



دانشگاه آزاد اسلامی

واحد پارس آباد مغان

گروه کامپیوتر

جزوه آموزشی

کارگاه سیستم عامل شبکه (بخش اول)

آموزش و تنظیم ویندوز ۲۰۰۳ سرور

مدرس: استاد شاپور جودی

تهیه و تنظیم: وحید بارگر

نیمسال دوم ۸۹-۸۸

فهرست مطالب

۱. جزئیات بخش اول:

- ۱-۱- تاریخچه ویندوز ۲۰۰۳ سرور و مقایسه با ۲۰۰۰ سرور
- ۱-۲- ویژگیهای ۲۰۰۳ سرور
- ۱-۳- نسخه Windows Server Enterprise Edition 2003 و شناخت نیازمندیهای سخت افزاری آن
- ۱-۴- شروع به نصب ویندوز ۲۰۰۳ سرور
- ۱-۴-۱- بررسی نصب ویندوز ۲۰۰۳ سرور به عنوان اولین سیستم عامل بر روی کامپیوتر
- ۱-۴-۲- بررسی نصب ویندوز ۲۰۰۳ سرور در کنار سیستم عامل دیگر

۲. جزئیات بخش دوم:

- ۲-۱- Active Directory
- ۲-۲- اشیاء و صفات در A.D
- ۲-۳- اجزای A.D
- ۲-۴- بررسی دامنه، درخت و جنگل
- ۲-۵- ارتباط Trust
- ۲-۶- بررسی ویژگیهای A.D
- ۲-۷- شروع به نصب A.D
- ۲-۷-۱- تنظیمات لازم قبل از نصب A.D
 - ۲-۷-۱-۱- بررسی نصب کارت شبکه
 - ۲-۷-۱-۱- بررسی IP سرور
 - ۲-۷-۲- نحوه نصب A.D از طریق DCpromo
 - ۲-۷-۳- نحوه نصب A.D از طریق پنجره Manage Your Server
 - ۲-۸- نحوه حذف A.D

۳. جزئیات بخش سوم:

- ۳-۱- بررسی تنظیم Domain بر روی کلاینتها
 - ۳-۱-۱- تنظیم آدرس IP کلاینت ها با سرور
 - ۳-۱-۲- Join کردن کلاینت به سرور
 - ۳-۱-۳- تست کردن ارتباط بین سرو و کلاینت (Ping)
 - ۳-۱-۴- بررسی خارج کردن کلاینت از Domain

۳-۲- بررسی DHCP در کلاینت و ۲۰۰۳ سرور

۳-۲-۱- تنظیم DHCP بر روی سرور برای پخش آدرس IP

۳-۲-۲- تنظیم DHCP بر روی کلاینت برای دریافت آدرس IP

۳-۳- بررسی ویژگیهای MMC

۳-۴- بررسی افزودن کامپیوتر در ۲۰۰۳ سرور

۴. جزئیات بخش چهارم:

۴-۱- بررسی ویژگیهای standalone

۴-۲- بررسی کاربران پیش فرض

۴-۳- بررسی ایجاد کاربر جدید

۴-۳-۱- بررسی کلمه رمز کاربر جدید

۴-۳-۲- بررسی قفل (lock) کردن کاربر

۴-۴- بررسی نحوه ورود از کلاینت

۴-۵- مشاهده مشخصات کاربران و تغییر در آنها

۴-۵-۱- محدود کردن زمان ورود کاربران

۴-۵-۲- محدود کردن ورود کاربران از کامپیوترها

۴-۵-۳- محدودیت زمانی برای فعال بودن کاربر

۴-۵-۴- اجازه ورود کاربران از راه دور به سیستم

۴-۶- جستجو در AD

۵. جزئیات بخش پنجم:

۵-۱- نصب فایل سرور

۵-۲- تنظیمات Disk Quota در ویندوز ۲۰۰۳ سرور

۵-۳- دستیابی آسان به پوشه اشتراکی (Map Network Drive)

۵-۴- حذف فایل سرور

۶. جزئیات بخش ششم:

۶-۱- کاربران Organizational Unit

۶-۲- تکثیر کاربران (برای مطالعه)

۶-۳- Group Policy در ویندوز ۲۰۰۳

۶-۴- افزودن مدیر جدید در سطح دامنه

۶-۵- محدود کردن مدیران

۶-۶- مدیریت مجوزها و بررسی انواع مجوز

۷. جزئیات بخش هفتم:

۷-۱- امنیت در ویندوز ۲۰۰۳ سرور

۷-۱-۱- امنیت با Event viewer

۷-۱-۲- امنیت با Syskey

۷-۱-۳- امنیت با Screen Server

۷-۱-۴- امنیت با Domain Security Policy

۷-۱-۴-۱- سیاست های امنیتی کلمه عبور

۷-۱-۴-۲- سیاست های امنیتی محلی

۷-۱-۴-۳- سیاست های امنیتی ثبت رخدادها

۷-۱-۵- امنیت با Security Configuration Wizard

۸. جزئیات بخش هشتم:

۸-۱- پشتیبان گیری

۸-۱-۱- مشخص کردن مسائلی قبل از پشتیبان گیری

۸-۱-۱-۱- تعیین مجوز پشتیبان گیری

۸-۱-۱-۱-۱- Backup Operators دادن مجوز

۸-۱-۱-۲- تعیین نحوه پشتیبان گیری

۸-۱-۱-۳- تعیین نوع اطلاعات پشتیبان گیری

۸-۱-۲- شروع به پشتیبان گیری

۸-۱-۲-۱- پیکربندی تنظیمات Backup

۸-۱-۲-۲- ایجاد یک پشتیبان گیری

۸-۱-۲-۳- زمانبندی کردن پشتیبان گیری

۸-۱-۲-۴- استفاده از Automated System Recovery Wizard

۸-۱-۲-۵- پشتیبان گیری از A.D

۸-۱-۳- بازیابی Backup

۹. جزئیات بخش نهم:

۹-۱- دستیابی به سرور از راه دور

۹-۱-۱- بررسی تنظیمات سرور برای دستیابی از راه دور

۹-۱-۱-۱- دادن نقش Remote Access Server

۹-۱-۱-۲- بررسی ایجاد Connection برای دستیابی از راه دور در سرور

۹-۱-۱-۳- بررسی تعیین اجازه برای دستیابی از راه دور

۹-۱-۲- بررسی تنظیمات کلاینت برای دستیابی از راه دور

۹-۱-۲-۱- بررسی ایجاد Connection برای دستیابی از راه دور در کلاینت

۹-۱-۲-۲- وصل شدن به سرور از راه دور

۱. جزئیات بخش اول:

همچنان که می دانیم ویندوز ۲۰۰۳ سرور بیشتر در یک محیط شبکه ای استفاده می شود و برای مدیریت چندین کاربر و چندین کامپیوتر استفاده می شود پس ابتدا بهتر است با مفاهیم شبکه آشنایی کوتاهی داشته باشیم.

شبکه ها از دید بعد جغرافیایی

LAN -

MAN -

WAN -

شبکه ها از دید اولویت کامپیوترها

- شبکه های نظیر به نظیر : شبکه هایی هستند که در آنها کامپیوترهای موجود در شبکه به یکدیگر اولویت خاصی دارند و در کل هر کامپیوتر شبکه هم می تواند به عنوان یک کلاینت عمل کند و هم به عنوان سرور . فرض کنید PC2 داده ای را از PC5 درخواست می کند که به صورت اشتراکی بر روی PC5 قرار دارد در این حالت PC5 به عنوان فراهم کننده سرویس (سرور) مطرح می شود و PC2 نیز از آن استفاده می کند که به عنوان مصرف کننده (کلاینت) مطرح می شود . حال پس از چند دقیقه این بار تحت شبکه PC5 داده ای را از PC2 درخواست می کند ، در این حالت PC5 به عنوان کلاینت و PC2 به عنوان فراهم کننده مطرح می شود .

بر روی کامپیوترهای موجود در شبکه نظیر به نظیر ، از سیستم عامل هایی مانند XP ، 98 و 2000 استفاده می شود. یعنی این سیستم عامل ها نیاز به عملیات خاص مدیریتی ندارند و فقط داده ها را در شبکه به اشتراک می گذارند .

مهمترین ایراد شبکه های نظیر به نظیر این است که بر روی منابع اشتراکی ، رمزهای عبور کاربران ، محدودیت دسترسی به منابع خاص شبکه، مدیریت متمرکز و کنترل شده ای وجود ندارد .

شبکه مبتنی بر سرور :

همچنان که از نام این شبکه پیداست در این شبکه یک کامپیوتر با نام سرور وجود دارد که فراهم کننده سرویس ها و خدمات شبکه لی می باشد در این مدل یک یا چند کامپیوتر به عنوان تامین کننده خدمات مشخص می شود که قابلیت های سخت افزاری این کامپیوترها ، بالاتر از یک کامپیوتر معمولی می باشد ، و ممکن است چندین کامپیوتر به عنوان استفاده کننده یا کلاینت در سطح شبکه قرار داشته باشند که از خدمات و سرویس های سرورها با صلاحدید مدیر شبکه می توانند استفاده کنند . اگر بخواهیم شبکه موجود در شکل ۱ را که یک شبکه نظیر به نظیر می باشد ، به یک شبکه مبتنی بر سرور تبدیل کنیم شاید نیازی به تغییرات سخت افزاری نباشد . کافی است یک کامپیوتر جدید با ویژگی سرور خریداری کرد و آن را به یک پورت دیگر هاب متصل کنیم .

حال سوال اینجاست که پس چه چیز این شبکه را تبدیل به یک شبکه مبتنی بر سرور می کند ؟

۱-۱- تاریخچه ویندوز ۲۰۰۳ سرور و مقایسه با ۲۰۰۰ سرور:

مایکروسافت برای این منظور بخش‌های زیادی از سیستم‌عامل ۲۰۰۰ را اصلاح و برخی از قسمت‌های آن از جمله سرویس اینترنتی IIS را بازنویسی و بازسازی کرده است. این شرکت برای اطمینان حاصل کردن از بهبود راندمان نرم‌افزار ۲۰۰۳ مدت تست بتای این محصول را به‌طور خاص افزایش داد و پس از عرضه چندین نسخه آزمایشی سرانجام محصول نهایی را در آستانه فصل دوم سال ۲۰۰۳ به بازار عرضه کرد. ویندوز ۲۰۰۳ یک ویندوز بسیار سبک و سریع است. در صورتی که ویندوز ۲۰۰۰ موجود خود را به نسخه ۲۰۰۳ ارتقاء دهید، پس از نصب تمام سرویس‌هایی که روی سیستم‌عامل قبلی در حال اجرا بوده‌اند، به‌کار خود ادامه خواهند داد و تنها قابلیت‌ها و اصلاحات جدید روی آن‌ها اعمال خواهند شد. اما اگر یک نسخه کاملاً تازه از ابتدا روی کامپیوتر نصب کنید، به‌طور پیش فرض اغلب سرویس‌های کاربردی (و نه زیربنایی) سیستم‌عامل (حدود بیست و چند سرویس از جمله سرویس‌های وب، FTP، SMTP و Active Directory) خاموش هستند. این مهم‌ترین دلیل سبک بودن و چابکی سرور در بدو امر است. یکی از تغییرات محسوس ویندوز ۲۰۰۳ نسبت به نسخه قبلی، نزدیک‌تر شدن قابلیت‌های آن به خصوصیات سایر سرورهای موجود در بازار (مانند یونیکس و لینوکس) و دورتر شدن سیستم‌عامل از پاره‌ای ویژگی‌های ویندوزهای معمولی مایکروسافت (OS Desktop Windows) است.

۱-۲- ویژگیهای ۲۰۰۳ سرور:

- ابزارهای جدید مدیریت از راه دور
- خدمات نصب راه دور (RIS) در سرور
- Remote Desktop
- Remote Assistance
- مدیریت سرویس دهنده‌های بدون سر (کامپیوترهایی که بدون مانیتور و... میباشند)
- ویژگیهای جدید اکتیو دایرکتوری (Active Directory)
- راههای جدید پیمایش و مدیریت اکتیو دایرکتوری
- پارتیشن دایرکتوری کاربردی
- بهبود تکرار (Replication)
- تغییر نام AD و دامنه‌ها
- بهبودهای ایجاد شده در قابلیت دسترسی و قابلیت اطمینان
- Automated System Recovery
- Emergency Management services
- User State Migration Tool

۳-۱- نسخه 2003 Windows Server Enterprise Edition و شناخت نیازمندیهای سخت افزاری آن:

"Windows Server Enterprise Edition 2003" که بر پایه همان نسخه استاندارد و با افزودن قابلیت های مهمی برای رفع نیازهای برنامه های کاربردی حساس تجاری تولید شده است.

مشخصات رایانه مورد نیاز به شرح ذیل می باشد:

پردازنده و پردازنده	پردازنده 133 MHz برای رایانه های شخصی بر مبنای پردازنده x86 و یا 733MHz برای پردازنده های "Itanium" با قابلیت پشتیبانی ۸ پردازنده ۳۲ یا ۶۴ بیتی .
حافظه	حداقل 128MB ، و حداکثر 32GB برای پردازنده های ۳۲ بیتی x86 و 64GB برای پردازنده های ۶۴ بیتی "Itanium" .
دیسک سخت	1.5GB فضای خالی برای پردازنده های x86 و 2GB برای پردازنده های "Itanium" . برای نصب در شبکه فضای بیشتری مورد نیاز خواهد بود.
دیسک گردان	دیسک گردان "CD-ROM" و یا "DVD-ROM" .
نمایشگر	"VGA" یا سخت افزار دیگری که قابلیت تغییر کنسول داشته باشد
غیره	نسخه ۶۴ بیت این ویرایش فقط بر روی سیستم هایی بر پایه پردازنده های ۶۴ بیتی ایتانیوم شرکت اینتل کار کرده و بر روی سیستم های ۳۲ بیتی به درستی نصب نخواهند شد.

ویندوز ۲۰۰۳ سرور به دو صورت ۳۲ بیتی و ۶۴ بیتی عرضه شده است که بر حسب نیاز باید یکی از نسخه های فوق را بر روی سیستم خود نصب کنیم. باید توجه داشته باشیم که اگر ویندوز ۲۰۰۳ مورد استفاده بر روی سرور ۶۴ بیتی باشد، باید نرم افزارهای نصب شده بر روی سرور نیز ۶۴ بیتی باشند (مجموعه Office ۶۴ بیتی و...)

بهتر است در راه اندازی شرکت های کوچک از نسخه ۳۲ بیتی استفاده شود. چون بیشتر نرم افزارهای موجود ۳۲ بیتی می باشد.

ممکن است بر روی سیستم دو نوع سیستم فایل FAT و NTFS داشته باشیم، ویندوز ۲۰۰۳ سرور بهتر است بر روی پارتیشن NTFS نصب شود، چون بیشتر امکانات ۲۰۰۳ سرور که در بخش های بعد توضیح خواهیم داد، بر روی NTFS عمل می کنند و نمی توانند بر روی FAT عمل کنند.

۴-۱- شروع به نصب ویندوز ۲۰۰۳ سرور:

پس از آنکه با قابلیت‌ها، ویژگی‌ها و حداقل نیازمندی‌های ویندوز ۲۰۰۳ سرور آشنا شدیم، حال می‌خواهیم بر روی کامپیوتر خود شروع به نصب ویندوز ۲۰۰۳ سرور نصب کنیم. ابتدا باید بدانیم چرا بر روی سیستم ۲۰۰۳ را نصب کنیم؟ و هدف از نصب آن چه می‌باشد؟ یعنی یک طراحی قبل از نصب داشته باشیم که در آن اهداف، تعداد کاربران، تعداد کامپیوترها به همراه آینده اندیشی و احتمال رشد شبکه مشخص باشد.

یک سوال: آیا ویندوز ۲۰۰۳ بر روی هر تک تک کامپیوترها نصب خواهد شد؟
خیر، ویندوز ۲۰۰۳ سرور را بر روی کامپوتری که می‌خواهیم خدمات و سرویس‌های مدیریتی و شبکه‌ای را فراهم سازد نصب می‌شود و بر روی کامپیوترهای دیگر کافی است نسخه‌هایی مانند XP وجود داشته باشد.

شروع به نصب:

قبل از نصب ویندوز سرور باید تعیین کنید که آیا می‌خواهید ویندوز ۲۰۰۳ سرور را به عنوان اولین سیستم عامل بر روی سیستم تان نصب کنید یا می‌خواهید ویندوز را در کنار سیستم عامل دیگر مانند XP نصب کنید. در اینجا اول نحوه نصب ویندوز ۲۰۰۳ سرور به عنوان اولین سیستم عامل را توضیح داده و در ادامه طریقه نصب ویندوز در کنار سیستم عامل دیگر (XP) را توضیح داده ایم.

نکته: اگر بر روی سیستم ویندوز XP وجود داشته باشد می‌توان از داخل آن ۲۰۰۳ سرور را نصب کرد اما نمی‌توان از داخل ویندوز ۲۰۰۳ سرور بر روی سیستم XP را نصب کنیم.

۱-۴-۱- بررسی نصب ویندوز ۲۰۰۳ سرور به عنوان اولین سیستم عامل بر روی کامپیوتر:

۱ - CD ویندوز را در CD-ROM بگذارید.

۲ - با توجه به اینکه CD بوت ایبل است به محض روشن کردن رایانه با فشردن دکمه Del وارد برنامه Setup سیستم می‌شویم.

در قسمت تعیین دستگاه‌های بوت کننده، نخستین گزینه را بر روی CD ROM قرار داده، با فشردن کلید F10 سپس Y و در آخر Enter تغییرات اعمال شده در برنامه Setup ذخیره و رایانه دوباره Boot می‌شود.

۳ - هنگامی که پیام Press any key to boot from CD-Rom دیده شد، دکمه‌ای را می‌فشاریم تا رایانه از روی CD بوت شده و پنجره ابتدایی نصب ویندوز ظاهر گردد.

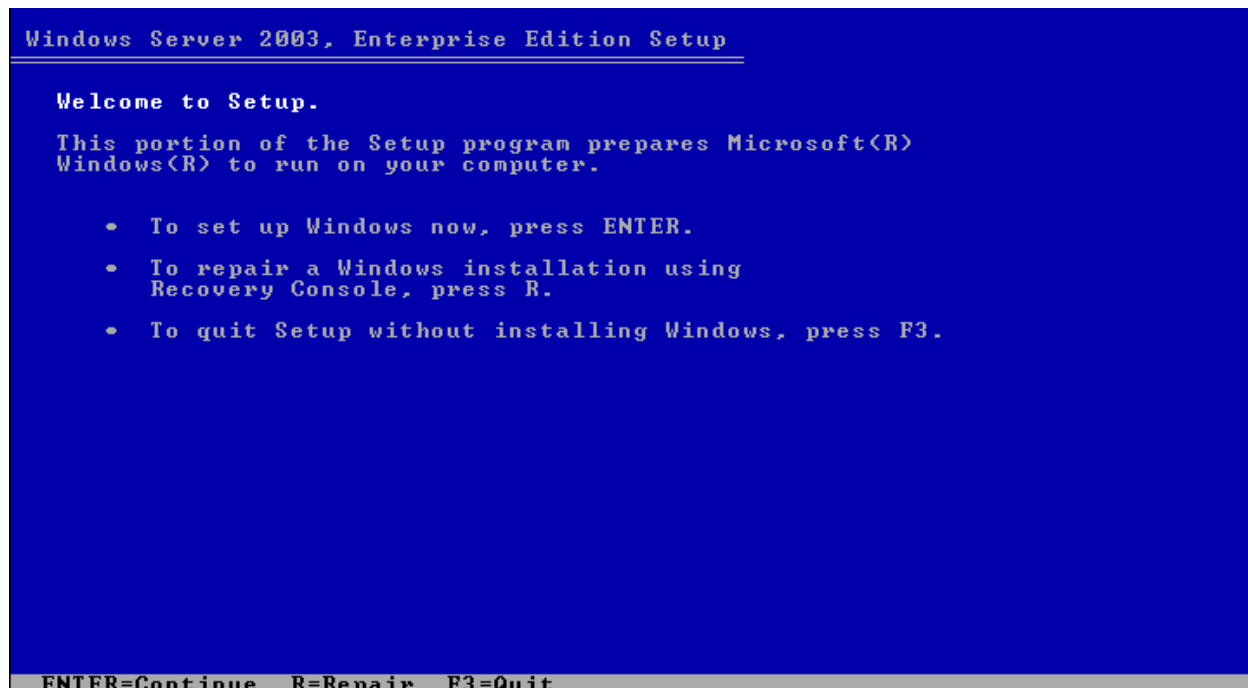
در این حال رایانه در حال بارگذاری راه اندازهای ویژه برای نصب ویندوز می‌باشد.



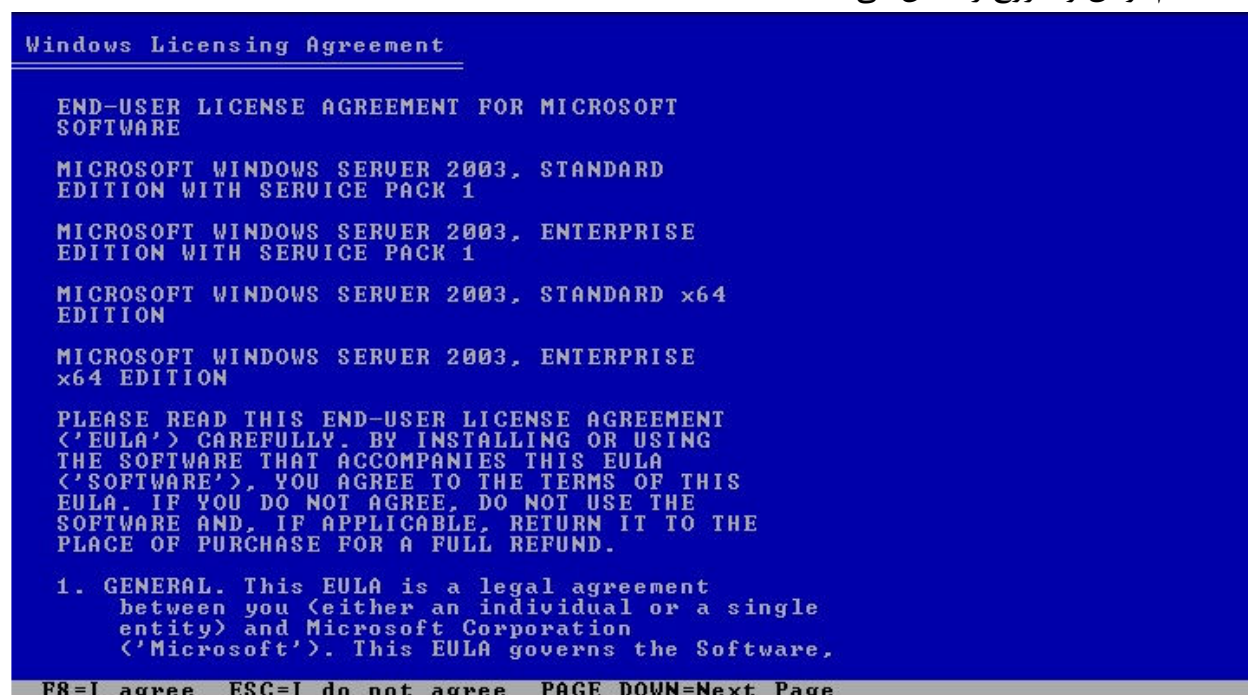
۴- سیستم در حال load (بار گذاری کردن) فایلها برای نصب وینوز می باشد.



۵ - در پنجره بعدی صفحه خوش آمد گویی ویندوز سرور ۲۰۰۳ را نشان می دهد که برای ادامه نصب کلید Enter را فشار می دهیم.

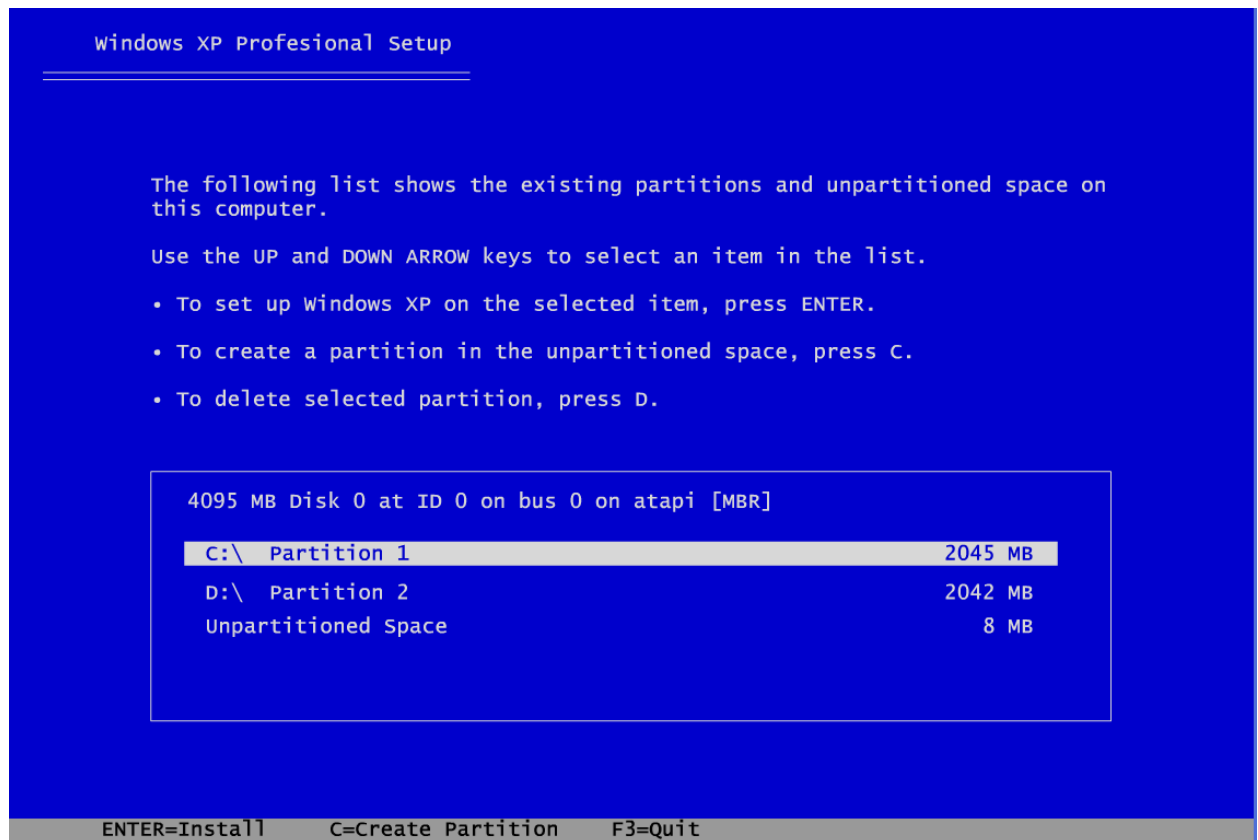


۶- سپس پنجره ای که حاوی توافق نامه و مجوز استفاده از این نسخه ویندوز است ظاهر می گردد. بدیهی است برای ادامه نصب باید موافقت خود را با زدن F8 اعلام نماییم. کلیدهای Page Up و Page Down کل متن را نشان خواهند داد. کلید Esc عدم توافق و خروج را نشان می دهد.

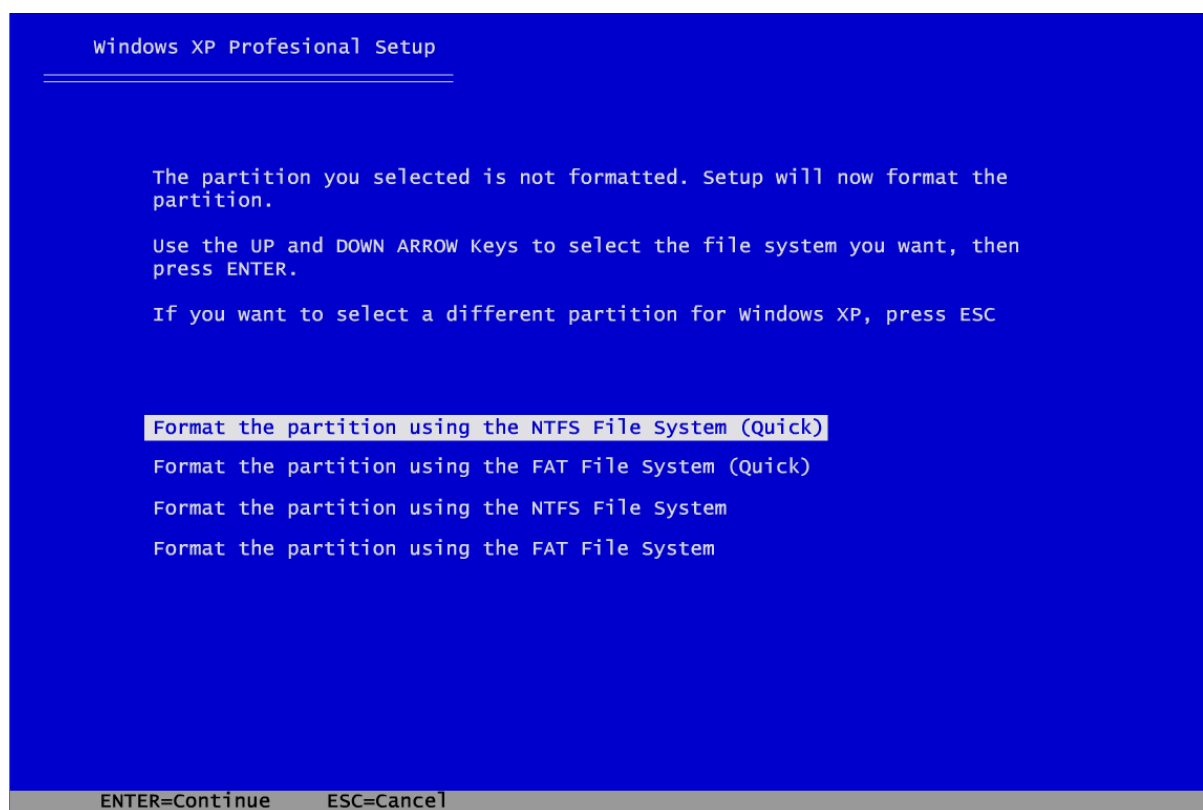


۷ - در این صفحه باید درایو مناسب برای نصب ویندوز را انتخاب کنیم.

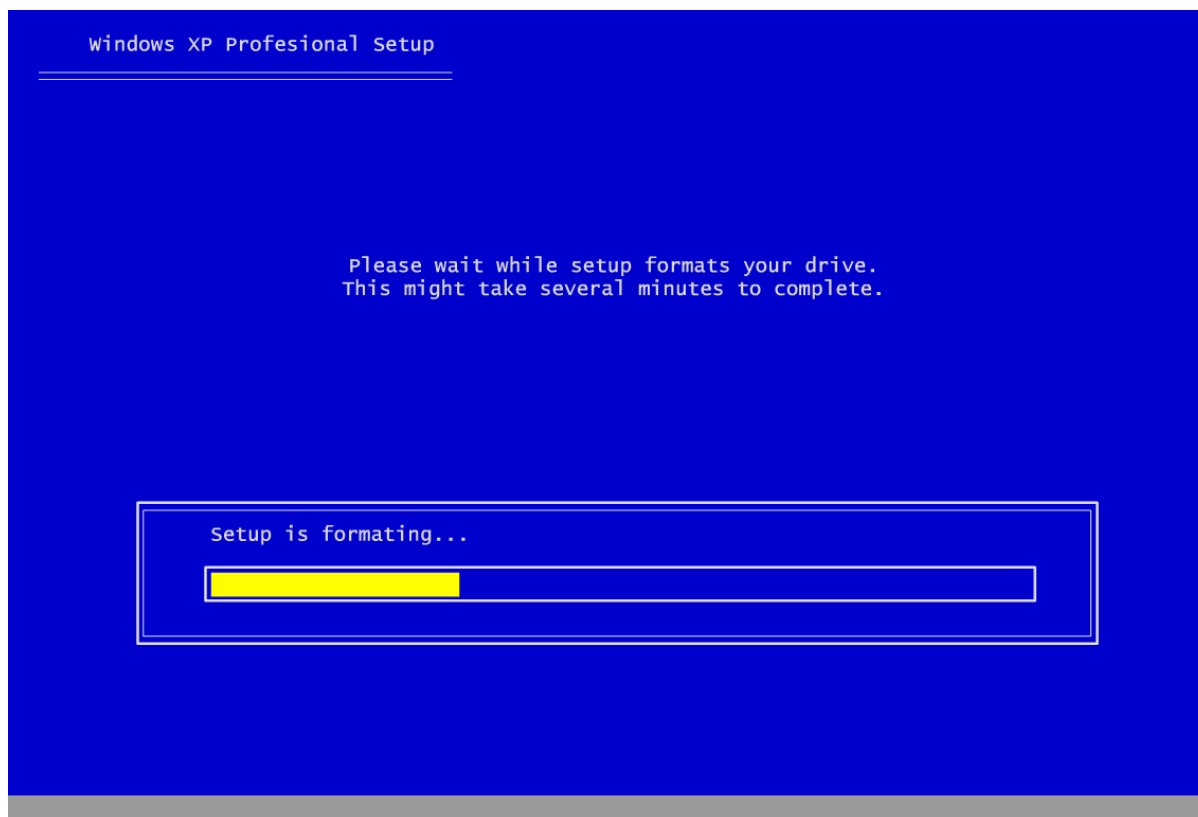
۸ - در اینجا ما موافق با نصب ویندوز بر روی پارتیشن ایجاد شده از قبل که اطلاعات مربوط به آن نشان داده شده هستیم کلید Enter را می زنیم.



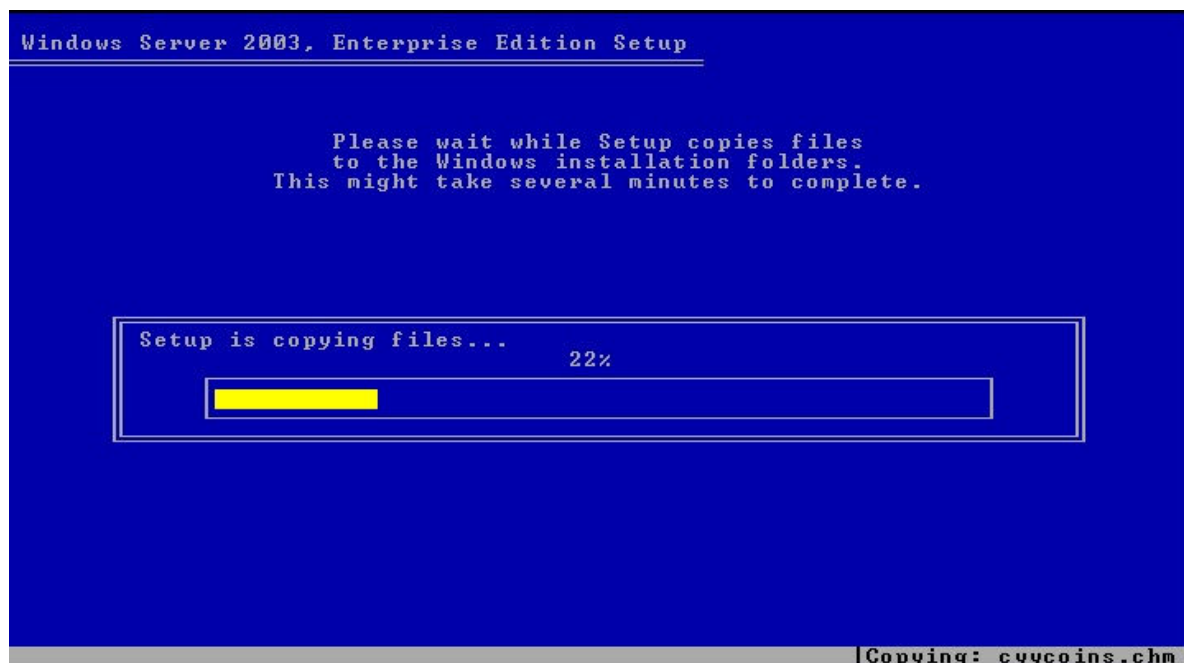
۹ - در این صفحه باید نوع فرمت ویندوز را مشخص کنیم که چون در ویندوز سرور ۲۰۰۳ بحث active directory وجود دارد پس باید فرمت از نوع NTFS باشد. اولین گزینه فرمت درایو را به صورت سریع و دومین گزینه فرمت درایو را به صورت عادی انجام میدهد.



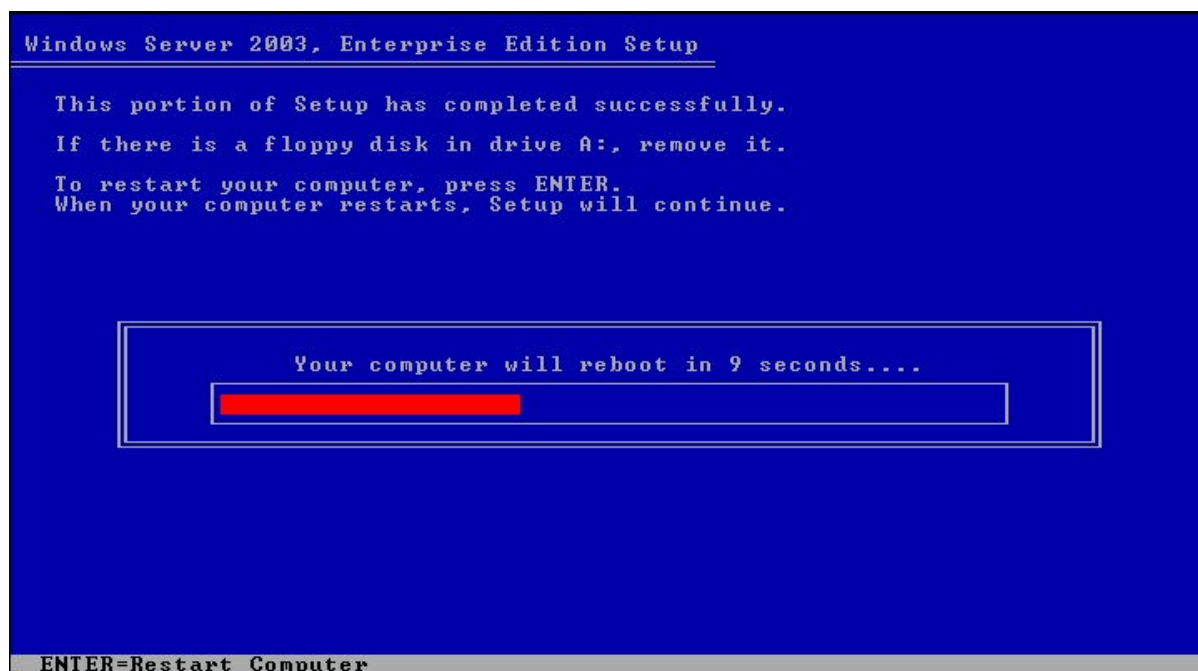
۱۰ - پس از انتخاب نوع فرمت و با فشردن کلید Enter ، Setup برنامه شروع به فرمت کردن درایو کرده و شروع به نصب فایل های مورد نیاز برای Boot شدن دوباره سیستم بر روی پارتیشن انتخابی می کند.(شاید از شما بخواهد برای فرمت کردن کلید F را فشار دهید)



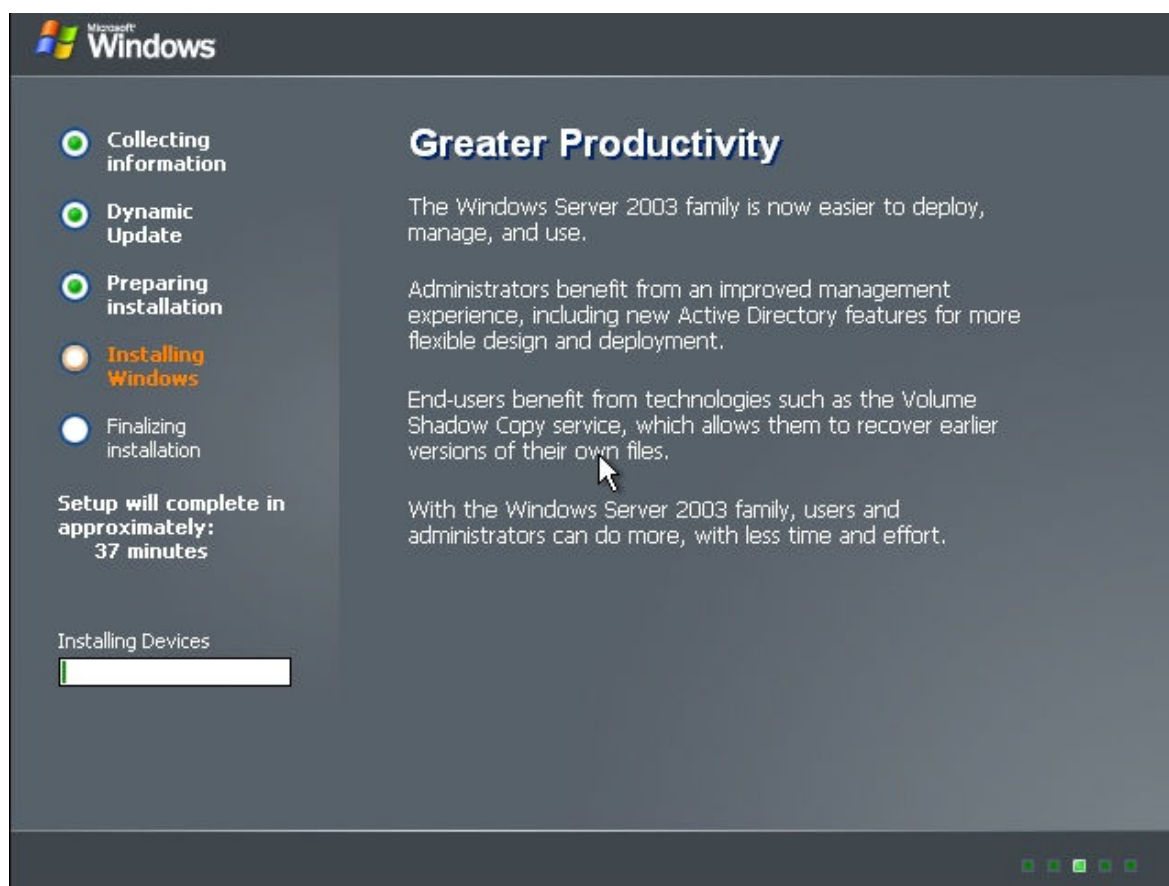
۱۱ - در مرحله بعدی برنامه Setup اطلاعات متنوعی را برای نصب خود تولید کرده و رایانه را مورد ارزیابی قرار می دهد.



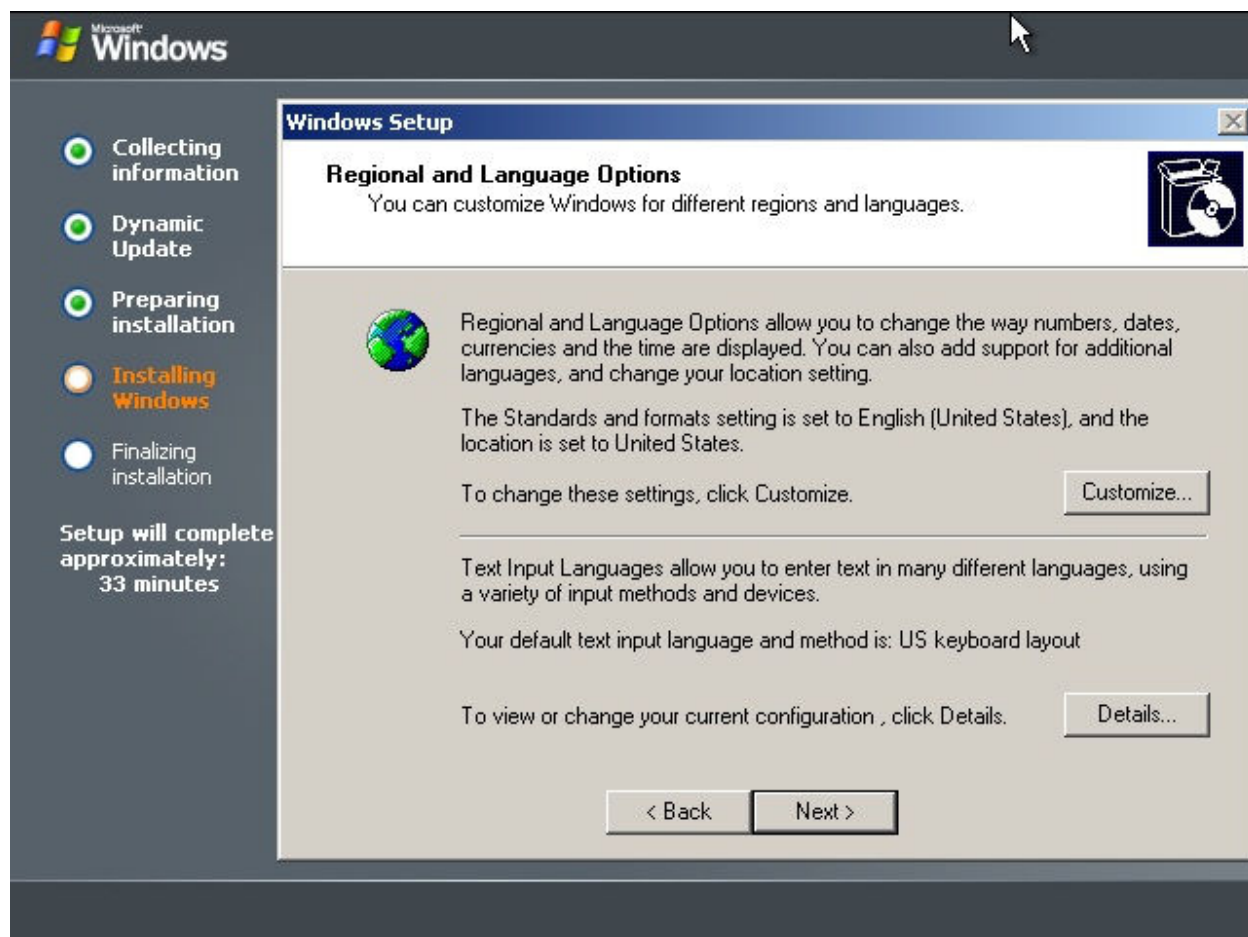
۱۲ - در این مرحله برنامه آماده راه اندازی دوباره - Restart / Reboot - سیستم می شود. بهتر است ۱۵ ثانیه درنگ کنیم تا این کار بصورت خودکار صورت پذیرد.



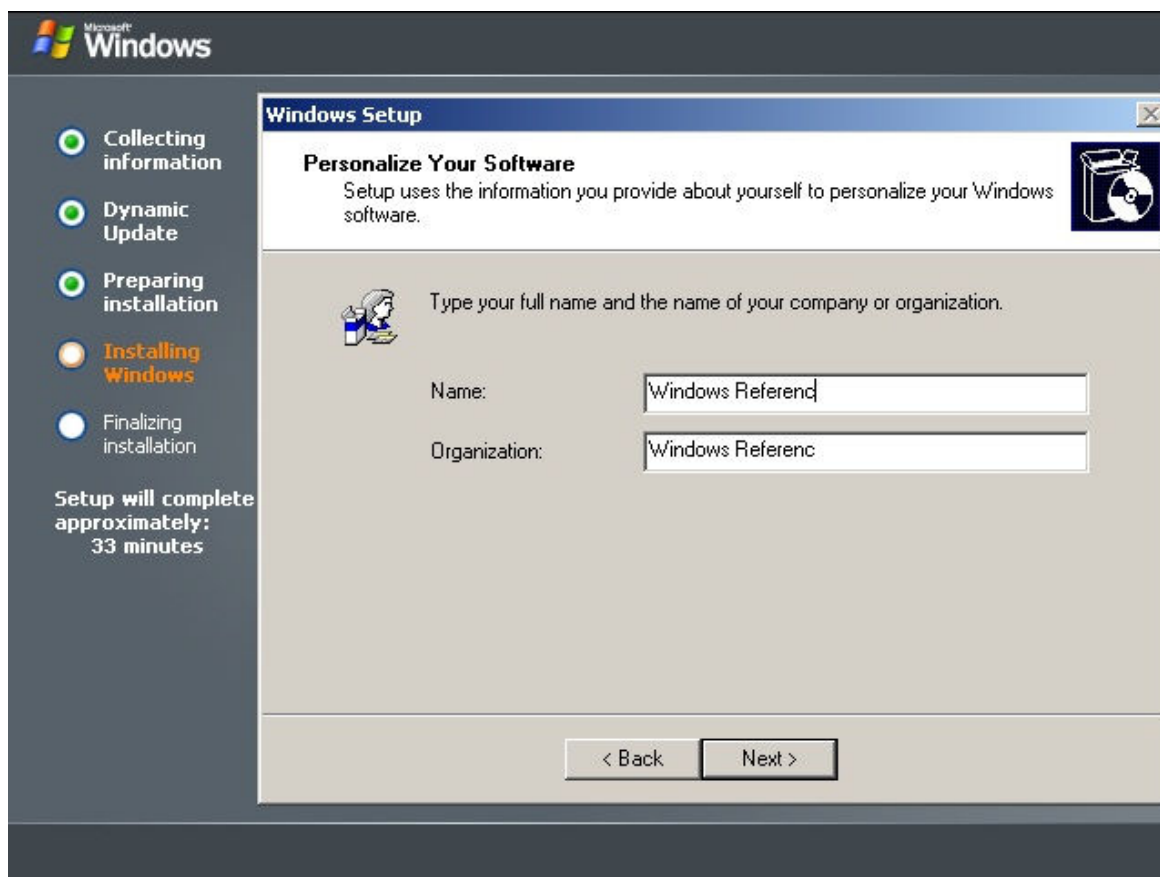
۱۳ - پس از آغاز دوباره کار رایانه ، صفحه بوت شدن ویندوز را خواهیم دید.(اگر تاکنون ویندوز XP نصب کرده باشید صفحه بعدی به چشمتان آشنا خواهد آمد ، تنها تفاوت تغییر رنگ آبی ویندوز XP به طوسی می باشد)



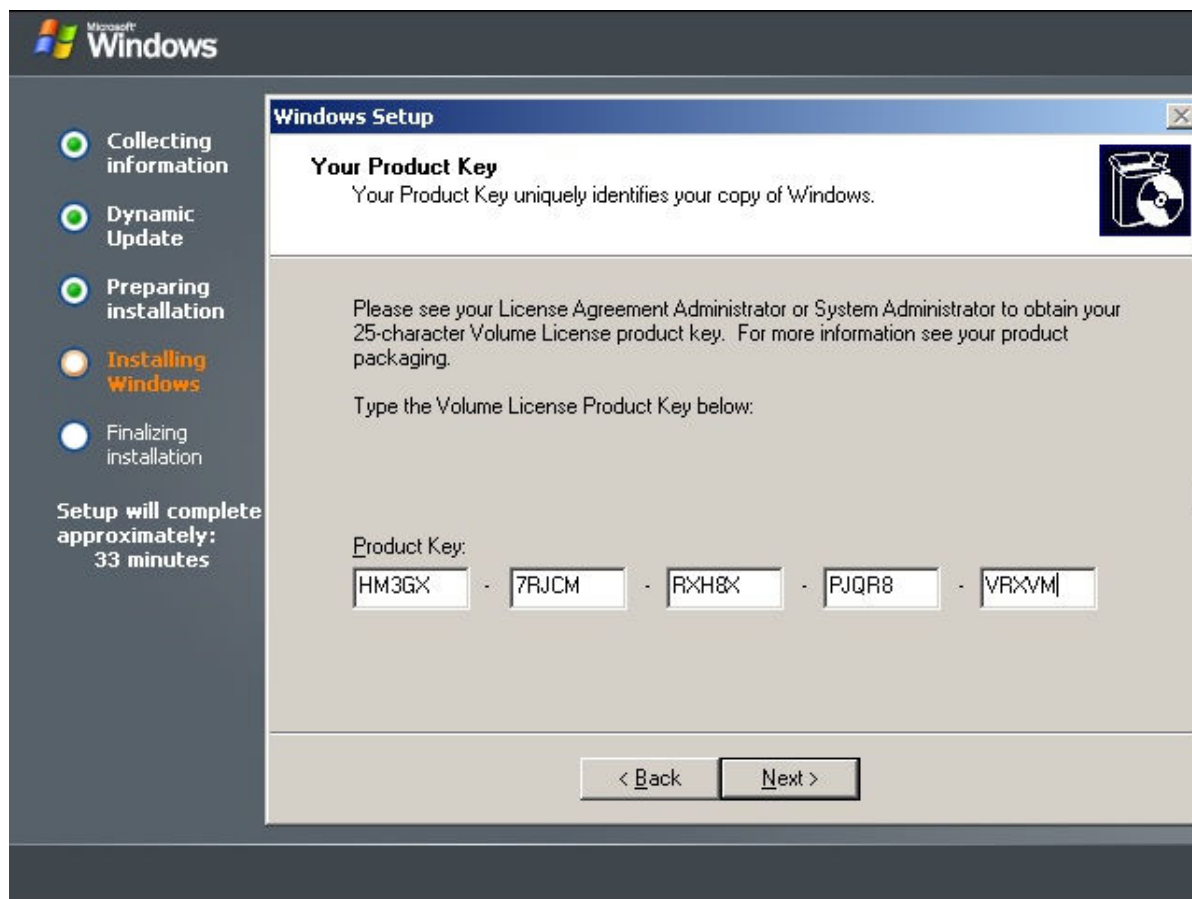
۱۴ - در این پنجره تنظیمات مربوط به زبان ویندوز را انجام داده و بر روی Next کلیک می کنیم.



۱۵ - در پنجره بعدی نام و نام سازمان خود را وارد کرده و بر روی Next کلیک می کنیم.



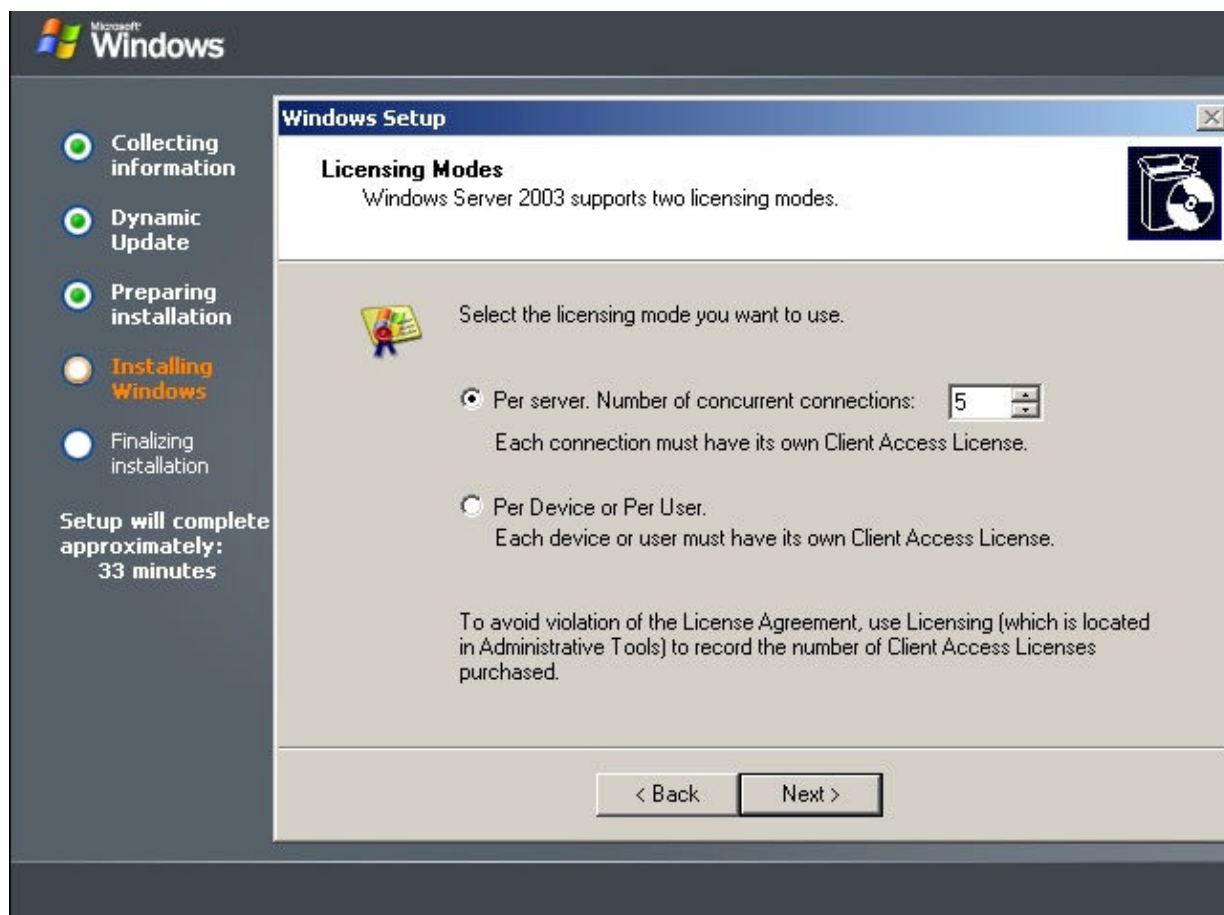
۱۶- در این صفحه شماره سریال ویندوز سرور ۲۰۰۳ را وارد کرده و بر روی Next کلیک می کنیم.



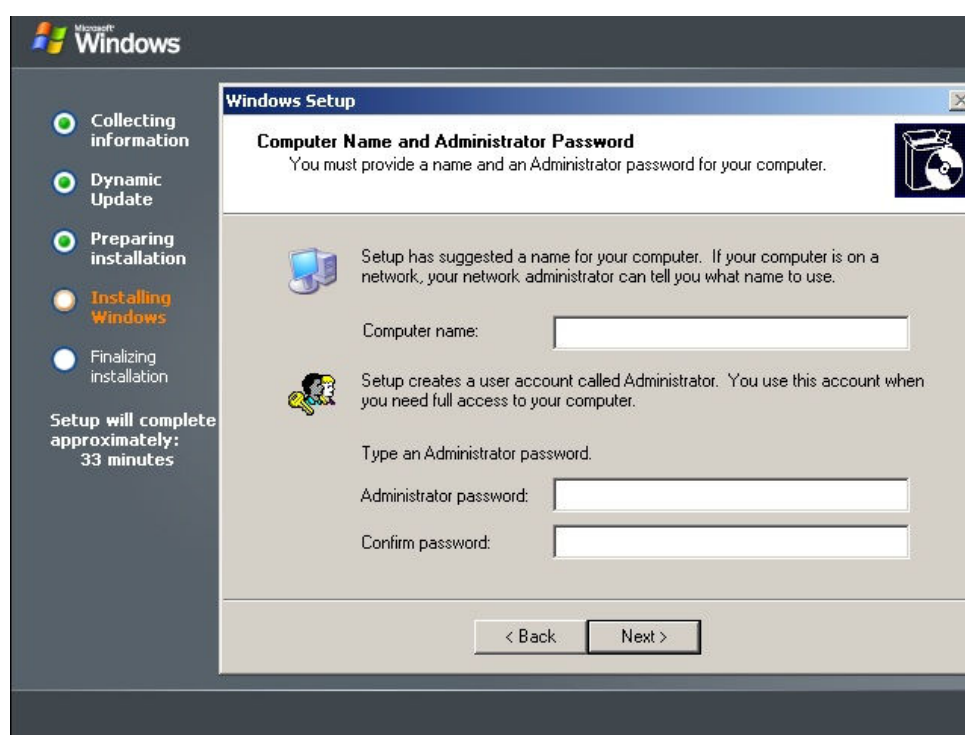
۱۷ - در این مرحله باید نوع مجوز استفاده از این ویندوز را معین کنیم: معمولاً در شبکه‌هایی که دارای یک رایانه سرویس دهنده می‌باشند انتخاب گزینه اول Per Server (همزمان چند کاربر یا Connection می‌تواند کار کند) درست‌تر می‌باشد.

انتخاب گزینه دوم Per Device or Per User معمولاً نشاندهنده آن است که تعداد اتصالات به سرویس دهنده بیش از تعداد کاربران موجود و در حال کار است.

که در اینجا گزینه اول را انتخاب کرده و بر روی Next کلیک می‌کنیم.



۱۸ - در اینجا نام دلخواه رایانه سرویس دهنده خود را وارد می کنیم. رایانه سرویس دهنده از این پس بدین نام در شبکه شناسایی خواهد شد. همچنین در این پنجره باید رمز مورد نظر برای مدیر شبکه را وارد و آن را دوباره تایید (Confirm) کنیم (کلمه رمز نباید از خاطرمาน برود). توجه داشته باشید که نام کاربری اصلی administrator می باشد و این رمز برای آن در نظر گرفته می شود.



• بررسی ویژگیهای کلمه رمز در ۲۰۰۳ سرور:

اگر رمز خود را به خوبی انتخاب نکرده باشید، پنجره ای زیر نمایان می شود که در آن ضوابط و معیارهای گزینش درست ذکر شده است. توصیه می شود رمز مورد نظر از ۲ قاعده اول ذیل پیروی کرده و از بین بقیه حداقل از ۳ قاعده تبعیت کند:

الف: حداقل ۶ حرف داشته باشد.

ب: در برگیرنده واژه های Admin یا Administrator نباشد.

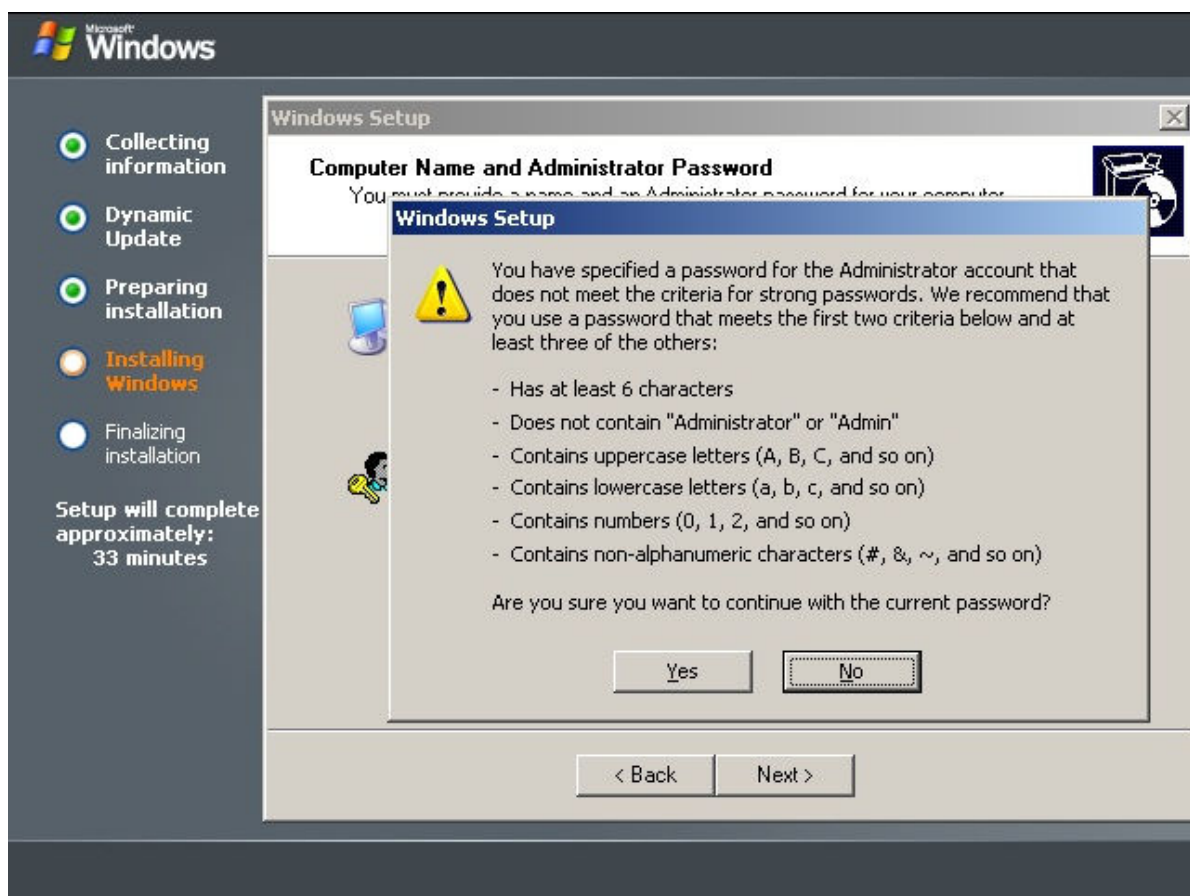
ج: حاوی حروف بزرگ (Uppercase) مانند A, B و غیره باشد.

د: حاوی حروف کوچک (Lowercase) مانند "a", "b" و غیره هم باشد.

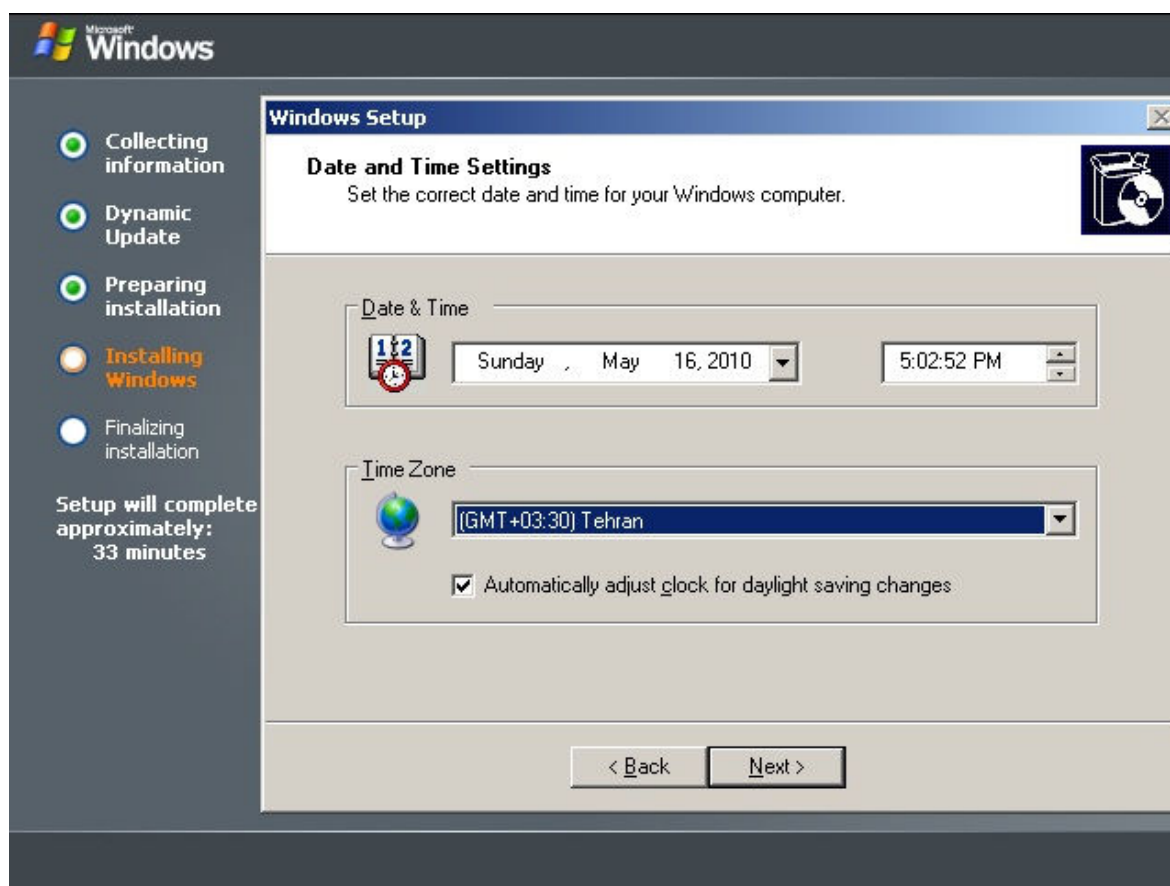
ه: حاوی اعداد نیز باشد.

و: حاوی کاراکترهای غیر حرفی و عددی (non-alphanumeric characters) مانند "&", "~", "\$", "#" و غیره هم باشد.

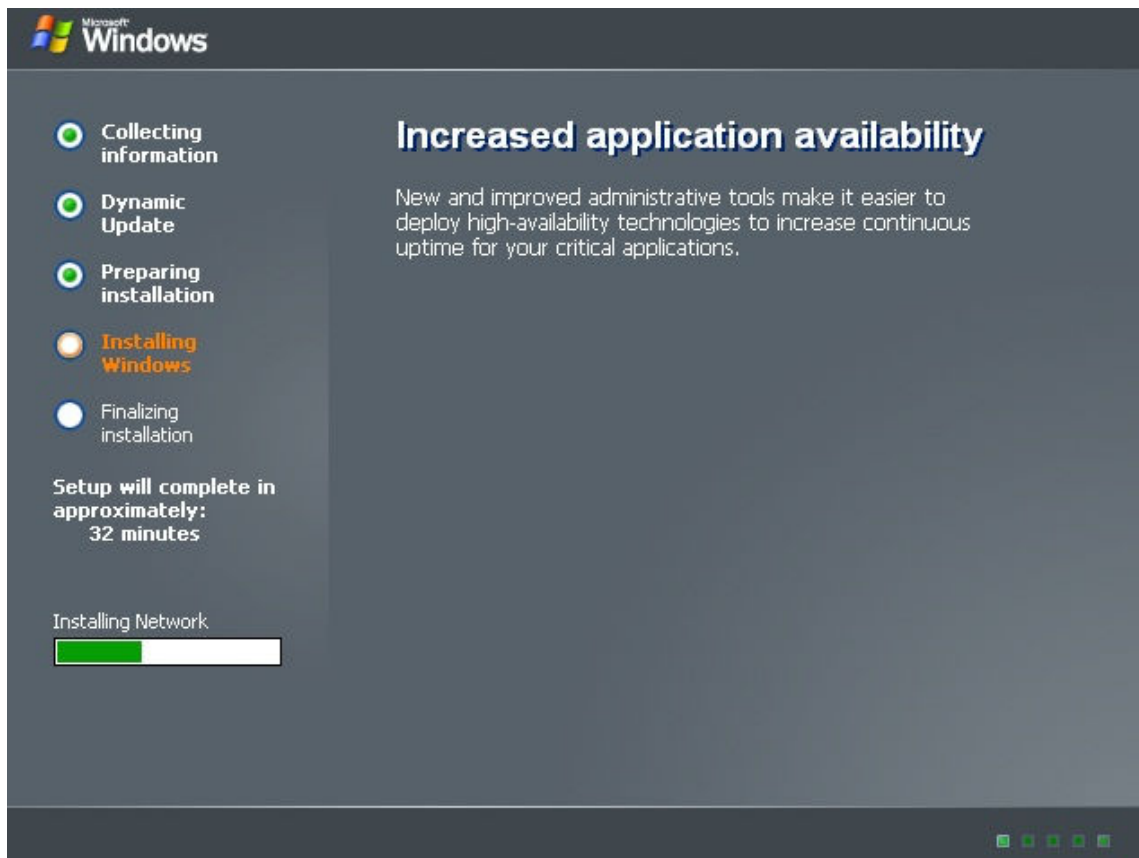
رمز مورد نظر باید دارای امنیت بوده و از یادتان نرود.



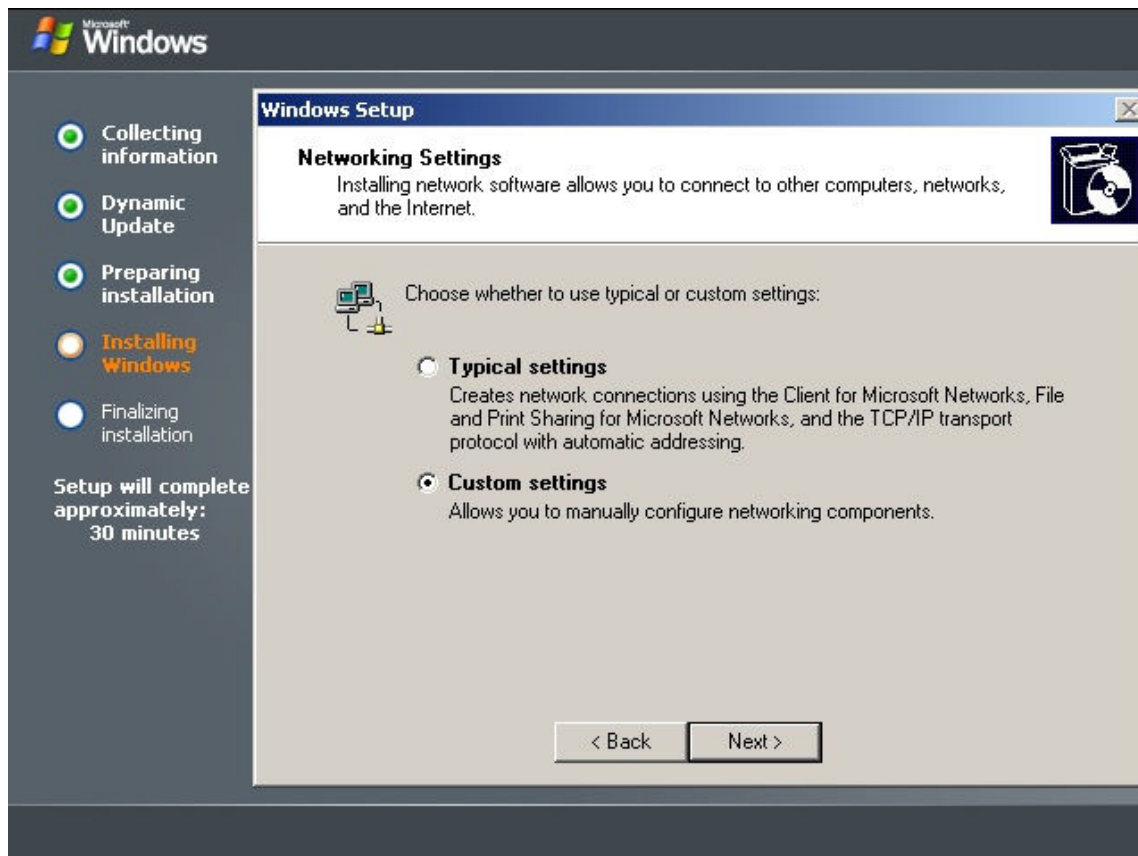
۱۹ - در پنجره بعدی تنظیمات زمان و تاریخ (Date and Time Settings) انجام می شود که براحتی قابل تنظیم بوده و ضمناً منطقه زمانی (Time Zone) شهر مورد نظرتان نیز در اینجا انتخاب می گردد.



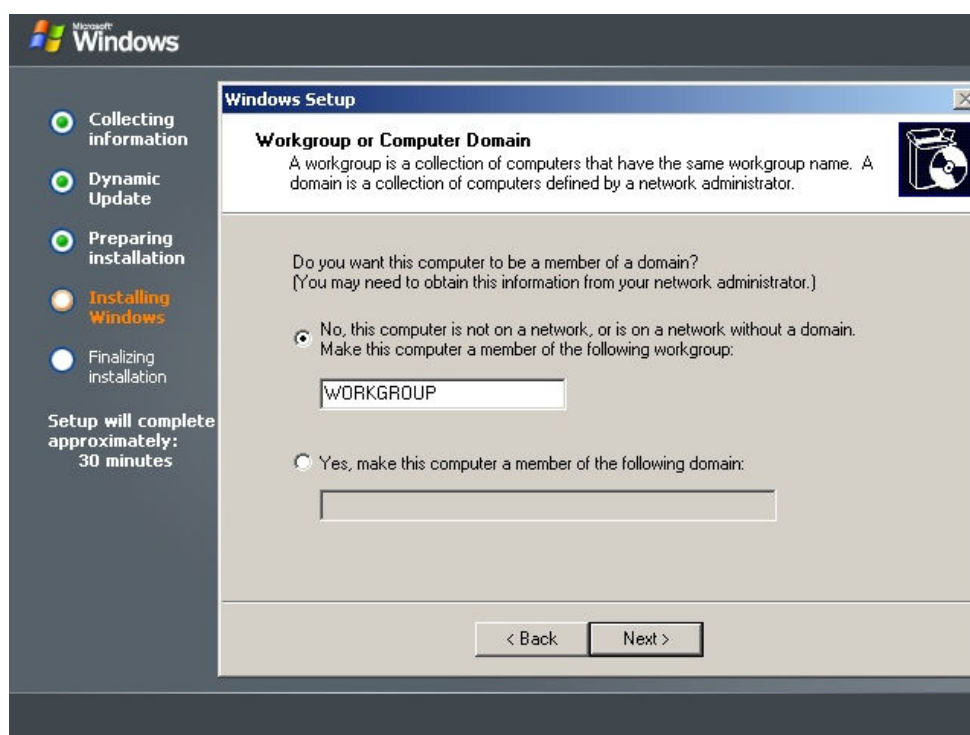
۲۰ - برنامه Setup ادامه یافته نصب مولفه های شبکه در این بخش انجام می گردد.



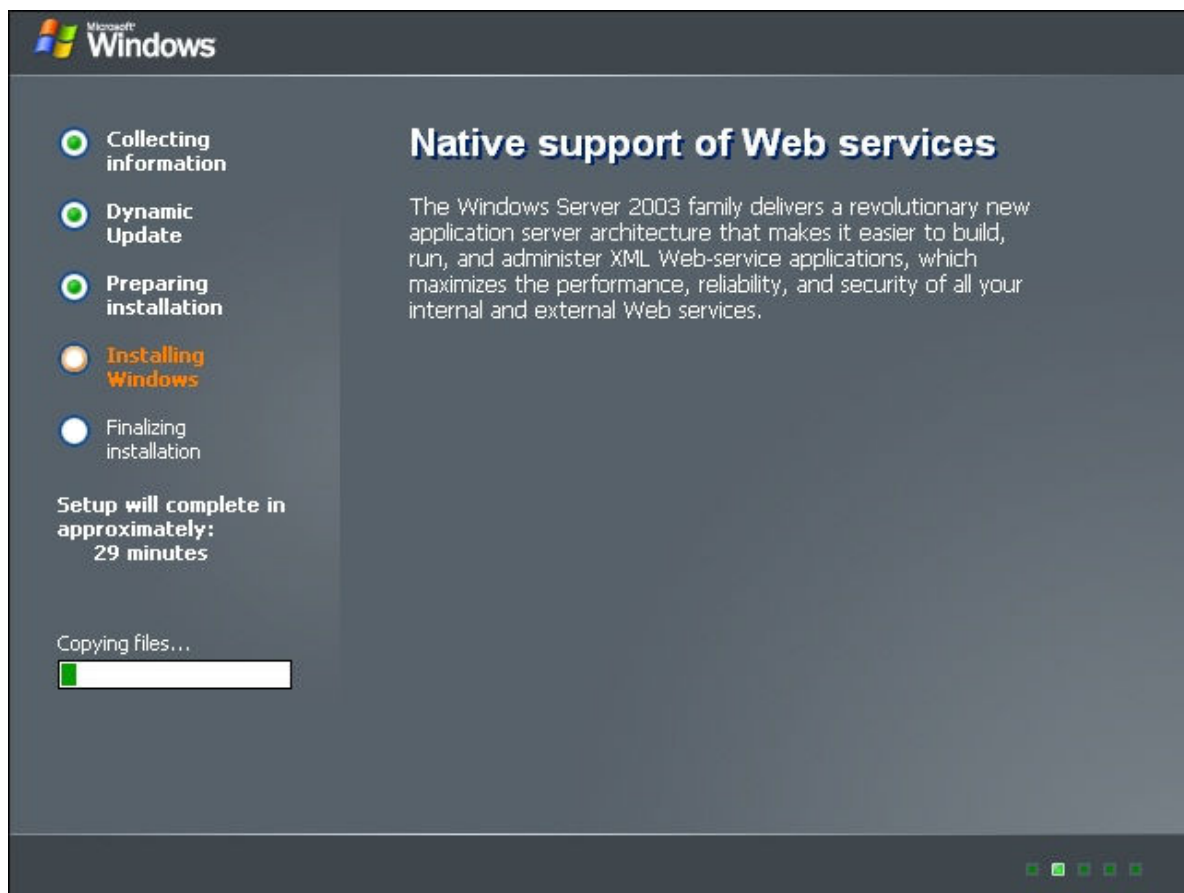
۲۱ - در پنجره بعدی باید برای تنظیمات مربوط به شبکه ، یکی از دو روش عادی و از پیش تعیین شده (Typical) و یا سفارشی (Custom) را انتخاب نماییم. اگر (Typical) را انتخاب کنیم تنظیمات IP را باید بعد از نصب انجام دهیم و با انتخاب گزینه Custom می توانیم تنظیمات IP را در این قسمت انجام دهیم. چون ما تنظیم کردن IP را در بخش "تنظیمات لازم قبل از نصب AD" بیان خواهیم کرد، گزینه Typical را انتخاب و بر روی Next کلیک کنید.



۲۲ - در این پنجره از بین دو روش "Workgroup" (نظیر به نظیر) و یا "Client-Server" (مبتنی بر سرور) که رایانه سرویس دهنده را تبدیل به یک کنترل کننده دامنه (Domain Controller) می کند (شرح آنها قبلاً داده شده) یکی را انتخاب می کنیم اگر قبلاً دامنه ای وجود نداشته باشد و برای اولین بار ۲۰۰۳ نصب می کنیم بهتر است گزینه اول را انتخاب کنیم. (نام این گروه کاری می تواند بصورت دلخواه داده شود).

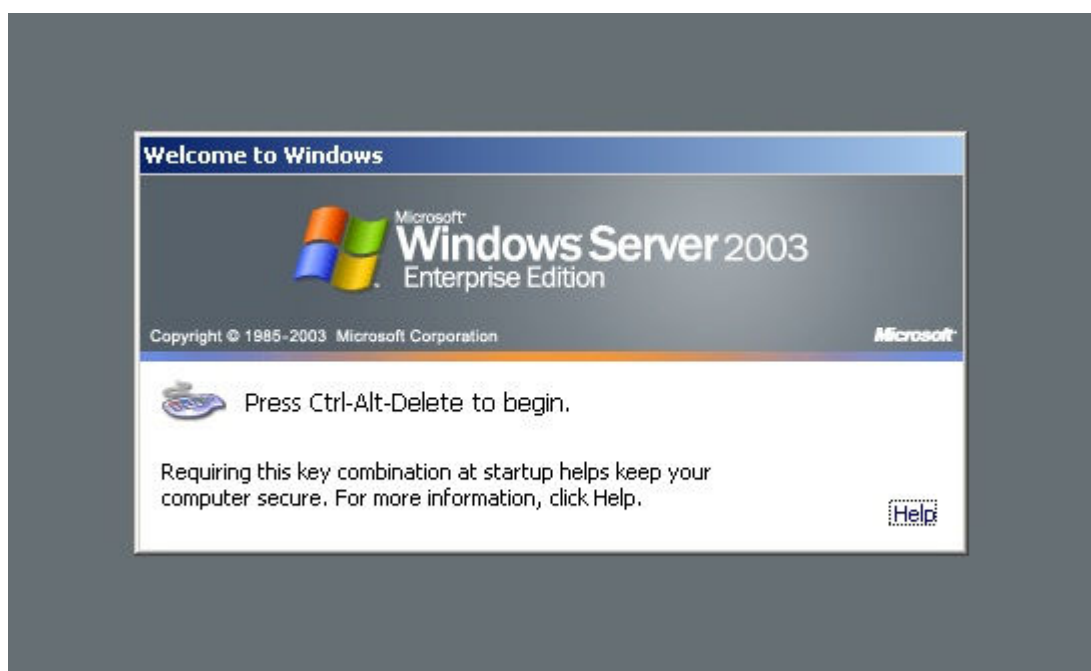


۲۳ - در پنجره بعدی زمانی صرف ادامه نصب ویندوز خواهد شد.



۲۴ - ویندوز ۲۰۰۳ برای اولین بار بر روی رایانه تان آغاز به کار می کند.

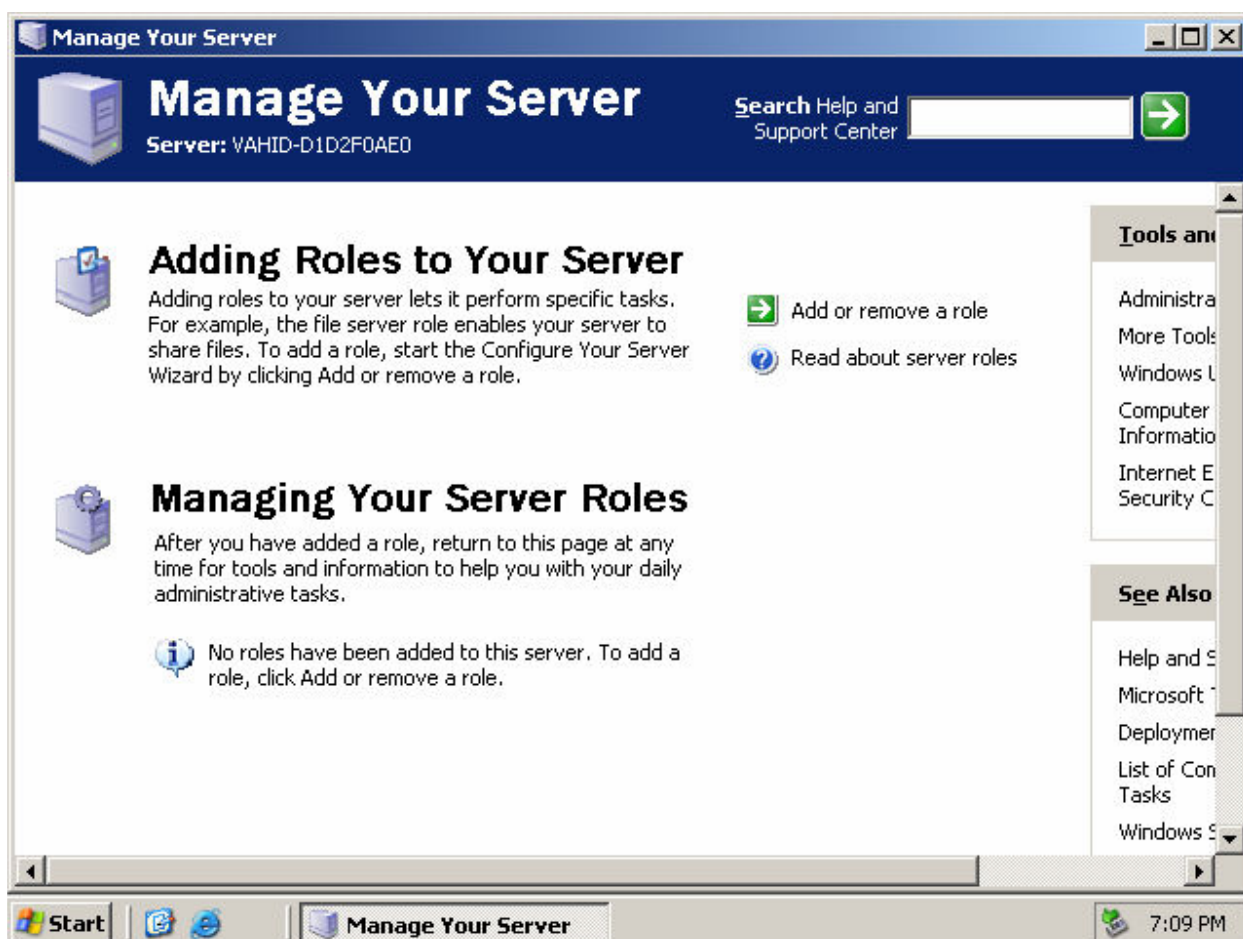
برای ورود دکمه های Ctrl+Alt را فشرده و کلید Delete را بزنید.



۲۵ - نام کاربری (Username) مدیر شبکه Administrator را خواهید دید. نام رمز که از یادتان نرفته است؟!!



۲۶ - با استفاده از پنجره Manage Your Server می توان سرویس دهنده را برای اعمال خاصی پیکربندی کرد.



۲-۴-۱- بررسی نصب ویندوز ۲۰۰۳ سرور در کنار سیستم عامل دیگر:

اگر یک سیستم عامل از قبل بر روی سیستم تان نصب باشد و بخواهید بدون اینکه سیستم قبلی را حذف کنید، ویندوز ۲۰۰۳ سرور را نیز نصب کنید مراحل زیر را دنبال نمایید:

۱ - CD ویندوز را در دخیل CD-ROM گذاشته و بر روی آیکن CD-ROM کلیک کنید.

۲- در پنجره ظاهر شده بر روی گزینه Install Windows Server 2003,Enterprise Edition برای نصب ویندوز کلیک نمایید.

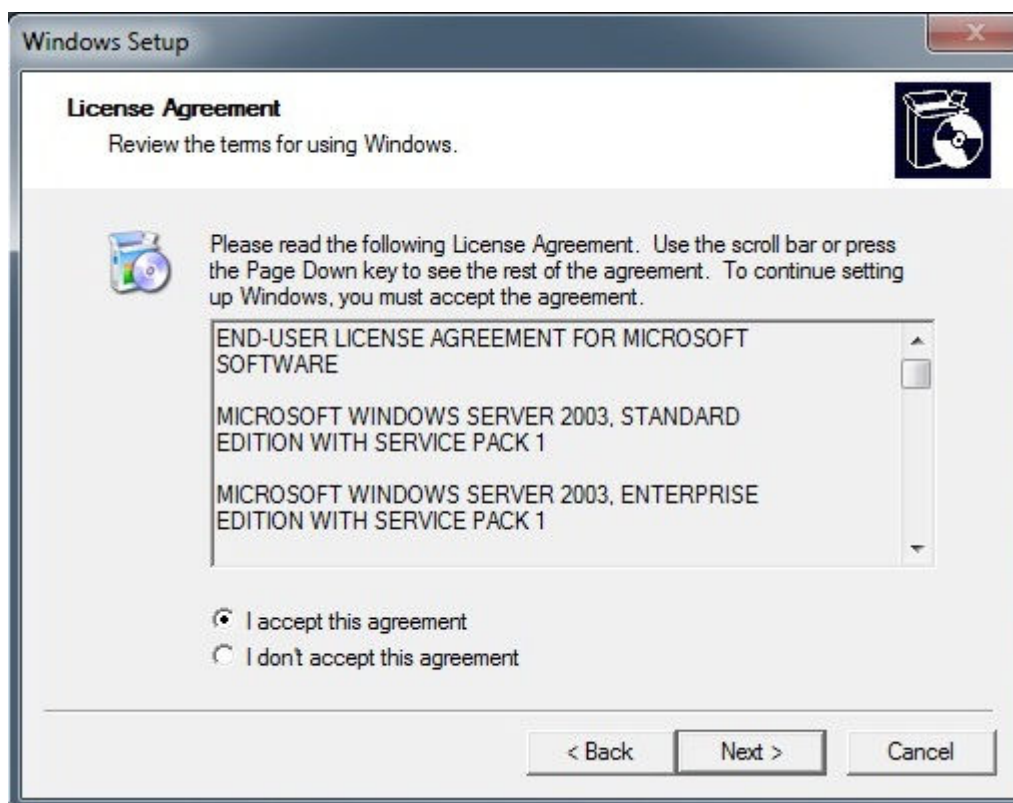


۳- پنجره خوش آمد گویی ویندوز ظاهر میشود بر روی Next کلیک نمایید.

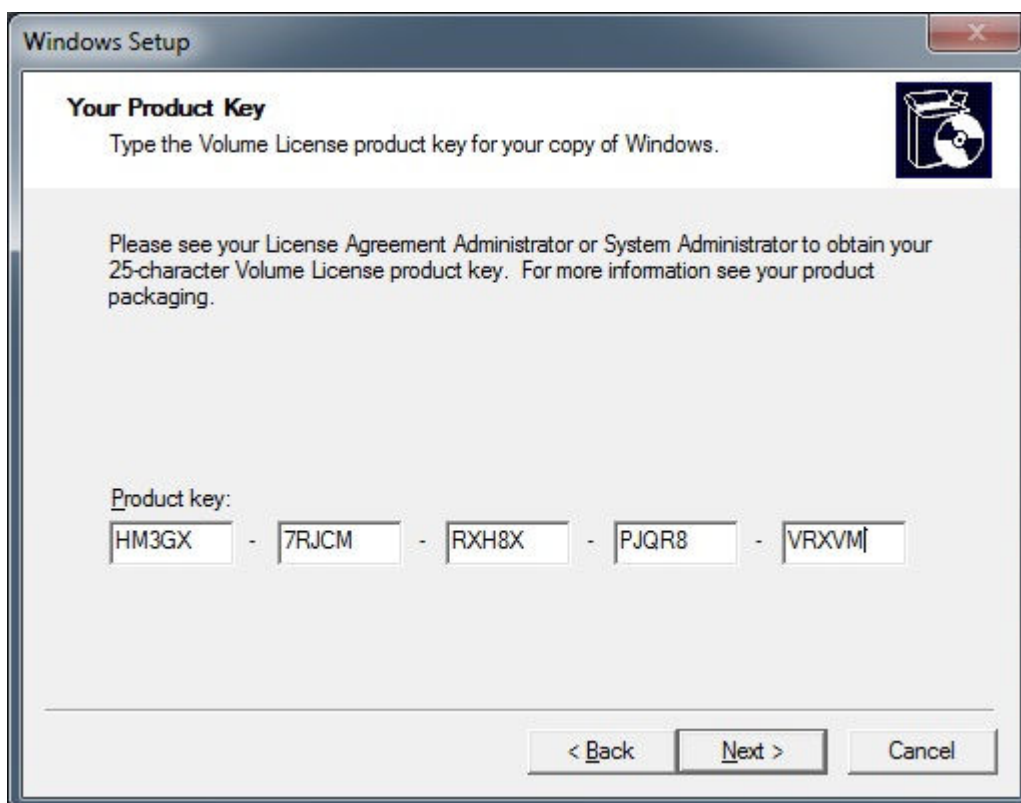


۴- در این پنجره قوانین ویندوز نشان داده می شود گزینه

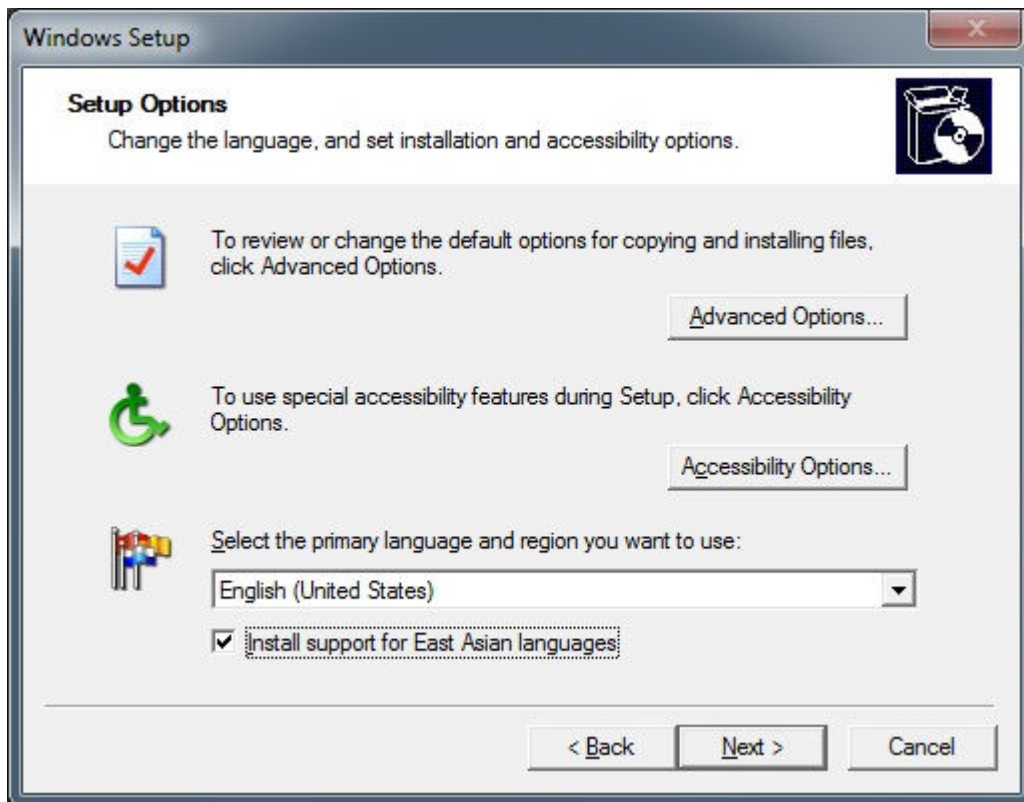
I accept this agreement را انتخاب بر روی Next کلیک کنید.



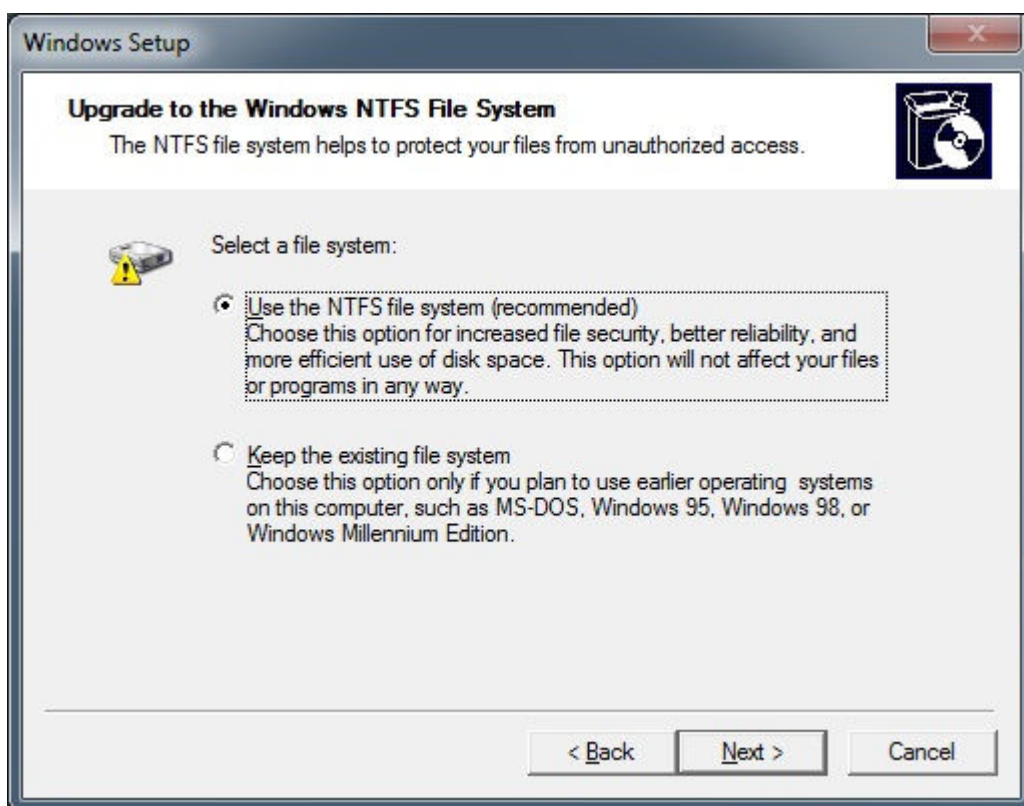
۵- سریال ویندوز را وارد کرده بر روی Next کلیک کنید.



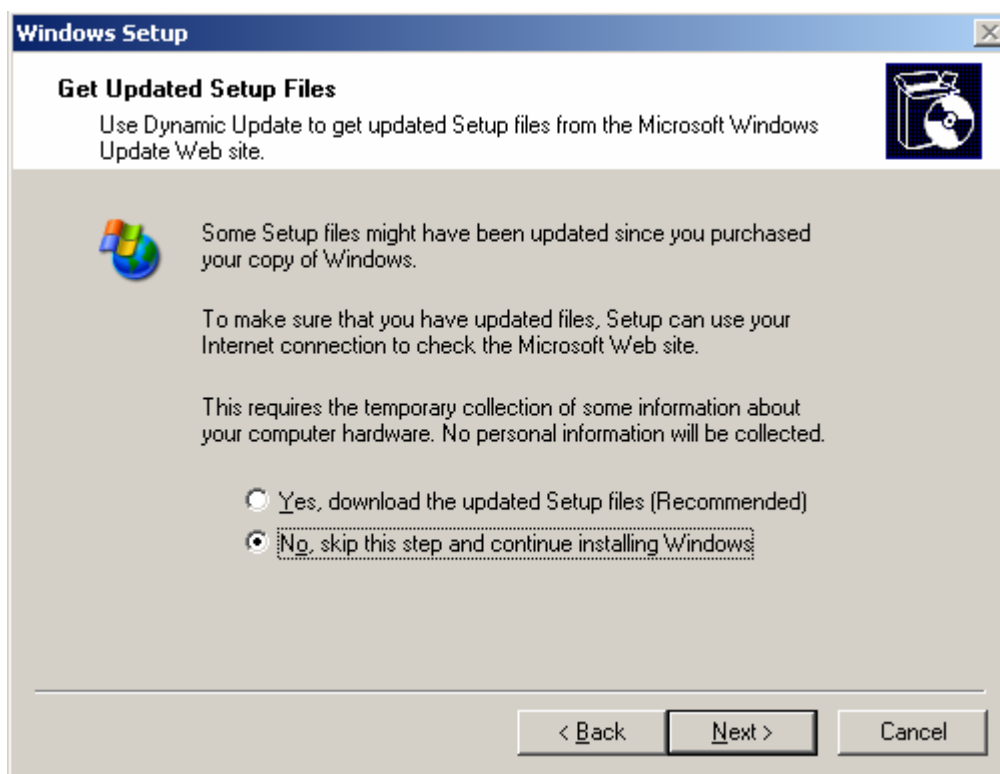
۶- در این پنجره تنظیمات زبان را انجام داده بر روی Next کلیک کنید.



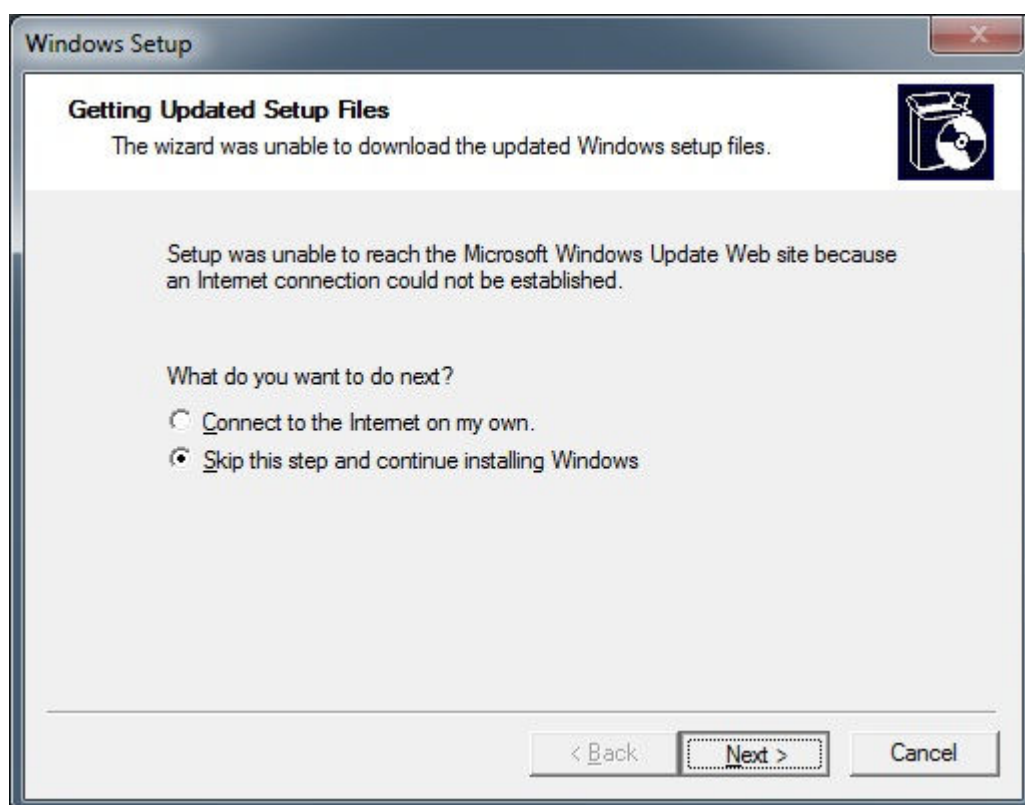
۷- در این پنجره نوع فرمت ای که سیستم عامل ۲۰۰۳ باید از آن استفاده کند را باید انتخاب کنید، که گزینه‌ها را انتخاب و بر روی Next کلیک کنید.



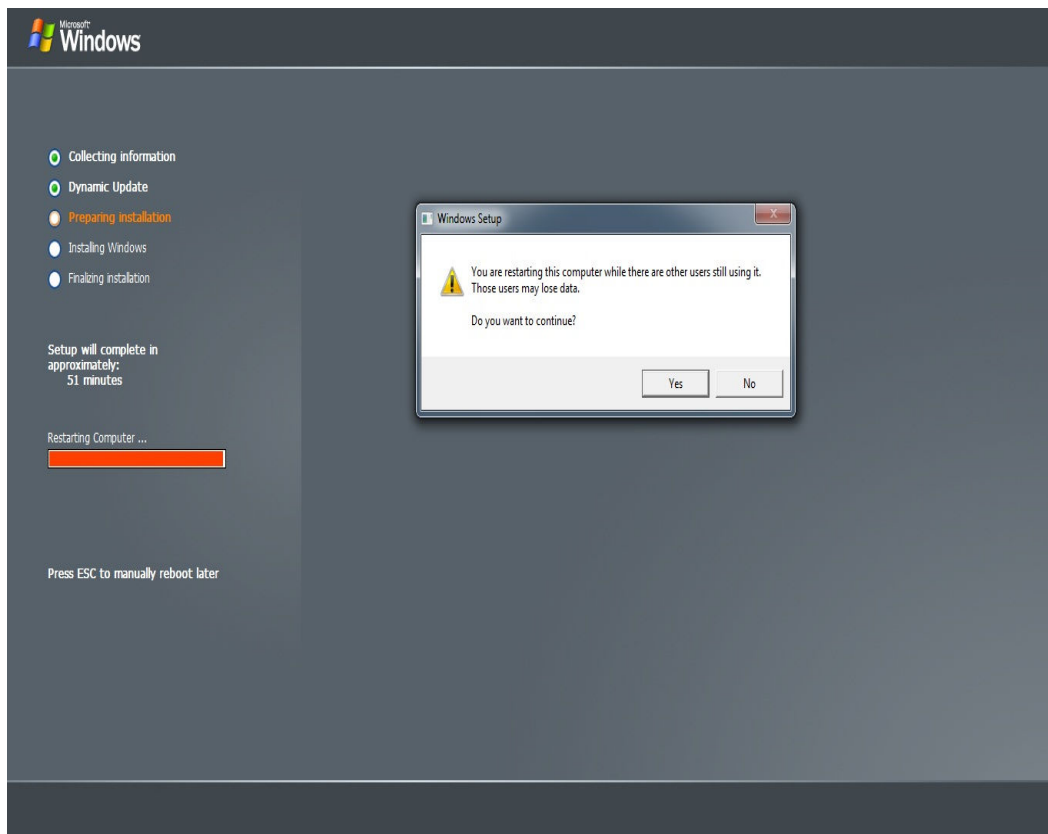
۸- در این قسمت پرسیده می شود که آیا می خواهید فایل‌های setup ویندوز را update کرده و نصب کنید، که گزینه No، skip this step and continue installing Windows را انتخاب کرده گزینه Next را کلیک کنید.



۹- در اینجا نیز از پرسیده می شود که آیا می خواهید به اینترنت وصل شوید برای update کردن فایلها، که گزینه skip this step and continue installing Windows را انتخاب کرده، Next را کلیک کنید.



۱۰- بعد از نصب فایلهای سیستمی پیغامی نمایش داده می شود که از شما می خواهد با تایید آن کامپیوتر را رستارت نماییم، تا بعد از رستارت کامپیوتر شروع به نصب ویندوز نماید.



۱۱- بقیه مراحل نصب ویندوز در کنار سیستم عامل، همانند "نصب ویندوز به عنوان اولین سیستم عامل بر روی کامپیوتر" از مرحله 15 به بعد می باشد(که در مبحث قبلی گفته شده است).

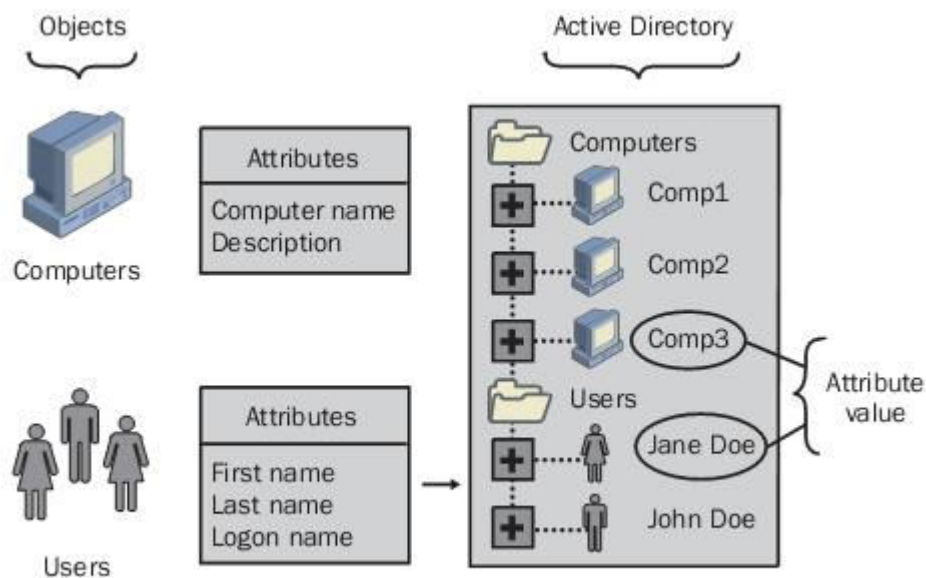
۲. جزئیات بخش دوم:

۲-۱- Active Directory:

AD یک سرویس دایرکتوری بوده که در Windows Server 2003 قرار داده شده است. اگر AD نصب کنیم سیستم ما یک سرور می شود در غیر اینصورت مانند client عمل می کند. هدف از نصب AD مدیریت کاربران در شبکه می باشد. بعد از نصب اکتیو دایرکتوری سرور تبدیل به Domain Controller (D.C) می شود. D.C وظیفه Authentication یا احراز هویت در Domain را بر عهده دارد. بدین معنی که زمانی که یک کاربر از روی کلاینت به Domain می خواهد login کند، نام و رمز کاربر به صورت کد شده به DC ارسال می شود. DC که اطلاعات تمامی کاربران را در Domain دارا می باشد. اطلاعاتی دریافتی را با اطلاعات خود که از کاربران دارد مقایسه می کند و در صورتی که صحیح باشد اگر اطلاعات در یافتی درست باشد

۲-۲- اشیاء و صفات در A.D:

یک دایرکتوری (Directory) مجموعه های ذخیره شده از اطلاعات درباره اشیا است که به نوعی با یکدیگر مرتبط اند. یک سرویس دایرکتوری (Directory Service) تمامی اطلاعاتی را که برای استفاده و مدیریت این اشیا لازم است، در یک محل متمرکز ذخیره نموده و بدین ترتیب نحوه ی یافتن و مدیریت این منابع را تسهیل می بخشد. هر داده ای که در Active Directory ذخیره می شود، به صورت اشیا (Objects) متفاوت، سازمان می یابد. یک شیء مجموعه مجزایی از صفات است که منابع شبکه را مشخص می کند. صفات (Attributes)، خصوصیات اشیا موجود در یک دایرکتوری را شامل می شود. به عنوان نمونه صفات یک User account (حساب کاربر) می تواند شامل نام، نام خانوادگی و نام Log on برای آن کاربر باشد. در حالی که صفات یک computer account ممکن است که شامل نام و مشخصات آن شیء باشد. بعضی از اشیا، که از آن ها به نام Container یاد می شود، خود دربردارنده اشیا دیگریند. به عنوان مثال یک domain، خود یک container است که می تواند شامل اشیا مانند حساب کاربران و کامپیوترها باشد. در شکل ۱ پوشه ی کاربران، یک container بوده که دارای اشیا مربوط به حساب کاربران است.



شکل ۱: ارتباط اشیا و صفات AD

۳-۲- اجزای A.D:

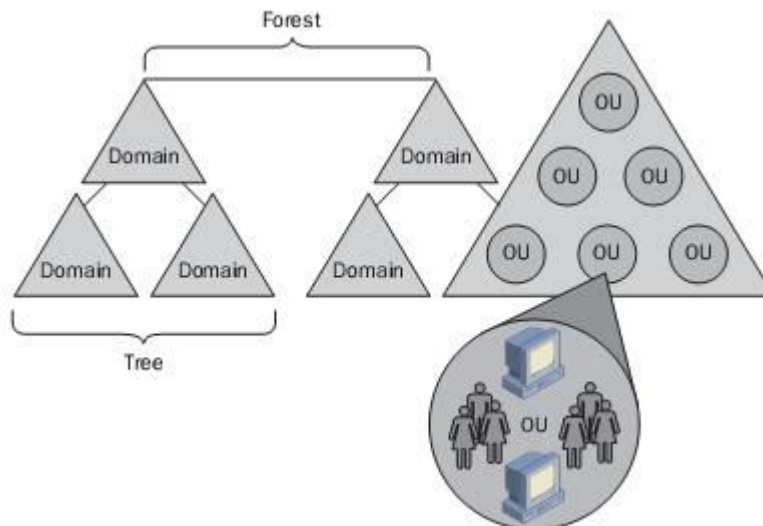
برای ایجاد یک ساختار دایرکتوری، اجزای زیادی مورد نیاز است:

- دامنه‌ها (Domains)
- واحدهای سازمانی (Organizational Units)
- درخت‌ها (Trees)
- جنگل‌ها (Forests)
- Domain Controller‌ها (DC)

در Active Directory، می‌توان منابع را به صورت یک ساختار منطقی سازمان داد (ساختاری که منعکس کننده‌ی مدل‌های سازمانی باشد)

گروه‌بندی منطقی منابع این امکان را فراهم می‌آورد تا یک منبع با استفاده از نامش به سادگی پیدا شود و این امر را از یادآوری محل فیزیکی منبع بی‌نیاز می‌سازد. در شکل ۲ رابطه‌ی domain‌ها، OU‌ها، tree‌ها و forest‌ها دیده می‌شود.

۴-۲- بررسی دامنه، درخت و جنگل:



شکل ۲: رابطه میان اجزای Active Directory

• دامنه Domain :

هسته‌ی اصلی ساختار منطقی در Active Directory، domain یا دامنه بوده که قادر به ذخیره‌ی میلیون‌ها شیء است. تمامی domain‌ها در دو ویژگی زیر مشترکند:

- تمام اشیای شبکه در یک Domain قرار دارند و هر Domain اطلاعات مربوط به همان Domain را داراست.
- Domain یک محدوده‌ی امنیتی است. دسترسی به اشیای Domain‌ها از طریق لیست‌های کنترل دسترسی یا ACL (Access Control List) میسر می‌شود.

ACL‌ها شامل مجوزهایی هستند که مرتبط با اشیای مورد نظر است. این مجوزها بیان می‌دارند که کدام یک از کاربران می‌توانند به یک شیء دسترسی داشته باشند و این دسترسی از چه نوع و در چه سطحی است. در خانواده‌ی Windows Server 2003، اشیای شامل فایل‌ها، پوشه‌ها، اشتراکات، چاپگرها و سایر اشیای Active Directory است. این نکته می‌بایست در نظر گرفته شود که هیچ یک از تنظیمات و سیاست‌های امنیتی مانند اختیارات مدیریتی، سیاست‌های امنیتی و ACL‌ها نمی‌توانند از یک Domain به Domain دیگر تغییر یابند. این امر بدان معنا است که یک مدیر در سطح یک Domain تنها دارای اختیاراتی است که وی را محدود به وضع سیاست‌ها در همان Domain می‌کند.

سطح عملیاتی دامنه (Domain Functional Level) که تحت عنوان حالت دامنه (Domain Mode) در Windows 2003 شناخته می‌شود، ویژگی‌های خاصی را در پهنه دامنه (Domain-Wide) و در محیط شبکه فراهم می‌آورد.

• واحدهای سازمانی Organization Units :

OU خود یک container بوده که اشیای یک دامنه (Domain) را در گروه‌های مدیریتی سازمان دهی می‌کند. یک OU برای اعمال و اجرای وظایف مدیریتی (مانند مدیریت منابع و کاربران) به کار رفته و می‌تواند شامل اشیایی مانند حساب‌های کاربران، گروه‌ها، کامپیوترها، چاپگرها، برنامه‌ها، فایل‌های به اشتراک گذاشته شده و حتی سایر OU‌ها از همان domain باشد. ساختار سلسله مراتبی یک OU در یک domain مستقل از ساختار سلسله مراتبی OU در domain‌های دیگر است.

• درخت‌ها Trees:

یک درخت (Tree)، سازمان دهی یا گروه‌بندی منطقی یک یا چند دامنه بوده که از طریق ایجاد یا اضافه کردن چند دامنه‌ی فرزند (Child Domain) به دامنه‌ی پدر (Parent Domain) فعلی به وجود می‌آید. دامنه‌ها در یک درخت، دارای یک فضای اسمی (Contiguous Namespace) یا ساختار نامی سلسله مراتبی مشترک هستند. بر اساس استانداردهای DNS، نام یک دامنه‌ی فرزند، ترکیبی از نام خود دامنه‌ی فرزند به همراه نام دامنه‌ی پدر است. در شکل ۴ Domain با نام microsoft.com به عنوان دامنه‌ی والد، و Domain های us.microsoft.com و uk.microsoft.com دامنه‌های فرزند آن هستند. علاوه بر آن خود دامنه‌ی uk.microsoft.com دارای یک دامنه‌ی فرزند با نام sls.uk.microsoft.com است.

