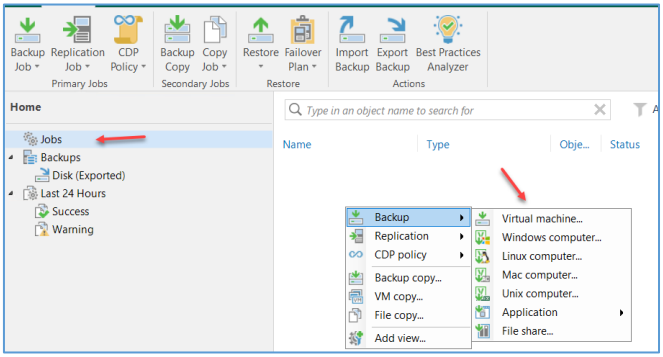


شکل ۱۳- ۵۵ اضافه کردید در لیست Repositories

بعد از انجام مراحل بالا برای تست وارد قسمت Fils شوید، در این قسمت می‌توانید سرورها و سیستم‌های کلاینتی خود را به لیست اضافه کنید و از آنها پشتیبان تهیّه کنید، برای تعریف سرور جدید و اضافه کردن آن به لیست باید بر روی Add Server کلیک کنید.

۱۳-۲ کار با Jobs در Veeam Backup

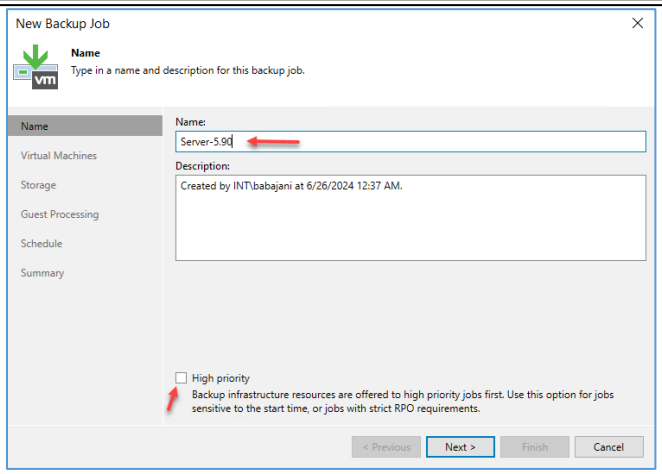
بعد از اینکه Repository را بررسی کردیم، حالا می‌خواهیم یک Job (کار) جدید ایجاد کنیم و از ماشین‌های مجازی خود پشتیبان تهیه کنیم، برای این کار به مانند شکل ۱۳-۵۶، در قسمت Home بر روی Jobs کلیک کنید و در صفحه‌ی باز شده کلیک راست کنید و گزینه‌ی Virtual machine را انتخاب کنید، گزینه‌های دیگر را در ادامه و در صورت نیاز بررسی می‌کنیم.



شکل ۱۳- ۵۶ کار با Jobs در Veeam Backup

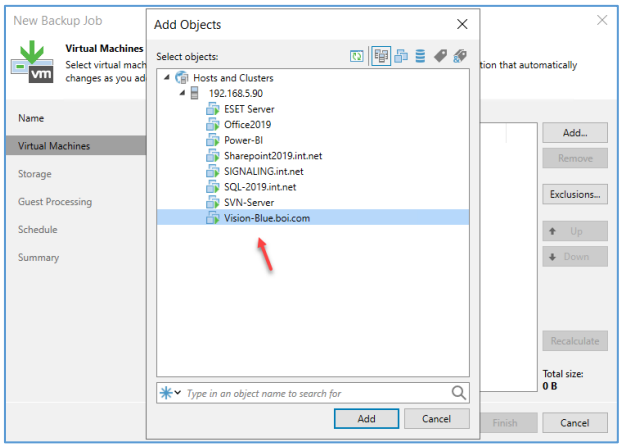
در شکل ۱۳-۵۷، یک نام برای کار خود وارد کنید و توضیحات مربوط به آن را در قسمت Description وارد کنید، توجه داشته باشید اگر می‌خواهید نرم‌افزار Veeam این Job را در اولویت بالاتری به نسبت Jobها دیگر قرار دهد می‌توانید تیک گزینه‌ی High priority را انتخاب کنید.

www.takbook.com



شکل ۱۳- ۵۷ کار با Jobs در Veeam Backup

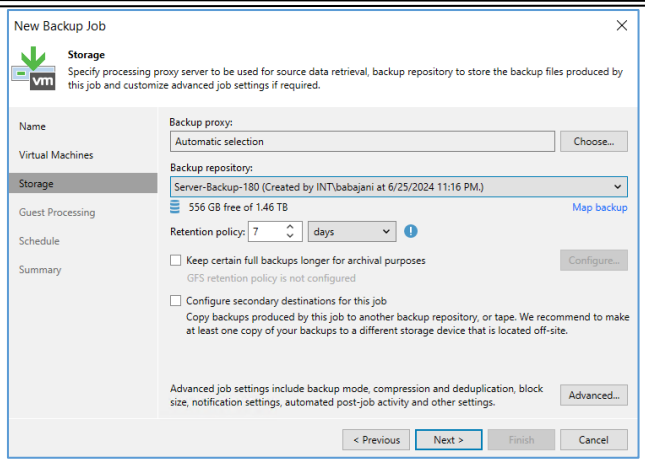
در شکل ۱۳–۵۸، بر روی Add کلیک کنید و یک یا چند ماشین مجازی خود را به لیست اضافه کنید و بر روی Next کلیک کنید.



شکل ۱۳- ۵۸ کار با Jobs در Veeam Backup

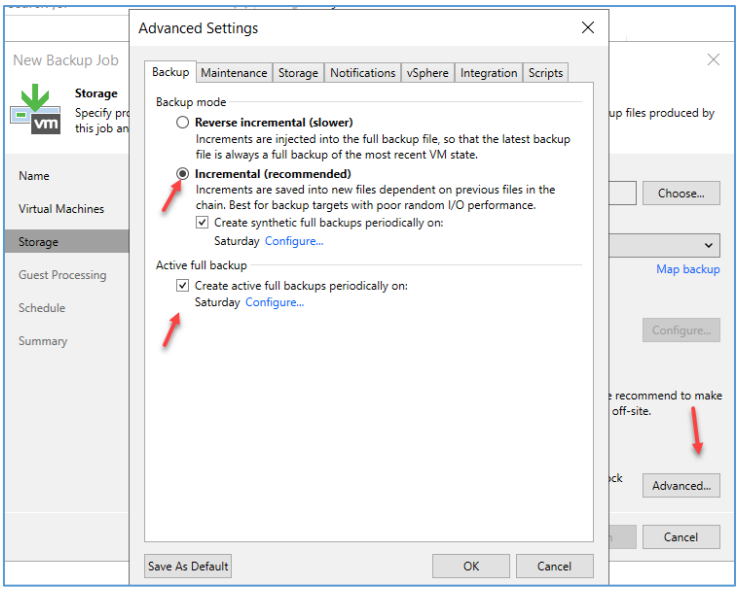
در شکل ۱۳–۵۹، در قسمت Backup Repository باید سرور مورد نظر خود را انتخاب کنید که بعد از انتخاب، مقدار فضای خالی از کل هارد را در زیر آن نمایش می‌دهد، اگر تیک گزینهٔ Configure secondary… را انتخاب کنید، می‌توانید در ادامه یک سرور Repository دیگری برای گرفتن پشتیبان دوّم انتخاب کنید، در قسمت Retention Policyکه عدد 7 نوشته شده مشخص می‌کند که تا 7 روز Backup مورد نظر را نگهداری می‌کند، گزینه‌ی Keep certain هم برای ایجاد یک Backup کامل در هفته، ماه و سال است که باید تیک آن را انتخاب و با کلیک بر روی Configure مقدار آن را مشخص کنید که در حال حاضر نیازی به این کار نیست.

www.takbook.com



شکل ۱۳- ۵۹ کار با Jobs در Veeam Backup

بعد از این کار به مانند شکل ۱۳-٦۰، بر روی Advanced کلیک کنید تا این گزینه را نیز بررسی کنیم، در قسمت Advanced و در تب Backup، گزینهٔ Incremental را برای انجام پشتیبان‌گیری از تغییرات انتخاب کنید و بعد، گزینهٔ Create active full را انتخاب کنید تا یک هفته، یک بار، یا چند بار از ماشین مورد نظر پشتیبان کامل تهیّه کند.

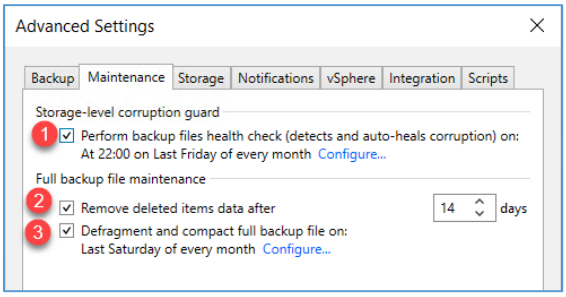


شکل ۱۳- ۶۰ کار با Jobs در Veeam Backup

در شکل ۱۳-٦۱ و در تب Maintenance، شمارهٔ یک، برای اینکه از وضعیّت سالم بودن فایل‌های پشتیبان خود مطّلع شویم، این گزینه را فعّال می‌کنیم، در قسمت شمارهٔ دو می‌توانید بر اساس روزهایی که نیاز به

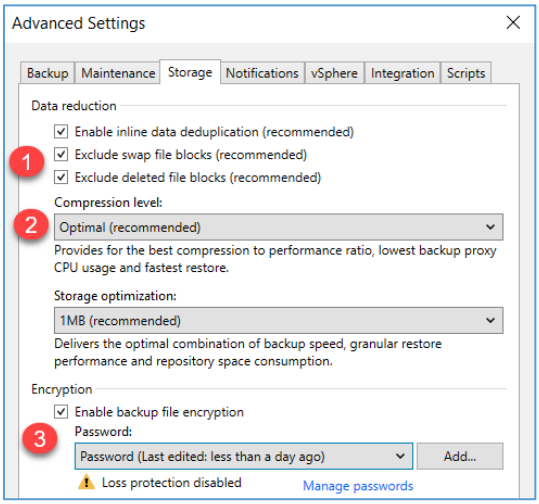
www.takbook.com

فایل پشتیبان دارید، یک عدد به جای عدد ۱۴ وارد کنید که تعداد روز نگهداری از فایل پشتیبان را به شما اعلام می‌کند، در قسمت شمارهٔ سه، اگر این گزینه را فعّال کنید، فایل‌های پشتیبان، Defragment خواهند شد تا فضای اضافی بین آنها کم شود.



شکل ۱۳- ۶۱ کار با Jobs در Veeam Backup

در شکل ۱۳-۶۲، در تب Storage و در قسمت اوّل می‌توانید تیک هر سه گزینه را که یک‌سری دستورالعمل برای کاهش حجم فایل پشتیبان است را انتخاب کنید، در قسمت شمارهٔ دو می‌توانید طبق سرعت پردازندهٔ خودتان، مقدار فشرده‌سازی فایل‌های پشتیبان را انتخاب کنید و در گزینهٔ پایین آن می‌توانید به نسبت سرعت شبکه، یکی از گزینه‌ها را انتخاب کنید، مثلاً اگر از شبکهٔ داخلی استفاده می‌کنید، انتخاب گزینه‌ی 1MB انتخاب خوبی است. در قسمت شماره‌ی سه می‌توانید با کلیک بر روی Add یک رمز عبور برای فایل‌های پشتیبان خود قرار دهید تا هر کسی نتواند از فایل‌ها استفاده کنید.



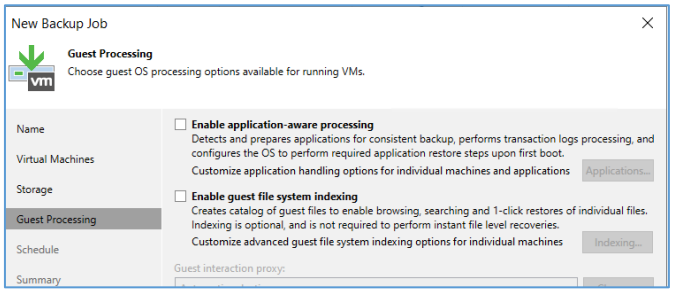
شکل ۱۳- ۶۲ کار با Jobs در Veeam Backup

در شکل ۱۳-۶۳، در تب Notification می‌توانید یک آدرس ایمیل وارد کنید تا تمام رویدادهایی که در این پشتیبانی انجام می‌شود، برای شما ایمیل شود، البته نیازی به تنظیم ان نیست و در ادامه در یک مبحث

www.takbook.com

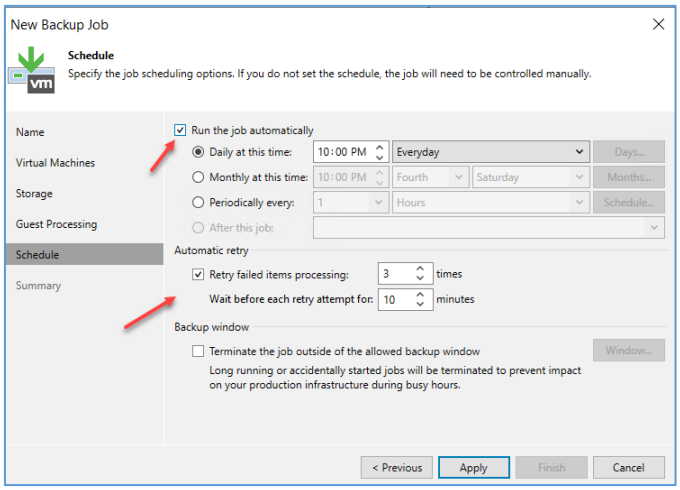
جدا این گزینه را فعال خواهیم کرد، بر روی OK کلیک کنید و صفحه‌ی Advanced را ببندید و بر روی Next کلیک کنید.

در شکل ۱۳-٦۳، با فعّال کردن این دو گزینه می‌توانید به نرم‌افزار این امکان را دهید تا بر روی سرویس‌ها، مانند Active Directory یا بر روی جدول‌های SQL تغییرات ایجاد کند که در ادامه این کار را انجام خواهیم داد و در حال حاضر نیازی به انتخاب این دو گزینه نیست.



شکل ۱۳- ۶۳ کار با Jobs در Veeam Backup

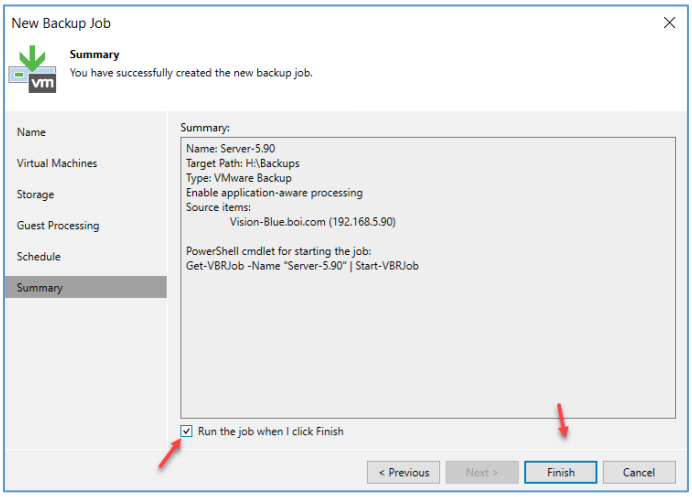
در شکل ۱۳-٦٤، باید زمان انجام کار را مشخّص کنید، بهتر است زمان مورد نظر در ساعات بیکاری شبکه باشد؛ بر روی Save کلیک کنید، در قسمت Automatic retry می‌توانید مشخص کنید که یک Job در صورت بروز مشکل چند بار تکرار شود که در اینجا 3 بار مشخص شده است و فاصله بین این تکرار 10 دقیقه در نظر گرفته شده است، در قسمت Backup Windows هم می‌توانید مشخص کنید در چه ساعتی این Job اجرا شود یا نشود.



شکل ۱۳- ۶۴ مشخص کردن زمان بندی

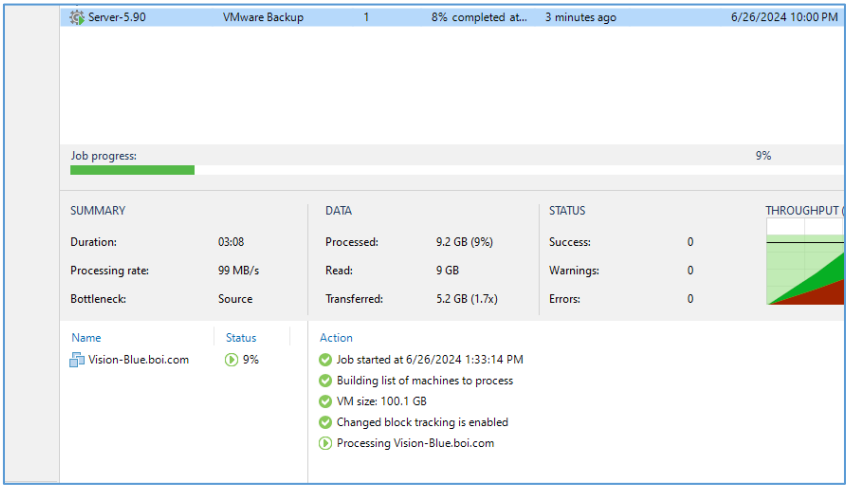
www.takbook.com

در شکل ۱۳-۶۵، اگر تیک گزینه‌ی مشخص شده را انتخاب کنید این Job شروع به کار می‌کند و از ماشین مورد نظر پشتیبان تهیه می‌کند.



شکل ۱۳- ۶۵ کار با Jobs در Veeam Backup

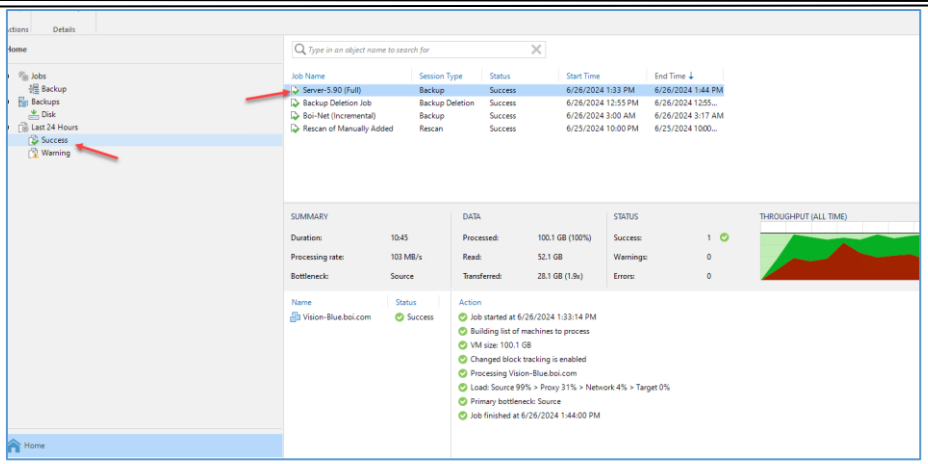
همان‌طور که در شکل ۱۳-۶۶، مشاهده می‌کنید، فایل پشتیبان در حال تکمیل است.



شکل ۱۳- ۶۶ اجرای Job مورد نظر

بعد از انجام شدن پشتیبان، به مانند شکل ۱۳-۶۷، در قسمت Success، می‌توانید موفّق بودن کار را مشاهده کنید.

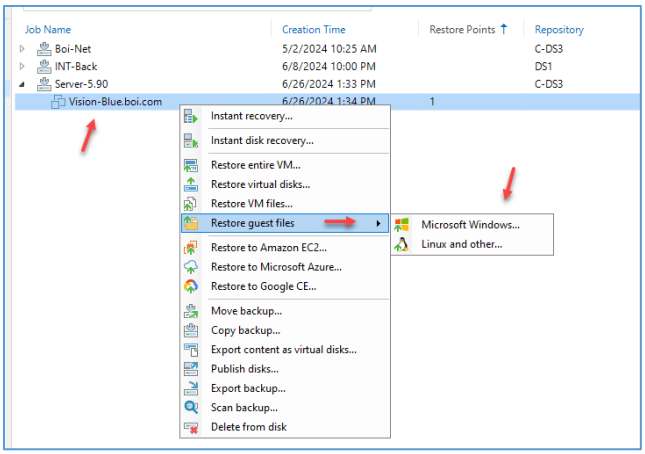
www.takbook.com



شکل ۱۳- ۶۷ اجرای Job مورد نظر

اگر به مانند شکل ۱۳-۶۸، وارد قسمت Disk شوید و Job مورد نظر را انتخاب کنید، در ستون Restore Point تعداد Backupهایی که برای Restore کردن در دسترس است مشخص شده است، در این شکل یک نوشته شده است که به دلیل اولین باراجرا شدن Job است اگر چند بار اجرا شود این عدد تغییر خواهد کرد.

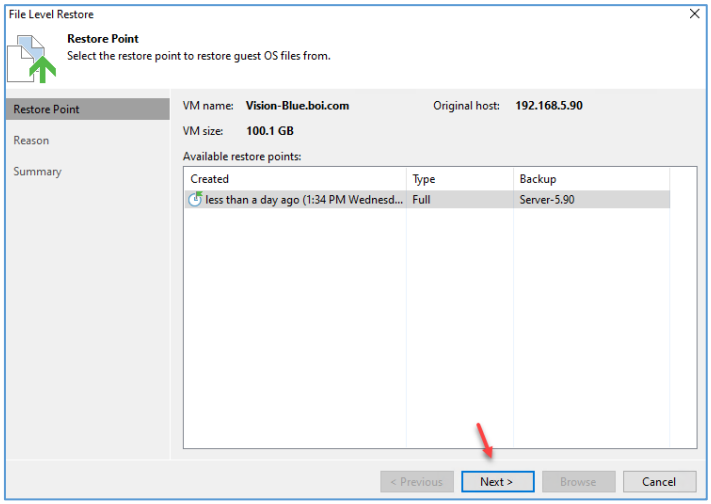
اگر بخواهید اطلاعات داخل یک ماشین مجازی را مشاهده کنیم و یک فایل مشخص را Restore کنیم به مانند شکل ۱۳-۶۸، بر روی ماشین مجازی که از آن Backup تهیه کردیم کلیک راست کنید واز قسمت Restore guest files گزینه‌ی Microsoft windows را انتخاب کنید.



شکل ۱۳- ۶۸ بررسی اطلاعات ماشین مجازی

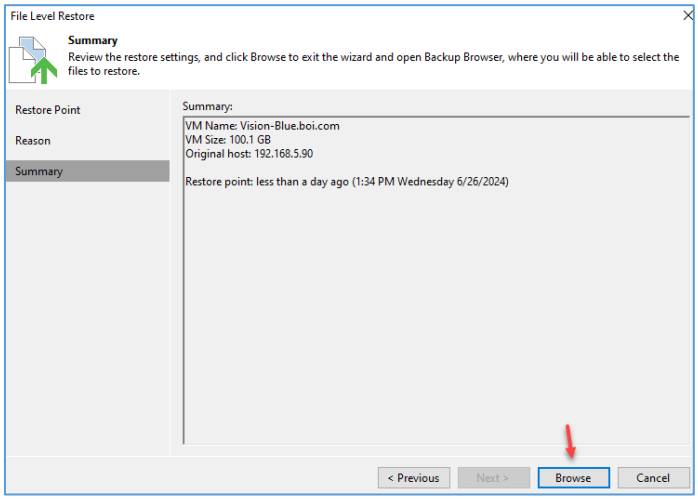
www.takbook.com

در شکل ۱۳-۶۹، باید یکی از زمان‌های Backup را انتخاب کنید، اگر توجه کنید در قسمت Type نوع فایل را برابر با Full قرار داده که نشان دهنده‌ی یک Backup کامل از ماشین مورد نظر است و حتی شما می‌توانید این نوع Backup را در یک جایی دیگر کپی و آن را Restore کنید.



شکل ۱۳- ۶۹ بررسی اطلاعات ماشین مجازی

در شکل ۱۳-۷۰، بر روی Browse کلیک کنید تا فایل‌های ماشین مجازی به شما نمایش داده شود.

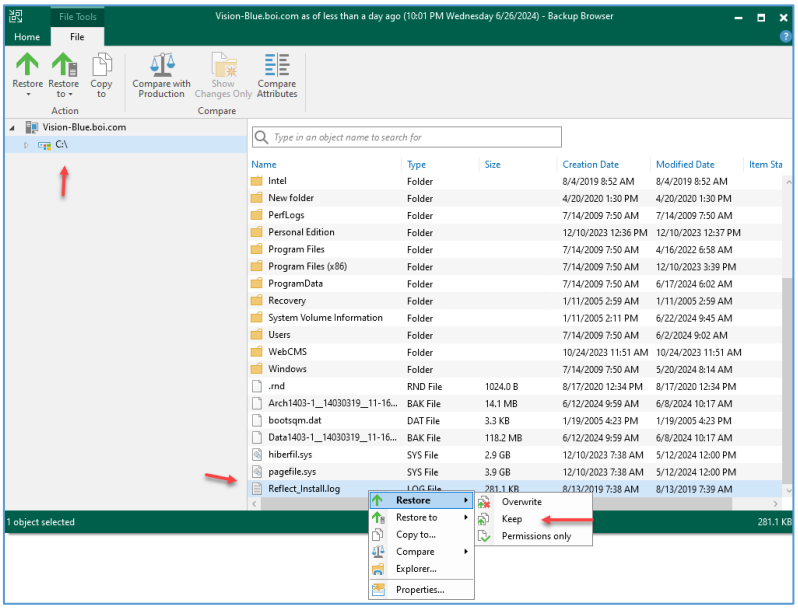


شکل ۱۳- ۷۰ بررسی اطلاعات ماشین مجازی

همان‌طور که در شکل ۱۳-۷۱، مشاهده می‌کنید اطلاعات ماشین مورد نظر نمایش داده شده و هر فایلی را که بخواهید می‌توانید Restore کنید، اگر به مانند شکل بر روی File مورد نظر کلیک راست کنید در قسمت Restore سه گزینه را مشاهده می‌کنید که گزینه‌ی Overwrite دقیقاً فایل را بر روی فایل اصلی کپی می‌کند،

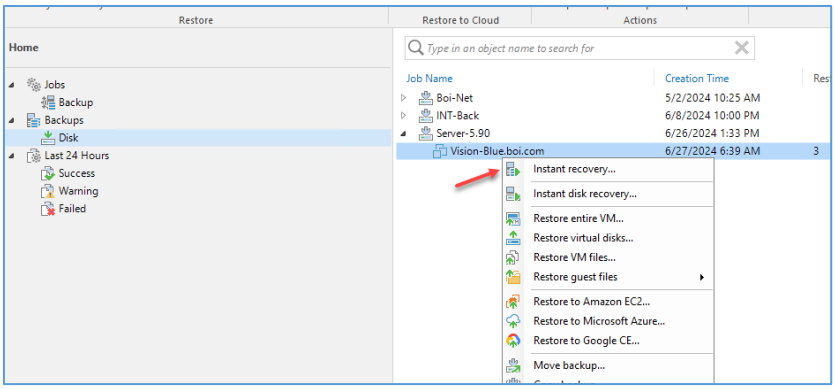
www.takbook.com

گزینه‌ی Keep فایل قبلی را نگه می‌دارد و یک فایل جدید با نام جدید ایجاد می‌کند، گزینه‌ی Permissions only هم فقط مجوزهای فایل مورد نظر را برمی‌گرداند.



شکل ۱۳- ۷۱ بررسی اطلاعات ماشین مجازی

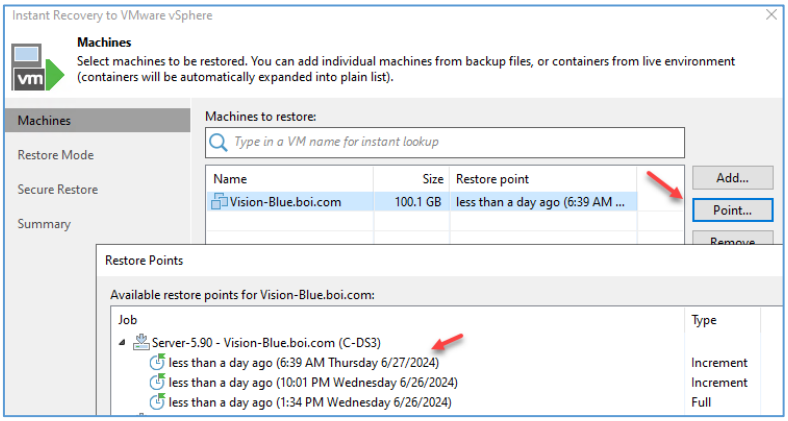
در روش قبلی توانستیم فایل‌های خاصی را از درون ماشین مجازی Restore کنیم، حالا می‌خواهیم کل ماشین مجازی را به روش‌های مختلف Restore کنیم، برای این کار به مانند شکل ۱۳-۷۲، در قسمت Disk بر روی ماشین مجازی مورد نظر کلیک راست کنید، گزینه‌های مختلفی را مشاهده می‌کنید، می‌توانید کل ماشین را برگردانید به همان جای قبلی و یا اینکه در جای جدید قرار دهید، و یا اینکه دیسک‌های ماشین مجازی را برگردانید و ... برای شروع بر روی Instant recovery کلیک کنید.



شکل ۱۳- ۷۲ بررسی Instant recovery

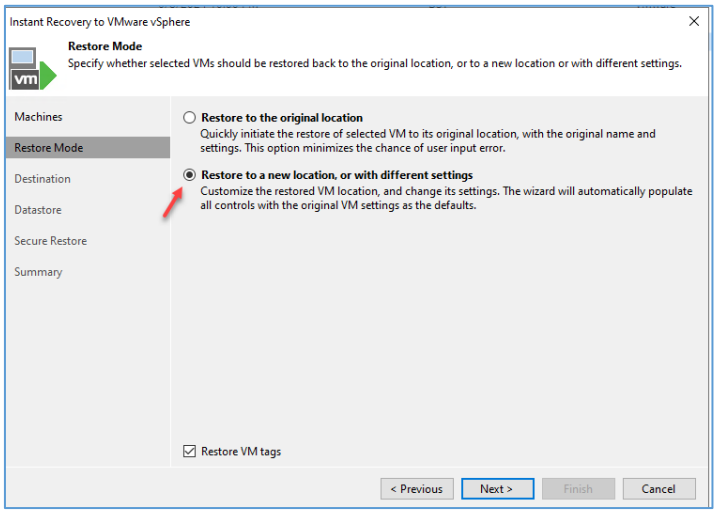
www.takbook.com

در شکل ۱۳-۷۳، می‌توانید با کلیک بر روی Point زمان و تاریخ مورد نظر Backup خود را انتخاب کنید، تا همان تاریخ Restore شود.



شکل ۱۳- ۷۳ بررسی *Instant recovery*

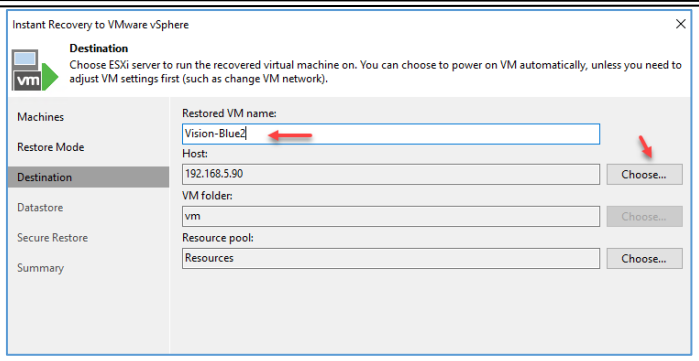
در شکل ۱۳-۷۴، دو گزینه وجود دارد که اگر گزینه‌ی اول را انتخاب کنید ماشین مورد نظر در همان مسیر و سرور کپی خواهد شد و دقیقاً جای ماشین قبلی را پر می‌کند، اگر بخواهیم در یک سرور جدید و با نام جدید Restore کنیم باید گزینه‌ی دوم را انتخاب می‌کنیم.



شکل ۱۳- ۷۴ بررسی *Instant recovery*

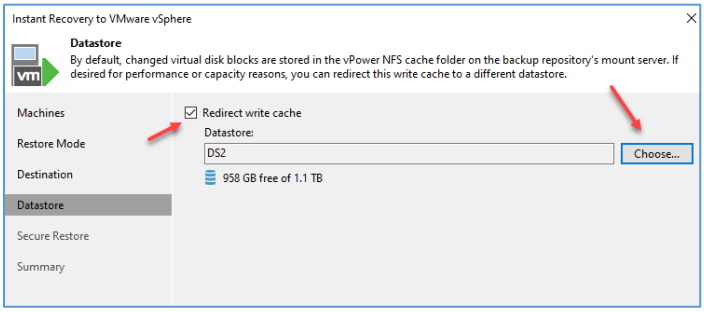
در شکل ۱۳-۷۵، باید نام جدید برای ماشین خود در نظر بگیرید و با کلیک بر روی Choose از قسمت Host می‌توانید سرور مورد نظر را تغییر دهید، که در این قسمت همان سرور قبلی انتخاب شده است.

www.takbook.com



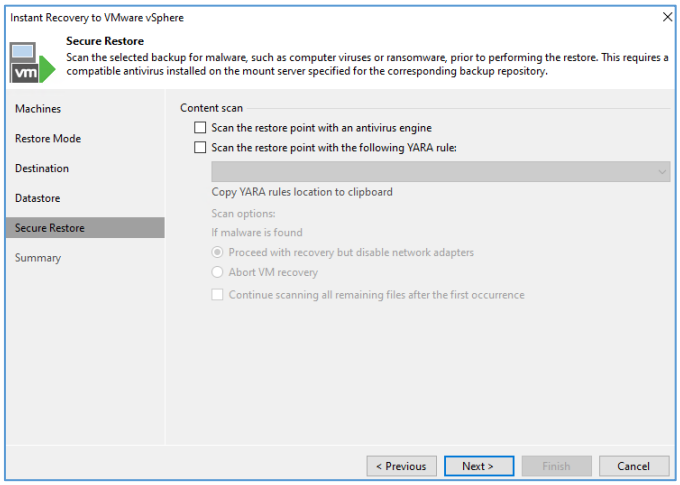
شکل ۱۳ - ۷۵ بررسی *Instant recovery*

در شکل ۱۳–۷٦، می‌توانید Datastore مربوط به ماشین مورد نظر را بر روی سرور تغییر دهید تا ماشین مورد نظر در هارد جدید کپی شود.



شکل ۱۳ - ۷۶ بررسی *Instant recovery*

در شکل ۱۳–۷۷، بر روی Next کلیک کنید.



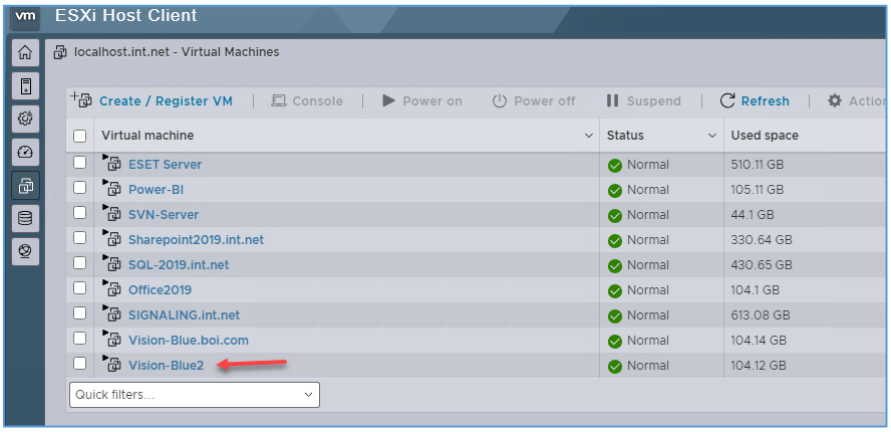
شکل ۱۳ - ۷۷ بررسی *Instant recovery*

www.takbook.com

در صفحه‌ی آخر هم اگر می‌خواهید ماشین مورد نظر بعد از Restore روشن شود و به کارت شبکه متصل شود باید هر دو تیک را انتخاب کنید.

نکته: زمانی که یک ماشین مجازی روشن است و در حال کار است، اگر ماشین مجازی دیگری را به مانند قسمت قبل Restore کنید و بعد روشن و به شبکه متصل کنید ارتباط یکی از ماشین‌ها با دومین بر هم خواهد خورد و Trust بین آنها از بین می‌رود.

بعد از اینکه Restore انجام شد، سری به سرور ESXi می‌زنیم و همان‌طور که در شکل ۱۳-۷۸، مشاهده می‌کنید ماشین مورد نظر با نام Vision-Blue2 فعال شده است و در دسترس است.



شکل ۱۳- ۷۸ بررسی سرور ESXi

۱۳-۳ استفاده از Veeam Agent

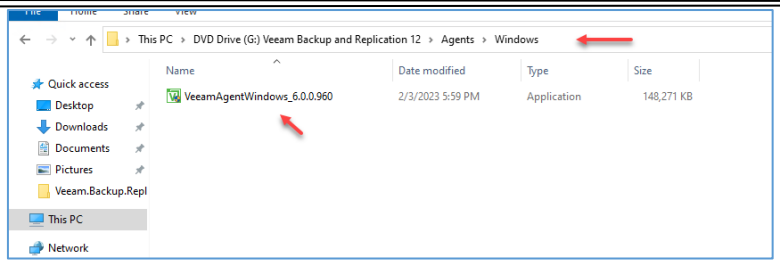
یکی از ابزارهای فوق‌العادهٔ نرم‌افزار Veeam، استفاده از سرویس Agent است که به شما این امکان را می‌دهد که از تمام سیستم‌های کلاینت، یک پشتیبان تهیّه کنید، یعنی اینکه با نصب این نرم‌افزار از سیستم‌های کاربران با تنظیمی که بر روی آنها انجام می‌دهید، پشتیبان تهیّه خواهد شد و با از دست دادن اطّلاعات کاربری، مشکلی برای برگشت نخواهید داشت، یعنی یک شبکهٔ کاملاً قابل اعتماد.

برای دانلود Veeam Agent به لینک زیر مراجعه کنید:

https://www.veeam.com/windows-cloud-server-backup-agent.html

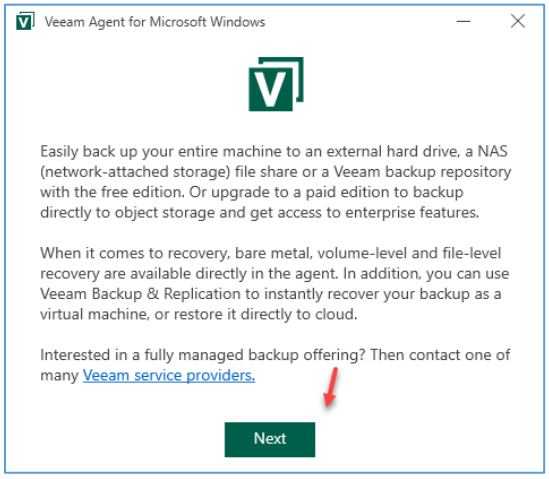
توجه داشته باشید از طریق DVD مربوط به فایل نصب Veeam Backup می‌توانید فایل Agent را اجرا کنید که در شکل ۱۳-۷۹، فایل را در آدرس مشخص شده مشاهده می‌کنید:

www.takbook.com



شکل ۱۳- ۷۹ نصب و راه‌اندازی *Agent*

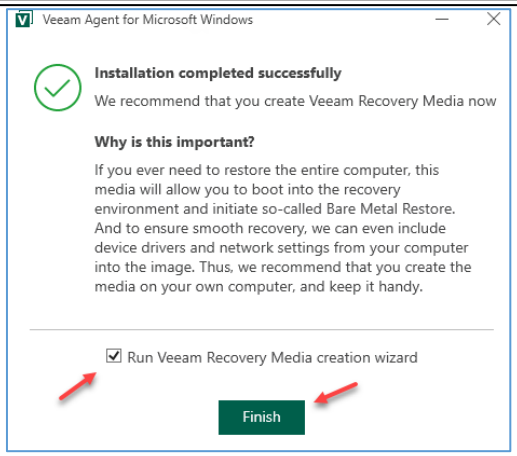
بعد از دانلود نرم‌افزار، آن را اجرا کنید و به مانند شکل ۱۳-۸۰، بر روی Next و در قسمت بعد بر روی I accept کلیک کنید تا نصب نرم‌افزار انجام شود.



شکل ۱۳- ۸۰ نصب و راه‌اندازی *Agent*

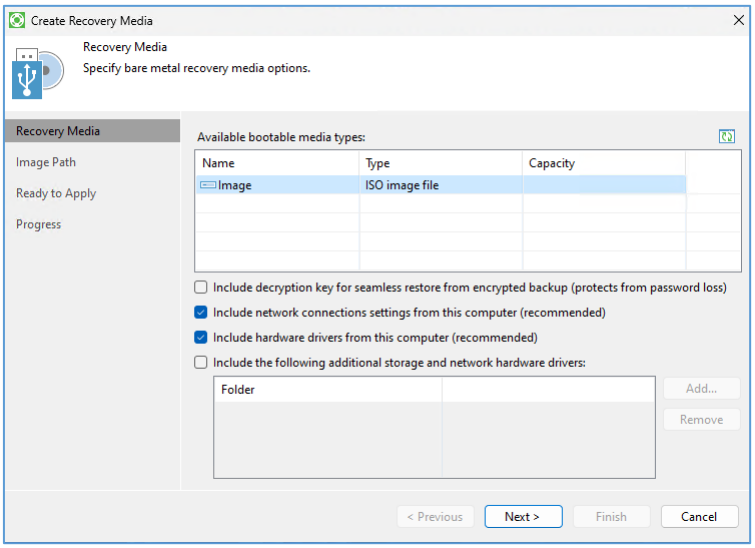
بعد از نصب به مانند شکل ۱۳-۸۱، تیک گزینه‌ی مورد نظر را انتخاب و بر روی Finish کلیک کنید.

www.takbook.com



شکل ۱۳- ۸۱ نصب و راه‌اندازی *Agent*

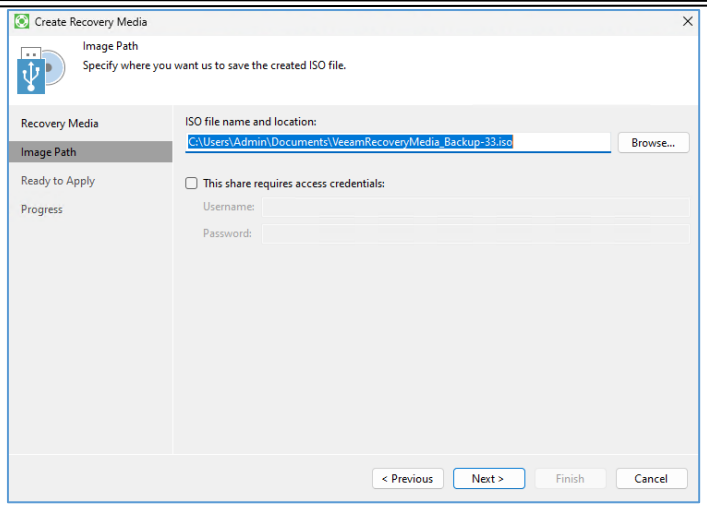
اولین صفحه‌ای که بعد از نصب برای شما ظاهر می‌شود شکل ۱۳-۸۲، است که این قسمت برای ایجاد یک فایل Image برای Recovery این سیستم است که بر روی Next کلیک کنید.



شکل ۱۳- ۸۲ نصب و راه‌اندازی *Agent*

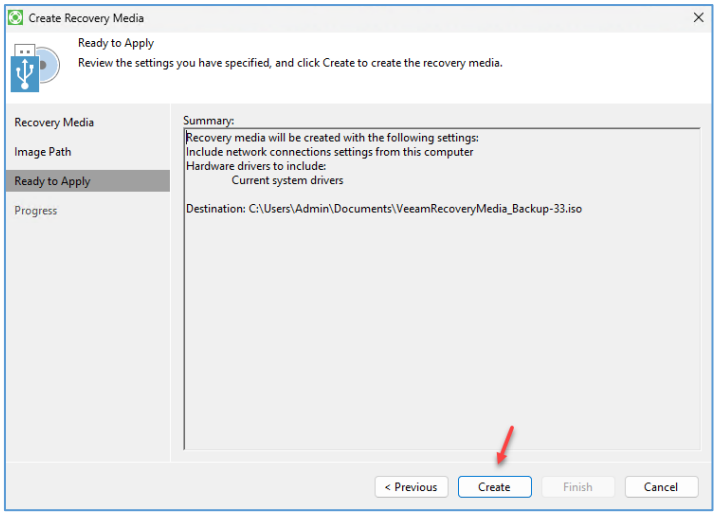
در شکل ۱۳-۸۳، می‌توانید مسیر مورد نظر را برای ذخیره شدن فایل Image انتخاب کنید.

www.takbook.com



شکل ۱۳ - ۸۳ نصب و راه‌اندازی *Agent*

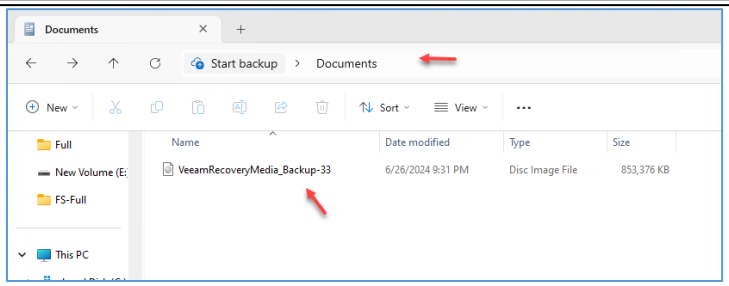
در شکل ۱۳-۸۴، بر روی Create کلیک کنید تا فایل مورد نظر ایجاد شود.



شکل ۱۳ - ۸۴ نصب و راه‌اندازی *Agent*

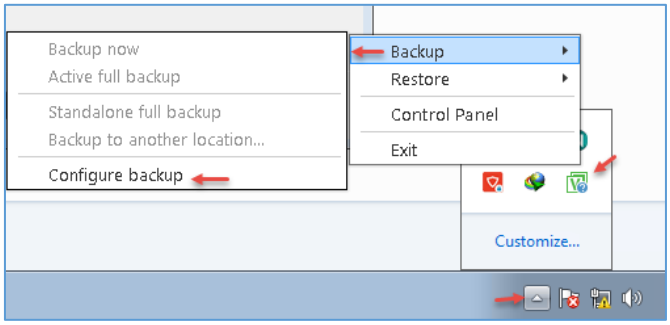
همان‌طور که در شکل ۱۳-۸۵، مشاهده می‌کنید فایل مورد نظر با حجم تقریبی ۸۰۰ مگابایت ایجاد شده و هر موقع ویندوز شما با مشکل روبرو شد می‌توانید از طریق Boot آن را Recovery کنید.

www.takbook.com



شکل ۱۳- ۸۵ پشتیبان گیری از ویندوز

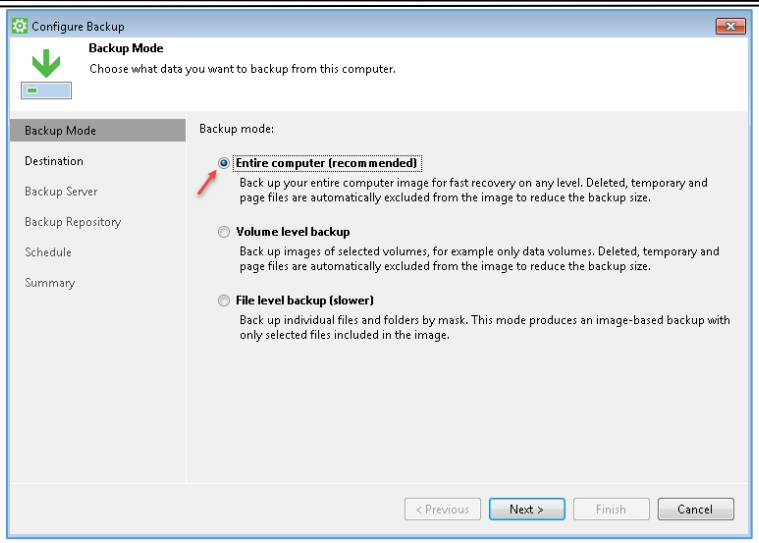
برای اینکه Agent را روی سیستم کاربر تنظیم کنیم به مانند شکل ۱۳-۸۶، در Taskbar بر روی آیکون آن کلیک راست کنید و از قسمت Backup، گزینهٔ Configure Backup را انتخاب کنید.



شکل ۱۳- ۸۶ نصب و راه‌اندازی Agent

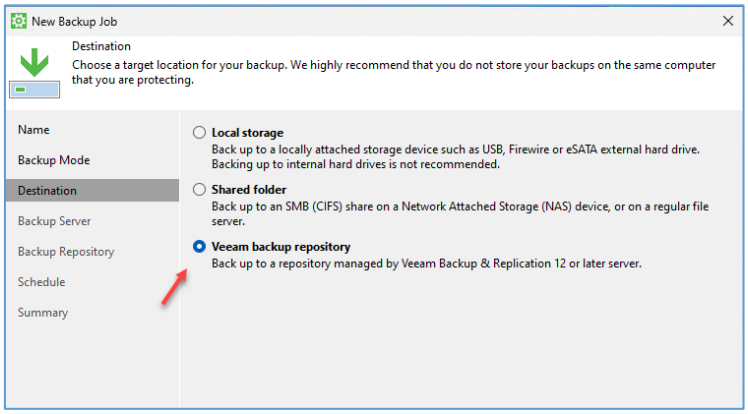
در شکل ۱۳-۸۷، سه گزینه را مشاهده می‌کنید که اگر گزینهٔ اوّل انتخاب شود، از کلّ اطّلاعات سیستم، پشتیبان تهیّه خواهد کرد، یعنی از همهٔ پارتیشن‌های موجود؛ در گزینهٔ دوّم می‌توانید پارتیشن مورد نظر خود را به صورت دستی انتخاب کنید و در قسمت آخر نیز می‌توانید فایل‌های مشخّص خود را در پارتیشن انتخاب کنید؛ در حال حاضر، گزینهٔ اوّل را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۳- ۸۷ نصب و راه‌اندازی *Agent*

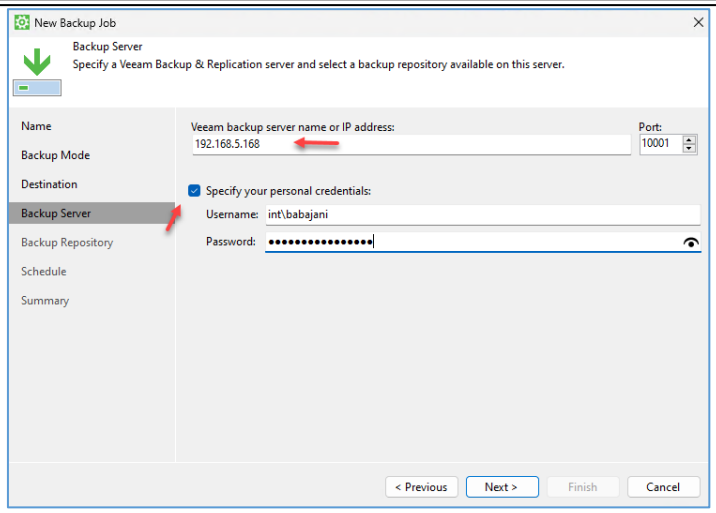
در شکل ۱۳-۸۸، باید مسیر ذخیره‌سازی را انتخاب کنید که این محل می‌تواند بر روی هارد دیسک خود سیستم باشد، یا بر روی شبکه یا بر روی مایکروسافت ondrive که البتّه در اینجا می‌خواهیم از گزینهٔ سوّم، یعنی backup Repository Veeam که قبلاً با هم ایجاد کردیم، استفاده کنیم.



شکل ۱۳- ۸۸ نصب و راه‌اندازی *Agent*

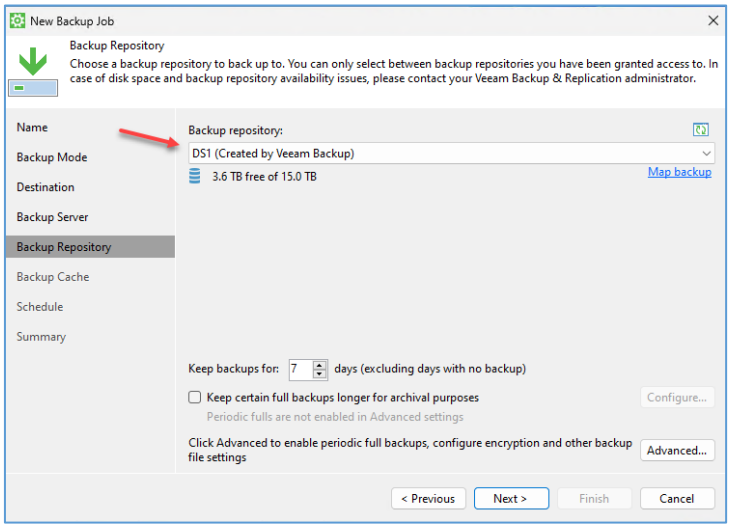
در شکل ۱۳-۸۹، باید آدرس سروری که بر روی آن، نرم‌افزار Backup & Repository را نصب کردید را وارد کنید و یک نام کاربری با دسترسی کامل را وارد کنید، اگر در موقع نصب نرم‌افزار، پورت آن را تغییر دادید، باید در این قسمت نیز تغییر دهید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۳- ۸۹ نصب و راه‌اندازی Agent

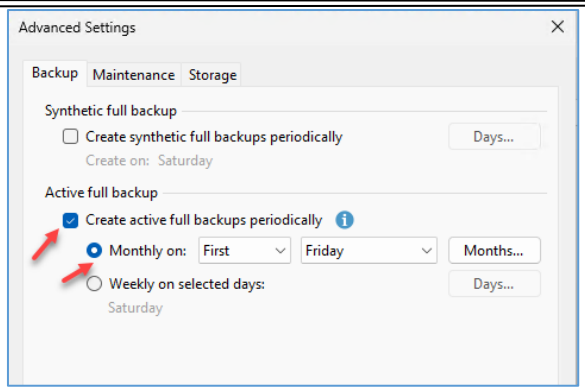
در شکل ۱۳-۹۰، باید Repository مورد نظر خود را انتخاب کنید، در قسمت پایین، مدّت‌زمان نگهداری از فایل پشتیبان را که به صورت پیش‌فرض، ۷ روز است را می‌توانید تغییر دهید، بر روی Advcanced کلیک کنید.



شکل ۱۳- ۹۰ نصب و راه‌اندازی Agent

به مانند شکل ۱۳-۹۱، در تب Backup می‌توانید تعداد دفعات گرفتن Backup Full را در طول ماه یا در طول هفته مشخّص کنید که در این قسمت باید تیک گزینه‌ی مورد نظر را فعّال کنید.

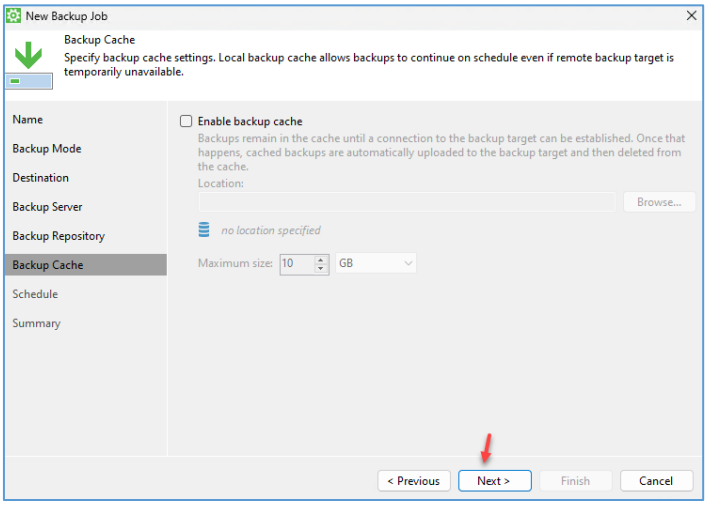
www.takbook.com



شکل ۱۳- ۹۱ نصب و راه‌اندازی *Agent*

در تب Storage می‌توانید حالت فشرده‌سازی و سرعت ذخیره‌سازی آن را مشخّص کنید و بر روی آن، رمز عبور قرار دهید که البتّه قبلاً این مورد را انجام دادیم.

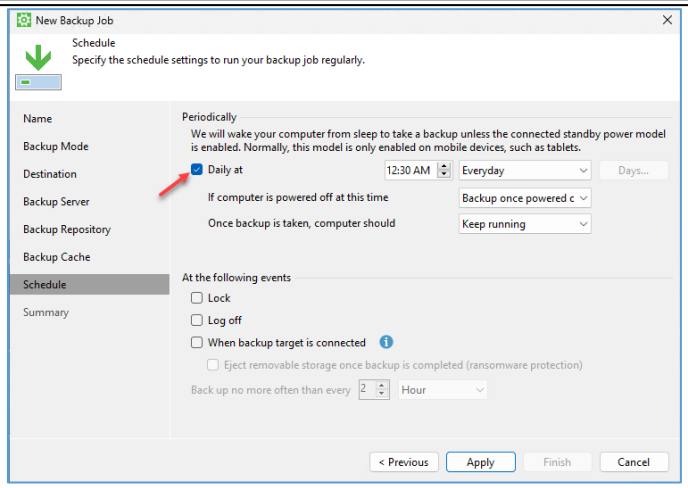
در شکل ۱۳-۹۲، نیاز به تغییری نیست و فقط بر روی Next کلیک کنید.



شکل ۱۳- ۹۲ نصب و راه‌اندازی *Agent*

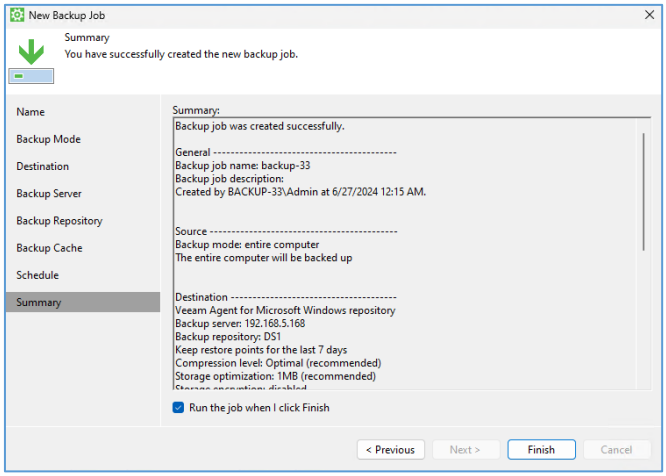
در شکل ۱۳-۹۳، می‌توانید مشخص کنید که چه زمانی کار Backup گیری به صورت اتوماتیک انجام شود، بر روی Apply کلیک کنید.

www.takbook.com



شکل ۱۳ - ۹۳ نصب و راه‌اندازی *Agent*

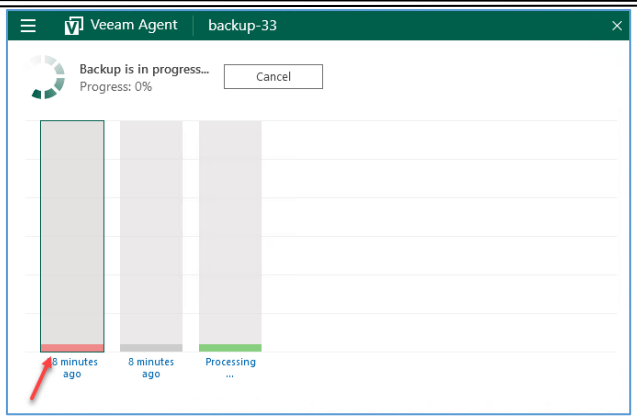
در شکل ۱۳-۹٤، تیک مورد نظر را انتخاب کنید و بر روی Finish کلیک کنید تا کار پشتیبانگیری آغاز شود.



شکل ۱۳ - ۹۴ نصب و راه‌اندازی *Agent*

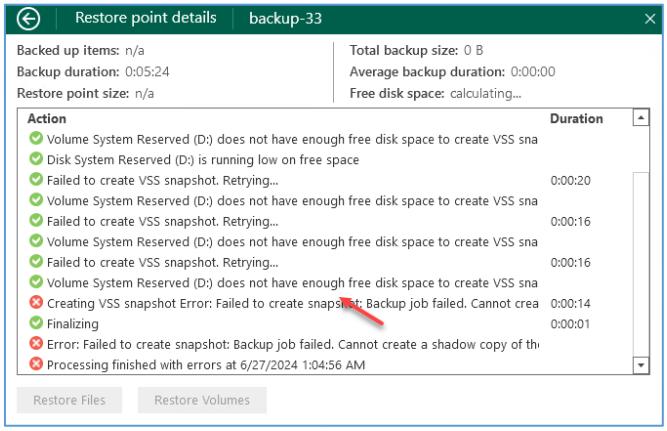
همان‌طور که در شکل ۱۳-۹۵، مشاهده می‌کنید نرم افزار با خطا روبرو شده، و برای حل مشکل باید خطا را بررسی کنید، برای این کار بر روی قسمتی که خطا داده کلیک کنید، توجه داشته باشید شاید برای سیستم شما خطایی رخ ندهد.

www.takbook.com



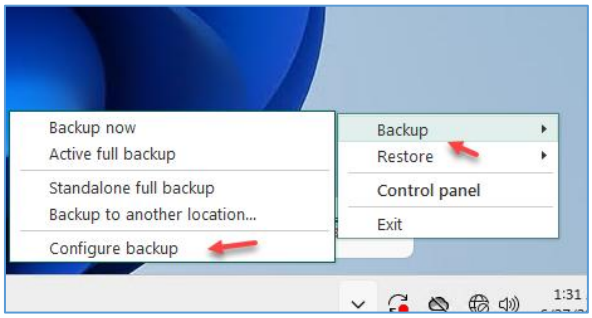
شکل ۱۳- ۹۵ نصب و راه‌اندازی Agent

در شکل ۱۳–۹٦، مشخص شده است که درایو D فضای کافی برای ایجاد Snapshot ندارد و باید این مورد را در Config اصلاح کنیم.



شکل ۱۳- ۹۶ نصب و راه‌اندازی Agent

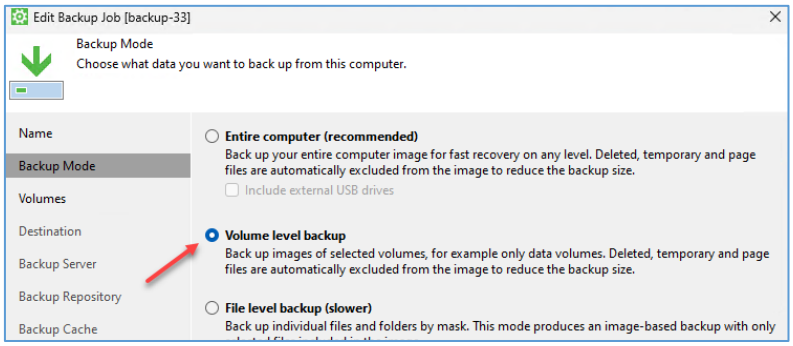
به مانند شکل ۱۳–۹۷، دوباره وارد Configure backup شوید.



شکل ۱۳- ۹۷ نصب و راه‌اندازی Agent

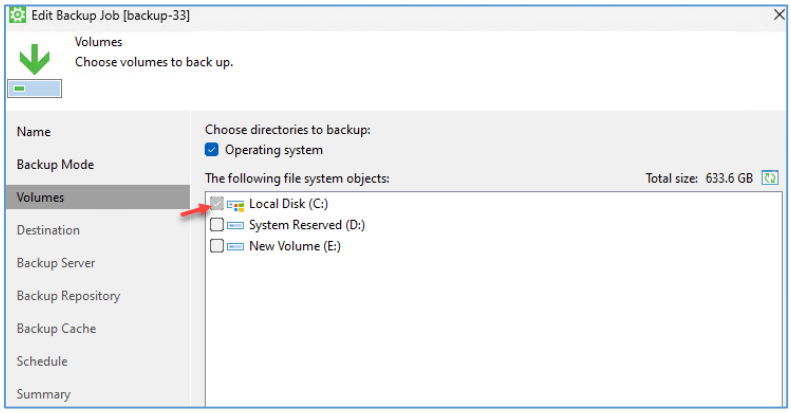
www.takbook.com

در شکل ۱۳-۹۸، گزینه‌ی Volume level backup را انتخاب کنید.



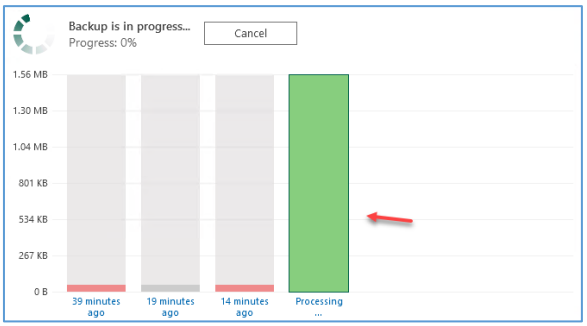
شکل ۱۳- ۹۸ نصب و راه‌اندازی *Agent*

در شکل ۱۳-۹۹، می‌توانید درایو مشخص شده‌ی خود را انتخاب کنید و یا اگر می‌خواهید از سیستم‌عامل شخص مورد نظر پشتیبان تهیه کنید باید تیک گزینه‌ی Operation system را انتخاب کنید.



شکل ۱۳- ۹۹ نصب و راه‌اندازی *Agent*

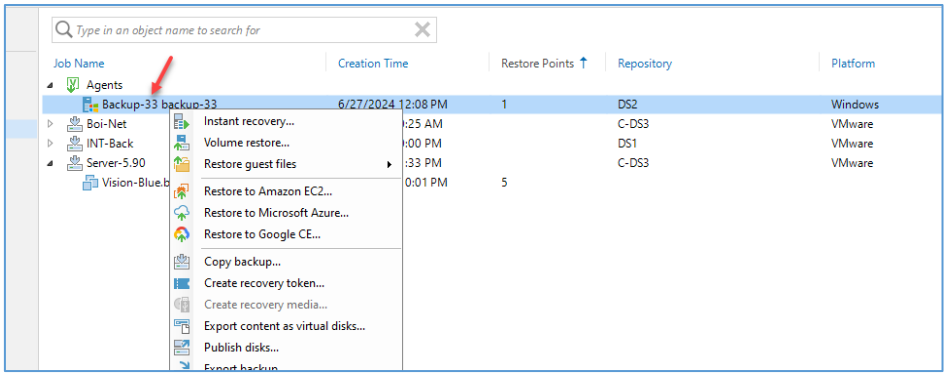
در دیگر صفحات هم تنظیمات به صورت قبل می‌باشد Next کنید و در صفحه‌ی آخر بر روی Finish کلیک کنید، تا عملیات به مانند شکل ۱۳-۱۰۰، انجام شود.



شکل ۱۳- ۱۰۰ نصب و راه‌اندازی *Agent*

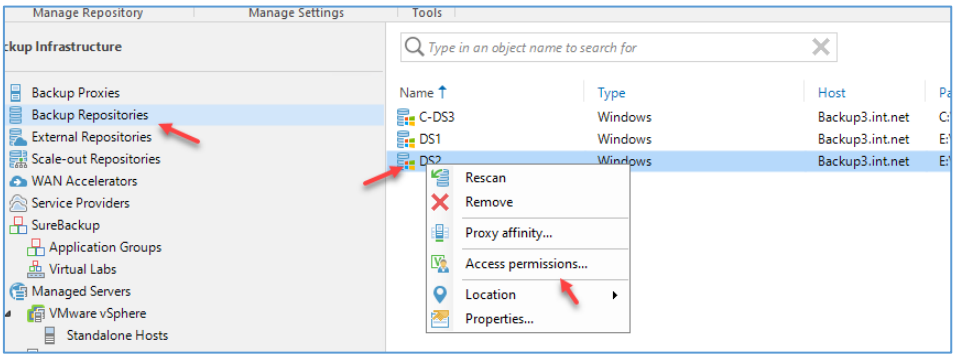
www.takbook.com

بعد از اینکه Backup انجام شود باید به مانند شکل ۱۳-۱۰۱، وارد Veeam Backup شوید و در قسمت Home وارد Disk شوید و گزینه‌ی Agent را انتخاب کنید و سیستمی که از آن پشتیبان تهیه کردید را مشاهده کنید، بر روی آن می‌توانید کلیک راست کنید و عملیات مشخص شده‌ی خود را انجام دهید.



شکل ۱۳- ۱۰۱ بررسی فایل Agent

یک نکته‌ی مهم این است که زمانی‌که به Repository متّصل می‌شوید باید یک دسترسی به آن منبع را برای این کاربر یا کاربرانی که در حال متّصل‌شدن به آن هستند، مشخص کنید؛ برای این کار وارد سرور Veeam شوید و در این صفحه از سمت چپ بر روی Backup Infrastructure کلیک کنید و در قسمت Repository، گزینه‌ی مورد نظر خود را که از قبل ایجاد کردید را انتخاب کنید و بر روی آن کلیک راست و گزینه‌ی Access Permissions را انتخاب کنید.

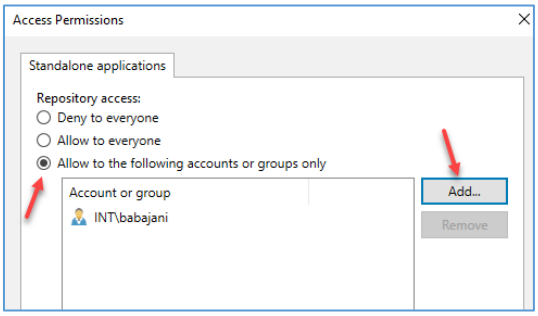


شکل ۱۳- ۱۰۲ بررسی فایل Agent

در شکل ۱۳-۱۰۳، باید دسترسی لازم را به کاربر مورد نظر دهید، البتّه می‌توانید گزینه‌ی Allow to everyone را انتخاب کنید که با فعّال‌کردن آن، همه می‌توانند به آن دسترسی داشته باشند که از نظر امنیّتی کار جالبی نیست، بهتر است گزینه‌ی سوّم را به مانند شکل انتخاب کنید و بر روی Add کلیک کنید و کاربر

www.takbook.com

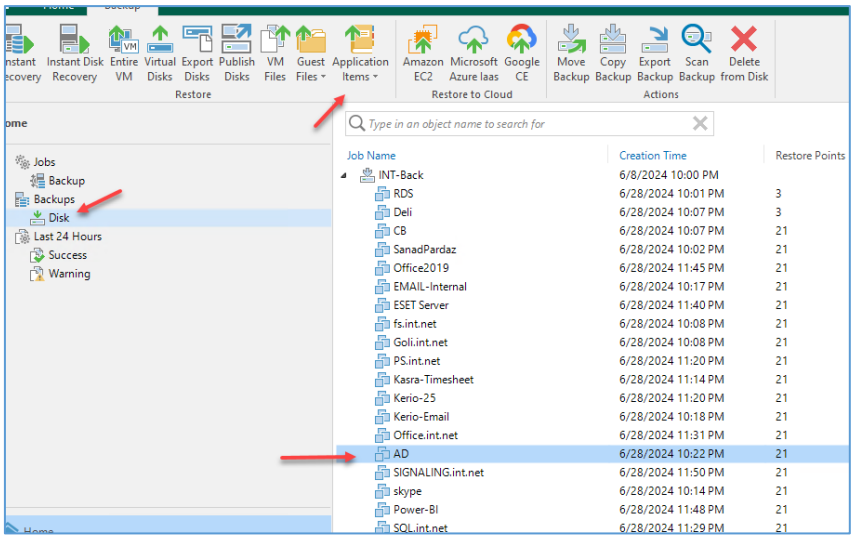
مورد نظر را به لیست اضافه کنید، در قسمت پایین صفحه می‌توانید بر روی فایل‌هایی که در این Repository قرار می‌گیرند، رمز قرار دهید.



شکل ۱۳- ۱۰۳ بررسی فایل Agent

۱۳-٤ کار با Application Item

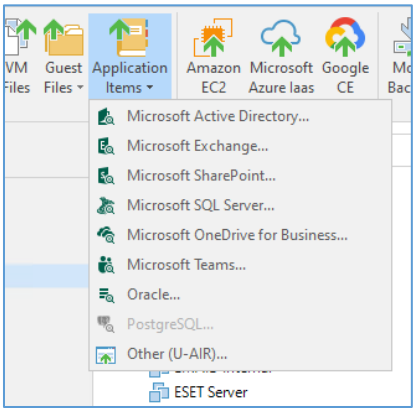
به مانند شکل ۱۳-۱۰٤، اگر بر روی ماشین مجازی مورد نظر خود که پشتیبان از آن تهیه کردیم کلیک کنید، یک‌سری ابزار در بالای صفحه برای شما نمایش داده خواهد شد که اگر بر روی Application Items کلیک کنید، چند گزینه را مشاهده می‌کنید، از آنجایی که سروری که ما از آن پشتیبان گرفتیم سرور Active Directory بود، می‌توانیم سرویس Microsoft Active Directory را انتخاب کنیم، این نوع سرویس‌ها یک‌سری ویژگی‌هایی به مدیران شبکه می‌دهند، مثلاً می‌توانیم یک کاربر که از Active Direcory حذف شده است را بازگردانیم.



شکل ۱۳- ۱۰۴ کار با Application Item

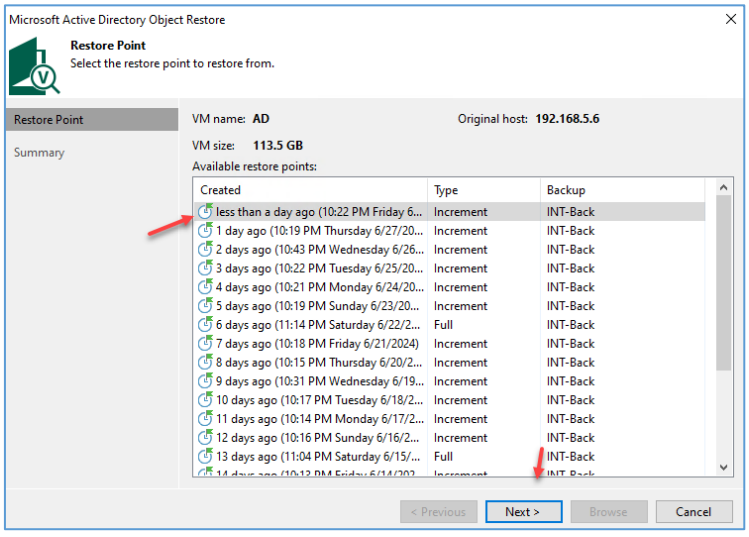
www.takbook.com

در شکل ۱۳-۱۰۵، ابزارهای مختلف از شرکت‌های مختلف را مشاهده می‌کنید که برای تست این موضوع روی ماشین Active Directory کلیک راست کردیم و گزینه‌ی Microsoft Active Directory را انتخاب می‌کنیم.



شکل ۱۳- ۱۰۵ کار با *Application Item*

در شکل ۱۳-۱۰۶، باید یکی از تاریخ های پشتیبان گرفته شده را انتخاب کنید.

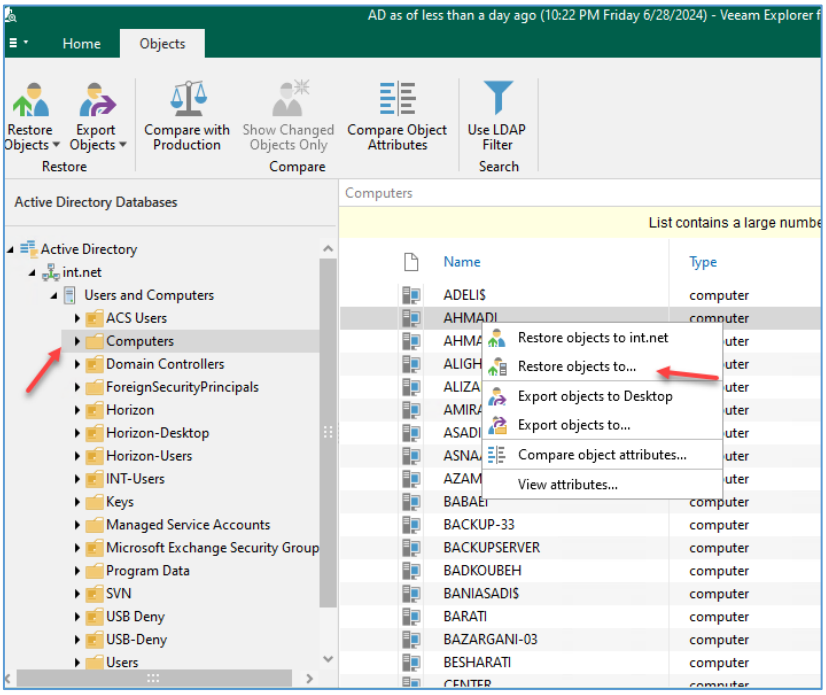


شکل ۱۳- ۱۰۶ کار با *Application Item*

همان‌طور که مشاهده می‌کنید در شکل ۱۳-۱۰۷، اطّلاعات سرور Active Directory شبکه‌ی ما به نمایش گذاشته شده است و قسمت جالب این موضوع این است که اگر کاربر، گروه، واحد سازمانی، کامپیوتر خاص و... از سرور حذف شود، شما می‌توانید به راحتی به مانند شکل بر روی مثلاً کامپیوتر مورد نظر کلیک راست کنید و دو گزینه‌ی اوّل را انتخاب کنید که گزینه‌ی یک برای برگرداندن کامپیوتر مورد نظر به

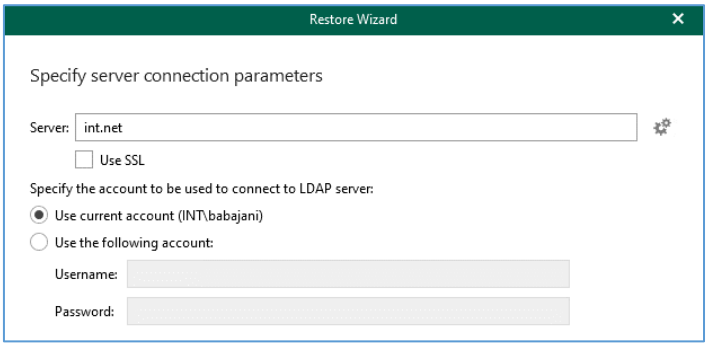
www.takbook.com

سیستمی که از آن پشتیبان تهیّه کردیم و گزینه‌ی شماره‌ی دو برای برگرداندن به سرور دیگر است، برای تست این موضوع، گزینه‌ی دوّم را انتخاب کنید.



شکل ۱۳-۱۰۷ بررسی *Active directory*

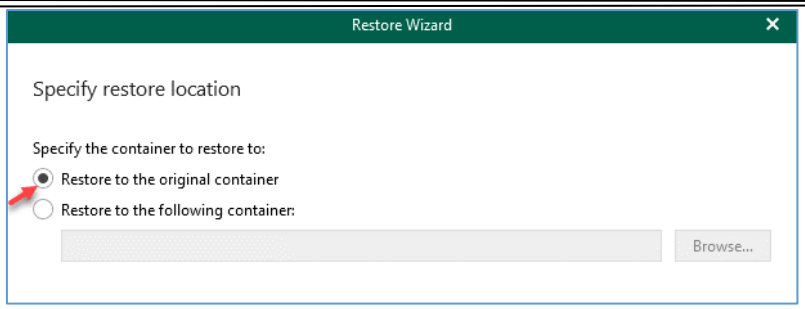
همان‌طور که در شکل ۱۳-۱۰۸، مشاهده می‌کنید، سرور مورد نظر انتخاب شد و در قسمت پایین آن می‌توانید کاربر ادمین خود را وارد کنید و یا از کاربری که با آن در حال کار هستید، استفاده کنید.



شکل ۱۳-۱۰۸ بررسی *Active directory*

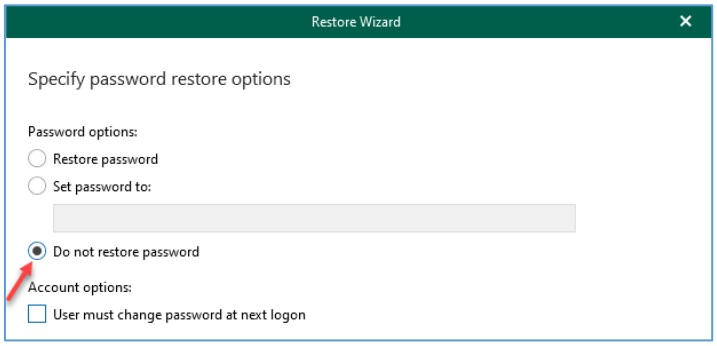
در شکل ۱۳-۱۰۹، می‌توانید مسیر Restore فایل را تغییر دهید، یا اینکه بر روی همان آدرس اصلی‌اش که گزینه‌ی اوّل است، قرار دهید.

www.takbook.com



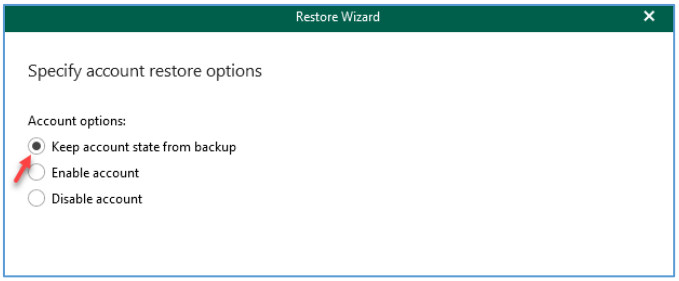
شکل ۱۳- ۱۰۹ بررسی *Active directory*

در شکل ۱۳-۱۱۰، اگر در حال Restore کردن یک کاربر بودید، می‌توانستید رمز عبور آن را تغییر دهید و یا رمز عبور قبلی آن را دوباره بازگردانید، امّا چون شی ما از نوع کامپیوتر است باید گزینه‌ی Do not… را انتخاب کنید.



شکل ۱۳- ۱۱۰ بررسی *Active directory*

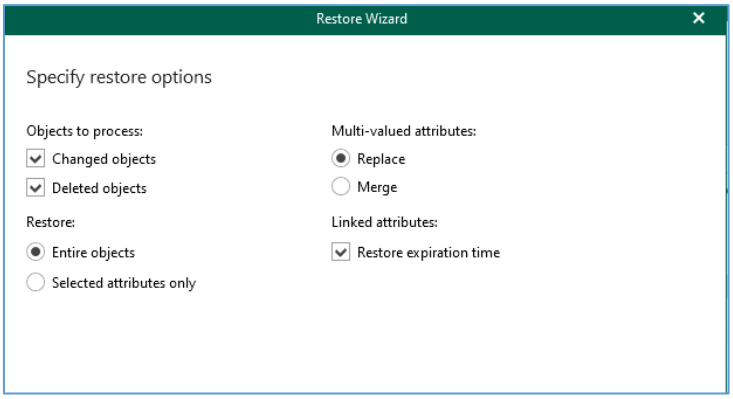
در شکل ۱۳-۱۱۱، می‌توانید اکانت مورد نظر را فعّال، غیر فعّال و در همان حالت پشتیبانی که گرفته شده است، قرار دهید.



شکل ۱۳- ۱۱۱ بررسی *Active directory*

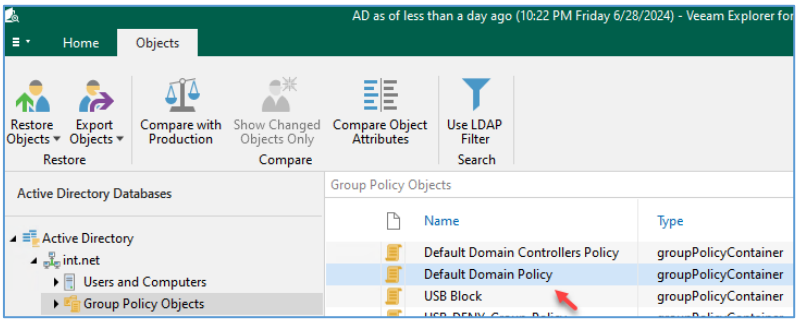
www.takbook.com

در شکل ۱۳-۱۱۲، می‌توانید تنظیمات بیشتری را بر روی اکانت اعمال کنید؛ بر روی Restore کلیک کنید، با این کار اکانت مورد نظر در سرور Restore خواهد شد و دیگر نیازی به Restore کردن کلّ سرور در جایگاه قبلی نیست، یعنی با این کار در زمان، بسیار صرفه‌جویی خواهد شد.



شکل ۱۳-۱۱۲ بررسی *Active directory*

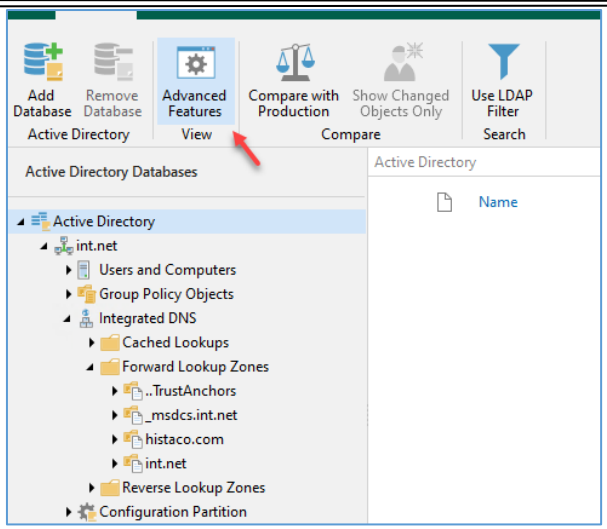
به صورت شکل ۱۳-۱۱۳، می‌توانید به راحتی تنظیمات Policy خود را به سرور بازگردانید که این می‌تواند یکی از ویژگی‌های خوب این نرم‌افزار باشد.



شکل ۱۳-۱۱۳ بررسی *Default Policy*

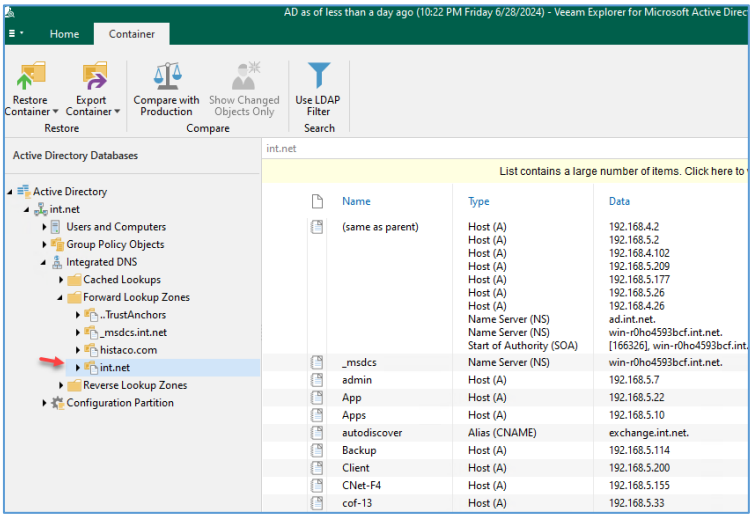
برای اینکه به سرویس‌های بیشتری دست پیدا کنید به مانند شکل ۱۳-۱۱٤، باید نام Active Direcory را انتخاب کنید و بعد در ابزار بالایی بر روی Advanced Features کلیک کنید.

www.takbook.com



شکل ۱۳- ۱۱۴ فعال‌سازی *Advanced Features*

به مانند شکل ۱۳-۱۱۵، بعد از کلیک بر روی Features Advanced، سرویس DNS نیز به گزینه‌ها اضافه می‌شود که به راحتی می‌توانید هر نوع تغییری که در سرور ایجاد شده است را به حالت اوّل بازگردانید که گزینه‌ی بسیار خوبی برای مدیر شبکه است.



شکل ۱۳- ۱۱۵ فعال‌سازی *Advanced Features*

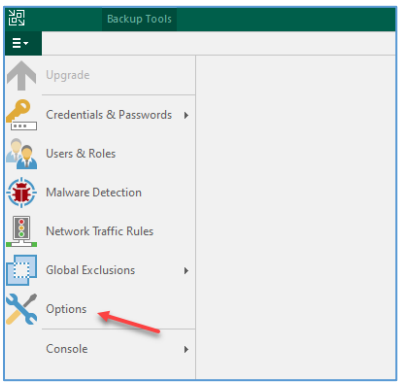
در کل، نرم‌افزار Veeam، سرورهای SharePoint, SQL, Exchange, Active Directory و... را در زیرمجموعه‌ی خود دارد.

www.takbook.com

۱۳-۵ فعال‌سازی ایمیل در Veeam Backup

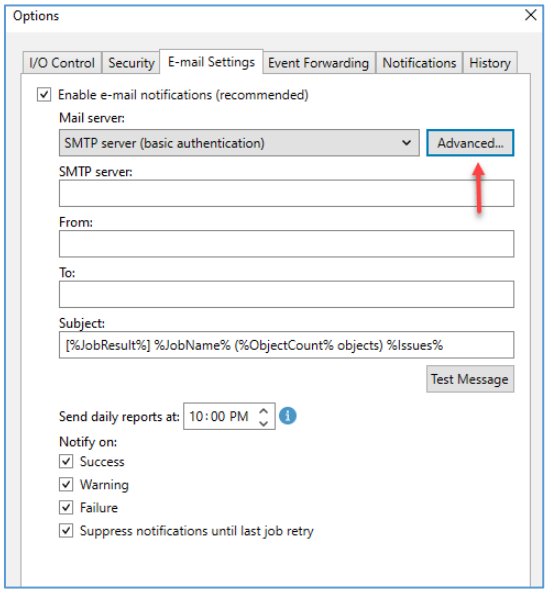
برای اینکه متوجه شوید که یک JOB به درستی اجرا شده است و Backup انجام شده است یا خیر باید تنظیمات ایمیل را در نرم‌افزار انجام دهید تا در هر بار که JOB اجرا می‌شود نتیجه‌ی آن به ایمیل مدیر شبکه ارسال شود.

به مانند شکل ۱۳-۱۱۶، بر روی آیکون مورد نظر کلیک کنید و در منوی باز شده بر روی Options کلیک کنید.



شکل ۱۳- ۱۱۶ فعال‌سازی ایمیل در Veeam Backup

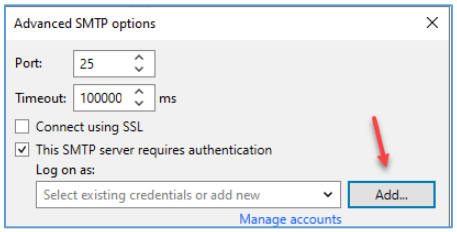
در شکل ۱۳-۱۱۷، وارد تب E-mail Settings شوید و برای اینکه Account ایمیل خود را وارد کنید، بر روی Advanced کلیک کنید.



شکل ۱۳- ۱۱۷ فعال‌سازی ایمیل در Veeam Backup

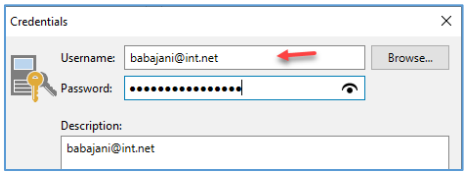
www.takbook.com

در شکل ۱۳–۱۱۸، بر روی Add کلیک کنید و اکانت خود را وارد کنید، توجه داشته باشید که اگر ایمیل شما از SSL و TLS پشتیبانی می‌کند باید تیک گزینه‌ی Connect using SSL را انتخاب کنید.



شکل ۱۳- ۱۱۸ فعال‌سازی ایمیل در Veeam Backup

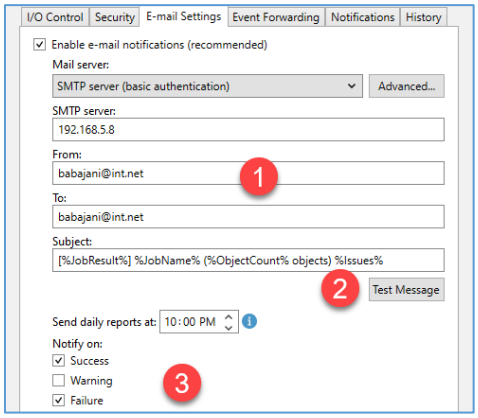
در شکل ۱۳–۱۱۹، اطلاعات Account را وارد می‌کنیم.



شکل ۱۳- ۱۱۹ فعال‌سازی ایمیل در Veeam Backup

در شکل ۱۳–۱۲۰، در قسمت اول باید آدرس ایمیل خود را وارد کنید، در قسمت SMTP Server باید آدرس سرور ایمیل خود را وارد کنید که می‌تواند داخلی و خارجی باشد، در قسمت From باید آدرسی را وارد کنید که می‌خواهد ایمیل را ارسال کند و در قسمت To، دریافت کننده ایمیل را وارد کنید.

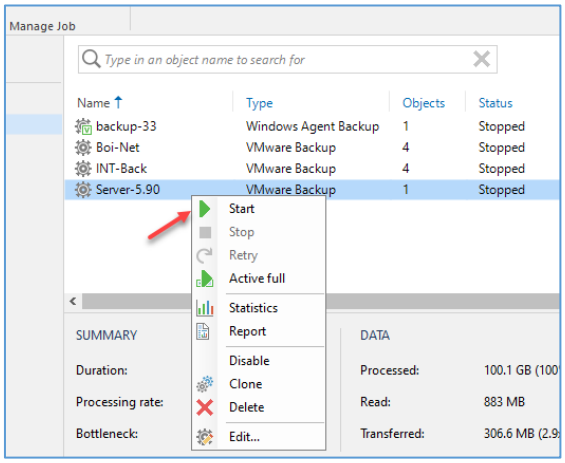
در قسمت شماره‌ی 2 بر روی Test Message کلیک کنید تا یک ایمیل تستی ارسال شود تا متوجه شویم که تنظیمات ایمیل را به درستی انجام دادیم، در قسمت شماره‌ی 3 باید مشخص کنیم چه ایمیلی به کاربر مورد نظر ارسال شود، در قسمت شماهری سه انتخاب کردیم که ایمیل‌هایی که برای انجام موفقیت آمیز و ایمیل‌هایی که برای عملیات ناتمام است برای کاربر مورد نظر ارسال شود.



شکل ۱۳- ۱۲۰ فعال‌سازی ایمیل در Veeam Backup

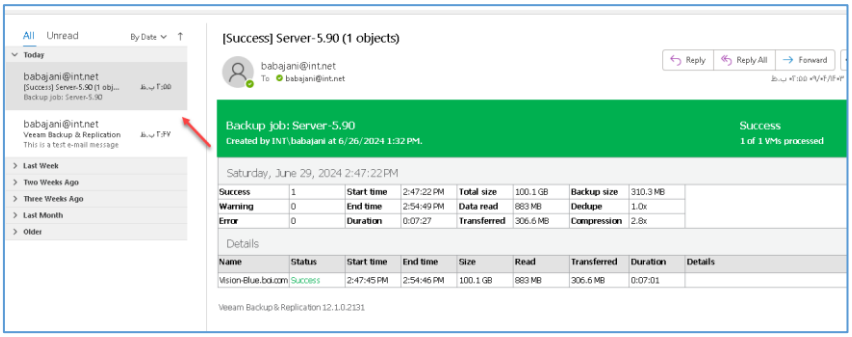
www.takbook.com

به مانند شکل ۱۳-۱۲۱، برای تست این موضوع یکی از Jobها را اجرا می‌کنیم تا پشتیبانگیری را انجام دهد و بعد از اتمام باید یک ایمیل برای کاربر مورد نظر ارسال کند که با هم این موضوع را بررسی می‌کنیم.



شکل ۱۳- ۱۲۱ فعال‌سازی ایمیل در Veeam Backup

همان‌طور که در شکل ۱۳-۱۲۲، مشاهده می‌کنید ایمیل مورد نظر ارسال شده و به کاربر مورد نظر رسیده است و با رنگ سبز یعنی موفقیت دریافت شده است.



شکل ۱۳- ۱۲۲ ایمیل در Veeam Backup

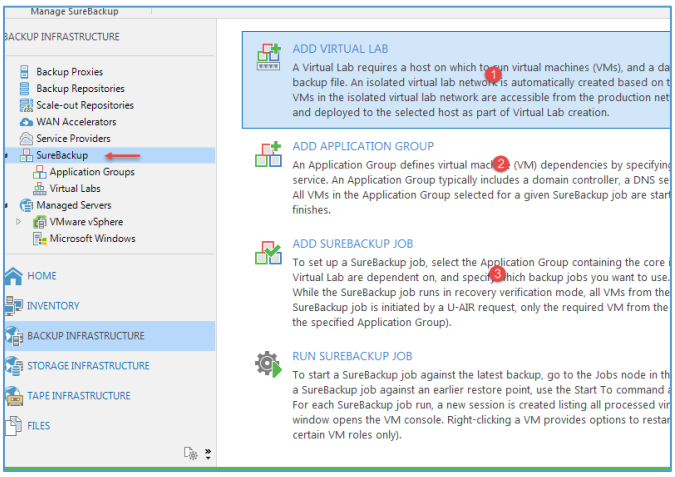
۱۳-۶ بررسی قابلیّت Sure Backup

زمانی‌که از ماشین‌ها و سرورهای فیزیکی خود پشتیبان تهیّه می‌کنید باید مطمئن شوید فایلی که برای پشتیبان ذخیره کردید، سالم است و یا در موقع Restore کارایی دارد یا نه، برای اینکه این مسائل را مشخّص کنید، شرکت Veeam، قابلیّت Sure Backup را برای این کار معرّفی کرد که در این قسمت با هم بررسی خواهیم کرد.

برای ورود به این قسمت به مانند شکل ۱۳-۱۲۳، وارد Infrastructure Backup شوید و بر روی Sure Backup کلیک کنید، در این قسمت، چند گزینه وجود دارد که در قسمت شماره‌ی یک بررسی عملکرد

www.takbook.com

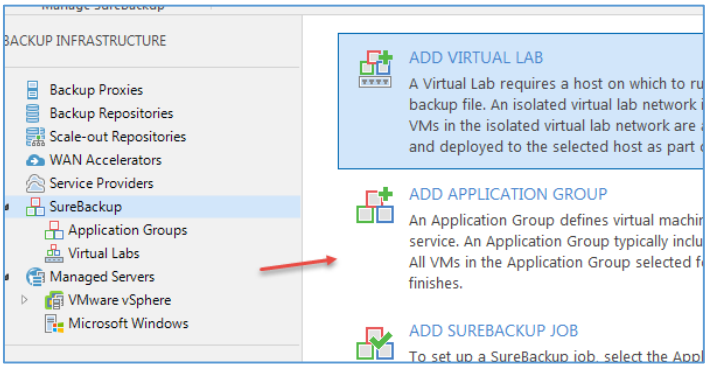
ماشین‌ها برای تست سلامتی که کاملاً جدا از شبکه‌ی ما است، در قسمت شماره‌ی دو که برای ایجاد گروه به کار می‌رود به این منظور به کار می‌رود که بعضی از ماشین‌ها دارای عملکرد مشابه هستند و حتماً باید در کنار هم اجرا شوند و این گروه نیز به خاطر همین موضوع ایجاد می‌شود، در قسمت شماره‌ی سه که یک وظیفه‌ی کاری (Task) است که برای صحّت عملکرد ماشین‌ها به کار می‌رود.



شکل ۱۳- ۱۲۳ بررسی قابلیّت *Sure Backup*

نرم‌افزار Veeam در این قابلیّت، سه تست کلّی را بر روی ماشین‌ها انجام می‌دهد که شامل: Test Heartbeat، Ping Test و Application Test است که در ادامه، بیشتر با این موضوعات آشنا خواهید شد.

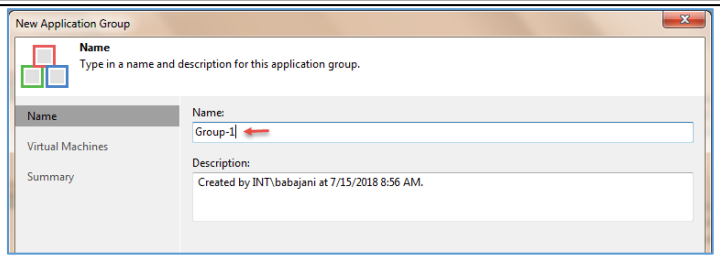
برای شروع کار به مانند شکل ۱۳-۱۲٤، باید بر روی Add Application Group کلیک کنید تا یک گروه از ماشین‌ها را برای تست آماده کنید.



شکل ۱۳- ۱۲۴ بررسی قابلیّت *Sure Backup*

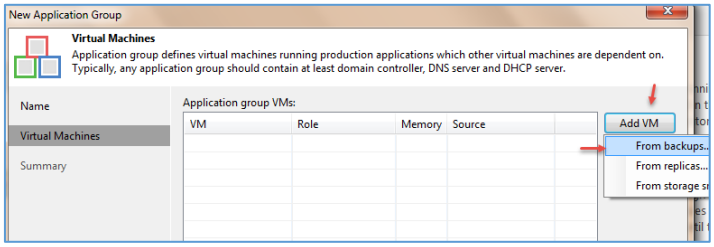
در شکل ۱۳-۱۲۵، نام گروه خود را وارد و بر روی Next کلیک کنید.

www.takbook.com



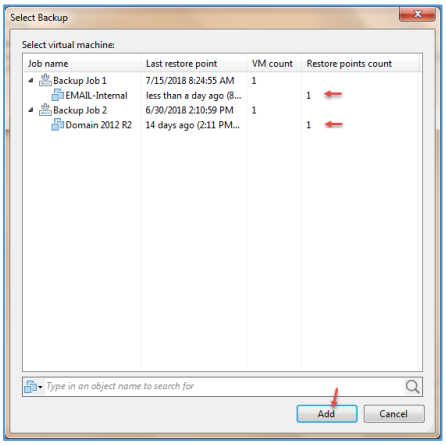
شکل ۱۳- ۱۲۵ بررسی قابلیّت *Sure Backup*

در شکل ۱۳-۱۲۶، باید ماشین مجازی خود را که از قبل از آن پشتیبان تهیّه کردید را به لیست اضافه کنید.



شکل ۱۳- ۱۲۶ بررسی قابلیّت *Sure Backup*

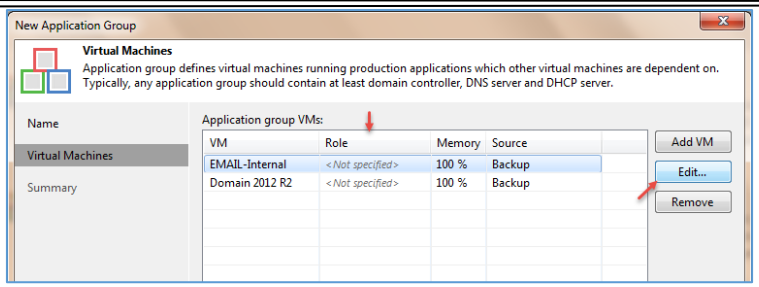
در شکل ۱۳-۱۲۷، دو ماشین مجازی را مشاهده می‌کنید که قبلاً از آنها پشتیبان تهیّه شده است، آنها را انتخاب و بر روی Add کلیک کنید.



شکل ۱۳- ۱۲۷ بررسی قابلیّت *Sure Backup*

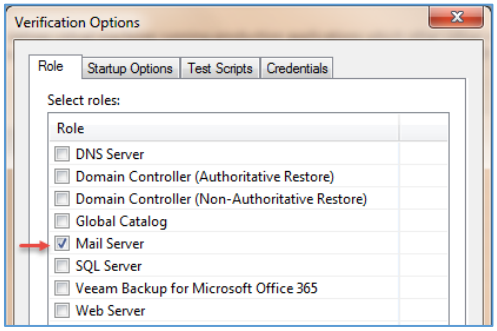
در شکل ۱۳-۱۲۸، باید Roleهای مربوط به ماشین مجازی مورد نظر را فعّال کنید تا در زمان تست، این Role نیز بررسی شود، پس برای انجام این کار ماشین مورد نظر را انتخاب و بر روی Edit کلیک کنید.

www.takbook.com



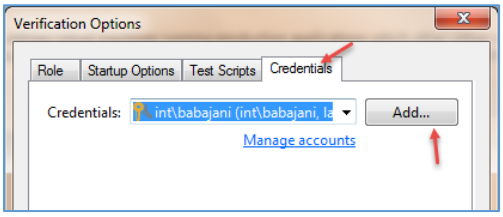
شکل ۱۳- ۱۲۸ بررسی قابلیّت *Sure Backup*

به مانند شکل ۱۳-۱۲۹، در تب Role باید Role را انتخاب کنید که مربوط به آن سرور است، مثلاً سروری که انتخاب کردیم یک ایمیل سرور داخلی است که سرویس ایمیل بر روی آن فعّال شده است.



شکل ۱۳- ۱۲۹ بررسی قابلیّت *Sure Backup*

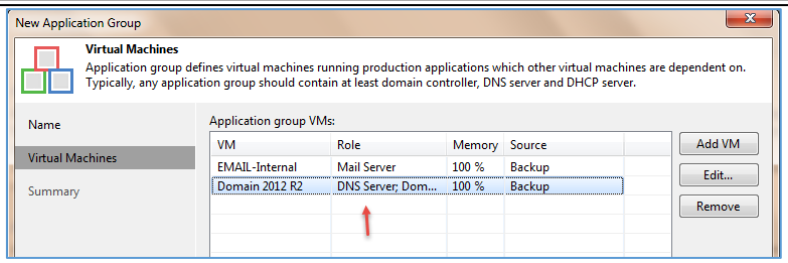
به مانند شکل ۱۳-۱۳۰، در تب Cerdentials باید نام کاربری که به سرور مورد نظر دسترسی دارد را انتخاب کنید و یا بر روی Add کلیک و آن را اضافه کنید.



شکل ۱۳- ۱۳۰ اضافه کردن *Account*

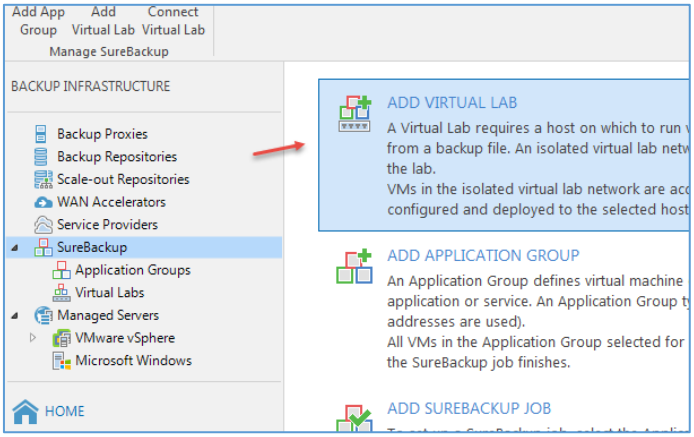
همان‌طور که در شکل ۱۳-۱۳۱، مشاهده می‌کنید برای هر دو سرور اطّلاعات Role ها وارد شده است، بر روی Next کلیک کنید.

www.takbook.com



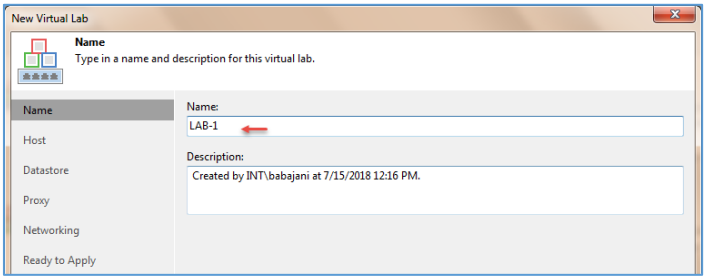
شکل ۱۳- ۱۳۱ اضافه کردن ماشین مجازی

به مانند شکل ۱۳-۱۳۲، بعد از ایجاد گروه مورد نظر و اضافه‌کردن سیستم به آن باید یک محیط مجازی برای تست ایجاد کنید، برای این کار بر روی ADD Virtual LAB کلیک کنید.



شکل ۱۳- ۱۳۲ ایجاد آزمایشگاه مجازی

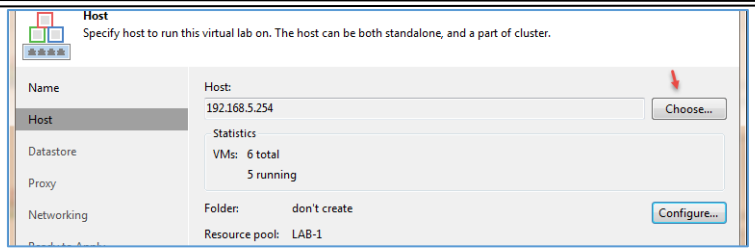
در شکل ۱۳-۱۳۳، نام LAB را وارد و بر روی Next کلیک کنید.



شکل ۱۳- ۱۳۳ آزمایشگاه مجازی

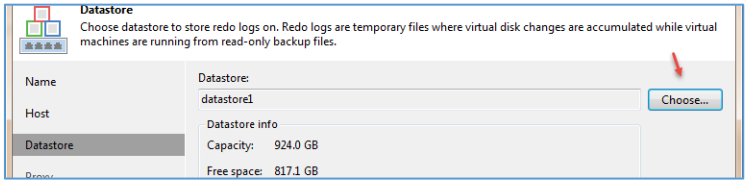
در شکل ۱۳-۱۳۴، باید یک سرور انتخاب کنید که بتوانید آزمایشگاه مجازی را بر روی آن اجرا کنید، البتّه سروری که انتخاب می‌کنید باید قدرت سخت‌افزاری و مقدار رم کافی را داشته باشد، در قسمت پایین، یک Pool به صورت اتوماتیک توسّط Veeam ایجاد خواهد شد.

www.takbook.com



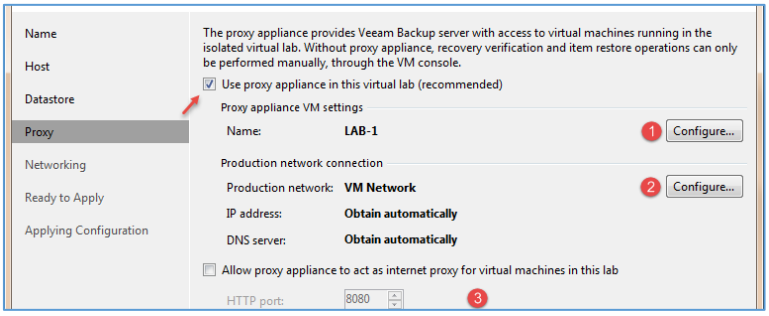
شکل ۱۳- ۱۳۴ انتخاب هاست ESXi

در شکل ۱۳-۱۳۵، باید یک فضای مناسب برای ذخیره‌سازی و اجرای ماشین‌ها انتخاب کنید، البتّه این فضا باید بر روی سروری باشد که در قسمت قبل، انتخاب می‌کنید.



شکل ۱۳- ۱۳۵ انتخاب دیتا استور

در شکل ۱۳-۱۳۶، که برای تست ارتباط شبکه‌ی بین ماشین‌ها در فضای مورد نظر است، تیک گزینه‌ی مورد نظر را انتخاب کنید، در قسمت شماره‌ی یک، یک نام برای آن مشخّص کنید و در قسمت شماره‌ی دو باید یکی از کارت‌های شبکه‌ی متّصل به سرور مورد نظر را انتخاب کنید، با کلیک بر روی Configure می‌توانید به صورت دستی IP ست کنید، در قسمت شماره‌ی سه اگر بخواهید به ماشین‌های مجازی که در حال تست هستند، اینترنت دهید باید آن را فعّال و تنظیم کنید، در حال حاضر برای تست کامل، تمام قابلیّت‌های نرم‌افزار آن را غیر فعّال کنید.

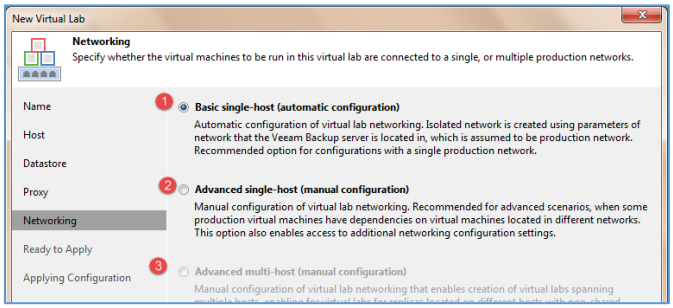


شکل ۱۳- ۱۳۶ انتخاب کارت شبکه

در شکل ۱۳-۱۳۷، در قسمت شماره‌ی یک، تنظیمات به صورت اتوماتیک برای شما انجام خواهد شد و نیاز به کار خاصّی نیست؛ در گزینه‌ی دو، اگر از یک سرور برای کار خود استفاده می‌کنید، می‌توانید آن را انتخاب کنید و تنظیمات را به صورت دستی انجام دهید، در قسمت شماره‌ی سه نیز اگر از چند سرور،

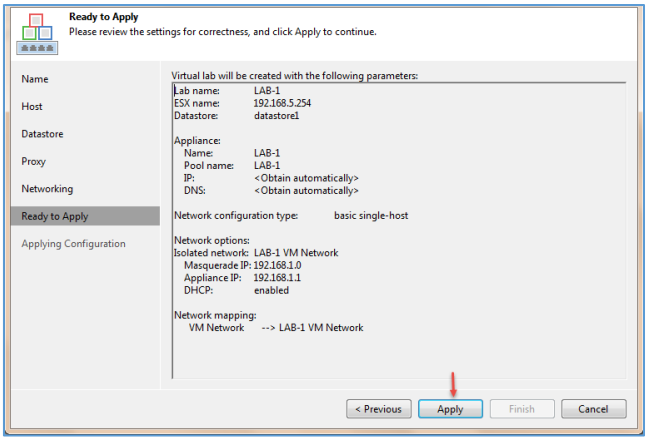
www.takbook.com

مثلاً سرور HP استفاده می‌کنید، می‌توانید این گزینه را انتخاب کنید، در حال حاضر گزینه‌ی یک را انتخاب و بر روی Next کلیک کنید.



شکل ۱۳- ۱۳۷ انتخاب حالت اتوماتیک

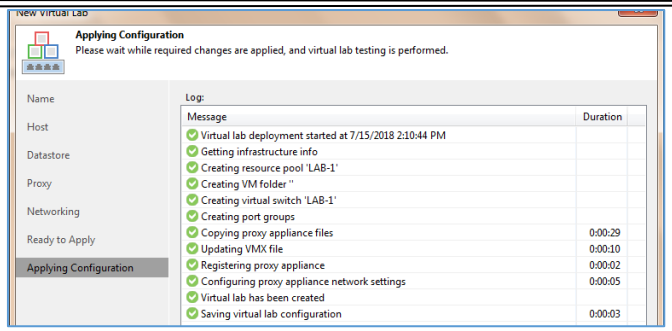
در شکل ۱۳-۱۳۸، اگر اطّلاعات مورد تأیید است بر روی Apply کلیک کنید تا آزمایشگاه مجازی مورد نظر ایجاد شود.



شکل ۱۳- ۱۳۸ تایید نهایی تنظیمات

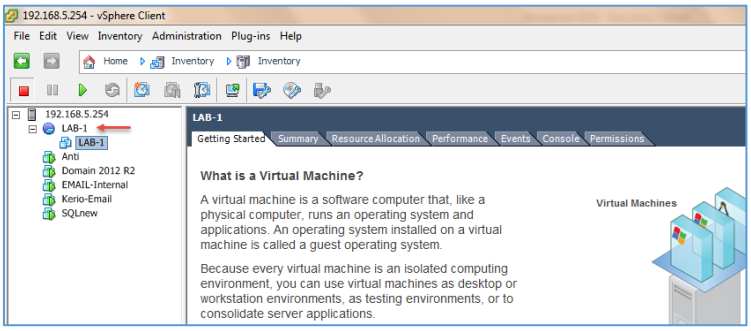
همان‌طور که در شکل ۱۳-۱۳۹،مشاهده می‌کنید، LAB مورد نظر با موفّقیّت ایجاد شده است.

www.takbook.com



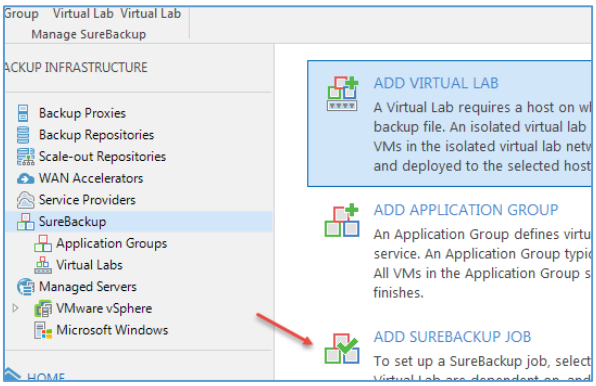
شکل ۱۳- ۱۳۹ تایید *LAB* نهایی

اگر از طریق نرم‌افزار Vsphere به سرور ESXi متّصل شوید، به مانند شکل ۱۳–۱۴۰، مشاهده خواهید کرد که یک Pool جدید با نام LAB-1 ایجاد شده است.



شکل ۱۳- ۱۴۰ ایجاد *LAB* مورد نظر در *ESXi*

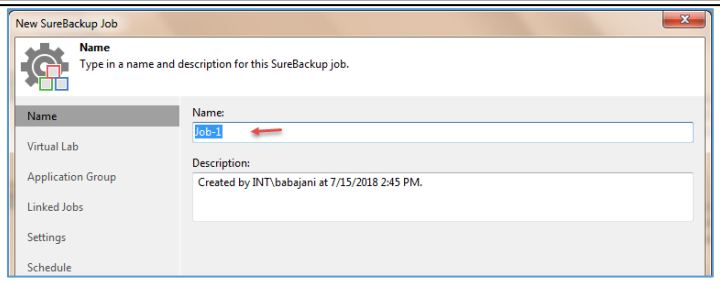
در شکل ۱۳–۱۴۱، باید تست خود را نهایی کنید، برای شروع، گزینه‌ی Job Add SureBackup را انتخاب کنید.



شکل ۱۳- ۱۴۱ ایجاد *Job* در *Sure*

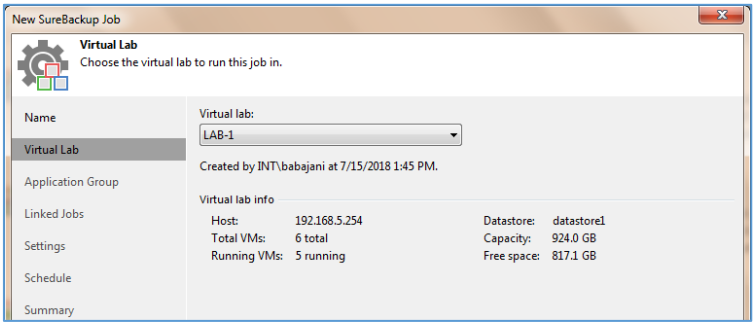
در شکل ۱۳–۱۴۲، نام مورد نظر خود را وارد و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۳- ۱۴۲ وارد کردن نام

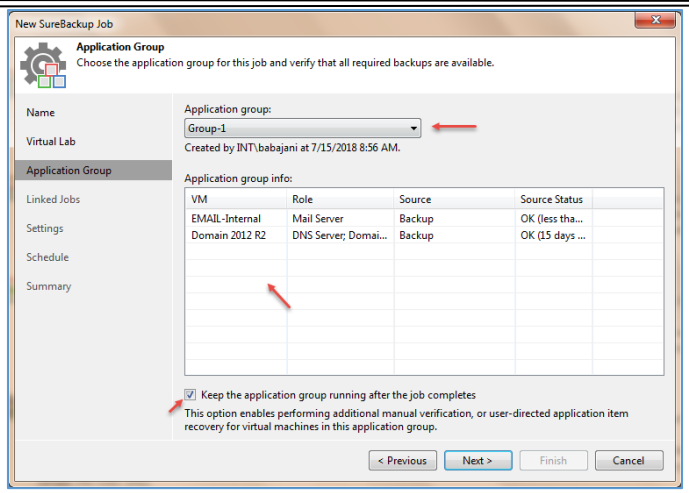
در شکل ۱۳-۱۴۳، باید Lab مورد نظر خود را انتخاب کنید که بعد از انتخاب، اطّلاعات آن نیز برای شما به نمایش گذاشته خواهد شد.



شکل ۱۳- ۱۴۳ انتخاب LAB

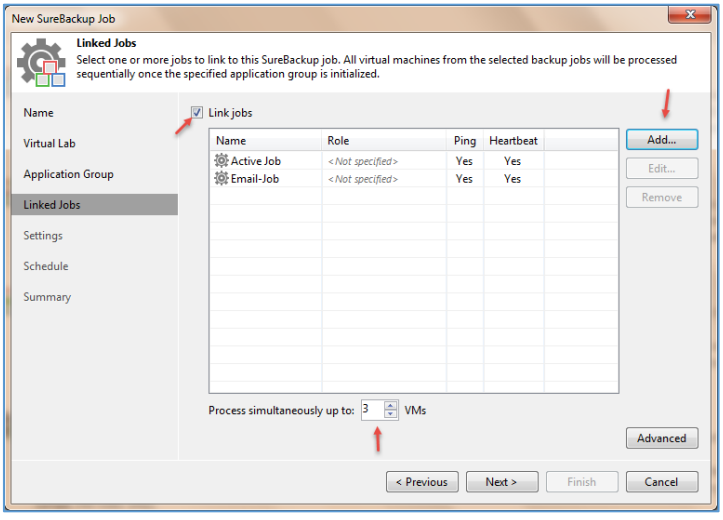
در شکل ۱۳-۱۴۴، باید گروه مورد نظر خود را که از قبل ایجاد کردید را انتخاب کنید که بعد از انتخاب، ماشین‌هایی که در آن قرار دارد برای شما به نمایش گذاشته می‌شود، با انتخاب تیک Keep the…، قبل از اینکهApplication Group فعّال شود، یک‌سری سرویس به آن اضافه خواهد شد که برای تست می‌تواند به شما کمک‌کند.

www.takbook.com



شکل ۱۳- ۱۴۴ انتخاب گروه مورد نظر

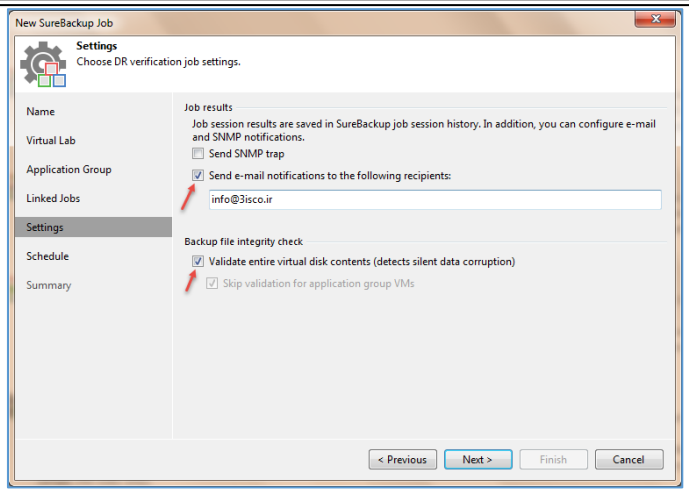
در شکل ۱۳-۱٤٤، باید Backup Job را که قبلاً با هم ایجاد کردیم را به لیست اضافه کنید و به مانند قبل، هر کدام از آنها که مربوط به ماشین مورد نظر است را انتخاب کنید و با کلیک بر روی Edit، دسترسی و همچنین، Role آن را نیز مشخّص کنید؛ در قسمت پایین، عدد سه، مشخّص‌کننده‌ی تعداد اجرای هم‌زمان ماشین مجازی است که می‌توانید این تعداد را تغییر دهید، در قسمت Advance می‌توانید Verfication و یا همان، تأیید را انجام دهید.



شکل ۱۳- ۱۴۵ انتخاب *Backup Job*

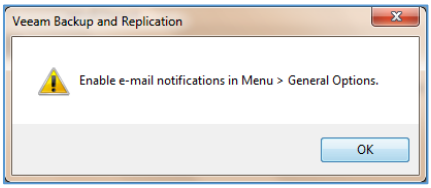
در شکل ۱۳-۱٤٦، باید یک ایمیل مشخّص کنید تا اطّلاعات این Job ایمیل شود تا از نتیجه‌ی کار آگاه شوید، تیک گزینه‌ی پائین را نیز بزنید تا چک نهایی بر روی فایل انجام شود.

www.takbook.com



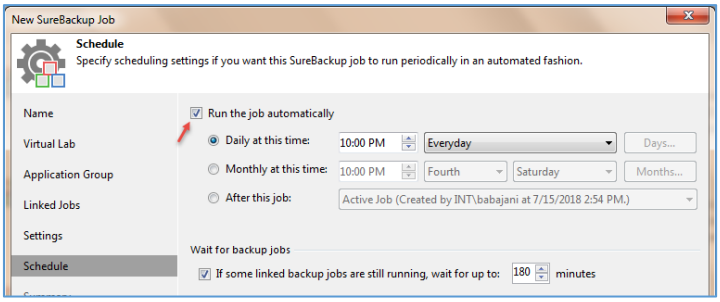
شکل ۱۳- ۱۴۶ وارد کردن آدرس ایمیل

به این نکته توجّه کنید که به مانند شکل ۱۳-۱۴۷، بعد از کلیک بر روی Next، یک پیغام به شما نمایش داده می‌شود و به این موضوع اشاره دارد که برای ارسال ایمیل باید تنظیمات مربوط به ایمیل انجام شود که بعد از این مراحل آن را انجام خواهیم داد.



شکل ۱۳- ۱۴۷ ایمیل آدرس

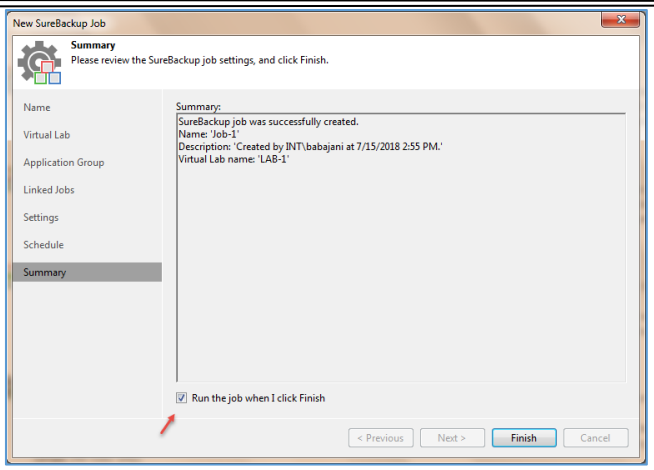
در شکل ۱۳-۱۴۸، می‌توانید زمان‌بندی برای خود مشخّص کنید تا این Job در زمان مشخّص، اجرا و اطّلاعات را ایمیل کند.



شکل ۱۳- ۱۴۸ ایجاد زمانبندی

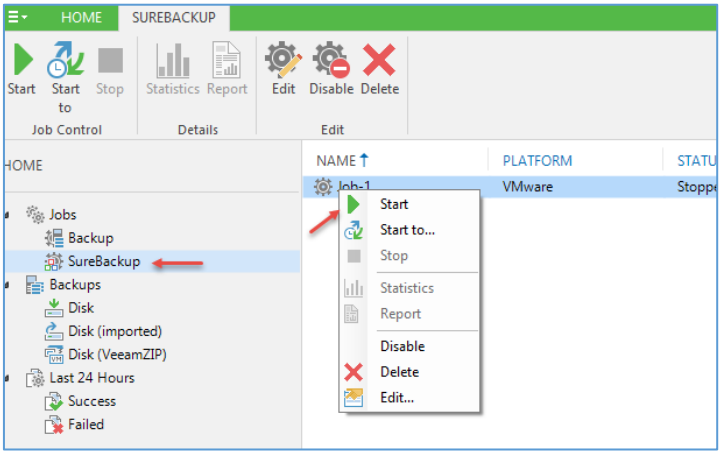
در شکل ۱۳-۱۴۹، تیک مورد نظر را بردارید و بر روی Finish کلیک کنید.

www.takbook.com



شکل ۱۳- ۱۴۹ اجرای Job مورد نظر

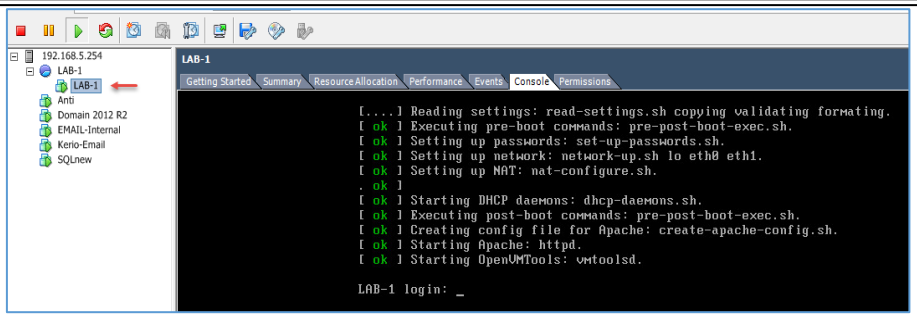
اگر به مانند شکل ۱۳-۱۵۰، به قسمت Job مراجعه کنید، گزینه‌ی SureBackup را مشاهده خواهید کرد که Job مورد نظر ما در آن قرار گرفته است، برای اجرای آن بر روی Start کلیک کنید.



شکل ۱۳- ۱۵۰ اجرای Job مورد نظر

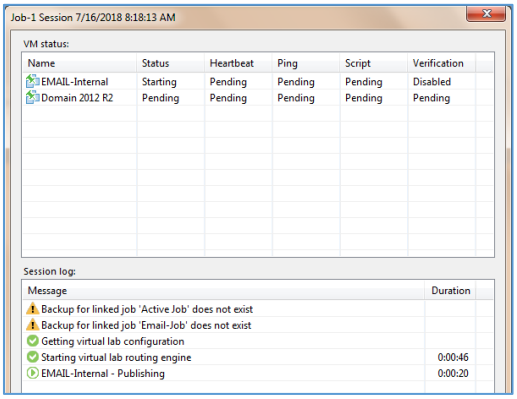
همان‌طور که در شکل ۱۳-۱۵۱، مشاهده می‌کنید، LAB مورد نظر روشن شده و در حال کار است.

www.takbook.com



شکل ۱۳- ۱۵۱ اجرای LAB در ESXi

در شکل ۱۳-۱۵۲، کار تست ماشین‌ها در حال انجام است و جزئیّات عملیّات، بعد از پایان کار به آدرس شما ایمیل خواهد شد.

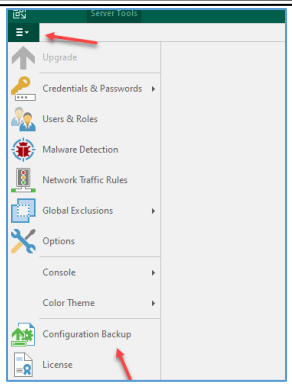


شکل ۱۳- ۱۵۲ تست آزمایشگاه مجازی

۱۳-۷ گرفتن Backup از تنظیمات نرم‌افزار

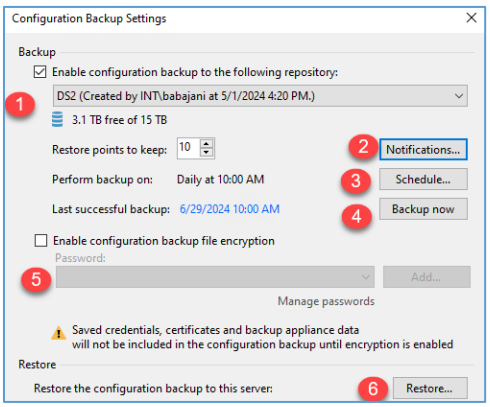
زمانی‌که تمام جزئیّات نرم‌افزار را برای شبکه آماده می‌کنید، بهتر است یک پشتیبان از تنظیمات مورد نظر تهیّه کنید تا بتوانید آن را در صورت بروز مشکل یا حذف‌کردن قسمتی از تنظیمات به حالت قبل بازگردانید. به مانند شکل ۱۳-۱۵۳، وارد نرم‌افزار شوید و بر روی آیکون مورد نظر در گوشه‌ی سمت چپ نرم‌افزار کلیک کنید تا منوی مورد نظر باز شود، در این قسمت بر روی گزینه‌ی Configuration Backup کلیک کنید.

www.takbook.com



شکل ۱۳- ۱۵۳ گرفتن Backup از تنظیمات

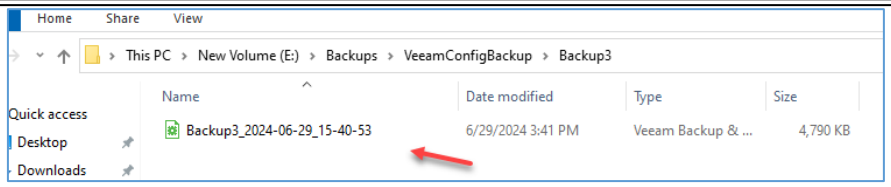
در شکل ۱۳-۱۵٤، در قسمت شماره‌ی یک باید یک سرور Repository برای ذخیره‌کردن این فایل پشتیبان انتخاب کنید، در قسمت شماره‌ی دو می‌توانید مشخص کنید که بعد از انجام Backup گزارشی به ایمیل شما ارسال شود یا خیر، در قسمت شماره‌ی سه می‌توانید زمان انجام این کار را به صورت اتوماتیک مشخّص کنید، در قسمت شماره‌ی چهار می‌توانید با کلیک بر روی Backup New از اطّلاعات یک، پشتیبان تهیّه کنید، امّا قبل از این کار و در قسمت شماره‌ی پنجم باید یک کاربر برای رمزنگاری آن انتخاب و یا اضافه کنید، در قسمت شماره‌ی شش با کلیک بر روی Restore می‌توانید در صورت بروز مشکل، تنظیمات قبلی را بازگردانید.



شکل ۱۳- ۱۵۴ گرفتن Backup از تنظیمات

بعد از اینکه از اطلاعات و تنظیمات Veeam یک بک آپ تهیه کردیم باید وارد آدرسی شویم که این بک آپ وجود دارد که در شکل ۱۳-۱۵۵، این موضوع را مشاهده می‌کنید و می‌توانید از آن استفاده کنید.

www.takbook.com



شکل ۱۳- ۱۵۵ گرفتن Backup از تنظیمات

www.takbook.com

www.takbook.com

فصل چهاردهم

Exchange Server 2019

با گسترش فناوری‌های ارتباطی و نیاز روزافزون به ابزارهای قدرتمند برای مدیریت ایمیل، پیام‌رسانی و همکاری تیمی، Exchange Server 2019 به‌عنوان یکی از راهکارهای پیشرفته مایکروسافت، جایگاه ویژه‌ای در دنیای فناوری اطلاعات یافته است.

هدف از نگارش این فصل، ارائه‌ی راهنمایی جامع و کاربردی برای متخصصین شبکه و مدیران فناوری اطلاعات است که به دنبال پیاده‌سازی، مدیریت و بهینه‌سازی Exchange 2019 در سازمان‌های خود هستند. Microsoft Exchange Server یکی از محصولات اصلی مایکروسافت در حوزه‌ی پیام‌رسانی و مدیریت ایمیل سازمانی است. این نرم‌افزار به‌عنوان یک سرور ایمیل قدرتمند، خدماتی فراتر از ارسال و دریافت ایمیل ارائه می‌دهد و امکانات پیشرفته‌ای برای تقویم، مدیریت وظایف، دفترچه آدرس، آرشیو ایمیل‌ها و اشتراک‌گذاری اسناد فراهم می‌کند.

ویژگی‌های کلیدی Exchange Server

- مدیریت ایمیل سازمانی

  Exchange Server امکان ارسال و دریافت ایمیل‌ها را با امنیت بالا و قابلیت مدیریت پیشرفته فراهم می‌کند. کاربران می‌توانند ایمیل‌های خود را با امکاناتی مانند فیلترهای ضد اسپم و ویروس، به‌صورت ایمن مدیریت کنند.
- تقویم و مدیریت زمان

  این نرم‌افزار امکان برنامه‌ریزی جلسات، مدیریت قرارها و هماهنگی بین تیم‌ها را با قابلیت اشتراک‌گذاری تقویم و مشاهده‌ی در دسترس بودن اعضا ارائه می‌دهد.
- دفترچه آدرس جهانی (GAL)

  Exchange Server یک دفترچه آدرس مرکزی ایجاد می‌کند که به همه‌ی کاربران در سازمان اجازه می‌دهد اطلاعات تماس همکاران خود را مشاهده و به اشتراک بگذارند.
- مدیریت وظایف و همکاری تیمی

  امکاناتی مانند وظایف (Tasks) و یادداشت‌ها (Notes) به کاربران اجازه می‌دهد تا پروژه‌ها را مدیریت کرده و بهره‌وری خود را افزایش دهند.
- ذخیره‌سازی و آرشیو

  با قابلیت آرشیو ایمیل‌ها، سازمان‌ها می‌توانند حجم ایمیل‌های جاری را کاهش داده و مدیریت بهتری بر اطلاعات ذخیره‌شده داشته باشند.
- امنیت و رعایت قوانین

www.takbook.com

با امکاناتی مانند رمزنگاری، مدیریت دسترسی، و ابزارهای پیشرفته برای رعایت قوانین (Compliance)، Exchange Server تضمین می‌کند که داده‌های حساس در برابر تهدیدات خارجی و داخلی محافظت شوند.

۱-۱٤ سخت‌افزار و نرم افزار مورد نیاز

در این قسمت می‌خواهیم به کمک یکدیگر Exchange Server 2019 را نصب و تنظیمات آن را انجام دهیم.
سخت‌افزاری که برای این سرور در نظر می‌گیرید، باید حداقل دارای ۳۰ گیگابایت رم باشد که ۲۰ گیگ آن برای سرویس MailBox است و ۱۰ گیگ آن هم برای سرویس Edge Transport استفاده می‌شود که البتّه با رم پایین‌تر از این هم نصب خواهد شد، امّا در روند کار شاید با خطا مواجه شوید. هر چقدر مقدار رم بیشتر باشد، سرویس بدون مشکل کار خواهد کرد، توصیه‌شده بسته به تعداد کاربران و حجم کاری، بین ۱۲۸ تا ۲٥٦ گیگابایت متغیر باشد.
پردازنده هم می‌تواند یک پردازنده‌ی ٦٤ بیتی دو هسته‌ای که حداقل دارای ۲.٤ گیگاهرتز سرعت است، باشد.
حداقل فضای هارد دیسک ۳۰ گیگابایت است که هر چقدر بیشتر باشد، بهتر خواهد بود، چون در ادامه‌ی کار به هر کاربر، فضایی تخصیص خواهیم داد که این فضا باید از همین هارد گرفته شود، پس حداقل ٦۰ گیگابایت در نظر بگیرید.
در حال حاضر در سازمانی که من در آن مشغول به کار هستم، حداقل رم برای سرور Exchange، ۳۲ گیگابایت و یک CPU Intel Xeon 2.27GHZ در نظر گرفته شده است که البتّه این مقدار رم در زمان درخواست‌های زیاد و سنگین، افزایش پیدا می‌کند.
پس سعی کنید قبل از راه‌اندازی چنین سرویس‌هایی حتماً سخت‌افزار مورد نظر آن را آماده و بعد اقدام به نصب آن کنید تا در زمان کار به مشکلی برنخورید.
اگر سخت‌افزار پایین باشد:

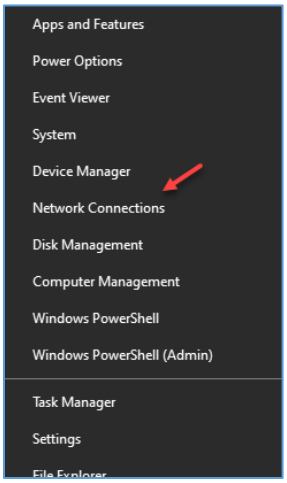
- سرویس‌ها دیر اجرا خواهند شد.
- زمانی که به یک کاربر ایمیل ارسال می‌کنید، شاید بعد از مدّت طولانی به دست کاربر برسد.

برای شروع از یک ویندوز سرور ۲۰۲٥ برای نصب Exchange 2019 استفاده می‌کنیم؛ بعد از نصب این ویندوز باید آن را عضو دومین مورد نظر خود کنیم، برای این کار به مانند زیر عمل می‌کنیم.

www.takbook.com

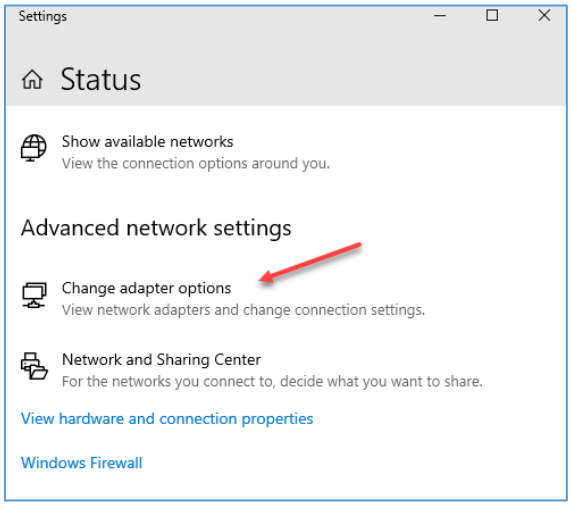
اوّلین کاری که انجام می‌دهیم باید آدرس IP را برای این سرور به صورت دستی وارد کنیم، یعنی اینکه اگر در شبکه‌ی خود از سرویس DHCP استفاده می‌کنیم و سرور به صورت اتوماتیک، IP دریافت کرد باید آن را به صورت دستی وارد کنیم تا در ادامه‌ی کار، آدرس آن تغییر نکند و ثابت باشد.

