

### 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.
- نحوه عضویت سرویس گیرنده‌ها و انواع Log on ها را شرح دهد.

#### ۱۲-۱- 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 سرویس‌دهی 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<sup>۱</sup> 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<sup>۲</sup> استفاده خواهد شد. برای راه اندازی Domain باید سرویس Active Directory را در یک سرویس‌دهنده Stand \_ alone نصب کنید (وقتی که شما ویندوز ۲۰۰۸ سرور نصب می‌کنید و رایانه شما عضو

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

## ۱۲-۲- 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 هر بخش، 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<sup>۱</sup> در Domain می‌باشد، یعنی زمانی که کاربر می‌خواهد از روی سرویس گیرنده به Domain وارد شود، نام و گذر واژه<sup>۲</sup> 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 سرویس گیرنده اطلاع می‌دهد، به طوری که از آن به بعد، کاربر می‌تواند برای دسترسی به تمامی منابع موجود در Domain دسترسی داشته باشد.

۱- Authent cat on

۲- Password

### ۱۲-۳-۱۲- مراحل نصب AD DS در ویندوز ۲۰۰۸ سرور

عملیاتی را که باید قبل از شروع به نصب AD DS انجام داد عبارت‌اند از :  
 – تنظیم کارت شبکه<sup>۱</sup> 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

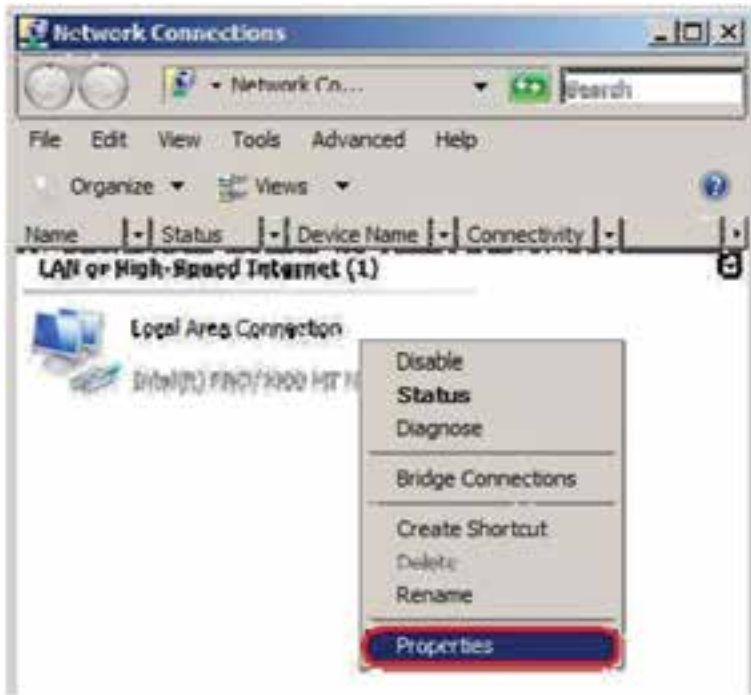
(ب) از Control Panel برنامه Network and Sharing اجرا کنید، سپس گزینه Manage network connections را انتخاب نمایید.



شکل ۱۲-۱

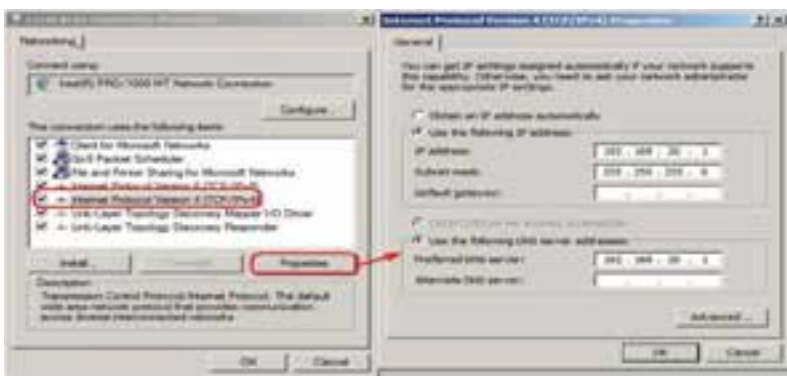
با اجرای هر کدام از دو روش قبلی پنجره Network Connections ظاهر می‌گردد. حال بر روی Local Area Connection کلیک راست نموده و سپس گزینه Properties را انتخاب نمایید.

۱- 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 ۱۲-۲

لازم به یادآوری است که برای سرورهای زیر ساخت<sup>۱</sup> در شبکه مانند DC، DNS، DHCP باید IP کارت شبکه را به صورت استاتیک (دستی) تنظیم نمایید. بنابراین اولین قدم در نصب AD DS تنظیم کردن IP کارت شبکه به صورت استاتیک می باشد. در ادامه در کادر Local Area Connection Properties (شکل ۱۲-۳) 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.