• جنگل‌ها Forests:

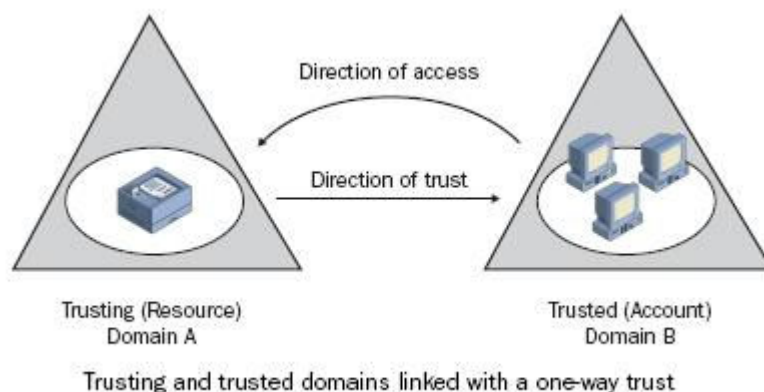
یک جنگل (Forest) دسته‌بندی یا سازماندهی سلسله مراتبی از یک یا چند درخت (Domain Tree) کاملاً مستقل و مجزا از هم است. یک جنگل دارای ویژگی‌هایی است: درخت‌ها در یک جنگل با توجه به دامنه‌هایشان، دارای ساختار نامی متفاوت هستند. دامنه‌ها در یک جنگل به صورتی کاملاً مستقل از هم عمل می‌کنند، ولی یک جنگل امکان ارتباط در تمامی سازمان را برقرار می‌سازد.

• DC (Domain Controller)

یک Domain Controller کامپیوتری است که دارای سیستم عامل Windows Server باشد و یک نسخه از دایرکتوری دامنه (Local Domain Database) یا replica را در خود ذخیره کند. هر دامنه می‌تواند بیش از یک Domain Controller داشته باشد. یک Domain Controller تنها می‌تواند به یک دامنه سرویس دهد. یک DC وظیفه‌ی شناسایی کاربرانی را که تلاش برای log on به دامنه دارند، را بر عهده دارد. علاوه بر آن سیاست‌های امنیتی برای یک دامنه را نیز تنظیم و حفظ می‌کند.

۵-۲- ارتباط Trust:

یک Trust، اتصالی میان دو دامنه است که در آن دامنه‌ی اعتماد کننده (trusting domain)، اطلاعات مربوط به دسترسی و شناسایی را از دامنه‌ی مورد اعتماد (trusted domain) کسب می‌کند. دو دامنه وجود دارند که موجب برقراری یک رابطه‌ی مطمئن و یا یک trust می‌شوند: دامنه‌ی اعتماد کننده (trusting) و دامنه‌ی مورد اعتماد (trusted). دامنه‌ی اعتماد کننده دامنه‌ای است که منابع را در اختیار داشته و به سایر دامنه‌ها برای استفاده از این منابع اعتماد دارد. دامنه‌ی مورد اعتماد در حقیقت استفاده کننده از منابع است. این مسئله در شکل زیر بهتر نمود می‌یابد.



شکل ۱۰: دامنه‌ی اطمینان کننده و دامنه‌ی مورد اعتماد قرار گرفته با یک اعتماد یک طرفه

به Domain B و Domain B به Domain C اعتماد یا trust دارد، بین Domain A و Domain C هیچ ارتباط مطمئن یا Trust برقرار نیست .

• جهت trust (direction): ها می‌توانند یک طرفه (one-way) یا دو طرفه (two-way) باشند. در یک اعتماد یک طرفه Domain A به Domain B trust دارد. در یک trust دو طرفه اگر Domain A به Domain B اعتماد داشته باشد، آنگاه Domain B نیز به Domain A اعتماد دارد.

۶-۲- بررسی ویژگیهای A.D:

Active Directory ویژگی‌های زیر را ارائه می‌کند:

- ذخیره‌ی متمرکز داده (Centralized data store)
- مقیاس پذیری (Scalability)
- قابلیت توسعه (Extensibility)
- قابلیت مدیریت (Manageability)
- ستفاده و تمرکز بر سیستم نام‌گذاری دامنه (Integration with Domain Name System)
- مدیریت تنظیمات سرویس گیرنده (Client configuration management)

۷-۲- شروع به نصب اکتیو دایرکتوری:

۱-۷-۲- بررسی تنظیمات لازم قبل از نصب اکتیو دایرکتوری:

برای نصب اکتیو دایرکتوری تنظیماتی را باید از قبل انجام داده باشید از جمله این تنظیمات:

- باید کارت شبکه سرور نصب شده باشد.
- IP سرور تنظیم شده باشد.

- کابل شبکه وصل شده باشد.
- CD ویندوز داخل CDROM باشد.

۱-۱-۷-۲- بررسی نصب کارت شبکه:

برای اینکه بدانید کارت شبکه نصب شده است یا نه؟ به مسیر زیر بروید:

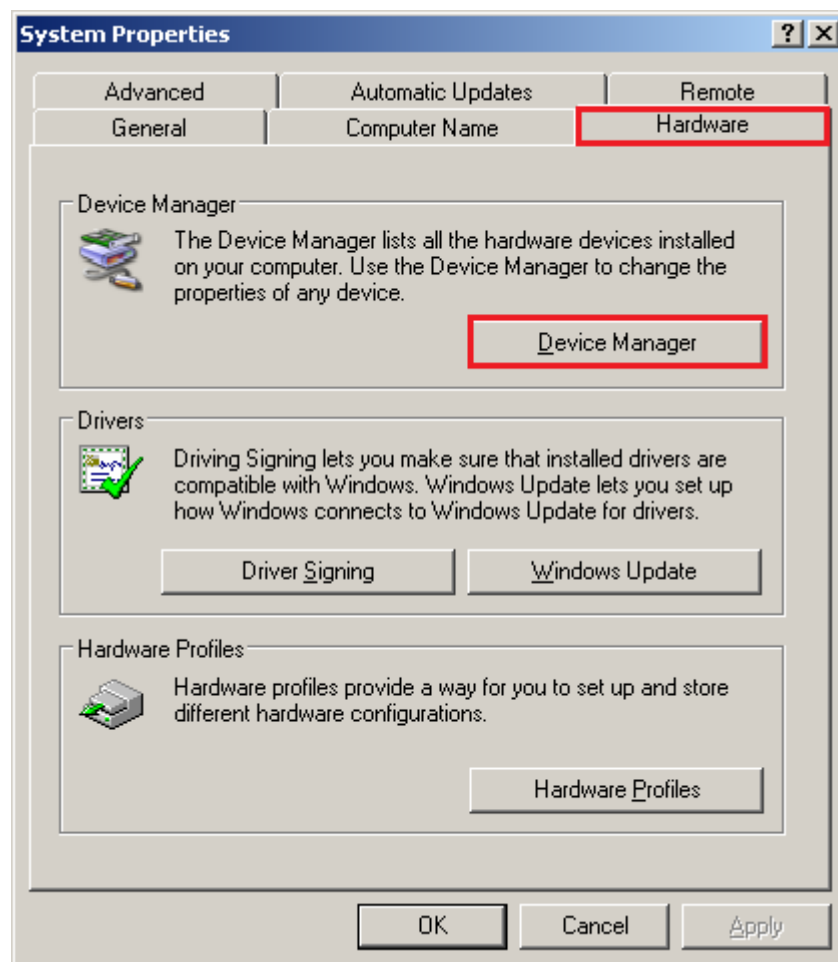
Start > Control Panel > Network Connection

اگر آیکن Local Area Connection در آنجا دیده شد نصب می باشد در غیر اینصورت باید نصب شود.

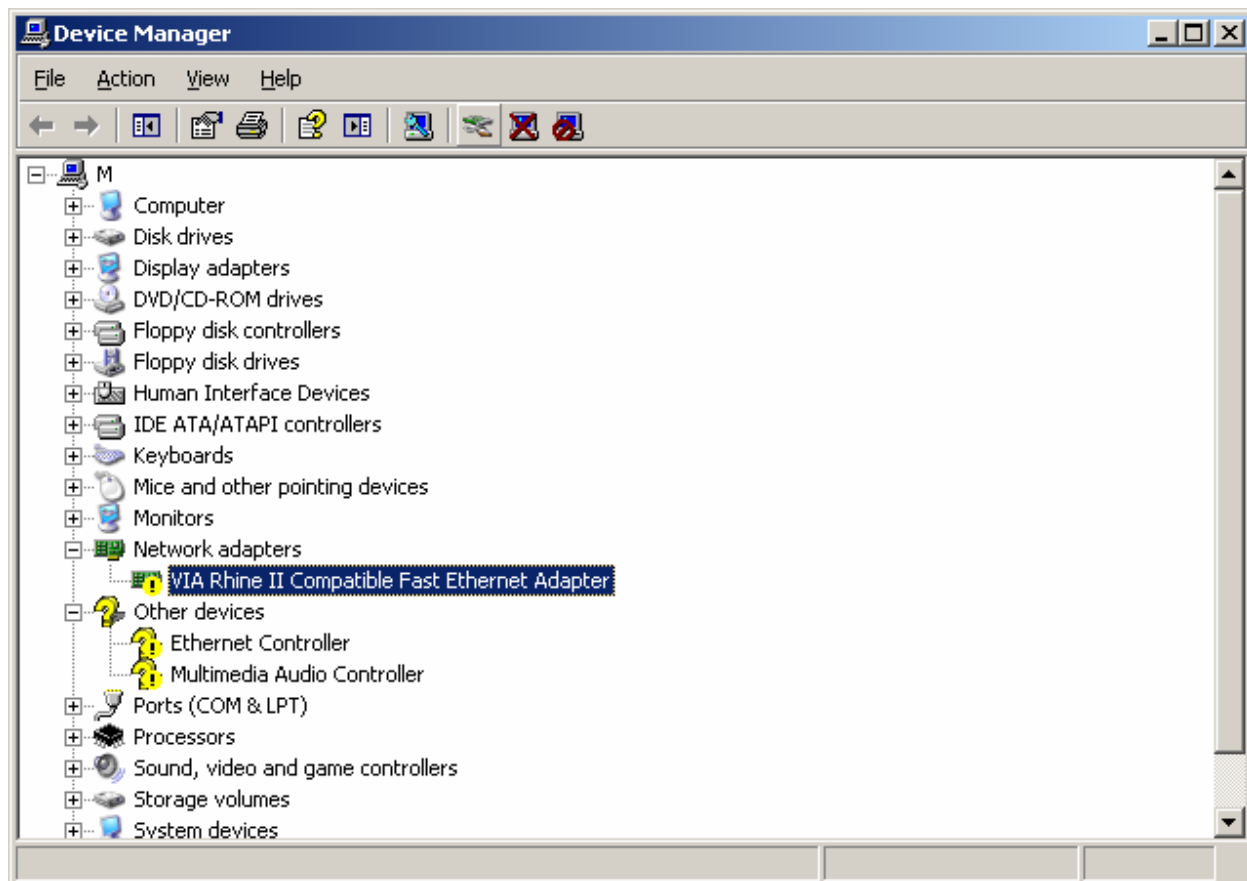


آموزش نصب کارت شبکه:

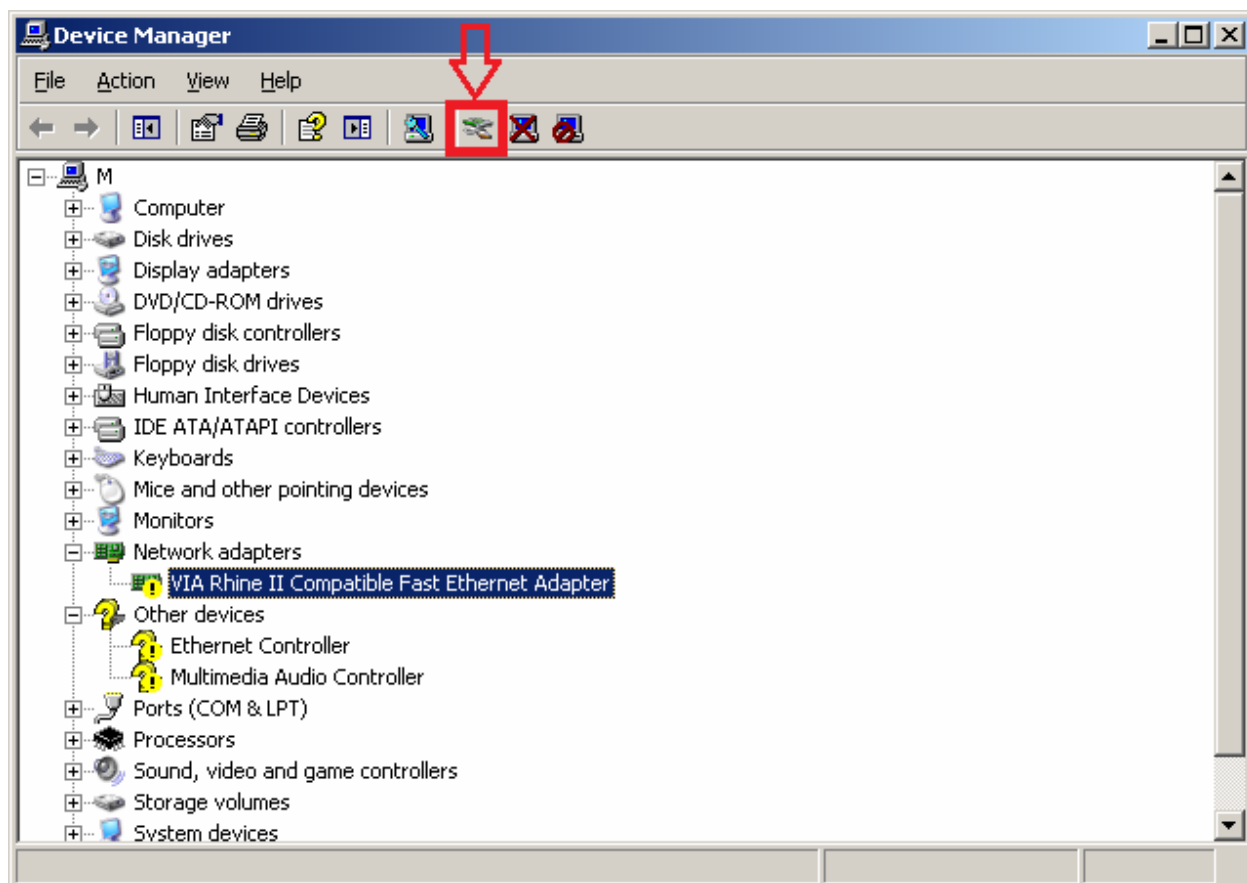
- ۱- برای نصب کارت شبکه باید CD درایور کارت شبکه را داخل CD-ROM قرار داده و روی My Computer کلیک راست کرده Properties را انتخاب کنید. در پنجره ظاهر شده بر روی Hardware و سپس بر روی Device Manager کلیک کنید.



۲- در این پنجره سیستم عامل سخت افزار هایی که نصب نشده اند و سیستم عامل آنها را نمی شناسد، کنار آنها را با یک علامت زرد رنگ نمایش میدهد.



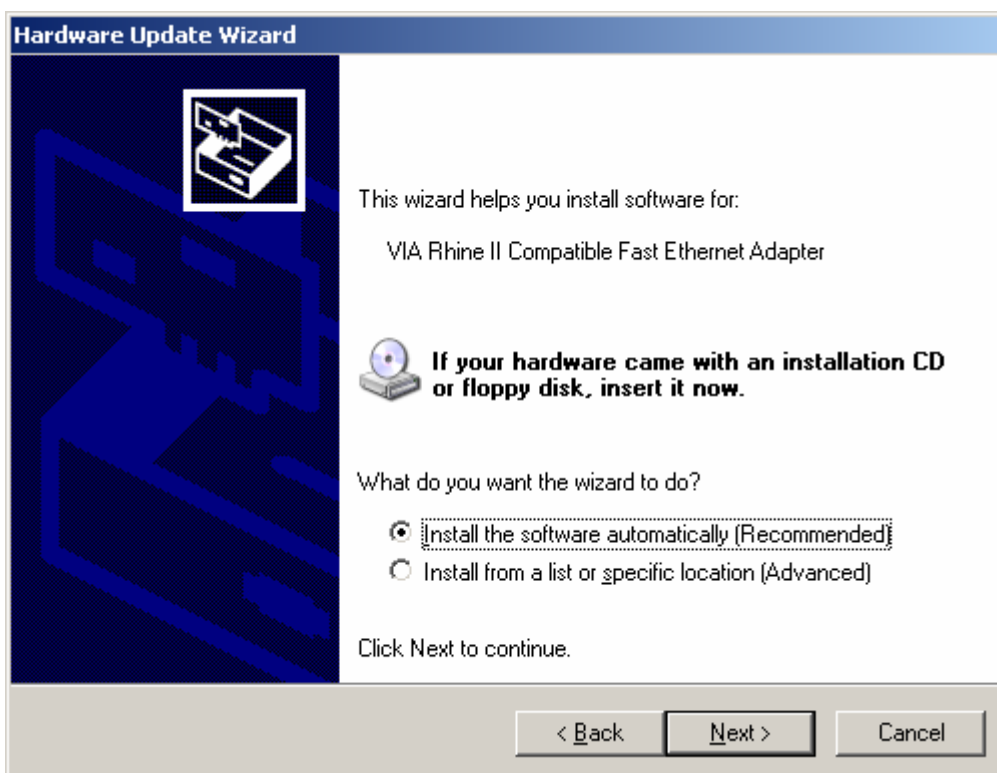
۳- برای نصب کارت شبکه از Network adapters کارت شبکه را انتخاب کرده، یا راست کلیک کرده و گزینه Update Driver Software را انتخاب کنید و یا بر روی آیکن مشخص شده کلیک کنید.



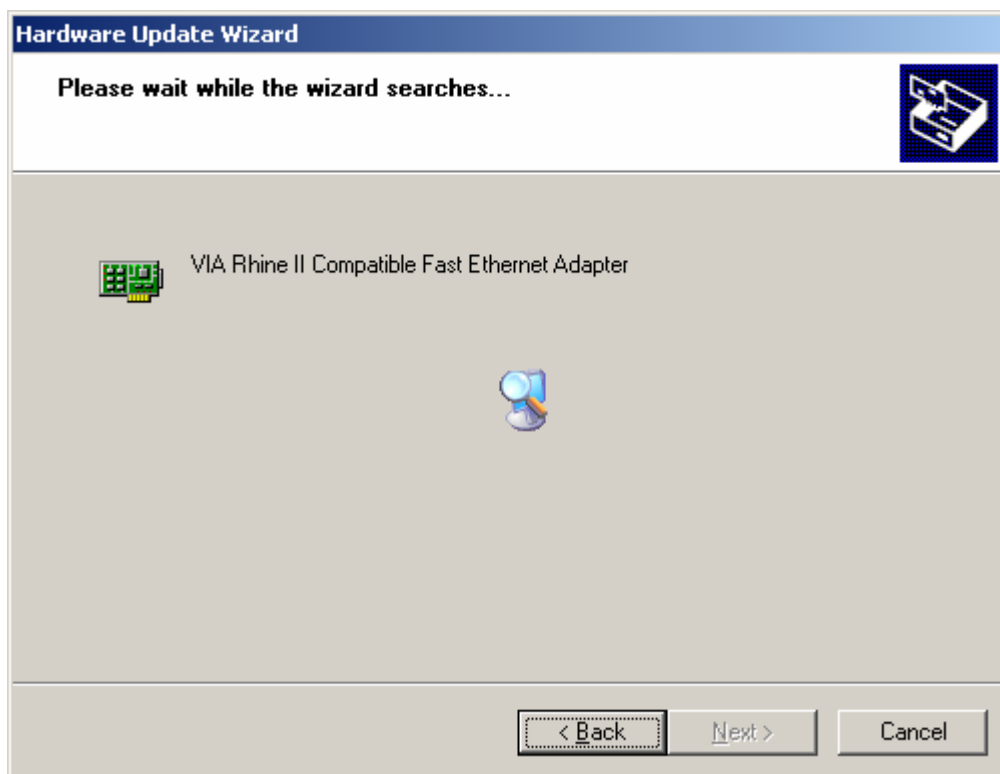
۴- در پنجره ظاهر شده گزینه اول را انتخاب و بر روی Next کلیک کنید.



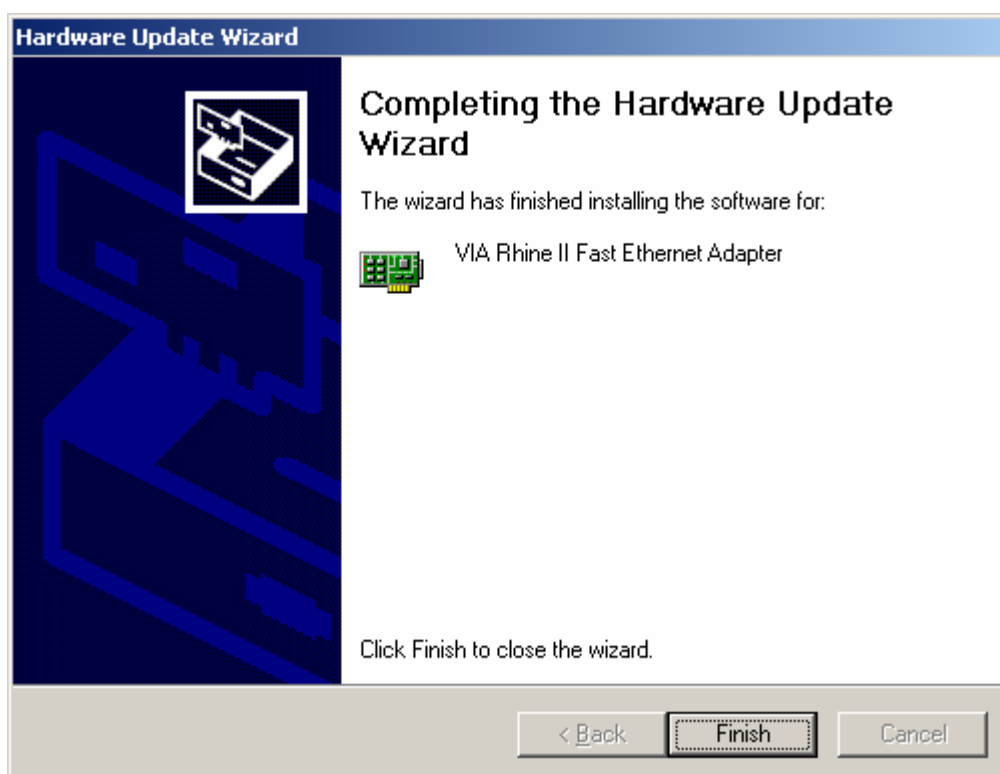
۵- در این پنجره گزینه اول را انتخاب کرده و Next کنید.



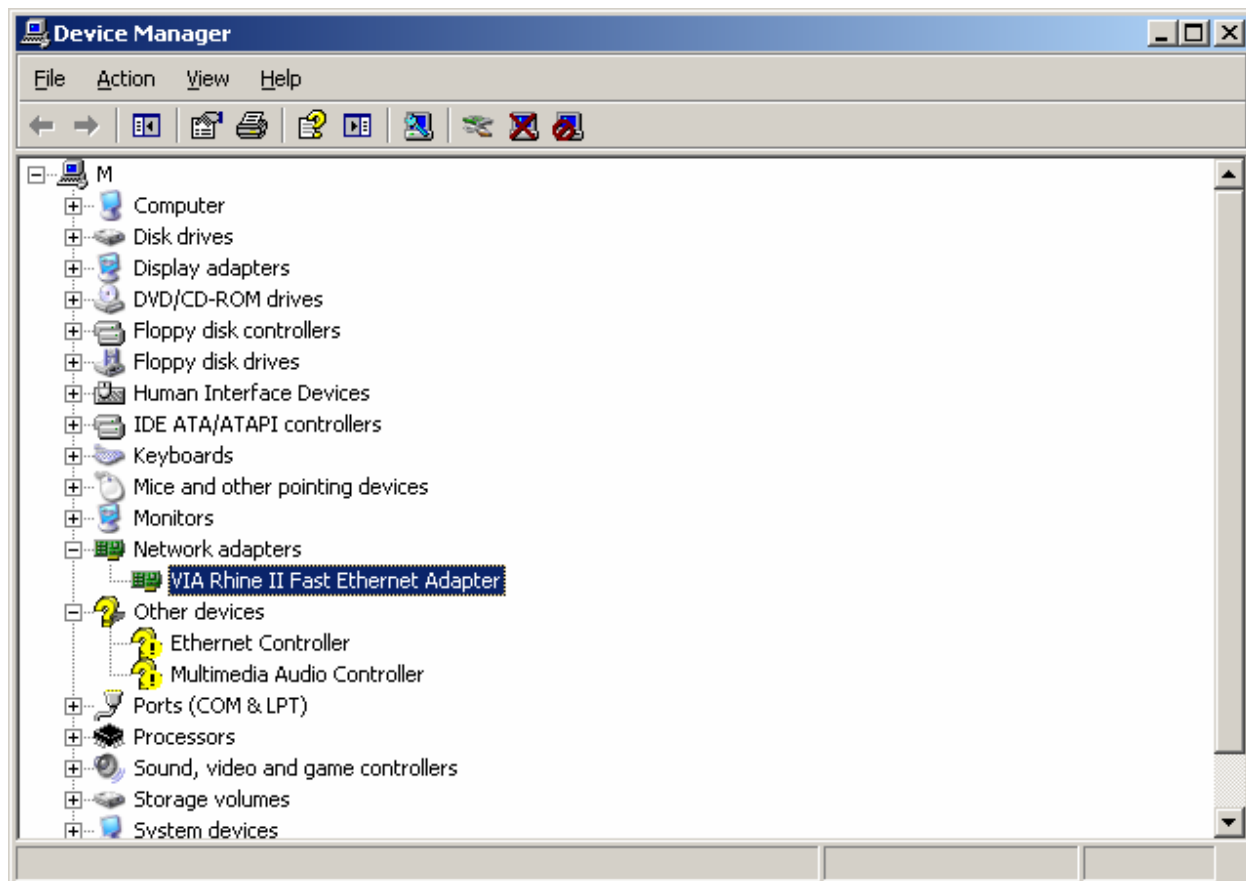
۶- در این پنجره کمی منتظر می مانید تا برنامه درایور کارت شبکه را از روی CD پیدا کرده و نصب کند.



۷- بعد از اتمام نصب پنجره زیر ظاهر می شود بر روی Finish کلیک کنید.



۸- اگر کارت شبکه درست نصب شده باشد علامت زرد دیگر نمایش داده نخواهد شد.



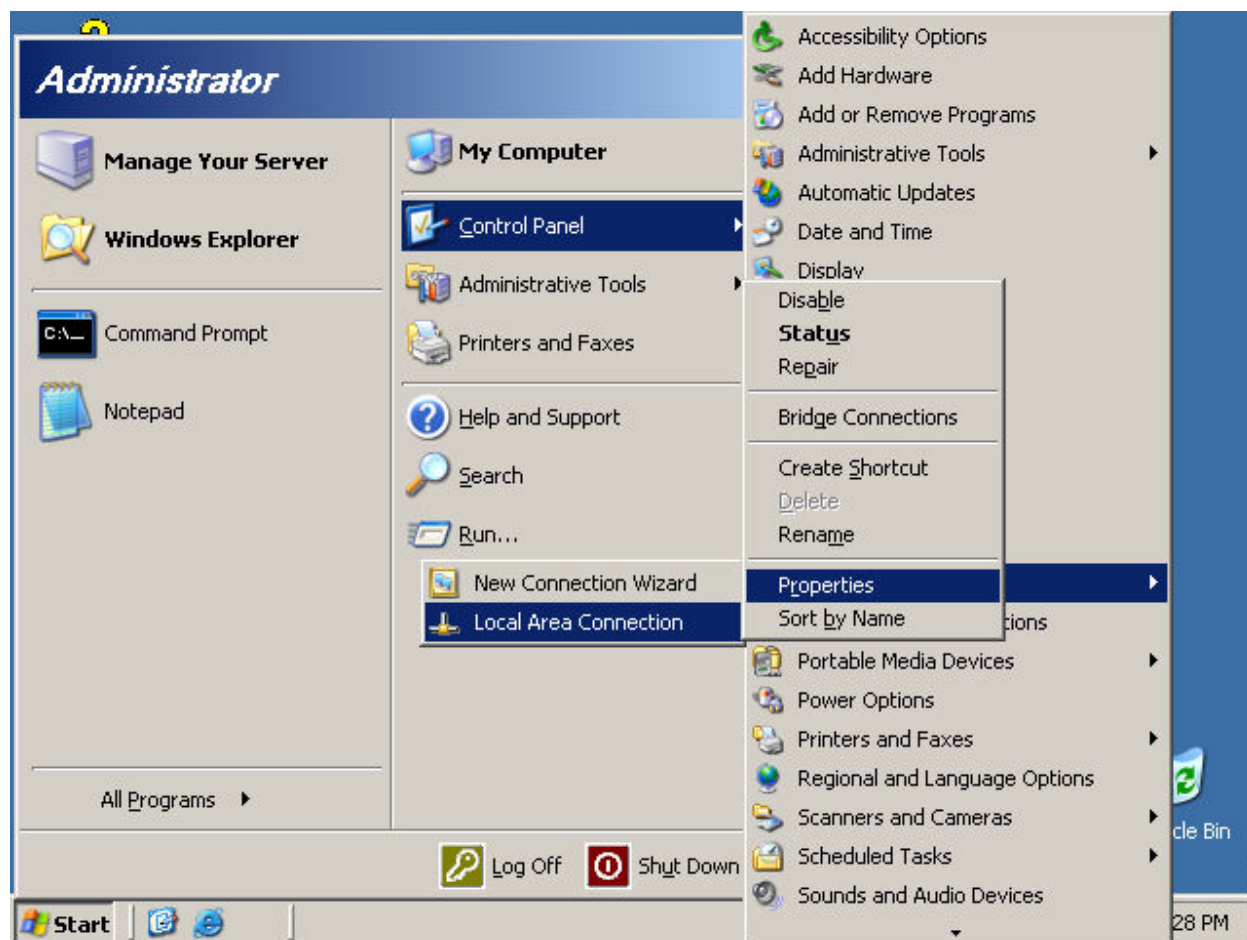
۲-۱-۷-۲- بررسی IP سرور:

اگر آدرس IP سرور را در هنگام نصب ویندوز تنظیم نکرده اید باید IP سرور را به صورت زیر، دستی تنظیم کنید:

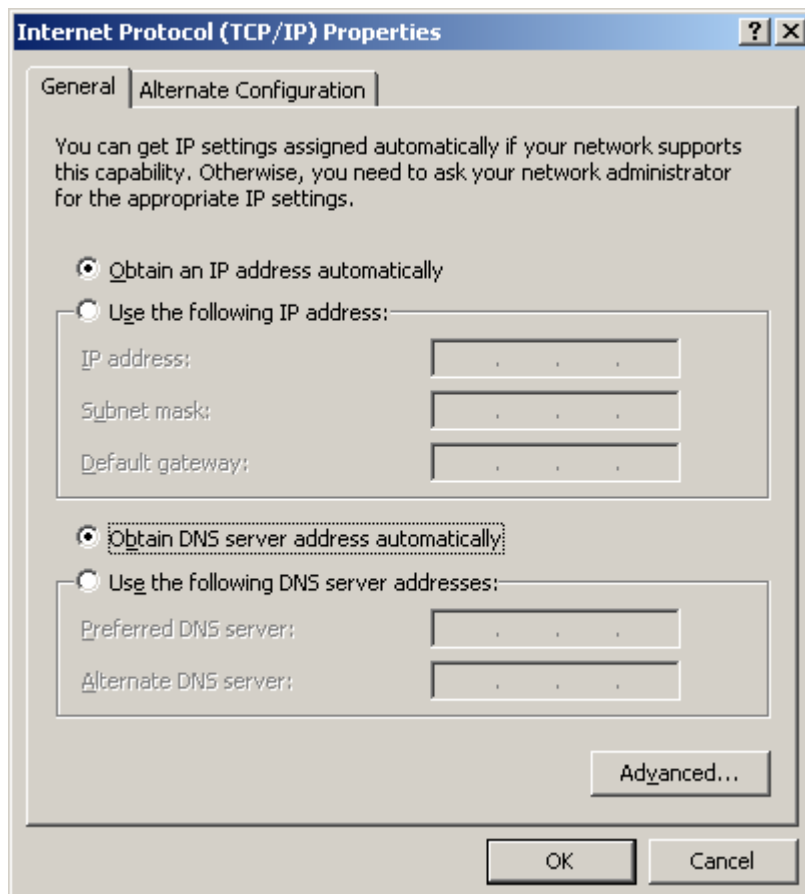
به مسیر زیر بروید:

Start > Control Panel > Network Connections

در منوی ظاهر شده روی Local Area Connection راست کلیک کرده و گزینه Properties کلیک کنید.



گزینه (TCP/IP) Internet Protocol را انتخاب و دکمه Properties بزنید تا همانطور که مشاهده می کنید پنجره Internet protocol (TCP/IP) Properties باز شود.



در این پنجره چهار انتخاب وجود دارد:

Obtain an IP address automatically: با انتخاب این گزینه IP به صورت اتوماتیک تنظیم می شود.

Use the following IP address: با انتخاب این گزینه IP را به صورت دستی تنظیم می کنیم.

Obtain DNS server address automatically: با انتخاب این گزینه DNS به صورت اتوماتیک تنظیم می شود.

Use the following DNS server address: با انتخاب این گزینه DNS را به صورت دستی تنظیم می کنیم.

در این پنجره برای دادن آدرس IP قسمت Use the following IP address را تیک می زنیم تا قسمت IP فعال شود. در داخل این پنجره سه قسمت وجود دارد:

ADDRESS IP:

در این قسمت آدرس IP را خواهیم داد.

مثلاً ۱۹۲,۱۶۸,۰,۱

SUBNET MASK: به معنای پوشش زیر شبکه در کلاس مورد نظر به صورت زیر است:

مثلاً در کلاس C ۲۵۵,۲۵۵,۲۵۵,۰

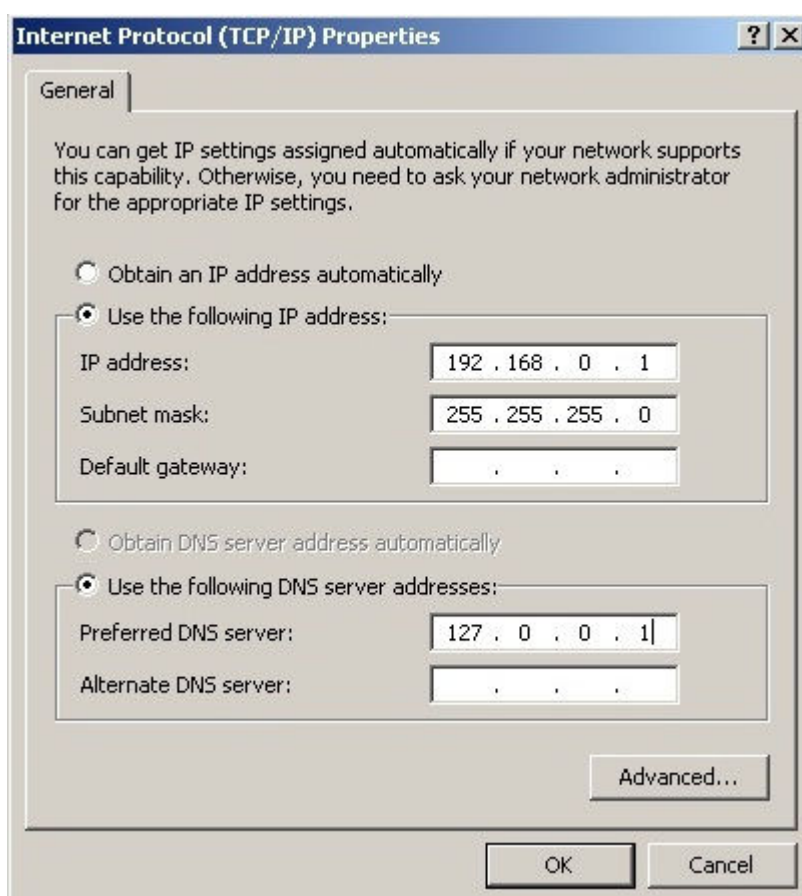
DEFAULT GETWAY: اگر در شبکه راه اندازی شده نیازی به وصل شدن به اینترنت نباشد لازم نیست که این گزینه تنظیم شود ولی اگر بخواهیم به اینترنت وصل شویم یکی از آدرس IP هایی را که می خواهیم به عنوان دروازه از آن استفاده کنیم را انتخاب و در تمام کامپیوتر ها وارد می کنیم.

(تنظیم Subnet Mask ضروری است ولی تنظیم Default Gateway اختیاری است.)

و در قسمت پایین Use the following DNS server address را انتخاب و DNS را به صورت دستی وارد می کنیم.

مثلاً ۱۲۷,۰,۰,۱

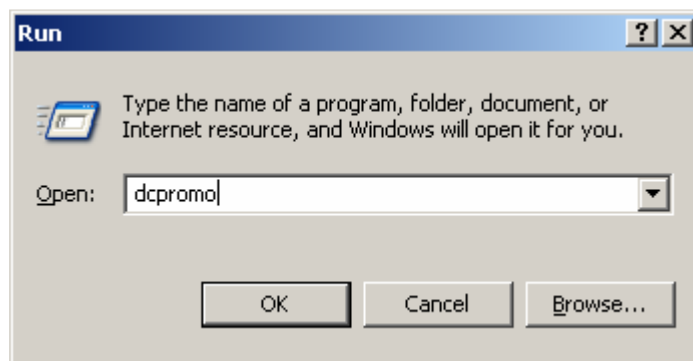
بعد از انجام این کارها IP و DNS سرور تنظیم شده است بر روی OK کلیک کنید.



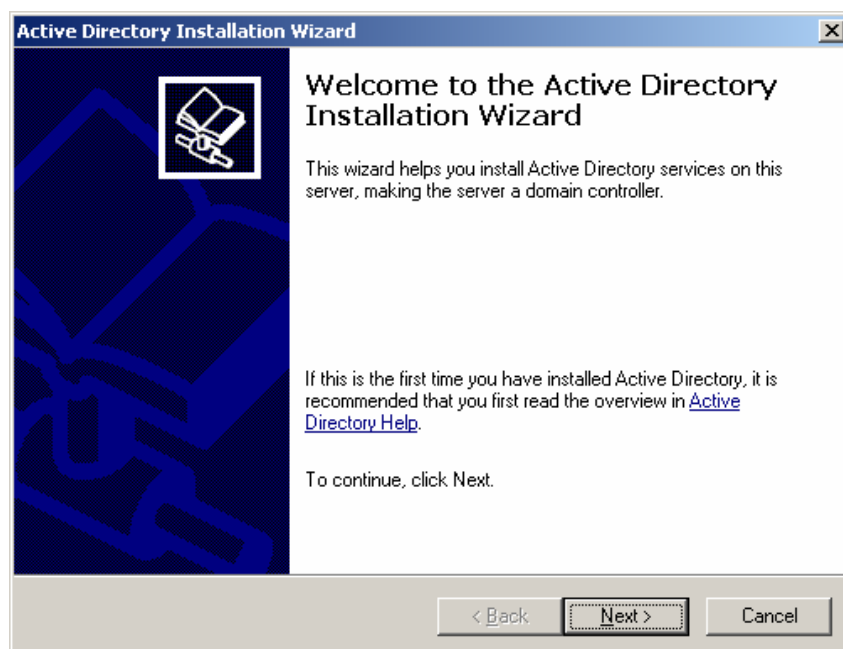
در پایان این قسمت دکمه Close را بزنید.

۲-۷-۲- بررسی نحوه نصب A.D از طریق DCPRMO:

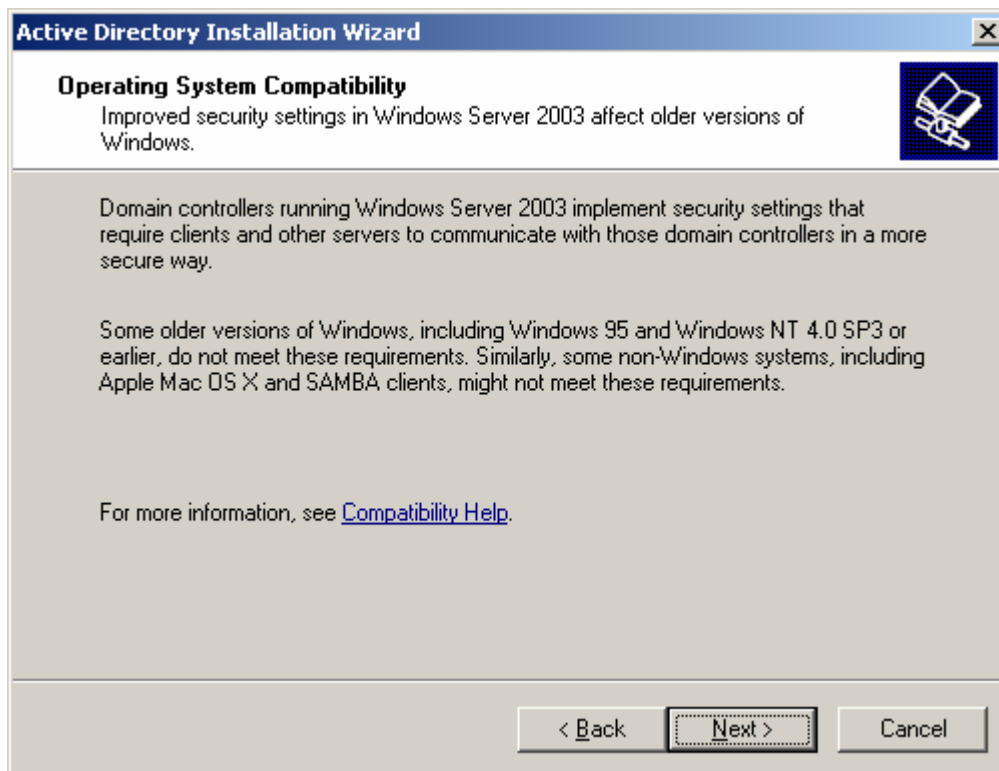
۱- روی منوی Start و سپس روی آیکن Run کلیک کرده در کادر Open تایپ کنید dcpromo و بر روی ok کلیک کنید.



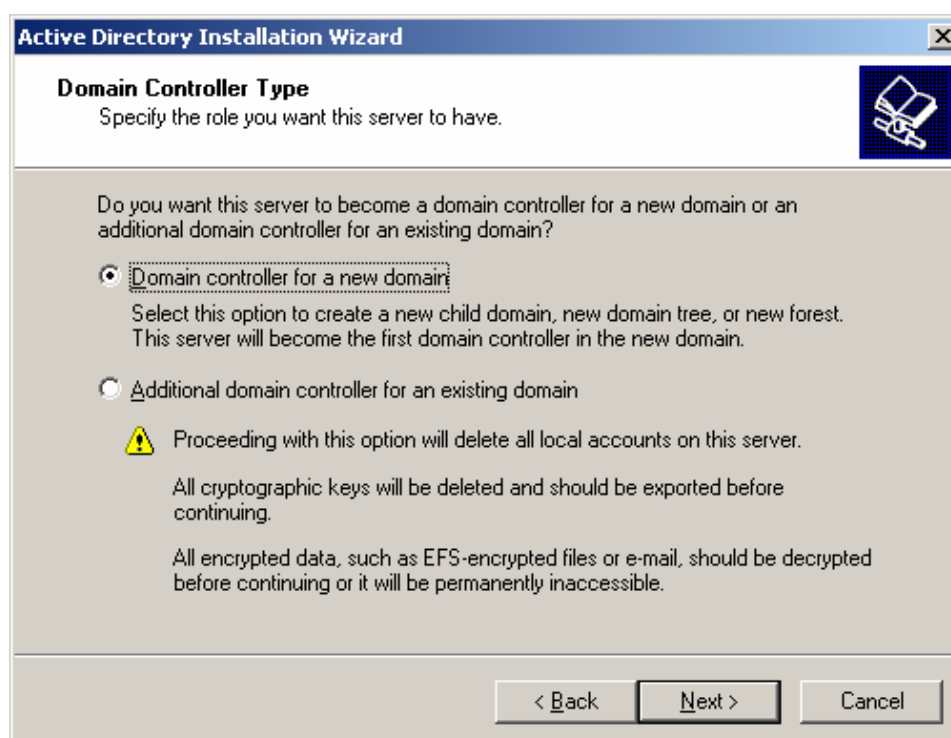
۲- در این صفحه پیام خوش آمد نصب AD ظاهر می شود.



۳- در این صفحه به شما هشدار می دهد که در صورتی که در شبکه خود کامپیوترهایی با سیستم عاملهای win 95 ، win NT ، apple Mac یا قدیمی تر داشته باشید نمی توانند به DC وصل شوند و عملیات Login را انجام دهند و نمی توانند از منابع به اشتراک گذاشته شده در شبکه استفاده کنند.

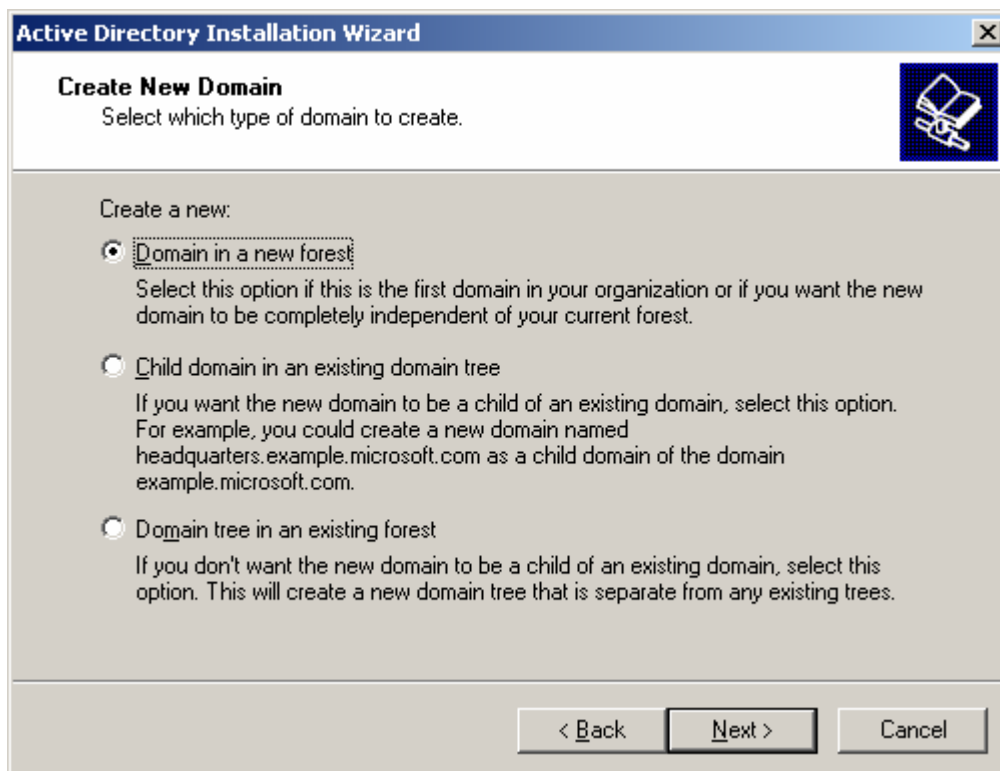


۴- در این پنجره دو گزینه وجود دارد در صورتی که گزینه اول را انتخاب کنید یعنی اینکه می خواهید اولین دامنه را به عنوان Domain controller ایجاد کنید در صورتی که گزینه دوم را انتخاب کنید یعنی اینکه می خواهید برای DC اول که قبلاً ایجاد کرده اید یک DC پشتیبان ایجاد کنید. چون شما قبلاً دامنه ای ایجاد نکرده اید گزینه اول را انتخاب و بر روی Next کلیک کنید.



۵- در این پنجره از شما می خواهد نوع Domain را که می خواهید ایجاد کنید را انتخاب کنید که در اینجا سه انتخاب وجود دارد:

- **Domain in a new forest**: انتخاب این گزینه یعنی اینکه شما دامنه ای را هنوز ایجاد نکرده اید و این دامنه به عنوان ریشه خواهد بود.
 - **Child domain in an existing domain tree**: اگر دامنه ریشه را قبلاً ایجاد کرده باشید و بخواهید دامنه ای را که اکنون ایجاد کنید فرزندی از یک درخت باشد این گزینه را انتخاب کنید.
 - **Domain tree in an existing forest**: اگر درختی را قبلاً ایجاد کرده باشید و بخواهید دامنه ای را که اکنون ایجاد کنید فرزندی از یک جنگل باشد این گزینه را انتخاب کنید.
- چون شما دامنه ای قبلاً ایجاد نکرده اید گزینه اول را انتخاب و بر روی Next کلیک کنید.



۶- در این صفحه که بسیار مهم می باشد شما باید نام Domain اکتیو دایرکتوری را همراه با یک پسوند وارد کنید. مثلاً به شکل vahid.local نامگذاری کرده و سپس روی دکمه NEXT کلیک کنید. به یاد داشته باشید که باید پسوند مثلاً "local" در انتهای اسم نوشته شود

برای انتخاب این اسم بایستی موارد زیر را در نظر داشته باشید :

۱- نام هیچ کامپیوتری در شبکه را برابر با نام Domain نگذارید.

۲- سعی کنید نامی را انتخاب کنید که بعداً زمانی که شبکه خود را به اینترنت وصل می کنید مشکل نداشته باشید. به عنوان مثال در صورتی که نام Domain خود را microsoft.com انتخاب کنید و شبکه خود را به اینترنت وصل کنید در داخل DNS یکسری مشکلات خواهید داشت و باید تنظیماتی را انجام دهید. (پیشنهاد می کنم که هر نامی را که دوست دارید انتخاب کنید و در انتهای آن "local" را اضافه کنید چراکه پسوند "local" در اینترنت وجود ندارد.

Active Directory Installation Wizard

New Domain Name
Specify a name for the new domain.

Type the full DNS name for the new domain
(for example: headquarters.example.microsoft.com).

Full DNS name for new domain:

vahid.local

< Back Next > Cancel

۷- در این صفحه میتوانید نام NetBIOS را تغییر دهید. بهتر است نام NetBIOS همانم دامین اما بدون قرار دادن پسوند local باشد. (تا نسخه های قدیمی ویندوز از طریق آن Domain جدید را شناسایی کنند) بر روی Next کلیک کنید.

Active Directory Installation Wizard

NetBIOS Domain Name
Specify a NetBIOS name for the new domain.

This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.

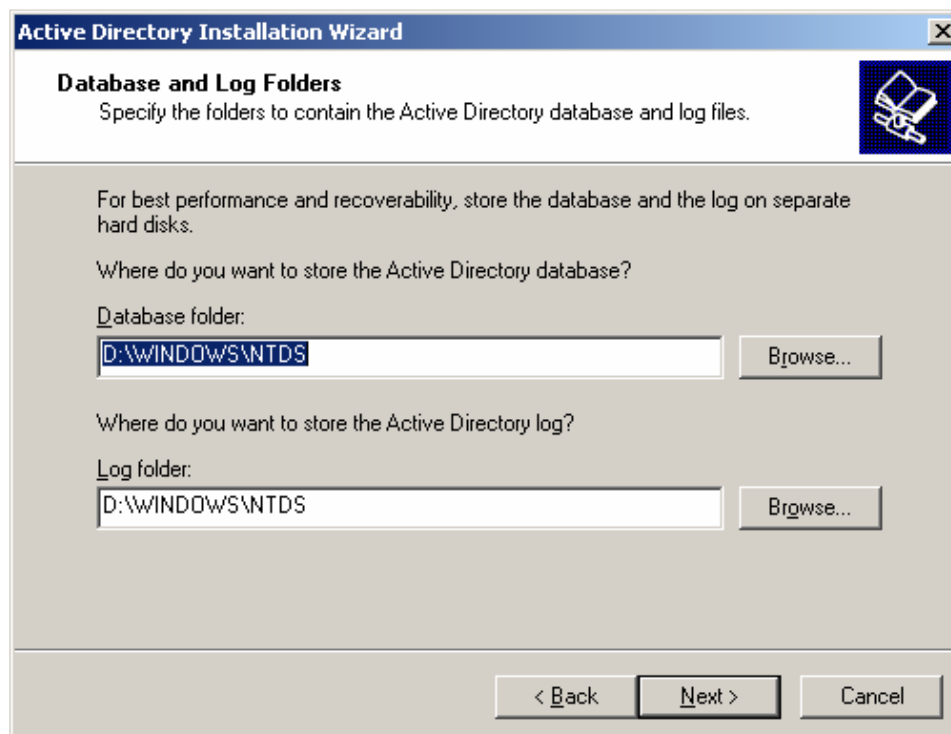
Domain NetBIOS name:

VAHID

< Back Next > Cancel

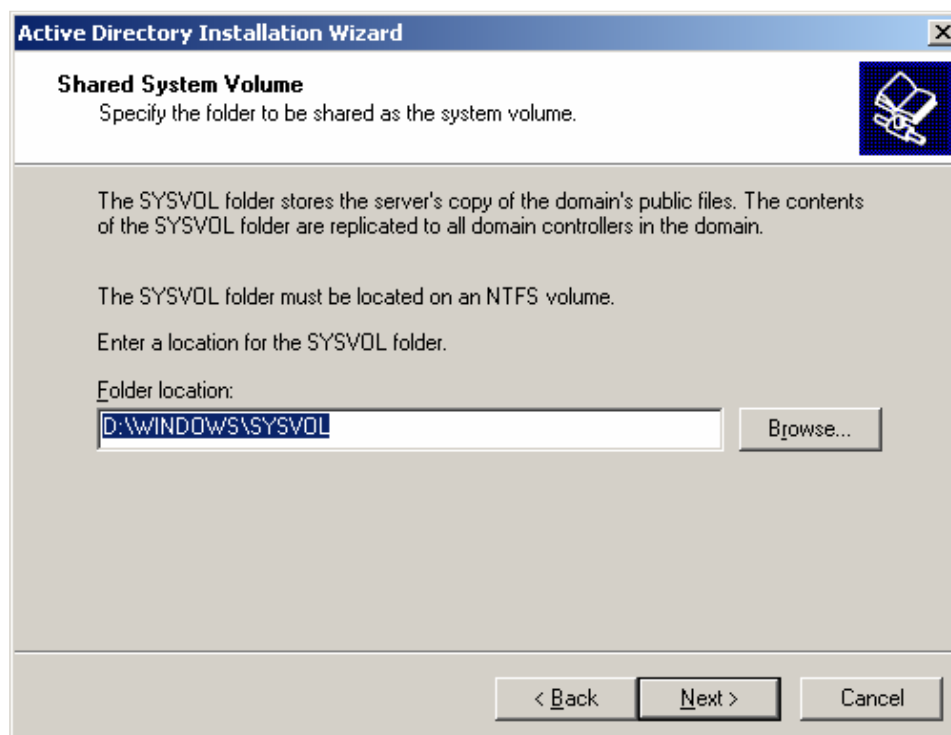
۸- در مسیر Database فایل هایی که قرار است اطلاعات و ویژگی های کاربران در آن ذخیره شود تنظیم می گردد.

در مسیر Log اطلاعات مربوط به فعالیت (زمان ورود، زمان خروج از سیستم) کاربران ذخیره می شود، که می توانید آن را تغییر دهید. بر روی Next کلیک کنید.



The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'Database and Log Folders' step. The title bar reads 'Active Directory Installation Wizard'. Below the title bar, the section is titled 'Database and Log Folders' with the instruction 'Specify the folders to contain the Active Directory database and log files.' A small icon of a folder with a document is on the right. The main area contains the text: 'For best performance and recoverability, store the database and the log on separate hard disks.' followed by 'Where do you want to store the Active Directory database?'. Below this is a text box labeled 'Database folder:' containing 'D:\WINDOWS\NTDS' and a 'Browse...' button. Then, 'Where do you want to store the Active Directory log?' is followed by a text box labeled 'Log folder:' also containing 'D:\WINDOWS\NTDS' and a 'Browse...' button. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

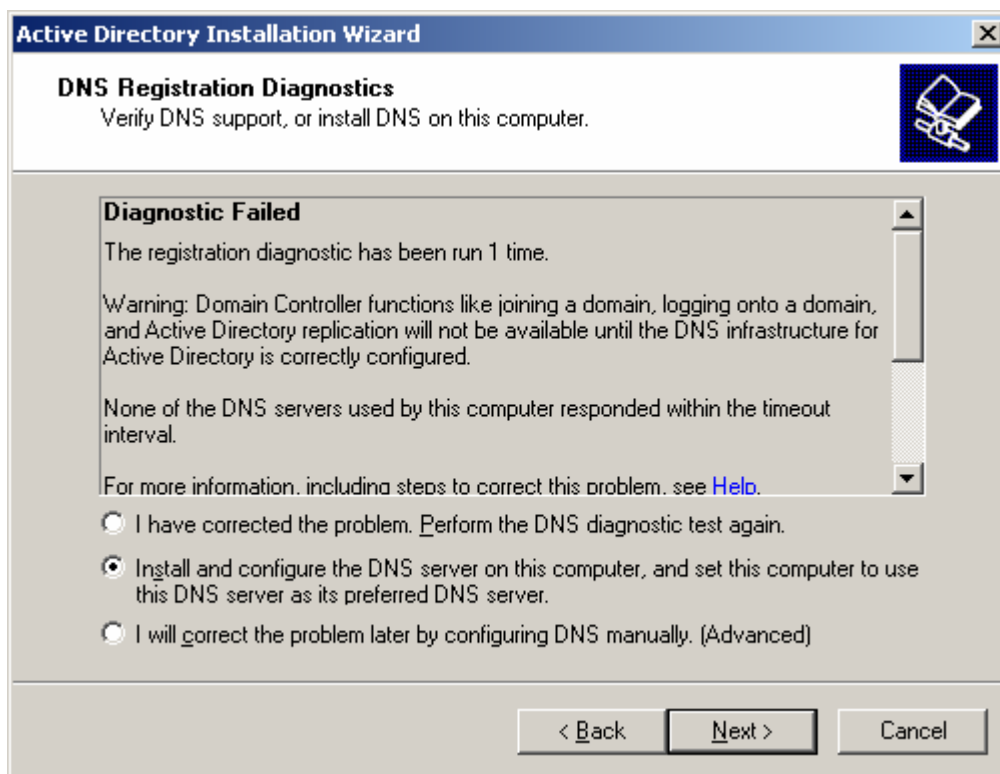
۹- در این صفحه آدرس پیش فرض فولدری که بین دامنه ها به اشتراک گذاشته می شود نمایش داده می شود. قابل ذکر است که محل این فولدر حتما باید بر پارتیشنی به فورمت NTFS باشد. فایل های موجود در این فولدر حاوی سیاست های کلی تعریف شده در داخل ساختار AD می باشد. همچنین مدیر می تواند در صورت بروز مشکل در دامنه، آن را از طریق دامنه های دیگر و از این مسیر بازیابی کند.



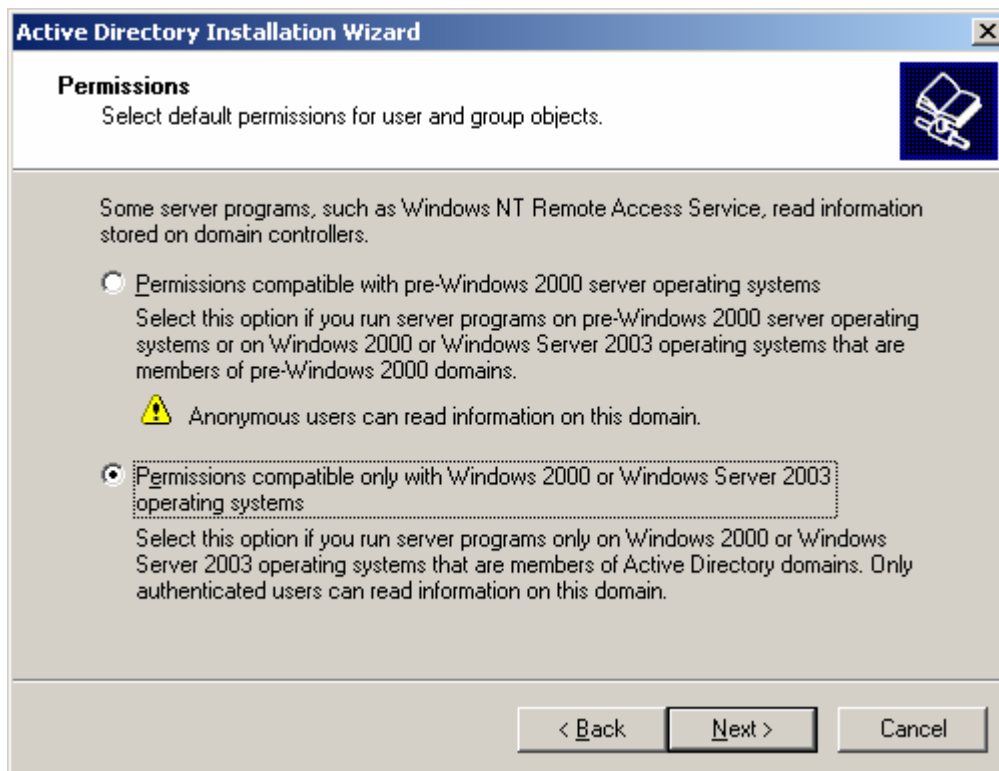
The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'Shared System Volume' step. The title bar reads 'Active Directory Installation Wizard'. Below the title bar, the section is titled 'Shared System Volume' with the instruction 'Specify the folder to be shared as the system volume.' A small icon of a folder with a document is on the right. The main area contains the text: 'The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.' followed by 'The SYSVOL folder must be located on an NTFS volume.' and 'Enter a location for the SYSVOL folder.' Below this is a text box labeled 'Folder location:' containing 'D:\WINDOWS\SYSVOL' and a 'Browse...' button. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

۱۰- اگر DNS را تنظیم نکرده باشید این پنجره ظاهر می شود (DNS برای دادن IP اتوماتیک در شبکه است) در این صفحه سه انتخاب وجود دارد:

- اگر قبلاً DNS نصب کرده باشید و الان با مشکل روبه رو شده باشید و بخواهید آن را برطرف کنید از این گزینه استفاده می کنید.
 - انتخاب گزینه دوم یعنی در حین نصب اکتیو دایرکتوری، DNS نیز به صورت خودکار نصب شود.
 - انتخاب گزینه سوم یعنی تنظیمات DNS را بعداً به صورت دستی انجام خواهیم داد.
- گزینه دوم را انتخاب کرده نا در حین نصب، DNS نیز نصب شود و بر روی Next کلیک کنید.




۱۱- در این مرحله انتخاب کلاینتهایی می باشد که با سرور ما ارتباط برقرار می کنند که گزینه اول برای پلاتفرم های قبل از ۲۰۰۰ می باشد و دومین گزینه پلاتفرم های ۲۰۰۰ و ۲۰۰۳ را پشتیبانی می کند که در شکل زیر مشاهده می کنید: گزینه دوم را انتخاب و Next کنید.



Active Directory Installation Wizard

Permissions
Select default permissions for user and group objects.

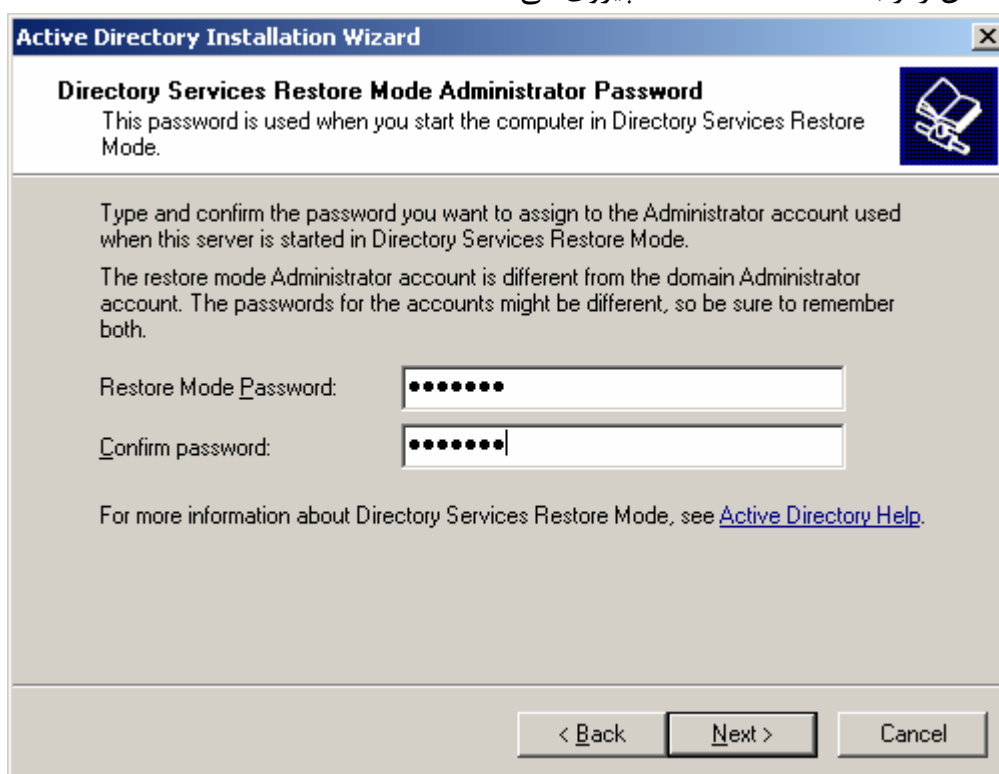
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.

☐ Permissions compatible with pre-Windows 2000 server operating systems
Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.
 Anonymous users can read information on this domain.

☒ Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems
Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.

< Back Next > Cancel

۱۲- در این صفحه باید رمزی را برای حالت DSRM یا (Directory Services Restore Mode) اختصاص دهید. از این رمز برای بازبازی AD در صورت لزوم استفاده می شود که باید با رمز Admin متفاوت باشد. (این رمز نیز از همان ویژگی های دادن رمز به Administrator پیروی می کند)



Active Directory Installation Wizard

Directory Services Restore Mode Administrator Password
This password is used when you start the computer in Directory Services Restore Mode.

Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.

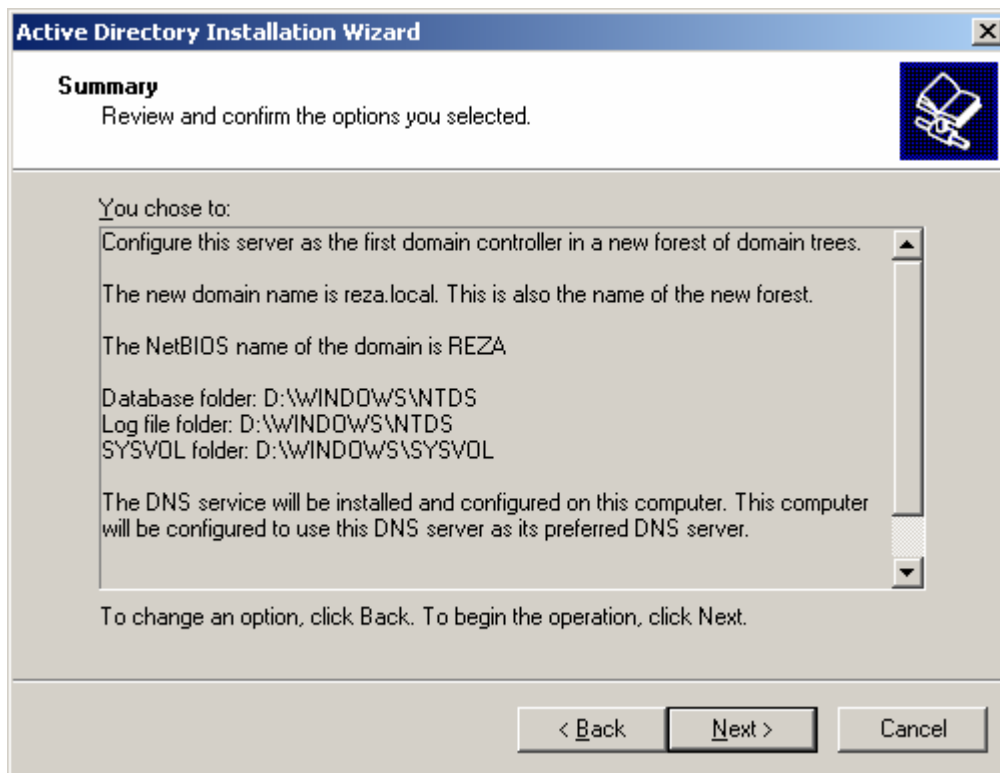
Restore Mode Password:

Confirm password:

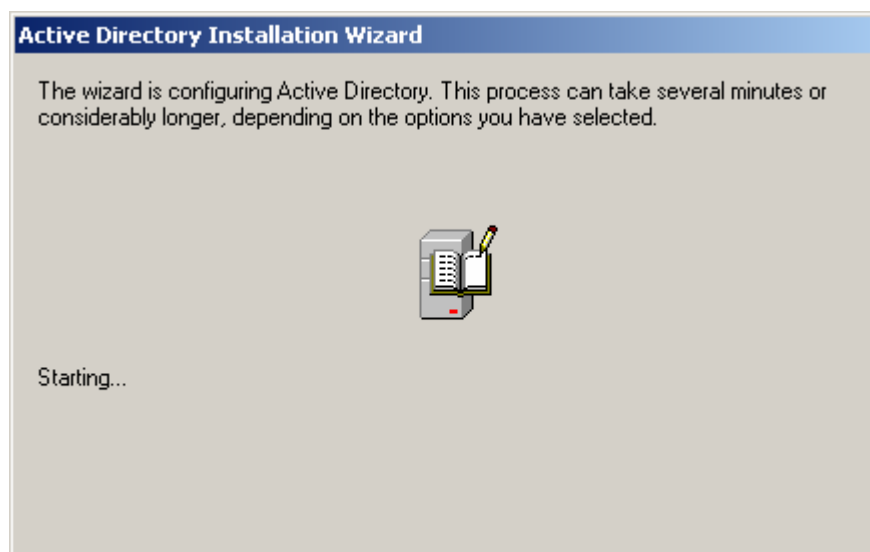
For more information about Directory Services Restore Mode, see [Active Directory Help](#).

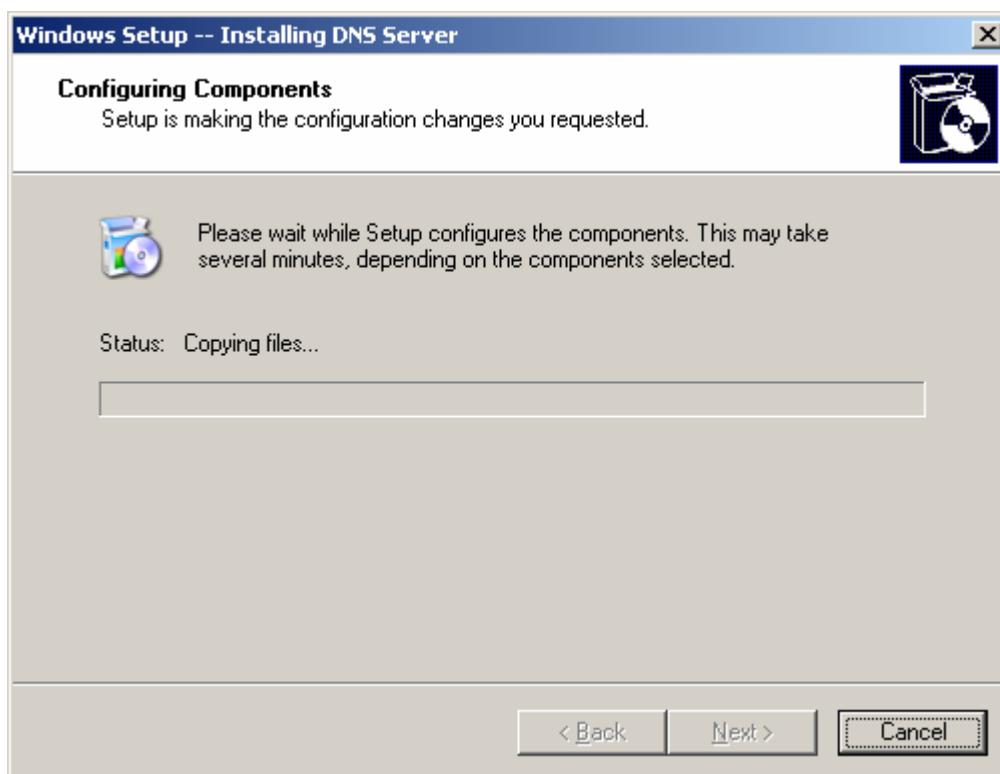
< Back Next > Cancel

۱۳- در صفحه نهایی تمامی تنظیماتی را که در صفحه های پیشین وارد نمودید به طور یکجا و به صورت Information نشان می دهد. در صورتی که مشکلی نمی بینید و تمامی تنظیمات درست است بر روی Next کلیک کنید تا عملیات نصب آغاز شود.

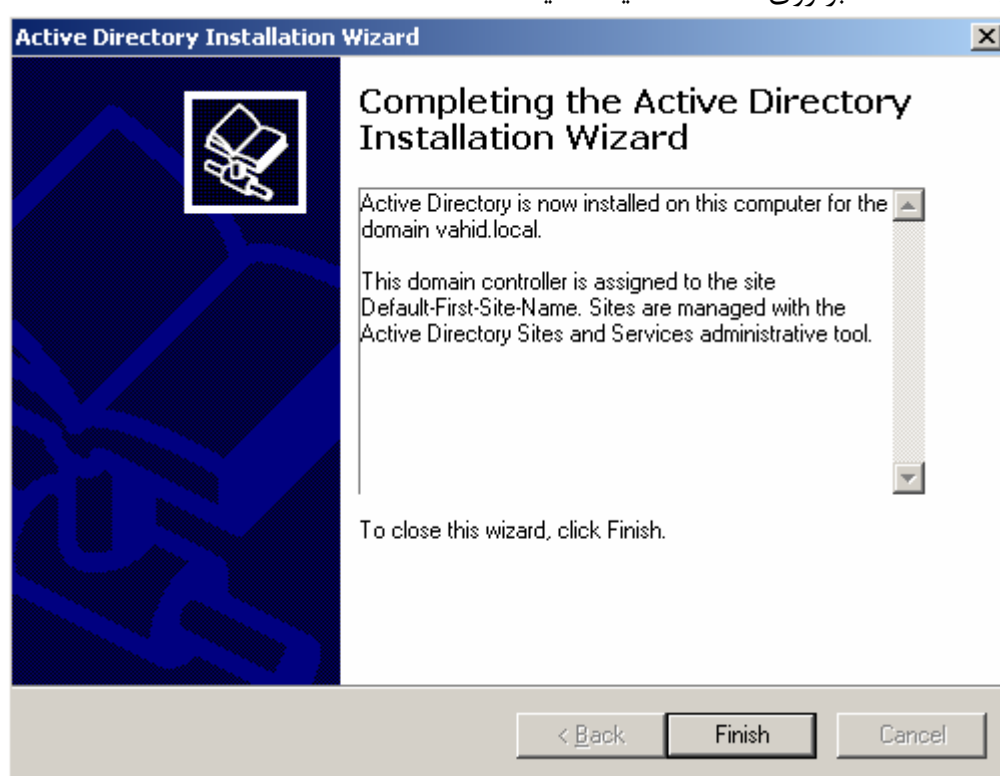


۱۴- پس از Next کردن صفحه زیر برای شما نمایان خواهد شد که عملیات مختلف نصب AD و پیکربندی آن را نشان می دهد .





۱۵- بعد از پایان یافتن نصب AD این پنجره نمایش داده می شود که توضیح می دهد AD بر روی این کامپیوتر با دامنه vahid.local ایجاد شده است. بر روی Finish کلیک کنید.



۱۶- بعد از پایان یافتن نصب اکتیو دایرکتوری این پنجره نشان داده می شود که از شما میخواهد برای بهتر اعمال شدن تنظیمات، سیستم را رستارت نمایید.

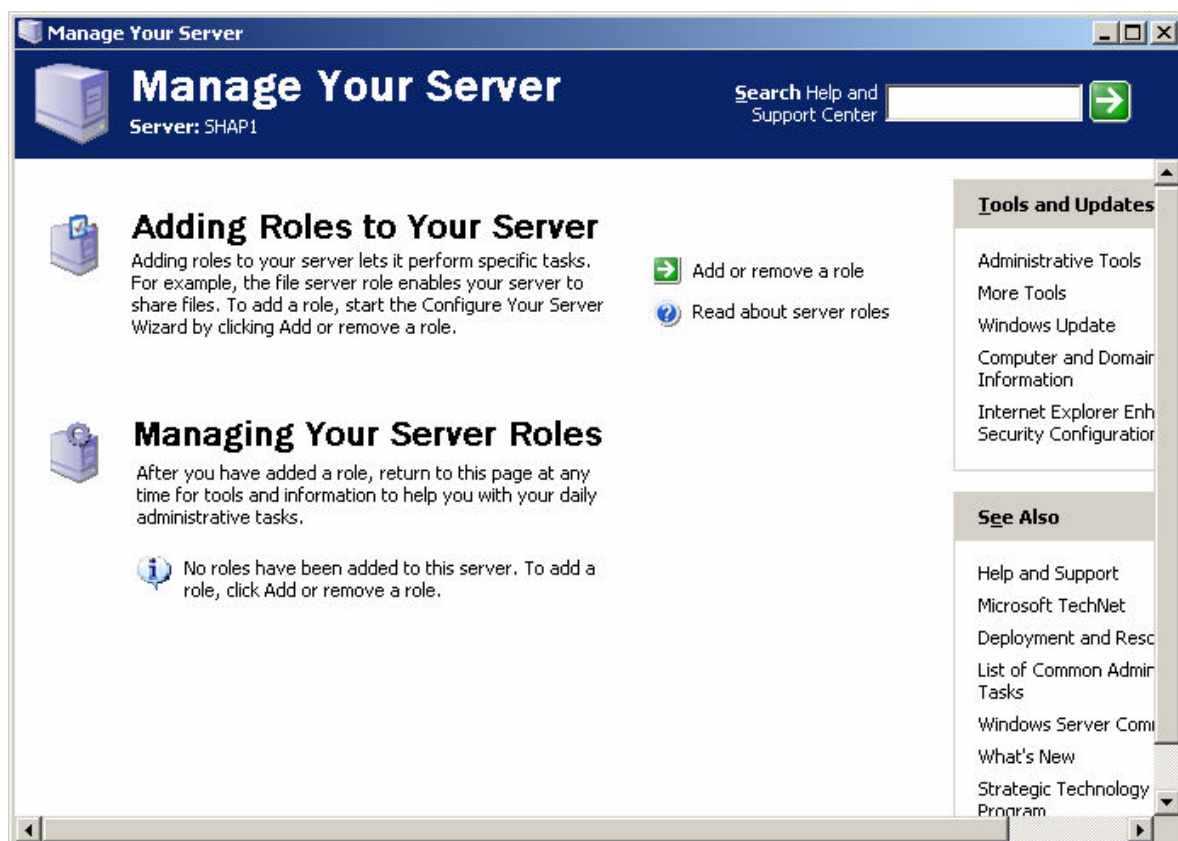


۱۷- در اینجا نیز بعد از راه اندازی مجدد در پنجره ورود به سیستم نام دامنه ای که ایجاد کرده ایم نمایش داده می شود.

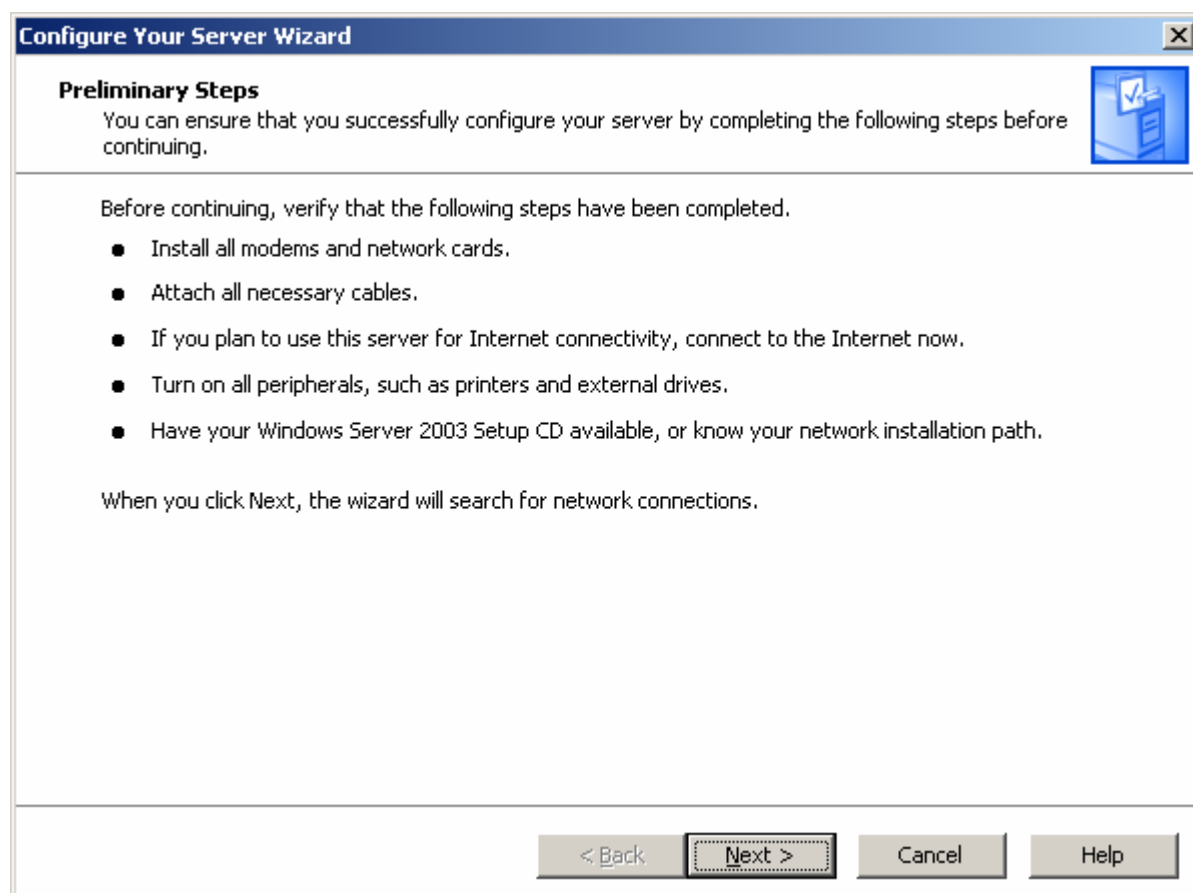


۳-۷-۲- بررسی نحوه نصب A.D از طریق پنجره Manage Your Server:

۱- پس از نصب و بالا آمدن ویندوز سرور ۲۰۰۳ پنجره زیر ظاهر می شود. در صورت ظاهر نشدن روی دکمه Start کلیک کرده و روی آیکن Manage Your Server کلیک کنید تا پنجره ی زیر باز شود. سپس روی گزینه Add or remove a role کلیک نمایید تا یک نقش جدید برای سرور ایجاد کنید.



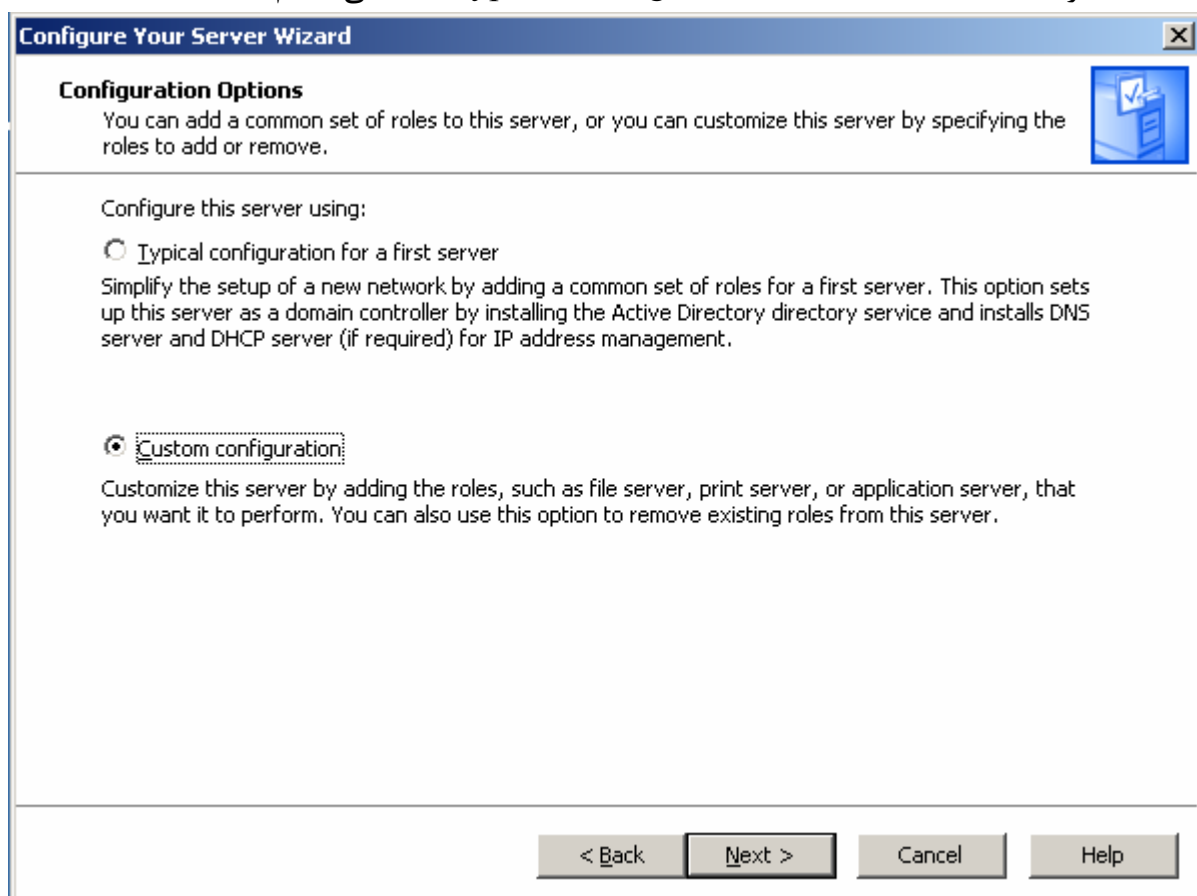
۲- در پنجره ای که ظاهر می شود به شما گفته میشود که قبل از اینکه مراحل نصب را طی کنید باید اول موارد خواسته شده مانند نصب مودم ها و کارت های شبکه، متصل کردن کابل ها، گذاشتن CD ویندوز داخل CD-ROM و ... را انجام داده، سپس روی دکمه Next کلیک کنید.



۳- این پنجره در نخستین بار که می خواهیم نقشی را به سرور دهید (AD و DNS و DHCP تنظیم نشده باشد) ظاهر می شود. در این پنجره دو گزینه وجود دارد:

- **Typical configuration for a first server:** با انتخاب این گزینه تنظیمات AD و DNS و DHCP سرور به صورت اتوماتیک تنظیم می شود.
- **Custom configuration:** با انتخاب این گزینه می تواند هر نقشی را که به سرور بدهید را به صورت دستی تنظیم کنید.

یکبار گزینه Custom configuration را انتخاب می کنیم تا پنجره ای که باز می شود را ببینید بعد Back می کنیم و نصب را با انتخاب گزینه Typical configuration for a first server ادامه می دهیم.



در این پنجره لیستی از نقشه‌هایی وجود دارد که هنوز هیچ یک از آنها به سرور داده نشده است. اگر بخواهیم با این روش نصب کنیم (Domain Controller(Active Directory را انتخاب و ادامه می دهیم ولی چون ما می خواهیم به صورت اتوماتیک نصب کنیم بر روی Back کلیک کرده تا به صفحه قبلی برگردیم.

Configure Your Server Wizard

Server Role

You can set up this server to perform one or more specific roles. If you want to add more than one role to this server, you can run this wizard again.

Select a role. If the role has not been added, you can add it. If it has already been added, you can remove it. If the role you want to add or remove is not listed, open [Add or Remove Programs](#).

Server Role	Configured
File server	No
Print server	No
Application server (IIS, ASP.NET)	No
Mail server (POP3, SMTP)	No
Terminal server	No
Remote access / VPN server	No
Domain Controller (Active Directory)	No
DNS server	No
DHCP server	No
Streaming media server	No
WINS server	No

Domain Controller (Active Directory)

Domain controllers store directory data and manage user logon processes and directory searches.

[Read about domain controllers](#)

View the [Configure Your Server log](#).

< Back Next > Cancel Help

۴- گزینه Typical configuration for a first server را انتخاب و بر روی Next کلیک کنید.

Configure Your Server Wizard

Configuration Options

You can add a common set of roles to this server, or you can customize this server by specifying the roles to add or remove.

Configure this server using:

☒ **Typical configuration for a first server**

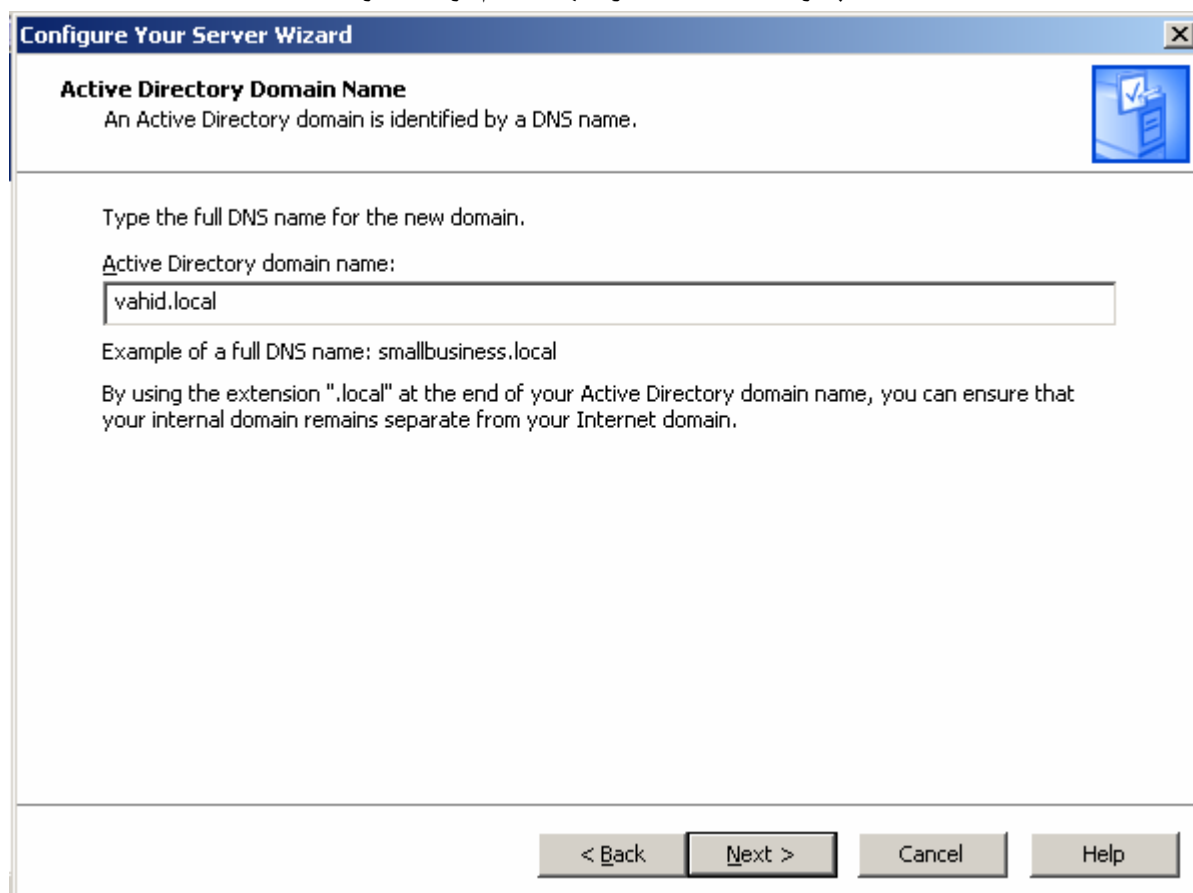
Simplify the setup of a new network by adding a common set of roles for a first server. This option sets up this server as a domain controller by installing the Active Directory directory service and installs DNS server and DHCP server (if required) for IP address management.

☐ Custom configuration

Customize this server by adding the roles, such as file server, print server, or application server, that you want it to perform. You can also use this option to remove existing roles from this server.

< Back Next > Cancel Help

۵- در این صفحه نام domain اکتیو دایرکتوری را به شکل vahid.local نامگذاری کنید و سپس روی دکمه NEXT کلیک کنید. (به یاد داشته باشید که باید پسوند ".local" در انتهای اسم نوشته شود)



Configure Your Server Wizard

Active Directory Domain Name
An Active Directory domain is identified by a DNS name.

Type the full DNS name for the new domain.

Active Directory domain name:
vahid.local

Example of a full DNS name: smallbusiness.local

By using the extension ".local" at the end of your Active Directory domain name, you can ensure that your internal domain remains separate from your Internet domain.

< Back Next > Cancel Help

۶- در این صفحه میتوانید نام NetBIOS را تغییر دهید. بهتر است نام NetBIOS همانم دامین اما بدون قرار دادن پسوند local باشد. (زمانی که می خواهیم Client را به Domain سرور وصل کنیم از نام NetBIOS استفاده می کنیم) بر روی Next کلیک کنید

Configure Your Server Wizard

NetBIOS Name
 Clients running versions of Windows other than Windows 2000, Windows XP, and the Windows Server 2003 family will use the NetBIOS domain name.

The default NetBIOS name is derived from the DNS domain name.

DNS domain name:

To change the default NetBIOS name, type a new name in the text box below.

NetBIOS domain name:

< Back Next > Cancel Help

۷- در این پنجره توضیح داده می شود که با انتخاب دکمه Next سه تا نقش AD ، DNS ، DHCP بر روی سرور نصب می شود، دکمه Next را بزنید.

Configure Your Server Wizard

Summary of Selections
 View and confirm the options you have selected.

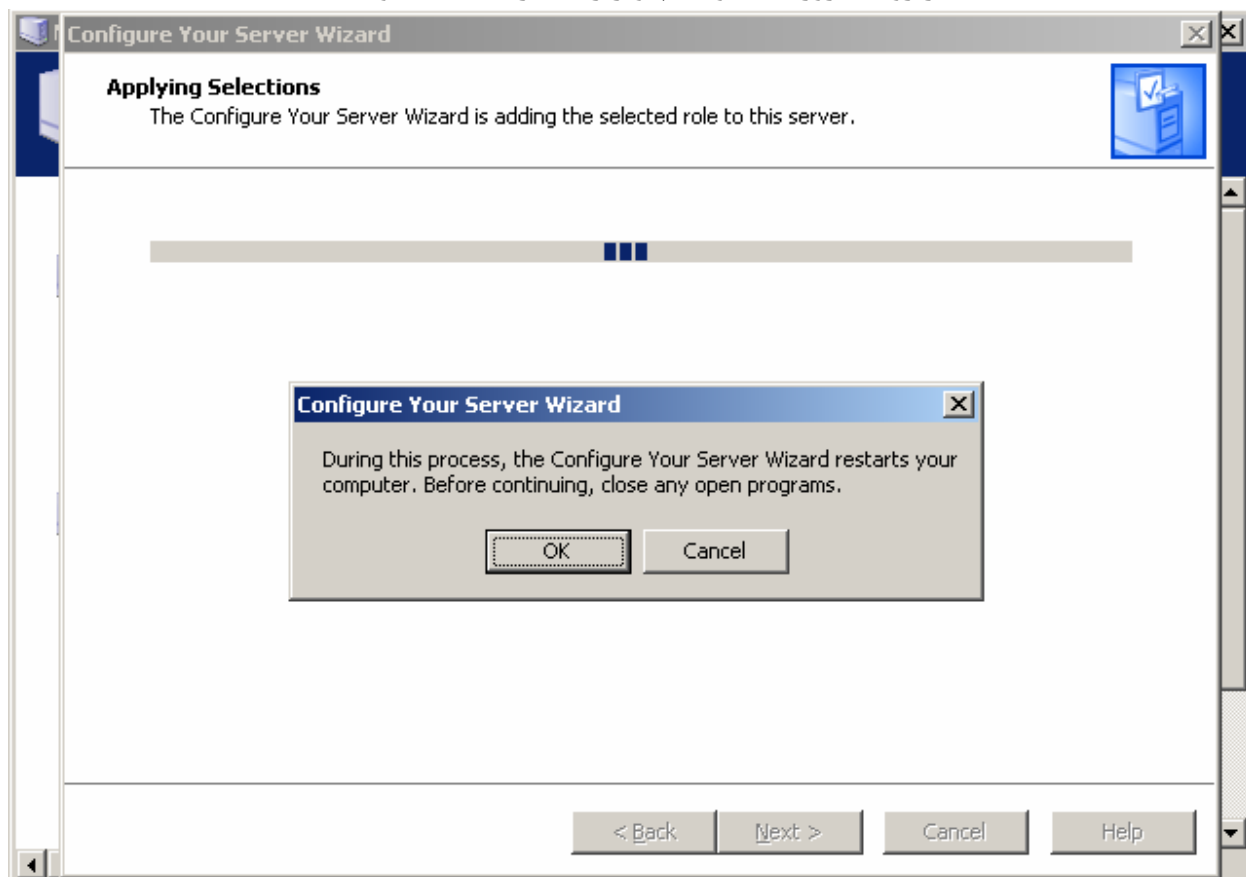
Summary:

Install DHCP server (if required)
 Install Active Directory and DNS server (sets up this server as a domain controller)
 Create the following full domain name: vahid.local

To change your selections, click Back. To continue setting up this role, click Next.

< Back Next > Cancel Help

۸- در این پنجره پیغام داده می شود که بعد از نصب، کامپیوتر به صورت اتوماتیک restart می شود. بر روی Ok کلیک کنید تا AD ، DNS ، DHCP بر روی سرور نصب و کامپیوتر راه اندازی مجدد شود.

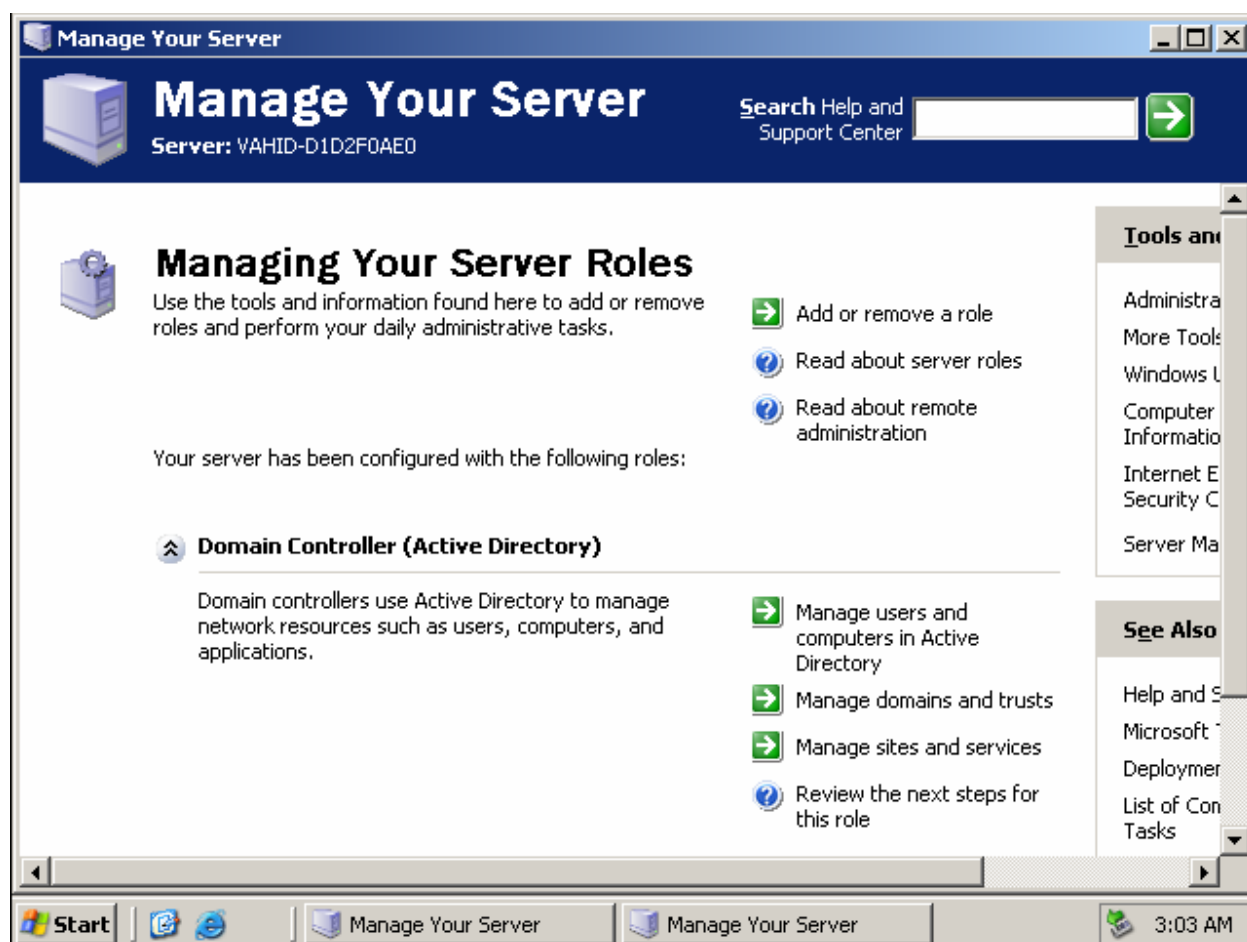


۹- در اینجا نیز بعد از راه اندازی مجدد در پنجره ورود به سیستم نام دامنه ای که ایجاد کرده اید نمایش داده می شود.

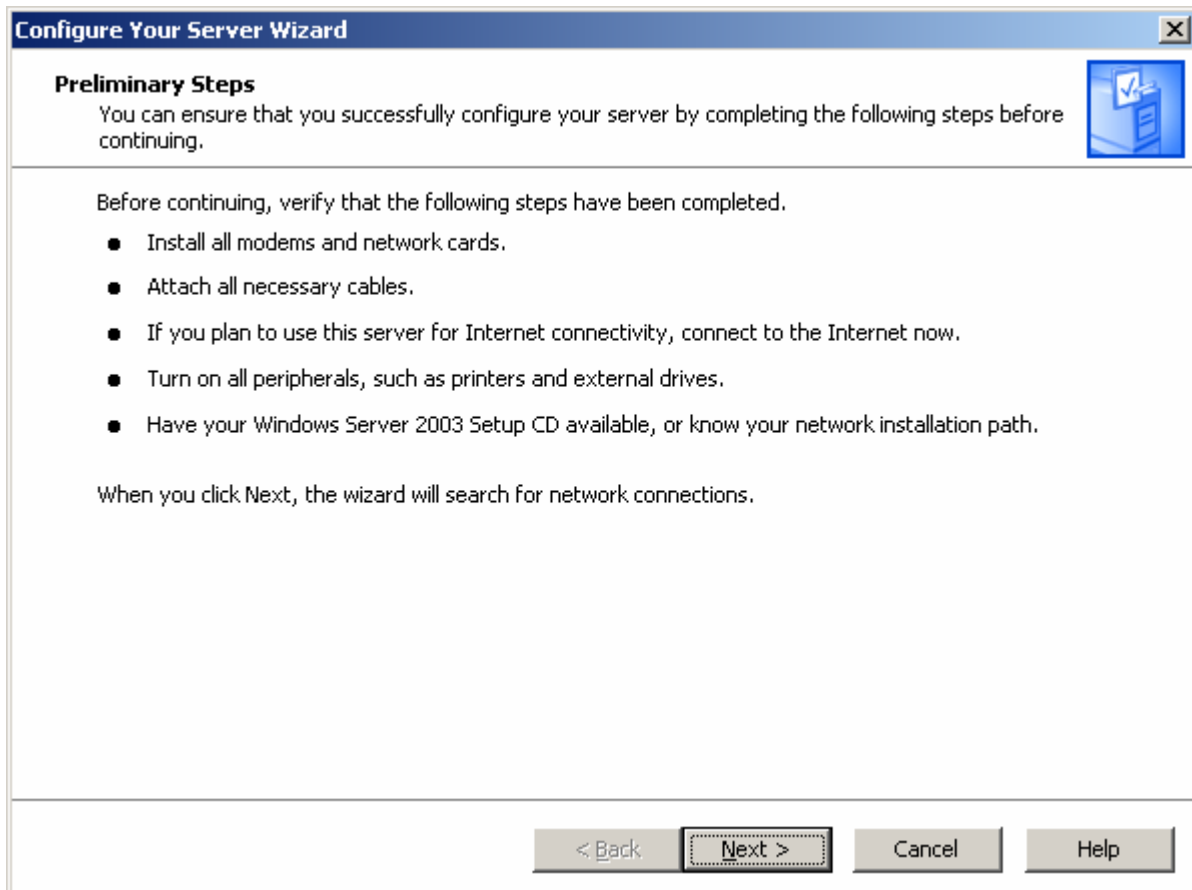


۸-۲- بررسی نحوه حذف A.D:

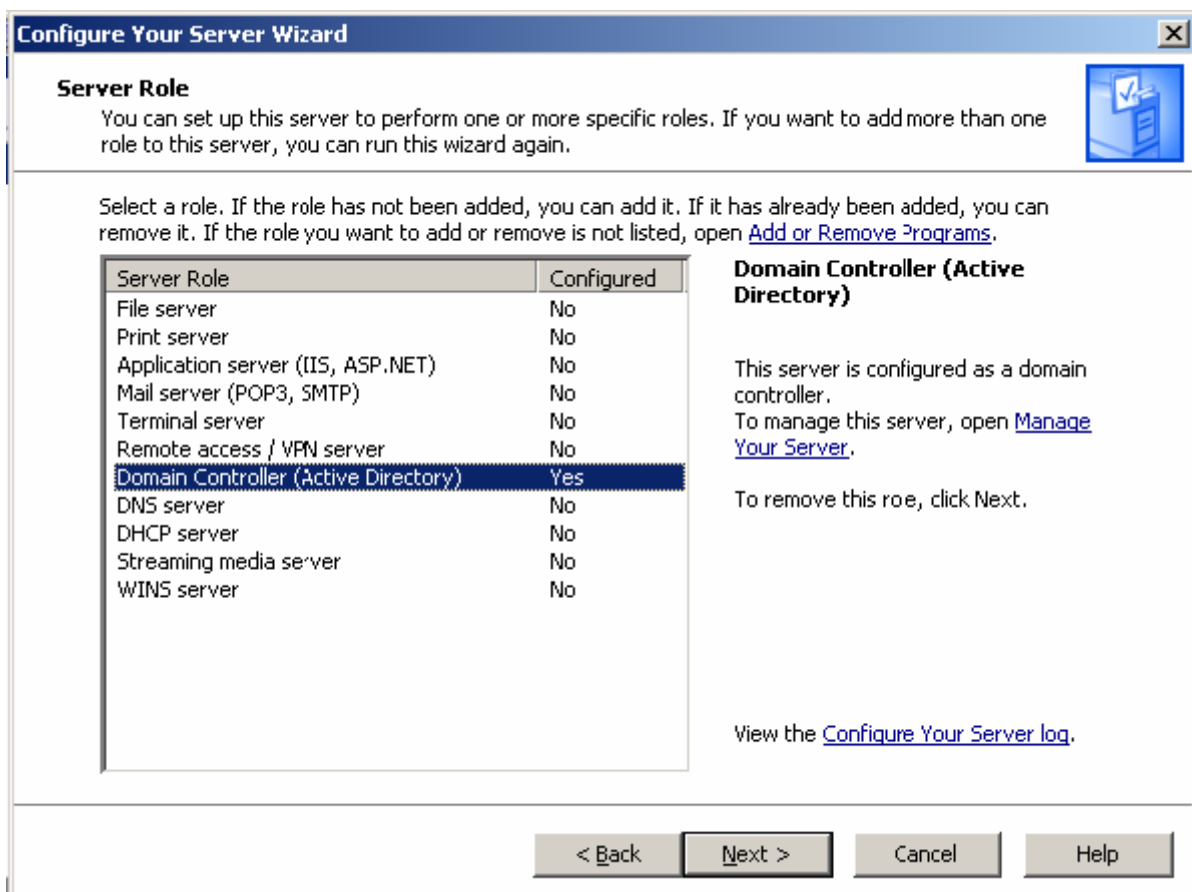
۱- روی دکمه Start کلیک کرده و روی آیکن Manage Your Server کلیک کرده تا پنجره ی زیر باز شود. سپس روی گزینه Add or remove a role کلیک کنید تا یک نقش جدید برای سرور اضافه یا حذف کنید. نکته: هر نقشی که برای سرور اضافه شده باشد در این پنجره نمایش داده میشود (اکتیو دایرکتوری نصب شده است).



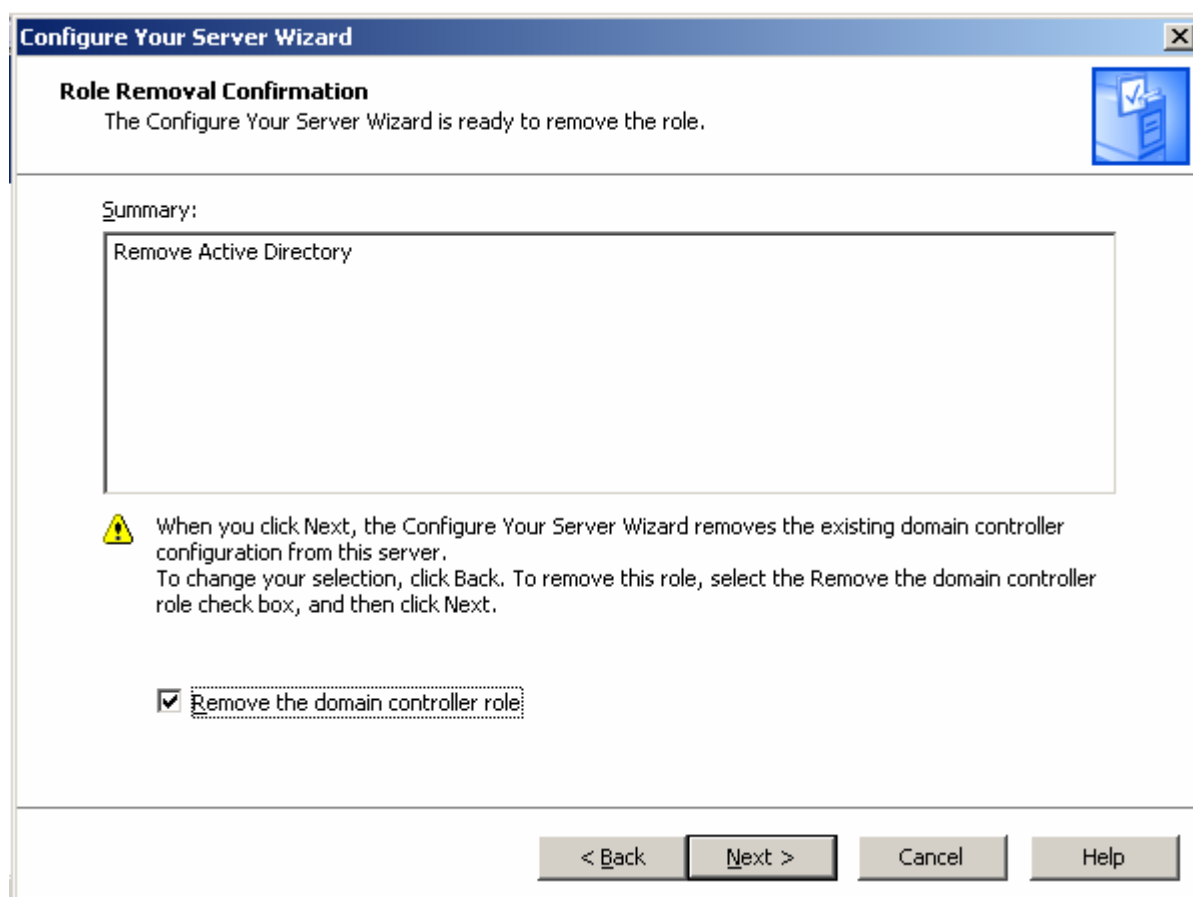
۲- در پنجره ای که ظاهر می شود به شما گفته میشود که قبل از اینکه مراحل را طی کنید باید اول موارد خواسته شده مانند نصب مودم ها و کارت های شبکه، متصل کردن کابل ها، گذاشتن CD ویندوز داخل CD-ROM و ... را انجام داده، سپس روی دکمه Next کلیک کنید.



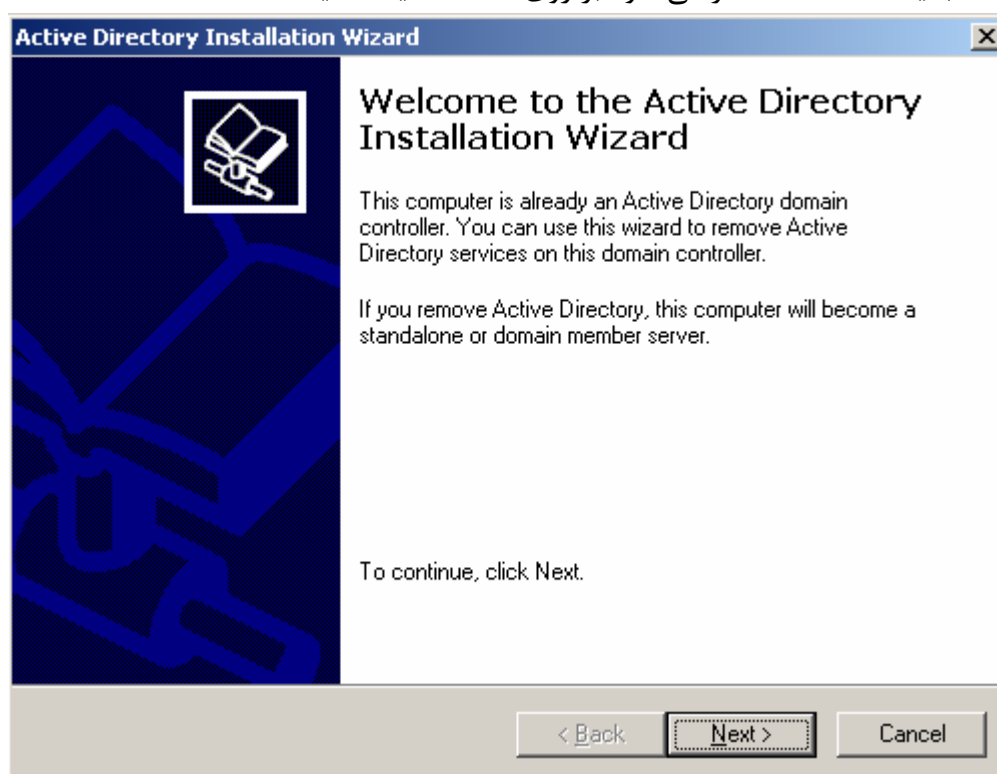
۳- Domain Controller (Active Directory) را انتخاب و Next را کلیک کنید.



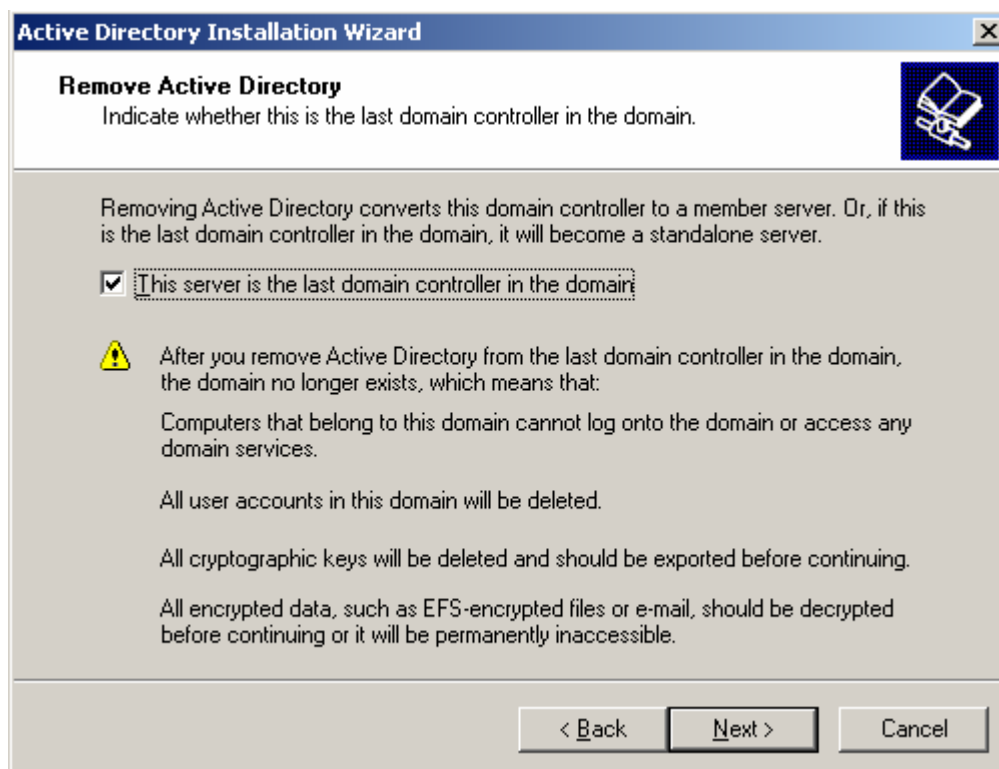
۴- در این پنجره تیک گزینه Remove the domain controller را انتخاب و بر روی Next کلیک کنید.



۵- صفحه ورود به نصب یا حذف AD ظاهر می شود بر روی Next کلیک کنید.

