فصل دوازدهم

نصب و راه اندازی Active Directory

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- Domain و اجزای Active Directory را تعریف کند.
- Active Directory را نصب کند.
- نحوهٔ عضویت سرویس گیرنده‌ها و انواع Log on ها را شرح دهد.

۱ـ۱۲ـ آشنایی با Active Directory Domain Services یا AD DS

همان‌طور که در فصل اول اشاره شد در شبکه دو مدل سرویس‌دهی وجود دارد : نظیر به نظیر (Workgroup) و مبتنی بر سرور. در مدل سرویس دهی نظیر به نظیر (Workgroup) که یک مدل ساده محسوب می‌شود، مدیر مرکزی وجود ندارد و هر کاربر مدیر رایانه خودش می‌باشد. در چنین مدلی اگر لازم باشد یک سیاست[۱] امنیتی یا مدیریتی برای رایانه‌ها یا کاربران شبکه تعیین شود، باید به صورت جداگانه در تک تک رایانه‌ها تنظیمات مربوطه انجام گیرد. اما در صورت نصب سیستم عامل سروری (مانند ویندوز ۲۰۰۸ سرور) و راه اندازی Domain، این امکان وجود دارد که بتوان تمامی رایانه‌ها یا کاربران با منابع موجود در شبکه را به صورت متمرکز مدیریت نمود یا اینکه یک سیاست امنیتی یا مدیریتی را بر روی تمام رایانه‌های موجود در شبکه اعمال کرد.

باید توجه داشت که Domain را فقط در یک سیستم عامل سروری می‌توان راه‌اندازی نمود که در این کتاب از سیستم عامل ویندوز ۲۰۰۸ سرور ویرایش مؤسسات[۲] استفاده خواهد شد.

برای راه اندازی Domain باید سرویس Active Directory را در یک سرویس‌دهنده Stand ــ alone نصب کنید (وقتی که شما ویندوز ۲۰۰۸ سرور نصب می‌کنید و رایانه شما عضو

---

۱ ــ Policy

۲ــ Windows Server 2008 Enterprise

Workgroup می‌باشد (حالت پیش فرض نصب) رایانه شما یک سرویس دهنده Stand ــ alone می‌باشد). توجه داشته باشید که بعد از نصب Active Directory سرویس دهنده به یک کنترل‌کننده دامنه Domain Controller تبدیل می‌شود که اصطلاحاً به آن DC می‌گویند.

۲ــ۱۲ــ اجزای Active Directory

وقتی که شما می‌خواهید یک تماس تلفنی برقرار نمایید، شماره مورد نظر را از دفترچه تلفن پیدا می‌کنید؛ یا وقتی که در یک ساختمان اداری بزرگ به دنبال اتاق خاصی می‌گردید، به راهنمای طبقات مراجعه می‌کنید و یا در کتابخانه در هنگام جستجوی یک کتاب خاص، به فهرست منابع مراجعه می‌کنید. دفترچه تلفن، راهنمای طبقات و فهرست منابع یک نوع دایرکتوری(Directory) محسوب می‌شوند.

دایرکتوری‌های شبکه، اطلاعاتی درباره منابع موجود روی شبکه مانند کاربران، رایانه‌ها، چاپگرها، پوشه‌های به اشتراک گذاشته شده را نگهداری می‌کنند. دایرکتوری‌ها بخش اساسی هر سیستم عامل سروری می‌باشند. در سیستم عامل‌های قدیمی به ازای هربخش، یک دایرکتوری مجزا وجود داشت. در سیستم عامل‌های جدید یک دایرکتوری به نام Active Directory تمام اطلاعات را نگهداری می‌کند که در ویندوز ۲۰۰۸ سرور به Active Directory Domain Service یا AD DS تغییر نام پیدا کرده است (لازم به ذکر است در ویندوز ۲۰۰۰ و ۲۰۰۳ سرور، سرویس دایرکتوری به Active Directory یا AD مشهور بود).

بعد از نصب AD DS رایانه شما به یک DC یا Domain Controller تبدیل می‌شود. DC اطلاعات امنیتی و بانک اطلاعاتی اشیای دایرکتوری را نگهداری می‌کند و وظیفه آن احراز هویت[۱] در Domain می‌باشد، یعنی زمانی که کاربر می‌خواهد از روی سرویس گیرنده به Domain وارد شود، نام و گذر واژه[۲] کاربر به صورت کد شده به DC ارسال می‌شود. DC که اطلاعات تمام کاربران Domain را دارد، اطلاعات دریافتی را با اطلاعات خود مقایسه می‌کند، در صورتی که اطلاعات درست باشد صحت اطلاعات کاربر را به سرویس‌گیرنده اطلاع می‌دهد، به‌طوری که از آن به بعد، کاربر می‌تواند برای دسترسی به تمامی‌منابع موجود در Domain دسترسی داشته باشد.

۱ــ Authentication

۲ــ Password

۳ـ۱۲ـ مراحل نصب AD DS در ویندوز ۲۰۰۸ سرور

عملیاتی را که باید قبل از شروع به نصب AD DS انجام داد عبارت‌اند از :

ـ **تنظیم کارت شبکه[1] برای دادن IP استاتیک** : از دو روش می‌توان به تنظیمات IP دسترسی پیدا نمود :

الف) با استفاده از فرمان ncpa.cpl (اجرای فرمان از طریق کادر Run)

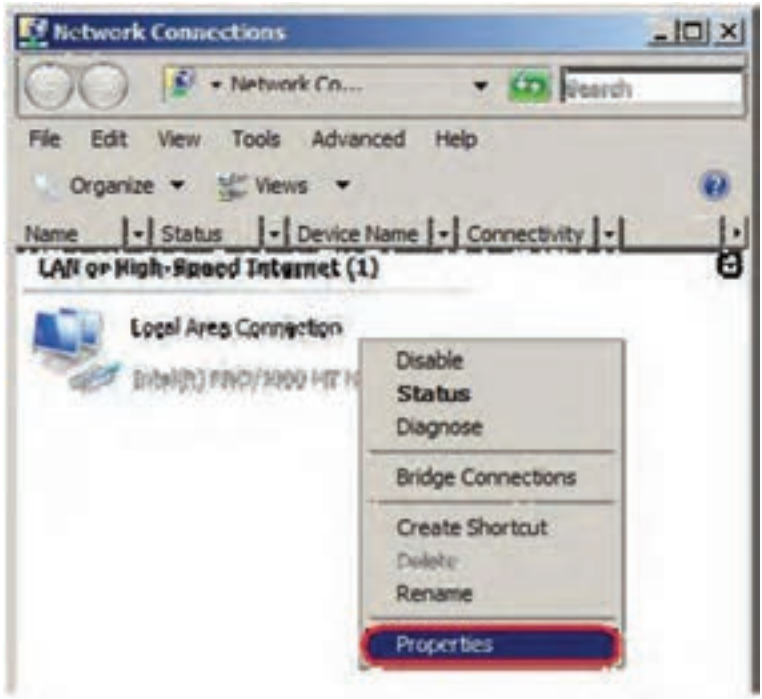
Start →Run → ncpa.cpl

ب) از Control Panel برنامه Network and Sharing اجرا کنید، سپس گزینه Manage network connections را انتخاب نمایید.

شکل ۱ـ۱۲

با اجرای هر کدام از دو روش قبلی پنجره Network Connections ظاهر می‌گردد. حال بر روی Local Area Connection کلیک راست نموده و سپس گزینه Properties را انتخاب نمایید.

۱ـ امروزه تمام مادربردها دارای کارت شبکه Onboard می‌باشند. در صورتی که سیستم شما مجهز به کارت شبکه نبود با استفاده از گزینه Add hardware در Control Panel یک کارت شبکه مجازی نصب کنید. ضمناً لازم است کارت شبکه رایانه مورد نظر به شبکه هم متصل باشد.

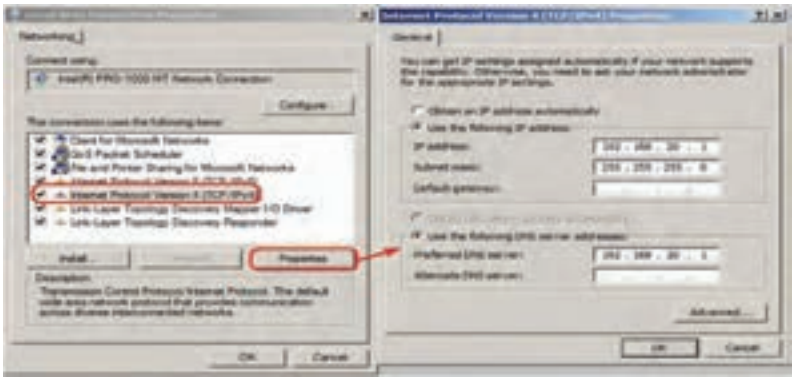


شکل ۲ــ۱۲

لازم به یادآوری است که برای سرورهای زیر ساخت[۱] در شبکه مانند DC، DNS،DHCP باید IP کارت شبکه را به‌صورت استاتیک (دستی) تنظیم نمایید. بنابراین اولین قدم در نصب AD DS تنظیم کردن IP کارت شبکه به صورت استاتیک می‌باشد.