شکل ۳-۱۲

گزینه Use the following 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 طور خودکار به 255.255.255.0 تبدیل می‌شود.

**نکته ۱:** به ازای کلاس‌های مختلف IPv4 مقدار Subnet Mask مطابق با جدول ۱-۱۲ تغییر خواهد کرد. عدد 255 به معنی ثابت بودن عدد Network در IPv4 می‌باشد.

جدول ۱-۱۲ 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 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 به طور 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 Server1) 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.

## ۱۲-۴- 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 :

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

Start → Administrative Tools → Server Manger

۲- 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 Select Server Roles

انتخاب نمایید و سپس بر روی Next

کلیک کنید.



شکل ۱۲-۴

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



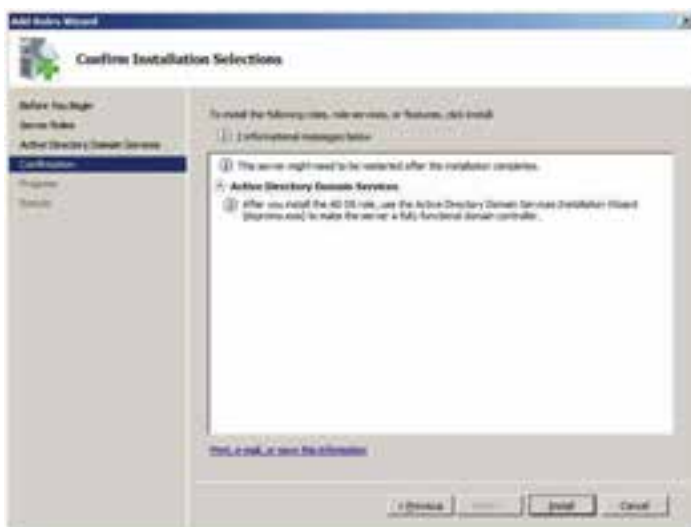
شکل ۱۲-۵

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



شکل ۱۲-۶

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



شکل ۷-۱۲

۵- صبر کنید تا کادر Installation Results ظاهر گردد.



شکل ۸-۱۲



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

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

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



شکل ۹-۱۲

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



شکل ۱۰-۱۲

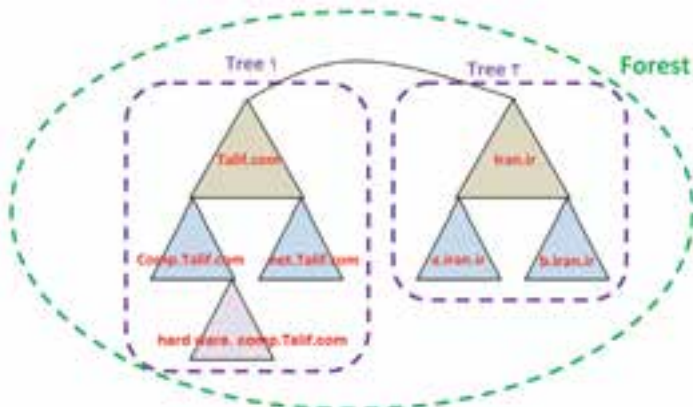
۷- در کادر Operating System Compatibility بر روی Next کلیک

کنید.



شکل ۱۱-۱۲

۸- در کادر Choose a Deployment Configuration چون شما اولین بار است اقدام به نصب AD می کنید، باید گزینه Create a new domain in a new forest را انتخاب کنید. (یعنی ایجاد یک Domain جدید در یک forest جدید) در اینجا باید اشاره کرد که DC فهرستی از Domain ها را به صورت سلسله مراتبی ذخیره می کند، بنابراین Domain واحد اصلی ساختار منطقی AD می باشد و از یک مجموعه به نام Forest (جنگل) تشکیل شده است و Forest (جنگل) نیز از یک یا چند Tree (درخت) تشکیل می شود. به عبارت دیگر Tree از یک یا چند Domain در فضای نام (Namespace) پیوسته تشکیل شده است که به صورت سلسله مراتبی می باشد (مانند شکل ۱۲-۱۲).



شکل ۱۲-۱۲

هر کدام از مثلث‌ها در شکل ۱۲-۱۲ 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.

۹- 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 Next را کلیک کنید.



شکل ۱۲-۱۳

۱۰- 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 Server 2003، Windows Server 2000 و Windows Server 2008.



شکل ۱۴-۱۲

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 Forest 2003 استفاده نمایید.



شکل ۱۵-۱۲

۱۱- ADDS برای نصب، به DNS Server نیاز دارد، از صفحه Additional Domain Controller 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.

