
بسم الله الرحمن الرحيم

مدرس:

سپیده برادران هزاوه

زمستان ۹۵

Configuration network servers

نحوه ارزشیابی

کار کلاسی و ارایه

۴ نمره

امتحان پایان ترم

۱۶ نمره

رئوس مطالب

- مفاهیم و پیکربندی زیرساخت Active Directory
- پیکربندی DNS و ساخت و نگهداری اشیای Active Directory
- زیرساخت فیزیکی
- توسعه و زیرساخت دسترسی

Active Directory

شاید اولین آزمون جهت فراگیری و کار با ویندوز سرور 2008 و 2008R2، نصب آن بر روی یک سیستم است که این سیستم می‌تواند یک ماشین فیزیکی و یا ماشینی مجازی[1] باشد. عملیات نصب به دو روش دستی[2] و خودکار قابل انجام است که البته انتخاب روش آن اختیاری است و به شرایط و محیط مورد نظر بستگی دارد.

در این فصل، قصد داریم عملیات نصب ویندوز سرور و ارتقاء یا مهاجرت از نسخه‌های قبلی (2003) به نسخه 2008R2 را مورد بررسی قرار داده و نکاتی کلیدی در رابطه با آن بیان کنیم. بطور کلی مهمترین مباحثی که در این فصل به آنها پرداخته خواهد شد عبارتند از:

- نصب ویندوز سرور (به صورت دستی و خودکار)
- ارتقاء به ویندوز سرور 2008 و 2008R2
- پیکربندی مقدماتی ویندوز سرور

تغییرات نصب نسبت به ویندوز سرور 2000 و 2003

عملیات نصب در ویندوز سرور 2008R2 بسیار راحت‌تر از نسخه‌های قبلی آن (2000 و 2003) شده است. بسیاری از افراد زمانی که عبارت " نصب ویندوز سرور " را می‌شنوند، عملیاتی پیچیده در ذهنشان مجسم می‌گردد در صورتی که اینگونه نخواهد بود. اگر این افراد قبلاً یکی از ویندوزهای ویستا یا ویندوز۷ را نصب کرده باشند، آنگاه متوجه خواهند شد که نصب ویندوز سرور 2008R2 نه تنها پیچیده نیست، بلکه بسیار ساده و لذت بخش می‌باشد. در هنگام نصب ویندوز سرور 2000 و 2003 سؤالات زیادی به منظور انجام تنظیمات و یا راه اندازی قابلیت‌ها از شما پرسیده می‌شود، اما در نسخه 2008R2، این سؤالات به حداقل رسیده است که این امر به لحاظ ایجاد امنیت بیشتر در هنگام نصب می‌باشد.

اما پاسخ به سؤالات کمتر در نصب ویندوز سرور به چه معناست؟ وقتی سؤالات کمتری پرسیده می‌شود، پس ویژگی‌ها و قابلیت‌های کمتری برروی سرور نصب خواهد شد. این امر موجب می‌شود تا شما تنها یک سرور با قابلیت‌های پیش‌فرض داشته باشید و با حجم زیادی از سرویس‌ها و عملکردها روبرو نخواهید بود. بنابراین می‌توانید پس از نصب با توجه به نوع عملیاتی که سرور در شبکه قرار است انجام دهد، آن را پیکربندی کنید. مسلماً این کار میزان حملات به سرور را کاهش خواهد داد، زیرا زمانی که شما سرویس‌های بیشتری نصب می‌کنید، اهداف بیشتری برای نفوذگران فراهم می‌کند.

---

1. Virtual Machine
2. Manual

۲-۲ نیازمندی‌های نصب ویندوز سرور 2008 و 2008R2

قبل از نصب ویندوز، لازم است از نیازهای سخت‌افزاری آن آگاه شوید. ما در اینجا حداقل نیازها، نیازهای پیشنهادی (مناسب)، و حداکثر نیاز سخت‌افزاری برای نصب ویندوز سرور 2008 و 2008R2 را در قالب دو جدول ارائه می‌دهیم. توجه داشته باشید که منظور از "حداقل"، دقیقاً کمترین سخت افزاری است که می‌توانید ویندوز سرور را بر روی آن نصب کنید. البته انتخاب سخت افزارها، به کاربردهای سرور در شبکه، برنامه‌های اجرا شونده بر روی آن، و سرویس‌هایی که قرار است ارائه دهد (با توجه به تعداد کاربران) بستگی دارد. بنابراین، لازم است ابتدا سخت افزارهای مناسب را فراهم نموده و سپس اقدام به نصب نمایید.

در جداول۲-۱ و ۲-۲، نیازمندی‌های ارائه شده توسط شرکت مایکروسافت، برای نصب ویندوز سرور 2008 و 2008R2 آورده شده است.

سخت افزار	حداقل	پیشنهاد شده	حداکثر
CPU	1.4GHz	2 GHz	٤ پردازنده برای ویرایش Standard ٨ پردازنده برای ویرایش Enterprise ٦٤ پردازنده برای ویرایش Datacenter
RAM	512 MB	2 GB یا بیشتر	32GB برای ویرایش Standard 2TB برای ویرایش‌های Enterprise، Datacenter و Itanium
Disk	10GB	40GB به اضافه فضایی برای برنامه‌ها و داده‌ها	
DVD-ROM	به دلیل اینکه نصب از روی DVD انجام می‌شود نیاز است.		
Display	Super-VGA (800-600) یا بالاتر		
Input Devices	صفحه کلید و ماوس		

پشتیبانی ۶۴ بیتی

اگر تا به حال با ویندوز سرور 2003 و 2008 کار کرده باشید، حتماً شنیده‌اید که این دو ویندوز در دو نسخه ۳۲ و ٦٤ بیتی موجود می‌باشند. منظور از x64، نسخه‌های ٦٤ بیتی و منظور از x86، نسخه‌های ۳۲ بیتی از نرم‌افزارها (یا سیستم‌عامل‌ها) می‌باشند. سیستم عامل ویندوز سرور 2008R2 و

برنامه‌هایی مانند Microsoft Exchange Server 2007 فقط به صورت ٦٤ بیتی یا x64 هستند.

لازم است نکاتی را در رابطه با راه‌اندازی سرورهای ٦٤ بیتی یادآور شویم:

- پشتیبانی سخت افزارها از x64 مسئله بزرگی نیست. بسیاری از تولید کنندگان، سال‌های زیادی است که پردازنده‌های x64 را به عنوان یکی از محصولات اصلی خود، تولید می‌کنند. بنابراین آگاهی از این موضوع که سخت افزار شما از ٦٤ بیت پشتیبانی می‌کند، کار سختی نیست.
- بسیاری از برنامه‌های ۳۲ بیتی قادرند بر روی ویندوز ویندوز سرور 2008R2 اجرا شوند. به کمک زیرسیستمی به نام WOW32[1] امکان شبیه‌سازی اکثر نرم‌افزارهای ۳۲ بیتی، و اجرای آنها بر روی ویندوز سرور 2008R2 فراهم شده‌است.
- امکان ارتقاء x86 به x64 وجود ندارد. در صورتی که سرور 2003 و یا 2008 شما، برروی پردازنده‌های x86 قرار دارند، نمی‌توانید آنها را به 2008R2 ارتقاء دهید و باید سخت افزارهای x64 تهیه کنید.
- درایورهای سخت افزاری شما باید متناسب با سیستم عامل باشند. لازم است قبل از نصب سخت افزارها و درایورهای مربوط به آن، از سازگاری آنها با سیستم عامل جدید اطمینان حاصل کنید تا در استفاده از آنها با مشکل مواجه نشوید.

همانطور که قبلاً اشاره شد، نصب ویندوزسرور 2008 و 2008 R2 بسیار ساده است. بطور کلی عملیاتی که برای نصب باید انجام شود عبارتند از:

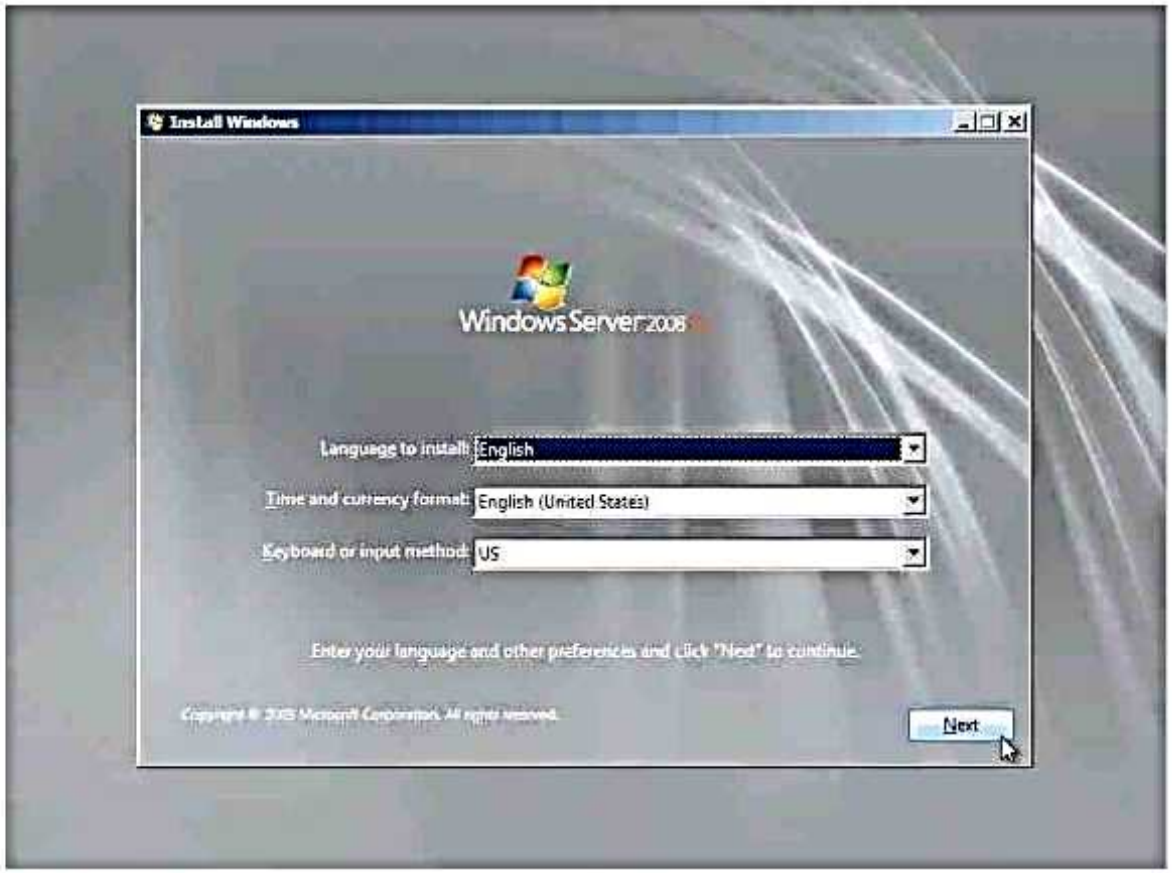
1. Windows-on-Windows

- بوت کردن سیستم از روی DVD ویندوز سرور 2008R2
- وارد نمودن کد License
- انتخاب ویرایش ویندوز
- انتخاب یکی از عملیات "نصب" یا "ارتقاء[۲]"
- پیکربندی فضای دیسک (هارد دیسک)
- تنظیم رمز عبور برای ورود مدیر
- ورود به سیستم

۲-۲ نصب دستی سیستم‌عامل

منظور از نصب دستی (یا کامل) سیستم عامل، اجرای عملیات نصب برروی سیستمی است که قبلاً فاقد سیستم عامل بوده و یا دیگر نیازی به سیستم عامل موجود بر روی آن نیست. ما در اینجا فرض را بر این قرار می‌دهیم که سیستم فاقد هرگونه سیستم عامل (قبلی) است و شما نیز تا به حال سیستم عاملی از این نوع را نصب نکرده‌اید. بنابراین مراحل کار را از ابتدا شرح خواهیم داد.

۱. اولین مرحله در نصب ویندوز سرور 2008R2، راه‌اندازی عملیات Boot از روی DVD ویندوز می‌باشد. برای انجام این کار، لازم است که در تنظیمات BIOS سیستم، راه‌اندازی عملیات را بر روی DVD-ROM (یا DVD-Writer) قرار دهید و پس از ذخیره تنظیمات، سیستم را Restart کنید. پس از انجام این عملیات، صفحه‌ای به صورت زیر، نشان داده خواهد شد.



همانطور که در شکل ۲-۱ مشاهده می‌کنید، در این صفحه سه گزینه در اختیار شما قرار داده می‌شود:

- Language to install: این گزینه زبان سرور را مشخص می‌کند. به عبارت دیگر، در این قسمت هر زبانی را که انتخاب کنید، عملیات نصب با آن انجام شده و پس از نصب، زبان پیش‌فرض ویندوز خواهد بود.
- Time and currency format: این گزینه مربوط به تنظیمات منطقه زمانی می‌باشد. با انتخاب منطقه زمانی، نحوه نمایش تاریخ و ساعت را در سرور مشخص می‌کنید.
- Keyboard or input method: این گزینه مربوط به تنظیمات زبان پیش‌فرض صفحه کلید شما می‌باشد.

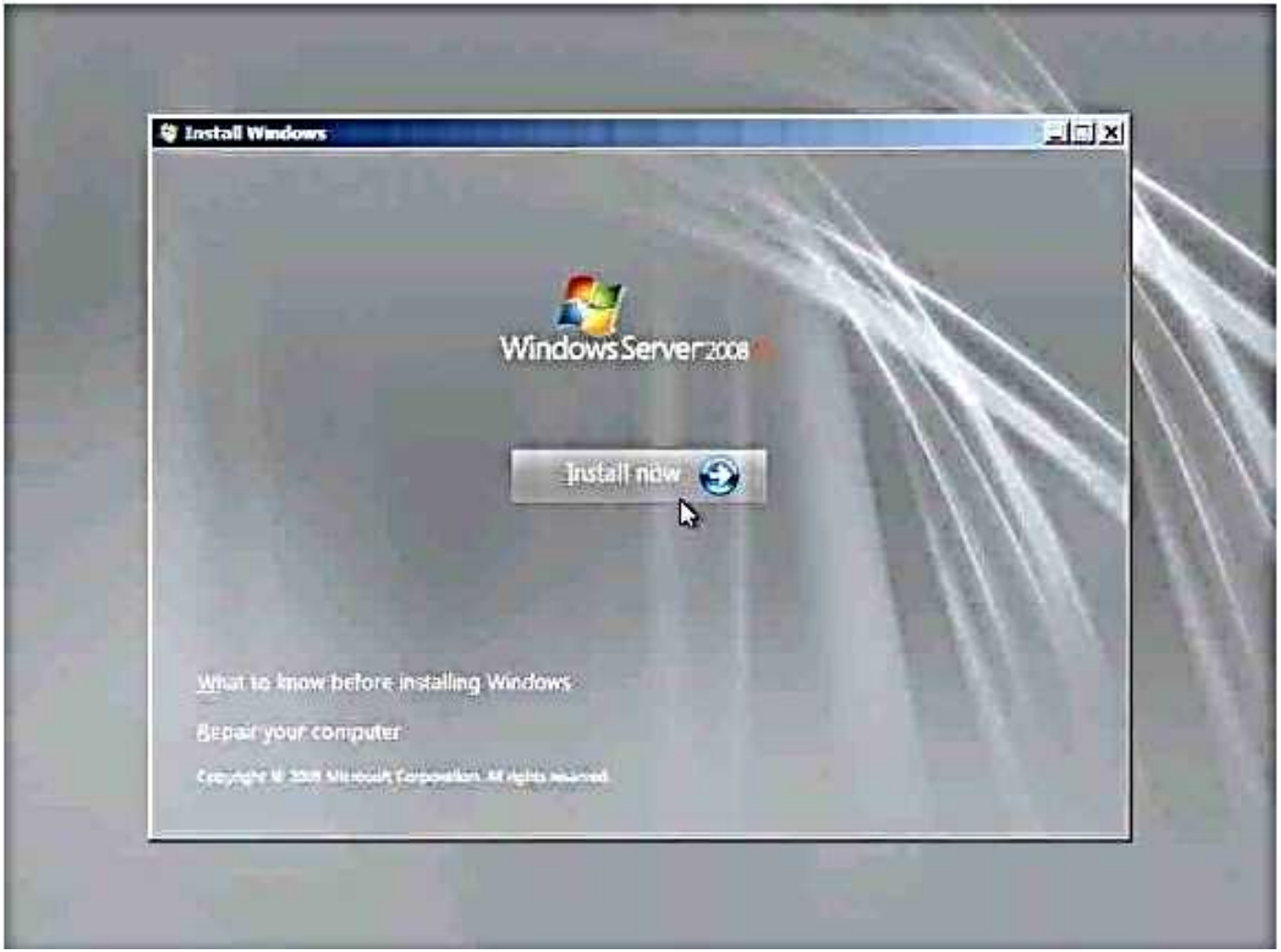
پس از انجام تنظیمات مورد نظر، برروی Next کلیک کنید.

۲. با ورود به مرحله جدید، مجدداً با چند گزینه مواجه خواهید شد. این گزینه‌ها عبارتند از:

- Install now: با کلیک برروی این دکمه، مراحل نصب ویندوز ادامه پیدا می‌کند.
- What to now before installing Windows: نکاتی را راجع به مراحل نصب ویندوز و دانستنی‌های قبل از آن بیان می‌کند.
- Repair your computer: چنانچه قبلاً ویندوزی برروی کامپیوتر وجود داشته باشد، عملیات Repair (ترمیم) را برروی آن انجام می‌دهد.

برروی دکمه Install now کلیک کنید.

برروی دکمه Install now کلیک کنید.



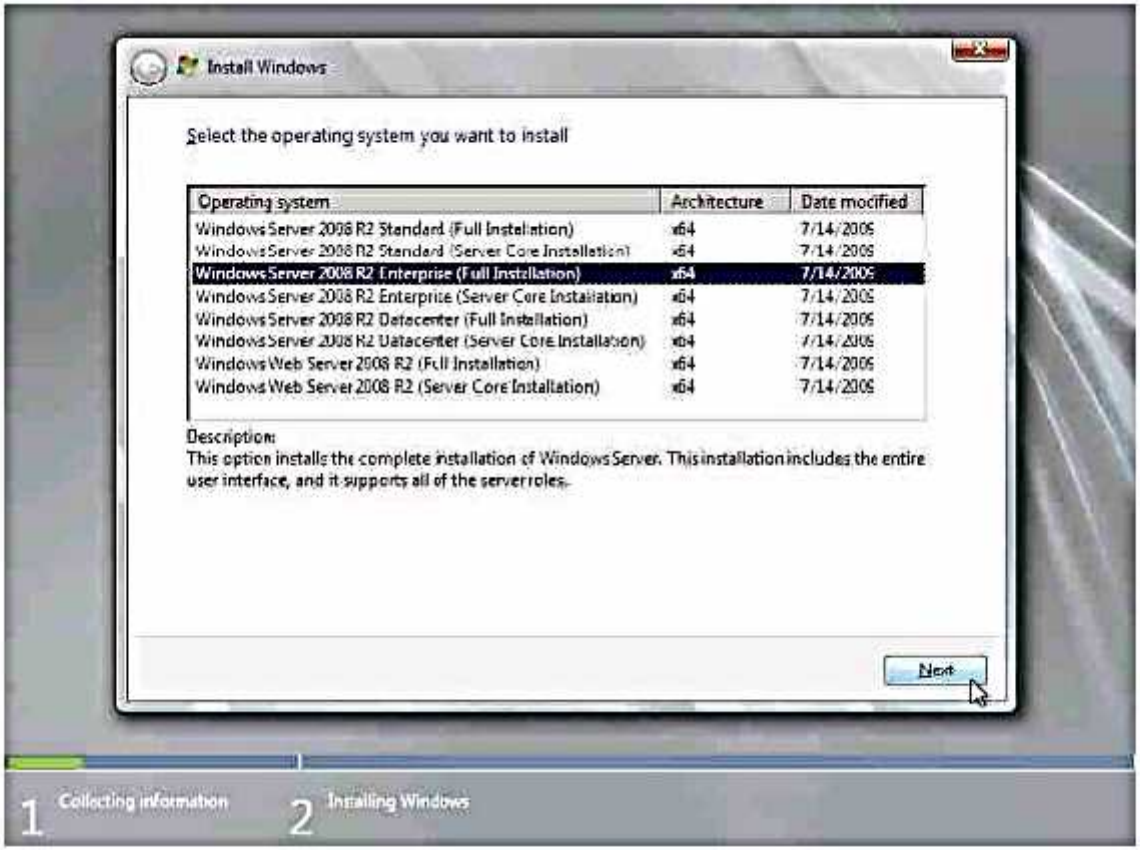
۳. در صفحه "Type your product key for activation" از شما کد License خواسته می‌شود. این کد جهت Active کردن ویندوز می‌باشد (چنانچه ویندوز را Active نکنید، امکان دریافت آپدیت‌های ویندوز از سایت ماکروسافت را نخواهید داشت). در صورتی که این کد را در اختیار دارید، آنرا وارد نموده و در غیر این صورت، با فعال نمودن گزینه Automatically active Windows when I'm online از این مرحله صرفنظر کنید. سپس برروی Next کلیک کنید.

٤. در صفحه "Select the operating system you want to install" باید ویرایشی[1] از ویندوز سرور 2008 R2 که قصد دارید آنرا برروی سیستم نصب کنید، انتخاب نمایید. در اینجا، چهار ویرایش قابل انتخاب است که عبارتند از: Standard، Enterprise، Datacenter و Web Server. هر ویرایش از قابلیت‌ها و ویژگی‌های خاص برخوردار است و باید با توجه به عملکرد سرور و سخت‌افزارهای آن، ویرایش مورد نظر را انتخاب نمایید. دقت داشته باشید که هر ویرایش به دو دسته Full Installation و Server Core Installation تقسیم می‌شود. در دسته اول (Full Installation)، حجم زیادی از ابزارها و واسطهای گرافیکی در اختیار خواهید داشت که مدیریت ویندوز را برای شما آسانتر می‌کند، اما در دسته دوم (Server Core Installation) فرض بر این است که شما جزء کاربران خط فرمان[2] هستید و بیشتر با کدها و دستورات، اعمال مدیریتی را انجام می‌دهید. بنابراین در این حالت، از واسطهای گرافیکی بسیار کمی استفاده شده است.

یکی از ویرایش‌های Standard یا Enterprise (Full Installation) را انتخاب و برروی Next کلیک کنید.

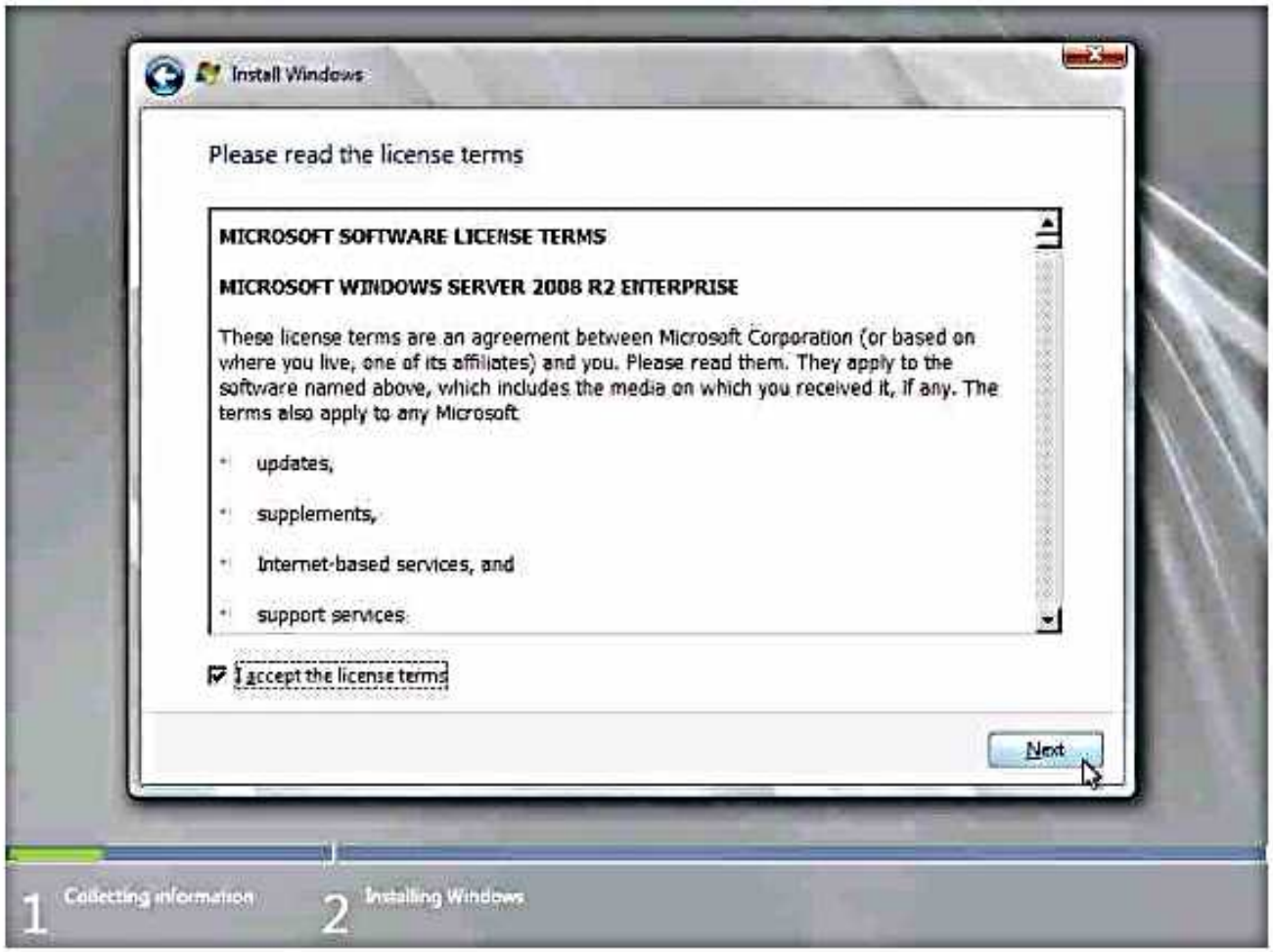
---

1. Edition



شکل ۲-۴

۵. در صفحه "Please read the license terms" مجموعه‌ای از قوانین برای استفاده از ویندوزسرور 2008R2 و License آن آورده شده است (این قوانین "توافق‌نامه مجوز کاربر نهایی[۱]" (EULA) شناخته می‌شوند). گزینه I accept the license terms را انتخاب نموده و بر روی Next کلیک کنید.

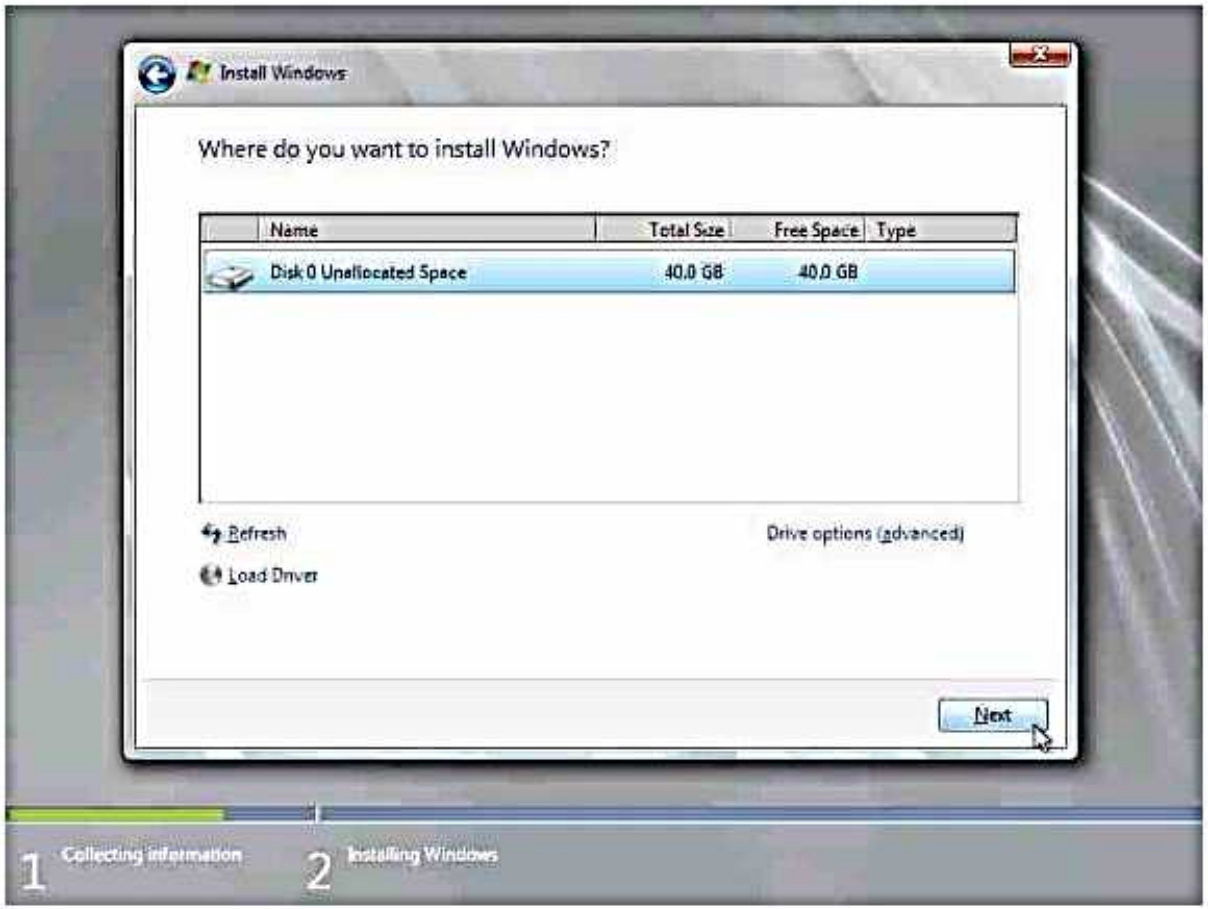


شکل ۲-۵

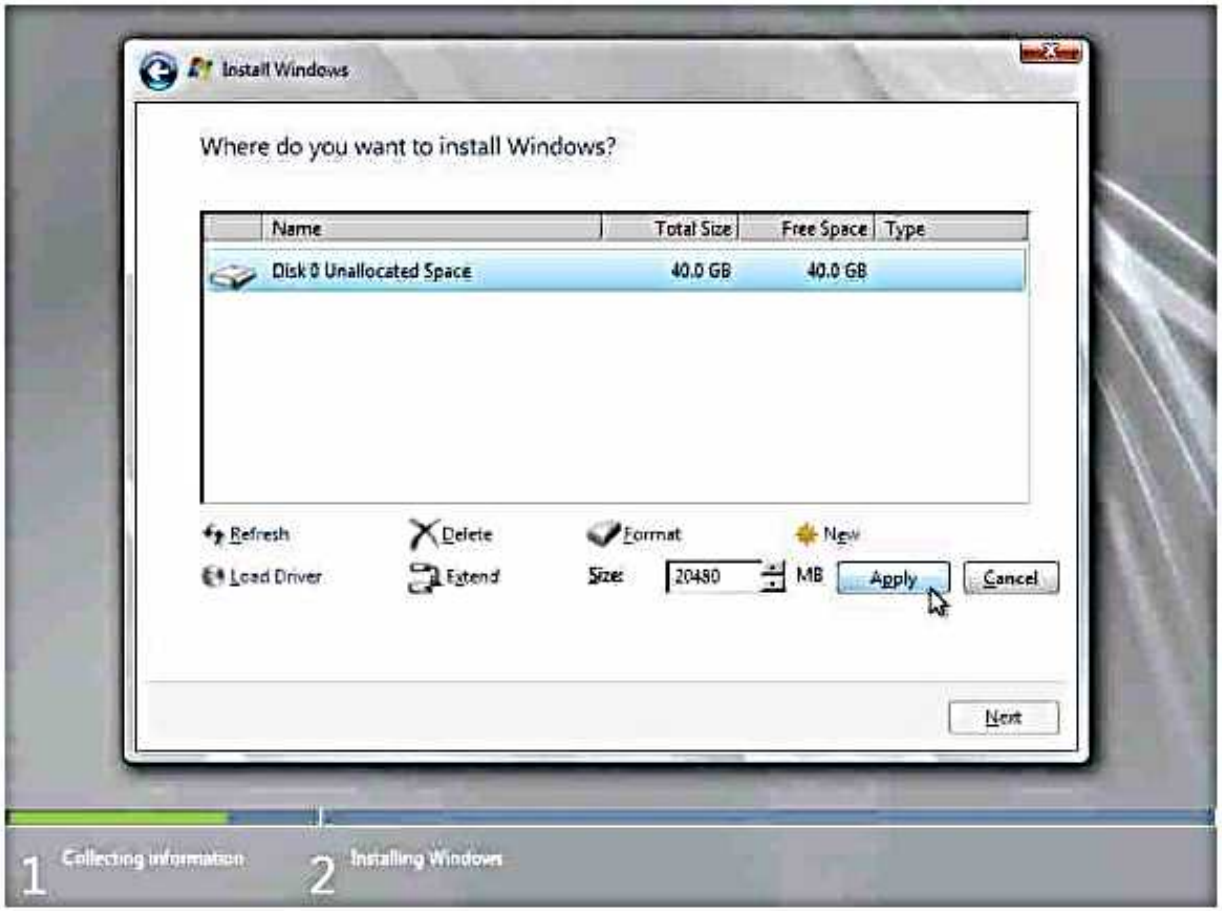
1. End User License Agreement

٦. در صفحه "Which type of installation do you want?" جهت نصب سیستم عامل گزینه Custom Advanced را انتخاب و برروی Next کلیک کنید (گزینه Upgrade بعداً شرح داده خواهد شد).