در ادامه در کادر Local Area Connection Properties (شکل ۳ــ۱۲) ابتدا گزینه Internet Protocol version 4 (TCP/IPv4) را انتخاب نموده و بر روی دکمه Properties کلیک نمایید تا کادر Internet Protocol version 4 (TCP/IPv4) Properties برای تنظیمات IP ظاهر گردد.

۱ــ Infrastructure servers



شکل ۳ــ۱۲

گزینه Use the fallowing IP Address : را برای تنظیم IP استاتیک انتخاب نمایید و در آدرس 192.168.20.1 (کلاس C) را در کادر IP Address وارد نمایید. Subnet Mask به طورخودکار به 255.255.255.0 تبدیل می‌شود.

نکته ۱: به ازای کلاس‌های مختلف IPv4 مقدار Subnet Mask مطابق با جدول ۱ــ۱۲ تغییر خواهد کرد. عدد 255 به معنی ثابت بودن عدد Network در IPv4 می‌باشد.

جدول ۱ــ۱۲ــ مقدار subnet mask به ازای کلاس‌های مختلف IPV4

Class IPv4	A	B	C
Subnet Mask	255.0.0.0	255.255.0.0	255.255.255.0

AD برای فعالیت به DNS نیاز دارد. باید توجه داشت که DNS را هم می‌توان از قبل نصب نمود و هم این که درحین نصب AD، آن را برای نصب فعال کرد (که به نصب همزمان AD DS با DNS Server اصطلاحاً Integrated یا مجتمع می‌گویند) پس می‌توان Preferred DNS Server را هم به صورت 192.168.20.1 را وارد کنید.

نکته ۱: اگر DNS سرور شما به‌طور جداگانه روی سرور دیگری در شبکه پیاده‌سازی شده باشد باید آدرس IP آن سرور را در DNS server قرار دهید.

توصیه می‌شود نام رایانه را نیز تغییر دهید، برای این کار بر روی My Computer کلیک راست نموده و گزینه Properties را انتخاب نمایید و در زبانه Computer Name دکمه Change را برای تغییر نام رایانه، به نام دلخواه (مثلاً Server۱) انتخاب نمایید، توجه داشته باشید که بعد از تغییر نام، باید سیستم را مجدداً راه اندازی (Restart) کنید.

نکته ۳: باید کاربر مدیر (Administrator) حتماً دارای کلمه عبور باشد،یعنی کلمه عبور کاربر مدیر(administrator) نمی‌تواند تعریف نشده باشد و با زدن کلید enter به جای کلمه عبور وارد شود.

۴ـ۱۲ـ مراحل اصلی نصب AD DS

به دو روش می‌توان AD DS را نصب نمود :

الف) با استفاده از فرمان dcpromo

ب) با استفاده از ویزارد نصب

مراحل نصب AD DS با استفاده از ویزارد نصب به صورت زیر می‌باشد :

۱ـ از مسیر زیر برنامه Server Manager را اجرا کنید.

Start → Administrative Tools → Server Manger

۲ـ در برنامه Server Manger روی Roles کلیک کنید، سپس بر روی Add Roles کلیک نمایید. تا Roleهای قابل نصب نمایش داده شوند، همان طور که مشاهده می‌کنید ۵ نقش (Role) در ارتباط با AD وجود دارد. حال گزینه Active Directory Domain services را در کادر Se lec t Server Roles انتخاب نمایید و سپس بر روی Next کلیک کنید.

شکل ۴ـ۱۲

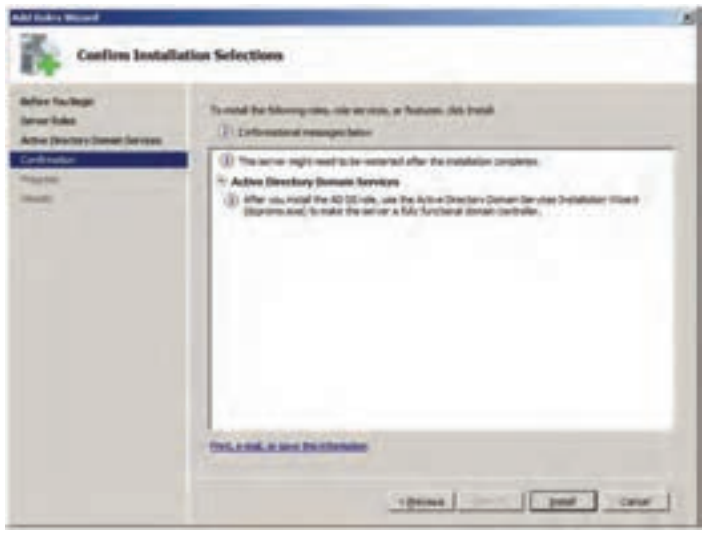
نکته : با استفاده از گزینه Add Role از منوی Action هم می‌توان به پنجره Select Server Roles دسترسی پیدا نمود.

شکل ۵ــ۱۲

۳ــ در کادر توضیحات مختصر راجع به AD DS،بر روی Next کلیک کنید.

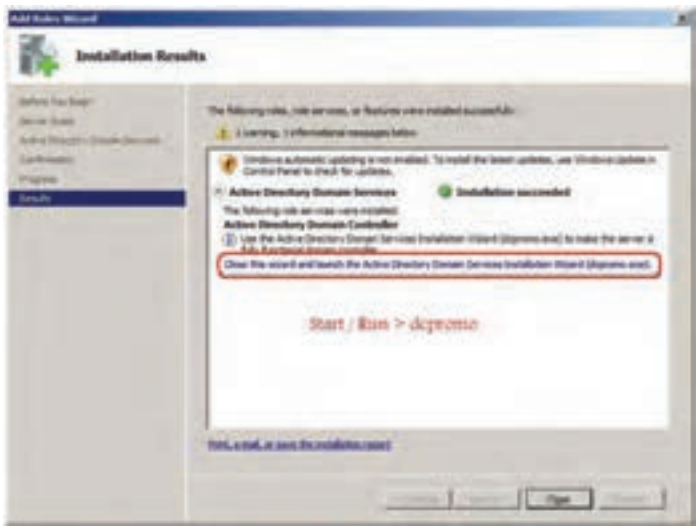
شکل ۶ــ۱۲

۴ــ در کادر Confirm Installation Selections بر روی دکمه Install کلیک کنید تا عملیات نصب شروع شود.



شکل ۷ــ۱۲

۵ــ صبر کنید تا کادر Installation Results ظاهر گردد.



شکل ۸ــ۱۲

برای ادامه کار احتیاج به اجرای برنامه Dcpromo داریم که برای اجرای آن دو راه وجود دارد :

الف) در پنجره Install Results بر روی لینکی که حاوی dcpromo.exe می‌باشد کلیک نمایید.

ب) فرمان dcpromo را از طریق Start→Run اجرا نمایید.

شکل ۹ــ۱۲

۶ــ برای ادامه نصب بر روی دکمه Next کلیک کنید تا کادر Operating System Compatibility که توضیحاتی برای سازگاری سیستم عامل می‌باشد نمایش داده شود، همچنین در انتهای کادر، آدرسی اینترنتی برای انجام تنظیمات مورد نظر قرار داده شده است.

شکل ۱۰ــ۱۲

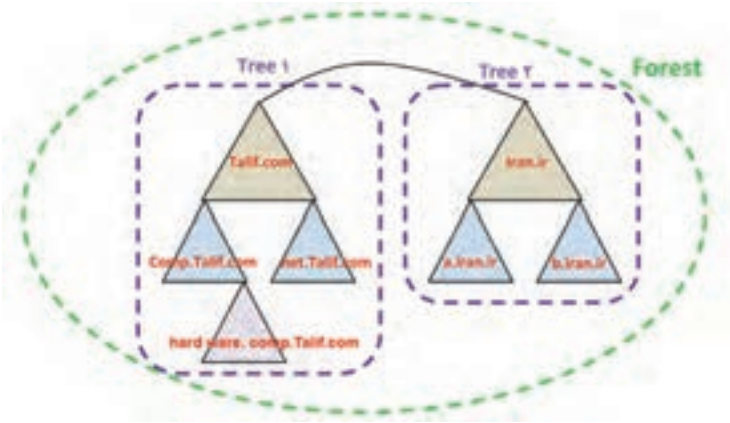
۷ــ در کادر Operating System Compatibility بر روی Next کلیک کنید.