با کلیک بر روی دکمه Next کادر هشدار شکل ۱۶-۱۲ ظاهر می‌شود، چنانچه شما بخواهید AD DS را با DNS Server به صورت مجتمع نصب کنید بر روی دکمه Yes کلیک کنید.



شکل ۱۶-۱۲

۱۲- در کادر Location for Database, log file, and SYSVOL می‌توانید محل ذخیره پوشه بانک اطلاعاتی (Database folder)، پوشه پرونده‌های Log مربوط به دایرکتوری (Log files folder) و ولوم پوشه (SYSVOL) را تعیین کنید.



شکل ۱۷-۱۲

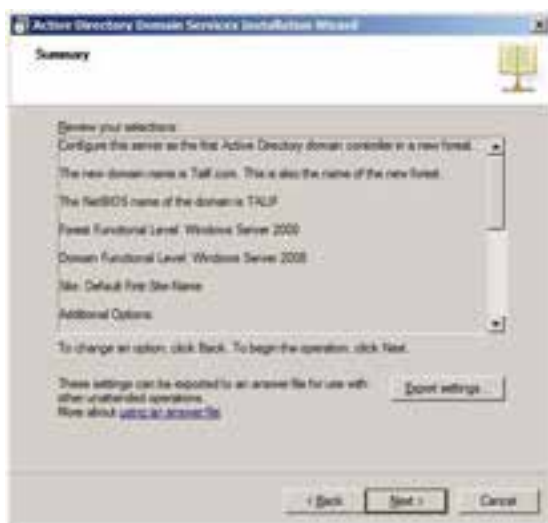
۱- در این پوشه اطلاعاتی از Domain که یک کپی از آن به نام DC فرستاده می‌شود، نگهداری شده و این پوشه حتماً باید در یک پارتیشن با پرونده سیستم NTFS قرار داشته باشد.

۱۳- 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 ۱۸-۱۲

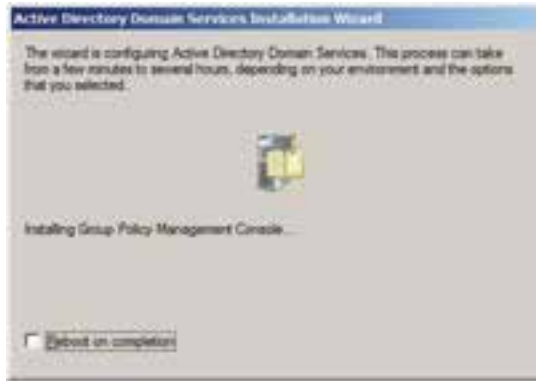
۱۴- پس از ورود رمز، روی Next کلیک کنید تا وارد صفحه Summary شوید.



شکل ۱۹-۱۲

۱۵- 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.

۱۶- 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 ۲۰-۱۲

۱۷- 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 ۲۱-۱۲



شکل ۱۲-۲۲

بعد از نصب ADDS و راه اندازی مجدد، سیستم کندتر بالا می آید. حالا رایانه ما به یک کنترل کننده دامنه (DC) تبدیل شده است.

### ۵-۱۲- تغییرات بعد از نصب AD DS در سیستم

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

۱- Active Directory Users and Computer

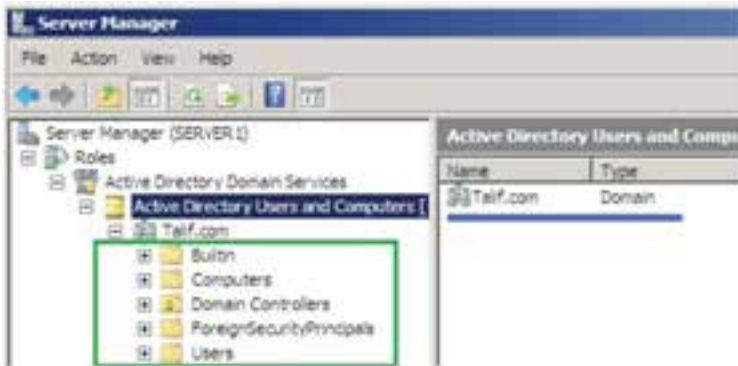
۲- Active Directory Domains and Trusts

۳- Active Directory Sites and Services

۴- Group Policy Management

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

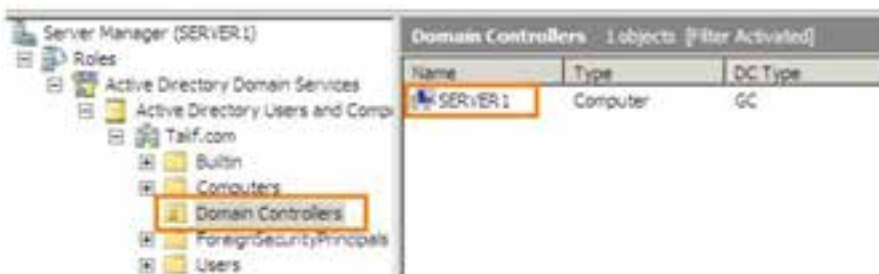
حال اگر برنامه Server Manager را باز کنید خواهید دید که در نام دامنه Talif.com در آن ثبت شده است. داخل دامنه Talif.com پوشه های مختلفی وجود دارد (شکل ۱۲-۲۳).