بر روی کلید ترکیبی WIN + X فشار دهید تا منوی شکل ۱۴-۱، ظاهر شود و گزینه‌ی Network Connections را انتخاب کنید.



شکل ۱۴- ۱ ورود به *Network Connection*

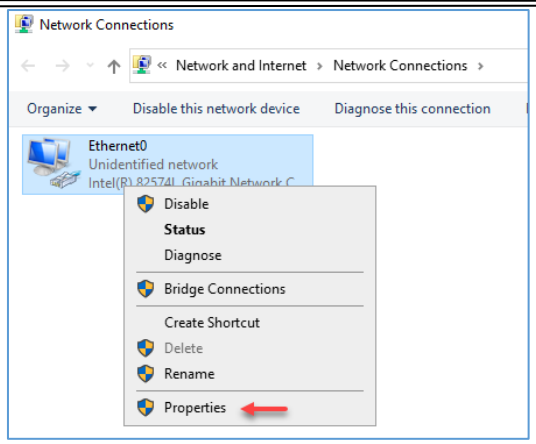
در شکل ۱۴-۲، گزینه‌ی Change adapter options را انتخاب کنید.



شکل ۱۴- ۲ تغییر آدرس *IP* کارت شبکه

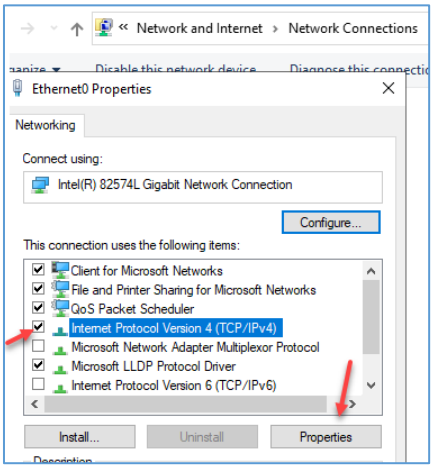
به مانند شکل ۱۴-۳، بر روی کارت شبکه‌ی خود کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.

www.takbook.com



شکل ۱۴- ۳ تغییر آدرس IP کارت شبکه

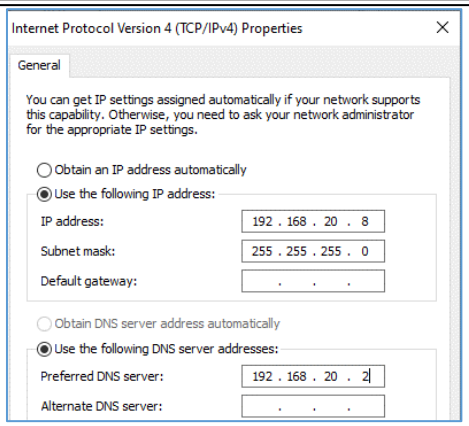
در شکل ۱٤-٤، اوّلین کاری که انجام می‌دهید انتخاب یکی از پروتکل‌های آدرس‌دهی می باشد که اگر فقط در شبکه‌ی خود از پروتکل IPv4 استفاده می‌کنید آن را در شکل انتخاب کنید و تیک کنار IPv6 را بردارید و بعد، گزینه‌ی IPv4 را انتخاب و سپس گزینه‌ی Properties را کلیک کنید.



شکل ۱۴- ۴ تغییر آدرس IP کارت شبکه

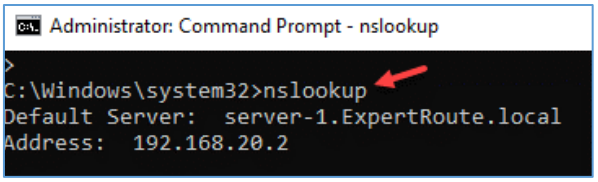
در شکل ۱٤-٥، آدرس سرور Exchange را وارد می‌کنیم، توجّه داشته باشید که در قسمت Preferred DNS Server، آدرس دومین خود را وارد کنید.

www.takbook.com



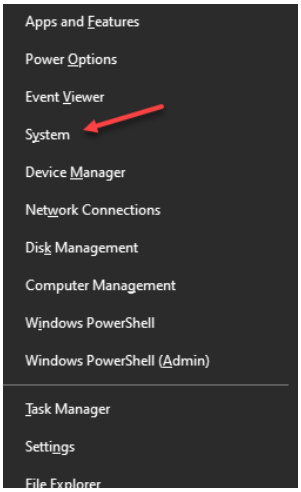
شکل ۱۴- ۵ تغییر آدرس IP کارت شبکه

بعد از اینکه آدرس را به صورت دستی وارد کردید، به مانند شکل ۱۴-۶، وارد CMD شوید و دستور Nslookup را اجرا کنید؛ با این کار مشخّص می‌شود که کلاینت سرور دومین را شناسایی کرده است.



شکل ۱۴- ۶ اجرای Nslookup

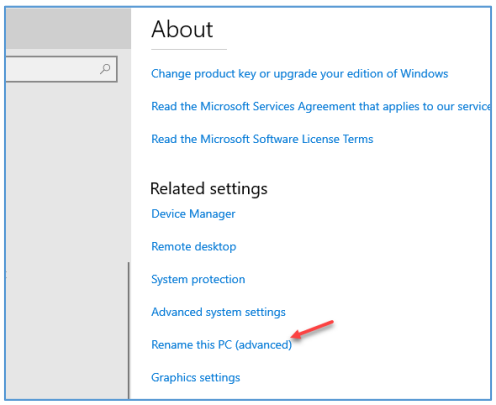
بعد از انجام کارهای بالا باید سرور مورد نظر را عضو دومین کنیم؛ برای این کار، به مانند شکل ۱۴-۷، کلید ترکیبی WIN + X را فشار دهید و گزینه‌ی System را انتخاب کنید.



شکل ۱۴- ۷ اجرای System

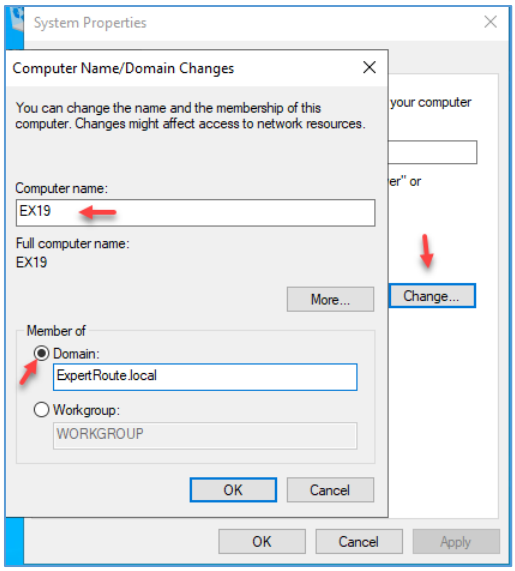
www.takbook.com

در شکل ۱۴–۸، گزینه‌ی Rename this PC را انتخاب کنید تا شکل بعد ظاهر شود.



شکل ۱۴- ۸اجرای Rename this PC

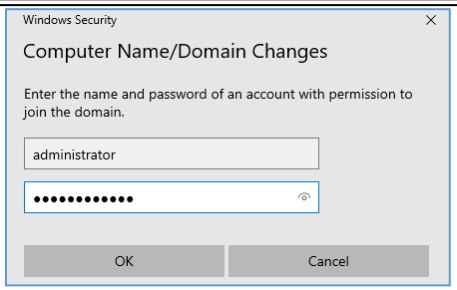
در شکل ۱۴–۹، بر روی گزینه‌ی Change کلیک کنید تا صفحه‌ی بالایی ظاهر شود. در این صفحه و در قسمت name computer، نام سرور خود را وارد کنید و در قسمت Member of، گزینه‌ی Domain را انتخاب کنید و نام دومین خود را وارد و بر روی OK کلیک کنید.



شکل ۱۴- ۹ تغییر نام ویندوز و عضویت در دومین

در شکل ۱۴–۱۰، نام کاربری و رمز عبور کاربر Administrator خود را وارد و بر روی OK کلیک کنید، بعد از این پنجره‌ای ظاهر می‌شود که عضو شدن در دومین را تأیید می‌کند؛ بر روی OK کلیک کنید و در صفحه‌ی بعد از آن هم بر روی OK کلیک کنید و سیستم را Restart کنید.

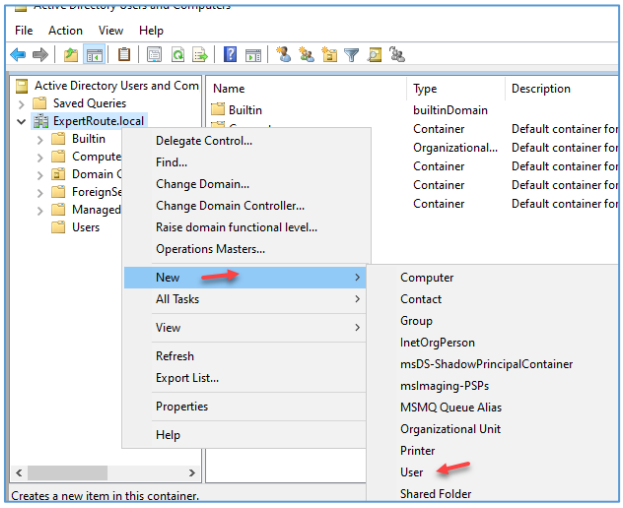
www.takbook.com



شکل ۱۴- ۱۰ تغییر نام ویندوز و عضویت در دومین

۱۴-۲ ایجاد کاربر ادمین با دسترسی کامل

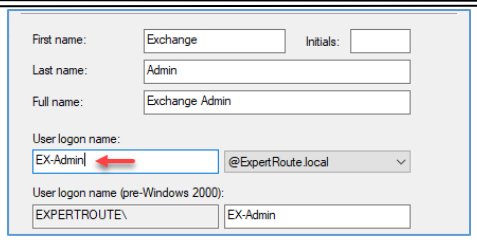
برای اینکه نرم‌افزار Exchange را نصب کنیم نیاز به کاربری داریم که عضو گروه‌هایی مانند Enterprise Admins و Schema Admins باشد تا توانایی نصب این نرم افزا را در شبکه داشته باشد، برای ایجاد این کاربر وارد Active Directory Users and Computer شوید و به مانند شکل ۱۴-۱۱، از قسمت New گزینه‌ی Users را انتخاب کنید.



شکل ۱۴- ۱۱ ایجاد کاربر ادمین با دسترسی کامل

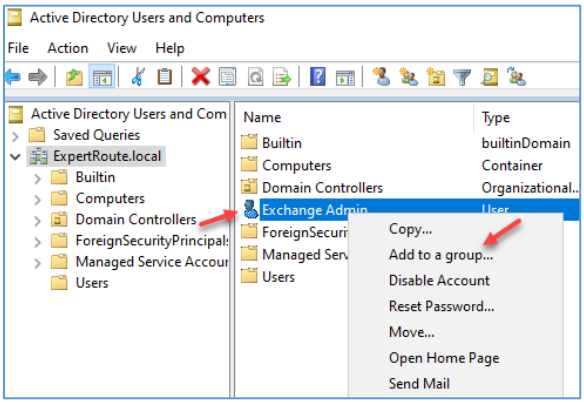
در شکل ۱۴-۱۲، نام کاربری را وارد کنید و رمز آن را مشخص و آن را ایجاد کنید.

www.takbook.com



شکل ۱۴- ۱۲ ایجاد کاربر ادمین با دسترسی کامل

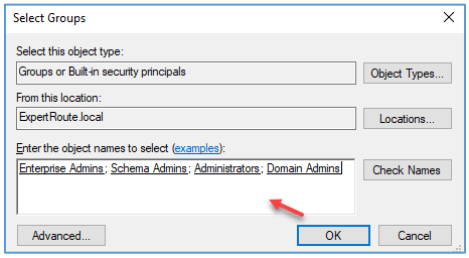
بعد از ایجاد کاربر مورد نظر بر روی آن کلیک راست کنید و گزینه‌ی Add to a group را انتخاب کنید تا بتوانیم این کاربر را عضو گروه‌های مشخص شده کنیم.



شکل ۱۴- ۱۳ ایجاد کاربر ادمین با دسترسی کامل

در شکل ۱۴-۱۴، چهار گروه مشخص شده را به لیست اضافه کنید:

- Enterprise Admins
- Schema Admins
- Administrators
- Domain Admins



شکل ۱۴- ۱۴ ایجاد کاربر ادمین با دسترسی کامل

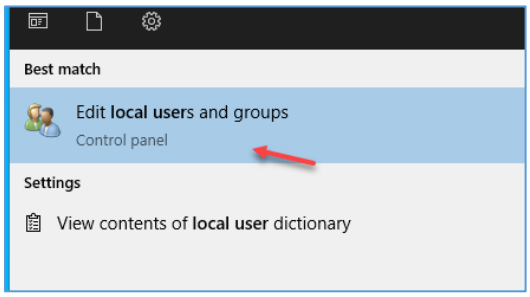
بعد از اینکه کاربر مورد نظر را عضو گروه مشخص شده کردید باید با همین کاربر به مانند شکل ۱۴-۱۵، وارد سرور Exchange شوید و کار نصب را آغاز کنید.

www.takbook.com



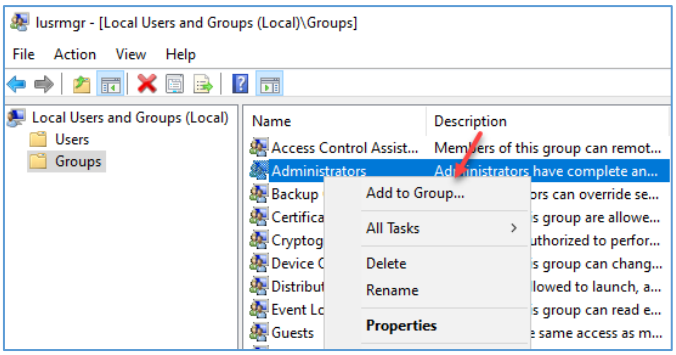
شکل ۱۴- ۱۵ ورود با کاربر ادمین

توجه داشته باشید بعد از اینکه وارد سرور شدید باید کاربر مورد نظر را عضو گروه Administrators کنید که گروه محلی سرور است، برای انجام این کار به مانند شکل ۱۴-۱۶، وارد سرویس Local Users and Groups شوید.



شکل ۱۴- ۱۶ عضویت در گروه Local

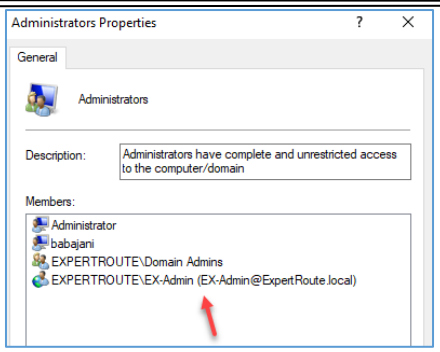
به مانند شکل ۱۴-۱۷، وارد Groups شوید و بر روی گروه Administrators کلیک راست کنید و گزینه‌ی Add to groups را انتخاب کنید.



شکل ۱۴- ۱۷ عضویت در گروه Local

در شکل ۱۴-۱۸، بر روی Add کلیک کنید و کاربر مورد نظر را که در دومین ایجاد کردیم به لیست اضافه کنید و بر روی OK کلیک کنید، توجه داشته باشید بعد از این کار سرور را Restart کنید.

www.takbook.com



شکل ۱۴- ۱۸ عضویت در گروه Local

۱۴-۳ نصب پیش‌نیازهای Exchange 2019

برای اینکه Exchange 2019 را به درستی نصب کنیم باید پیش‌نیازهای آن را هم نصب کنیم، برای این کار از لینک زیر فایل‌های مورد نظر را دانلود و نصب کنید:

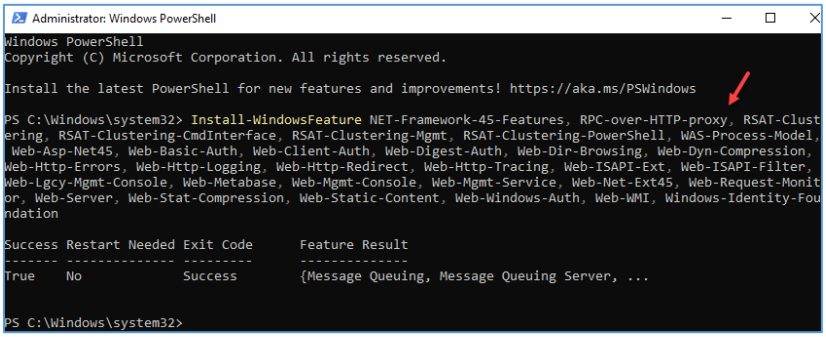
https://expertroute.ir/PRE-EX-2019.zip

در این فایل فشرده دو نرم افزار Visual C++ redistributable package 2013 و Unified Communications Managed API 4.0 Runtime قرار دارد هر دوی آنها را نصب کنید.

در ادامه کار باید از طریق PowerShell دستورات زیر را به صورت کامل اجرا کنید.

```
Install-WindowsFeature NET-Framework-45-Features, RSAT-ADDS, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation
```

همان‌طور که در شکل ۱۴-۱۹، مشاهده می‌کنید دستورات مورد نظر به درستی نصب شده است.



شکل ۱۴- ۱۹ نصب پیش‌نیازها

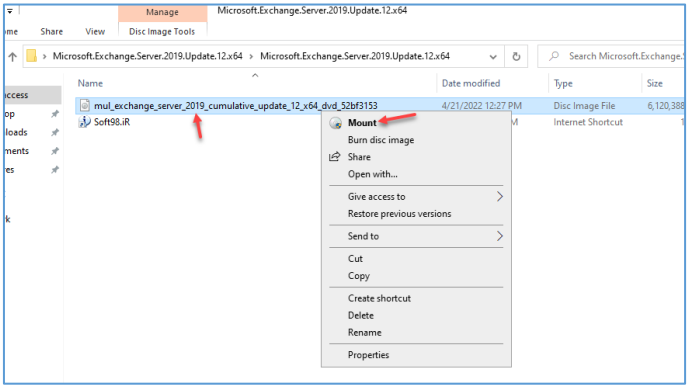
www.takbook.com

بعد از نصب پیش نیاز های مورد نظر باید نرم افزار URL Rewrite Module را از لینک زیر دانلود و نصب کنید:

https://download.microsoft.com/download/1/2/8/128E2E22-C1B9-44A4-BE2A-5859ED1D4592/rewrite_amd64_en-US.msi

در ادامه کار باید آخرین ورژن Exchange 2019 را از لینک زیر دانلود و نصب را آغاز کنیم:
https://www.microsoft.com/en-us/download/details.aspx?id=105878

بعد از دانلود فایل مورد نظر به مانند شکل ۱۴-۲۰، بر روی فایل مورد نظر کلیک راست کنید و گزینه‌ی Mount را انتخاب کنید و در صفحه باز شده بر روی Setup کلیک کنید.



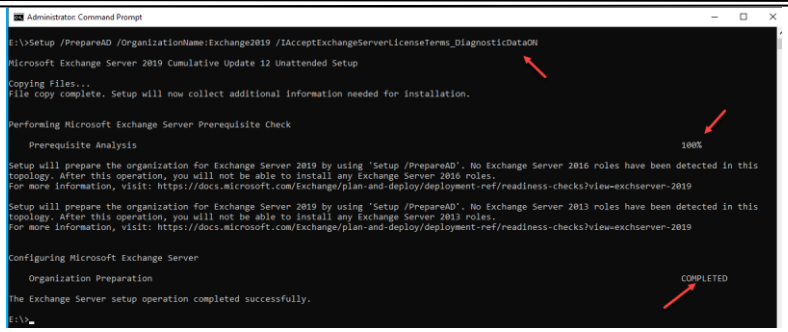
شکل ۱۴- ۲۰ نصب *Exchange 2019*

قبل از شروع به کار باید برای آماده‌سازی دومین خود برای نصب Exchange server 2019 از دستور زیر استفاده کنیم:

.\Setup.EXE /PrepareAD /OrganizationName:Exchange2019 /IAcceptExchangeServerLicenseTerms_DiagnosticDataON

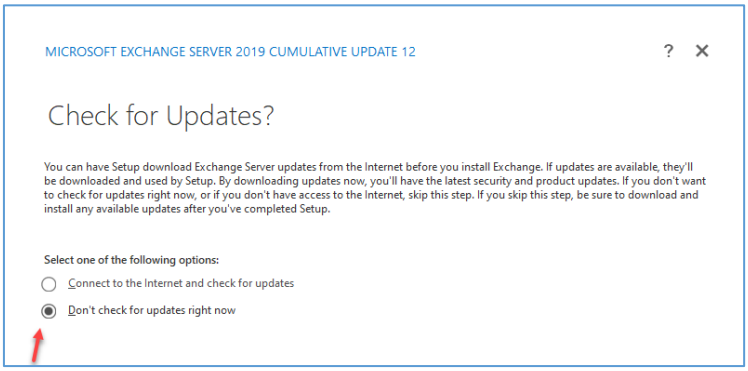
همان‌طور که در شکل ۱۴-۲۱، مشاهده می‌کنید اول وارد درایوی شدیم (E:) که DVD مربوط به Exchange 2019 در آن قرار دارد یعنی با وارد کردن E: می‌توانید وارد درایو مورد نظر شویم و بعد دستور بالا را اجرا کردیم، با این کار تنظیمات اولیه انجام می‌شود و یک OU با نام Exchange2019 در Active ایجاد می‌شود.

www.takbook.com



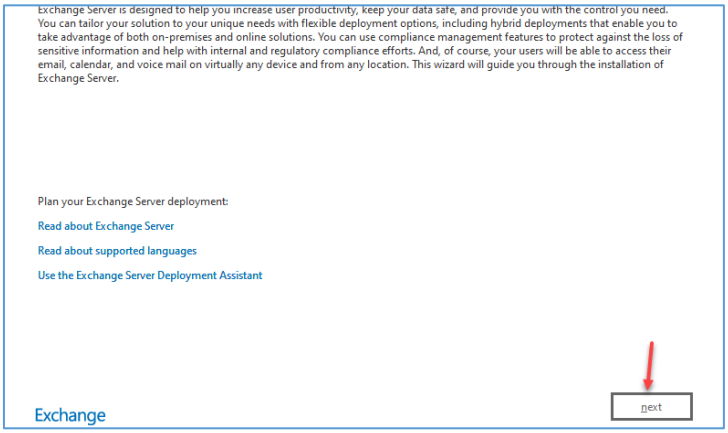
شکل ۱۴- ۲۱ نصب Exchange 2019

بعد از انجام تمام مراحل بالا وارد درایو Exchange شوید و فایل Setupe را اجرا کنید، به مانند شکل ۱۴-۲۲، گزینه‌ی مورد نظر را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۴- ۲۲ نصب Exchange 2019

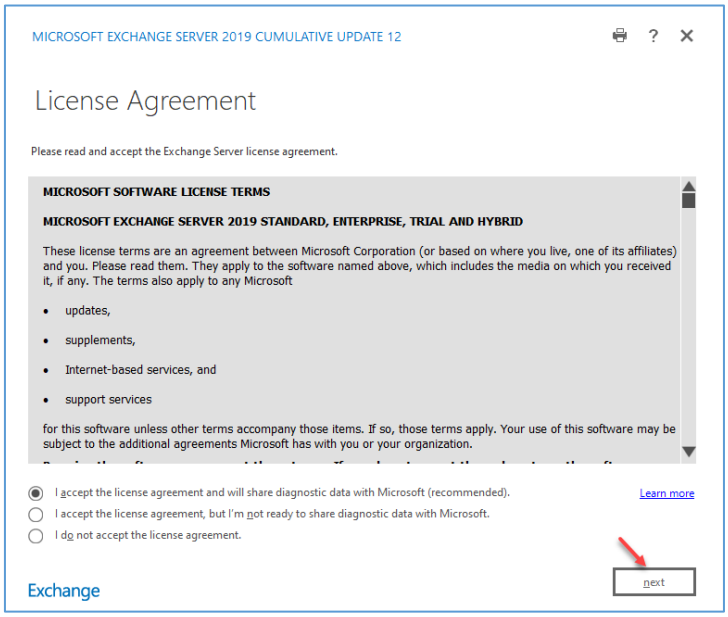
در شکل ۱۴-۲۳، می‌توانید توضیحات این نرم‌افزار را بررسی کنید و بر روی Next کلیک کنید.



شکل ۱۴- ۲۳ نصب Exchange 2019

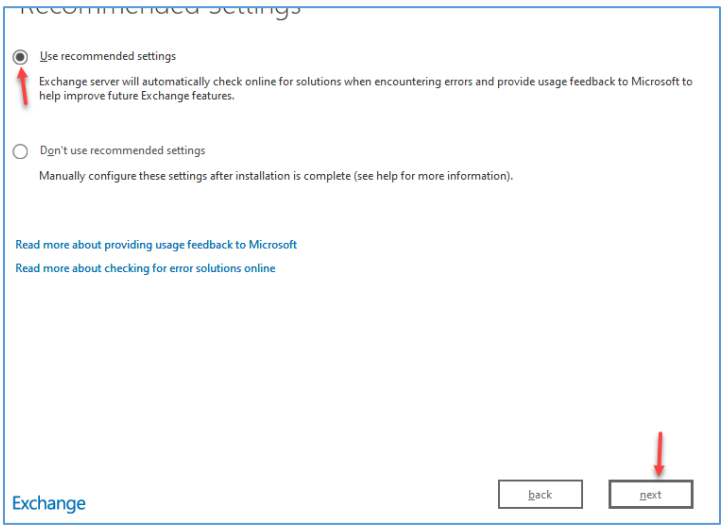
www.takbook.com

در شکل ۱۴-۲۴، قراردادنامه استفاده از این نرم‌افزار را مطالعه و در صورت تایید بر روی Next کلیک کنید.



شکل ۱۴- ۲۴ نصب Exchange 2019

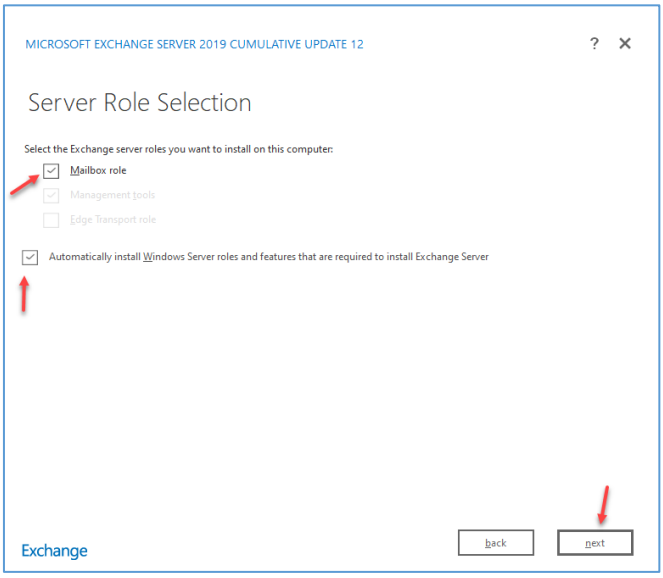
در شکل ۱۴-۲۵، اگر می‌خواهید مایکروسافت اطلاعات این نرم افزار را در اختیار داشته باشد و در صورت مشکل به شما کمک کند می‌توانید گزینه‌ی اول را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۴- ۲۵ نصب Exchange 2019

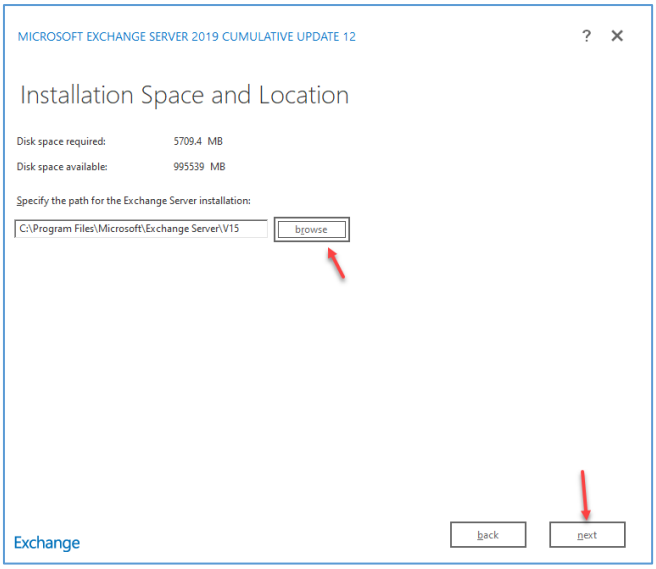
www.takbook.com

به مانند شکل ۱٤-۲٦، برای نصب کامل نرم‌افزار Exchange 2019 گزینه‌های مورد نظر را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۴- ۲۶ نصب Exchange 2019

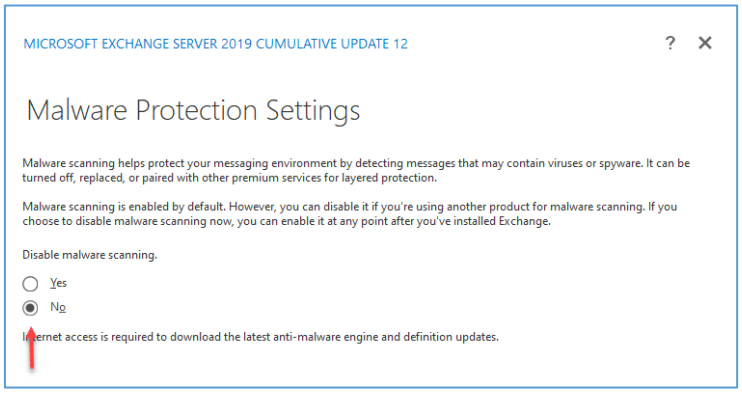
در شکل ۱٤-۲۷، می‌توانید مسیر نصب را طبق حجمی که مورد نیاز است انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۴- ۲۷ نصب Exchange 2019

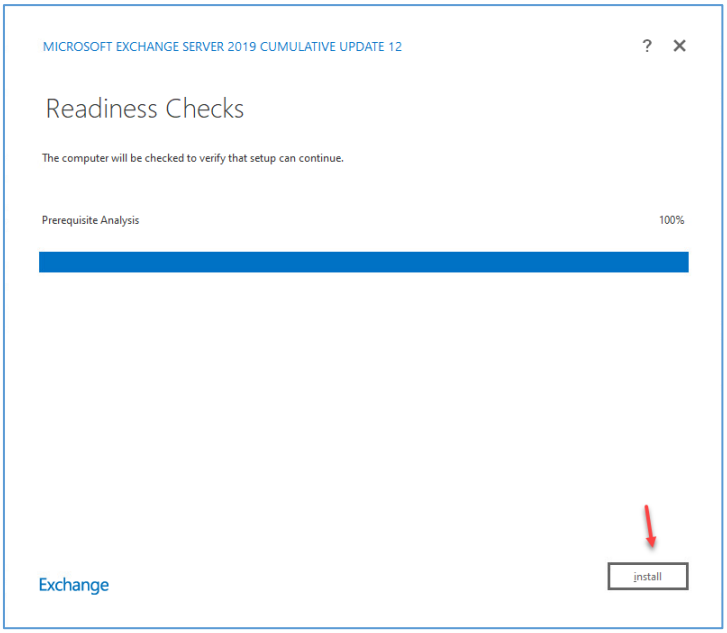
www.takbook.com

در شکل ۱۴-۲۸، اگر می‌خواهید سرویس آنتی ویروس غیرفعال شود باید گزینه‌ی Yes را انتخاب کنید وگرنه می‌توانید گزینه‌ی No را انتخاب و بر روی Next کلیک کنید.



شکل ۱۴- ۲۸ نصب *Exchange 2019*

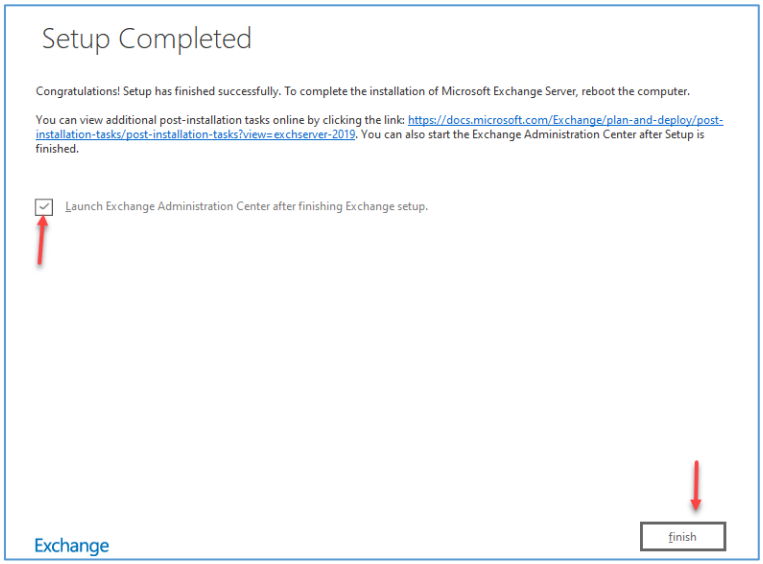
در آخر تمام پیش‌نیاز های نصب را بررسی می‌کند و در صورتی که مشکلی نباشد شکل ۱۴-۲۹، ظاهر می‌شود و اگر هم یک اخطار را مشخص کرده است، این اخطار به خاطر سرویس Exchange Emergency Mitigation (EM) service است که سرورتان باید انلاین و به اینترنت متصل باشد تا بتواند به سرور مایکروسافت متصل شود و از آخرین ویژگی‌های امنیتی مطلع شود، بر روی Install کلیک کنید تا کار نصب آغاز شود.



شکل ۱۴- ۲۹ نصب *Exchange 2019*

www.takbook.com

بعد از چند دقیقه تمام سرویس‌های مورد نیاز نصب می‌شود و شکل ۱۴-۳۰، ظاهر خواهد شد که باید تیک گزینه‌ی مورد نظر را انتخاب و بر روی Finish کلیک کنید.

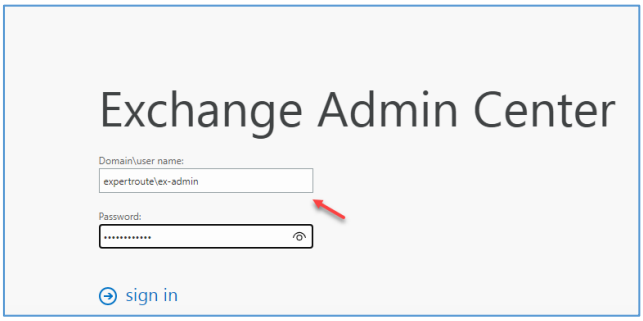


شکل ۱۴- ۳۰ نصب Exchange 2019

۱۴-۵ بررسی صفحه مدیریتی Exchange 2019

همان‌طور که در تصویر ۱۴-۳۱، مشاهده می‌کنید، صفحه‌ی ورود به مدیریّت اجرا شده است که شما باید نام کاربری که با آن Exchange را نصب کردید را به همراه نام دومین وارد کنید و بعد بر روی Sign in کلیک کنید، به این نکته توجه کنید که آدرس صفحه مدیریتی به صورت زیر است، به جای ex19 باید نام سرور خود را وارد کنید.

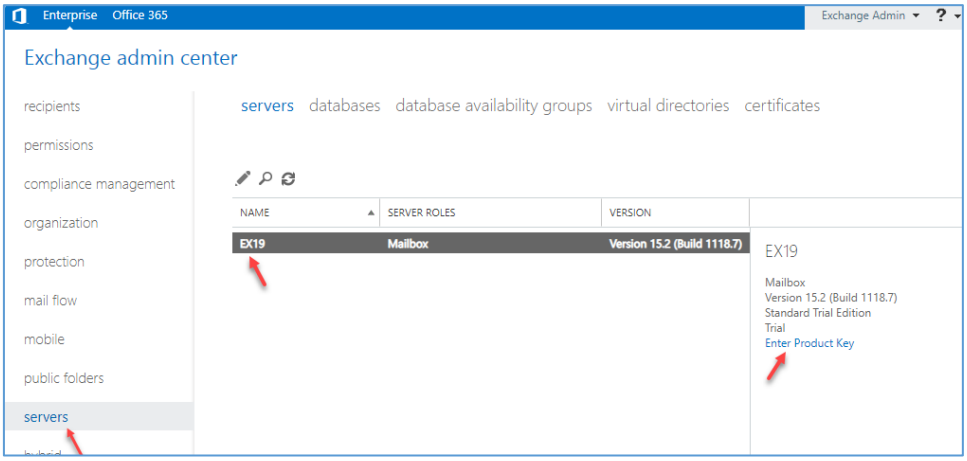
https://ex19/ecp/



شکل ۱۴- ۳۱ بررسی صفحه مدیریتی

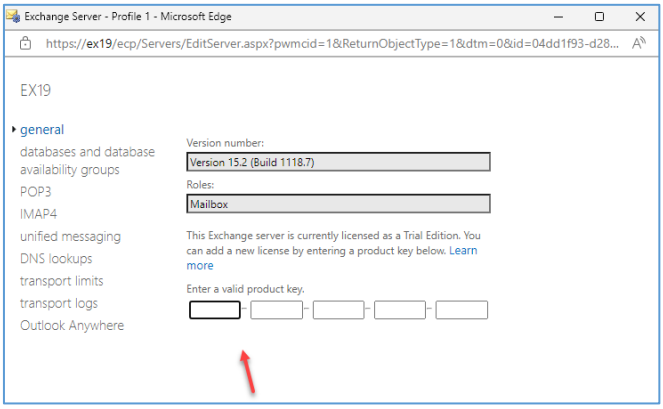
www.takbook.com

اوّلین کاری که بعد از ورود به صفحه‌ی مدیریّت exchange انجام می‌دهید، این است که این نرم‌افزار را فعّال کنید؛ برای این کار از سمت چپ بر روی Servers کلیک کنید و بعد در صفحه‌ی باز شده، وارد تب Servers شوید؛ در این صفحه و در سمت راست بر روی Enter Product Key کلیک کنید.



شکل ۱۴- ۳۲ بررسی صفحه مدیریتی

در شکل ۱۴-۳۳، در قسمت Enter a valid product key، سریال نرم‌افزار را که خریداری کردید را وارد کنید و بر روی Save کلیک کنید.

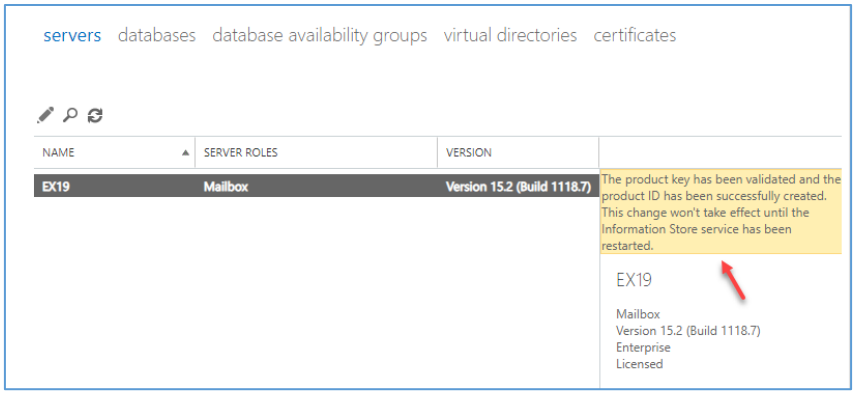


شکل ۱۴- ۳۳ بررسی صفحه مدیریتی

Enterprise: YCQY7-BNTF6-R337H-69FGX-P39TY
Standard: G3FMN-FGW6B-MQ9VW-YVFV8-292KP

www.takbook.com

بعد از ظاهر شدن این پیامدر شکل ۱۴-۳۵، به شما اعلام می‌شود که سریال ورودی درست بوده و برای اینکه به صورت کامل از نرم‌افزار استفاده کنید، بهتر است سرور را Restart کنید و یا اینکه سرویس‌های مربوط به این نرم‌افزار را Restart کنید.



شکل ۱۴- ۳۴ بررسی صفحه مدیریتی

اگر دوباره وارد صفحه‌ی مدیریّت شوید و سپس وارد قسمت Servers شوید، متوجّه خواهید شد که سرور فعّال شده است و می‌توانید با خیال راحت به ادامه‌ی کار بپردازید.

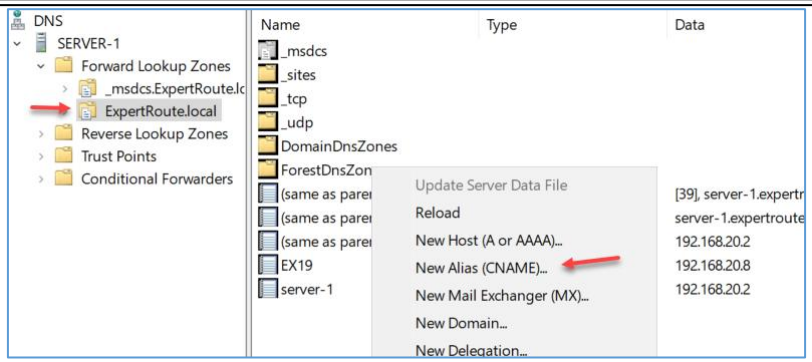
۱۴-۶ تنظیم سرویس DNS

برای اینکه سرور Exchange به درستی فعالیت کند نیاز به تنظیم DNS برای آن داریم، برای این کار وارد سرویس DNS در سرور دومین شوید و یک Cname با نام Autodiscover ایجاد و به سرور Exchange 2019 متّصل کنید تا در ادامه‌ی کار به مشکل برنخورید؛ این Cname مربوط به سرور Exchange است و مورد نیاز است.

توجه داشته باشید که Autodiscover یک سرویس در Exchange است و به کاربران کمک می‌کند تا به صورت خودکار به Exchange و ایمیل خودشان متصل شوند، یعنی مثلاً اگر کاربر مورد نظر وارد اکانت خود شود و نرم افزار Outlook را اجرا کند با فعال بودن سرویس Autodiscover این ارتباط به صورت خودکار انجام خواهد گرفت و نیازی به تنظیم دستی نیست.

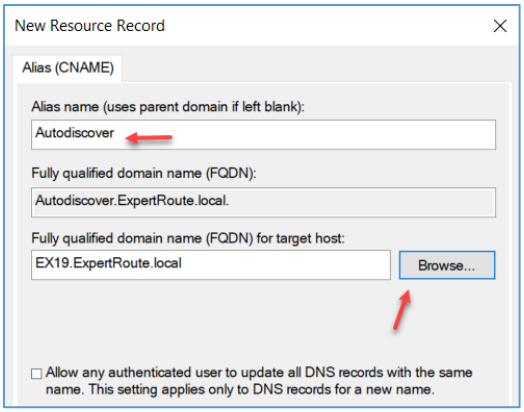
وارد سرور دومین شوید و در جستجو، DNS را اجرا کنید؛ به مانند شکل ۱۴-۳۵، بر روی نام دومین خود کلیک راست کنید و گزینه‌ی New Alias (CNAME) را انتخاب کنید.

www.takbook.com



شکل ۱۴- ۳۵ تنظیم سرویس DNS

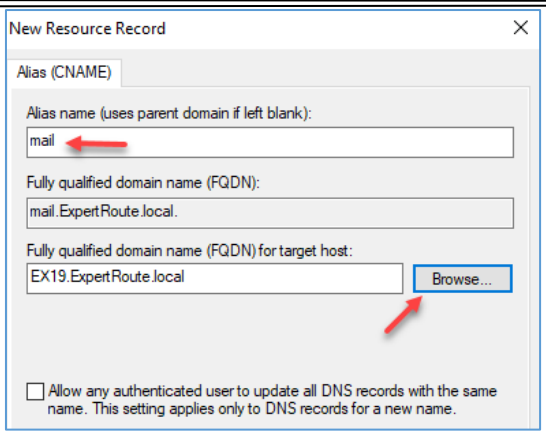
در شکل ۱۴-۳۶، در قسمت Alias name، نام Autodiscover را وارد کنید و از قسمت FQDN بر روی Brwse کلیک کنید و نام سرور Exchange خود را انتخاب کنید که شبیه به شکل ۱۴-۳۶، است، بر روی OK کلیک کنید تا Cname مورد نظر ایجاد شود.



شکل ۱۴- ۳۶ تنظیم سرویس DNS

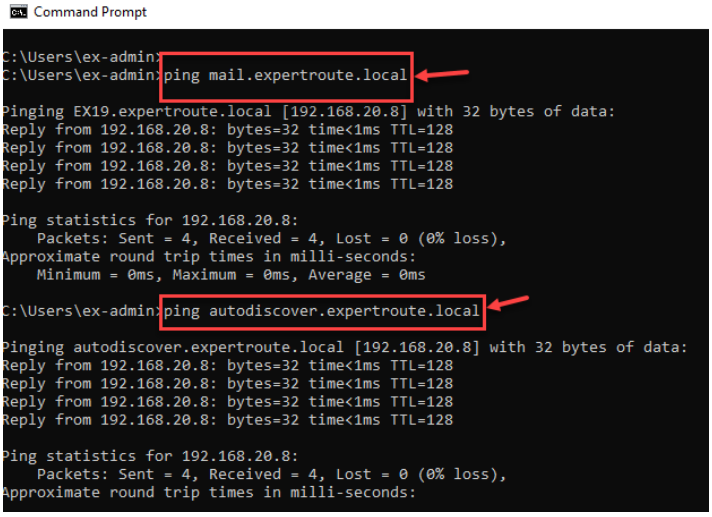
گزینه‌ی دیگری که باید ایجاد کنید آدرس mail.expertroute.local است که به مانند شکل ۱۴-۳۷، یک Cname برای آن ایجاد می‌کنید.

www.takbook.com



شکل ۱۴- ۳۷ تنظیم سرویس DNS

بعد از اینکه DNS را تنظیم کردید وارد سرور Exchange شوید و این دو آدرس را Ping بگیرد تا درستی کار مشخص شود، این کار را در شکل ۱۴–۳۸، مشاهده می‌کنید.



شکل ۱۴- ۳۸ تست ارتباط

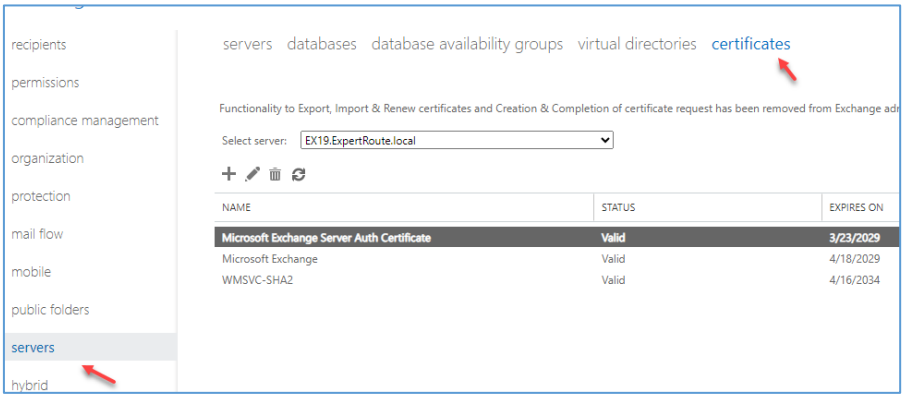
۱۴–۷ تنظیم گواهینامه داخلی برای کاربران

یکی ازمهمترین بخش‌هایی که در Exchange باید به درستی تنظیم کنید ایجاد و فعال‌سازی گواهینامه‌های امنیتی است که درست تنظیم کردن آن بسیار مهم است، در این قسمت می‌خواهیم با هم این کار را انجام دهیم.

www.takbook.com

اگر وارد صفحه‌ی مدیریتی ایکسچنج شوید و از قسمت Server وارد تب Certificate شوید چندین گواهینامه را مشاهده می‌کنید که به صورت اتوماتیک ایجاد شده‌اند و به هیچ عنوان نباید تغییراتی بر روی آنها ایجاد کنید.

در گذشته طبق شکل ۱۴-۳۹، با کلیک بر روی آیکون + می‌توانستیم یک گواهینامه‌ی امنیتی ایجاد کنیم، اما در آپدیت‌های نهایی این نرم‌افزار برای انجام این کار باید از دستورات Powershell استفاده کنیم.

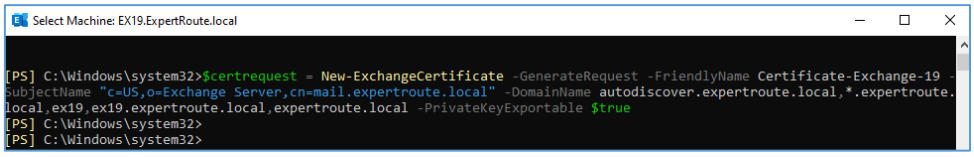


شکل ۱۴- ۳۹ تنظیم گواهینامه برای کاربران

دستور زیر را در نظر بگیرید:

```
$certrequest = New-ExchangeCertificate -GenerateRequest -FriendlyName Certificate-Exchange-19 -SubjectName "c=US,o=Exchange Server,cn=mail.expertroute.local" -DomainName autodiscover.expertroute.local,*.expertroute.local,ex19,ex19.expertroute.local,expertroute.local -PrivateKeyExportable $true
```

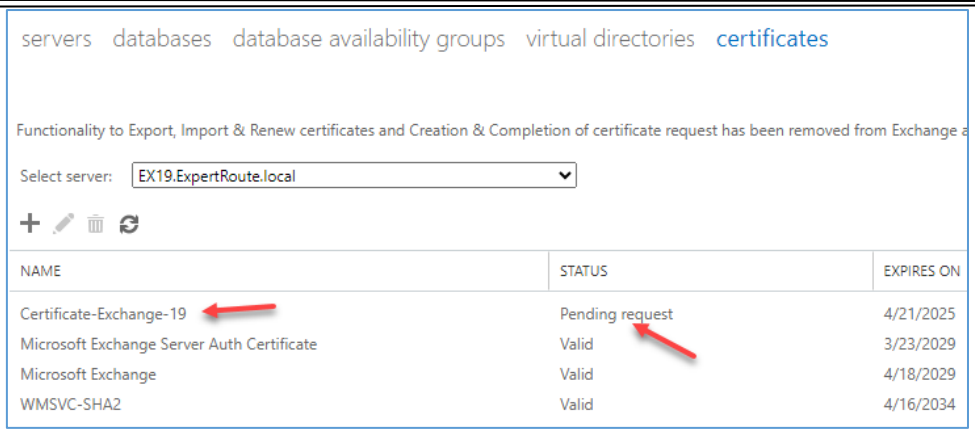
به مانند شکل ۱۴-۴۰، در دستور بالا باید دقت کنید تا اشتباهی انجام ندهید، به جای Certificate-Exchange-19 می‌توانید هر اسمی به دلخواه وارد کنید و این اسم همان اسم گواهینامه شما است، در قسمت SubjectName اطلاعات کشور و شهر خود را وارد کنید و در قسمت cn باید آدرس mail.expertroute.local را وارد کنید در ادامه کار و در مهمترین قسمت شما باید جلوی Domain تمام آدرس‌های مشخص شده را وارد کنید و فقط دومین خود را تغییر دهید.



شکل ۱۴- ۴۰ تنظیم گواهینامه برای کاربران

همان‌طور که در شکل ۱۴-۴۱، مشاهده می‌کنید بعد از اجرای دستور بالا یک Certificate جدید با نامی که وارد کردیم در Exchange ایجاد شده است ولی اگر به قسمت وضعیت (Status) توجه کنید گواهینامه‌ی جدید در حالت Pending Request قرار دارد و باید فعال شود.

www.takbook.com

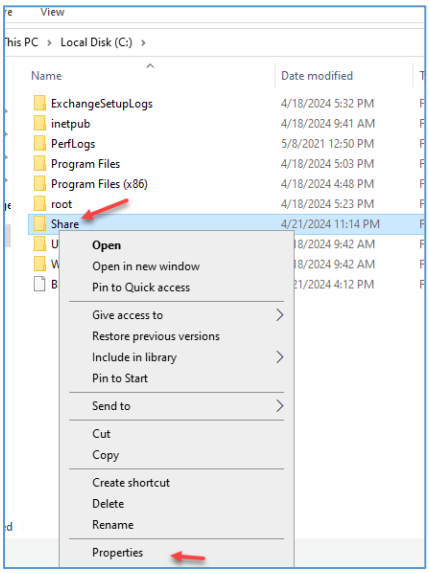


شکل ۱۴- ۴۱ تنظیم گواهینامه برای کاربران

برای فعال‌سازی این گواهینامه باید از آن یک خروجی بگیرید، برای این کار از دستور زیر برای خروجی گرفتن از این گواهینامه استفاده می‌کنیم.

قبل از اینکه از دستور مورد نظر استفاده کنیم باید یک پوشه در درایو C ایجاد و آن را برای کاربر Admin به اشتراک بگذارید تا بتوانیم فایل مورد نظر خود را در آن قرار دهیم.

به مانند شکل ۱۴-۴۲، یک پوشه جدید با نام Share ایجاد شده و با کلیک راست بر روی آن گزینه‌ی Properties را انتخاب کنید.



شکل ۱۴- ۴۲ تنظیم گواهینامه برای کاربران

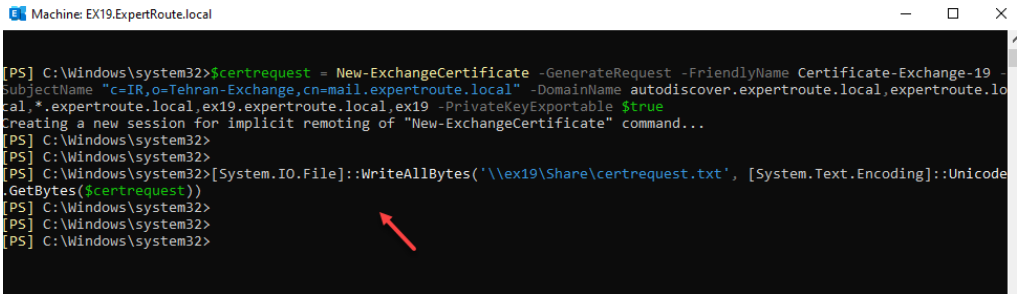
www.takbook.com

در تب Sharing بر روی Share کلیک کنید و در صفحه‌ی باز شده کاربر یا کاربران مورد نظر خود را به لیست اضافه کنید و بر روی Share کلیک کنید، به این ترتیب یک پوشه به اشتراک گذاری شده برای ادامه کار آماده شده است.

برای خروجی گرفتن از دستور زیر استفاده می‌کنیم، در این دستور به جای \\ex19\Share\certrequest.txt باید آدرس Share شده‌ی سرور خود را وارد کنید و certrequest.txt نام فایل است که اطلاعات گواهینامه در آن قرار می‌گیرد.

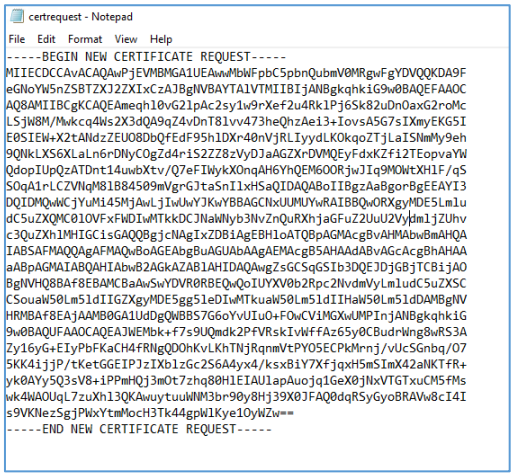
```
[System.IO.File]::WriteAllBytes('\\ex19\Share\certrequest.txt',
[System.Text.Encoding]::Unicode.GetBytes($certrequest))
```

همان‌طور که در شکل ۱۴-۴۳، مشاهده می‌کنید دستور مورد نظر به درستی اجرا شده است



شکل ۱۴- ۴۳ تنظیم گواهینامه برای کاربران

حالا اگر وارد پوشه مورد نظر شوید یک فایل به مانند شکل ۱۴-۴۴، مشاهده می‌کنید که باید آن را باز کنید و به طور کامل از آن کپی تهیه کنید تا آن را به سرور Certificate خود که همان سرور Active Directory است معرفی کنیم و از آن یک فایل خروجی تهیه کنیم.



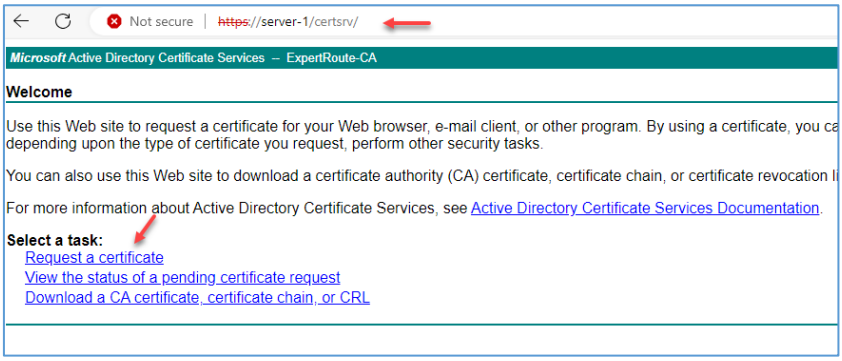
شکل ۱۴- ۴۴ گواهینامه داخلی

مرورگر خود را باز کنید و آدرس زیر را اجرا کنید:

www.takbook.com

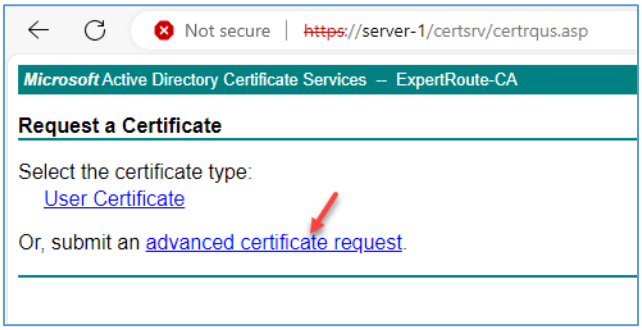
https://server-1/certsrv/

با اجرای این آدرس Microsoft Active Directory Certificate Services که قبلاً در درس‌های قبلی آن را بررسی کردیم باز خواهد شد و به مانند شکل ١٤-٤٥، باید بر روی Request a certificate کلیک کنید، توجه داشته باشید در آدرس بالا به جای Server-1 باید آدرس سرور Active خود را وارد کنید.



شکل ۱۴ - ۴۵ ایجاد گواهینامه برای سرور

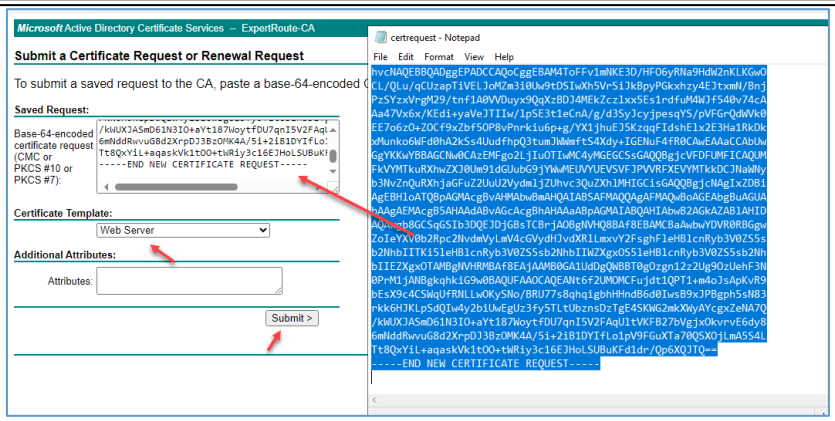
در شکل ١٤-٤٦، بر روی advanced certificate request کلیک کنید.



شکل ۱۴ - ۴۶ ایجاد گواهینامه برای سرور

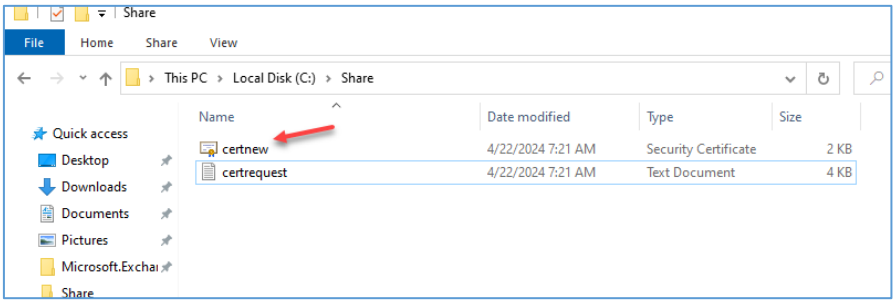
در شکل ١٤-٤٧، باید اطلاعات فایلی که با هم ایجاد کردیم را در این قسمت وارد کنید و در قسمت Certificate Template گزینه‌ی Web Server را انتخاب کنید.

www.takbook.com



شکل ۱۴ - ۴۷ / ایجاد گواهینامه برای سرور

بعد از کلیک بر روی Submit در صفحه‌ی بعد بر روی Download کلیک کنید و به مانند شکل ۱۴–۴۸، فایل دانلود شده را در پوشه Share قرار دهید.



شکل ۱۴ - ۴۸ / ایجاد گواهینامه برای سرور

حالا باید با استفاده از دستور زیر فایل نهایی را به Exchange معرفی کنیم تا گواهینامه مورد نظر فعال شود، در دستور زیر به جای قسمت مشخص شده باید آدرس سرور خودتون رو وارد کنید:

```
Import-ExchangeCertificate -FileData ([System.IO.File]::ReadAllBytes('\\ex19\Share\certnew.cer')) -PrivateKeyExportable:$true -Password (ConvertTo-SecureString -String 'EP@$*2024' -AsPlainText -Force)
```

همان‌طور که در شکل ۱۴–۴۹، مشاهده می‌کنید دستور زیر اجرا شده و گواهینامه مورد نظر فعال شده است.

www.takbook.com

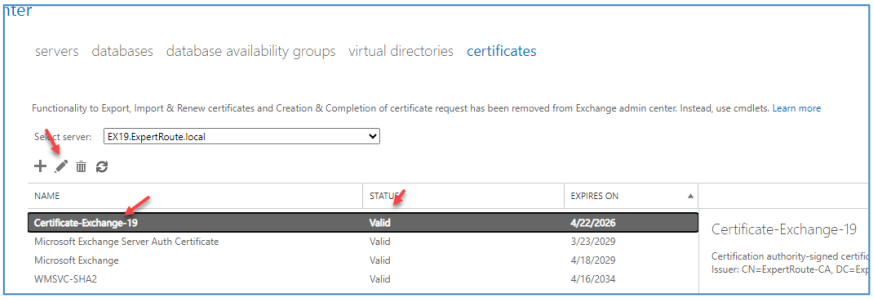

```
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>Import-ExchangeCertificate -FileData ([System.IO.File]::ReadAllBytes('\\ex19\Share\certnew.cer'
)) -PrivateKeyExportable:$true -Password (ConvertTo-SecureString -String 'EP@$*2024' -AsPlainText -Force)

Thumbprint                                Services   Subject
----------                                --------   -------
6CF17BDB68EE3FC05FDCDB4714AC81B369C4173A  IP.....    CN=mail.expertroute.local, O=Exchange Server, C=US


[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
```

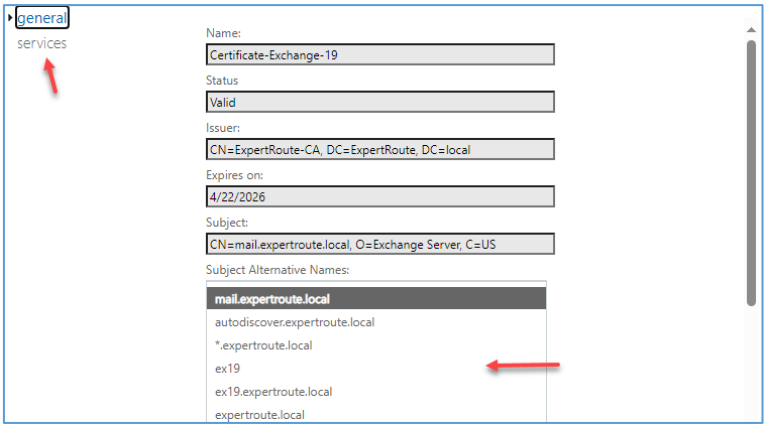
شکل ۱۴- ۴۹ ایجاد گواهینامه برای سرور

حالا اگر به مانند شکل ۱۴-۵۰، وارد صفحه‌ی مدیریتی Exchange شوید و در قسمت Certificate گواهینامه مورد نظر را مشاهده می‌کنید که قسمت Status آن به Valid تغییر کرده است.



شکل ۱۴- ۵۰ بررسی گواهینامه سرور

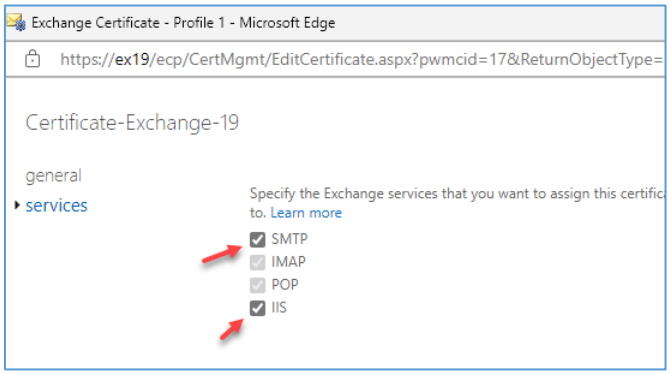
برای اینکه از این گواهینامه در کل سرور استفاده کنیم باید سرویس‌های مورد نظر را بر روی آن فعال کنیم، برای این کار بر روی گواهینامه مورد نظر دو بار کلیک کنید، به مانند شکل ۱۴-۵۱، در این صفحه اگر به قسمت Subject Alternative Name دقت کنید آدرس‌هایی که در دستورات وارد کردیم در این لیست قرار گرفتن و این برای فعال شدن گواهینامه خیلی مهم است، وارد تب Services شوید.



شکل ۱۴- ۵۱ بررسی گواهینامه سرور

www.takbook.com

در شکل ۱۴-۵۲، باید تیک همه‌ی سرویس‌های موجود را انتخاب کنید تا این گواهینامه به صورت کامل بر روی سرور فعال شود.

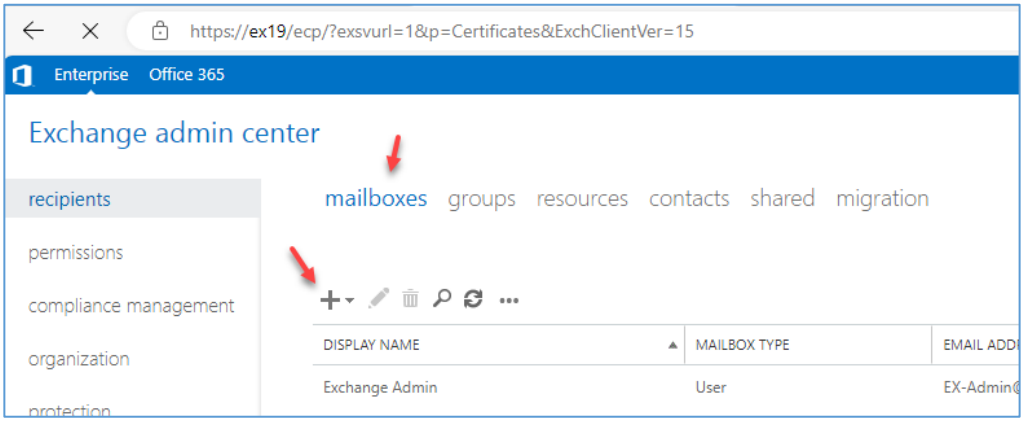


شکل ۱۴-۵۲ فعال‌سازی سرویس بر روی گواهینامه

بعد از تعریف گواهینامه در سرور Exchange، تمام کلاینت‌ها به صورت اتوماتیک، این گواهینامه را دریافت می‌کنند!؛ بله، اگر کلاینتی در شبکه‌ی شما عضو دومین باشد، به خاطر اینکه به دومین متّصل شده است، پس سرور دومین گواهینامه‌های خود را به کلاینت‌های خود می‌دهد تا در شبکه معتبر باشند.

۱۴-۸ تعریف کاربر در Exchange

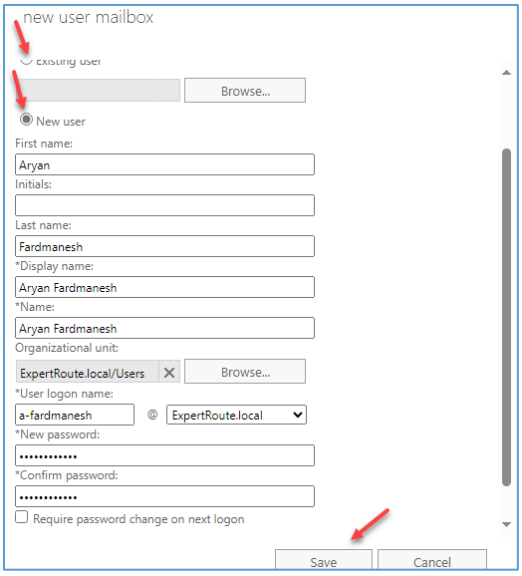
بعد از اینکه همه چیز برای تست نهایی حاضر شد باید کاربران خود را به لیست Exchange اضافه و برای آنها ایمیل تعریف کنیم، برای این کار به مانند شکل ۱۴-۵۳، در صفحه‌ی مدیریتی از قسمت Recipients بر روی تب Mailboxes کلیک کنید، در این صفحه یک کاربر به صورت پیش‌فرض وجود دارد و این کاربر همان کاربر Admin است که با آن نرم‌افزار را نصب و تنظیم کردیم، برای اینکه کاربر جدید ایجاد کنیم باید بر روی آیکون + کلیک کنید و گزینه‌ی User mailbox را انتخاب کنید.



شکل ۱۴-۵۳ تعریف کاربر در Exchange

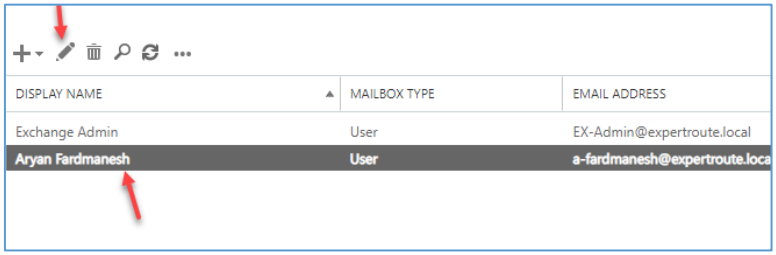
www.takbook.com

در شکل ۱۴-۵۴، دو قسمت وجود دارد یکی اینکه اگر از قبل کاربری در Active Directory تعریف کرده باشید می‌توانید گزینه‌ی Existing user را انتخاب کنید و با کلیک بر روی Browse کاربر را به لیست اضافه کنید و اگر هم به مانند شکل می‌خواهید یک کاربر جدید ایجاد کنید که هم در Active directory و هم در Exchange فعال شود باید گزینه‌ی New user را انتخاب کنید و اطلاعات کاربر مورد نظر را وارد کنید و بر روی Save کلیک کنید اگر تیک گزینه‌ی Require password change on next logon را انتخاب کنید کاربر مورد نظر بعد از ورود می‌تواند رمز عبور خود را تغییر دهد.



شکل ۱۴- ۵۴ تعریف کاربر

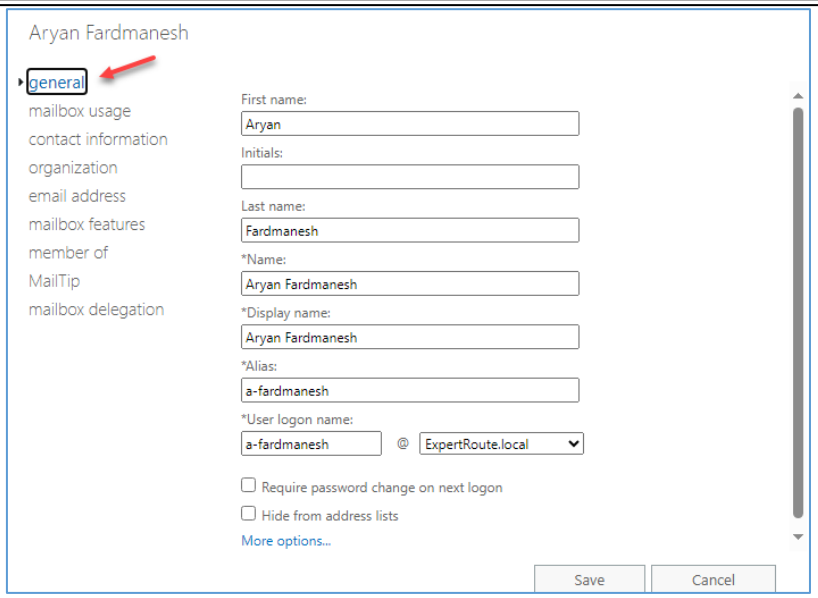
به مانند شکل ۱۴-۵۵، بعد از ایجاد کاربر مورد نظر بر روی آن دو بار کلیک کنید تا اطلاعات داخل آن را هم بررسی کنیم.



شکل ۱۴- ۵۵ تعریف کاربر

به مانند شکل ۱۴-۵۶، اگر وارد تب General شوید می‌توانید اطلاعات کاربر مورد نظر را مانند نام، نام خانوادگی، نام کاربری و .... را تغییر دهید.

www.takbook.com

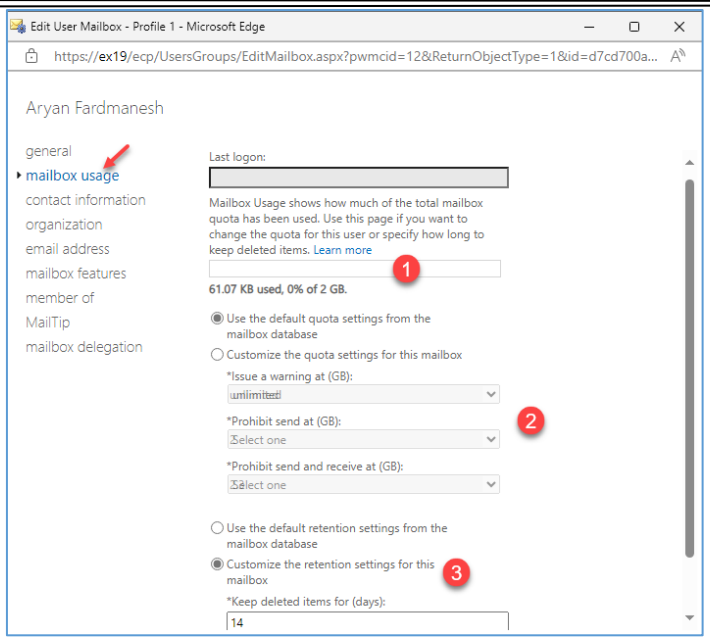


شکل ۱۴ - ۵۶ بررسی کاربر در *Exchange*

به مانند شکل ۱۲–۵۷، در تب Mailbox usage می‌توانید مشاهده کنید که چه مقدار فضا به کاربر مورد نظر تخصیص داده شده است، که به صورت پیش‌فرض ۲ گیگابایت تخصیص داده شده است که در قسمت شماره‌ی یک مشخص شده است، ولی اگر بخواهید این مقدار را تغییر دهید باید در قسمت شماره‌ی دو گزینه‌ی Customize را انتخاب کنید و مقدار فضای مورد نظر خود را وارد کنید و یا اینکه گزینه‌ی Ultimate را انتخاب کنید تا مقدار فضای کاربر بی‌نهایت شود.

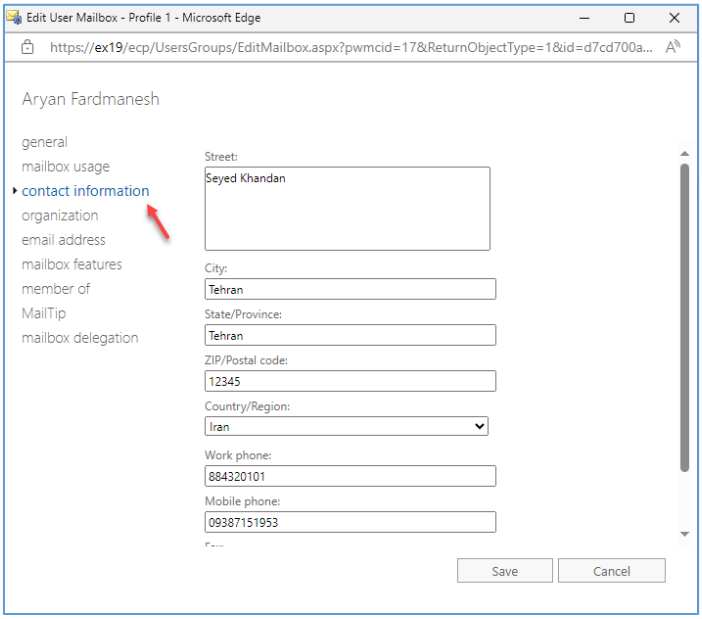
به بیان دیگر عدد قسمت Prohibit send and… را که برای ارسال ایمیل است را تغییر داده و یا اینکه برای دریافت و ارسال ایمیل، عدد Porhibit send and receive را تغییر داد؛ عددی که در قسمت issue a warning مشاهده می‌کنید، مقدار فضایی است که اگر کاربر به این سقف برسد، اخطار ارسال خواهد شد؛ در قسمت آخر هم که عدد ۱٤ نوشته شده است به این نکته اشاره دارد که اطّلاعات حذف شده توسط کاربر تا حداکثر ۱٤ روز در سرور نگهداری می‌شود و بعد از آن به طور کامل حذف خواهد شد که این عدد هم قابل تغییر است.

www.takbook.com



شکل ۱۴ - ۵۷ بررسی کاربر در Exchange

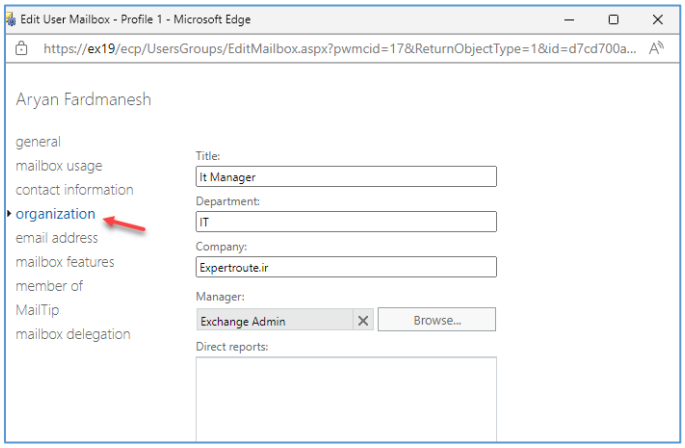
به مانند شکل ۱٤–۵۸، در قسمت contact information باید اطلاعات تکمیلی کاربر را وارد کنید، توجه کنید تغییراتی که در این قسمت وارد می‌کنید در Active Directory هم به صورت اتوماتیک ثبت خواهد شد.



شکل ۱۴ - ۵۸ بررسی کاربر در Exchange

www.takbook.com

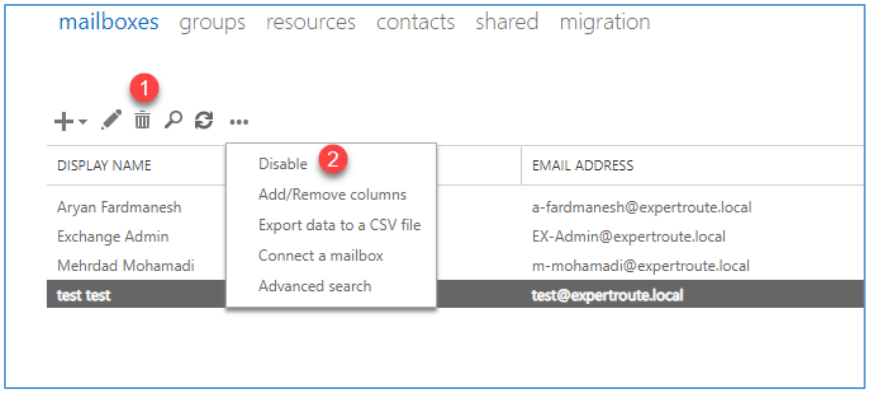
به مانند شکل ۱٤-۵۹، در قسمت organization باید اطلاعات تکمیلی مانند مدیر کاربر، قسمتی که کار می‌کند و ... را وارد کنید.



شکل ۱۴- ۵۹ بررسی کاربر در Exchange

نکته‌ی بسیار مهم

یکی از مشکلاتی که همه‌ی مدیران شبکه و از جمله شما، هنگامی‌که برای اوّلین بار با این نرم‌افزار کار می‌کنید، این است که اگر زمانی بخواهید یک کاربر را از لیست ایمیل‌ها حذف کنید، به مانند شکل ۱٤-٦۰، یک آیکون سطل زباله (شماره‌ی یک) مشاهده می‌کنید که اگر چنانچه بر روی این آیکون کلیک کنید و در صفحه‌ی باز شده بر روی Yes کلیک کنید، کاربر شما به طور کامل هم از این لیست و هم از Active Directory شما حذف خواهد شد، پس مواظب باشید که اگر می‌خواهید کاربری را از این لیست حذف کنید در کنار آن یک خط ... سه تا نقطه مشاهده می‌کنید که با کلیک بر روی آن (شماره‌ی دو) یک منو باز می‌شود و بعد، شما می‌توانید گزینه‌ی disable را انتخاب کنید تا کاربر فقط و فقط از لیست حذف شود و نه از Active directory حذف نشود، پس مواظب باشید.

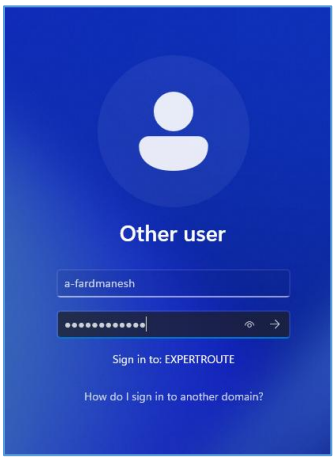


شکل ۱۴- ۶۰ حذف کاربر در Exchange

www.takbook.com

۱٤-۹ متصل شدن از طریق Outlook

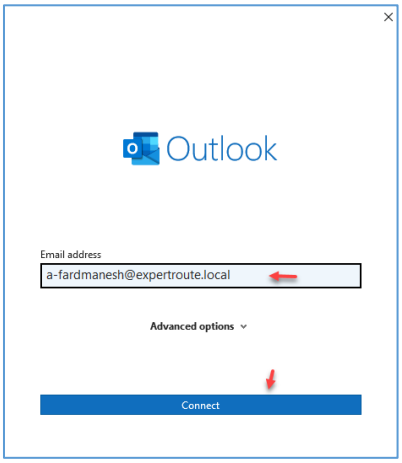
برای اینکه از طریق Outlook به سرور Exchange متصل شویم نیاز به یک کلاینت داریم که عضو شبکه باشد و این کار را قبلاً در بخش‌های قبلی کتاب انجام دادیم، بعد از اجرای کلاینت مورد نظر با کاربر جدیدی که ایجاد کردیم (a-fardmanesh) به مانند شکل ۱٤-٦۱، وارد سرور شوید.



شکل ۱۴- ۶۱ ورود به کلاینت

بعد از ورود، نرم‌افزار Outlook را اجرا کنید، توجه داشته باشید که باید نرم‌افزار آفیس را قبلاً نصب کرده باشید.

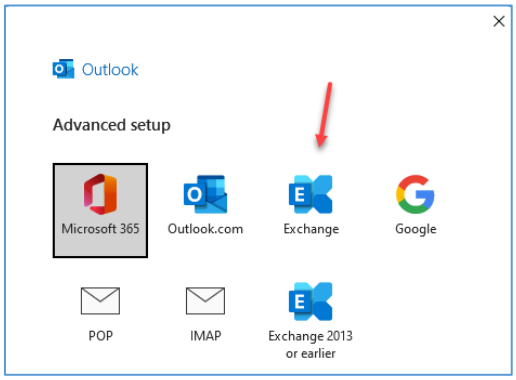
بعد از اجرای نرم‌افزار Outlook به صورت پیش‌فرض به مانند شکل ۱٤-٦۲، نام کاربری شما را که از طریق Active وارد شدید به صورت اتوماتیک شناسایی می‌کند و فقط بر روی Connect کلیک کنید.



شکل ۱۴- ۶۲ متصل شدن به Exchange

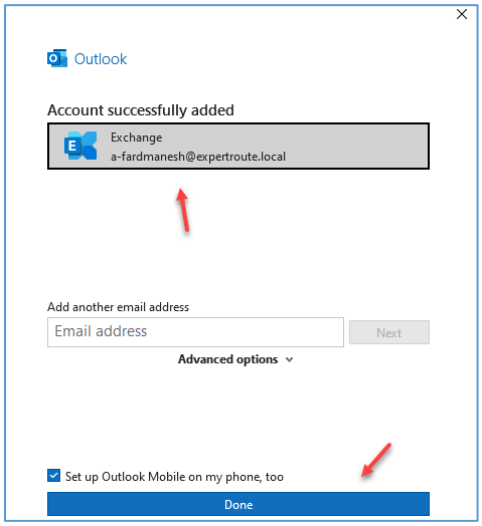
www.takbook.com

در شکل ۱۴-۶۳، چند گزینه به شما نمایش داده می‌شود و شما باید گزینه‌ی Exchange را انتخاب کنید، اما اگر ورژن Exchange شما قبل از 2013 است باید گزینه‌ی Exchange 2013 را انتخاب کنید.



شکل ۱۴- ۶۳ تنظیم اتلوک برای ارتباط

همان‌طور که در شکل ۱۴-۶۴، مشاهده می‌کنید عملیات با موفقیت انجام شده است، اگر می‌خواهید عملیات بر روی موبایل هم انجام دهید باید تیک گزینه‌ی آخر را انتخاب کنید، وگرنه نیازی به این کار نیست.



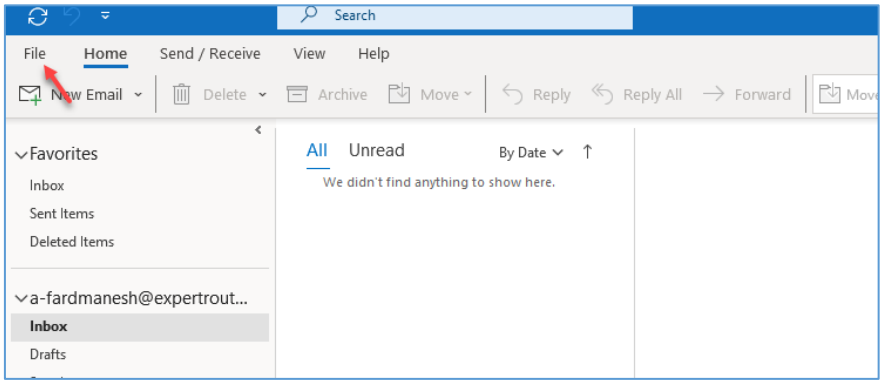
شکل ۱۴- ۶۴ تنظیم اتلوک برای ارتباط

نکته مهم

زمانی که از طریق Exchange به ایمیل خود متصل می‌شوید هیچ دیتابیسی در سیستم کاربر ایجاد نخواهد شد و تمام اطلاعات در سرور موجود است که همین موضوع باعث ایجاد امنیت بیشتر برای ایمیل‌ها خواهد بود و به این نکته اشاره دارد که باید فضای ذخیره‌سازی سرور Exchange بیشتر باشد.

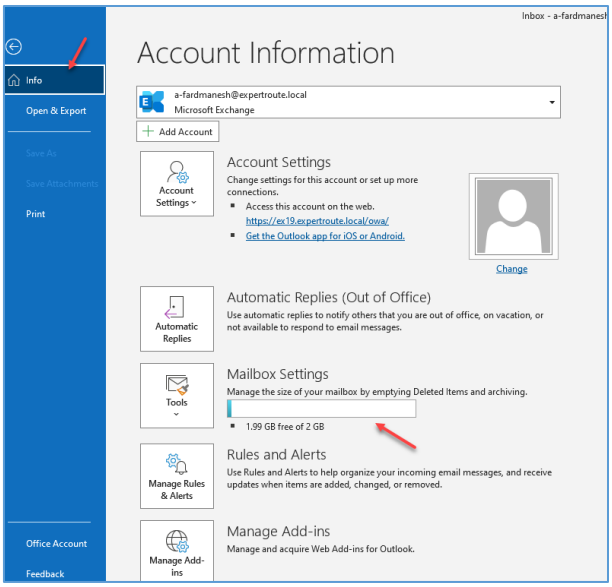
www.takbook.com

در شکل ١٤-٦٥، وارد ایمیل مورد نظر شدیم و می‌توانیم کار خود را آغاز کنیم، برای بررسی بیشتر بر روی File کلیک کنید.



شکل ۱۴ - ۶۵ تنظیم اتلوک برای ارتباط

همان‌طور که در شکل ١٤-٦٦، مشاهده می‌کنید مقدار فضای در نظر گرفته برای کاربر مورد نظر ۲ گیگابایت است که قبلاً این مورد را بررسی کردیم.

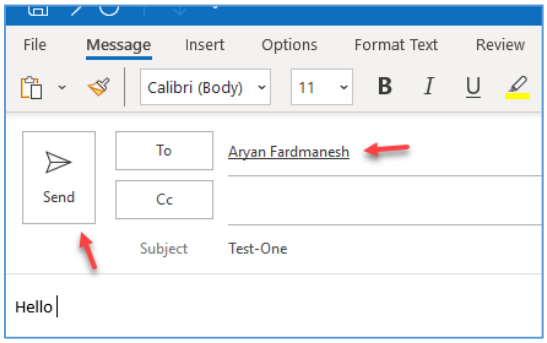


شکل ۱۴ - ۶۶ تنظیم اتلوک برای ارتباط

برای اینکه یک ایمیل تستی ارسال کنیم باید به مانند شکل ١٤-٦٧، بر روی New Email کلیک کنیم و در شکل باز شده و در قسمت To می‌توانیم آدرس ایمیل مورد نظر خود را وارد و یا اینکه بر روی To کلیک

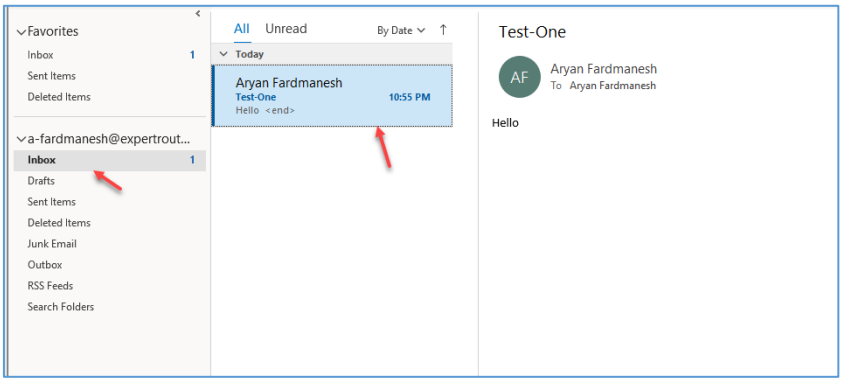
www.takbook.com

کنید و گزینه‌ی مورد نظر خود را با دو بار کلیک کردن انتخاب کنید و بر روی OK کلیک کنید، در شکل هم عنوان و متن ایمیل را وارد و بر روی Send کلیک کنید.



شکل ۱۴ - ۶۷ ارسال ایمیل تستی

همان‌طور که در شکل ١٤-٦٨، مشاهده می‌کنید ایمیل مورد نظر به درستی ارسال شده و به مخاطب رسیده، البته در این قسمت مخاطب را خود کاربر قرار دادیم که این موضوع برای نمایش سریع اطلاعات بود ولی شما می‌توانید به هر کاربری آن را ارسال کنید.



شکل ۱۴ - ۶۸ دریافت ایمیل

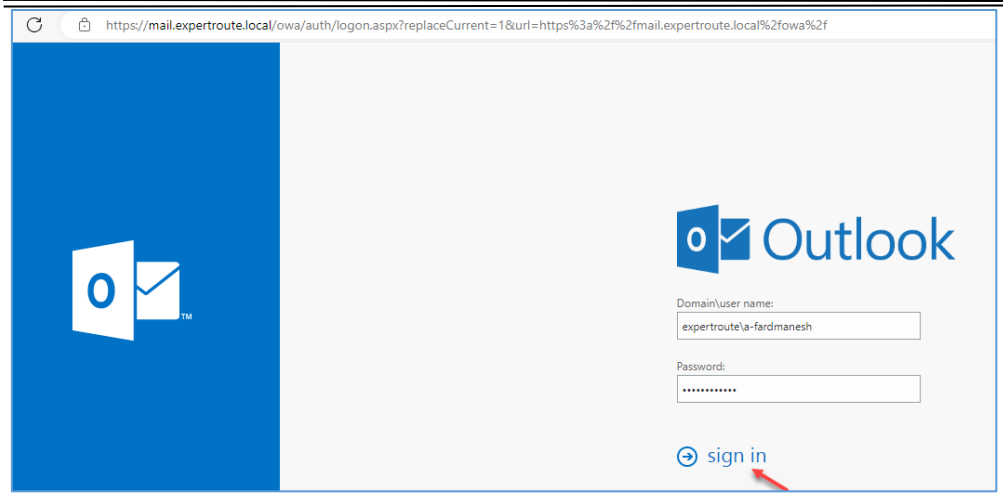
١٤-١٠ بررسی Outlook تحت وب

روش دیگری هم وجود دارد که می‌توانید از طریق آن به ایمیل خود متصل شوید که آن هم از طریق اتلوک تحت وب است که آدرس آن به صورت زیر می‌باشد، در این آدرس به جای دومین باید دومین خود را وارد کنید.

https://mail.expertroute.local/owa/

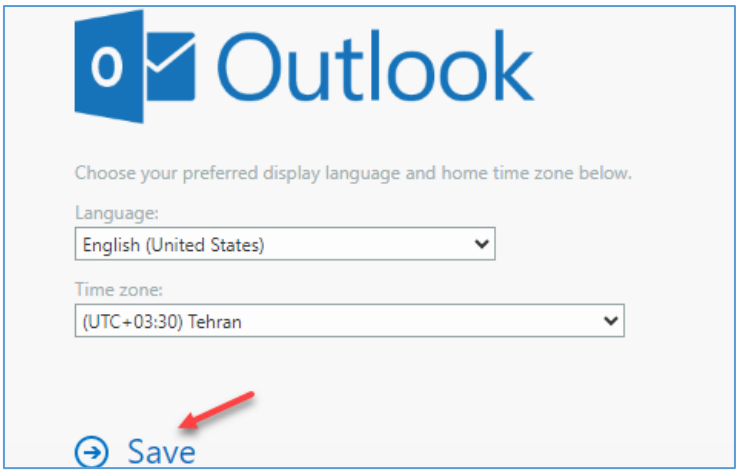
شکل ١٤-٦٩، صفحه‌ی اتلوک تحت وب است که باید نام کاربری را به صورت Domain\user وارد کنید که در شکل مشخص شده است.

www.takbook.com



شکل ۱۴- ۶۹ بررسی Outlook تحت وب

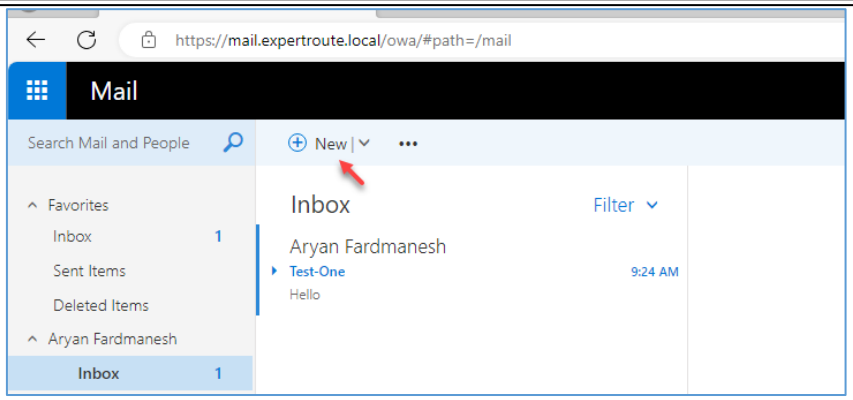
در شکل ۱٤-۷۰، هم باید منطقه زمانی و زبان مورد نظر خود را انتخاب کنید و بر روی Save کلیک کنید.



شکل ۱۴- ۷۰ بررسی Outlook تحت وب

همان‌طور که در شکل ۱٤-۷۱، مشاهده می‌کنید ایمیل قبلی که با هم ارسال کردیم در Inbox وجود دارد و شما می‌توانید با کلیک بر روی New ایمیل جدید اراسل کنید.

www.takbook.com

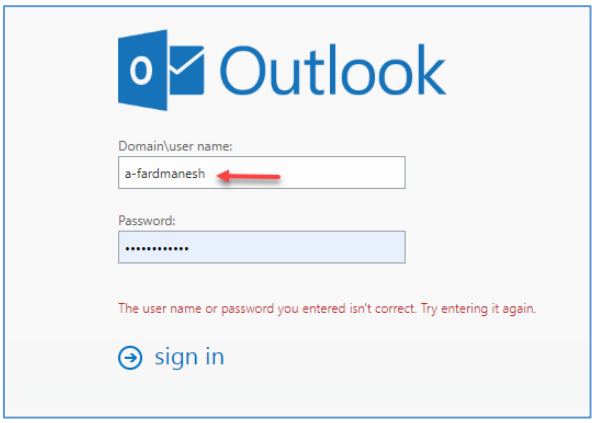


شکل ۱۴- ۷۱ بررسی Outlook تحت وب

۱۱-۱٤ تغییر روش ورود کاربران به Outlook تحت وب

در این قسمت می‌خواهیم روش ورود کاربران به قسمت تحت وب Outlook را تغییر دهیم، به این صورت که دیگر نیاز نباشد کاربر قبل از نام کاربری خود، حتماً نام دومین را وارد کند وتنها با وارد کردن نام کاربری خود وارد ایمیل خود شود.

همان‌طور که در شکل ۱٤-۷۲، مشاهده می‌کنید، کاربر مورد نظر نمی‌تواند با نام کاربری a-fardmanesh وارد ایمیل خود شود و حتماً باید نام دومین را به همراه نام کاربری وارد کند، یعنی به صورت expertroute\ a-fardmanesh.

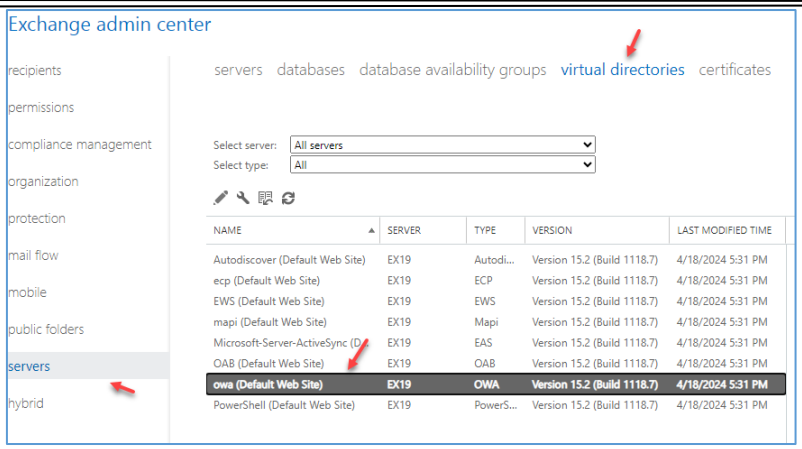


شکل ۱۴- ۷۲ ورود کاربران به Outlook تحت وب

برای اینکه هر دو حالت را فعّال کنیم، وارد قسمت مدیریّتی Exchange 2019 می‌شویم.

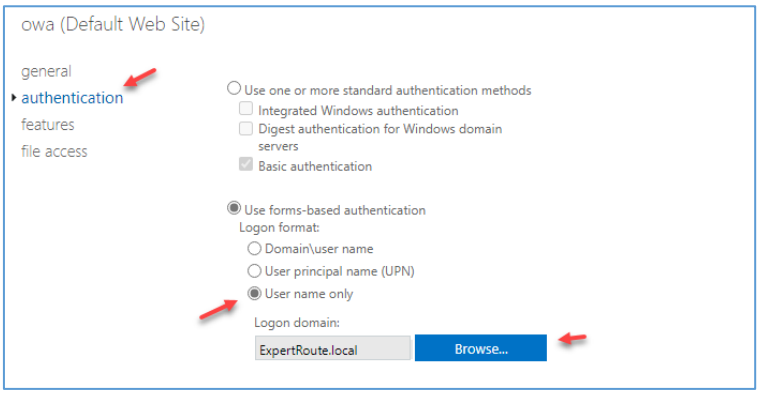
به مانند شکل ۱٤-۷۳، در صفحه مدیریّت از سمت چپ بر روی Server کلیک کنید و در صفحه‌ی باز شده بر روی تب virtual directories کلیک کنید و از لیست مورد نظر گزینه‌ی OWA را انتخاب و بر روی دکمه‌ی ویرایش کلیک کنید، یا دو بار بر روی گزینه‌ی OWA کلیک کنید.

www.takbook.com



شکل ۱۴- ۷۳ ورود کاربران به Outlook تحت وب

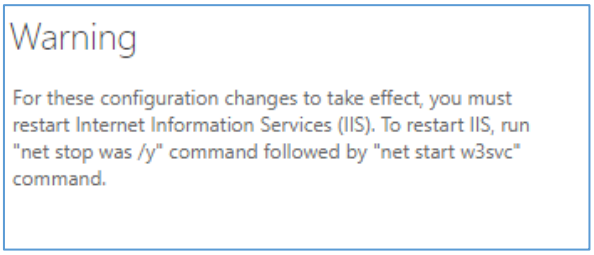
در شکل ۱٤-۷٤، از سمت چپ بر روی authentication کلیک کنید و در صفحه‌ی باز شده، گزینه‌ی Use forms-based authentication را انتخاب کنید که سه گزینه‌ی دیگر، زیر مجموعه‌ی آن هستند که گزینه‌ی اوّل، یعنی Domain\user name، همان روشی است که همه‌ی کاربران در حال حاضر با وارد کردن نام دومین، قبل از نام کاربری وارد ایمیل خود می‌شوند، گزینه‌ی User principal name (UPN) که اگر این گزینه را انتخاب کنید، باید نام کاربری خود را به صورت User@domain.com وارد کنید که در این قسمت باید به جای domain.com، نام کامل دومین خود را وارد کنید و به جای USER، نام کاربری خود را وارد نمایید. این روش، راه معمولی است که کاربران ایمیل‌های عمومی، مانند Gmail و Yahoo از آن استفاده می‌کنند؛ گزینه‌ی آخر هم User name only است که با انتخاب آن باید با کلیک بر روی Browse، نام دومین مورد نظر خود را انتخاب کنید و بر روی Save کلیک کنید.



شکل ۱۴- ۷۴ تغییر روش ورود کاربر

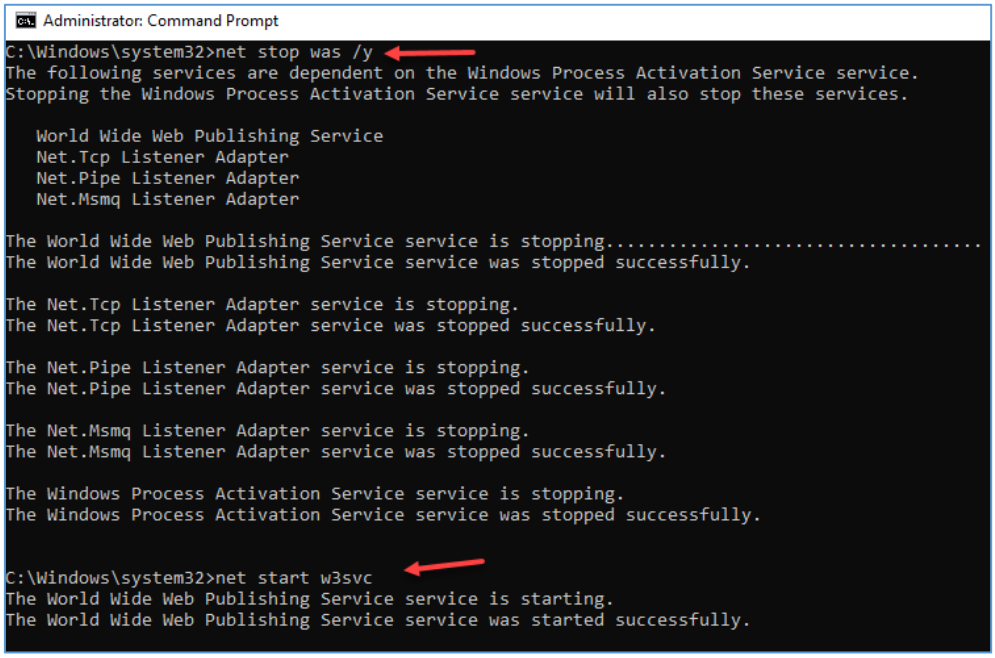
www.takbook.com

با انجام کار قبلی، پیغام اخطار شکل ۱۴-۷۵، زیر نمایان می‌شود، و اعلام می‌دارد که اگر چنانچه مایلید این تنظیماتی که انجام دادید بر روی سرور اعمال شود، باید دستورات net stop was /y و در ادامه دستور net start w3svc را اجرا کنید.



شکل ۱۴- ۷۵ تغییر روش ورود کاربر

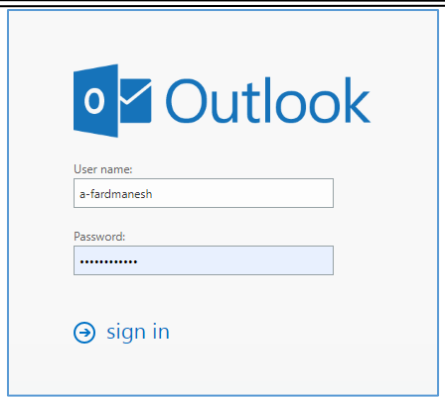
همان‌طور که در شکل ۱۴-۷۶، مشاهده می‌کنید سرویس‌های مورد نظر Stop و دوباره اجرا شده‌اند تا تنظیمات مورد نظر اعمال شود.



شکل ۱۴- ۷۶ اجرای دوباره سرویس

با انجام این کار، کاربران می‌توانند با نام کاربری خود وارد ایمیل شوند که این موضوع را در شکل ۱۴-۷۷، مشاهده می‌کنید.

www.takbook.com



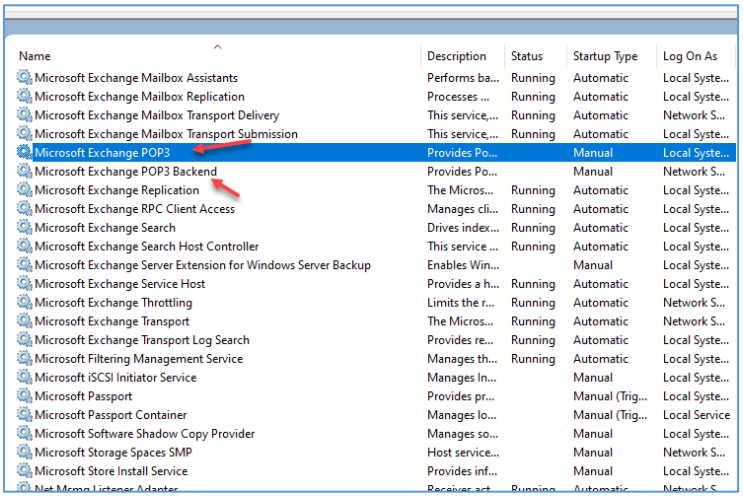
شکل ۱۴- ۷۷ ورود کاربر

۱۴-۱۲ متصل شدن از طریق سرویس POP3

در بعضی مواقع نیاز است که از طریق پروتکل‌های دیگری به سرور ایمیل متصل شویم، برای همین پروتکل POP3 که از پروتکل‌های قدیمی است وجود دارد که با هم این پروتکل را راه‌اندازی می‌کنیم.

برای شروع کار باید وارد سرور Exchange شوید و Services را از طریق Start اجرا کنید که شکل ۱۴-۷۸، ظاهر می‌شود.

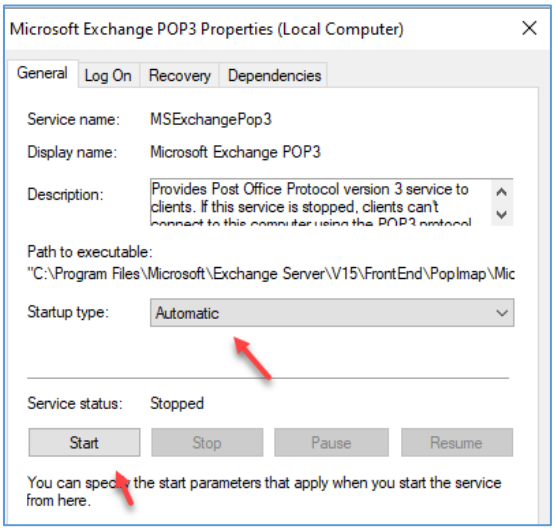
در شکل ۱۴-۷۸، اگر به سرویس‌های Exchange دقت کنید سرویس POP3 را مشاهده می‌کنید که Start نشده است و در حالت Manual قرار دارد که باید بر روی آن دو بار کلیک کنید، این کار را دقیقاً برای سرویس POP3 Backend هم انجام دهید.



شکل ۱۴- ۷۸ متصل شدن از طریق سرویس POP3

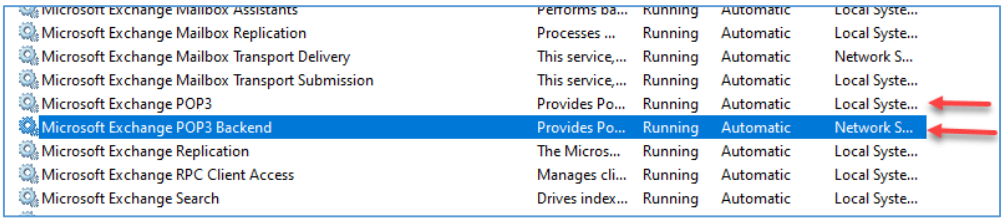
www.takbook.com

در شکل ۱۴-۷۹، در قسمت Startup type گزینه‌ی Automatic را انتخاب کنید و در آخر بر روی Start کلیک کنید، دقیقاً همین کار را برای POP3 Backend انجام دهید.



شکل ۱۴- ۷۹ تغییر در سرویس POP3

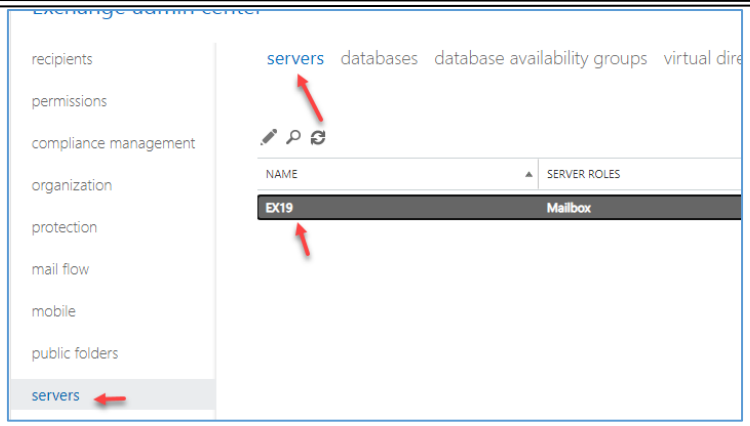
همان‌طور که در شکل ۱۴-۸۰، مشاهده می‌کنید هر دو سرویس در حالت Automatic قرار گرفته و فعال شدند.



شکل ۱۴- ۸۰ اجرای سرویس POP3

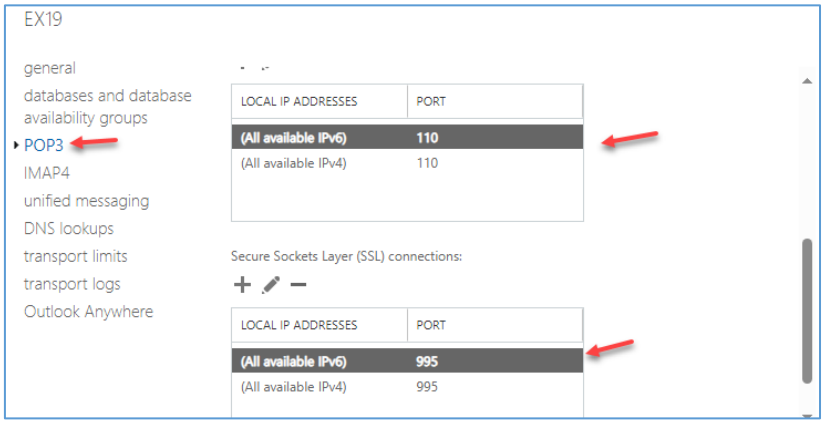
بعد از انجام مراحل قبل به مانند شکل ۱۴-۸۱، وارد صفحه مدیریتی شوید و از قسمت Servers بر روی نام سرور دو بار کلیک کنید.

www.takbook.com



شکل ۱۴- ۸۱ بررسی سرویس POP3

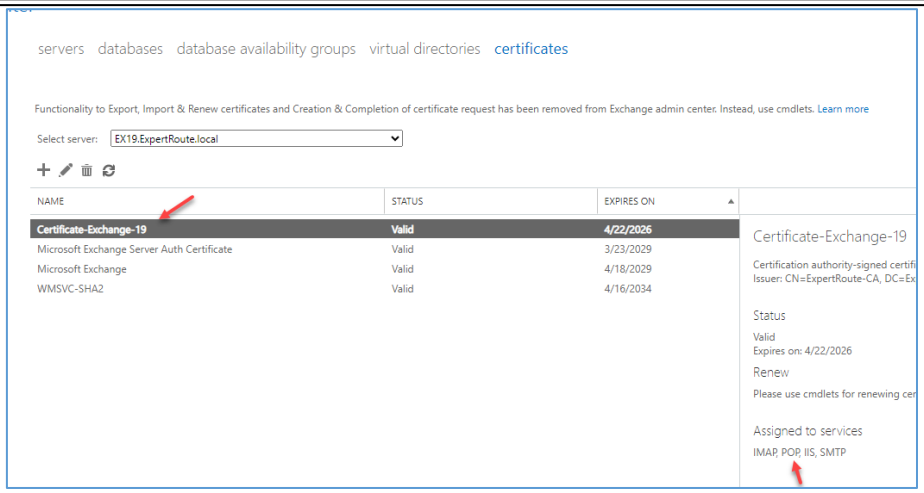
در شکل ۱۴-۸۲، از قسمت POP3 می‌توانید پورت‌های متصل شدن به این سرویس را مشاهده کنید که پورت 110 یک پورت عمومی و از نظر امنیتی ضعیف است و پورت ۹۹۵ یک پورت با امنیت بالا است که از گواهینامه‌ی امنیتی استفاده می‌کند که در قسمت‌های قبل ایجاد کردیم.



شکل ۱۴- ۸۲ بررسی سرویس POP3

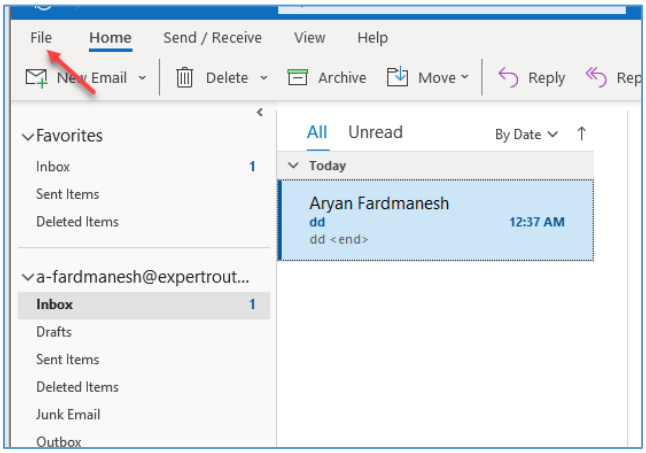
در ادامه اگر یک نگاهی به گذشته بندازیم و در قسمت Certificate، گواهینامه‌ای که با هم ایجاد کردیم را بررسی کنیم، به مانند شکل ۱۴-۸۳، متوجه خواهید شد که گواهینامه‌ی مورد نظر برای سرویس POP فعال شده است.

www.takbook.com



شکل ۱۴-۸۳ بررسی سرویس POP3

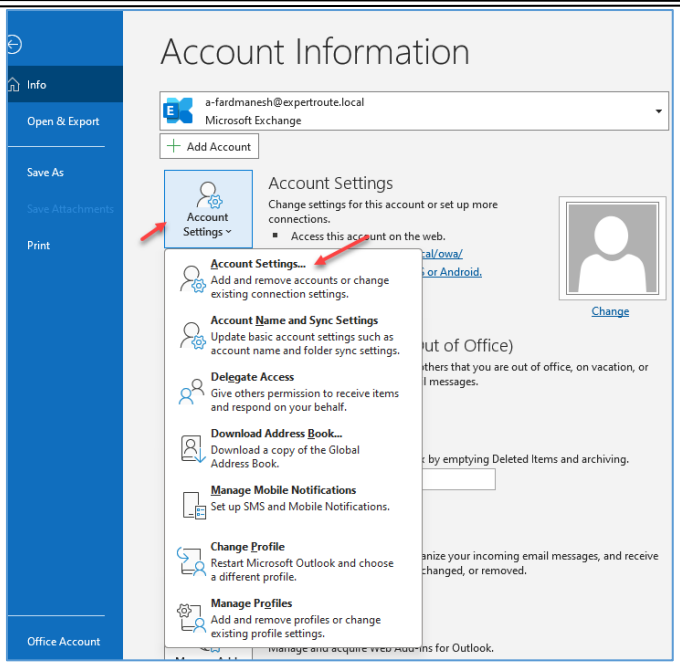
در ادامه باید وارد کلاینت شویم و این سرویس را برای کاربر مورد نظر فعال کنیم، برای این کار باید وارد Outlook شویم و تنظیمات را انجام دهیم، قبلاً با کاربر A-Fardmanesh به Outlook متصل شدیم برای همین برای اینکه یک اکانت جدید اضافه کنیم به مانند شکل ۱۴-۸۴، بر روی File کلیک کنید.



شکل ۱۴-۸۴ بررسی سرویس POP3

در شکل ۱۴-۸۵، بر روی Account Settings کلیک کنید.

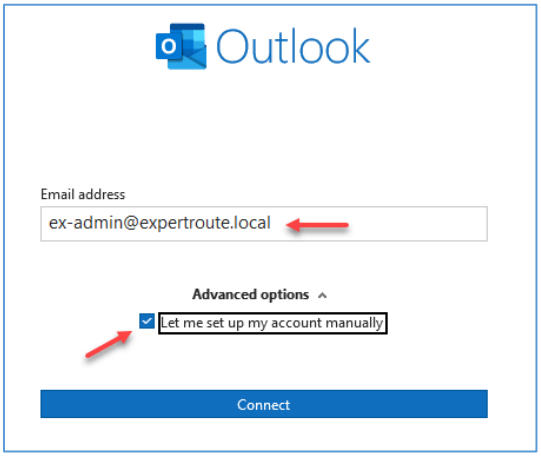
www.takbook.com



شکل ۱۴- ۸۵ بررسی سرویس POP3

همان‌طور که در شکل ۱٤-۸٦، مشاهده می‌کنید یک اکانت در لیست قرار دارد که در تب Type مشخص کرده است که این اکانت از نوع Microsoft Exchange است که در قسمت قبل تنظیم کردیم، برای اینکه این سرویس را فعال کنیم بر روی New کلیک کنید.

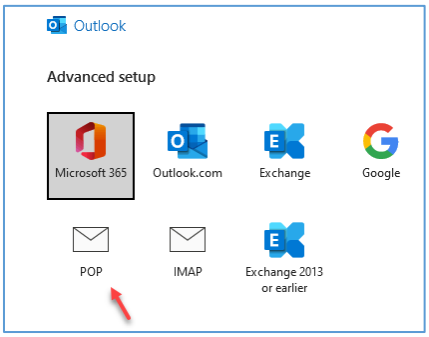
به مانند شکل ۱٤-۸٦، باید آدرس کاربر مورد نظر را وارد کنید و برای اینکه تنظیمات را به صورت دستی انجام دهید تیک گزینه‌ی مورد نظر را انتخاب و بر روی Connect کلیک کنید.



شکل ۱۴- ۸۶ بررسی سرویس POP3

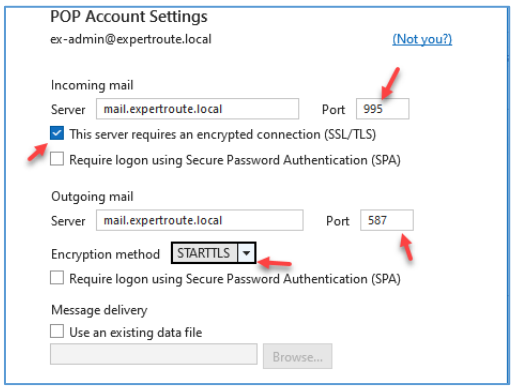
www.takbook.com

در شکل ۱۴-۸۷، گزینه‌ی POP را انتخاب کنید.



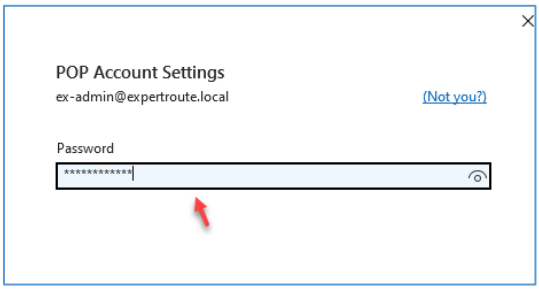
شکل ۱۴- ۸۷ بررسی سرویس POP3

در شکل ۱۴-۸۸، در قسمت Incoming آدرس سرور Email خود را وارد کنید و در قسمت پورت عدد ۹۹۵ را وارد کنید، در زیر آن تیک گزینه‌ی SSL/TLS را انتخاب کنید، در ادامه و در قسمت Outgoing آدرس سرور را وارد و پورت ۵۸۷ را وارد کنید و در قسمت Encryption method گزینه‌ی مورد نظر را انتخاب کنید.



شکل ۱۴- ۸۸ تنظیم دسترسی در اتلوک

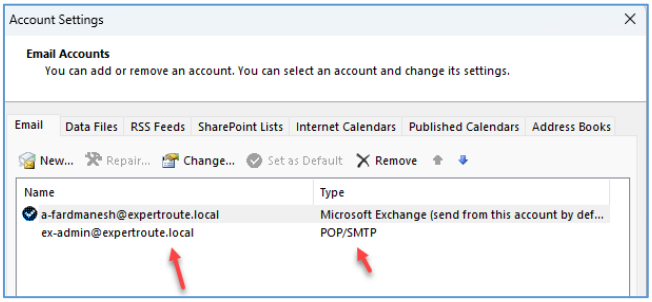
در ادامه به مانند شکل ۱۴-۸۹، رمز عبور کاربر مورد نظر را وارد کنید.



شکل ۱۴- ۸۹ تنظیم دسترسی در اتلوک

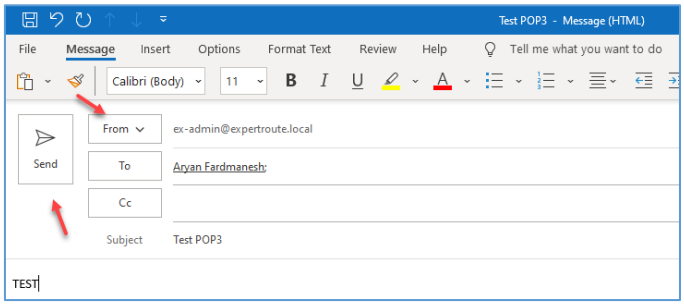
www.takbook.com

همان‌طور که در شکل ۱۴–۹۰، مشاهده می‌کنید، ایمیل مورد نظر از نوع PoP به لیست اضافه شده است.



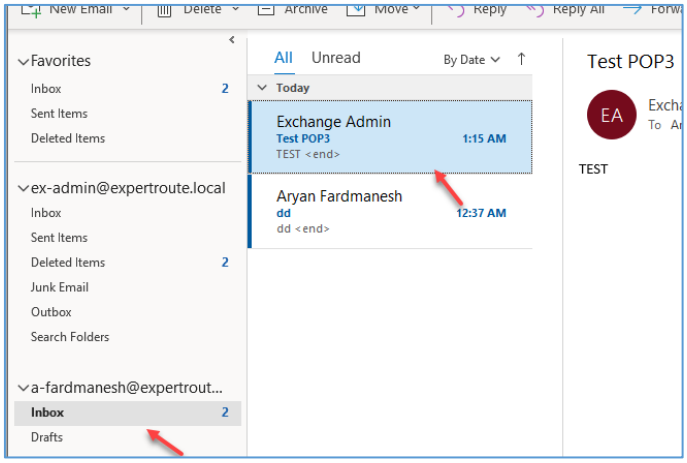
شکل ۱۴- ۹۰ تنظیم دسترسی در اتلوک

برای اینکه ایمیل ارسال کنیم به مانند شکل ۱۴–۹۱، باید از قسمت From آدرس ایمیل جدید که اضافه کردیم را انتخاب کنید و ایمیل خود را برای کاربر مورد نظر ارسال کنید.



شکل ۱۴- ۹۱ ارسال ایمیل در اتلوک

همان‌طور که در شکل ۱۴–۹۲، مشاهده می‌کنید ایمیل مورد نظر به دست کاربر رسیده است و این نشان می‌دهد که پروتکل مورد نظر به درستی کار می‌کند.



شکل ۱۴- ۹۲ ارسال ایمیل در اتلوک

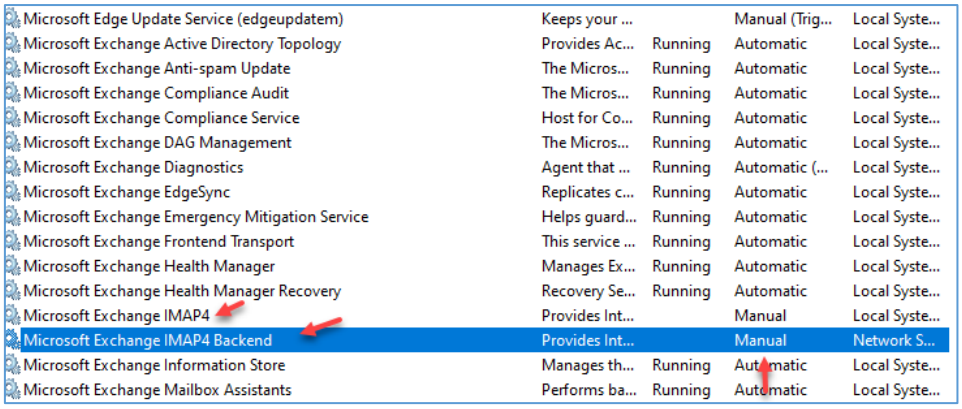
www.takbook.com

نکته‌ی مهمی که در این ارتباط وجود دارد این است که دیتابیس در این حالت بر روی سیستم کاربر کپی می‌شود و باید به این نکته خوب توجه کنید که اگر این دیتابیس پاک شود دیگر ایمیل‌ها در دسترس نیست، منظور از ایمیل‌ها ایمیل‌هایی هست که از طریق این روش ارسال می‌شوند.

۱۳-۱٤ متصل شدن از طریق سرویس IMAP

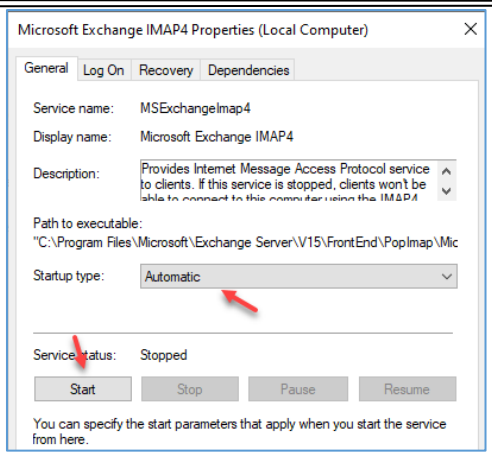
یکی دیگر از پروتکل‌های ایمیل، IMAP است که این نوع پروتکل طرف سرور است یعنی اینکه تمام اطلاعات کاربران در سمت سرور است و هیچ گونه فایلی در کلاینت ذخیره نخواهد شد، یعنی کاربر برای مشاهده ایمیل خود حتماً باید از طریق سرور عمل کند و سرور هم باید در دسترس باشد، در روش Exchange از پروتکل (Messaging Application Programming Interface) **MAPI** استفاده می‌شود اما در این روش از پروتکل عمومی IMAP.

برای شروع به مانند شکل ۱٤-۹۳، وارد Services در سرور Exchange شوید، طبق شکل دو سرویس IMAP را مشاهده می‌کنید که باید به مانند شکل ۱٤-۹٤، آنها را در حالت Automatic قرار دهید و Start کنید.



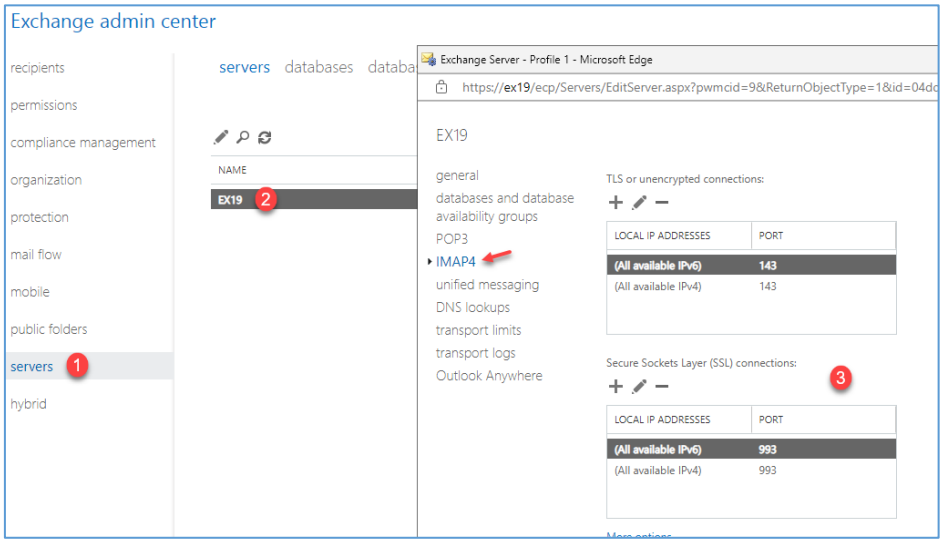
شکل ۱۴- ۹۳ سرویس IMAP

www.takbook.com



شکل ۱۴- ۹۴ سرویس IMAP

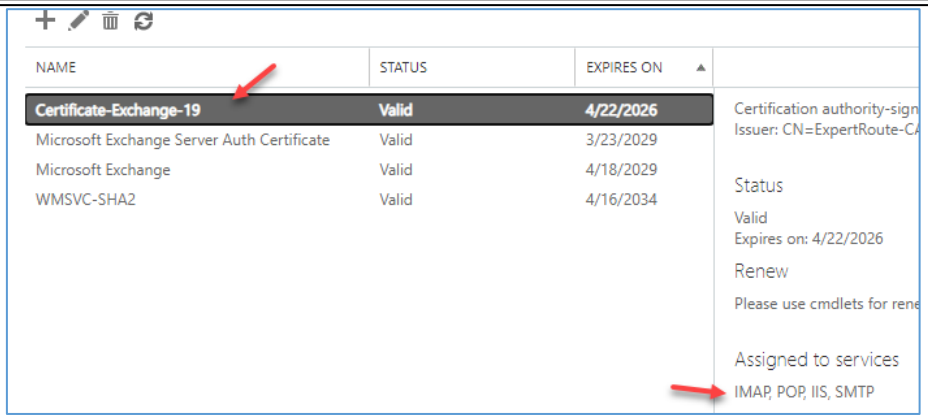
اگر به مانند شکل ۱۴-۹۵، در صفحه مدیریتی وارد Servers شوید و بر روی نام سرور دو بار کلیک کنید، به مانند شکل در قسمت IMAP4 می‌توانید پورت‌های این سرویس را مشاهده کنید که ۱۴۳ پورت عادی و امنیت پایین است و پورت ۹۹۳ پورت با امنیت بالا است.



شکل ۱۴- ۹۵ سرویس IMAP

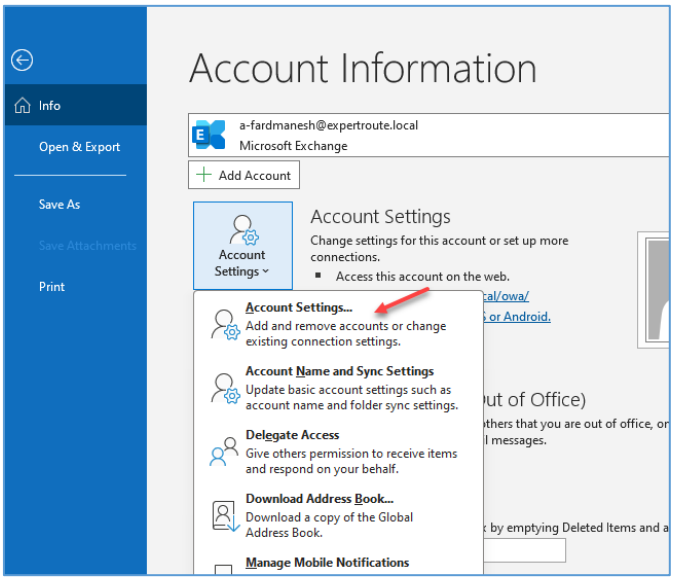
همان‌طور که بیان کردیم در قسمت گواهینامه هم باید سرویس IMAP بر روی گواهینامه فعال شده باشد که در شکل ۱۴-۹۶، این موضوع مشخص شده است.

www.takbook.com



شکل ۱۴- ۹۶ سرویس IMAP

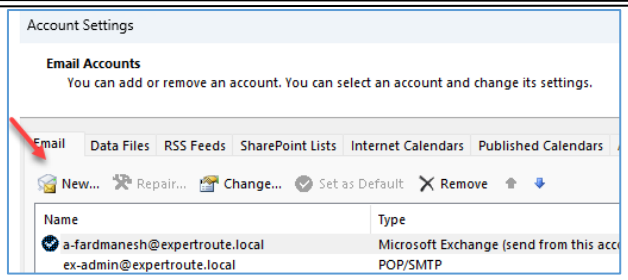
برای تست این پروتکل وارد کلاینت می‌شویم و به مانند شکل ۱۴-۹۷، برای ایجاد اکانت جدید در اتلوک بر روی Account Settings کلیک کنید.



شکل ۱۴- ۹۷تنظیم سرویس IMAP در اتلوک

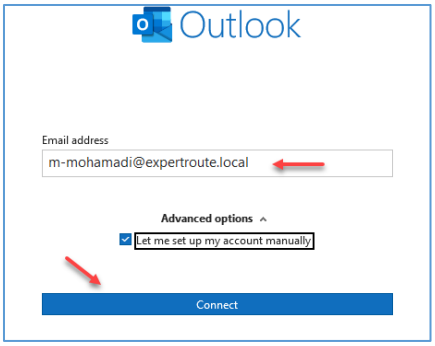
در شکل ۱۴-۹۸، بر روی New کلیک کنید تا اکانت جدید به لیست اضافه کنیم.

www.takbook.com



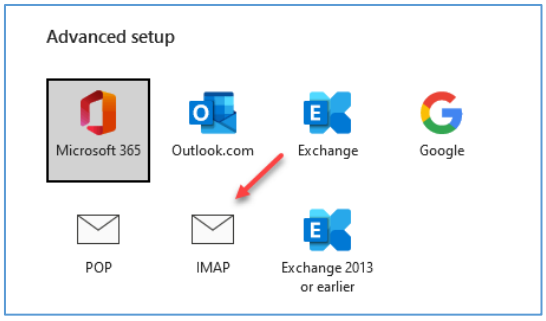
شکل ۱۴- ۹۸ تنظیم سرویس IMAP در اتلوک

در شکل ۱۴-۹۹، نام کاربری خود را وارد و تیک گزینه‌ی مورد نظر را انتخاب می‌کنیم.



شکل ۱۴- ۹۹ تنظیم سرویس IMAP در اتلوک

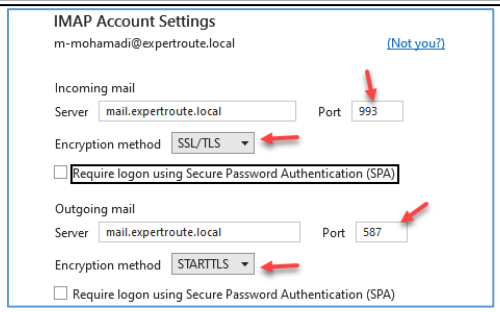
در شکل ۱۴-۱۰۰، گزینه‌ی IMAP را انتخاب کنید.



شکل ۱۴- ۱۰۰ تنظیم سرویس IMAP در اتلوک

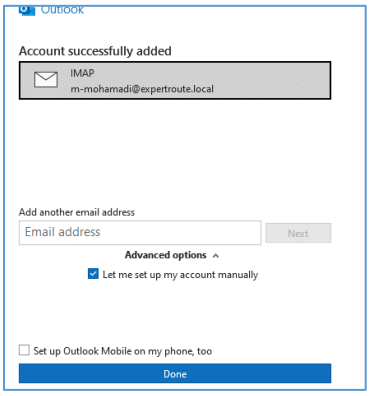
در شکل ۱۴-۱۰۱، نام سرور را در Incoming و هم در Outgoing وارد کنید و برای Incoming پورت 993 را وارد کنید و گزینه‌ی SSL/TLS را انتخاب کنید، و برای Outgoing هم پورت 587 به همراه STARTTLS را انتخاب کنید.

www.takbook.com



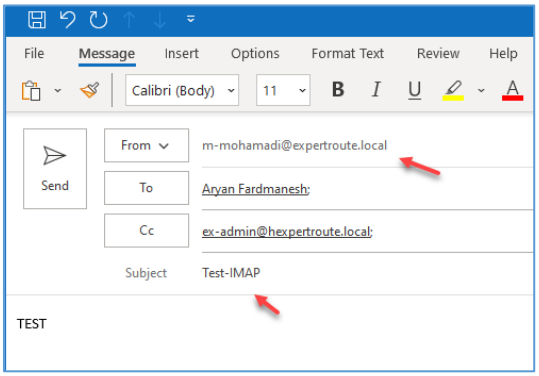
شکل ۱۴- ۱۰۱ متصل شدن به سرویس IMAP

همان‌طور که در شکل ۱۴-۱۰۲، مشاهده می‌کنید، اکانت مورد نظر با استفاده از IMAP به لیست اضافه شده است.



شکل ۱۴- ۱۰۲ متصل شدن به سرویس IMAP

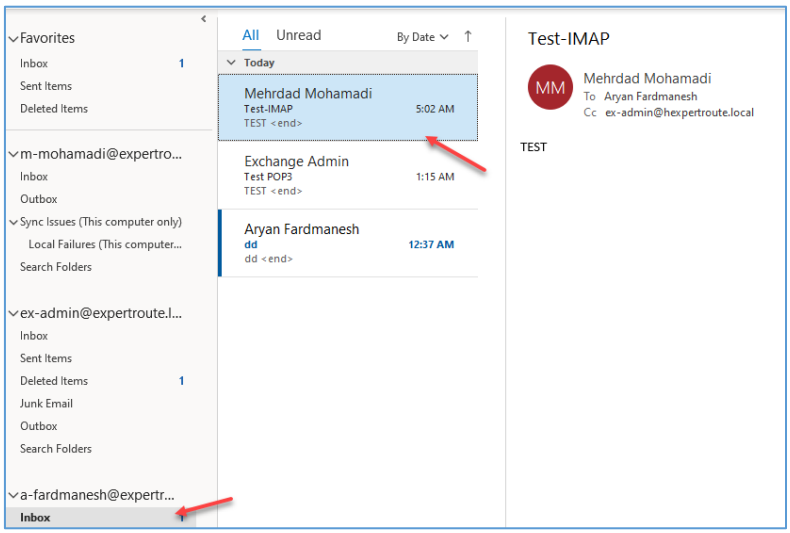
به مانند شکل ۱۴-۱۰۳، بعد از ایجاد حساب از طریق همان حساب یک ایمیل به کاربر دیگر ازسال می‌کنیم و آن را تست می‌گیریم.



شکل ۱۴- ۱۰۳ ارسال ایمیل

www.takbook.com

همان‌طور که در شکل ۱۴-۱۰۴،مشاهده می‌کنید ایمیل مورد نظر به کاربر ارسال شده است.



شکل ۱۴-۱۰۴ دریافت ایمیل IMAP

۱۴-۱۴ ایجاد گروه در Exchange 2019

در همه سازمان‌ها و شرکت‌ها گروه‌های مختلفی در حال کار می‌باشند که هر کدام از این گروه‌ها دارای چندین عضو هستند، شاید بخواهید برای همه کاربران آن گروه یک ایمیل اطلاع‌رسانی ارسال کنید، برای این کار باید گروه ایجاد کنید که با هم این موضوع را بررسی می‌کنیم.