شکل ۱۱ــ۱۲

۸ ــ در کادر Choose a Deployment Configuration چون شما اولین بار است اقدام به نصب AD می‌کنید، باید گزینه Create a new domain in a new forest را انتخاب کنید.(یعنی ایجاد یک Domain جدید در یک forest[1] جدید)

در اینجا باید اشاره کرد که DC فهرستی از Domainها را به صورت سلسله مراتبی ذخیره می‌کند، بنابراین Domain واحد اصلی ساختار منطقی AD می‌باشد و AD از یک مجموعه به نام Forest (جنگل) تشکیل شده است و Forest (جنگل) نیز از یک یا چند Tree (درخت) تشکیل می‌شود. به عبارت دیگر Tree از یک یا چند Domain در فضای نام (Namespace) پیوسته تشکیل شده است که به صورت سلسله مراتبی می‌باشد (مانند شکل ۱۲ــ۱۲).

۱ــ جنگل



شکل ۱۲ــ۱۲

هر کدام از مثلث‌ها در شکل ۱۲ــ۱۲ یک Domain می‌باشند و هر ردیف پایین‌تر به عنوان Child Domain (دامنه فرزند) برای ردیف بالایی می‌باشد و Domain بالاتر به عنوان Parent Domain (دامنه والدین) شناخته می‌شود. اولین Domain تعریف شده در یک Forest را Root Domain نیز می‌گویند.

۹ــ در صفحه Name the Forest Root Domain ، در کادر FQDN of the forest root Domain باید آدرس کامل یا FQDN را وارد نمایید. آدرس Talif.com را به عنوان آدرس Domain در نظر بگیرید (که به عنوان دامنه ریشه می‌باشد) سپس Nextرا کلیک کنید.

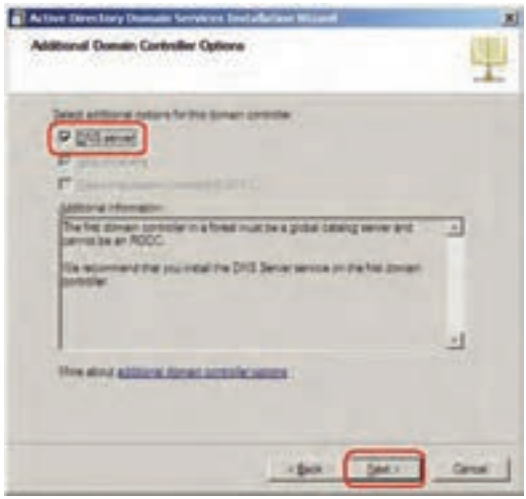
شکل ۱۳ــ۱۲

۱۰ــ بعد از وارد کردن نام دامنه ریشه، باید سطح عملکرد Forest را تعیین کنید، در اینجا شما می‌توانید سه سطح را تعیین کنید که عبارتند از ،Windows Server2003 Windows Server 2008 و Windows Server 2000.

شکل ۱۴ــ۱۲

توجه داشته باشید اگر شما Windows Server 2008 را انتخاب کنید، دیگر نمی‌توانید از DC این سرور در ویندوزهای سرور نسخه پایین‌تر مانند Windows Server 2000 یا 2003 در Forest استفاده نمایید.

۱۱ــ AD DS برای نصب، به DNS Server نیاز دارد، از صفحهٔ Additional Domain Cont roller Options چنانچه قبلاً سرویس DNS را نصب نکرده باشید می‌توانید DNS Server را با فعال کردن آن نصب کنید. اگر از قبل DNS Server را در این سرور نصب کرده باشید گزینه DNS Server غیر فعال خواهد بود.



شکل ۱۵ــ۱۲

با کلیک بر روی دکمه Next کادر هشدار شکل ۱۶ــ۱۲ ظاهر می‌شود، چنانچه شما بخواهید AD DS را با DNS Server به صورت مجتمع نصب کنید بر روی دکمه Yes کلیک کنید.

شکل ۱۶ــ۱۲

۱۲ــ در کادرLocation for Database, log file, and SYSVOLمی‌توانید محل ذخیره پوشه بانک اطلاعاتی(Database folder)، پوشه پرونده‌های Log مربوط به دایرکتوری (Log files folder) و ولوم پوشه (SYSVOL)[1] را تعیین کنید.

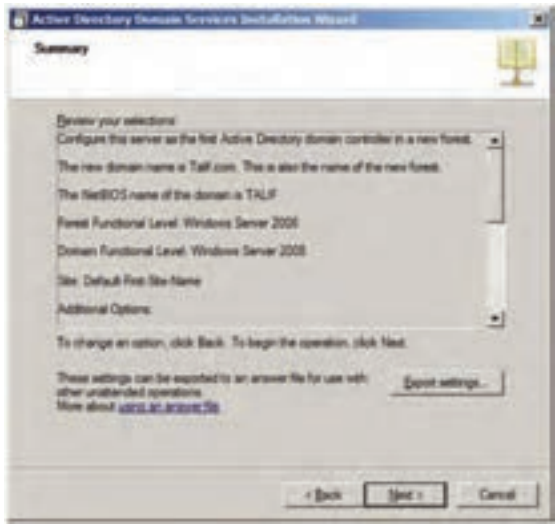
شکل ۱۷ــ۱۲

۱ــ در این پوشه اطلاعاتی از Domain که یک کپی از آن به نام DC فرستاده می‌شود، نگهداری شده و این پوشه حتماً باید در یک پارتیشن با پرونده سیستم NTFS قرار داشته باشد.

۱۳ــ در صفحه Directory Services Restore Mode Administrator Password می‌توانید برای حالت بازیابی (Restore Mode) رمز در نظر بگیرید این رمز بهتر است با رمز کاربر مدیر ورود به ویندوز متفاوت باشد.

شکل ۱۸ــ۱۲

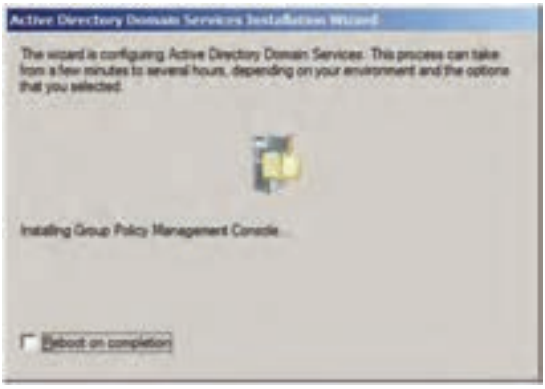
۱۴ــ پس از ورود رمز، روی Next کلیک کنید تا وارد صفحه Summary شوید.



شکل ۱۹ــ۱۲

۱۵ــ در صفحه Summary اگر بخواهید از تنظیمات انجام شده خروجی بگیرید، بر روی دکمه Export Settings کلیک نموده و نام محل ذخیره را تعیین نمایید.

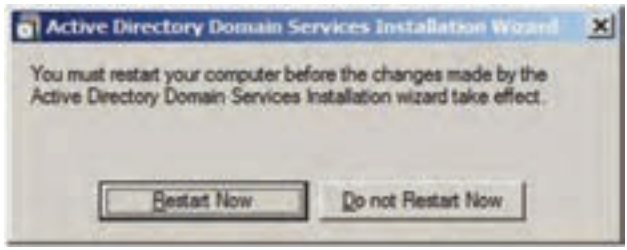
۱۶ــ در ادامه بر روی Next کلیک کنید تا تنظیمات کامل شود. توجه داشته باشید که بعد از انجام تنظیمات سیستم باید دوباره راه اندازی (Restart) شود. گاهی اوقات گذر از این مرحله ممکن است چند دقیقه تا چند ساعت طول بکشد.



شکل ۲۰ــ۱۲

۱۷ــ صبر کنید تا کادر پیغام پایان عملیات ویزارد نصب، ظاهر شود و سپس بر روی دکمه Finish کلیک کنید و در کادر ظاهر شده، حتماً بر روی گزینه Restart Now برای راه اندازی مجدد سیستم عامل کلیک نمایید.

شکل ۲۱ــ۱۲



شکل ۲۲ــ۱۲

بعد از نصب AD DS و راه‌اندازی مجدد، سیستم کندتر بالا می‌آید. حالا رایانه ما به یک کنترل کننده دامنه (DC) تبدیل شده است.

۵ــ۱۲ــ تغییرات بعد از نصب AD DS در سیستم

اگر به بخش Administrative Tools مراجعه کنید، خواهید دید که آیتم‌هایی به آن در رابطه با Active Directory اضافه شده است که عبارتند از :

۱ــ Active Directory Users and Computer

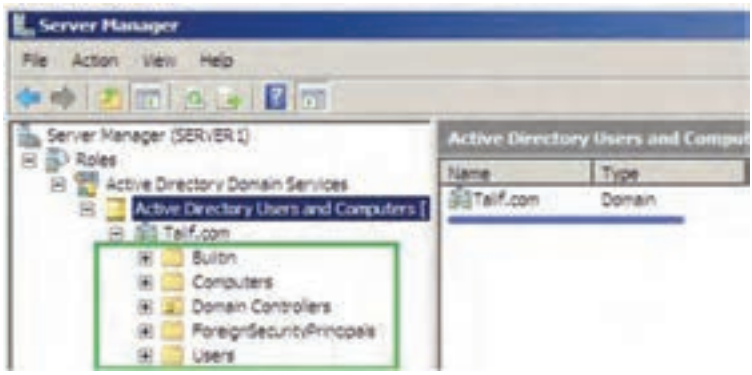
۲ــ Active Directory Domains and Trusts

۳ــ Active Directory Sites and Services

۴ــ Group Policy Management

۵ــ DNS (به خاطر فعال کردن DNS Server در حین نصب AD DS)

حال اگر برنامه Server Manager را باز کنید خواهید دید که در نام دامنه Talif.com در آن ثبت شده است. داخل دامنه Talif.com پوشه‌های مختلفی وجود دارد (شکل ۲۳ــ۱۲).