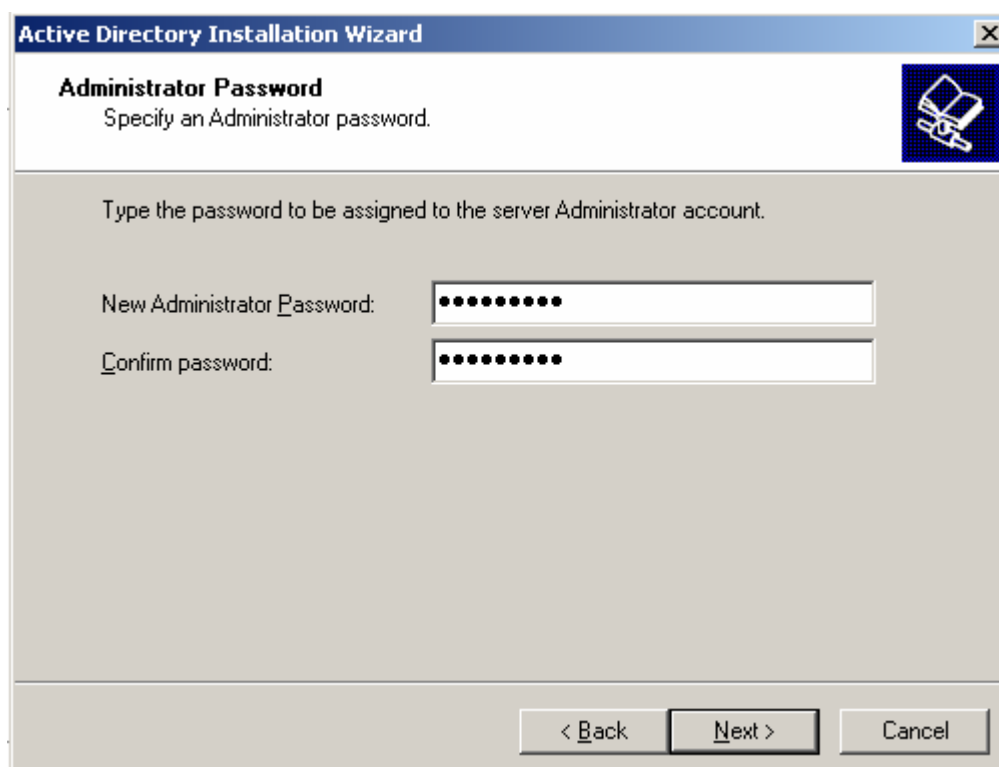


۶- این صفحه نشان می دهد که قرار دادن تیک باعث حذف کنترل کننده دامنه شده و سیستم بصورت Standalone تبدیل خواهد شد (کنترل کاربر و کامپیوتر در حد ضعیف خواهد بود). علاوه بر آن کلیه کامپیوترهای موجود در دامنه نمی توانند به دامنه دستیابی داشته باشند و کاربران ایجاد شده در سطح دامنه نیز حذف خواهند شد.



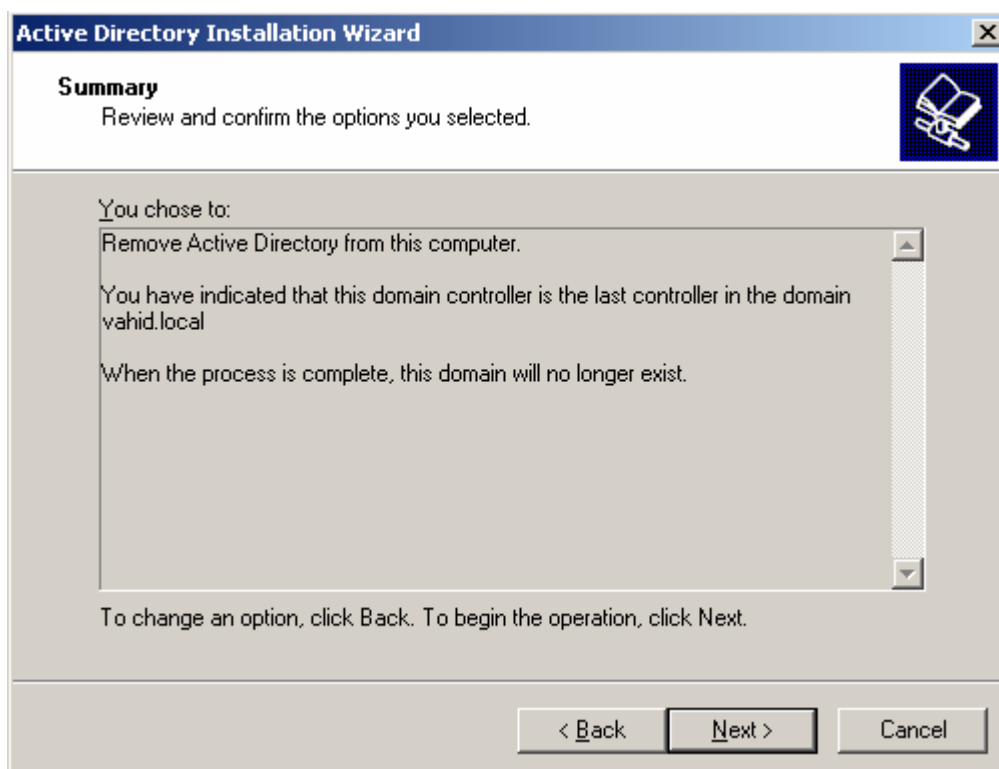
The screenshot shows the 'Active Directory Installation Wizard' window. The title bar reads 'Active Directory Installation Wizard'. The main heading is 'Remove Active Directory'. Below it, the instruction says 'Indicate whether this is the last domain controller in the domain.' There is a checkbox labeled 'This server is the last domain controller in the domain' which is checked. To the right of the checkbox is a warning icon. Below the checkbox, there is a warning message: 'After you remove Active Directory from the last domain controller in the domain, the domain no longer exists, which means that: Computers that belong to this domain cannot log onto the domain or access any domain services. All user accounts in this domain will be deleted. All cryptographic keys will be deleted and should be exported before continuing. All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

۷- در این قسمت باید رمز Administrator دو بار داده شود. به این علت که ممکن است زیر مدیرها بخواهند دامنه را حذف کنند این پنجره نشان می دهد که فقط مدیر اصلی با وارد کردن رمز خود می تواند دامنه را حذف کند.

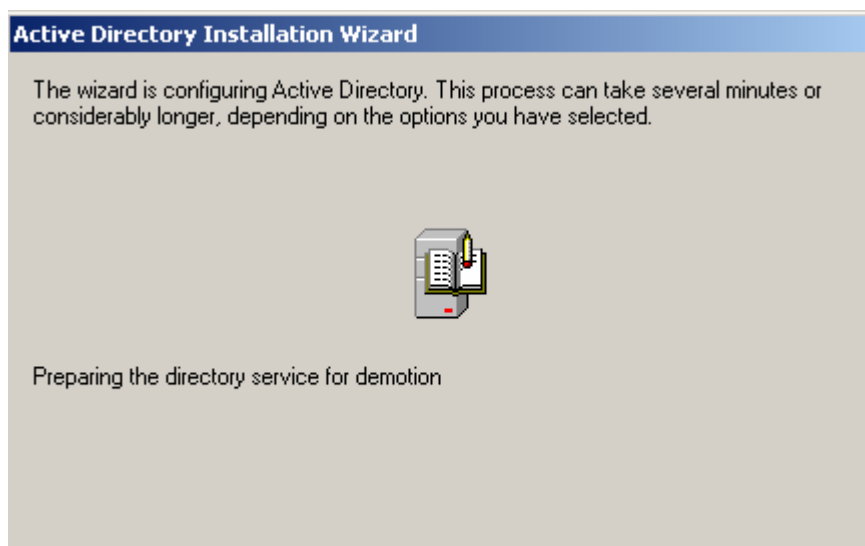


The screenshot shows the 'Active Directory Installation Wizard' window. The title bar reads 'Active Directory Installation Wizard'. The main heading is 'Administrator Password'. Below it, the instruction says 'Specify an Administrator password.' There is a text box for 'New Administrator Password:' and another text box for 'Confirm password:'. Both text boxes contain a series of dots. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

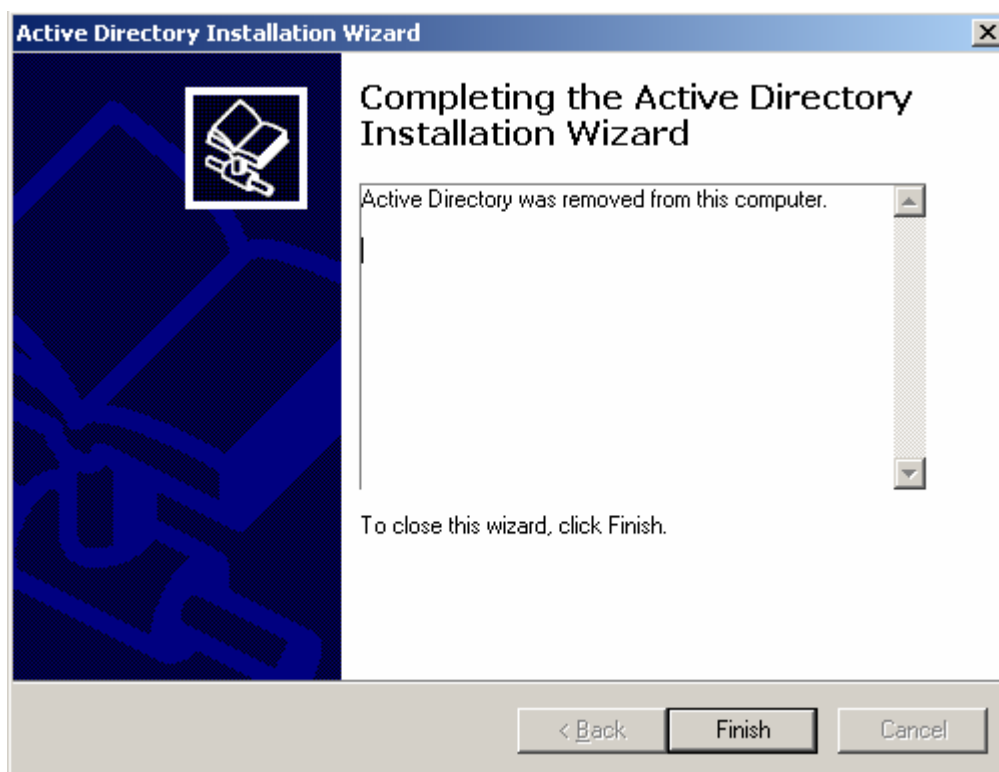
۸- در این قسمت خلاصه توضیحاتی که قرار است با این انتخاب شما اتفاق بیافتد نمایش داده می شود. اگر بر روی Next کلیک کنید AD با کل دامنه ای که تعریف شده است از سرور حذف می شود.



۹- چند دقیقه باید منتظر بمانید تا اکتیو دایرکتوری حذف شود.



۱۰- این پنجره نشان می دهد که اکتیو دایرکتوری به طور کامل از روی سرور حذف شده است.



۱۱- بعد از پایان یافتن حذف اکتیو دایرکتوری این پنجره نشان داده می شود که از شما میخواهد برای بهتر اعمال شدن تنظیمات، سیستم را رستارت نمایید.



۱-۳- بررسی تنظیم Domain بر روی کلاینتها:

پس از آنکه AD نصب شد، هدف اصلی آن مدیریت کامپیوترها و کاربران می باشد. اگر توجه داشته باشیم کاربران موجود در سطح سیستم نمی توانند از طریق کامپیوتر که ۲۰۰۳ سرور بر روی آن نصب شده است وارد دامنه شوند. سوال این گونه مطرح می شود که این کاربران در سطح دامنه به چه نحوی وارد دامنه شوند؟ برای اینکار باید کامپیوترهای با نام کلاینت در نظر گرفته و برای دستیابی به دامنه توسط کاربرها، این کامپیوترها را به دامنه Join کنیم که برای این کار مراحل زیر را طی می کنیم:

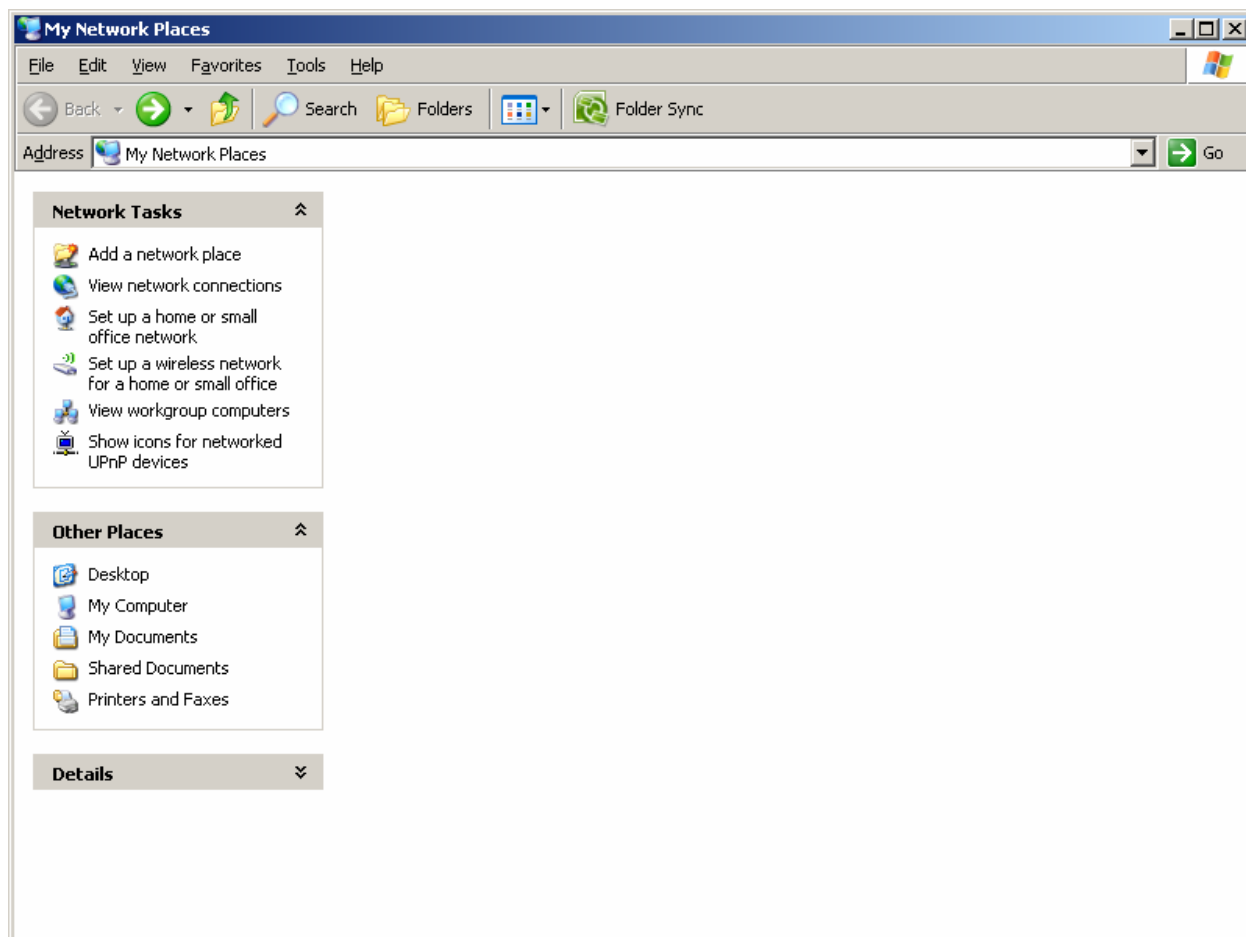
۱-۱-۳- تنظیم آدرس IP کلاینت ها با سرور:

برای تنظیم کردن آدرس IP این مراحل را انجام دهید:

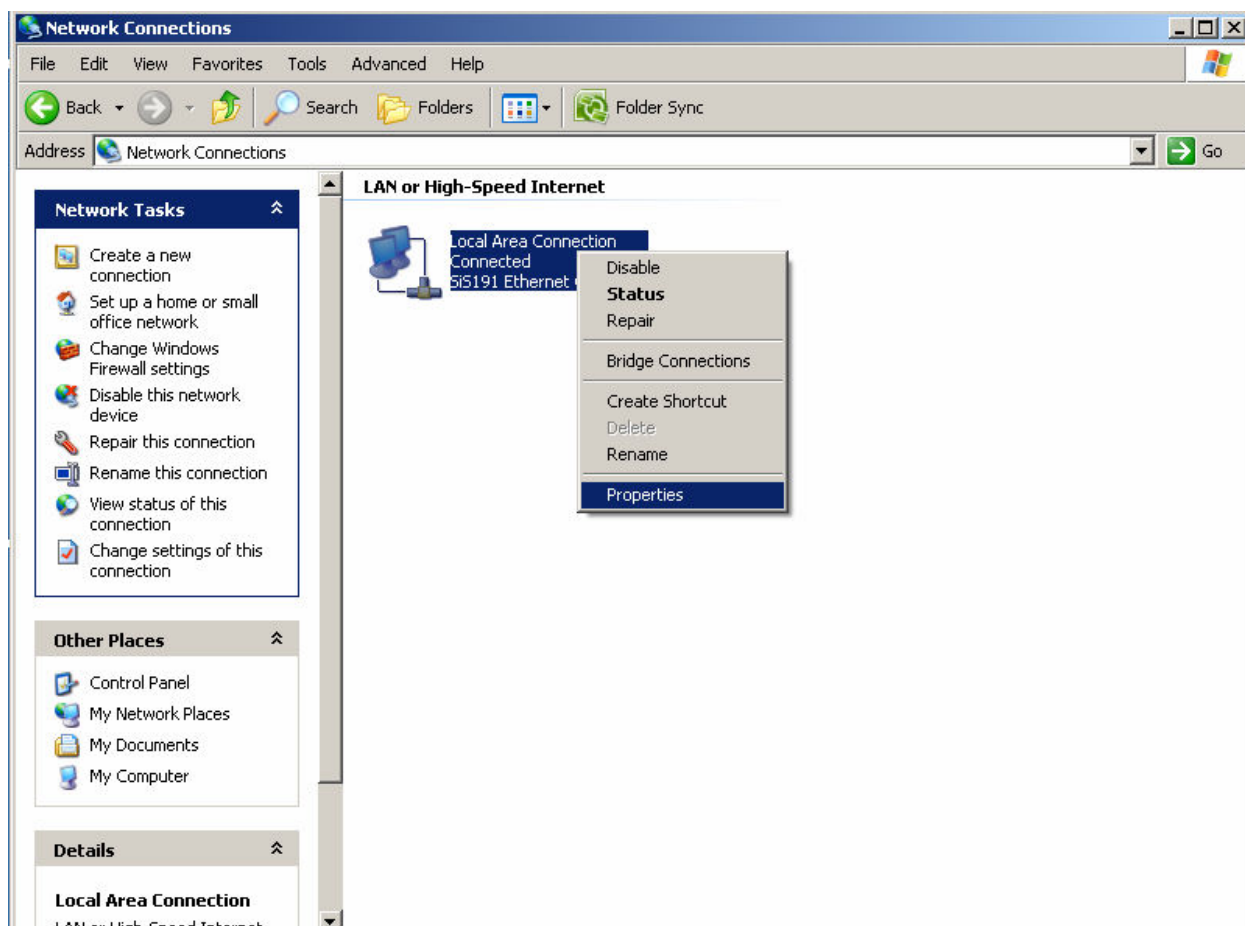
Start > My Network places

(در اینجا سیستم عامل کلاینت ویندوز XP و کارت شبکه کلاینت نیز نصب می باشد).

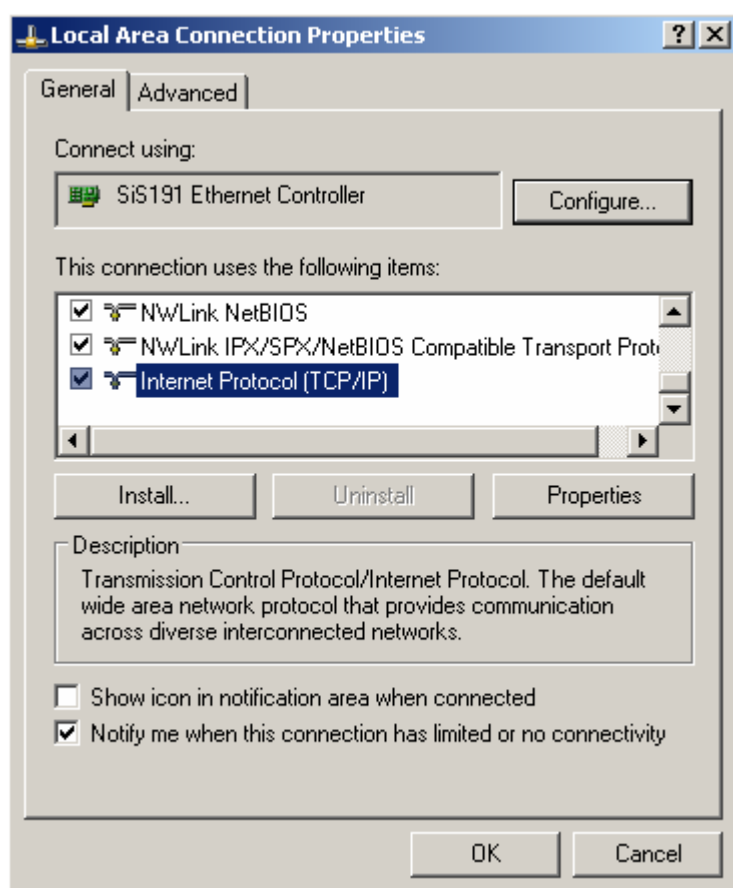
در پنجره ظاهر شده روی View network connections کلیک کنید.



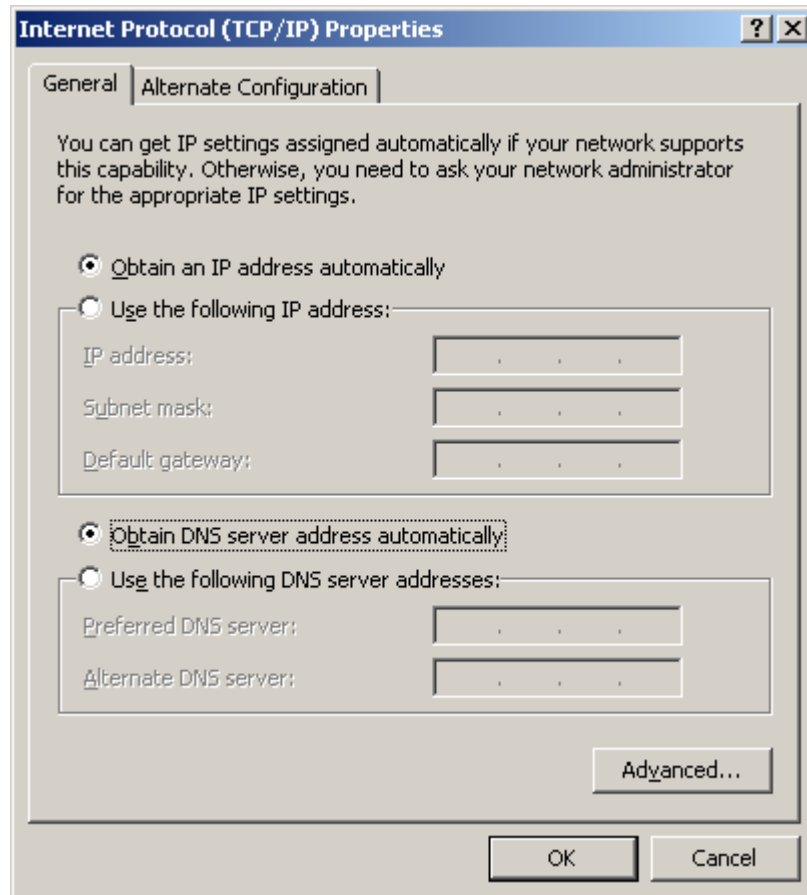
۲- در این پنجره بر روی Local Area Connection کلیک راست کرده و Properties را انتخاب کنید.



۳- تیک internet Protocol(TCP/IP) را گذاشته بر روی Properties کلیک کنید.



۴- این پنجره نمایش داده می شود.



در این پنجره برای دادن آدرس IP قسمت Use the following IP address را تیک می زنیم تا قسمت IP فعال شود.

ADDRESS IP:

در این قسمت آدرس IP را خواهیم داد. چون می خواهیم با سرور ارتباط داشته باشیم و IP سرور را ۱۹۲,۱۶۸,۰,۱ داده ایم و چون کلاس IP سرور از نوع کلاس آیی C می باشد فقط می توانیم قسمت آخر IP را تغییر دهیم.

مثلاً می توانیم IP اولین کلاینت را بدهیم 192.168.0.2

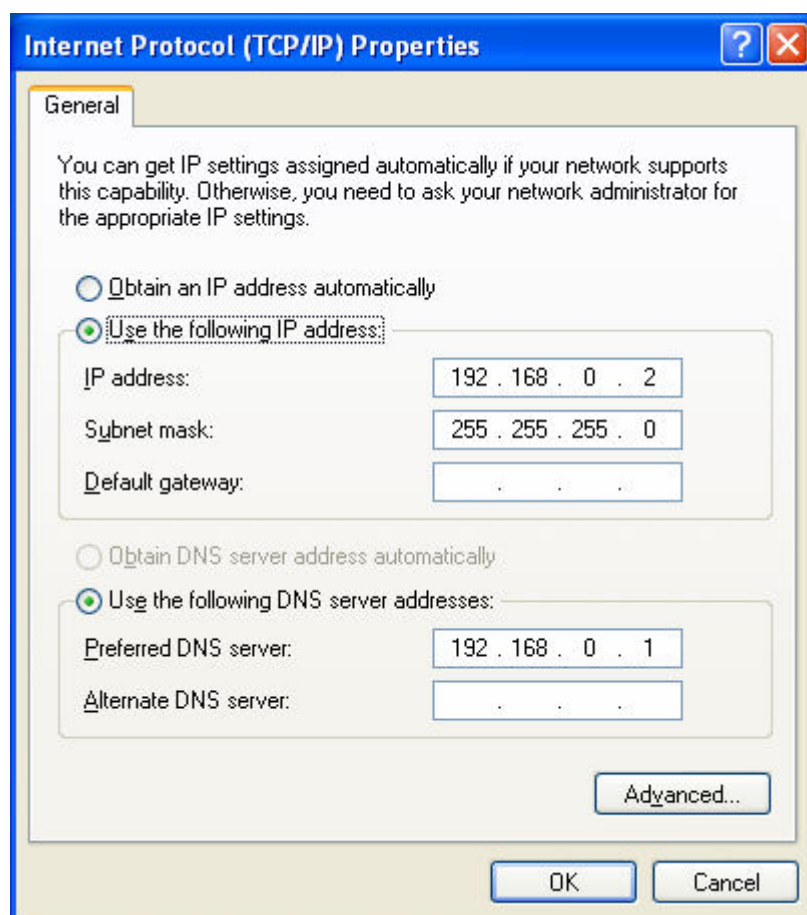
SUBNET MASK: به معنای پوشش زیر شبکه در کلاس مورد نظر به صورت زیر است:

در کلاس C ۲۵۵,۲۵۵,۲۵۵,۰

DEFAULT GETWAY: همانطور که قبلاً گفته شد اگر در شبکه راه اندازی شده نیازی به وصل شدن به اینترنت نباشد لازم نیست که این گزینه تنظیم شود ولی اگر بخواهیم به اینترنت وصل شویم یکی از آدرس IP هایی را که می خواهیم به عنوان دروازه از آن استفاده کنیم را انتخاب و در تمام کامپیوتر ها وارد می کنیم.

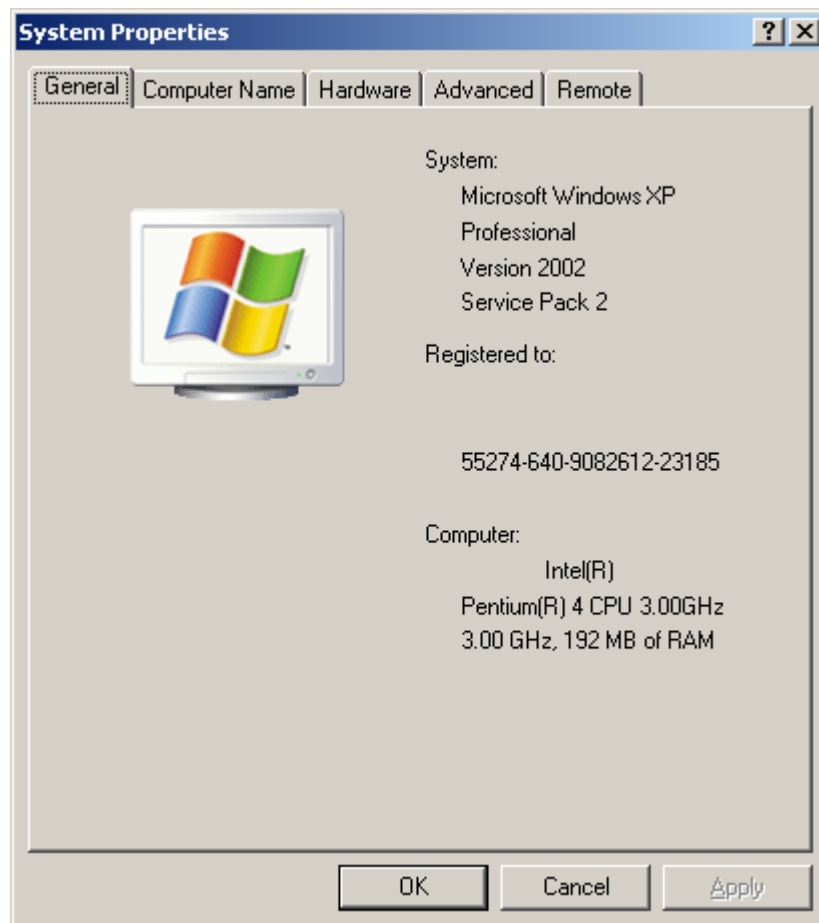
و در قسمت پایین Use the following DNS server address را انتخاب و DNS را به صورت دستی وارد می کنیم. در این قسمت اگر IP سرور را وارد کنیم بهتر عمل خواهد کرد. (۱۹۲,۱۶۸,۰,۱)

بعد از انجام این کارها IP و DNS سرور تنظیم شده است بر روی OK کلیک می کنیم

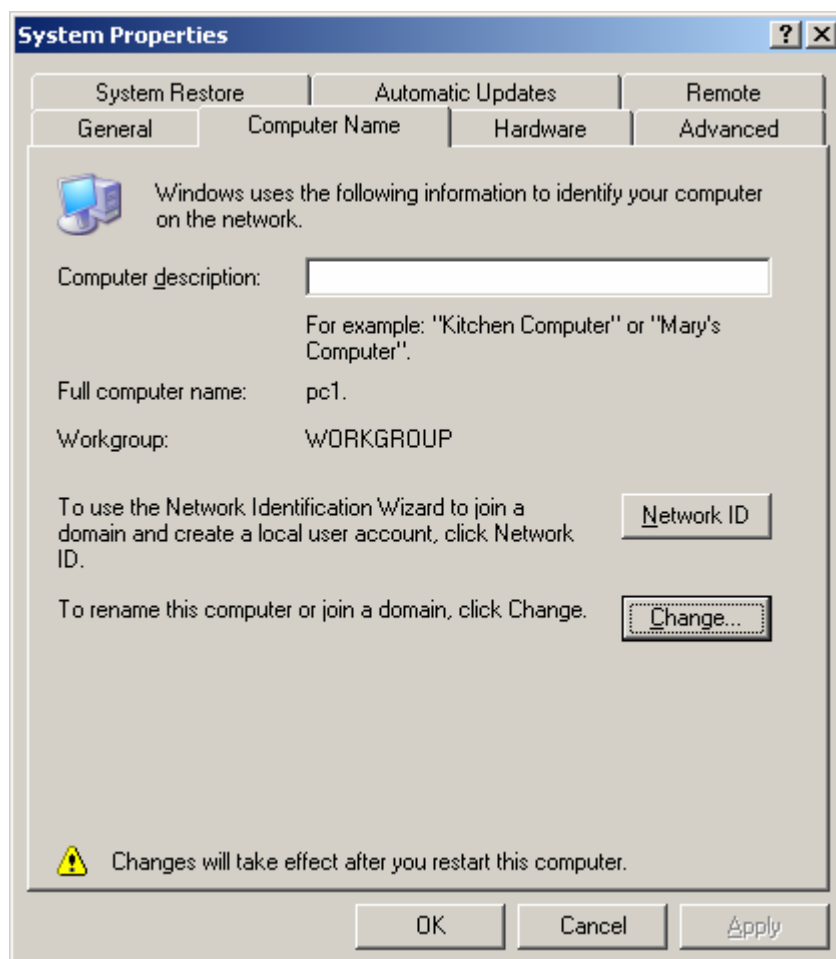


۲-۱-۳ Join کردن کلاینت به سرور:

بعد از تنظیم کردن آدرس IP کلاینت با سرور بر روی My Computer کلیک راست کرده و properties را انتخاب می کنیم.



در پنجره باز شده بر روی Computer Name و سپس بر روی Change کلیک می کنیم.



این پنجره نمایش داده میشود.

Computer Name Changes ? X

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name:
pc1

Full computer name:
pc1.

More...

Member of

☐ Domain:
[Empty field]

☒ Workgroup:
WORKGROUP

OK Cancel

در این پنجره بخش Domain را فعال کرده و Domain سرور را وارد می کنیم.
نکته: در اینجا باید دامنه را بدون پسوند local وارد کنید.

Computer Name Changes ? X

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name:
pc1

Full computer name:
pc1.

More...

Member of

☒ Domain:
vahid

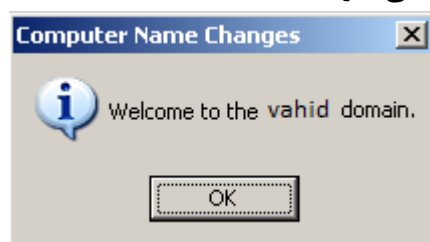
☐ Workgroup:
WORKGROUP

OK Cancel

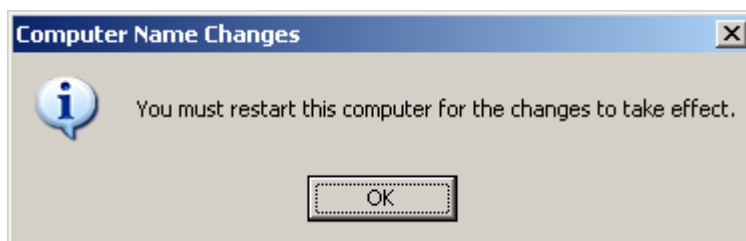
در این پنجره باید نام کاربری و رمز ورود به سرور را وارد کنید. چون شما هنوز کاربری را ایجاد نکرده اید می توانید برای Join کردن نام کاربری و رمز مدیر را وارد کنید.
(نام کاربری: administrator)



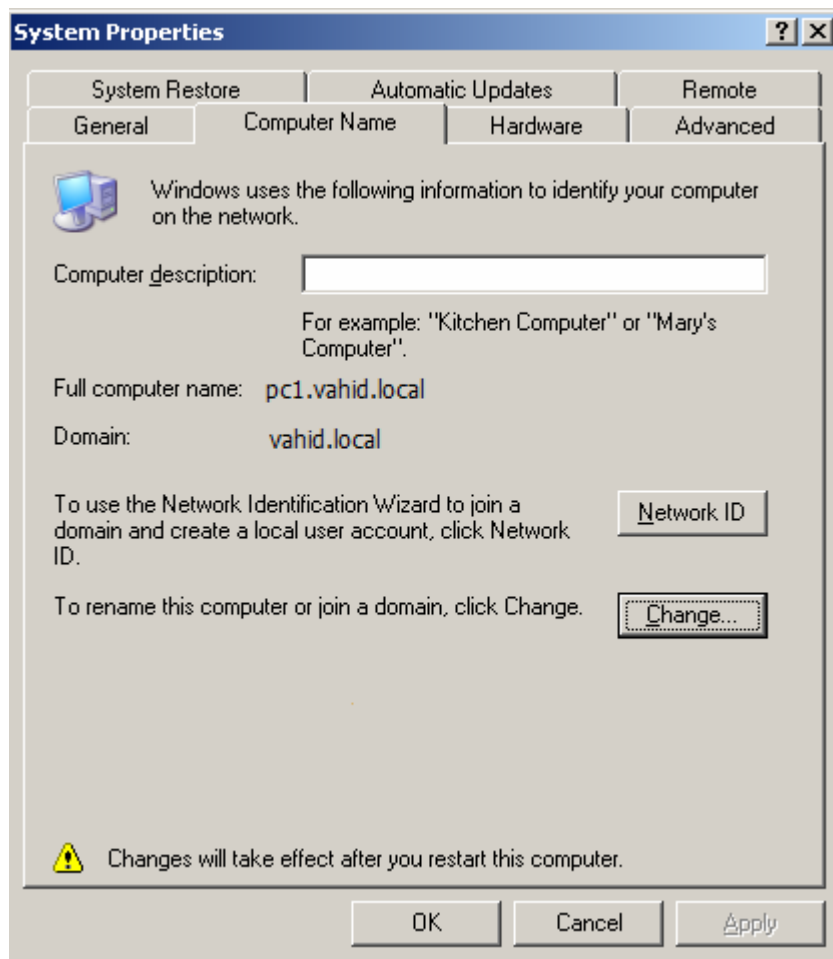
پیغام خوش آمد گویی به دامنه نمایش داده می شود. OK کنید.



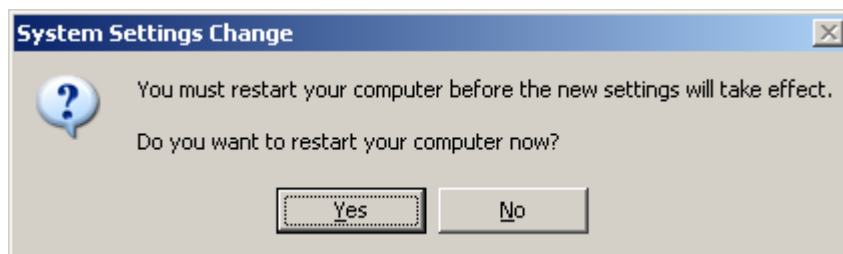
در این پیغام به شما گفته می شود که برای اعمال تغییرات باید کامپیوتر را رستارت نمایید. OK کنید.



OK کنید.



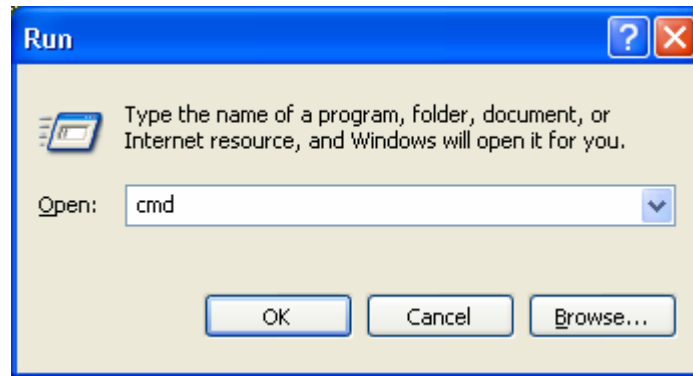
در این پنجره از شما پرسیده می شود که آیا می خواهید برای اعمال تغییرات، کامپیوتر را ریستارت نمایید؟ بر روی Yes کلیک کنید تا کامپیوتر ریستارت شود.



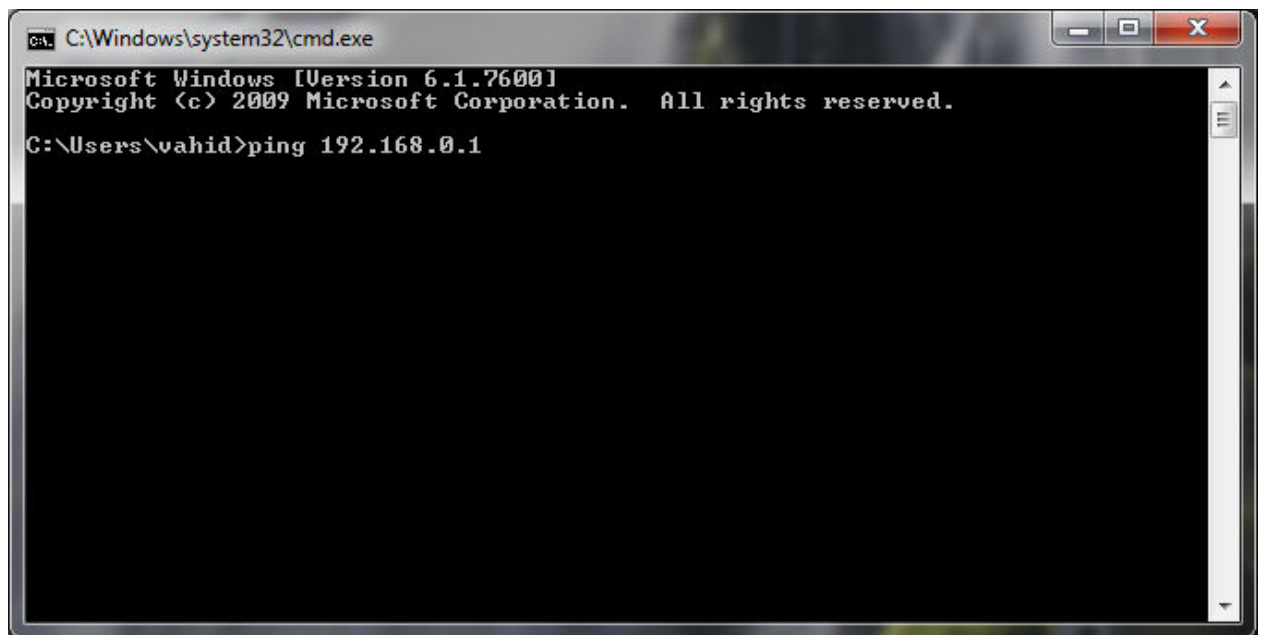
۳-۱-۳- تست کردن ارتباط بین سرور و کلاینت (Ping):

برای اینکه بدانید بین کامپیوتر Server و User ارتباط وجود دارد و همدیگر را می شناسند دستور Ping را برای هر دو سیستم اجرا کنید.

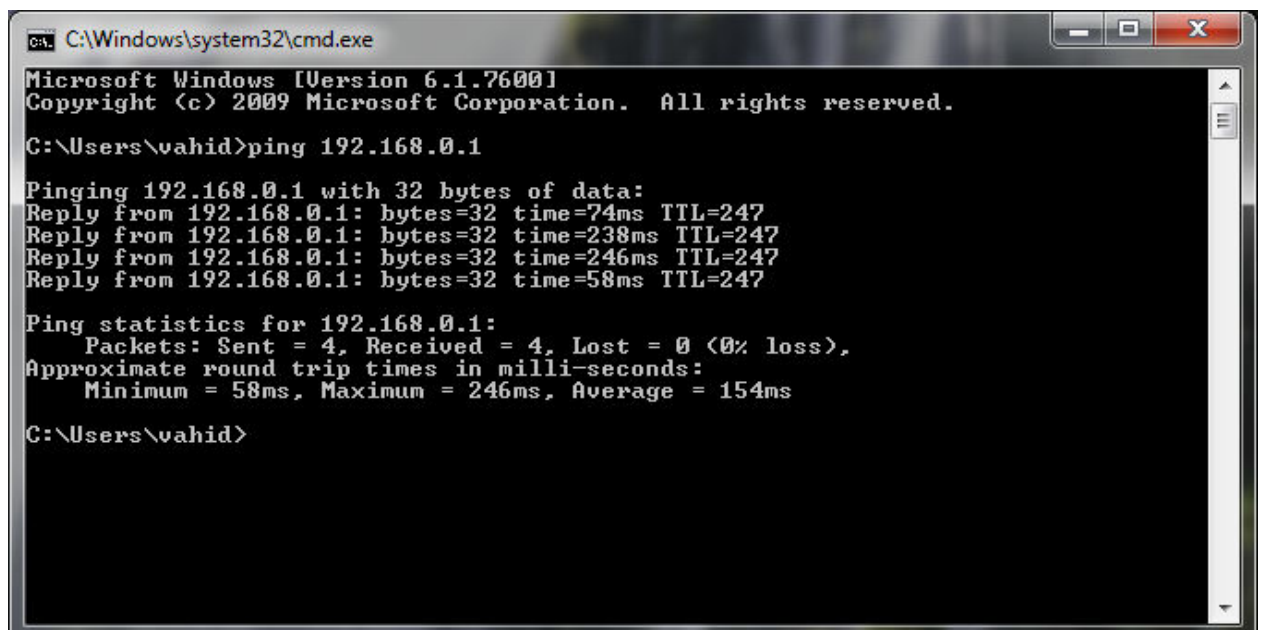
برای این کار در منوی Start روی گزینه Run کلیک کرده و دستور CMD را تایپ کنید.



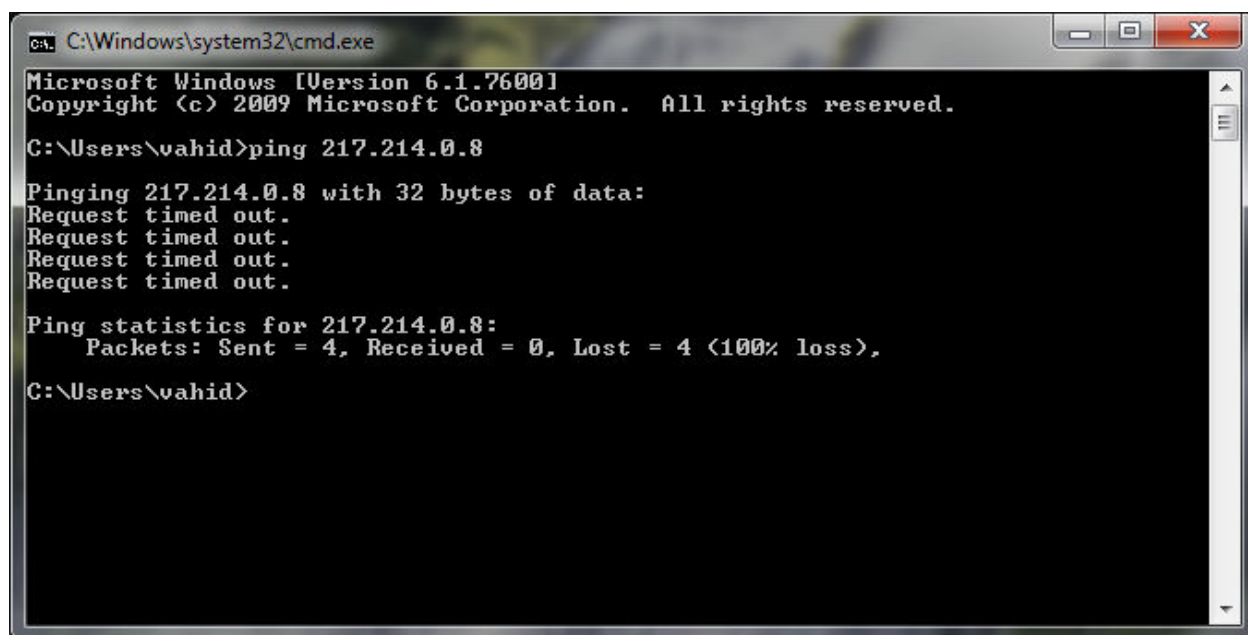
در این پنجره دستور Ping را همراه آدرس IP سیستمی را که میخواهید با آن ارتباط برقرار کنید را تایپ کرده و Enter را بزنید. (برای مثال در یکی از Userها دستور Ping و IP سرور را تایپ کرده و بر روی OK کلیک کنید)



اگر در پنجره جدید باز شده پیغام های Reply از IP سرور نمایش داده شد، ارتباط وجود دارد. (مانند شکل زیر)



اگر پیغام Request timed out نشان داده شد ارتباط وجود ندارد. (مانند شکل زیر)