شکل ۱۲-۲۳



در پوشه Built-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. در حال حاضر رایانه جاری که DC روی آن نصب شده است نمایش داده می‌شود.



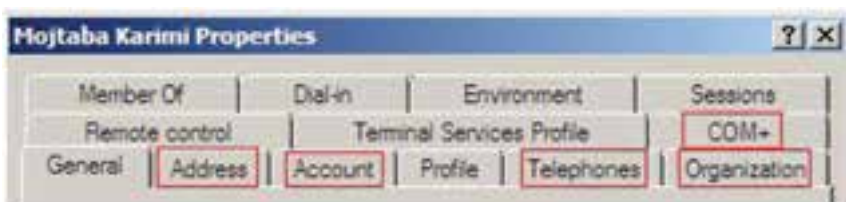
شکل ۲۴-۱۲

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 دیگری باشد 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 در 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 ۲۵-۱۲ رؤیت می‌شود.



شکل ۱۲-۲۵

حال اگر در پوشه 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 - alone به ۱۳ زبانه در حالت DC ارتقاء یافته است. (زبانه‌هایی که با کادر قرمز مشخص شده‌اند پس از نصب AD اضافه شده‌اند)



شکل ۱۲-۲۶

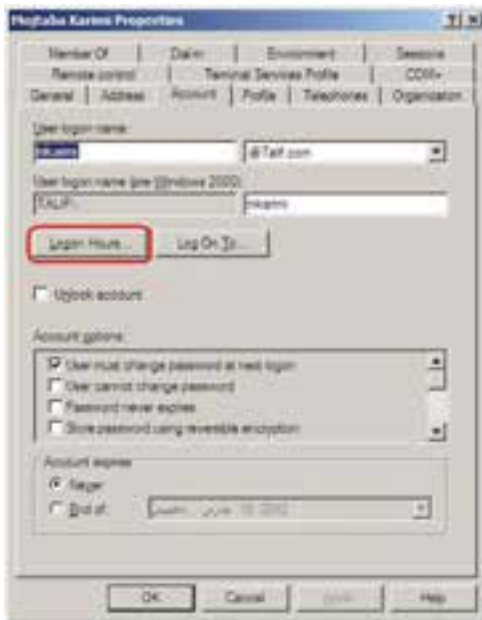
توجه داشته باشید در زبانه‌هایی که از قبل در حالت Stand - alone وجود داشته‌اند در حالت DC دارای مشخصات بیشتر و جزئی‌تر می‌باشند مانند زبانه General که نسبت به قبل، مشخصاتی مانند اداره، شماره تلفن، ایمیل و آدرس وب سایت به آن اضافه شده است (شکل ۱۲-۲۷).



شکل ۱۲-۲۷

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

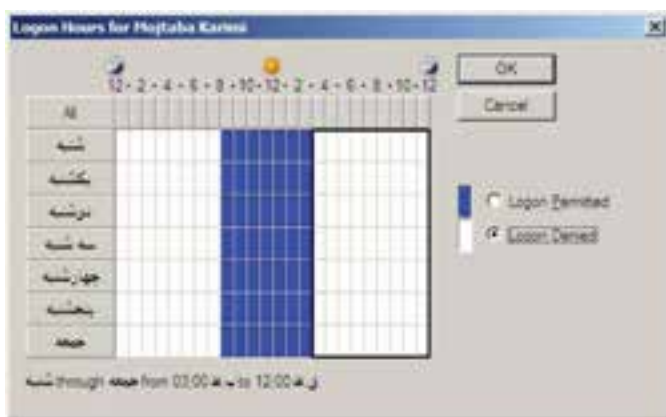
همان اسم کاربر به عنوان Logon Name در نظر گرفته می‌شود. در کادر بعدی نام دامنه را انتخاب کنید (Talif.com). اگر چند Domain داشته باشید لیست Domainها قابل انتخاب می‌باشد.



شکل ۱۲-۲۸

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.