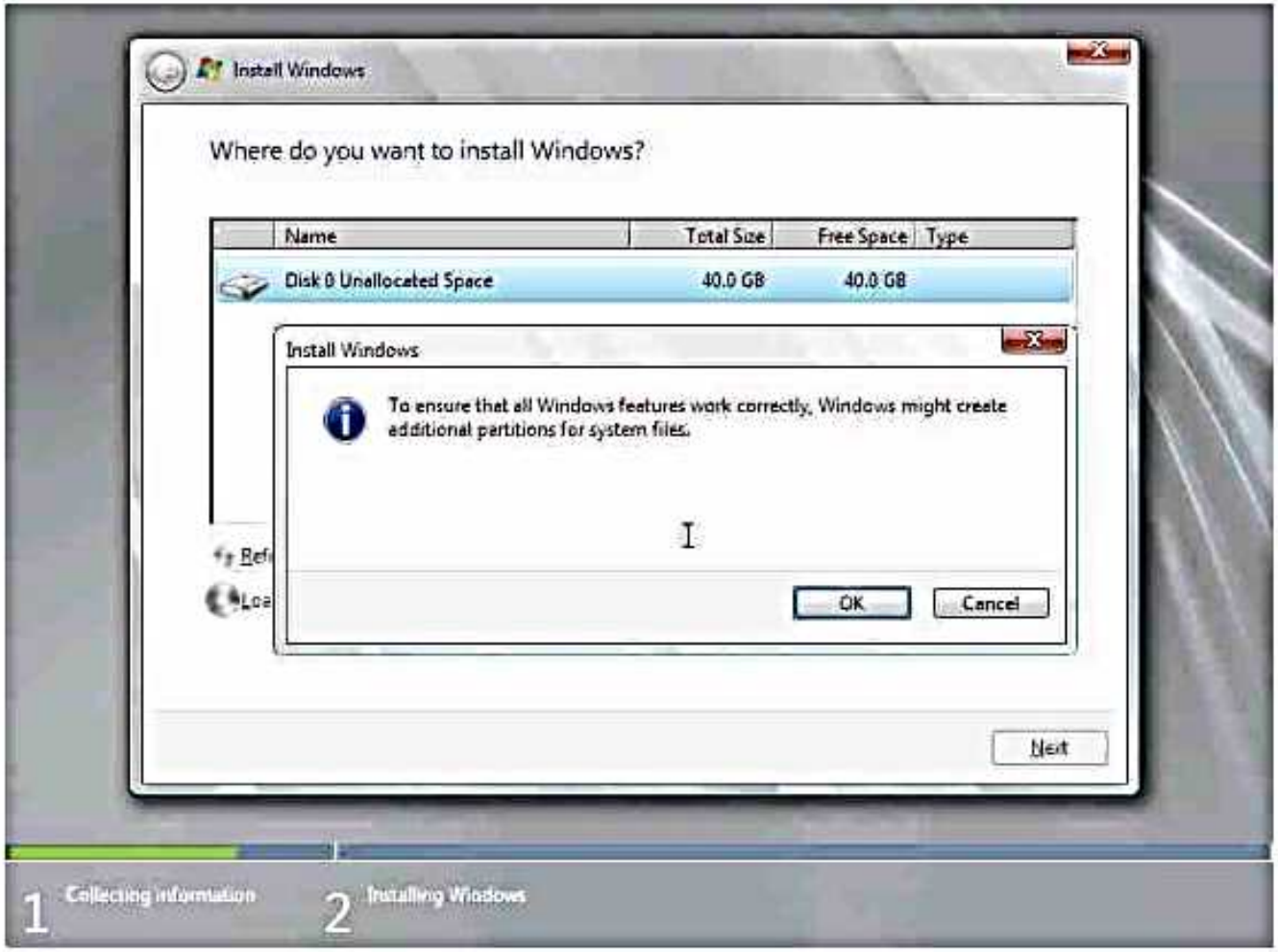
۷. در صفحه "Where do you want to install Windows" باید محل نصب ویندوز را مشخص کنید. در اینجا، فضای هارد دیسک قبلاً پارتیشن‌بندی نشده و کل فضای آن به یک پارتیشن تبدیل شده است. اگر قصد دارید در همین پارتیشن ویندوز را نصب نمایید بر روی Next کلیک کنید.



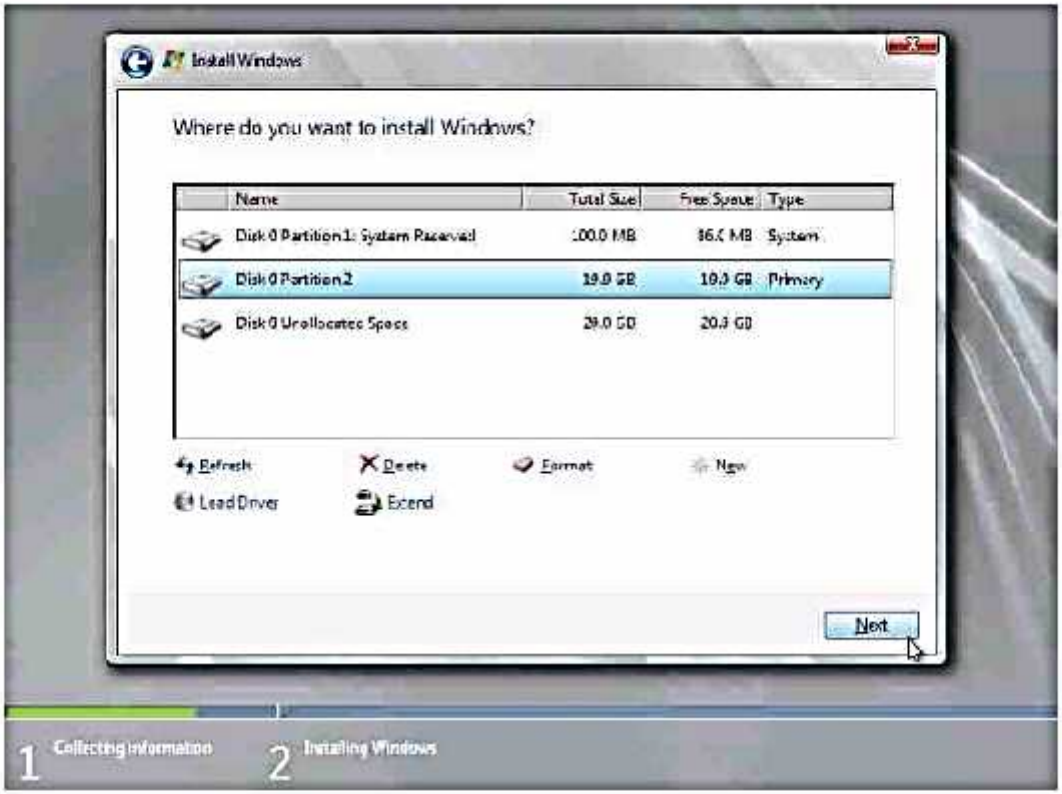
۸. در صورتی که قصد دارید فضای هارد دیسک خود را به چندین پارتیشن تقسیم نموده و ویندوز را در یکی از آنها نصب کنید، می‌توانید از پایین پنجره، بر روی Drive options کلیک نموده و New را انتخاب کنید. سپس در قسمت Size حجم پارتیشن را تعیین و بر روی Apply کلیک کنید.



۹. پیغامی ظاهر شده و اعلام می‌کند که یک پارتیشن اضافی برای فایل‌های سیستمی نیز ایجاد می‌گردد. برروی OK کلیک کنید.



۱۰. پس از ایجاد پارتیشن (درایو)، آنرا انتخاب نموده و بر روی Next کلیک کنید.

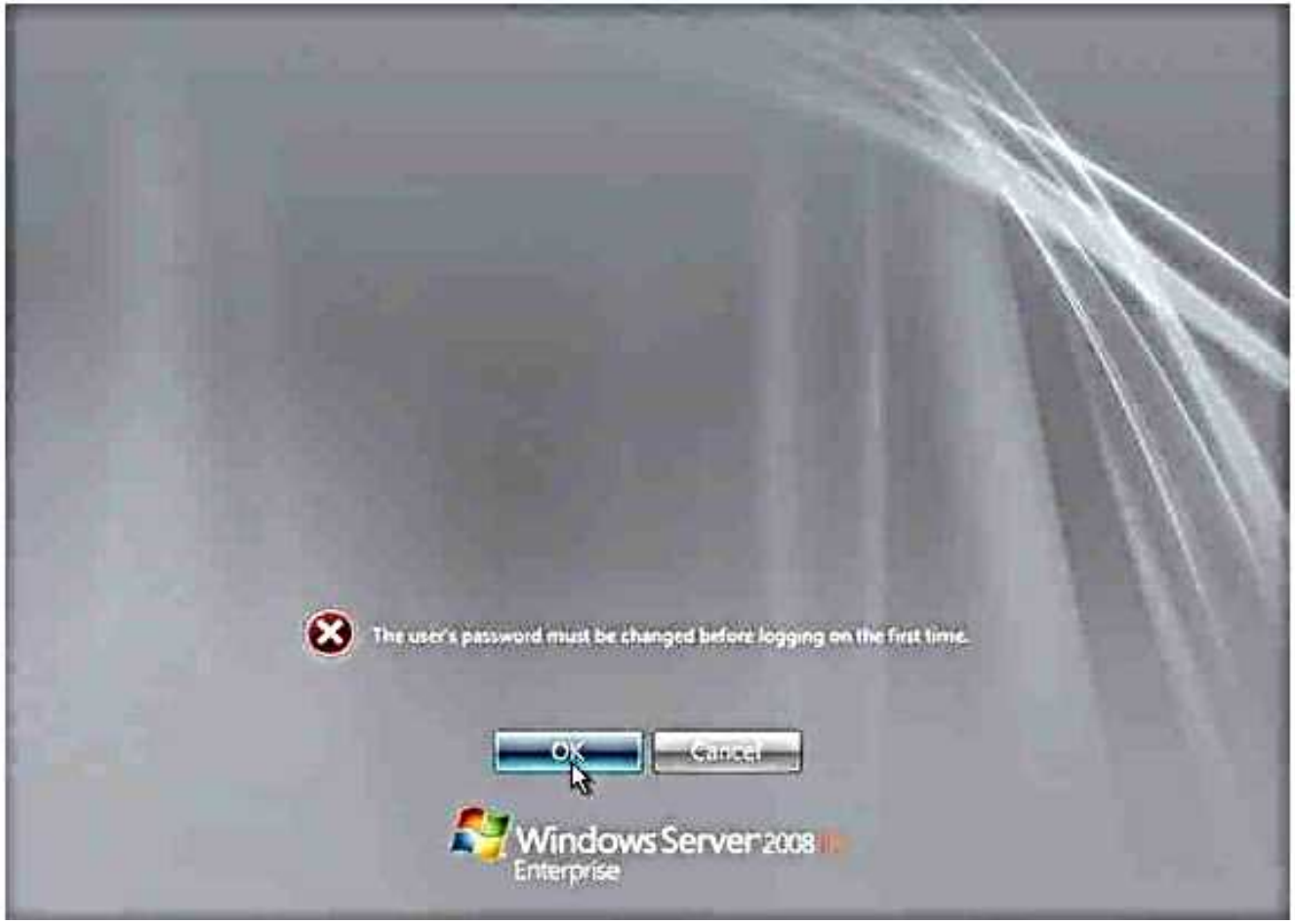


شکل ۲-۱۰

۱۱. با مشاهده صفحه "Installing Windows" عملیات نصب ویندوز آغاز می‌گردد. منتظر بمانید تا این عملیات به اتمام برسد. ممکن است در طی این عملیات، سیستم چند بار Restart شود، بنابراین بدون نیاز به انجام کار اضافه، تا پایان عملیات منتظر بمانید.

۱۱. با مشاهده صفحه "Installing Windows" عملیات نصب ویندوز آغاز می‌گردد. منتظر بمانید تا این عملیات به اتمام برسد. ممکن است در طی این عملیات، سیستم چند بار Restart شود، بنابراین بدون نیاز به انجام کار اضافه، تا پایان عملیات منتظر بمانید.

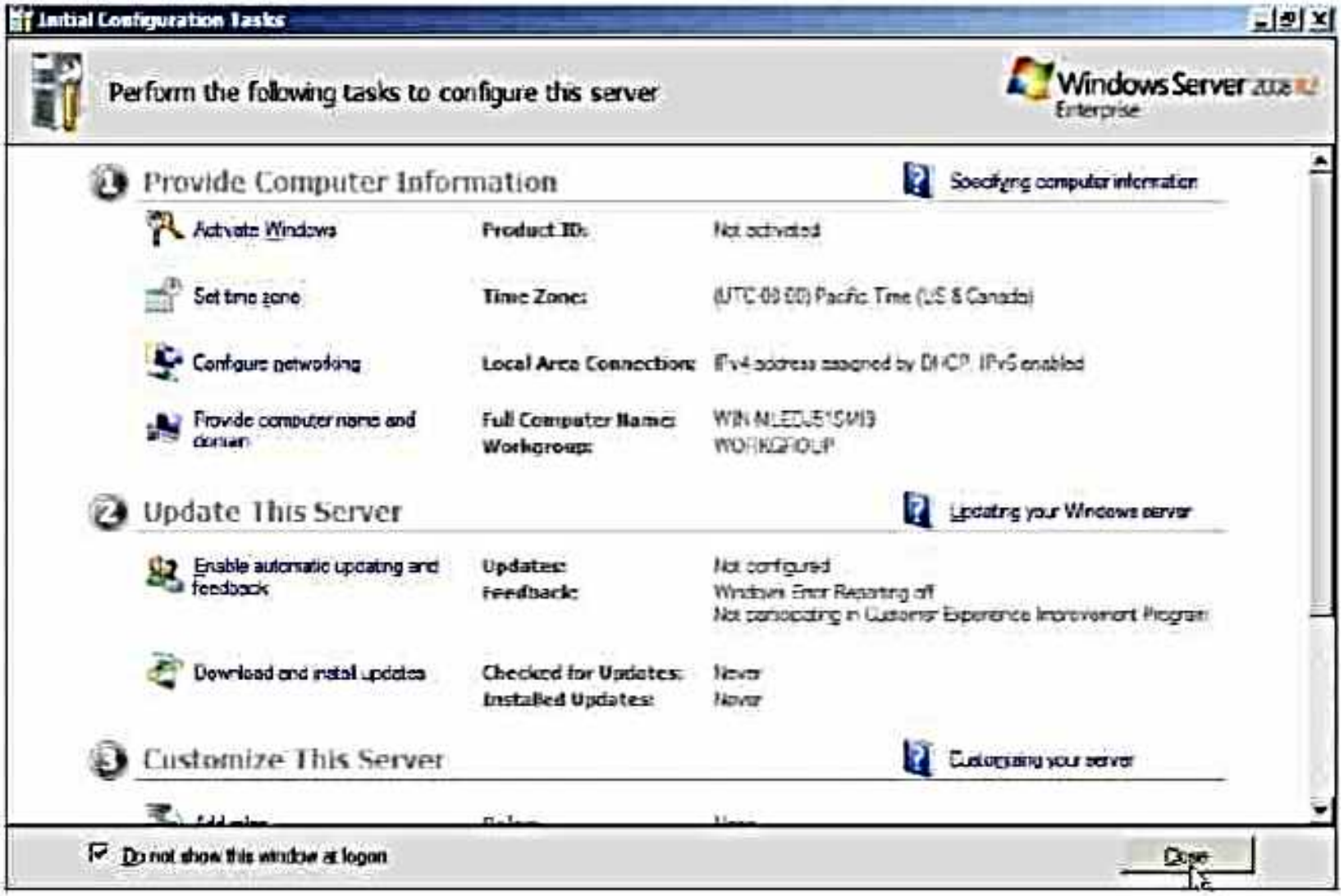
۱۲. پس از پایان عملیات نصب، صفحه‌ای شبیه زیر نشان داده خواهد شد. در این صفحه، ویندوز سرور 2008R2 از شما می‌خواهد که رمز عبور را تغییر دهید. بر روی OK کلیک کنید.



۱۳. با مشاهده صفحه زیر، در قسمت‌های مشخص شده رمز عبور یکسانی وارد نموده و برروی دکمه جهتی (→) کلیک کنید. دقت کنید که رمز عبور باید حداقل ترکیبی از هشت یا نه کاراکتر و متشکل از حروف بزرگ، حروف کوچک و اعداد باشد (از کاراکترهایی مانند @ نیز می‌توان استفاده نمود).

۱٤. پس از انتخاب رمز عبور، قادر خواهید بود به عنوان مدیر[1] وارد سیستم شوید. توجه داشته باشید که اولین ورود شما به داخل سیستم ممکن است کمی طول بکشد، این امر به دلیل آماده‌سازی تنظیمات شما و برخی از آیتم‌های موجود در Desktop می‌باشد.

۱۵. بعد از ورود کامل به سیستم و مشاهده دسکتاپ، پنجره‌ای تحت عنوان Initial Configuration Tasks نشان داده خواهد شد. در این پنجره، ابزارهایی جهت پیکربندی[2] اولیه سرور قرار داده شده است و به کمک آنها می‌توانید سرور را به صورت ابتدایی پیکربندی کنید، اما پیشنهاد ما این است که این کار را به کمک Server Manager انجام دهید (این ابزار، از طریق منوی Start یا خط فرمان (Cmd) قابل دسترسی می‌باشد. در همین فصل، نحوه کار با Server Manager را شرح خواهیم داد).


Initial Configuration Tasks
Perform the following tasks to configure this server
Windows Server
Enterprise
Provide Computer Information
Specifying computer information
Activate Windows
Product ID:
Not activated
Set time zone
Time Zone:
(UTC-08:00) Pacific Time (US & Canada)
Configure networking
Local Area Connection:
Provide computer name and domain
Full Computer Name:
Workgroup:
WORKGROUP
Update This Server
Updating your Windows server
Enable automatic updating and feedback
Updates:
Not configured
Feedback:
Windows Error Reporting off
Not participating in Customer Experience Improvement Program
Download and install updates
Checked for Updates:
Never
Installed Updates:
Never
Customize This Server
Customizing your server
Do not show this window at logon
Close

نصب و راه اندازی

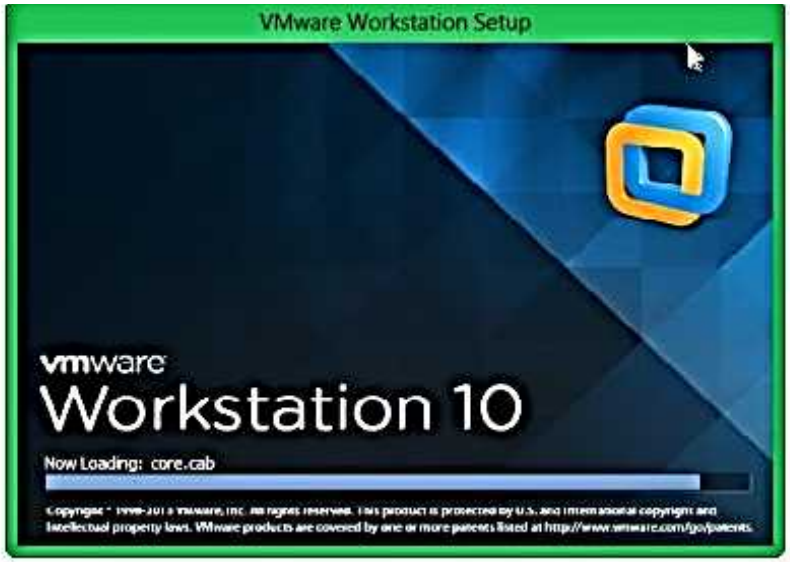
VM Ware

شروع کار

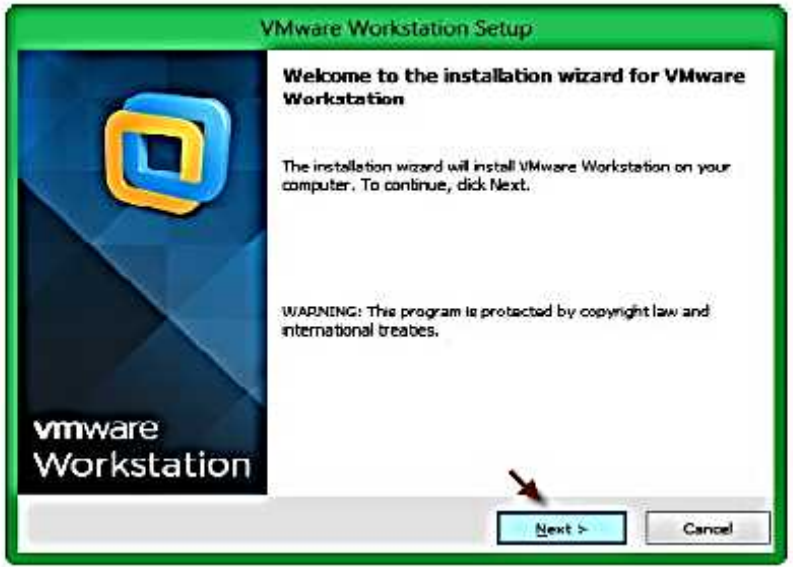
این نرم‌افزار با هزاران کاربر در سراسر جهان، کارایی را در آفریدن نرم‌افزارها بهبود می‌بخشد، هزینه‌ها را کاهش می‌دهد، نرمش و انعطاف پذیری را بالا می‌برد و راه امن تری برای پاسخ گرفتن از برنامه‌ها را در دسترس ما می‌گذارد. VMware جزساده کردن پردازش می‌تواند گسترش، تست نرم‌افزار و شتاب دادن به گسترش برنامه‌های کاربردی، سازگاری برنامه‌های کاربردی و پیاده سازی عملی فرستادن از یک سیستم عامل به سیستم عامل دیگر را بیمه کند و توانایی آزمایش این که آیا این جابجایی و جایگزینی سیستم عامل، زیانی برای شبکه یا دیگر نرم‌افزارهای کاربردی در حال کار دارد یا خیر را نمایان می‌سازد.

VMware دارای ویژگی هایی زیر می‌باشد:

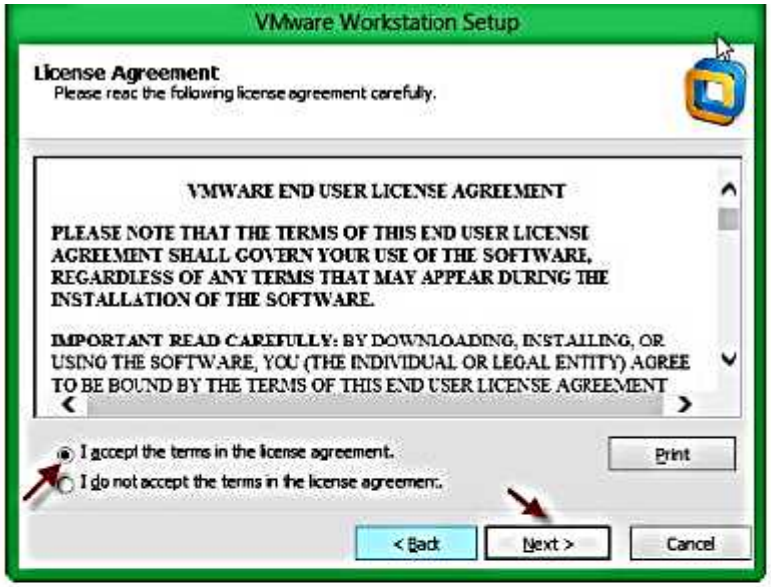
- ✓ توانایی بهره گیری از توان سخت افزارها.
- ✓ توانایی سرپرستی سرورها بگونه یکتا در یک ماشین سخت افزاری.
- ✓ اجرای برنامه‌های سیستم‌های عامل گوناگون بر روی یک ماشین.
- ✓ شبکه بندی (Virtual Networking)
- ✓ انجام تراکنشها بگونه Real time
- ✓ درمیان گذاری پوشه‌ها به صورت Drag and Drop



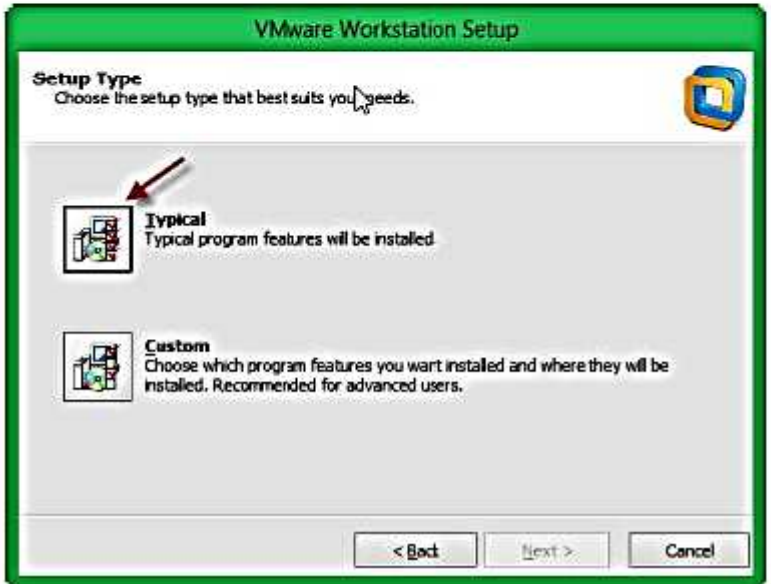
نرم افزار در حال خارج شدن از حالت فشرده و اجرای حالت اصلی.



در این صفحه که صفحه خوش آمد گویی می باشد ، یک اخطار همون اول کار می دهد که می گوید لطفاً این نرم افزار را به صورت کپی استفاده نکنید

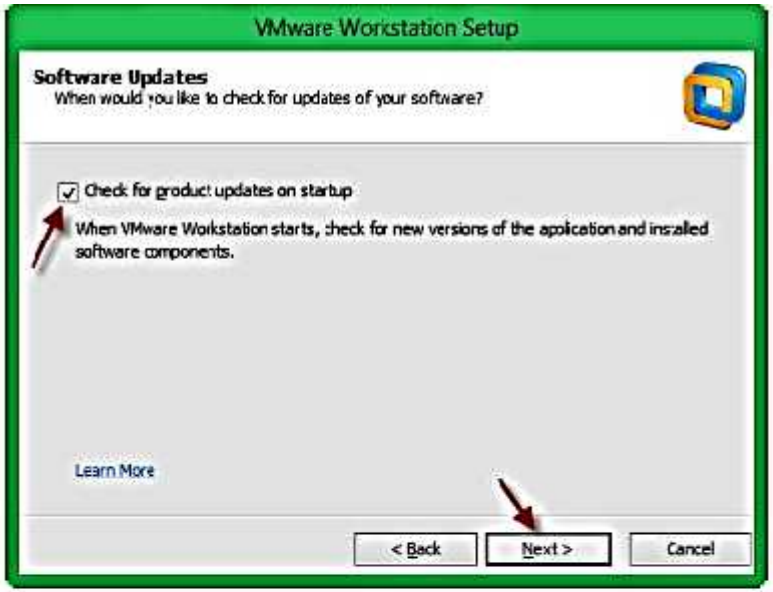


در این قسمت توافقنامه این نرم افزار را خوانده و اگر قبول دارید بر روی گزینه I Accept ... کلیک کنید و بعد بر روی Next کلیک کنید.

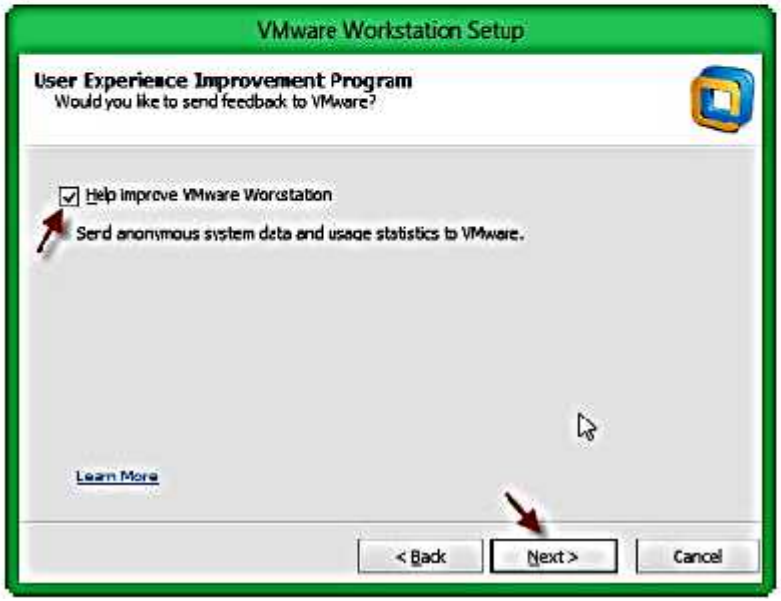


در این قسمت بر روی Typical کلیک کنید

در این قسمت با کلیک کردن بر روی Change... می توانید مسیر نصب برنامه را مشخص کنید، بعد از این کار بر روی Next کلیک کنید.

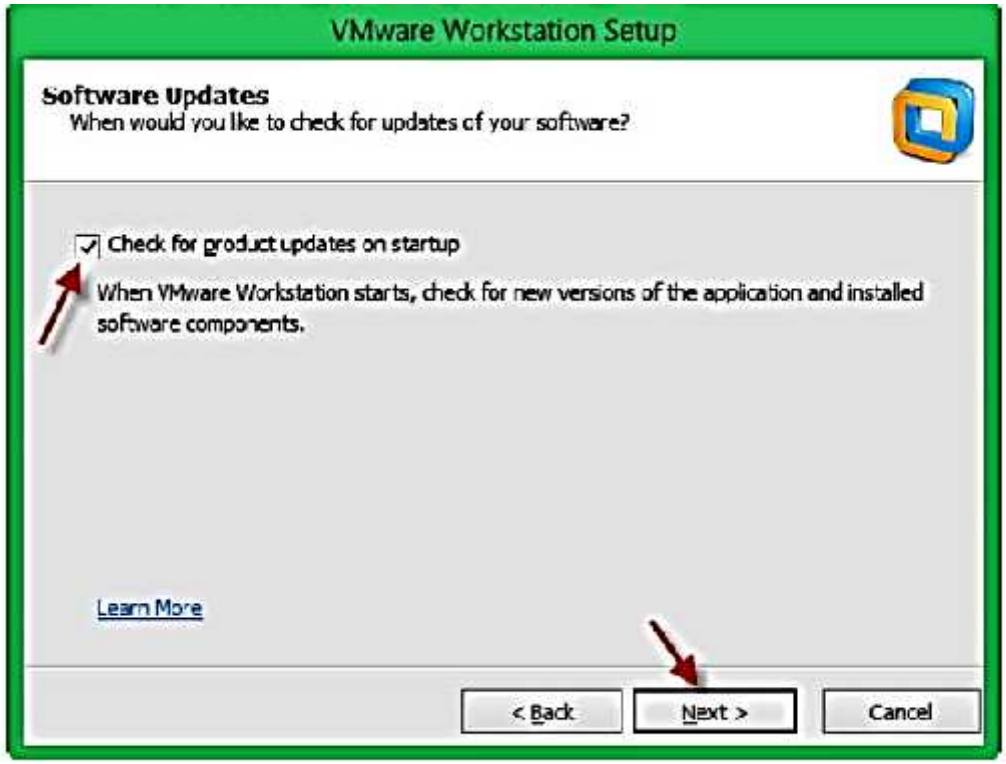


در این قسمت اگر نرم افزاری که در حال نصب آن هستید یک نرم افزار با سریال نامبر خریداری شده باشد تیک گزینه Check for Product Updates on startup را بزنید ماشین مجازی در حال اجرا به دنبال نسخه جدید خود بگردد اگر هم این نسخه کرک شده است این کار لازم نیست ، بر روی Next کلیک کنید.

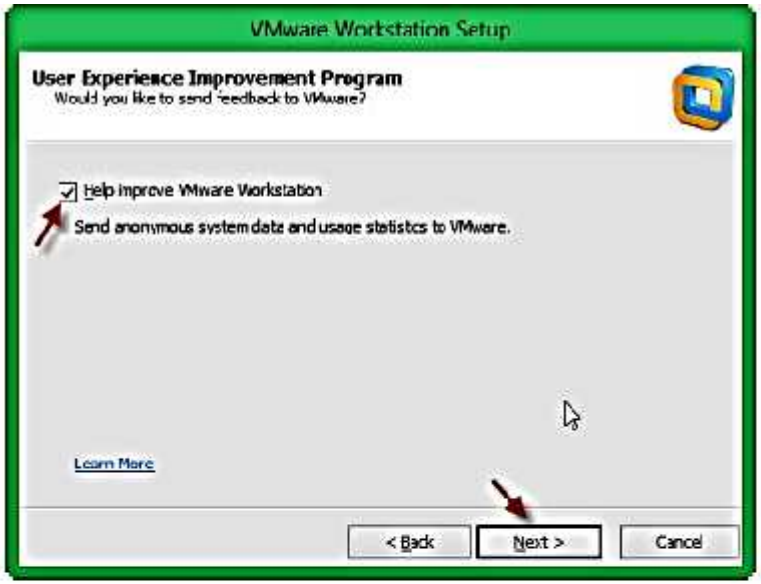


در این قسمت هم مانند قسمت قبلی اگر نرم افزار اصلی و کرک شده نمی باشد بر روی گزینه مورد نظر کلیک کنید تا مشکلات احتمالی این نرم افزار به سایت اصلی آن فرستاده شود.

بر روی Next کلیک کنید.



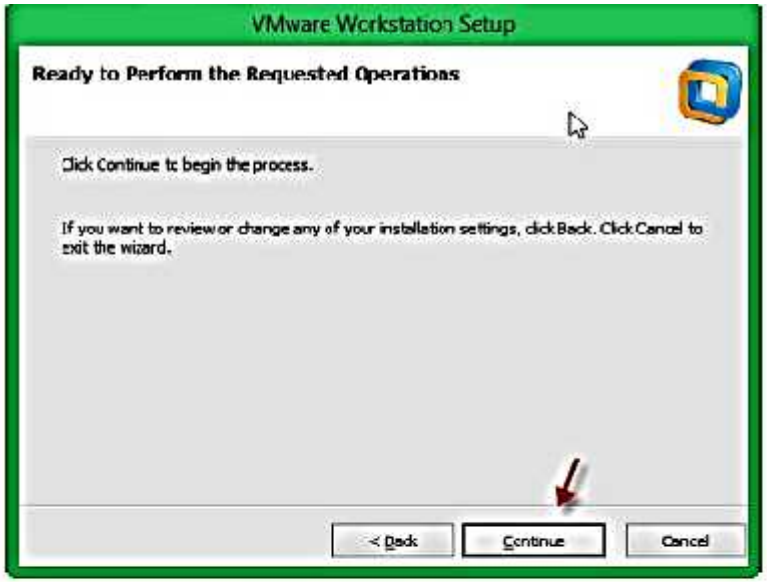
در این قسمت اگر نرم افزاری که در حال نصب آن هستید یک نرم افزار با سریال نامبر خریداری شده باشد تیک گزینه Check for Product Updates on startup را بزنید ماشین مجازی در حال اجرا به دنبال نسخه جدید خود بگردد اگر هم این نسخه کرک شده است این کار لازم نیست ، بر روی Next کلیک کنید.



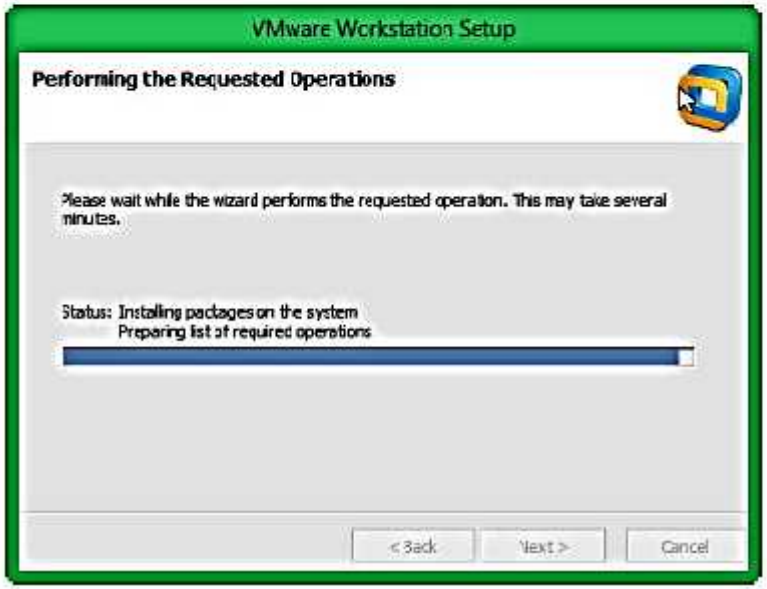
در این قسمت هم مانند قسمت قبلی اگر نرم افزار اصلی و کرک شده نمی باشد بر روی گزینه مورد نظر کلیک کنید تا مشکلات احتمالی این نرم افزار به سایت اصلی آن فرستاده شود.

بر روی Next کلیک کنید.