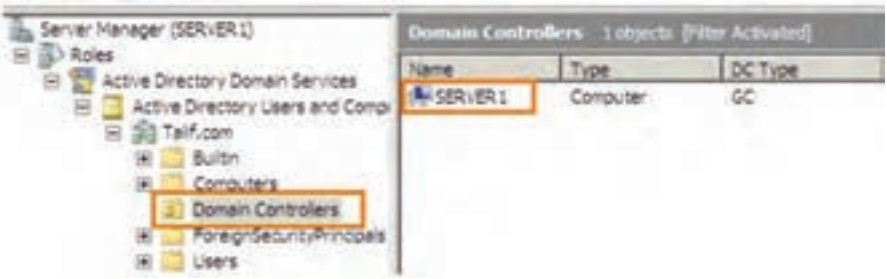


شکل ۲۳ــ۱۲

در پوشه Built ـ in لیست کاربران و گروه‌های کاربری داخل شبکه قرار دارد.

در پوشه Computers لیست رایانه‌های شبکه را نشان می‌دهد که عضو Domain هستند. وقتی که شما با رایانه‌ای به دامنه Talif.com متصل می‌شوید (Join) نام آن رایانه در فهرست Computers اضافه می‌شود.

پوشه Domain Controller لیست DC های داخل شبکه را نمایش خواهد داد. درحال حاضر رایانه جاری که DC روی آن نصب شده است نمایش داده می‌شود.



شکل ۲۴ـ۱۲

پوشه ForeignSecurityPrincipals حاوی آیتم‌هایی است که از یک دامنه دیگر وارد دامنه ما شده‌اند، مانند : دیسک سختی که داخل آن فهرست‌های اشتراکی وجود دارد و مربوط به دامنه‌های دیگرمی‌باشد و وارد دامنه ما شده است.

پوشه Users لیست کاربرانی که روی رایانه ما نصب شده‌اند را نمایش می‌دهد. ضمناً اگر DC دیگری هم وجود داشته باشد و به رایانه ما متصل باشد، لیست کاربران آن دامنه نیز قابل رؤیت خواهد بود.

در Server Manager در بخش Configuration همانطور که ملاحظه می‌کنید Local Groups and Users را نمی‌بینید و این به خاطر تبدیل رایانه ما به DC می‌باشد. لیست کاربران و گروه‌ها به صورت مشترک در پوشه Users وجود دارند.

حال اگر بر روی یک کاربر در Users کلیک راست کنید گزینه‌های بیشتری مانند شکل ۲۵ـ۱۲ رؤیت می‌شود.

شکل ۱۲ــ۲۵

حال اگر در پوشهٔ Users ویژگی‌های یک کاربر را نمایش بدهید، ملاحظه خواهید کرد که زبانه‌های بیشتری به کادر ویژگی‌های کاربر اضافه شده است. از ۸ زبانه در حالت Stand ــ alone به ۱۳ زبانه در حالت DC ارتقاء یافته است. (زبانه‌هایی که با کادر قرمز مشخص شده‌اند پس از نصب AD اضافه شده‌اند)

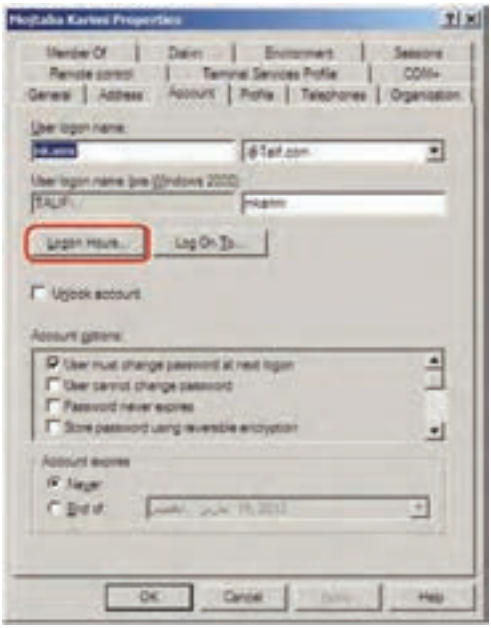
شکل ۱۲ــ۲۶

توجه داشته باشید در زبانه‌هایی که از قبل در حالت Stand ــ alone وجود داشته‌اند در حالت DC دارای مشخصات بیشتر و جزیی‌تر می‌باشند مانند زبانه General که نسبت به قبل، مشخصاتی مانند اداره، شماره تلفن، ایمیل و آدرس وب سایت به آن اضافه شده است (شکل ۱۲ــ۲۷).

شکل ۲۷ــ۱۲

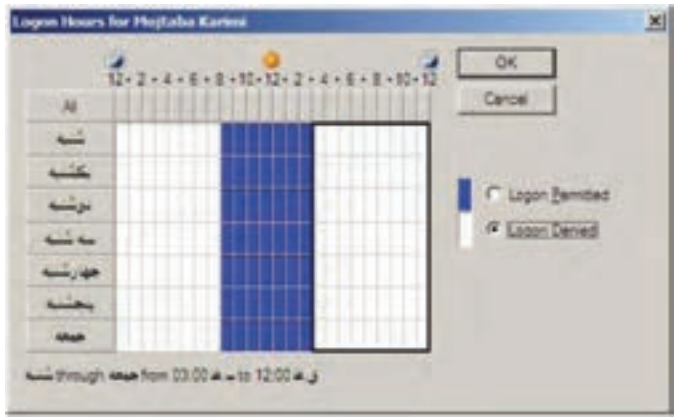
در زبانه Account یا حساب کاربری می‌توانید در User Logon Name نام کاربری برای Logon شدن را وارد کنید. البته اگر Logon Name را مشخص نکنید همان اسم کاربر به عنوان Logon Name در نظر گرفته می‌شود. در کادر بعدی نام دامنه را انتخاب کنید (Talif.com). اگر چند Domain داشته باشید لیست Domainها قابل انتخاب می‌باشد.

همچنین می‌توانید برای حسابتان تاریخ انقضا (Account Expire) مشخص کنید. پیش فرض گزینه Never می‌باشد یعنی کاربر تاریخ انقضا نداشته باشد و با تعیین تاریخ در بخش End of، می‌توانید تاریخ انقضا برای کاربر تعیین کنید.



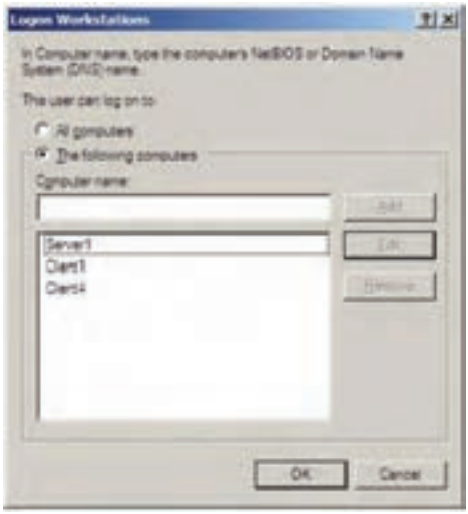
شکل ۲۸ــ۱۲

در Logon Hours می‌توانید ساعت‌هایی را که کاربر می‌تواند در آن ساعت‌های خاص در ایام هفته Logon کند را مشخص کنید.



شکل ۲۹ــ۱۲

با توجه به شکل ۲۹ــ۱۲ خانه‌هایی که به رنگ آبی پر شده‌اند بیانگر این می‌باشد که در آن ساعت از روز هفته، کاربر اجازهٔ logon کردن را دارد و در بقیه ساعات روز در هفته کاربر اجازه Logon کردن را ندارد. برای تعیین ساعت‌های دلخواه ابتدا با انتخاب گزینه‌های Logon Permitted (ورود مجاز) و Logon Denied (عدم ورود) و با کلیک کردن روی سلول‌های مورد آن را به رنگ آبی (ورود مجاز) و یا به رنگ سفید (ورود غیرمجاز) درآورید.



شکل ۳۰ــ۱۲

با استفاده از Log On To در زبانه Account می‌توان مشخص نمود کاربر جاری از تمام رایانه‌های عضو دامنه بتواند Logon شود یا اینکه از رایانه‌های خاصی بتواند وارد شبکه شود. در حالت پیش فرض کاربر از تمام رایانه‌های موجود در شبکه می‌تواند Logon شود.