سه نوع گروه در Exchange وجود دارد که به صورت زیر می‌باشد:

1- Destribution Group
2- Security Group
3- Dynamic destribution Group

گروه‌های Security توانایی دریافت Permisions را دارا می‌باشند و اینکه مقدار Load سرور Active Directory برای گروه‌های Security بالاتر است و آن هم به خاطر بررسی Authentication است.

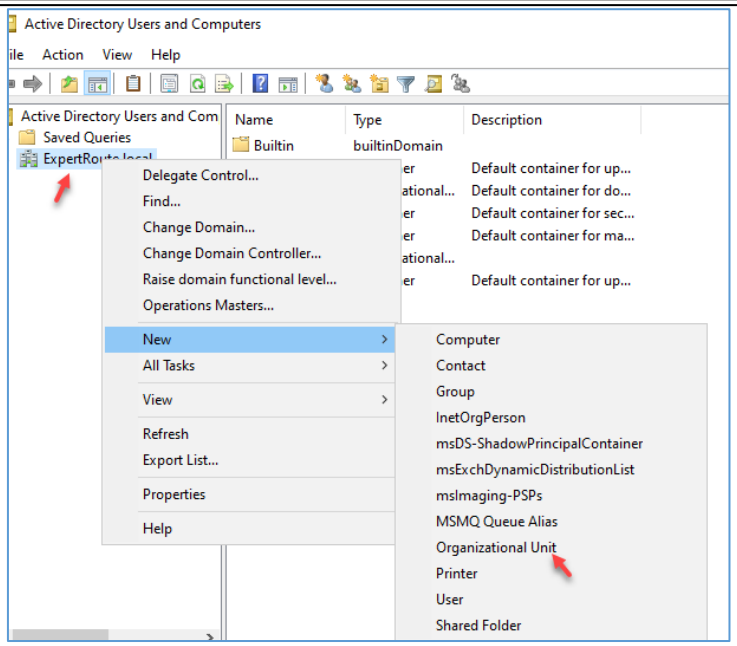
Mailbox -enable یعنی کاربر ایمیل دارد.

Mail-enable یعنی کاربر فقط آدرس ایمیل دارد و نه MailBox.

قبل از هر کاری برای گروه‌هایی که می‌خواهیم ایجاد کنیم در Active Directory یک OU ایجاد می‌کنیم تا این گروه‌ها را در آن قرا دهیم.

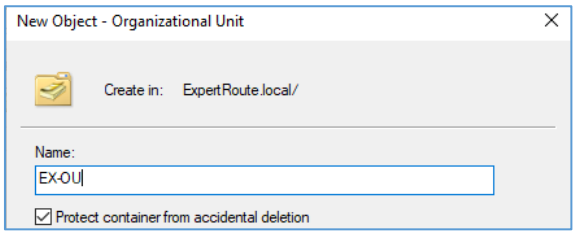
برای انجام این کار سرویس Active directory Users and Computers را اجرا کنید و به مانند شکل ۱۴-۱۰۵، گزینه‌ی Organizational Unit را اجرا کنید.

www.takbook.com



شکل ۱۴- ۱۰۵ ایجاد گروه در Exchange 2019

نام EX-OU را برای آن وارد می‌کنیم.



شکل ۱۴- ۱۰۶ ایجاد گروه در Exchange 2019

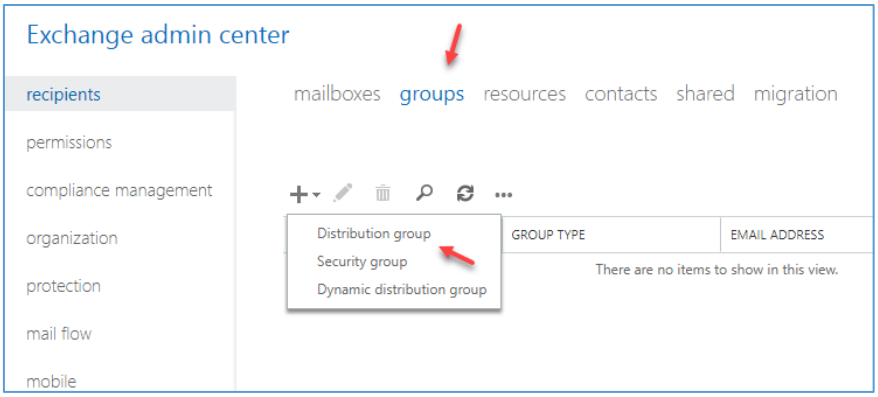
در ادامه کار می‌خواهیم گروه مورد نظر خود را ایجاد کنیم، توجه داشته باشید گروه‌هایی که در این قسمت ایجاد می‌کنید به صورت اتوماتیک در Active هم ایجاد خواهند شد. برای شروع به مانند شکل ۱۴-۱۰۷، وارد قسمت مدیریّتی Exchange شوید و از سمت چپ بر روی Recipients کلیک کنید و در صفحه باز شده وارد تب Group شوید و بر روی علامت + کلیک کنید و گزینه Distribution group را انتخاب کنید. توجه داشته باشید سه گروه در این قسمت وجود دارد:

۱- گروه Distribution Group برای توزیع ایمیل‌ها به گروهی از کاربران استفاده می‌شود و اعضای گروه فقط ایمیل دریافت می‌کنند.

۲- گروه Security Group علاوه بر ارسال ایمیل، می‌توان از آن برای مدیریت دسترسی‌ها به منابع (مانند فایل‌ها و فولدرها) استفاده کرد.

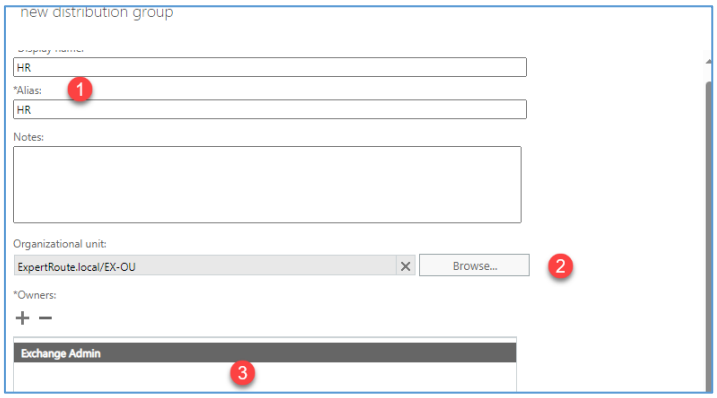
www.takbook.com

۳- Dynamic Distribution Group در این گروه‌ها اعضای آن‌ها به‌صورت پویا و براساس فیلترها (مانند موقعیت مکانی، عنوان شغلی) مشخص می‌شوند.



شکل ۱۴ - ۱۰۷ / ایجاد گروه در ایکسچنج

در شکل ۱٤-۱۰۸، در قسمت Name نام گروه خود را وارد کنید (فارسی یا انگلیسی) و در قسمت Alias یک اسم به انگلیسی برای این گروه وارد کنید، به این علت انگلیسی وارد می‌کنیم که این اسم به عنوان نام ایمیل این گروه در نظر گرفته خواهد شد یعنی در شکل ۱٤-۱۰۸، اگر کسی بخواهد برای گروه HR ایمیلی ارسال کند باید به آدرس HR@expertroute.local ارسال کند، در قسمت Owners می‌توانید مدیر گروه را با کلیک بر روی + به لیست اضافه کنید که البته به صورت پیش‌فرض کاربر ex-admin در لیست وجود دارد، بعد از انجام این کار صفحه را به پایین اسکرول کنید.



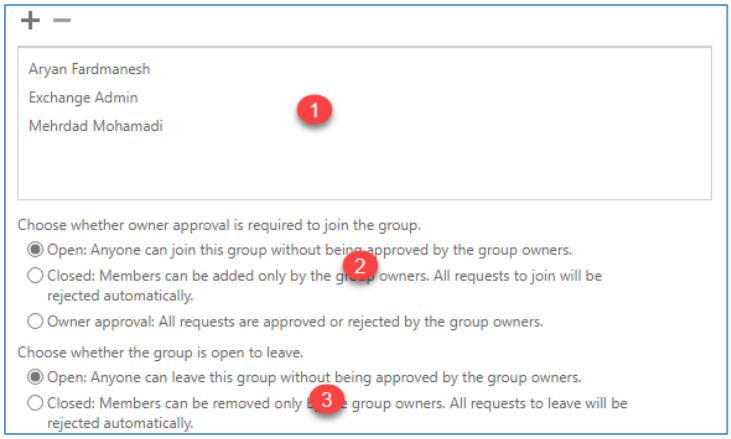
شکل ۱۴ - ۱۰۸ / ایجاد گروه در ایکسچنج

در پایین صفحه و در قسمت Add Members کاربران خود را عضو این گروه کنید که این کار را در شکل ۱٤-۱۰۹، مشاهده می‌کنید ، در قسمت شماره‌ی دو با انتخاب گزینه‌ی اول یعنی گزینه‌ی Open: Anyone

www.takbook.com

can join this group without being approved by the group owners می‌توانید مشخّص کنید که هر کسی می‌تواند عضو گروه شود یا اینکه با انتخاب گزینه‌ی دوم یعنی Closed: Members can be added only by the group owners. All requests to join will be rejected automatically بعد از ایجاد گروه بسته باشد و کسی نتواند عضو آن شود و در در آخر با انتخاب Owner approval: All requests are approved or rejected by the group owners کاربران برای عضویت در گروه باید درخواست خودشان را ارسال کنند و بعد از تایید مدیریت، کاربر مورد نظر می‌تواند عضو آن گروه شود، در حال حاضر گزینه اوّل را انتخاب کنید و بر روی Save کلیک کنید.

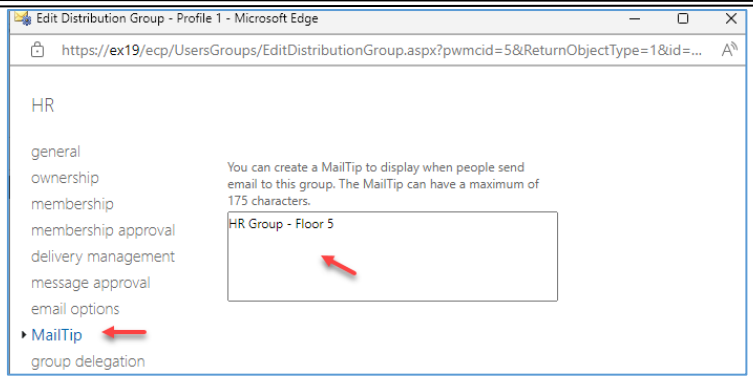
در قسمت شماره‌ی سه مشخص می‌کنید که کاربرانی که عضو این گروه می‌شوند آیا اجازه دارند از گروه خارج شوند یا نه.



شکل ۱۴ - ۱۰۹ / ایجاد گروه در ایکسچنج

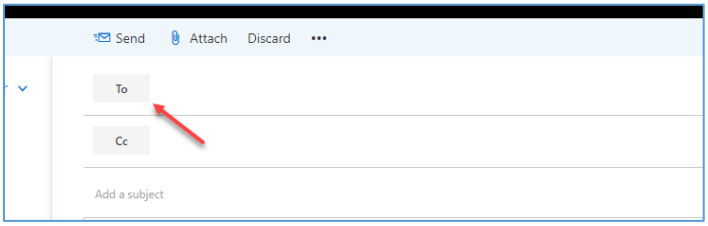
بعد از ایجاد گروه بر روی آن دوبار کلیک کنید تا صفحه شکل ۱۴-۱۱۰، ظاهر شود، گزینه‌های مختلفی وجود دارد که با بیشتر آن در زمان ایجاد گروه آشنا هستید، گزینه‌ای با نام MailTip در این قسمت وجود دارد که می‌توانید توضیحاتی را در مورد این گروه وارد کنید که کاربر در زمان ارسال ایمیل آن را مشاهده کند، پس توضیحاتی را در این قسمت وارد می‌کنیم و بر روی Save کلیک می‌کنیم.

www.takbook.com



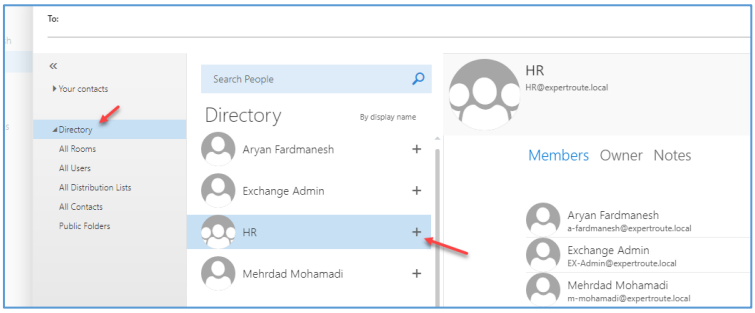
شکل ۱۴- ۱۱۰ ایجاد گروه در ایکسچنج

به مانند شکل ۱۴-۱۱۱، وارد ایمیل تحت وب شوید و در قسمت ارسال ایمیل بر روی گزینه‌ی TO کلیک کنید.



شکل ۱۴- ۱۱۱ ارسال ایمیل به گروه مورد نظر

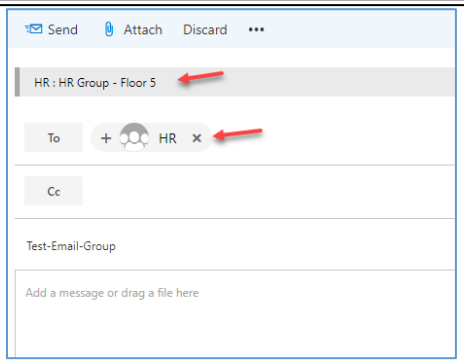
به مانند شکل ۱۴-۱۱۲، از سمت چپ بر روی Directory کلیک کنید که گروه مورد نظر را مشاهده می‌کند و اعضای آن هم مشخص شده است، بر روی + کلیک کنید تا به لیست اضافه شود.



شکل ۱۴- ۱۱۲ ارسال ایمیل به گروه مورد نظر

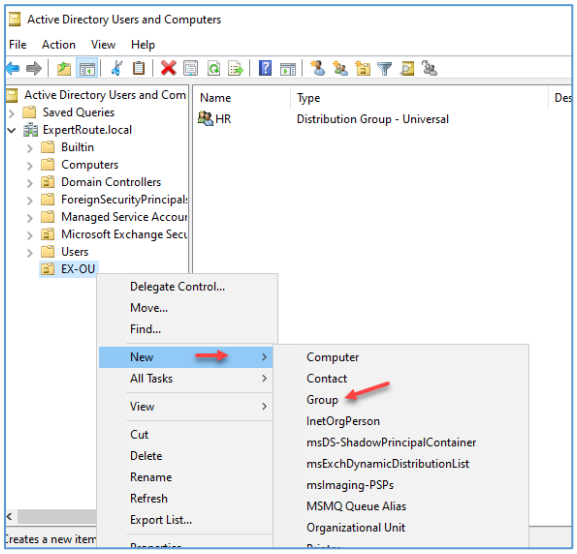
اگر به شکل ۱۴-۱۱۳، توجه کنید، در قسمت بالای آدرس گروه، همان توضیحاتی که برای گروه نوشتیم مشخص شده است، با ارسال ایمیل به گروه مورد نظر به تمام کاربران آن ایمیل ارسال می‌شود.

www.takbook.com



شکل ۱۴- ۱۱۳ ارسال ایمیل به گروه مورد نظر

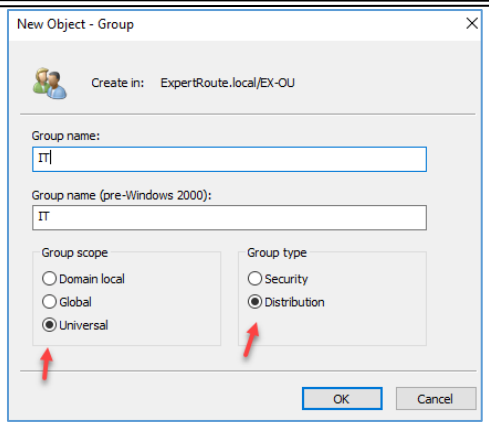
شما می‌توانید از طریق Active Directory هم گروه ایجاد کنید و آن در در Exchange فعال کنید، باید به این نکته توجه کنید که گروهی که در Active ایجاد می‌کنید به صورت اتوماتیک در Exchange فعال نخواهد شد و آن را باید با دستوری فعال کنیم، به مانند شکل ۱۴-۱۱۴،وارد Active می‌شویم و Group را انتخاب می‌کنیم.



شکل ۱۴- ۱۱۴ ایجاد گروه در Active Directory

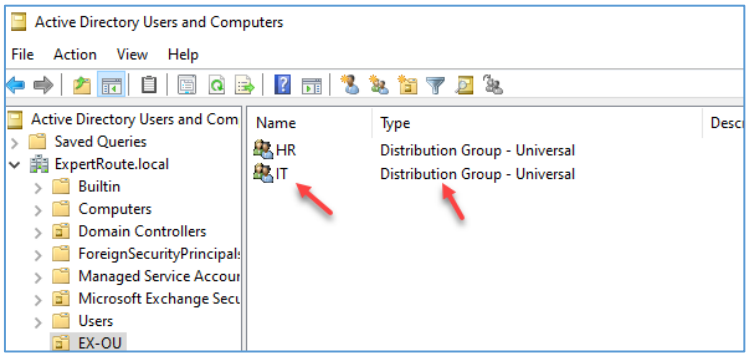
در شکل ۱۴-۱۱۵، در قسمت Scope باید گزینه‌ی Universal را انتخاب کنید که در مورد گروه‌ها در اوایل کتاب توضیحات مورد نظر را دادیم، در قسمت Type هم گزینه‌ی Distribution را انتخاب کنید و بر روی OK کلیک کنید.

www.takbook.com



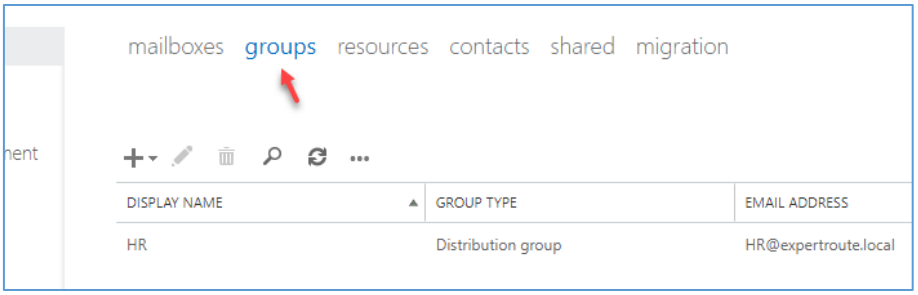
شکل ۱۴- ۱۱۵ ایجاد گروه در *Active Directory*

همان‌طور که در شکل ۱۴-۱۱۶، مشاهده می‌کنید گروه مورد نظر در OU مشخص شده ایجاد شده است حتی گروهی که در Exchange هم ایجاد کردیم موجود است.



شکل ۱۴- ۱۱۶ ایجاد گروه در *Active Directory*

اگر به مانند شکل ۱۴-۱۱۷، وارد Exchange شوید و در بخش گروها نگاه کنید متوجه خواهید شد گروه IT در لیست وجود ندارد و برای همین منظور برای ایجاد MailBox برای این گروه باید از دستور زیر در PowerShell استفاده کنید:



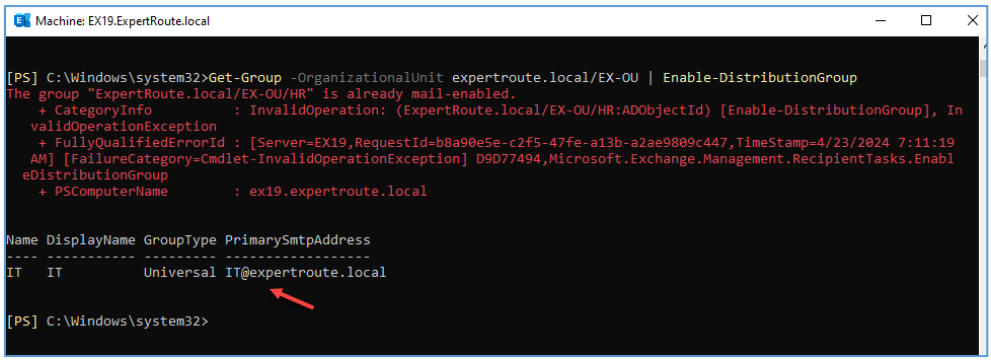
شکل ۱۴- ۱۱۷ ایجاد گروه

www.takbook.com

دستور زیر را در PowerShell مربوط به Exchange اجرا می‌کنیم:

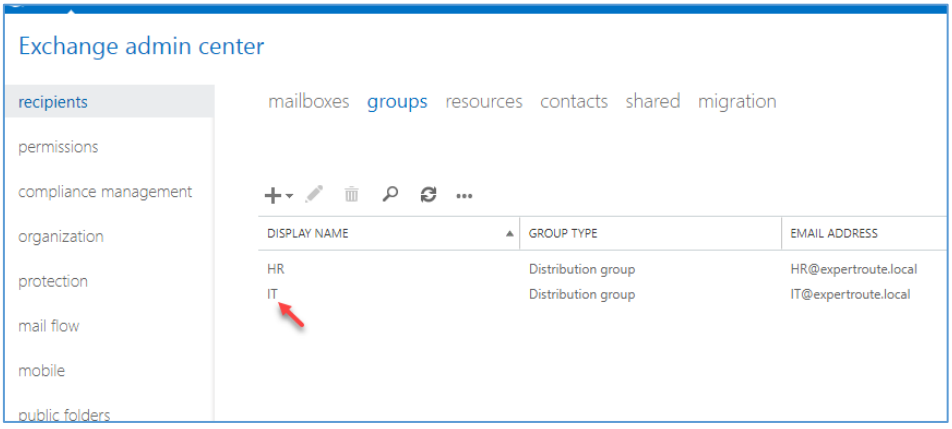
```
Get-Group -OrganizationalUnit expertroute.local/EX-OU | Enable-DistributionGroup
```

همان‌طور که در شکل ۱۴-۱۱۸، مشاهده می‌کنید با اجرای دستور بالا گروه IT در Exchange فعال شد و یک Mailbox به آن تخصیص داده شده است، اگر به شکل توجه کنید خطایی هم رخ داده است و این خطا به این موضوع اشاره دارد که در OU مورد نظر یک گروه دیگر به نام HR وجود دارد که ما قبلاً آن را در Exchange فعال کرده بودیم و به همین خاطر نمی‌تواند دوباره آن را فعال کند و خطا می‌دهد.



شکل ۱۴- ۱۱۸ بروزرسانی گروه در Exchange

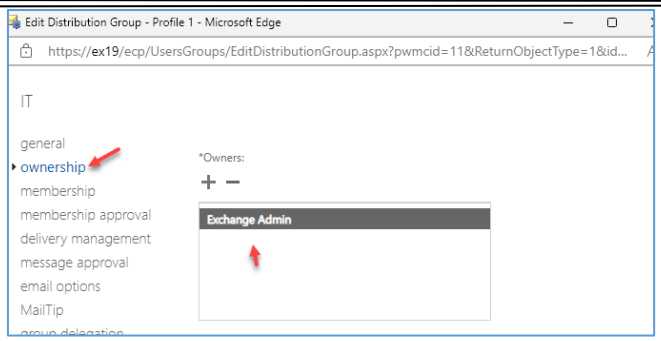
حالا اگر به مانند شکل ۱۴-۱۱۹، در صفحه‌ی مدیریتی Exchange وارد گروه شوید، گروه جدید IT را به مانند شکل مشاهده می‌کنید که فعال شده است و می‌توانید به آن ایمیل بزنید.



شکل ۱۴- ۱۱۹ بروزرسانی گروه در Exchange

توجه داشته باشید وقتی گروهی از طریق Active ایجاد می‌کنید باید تنظیمات آن را در Exchange تکمیل کنید، مثلاً Owner آن را به مانند شکل ۱۴-۱۲۰، مشخص کنید و یا اعضای آن را.

www.takbook.com

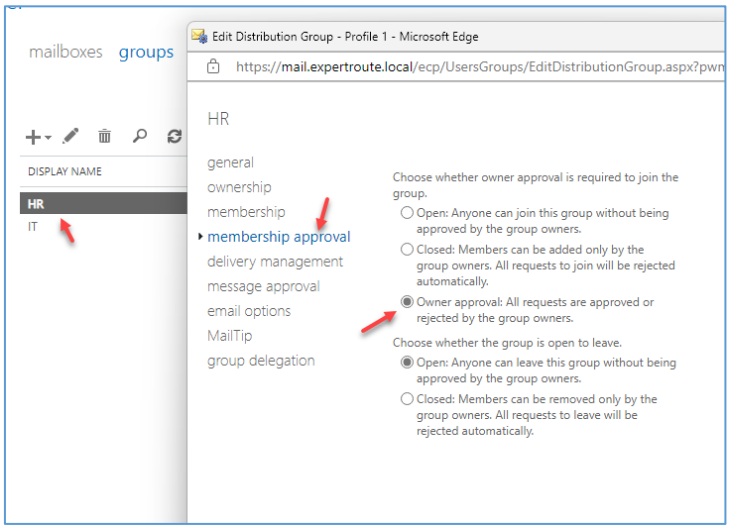


شکل ۱۴- ۱۲۰مشخص کردن Owner گروه

۱۵-۱۴ نحوه درخواست کاربر برای عضو شدن در گروه

برای اینکه کاربران بتوانند درخواست عضویت در گروه را بدهند باید به صورت زیر عمل کنید.

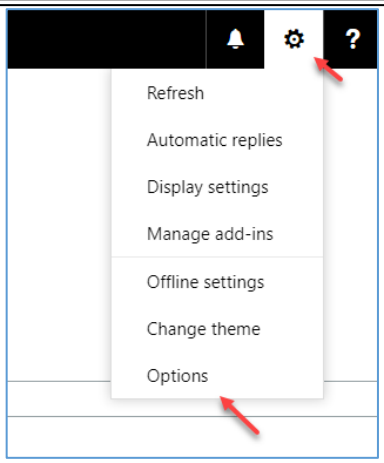
وارد صفه‌ی مدیریتی Exchange شوید و دو بار بر روی گروه مرود نظر کلیک کنید و به مانند شکل ۱۴-۱۲۱، وارد قسمت membership approval شوید و گزینه‌ی Owner approval: All requests are approved or rejected by the group owners را انتخاب کنید تا کاربران برای عضویت در گروه درخواست دهند.



شکل ۱۴- ۱۲۱ درخواست کاربر برای عضو شدن در گروه

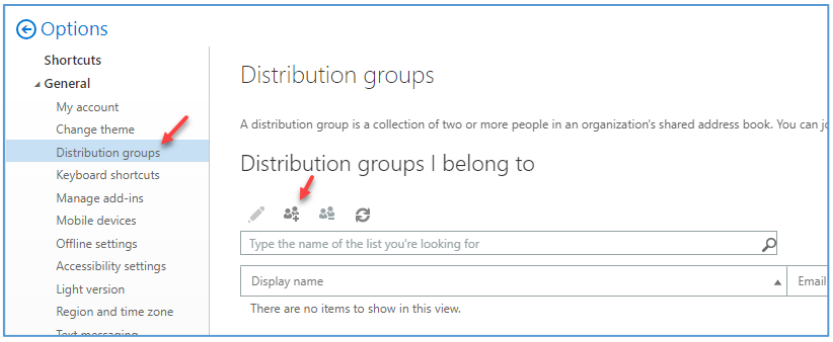
بعد از انجام کار بالا با نام کاربری مورد نظر خود وارد ایمیل تحت وب با آدرس https://mail.expertroute.local/owa شوید و به مانند شکل ۱۴-۱۲۲، وارد Options شوید، توجه داشته باشید که کاربر مورد نظر نباید عضو آن گروه باشد.

www.takbook.com



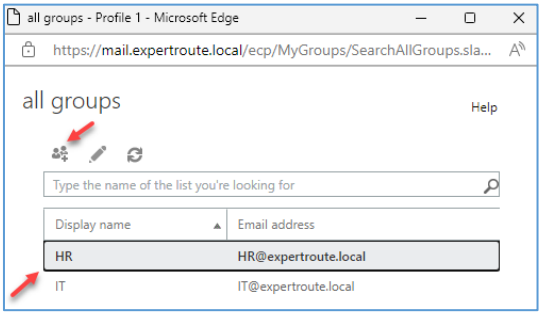
شکل ۱۴- ۱۲۲ درخواست کاربر برای عضو شدن در گروه

در ادامه کار به مانند شکل ۱۴-۱۲۳، از قسمت General گزینه‌ی Distribution groups را انتخاب کنید و در صفحه باز شده بر روی آیکون مشخص شده کلیک کنید که برای عضو شدن در گروه مورد نظر است.



شکل ۱۴- ۱۲۳ درخواست کاربر برای عضو شدن در گروه

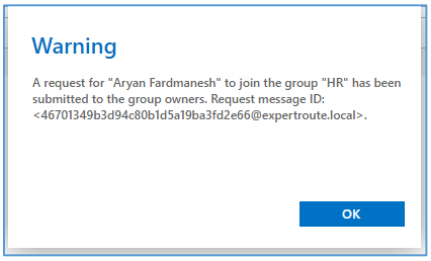
در شکل ۱۴-۱۲۴، گروه‌هایی که در شکل مشاهده می‌کنید در لیست قرار دارد و باید آن را انتخاب و بر روی آیکون Join کلیک کنید.



شکل ۱۴- ۱۲۴ درخواست کاربر برای عضو شدن در گروه

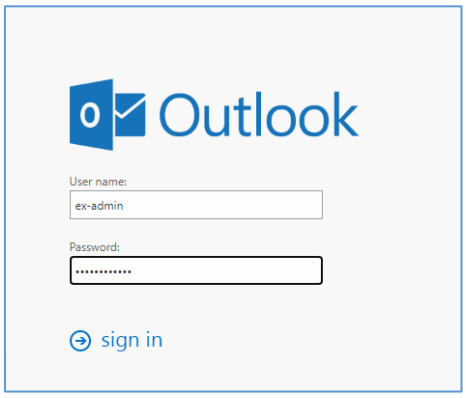
www.takbook.com

بعد از اینکه بر روی Join کلیک کردید شکل ۱۴-۱۲۵، ظاهر می‌شود که یک پیغام Join برای مدیر گروه ارسال شده است و مدیر مورد نظر باید آن را تایید کند.



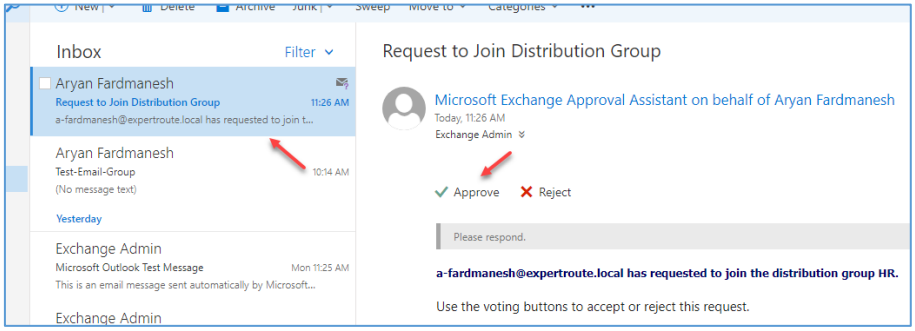
شکل ۱۴- ۱۲۵ درخواست کاربر برای عضو شدن در گروه

به مانند شکل ۱۴-۱۲۶، با استفاده از نام کاربری مدیر وارد ایمیل می‌شویم.



شکل ۱۴- ۱۲۶ ورود به ایمیل

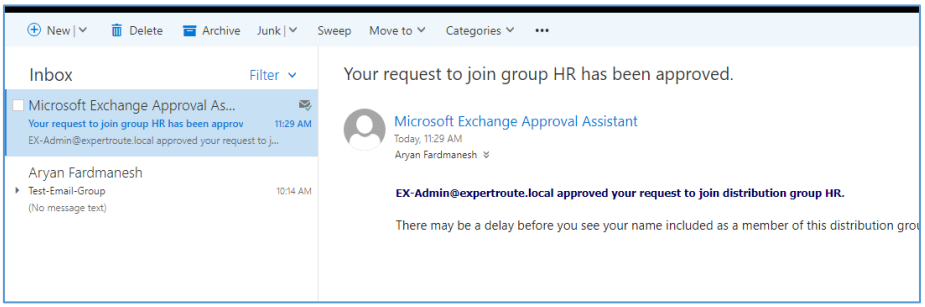
همان‌طور که در شکل ۱۴-۱۲۷، مشاهده می‌کنید، یک ایمیل درخواست برای مدیر گروه ارسال شده است که با کلیک بر روی دکمه Approve عضویت کاربر مورد نظر در گروه مشخص شده تایید می‌شود، و بعد از تایید این ایمیل حذف خواهد شد.



شکل ۱۴- ۱۲۷ درخواست کاربر برای عضو شدن در گروه

www.takbook.com

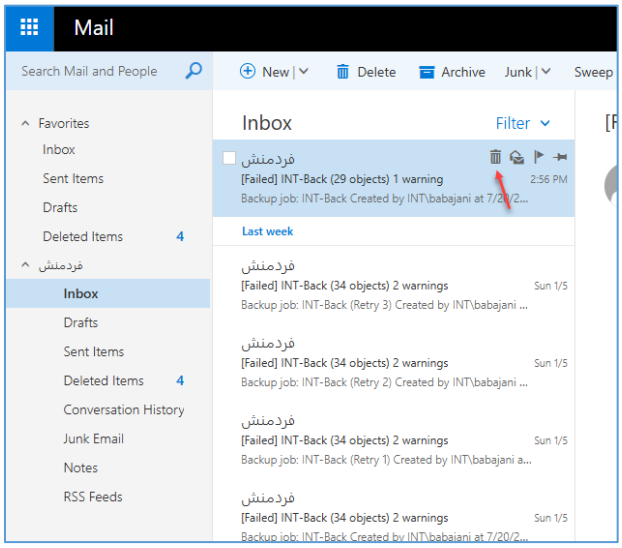
بعد از تایید اگر وارد ایمیل کاربر مورد نظر خود شوید یک پیغام به صورت شکل ۱۴-۱۲۸، مشاهده می‌کنید که نوشته است درخواست عضویت در گروه مورد نظر تایید شده است.



شکل ۱۴- ۱۲۸ درخواست کاربر برای عضو شدن در گروه

۱۴-۱۶ برگشت دادن ایمیل‌های حذف شده

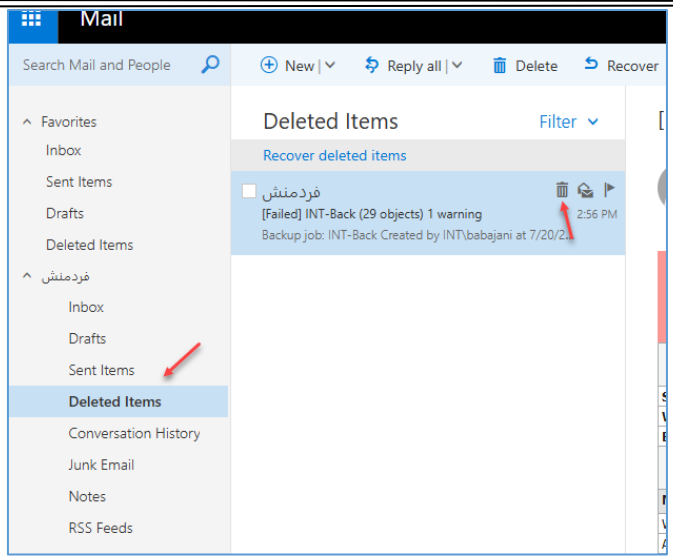
در این قسمت می‌خواهیم بر روی Email Recover بررسی داشته باشیم که این روش به ما کمک می‌کند در زمانی که یک ایمیل را از سرور ایمیل خود حذف کردیم، دوباره آن را به ایمیل خود برگشت دهیم؛ برای این کار وارد ایمیل تحت وب خود شوید و یکی از ایمیل‌های دریافتی خود را به مانند شکل ۱۴-۱۲۹، حذف کنید.



شکل ۱۴- ۱۲۹ برگشت دادن ایمیل‌های حذف شده

بعد از انجام کار بالا به مانند شکل ۱۴-۱۳۰، از سمت چپ وارد قسمتDeleted Items شوید و دوباره، ایمیل خود را از قسمت حذف‌شده‌ها یا همان Trash حذف کنید تا کاملاً از ایمیل شما حذف شود.

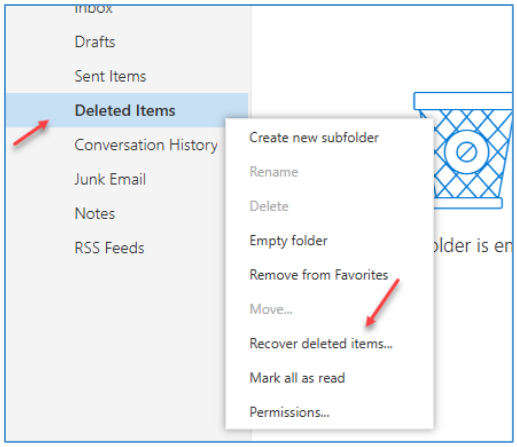
www.takbook.com



شکل ۱۴- ۱۳۰ برگشت دادن ایمیل‌های حذف شده

زمانی که شما این کار را انجام می‌دهید، به واقع دیگر ایمیلی وجود نخواهد داشت، امّا روشی وجود دارد که می‌شود ایمیل‌های حذف شده را دوباره برگرداند.

برای برگشتن دادن ایمیل‌های حذف شده باید به مانند شکل ۱٤-۱۳۱، بر روی گزینه‌ی Deleted Items کلیک راست کنید و گزینه‌ی Recover deleted items را انتخاب کنید.

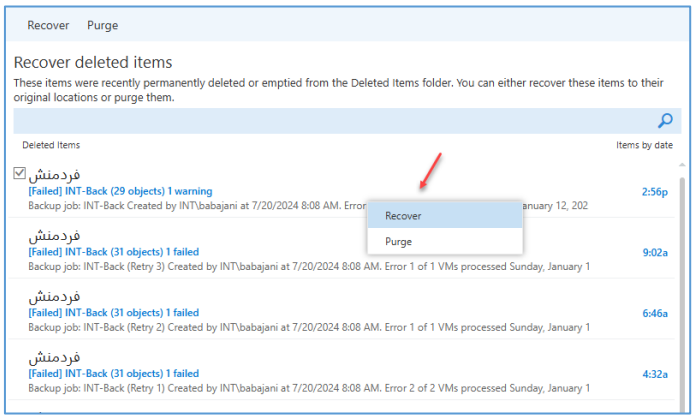


شکل ۱۴- ۱۳۱ برگشت دادن ایمیل های حذف شده

همان‌طور که در شکل ۱٤-۱۳۲، مشاهده می‌کنید، ایمیل مورد نظر در لیست قرار دارد و برای برگشت به ایمیل باید آن را انتخاب و بر روی آن کلیک راست کنید و گزینه‌ی Recover را انتخاب و در صفحه‌ی باز شده بر روی OK کلیک کنید تا ایمیل حذف شده به جایگاه اوّل خودش برگردد. گزینه‌ای دیگر با نام Purge قرار دارد که با انتخاب

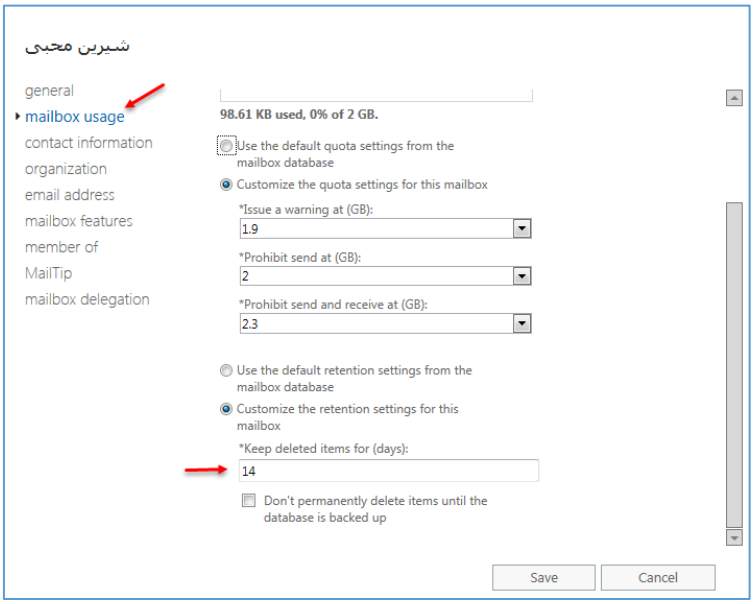
www.takbook.com

آن و کلیک بر روی OK، ایمیل‌های انتخاب شده برای همیشه از لیست Recover هم حذف خواهند شد و دیگر نمی‌توانید به آنها دسترسی داشته باشید.



شکل ۱۴- ۱۳۲ برگشت دادن ایمیل های حذف شده

نکته: مطلبی که اینجا باید به آن اشاره کنیم، این است که این ایمیل‌های حذف شده به مدّت مشخّصی که قبلاً در صفحات قبل آن را بررسی کردیم در لیست قرار می‌گیرد؛ در صفحه‌ی شکل ۱۴-۱۳۳، قسمتی که ۱۴ وارد شده است را مشاهده کنید، این عدد به این منظور است که اطّلاعات تا ۱۴ روز در قسمت Recover باقی می‌مانند و بعد از آن، از سرور حذف خواهند شد. این صفحه مربوط به قسمت Administrator سرور exchange است که در قسمت معرّفی کاربر در قمست قبل بررسی کردیم.



شکل ۱۴- ۱۳۳ برگشت دادن ایمیل های حذف شده

www.takbook.com

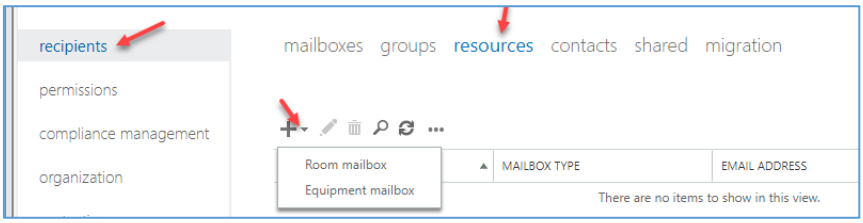
۱۷-۱٤بررسی Resources در Exchange 2019

یکی از ویژگی‌های جالب در Exchange ایجاد ایمیل برای یک اتاق خاص مانند اتاق جلسات و یا یک دستگاه خاص است.

به بیان دیگر با ایجاد این نوع ایمیل شما اگر نیاز به این دارید که مثلاً در یک تاریخ مشخص اتاق جلسات را رزرو کنید از طریق این ایمیل می‌توانید متوجه شوید که اتاق خالی است یا رزرو شده.

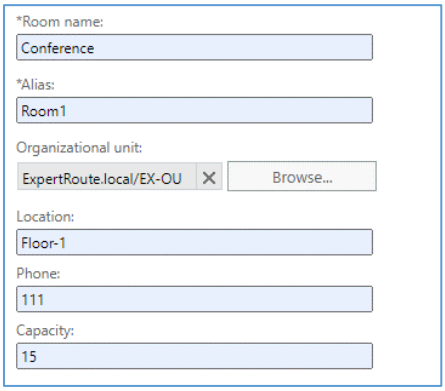
برای انجام این کار وارد صفحه‌ی مدیریتی شوید و به مانند شکل۱٤-۱۳٤، از قسمت recipients وارد تب Resources شوید و بر روی آیکون مشخص شده کلیک کنید، دو گزینه را مشاهده می‌کنید که گزینه‌ی اول (Room mailbox) مربوط به اتاق‌ها خاص مانند اتاق جلسات است و گزینه‌ی دوم (Equipment mailbox) برای دستگاه‌های شبکه به کار می‌رود، مانند لپ تاپ، ویدئو پروژکتور و ...

برای شروع کار بر روی Room mailbox کلیک کنید.



شکل ۱۴- ۱۳۴ بررسی Resources در Exchange 2019

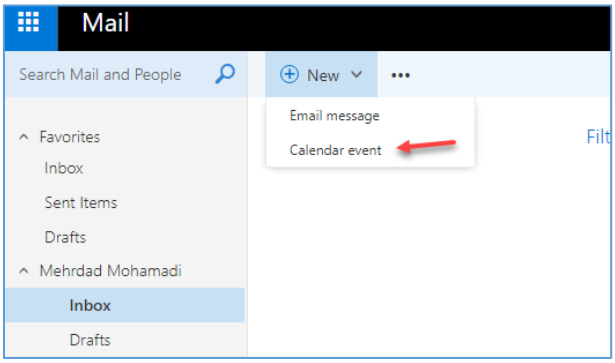
به مانند شکل ۱٤-۱۳۵، باید نام اتاق را وارد کنید و در قسمت Alias یک نام به انگلیسی وارد کنید چون این نام همان نام ایمیل خواهد بود، در قسمت Organizational نام OU خود را انتخاب کنید و در قسمت Location موقعیت و منطقه جغرافیایی اتاق خود را مشخص کنید و در قسمت Phone شماره داخلی اتاق و در آخر هم ظرفیت اتاق را مشخص کنید.



شکل ۱۴- ۱۳۵ بررسی Resources در Exchange 2019

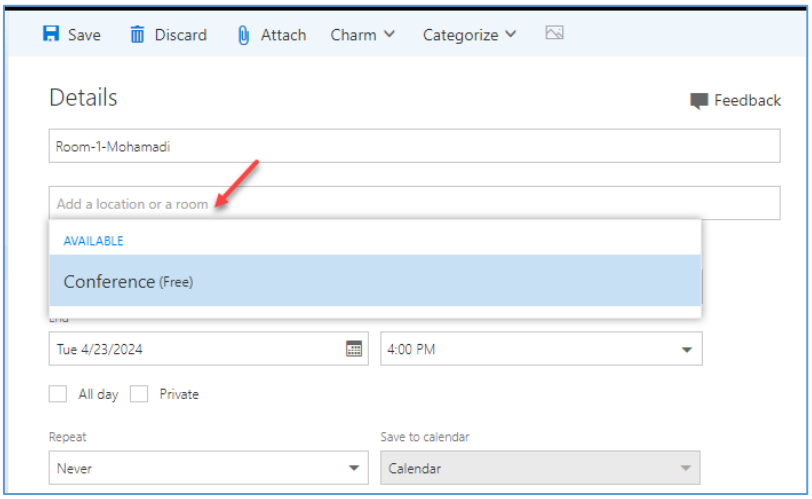
www.takbook.com

در ادامه کار بعد از ایجاد اتاق مورد نظر به مانند شکل ۱۴-۱۳۶، وارد Outlook تحت وب شوید و بر روی آیکون New کلیک کنید و گزینه‌ی Calender event را انتخاب کنید.



شکل ۱۴- ۱۳۶ بررسی Resources در Exchange 2019

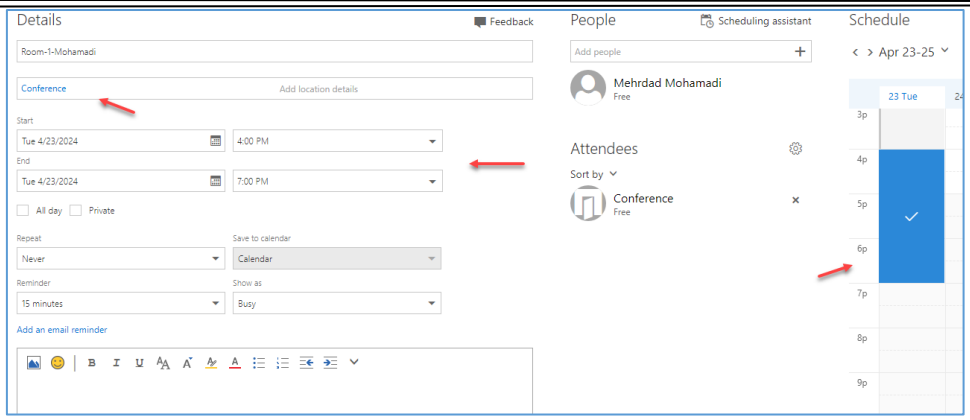
به مانند شکل ۱۴-۱۳۷، در قسمت Location کلیک کنید، بعد از کلیک کردن لیست اتاق‌هایی که موجود است را به ما نمایش می‌دهد که همان‌طور که مشاهده می‌کنید یک اتاق با نام Conference موجود است که در تاریخ و ساعتی که انتخاب شده Free نوشته شده و این یعنی اتاق آزاد است.



شکل ۱۴- ۱۳۷ بررسی Resources در Exchange 2019

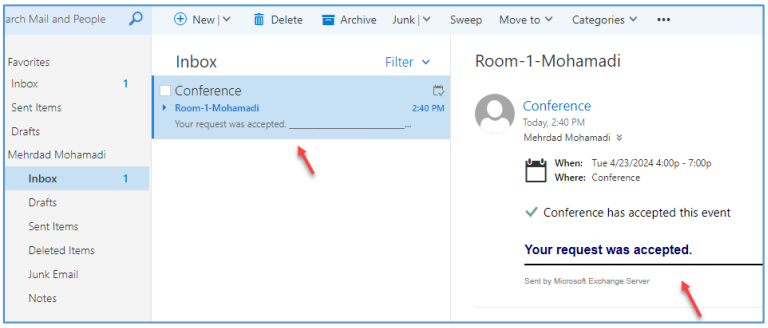
به مانند شکل ۱۴-۱۳۸، بعد از انتخاب اتاق مورد نظر و ساعت و تاریخ مشخص شده در سمت راست هم زمان و تاریخ با رنگ آبی مشخص می‌شود، در آخر بر روی Send کلیک کنید تا اطلاعات به اتاق مورد نظر ارسال شود.

www.takbook.com



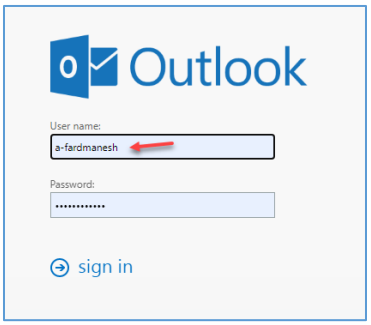
شکل ۱۴- ۱۳۸ بررسی Resources در Exchange 2019

به مانند شکل ۱۴-۱۳۹، بعد از کلیک بر روی Send کاربر مورد نظر یک ایمیل دریافت می‌کند که در این ایمیل تایید می‌کند که در تاریخ مشخص شده درخواست شما تایید شده است و زمان اتاق جلسات به شما تعلق دارد.



شکل ۱۴- ۱۳۹ بررسی Resources در Exchange 2019

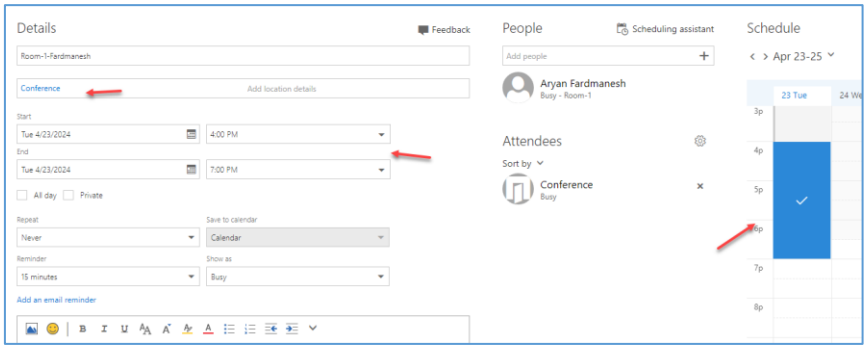
حالا برای اینکه ببینیم این کار عملی است یا نه با یک کاربر دیگر وارد Outlook تحت وب می‌شویم که این موضوع را در شکل ۱۴-۱۴۰، مشاهده می‌کنید.



شکل ۱۴- ۱۴۰ بررسی Resources در Exchange 2019

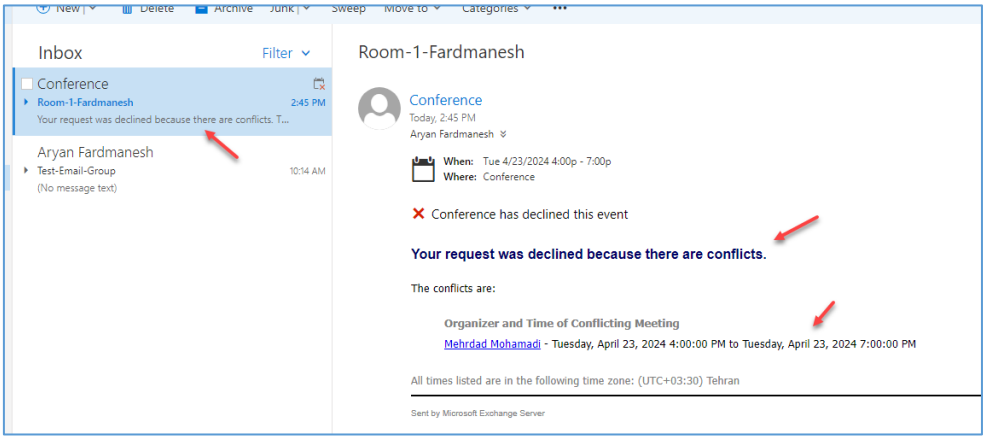
www.takbook.com

به مانند شکل ۱۴-۱۴۱، بعد از ورود دوباره همان مسیر را برای رزرو کردن وقت اتاق جلسات بررسی می‌کنیم، همان‌طور که مشاهده می‌کنید کاربر دیگری در همان تاریه و ساعت اتاق مورد نظر را انتخاب کرده است، بعد از انتخاب، آن را برای اتاق مشخص شده ارسال می‌کنیم.



شکل ۱۴- ۱۴۱ بررسی Resources در Exchange 2019

بعد از ارسال، یک ایمیل برای شما ارسال می‌شود که به این موضوع اشاره دارد که در این تاریخ و زمان کاربر دیگری با نام Mehrdad Mohamadi اتاق جلسات مورد نظر را رزو کرده است و این درخواست رد شده است و دوباره باید یک زمان دیگر را مشخص کنید.



شکل ۱۴- ۱۴۲ بررسی Resources در Exchange 2019

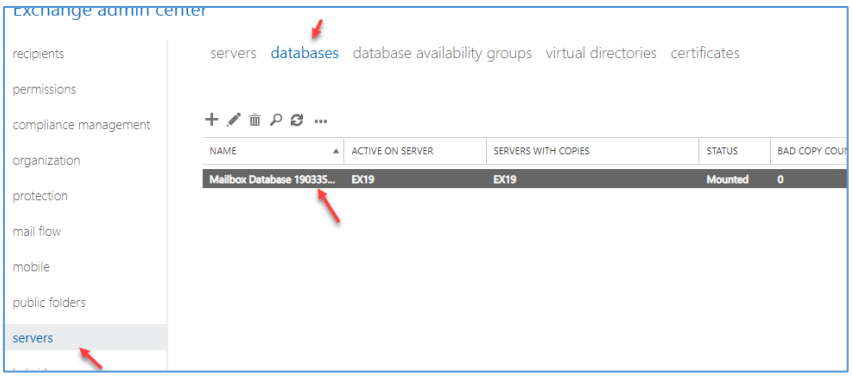
۱۸-۱۴ بررسی و انتقال دیتابیس در Exchange 2019

همان‌طور که در قسمت قبل بررسی کردیم، یک سرور Exchange، دارای یک یا چند Database است که در یک مکان مشخّص شده قرار می‌گیرند و تمام اطّلاعات در این DataBase ها قرار دارند و با ایجاد مشکل کوچک، DataBase با مشکل مواجه خواهد شد و در نتیجه، سرور Exchange را از دست خواهیم داد. در

www.takbook.com

این قسمت می‌خواهیم تحلیلی بر DataBase داشته باشیم و مکان مورد نظر آن را پیدا کنیم و بعد آن را به مکان بهتر و امن‌تر انتقال دهیم.

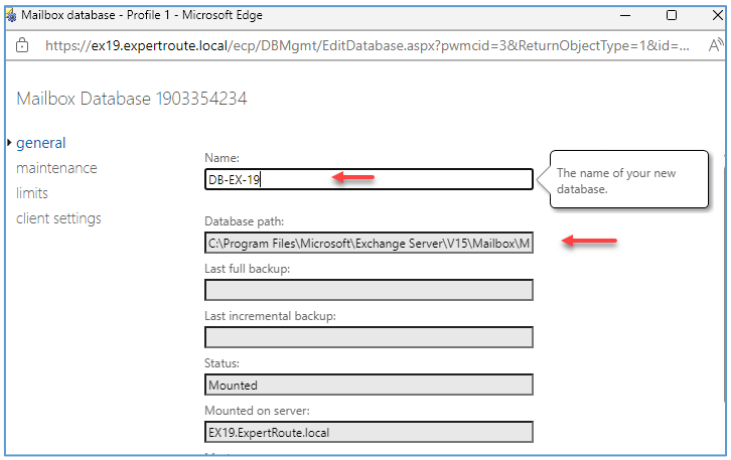
به مانند شکل ۱۴-۱۴۳، اگر وارد قسمت مدیریّتی سرور Exchange شوید و از سمت چپ بر روی Server کلیک کنید و بعد وارد تب Databases شوید، می‌توانید دیتابیس موجود و فعّال را مشاهده کنید، مکان این دیتابیس به صورت پیش‌فرض در ریشه‌ی ویندوز که بیشتر درایو C می‌باشد، قرار دارد؛ بر روی آن دو بار کلیک کنید.



شکل ۱۴-۱۴۳ انتقال دیتابیس در Exchange 2019

همان‌طور که در شکل ۱۴-۱۴۴، مشاهده می‌کنید، در قسمت Name نام دیتابیس نوشته شده است و پیشنهاد این است که نام را به دلخواه خود تغییر دهید تا شناسایی دیتابیس آسان‌تر باشد و در ادامه و در قسمت Database path می‌توانید آدرس ذخیره شدن دیتابیس مورد نظر را مشاهده کنید که در آدرس زیر ذخیره شده است:

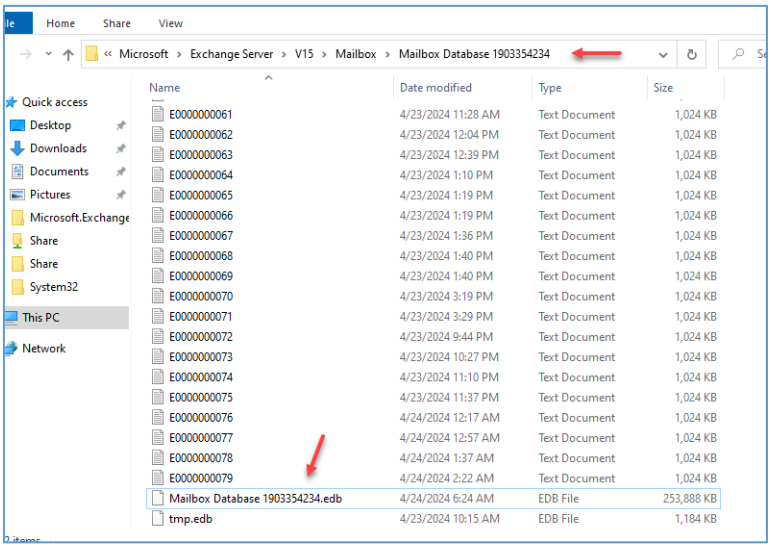
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1903354234\Mailbox Database 1903354234.edb



شکل ۱۴-۱۴۴ انتقال دیتابیس در Exchange 2019

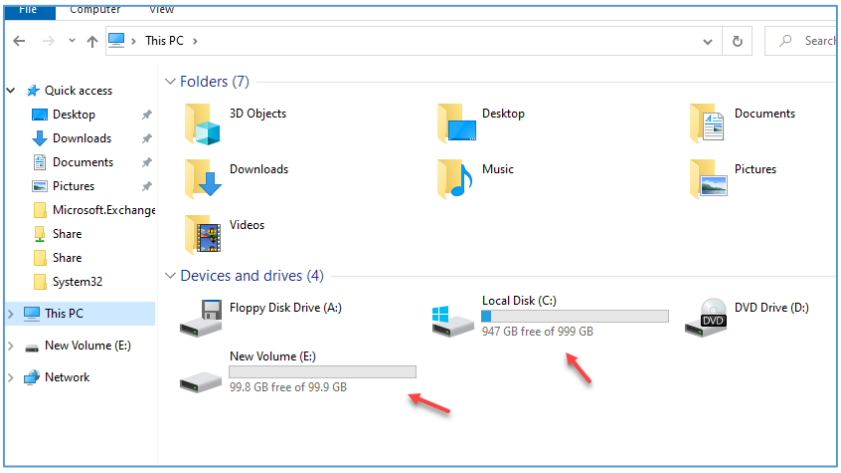
www.takbook.com

اگر به شکل ۱۴-۱۴۵، دقت کنید در آدرس مشخص شده دیتابیس مورد نظر موجود است.



شکل ۱۴- ۱۴۵ انتقال دیتابیس در Exchange 2019

اگر چنانچه مقدار فضای هاردی که این دیتابیس در آن قرار دارد پر شود و یا اینکه از نظر امنیتی مشکلی وجود داشته باشد باید این دیتابیس را به مکان بهتر انتقال داد، به مانند شکل ۱۴-۱۴۶، برای تست این موضوع بر روی سرور Exchange یک هارد جدید اضافه کردیم و می‌خواهیم دیتابیس را از درایو C به درایو دیگر انتقال دهیم، اگر وارد This PC شویم هارد دوم که درایو E هست را مشاهده می‌کنید.



شکل ۱۴- ۱۴۶ انتقال دیتابیس در Exchange 2019

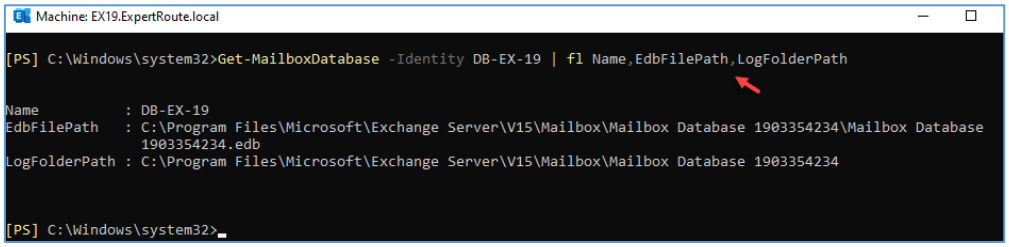
www.takbook.com

وارد سرور Exchange 2019 شوید و در قسمت جستجو سرویس Exchange Management shell را اجرا کنید.

در خط فرمان، دستور زیر را وارد کنید:

```
Get-MailboxDatabase -Identity DB-EX-19 | fl Name,EdbFilePath,LogFolderPath
```

در دستور بالا، شما به جای DB-EX-19، نام دیتابیس را وارد کنید و بر روی Enter فشار دهید، توجه داشته باشید نام دیتابیس را در قسمت قبل تغییر دادیم.



شکل ۱۴- ۱۴۷ انتقال دیتابیس در Exchange 2019

همان‌طور که در شکل ۱۴-۱۴۷، مشاهده می‌کنید، دستور بالا به درستی اجرا شده است که دو مسیر را برای شما مشخّص کرده است، یکی Edbfilepath که این مسیر، مسیر Database شما است که در مسیر زیر قرار دارد:

C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1903354234\Mailbox Database 1903354234.edb

مسیر دیگر با عنوان LogFolderPath است که مربوط به رویدادهای (Logs) دیتابیس مور نظر است که در مسیر زیر قرار دارد:

C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 1903354234

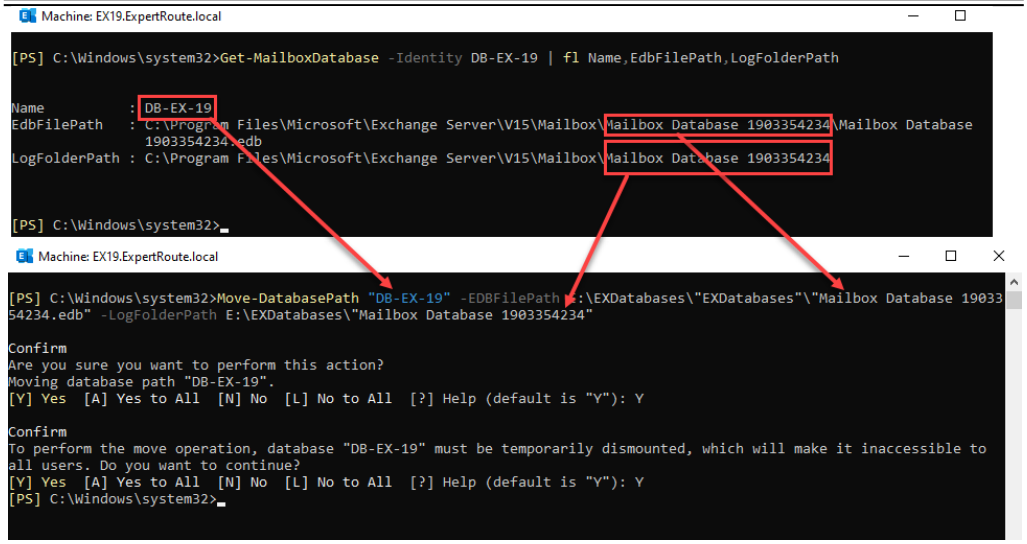
با این حساب، شما دو مسیر دارید که در درایو C قرار دارند که در ادامه می‌خواهیم این اطّلاعات را به مسیری به غیر از درایو C ارسال کنیم تا در صورت از دست رفتن ویندوز، اطّلاعات ما هم از دست نرود و بتوانیم دوباره از آنها استفاده کنیم.

برای شروع در همان Exchange Management Shell، دستورات زیر را وارد کنید.

دستور انتقال دیتابیس و Log به صورت زیر است:

```
Move-DatabasePath "DB-EX-19" -EDBFilePath E:\EXDatabases\"EXDatabases"\"Mailbox Database 1903354234.edb" -LogFolderPath E:\EXDatabases\"Mailbox Database 1903354234
"
```

www.takbook.com



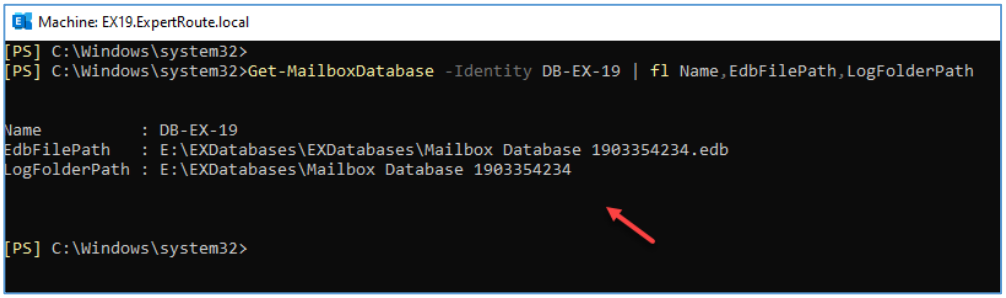
شکل ۱۴- ۱۴۸ انتقال دیتابیس در Exchange 2019

با توجه به شکل ۱۴-۱۴۸، شکل اول مربوط به دستور اوّل است که با هم انجام دادیم، امّا شکل دوم، مربوط به انتقال دیتابیس است که در شکل اوّل، جایی که مستطیل مشخّص شده، نام دیتابیس شما است که باید آن را در دستور بالا وارد کنید.

فقط توجّه داشته باشید در نام دیتابیس سوم که با رنگ قرمز مشخّص شده است، حتماً پسوند edb را در آخر آن قرار دهید، منظور Mailbox Database 1903354234.edb است.

در تصویر ۱۴-۱۴۸، بعد از اینکه دستور را اجرا کردید، کلمه‌ی Y را وارد و Enter کنید؛ این کار را دوبار انجام دهید، یا اینکه یک بار A را وارد کنید.

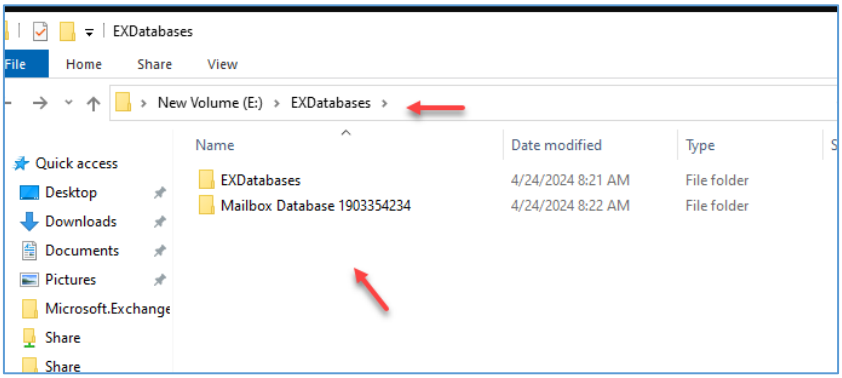
اگر بعد از انتقال، دستور شکل ۱۴-۱۴۹، را دوباره اجرا کنید، مشاهده خواهید کرد که مسیر تغییر کرده است.



شکل ۱۴- ۱۴۹ انتقال دیتابیس در Exchange 2019

www.takbook.com

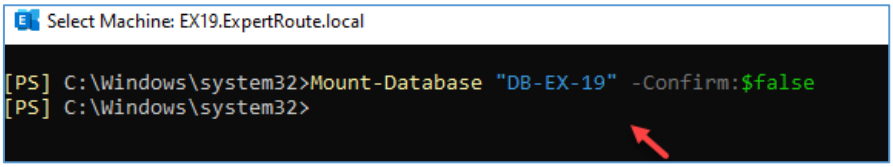
اگر به مانند شکل ۱٤-۱۵۰، وارد درایو E شوید می‌توانید مشاهده کنید که دیتابیس مورد نظر با موفقیت انتقال داده شده است.



شکل ۱۴- ۱۵۰ انتقال دیتابیس در Exchange 2019

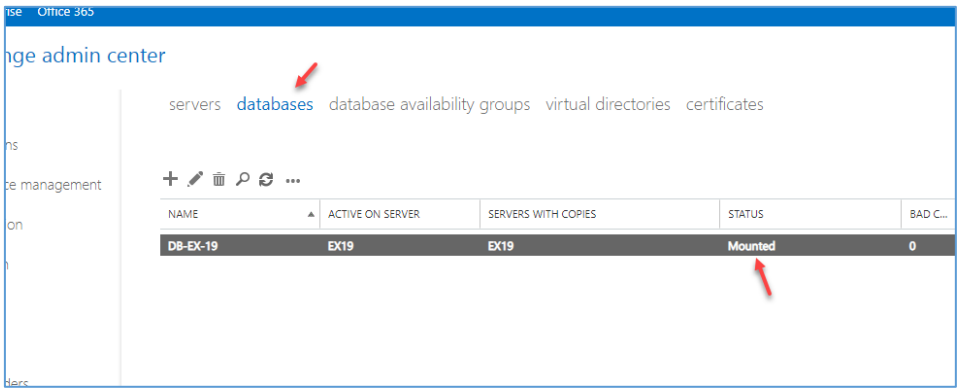
بعد از انتقال دیتابیس باید با دستور زیر دیتابیس مورد نظر را فعال کنیم که این مضووع را در شکل ۱٤-۱۵۱، مشاهده می‌کنید.

```
Mount-Database "DB-EX-19" -Confirm:$false
```



شکل ۱۴- ۱۵۱ انتقال دیتابیس در Exchange 2019

اگر وارد سرور شوید به مانند شکل ۱٤-۱۵۲، مشاهده خواهید کرد که دیتابیس مورد نظر در مسیر جدید Mounted و فعال شده است.



شکل ۱۴- ۱۵۲ انتقال دیتابیس در Exchange 2019

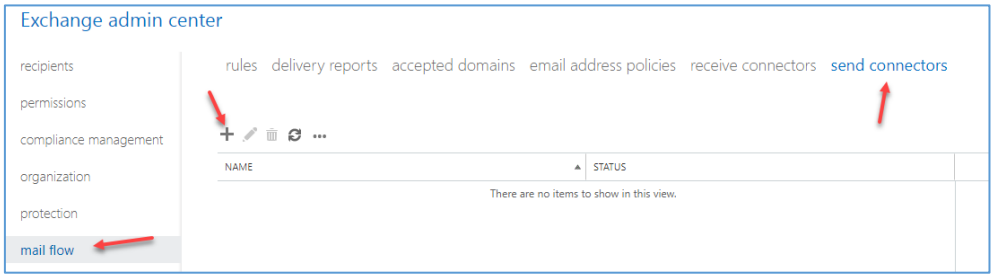
www.takbook.com

۱۹-۱٤ ارسال ایمیل به خارج از شبکه (اینترنت)

در این قسمت می‌خواهیم تنظیماتی انجام دهیم تا کاربر بتواند ایمیل خود را به ایمیلی، غیر از ایمیل داخلی شبکه مانند یاهو و جی‌میل ارسال کند.

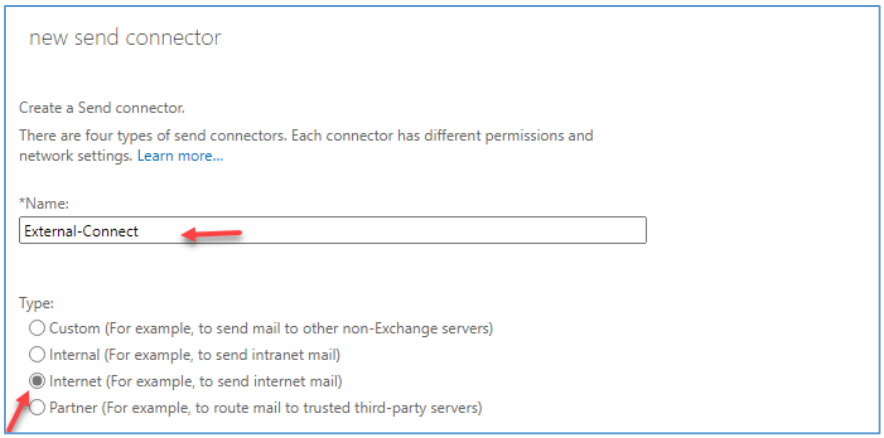
نکاتی که در این زمینه وجود دارد این است که اگر عملیات زیر را انجام دهید ایمیل به سرورهای داخل اینترنت ارسال خواهد شد و باید توجه داشت که چون آدرس دومین ما یک آدرس داخلی خود شبکه است و در دنیای اینترنت ناشناخته است بدون شک ایمیل‌ها در پوشه Spam قرار خواهند گرفت که انشاالله در ادامه راه حل این نوع مشکلات را بیان خواهیم کرد.

به مانند شکل ۱٤-۱۵۳، وارد صفحه‌ی مدیریّتی Exchange 2019 شوید و از سمت چپ بر روی Mail Flow کلیک کنید و در صفحه‌ی باز شده بر روی تب Send Connectors کلیک کنید و بعد برای ایجاد rule جدید بر روی آیکون + کلیک کنید.



شکل ۱۴- ۱۵۳ ارسال ایمیل به خارج از شبکه

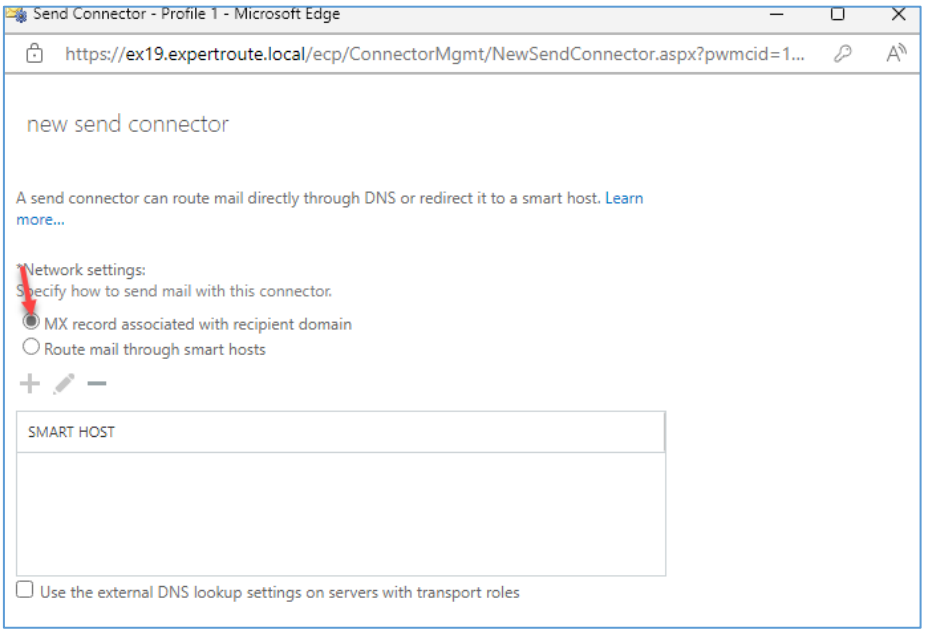
در شکل ۱٤-۱۵٤، یک نام برای Rule خود وارد کنید و از قسمت Type، گزینه‌ی Internet را انتخاب و بر روی Next کلیک کنید.



شکل ۱۴- ۱۵۴ ارسال ایمیل به خارج از شبکه

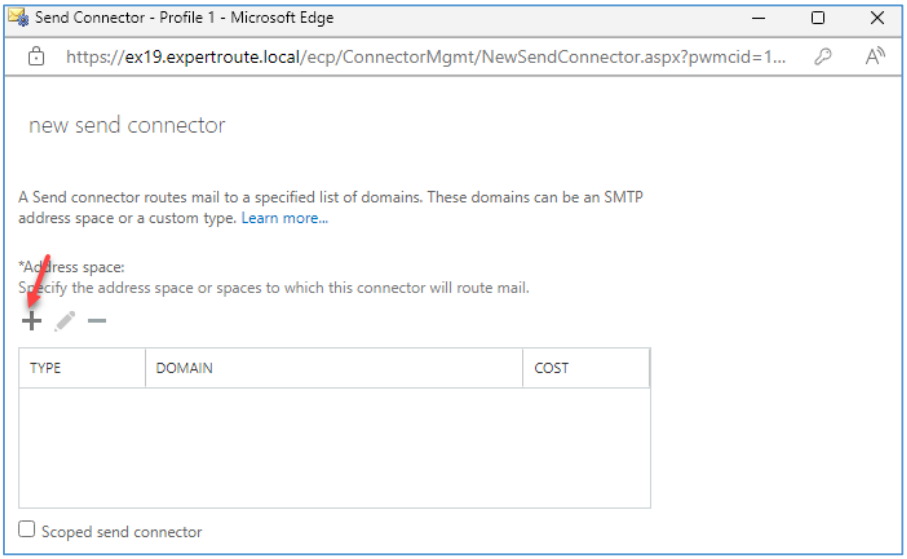
www.takbook.com

در شکل ۱۴–۱۵۵، گزینه‌ی MX Record را انتخاب و بر روی Next کلیک کنید.



شکل ۱۴- ۱۵۵ ارسال ایمیل به خارج از شبکه

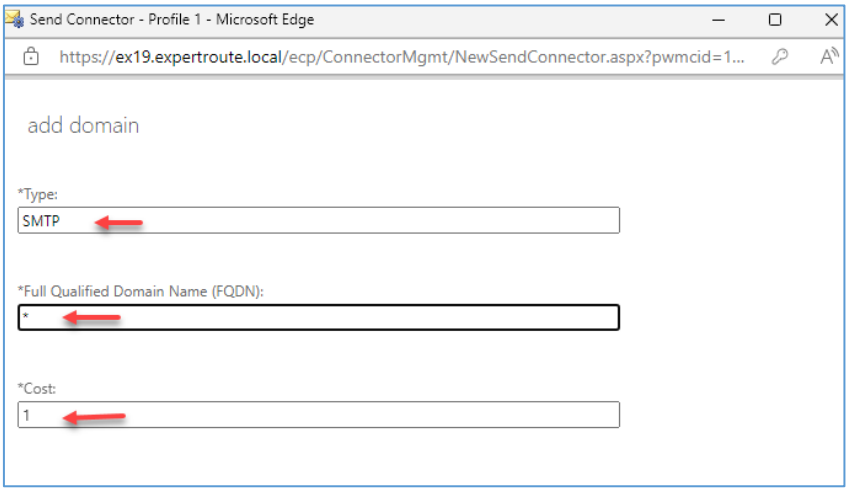
در شکل ۱۴–۱۵۶، باید مشخّص کنید که ایمیل به چه آدرسی در خارج از شبکه ارسال شود که برای این کار باید بر روی آیکون + کلیک کنید.



شکل ۱۴- ۱۵۶ ارسال ایمیل به خارج از شبکه

www.takbook.com

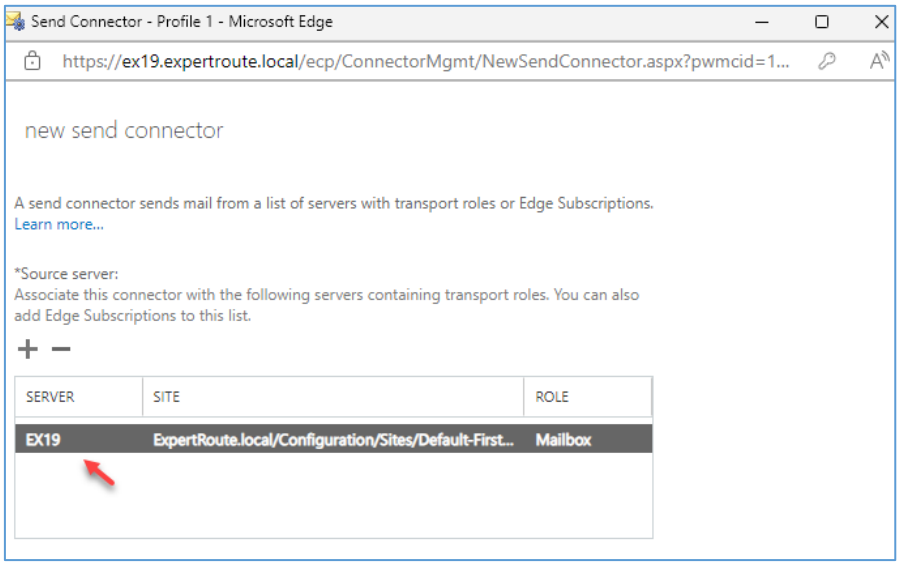
در شکل ۱۴-۱۵۷، در قسمت Full Qualified Domain Name، آدرس مورد نظر را با * وارد کنید تا کاربر بتواند هر آدرسی را در ایمیل خود وارد کند؛ بر روی Save و بعد بر روی Next کلیک کنید.



شکل ۱۴- ۱۵۷ ارسال ایمیل به خارج از شبکه

در شکل ۱۴-۱۵۸، بر روی + کلیک کنید و سرور Exchange خود را به لیست اضافه کنید و بر روی Finish کلیک کنید تا Rule مورد نظر ایجاد شود.

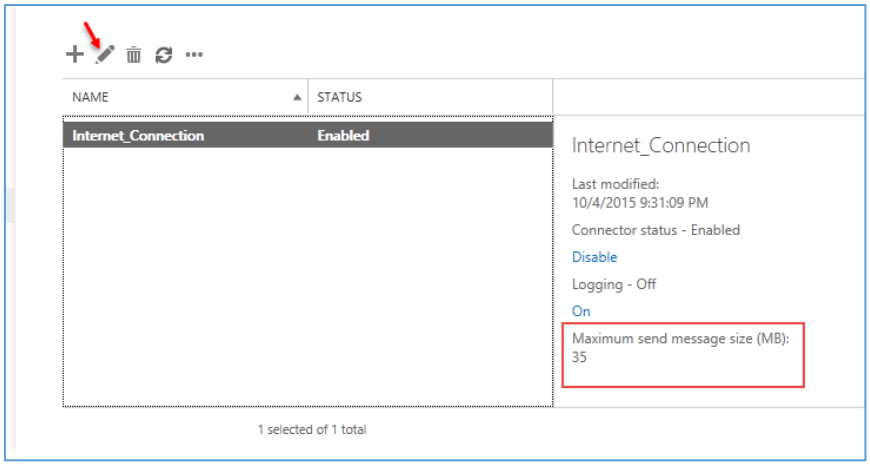
با این کار، کاربر می‌تواند از طریق Exchange به آدرسی در خارج از شبکه، ایمیل ارسال کند.



شکل ۱۴- ۱۵۸ ارسال ایمیل به خارج از شبکه

www.takbook.com

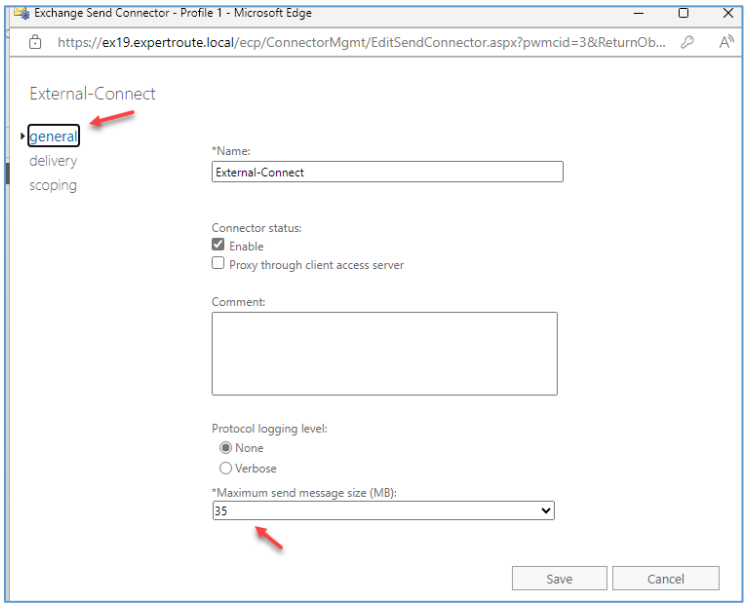
همان‌طور که در شکل ۱۴-۱۵۹، مشاهده می‌کنید، Rule مورد نظر ایجاد شده است، خوب به شکل نگاه کنید؛ در قسمت جزئیّات، حداکثر اندازه‌ی ارسال ایمیل برای کاربر، ۳۵ مگابایت به صورت پیش‌فرض در نظر گرفته شده است که برای تغییر آن بر روی آیکون مداد کلیک کنید.



شکل ۱۴- ۱۵۹ ارسال ایمیل به خارج از شبکه

به مانند شکل ۱۴-۱۶۰، بعد از ایجاد کانکشن آن را باز کنید و در قسمت General و از قسمت پایین می‌توانید حداکثر اندازه‌ی ایمیل را مشخّص کنید.

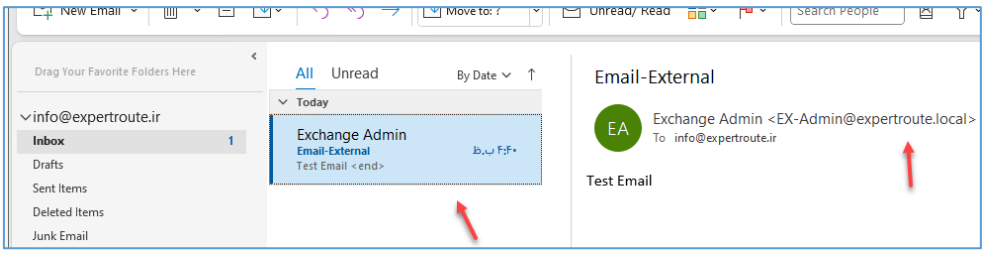
نکته: برای اینکه به سروری خارج از شبکه‌ی داخلی، ایمیل ارسال کنید به اینترنت نیاز دارید.



شکل ۱۴- ۱۶۰ ارسال ایمیل به خارج از شبکه

www.takbook.com

بعد از انجام مراحل بالا حالا می‌توانید از طریق Outlook به ایمیل های خارج از شبکه‌ی داخلی Email بزنید که در شکل ۱۴-۱۶۱، این موضوع مشخص شده است و ایمیل داخلی برای سرور خارجی expertroute.ir ارسال شده است.



شکل ۱۴- ۱۶۱ ارسال ایمیل به خارج از شبکه

۱۴-۲۰ ایجاد دومین خارجی و تنظیم آن در Exchange

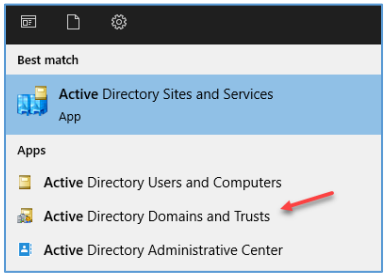
یکی از مهمترین بخش‌ها در سرور Exchange این است که باید سرور ایمیل خود را به دنیای اینترنت متصل کنید و به کاربران خود دسترسی دهید تا به اینترنت متصل شوند، برای این‌کار نیاز به چند چیز داریم:

۱- دومین خارجی که در اینترنت معتبر باشد.
۲- آدرس IP ثابت که باید از سرویس دهنده‌ی اینتنرت تهیه کنید.
۳- گواهینامه SSL برای آدرس خارجی
۴- تغییر DNSهای مهم در شبکه‌ی داخلی و خارجی

۱-۲۰-۱۴ تعریف دومین خارجی

برای شروع یک دومین خارجی با نام saharghateamin.com داریم که می‌خواهیم به سرور ایکسچنج خود متصل کنیم.

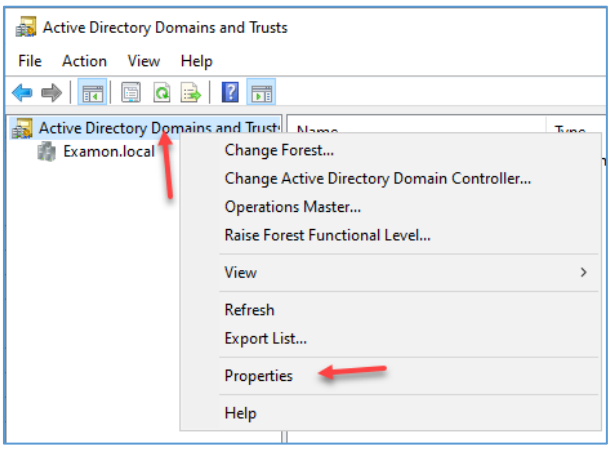
به مانند شکل ۱۴-۱۶۲، اولین کاری که انجام می‌دهیم این است که وارد سرور Active Directory شویم و سرویس Active Directory Domains and Trusts را اجرا کنید.



شکل ۱۴- ۱۶۲ ایجاد دومین خارجی

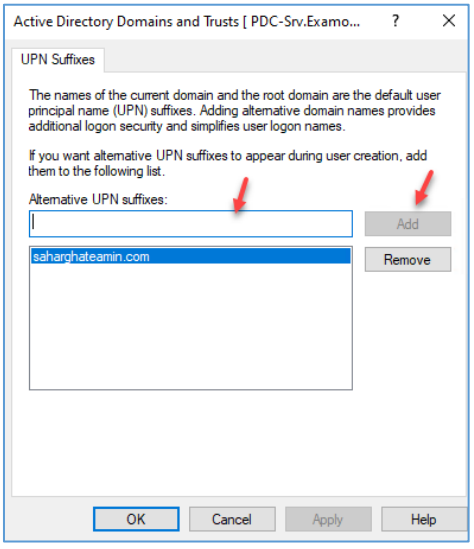
www.takbook.com

مانند شکل ۱۴-۱۶۳، بر روی نام اصلی کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۱۴- ۱۶۳ / ایجاد دومین خارجی

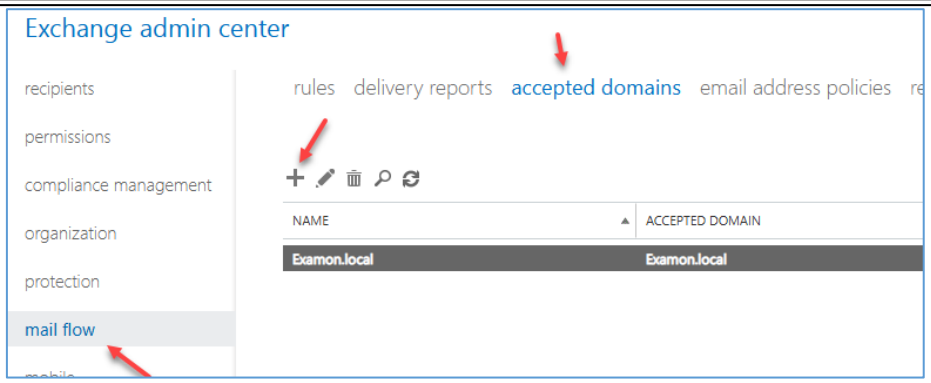
به مانند شکل ۱۴-۱۶۴، دومین خارجی خود را وارد و بر روی Add کلیک کنید تا به لیست اضافه شود.



شکل ۱۴- ۱۶۴ / ایجاد دومین خارجی

بعد از اضافه کردن دومین در Active Directory باید وارد سرور Exchange شوید و صفحه‌ی مدیریتی را باز کنید، به مانند شکل ۱۴-۱۶۵، برای اینکه بتوانیم دومین خارجی یا هر دومین دیگری را به لیست Exchange اضافه کنیم باید وارد mail flow شویم و به مانند شکل وارد تب Accepted domains شویم و بر روی + کلیک کنیم.

www.takbook.com



شکل ۱۴ - ۱۶۵ ایجاد دومین خارجی

در شکل ۱۴-۱۶۶، نام دومین را وارد کنید و بر روی Save کلیک کنید، توجه داشته باشید گزینه‌هایی که در زیر مشاهده می‌کنید برای:

Authoritative

سرور اکسچنج به‌طور کامل مسئول دریافت ایمیل‌ها برای دامنه مورد نظر است، ایمیل فقط به کاربرانی که در این دامنه تعریف شده‌اند، تحویل داده می‌شود، اگر ایمیلی به آدرسی که در سازمان شما وجود ندارد ارسال شود، بلافاصله رد می‌شود.

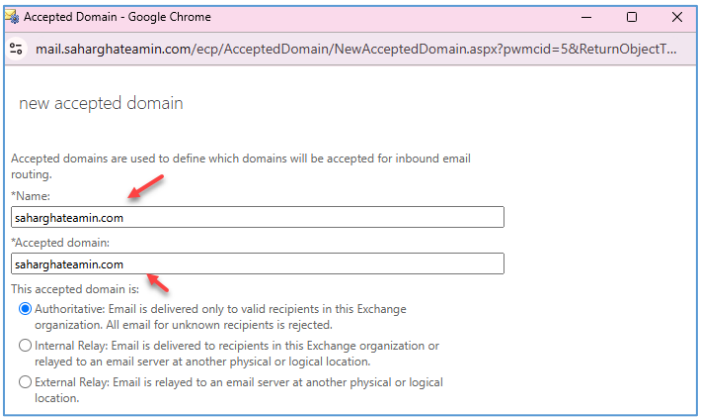
Internal Relay

ایمیل‌های دریافتی ابتدا در سرور اکسچنج بررسی می‌شوند، اگر گیرنده در سازمان شما تعریف شده باشد، ایمیل به کاربر تحویل داده می‌شود، اگر گیرنده تعریف نشده باشد، ایمیل به سرور دیگری (مانند سرور دیگر در یک شعبه) ارسال می‌شود.

External Relay

ایمیل‌های دریافتی به‌طور مستقیم به سرور دیگری در بیرون از سازمان شما ارسال (Relay) می‌شوند.

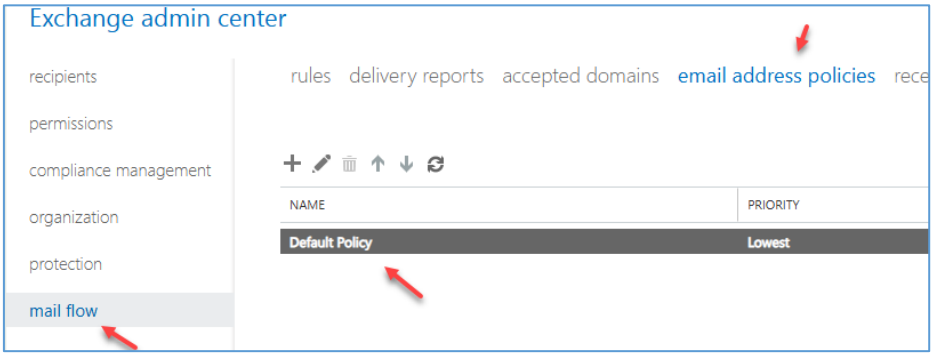
سرور اکسچنج هیچ مسئولیتی در تحویل نهایی ایمیل ندارد.



شکل ۱۴ - ۱۶۶ ایجاد دومین خارجی

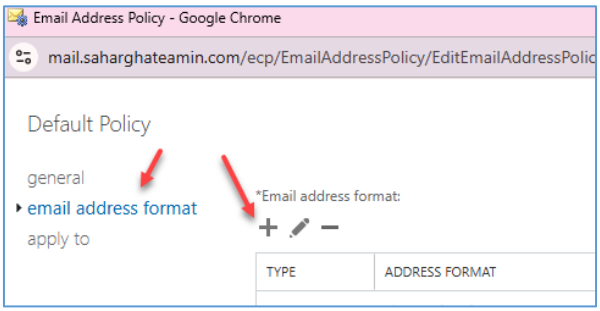
www.takbook.com

در ادامه کار باید Policy مربوط به تعریف دومین کاربران را دستکاری کنیم، برای این کار به مانند شکل ۱۶۷-۱٤، وارد تب email address policies شوید و بر روی Default Policy دو بار کلیک کنید.



شکل ۱۴- ۱۶۷ ایجاد دومین خارجی

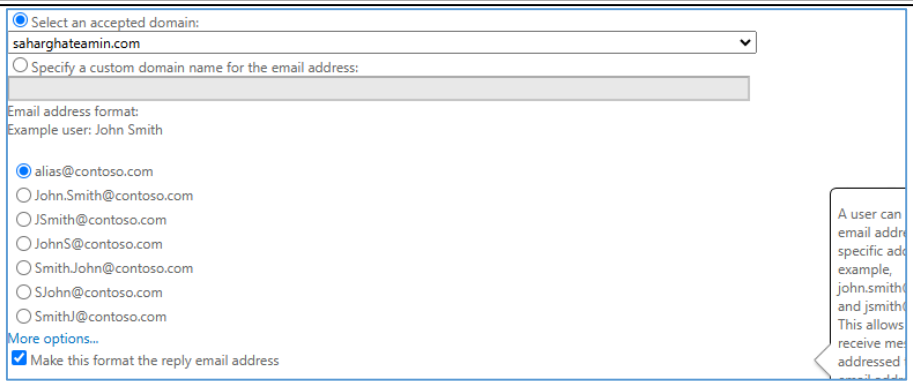
در ادامه کار به مانند شکل وارد email Address format شوید و بر روی + کلیک کنید.



شکل ۱۴- ۱۶۸ ایجاد دومین خارجی

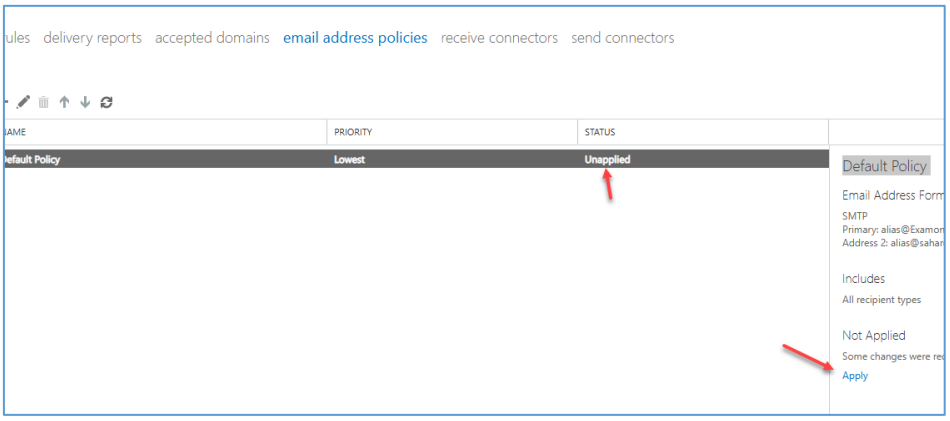
در شکل ۱۶۹-۱٤، باید دومین خارجی را انتخاب کنید و فرمت ایمیل را هم می‌توانید مشخص کنید و در آخر هم با انتخاب تیک گزینه‌ی Make this format the reply email address این آدرس به عنوان آدرس اصلی کاربران انتخاب خواهد شد.

www.takbook.com



شکل ۱۴- ۱۶۹ /ایجاد دومین خارجی

بعد از ایجاد تغییرات، برای اینکه این Policy به همه کاربران اعمال شود باید به مانند شکل ۱۴-۱۷۰، بر روی Apply کلیک و در صفحه باز شده بر روی Yes کلیک کنید.

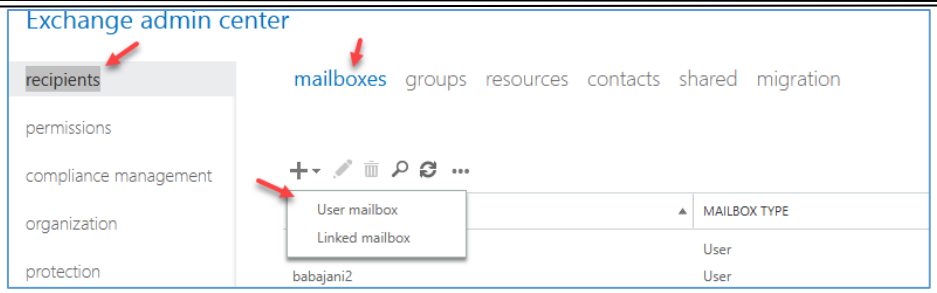


شکل ۱۴- ۱۷۰ /ایجاد دومین خارجی

۲-۲۰-۱۴ تعریف کاربر با دومین جدید

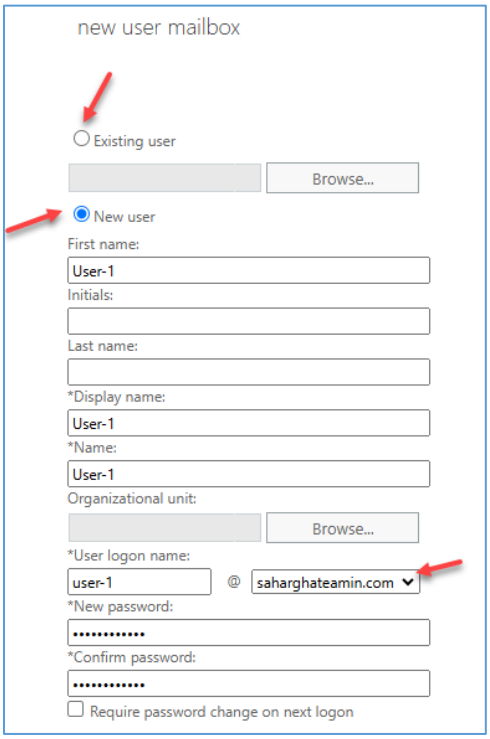
در ادامه کار باید نام کاربر جدید تعریف کنیم و تست بگیریم که آیا کاربر جدید با دومین تعریفی وارد سرور می‌شود یا نه، برای این کار به مانند شکل ۱۴-۱۷۱، وارد recipients شوید و وارد تب mailboxes شوید و گزینه‌ی User mailbox را انتخاب کنید.

www.takbook.com



شکل ۱۴- ۱۷۱ ایجاد دومین خارجی

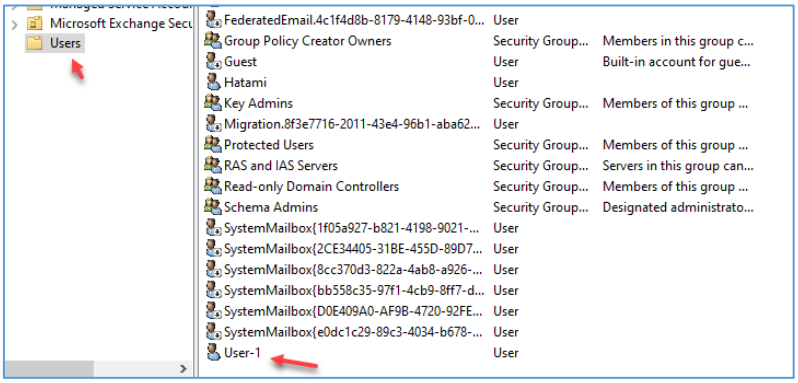
در ادامه کار به مانند شکل ۱٤-۱۷۲، اگر بخواهید کاربران خود را از Active Directory انتخاب کنیم باید بر روی Browse در قسمت Existing user کلیک کنید؛ وگرنه می‌توانید از خود Exchange بخواهید برای شما یک کاربر جدید ایجاد کند، پس گزینه‌ی New user را انتخاب می‌کنیم و نام کاربر مورد نظر را وارد و رمز عبور آن را مشخص می‌کنیم، فقط در قسمت User logon name باید نام دومین خارجی خود را انتخاب کنید و بر روی Save کلیک کنید.



شکل ۱۴- ۱۷۲ ایجاد دومین خارجی

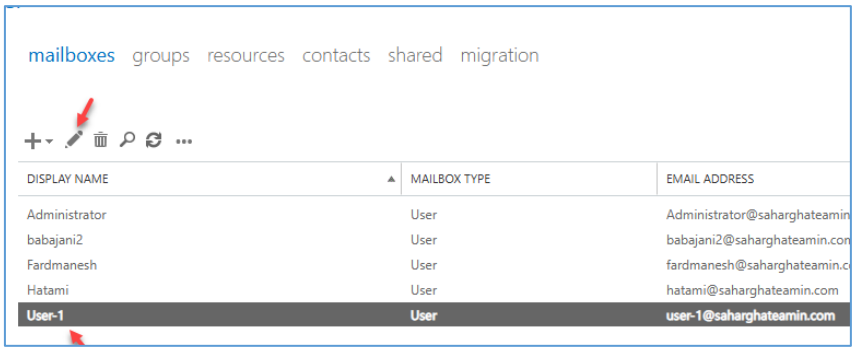
www.takbook.com

توجه داشته باشید که کاربری که از طریق Exchange ایجاد می‌کنید در Active directory هم به صورت اتوماتیک ایجاد می‌شود که در شکل ۱۴-۱۷۳، این موضوع را مشاهده می‌کنید.



شکل ۱۴- ۱۷۳ / ایجاد دومین خارجی

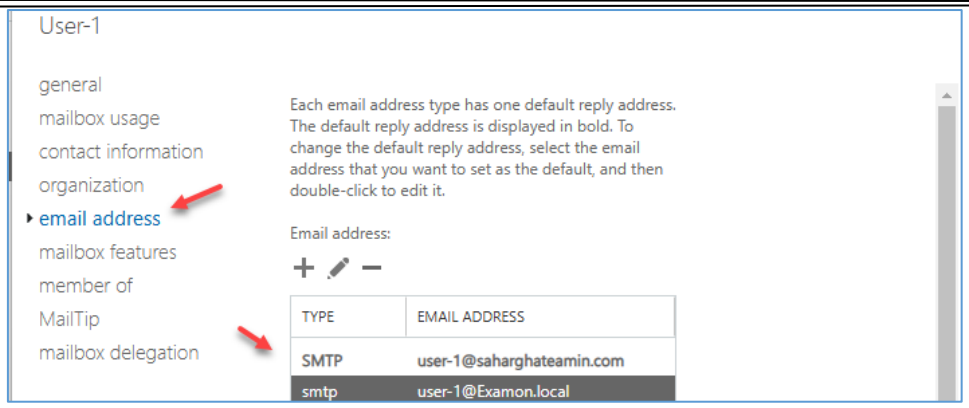
در ادامه کار به مانند شکل ۱۴-۱۷۴، بعد از ایجاد کاربر جدید آن را انتخاب و بر روی آیکون ویرایش کلیک کنید.



شکل ۱۴- ۱۷۴ / ایجاد دومین خارجی

اگر به مانند شکل ۱۴-۱۷۵، وارد تب Email Address شوید مشاهده می‌کنید که هر دو دومین داخلی و خارجی برای کاربر جدید تعریف شده است، یعنی کاربر جدید برای ورود به ایمیل خود در شبکه داخلی از آدرس داخلی و در شبکه خارجی از آدرس خارجی استفاده می‌کند.

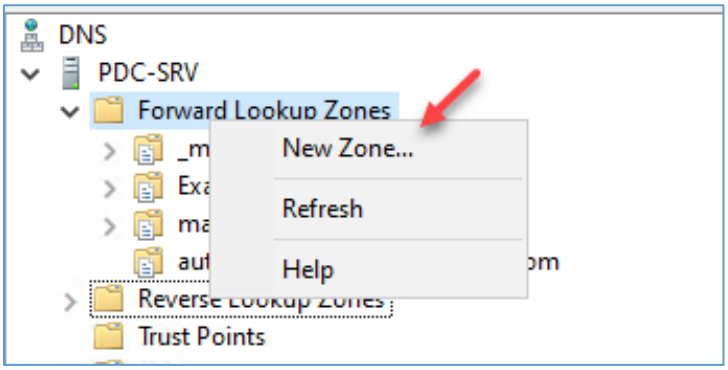
www.takbook.com



شکل ۱۴- ۱۷۵ ایجاد دومین خارجی

۳-۲۰-۱٤ تنظیم DNS داخلی و خارجی

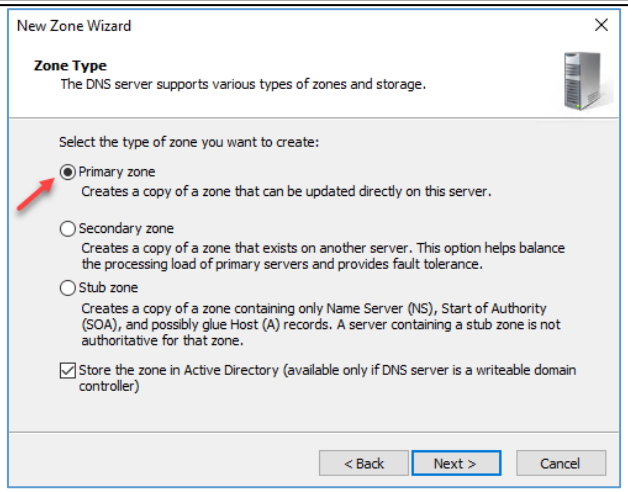
بعد از انجام تنظیمات قبلی حالا باید DNS داخلی و خارجی را برای ایکسچنج تنظیم کنیم، برای این کار اول وارد سرور Active Directory می‌شویم و سرویس DNS را اجرا می‌کنیم و در شکل ۱٤-۱۷٦، بر روی Forward Lookup Zones کلیک راست می‌کنیم و گزینه‌ی New Zone را انتخاب می‌کنیم.



شکل ۱۴- ۱۷۶ تنظیم DNS داخلی و خارجی

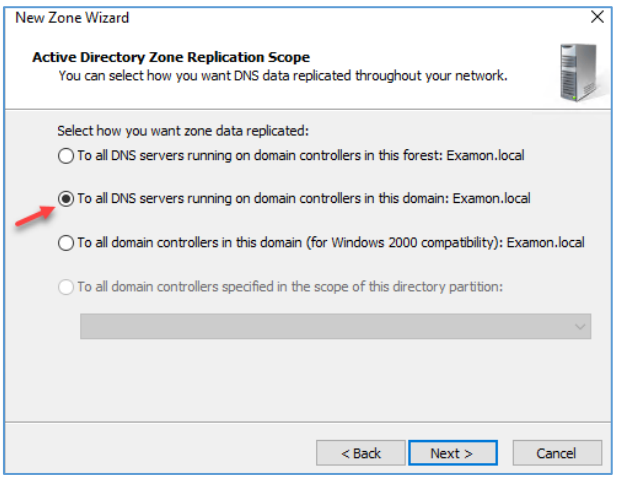
در شکل ۱٤-۱۷۷، گزینه‌ی Primary zone را انتخاب کنید.

www.takbook.com



شکل ۱۴- ۱۷۷ تنظیم DNS داخلی و خارجی

در شکل ۱۴–۱۷۸، بر روی Next کلیک کنید.

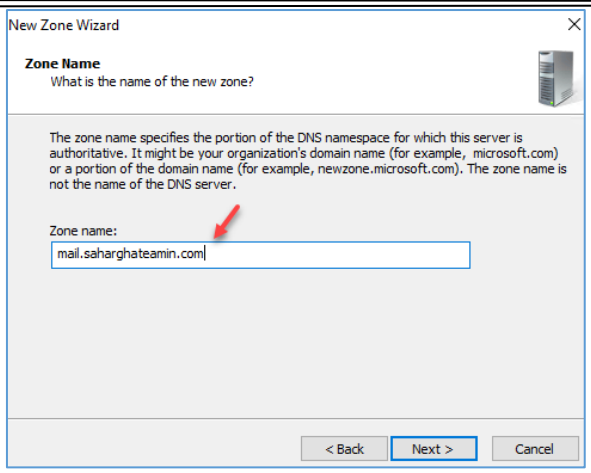


شکل ۱۴- ۱۷۸ تنظیم DNS داخلی و خارجی

در شکل ۱۴–۱۷۹، باید آدرس دومین خارجی را وارد کنید که این آدرس همان آدرسی است که کلاینت‌ها از طریق آن قادر هستند به شرکت شما متصل شوند.

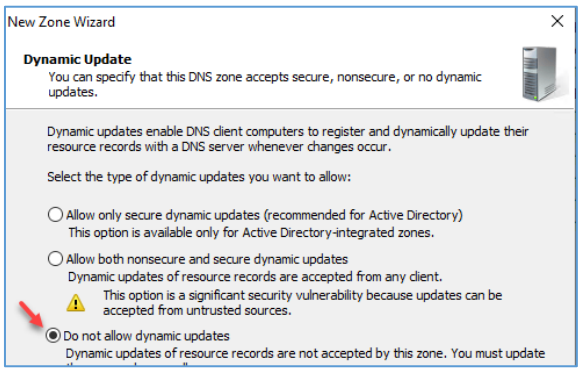
به این نکته توجه کنید که این نام در DNS خارجی هم باید تعریف شود که در ادامه انجام خواهیم داد.

www.takbook.com



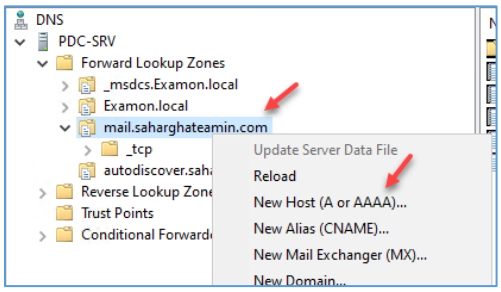
شکل ۱۴- ۱۷۹ تنظیم DNS داخلی و خارجی

در شکل ۱۴-۱۸۰، نیازی به آپدیت Zone مورد نظر نیست و گزینه‌ی آخر را انتخاب کنید و بر روی Next کلیک و در صفحه‌ی آخر هم بر روی Finish کلیک کنید.



شکل ۱۴- ۱۸۰ تنظیم DNS داخلی و خارجی

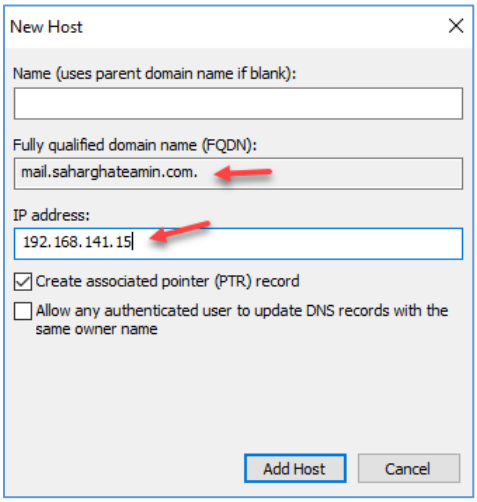
بعد از ایجاد Zone مورد نظر به مانند شکل ۱۴-۱۸۱، بر روی آن کلیک راست کنید و گزینه‌ی AAA را انتخاب کنید.



شکل ۱۴- ۱۸۱ تنظیم DNS داخلی و خارجی

www.takbook.com

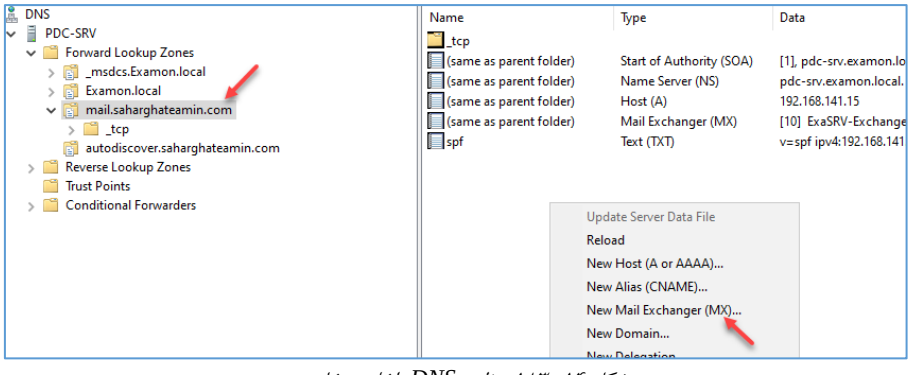
در شکل ۱۴-۱۸۲، باید IP address مربوط به سرور ایکسچنج خود را وارد کنید و بر روی Add Host کلیک کنید.



شکل ۱۴-۱۸۲ تنظیم DNS داخلی و خارجی

در ادامه باید دو رکرود دیگر هم تعریف کنیم، یکی MX و دیگری SPF که از رکورد MX در DNS برای تعیین سرورهای ایمیل که مسئول دریافت ایمیل برای یک دامنه خاص هستند، استفاده می‌شود. این رکورد مشخص می‌کند که ایمیل‌هایی که به دامنه شما ارسال می‌شوند، باید به کدام سرور تحویل داده شوند و همچنین رکورد SPF یک مکانیسم است که به جلوگیری از جعل آدرس‌های ایمیل (spoofing) و اسپم کمک می‌کند. این رکورد به سرورهای ایمیل می‌گوید که کدام سرورها مجاز به ارسال ایمیل از طرف دامنه خاص هستند.

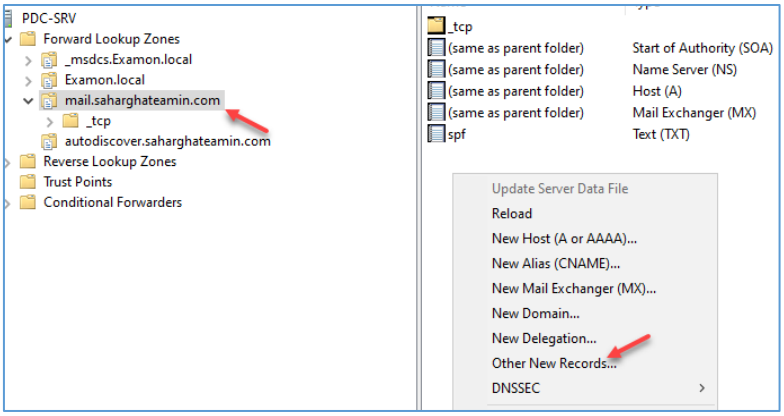
برای تعریف رکورد MX به مانند شکل ۱۴-۱۸۳، بر روی نام دامنه خود کلیک راست کنید و گزینه‌ی New Mail Exchanger (MX) را انتخاب کنید.



شکل ۱۴-۱۸۳ تنظیم DNS داخلی و خارجی

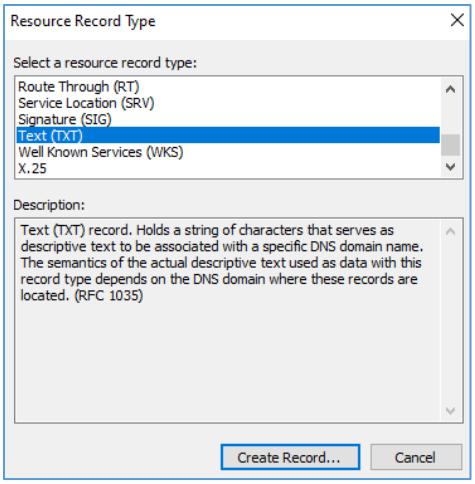
www.takbook.com

در شکل ۱۴-۱۸۴، باید بر روی Browse کنید و آدرس سرور Exchange داخلی خود را انتخاب و بر روی OK کلیک کنید، در ادامه کار باید رکورد SPF را ایجاد کنیم برای این کار بر روی آدرس اصلی سرور خود کلیک راست کنید و گزینه‌ی Other New Records را انتخاب کنید.



شکل ۱۴- ۱۸۴ تنظیم DNS داخلی و خارجی

در شکل ۱۴-۱۸۵، گزینه‌ی Text را انتخاب کنید و بر روی Create Record کلیک کنید.

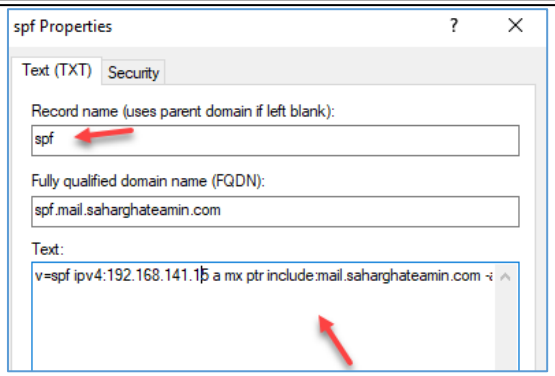


شکل ۱۴- ۱۸۵ تنظیم DNS داخلی و خارجی

در شکل ۱۴-۱۸۶ نام آن را spf در نظر بگیرید و مقدار Text را برابر با مقدار زیر قرار بدهید.

v=spf ipv4:192.168.141.15 a mx ptr include:mail.saharghateamin.com -all

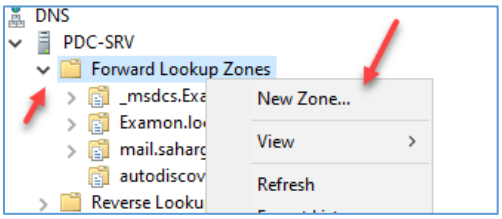
www.takbook.com



شکل ۱۴- ۱۸۶ تنظیم DNS داخلی و خارجی

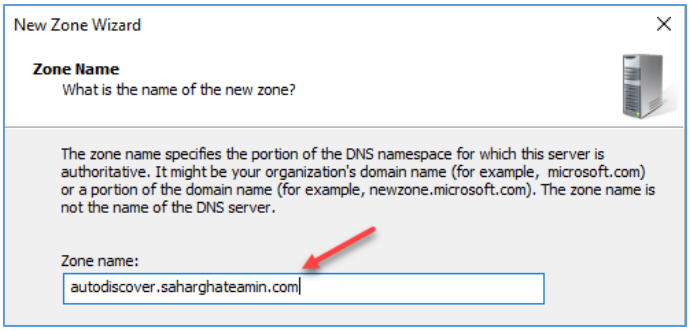
بعد از ایجاد Zone مربوط به mail حالا باید Zone مربوط Autodiscover را تعریف کنیم، Autodiscover در سرور Exchange یک سرویس کلیدی است که برای ساده‌سازی تنظیمات و پیکربندی کلاینت‌ها (مانند Outlook) طراحی شده است. این سرویس به صورت خودکار تنظیمات موردنیاز برای اتصال به سرور Exchange را فراهم می‌کند و نیازی به تنظیمات دستی را کاهش می‌دهد.

برای انجام این کار به مانند شکل ۱۴–۱۸۷، بر روی نام سرور کلیک راست و گزینه‌ی New Zone را انتخاب کنید.



شکل ۱۴- ۱۸۷ تنظیم DNS داخلی و خارجی

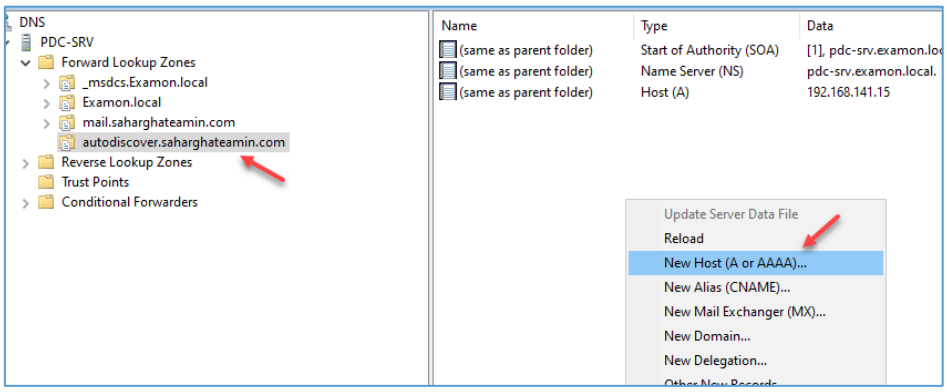
در ادامه به مانند شکل ۱۴–۱۸۸، نام سرور را باید به صورت autodiscover.saharghateamin.com وارد کنید که بعد از نام Autodiscover باید نام سرور دومین خود را وارد کنید.



شکل ۱۴- ۱۸۸ تنظیم DNS داخلی و خارجی

www.takbook.com

بعد از ایجاد Zone مورد نظر وارد آن شوید و به مانند شکل ۱۴-۱۸۹، گزینه‌ی AAA را انتخاب کنید.

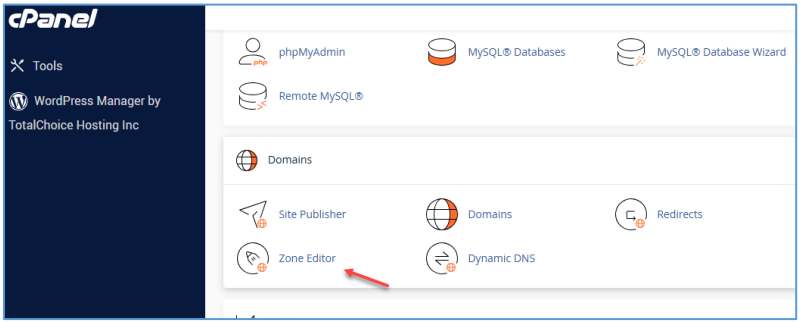


شکل ۱۴- ۱۸۹ تنظیم DNS داخلی و خارجی

در صفحه‌ی باز شده، فقط کافی است آدرس سرور Exchange را وارد کنید و بر روی Add Host کلیک کنید.

بعد از اینکه DNS داخلی را آماده کردیم باید وارد مهمترین بخش کار شویم، یعنی DNS خارجی که می‌تواند دارای Cpanel یا Direct Admin باشد و باید وارد آنها شویم و تنظیمات مورد نظر را برای سرور Exchange تغییر دهیم.

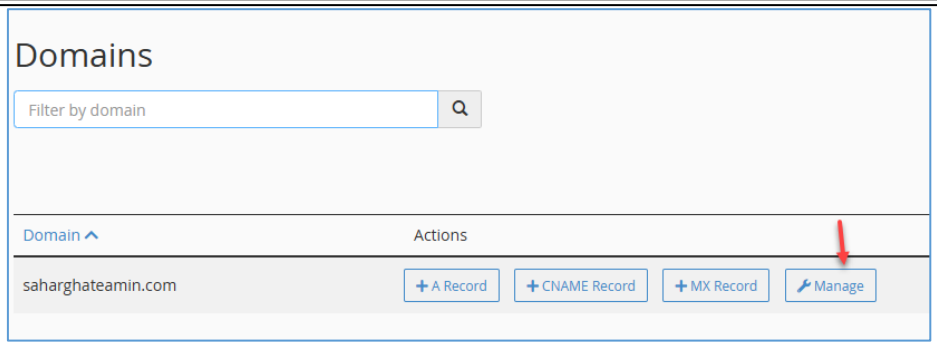
برای اینکه DNS مربوط به دومین saharghateamin.com را تنظیم کنیم باید به مانند شکل ۱۴-۱۹۰، گزینه‌ی Zone Editor را انتخاب کنید تا وارد تنظیمات DNS شوید.



شکل ۱۴- ۱۹۰ تنظیم DNS خارجی

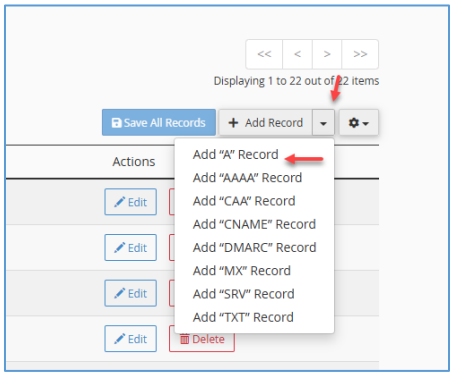
در ادامه کار و به مانند شکل ۱۴-۱۹۱، بر روی Manage کلیک کنید.

www.takbook.com



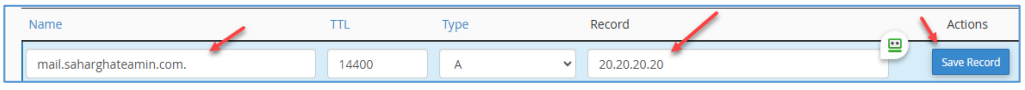
شکل ۱۴- ۱۹۱ تنظیم DNS خارجی

برای شروع کار به مانند شکل ۱۴-۱۹۲، باید دو تا A Record ایجاد کنید و دو آدرس mail.saharghateadmin.com و Autodiscover. saharghateadmin.com را به آدرس IP شبکه داخلی متصل می‌کنیم.

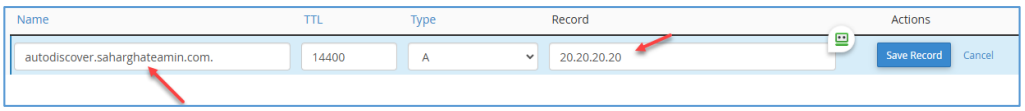


شکل ۱۴- ۱۹۲ تنظیم DNS خارجی

در شکل ۱۴-۱۹۳ و ۱۴-۱۹۴، باید آدرس سرور را به همراه آدرس IP ثابت شبکه‌ی داخلی خود که قرار است به سمت سرور ایکسچنج NAT شود را انتخاب کنید، در هر دو شکل هر دو آدرس مورد نظر به همراه آدرس IP ثابت تعریف شده است.



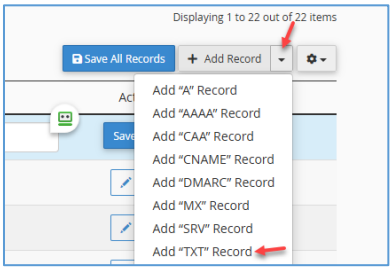
شکل ۱۴- ۱۹۳ تنظیم DNS خارجی



شکل ۱۴- ۱۹۴ تنظیم DNS خارجی

www.takbook.com

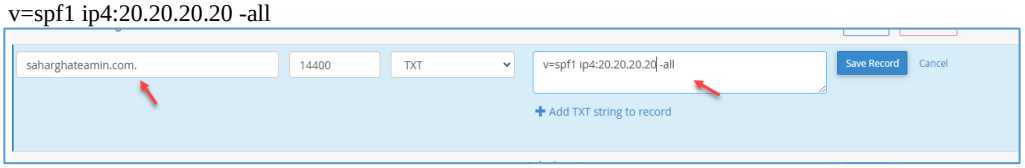
بعد از اینکه A رکورد ایجاد کردید باید یک رکورد SPF ایجاد کنید که برای این کار باید به مانند شکل ۱۴-۱۹۵، از رکورد TXT استفاده کنید.



شکل ۱۴- ۱۹۵ تنظیم DNS خارجی

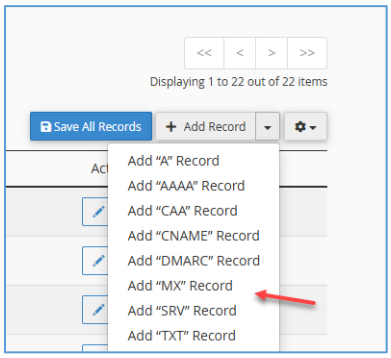
در شکل ۱۴-۱۹۶، باید نام دومین را در قسمت اول و متن زیر را که د رآن باید آدرس IP ثابت شبکه خود را وارد کنید را در قسمت مشخص شده قرار دهید.

v=spf1 ip4:20.20.20.20 -all



شکل ۱۴- ۱۹۶ تنظیم DNS خارجی

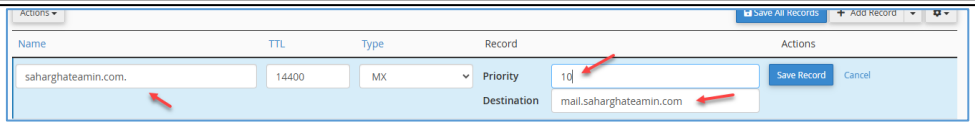
در آخر کار هم به مانند شکل ۱۴-۱۹۷، باید یک رکورد MX ایجاد کنیم و آن را به سمت آدرس mail.saharghateadmin.com ارسال کنید، برای این کار بر روی Add MX کلیک کنید.



شکل ۱۴- ۱۹۷ تنظیم DNS خارجی

به مانند شکل ۱۴-۱۹۸، در قسمت اول نام دومین اصلی و شاخه را وارد کنید، و در قسمت Destination آدرس mail.saharghateamin.com را وارد کنید و مقدار Priority را برابر 10 قرار دهید.

www.takbook.com



شکل ۱۴- ۱۹۸ تنظیم DNS خارجی

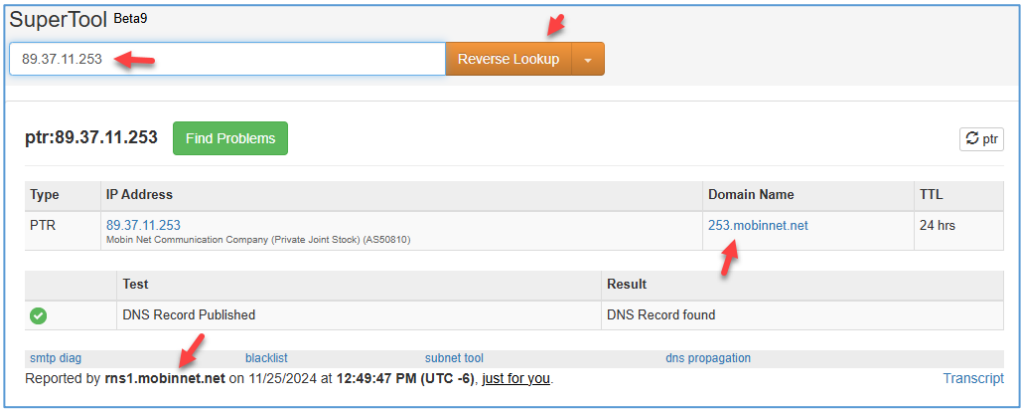
تمام اطلاعاتی که در دومین خارجی وارد کردید را ذخیره کنید.

۱۴-۲۰-۴ تعریف رکورد PTR

رکورد PTR (Pointer Record) یکی از انواع رکوردهای DNS است که برای انجام Reverse DNS Lookup استفاده می‌شود. این رکورد، یک آدرس IP را به نام دامنه متناظر آن نگاشت می‌کند، بسیاری از سرورهای ایمیل (مثل Gmail) از رکورد PTR برای بررسی صحت فرستنده استفاده می‌کنند تا از اسپم جلوگیری شود.

این بحث چون مهم بوده آن را با قسمت قبلی جدا کردم، شما وقتی یک آدرس ثابت از شرکت ارائه دهنده‌ی اینترنت دریافت می‌کنید باید بررسی کنید که رکورد PTR آن آدرس IP به چه صورت است.

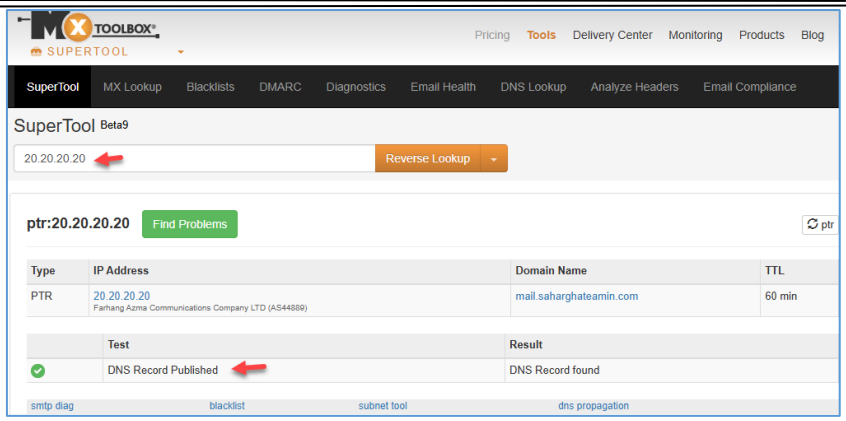
مثلاً یک IP ثابت داریم (89.37.11.253) و می‌خواهیم بفهمیم که این آدرس بر روی چه سروری قرار دارد، برای بررسی این موضوع وارد سایت mxtoolbox.com که در آخر همین فصل توضیح دادم شوید و به مانند شکل ۱۴-۱۹۹، آدرس IP مورد نظر را وارد و بر روی Reverse Lookup کلیک کنید، همان‌طور که در خروجی مشاهده می‌کنید آدرس مورد نظر به آدرس 253.mobinnet.net متصل شده است و این یعنی اینکه آدرس IP مورد نظر برای شرکت مبین نت است و شما باید با مبین نت تماس بگیرید و بگویید که مقدار PTR این آدرس را به آدرس ایمیل شما تغییر دهد.



شکل ۱۴- ۱۹۹ تعریف رکورد PTR

که من هم برای آدرس خود یعنی 20.20.20.20 همین کار را انجام دادم و این آدرس به سمت سرور ایمیل خودمان تغییر حالت داده است که در شکل ۱۴-۲۰۰، این موضوع را مشاهده می‌کنید.

www.takbook.com



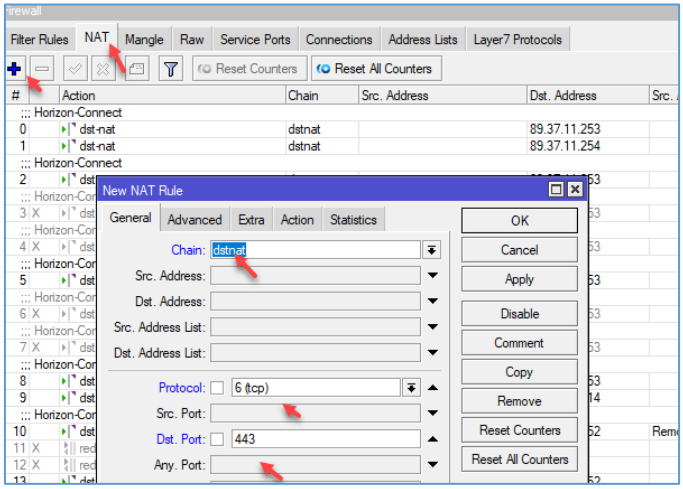
شکل ۱۴- ۲۰۰ تعریف رکورد PTR

۱۴-۲۰-۵ تنظیم فایروال برای ورود به شبکه داخلی

برای اینکه کاربران به راحتی بتوانند از طریق آدرسی که در دومین خارجی مشخص کردیم به ایمیل دسترسی داشته باشند، باید وارد روتر یا فایروال خود شوید و آدرس خارجی را به سرور ایکسچنج داخلی NAT یا Forward کنید.

توجه داشته باشید، برای پورت‌ها 587,25,443 باید تنظیمات را انجام دهید.

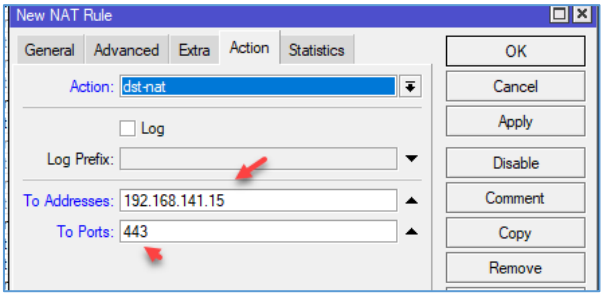
برای این‌کار ما از روتر میکروتیک استفاده می‌کنیم، در روتر میکروتیک وارد قسمت فایروال شوید و وارد تب NAT شوید و بر روی آیکون + کلیک کنید، به مانند شکل ۱۴-۲۰۱، در قسمت Chain گزینه‌ی dstnat که اشاره به منابع خارجی ورودی به شبکه دارد و در قسمت Protocol گزینه‌ی TCP و در قسمت پورت هم باید پورت 443 را وارد کنیم.



شکل ۱۴- ۲۰۱ ورود به شبکه داخلی

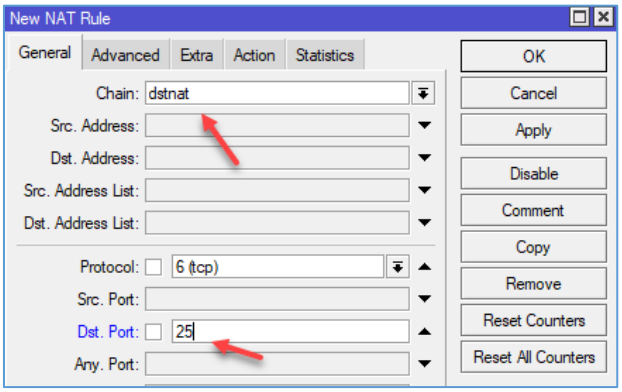
www.takbook.com

در ادامه کار طبق شکل ۱۴-۲۰۲، وارد تب Action شوید و از قسمت Action گزینه‌ی dst-nat را انتخاب کنید و در قسمت To Addresses آدرس سرور Exchange که آدرس آن 192.168.141.15 را وارد کنید و در قسمت پورت هم باید پورت 443 را وارد کنید.