در این صفحه با انتخاب گزینه های مورد نظر shortcut این نرم افزار در محل های مشخص شده برای اجرا قرار می گیرد ، بر روی Next کلیک کنید.



در این قسمت برای نصب نرم افزار بر روی Continue کلیک کنید.



نرم افزار در حال نصب می باشد....

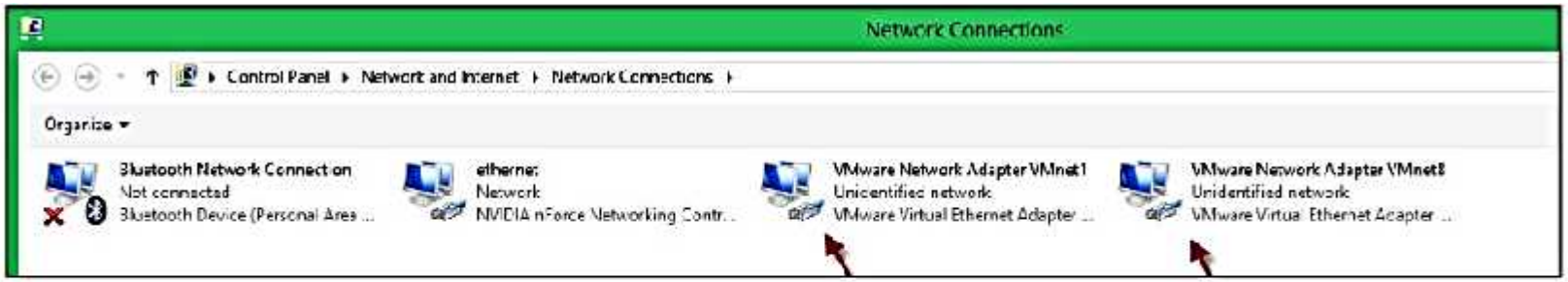
نصب نرم افزار به پایان رسیده و بر روی Finish کلیک کنید.

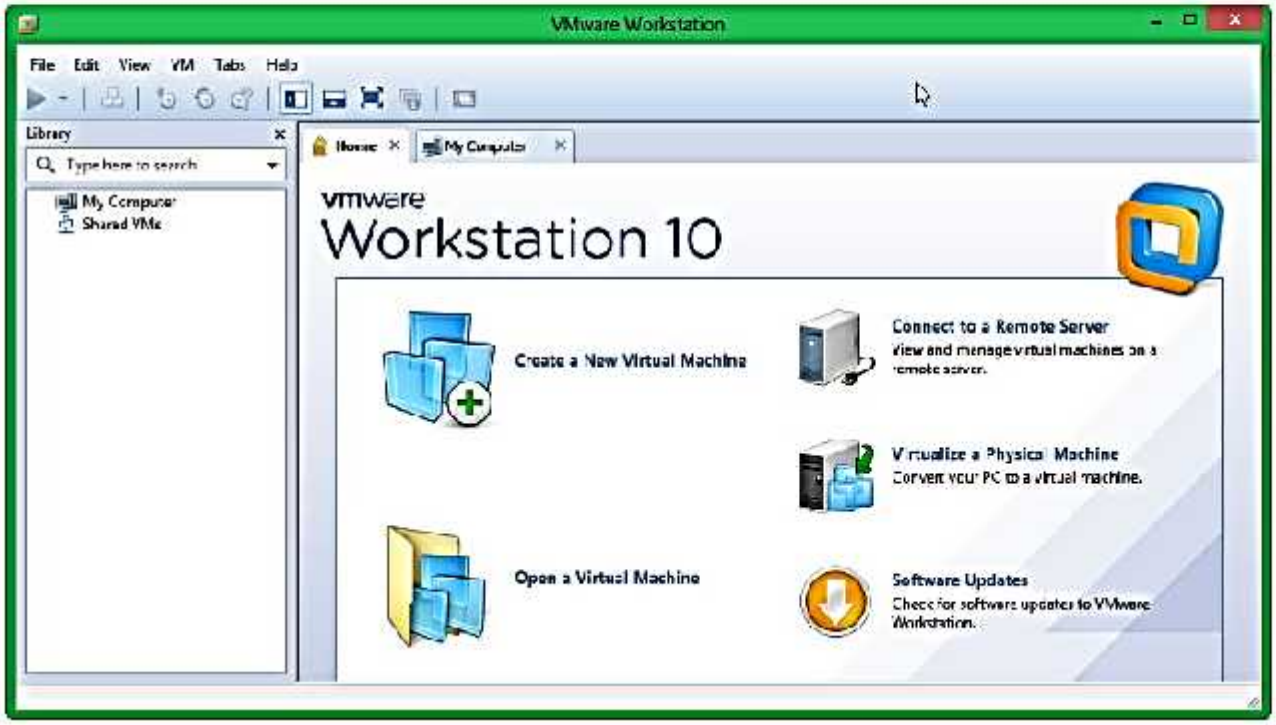
نکته: قبل از این صفحه، صفحه سریال این نرم افزار ظاهر می شود که باید آن را وارد کنید.

برای اجرای نرم افزار VMware در صفحه Desktop بر روی  کلیک کنید تا صفحه زیر ظاهر شود.

در زمان اجرا شدن اگر بر روی سیستم خود نرم افزار آنتی ویروس NOD32 را نصب شده دارید به شما پیام می دهد که کارت شبکه جدید ایجاد شده است با IP مشخص شده در عکس، که از شما سؤال می شود که این کارت شبکه در کجا کار می کند ؟ در شبکه اینترنت و یا در شبکه داخلی که شما گزینه دوم را طبق شکل انتخاب کنید بعد از انتخاب دوباره این صفحه ظاهر می شود برای کارت شبکه دوم، که بر روی گزینه مشخص شده کلیک کنید.

توجه داشته باشید زمانی که VMware نصب می شود دو کارت شبکه مجازی به لیست Network Connection ها اضافه می کند که این موضوع را می توانید از طریق زیر مشاهده کنید:



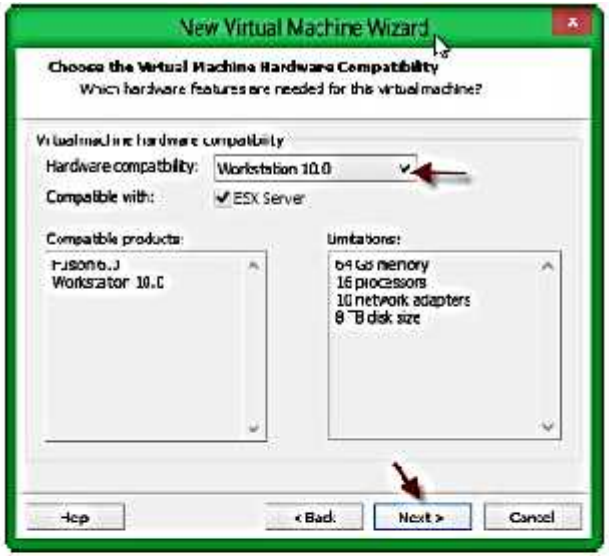


بعد از اجرا شدن نرم افزار صفحه ای مانند شکل مقابل مشاهده می کنید که هر کدام از این بخش ها را به طور مفصل با هم بررسی می کنیم.

بخش اول: Create a New Virtual Machine

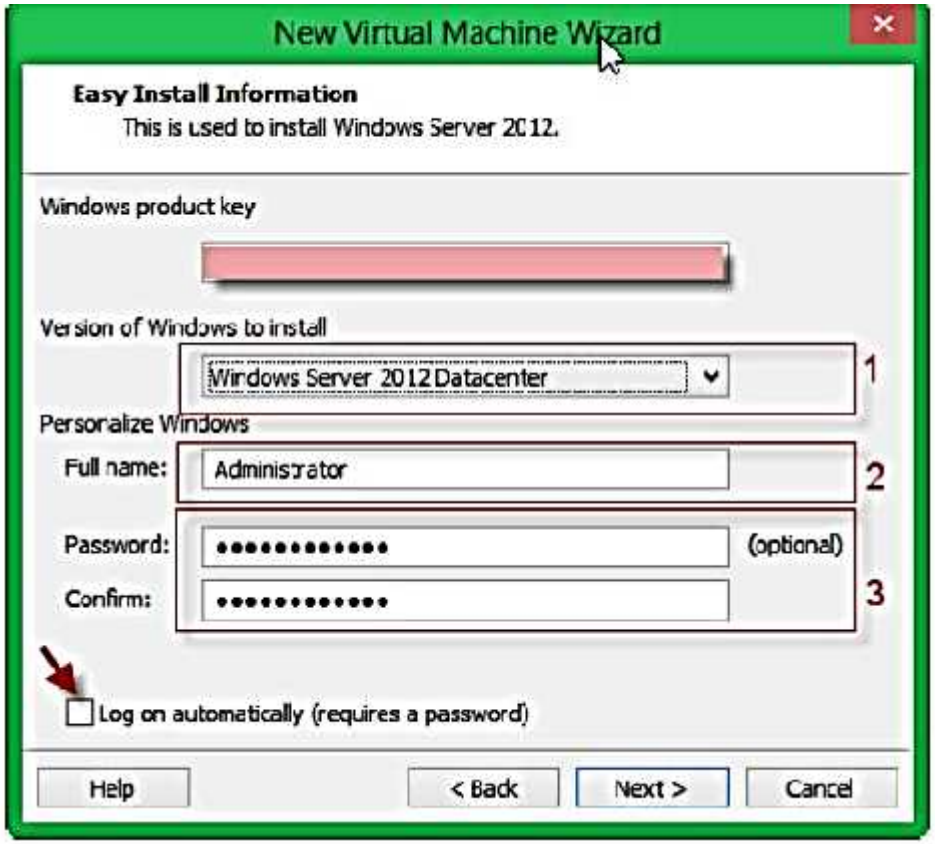
در این بخش می توانیم یک ماشین مجازی با امکانات سخت افزاری و نرم افزاری متفاوت ایجاد کنیم، برای انجام این کار بر روی گزینه مورد نظر کلیک کنید.

در این قسمت دو گزینه موجود است که یکی بصورت تنظیمات سریع و آسان و یکی دیگر به صورت تنظیمات پیشرفته وجود دارد که می‌توانیم نوع هارد دیسک،نحوه ذخیره سازی و ...را مشخص کنیم در این آموزش گزینه دوم را انتخاب می کنیم تا گزینه اول را هم گفته باشیم، بعد از انتخاب گزینه مورد نظر بر روی Next کلیک کنید.



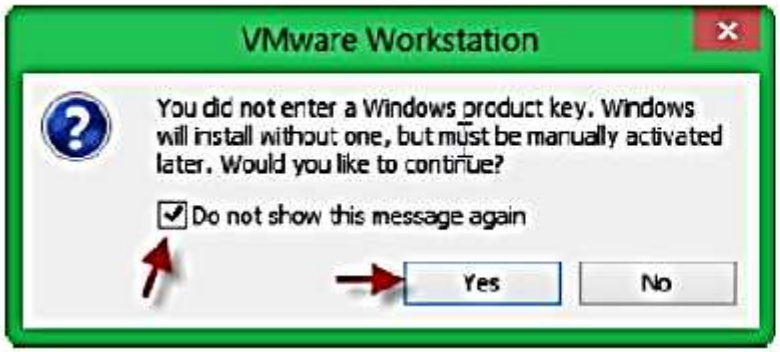
در این قسمت گزینه اول را انتخاب کنید تا تمام نرم فزار های جدید را بتوان روی این ماشین مجازی اجرا کرد، مثلاً ویندوز سرور ۲۰۱۲ را نمی توانید روی VMware 8 اجرا کنید، بعد از انتخاب گزینه اول بر روی Next کلیک کنید.

در این قسمت که شما باید، برای ماشین مجازی مشخص کنید که چه چیزی را باید اجرا کند . اگر قسمت اول را انتخاب کنید سیستم عامل ز طریق DVD/CD خوانده می شود، در قسمت دوم می توانید ز سیستم عامل خود IMAGE تهیه کنید با پسوند ISO باشد و یا با انتخاب گزینه آخر معرفی سیستم عمل را بعداً انجام می دهید. در این قسمت ویندوز سرور ۲۰۱۲ را می خواهیم اجرا کنیم که در قسمت دوم وارد کردیم.

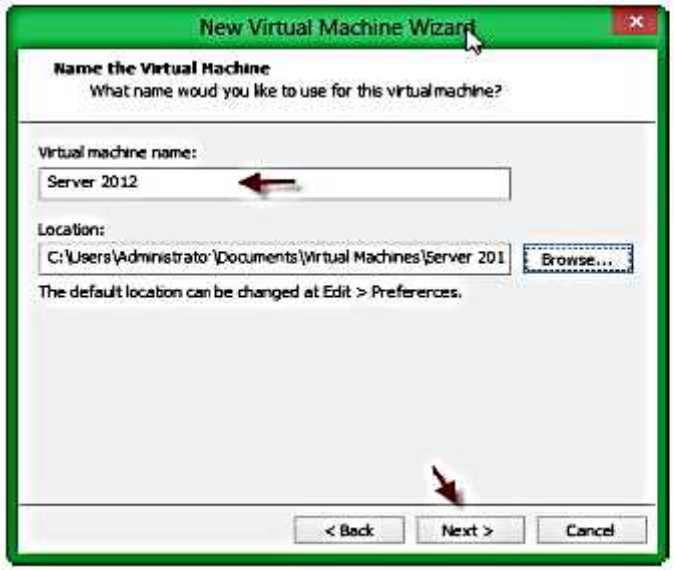


این قسمت که برای راحتی کار شما طراحی شده است می توانید در قسمت Product Key رمز عبور سیستم عامل خود را وارد کنید که شاید ویندوز شما کرک شده باشد و لازم به وارد کردن رمز نداشته باشد، در قسمت های بعدی که با شماره مشخص شده است، در قسمت اول ورژن سیستم عامل خود را

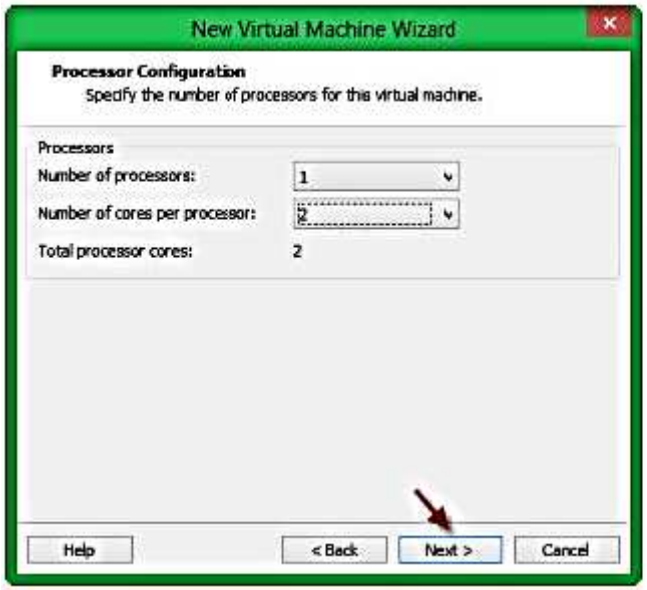
مشخص کنید، حتماً به صورت درست انتخاب کنید که در حال نصب ویندوز با مشکل مواجه نشوید؛ در قسمت های دو و سه نام کاربری و رمز عبور مربوط به سیستم عامل مورد نظر را مشخص کنید تا از شما در زمان نصب سیستم عامل سؤال نشود ، در قسمت آخر اگر تیک گزینه Log On automatically را بزنید به صورت خودکار وارد ویندوز می شود البته توسط نام کاربری و رمز عبوری که در قسمت دو و سه مشخص می کنید. بعد از وارد کردن اطلاعات بر روی Next کلیک کنید.



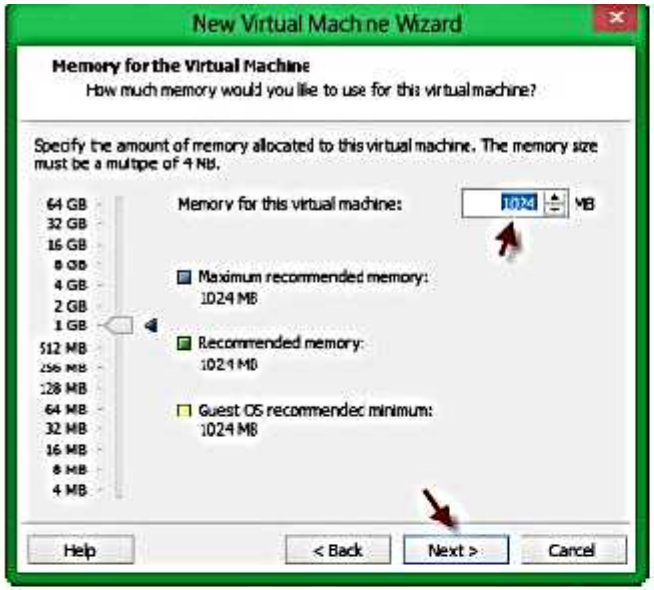
این پنجره زمانی ظاهر می شود که شماره سریال را وارد نکرده باشید و می گوید که باید به صورت دستی ویندوز را فعال کنید.



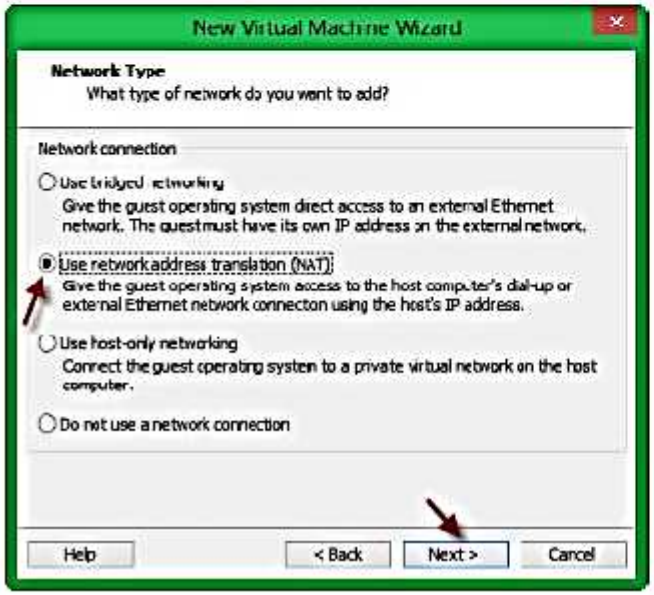
در قسمت اول نام سیستم عامل خود را وارد کنید و در قسمت Location آدرس ذخیره شدن این ماشین را مشخص کنید، در پایان بر روی Next کلیک کنید.



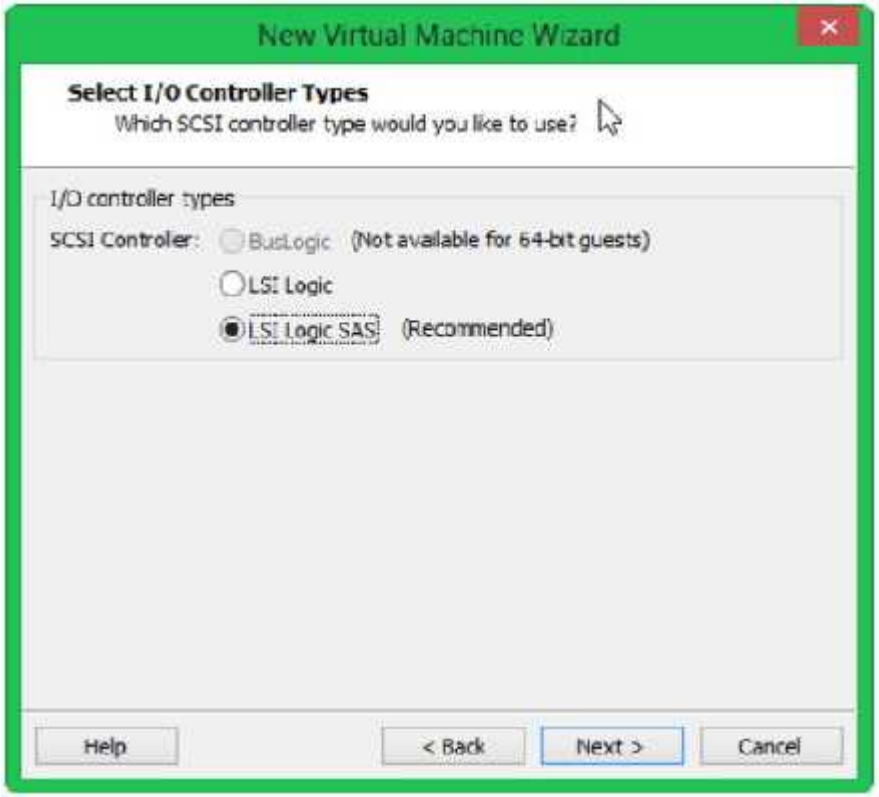
در قسمت Number of Processors تعداد CPU سیستم اصلی خود را مشخص کنید و در قسمت Number of cores per processor تعداد هسته CPU خود را مشخص کنید، اگر بیشتر از حد انتخاب کنید به شما اخطار می دهد.



در این قسمت به اندازه نیاز خود و به اندازه رم سیستم خود می توانید برای این ماشین مجازی حافظه ایجاد کنید، اگر توجه کنید سه مربع زرد، سبز، آبی وجود دارد که می توانید با انتخاب هر کدام از از آنها مقدار حافظه مورد نیاز سیستم را مشخص کنیم ، البته اگر بر روی رنگ سبز کلیک کنید مقدار حافظه متعادل به نسبت سیستم شما برای این ماشین مجازی در نظر می گیرد.



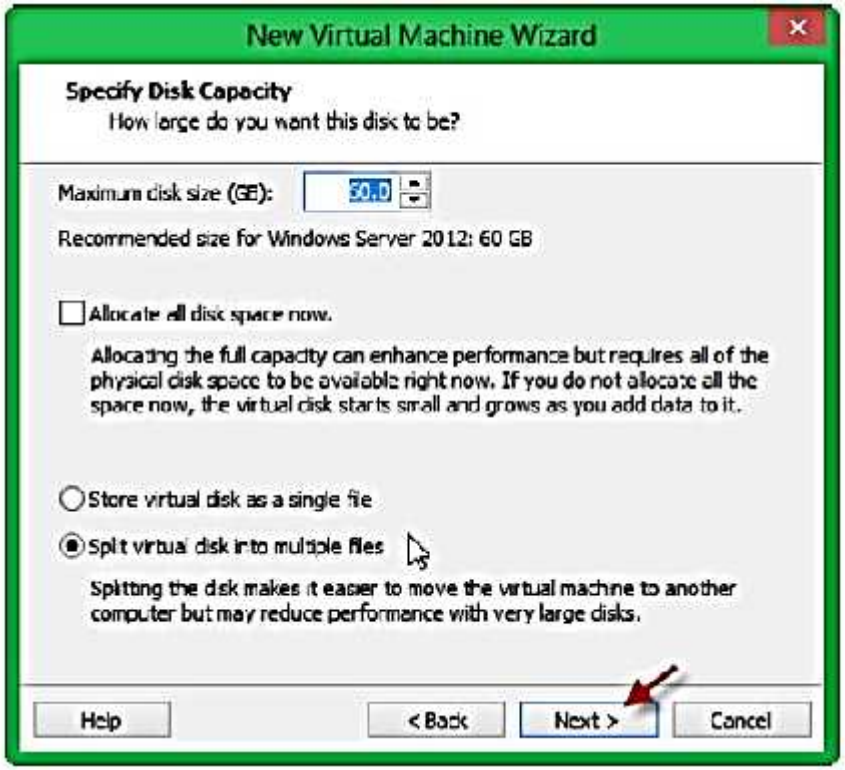
در این قسمت گزینه های مختلف برای ارتباط کارت شبکه با شبکه های مختلف وجود دارد که اگر قسمت اول را انتخاب کنید می توانید با کارت شبکه اصلی سیستم خود در ارتباط باشید، گزینه دوم هم به صورت کارت شبکه مجازی به شبکه متصل می شود، گزینه سوم هم برای ارتباط داخلی شبکه خود سیستم عامل می باشد؛ و با انتخاب گزینه آخر سیستم عامل به شبکه متصل نمی شود، که در اینجا گزینه دوم انتخاب می شود و بر روی next کلیک کنید.



در این قسمت نوع I/O controller را مشخص کنید که زیاد هم مهم نمی باشد. بر روی Next کلیک کنید.

در این قسمت نوع ارتباط هارد دیسک مجازی را انتخاب کنید ، که سعی کنید روی پیش فرض قرار داشته باشد و تغییر ندهید، بر روی Next کلیک کنید.

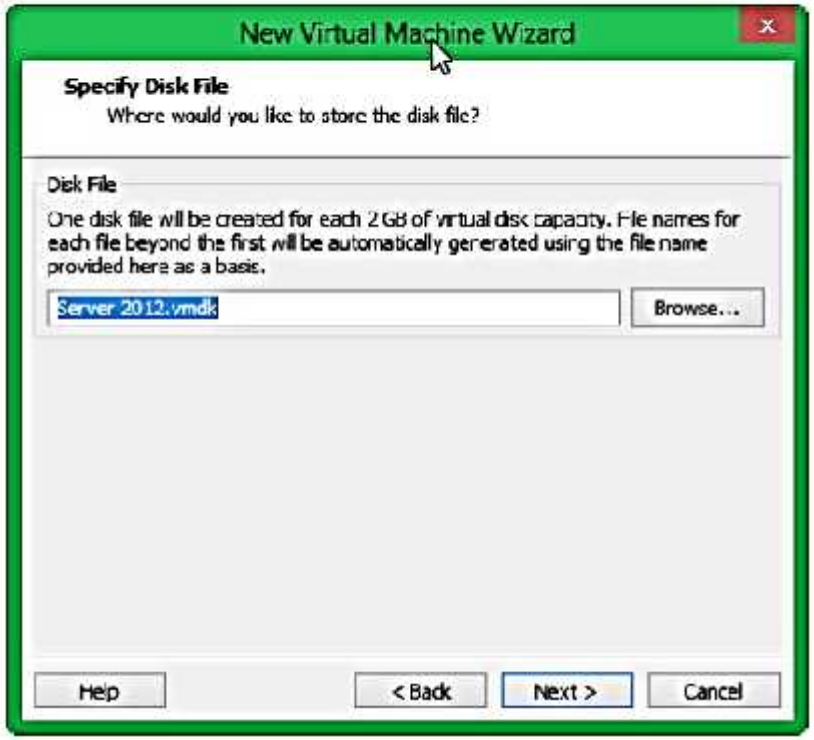
در این قسمت سه گزینه وجود دارد که با انتخاب گزینه اول می توانید هارد دیسک مجازی جدید ایجاد کنید، در قسمت دوم می توانید هارد دیسکی را که قبلاً ایجاد کرده اید به این ماشین معرفی کنید مثلاً شاید شما یک ویندوز را نصب کردید و از طریق این روش می توانید هارد دیسک آن ویندوز را به این ماشین معرفی کنید، گزینه آخر هم استفاده مستقیم از هارد دیسک اصلی سیستم می باشد. گزینه اول را انتخاب و بر روی Next



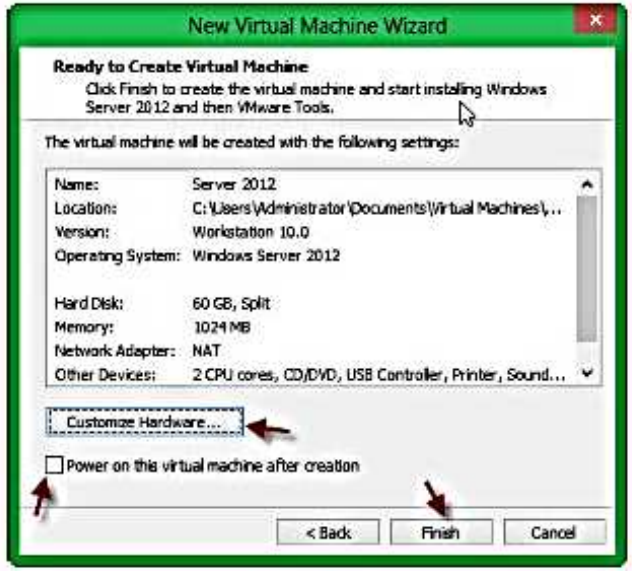
در قسمت Maximum می توانید مقدار اختصاص داده شده به هارد دیسک مجازی را مشخص کنید، اگر تیک گزینه Allocate all disk space now را بزنید یعنی اینکه کل این فضای ۶۰ گیگابایت به این ماشین مجازی اختصاص داده می شود و اشغال می شود که این کار را انجام ندهید، دو گزینه آخر هم برای

در قسمت Maximum می توانید مقدار اختصاص داده شده به هارد دیسک مجازی را مشخص کنید، اگر تیک گزینه Allocate all disk space now را بزنید یعنی اینکه کل این فضای ۶۰ گیگابایت به این ماشین مجازی اختصاص داده می شود و اشغال می شود که این کار را انجام ندهید، دو گزینه آخر هم برای

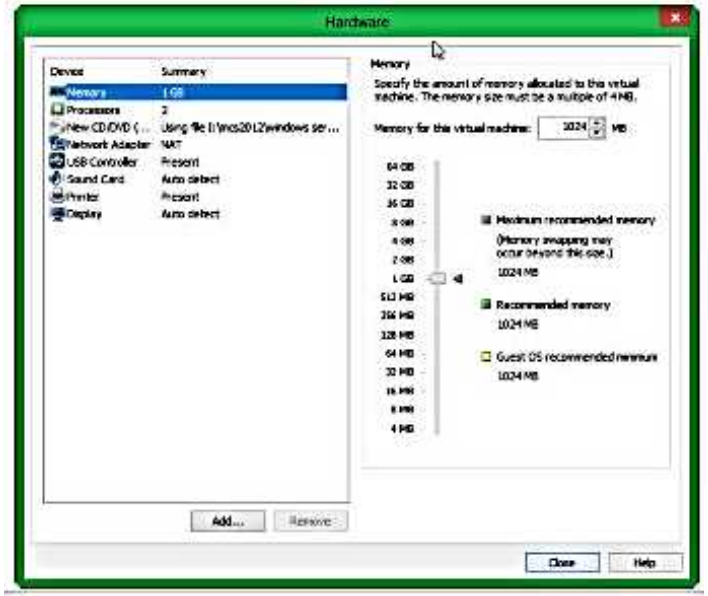
مشخص کردن ذخیره اطلاعات در یک فایل تکی یا چند فایل می باشد که می توانید یکی از آنها را انتخاب کنید . بر روی Next کلیک کنید.



در این قسمت می توانید هارد دیسک مجازی خود را در محل مورد درخواستی خود ذخیره کنید و از این فایل بعد ها استفاده کنید یعنی همان قسمتی که در شکل دوم صفحه قبل گفتم. بر روی Next کلیک کنید.



در این قسمت کل اطلاعات وارد شده را به صورت خلاصه به شما نمایش می دهد ، اگر تیک گزینه Power on This Virtual Machine را بردارید بعد از اینکه بر روی Finish کلیک کنید، سیستم مجازی خود بخود روشن نمی شود ، اگر بر روی Customize Hardware کلیک کنید می توانید سخت افزار این ماشین مجازی را مانند شکل زیر مشاهده کنید.

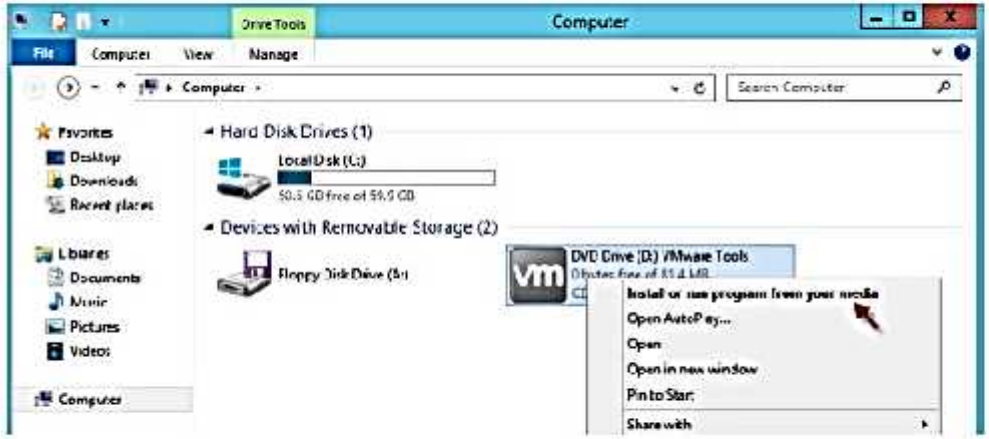


همانطور که مشاهده می کنید ، کل سخت افزار این سیستم را می توانید مشاهده کنید و یا آن ها را می توانید تغییر دهید. بر روی close کلیک و بر روی Finish کلیک کنید تا کار نصب به پایان برسد.

نصب VMware Tools :

یکی از ابزار های جانب و کاربردی در این نرم افزار استفاده از VMware Tools می باشد که با نصب این ابزار، کارت صدا، کارت گرافیک و.... نصب می شوند و باعث عملکرد بهتر ماشین مجازی می شود.

این ابزار زمانی که یک ماشین مجازی ایجاد می کنید به صورت خودکار نصب می شود ، اگر به صورت خودکار انجام نشد وارد منوی VM شوید و گزینه VMware Tools را انتخاب کنید، اگر به صورت خودکار اجرا نشد وارد My Computer سیستم مجازی خود شوید و VMware Tools را اجرا کنید.

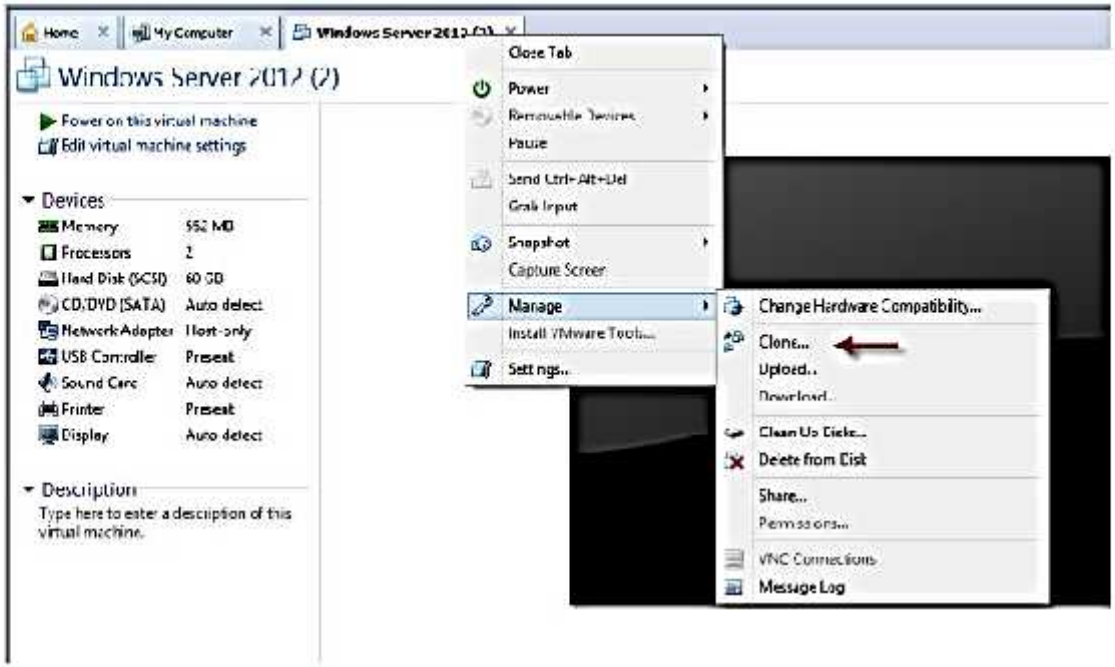


مانند شکل مقابل بر روی VMware Tools کلیک راست کرده و گزینه Install or run... را انتخاب کنید.