زبانه Address برای ورود یا تعیین مشخصات آدرس دقیق پستی کاربر می‌باشد.

شکل ۱۲ــ۳۱

در زبانه Telephone می‌توانید شماره تلفن منزل، شماره پیجر، شماره تلفن همراه و یا شماره فاکس را وارد کنید.

شکل ۱۲ــ۳۲

در زبانه Organization می‌توان اطلاعات مربوط به مشخصات اداری کاربر از قبیل عنوان شغلی[1]، گروه یا دپارتمان، نام شرکت و مدیر کاربر در شبکه و همچنین گزارشی راجع به کاربر را تعیین نمود.

شکل ۳۳ــ۱۲

با زبانه Member of می‌توان تعیین کرد که کاربر شما عضو کدام گروه می‌باشد به طور مثال کاربر ایجاد شده عضو گروه Domain Users می‌باشد.

۶ــ۱۲ــ گروه‌ها در AD DS

در AD کادر ایجاد گروه نیز با کادر گروه در Stand ــ alone متفاوت می‌باشد.

در زمان ایجاد گروه باید نوع و دامنه گروه را مشخص کنید

Group Type (نوع گروه) که شامل دو قسمت می‌باشد :

الف) Security Group (گروه امنیتی) : برای مجوز دادن استفاده می‌شود.

ب) Distribution Group (گروه توزیع) : از آنها به عنوان لیست استفاده

۱ــ Job Title

می‌شود مانند استفاده از لیست برای ارسال ایمیل گروهی

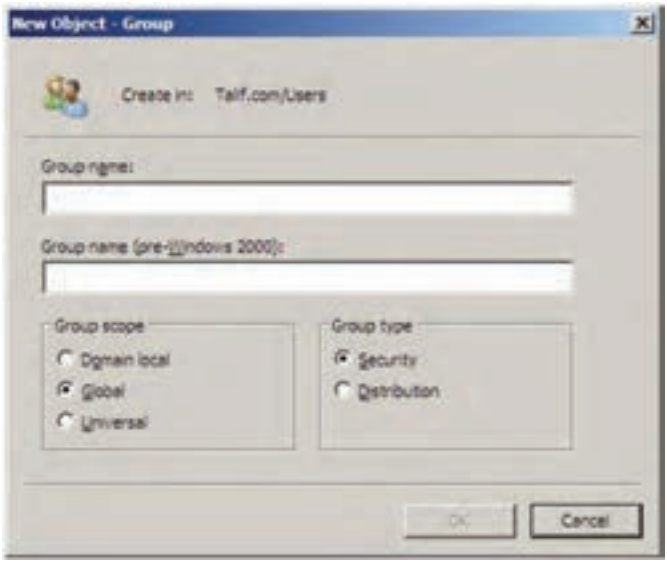
Group scopes (حوزه گروه) بیانگر محدوده عملکرد یک گروه می‌باشد که شامل سه نوع می‌باشد :

۱ــ Domain Local Group : اعضای گروه می‌توانند از گروه‌های دیگر نیز باشند و فقط به منابع یک Domain دسترسی دارند.

۲ــ Global Group : اعضای این گروه شامل حساب‌ها و گروه‌هایی است که در آن دامنه تعریف شده‌اند. اعضای این گروه می‌توانند به تمام دامنه‌های Forest دسترسی داشته باشند.

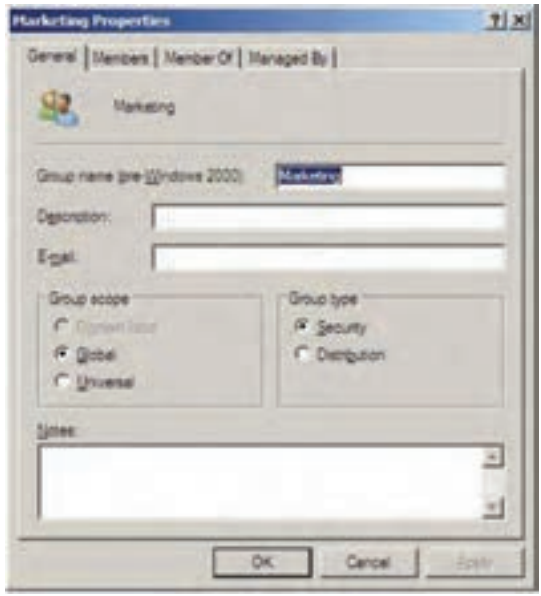
۳ــ Universal Group : اعضای این گروه می‌تواند از دامنه‌ای در جنگل یا درخت باشد. و می‌تواند به منابع تمام دامنه‌ها دسترسی داشته باشد.

برای ایجاد گروه جدید با کلیک راست بر روی Users می‌توانید گزینه New و سپس Group را انتخاب نمایید.



شکل ۳۴ــ۱۲

بعد از ایجاد گروه جدید با دابل کلیک بر روی نام گروه و یا کلیک راست بر روی نام گروه و انتخاب گزینه Properties کادر ویژگی گروه نمایش داده می‌شود.



شکل ۳۵ــ۱۲

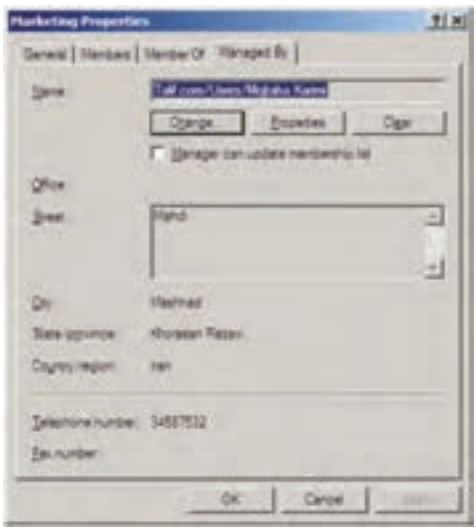
در زبانه Members لیست گروه‌هایی که عضو گروه جاری هستند را نمایش می‌دهد و امکان اضافه کردن گروه جدید به لیست هم وجود دارد.

شکل ۳۶ــ۱۲

در زبانه Member Of می‌توان لیست گروه‌هایی که، گروه جاری عضو آنها می‌باشد را نمایش داد و همچنین می‌توان گروه جاری را به عضویت گروه‌های دیگر درآورد.

شکل ۳۷ــ۱۲

در کادر ویژگی گروه‌ها، زبانه Managed By نسبت به Stand ــ alone جدید می‌باشد که توسط آن می‌توانید نام مدیر گروه را مشخص کنید. با انتخاب نام مدیر گروه، مشخصات مدیر که در User Properties ثبت کرده‌اید در این زبانه نیز نمایش داده می‌شود.



شکل ۳۸ــ۱۲

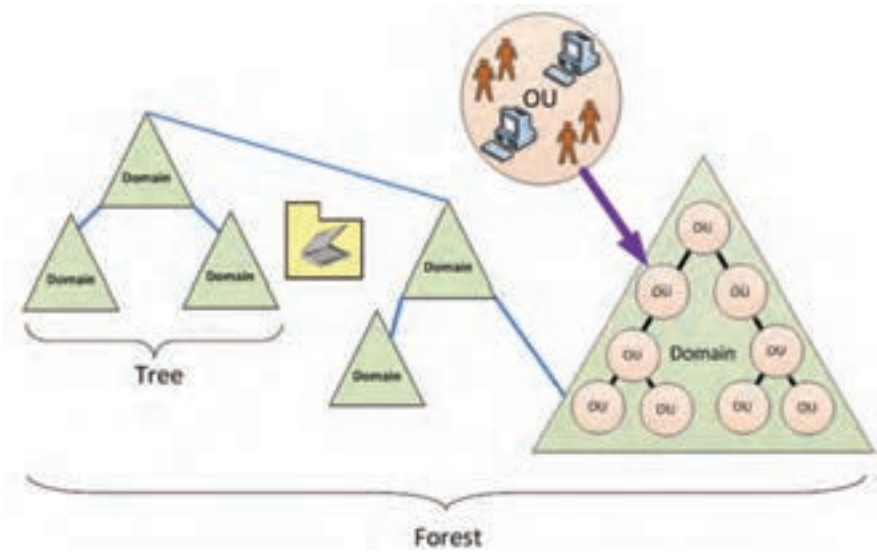
۷ـ۱۲ـ کاربرد Organizational Unit

در هر سازمان برای مدیریت ساده‌تر و ساختار یافته از یک سری واحدهای سازمانی استفاده می‌شود. به عنوان مثال استفاده از واحدهای مختلف نظیر کار گزینی، امور اداری، حسابداری، آموزش، روابط عمومی، IT و... در بسیاری از شرکت‌ها و سازمان‌ها معمول و مرسوم می‌باشد.