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



شکل ۱۲-۲۹

با توجه به شکل ۱۲-۲۹ خانه‌هایی که به رنگ آبی پر شده‌اند بیانگر این می‌باشند که در آن ساعت از روز هفته، کاربر اجازه 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 ۱۲-۳۰

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 ۱۲-۳۱

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



شکل ۱۲-۳۲

در زبانه Organization می‌توان اطلاعات مربوط به مشخصات اداری کاربر از قبیل عنوان شغلی<sup>۱</sup>، گروه یا دپارتمان، نام شرکت و مدیر کاربر در شبکه و همچنین گزارشی راجع به کاربر را تعیین نمود.



شکل ۱۲-۳۳

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.

## ۱۲-۶- گروه‌ها در AD DS

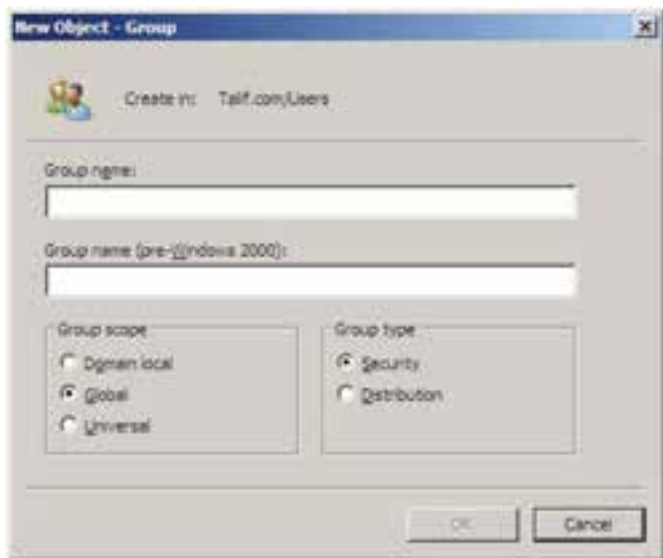
در AD کادر ایجاد گروه نیز با کادر گروه در Stand - alone متفاوت می‌باشد. در زمان ایجاد گروه باید نوع و دامنه گروه را مشخص کنید  
 Group Type (نوع گروه) که شامل دو قسمت می‌باشد:  
 الف) Security Group (گروه امنیتی): برای مجوز دادن استفاده می‌شود.  
 ب) Distribution Group (گروه توزیع): از آنها به عنوان لیست استفاده

می‌شود مانند استفاده از لیست برای ارسال ایمیل گروهی  
Group scopes (حوزه گروه) بیانگر محدوده عملکرد یک گروه می‌باشد که  
شامل سه نوع می‌باشد :

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

۲- **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.

۳- **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 ۱۲-۳۴

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 ۱۲-۳۵

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 ۱۲-۳۶



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 ۱۲-۳۷

در کادر ویژگی گروه‌ها، زبانه Managed By نسبت به Stand-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 ۱۲-۳۸

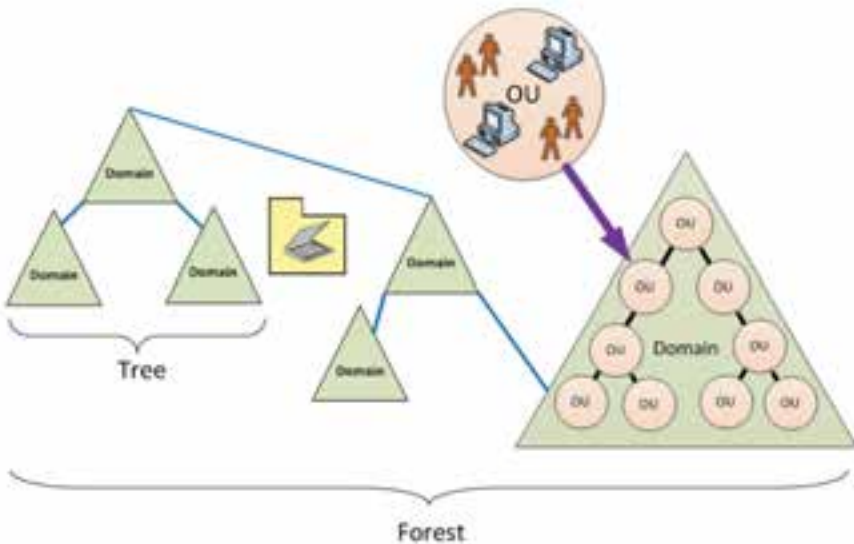
## ۱۲-۷- کاربرد Organizational Unit

در هر سازمان برای مدیریت ساده تر و ساختار یافته از یک سری واحدهای سازمانی استفاده می شود. به عنوان مثال استفاده از واحدهای مختلف نظیر کارگزینی، امور اداری، حسابداری، آموزش، روابط عمومی، IT و... در بسیاری از شرکت ها و سازمان ها معمول و مرسوم می باشد.