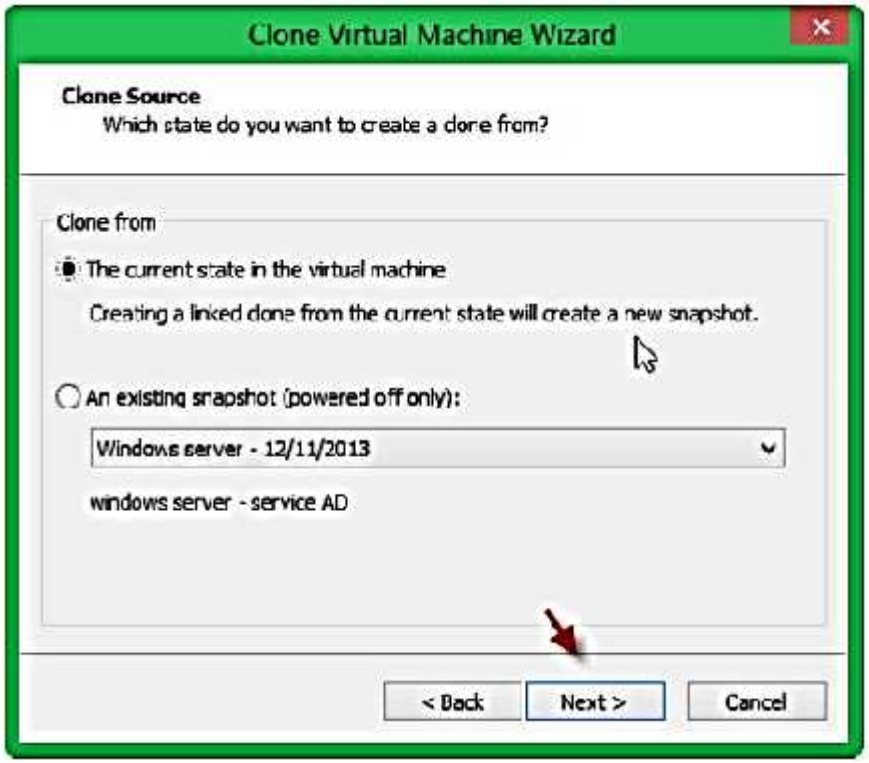
در صفحه باز شده بر روی Next کلیک کنید و این ابزار را بر روی سیستم مجازی خود نصب کنید ، تا بهره دهی ماشین مجازی شما افزایش پیدا کند.

Clone گرفتن از ماشین مجازی:

با این ابزار شما می توانید یک کپی از ماشین مجازی خود تهیه کنید، و از آن استفاده کنید. مثلاً شما یک ویندوز سرور را نصب می کنید که نصب آن کمی زمان می برد، و احتیاج به دو تا سرور دارید برای همین می توانید زمانی که یک ویندوزسرور را نصب کردید از آن یک کپی تهیه کنید و استفاده کنید ، برای انجام این کار باید روی ماشین مجازی کلید راست کنید و از Manage گزینه Clone را مانند شکل زیر انتخاب کنید، البته این کار را هم می توانید از طریق منوی VM و بعد انتخاب Manage و انتخاب Clone انجام دهید.



در صفحه باز شده بر روی Next کلیک کنید.

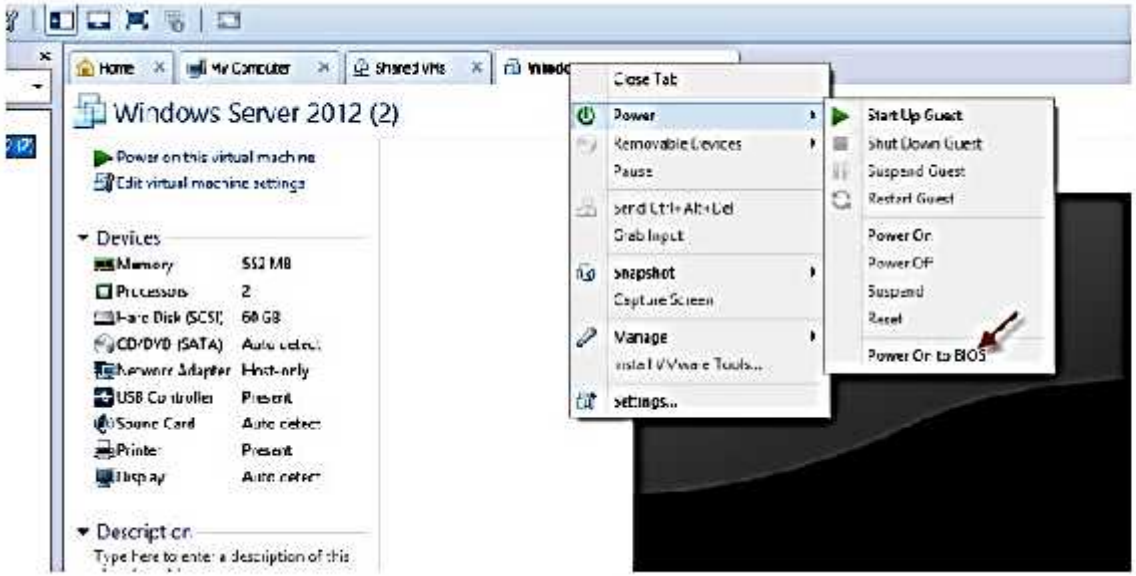


در این قسمت اگر گزینه اول را انتخاب کنید به صورت معمول از ویندوز شما Clone تهیه می کند و اگر گزینه دوم Snapshot را انتخاب کنید، کپی را از Snapshot تهیه شده قبل انجام می دهد ، پس گزینه اول را انتخاب و Next کنید.

در این صفحه دو گزینه وجود دارند، اگر گزینه اول را انتخاب کنید یک **Shortcut** از ماشین مجازی موجود تهیه می کند که زیاد هم جالب نیست چون با ایجاد مشکل در فایل اصلی این **Clone** هم از کار می افتد، اما اگر گزینه دوم را انتخاب کنید می توانید یک کپی کامل از ماشین مجازی ایجاد کنید که ارتباطی با ماشین مجازی اصلی ندارد ، در این قسمت گزینه دوم را انتخاب می-کنیم. بر روی **Next** کلیک کنید.

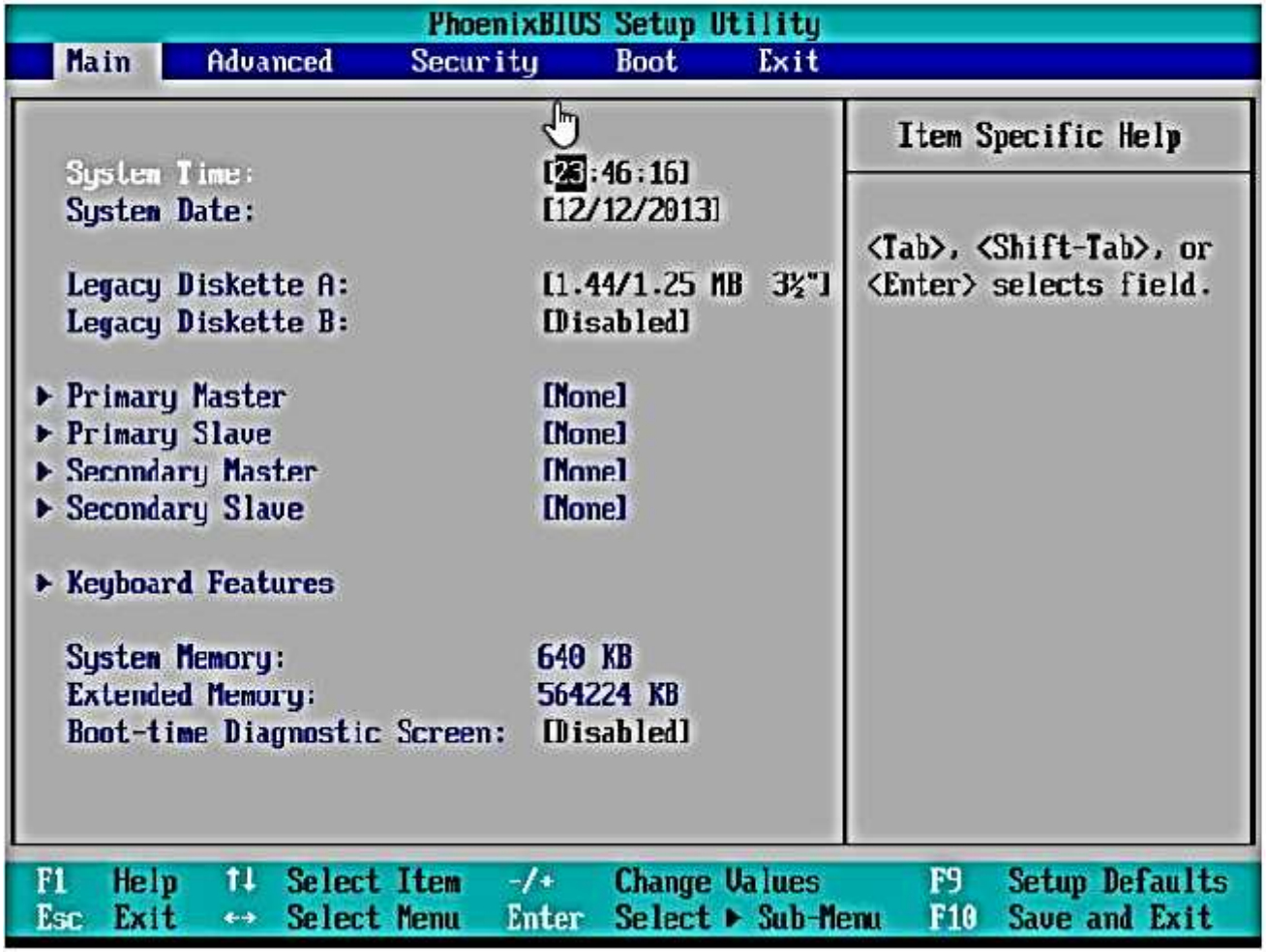
در این قسمت می توانید نام ماشین خود را وارد و مسیر ذخیره سازی آن را انتخاب کنید، با کلیک کردن بر روی دکمه **Finish** کار ایجاد **Clone** آغاز می شود و می-توانید از این **Clone**استفاده کنید.

ورود به Bios ماشین مجازی:



برای اینکه وارد BIOS ماشین مجازی خود شویم، روی سرور مورد نظر کلیک راست کنید و از Power گزینه Power On to BIOS را انتخاب کنید، بعد از آن ماشین مورد

نظر اجرا شده و وارد محیط BIOS مانند شکل زیر می شود:



۲-۵ بررسی ابزارهای Initial Configuration Tasks

همانطور که قبلاً اشاره شد، بعد از نصب کامل ویندوز سرور و ورود به سیستم، پنجره‌ای تحت عنوان "Initial Configuration Tasks" نمایش داده خواهد شد. ابزارهای موجود در این پنجره، به شما امکان می‌دهند تا به سرعت بتوانید اقداماتی را جهت پیکربندی سرور انجام دهید. این ابزارها عبارتند از:

- **Active Windows**: هر نسخه از ویندوز، پس از نصب نیازمند فعال‌سازی[1] می‌باشد. تا زمانی که ویندوز را فعال نکرده باشید، استفاده از تمام عملکردهای آن امکان‌پذیر نمی‌باشد (فعال‌سازی از طریق اینترنت، کد License و برنامه Genuine Microsoft امکان‌پذیر است).
- **Set time zone**: در این قسمت می‌توانید منطقه زمانی و تاریخ سرور را تنظیم کنید.
- **Configure networking**: به کمک این ابزار می‌توانید تنظیمات مربوطه جهت اتصال سرور به شبکه را انجام دهید.

- **Provide Computer Name and Domain**: این قسمت مربوط به انتخاب نام برای کامپیوترها و ایجاد Domain جهت اتصال کاربران شبکه به سرور می‌باشد.
- **Enable automatic updating and feedback**: در این قسمت می‌توانید امکان دریافت خودکار آپدیت‌های مهم و امنیتی مایکروسافت از طریق اینترنت را فعال کنید. البته این امکان به صورت دستی و یا به کمک Group Policy نیز امکان‌پذیر است.
- **Download and install updates**: به کمک این قسمت می توانید آپدیت‌ها را دریافت نموده و آنها را برروی سرور نصب کنید.
- **Add roles**: امکان اضافه کردن سرویس‌ها و قابلیت‌های بیشتر به سرور را فراهم می‌نماید.
- **Add features**: این ابزار نیز جهت افزودن قابلیت‌ها به سرور استفاده می‌شود.
- **Enable Remote Desktop**: به کمک این ابزار قادر خواهید بود سرور خود را با استفاده از نرم افزار Remote Desktop کنترل کنید، البته به شرطی که سرور به شبکه متصل باشد.

---

1. Activation

- **Configure Windows Firewall**: فایروال اجازه دسترسی به سرویس‌های شبکه را از راه دور فراهم می‌کند و بطور پیش‌فرض بر روی ویندوز سرور فعال است. پیکربندی فایروال به صورت دستی و یا از طریق Active Directory Group Policy نیز امکان‌پذیر است.

۲-۶ پیکربندی سرور به کمک Server Manager

مایکروسافت همواره در تلاش بوده است که برای راحتی مدیران، ابزارهای گرافیکی زیادی را جهت پیکربندی سرور در اختیار آنها قرار دهد. یکی از این ابزارها که اخیراً نیز با آن آشنا شدید، پنجره Initial Configuration Tasks است که فقط جهت پیکربندی مقدماتی سرور قابل استفاده می‌باشد. ابزار دیگر، Server Manager است که بر خلاف قبلی، امکانات بسیاری را جهت مدیریت و پیکربندی سرور فراهم می‌نماید. در شکل ۲-۲۲، تصویر این ابزار نشان داده شده است.


Server Manager
File Action View Help
Server Manager (WIN-943UKRNR7
Roles
Features
Diagnostics
Configuration
Storage
Server Manager (WIN-943UKRNR7TT)
Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.
Server Summary
Server Summary Help
Computer Information
Full Computer Name: WIN-943UKRNR7TT
Workgroup: WORKGROUP
Remote Desktop: Disabled
Server Manager Remote Management: Disabled
Product ID: 00477-OEM-6400101-10502 (Activated)
Change System Properties
View Network Connections
Configure Remote Desktop
Configure Server Manager Remote Management
Do not show me this console at logon
Security Information
Go to Windows Firewall
Last Refresh: Today at 4:03 PM Configure refresh

کنسول (پنجره) Server Manager، از روش‌های مختلفی قابل دسترسی می‌باشد:

- از مسیر Server Manager «Administrative Tools «Start
- از مسیر Program and Features «Control Panel «Start
- نوشتن دستور `ServerManager.exe` در خط فرمان (Cmd)

۲-۶-۱ اقدامات پیکربندی متداول

زمانی که یک سرور جدید را راه اندازی می‌کنید، به انجام تعدادی اقدام رایج جهت قرار دادن آن در شبکه نیازمند هستید. در ادامه این اقدامات را مورد بررسی قرار می‌دهیم.

تغییر تنظیمات شبکه

اولین اقدام جهت اتصال سرور به شبکه‌هایی که از IPv4 استفاده می‌کنند، انجام تنظیمات مربوط به آدرس IPv4 برروی سرور می‌باشد. این کار باعث می‌شود تا سایر دستگاه‌های موجود در شبکه بتوانند با سرور ارتباط برقرار کنند. جهت انجام این تنظیمات مراحل زیر را دنبال کنید:

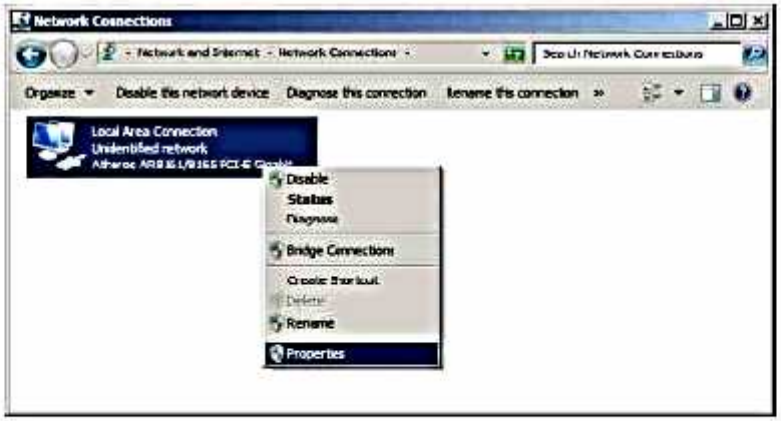
۱. کنسول Server Manager را باز نموده و از پنل سمت چپ، برروی Server Manager کلیک کنید.
۲. در قسمت Server Summary، برروی گزینه View Network Connections (که به صورت لینک آبی رنگ است) کلیک کنید.

شکل ۲-۲۲

۳. پنجره‌ای تحت عنوان "Network Connection" نشان داده خواهد شد. (البته این پنجره از طریق Control Panel و یا نوشتن دستور `ncpa.cpl` در Cmd نیز قابل دسترسی می‌باشد)

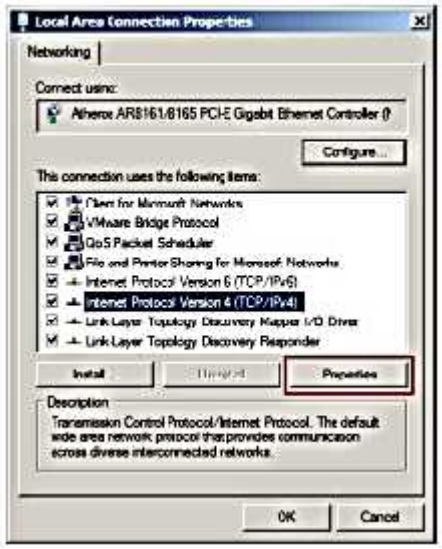
در این پنجره، به ازای هر کارت شبکه (NIC)[1] که برروی سرور قرار دارد، یک کانکشن[2] مشاهده می‌کنید. جهت اتصال به شبکه، باید کانکشنی را انتخاب کنید که قصد دارید از طریق آن به شبکه متصل شوید (ممکن است از کارت شبکه جهت اتصال به اینترنت نیز استفاده شود). در اینجا سرور ما ساده است و تنها دارای یک کارت شبکه می‌باشد. برروی کانکشن Local Area Connection کلیک راست نموده و Properties را انتخاب کنید.

1. Network Interface Card
2. Connection



شکل ۲-۲۳

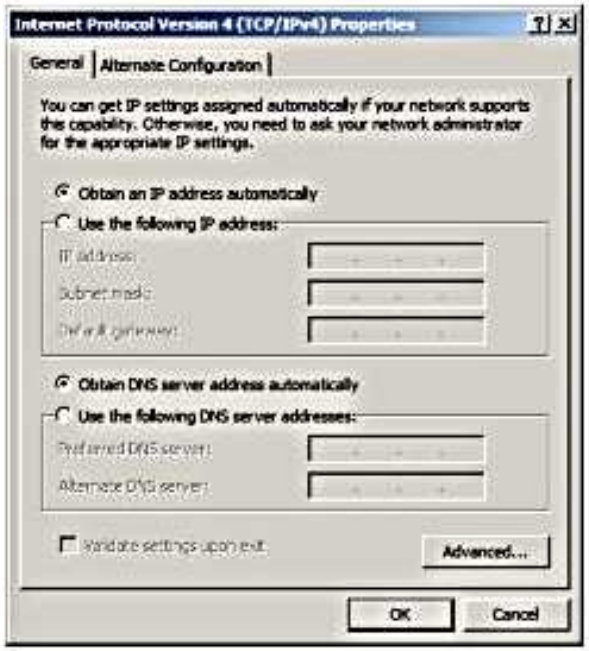
٤. در پنجره "Local Area Connection Properties" گزینه Internet Protocol Version 4 (TCP/IPv4) را انتخاب و برروی Properties کلیک کنید.



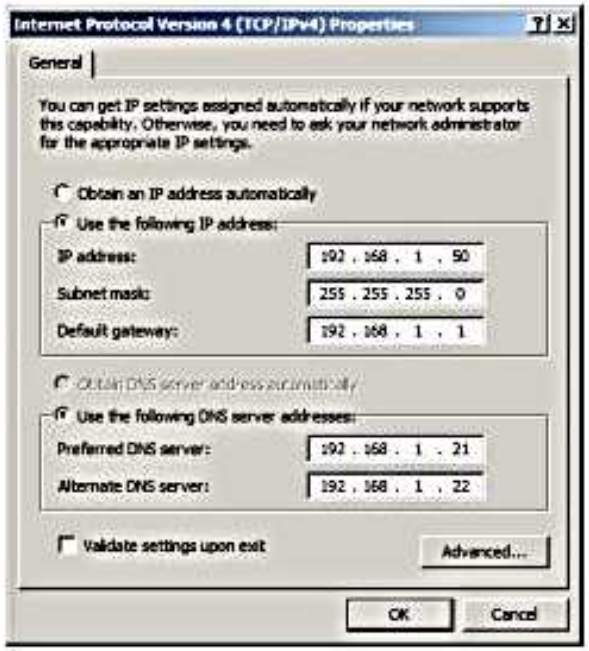
۵. در ویندوز سرور 2008R2، TCP/IP بطور پیش‌فرض پیکربندی نشده است و کارت شبکه آدرس IP خود را بطور خوکار از سرویس DHCP دریافت می‌کند (شکل ۲-۲۵). در اینجا قصد داریم، پیکربندی TCP/IP را بطور دستی انجام دهیم. بنابراین از تب General گزینه "Use the following IP address" را انتخاب کنید (شکل ۲-۲۶). پس از انتخاب گزینه ذکر شده، مکان‌هایی جهت وارد نمودن آدرس IP، قاب زیرشبکه[3]، آدرس دروازه[4]، و آدرس سرورDNS فعال می‌گردد. در این

1. Network Interface Card
2. Connection
3. Subnet mask
4. Default Gateway

مکان‌ها آدرس‌های مورد نظر را (با توجه به نظر مدیر شبکه) وارد نموده و برروی Ok کلیک کنید.



شکل ۲-۲۵



شکل ۲-۲۶

تغییر تنظیمات شبکه در خط فرمان

کلیه تنظیماتی که در بالا انجام شد، با استفاده از دستور netsh در خط فرمان نیز امکان‌پذیر است. برای این کار، ابتدا نیاز به نام کارت شبکه دارید. به این منظور می‌توانید با نوشتن دستور ipconfig در Cmd نام آنرا بدست آورید. جهت اختصاص آدرس IP به کارت شبکه، دستور زیر را در Cmd تایپ کنید:

```
netsh interface ip set address name="Local Area Connection" static
192.168.1.50 255.255.255.0 192.168.1.1
```

بطور کلی، قالب دستور netsh به صورت زیر می‌باشد:

```
netsh interface ip set address name="<Connection Name>" static <IP
Address> <Subnet Mansk> <Default Gateway>
```

جهت انجام تنظیمات DNS، دستور زیر را تایپ کنید:

```
netsh interface ip set dns "Local Area Connection" static
192.168.1.21
```

قالب کلی این دستور به صورت زیر می‌باشد:

```
netsh interface ip set dns "<Connection Name>" static <DNS Server IP
Address>
```

در صورتی که در شبکه، از یک سرور DNS ثانویه نیز استفاده می‌کنید، می‌توانید با دستور زیر، آدرس آنرا وارد کنید. این دستور با دستور قبلی کمی متفاوت است:

```
netsh interface ip add dns "Local Area Connection" 192.168.1.22
```

پس از اجرای این دستورات، تنظیمات مورد نظر باید برروی سرور شما اعمال شده باشند. جهت اطمینان از این موضوع، می‌توانید دستور ipconfig را در Cmd تایپ کنید. پس از تایپ کردن این دستور و فشردن کلید Enter بر روی صفحه کلید، نتیجه عملیات چیزی شبیه به زیر خواهد بود:

```
C:\>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

 Connection-specific DNS Suffix  . :
 Link-local IPv6 Address . . . . . : fe80::5819:d35b:1b24:de7f%10
 IPv4 Address. . . . . . . . . . . : 192.168.1.50
 Subnet Mask . . . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter Local Area Connection* 3:

 Media State . . . . . . . . . . . : Media disconnected
 Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 4:

 Connection-specific DNS Suffix  . :
 IPv6 Address. . . . . . . . . . . : 2001:0:4137:9e50:1817:3f21:3f57:fc97
Link-local IPv6 Address. . . . . . : fe80::1817:3f21:3f57:fc97%12
 Default Gateway . . . . . . . . . : ::
```

دستورات بالا، پیکربندی IPv4 را بر روی کارت شبکه‌ای به نام Local Area Connection نشان می‌دهند. در صورت نیاز به کسب اطلاعات بیشتر در مورد این پیکربندی، می‌توانید دستور ipconfig /all را تایپ کنید.

پس از پیکربندی IPv4 بر روی کارت شبکه، مرحله بعد، تست ارتباط با شبکه می‌باشد. این کار با استفاده از دستور ping در محیط Cmd امکان‌پذیر است. این دستور، با فرستادن بسته‌های تست به یکی از ماشین‌های متصل به شبکه، ارتباط ماشین فعلی با آنرا بررسی می‌کند. در مثال زیر، برقراری ارتباط با ماشینی که دارای آدرس 192.168.1.2 می‌باشد، بررسی شده است:

```
C:\Windows\system32>Ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
```

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

در این مثال، چهار بسته ارسال می‌شود و متناسباً چهار بسته باید دریافت شود. در صورتی که به ازای هر کدام از بسته‌های ارسالی، پاسخی دریافت نشود، ارتباط با مشکل مواجه شده است. این مشکل می‌تواند مربوط به پیکربندی شبکه، کارت شبکه، کابل یا سایر سخت افزارهای شبکه باشد.

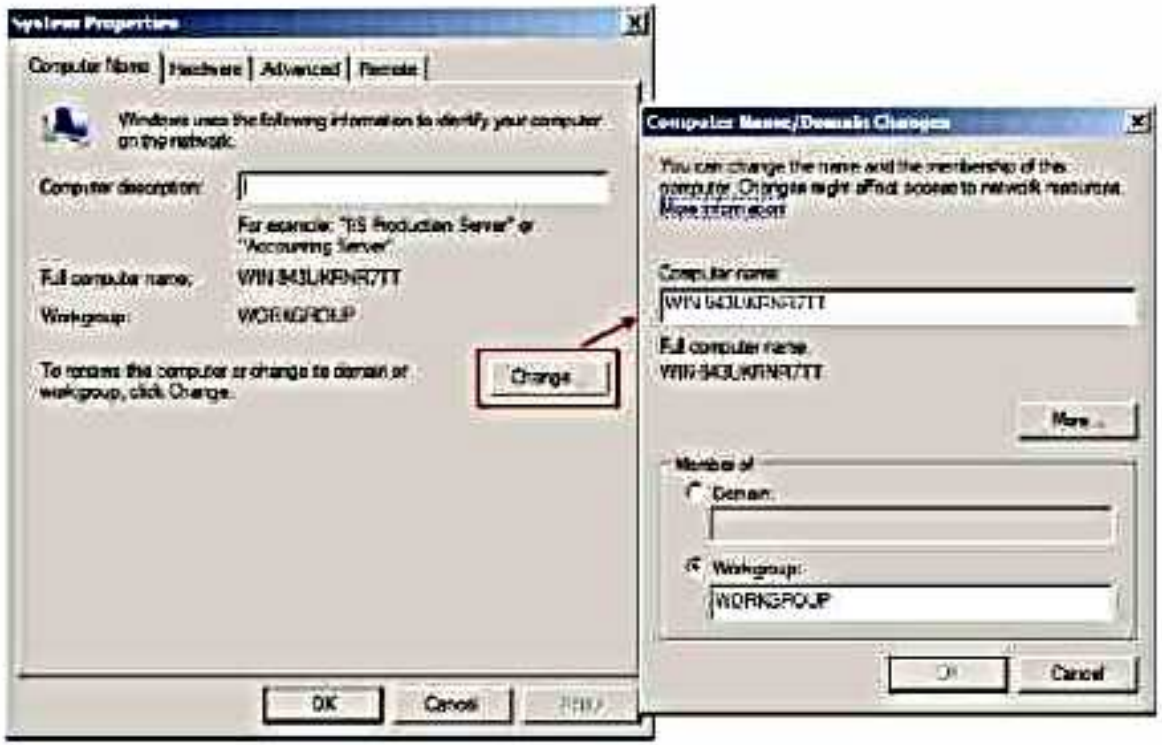
منظور از دروازه یا Gateway، وسیله‌ای است که امکان ارتباط یک شبکه را با خارج از آن فراهم می‌سازد. به عنوان مثال Router و Modem هر کدام می‌توانند به عنوان Gateway در نظر گرفته شوند.

تغییر نام سرور

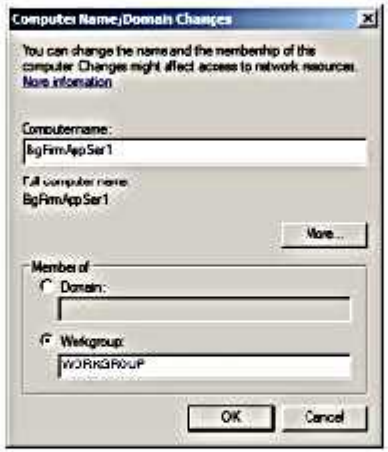
هر کامپیوتر در شبکه، باید دارای یک نام منحصر بفرد باشد تا بتواند توسط سایر کامپیوترها شناسایی شود. در بسیاری از موارد انتخاب این نام اختیاری است و کاربران می‌توانند با توجه به نظر خود آنرا انتخاب کنند، اما در مواردی استانداردهای سازمان تعیین‌کننده این نام می‌باشد (نام انتخابی می‌تواند ترکیبی از حروف و ارقام باشد). جهت انتخاب نام و یا تغییر نام سرور، مراحل زیر را دنبال کنید:

۱. کنسول Server Manager را باز نموده و از قسمت Server Summary، گزینه Change Computer Setting را انتخاب کنید (این گزینه از مسیر «Computer» «Properties» Change setting نیز قابل دسترسی می‌باشد).

۲. در پنجره "System Properties"، از تب Computer Name، برروی دکمه Change کلیک کنید تا پنجره Computer Name/Domain Changes نشان داده شود.

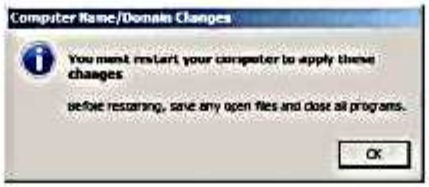


۳. زمانی که ویندوز را بطور کامل نصب می‌کنید، یک نام تصادفی به سرور داده اختصاص داده می‌شود. این نام کمی پیچیده است و جهت پیگیری سرور در شبکه مناسب نمی‌باشد، بنابراین بهتر است آنرا تغییر دهید. برای انجام این کار، نام مورد نظر را در قسمت Computer name وارد نموده و بر روی OK کلیک کنید. توجه داشته باشید که نام انتخابی، قبلاً برروی کامپیوتر دیگری تنظیم نشده باشد، زیرا در این صورت با مشکلاتی مواجه خواهید شد.



شکل ۲-۲۸

٤. پیغامی ظاهر شده و اعلام می‌کند که جهت اِعمال تغییر نام باید کامپیوتر را Restart کنید. برروی OK کلیک کنید. پس از راه اندازی سرور، نامی که انتخاب نموده‌اید بر روی آن اعمال می‌گردد.



٤. پیغامی ظاهر شده و اعلام می‌کند که جهت اِعمال تغییر نام باید کامپیوتر را Restart کنید. بـرروی OK کلیک کنید. پس از راه اندازی سرور، نامی که انتخاب نموده‌اید بر روی آن اعمال می‌گردد.

شکل ۲-۲۹

تغییر نام سرور در خط فرمان

کلیه مراحل تغییر نام، با نوشتن دستور netdom در خط فرمان نیز امکان‌پذیر است:

```
C:\Windows\system32>netdom /renamecomputer WIN-943UKRNR7TT
/newname:BIGFIRMAPPSER1
This operation will rename the computer WIN-943UKRNR7TT
to BIGFIRMAPPSER1.
Certain services, such as the Certificate Authority, rely on a fixed machine
name. If any services of this type are running on WIN-DCL9MRNLVOH,
then a computer name change would have an adverse impact.

Do you want to proceed (Y or N)?
Y
```

```
The computer needs to be restarted in order to complete the operation.

The command completed successfully.
```

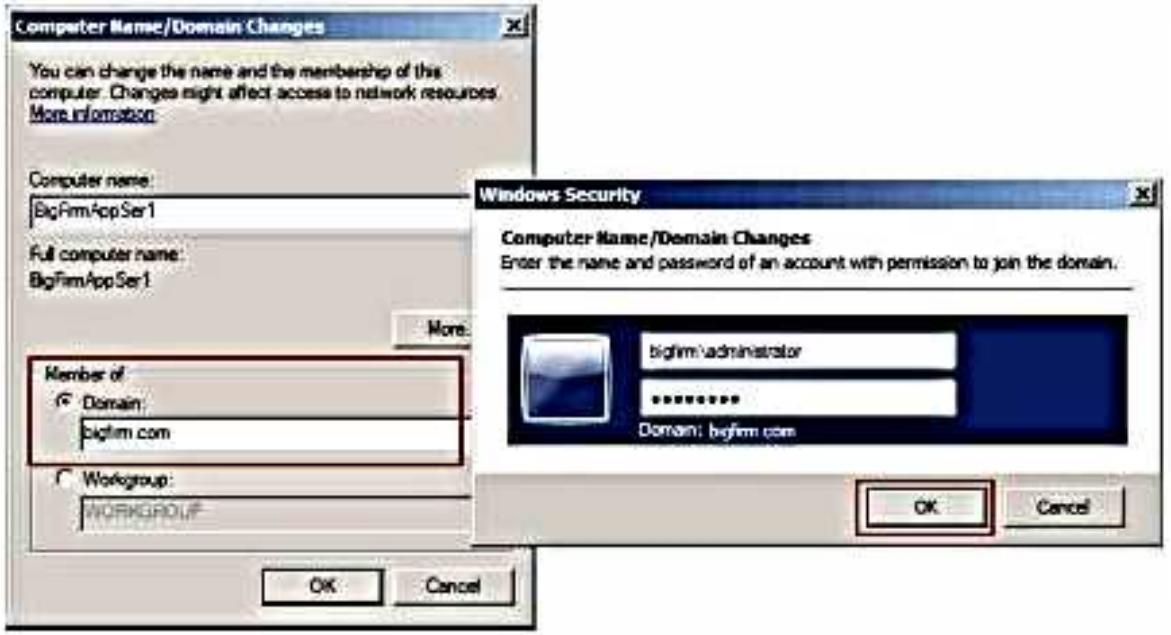
قالب کلی این دستور، به صورت زیر می‌باشد:

```
netdom /renamecomputer <Current Computer Name> /newname:<New Name>
```

پس از اجرای دستور netdom، باید سرور را به صورت دستی Restart کنید. پس از راه‌اندازی، می‌توانید از قسمت Server Summary در Server Manager، نام جدید سرور را مشاهده کنید.