در هر واحد سازمانی تعدادی کارمند و مقداری منابع مثل رایانه، چاپگر و... یک مدیر برای آن واحد وجود دارد. برای مدیریت راحت‌تر شبکه، می‌توانید در یک Domain، واحدهای مختلف سازمانی ایجاد نمایید که به آن‌ها اصطلاحاً Organizational Unit می‌گویند و به اختصار با نام OU به آن‌ها اشاره می‌شود.

هر OU می‌تواند تعداد زیادی کاربر، رایانه، چاپگر و حتماً مدیر داشته باشد و حتی می‌توان سیاست‌های خاص برای آن‌ها در نظر گرفت.

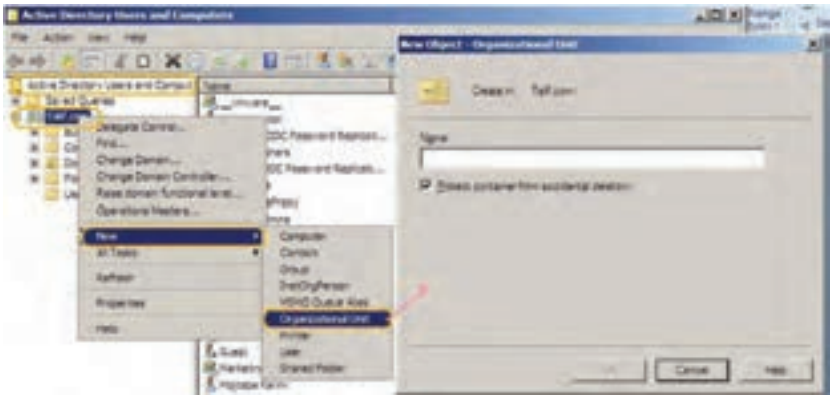
در واقع یک Domain را می‌توان به تعدادی OU تقسیم کرده و منابع و کاربران را نیز بین آن‌ها تقسیم نمود و حتی مدیریت آن‌ها را نیز به کاربران خاص واگذار نمود.



شکل ۳۹ـ۱۲

برای ایجاد یک OU جدید مراحل زیر را انجام دهید :

ابتدا برنامه Active Directory User and Computer از مسیر Start → Administrative Tools را اجرا کنید. بر روی Talif.com کلیک راست نموده و گزینه Organization Unit از New را انتخاب نمایید (مطابق شکل ۴۰ـ۱۲).



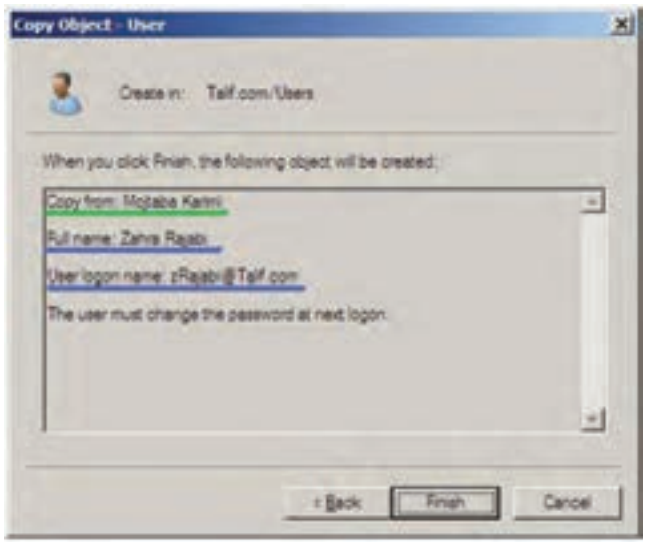
شکل ۴۰ـ۱۲

در کادر New Object ـ Organization Unit نام OU مورد نظر را وارد کنید. (مثلاً Customer1)

با کلیک بر روی OK، در زیر گروه Talif.com پوشه Customer1 که به عنوان یک OU می‌باشد اضافه شده است. حال می‌توانید برای این OU کاربر جدید، گروه جدید، رایانه جدید، چاپگر جدید و . . . اضافه نمایید. برای زمانی که مشخصات دسترسی کاربران یک OU شبیه هم بود شما می‌توانید بعد از ایجاد کاربر آن را تکثیر نمایید. مراحل کپی کردن یک کاربر روی کاربر مورد نظر Mojtaba) (Karimi کلیک راست نموده سپس گزینه Copy... را انتخاب نمایید. در کادر Copy Object User مشخصات کاربر جدید را وارد کنید (شکل ۴۱ـ۱۲).

شکل ۴۱ـ۱۲

با کلیک بر روی Next کادر دریافت کلمه عبور ظاهر می‌گردد، بعد از ورود کلمه عبور و کلیک بر روی دکمه Next گزارش ایجاد کاربر ظاهر می‌گردد که در آن مشخص شده که کاربر جدید از روی کاربر Mojtaba Karimi ایجاد شده است.



شکل ۴۲ـ۱۲

توجه داشته باشید با کپی کردن یک کاربر، پارامترهایی چون نام کشور ـ استان و شهر تنظیماتی چون Log on To Hours و Logon Account Expire از کاربر قبلی بر روی کاربر جدید نیز اعمال می‌شود.

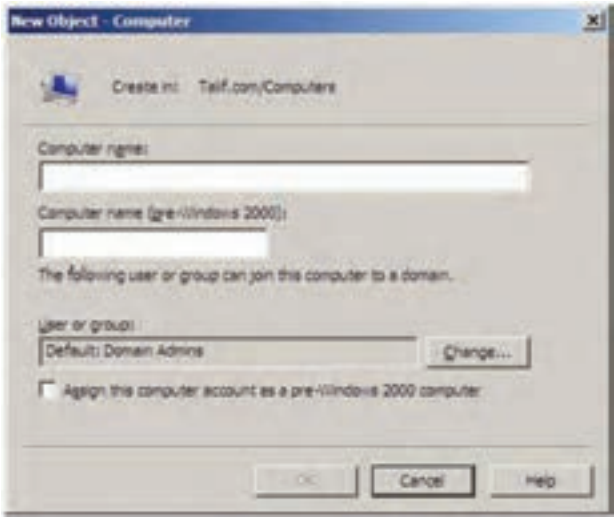
۸ـ۱۲ـ Computer Account

یکی دیگر از اجزای AD، Computers می‌باشد. Computer Account فقط برای سیستم عامل‌هایی که دارای تکنولوژی NT هستند استفاده می‌شود (مانند Windows NT,2000,XP,2003,Vista,7,2008).

وقتی با ویندوزهای با تکنولوژی NT به دامنه (Domain) ویندوز سرور متصل می‌شوید یک حساب رایانه‌ای (Computer Account) به فهرست Computers اضافه می‌شود. شما می‌توانید حساب‌های کاربری و رایانه‌ای را غیر فعال (Disable)، تنظیم مجدد (Reset) و حذف نمایید.

به دو طریق می‌توان یک حساب رایانه‌ای برای اتصال به Domain ایجاد نمود.

۱ــ کلیک راست بر روی Computers در Active Directory User and Computer و انتخاب گزینه New و زیر گزینه Computers که کادر Newobjet – Computer را برای ورود اطلاعات Computer Account نمایش می‌دهد.



شکل ۴۳ــ۱۲

کافی است در کادر Computer name نام رایانه را وارد کنید.

۲ــ از روی یک رایانه‌ای موجود در شبکه می‌توان یک حساب رایانه‌ای برای اتصال به Domain ایجاد نمود.

۹ــ۱۲ــ مراحل اتصال یک کلاینت به Domain

الف) در رایانه سرویس گیرنده (کلاینت) که دارای یکی از ویندوزهای XP، Vista و 7 می‌باشد ابتدا بر روی My Computer کلیک راست نموده سپس گزینه Properties را انتخاب نمایید.(در Windows XP[1])

۱ــ در Windows Vista یا Windows 7 بعد از انتخاب Properties باید بر روی گزینه Change Settingsکلیک نمایید تا به زبانه Computer Nameدسترسی پیدا کنید.

ب) زبانه Computer Name را انتخاب نمایید و بر روی دکمه Change... کلیک نمایید.

ج) ابتدا در بخش Member of گزینه Domain را انتخاب نموده سپس نام دامنه (Talif.com) را وارد کنید. سپس بر روی OK کلیک کنید.

د) اگر ارتباط با دامنه Talif.com بر قرار شد کادر زیر برای دریافت نام کاربر و کلمه ورود نمایش داده می‌شود.

شکل ۴۴ــ۱۲

هـ) توجه داشته باشید که باید نام و کلمه عبور کاربر Administrator در ویندوز سرور ۲۰۰۸ که یک Domain می‌باشد را وارد کنید. در صورتی کلمه عبور و نام کاربر را درست وارد نمودید پیغام خوش آمدگویی به دامنه Talif.com ظاهر می‌گردد.

شکل ۴۵ــ۱۲

و) همچنین صفحه مشخصات رایانه با تعاریف جدید نمایش داده می‌شود.

شکل ۴۶ــ۱۲

ز) با کلیک کردن بر روی دکمه OK کادر پیغام زیرمبنی بر راه‌اندازی مجدد سیستم ظاهر می‌گردد.