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\vahid>ping 217.214.0.8

Pinging 217.214.0.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

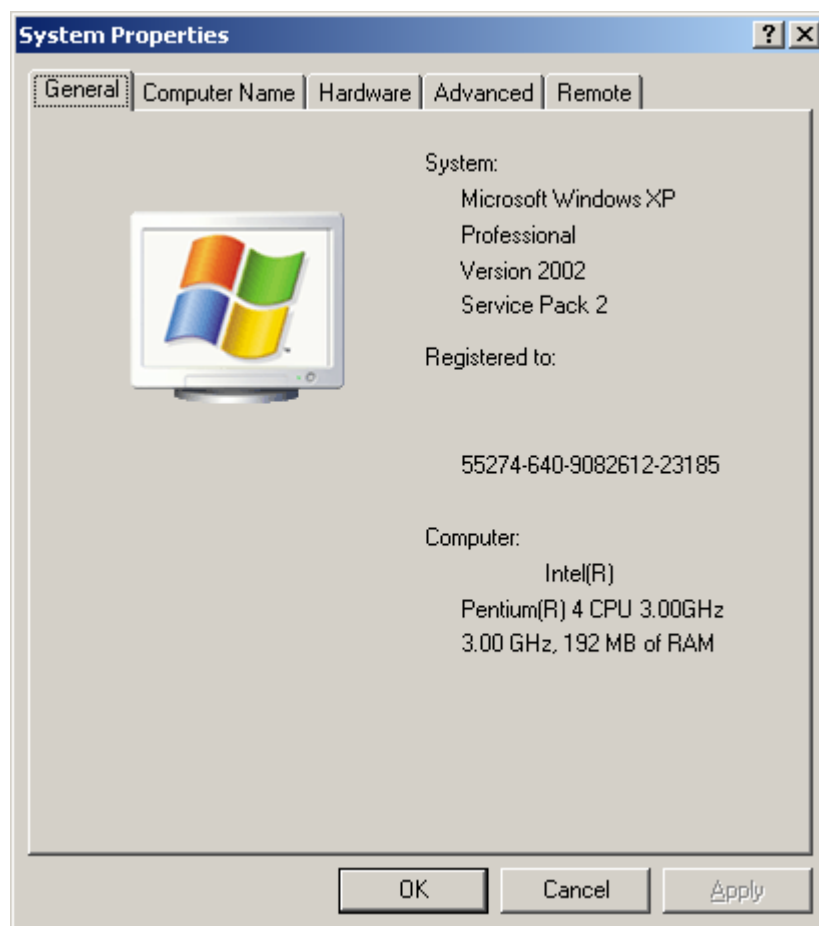
Ping statistics for 217.214.0.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\vahid>
```

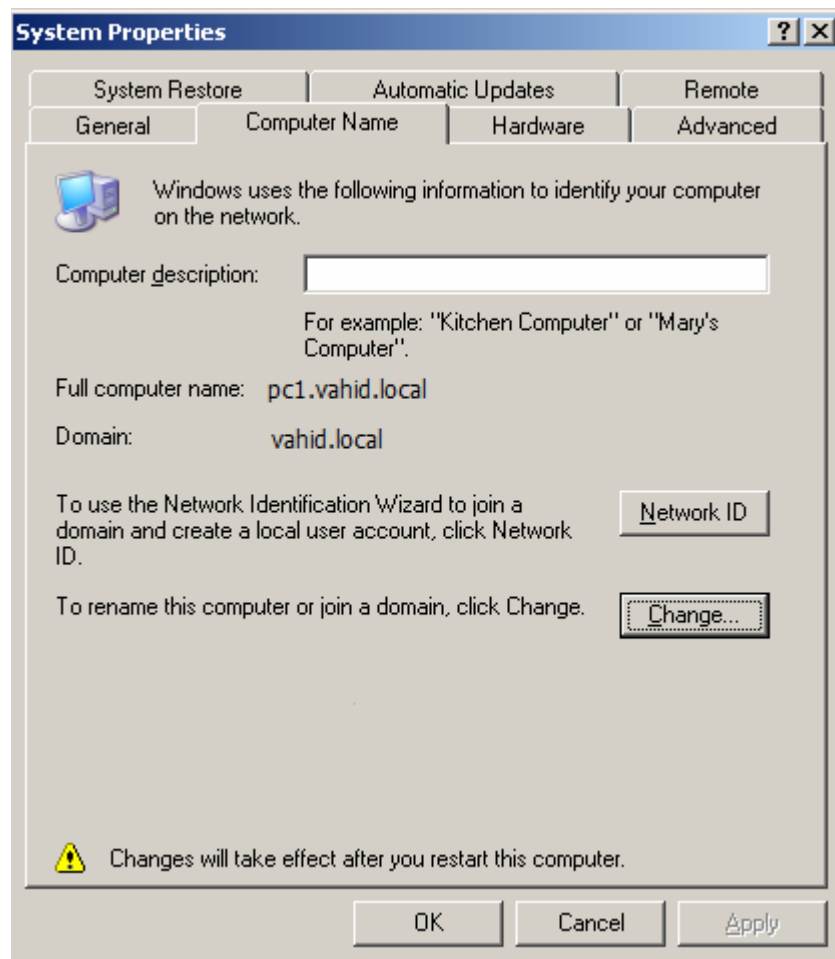
۴-۱-۳- بررسی خارج کردن کلاینت از Domain:

اگر بخواهید کامپیوتری را که عضو دامنه است را از دامنه خارج کنید، این مراحل را انجام دهید:

بر روی My Computer کلیک راست و properties را انتخاب کنید.



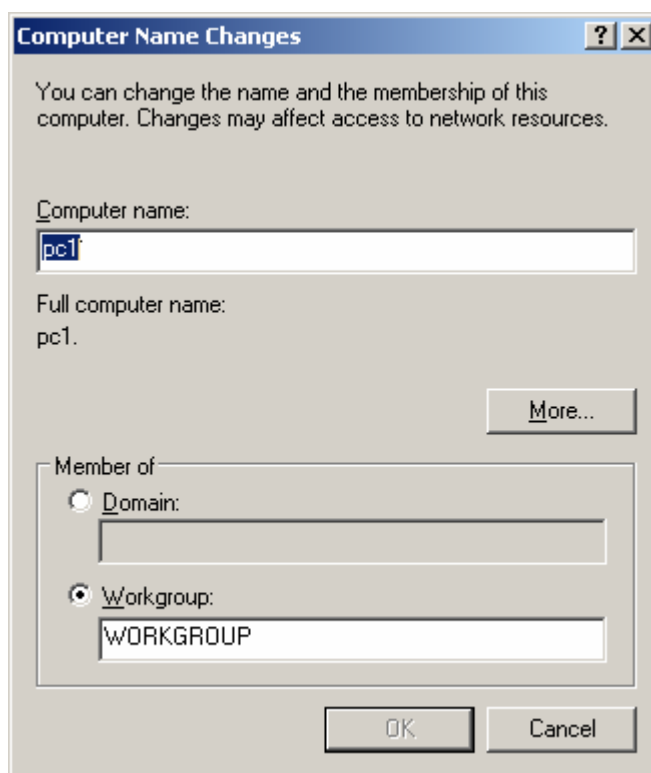
در پنجره باز شده بر روی Computer Name و سپس بر روی Change کلیک کنید.



این پنجره نمایش داده میشود.



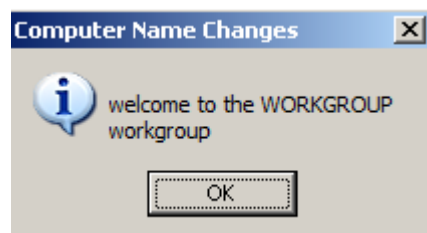
در این پنجره بخش Workgroup را فعال کرده و اگر می خواهید عضوی از یک محیط کاری باشید نام آن را در قسمت Work group وارد کرده و OK کنید. مثلاً در اینجا نام محیط کاری همان WORKGROUP است.



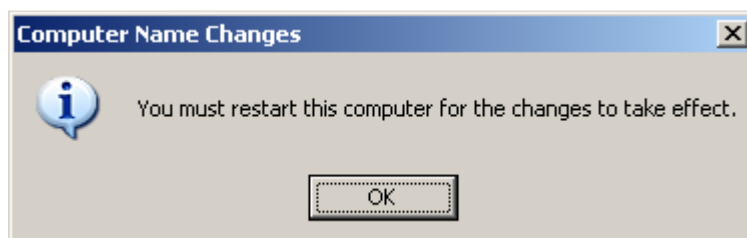
در این پنجره باید نام کاربری و رمز دامنه ای که از آن استفاده می کردید را وارد کنید تا از آن دامنه خارج شود.



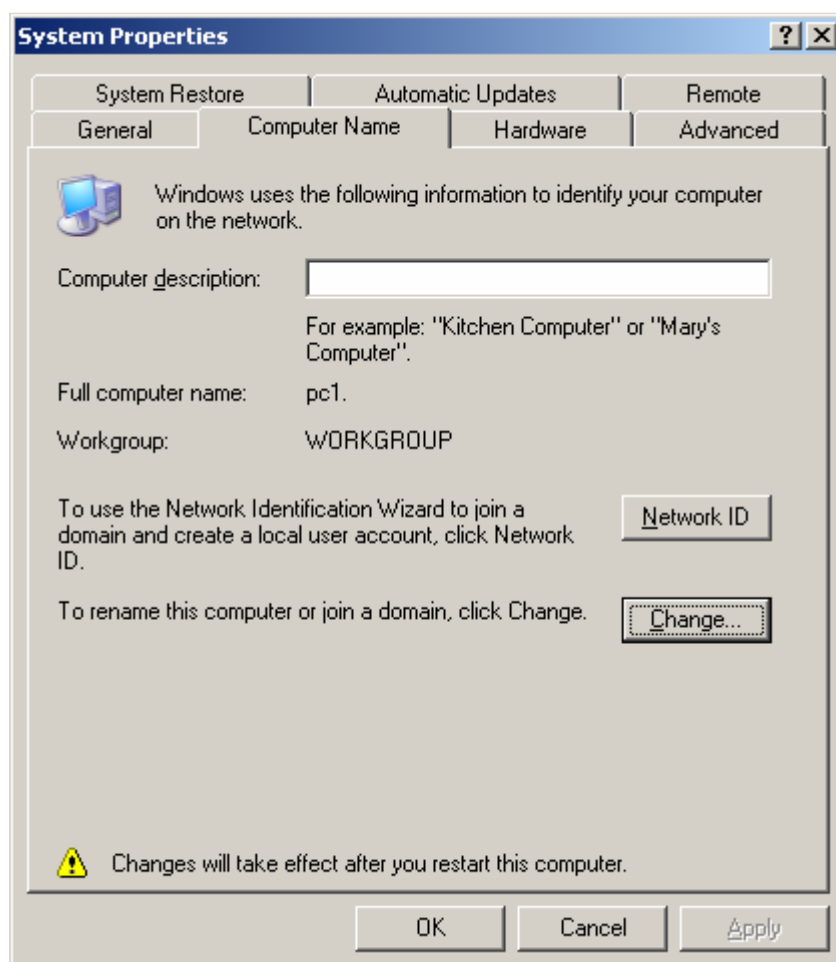
پیغام خوش آمد گویی به Work group نمایش داده می شود. OK کنید.



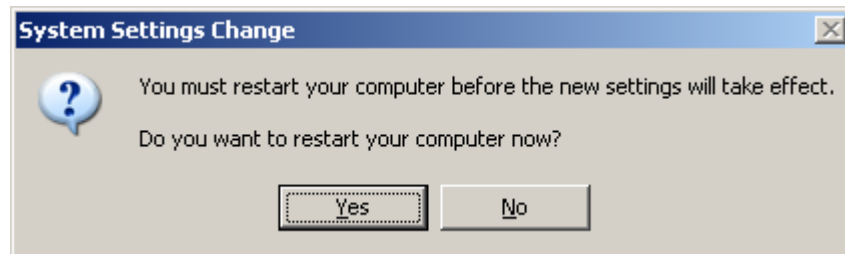
در این پیغام به شما گفته می شود که برای اعمال تغییرات باید کامپیوتر را رستارت نمایید. OK کنید.



OK کنید.



در این پنجره از شما می پرسد که آیا می خواهید برای اعمال تغییرات کامپیوتر را رستارت نمایید؟ بر روی Yes کلیک کنید تا کامپیوتر رستارت شود.

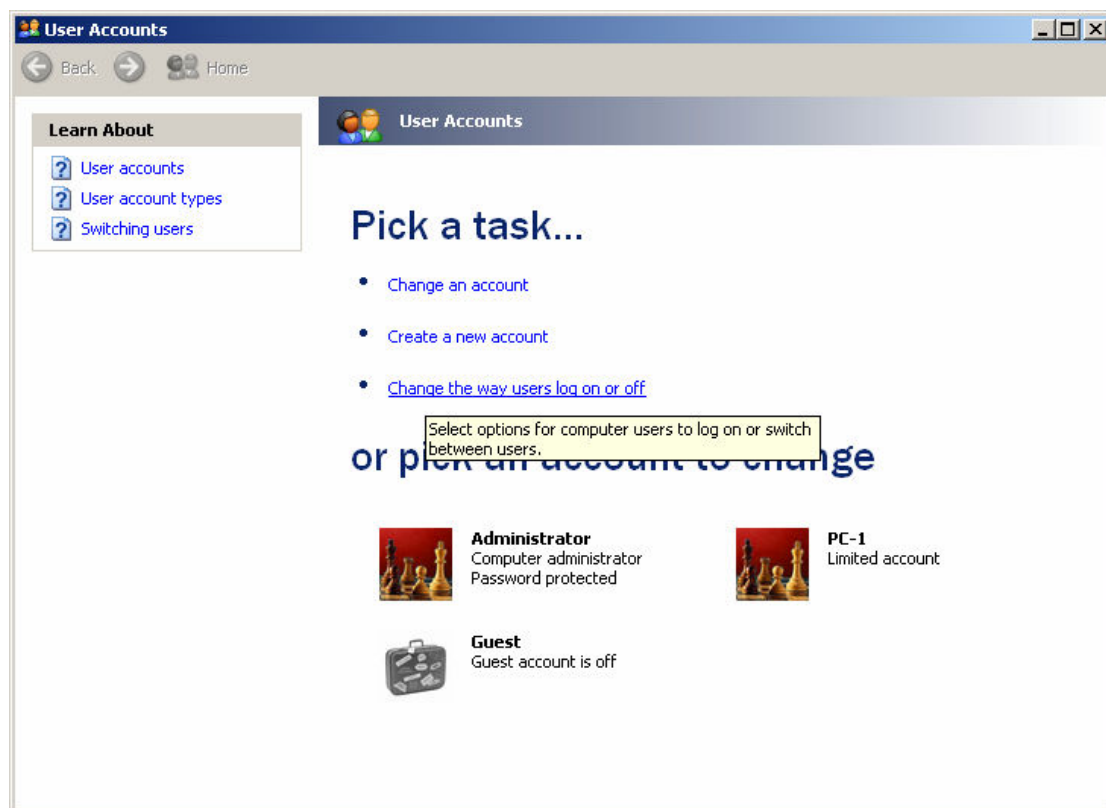


اگر می خواهید صفحه ورود به ویندوز نیز مانند قبل شود این مراحل را انجام دهید:

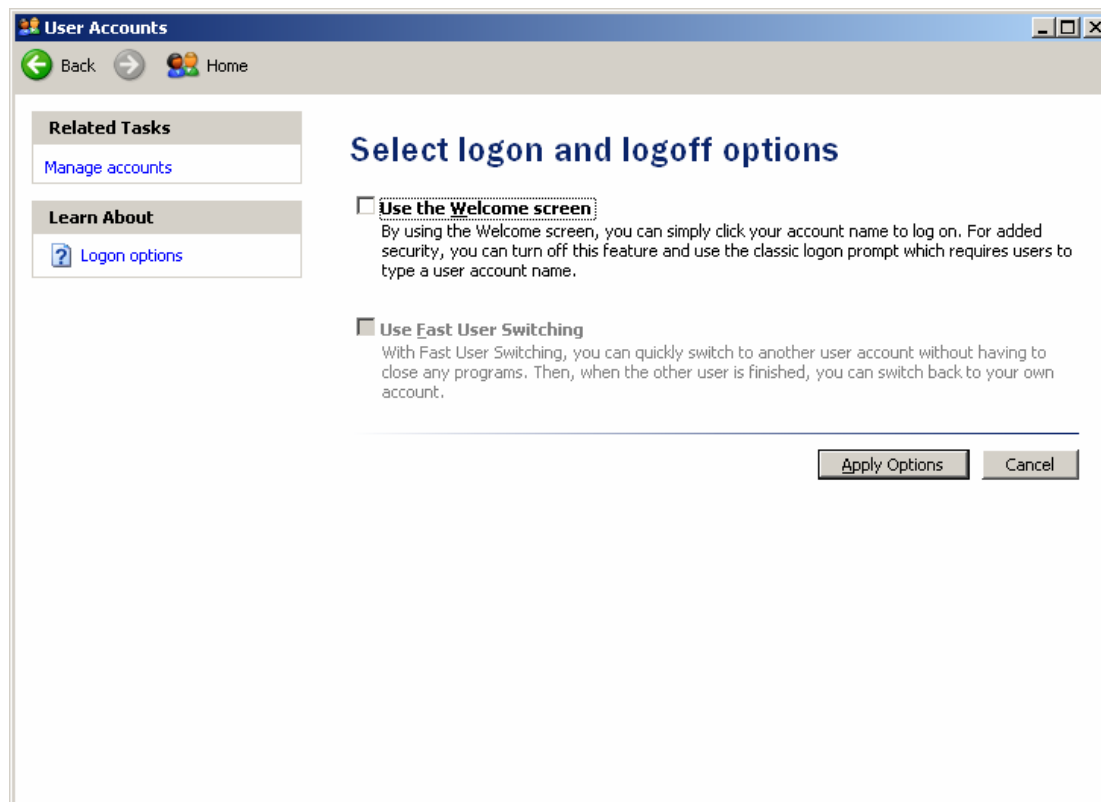
به مسیر زیر بروید:

Start > Control Panel > User Accounts

بر روی **Change the way users log on or off** کلیک کنید.



در پنجره ظاهر شده گزینه **Use the Welcome screen** را انتخاب و بر روی **Apply options** کلیک کنید.



۲-۳- بررسی DHCP در ۲۰۰۳ سرور:

برخی مواقع ممکن است وارد کردن آدرس IP بصورت دستی مشکلاتی را به وجود آورد برای مثال ممکن است IP تکراری برای کلاینت ها داده شود که در این حالت کلاینت ها به سرور Join نخواهد شد. برای رفع این مشکل می توانیم در ۲۰۰۳ از تنظیم اتوماتیک آدرس های IP یا DHCP استفاده کنیم.

DHCP (Dynamic Host Configuration Protocol) یکی از سرویسهای بسیار مهم و پرکاربرد سیستم عاملهای مایکروسافت است.

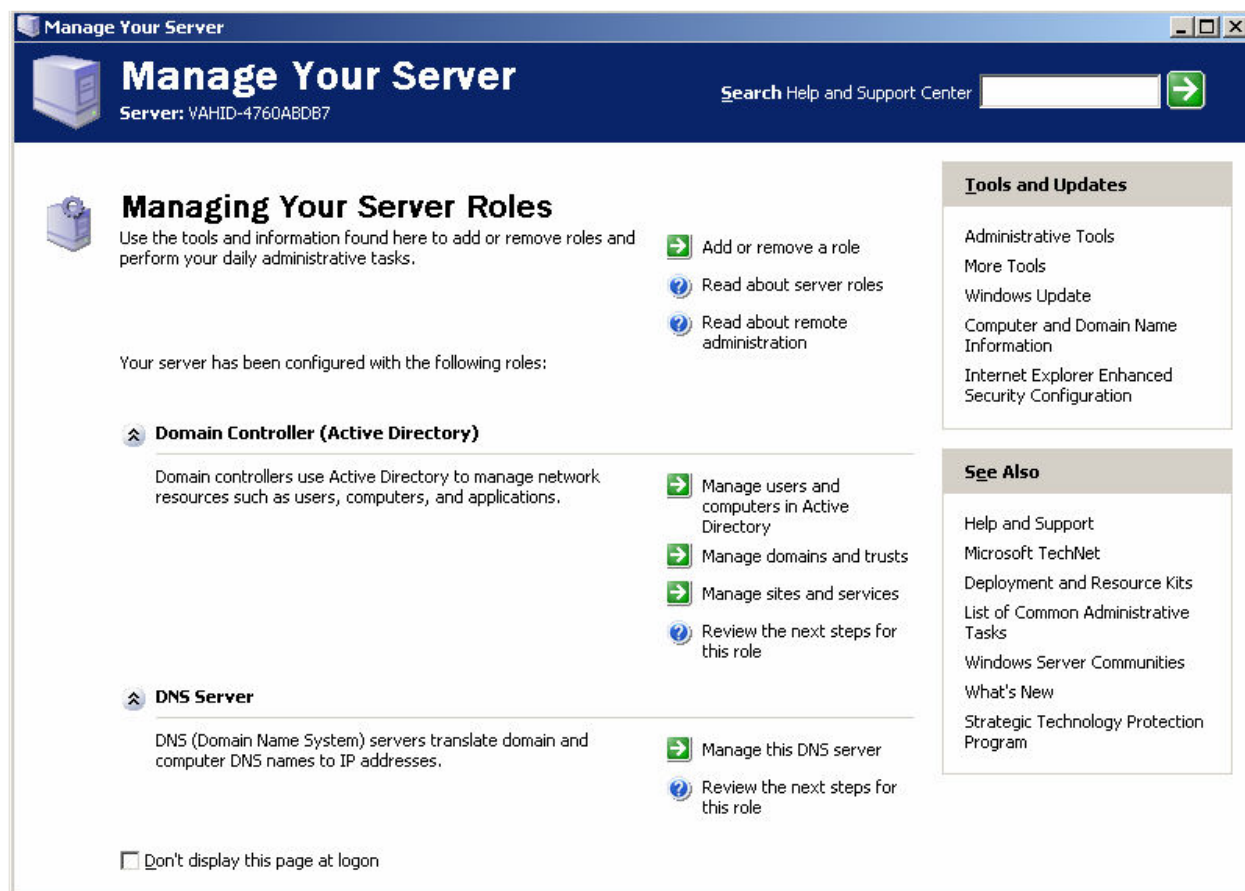
این سرویس امکان تعریف آدرس IP و دیگر تنظیمات مورد نیاز کامپیوتر های سرویس گیرنده (Client) به طور اتوماتیک را فراهم می آورد. میدانیم که در صورت ازدیاد تعداد کامپیوتر های سرویس گیرنده در شبکه های بزرگ مدیریت این شبکه ها بسیار سخت و زمان بر میباشد. همچنین تعریف و مدیریت تنظیماتی آدرسی این کامپیوترها نیز بطبع سخت خواهد شد.

فرض بر این است که شبکه شما دارای ۱۰۰ کامپیوتر سرویس گیرنده و ۳ کامپیوتر سرویس دهنده میباشد. یکی از این کامپیوترها قرار است نقش DHCP Server را در شبکه ایفا کند. به صورت پیش فرض هیچ Scope یا همان محدوده IP وجود ندارد.

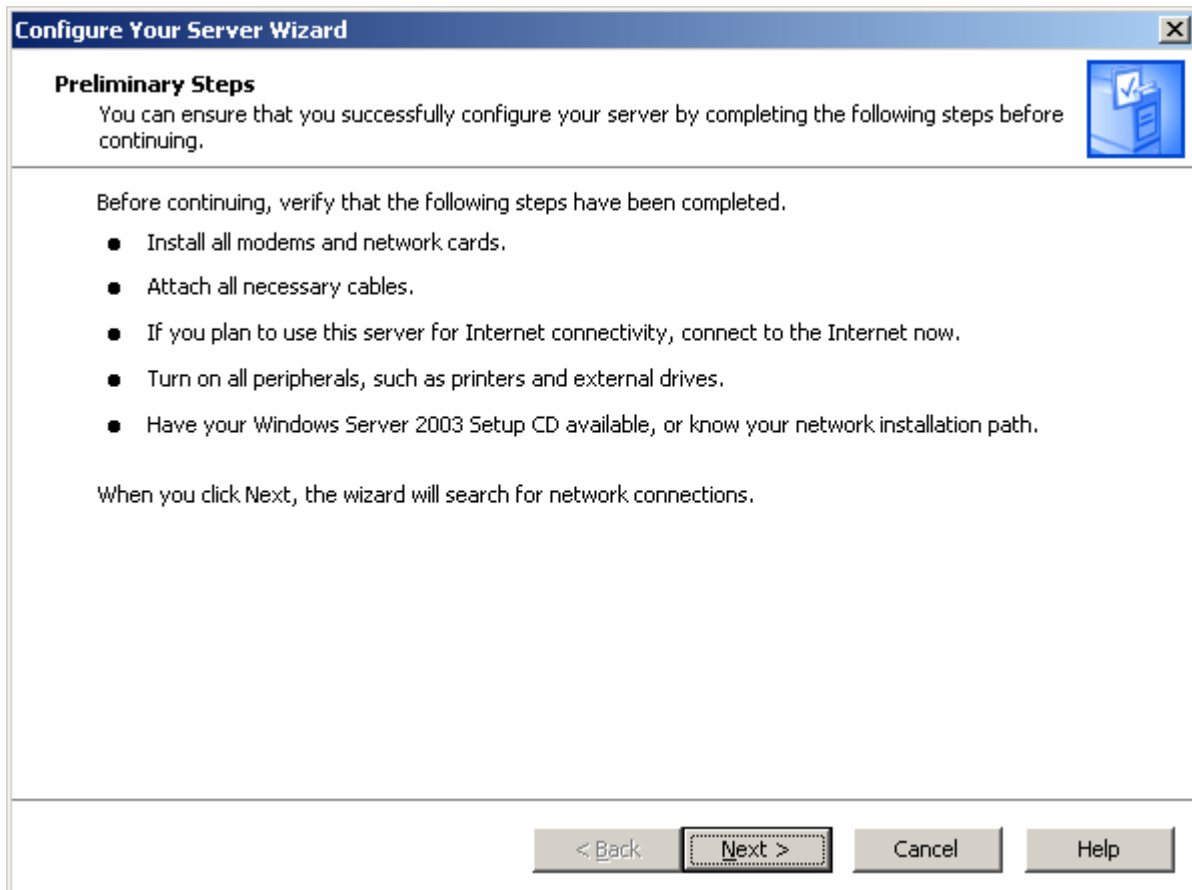
۱-۲-۳- تنظیم DHCP بر روی سرور برای پخش آدرس IP:

برای نصب DHCP Server بر روی سرور این مراحل را انجام دهید:

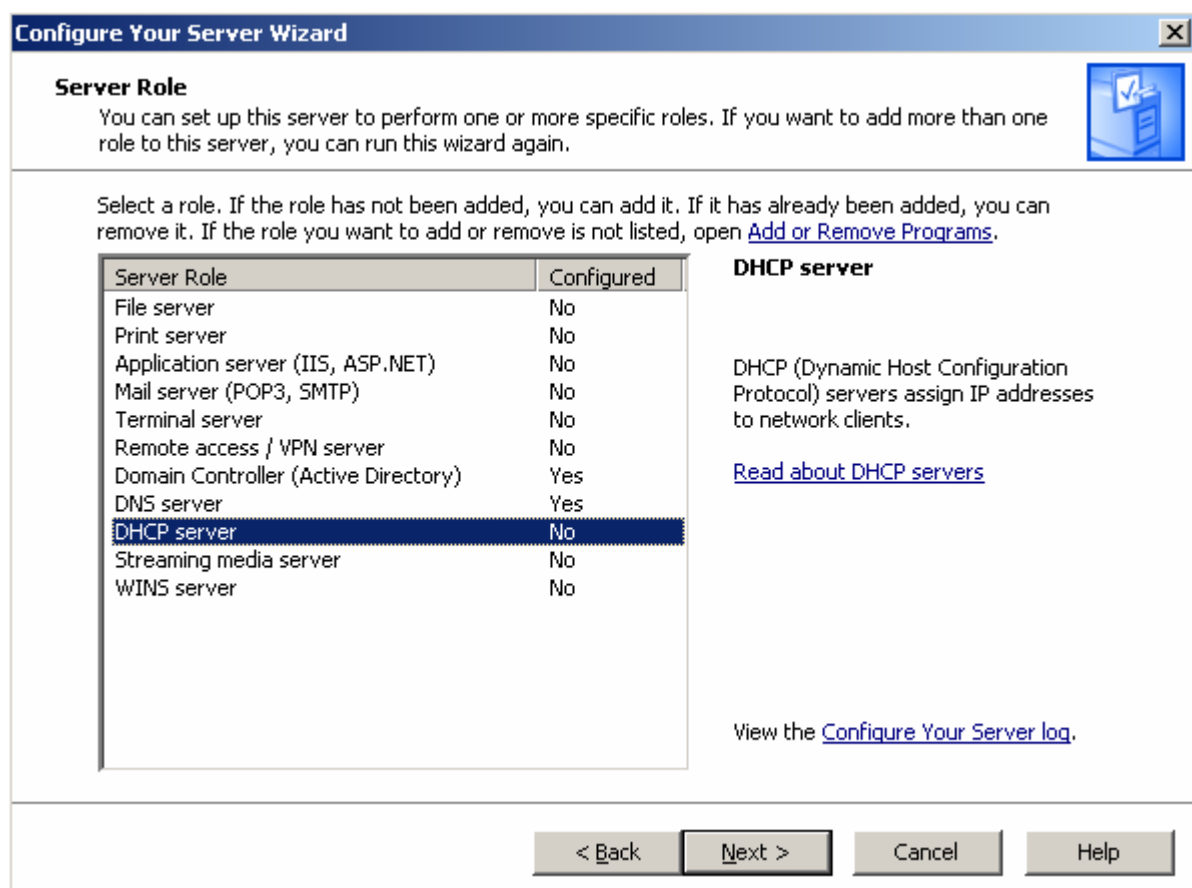
در پنجره Manage Your Server بر روی Add or remove a role کلیک کنید.



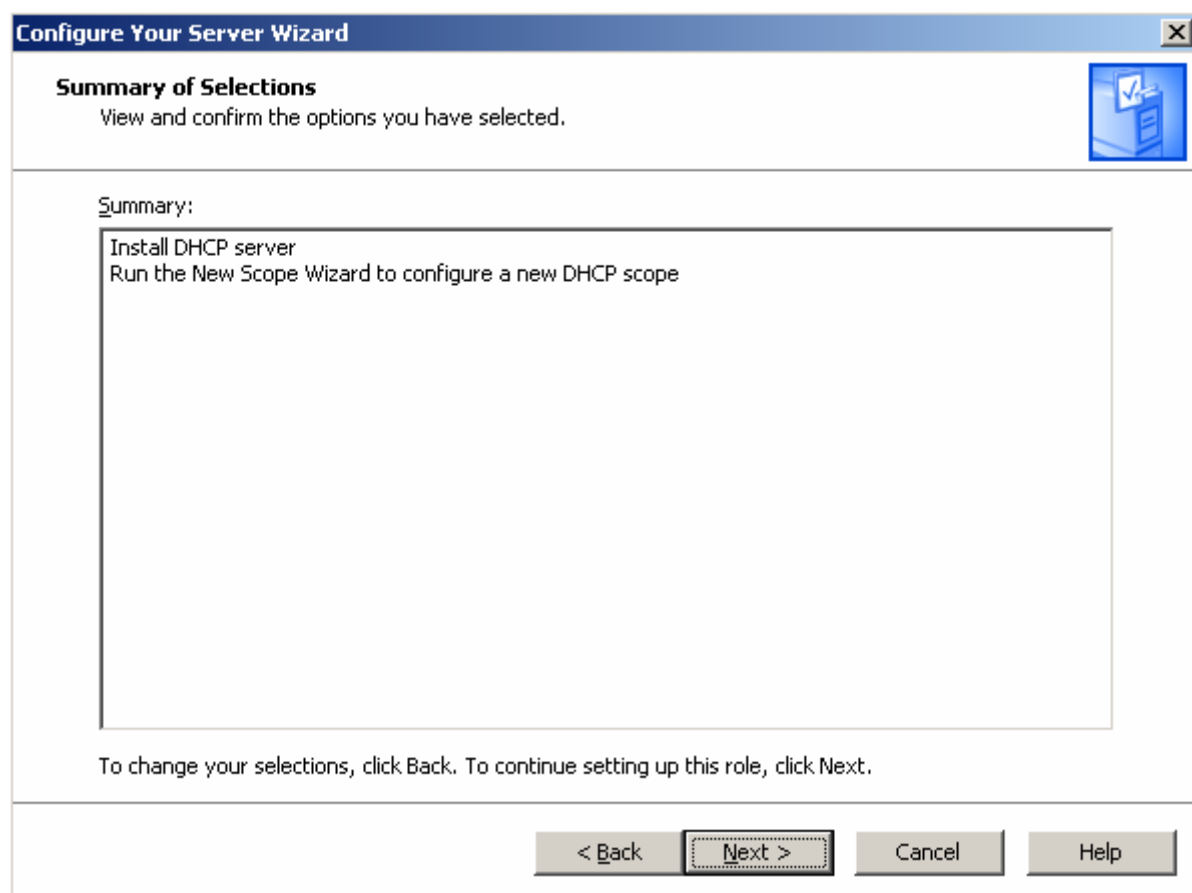
در پنجره ای که ظاهر می شود به شما گفته میشود که قبل از اینکه مراحل نصب را طی کنید باید اول موارد خواسته شده مانند نصب مودم ها و کارت های شبکه، متصل کردن کابل ها، گذاشتن CD ویندوز داخل CD-ROM و ... را انجام داده، سپس روی دکمه Next کلیک کنید.



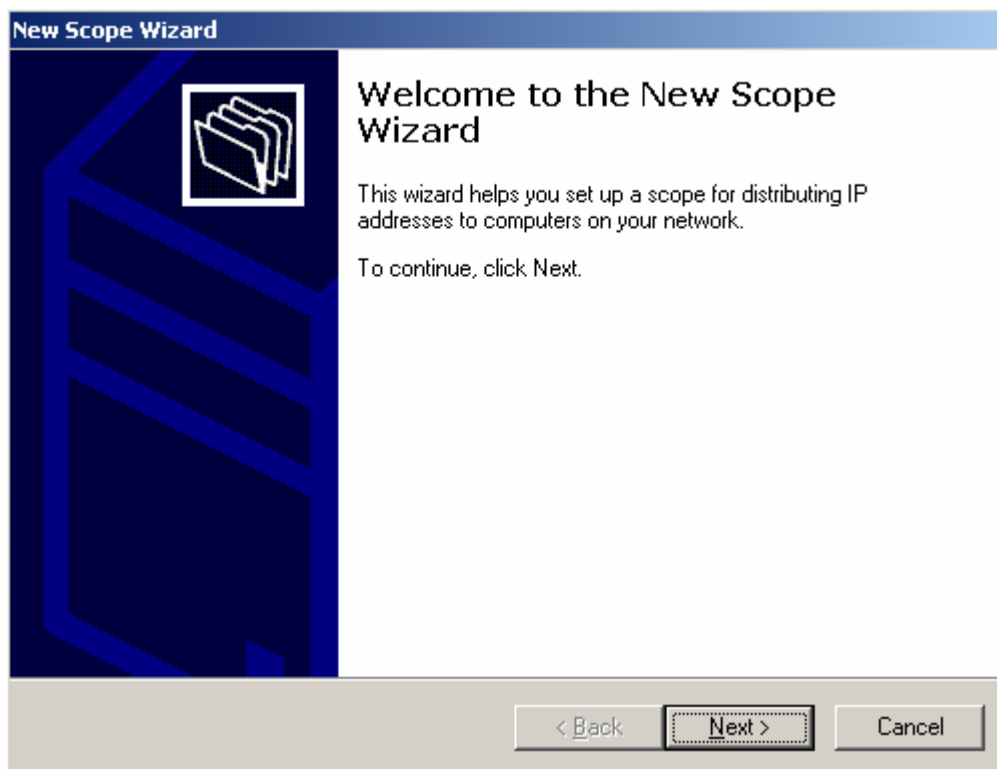
DHCP Server را انتخاب و Next کنید.



در این پنجره توضیح داده می شود که شما در حال نصب DHCP برای سرور و همچنین در حال ایجاد یک scope جدید می باشید. Next کنید.



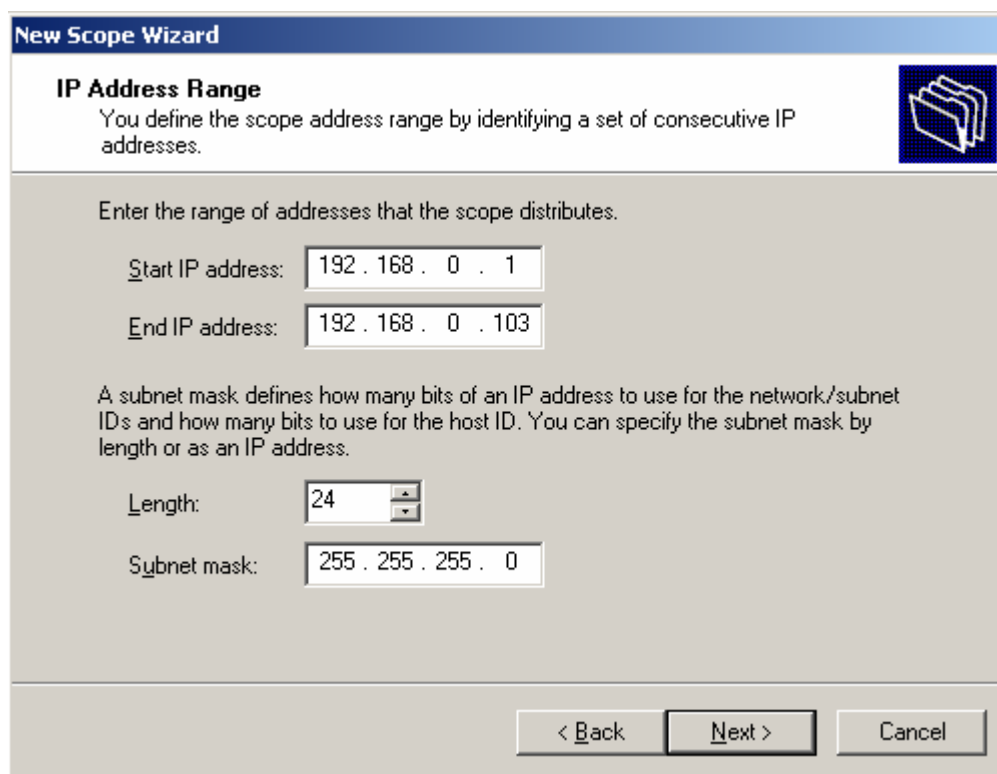
صفحه خوش آمد گویی برای ایجاد scope نمایش داده می شود که برای ادامه بر روی Next کلیک کنید.



در این مرحله در قسمت Name برای Scope خود یک نام در نظر میگیریم (در این مثال از نام Test استفاده می کنیم). بعد از زدن دکمه Next وارد مرحله بعدی که همان تعریف محدوده IP یا همان IP Address Range است میشوید.

در این قسمت آدرس شروع و پایان محدوده آدرسی را که می خواهیم تعریف کنیم را وارد میکنیم. شبکه ما متشکل از ۱۰۰ سرویس گیرنده و ۳ سرویس دهنده است پس ما نیاز به ۱۰۳ آدرس IP داریم. پس شروع محدوده را از آدرس ۱۹۲،۱۶۸،۰،۱ در نظر میگیریم و پایان محدوده را ۱۹۲،۱۶۸،۰،۱۰۳ تعریف میکنیم.

قسمت پایین محدوده آدرس به Subnet Mask تعلق دارد. این گزینه برای تعریف Subnet یا تقسیم یه شبکه به منظور افزایش یا کاهش تعداد NetID و HostID در یک کلاس خاص انجام میگیرد. در قسمت Subnet mask کلیک کنید تا به صورت خودکار با توجه به کلاس آدرس IP که وارد کرده اید mask آن نیز در نظر گرفته شود.



New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 0 . 1

End IP address: 192 . 168 . 0 . 103

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

در این مرحله امکان Exclude کردن برخی از آدرسها وجود دارد. بدین معنی که بطور مثال تعریف آدرسهای سرورها بصورت دستی با Manual میباشد. به عبارت دیگر برای تعریف آدرسهای سرورها از DHCP استفاده نمیکنیم و این آدرسها را به صورت دستی به این کامپیوترها میدهیم. آدرسهای 192.168.0.1 تا 192.168.0.3 را Exclude می کنیم.

New Scope Wizard

Add Exclusions
Exclusions are addresses or a range of addresses that are not distributed by the server.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: 192 . 168 . 0 . 1 End IP address: 192 . 168 . 0 . 3 **Add**

Excluded address range:

Remove

< **Back** **Next >** **Cancel**

بر روی **Add** کلیک کنید تا IP به Excluded اضافه شود.

New Scope Wizard

Add Exclusions
Exclusions are addresses or a range of addresses that are not distributed by the server.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: End IP address: **Add**

Excluded address range:

192.168.0.1 to 192.168.0.3 **Remove**

< **Back** **Next >** **Cancel**

در مرحله بعد **Lease Duration** یا زمان گرفتن آدرس از یک کامپیوتر را تعریف میکنیم. برای مثال اگر این گزینه روی ۸ روز تعریف شود در این مدت زمان به طور دائم درخواست به طرف ماشینی که دارای آدرس از طرف DHCP است ارسال میشود. اگر در این زمان به هر دلیل ماشین پاسخی برای تمدید آدرس به سمت سرور ارسال ننماید پس از این مدت زمان آدرس از این ماشین گرفته شده و در اختیار دیگر ماشینهایی که نیاز به آدرس دارند قرار می گیرد.

New Scope Wizard

Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

< Back Next > Cancel

این پنجره مرحله Configure DHCP Options میباشد که برای تعریف آدرسهای مورد نیاز Client بجز آدرس IP همانند آدرس Gateway یا همان دروازه خروجی مثلاً برای ارتباط با دیگر شبکه ها، تعریف DNS Server و Wins Server نیاز است تعریف می شود. اگر مایل به تعریف این آدرسها هستید گزینه Yes, I want to configure this option now و در صورت عدم نیاز و تعریف این گزینه ها در آینده هستید گزینه No, I will configure this option later (که ما در این مثال این گزینه را انتخاب می کنیم) را بزنید.

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

☐ Yes, I want to configure these options now

☒ No, I will configure these options later

< Back Next > Cancel

در نهایت با زدن دکمه های Finish عمل تعریف Scope پایان می یابد.

New Scope Wizard

Completing the New Scope Wizard

You have successfully completed the New Scope wizard.

Before clients can receive addresses you need to do the following:

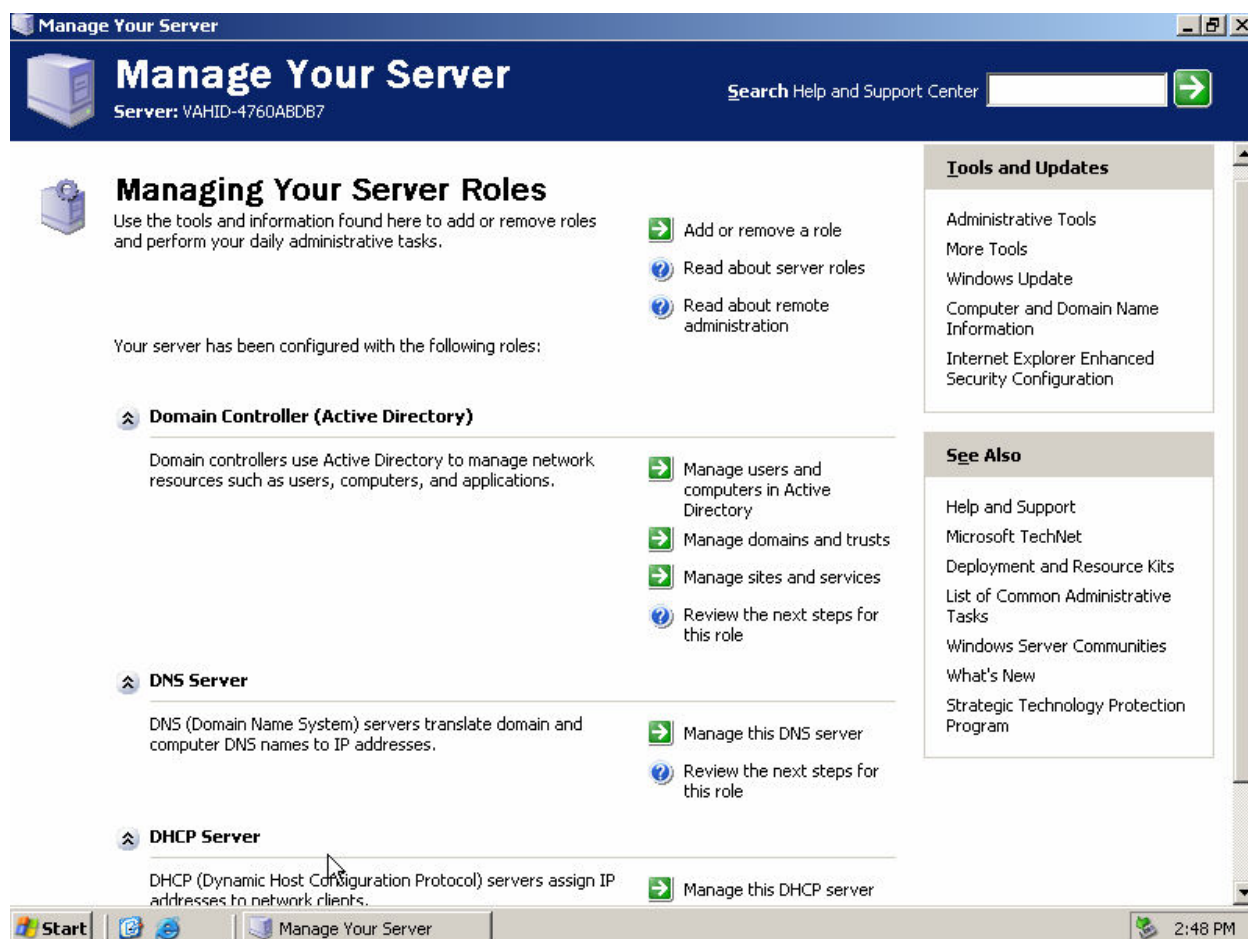
1. Add any scope specific options (optional).
2. Activate the scope.

To close this wizard, click Finish.

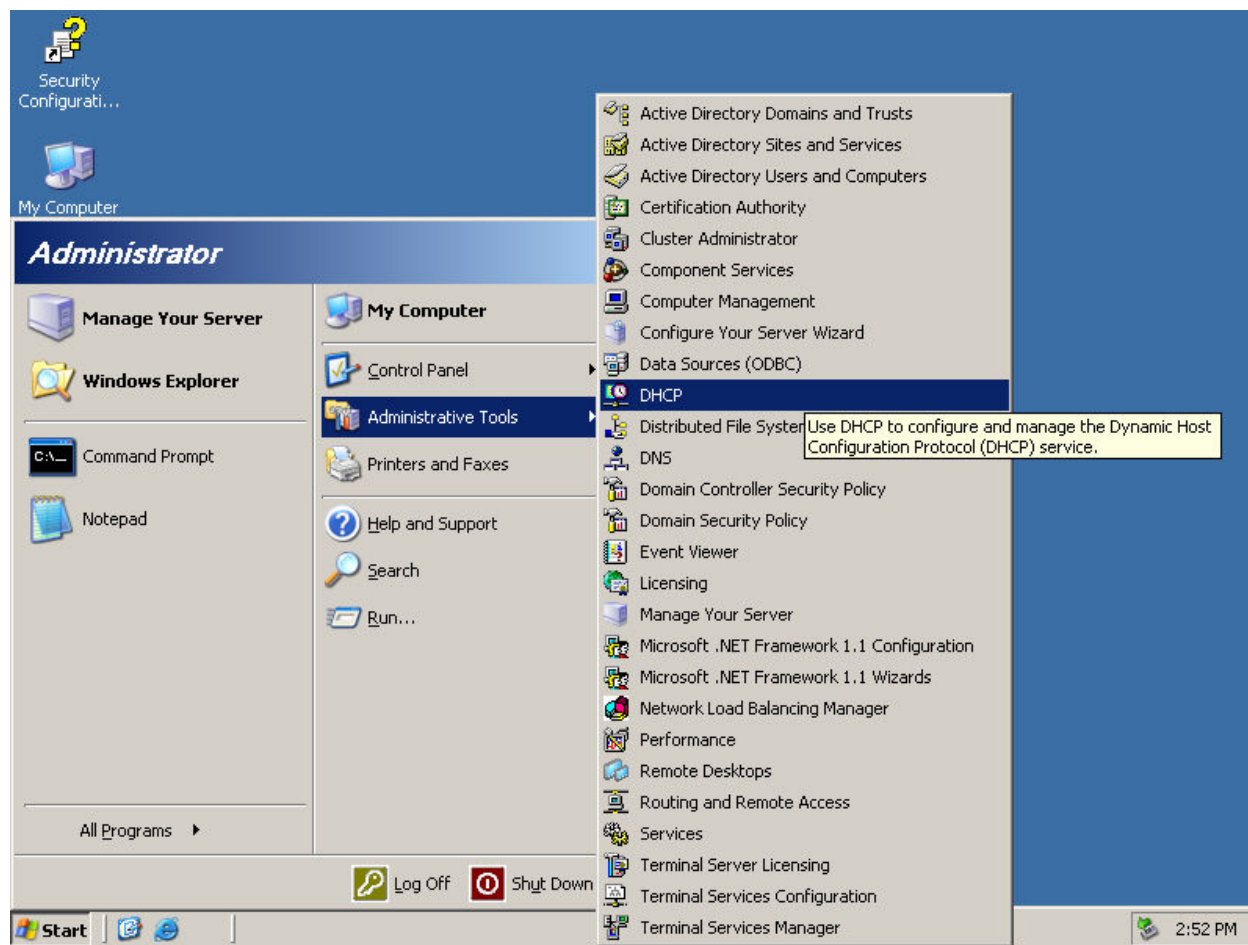
< Back Finish Cancel



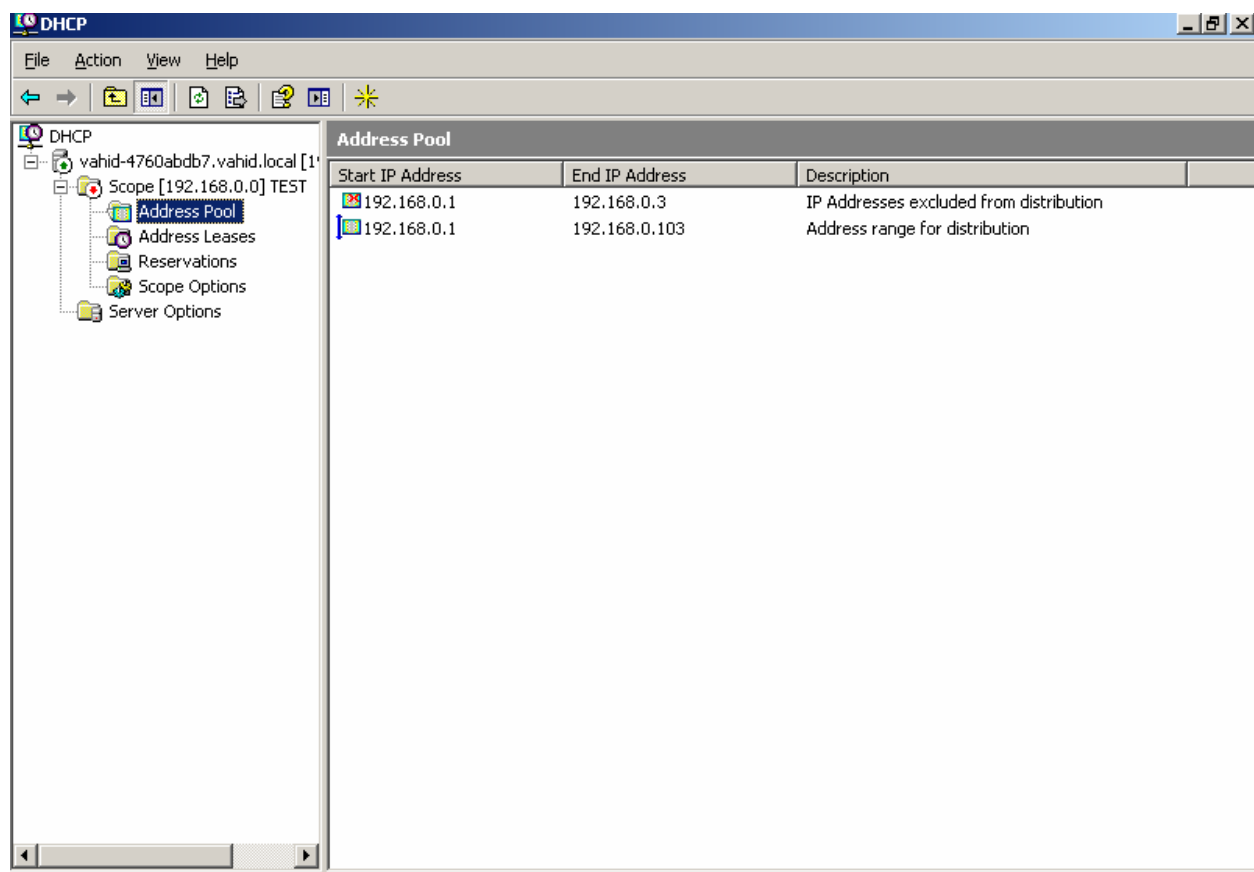
در پایین صفحه Manage Your Server مشاهده می کنید که نقش DHCP Server نیز به سرور اضافه شده است.



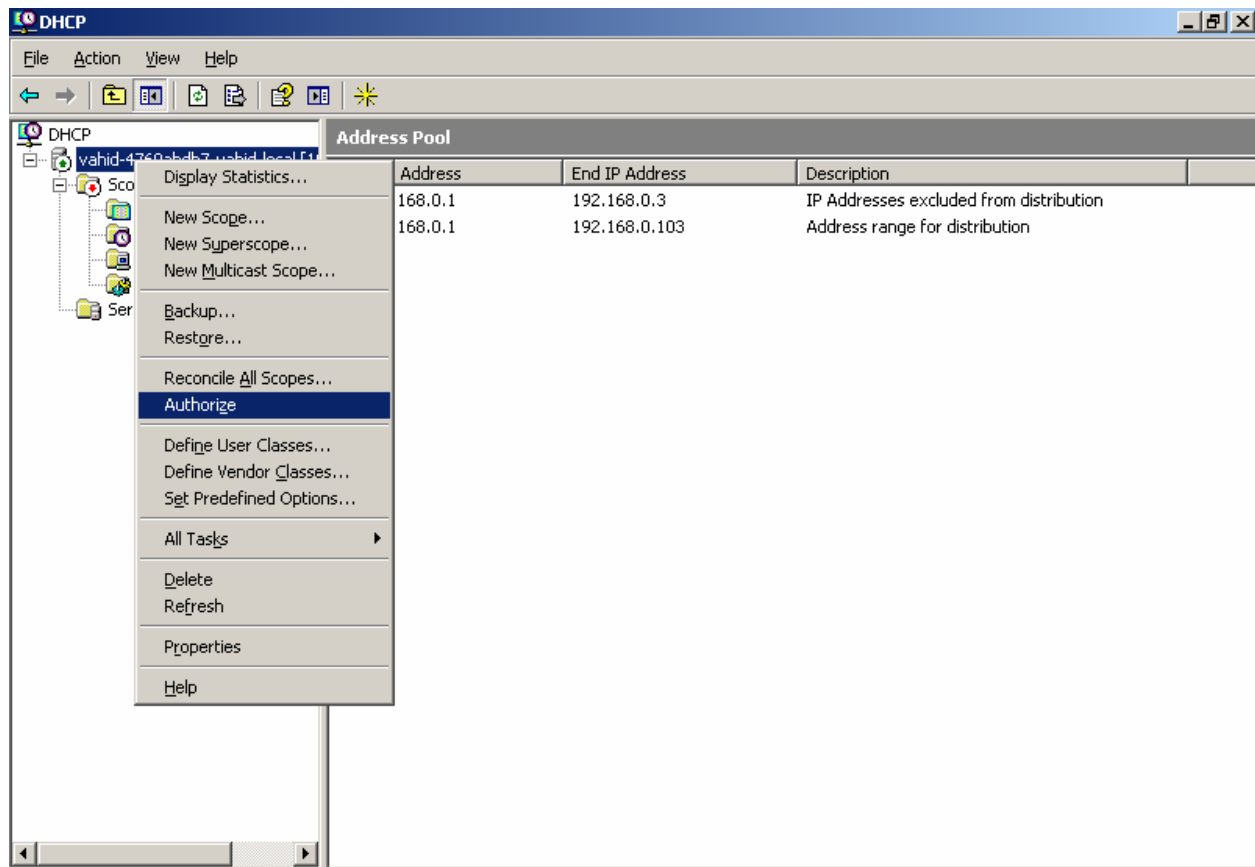
بعد از پایان یافتن مراحل نصب برای استفاده از سرویس DHCP به بخش مدیریت DHCP می رویم.



در این پنجره مشاهده می کنید که Scope ما در قسمت سمت چپ به صورت زیر دیده می شود.



برای فعال کردن این Scope کافی است روی سرور کلیک راست کرده وار منوی باز شده گزینه Authorize را انتخاب کنیم.

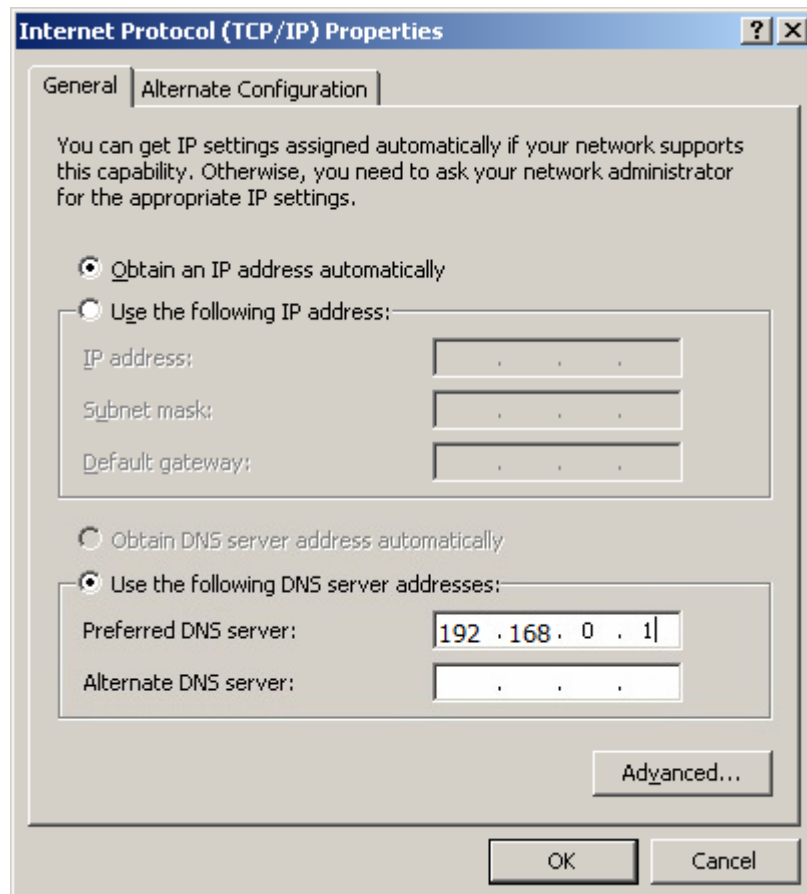


حال سرور DHCP جهت دادن آدرسهای مشخص شده آماده است و اگر این سرور به شبکه متصل باشد Client ها با ارسال درخواست از این سرور آدرس می گیرند.

۲-۲-۳- تنظیم DHCP بر روی کلاینت برای دریافت آدرس IP:

برای تنظیم DHCP بر روی کلاینت فقط کافی است:

گزینه Obtain an IP address automatically (تعیین IP به صورت اتوماتیک) را انتخاب کنید.



۳-۳- بررسی ویژگیهای MMC:

معرفی Microsoft Management Console یکی از اصلی ترین ابزارها برای مدیریت ویندوز سرور ۲۰۰۳ MMC می باشد. MMC امکان ایجاد واسط کاربری های استاندارد را که شامل یک یا چند برنامه کاربردی که اصطلاحاً Snap-in گفته می شوند را می دهد. شما با این برنامه ها می توانید محیط ویندوز خود یا سایر کامپیوترهای شبکه را تنظیم کنید .

ساختن یک MMC دلخواه:

با ایجاد یک MMC دلخواه دیگر لازم به اجرای چند برنامه مورد نظر ندارید تنها کفایت آنها را در MMC خودتان اضافه کنید و تنها با یک کلیک بین آنها حرکت کنید.

Console Option:

Console Option مشخص می کند که یک MMC چگونه آیتمهای موجود در Console Tree باز شوند

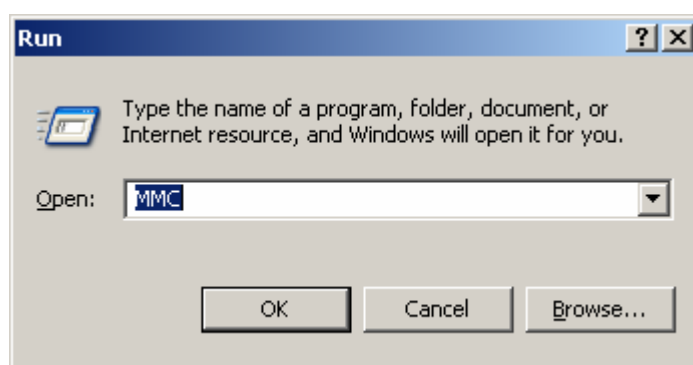
Author Mode:

هنگامیکه شما یک MMC را در حالت Author Mode ذخیره می کنید (این حالت پیش فرض است) تمامی گزینه های MMC نمایش داده خواهند شد.

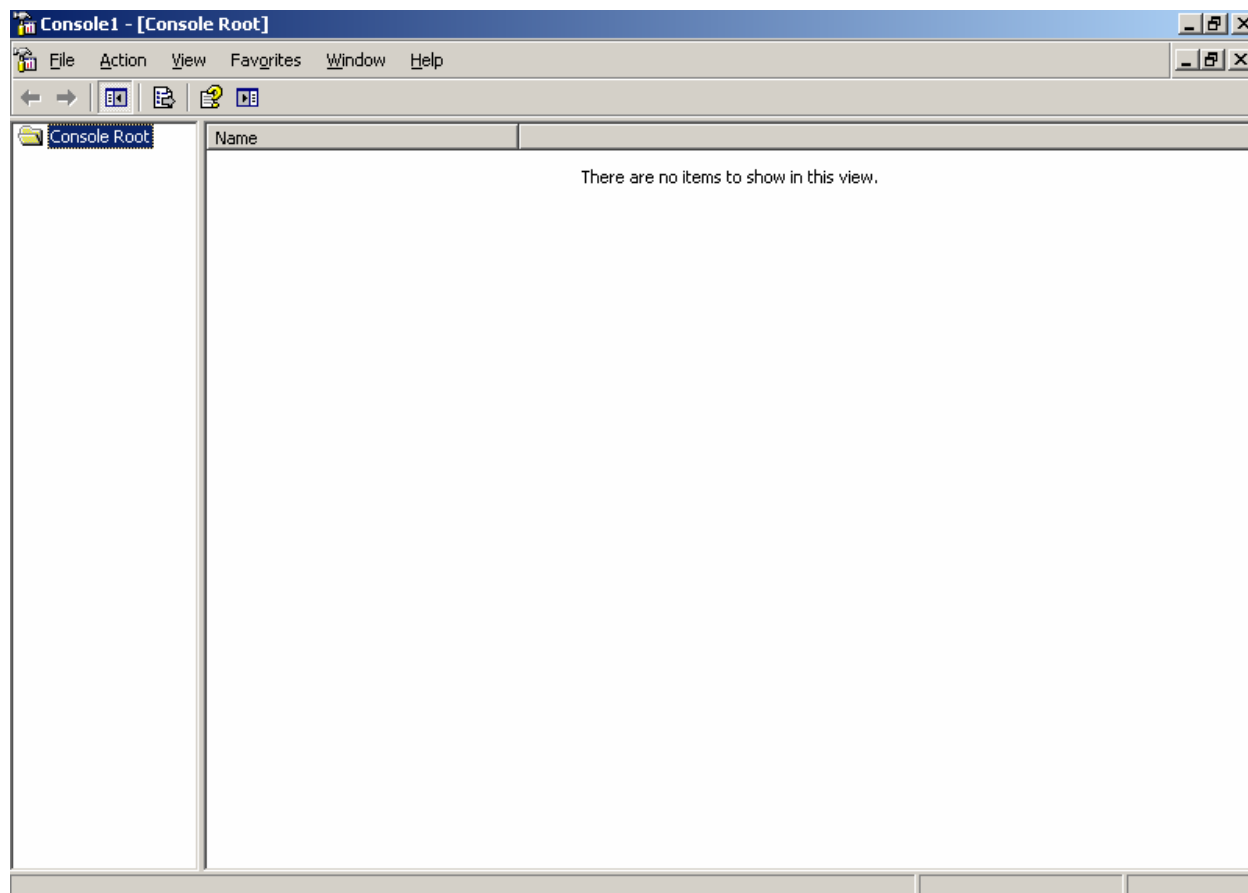
فرض کنید که می خواهیم یک کنسول ایجاد کنیم که بتوانیم سخت افزارهای مختلف نصب شده بر روی کلاینت ها را از طریق کنسول مدیریت کنیم. برای ایجاد این Console مدیریتی در MMC مراحل زیر را طی خواهید کرد:

بر روی Start->Run کلیک کنید.

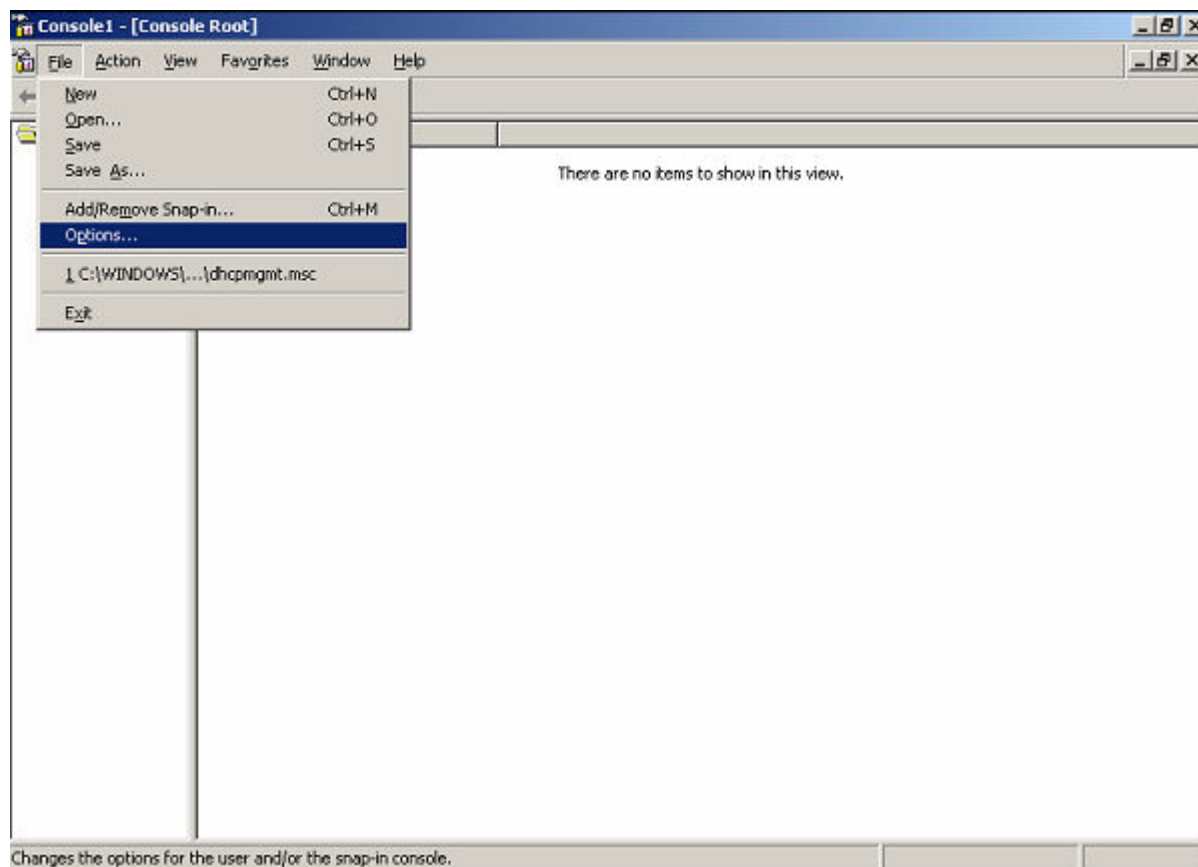
در قسمت Open عبارت MMC را تایپ کنید.



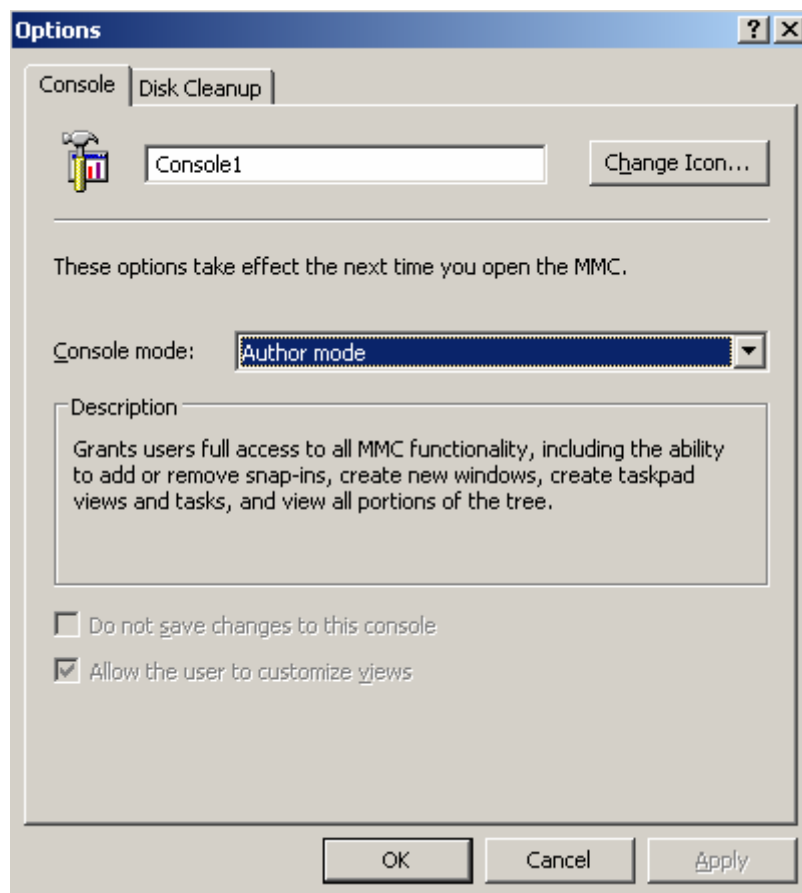
پنجره Console1 و Console Root نمایش داده می شود.



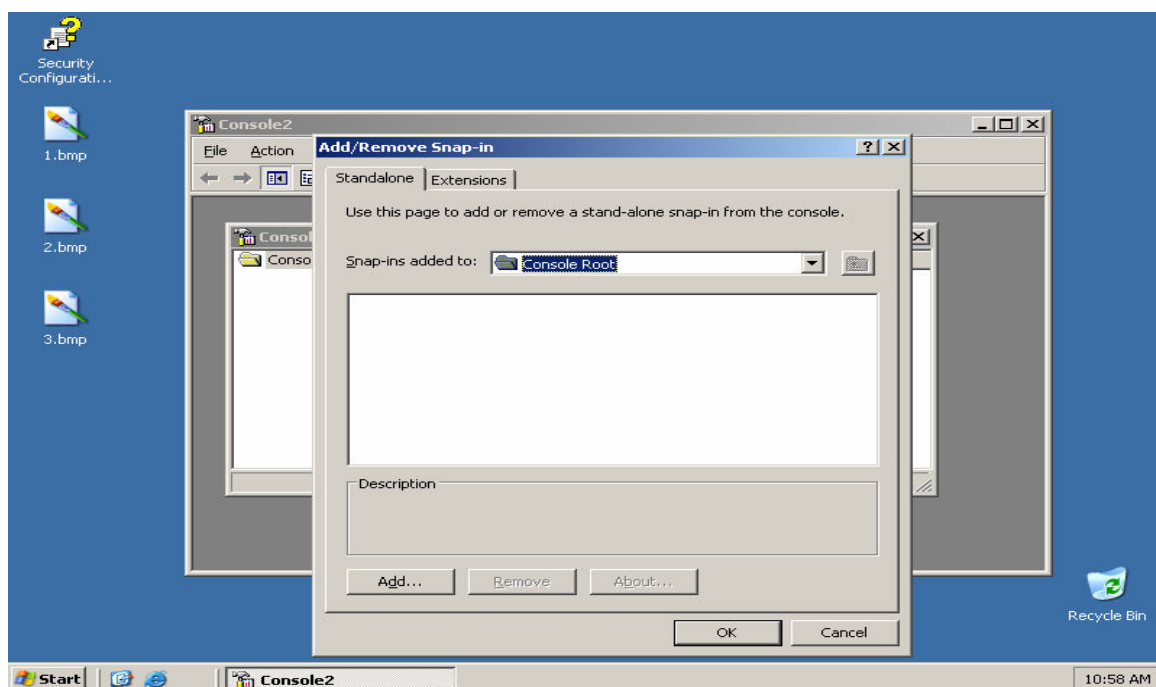
از منوی File گزینه Option را انتخاب کنید تا تنظیمات Console را مشاهده کنید و ببینید که در چه مدی قرار دارد.



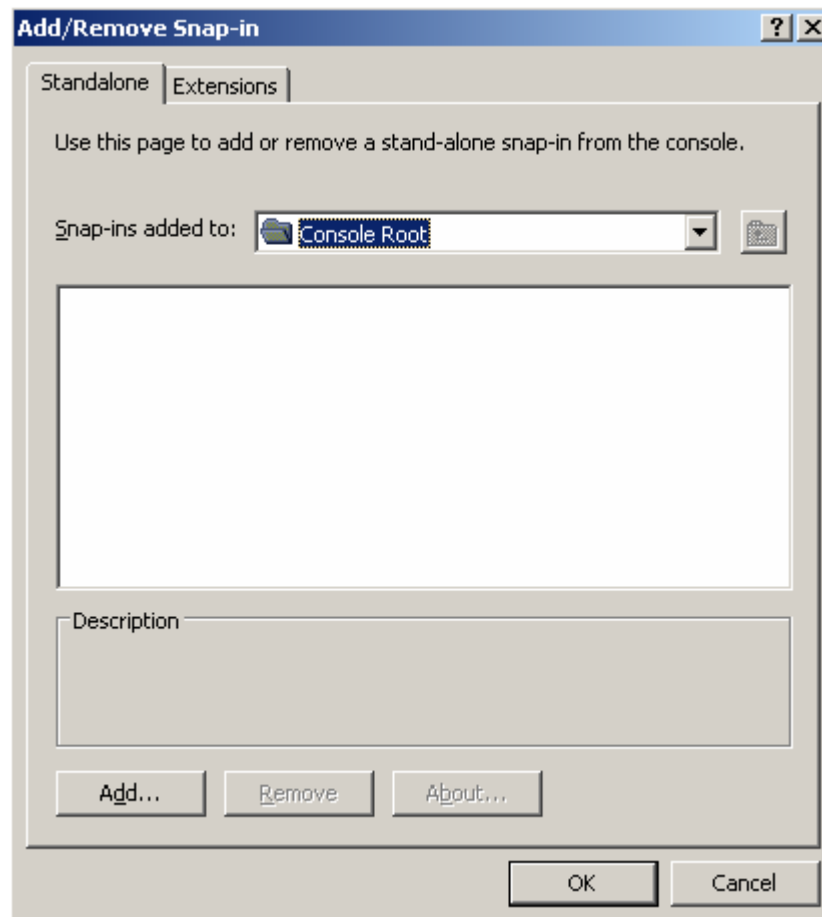
چک کنید که در حالت Author باشد و سپس بر روی Ok کلیک کنید.



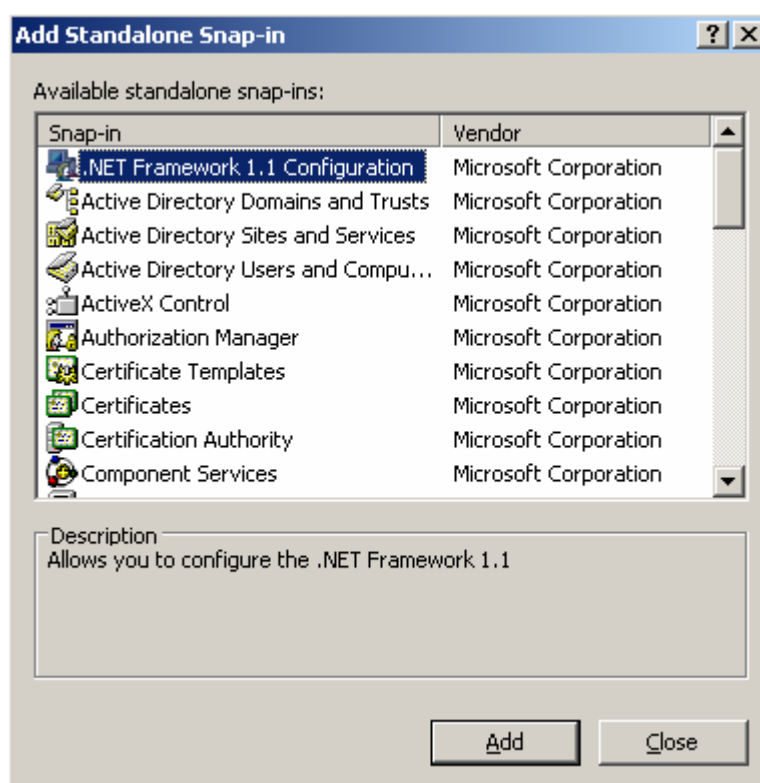
برای اضافه کردن کنسول از منوی فایل گزینه Add/Remove Snap-In را انتخاب کنید.



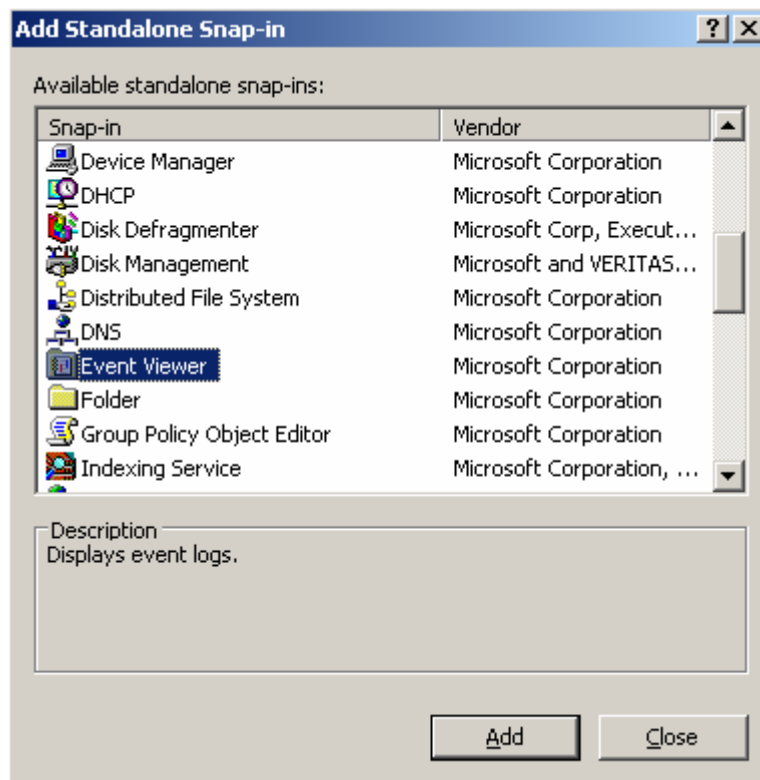
پنجره Add/Remove Snap-In ظاهر می شود و صفحه standalone فعال است.



برای اضافه کردن کنسول جدید در پنجره Add/Remove Snap-In بر روی Add کلیک کنید تا پنجره Add standalone Snap-In ظاهر شود.

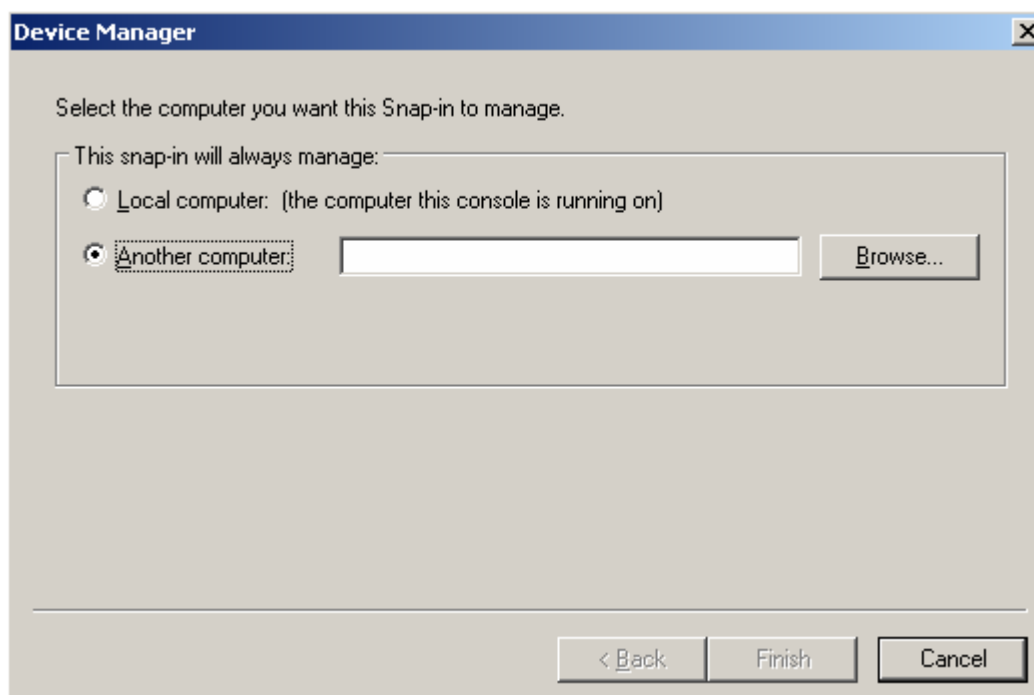


در این پنجره Device Manager را انتخاب و کلید Add را فشار دهید.



پنجره Select Computer باز می شود و به شما اجازه می دهد تا کامپیوتری که می خواهید مدیریت کنید را انتخاب کنید. اگر گزینه Local Computer را انتخاب کنید برنامه Device Manager بر روی کامپیوتر شما اجرا خواهد شد و اگر گزینه Another Computer را انتخاب کنید و کامپیوتر شما در شبکه قرار داشته باشد می توانید کامپیوتر مورد نظر خود را انتخاب کنید.

گزینه Another computer را انتخاب کنید و بر روی Browse کلیک کنید.



در این پنجره برای انتخاب کامپیوترهای مورد نظر بر روی Advanced کلیک کنید.

۴-۳- بررسی افزودن کامپیوتر در ۲۰۰۳ سرور:

این اکانت ها نیز یکی از Object های AD است. این اکانتها برای سیستم عامل هایی که عضو Domain می شوند وجود دارند:

۱- Windows NT

۲- Windows 2000

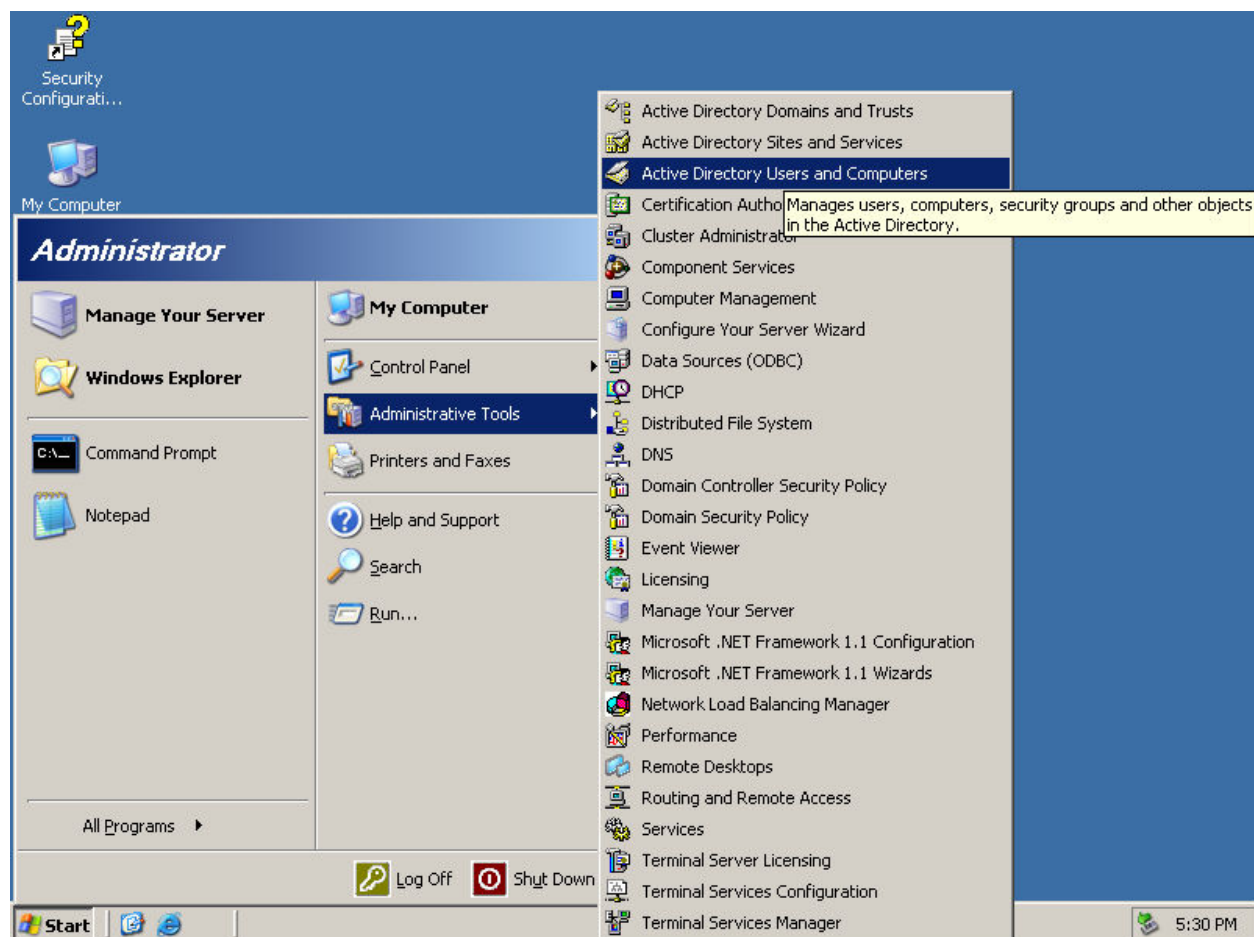
۳- Windows XP

۴- Windows 2003

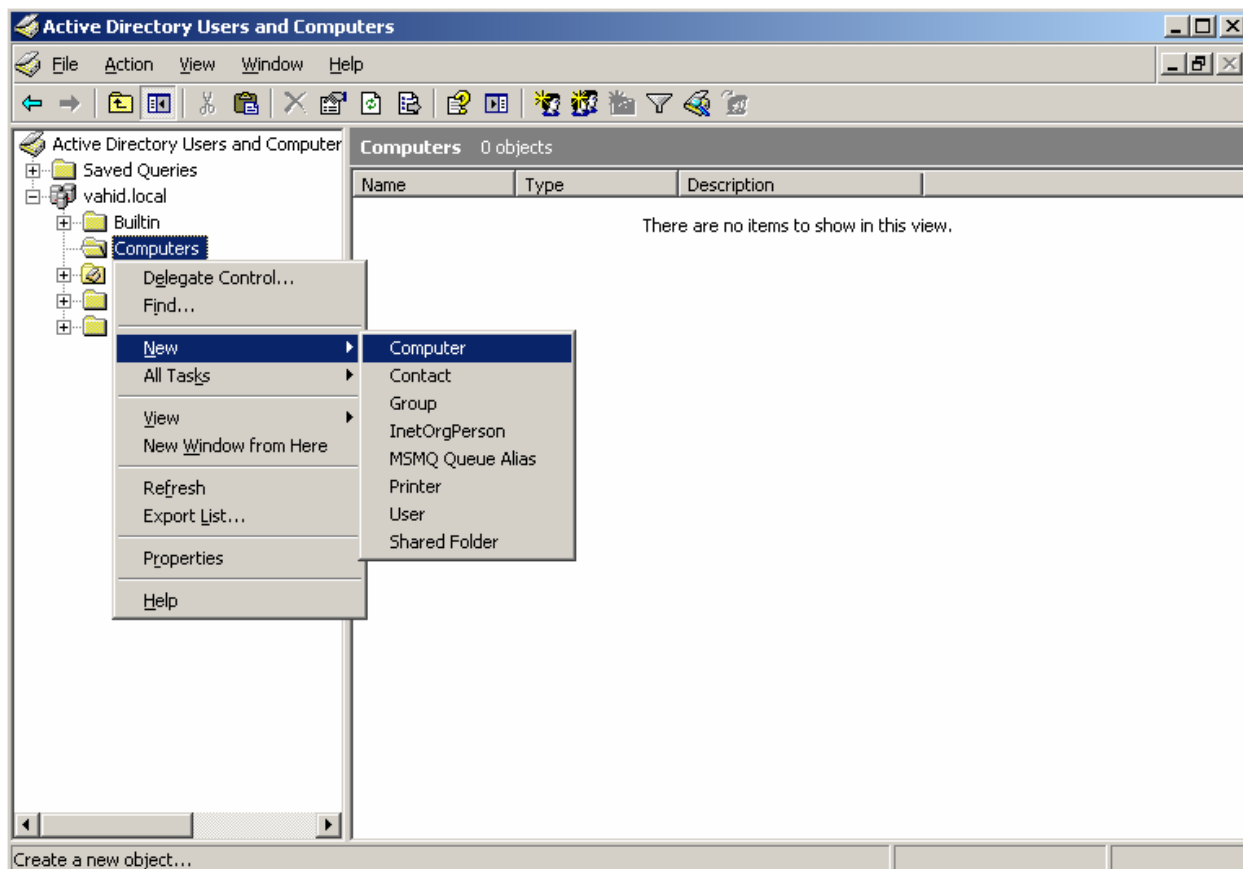
از این Object ها برای مواردی از جمله نصب برنامه ها به صورت اتوماتیک روی کامپیوترها می توان نام برد. بدین معنی که کاربران اجازه Logon از کامپیوتر هایی را دارند که برای آن کامپیوتر در AD یک Computer Account وجود داشته باشند. در صورت غیر فعال شدن یک Computer Account هیچ کاربری اجازه Logon از روی آن را نخواهد داشت.

برای اضافه کردن یک کامپیوتر در ویندوز ۲۰۰۳ سرور این مراحل را انجام دهید:

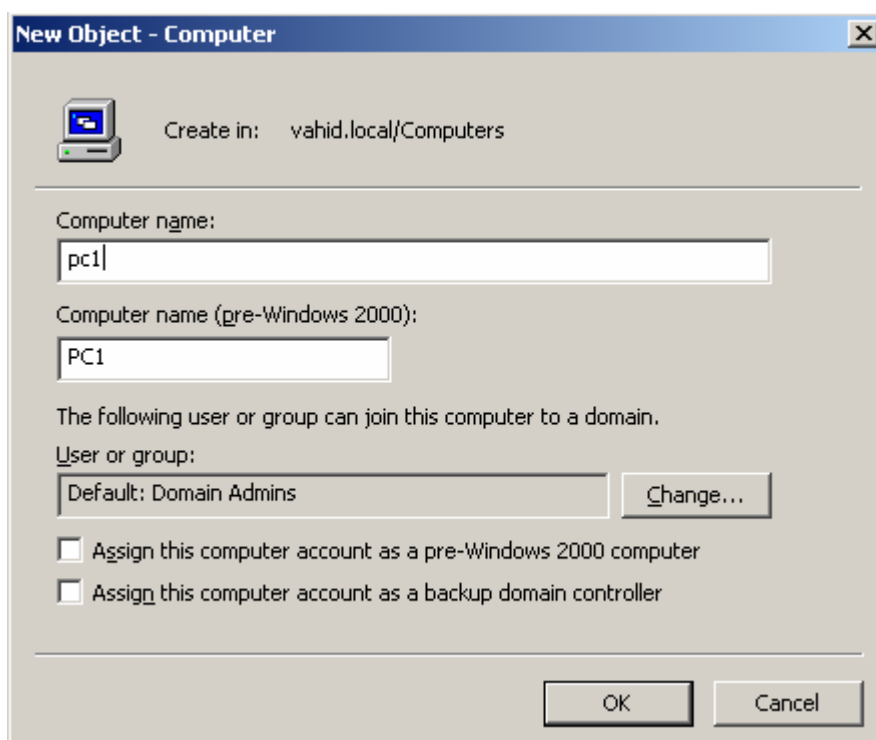
برای این کار از مسیر Start > Administrative tools بر روی Active directory users and computers کلیک کنید.



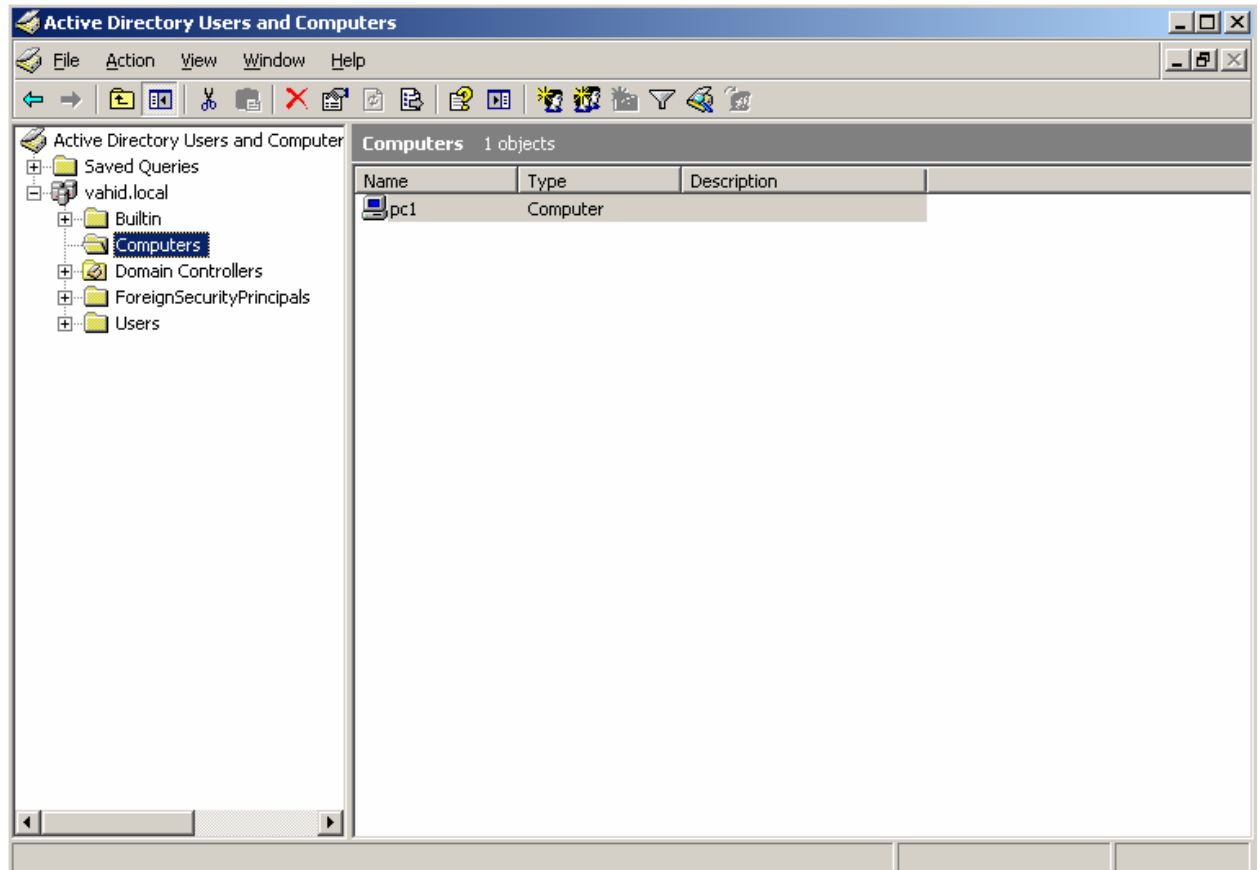
در زیر شاخه دامنه بر روی پوشه Computer راست کلیک کرده و از منوی ظاهر شده بر روی New و سپس بر روی Computer کلیک کنید.



در این پنجره باید نام کامپیوتری را که می خواهید اضافه کنید را وارد کرده بر روی OK کلیک کنید.



در این صفحه مشاهده می کنید که کامپیوتر Pc۱ به لیست Computers اضافه گردید.



۴. جزئیات بخش چهارم:

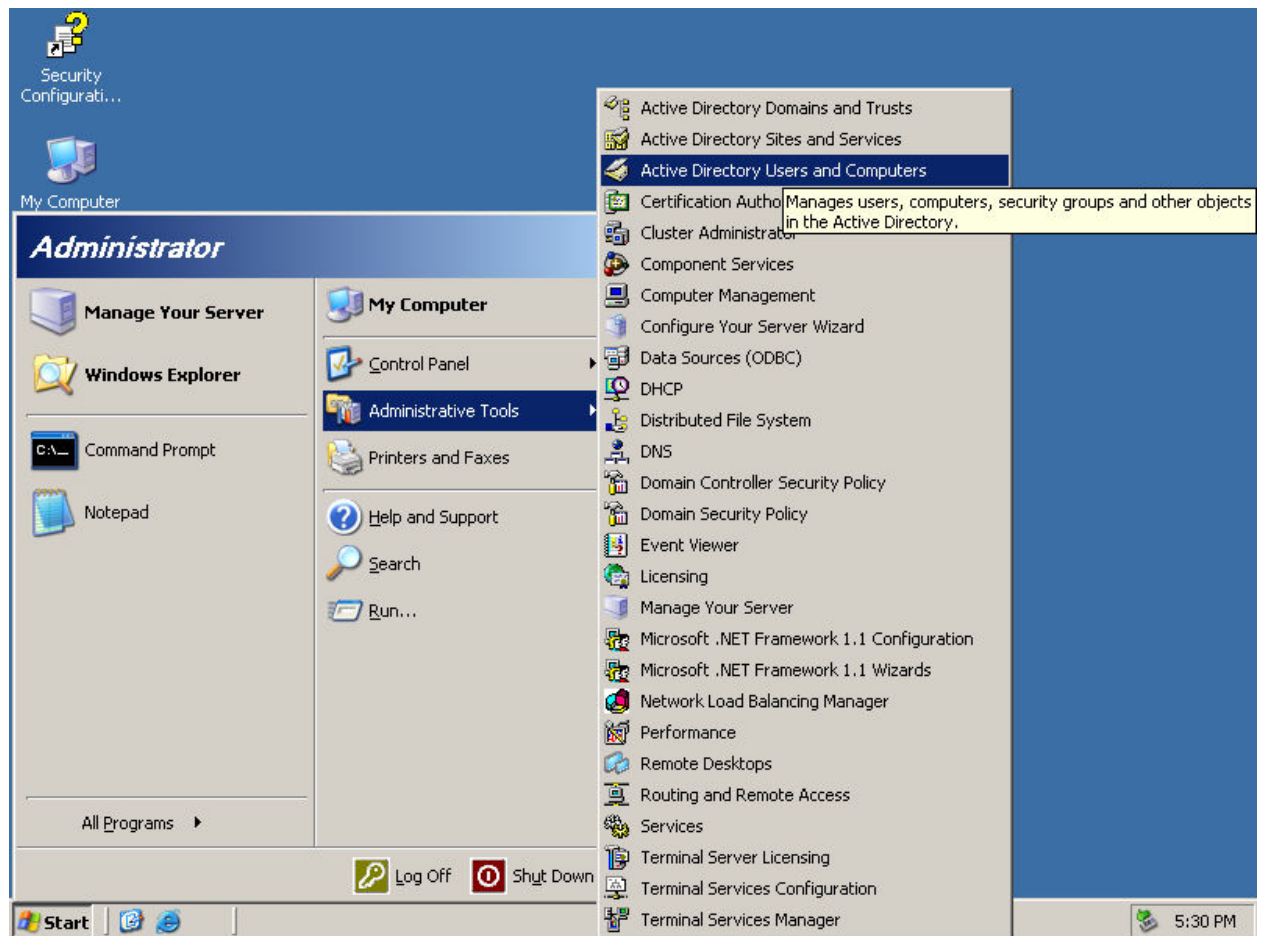
۴-۱- بررسی ویژگیهای standalone:


ویژگی Standalone در ۲۰۰۳ سرور یک مدل پایه ای برای مدیریت کاربران در سطح سرور می باشد به این صورت که فقط کاربران یک سرور و کامپیوترهای آن توسط Standalone مدیریت می شود. این بخش را می توان به WordPad خود ویندوز نسبت داد که امکانات پایه ای را برای تایپ فراهم می سازد و همچنان که برای داشتن یک محیط تایپی بهتر، از Word مجموعه Office استفاده می شود. برای مدیریت کاربران و کامپیوترها نیز در ۲۰۰۳ سرور از AD بهتر است استفاده شود.

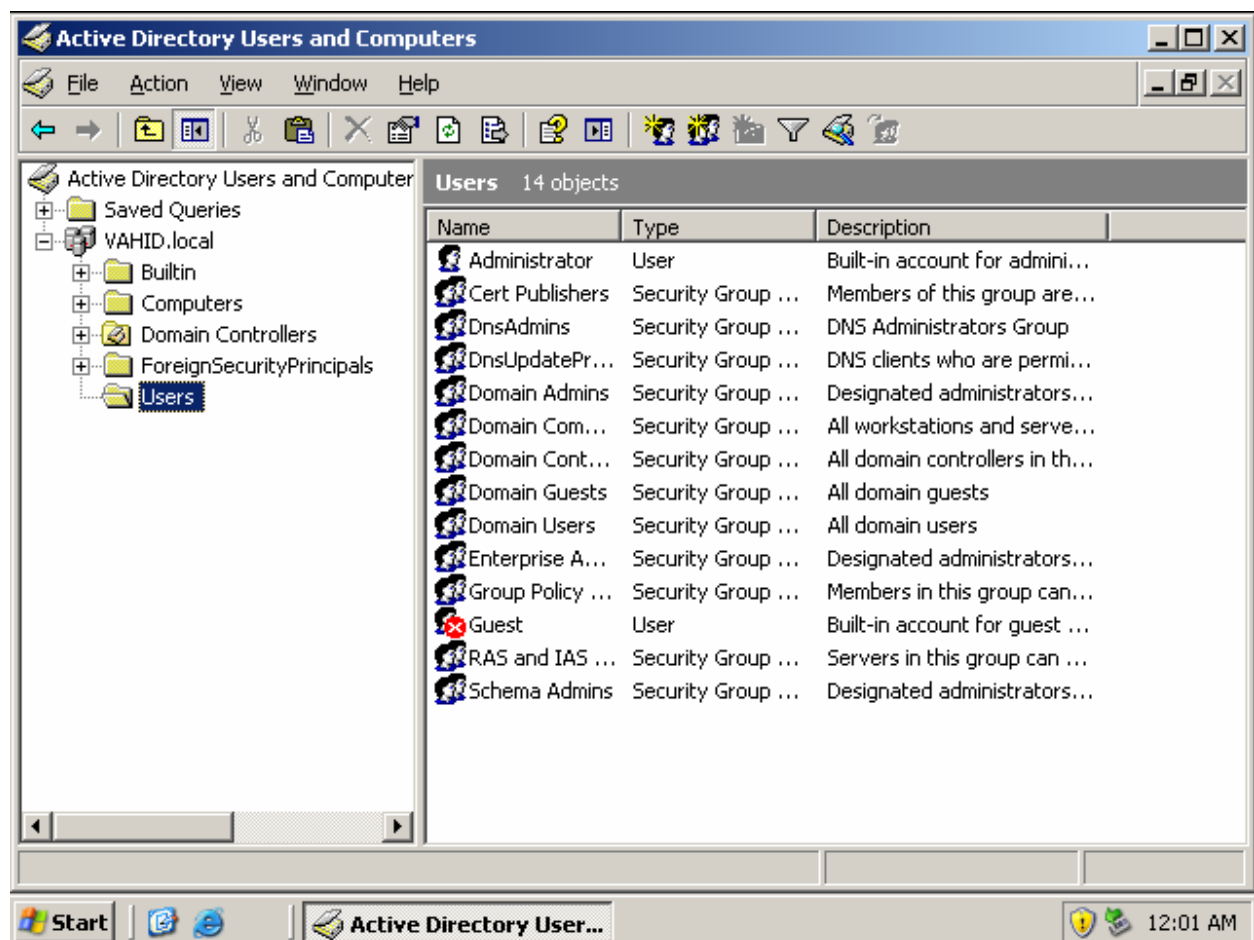
۴-۲- بررسی کاربران پیش فرض:

بعد از اینکه AD را بر روی سیستم نصب شد وقتی به ابزار مدیریتی Active Directory User and Computers برای مدیریت کاربران و کامپیوتر، از مسیر زیر بروید:

Start > Administrative Tools > Active Directory User and Computers

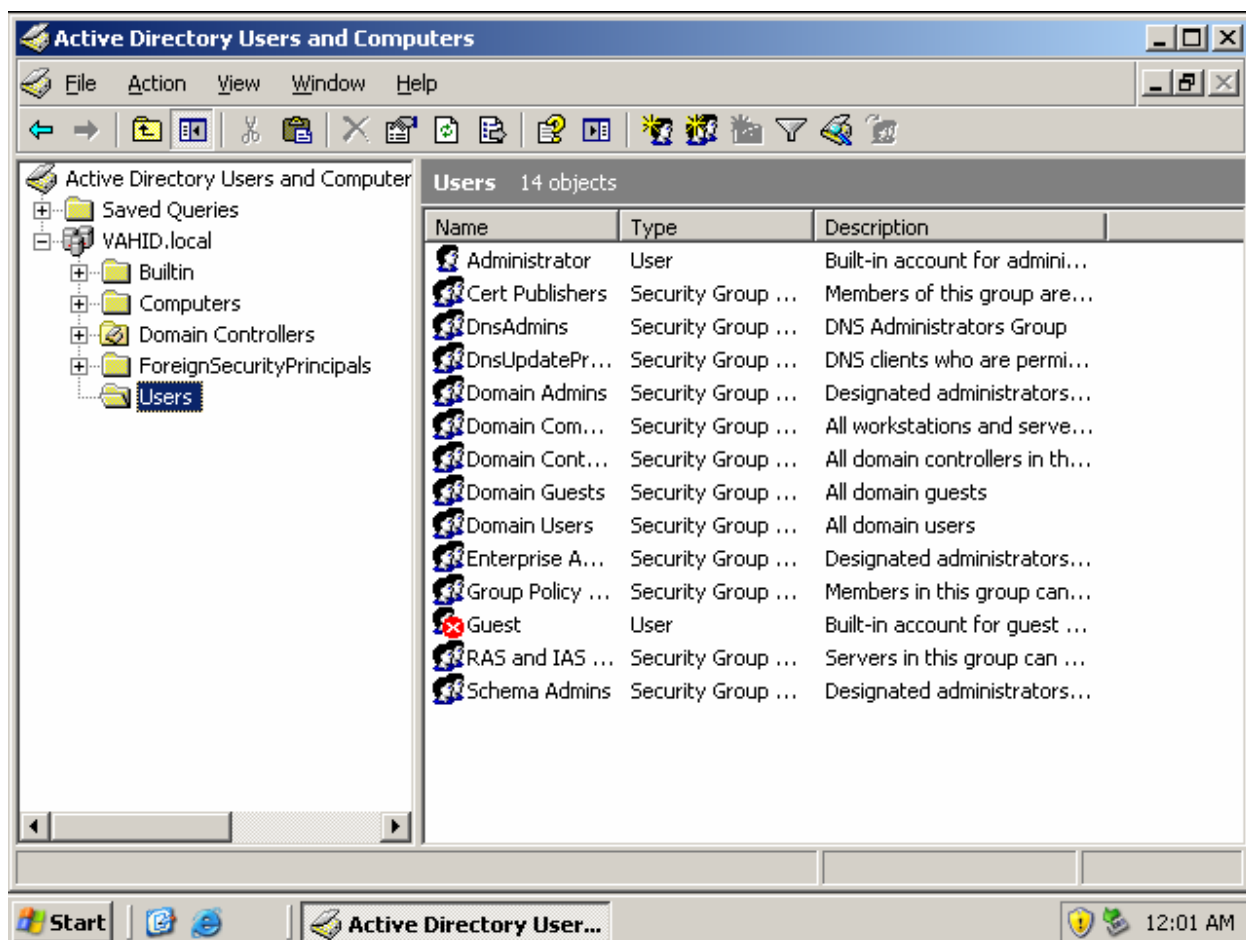


در این پنجره دامنه ای را که با نام Vahid.local ایجاد کردیم مشاهده می کنید. بر روی علامت + کلیک میکنیم تا لیستی از پوشه هایی که در vahid.local است نمایش داده شود. بر روی User (کاربر) کلیک می کنیم تا کاربرانی که بطور پیش فرض وجود دارند نمایش داده شوند. فقط کاربر administrator به عنوان مدیر شناخته می شود. کاربرانی که با این علامت  نشان داده می شوند غیر فعال (lock) هستند. کاربر administrator را می توان غیر فعال کرد ولی نمی توان آن را حذف کرد. کاربری به نام Guest نیز به صورت پیش فرض وجود دارد ولی غیر فعال می باشد. که می توان آن را حذف کرد.

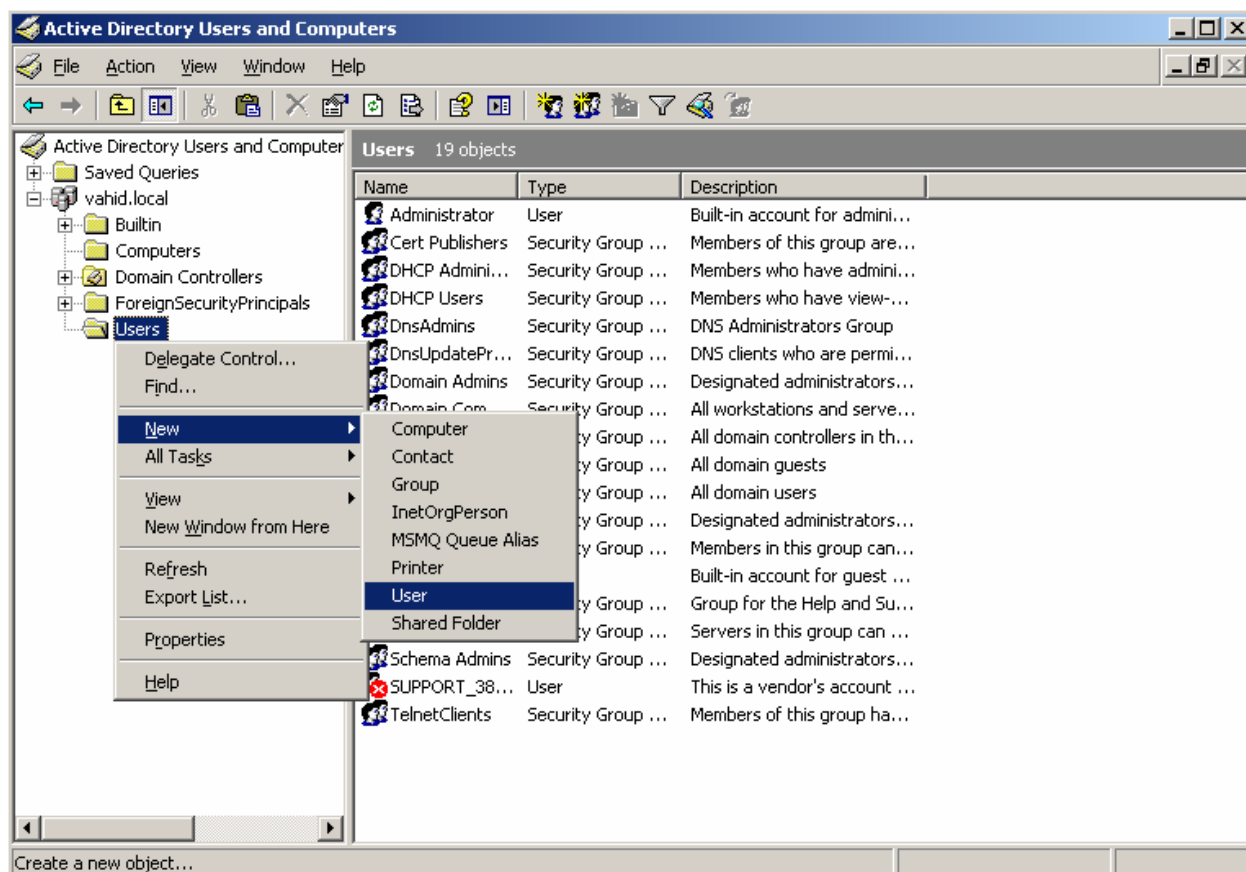


۳-۴- بررسی ایجاد کاربر جدید:

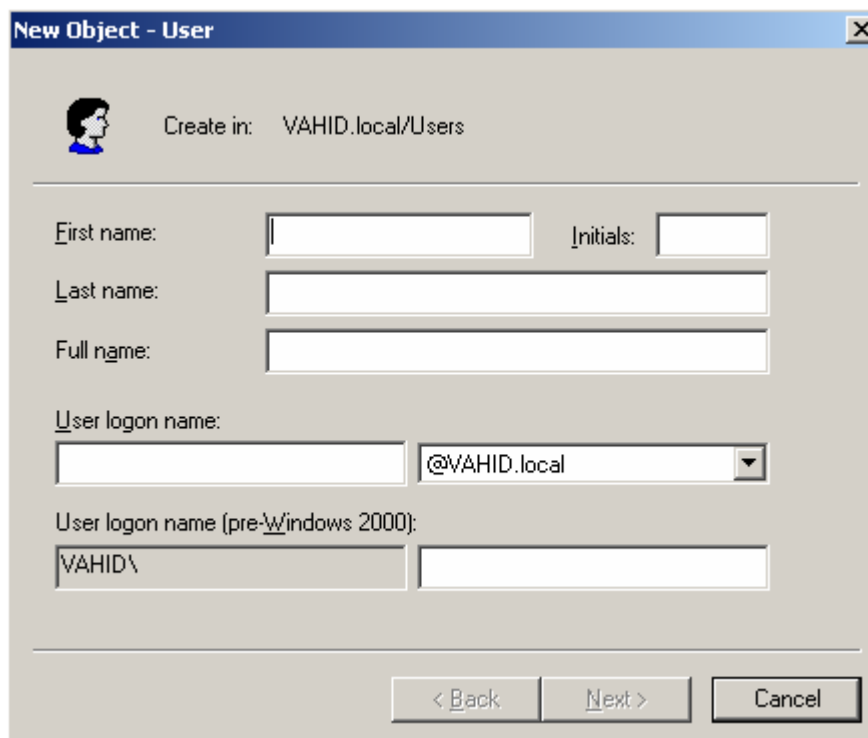
همانطور که قبلاً گفته شد هدف از نصب اکتیو دایرکتوری مدیریت کاربران در شبکه می باشد. برای ایجاد یک کاربر به Active Directory User and Computer بروید.



برای ایجاد یک کاربر جدید بر روی User راست کلیک کرده و از صفحه ظاهر شده بر روی گزینه New رفته و از لیست باز شده بر روی گزینه User برای ایجاد کاربر جدید کلیک کنید.



پنجره New Object-User نمایش داده می شود که باید مشخصات کاربر جدیدی را که می خواهید ایجاد کنید را وارد کنید.



First name: باید نام کاربر را وارد کنید.

Last name: نام خانوادگی کاربر را وارد کنید.

Full name: نام کامل کاربر که از نام و نام خانوادگی کاربر تشکیل شده و به صورت اتوماتیک نمایش داده خواهد شد.

User logon name: باید نامی را وارد کنید که قرار است کاربر با آن نام log on شود. (توجه کنید اسمی که در logon وارد می کنید باید در Domain منحصر به فرد باشد)

User logon name (per-windows 2000): نامی که برای ۲۰۰۳ سرو در نظر گرفته می شود به صورت پیش فرض برای ۲۰۰۰ نیز در نظر گرفته می شود.

مشخصات را وارد کرده بر روی Next کلیک کنید.

New Object - User

Create in: vahid.local/Users

First name: reza Initials:

Last name:

Full name: reza

User logon name: reza @vahid.local

User logon name (pre-Windows 2000): VAHID\ reza

< Back Next > Cancel

در پنجره زیر باید پسوردی برای کاربری که می خواهید ایجاد کنید اختصاص دهید.

۱-۳-۴- بررسی کلمه رمز کاربر جدید:

در پایین پنجره نیز چهار انتخاب وجود دارد:

User must change password at next logon: اگر علامت داشته باشد کاربر باید در اولین ورود به Domain رمز عبور خود را تغییر دهد.

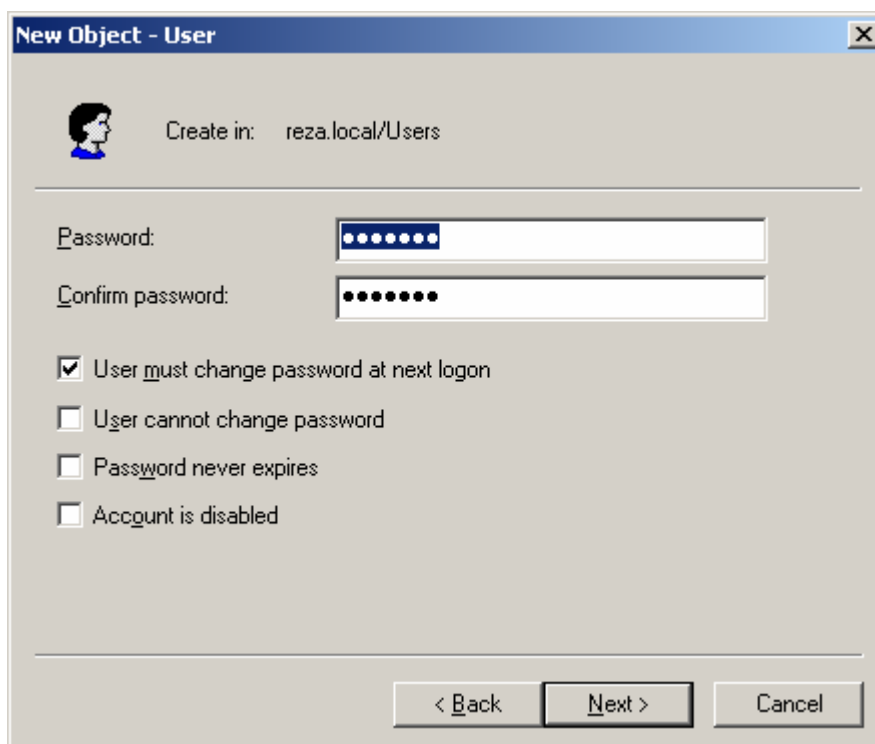
User cannot change password: اگر علامت داشته باشد به هیچ عنوان کاربر نمی تواند رمز خود را تغییر دهد.
نکته: توجه داشته باشید که نمی توان تیک را هم در گزینه اول و هم در گزینه دوم قرار داد.

Password never expires: اگر علامت داشته باشد پسورد همیشه باقی می ماند ولی اگر علامت را برداریم بعد از ۴۲ روز (پیش فرض) برای کاربر پیغام می آید که باید رمز خود را تغییر دهد.

Account is disabled: اگر علامت داشته باشد این نام کاربری ایجاد می شود ولی به طور موقت غیر فعال می ماند تا زمانی که خودمان آن را فعال کنیم. (این گزینه بیشتر در ادارتی که کارمندان آنها به مرخصی می روند کاربرد دارد)

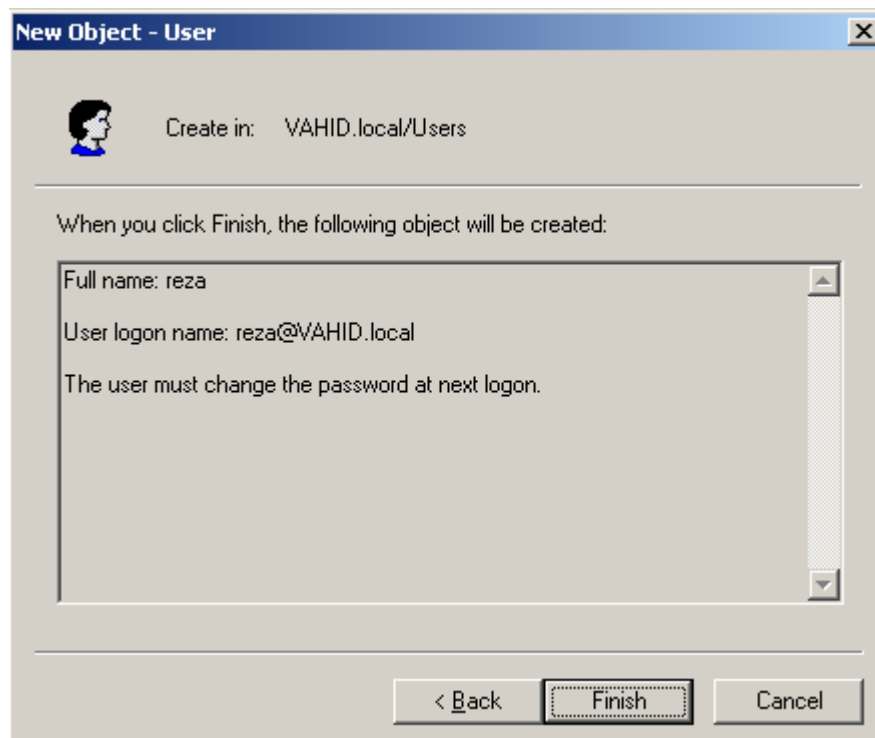
نکته: توجه داشته باشید که در دادن پسورد کاربر نیز مانند پسورد مدیر باید ویژگی های که برای پسورد به صورت پیش فرض در نظر گرفته شده است باید رعایت نمایید (حداقل ۶ کاراکتر، ترکیبی از: اعداد، حروف کوچک، حروف بزرگ و...) که البته این ویژگی را بعداً می توانیم تغییر دهیم.

پسورد را وارد کرده و این گزینه User must change password at next logon را انتخاب و بر روی Next کلیک می کنید.



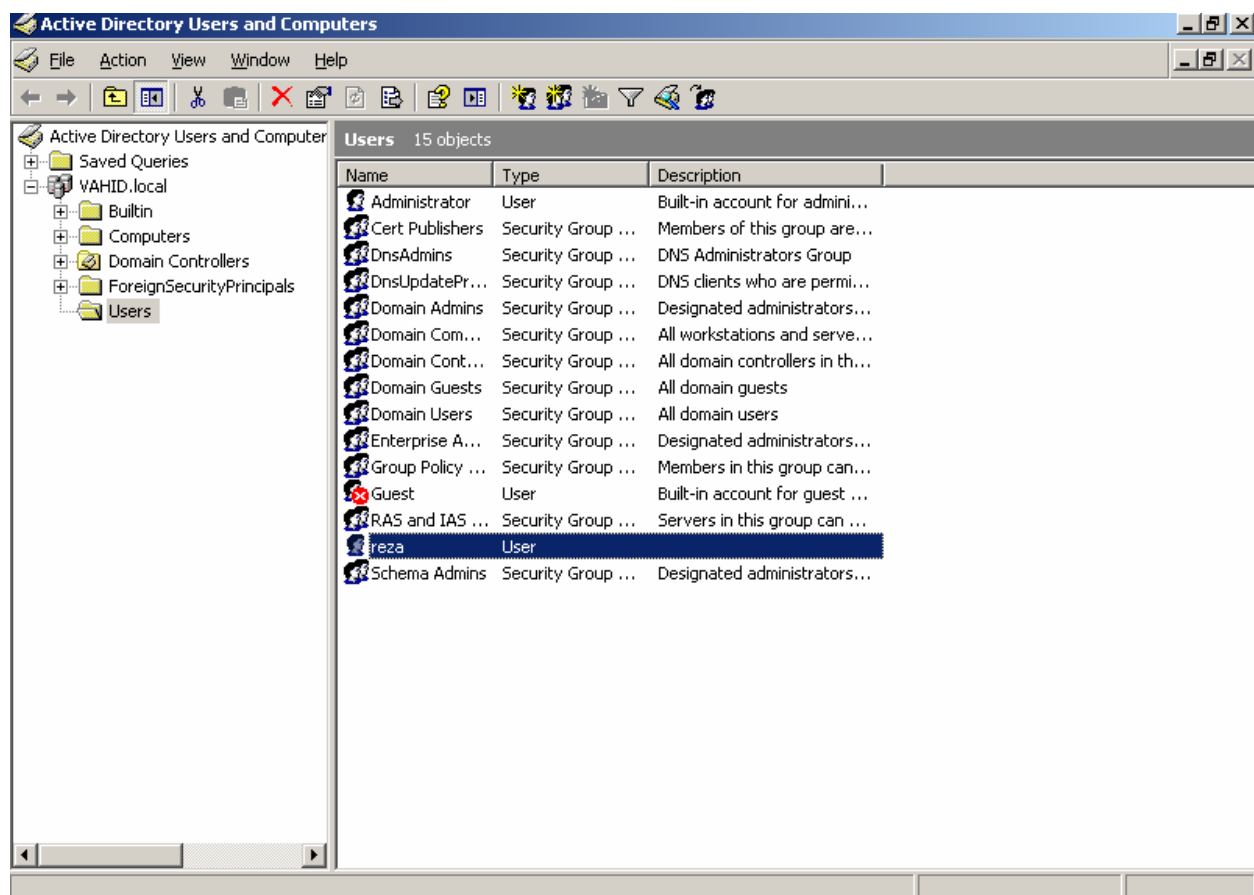
The dialog box is titled "New Object - User". It features a user icon and the text "Create in: reza.local/Users". Below this, there are two password input fields: "Password:" and "Confirm password:", both filled with dots. A list of checkboxes follows: "User must change password at next logon" (checked), "User cannot change password" (unchecked), "Password never expires" (unchecked), and "Account is disabled" (unchecked). At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

در این پنجره توضیح داده می شود که با کلیک بر روی Finish کاربری با مشخصات زیر ایجاد می شود.



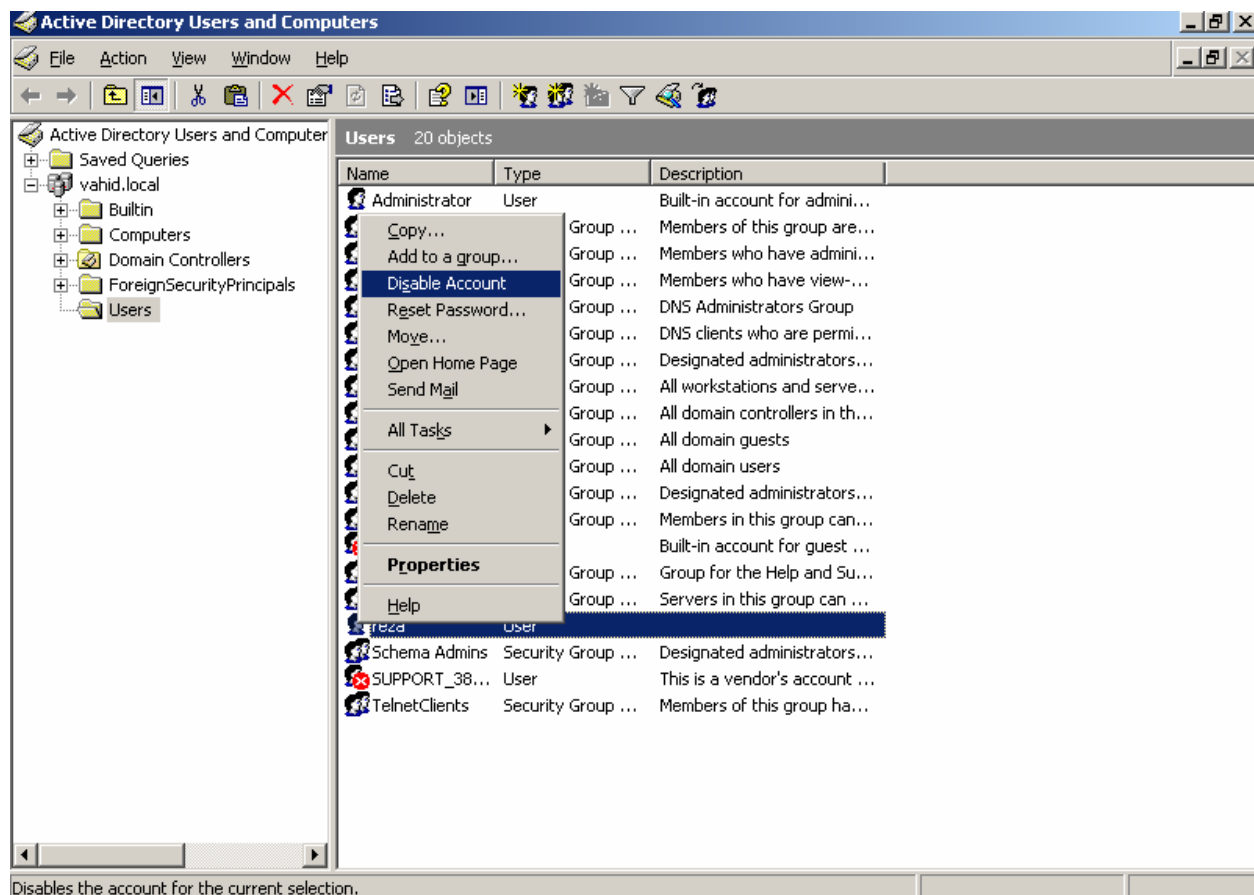