اتصال سرور به یک دامنه[1]

قبل از اینکه بتوانیم منابع موجود در سرور را با سایر اعضاء شبکه به اشتراک گذاریم، نیازمند اتصال آن به یک دامنه هستیم. در اینجا قصد داریم سرور را به دامنه‌ای با نام bigfirm.com متصل کنیم. جهت انجام این کار، در قسمت Member of از پنجره Computer Name گزینه Domain را انتخاب کنید. سپس نام دامنه را وارد نموده و بر روی OK کلیک کنید. پس از کلیک، از شما نام کاربری و رمز عبور یک حساب کاربری که اجازه افزودن سرور به دامنه را دارد، درخواست می‌شود. این کاربر ممکن است مدیر سرور (نام کاربری: bigfirm\administrator) و یا فردی باشد که در اکتیو دایرکتوری[2] این مجوز به او داده شده باشد (به عنوان مثال bigfirm\user1). پس از وارد نمودن موارد درخواست شده تمام پنجره‌ها را ببندید و کامپیوتر را Restart کنید. پس از راه‌اندازی، این سرور از امکانات Group Policy، کاربران Active Directory، مدیریت مرکزی و ... برخوردار می‌گردد.



شکل ۲-۳۰

1. Domain
2. Active Directory

اتصال سرور به دامنه در خط فرمان

اتصال سرور به دامنه، از طریق دستورات خط فرمان نیز امکان پذیر است. به عنوان مثال با دستور زیر کامپیوتری به نام bigfirmappsvr1 به دامنه bigfirm.com متصل می‌شود:

```
C:\>netdom join bigfirmappsvr1 /Domain:bigfirm.com
/UserD:bigfirm\administrator /PasswordD:*

Type the password associated with the domain user:********
The computer needs to be restarted in order to complete the operation:
The command completed successfully.
```

قالب کلی این دستور به صورت زیر است:

```
netdom join <Current Computer Name> /Domain:<Domain Name>
/UserD:<User Name> /PasswordD:*
```

پس از اجرای دستور، به شما اعلام می‌شود که باید سرور را Restart کنید. البته می‌توانید این کار را با اضافه نمودن پارامتر /reboot به انتهای دستور بالا، به صورت خودکار انجام دهید. به دستور زیر توجه کنید:

```
C:\>netdom join bigfirmappsvr1 /Domain:bigfirm.com /UserD
:bigfirm\administrator /PasswordD:* /REBoot
```

فعال‌سازی Remote Desktop برروی سرور

بسیاری از مدیران ویندوز تمایل دارند که سرور را از راه دور و از طریق کامپیوترهای شخصی خود کنترل کنند. این کار با فعال کردن سرویس Remote Desktop برروی سرور امکان‌پذیر است. پس از فعال‌سازی این سرویس، می‌توانید به کمک ابزار Remote Desktop که برروی کامپیوتر و یا لپ‌تاپ شما قرار دارد و همچنین از طریق یک اتصال TCP با پورت ۳۳۸۹ یا به عبارت دیگر از طریق "پروتکل مدیریت از راه دور دسکتاپ[1]" (RDP)، سرور را مدیریت کنید. این پروتکل باید توسط مدیر سرور فعال گردد.

جهت فعال‌سازی، مراحل زیر را دنبال کنید:

۱. در کنسول Server Manager و از قسمت Server Summary، برروی گزینه Configure Remote Desktop کلیک کنید.
۲. در پنجره System Properties، تب Remote را انتخاب نمایید.
۳. در قسمت Remote Desktop، سه گزینه جهت فعال‌سازی/غیر فعال کردن Remote Desktop وجود

---

1. Remote Desktop Protocol

دارد. این گزینه‌ها عبارتند از:

- **Do not allow connections to this computer**: این گزینه که به صورت پیش‌فرض نیز انتخاب شده است، استفاده از Remote Desktop را در حالت غیرفعال قرار می‌دهد.
- **Allow connections from computers running any version ...**: این گزینه، به نسخه‌هایی از برنامه Remote Desktop که پایین‌تر از نسخه ٦ در ویندوز سرور 2008R2 هستند اجازه می‌دهد تا به سرور متصل شوند. نسخه ٦، در ویندوز ویستا و بعد از آن به کار گرفته شده است و شامل قابلیت‌های امنیتی جدید می‌باشد. کاربرانی که از نسخه‌های پایین‌تر این برنامه در ویندوزهای XP و سرور 2003 استفاده می‌کنند، می‌توانند از طریق سایت مایکروسافت (به صورت رایگان) نسخه جدید این برنامه را دریافت کنند.
- **Allow connections only from computers running Remote Desktop with ...**: پیشنهاد مایکروسافت این است که جهت دسترسی به RDP، از این گزینه استفاده کنید. توجه داشته باشید که در این گزینه باید بر روی همه کامپیوترهای مورد نظر حداقل نسخه ٦ از برنامه Remote Desktop را داشته باشید.

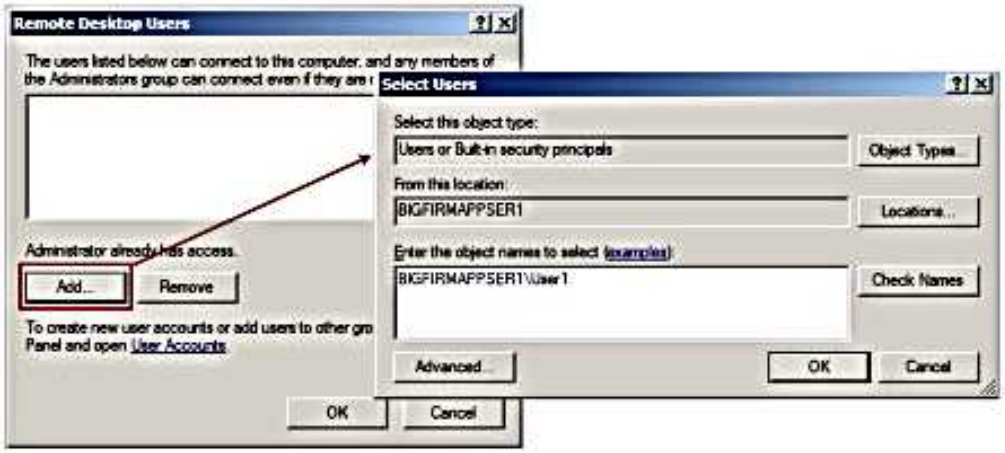
شکل ۲-۳۱

با توجه به نوع شبکه و کاربران خود، یکی از گزینه‌های مذکور را انتخاب کنید.

٤. بطور پیش‌فرض، همه مدیران سرور می‌توانند به RDP دسترسی داشته باشند. اما گاهی اوقات نیاز است به تعدادی از کاربران نیز، امکان دسترسی به سرور ولی در سطح پایین‌تری نسبت به مدیران داده شود. جهت انجام این کار، بر روی دکمه Select Users کلیک کنید.

شکل ۲-۳۲

۵. در پنجره "Remote Desktop Users"، برروی دکمه Add کلیک نموده و نام کاربر یا گروه مورد نظر را وارد کنید. سپس برروی OK کلیک نموده و پنجره‌ها را ببندید (می‌توانید از طریق دکمه Advanced جستجوی پیشرفته‌تری را برای پیدا کردن کاربران و کامپیوترها اجرا کنید).



Active Directory

اکتیو دایرکتوری یک پایگاه‌داده مرکزی در ویندوز سرور است که تمامی اطلاعات مربوط به اشیاء متصل به شبکه را در خود نگهداری می‌کند. با اینکه تاکنون مطالب زیادی در مورد ساختار پیچیده اکتیو دایرکتوری نوشته شده است، بسیاری از سازمان‌ها ترجیح می‌دهند که به دلیل سهولت کار، از ساختار مبتنی بر یک دامنه استفاده کنند. پیاده‌سازی ساختار تک‌دامنه‌ای بسیار ساده است، ولی در مواردی که تعداد کاربران بیش از ۵۰۰۰۰ باشند و یا به دلایل خاصی دامنه‌های بیشتری نیاز باشد، این ساختار توصیه نمی‌گردد.

ایجاد یک دامنه نسبتاً ساده است. کافی است یک نام برای آن انتخاب نموده و با راه‌اندازی ویزارد نصب کنترل‌کننده دامنه یا DCPromo، سرور خود را به یک کنترل‌کننده دامنه[1] (DC) تبدیل کنید. مهمترین ابزاری که در مدیریت دامنه‌ها به کار خواهید برد، ابزاری بنام Active Directory Users and Computers می‌باشد. به کمک این ابزار می‌توانید کاربران و اشیاء کامپیوتری را در دامنه ایجاد نموده و آنها را در قالب یک واحد سازمانی[2] (OU) سازماندهی کنید. البته ایجاد اشیاء اکتیو دایرکتوری از طریق خط فرمان نیز امکان‌پذیر می‌باشد.

۶-۱ آشنایی با مفاهیم پایه اکتیو دایرکتوری

قبل از پرداختن به بحث اکتیو دایرکتوری لازم است با تعدادی از مفاهیم و اصطلاحات پایه آشنا شوید. در ادامه این اصطلاحات را به صورت مختصر معرفی نموده و سپس در طول فصل با آنها بیشتر آشنا خواهید شد.

۶-۱-۱ Workgroup

یک شبکه Workgroup گروهی از کاربران هستند که به یک شبکه محلی[5] (LAN) متصل شده و در آن هر کامپیوتر دارای حساب‌های کاربری مجزایی می‌باشد. کاربری که با استفاده از یک حساب

---

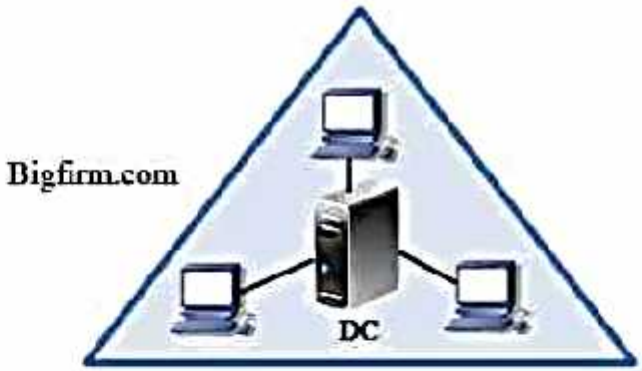
1. Domain Controller
2. Organizational Unit
3. Single-domain forest
4. Fine-Grained Password Policies
5. Local Area Network

کاربری می‌تواند به یک کامپیوتر وارد شود، برای ورود به کامپیوتری دیگر نیازمند حساب کاربری جداگانه‌ای می‌باشد. در این شبکه‌ها، استفاده از حساب‌های کاربری متعدد برای کاربران یکسان چندان جالب نمی‌باشد زیرا هر کاربر با تعدادی از حساب‌های کاربری و رمز عبورهای متفاوت سرو کار دارد.

شبکه‌های Workgroup معمولا برای سازمان‌هایی که دارای تعداد کمتر از ۱۰ کامپیوتر هستند مناسب است، اما زمانی که این تعداد افزایش پیدا می‌کند، مدیریت آن‌ها سخت‌تر شده و در نتیجه به یک دامنه نیاز می‌باشد.

Domain ۲-۱-۶

زمانی که تعداد کامپیوترهای یک سازمان از تعداد کامپیوترهای یک شبکه Workgroup (معمولاً ۱۰ کامپیوتر) فراتر می‌رود، با استفاده از ویزاردی به نام " ویزارد استقرار کنترل‌کننده دامنه[1]" (DCPromo) یک دامنه (مثل Bigfirm.com) برروی سرور ایجاد شده و سرور را به یک DC تبدیل می‌کند. DC سروری است که یک کپی از اکتیو دایرکتوری را نگهداری (میزبانی) می‌کند.



شکل ۶-۱

۶-۱-۳ Active Directory Domain Services (AD DS)

AD DS سرویسی است که برای تبدیل سرور به یک DC استفاده می‌شود. در اصل، این سرویس یک پایگاه‌داده از اشیائی (مثل کاربران، کامپیوترها و گروه‌ها) است که جهت سازماندهی متمرکز و مدیریت تمامی اشیاء در سازمان استفاده می‌شود. یک کاربر می‌تواند تنها با در اختیار داشتن یک حساب کاربری در اکتیو دایرکتوری از چندین کامپیوتر در سازمان استفاده کند بدون اینکه برای ورود به هر کامپیوتر نیاز به حساب جداگانه‌ای داشته باشد.

کپی‌هایی از اکتیو دایرکتوری برروی DCها نگهداری می‌شوند. معمولا برای اهداف افزونگی[2]، حداقل از دو DC استفاده می‌شود تا در مواقع از کار افتادن یکی از آنها بتوان از دیگری استفاده نمود.

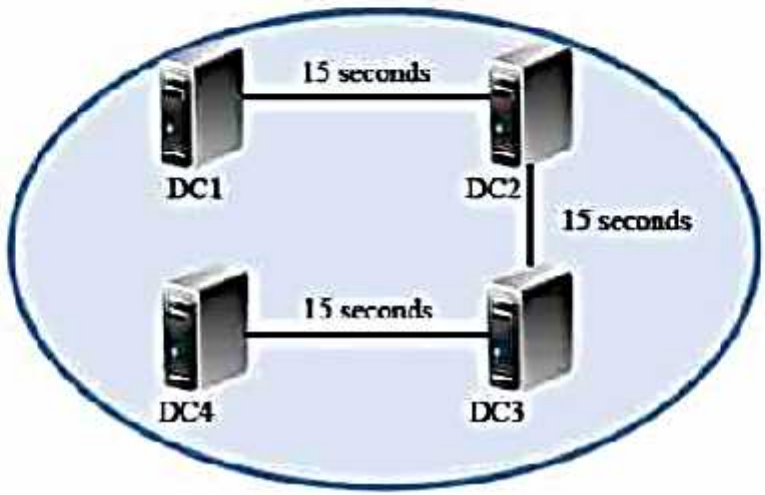
---

1. Domain Controller Promotion
2. Redundant

هر تغییری که در اکتیو دایرکتوری ایجاد شود با استفاده از پروسه‌ای به نام Replication (تکثیر) به هر کدام از این DCها ارسال می‌گردد.

۶-۱-۴ Replication

زمانی که هر شیء (مثل User Account) توسط اکتیو دایرکتوری (AD) اضافه، حذف و یا مورد تغییر واقع می‌شود، این تغییرات به تمام DCها در یک دامنه فرستاده شده و برروی آنها اعمال می‌گردد. ارسال تغییرات از هر DC به دیگری ۱۵ ثانیه طول می‌کشد. چنانچه تعداد DCها در سازمان بیش از چهار عدد باشند، در قالب یک مدار منطقی سازماندهی شده و طی پروسه Replication، تغییرات اعمال شده برروی یک DC در طول مدار منعکس شده و به سایر DCها تحویل داده می‌شود، سپس برروی آنها اعمال می‌گردد.



Objects ۵-۱-۶

اشیاء در اکتیو دایرکتوری بیانگر آیتم‌هایی هستند که بطور واقعی وجود دارند. رایجترین اشیاء، کاربران و کامپیوترها هستند که بیانگر افراد و کامپیوترهای موجود در سازمان می‌باشند. اشیاء بوسیله AD DS مدیریت و نگهداری می‌شوند. به عنوان مثال برای نشان دادن کاربری مثل Sally، یک شیء User Account به نام Sally ایجاد می‌شود. پس از آن کاربری با نام Sally می‌تواند با حساب کاربری خود به دامنه وارد شده و از منابع اشتراک گذاشته در آن مثل فایل‌ها، پوشه‌ها، پرینترها و ایمیل استفاده کند. البته این کار زمانی امکان‌پذیر است که مجوزهای لازم به آن کاربر داده شده باشد. بطور مشابه، یک شیء Computer Account می‌تواند برای نشان دادن کامپیوتر Sally ایجاد شود. هر شیء دارای مشخصاتی است که می‌تواند مورد تغییر قرار گیرد از جمله First name، Last name، Logon name، Display name و Password برای یک شیء کاربر.

تمامی اشیاء AD DS و نوع آنها از قبل تعیین شده هستند بنابراین امکان ایجاد اشیاء دلخواه و یا مشخصات دلخواه برای آنها وجود ندارد. کلیه این اشیاء و مشخصات آنها در Schema مشخص شده‌اند.

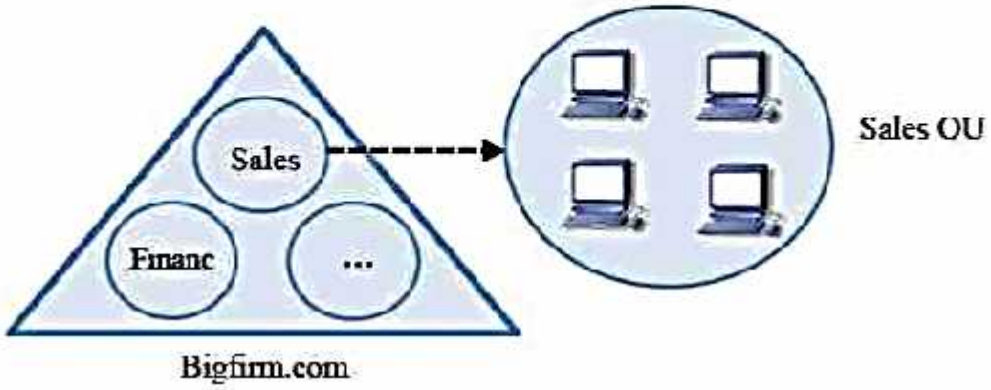
Schema ۶-۱-۶

Schema (اسکیما)، کلیه اشیاء قابل استفاده در اکتیو دایرکتوری را تعریف نموده و شامل لیستی از مشخصاتی است که این اشیاء را توصیف می‌کنند. اشیاء Schema در حالت عادی قابل تغییر نیستند اما گاهی اوقات و به دلایل خاص باید تغییراتی در آنها اعمال شود. به عنوان مثال زمانی که برنامه-هایی مانند Exchange Server 2007 (برای ایمیل) نصب می‌شوند، Schema باید برای پذیرفتن اشیاء جدید تغییر کند (یا به عبارتی گسترش یابد).

Organizational units ۶-۱-۷

واحدهای سازمانی (OU)، برای سازماندهی اشیاء در اکتیو دایرکتوری استفاده می‌شوند. در واقع OUها مانند کانتینرهایی[1] هستند که جهت نگهداری اشیاء مورد استفاده قرار می‌گیرند. با قرار دادن اشیاء در این کانتینرها مدیریت آنها آسانتر می‌شود. به عنوان مثال می‌توانید یک OU با نام Sales (فروش) ایجاد نموده و تمام کاربران و کامپیوترهای بخش فروش را در آن قرار دهید.

OUها دو مزیت ممتاز دارند: اول، می‌توان برروی آنها مجوزهایی[2] برای دسترسی اشیاء تعیین نمود. دوم، می‌توان انواع Group Policyها را ایجاد نموده و به آنها پیوند داد. به عنوان مثال Maria مسئول تمام کاربران و کامپیوترها در بخش فروش است. اگر این اشیاء در یک OU به نام Sales قرار داده شوند، Maria برای مدیریت آنها می‌تواند برروی آن OU مجوزی اعمال نموده تا برروی تمام کاربران و کامپیوترها اعمال شود. بطور مشابه می‌توانند با استفاده از اشیاء Group Policy (GPO) تنظیمات و پیکربندی‌های گوناگونی را برروی کاربران و کامپیوترهای این OU اعمال کنند.



Group Policy ۸-۱-۶

سیاست گروهی به شما امکان می‌دهد که تنظیماتی را پیکربندی نموده و آنها را برروی اشیاء کاربران و یا کامپیوترها اعمال کنید. به عنوان مثال برای اطمینان از اینکه فایروال برروی تمام کامپیوترهای بخش فروش فعال است می‌توانید تمام کامپیوترهای این بخش را در یک OU به نام Sales قرار داده، یک شیء Group Policy (GPO) که فایروال را فعال می‌کند پیکربندی نموده و سپس آنرا به Sales OU پیوند دهید. در این حالت تفاوتی ندارد که در این OU پنج کامپیوتر و یا ۵۰۰۰ کامپیوتر قرار داشته باشد. یک GPO تنظیمات را بر تمام کامپیوترهای داخل OU اعمال می‌کند.

می‌توانید GPOها را برروی OUها، دامنه‌ها یا سایت‌ها پیوند دهید. به عنوان مثال اگر قصد دارید که برروی کامپیوترهای تمام کاربران در دامنه فایروال فعال باشد، بجای پیوند GPO به یک OU باید آنرا به دامنه مورد نظر پیوند دهید. دقت داشته باشید که در هنگام ایجاد یک دامنه دو GPO بطور پیش‌فرض ایجاد می‌شوند: Default domain policy و Default domain controllers policy.

Default domain policy ۹-۱-۶

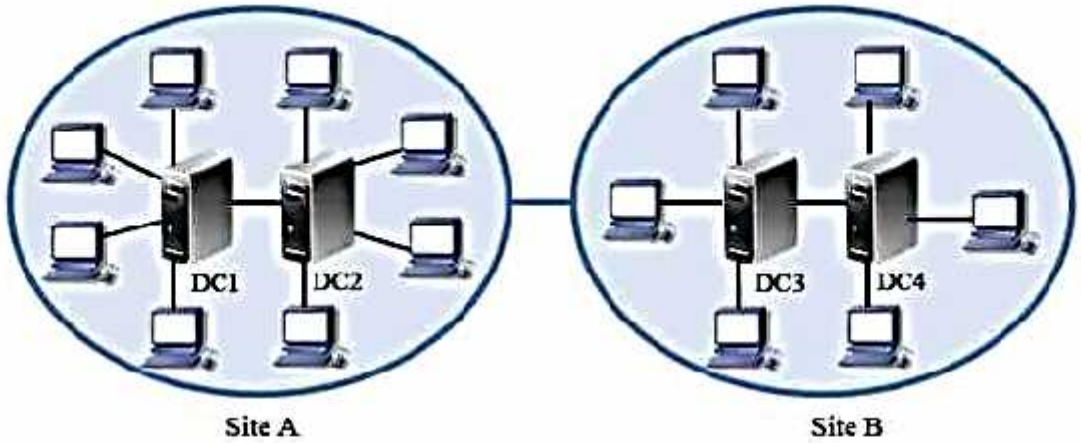
Default domain policy (سیاست پیش‌فرض دامنه)، یک GPO است که در زمان ایجاد یک دامنه، بطور پیش‌فرض ایجاد و پیکربندی شده و در سطح دامنه پیوند می‌شود. تنظیمات این GPO بر تمام کاربران و کامپیوترهای داخل دامنه اعمال می‌گردد. این سیاست با بعضی تنظیمات اولیه امنیتی مانند نیاز به رمز عبور آغاز می‌شود و می‌توان تنظیمات آنرا مورد تغییر قرار داد.

Default domain controllers policy ۱۰-۱-۶

Default domain controllers policy (سیاست پیش‌فرض DC) ، همانند GPO قبلی بوده با این تفاوت که در سطح DC پیوند می‌شود. زمانی که یک دامنه ایجاد می‌شود، یک OU نیز به همراه آن ایجاد شده (Domain Controllers OU) و تمام DCها در آن قرار داده می‌شوند. با پیوند سیاست پیش‌فرض برروی این OU، تمام DCهای داخل آن از این سیاست برخوردار می‌گردند.

Site ۱۱-۱-۶

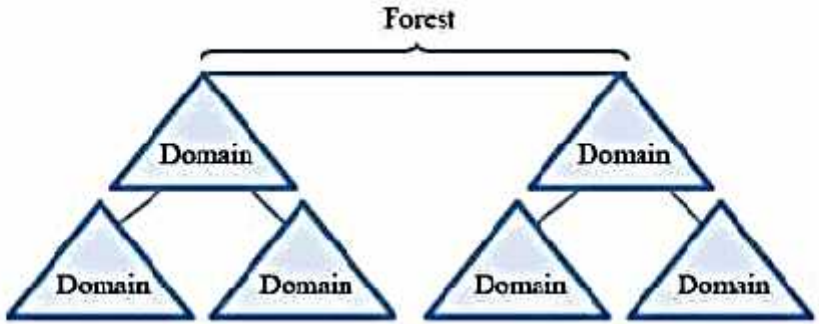
یک سایت، به گروهی از کامپیوترهای متصل بهم، و در بعضی موارد به گروهی از زیرشبکه‌های متصل بهم نیز گفته می‌شود. محدوده عملکرد سازمان‌های تجاری معمولاً خارج از یک محل است. کامپیوترهایی که در یک محل قرارداشته و از طریق یک شبکه LAN به یکدیگر متصل هستند، یک سایت را تشکیل می‌دهند. اگر یک اداره به صورت Remote ایجاد شده باشد، به عنوان یک سایت پیکربندی می‌شود. ممکن است چندین دامنه در یک سایت، و یا چندین سایت در یک دامنه (زمانی‌که هر زیرشبکه را به عنوان یک سایت درنظر بگیریم) وجود داشته باشد.



شکل ۶-۳

Forest ۱۲-۱-۶

جنگل، گروهی از یک یا بیشتر از یک دامنه است که اکتیو دایرکتوری یکسانی را با یکدیگر به اشتراک می‌گذارند. یک جنگل، تنها می‌تواند دارای یک Schema و یک Global Catalog باشد.



Global Catalog ۱۳-۱-۶

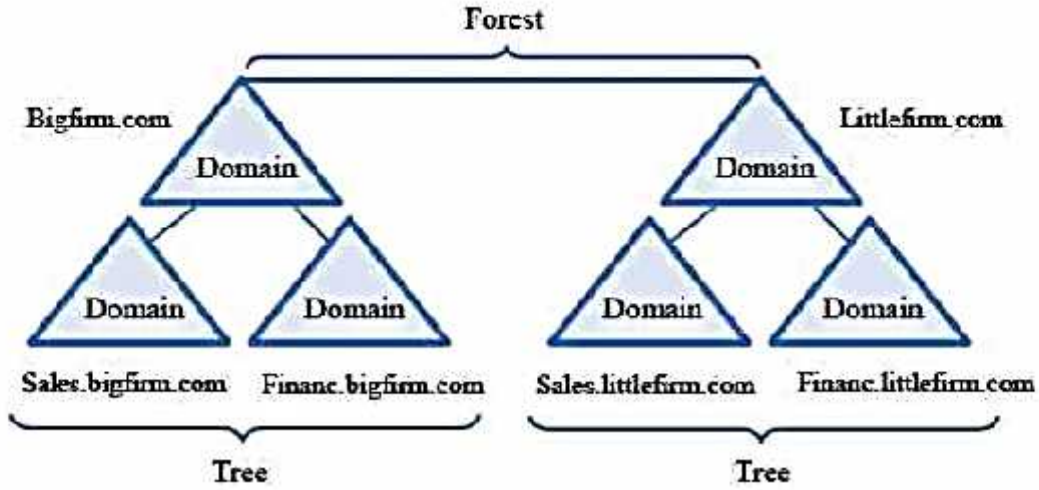
کاتالوگ عمومی (GC) لیستی از تمام اشیاء در یک جنگل است. این کاتالوگ به راحتی قابل جستجو بوده و اغلب توسط برنامه‌های مختلف به منظور جستجوی اشیاء AD DS استفاده می‌گردد. GC، برروی DCهایی قرار دارد که به عنوان سرور GC تعیین شده‌اند.

از آنجایی که تنها یک GC می‌تواند در یک جنگل وجود داشته باشد و هر جنگل می‌تواند شامل چندین دامنه باشد، بنابراین حجم فایل GC می‌تواند کمی بزرگ باشد. برای محدود کردن حجم آن، اشیاء داخل GC تنها می‌توانند دارای زیرمجموعه‌ای از مشخصات اصلی باشند. به عنوان مثال اگر یک حساب کاربری دارای ۱۰۰ مشخصه برای توصیف آن باشد، تنها ۱۰ مشخصه از آن در GC آورده

Tree ۱۴-۱-۶

درخت، به مجموعه‌ای از دامنه‌ها با فضای نام مشترک گفته می‌شود. به زبان ساده‌تر، دو بخش ریشه در فضای نام همه این دامنه‌ها یکسان است. به عنوان مثال اگر اولین دامنه در درخت Bigfirm.com باشد، دامنه‌های فرزند آن (زیردامنه‌ها) می‌توانند Sales.bigfirm.com و Financ.bigfirm.com باشند. بنابراین مجموع این دامنه‌ها که دو بخش اصلی آنها (Bigfirm.com) مشترک است، یک درخت را تشکیل می‌دهند.

یک جنگل می‌تواند بیشتر از یک درخت را شامل شود. به عنوان مثال، علاوه بر درخت Bigfirm.com می‌تواند شامل درختی با فضای نام مشترک Littlefirm.com نیز باشد. فضای نام این درخت‌ها یکسان نیستند ولی چون در یک جنگل قرار دارند، Schema و Global Catalog در آنها مشترک است.



۶-۲ جنگل تک دامنه‌ای

اکثر شبکه‌ها تنها از یک دامنه در اکتیو دایرکتوری استفاده می‌کنند. هر سازمانی که در اثر رشد تعداد کامپیوترها از حالت Workgroup خارج می‌شود، و یا سازمان‌هایی که نیاز خاصی به افزودن دامنه ندارند، از یک دامنه استفاده می‌کنند.

بطور کلی توصیه می‌شود زمانی که تعداد کاربران به حداکثر بین ۱۰ تا ۲۰ کاربر می‌رسد، نوع شبکه را از Workgroup به دامنه انتقال دهید. با این کار هر کاربر تنها نیاز به داشتن مشخصات یک حساب کاربری دارد و از هر کامپیوتری در دامنه می‌تواند به حساب خود وارد شود.

همانطور که قبلا اشاره نمودیم استفاده از یک دامنه در شبکه کافی است مگر اینکه نیاز به افزودن دامنه ثانویه‌ای باشد. معمولاً افزودن این دامنه به یکی از دلایل زیر رخ می‌دهد:

- تعداد اشیاء کاربران و کامپیوترها بیشتر از ۱۰۰،۰۰۰ (۵،۰۰۰ کامپیوتر به اضافه کاربران آنها) باشد و بنابراین پردازش‌های Replication با سرعت کمی انجام می‌شود.
- به دلیل تغییرات مداوم، کارایی Replication تحت فشار قرار دارد.
- شبکه از چندین قسمت که در محل‌های مختلفی قرار دارند تشکیل شده و این محل‌ها با استفاده از اتصالات WAN با سرعت کم، با یکدیگر ارتباط دارند. بنابراین کارایی Replication تحت فشار قرار گرفته است.

توجه داشته باشید که بیشتر این موارد مربوط به Replication می‌باشد. اگر در شبکه کمتر از ۱۰۰،۰۰۰ شیء کاربر و کامپیوتر دارید و فرایند Replication به خوبی انجام می‌شود نیازی به استفاده از دامنه ثانویه نیست.

از لحاظ فنی، یک دامنه یک جنگل نیز می‌باشد. اولین دامنه در جنگل، دامنه ریشه[1] است و یک جنگل تک دامنه‌ای تنها شامل دامنه ریشه می‌باشد. در سازمان‌های خیلی بزرگ ممکن است چندین جنگل به منظور فعال‌سازی Schemaها، مدیریت منابع مختلف، تقسیم‌بندی دسترسی مدیر شبکه و یا حتی به دلایل جغرافیایی یا سیاسی ایجاد شود. مدیریت و ایجاد تغییر در دامنه‌های موجود در جنگل‌های چند دامنه‌ای نیازمند دقت و اطمینان زیادی می‌باشد زیرا سایر دامنه‌ها نیز باید لحاظ گردند. اما مدیریت جنگل‌های تک دامنه‌ای به دلیل عدم وجود دامنه‌های دیگر کار نسبتاً ساده‌ای می‌باشد.

۶-۲-۱ مزایای استفاده از یک دامنه

زمانی که تنها از یک دامنه استفاده می‌شود، تمام اشیاء اکتیو دایرکتوری (مانند کاربران، کامپیوترها و ...) که در سازمان مورد استفاده قرار می‌گیرند، در آن قرار داده می‌شوند. استفاده از چنگل‌های تک دامنه‌ای دارای چندین مزیت به شرح زیر می‌باشد:

- **کم هزینه:** هر دامنه می‌تواند فعالیت خود را با یک DC آغاز کند. در مواردی که نیاز باشد می‌توان از یک DC ثانویه نیز به عنوان پشتیبان استفاده نمود. افزودن هر دامنه اضافه نیازمند سرورهای اضافه و بنابراین سخت افزارها و نرم افزارهای بیشتری می‌باشد. علاوه بر آن، هزینه‌هایی نیز برای مدیریت این سرورها مصرف می‌شود. بدین ترتیب زمانی که نیاز چندانی به وجود دامنه ثانویه نباشد می‌توان با صرف هزینه‌ای کم یک دامنه راه‌اندازی نموده و با استفاده از آن کاربران و شبکه را مدیریت نمود.

---

1. Root Domain

- **مدیریت آسانتر:** هر دامنه‌ای که ایجاد می‌شود، به دنبال آن حساب‌های کاربری، گروه‌ها، انواع سیاست‌های گروهی و ... نیز باید ایجاد شوند. زمانی که از یک دامنه استفاده شود با حجم کمتری از این اشیاء روبرو خواهید بود و بنابراین (نسبت به زمانی که چندین دامنه در اختیار دارید) به آسانی می‌توانید آنها را مدیریت کنید.
- **بازیابی فاجعه[1] ساده‌تر:** اغلب دیده می‌شود که سرورهای موجود در شبکه ناموفق عمل کرده و یا بطور ناگهانی از کار می‌افتند. برای رفع چنین مشکلاتی باید از اطلاعات این سرورها Backup تهیه نموده و در صورت نیاز آنها را بازگردانی کرد. زمانی که از یک دامنه استفاده می‌کنید، تعداد سرورهای کمتری مورد استفاده قرار می‌دهید بنابراین بازگردانی این سرورها در صورت از کار افتادن و یا وقوع هر مشکلی ساده‌تر خواهد بود.

یکی از دلایلی که در گذشته مدیران شبکه‌ها را مجبور به ایجاد چندین دامنه می‌کرد، اعمال سیاست‌های رمزعبور مختلف بر روی یک دامنه بود. از ویندوز سرور 2008 به بعد، این مسئله برطرف شده و به کمک سیاست‌های دانه‌ریز رمز عبور می‌توان چندین Password Policy بر روی یک دامنه ایجاد کرد (بعداً در همین فصل به این موضوع خواهیم پرداخت).

۶-۲-۲ ایجاد جنگل تک دامنه‌ای

زمانی که ویندوزسرور 2008R2 را برای اولین بار نصب می‌کنید، ایجاد دامنه در آن بسیار ساده خواهد بود. کافی است ویزارد Domain Controller Promotion یا همان DCPromo را اجرا نموده و سرور خود را به یک DC تبدیل کنید. این ویزارد، سرویس‌های مربوط به دامنه در اکتیو دایرکتوری یا Active Directory Domain Services را برروی سرور راه‌اندازی (یا حذف) می‌کند. ویزارد DCPromo برروی هر نسخه از ویندوز سرور (مثل2000، 2003، 2008 و ...) قابل اجرا است اما قابلیت‌های دامنه در این نسخه‌ها متفاوت می‌باشد.