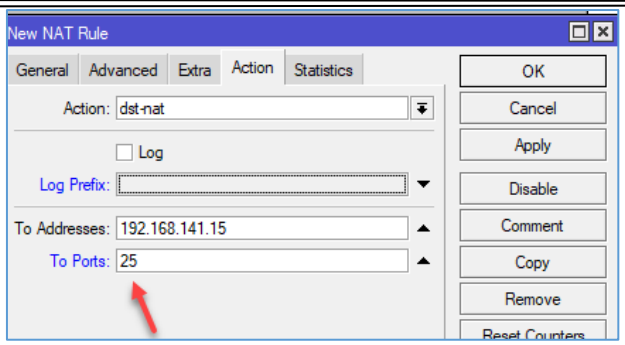
شکل ۱۴- ۲۰۲ ورود به شبکه داخلی

بعد از ایجاد این Rule باید دقیقاً همین کار را برای پورت 25 انجام دهید، برای این کار به مانند شکل ۱۴-۲۰۳ و ۱۴-۲۰۴، از Rule قبلی یک Copy تهیه کنید و به مانند شکل فقط مقدار پورت آن را به 25 تغییر دهید.



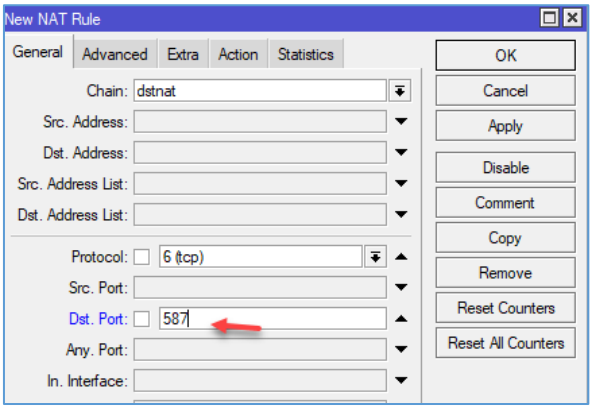
شکل ۱۴- ۲۰۳ ورود به شبکه داخلی

www.takbook.com

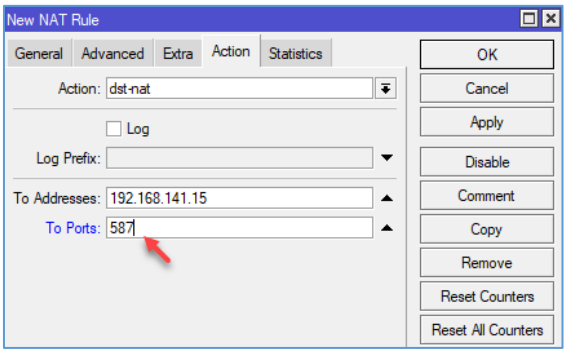


شکل ۱۴- ۲۰۴ ورود به شبکه داخلی

به مانند شکل ۱۴–۲۰۵ و ۱۴–۲۰۶، برای پورت 587 هم همین کار را انجام دهید.



شکل ۱۴- ۲۰۵ ورود به شبکه داخلی



شکل ۱۴- ۲۰۶ ورود به شبکه داخلی

www.takbook.com

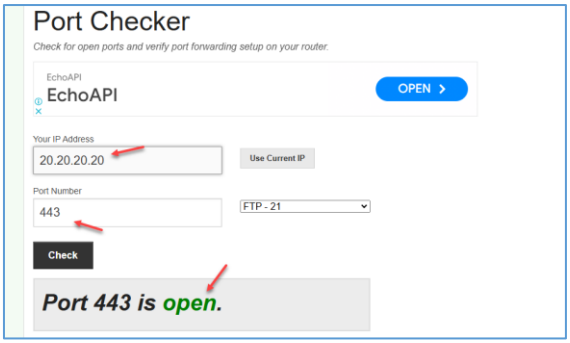
همان‌طور که می‌دانید پورت ۵۸۷ به‌عنوان یکی از پورت‌های استاندارد در پروتکل SMTP (Simple Mail Transfer Protocol) استفاده می‌شود. این پورت مخصوص ارسال ایمیل‌ها از سمت کلاینت به سرور ایمیل طراحی شده است و به‌طور گسترده‌ای برای ارسال ایمیل‌های امن به کار می‌رود.

پورت ۲۵ یکی از قدیمی‌ترین و اصلی‌ترین پورت‌ها در پروتکل SMTP است که برای انتقال ایمیل‌ها طراحی شده است، این پورت عمدتاً برای ارتباط بین سرورهای ایمیل (SMTP Relay) استفاده می‌شود.

پورت ٤٤٣ استانداردی است که برای انتقال داده‌ها از طریق HTTPS (Hypertext Transfer Protocol Secure) استفاده می‌شود. این پورت برای مرور وب امن و رمزنگاری‌شده به کار می‌رود.

به این نکته مهم توجه کنید که در فایروال مربوط به سرورها باید به این پورت‌ها دسترسی بدهید تا مشکلی در ارتباط ایجاد نشود.

با استفاده از آدرس portchecker.co می‌توانید چک کنید که NAT که ایجاد کرده‌اید برای پورت مورد نظر فعال شده است یا خیر، مثلاً در شکل ۱٤۰–۲۰۷، با استفاده از آدرس ثابت و مشخص کردن پورت 443 مشاهده می‌کنید پورت مورد نظر باز است و این یعنی اینکه کار خود را به درستی انجام دادیم.



شکل ۱۴- ۲۰۷ ورود به شبکه داخلی

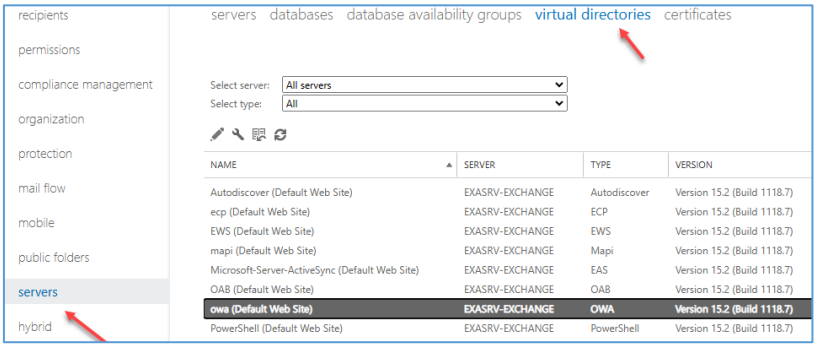
٦-۲۰-۱٤ تغییر آدرس داخلی و خارجی

برای اینکه بتوانیم ایمیل Exchange خود را از طریق اینترنت به راحتی مشاهده کنیم باید آدرس‌های خارجی را تغییر دهیم، همان‌طور که در قسمت DNS بررسی کردیم آدرس DNS اصلی ما برای متصل شدن به سرور mail.saharghateamin.com است و باید این آدرس را در تک تک دایرکتوری‌ها وارد کنیم.

دایرکتوری یعنی در Exchange Server، بخش Servers و تب Virtual Directories نقش مهمی در مدیریت و تنظیم سرویس‌هایی که کاربران برای دسترسی به سرور Exchange از آنها استفاده می‌کنند، دارد. این قسمت به شما اجازه می‌دهد تا تنظیمات دسترسی به سرویس‌های مختلف مانند Outlook Web App (OWA)، ActiveSync، و Autodiscover را پیکربندی کنید که شکل ۱٤–۲۰۸، گویای این موضوع است، هر کدام از این دایرکتوری‌ها دارای آدرس داخلی و خارجی هستند که باید آنها را طبق تنظیمات خود تغییر

www.takbook.com

دهیم، بهترین راه این است که از یک فایل PowerShell استفاده کنیم تا آدرس دلخواه ما به صورت اتوماتیک تغییر کند.

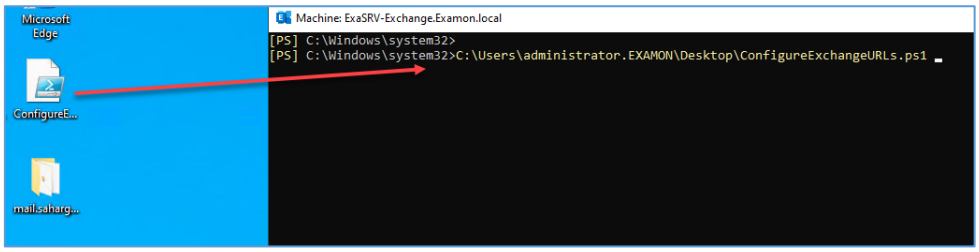


شکل ۱۴- ۲۰۸ تغییر آدرس داخلی و خارجی

برای شروع کار از طریق لینک زیر فایل PowerShell را دانلود کنید:

https://histaco.com/PowerShell/ConfigureExchangeURLs.ps1

در ادامه کار وارد سرور Exchange شوید و سرویس Management Shell را اجرا کنید، و به مانند شکل ۱۴-۲۰۹، فایلی که دانلود کردید را بکشید و در خط فرمان رها کنید.



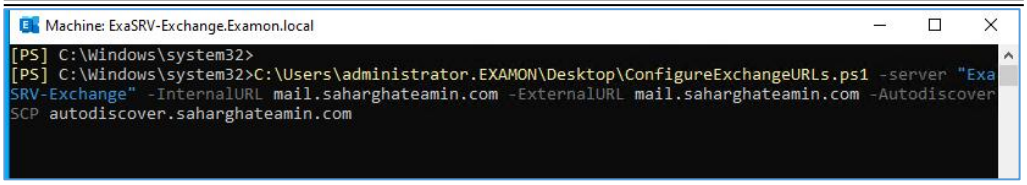
شکل ۱۴- ۲۰۹ تغییر آدرس داخلی و خارجی

در ادامه کار باید دستور زیر را در انتهای فایل بالا قرار دهید و اجرا کنید تا به صورت اتوماتیک آدرس‌ها تغییر کنند، توجه داشته باشید شما باید به جای mail.saharghateamin.com و autodiscover.saharghateamin.com باید آدرس‌های مورد نظر خود را وارد کنید، به جای ExaSRV-Exchange هم باید نام سرور Exchange خود را وارد کنید.

-server "ExaSRV-Exchange" -InternalURL mail.saharghateamin.com -ExternalURL mail.saharghateamin.com -AutodiscoverSCP autodiscover.saharghateamin.com

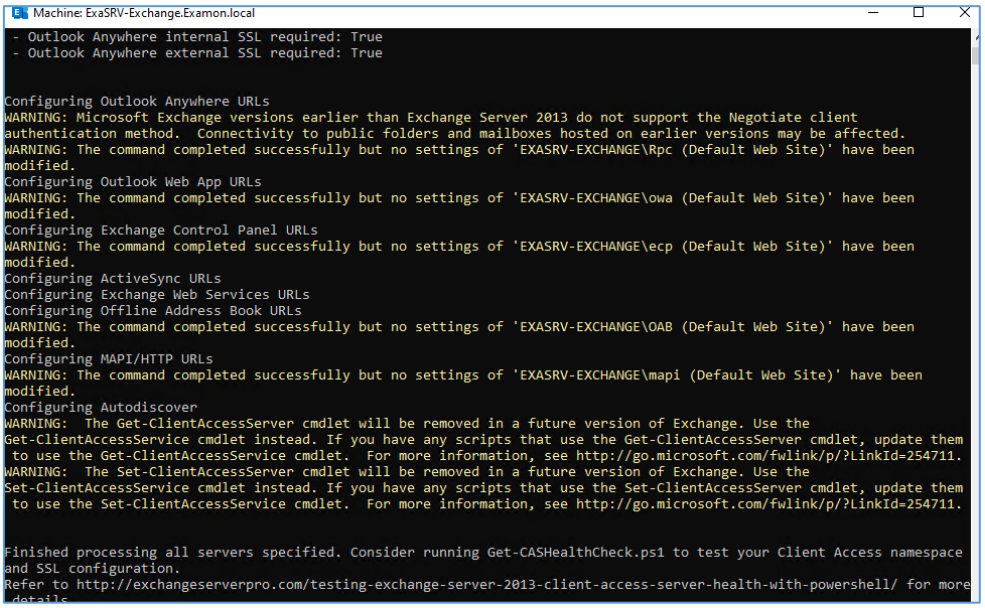
یعنی دستور نهایی بصورت شکل ۱۴-۲۱۰، خواهد بود که با فشار دادن دکمه Enter به صورت اتوماتیک عملیات انجام خواهد شد.

www.takbook.com



شکل ۱۴- ۲۱۰ تغییر آدرس داخلی و خارجی

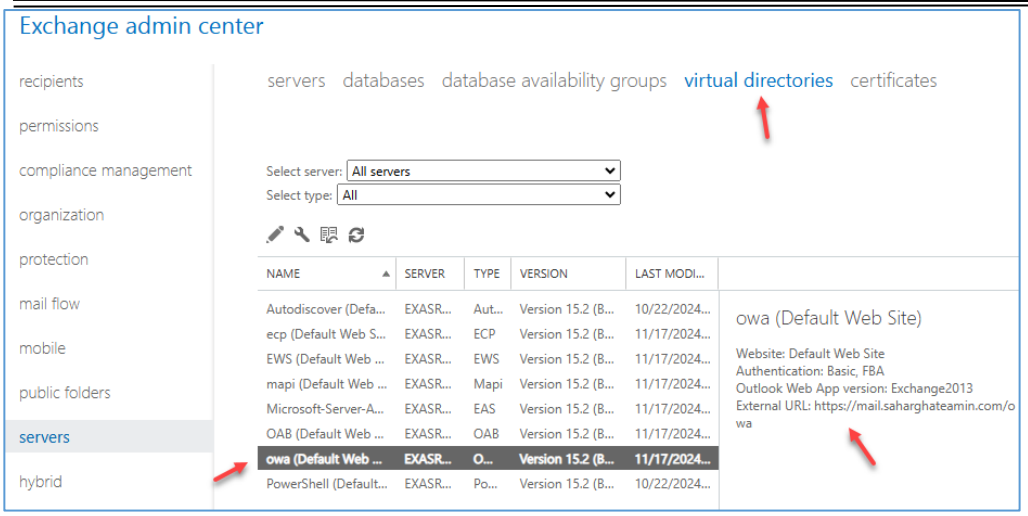
همان‌طور که در شکل ۱۴-۲۱۱، مشاهده می‌کنید تغییرات به درستی انجام شده است.



شکل ۱۴- ۲۱۱ تغییر آدرس داخلی و خارجی

حالا می‌توانید به مانند شکل ۱۴-۲۱۲، وارد تب virtual directories شوید و بر روی یکی از دایرکتوری‌ها مثلاً OWA کلیک کنید که در قسمت کناری آن آدرس External URL نوشته شده است که همان آدرس خارجی است که در قسمت قبل تعریف کردیم.

www.takbook.com



شکل ۱۴- ۲۱۲ تغییر آدرس داخلی و خارجی

۷-۲۰-۱٤ ایجاد گواهینامه خارجی برای سرور Exchange

تا به این مرحله توانستیم DNS داخلی و خارجی را تعریف کنیم، فایروال را تنظیم کنیم و همچنین آدرس‌های خارجی را در سرور Exchange ایجاد کنیم، در مرحله آخر می‌خواهیم برای دو آدرسی که با هم ایجاد کردیم یک گواهینامه SSL ایجاد کنیم تا سرویس ما به درستی اجرا شود.

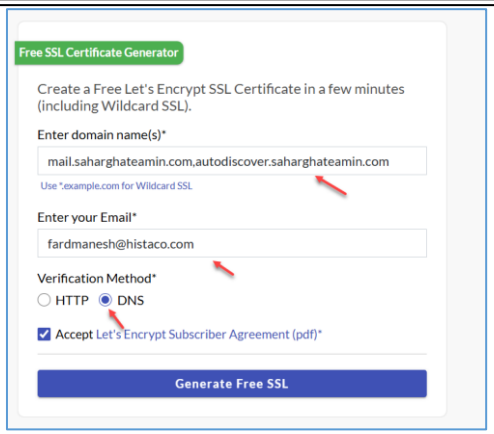
بهترین حالت این است که این گواهینامه را از یک سرویس دهنده‌ی گواهینامه SSL خریداری کنید و تا یک سال آن را داشته باشید، اما برای محیط آزمایشگاهی و برای اینکه هزینه نکنید باید از سایت رایگان استفاده کنید، برای شروع وارد سایت زیر شوید.

https://sslfree.io/

توجه داشته باشید سایتی که از آن قرار است SSL تهیه کنید باید چند آدرس را پشتیبانی کند یعنی Wildcard SSL باشد، این سایت به صورت رایگان این‌کار را انجام می‌دهد و یک گواهینامه سه ساله در اختیار ما می‌گذارد.

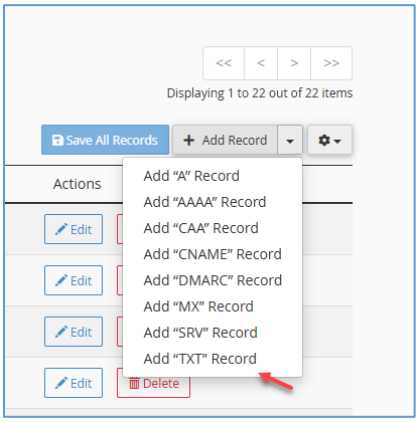
به مانند شکل ۱٤-۲۱۳، در قسمت اول باید هر دو آدرسی که در قسمت قبل مشخص کردیم را در این قسمت وارد کنید و در قسمت دوم یک آدرس ایمیل به دلخواه وارد کنید و در قسمت Verification Method باید گزینه‌ی DNS را انتخاب کنید و بر روی Generate Free SSL کلیک کنید.

www.takbook.com



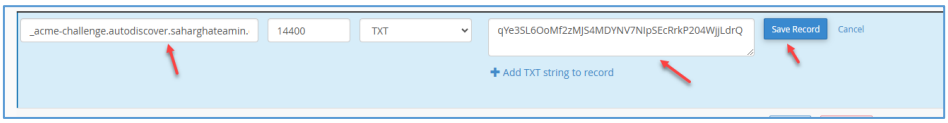
شکل ۱۴- ۲۱۳ ایجاد گواهینامه خارجی

وقتی که بر روی Generate Free SSL کلیک کنید دو آدرس DNS به صورت شکل ۱۴-۲۱۷، به شما نمایش داده می‌شود که این دو آدرس از نوع TXT هستند و باید در سرور دومین شما تعریف شوند تا این قسمت مورد تایید قرار بگیرد، وارد سرور دومین شوید و در بخش DNS به مانند شکل ۱۴-۲۱۸، بر روی Add TXT کلیک کنید.



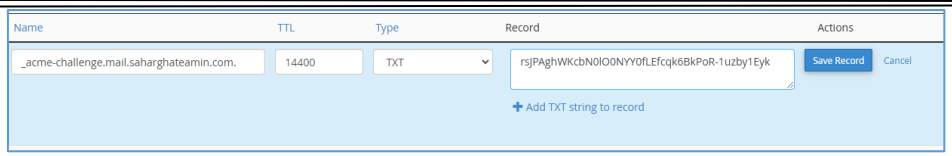
شکل ۱۴- ۲۱۴ ایجاد گواهینامه خارجی

به مانند شکل ۱۴-۲۱۵ و ۱۴-۲۱۶، باید دو آدرس مورد نظر را هر کدام جداگانه در فایل TXT قرار دهید.



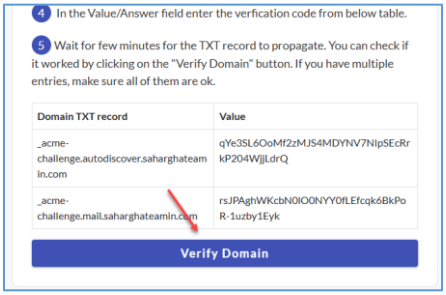
شکل ۱۴- ۲۱۵ ایجاد گواهینامه خارجی

www.takbook.com



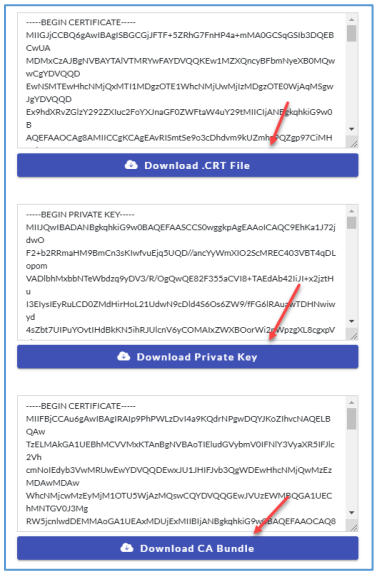
شکل ۱۴- ۲۱۶ / ایجاد گواهینامه خارجی

بعد از قرار دادن آدرس DNS در سرور وارد همان سایت قبلی که برای SSL بود شوید و به مانند شکل ۱٤-۲۱۷، بر روی Verify Domain کلیک کنید تا کار به اتمام برسد.



شکل ۱۴- ۲۱۷ / ایجاد گواهینامه خارجی

بعد از تایید گواهینامه مورد نظر، به مانند شکل ۱٤-۲۱۸، سه فایل برای شما در نظر گرفته می‌شود که همه آنها را باید دانلود کنید.



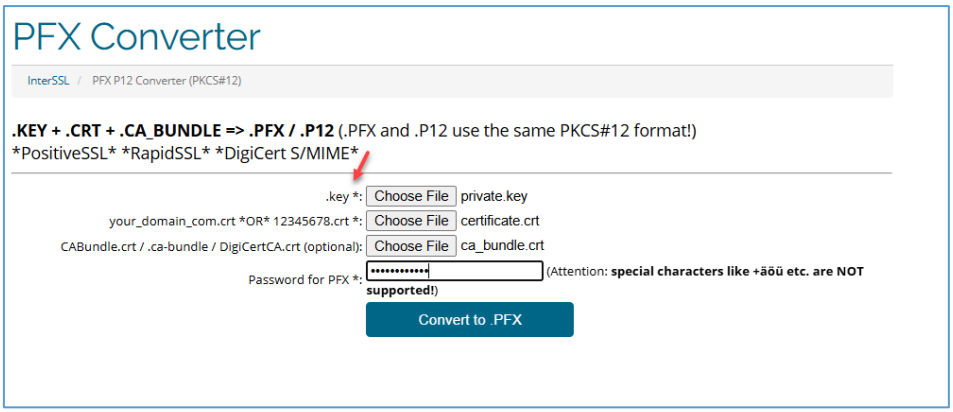
شکل ۱۴- ۲۱۸ / ایجاد گواهینامه خارجی

www.takbook.com

بعد از دانلود فایل باید آنها را به یک فایل PFX تبدیل کنیم تا در سرور Exchange نصب کنیم، برای این کار وارد سایت زیر شوید.

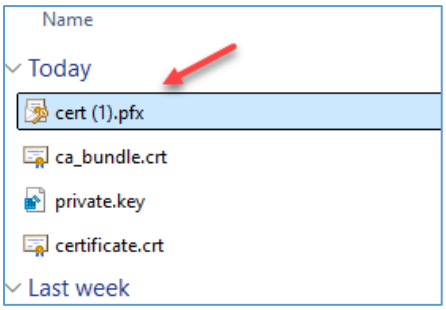
https://www.interssl.com/

بعد از ورود به ساست به مانند شکل ۱۴-۲۱۹، باید دقیقاً پسوند فایل‌ها با نام آنها یکی باشد، به مثالی که خودش زده دقیت کنید متوجه خواهید شد، هر سه فایل را به سایت معرفی کنید و یک رمز عبور هم برای آن مشخص کنید و بر روی Convert to .PFX کلیک کنید.



شکل ۱۴- ۲۱۹ / ایجاد گواهینامه خارجی

به مانند شکل ۱۴-۲۲۰، بعد از ایجاد فایل PFX باید آن را وارد سرور Exchange کنید و اجرا کنید.



شکل ۱۴- ۲۲۰ / ایجاد گواهینامه خارجی

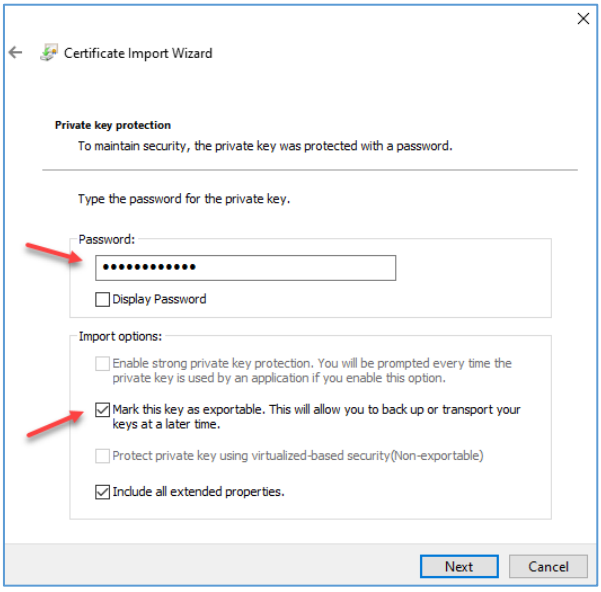
در شکل ۱۴-۲۲۱، گزینه‌ی Local Machine را انتخاب کنید تا گواهینامه بر روی سرور نصب شود.

www.takbook.com



شکل ۱۴ - ۲۲۱ / ایجاد گواهینامه خارجی

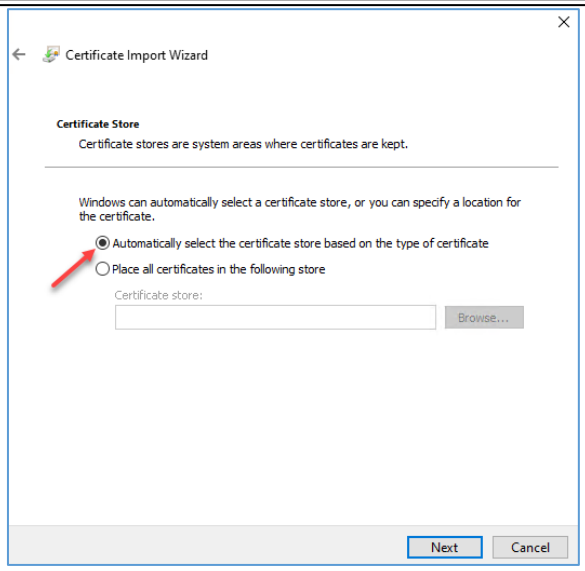
در شکل ۱۴–۲۲۲، باید همان رمزی که در هنگام ایجاد فایل PFX ایجاد کردید را وارد کنید و تیگ گزینه‌ی زیری آن را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۴ - ۲۲۲ / ایجاد گواهینامه خارجی

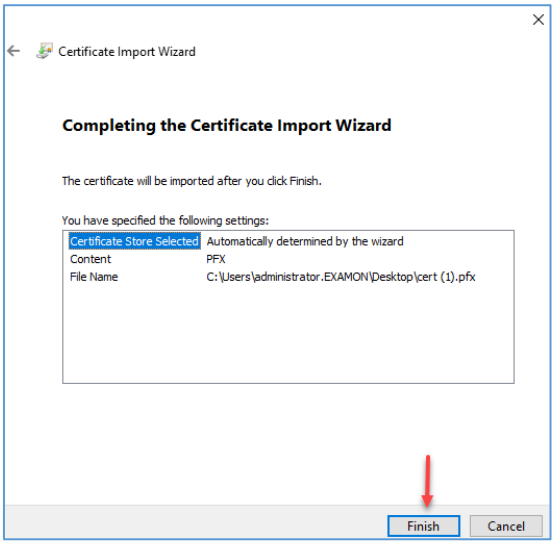
در شکل ۱۴–۲۲۳، گزینه‌ی Automatic را انتخاب کنید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۴ - ۲۲۳ / ایجاد گواهینامه خارجی

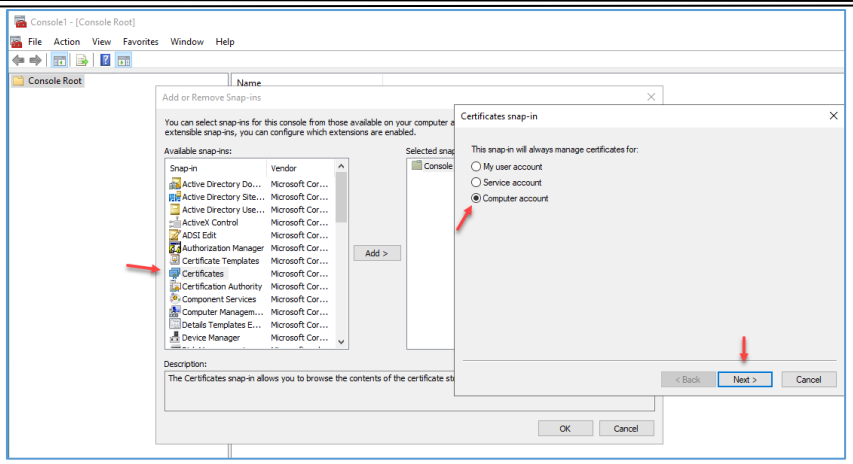
در شکل ۱۴-۲۲۴، بر روی Finish کلیک کنید تا گواهینامه مورد نظر نصب شود.



شکل ۱۴ - ۲۲۴ / ایجاد گواهینامه خارجی

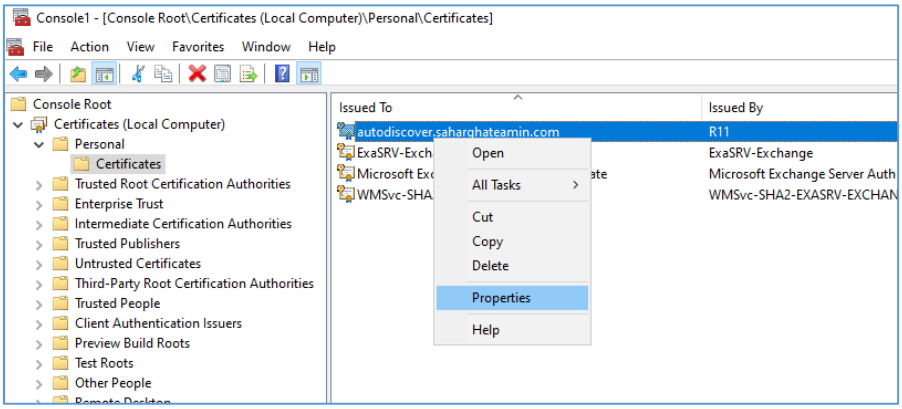
بعد از نصب گواهینامه اگر وارد سرویس Certificate شوید که به مانند شکل ۱۴-۲۲۵، از طریق MMC می‌توانید آن را اجرا کنید.

www.takbook.com



شکل ۱۴ - ۲۲۵ ایجاد گواهینامه خارجی

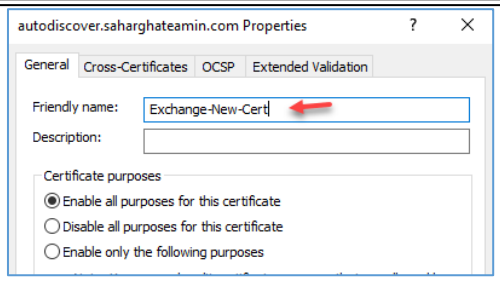
به مانند شکل ۱۴-۲۲۶، اگر وارد قسمت Personal و قسمت Certificate شوید متوجه خواهید شد که گواهینامه مورد نظر در سرویس ثبت شده است که برای اینکه نام آن را در سرور Exchange مشخص کنیم بر روی آن کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۱۴ - ۲۲۶ ایجاد گواهینامه خارجی

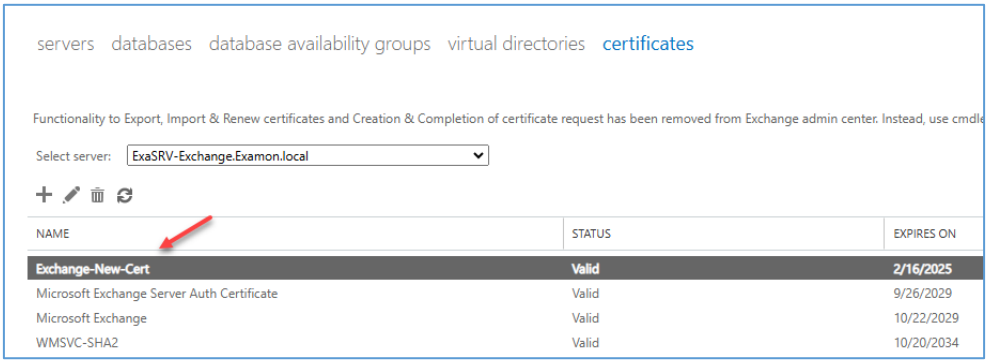
در شکل ۱۴-۲۲۷، باید یک نام برای گواهینامه مورد نظر خود وارد کنید.

www.takbook.com



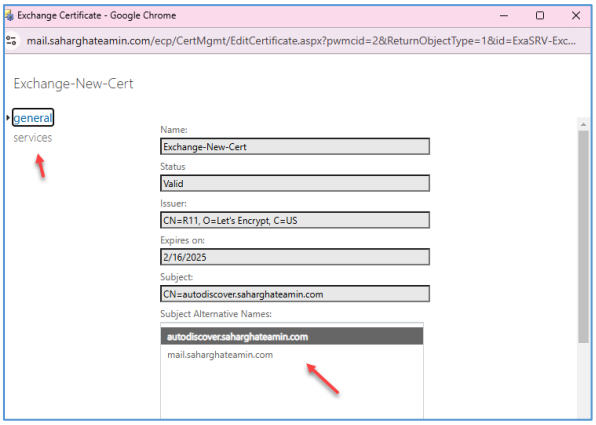
شکل ۱۴ - ۲۲۷ / ایجاد گواهینامه خارجی

بعد از اتمام کار حالا می‌توانیم وارد سرور Exchange و صفحه‌ی مدیریتی آن شویم و به مانند شکل ۱۴-۲۲۸، این گواهینامه را مشاهده کنیم که به صورت اتوماتیک Valid شده است.



شکل ۱۴ - ۲۲۸ / ایجاد گواهینامه خارجی

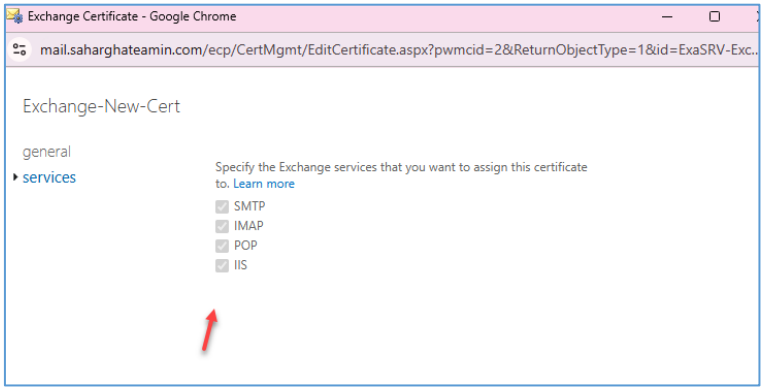
به مانند شکل ۱۴-۲۲۹، اگر بر روی گواهینامه‌ی مورد نظر کلیک کنید هر دو آدرسی که تعریف کردیم در لیست مشاهده می‌کنید، برای اینکه سرویس‌های Exchange را بر روی همین گواهینامه فعال کنیم باید وارد تب Services شویم.



شکل ۱۴ - ۲۲۹ / ایجاد گواهینامه خارجی

www.takbook.com

به مانند شکل ۱۴-۲۳۰، باید همه‌ی سرویس‌ها را انتخاب و بر روی Save کلیک کنید.

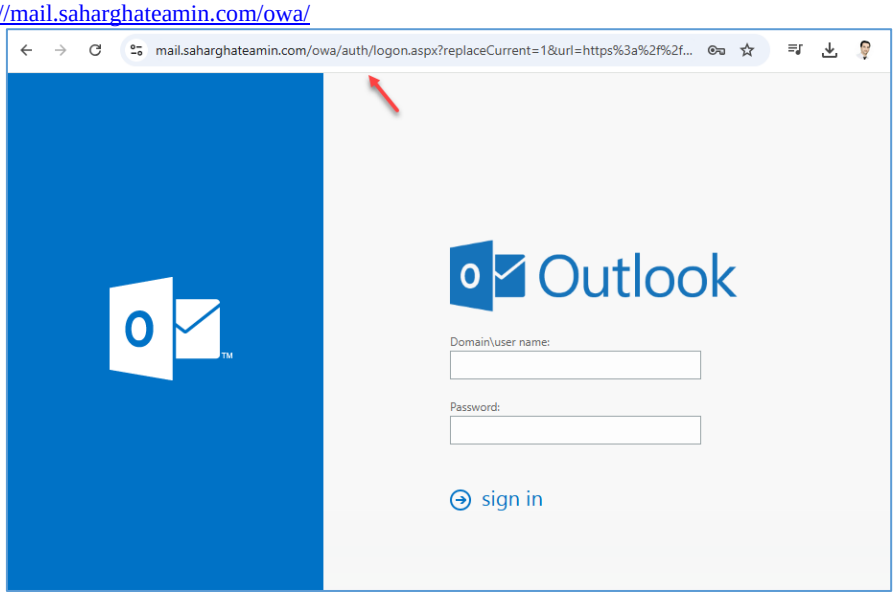


شکل ۱۴- ۲۳۰ ایجاد گواهینامه خارجی

بعد از اتمام کار سرور مورد نظر را Restart کنید تا تمام تنظیمات اعمال شود.

حالا اگر بخواهیم از بیرون به سایت مورد نظر دسترسی داشته باشیم می‌توانیم از پروتکل SSL استفاده کنیم، یعنی اگر به مانند شکل ۱۴-۲۳۱، آدرس زیر را اجرا کنیم وارد صفحه‌ی Login خواهیم شد که دارای SSL است.

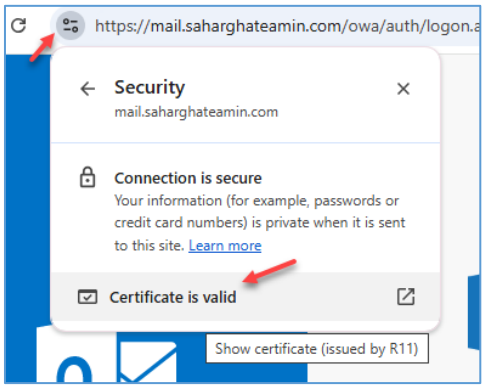
https://mail.saharghateamin.com/owa/



شکل ۱۴- ۲۳۱ ایجاد گواهینامه خارجی

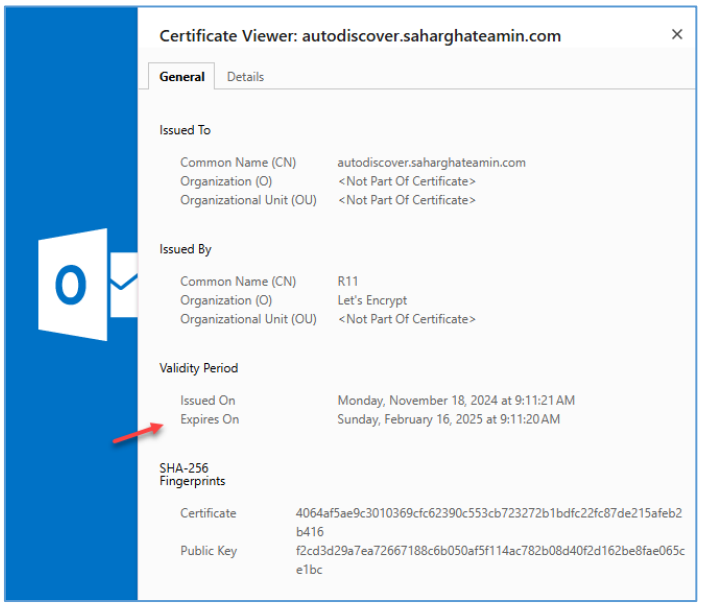
اگر به مانند شکل ۱۴-۲۳۲، بر روی Icon مورد نظر که مربوط به SSL است کلیک کنید در قسمت Security می‌توانید گواهینامه مورد نظر را با کلیک بر روی Certificate is Valid مشاهده کنید.

www.takbook.com



شکل ۱۴ - ۲۳۲ / ایجاد گواهینامه خارجی

در شکل ۱۴-۲۳۳، این گواهینامه را مشاهده می‌کنید که از شرکت Let's Encrypt صادر شده است و تاریخ ایجاد و انقضا آن مشخص شده است.

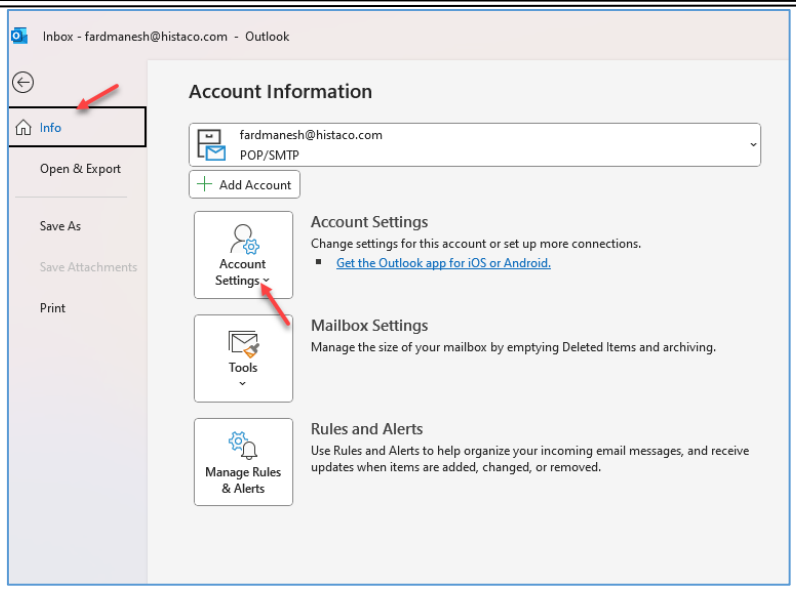


شکل ۱۴ - ۲۳۳ / ایجاد گواهینامه خارجی

۸-۲۰-۱۴ متصل شدن Outlook از طریق Exchange

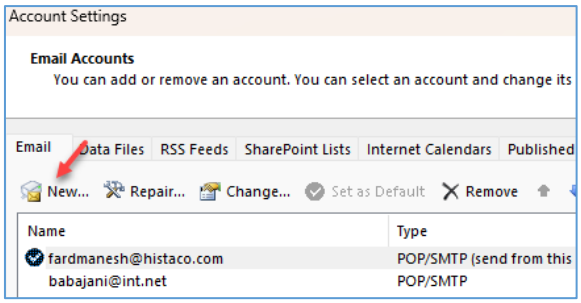
برای اینکه از طریق Outlook به Exchange متصل شویم می‌توانیم به صورت شکل ۱۴-۲۳۴، عمل کنیم، وارد Outlook شوید و از قسمت File وارد Info شوید و بر روی Account Settings کلیک کنید.

www.takbook.com



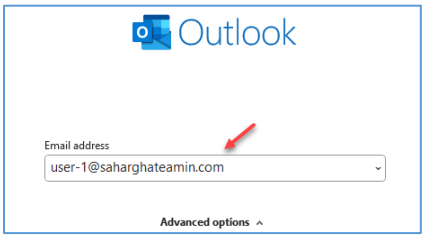
شکل ۱۴- ۲۳۴ متصل شدن Outlook از طریق Exchange

در شکل ۱۴-۲۳۵، بر روی New کلیک کنید.



شکل ۱۴- ۲۳۵ متصل شدن Outlook از طریق Exchange

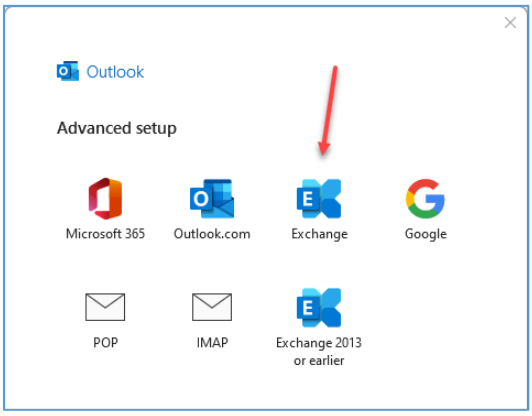
در شکل ۱۴-۲۳۶، باید کاربری را که در اوایل این بخش ایجاد کردیم را وارد کنید و تیک گزینه‌ی manually را انتخاب کنید.



شکل ۱۴- ۲۳۶ متصل شدن Outlook از طریق Exchange

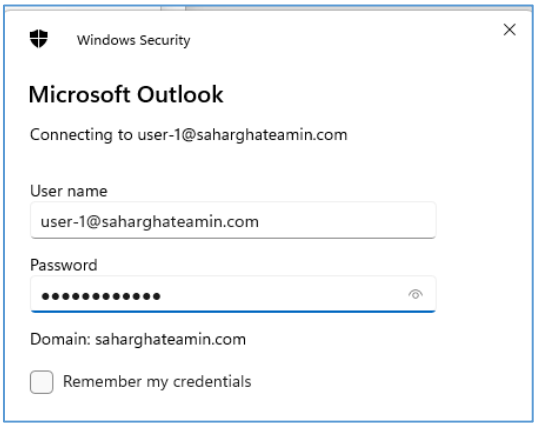
www.takbook.com

در شکل ۱۴-۲۳۷، گزینه‌ی Exchange را انتخاب کنید.



شکل ۱۴- ۲۳۷ متصل شدن Outlook از طریق Exchange

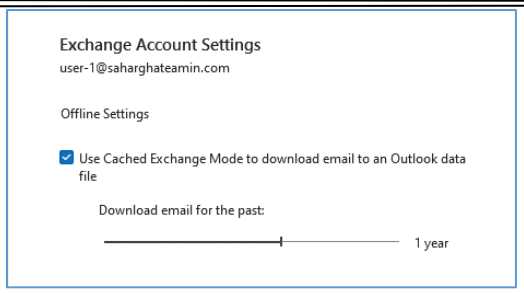
در ادامه از شما نام کاربری و رمز عبور کاربر مورد نظر را می‌پرسد که به مانند شکل ۱۴-۲۳۸، باید اطلاعات را وارد کنید.



شکل ۱۴- ۲۳۸ متصل شدن Outlook از طریق Exchange

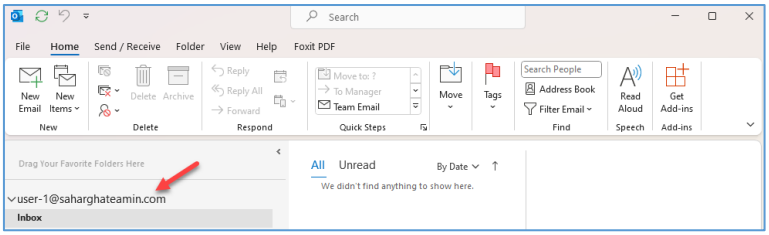
و در شکل ۱۴-۲۳۹، به این نکته اشاره دارد که اگر تیک گزینه‌ی مورد نظر انتخاب شود تا مقدار زمانی که مشخص می‌کنید ایمیل‌ها از سرور دریافت و در یک محل داخلی ذخیره خواهد شد تا در صورت آفلاین بودن سرور Exchange اطلاعات در دسترس باشد.

www.takbook.com



شکل ۱۴- ۲۳۹ متصل شدن Outlook از طریق Exchange

همان‌طور که در شکل ۱۴-۲۴۰، مشاهده می‌کنید با موفقیت به سرور Exchange متصل شدیم.

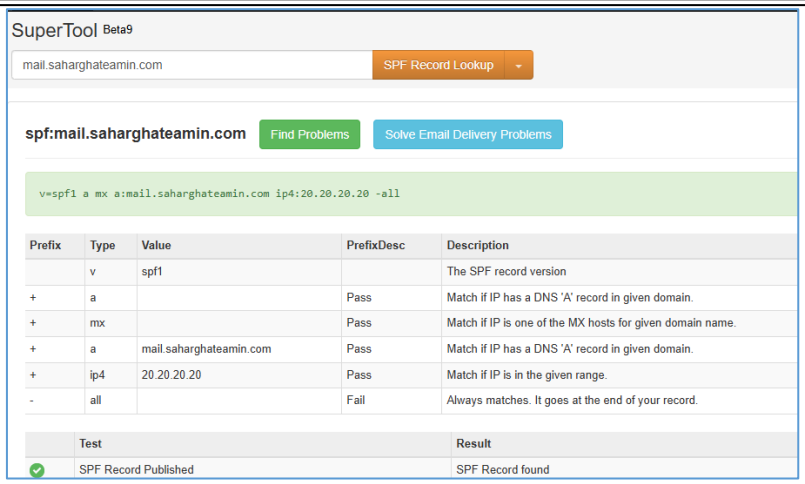


شکل ۱۴- ۲۴۰ متصل شدن Outlook از طریق Exchange

توجه به این نکته مهم است که وقتی یک سرور Email راه‌اندازی می‌کنید، باید چک کنید که این سرور از همه لحاظ به درستی تنظیم شده است، برای چک کردن این موضوع می‌توانیم از سایت قدرتمند mxtoolbox استفاده کنیم.

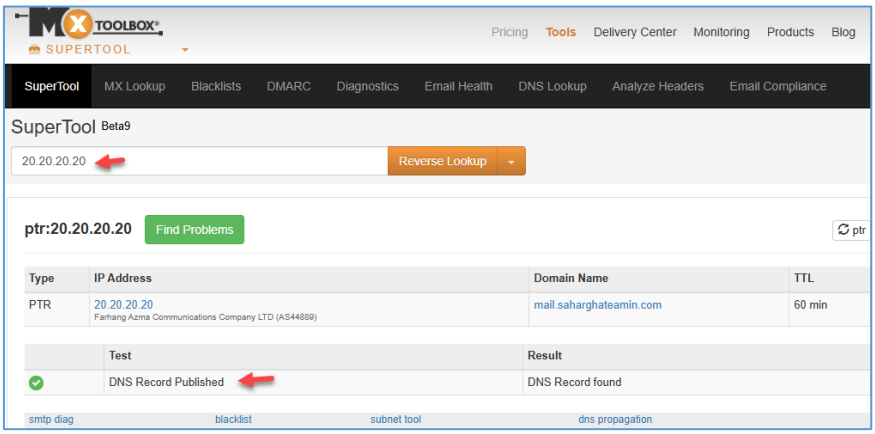
مثلاً برای بررسی مقدار SPF که در بخش‌های قبلی گفتیم باید از SPF Record Lookup استفاده کنیم، آدرس email خود را به مانند شکل ۱۴-۲۴۱، وارد می‌کنیم که بعد از کلیک بر روی دکمه مورد نظر دقیقاً همان SPF که با هم ایجاد کردیم در خروجی مشخص شده است و تایید شده است.

www.takbook.com



شکل ۱۴- ۲۴۱ متصل شدن Outlook از طریق Exchange

یکی از مهمترین کارها در این بخش این است که رکورد PTR را بررسی کنیم، اگر رکورد PTR که همان تبدیل IP به نام است درست تعریف نشده باشه اکثر ایمیل سرورها ایمیل ما را قبول نخواهند کرد، در شکل ۱۴-۲۴۲، مقدار رکورد PTR برای سایت ما پیدا شد.



شکل ۱۴- ۲۴۲ متصل شدن Outlook از طریق Exchange

www.takbook.com

www.takbook.com

فصل پانزدهم

Skype For Business 2019

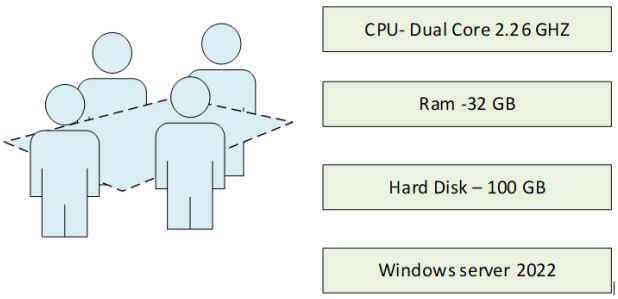
Skype for Business یک پلتفرم ارتباطی سازمانی از مایکروسافت است که امکانات مختلفی برای ارتباطات داخلی و خارجی شرکت‌ها فراهم می‌کند. این نرم‌افزار که ابتدا با نام Lync شناخته می‌شد، در سال ۲۰۱۵ با نام Skype for Business معرفی شد و امکانات Skype را با ویژگی‌های سازمانی ترکیب کرد.

ویژگی‌های کلیدی:

- چت و پیام‌رسانی فوری (IM): امکان ارسال پیام‌های متنی سریع بین کاربران.
- تماس صوتی و تصویری: برقراری تماس‌های صوتی و تصویری با کیفیت بالا.
- کنفرانس‌های ویدئویی و صوتی: برگزاری جلسات گروهی با پشتیبانی از صدها شرکت‌کننده.
- اشتراک‌گذاری صفحه (Screen Sharing): اشتراک‌گذاری صفحه‌نمایش برای ارائه‌ها یا پشتیبانی فنی.
- یکپارچگی با مجموعه آفیس: هماهنگی کامل با ابزارهایی مثل Outlook برای برنامه‌ریزی جلسات.
- انتقال فایل: امکان ارسال فایل به صورت سریع بین کاربران.
- قابلیت‌های تلفنی (Enterprise Voice): استفاده به عنوان PBX سازمانی برای مدیریت تماس‌های تلفنی.
- امنیت سازمانی: رمزنگاری داده‌ها و کنترل دسترسی برای امنیت بیشتر.

۱۵-۱ پیش‌نیاز نصب Skype For Business 2019

سرور Skype For Business، نیاز به سخت‌افزار شکل ۱۵-۱،دارد.



شکل ۱۵- ۱ سخت‌افزار Skype For Business

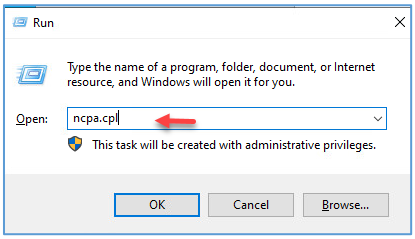
در شکل ۱۵-۱ ، به حداقل یک CPU دو هسته‌ای با سرعت ۲.۲۶ گیگاهرتز نیاز است که البتّه اگر بالاتر هم باشد، کارایی بهتری دارد. مقدار رم ۳۲ گیگابایت در نظر گرفته شده است که رم در سرور Skype، نقش

www.takbook.com

مهمّی دارد و هر چقدر بیشتر باشد، سرور در مواقع بار زیاد، عکس‌العمل خوبی از خود نشان خواهد داد؛ توجّه داشته باشید از رم پایین‌تر هم برای نصب می‌توانید استفاده کنید، مقدار هارد دیسک را هم ۱۰۰ گیگابایت در نظر بگیرید، البتّه حداقل حجم آن، ۷۲ گیگ است. در آخر هم نیاز به ویندوز سرور 2012 R2 به بالا داریم که در این کتاب از windows Server 2025 استفاده شده است، سعی کنید تمام موارد ذکر شده در بالاترین سطح قرار داشته باشد.

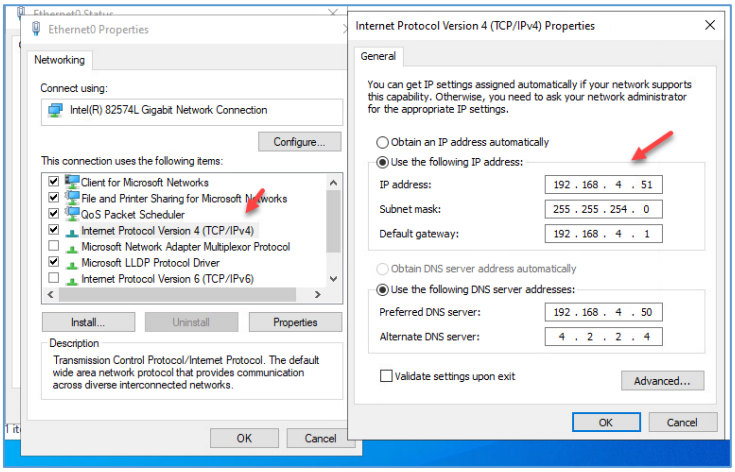
برای شروع یک سرور جدید با ویندوز سرور 2025 ایجاد می‌کنیم و تنظیمات کارت شبکه و نام آن را به صورت زیر تغییر می‌دهیم.

به مانند شکل ۱۵-۲، بعد از ایجاد سرور با دستور ncpa.cpl وارد Network Connection شوید.



شکل ۱۵- ۲ تغییر آدرس IP

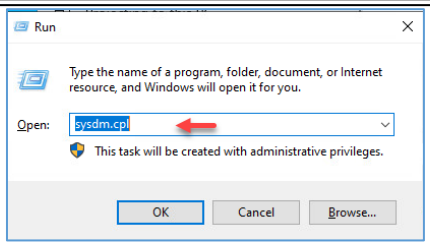
بعد از باز شدن صفحه‌ی مورد نظر IP آن را به مانند شکل ۱۵-۳، مشخص کنید.



شکل ۱۵- ۳ تغییر آدرس IP

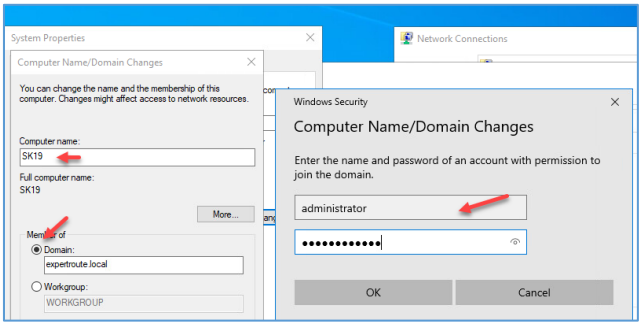
در ادامه کار یک نام برای سرور مورد نظر مشخص کنید و آن را عضو دومین خود کنید، برای ورود به صفحه‌ی مورد نظر دستور sysdm.cpl را در Run اجرا کنید، این موضوع را در شکل ۱۵-٤، مشاهده می‌کنید.

www.takbook.com



شکل ۱۵ - ۴ تغییر نام سرور

در شکل ۱۵-۵، نام سرور و آدرس دومین را وارد کنید، و نام کاربری و رمز عبور ادمین را وارد تا سرور مورد نظر عضو دومین شود.



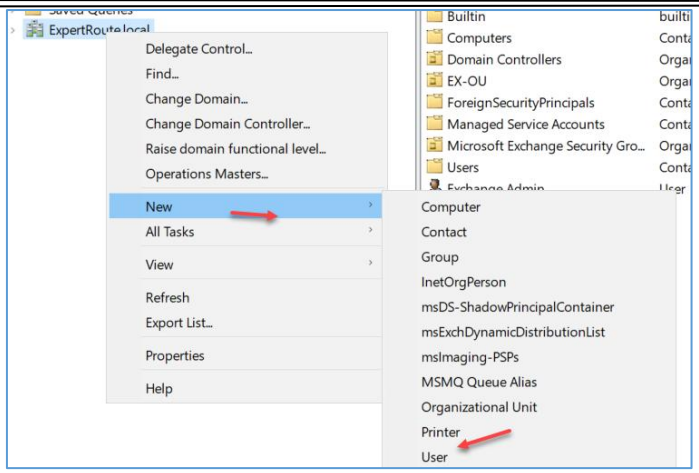
شکل ۱۵ - ۵ تغییر نام سرور

بعد از اینکه سرور مورد نظر را عضو دومین کردید برای ورود به آن نیاز به یک کاربر ارشد داریم که عضو گروه‌های مشخص شده‌ی زیر باشد:

- Administrator
- Schema Admins
- Domain Admins
- Enterprise Admins

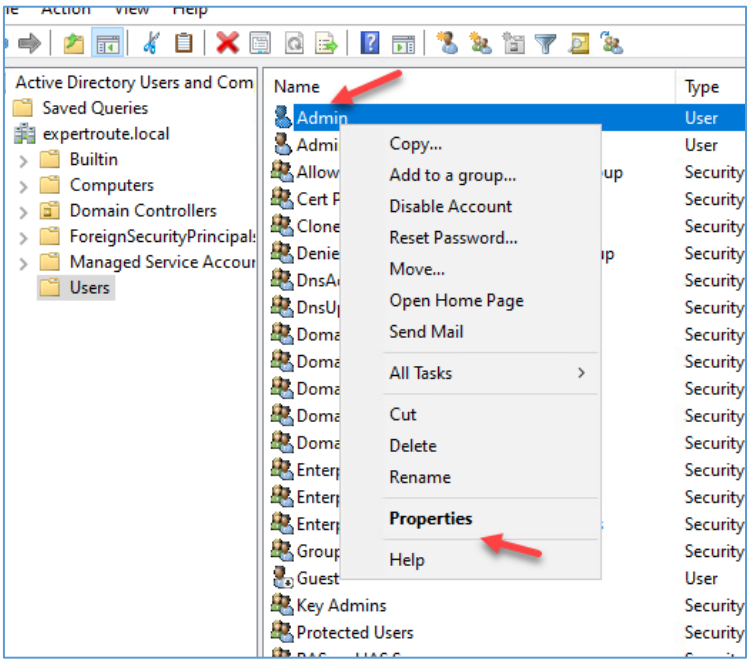
برای ایجاد کاربر وارد Active Directory Users and Computers شوید و به مانند شکل ۱۵-۶، از قسمت New گزینه‌ی User را انتخاب کنید.

www.takbook.com



شکل ۱۵- ۶ ایجاد کاربر جدید

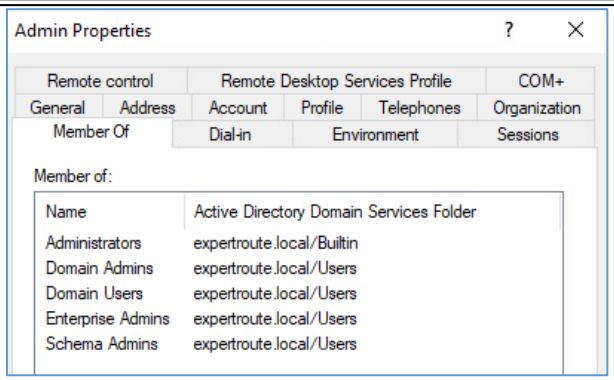
بعد از ایجاد کاربر جدید به مانند شکل ۱۵-۷، بر روی آن کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۱۵- ۷ دسترسی کاربر ارشد

در ادامه کار و به مانند شکل ۱۵-۸، وارد تب Member of شوید و کاربر مورد نظر را عضو گروه‌های مشخص شده کنید.

www.takbook.com

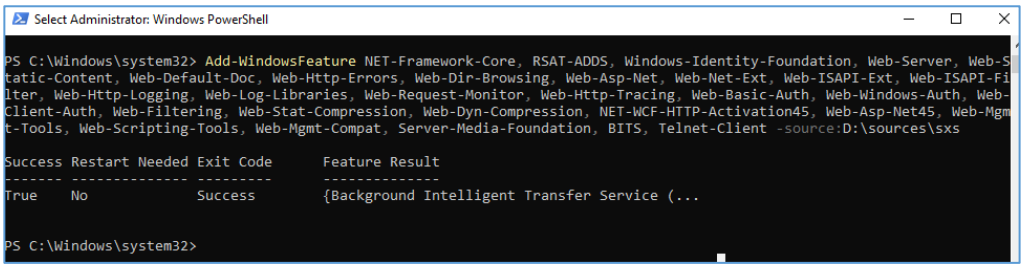


شکل ۱۵- ۸ دسترسی کاربر ارشد

بعد از ایجاد کاربر و عضو کردن در گروه مورد نظر وارد ویندوز سرور مربوط به Skype For Businnes شوید و برای شروع به کار سرویس PowerShell را باز کنید و دستورات زیر را وارد کنید، توجه داشته باشید که باید DVD ویندوز سرور را داخل درایو قرار دهید تا در هنگام نصب ابزارها، در صورت نیاز به آن رجوع شود، دستور source:D:\sources\sxs- در زیر یعنی به درایوی که ویندوز سرور در آن قرار دارد اشاره می‌کند.

```
Import-Module ServerManager
Add-WindowsFeature NET-Framework-Core, RSAT-ADDS, Windows-Identity-Foundation, Web-Server, Web-Static-Content, Web-Default-Doc, Web-Http-Errors, Web-Dir-Browsing, Web-Asp-Net, Web-Net-Ext, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Http-Logging, Web-Log-Libraries, Web-Request-Monitor, Web-Http-Tracing, Web-Basic-Auth, Web-Windows-Auth, Web-Client-Auth, Web-Filtering, Web-Stat-Compression, Web-Dyn-Compression, NET-WCF-HTTP-Activation45, Web-Asp-Net45, Web-Mgmt-Tools, Web-Scripting-Tools, Web-Mgmt-Compat, Server-Media-Foundation, BITS, Telnet-Client -source:D:\sources\sxs
```

همان‌طور که در شکل ۱۵-۹، مشاهده می‌کنید دستورات مورد نظر به درستی نصب شده است.



شکل ۱۵- ۹ نصب پیش‌نیاز

قبل از اینکه نصب را آغاز کنیم باید تنظیمات DNS مربوط به Skype for Business Server 2019 را که خیلی مهم است با هم انجام دهیم.

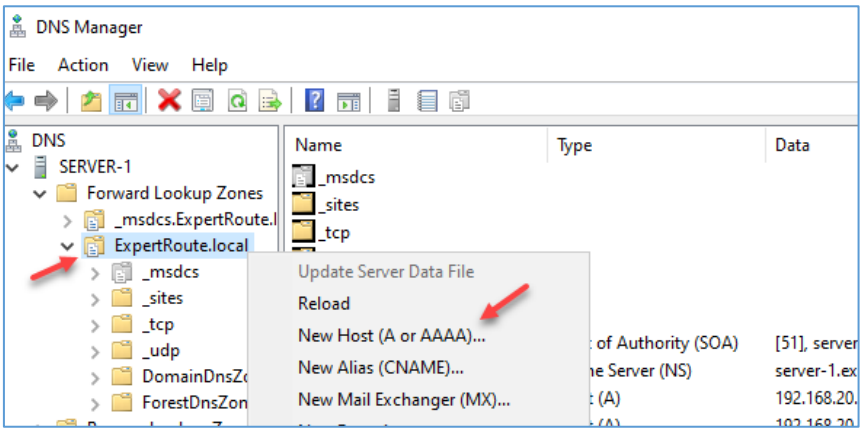
وارد سرویس DNS در سرور Active شوید و به مانند زیر عمل کنید.

www.takbook.com

۱۵-۲ تنظیمات DNS برای Skyep For Business 2019

نرم‌افزار Skype For Business در هنگام نصب، نیاز به چند A Record در سرویس DNS دارد که باید آنها را به صورت دستی ایجاد کنید و این مورد در عملکرد این سرویس بسیار مهم خواهد بود؛ برای این کار وارد سرور دومین شوید و سرویس DNS را اجرا کنید.

برای شروع به مانند شکل ۱۵-۱۰، از سمت چپ بر روی Forward Lookup Zones کلیک کنید و بعد، نام دومین خود را انتخاب کنید و در صفحه‌ی باز شده کلیک راست کنید و گزینه‌ی New Host (A or AAAA) را انتخاب کنید.

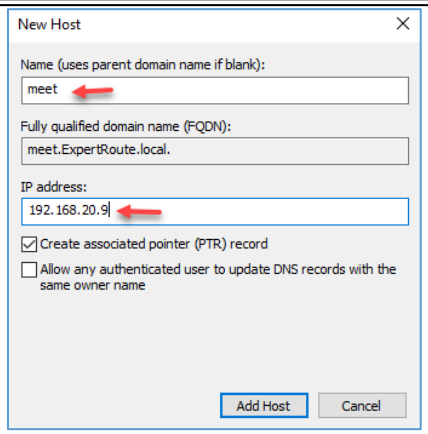


شکل ۱۵- ۱۰ تنظیمات DNS

در شکل ۱۵-۱۱، در قسمت Name، باید نام Meet را وارد کنید و در قسمت IP address، آدرس سرور Skype را وارد کنید و بعد بر روی Add Host کلیک کنید. همین کار را باید برای اسم‌های زیر هم انجام دهید، یعنی به جای اسم Meet در شکل زیر، اسامی مشخص‌شده را وارد کنید:

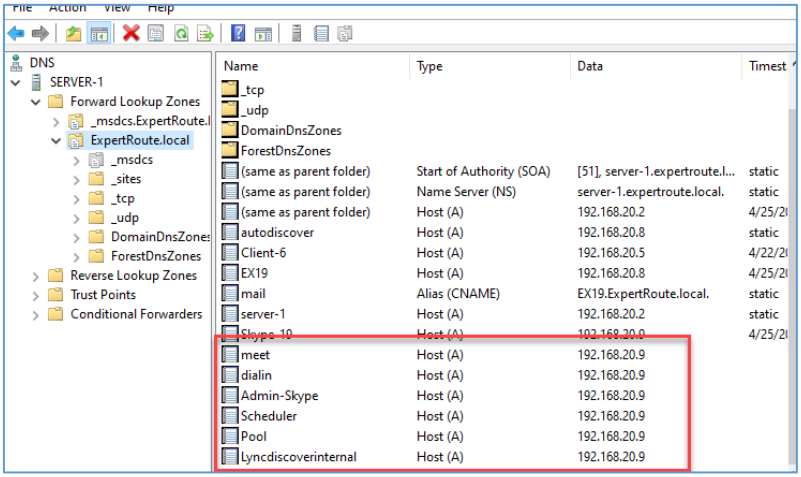
- Dialin
- Admin-Skype
- Scheduler
- Pool
- Lyncdiscoverinternal
- Lyncdiscover

www.takbook.com



شکل ۱۵- ۱۱ تنظیمات DNS

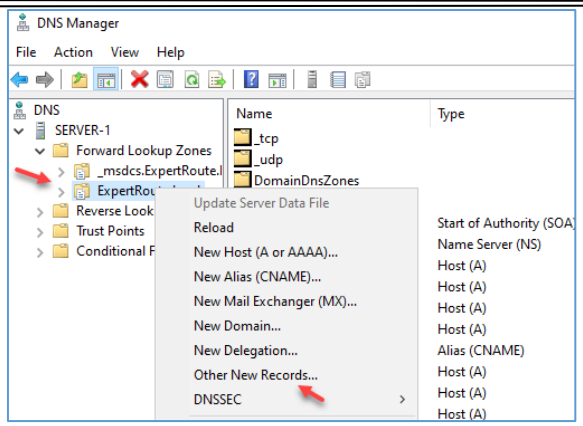
همان‌طورکه در شکل ۱۵-۱۲، مشاهده می‌کنید، هر ٦ اسم در لیست ایجاد شده است؛ توجّه داشته باشید که این کار را دقیق انجام دهید تا در موقع نصب Skype For business با مشکل مواجه نشوید.



شکل ۱۵- ۱۲ تنظیمات DNS

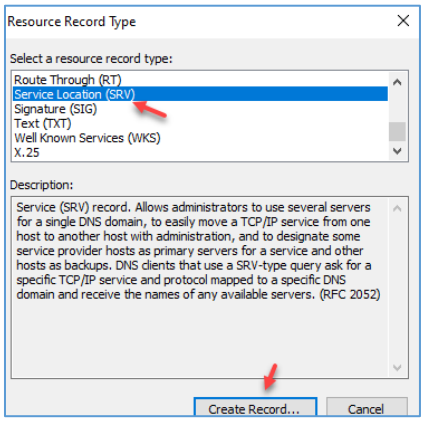
در ادامه‌ی کار باید یک SRV Records ایجاد کنید؛ برای این کار به مانند شکل ۱۵-۱۳، بر روی نام دومین خود کلیک راست کنید و گزینه‌ی Other New Recordes را انتخاب کنید.

www.takbook.com



شکل ۱۵- ۱۳ تنظیمات DNS

در شکل ۱۵-۱٤، از لیست مورد نظر، گزینه‌ی Service Location را انتخاب و بر روی Create Record کلیک کنید.

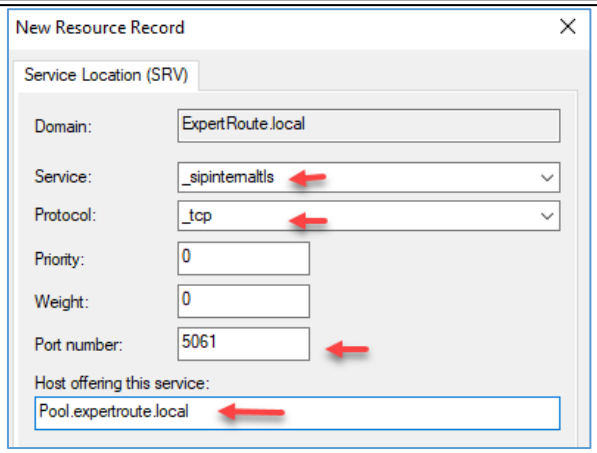


شکل ۱۵- ۱۴ تنظیمات DNS

در شکل ۱۵-۱۱۵، در قسمت Service، نام _sipinternaltls را وارد کنید و در قسمت Protocol، نام _tcp را وارد کنید.

در قسمت Port Number، عدد ۵۰۶۱ که مربوط به پروتکل SIP است را وارد کنید؛ در قسمت آخر هم، همان نام Pool که در قسمت قبل ایجاد کردید را در این قسمت به همراه نام کامل دومین وارد و بر روی OK کلیک کنید.

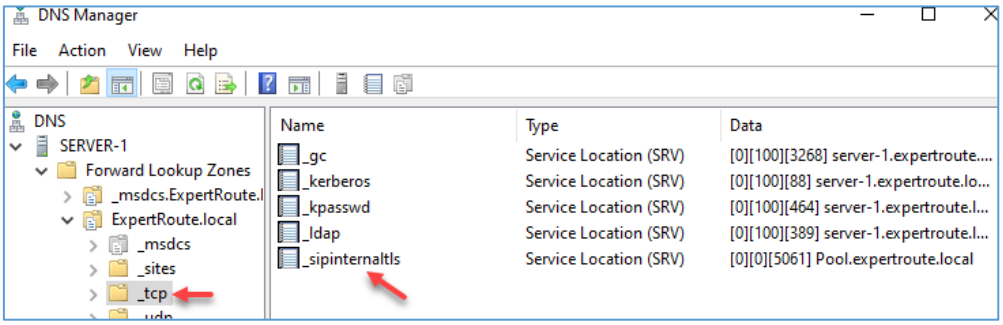
www.takbook.com



شکل ۱۵- ۱۵ تنظیمات DNS

اگر علاقمندید در مورد شماره‌ی پورت‌های نرم‌افزار Skype اطّلاعات کسب کنید، می‌توانید اینجا را کلیک کنید.

همان‌طورکه در شکل ۱۵-۱۶، مشاهده می‌کنید، همه چیز به درستی ایجاد شده است.

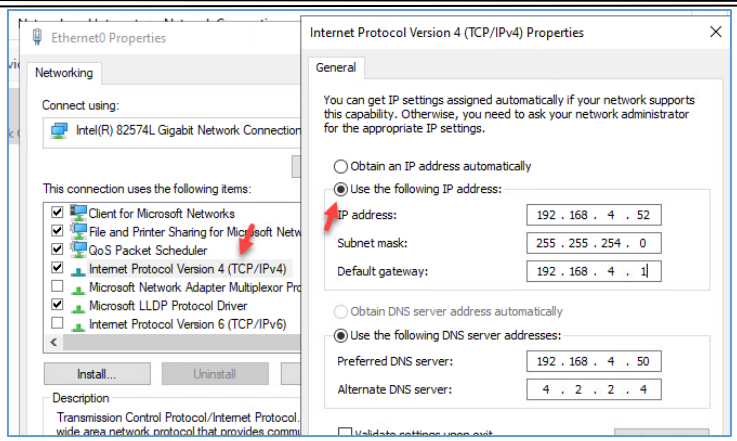


شکل ۱۵- ۱۶ تنظیمات DNS

۱۵-۳ نصب SQL Server 2022

برای اینکه از تمام امکانات Skype for business استفاده کنیم باید یک سرور SQL هم به صورت جداگانه آماده کنیم و آن را به Skype متصل کنیم، برای این کار به مانند شکل ۱۵-۱۷، سرور دومی با نام SQL ایجاد و آن را عضو شبکه می‌کنیم و بر روی SQL Server 2022 نصب می‌کنیم.

www.takbook.com



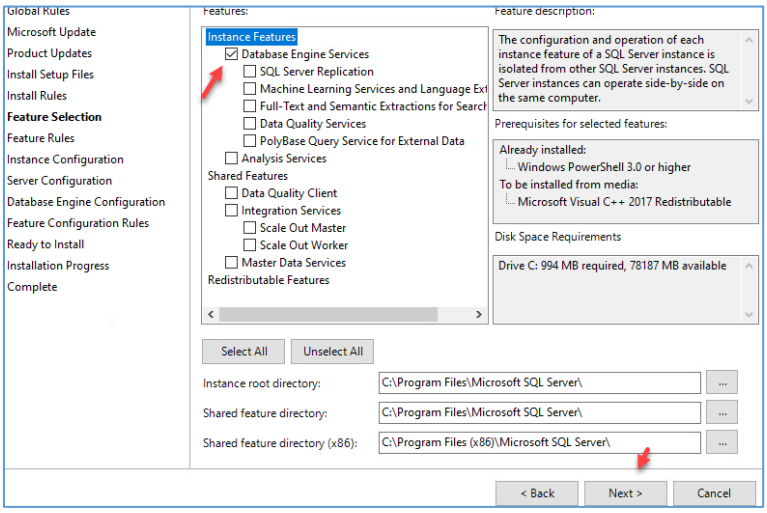
شکل ۱۵- ۱۷ تنظیمات IP

بعد از اینکه سرور SQL را عضو دومین کردیم باید با کاربر Admin وارد آن شوید و نرم‌افزار SQL Server 2022 را که لینک آن در زیر قرار دارد را نصب کنید.

https://dl2.soft98.ir/programing/Microsoft.SQL.Server.2022.Enterprise.x64.rar?1723982206

نصب SQL را در فصل‌های قبلی با هم بررسی کردیم و نیازی به آموزش دوباره آن نیست فقط در هنگام نصب باید موارد زیر را رعایت کنید.

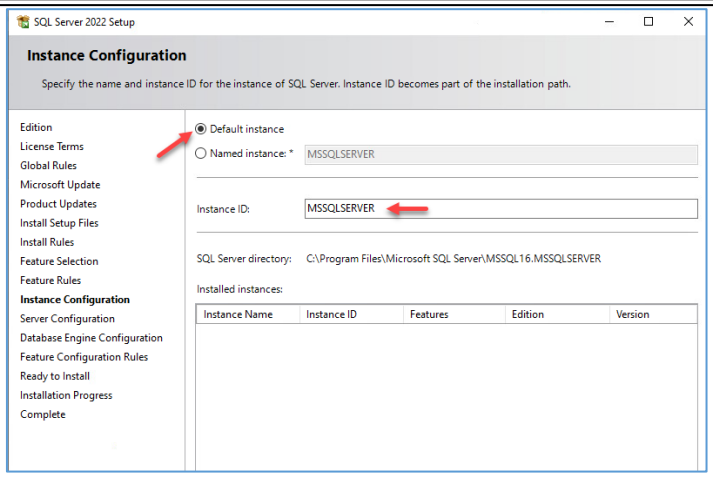
در شکل ۱۵–۱۸، فقط باید تیک گزینه‌ی Database Engine Services را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۵- ۱۸ نصب SQL Server 2022

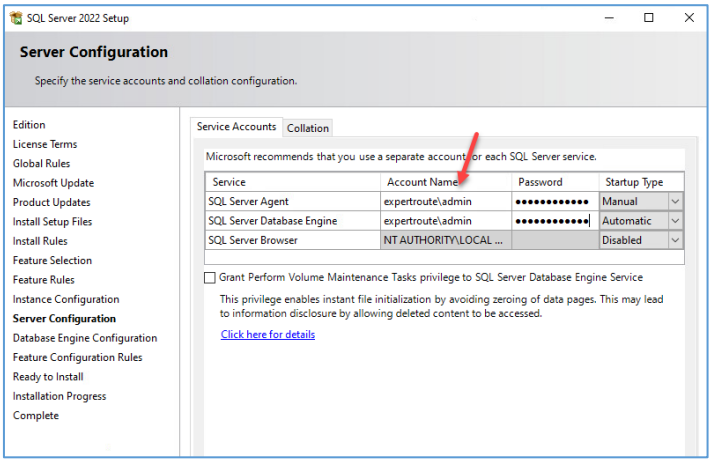
در شکل ۱۵–۱۹، نیازی به تغییر Instance نیست و فقط بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۵- ۱۹ نصب *SQL Server 2022*

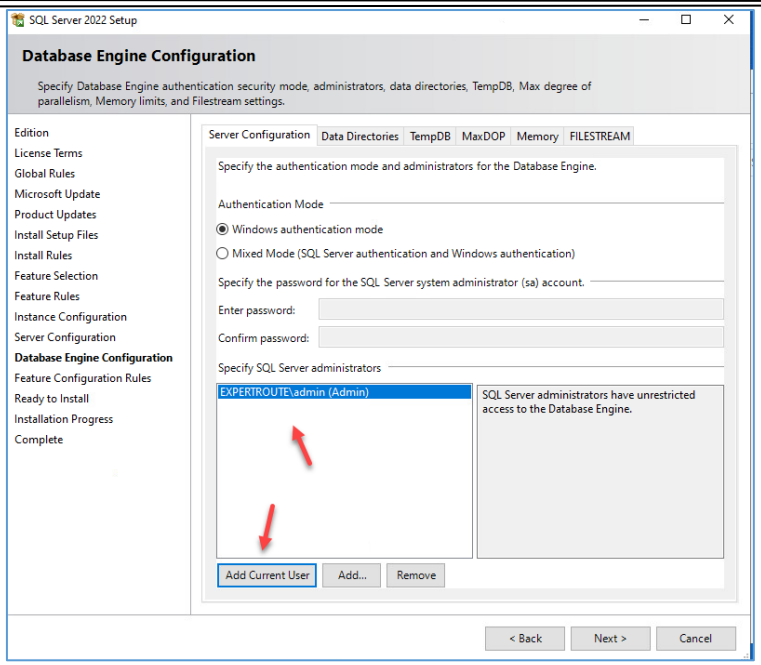
در شکل ۱۵–۲۰، باید نام دومین و نام کاربری را به همراه رمز عبور در قسمت مشخص شده وارد کنید.



شکل ۱۵- ۲۰ تنظیمات *DNS*

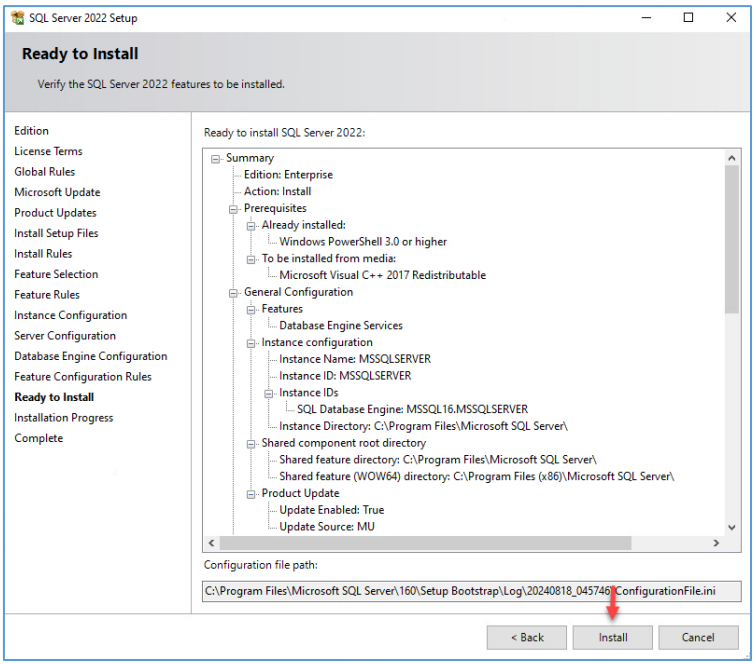
در شکل ۱۵–۲۱، بر روی Add Current User کلیک کنید تا کاربر Admin به لیست اضافه شود و دسترسی لازم را داشته باشد.

www.takbook.com



شکل ۱۵- ۲۱ نصب SQL Server 2022

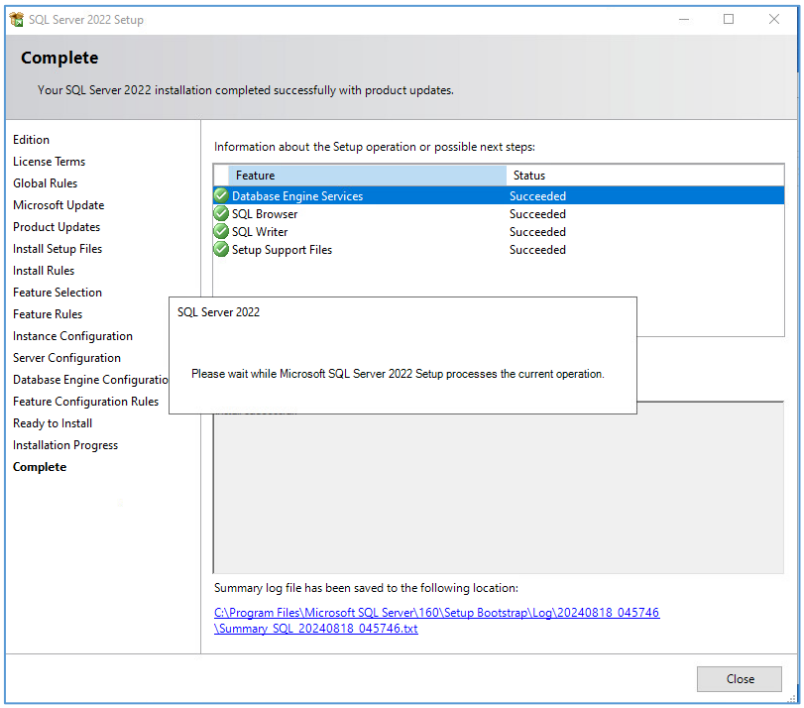
در شکل ۱۵-۲۲، بر روی Install کلیک کنید تا کار نصب آغاز شود.



شکل ۱۵- ۲۲ نصب SQL Server 2022

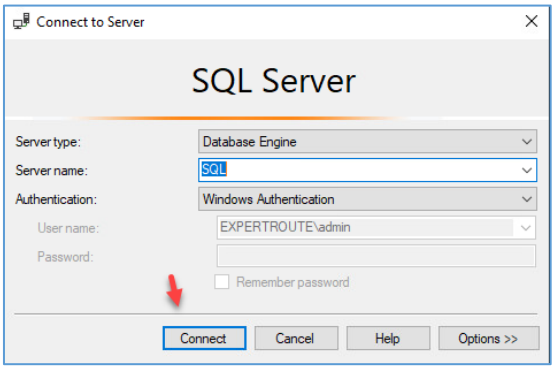
www.takbook.com

همان‌طور که در شکل ۱۵-۲۳، مشاهده می‌کنید نرم‌افزار SQL نصب شده است.



شکل ۱۵- ۲۳ نصب SQL Server 2022

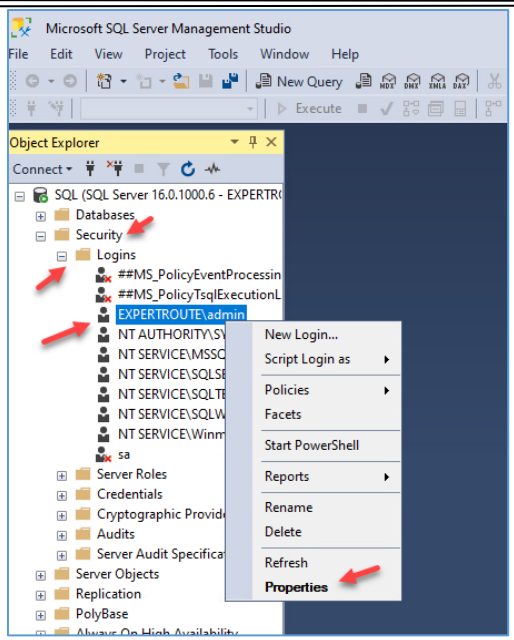
نرم افزار SQL server Management Studio را هم باید بر روی سرور نصب کنید که قبلاً در فصل‌های قبلی این کار را انجام دادیم، آن را اجرا می‌کنیم و به مانند شکل ۱۵-۲۴، وارد تنظیمات SQL می‌شویم.



شکل ۱۵- ۲۴ نصب SQL Server 2022

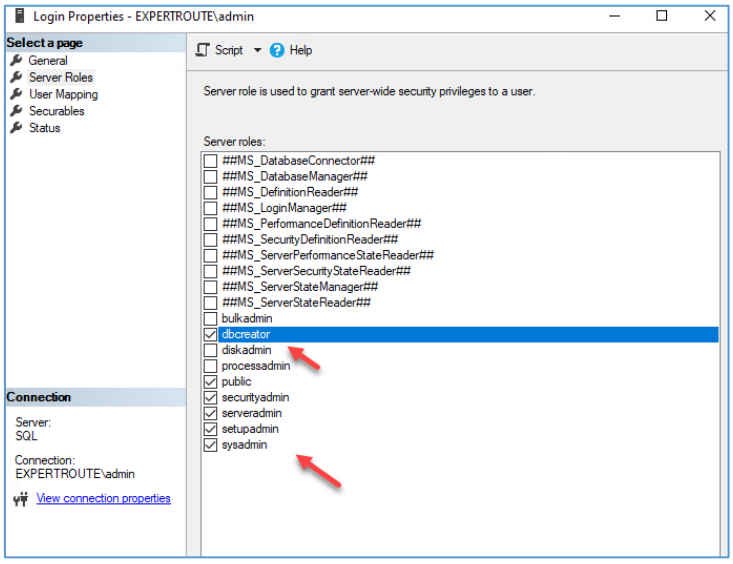
به مانند شکل ۱۵-۲۵، وارد قسمت Security شوید و از قسمت Login بر روی کاربر مورد نظر خود کلیک راست کنید و گزینه‌ی Propeties را انتخاب کنید.

www.takbook.com



شکل ۱۵- ۲۵ نصب *SQL Server 2022*

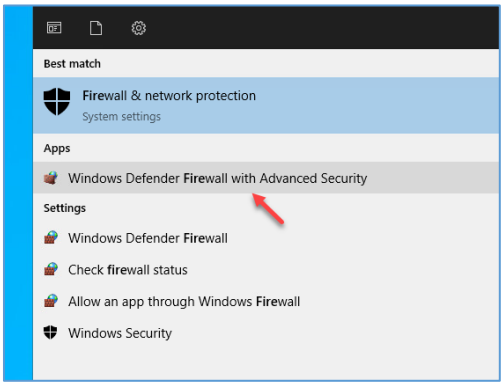
در شکل ۱۵-۲٦، وارد قسمت Server Roles شوید و تیک گزینه‌ی های مورد نظر را انتخاب کنید تا دسترسی کاربر مورد نظر کامل شود.



شکل ۱۵- ۲۶ نصب *SQL Server 2022*

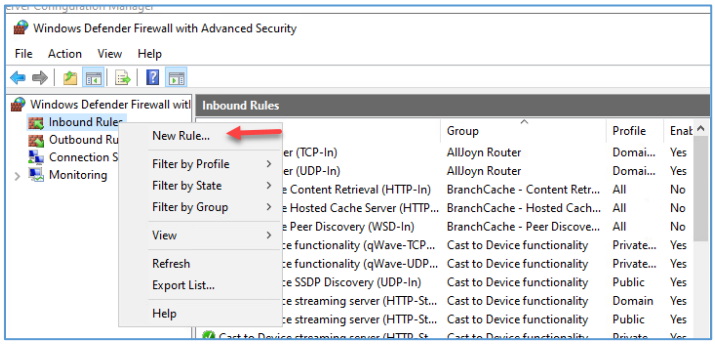
www.takbook.com

بعد از انجام مراحل قبل، در همان سرور SQL به مانند شکل ۱۵-۲۷، وارد فایروال شوید تا به پورت SQL دسترسی لازم را دهیم و بتوانیم از طریق سرور اسکایپ به آن متصل شویم.



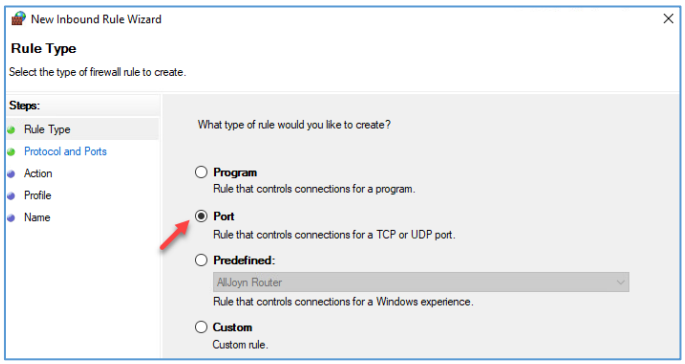
شکل ۱۵- ۲۷ تنظیم فایروال SQL

در شکل ۱۵-۲۸، بر روی Inbound Rules کلیک راست کنید و گزینه‌ی New Rule را انتخاب کنید.



شکل ۱۵- ۲۸ تنظیم فایروال SQL

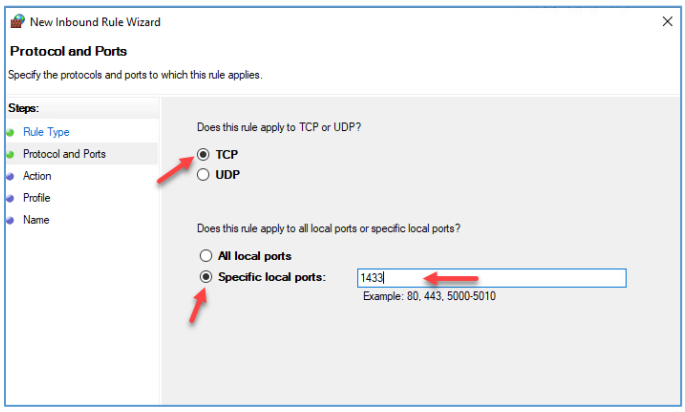
در شکل ۱۵-۲۹، گزینه‌ی Port را انتخاب کنید.



شکل ۱۵- ۲۹ تنظیم فایروال SQL

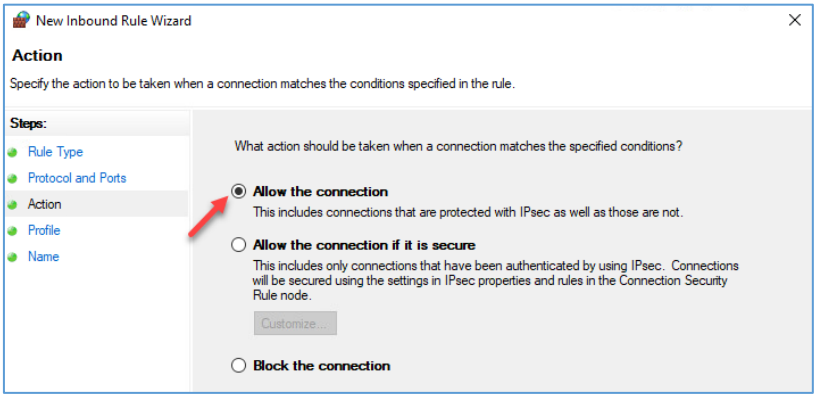
www.takbook.com

در شکل ۱۵-۳۰، باید پورت 1433 را وارد و بر روی Next کلیک کنید.



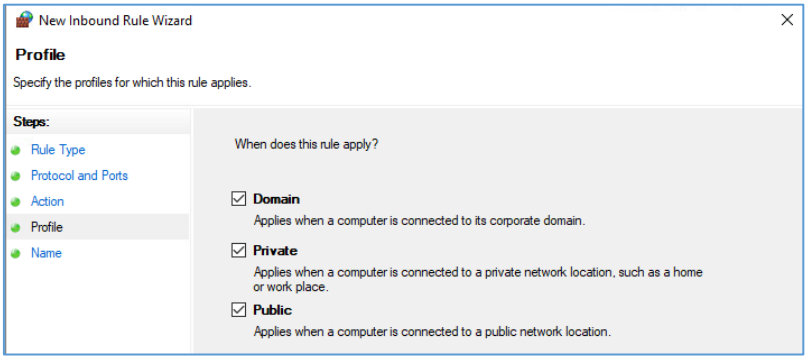
شکل ۱۵- ۳۰ تنظیم فایروال SQL

در شکل ۱۵-۳۱، گزینه‌ی اول را انتخاب و بر روی Next کلیک کنید.



شکل ۱۵- ۳۱ تنظیم فایروال SQL

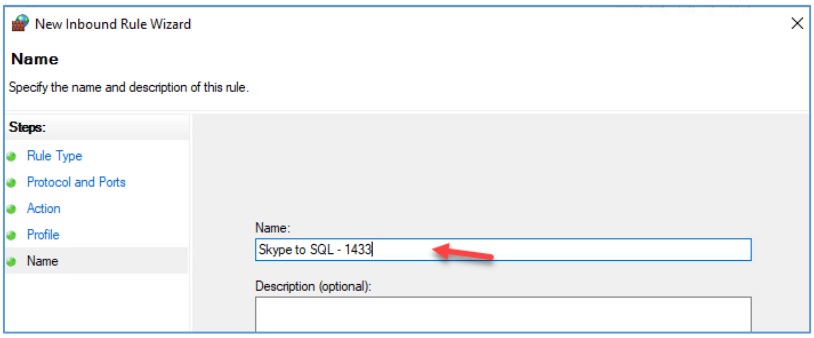
در شکل ۱۵-۳۲، بر روی Next کلیک کنید.



شکل ۱۵- ۳۲ تنظیم فایروال SQL

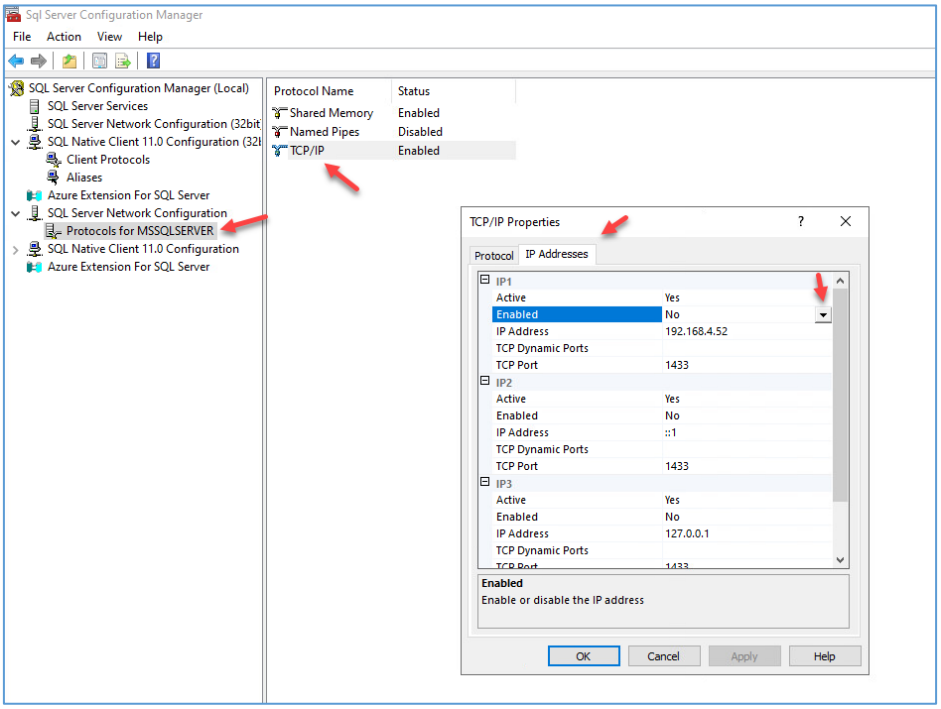
www.takbook.com

در شکل ۱۵-۳۳، نام دلخواه خود را وارد و بر روی Finish کلیک کنید.



شکل ۱۵- ۳۳ تنظیم فایروال SQL

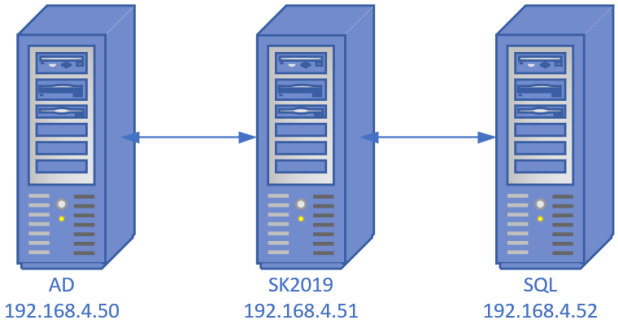
بعد از تنظیم فایروال باید به این نکته اشاره کنیم که برای دسترسی شبکه به SQL باید تنظیمی را در SQL انجام دهید، برای انجام این کار سرویس SQL Server Configuration Manager را به مانند شکل ۱۵-۳۴، اجرا کنید و از قسمت SQL Server Network Configuration بر روی Protocoles For MSSQL Server کلیک کنید و در صفحه‌ی باز شده گزینه‌ی TCP/IP را انتخاب کنید و در صفحه باز شده‌ی شکل ۱۵-۳۴، وارد تب IP addresses شوید و از قسمت IP1 گزینه‌ی Enabled را Yes کنید.



شکل ۱۵- ۳۴ تنظیم فایروال SQL

www.takbook.com

تا به اینجا سرورهای SKYPE و SQL را راه‌اندازی کردیم و حالا باید نرم‌افزار Skype For Business را بر روی سرور SK2019 نصب کنیم.

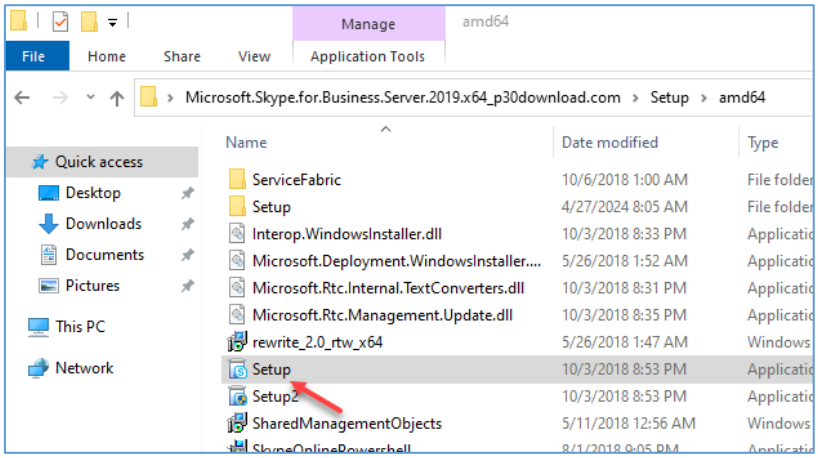


۱۵-٤ نصب Skype For Business 2019

بعد از انجام تمام مراحل بالا همه چیز برای نصب Skype For business آماده است، برای دانلود این نرم‌افزار می‌توانید از طریق لینک زیر اقدام کنید:

https://www.microsoft.com/en-gb/evalcenter/download-skype-business-server-2019

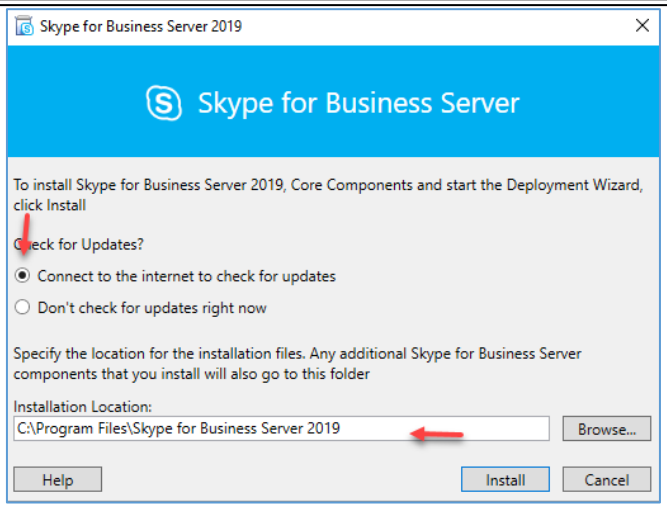
بعد از دانلود فایل مورد نظر، بر روی فایل Setup.exe دو بار کلیک کنید.



شکل ۱۵- ۳۵ نصب و راه‌اندازی Skype For Business

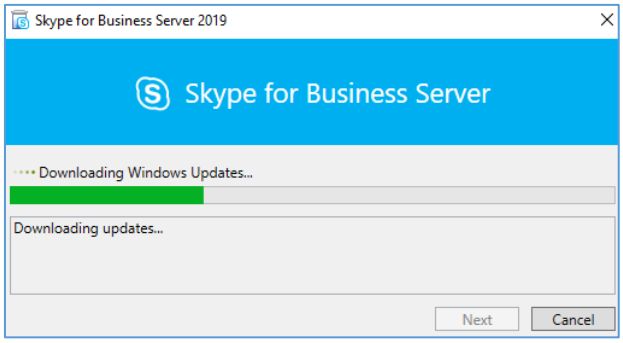
در شکل ۱۵-۳٦، اگر می‌خواهید آپدیت جدید نرم‌افزار دریافت شود گزینه‌ی اول را انتخاب کنید و مسیر ذخیره‌سازی آن را هم مشخص کنید.

www.takbook.com



شکل ۱۵- ۳۶ نصب و راه‌اندازی *Skype For Business*

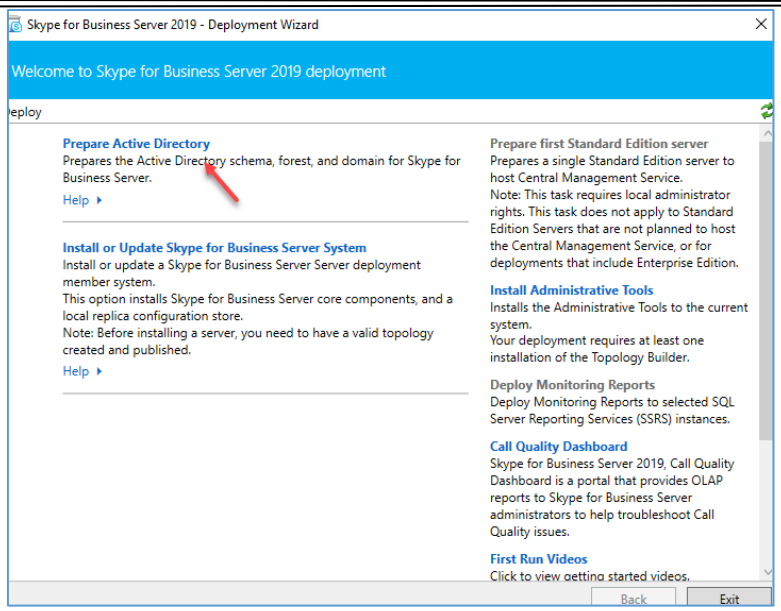
بعد از اینکه گزینه‌ی آپدیت انتخاب شد، در شکل ۱۵-۳۷، مشاهده می‌کنید که آخرین آپدیت در حال دریافت از سایت مایکروسافت است.



شکل ۱۵- ۳۷ نصب و راه‌اندازی *Skype For Business*

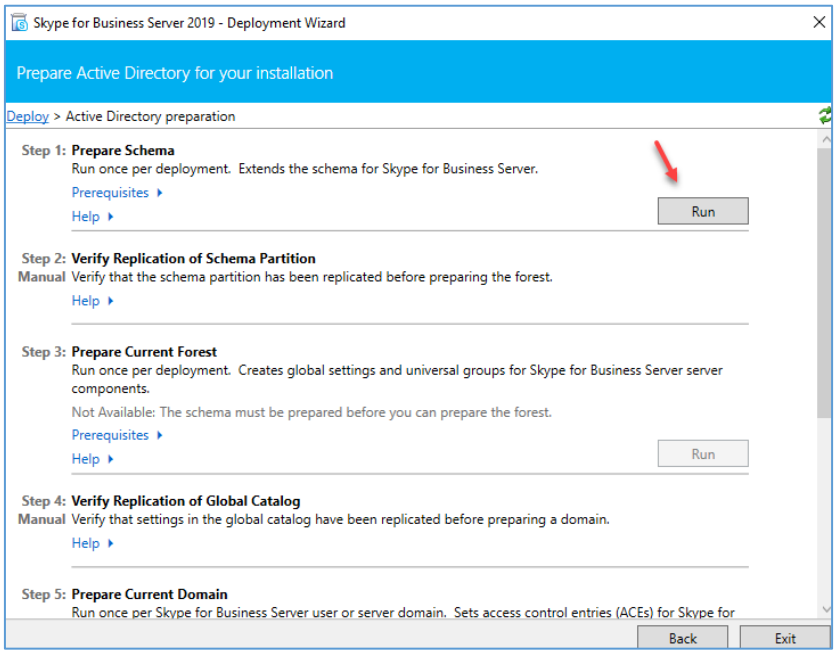
در شکل ۱۵-۳۸، برای شروع کار باید نرم‌افزار را با Active Directory هماهنگ کنیم، برای شروع بر روی Prepare Active Directory کلیک کنید.

www.takbook.com



شکل ۱۵- ۳۸ نصب و راه‌اندازی *Skype For Business*

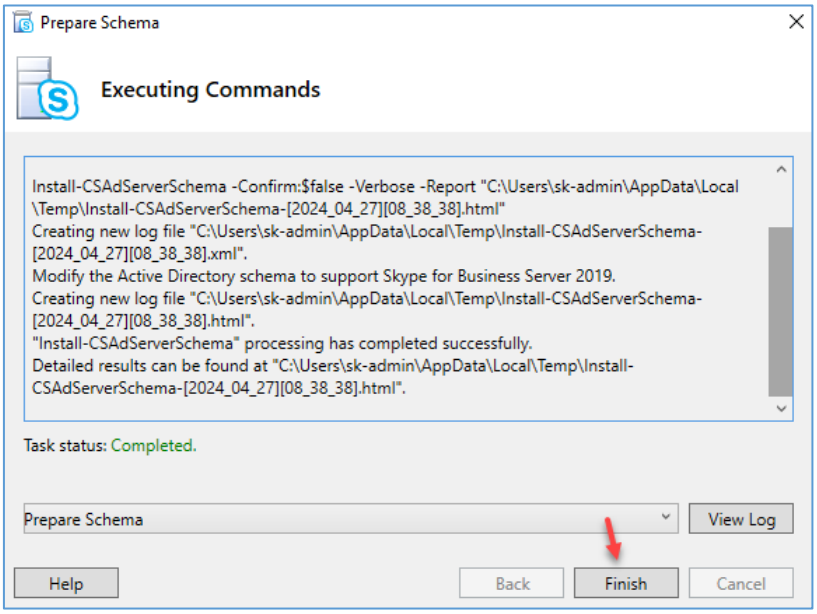
در شکل ۱۵-۳۹، سه مرحله وجود دارد که آنها را باید به ترتیب انجام دهید، به مانند شکل بر روی Run کلیک کنید.



شکل ۱۵- ۳۹ نصب و راه‌اندازی *Skype For Business*

www.takbook.com

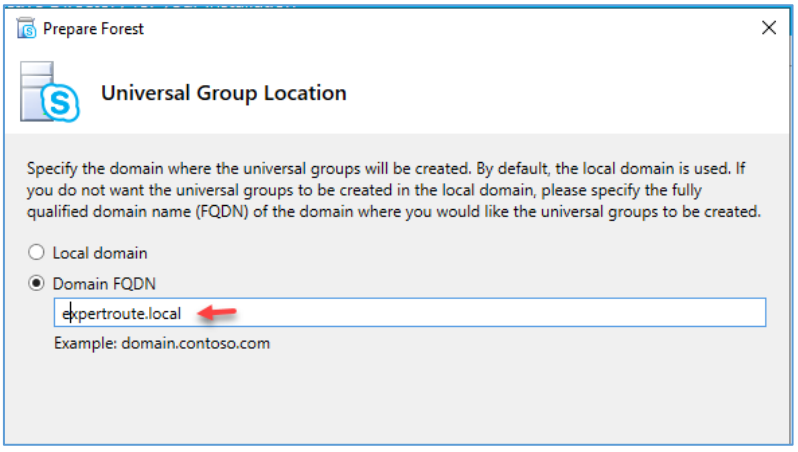
در شکل ۱۵-۴۰، بر روی Next کلیک کنید تا کار مورد نظر انجام شود و در آخر بر روی Finish کلیک کنید، توجه داشته باشید باید کلمه Completed را به مانند شکل ۱۵-۴۰، مشاهده کنید.



شکل ۱۵- ۴۰ نصب و راه‌اندازی Skype For Business

بعد از انجام مرحله‌ی اول بر روی مرحله‌ی دوم یعنی Prepare Current Forest کلیک کنید.

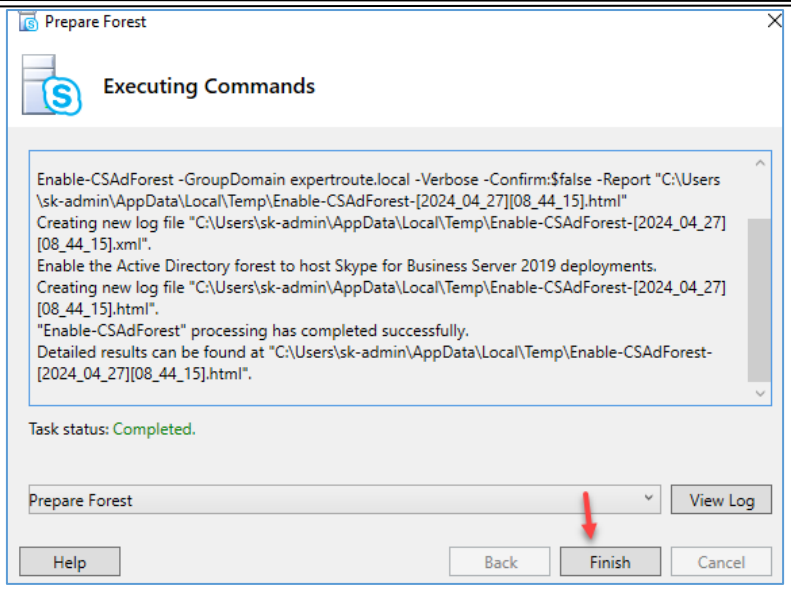
در شکل ۱۵-۴۱، گزینه‌ی Domain FQDN را انتخاب و آدرس دومین خود را وارد کنید.



شکل ۱۵- ۴۱ نصب و راه‌اندازی Skype For Business

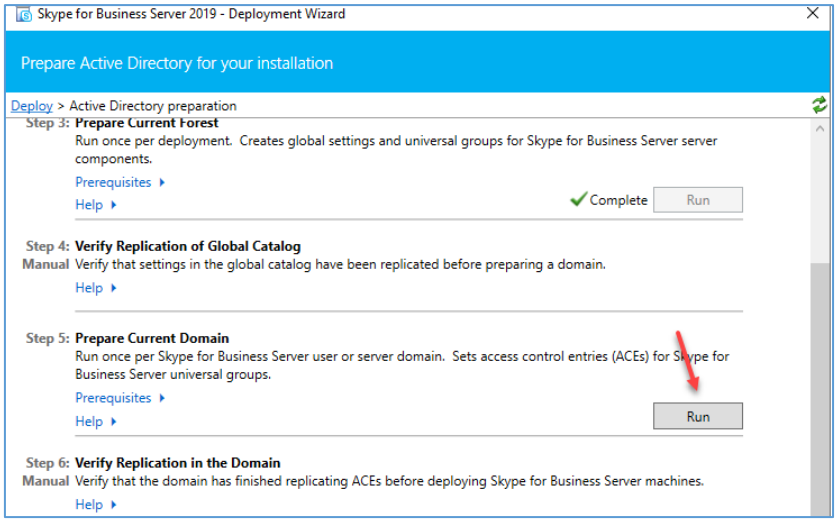
در آخر هم بعد از تایید به مانند شکل ۱۵-۴۲، بر روی Finish کلیک کنید.

www.takbook.com



شکل ۱۵- ۴۲ نصب و راه‌اندازی *Skype For Business*

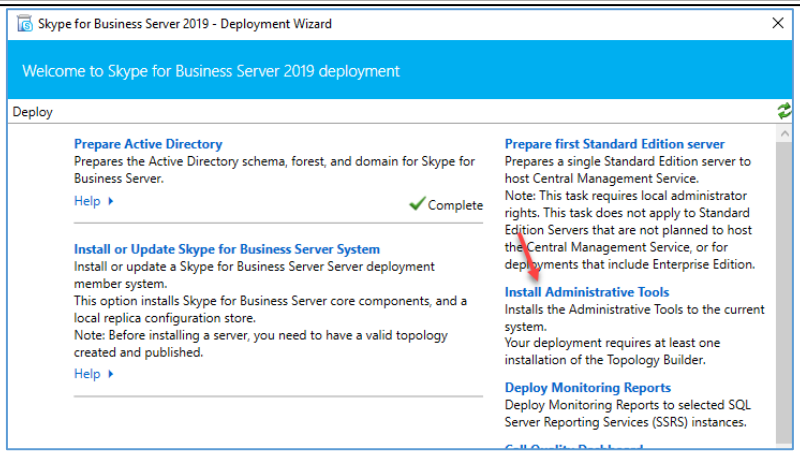
به مانند شکل ۱۵-٤۳، بر روی مرحله‌ی سوم کلیک کنید تا کار به اتمام برسد.



شکل ۱۵- ۴۳ نصب و راه‌اندازی *Skype For Business*

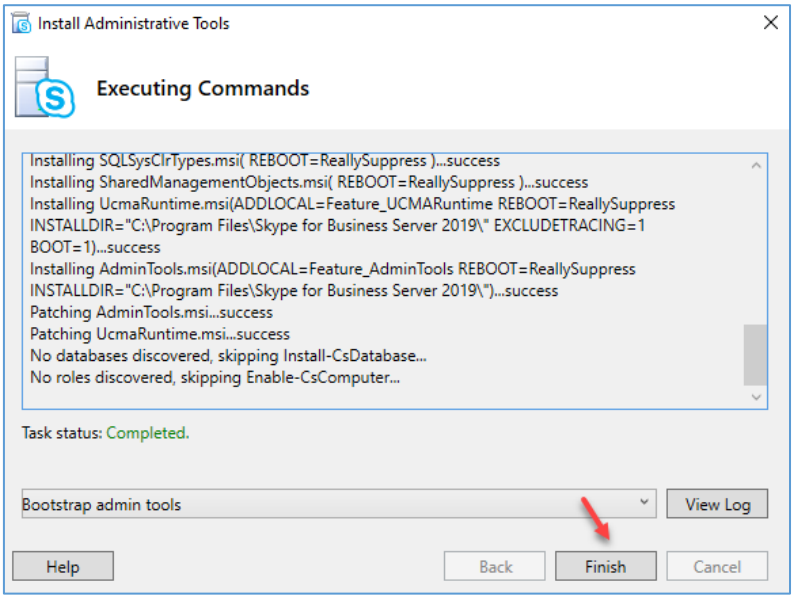
بر روی Back کلیک کنید و به صفحه‌ی اول برگردید، همان‌طور که در شکل ۱۵-٤٤، مشاهده می‌کنید قسمت اول به طور کامل تکمیل شده است و در ادامه بر روی Install Administrative Tools کلیک کنید.

www.takbook.com



شکل ۱۵- ۴۴ نصب و راه‌اندازی Skype For Business

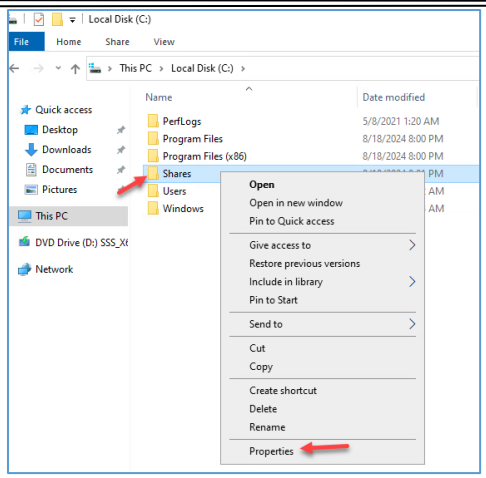
همان‌طور که در شکل ۱۵-۴۵، مشاهده می‌کنید این مرحله هم به درستی نصب شده است.



شکل ۱۵- ۴۵ نصب و راه‌اندازی Skype For Business

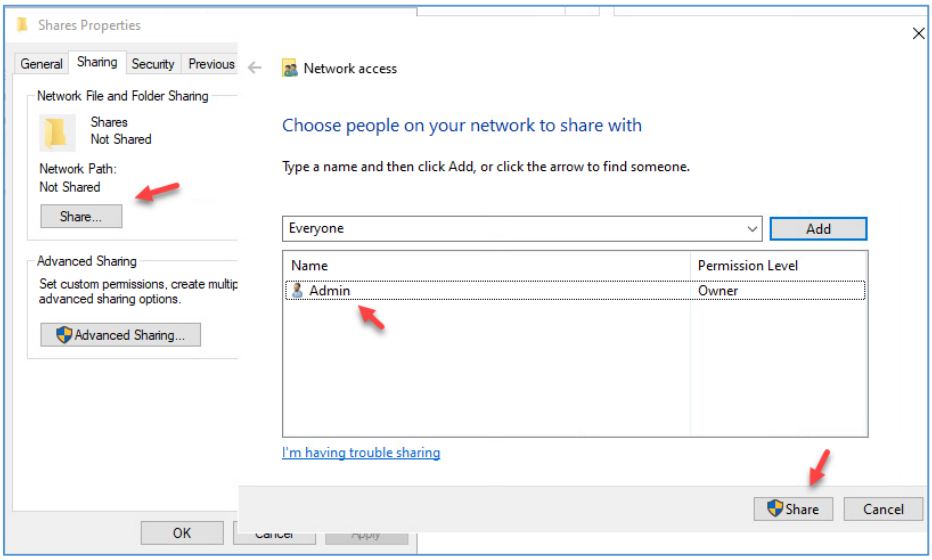
در ادامه کار برای اینکه تنظیمات مربوط به نرم‌افزار Skype For Business را در یک مکان مشخص قرار دهیم باید یک پوشه Share شده ایجاد کنیم، این پوشه می‌تواند در سرور Skype باشد و یا هر سروری دیگر که به شبکه متصل است، ما این پوشه را در سروری SQL ایجاد می‌کنیم و از آن استفاده می‌کنیم، به مانند شکل ۱۵-۴۶، وارد درایو C سرور SQL می‌شویم و یک فولدر با نام Shares ایجاد و وارد جزئیات آن می‌شویم.

www.takbook.com



شکل ۱۵- ۴۶ نصب و راه‌اندازی Skype For Business

به مانند شکل ۱۵-۴۷، وارد تب Sharing شوید و بر روی Share کلیک کنید و در صفحه‌ی باز شده بر روی Share کلیک کنید تا پوشه مورد نظر برای کاربر Admin به اشتراک گذاشته شود.



شکل ۱۵- ۴۷ نصب و راه‌اندازی Skype For Business

شکل ۱۵- ۴۸ نصب و راه‌اندازی Skype For Business

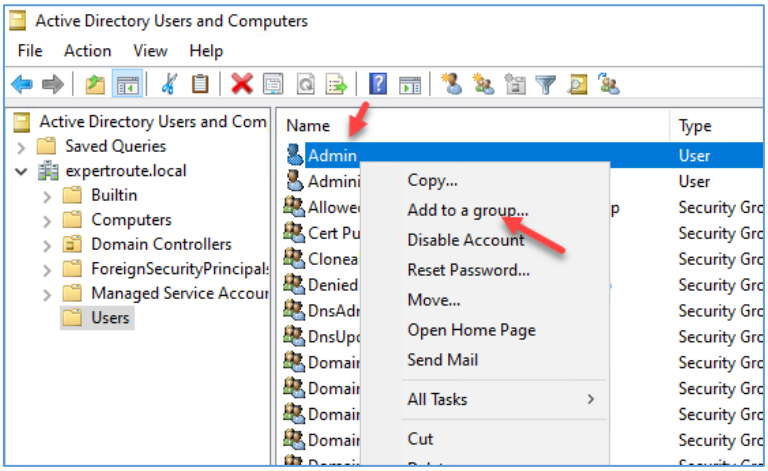
یک نکته مهم در این قسمت وجود دارد و آن هم این است که کاربر Admin باید عضو گروهای خاصی که در زیر لیست آن را مشاهده می‌کنید شود.

- RTC Component Universal Services
- RTC Universal Server Admins

www.takbook.com

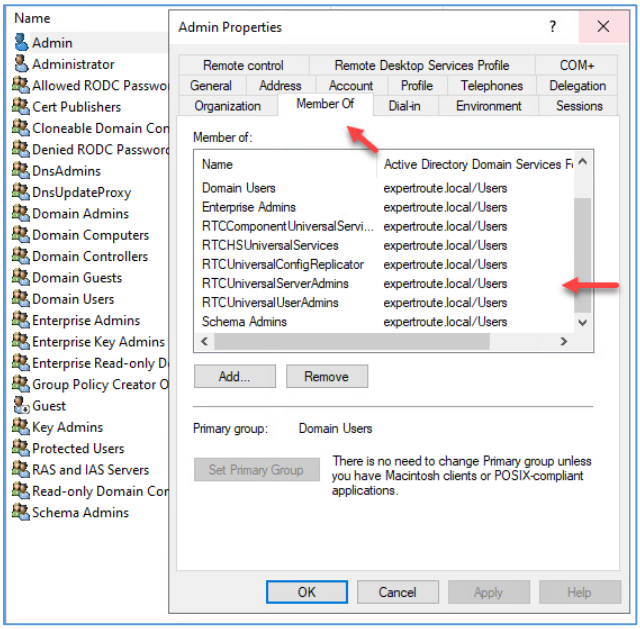
- RTC Universal Config Replicator
- RTCHS Universal Services
- RTC Universal user Admins

برای انجام این کار وارد Active Directory شوید و کاربر Admin را به مانند شکل ۱۵-۴۹، عضو این گروه‌ها کنید.



شکل ۱۵- ۴۹ نصب و راه‌اندازی Skype For Business

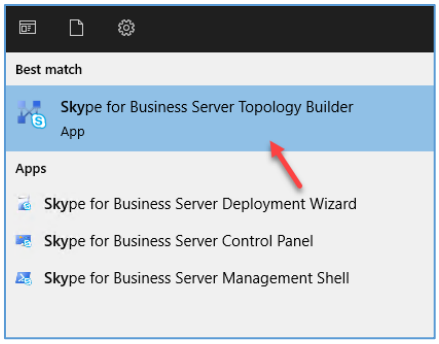
همان‌طور که در شکل ۱۵-۵۰، مشاهده می‌کنید گروه‌های مورد نظر به لیست اضافه شده است.



شکل ۱۵- ۵۰ نصب و راه‌اندازی Skype For Business

www.takbook.com

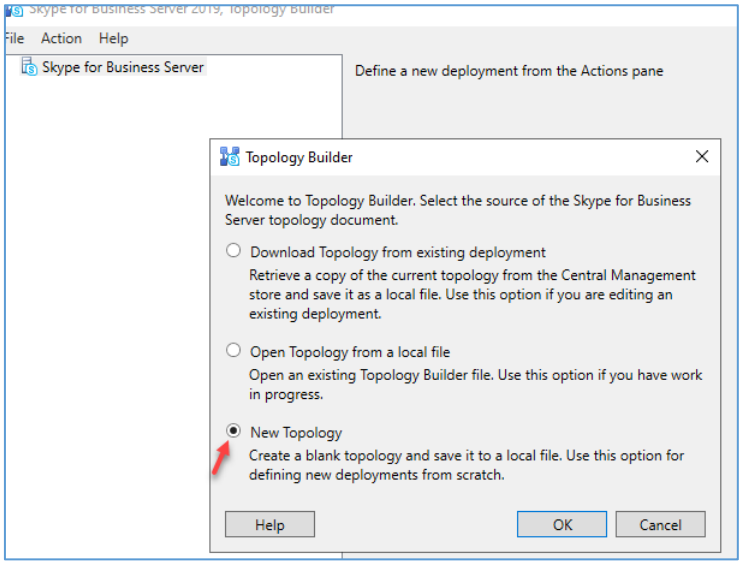
در ادامه کار باید وارد سرویس Skype for Business Server Topology Builder شویم و تنظیمات اصلی سرور را انجام دهیم، برای این کار به مانند شکل ۱۵-۵۱، در جستجو سرویس مورد نظر را انتخاب و اجرا کنید.



شکل ۱۵- ۵۱ نصب و راه‌اندازی *Skype For Business*

در شکل ۱۵-۵۲، برای شروع باید یک Topology ایجاد کنید؛ هر Topology دارای تنظیمات خاصّ خود است. در این صفحه، گزینه‌ی New Topology را انتخاب و بر روی OK کلیک کنید.

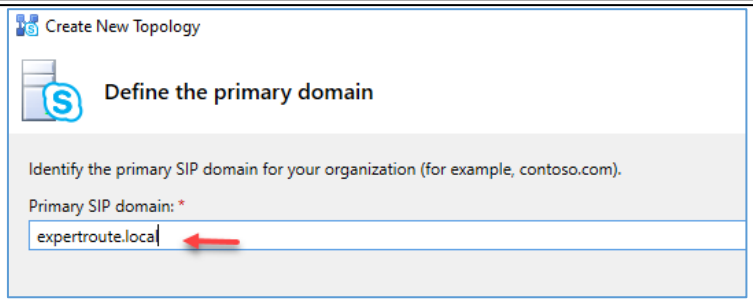
بعد از OK، صفحه‌ای باز می‌شود که باید این Topology را در جای مشخّص ذخیره کنید.



شکل ۱۵- ۵۲ نصب و راه‌اندازی *Skype For Business*

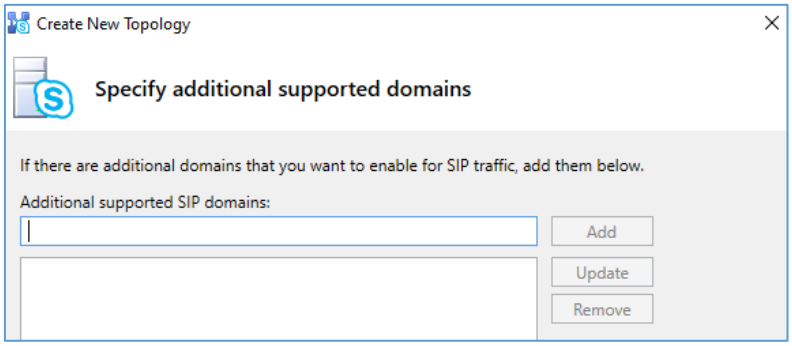
در شکل ۱۵-۵۳، باید آدرس دومین خود را وارد کنید.

www.takbook.com



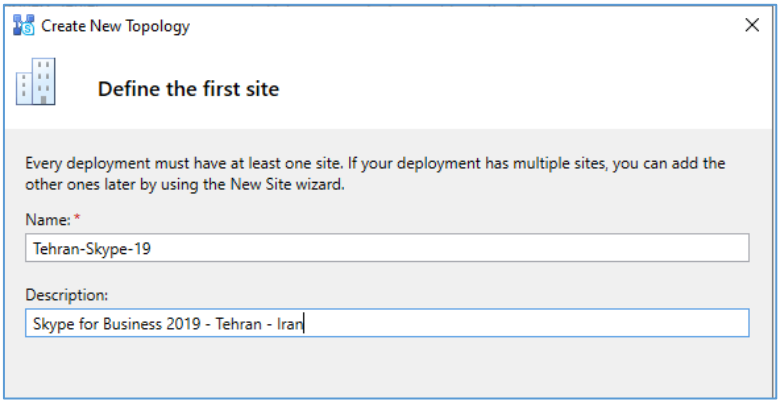
شکل ۱۵- ۵۳ نصب و راه‌اندازی *Skype For Business*

در شکل ۱۵-۵٤، اگر دومین دیگری دارید و نیاز است تعریف کنید باید آدرس آن را در این قسمت اضافه کنید.



شکل ۱۵- ۵۴ نصب و راه‌اندازی *Skype For Business*

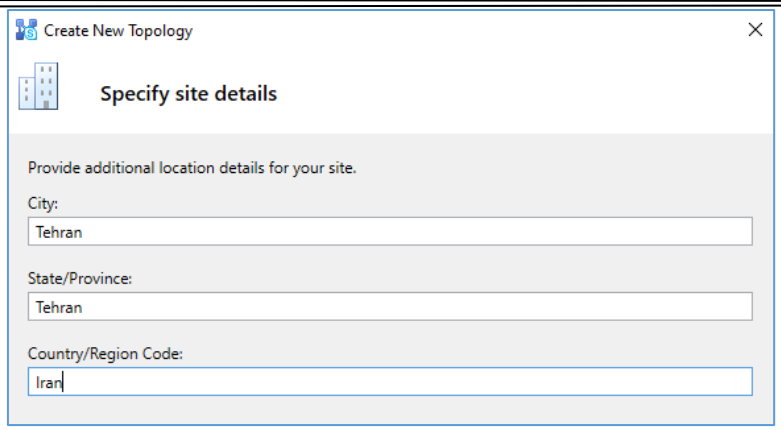
در شکل ۱۵-۵۵، یک نام به همراه توضیحات مورد نظر خود را واردکنید.



شکل ۱۵- ۵۵ نصب و راه‌اندازی *Skype For Business*

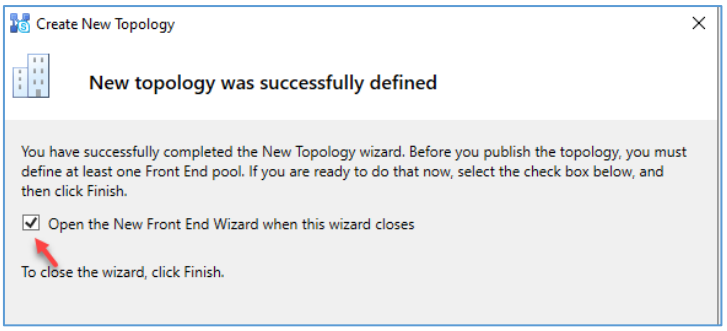
در شکل ۱۵-۵٦، نام شهر، استان و کشور را وارد کنید.

www.takbook.com



شکل ۱۵- ۵۶ نصب و راه‌اندازی Skype For Business

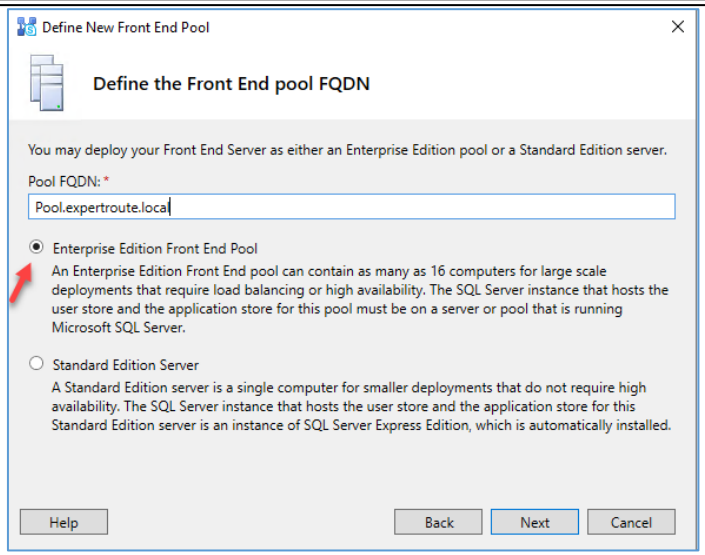
در شکل ۱۵-۵۷، تیک گزینه‌ی مورد نظر را انتخاب کنید تا صفحه‌ی بعد ظاهر شود.



شکل ۱۵- ۵۷ نصب و راه‌اندازی Skype For Business

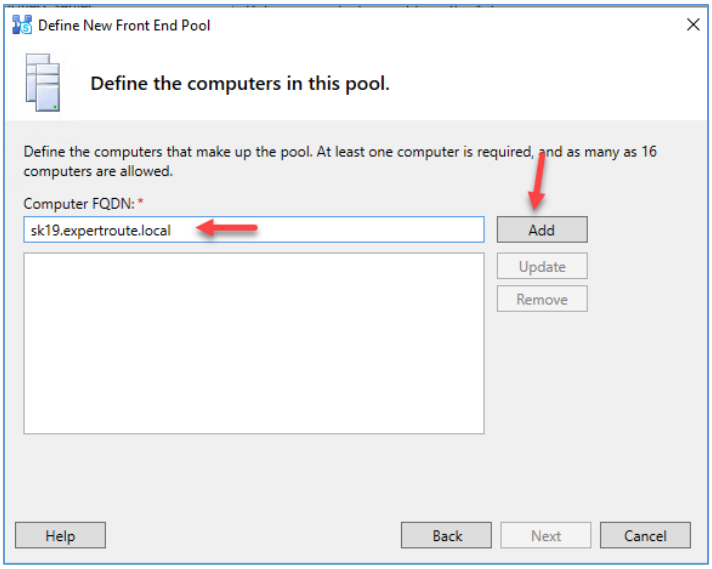
در شکل ۱۵-۵۸، دو گزینه را مشاهده می‌کنید، اگر گزینه‌ی Enterprise را انتخاب کنید باید برای نصب Skype بیشتر از یک سرور داشته باشید، مثلاً برای SQL نیاز به یک سرور دوم است که همین کار را هم انجام دادیم و سرور SQL را آماده و نرم‌افزار آن را نصب کردیم، یکی از ویژگی‌های گزینه‌ی Enterprise این است که ویژگی Load Balancing و High availability را می‌توان بر روی شبکه فعال کرد، آدرس Pool که در تنظیمات DNS ایجاد کردیم را در این قسمت وارد می‌کنیم.

www.takbook.com



شکل ۱۵- ۵۸ نصب و راه‌اندازی *Skype For Business*

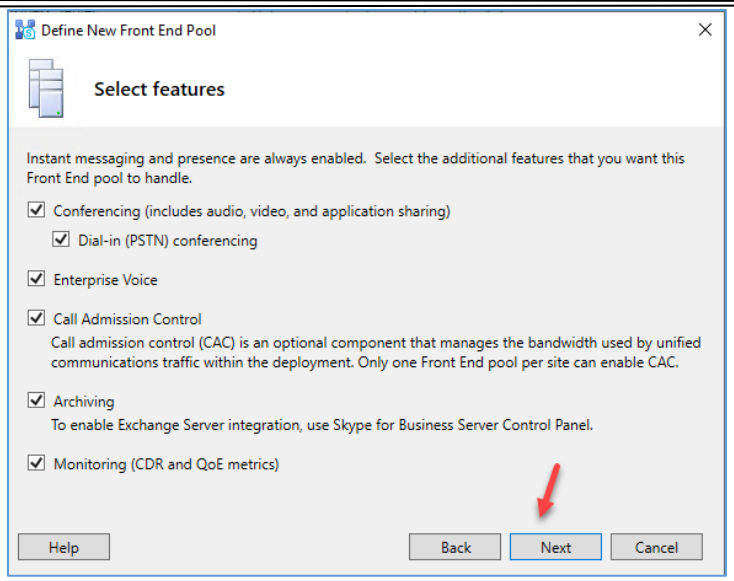
در شکل ۱۵-۵۹، باید نام سرور اسکایپ را وارد کنید که نام سرور همان SK19 است که در قسمت قبل مشاهده کردید.