شکل ۴۷ــ۱۲

ح) بعد از انجام تنظیمات فوق، رایانه سرویس گیرنده باید مجدداً راه اندازی شود. به طوری که بعد از بالا آمدن سیستم عامل صفحه Logon ویندوز به صورت منوی کشویی برای نام کاربر جهت اتصال به Domain ظاهر می‌گردد.

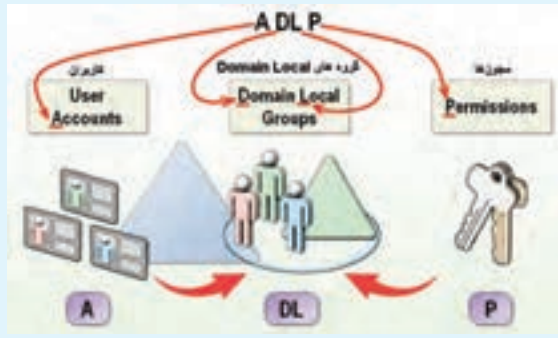
۱۰ـ۱۲ـ روش‌های اعطای مجوز به کاربران

از روش‌های مختلفی برای اعطای مجوز به کاربران به کمک گروه‌ها می‌توان استفاده نمود. در این‌جا به چند روش اشاره می‌شود.

۱ـ۱۰ـ۱۲ـ روش AGP : در این روش کاربران (Account)ها در گروه‌های مختلف از نوع Global دسته‌بندی می‌شوند. همان‌طوری که قبلاً هم بیان شد، این دسته‌بندی از نظر نوع کار و محل جغرافیایی کاربران انجام می‌شود. سپس مجوز (permission) لازم به گروه‌ها اعطا می‌شود. از این روش در شبکه‌هایی که تعداد objectها زیاد نیست می‌توان استفاده کرد.

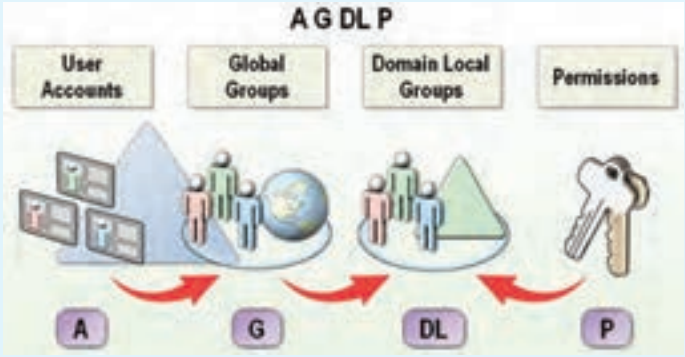
۲ـ۱۰ـ۱۲ـ روش ADLP : دراین روش می‌توانید کاربران (Account)ها را در گروه‌های مختلف از نوع Domain Local دسته‌بندی کنید. سپس به گروه‌های مورد نظر مجوز لازم اعطا کنید (شکل ۴۸ـ۱۲).

شکل ۴۸ـ۱۲



شکل ۴۹ـ۱۲

۳ــ۱۰ــ۱۲ــ AGDLP : در این روش کاربران (Account)ها را در گروه‌های مختلف از نوع Global دسته‌بندی کنید. سپس گروه‌های از نوع Domain Local ایجاد کرده و به آن‌ها مجوز (Permission) لازم را اعطا کنید. حال تمامی گروه‌های Global که لازم است مجوزهای مربوطه را داشته باشند، به عضویت گروه‌های Domain Local درآورید.



شکل ۵۰ــ۱۲

از این روش در شبکه‌هایی که تعداد object های زیادی دارند و یا شبکه‌هایی که از چندین Domain تشکیل شده‌اند می‌توان استفاده کرد.

۱۱ــ۱۲ــ آشنایی با گروه‌های Built-in

گروه‌های Built-in گروه‌هایی هستند که زمان نصب Active Directory به صورت اتوماتیک ایجاد می‌شوند. این گروه‌ها را در ابزار Active Directory Users and Computers در پوشه‌های Built-in و Users می‌توان مشاهده نمود.

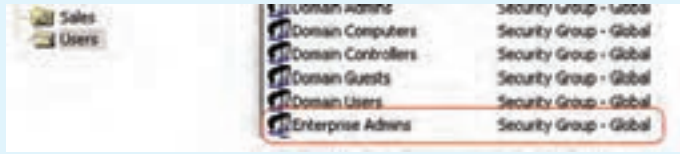
۱ــ۱۱ــ۱۲ــ گروه‌های Built-in Global : این گروه‌ها در پوشهٔ Users در ابزار Active Directory Users and Computer قرار دارند و عبارتند از :

■ **Domain users** : این گروه شامل تمامی کاربران Domain می‌شود. هر کاربری که در Domain ایجاد می‌شود، به صورت اتوماتیک به عضویت این گروه درمی‌آید.

■ **Domain Admins** : اعضای این گروه می‌توانند Domain را مدیریت کنند و به عنوان مدیر Domain شناخته می‌شوند. فقط Administrator همان Domain به

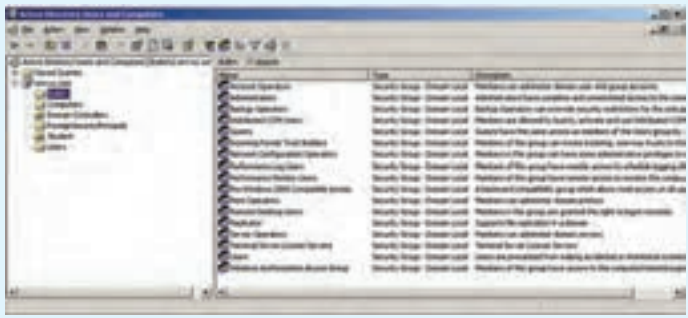
صورت پیش‌فرض عضو این گروه می‌باشد.

■ **Enterprise Admins** : اعضای این گروه می‌توانند Forest را مدیریت کنند. یعنی توان مدیریت در تمامی Domainهای Forest را خواهند داشت. به صورت پیش‌فرض Administrator اولین Domain عضو این گروه می‌باشد. این گروه به صورت پیش‌فرض از نوع Global می‌باشد. اما اگر سطح کارکرد Domain را به Native ۲۰۰۰ یا به ۲۰۰۳ Server تغییر دهید، این گروه به صورت اتوماتیک به نوع Universal تبدیل خواهد شد.



شکل ۱۲ــ۵۱

شکل ۱۲ــ۵۲



شکل ۱۲ــ۵۳

۲ــ۱۱ــ۱۲ــ گروه‌های Built-in Domain Local : این گروه‌ها در پوشه Built-in در ابزار Active Directory Users and Computers قرار دارند عبارتند از :

■ **Administrators** : اعضای این گروه می‌توانند DCها را مدیریت کنند و

تمامی مجوزها روی این رایانه‌ها قرار خواهند داشت.

■ **Server operators** : اعضای این گروه می‌توانند در انجام بعضی ازکارهای مدیریتی به مدیر شبکه کمک کنند به‌عنوان مثال می‌توانند عملیات زیر را روی DCها انجام دهند.

- Log on کردن
- Shut down کردن
- قالب‌بندی کردن درایوها
- تغییرساعت

■ **Account operators** : اعضای این گروه می‌توانند عملیات مدیریتی همچون ایجاد، حذف و ... را روی Accountها (شامل : کاربران، گروه‌ها و رایانه) انجام دهند. به‌عنوان مثال اعضای این گروه می‌توانند یک کاربر و یک گروه ایجاد کرده و آن کاربر را به عضویت آن گروه درآورند.

■ **Print operators** : اعضای این گروه می‌توانند چاپگرهای Domain را مدیریت نمایند.

● **Backup operators** : اعضای این گروه می‌توانند عملیات Backup گرفتن از اطلاعات و برگرداندن اطلاعات (Restore کردن) را انجام دهند.

■ **Network configuration operators** : اعضای این گروه می‌توانند تنظیمات شبکه را تغییر دهند. به عنوان مثال این اعضا می‌توانند آدرس IP را روی کارت شبکه DC تغییر دهند.

۳ــ۱۱ــ۱۲ــ گروه‌های Built-in system : این گروه‌ها، گروه‌هایی هستند که لیست اعضای آن‌ها را نمی‌توان دید و یا تغییر داد. اما می‌توانید از آن‌ها برای انجام کارهای مدیریتی استفاده کنید، به عنوان مثال می‌توانید به این گروه‌ها مجوز اعطا کنید. این گروه‌ها عبارتند از :

■ **Every one** : این گروه شامل تمامی کاربرانی می‌شود که به یک رایانه متصل می‌باشند (تمامی کاربران شناخته شده و یا ناشناخته).

■ **Authenticated users** : تمامی کاربران که عمل authentication برای

آن‌ها اتفاق می‌افتد یا به عبارت دیگر دارای account می‌باشند.