اگرچه ویزارد DCPromo راه‌اندازی DC برروی یک دامنه را به سادگی انجام می‌دهد، اما در هنگام نصب با مراحلی برخورد می‌کنید که آگاهی از آنها لازم است. در ادامه، این مراحل را معرفی نموده و سپس هریک را مورد بررسی قرار می‌دهیم:

- پیکربندی سرور
- بررسی سازگاری سیستم‌عامل[۲]
- پیکربندی توسعه[۳]

---

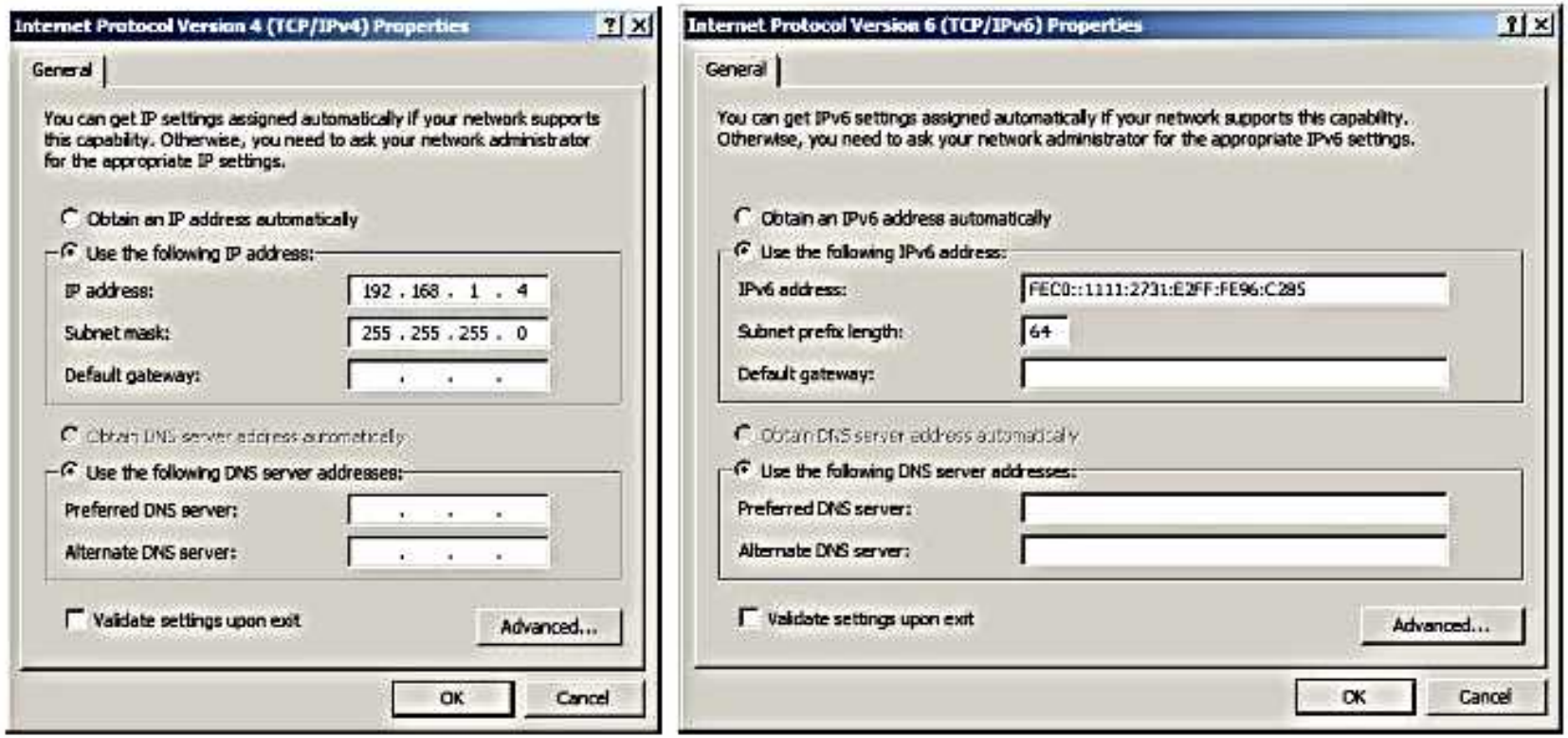
1. Disaster recovery
2. Operating System Compatibility
3. Deployment Configuration

- نام دامنه
- سطح عملکرد جنگل[1]
- سطح عملکرد دامنه[2]
- پیکربندی DNS
- محل قرارگیری فایل‌ها
- رمز عبور مدیر DSRM[3]

قبل از اجرای DCPromo (پیکربندی سرور)

قبل از اجرای DCPromo باید مطمئن شوید که سرور به درستی پیکربندی شده است. دو اقدام اصلی در این رابطه، انتخاب نام و آدرس IP برای سرور است.

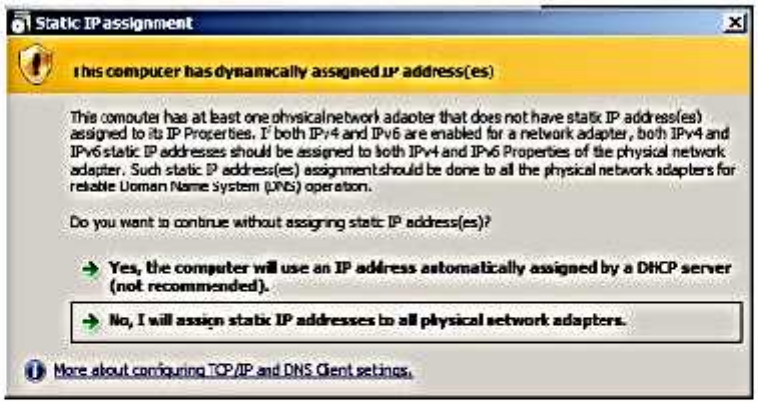
- **نام سرور**: قبل از اینکه سرور را به یک DC تبدیل کنید، بهتر است یک نام برای آن انتخاب نموده و برروی آن اعمال کنید. معمولاً سازمان‌ها از نام‌های DC1، DC2 و مانند آن استفاده می‌کنند. انتخاب این نام بستگی به نظر مدیر شبکه و سیاست‌های سازمان دارد. جهت تنظیم نام برروی سرور می‌توانید مسیر Computer» Properties» Change Settings» Change را دنبال نموده و با مشاهده پنجره Computer Name، نام کامپیوتر (یا سرور) را تغییر دهید.
- **آدرس IP**: DC باید دارای یک آدرس IP ثابت باشد. در ویندوز سرور 2008R2 از هر دو نوع IPv4 و IPv6 پشتیبانی می‌شود بنابراین می‌توانید هر دو نوع آدرس را اختصاص دهید.



شکل ۶-۷

1. Forest Functional Level
2. Domain Functional Level
3. Directory Services Restore Mode

اگر IPv4 را به صورت دستی اختصاص دهید ولی اختصاص آدرس IPv6 برروی خودکار تنظیم شده باشد، در هنگام نصب DCPromo با خطای زیر مواجه خواهید شد.



شکل ۶-۸

امکان نصب DCPromo بدون اختصاص آدرس IP ثابت به سرور وجود دارد اما ممکن است در هنگام پیکربندی DNS در این فرایند با مشکلاتی روبرو شوید. بنابراین بهترین کار این است که قبل از اجرای DCPromo آدرس IP ثابتی را به سرور اختصاص دهید. چنانچه قصد دارید سرور DNS را در این ویزارد پیکربندی کنید (روش پیشنهادی برای پیکربندی سرور DNS)، باید آدرسی برای این سرور نیز فراهم کنید.

سازگاری سیستم عامل (Operating System Compatability)

طی سال‌های گذشته، در رابطه با استفاده از کامپیوتر و سیستم‌های کامپیوتری چیزی که زیاد شنیده می‌شد و یا مطالب زیادی در مورد آن انتشار پیدا می‌کرد، این بود که این سیستم‌ها توسط ویروس‌ها و به دلایل سرگرمی مورد حمله قرار می‌گرفتند. امروزه وضعیت فرق کرده است و این حملات بیشتر بجای سرگرمی برای سرقت اطلاعات و دریافت پول از سازمان مورد حمله انجام می‌شوند. مدیران شبکه باید از فعال‌سازی هر حفره امنیتی که موجب باز نمودن راه نفوذ به شبکه می‌شود پیشگیری کنند. یکی از این حفره‌ها این است که کاربران ویندوز NT 4.0 و کاربرانی که از سیستم‌های غیر مایکروسافت SMB[1] (مثل لینوکس) استفاده می‌کنند، سعی می‌کنند توسط DCها تأیید هویت شوند.

شیوه کدگذاری که در ویندوز NT 4.0 به کار می‌رود امروزه به عنوان یک شیوه فاقد امنیت به شمار رفته و قابل استفاده نیست. به منظور تقویت این شیوه، مایکروسافت نصب پیش‌فرض دامنه در ویندوز سرور 2008 و 2008R2 را امن‌تر نموده است. یکی از اقداماتی که در این زمینه انجام شده، تنظیماتی تحت عنوان " Allow cryptography algorithms compatible with Windows NT 4.0" می‌باشد.

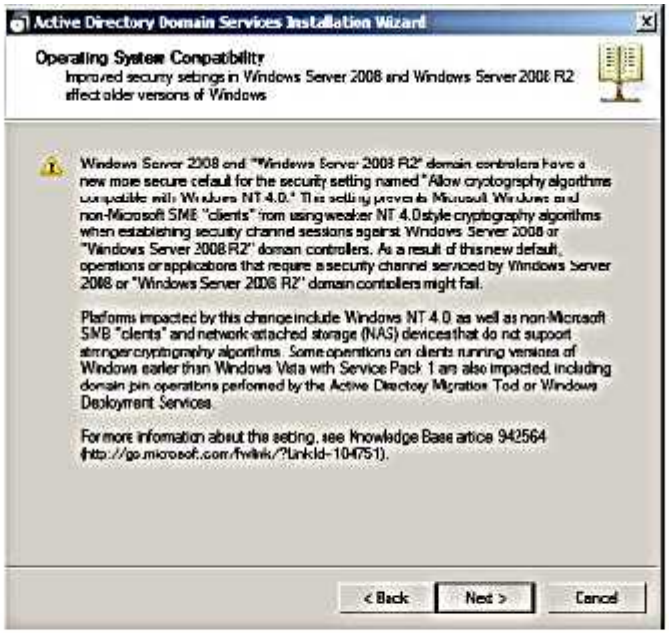
---

1. Server Message Block

این تنظیمات برای جلوگیری از اتصال کاربرانی است که از شیوه کدگذاری ضعیف Windows NT 4.0 استفاده می‌کنند.

با اینکه افزایش امنیت یک مزیت محسوب می‌شود ولی اثرات جانبی نیز به همراه دارد. یکی از این اثرات، کاهش قابلیت استفاده از سیستم‌ها در شبکه می‌باشد. به عنوان مثال کاربران قدیمی ویندوز NT 4.0، بعضی کاربران SAMBA SMB (نرم افزاری برای ارائه خدمات فایل و پرینت در سیستم‌های یونیکس و لینوکس) و حتی بعضی از وسایل ذخیره‌ساز متصل به شبکه[۲] (NAS) ممکن است در هنگام اتصال به شبکه با مشکل مواجه شوند. پیشنهاد مایکروسافت این است که برای جلوگیری از به خطر افتادن امنیت شبکه، این کاربران سیستم عامل‌های خود را به نسخه‌های جدیدتر (یا به نسخه‌های ویندوز) ارتقاء دهند.

ویزارد DCPromo امکان ایجاد تغییرات در این تنظیمات را فراهم نمی‌کند ولی در صفحه "Operating System Compatibility" هشدارهایی را در این رابطه متذکر می‌شود. در شکل ٦-٩ این صفحه نمایش داده شده است.



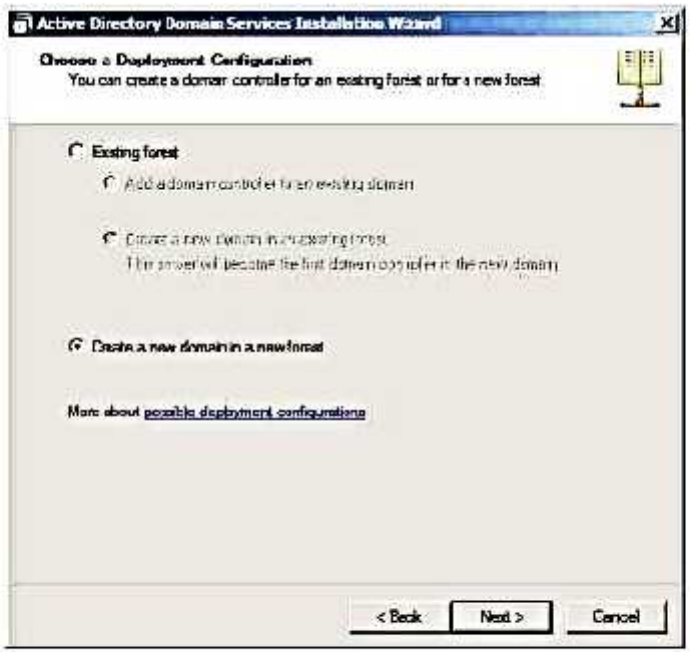
شکل ۶-۹

پیکربندی‌های توسعه (Deployment Configuration)

این پیکربندی‌ها به شما اجازه می‌دهد که تعیین کنید آیا دامنه شما در یک جنگل جدید ایجاد شود و یا در جنگلی که در حال حاضر وجود دارد. در صورتی که دامنه را در جنگل فعلی ایجاد کنید، می‌توانید DC دیگری را به دامنه اضافه کنید. برای ایجاد اولین DC، انتخاب شما ساده خواهد بود. یک دامنه جدید در یک جنگل جدید ایجاد می‌کنید.

---

1. Network Attached Storage

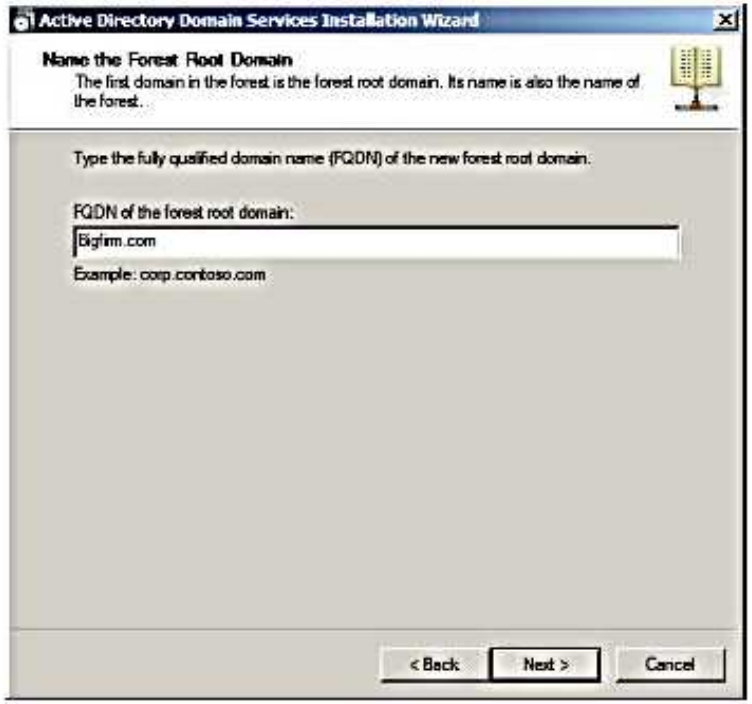


شکل ۶-۱۰

اختصاص نام به دامنه ریشه (Name the Forest Root Domain)

اولین دامنه در هر جنگل، به دامنه ریشه اشاره دارد. در زمان ایجاد یک دامنه ریشه باید از یک FQDN[1] برای آن استفاده کنید. این FQDN از دو جزء تشکیل می‌شود، مانند Bigfirm.com یا Mydomain.net که دومین قسمت در این FQDNها (com. و net. در این مثال) اشاره به نام دامنه سطح بالا دارد. تعدادی از دامنه‌های سطح بالا که ممکن است در اینترنت مشاهده کنید عبارت‌اند از: org.، tv.، ir.، biz.، gov. و ...

در شکل ٦-١١ (و مثال ما) نام FQDN انتخاب شده برای دامنه به صورت Bigfirm.com است.



شکل ۶-۱۱

1. Fully Qualified Domain Name

در این صفحه باید از FQDNهای دوقسمتی استفاده کنید اما توجه داشته باشید که نام انتخابی شما با نام‌های معتبری که در اینترنت وجود دارند یکسان نباشد.

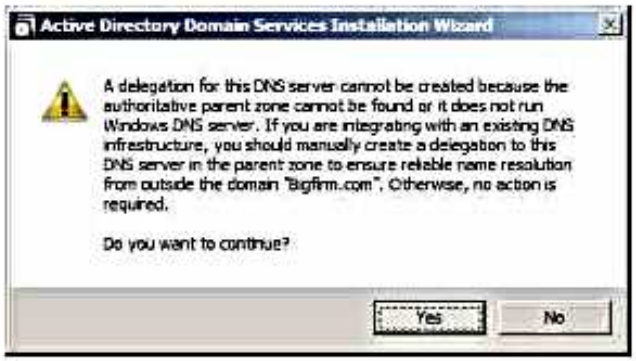
اکتیو دایرکتوری و DNS

در فصل ۵ راجع به رابطه اکتیو دایرکتوری و DNS صحبت کردیم. چیزی که بطور مختصر لازم است بدانید این است که DNS یکی از نیازمندی‌های اکتیو دایرکتوری می‌باشد. رکوردهای SRV در DNS محل نگهداری DCهایی هستند که سرویس‌های خاصی را اجرا می‌کنند.

DNS با اکتیو دایرکتوری بسیار یکپارچه است، بنابراین زمانی که مشکلی در اکتیو دایرکتوری رخ می‌دهد اولین چیزی که مورد بررسی قرار می‌گیرد سرور DNS است. معمولاً گفته می‌شود که ۷۰ درصد مشکلات اکتیو دایرکتوری مربوط به DNS است. اگر DNS به خوبی عمل نکند و یا بطور صحیح پیکربندی نشده باشد، اکتیو دایرکتوری نیز قادر به اجرا نمی‌باشد.

از آنجایی که DNS می‌تواند پیچیده باشد، DCPromo فرایند نصب و پیکربندی اولیه سرور DNS را به صورت بسیار ساده‌ای انجام می‌دهد. در هنگام اجرای DCPromo، این ویزارد تشخیص می‌دهد که DNS نصب نشده است و بنابراین پیشنهاد پیکربندی آنرا به شما ارائه می‌دهد. چنانچه اجازه کار به آن داده شود، سرور DNS به خوبی پیکربندی خواهد شد.

DCPromo در ابتدا سعی می‌کند یک Delegation برای سرور DNS ایجاد کند اما اگر DNS نصب نشده باشد این عمل با شکست مواجه شده و پیغامی مشابه زیر به شما نشان داده می‌شود، که البته این پیغام عادی است.



شکل ۶-۱۲

پس از دریافت این پیغام، برروی Yes کلیک کنید تا فرایند نصب ادامه یابد و DCPromo، DNS را پیکربندی کند. این ویزارد، Zone مربوط به DNS را به صورت " Zone یکپارچه با اکتیودایرکتوری[1]" ایجاد می‌کند.

1. Active Directory Integrated Zone

سطح عملکرد جنگل (Set Forest Functional Level)

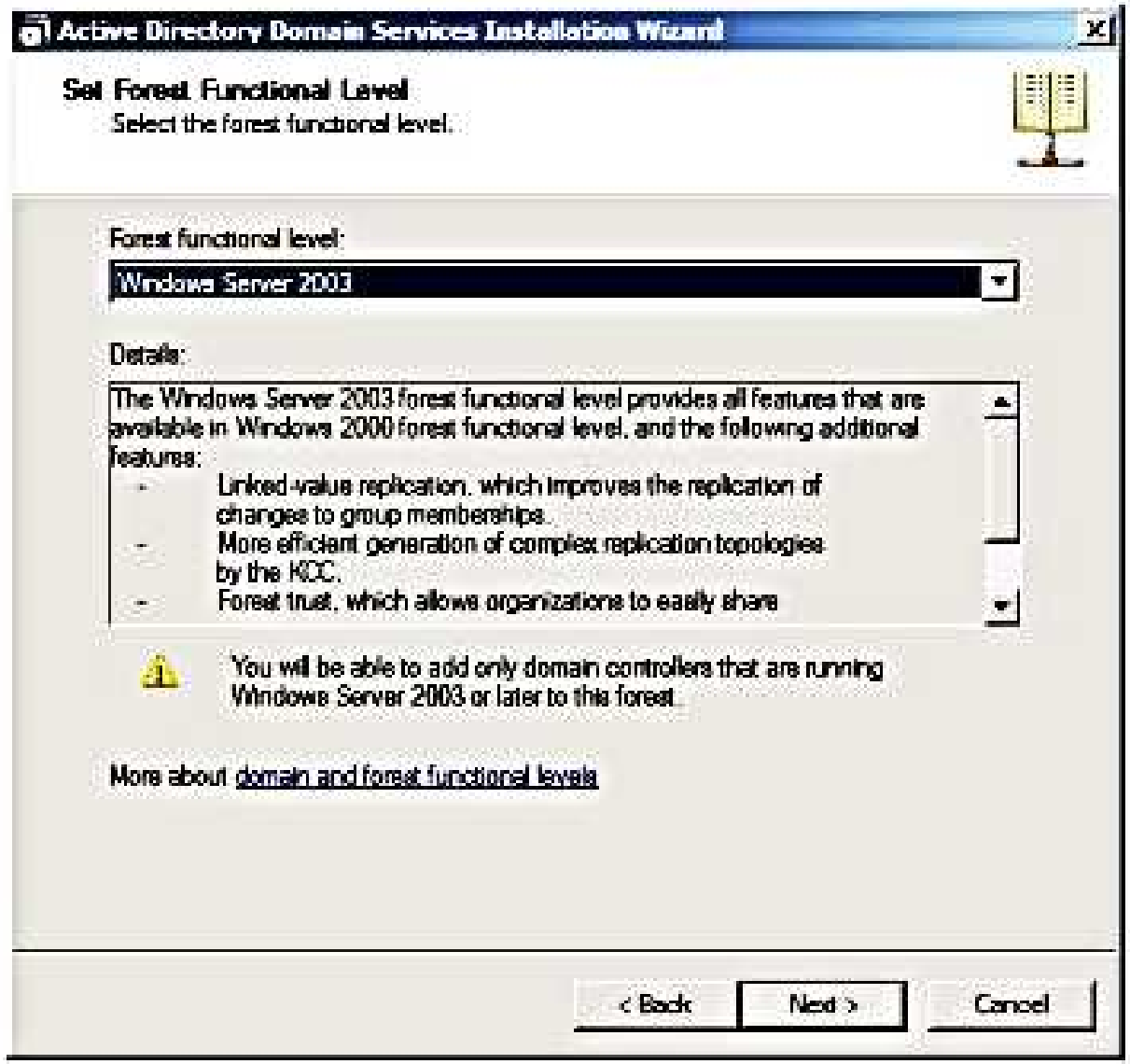
این سطح قابلیت‌های یک جنگل را مشخص می‌کنند. بخاطر داشته باشید که سطح عملکرد دامنه باید منطبق با قدیمی‌ترین سیستم عامل اجرا شونده برروی DC در دامنه باشد. بطور مشابه، سطح عملکرد جنگل نیز باید منطبق با قدیمی‌ترین سیستم عامل اجرا شونده برروی DC در جنگل باشد. به عنوان مثال اگر سطح Windows Server 2008 را برای سطح عملکرد جنگل انتخاب کنید، تنها انتخاب‌های شما برای سطح عملکرد دامنه، Windows Server 2008 و Windows Server 2008 R2 خواهد بود.

موارد زیر برای سطوح عملکرد جنگل توسط DCPromo پیشنهاد می‌شوند:

- Windows Server 2000
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

همانطور که امکان افزایش سطح عملکرد دامنه وجود دارد، افزایش سطح جنگل (در آینده) نیز امکان‌پذیر است. تنها نکته‌ای که لازم است بدانید این است که ابتدا باید سطح عملکرد دامنه و سپس سطح عملکرد جنگل را افزایش دهید. اگر در شبکه از چندین دامنه استفاده می‌کنید، ابتدا باید سطوح تمام دامنه‌ها در جنگل و سپس سطح جنگل را افزایش دهید.

با اجرای DCPromo در پنجره‌ای همانند شکل ٦-١٣ می‌توانید سطح عملکرد جنگل را تعیین کنید. برای انجام این کار کافی است سطح عملکرد یکسان با آنچه در سطح عملکرد دامنه تعیین نمودید را انتخاب کنید. به عنوان مثال اگر سطح عملکرد دامنه Windows Server 2008 R2 بود سطح عملکرد جنگل نیز باید Windows Server 2008 R2 انتخاب شود.


Active Directory Domain Services Installation Wizard
Set Forest Functional Level
Select the forest functional level.
Forest functional level:
Windows Server 2003
Details:
The Windows Server 2003 forest functional level provides all features that are available in Windows 2000 forest functional level, and the following additional features:
- Linked-value replication, which improves the replication of changes to group memberships.
- More efficient generation of complex replication topologies by the KCC.
- Forest trust, which allows organizations to easily share
You will be able to add only domain controllers that are running Windows Server 2003 or later to this forest.
More about domain and forest functional levels
< Back
Next >
Cancel

تنظیم سطح عملکرد دامنه (Set Domain Functional Level)

در هنگام اجرای ویزارد DCPromo از شما خواسته می‌شود که سطح عملکرد دامنه و سطح عملکرد جنگل را مشخص کنید. این سطوح در واقع بیانکر سیستم‌عامل‌هایی هستند که توسط DCها در شبکه مورد استفاده قرار می‌گیرند، بنابراین باید منطبق با قدیمی‌ترین سیستم‌عامل انتخاب شوند. چهار سطح عملکرد برای دامنه موجود می‌باشد. این سطوح عبارتند از:

- Windows Server 2000 native
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

با انتخاب هر سطح می‌توان از DCهایی که دارای نسخه‌های بالاتر و یا یکسان با سطح مورد نظر هستند استفاده کرد. به عنوان مثال با انتخاب سطح Windows Server 2008 می‌توان از سیستم عامل‌های ویندوز سرور 2008 و 2008R2 به عنوان DC استفاده نمود.

این انتخاب شما DCهایی که در آینده اضافه می‌شوند را نیز تحت تأثیر قرار می‌دهد. فرض کنید یک سرور با ویندوز سرور 2008R2 را به یک DC تبدیل نموده و سطح عملکرد Windows Server 2008 R2 را برای دامنه انتخاب می‌کنید. پس از مدتی تصمیم می‌گیرید که یک DC ثانویه به عنوان پشتیبان اضافه کنید. برروی این سرور ثانویه حتماً باید ویندوز سرور 2008R2 اجرا شود. چنانچه سرور دیگری با ویندوز سرور 2003 داشته باشید نمی‌توانید در این دامنه آنرا به DC تبدیل کنید. با توجه به این مسئله، دو عامل مهم را در هنگام انتخاب سطح عملکرد باید در نظر داشته باشید:

- همیشه می‌توان سطح عملکرد را به سطوح بالاتر افزایش داد.
- هرگز امکان کاهش سطح عملکرد وجود ندارد

در واقع این کار مثل اضافه کردن نمک به غذا می‌باشد. می‌توان مقدار نمک غذا را افزایش داد اما پس از افزودن، امکان کاهش آن وجود ندارد. بنابراین همانند اضافه کردن نمک به غذا که با احتیاط باید انجام شود بهتر است سطح عملکرد دامنه را نیز کمی پایین در نظر بگیرید (مثلاً Windows Server 2003) تا در صورت نیاز بتوان آنرا افزایش داد.

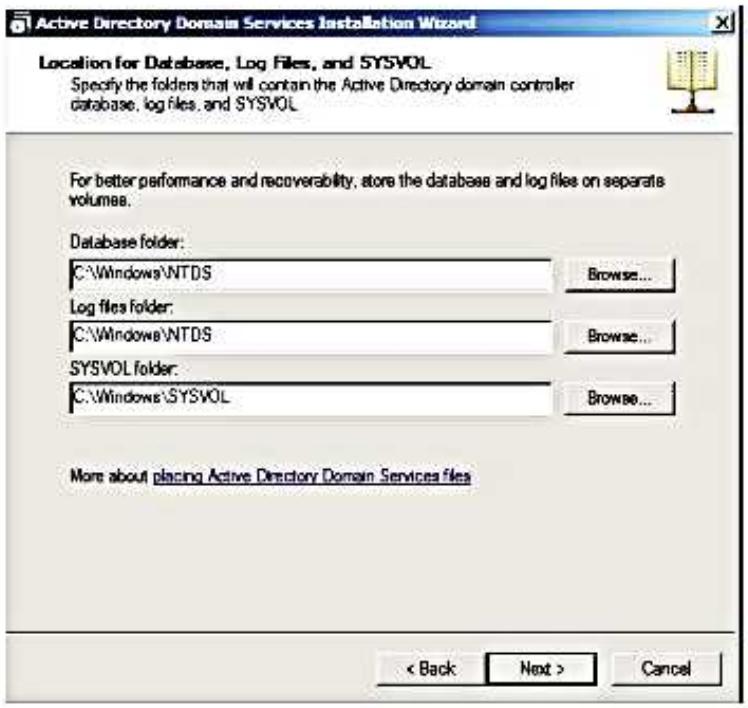
زمانی که DCpromo را اجرا می‌کنید، پنجره‌ای همانند زیر برای تعیین سطح عملکرد دامنه نشان داده می‌شود. چنانچه در شبکه از DCهایی استفاده می‌کنید که برروی سیستم عامل‌های قدیمی‌تر اجرا می‌شوند بهتر است پایین‌ترین سطح مورد استفاده را انتخاب کنید. بعداً می‌توانید این سطح را در صورت نیاز افزایش دهید.

شکل ۶-۱۴

محل قرارگیری فایل‌ها و SYSVOL (Location for Database, Log Files, and SYSVOL)

یکی دیگر از تنظیماتی که در ویزارد DCPromo باید انجام شود، تعیین محل قرارگیری فایل‌های اکتیو دایرکتوری و همچنین محل پوشه اشتراکی SYSVOL می‌باشد.

پوشه اشتراکی SYSVOL برای اشتراک‌گذاری اطلاعاتی مانند اسکریپت‌ها و اشیاء Group Policy بین DCها استفاده می‌شود. SYSVOL باید در یک درایو با فرمت NTFS قرار داشته باشد. به منظور بهینه‌سازی عملکرد سرور، می‌توان پایگاه‌داده و فایل‌های Log اکتیو دایرکتوری را در درایوهای جداگانه‌ای قرار داد.



در اصل، اکتیو دایرکتوری یک پایگاه‌داده عظیم است که شامل فایل داده اصلی و یک فایل مربوط به تراکنش‌های Log (ورود) می‌باشد. تغییراتی که در این پایگاه‌داده اعمال می‌شوند، ابتدا برروی فایل تراکنش Log نوشته شده و سپس این فایل‌ها به صورت دوره‌ای مورد بررسی قرار می‌گیرند. این کار در واقع روشی برای اعلام ایجاد تغییرات برروی پایگاه‌داده می‌باشد.

تراکنش‌های Log امکان تحمل خطا و قابلیت بازیابی مطمئنی را برای پایگاه‌داده اکتیو دایرکتوری فراهم می‌کنند. زمانی که سرور در اثر ایجاد یک تغییر در اکتیو دایرکتوری عملکردش را از دست می‌دهد، با استفاده از Log و بررسی موفق یا عدم موفق بودن اعمال یک تغییر می‌تواند مطمئن شود که پایگاه‌داده در زمان Boot شدن سرور در وضعیت مناسب و سازگاری قرار دارد.

از دیدگاه کارایی، امکان افزایش کارایی DC با استفاده از انتقال پایگاه‌داده و فایل تراکنش log به درایو دیگری وجود دارد. یک پیکربندی دیسک بهینه برای قرارگیری فایل‌های اکتیو دایرکتوری می‌تواند به صورت زیر انجام شود:

- درایو C:\ : سیستم عامل
- درایو D:\ : فایل پایگاه‌داده اکتیو دایرکتوری و SYSVOL
- درایو E:\ : فایل تراکنش log

در این پیکربندی هر درایو نیازمند یک دیسک فیزیکی می‌باشد، زیرا استفاده از یک درایو با سه پارتیشن بهبود چندانی در کارایی ایجاد نمی‌کند. چنانچه دیسک‌های انتخابی شما از سرعت‌های متفاوتی برخوردار هستند باید سریع‌ترین دیسک را به سیستم عامل، دیسکی که سرعت کمتری دارد را به فایل تراکنش log و کندترین دیسک را نیز به فایل پایگاه‌داده اکتیو دایرکتوری و SYSVOL اختصاص دهید. علت این کار این است که سیستم عامل و فایل تراکنش log از عملکرد سنگین‌تری برخوردار هستند.

اجازه دهید مثالی در این رابطه ارائه دهیم. فرض کنید تعداد کاربران دامنه شما ۱۰۰ کاربر هستند. در اینصورت می‌توانید فایل پایگاه‌داده و log را در همان دیسک سیستم عامل (C:\) قرار دهید بدون اینکه مشکلی در کارایی بوجود آید. اما حالتی را در نظر بگیرید که تعداد کاربران ۵۰،۰۰۰ کاربر باشند. در اینصورت باید برای کاهش فشار و بهینه‌سازی عملکرد، فایل‌های log و پایگاه‌داده را در درایوهای متفاوتی ذخیره کنید.

اگر در ابتدا تمام فایل‌ها را در یک محل ذخیره کرده باشید و بعداً تصمیم بگیرید که این فایل‌ها را به درایو دیگری منتقل کنید، این کار امکان‌پذیر است. با استفاده از ابزار NTDSUtil در خط فرمان، دستوری تحت عنوان Files برای انتقال این فایل‌ها در نظر گرفته شده است. البته برای انتقال فایل‌ها باید در حالت Directory Services Restore Mode قرار داشته باشید.

رمز عبور مدیر Directory Services Restore Mode

اگر نیاز به نگهداری یا بازسازی اکتیو دایرکتوری داشته باشید، باید این کار را با استفاده از Directory Services Restore Mode (DSRM) انجام دهید. برای دسترسی به این حالت باید در هنگام راه‌اندازی سرور کلید F8 را فشار دهید تا به منوی تنظیمات پیشرفته[1] هدایت شوید. سپس در این منو باید گزینه Directory Services Restore Mode را انتخاب نموده و enter را فشار دهید. با ورود به حالت DSRM چون هنوز اکتیو دایرکتوری اجرا نشده است، نمی‌توانید با یک حساب کاربری به آن وارد شوید. در عوض می‌توانید برای مدیریت، از یک حساب کاربری مخصوص با رمز عبوری متفاوت استفاده کنید. در DCPromo باید رمز عبور این حساب کاربری را مشخص کنید. در شکل زیر پنجره مربوطه ("Directory Services Restore Mode Administrator Password") نشان داده شده است.

دقت داشته باشید که این رمز عبور را در جایی مطمئن ثبت نموده و نگهداری کنید. بدون این رمز عبور قادر نخواهید بود به DSRM دسترسی پیدا کنید. بسیاری از سازمان‌ها این رمز عبور را مشابه با رمز عبور مدیر سرور (رمزی که در هنگام Logon شدن به سرور استفاده می‌شود) انتخاب می‌کنند اما توجه داشته باشید که اینها با یکدیگر متفاوت هستند.