شکل ۱۵- ۵۹ نصب و راه‌اندازی *Skype For Business*

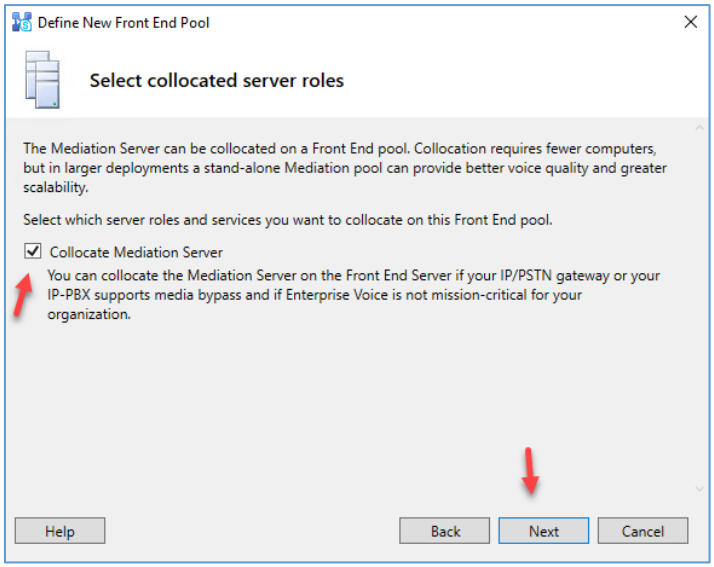
در شکل ۱۵-۶۰، همه‌ی ویژگی‌های نرم افزار را انتخاب کنید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۵- ۶۰ نصب و راه‌اندازی *Skype For Business*

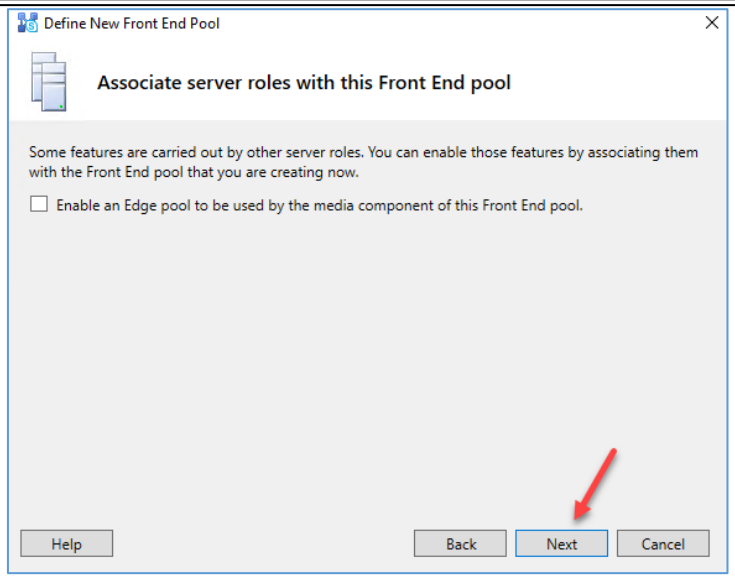
در شکل ۱۵-۶۱، تیک آن را انتخاب و بر روی Next کلیک کنید.



شکل ۱۵- ۶۱ نصب و راه‌اندازی *Skype For Business*

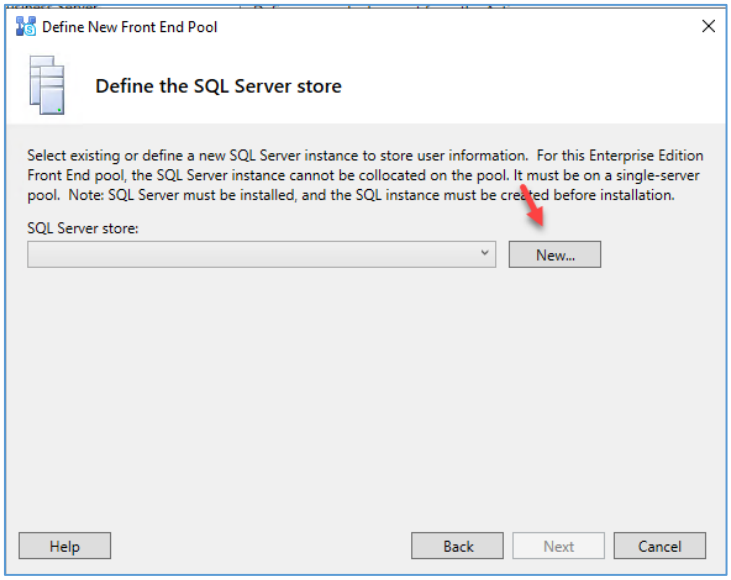
در شکل ۱۵-۶۲، فقط بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۵- ۶۲ نصب و راه‌اندازی *Skype For Business*

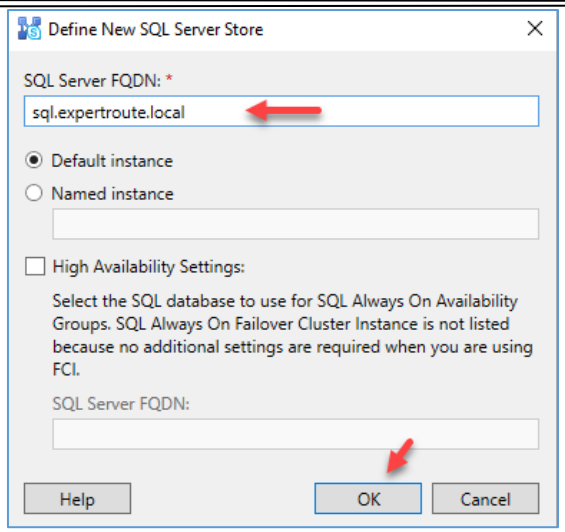
در شکل ۱۵-۶۳، باید سرور SQL که با هم ایجاد کردیم را به نرم‌افزار معرفی کنید، برای این کار باید بر روی New کلیک کنید.



شکل ۱۵- ۶۳ نصب و راه‌اندازی *Skype For Business*

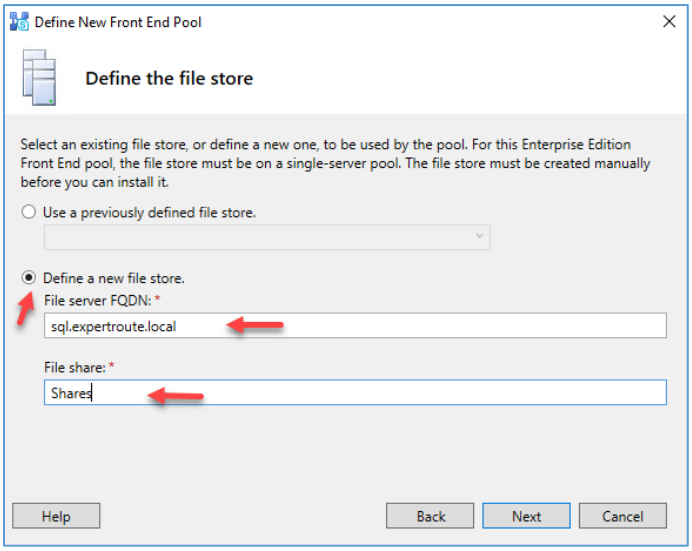
در شکل ۱۵-۶۴، باید آدرس سرور SQL را وارد کنید، اگر هم Instance جدید تعریف کردید باید آن را در قسمت Name instance وارد کنید وگرنه نیاز به وارد کردن آن نیست.

www.takbook.com



شکل ۱۵- ۶۴ نصب و راه‌اندازی *Skype For Business*

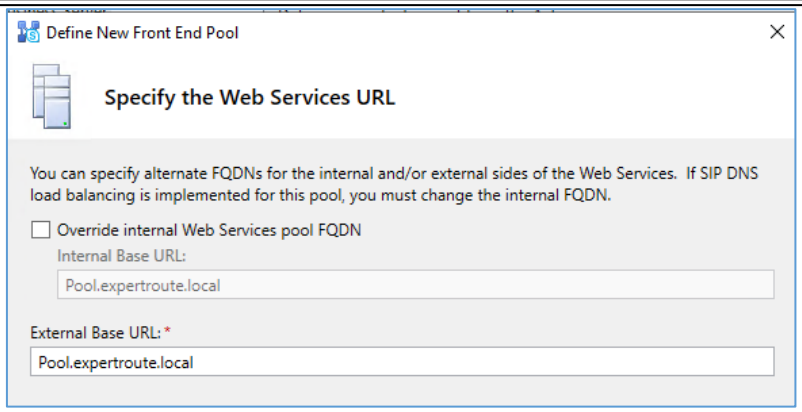
در شکل ۱۵-۶۵، باید همان فولدری را که در سرور SQL به اشتراک گذاشتیم را معرفی کنیم.



شکل ۱۵- ۶۵ نصب و راه‌اندازی *Skype For Business*

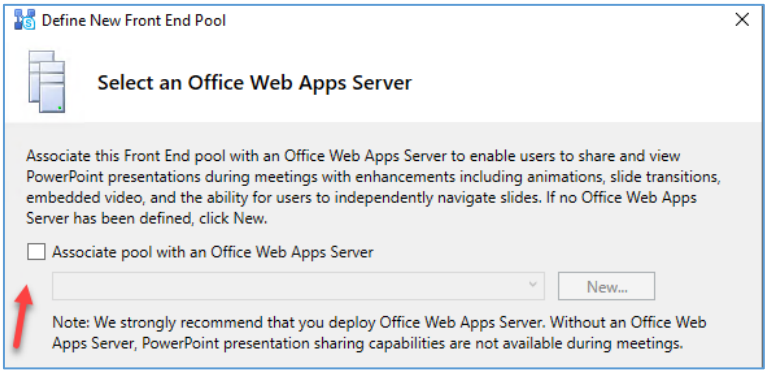
در شکل ۱۵-۶۶، فقط بر روی Next کلیک کنید.

www.takbook.com



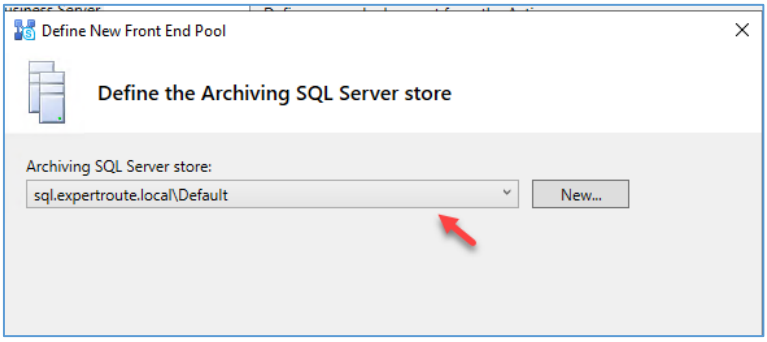
شکل ۱۵- ۶۶ نصب و راه‌اندازی *Skype For Business*

در شکل ۱۵-۶۷، اگر آفیس تحت وب دارید می‌توانید بر روی New کلیک کنید و آدرس آن را وارد کنید وگرنه تیک آن را بردارید و بر روی Next کلیک کنید.



شکل ۱۵- ۶۷ نصب و راه‌اندازی *Skype For Business*

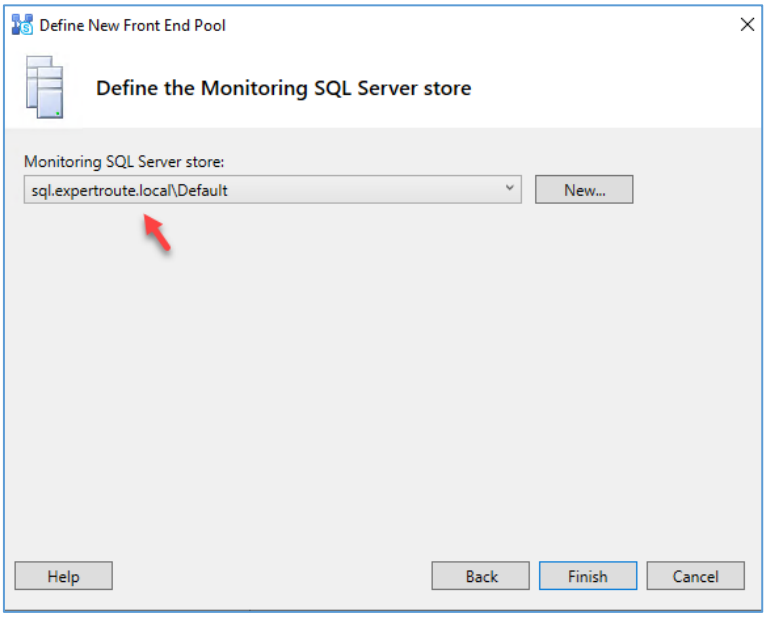
به مانند شکل ۱۵-۶۸، برای قسمت Archiving هم همان تنظیمات SQL را که انجام دادید انتخاب کنید.



شکل ۱۵- ۶۸ نصب و راه‌اندازی *Skype For Business*

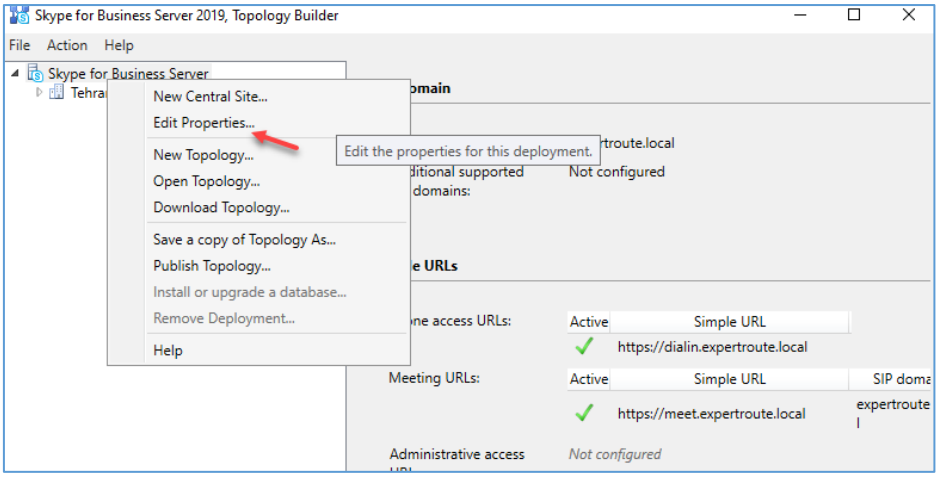
www.takbook.com

در شکل ۱۵-۶۹، باید تنظیمات SQL را انتخاب کنید تا اطلاعات مربوط به Monitoring بر روی آن قرار بگیرد.



شکل ۱۵- ۶۹ نصب و راه‌اندازی Skype For Business

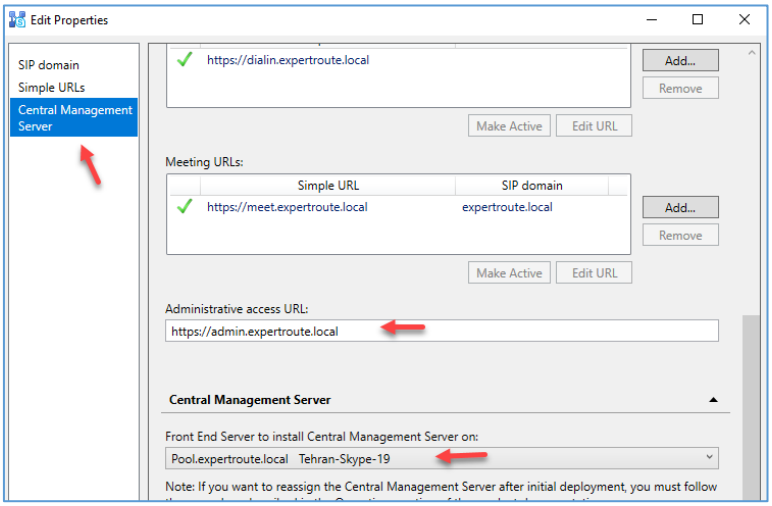
بعد از ایجاد توپولوژی مورد نظر به مانند شکل ۱۵-۷۰، بر روی آن کلیک راست کنید و گزینه‌ی Edit Properties را انتخاب کنید.



شکل ۱۵- ۷۰ نصب و راه‌اندازی Skype For Business

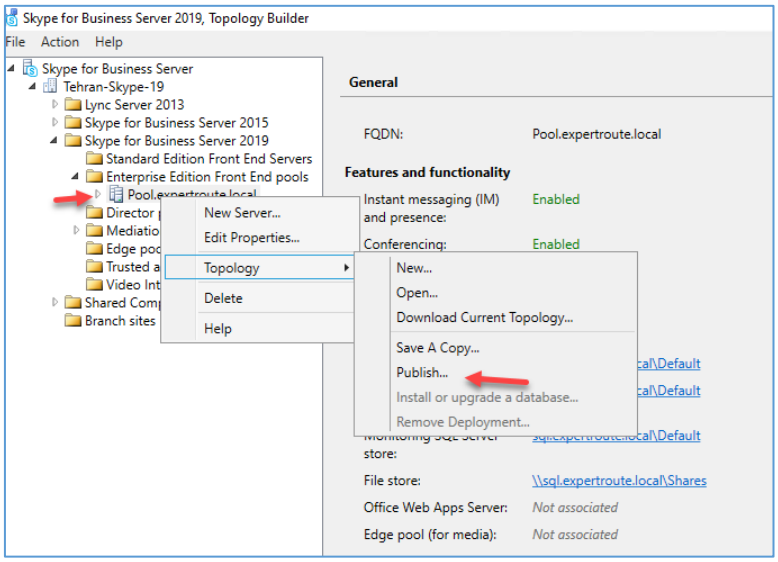
www.takbook.com

در شکل ۱۵-۷۱، در قسمت Administrative آدرس صفحه‌ی مدیریتی Skype را که قبلاً در DNS ایجاد کردیم را وارد کنید و در قسمت آخر هم Pool مورد نظر را انتخاب کنید.



شکل ۱۵- ۷۱ نصب و راه‌اندازی Skype For Business

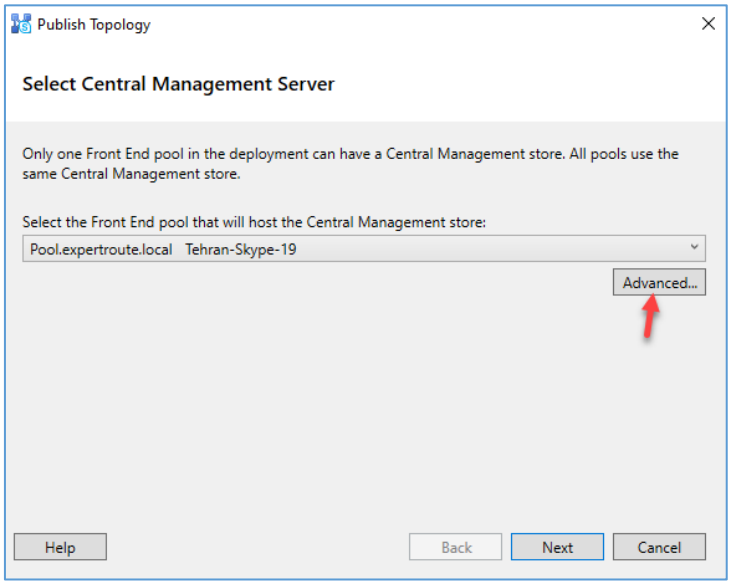
بعد از اتمام تمام مراحل بالا حالا باید اطلاعات و تنظیمات مورد نظر خود را فعال کنیم، برای این کار به مانند شکل ۱۵-۷۲، بر روی نام فایل خود کلیک راست کنید و از قسمت Topology بر روی Publish کلیک کنید.



شکل ۱۵- ۷۲ نصب و راه‌اندازی Skype For Business

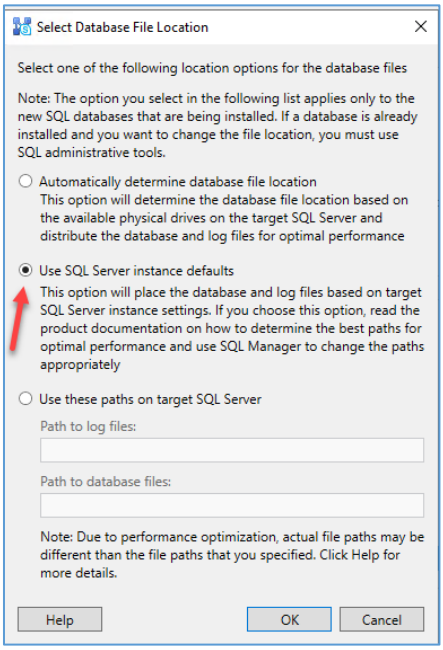
www.takbook.com

در شکل ۱۵-۷۳، به صورت خودکار Pool مورد نظر ایجاد شده است که باید بر روی Advanced کلیک کنید.



شکل ۱۵- ۷۳ نصب و راه‌اندازی *Skype For Business*

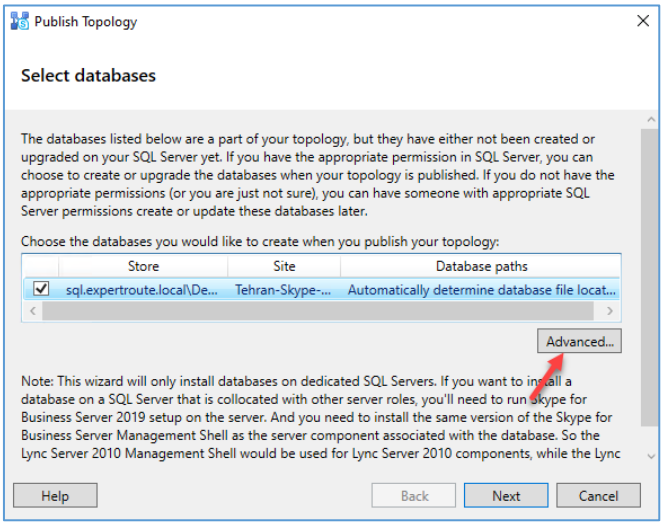
در شکل ۱۵-۷۴، باید گزینه‌ی Use SQL Server instance defults را انتخاب کنید.



شکل ۱۵- ۷۴ نصب و راه‌اندازی *Skype For Business*

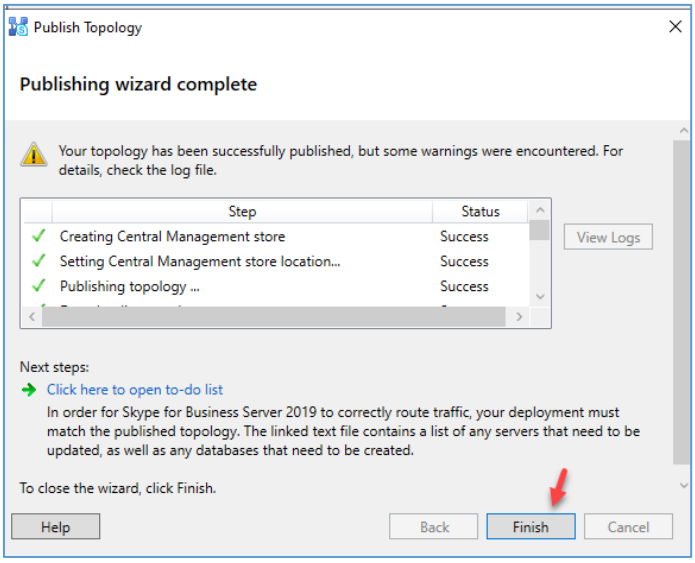
www.takbook.com

در ادامه و در شکل ۱۵-۷۶، بر روی Advanced کلیک و گزینه‌ی Use SQL Server instance defults را انتخاب کنید.



شکل ۱۵- ۷۵ نصب و راه‌اندازی Skype For Business

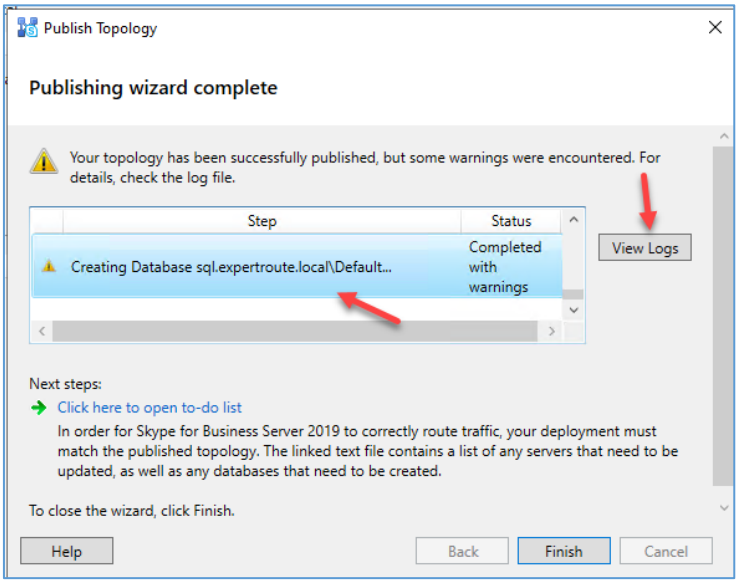
بعد از چند دقیقه تنظیمات بر روی سرور SQL اعمال و فایل‌ها در پوشه‌ی Shares قرار می‌گیرند و شکل نهایی به صورت ۱۵-۷۶، خواهد بود، توجه داشته باشید یک اخطار به ما اعلام کرده است که با هم آن را بررسی می‌کنیم.



شکل ۱۵- ۷۶ نصب و راه‌اندازی Skype For Business

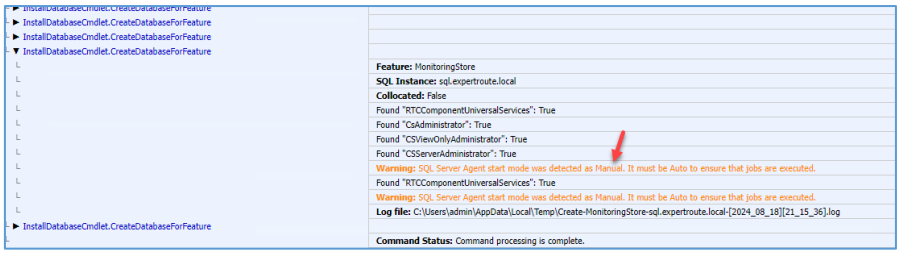
www.takbook.com

به مانند شکل ۱۵–۷۷، بر روی اخطار مورد نظر کلیک و بعد بر روی View Logs کلیک می‌کنیم تا مرورگر باز شود.



شکل ۱۵- ۷۷ نصب و راه‌اندازی *Skype For Business*

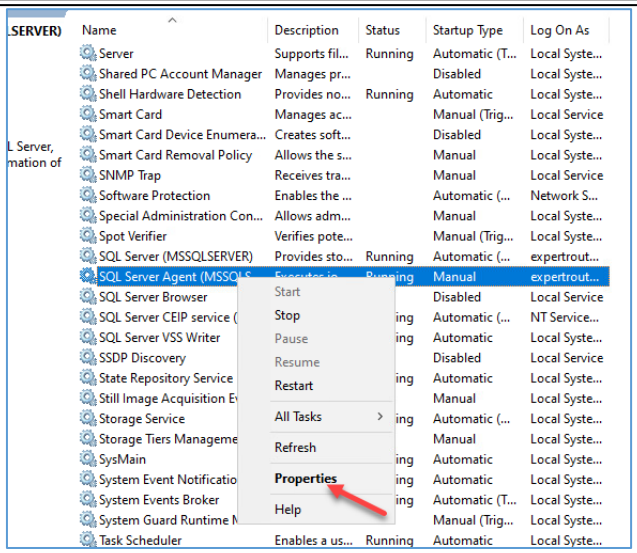
اگر به قسمتی که Warning دریافت کردیم مراجعه کنیم، به مانند شکل ۱۵–۷۸، مشخص است که مشکل از سرویس Agent در سرور SQL است که باید بر روی حالت اتوماتیک باشد ولی بر روی نرمال است.



شکل ۱۵- ۷۸ نصب و راه‌اندازی *Skype For Business*

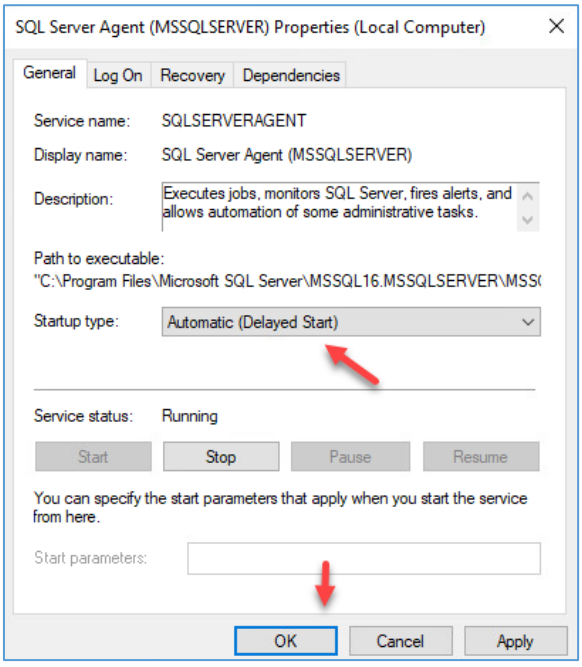
به مانند شکل ۱۵–۷۹، وارد سرور SQL می‌شویم و سرویس SQL Agent را بر روی Automatic قرار می‌دهیم.

www.takbook.com



شکل ۱۵- ۷۹ نصب و راه‌اندازی *Skype For Business*

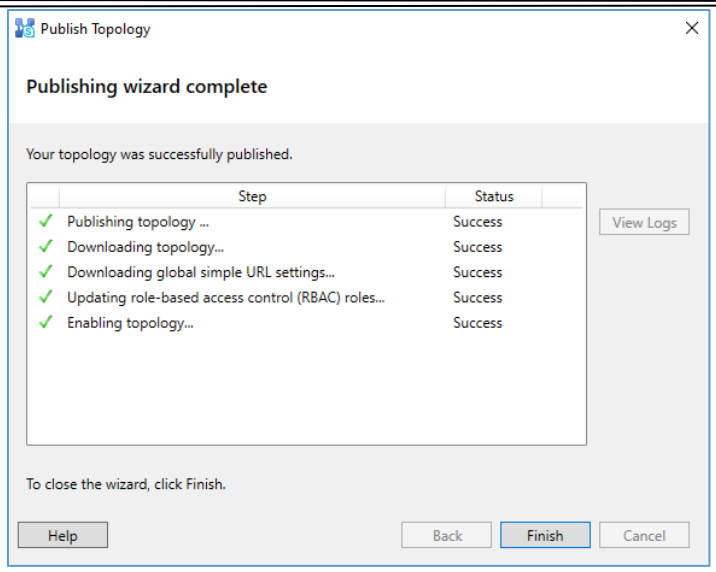
در شکل ۱۵-۸۰، بر روی حالت Automatic قرار می‌دهیم.



شکل ۱۵- ۸۰ نصب و راه‌اندازی *Skype For Business*

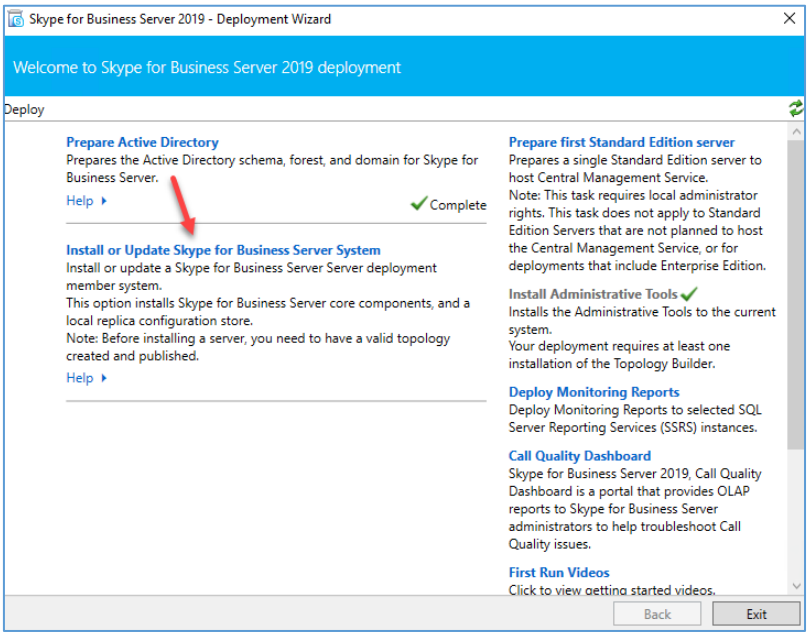
حالا اگر دوباره تنظیمات را در سرور اصلی Publish کنید شکل ۱۵-۸۱، بدون اخطار خواهد بود.

www.takbook.com



شکل ۱۵- ۸۱ نصب و راه‌اندازی *Skype For Business*

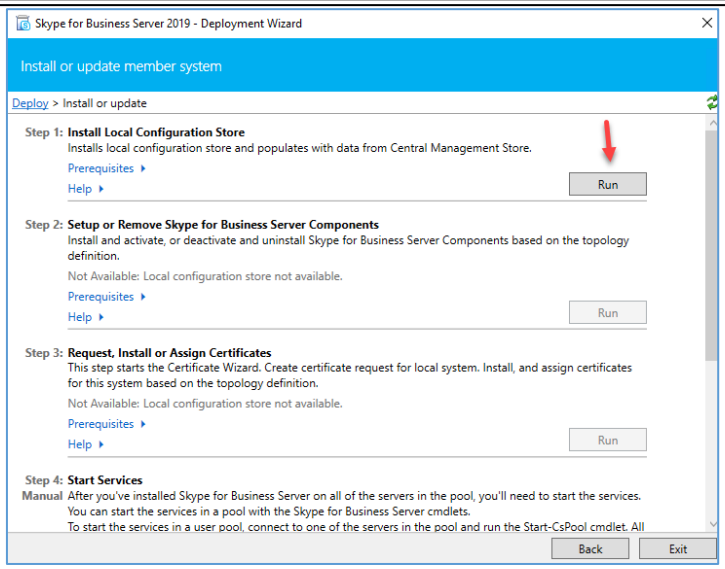
بعد از انجام مراحل بالا باید سرویس Deployment را اجرا کنید و در شکل باز شده‌ی ۱۵-۸۲، بر روی Install or Update Skype for Business Server System کلیک کنید.



شکل ۱۵- ۸۲ نصب و راه‌اندازی *Skype For Business*

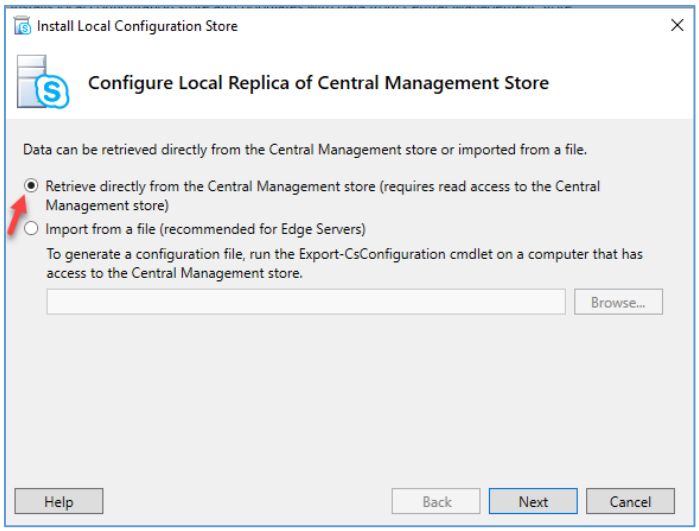
در شکل ۱۵-۸۳، از قسمت Install Local Configuration Store بر روی Run کلیک کنید.

www.takbook.com



شکل ۱۵- ۸۳ نصب و راه‌اندازی *Skype For Business*

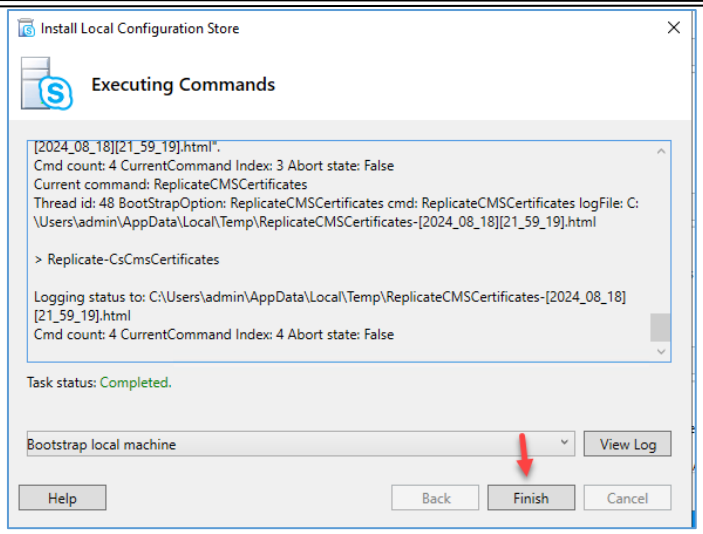
در شکل ۱۵-۸٤، گزینه‌ی اول را انتخاب کنیم و بر روی Next کلیک کنیم که بعد از چند دقیقه تنظیمات اعمال خواهد شد.



شکل ۱۵- ۸۴ نصب و راه‌اندازی *Skype For Business*

همان‌طور که در شکل ۱۵-۸۵، مشاهده می‌کنید با موفقیت تنظیمات اعمال شد.

www.takbook.com



شکل ۱۵- ۸۵ نصب و راه‌اندازی Skype For Business

قبل از ادامه کار، اگر از ویندوز سرور ۲۰۲۵ برای نصب Skype For Business استفاده می‌کنید باید اسکریپت زیر در Powershell اجرا کنید تا تنظیمات مورد نظر اعمال شود، برای این کار سرویس PowerShell ISE را اجرا کنید و کد زیر را در آن اجرا کنید.

```
$providerName = "AesProvider"
$keyContainerName = "iisCustomConfigurationKey"

$exe = Get-ChildItem -Path "$env:SystemRoot\Microsoft.NET\Framework64" -Filter "aspnet_regiis.exe" -Recurse -ErrorAction SilentlyContinue | Select-Object -First 1

if ($exe -eq $null)}
  Write-Error "aspnet_regiis.exe not found. Exiting;"
  Exit
{

$existingProvider = Get-WebConfiguration -PSPath 'MACHINE/WEBROOT/APPHOST' -Filter "configProtectedData/providers/add[@name='$providerName']"
if ($null -ne $existingProvider) { # Provider already exists
  Write-Host "Script has already run. $providerName already exists. Exiting"
  Exit 0
{

$ &exe.FullName -pc $keyContainerName -exp
$ &exe.FullName -pa $keyContainerName "BUILTIN\IIS_IUSRS"
$ &exe.FullName -pa $keyContainerName "NT SERVICE\WMSVC"
```

www.takbook.com

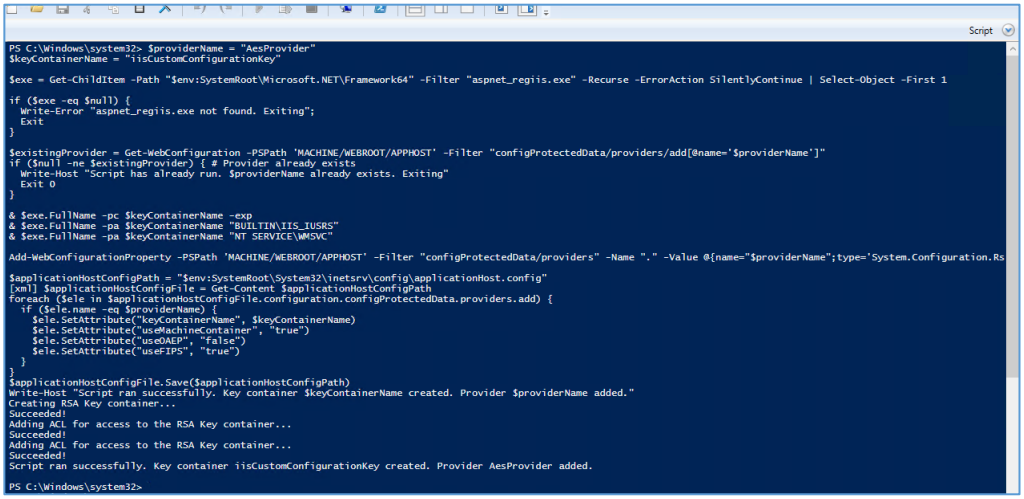

```
Add-WebConfigurationProperty -PSPath 'MACHINE/WEBROOT/APPHOST' -Filter "configProtectedData/providers" -Name "." -Value @{name="$providerName";type='System.Configuration.RsaProtectedConfigurationProvider,System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a'}

$applicationHostConfigPath = "$env:SystemRoot\System32\inetsrv\config\applicationHost.config"
[xml] $applicationHostConfigFile = Get-Content $applicationHostConfigPath
foreach ($ele in $applicationHostConfigFile.configuration.configProtectedData.providers.add){}
  if ($ele.name -eq $providerName){}
$    ele.SetAttribute("keyContainerName", $keyContainerName)
$    ele.SetAttribute("useMachineContainer", "true")
$    ele.SetAttribute("useOAEP", "false")
$    ele.SetAttribute("useFIPS", "true")
{
{
$applicationHostConfigFile.Save($applicationHostConfigPath)
Write-Host "Script ran successfully. Key container $keyContainerName created. Provider $providerName added."
```

اگر با کپی فایل مشکل دارید می‌توانید از لینک زیر فایل را دانلود کنید:

https://expertroute.ir/SK-2025.txt

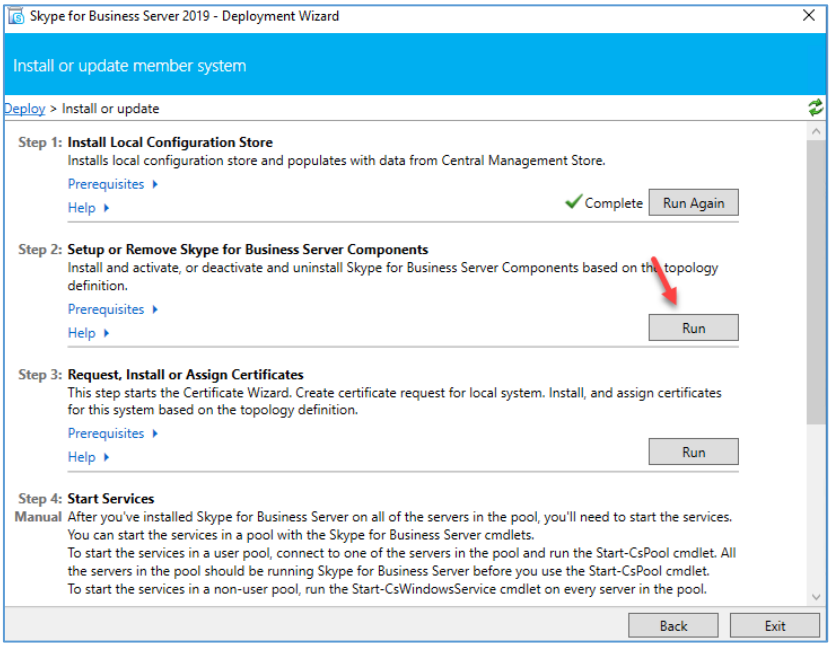
همان‌طور که در شکل ۱۵-۸۶، مشاهده می‌کنید فایل مورد نظر اجرا شده است و تنظیمات مورد نظر اعمال شده است.



شکل ۱۵-۸۶ نصب و راه‌اندازی Skype For Business

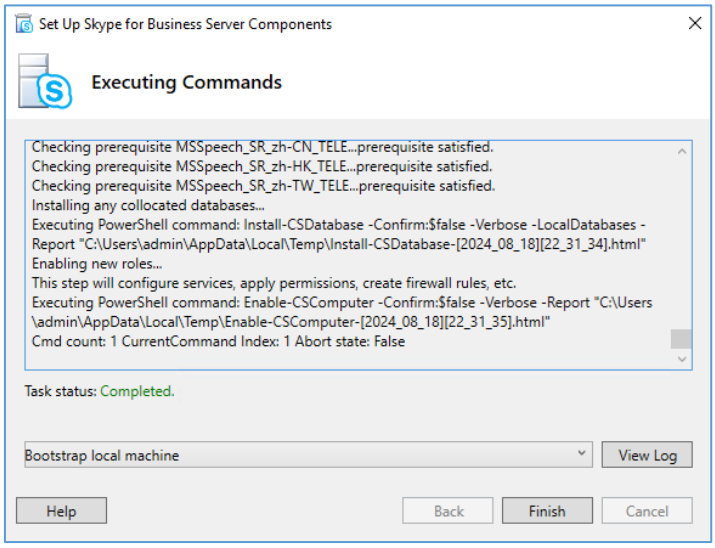
www.takbook.com

به مانند شکل ۱۵-۸۷، بر روی قسمت Setup or Remove Skype for Business Server Components کلیک کنید.



شکل ۱۵- ۸۷ نصب و راه‌اندازی *Skype For Business*

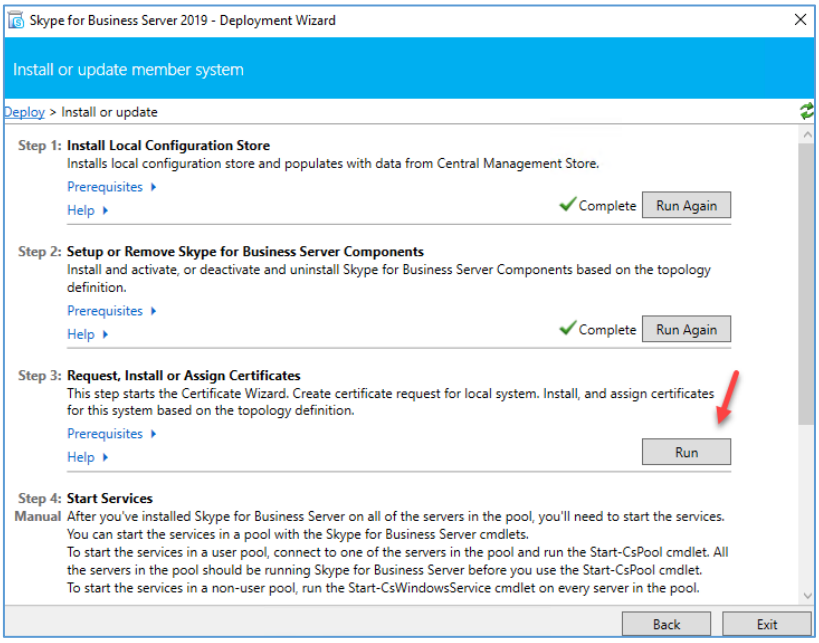
بعد از چند دقیقه تنظیمات مورد نظر به مانند شکل ۱۵-۸۸، اعمال خواهد شد.



شکل ۱۵- ۸۸ نصب و راه‌اندازی *Skype For Business*

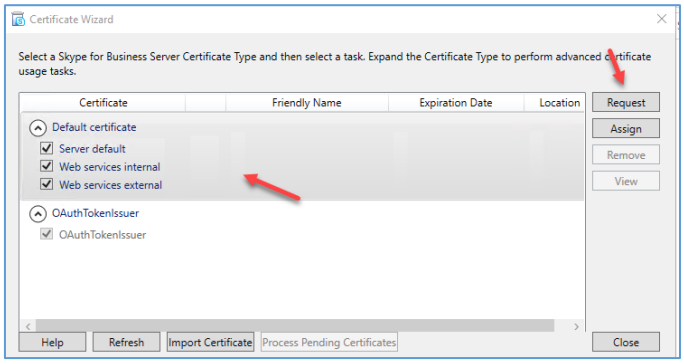
www.takbook.com

در شکل ۱۵-۸۹، در قسمت سوم یعنی Request, install or Assign Certificates می‌توانید گواهینامه مورد نظر را به سرور معرفی کنید.



شکل ۱۵- ۸۹ نصب و راه‌اندازی Skype For Business

در شکل ۱۵-۹۰، دو قسمت وجود دارد که برای درخواست گواهینامه داخلی طراحی شده است، برای شروع کار باید Default Certificate را انتخاب کنید و بر روی Request کلیک کنید.

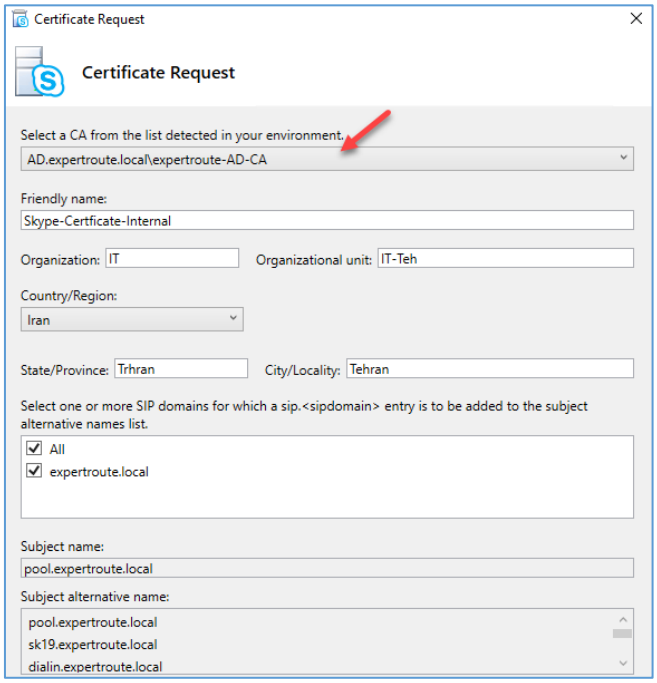


شکل ۱۵- ۹۰ نصب و راه‌اندازی Skype For Business

در شکل ۱۵-۹۱، در قسمت CA باید نام سروری که بر روی آن سرویس Certificate را راه‌اندازی کردید را مشخص کنید که اصولاً این سرویس بر روی سرور Active Directory نصب می‌شود که قبلاً هم آموزش

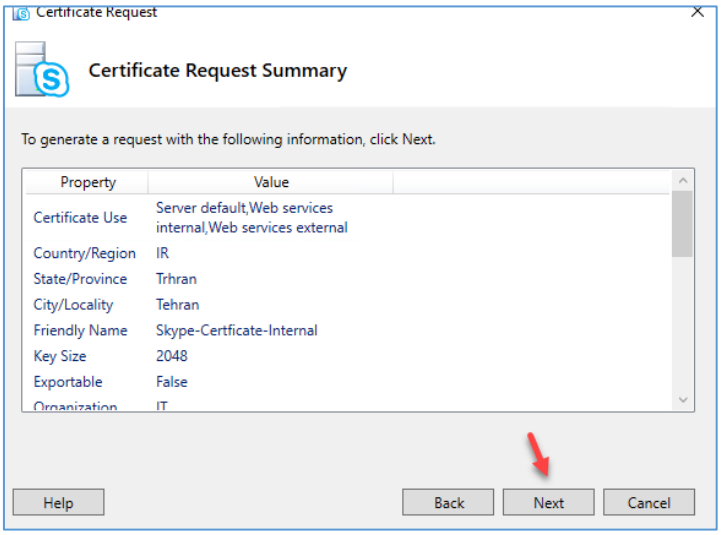
www.takbook.com

نصب آن را بررسی کردیم، در قسمت‌های دیگر اطلاعات دلخواه خود را وارد کنید و بر روی تیک ALL کلیک کنید تا دومین شما انتخاب شود و در آخر بر روی Next کلیک کنید.



شکل ۱۵- ۹۱ نصب و راه‌اندازی *Skype For Business*

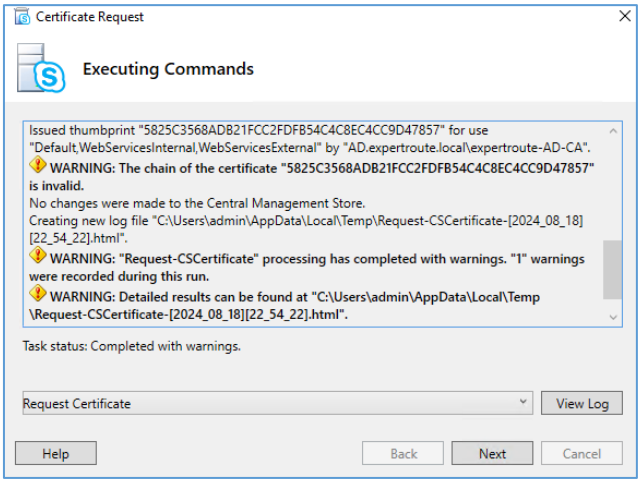
در شکل ۱۵-۹۲، اطلاعات نهایی را بررسی کنید و بر روی Next کلیک کنید تا تنظیمات اعمال شود.



شکل ۱۵- ۹۲ نصب و راه‌اندازی *Skype For Business*

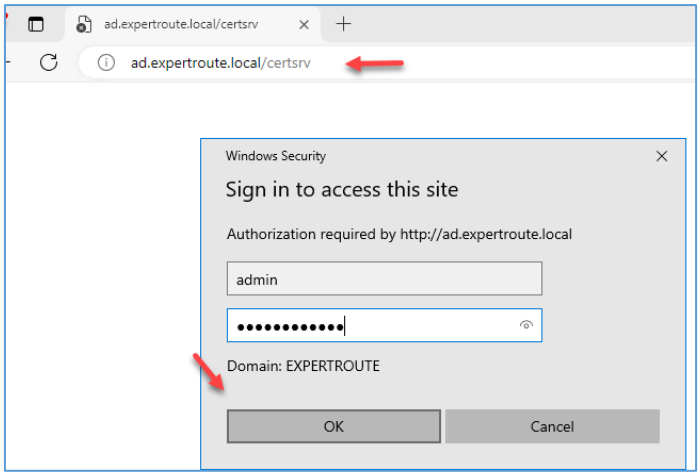
www.takbook.com

بعد از اینکه بر روی Next کلیک کردید در بعضی مواقع با اخطار صفحه‌ی شکل ۱۵-۹۳، مواجه خواهید شد که به این موضوع اشاره دارد که اول باید گواهینامه‌ی سرور AD را بر روی سرور SK2019 نصب کنید و بعد دوباره درخواست دهید تا تنظیمات به درستی اعمال شود.



شکل ۱۵- ۹۳ نصب و راه‌اندازی Skype For Business

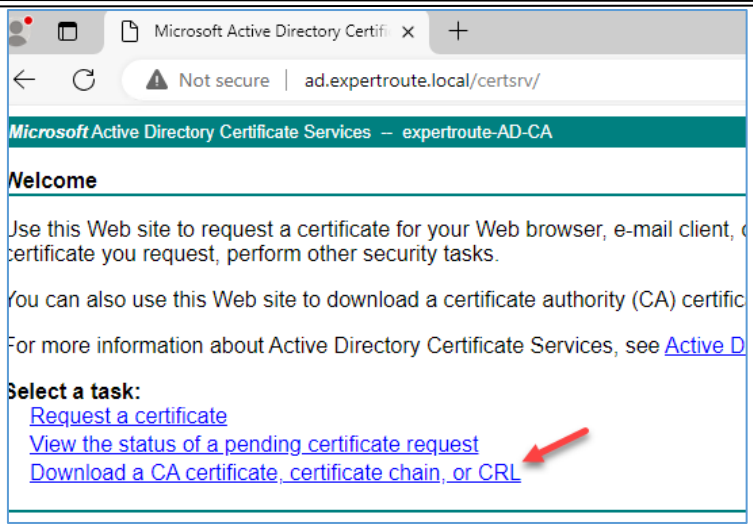
برای اعمال گواهینامه بر روی سرور SK2019 باید مرورگر خود را باز کنید و وارد آدرس زیر شوید:
http://ad.expertroute.local/certsrv
توجه داشته باشید به جای ad.expertroute.local آدرس سرور Active خود راوارد کنید.
در شکل ۱۵-۹٤، باید نام کاربری Admin را وارد کنید.



شکل ۱۵- ۹۴ نصب و راه‌اندازی Skype For Business

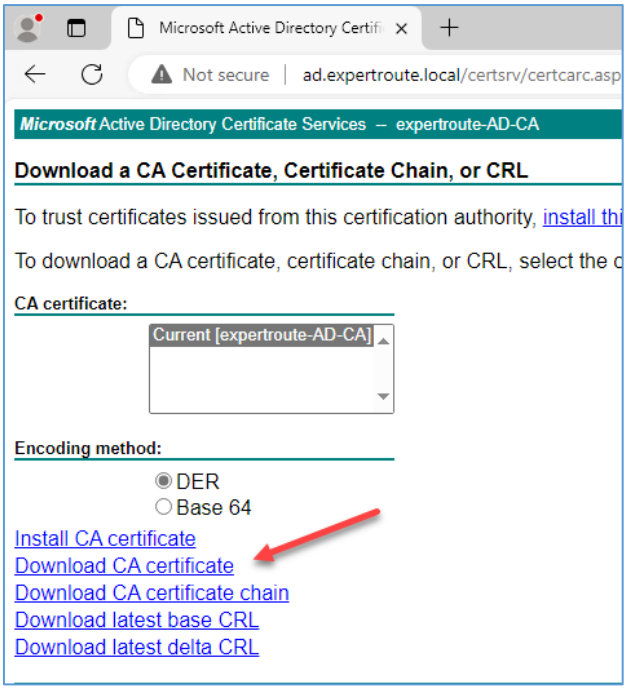
در شکل ۱۵-۹۵، بر روی لینک Download کلیک کنید.

www.takbook.com



شکل ۱۵- ۹۵ نصب و راه‌اندازی *Skype For Business*

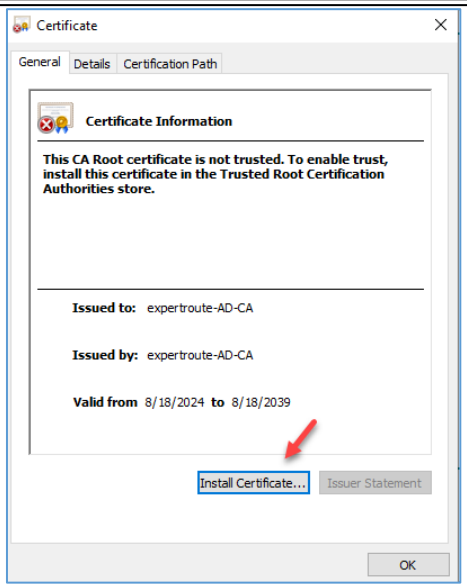
در شکل ۱۵-۹۶، هم بر روی Download CA certificate کلیک کنید.



شکل ۱۵- ۹۶ نصب و راه‌اندازی *Skype For Business*

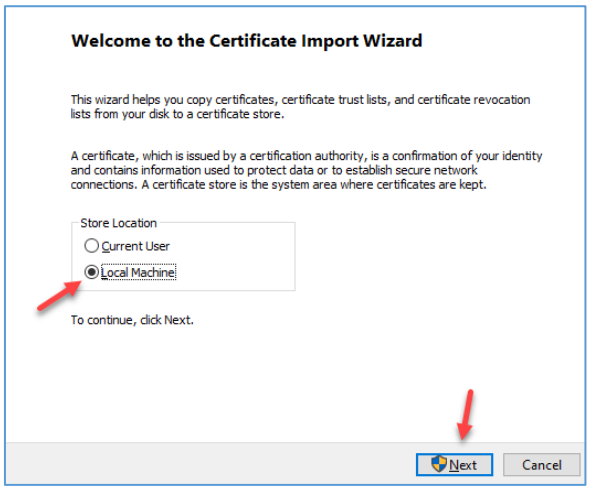
بعد از گواهینامه‌ی مورد نظر آن را باز کنید و به مانند شکل ۱۵-۹۷، بر روی Install Certificate کلیک کنید.

www.takbook.com



شکل ۱۵- ۹۷ نصب و راه‌اندازی *Skype For Business*

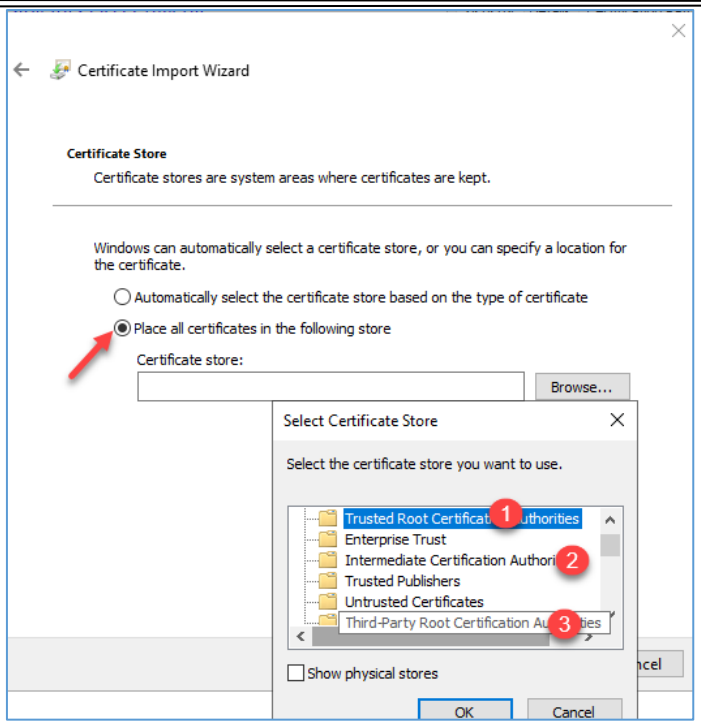
در شکل ۱۵-۹۸، گزینه‌ی Local Machine را انتخاب کنید تا گواهینامه بر روی سیستم شما نصب شود.



شکل ۱۵- ۹۸ نصب و راه‌اندازی *Skype For Business*

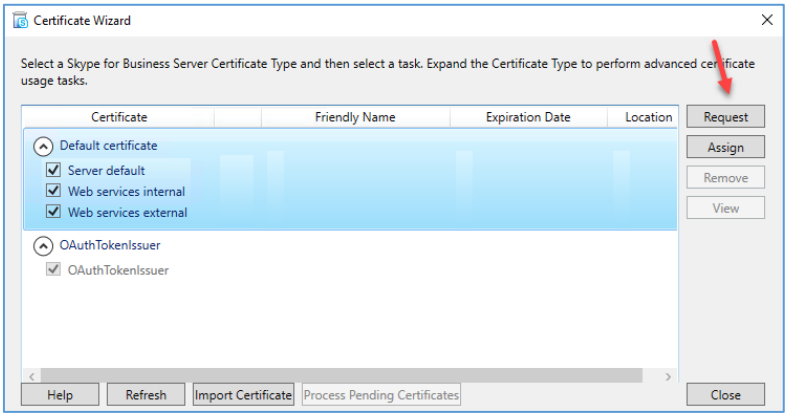
در شکل ۱۵-۹۹، گزینه‌ی Place all Certificate in the following store را انتخاب کنید و بر روی Browse کلیک کنید و باید هر سه گزینه را انتخاب کنید تا گواهینامه در این قسمت‌ها نصب شود، یعنی سه بار باید این کار را انجام دهید.

www.takbook.com



شکل ۱۵- ۹۹ نصب و راه‌اندازی *Skype For Business*

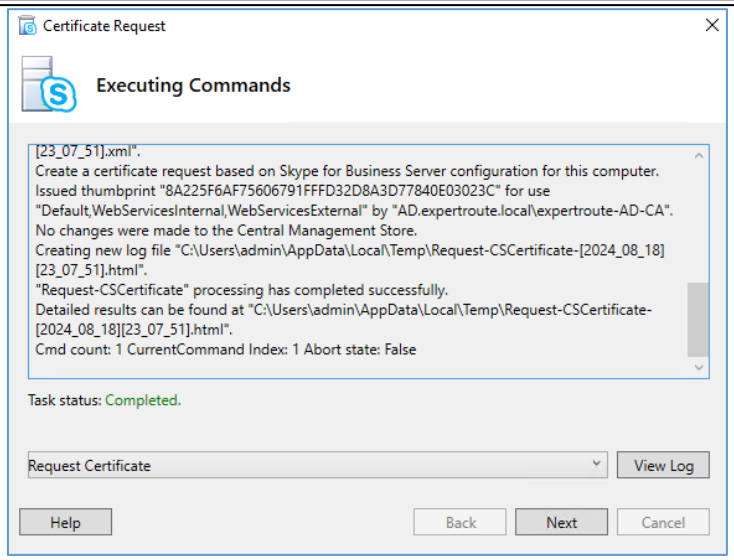
بعد از انجام مراحل بالا دوباره وارد تنظیمات Skype شوید و به مانند شکل ۱۵-۱۰۰، درخواست گواهینامه را دوباره تکرار کنید.



شکل ۱۵- ۱۰۰ نصب و راه‌اندازی *Skype For Business*

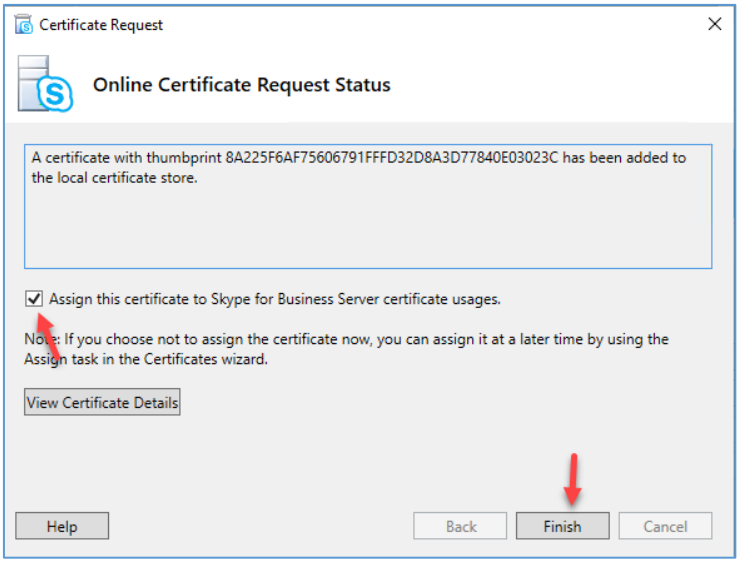
همان‌طور که در شکل ۱۵-۱۰۱، مشاهده می‌کنید گواهینامه مورد نظر با موفقیت نصب شده است.

www.takbook.com



شکل ۱۵- ۱۰۱ نصب و راه‌اندازی *Skype For Business*

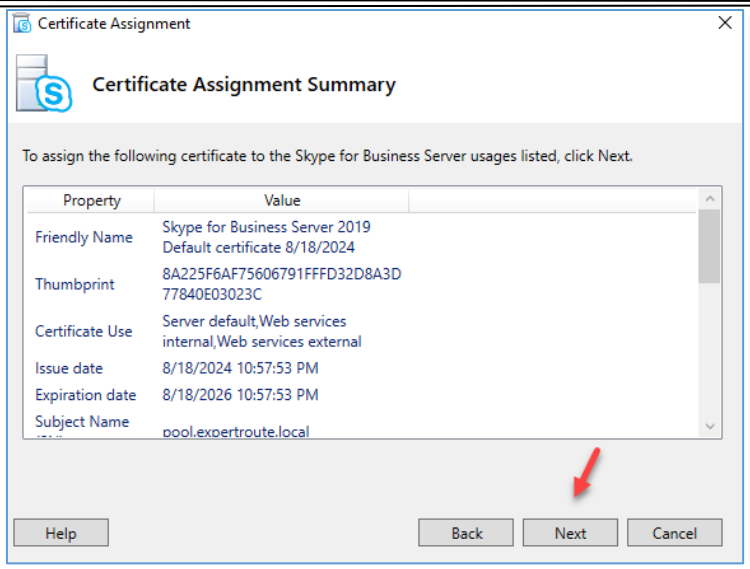
در ادامه شکل ۱۵-۱۰۲، را مشاهده می‌کنید که بعد از درخواست باید گواهینامه را فعال کنید که تیک گزینه‌ی مورد نظر را انتخاب و Finish کنید.



شکل ۱۵- ۱۰۲ نصب و راه‌اندازی *Skype For Business*

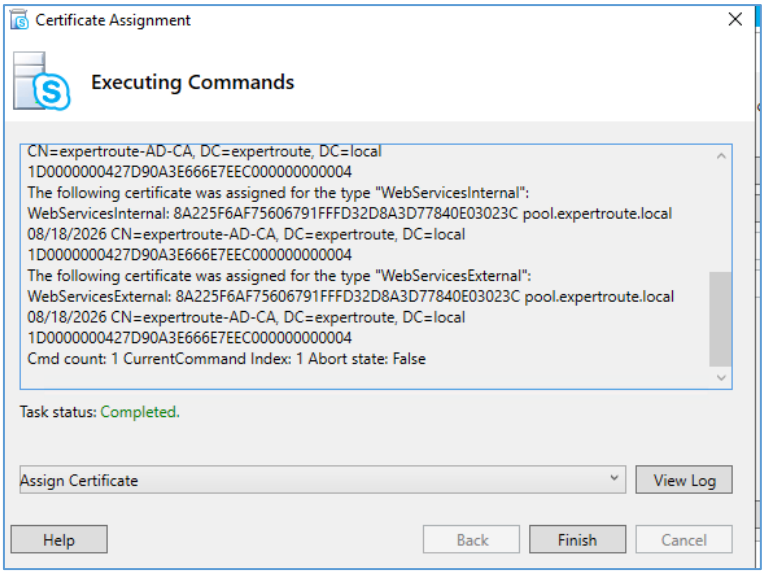
در شکل ۱۵-۱۰۳، بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۵- ۱۰۳ نصب و راه‌اندازی *Skype For Business*

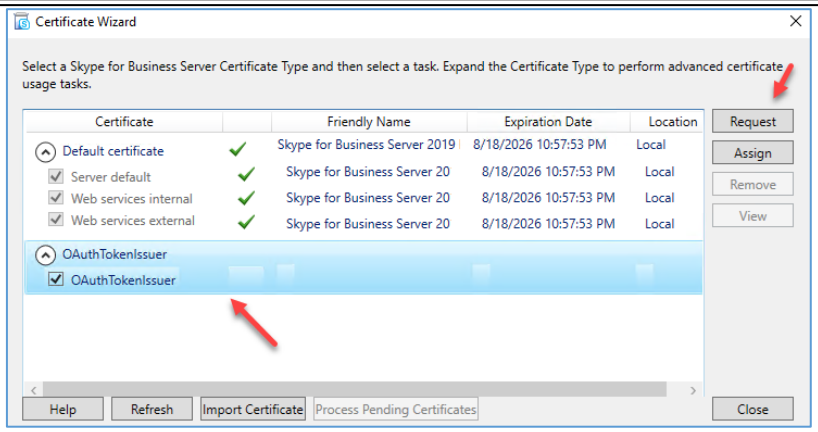
همان‌طور که در شکل ۱۵-۱۰۴، مشاهده می‌کنید این قسمت هم با موفقیت انجام شده است.



شکل ۱۵- ۱۰۴ نصب و راه‌اندازی *Skype For Business*

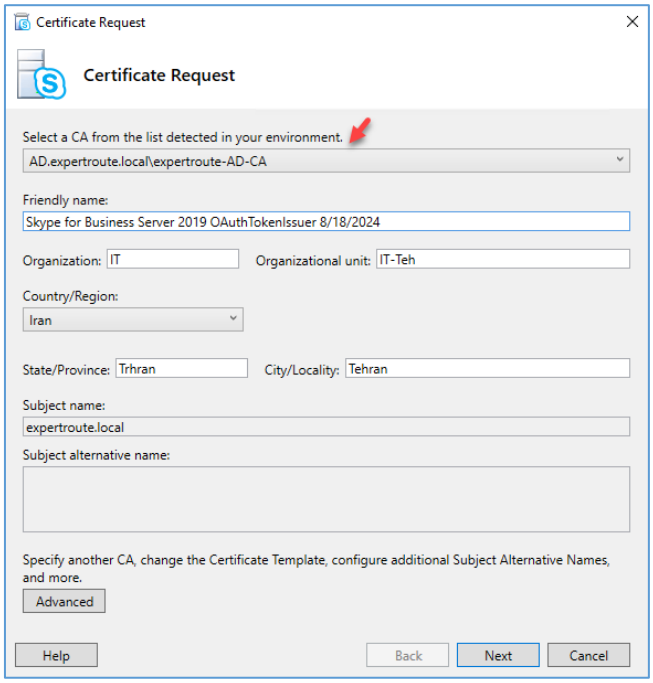
در ادامه کار گزینه‌ی دوم را به مانند شکل ۱۵-۱۰۵، انتخاب و بر روی Request کلیک کنید.

www.takbook.com



شکل ۱۵- ۱۰۵ نصب و راه‌اندازی *Skype For Business*

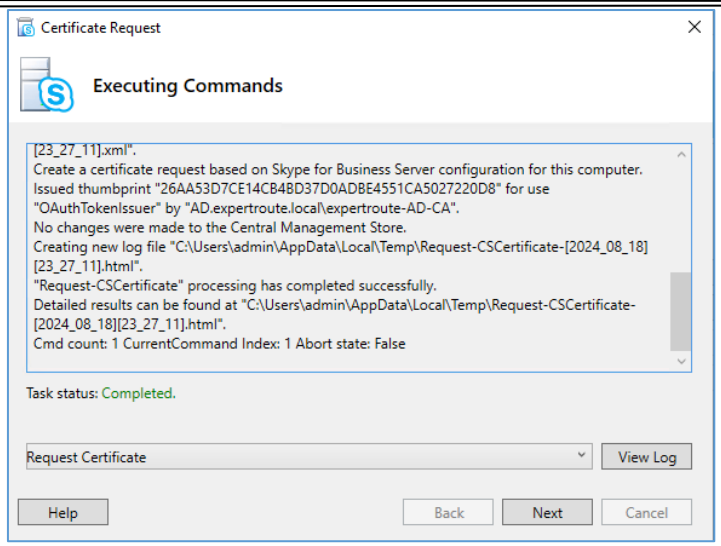
در شکل ۱۵-۱۰۶، فقط بر روی Next کلیک کنید.



شکل ۱۵- ۱۰۶ نصب و راه‌اندازی *Skype For Business*

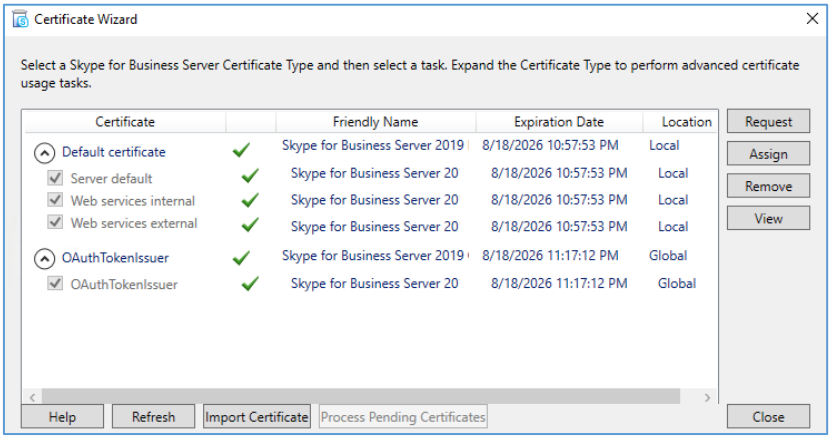
در ادامه بر روی Finish و Next کلیک کنید تا تنظیمات نهایی اعمال شود و شکل نهایی به صورت ۱۵-۱۰۷ باشد.

www.takbook.com



شکل ۱۵- ۱۰۷ نصب و راه‌اندازی *Skype For Business*

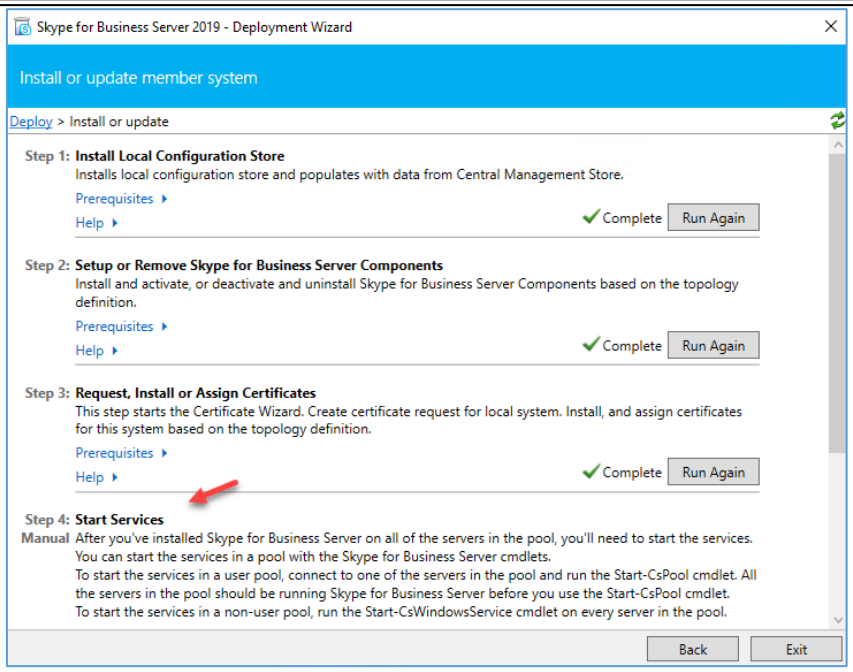
همان‌طور که در شکل ۱۵-۱۰۸، مشاهده می‌کنید گواهینامه به صورت کامل بر روی سرور اعمال شده است.



شکل ۱۵- ۱۰۸ نصب و راه‌اندازی *Skype For Business*

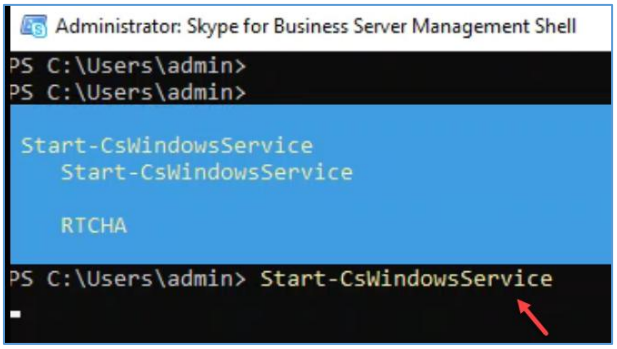
در ادامه کار باید سرویس‌های مربوط به Skype for Business را به مانند شکل ۱۵-۱۰۹، اجرا کنیم.

www.takbook.com



شکل ۱۵- ۱۰۹ نصب و راه‌اندازی Skype For Business

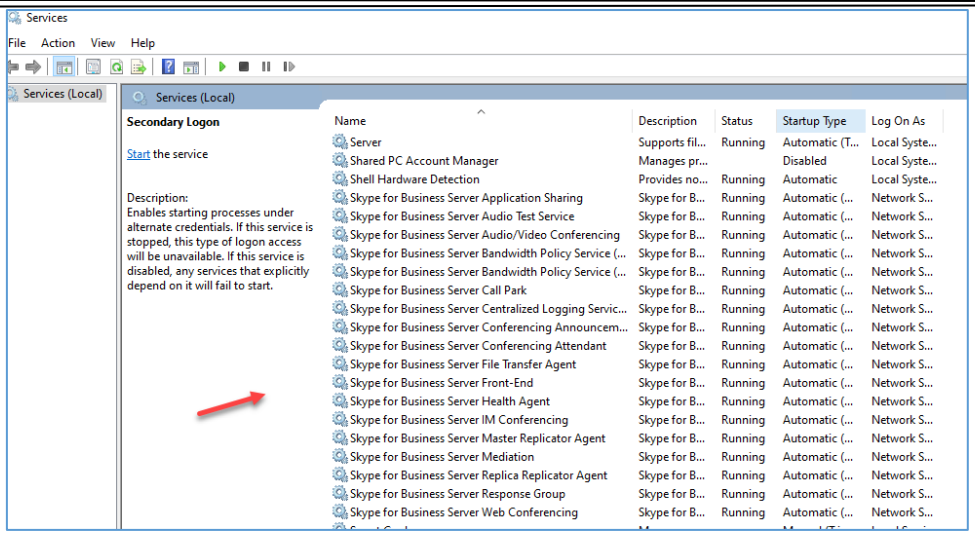
برای اجرای سرویس باید وارد PowerShell شویم و به مانند شکل ۱۵-۱۱۰، تمام سرویس‌های Skype For business را با دستور Start-CsWindowsService فعال کنیم.



شکل ۱۵- ۱۱۰ نصب و راه‌اندازی Skype For Business

به مانند شکل ۱۵-۱۱۱، اگر وارد Services شوید تمام سرویس‌های Skype For Business را مشاهده می‌کنید که فعال شده است.

www.takbook.com

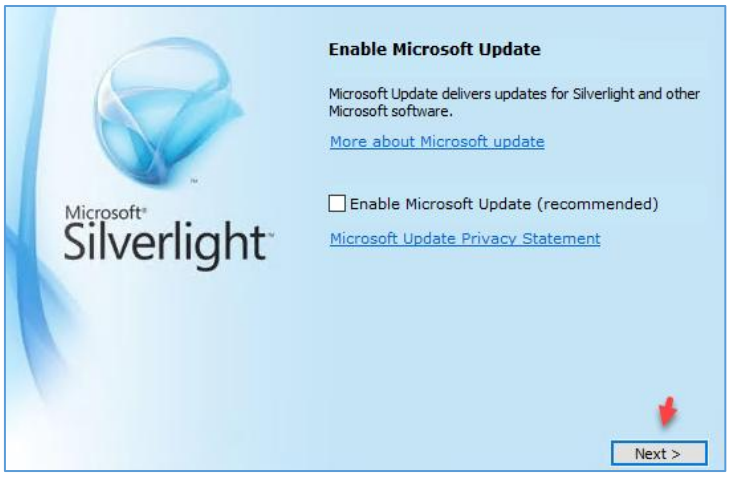


شکل ۱۵- ۱۱۱ نصب و راه‌اندازی Skype For Business

در ادامه کار باید سرویس Skype for business Control panel را اجرا کنیم، برای اجرای این سرویس باید نرم‌افزار Sliverlight را بر روی سرور نصب کنید، برای این‌کار باید از لینک زیر آن را دانلود کنید.

https://soft98.ir/software/1459-microsoft-silverlight-dl.html

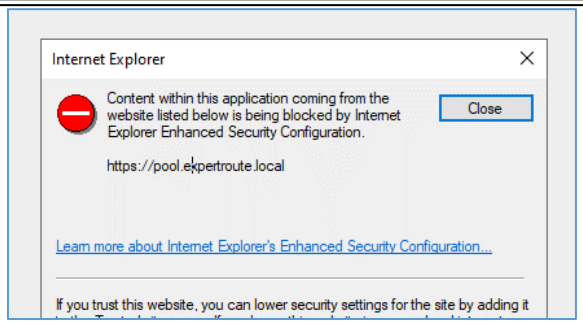
به مانند شکل ۱۵-۱۱۲، بعد از دانلود آن را نصب کنید.



شکل ۱۵- ۱۱۲ نصب و راه‌اندازی Skype For Business

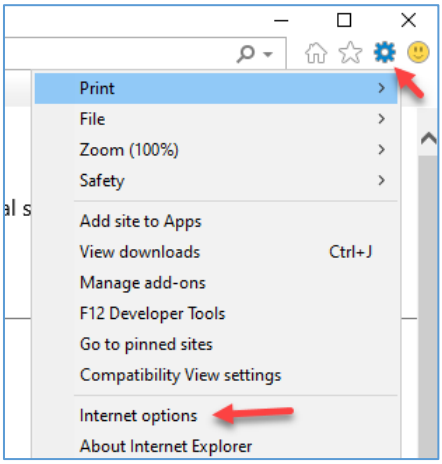
در ادامه باید سرویس Skype for Business Server Control Panel را اجرا کنیم، بعد از اجرا شاید با پیغام شکل ۱۵-۱۱۳، روبرو شوید که باید آدرس مورد نظر را Trust کنید، آدرس را کپی کنید و نرم‌افزار Internet Explorer را اجرا کنید.

www.takbook.com



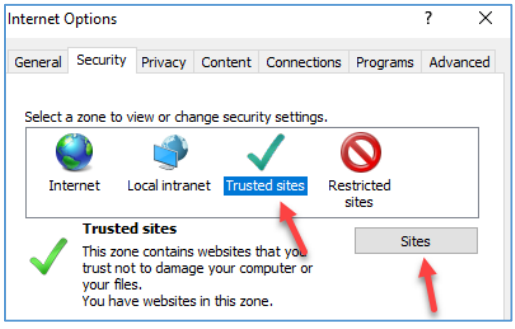
شکل ۱۵- ۱۱۳ نصب و راه‌اندازی *Skype For Business*

به مانند شکل ۱۵-۱۱٤، از قسمت Settings وارد Internet Options شوید.



شکل ۱۵- ۱۱۴ نصب و راه‌اندازی *Skype For Business*

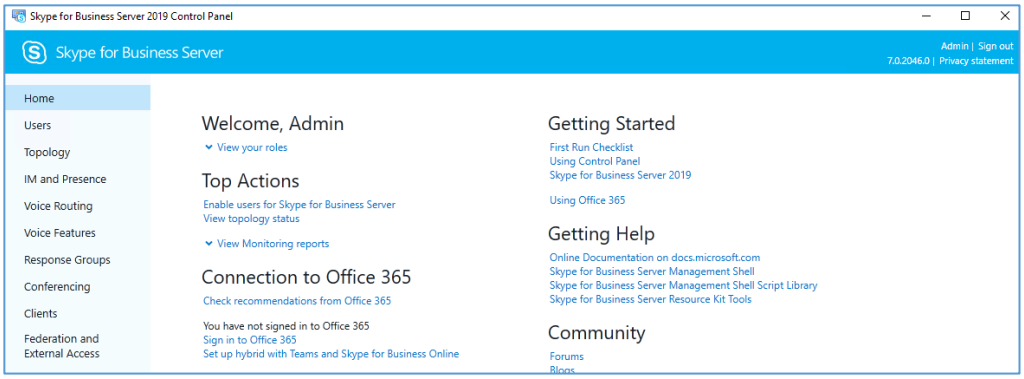
به مانند شکل ۱۵-۱۱۵، بر روی Trusted sites کلیک کنید و بر روی Sites کلیک کنید و آدرس مورد نظر را در آن اضافه کنید.



شکل ۱۵- ۱۱۵ نصب و راه‌اندازی *Skype For Business*

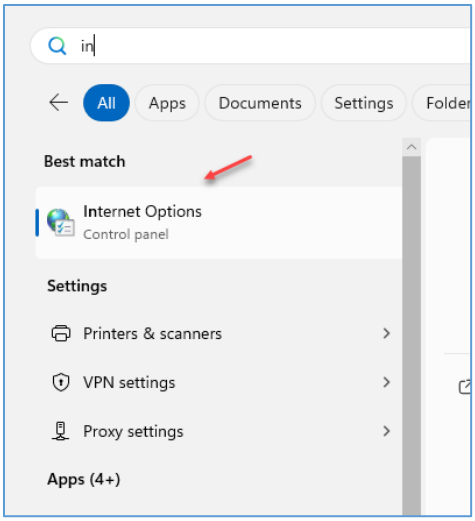
www.takbook.com

اگر دوباره صفحه‌ی Control Panel را اجرا کنید شکل ۱۵-۱۱۶، ظاهر خواهد شد و صفحه‌ی اول باز خواهد شد.



شکل ۱۵- ۱۱۶ نصب و راه‌اندازی Skype For Business

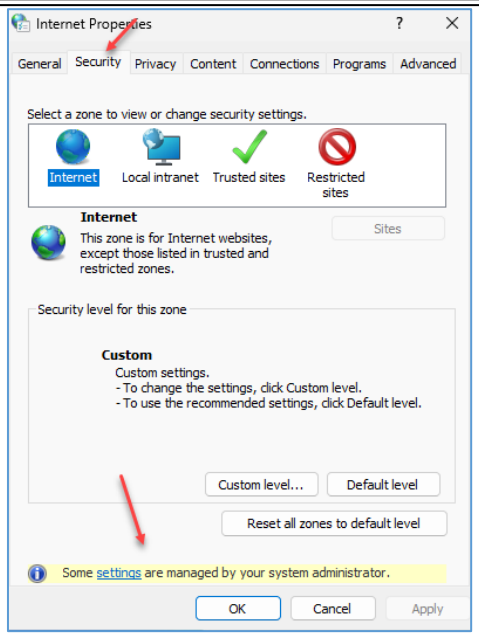
نکته در ویندوز سرور جدید ۲۰۲۵ خبری از Internet Explorer نیست ولی به جای آن Internet Options وجود دارد که باید به مانند شکل ۱۵-۱۱۷، اجرا کنید.



شکل ۱۵- ۱۱۷ نصب و راه‌اندازی Skype For Business

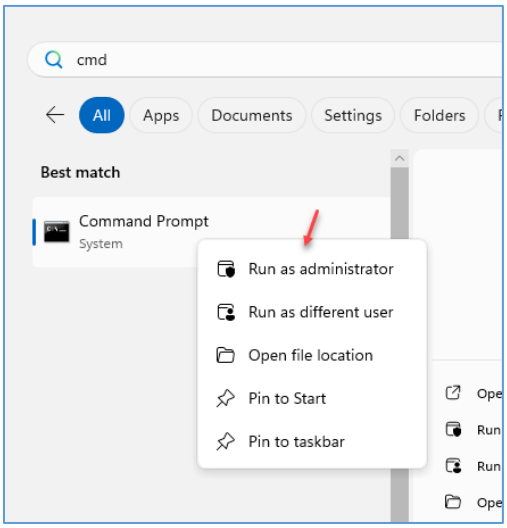
به مانند شکل ۱۵-۱۱۸، اگر وارد تب Security شوید با پیغام Some settings are managed by your system administrator روبرو می‌شوید و به شما اجازه نمی‌دهد تا آدرسی را اضافه کنید.

www.takbook.com



شکل ۱۵- ۱۱۸ نصب و راه‌اندازی *Skype For Business*

برای حل این مشکل باید دستورات زیر را در CMD اجرا کنید به مانند شکل ۱۵-۱۱۹، CMD را با دسترسی کاربر Administrator اجرا کنید.



شکل ۱۵- ۱۱۹ نصب و راه‌اندازی *Skype For Business*

دستورات زیر را در CMD وارد و اجرا کنید.

```
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies" /f
```

www.takbook.com


```
reg delete "HKCU\Software\Microsoft\WindowsSelfHost" /f

reg delete "HKCU\Software\Policies" /f

reg delete "HKLM\Software\Microsoft\Policies" /f

reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies" /f

reg delete
"HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsStore\WindowsUpdate"
/f

reg delete "HKLM\Software\Microsoft\WindowsSelfHost" /f

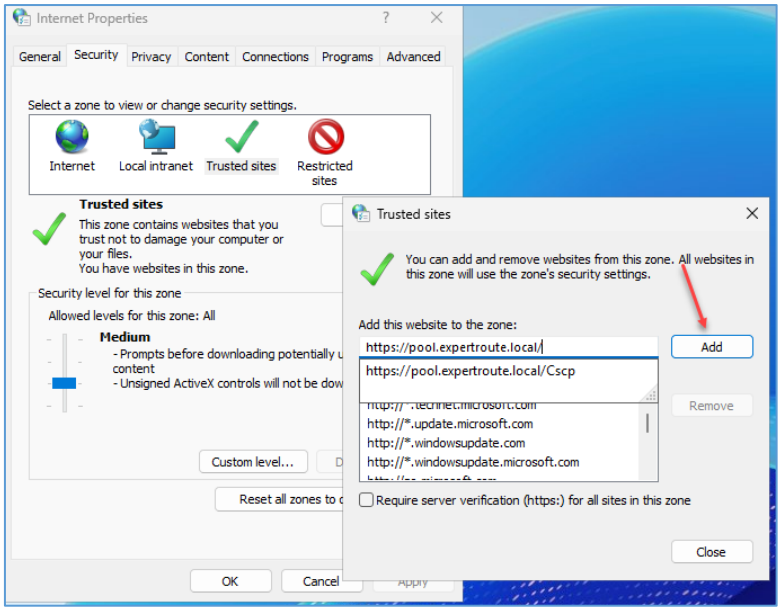
reg delete "HKLM\Software\Policies" /f

reg delete "HKLM\Software\WOW6432Node\Microsoft\Policies" /f

reg delete
"HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Policies" /f

reg delete
"HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\WindowsStore\Win
dowsUpdate" /f
```

بعد از اجرای دستورات سرور را Restart کنید و اگر دوباره وارد Internet Options شوید به مانند شکل ۱۲۰-۱۵، مشاهده می‌کنید که دیگر خبری از پیغام مورد نظر نیست.



شکل ۱۵- ۱۲۰ نصب و راه‌اندازی *Skype For Business*

www.takbook.com

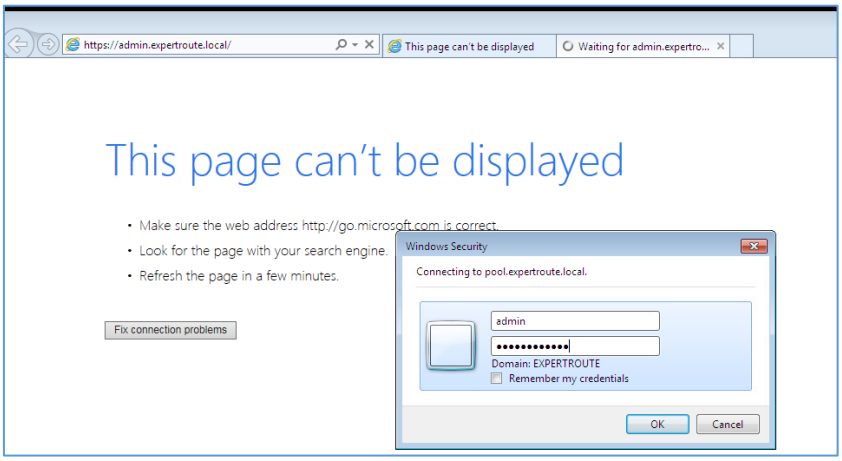
۱۵-۵ اجرای قسمت مدیریّتی Skype از طریق Web

همان‌طور که می‌دانید در هنگام کانفیگ سرور Skype، آدرسی برای قسمت مدیریّتی Skype به آدرس https://admin.expertroute.local وارد کردیم که این آدرس به مانند سرویس Control Panel عمل می‌کند.

نکته: برای اینکه این سرویس را در وب اجرا کنید، نیاز به نرم‌افزار Silver Light دارید که در قسمت‌های قبل، روی سرور Skype نصب کردیم، پس وارد سرور Skype می‌شویم و Internet Explorer را اجرا می‌کنیم. آدرس زیر را در Address bar وارد و اجرا کنید:

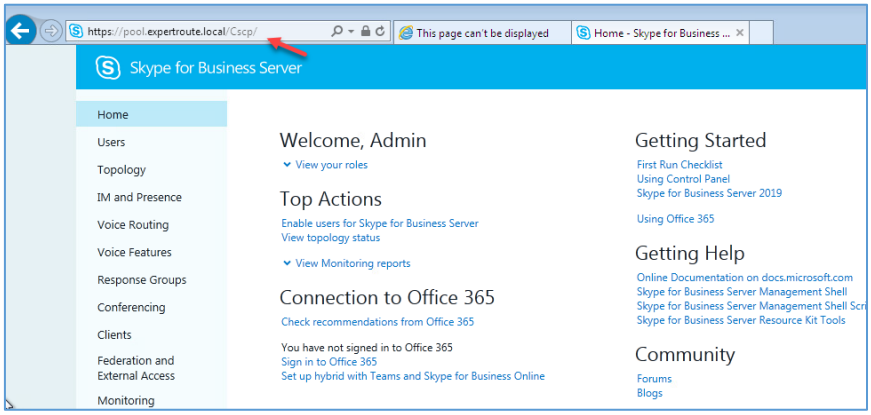
https://admin.Expertroute.local

در آدرس بالا به جای expertroute.local نام دومین خود را وارد کنید، بعد از اجرا به مانند شکل ۱۵-۱۲۱، از شما نام کاربری درخواست می‌شود که باید وارد و ok کنید.



شکل ۱۵- ۱۲۱ نصب و راه‌اندازی Skype For Business

همان‌طور که در شکل ۱۵-۱۲۲، مشاهده می‌کنید، آدرس مورد نظر به درستی اجرا شده است.



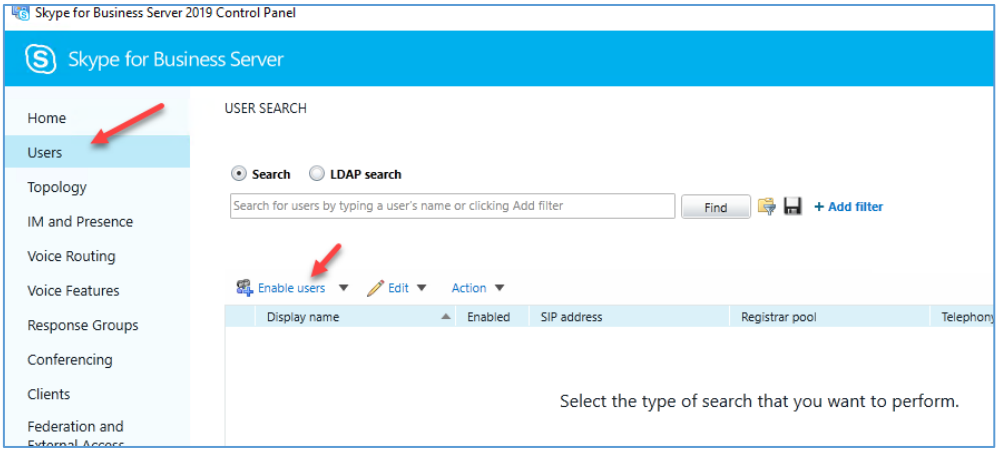
شکل ۱۵- ۱۲۲ نصب و راه‌اندازی Skype For Business

www.takbook.com

۱۵-۶ متصل شدن کاربر به سرور

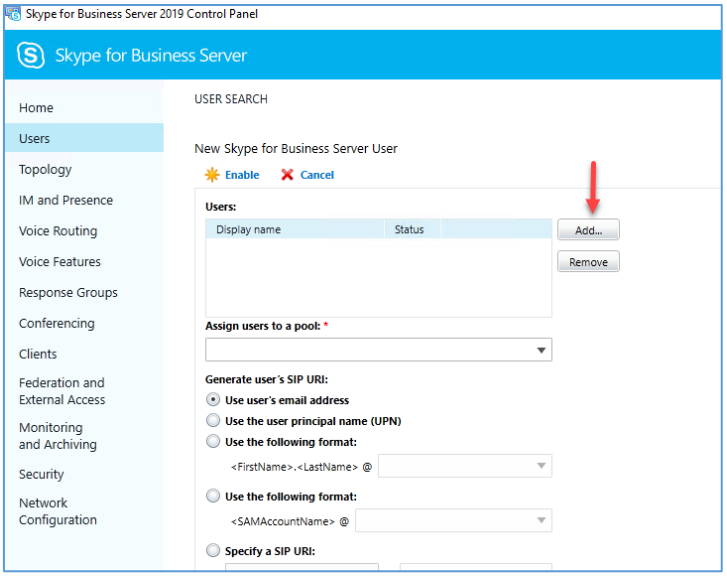
بعد از اتمام کار و نصب کامل Skype For Business 2019 باید تست عملکرد را انجام دهیم، برای این کار اول از همه یک کاربر را باید به سرویس اضافه کنیم.

برای شروع به مانند شکل ۱۵-۱۲۳، وارد Control Panel شوید و از قسمت Users بر روی Enable users کلیک کنید.



شکل ۱۵- ۱۲۳ نصب و راه‌اندازی *Skype For Business*

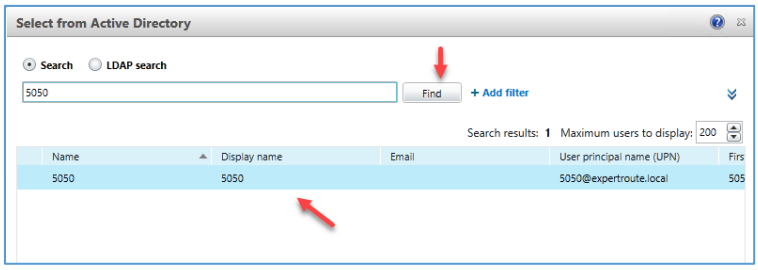
به مانند شکل ۱۵-۱۲٤، بر روی Add کلیک کنید.



شکل ۱۵- ۱۲۴ نصب و راه‌اندازی *Skype For Business*

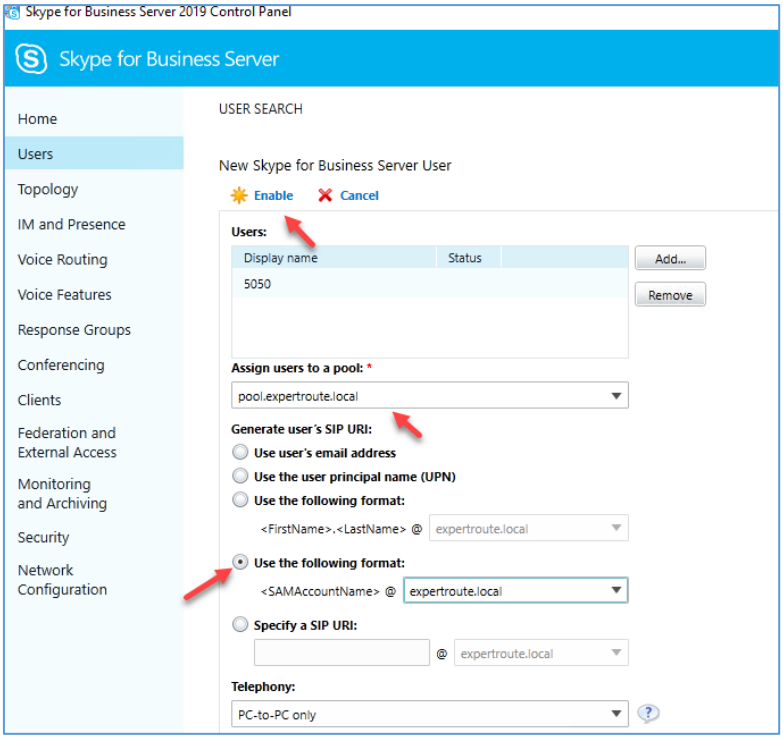
www.takbook.com

در شکل ۱۵-۱۲۵، در کادر مشخص شده کاربر 5050 را وارد کنید و آن را به لیست اضافه کنید.



شکل ۱۵ - ۱۲۵ نصب و راه‌اندازی *Skype For Business*

در شکل ۱۵-۱۲۶، کاربر به لیست اضافه شده است، و از قسمت Assign باید Pool مورد نظر خود را انتخاب کنید و در قسمت SIP URL باید قالب ورود کاربران را مشخص کنید که گزینه‌ی دوم را انتخاب می‌کنیم، یعنی کاربران برای ورود باید آدرس را به صورت user@expertroute.local وارد کنند.



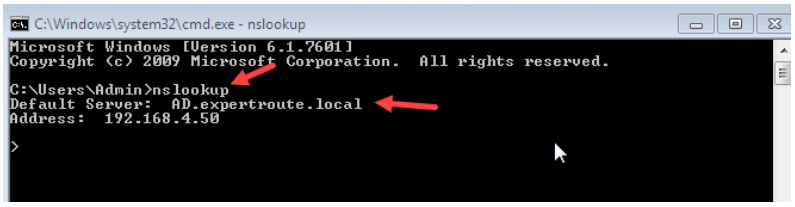
شکل ۱۵ - ۱۲۶ نصب و راه‌اندازی *Skype For Business*

حالا همه چیز آماده است که کاربران وارد سیستم شوند و بتوانند با هم ارتباط برقرار کنند، توجه داشته باشید که کاربران باید عضو دومین باشند تا بتوانند گواهینامه‌های صادر شده را به صورت اتوماتیک دریافت کنند اگر عضو نباشند، باید گواهینامه را به صورت دستی نصب کنیم.

www.takbook.com

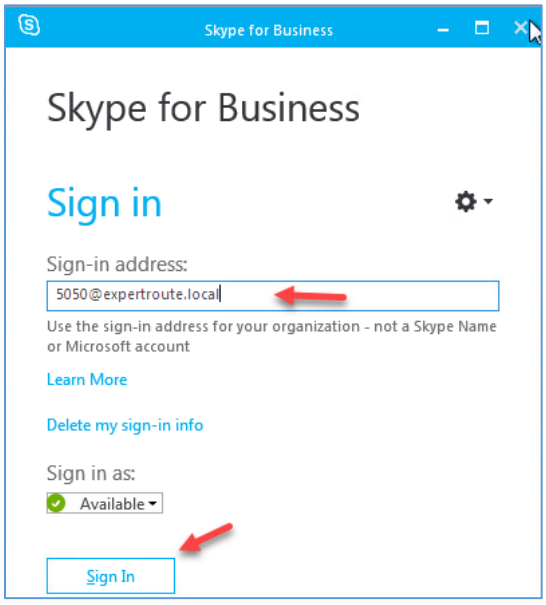
برای اینکه Skype For Business Client را بر روی کلاینت‌ها نصب کنید می‌توانید از مجموعه آفیس استفاده کنید که این برنامه داخل آن قرار دارد.

وارد کلاینت می‌شویم و اولین کاری که انجام می‌دهیم این است که بررسی کنیم که آیا کلاینت مورد نظر سرور دومین را می‌بیند یا نه که باید از دستور Nslookup در CMD استفاده کنیم، همان‌طور که در شکل ۱۵-۱۲۷، مشاهده می‌کنید سرور مورد نظر در دسترس است.



شکل ۱۵- ۱۲۷ نصب و راه‌اندازی *Skype For Business*

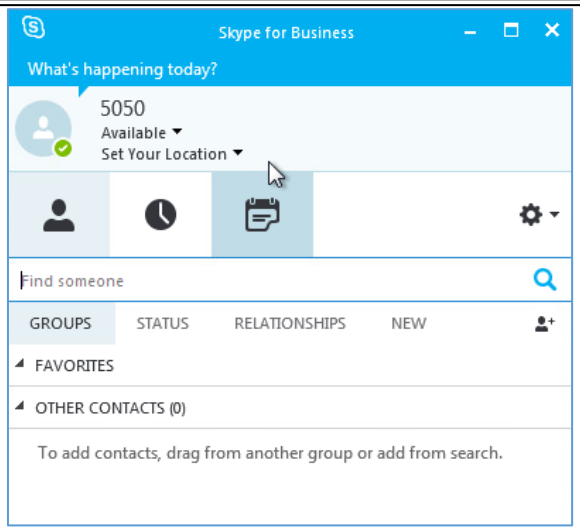
به مانند شکل ۱۵-۱۲۸، حالا نرم‌افزار Skype for business را اجرا می‌کنیم و آدرس کاربری که در سرور اضافه کردیم را وارد می‌کنیم و بر روی Sign in کلیک می‌کنیم تا وارد شویم.



شکل ۱۵- ۱۲۸ نصب و راه‌اندازی *Skype For Business*

همان‌طور که در شکل ۱۵-۱۲۹، مشاهده می‌کنید توانستیم با موفقیت وارد سامانه شویم.

www.takbook.com



شکل ۱۵- ۱۲۹ نصب و راه‌اندازی *Skype For Business*

۱۵-۷ راه‌اندازی سرور EDGE

رسیدیم به مهمترین بخش نرم‌افزار Skype For business، محبوبیت این نرم‌افزار این است که می‌توانید آن را بر روی موبایل خود نصب کنید و به آن متصل شوید که با این کار می‌توانید برای کاربران خود امکانات صوتی و تصویری جالبی را خلق کنید.

در دیاگرام شکل ۱۵-۱۳۰، سرورهایی که تا به این لحظه ایجاد کردیم را مشاهده می‌کنید که در قسمت LAN یعنی شبکه‌ی داخلی قرار دارد.

در ادامه کار و برای اینکه کاربران خارج از شبکه بتوانند با Skype For Business در ارتباط باشند باید یک سرور جدید ایجاد کنیم و آن را در منطقه DMZ قرار دهیم، منظور از DMZ این است که سرور مورد نظربیرون از شبکه‌ی دومین قرار دارد و به صورت Workgroup کار می‌کند.

برای ارتباط از طریق اینترنت نیاز به موارد زیر داریم.

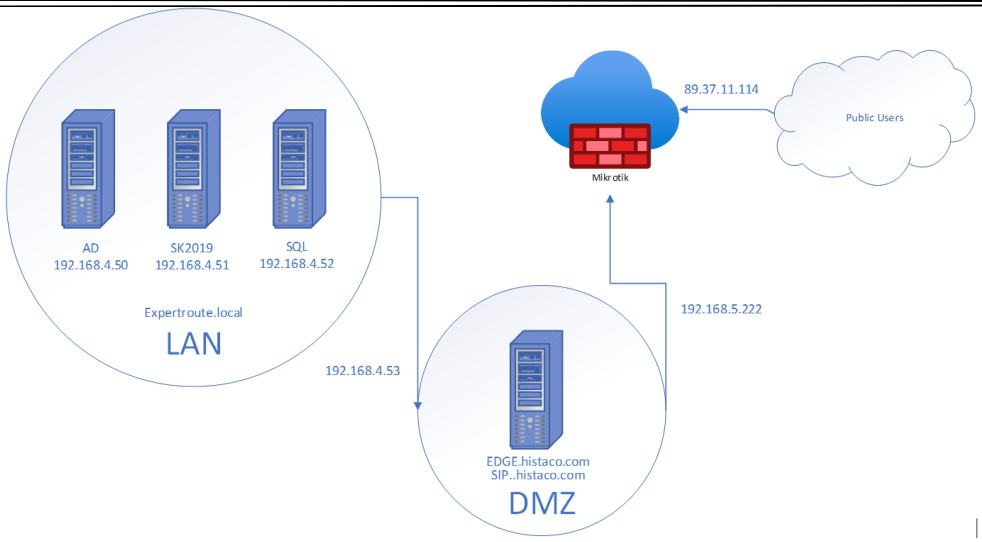
۱- حدقل یک و حداکثر سه آدرس Static که در اینترنت اعتبار داشته باشد.

۲- نیاز به روتر/فایروال دارم که بتوانیم Route یا NAT انجام دهیم.

۳- نیاز به سرور EDGE داریم که بر روی آن دو کارت شبکه نصب شده باشد.

٤- نیاز به یک دومین خارجی داریم که بتوانیم آن را به سمت سرور داخلی ارتباط دهیم.

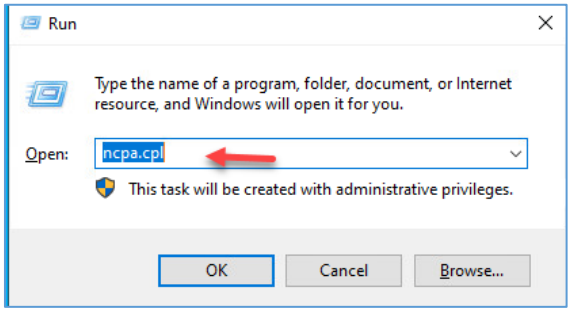
www.takbook.com



شکل ۱۵- ۱۳۰ راه‌اندازی سرور EDGE

برای شروع کار یک سرور با نام EDGE ایجاد و IP آن را به صورت دستی وارد می‌کنیم، طبق سناریو شکل ۱۵-۱۳۰، این سرور دو کارت شبکه دارد که به دو شبکه مختلف متصل می‌شود، یکی شبکه‌ی داخلی که به سمت سرور Skype است و دیگری شبکه‌ی خارجی که به سمت روتر میکروتیک می‌رود.

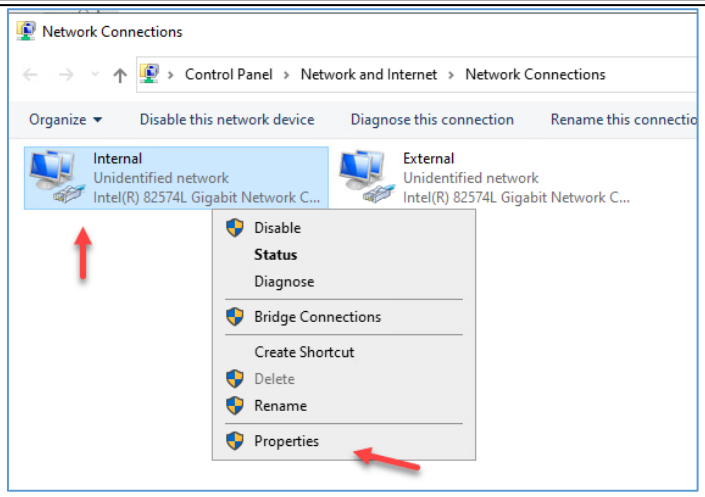
به مانند شکل ۱۵-۱۳۱، با دستور ncpa.cpl وارد کارت شبکه‌ی سرور EDGE شوید.



شکل ۱۵- ۱۳۱ راه‌اندازی سرور EDGE

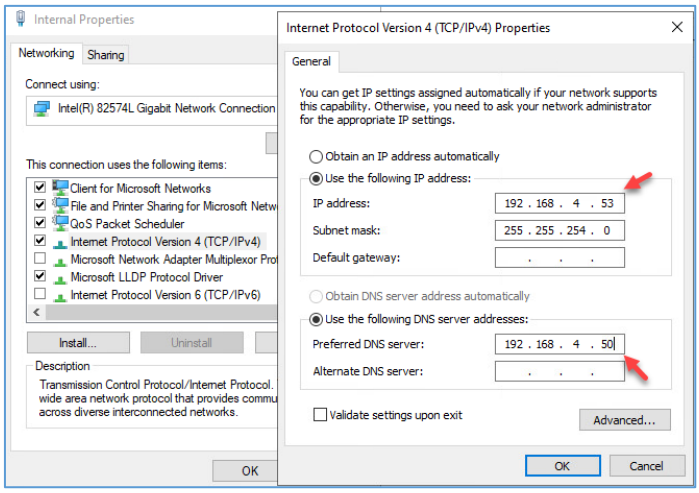
به مانند شکل ۱۵-۱۳۲، باید نام هر کارت شبکه را طبق سناریویی که مشخص کردیم وارد کنید و تنظیمات IP آن را هم انجام دهید، بر روی کارت شبکه‌ی Internal کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.

www.takbook.com



شکل ۱۵- ۱۳۲ راه‌اندازی سرور EDGE

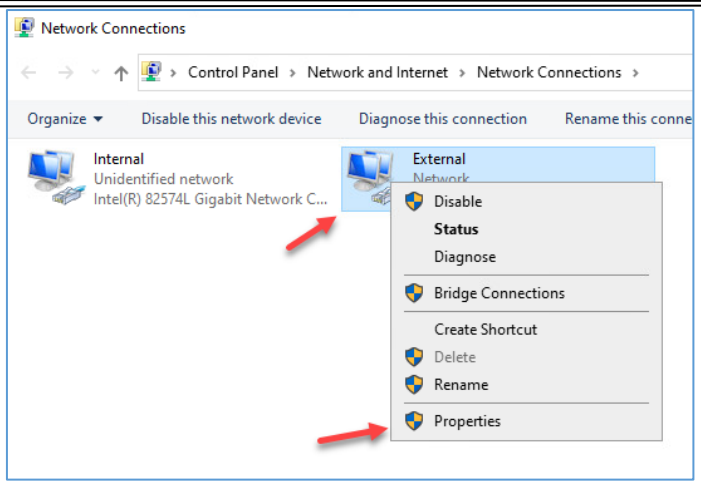
در شکل ۱۵-۱۳۳، باید آدرس شبکه‌ی داخلی را وارد کنید و قسمت gateway را برای این کارت شبکه خالی بگذارید و فقط در قسمت DNS آدرس سرور DNS داخلی را وارد کنید.



شکل ۱۵- ۱۳۳ راه‌اندازی سرور EDGE

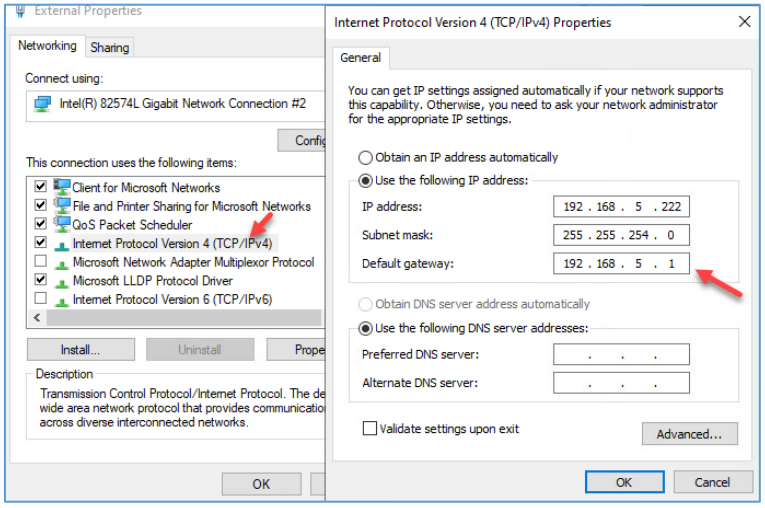
به مانند شکل ۱۵-۱۳٤، بر روی کارت شبکه‌ی External کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.

www.takbook.com



شکل ۱۵- ۱۳۴ راه‌اندازی سرور EDGE

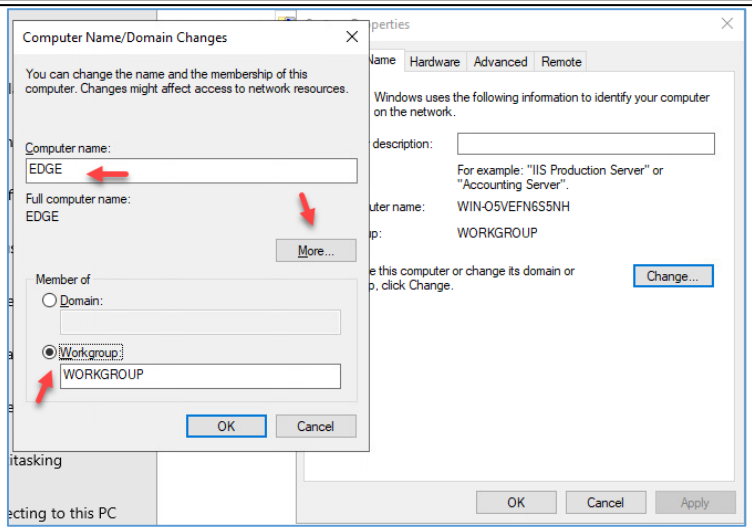
به مانند شکل ۱۵-۱۳۵، در کارت شبکه‌ی External باید آدرس 192.168.5.222 را وارد کنیم و تنها تفاوتش با کارت شبکه‌ی داخلی داشتن Gateway است تا اطلاعات به سمت بیرون ارسال شود.



شکل ۱۵- ۱۳۵ راه‌اندازی سرور EDGE

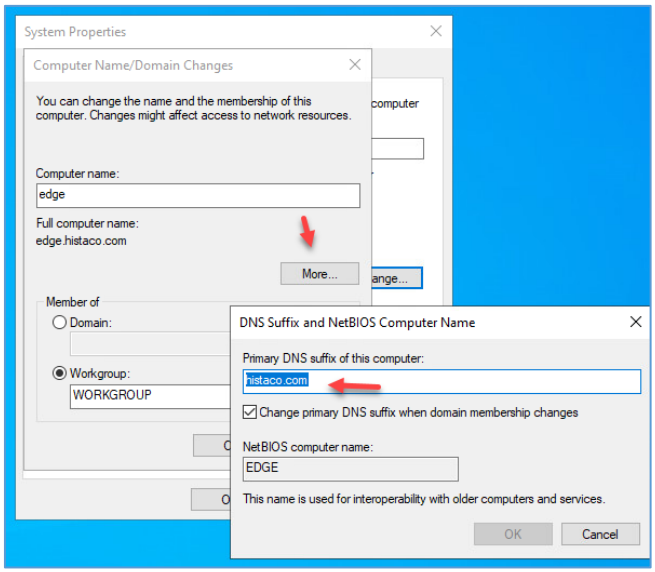
در ادامه کار باید نام سرور را تغییر دهید، برای این کار به مانند شکل ۱۵-۱۳۶، وارد پنجره‌ی زیر شوید و نام را تغییر دهید، توجه داشته باشید این سرور نباید عضو دومین باشد و باید در همان حالت Workgroup باقی بماند.

www.takbook.com



شکل ۱۵- ۱۳۶ راه‌اندازی سرور EDGE

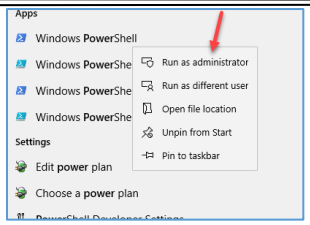
به مانند شکل ۱۵-۱۳۷، بعد از وارد کردن نام سرور بر روی More کلیک کنید و نام دومین خارجی خود را وارد کنید و بر روی OK کلیک کنید و در آخر سرور را Restart کنید.



شکل ۱۵- ۱۳۷ راه‌اندازی سرور EDGE

در ادامه کار باید یک سری ابزارها را در سرور EDGE نصب کنیم، برای این کاربه مانند شکل ۱۵-۱۳۸، PowerShell را اجرا کنید.

www.takbook.com

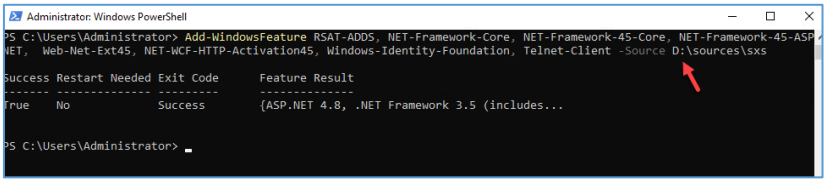


شکل ۱۵- ۱۳۸ راه‌اندازی سرور EDGE

بعد از اجرا باید کد زیر را وارد و اجرا کنید، توجه داشته باشید باید DVD ویندوز سرور هم داخل دستگاه باشد که درایو D مربوط به این DVD است.

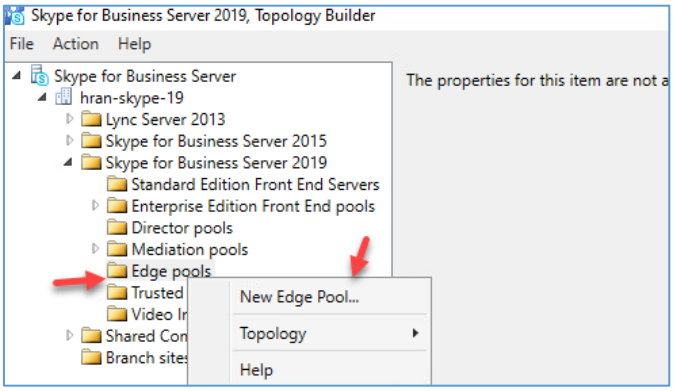
```
Add-WindowsFeature RSAT-ADDS, NET-Framework-Core, NET-Framework-45-Core, NET-Framework-45-ASPNET,  Web-Net-Ext45, NET-WCF-HTTP-Activation45, Windows-Identity-Foundation, Telnet-Client –Source D:\sources\sxs
```

همان‌طور که در شکل ۱۵-۱۳۹، مشاهده می‌کنید دستورات مورد نظر با موفقیت اجرا و سرویس‌های آن نصب شده است.



شکل ۱۵- ۱۳۹ راه‌اندازی سرور EDGE

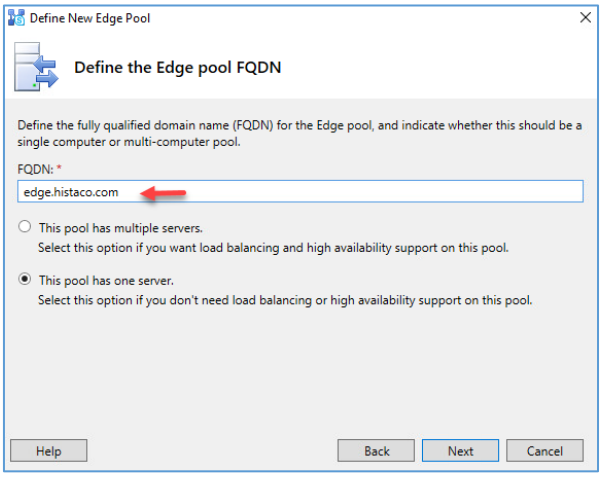
در ادامه کار باید وارد سرور اصلی Skype که با نام SK2019 ایجاد کردیم شویم و تنظیمات مربوط به سرور EDGE را انجام دهیم، برای این کار باید سرویس Topology Builder را اجرا کنید و وارد تنظیمات شوید و به مانند شکل ۱۵-۱۴۰، بر روی Edge Pools کلیک راست کنید و گزینه‌ی New Edge Pool را انتخاب کنید.



شکل ۱۵- ۱۴۰ راه‌اندازی سرور EDGE

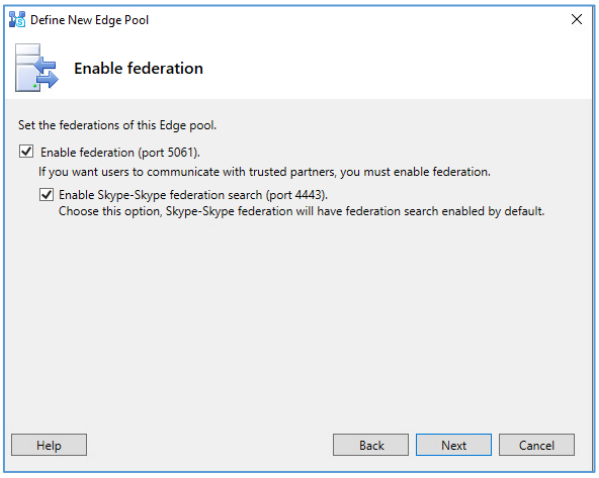
www.takbook.com

در شکل ۱۵-۱۴۱، باید نام سرور Edge را به همراه نام دومین که در قسمت قبل مشخص کردیم را وارد کنید.



شکل ۱۵- ۱۴۱ راه‌اندازی سرور EDGE

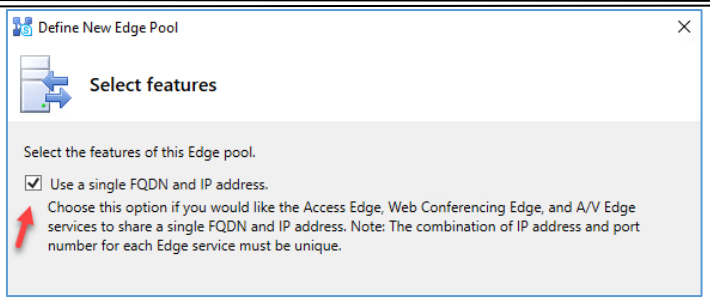
در شکل ۱۵-۱۴۲، تیک مورد نظر را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۵- ۱۴۲ راه‌اندازی سرور EDGE

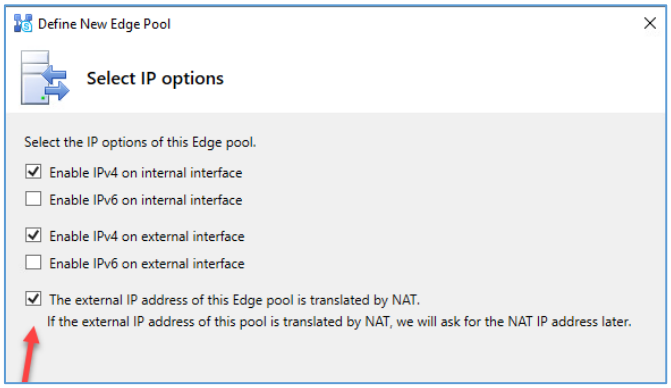
در شکل ۱۵-۱۴۳، باید مشخص کنید که چه تعداد آدرس Public داریم، اگر یک آدرس دارید باید تیک گزینه‌ی مورد نظر انتخاب کنید و اگر هم سه آدرس IP دارید نباید انتخاب کنید، در این قسمت یک آدرس IP داریم پس باید تیک گزینه‌ی مورد نظر را انتخاب کنیم.

www.takbook.com



شکل ۱۵- ۱۴۳ راه‌اندازی سرور EDGE

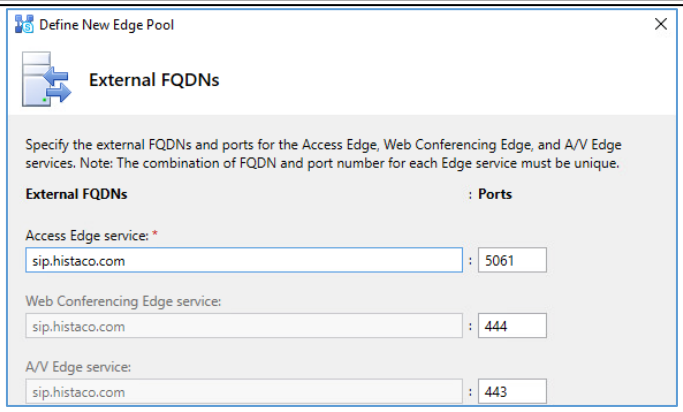
به مانند شکل ۱۵-۱٤٤، باید مشخص کنیم که برای ارتباط داخلی و خارجی از کدام ورژن IP استفاده می‌کنیم و اگر هم یک روتر دارید که می‌خواهد آدرس‌ها را NAT کنید باید تیک گزینه‌ی The External ip address of… را انتخاب کنید.



شکل ۱۵- ۱۴۴ راه‌اندازی سرور EDGE

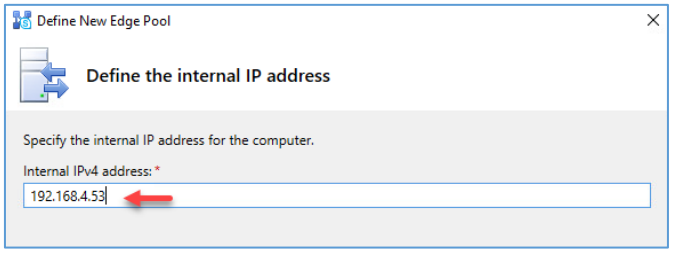
در شکل ۱۵-۱٤٥، باید آدرس Sip را به همراه نام دومین خود وارد کنید، توجه داشته باشید اگر سه آدرس IP داشته باشیم نیاز نبود یک آدرس وارد کنیم و برای هر سرویس می‌توانیم یک آدرس مشخص وارد کنید.

www.takbook.com



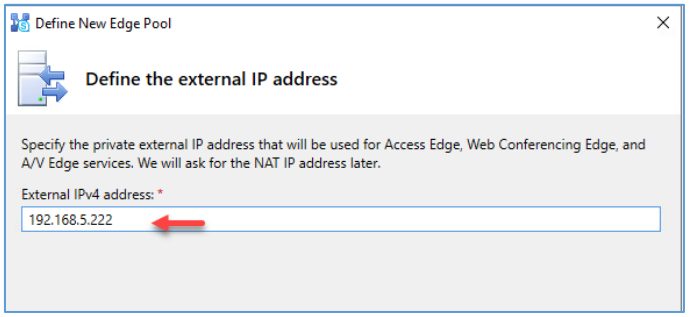
شکل ۱۵- ۱۴۵ راه‌اندازی سرور EDGE

در شکل ۱۵-۱٤٦، باید طبق سناریویی که در بالا بررسی کردیم باید آدرس داخلی سرور EDGE را وارد کنید.



شکل ۱۵- ۱۴۶ راه‌اندازی سرور EDGE

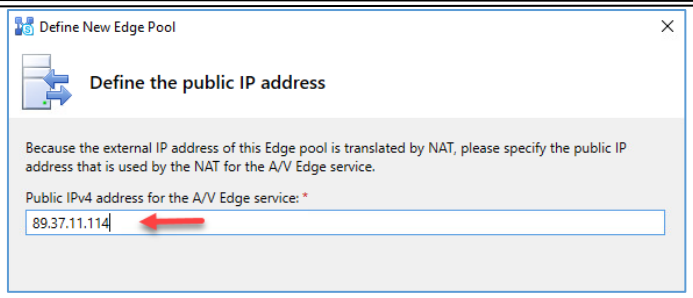
در شکل ۱۵-۱٤۷، باید آدرس خارجی سرور EDGE را وارد کنید.



شکل ۱۵- ۱۴۷ راه‌اندازی سرور EDGE

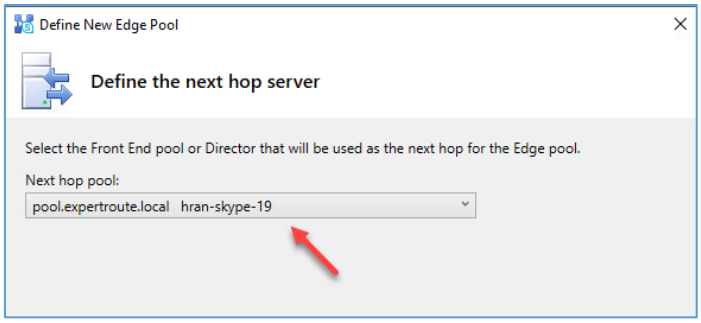
در شکل ۱۵-۱٤۸، باید آدرس IP خارجی که در اینترنت اعتبار دارد را وارد کنید.

www.takbook.com



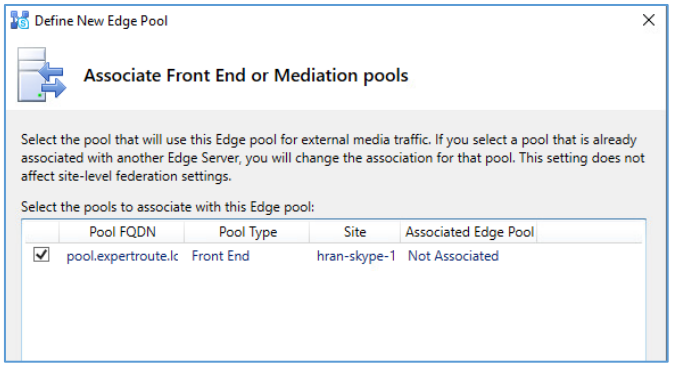
شکل ۱۵- ۱۴۸ راه‌اندازی سرور EDGE

در شکل ۱۵-۱۴۹، باید Pool را انتخاب کنید.



شکل ۱۵- ۱۴۹ راه‌اندازی سرور EDGE

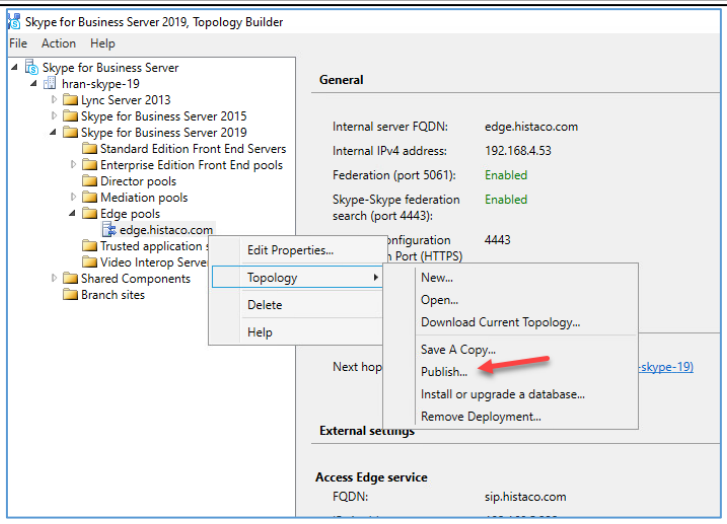
در شکل ۱۵-۱۵۰، بر روی Finish کلیک کنید.



شکل ۱۵- ۱۵۰ راه‌اندازی سرور EDGE

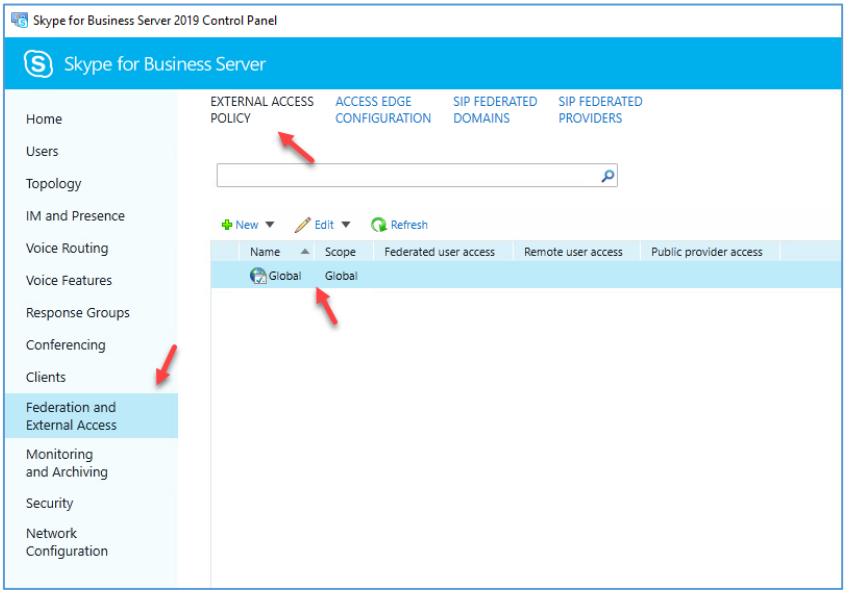
بعد از تنظیم Edge سرور باید این تنظیمات را Publish کنید تا بر روی Skype اعمال شود، برای این کار به مانند شکل ۱۵-۱۵۱، عمل کنید.

www.takbook.com



شکل ۱۵- ۱۵۱ راه‌اندازی سرور EDGE

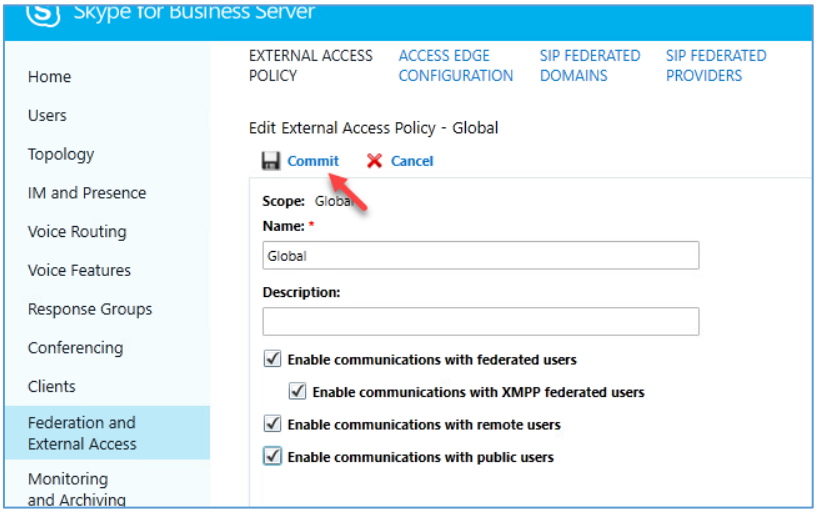
بعد از انجام مراحل قبل به مانند شکل ۱۵-۱۵۲، باید وارد سرویس Control Panel مربوط به Skype شوید و بر روی Federation and External Access کلیک کنید و از قسمت External Access Policy بر روی گزینه‌ی Global دو بار کلیک کنید.



شکل ۱۵- ۱۵۲ راه‌اندازی سرور EDGE

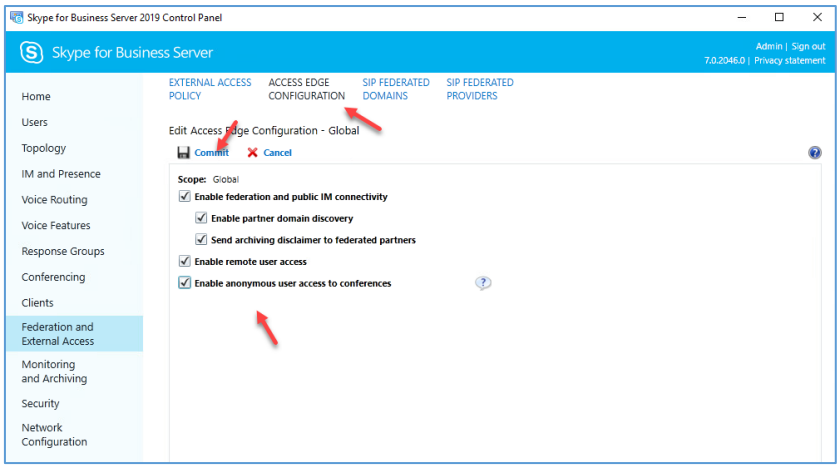
www.takbook.com

در شکل ۱۵-۱۵۳، تیک گزینه‌های مشخص شده را انتخاب و بر روی Commit کلیک کنید، این قسمت برای دسترسی کاربران بیرون از شبکه به سرور Skype است.



شکل ۱۵-۱۵۳ راه‌اندازی سرور EDGE

به مانند شکل ۱۵-۱۵٤، وارد Access EDGE Configuration شوید و تیک گزینه‌های مشخص شده را انتخاب کنید و بر روی Commit کلیک کنید.



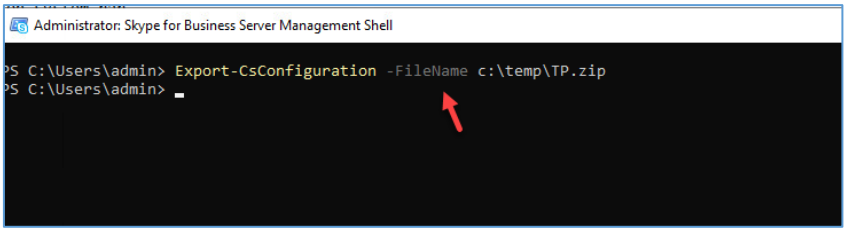
شکل ۱۵-۱۵۴ راه‌اندازی سرور EDGE

در ادامه کار و بعد از اتمام تنظیمات در سرور Skype باید از این تنظیمات یک خروجی تهیه و در سرور EDGE استفاده کنیم، برای این کار سرویس Management Shell را اجرا کنید و دستور زیر را اجرا کنید.

```
Export-CsConfiguration -FileName c:\temp\TP.zip
```

www.takbook.com

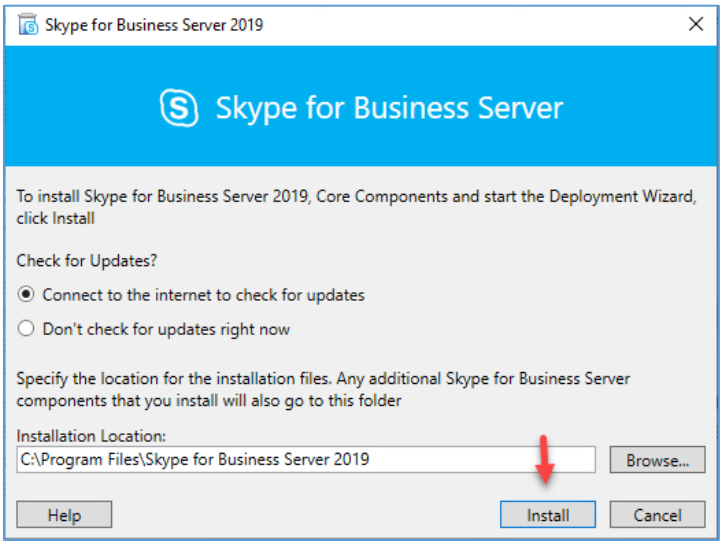
همان‌طور که در شکل ۱۵-۱۵۵، مشاهده می‌کنید دستور مورد نظر اجرا شده است و فایل مورد نظر در مسیر مشخص شده ایجاد شده است، توجه داشته باشید باید پوشه‌ی temp را در مسیر مشخص شده ایجاد کنید.