This dialog box, also titled "New Object - User", shows a summary of the user to be created. It includes a user icon and "Create in: VAHID.local/Users". A text area contains the following information: "When you click Finish, the following object will be created:", "Full name: reza", "User logon name: reza@VAHID.local", and "The user must change the password at next logon." At the bottom, the buttons are "< Back", "Finish", and "Cancel".

در پنجره زیر مشاهده می کنید که کاربری با نام Reza به لیست کاربران اضافه شده است.

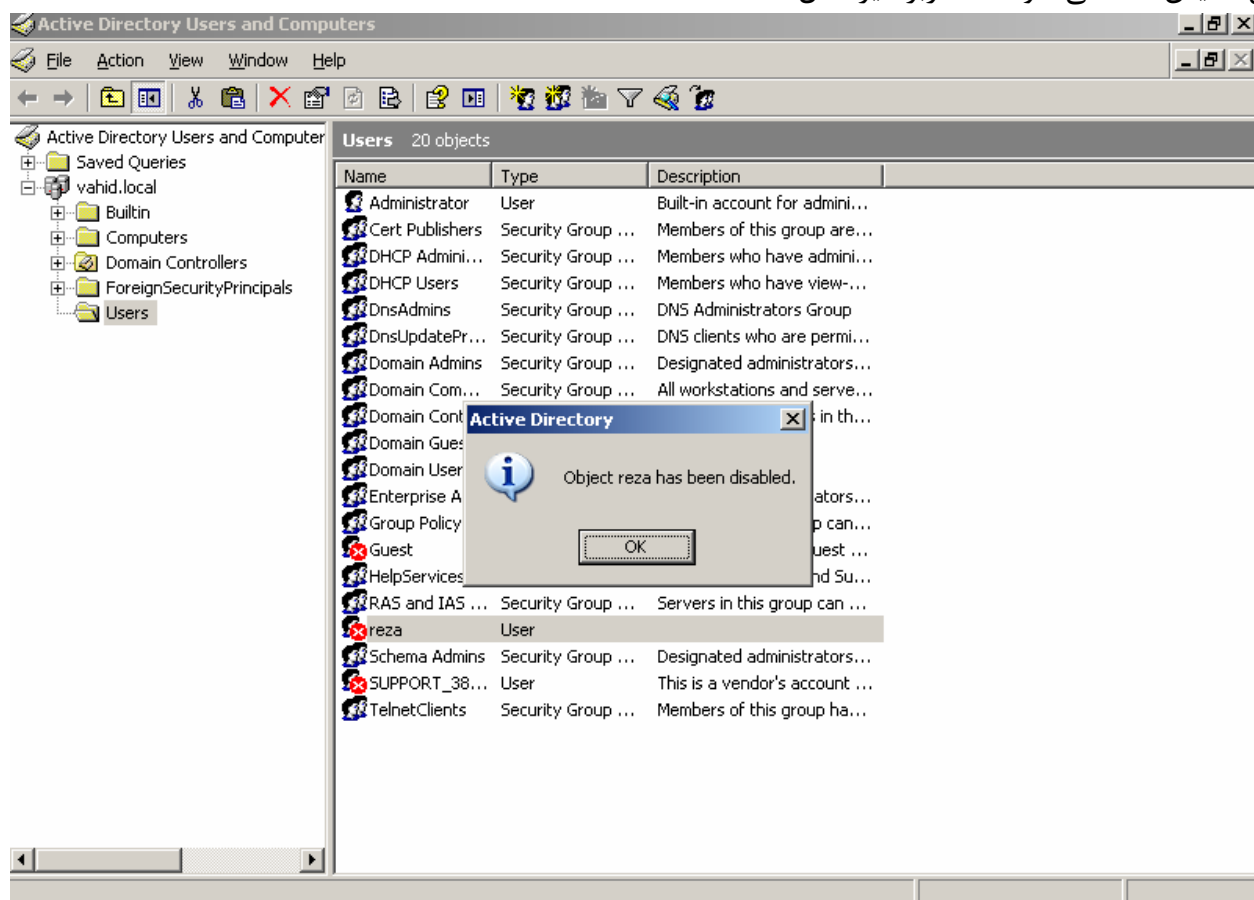


۲-۳-۴- بررسی قفل (lock) کردن کاربر:

اگر بخواهیم کاربری را به صورت موقت غیر فعال کنیم، برای این کار بر روی کاربر راست کلیک کرده و گزینه Disable Account انتخاب کنید.



پیغامی نمایش داده می شود که کاربر غیر فعال شد.



برای دوباره فعال کردن کاربر اگر بر روی کاربر راست کلیک کرده و Enable Account را انتخاب کنید کاربر دوباره فعال می شود.

۴-۴ - بررسی نحوه ورود از کلاینت:

بعد از اینکه کاربر ایجاد کردید اگر بخواهید از کلاینتی که با سرور Join است با نام کاربری وارد شوید در قسمت User name باید نام کاربری و در قسمت Password باید رمز کاربر را وارد نمایید.



بعد از وارد کردن نام کاربری ، رمز و کلیک بر روی ok برای ورود به دامنه ،این پنجره به این علت ظاهر شد که در تعریف کاربر و در قسمت رمز، گزینه User must change password at next logon انتخاب شده است یعنی باید در اولین باری که می خواهید با این نام کاربری به domain وصل شوید باید رمز کاربری خود را تغییر دهید در غیر اینصورت نخواهید توانست وارد دامنه شوید.



در قسمت New password رمز جدید و در قسمت Confirm New password تکرار رمز جدید را وارد کرده و ok کنید.



The screenshot shows the 'Change Password' dialog box in Windows Server 2003 Enterprise Edition. The dialog has a title bar 'Change Password' and a header with the Microsoft logo and 'Windows Server 2003 Enterprise Edition'. Below the header, it says 'Copyright © 1985-2003 Microsoft Corporation'. The main area contains five input fields: 'User name:' with 'reza', 'Log on to:' with a dropdown menu showing 'VAHID', 'Old Password:' with masked characters, 'New Password:' with masked characters, and 'Confirm New Password:' with masked characters. At the bottom right are 'OK' and 'Cancel' buttons.

پیغامی ظاهر می شود که رمز کاربری تغییر داده شد. با ok کردن آن وارد سیستم می شود و می توانید با نام کاربری از دامنه استفاده نمایید.




The screenshot shows the 'Change Password' dialog box with a confirmation message. A small dialog box is overlaid on top of the main dialog, containing an information icon and the text 'Your password has been changed.' with an 'OK' button. The main dialog box is partially obscured but still visible, showing the same fields as the previous screenshot.

۵-۴- مشاهده مشخصات کاربران و تغییر در آنها:

برای اینکه بتوانید مشخصات کاربری که ایجاد کرده اید را مشاهده کنید، در Active Directory User and Computer بر روی کاربر راست کلیک کرده و Properties را انتخاب کنید. پنجره زیر باز میشود که در آن می توانید مشخصات کاربران را مشاهده و تغییرات لازم را انجام دهید.

reza Properties [?] [X]

Member Of	Dial-in	Environment	Sessions
Remote control	Terminal Services Profile		COM+
General	Address	Account	Profile
	Telephones	Organization	

 reza

First name: Initials:

Last name:

Display name:

Description:

Office:

Telephone number:

E-mail:

Web page:

۱-۵-۴- محدود کردن زمان ورود کاربران:

بر روی زبانه Account و سپس بر روی Logon hours کلیک کنید.

reza Properties [?] [X]

Member Of | Dial-in | Environment | Sessions

Remote control | Terminal Services Profile | COM+

General | Address | Account | Profile | Telephones | Organization

User logon name:
 @

User logon name (pre-Windows 2000):

☐ Account is locked out

Account options:

☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Store password using reversible encryption

Account expires:

☒ Never

☐ End of:

این پنجره به شما نشان می دهد که این کاربر در چه ساعاتی از شبانه روز در یک هفته می تواند اجازه Logon به Domain را دارد. شما این محدودیت را به ازای هر شبانه روز و هر روز در هفته می توانید تعیین کنید. خانه هایی که به رنگ آبی پر شده اند بیانگر این می باشند که در آن ساعت و روز کاربر اجازه Logon کردن دارد.

Logon Hours for reza [X]

12 • 2 • 4 • 6 • 8 • 10 • 12 • 2 • 4 • 6 • 8 • 10 • 12

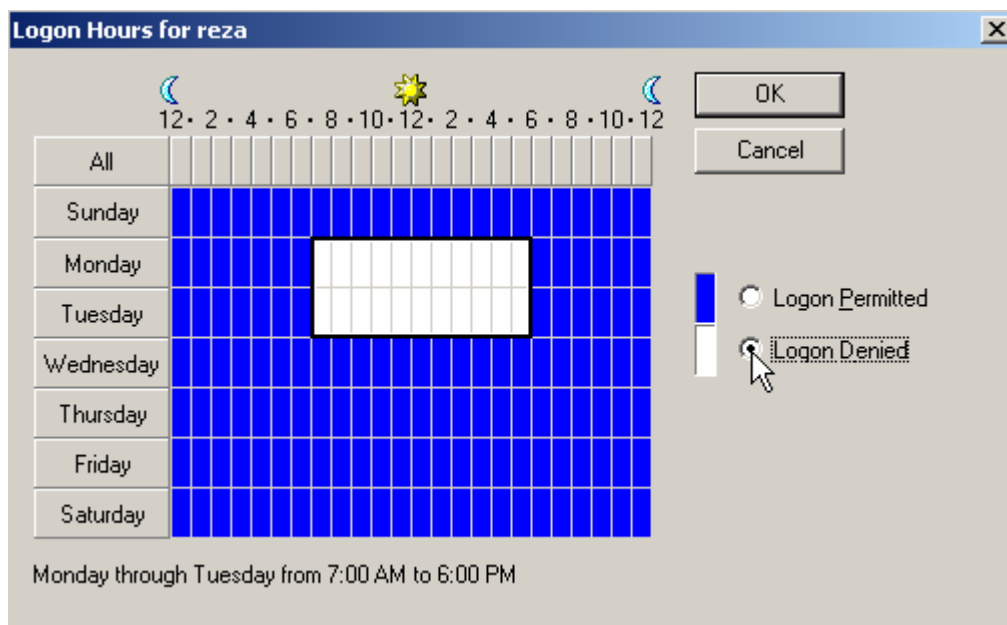
OK Cancel

All	12	2	4	6	8	10	12	2	4	6	8	10	12
Sunday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Monday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Tuesday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Wednesday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Thursday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Friday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Saturday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue

☒ Logon Permitted
☐ Logon Denied

Sunday from 12:00 AM to 1:00 AM

شما به راحتی می توانید با انتخاب یک خانه و یا Select کردن جمعی از خانه ها و با کلیک بر روی Logon Denied به رنگ سفید (به منزله اجازه ندادن برای Logon شدن) و یا با کلیک بر روی Logon Permitted به رنگ آبی (به منزله اجازه دادن برای Logon شدن) در آورید. که ما در اینجا با انتخاب قسمت پایین به کاربر اجازه نمی دهیم بین ساعات ۶ صبح تا ۷ بعدظهر روزهای دوشنبه و سه شنبه بتواند به دامنه وارد شود.



۲-۵-۴- محدود کردن ورود کاربران:

در زبانه Account ، بر روی Log On To کلیک کنید.

reza Properties

Member Of: Dial-in: Environment: Sessions:

Remote control: Terminal Services Profile: COM+:

General: Address: Account: Profile: Telephones: Organization:

User logon name:
 reza @vahid.local

User logon name (pre-Windows 2000):
 VAHID\ reza

Logon Hours... Log On To...

☐ Account is locked out

Account options:

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Store password using reversible encryption

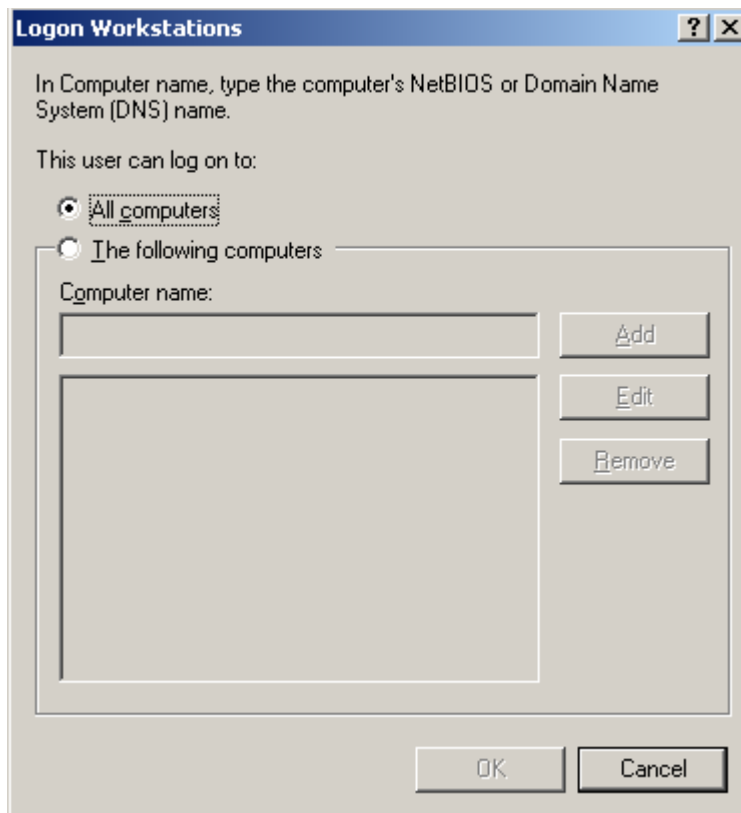
Account expires:

☒ Never

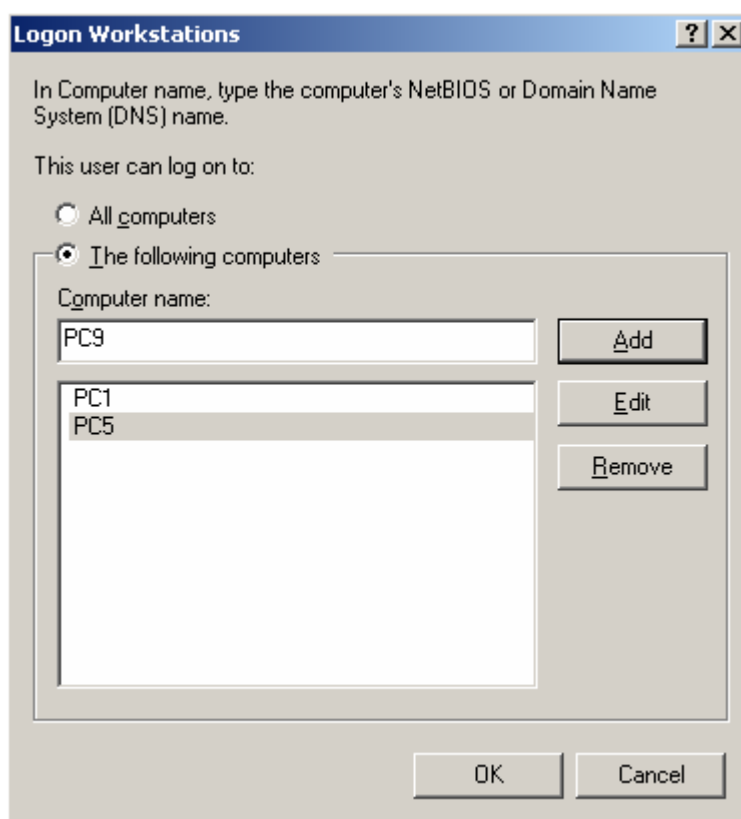
☐ End of: Wednesday, June 23, 2010

OK Cancel Apply

در این پنجره تنظیمات پیش فرض طوری تنظیم شده است که کاربر مربوط، از روی هر کامپیوتری که به Domain وصل باشد می تواند Logon شود. شما با انتخاب گزینه The following computers می توانید کاربر را محدود کنید تا کاربر از روی همان کامپیوترهایی که مد نظر شما است فقط بتواند Logon کند.



برای انجام این کار بر روی The following computers کلیک کرده، سپس در قسمت Computer name اسامی کامپیوترها را نوشته و بر روی Add کلیک کنید.



۳-۵-۴- محدودیت زمانی برای فعال بودن کاربر:

در پایین زبانه Account در بخش Account expires شما می توانید محدودیت زمانی برای فعال بودن کاربر تعریف نمایید. تنظیم پیش فرض این بخش روی گزینه Never می باشد. بدین معنی که اعتبار این کاربر منقضی نخواهد شد.

The image shows a Windows XP-style dialog box titled "reza Properties". It has several tabs: "Member Of", "Dial-in", "Environment", "Sessions", "Remote control", "Terminal Services Profile", "COM+", "General", "Address", "Account", "Profile", "Telephones", and "Organization". The "Account" tab is currently selected. Inside this tab, there are fields for "User logon name:" (containing "reza" and "@vahid.local" in a dropdown) and "User logon name (pre-Windows 2000):" (containing "VAHID\" and "reza"). Below these are buttons for "Logon Hours..." and "Log On To...". There is a checkbox for "Account is locked out" which is unchecked. Under "Account options:", there is a list box containing four items, all with unchecked checkboxes: "User must change password at next logon", "User cannot change password", "Password never expires", and "Store password using reversible encryption". At the bottom of the dialog, there is a section for "Account expires" with two radio buttons: "Never" (which is selected) and "End of:" (which is unselected). Next to "End of:" is a date dropdown menu showing "Wednesday, June 23, 2010". At the very bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

با انتخاب گزینه End of و انتخاب تاریخ از لیست و تقویم مقابل می توانید تاریخ انقضاء برای کاربر تعریف کنید.

reza Properties [?] [X]

Member Of: Dial-in: Environment: Sessions:

Remote control: Terminal Services Profile: COM+:

General: Address: Account: Profile: Telephones: Organization:

User login name: reza @vahid.local

User login name (pre-Windows 2000): VAHID\ reza

Logon Hours... Log On To...

☐ Account is locked out

Account options:

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Store password

Account expires:

☐ Never

☒ End of: Wednesday, June 23, 2010

Calendar: June, 2010

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

Today: 5/24/2010

OK Cancel Apply

۴-۵-۴- اجازه ورود کاربران از راه دور به سیستم :

در زبانه Dial-in گزینه هایی وجود دارد که با فعال کردن آنها می توانید اجازه ورود به سیستم از راه دور را به کاربر دهید.

reza Properties [?] [X]

Remote control		Terminal Services Profile		COM+	
General	Address	Account	Profile	Telephones	Organization
Member Of		Dial-in	Environment	Sessions	

Remote Access Permission (Dial-in or VPN)

☐ Allow access
☒ Deny access
☐ Control access through Remote Access Policy

☐ Verify Caller-ID:

Callback Options

☒ No Callback
☐ Set by Caller (Routing and Remote Access Service only)
☐ Always Callback to:

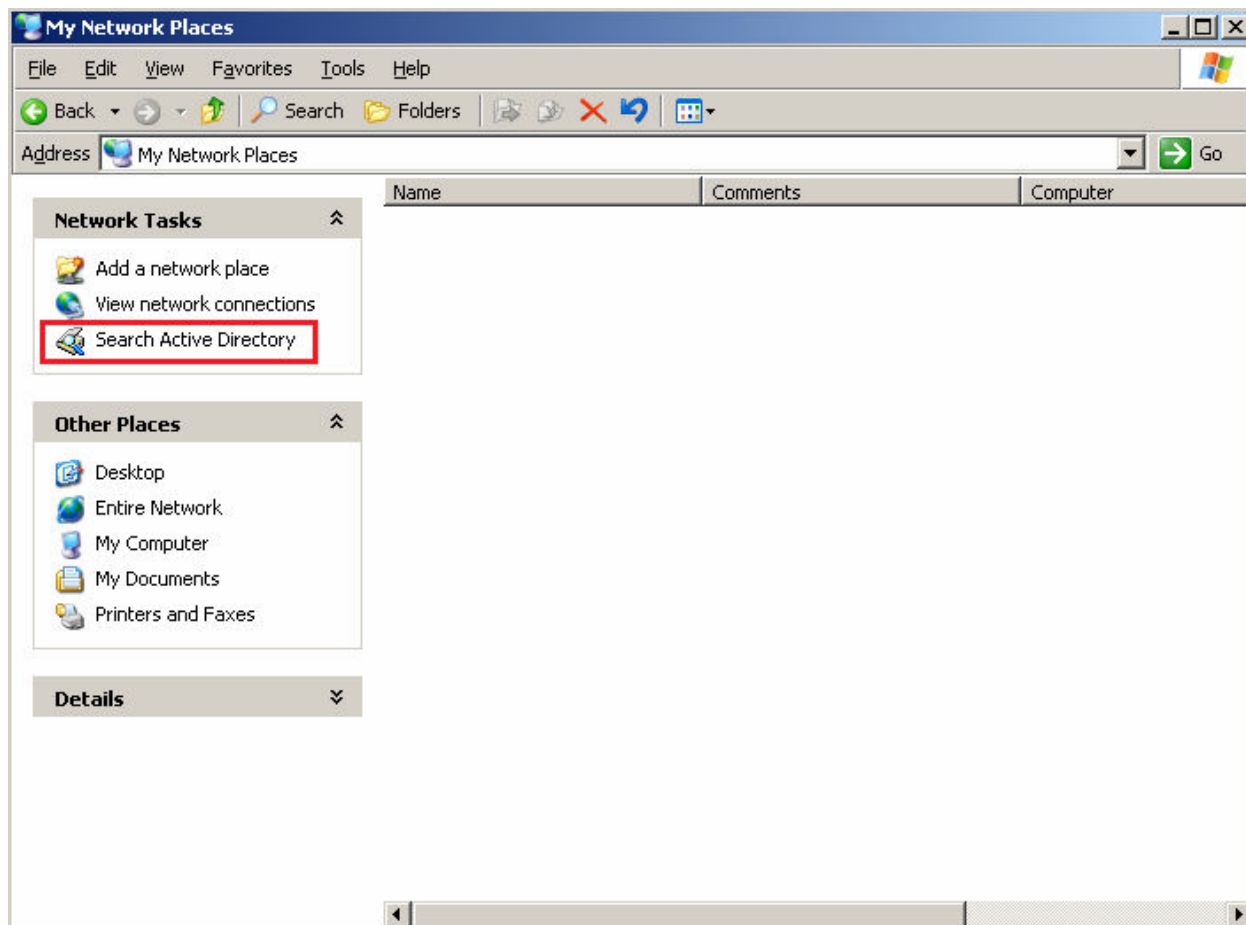
☐ Assign a Static IP Address

☐ Apply Static Routes

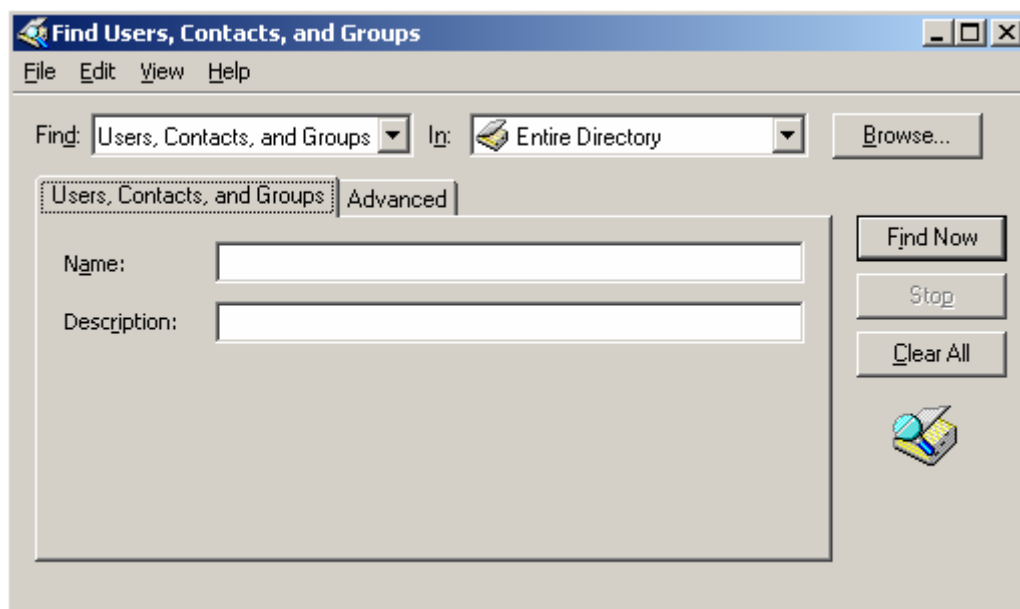
Define routes to enable for this Dial-in connection.

۶-۴- جستجو در AD:

اگر بخواهید در سطح AD جستجو کنید برای این کار این مراحل را انجام دهید:
 در پنجره My Network Places بر روی Search Active Directory کلیک کنید.



پنجره زیر نمایش داده می شود که می توانید تنظیمات آن را بر حسب نیازتان انجام دهید.



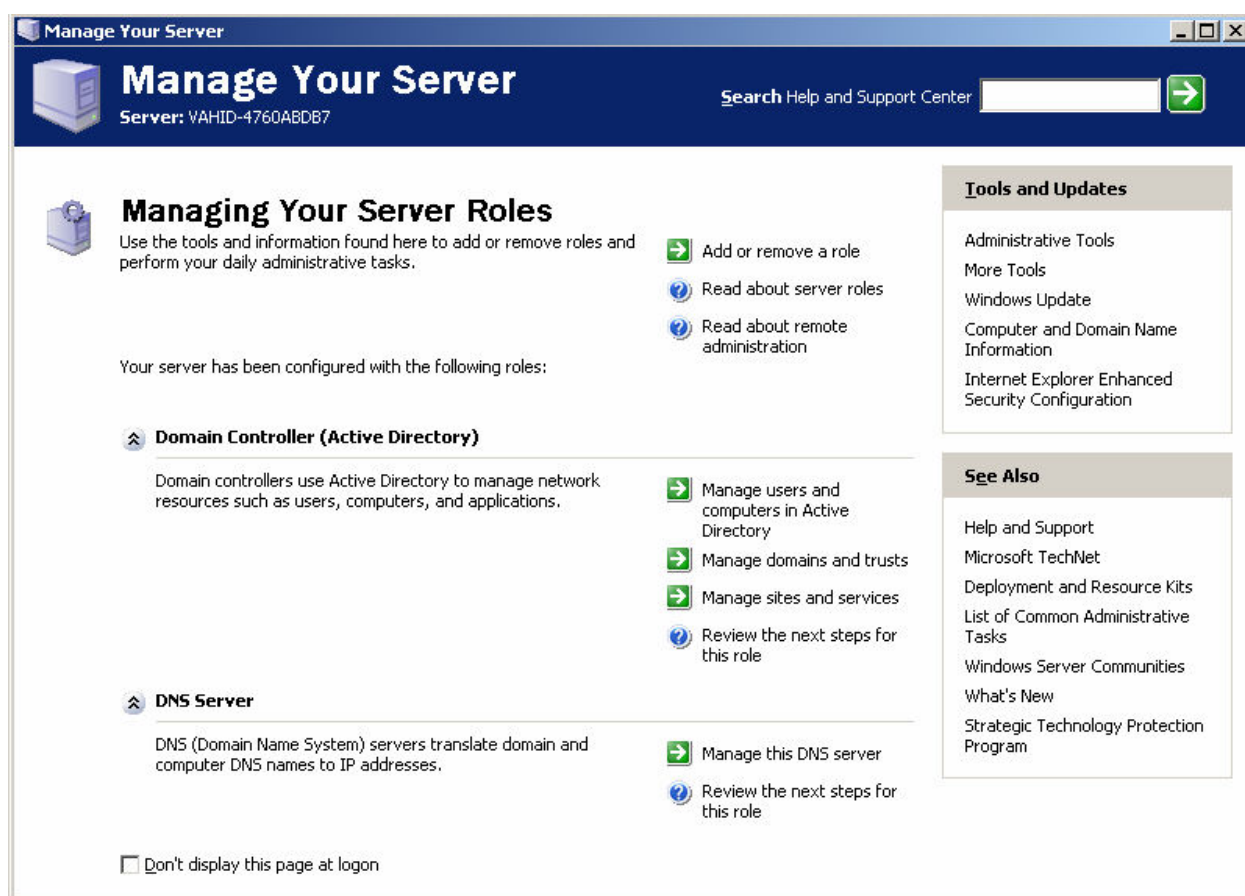
۵. جزئیات بخش پنجم:

۱-۵- نصب فایل سرور:

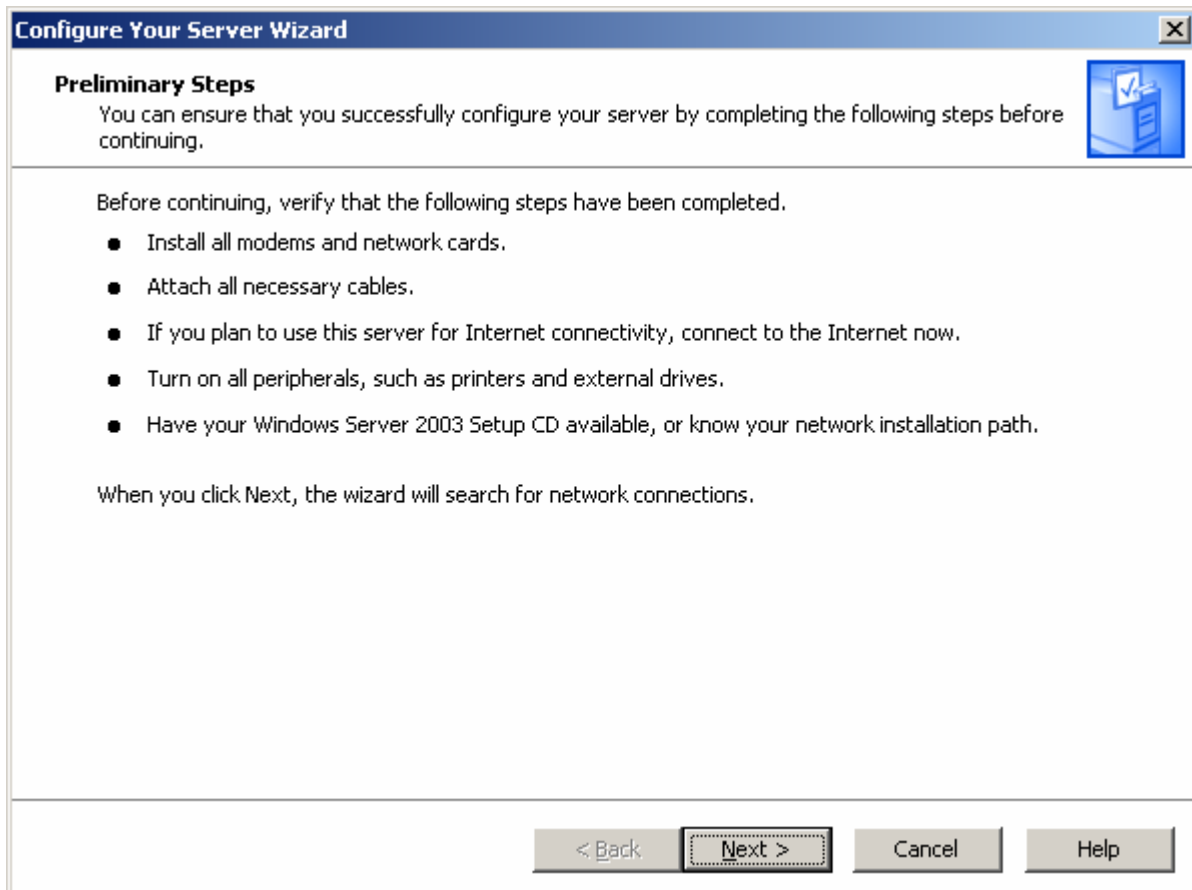
فایل سرور برای ذخیره داده ها یا فایل های کاربران شبکه (Quota) و یا برای اشتراک قایل های خاص بین کاربران شبکه (Sharing) مورد استفاده قرار می گیرد.

برای نصب فایل سرور این مراحل را انجام دهید:

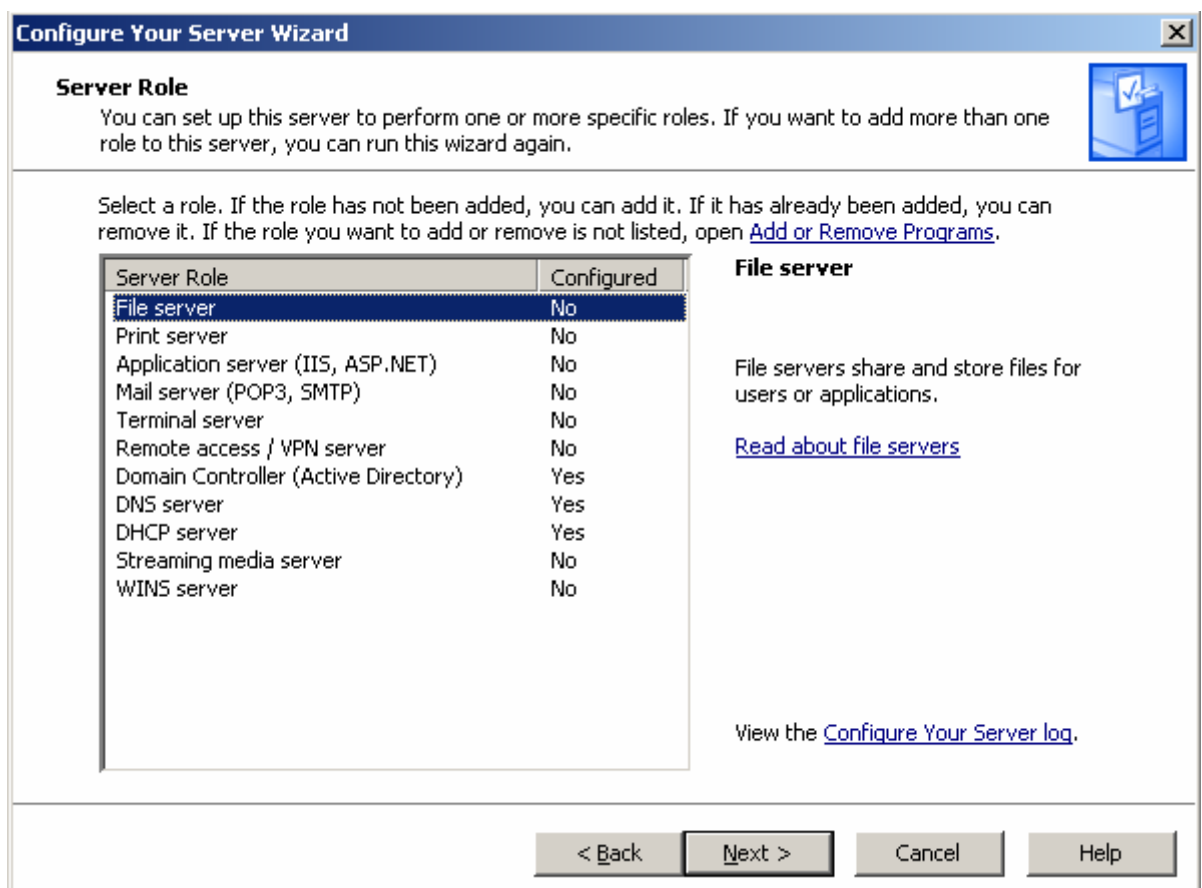
۱- در پنجره Manage Your Server بر روی Add or remove a role کلیک کنید.



۲- روی دکمه Next کلیک کنید.



۳- در این پنجره بر روی File Server کلیک کرده سپس بر روی Next کلیک کنید.



۴- این پنجره مربوط به تنظیمات Disk Quota می باشد که اگر تیک گزینه Set up default disk quota را انتخاب کنید می توانید میزان فضای استفاده کاربران را محدود کنید. در صورتی که این کار انجام ندهید کاربران می توانند داخل پوشه مخصوص خود روی سرور بدون محدودیت (البته اندازه ظرفیت درایوی که پوشه های کاربران داخل آن است) اطلاعات ذخیره نماید. توجه داشته باشید که در این قسمت میزان فضایی که مشخص می کنید برای کل کاربران یکسان در نظر گرفته می شود. اگر بخواهید برای عده ای از کاربران میزان فضا را تغییر دهید مراحل انجام این کار را در قسمت تنظیمات مربوط به Disk quota خواهیم گفت.

گزینه Set up default disk quota را انتخاب می کنیم تا گزینه های پایین فعال شود:

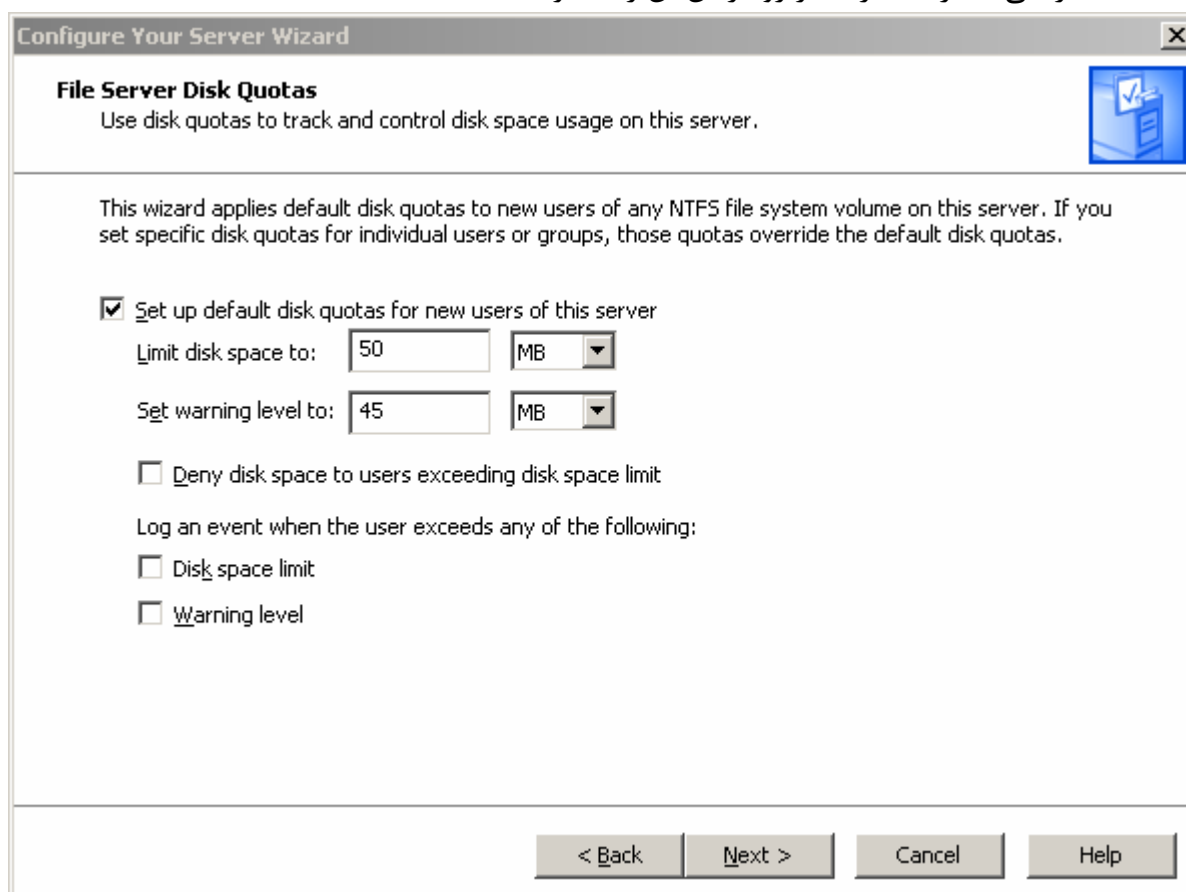
Limit disk space to: در این قسمت باید میزان فضایی را که می خواهید برای کاربران در نظر بگیرید را مشخص کنید.

Set warning level to: در این قسمت میزان فضایی را مشخص می کنید که بعد از رسیدن هر کاربر به آن مقدار فضا، پیغامی برای آن کاربر ارسال می شود که نشان دهنده نزدیک شدن به پایان میزان فضای قابل دسترسی کاربر است.

Deny disk space to user exceeding disk space limit: با قرار دادن تیک این گزینه، دیگر محدودیت فضا برای کاربران در نظر گرفته نخواهد شد و وقتی از فضای تعیین شده بالاتر روند فقط به آنها پیغام داده خواهد شد. اگر این گزینه را تیک دار نکید کاربر نمی تواند بعد از پر شدن فضای تعیین شده فایل ذخیره نماید.

Disk space limit: قرار دادن تیک این گزینه یعنی ثبت شود کاربر در کدام زمان از فضا استفاده کرده است.

Warning level: زمانی که از هشدار بالاتر رود زمان آن را ذخیره کند.



Configure Your Server Wizard

File Server Disk Quotas
Use disk quotas to track and control disk space usage on this server.

This wizard applies default disk quotas to new users of any NTFS file system volume on this server. If you set specific disk quotas for individual users or groups, those quotas override the default disk quotas.

☒ **S**et up default disk quotas for new users of this server

Limit disk space to: MB

Set warning level to: MB

☐ **D**eny disk space to users exceeding disk space limit

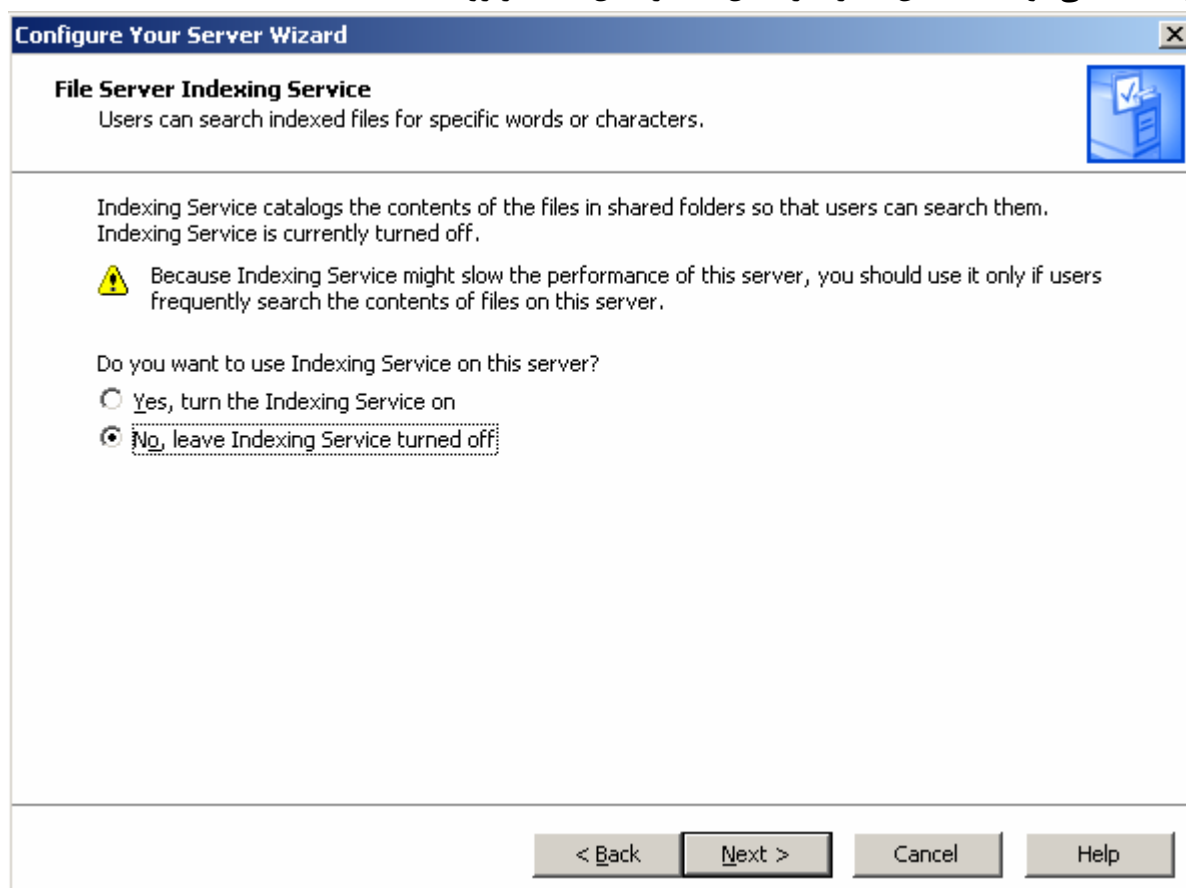
Log an event when the user exceeds any of the following:

☐ **D**isk space limit

☐ **W**arning level

< Back Next > Cancel Help


۵- در این صفحه می توانید شاخص گذاری را فعال یا غیر فعال کنید. بر روی Next کلیک کنید.



Configure Your Server Wizard

File Server Indexing Service
Users can search indexed files for specific words or characters.

Indexing Service catalogs the contents of the files in shared folders so that users can search them. Indexing Service is currently turned off.

 Because Indexing Service might slow the performance of this server, you should use it only if users frequently search the contents of files on this server.

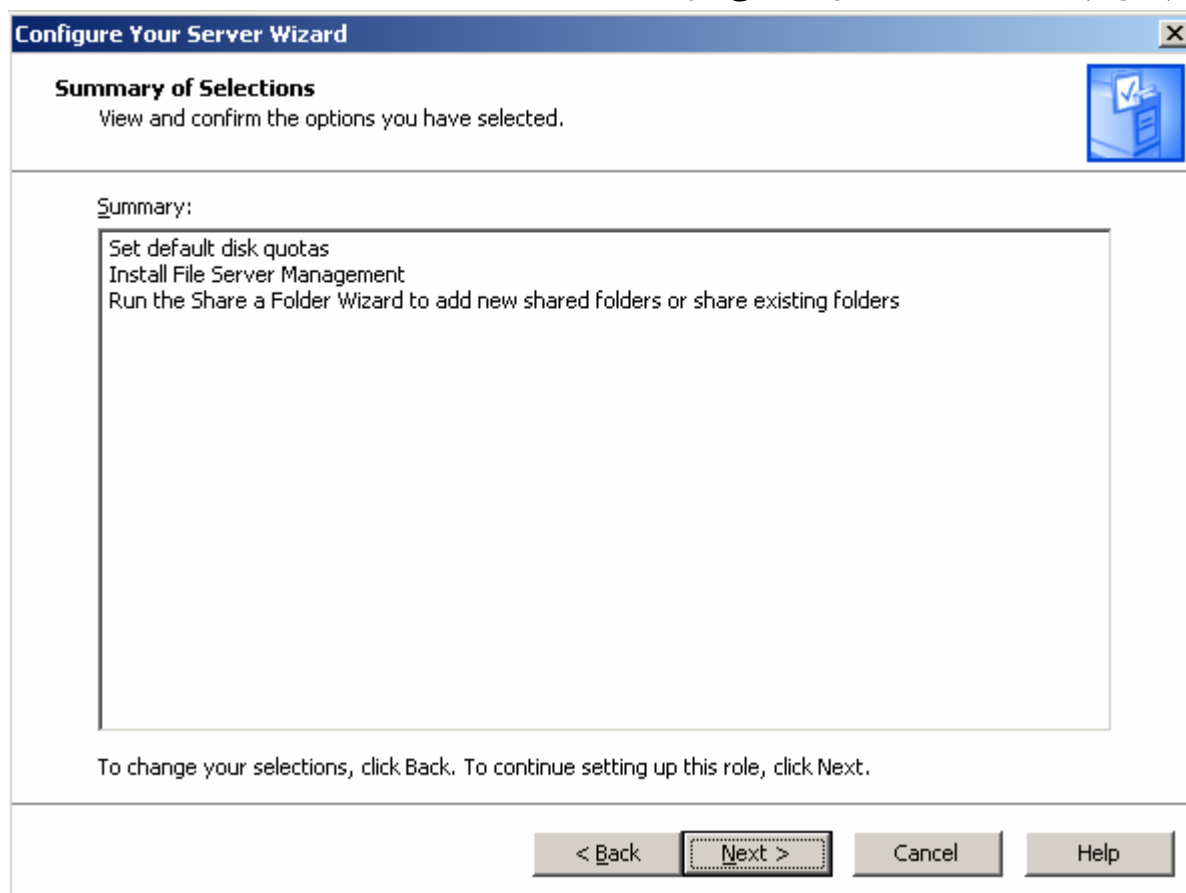
Do you want to use Indexing Service on this server?

☐ **Y**es, turn the Indexing Service on

☒ **N**o, leave Indexing Service turned off

< Back Next > Cancel Help

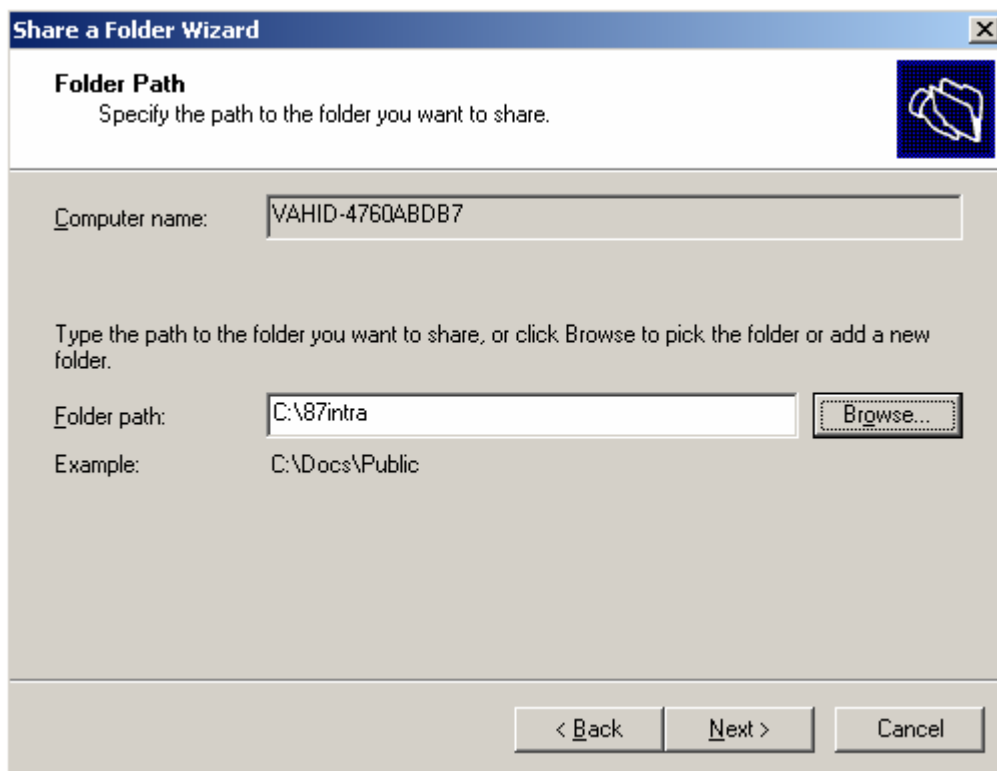
۶- در این پنجره چکیده تنظیمات نمایش داده می شود.



۷- پنجره خوش آمد گویی برای اشتراک گذاری فایل نمایش داده می شود.



۸- در قسمت Folder path باید مسیر فولدري را که می خواهید فایل های اشتراکی کاربران در آنجا نگهداری شود را انتخاب نمایید.



Share a Folder Wizard

Folder Path
Specify the path to the folder you want to share.

Computer name: VAHID-476QABDB7

Type the path to the folder you want to share, or click Browse to pick the folder or add a new folder.

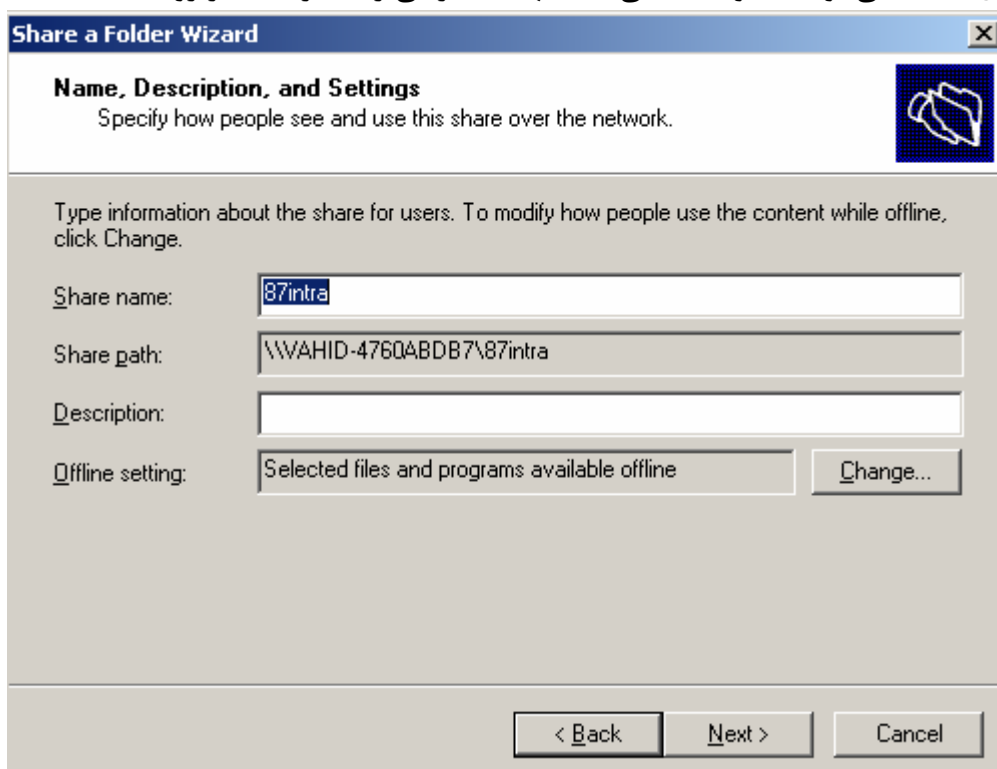
Folder path: C:\87intra Browse...

Example: C:\Docs\Public

< Back Next > Cancel

اگر بخواهید فولدر اشتراکی مورد نظر برای کاربران با نام خاصی نمایش داده شود می توانید در قسمت Share name نام دلخواه خود را وارد کنید تا کاربران فولدر را با آن نام ببینند.

با کلیک بر روی Change می توانید نحوه دستیابی به فایل‌های اشتراکی را تغییر دهید. بر روی Next کلیک کنید.



Share a Folder Wizard

Name, Description, and Settings
Specify how people see and use this share over the network.

Type information about the share for users. To modify how people use the content while offline, click Change.

Share name: 87intra

Share path: \\VAHID-476QABDB7\87intra

Description:

Offline setting: Selected files and programs available offline Change...

< Back Next > Cancel

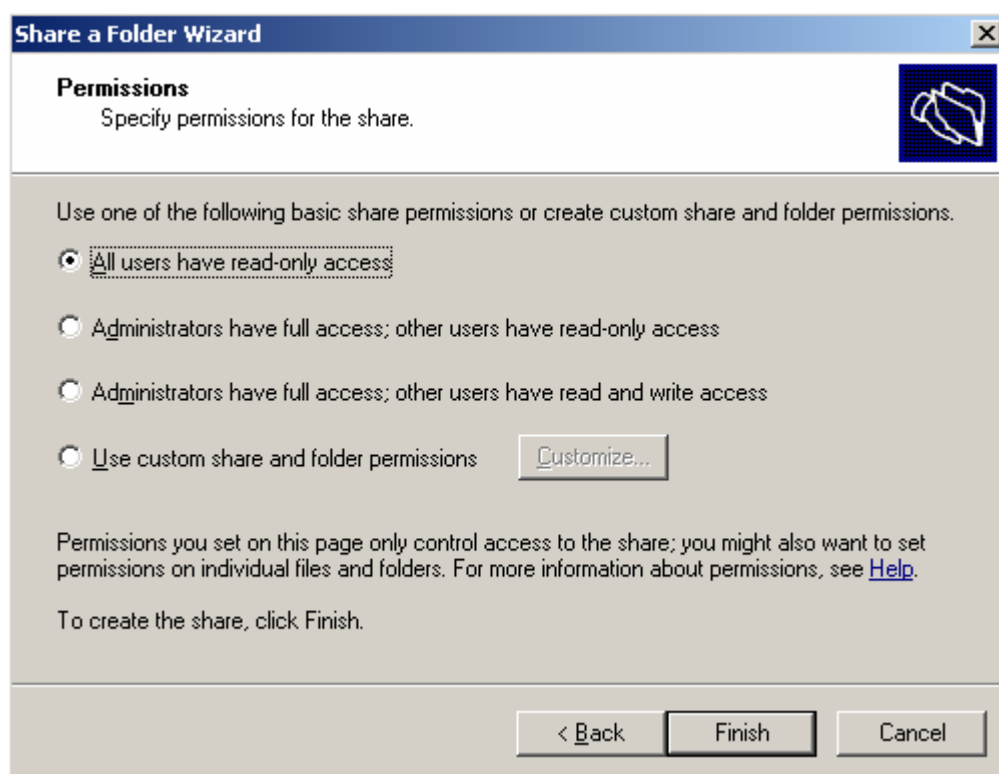
۹- این گزینه ها مربوط به مجوز دستیابی به پوشه ها می باشد:

All users have read-only access: مجوز همه کاربران فقط برای خواندن.

Administrators have full access; other users have read-only access: مدیران می توانند کاملاً دستیابی داشته باشند، کاربران فقط اجازه خواندن دارند.

Administrators have full access; other users have read and write access: مدیران می توانند کامل دستیابی داشته باشند، کاربران می توانند بخوانند و هم بنویسند.

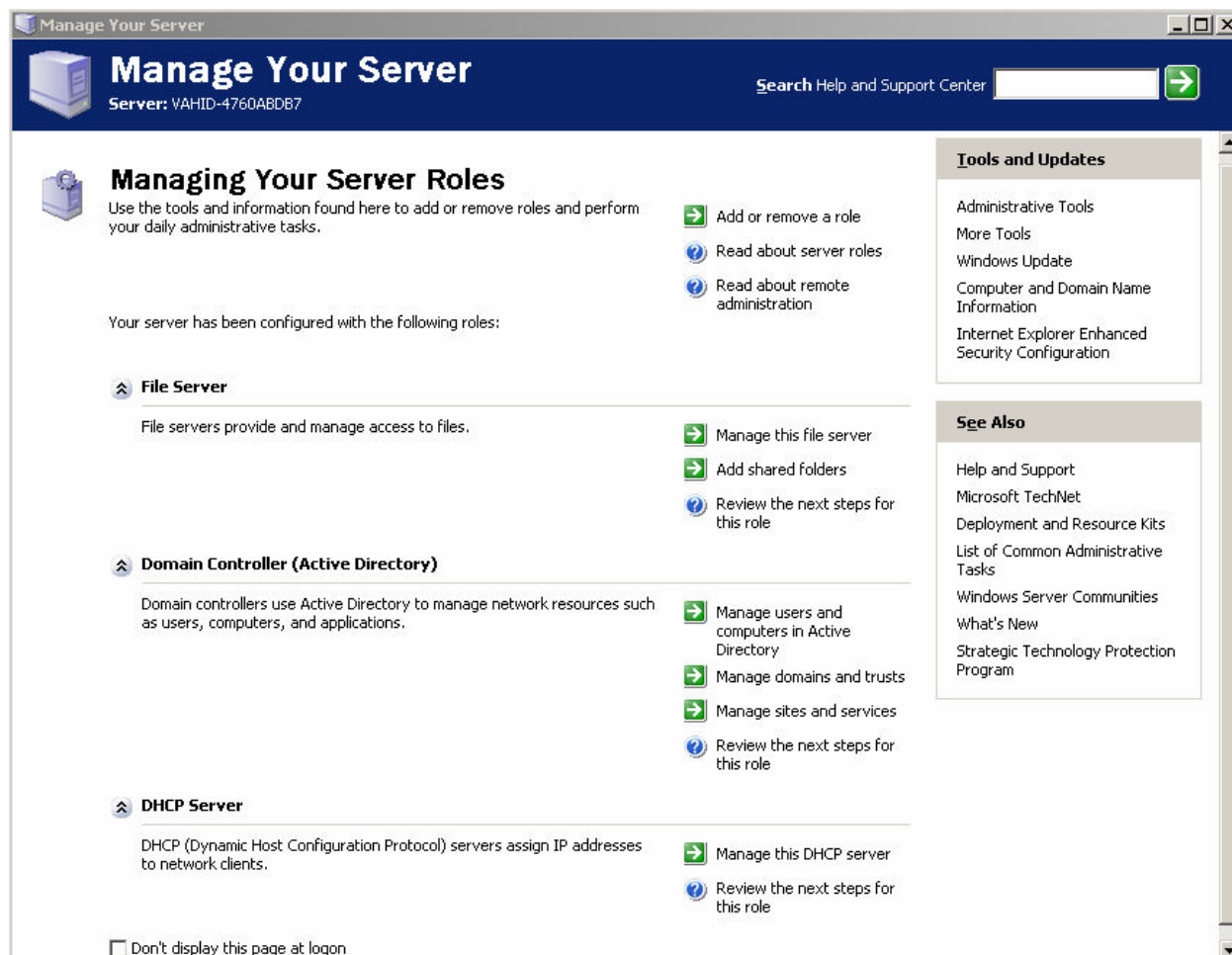
Use custom share and folder permissions: می توانید با انتخاب این گزینه می توانید تنظیمات مجوز دستیابی را به صورت دستی انجام دهید.



۱۰- در این صفحه توضیح داده میشود که این سرور هم اکنون به عنوان فایل سرور شناخته می شود.



۱۱- در این صفحه نیز مشاهده می کنید که نقش File Server به سرور داده شده است.



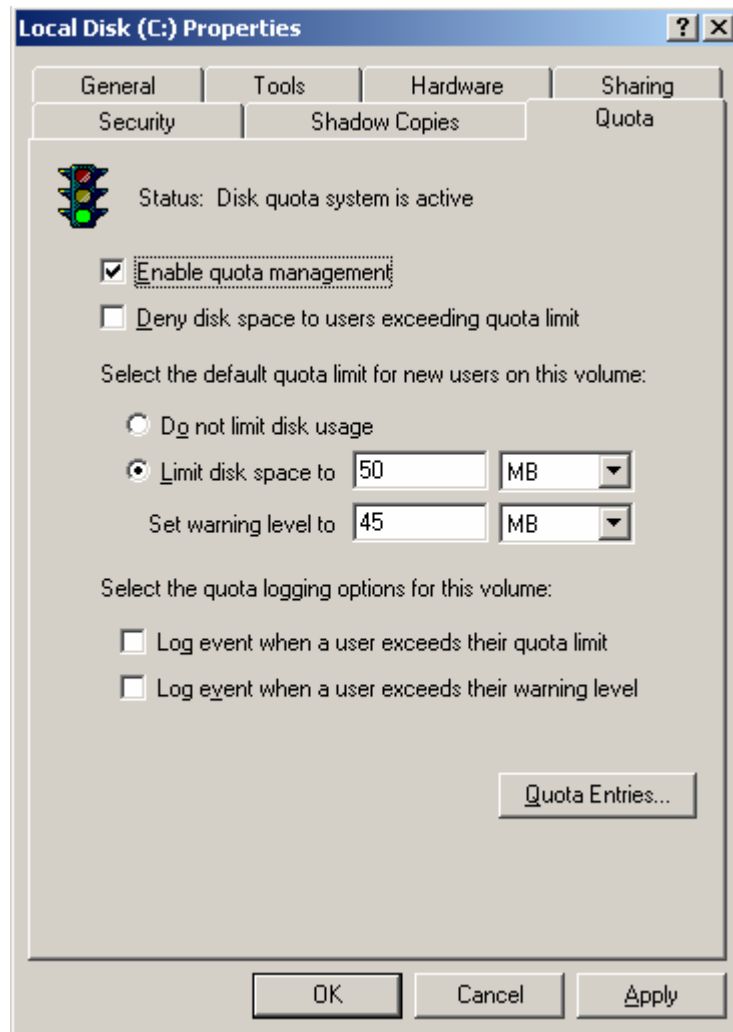
۲-۵- تنظیمات Disk Quota در ویندوز ۲۰۰۳ سرور:

همانطور که قبلاً گفتیم از Disk Quota برای محدود کردن فضای استفاده کاربران از حافظه سرور استفاده می شود. در صورتی که این کار را انجام ندهید کاربران می توانند داخل پوشه مخصوص خود روی سرور بدون محدودیت (البته اندازه ظرفیت درایوی که پوشه های کاربران داخل آن است) اطلاعات ذخیره نماید. در تنظیمات Disk Quota می توانید برای هر کاربری که خواستید می توانید فضای بیشتری اختصاص دهید. مورد های استفاده این بخش بیشتر در مورد میزبانی سایت های اینترنتی می باشد به طور مثال برای تخصیص فضای یک وب سایت از یک سرور آنلاین از این امکانات چه در ویندوز و چه در سرور های لینوکس استفاده می نماییم نرم افزار های مختلفی نیز برای تنظیم این بخش در سرور های مختلف ارائه شده اند.

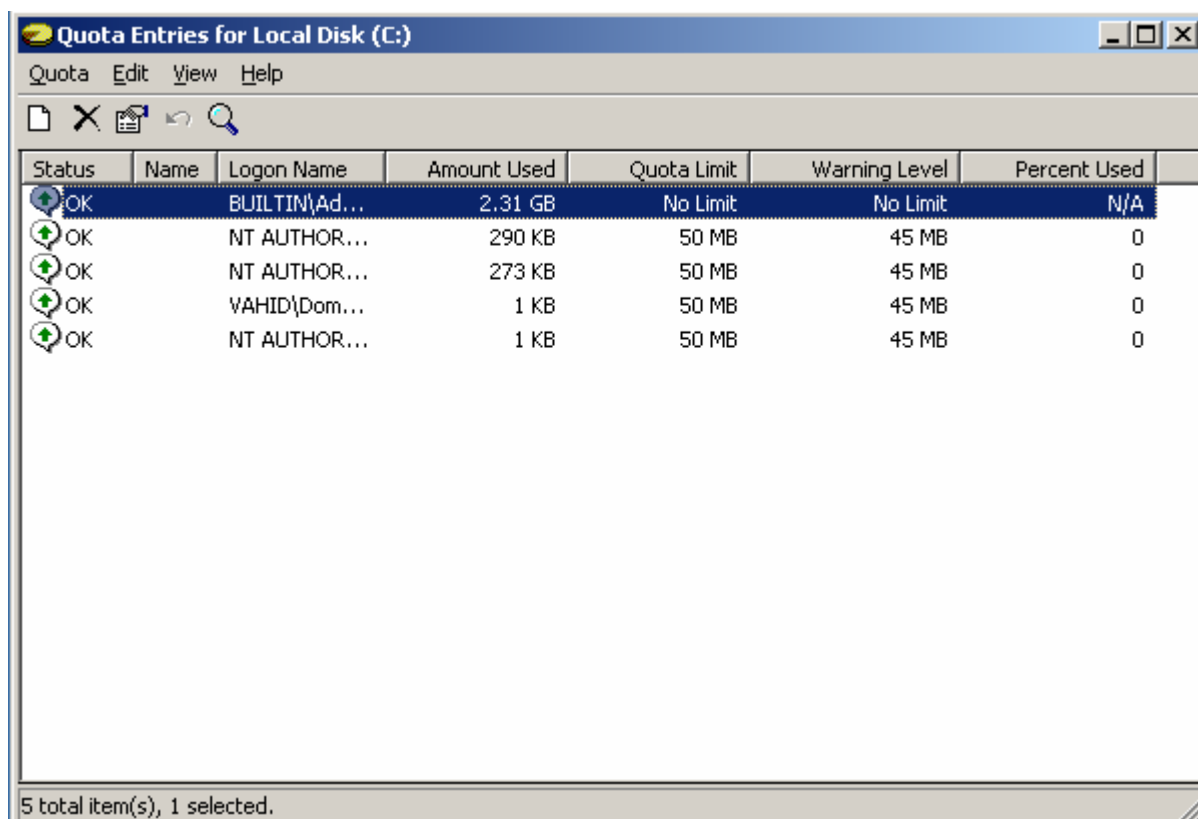
برای محدود کردن فضای دسترسی کاربران این مراحل را انجام دهید:

۱- در My Computer بر روی یکی از درایوها که می خواهید تنظیمات Disk Quota را بر روی آن انجام دهید راست کلیک کرده و بر روی زبانه Quota کلیک کنید. توجه داشته باشید که هنگام نصب فایل سرور تنظیمات Disk Quota را فعال و برای همه کاربران 50MB فضا اختصاص داده ایم که اگر خواستید می توانید این فضا را افزایش دهید. (اگر هنگام

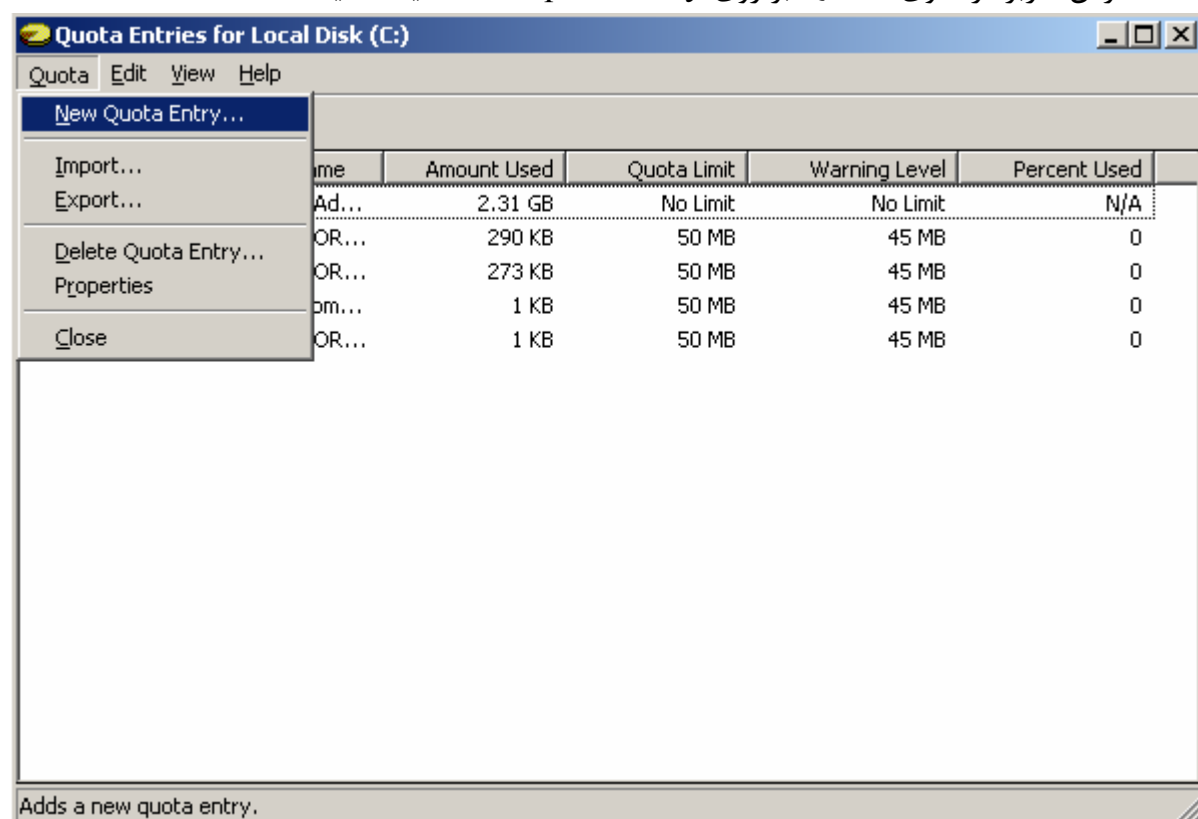
نصب فایل سرور تنظیمات Disk Quota را انجام نمی دادیم این صفحه غیر فعال خواهد بود که با قرار دادن تیک Enable Quota management می توانستیم این صفحه را فعال کنیم)