شاید پس از مدتی نیاز داشته باشید که رمز عبور DSRM را تغییر دهید. این کار با استفاده از ابزار NTDSUtil در خط فرمان امکان‌پذیر است. NTDSUtil شامل دستور Set DSRM Password است که با استفاده از آن می‌توان رمز عبور DSRM را تغییر داد. جهت آگاهی از سایر دستورهای استفاده شده توسط NTDSUtil می‌توانید از علامت ?/ استفاده کنید.

1. Advanced Options

اجرای DCPromo

پس از آشنایی با مراحل پیشِ رو در ویزارد DCPromo، می‌توانید این ویزارد را جهت تبدیل سرور به DC و ایجاد جنگل تک دامنه‌ای اجرا کنید. در کنسول Server Manager نیز Roleای به نام Active Directory Domain Services تعبیه شده است اما نصب این Role تنها تعدادی ویژگی به DC اضافه می‌کند.

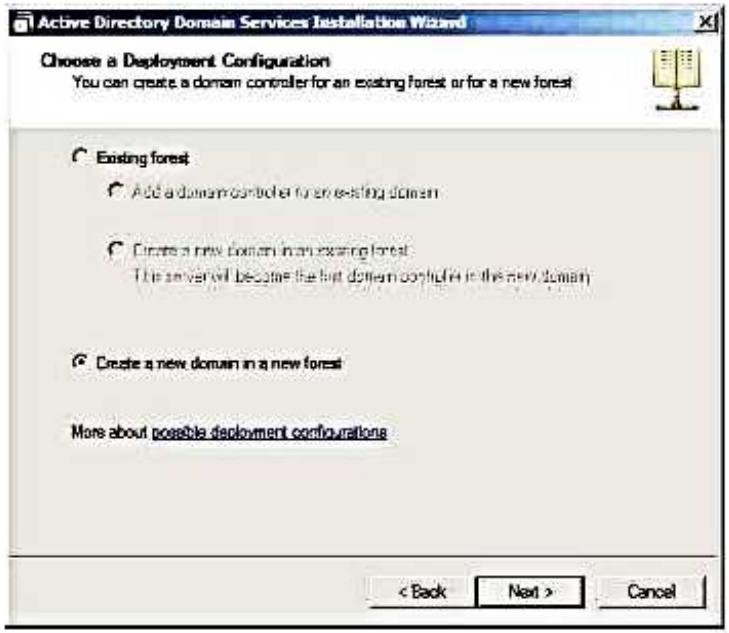
قبل از اجرای DCPromo لازم است تمام Roleهایی که نصب کرده‌اید را حذف کنید، زیرا این ویزارد باید قبل از نصب هر Role دیگری اجرا شود. جهت تبدیل سرور به DC (و ایجاد جنگل تک دامنه‌ای) مراحل زیر را دنبال کنید:

۱. با حساب کاربری مدیر (Administrator) به ویندوز وارد شوید.
۲. از منوی Start و در قسمت جستجو، عبارت DCPromo را وارد نموده و enter را فشار دهید.
۳. با مشاهده صفحه "Welcom to the Active Directory Domain Services Installation Wizard" ویزارد DCPromo آغاز می‌گردد. برروی Next کلیک کنید.

شکل ۶-۱۷

٤. در صفحه "Operating System Capability"، اطلاعات مربوط به سازگاری سیستم عامل‌های قابل اتصال به DC را مشاهده نموده و برروی Next کلیک کنید (شکل ٦-٩).

٥. در صفحه "Choose a Deployment Configuration" گزینه Create a new domain in a new Forest را انتخاب نموده و برروی Next کلیک کنید.



شکل ۶-۱۸

۶. در صفحه "Name the Forest Root Domain" (شکل ۶-۱۱)، نام FQDN دامنه را وارد نموده و برروی Next کلیک کنید (در اینجا از Bigfirm.com استفاده شده است).

۷. در صفحه "Set Forest Functional Level"، گزینه Windows Server 2003 را انتخاب و برروی Next کلیک کنید (شکل ۶-۱۳).

۸. در صفحه"Set Domain Functional Level"، گزینه Windows Server 2003 را انتخاب و برروی Next کلیک کنید (شکل ۶-۱۴).

۹. در صفحه "Additional Domain Controller Options"، مطمئن شوید که گزینه DNS انتخاب شده است. با انتخاب این گزینه DCPromo سرویس DNS را به همراه خود نصب می‌کند. دقت داشته باشید که گزینه Global Catalog بطور پیش‌فرض انتخاب شده است ولی قابل تغییر نیست. علت این است که اولین DC در دامنه به عنوان Global Catalog Server (GC Server) درنظر گرفته می‌شود.

۱۰. اگر در تنظیمات TCP/IP دریافت آدرس IP (IPv4 یا IPv6) از سرور DHCP و به صورت خودکار باشد، پیغامی ظاهر شده و اعلام می‌کند که کارت شبکه سرور دارای آدرس IP ایستا[1] (ثابت) نیست. پیشنهاد می‌شود که یک آدرس ایستا (با انتخاب گزینه No, I will assign static IP addresses to all physical network adapters) به آن اختصاص دهید. در صورتی که که این آدرس IPv4 را در اختیار دارید وارد نموده و همچنین IPv6 را نیز فعال کنید. در غیر اینصورت برروی Yes, the computer will use an IP address automatically assigned by DHCP server کلیک کنید تا فرایند نصب ادامه یابد (شکل ٦-٨).

۱۱. DCPromo سعی می‌کند که یک سرور DNS را موقعیت‌یابی کند. چنانچه سروری وجود نداشته باشد، پیغامی ظاهر شده و اعلام می‌کند که برای دامنه هیچ Zoneای ایجاد نشده است. این پیغام عادی است. DCPromo، سرور DNS را پیکربندی خواهد نمود. برروی Yes کلیک کنید تا فرایند نصب ادامه پیدا کند (شکل ٦-١٢).

۱۲. در صفحه "Location for Database, Log Files,and SYSVOL" باید محل قرارگیری فایل‌های پایگاه‌داده، فایل‌های log و همچنین SYSVOL را تعیین کنید. بهتر است از همین مسیرهای پیش‌فرض استفاده کنید. برروی Next کلیک کنید (شکل ٦-١٥).

۱۳. در صفحه "Directory Services Restore Mode Administrator Password"، رمز عبور مدیر DSRM را وارد کنید. برای امنیت بیشتر این رمز را ترکیبی از حروف، اعداد و علائم انتخاب کنید (مانند P@ssw0rd). برروی Next کلیک کنید (شکل ٦-١٦).

۱۴. در صفحه "Summary" خلاصه‌ای از تنظیمات انجام شده نشان داده می‌شود. این تنظیمات چیزی شبیه شکل ٦-۱۹ خواهد بود.

شکل ۶-۲۰

1. Static IP Address

۱۵. برروی Next کلیک کنید تا فرایند نصب DC آغاز شود. با شروع فرایند، صفحه زیر را مشاهده خواهید نمود. در این صفحه، تیک مربوط به گزینه Reboot on completion را فعال نموده تا پس از اتمام عملیات، سیستم بطور خودکار Reboot (Restart) شود.

شکل ۶-۲۱

۱۶. پس از راه‌اندازی سرور، در هنگام ورود از شما رمز عبور خواسته می‌شود. این رمز، همان رمز عبور مدیر سرور است که قبل از تبدیل سرور به یک DC از آن استفاده می‌کردید.

ویزارد DCPromo را می‌توان با استفاده از یک فایل پاسخ (و به صورت خودکار) نیز انجام داد. برای انجام این کار، مراحل زیر را دنبال کنید:

ویزارد DCPromo را می‌توان با استفاده از یک فایل پاسخ (و به صورت خودکار) نیز انجام داد. برای انجام این کار، مراحل زیر را دنبال کنید:

۱. در صفحه "Summary" از DCPromo، برروی دکمه Export Setting کلیک کنید. این دکمه تنظیمات انجام شده توسط شما را در قالب یک فایل پاسخ ذخیره می‌کند.
۲. پنجره "Save unattend file" ظاهر می‌شود. نام DCPromoexport و مسیر C:\ (ریشه درایو C) را جهت ذخیره فایل انتخاب نموده و برروی Save کلیک کنید.
۳. از مسیر Start » Comand Prompt خط فرمان (Cmd) را اجرا کنید.
٤. در Cmd، عبارت `cd\` را تایپ نموده و enter را فشار دهید.
٥. عبارت `notepad DCPromoexport.txt` را تایپ نموده و enter را فشار دهید. برنامه Notepad اجرا شده و محتویات فایل پاسخی که ایجاد نموده‌اید را نشان می‌دهد. در این فایل خطوطی که با علامت (;) شروع می شوند جنبه توضیحی داشته و نادیده گرفته می‌شوند.

توجه داشته باشید که در مقابل عبارت `SafeModeAdminPassword` هیچ رمز عبوری وجود ندارد. پس از علامت مساوی (=) در این خط، یک رمز عبور مانند P@ssw0rd وارد کنید. این خط باید چیزی شبیه زیر باشد:

```
SafeModeAdminPassword=P@ssw0rd
```

٦. به عنوان یک اقدام امنیتی، DCPromo در هر بار اجرا، رمز عبور نوشته شده پس از علامت (=) را پاک می‌کند. به همین دلیل اگر قصد دارید از این رمز عبور به صورت مداوم استفاده کنید، یا باید در هر بار استفاده این رمز را وارد نموده و یا فایل را به صورت Read-Only ذخیره کنید. همچنین برای Restart شدن سرور پس از اتمام عملیات می توانید علامت (;) را قبل از عبارت `RebootOnCompletion=Yes` حذف کنید. برای اعمال تغییرات و ذخیره آنها برروی فایل، کلیدهای Crtl+S را فشار دهید.

٧. مجددا به Cmd بازگشته و عبارت `DCPromo.exe /unattend:c:\DCPromoexport.txt` را وارد کنید. پس از فشردن enter، DCPromo از روی فایل پاسخ اجرا خواهد شد.

۶-۴ ایجاد واحدهای سازمانی(OU)، حساب‌های کاربری و گروه‌ها

پس از ایجاد دامنه، نوبت به ایجاد اشیائی مثل OUها، حساب‌های کاربران، حساب‌های کامپیوتری، گروه‌ها و مانند آنها است. اصلی‌ترین ابزاری که در این رابطه استفاده می‌شود، Active Directory Users and Computers (ADUC) می‌باشد. ADUC به شما امکان می‌دهد تا به سادگی و فقط با چند کلیک هر چیزی را ایجاد کنید. البته ایجاد این اشیاء از طریق خط فرمان نیز امکان‌پذیر است. استفاده از خط فرمان برای ایجاد اشیاء به دو دلیل مفید است:

- اگر از Server Core استفاده کنید، امکان دسترسی به ADUC وجود ندارد.
- هر چیزی که از طریق خط فرمان ایجاد می‌شود را می توان به صورت Script ذخیره نمود.

۶-۴-۱ ایجاد واحدهای سازمانی

واحدهای سازمانی به منظور سازماندهی اشیاء در اکتیو دایرکتوری مورد استفاده قرار می‌گیرند. هر شیء (مانند کاربر، کامپیوتر، گروه و ...) جهت مدیریت آسانتر می‌تواند در OU قرار گیرد.

معمولاً OUها بر طبق بخش‌های سازمان ایجاد می‌شوند. مثلاً (بخش فروش و ...) اما دو دلیل فنی که مدیران برای ایجاد OUها به کار می‌گیرند عبارتند از:

- مدیریت گروه‌ها از طریق Group Policy
- مدیریت گروه‌ها از طریق Delegation (واگذاری)

مدیریت گروه‌ها از طریق Group Policy

امکان پیوند اشیاء Group Policy (GPO) به سایت‌ها، دامنه‌ها و OUها وجود دارد. بنابراین اگر قصد دارید برروی تعدادی از کاربران سیاست‌های خاصی را اعمال کنید می‌توانید حساب‌های آنها را در یک OU قرار داده و سپس GPO را به این OU پیوند دهید.

با این حال اگر بدون ایجاد OUها قصد اعمال سیاست خاصی را داشته باشید، این سیاست‌ها برروی تمام کاربران دامنه اعمال می‌شوند. فرض کنید قصد دارید یک برنامه را با استفاده از Group Policy در اختیار تمام کاربران بخش فروش قرار دهید. اگر GPOها را برروی دامنه اعمال کنید، برنامه مورد نظر نه تنها در اختیار کاربران بخش فروش، بلکه در اختیار تمام کاربران دامنه قرار می‌گیرد. حال اگر یک OU ایجاد نموده و کاربران این بخش را در آن قرار دهید و GPO را برروی آن اعمال کنید، تنها کاربران این بخش قادر به دریافت برنامه خواهند بود.

مدیریت گروه‌ها از طریق Delegation (واگذاری)

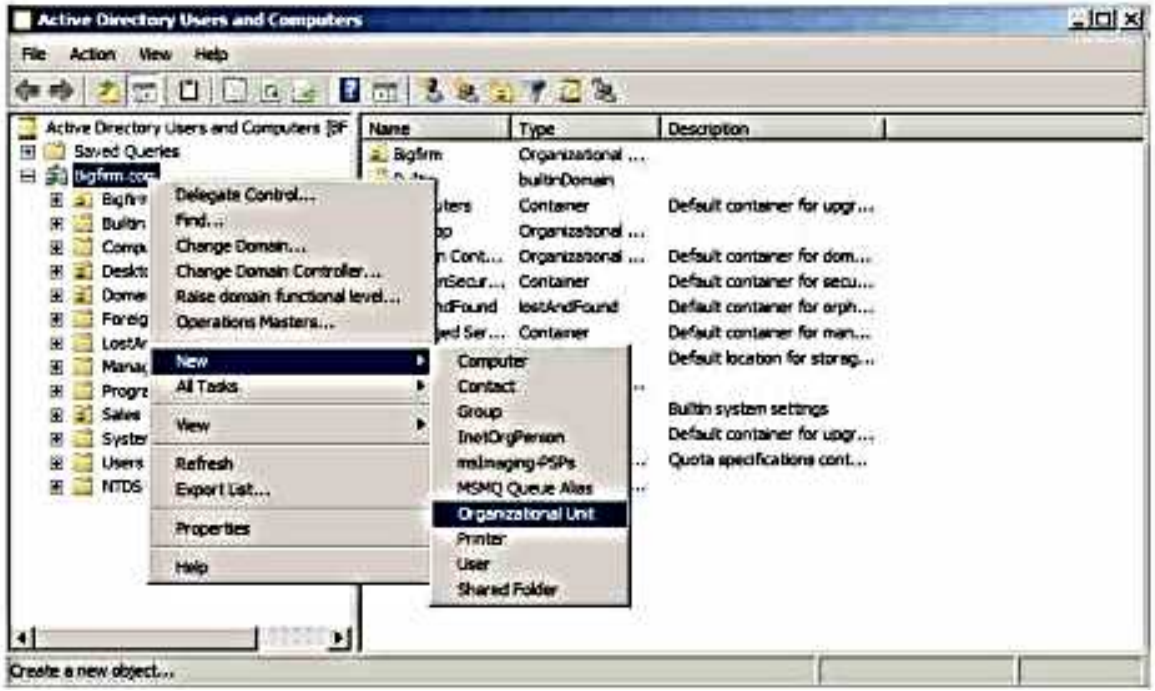
فرض کنید که در سازمان، شخصی به نام Sally وجود دارد که تنها او قادر است خدمات IT را به پرسنل ارائه داده و از آنها پشتیبانی کند. این شخص قادر است اعمالی مانند ایجاد حساب‌ها، تغییر رمز عبور کاربران، انجام عیب‌یابی‌های پایه و مانند آن را انجام دهد. با توجه به اینکه این شخص فقط باید برای کاربران بخش فروش این اقدامات را انجام دهد، می‌توان با استفاده از ویزاردی به نام "Delegation of Control Wizard" انجام این کار به او واگذار کرده و مجوزهای لازم را برروی آن اعمال نمود (بعداً در مورد این ویزارد صحبت خواهیم کرد).

ایجاد OUها به کمک ADUC

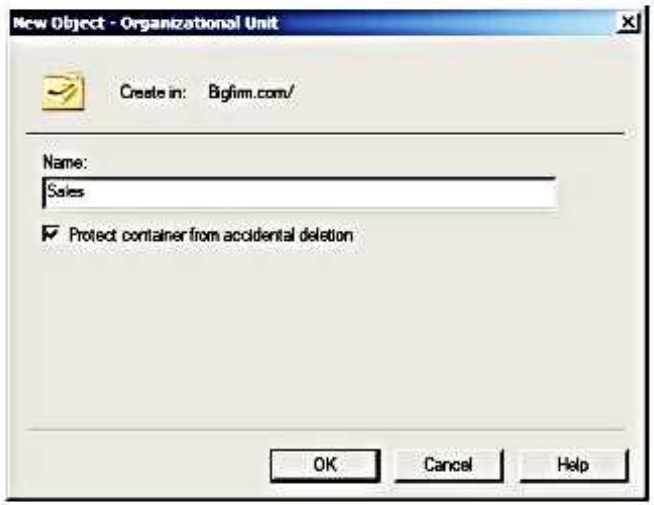
برای ایجاد OU با استفاده از ADUC مراحل زیر را دنبال کنید:

۱. ADUC را از مسیر Start «Administrative Tools «Active Directory Users and Computers اجرا کنید.

۲. برروی نام دامنه کلیک‌راست نموده و New « Organizational Unit را انتخاب کنید.



۳. در قسمت Name از پنجره باز شده، Sales را وارد نموده و گزینه Protect container from accidental deletion را فعال کنید. سپس برروی OK کلیک کنید.



شکل ۶-۳۰

٤. چنانچه قصد داشته باشید در داخل یک OU (در اینجا Sales)، OU دیگری (OU فرزند[1]) ایجاد کنید، کافی است برروی نام OU کلیک‌راست نموده و New « Organization Unit را انتخاب کنید. سپس نام آنرا وارد نموده (در اینجا Users) و برروی OK کلیک کنید. نام این OU در زیر نام OU اصلی قابل مشاهده می‌باشد.

شکل ۶-۳۱

نام‌های ممتاز LDAP

اکتیو دایرکتوری برای برقراری ارتباط از پروتکلی با نام LDAP[2] استفاده می‌کند. این پروتکل برای متمایز کردن اشیاء اکتیو دایرکتوری از یک سری نام‌های ممتاز[3] (DN) استفاده می‌کند که آشنایی با اجزای آن جهت ایجاد اشیاء به کمک خط فرمان ضروری می‌باشد.

فرمتی که DN استفاده می‌کند به صورت objectType=objectName (نام شیء = نوع شیء) به همراه

---

1. Child OU
2. Lightweight Directory Access Protocol
3. Distinguished Name

چندین نوع شیء است که بوسیله کاما از یکدیگر جدا شده‌اند. به عنوان مثال نام دامنه Bigfirm.com از دو جزء bigfirm و com تشکیل شده است که به صورت dc=bigfirm,dc=com شناخته می‌شود.

واحدهای سازمانی دارای نوع ou. و کانتینر Users و Computers نیز دارای نوع cn می‌باشند، بدین ترتیب DN مربوط به واحد سازمانی Sales در دامنه Bigfirm.com به صورت زیر نمایش داده می‌شود:

```
ou=Sales,dc=bigfirm,dc=com
```

کانتینر Users نیز دارای DN زیر می‌باشد:

```
cn=Users,dc=bigfirm,dc=com
```

یک حساب کاربری با نام Sally.Smith در واحد سازمانی Sales دارای DN زیر می‌باشد:

```
cn=Sally.Smith,ou=Sales,dc=bigfirm,dc=com
```

یک حساب کاربری با نام Joe.Johnson در کانتینر Users دارای DN زیر می‌باشد:

```
cn=Joe.Johnson,cn=Users,dc=bigfirm,dc=com
```

اگر OUها به صورت تو در تو باشند یا هر OU شامل تعدادی OU دیگر باشد، در DN ابتدا OUای که سطح پایین‌تر است قرار می‌گیرد. به عنوان مثال اگر Sales OU یک OU فرزند با نام Users داشته باشد و این OU نیز دارای کاربری به نام Maria باشد، DN آن به صورت زیر خواهد بود:

```
cn=Maria,ou=Users,ou=Sales,dc=bigfirm,dc=com
```

اگر DN شامل هرگونه فاصله‌ای باشد، باید آنرا در داخل علامت نقل قول (") قرار داد تا مطمئن شوید که به درستی تفسیر می‌شود. مثال زیر فاقد فاصله است پس نیازی به نقل قول ندارد:

```
cn=Maria,ou=Users,ou=Sales,dc=bigfirm,dc=com
```

اما DN زیر دارای فضای خالی است پس باید در داخل نقل قول قرار گیرد:

```
"cn=Maria, ou=Users, ou=Sales, dc=bigfirm, dc=com"
```

DNهای LDAP حساس به بزرگی و کوچکی حروف نیستند بنابراین دو DN زیر با یکدیگر برابرند:

```
cn=Maria,ou=Users,ou=Sales,dc=bigfirm,dc=com
CN=maria,OU=users,OU=sales,DC=BigFirm,DC=Com
```

ایجاد OUها به کمک DSAdd (خط فرمان)

با کمی آگاهی در مورد DNها می‌توانید تعدادی از OUها را به کمک خط فرمان و ابزار DSAdd ایجاد کنید. با استفاده از این ابزار امکان ایجاد اشیاء زیر وجود دارد:

- OU
- User
- Computer
- Group
- Contact

دستوراتی که برای ایجاد هریک از این اشیاء استفاده می‌شود، در جدول ٦-١ آورده شده است.

جدول ۶-۱ دستورات ایجاد اشیاء اکتیو دایرکتوری در خط فرمان

دستور	شرح
Dsadd computer	افزودن کامپیوتر به اکتیو دایرکتوری
Dsadd contact	افزودن تماس به اکتیو دایرکتوری
Dsadd group	افزودن گروه به اکتیو دایرکتوری
Dsadd ou	افزودن واحد سازمانی به اکتیو دایرکتوری
Dsadd user	افزودن کاربر به اکتیو دایرکتوری

برای اجرای DSAdd باید از خط فرمان استفاده کنید. قبل از اینکه بخواهید این ابزار را در Cmd به کار ببرید، ابتدا آنرا به صورت DSAdd /? وارد نموده تا اطلاعاتی راجع به آن دریافت کنید. حال برای دریافت اطلاع در مورد هر یک از دستورات این ابزار، مثلاً ایجاد OU می‌توانید آنرا به صورت DSAdd ou /? وارد کنید.

برای اینکه بتوانید با این دستورات ساده‌تر کار کنید، بهتر است آنها را با استفاده از علامت (>) در یک فایل متنی ذخیره کنید. این کار با اجرای دستور زیر قابل انجام می‌باشد:

```
DSAdd ou /? > DSAddhelp.txt
```

برای مشاهده فایل ایجاد شده نیز می‌توانید از دستور زیر استفاده کنید:

```
notepad DSAddhelp.txt
```

قالب کلی استفاده از دستور DSAdd OU به صورت زیر می‌باشد:

```
DSAdd ou DN
```

با اینکه گزینه‌های زیادی در این دستور قابل استفاده هستند ولی تنها پارامتر مورد نیاز، DN

است. فرض کنید قصد دارید تعدادی از کاربران که در بخش مالی قرار دارند را با استفاده از Group Policy مدیریت کنید. با استفاده از دستور زیر می‌توانید یک OU به نام Financ ایجاد نموده و این کاربران را در آن قرار دهید. در این دستور، DN به صورت ou=test,dc=bigfirm,dc=com می‌باشد.

```
DSAdd ou ou=financ,dc=bigfirm,dc=com
```

پس از اجرای این دستور چنانچه ADUC را اجرا کنید می‌توانید OU با نام Financ را مشاهده نمایید. دقت داشته باشید هر دستوری که به کمک خط فرمان وارد می‌کنید را می‌توان به صورت فایل‌های batch (.bat) ذخیره نموده و به راحتی مورد استفاده قرار داد. به عنوان مثال می‌توانید تمام دستورات مربوط به DSAdd را در یک فایل متنی وارد نموده و سپس آنرا با پسوند bat. ذخیره کنید. این فایل به راحتی در خط فرمان قابل اجرا می‌باشد. استفاده از فایل‌های batch زمانی کاربرد دارد که بخواهید از دستورات به دفعات زیادی استفاده کنید. این کار موجب صرفه‌جویی در وقت شما خواهد شد.

۶-۴-۲ ایجاد حساب‌های کاربری و کامپیوتری

پس از ایجاد OUها ممکن است بخواهید تعدادی حساب نیز ایجاد کنید. هم کاربران و هم کامپیوترها برای دسترسی به دامنه نیازمند حساب می‌باشند. همانند OUها می‌توانید با استفاده از Active Directory Users and Computers (ADUC) یا DSAdd، حساب‌های کاربری و کامپیوتری را ایجاد کنید.

حساب‌های کامپیوتری معمولاً زمانی که یک کامپیوتر به دامنه متصل می‌شود، بطور خودکار

ایجاد می‌شوند. بطور پیش‌فرض این حساب‌ها در کانتینر Computers قرار می‌گیرند اما می‌توانید با استفاده از ابزار redircmp در خط فرمان تغییراتی در محل قرارگیری آنها ایجاد کنید. قالب این دستور به صورت زیر می‌باشد:

```
Redircmp <DN>
```

به عنوان مثال زمانی که یک کامپیوتر به دامنه متصل می‌شود، در صورتی که بخواهید حساب آن کامپیوتر در واحد سازمانی Sales ایجاد شود می‌توانید دستور زیر را وارد کنید:

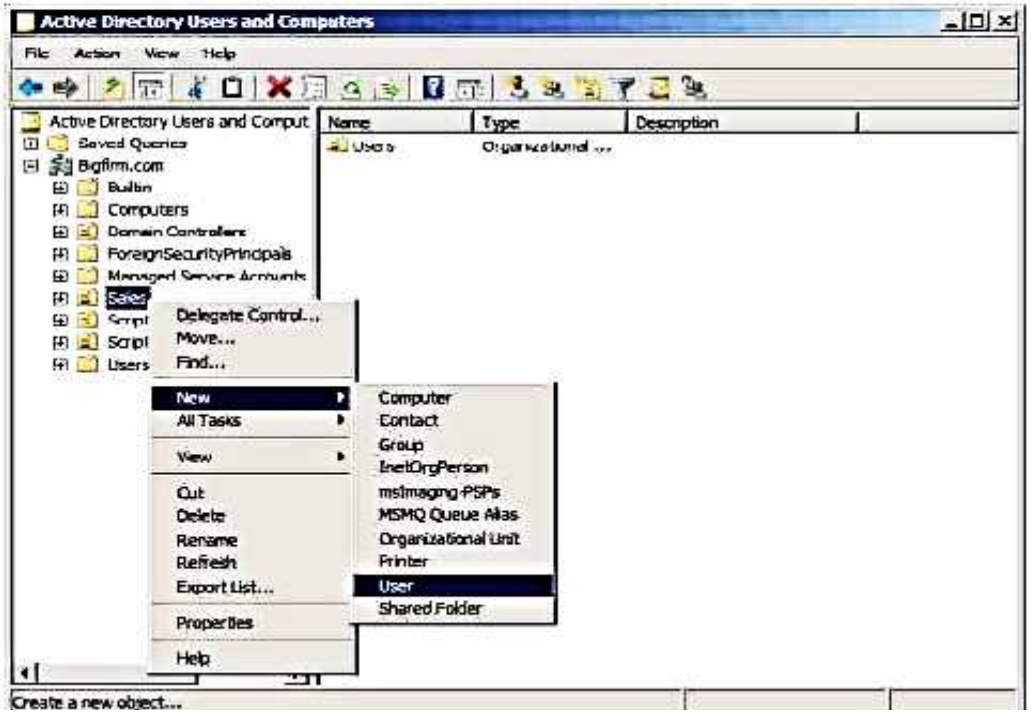
```
Redircmp "OU=Sales,DC=bigfirm,dc=com"
```

ایجاد حساب‌ها به کمک ADUC

برای ایجاد حساب از طریق ADUC مراحل زیر را دنبال کنید:

۱. ADUC را از مسیر Start « Administrative Tools « Active Directory Users and Computers اجرا کنید.

۲. برروی واحد سازمانی Sales که اخیراً ایجاد کردید کلیک‌راست نموده و New « User را انتخاب کنید.



۳. فیلدهای First name، Last name و Logon name را برای کاربر وارد نموده و برروی Next کلیک کنید.

شکل ۶-۳۳

٤. در فیلدهای Password و Confirm Password، رمز عبوری را برای کاربر وارد نموده و مطمئن شوید که گزینه "User must change password at next logon" فعال است. این گزینه به کاربران امکان می‌دهد که پس از اولین ورود به حساب خود بتوانند رمز عبور را تغییر دهند.

- چنانچه حساب کابری توسط چندین کاربر مختلف استفاده می‌شود، گزینه "User cannot change password" را فعال کنید.
- در صورتی که که قصد ندارید رمز عبور تعیین شده هرگز منقضی شود، گزینه "Password never expires" را فعال کنید.
- چنانچه فعلاً قصد فعال‌سازی این حساب کابری را ندارید می‌توانید گزینه "Account is disabled" را فعال کنید.

۵. پس از انجام تنظیمات برروی Next کلیک کنید.

٦. در صفحه "Summary" خلاصه‌ای از تنظیمات انجام شده قابل مشاهده می‌باشد. برروی Finish

ایجاد حساب به کمک DSAdd (خط فرمان)

با استفاده از ابزار DSAdd در خط فرمان می‌توانید حساب‌ها را نیز ایجاد کنید. قالب کلی این دستور برای ایجاد حساب‌ها به صورت زیر می‌باشد:

```
DSAdd user <DN>
```

پس از اجرای این دستور حتما باید یک رمز عبور برای حساب تعیین کنید زیرا بدون آن امکان ایجاد حساب وجود ندارد. سایر اطلاعات مانند نام کاربری و ... اختیاری هستند و می‌توانید از وارد کردن آنها صرفنظر کنید.

دستور DSAdd user شامل پارمترهای بسیاری می‌باشد که در ادامه، تعدادی از این پارامترها آورده شده است:

- Pwd: Password
- Fn: First name
- Ln: Last name
- Display: Display name
- Samid: SAMID name
- Upn: User principal name

دستور زیر، کاربری به نام John Smith را به کانتینر Users اضافه می‌کند:

```
dsadd user "cn=John Smith,cn=users,dc=bigfirm,dc=com" -upn "John
Smith" -fn "john" -ln "Smith" -display "John Smith" -pwd "p@ss0000"
-disabled no
```

اگر این حساب را با استفاده از ADUC ایجاد می‌کردید، مقادیر فیلدها همانند تصویر زیر بود.

- فیلد Full name در ADUC همان Display name می‌باشد. زمانی که در حال ایجاد کاربر از طریق ADUC هستید، با وارد کردن First name و Last name این فیلد بطور خودکار تکمیل می‌شود ولی در DSAdd باید مقدار آن مشخص شده و یا خالی گذاشته شود.
- فیلد User logon name در ADUC با پارامتر upn در DSAdd مشخص می‌شود.
- پارامتر samid نام ورود موروثی را مشخص می‌کند و همانند مقدار تعیین شده در فیلد User logon name می‌باشد.

یکی از نکاتی که در حین ایجاد حساب کاربری باید رعایت شود، تغییر رمز عبور توسط کاربر پس از اولین ورود به حساب کاربری خود می‌باشد. در DSAdd این امکان با استفاده از پارامتر mustchpwd قابل اعمال است. زمانی که مقدار این پارامتر Yes باشد، کاربر باید رمز عبور خود را تغییر دهد.

اکنون برای ایجاد یک کاربر به نام Maria.Smith در واحد سازمانی Sales و با رمز عبور P@ssw0rd می‌توانید از دستور زیر استفاده کنید. دقت داشته باشید که کلیه این پارامترها باید به صورت یک دستور و دنباله همدیگر نوشته شوند و فاصله‌ها و علائم در آن رعایت گردند.

۶-۴-۳ ایجاد گروه‌ها

مهمترین دلیل استفاده از گروه‌ها، سازماندهی کاربران در آنها می‌باشد. این سازماندهی به منظور اعمال مجوزها برروی کاربران این گروه‌ها می‌باشد. به عنوان مثال چنانچه قرار باشد برروی کاربران یک بخش (مثل بخش فروش) مجوزهایی اعمال شود، به جای تک تک کاربران می‌توان یک گروه با نام (مثلاً) G_Sales ایجاد نموده و این کاربران را در آن قرار داد، سپس مجوزهای لازم را برروی گروه اعمال نمود. اکنون اگر هر کاربر جدیدی به گروه اضافه شود، این مجوزها برروی آن اعمال خواهد شد.

دو نوع کلی برای گروه‌ها وجود دارد: Distribution (توزیع) و Security (امنیت). گروه‌های نوع Distribution برای ایمیل، و گروه‌های Security برای اعمال مجوزها و همچنین ایمیل استفاده می‌شوند.

گروه‌ها علاوه بر نوع، دارای ناحیه[1] نیز می‌باشند. این نواحی به سه دسته تقسیم می‌شوند:

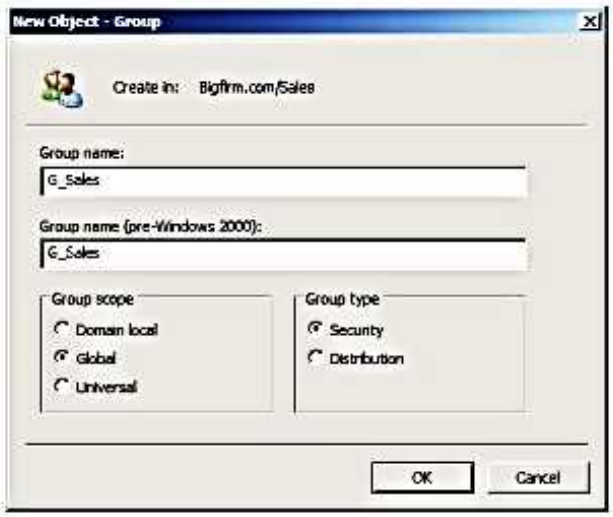
- **Global**: متداول‌ترین نوع از گروه‌ها هستند که به منظور سازماندهی کاربران استفاده می‌شوند. می‌توان کاربران را در این گروه‌ها قرار داده و مجوزهای لازم را برروی گروه اعمال نمود.

1. Scope

- **Domain Local**: در بعضی از دامنه‌ها، این گروه‌ها با استفاده از استراتژی "A G DL P" استفاده می‌شوند که در آن، A بیانگر حساب کاربری (Account)، G بیانگر Global group، DL بیانگر گروه‌های Domain Local، و P نیز بیانگر مجوز (Permissin) می‌باشد. در واقع این شیوه بیان می‌کند که حساب‌های کاربری در گروه‌های Global و خود این گروه‌ها در گروه‌های Domain Local قرار دارند و مجوزها نیز برروی گروه‌های Domain Local اعمال می‌شوند.
- **Universal**: این گروه‌ها فقط در محیط‌های چند دامنه‌ای استفاده می‌شوند.

رایجترین روش ایجاد هر یک از گروه‌های بالا استفاده از ADUC می‌باشد. مراحل زیر، نحوه ایجاد گروهی از نوع global security را نشان می‌دهند. در اینجا فرض بر این است که قبلاً یک واحد سازمانی با نام Sales در دامنه ایجاد شده است:

۱. ADUC را اجرا کنید.
۲. برروی واحد سازمانی Sales کلیک‌راست نموده و New » Group را انتخاب کنید.
۳. در فیلد "Group name" نام G_Sales را وارد نموده و برروی OK کلیک کنید.