در هر واحد سازمانی تعدادی کارمند و مقداری منابع مثل رایانه، چاپگر و... یک مدیر برای آن واحد وجود دارد. برای مدیریت راحت تر شبکه، می توانید در یک Domain، واحدهای مختلف سازمانی ایجاد نمایید که به آنها اصطلاحاً Organizational Unit می گویند و به اختصار با نام OU به آنها اشاره می شود.

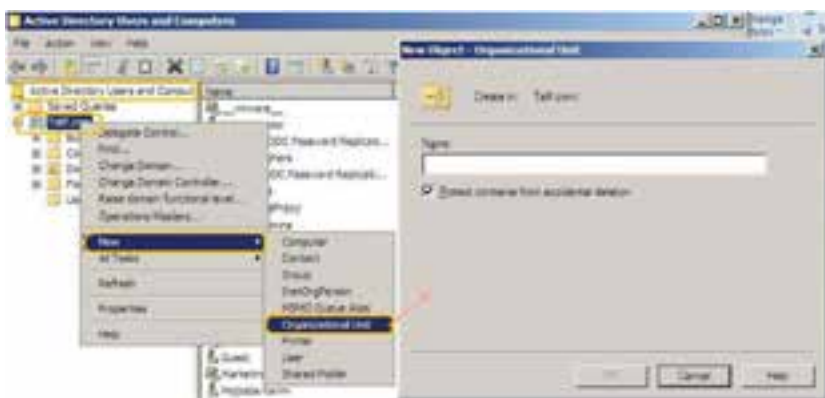
هر OU می تواند تعداد زیادی کاربر، رایانه، چاپگر و حتماً مدیر داشته باشد و حتی می توان سیاست های خاص برای آنها در نظر گرفت.

در واقع یک Domain را می توان 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 ۱۲-۳۹

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 ۱۲-۴۰).



شکل ۱۲-۴۰

در کادر New Object – 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



شکل ۱۲-۴۱

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 ۱۲-۴۱).

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 ۱۲-۴۲

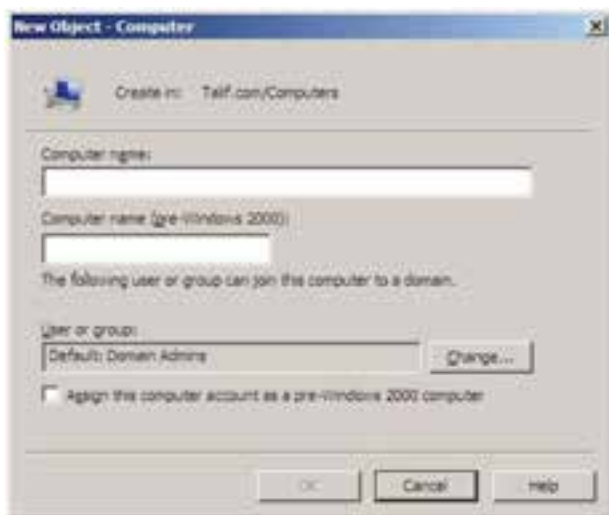
توجه داشته باشید با کپی کردن یک کاربر، پارامترهایی چون نام کشور - استان و شهر تنظیماتی چون Log on To Hours و Logon Account Expire از کاربر قبلی بر روی کاربر جدید نیز اعمال می‌شود.

## ۱۲-۸- 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.  
 ۱- کلیک راست بر روی Computers در Active Directory User and Computer  
 and انتخاب گزینه New و زیرگزینه Computers که کادر  
 Computer Newobject را برای ورود اطلاعات Computer Account نمایش  
 می‌دهد.



شکل ۴۳-۱۲

کافی است در کادر Computer name نام رایانه را وارد کنید.  
 ۲- از روی یک رایانه‌ای موجود در شبکه می‌توان یک حساب رایانه‌ای برای  
 اتصال به Domain ایجاد نمود.

## ۹-۱۲- 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)

۱- در Windows Vista یا Windows 7 بعد از انتخاب Properties باید بر روی گزینه Change Settings کلیک نمایید تا به

زبانه Computer Name دسترسی 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 برقرار شد کادر زیر برای دریافت نام کاربر و کلمه ورود نمایش داده می‌شود.



شکل ۱۲-۴۴

ه) 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 پیام خوش آمدگویی به دامنه Talif.com ظاهر می‌گردد.



شکل ۱۲-۴۵

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



شکل ۱۲-۴۶

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



شکل ۱۲-۴۷

ح) بعد از انجام تنظیمات فوق، رایانه سرویس گیرنده باید مجدداً راه‌اندازی 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.