۲- همچنان که می دانید فضای داده شده در بالا برای همه کاربران یکسان می باشد حال فرض کنید می خواهیم به کاربر خاصی میزان فضای بیشتری را در نظر بگیریم. برای این کار بر روی Quota Entries کلیک کنید تا پنجره زیر ظاهر شود. در این صفحه مشاهده می کنید که برای مدیر یا Admin به صورت پیش فرض داده ای فضای نامحدود (No Limit) در نظر گرفته می شود. برای کاربران پیش فرض 50MB فضا اختصاص داده شده برای اینکه بتوانید به کاربری در شبکه، مقدار فضای اختصاص داده شده به آن را تغییر دهید، باید آن را به /این لیست/ اضافه نمایید.



۳- برای اضافه کردن کاربر، از منوی Quota بر روی New quota entry کلیک کنید.



۴- این پنجره نمایش داده می شود که اگر نام User را می دانید با تایپ کردن آن در قسمت Enter the object names to select و OK کردن، آن را به لیست Quota Entries اضافه کنید.

۵- اگر نام آن را دقیق نمی دانید بر روی **Advanced** کلیک کنید. این پنجره نمایش داده می شود.

Name (RDN)	E-Mail Address	In Folder

۶- بر روی **Find Now** کلیک کنید تا لیست کاربران موجود را نمایش دهد. و با دوبار کلیک بر روی کاربر، آن را انتخاب کنید.

Select Users [?] [X]

Select this object type:

From this location:

Common Queries

Name:

Description:

☐ Disabled accounts
☐ Non expiring password

Days since last login:

Search results:

Name (RDN)	E-Mail Address	In Folder
Administrator		vahid.local/Users
ali		vahid.local/Users
Guest		vahid.local/Users
model		vahid.local/87intra
mohsen amiri		vahid.local/87intra
reza		vahid.local/Users
SUPPORT_3...		vahid.local/Users

۷- کاربری که انتخاب کرده اید در این صفحه دیده می شود.

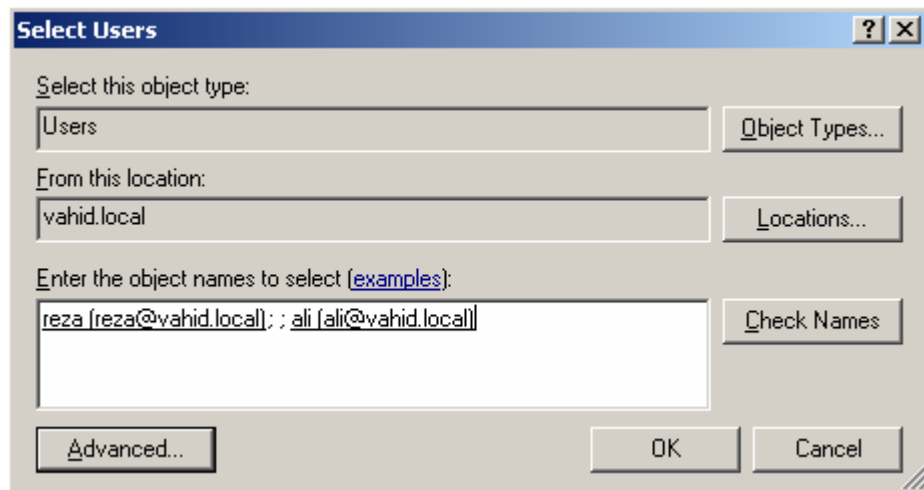
Select Users [?] [X]

Select this object type:

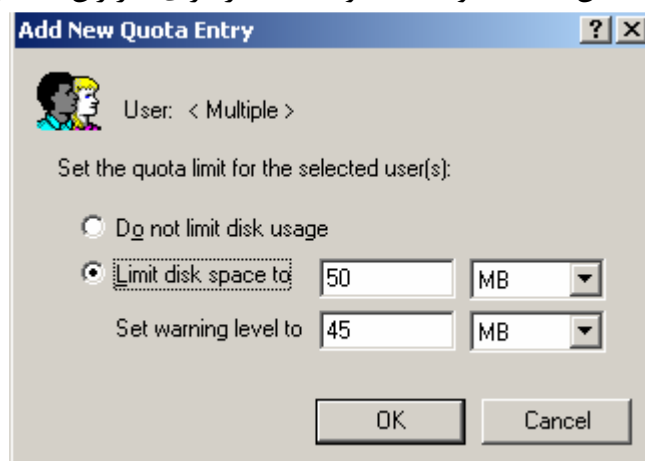
From this location:

Enter the object names to select (examples):

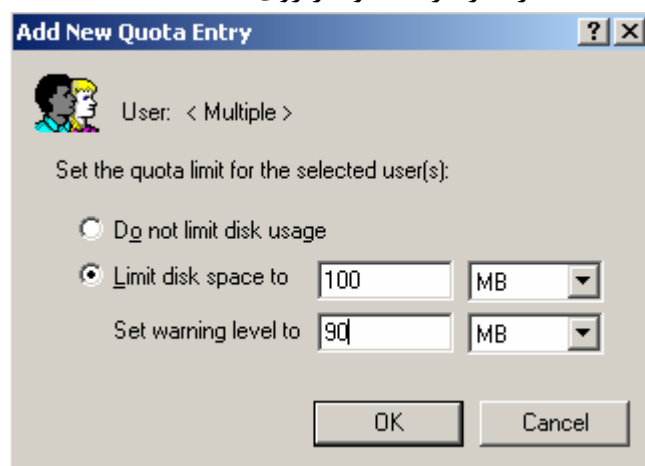
۸- اگر خواستید کاربر دیگری را نیز انتخاب کنید دوباره بر روی **Advanced** کلیک و کاربر را انتخاب کنید. به این لیست اضافه می شود. بعد از انتخاب کاربران بر روی **OK** کلیک کنید.



۹- در این صفحه شما می توانید مقدار فضا را برای کاربرهایی که انتخاب کرده اید تغییر دهید: Do not limit disk usage: با انتخاب این گزینه، محدودیت فضا برای این کاربران در نظر گرفته نمی شود. Limit disk space to: با انتخاب این تیک می توانید محدودیت فضا را برای کاربران انتخابی تغییر دهید.



۱۰- مثلاً برای این کاربران 100MB فضا در نظر گرفته شود. بر روی OK کلیک کنید.



۱۱- در این پنجره می بینید کاربرانی با نام های Reza و Ali به لیست اضافه شده است و برای آنها ۱۰۰MB فضا در نظر گرفته شده است.

Status	Name	Logon Name	Amount Used	Quota Limit	Warning Level	Percent Used
OK	ali	ali@vahid.local	0 bytes	100 MB	90 MB	0
OK	reza	reza@vahid...	0 bytes	100 MB	90 MB	0
OK	BUILTIN\Ad...		2.31 GB	No Limit	No Limit	N/A
OK	NT AUTHOR...		290 KB	50 MB	45 MB	0
OK	NT AUTHOR...		273 KB	50 MB	45 MB	0
OK	VAHID\Dom...		1 KB	50 MB	45 MB	0
OK	NT AUTHOR...		1 KB	50 MB	45 MB	0

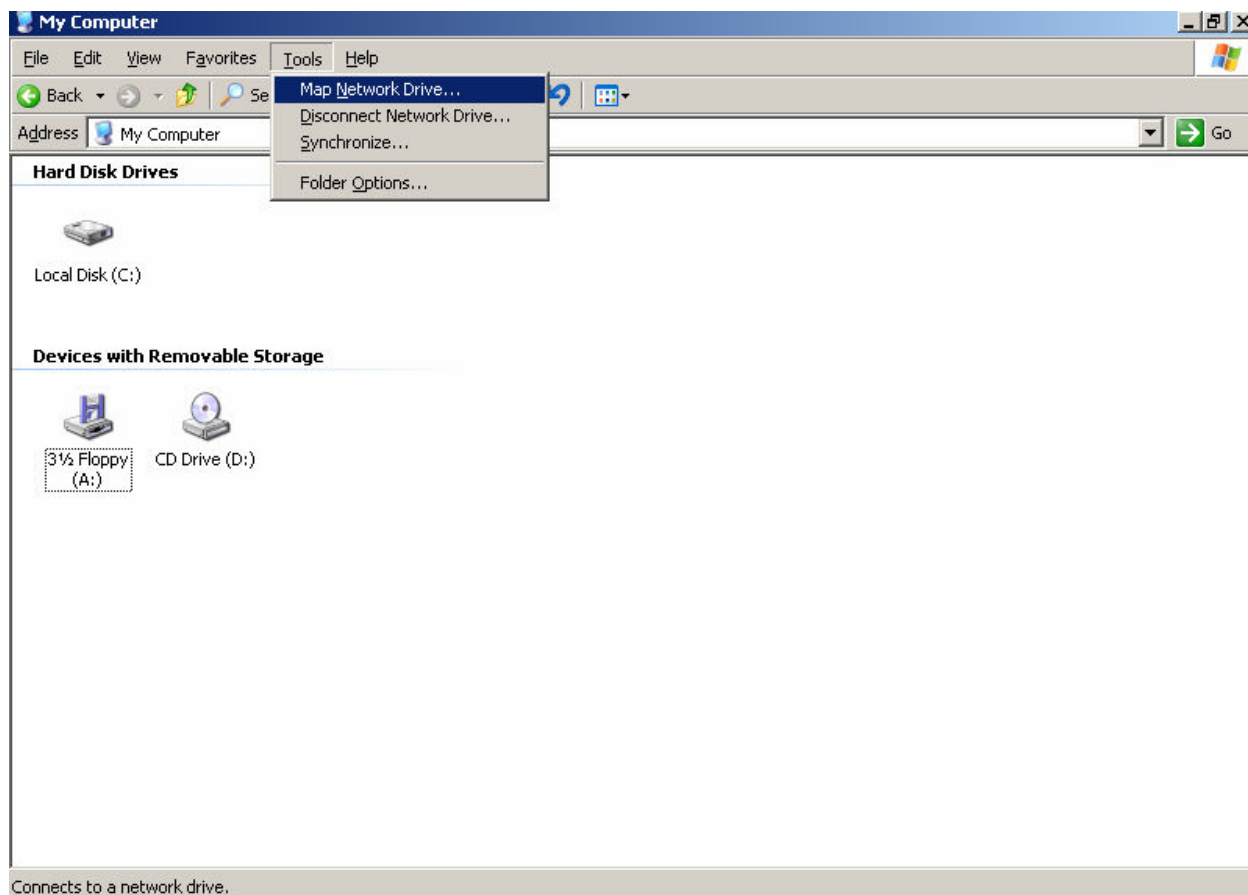
7 total item(s), 1 selected.

۳-۵- دستیابی آسان به پوشه اشتراکی (Map Network Drive):

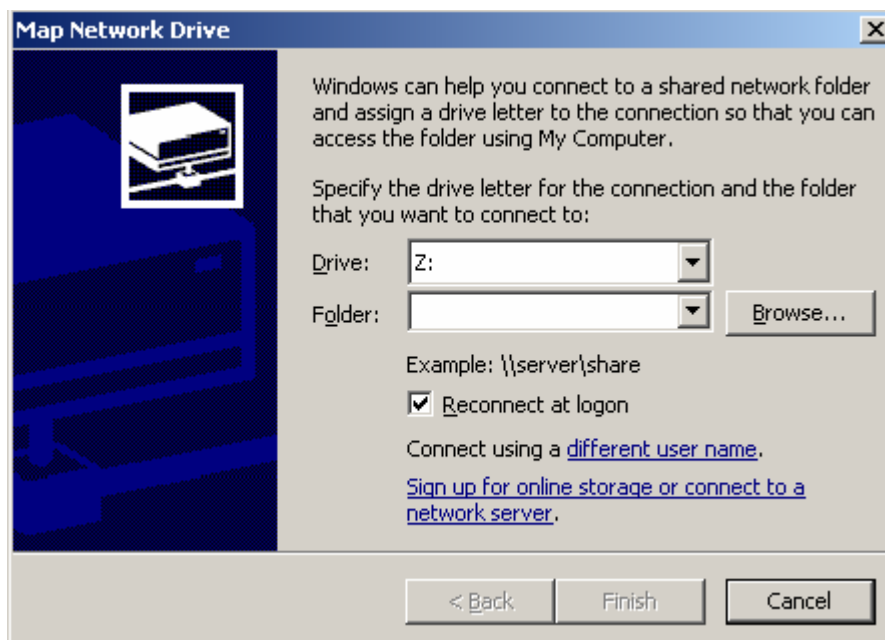
برای این که کاربر وقتی به سرور وصل میشود بتواند به پوشه اشتراکی در سرور راحت تر دست یابد می تواند آن پوشه را به صورت یک درایو مجازی در My Computer ایجاد کند تا با کلیک بر روی آن درایو، به پوشه اشتراکی دست یابد.

برای ایجاد یک Map Network Drive این مراحل را طی کنید:

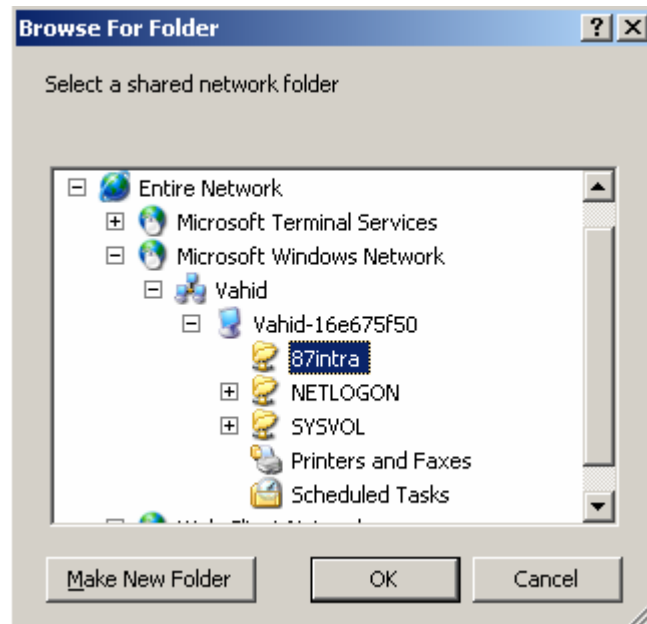
۱- در My Computer از منوی Tools بر روی Map Network Drive کلیک کنید.



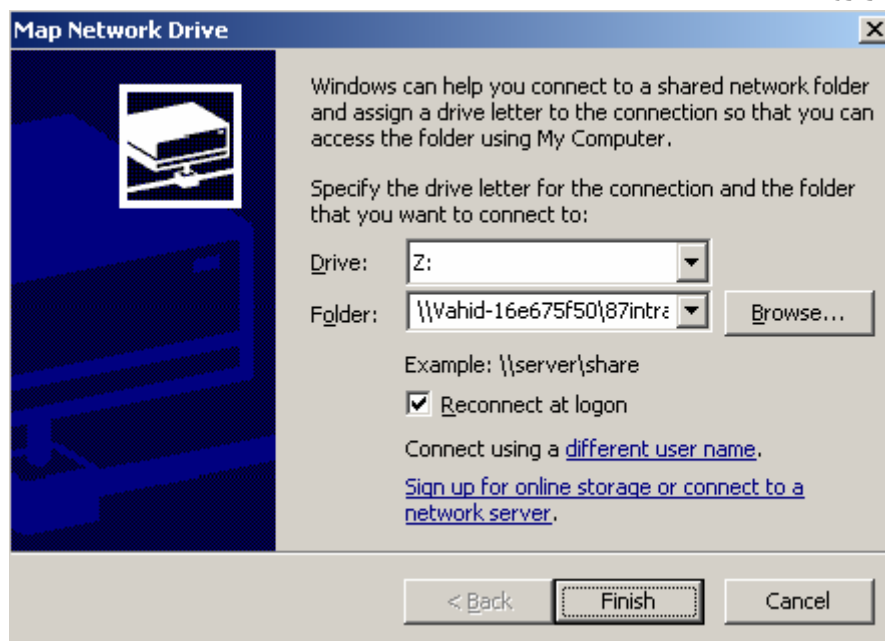
۲- در این پنجره برای درایو مجازی، نام Z در نظر گرفته شده است که می توانید آن را تغییر دهید. برای دادن مسیر فولدر اشتراکی بر روی Browse کلیک کنید.



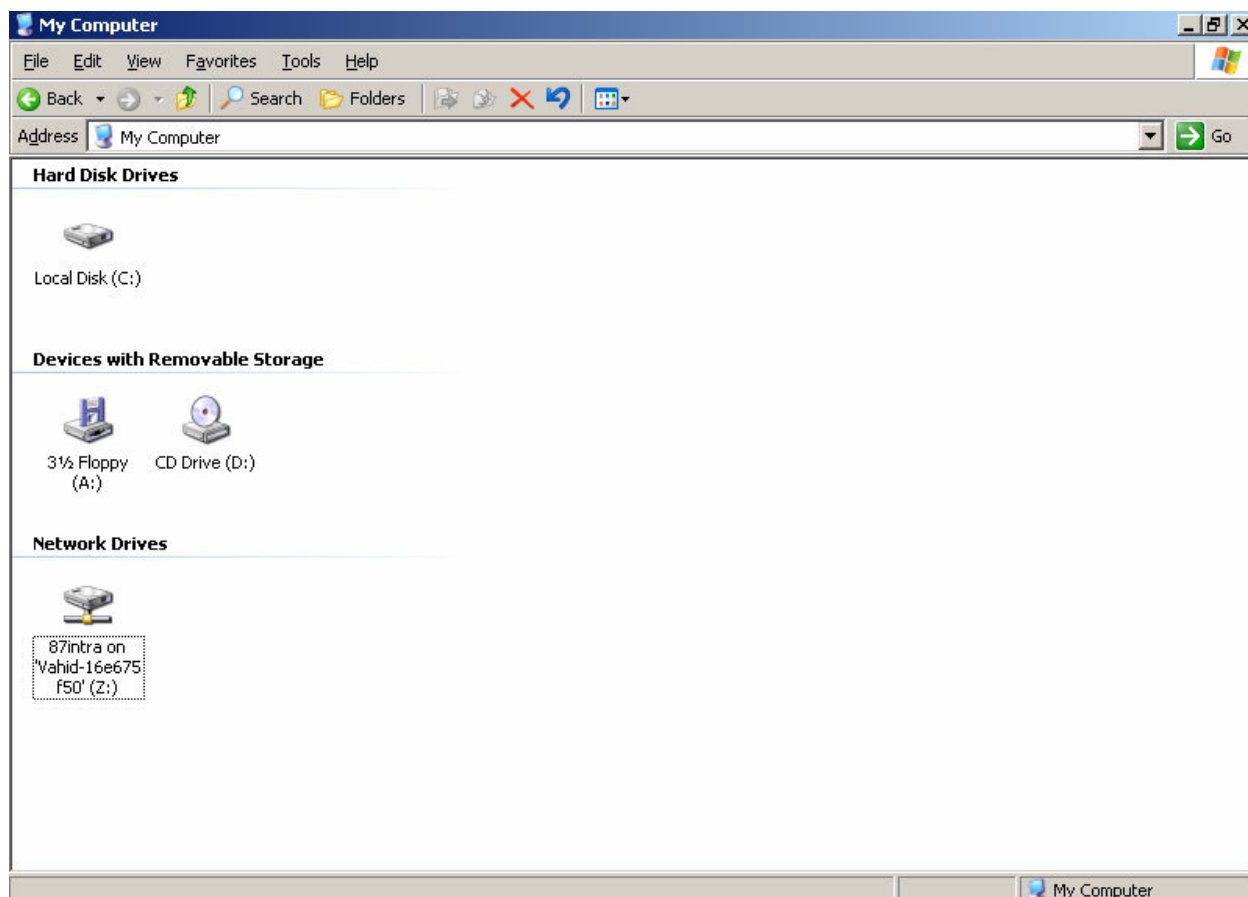
۳- در این پنجره فولدر اشتراکی را انتخاب و بر روی OK کلیک کنید.



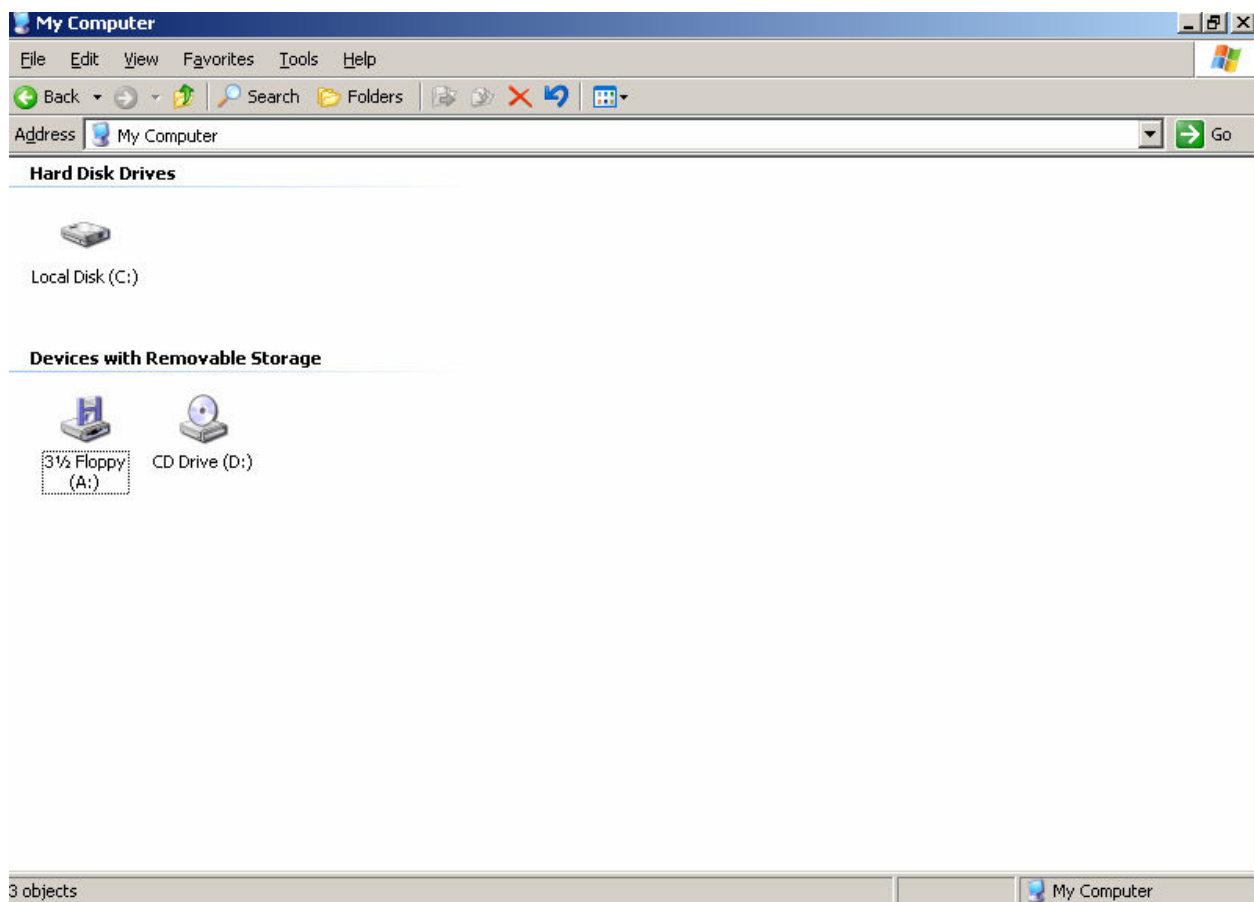
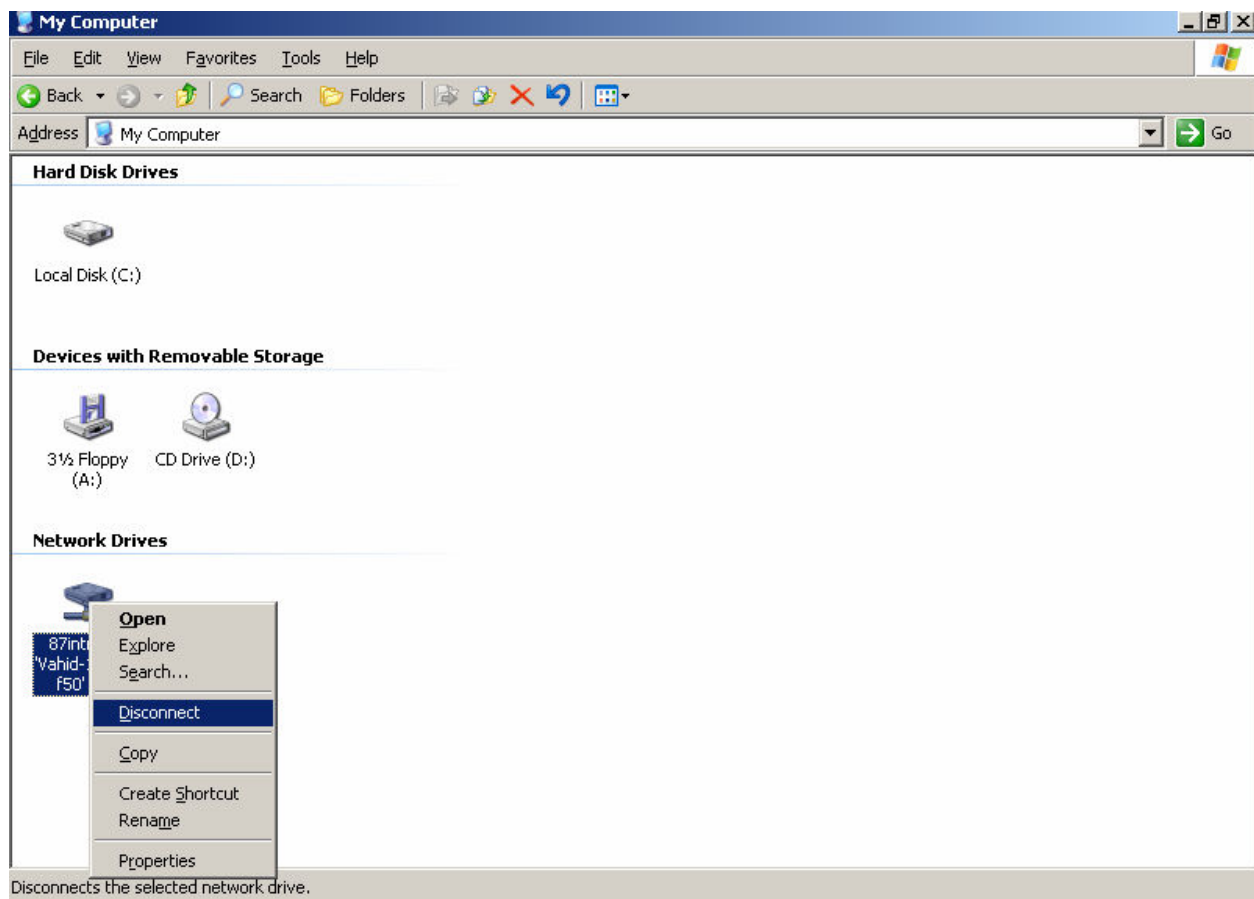
۴- گزینه Reconnect at logon برای این است که اگر می خواهید با Logon شدن شما درایو مجازی باقی بماند تیک این گزینه را قرار دهید. بر روی Finish کلیک کنید.



۵- در پنجره My computer درایو جدیدی را با نام Z مشاهده می کنید که اگر بر روی آن دوبار کلیک کنید داخل پوشه اشتراکی را نشان می دهد.

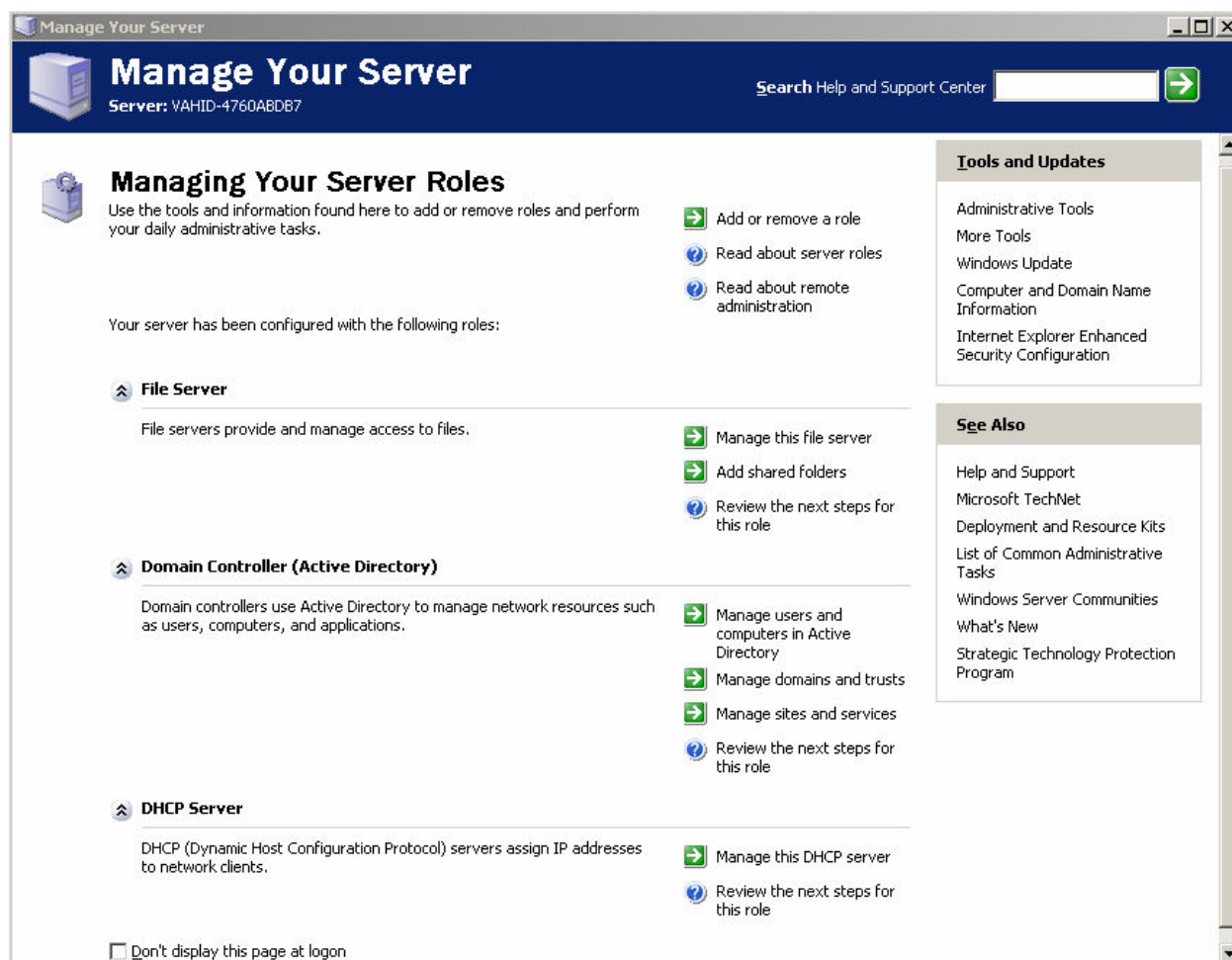


اگر زمانی بخواهید این درایو را حذف کنید بر روی آن راست کلیک کرده و گزینه Disconnect را انتخاب کنید تا حذف شود.

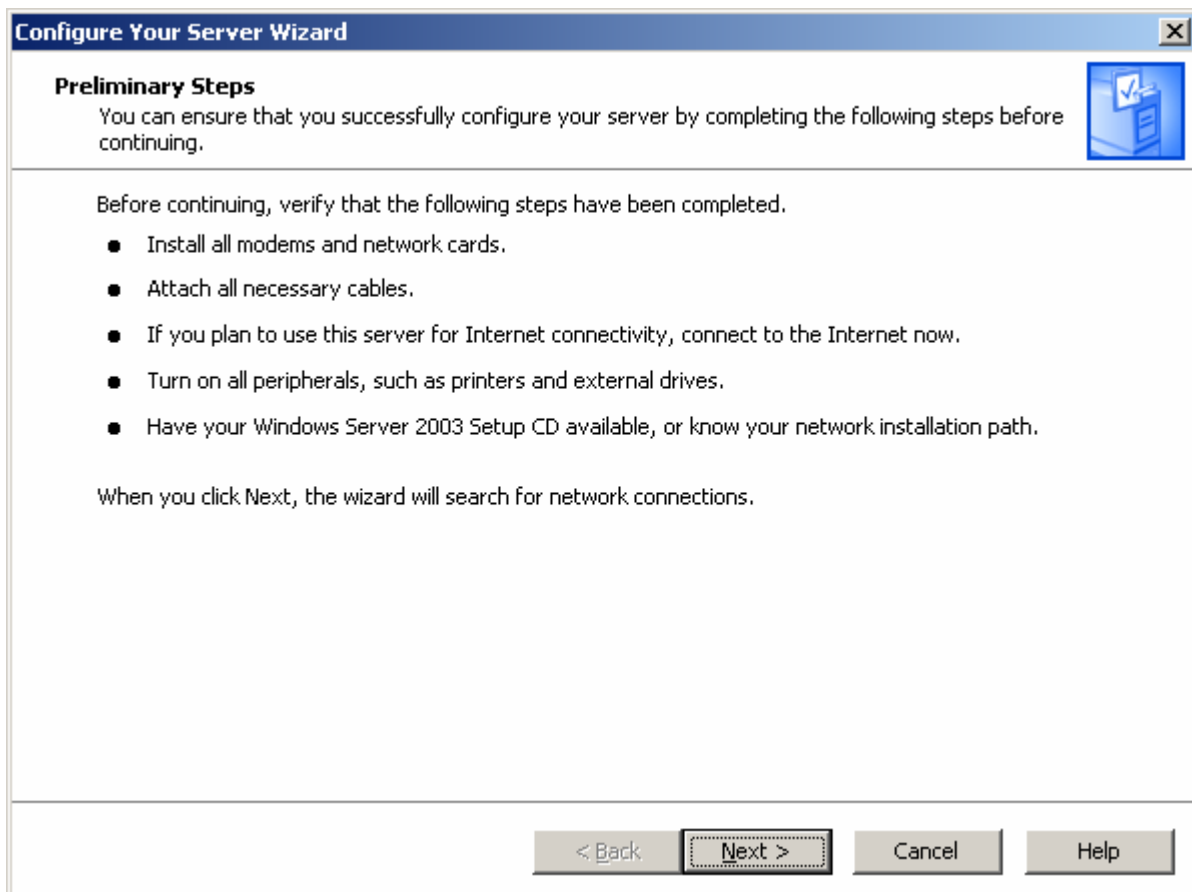


۴-۵- بررسی نحوه حذف File Server:

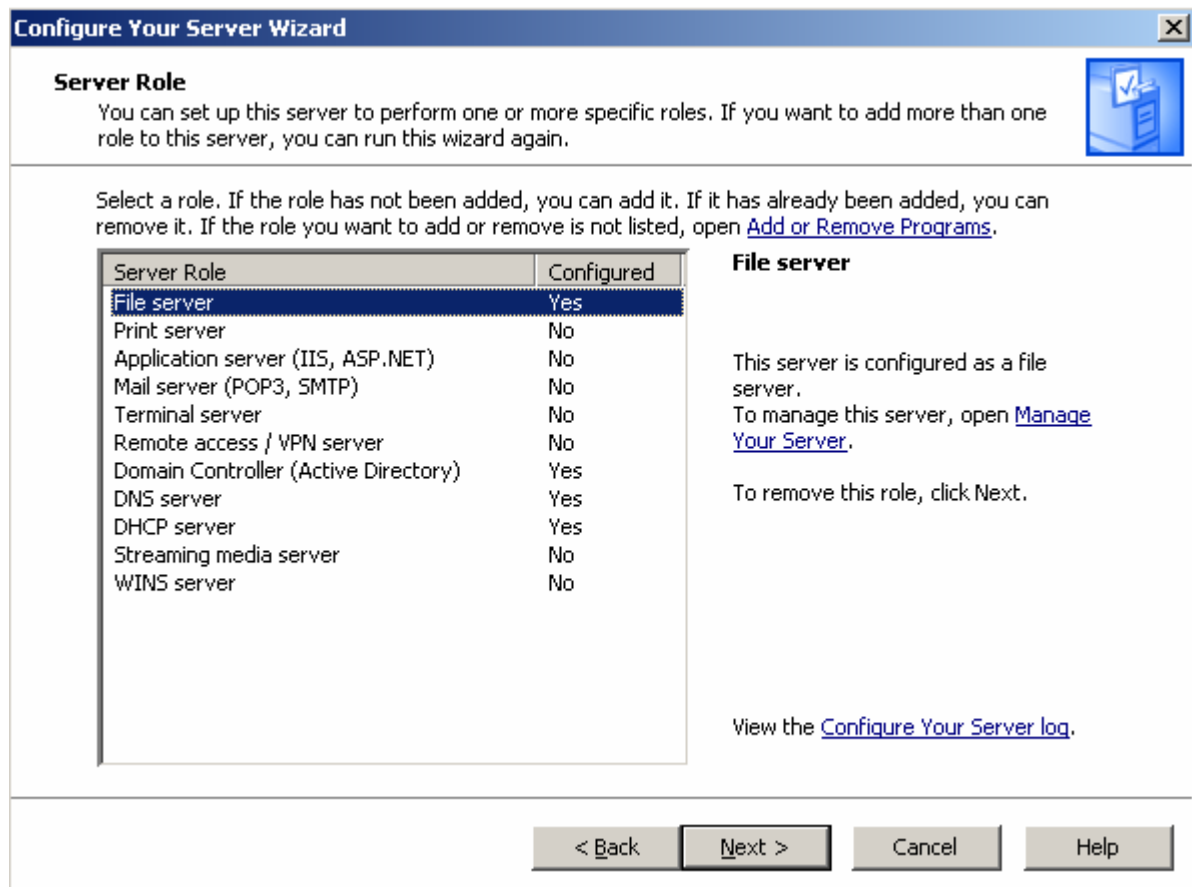
۱- روی دکمه Start کلیک کرده و روی آیکن Manage Your Server کلیک کرده تا پنجره ی زیر باز شود. سپس روی گزینه Add or remove a role کلیک کنید تا یک نقش جدید برای سرور اضافه یا حذف کنید.



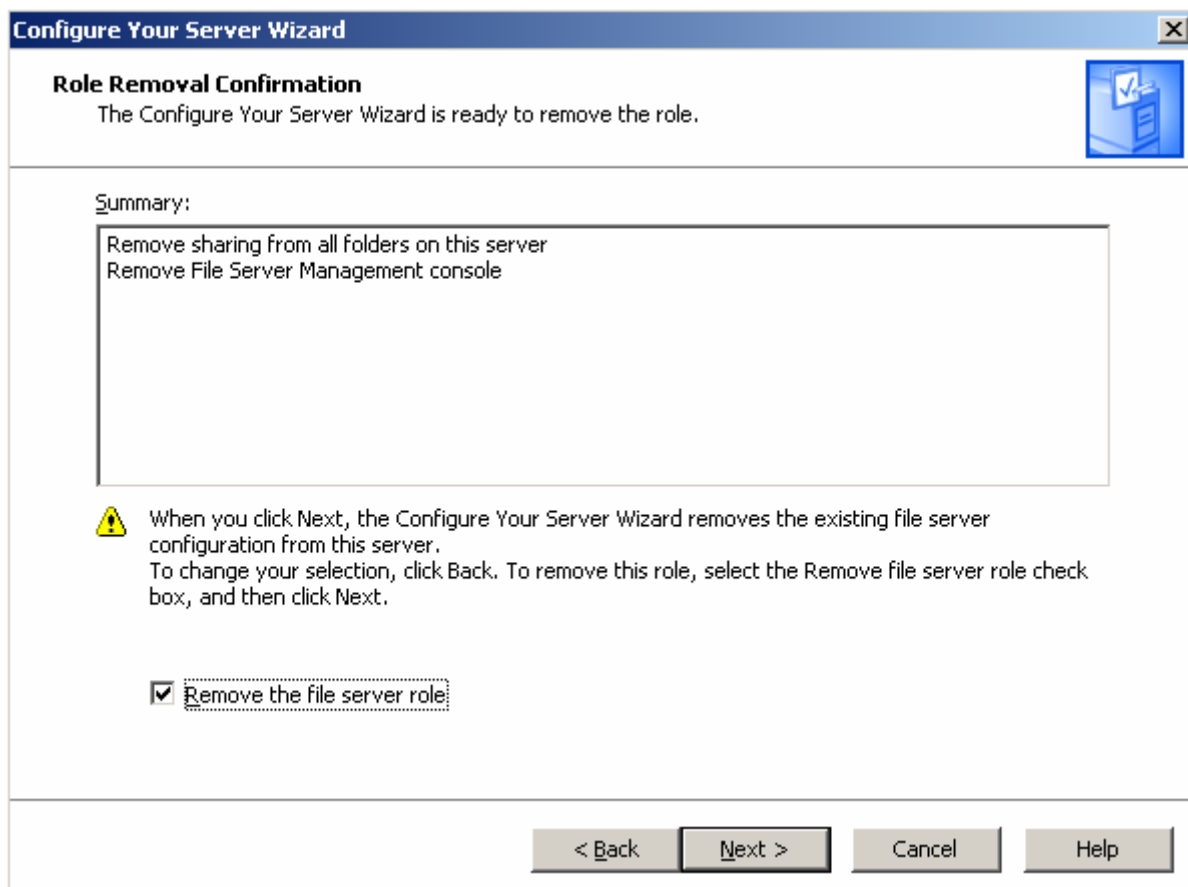
۲- روی دکمه Next کلیک کنید.



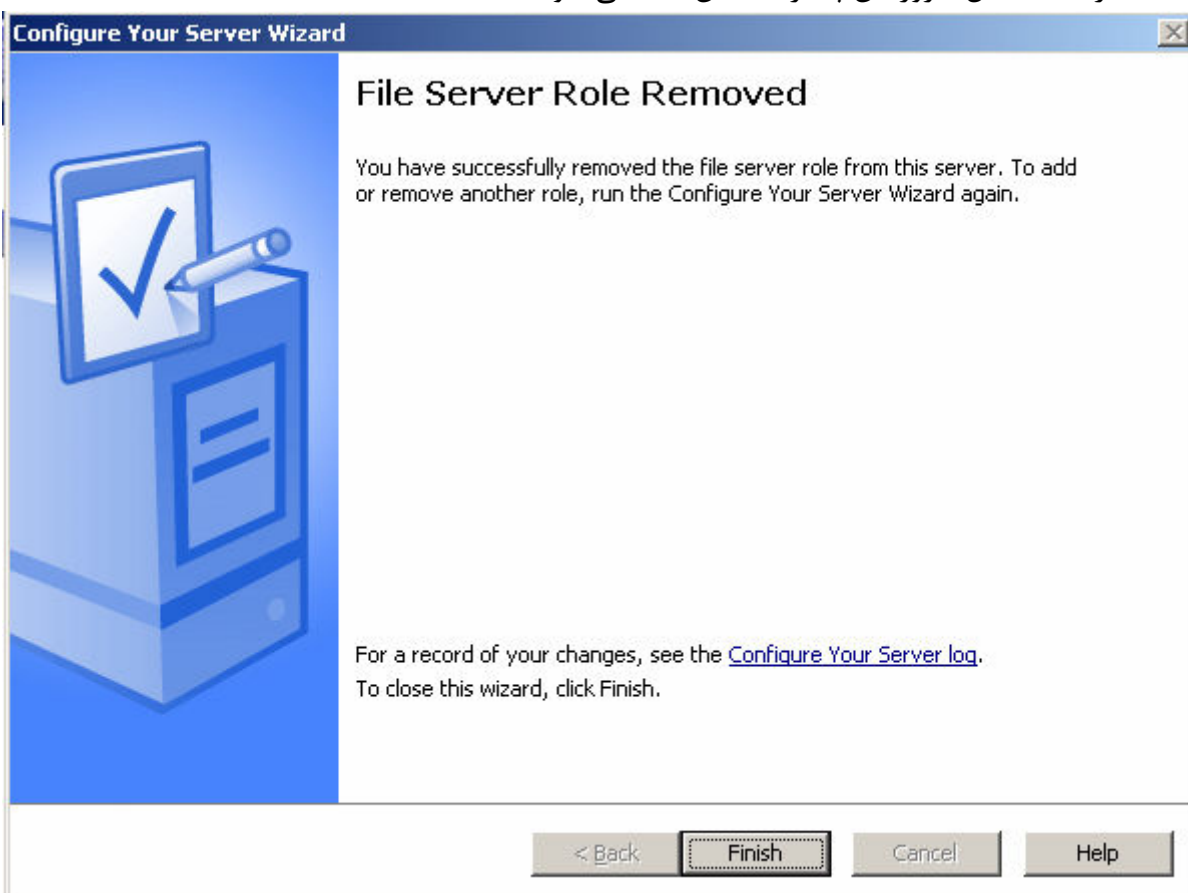
۳- در این پنجره بر روی File Server کلیک کرده سپس Next کنید.



۴- در پنجره زیر تیک گزینه ☒ Remove the file server role را برای حذف فایل سرور قرار داده، بر روی Next کلیک کنید.



۵- بعد از حذف فایل سرور این پنجره نمایش داده می شود.



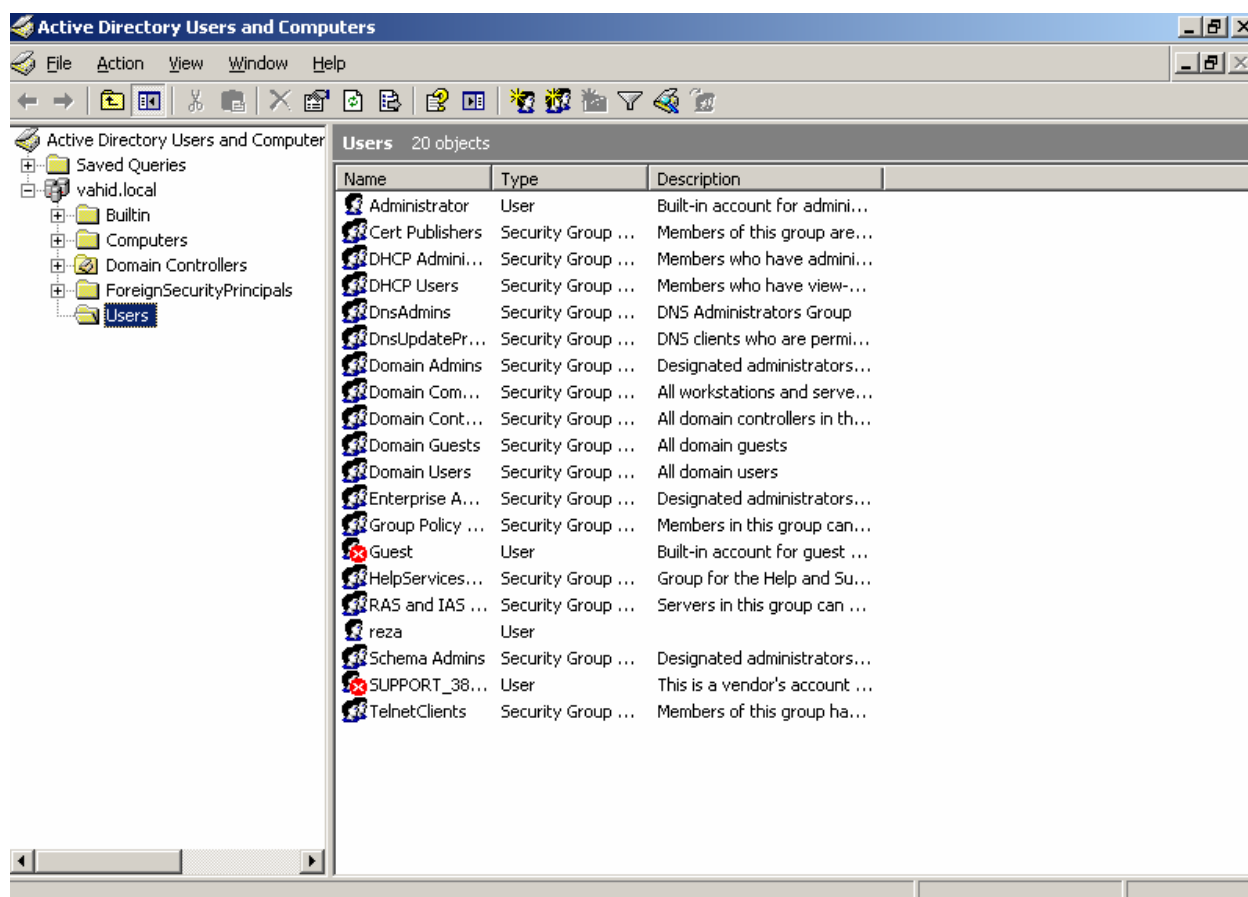
۶. جزئیات بخش ششم:

۱-۶- کاربران Organizational Unit:

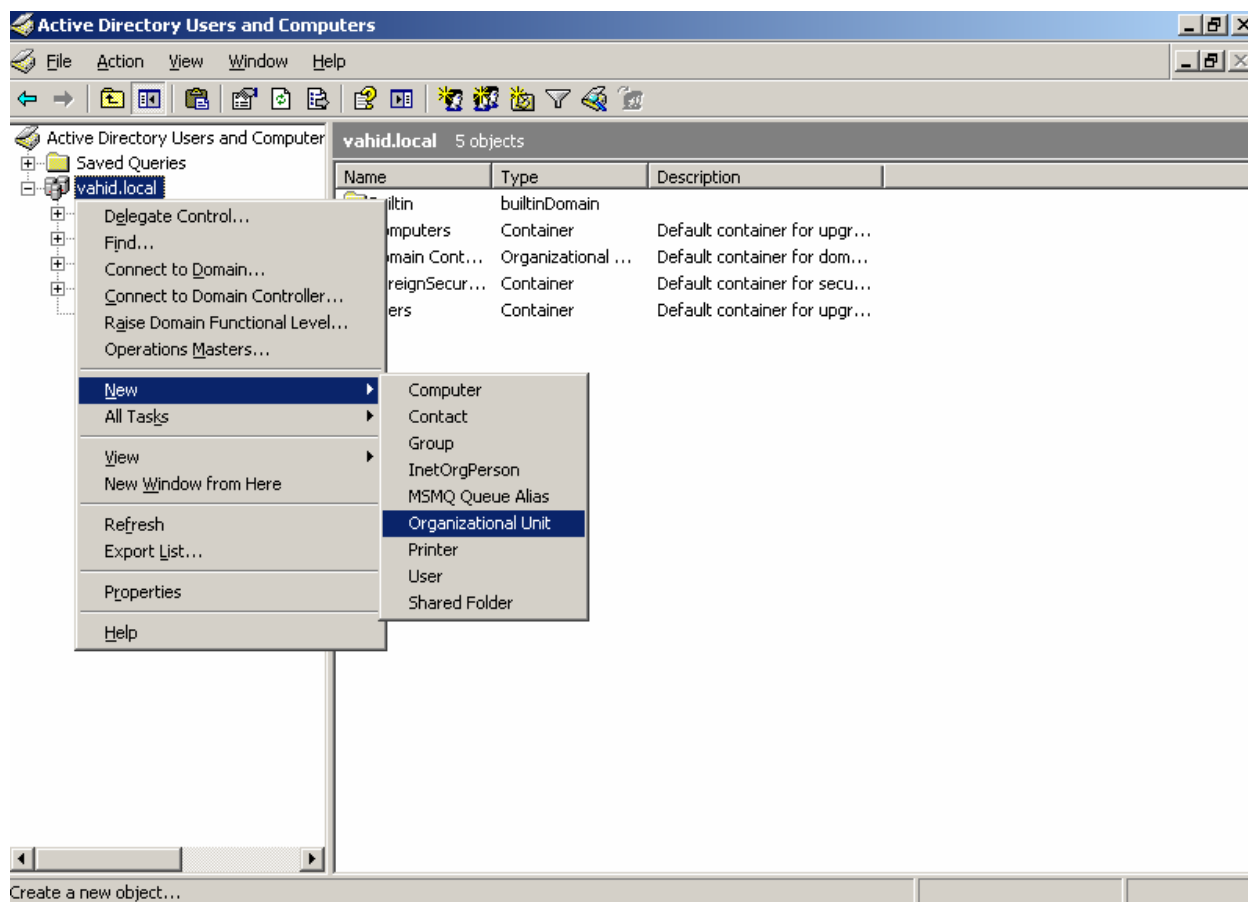
همچنان که می دانیم در یک شرکت یا سازمان ممکن است واحدهای سازمانی مختلفی وجود داشته باشد که این واحدها متشکل از کاربران و کامپیوترها می باشد. اگر بخواهیم یک سیاست خاص را برای گروهی از کاربران یا کامپیوترها ایجاد کنیم، تنظیم این سیاست را برای تک تک کاربران و کامپیوترها مشکل خواهد بود، برای رفع این مشکل در سطح دامنه می توانیم واحد سازمانی یا OU ایجاد کنیم و کاربران یا کامپیوترها را عضو این OU قرار دهیم و سپس سیاست گروهی را بر روی آن OU اعمال کنیم.

برای ایجاد یک OU جدید مراحل زیر را طی می کنیم:

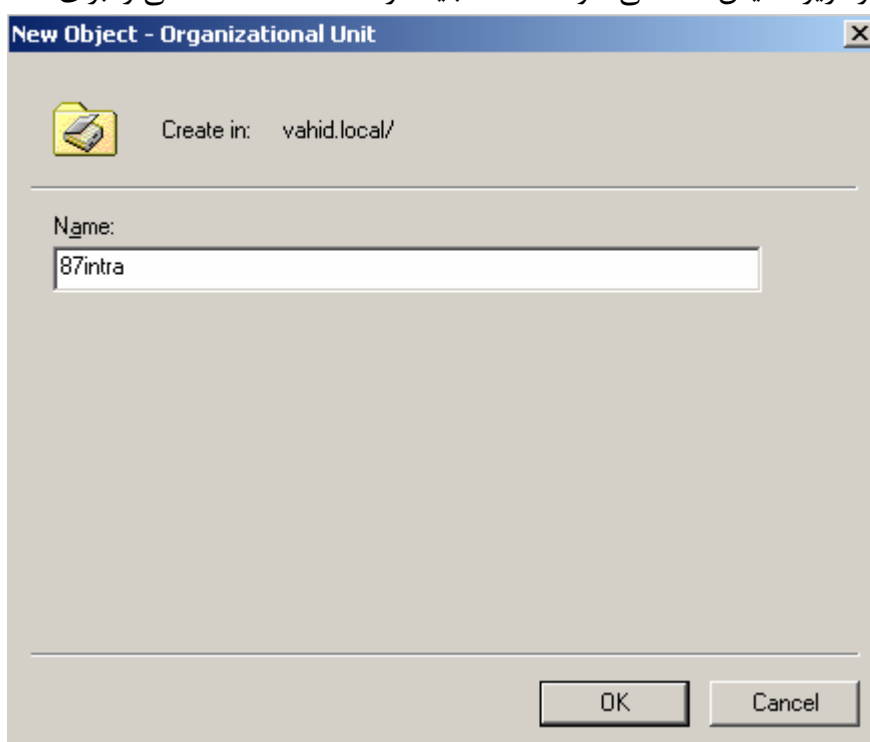
Start > Administrative Tools > Active Directory User and Computers
که شکل زیر ظاهر می شود.



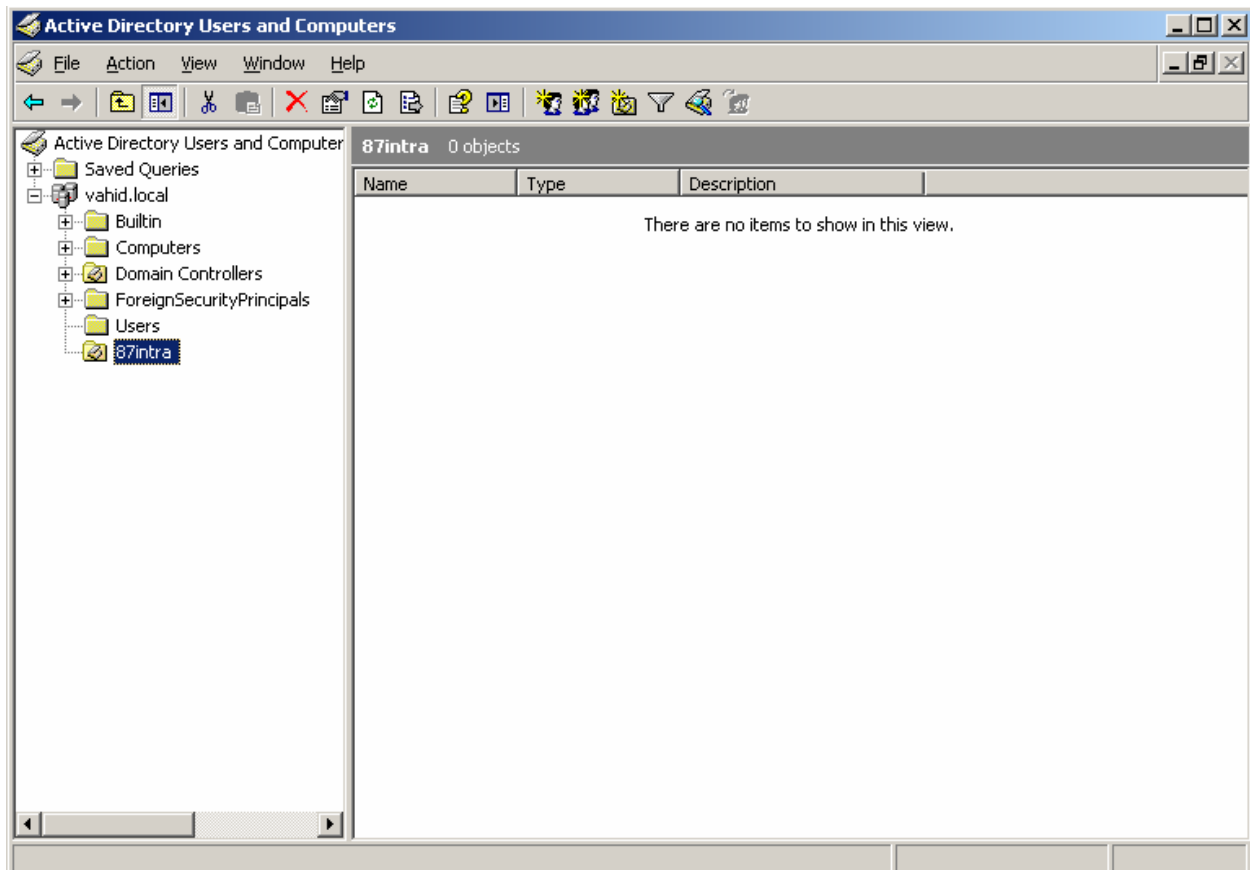
بر روی دامنه راست کلیک کرده و New و سپس بر روی Organizational Unit کلیک کنید.



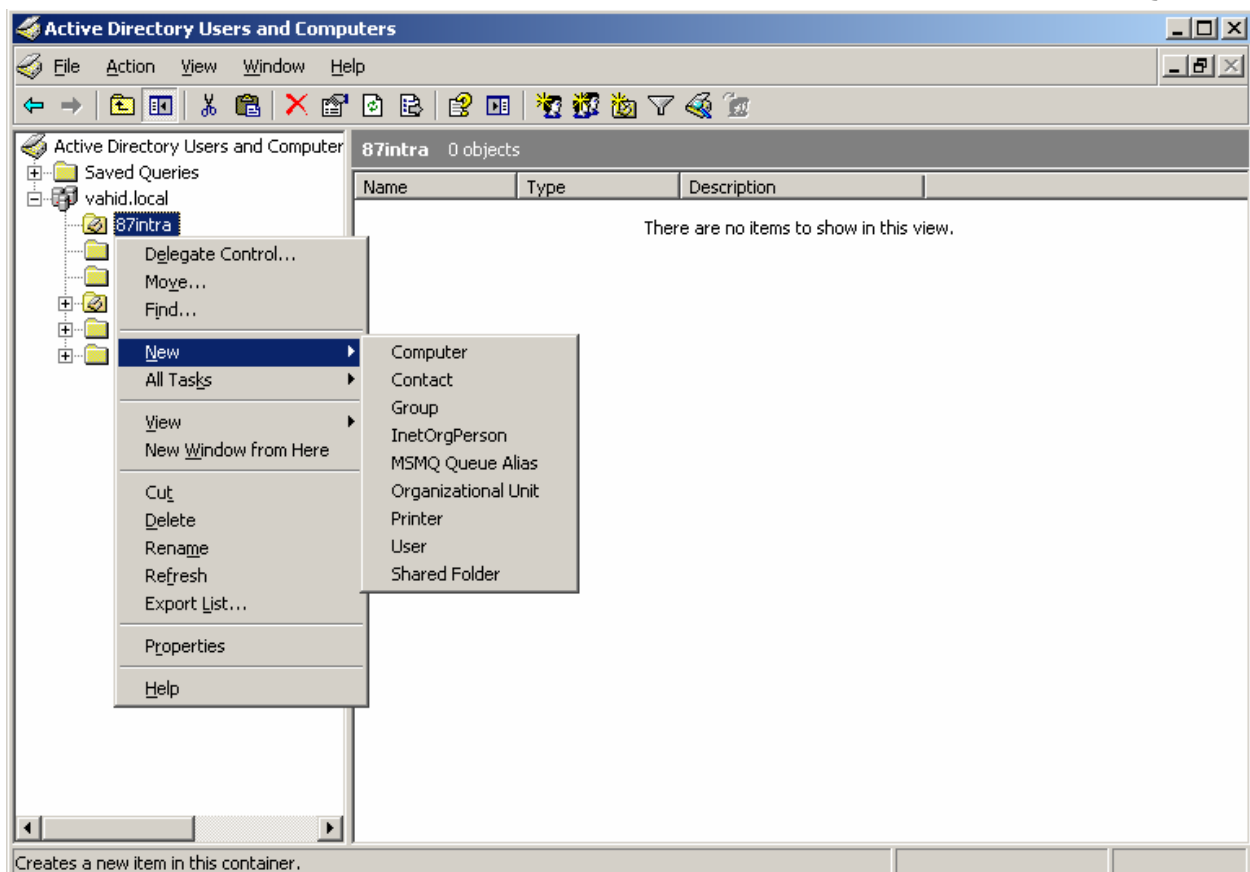
بعد از Next کردن پنجره زیر نمایش داده می شود که شما باید در قسمت Name نامی را برای OU وارد کنید.



همانطور که مشاهده می کنید یک OU جدید ایجاد شده است. حال در این OU می توانید کاربر و یا کامپیوتر جدید ایجاد نمائید و یا کاربران و کامپیوترهای موجود را به داخل آن انتقال (Move) دهید.

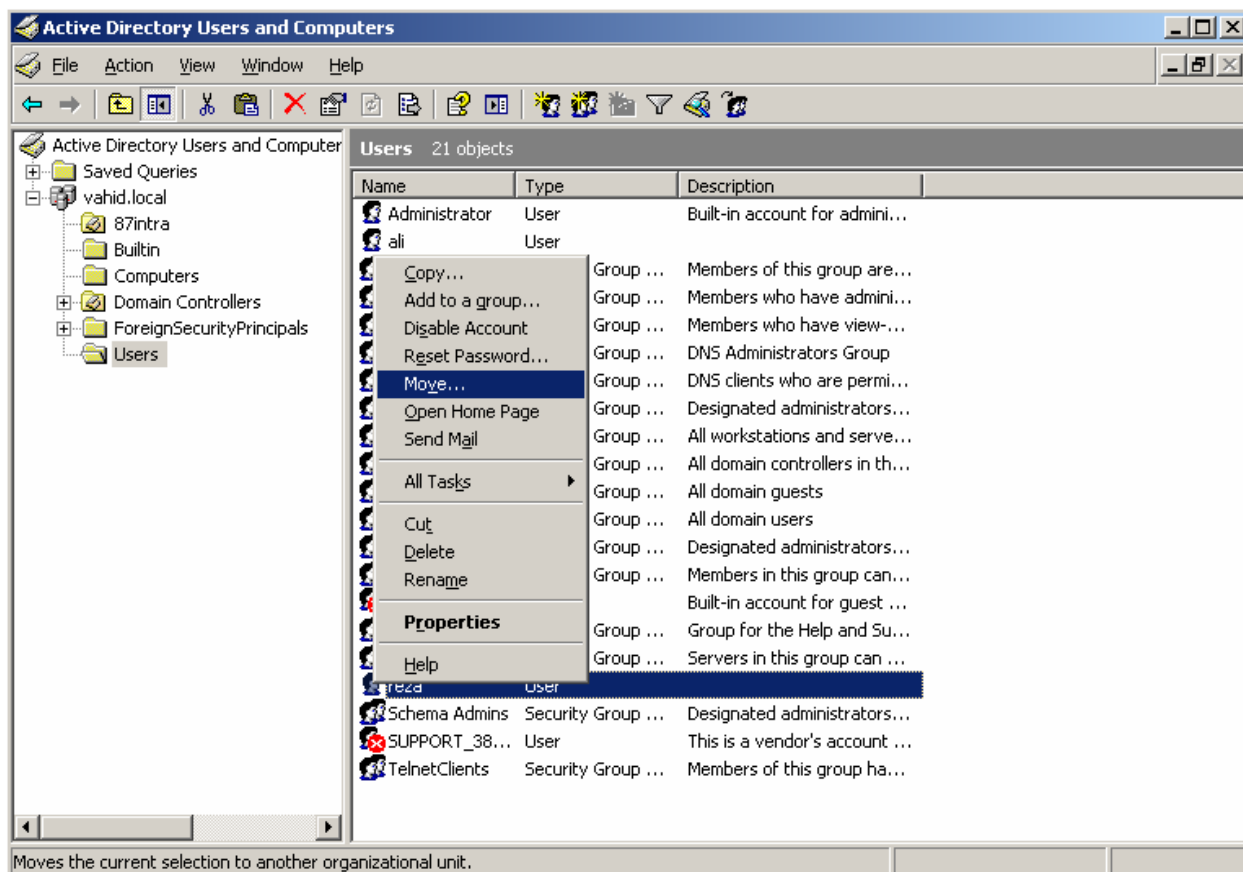


برای ایجاد یک User یا Computer جدید داخل این گروه، بر روی آن راست کلیک کرده و New و سپس User یا Computer را انتخاب کنید.

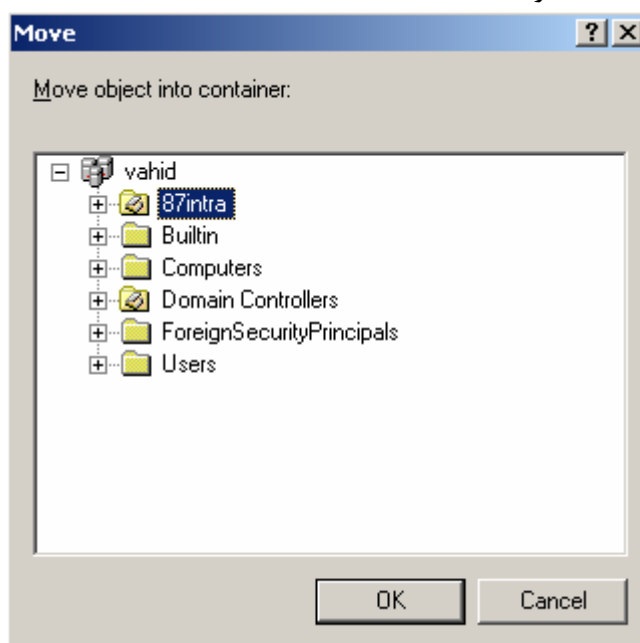


بقیه مراحل مانند ایجاد User یا Computer در دامنه است، که در قسمت های قبلی گفته شد.

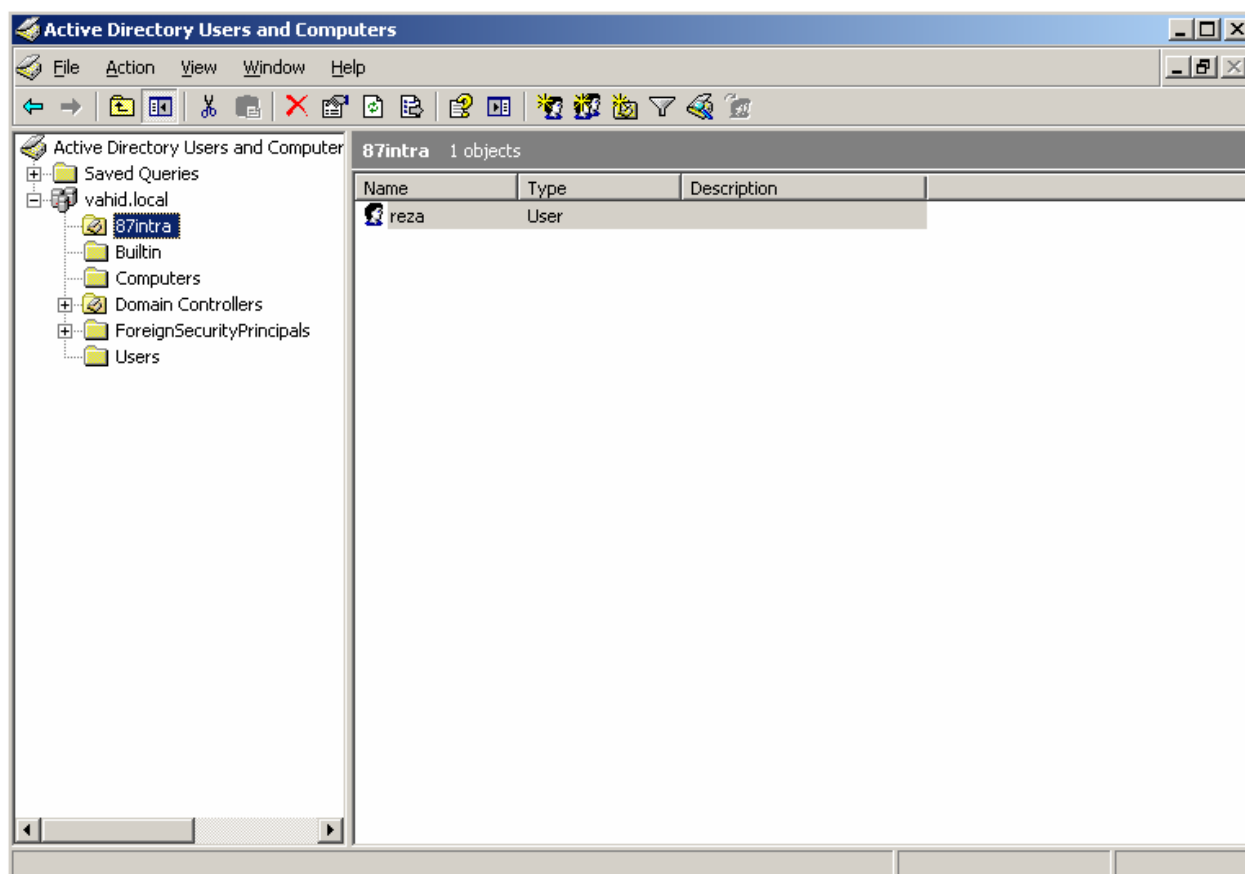
اگر می خواهید به عنوان مثال کاربری را از بخش User به سازمان 87 intra انتقال دهید، برای این کار بر روی کاربر در بخش User راست کلیک کرده و سپس Move را انتخاب کنید.



در پنجره ظاهر شده نام سازمان را انتخاب و OK کنید.



همانطور که می بینید کاربر به داخل سازمان انتقال یافته است.

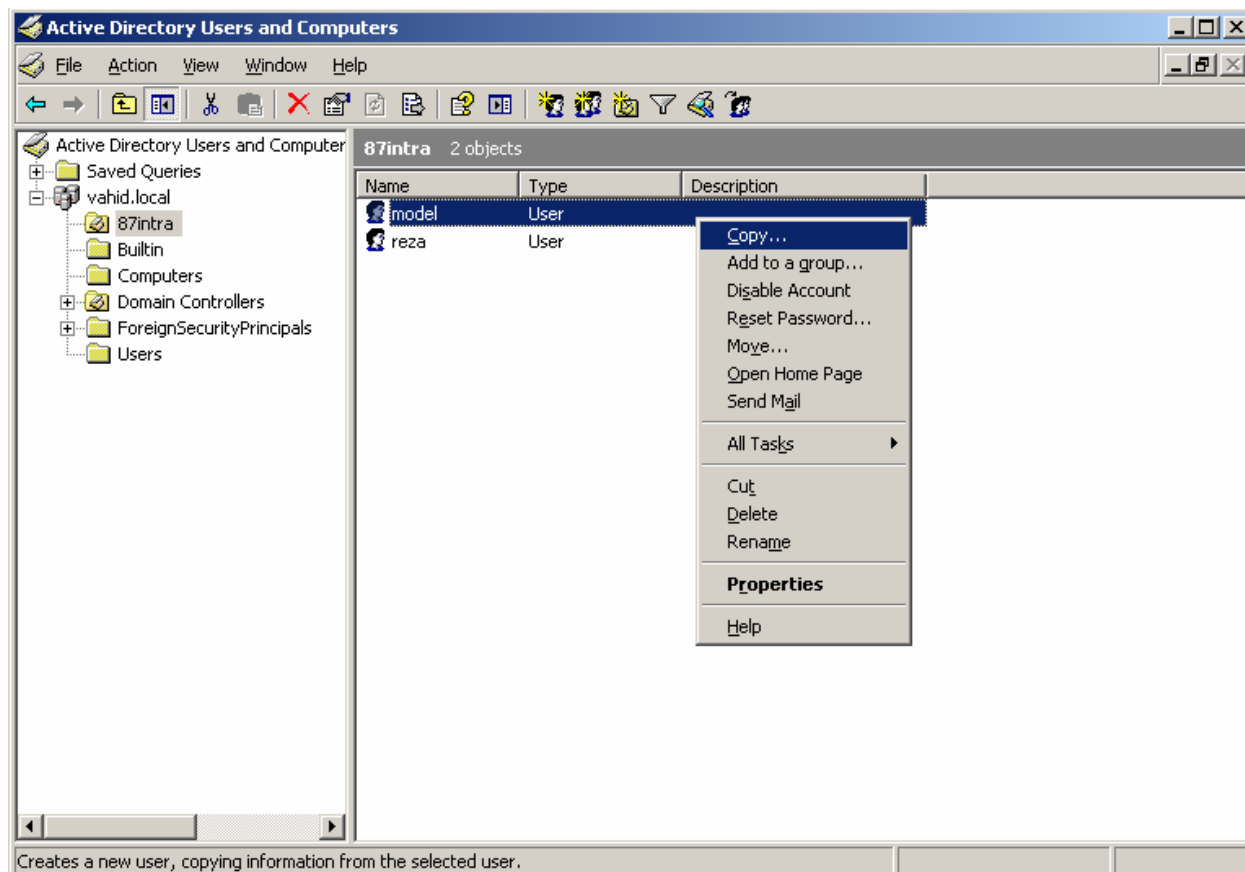


۲-۶- تکثیر کاربران:(برای مطالعه)

در قسمت قبل در ارتباط با یک Domain بحث کردیم که شامل تعداد زیادی OU نیز می باشد. فرض کنید کاربرانی را که در این OUها ایجاد می کنید بسته به واحد سازمانی مشخصاتی متفاوت از هم داشته باشند. به عنوان مثال کاربران یک واحد در روزها و ساعات خاصی از هفته بتوانند Logon کنند یا تاریخ انقضا آنها آخر سال باشد و یا عضو گروه های خاص باشند، از روی کامپیوتر های خاص بتوانند Logon کنند و...، به طوری که این مشخصات متفاوت از مشخصات واحدهای دیگر باشد.

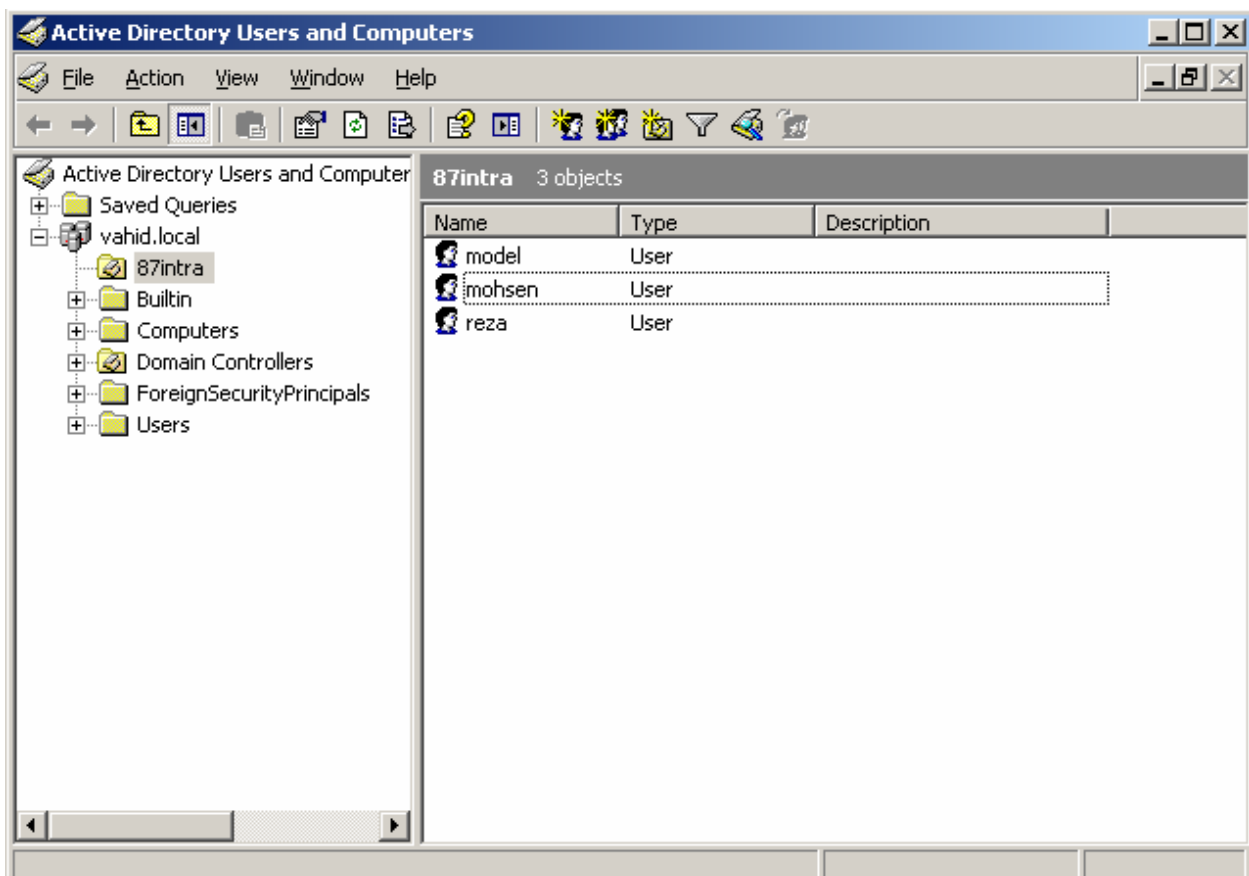
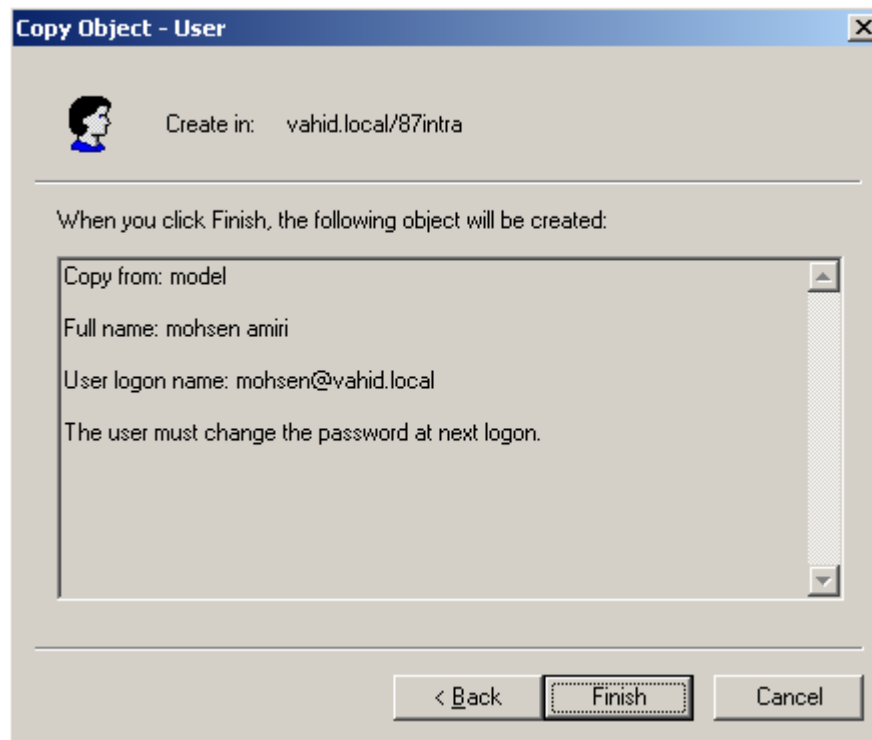
در این حالت هر زمان که شما یک کاربر جدید برای این واحد ایجاد می کنید تمامی این تنظیمات را از نو برای آن کاربر باید انجام دهید و باید دقت کنید که اشتباهی صورت نگیرد، حال اگر مشخصات کاربران واحدهای مختلف متفاوت باشند کار برای شما سخت تر هم خواهد شد.

راه حل بهتری که داریم، این است که یک کاربر نمونه برای هر واحد ایجاد کنید. برای هر کدام از آنها، مشخصات را بر اساس نیاز آن واحد تعیین کنید و سپس برای کپی گرفتن از این کاربر بر روی آن کلیک راست کرده و گزینه Copy را انتخاب کنید.



که پنجره ای به صورت زیر ظاهر می شود (اگر توجه کنید، در بالای شکل عبارت User – Copy Object نوشته شده است) که باید مشخصات کاربر جدید را در آن وارد کنید.

در پنجره بعدی، بعد از اینکه رمز کاربر را وارد کرده و Next کردید، این پنجره نمایش داده می شود که توضیح می دهد کاربر جدیدی که ایجاد می کنید Copy ای از کاربر model (کاربری که به عنوان نمونه درست کرده ایم) می باشد.



۳-۶- Group Policy در ویندوز ۲۰۰۳:

محصولات ویندوز ۲۰۰۳ برای مدیریت بهتر کامپیوتر روشهای مختلفی را ارائه داده است. با استفاده از گزینه های موجود در کنترل پنل شما می توانید در بخش های اصلی کامپیوتر تغییراتی انجام دهید. اما روش دیگر استفاده از G.P میباشد. در محیط Domain شبکه، از G.P برای پیکر بندی و سفارشی نمودن کامپیوترهای موجود در شبکه استفاده می کنند. اگر شما در حالت Standalone باشید یا یک گروه کاری ایجاد کرده باشید فقط کامپیوتر خود را با استفاده از G.P می توانید تنظیم کنید.

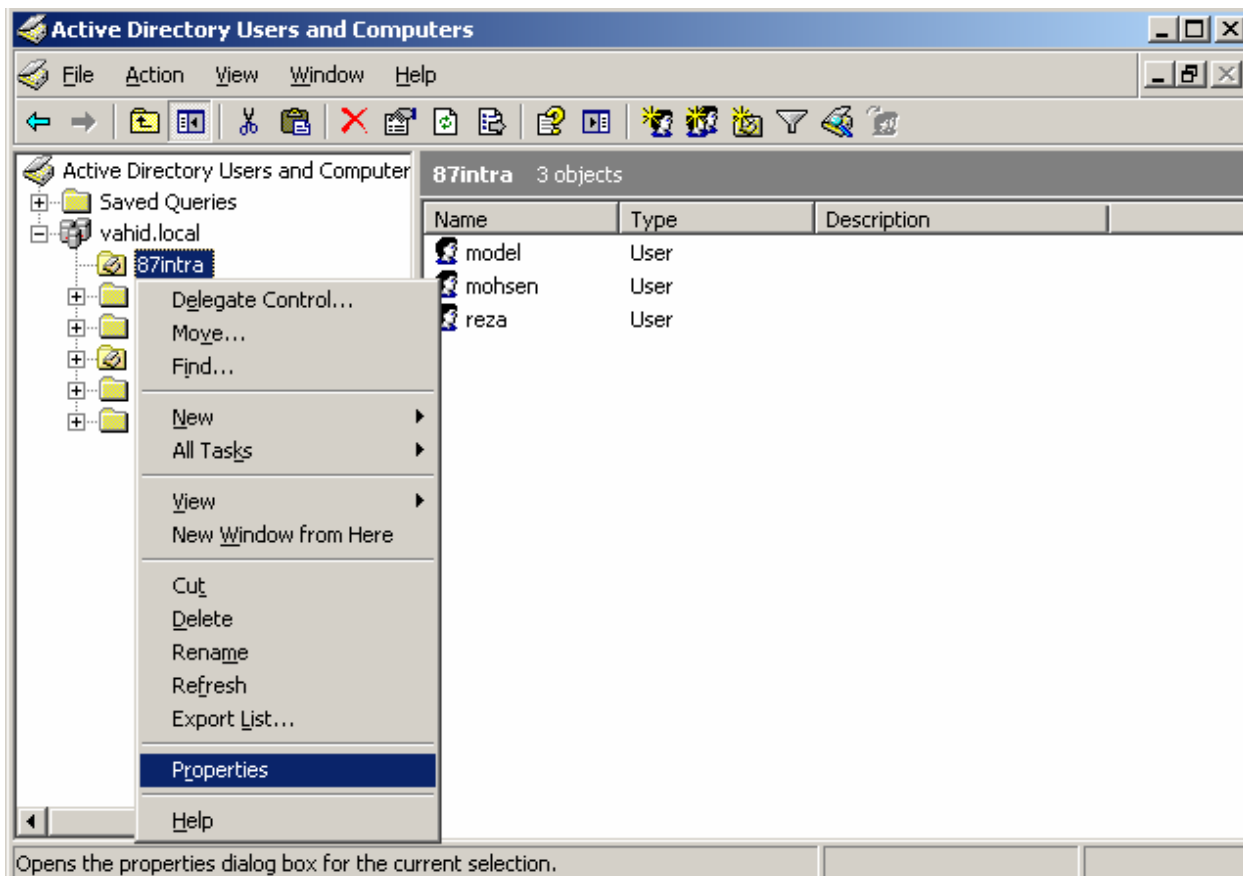
Group Policy به سرورها و مدیران شبکه قدرت تنظیم و اعمال اجباری سیاست های خود روی کاربران و کامپیوترهایی که بعنوان کلاینت در شبکه قرار دارند را می دهد. برخی از سیاست هایی که توسط Group Policy روی کامپیوتری، کاربری یا گروهی خاص از روی سرور انجام می شود:

- نصب برنامه های کاربردی روی سیستم.
- تنظیمات موارد امنیتی.
- اجرای اسکریپت هایی هنگام Log on یا Log off.
- اجرای اسکریپت هایی هنگام بالا آمدن یا خاموش شدن سیستم.
- حذف و اضافه نمودن گزینه ای Taskbar، menu start و کنترل پانل.
- ...

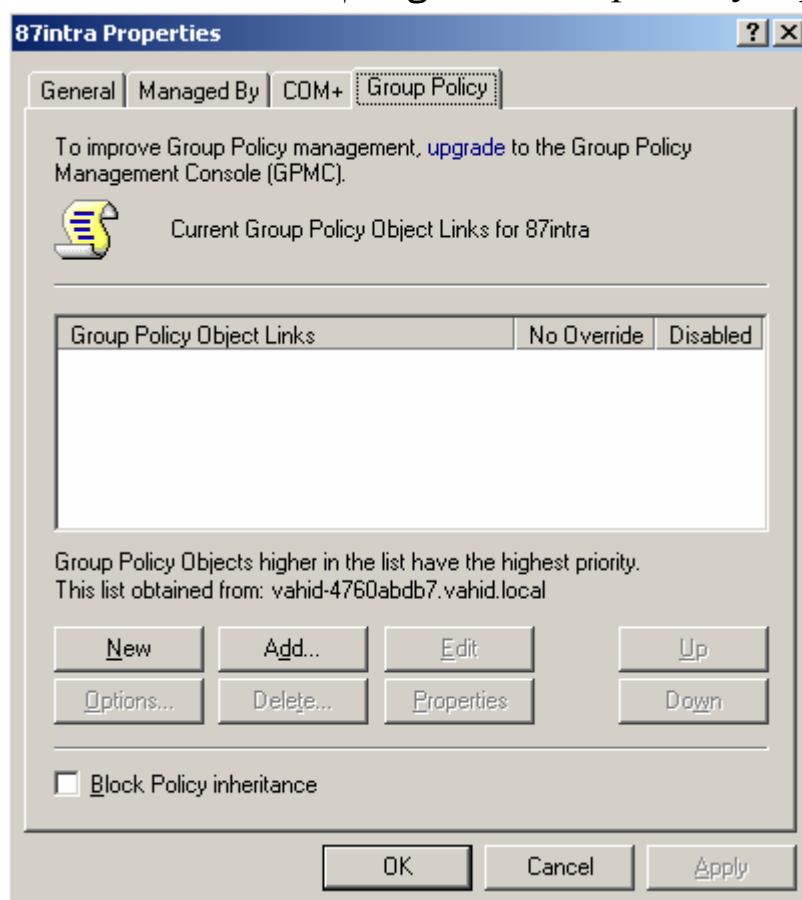
برخی از تنظیمات Policy Group مخصوص کاربر و برخی دیگر از تنظیمات مخصوص کامپیوتر است. یعنی اگر تنظیمات روی کاربر اعمال گردد، آن کاربر از هر کامپیوتر وارد شبکه گردد آن سیاست و تنظیمات روی نام کاربری (Username) (وی اعمال می شود و به کامپیوتر بستگی ندارد و برخی از سیاست ها (Policy ها) که روی کامپیوتر اعمال می شود به کاربر بستگی ندارد.

ما می توانیم سیاست را بر روی دامنه یا یک سازمان اعمال کنیم. در اینجا ما پس از آنکه یک OU ایجاد کردیم، حال می خواهیم بر روی آن یک سیاست اعمال کنیم. برای این کار مراحل زیر را طی می کنیم:

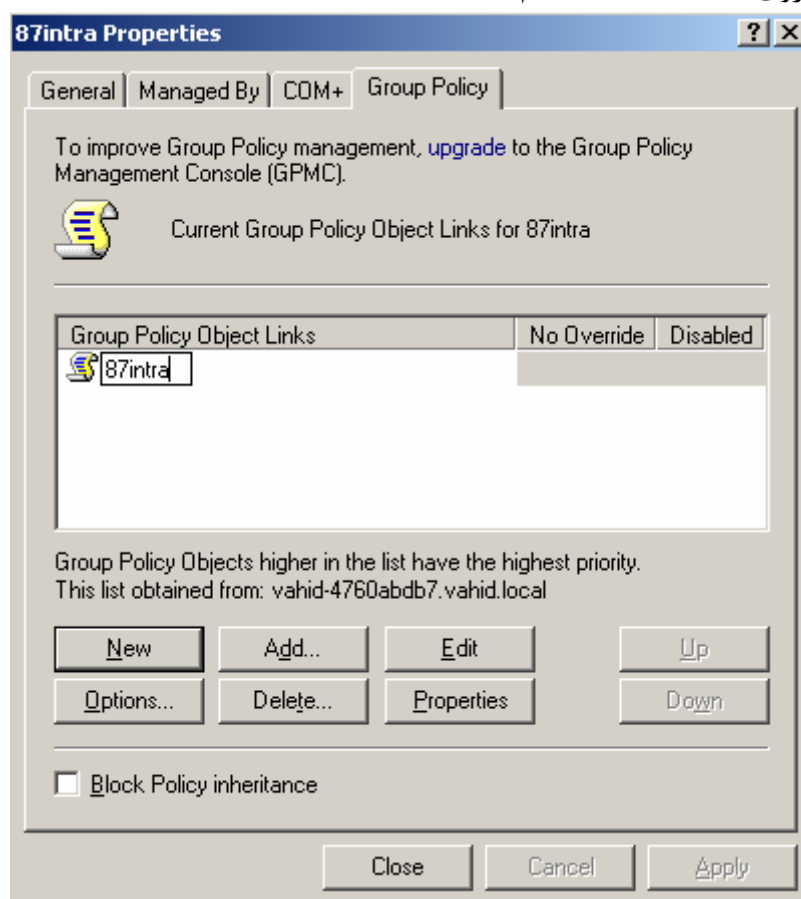
بر روی سازمانی که می خواهیم سیاستی بر روی آن اعمال کنیم، راست کلیک و Properties را انتخاب میکنیم.



در پنجره باز شده بر روی زبانه Group Policy کلیک می کنیم.

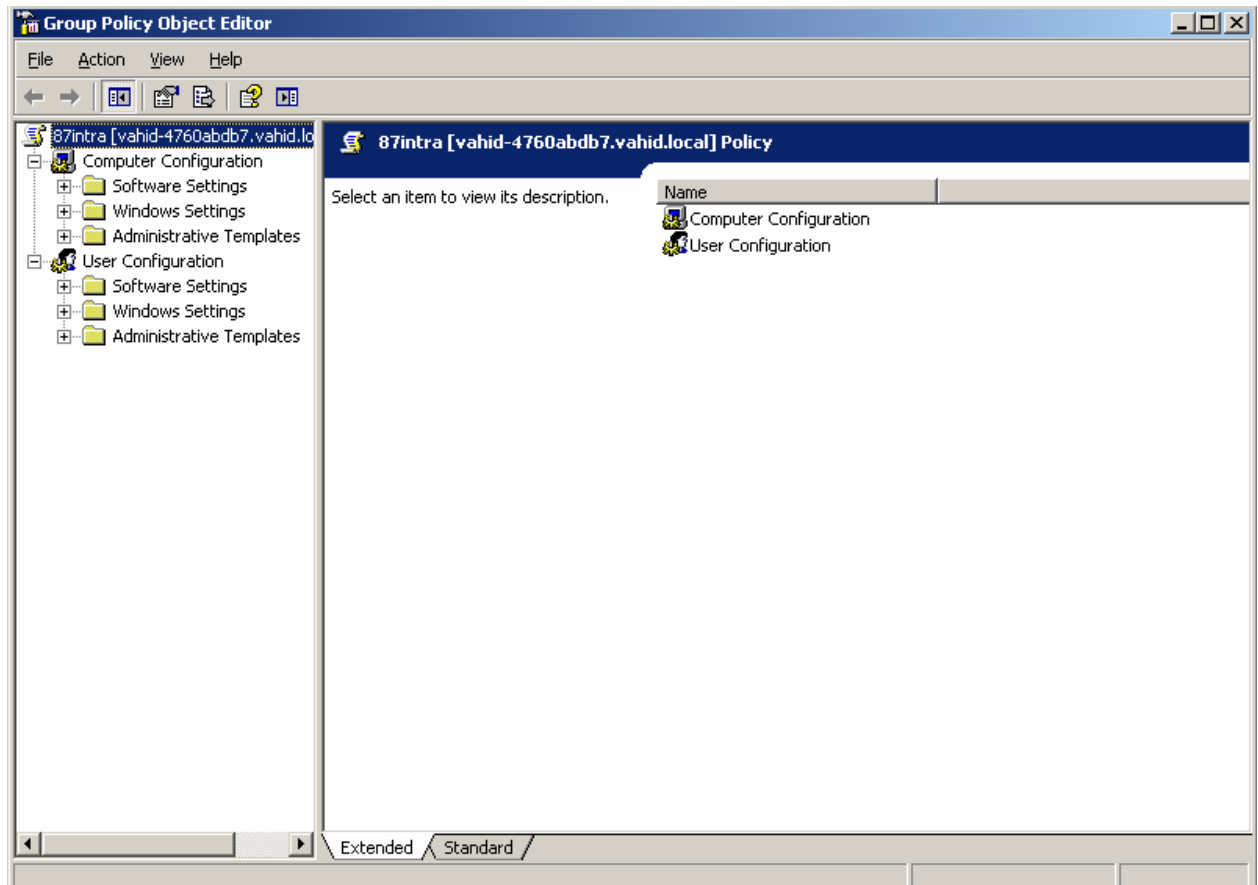


در Group Policy برای ایجاد یک سیاست جدید بر روی Add کلیک و برای سیاست جدید نامی را تایپ می کنیم. برای اعمال سیاست بر روی Edit کلیک میکنیم.



پنجره جدیدی باز می شود که در آن دو گزینه وجود دارد:

بخش Computer Configuration: سیاست هایی که می توانیم بر روی کامپیوترهایی که در این سازمان قرار دارند اعمال کنیم. این تنظیمات بر روی همه کاربران کامپیوترهای مذکور اثر میگذارد. مدیران شبکه می توانند بوسیله فعال یا غیر فعال کردن تنظیمات، سیاست های مختلفی را انجام دهند.



در بخش **Computer Configuration** نیز سه گزینه وجود دارد:

۱- **Software Settings**: این آیتم شامل بخش **Software Installation** می باشد. که در این بخش می توانیم تنظیمات نرم افزار برای کامپیوترها را اعمال کنیم. در این بخش می توانیم نرم افزارها را به کامپیوترها اضافه، حذف، به روز رسانی و... کنیم (فقط مدیر می تواند حذف کند).

۲- **Windows setting**: در این بخش می توانیم تنظیمات ویندوز را برای سیاست خاصی تغییر دهیم.

بخش **Windows setting** نیز شما دو گزینه می باشد:

۱-۲- **Script**: با استفاده از این اسکریپت ها می توانیم برای کامپیوترها سیاستی را تعیین کنیم که در چه زمانی روشن و در چه زمانی خاموش شوند.

۲-۲- **Security Setting**: تنظیمات **Security Setting** مربوط به امنیت کامپیوترها و کل شبکه می باشد. که در این بخش می توانیم تنظیمات امنیتی را برای دامنه یا هر قسمت از OU انجام دهیم.

۲- Administrative Templates: توضیح این بخش در بحث مربوط به محدود کردن مدیران مفصلاً بحث خواهد شد.

بخش User Configuration: سیاست هایی که می توانیم بر روی کاربران موجود در این سازمان اعمال کنیم.

بخش User Configuration نیز شامل چهار گزینه می باشد:

۱- Software Settings: این گزینه شامل بخش Software Installation می باشد. که در این بخش می توانیم تنظیمات نرم افزاری را برای کاربران اعمال کنیم تا کاربران به نرم افزار های مورد نیاز خود راحت تر دسترسی یابند.

۲- Windows settings: تنظیمات ویندوز در این بخش قرار دارد که به همه کاربران موجود در گروه اعمال می شود.

در بخش Windows settings پنج گزینه وجود دارد:

۱-۲ Remote Installation Services: با استفاده از این بخش می توان سیاست هایی را برای استفاده کاربر از ابزار کنترل از راه دور (RIS) اعمال کرد.

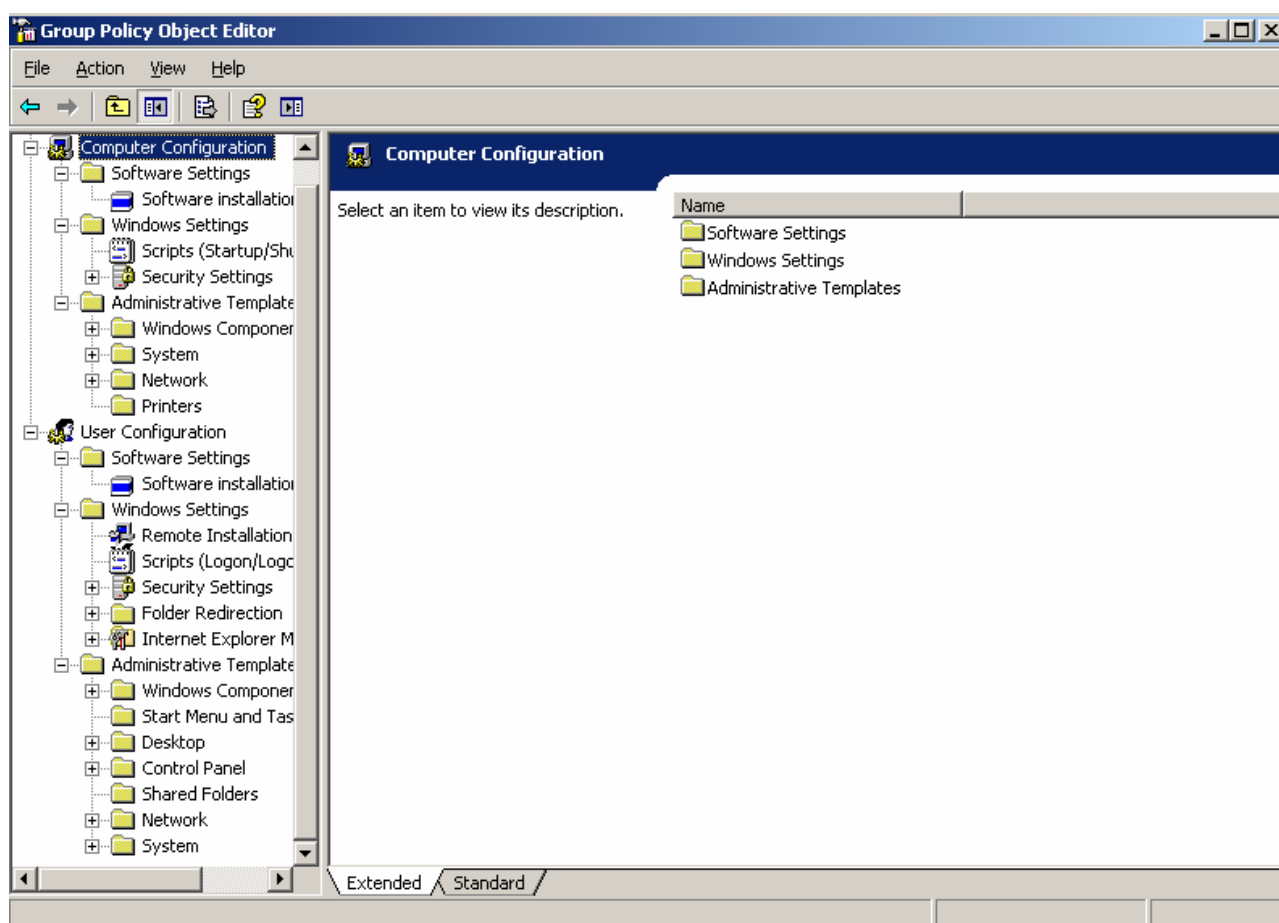
۲-۲ Script: با استفاده از این اسکریپت ها می توان اسکریپت های ورود و خروج را مشخص کرد.

۳-۲ Security Setting: تنظیمات Security Setting مربوط به امنیت کامپیوترها و کل شبکه می باشد. که در این بخش می توانیم تنظیمات امنیتی را برای دامنه یا هر قسمت از OU انجام دهیم. برای مثال به طور پیش فرض همه نرم افزارها می توانند اجرا شوند. می توان در این بخش سیاستی را اعمال کرد تا نرم افزاری بدون توجه به حقوق کاربر اجرا نشوند.

۴-۲ Folder Redirection: برای پشتیبان گیری داده های کاربر از روی یک کامپیوتر بر روی سرور مورد استفاده قرار می گیرد. می توان سیاستی را اعمال کرد تا به طور اتوماتیک از داده ها پشتیبان گرفته شود.

۵-۲ Internet Explorer Maintenance: حاوی تنظیماتی برای اعمال روی Internet Explorer می باشد.

۳- Administrative Template: این بخش نیز مربوط به تنظیمات برای مدیران می باشد. که در بحث های بعدی راجع به آن توضیح خواهیم داد.



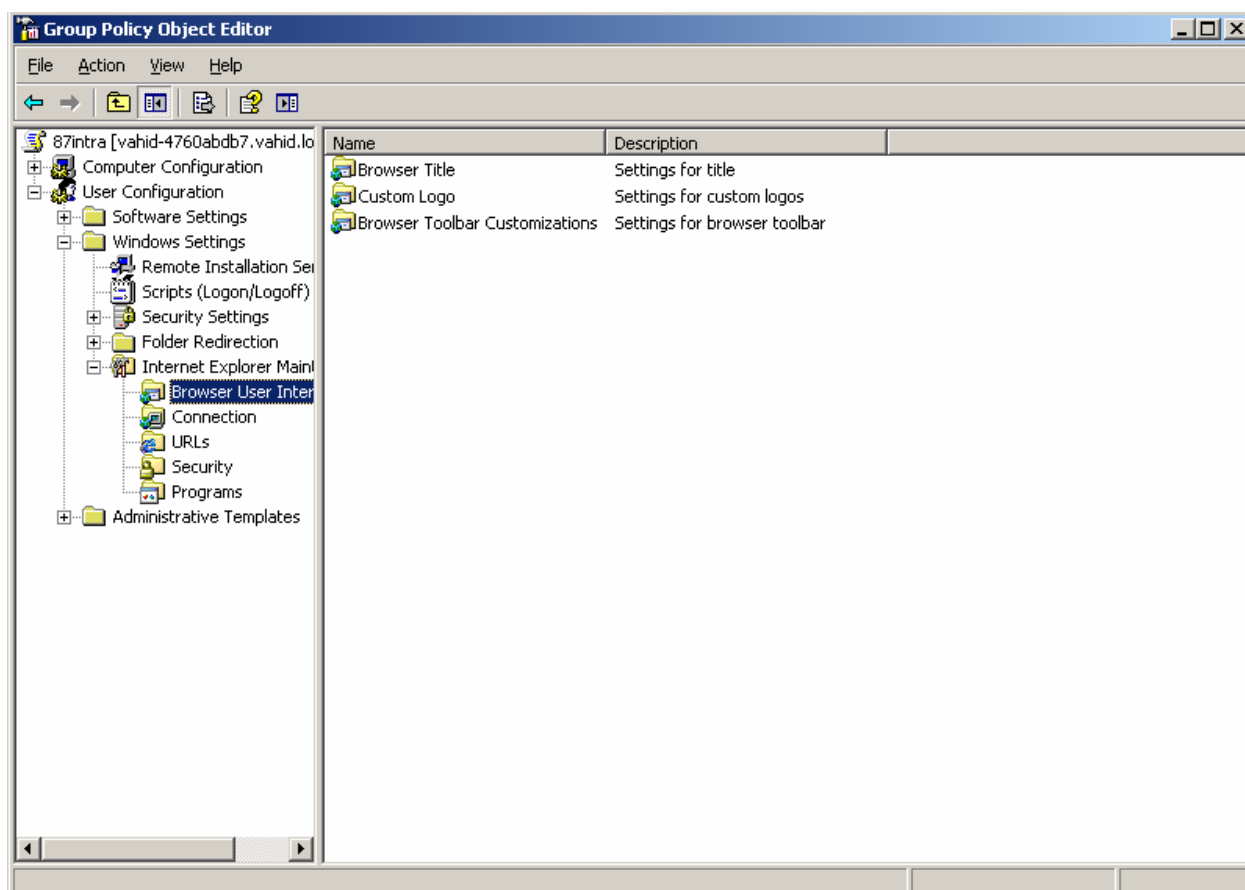
برای درک بهتر شما چند مثال را به صورت عملی انجام می دهیم تا بهتر مفهوم Group Policy را درک کنید.

تغییر Title Bar اینترنت اکسپلورر:

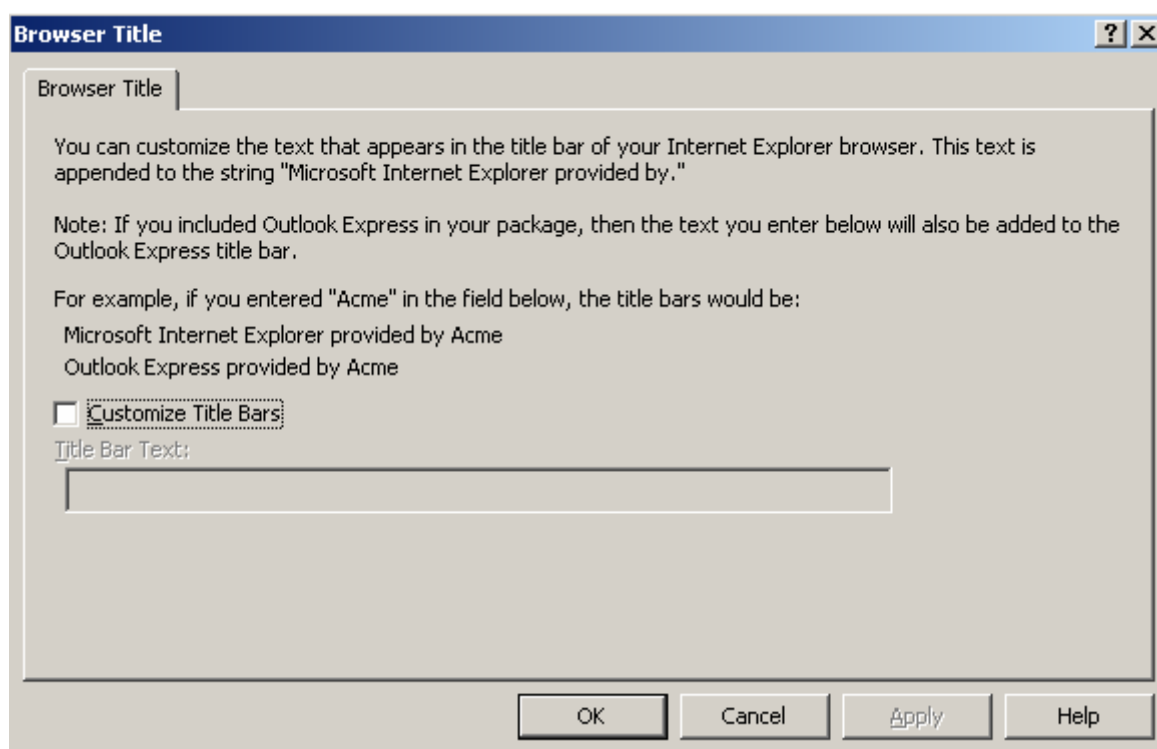
شاید بخواهید در صفحه اینترنت اکسپلورر تمام کاربرانی که در شبکه محلی از اینترنت استفاده می کنند ، نام سازمان خود را در Title bar ببینند. برای انجام این کار مراحل زیر را انجام دهید :

به مسیر زیر بروید:

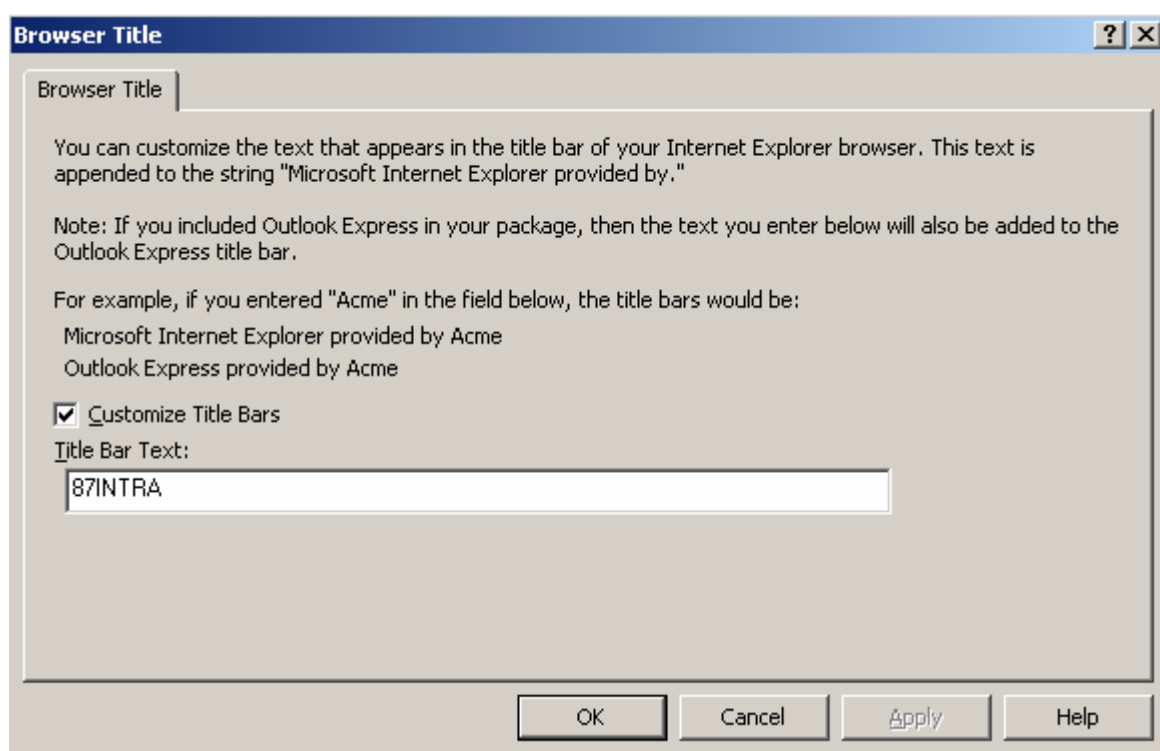
User Configuration \ Window Setting \ Internet Explorer Maintenance \
Browser User Interface\



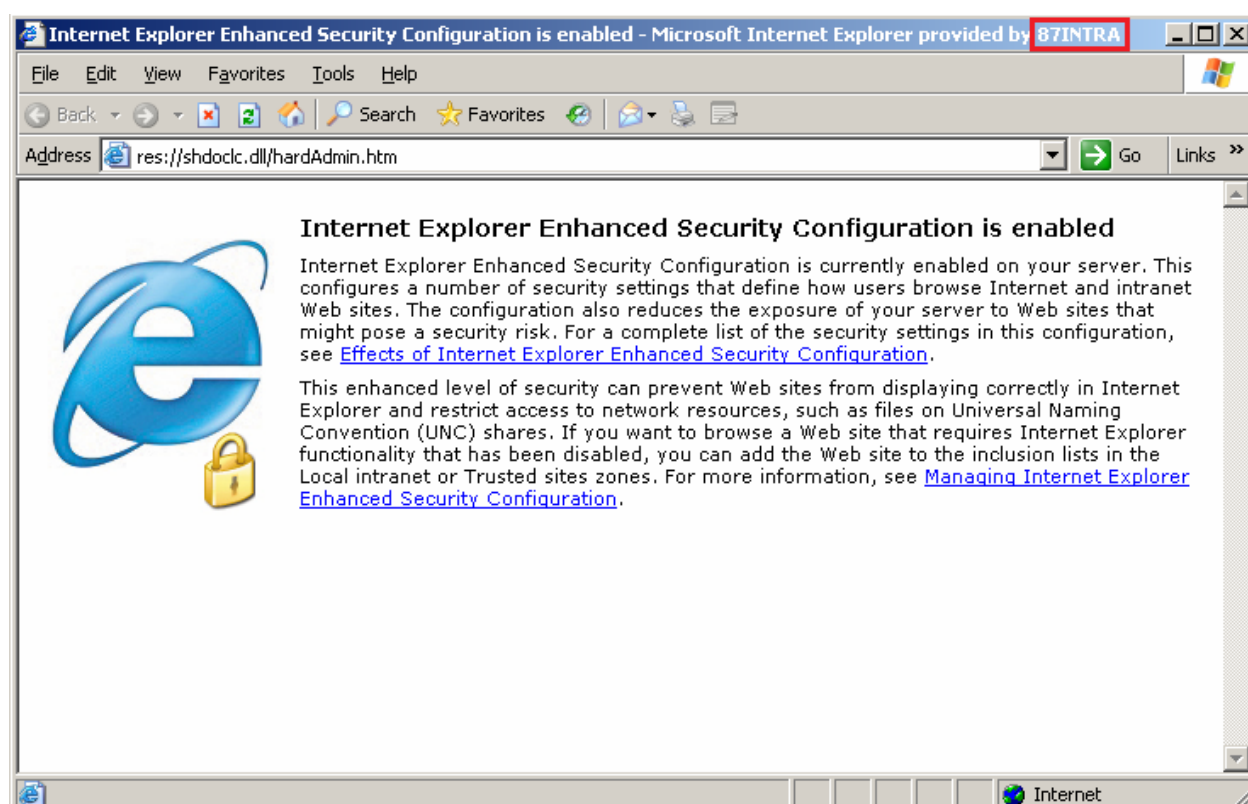
از صفحه سمت راست گزینه Browser Title را انتخاب کنید. پنجره زیر نمایش داده می شود.



ابتدا تیک مربوط به Customize Title Bars را زده و متن دلخواه خود را داخل Title Bar Text بنویسید.



بعد از انجام این کار وقتی کاربری در این سازمان وارد Domain شد هر وقت پنجره Internet Explorer را باز کرد نام سازمان خود را در قسمت Title Bar خواهد دید.

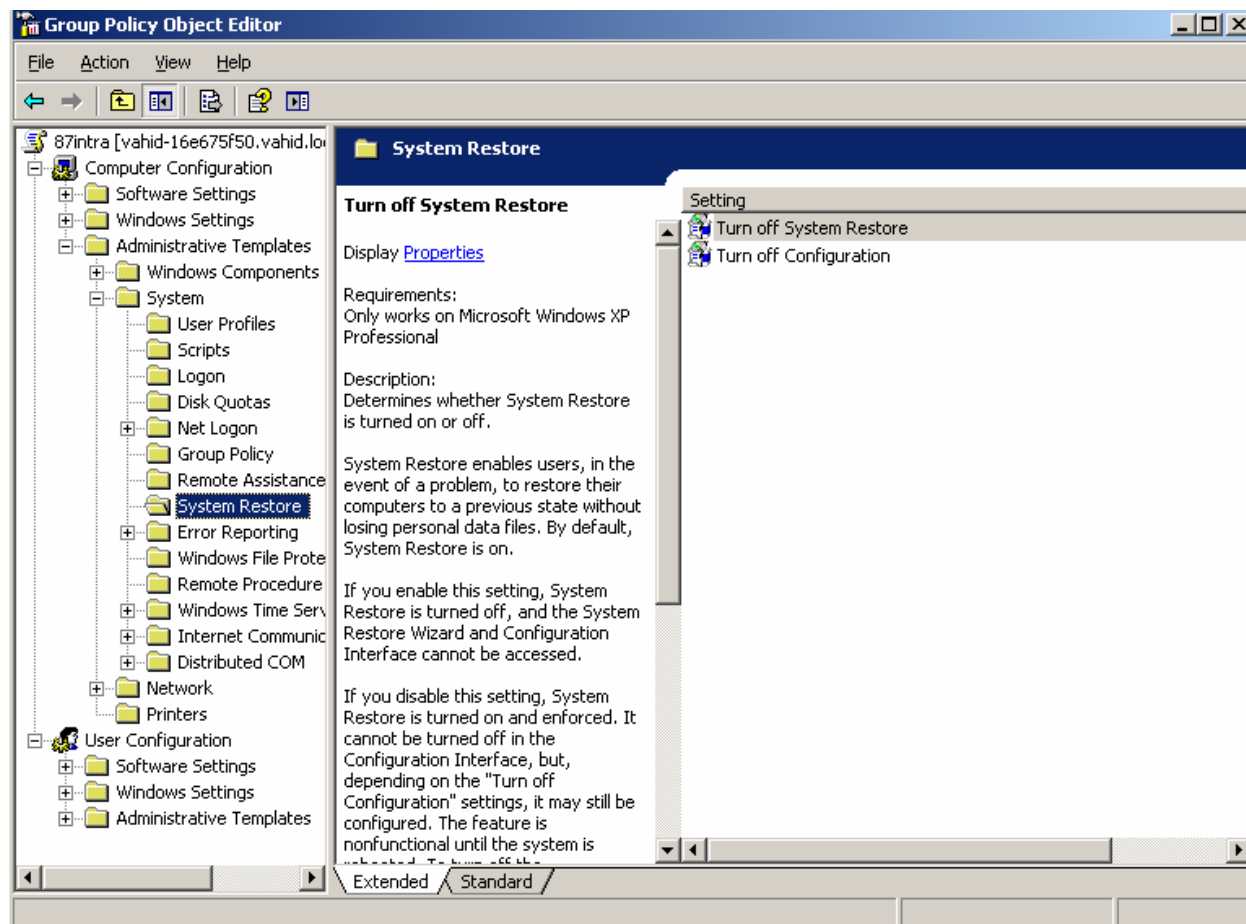


غیر فعال کردن System Restore :

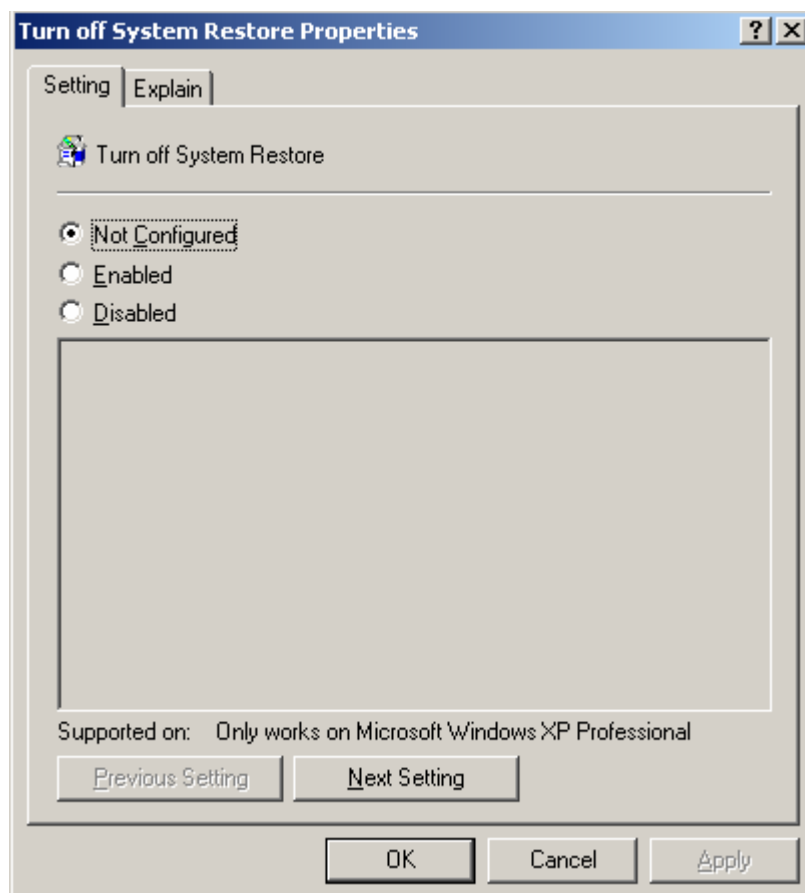
اگر می خواهید به کامپیوتر های موجود در این سازمان اجازه Restore کردن تنظیمات را ندهید این مراحل را طی نمایید:

به مسیر زیر بروید:

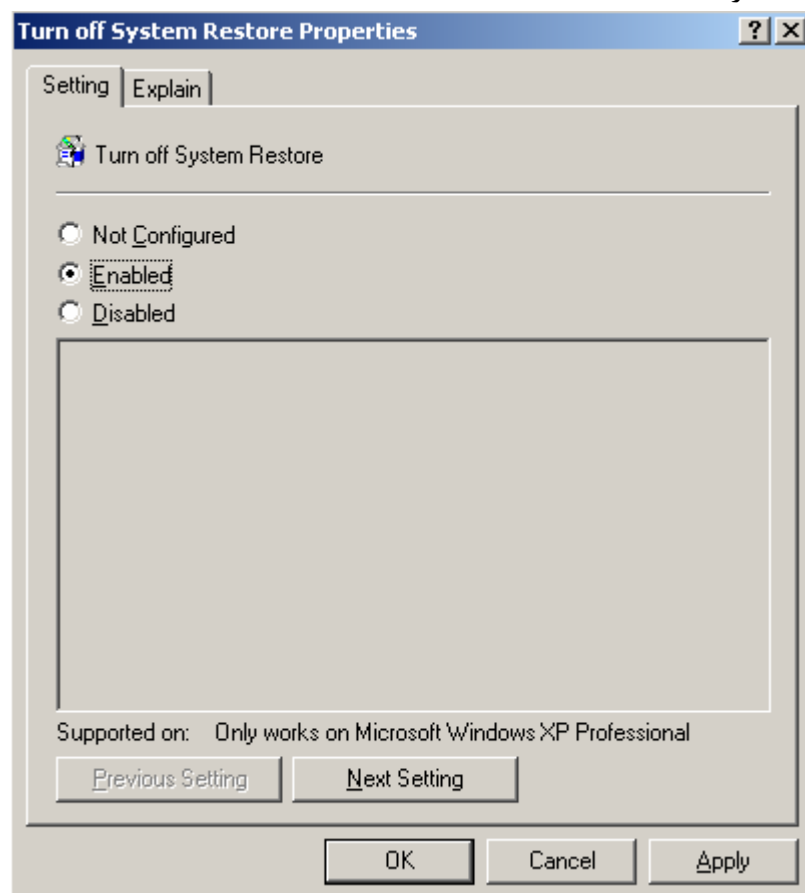
Computer Configuration \ Administrative Templates \ System \ System Restore\



از صفحه سمت راست گزینه Turn off System Restore را انتخاب کنید. پنجره زیر نمایش داده می شود.



در این پنجره گزینه Enabled را انتخاب کنید.



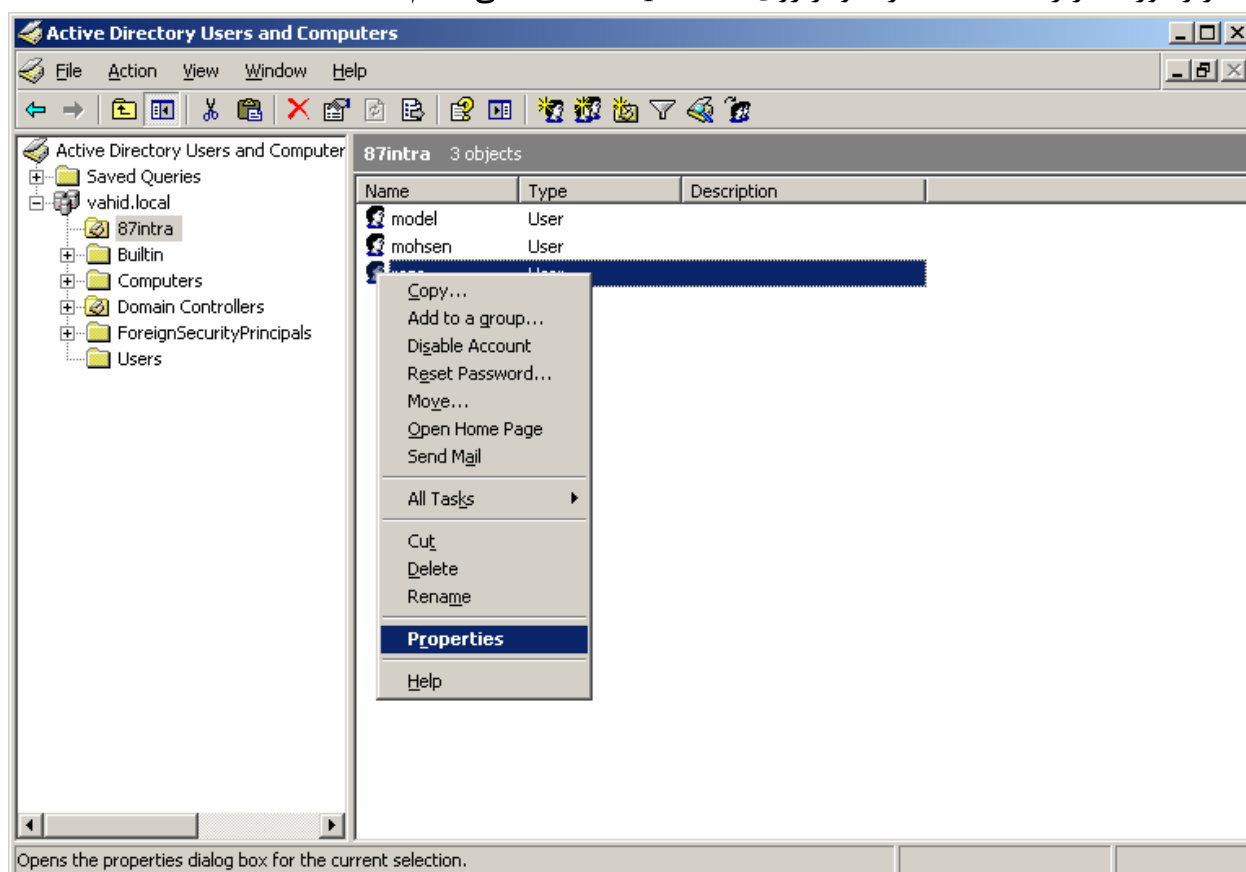
بعد از انجام این کار هیچ کدام از کاربران Domain از کامپیوترهای موجود در این سازمان نمی توانند از System Restore استفاده نمایند.

۴-۶- افزودن مدیر جدید در سطح دامنه:

در سطح سرور فقط یک مدیر (administrator) وجود دارد اگر بخواهیم مدیری را اضافه کنیم به عنوان مدیر فرعی می باشد. مدیر فرعی برای وارد شدن به خود سرور و کاربر برای وارد شدن از کلاینت به دامنه می باشد. در این قسمت ما قصد داریم تا کاربری را که قبلاً ایجاد کرده ایم به آن ویژگی Administrator بدهیم تا بتواند وارد سرور شود و بعضی از کارهای مدیریتی را انجام دهد.

برای دادن مجوز Administrator این مراحل را طی می نمایم:


بر روی کاربر مورد نظر راست کلیک کرده و بر روی Properties کلیک می کنیم.



در این پنجره بر روی زبانه Member Of کلیک می کنیم.

reza Properties [?] [X]

Member Of	Dial-in	Environment	Sessions
Remote control	Terminal Services Profile		COM+
General	Address	Account	Profile
	Telephones	Organization	

 reza

First name: Initials:

Last name:

Display name:

Description:

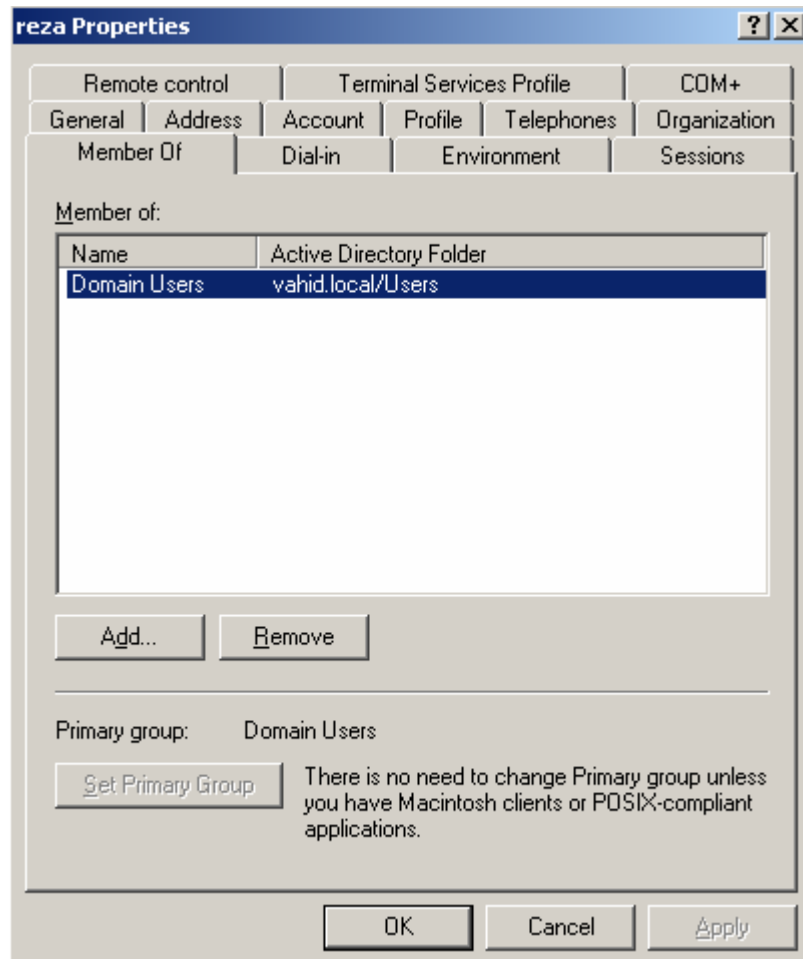
Office:

Telephone number:

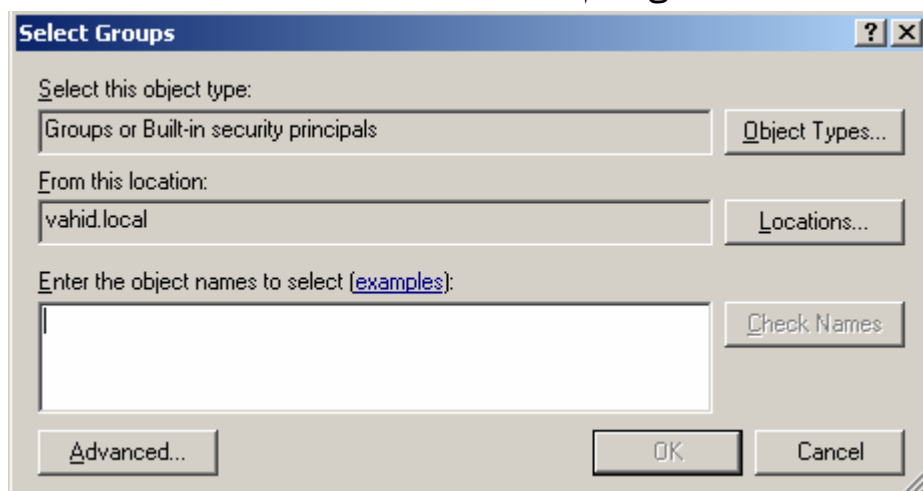
E-mail:

Web page:

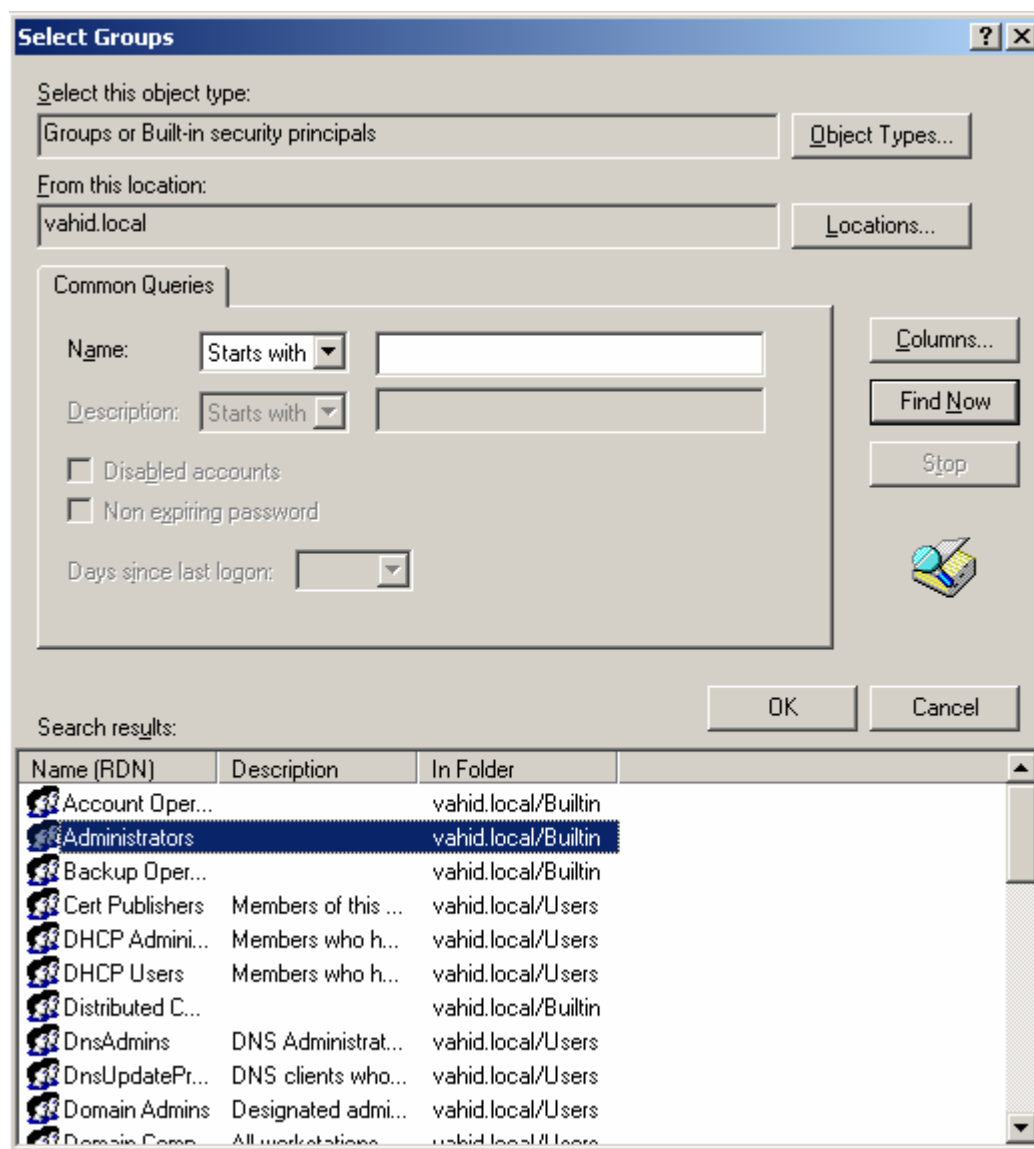
در این پنجره بر روی Add کلیک می کنیم.



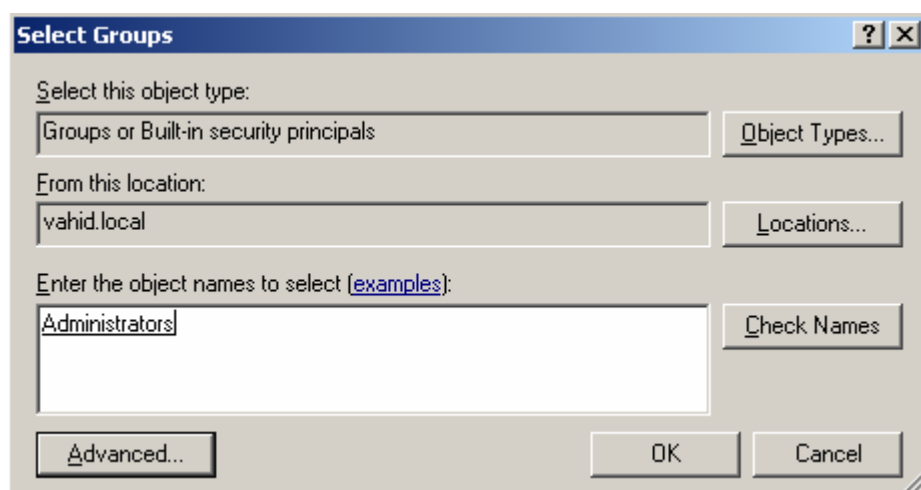
در این پنجره بر روی **Advanced** کلیک می کنیم.



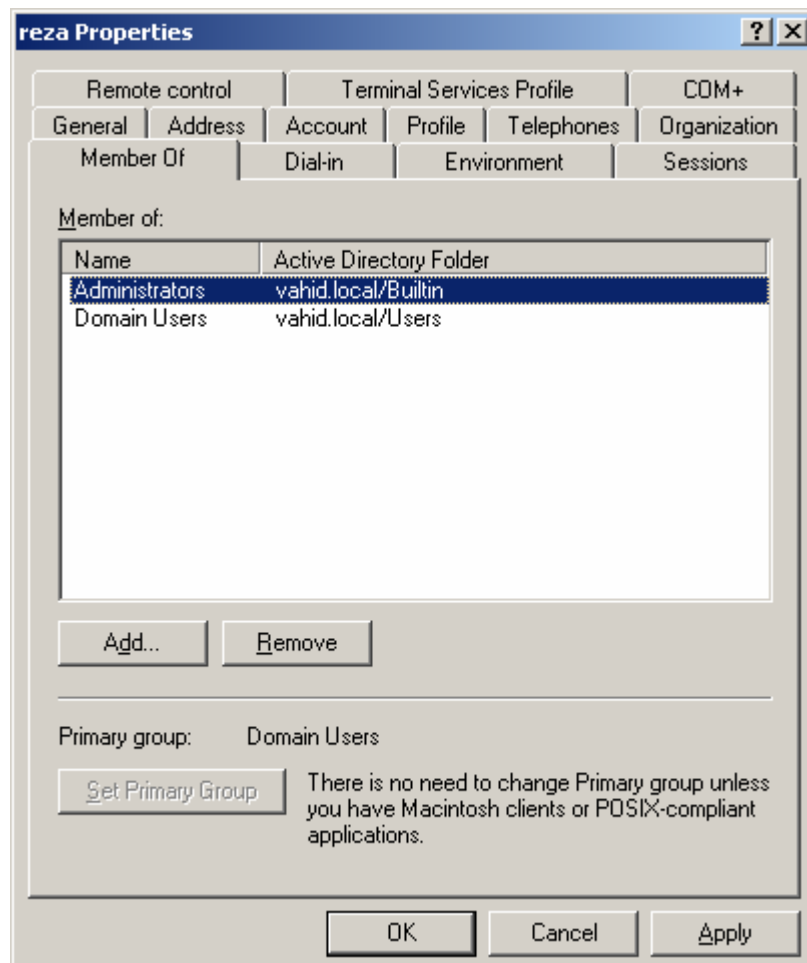
در این پنجره بر روی **Find Now** کلیک می کنیم.
در لیست نمایش داده شده **Administrator** را انتخاب و **OK** می کنیم.



OK را می زنیم.



در این پنجره نیز بر روی OK کلیک می کنیم.



بعد از انجام این مراحل کاربر Reza می تواند با عنوان مدیر فرعی وارد سرور شود و تغییرات اعمال کند.

Logoff می کنیم.

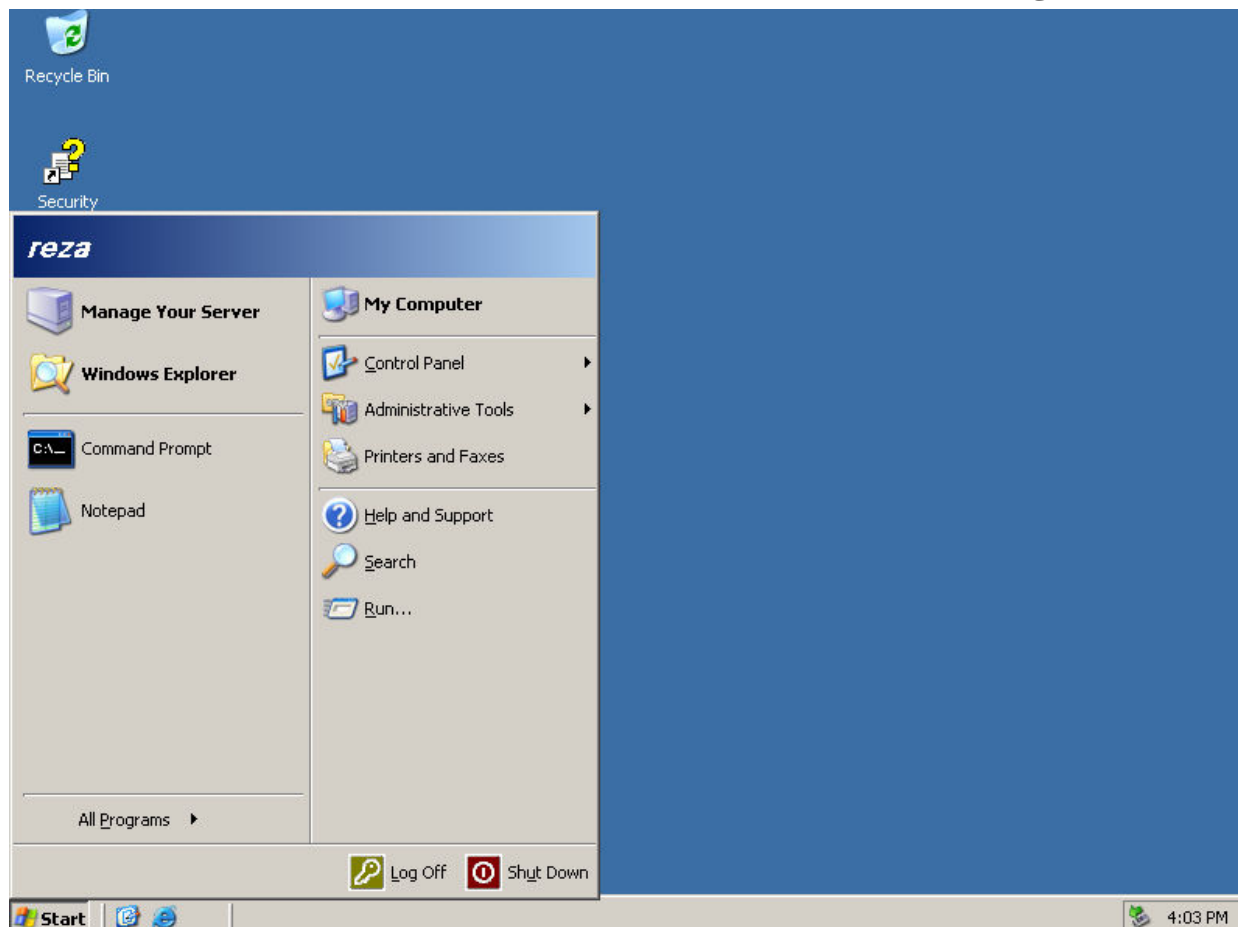
در پنجره زیر اول می خواهیم با نام Ashkan که قبلاً ایجاد کرده ایم وارد سرور شویم. مشاهده می کنید که پیغام خطایی مبنی بر اینکه این کاربر به عنوان administrator تعریف نشده است.



اکنون می خواهیم با نام کاربری Reza که آن را به عنوان مدیر فرعی تعریف کرده ایم وارد سرور بشویم.



همچنان که مشاهده می شود دیگر پیغام خطای قبلی ظاهر نمی شود. و desktop مدیر فرعی ایجاد شده (Reza) به صورت شکل زیر ظاهر می شود.



۵-۶- محدود کردن مدیران:

ما می توانیم کاربرانی را که در سطح دامنه، مدیر فرعی تعریف کرده ایم را محدود کنیم تا آنها موقعی که وارد سرور می شوند نتوانند آن کارها را انجام دهند.

برای محدود کردن مدیران فرعی به پنجره Group Policy Object Editor بروید:

اگر گزینه Computer Configuration را انتخاب کنید بخش Administrative Template وجود دارد که برای محدود کردن مدیران فرعی هنگام ورود به سرور بر روی کامپیوتر اعمال می شود. و اگر گزینه User Configuration را انتخاب کنید باز هم گزینه Administrative Template وجود دارد که برای محدود کردن کاربران، بر روی خود کاربران اعمال می شود.

بخش Administrative Template مربوط به پیکربندی سیستم عامل برای کاربران مدیران فرعی می باشد که توسط Admin ایجاد شده اند. و ما می خواهیم توسط مدیر اصلی آنها را محدود کنیم.

در بخش Computer Configuration چهار گزینه وجود دارد:

- ۱- Windows Components: با استفاده از این بخش می توان تنظیمات پیکربندی اجزای سیستم عامل را انجام داد.
- ۲- System: با استفاده از این بخش می توان امکاناتی همچون سهمیه بندی دیسک، رفتار اسکرپیت ورود و اجزای مختلف سیستم را تنظیم کرد.
- ۳- Network: در این بخش می توان برای گروه، سیاست های خاصی را در رابطه با شبکه انجام داد.
- ۴- Printers: در این بخش تنظیمات ریجستری مربوط به چاپگرهای شبکه می باشد.

بخش Administrative Template شامل پنج گزینه می باشد:

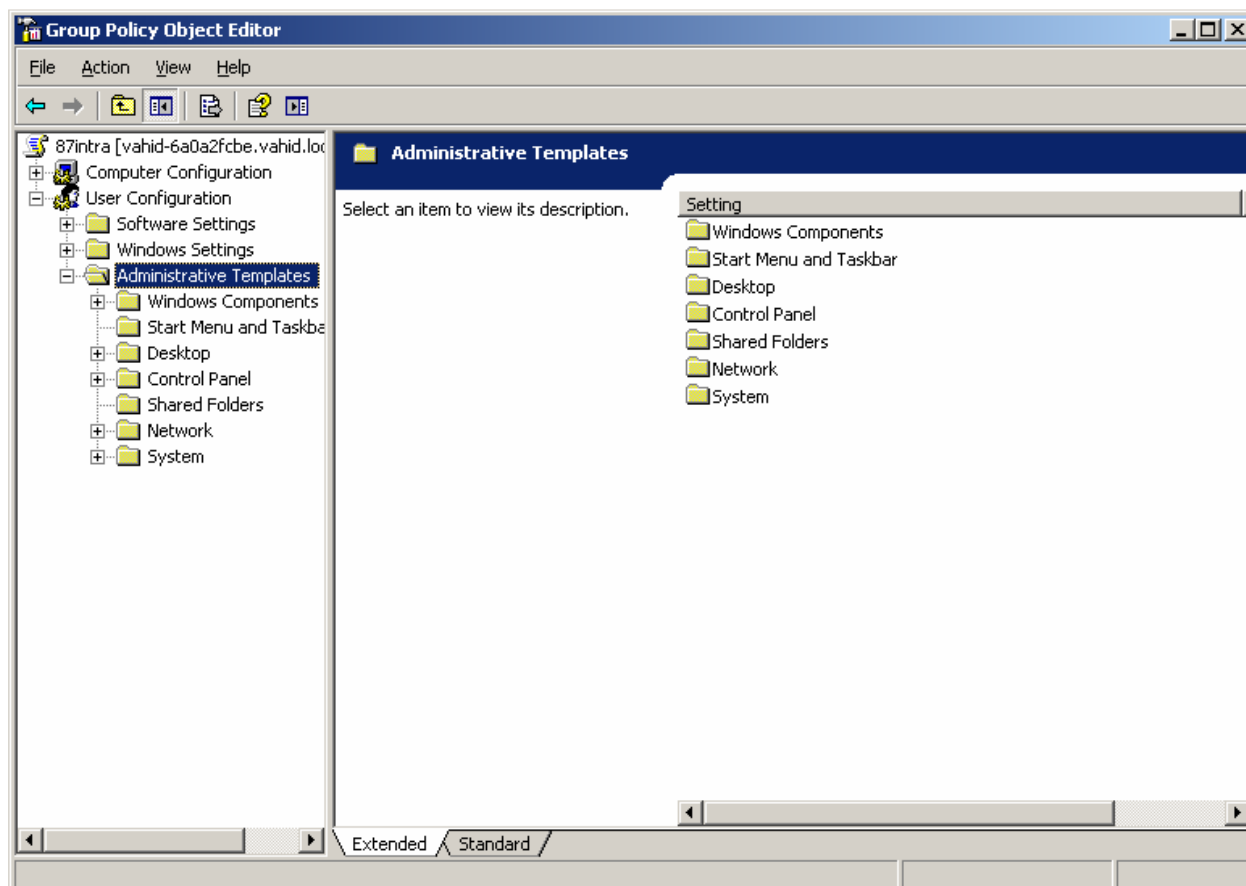
- ۱- Windows Components: با استفاده از این بخش می توان تنظیماتی را روی اجزای سیستم عامل مانند Task Scheduler, Windows Media Player و... را انجام داد.
- ۲- Start Menu and Taskbar: با استفاده از این بخش می توان تنظیماتی روی منوی Start و نوار وظیفه انجام داد.
- ۳- Control Panel: در این بخش می توان تنظیماتی را روی پانل کنترل کاربران مانند قابل مشاهده بودن Add/Remove Programs، انتخابهای زبان و دستیابی کاربر به پانل کنترل انجام داد.
- ۴- Network: در این بخش می توان برای گروه، سیاست های خاصی را در رابطه با شبکه انجام داد.
- ۵- System: با استفاده از این بخش می توان امکاناتی همچون سهمیه بندی دیسک، رفتار اسکرپیت ورود و اجزای مختلف سیستم را تنظیم کرد.

یک مثال را در رابطه با محدود کردن مدیران فرعی را انجام می دهیم تا بهتر مفهوم آن را درک نمایید.

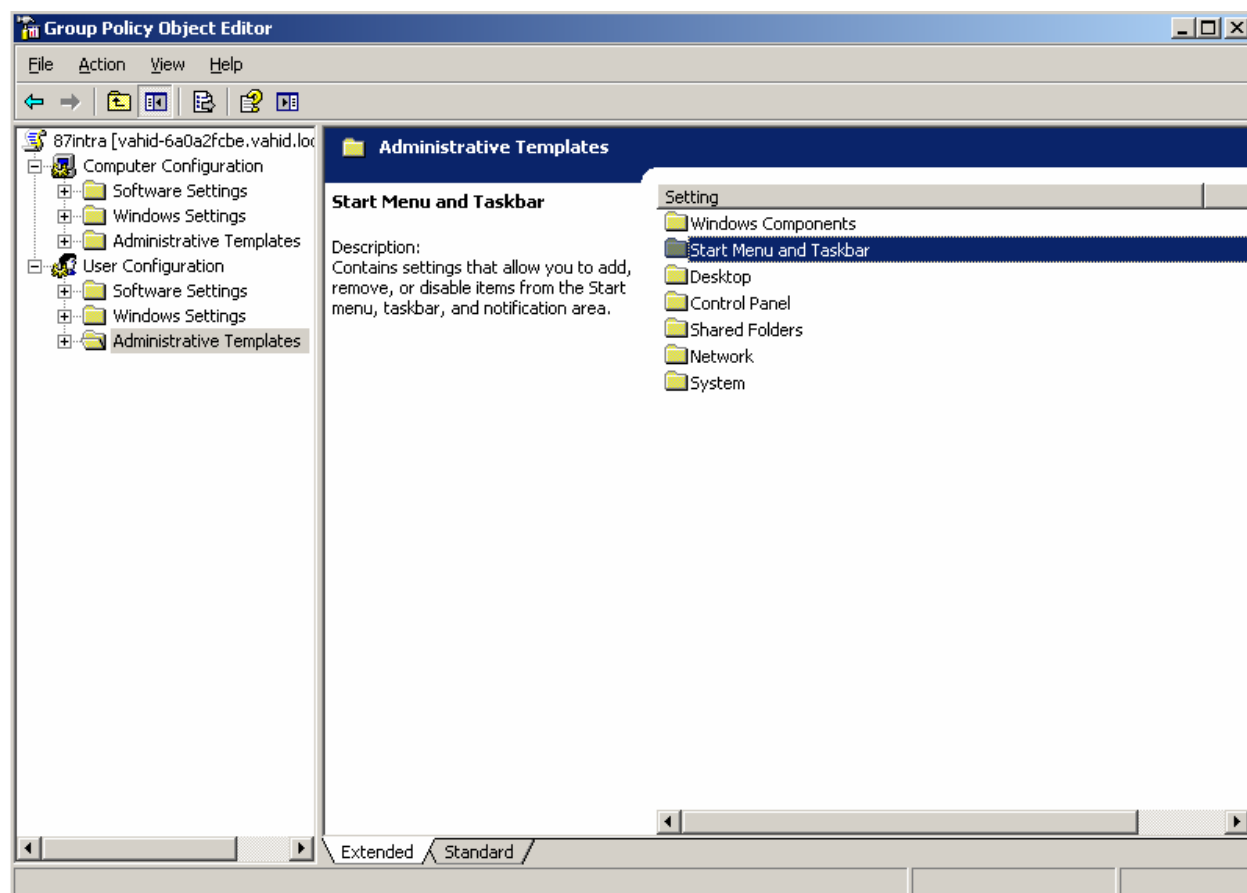
برای محدود کردن مدیران فرعی در پنجره Group Policy Object Editor به این مسیر بروید:

User Configuration>Administrative Templates

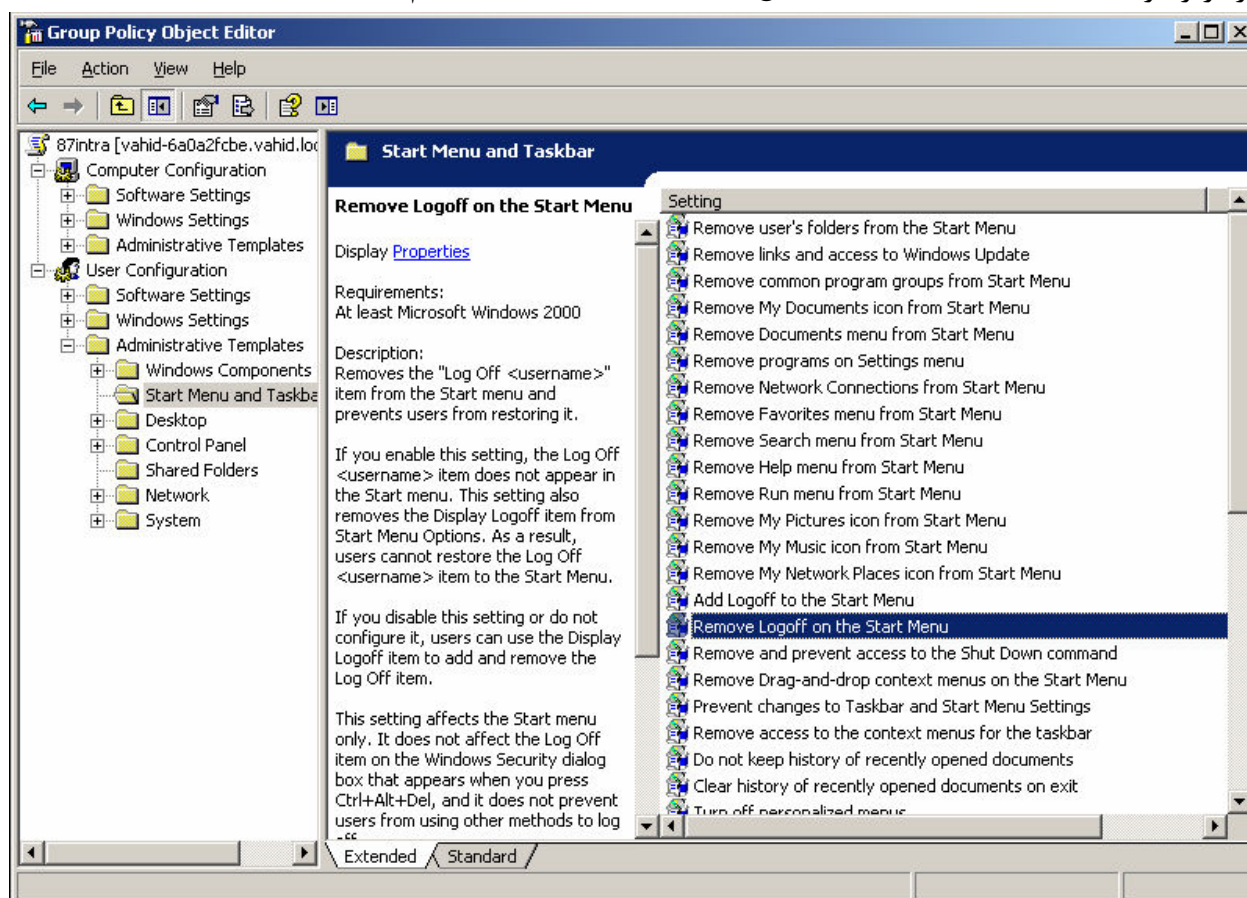
در داخل Administrative Templates لیست تنظیمات مختلفی وجود دارد که می توانیم برای مدیران فرعی اعمال کنیم.



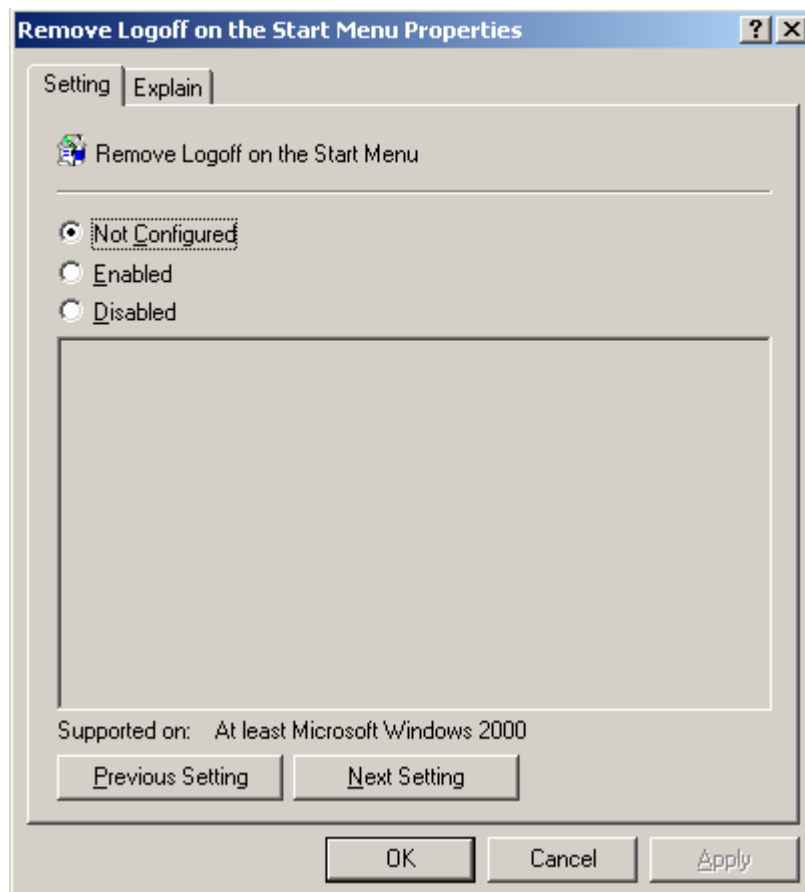
به عنوان مثال می خواهیم گزینه Logoff را از منوی Start حذف کنیم تا وقتی مدیر فرعی وارد سرور می شود نتواند Logoff کند.
در Administrative Templates بر روی Start Menu and Taskbar کلیک میکنیم.



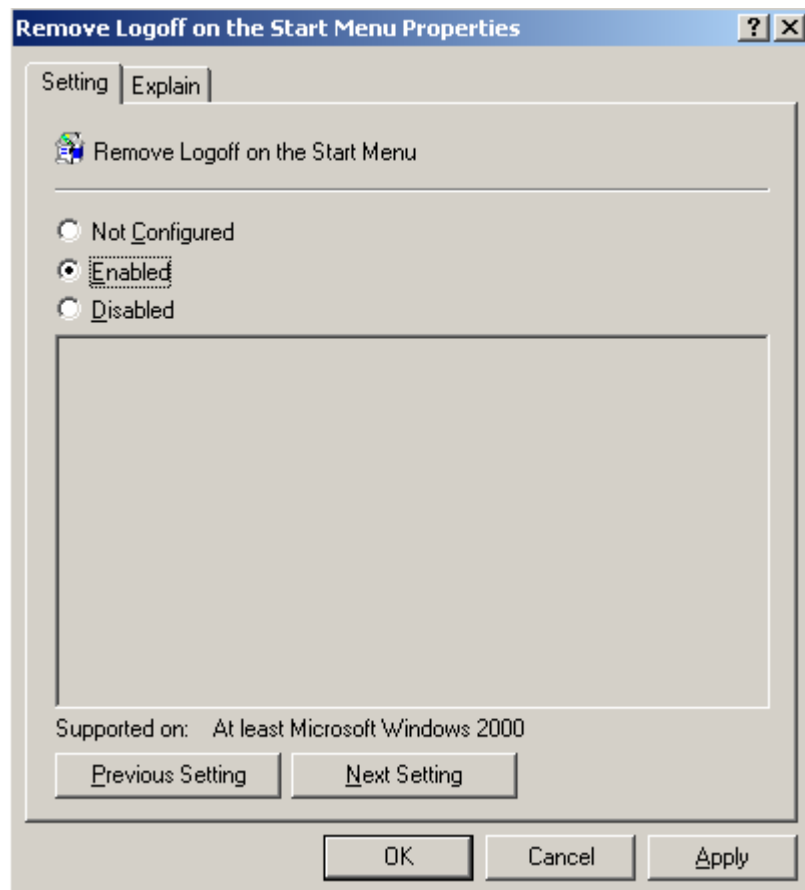
در پنجره زیر گزینه Remove Logoff on the Start Menu کلیک میکنیم.



در پنجره زیر گزینه Enabled را انتخاب می کنیم. یعنی با انتخاب این گزینه فعال می کنیم حذف Logoff را از استارت منو.



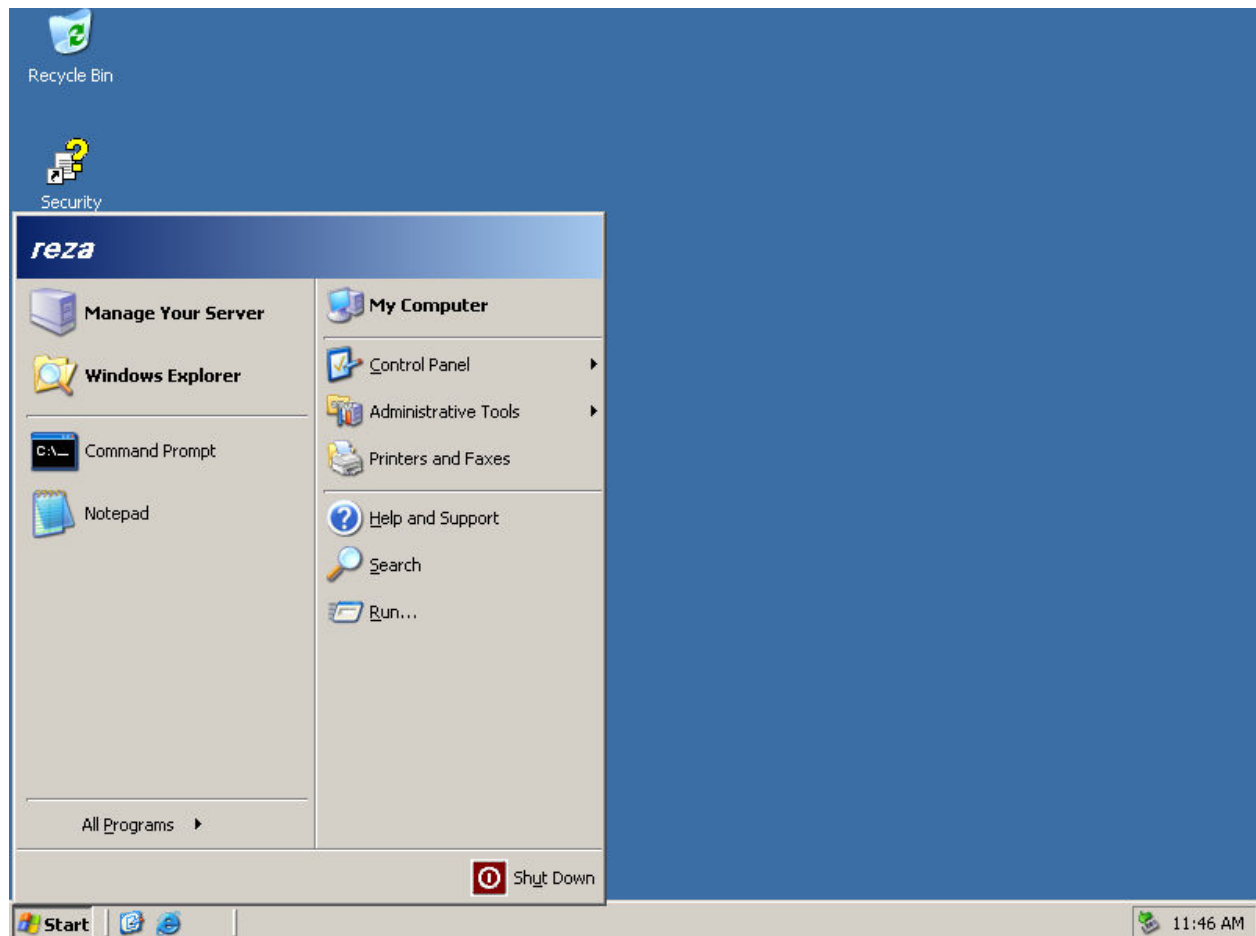
بعد از انتخاب Ok می کنیم.



اکنون می خواهیم با نام کاربری Reza که قبلاً آن را به عنوان مدیر فرعی تعریف کرده ایم وارد سرور شویم.



در پنجره زیر مشاهده می کنید که گزینه Logoff در استارت منو نمایش داده نمی شود.

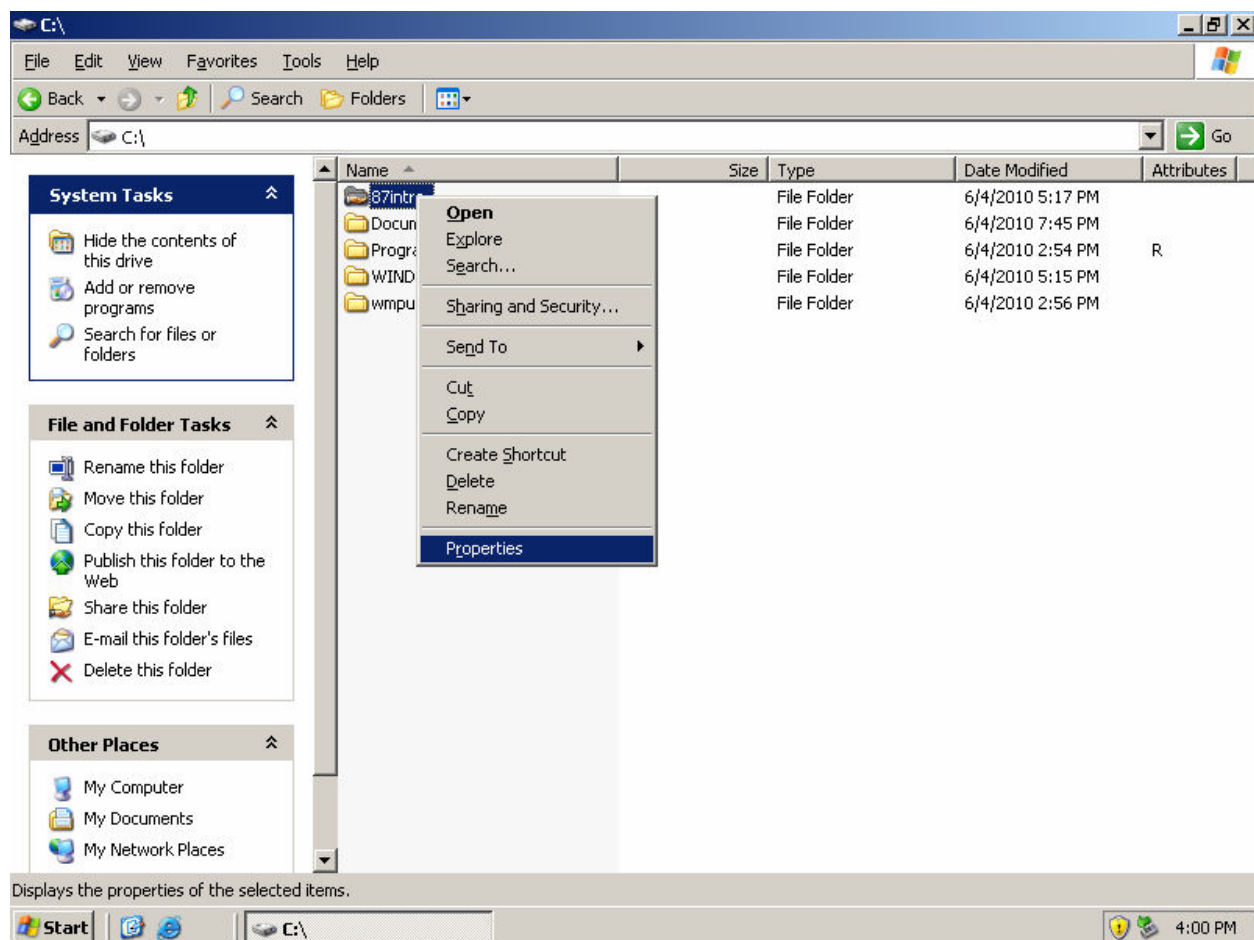


۶-۶- مدیریت مجوزها و بررسی انواع مجوز:

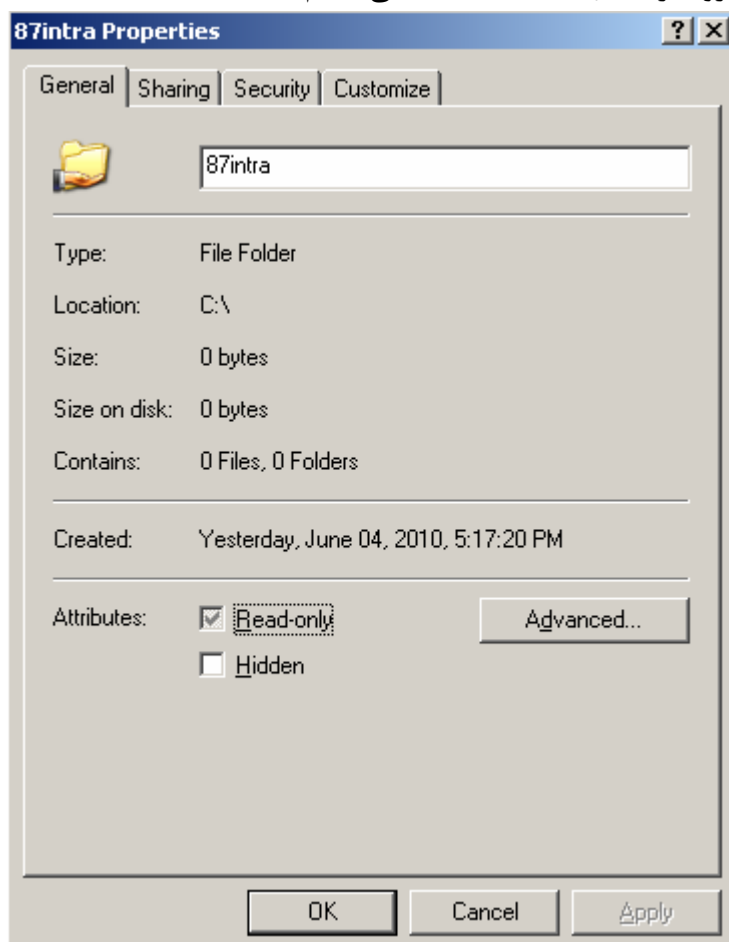
در این بخش می خواهیم مجوز های دستیابی به فایل های اشتراکی را بررسی کنیم. وقتی پوشه ای را بر روی سرور به اشتراک می گذاریم به طور اتوماتیک مجوز هایی برای دستیابی کاربران به پوشه ایجاد می شود. به طور پیش فرض همه کاربران فقط اجازه خواندن فایل را دارند و نمی توانند در آن تغییرات اعمال کنند، فقط کاربر Administrator همه جوازهای دستیابی را دارد.

اگر بخواهیم جواز کاربری را برای دستیابی به پوشه اشتراکی را افزایش یا کاهش دهیم این مراحل را انجام می دهیم:

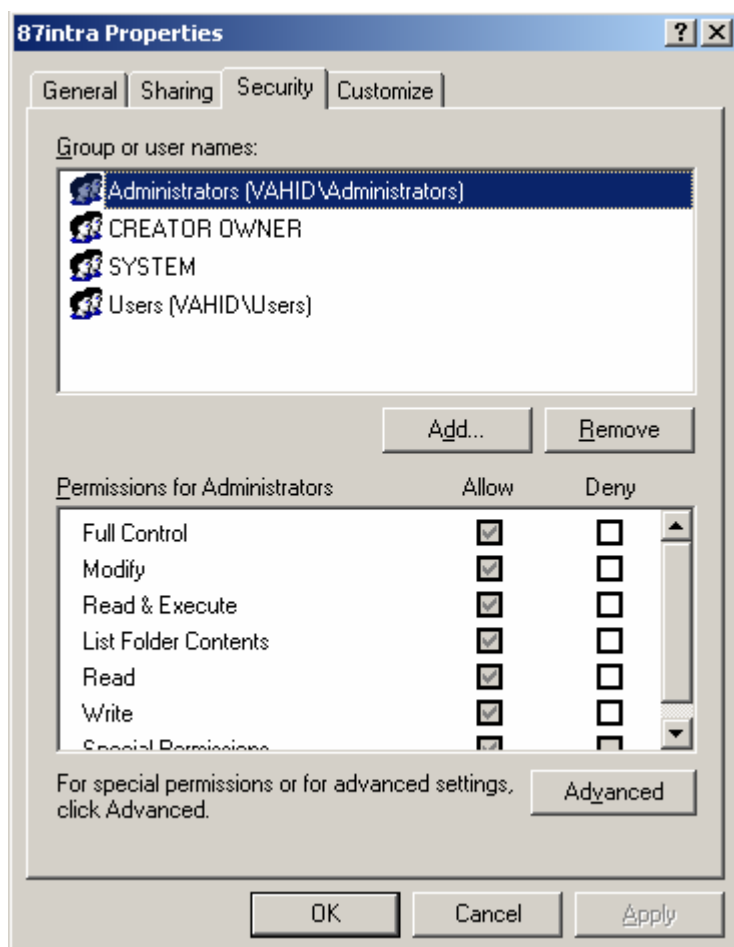
بر روی پوشه اشتراکی راست کلیک و Properties را انتخاب می کنیم.



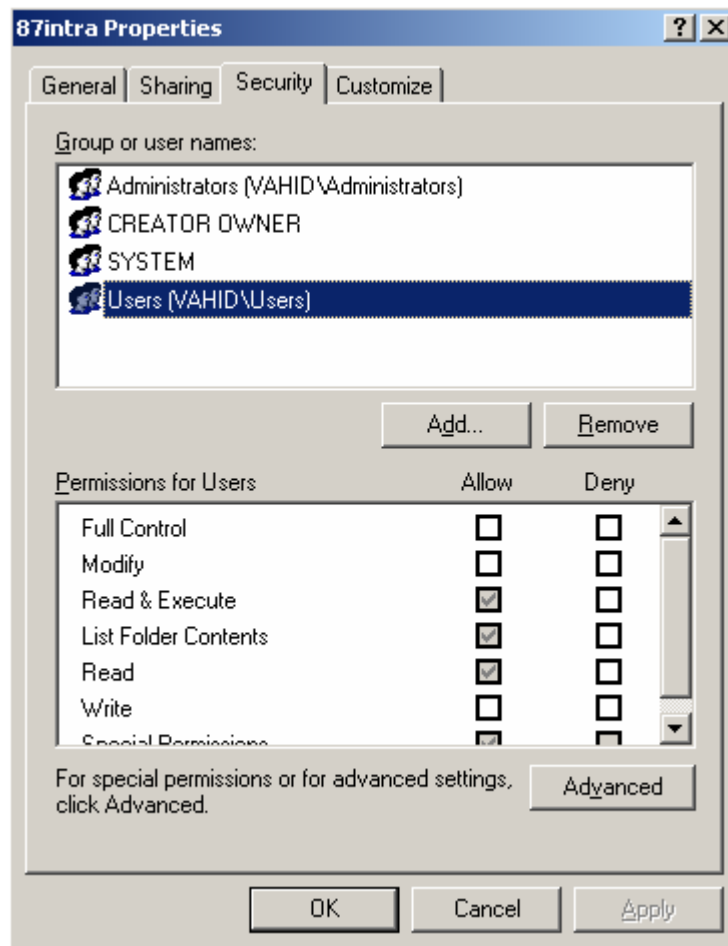
در پنجره نمایش داده شده بر روی زبانه Security کلیک می کنیم.



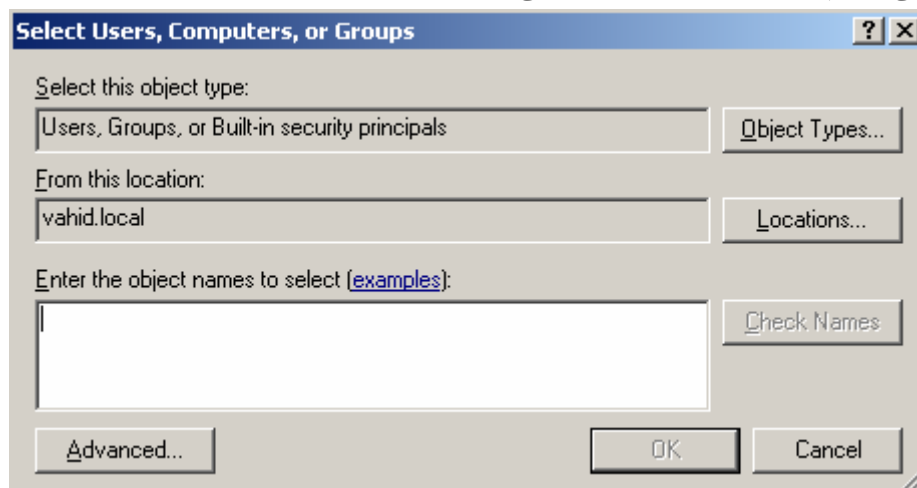
در پنجره زیر مشاهده می کنید که Administrator همه جوازهای دستیابی را دارد.



اگر بر روی User کلیک کنید می بینید که کاربران فقط بعضی از مجوز ها را دارند که البته می توانید آن را افزایش دهید. (اگر افزایش دهیم بر روی همه کاربران اعمال می شود)
 Read&Execute: جواز خواندن و اجرا کردن
 List Folder Contents: فهرست کردن محتویات پوشه
 Read: خواندن



حال می خواهیم به کاربری خاص مجوز های دستیابی را افزایش یا کاهش دهیم.
بر روی Add کلیک می کنیم، پنجره زیر نمایش داده می شود.



بر روی Advanced کلیک می کنیم تا لیست کاربران نمایش داده شود.

Select Users, Computers, or Groups [?] [X]

Select this object type:

From this location:

Common Queries


Name:

Description:

☐ Disabled accounts

☐ Non expiring password

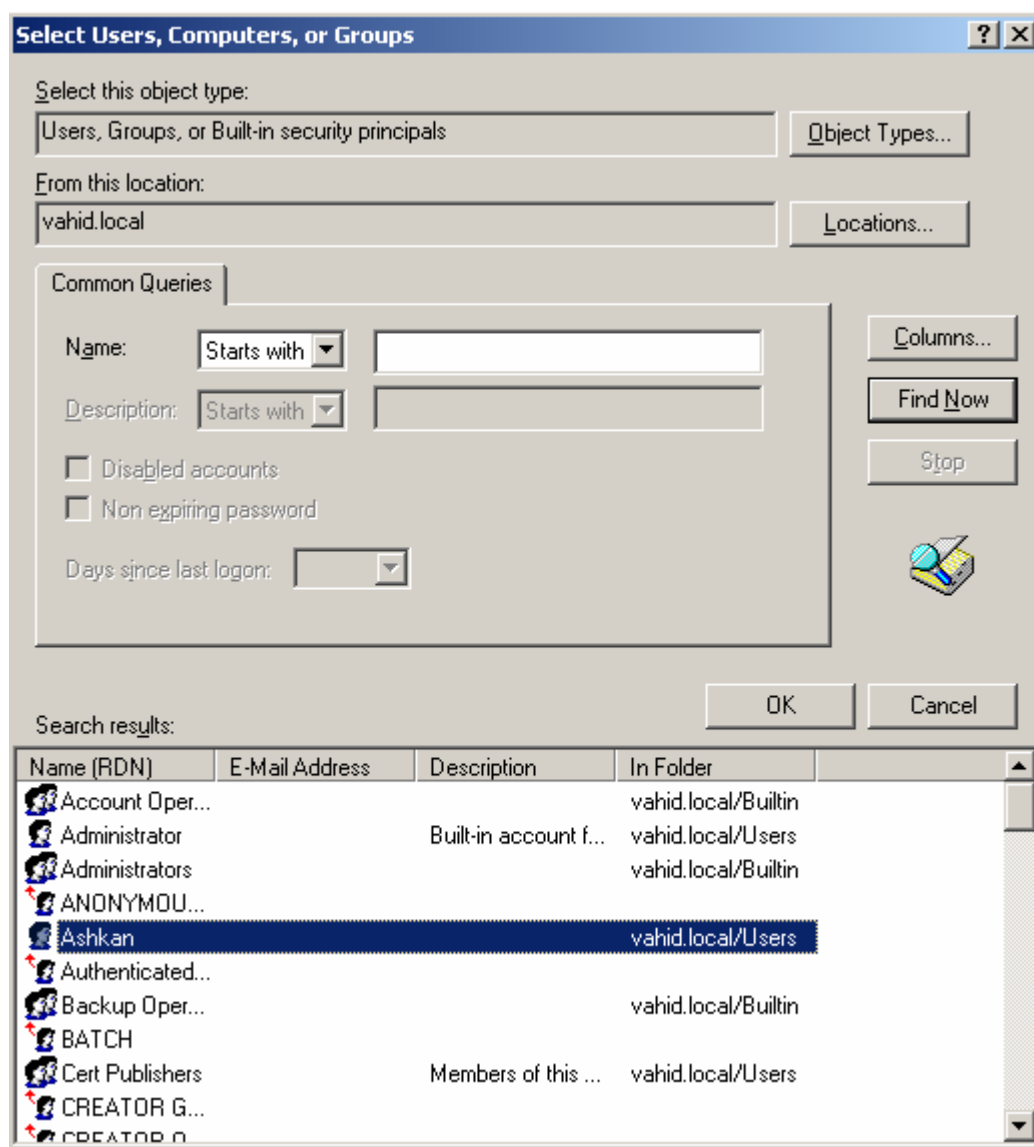
Days since last logon:



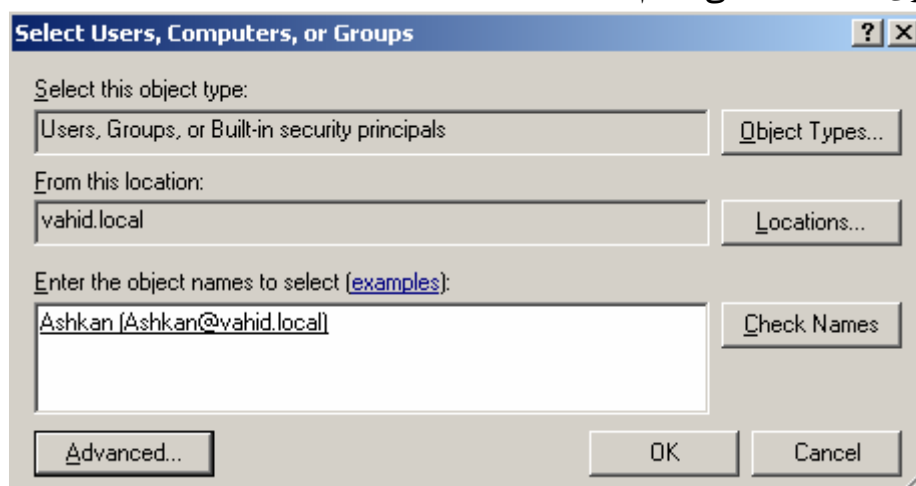
Search results:

Name (RDN)	E-Mail Address	Description	In Folder

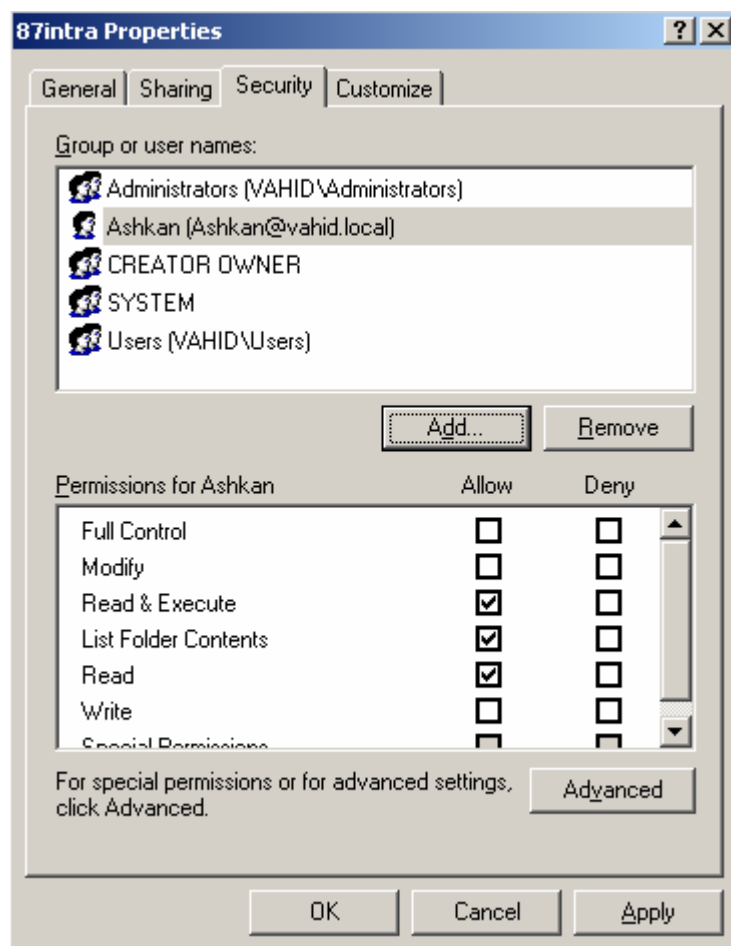
از لیست کاربران موجود کاربری را که می خواهیم مجوز دستیابی آن را افزایش دهیم انتخاب و بر روی OK کلیک می کنیم.



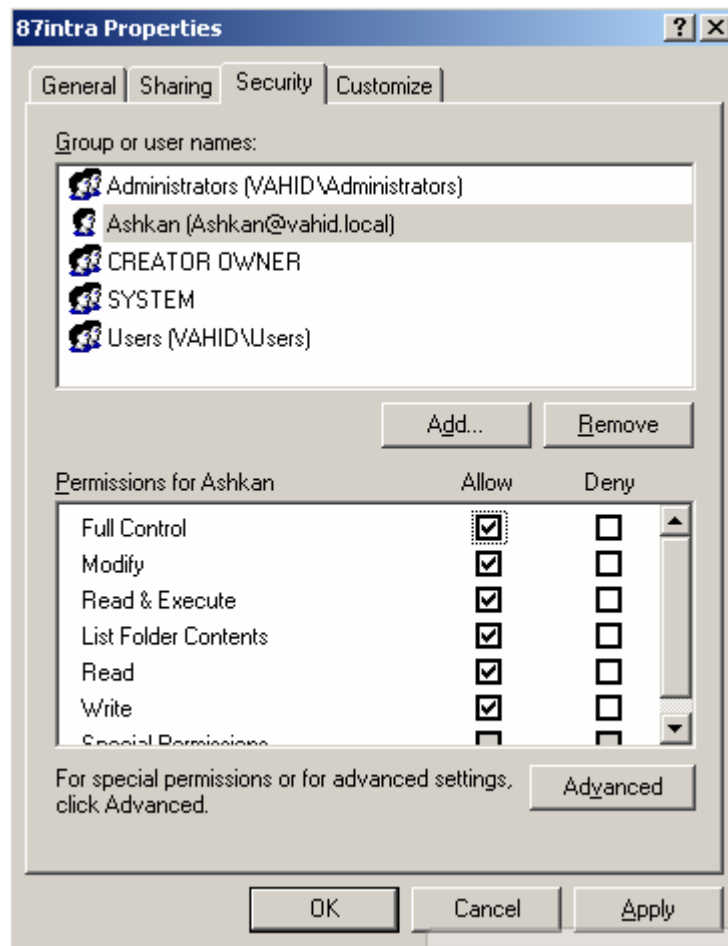
در این پنجره نیز بر روی OK کلیک می کنیم.



در این پنجره مشاهده می کنید که کاربر Ashkan به لیست اضافه شده است. اگر در لیست پایین تیک گزینه های Allow را قرار دهیم یعنی مجوز انجام آن کار را به کاربر داده ایم، اگر تیک را هم بر داریم یعنی کاربر مجوز انجام آن کار را ندارد.



همه جوازهای دستیابی را در اختیار این کاربر قرار می دهیم.



۷. جزئیات بخش ششم:

۷-۱- امنیت در ویندوز ۲۰۰۳ سرور:

امنیت: شناخت آسیب ها و جلوگیری از نفوذ افراد غیر مجاز به شبکه یا کامپیوتر

مکانیزم تعیین اعتبار و اهراز هویت در ویندوز ۲۰۰۳ سرور:

ویندوز ۲۰۰۳ سرور برای اهراز هویت از دو پروتکل اصلی استفاده می نماید:

- پروتکل کربروس Kerberos v5
- NTLM

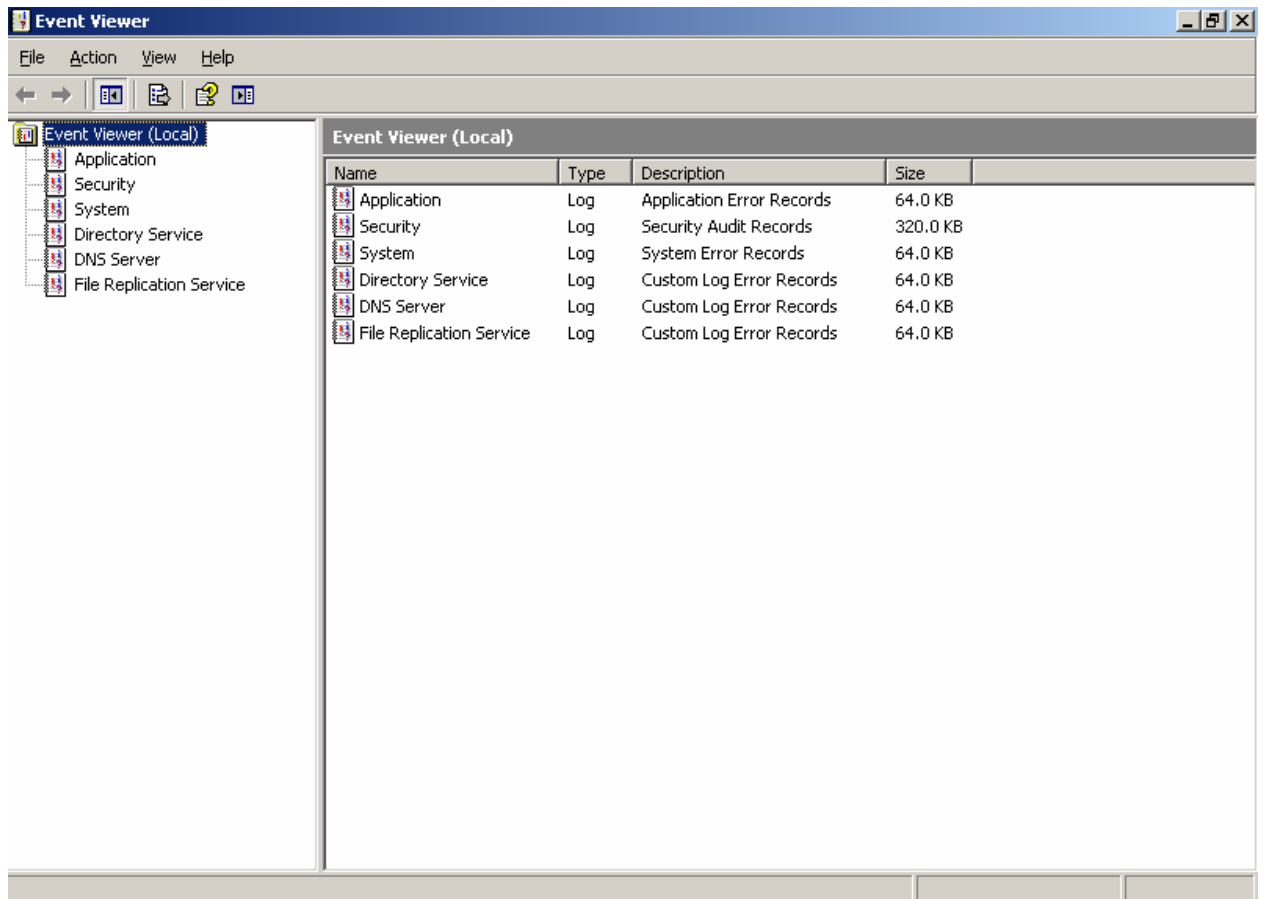
در بحث امنیت ۲۰۰۳ سرور مختلف تب های امنیتی وجود دارد که در اینجا ما به توضیح برخی از آنها می پردازیم:

۱-۷-امنیت با Event Viewer:

در ویندوز ۲۰۰۳ سرور ابزاری به نام Event Viewer برای نگهداری گزارش رخدادها وجود دارد که در آنجا تمامی رخدادها که در سطح سرور اتفاق می افتد نگهداری می شود. برای اینکه بتوانید این رخدادها را مشاهده کنید به مسیر زیر بروید:

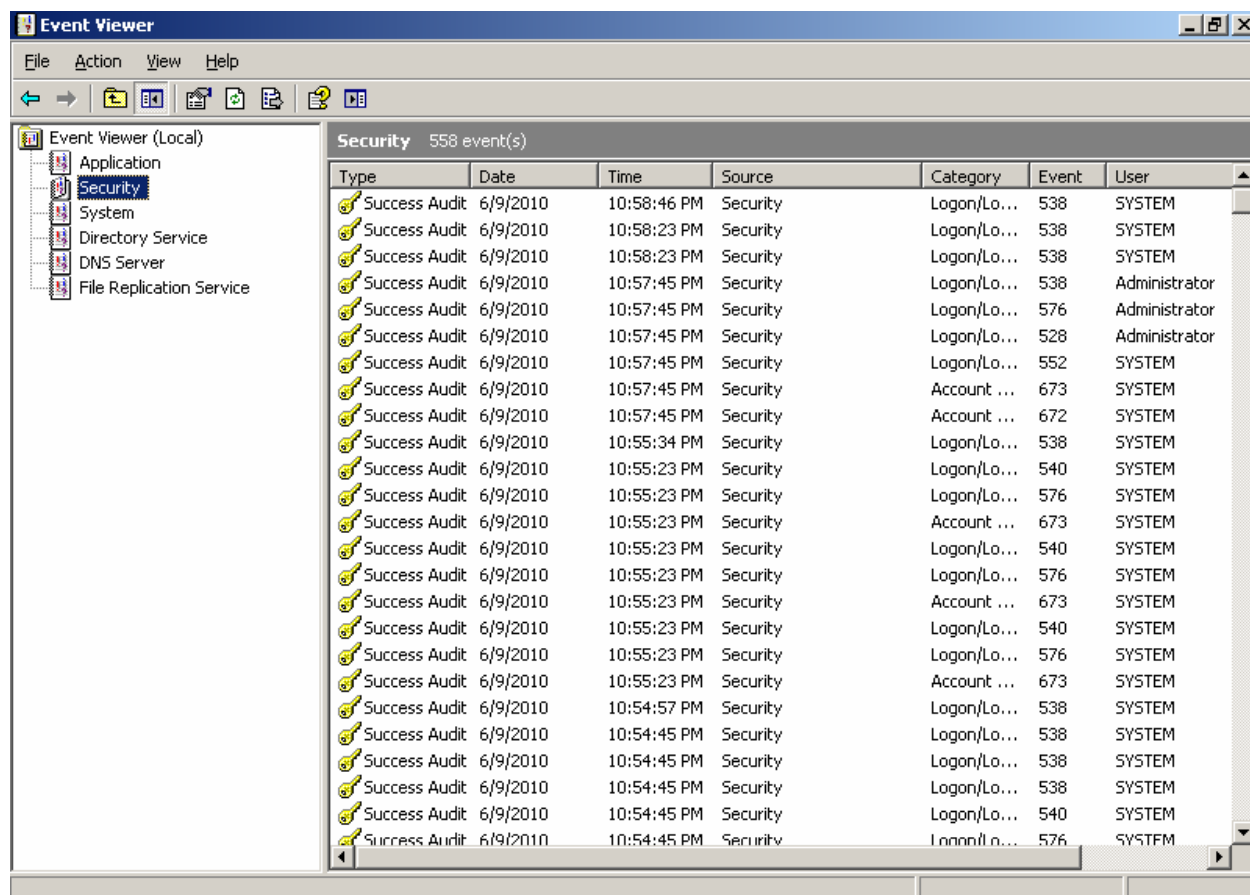
Start > Administrative Tools > Event viewer

پنجره زیر نمایش داده می شود.



در بخش Security علاوه بر اینکه تمامی رخدادها نگهداری می شود، بلکه تلاش ها برای استفاده های غیر مجاز در سطح سرور نیز به صورت هشدار در این بخش نگهداری می شود. گزارش های غیر مجاز می تواند شامل موارد زیر باشد:

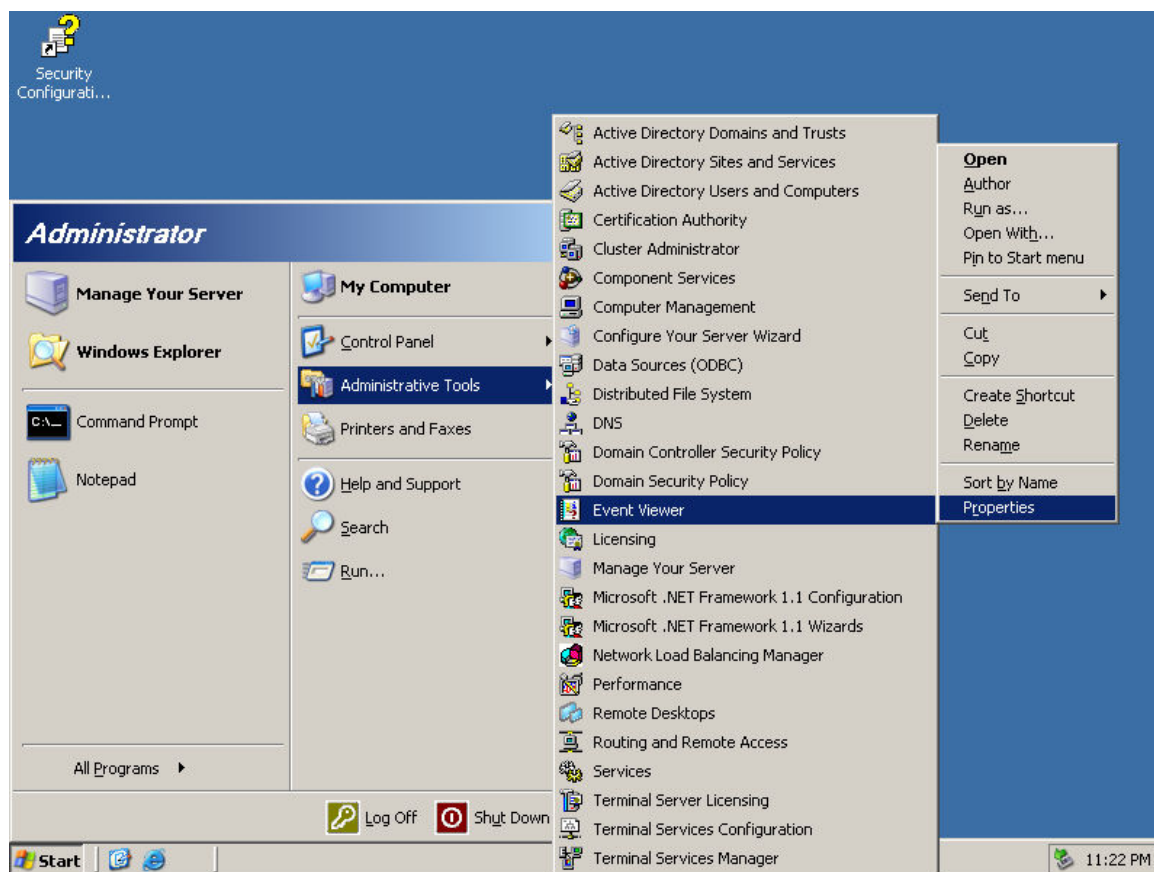
- تلاش های نامعتبر برای ورود
- استفاده ناموفق از امتیازها
- تلاش برای تغییر دادن امتیازات امنیتی
- تلاش برای خاموش کردن سرویس دهنده
- ...



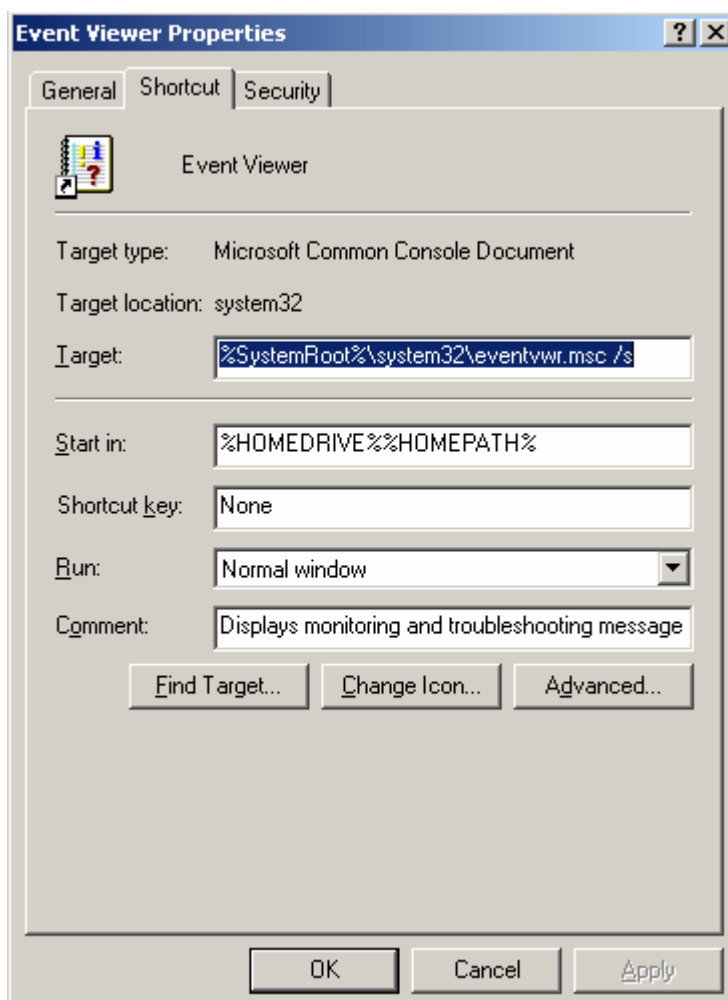
محافظت از ابزار Event Viewer:

به خاطر دلایل امنیتی لازم است که سطح دسترسی به این ابزار محدود شود (به صورت پیش فرض هر کسی که وارد سرور میشود می تواند به این ابزار دسترسی یابد) تا نتوانند گزارشات را غیر فعال یا پاک کنند. برای محدود کردن این مراحل را طی کنید:

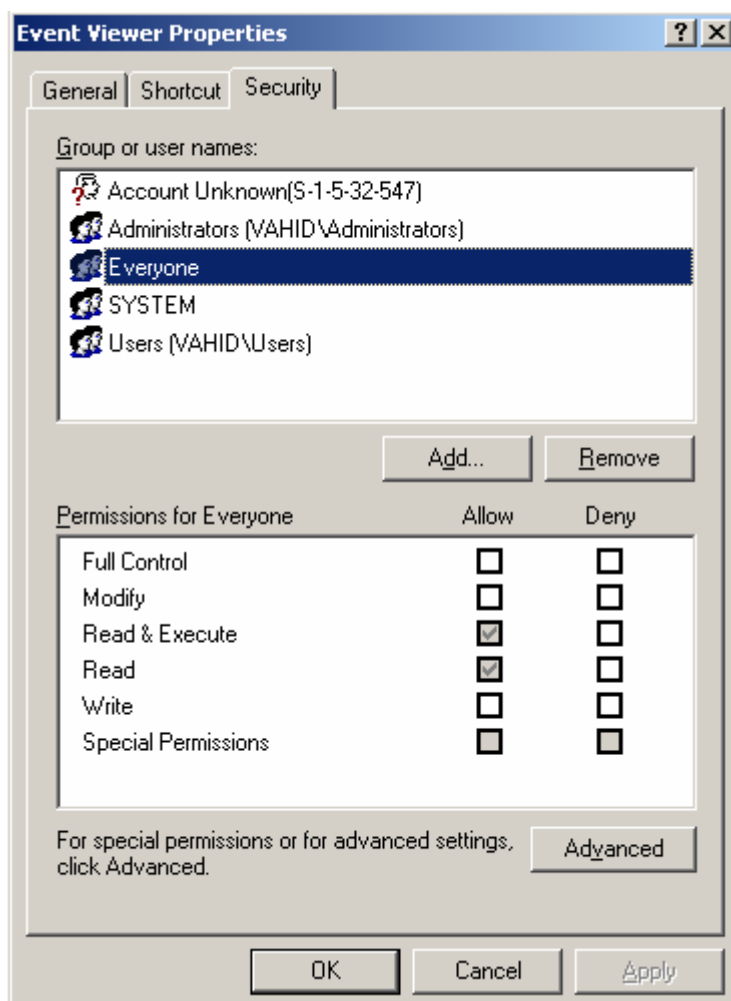
بر روی Event Viewer راست کلیک کرده و Properties را انتخاب کنید.



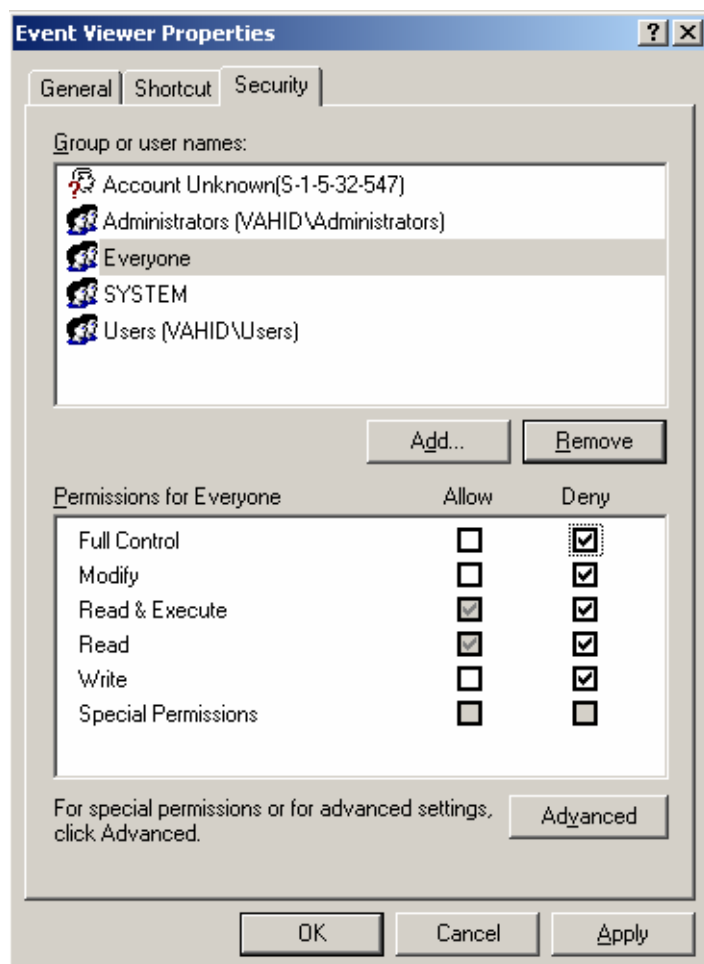
پنجره زیر ظاهر می شود بر روی زبانه Security کلیک کنید.



در این پنجره مشاهده می کنید که گروه Everyone به طور پیش فرض می تواند این فایل ها را بخواند.



برای محدود کردن در قسمت Permissions for Everyone، تیک Deny را جلوی گزینه Full Control قرار دهید. (مانند شکل زیر)



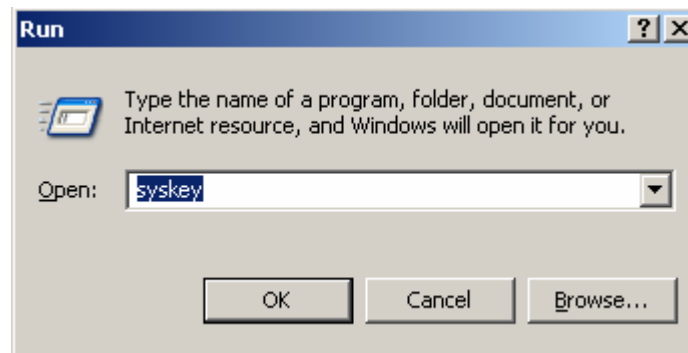
اگر بخواهید به کاربری خاص اجازه دسترسی دهید، می توانید بر روی Add کلیک کنید و آن کاربر را به این لیست اضافه و اجازه دسترسی آن را افزایش دهید.

۲-۱-۷- امنیت با Syskey:

کلید سیستم (Syskey) برای گذاشتن رمز دوم به کار می رود که به صورت پیش فرض بر روی ویندوز های XP، ۲۰۰۰ و ۲۰۰۳ نصب می شود ولی غیر فعال می باشد. اگر کلید سیستم را فعال کنید علاوه بر اینکه از کاربر هنگام ورود رمز عبور کاربری پرسیده می شود بلکه باید رمز Syskey را نیز وارد نماید.

اگر بخواهید Syskey را فعال کنید این مراحل را طی نمایید:

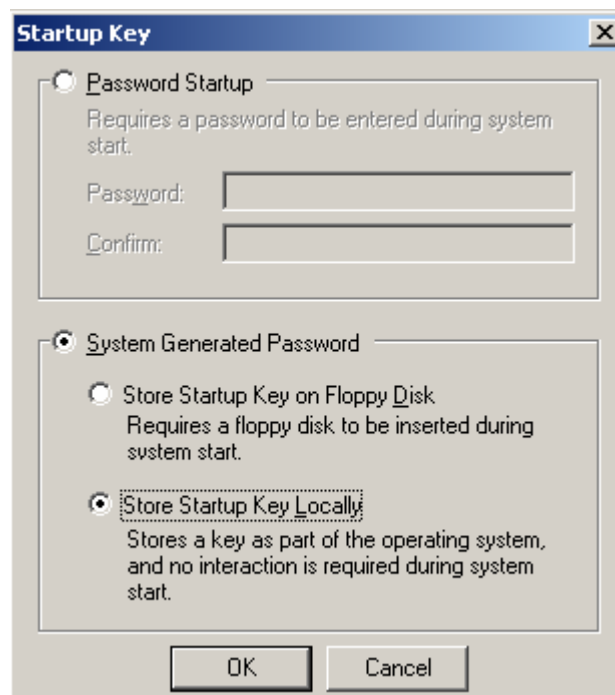
در قسمت Run عبارت Syskey را تایپ و OK کنید.



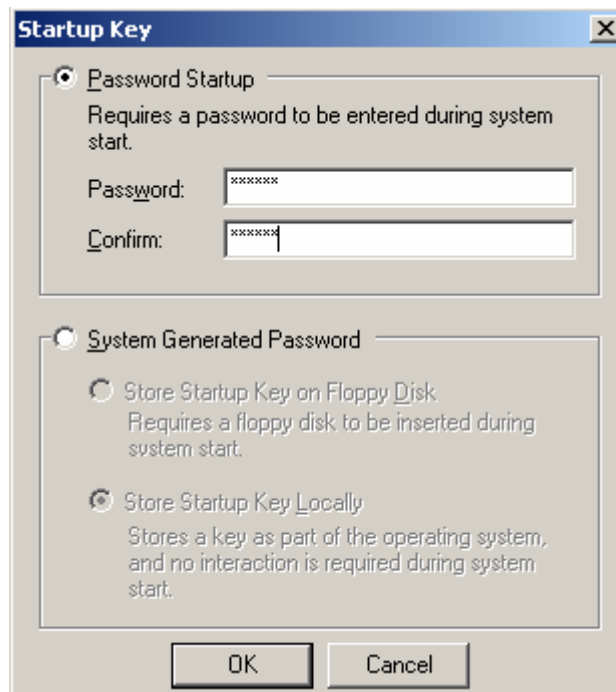
پنجره زیر نمایش داده می شود. بر روی Update کلیک کنید.



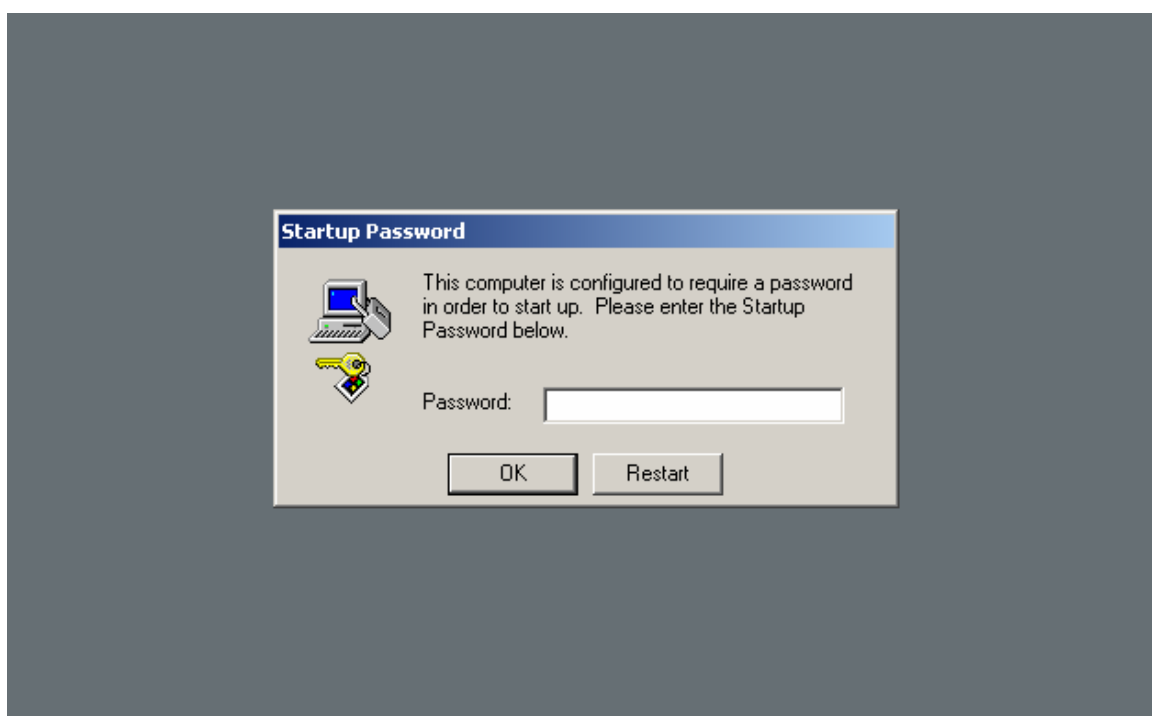
پنجره زیر نمایش داده می شود.



بر روی Startup کلیک کرده و رمزی را برای Syskey اختصاص داده و OK کنید.



اگر سیستم را رستارت نمایید بعد از Load شدن ویندوز پنجره زیر را مشاهده می نمایید که باید برای ورود رمز Syskey را وارد نمایید. (اگر رمز را سه بار اشتباه وارد نمایید سیستم رستارت می شود)

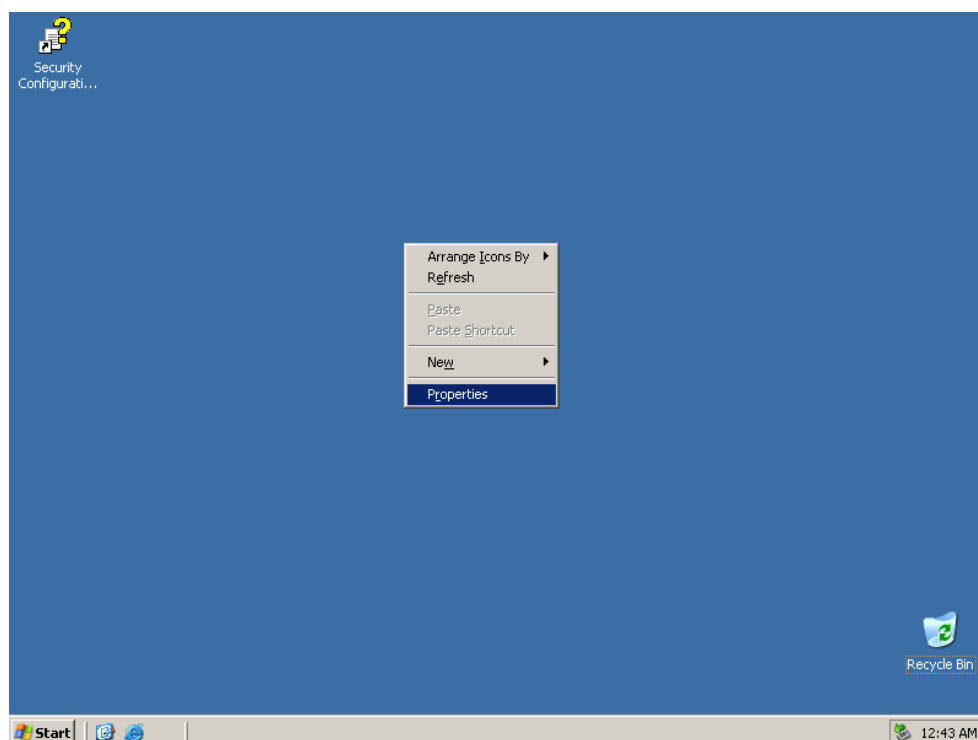


۳-۱-۷- امنیت با Screen Server:

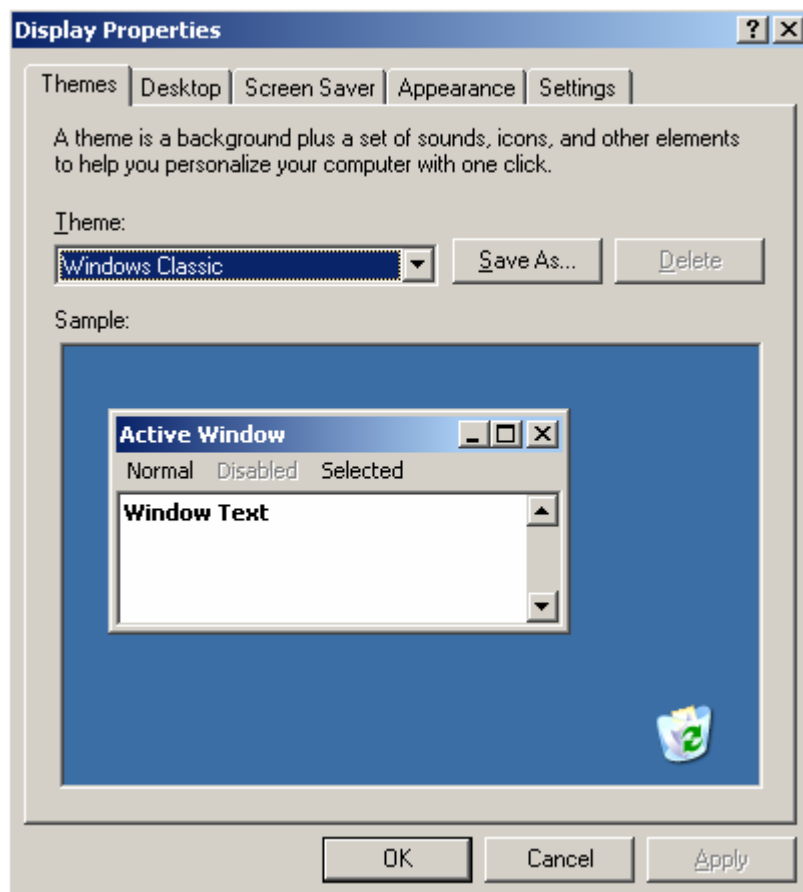
اگر در ویندوز ۲۰۰۳ سرور برای محافظ صفحه کلمه عبوری را اختصاص دهیم باعث می شود تا پس از سپری شدن مدت معینی که صفحه بدون فعالیت ماند به صورت اتوماتیک قفل شود. این عمل به عنوان یک کار امنیتی موقعی موثر است که کاربر یا مدیری برای یک مدت کوتاهی سیستم را ترک میکنند و یادشان می رود سیستم را قفل کنند. پس از اینکه صفحه قفل شد فقط کاربر یا مدیری می تواند قفل را باز کند که قبل از قفل شدن وارد سیستم شده بود.

برای فعال کردن قفل Screen Server این مراحل را طی نمایید:

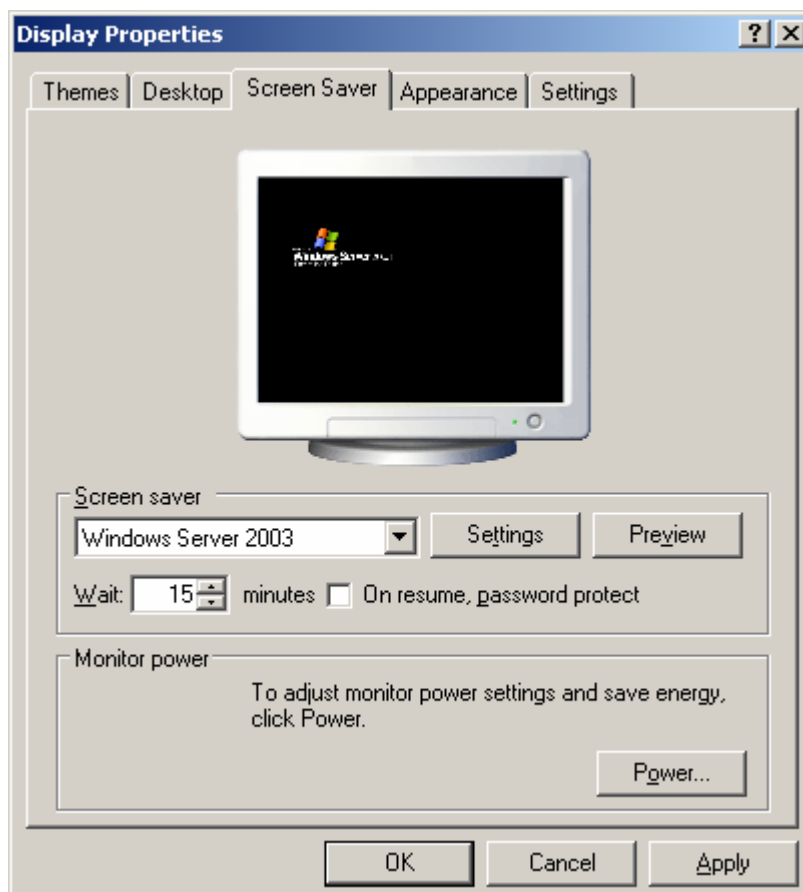
در میز کار کلیک راست کرده و گزینه Properties را انتخاب کنید.



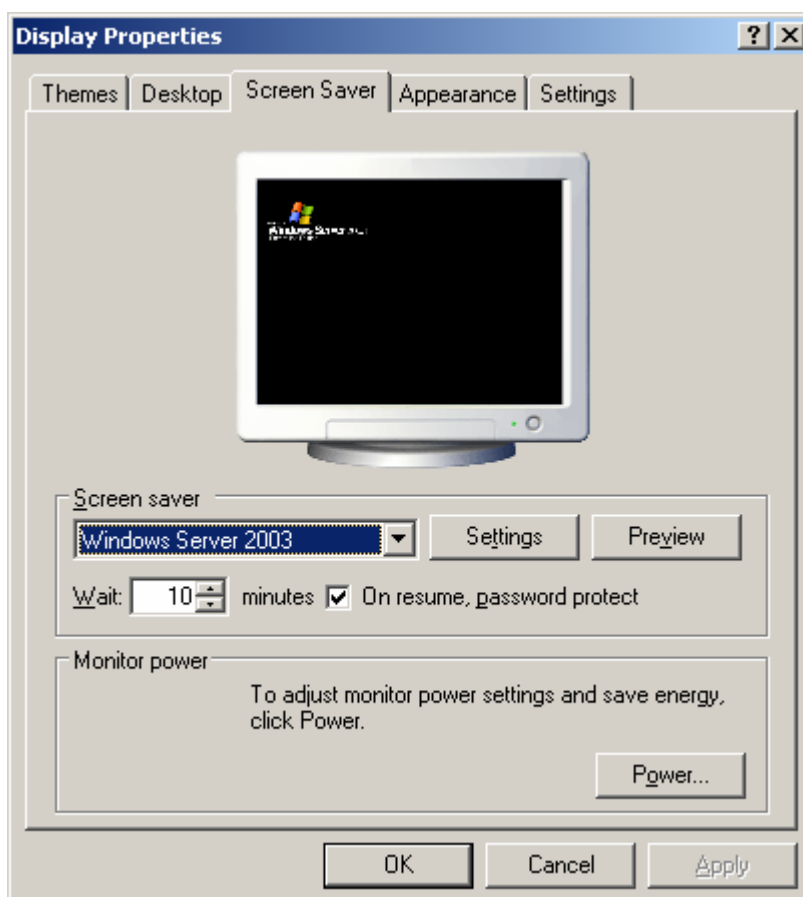
در پنجره مشاهده شده بر روی زبانه Screen Server کلیک کنید.



پنجره مربوط به تنظیمات Screen Server را مشاهده می کنید. در این پنجره اگر خواستید می توانید از منوی کشویی Screen Server تصویر محافظ صفحه را عوض کنید.



در بخش Wait باید زمانی را که می خواهید سیستم بعد از سپری شدن آن زمان، قفل شود را مشخص کنید (برای مثال ۱۰ دقیقه) سپس تیک گزینه On resum, password protect را قرار دهید.



اگر بعد از انجام این مراحل صفحه ۱۰ دقیقه بدون فعالیت بماند Screen Server اجرا و صفحه قفل می شود.



اگر کلیدی را فشار دهید صفحه قفل ظاهر می شود. برای باز کردن قفل، کاربر یا مدیر باید کلیدهای ترکیبی Ctrl+Alt+Delet را فشار داده و رمز خود را وارد نماید.

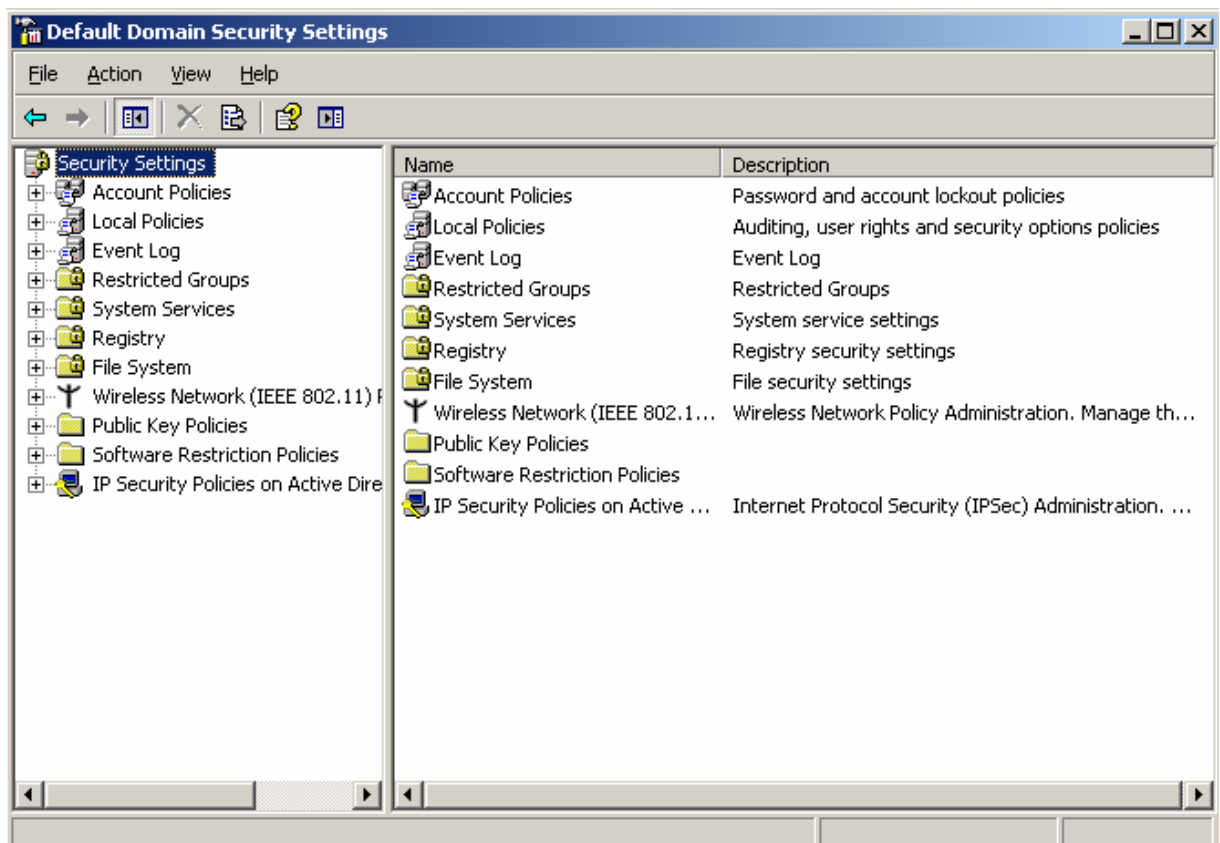


۴-۱-۷- امنیت با Domain Security Policy

این ابزار برای اعمال سیاستهای امنیتی در دامنه به کار می رود. سیاست های امنیتی را می توان برای موارد زیر اعمال کرد:

- سیاست های امنیتی کلمه عبور
- سیاست های امنیتی محلی
- سیاست های امنیتی ثبت رخدادها
- و...

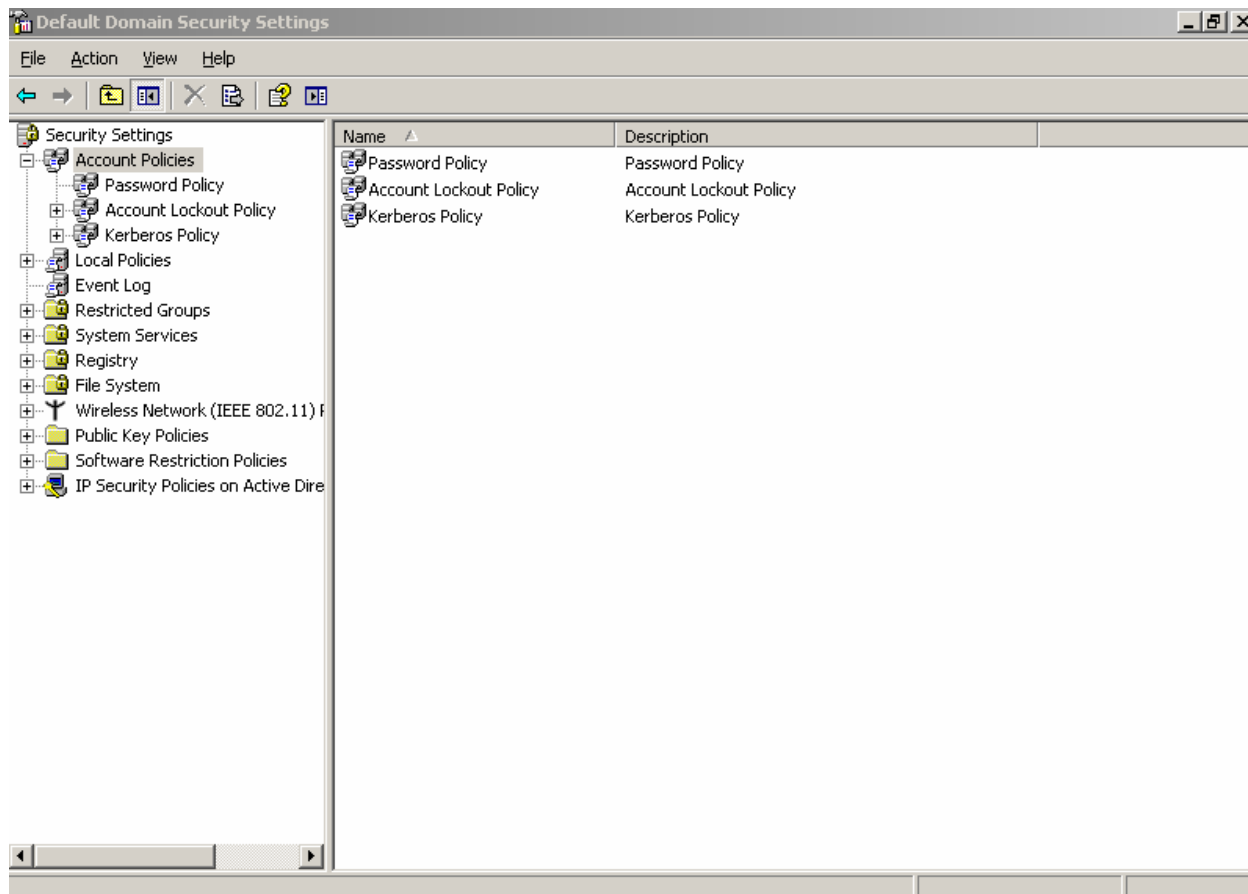
برای اعمال سیاست های امنیتی در دامنه با حقوق مدیریتی، وارد ابزار Domain Security Policy از مسیر زیر بشوید.
Start > Administrative Tools > Domain Security Policy
 پنجره زیر نمایش داده می شود.



۱-۴-۷- سیاست های امنیتی کلمه عبور:

بخش Account Policies مربوط به سیاست های برای امنیت کلمه عبور می باشد. بخش Account Policies برای پیکربندی موارد زیر بکار می رود:

- Password Policy: با استفاده از این بخش می توان سیاست هایی را برای مدیریت کلمه عبور کاربر انجام داد.
- Account Lockout Policy: این بخش مربوط به تنظیماتی برای اعمال سیاست هایی برای قفل کاربری می باشد.
- Kerberos Policy: تنظیماتی برای اعمال سیاست های کربروس می باشد.



:Password Policy

اگر خاطرتان باشد هنگام ایجاد کاربر و اختصاص دادن رمز به کاربر می بایستی برخی ویژگی هایی که به صورت پیش فرض در نظر گرفته شده بود را رعایت می کردید. اگر به این بخش بروید آن ویژگی هایی که به صورت پیش فرض در نظر گرفته شده اند را می توانید ببینید و اگر خواستید آنها را می توانید تغییر دهید.

بر روی Password Policy کلیک کنید. پنجره زیر نمایش داده می شود. که در سمت راست شش گزینه وجود دارد:

Enforce password history: این گزینه برای ذخیره سازی تاریخچه پسورد می باشد که می توانید با کلیک بر روی آن تعداد روزهای ذخیره سازی را افزایش، کاهش یا این گزینه را غیر فعال کنید.

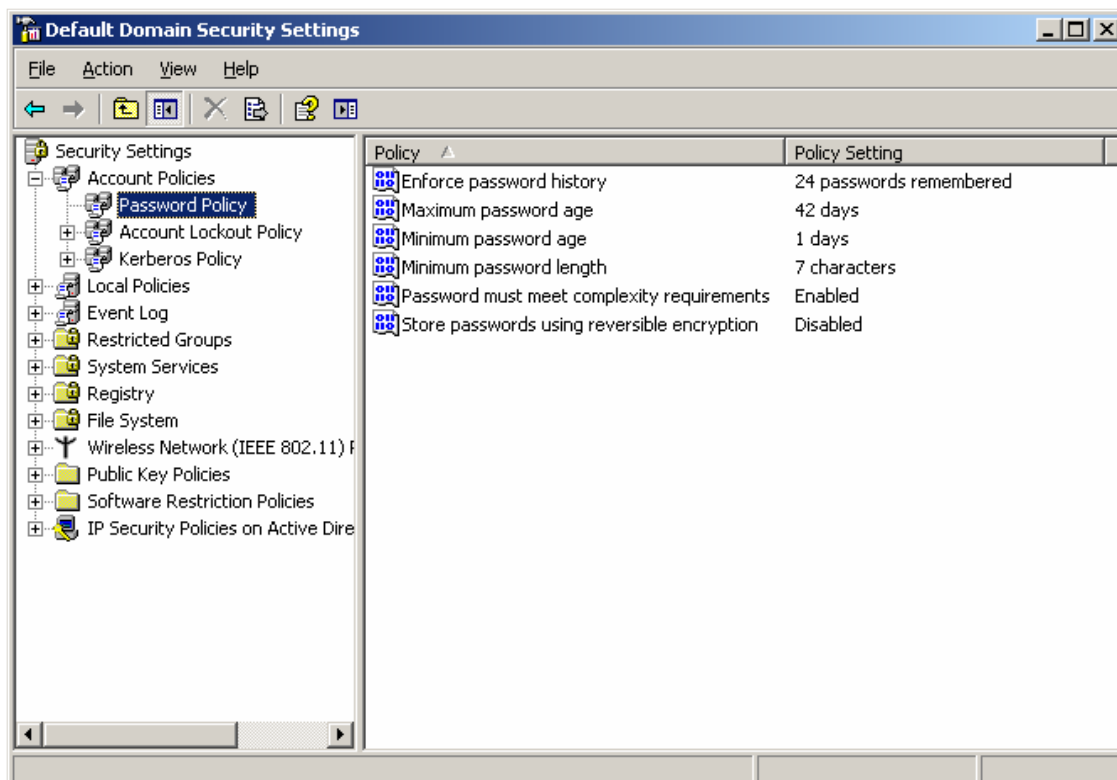
Maximum password age: می توانید با کلیک بر روی این گزینه حداکثر روزی را که بعد از ایجاد کاربر (پیش فرض ۴۲ روز) برای کاربر پیغام می آید که باید رمز خود را تغییر دهد را افزایش یا کاهش دهید.

Minimum password age: در اینجا هم می توانید حداقل تعداد روزها را افزایش یا کاهش دهید.

Minimum password length: می توانید با کلیک بر روی این گزینه حداقل طولی که باید پسورد کاربر داشته باشد را افزایش یا کاهش دهید.

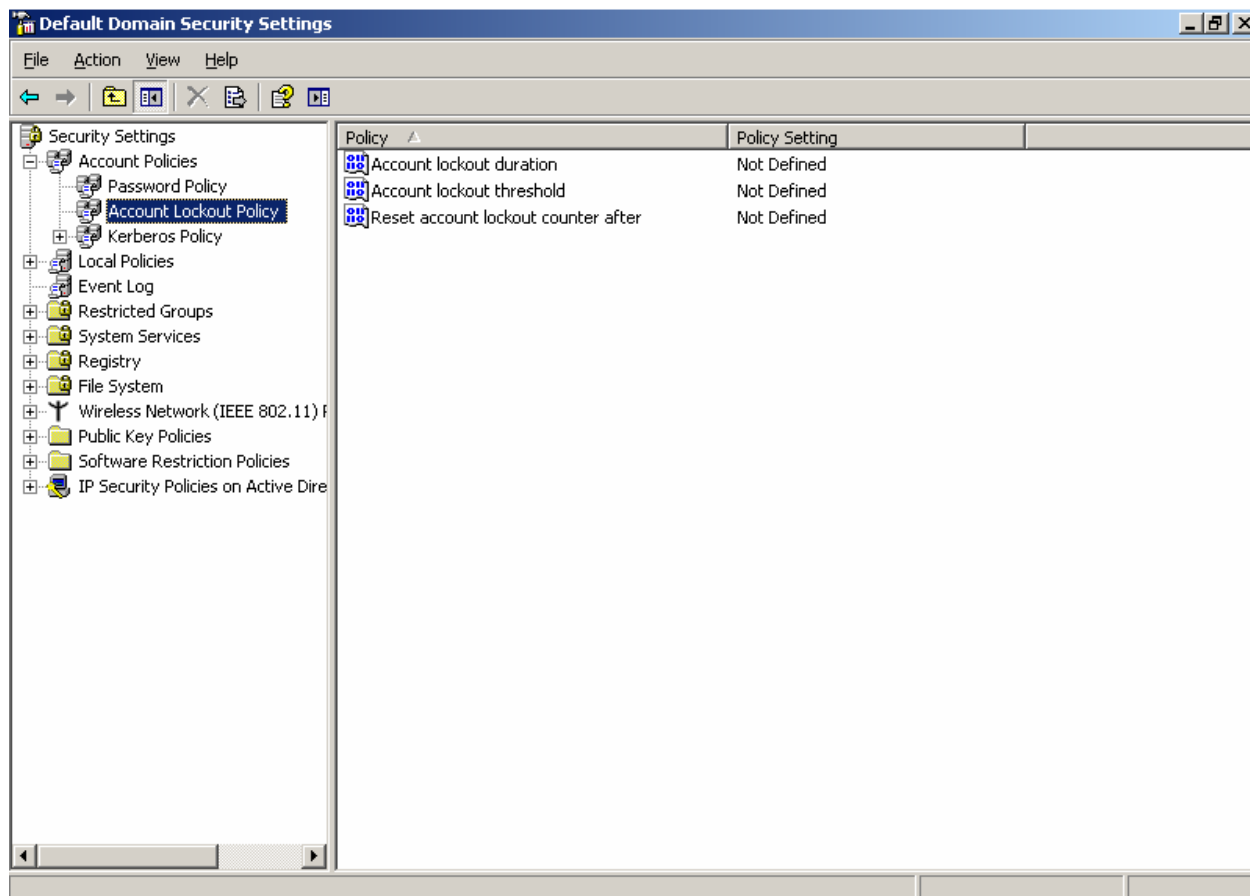
Password must meet complexity requirements: این گزینه برای این است که آیا رمز کاربر دارای پیچیدگی باشد یا نه؟ بدین صورت که ترکیبی از حرف بزرگ و کوچک آیا در آن رعایت شود یا نه؟ که به صورت پیش فرض **Enabled** می باشد یعنی رعایت شود. و می توانید با کلیک بر روی این گزینه و انتخاب **Disabled** این ویژگی را غیر فعال کنید.

Store passwords using reversible encryption: این گزینه برای این است که آیا هنگام ذخیره پسورد آن را به صورت کد شده نمایش دهد یا نه؟ که به صورت پیش فرض این ویژگی غیر فعال (Disabled) می باشد که با کلیک بر روی این گزینه می توانید این ویژگی را فعال کنید.

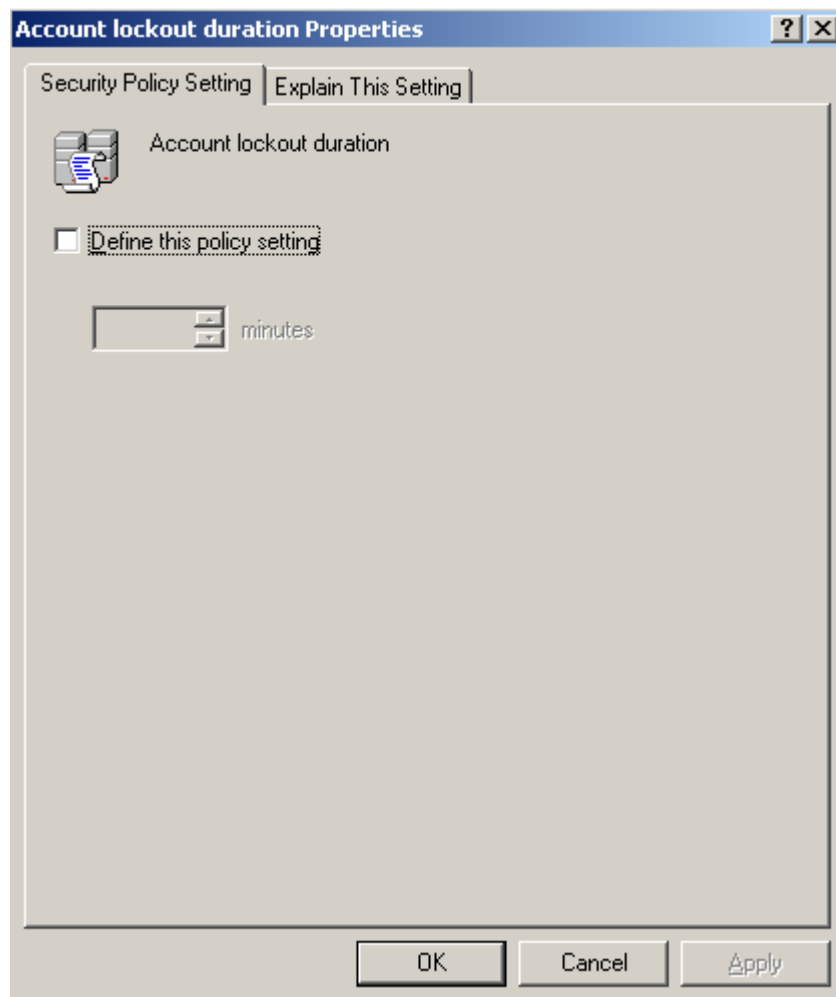


:Account Lockout Policy

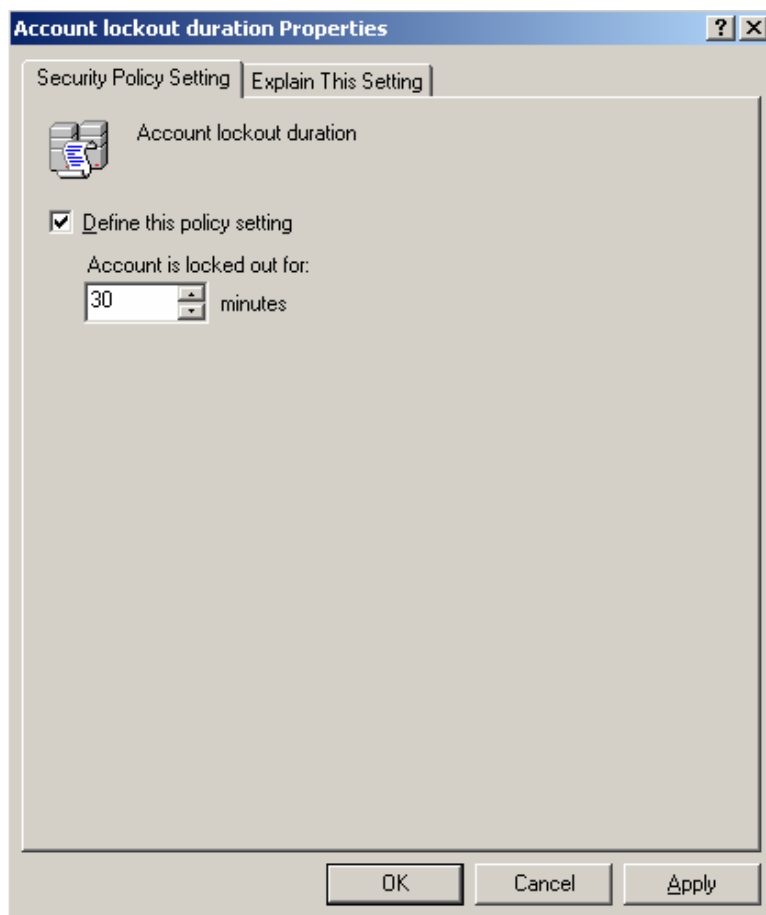
در این بخش می توان سیاست هایی را در رابطه با قفل اکانت اعمال کرد. در رابطه با قفل اکانت توصیه های وجود دارد. یکی از توصیه ها که در رابطه با این سیاست وجود دارد این است که قفل کاربری نباید فعال شود برای اینکه اگر سیاست های کلمه رمز به خوبی تنظیم شوند هیچ نفوذ گری نخواهد توانست در مدت کوتاهی کلمه رمز را پیدا کند. علاوه بر این اگر نفوذ گر از برنامه های اتوماتیک برای دستیابی به کلمه عبور استفاده کند، این برنامه ها اغلب تعداد زیادی از اکانت ها را آزمایش می کنند که این کار می تواند باعث قفل برخی یا همه اکانت های سرویس دهنده شود. (اکانت Administrator نمی تواند قفل شود)



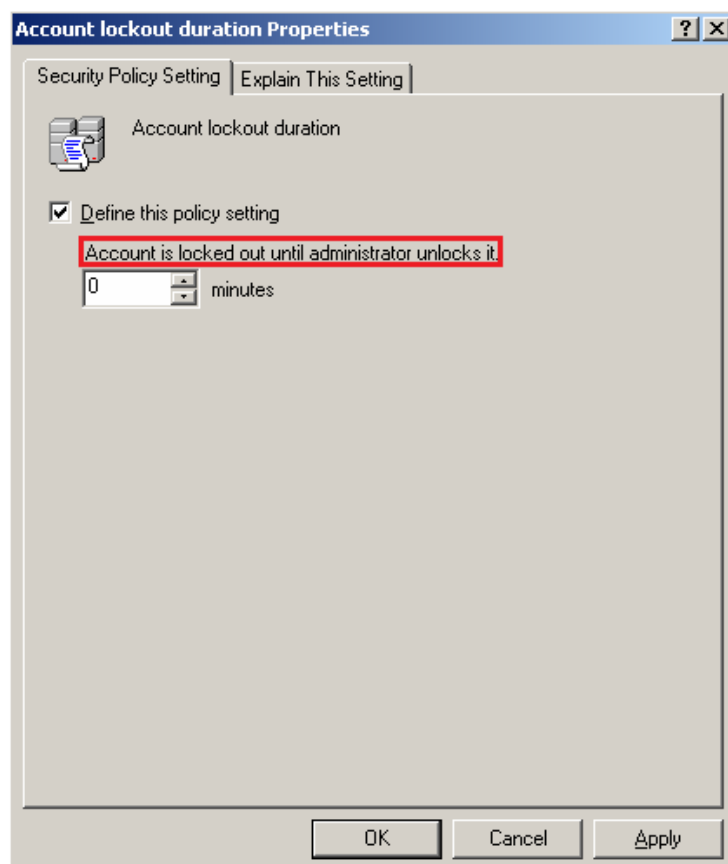
اگر می خواهید این سیاست را فعال کنید باید گزینه های زیر را تنظیم نمایید:
بر روی Account lockout duration کلیک کنید تا پنجره زیر نمایش داده شود.



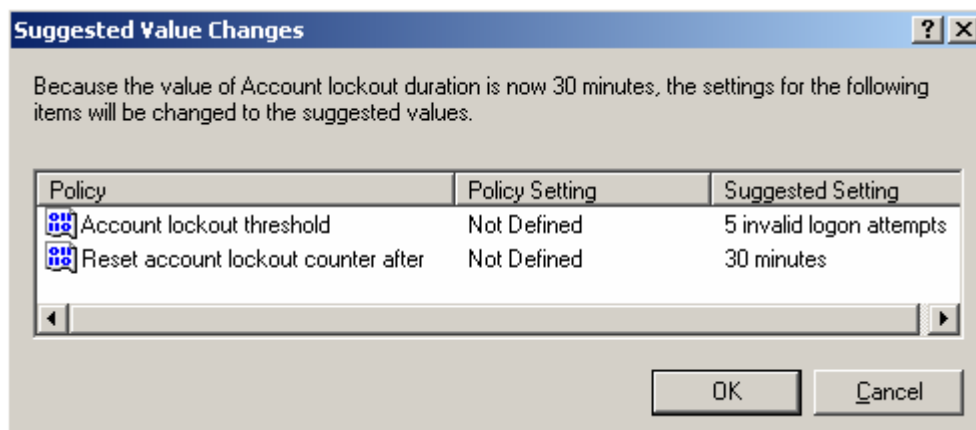
کادر Define this policy setting را انتخاب کنید. قسمت minutes فعال می شود. در قسمت minutes باید زمانی را مشخص کنید که بعد از سپری شدن آن زمان اکانت دوباره فعال شود. (برای مثال اگر روی ۳۰ دقیقه تنظیم کنید بعد از اینکه چند بار از کلمه عبور نامعتبر استفاده کردید به مدت ۳۰ دقیقه آن اکانت قفل می شود)



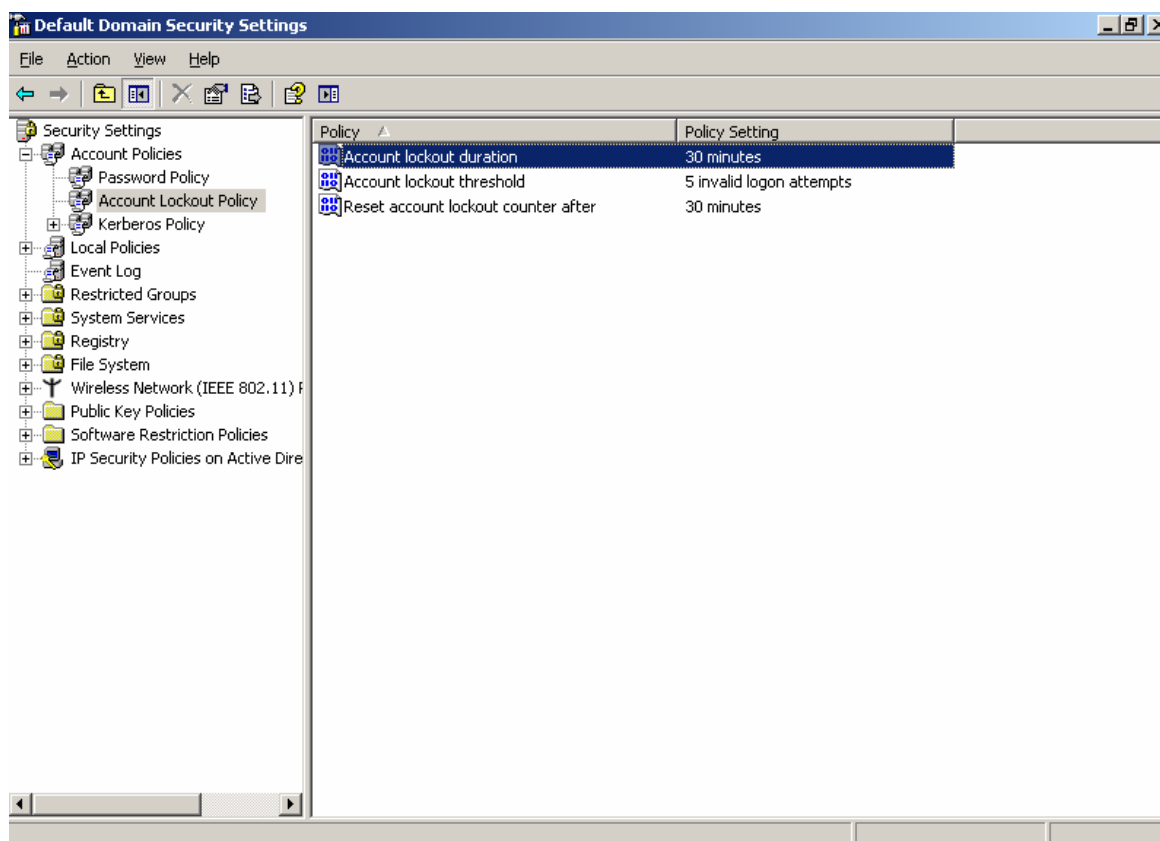
اگر صفر کنید مشاهده می کنید که پیغام بالای بخش minutes تغییر می کند. مبنی بر اینکه تا زمانی که یک مدیر اکانت را فعال نکند آن اکانت فعال نمی شود.



OK کنید. پنجره ای نمایش داده می شود که نشان می دهد به صورت پیش فرض برای Account lockout threshold (تعداد تلاش های ناموفق) ۵ بار و برای Reset account lockout counter after (مدت زمان قفل قبل از ریست شدن) ۳۰ دقیقه در نظر گرفته می شود. OK کنید.



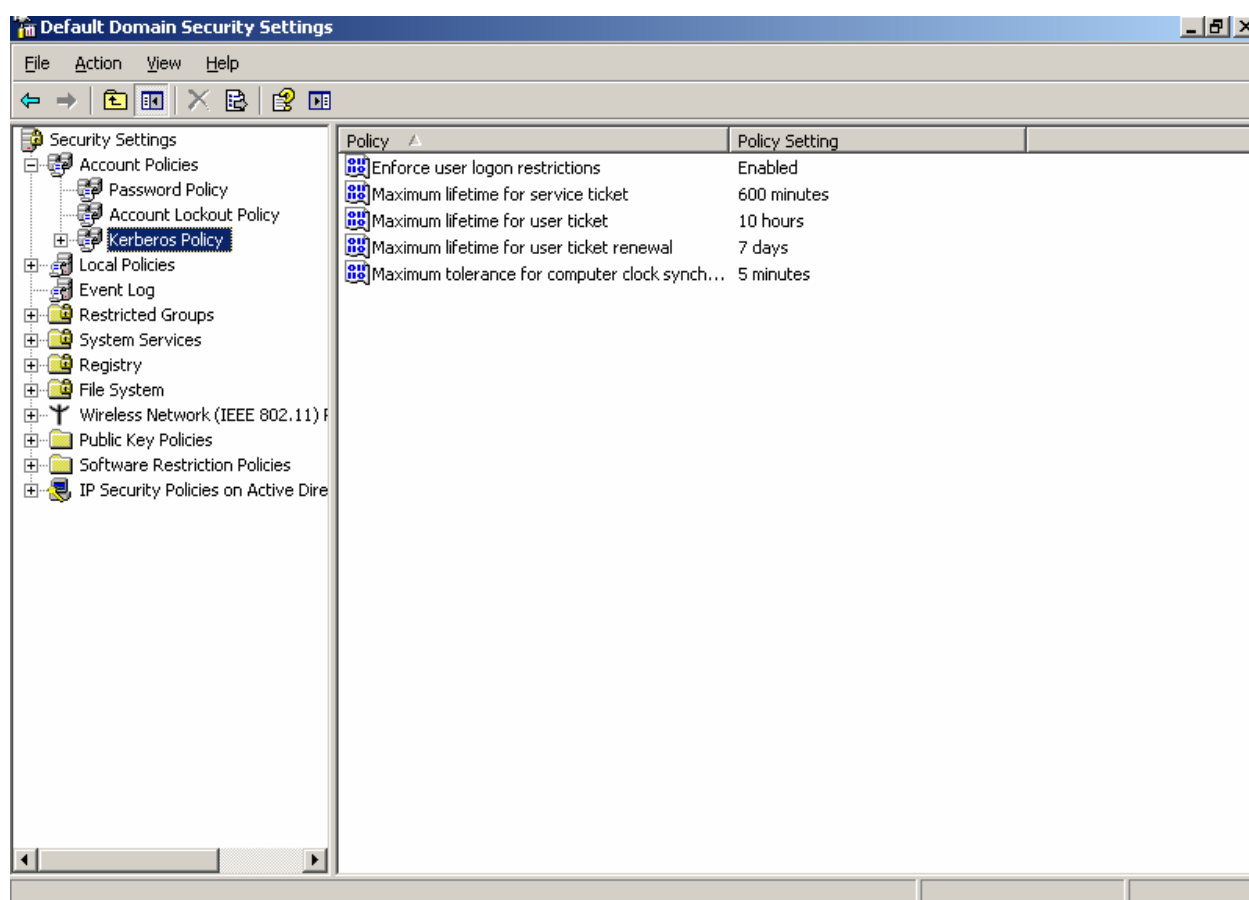
اگر بخواهید میتوانید تعداد تلاش های ناموفق و مدت زمان قفل قبل از ریست شدن را با کلیک بر روی هر یک از آنها تغییر دهید.



:Kerberos Policy

در این بخش می توان سیاست هایی را برای تنظیمات کربروس انجام داد.

نکته: مدیران دامنه نباید در تنظیمات کربروس تغییراتی را انجام دهند، مگر اینکه دقیقاً با آن آشنایی داشته باشند.



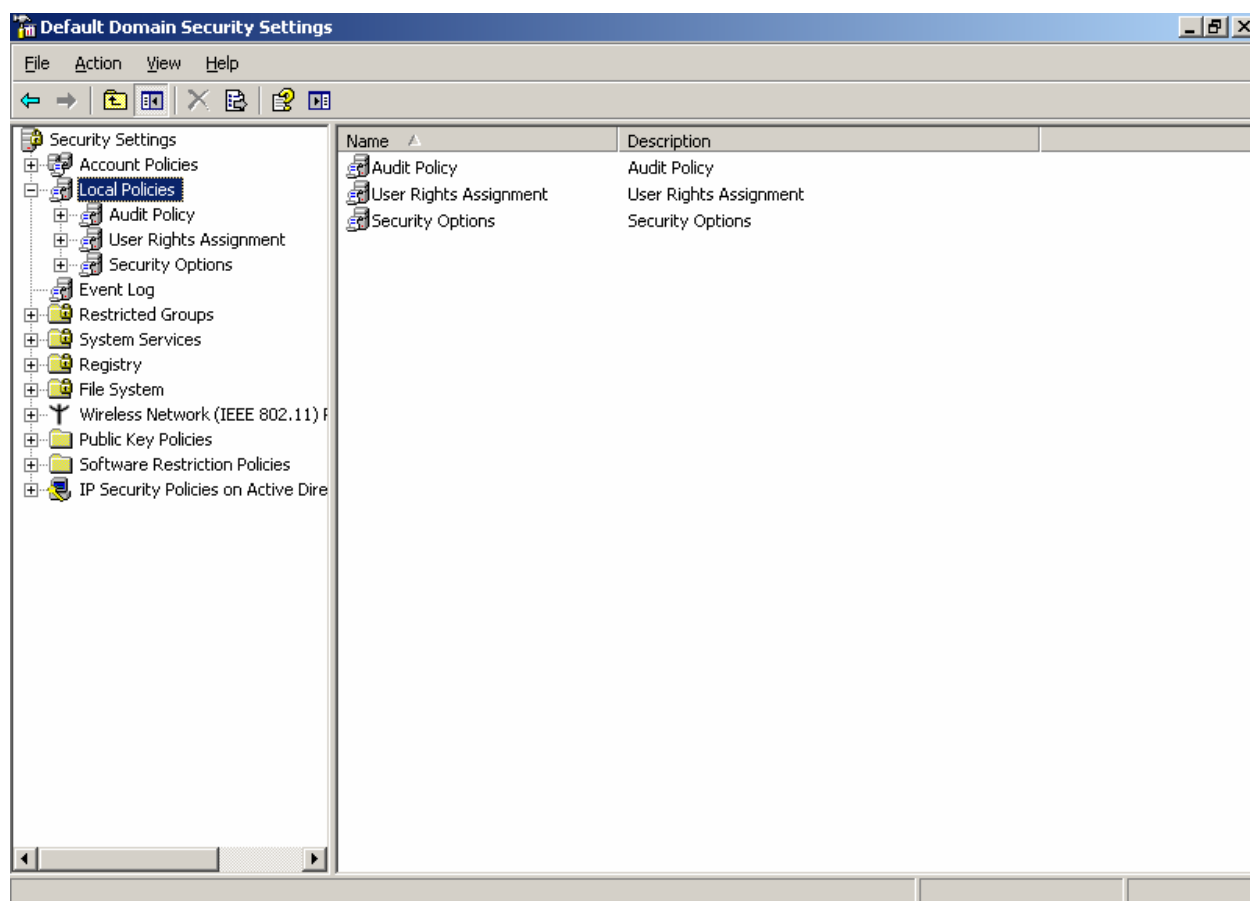
۲-۴-۱-۷- سیاست های امنیتی محلی:

سیاست های امنیتی است که بر روی کاربران یا کامپیوتر ها انجام می شود. بخش Local Policies برای پیکربندی موارد زیر بکار می رود:

- Audit Policy: این بخش مربوط به تنظیماتی برای نگهداری رخدادها می باشد. می توانید تنظیم کنید که چه رخدادهای امنیتی در گزارش رخدادها ذخیره شود.

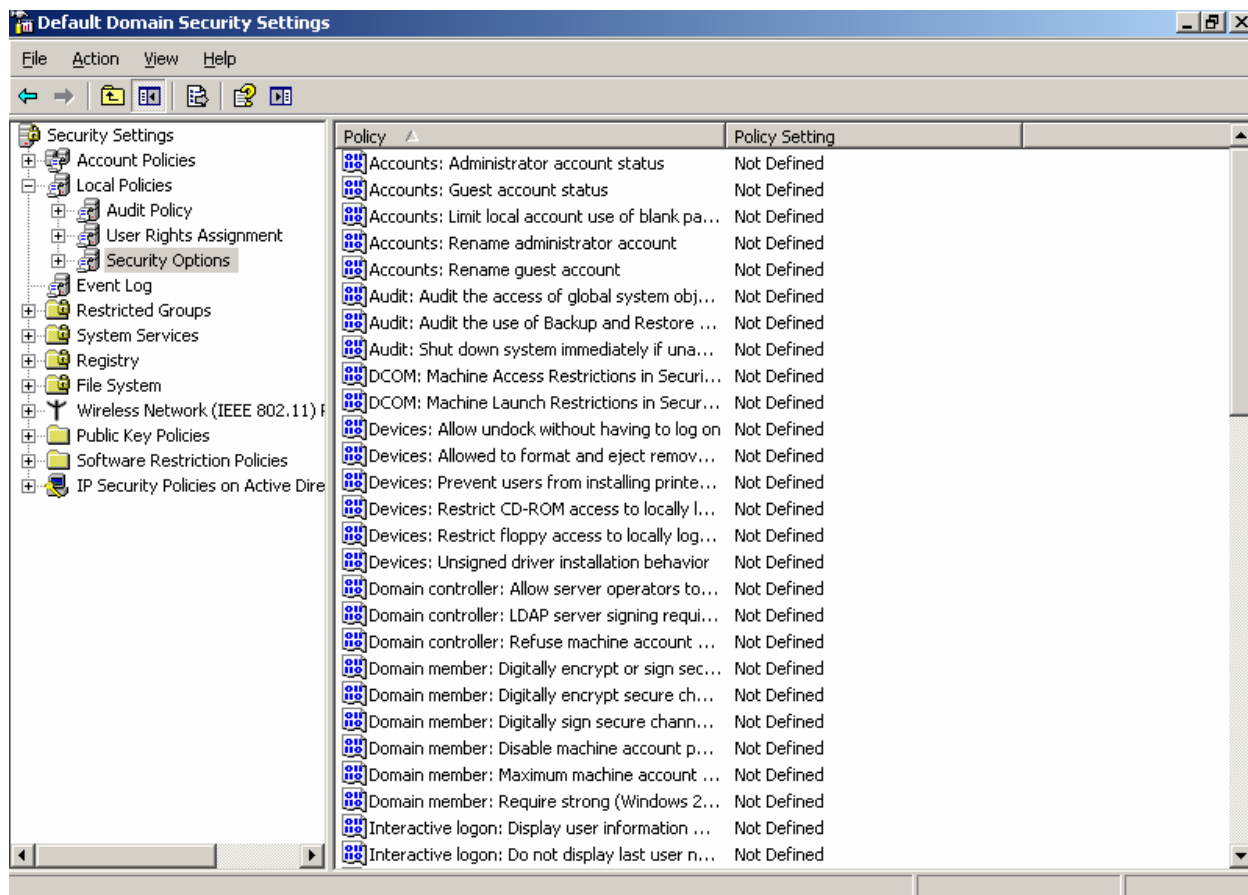
- User Right Assignment: اعمالی است که در رابطه با حق کاربری می باشد. (مثلاً می توانیم اجازه ندهیم کاربر shutdown کند)

- Security Options: در این بخش می توان تنظیمات امنیتی کامپیوتر را تغییر داد.



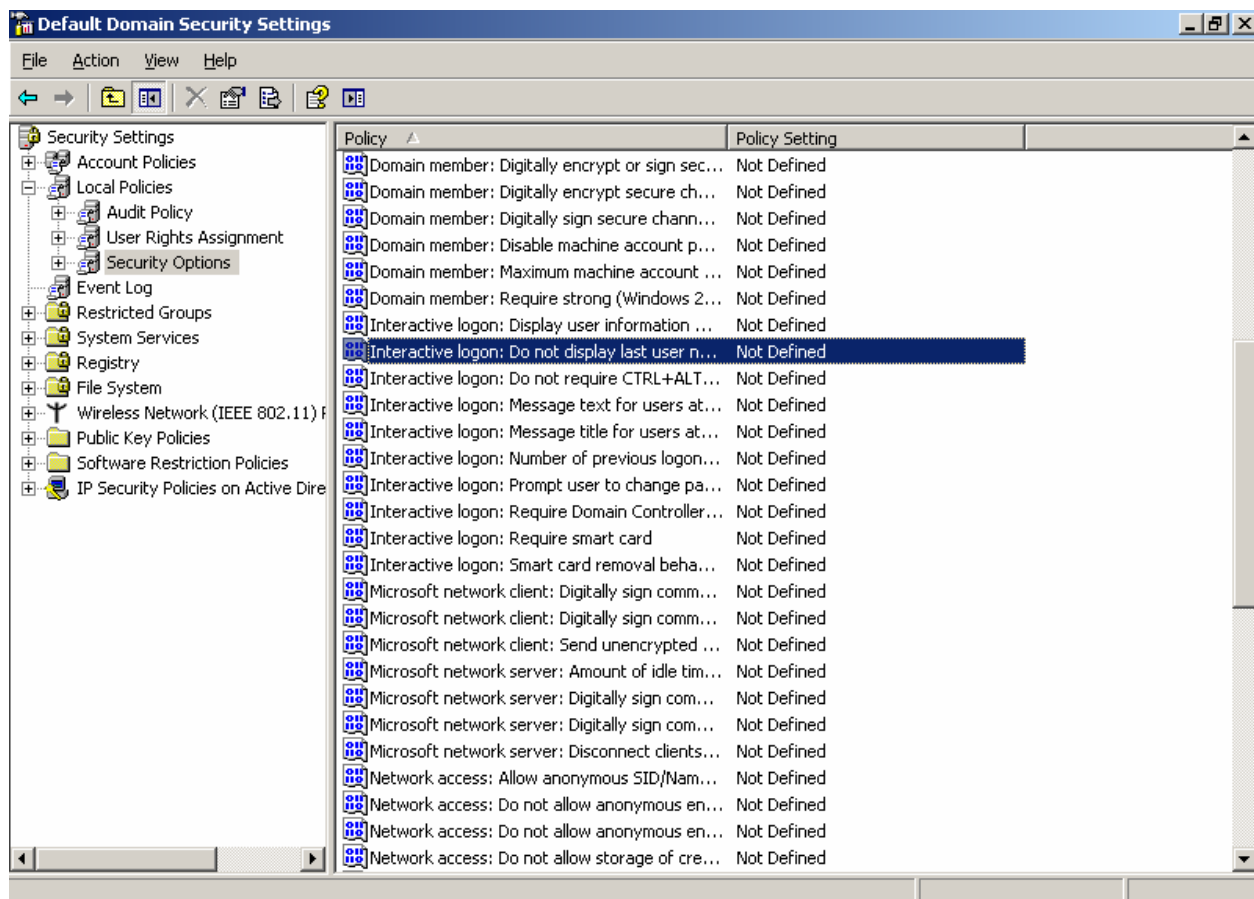
- Security Options

بر روی Security Options کلیک کنید. در سمت راست لیستی از گزینه های امنیتی را مشاهده می کنید.

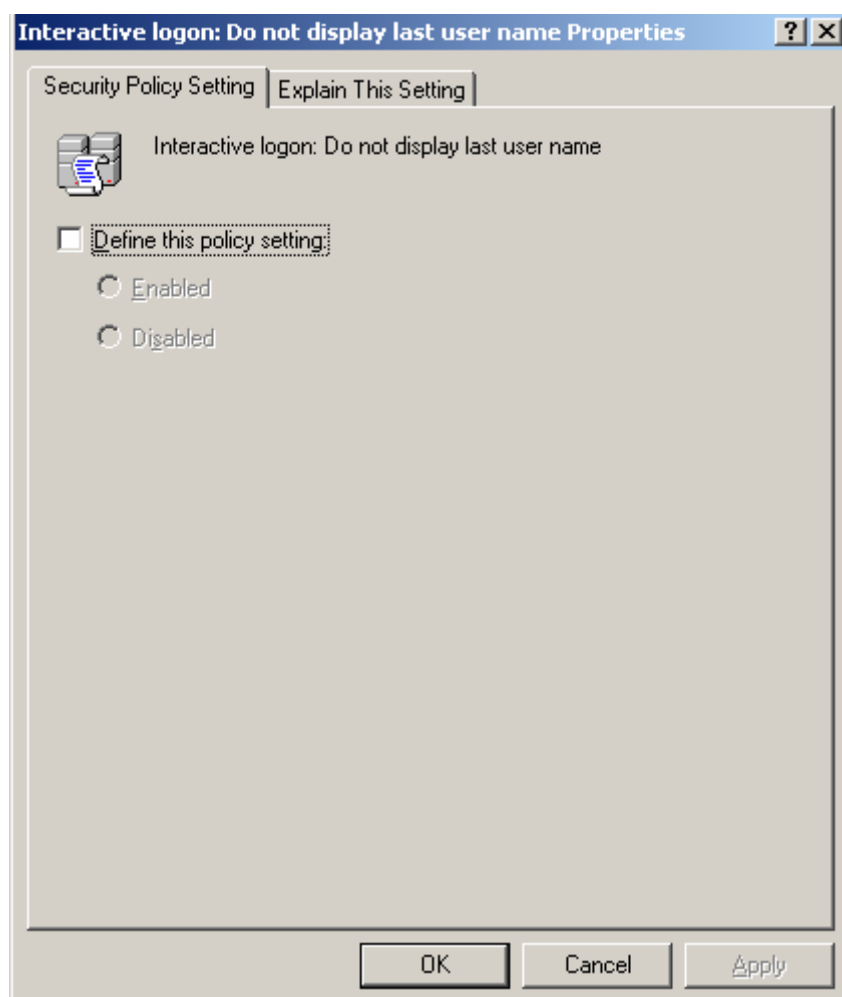


در ویندوز ۲۰۰۳ سرور تعدادی سیاستهای امنیتی وجود دارد که توصیه می شود برای امنیت بیشتر آنها را انجام دهید که مهمترین آنها عبارتند از:

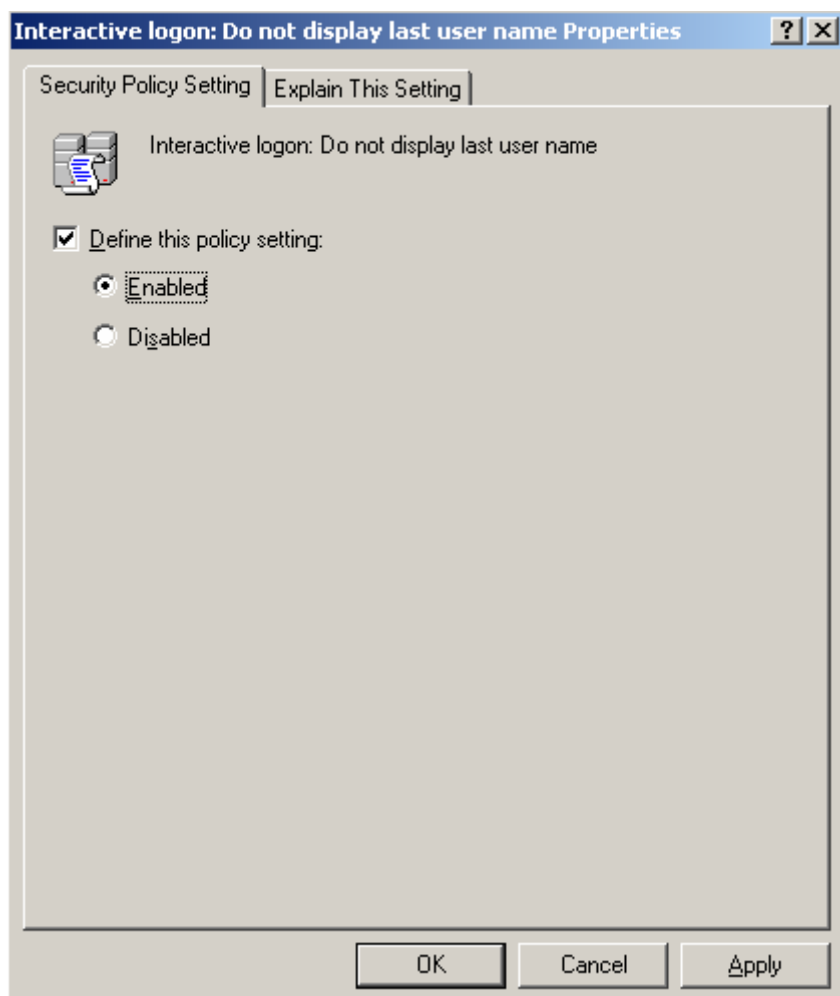
- ۱- Do Not Display Last User Name on Logon Screen: اگر این سیاست را فعال کنید هنگام ورود به سیستم نام کاربری (User Name) قبلی مشاهده نخواهد شد. به این ترتیب نفوذ گران مجبور خواهند بود هم نام کاربری و هم پسورد را حدس بزنند. به صورت پیش فرض غیر فعال است که باید آن را فعال کنید. برای فعال کردن بر روی گزینه Do Not Display Last User Name on Logon Screen کلیک کنید.



پنجره زیر نمایش داده می شود.



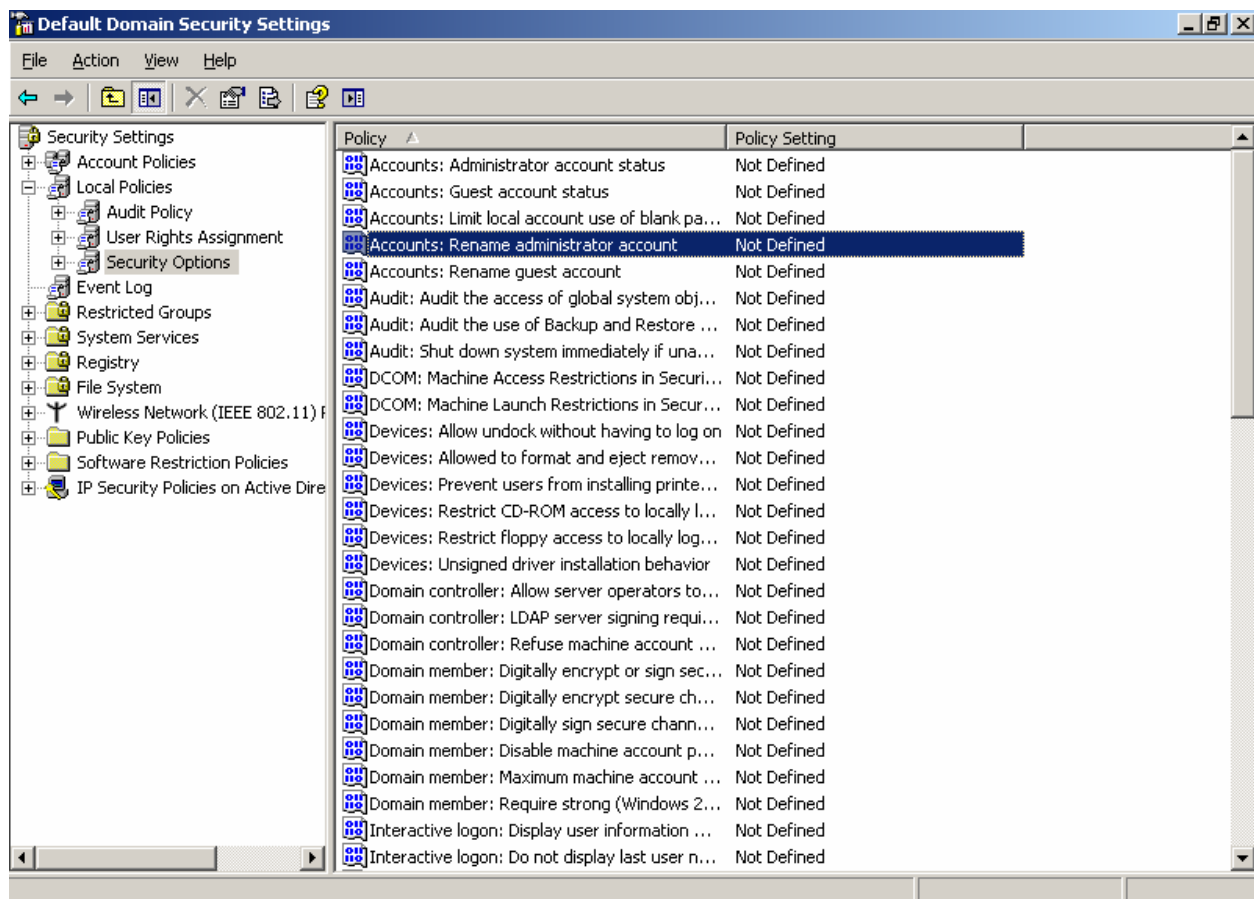
در پنجره نمایش داده شده کادر Define this policy setting را انتخاب کرده و گزینه Enabled را انتخاب کنید.



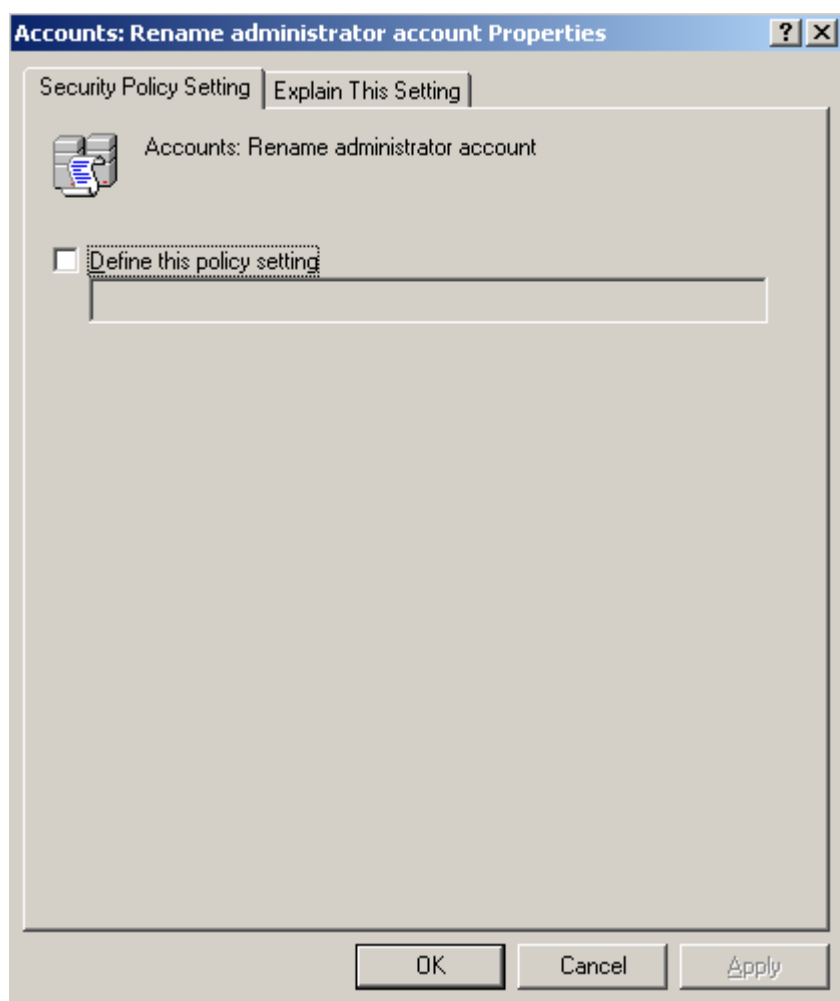
اگر کامپیوتر را رستارت نمایید در هنگام ورود نام کاربری مشاهده نخواهد شد.

۲- Rename Administrator Account: با استفاده از این گزینه بهتر است نام کاربری Administrator را تغییر دهید. چون نفوذگر با حدس زدن نام کاربری Administrator تلاش های خود را برای احتمال ورود به سیستم کاهش می دهد.

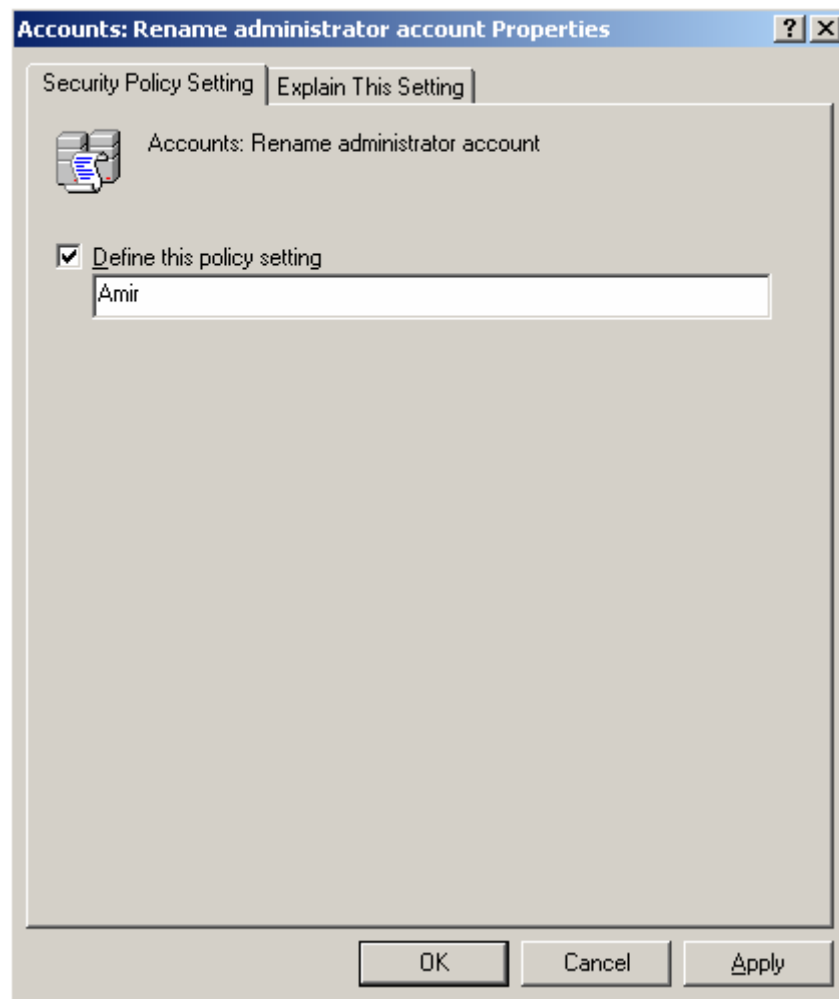
برای این کار بر روی Rename Administrator Account کلیک کنید.



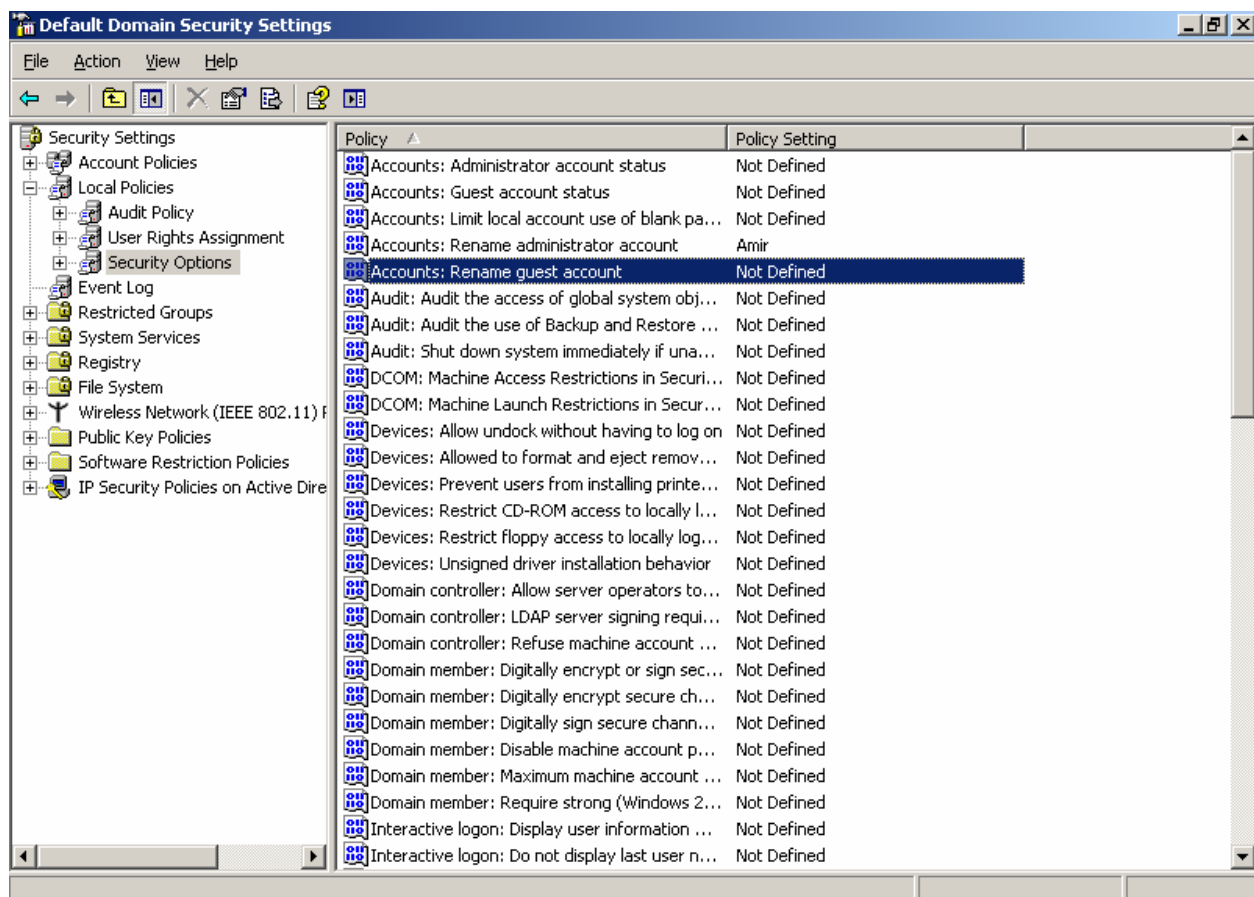
پنجره زیر ظاهر می شود.



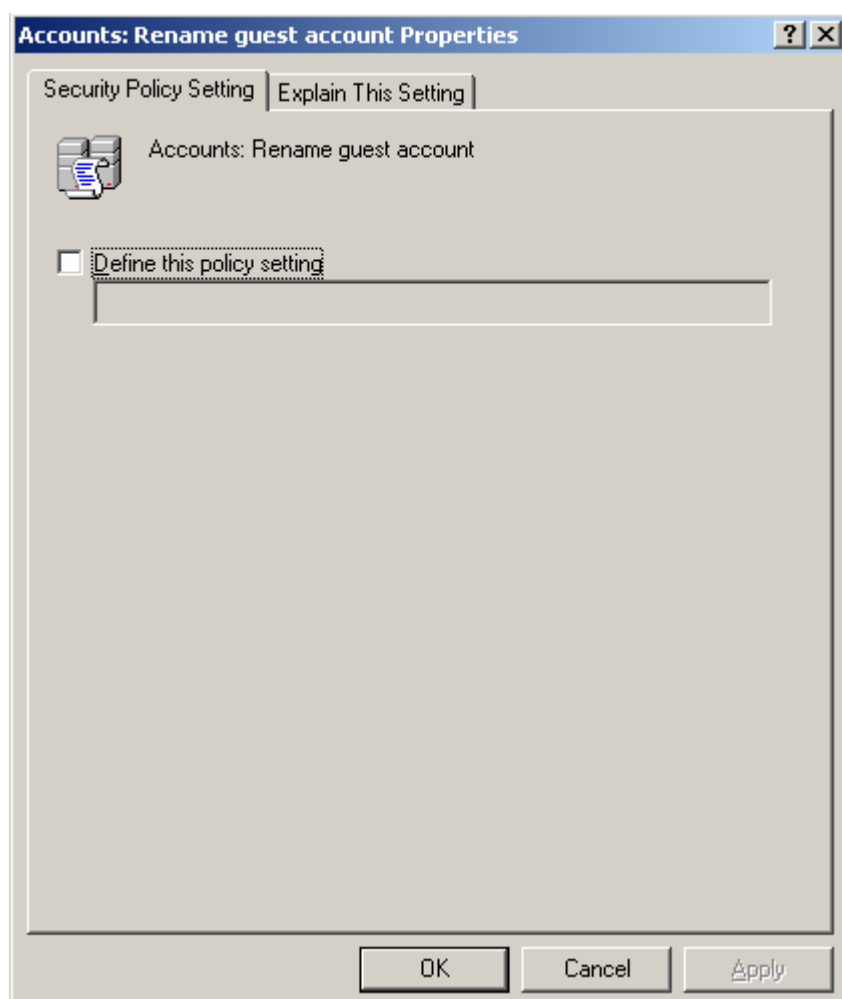
کادر Define this policy setting را انتخاب و نامی جدید را وارد نمایید.



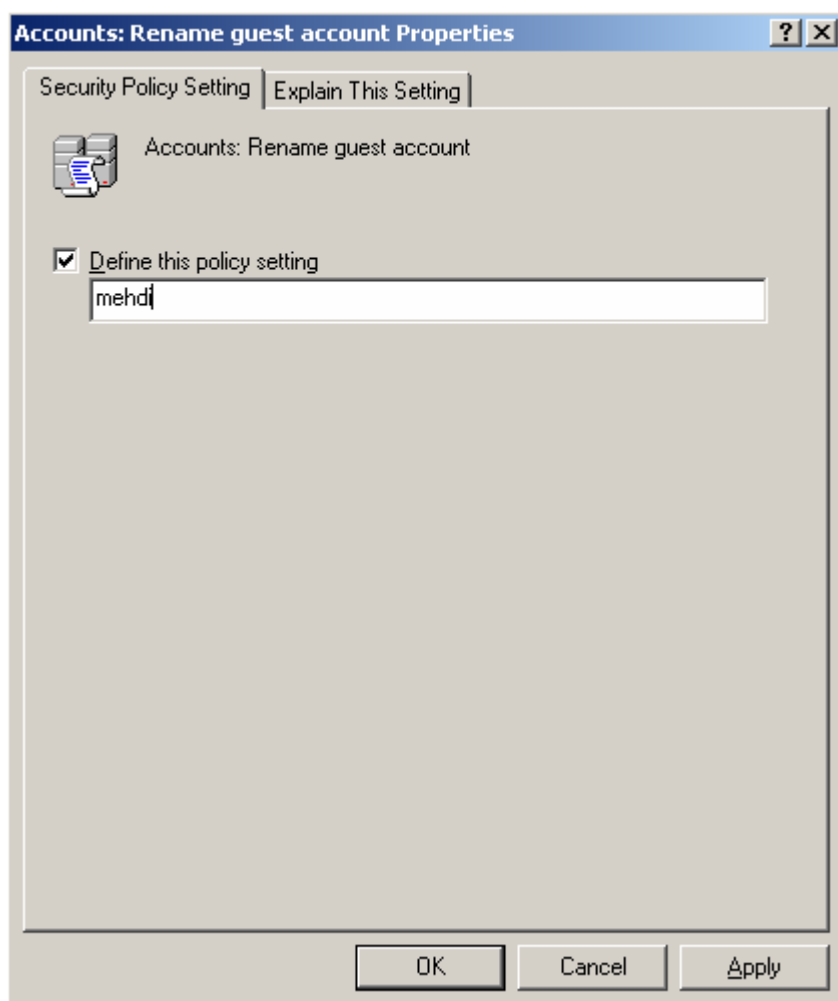
۳- Rename Guest Account: با استفاده از این گزینه بهتر است نام کاربری Guest را تغییر دهید. چون نفوذگر با حدس زدن نام کاربری Guest تلاش های خود را برای احتمال ورود به سیستم کاهش می دهد. برای این کار بر روی Rename Administrator Account کلیک کنید.



پنجره زیر ظاهر می شود.

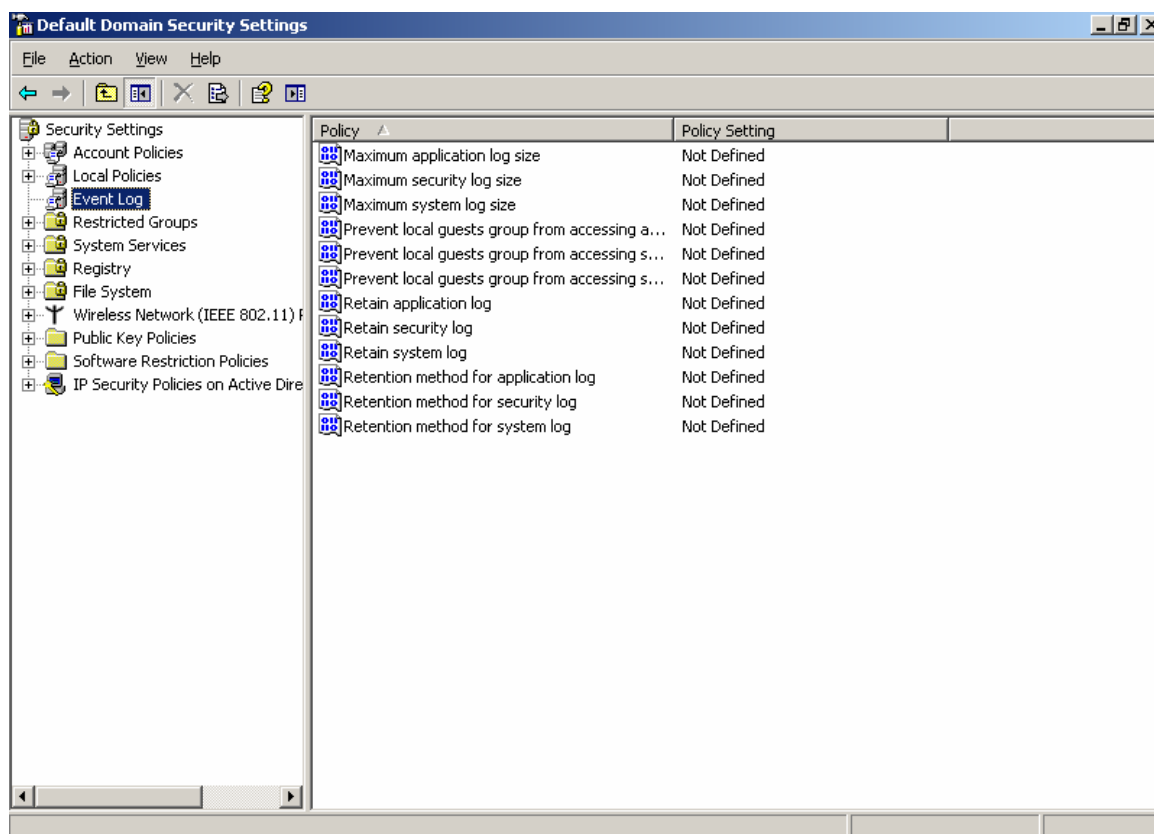


کادر Define this policy setting را انتخاب و نامی جدید را وارد نمایید.