شکل ۶-۳۶

٤. مجدداً برروی واحد سازمانی Sales کلیک‌راست نموده و New » Group را انتخاب کنید. این بار نام G_SalesAdmins را وارد نموده و برروی OK کلیک کنید. با استفاده از این گروه می‌توانید مجوزهای لازم را به مدیر واحد سازمانی OU بدهید.

واگذاری[1] کنترل

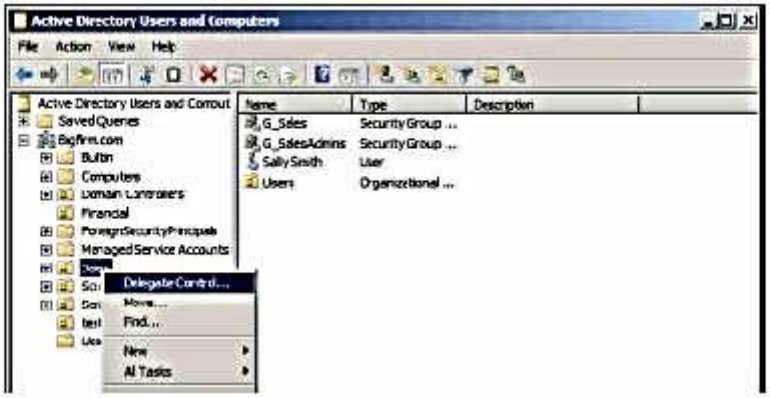
یکی از دلایل ایجاد OUها واگذاری کنترل تعدادی از کاربران به فرد (یا افرادی) می‌باشد. به عنوان مثال فرض کنید که کلیه اقدامات مدیریت IT در بخش فروش به دو کاربر واگذار شده است. این دو

1. Delegating

کاربر باید قادر باشند کلیه اقدامات را برای هر کاربر در بخش فروش انجام دهند ولی قادر به انجام اقدامات مدیریتی برای سایر کاربران در دامنه نباشند.

برای انجام این کار باید ابتدا یک واحد سازمانی با نام Sales ایجاد نموده و تمام کاربران و کامپیوترهای بخش فروش را در آن قرار دهید. همچنین باید یک گروه Global (مثلاً G_SalesAdmins) ایجاد نموده و حساب کاربری مدیر IT بخش فروش را در آن قرار دهید. پس از انجام این اقدامات می‌توانید مراحل زیر را برای دادن مجوز به این گروهِ Global (که حساب‌های کاربری مدیران IT در آن قرار دارد) با استفاده از ویزاردی به نام "Delegation of Control Wizard" دنبال کنید:

۱. Active Directory Users and Computers را اجرا کنید.
۲. برروی واحد سازمانی Sales کلیک‌راست نموده و گزینه Delegate Control را انتخاب کنید.

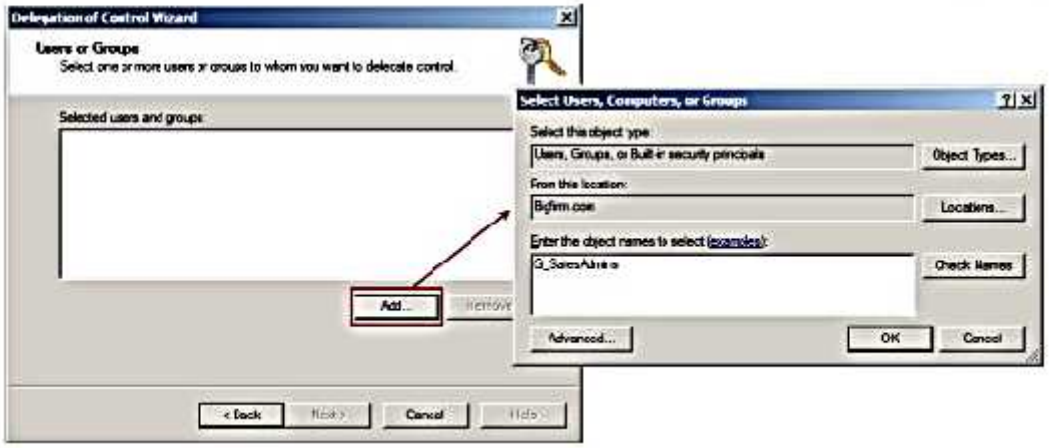


شکل ۶-۳۷

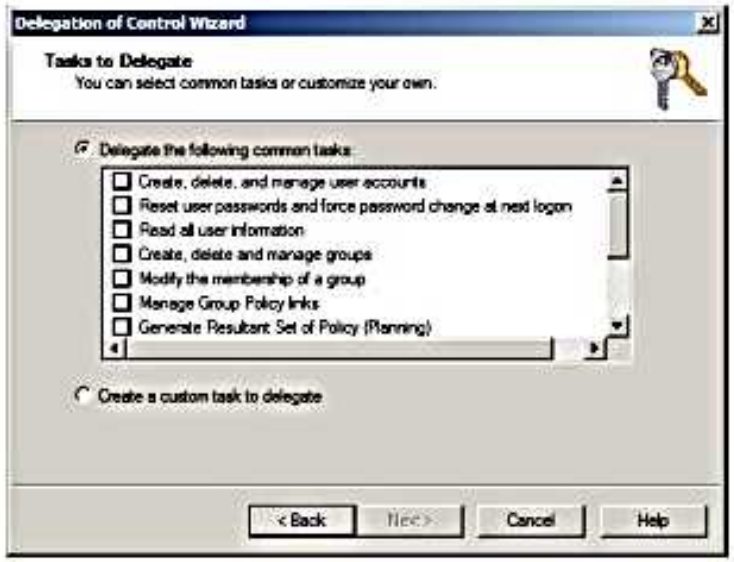
۳. در صفحه "Welcom to the Delegation of Control Wizard" برروی Next کلیک کنید.

٤. در صفحه "Users or Groups" برروی دکمه Add کلیک کنید.

٥. در قسمت "Enter the object names to select" نام G_SalesAdmins را وارد نموده و برروی OK کلیک کنید.

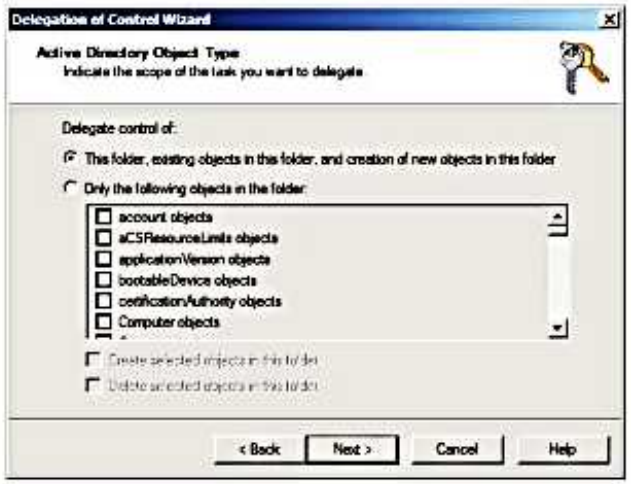


۶. برروی Next کلیک کنید تا به صفحه "Tasks to Delegate" هدایت شوید. در این صفحه دو گزینه قابل انتخاب است. با انتخاب گزینه اول (Delegate the following common tasks) می‌توانید به لیستی از مجوزهای قابل اعمال برروی گروه دسترسی پیدا کنید. با فعال کردن هر مجوز می‌توانید آنرا برای اختصاص دادن انتخاب کنید.



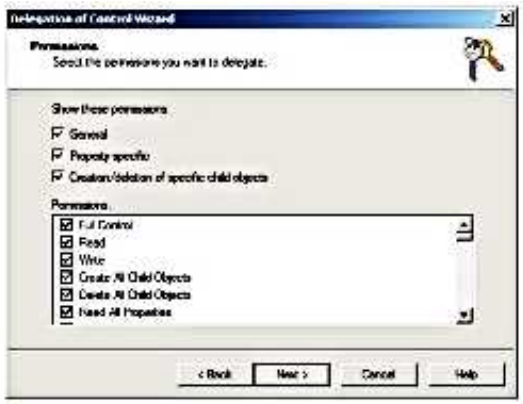
۷. گزینه دوم (Create a custom task to delegate) زمانی استفاده می‌شود که بخواهید مجوز انجام هر کاری را به مدیران بدهید. بنابراین در اینجا گزینه دوم را انتخاب نموده و برروی Next کلیک کنید.

۸. در صفحه "Active Directory Object Type" نیز تعدادی گزینه وجود دارد. با استفاده از این گزینه‌ها می‌توانید مجوزها را به اشیاء خاصی مثل کاربران، کامپیوترها و ... محدود کنید. گزینه This folder, existing objects in this folder ... را انتخاب نموده و برروی Next کلیک کنید.



شکل ۶-۴۰

۹. در صفحه "Permissions" مجوز Full Controll را در قسمت Permissions انتخاب نموده و سپس برروی Next کلیک کنید.

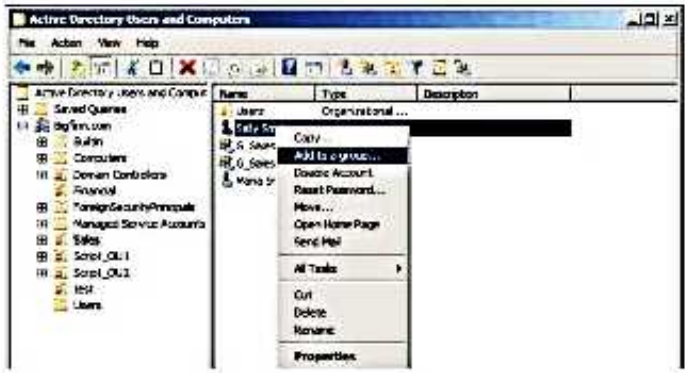


شکل ۶-۴۱

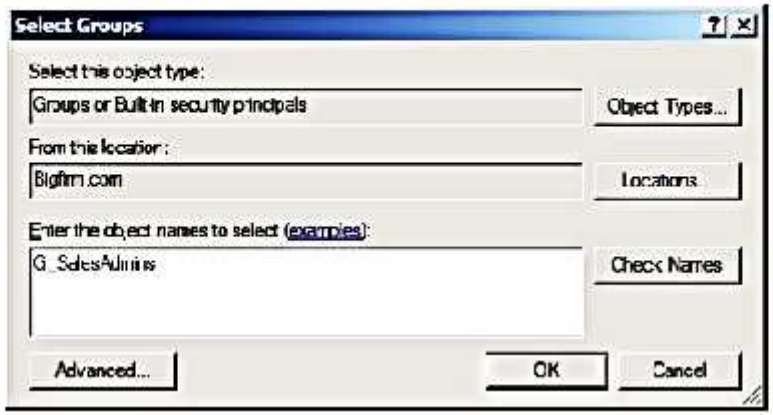
۱۰. در صفحه "Completing the Delegation"، خلاصه‌ای از تنظیمات را مشاهده نموده و برروی Finish کلیک کنید.

اکنون پس از ایجاد گروه لازم است که کاربران را به آن اضافه کنید. جهت افزودن کاربران به گروهی که اخیراً ایجاد نمودید مراحل زیر را دنبال کنید:

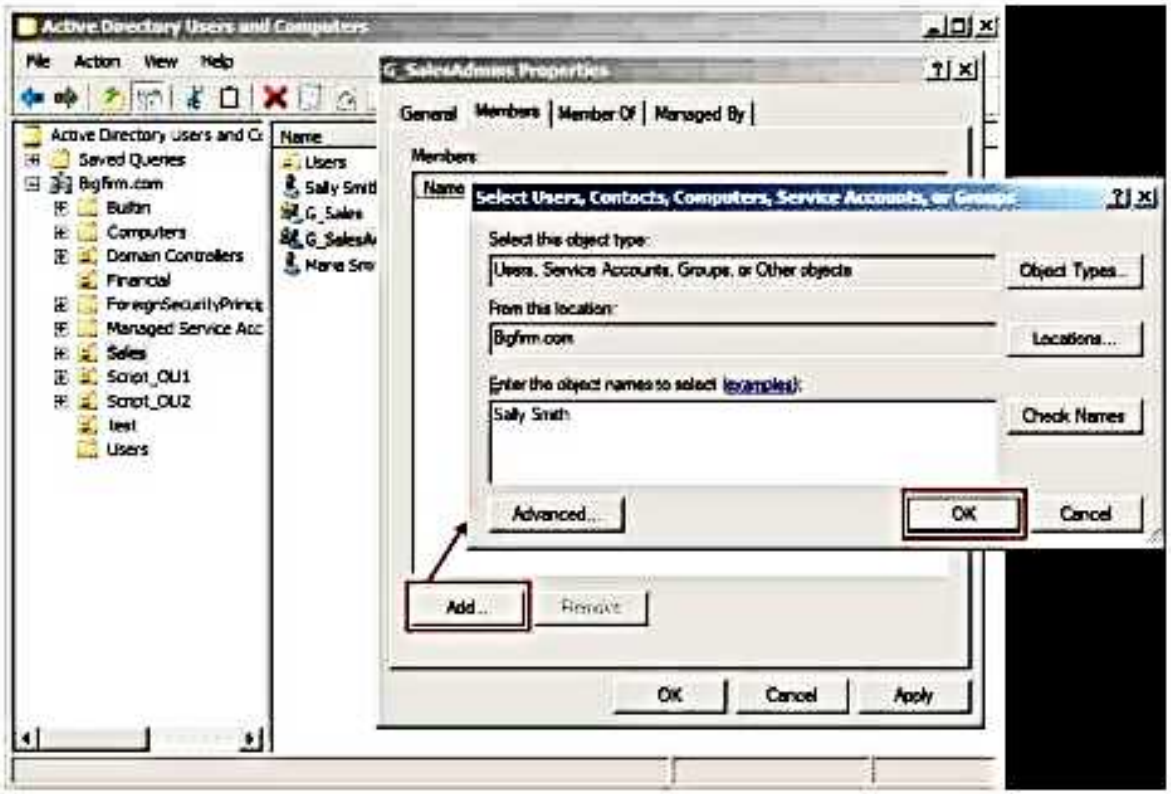
۱۱. در کنسول ADUC برروی کاربر کلیک‌راست نموده و گزینه Add to a group را انتخاب کنید.



۱۲. در صفحه "Select Groups" نام گروه را وارد نموده و برروی OK کلیک کنید.



افزودن کاربر به گروه از طریق تب Members در Properties گروه نیز امکان‌پذیر می‌باشد. در این تب باید پس از کلیک برروی Add، نام کاربر را وارد نموده و برروی OK کلیک کنید.



۶-۵ اقدامات نگهداری از دامنه

پس از راه‌اندازی یک دامنه لازم است با تعدادی اقدام جهت نگهداری از آن آشنا شوید. در این قسمت اقدامات پایه در این رابطه را مورد بحث قرار می‌دهیم. این اقدامات عبارتند از:

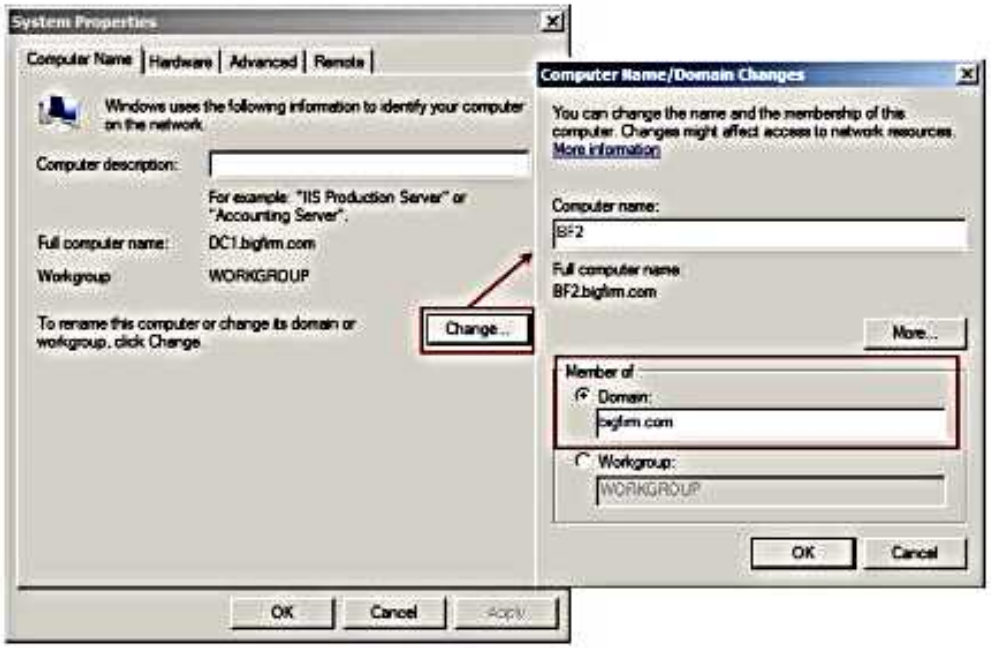
- پیوستن به یک دامنه
- انهدام یک DC
- عیب‌یابی ADI DNS
- افزایش سطح عملکرد دامنه و جنگل
- استفاده از NetDom

در ادامه، هریک از این اقدامات را مورد بررسی قرار خواهیم داد.

۶-۵-۱ پیوستن به یک دامنه

برای اتصال ویندوز سرور 2008R2 به یک دامنه، مراحل زیر را دنبال کنید (دقت داشته باشید زمانی که یک سرور به دامنه متصل می‌شود، از آن لحظه به بعد با مفهوم Member Server شناخته می‌شود):

۱. وارد سرور مورد نظر شوید.
۲. از منوی Start، برروی Computer کلیک‌راست نموده و Properties را انتخاب کنید.
۳. برروی Change Settings (یا Advanced System Settings) کلیک کنید.
٤. در پنجره "System Properties" تب Computer Name را انتخاب نموده و برررروی دکمه Change کلیک کنید.
٥. در قسمت Member of، گزینه Domain را انتخاب نموده و نام دامنه‌ای که قصد دارید به آن متصل شوید (در اینجا bigfirm.com) را وارد کنید.



۶. از شما مشخصات کاربری که دارای مجوز (مدیر) برای دسترسی به دامنه (bigfirm.com) است درخواست می‌شود. نام کاربری و رمز عبور را وارد نموده و برروی OK کلیک کنید.

شکل ۶-۴۶

۷. پس از مدت کوتاهی، پنجره خوشامدگویی نشان داده می‌شود. برروی OK کلیک کنید.

۸. از شما خواسته می‌شود که کامپیوتر را Restart کنید. مجدداً برروی OK کلیک کنید.

۹. برروی Close کلیک نموده و پنجره "System Properties" را ببندید. بار دیگر به شما اعلام می‌شود

که سرور باید Restart شود. برروی Restart Now کلیک کنید. پس از Restart، سرور به دامنه مورد نظر متصل شده و به عنوان یک Member Server شناخته می‌شود.

۶-۵-۲ انهدام یک DC

گاهی اوقات نیاز است که یکی از DCها را از حالت سرویس‌دهی خارج نمود. به این عمل "انهدام[1]" گفته می‌شود. زمانی‌که یک DC را منهدم می‌کنید، کلیه اجزاء اکتیو دایرکتوری در آن را حذف نموده و آنرا به یک Member Server تبدیل می‌کنید.

ساده‌ترین راه برای انهدام یک DC، راه‌اندازی DCPromo برروی آن می‌باشد. البته پس از انهدام، سرور هنوز قادر به اجرا است ولی عملکردهای مورد انتظار (از یک DC) را نخواهد داشت.

چنانچه به دلیل شکست سرور DC نتوان DCPromo را برای حذف آن اجرا نمود، می‌توانید از طریق اکتیو دایرکتوری آنرا حذف کنید. با استفاده از ابزار Active Directory Users and Computers به سادگی می‌توان عمل حذف یک DC را انجام داد. برای انجام این کار مراحل زیر را دنبال کنید:

۱. ADUC را اجرا نموده و از پنل سمت چپ، برروی Domain Controllers کلیک کنید.
۲. در پنل سمت راست، برروی DC مورد نظر کلیک‌راست نموده و Delete را انتخاب کنید.

شکل ۶-۴۷

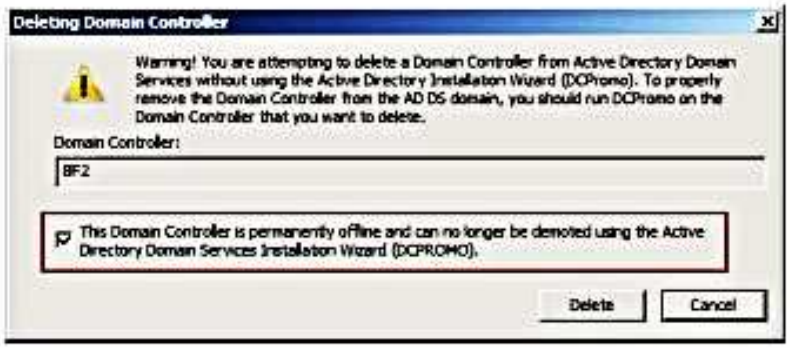
۳. مطمئن شوید که DC را درست انتخاب نموده‌اید، سپس برروی Yes کلیک کنید.

شکل ۶-۴۸

٤. پیغامی ظاهر شده و اعلام می‌کند که شما در حال حذف کردن یک DC از اکتیو دایرکتوری بدون

1. Decommissioning

اجـرای DCPromo هسـتید. ایـن پیغـام توصـیه مـی‌کنـد کـه از DCPromo اسـتفاده کنیـد. گزینـه This Domain Controller is permanently offline and... را فعال نموده و برروی Delete کلیک کنید.



شکل ۶-۴۹

۵. اگر DC یک Global Catalog Server است، هشداری در مورد ادامه مراحل ظاهر مـی‌شـود. بـرروی Yes کلیک کنید.

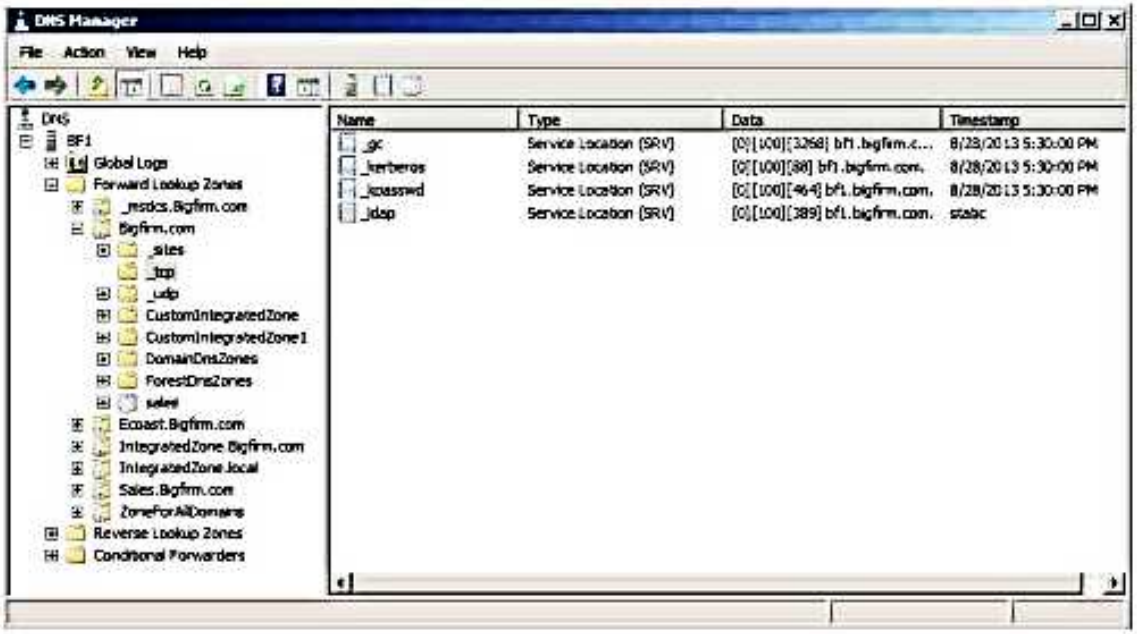
٦. اگر برروی سرور، اقدامات اصلی (Operations Master Roles) نگهداری می‌شوند از شـما خواسـته می‌شود که آنها را به DC دیگری انتقال دهید. برروی OK کلیک کنید. پـس از آن عملکـرد ایـن DC متوقف خواهد شد.

اگر بعداً DC ناموفق به حالت اجرا بازگردد، نمی‌توانید به صورت عادی از DCPromo برای حذف اکتیو دایرکتوری در آن استفاده کنید. بنابراین باید بجای عبارت DCPromo در خط فرمان، از عبارت DCPromo /forceremoval استفاده کنید. پارامتر /forceremoval باعث می‌شود که اکتیو دایرکتوری بدون نیاز به دسترسی به سایر DCها در دامنه حذف گردد.

۶-۵-۳ عیب‌یابی ADI DNS

یکی از مشکلات رایجی که در DNS رخ می‌دهد، عدم ایجاد رکوردهای SRV در حین اجرای (Reboot) سرور DNS می‌باشد. ایجاد این رکوردها برعهده سرویس Netlogon می‌باشد و زمانی که این سرویس با وقفه روبرو شود، ایجاد رکوردها و در نتیجه اجرای DNS نیز با مشکل مواجه می‌شوند. همانطور که قبلاً شرح دادیم، رکوردهای SRV برای تشخیص موقعیت DCها و همچنین انواع سرویس‌ها برروی دامنه مورد استفاده قرار می‌گیرند. سرویس‌های ارائه شده توسط DC و یا سایر سرویس‌ها با استفاده از رکوردهای SRV در DNS موقعیت سرورها را تشخیص داده و در صورت وجود داشتن، از آنها استفاده می‌کنند.

در شکل زیر، کنسول DNS Manager زمانی که رکوردهای SRV در آن ایجاد شده‌اند نشان داده شده است. توجه داشته باشید که نام تعدادی پوشه با نماد " _ " آغاز شده است (_msdcs ، _sites ، _tcp و _udp). این پوشه‌ها حاوی رکوردهای SRV می‌باشند.



شکل ۶-۵۰

چنانچه در حین اتصال به DNS با مشکل مواجه شدید و رکوردهای SRV در پوشه‌های مورد نظر وجود نداشتند، به سادگی می‌توان این مشکل را برطرف نمود. به خط فرمان (Cmd) بروید و از دو دستور زیر استفاده کنید.

```
Net stop netlogon
Net start netlogon
```

۶-۵-۴ افزایش سطح عملکرد دامنه و جنگل

پس از ایجاد جنگل (Forest) ممکن است بخواهید سطح دامنه و یا جنگل را افزایش دهید. مهمترین دلیل انجام این کار استفاده از قابلیت‌ها و ویژگی‌های سطوح بالاتر می‌باشد. دقت داشته باشید زمانی که سطح عملکرد را افزایش می‌دهید امکان بازگرداندن آن وجود ندارد. به عنوان مثال اگر سطح عملکرد دامنه را از Windows Server 2003 به Windows Server 2008 R2 افزایش دهید دیگر نمی‌توانید هیچ سروری که دارای سیستم عامل قبل از Windows Server 2008 R2 است را به DC تبدیل کنید. بنابراین اگر مطمئن هستید که تغییری در برنامه شما رخ نمی‌دهد این کار را انجام دهید.

دو ابزاری که به منظور افزایش سطح عملکرد دامنه و جنگل استفاده می‌شوند عبارتند از:

- Active Directory Users and Computers (برای افزایش سطح عملکرد دامنه)
- Active Directory Domains and Trusts (برای افزایش سطح عملکرد جنگل)

۶-۶ ایجاد سیاست‌های دانه ریز رمز عبور[1]

تا قبل از ویندوز سرور 2008 اگر شما به بیش از یک Password Policy در سازمان نیاز داشتید، باید یک دامنه جداگانه برای آن ایجاد می‌کردید. این مسئله یک چالش بزرگ برای سازمان‌ها محسوب می‌شد. به ویندوز سرور 2008 این مشکل نیز برطرف گردیده و امکان داشتن چندین Password Policy برروی یک دامنه فراهم شده است.

با استفاده از سیاست‌های دانه ریز رمز عبور امکان اختصاص سیاست‌های مشخصی برای تک تک

1. Fine-Grained Password Policies

کاربران یا گروه‌ها فراهم شده است. با استفاده از این سیاست‌ها می‌توانید مشخص کنید که رمز عبورها شامل موارد زیر باشند:

- تاریخچه رمزعبور
- حداکثر عمر رمز عبور
- حداقل عمر رمز عبور
- حداقل طول رمز عبور
- نیاز به پیچیدگی در رمز عبور
- ذخیره کردن رمزهای عبور با استفاده از رمزگذاری بازگشتی

این موارد به مفهوم "دانه ریز" اشاره دارند زیرا شما می‌توانید آنها را در پایین‌ترین سطح (همانند دانه‌های شن و ماسه) اختصاص دهید. اگر شما حتی یک کاربر داشته باشید که رمز عبور آن باید از سیاست خاصی پیروی کند می‌توانید آنرا برروی کاربر اعمال کنید. البته معولاً سیاست‌ها بجای یک کاربر، برروی گروهی از کاربران اعمال می‌شوند.

پیاده‌سازی Password Policyها از طریق موارد زیر امکان‌پذیر می‌باشد:

- ایجاد "شیء تنظیمات رمز عبور[1]" (PSO) و ذخیره آن در "کانتینر تنظیمات رمز عبور[2]" (PSC)
- اعمال PSO برروی کاربر یا گروه Global Security

۶-۶-۱ نیازمندی‌های سیاست‌های دانه ریز رمز عبور

قبل از اقدام به پیاده‌سازی سیاست‌های دانه ریز رمز عبور باید مطمئن شوید که محیط مورد نظر از این سیاست‌ها پشتیبانی می‌کند، بنابراین حداقل سطح عملکرد دامنه باید Windows Server 2008 باشد. همچنین برای ایجاد PSO باید دارای حساب کاربری با مجوز مدیر دامنه باشید (زیرا تنها مدیران قادر به ایجاد PSOها هستند).

۶-۶-۲ ایجاد PSO

برای ایجاد PSO می‌توانید از ابزار ADSI Edit که در مسیر «Start» Administrative Tools قرار دارد استفاده کنید. زمانی که برای اولین بار PSO را ایجاد می‌کنید لازم است تنظیمات آن را مورد تغییر قرار دهید. تعدادی از این تنظیمات عبارتند از:

- **msDS-PSOAppliesTo**: این مشخصه تعیین کننده نوع شیئی است که PSO برروی آن اعمال می‌شود. ورودی‌های این مقدار نام‌های DN مربوط به کاربران یا گروه‌ها می‌باشد.
- **msDS-MinimumPasswordLength**: این مشخصه تعیین کننده حداقل طول رمز عبور برای

1. Password Settings Object
2. Password Settings Container

حساب‌های کاربری است که از این PSO استفاده می‌کنند. هر مقداری بین ۰ تا ۲۵۵ برای این مشخصه معتبر است.

- **msDS-MinimumPasswordAge**: حداقل عمر رمز عبور برای حساب‌های کاربری را مشخص نموده و هر مقداری از 00:00:00:00 تا مقدار مشخصه msDS-MaximumPasswordAge می‌تواند برای آن مورد استفاده قرار گیرد.
- **msDS-MaximumPasswordAge**: حداکثر عمر رمز عبور برای حساب‌های کاربری را مشخص نموده و تعیین می‌کند که رمز عبور چه زمانی باید تغییر کند. هر مقداری بین msDS-MinimumPasswordAge تا Never قابل انتخاب می‌باشد. به عنوان مثال برای اطمینان از اینکه کاربران هر ۱۵ روز رمز عبور خود را تغییر می‌دهند، می‌توانید از مقدار 15:00:00:00 استفاده کنید. مشخصه msDS-MaximumPasswordAge نمی‌تواند با صفر مقداردهی شود.

فرمت مدت زمان عمر رمز عبور به صورت d:hh:mm:ss می‌باشد که در آن، d بیانگر تعداد روزها، h بیانگر تعداد ساعات، m بیانگر تعداد دقیقه‌ها و s بیانگر تعداد ثانیه‌ها می‌باشد. به عنوان مثال مقدار 1:05:30:45 بیانگر مدت عمر یک روز و ۵ ساعت و ۳۰ دقیقه و ۴۵ ثانیه می‌باشد.

- **msDS-PasswordHistoryLength**: این مقدار تعیین کننده تعداد رمز عبورهایی است که باید تغییر کنند تا یک رمز عبور بتواند مجدداً تکرار شود.
- **msDS-PasswordComplexityEnabled**: وضعیت فعال بودن پیچیدگی برای انتخاب رمز عبور را مشخص نموده و اطمینان می‌دهد که رمز عبور کاربران حداقل نیازهای پیچیدگی را رعایت می‌کنند (مثلا اینکه ترکیبی از حروف، اعداد و کاراکترهای خاصی چون @ ... باشند). این مقدار می‌تواند True (فعال) و False (غیرفعال) باشد.
- **msDS-PasswordSettingsPrecedence**: اولویت PSOها را زمانی که چندین شیء PSO برروی کاربر اعمال شده باشد مشخص می‌کند و کمترین مقدار در این قسمت بیانگر بالاترین اولویت است. به عنوان مثال یک PSO با اولویت ۱۰ می‌تواند بجای PSO با اولویت ۲۰ اعمال شود. در این قسمت هر عدد بزرگتر از صفر معتبر است.
- **msDS-PasswordReversibleEncryptionEnabled**: وضعیت کدگذاری بازگشتی برای رمزهای عبور را مشخص نموده و می‌تواند با یکی از مقادیر True یا False مقداردهی شود.
- **msDS-LockoutThreshold**: تعیین کننده تعداد دفعاتی است که یک کاربر سعی می‌کند با وارد نمودن رمز عبور به حساب کاربری خود وارد شود. پس از تعداد مشخص شده در این قسمت، چنانچه رمز عبور صحیحی وارد نشود آن حساب قفل می‌شود. این مقدار می‌تواند بین ۰ تا

۶۵۵۳۵ باشد.

- **msDS-LockoutObservationWindow:** این مشخصه تعیین می‌کند که زمان لازم برای بازگردانی تعداد دفعات وارد نمودن رمز عبور به ۰ چقدر باشد. به عنوان مثال فرض کنید که آستانه ورود رمز عبور ۳ بار باشد. یک کاربر زمانی که ۲ بار رمز عبور را وارد کند، تنها یکبار دیگر برای وارد کردن رمز عبور صحیح فرصت دارد. اکنون چنانچه مقدار LockoutObservationWindow با 0:00:30:00 (۳۰ دقیقه) تنظیم شده باشد، کاربر پس از ۲ بار وارد کردن رمز عبور می‌تواند به مدت ۳۰ دقیقه صبر نموده تا شمارنده به صفر بازگردد. پس از آن مجدداً سه فرصت برای ورود رمز عبور برای آن کاربر فراهم می‌گردد. مقادیر مجاز برای این مشخصه، از 00:00:00:01 تا مقدار msDS-LockoutDuration می‌باشند.
- **msDS-LockoutDuration:** این مشخصه تعیین می‌کند که حساب یک کاربر در اثر وارد کردن رمز عبورهای اشتباه (بیش از تعداد دفعات مجاز) چه مدت بسته باشد. یا به عبارت دیگر، کاربر چه مدتی باید برای وارد کردن مجدد رمز عبور منتظر بماند.