## ۱۰-۱۲- روش های اعطای مجوز به کاربران

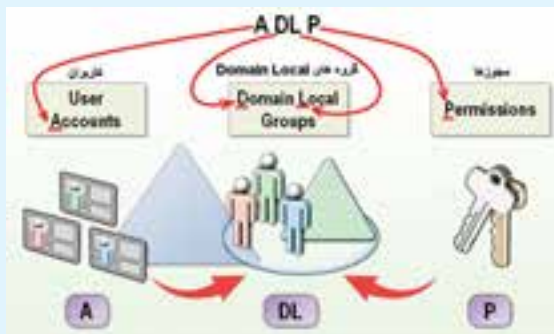
از روش های مختلفی برای اعطای مجوز به کاربران به کمک گروه ها می توان استفاده نمود. در این جا به چند روش اشاره می شود.

۱-۱۰-۱۲- روش AGP: در این روش کاربران (Account) ها در گروه های مختلف از نوع Global دسته بندی می شوند. همان طوری که قبلاً هم بیان شد، این دسته بندی از نظر نوع کار و محل جغرافیایی کاربران انجام می شود. سپس مجوز (permission) لازم به گروه ها اعطا می شود. از این روش در شبکه هایی که تعداد object ها زیاد نیست می توان استفاده کرد.

۲-۱۰-۱۲- روش ADLP: در این روش می توانید کاربران (Account) ها را در گروه های مختلف از نوع Domain Local دسته بندی کنید. سپس به گروه های مورد نظر مجوز لازم اعطا کنید (شکل ۴۸-۱۲).



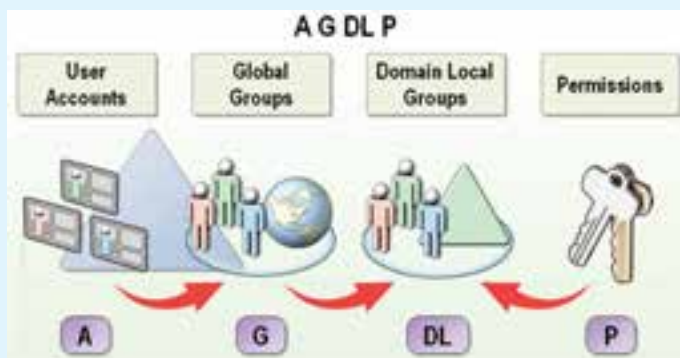
شکل ۴۸-۱۲



شکل ۴۹-۱۲



۳-۱۰-۱۲-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 در آورید.



شکل ۵۰-۱۲

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

### ۱۱-۱۲-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.

#### ۱-۱۱-۱۲- گروه‌های Built in Global 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 در می‌آید.

■ **Domain Admins**: اعضای این گروه می‌توانند Domain را مدیریت کنند

و به عنوان مدیر Domain شناخته می‌شوند. فقط Administrator همان Domain به

صورت پیش فرض عضو این گروه می باشد.

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



شکل ۱۲-۵۱



شکل ۱۲-۵۲



شکل ۱۲-۵۳

۲-۱۱-۱۲- گروه های **Built in Domain Local** : این گروه ها در پوشه Built in در ابزار Active Directory Users and Computers قرار دارند عبارتند از :

■ **Administrators** : اعضای این گروه می توانند DC ها را مدیریت کنند و

تمامی مجوزها روی این رایانه‌ها قرار خواهند داشت.

### ■ **Server operators** : اعضای این گروه می‌توانند در انجام بعضی از کارهای

مدیریتی به مدیر شبکه کمک کنند به عنوان مثال می‌توانند عملیات زیر را روی DC‌ها انجام دهند.

○ Log on کردن

○ Shut down کردن

○ قالب بندی کردن درایوها

○ تغییر ساعت

### ■ **Account operators** : اعضای این گروه می‌توانند عملیات مدیریتی همچون

ایجاد، حذف و ... را روی Account‌ها (شامل : کاربران، گروه‌ها و رایانه) انجام دهند. به عنوان 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.

### ۳-۱۱-۱۲ 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.

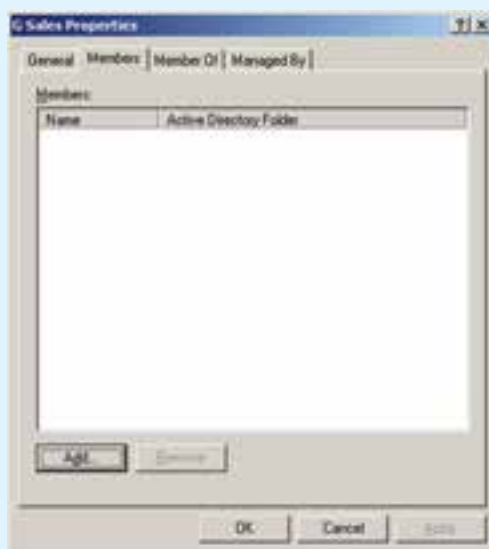
## ۱۲-۱۲- پیاده‌سازی روش‌های مختلف اعطای مجوز به کاربران

۱-۱۲-۱ پیاده‌سازی روش **AGP**: در این روش ابتدا يك گروه از نوع

Global به همان شیوه‌ای که در مراحل قبل یاد گرفتید با نام G sale ایجاد کنید.