■ **Anonymous Logon** : این گروه شامل کاربرانی است که به صورت ناشناس به یک رایانه متصل می‌شوند.

■ **Dialup** : این گروه شامل کاربرانی است که از طریق Dialup به رایانه متصل می‌شوند.

■ **Network** : شامل کاربرانی است که از طریق شبکه به یک رایانه متصل می‌شوند.

زمانی که به کاربران مجوز اعطا می‌کنید در لیستی که کاربران و گروه‌ها نمایش داده می‌شوند، می‌توانید گروه‌های سیستمی را مشاهده کنید.

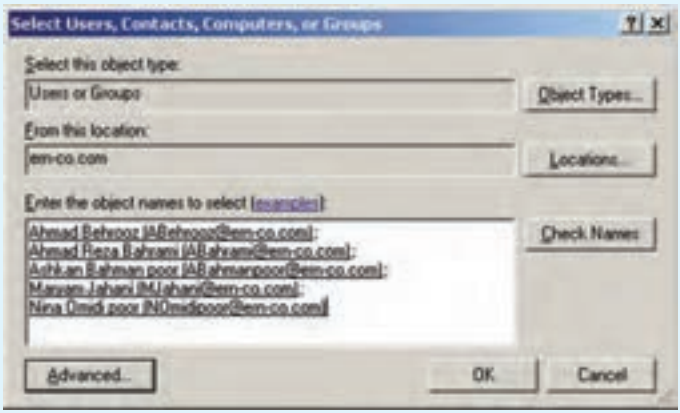
۱۲ـ۱۲ـ پیاده‌سازی روش‌های مختلف اعطای مجوز به کاربران

۱ـ ۱۲ـ۱۲ـ پیاده‌سازی روش AGP : در این روش ابتدا یك گروه از نوع Global به همان شیوه‌ای که در مراحل قبل یاد گرفتید با نام G sale ایجاد کنید.

سپس مطابق شکل ۱۲ـ۵۴ از این گروه Properties گرفته و در زبانه Members لیست اعضای این گروه را مشاهده می‌کنید.

شکل ۱۲ـ۵۴

حال اگر روی کلید Add کلیک کنید پنجرهٔ شکل ۱۲ـ۵۰ نمایش داده خواهد شد. در این پنجره می‌توانید اسامی کاربران را تایپ کرده و به لیست اضافه نمایید و یا برای انتخاب کاربران از لیست روی کلید Advanced کلیک کرده و سپس روی گزینهٔ Find Now کلیک نمایید تا لیستی از کاربران و گروه‌ها نمایش داده شوند.



شکل ۱۲ـ۵۵

حال کاربران مورد نظر را به کمک کلیدهای Ctrl و یا Shift انتخاب کرده و به لیست اضافه نمایید. مشاهده خواهید کرد که این کاربران در زبانه Members لیست شده‌اند. روی گزینه OK کلیک کنید.

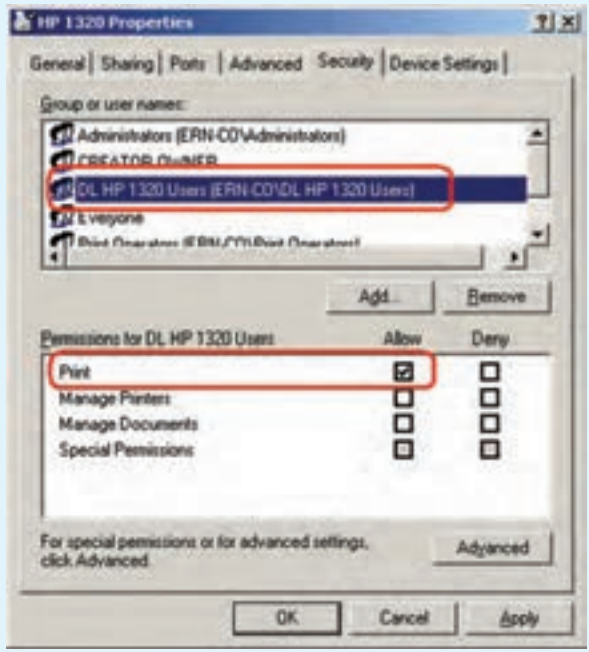
شکل ۱۲ـ۵۶

حال در هر جایی که منابع قرار دارند به این گروه مجوز می‌دهید. به عنوان مثال فرض کنید که یک پوشه به اشتراک گذاشته شده به‌نام Sale Data وجود دارد. روی این پوشه کلیک راست کرده و گزینه Sharing and security را انتخاب کنید، در پنجره ظاهر شده روی Permissions کلیک کنید تا پنجره شکل ۱۲ـ۵۶ ظاهر شود.

در این پنجره گروه Everyone را حذف کرده و سپس گروه G sale را به لیست اضافه کرده و مجوزهای لازم را به آن انتساب دهید.

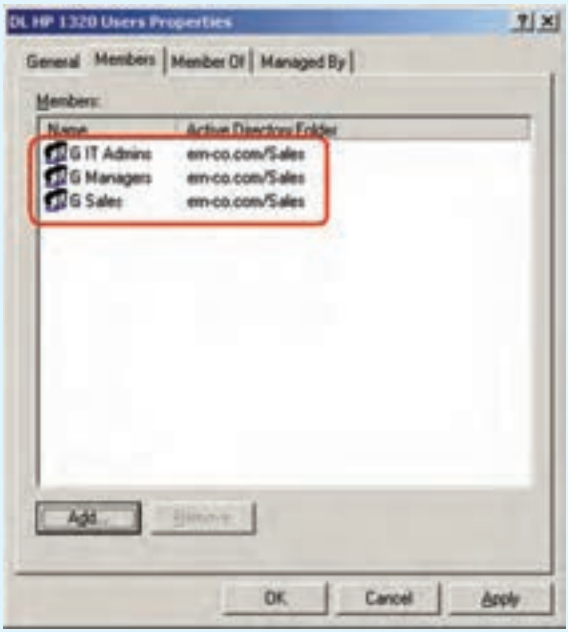
۲ــ ۱۲ ــ۱۲ــ پیاده‌سازی روش ADLP : این روش مشابه روش قبلی می‌باشد با این تفاوت که گروه را با نام DL Sales ایجاد کرده و نوع آن را Domain Local انتخاب کنید. بقیه مراحل مشابه مثال قبل می‌باشد.

۳ــ ۱۲ ــ۱۲ــ پیاده‌سازی روش AGDLP : دراین روش ابتدا یک دسته‌بندی منطقی برای کاربران درنظر گرفته و سپس گروه‌هایی از نوع Global را ایجاد کنید و کاربران را براساس آن دسته‌بندی به عضویت گروه‌های مختلف درآورید. سپس یک گروه از نوع Domain Local ایجاد نمایید و مجوزهای لازم روی منبع موردنظر را به آن اعطا نمایید. به عنوان مثال یک گروه با نام DL HP ۱۳۲۰ Users از نوع Domain Local ایجاد نموده و مجوز Print را روی یک چاپگر به اشتراک گذاشته شده به آن اعطا کنید (شکل ۵۷ــ۱۲).



شکل ۵۷ــ۱۲

حال تمامی گروه‌های از نوع Global را که قرار است مجوز Print روی این چاپگر داشته باشند، به عضویت گروه DL HP ۱۳۲۰ users درآورید (شکل ۵۸ــ۱۲).



شکل ۵۸ــ۱۲

خودآزمایی و پژوهش

۱ــ Domain Controller چیست؟ وظایف و ویژگی‌های آن‌ها را شرح دهید.

۲ــ Forest چیست؟

۳ــ Child Domain را با ذکر مثال تعریف کنید.

۴ــ آیا یک رایانه می‌تواند به طور همزمان عضو چند Domain باشد؟

۵ــ بررسی کنید که چه روش دیگری برای نصب Active Directory وجود دارد؟

۶ــ تفاوت Security Group و Distribution در چیست؟

۷ــ چطور می‌توان در یک سطح وزارتخانه برای کاربران مجوزهای لازم را صادر کرد؟

۸ــ اگر بخواهیم برای یک مدرسه، شبکه‌ای ایجاد کنیم که شامل کلیه دانش‌آموزان و معلمان و مدیران باشند از کدام روش باید برای اعطای مجوز به کاربران استفاده کنیم؟ توضیح دهید.

۹ــ انواع Account را نام ببرید.

۱۰ــ کاربرد Account Expires چیست و رابطه آن را Password never expires بنویسید.

۱۱ــ یک کاربر به عنوان Student ایجاد کرده که دارای ویژگی‌های زیر باشد.

الف) فقط روزهای زوج از ساعت ۱۰ الی ۱۴ بتواند Log on کند.

ب) فقط روی ۳ عدد از سرویس گیرنده‌ها بتوانند Log on کند.

ج) بتواند چاپگر را مدیریت کند.

د) بتواند تنظیمات شبکه، IP سیستم‌ها را عوض کند.

هـ) بتواند از طریق Dial up به شبکه متصل شود.