شکل ۱۵- ۱۵۵ راه‌اندازی سرور EDGE

پس تا به اینجای کار سرور EDGE را آماده کردیم و تنظیمات نام و شبکه‌ی آن را انجام دادیم، بعد از آن وارد سرور SK2019 یا همون FrontEnd شدیم و تنظیمالت مربوط به سرور EDGE را انجام دادیم و از آن خروجی فایل zip گرفتیم و دوباره برگشتیم به سرور EDGE.

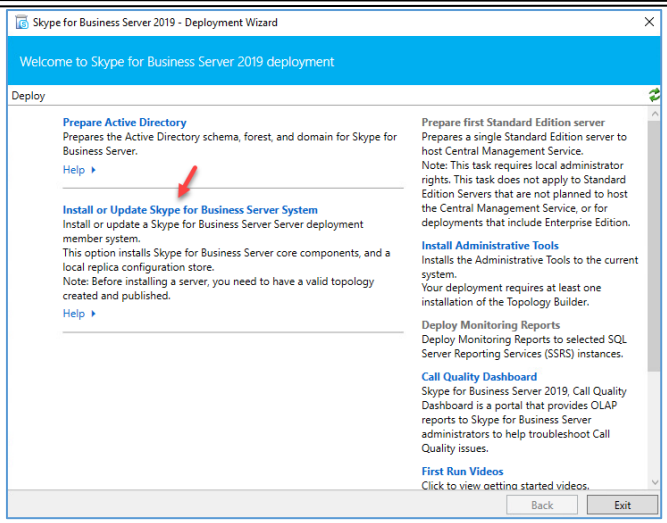
در سرور EDGE باید نرم‌افزار Skype را نصب کنید، برای همین موضوع فایل نصبی را اجرا کنید و در شکل ۱۵-۱۵۶، بر روی install کلیک کنید.



شکل ۱۵- ۱۵۶ راه‌اندازی سرور EDGE

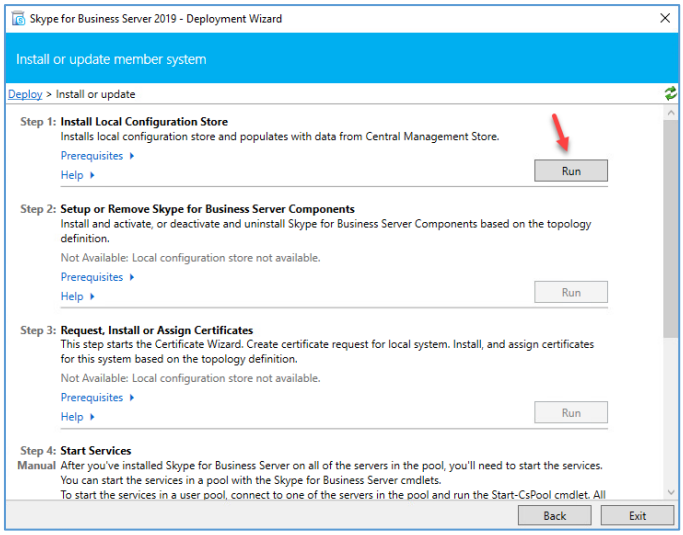
در شکل ۱۵-۱۵۷، باید بر روی Install or Update Skype for… کلیک کنید.

www.takbook.com



شکل ۱۵- ۱۵۷ راه‌اندازی سرور EDGE

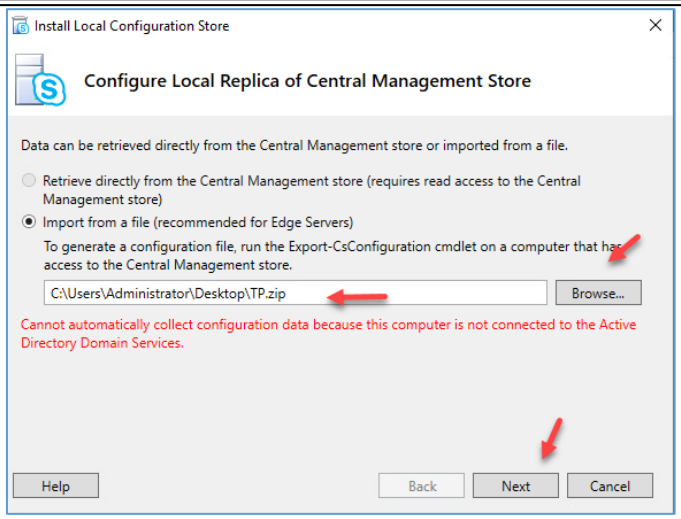
در شکل ۱۵–۱۵۸، بر روی گزینه‌ی مورد نظر کلیک کنید.



شکل ۱۵- ۱۵۸ راه‌اندازی سرور EDGE

در شکل ۱۵–۱۵۹، باید با کلیک بر روی Browse فایل Zip که در سرور Sk2019 ایجاد کردید را معرفی کنید و بر روی Next کلیک کنید.

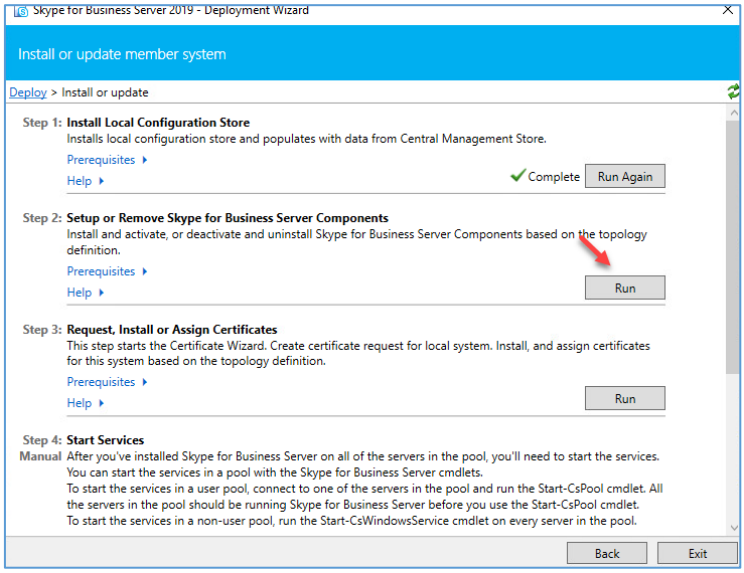
www.takbook.com



شکل ۱۵- ۱۵۹ راه‌اندازی سرور EDGE

همان‌طور که در شکل ۱۵-۱۶۰، مشاهده می‌کنید، تنظیمات با موفقیت اعمال شده است.

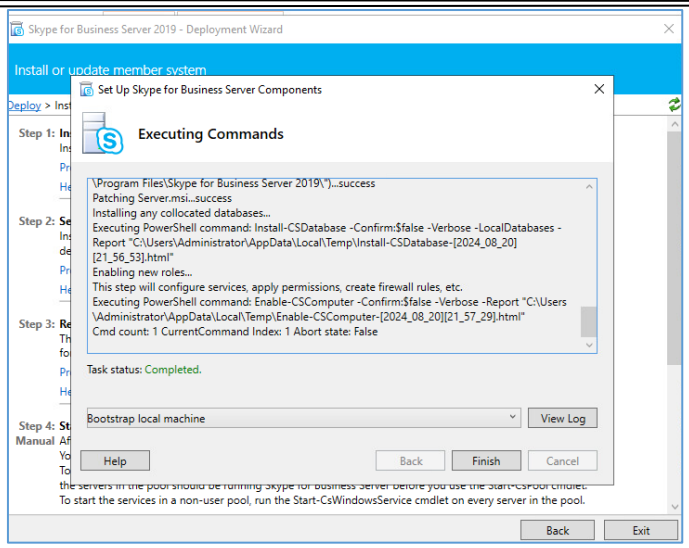
در شکل ۱۵-۱۶۰، بر روی گزینه‌ی مورد نظر کلیک کنید تا سرویس‌های مشخص شده نصب شوند، توجه داشته باشید تعداد سرویس‌هایی که برای سرور EDGE در نظر گرفته می‌شود نصف تعداد سرویس‌های سرور اصلی SKYPE است.



شکل ۱۵- ۱۶۰ راه‌اندازی سرور EDGE

همان‌طور که در شکل ۱۵-۱۶۱، مشاهده می‌کنید این قسمت هم به صورت کامل نصب شده است.

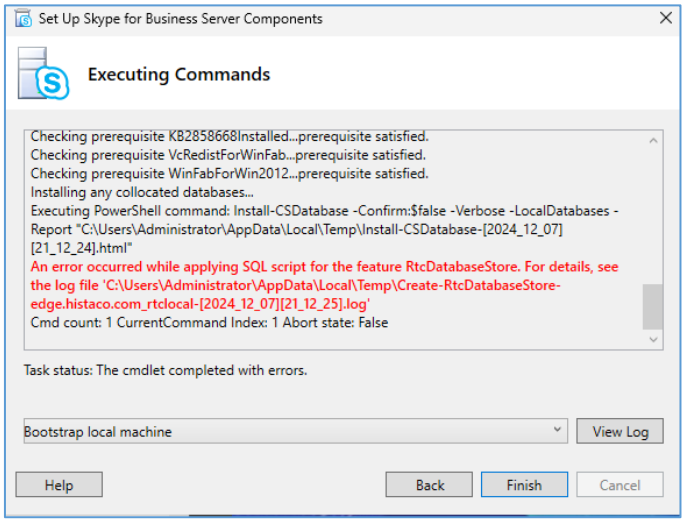
www.takbook.com



شکل ۱۵- ۱۶۱ راه‌اندازی سرور EDGE

نکته مهم:

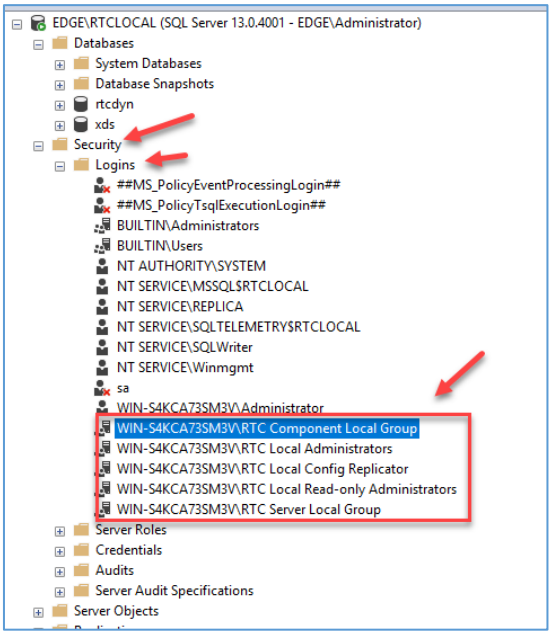
در مرحله شکل ۱۵-۱۶۱، در بعضی از سرورها با مشکل شکل ۱۵-۱۶۲، روبرو می‌شوید، در این شکل به این نکته اشاره شده است که توانایی ایجاد Database وجود ندارد.



شکل ۱۵- ۱۶۲ راه‌اندازی سرور EDGE

www.takbook.com

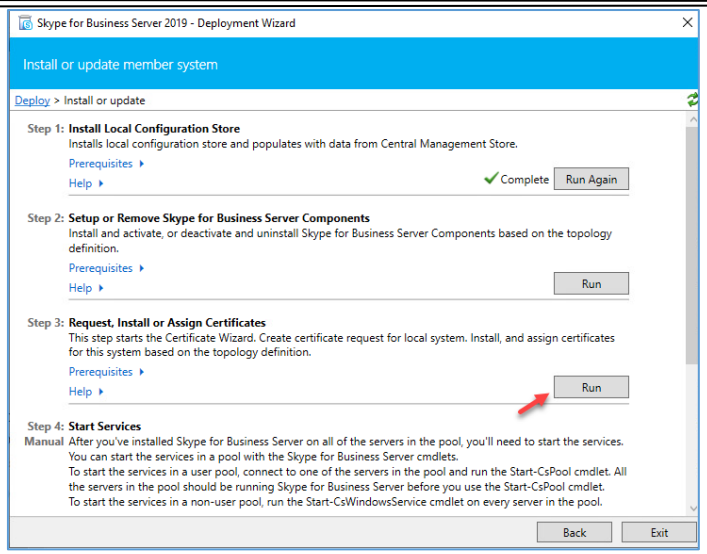
برای حل این مشکل باید نرم‌افزار SQL Server Management را بر روی سرور Edge نصب کنید و به مانند شکل ۱۵-۱۶۳، وارد قسمت Security شوید و گروه‌هایی که در شکل مشخص کردیم را حذف کنید تا مشکل حل شود.



شکل ۱۵- ۱۶۳ راه‌اندازی سرور EDGE

در مرحله‌ی آخر که مهمترین بخش هم است باید گواهینامه‌های داخلی و خارجی را فعال کنیم، برای این کار باید به مانند شکل ۱۵-۱۶۴، بر روی گزینه‌ی سوم کلیک کنید.

www.takbook.com

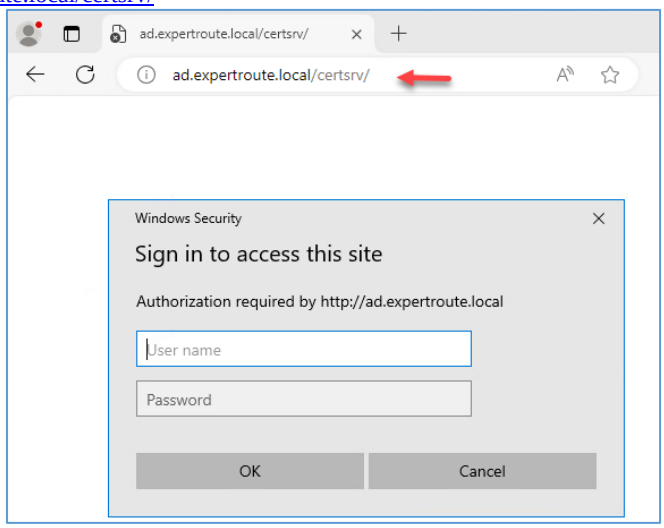


شکل ۱۵- ۱۶۴ راه‌اندازی سرور EDGE

۱۵-۷-۱ نصب گواهینامه داخلی و خارجی

قبل از اینکه این مرحله را بررسی کنیم اول باید به سرور Certificate داخلی متصل شویم و گواهینامه اصلی شبکه‌ی داخلی را نصب کنیم، برای این کار وارد آدرس زیر می‌شویم و به مانند شکل ۱۵-۱۶۵، نام کاربری و رمز ادمین را وارد می‌کنیم.

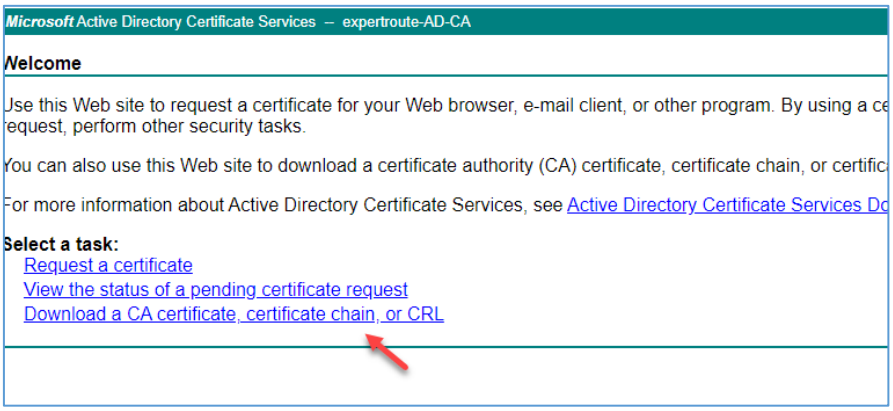
http://ad.expertroute.local/certsrv/



شکل ۱۵- ۱۶۵ نصب گواهینامه داخلی و خارجی

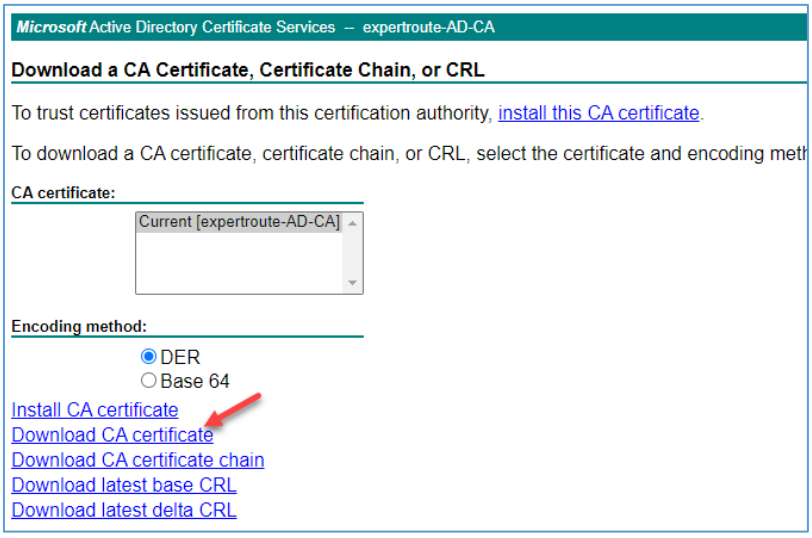
www.takbook.com

در شکل ۱۵-۱۶۶، بر روی ...Download کلیک کنید تا گواهینامه CA Root را دانلود کنید.



شکل ۱۵- ۱۶۶ نصب گواهینامه داخلی و خارجی

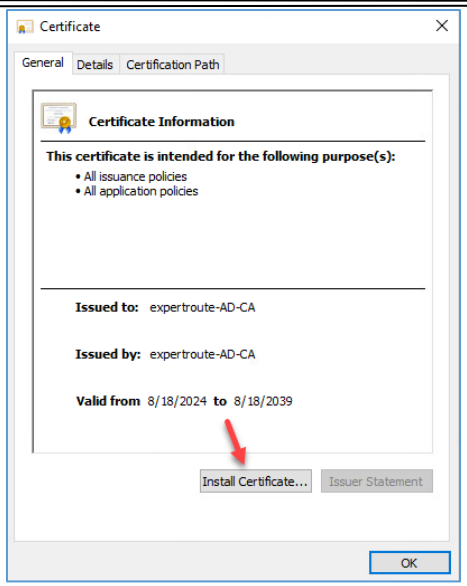
در شکل ۱۵-۱۶۷، بر روی Download CA Certificate کلیک کنید.



شکل ۱۵- ۱۶۷ نصب گواهینامه داخلی و خارجی

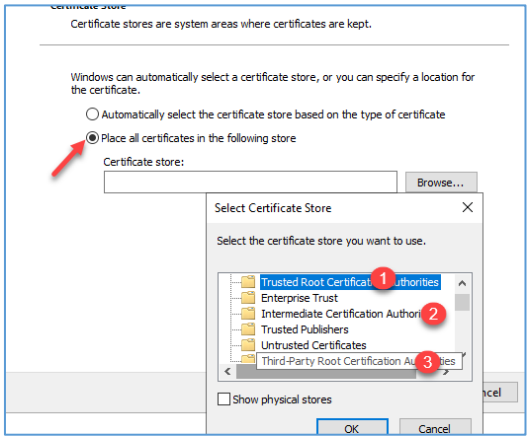
بعد از دانلود، به مانند شکل ۱۵-۱۶۸، گواهینامه‌ی مورد نظر را باز کنید و بر روی Install کلیک کنید.

www.takbook.com



شکل ۱۵- ۱۶۸ نصب گواهینامه داخلی و خارجی

در شکل ۱۵-۱۶۹، گزینه‌ی Place all Certificate in the following store را انتخاب کنید و بر روی Browse کلیک کنید و باید هر سه گزینه را انتخاب کنید تا گواهینامه در این قسمت‌ها نصب شود، یعنی سه بار باید این کار را انجام دهید.

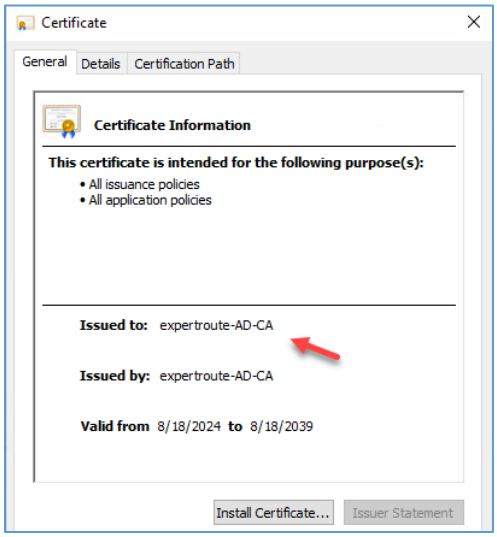


شکل ۱۵- ۱۶۹ نصب گواهینامه داخلی و خارجی

به مانند شکل ۱۵-۱۷۰، دوباره همان Certificate را باز کنید، در قسمت Issued to یا Issued by یک نام نوشته شده است، این نام به این معنا است که گواهینامه اصلی شما بر روی این نام ایجاد شده است و

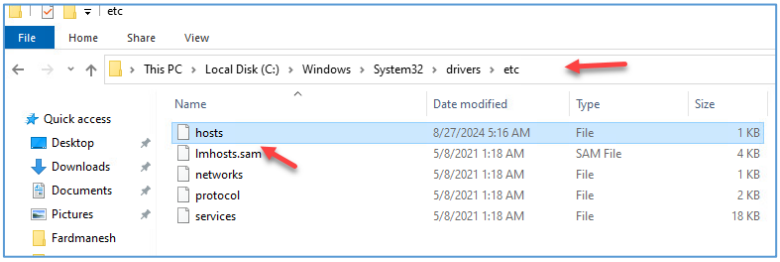
www.takbook.com

برای اینکه سرور EDGE با سرور CA یا همان Certificate ارتباط Trust داشته باشد باید به صورت زیر عمل کنید.



شکل ۱۵- ۱۷۰ نصب گواهینامه داخلی و خارجی

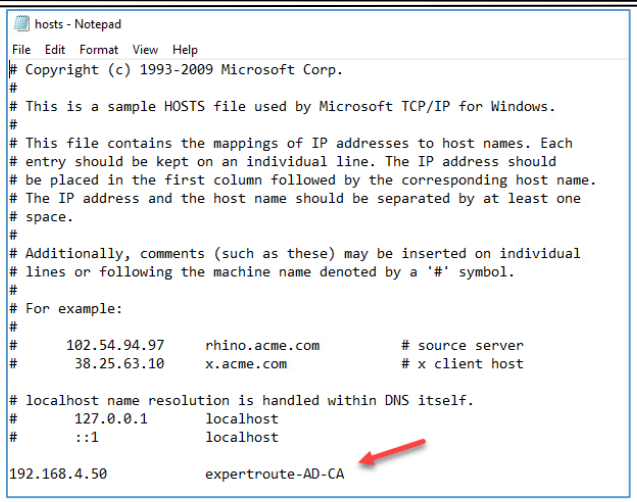
به مسیر مشخص شده در شکل ۱۵-۱۷۱، بروید و فایل hosts را با Notepad باز کنید.



شکل ۱۵- ۱۷۱ نصب گواهینامه داخلی و خارجی

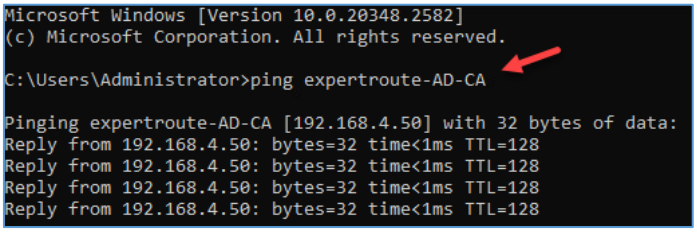
در شکل ۱۵-۱۷۲، خط مورد نظر را به آخر فایل اضافه کنید، توجه داشته باشید این اسم به IP سرور CA که در این کتاب سرور Active است اشاره می‌کند، فایل را ذخیره کنید، توجه داشته باشید اگر فایل مورد نظر ذخیره نشد باید آن را بکشید و در Desktop قرار دهید و بعد تغییرات را ذخیره و در محل اصلی قرار دهید.

www.takbook.com



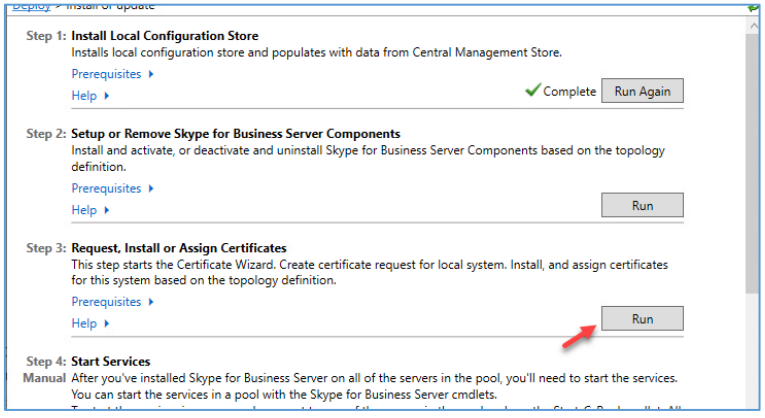
شکل ۱۵- ۱۷۲ نصب گواهینامه داخلی و خارجی

بعد از ذخیره کردن آن باید به مانند شکل ۱۵-۱۷۳، با دستور Ping بررسی کنیم که به سرور دسترسی داریم یا نه.



شکل ۱۵- ۱۷۳ نصب گواهینامه داخلی و خارجی

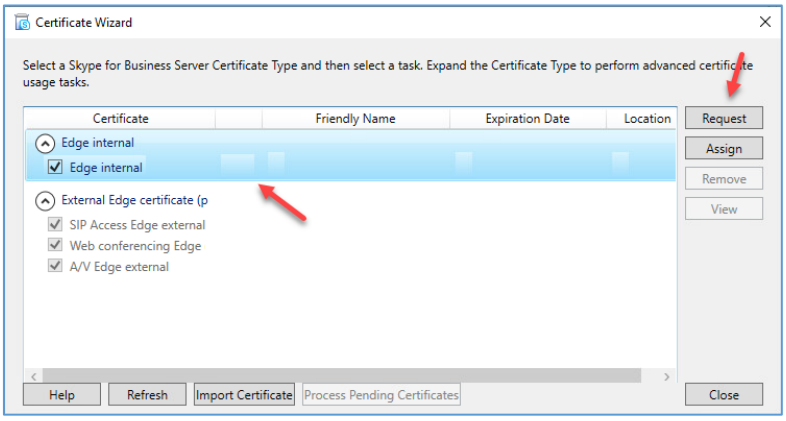
به مانند شکل ۱۵-۱۷٤، دوباره وارد Deployment Wizard می‌شویم و بر روی Run کلیک می‌کنیم.



شکل ۱۵- ۱۷۴ نصب گواهینامه داخلی و خارجی

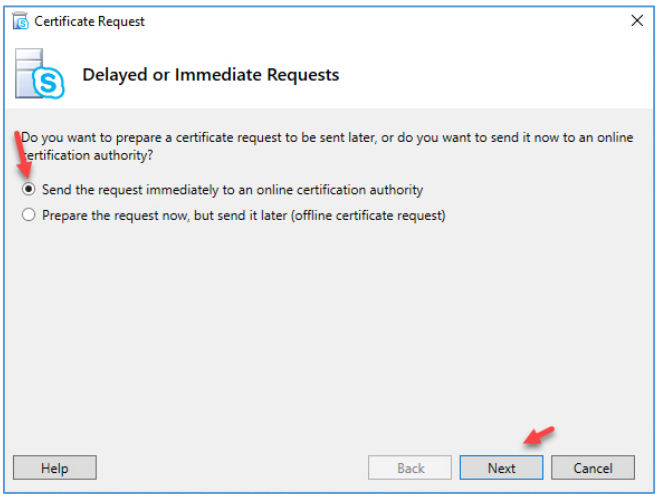
www.takbook.com

در شکل ۱۵-۱۷۵، دو قسمت را مشاهده می‌کنید، یکی برای Certificate داخلی و دیگری برای Certificate خارجی، گواهینامه داخلی را انتخاب و برای روی Request کلیک کنید.



شکل ۱۵- ۱۷۵ نصب گواهینامه داخلی و خارجی

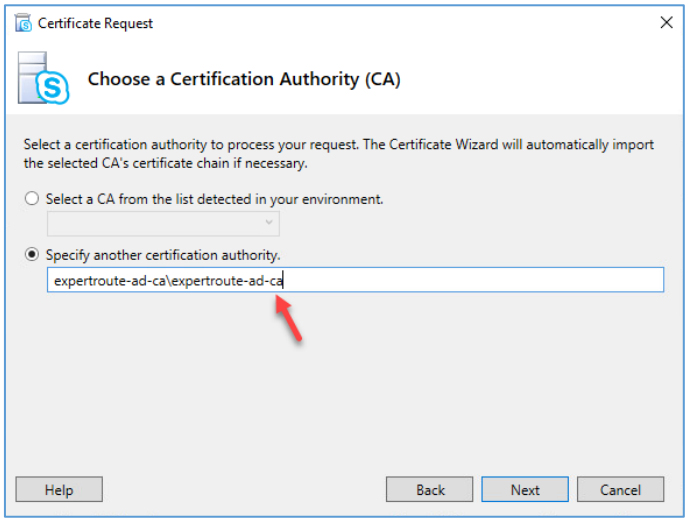
در شکل ۱۵-۱۷۶، دو روش وجود دارد، یکی به صورت آنلاین است که می‌توانیم از CA داخلی خود درخواست گواهینامه را بدهیم و دیگری به صورت آفلاین است که باید یک فایل از CA دریافت و آن را به CA عمومی که در اینترنت وجود دارد انتقال دهیم، در این قسمت گزینه‌ی Send the reauest… که به صورت آنلاین است را انتخاب کنید.



شکل ۱۵- ۱۷۶ نصب گواهینامه داخلی و خارجی

www.takbook.com

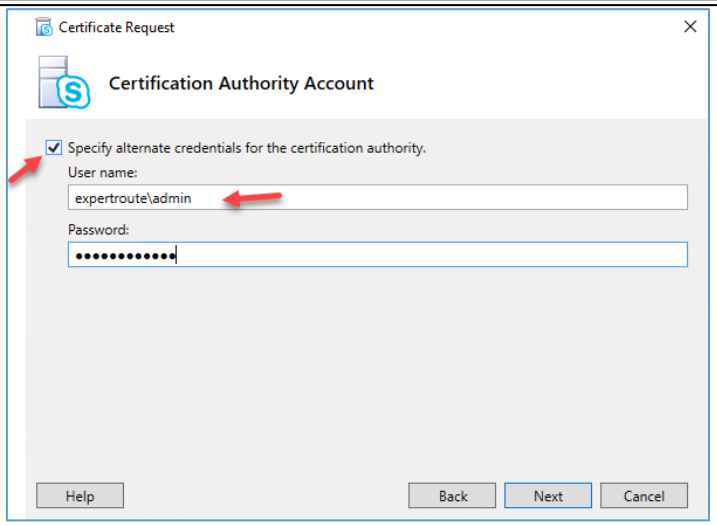
در شکل ۱۵-۱۷۷، دو قسمت را مشاهده می‌کنید، در قسمت اول اگر سرور EDGE شما عضوی از دومین بود در لیست کشویی مورد نظر سرور CA به صورت اتوماتیک نشان داده می‌شود ولی چون EDGE عضوی از دومین نیست و به صورت Workgroup کار می‌کند هیچ گزینه‌ای نشان داده نمی‌شود، پس باید گزینه‌ی دوم را انتخاب کنید و بعد باید نام سرور به همراه نام گواهینامه که در قسمت قبل بررسی کردیم را وارد کنید، فقط بین نام سرور و نام گواهینامه باید علامت \ قرار دهید.



شکل ۱۵- ۱۷۷ نصب گواهینامه داخلی و خارجی

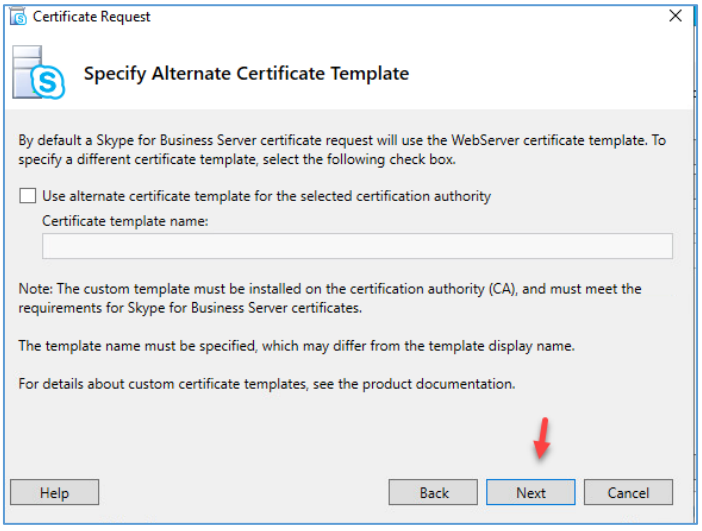
در شکل ۱۵-۱۷۸، باید نام کاربری و رمز ادمین را وارد کنید تا بتوانیم به سرور CA متصل شویم و گواهینامه ایجاد کنیم.

www.takbook.com



شکل ۱۵- ۱۷۸ نصب گواهینامه داخلی و خارجی

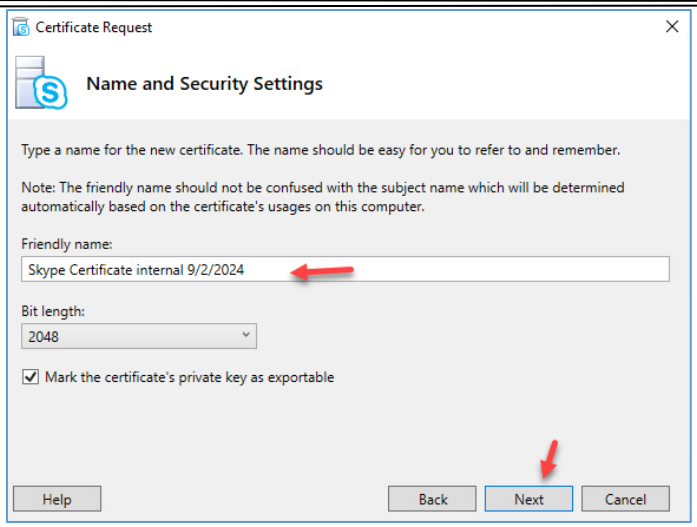
در شکل ۱۵-۱۷۹، به گزینه‌ای دست نزنید و فقط بر روی Next کلیک کنید.



شکل ۱۵- ۱۷۹ نصب گواهینامه داخلی و خارجی

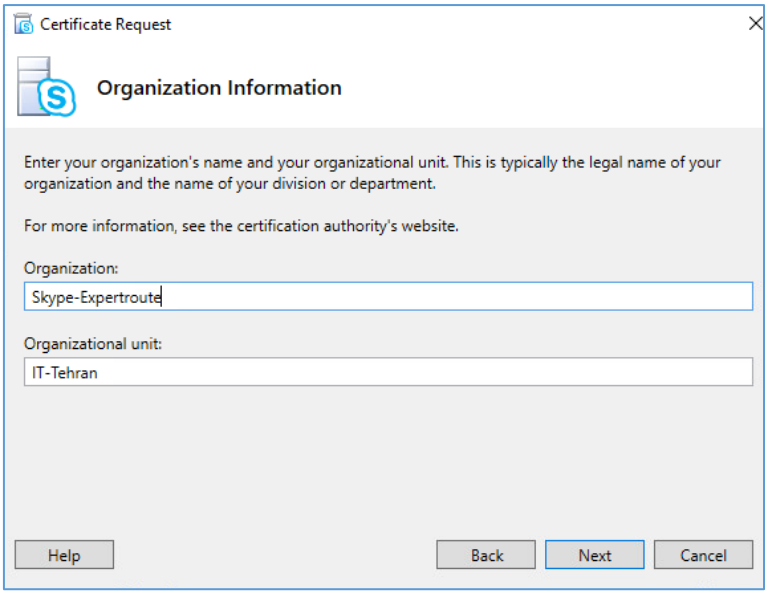
در شکل ۱۵-۱۸۰، نام گواهینامه خود را وارد و بر روی next کلیک کنید.

www.takbook.com



شکل ۱۵- ۱۸۰ نصب گواهینامه داخلی و خارجی

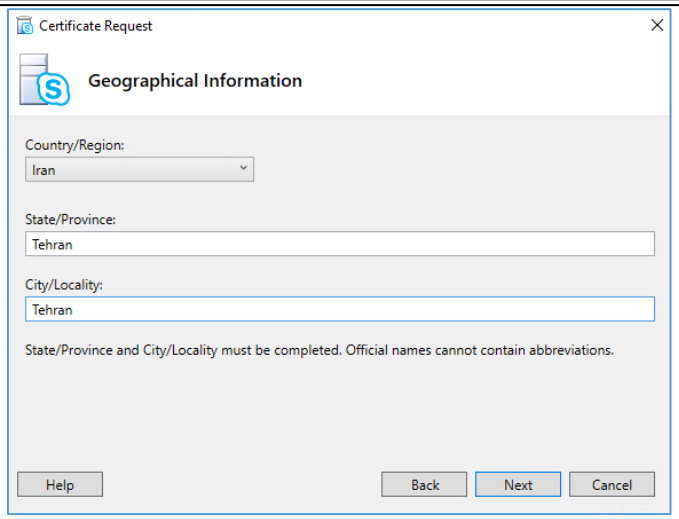
در شکل ۱۵-۱۸۱، باید نام Organization خود را وارد کنید، این نام می‌تواند دلخواه باشد.



شکل ۱۵- ۱۸۱ نصب گواهینامه داخلی و خارجی

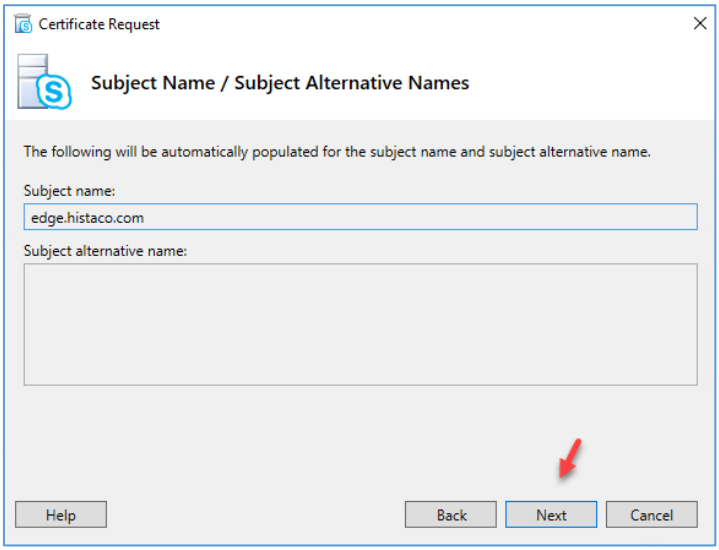
در شکل ۱۵-۱۸۲، باید نام کشور و شهر خود را مشخص کنید.

www.takbook.com



شکل ۱۵- ۱۸۲ نصب گواهینامه داخلی و خارجی

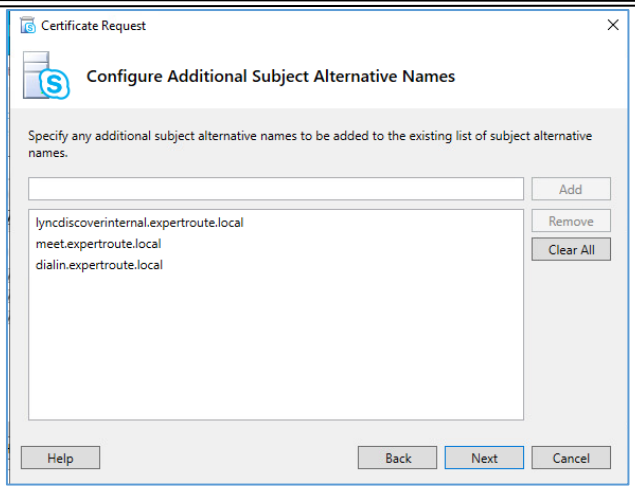
در شکل ۱۵-۱۸۳، بر روی Next کلیک کنید.



شکل ۱۵- ۱۸۳ نصب گواهینامه داخلی و خارجی

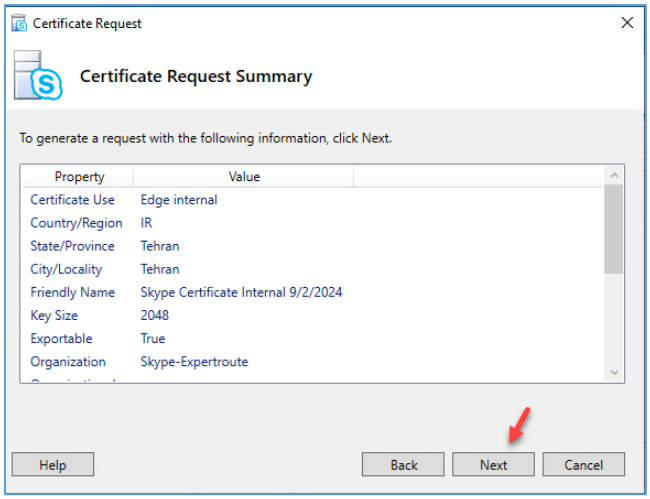
در شکل ۱۵-۱۸٤، باید آدرس‌های اضافه‌ی زیر را را هم وارد کنید تا در گواهینامه مورد نظر قرار بگیرد.

www.takbook.com



شکل ۱۵- ۱۸۴ نصب گواهینامه داخلی و خارجی

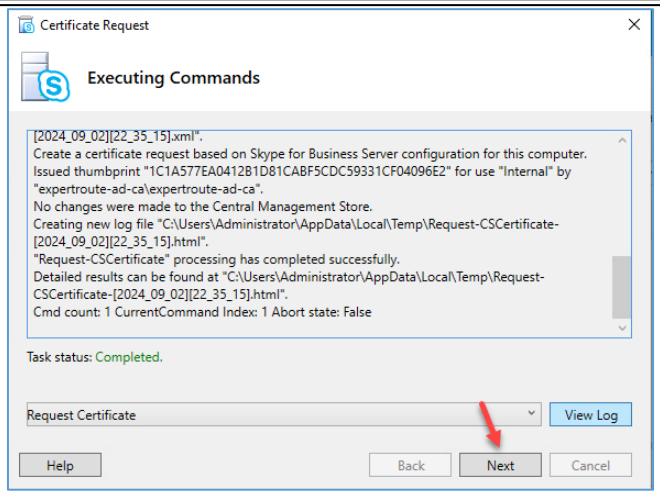
در شکل ۱۵-۱۸۵، بر روی Next کلیک کنید تا گواهینامه مورد نظر ایجاد شود.



شکل ۱۵- ۱۸۵ نصب گواهینامه داخلی و خارجی

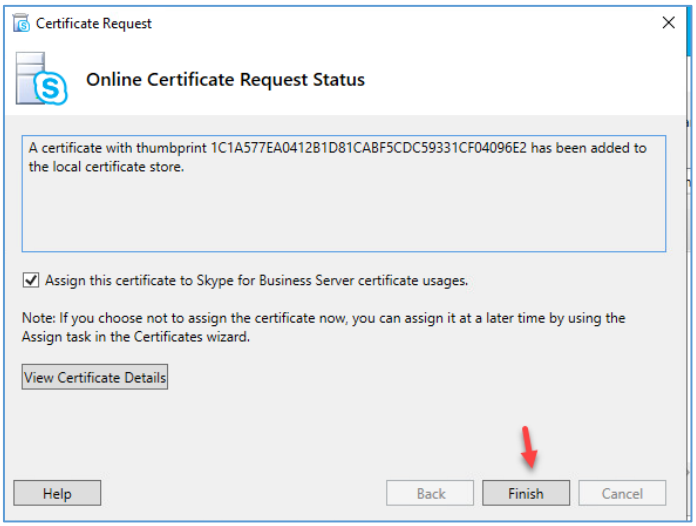
همان‌طور که در شکل ۱۵-۱۸۶، مشاهده می‌کنید گواهینامه‌ی مورد نظر با موفقیت ایجاد شده است، بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۵- ۱۸۶ نصب گواهینامه داخلی و خارجی

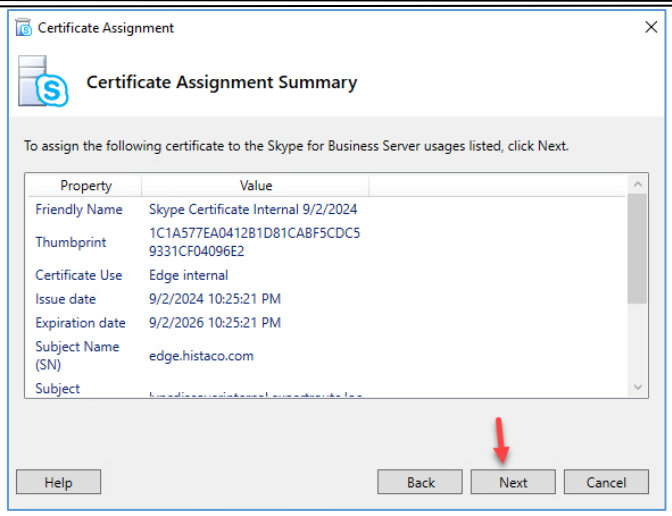
در شکل ۱۵-۱۸۷، بر روی Finish کلیک کنید تا صفحه‌ی Assign ظاهر شود تا بتوانیم گواهینامه را بر روی Skype نصب کنیم.



شکل ۱۵- ۱۸۷ نصب گواهینامه داخلی و خارجی

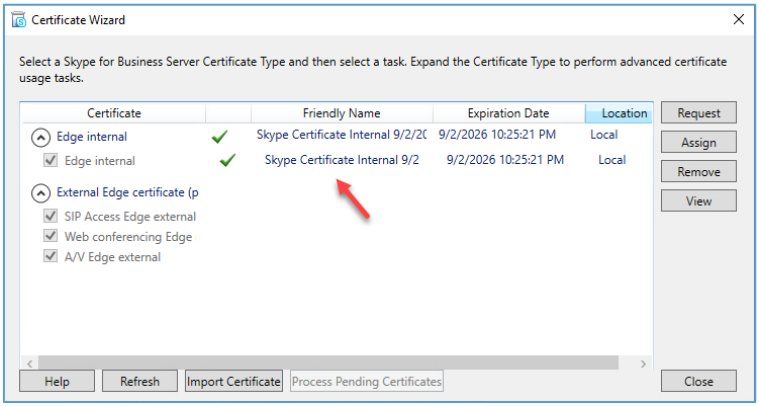
در شکل ۱۵-۱۸۸، بر روی Next کلیک کنید تا کار Assign گواهینامه انجام شود.

www.takbook.com



شکل ۱۵- ۱۸۸ نصب گواهینامه داخلی و خارجی

همان‌طور که در شکل ۱۵-۱۸۹، مشاهده می‌کنید، گواهینامه‌ی داخلی با موفقیت نصب شده است و همه چیز برای نصب گواهینامه خارجی آماده است.

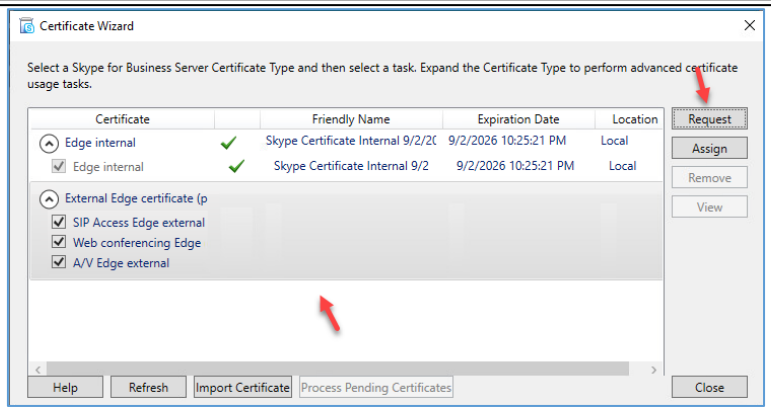


شکل ۱۵- ۱۸۹ نصب گواهینامه داخلی و خارجی

برای نصب گواهینامه خارجی اول باید یک درخواست گواهینامه داخلی بدهیم و بعد آن گواهینامه را در سایت‌های معتبر وارد و یک فایل خروجی از آن تهیه کنیم.

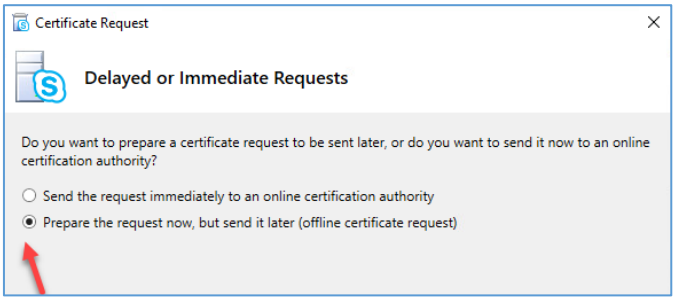
برای شروع به مانند شکل ۱۵-۱۹۰، گواهینامه مورد نظر را انتخاب و بر روی Request کلیک کنید.

www.takbook.com



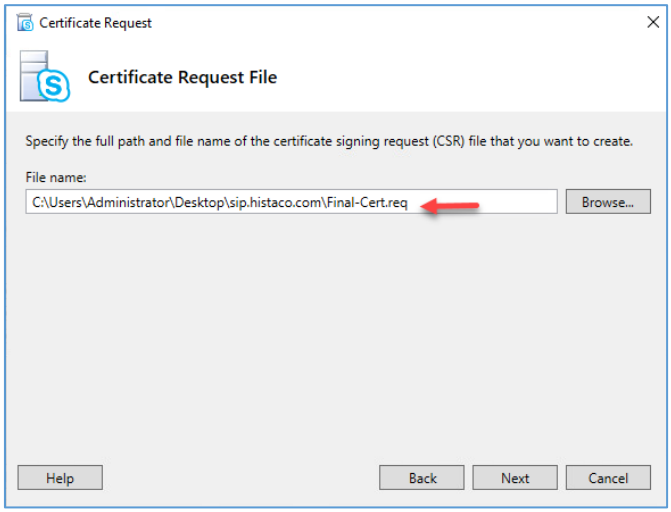
شکل ۱۵- ۱۹۰ نصب گواهینامه داخلی و خارجی

در شکل ۱۵-۱۹۱، باید گزینه‌ی دوم یعنی آفلاین را انتخاب کنیم تا یک فایل با پسوند Req ایجاد شود.



شکل ۱۵- ۱۹۱ نصب گواهینامه داخلی و خارجی

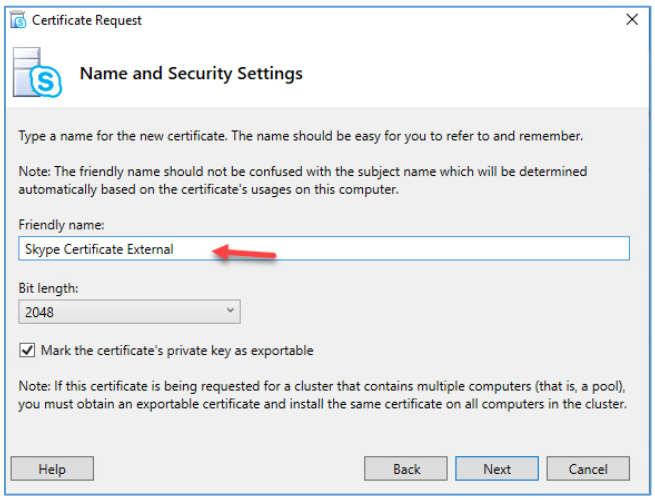
در شکل ۱۵-۱۹۲، باید نام یک فایل را به دلخواه وارد کنید تا اطلاعات در آن کپی شود.



شکل ۱۵- ۱۹۲ نصب گواهینامه داخلی و خارجی

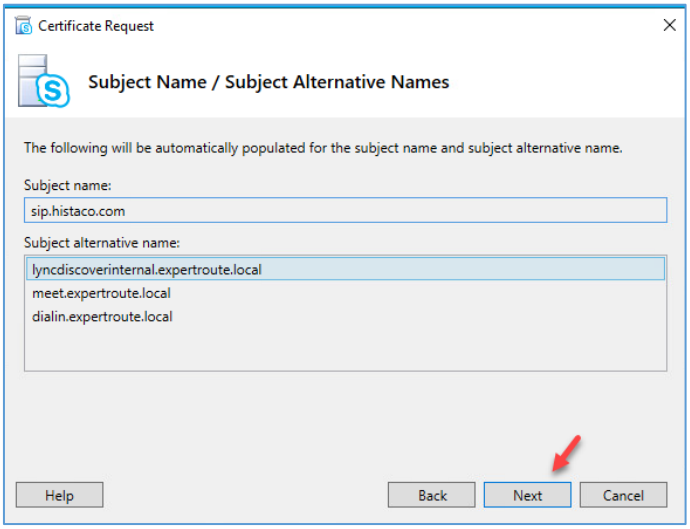
www.takbook.com

در شکل ۱۵-۱۹۳، نام Certificate خود را وارد و بر روی Next کلیک کنید.



شکل ۱۵- ۱۹۳ نصب گواهینامه داخلی و خارجی

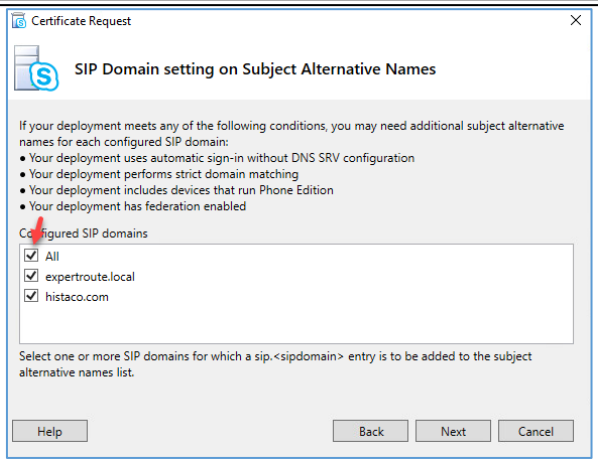
در شکل ۱۵-۱۹٤، بر روی Next کلیک کنید.



شکل ۱۵- ۱۹۴ نصب گواهینامه داخلی و خارجی

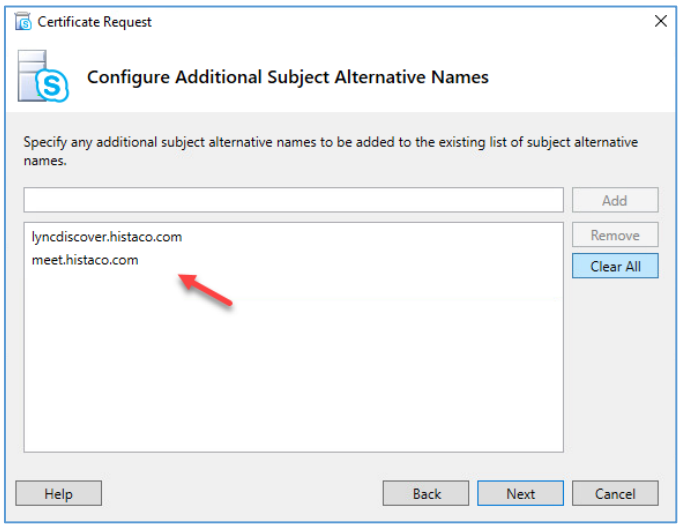
در شکل ۱۵-۱۹۵، هر دو دومین را انتخاب کنید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۵- ۱۹۵ نصب گواهینامه داخلی و خارجی

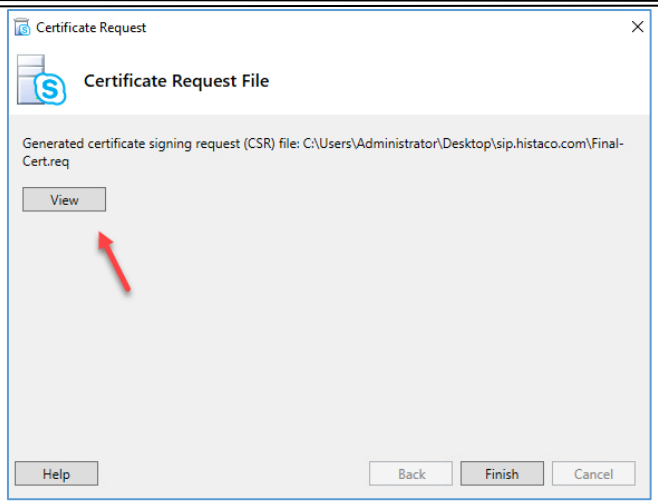
در شکل ۱۵-۱۹۶، باید دو FQDN را به لیست اضافه کنید، توجه داشته باشید این آدرس‌ها در زمانی که گواهینامه ایجاد می‌کنید در زیر مجموعه‌ی آن قرار می‌گیرند و همین موضوع باعث می‌شود آدرس مورد نظر Trsut شود و Skype شما از بیرون متصل شود.



شکل ۱۵- ۱۹۶ نصب گواهینامه داخلی و خارجی

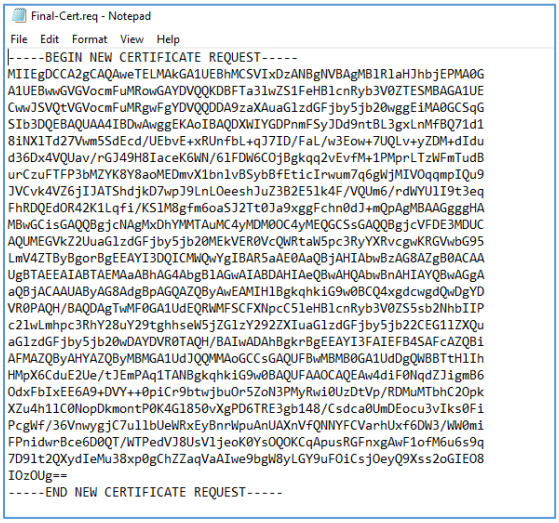
بعد از ایجاد فایل مورد نظر به مانند شکل ۱۵-۱۹۷، بر روی View کلیک کنید.

www.takbook.com



شکل ۱۵- ۱۹۷ نصب گواهینامه داخلی و خارجی

در ادامه کار به مانند شکل ۱۵-۱۹۸، اطلاعات فایل را باید کپی بگیرید و در یک سایتی که SSL عمومی ارائه می‌دهد وارد کنیم.

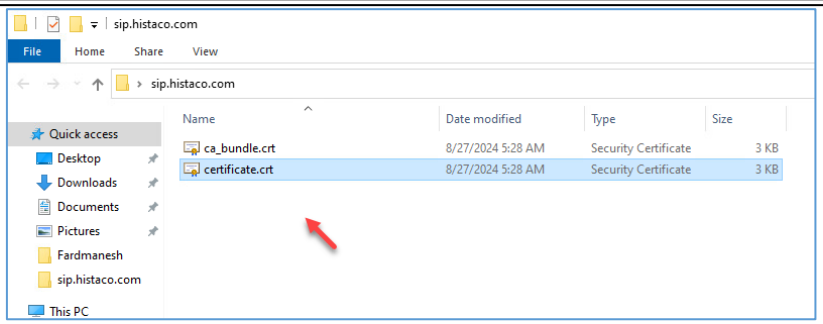


شکل ۱۵- ۱۹۸ نصب گواهینامه داخلی و خارجی

در مورد ایجاد فایل SSL در سرور های خارجی اگر نیاز به کمک داشتید می‌توانید با بنده در تماس باشید.

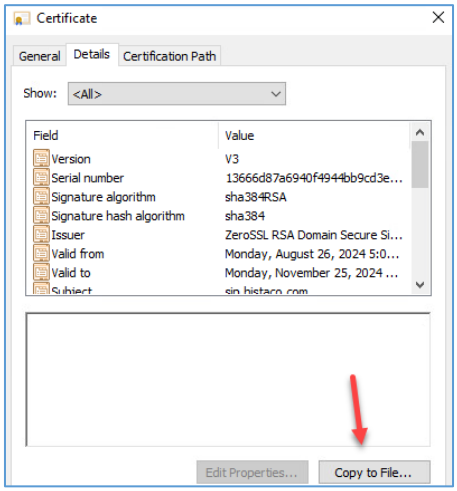
بعد از اینکه از سرورهای عمومی فایل SSL دریافت کردید باید پسوند آنها را به Cer تغییر دهید برای این کار به مانند شکل ۱۵-۱۹۷، بر روی Certficate.crt دوبار کلیک کنید.

www.takbook.com



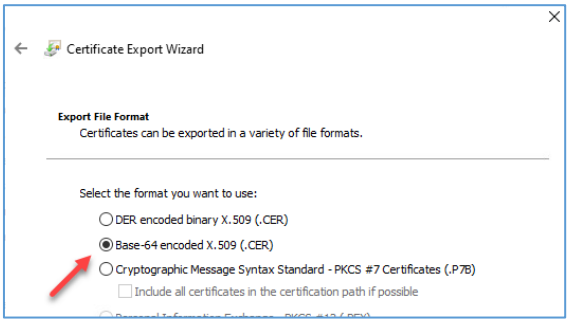
شکل ۱۵- ۱۹۹ نصب گواهینامه داخلی و خارجی

در شکل ۱۵-۲۰۰، وارد تب Details شوید و بر روی Copy to File کلیک کنید.



شکل ۱۵- ۲۰۰ نصب گواهینامه داخلی و خارجی

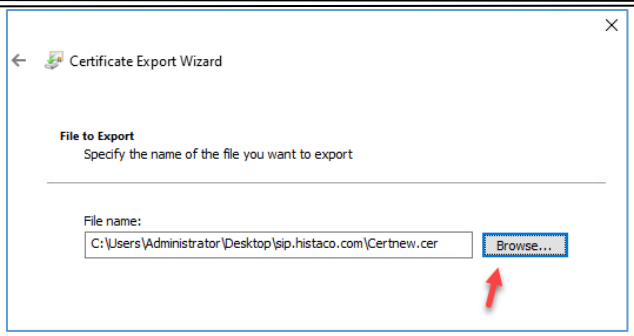
در شکل ۱۵-۲۰۱، گزینه‌ی دوم را انتخاب و بر روی Next کلیک کنید.



شکل ۱۵- ۲۰۱ نصب گواهینامه داخلی و خارجی

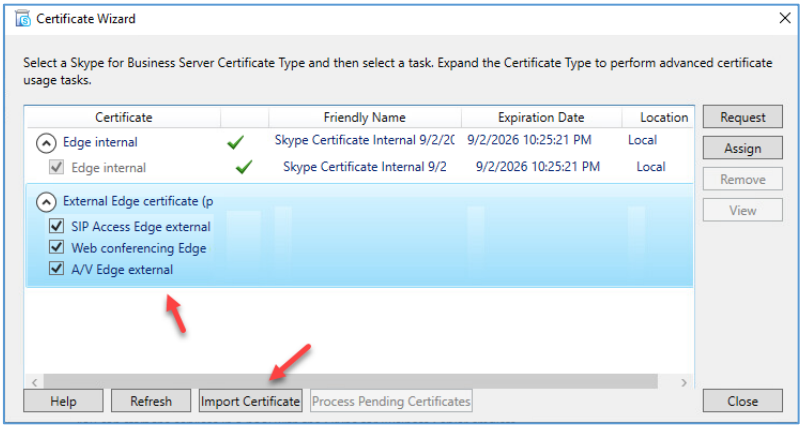
در شکل ۱۵-۲۰۲، یک مسیر مشخص کنید و فایل را با پسوند Cer ذخیره کنید.

www.takbook.com



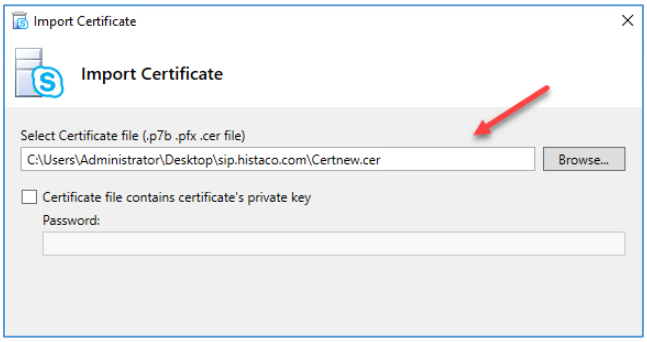
شکل ۱۵- ۲۰۲ نصب گواهینامه داخلی و خارجی

بعد از ایجاد گواهینامه‌ی مورد نظر باید به مانند شکل ۱۵-۲۰۳، به قسمت قبل برگردیم و بر روی Import Certificate کلیک کنیم.



شکل ۱۵- ۲۰۳ نصب گواهینامه داخلی و خارجی

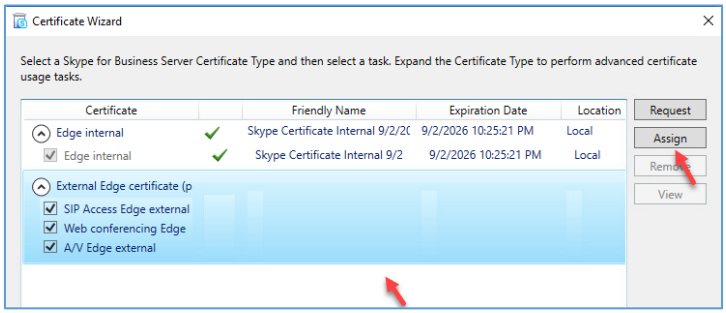
طبق شکل ۱۵-۲۰۴، گواهینامه جدید را انتخاب می‌کنیم و بر روی Next کلیک می‌کنیم تا وارد سرور Skype شود.



شکل ۱۵- ۲۰۴ نصب گواهینامه داخلی و خارجی

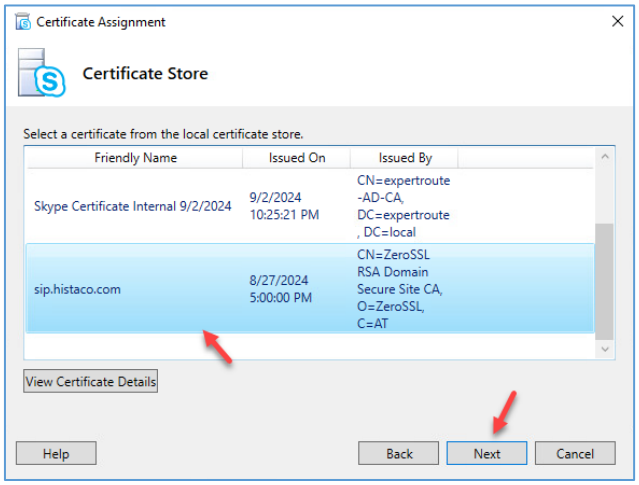
www.takbook.com

به مانند شکل ۱۵–۲۰۵، گواهینامه مورد نظر در Store قرار گرفته است و باید آن را در Skype اضافه کرد تا سرویس‌ها فعال شوند برای این‌کار بر روی Assign کلیک کنید.



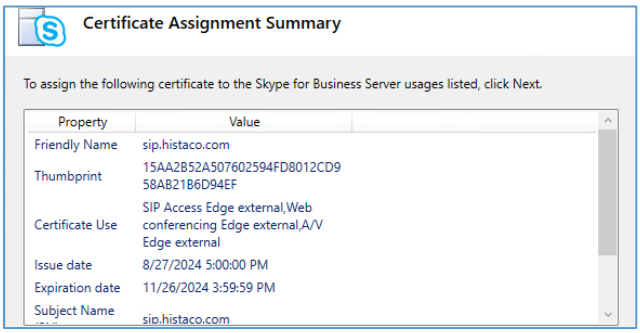
شکل ۱۵– ۲۰۵ نصب گواهینامه داخلی و خارجی

گواهینامه‌ای که Import کرده بودید را به مانند شکل ۱۵–۲۰۶، انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۵– ۲۰۶ نصب گواهینامه داخلی و خارجی

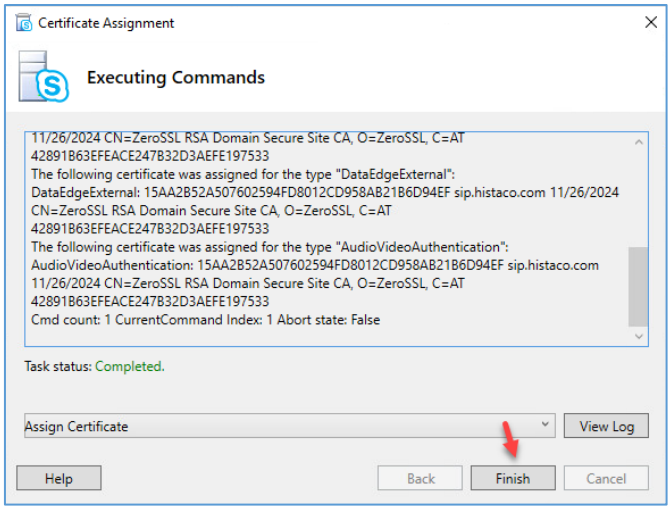
در شکل ۱۵–۲۰۷، بر روی Next کلیک کنید تا گواهینامه وارد Skype شود.



شکل ۱۵– ۲۰۷ نصب گواهینامه داخلی و خارجی

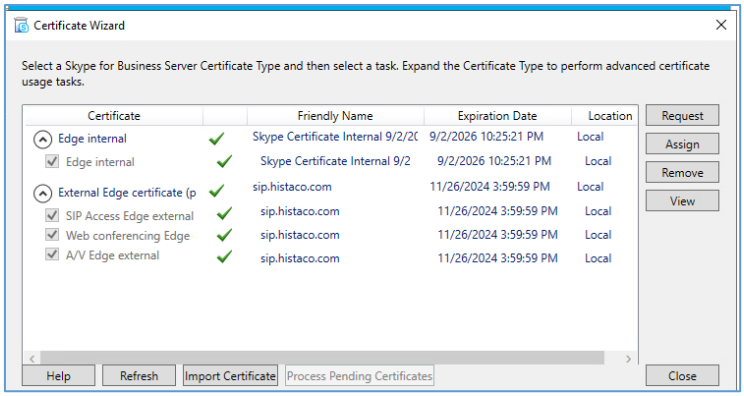
www.takbook.com

همان‌طور که در شکل ۱۵–۲۰۸، مشاهده می‌کنید با موفقیت کار انجام شده است، توجه داشته باشید در این قسمت نباید هیچ خطا یا اخطاری داشته باشید چون سرویس اصلی که پورت 5061 بر روی آن فعال است اجرا نخواهد شد.



شکل ۱۵- ۲۰۸ نصب گواهینامه داخلی و خارجی

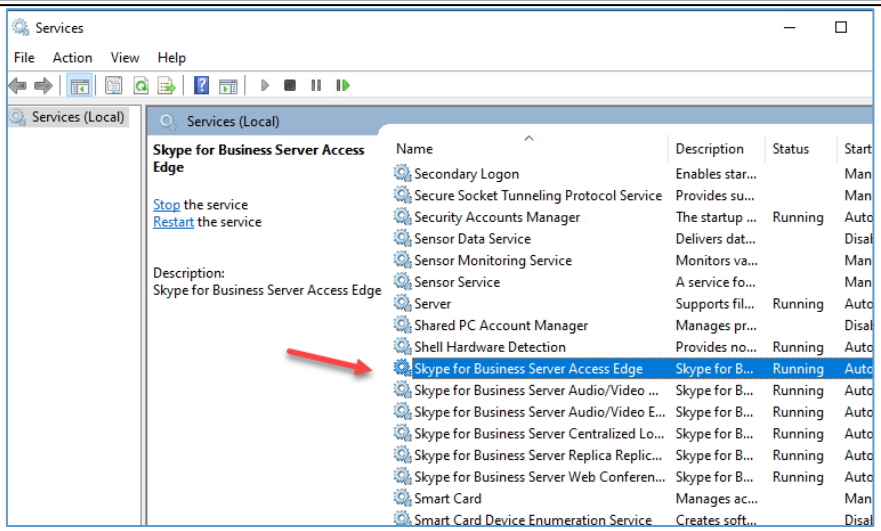
در شکل ۱۵–۲۰۹، با موفقیت گواهینامه‌ی داخلی و خارجی نصب شده است.



شکل ۱۵- ۲۰۹ نصب گواهینامه داخلی و خارجی

اگر به مانند شکل ۱۵–۲۱۰، وارد Services شویم، سرویس‌های مربوط به EDGE را مشاهده می‌کنید که با موفقیت اجرا شده‌اند.

www.takbook.com



شکل ۱۵- ۲۱۰ نصب گواهینامه داخلی و خارجی

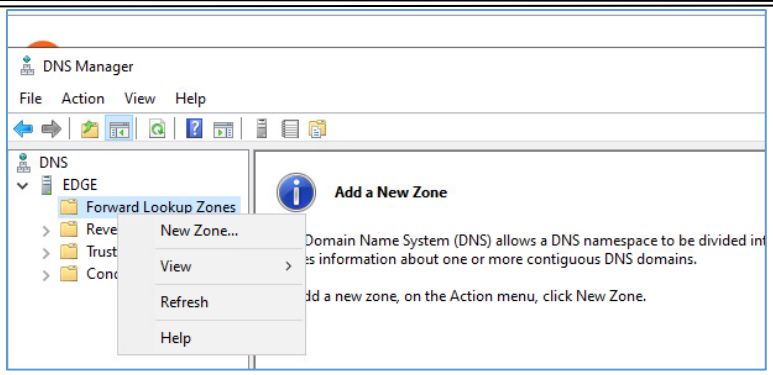
نکته مهم: قبل از انجام کار بعدی یعنی " تنظیم DNS داخلی و خارجی" می‌توانید تست عملکرد را انجام دهید و نیازی به تنظیم آن نیست و می‌توانید مستقیم به بخش " فعال کردن دومین خارجی در شبکه داخلی" مراجعه کنید، اگر با مشکل روبرو شدید می‌توانید قسمت بعدی یعنی " تنظیم DNS داخلی و خارجی " را انجام دهید.

۲-۷-۱۵ تنظیم DNS داخلی و خارجی

بعد از اینکه گواهینامه را با موفقیت بر روی سرور نصب کردید باید سرویس DNS داخلی و خارجی را تنظیم کنیم، اولین کاری که انجام می‌دهیم این است که وارد Server Manger می‌شویم و سرویس DNS را نصب می‌کنیم و بعد از نصب آن را اجرا می‌کنیم، توجه داشته باشید سرویس DNS باید در سرور EDGE نصب شود.

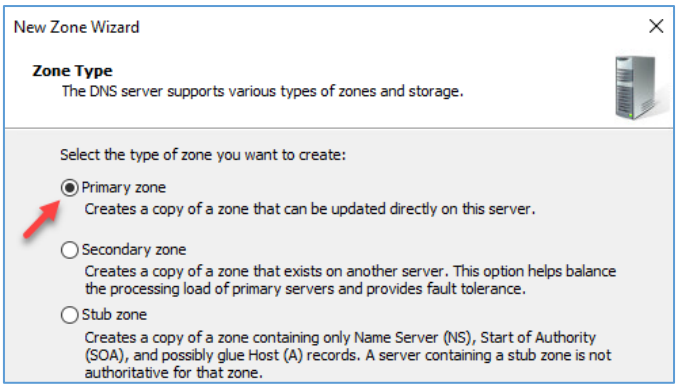
بعد از نصب سرویس را به مانند شکل ۱۵-۲۱۱، اجرا و بر روی Forward Lookup Zones کلیک راست کنید و گزینه‌ی New Zone را انتخاب کنید.

www.takbook.com



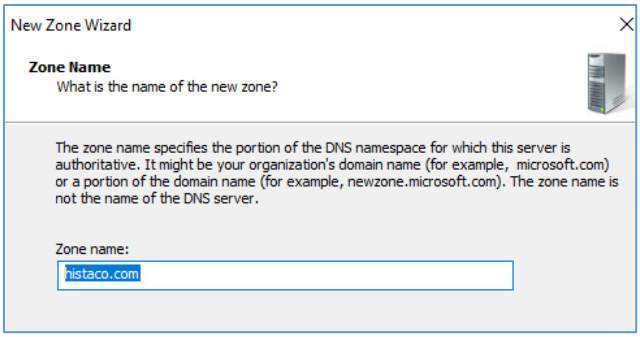
شکل ۱۵- ۲۱۱ تنظیم DNS داخلی و خارجی

در شکل ۱۵-۲۱۲، گزینه‌ی Primary Zone را انتخاب کنید.



شکل ۱۵- ۲۱۲ تنظیم DNS داخلی و خارجی

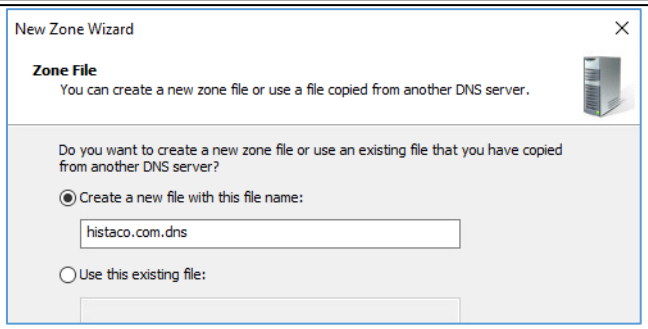
در شکل ۱۵-۲۱۳، باید نام دویمن خارجی خود را وارد کنید.



شکل ۱۵- ۲۱۳ تنظیم DNS داخلی و خارجی

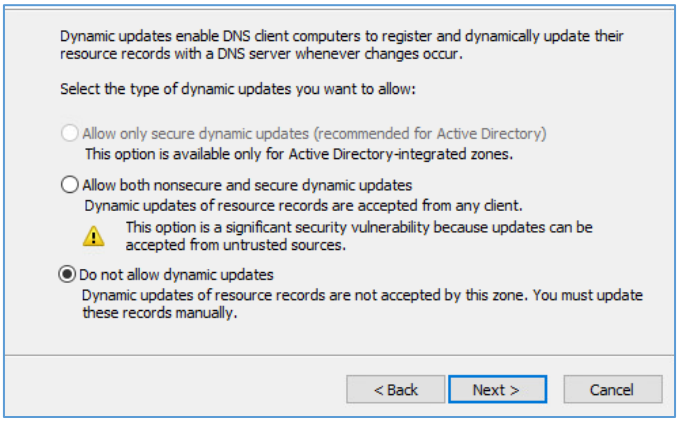
در شکل ۱۵-۲۱٤، گزینه‌ی اول را انتخاب و بر روی Next کلیک کنید.

www.takbook.com



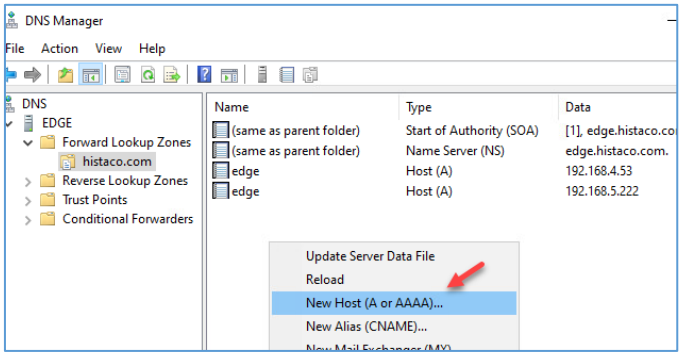
شکل ۱۵- ۲۱۴ تنظیم DNS داخلی و خارجی

در شکل ۱۵-۲۱۵، فقط بر روی Next کلیک کنید.



شکل ۱۵- ۲۱۵ تنظیم DNS داخلی و خارجی

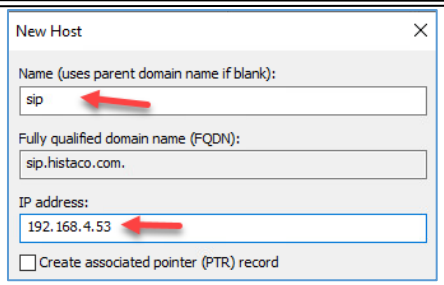
بعد از ایجاد Zone مورد نظر به مانند شکل ۱۵-۲۱۶، دو آدرس Internal و External به صورت اتوماتیک ایجاد می‌شود و در ادامه کار باید چند A رکورد جدید ایجاد کنیم و چند آدرس را به لیست اضافه کنیم.



شکل ۱۵- ۲۱۶ تنظیم DNS داخلی و خارجی

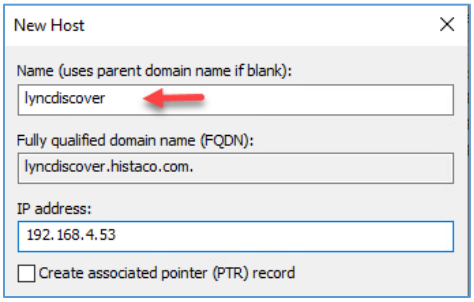
در شکل ۱۵-۲۱۷، آدرس sip را وارد کنید و IP که به سمت شبکه‌ی داخلی است را وارد کنید.

www.takbook.com



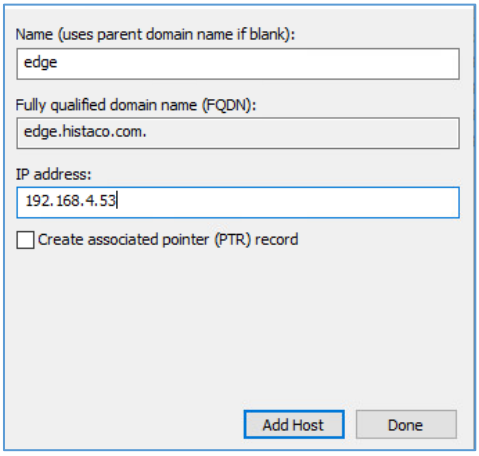
شکل ۱۵- ۲۱۷ تنظیم DNS داخلی و خارجی

به مانند شکل ۱۵–۲۱۸، دوباره یک A رکورد جدید ایجاد کنید و آدرس lyncdiscover را وارد کنید و آدرس شبکه‌ی داخلی را بدهید.



شکل ۱۵- ۲۱۸ تنظیم DNS داخلی و خارجی

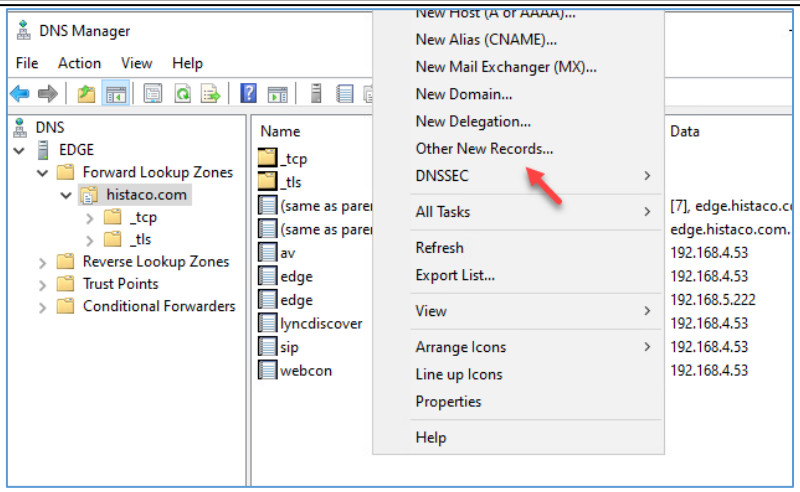
به مانند شکل ۱۵–۲۱۹، یکی دیگر برای آدرس edge ایجاد کنید.



شکل ۱۵- ۲۱۹ تنظیم DNS داخلی و خارجی

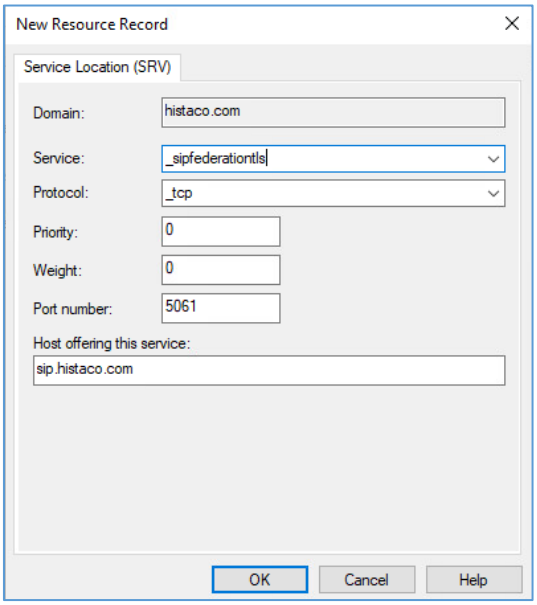
در ادامه کار به مانند شکل ۱۵–۲۲۰، بر روی صفحه خالی کلیک راست کنید و گزینه‌ی Other New Records را انتخاب کنید.

www.takbook.com



شکل ۱۵- ۲۲۰ تنظیم DNS داخلی و خارجی

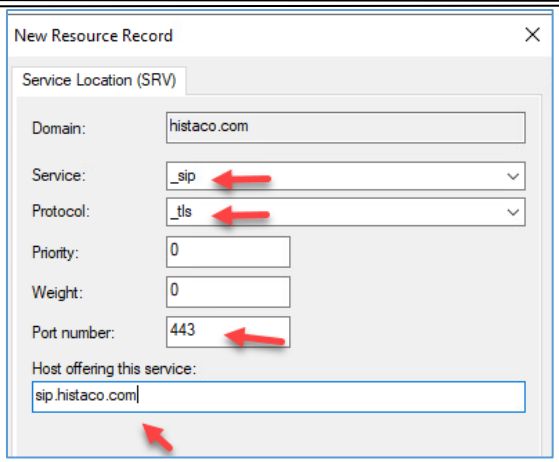
یک رکودر SRV ایجاد می‌کنیم و به مانند شکل ۱۵-۲۲۱، اطلاعات آن را وارد می‌کنیم، در قسمت Service باید sipfederaiontls_ را وارد کنید و پروتکل آن را tcp_ در نظر بگیرید و پورت آن را هم 5061 که به سمت سرور sip.histaco.com ارسال می‌شوند.



شکل ۱۵- ۲۲۱ تنظیم DNS داخلی و خارجی

دوباره یک SRV رکورد جدید ایجاد می‌کنیم و به مانند شکل ۱۵-۲۲۲، سرویس sip_ را به همراه پروتکل tls وارد می‌کنیم و به سمت sip.histaco.com ارسال می‌کنیم.

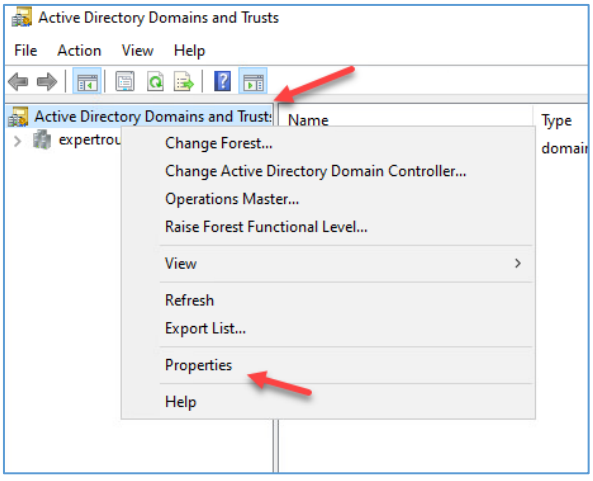
www.takbook.com



شکل ۱۵- ۲۲۲ تنظیم DNS داخلی و خارجی

۳-۷-۱۵ فعال کردن دومین خارجی در شبکه داخلی

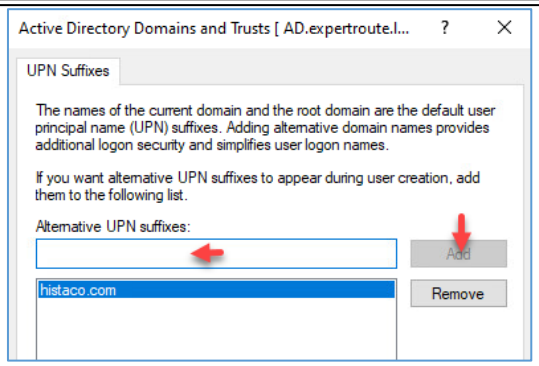
در این مرحله باید دومین خارجی خود را که بر روی آن Certificate فعال کردید را به شبکه داخلی معرفی کنیم، برای این کار باید وارد Active Directory شویم و به مانند شکل ۱۵-۲۲۳، سرویس Active Directory Domain and Trust را اجرا کنید و بر روی عنوان سرور کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.



شکل ۱۵- ۲۲۳ فعال کردن دومین خارجی در شبکه داخلی

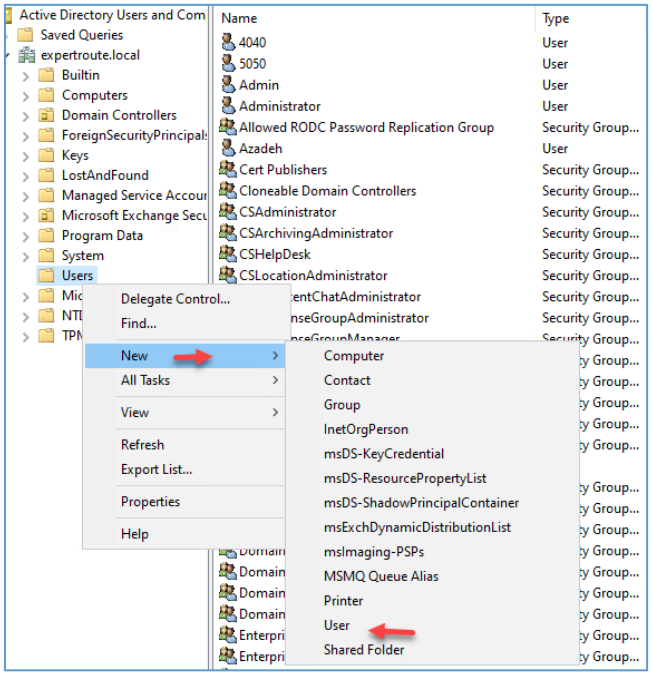
در ادامه و در شکل ۱۵-۲۲٤، Alternative UPN suffixes نام دومین خارجی خود را وارد و بر روی Add کلیک کنید تا به لیست اضافه شود.

www.takbook.com



شکل ۱۵ - ۲۲۴ فعال کردن دومین خارجی در شبکه داخلی

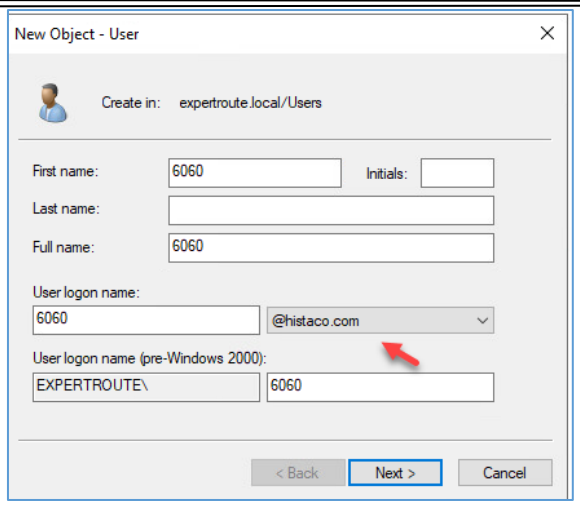
بعد از این کار باید به مانند شکل ۱۵-۲۲۵، وارد سرویس Active Dierctory Users and Computers شوید و یک کاربر جدید ایجاد کنید.



شکل ۱۵ - ۲۲۵ فعال کردن دومین خارجی در شبکه داخلی

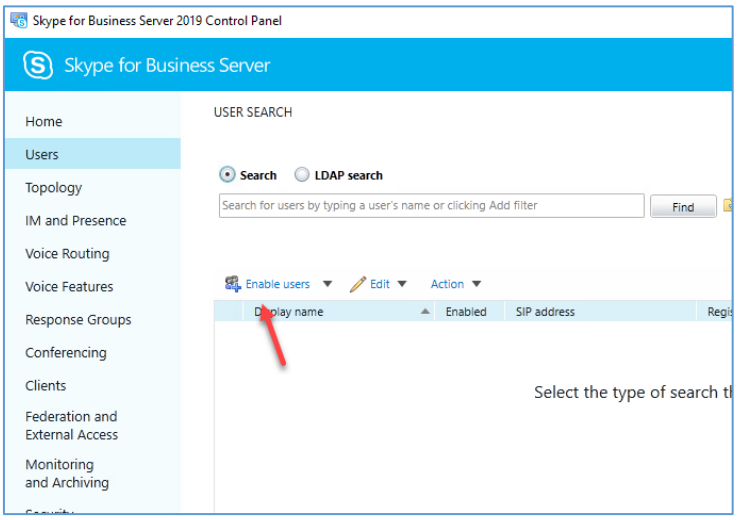
در هنگام ایجاد کاربر جدید به مانند شکل ۱۵-۲۲۶، دومین خارجی را انتخاب کنید.

www.takbook.com



شکل ۱۵ - ۲۲۶ فعال کردن دومین خارجی در شبکه داخلی

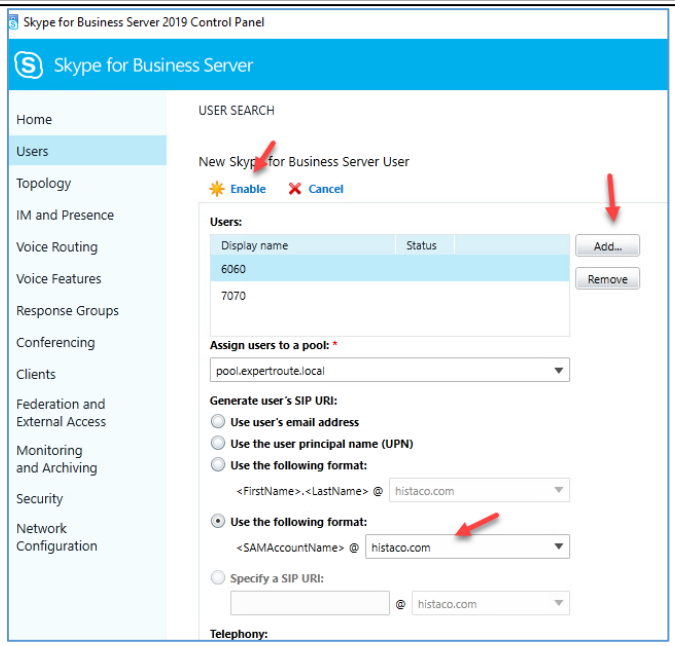
دو کاربر جدید با شماره 6060 و 7070 ایجاد کردیم که نام دومین آنها histaco.com است، در ادامه کار باید وارد سرور Skype (sk19) شوید و سرویس Skype For business control panel را اجرا کنید و در صفحه باز شده به مانند شکل ۱۵–۲۲۷، وارد Users شوید و بر روی Enable users کلیک کنید.



شکل ۱۵ - ۲۲۷ فعال کردن دومین خارجی در شبکه داخلی

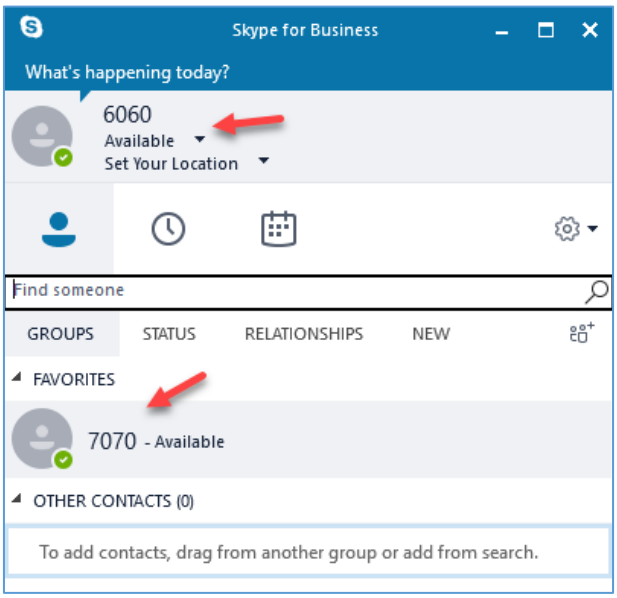
به مانند شکل ۱۵–۲۲۸، بر روی Add کلیک کنید و کاربران مورد نظر خود را به لیست اضافه کنید، بعد از این کار باید در قسمت دومین نام دومین جدید خود را انتخاب کنید تا کاربران خارج از شبکه بتوانند وارد Skype شوند، بعد از تنظیم اطلاعات بر روی Enable کلیک کنید تا کاربران به لیست اضافه شوند.

www.takbook.com



شکل ۱۵ - ۲۲۸ فعال کردن دومین خارجی در شبکه داخلی

بعد از این کار همه چیز آماده است تا بتوانید با استفاده از کاربران خارج از شبکه، وارد skype شوید، در شکل ۱۵-۲۲۹، همین موضوع مشخص شده است و دو کاربری که ایجاد کردیم با موفقیت توانستن وارد شبکه شوند.



شکل ۱۵ - ۲۲۹ فعال کردن دومین خارجی در شبکه داخلی

www.takbook.com

www.takbook.com

فصل شانزدهم

VMware Horizon

VMware Horizon یک پلتفرم جامع برای مجازی‌سازی دسکتاپ‌ها و برنامه‌ها است که به شرکت‌ها و سازمان‌ها امکان می‌دهد دسترسی به دسکتاپ‌های مجازی و برنامه‌ها را برای کاربران فراهم کنند. این سیستم از راه دور روی دستگاه‌های مختلف (کامپیوتر، لپ‌تاپ، تبلت و موبایل) قابل استفاده است. با Horizon، کاربران می‌توانند به دسکتاپ‌ها و برنامه‌های ویندوزی و دیگر سیستم‌عامل‌ها از هر کجا دسترسی داشته باشند.

ویژگی‌های کلیدی VMware Horizon:

- دسکتاپ‌های مجازی (VDI): Horizon به کاربران امکان می‌دهد دسکتاپ‌های مجازی ویندوز و لینوکس را در محیط‌های محلی یا ابری اجرا کنند. این ویژگی به کاربران اجازه می‌دهد که از دستگاه‌های خود به دسکتاپ‌های سازمانی دسترسی داشته باشند.
- مجازی‌سازی برنامه‌ها: به جای نصب برنامه‌ها روی هر دستگاه، VMware Horizon می‌تواند برنامه‌ها را به صورت مجازی به کاربران ارائه دهد. کاربران به این برنامه‌ها از طریق یک رابط وب یا یک کلاینت خاص دسترسی پیدا می‌کنند.
- مدیریت متمرکز: Horizon مدیریت دسکتاپ‌ها و برنامه‌های مجازی را از یک مکان مرکزی ساده می‌کند. این موضوع به سازمان‌ها کمک می‌کند تا به‌روزرسانی‌ها، پچ‌ها و مدیریت امنیتی را به طور موثرتر انجام دهند.
- امنیت بالا: VMware Horizon از پروتکل‌های امنیتی پیشرفته و رمزنگاری برای محافظت از داده‌ها و دسترسی کاربران استفاده می‌کند. این موضوع برای سازمان‌هایی که نیاز به رعایت استانداردهای امنیتی بالایی دارند، بسیار مهم است.
- دسترسی چند دستگاهی: با Horizon، کاربران می‌توانند از دستگاه‌های مختلفی مانند لپ‌تاپ، کامپیوتر شخصی، تبلت یا گوشی‌های هوشمند به دسکتاپ‌ها و برنامه‌های مجازی خود دسترسی پیدا کنند.
- قابلیت‌های گرافیکی پیشرفته: این پلتفرم از کارت‌های گرافیکی مجازی و تکنولوژی‌هایی مانند NVIDIA GRID پشتیبانی می‌کند تا عملکرد گرافیکی بالا برای برنامه‌های سنگین (مانند CAD و طراحی گرافیکی) فراهم شود.

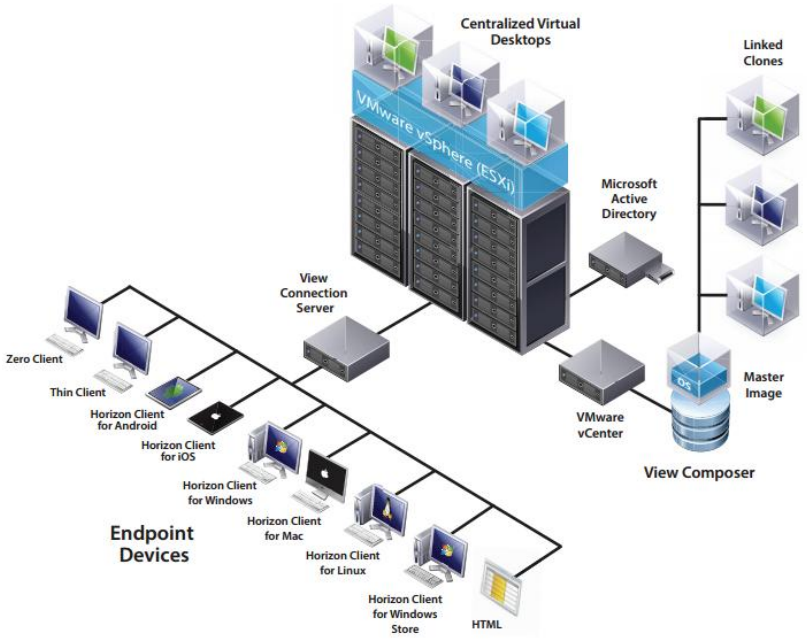
www.takbook.com

- یکپارچگی با سایر محصولات VMware: VMware Horizon به خوبی با سایر محصولات VMware مانند vSphere (پلتفرم مجازی‌سازی سرورها) و vSAN (ذخیره‌سازی مجازی) یکپارچه می‌شود و عملکرد بهتر و مدیریت ساده‌تری را فراهم می‌کند.

مزایای استفاده از VMware Horizon:

- کاهش هزینه‌ها: به دلیل کاهش نیاز به سخت‌افزارهای محلی و تمرکز منابع در دیتا سنترها، هزینه‌های کلی کاهش می‌یابد.
- افزایش انعطاف‌پذیری: کارمندان می‌توانند از هر مکانی و با هر دستگاهی به محیط کاری خود دسترسی داشته باشند.
- افزایش امنیت: داده‌ها در محیط‌های کنترل شده دیتاسنتر باقی می‌مانند و در دستگاه‌های کاربران ذخیره نمی‌شوند.
- مدیریت ساده‌تر: به‌روزرسانی‌ها، پچ‌ها و تغییرات به‌راحتی و به‌صورت متمرکز اعمال می‌شوند.

۱-۱٦ اجزای کلیدی VMware Horizon



شکل ۱۶- ۱ اجزای کلیدی VMware Horizon

www.takbook.com

Connection Server: این سرور نقش اصلی در مدیریت ارتباطات بین کاربران و دسکتاپ‌های مجازی را بر عهده دارد. وظایف آن شامل تأیید اعتبار کاربران، مدیریت نشست‌ها و تخصیص منابع دسکتاپ به کاربران است.

Horizon Client: این نرم‌افزار در دستگاه کاربران نصب می‌شود و به آنها امکان دسترسی به دسکتاپ‌های مجازی و برنامه‌های ارائه‌شده از طریق VMware Horizon را می‌دهد. Horizon Client در سیستم‌عامل‌های مختلفی از جمله Windows، macOS، iOS، Android، و Linux موجود است.

VMware vSphere: زیرساخت مجازی‌سازی که VMware Horizon بر روی آن اجرا می‌شود. vSphere مسئول مدیریت ماشین‌های مجازی است که به عنوان دسکتاپ‌های مجازی یا سرورهای برنامه عمل می‌کنند.

ESXi: هایپروایزر که ماشین‌های مجازی را روی سرورها اجرا می‌کند.

vCenter Server: برای مدیریت متمرکز زیرساخت مجازی از جمله ماشین‌های مجازی، ذخیره‌سازی، و شبکه کاربرد دارد.

Horizon Agent: این نرم‌افزار در دسکتاپ‌های مجازی و سرورهایی که برنامه‌ها روی آنها اجرا می‌شوند نصب می‌شود. Horizon Agent ارتباط بین Connection Server و Horizon Client را برقرار می‌کند و از ویژگی‌هایی مانند ریموت دسکتاپ پشتیبانی می‌کند.

Composer Server (اختیاری): View Composer سروری است که برای ایجاد و مدیریت دسکتاپ‌های مجازی Linked Clone استفاده می‌شود. با استفاده از Composer، شما می‌توانید دسکتاپ‌های مجازی را به صورت کارآمدتری مدیریت کنید و فضای ذخیره‌سازی را بهینه‌سازی کنید.

Instant Clones: این ویژگی به VMware Horizon امکان می‌دهد که دسکتاپ‌های مجازی جدید را به سرعت و با استفاده از یک تصویر پایه (Base Image) ایجاد کند. دسکتاپ‌های Instant Clone سریع‌تر از دسکتاپ‌های Linked Clone تولید می‌شوند و برای سازمان‌هایی که به مقیاس‌پذیری بالا نیاز دارند، ایده‌آل هستند.

Horizon Administrator Console: این کنسول مدیریتی یک رابط وب برای مدیریت و نظارت بر زیرساخت Horizon ارائه می‌دهد. مدیران می‌توانند از طریق این کنسول کاربران، دسکتاپ‌ها، برنامه‌ها و منابع مجازی را مدیریت کنند.

www.takbook.com

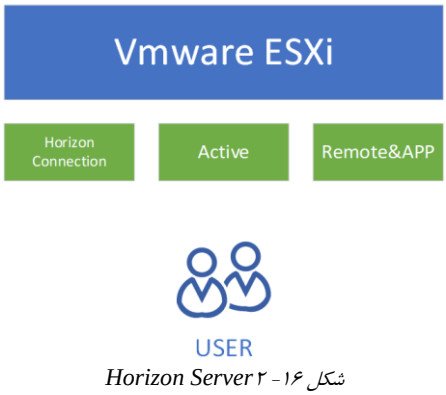
Unified Access Gateway (UAG): این دروازه امنیتی به کاربران امکان می‌دهد که از طریق اینترنت و بدون نیاز به VPN به دسکتاپ‌ها و برنامه‌های Horizon دسترسی پیدا کنند. UAG امنیت دسترسی را تضمین می‌کند و از پروتکل‌های امنیتی پیشرفته برای رمزنگاری ارتباطات استفاده می‌کند.

App Volumes: یک راهکار مدیریت برنامه‌ها که به سازمان‌ها اجازه می‌دهد برنامه‌ها را به‌صورت جداگانه از دسکتاپ‌ها مدیریت و توزیع کنند. این باعث می‌شود که برنامه‌ها بدون نیاز به نصب مجدد روی دسکتاپ‌ها قابل استفاده باشند و مدیریت و به‌روزرسانی آنها به سرعت انجام شود.

۲-۱٦ نصب و راه‌اندازی سرور Horizon Connection Server

برای شروع کار می‌خواهیم اولین سرور و اصلی‌ترین سرور یعنی Horizon Connection Server بر روی شبکه خود نصب کنیم و تست اولیه را انجام دهیم.

در شکل ۱٦-۲، یک سرور ESXi را مشاهده می‌کنید که بر روی آن یک سرور Active، یک سرور Horizon Connection و یک سرور Remote&APP قرار دارد که باید هر سه آنها را ایجاد کنیم، چون در فصل‌های قبلی کتاب سرور Active را ایجاد کردیم نیاز به ایجاد کردن آن نیست و فقط دو ماشین دیگر را ایجاد می‌کنیم.



شکل ۱۶-۲ *Horizon Server*

سخت‌افزار مورد نیاز برای راه‌اندازی این سرور به مانند جدول ۱٦-۱، است:

جدول ۱۶- ۱ سخت‌افزار مورد نیاز

اجزاء سخت‌افزاری	نیازمندی‌های حداقل	نیازمندی مناسب
پردازنده	Pentium IV 2.0GHz processor or higher	4 CPUs

www.takbook.com

کارت شبکه	۱۰۰ مگابایت	۱ گیگابایت
حافظه رم برای Windows Server 2008 R2 64-bit	٤ گیگ و بالاتر	بیشتر از ۱۰ گیگ برای پیاده‌سازی ۵۰ دسکتاپ
حافظه رم برای Windows Server 2025 R2 64-bit	8 گیگ و بالاتر	بیشتر از ۱۰ گیگ برای پیاده‌سازی ۵۰ دسکتاپ

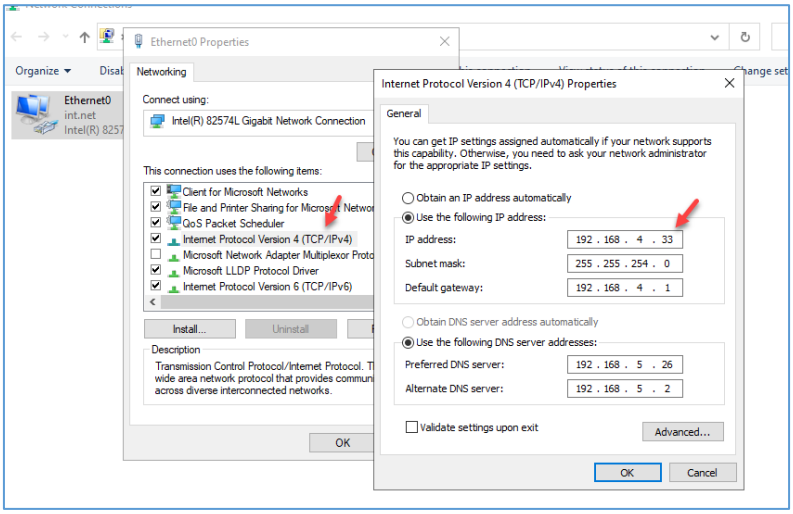
سیستم‌عامل‌هایی که پشتیبانی می‌کند شامل جدول ۱٦-۲، است:

جدول ۱۶- ۲ نرم‌افزار مورد نیاز

سیستم عامل	ورژن	نسخه
Windows Server 2008 R2 SP1	64-bit	StandardEnterpriseDatacenter
Windows Server 2012 R2	64-bit	StandardDatacenter
Windows Server 2016	64-bit	StandardDatacenter
Windows Server 2019	64-bit	StandardDatacenter
Windows Server 2025	64-bit	StandardDatacenter

اول از همه سرور Horizon Connection را راه‌اندای می‌کنیم، برای انجام این کار یک ماشین مجازی بر روی سرور ESXi راه‌اندازی می‌کنیم و ویندوز سرور آن را ورژن 2025 در نظر می‌گیریم و تنظیمات مربوط به IP و نام را به صورت زیر انجام می‌دهیم.

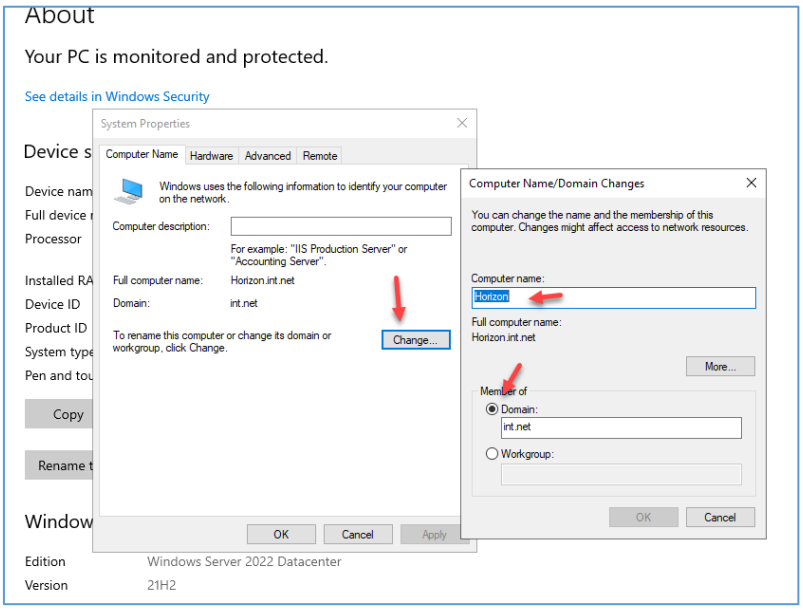
به مانند شکل ۱٦-۳، باید IP سرور Horizon Connection را باید به صورت دستی وارد کنیم که به صورت زیر وارد می‌کنیم، پس آدرس 192.168.4.33 را برای آن در نظر می‌گیریم.



شکل ۱۶- ۳ تغییر IP Address

www.takbook.com

در ادامه به مانند شکل ۱٦-٤، نام سرور را به Horizon تغییر می‌دهیم و آن را عضو دومین خود می‌کنیم.



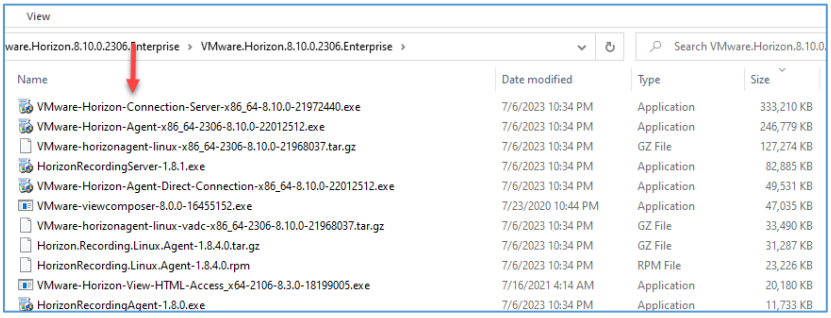
شکل ۱۶- ۴ تغییر نام سرور

بعد از اینکه ماشین را اجرا و IP و نام آن را تغییر دادید و عضو دومین مورد نظر خود کردید باید از لینک زیر آخرین ورژن VMware Horizon View را دانلود کنید:

https://soft98.ir/internet/network/2104-vmware-horizon.html

بعد از دانلود، به مانند شکل ۱٦-٥، پوشه نرم‌افزار را در سرور Horizon که با هم راه انداختیم باز کنید و بر روی VMware Horizon Connection Server دو بار کلیک کنید.

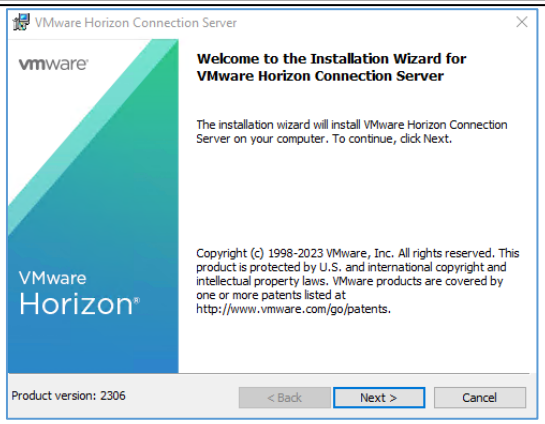
توجه داشته باشید، کاربر دومینی که با آن در حال نصب VMware Horizon هستید باید دسترسی کامل به شبکه داشته باشد.



شکل ۱۶- ۵ نصب و راه‌اندازی Horizon Connection

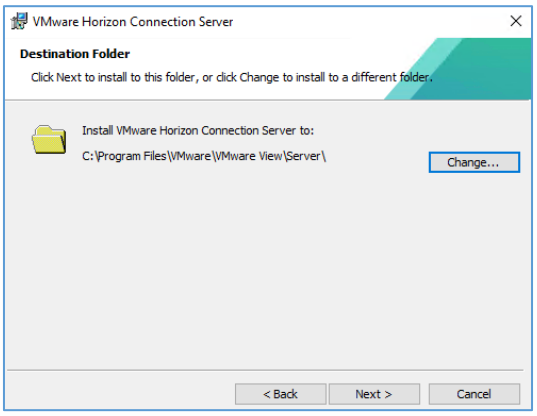
در شکل ۱٦-٦، بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۶- ۶ نصب و راه‌اندازی Horizon Connection

در شکل ۱۶-۷، مسیر نصب نرم‌افزار را مشخص کنید.

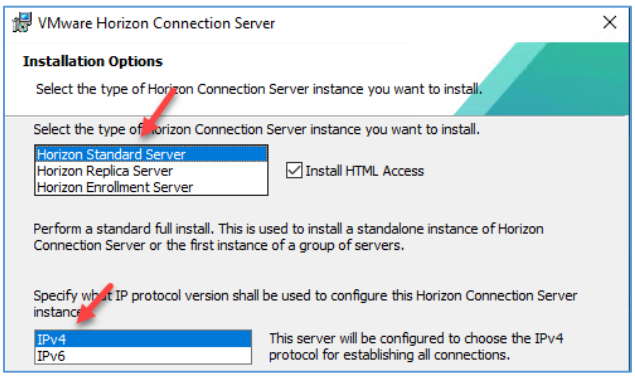


شکل ۱۶- ۷ نصب و راه‌اندازی Horizon Connection

در شکل ۱۶-۸، سه گزینه وجود دارد که گزینه‌ی اول که Standrad است و باید همین گزینه را انتخاب کنید، اما در مورد Horizon Replica Server در VMware Horizon، یکی از اجزای کلیدی برای ایجاد افزونگی (Redundancy) و تحمل‌پذیری خطا در محیط‌های مجازی‌سازی دسکتاپ (VDI) است. این سرور برای گسترش عملکرد و قابلیت اطمینان Connection Server به کار می‌رود و به عنوان یک کپی (Replica) از Horizon Connection Server اصلی عمل می‌کند و همچنین در Horizon Enrollment Server یک مؤلفه حیاتی برای پیاده‌سازی True SSO (Single Sign-On واقعی) است. True SSO به کاربران اجازه می‌دهد بدون نیاز به وارد کردن چندباره رمز عبور، به دسکتاپ‌ها و برنامه‌های مجازی متصل شوند. Enrollment Server به طور خاص برای مدیریت صدور گواهی‌های دیجیتال مورد نیاز برای احراز هویت کاربران استفاده می‌شود.

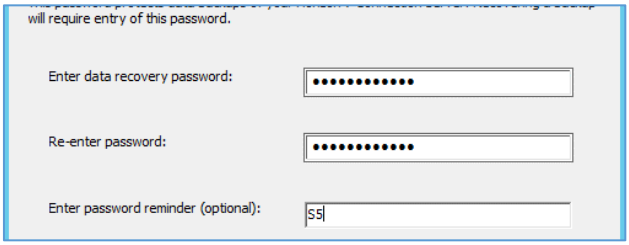
www.takbook.com

همچنین پروتکل IPv4 را انتخاب و بر روی Next کلیک کنید.



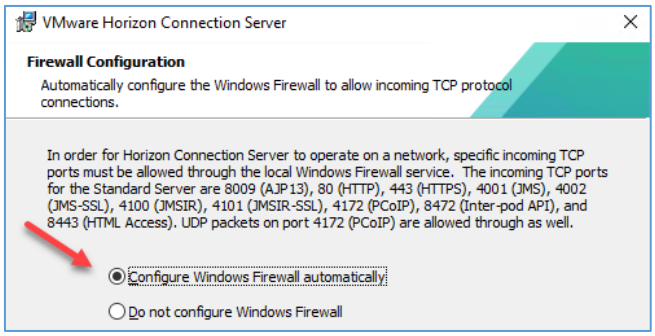
شکل ۱۶- ۸ نصب و راه‌اندازی Horizon Connection

در شکل ۱٦-۹، باید یک رمز عبور پیچیده برای حالت Recovery وارد کنید تا در موقع نیاز از آن استفاده کنیم.



شکل ۱۶- ۹ نصب و راه‌اندازی Horizon Connection

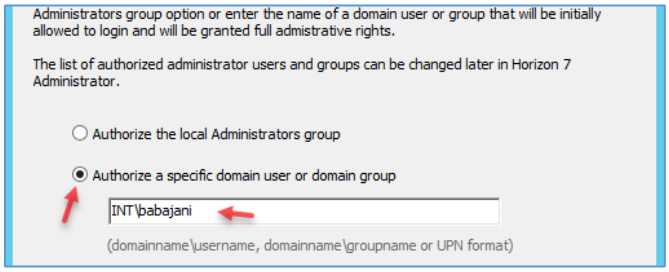
در ادامه کار برای اینکه تمام پورت‌ها به صورت اتوماتیک در سرویس فایروال ویندوز سرور Set شود به مانند شکل ۱٦-۱۰، گزینه‌ی اول را انتخاب و بر روی Next کلیک کنید.



شکل ۱۶- ۱۰ نصب و راه‌اندازی Horizon Connection

www.takbook.com

در شکل ۱٦-۱۱، باید یک نام کاربری که در شبکه دومین شما دسترسی کامل به گروه‌های حساس که قبلاً بررسی کردیم را دارد وارد کنید که بعد از نصب هم با همین کاربر باید وارد سرور شویم.



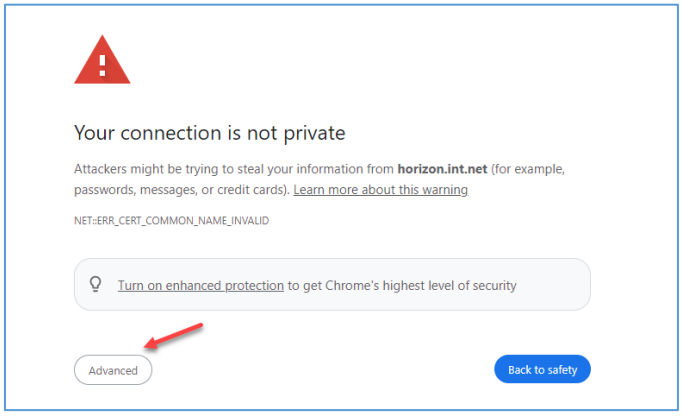
شکل ۱۶- ۱۱ نصب و راه‌اندازی *Horizon Connection*

بعد از نصب می‌توانید از طریق آدرس زیر به صفحه‌ی مدیریتی از طریق وب متصل شوید، هم از IP می‌توانید استفاده کنید و هم از نام:

https://horizon.int.net/admin/

https://192.168.4.33/admin

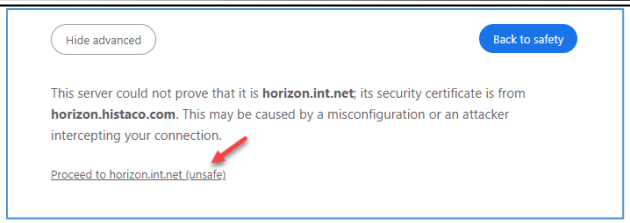
چون صفحه مورد نظر دارای SSL اصلی نیست با خطای شکل ۱٦-۱۲، روبرو خواهید شد که باید بر روی Advanced کلیک کنید.



شکل ۱۶- ۱۲ نصب و راه‌اندازی *Horizon Connection*

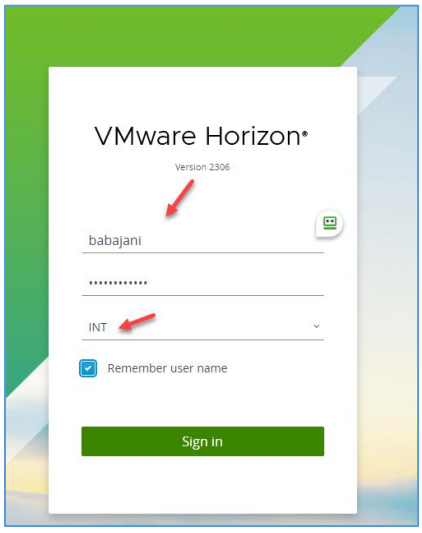
در شکل ۱٦-۱۳، بر روی Proceed to horizon.int.net (unsafe) کلیک کنید تا صفحه‌ی اصلی باز شود، توجه داشته باشید در مورد گواهینامه SSL و نحوه‌ی دیافت آن از سایت‌های خارجی صحبت خواهیم کرد.

www.takbook.com



شکل ۱۶- ۱۳ نصب و راه‌اندازی *Horizon Connection*

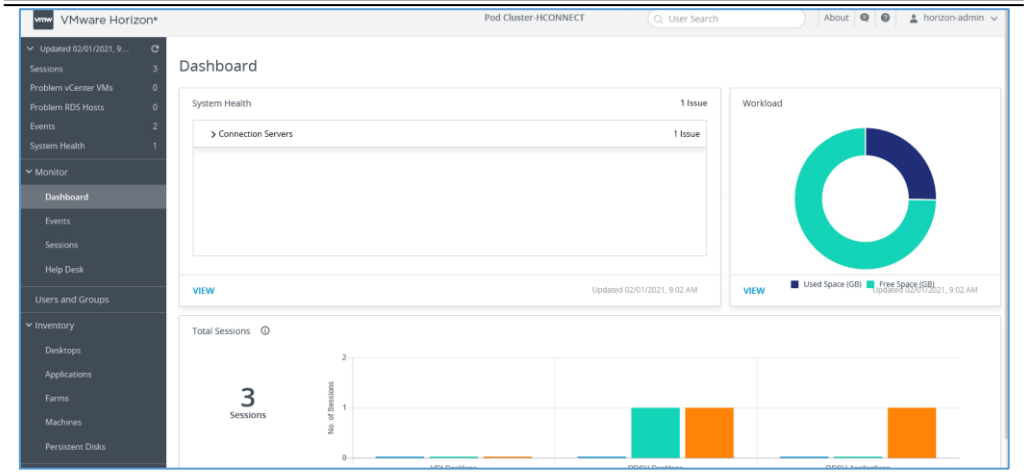
همان‌طور که در شکل ١٦-١٤، مشاهده می‌کنید صفحه‌ی مورد نظر باز شده است و باید نام کاربری دومین خود را که در هنگام نصب وارد کردید را وارد و بر روی Sign in کلیک کنید.



شکل ۱۶- ۱۴ نصب و راه‌اندازی *Horizon Connection*

همان‌طور که در شکل ١٦-١٥، مشاهده می‌کنید صفحه اصلی نرم‌افزار برای ما ظاهر شده است و باید تنظیمات اولیه آن را انجام دهیم.

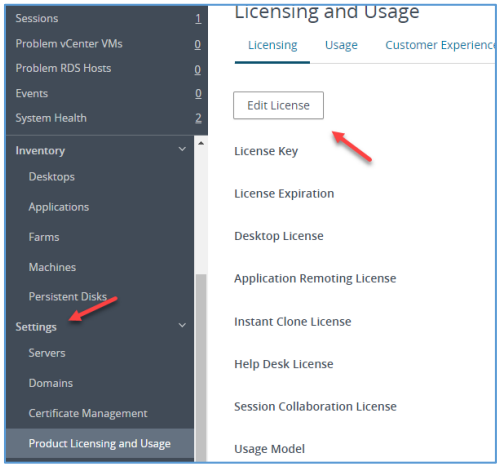
www.takbook.com



شکل ۱۶- ۱۵ نصب و راه‌اندازی *Horizon Connection*

۱۶-۳ تعریف لایسنس در Horizon Connection

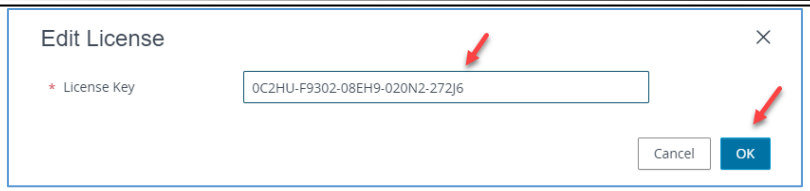
بعد از ورود به صفحه‌ی مدیریتی باید لایسنس نرم‌افزار را تعریف کنیم، به مانند شکل ۱۶-۱۶، برای این کار از قسمت Settings وارد Product Licensing and Usage شوید و بر روی Edit License کلیک کنید.



شکل ۱۶- ۱۶ نصب و راه‌اندازی *Horizon Connection*

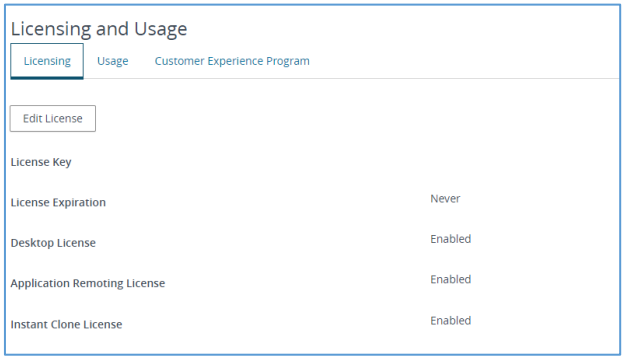
در شکل ۱۶-۱۷، باید لایسنس نرم‌افزار را وارد کنید و بر روی OK کلیک کنید.

www.takbook.com



شکل ۱۶ - ۱۷ نصب و راه‌اندازی Horizon Connection

همان‌طور که در شکل ۱۶–۱۸، مشاهده می‌کنید لایسنس مورد نظر فعال شده است و نرم‌افزار آماده کار است.



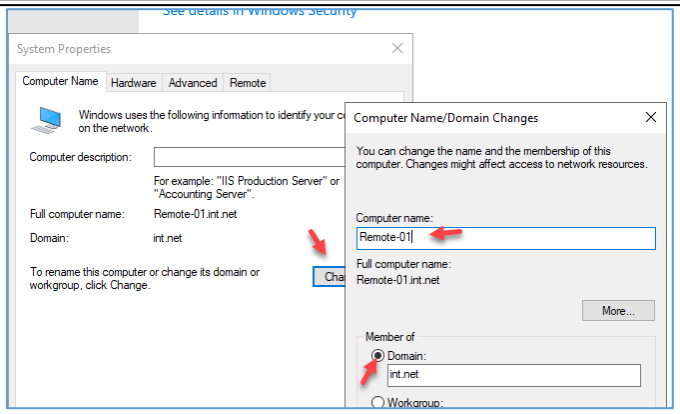
شکل ۱۶ - ۱۸ نصب و راه‌اندازی Horizon Connection

۱۶–۴ ایجاد ماشین مجازی برای سرویس Remote

بعد از اینکه تنظیمات اولیه را انجام دادیم می‌خواهیم بر روی همان سرور ESXi یک سرور جدید راه‌اندازی کنیم که کار این سرور این است که کاربران بتوانند به آن Remote بزنن و نرم‌افزارها را بتوانیم روی آن اجرا کنند.

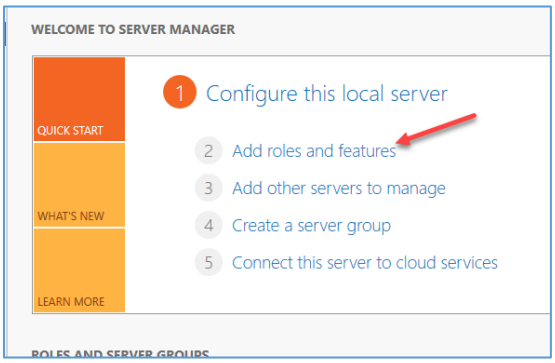
برای این کار یک ماشین مجازی با ویندوز سرور 2025 فعال کردیم که مقدار رم آن را ۱۰ گیگابایت در نظر گرفتیم و بعد از ورود به مانند شکل ۱۶–۱۹، نام آن را به Remote-01 تغییر می‌دهیم و آن را عضو دومین می‌کنیم، نیازی به وارد کردن دستی IP نیست و همان IP از DHCP کافی است هر چند می‌توانید این آدرس را به صورت دستی هم برای این سرور تعریف کنید.

www.takbook.com



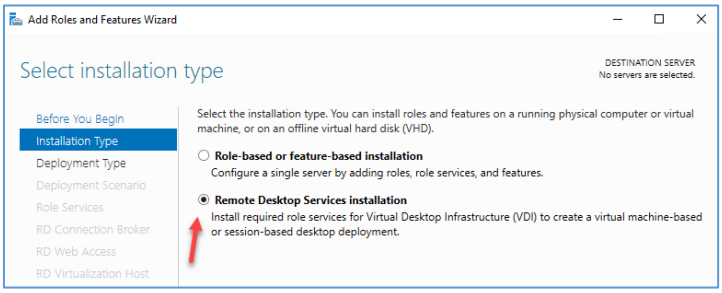
شکل ۱۶- ۱۹ ایجاد ماشین مجازی برای سرویس *Remote*

بعد از اینکه سرور را عضو دومین کردید باید سرویس Remote Desktop را بر روی آن راه‌اندازی کنیم، برای این کار به مانند شکل ۱۶-۲۰، وارد Server Manager شوید و بر روی Add roles and features کلیک کنید.



شکل ۱۶- ۲۰ ایجاد ماشین مجازی برای سرویس *Remote*

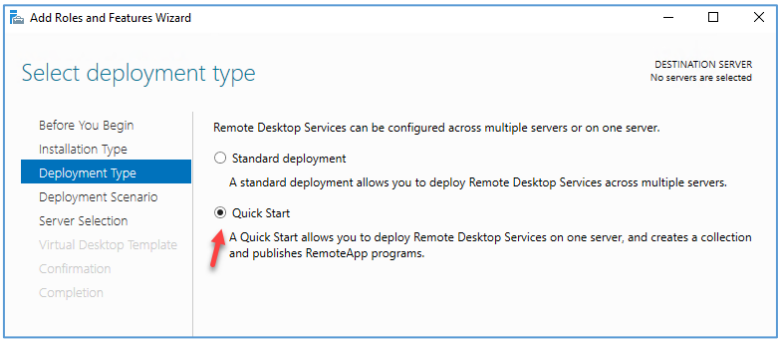
در شکل ۱۶-۲۱، گزینه‌ی Remote Desktop Service Installation را انتخاب کنید.



شکل ۱۶- ۲۱ ایجاد ماشین مجازی برای سرویس *Remote*

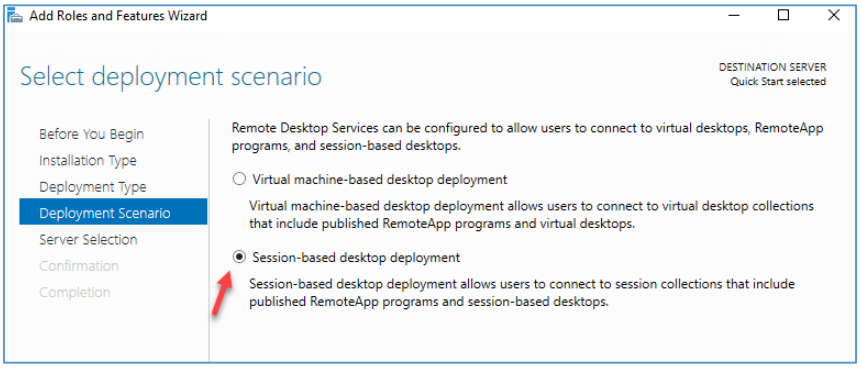
www.takbook.com

در شکل ۱۶-۲۲، برای این‌که کار خود را سریعاً انجام دهیم و درگیر دریافت لایسنس از سایت مایکروسافت نشویم بهتر است گزینه‌ی Quick Start را انتخاب کنید.



شکل ۱۶- ۲۲ ایجاد ماشین مجازی برای سرویس Remote

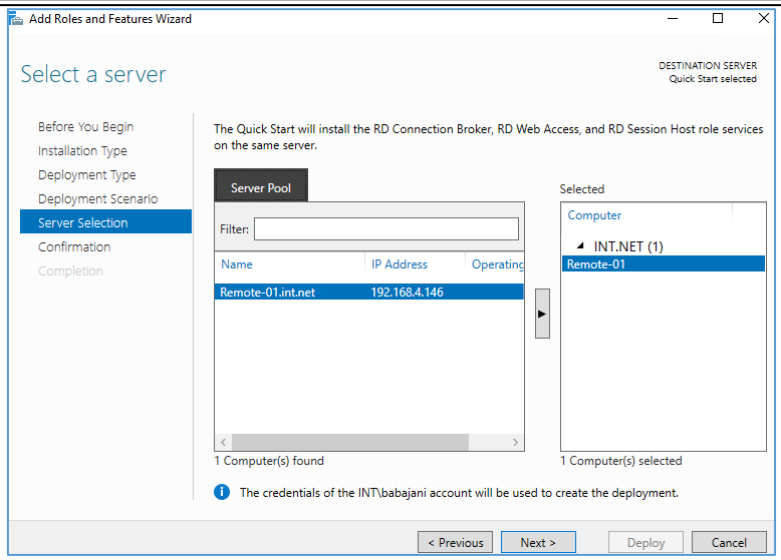
در شکل ۱۶-۲۳، گزینه‌ی Session-based desktop deployment را انتخاب کنید.



شکل ۱۶- ۲۳ ایجاد ماشین مجازی برای سرویس Remote

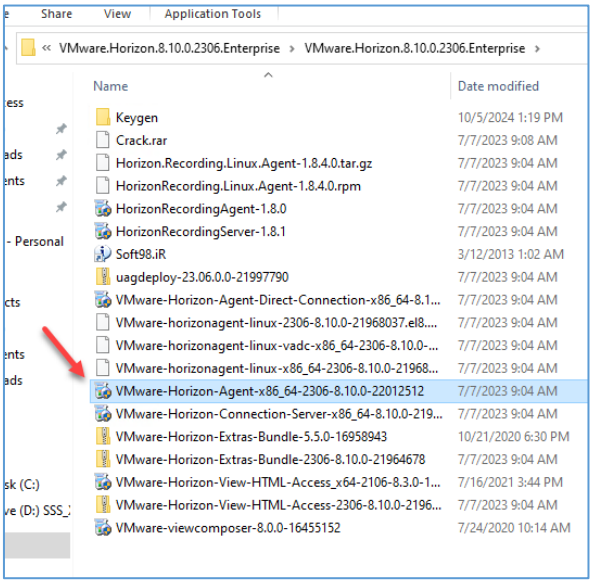
به مانند شکل ۱۶-۲۴، فقط بر روی Next کلیک کنید و در صفحه‌ی بعد بر روی Deploy کلیک کنید تا سرویس مورد نظر نصب شود.

www.takbook.com



شکل ۱۶ - ۲۴ ایجاد ماشین مجازی برای سرویس Remote

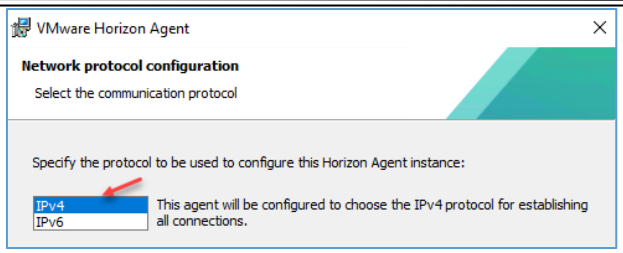
بعد از نصب سرویس باید سرویس Horizon Agent را بر روی این سرور نصب کنیم تا بتوانیم آن را از طریق Horizon Connection مدیریت کنیم، در پوشه نصبی نرم‌افزار، بر روی VMware-Horizon-Agent دوبار کلیک کنید.



شکل ۱۶ - ۲۵ ایجاد ماشین مجازی برای سرویس Remote

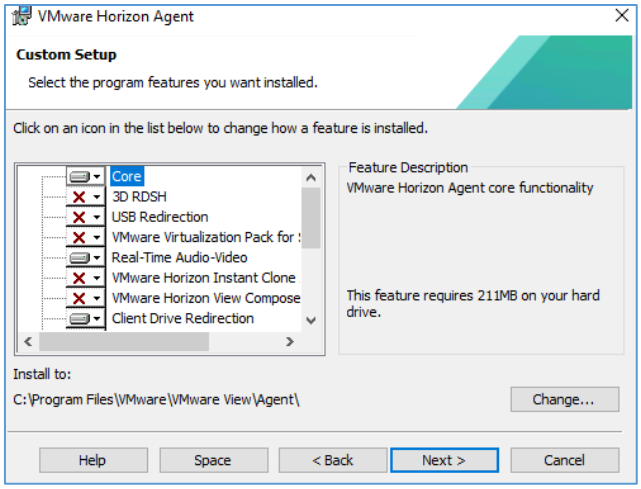
بعد از اجرا به مانند شکل ۱۶-۲۶، پروتکل IPv4 را انتخاب کنید.

www.takbook.com



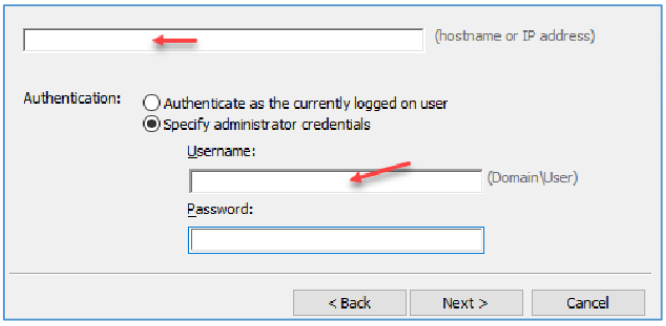
شکل ۱۶- ۲۶ ایجاد ماشین مجازی برای سرویس Remote

در شکل ۱۶-۲۷، می‌توانید مسیر نصب خود را تغییر دهید.