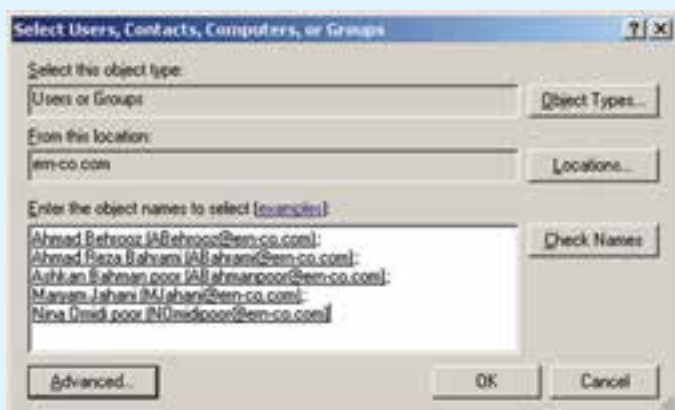
سپس مطابق شکل ۱۲-۵۴ از این گروه Properties گرفته و در زبانه Members

لیست اعضای این گروه را مشاهده می‌کنید.



شکل ۱۲-۵۴

حال اگر روی کلید Add کلیک کنید پنجره شکل ۱۲-۵۰ 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 گزینه Find Now کلیک نمایید تا لیستی از کاربران و گروه‌ها نمایش داده شوند.



شکل ۱۲-۵۵

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.



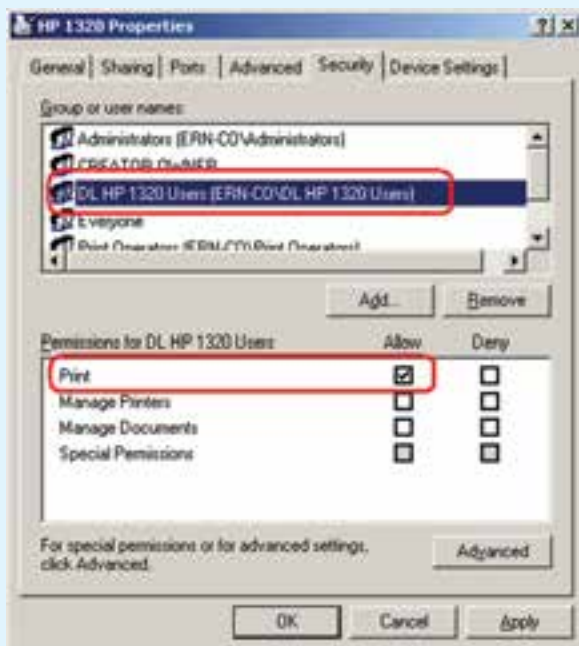
شکل ۱۲-۵۶

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 به نام 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 ۱۲-۵۶ 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.

۲-۱۲- 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.

۳-۱۲- پیاده‌سازی روش AGDLP: در این روش ابتدا یک دسته‌بندی منطقی برای کاربران در نظر 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 ۱۲-۵۷).



شکل ۱۲-۵۷

حال تمامی گروه‌های از نوع Global را که قرار است مجوز Print روی این چاپگر داشته باشند، به عضویت گروه DL HP ۱۳۲۰ users درآوردید (شکل ۵۸-۱۲).



شکل ۵۸-۱۲

### خودآزمایی و پژوهش

- ۱- Domain Controller چیست؟ وظایف و ویژگی‌های آن‌ها را شرح دهید.
- ۲- Forest چیست؟
- ۳- Child Domain را با ذکر مثال تعریف کنید.
- ۴- آیا یک رایانه می‌تواند به طور همزمان عضو چند Domain باشد؟
- ۵- بررسی کنید که چه روش دیگری برای نصب Active Directory وجود دارد؟
- ۶- تفاوت Security Group و Distribution در چیست؟

- ۷- چگونه می‌توان در یک سطح وزارتخانه برای کاربران مجوزهای لازم را صادر کرد؟
- ۸- 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.
- ۹- انواع Account را نام ببرید.
- ۱۰- کاربرد Account Expires چیست و رابطه آن را Password never expires بنویسید.
- ۱۱- 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 سرویس‌گیرنده‌ها بتواند Log on کند.
- ج) بتواند چاپگر را مدیریت کند.
- د) بتواند تنظیمات شبکه، IP سیستم‌ها را عوض کند.
- ه) بتواند از طریق Dial up به شبکه متصل شود.
-