شکل ۱۶- ۲۷ ایجاد ماشین مجازی برای سرویس Remote

در شکل ۱۶-۲۸، باید آدرس سرور Horizon Connection که آدرسش horizon.int.net بود و یا آدرس IP که 192.168.4.33 بود را وارد کنید و در قسمت نام کابری و رمز عبور باید همان نام کاربری که دسترسی کامل به شبکه دارد و با آن Horizon Connection را نصب کردیم را وارد کنید.



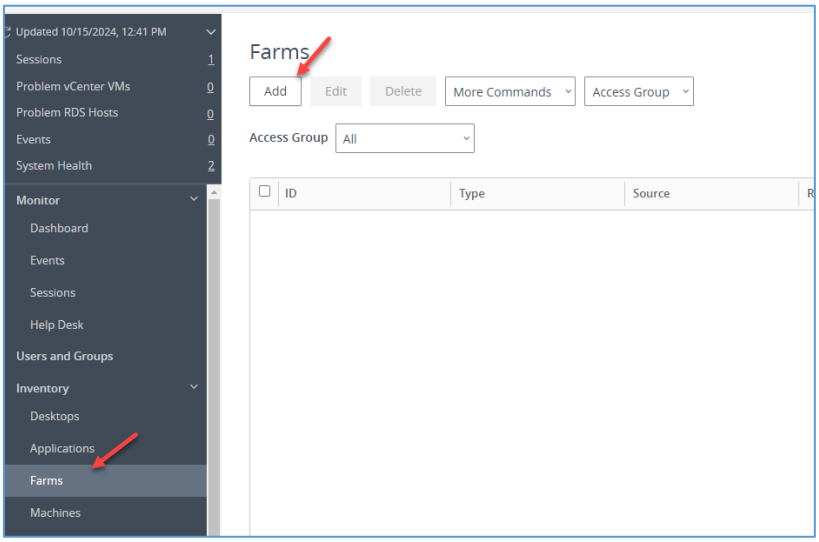
شکل ۱۶- ۲۸ ایجاد ماشین مجازی برای سرویس Remote

www.takbook.com

بعد از نصب Agent سرور را Restart کنید تا تنظیمات اعمال شود، در ادامه کار می‌خواهیم وارد Horizon Connection شویم و این سرور را به آن متصل کنیم.

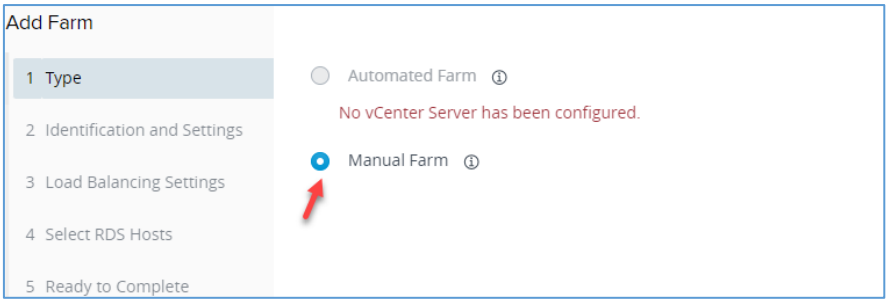
۱۶-۵ ایجاد Farm در Horizon Connection

برای این‌که به منابع شبکه یعنی Desktop و Aplicationها دسترسی داشته باشیم باید Farm ایجاد کنیم، برای این کار به مانند شکل ۱۶-۲۹، از قسمت Inventory بر روی Farms کلیک کنید و در صفحه‌ی باز شده بر روی Add کلیک کنید.



شکل ۱۶- ۲۹ ایجاد Farm در Horizon Connection

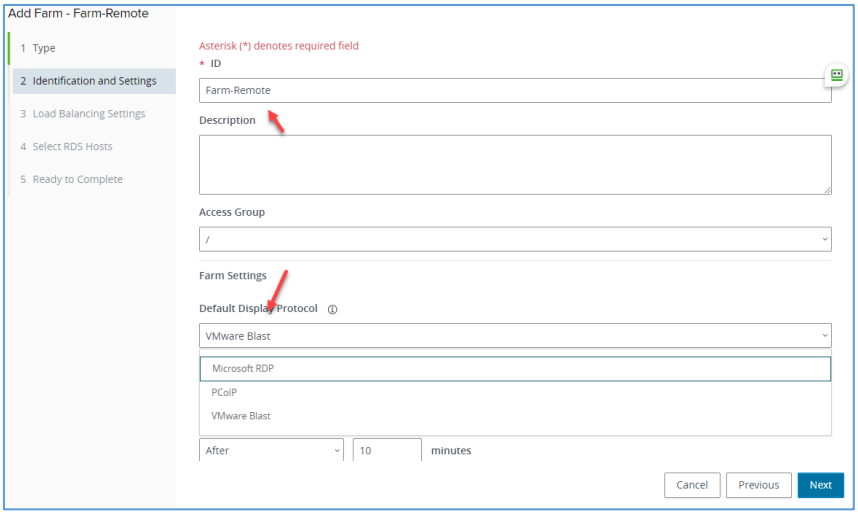
در شکل ۱۶-۳۰، دو گزینه را مشاهده می‌کنید که یکی برای متصل شدن به Vcenter است و دیگری به صورت دستی است که چون در حال حاضر از Vcenter استفاده نکردیم گزینه‌ی دوم یعنی دستی را انتخاب کنید.



شکل ۱۶- ۳۰ ایجاد Farm در Horizon Connection

www.takbook.com

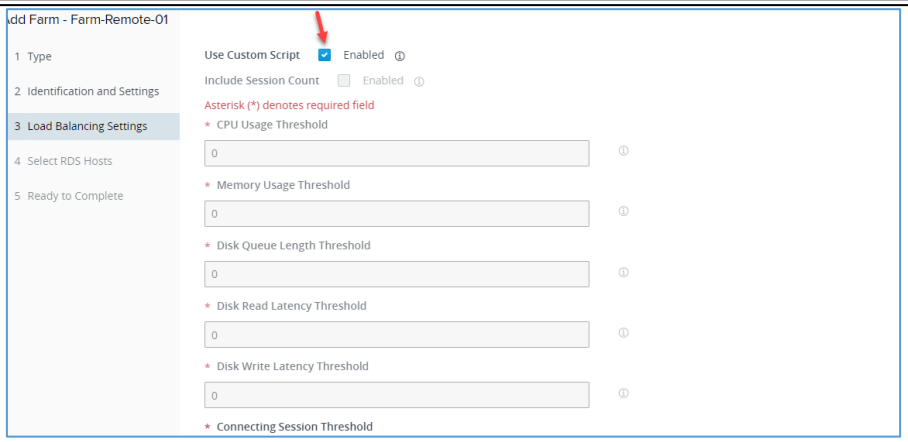
در ادامه کار و در شکل ۱۶-۳۱، یک نام برای Farm خود وارد کنید، تنظیمات دیگری هم وجود دارد نحوه‌ی ارتباط با سرور که بهتر است پروتکل VMware Blast را انتخاب کنید اگر بخواهیم در مورد این پروتکل صحبت کنیم باید بگوییم که VMware Blast یک پروتکل نمایش ریموت است که توسط VMware برای فراهم کردن دسترسی از راه دور به دسکتاپ‌های مجازی (Virtual Desktops) و برنامه‌ها در محیط‌های VDI (Virtual Desktop Infrastructure) استفاده می‌شود. این پروتکل به طور ویژه برای کارایی بهتر و بهبود تجربه کاربر در محیط‌های کاری مجازی طراحی شده است.



شکل ۱۶- ۳۱ ایجاد Farm در Horizon Connection

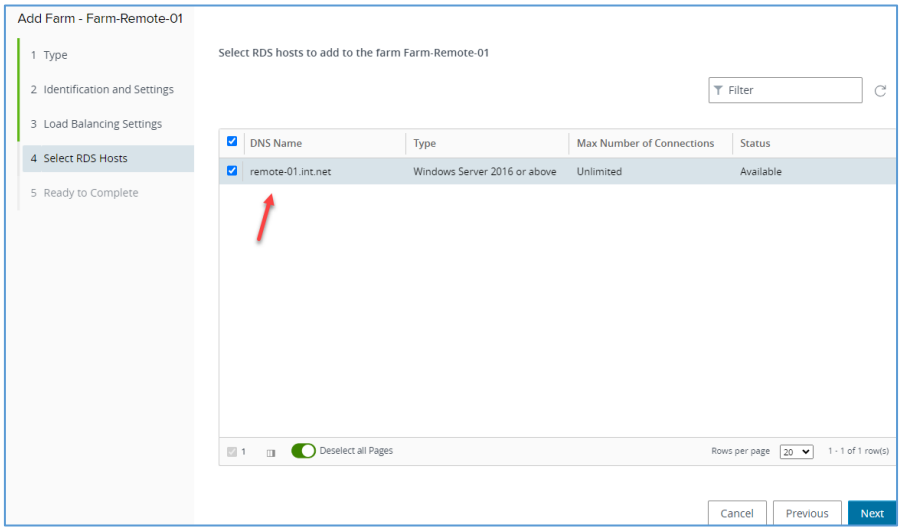
در شکل ۱۶-۳۲، می‌توانید به Farm مورد نظر منابع سخت‌افزاری تخصیص دهید و حد آن را مشخص کنید که در حال حاضر نیازی به این کار نیست تیک گزینه‌ی اول را انتخاب کنید و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۶- ۳۲ ایجاد Farm در Horizon Connection

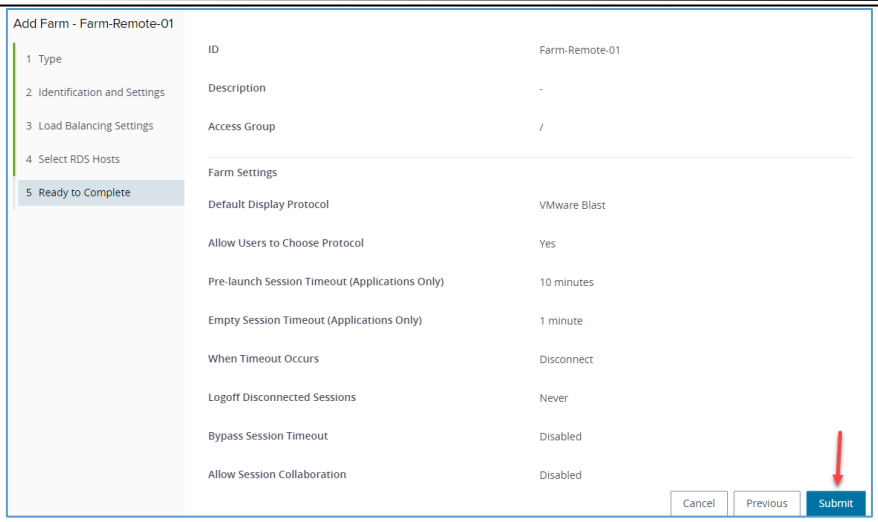
در شکل ۱۶-۳۳، همان سرور Remote-01 که با هم راه‌اندازی کردیم و روی آن سرویس Remote Desktop را فعال کردیم و بعد هم سرویس VMware Agent را نصب کردیم در لیست ما قرار گرفته است که این کار به صورت اتوماتیک انجام می‌شود.



شکل ۱۶- ۳۳ ایجاد Farm در Horizon Connection

در شکل ۱۶-۳٤، اگر تنظیمات مورد تایید شما است بر روی Submit کلیک کنید.

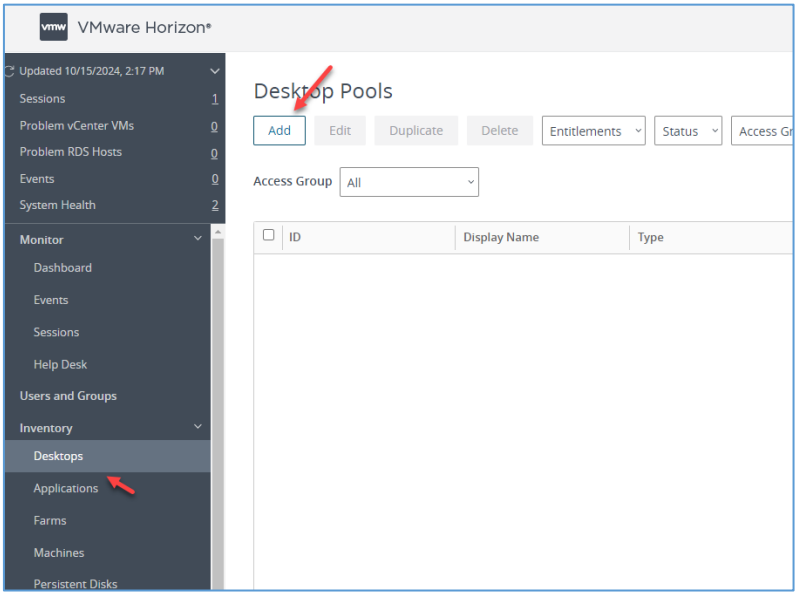
www.takbook.com



شکل ۱۶-۳۴ ایجاد Farm در Horizon Connection

۱۶-۶ ایجاد Desktop Pool

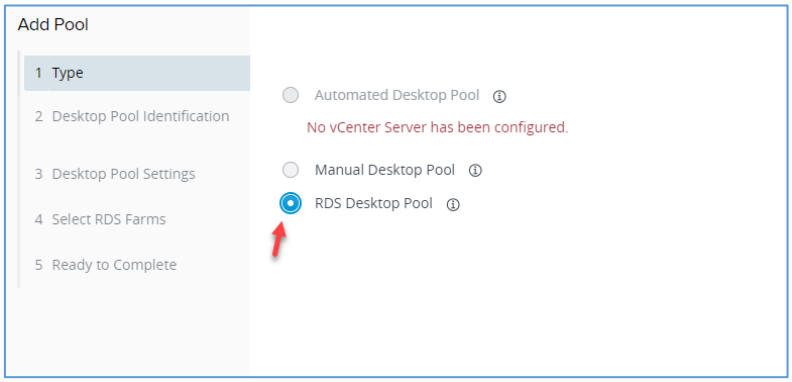
در ادامه و بعد از ایجاد Farm باید یک Desktop Pool ایجاد کنیم، برای این کار طبق شکل ۱۶-۳۵، از سمت چپ بر روی Desktops کلیک کنید و در صفحه‌ی باز شده بر روی Add کلیک کنید.



شکل ۱۶-۳۵ ایجاد Desktop Pool

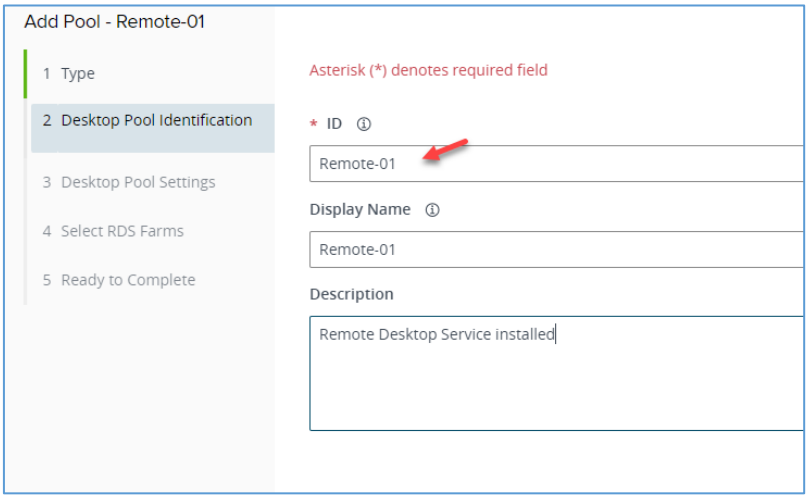
www.takbook.com

دو گزینه‌ی اول در شکل ۱۶-۳۶، نیاز به Vcenter دارند که فعلاً به سرور متصل نکردیم که حال حاضر باید گزینه‌ی RDS را انتخاب کنید.



شکل ۱۶-۳۶ ایجاد Desktop Pool

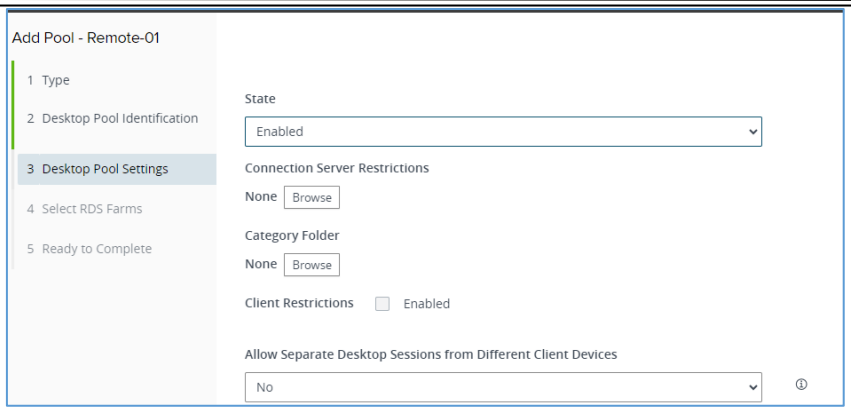
به مانند شکل ۱۶-۳۷، نام Desktop Pool را به همراه توضیحات وارد کنید.



شکل ۱۶-۳۷ ایجاد Desktop Pool

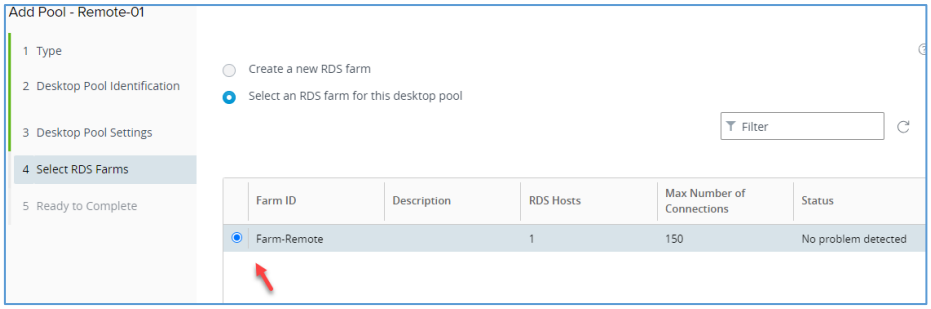
در شکل ۱۶-۳۸، نیاز به تغییری نیست و بر روی Next کلیک کنید.

www.takbook.com



شکل ۱۶- ۳۸ ایجاد *Desktop Pool*

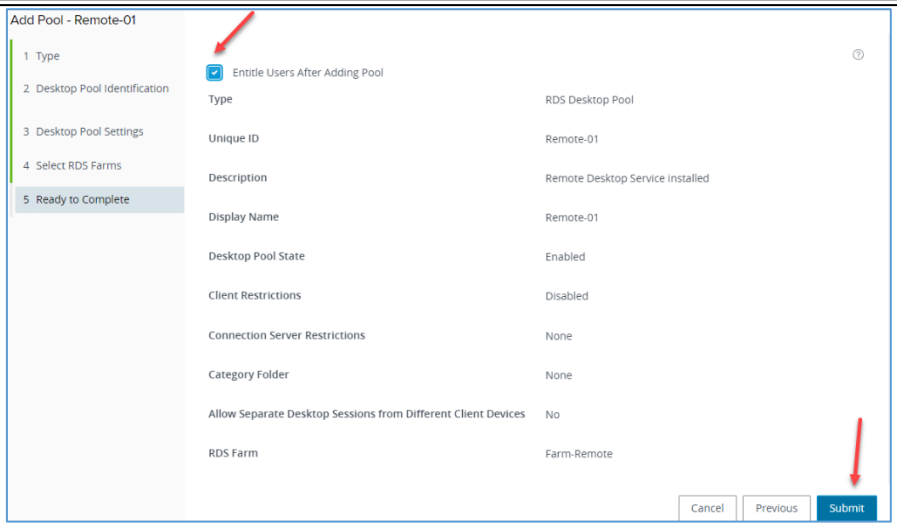
در شکل ۱۶-۳۹، باید Farm مورد نظر که به هم ایجاد کردیم را انتخاب کنید.



شکل ۱۶- ۳۹

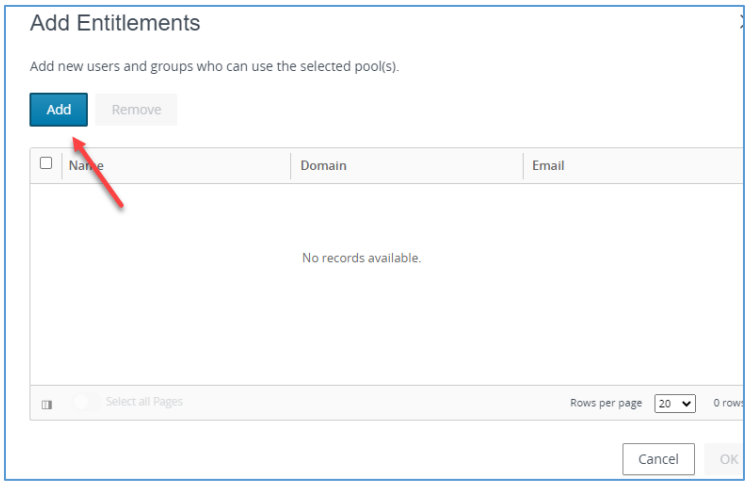
در شکل ۱۶-۴۰، قبل از اینکه بر روی Submit کلیک کنید، برای اینکه به کاربران دسترسی دهیم باید تیک گزینه‌ی Entitle Users After Adding Pool را انتخاب کنید.

www.takbook.com



شکل ۱۶- ۴۰ ایجاد *Desktop Pool*

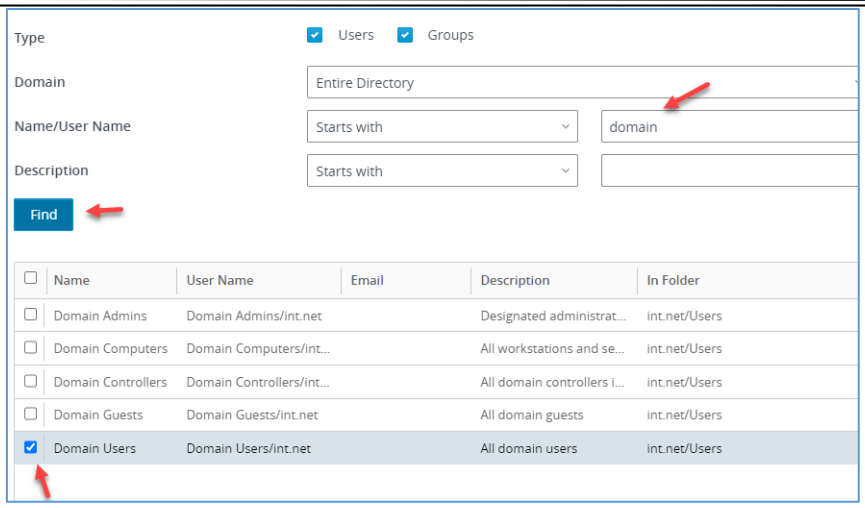
در شکل ۱۶-۴۱، بر روی Add کلیک کنید و کاربر و گروه مورد نظر خود را که قرار است به این Desktop Pool دسترسی داشته باشد را وارد کنید.



شکل ۱۶- ۴۱ ایجاد *Desktop Pool*

همان‌طور که در شکل ۱۶-۴۲، مشاهده می‌کنید گروه Domain Users که همه کاربران عضو آن هستند را انتخاب کردیم، با این کار تمام کاربران به Desktop Pool مورد نظر دسترسی دارند.

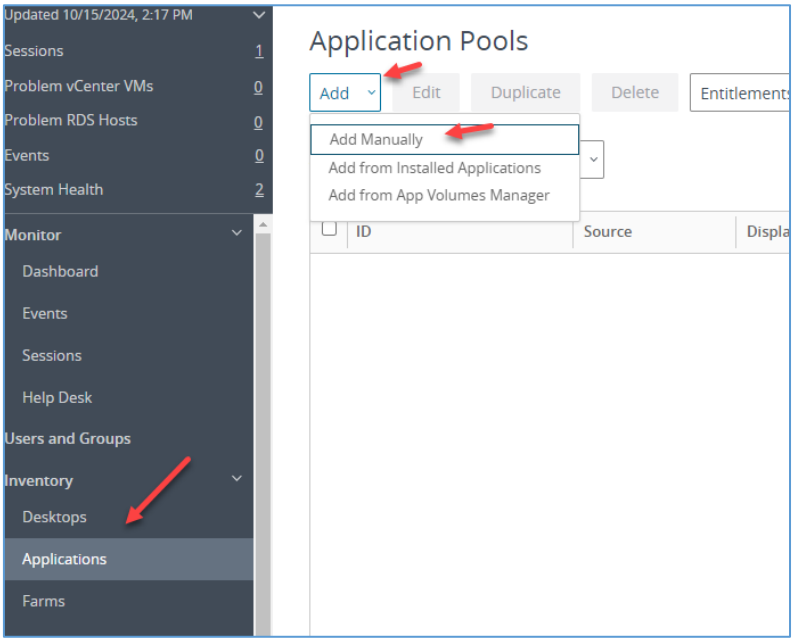
www.takbook.com



شکل ۱۶- ۴۲ ایجاد *Desktop Pool*

۱۶-۷ ایجاد Application Pool

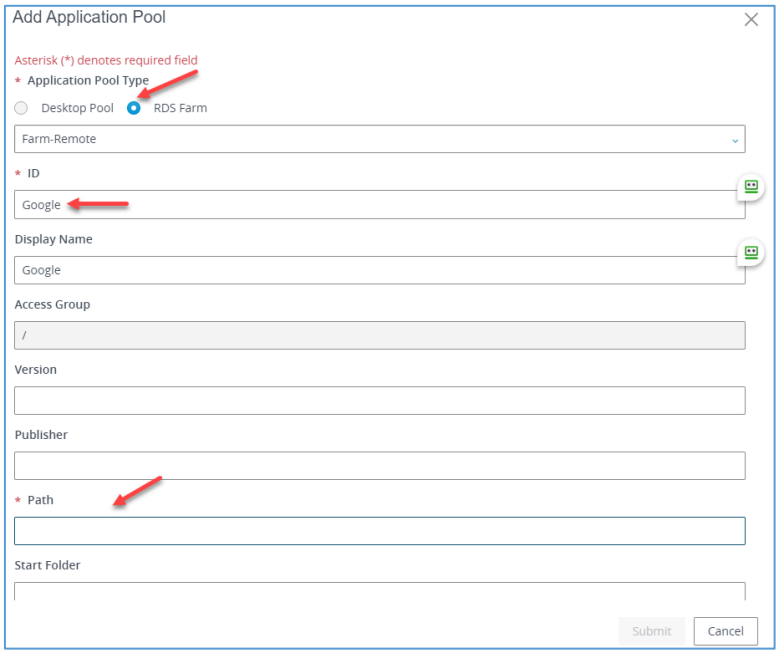
بعد از ایجاد Desktop Pool می‌خواهیم نرم‌افزارها را هم، برای کاربران به اشتراک بگذاریم برای این کار به مانند شکل ۱۶-۴۳، وارد Applications شوید و به مانند شکل بر روی Add کلیک کنید که سه گزینه را مشاهده می‌کنید گزینه‌ی اول یعنی Add Manually را انتخاب کنید.



شکل ۱۶- ۴۳ ایجاد *Application Pool*

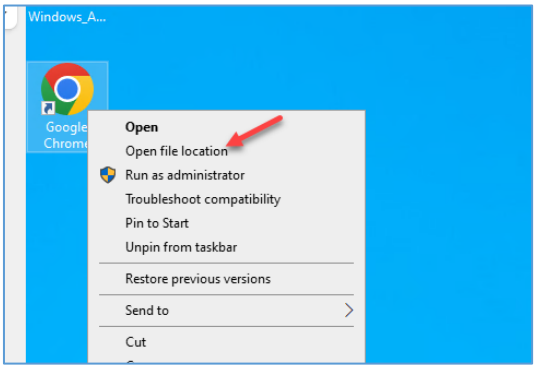
www.takbook.com

در شکل ۱۶-۴۴، باید RDS Farm را انتخاب کنیم و نام برنامه خود را وارد کنید که در اینجا می‌خواهیم Google Chrome را اجرا کنیم نام Google را وارد می‌کنیم و در مهمترین بخش یعنی Path باید آدرس برنامه را وارد کنیم که این آدرس را باید از سرور Remote-01 دریافت کنیم که با هم وارد آن سرور می‌شویم.



شکل ۱۶- ۴۴ / ایجاد Application Pool

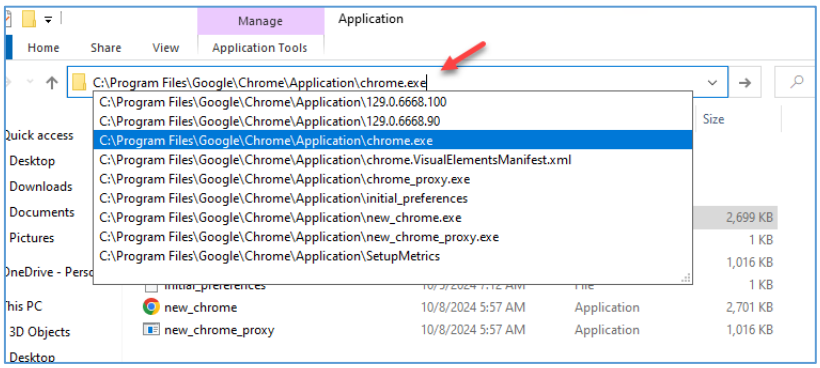
برای بدست آوردن آدرس برنامه مورد نظر وارد سرور Remote-01 می‌شویم و به مانند شکل ۱۶-۴۵، بر روی آیکون Chrome کلیک راست کنید و گزینه‌ی Open file location را انتخاب کنید.



شکل ۱۶- ۴۵ / ایجاد Application Pool

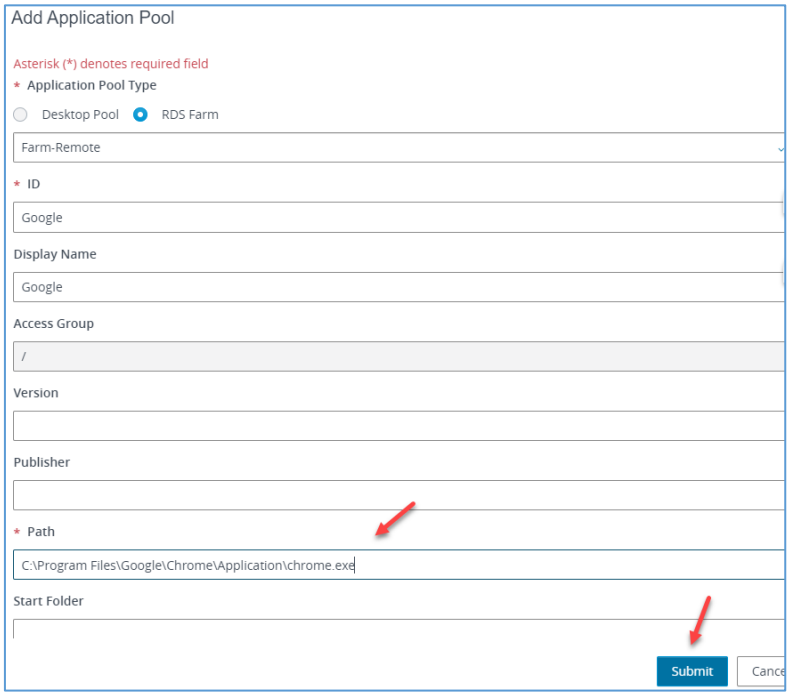
www.takbook.com

آدرس برنامه را به صورت شکل ۱٦-٤٦، کپی بگیرید.



شکل ۱۶ - ۴۶ ایجاد *Application Pool*

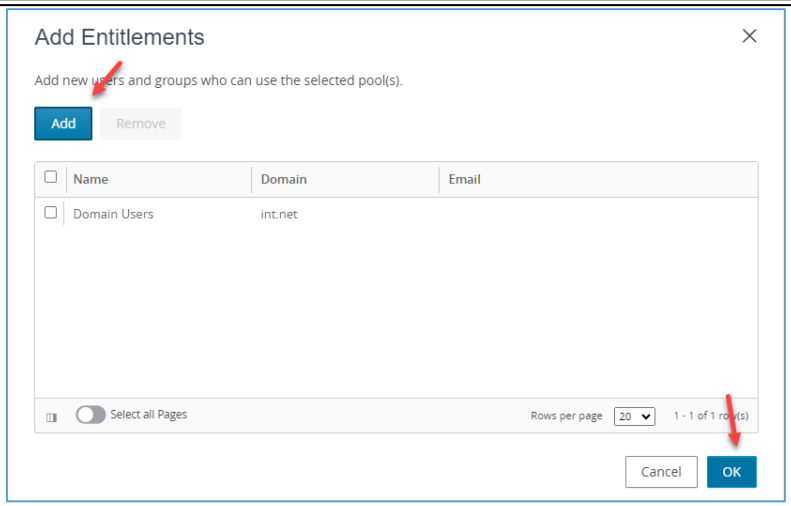
همان‌طور که در شکل ۱٦-٤٧، مشاهده می‌کنید آدرس مورد نظر را به برنامه اضافه کردیم، بر روی Submit کلیک کنید.



شکل ۱۶ - ۴۷ ایجاد *Application Pool*

در شکل ۱٦-٤٨، باید گروه یا کاربر مورد نظر خود را وارد کنید تا به نرم‌افزار مورد نظر دسترسی داشته باشند.

www.takbook.com



شکل ۱۶- ۴۸ ایجاد *Application Pool*

۱۶-۸ کار با VMware Horizon Client Web

بعد از اینکه Desktop Pool و Application Pool را به صورت دستی ایجاد کردیم، برای اینکه کاربران به آن دسترسی داشته باشند دو حالت وجود دارد.

۱- از طریق وب
۲- از طریق نرم‌افزار Horizon Client

برای اینکه از طریق وب به این موارد دسترسی داشته باشیم باید آدرس سرور را به صورت زیر وارد کنیم.

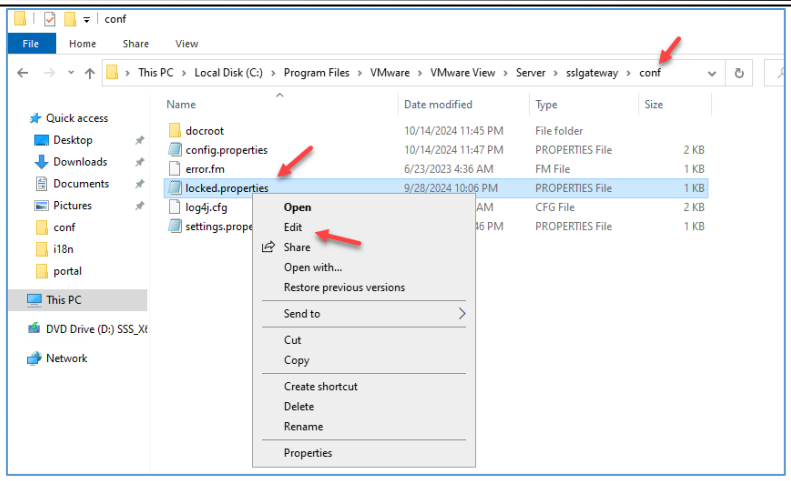
https://horizon.int.net
https://192.168.4.33

قبل از هر کاری برای اینکه با مشکلات HTTPS روبرو نشویم به مانند شکل ۱۶-۴۹، وارد آدرس زیر در سررو Horizon شوید و فایل مورد نظر را با Notpad باز کنید.

C:\Program Files\VMware\VMware View\Server\sslgateway\conf

توجه داشته باشید اگر فایل مورد نظر وجود نداشت آن را ایجاد کنید و نام آن را به همراه پسوند به صورت locked.properties وارد کنید.

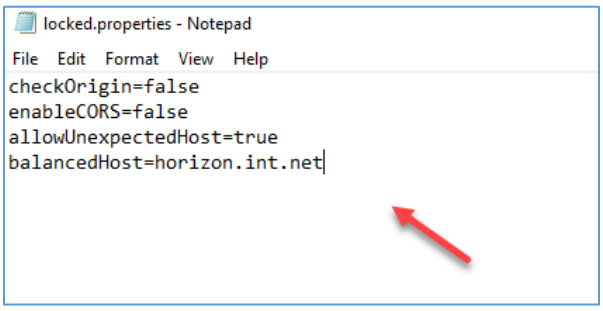
www.takbook.com



شکل ۱۶- ۴۹ کار با *VMware Horizon Client Web*

بعد از باز کردن فایل مورد نظر متن زیر را به مانند شکل ۱۶-۵۰، در آن قرار دهید و فایل مورد نظر را ذخیره کنید.

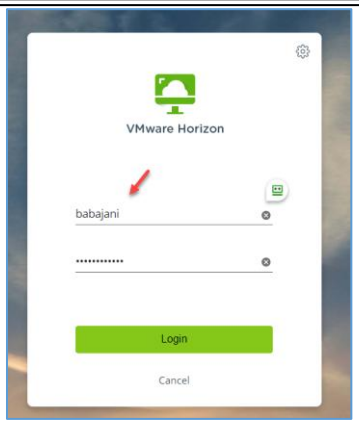
```
checkOrigin=false
enableCORS=false
allowUnexpectedHost=true
balancedHost=horizon.int.net
```



شکل ۱۶- ۵۰ کار با *VMware Horizon Client Web*

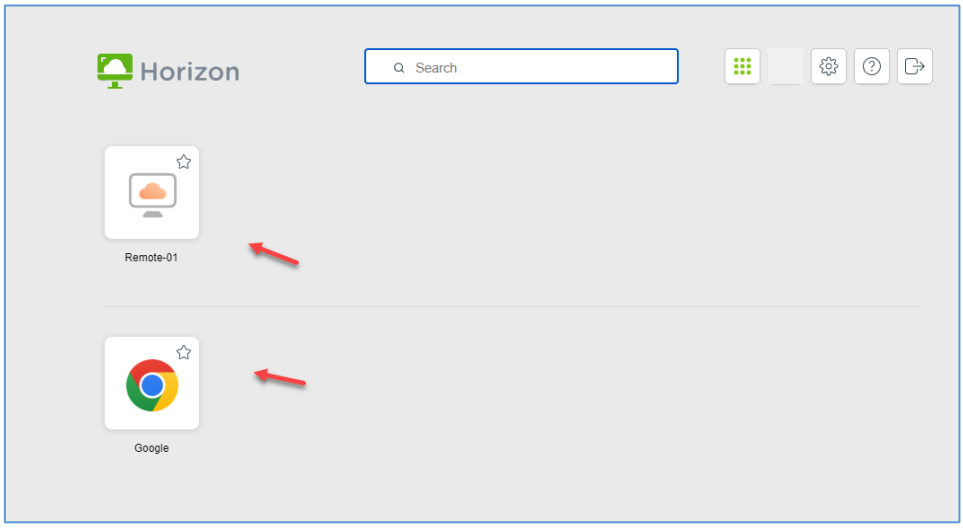
حالا می‌توانیم وارد آدرس سرور تحت وب شویم که شکل ۱۶-۵۱، برای شما نماش داده خواهد شد که باید نام کاربری و رمز عبور دومین خود را وارد کنید.

www.takbook.com



شکل ۱۶- ۵۱ کار با VMware Horizon Client Web

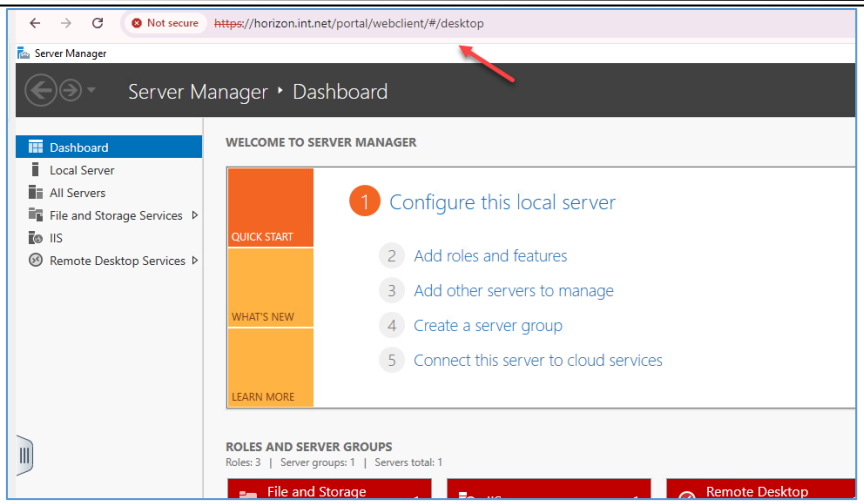
همان‌طور که در شکل ۱۶-۵۲، مشاهده می‌کنید هر دو گزینه‌ی Desktop و Application در لیست ظاهر شده و می‌توانیم از آنها استفاده کنیم، برای تست Remote-01 که سرور مجازی است را انتخاب می‌کنیم و وارد سرور می‌شویم.



شکل ۱۶- ۵۲ کار با VMware Horizon Client Web

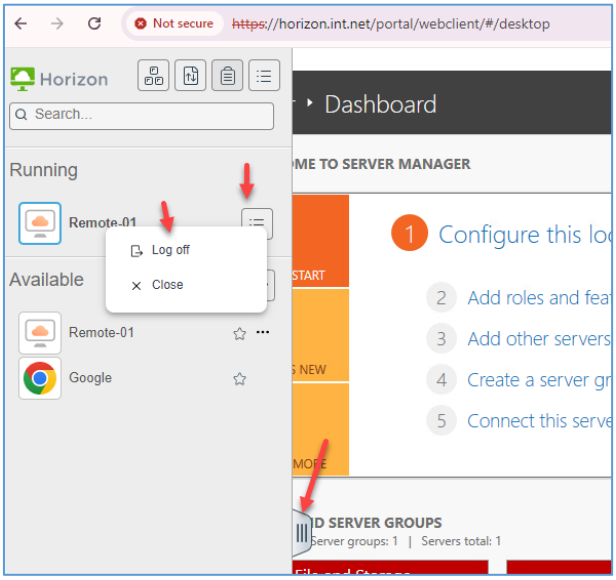
همان‌طور که در شکل ۱۶-۵۳، مشاهده می‌کنید، از طریق وب وارد سرور مورد نظر شدیم.

www.takbook.com



شکل ۱۶-۵۳ کار با *VMware Horizon Client Web*

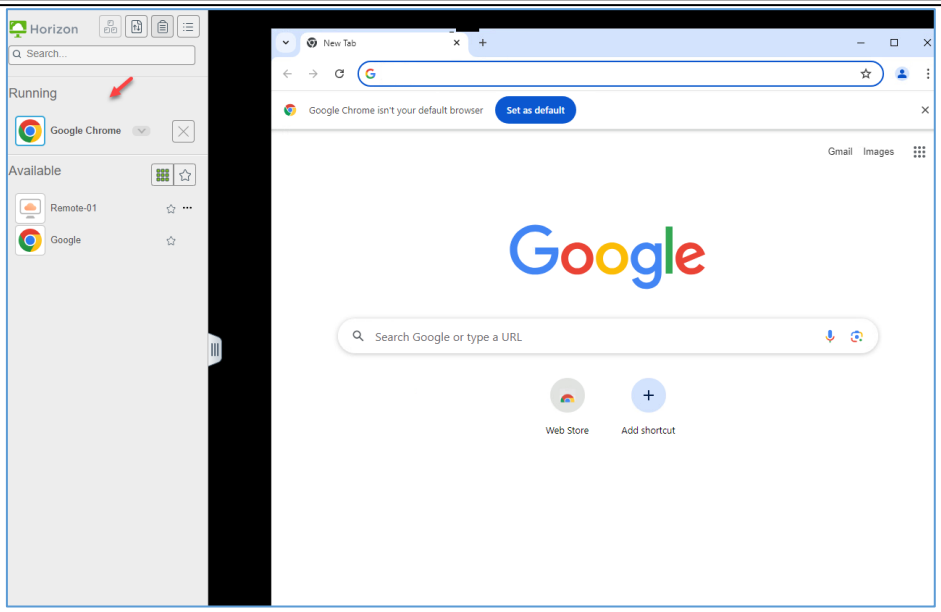
برای خروج از سرور مورد نظر باید به مانند شکل ۱۶-۵۴، منوی کشویی را باز کنید و بر روی آیکون مشخص شده در شکل کلیک کنید و گزینه‌ی Log off را انتخاب کنید تا از سرور خارج شویم.



شکل ۱۶-۵۴ کار با *VMware Horizon Client Web*

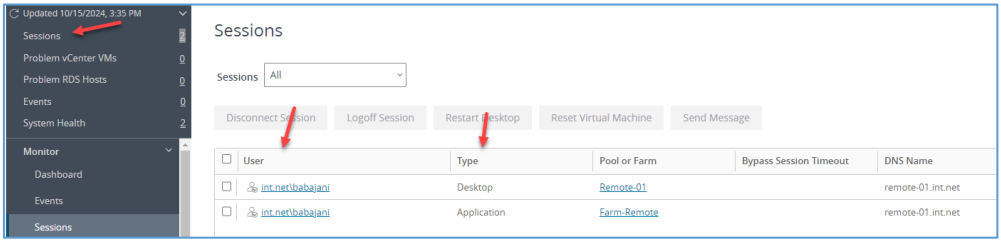
در ادامه طبق شکل ۱۶-۵۵، بر روی Google کلیک کنید تا نرم افزار مورد نظر باز شود، که در شکل این موضوع مشخص شده است.

www.takbook.com



شکل ۱۶- ۵۵ کار با *VMware Horizon Client Web*

بعد از اینکه Desktop و Application را باز کردید اگر طبق شکل ۱۶-۵۶، وارد Admin در Horizon View شوید، اگر به قسمت Sessions مراجعه کنید، متوجه خواهید شد که دو نشست فعال است که توسط کاربر babajani فعال شده و نوع آنها هم مشخص شده است.



شکل ۱۶- ۵۶ کار با *VMware Horizon Client Web*

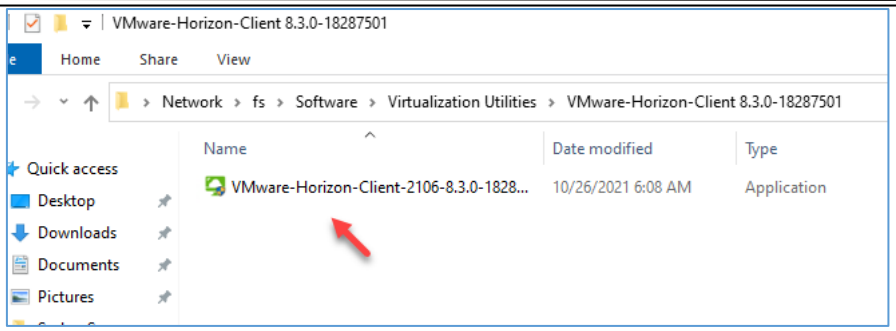
۱۶-۹ کار با Horizon Client Application

از لینک زیر می‌توانید VMware Horizon Client را دانلود کنید:

https://dl2.soft98.ir/soft/u-v/VMware.Horizon.Client.8.10.0.rar?1728994798

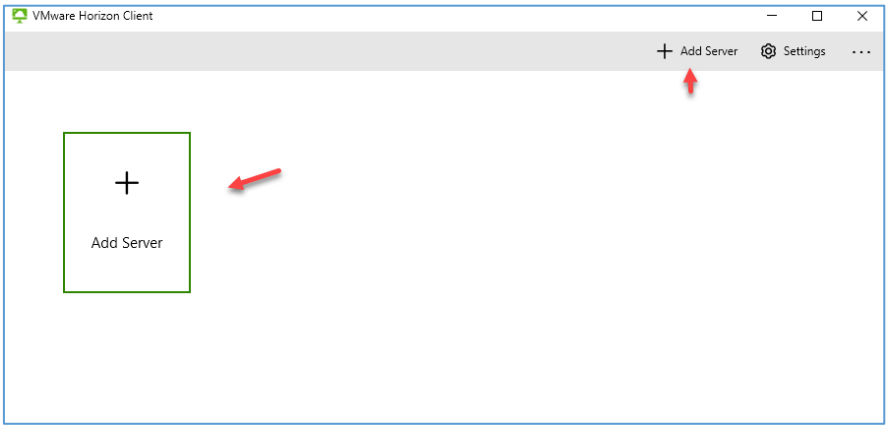
بعد از دانلود به مانند شکل ۱۶-۵۷، فایل را اجرا و برنامه را نصب کنید.

www.takbook.com



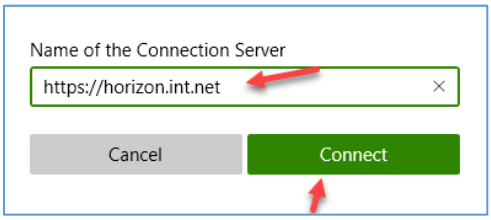
شکل ۱۶-۵۷ *Horizon Client Application*

بعد از نصب نرم‌افزار آن را اجرا کنید و به مانند شکل ۱۶-۵۸، برای اضافه کردن سرور مورد نظر بر روی Add Server کلیک کنید.



شکل ۱۶-۵۸ *Horizon Client Application*

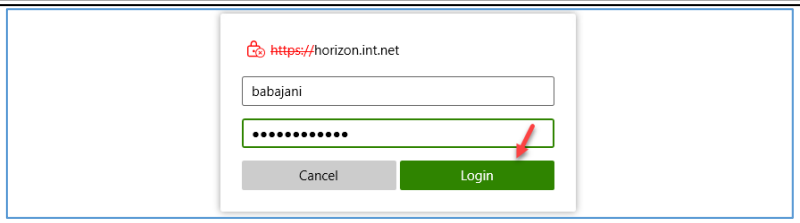
در شکل ۱۶-۵۹، باید آدرس سرور Horizon View را وارد کنید.



شکل ۱۶-۵۹ *Horizon Client Application*

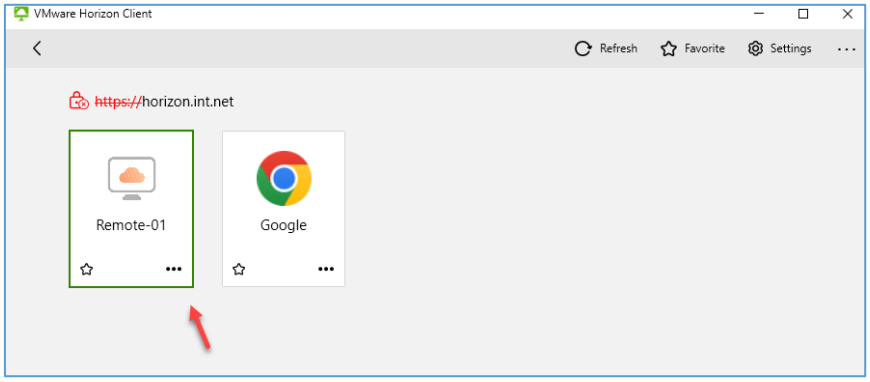
در شکل ۱۶-۶۰، باید نام کاربری و رمز عبور را وارد کنید، اگر توجه کرده باشید SSL به صورت رنگ قرمز در آمده و قابل قبول نیست، در ادامه نحوه‌ی دریافت SSL را با هم بررسی می‌کنیم.

www.takbook.com



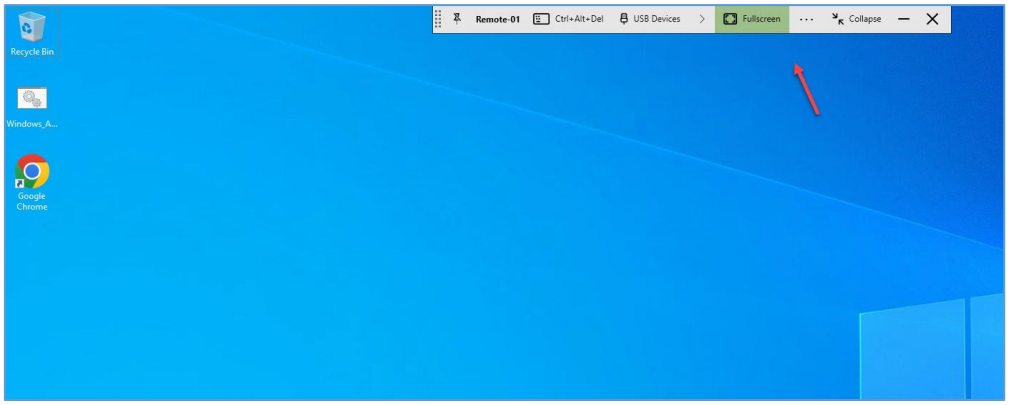
شکل ۱۶- ۶۰ Horizon Client Application

همان‌طور که در شکل ۱۶-۶۱، مشاهده می‌کنید وارد سرور شدیم و دو مورد در دسترس است و می‌توانیم اجرا کنیم، برای تست بر روی Remote-01 که همان سرور مجازی است کلیک می‌کنیم.



شکل ۱۶- ۶۱ Horizon Client Application

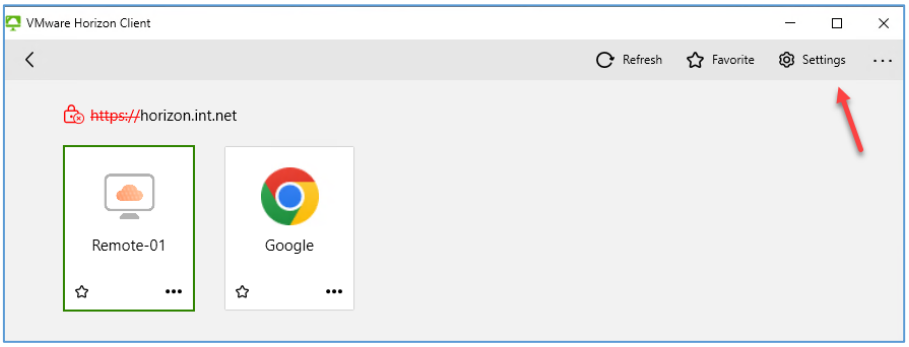
همان‌طور که در شکل ۱۶-۶۲، مشاهده می‌کنید توانستیم به سرور مورد نظر ریموت بزنیم، تفاوتی که این روش با روش قبلی دارید این است که کیفیت و سرعت بالاتری به نسبت روش Web دارد و همچنین نتظیمات اضافه‌ای که با هم بررسی می‌کنیم.



شکل ۱۶- ۶۲ Horizon Client Application

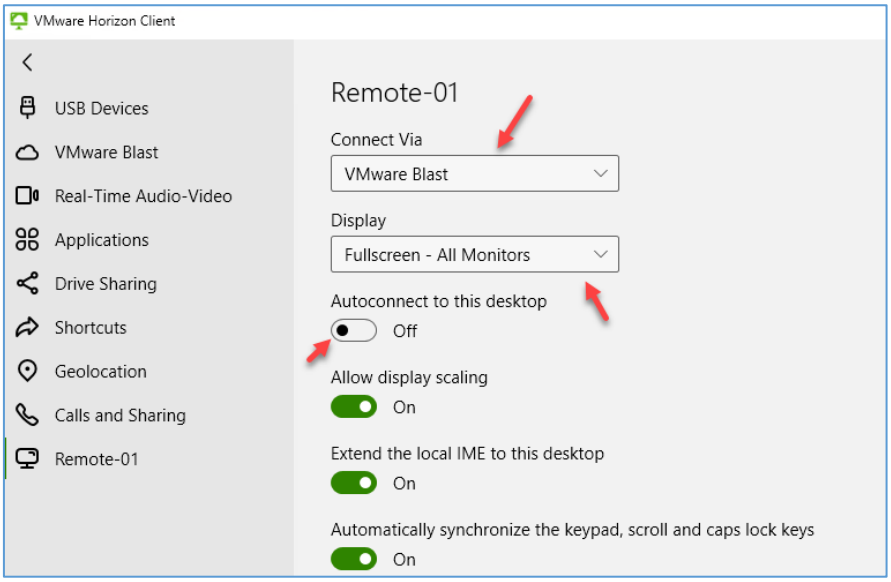
www.takbook.com

اگر دوباره به صفحه‌ی اول نرم‌افزار VMware Client برگردید طبق شکل ۱۶-۶۳، گزینه‌ی Settings را مشاهده می‌کنید که دارای تنظیمات مختلفی است.



شکل ۱۶-۶۳ *Horizon Client Application*

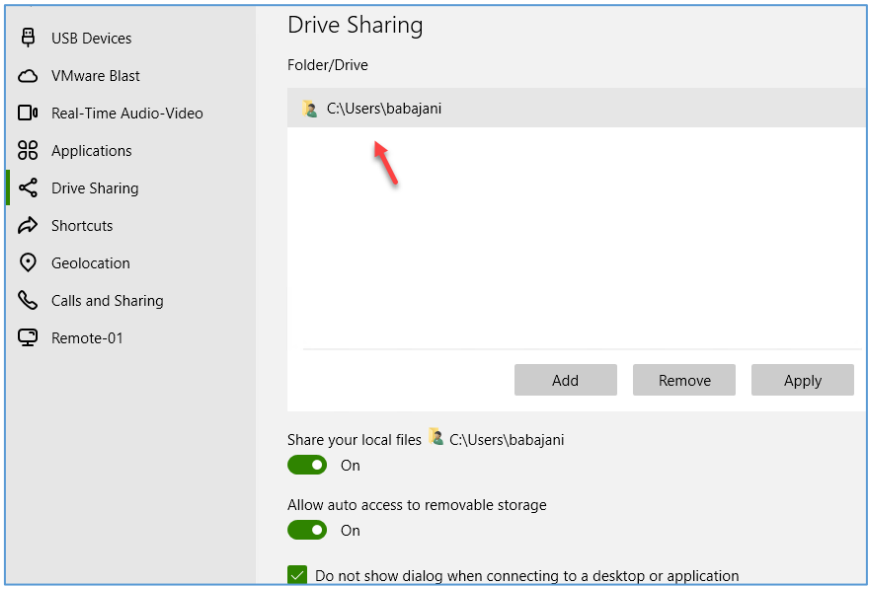
همان‌طور که در شکل ۱۶-۶۴، مشاهده می‌کنید از سمت چپ گزینه‌ی Remote-01 که همان Desktop Pool ما است مشخص است و در سمت راست تنظیمات آن را مشاهده می‌کنید، در قسمت Connect Via می‌توانید پروتکل ارتباطی را مشخص کنید که بهترین گزینه VMware Blast است، در قسمت Display اگر مثلاً دو تا مانیتور داشته باشید ماشین مورد نظر بر روی چند صفحه نمایش داده خواهد شد که می‌توانید آن را تغییر دهید، اگر گزینه‌ی Autoconnect to this desktop را فعال کنید، به محض اینکه وارد سرور شوید دقیقاً همین ماشین برای شما به صورت اتوماتیک باز خواهد شد، گزینه‌های دیگر برای Sync کردن سیستم شما با سیستم ماشین مجازی مورد نظر است.



شکل ۱۶-۶۴ *Horizon Client Application*

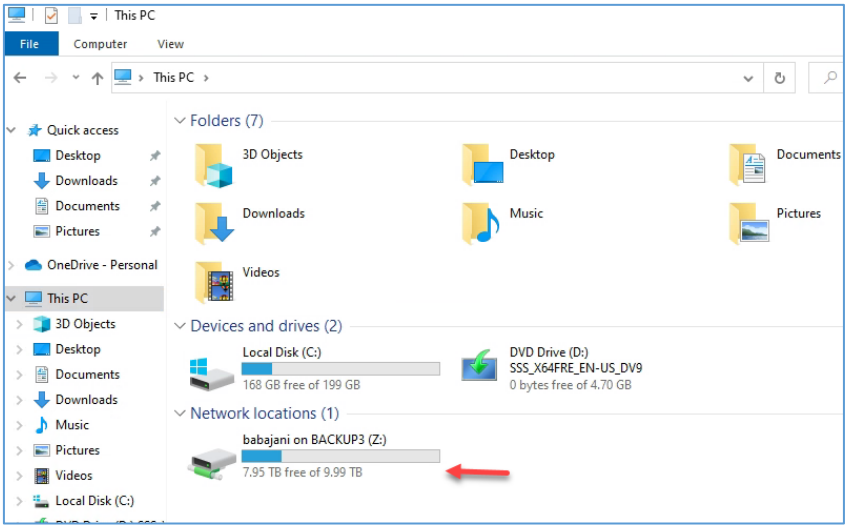
www.takbook.com

اگر به مانند شکل ۱۶-۶۵، وارد Drive Sharing شوید می‌توانید یک فولدر و یک مسیر مشخص کنید که این مسیر در ماشین مجازی مورد نظر قرار می‌گیرید و هر فایلی را که می‌خواهید بین سیستم اصلی خودتان با ماشین مجازی مورد نظر انتقال دهید می‌توانید از این گزینه استفاده کنید.



شکل ۱۶- ۶۵ *Horizon Client Application*

اگر به مانند شکل ۱۶-۶۶، دوباره وارد ماشین مجازی شوید و This PC را باز کنید یک فولدر MAP یا همان Share شده را مشاهده می‌کنید که مربوط به سیستم فیزیکی شما است.



شکل ۱۶- ۶۶ *Horizon Client Application*

www.takbook.com

۱۰-۱٦ نصب SSL و ارتباط از طریق اینترنت

SSL (Secure Sockets Layer) یک پروتکل امنیتی است که برای ایجاد ارتباط امن بین سرور و کلاینت در شبکه‌های ناامن مانند اینترنت استفاده می‌شود. این پروتکل از رمزنگاری استفاده می‌کند تا داده‌هایی که بین کلاینت و سرور منتقل می‌شوند، از دسترسی‌های غیرمجاز محافظت شوند.

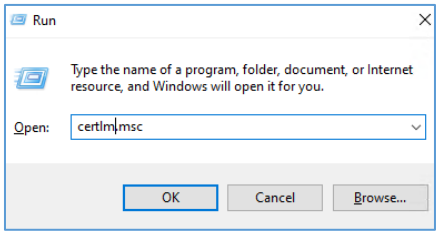
در VMware Horizon یکی از مهمترین بخش‌ها این است که سرویس SSL را پیاده‌سازی کنیم تا بتوانیم به راحتی از طریق اینترنت به سرور دسترسی داشته باشیم.

برای این کار موارد زیر مورد نیاز است:

۱- داشتن IP Static
۲- داشتن دومین شخصی
۳- تنظیم فایروال مانند میکروتیک
۴- دریافت گواهینامه SSL
۵- داشتن سرویس Certificate در شبکه‌ی داخلی

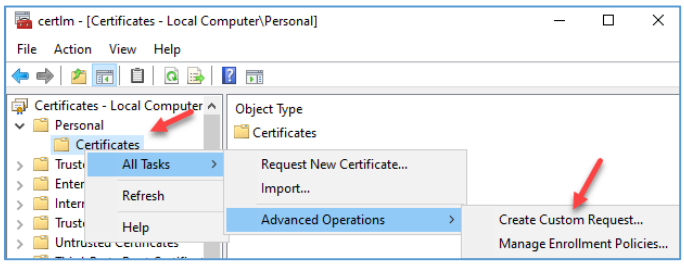
ایجاد گواهینامه داخلی

برای انجام این کار اول وارد سرور Horizon شوید و به مانند شکل ۱٦-٦۷، در Run دستور Certlm.msc را اجرا کنید تا سرویس Certificate برای Computer Account باز شود.



شکل ۱۶ - ۶۷ نصب SSL و ارتباط از طریق اینترنت

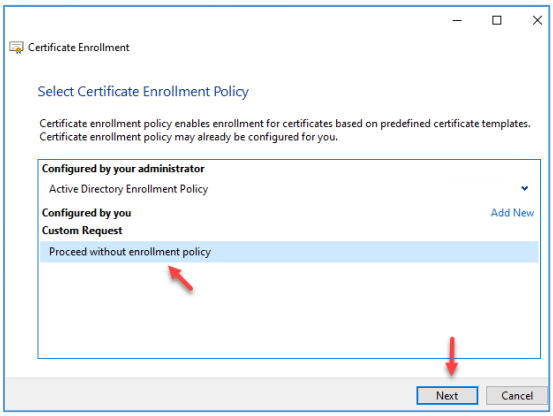
بعد از باز شدن سرویس مورد نظر به مانند شکل ۱٦-٦۸، وارد Personal شوید و بر روی Certificate کلیک راست کنید و از قسمت Advanced Operations گزینه‌ی Create Custom Reauest را انتخاب کنید.



شکل ۱۶ - ۶۸ نصب SSL و ارتباط از طریق اینترنت

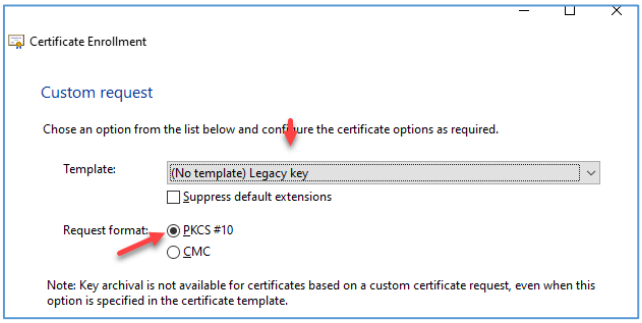
www.takbook.com

در شکل ۱۶-۶۹، گزینه‌ی Proceed without enrollment policy را انتخاب و بر روی Next کلیک کنید.



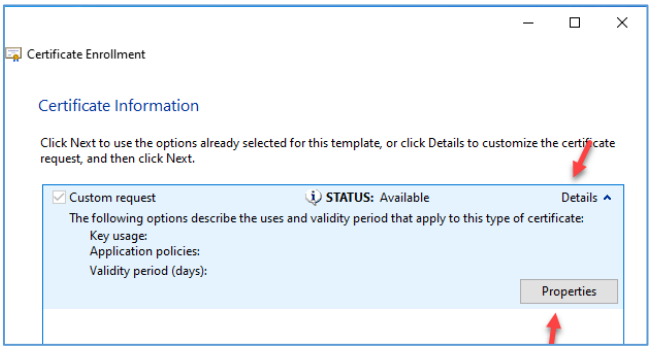
شکل ۱۶- ۶۹ نصب SSL و ارتباط از طریق اینترنت

در شکل ۱۶-۷۰، باید گزینه‌ی Legacy Key را انتخاب کنید و در گزینه‌ی زیری آن باید PKCS#10 را انتخاب کنید.



شکل ۱۶- ۷۰ نصب SSL و ارتباط از طریق اینترنت

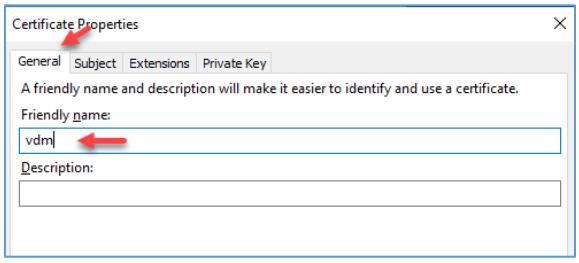
در شکل ۱۶-۷۱، بر روی Details کلیک و گزینه‌ی Properties را انتخاب کنید.



شکل ۱۶- ۷۱ نصب SSL و ارتباط از طریق اینترنت

www.takbook.com

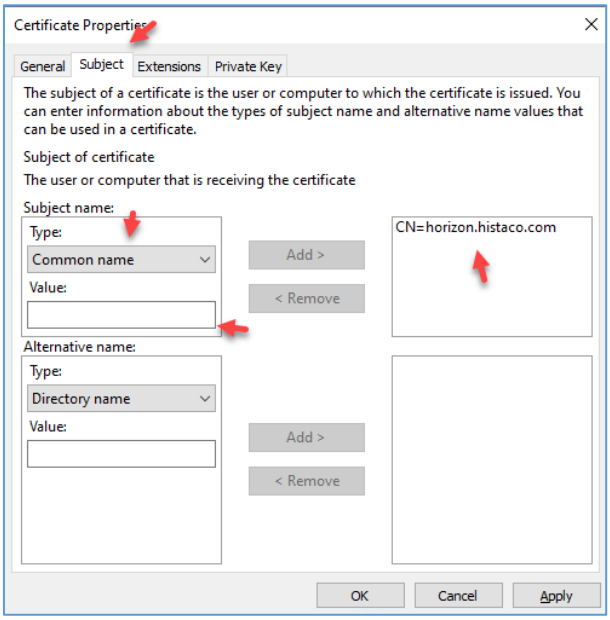
در شکل ۱۶-۷۲، در تب General و در قسمت Frindly Name باید کلمه vdm را وارد کنید، توجه کنید دقیقاً همین کلمه وارد شود.



شکل ۱۶- ۷۲ نصب SSL و ارتباط از طریق اینترنت

در شکل ۱۶-۷۳، وارد تب Subject شوید و گزینه‌ی Common name را انتخاب کنید و نام دقیق دومین خارجی خود به همراه نام سرور را وارد کنید و بر روی Add کلیک کنید تا به لیست اضافه شود.

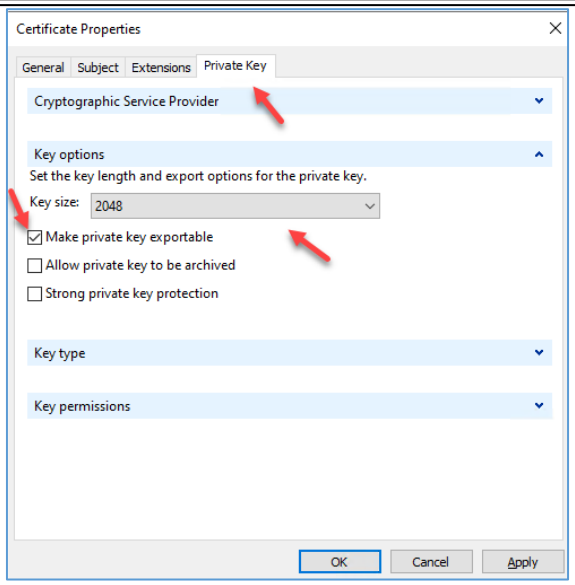
نکته مهم: بعضی از سایت هایی که گواهینامه صادر میکنند به کشور ایران حساس هستند و باید کد کشور را بر روی US قرار دهید، البته در صورت نیاز این کار را انجام دهید.



شکل ۱۶- ۷۳ نصب SSL و ارتباط از طریق اینترنت

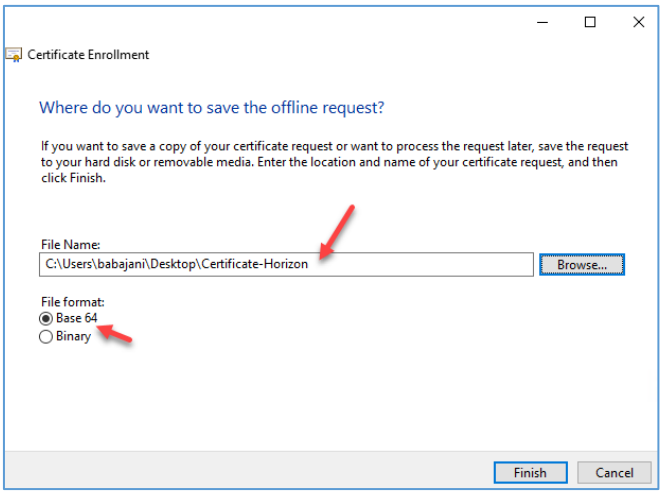
در ادامه کار به مانند شکل ۱۶-۷۴، وارد تب Private Key شوید و مقدار key size را به 2048 تغییر دهید و تیک گزینه‌ی مورد نظر را انتخاب کنید و در آخر بر روی OK کلیک کنید.

www.takbook.com



شکل ۱۶- ۷۴ نصب SSL و ارتباط از طریق اینترنت

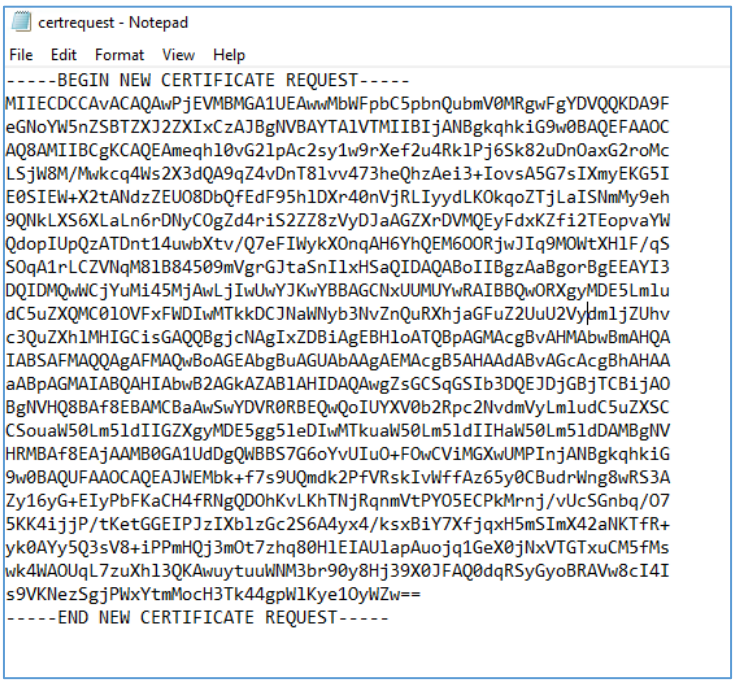
در شکل ۱۶-۷۵، باید بر روی Browse کلیک کنید و یک نام وارد و مسیر ذخیره کردن را مشخص کنید، در ادامه گزینه‌ی Base 64 را انتخاب کنید و بر روی Finish کلیک کنید.



شکل ۱۶- ۷۵ نصب SSL و ارتباط از طریق اینترنت

فایل مورد نظر در مسیر مورد مشخص شده ذخیره شد و اگر طبق شکل ۱۶-۷۶، آن را باز کنید کدی را مشاهده می‌کنید که باید از کل آن کپی بگیرید و آن را در یک سایت ارائه دهنده‌ی SSL کپی کنیم.

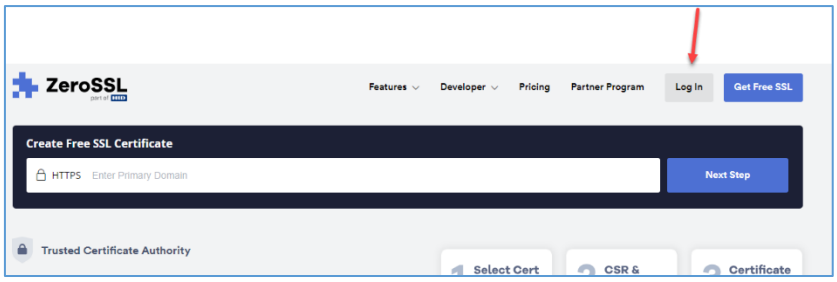
www.takbook.com



شکل ۱۶- ۷۶ نصب SSL و ارتباط از طریق اینترنت

برای اینکه از یک گواهینامه‌ی عمومی استفاده کنیم باید از سایت‌های پولی یا عمومی استفاده کنیم، برای اینکه بخواهیم به صورت رایگان استفاده کنیم باید از سایت https://zerossl.com استفاده کنیم.

به مانند شکل ۱۶–۷۷، وارد سایت شوید و بر روی Login کلیک کنید.

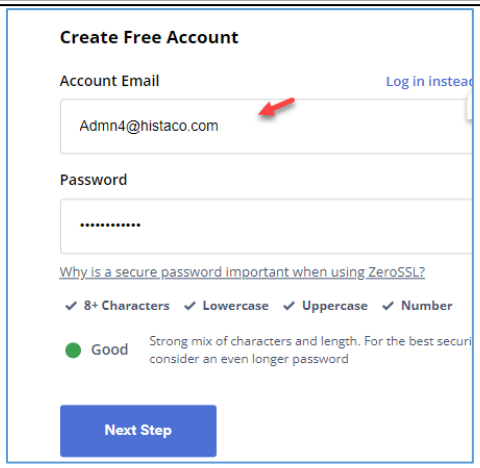


شکل ۱۶- ۷۷ نصب SSL و ارتباط از طریق اینترنت

اگر از قبل حساب دارید وارد شوید و اگر ندارید برای ایجاد حساب بر روی Get started for free کلیک کنید.

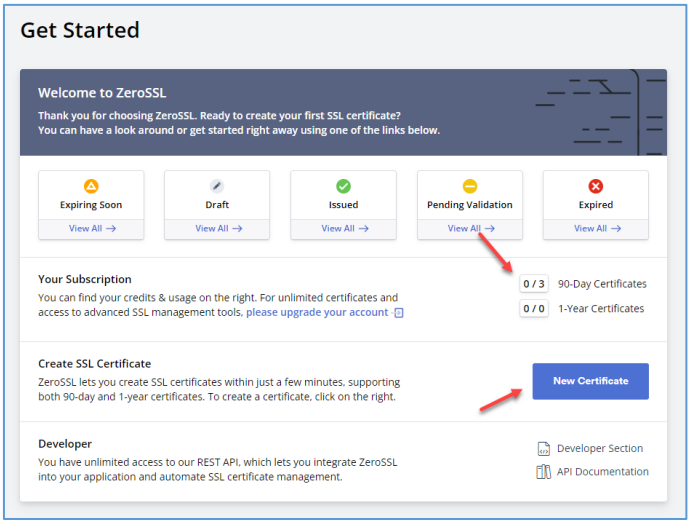
در شکل ۱۶–۷۸، فقط کافی است یک ایمیل و یک رمز عبور مشخص کنید که بعدش وارد آن می‌شوید.

www.takbook.com



شکل ۱۶- ۷۸ نصب SSL و ارتباط از طریق اینترنت

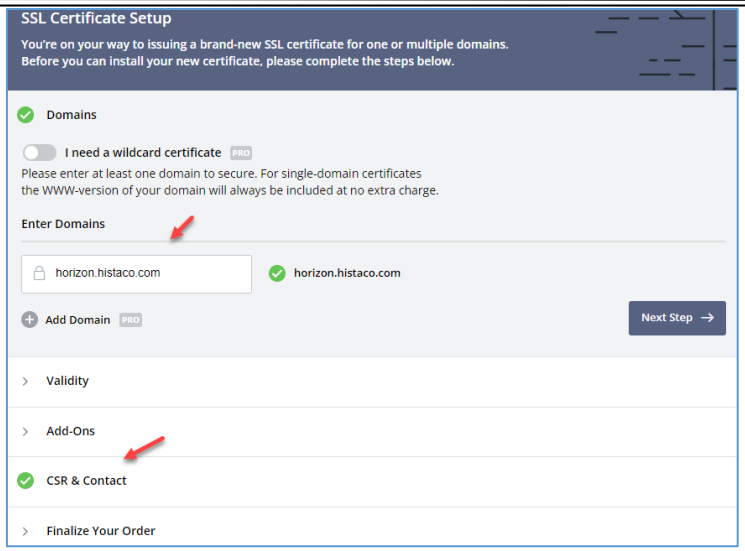
همان‌طور که در شکل ۱۶-۷۹، مشاهده می‌کنید در طرح رایگان فقط سه تا گواهینامه می‌توانید فعال کنید، بر روی New Certificate کلیک کنید.



شکل ۱۶- ۷۹ نصب SSL و ارتباط از طریق اینترنت

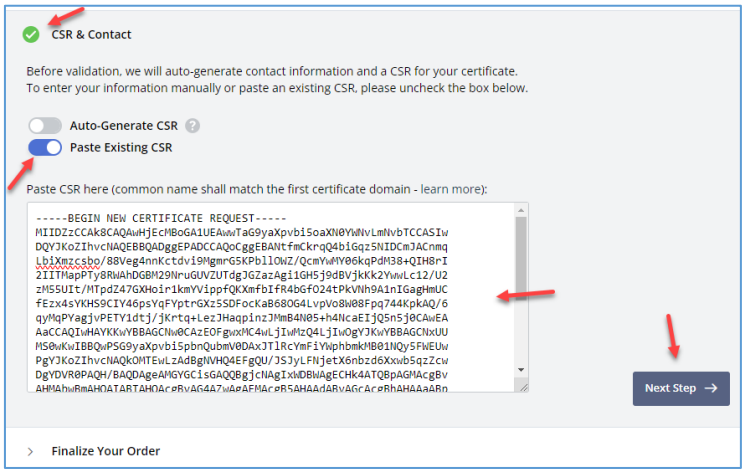
در شکل ۱۶-۸۰، باید آدرس سرور را وارد کنید، این آدرس دقیقاً باید همان آدرسی باشد که در هنگام گواهینامه داخلی وارد کردیم، برای اینکه آن کد گواهینامه را در این سایت کپی کنید باید بر روی CSR & Contact کلیک کنید.

www.takbook.com



شکل ۱۶- ۸۰ نصب SSL و ارتباط از طریق اینترنت

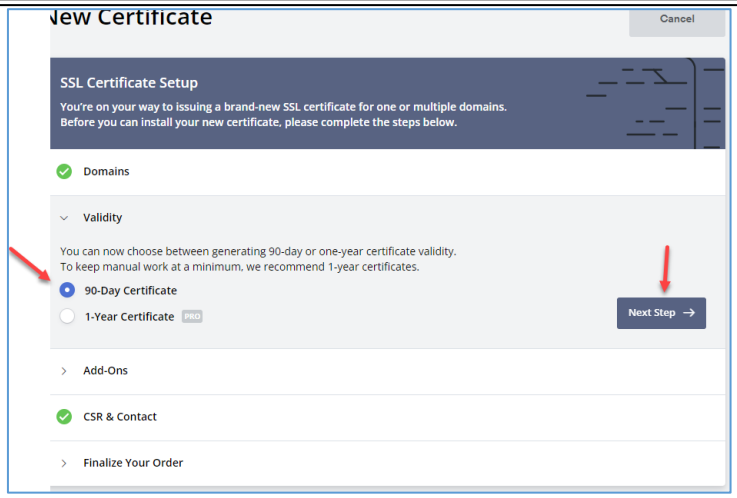
در شکل ۱۶-۸۱، برای اینکه کد مورد نظر را Past کنیم باید گزینه‌ی Past Existing را انتخاب کنیم و کد را در داخل باکس مورد نظر قرار دهیم و بر روی Next Step کلیک کنیم.



شکل ۱۶- ۸۱ نصب SSL و ارتباط از طریق اینترنت

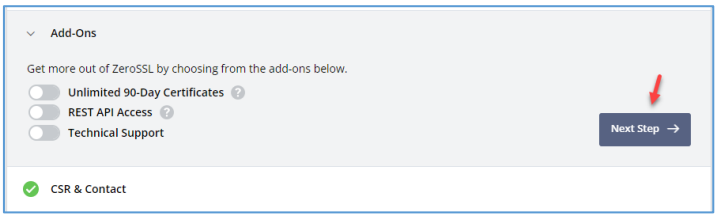
در شکل ۱۶-۸۲، باید گزینه‌ی 90 روز را انتخاب کنید و بر روی Next کلیک کنید، با این کار این گواهینامه تا 90 روز اعتبار دارد، البته بعد از اتمام دوباره به همین صورت می‌توانید آن را فعال کنید.

www.takbook.com



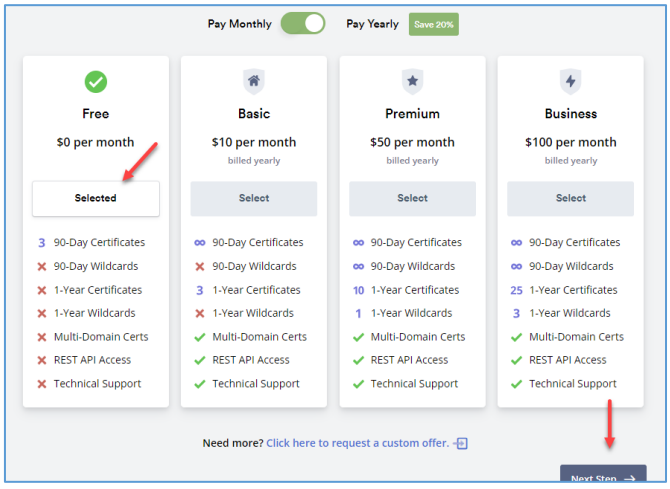
شکل ۱۶- ۸۲ نصب SSL و ارتباط از طریق اینترنت

در شکل ۱۶-۸۳، فقط بر روی Next کلیک کنید.



شکل ۱۶- ۸۳ نصب SSL و ارتباط از طریق اینترنت

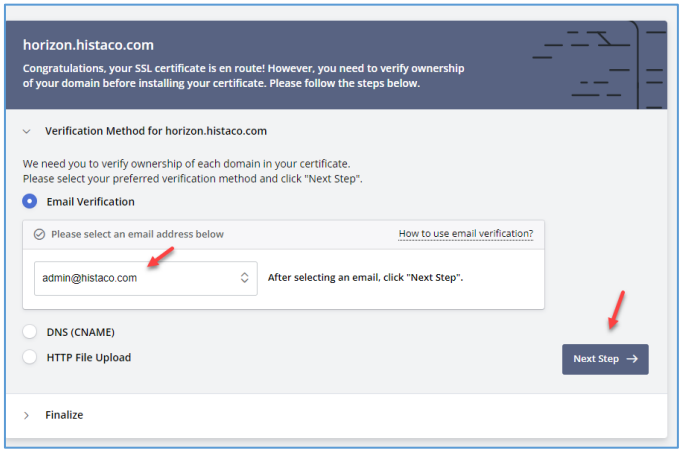
در شکل ۱۶-۸۴، باید پلن رایگان را انتخاب کنید و بر روی Next کلیک کنید.



شکل ۱۶- ۸۴ نصب SSL و ارتباط از طریق اینترنت

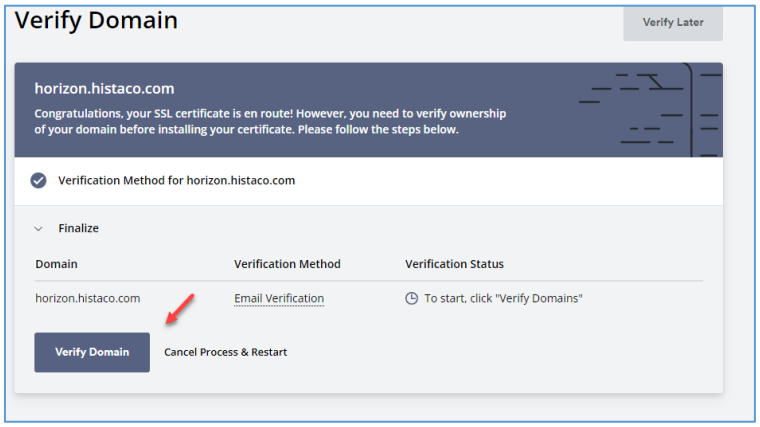
www.takbook.com

بعد از اتمام کار وارد شکل ۱۶-۸۵، می‌شوید که باید یک آدرس ایمیل واقعی که در دومیت و هاست شما فعال است وارد کنید تا یک کد برای شما ارسال شود و بعد از آن گواهینامه فعال خواهد شد، پس آدرس ایمیل خود را انتخاب و بر روی Next کلیک کنید، همان‌طور که گفتیم باید این آدرس موجود و فعال داشته باشد.



شکل ۱۶- ۸۵ نصب SSL و ارتباط از طریق اینترنت

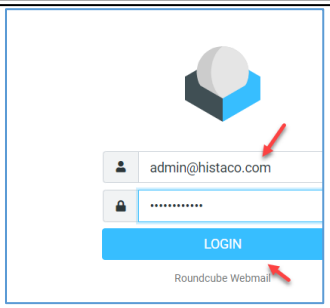
در شکل ۱۶-۸۶، بر روی Verify Domain کلیک کنید تا یک ایمیل به آدرس مشخص شده ارسال شود.



شکل ۱۶- ۸۶ نصب SSL و ارتباط از طریق اینترنت

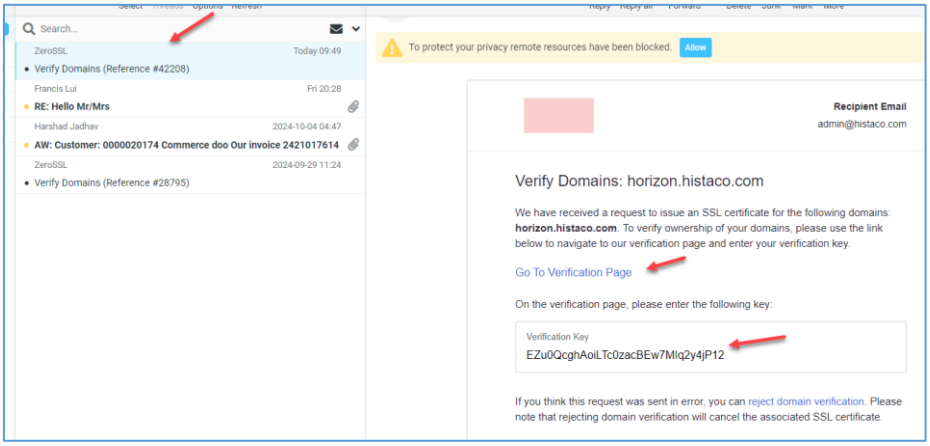
در ادامه کار به مانند شکل ۱۶-۸۷، وارد ایمیل سازمانی خود می‌شویم.

www.takbook.com



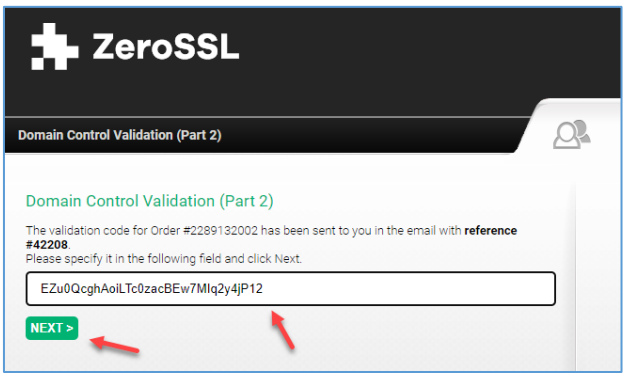
شکل ۱۶- ۸۷ نصب SSL و ارتباط از طریق اینترنت

همان‌طور که در شکل ۱۶-۸۸، مشاهده می‌کنید یک ایمیل از سایت ZeroSSL دریافت شده است که باید کد مورد نظر را کپی بگیرید و بر روی Link مشخص شده کلیک کنید.



شکل ۱۶- ۸۸ نصب SSL و ارتباط از طریق اینترنت

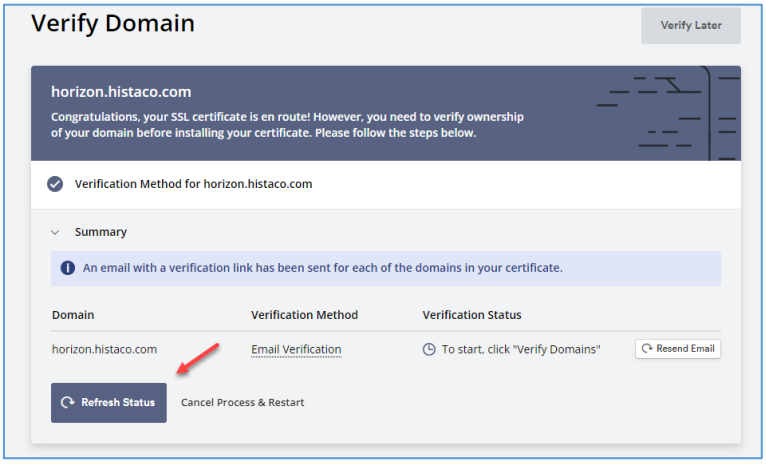
در شکل ۱۶-۸۹، کد مورد نظر را وارد و بر روی Next کلیک کنید تا کد تایید شود.



شکل ۱۶- ۸۹ نصب SSL و ارتباط از طریق اینترنت

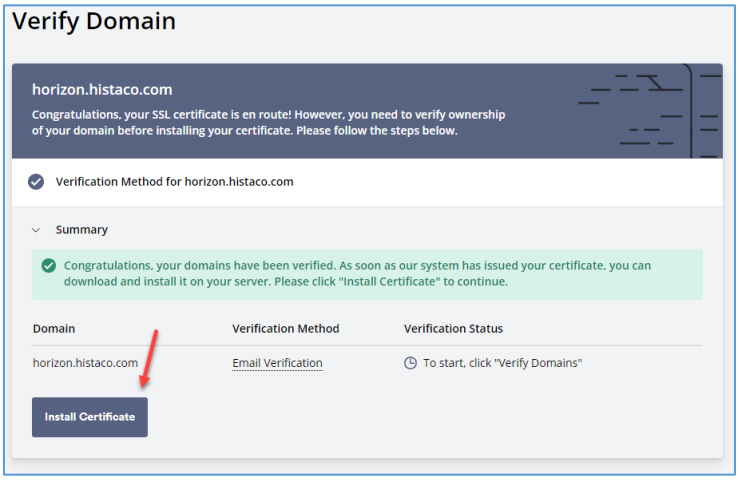
www.takbook.com

دوباره به همان سایت برگردید و طبق شکل ۱٦-۹۰، بر روی Refresh Satus کلیک کنید.



شکل ۱۶- ۹۰ نصب SSL و ارتباط از طریق اینترنت

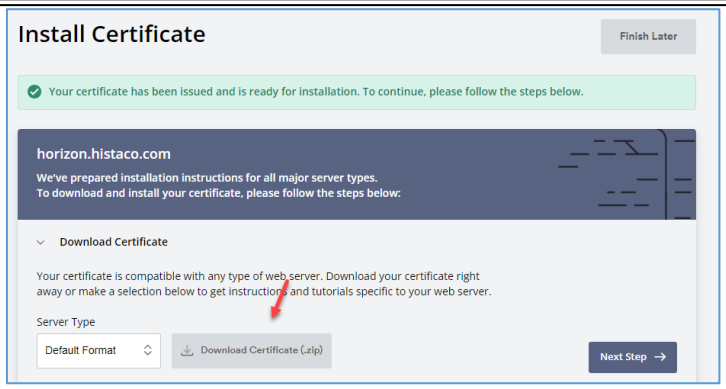
همان‌طور که در شکل ۱٦-۹۱، مشاهده می‌کنید گواهینامه‌ی مورد نظر فعال شده است و برای ادامه کار بر روی Install Certificate کلیک کنید.



شکل ۱۶- ۹۱ نصب SSL و ارتباط از طریق اینترنت

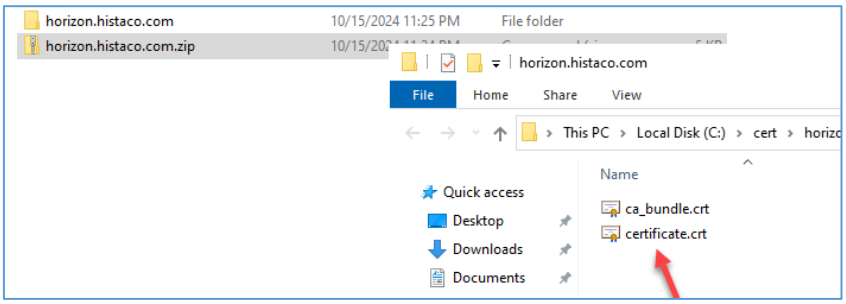
در شکل ۱٦-۹۲، روی Download کلیک کنید تا گواهینامه دانلود شود، و بعد از دریافت، باید آن را به سرور horizon انتقال دهید.

www.takbook.com



شکل ۱۶- ۹۲ نصب SSL و ارتباط از طریق اینترنت

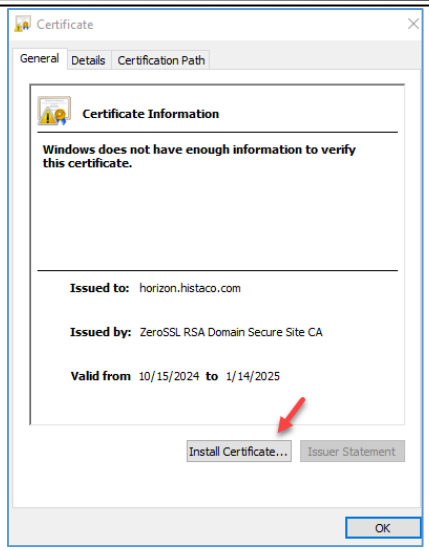
به مانند شکل ۱۶-۹۳، فایل فشرده را اکسترکت کنید و بر روی فایل Certificate.crt دو بار کلیک کنید.



شکل ۱۶- ۹۳ نصب SSL و ارتباط از طریق اینترنت

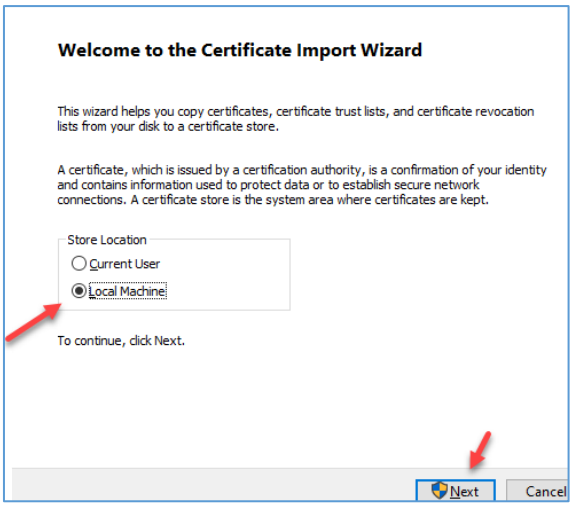
به مانند شکل ۱۶-۹۴، بر روی install Certificate کلیک کنید.

www.takbook.com



شکل ۱۶- ۹۴ نصب SSL و ارتباط از طریق اینترنت

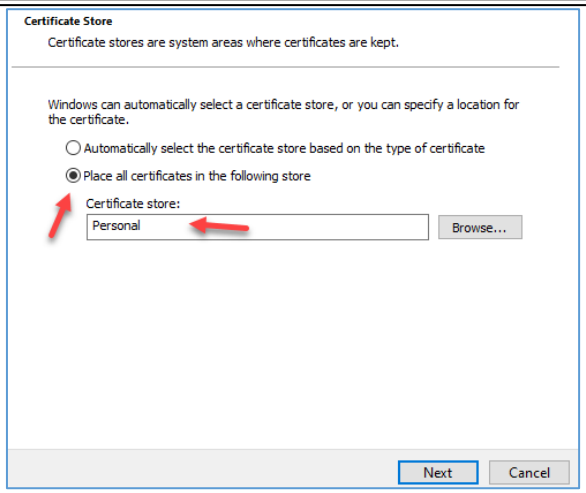
در شکل ۱۶-۹۵، گزینه‌ی Local Machine را انتخاب کنید.



شکل ۱۶- ۹۵ نصب SSL و ارتباط از طریق اینترنت

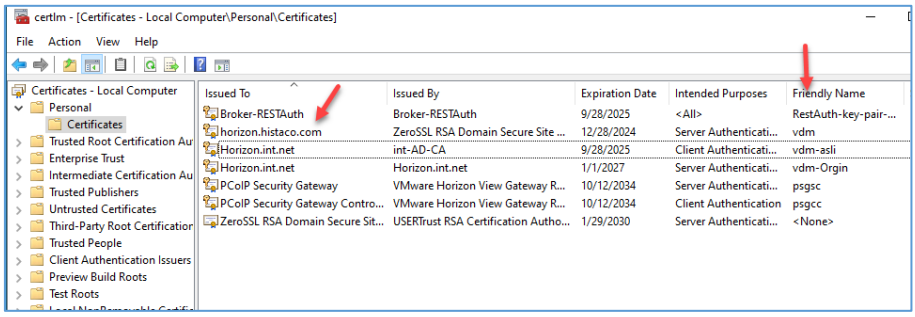
در شکل ۱۶-۹۶، باید بر روی Browse کلیک کنید و گزینه‌ی Personal را انتخاب کنید و در صفحه‌ی بعد بر روی Finish کلیک کنید تا گواهینامه‌ی مورد نظر در سرور قرار بگیرد.

www.takbook.com



شکل ۱۶- ۹۶ نصب SSL و ارتباط از طریق اینترنت

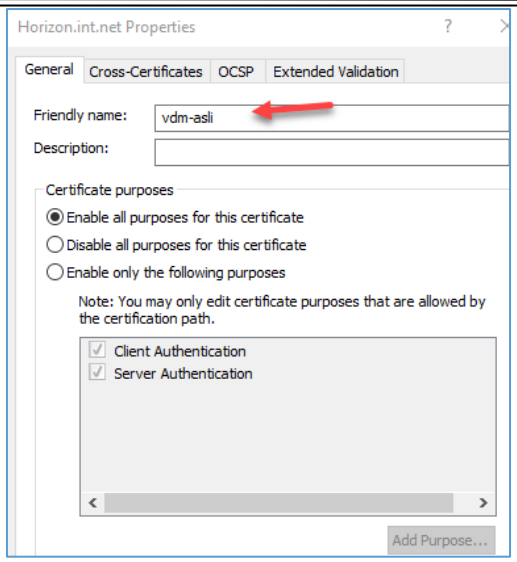
بعد از این کار در Run دستور Certlm.msc را وارد کنید و در شکل ۱۶-۹۷، وارد Certificate شوید، همان‌طور که مشاهده می‌کنید، گواهینامه‌ی خارجی در قسمت مورد نظر قرار گرفته است و یکی از مهمترین تغییری که باید در اینجا انجام دهیم این است که شما الان دو تا نام vdm در قسمت Frindly Name دارید که باید گواهینامه‌ی قدیمی را به نام دیگر به مانند شکل تغییر دهید، برای تغییر کافی است بر روی گواهینامه کلیک راست و گزینه‌ی Properties را انتخاب کنید.



شکل ۱۶- ۹۷ نصب SSL و ارتباط از طریق اینترنت

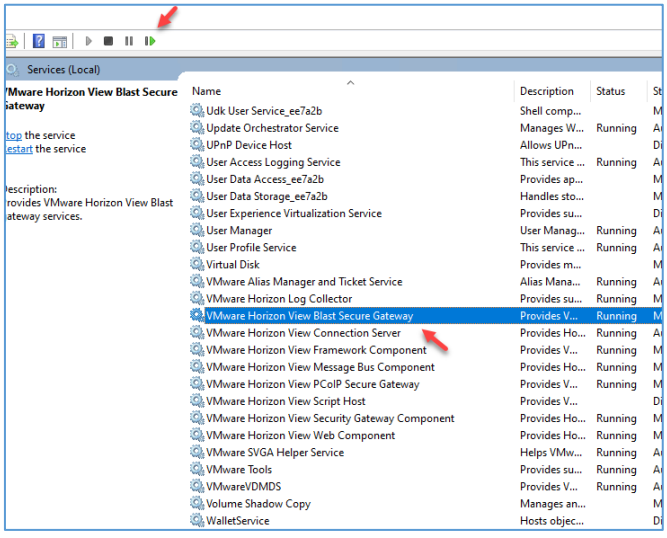
در شکل ۱۶-۹۸، Frindly Name گواهینامه‌ی داخلی را به نام دیگر تغییر می‌دهیم.

www.takbook.com



شکل ۱۶- ۹۸ نصب SSL و ارتباط از طریق اینترنت

بعد از انجام مراحل بالا باید سرور را ری استارت کنید تا SSL مورد نظر در کل سرور فعال شود و یا اینکه به مانند شکل ۱۶-۹۹، وارد سرویس‌ها شوید و سرویس مورد نظر را Restart کنید.

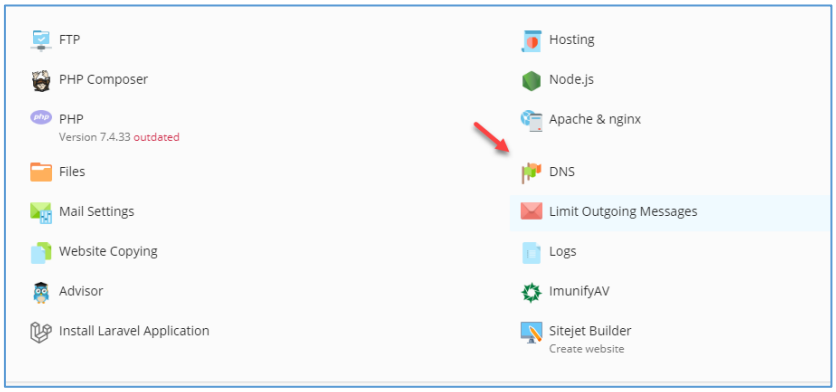


شکل ۱۶- ۹۹ نصب SSL و ارتباط از طریق اینترنت

هنوز کار به اتمام نرسیده است و باید دو مرحله دیگر را انجام دهیم، مرحله اول تعریف نام Horizon در دومین خارجی و متصل کردن آن به روتر خود از طریق IP Static و مرحله‌ی دوم تنظیم فایروال در روتر است تا به درخواست‌های ورودی پاسخ دهد.

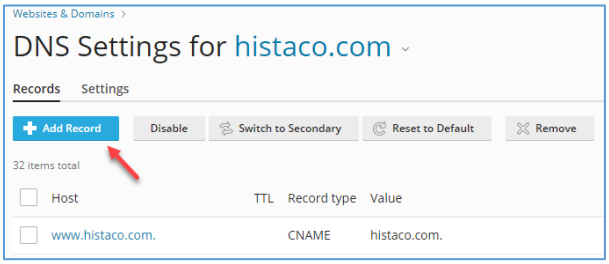
www.takbook.com

برای تنظیم نام در دومین، وارد هاست خود می‌شویم که دارای نرم‌افزار Plesk است و به مانند شکل ۱۶-۱۰۰، بر روی DNS کلیک می‌کنیم.



شکل ۱۶- ۱۰۰ نصب SSL و ارتباط از طریق اینترنت

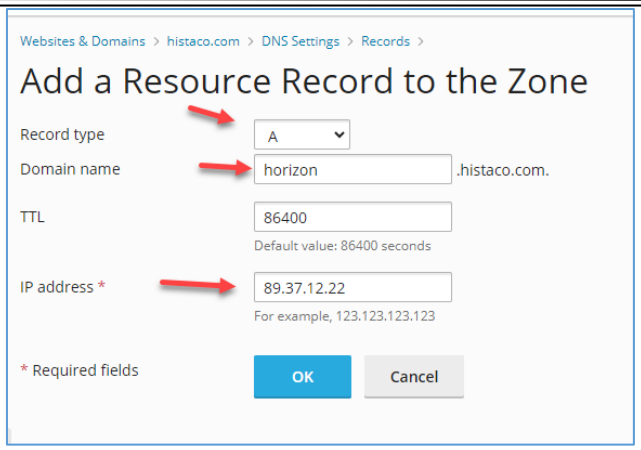
در شکل ۱۶-۱۰۱، باید بر روی Add Record کلیک کنید.



شکل ۱۶- ۱۰۱ نصب SSL و ارتباط از طریق اینترنت

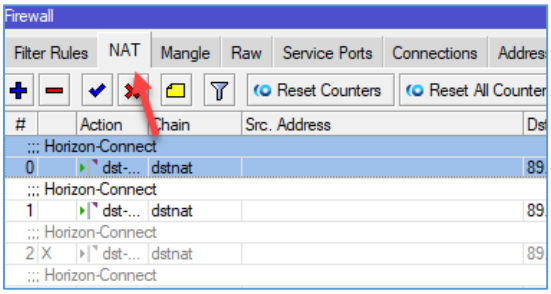
در شکل ۱۶-۱۰۲، باید در قسمت Record rype گزینه‌ی A را انتخاب کنید و در قسمت Domain name باید نامی که در گواهینامه وارد کردیم را وارد کنید و در قسمت آدرس هم باید آدرس IP static شبکه خود را وارد کنید که به روتر متصل است.

www.takbook.com



شکل ۱۶- ۱۰۲ نصب SSL و ارتباط از طریق اینترنت

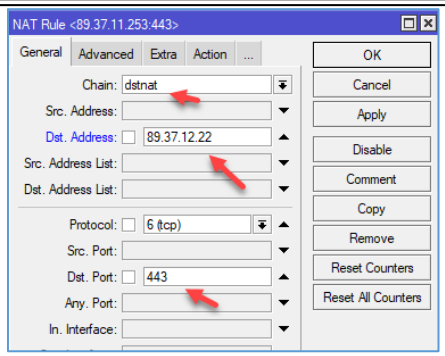
بعد از انجام این کار باید وارد روتر شویم و فایروال را تنظیم کنیم، روتر ما در این قسمت مثل همیشه میکرتیک است و برای تنظیم باید وارد IP و بعد Firewall شوید و به مانند شکل ۱۶-۱۰۳، وارد تب Nat شوید و بر روی آیکون + کلیک کنید.



شکل ۱۶- ۱۰۳ نصب SSL و ارتباط از طریق اینترنت

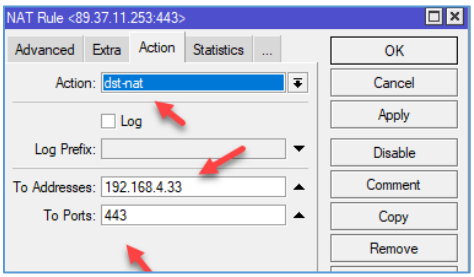
اولین پورتی که باید باز کنیم پورت معروف 443 است که مربوط به گواهینامه SSL است و به مانند شکل ۱۶-۱۰۴، در قسمت Chain باید گزینه‌ی dstnat که مربوط به ترافیک خارجی است را انتخاب کنید و در قسمت Dst.Address باید آدرس IP startic خود را وارد کنید و در قسمت Protocol هم باید پروتکل tcp را انتخاب کنید و در قسمت Dst. Port پورت 443 را وارد کنید.

www.takbook.com



شکل ۱۶- ۱۰۴ نصب SSL و ارتباط از طریق اینترنت

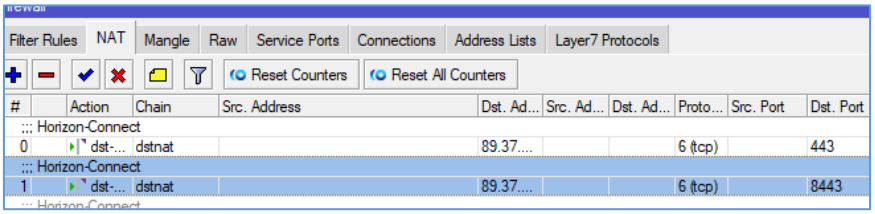
در ادامه به مانند شکل ۱۶-۱۰۵، وارد تب Action شوید و در قسمت To Address باید آدرس IP سرور داخلی خود را وارد کنید و در قسمت To Ports هم باید پورت 443 را وارد کنیم، بر روی OK کلیک کنید تا rule مورد نظر ایجاد شود.



شکل ۱۶- ۱۰۵ نصب SSL و ارتباط از طریق اینترنت

در ادامه باید برای پورت 8443 هم یک Rule تغریف کنیم، این پورت برای پروتکل Blast Extreme است که به طور پیش‌فرض از پورت 8443 برای اتصالات رمزنگاری شده با SSL/TLS استفاده می‌کند.

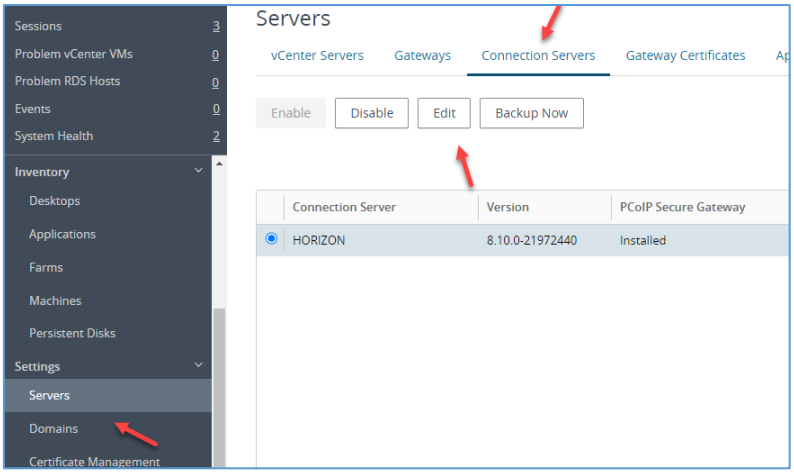
کافی است فقط از Rule قبلی یک کپی تهیه و مقدار پورت آن را به 8443 تغییر دهید که در شکل ۱۶-۱۰۶، همین موضوع را مشاهده می‌کنید و هر دو Rule ایجاد شده است.



شکل ۱۶- ۱۰۶ نصب SSL و ارتباط از طریق اینترنت

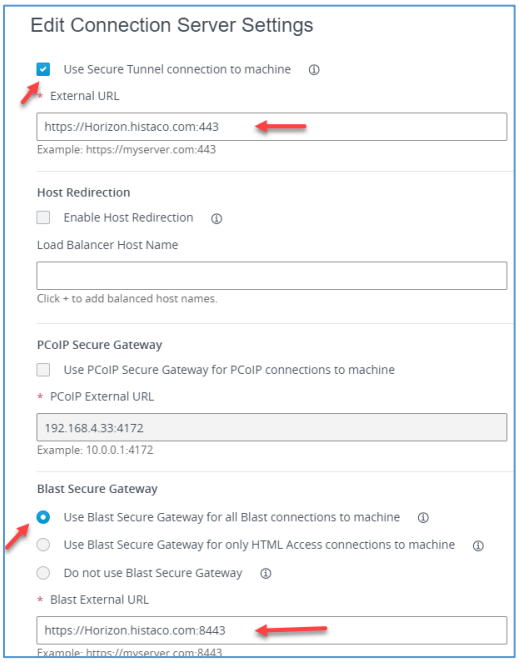
www.takbook.com

خوب برای ادامه کار و تنظیم نهایی باید طبق شکل ۱۶-۱۰۷، وارد صفحه‌ی مدیریتی Horizon شویم و از قسمت Settings بر روی Servers کلیک کنید و بعد وارد تب Connection Servers شوید و سرور مورد نظر خود را انتخاب و بر روی Edit کلیک کنید.



شکل ۱۶- ۱۰۷ نصب SSL و ارتباط از طریق اینترنت

در شکل ۱۶-۱۰۸، که خیلی مهم است باید آدرس سرور را که بر روی آن SSL فعال کردیم را در قسمت‌های مشخص شده وارد کنید و همچنین پورت آنها را هم جلوی آن بنویسید.

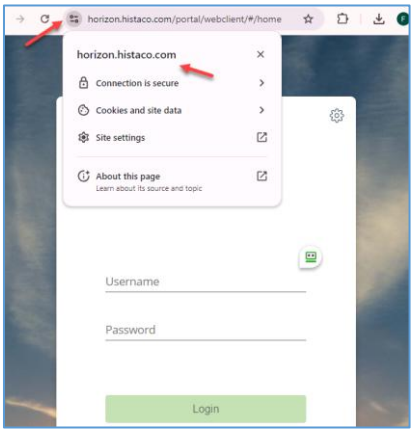


شکل ۱۶- ۱۰۸ نصب SSL و ارتباط از طریق اینترنت

www.takbook.com

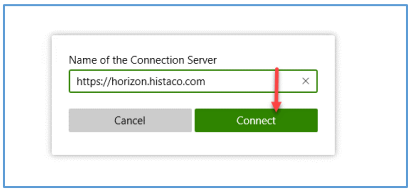
در اینجا کار به اتمام می‌رسد و شما می‌توانید از طریق SSL عمومی و اصلی به سرور خود متصل شوید برای تست این موضوع سایت را از طریق وب و کلاینت باز می‌کنیم.

طبق شکل ۱۶-۱۰۹، همان‌طور که در نسخه‌ی تحت وب مشاهده می‌کنید، SSL به خوبی در حال کار است و سایت با استفاده از آن و بدون هیچ خطایی اجرا شده است، یعنی شما می‌توانید از هر نقطه از جهان به اطلاعات دسترسی داشته باشید.

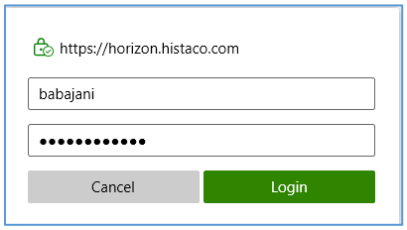


شکل ۱۶- ۱۰۹ نصب SSL و ارتباط از طریق اینترنت

اگر نسخه‌ی کلاینت را هم اجرا کنیم به مانند شکل ۱۶-۱۱۰، SSL نمایش داده خواهد شد و می‌توانید با خیال راحت وارد آن شوید.

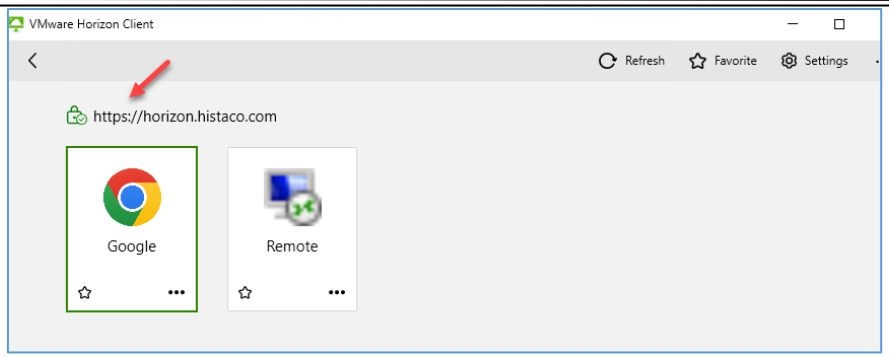


شکل ۱۶- ۱۱۰ نصب SSL و ارتباط از طریق اینترنت



شکل ۱۶- ۱۱۱ نصب SSL و ارتباط از طریق اینترنت

www.takbook.com



شکل ۱۶- ۱۱۲ نصب SSL و ارتباط از طریق اینترنت

در قسمت‌های قبلی به صورت دستی توانستیم ماشین مجازی ایجاد کنیم و آن را به Horizon متصل کنیم و همین‌طور نرم‌افزارهای مورد نیاز را برای کاربران Share کنیم، حالا همه این حالت‌ها را می‌خواهیم به صورت اتومالتیک و با استفاده از نرم‌افزار قدرتمند Vcenter انجام دهیم.

۱۶-۱۱ دسترسی Horizon به سرور VCenter

در مورد نصب و راه‌اندازی Vcenter به صورت کامل در این کتاب توضیح دادیم، و در این قسمت می‌خواهیم آن را به Horizon متصل کنیم، برای شروع باید یک Rule در Vcenter ایجاد کنیم و دسترسی مورد نیاز را به Horizon بدهیم.

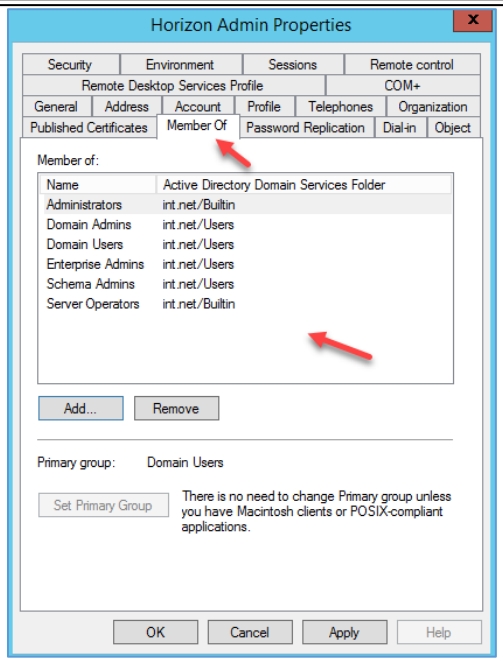
مرحله اول – ایجاد کاربر Active Directory

در مرحله اول باید کاربری را برای متصل شدن بین این دو نرم افزار مشخص کنیم، باید کاربری را در Active Directory مشخص کنید که دسترسی کامل به شبکه داشته باشد، یعنی باید عضو چند گروه زیر باشد که لیست آن را در زیر مشاهده می‌کنید.

- Enterprise Admins(مدیران سازمانی)
- Domain Admins(مدیران دامنه)
- Administrators(مدیران)
- Schema Admins(مدیران اسکیما)
- Server Operators(اپراتورهای سرور)

پس برای اینکه این دسترسی‌ها را به کاربر مورد نظر دهیم باید وارد Active directory شوید و به مانند شکل ۱۶-۱۱۳، کاربر Horizon-Admin که ایجاد کردیم را عضو گروه‌های مورد نظر کنید:

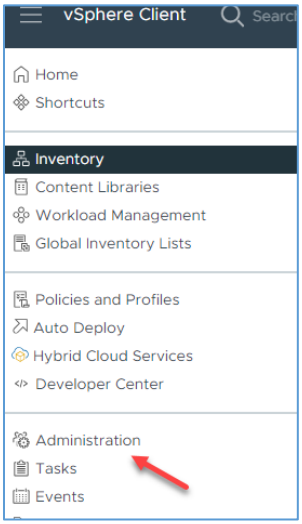
www.takbook.com



شکل ۱۶-۱۱۳ دسترسی Horizon به سرور VCenter

مرحله دوم – ایجاد Rule در Vcenter

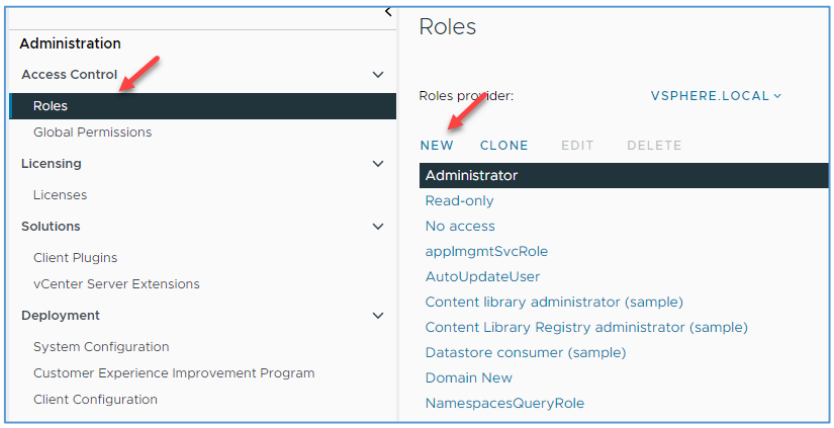
در ادامه کار و برای اینکه Horizon به Vcenter متصل شود باید یک Rule در Vcenter ایجاد کنیم، برای این کار وارد Vcenter شوید و در صفحه باز شده بر روی منوی مشخص شده کلیک کنید و گزینهٔ Administration را انتخاب کنید.



شکل ۱۶-۱۱۴ ایجاد Rule در Vcenter

www.takbook.com

برای ایجاد Role جدید طبق شکل ۱۶-۱۱۵، برای Horizon بر روی New کلیک کنید.



شکل ۱۶-۱۱۵ ایجاد Rule در Vcenter

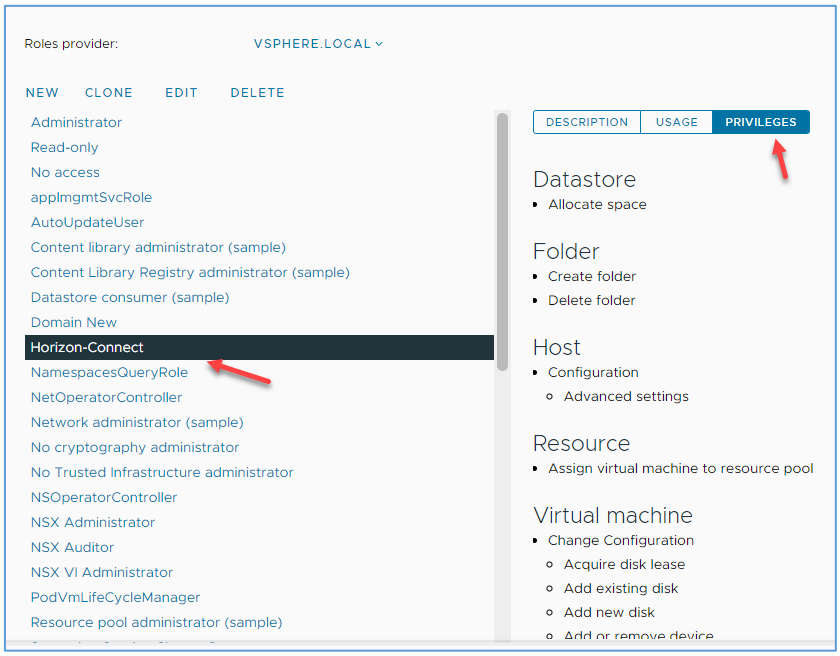
برای اینکه دسترسی لازم را به کاربر مورد نظر دهیم باید از جدول ۱۶-۳، استفاده کنیم:

جدول ۱۶-۳

نام گروه	دسترسی مورد نیاز که باید انتخاب شود
Folder	Create Folder Delete Folder
Datastore	Allocate space
Virtual Machine	In Configuration: Add or remove device Advanced Modify device settings In Interaction: Power Off Power On Reset Suspend Perform wipe or shrink operations In Inventory: Create new Create from existing Remove In Provisioning: Customize Deploy template Read customization specifications Clone Template Clone Virtual Machine
Resource	Assign virtual machine to resource pool
Global	Act as vCenter Server
Host	In Configuration: Advanced settings

www.takbook.com

بعد از ایجاد Role مورد نظر می‌توانید به مانند شکل ۱۶-۱۱۶، وارد تب Privileges شوید.

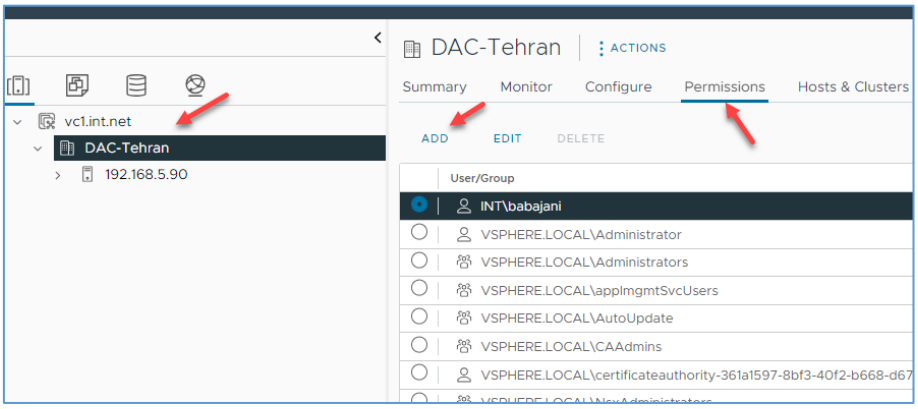


شکل ۱۶-۱۱۶ ایجاد Rule در Vcenter

مرحله سوم – دسترسی دادن به کاربر مورد نظر

قبل از اینکه کاربر مورد نظر را عضو Vcenter کنیم باید خود Vcenter عضو دومین باشد که در فصل مربوط به Vcenter توضیحات لازم داده شده است.

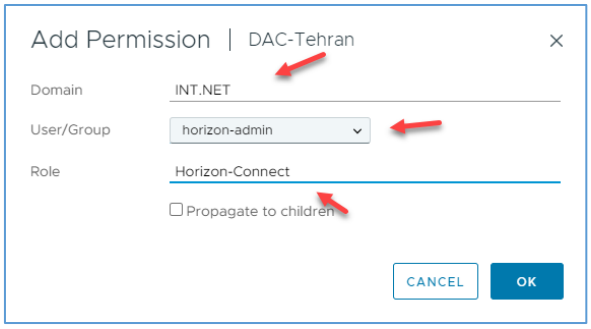
برای اینکه کاربری که در Active ایجاد کردیم را در Vcenter تعریف کنیم به مانند شکل ۱۶-۱۱۷، بر روی DataCenter که ایجاد کردید کلیک کنید و وارد تب Permissions شوید و بر روی Add کلیک کنید.



شکل ۱۶-۱۱۷ دسترسی دادن به کاربر

www.takbook.com

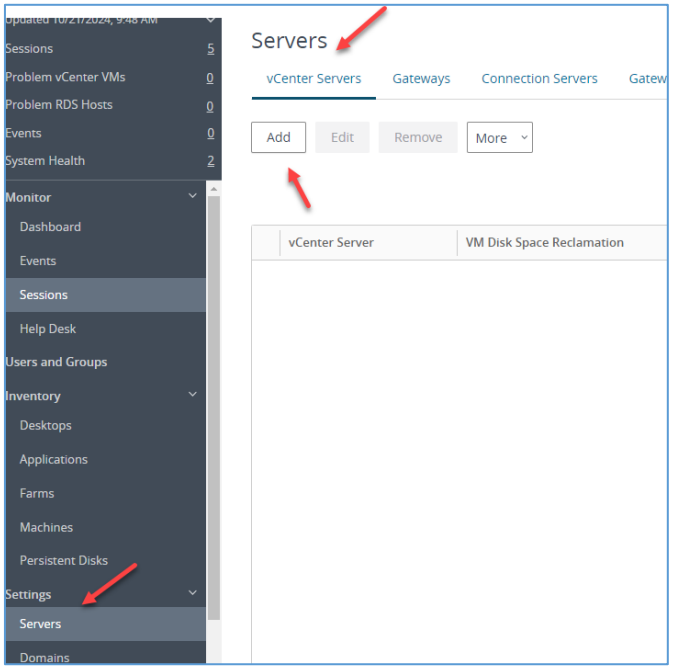
در شکل ۱۶–۱۱۸، باید کاربر موردنظری که ایجاد کردیم را به این لیست اضافه کنیم، برای این کار بر روی Add کلیک کنید و طبق شکل نام دومین، نام کاربر و نام Role موردنظر را انتخاب و بر روی OK کلیک کنید.



شکل ۱۶- ۱۱۸ دسترسی دادن به کاربر

مرحله چهارم – اتصال vCenter به Horizon

در این مرحله می‌خواهیم Horizon را به Vcenter متصل کنیم برای این کار به مانند شکل ۱۶–۱۱۹، وارد صفحه‌ی مدیریتی Horizon شوید و از قسمت Settings بر روی Servers کلیک کنید و در صفحه‌ی باز شده وارد تب Vcenter Servers شوید و بر روی Add کلیک کنید.



شکل ۱۶- ۱۱۹ اتصال vCenter به Horizon

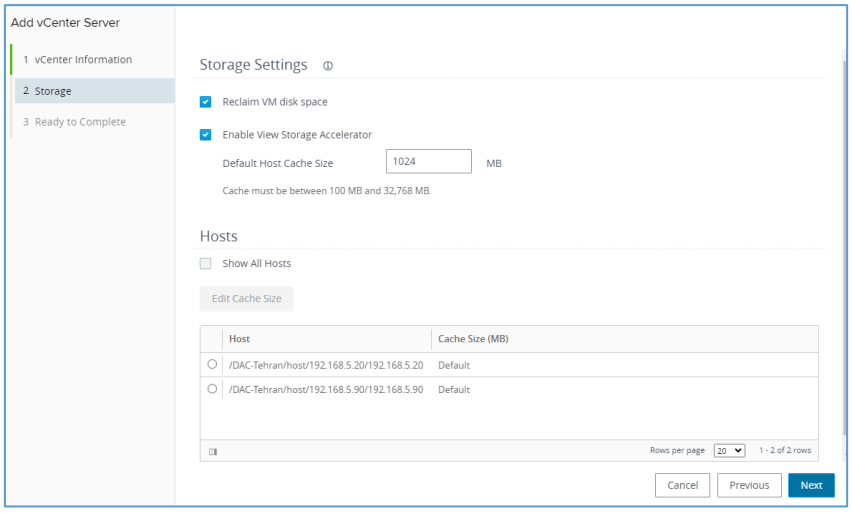
www.takbook.com

در شکل ۱۶-۱۲۰، آدرس سرور Vcenter را وارد کنید و در قسمت Username باید همان کاربری که را که در Vcenter به آن دسترسی دادیم تعریف کنیم و بر روی next کلیک کنیم.



شکل ۱۶- ۱۲۰ اتصال vCenter به Horizon

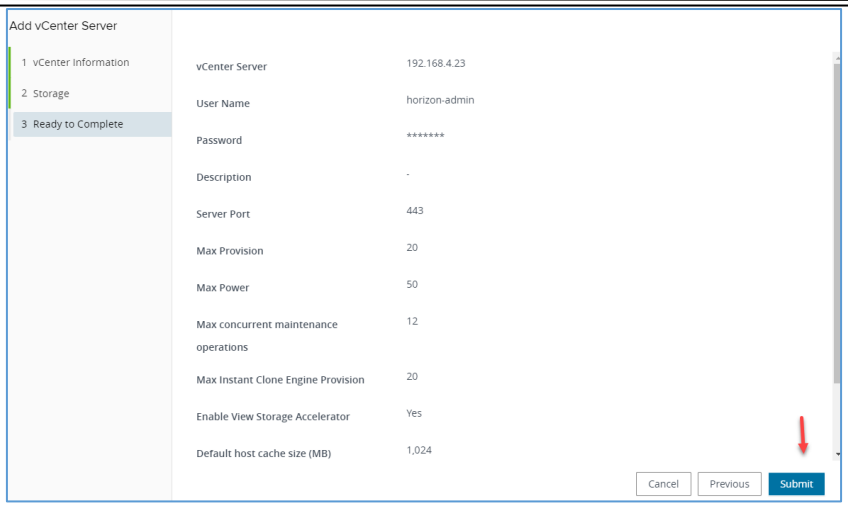
شکل ۱۶-۱۲۱، مربوط به فضای ذخیره‌سازی است و نیازی به تغییر گزینه‌ای نیست و بر روی Next کلیک کنید.



شکل ۱۶- ۱۲۱ اتصال vCenter به Horizon

در شکل ۱۶-۱۲۲، بر روی Submit کلیک کنید تا Vcenter به لیست اضافه شود.

www.takbook.com



شکل ۱۶- ۱۲۲ اتصال vCenter به Horizon

www.takbook.com

فصل هفدهم

امنیت شبکه

۱۷-۱ مفاهیم امنیتی

ایجاد امنیت در شبکه کار آسانی نیست. همواره باید مراقب باشید تا اطلاعات شما افشا نشود یا شبکه‌تان مورد حمله قرار نگیرد. با این حال، می‌توانید با پیاده‌سازی راه‌حل‌های امنیتی مناسب، این تهدیدات را به حداقل برسانید. برای این منظور، لازم است تهدیدات را شناسایی کرده و اقدامات لازم برای پیشگیری از آن‌ها را به‌درستی اجرا کنید.

اگر امنیت شبکه برای شما اهمیت دارد، باید از مجموعه‌ای از قواعد پیروی کنید تا با مشکلات مواجه نشوید. این قواعد شامل سه هدف اصلی است: محرمانگی (Confidentiality)، یکپارچگی (Integrity) و دردسترس‌بودن (Availability) که به اختصار CIA نامیده می‌شوند. بیشتر مشکلات امنیتی شبکه در یکی از این سه بخش قرار می‌گیرند. بنابراین، باید تلاش کنید دانش و دیدگاه خود را در این زمینه‌ها گسترش دهید.

۱۷-۲ بررسی شرایط امنیتی

در این بخش، به بررسی ریسک‌های شبکه می‌پردازیم. این ریسک‌ها می‌توانند شامل تهدیداتی باشند که امنیت، عملکرد و دسترسی‌پذیری شبکه را به خطر می‌اندازند. شناسایی و تحلیل این ریسک‌ها اولین گام برای طراحی راهکارهای مناسب جهت کاهش آسیب‌ها است.



شکل ۱۷- ۱ شرایط امنیتی

برخی از مهم‌ترین ریسک‌های شبکه عبارت‌اند از:

www.takbook.com

منابع یا دارایی‌های سازمان (Assets)

منابع یا دارایی‌های سازمان (Assets) به تمام موارد با ارزشی اشاره دارد که برای سازمان اهمیت حیاتی دارند و باید از آن‌ها محافظت شود. این دارایی‌ها می‌توانند فیزیکی، دیجیتالی یا حتی انسانی باشند. اهمیت این منابع از این جهت است که از دست دادن آن‌ها می‌تواند به عملیات، امنیت و حتی اعتبار سازمان آسیب وارد کند.

در جدول ۱۷-۱، منابع موجود را مشاهده می‌کنید.

جدول ۱۷- ۱ منابع یا دارایی‌های سازمان

منابع فیزیکی	تجهیزات شبکه (سوئیچ‌ها، روترها، سرورها) ساختمان‌ها و زیرساخت‌ها سخت‌افزارها و دستگاه‌های ذخیره‌سازی
منابع دیجیتالی	داده‌ها: اطلاعات مشتریان، گزارش‌ها، پایگاه‌های داده نرم‌افزارها: سیستم‌های عملیاتی، برنامه‌های کاربردی
منابع انسانی	دانش و مهارت‌های کارکنان مدیران و متخصصان

آسیب پذیری (Vulnerability)

نقص یا ضعف در طراحی، پیاده‌سازی، بهره‌برداری یا مدیریت یک سیستم می‌تواند مورد سوءاستفاده قرار گیرد و سیاست امنیتی سیستم را نقض کند.

به طور کلی، مهاجمان از آسیب‌پذیری‌هایی که ممکن است در نرم‌افزار، سخت‌افزار یا حتی نیروی انسانی سازمان وجود داشته باشد، برای حمله به شبکه بهره‌برداری می‌کنند. امروزه بیشتر سازمان‌ها با انجام ارزیابی‌های جامع، سعی در شناسایی و رفع این آسیب‌پذیری‌ها دارند.

طبقه‌بندی آسیب‌پذیری‌ها به صورت زیر بیان می‌شود:

- Policy flaws (نقص در سیاست سازمان)
- Design errors (طراحی اشتباه)
- Protocol weaknesses (ضعف در پروتکل)
- Misconfiguration (تنظیمات اشتباه)
- Software vulnerabilities (آسیب‌پذیری نرم‌افزار)
- Human factors (عوامل انسانی)

www.takbook.com

■ Malicious software (نرم‌افزارهای مخرب)

■ Hardware vulnerabilities (آسیب‌پذیری سخت‌افزاری)

■ Physical access to network resources (دسترسی فیزیکی به منابع شبکه)

تهدیدات (Threat)

تهدیدات زمانی رخ می‌دهد که مهاجم در بخش قبلی (**Vulnerability**)، آسیب‌پذیری‌های یک سیستم را شناسایی کند و بتواند از آن طریق به شبکه ما ضربه بزند، یک مثال ساده در این بخش، می‌تواند به اشتراک گذاشتن یک پوشه با دسترسی اشتباه باشد.

عامل تهدید (Threat agent)

عامل تهدید، کسی است که تهدیدات را به وجود می‌آورد، مثلاً مهاجمی که از ACL یا همان Access List اشتباه استفاده می‌کند می‌تواند عامل تهدید باشد که این عامل‌ها می‌توانند آسیب‌پذیری‌ها را شناسایی و از آنها برای حمله به شبکه استفاده کنند، البته همه عامل‌ها این کار را انجام نمی‌دهند.

ریسک (Risk)

احتمال یک خطر است که توسط یک عامل تعدید (Threat agent) از طریق پیدا کردن یک آسیب‌پذیری در شبکه به وجود می‌آید، کاهش ریسک‌های یک شبکه بسته به سیاست‌هایی دارد که مدیر شبکه پیاده‌سازی می‌کند.

روش‌هایی که در اقدام متقابل می‌توان از آنها استفاده کرد شامل موارد زیر است:

۱- اجرایی (Administrative) که شامل استانداردها، رویه‌ها، دستورالعمل‌ها و سیاست‌های سازمان است که باید به صورت کتبی از همه کاربران تعهد گرفت تا خلاف آن عمل نکنند.

۲- فیزیکی (Physical) شامل کنترل‌های فیزیکی دقیق برای تجهیزات شبکه خود است، مثلاً می‌توانید برای اتاق سرور خود از درب‌های ضد سرقت پیشرفته و نسوز استفاده کنید و یا اینکه برای رک‌های دیواری که در هر طبقه موجود هستند را قفل کنید، طراحی باید به صورتی باشد که کاربران به هیچ قطعه یا سیمی دسترسی نداشته باشند.

۳- منطقی (Logical) که شامل کنترل‌های منطقی شامل گذرواژه‌ها ، فایروال‌ها ، سیستم‌های پیشگیری از نفوذ، لیست‌های دسترسی ، تونل‌های VPN و... کنترل‌های منطقی اغلب به عنوان فنی گفته می‌شوند، کنترل می‌کند.

در معرض قرار گرفتن (Exposure)

www.takbook.com

وقتی که به یک پوشه به اشتراک گذاشته شده یک دسترسی اشتباه می‌دهید، آن پوشه در معرض تهدیدات قرار خواهد گرفت و امنیت شرکت را زیر سوال خواهد برد.

اقدام متقابل (Countermeasure)

اقدام متقابل، ریسک‌های یک شبکه را کاهش خواهد داد، برای انجام یک کار در شبکه سه موضوع آسیب‌پذیری، تهدیدات و ریسک باید مورد توجه قرار گیرد تا بتوان اقدام متقابل را برای آنها انجام داد.

فرآیند مدیریت ریسک (Risk Management Process)

فرآیند مدیریت ریسک شامل یک سرس عملیات است که عبارتند از:

- ✓ شناسایی کردن منابع و ارزش‌های سازمان
- ✓ شناسایی تهدیدات
- ✓ شناسایی آسیب‌پذیری
- ✓ تعیین احتمال حمله
- ✓ شناسایی ضربه
- ✓ تعیین ریسک به عنوان ترکیبی از احتمال و تاثیر.

طبقه‌بندی منابع (Asset Classification)

اولین قدم در ارزیابی ریسک‌ها شناسایی منابع و ارزش‌های آن سازمان است، دارایی‌هایی که در یک سازمان وجود دارد مشهود و غیر مشهود است که این دارایی‌های مشهود عبارتند از:
کاربران، کامپیوترها، امکانات و منابع، ولی دارایی‌های غیر مشهود شامل مالکیت معنوی داده‌ها و شهرت سازمانی است.

۳-۱۷ شناخت تهدیدات شبکه فعلی

تهدیدات امروز به طور مداوم در حال تغییر هستند و تهدیدهای جدیدی ظهور می‌کند، در این قسمت می‌خواهیم به دسته‌های مختلف تهدیدات شبکه بپردازیم:

۱-۳-۱۷ مهاجمان نهایی (Potential Attackers)

این اصطلاح به افرادی یا گروه‌هایی اشاره دارد که ممکن است به دلایل مختلف اقدام به حمله به شبکه، سیستم‌ها یا اطلاعات کنند. مهاجمان می‌توانند انگیزه‌های متنوعی داشته باشند، از سود مالی و رقابت گرفته تا خرابکاری یا ایجاد بی‌ثباتی. در ادامه برخی از انواع مهاجمان نهایی آورده شده است:

- هکرها (Hackers)

www.takbook.com

- افراد یا گروه‌هایی که با استفاده از دانش فنی خود به دنبال نفوذ به شبکه‌ها و سیستم‌ها هستند. هکرها ممکن است با نیت تخریب، سرقت اطلاعات یا حتی برای آزمایش مهارت‌های خود عمل کنند.
- تروریست‌ها (Terrorists)

گروه‌هایی که از حملات سایبری به‌عنوان ابزاری برای ضربه زدن به زیرساخت‌های حیاتی یا ایجاد وحشت استفاده می‌کنند.

- کارکنان ناراضی (Disgruntled Employees)

افرادی درون یک سازمان که به دلیل نارضایتی از محیط کار، مدیریت یا سایر مسائل اقدام به نفوذ یا آسیب رساندن به منابع داخلی می‌کنند.

- رقبای تجاری (Competitors)

شرکت‌ها یا افراد رقیب که ممکن است از جاسوسی صنعتی یا نفوذ به شبکه برای کسب مزیت رقابتی استفاده کنند.

- خریداران داده‌ها (Data Brokers)

افرادی که به دنبال سرقت اطلاعات حساس برای فروش به دیگران یا استفاده از آن برای سود مالی هستند.

- فعالان سایبری (Hacktivists)

گروه‌هایی که برای حمایت از یک آرمان یا اعتراض به سیاست‌ها و تصمیمات خاص، حملات سایبری انجام می‌دهند.

- مجرمان سازمان‌یافته (Organized Crime)

گروه‌های حرفه‌ای که با هدف سرقت اطلاعات مالی، هویت یا انجام فعالیت‌های کلاهبردارانه اقدام به نفوذ می‌کنند.

- افراد کنجکاو یا آماتور (Script Kiddies)

کسانی که دانش محدودی در زمینه نفوذ دارند و از ابزارهای آماده برای امتحان کردن یا ایجاد اختلال استفاده می‌کنند.

www.takbook.com

۲-۳-۱۷ روش‌های حمله (Attack Methods)

هکرها معمولاً از روش‌ها و تکنیک‌های پیچیده برای نفوذ به شبکه‌ها و سیستم‌ها استفاده می‌کنند و در عین حال تلاش می‌کنند که هویت و ردپای خود را مخفی نگه دارند. برخی از این روش‌ها شامل موارد زیر هستند:

- استفاده از بدافزارها (Malware)

شامل ویروس‌ها، تروجان‌ها، کی‌لاگرها و باج‌افزارها که به سیستم‌ها نفوذ کرده و داده‌ها را سرقت یا خراب می‌کنند.

- حملات مهندسی اجتماعی (Social Engineering)

فریب کاربران برای افشای اطلاعات محرمانه یا اجرای دستورات مخرب، مانند حملات فیشینگ یا تماس‌های تلفنی جعلی.

- تکنیک‌های اسکن و شناسایی (Scanning and Reconnaissance)

هکرها ابتدا شبکه و سیستم‌ها را اسکن می‌کنند تا آسیب‌پذیری‌ها و نقاط ضعف را شناسایی کنند.

- حملات بی‌رحمانه (Brute Force Attacks)

تلاش برای شکستن رمز عبور یا کلیدهای رمزنگاری با امتحان کردن تمام ترکیب‌های ممکن.

- تزریق کد (Code Injection)

شامل روش‌هایی مانند SQL Injection و Command Injection برای نفوذ به برنامه‌ها و پایگاه‌های داده.

- جاسوسی بسته‌ها (Packet Sniffing)

نظارت بر ترافیک شبکه برای دسترسی به اطلاعات حساس مانند رمز عبور و پیام‌ها.

- مخفی‌سازی (Obfuscation)

استفاده از تکنیک‌هایی برای پنهان کردن بدافزارها یا ردپای حملات، مانند رمزگذاری فایل‌های مخرب.

- استفاده از کانال‌های مخفی (Covert Channels)

انتقال اطلاعات یا کنترل سیستم‌ها از طریق کانال‌های پنهان که شناسایی آن‌ها دشوار است.

- حملات DDoS (Distributed Denial of Service)

ارسال حجم عظیمی از ترافیک به سرور یا شبکه برای مختل کردن خدمات و ایجاد از کار افتادگی.

- استفاده از آسیب‌پذیری‌های روز صفر (Zero-Day Exploits)

www.takbook.com

بهره‌برداری از ضعف‌های ناشناخته یا بدون وصله در نرم‌افزارها و سیستم‌ها.

- مهاجرت از یک سیستم به سیستم دیگر (Lateral Movement)

نفوذ اولیه به یک سیستم و سپس گسترش دسترسی به سایر سیستم‌ها در شبکه.

- استفاده از حساب‌های کاربری دزدیده‌شده

بهره‌گیری از اطلاعات ورود سرقت‌شده برای دسترسی به سیستم‌ها و داده‌ها.

۱۷-٤ راه‌های حمله (Attack Vector)

مهاجمان می‌توانند از چندین مسیر مختلف به شبکه یک سازمان نفوذ کنند. این مسیرها یا راه‌های حمله، به‌نوعی دروازه‌های ورودی به سیستم‌ها و داده‌ها هستند. همان‌طور که اشاره کردید، حملات لزوماً از بیرون سازمان انجام نمی‌شود و گاهی مهاجمین می‌توانند از داخل سازمان به شبکه نفوذ کنند. در ادامه، برخی از مهم‌ترین راه‌های حمله آورده شده است:

- حملات داخلی (Insider Attacks):پ

افراد داخل سازمان، مانند کارکنان ناراضی یا کاربرانی که به اشتباه به اطلاعات حساس دسترسی پیدا کرده‌اند، می‌توانند به شبکه حمله کنند. این افراد می‌توانند از اطلاعات درون‌سازمانی برای نفوذ یا تخریب استفاده کنند.

- درب‌های پشتی (Backdoors)

درب‌های پشتی راه‌هایی هستند که به‌طور عمدی یا به‌وسیله آسیب‌پذیری‌ها ایجاد می‌شوند و به مهاجم این امکان را می‌دهند که به سیستم وارد شود، بدون اینکه شناسایی شود. این درب‌های پشتی ممکن است در نرم‌افزارها یا تجهیزات شبکه به‌صورت مخفیانه فعال شوند.

- حملات فیشینگ (Phishing)

هکرها ممکن است با ارسال ایمیل‌های جعلی به کارمندان تلاش کنند تا اطلاعات حساس مانند نام کاربری، رمز عبور یا اطلاعات کارت اعتباری را سرقت کنند. کاربر ممکن است از روی بی‌اطلاعی وارد یک وب‌سایت مخرب شود و اطلاعات خود را فاش کند.

- حملات از طریق دستگاه‌های متصل (Connected Devices)

دستگاه‌های متصل به شبکه مانند چاپگرها، دوربین‌ها، دستگاه‌های IoT و حتی تلفن‌های همراه می‌توانند به‌عنوان یک نقطه نفوذ عمل کنند. مهاجم می‌تواند از این دستگاه‌ها برای دسترسی به شبکه استفاده کند.

- حملات مبتنی بر ضعف‌های نرم‌افزاری (Software Vulnerabilities)

www.takbook.com

استفاده از آسیب‌پذیری‌های شناخته‌شده یا روز صفر در نرم‌افزارها برای نفوذ به سیستم‌ها. این ضعف‌ها می‌توانند به مهاجم این امکان را دهند که به‌راحتی به سیستم‌های داخلی دسترسی پیدا کند.

- حملات از طریق شبکه‌های بی‌سیم (Wireless Networks)

شبکه‌های بی‌سیم، به‌ویژه اگر به‌درستی محافظت نشوند، ممکن است یک راه آسیب‌پذیر برای حمله به شبکه‌های داخلی باشند. هکرها ممکن است به راحتی با استفاده از ابزارهای مناسب به شبکه‌های Wi-Fi نفوذ کنند.

- حملات از طریق رسانه‌های قابل حمل (Removable Media)

دستگاه‌هایی مانند USBها، دیسک‌ها یا کارت‌های حافظه می‌توانند به‌عنوان وسیله‌ای برای انتقال بدافزار یا اطلاعات دزدیده‌شده استفاده شوند.

- حملات از طریق سرویس‌های ابری (Cloud Services)

خدمات ابری که در دسترس کارکنان یا تیم‌های مختلف هستند، ممکن است به‌عنوان نقطه‌ای برای نفوذ یا دزدیدن اطلاعات حساس استفاده شوند.

۱۷-۵ استفاده از اصول اساسی امنیت در شبکه

در این بخش رویکردهایی برای بهبود شبکه مشخص شده است که می‌تواند از مواردی که در بالا بیان کردیم پیشگیری کند.

۱۷-۵-۱ محرمانه بودن (Confidentiality)

محرمانه بودن یکی از اصول اصلی امنیت اطلاعات است که هدف آن جلوگیری از دسترسی غیرمجاز به اطلاعات حساس است. برای حفظ محرمانه بودن، باید اطمینان حاصل کنید که تنها افراد مجاز به داده‌ها و اطلاعات حساس دسترسی داشته باشند و از افشای اطلاعات به بیرون سازمان جلوگیری شود.

برای ایجاد محرمانه بودن و کنترل سطح دسترسی، سه اصل اصلی وجود دارد که باید به‌طور دقیق پیاده‌سازی شوند:

شناسایی (Identification)

شناسایی فرآیندی است که در آن سیستم یا سازمان کاربر را شناسایی می‌کند و او را به‌عنوان یک کاربر خاص در شبکه یا سیستم مشخص می‌کند. این فرآیند معمولاً با استفاده از شناسه کاربری (username) انجام می‌شود.

www.takbook.com

احراز هویت (Authentication)

احراز هویت فرایندی است که در آن سیستم بررسی می‌کند که آیا فرد شناسایی شده، همان کسی است که ادعا می‌کند. این فرآیند معمولاً با استفاده از اطلاعاتی مانند رمز عبور، اثر انگشت، یا تایید دو مرحله‌ای انجام می‌شود.

مجوز دسترسی (Authorization)

پس از احراز هویت، سیستم باید مشخص کند که فرد، مجاز به انجام چه عملیاتی است. این عملیات شامل تعیین سطح دسترسی به منابع مختلف سیستم یا شبکه است، به‌طوری‌که هر کاربر تنها به منابعی که برای انجام وظایفش لازم است دسترسی داشته باشد.



شکل ۱۷- ۲ محرمانه بودن

۲-۵-۱۷ یکپارچگی (Integrity)

یکپارچگی به معنی حفظ صحت و کامل بودن داده‌ها است. هدف اصلی یکپارچگی داده‌ها این است که از تغییرات غیرمجاز، دستکاری یا حذف اطلاعات جلوگیری شود. این امر برای اطمینان از اینکه داده‌ها در طول زمان دقیق و معتبر باقی می‌مانند، ضروری است.

برای اطمینان از یکپارچگی، سه مرحله اصلی که قبلاً ذکر شد، یعنی شناسایی (Identification)، احراز هویت (Authentication) و مجوز دسترسی (Authorization)، نقش کلیدی ایفا می‌کنند. این سه مرحله به شما کمک می‌کنند تا:

- شناسایی (Identification): فرد یا سیستم‌های دخیل در تعامل با داده‌ها شناسایی شوند.
- احراز هویت (Authentication): اطمینان حاصل کنید که تنها افراد یا سیستم‌های معتبر و شناخته‌شده مجاز به دسترسی به داده‌ها هستند.
- مجوز دسترسی (Authorization): مشخص می‌کند که هر کاربر یا سیستم مجاز به انجام چه اقداماتی روی داده‌ها است.

www.takbook.com



فصل ۱۷- ۳ یکپارچگی

۳-۵-۱۷ در دسترس بودن (Availability)

در دسترس بودن به معنای اطمینان از این است که اطلاعات و منابع شبکه به‌طور مداوم و بدون وقفه در دسترس کاربران مجاز قرار گیرند، به‌ویژه زمانی که به آن‌ها نیاز دارند. این اصل به‌طور خاص بر تضمین عملکرد صحیح سیستم‌ها و خدمات در تمام مدت زمان فعالیت تأکید دارد.

هدف از در دسترس بودن این است که حتی در شرایط بحرانی یا پس از حملات سایبری، سیستم‌ها و داده‌ها از دسترس خارج نشوند. این شامل ذخیره‌سازی داده‌ها، دسترسی به آن‌ها و خدمات آنلاین است.

برای اطمینان از در دسترس بودن، روش‌ها و تکنیک‌های مختلفی باید پیاده‌سازی شوند، از جمله:

- پشتیبان‌گیری (Backup)

انجام پشتیبان‌گیری منظم از داده‌ها و سیستم‌ها به‌منظور بازیابی سریع در صورت بروز مشکل یا خرابی.

- حفاظت در برابر حملات (Protection Against Attacks)

استفاده از فایروال‌ها، سیستم‌های تشخیص و جلوگیری از نفوذ (IDS/IPS)، و سایر ابزارهای امنیتی برای جلوگیری از حملات DDoS یا سایر تهدیدات که ممکن است در دسترس بودن سیستم‌ها را مختل کنند.

- مراقبت از سخت‌افزار و نرم‌افزار:

نظارت مداوم بر سلامت سخت‌افزارها و نرم‌افزارها و استفاده از روش‌های تعمیر و نگهداری مناسب برای جلوگیری از خرابی‌ها.

- طراحی مقاوم (Fault Tolerant Design)

www.takbook.com

پیاده‌سازی معماری‌هایی که از خرابی سیستم جلوگیری کرده و در صورت بروز مشکل، سیستم به‌طور خودکار به حالت عملیاتی بازگردد.

- مقیاس‌پذیری (Scalability)

طراحی سیستم‌ها به‌گونه‌ای که قادر باشند با افزایش تعداد کاربران یا حجم داده‌ها بدون کاهش عملکرد، همچنان در دسترس باقی بمانند.

در دسترس بودن نه‌تنها به‌طور مستقیم به عملکرد شبکه و سیستم‌ها مربوط می‌شود، بلکه از جنبه‌های امنیتی نیز اهمیت دارد. اگر سیستمی همیشه در دسترس نباشد، می‌تواند به فرصت مناسبی برای مهاجمان تبدیل شود و منجر به مشکلاتی برای سازمان شود.

۱۷-۶ تعاریف اولیه در امنیت اطلاعات

۱۷-۶-۱ کمترین امتیاز (Least Privilege)

مفهوم کلی این تعریف در مورد این است که به هر کسی به اندازه‌ی نیازش دسترسی بدهید، که این موضوع می‌تواند برای یک کاربر باشد و یا یک فرآیند، برای فعال کردن حداقل‌ها، باید سازمان‌ها تمامی کارکردهای کاربران را شناسایی و بر اساس آن دسترسی‌ها را اولویت‌بندی کنند تا کسی بیشتر از نیاز خود به منابع شبکه دسترسی نداشته باشد.

یک سری قوانین سازمانی وجود دارد که از اصل کمترین امتیاز (Least Privilege) حمایت می‌کنند:

۱- تعداد اکانت‌هایی که دارای مجوزهای زیاد در شبکه هستند را محدود کنید.

۲- مدیران شبکه باید از یک اکانت با دسترسی معمولی برای عملیات معمول خود استفاده کنند.

۳- دسترسی‌ها ابزاری محبوب برای مهاجم‌ها هستش که باید دقت لازم در این زمینه را داشته باشیم و آن را محدود کنیم.

۱۷-۶-۲ دسترسی به هیچ چیز (Access to Nothing)

سعی کنید به صورت پیش‌فرض دسترسی‌ها را برای همه کاربرانی که برای اولین بار به شبکه متصل می‌شوند ببندید، این کار یکی از بهترین عملکردهای امنیتی محسوب خواهد شد که افراد ناشناس نتوانند به راحتی به شبکه دسترسی داشته باشند.

۱۷-۶-۳ دفاع در عمق (Defense in Depth)

استراتژی دفاع از عمق به این موضوع اشاره دارد که برای ایجاد امنیت باید از چند لایه‌ی امنیتی برای رسیدن به اطلاعات استفاده کرد، یکی از این استراتژی‌ها استفاده از کنترل دسترسی‌ها در شبکه است.

www.takbook.com

۱۷-۶-٤ تفکیک وظایف (Separation of Duties)

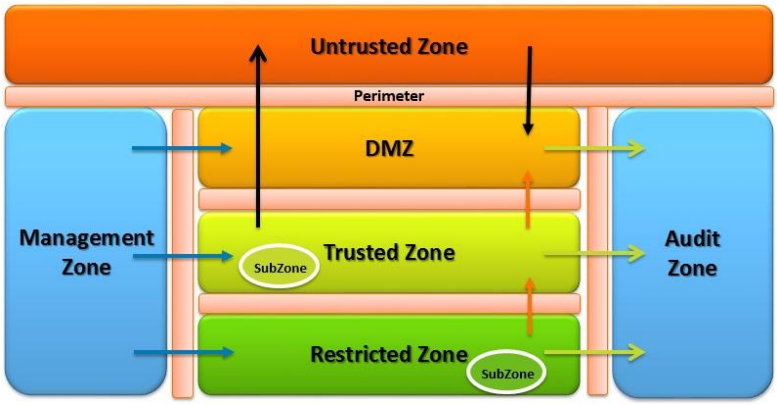
برای کاربران باید وظایف مشخص معین شود و هر کسی وظایف مربوط به خود را انجام دهد، با این کار از تقلب در کارها جلوگیری خواهد شد، مثلاً می‌توانیم برای یک کار که قرار است انجام شود دو مدیر تعیین کنیم تا هر دو مجوز آن کار را صادر کنند و با یک نفر آن کار انجام نشود.

۱۷-۶-۵ چرخش کار (Job Rotation)

در این بخش باید آموزش‌های لازم داده شود تا از انجام تقلب جلوگیری شود، در چرخش کار باید یک نسخه از اطلاعات شبکه داشته باشیم.

۱۷-۷ مناطق امنیتی مشترک شبکه

مناطق امنیتی شبکه به بخش‌های مختلف یک شبکه اطلاق می‌شود که بر اساس سطح امنیتی و نیازهای خاص سازمان، به‌طور منطقی تقسیم‌بندی شده‌اند. این مناطق به‌طور معمول برای کنترل و مدیریت دسترسی به منابع شبکه و اطلاعات حساس استفاده می‌شوند. با تقسیم‌بندی شبکه به مناطق امنیتی مختلف، می‌توان امنیت را بهتر مدیریت کرده و به مهاجمین امکان دسترسی به تمام بخش‌ها را محدود کرد. در شکل ۱۷-٤، برخی از مناطق امنیتی متداول در شبکه‌ها بررسی شده است:



شکل ۱۷- ۴ مناطق امنیتی مشترک شبکه

۱۷-۷-۱ منطقه DMZ

یک زیرشبکه منطقی یا فیزیکی است که اطلاعات شبکه داخلی را به بیرون از سازمان یعنی فضای اینترنت ارسال می‌کند، هدف از یکDMZ ، اضافه کردن یک لایه امنیتی بیشتر به شبکه محلی یک سازمان است؛ یک مهاجم خارجی به جای دیگر قسمت‌های شبکه، تنها به تجهیزاتی که در DMZ هستند دسترسی دارد و با این کار خطرات ناشی از دسترسی غیرمجاز به شبکه اصلی کاهش پیدا خواهد کرد، DMZ فقط و فقط

www.takbook.com

برای جلوگیری از دسترسی افراد به شبکه داخلی (Intranet) و یا همان محلی است و اگر مهاجمی از داخل شبکه بخواهد جاسوسی کند، نمی‌تواند کاری انجام دهد، بهترین راه استفاده از این نوع شبکه‌ها استفاده از یک دستگاه Firewall برای جدا کردن سه شبکه Internet، DMZ و Intranet است.

۱۷-۷-۲ منطقه Interanet

Intranet به شبکه‌ی داخلی اشاره می‌کند که به عنوان یک شبکه خصوصی شناخته می‌شود و در این شبکه می‌توان هر نوع پروتکلی را اجرا و استفاده کرد، در این نوع شبکه‌ها به مانند شبکه اینترنت می‌توانید سرورهای ایمیل، وب، FTP و دیگر پروتکل‌ها را پیاده‌سازی کرد، این نوع شبکه‌های با استفاده از فایروال‌ها محافظت می‌شود و کسی نمی‌توانید بدون اجازه به آن دست پیدا کند.

۱۷-۷-۳ منطقه Extranet

Extranet بخشی از یک شبکه خصوصی است که مدیران شبکه‌ی یک سازمان برای متصل شدن کاربران خارج از سازمان به شبکه از روش‌های امنی استفاده می‌کنند تا کاربران بر روی سیستم خارجی خود مانند سیستم داخل منزل یا جایی دیگر شبکه داخلی آن سازمان را داشته باشند، یکی از روش‌های پیاده‌سازی این نوع شبکه‌ها فعال‌سازی پروتکل VPN است که این کار را با امنیت کامل و سریع انجام می‌دهد.

۱۷-۷-٤ منطقه شفاف (Transparent Zone)

این ناحیه معمولاً به‌طور شفاف و بدون دخالت خاص از دیگر بخش‌ها عمل می‌کند. این منطقه ممکن است شامل تجهیزات و زیرساخت‌هایی باشد که نیاز به امنیت سطح پایین‌تری دارند و به‌طور معمول برای ارتباطات ساده و موقت طراحی می‌شوند.

۱۷-۷-۵ منطقه اعتماد (Trusted Zone)

این منطقه شامل بخش‌هایی از شبکه است که به‌طور کامل به شبکه داخلی اعتماد دارند و دسترسی به آن‌ها محدود به کاربران یا دستگاه‌های خاص است. این منطقه معمولاً دسترسی به منابع حساس مانند پایگاه‌های داده یا سرورهای اصلی سازمان را فراهم می‌کند.

www.takbook.com

۱۷-۷-٦ منطقه با دسترسی محدود (Restricted Zone)

این ناحیه به‌طور خاص برای داده‌های حساس یا سیستم‌های حیاتی طراحی شده است که نیاز به سطح امنیتی بالایی دارند. دسترسی به این منطقه به‌شدت محدود است و تنها افراد یا سیستم‌های خاص با مجوز می‌توانند به آن وارد شوند.

۱۷-۷-۸ منطقه VPN (Virtual Private Network)

این منطقه شامل شبکه‌ای است که از طریق تونل‌های امن VPN به شبکه داخلی متصل می‌شود. شبکه VPN معمولاً برای اتصال کاربرانی که از راه دور به شبکه دسترسی دارند، طراحی می‌شود. امنیت این منطقه از طریق رمزگذاری و احراز هویت شدید محافظت می‌شود.

۱۷-۸ طراحی شبکه و چشم‌انداز تهدیدات امنیتی

در این قسمت، هدف بررسی اصول طراحی شبکه و شناسایی تهدیدات امنیتی است که می‌تواند بر شبکه‌ها تاثیر بگذارد. این دو موضوع در کنار هم به مدیران شبکه کمک می‌کنند تا طراحی بهینه‌تری داشته باشند و در عین حال تهدیدات امنیتی احتمالی را در نظر بگیرند و اقدامات پیشگیرانه‌ای را برای مقابله با آن‌ها اتخاذ کنند.

۱۷-۸-۱ شبکه محوطه دانشگاه یا Campus-Area Network (CAN)

شبکه محوطه دانشگاه یا Campus-Area Network (CAN)، شبکه‌ای است که معمولاً در محیط‌های بزرگ مانند دانشگاه‌ها، مراکز تحقیقاتی، شرکت‌های بزرگ یا هر مجموعه‌ای که نیاز به اتصال و ارتباط میان ساختمان‌های متعدد دارد، ایجاد می‌شود. این شبکه به‌طور خاص برای اتصال سیستم‌ها، سرورها، رایانه‌ها، و سایر تجهیزات در چندین ساختمان یا محل در یک منطقه جغرافیایی محدود طراحی شده است.

ویژگی‌ها و ساختار شبکه CAN:

- محدوده جغرافیایی: CAN معمولاً در یک محوطه محدود مانند یک دانشگاه، پارک صنعتی یا کمپانی با چندین ساختمان پراکنده در یک منطقه جغرافیایی خاص (مثلاً چند کیلومتر مربع) برقرار می‌شود. این شبکه در مقایسه با شبکه‌های بزرگتر مانند WAN (شبکه‌های گسترده) محدودتر است اما از شبکه‌های LAN (شبکه محلی) نیز وسیع‌تر می‌باشد.
- اتصال بین ساختمان‌ها: شبکه CAN برای برقراری ارتباط میان ساختمان‌های مختلف در یک محوطه دانشگاهی یا صنعتی استفاده می‌شود. این ارتباط می‌تواند از طریق کابل‌های فیبر نوری،

www.takbook.com

کابل‌های مسی (Ethernet)، ارتباطات بی‌سیم یا حتی فناوری‌های جدیدتر مانند 5G یا Wi-Fi انجام گیرد.

- مدیریت مرکزی: در شبکه‌های CAN، معمولاً یک مرکز داده مرکزی (Data Center) برای مدیریت و نظارت بر تمامی خدمات و تجهیزات موجود در شبکه استفاده می‌شود. این مرکز می‌تواند سرورها، تجهیزات ذخیره‌سازی و سایر منابع زیرساختی را در خود داشته باشد که از یک نقطه متمرکز مدیریت می‌شوند.
- عملکرد و مقیاس‌پذیری: شبکه CAN باید از عملکرد بالا و مقیاس‌پذیری مناسبی برخوردار باشد تا بتواند تعداد زیادی دستگاه و کاربر را در سطح دانشگاه یا سازمان پشتیبانی کند. برای این منظور، طراحی و پیاده‌سازی مناسب زیرساخت‌های شبکه و مدیریت ترافیک شبکه ضروری است.

مزایای شبکه CAN

- مقیاس‌پذیری بالا

قابلیت گسترش شبکه به سادگی با اضافه کردن تجهیزات جدید مانند سوئیچ‌ها، روترها و نقطه‌های دسترسی جدید.

- قابلیت مدیریت و نظارت متمرکز

از آنجا که همه تجهیزات در یک منطقه جغرافیایی متمرکز هستند، مدیریت شبکه و نظارت بر آن به‌طور متمرکز آسان‌تر است.

- بهره‌وری از منابع مشترک

کاربران می‌توانند به راحتی از منابع مشترک مانند سرورها، چاپگرها و دیتابیس‌ها استفاده کنند که هزینه‌ها را کاهش می‌دهد.

- امنیت بالا

با وجود اینکه شبکه CAN محدوده جغرافیایی خاصی را پوشش می‌دهد، امکان اعمال سیاست‌های امنیتی دقیق و بهینه‌سازی شده برای کنترل دسترسی به منابع مختلف فراهم است.

۲-۸-۱۷ شبکه Wide-Area Network (WAN)

شبکه WAN به‌طور عمومی به شبکه‌هایی اطلاق می‌شود که نواحی جغرافیایی وسیعی را پوشش می‌دهند. این شبکه‌ها معمولاً از طریق تکنولوژی‌های مختلف ارتباطی مانند خطوط اجاره‌ای، فیبر نوری، ماهواره و رادیو در فواصل دور به هم متصل می‌شوند. شبکه WAN برای ارتباط دفاتر و شعب مختلف یک سازمان یا شرکت، ارتباط میان مراکز داده یا حتی ارتباط میان کشورها و قاره‌ها به‌کار می‌رود.

www.takbook.com

ویژگی‌ها و مزایای شبکه WAN

- پوشش جغرافیایی وسیع: WAN قادر است چندین شهر، کشور یا قاره را به هم متصل کند. این شبکه‌ها برای سازمان‌هایی که دفاتر مختلف در مکان‌های جغرافیایی دور از هم دارند ضروری است.
- ارتباطات سریع و امن: شبکه WAN از خطوط ارتباطی امن و سریع برای انتقال داده‌ها استفاده می‌کند. ارتباطات میان شعب یا مراکز مختلف شرکت از طریق WAN می‌تواند به‌صورت پیوسته و بدون قطعی انجام گیرد.
- انتقال داده‌های بزرگ: WAN امکان انتقال حجم‌های بالای داده میان دفاتر و مراکز مختلف را فراهم می‌آورد. این امکان برای سازمان‌هایی که نیاز به دسترسی به منابع مشترک یا انتقال اطلاعات حساس دارند، حیاتی است.
- استفاده از تکنولوژی‌های مختلف: WAN می‌تواند از فناوری‌های مختلفی مانند MPLS (Multiprotocol Label Switching)، VPN (Virtual Private Network)، و حتی ارتباطات ماهواره‌ای استفاده کند.

۳-۸-۱۷شبکه Data Center

Data Center یا مرکز داده به مجموعه‌ای از تجهیزات سخت‌افزاری و نرم‌افزاری اطلاق می‌شود که برای ذخیره‌سازی، مدیریت، و پردازش حجم زیادی از داده‌ها و اطلاعات طراحی شده است. شبکه Data Center به شبکه‌ای گفته می‌شود که تمامی دستگاه‌ها، سرورها، ذخیره‌سازها، تجهیزات شبکه و منابع دیگر را در مرکز داده به هم متصل کرده و ارتباط بین این اجزا را امکان‌پذیر می‌سازد. این شبکه باید بتواند حجم بالای داده‌ها را در زمان‌های مختلف پردازش کند و به‌طور مداوم و بدون قطعی عملکرد مطلوبی داشته باشد.

اجزای اصلی شبکه Data Center

- سرورها (Servers): سرورها در Data Center به پردازش داده‌ها و ارائه خدمات مختلف به کاربران و دستگاه‌ها پرداخته و معمولاً در یک چیدمان سازمان‌یافته در رک‌ها قرار دارند.
- دستگاه‌های ذخیره‌سازی (Storage Devices): تجهیزات ذخیره‌سازی داده‌ها مانند SAN (Storage Area Network) و NAS (Network Attached Storage) برای ذخیره‌سازی اطلاعات و دسترسی سریع به داده‌ها استفاده می‌شود.

www.takbook.com

- تجهیزات شبکه (Networking Equipment): سوئیچ‌ها، روترها و فایروال‌ها برای برقراری ارتباط بین سرورها، دستگاه‌های ذخیره‌سازی و سایر تجهیزات Data Center ضروری هستند. این تجهیزات معمولاً برای افزایش سرعت و امنیت ارتباطات استفاده می‌شوند.
- سیستم‌های خنک‌کننده (Cooling Systems): به دلیل مصرف بالای انرژی و تولید گرمای زیاد، سیستم‌های خنک‌کننده برای حفظ دمای مطلوب در Data Center ضروری هستند.
- منبع تغذیه بی‌وقفه (UPS): برای جلوگیری از قطعی برق و محافظت از تجهیزات در برابر نوسانات برق، از سیستم‌های UPS (Uninterruptible Power Supply) استفاده می‌شود.

ویژگی‌ها و اهمیت شبکه Data Center

- پایداری و قابلیت اطمینان: Data Center باید از پایداری بالایی برخوردار باشد. این مرکز داده باید قادر به ارائه خدمات به‌طور مستمر و بدون توقف باشد. به همین دلیل معمولاً از طراحی‌هایی مانند نوار قرمز و حفاظت از داده‌ها برای جلوگیری از قطعی و از دست دادن داده‌ها استفاده می‌شود.
- مقیاس‌پذیری: شبکه Data Center باید مقیاس‌پذیر باشد تا بتواند به‌راحتی منابع مورد نیاز را بر اساس حجم کاری متغیر افزایش یا کاهش دهد.
- دسترسی سریع به داده‌ها: داده‌ها باید به سرعت و به‌صورت موثر در داخل Data Center منتقل شوند. شبکه‌های با سرعت بالا و اتصالات سریع میان سرورها و دستگاه‌های ذخیره‌سازی برای کارایی بالا و کاهش زمان تأخیر اهمیت دارند.
- امنیت داده‌ها: امنیت در Data Center از اهمیت زیادی برخوردار است. اطلاعات ذخیره شده باید از حملات خارجی، هکرها و تهدیدات داخلی محافظت شوند. این امر نیازمند استفاده از فایروال‌ها، سیستم‌های شناسایی و پیشگیری از نفوذ (IDS/IPS)، رمزنگاری و سیاست‌های دسترسی مناسب است.

۱۷-۸-٤ شبکه‌های Small office/Home office

شبکه‌های Small Office/Home Office (SOHO) به شبکه‌هایی اطلاق می‌شود که معمولاً در محیط‌های کاری کوچک مانند دفاتر کوچک (small offices) یا دفاتر خانگی (home offices) ایجاد می‌شوند. این شبکه‌ها برای کاربران با نیازهای محدود و حجم کار کم طراحی شده‌اند، اما همچنان نیاز به اتصال به اینترنت و تبادل داده‌های محلی دارند.

www.takbook.com

۵-۸-۱۷ امنیت شبکه برای یک محیط مجازی

در دنیای امروز، بسیاری از سازمان‌ها و شرکت‌ها به سمت استفاده از محیط‌های مجازی (Virtualized Environments) می‌روند تا بهره‌وری و مقیاس‌پذیری شبکه خود را افزایش دهند. در این محیط‌ها، ماشین‌های مجازی (VM)، شبکه‌های مجازی (Virtual Networks) و ذخیره‌سازی مجازی برای اجرای برنامه‌ها و خدمات مورد استفاده قرار می‌گیرند. با این حال، در کنار مزایای بسیاری که این فناوری‌ها به همراه دارند، تهدیدات امنیتی جدیدی نیز ایجاد می‌کنند. بنابراین، امنیت شبکه در یک محیط مجازی اهمیت ویژه‌ای دارد.

چالش‌های امنیتی در محیط‌های مجازی:

- جداسازی ماشین‌های مجازی (VM Isolation): در محیط‌های مجازی، ممکن است چندین ماشین مجازی (VM) روی یک سرور فیزیکی اجرا شوند. اگر یک ماشین مجازی به‌طور موفقیت‌آمیز هک شود، مهاجم می‌تواند دسترسی به ماشین‌های مجازی دیگر را نیز پیدا کند. بنابراین، اطمینان از جدا بودن مناسب این ماشین‌ها از یکدیگر ضروری است.
- مدیریت دسترسی و احراز هویت: دسترسی به ماشین‌های مجازی، سرورها و منابع شبکه باید محدود به افراد مجاز شود. این موضوع شامل استفاده از روش‌های احراز هویت چندعاملی (MFA) و همچنین سیاست‌های کنترل دسترسی مبتنی بر نقش (RBAC) است تا از دسترسی غیرمجاز جلوگیری شود.
- تهدیدات حملات به Hypervisor: Hypervisor (ماشین‌ساز مجازی) نرم‌افزاری است که ماشین‌های مجازی را مدیریت می‌کند. حملات به Hypervisor می‌توانند تهدیداتی برای تمام ماشین‌های مجازی موجود در آن ایجاد کنند. بنابراین، تأمین امنیت Hypervisor به همان اندازه که برای ماشین‌های مجازی مهم است، اهمیت دارد.
- امنیت شبکه مجازی (Virtual Network Security): در محیط‌های مجازی، شبکه‌های مجازی به طور مداوم و دینامیک ایجاد و حذف می‌شوند. این وضعیت می‌تواند باعث ایجاد چالش‌هایی برای شناسایی و کنترل ترافیک شبکه شود. حفاظت از شبکه‌های مجازی و نظارت بر ترافیک بین ماشین‌های مجازی بسیار مهم است.
- مدیریت پیکربندی و به‌روزرسانی‌ها: محیط‌های مجازی نیاز به پیکربندی و به‌روزرسانی مداوم دارند. هرگونه خطا در پیکربندی یا عدم انجام به‌روزرسانی‌های امنیتی می‌تواند منجر به ایجاد آسیب‌پذیری‌هایی در سیستم‌ها شود. این مسئله به ویژه در محیط‌های بزرگ‌تر که از ماشین‌های مجازی و زیرساخت‌های پیچیده استفاده می‌کنند، بیشتر نمود پیدا می‌کند.

www.takbook.com

- تهدیدات مبتنی بر ذخیره‌سازی: ذخیره‌سازی داده‌ها در محیط‌های مجازی باید با دقت مدیریت شود. داده‌های حساس که در ماشین‌های مجازی ذخیره می‌شوند باید رمزگذاری شوند و اطمینان حاصل شود که تنها افراد مجاز به این داده‌ها دسترسی دارند.

۹-۱۷چشم انداز تهدید امنیتی شبکه

تهدیدات امنیتی امروزه بسیار گسترده و پیچیده‌تر شده است، در این قسمت سعی کریدم در مورد انگیزه‌های مهاجمان برای حمله به شبکه، افرادی که مورد حمله قرار می‌گیرند و چگونگی جلوگیری از حملات صحبت کنیم.

انگیزه‌های مهاجمان برای حمله به شبکه شما چیست؟

- مالی (Financial): یکی از مهمترین دلایل اینکه مهاجمان به شبکه‌های مختلف حمله می‌کنند، این است که بتوانند از منابع مالی آن سازمان استفاده کنند، مانند هک کردن سایت‌های بانکی و به سرقت بردن اطلاعات هزاران کاربر و استراخ از آن.

- اختلال (Disruption): در اکثر موارد مهاجم فقط برای ایجاد اختلال در شبکه شروع به هک کردن سایت یا سرور مورد نظر می‌کند؛ که دلایل مختلفی هم دارد، مثلاً کاربر مورد نظر برای اینکه خود را مطرح کند شروع به هک کردن سایت می‌کند و با قرار دادن اطلاعات خود در صفحه سایت خود را مطرح می‌کند.

- ژئوپلیتیک (Geopolitical): در این نوع حملات که به جنگ سایبری معروف است، گروهی از هکرها به سرورها مهم یک کشور حمله می‌کنند تا آنها را از کار بیندازند.

۱-۹-۱۷ بررسی حملات انکار سرویس

این نوع حملات با نام DOS (Denial-of-Service) و DDOS (Distributed Denial-of-Service) شناخته می‌شود که اصولاً برای از کار انداختن سرور یا سرورها به کار می‌رود، تلاش این نوع حملات برای از کار انداختن سرویس‌های تحت وب مانند هاستینگ و... است که با این کار سایت مورد حمله برای دقایقی یا برای همیشه از کار خواهد افتاد، تفاوت بین حمله DOS با DDOS این است که حمله DOS از طریق یک سیستم انجام می‌شود ولی حمله DDOS که به عنوان حمله توزیع شده شناخته می‌شود با استفاده از چندین سرور انجام می‌گیرد، با این کار روترها، سوئیچ‌ها و دیگر دستگاه‌ها متصل به شبکه با افزایش درخواست‌ها مواجه می‌شوند و همین موضوع باعث می‌شود کارایی CPU افزایش یابد و دستگاه از کار بیفتد.

روش‌های حمله:

www.takbook.com

۱- تداخل در ارتباط کاربران با شبکه.
۲- ریسیت کردن کانکشن‌های TCP در ارتباط‌ها.
۳- ایجاد تداخل در دستگاه‌های شبکه.
۴- ایجاد اختلال در وضعیت روترها مانند اطلاعات مسیریابی.
۵- مصرف حداکثری منابع مانند پهنای باند، دیسک و...

۱۷-۹-۲ بررسی روش‌های مهندسی اجتماعی

یکی از بهترین راه‌های ایجاد نفوذ به شبکه سازمان استفاده از منابع انسانی آن است، در این نوع حملات هکرها با استفاده از روش‌هایی، اطلاعات مهم یک سازمان را از کاربران آن بدست می‌آورند، مانند جعل آدرس ایمیل، پنجره‌های Pop-Ip در وب‌سایت‌ها، ساخت وب‌سایت‌های جعلی و از همه مهمتر کلاهبرداری از طریق تلفن است.

چگونه باید در برابر این نوع حملات دفاع کرد:

۱- مدیریت کامل رمزهای عبور با استفاده از سیاست‌ها پیچیدگی رمز عبور و تاریخ انقضاء آن، البته نرم‌افزارهایی مانند ACS می‌توانند بسیار کمک کننده باشند، در مورد ACS در ادامه توضیح جامع خواهیم داد.
۲- استفاده از احراز هویت دوعاملی.
۳- استفاده از آنتی ویروس‌ها و ضدفیشینگ‌ها.
۴- طبقه‌بندی اطلاعات حساس و غیرحساس.
۵- محافظت از زباله‌های اداری که دو ریخته می‌شود.
۶- استفاده از نگهبانان امنیتی برای محافظت از سازمان.

۱۷-۱۰ روش های موجود برای شناسایی بد افزار

۱- Packet captures: برای شناسایی بدافزار باید جمع‌آوری، ذخیره و تجزیه و تحلیل بسته‌هایی که در شبکه در حال رد و بدل هستند را انجام دهید، البته به علت حجم بالای اطلاعات پیدا کردن آنها بسیار سخت خواهد بود.
۲- Snort: یک سیستم شناسایی هوشمند است که یک نرم‌افزار منبع باز بوده و توسط شرکت Sourcefire توسعه یافته است و اکنون بخشی از شرکت سیسکو است و در حال حاضر با نام (IPS , IDS) شناخته می‌شود، این سیستم برای جلوگیری از تهدیدات، شناسایی، اجرای سیاست‌های لازم و.... کاربر دارد.

www.takbook.com

۳- NetFlow: یکی از پروتکل‌های اختصاصی شرکت سیسکو است که آن را برای عیب‌یابی، مانیتورینگ و برای بدست آوردن داده‌های آماری ایجاد کرده است، یکی از مهمترین دلایل استفاده از این سیستم برای جلوگیری از حملاتی است که به شبکه شما انجام می‌شود.

۴- بررسی رویدادهای IPS: دستگاه‌های IPS برای شناسایی حملات کاربرد دارند و بسته‌های عبوری در شبکه را بررسی می‌کنند، از IPS برای ارتباط دو شبکه در دو نقطه مختلف می‌توان استفاده کرد تا Wormها و دیگر ابزارهای مخرب شناسایی شوند.

۵- حفاظت از بدافزار پیشرفته: در این بخش شرکت سیسکو AMP را طراحی کرده که در دستگاه‌های FirePOWER به کار گرفته شده است، این سیستم از نفوذ پیشگیری می‌کند و حتی فایل‌های درون شبکه را هم بررسی می‌کند تا در صورت وجود فایل‌های مخرب و تهدیدها آنها را شناسایی کند.

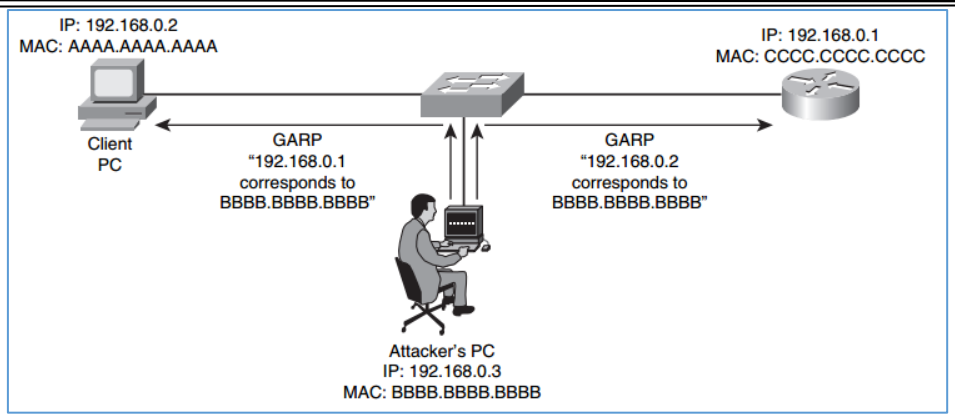
۶- سیستم جلوگیری از نفوذ نسل بعدی (Cisco FirePOWER (NGIPS : راه‌حل چند لایه محافظت پیشرفته در بازرسی را فراهم می‌کند که این محصول در دستگاه‌های ASA که در ادامه کار بررسی می‌کنیم ارائه می‌شود.

۱۱-۱۷تحلیل و بررسی Dynamic Arp Inspection

پروتکل ARP که مخفف کلمه‌ی Address Resolution Protocol است، برای تبدیل آدرس IP (لایه‌ی شبکه) به آدرس MAC (لایه‌ی پیوند داده) کاربرد دارد، که این پروتکل یک پروتکل ضروری برای لایه‌ی اینترنت است.

به علت اینکه پروتکل ARP بیشترین کاربرد را دارد، مهاجم‌ها با روش‌های غیرقانونی سعی در دور زدن آن دارند. در شکل ۱۷-۵، سیستم "Client PC " را مشاهده می‌کنید که با روتر پیش‌فرض آن 192.168.0.1 است و اطلاعات را با این روتر رد و بدل می‌کند، اگر در این بین یک سیستم مهاجم با نام " Attacker's PC" وجود داشته باشد، برای اینکه خود را به جای سیستم " Client PC " به روتر معرفی کند، با ارسال پیام‌های ARP (GRAP) هم به کلاینت و هم به روتر خود را در وسط کار قرار می‌دهد، مثلاً در این شکل "Attacker's PC " آدرس مک خود را به جای آدرس مک روتر "BBBB.BBBB.BBBB" جا می‌زند و این کار باعث می‌شود که سیستم مورد نظر اطلاعات خود را به مهاجم ارسال کند و به همین ترتیب مهاجم با دستکاری در آن اطلاعات را به سمت روتر مورد نظر خود ارسال می‌کند؛ این نوع حملات با نام ARP spoofing شناخته می‌شوند و از نوع man-in-the-middle است.

www.takbook.com



شکل ۱۷- ۵ بررسی *Dynamic Arp Inspection*

توجه داشته باشید که GRAP که به اختصار به نام Gratuitous Address Resolution Protocol شناخته می‌شود کمکی برای شناسایی آدرس IP تکراری در شبکه است که این کار را با ارسال Broadcast در شبکه انجام می‌دهد، باارسال broadcast سیستم‌هایی که در شبکه قرار دارند اگر به این پیغام پاسخ دهند یعنی اینکه آدرس مورد نظر متعلق به آنها است و نمی‌توان از آن استفاده کرد.

۱۷-۱۲ بررسی Port Security

در این قسمت می‌خواهیم روش امنیتی Port Security را بر روی سوئیچ‌های سیسکو راه اندازی کنیم، مثالی که برا این روش میتوان زد این است که اگر شبکه سازمان خود را در نظر بگیرید و کاربران شما بخواهند از منابع شبکه در سیستمی استفاده کند که عضو آن شبکه نیست و واقعاً می‌تواند برای شبکه شما بسیار بد و یک ضعف امنیتی بزرگ باشد، اگر کاربر کابل شبکه متصل شده به سوئیچ را به لپ تاپ شخصی خود متصل کند، می‌تواند به منابع شبکه دسترسی پیدا کند.

اما شرکت سیسکو برای جلوگیری از دزدیده شدن اطلاعات به این شکل روشی را تهت عنوان Port Security در سوئیچ‌های خود اضافه کرده که اگر چنانچه کاربری از یک سیستم غیر مجاز برای متصل شدن به شبکه استفاده کند، پورت مربوط به آن سیستم در سوئیچ خاموش خواهد شد و فقط و فقط توسط مدیر شبکه روشن می‌شود.

اهداف و ویژگی‌های Port Security

- محدود کردن دسترسی به پورت‌ها: با استفاده از Port Security، می‌توان محدودیت‌هایی برای تعداد دستگاه‌هایی که می‌توانند به یک پورت سوئیچ متصل شوند، ایجاد کرد. این ویژگی می‌تواند از حملات مبتنی بر دسترسی غیرمجاز به شبکه جلوگیری کند.

www.takbook.com

- مقابله با حملات MAC Spoofing: یکی از اهداف اصلی Port Security جلوگیری از حملات MAC Spoofing است. در این حملات، مهاجم سعی می‌کند آدرس MAC خود را تغییر دهد تا مانند یک دستگاه معتبر به شبکه متصل شود. Port Security می‌تواند فقط آدرس‌های MAC مشخص‌شده را روی هر پورت اجازه دهد و ترافیک سایر آدرس‌های MAC را مسدود کند.
- کنترل تعداد آدرس‌های MAC: Port Security به شما این امکان را می‌دهد که تعداد آدرس‌های MAC مجاز را در هر پورت تعیین کنید. به‌عنوان مثال، می‌توانید تنظیم کنید که فقط یک آدرس MAC مجاز در یک پورت وجود داشته باشد، و اگر دستگاه جدیدی با آدرس MAC متفاوت به پورت متصل شود، دسترسی قطع شود.
- حالت‌های مختلف واکنش: Port Security می‌تواند در صورت شناسایی یک دستگاه غیرمجاز به پورت، به‌طور خودکار یک اقدام خاص انجام دهد. سه حالت رایج وجود دارد:
  Protect دستگاه‌های غیرمجاز مسدود می‌شوند، ولی هیچ پیامی به مدیر شبکه ارسال نمی‌شود.
  Restrict دستگاه‌های غیرمجاز مسدود می‌شوند و پیامی به مدیر شبکه ارسال می‌شود.
  Shutdown پورت به‌طور کامل غیرفعال می‌شود و هیچ ترافیکی از آن عبور نمی‌کند.
- ثبت و مانیتورینگ: Port Security به شما این امکان را می‌دهد که تمامی رویدادهای امنیتی مانند شناسایی دستگاه‌های غیرمجاز و تغییرات در آدرس‌های MAC را ثبت کنید. این اطلاعات می‌توانند به شناسایی تهدیدات و حملات شبکه کمک کنند.

۱۳-۱۷ بررسی CoPP

Control Plane Policing (CoPP) یکی از روش‌های مدیریت ترافیک در شبکه است که به‌ویژه برای محافظت از پلن کنترل (Control Plane) در دستگاه‌های شبکه مانند روترها و سوئیچ‌ها استفاده می‌شود. پلن کنترل به اجزای شبکه‌ای مانند پروتکل‌های مسیریابی و تنظیمات کنترل دستگاه‌ها اشاره دارد که مدیریت و تنظیمات اولیه شبکه را انجام می‌دهند. اگر این بخش از شبکه تحت حملات قرار گیرد، می‌تواند عملکرد شبکه را مختل کند. CoPP برای جلوگیری از این نوع حملات و مدیریت ترافیک ورودی به پلن کنترل به کار می‌رود.

ویژگی‌های CoPP

- اولویت‌بندی ترافیک: CoPP امکان اولویت‌بندی ترافیک را به روتر یا سوئیچ می‌دهد. این امر به این معناست که ترافیک ضروری برای عملکرد صحیح دستگاه، مانند ترافیک پروتکل‌های مسیریابی (RIP, OSPF, BGP) و تنظیمات دستگاه، باید در اولویت قرار گیرد.

www.takbook.com

- کنترل دسترسی به Control Plane: CoPP به شما این امکان را می‌دهد که فقط ترافیک خاصی را به پلن کنترل اجازه دهید، در حالی که سایر ترافیک‌ها را مسدود می‌کند. این امر از حملات DOS یا حملات دیگر که قصد دارند منابع پلن کنترل را اشغال کنند، جلوگیری می‌کند.
- محافظت از منابع حساس: منابعی مانند جدول مسیریابی، پروتکل‌های مسیریابی و سرویس‌های مدیریتی می‌توانند هدف حملات و سوءاستفاده قرار گیرند. CoPP از این منابع محافظت می‌کند و عملکرد دستگاه را تحت فشار قرار نمی‌دهد.
- اعمال سیاست‌های امنیتی: با استفاده از CoPP، می‌توانید سیاست‌های مختلفی برای ترافیک ورودی به دستگاه‌های شبکه تعریف کنید، به طوری که هر نوع ترافیک غیرمجاز یا مشکوک مسدود شود.

روش‌های پیاده‌سازی CoPP

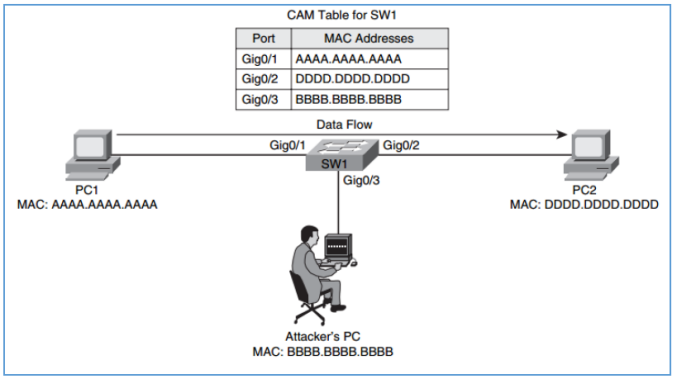
- استفاده از Access Control Lists (ACLs): برای محدود کردن ترافیک ورودی به Control Plane، می‌توان از ACLs استفاده کرد. ACLها ترافیک شبکه را بر اساس آدرس‌های IP، پروتکل‌ها یا پورت‌ها فیلتر می‌کنند.
- سیستم‌های Queue و Class Maps: در این روش، می‌توان با استفاده از کیوها (Queues) و کلاس‌های خاص (Class Maps)، ترافیک مختلف را شبیه‌سازی کرده و از آن‌ها برای اولویت‌بندی یا محدودسازی استفاده کرد.
- Rate Limiting: در این روش، می‌توان محدودیت‌هایی برای نرخ ترافیک ورودی به پلن کنترل اعمال کرد تا از حملات با حجم بالا جلوگیری شود.
- Policing: Policing به معنای محدود کردن نرخ ترافیک در پلن کنترل است. اگر ترافیک ورودی از حد مجاز بیشتر شود، بر اساس سیاست‌های CoPP، ترافیک اضافی ممکن است رها شده یا از سیستم حذف شود.

۱۷-۱٤ تحلیل و بررسی Spoofing MAC Addresses

همان‌طور که می‌دانید آدرس MAC یک آدرس منحصر به فرد می‌باشد و برای هر دستگاه یک آدرس در نظر گرفته خواهد شد، نوع دیگری از حمله جعل کردن آدرس Mac است که در زیر این روش را بررسی خواهیم کرد.

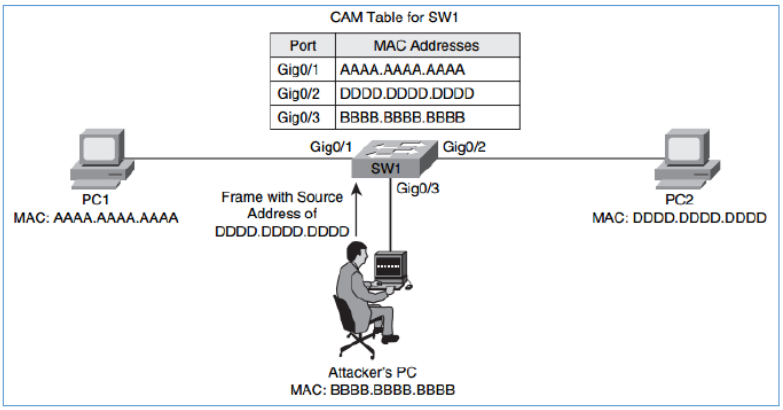
در شکل ۱۷-٦، سه سیستم را مشاهده می‌کنید که به سوئیچ متصل شده‌اند و آدرس MAC آنها در جدول سوئیچ ثبت شده است.

www.takbook.com



شکل ۱۷-۶ سناریو *Spoofing MAC Addresses*

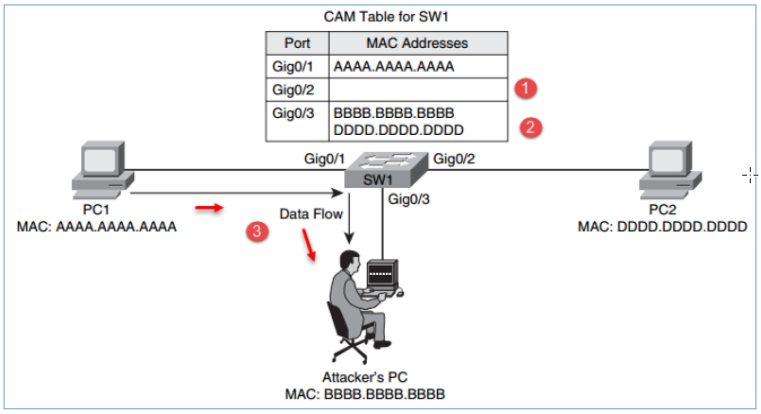
در شکل ۱۷–۷، سیستم "Attacker's Pc " با ارسال یک Frame در شبکه آدرس مک جعلی خود یعنی DDDD.DDDD.DDDD که مربوط به PC2 است را به سوئیچ اعلام می‌کند، سوئیچ هم در زمان مشخص شده جدول خود را آپدیت می‌کند و با این کار ترافیکی که قبل از آن به سیستم PC2 ارسال می‌شد به سمت سیستم Attacker's ارسال می‌شود و با این روش اطلاعات به خطر خواهد افتاد.



شکل ۱۷-۷ سناریو *Spoofing MAC Addresses*

همان‌طور که در شکل ۱۷–۸، مشاهده می‌کنید، در قسمت اول در جدول سوئیچ آدرس MAC در پورت Gig0/2 که قبلاً به PC2 متصل شده بود خالی شده است و به جای آن در قسمت دوم پورت Gig0/3 دارای دو آدرس MAC است که یکی از آنها آدرس MAC جعلی مربوط به PC2 است و در قسمت شماره‌ی سه تمام ترافیک به روتر مهاجم ارسال خواهد شد.

www.takbook.com



شکل ۱۷-۸ سناریو *Spoofing MAC Addresses*

www.takbook.com

فصل هجدهم

برنامه‌نویسی پایتون در شبکه

زبان برنامه‌نویسی پایتون (Python) یکی از پرکاربردترین و محبوب‌ترین زبان‌های برنامه‌نویسی در دنیای امروز است. دلایل زیادی برای این محبوبیت وجود دارد که باعث می‌شود پایتون انتخاب اول بسیاری از برنامه‌نویسان و توسعه‌دهندگان نرم‌افزار باشد. در ادامه، ویژگی‌ها و دلایل استفاده از پایتون را توضیح می‌دهم:

ساده و خوانا بودن سینتکس (Syntax)

پایتون به خاطر ساده و خوانا بودن سینتکس آن معروف است. به عبارت دیگر، قواعد نگارشی و نحوه نوشتن کد در پایتون به زبان طبیعی انسان نزدیک است، به طوری که افراد تازه‌کار به راحتی می‌توانند آن را یاد بگیرند و کدهای آن را متوجه شوند.

مثال:

```
print("Hello, World!")
```

این کد به راحتی پیام "Hello, World!" را چاپ می‌کند.

در مجموع، پایتون به دلیل سادگی، تنوع کاربرد و جامعه کاربری بزرگ، یکی از بهترین گزینه‌ها برای یادگیری و استفاده در برنامه‌نویسی است.

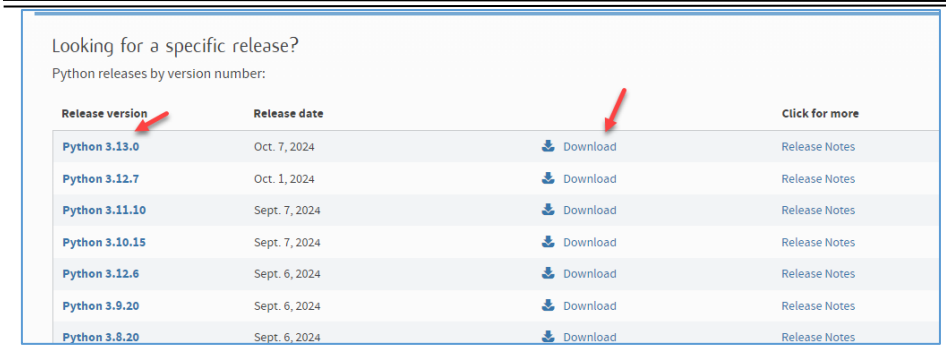
پایتون در زمینه شبکه (Networking) نقش بسیار مهمی ایفا می‌کند و ابزارها و کتابخانه‌های مختلفی برای برنامه‌نویسی شبکه ارائه می‌دهد. این زبان به دلیل سادگی و قدرتمندی خود، گزینه مناسبی برای ساختن و مدیریت برنامه‌های شبکه‌ای است.

توجه داشته باشید در این فصل نحوه‌ی استفاده از کدهای پایتون برای دستگاه‌ها و نرم‌افزار شبکه مورد بررسی قرار می‌گیرد و خود آموزش برنامه نویسی از صفر را باید بلد باشید، ولی نگران نباشید کار با این کدها بسیار آسان خواهد بود.

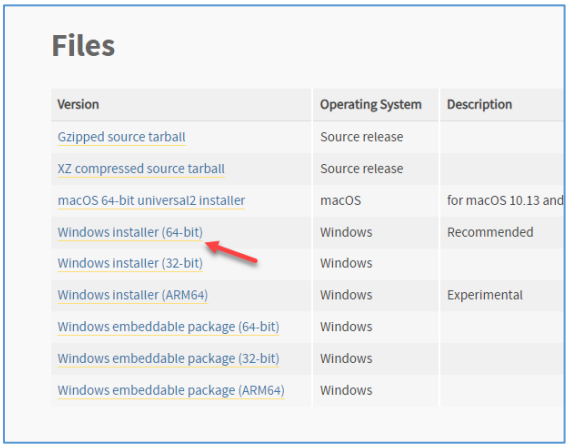
در حال حاضر آخرین ورژن نرم‌افزار پایتون 3.13.0 است که به صورت رایگان می‌توانید از لینک زیر آن را برای ویندوز و یا دیگر سیستم‌عامل‌ها دانلود کنید، که این موضوع را در شکل ۱۸-۱ و ۱۸-۲، مشاهده می‌کنید.

https://www.python.org/downloads/

www.takbook.com

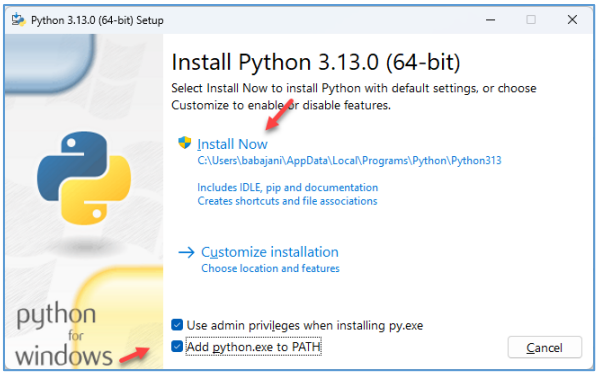


شکل ۱۸- ۱ دانلود پایتون



شکل ۱۸- ۲ دانلود پایتون

بعد از دانلود، فایل را اجرا کنید و به مانند شکل ۱۸-۳، تیک گزینه‌ی Add Python 3.8 to PATH را انتخاب کنید و بر روی Install Now کلیک کنید.



شکل ۱۸- ۳ نصب پایتون

www.takbook.com

نصب نرم‌افزار به سادگی انجام خواهد شد و بعد از نصب می‌توانید برنامه را به صورت تکی و یا در CMD اجرا کنید، در ادامه می‌خواهیم نحوه‌ی برنامه‌نویسی در شبکه را بیاموزیم.

۱-۱۸ سوکت چیست

سوکت (Socket) یک نقطه ارتباطی است که به دو سیستم اجازه می‌دهد تا به یکدیگر متصل شوند و داده‌ها را از طریق شبکه انتقال دهند. در واقع، سوکت‌ها رابط‌هایی بین برنامه‌های نرم‌افزاری و شبکه هستند که به آنها امکان می‌دهند تا داده‌ها را ارسال و دریافت کنند. این ارتباط می‌تواند بین دستگاه‌های مختلف یا بین برنامه‌های مختلف در یک دستگاه صورت گیرد.

سوکت‌ها معمولاً با ترکیب آدرس IP (برای مشخص کردن دستگاه) و شماره پورت (برای مشخص کردن برنامه یا سرویس) شناخته می‌شوند. به عنوان مثال، یک سوکت می‌تواند به این صورت باشد: 192.168.1.10:80 که در آن 192.168.1.10 آدرس IP دستگاه و 80 شماره پورت است.

انواع سوکت‌ها شامل موارد زیر می‌شود:

سوکت‌های استریم (TCP Socket): از پروتکل TCP استفاده می‌کنند و برای ارتباطات پایدار و قابل اعتماد مناسب هستند.

سوکت‌های دیتاگرام (UDP Socket): از پروتکل UDP استفاده می‌کنند و برای ارتباطات سریع‌تر ولی بدون تضمین تحویل، مناسب هستند.

سوکت‌ها به طور گسترده در برنامه‌های شبکه‌ای مانند مرورگرهای وب، سرویس‌های ایمیل، و سایر اپلیکیشن‌های تحت شبکه استفاده می‌شوند.

اگر بخواهیم درباره سوکت بحث کنیم باید بگوییم که چندین نوع سوکت در دسترس است که بیتشرین آنها دو نوع Connection Oriented و Connection Less هستند، نوع اول Connection Oriented هستند که به سوکت‌های Stream معروفند، که مبتنی بر پروتکل TCP است، یعنی اینکه قبل از مبادله اطلاعات باید یک اتصال مطمئن برقرار شود که اطلاعات به صورت درست و با امنیت به مقصد برسد، از این نوع سوکت برای ارتباط پروتکل‌هایی همانند FTP، HTTP وSMTP استفاده می‌شود. در سوکت Connection Less که به سوکت‌های Datagram معروفند و مبتنی بر پروتکل UDP هستند، یعنی اینکه قبل از مبادله اطلاعات هیچ امنیتی بین دو مبدأ و مقصد برقرار نمی‌شود و فقط سرعت در این ارتباط مهم است، از این نوع سوکت بیشتر برای انتقال صدا و تصویر استفاده می‌کنند.

متداول‌ترین نوع برنامه‌های سوکت، برنامه‌های مبتنی بر مشتری-سرور (client-server) است که در آن یک طرف به عنوان سرور عمل می‌کند و منتظر ارتباط از طریق مشتری است.

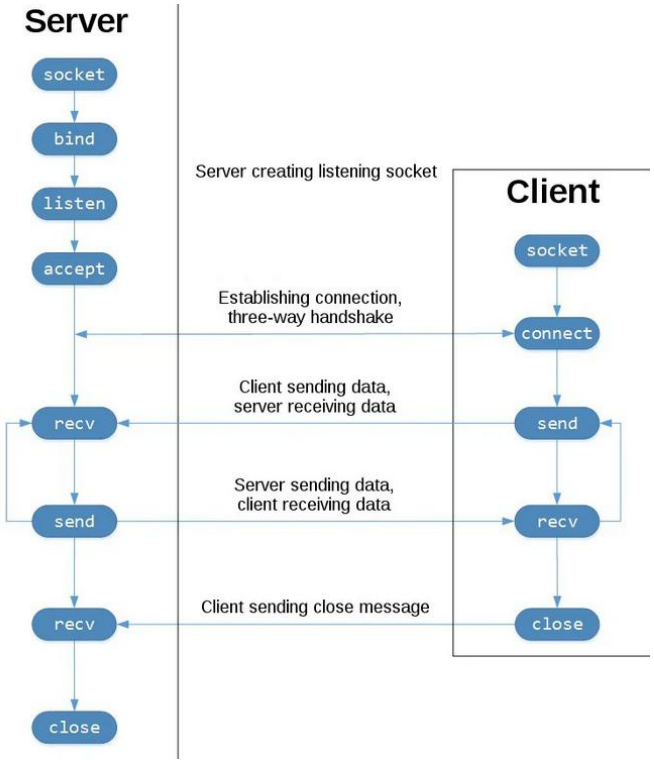
www.takbook.com

زبان برنامه‌نویسی پایتون دارای ماژول‌های بسیار گسترده‌ای است، در بخش شبکه هم دو ماژول Socket و Scapy بیشترین کاربرد را دارد و در این قسمت از آموزش از آنها استفاده خواهیم کرد.

در زیر توابع اصلی Socket API را مشاهده می‌کنید که هر کدام از آنها برای امر خاصی طراحی شده‌اند:

- `socket()`
- `bind()`
- `listen()`
- `accept()`
- `connect()`
- `connect_ex()`
- `send()`
- `recv()`
- `close()`

در شکل ۱۸-٤، نحوه ایجاد توابع را در پایتون مشاهده می‌کنید که کلاینت و سرور برای ایجاد ارتباط به چه صورت عمل می‌کنند.



شکل ۱۸- ۴ بررسی سوکت در پایتون

www.takbook.com

بررسی ماژول Socket

برای ایجاد یک سوکت می‌توانید از تابع socket.socket() استفاده کنید، که دستور کلی آن به صورت زیر است:

```
import socket
s= socket.socket (socket_family, socket_type, protocol=0)
```

در دستور بالا، با استفاده از import ماژول Socket صدا زده شد و در ادامه برای ایجاد سوکت باید از تابع socket.socket استفاده کرد که خود این تابع دارای چند قسمت است:

- socket_family: آدرس و پروتکل مورد نظر را نشان می‌دهد.
- socket_type : نوع سوکت را نمایش می‌دهد که می‌تواند SOCK_STREAM یا SOCK_DGRAM باشد.
- protocol : این مورد اختیاری است و معمولا به صورت پیش‌فرض مقدار آن صفر است.

برای اینکه بیشتر با این تابع آشنا شویم، یک مثال را با هم بررسی می‌کنیم:

برای اجرای یک کد ساده پایتون در شبکه می‌خواهیم یک پورت را در سرور صدا بزنیم و کلاینت به آن پورت متصل شود، به معنای ساده‌تر باید یک سوکت بر روی پورت فعال کنیم تا به حالت LISTENING برود و بعد یک کلاینت به این پورت پاسخگو خواهد بود.
اولین کد را در سمت سرور وارد می‌کنیم، توجه داشته باشید برای راحتی کار شما سرور و کلاینت را در یک سیستم قرار دادیم تا بتوانیم به صورت سریع این موضوع را تست بگیریم.

```
import socket

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

s.bind(("192.168.4.102", 83))
s.listen(1)
connection, client = s.accept()
```

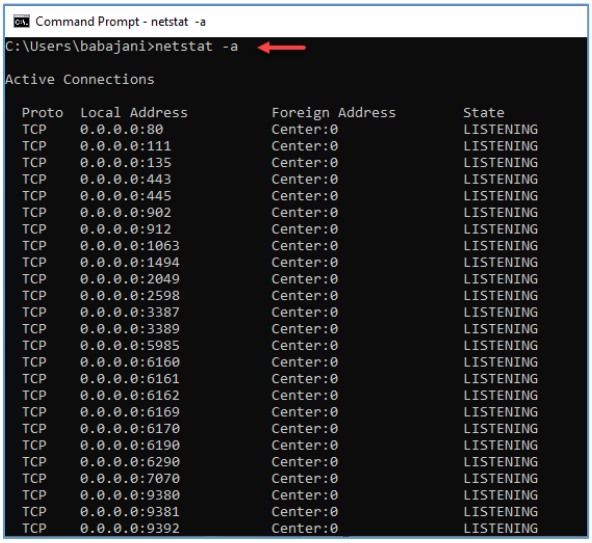
در دستور بالا در خط اول، کتابخانه‌ی socket صدا زده شد، و در خط دوم تابع socket.socket با دو آرگمان صدا زده شده که آرگمان socket.AF_INET برای آدرس‌دهی IPv4 به کار می‌رود و آرگمان socket.SOCK_STREAM برای ایجاد یک ارتباط TCP امن استفاده می‌شود.
در خط سوم با استفاده از تابع bind می‌توان آدرس IP و پورت مورد نظر را تعیین کرد، آدرس IP همان آدرس سیستمی است که در حال کار با آن هستیم و توجه داشته باشید که پورتی که وارد می‌کنید

www.takbook.com

باید بر روی سیستم آزاد باشد و توسط برنامه دیگری استفاده نشود که در اینجا پورت 83 را وارد می‌کنیم، البه برای اینکه بفهمید چه پورتی در سیستم شما در حال استفاده است، باید از دستور زیر در CMD ویندوز خود استفاده کنید:

Netstat -a

توجه داشته باشید که کلید a- تمام اتصالات TCP فعال و پورت‌های TCP و UDP را که کامپیوتر در آن گوش می‌دهد (listening) را نشان می‌دهد.



شکل ۱۸ - ۵ بررسی اتصالات

همان‌طور که در شکل ۱۸–۵، مشاهده می‌کنید تمام پورت‌های فعال در سیستم مشخص شده است، برگردیم به کد و خط چهارم که s.listen است که این تابع می‌تواند محدودیتی برای تعداد کانکشن های ایجاد شده با سرور را مشخص کند که در این کد عدد 1 در نظر گرفته شده است.

در خط آخر هم منتظر پاسخ از طرف کلاینت می‌نشیند و بعد از دریافت پاسخ کد به اتمام می‌رسد.

بعد از اینکه کد را وارد کردید آن را در یک فایل با نام C1.py ذخیره کنید.

یک فایل دیگر با نام C2.py برای کلاینت ایجاد کنید و کد زیر را در آن وارد کنید.

```
Import socket

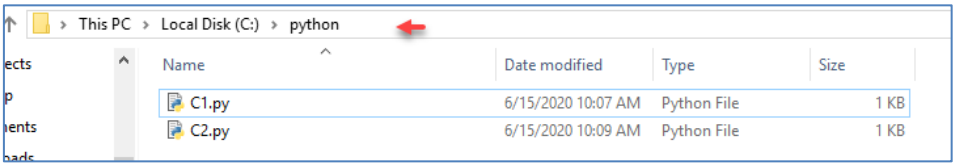
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

www.takbook.com


```
s.connect(("192.168.5.165", 83))
```

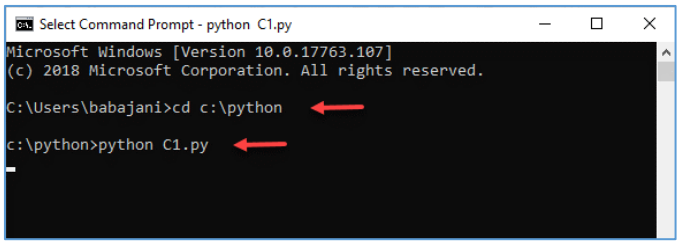
در خط سوم این کد پاسخ سرور داده می‌شود و یک ارتباط TCP ایجاد می‌شود، برای تست این موضوع باید به صورت زیر عمل کنید:

همان‌طور که در شکل ۱۸-۶، مشاهده می‌کنید دو فایل مورد نظر ایجاد شده است.



شکل ۱۸- ۶ ایجاد کد پایتون

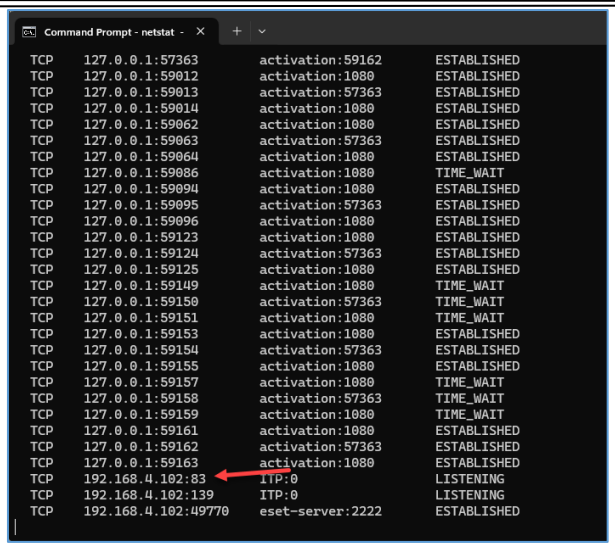
به مانند شکل ۱۸-۷، برای اجرای کد اول وارد CMD شوید و با دستور cd c:\python وارد پوشه‌ای شوید که دو فایل در آن قرار دارد و در آخر با دستور python C1.py کد اول یعنی سرور را اجرا کنید.



شکل ۱۸- ۷ اجرای فایل پایتون

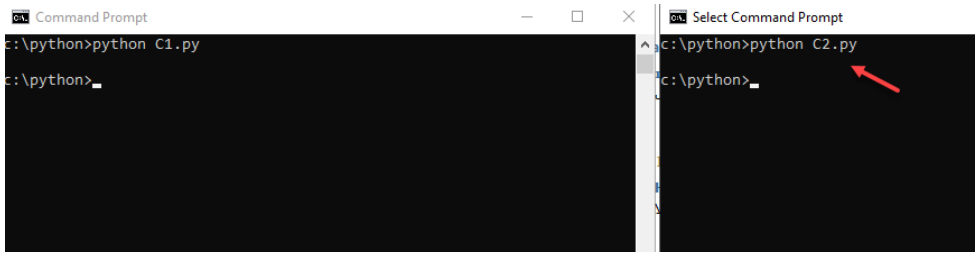
اگر با دستور netstat -a کانکشن‌ها را لیست کنید، همان‌طور که در شکل ۱۸-۸، مشاهده می‌کنید، آدرس IP به همراه پورت 83 را مشاهده می‌کنید که در حالت LISTENING قرار دارند و منتظر پاسخ از سمت کلاینت هستند.

www.takbook.com



شکل ۱۸- ۸ اجرای فایل پایتون

به مانند شکل ۱۸-۹، یک CMD دیگر باز کنید و فایل دوم یعنی C2.py را اجرا کنید، مشاهده می‌کنید که بعد از اجرای C2.py کد C1.py هم به اتمام رسیده است.



شکل ۱۸- ۹ اجرای فایل پایتون

با این کار توانستیم یک ارتباط ساده با سوکت ایجاد کنیم، توجه داشته باشید چون از یک سیستم هم برای سرور و هم برای کلاینت استفاده کردیم می‌توانستید به جای آدرس IP از کلمه‌ی localhost استفاده کنید.

برای اینکه بیشتر با پایتون در شبکه آشنا شوید یک مثال دیگر را هم با هم بررسی می‌کنیم، در سمت سرور کد زیر را وارد کنید:

```
# echo_server.py
import socket

host = ''         # Symbolic name meaning all available interfaces
port = 12345      # Arbitrary non-privileged port
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.bind((host, port))
s.listen(1)
```

www.takbook.com


```
conn, addr = s.accept()
print('Connected by', addr)
while True:
    data = conn.recv(1024)
    if not data: break
    conn.sendall(data)

conn.close()
```

همان‌طور که در کد بالا مشاهده می‌کنید پورت مورد نظر 12345 در نظر گرفته شده است، در دستور Print در سمت سرور آدرس IP و پورتی که به همراه پورت مورد نظر که از طریق کلاینت دریافت می‌کند را چاپ خواهد کرد، عدد 1024 در شرط While اشاره به اندازه‌ی بافر دارد تا کد در بافر اجرا شود.
کد بالا را با نام C3.py در همان پوشه‌ی Pyhton ذخیره کنید.

کد کلاینت هم به صورت زیر خواهد بود:

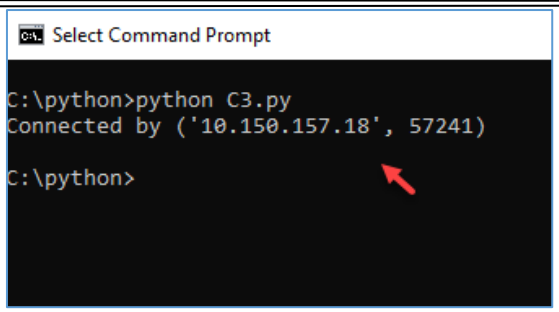
```
# echo_client.py
import socket

host = socket.gethostname()
port = 12345                    # The same port as used by the server
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((host, port))
s.sendall(b'Hello, world')
data = s.recv(1024)
s.close()

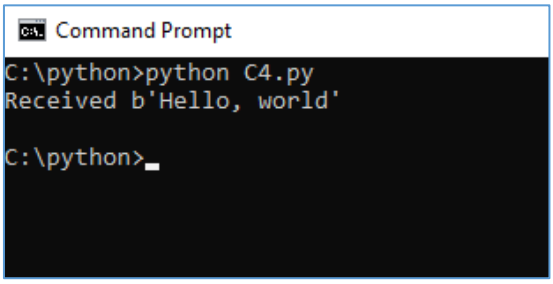
print('Received', repr(data))
```

در این کد هم پورت را 12345 در نظر گرفتیم، این کد را هم با نام C4.py در همان پوشه ذخیره کنید.
اگر سرور و کلاینت را به همان روشی که قبلاً گفتیم اجرا کنید، نتیجه کار چیزی شبیه به شکل ۱۸ – ۱۰، خواهد بود که در سمت سرور آدرس IP و پورت کلاینت مشخص می‌شود و در سمت کلاینت هم کلمه‌ی Hello, Word چاپ خواهد شد.

www.takbook.com



شکل ۱۸- ۱۰ اجرای فایل پایتون



شکل ۱۸- ۱۱ اجرای فایل پایتون

در این قسمت می‌خواهیم کارهای مفیدی که با پایتنون می‌توانیم در شبکه انجام دهیم را با هم بررسی می‌کنیم.

توجه داشته باشید در پایتون کتابخانه‌های زیادی برای کارهای مختلف وجود دارد که ما در بحث شبکه از آنها استفاده خواهیم کرد.

در پایتون، کتابخانه‌ها (Libraries) مجموعه‌ای از کدها، ماژول‌ها و توابع آماده هستند که برای انجام وظایف مختلف می‌توانند مورد استفاده قرار گیرند. این کتابخانه‌ها به توسعه‌دهندگان کمک می‌کنند تا بدون نیاز به نوشتن کد از صفر، از قابلیت‌ها و توابع از پیش تعریف‌شده استفاده کنند و کارهای پیچیده را سریع‌تر و به‌صورت بهینه‌تر انجام دهند.

کتابخانه‌ها در پایتون معمولاً به صورت پکیج‌های مجزا ارائه می‌شوند و می‌توان آنها را با استفاده از مدیر بسته‌ها مانند pip نصب کرد.

۱۸-۲ کار با کتابخانه Netmiko در پایتون

یکی از خصوصیات مهم برنامه نویسی پایتون این است که دارای کتابخانه‌های عظیمی است که توسط افراد یا تیم پایتون برای کارهای مختلف نوشته شده است، در شبکه هم برای کار با دستگاه‌های شبکه

www.takbook.com

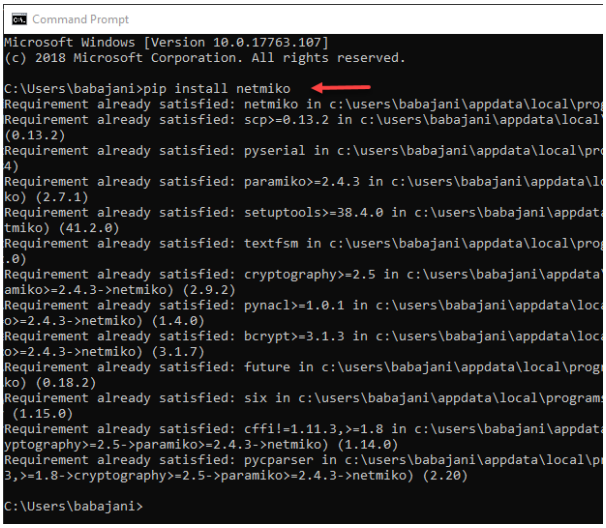
مانند دستگاه‌های سیسکو یک کتابخانه‌ی قدرتمند با نام Netmiko وجود دارد که توسط Kirk Byers نوشته شده است، برای دریافت توضیحات بیشتر می‌توانید به سایت زیر مراجعه کنید:

https://pynet.twb-tech.com/blog/automation/netmiko.html

در این کتابخانه شما می‌توانید از طریق دستوراتی که در ادامه مورد بررسی قرار می‌دهیم به روتر سیسکو متصل شوید و دستورات مورد نظر خود را اجرا کنید.

برای شروع کار، اول باید کتابخانه‌ی Netmiko را از اینترنت دانلود و نصب کنیم، برای این‌کار وارد CMD شوید و دستور زیر را وارد کنید. (شکل ۱۸-۱۲)

pip install netmiko



شکل ۱۸- ۱۲ خروجی برنامه

همان‌طور که در شکل ۱۸-۱۲، مشاهده می‌کنید دستور مورد نظر کتابخانه‌ی Netmiko را از اینترنت دانلود و بر روی سیستم نصب کرد، توجه داشته باشید این دستور زمانی اجرا می‌شود که قبل از آن پایتون را بر روی سیستم خود نصب کرده باشید.

در ادامه کار یک CMD باز کنید و دستور Python را اجرا کنید، با این کار وارد خط فرمان پایتون خواهیم شد و دستورات را به مانند زیر وارد کنید:

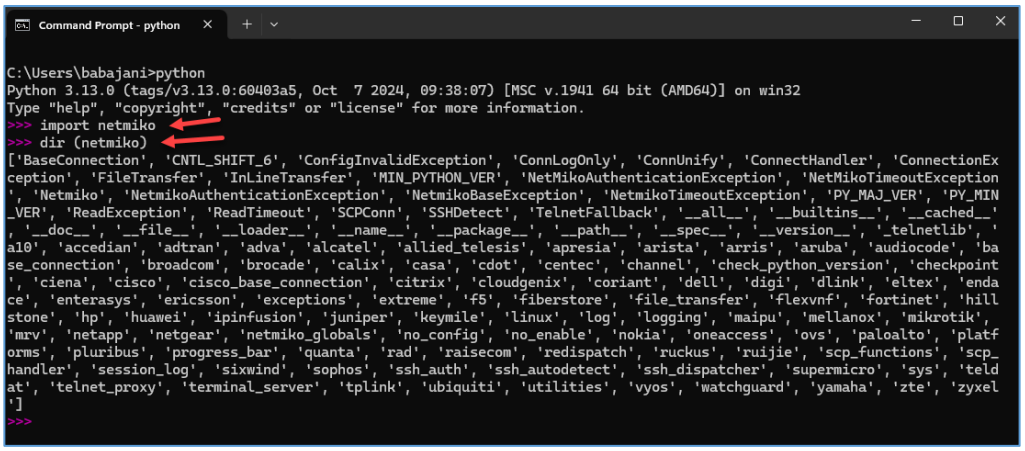
>>> **import netmiko**(این دستور کتابخانه مورد نظر را وارد می‌کند)

www.takbook.com

>>> **dir(netmiko)** (این دستور، تمام دیکشنری‌های مربوط به این کتابخانه را نشان می‌دهد)

['BaseConnection', 'CNTL_SHIFT_6', 'ConnectHandler', 'FileTransfer', 'InLineTransfer', 'NetMikoAuthenticationException', 'NetMikoTimeoutException', 'Netmiko', 'NetmikoAuthenticationException', 'NetmikoTimeoutException', 'SCPConn', 'SSHDetect', '__all__', '__builtins__', '__cached__', '__doc__', '__file__', '__loader__', '__name__', '__package__', '__path__', '__spec__', '__version__', '_textfsm', 'a10', 'accedian', 'alcatel', 'apresia', 'arista', 'aruba', 'base_connection', 'calix', 'checkpoint', 'ciena', 'cisco', 'cisco_base_connection', 'citrix', 'cloudgenix', 'coriant', 'dell', 'dlink', 'eltex', 'endace', 'enterasys', 'extreme', 'f5', 'file_transfer', 'flexvnf', 'fortinet', 'hp', 'huawei', 'ipinfusion', 'juniper', 'keymile', 'linux', 'log', 'logging', 'mellanox', 'mikrotik', 'mrv', 'netapp', 'netmiko_globals', 'nokia', 'oneaccess', 'ovs', 'paloalto', 'platforms', 'pluribus', 'quanta', 'rad', 'redispatch', 'ruckus', 'ruijie', 'scp_functions', 'scp_handler', 'sophos', 'ssh_autodetect', 'ssh_dispatcher', 'ssh_exception', 'terminal_server', 'ubiquiti', 'utilities', 'vyos', 'watchguard']

دستورات بالا را در شکل ۱۸-۱۳، مشاهده می‌کنید:



شکل ۱۸- ۱۳ خروجی دستور dir(netmiko)

۱۸-۳ نصب Visual Studio Code (VS Code)

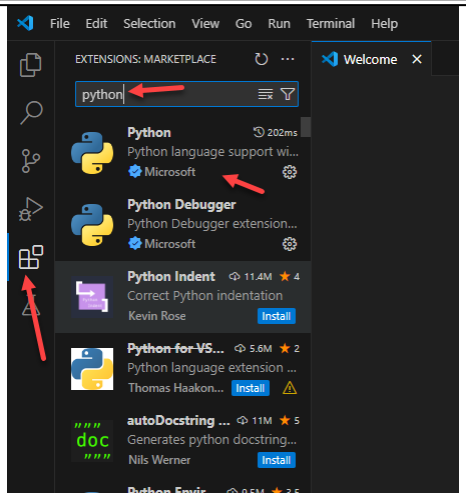
Visual Studio Code (VS Code) یک ویرایشگر کد منبع متن‌باز است که توسط مایکروسافت توسعه داده شده است. این ویرایشگر به دلیل ویژگی‌های متنوع و قابلیت‌های گسترده‌اش به سرعت در بین توسعه‌دهندگان محبوب شده است.

برای اینکه از کدهای پایتون استفاده کنیم باید برنامه آن را از لینک زیر دانلود و نصب کنیم:

https://code.visualstudio.com/download

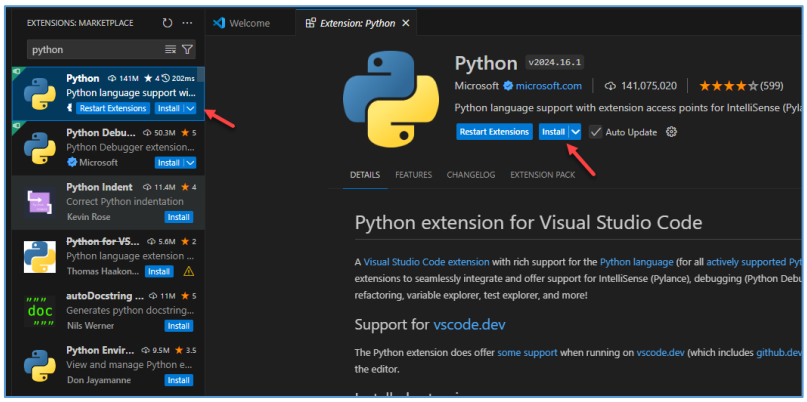
بعد از نصب، آن را اجرا کنید، بعد از اجرا به ماند شکل ۱۸-۱٤، بر روی آیکون Extenction کلیک کنید و در قسمت جستجو کلمه Python را وارد کنید و بر روی اولین گزینه کلیک کنید.

www.takbook.com



شکل ۱۸- ۱۴ نصب *Visual Studio Code (VS Code)*

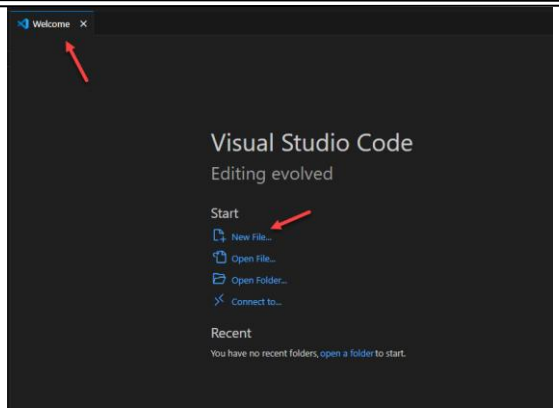
در شکل ۱۸-۱۵، بر روی Install کلیک کنید تا افزونه پایتون بر روی این نرم افزار در دسترس باشد.



شکل ۱۸- ۱۵ نصب *Visual Studio Code (VS Code)*

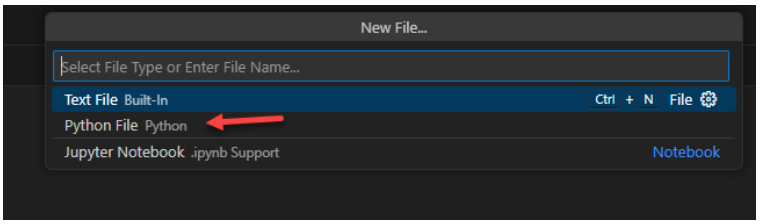
برای شروع کار با برنامه Visual Studio Code باید به مانند شکل ۱۸-۱۶، در تب Welcome بر روی New File کلیک کنید.

www.takbook.com



شکل ۱۸- ۱۶ نصب *Visual Studio Code (VS Code)*

در شکل ۱۸–۱۷، گزینه‌ی python File را انتخاب کنید.



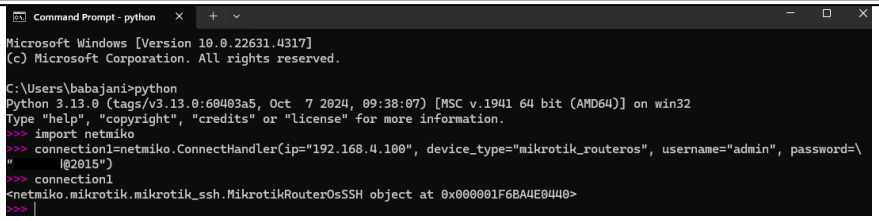
شکل ۱۸- ۱۷ نصب *Visual Studio Code (VS Code)*

خوب همه چیز برای اجرای دستور اصلی آماده است، برای متصل شدن به روتر میکروتیک باید سرویس SSH آن را که قبلاً در فصل مربوط به میکروتیک توضیح دادیم روشن کنید و بعد از روشن کردن، برای متصل شدن از طریق پایتون باید از گزینه‌ی ConnectHandler استفاده کنیم، که این گزینه را در دستور زیر مشاهده می‌کنید:

```
import netmiko
connection1=netmiko.ConnectHandler(ip="192.168.4.100",
device_type="mikrotik_routeros", username="admin",
password="Test@2015")
```

در دستور بالا باید آدرس IP، نوع دستگاه، نام کاربری و رمزعبور روتر میکروتیک را وارد کنید، این تنظیمات بعد از اجرا در متغییر connection1 قرار می‌گیرند که در شکل ۱۸–۱۸، این متغییر صدا زده شده و به درستی به دستگاه متصل شده است و در ادامه می‌توانیم از متغیر connection1 استفاده کنیم.

www.takbook.com



شکل ۱۸- ۱۸اجرای کد

اگر بخواهیم دیکشنری مربوط به متغییر connection1 را مشاهده کنیم باید از دستور زیراستفاده کنید:

>>> **dir(connection1)**



شکل ۱۸- ۱۹ اجرای کد

همان‌طور که شکل ۱۸-۱۹، مشاهده می‌کنید، دستوراتی را که می‌توانید برای ارتباط با روتر از آنها استفاده کنید مشخص شده است، برای تست عملکرد آنها از دستور زیر برای نمایش Interfaceهای روتر میکروتیک استفاده می‌کنیم:

```
print(connection1.send_command("/interface print"))
```

همان‌طور که در خروجی مشاهده می‌کنید تمام Interface های روتر میکروتیک نمایش داده شده است و این نشان دهنده این است که کار به درستی انجام شده است، اگر به زیر دستور نگاه کنید دستور اصلی در روتر میکروتیک هم نمایش داده شده است.

```
>>> print(connection1.send_command("/interface print"))
[admin@Free-Link-1] /interface> /interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                TYPE       ACTUAL-MTU L2MTU     MAX-L2MTU MAC-ADDRESS
 0     Internet                            ether            1500  1598       2028 2C:C8:1B:34:2F:DE
 1     Loca3                               ether            1500  1598       2028 2C:C8:1B:34:2F:DB
 2     ether2                              ether            1500  1598       2028 2C:C8:1B:34:2F:DC
```

www.takbook.com


```
 3  R  ether3                          ether            1500  1598       2028 2C:C8:1B:34:2F:DD
 4     pwr-line1                       ether            1500  1598       2028 2C:C8:1B:34:2F:DF
 5  R  wlan4                           wlan             1500  1600       2290 48:A9:8A:52:33:72
>>>
```

برای اینکه این دستورات را در یک فایل ذخیره کنیم و آن را صدا بزنیم باید به صورت زیر عمل کنید:

```
import netmiko
connection1=netmiko.ConnectHandler(ip="192.168.4.100",
device_type="mikrotik_routeros", username="admin",
password="Test@2015")
print(connection1.send_command("/interface print"))
```

دستورات بالا را در یک فایل ذخیره و آن را به صورت شکل ۱۸-۲۰، اجرا کنید.

```
PS G:\Python> python interface-mikrotik.py
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                TYPE       ACTUAL-MTU L2MTU  MAX-L2MTU MAC-ADDRESS
 0     Internet                            ether            1500  1598       2028 2C:C8:1B:34:2F:DE
 1     Loca3                               ether            1500  1598       2028 2C:C8:1B:34:2F:DB
 2     ether2                              ether            1500  1598       2028 2C:C8:1B:34:2F:DC
 3  R  ether3                              ether            1500  1598       2028 2C:C8:1B:34:2F:DD
 4     pwr-line1                           ether            1500  1598       2028 2C:C8:1B:34:2F:DF
 5  R  wlan4                               wlan             1500  1600       2290 48:A9:8A:52:33:72
PS G:\Python>
```

شکل ۱۸ - ۲۰ اجرای کد

همان‌طور که مشاهده می‌کنید، با صدا زدن فایل interface-mikrotik.py که دستورات بالا در آن قرار داشت، خروجی Interfaceهای روتر میکروتیک را به ما نشان داد.

برای اینکه کد برنامه را به شکل زیباتر و قابل فهم‌تر بنویسیم می‌توانیم از کدهای زیر برای این کار استفاده کنیم:

```
from netmiko import ConnectHandler

# Establish a connection to the router
Connect_Router= {
    'device_type': 'mikrotik_routeros',
    'host':   '192.168.4.100',
    'username': 'admin',
    'password': Test@2015',
    'port' : 22,
}
```

www.takbook.com


```
net_connect = ConnectHandler(**Connect_Router)

# Operational Command Example
output = net_connect.send_command('/interface print')
print(output)
```

در بالا با دستور From فقط گزینه‌ی ConnectHandler را از کتابخانه‌ی netmiko فراخوانی کردیم و دیگر نیاز به فراخوانی کل کتابخانه نیست، بعد از آن یک متغییر رشته‌ای با نام Connect_Router ایجاد می‌کنیم و اطلاعات ارتباطی با روتر را برای آن مشخص می‌کنیم.

بعد از آن نتیجه‌ی دستور ConnectHandler(**Connect_Router) را درون متغییر net_connect ریخته و دستور interface print را ازآن درخواست می‌کنیم و در خروجی چاپ می‌کنیم.

در مجموع استفاده از زبان پایتون به صورت حرفه‌ای در شبکه، شما را در ایجاد یک شبکه‌ی کاملاً اتوماتیک کمک خواهد کرد، هر چند در این بخش فقط یک بخش کوچکی از آن را بررسی کردیم ولی با تمرین و پیدا کردن منابع بهتر می‌توانید به بهترین نحو از آن استفاده کنید.

۱۸-٤ Backup گرفتن از روتر میکروتیک

برای اینکه بتوانیم با یک کلیک از روتر خود بک آپ تهیه کنیم، می‌توانیم از طریق دستور زیر این کار را انجام دهیم، توجه داشته باشید در این کد برای اینکه در هر بار اجرا ساعت و تاریخ به فایل مورد نظر اضافه شود باید کد را به صورت زیر اجرا کنیم.

```
from netmiko import ConnectHandler
from datetime import datetime
Connect_Router= {
    'device_type': 'mikrotik_routeros',
    'host':   '192.168.4.100',
    'username': 'admin',
    'password': 'Test@2015',
    'port' : 22,
}

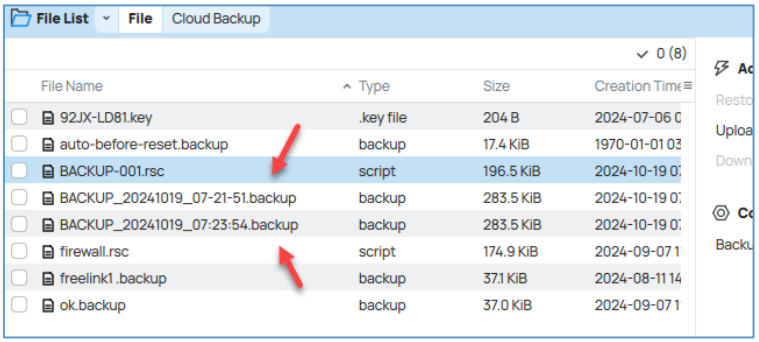
net_connect = ConnectHandler(**Connect_Router)


backup_name =
f"BACKUP_{datetime.now().strftime('%Y%m%d_%H:%M:%S')}"
```

www.takbook.com


```
command = f'/system backup save dont-encrypt=yes
name={backup_name}'
output = net_connect.send_command(command)
print(output)
```

بعد از اجرا اگر طبق شکل ۱۸-۲۱، به قسمت Files مراجعه کنید مشاهده خواهید کرد که پشتیبان‌گیری به صورت اتوماتیک انجام شد.



شکل ۱۸- ۲۱ اجرای کد

در دستور بالا برای اینکه تاریخ و ساعت به فایل اضافه شود از دستور زیر استفاده کردیم که در قسمت اول تاریخ و در قسمت دوم ساعت قرار گرفته است.

```
datetime.now().strftime('%Y%m%d_%H:%M:%S')
```

۱۸-۵ خروجی گرفتن از فایروال میکروتیک و ایجاد Rule

در این قسمت می‌خواهیم یک پرینت از وضعیت Ruleها در فایروال میکروتیک را ببینیم و یک Rule جدید ایجاد کنیم، برای انجام این کار نیاز به کتابخانه‌ی paramiko داریم که با دستور زیر آن را نصب کنید.

```
pip install paramiko
```

بعد از نصب کتابخانه، برای این که از این کتابخانه و دستورات آن استفاده کنیم باید از دستور زیر استفاده کنیم، در این دستور اول از همه اطلاعات روتر میکروتیک دریافت شده و بعد از آن دستورالعمل دسترسی به SSH مشخص شده است در ادامه با سرویس SSH به روتر متصل می‌شویم و با دستور client.exec_command دستورات مورد نظر که در میکروتیک اجرا می‌شود را می‌نویسیم، اولین دستور / ip firewall filter print که پرنتی از Rule هایی که در حال حاضر وجود دارد را نمایش می‌دهد، و در ادامه یک Rule جدید با دستور / ip firewall filter add chain=input action=drop src-address=192.168.88.0/24 comment="Drop all traffic from 192.168.88.0/24 ایجاد می‌کنیم که جلوی ورود IPهای رنج مشخص شده را می‌گیرد.

```
import paramiko
```

www.takbook.com


```
# MikroTik Information
hostname = '192.168.4.100'  # IP Mikrotik
username = 'admin'          # User name
password = 'Test@2015'   # Pass

# ایجاد یک شیء SSHClient
client = paramiko.SSHClient()
client.load_system_host_keys()
client.set_missing_host_key_policy(paramiko.AutoAddPolicy())

try:
    client.connect(hostname, username=username,
password=password)

    stdin, stdout, stderr = client.exec_command('/ip firewall
filter print')
    output = stdout.read().decode('utf-8')
    print("Current Firewall Rules:")
    print(output)

    add_rule_command = '/ip firewall filter add chain=input
action=drop src-address=192.168.88.0/24 comment="Drop all traffic
from 192.168.88.0/24"'
    stdin, stdout, stderr = client.exec_command(add_rule_command)

    error = stderr.read().decode('utf-8')
    if error:
        print("Error adding rule:", error)
    else:
        print("New firewall rule added.")

finally:
    # قطع اتصال
    client.close()
```

همان‌طور که در شکل ۱۸-۲۲، مشاهده می‌کنید خروجی به درستی اجرا شده و یک Print از Ruleهای موجود نمایش داده شده و یک Rule هم ایجاد شده است.

www.takbook.com


```
32
33      # بررسی خروجی یا خطا
34      error = stderr.read().decode('utf-8')
35      if error:
36          print("Error adding rule:", error)
37      else:
38          print("New firewall rule added.")
39

PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

Current Firewall Rules:
Flags: X - disabled, I - invalid, D - dynamic


New firewall r g:; cd 'g:\Python'; & 'c:\Users\babajani\AppData\Local\Programs\Python\Python313\python.exe'
'--' 'G:\Python\C1.py' ^C
PS G:\Python>
PS G:\Python>  g:; cd 'g:\Python'; & 'c:\Users\babajani\AppData\Local\Programs\Python\Python313\python.exe'
'--' 'G:\Python\C1.py'
Current Firewall Rules:
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=accept in-interface=Loca3 log=no log-prefix=""

 1    chain=output action=accept protocol=tcp log=no log-prefix=""

 2    chain=forward action=accept protocol=tcp dst-port=80 log=no log-prefix=""


New firewall rule added.
PS G:\Python>
```

شکل ۱۸ - ۲۲ کد مربوط به میکروتیک

همان‌طور که در شکل ۱۸–۲۳، مشاهده می‌کنید Rule مورد نظر در فایروال میکروتیک ایجاد شده است:

Firewall | Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

New

#	Action	Chain	Src. Address	Dst. Addre...	Prot...	Src. Port	Dst. Port	In. Inte...	Out. In...	In. Inte...	Out. In...	Src. Ad...	Dst. Ad...	Bytes	Packets
0	acc...	forward						Loca3						0 B	0
1	acc...	output			6 (tc...									11.0 KiB	43
2	acc...	forward			6 (tc...		80							12.5 KiB	126
	Drop all traffic from 192.168.88.0/24														
3	drop	input	192.168.88....											0 B	0

شکل ۱۸ - ۲۳ کد مربوط به میکروتیک

۱۸–۵–۱ نمایش لیست IPهای DHCP

با استفاده از دستورات زیر می‌خواهیم به روتر میکروتیک متصل شویم و لیستی از DHCP Lease را نمایش دهیم، در شکل ۱۸–۲٤، تمام موارد به مانند قسمت قبلی است و فقط دستور ip dhcp-server lease / print را اضافه و اجرا می‌کنیم.

```
import paramiko


hostname = '192.168.4.100'
username = 'admin'
password = 'Test@2015'
```

www.takbook.com


```
client = paramiko.SSHClient()
client.load_system_host_keys()
client.set_missing_host_key_policy(paramiko.AutoAddPolicy())

try:

    client.connect(hostname, username=username,
password=password)

    stdin, stdout, stderr = client.exec_command('/ip dhcp-server
lease print')

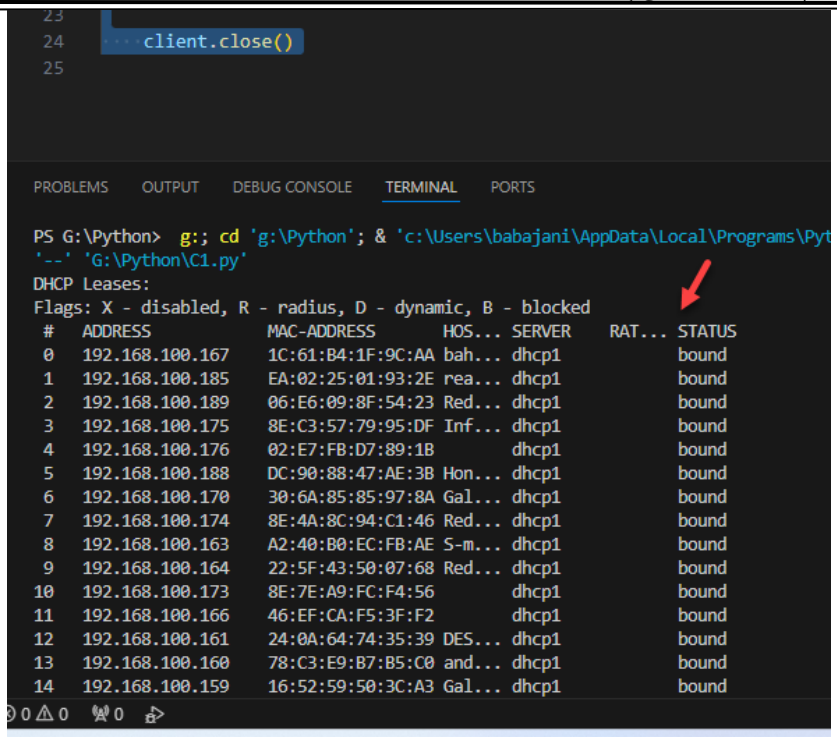
    output = stdout.read().decode('utf-8')
    print("DHCP Leases:")
    print(output)

finally:

    client.close()
```

همان‌طور که در شکل ۱۸-۲٤، مشاهده می‌کنید، تمام کلاینت‌هایی که از سرویس DHCP آدرس دریافت کرده‌اند را مشاهده می‌کنید.

www.takbook.com



شکل ۱۸-۲۴ نمایش لیست IP های DHCP

۱۸-۵-۲ کار با API میکروتیک در پایتون

API (Application Programming Interface) رابط برنامه‌نویسی کاربردی است. به زبان ساده، API مجموعه‌ای از قوانین و پروتکل‌هایی است که به برنامه‌ها اجازه می‌دهد با یکدیگر ارتباط برقرار کنند و داده‌ها یا عملکردها را به اشتراک بگذارند.

مفهوم کلی API:

API را می‌توان به عنوان واسطی بین دو نرم‌افزار یا سیستم در نظر گرفت که به آن‌ها امکان می‌دهد بدون نیاز به دانستن جزئیات داخلی یکدیگر، اطلاعات و دستورات را تبادل کنند. APIها به توسعه‌دهندگان این امکان را می‌دهند تا از قابلیت‌های موجود در نرم‌افزارهای دیگر استفاده کنند، بدون این که نیاز باشد آن قابلیت‌ها را از ابتدا پیاده‌سازی کنند.

مثال‌هایی از APIهای رایج:

Google Maps API: برای نمایش نقشه‌ها و مسیریابی در وب‌سایت‌ها و اپلیکیشن‌ها استفاده می‌شود.

Twitter API: به توسعه‌دهندگان اجازه می‌دهد که توییت‌ها را ارسال، جستجو و داده‌های کاربر را مدیریت کنند.

www.takbook.com

Weather API: ارائه اطلاعات وضعیت آب و هوا برای مناطق مختلف.

APIهای مورد استفاده در شبکه:

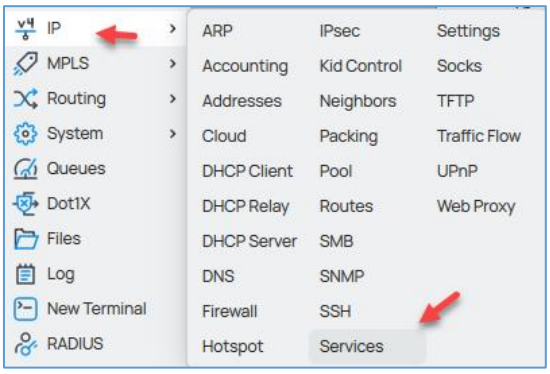
MikroTik API: برای مدیریت و کنترل تجهیزات MikroTik از طریق برنامه‌های خارجی.

REST API: یکی از رایج‌ترین انواع API است که بر مبنای پروتکل HTTP کار می‌کند و اغلب برای سرویس‌های وب استفاده می‌شود.

چگونگی استفاده از API:

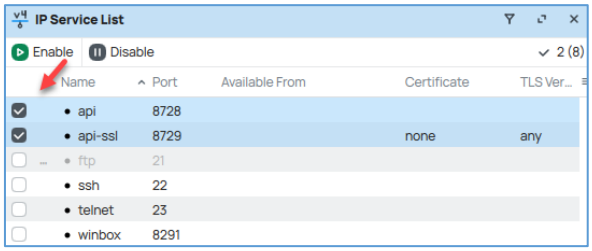
برای استفاده از API، معمولاً باید درخواست‌هایی به سرور API ارسال کنید و پاسخ‌هایی دریافت کنید. این درخواست‌ها می‌توانند شامل عملیات‌هایی مثل خواندن اطلاعات، ایجاد داده‌های جدید، به‌روزرسانی یا حذف باشند.

برای بررسی این موضوع در میکروتیک API را فعال می‌کنیم و از طریق پایتون اطلاعاتی را از میکروتیک دریافت می‌کنیم، برای فعال‌سازی API باید به مانند شکل ۱۸-۲۵، وارد میکروتیک شوید و از قسمت IP وارد Services شوید.



شکل ۱۸- ۲۵ کار با API میکروتیک در پایتون

در شکل ۱۸-۲۶، هر دو گزینه را انتخاب و فعال کنید.

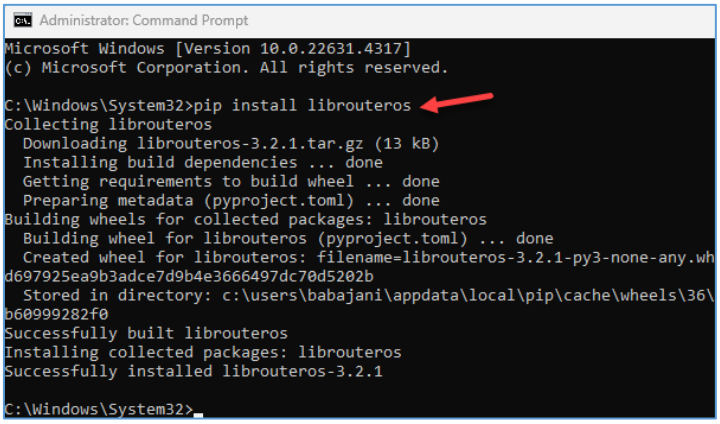


شکل ۱۸- ۲۶ کار با API میکروتیک در پایتون

www.takbook.com

در ادامه برای اینکه از API در پایتون استفاده کنیم باید کتابخانه‌ی librouteros را نصب کنیم و از آن استفاده کنیم که برای این کار باید از دستور زیر استفاده کنیم که این موضوع را در شکل ۱۸-۲۷، مشاهده می‌کنید.

pip install librouteros



شکل ۱۸- ۲۷ کار با API میکروتیک در پایتون

برای تست این موضوع از مثال زیر استفاده می‌کنیم که در این مثال به API میکروتیک متصل می‌شویم و لیست آدرس Interfaceهای مورد نظر را print می‌گیریم.

در کد زیر با استفاده از تابع connect، به دستگاه میکروتیک با استفاده از API متصل می‌شویم. برای اتصال به API، اطلاعات ورود شامل host، username و password مورد نیاز است.

پس از اتصال، با استفاده از مسیر interface/، لیست اینترفیس‌ها دریافت شده و در یک حلقه چاپ می‌شود. همان‌طور که مشاهده می‌کنید نحوه‌ی نوشتن دستورات کاملاً متفاوت است و مانند متصل شدن با SSH نیست و نباید مستقیم همان دستور در میکروتیک را واردکنید.

```
from librouteros import connect

# MikroTik connection details
host = '192.168.4.100'    # MikroTik IP address
username = 'admin'       # Username
password = 'Test@2015'    # Password

# Connect to MikroTik API
try:
    api = connect(username=username, password=password,
host=host)
```

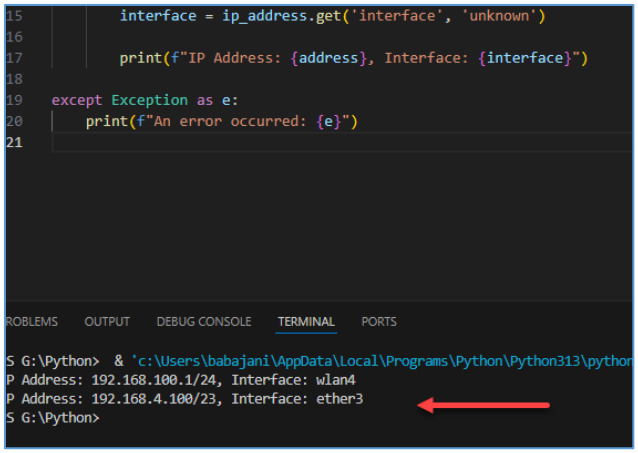
www.takbook.com


```
    # Retrieve and display IP address information
    for ip_address in api.path('ip', 'address'):
        address = ip_address.get('address', 'unknown')
        interface = ip_address.get('interface', 'unknown')

        print(f"IP Address: {address}, Interface: {interface}")

except Exception as e:
    print(f"An error occurred: {e}")
```

همان‌طور که در شکل ۱۸–۲۸، مشاهده می‌کنید خروجی به درستی نمایش داده شده است.



شکل ۱۸- ۲۸ کار با API میکروتیک در پایتون

برای اینکه بهتر موضوع API رامتوجه شوید یک مثال دیگر را با هم بررسی می‌کنیم، در این مثال لیست کاربرانی که در PPP تعریف کردیم در خروجی نمایش داده خواهد شد.

در کد زیر با استفاده از تابع connect به روتر MikroTik از طریق APIمتصل می‌شویم تا به اطلاعات کاربران PPP دسترسی پیدا کنیم.

مسیر api.path('ppp', 'secret') برای دریافت اطلاعات کاربران PPP استفاده می‌شود این اطلاعات شامل نام کاربری (name)، پروفایل کاربر (profile)، نوع سرویس (service) و وضعیت فعال یا غیرفعال بودن کاربر (disabled) استخراج و نمایش داده می‌شود.

```
from librouteros import connect

# MikroTik connection details
host = '192.168.4.1'     # MikroTik IP address
username = 'admin'        # Username
```

www.takbook.com


```
password = Test@2015'     # Password

# Connect to MikroTik API
try:
    api = connect(username=username, password=password,
host=host)

    # Retrieve and display PPP user information
    for user in api.path('ppp', 'secret'):
        name = user.get('name', 'unknown')
        profile = user.get('profile', 'unknown')
        service = user.get('service', 'unknown')
        disabled = user.get('disabled', False)

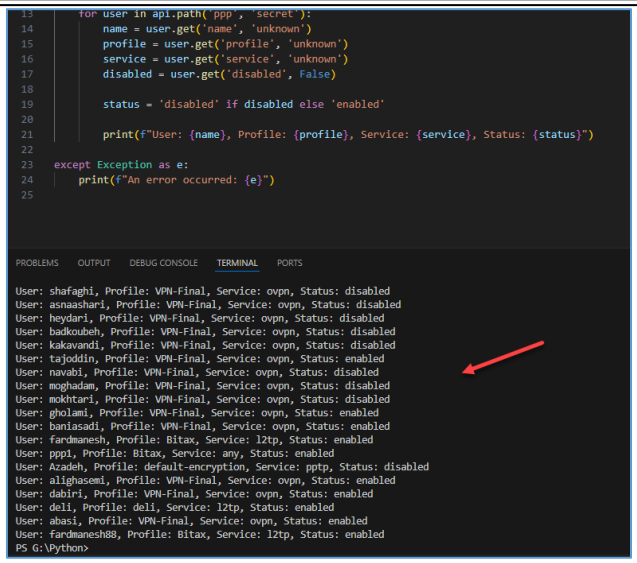
        status = 'disabled' if disabled else 'enabled'

        print(f"User: {name}, Profile: {profile}, Service:
{service}, Status: {status}")

except Exception as e:
    print(f"An error occurred: {e}")
```

در شکل ۱۸–۲۹، خروجی کار را مشاهده می‌کنید که لیست کاملی از کاربران PPP نمایش داده شده است.

www.takbook.com



شکل ۱۸- ۲۹ کار با API میکروتیک در پایتون

۱۸-۶ تغییر آدرس کارت شبکه‌ی ویندوز

کدهای پایتون را می‌توانید در تمام سیستم‌ها اجرا کنید، در این قسمت می‌خواهیم تنظیمات کارت شبکه را تغییر دهیم، برای این کار می‌توانیم از کد زیر استفاده کنید، در کد زیر و در قسمت interface_name باید نام Interface خود را در ویندوز مشخص و در این قسمت وارد کنید که برای ویندوز ما Ethernet3 است، در ادامه با استفاده از دستور netsh interface ip set address name آدرس IP، Subnet، Gateway را تغییر می‌دهیم، توجه داشته باشید این کد را باید با دسترسی Administrator ارسال کنید.

```
import subprocess
#ip_address-New
new_ip_address = "10.10.10.210"
subnet_mask = "255.255.0.0"
gateway = "10.10.10.1"
interface_name = "Ethernet3"
try:

    print(f"Changing IP address on interface '{interface_name}'
to {new_ip_address}...")
```

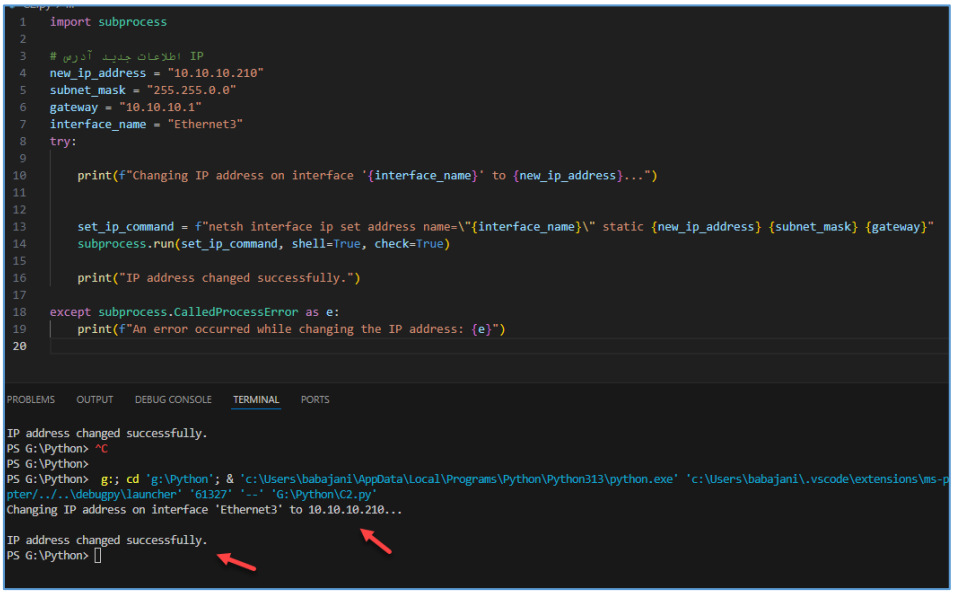
www.takbook.com


```
    set_ip_command = f"netsh interface ip set address
name=\"{interface_name}\" static {new_ip_address} {subnet_mask}
{gateway}"
    subprocess.run(set_ip_command, shell=True, check=True)

    print("IP address changed successfully.")

except subprocess.CalledProcessError as e:
    print(f"An error occurred while changing the IP address:
{e}")
```

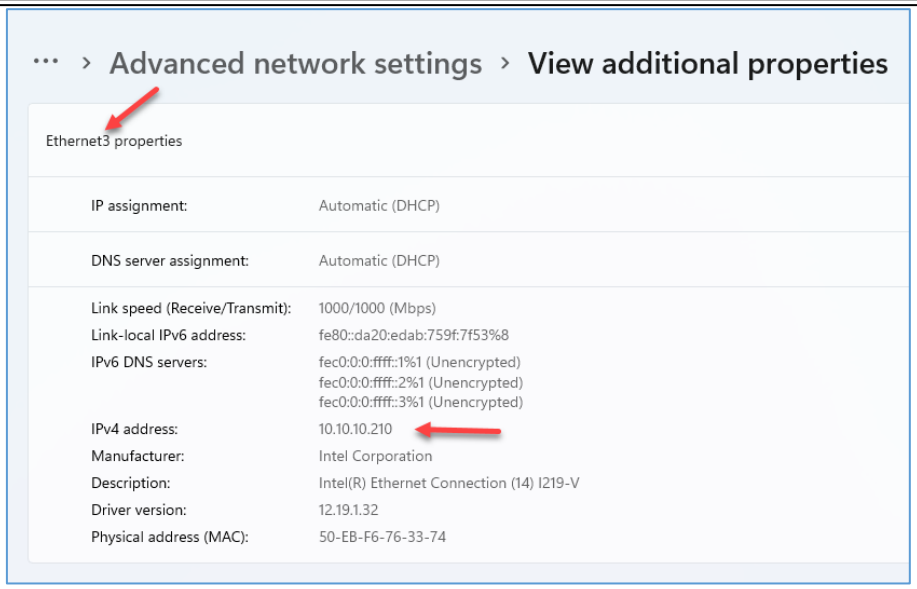
همان‌طور که در شکل ۱۸–۳۰، مشاهده می‌کنید، تغییرات با موفقیت روی کارت شبکه‌ی مورد نظر اعمال شده است.



شکل ۱۸- ۳۰ تغییر آدرس کارت شبکه‌ی ویندوز

اگر داخل ویندوز هم بررسی کنیم مشاهده خواهید کرد که آدرس مورد نظر برای کارت شبکه‌ی مشخص شده به مانند شکل ۱۸–۳۱، تغییر کرده است.

www.takbook.com



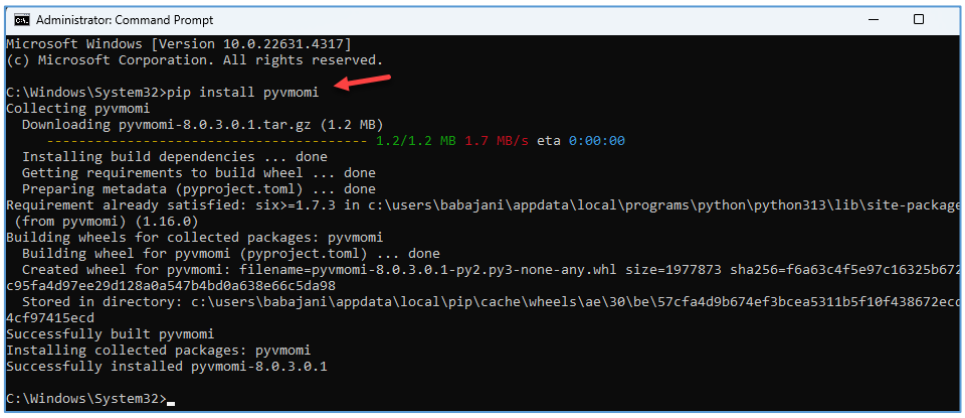
شکل ۱۸- ۳۱ تغییر آدرس کارت شبکه‌ی ویندوز

۱۸-۷ کار با ESXi در پایتون

همان‌طور که گفتیم پایتون برای هر کاری یک کتابخانه مخصوص به خودش دارد و برای اینکه در این قسمت با سرور ESXi کار کنیم باید از کتابخانه‌ی pyvmomi استفاده کنیم، برای نصب آن بر روی سیستم خود CMD را باز کنید و دستور زیر را اجرا کنید.

```
pip install pyvmomi
```

همان‌طور که در شکل ۱۸-۳۲، مشاهده می‌کنید کتابخانه مورد نظر نصب شده است و می‌توانیم از آن استفاده کنیم.



شکل ۱۸- ۳۲ کار با ESXi در پایتون

www.takbook.com

۱-۷-۱۸ نمایش ماشین‌های ESXi

برای نمایش ماشین‌های سرور ESXi باید از کد زیر استفاده کنیم، در خط اول کتابخانه pyvim را صدا می‌زنیم و با استفاده از دستور import ssl گواهینامه‌ی مربوط به ESXi را صدا می‌زنیم و با دستور ssl._create_unverified_context از گواهینامه‌ی نامعتبر داخلی صرف‌نظر می‌کنیم تا کار ادامه پیدا کند.

در قسمت دوم اطلاعات متصل شدن به سرور ESxi را مشاهده می‌کنید، در قسمت سوم به سرور Esxi متصل می‌شویم، در قسمت چهارم باید مشخص کنیم که دنبال چه چیز در سرور Esxi می‌گردیم و در قسمت آخر هم لیست ماشین‌های مجازی را با دستور vm به ما نمایش می‌دهد.

```
from pyVim.connect import SmartConnect, Disconnect
from pyVmomi import vim
import ssl
context = ssl._create_unverified_context()

# Esxi Server
esxi_host = "192.168.5.6"
esxi_user = "root"
esxi_password = "Test@1999"

# Esxi Connect
si = SmartConnect(host=esxi_host, user=esxi_user,
pwd=esxi_password, sslContext=context)

# View information
content = si.RetrieveContent()
container = content.rootFolder  # Search Start
viewType = [vim.VirtualMachine]  # Object
recursive = True  # Return
containerView =
content.viewManager.CreateContainerView(container, viewType,
recursive)

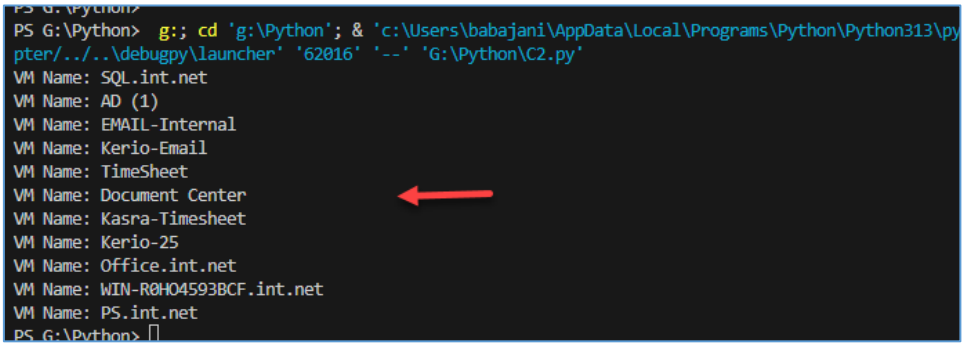
# List Cirtual machine
virtual_machines = containerView.view
for vm in virtual_machines:
    print(f"VM Name: {vm.name}")

#Disconnect Esxi
```

www.takbook.com


```
Disconnect(si)
```

همان‌طور که در خروجی شکل ۱۸-۳۳، مشاهده می‌کنید کد مورد نظر با موفقیت اجرا شده است و تمام ماشین‌های مجازی ESXi مورد نظر نمایش داده شده است.



شکل ۱۸- ۳۳ نمایش ماشین‌های ESXi

۱۸-۷-۲ ریست کردن یک ماشین مجازی در ESXi

در قسمت قبل توانستیم با استفاده از کد پایتون به ESXI متصل شویم و ماشین‌ها را پیدا کنیم، حالا می‌خواهیم همان کد را تغیر دهیم و یک ماشین را به انتخاب خودمان Restart کنیم، برای این کار از کد زیر استفاده می‌کنیم، توجه داشته باشید تمام توضیحات را در دستورات نوشتم تا راحت کدها را بشناسید، دستور vm.ResetVM_Task() برای ری استارت کردن ماشین مجازی به کار می‌رود.

```
from pyVim.connect import SmartConnect, Disconnect
from pyVmomi import vim
import ssl

# SSL بی‌اعتبار کردن بررسی (برای محیط‌های آزمایشی)
context = ssl._create_unverified_context()

# ESXi اطلاعات ورود به سرور
esxi_host = "192.168.5.6"
esxi_user = "root"
esxi_password = "Test@1999"

# ESXi اتصال به سرور
si = SmartConnect(host=esxi_host, user=esxi_user,
pwd=esxi_password, sslContext=context)
```

www.takbook.com


```
# بازیابی محتوا
content = si.RetrieveContent()

# تابع برای پیدا کردن ماشین مجازی با استفاده از نام
def get_vm_by_name(content, vm_name):
    container =
content.viewManager.CreateContainerView(content.rootFolder,
[vim.VirtualMachine], True)
    for vm in container.view:
        if vm.name == vm_name:
            return vm
    return None

# نام ماشین مجازی که می‌خواهید ریست کنید
vm_name = "TimeSheet"

# پیدا کردن ماشین مجازی
vm = get_vm_by_name(content, vm_name)

if vm:
    # چک کردن وضعیت ماشین مجازی
    if vm.runtime.powerState ==
vim.VirtualMachinePowerState.poweredOn:
        print(f"ریست کردن ماشین مجازی: {vm.name}")
        vm.ResetVM_Task()  # ریست کردن ماشین مجازی
    else:
        print(f"ماشین مجازی {vm.name} خاموش است.")
else:
    print(f"ماشین مجازی با نام {vm_name} پیدا نشد.")

# قطع اتصال
Disconnect(si)
```

توجه داشته باشید در کد بالا به جای تابع vm.ResetVM_Task() که برای Restart کردن ماشین مجازی کاربرد دارد می‌توانید از کدهای زیر استفاده کنید:

۱- PowerOffVM_Task() : خاموش کردن ماشین مجازی.

www.takbook.com

۲- PowerOnVM_Task() : روشن کردن ماشین مجازی.
۳- SuspendVM_Task() : تعلیق کردن ماشین مجازی.
۴- Destroy_Task() : برای حذف ماشین مجازی.

۳-۷-۱۸ ایجاد ماشین مجازی و روشن کردن آن

در این قسمت می‌خواهیم با استفاده از کد پایتون یک ماشین مجازی با نام Clinet1 ایجاد کنیم و آن را روشن کنیم، برای انجام این کار باید از کد زیر استفاده کنیم:

در کد زیر قسمت ESXi server connection details اطلاعات مربوط به سرور را وارد می‌کنیم، در قسمت Assume there is a datacenter, resource pool, and datastore available برای متصل کردن به دیتاسنتر و منابع Esxi قسمت بعدی یعنی Set the VM storage path in the datastore برای مشخص کردن Datastore به کار می‌رود، قسمت VM configuration (name, CPU, RAM, guest OS, and storage path) برای تنظیمات سخت‌افزاری ماشین مجازی است، قسمت Create the virtual machine برای ایجاد ماشین مجازی کاربرد دارد و قسمت Check the result of VM creation برای بررسی نتیجه ایجاد ماشین مجازی کاربرد دارد، قسمت Get the created virtual machine برای پیدا کردن ماشین مجازی که تازه ایجاد شده کاربر دارد و قسمت Power on the virtual machine هم برای روشن کردن ماشین مجازی کاربرد دارد.

```
from pyVim.connect import SmartConnect, Disconnect
from pyVmomi import vim
import ssl

# Disable SSL certificate verification
context = ssl._create_unverified_context()

# ESXi server connection details
si = SmartConnect(host="192.168.5.6", user="root",
pwd="Test@1999", sslContext=context)
content = si.RetrieveContent()

# Assume there is a datacenter, resource pool, and datastore
available
datacenter = content.rootFolder.childEntity[0]
resource_pool = datacenter.hostFolder.childEntity[0].resourcePool
datastore = datacenter.datastore[0]

# Set the VM storage path in the datastore
```

www.takbook.com


```
vm_folder = datacenter.vmFolder
datastore_path = f"[{datastore.name}] New_VM/New_VM.vmx"

# VM configuration (name, CPU, RAM, guest OS, and storage path)
vm_config = vim.vm.ConfigSpec(
    name="Client1",
    memoryMB=1024,  # 1GB RAM
    numCPUs=1,  # 1 CPU
    guestId="otherGuest64",  # guest OS type
    files=vim.vm.FileInfo(vmPathName=datastore_path)  # VM
storage path
)

# Create the virtual machine
task = datacenter.vmFolder.CreateVM_Task(config=vm_config,
pool=resource_pool)
print("Creating virtual machine...")
while task.info.state not in [vim.TaskInfo.State.success,
vim.TaskInfo.State.error]:
    pass

# Check the result of VM creation
if task.info.state == vim.TaskInfo.State.success:
    print(f"Virtual machine {vm_config.name} created
successfully.")

    # Get the created virtual machine
    vm = task.info.result

    # Power on the virtual machine
    print(f"Powering on virtual machine {vm_config.name}...")
    power_on_task = vm.PowerOnVM_Task()
    while power_on_task.info.state not in
[vim.TaskInfo.State.success, vim.TaskInfo.State.error]:
        pass

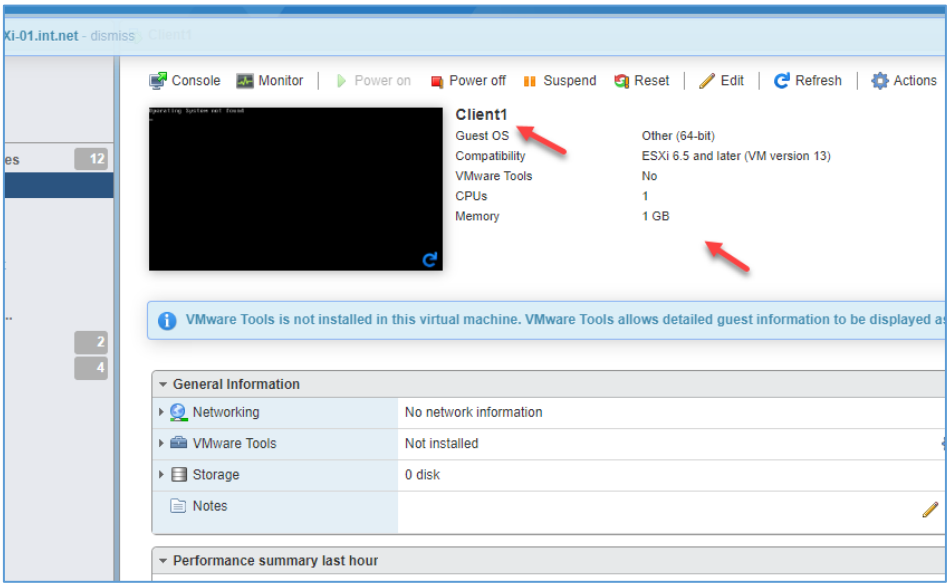
    if power_on_task.info.state == vim.TaskInfo.State.success:
```

www.takbook.com


```
        print(f"Virtual machine {vm_config.name} powered on
successfully.")
    else:
        print(f"Error powering on virtual machine:
{power_on_task.info.error.msg}")
else:
    print(f"Error: {task.info.error.msg}")

# Disconnect from the server
Disconnect(si)
```

بعد از اجرای کد مورد نظر اگر وارد Esxi شوید ماشین مورد نظر را به مانند شکل ۱۸-۳٤،مشاهده خواهید کرد.



شکل ۱۸- ۳۴ ریست کردن یک ماشین مجازی در ESXi

۱۸-۷-٤ روشن کردن تمام ماشین‌ها در ESXi

در بعضی مواقع نیاز دارید با یک کلیک تمام ماشین‌های موجود در ESXi را روشن کنید، برای این کار هم می‌توانیم از قدرت پایتون استفاده کنیم، برای انجام این کار از کد زیر استفاده می‌کنیم، در این کد و قسمت Disable SSL certificate verification برای صرف نظر کردن از SSL نامعتبر سرور است، در قسمت ESXi server connection details برای متصل شدن به سرور ESXi نوشته شده است، قسمت Function to power on all powered off VMs هم یک تابع برای روشن کردن همه‌ی ماشین‌های مجازی خاموش است، در آخر

www.takbook.com

کار هم در قسمت Power on all powered off VMs همه ماشین‌های خاموش روشن می‌شوند و در خط آخر ارتباط قطع خواهد شد.

```
from pyVim.connect import SmartConnect, Disconnect
from pyVmomi import vim
import ssl

# Disable SSL certificate verification
context = ssl._create_unverified_context()

# ESXi server connection details
si = SmartConnect(host="192.168.5.6", user="root",
pwd="Test@1999", sslContext=context)
content = si.RetrieveContent()

# Function to power on all powered off VMs
def power_on_all_vms(content):
    # Get the datacenter
    datacenter = content.rootFolder.childEntity[0]  # Assumes
there is at least one datacenter
    vms = datacenter.vmFolder.childEntity

    for vm in vms:
        if isinstance(vm, vim.VirtualMachine):
            if vm.runtime.powerState ==
vim.VirtualMachinePowerState.poweredOff:
                print(f"Powering on VM: {vm.name}...")
                task = vm.PowerOnVM_Task()

                # Wait for the power on task to complete
                while task.info.state not in
[vim.TaskInfo.State.success, vim.TaskInfo.State.error]:
                    pass

                if task.info.state == vim.TaskInfo.State.success:
                    print(f"VM {vm.name} powered on
successfully.")
                else:
```

www.takbook.com


```
                    print(f"Error powering on VM {vm.name}:
{task.info.error.msg}")

# Power on all powered off VMs
power_on_all_vms(content)

# Disconnect from the server
Disconnect(si)
```

www.takbook.com

www.takbook.com

منابع کتاب

- CCNA 200-3001 Farshid Fardmanesh – Azadeh Mehrayin
- CCNP Enarsi Farshid Fardmanesh - Azadeh Mehrayin
- CCNA Security Farshid Fardmanesh - Azadeh Mehrayin
- CompTIA Network+ Study Guide Exam N10-008 – Todd Lammle
- VMware vSphere Essentials - Luciano Patrão
- Learning VMware vSphere – Abhilash
- Mastering VMware vSphere 6 - Nick Marshall, Scott Lowe (Foreword by) with Grant Orchard, Josh Atwell
- CompTIA Security+ SY0-601 Cert Guide, 5th Edition – Omar Santos, Ron Taylor
- Networking with MikroTik: MTCNA Study Guide – Tyler Hart
- Mastering Veeam Backup & Replication – Third Edition - Chris Childerhose

برای بررسی مشکلات و دریافت اطلاعات مربوط به این کتاب می‌توانید وارد کانال تلگرام مربوط به این کتاب شوید:

https://t.me/+GsNYIHTJOQQ1MmRk