۳-۴-۱-۷- سیاست های امنیتی ثبت رخدادها:

بخش Event Log مربوط به تنظیماتی برای ایجاد سیاست هایی برای ثبت رخدادهای امنیتی می باشد. بر روی Event Log کلیک کنید. در سمت راست لیستی از گزینه هایی که در این بخش وجود دارد را مشاهده می کنید. این گزینه در رابطه با نحوه ذخیره رخدادها می باشد که در صورت تمایل می توانید بر روی آنها کلیک و سیاست آنها را تغییر دهید.



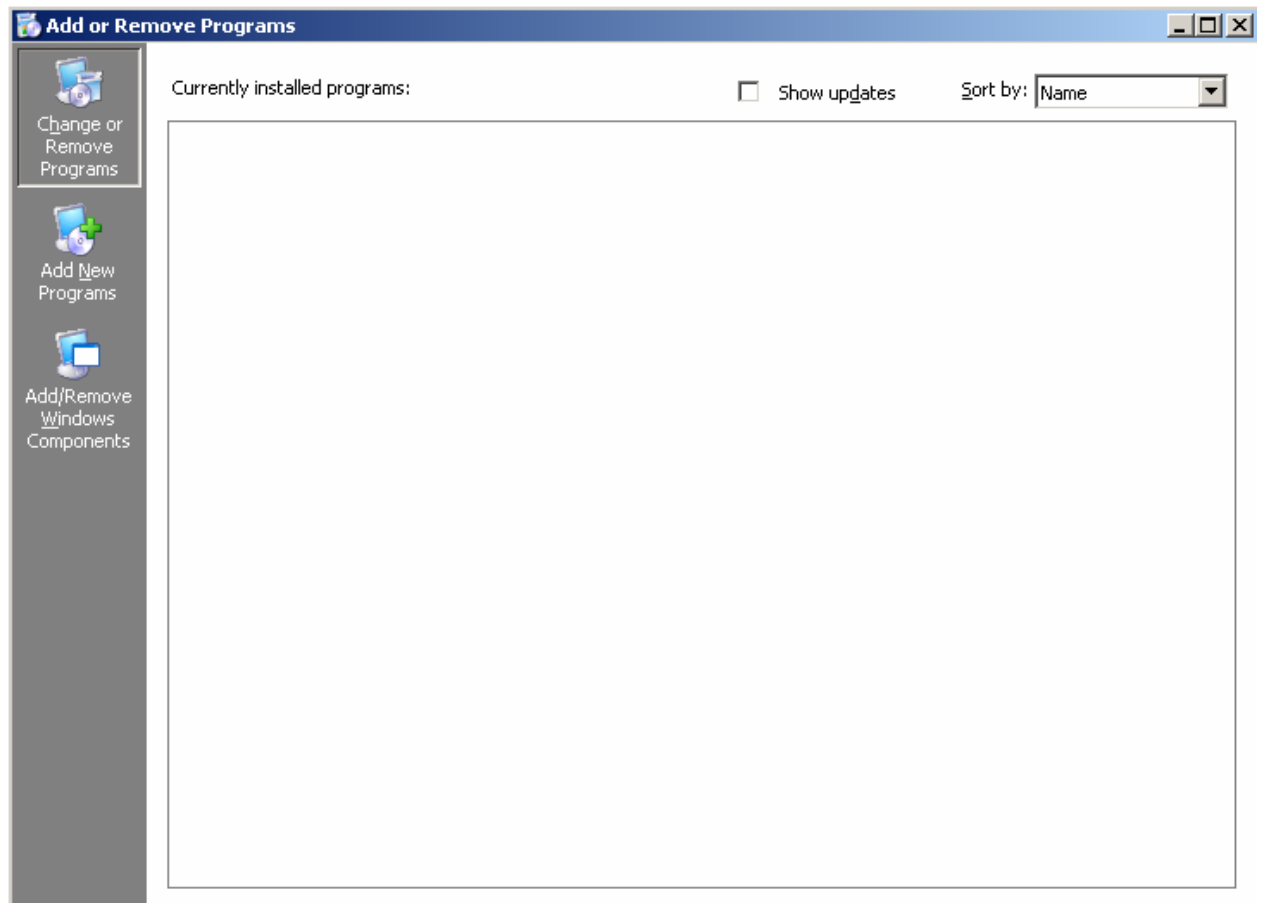
۵-۱-۷- امنیت با Security Configuration Wizard :

در ویندوز ۲۰۰۳ سرور یک سرویس به نام Security Configuration Wizard برای امنیت پیشرفته وجود دارد که به صورت پیش فرض نصب نمی باشد. اگر در یک شبکه امنیت در سطح بالا مطرح باشد باید از این سرویس استفاده شود. در این بخش می خواهیم این سرویس را برای سرور نصب کنیم. برای نصب کردن این سرویس CD ویندوز سرور را داخل CD-ROM قرار داده و این مراحل را انجام می دهیم:

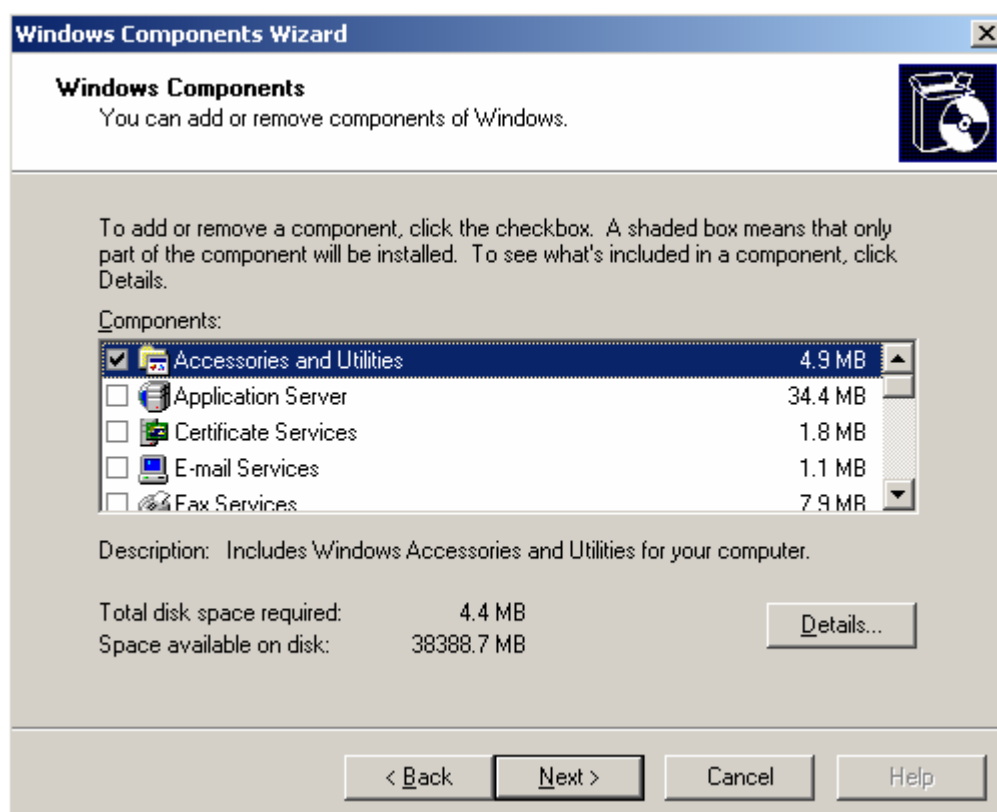
به مسیر زیر می رویم:

Start > Control Panel > Add or Remove Program

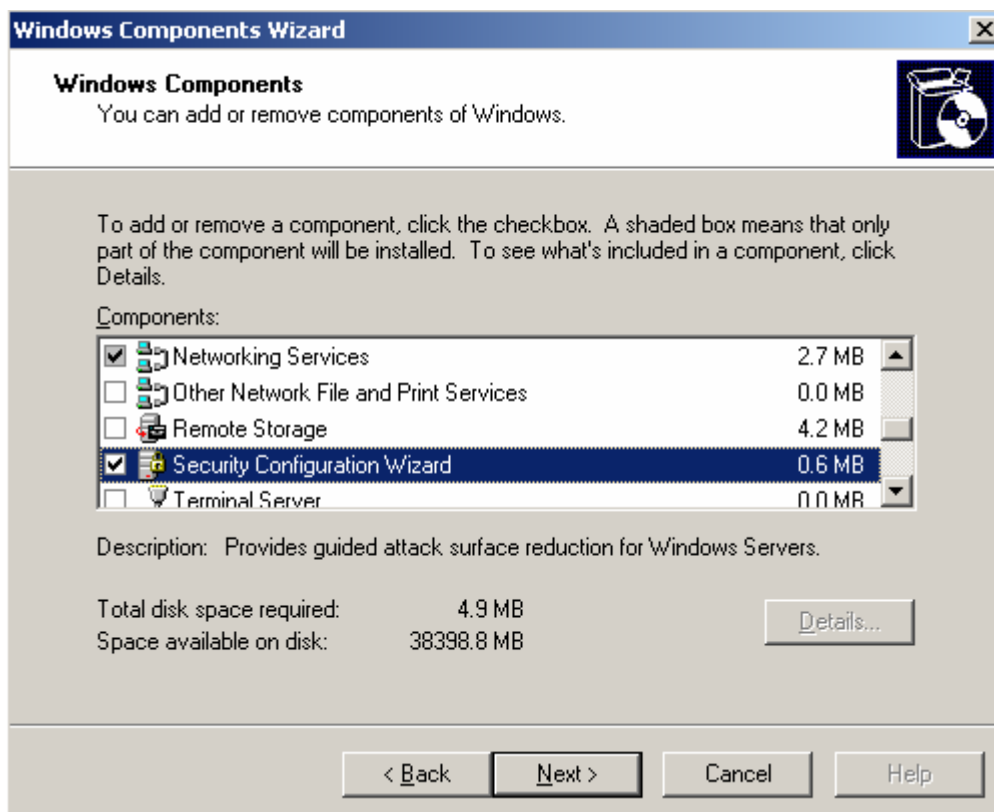
در پنجره Add or Remove Program بر روی Add /Remove Windows Components کلیک می کنیم.



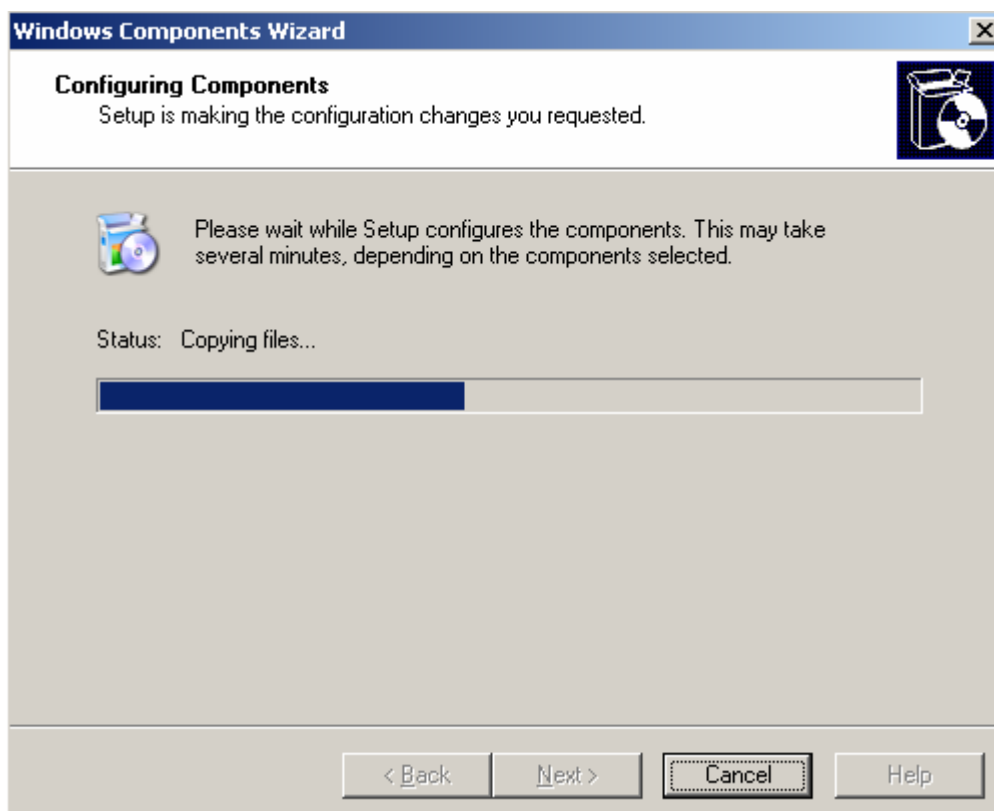
پنجره زیر نمایش داده می شود.



در بخش Components کادر Security Configuration Wizard را انتخاب و بر روی Next کلیک می نمایم.



بعد از Next کردن کامپیوتر شروع به نصب این سرویس بر روی سرور میکند.



بعد از پایان یافتن نصب پنجره زیر نمایش داده می شود بر روی Finish کلیک نمایید.



حال این سرویس بر روی Server نصب می باشد.

۸. جزئیات بخش هشتم:

۸-۱- پشتیبان گیری:

اطلاعات ممکن است به دلایل مختلفی از جمله خرابی بخشهایی از کامپیوتر، بلایای طبیعی از دست رفته و یا در اثر اشتباهات کاربری حذف شوند. در ویندوز ۲۰۰۳ سرور ابزارهای مختلفی برای بازیابی اطلاعات یک سیستم یا کل سیستم وجود دارد که در این بخش ما به توضیح ابزار Backup برای پشتیبان گیری از ویندوز ۲۰۰۳ سرور می پردازیم.

۸-۱-۱- مشخص کردن مسائلی قبل از پشتیبان گیری:

قبل از شروع کردن به پشتیبان گیری باید موارد زیر را مشخص کنید:

- تعیین مجوز پشتیبان گیری

- تعیین نحوه پشتیبان گیری
- تعیین نوع اطلاعات پشتیبان گیری

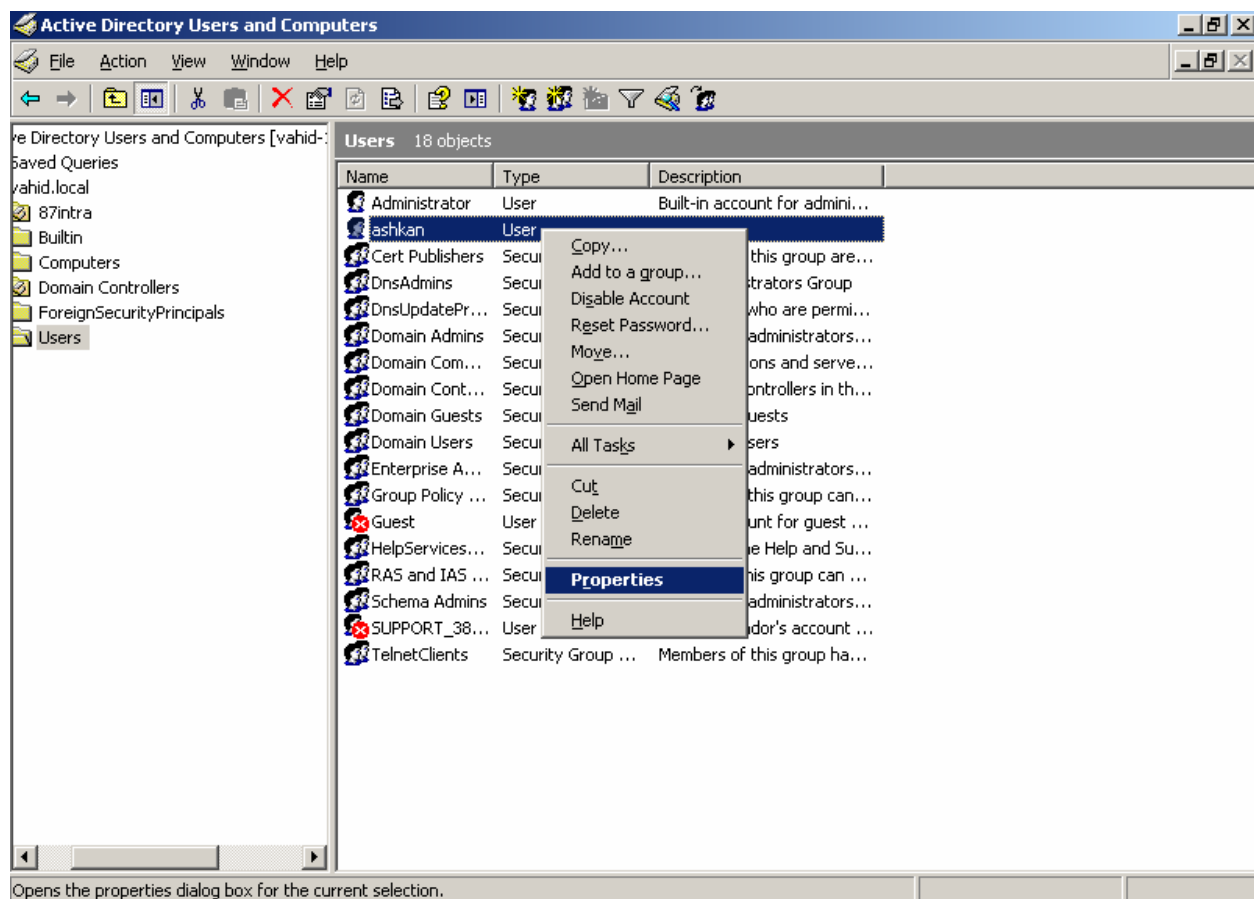
۱-۱-۱-۸- تعیین مجوز پشتیبان گیری:

برای پشتیبان گیری از فایل ها و پوشه های سیستم کاربر باید عضو گروه Administrator و یا عضو گروه Backup Operators باشد در غیر این صورت نمی تواند از فایل ها و پوشه های سرور پشتیبان بگیرد.

۱-۱-۱-۸- دادن مجوز Backup Operators:

اگر بخواهید به کاربری خاص مجوز Backup Operators بدهید این مراحل را طی نمایید:

در اکتیو دایرکتوری بر روی کاربری که می خواهید مجوز Backup Operators را بدهید راست کلیک کرده و Properties را انتخاب کنید.



بر روی زبانه Member Of کلیک کنید.

ashkan Properties

Member Of | Dial-in | Environment | Sessions

Remote control | Terminal Services Profile | COM+

General | Address | Account | Profile | Telephones | Organization

ashkan

First name: ashkan Initials:

Last name:

Display name: ashkan

Description:

Office:

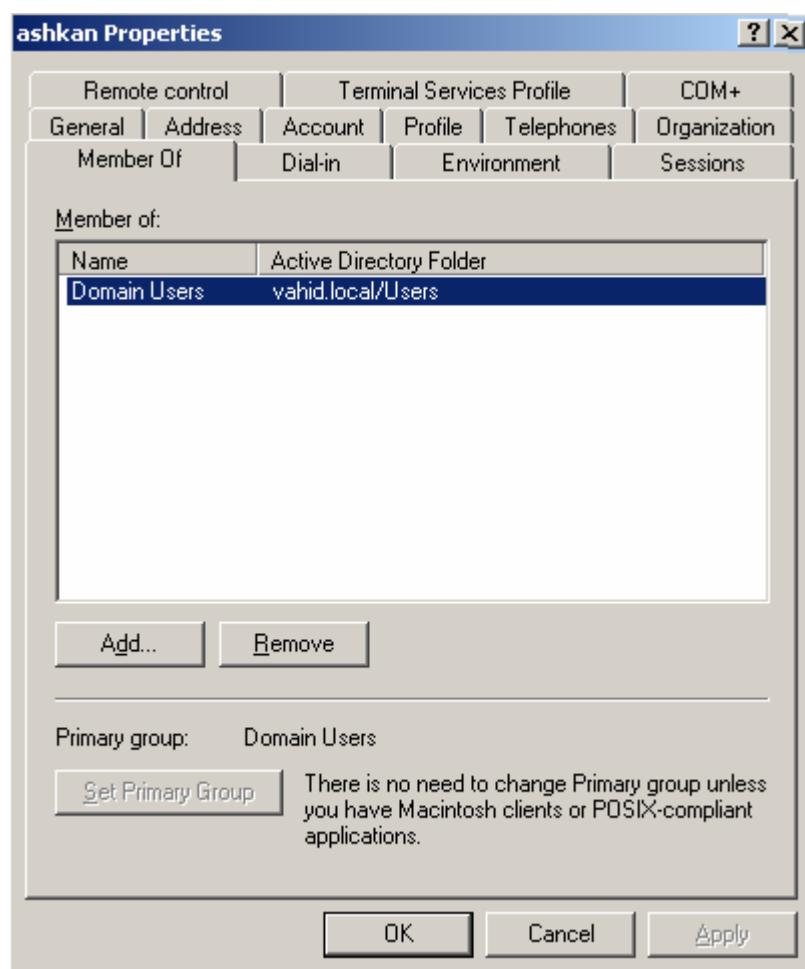
Telephone number: Other...

E-mail:

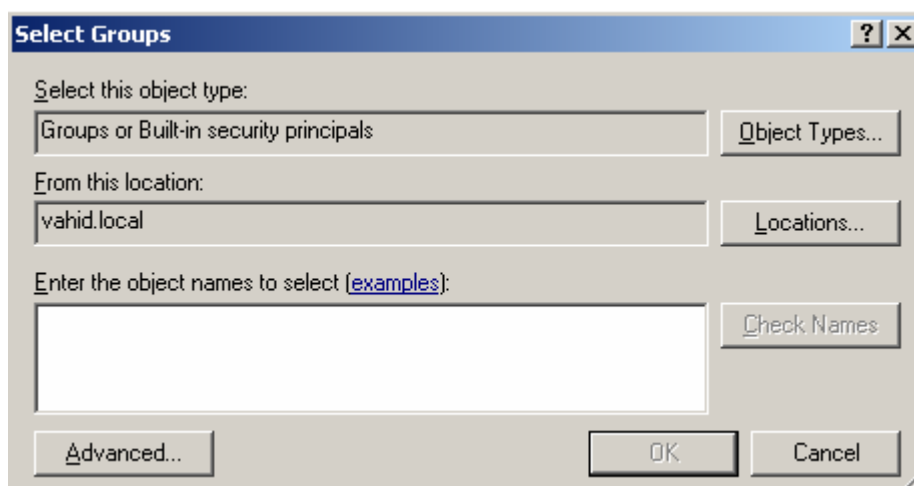
Web page: Other...

OK Cancel Apply

برای دادن مجوز بر روی Add کلیک کنید.



بر روی Advanced کلیک کنید.



در پنجره ظاهر شده بر روی Find Now کلیک کنید.

Select Groups [?] [X]

Select this object type:

From this location:

Common Queries


Name:

Description:

☐ Disabled accounts

☐ Non expiring password

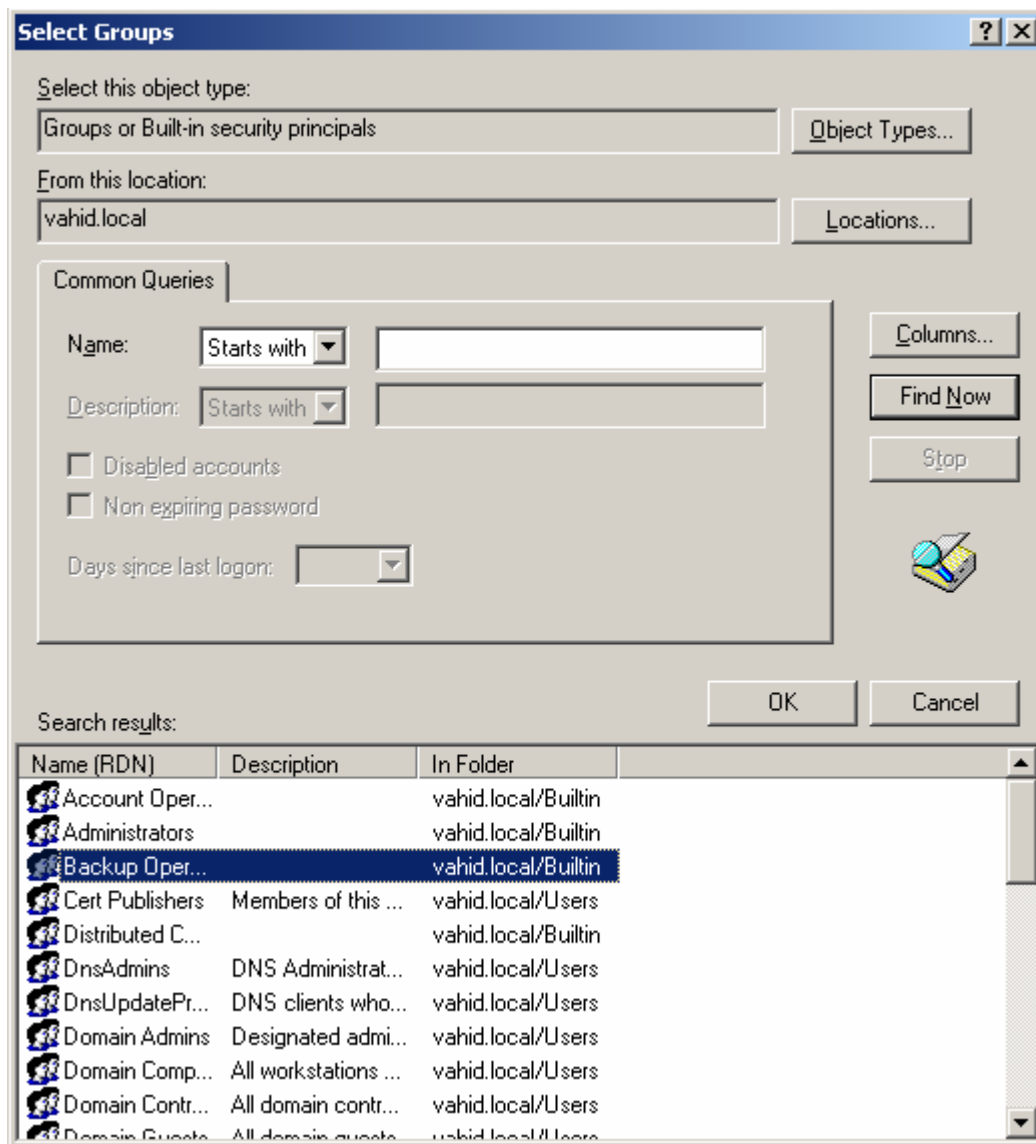
Days since last logon:



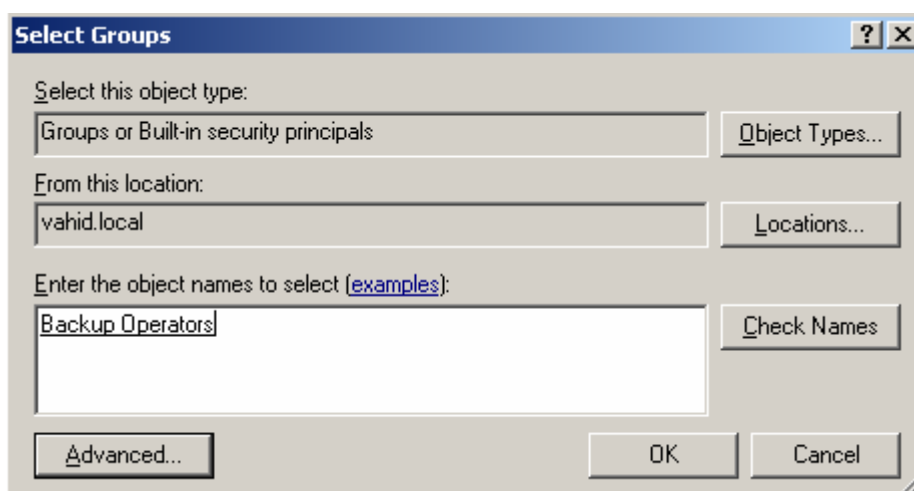
Search results:

Name (RDN)	Description	In Folder

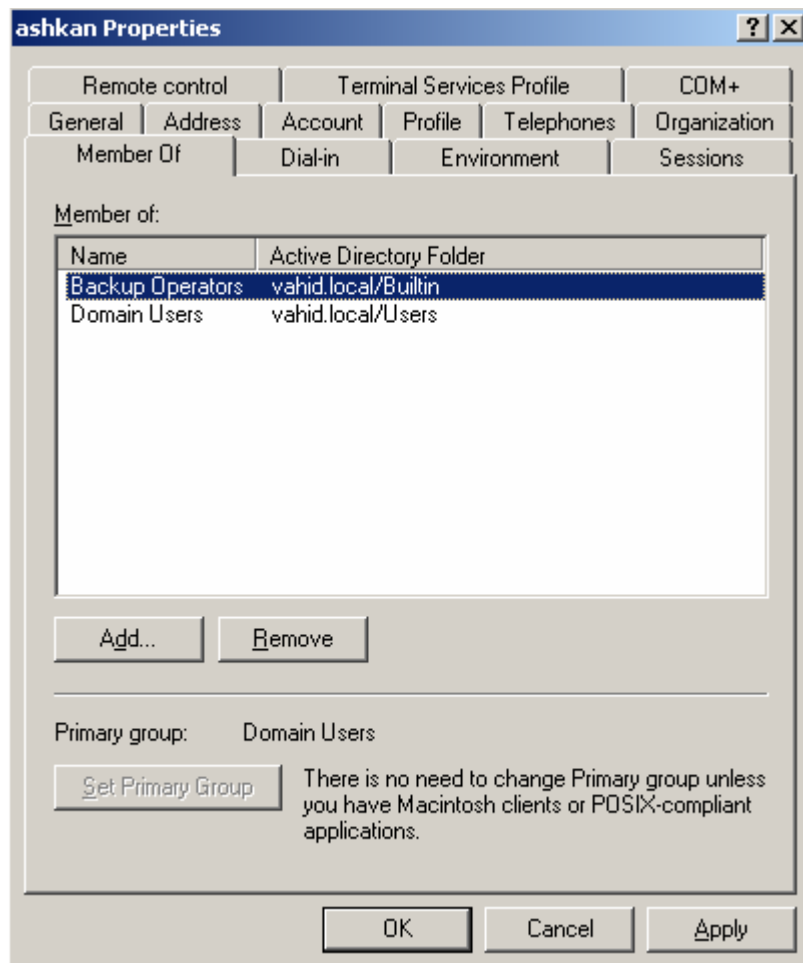
از لیست ظاهر شده Backup Operators کلیک کرده و OK کنید.



OK کنید.



در لیست Member Of مشاهده میکنید که مجوز Backup Operators به کاربر داده شده است. OK کنید.



بعد از انجام این مراحل کاربر Ashkan مجوز ورود به سرور و پشتیبان گیری از فایل های سرور را دارد.

۲-۱-۱-۸- تعیین نحوه پشتیبان گیری:

در ویندوز سرور ۲۰۰۳ پنج نوع پشتیبان گیری وجود دارد:

- Normal:
- Copy:
- Incremental:
- Differential:
- Daily:

۳-۱-۱-۸- تعیین نوع اطلاعات پشتیبان گیری:

به سه نوع می توانید از سیستم Backup بگیرید:

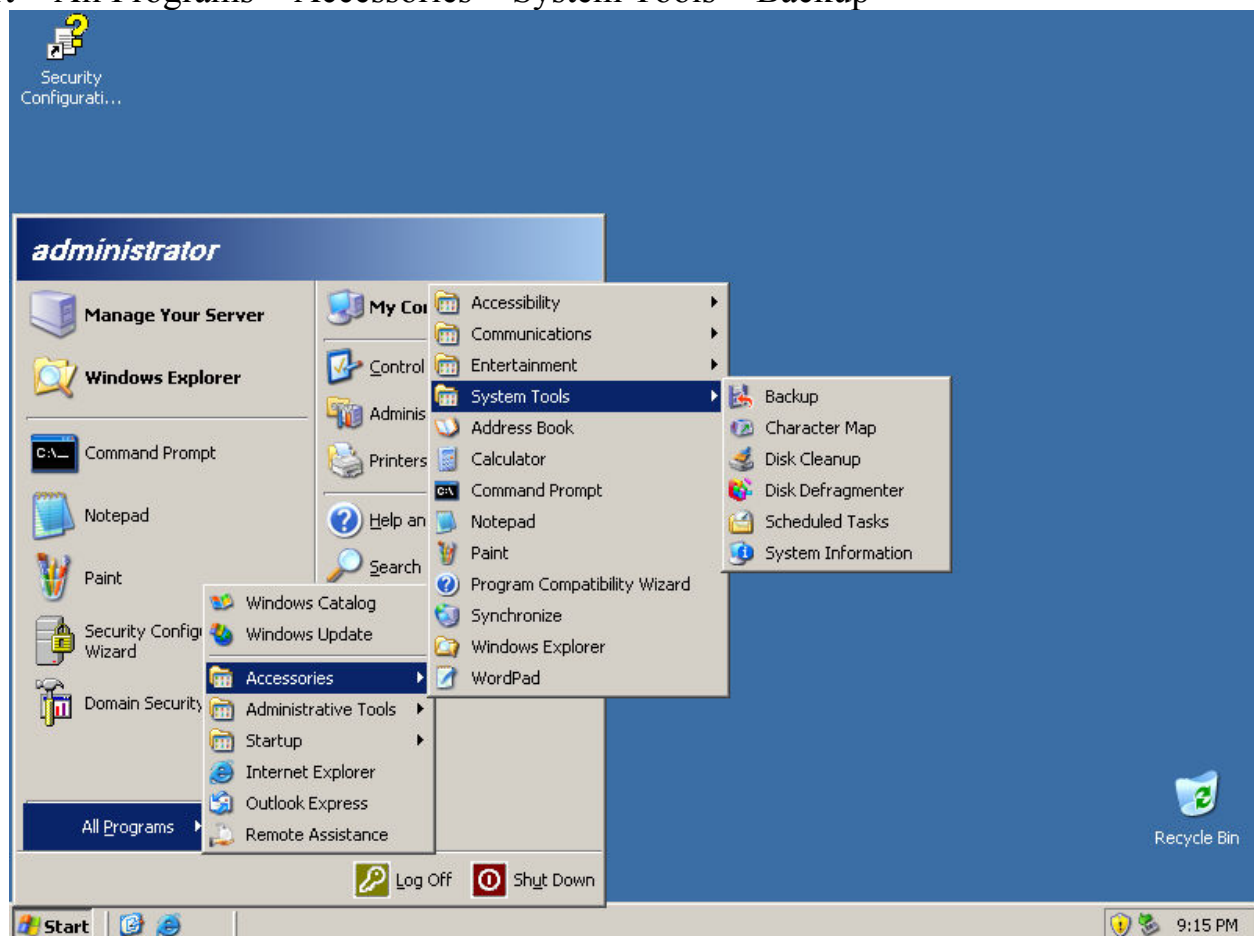
- پشتیبان گرفتن به صورت کامل (از همه چیز کامپیوتر)
- پشتیبان گرفتن فقط از فایل های انتخابی
- پشتیبان گرفتن از System State (اطلاعات مربوط به تنظیمات سیستمی: رجستری، پایگاه داده، کنترل کننده دامنه، اکتیو دایرکتوری و...)

۲-۱-۸- شروع به پشتیبان گیری:

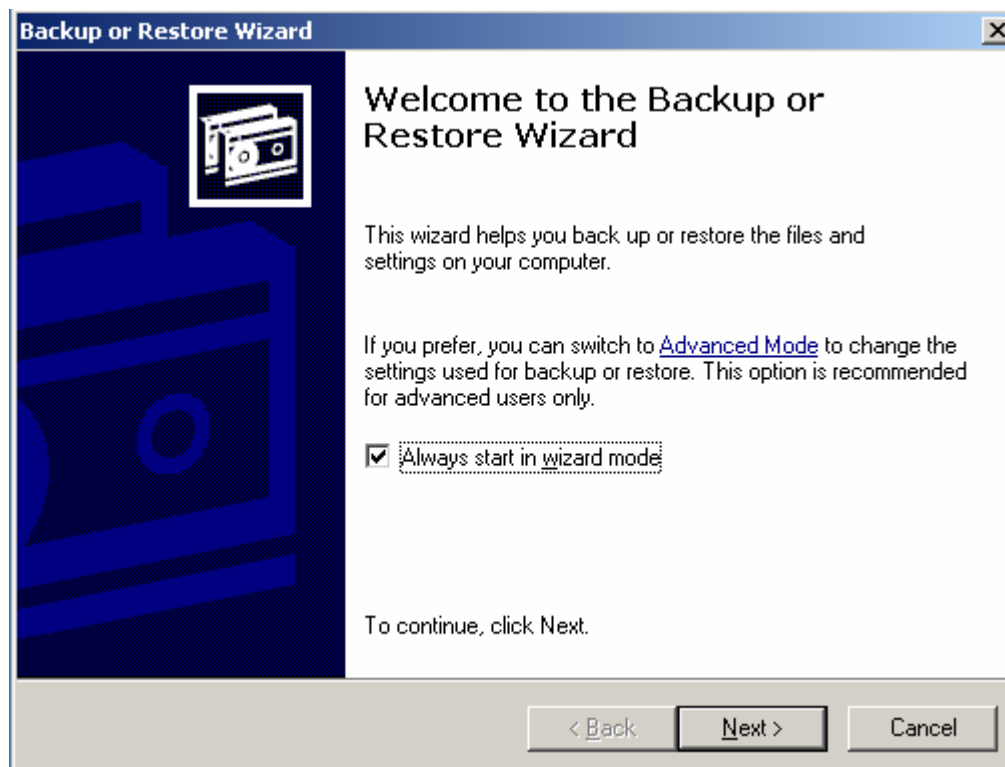
برای استفاده از ابزار Backup این مراحل را انجام دهید:

به مسیر زیر بروید:

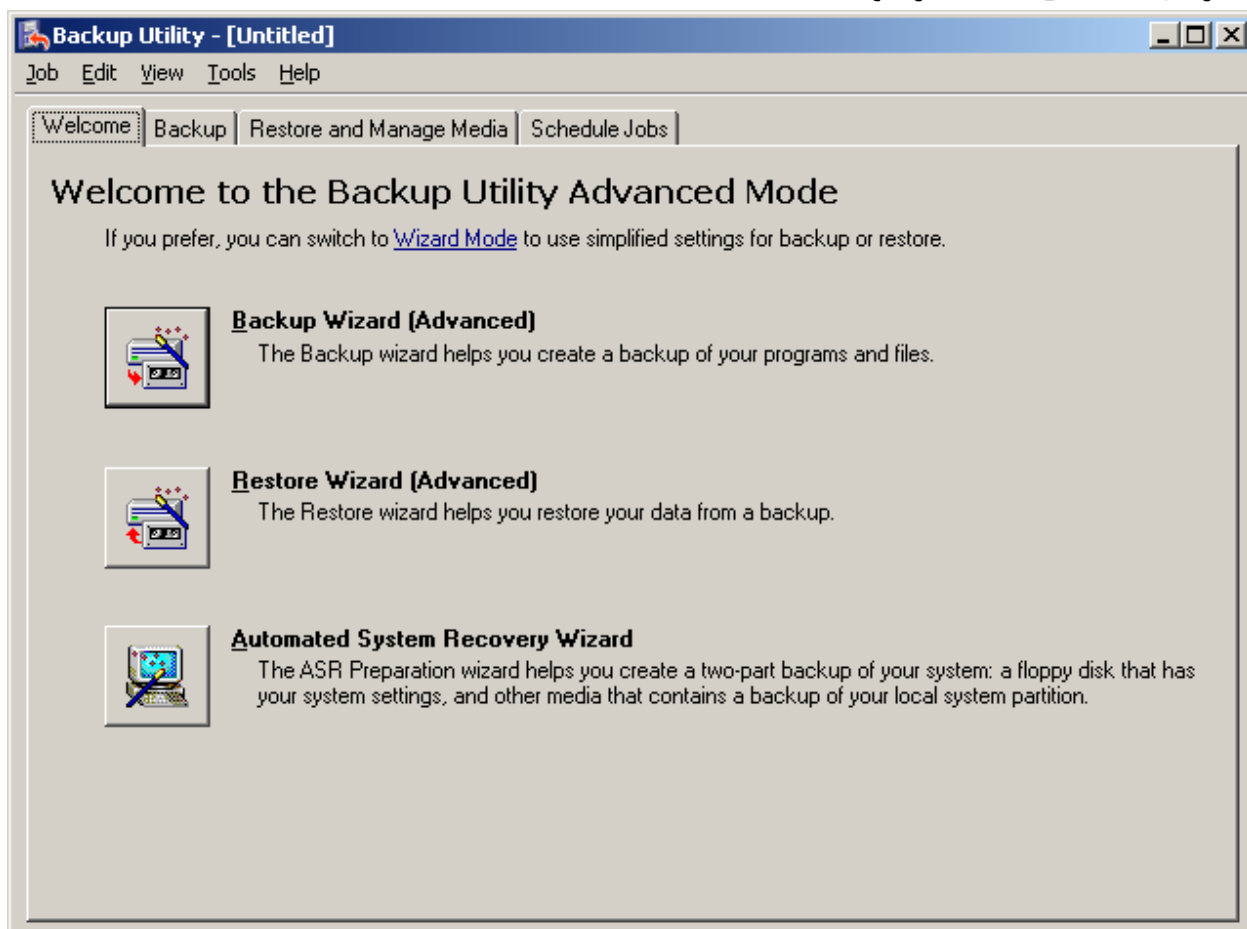
Start > All Programs > Accessories > System Tools > Backup



پنجره خوش آمدگویی به Backup or Restore ظاهر می شود. اگر می خواهید با تنظیمات پیش فرض پشتیبان بگیرید بر روی Next کلیک کرده و پنجره های آن را طی نمایید. روش دوم این است که تنظیمات پشتیبان گیری را خودتان تنظیم نمایید برای این کار بر روی Advanced Mode کلیک نمایید.

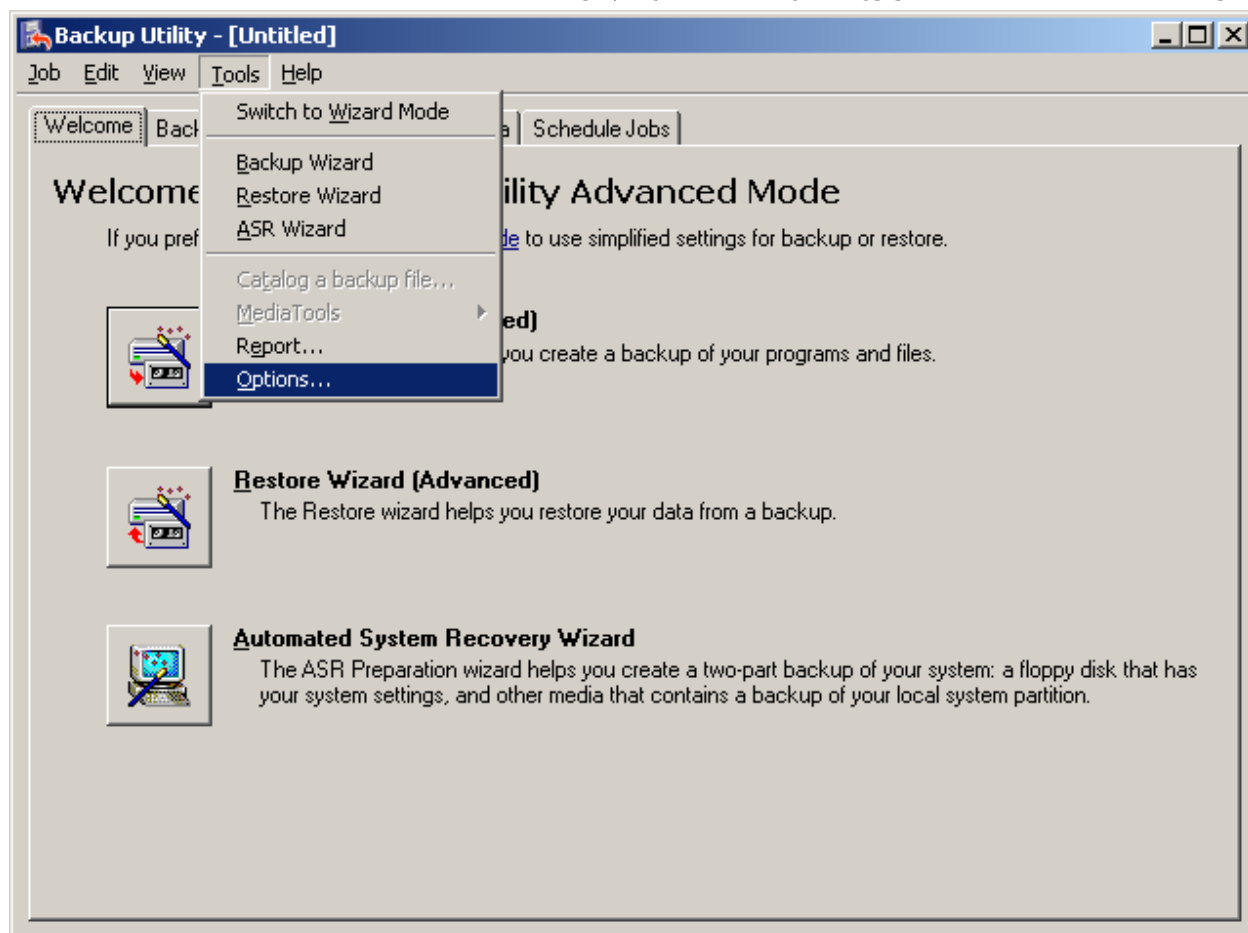


پنجره Backup Utility باز شود.



۱-۲-۸- پیکربندی تنظیمات Backup:

برای پیکربندی تنظیمات Backup بر روی منوی Tools و سپس Options کلیک نمایید.



در پنجره Options می توانید تنظیمات پیش فرض را بر حسب نیازتان تغییر دهید.

تنظیمات برگه General:

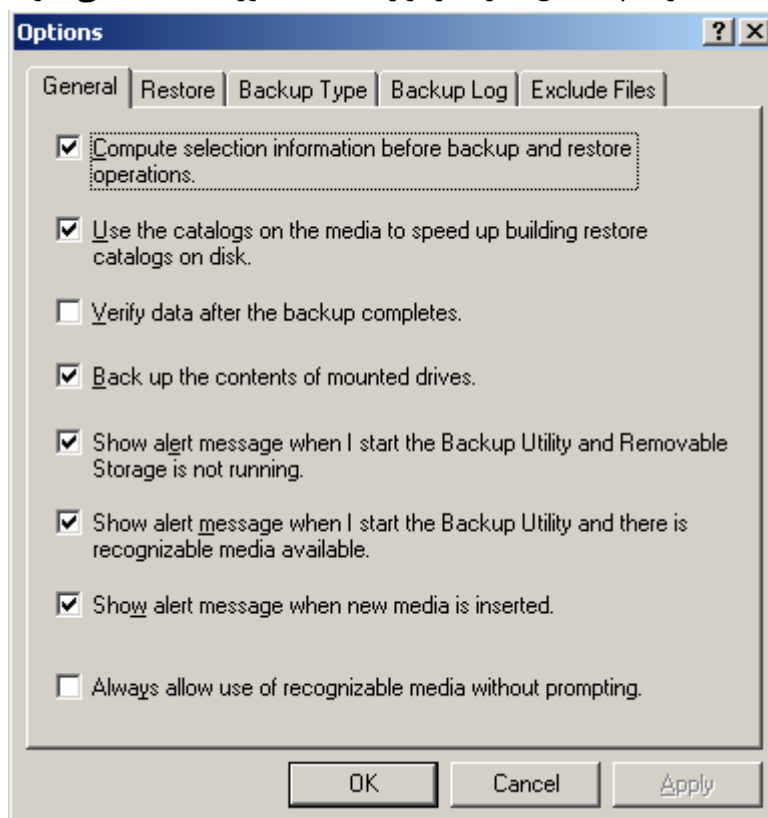
Compute selection information before backup and restore operations: اگر کادر مربوط به این گزینه را انتخاب نمایید سیستم قبل از شروع به پشتیبان گرفتن تعداد فایل ها و پوشه های انتخاب شده برای پشتیبان گیری را محاسبه و نمایش می دهد.

Use the catalogs on the media to speed up building restore catalogs on disk: اگر این گزینه را انتخاب کنید سیستم قبل از Restore کردن یک کاتالوگ در دیسک می سازد.

Verify data after the backup completes: با انتخاب این گزینه بعد از اتمام پشتیبان گیری یک بررسی برای اطمینان از درست انجام شدن فرایند پشتیبان گیری صورت می گیرد

Back up the contents of mounted drives: اگر درایوتان بالا برده شده باشد و بخواهید از آن پشتیبان بگیرید باید این گزینه را انتخاب کنید. اگر این گزینه را انتخاب نکنید فقط از مسیر درایو بالا برده شده پشتیبان گرفته می شود.

گزینه های بعدی زمانی استفاده می شود که بخواهید برای پشتیبان گیری از سرویس Removable Storage استفاده نمایید. (Removable Storage برای پشتیبان گیری از نوار یا دیسک نوری استفاده می شود)



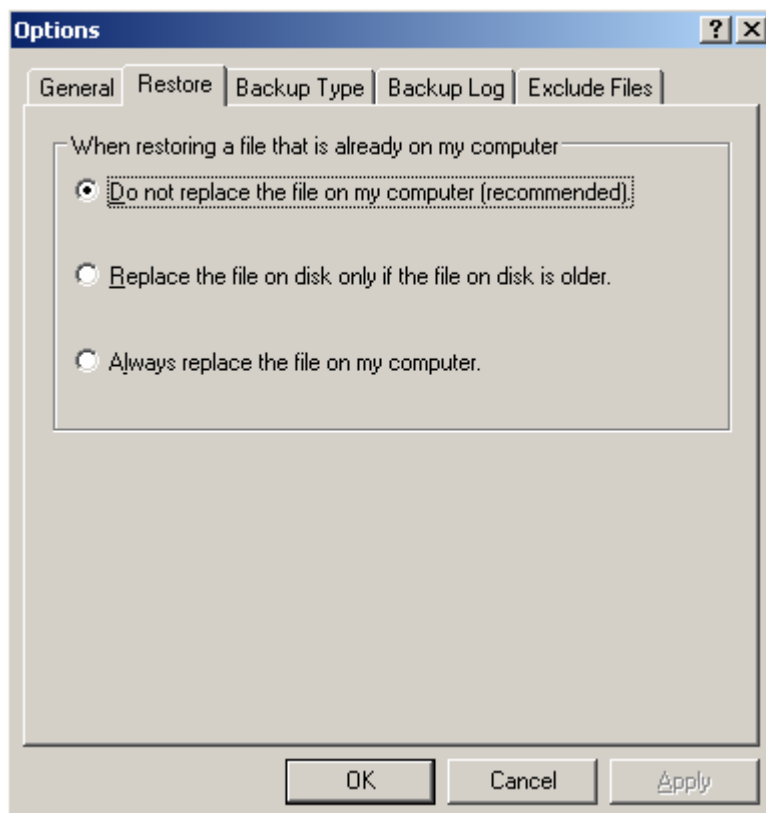
تنظیمات برگه Restore:

تنظیمات برگه Restore برای بازیابی اطلاعات استفاده می شود و شامل سه گزینه می باشد که باید یکی از آنها را انتخاب کنید:

Do not replace the file on my computer (recommended): عدم جایگزینی فایل های پشتیبانی موجود

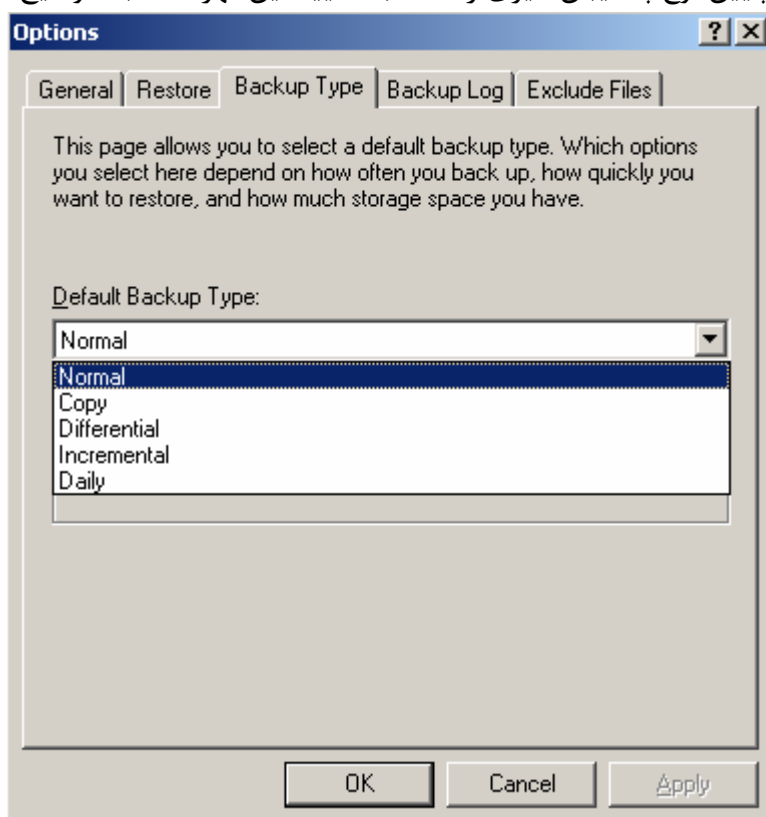
Replace the file on disk only if the file on disk is older: در صورتی که فایل های پشتیبان گرفته شده از فایل های روی سیستم جدیدتر باشد Restore صورت گیرد.

Always replace the file on my computer: در هر صورت فایل های جایگزین صورت گیرد.



تنظیمات برگه Backup Type:

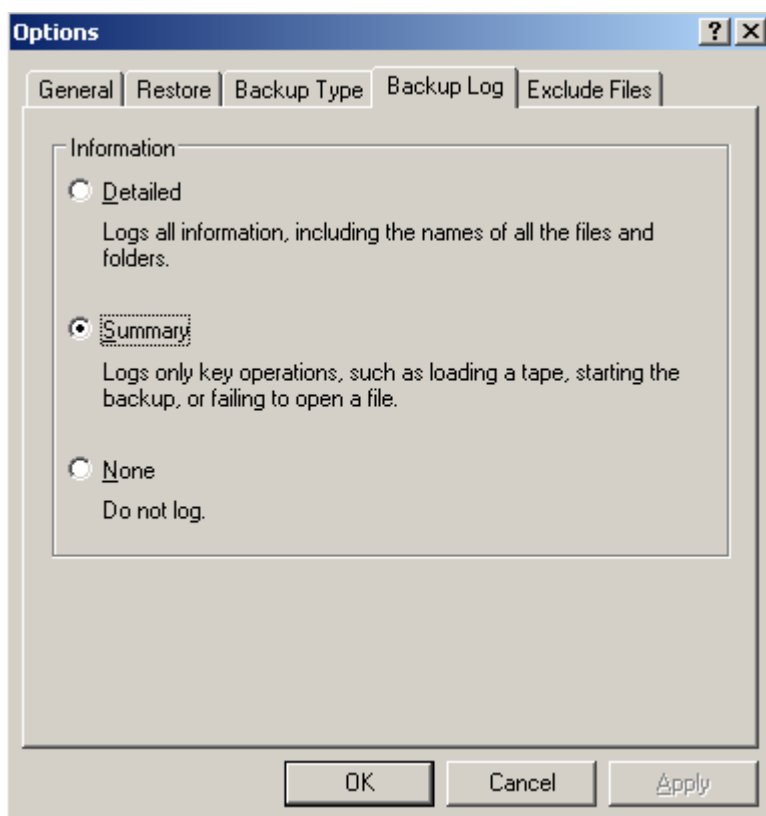
شما باید از فهرست کشویی پایین نوع پشتیبان گیری را انتخاب نمایید (این فهرست قبلاً توضیح داده شده است)



تنظیمات برگه Backup Log:

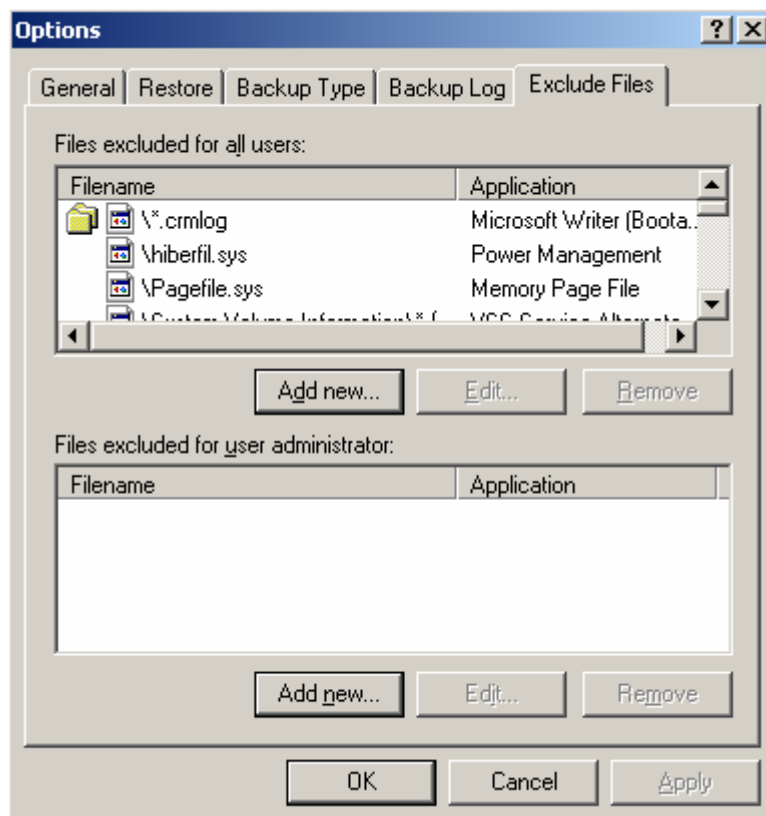
این برگه مربوط به نحوه گزارشگیری بعد از پایان پشتیبان گیری می باشد که شامل سه گزینه می باشد:
 Detailed: گزارشگیری همراه با جزئیات باشد.
 Summary: گزارشگیری به صورت چکیده باشد.

None: گزارشگیری نشود.



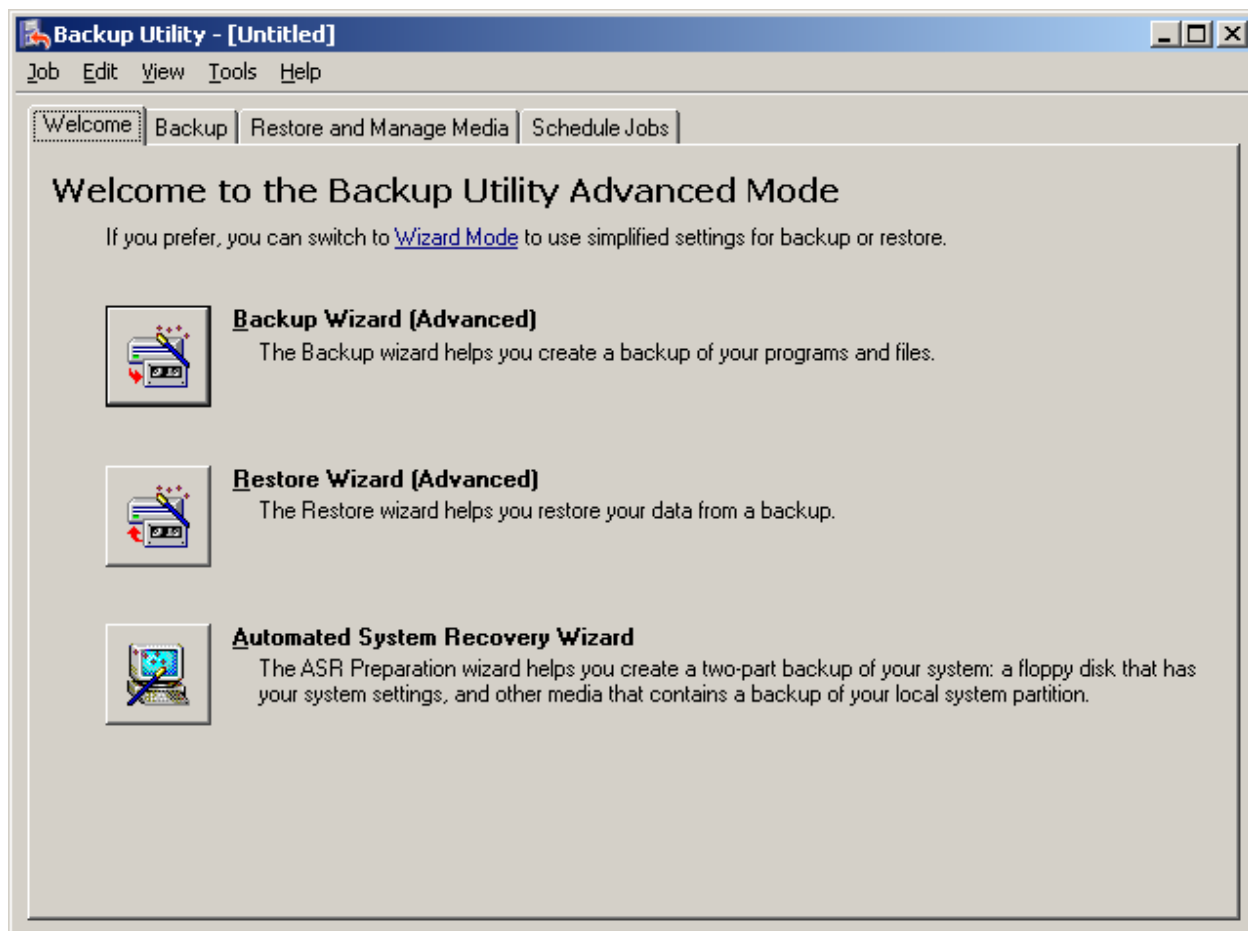
تنظیمات برگه **Exclude Files**:

در این برگه لیست فایل هایی که از آنها پشتیبان گرفته نمی شود نمایش داده می شود که می توانید با کلیک بر روی Add new فایل هایی را به این لیست اضافه نمایید.



۲-۲-۱-۸- ایجاد یک پشتیبان گیری:

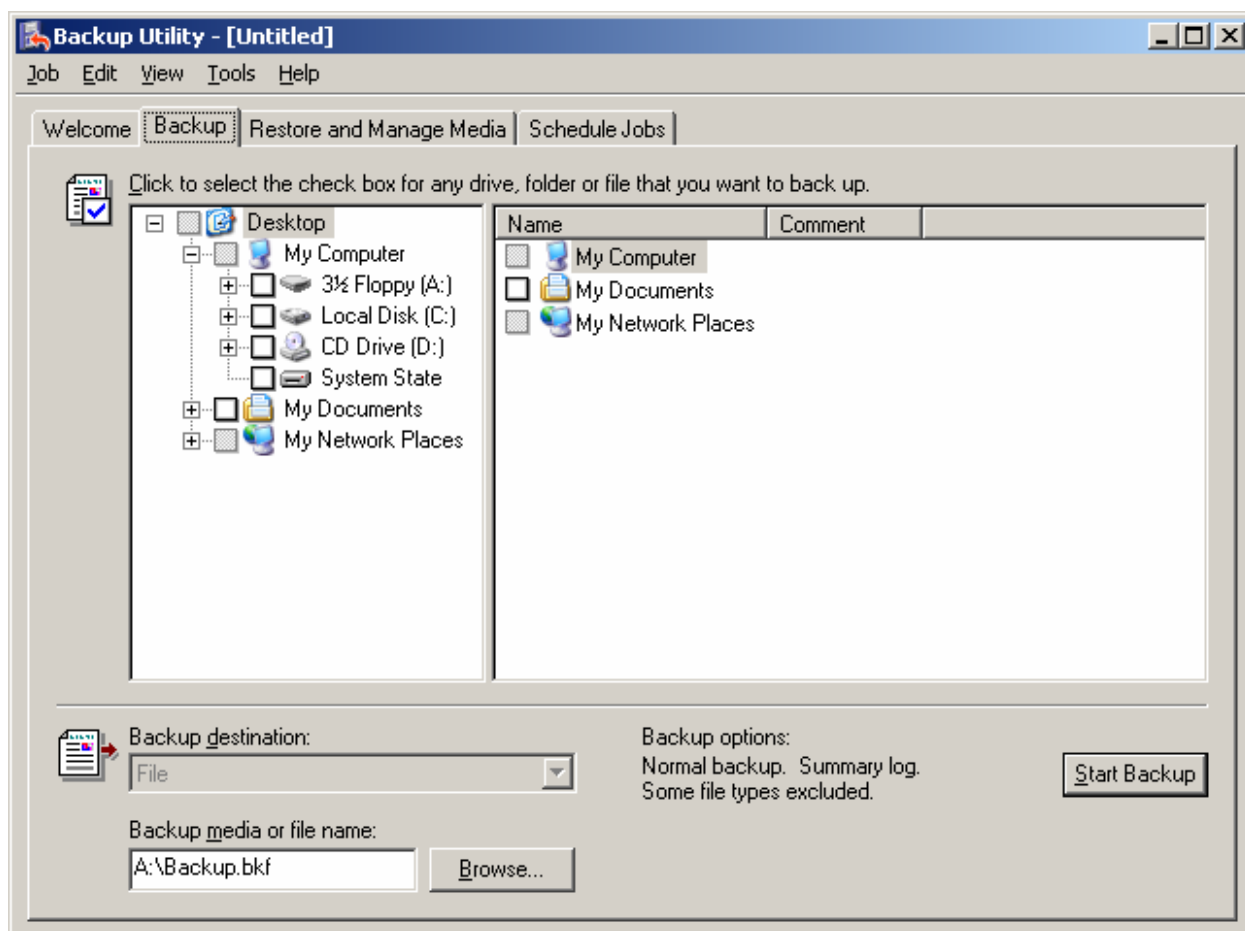
برای گرفتن پشتیبان این مراحل را طی نمایید:
در پنجره Backup Utility بر روی زبانه Backup کلیک نمایید.



در این پنجره باید اجزایی (کل سیستم، فایل های انتخابی، System State) را که می خواهید از آنها پشتیبان گیری صورت بگیرید را انتخاب نمایید.

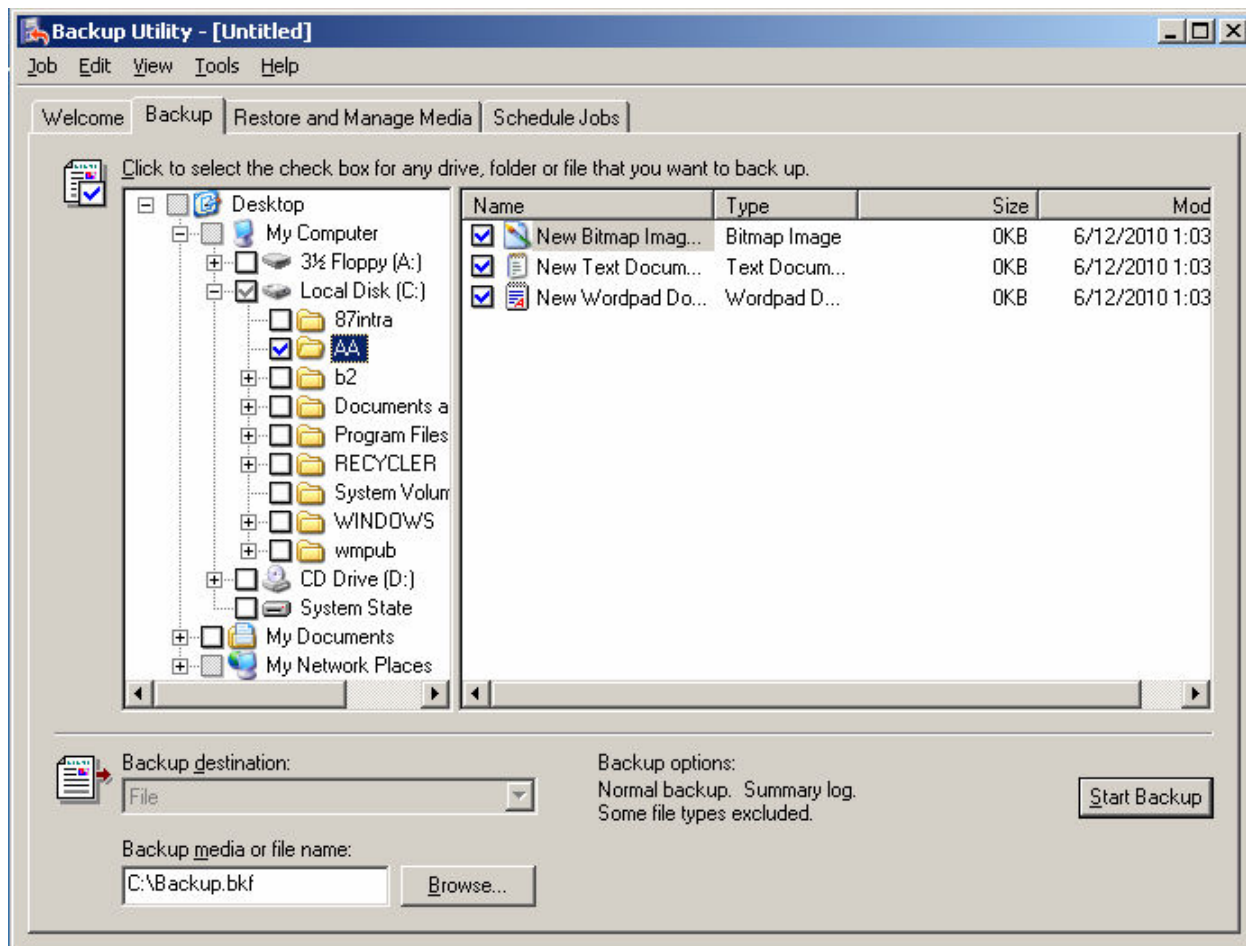
در پایین پنجره Backup برای انتخاب محل ذخیره پشتیبان دو گزینه وجود دارد:

- Backup destination: پشتیبان گیری روی نوار (اگر سیستم یک وسیله نوار را تشخیص دهد این گزینه فعال می شود).
- Backup media or file name: پشتیبان گیری روی یک درایو.



در این قسمت ما می خواهیم برای درک بهتر شما از پوشه ای به نام AA که در درایو C سیستم ما وجود دارد پشتیبان بگیریم. برای پشتیبان گیری این مراحل را انجام می دهیم:

- ۱- پوشه AA را انتخاب می کنیم.
- ۲- بر روی Brows کلیک کرده و مسیری را برای ذخیره فایل پشتیبان انتخاب می نماییم.
- ۳- بر روی Start Backup کلیک می نماییم.



۴- پنجره زیر نمایش داده می شود که اطلاعات بیشتری را در باره فایل پشتیبان در اختیار ما می گذارد:

- **Append this backup to the media:** اگر این گزینه را انتخاب کنیم در مسیری که فایل پشتیبان ما ذخیره می شود اگر فایل پشتیبان دیگری هم قبلاً در آن مسیر ذخیره کرده باشیم، این فایل پشتیبان به آن چسبیده می شود.
- **Replace the data on the media with this backup:** با انتخاب این گزینه فایل پشتیبان جدید را بر روی فایل پشتیبان قبلی می نویسد.

اگر بر روی **Advanced** کلیک نماییم انتخاب های پیکربندی **Backup** نمایش داده می شود که ما قبلاً راجع به پیکربندی **Backup** توضیح داده ایم.

Schedule : مربوط به زمان بندی برای گرفتن پشتیبان می باشد که در قسمت های بعد توضیح خواهیم داد.

۵- بر روی **Start Backup** کلیک می نماییم.

Backup Job Information [?] [X]

Backup description:



If the media already contains backups:
☒ Append this backup to the media.
☐ Replace the data on the media with this backup.

If the media is overwritten, use this label to identify the media:

☐ Allow only the owner and the Administrator access to the backup data.

۶- برنامه شروع به پشتیبان گرفتن می نماید.

Backup Progress [?] [X]

Drive:

Label:

Status:

Progress:

Elapsed:

Time:

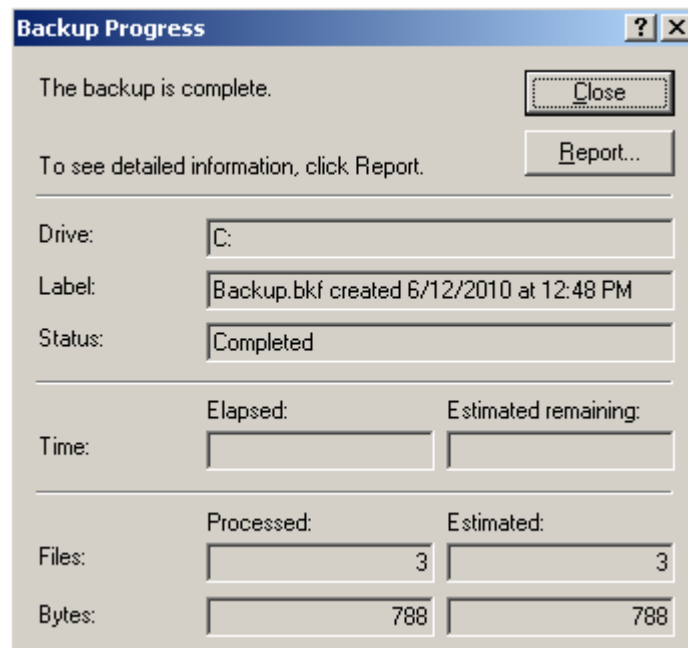
Processing:

Processed:

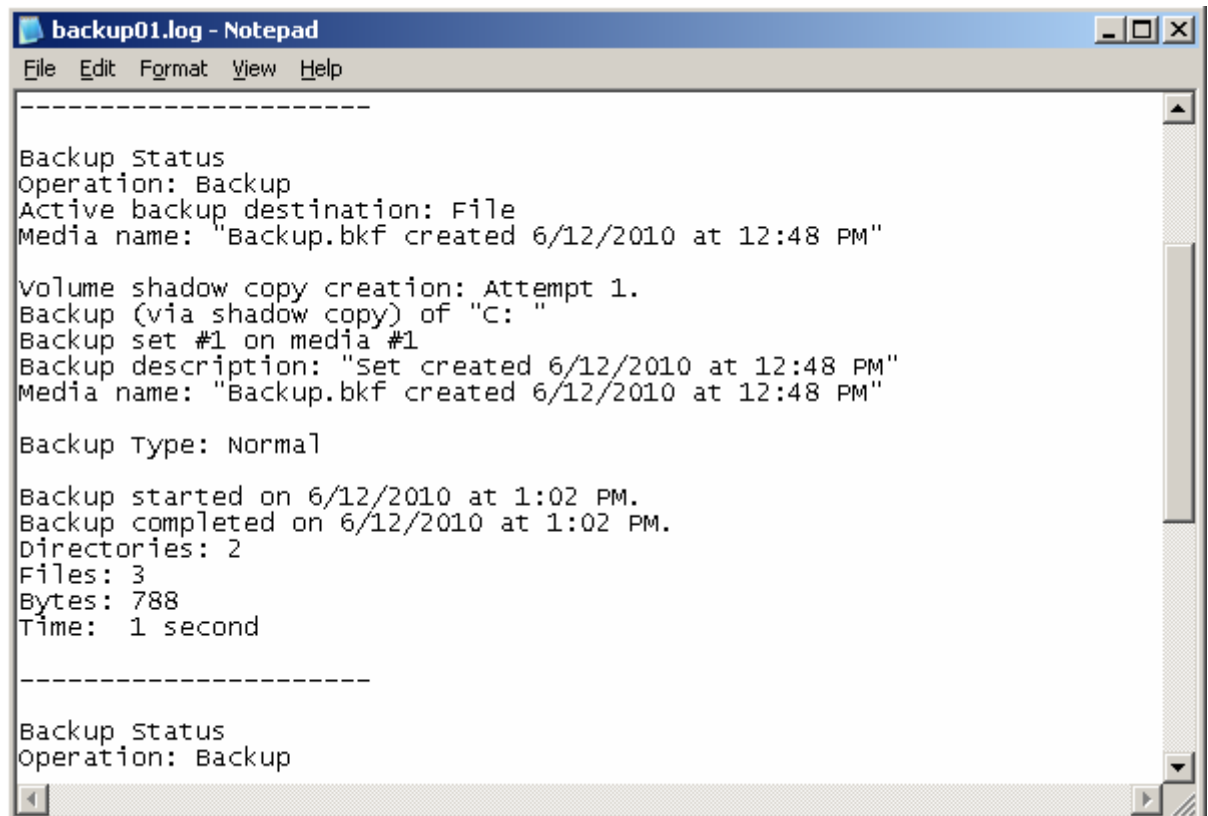
Files:

Bytes:

۷- بعد از اتمام فرایند پشتیبان گیری دکمه Report نمایش داده می شود.



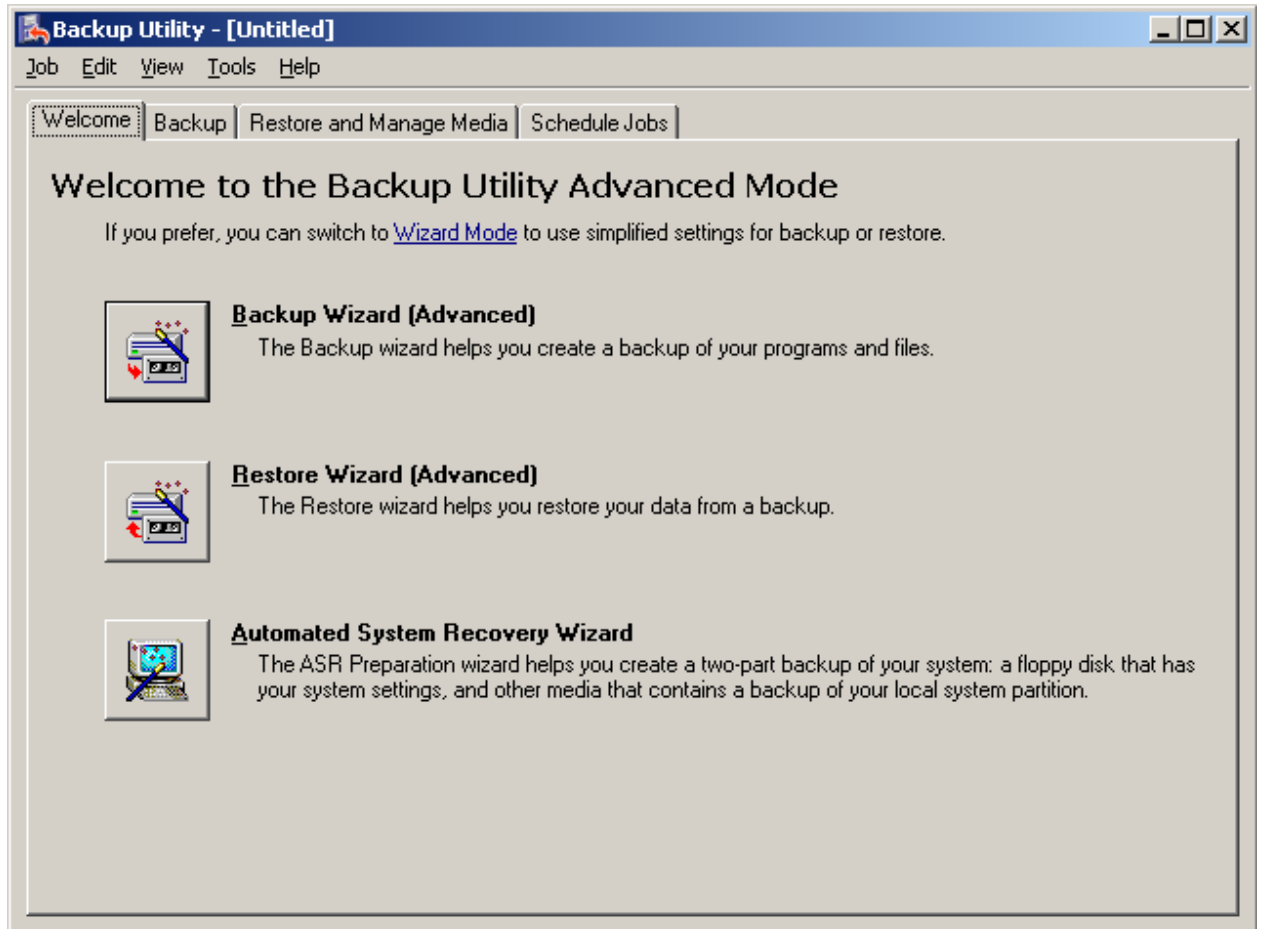
۸- برای دیدن گزارش پشتیبان گیری بر روی آن کلیک می نماییم.



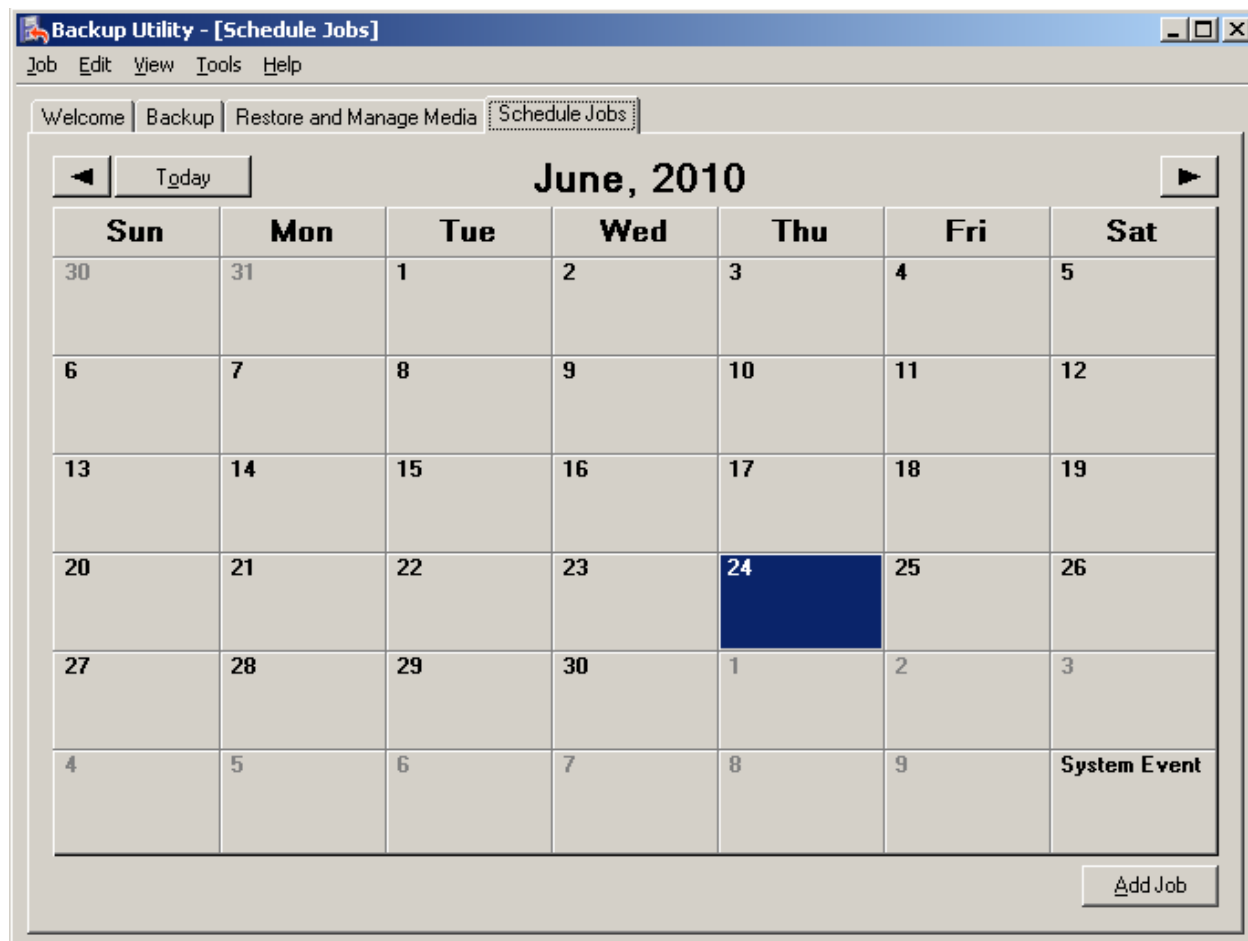
۳-۲-۱-۸- زمانبندی کردن پشتیبان گیری:

اگر می خواهید فرایند پشتیبان گیری را زمانبندی کنید تا در روزهای مشخص پشتیبان گیری به صورت اتوماتیک صورت پذیرد این مراحل را انجام دهید.

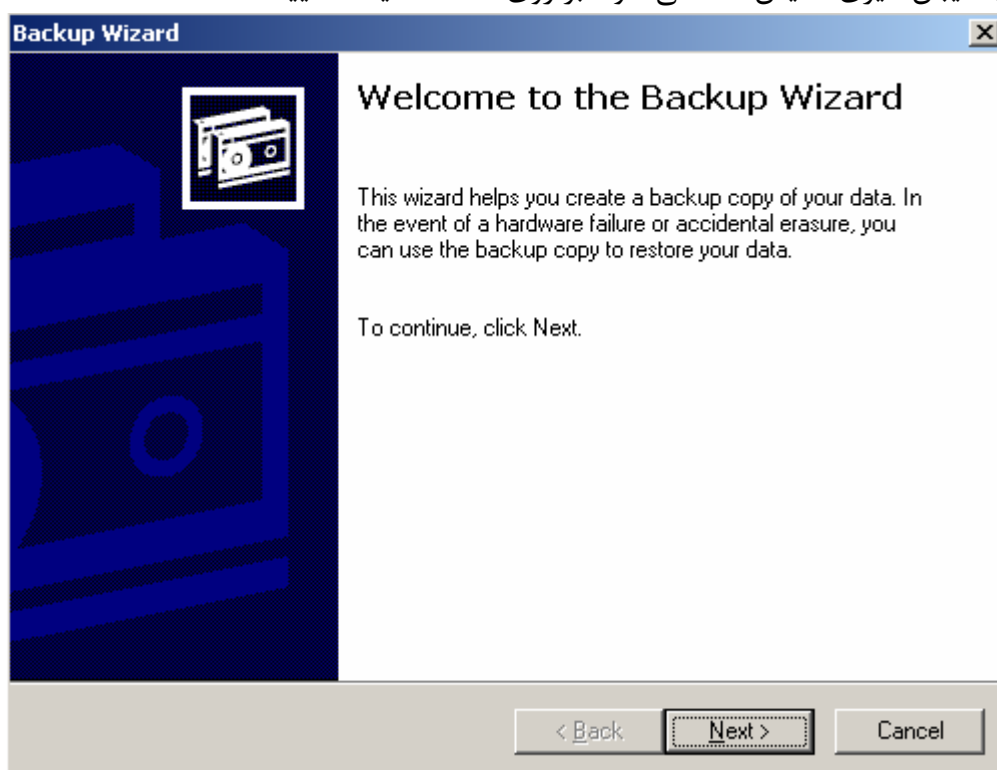
در پنجره Backup Utility بر روی برگه Schedule Jobs کلیک نمایید.



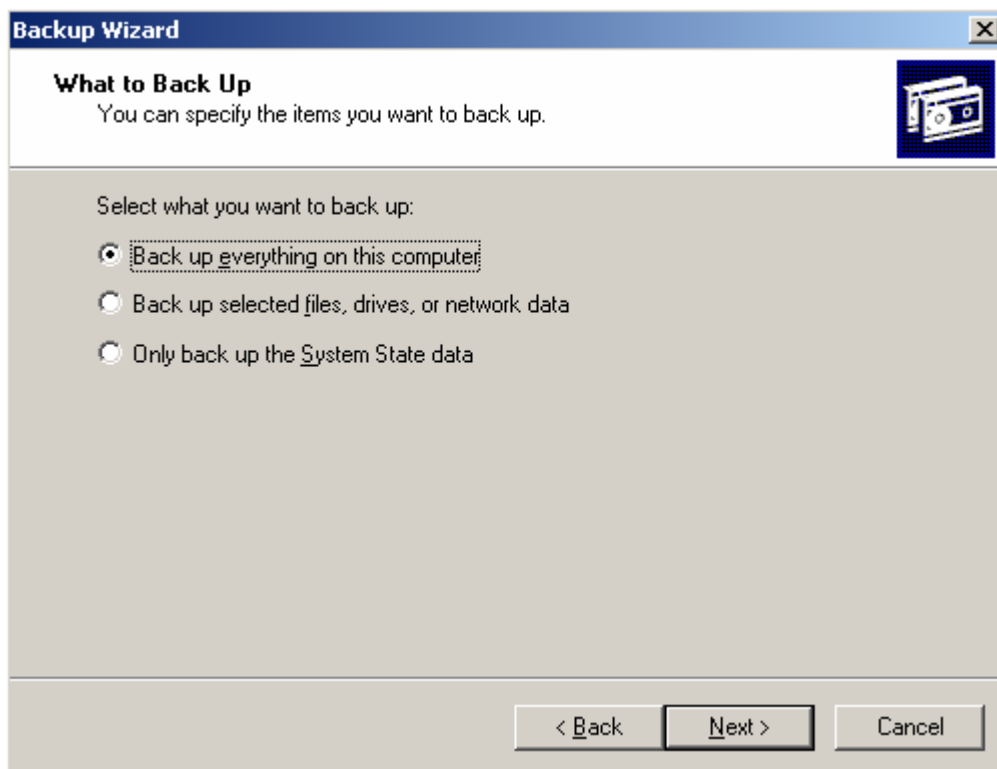
در برگه Schedule Jobs بر روی Add Job کلیک نمایید.



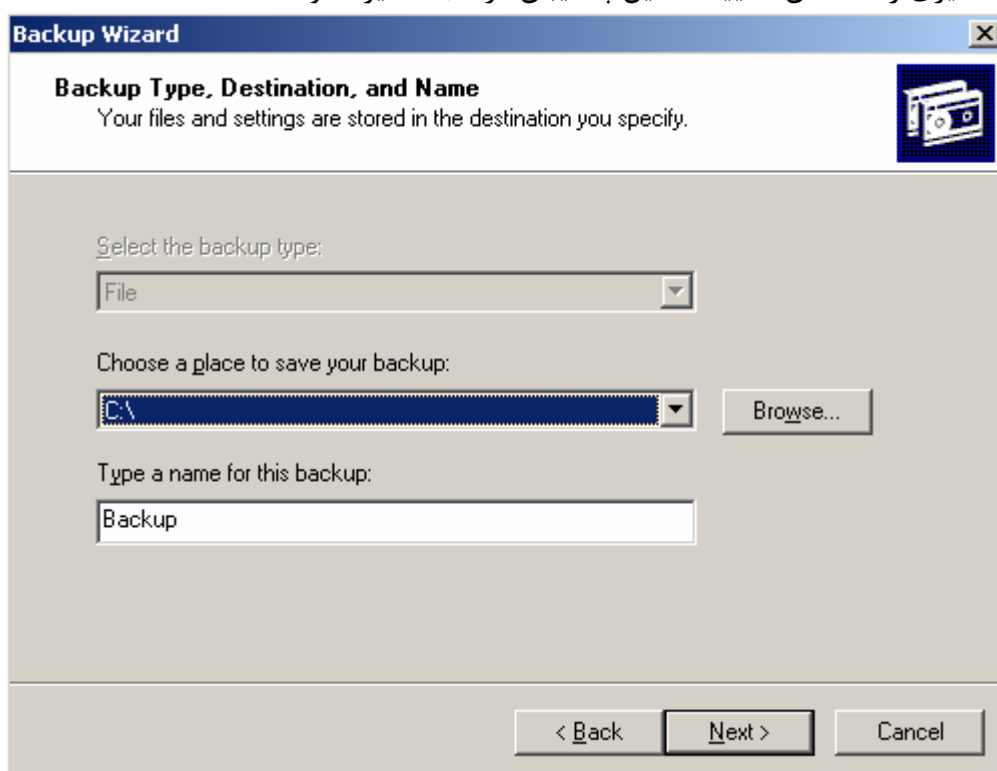
پنجره Wizard پشتیبان گیری نمایش داده می شود. بر روی Next کلیک نمایید.



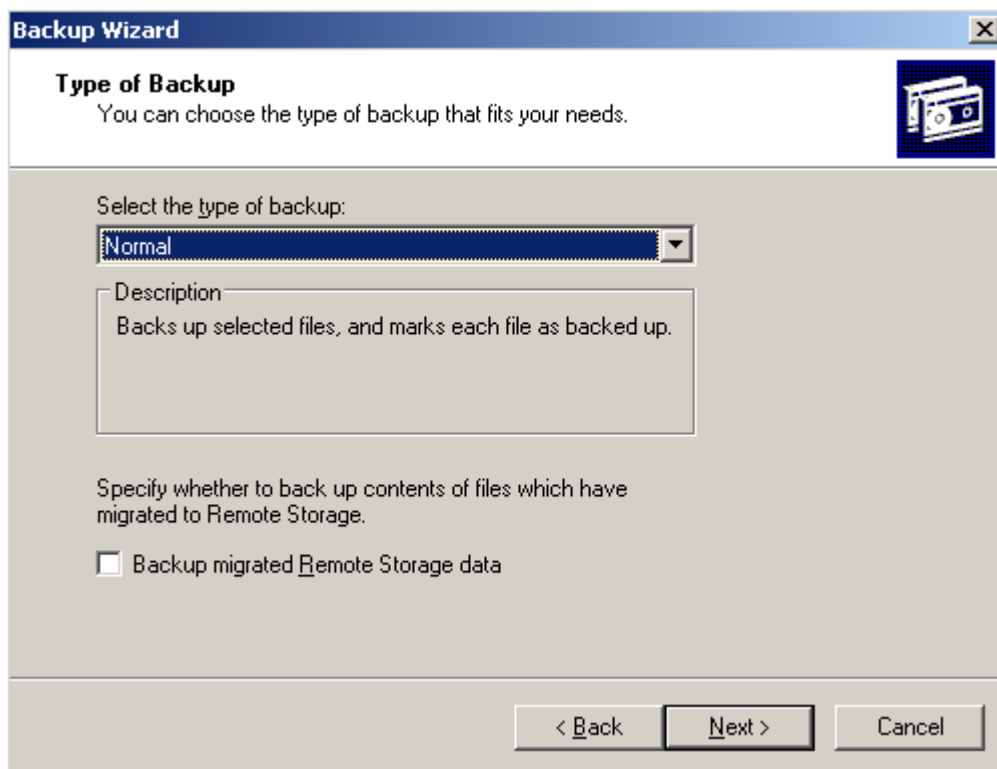
در این پنجره باید اجزایی را که می خواهد برای پشتیبان گیری از آن زمانبندی کنید را انتخاب کرده و Next نمایید.



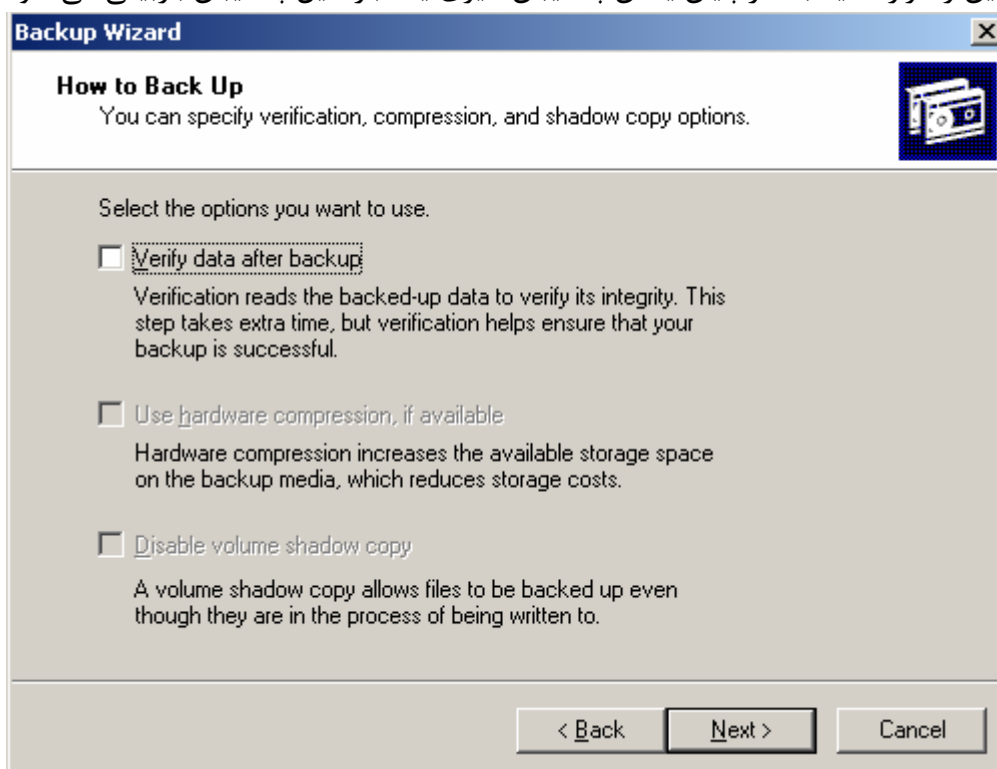
در این پنجره باید مسیری را مشخص نمایید تا فایل پشتیبان در آنجا ذخیره شود.



در این پنجره باید نوع پشتیبان گیری را انتخاب نمایید و بر روی Next کلیک نمایید.



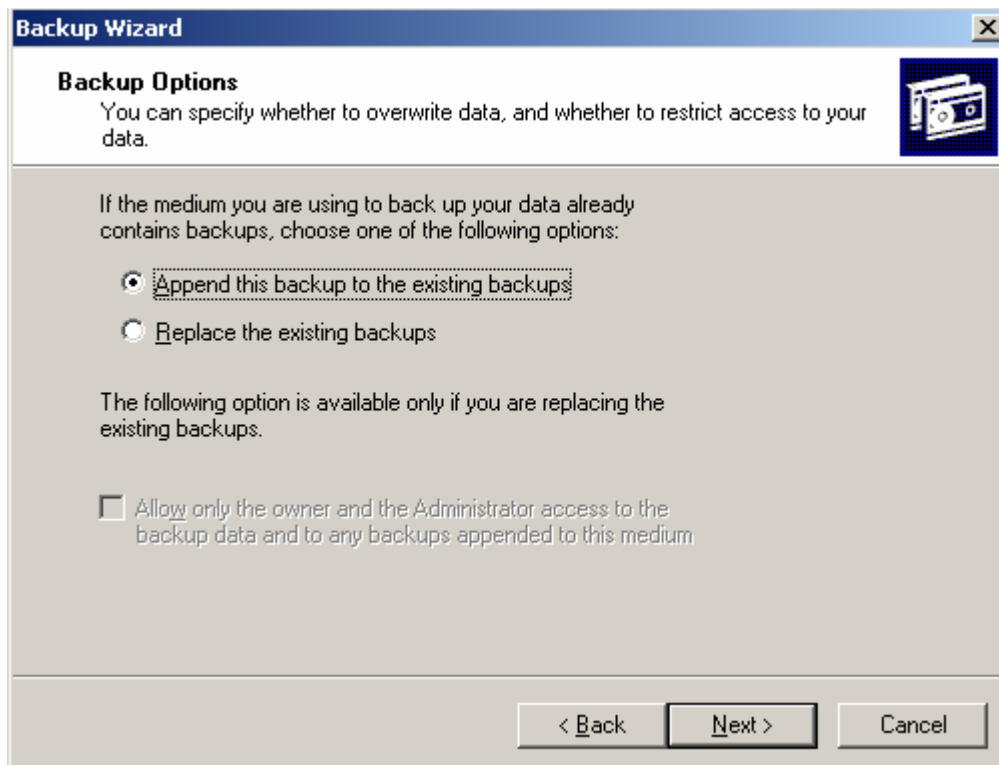
اگر تیک گزینه پایین را قرار دهید بعد از پایان یافتن پشتیبان گیری یک بار فایل پشتیبان بازیابی می شود.



در این پنجره دو انتخاب وجود دارد:

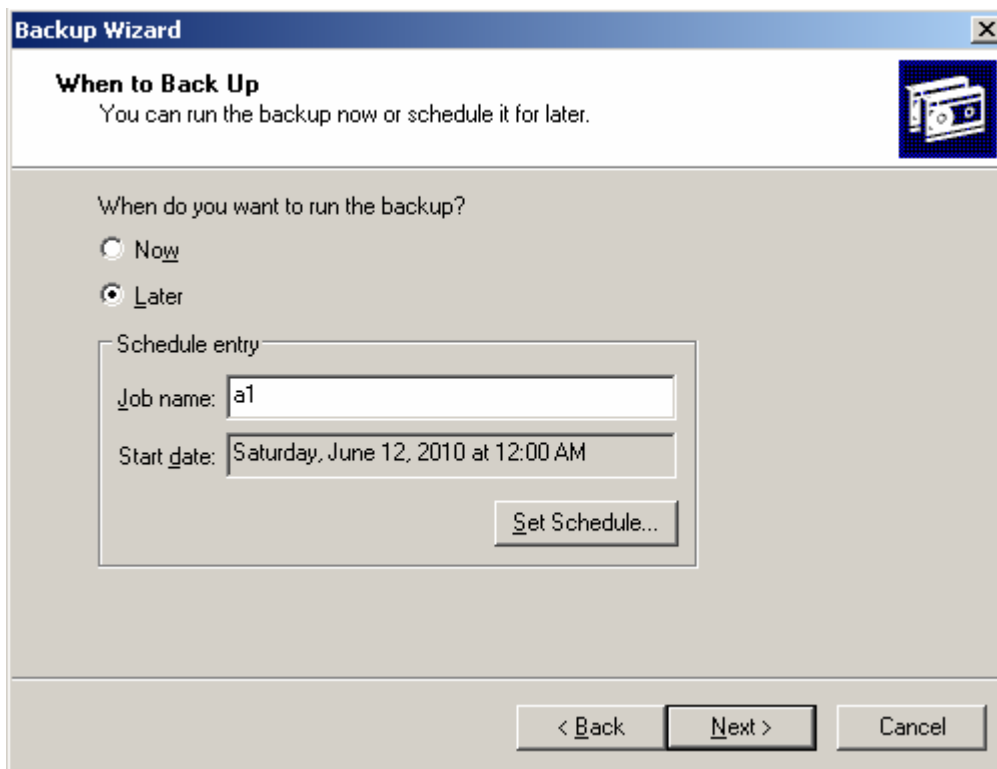
- Append this backup to the existing backups: اگر این گزینه را انتخاب کنیم در مسیری که فایل پشتیبان ما ذخیره می شود اگر فایل پشتیبان دیگری هم قبلاً در آن مسیر ذخیره کرده باشیم، این فایل پشتیبان به آن چسبیده می شود.

- **Replace the existing backups:** با انتخاب این گزینه فایل پشتیبان جدید را بر روی فایل پشتیبان قبلی می نویسد.

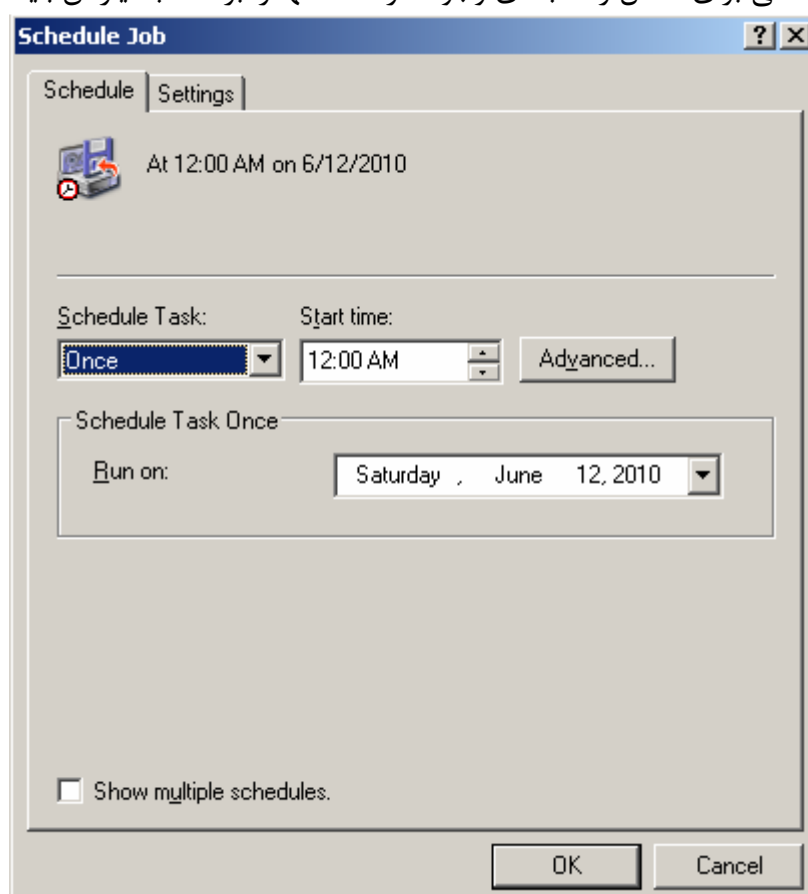


در این پنجره دو انتخاب برای زمانی که می خواهید فرایند پشتیبان گیری صورت گیرد وجود دارد:
Now: از اکنون شروع شود.
Later: بعداً شروع نماید.

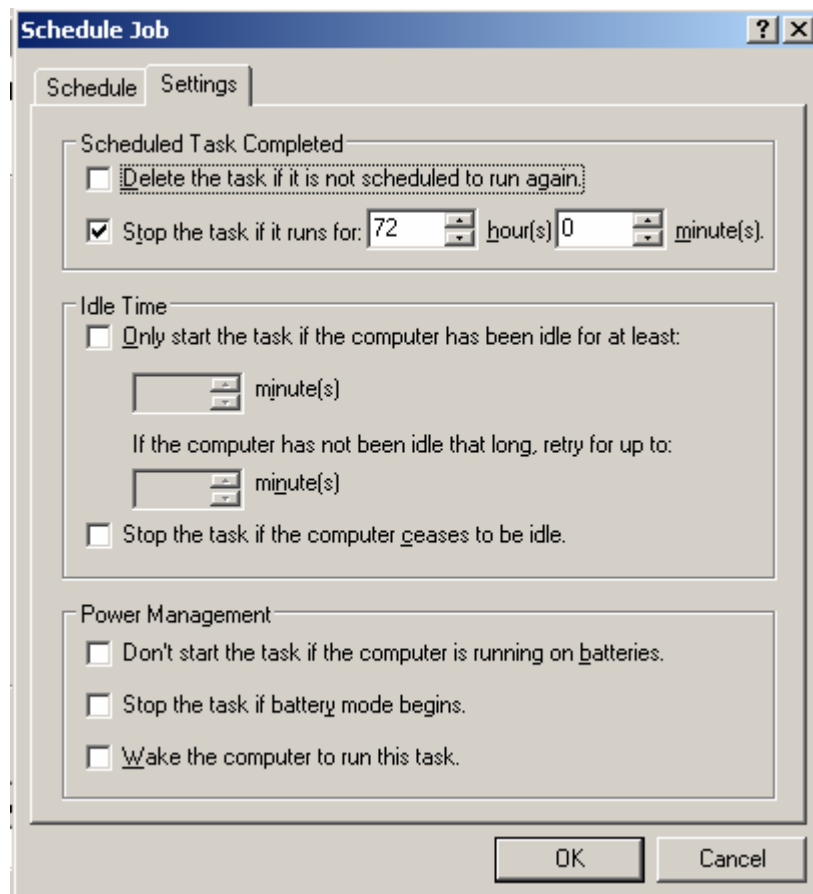
برای انتخاب زمانبندی بر روی **Set Schedule** کلیک نمایید.



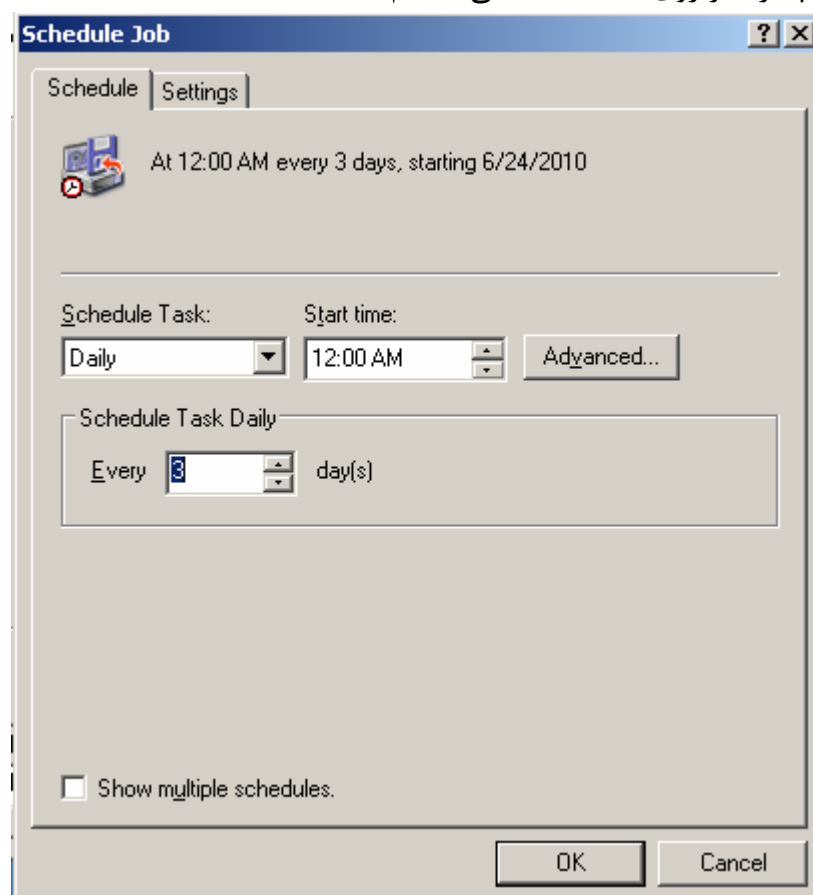
در این پنجره تنظیمات مختلفی برای اعمال زمانبندی وجود دارد. که آنها را بر حسب نیازتان باید تنظیم نمایید.



اگر بر روی زبانه Settings کلیک نمایید تنظیمات دیگری برای زمانبندی وجود دارد.



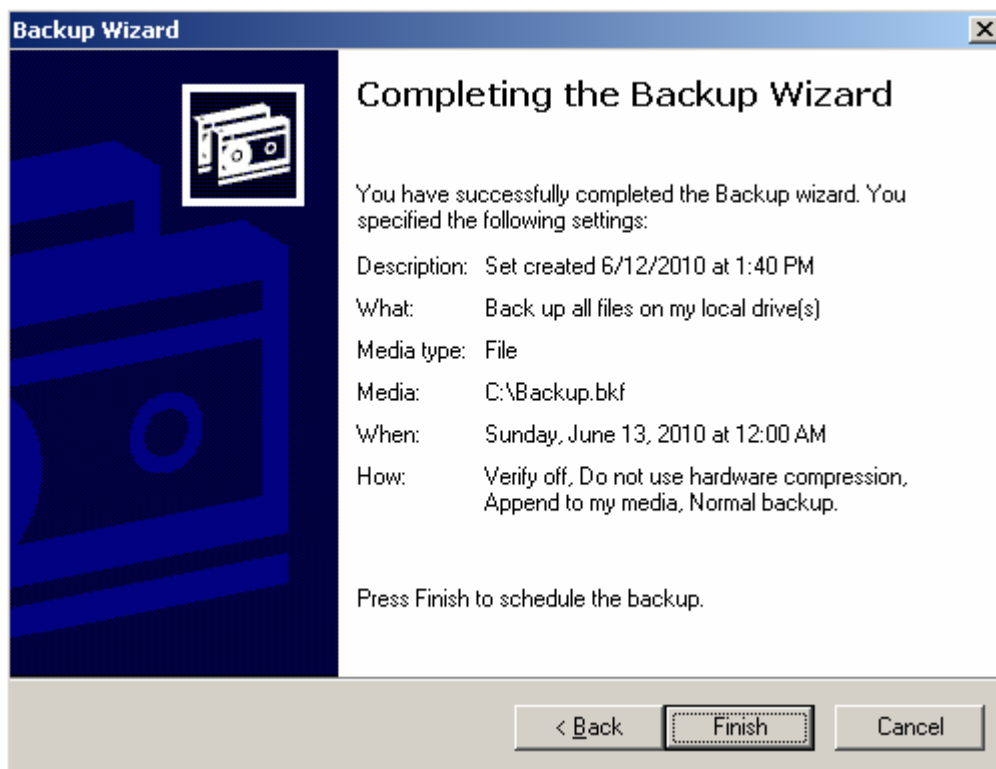
برای مثال ما زمانبندی را به صورت زیر تنظیم می نماییم که هر ۳ روز ساعت 12:00 قبل از ظهر عملیات پشتیبان گیری به صورت اتوماتیک صورت پذیرد. بر روی OK کلیک می نماییم.



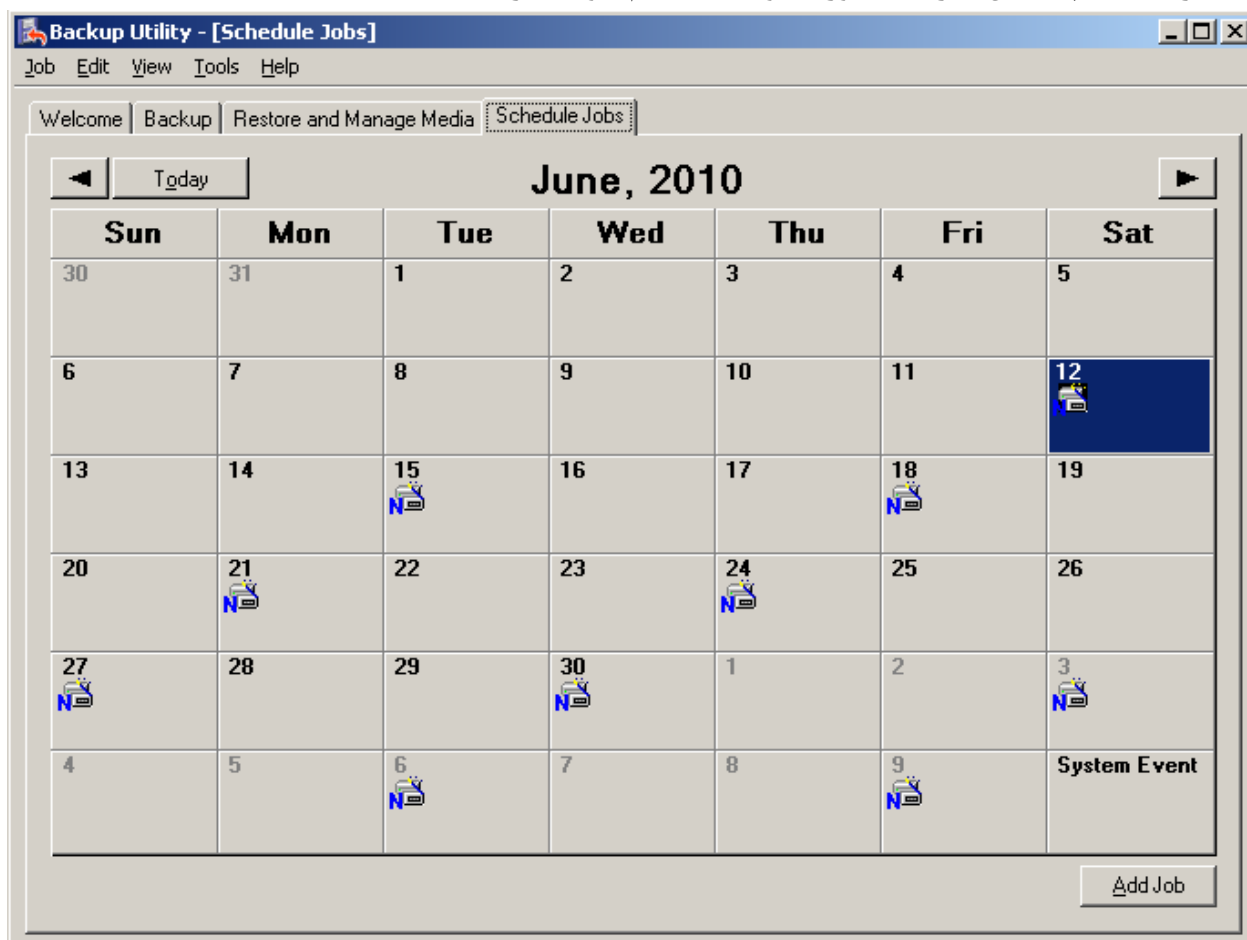
در این صفحه بر روی Next کلیک می نماییم.

پنجره زیر ظاهر می شود که برای ایجاد یک زمانبندی برای پشتیبان گیری باید password مدیر را وارد می نماییم. (اگر شما به عنوان Backup Operators می خواهید برای پشتیبان گیری عملیات زمانبندی را انجام دهید باید پسورد خود را وارد نمایید)

در این پنجره توضیحاتی در باره تنظیماتی که برای زمانبندی انجام داده ایم نمایش داده می شود. بر روی Finish کلیک می نماییم.



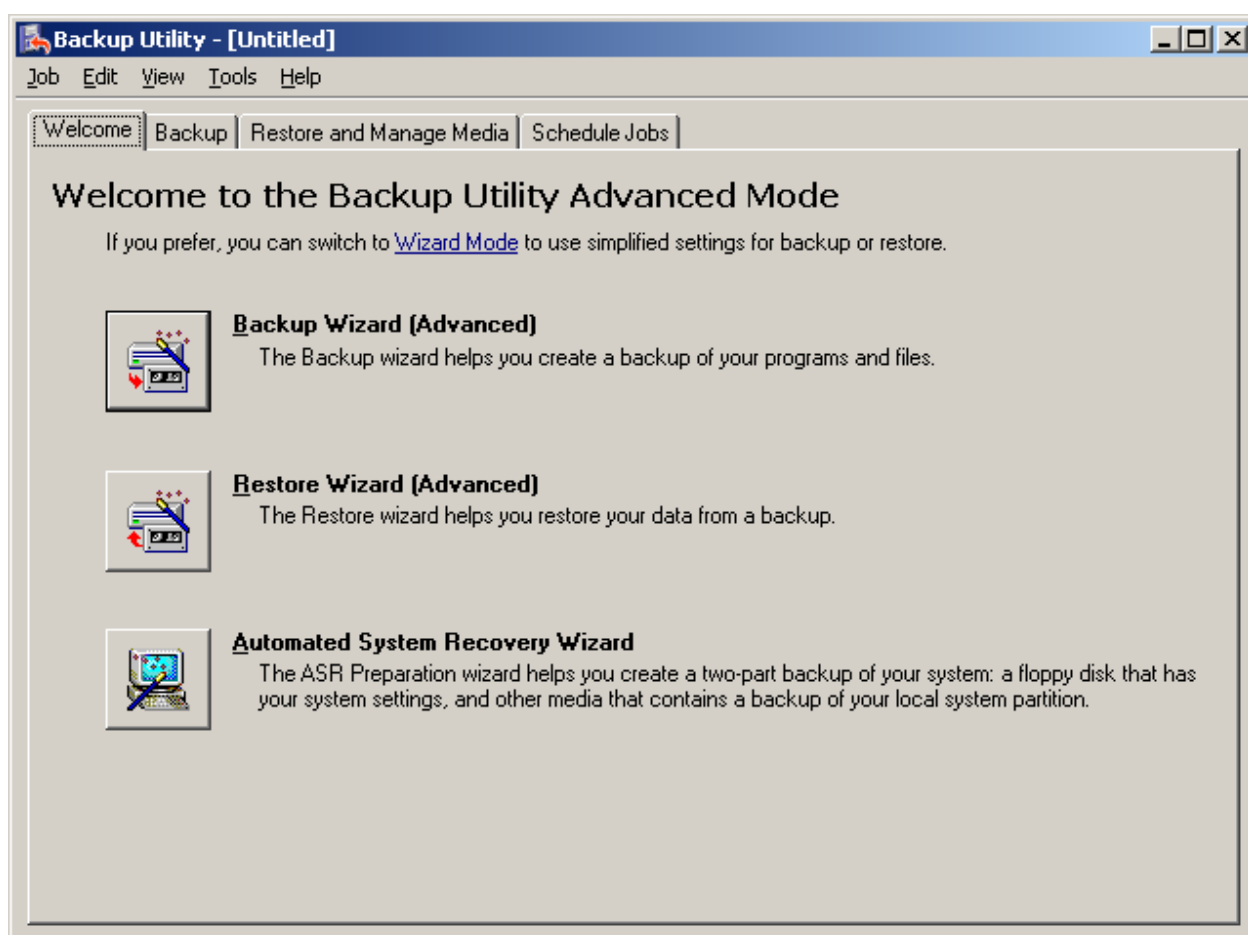
بعد از انجام این مراحل در پنجره زیر مشاهده می نمایید که تنظیمات زمانبندی انجام شده است به صورتی که هر ۳ روز یک بار عملیات پشتیبان گیری به صورت اتوماتیک انجام خواهد گرفت.



۴-۲-۱-۸: Automated System Recovery Wizard

از این گزینه برای این کار استفاده می شود که به دلایل مختلف ممکن است ویندوز ۲۰۰۳ سرور Load نشود بهتر است با استفاده از این گزینه یک دیسک Backup ایجاد نمایید و سپس اگر به هر دلایلی ویندوز ۲۰۰۳ سرور Load نشد، سی دی ویندوز را داخل CD-ROM قرار داده و شروع به نصب ویندوز نمایید در صفحه آبی رنگ Setup وقتی در قسمت پایین متن

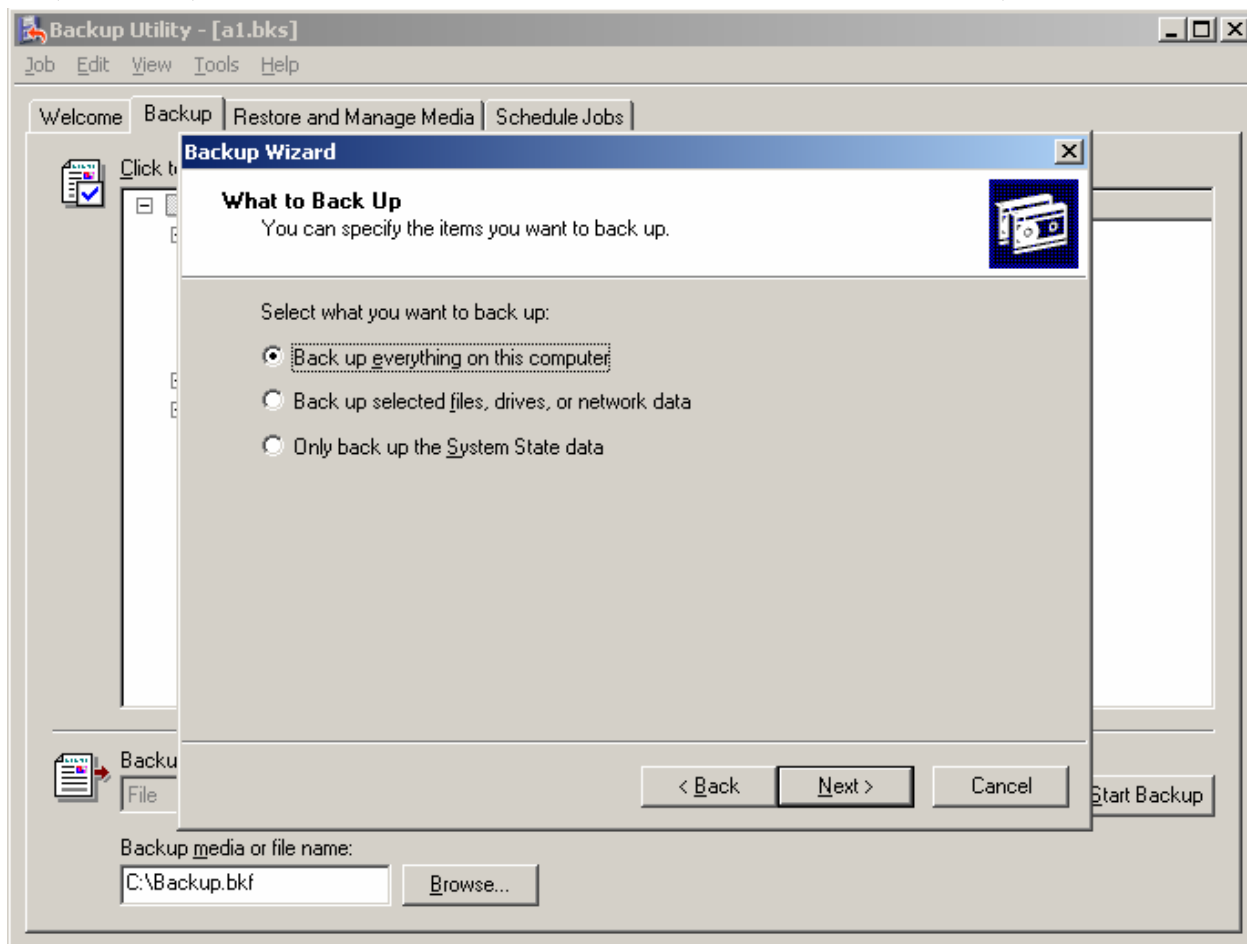
Wizard Press F2 to Automated System Recovery ظاهر شد کلید F2 را فشار داده و دیسکت Backup را داخل فلاپی درایو قرار دهید تا از طریق این فلاپی فایل های سیستمی کپی شود و ویندوز دوباره شروع به کار نماید. (این کار بعضی مواقع مفید می باشد)



۵-۲-۱-۸: پشتیبان گیری از A.D:

یک روشی که می توانید از آن برای پشتیبان گرفتن از A.D و بازیابی آن هنگام Load نشدن ویندوز استفاده کنید به صورت زیر می باشد:

برای این کار در هنگام Backup گرفتن، آن را به گزینه Backup everything on this computer تنظیم کرده و پشتیبان گیری را انجام دهید(بهتر است این کار را پس از آنکه کلیه کاربران و کامپیوترها تنظیم شدند انجام دهید).

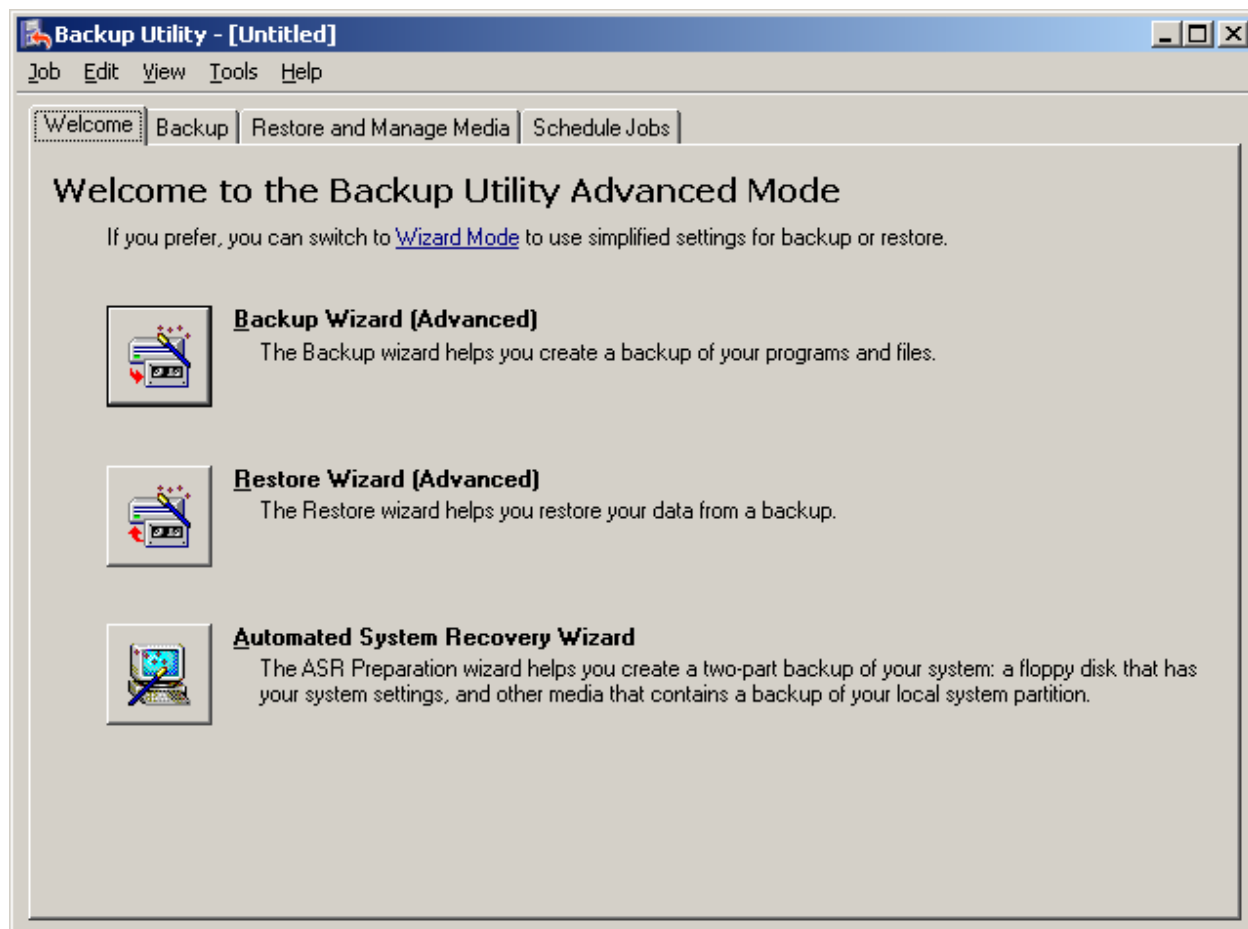


حال برای مثال زمانی فرا رسیده که ویندوز ۲۰۰۳ سرور خراب شده و Load نمی شود و توسط پشتیبان فلاپی هم Load نمی شود و شما مجبورید ویندوز را حذف و دوباره نصب نمایید. برای اینکه بتوانید بعد از نصب دوباره ویندوز ۲۰۰۳ سرور از پشتیبانی که از A.D گرفته اید بتوانید استفاده نمایید باید ویندوز ۲۰۰۳ سرور را بر روی همان پارتیشنی که قبلاً نصب کرده بودید دوباره نصب نمایید. سپس بعد از نصب ویندوز جدید باید A.D را با همان نام دامنه قبلی دوباره بر روی سرور نصب نمایید. بعد از انجام این مراحل اگر فایل پشتیبان را بازیابی و کامپیوتر را رستارت نمایید مشاهده خواهید کرد که تنظیمات A.D به حالت قبل برگشته است.

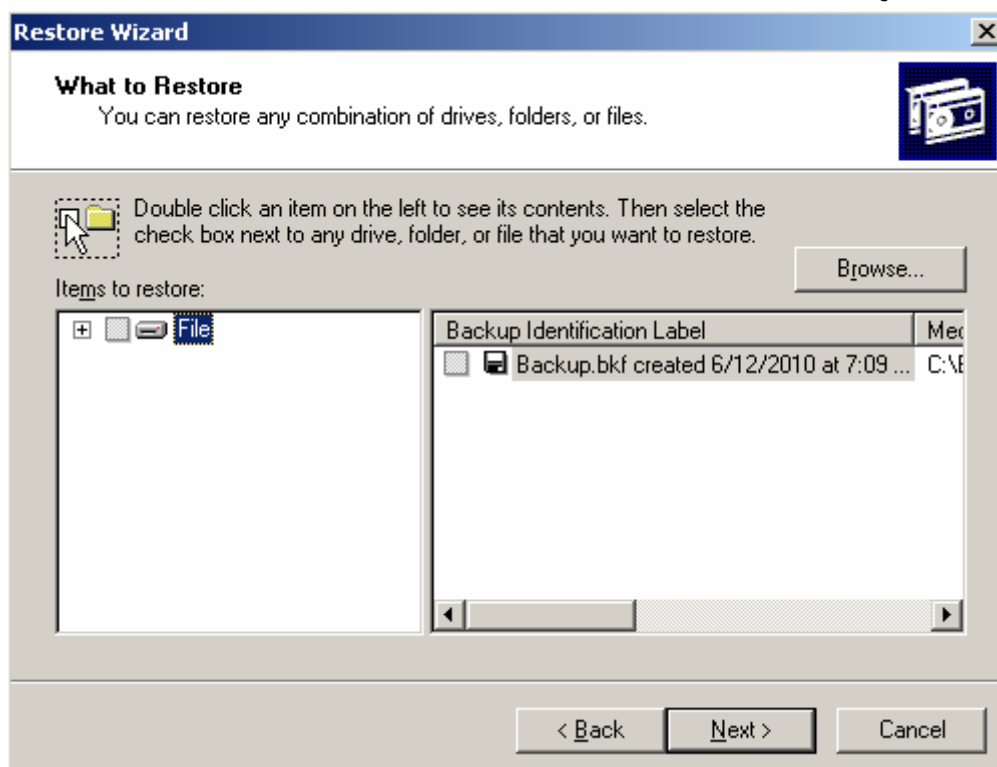
۳-۱-۸- بازیابی Backup:

در این قسمت برای بازیابی کردن فایل، ما همان پوشه ای را که در قسمت قبل از آن پشتیبان گرفتیم را در مسیر دیگر بازیابی می کنیم.

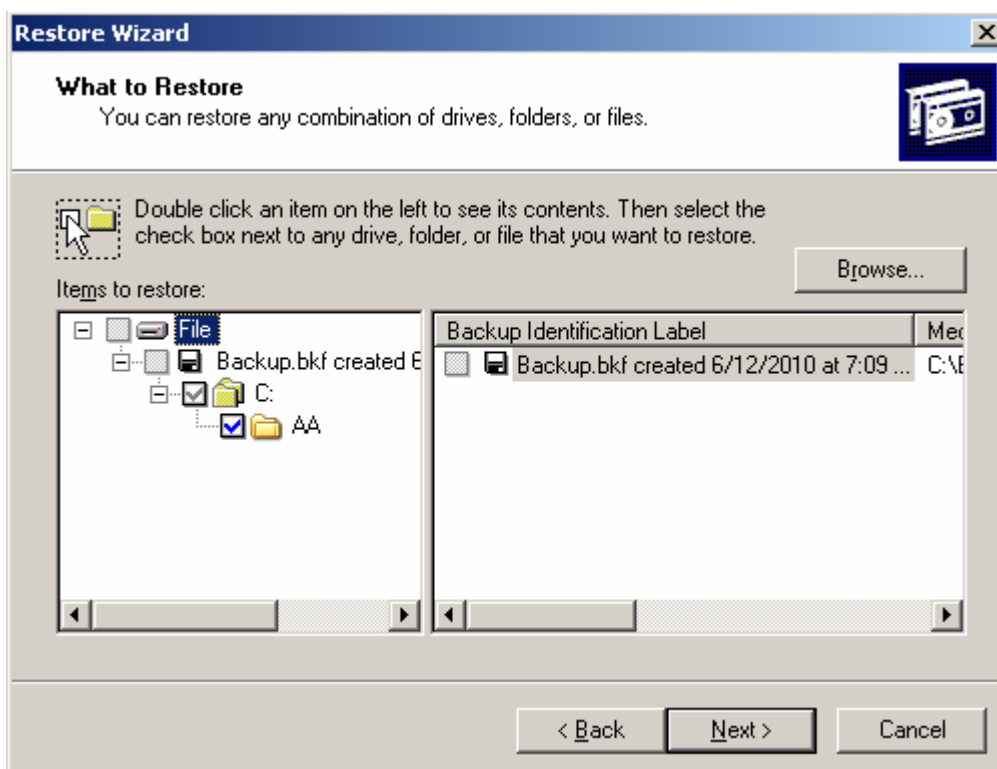
برای بازیابی کردن فایل های پشتیبان در پنجره Backup بر روی زبانه Restore and Manage Media کلیک می نمایم.



این پنجره نمایش داده میشود.



فایل پشتیبان را انتخاب و بر روی Next کلیک می نمایم.



پنجره Wizard بازیابی نمایش داده می شود. اگر بر روی Finish کلیک نمایم فایل پشتیبان روی همان پوشه اصلی بازیابی می شود. چون ما می خواهیم فایل در مسیر دیگر بازیابی شود بر روی Advanced کلیک می نمایم.

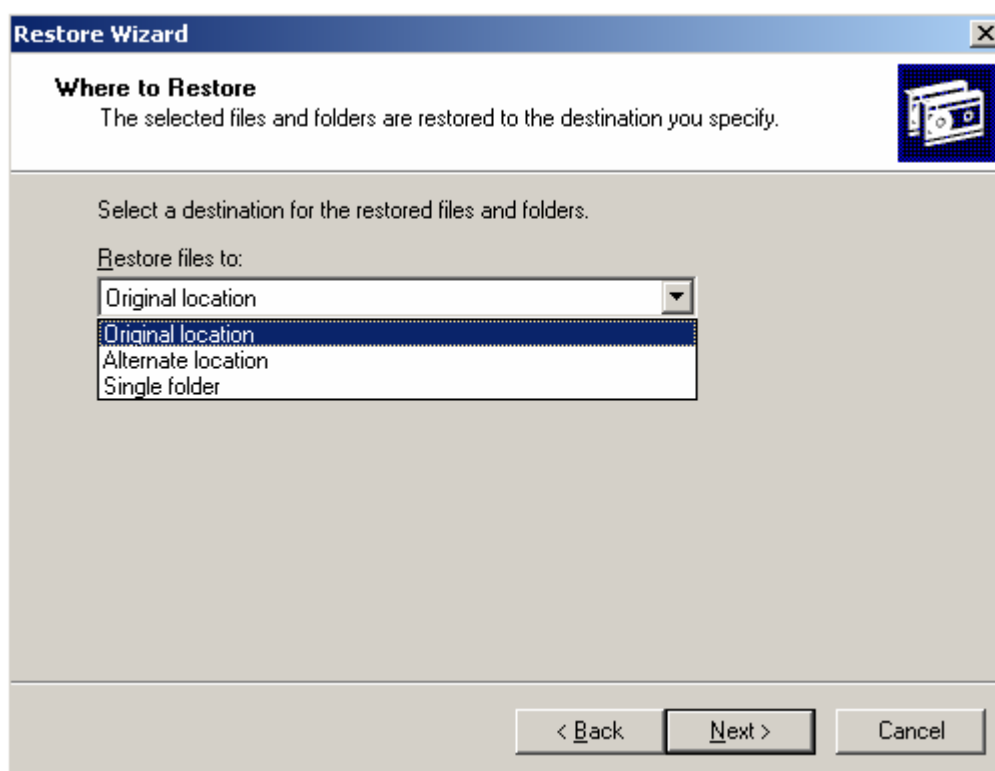


در این پنجره در فهرست کشویی ۳ انتخاب وجود دارد:

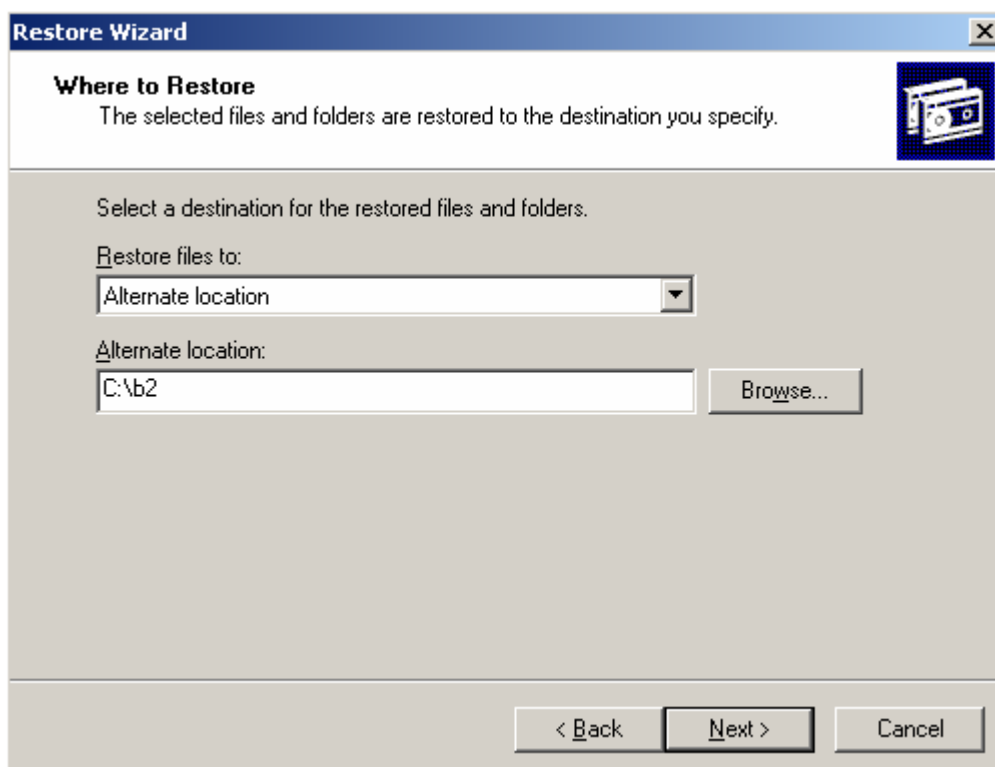
Original location: اگر این گزینه را انتخاب کنیم بازیابی در همان پوشه اصلی انجام می شود.

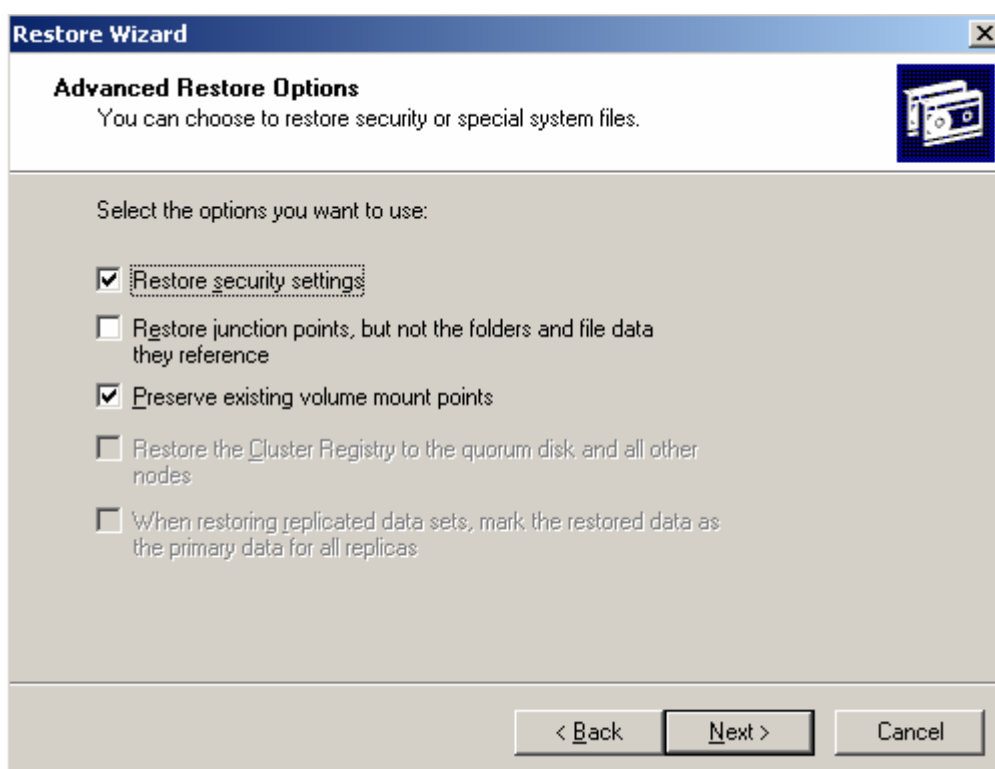
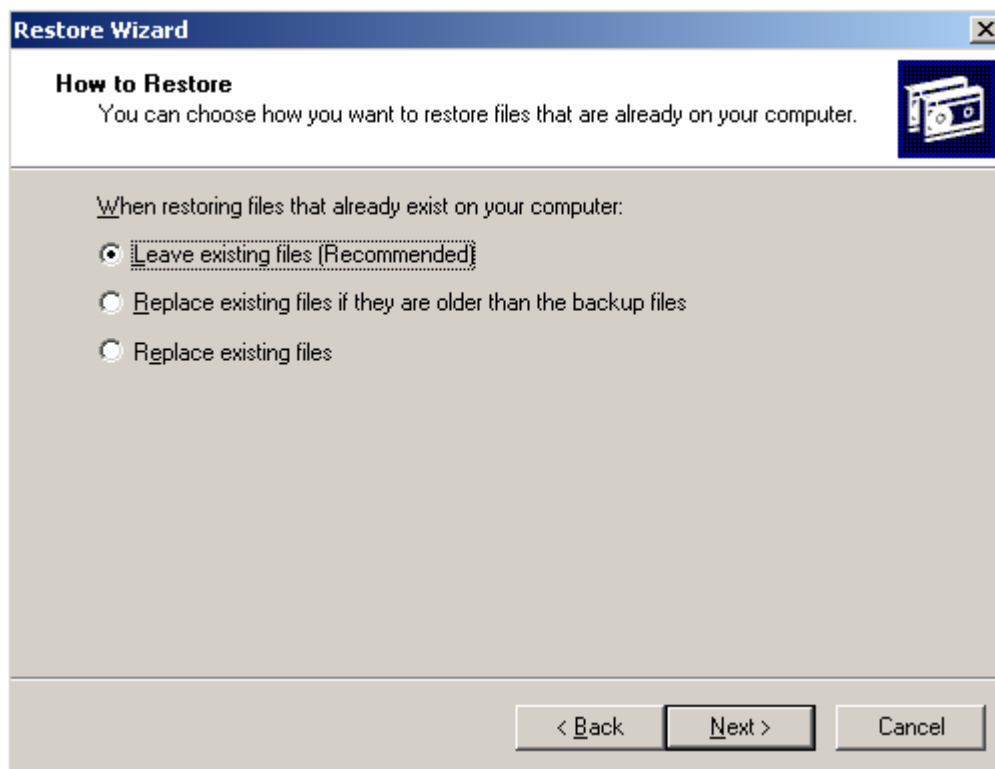
Alternate location: با انتخاب این گزینه کادر در پایین صفحه ظاهر می شود که در آن کادر با مشخص کردن یک پوشه، فایل در همان پوشه ای که مشخص می کنیم بازیابی می شود.

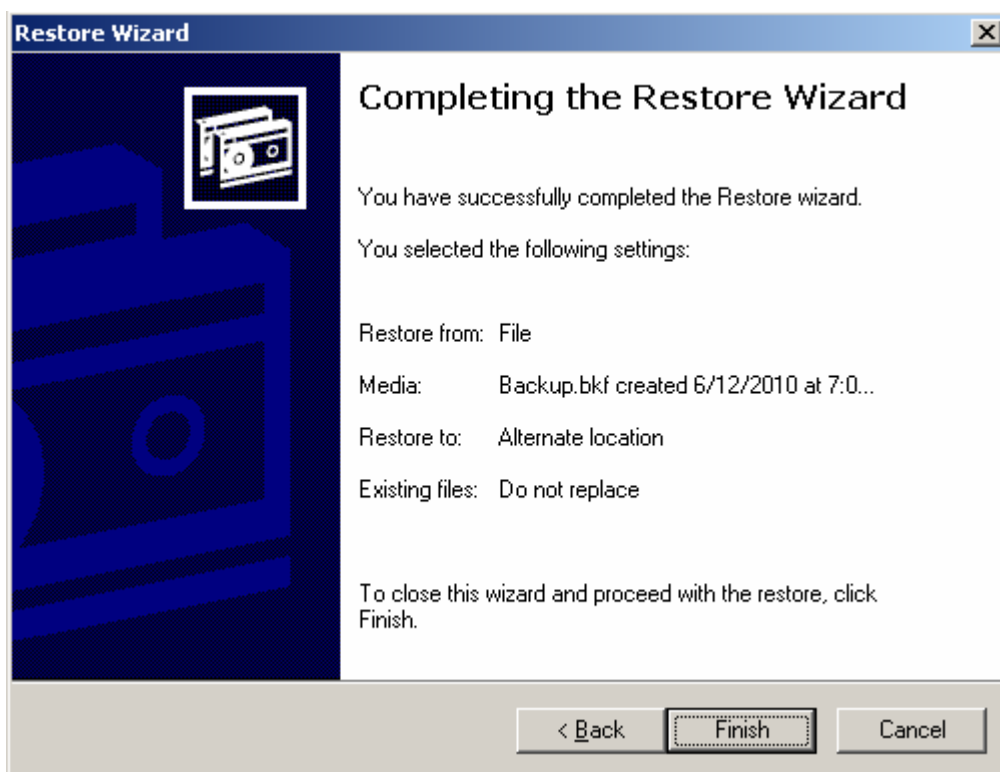
Single folder: اگر این گزینه را انتخاب نماییم فقط یک پوشه ایجاد شده و همهٔ فایل‌ها داخل آن پوشه بازیابی خواهند شد. (این انتخاب فقط فایل‌ها را بازیابی می‌کند)



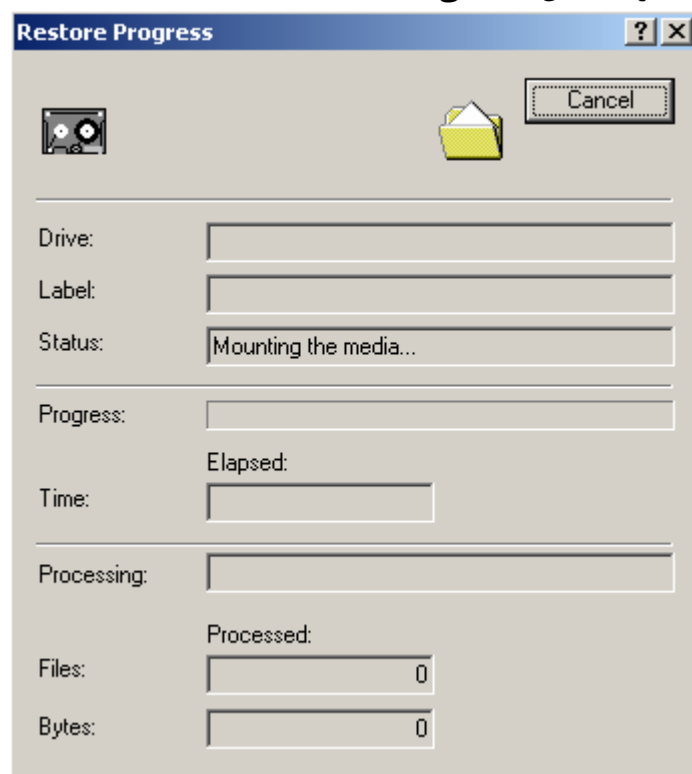
گزینه دوم را انتخاب و مسیر پوشه‌ای را که می‌خواهیم فایل‌ها در آنجا بازیابی شوند را مشخص می‌کنیم. و بر روی Next کلیک می‌نماییم.



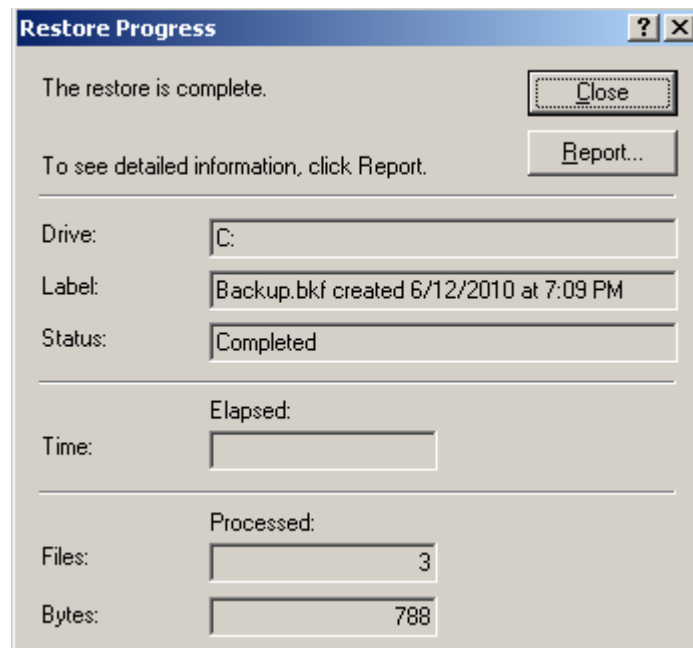




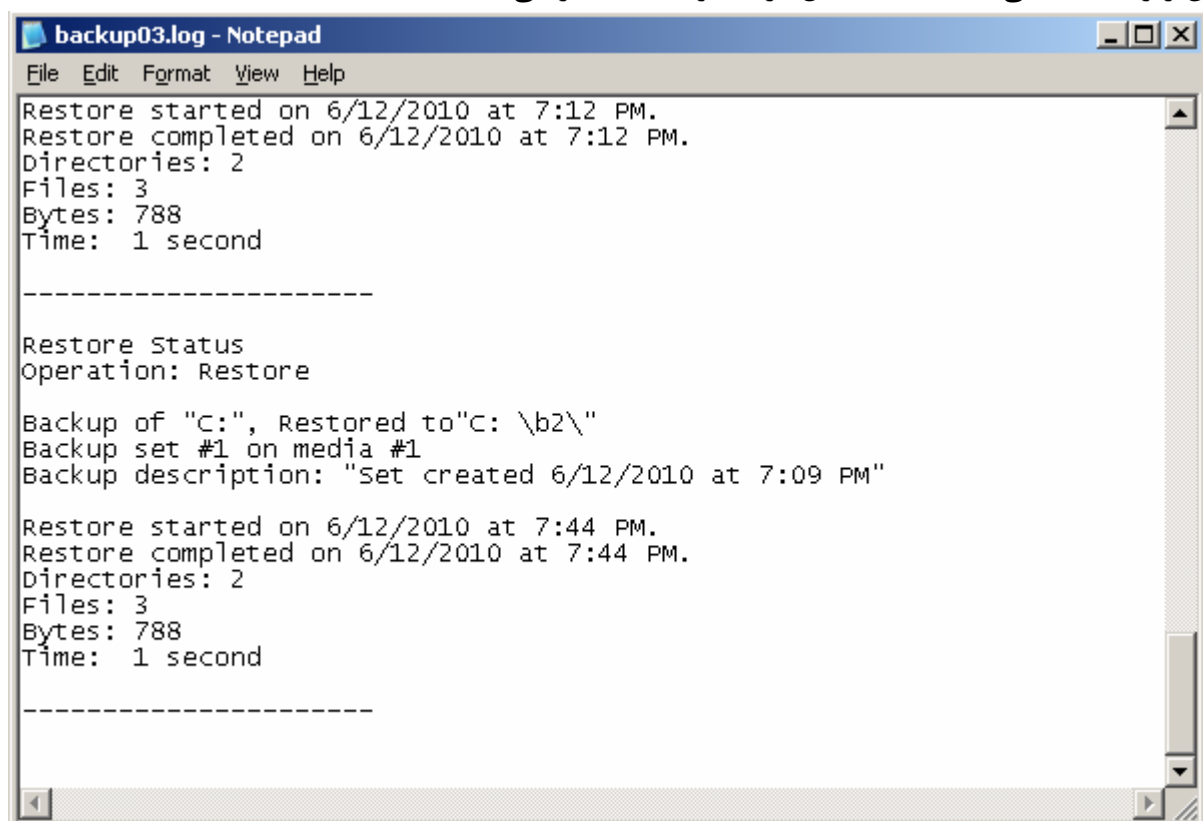
برنامه شروع به بازیابی فایل در مسیر مشخص شده می نماید.



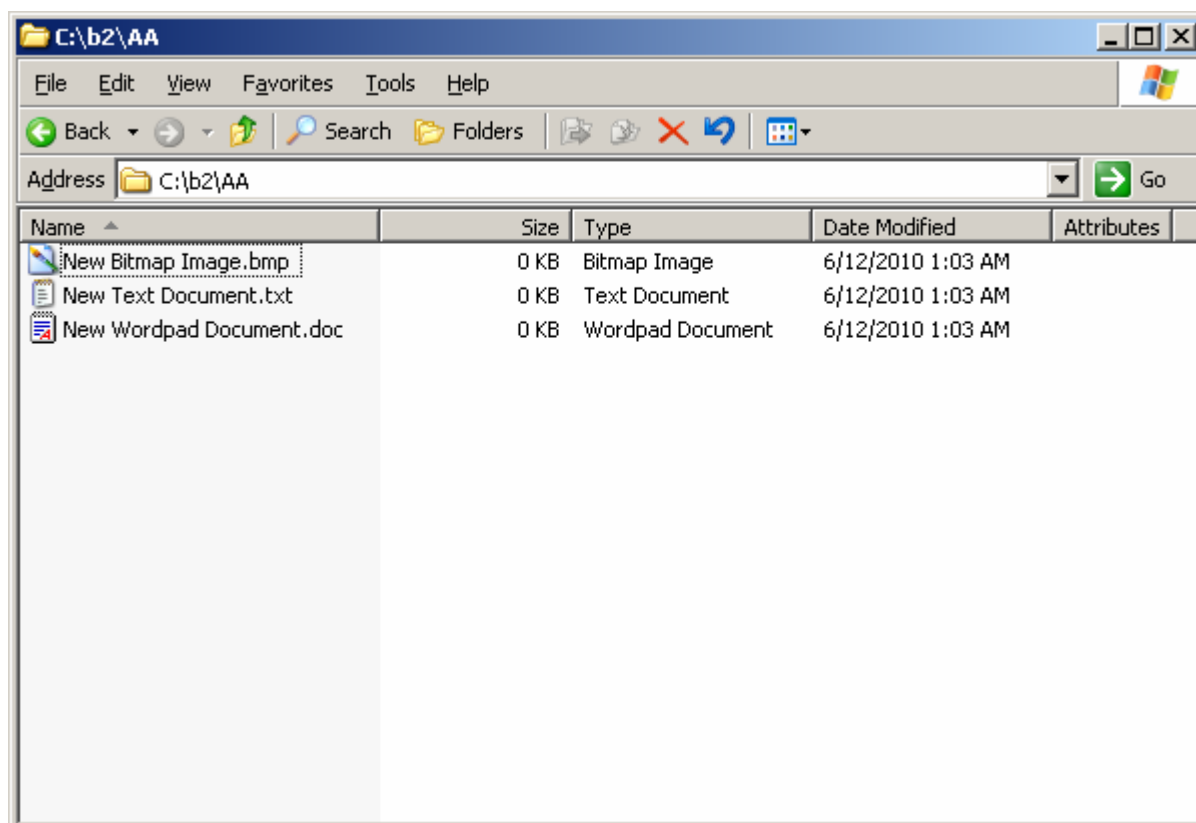
بعد از پایان بازیابی برای دیدن گزارش بازیابی بر روی Report کلیک می نمایم.



در گزارش زیر مشاهده می نمایید که ۳ فایل در مسیر C:\b2\ بازیابی شده است.



اگر در My Computer به همان مسیر برویم فایل های بازیابی شده را مشاهده خواهیم کرد.



۹. جزئیات بخش نهم:

۹-۱- دستیابی به سرور از راه دور:

در این بخش قصد داریم مراحل را که برای برقراری ارتباط از راه دور از طریق خط تلفن لازم است تنظیم شود را انجام دهیم. این مراحل عبارتند از:

- بررسی تنظیمات سرور برای دستیابی از راه دور
 - دادن نقش Remote Access Server
 - بررسی ایجاد Connection برای دستیابی از راه دور در سرور
 - بررسی تعیین اجازه برای دستیابی از راه دور
- بررسی تنظیمات کلاینت برای دستیابی از راه دور
 - بررسی ایجاد Connection برای دستیابی از راه دور در کلاینت
 - وصل شدن به سرور از راه دور

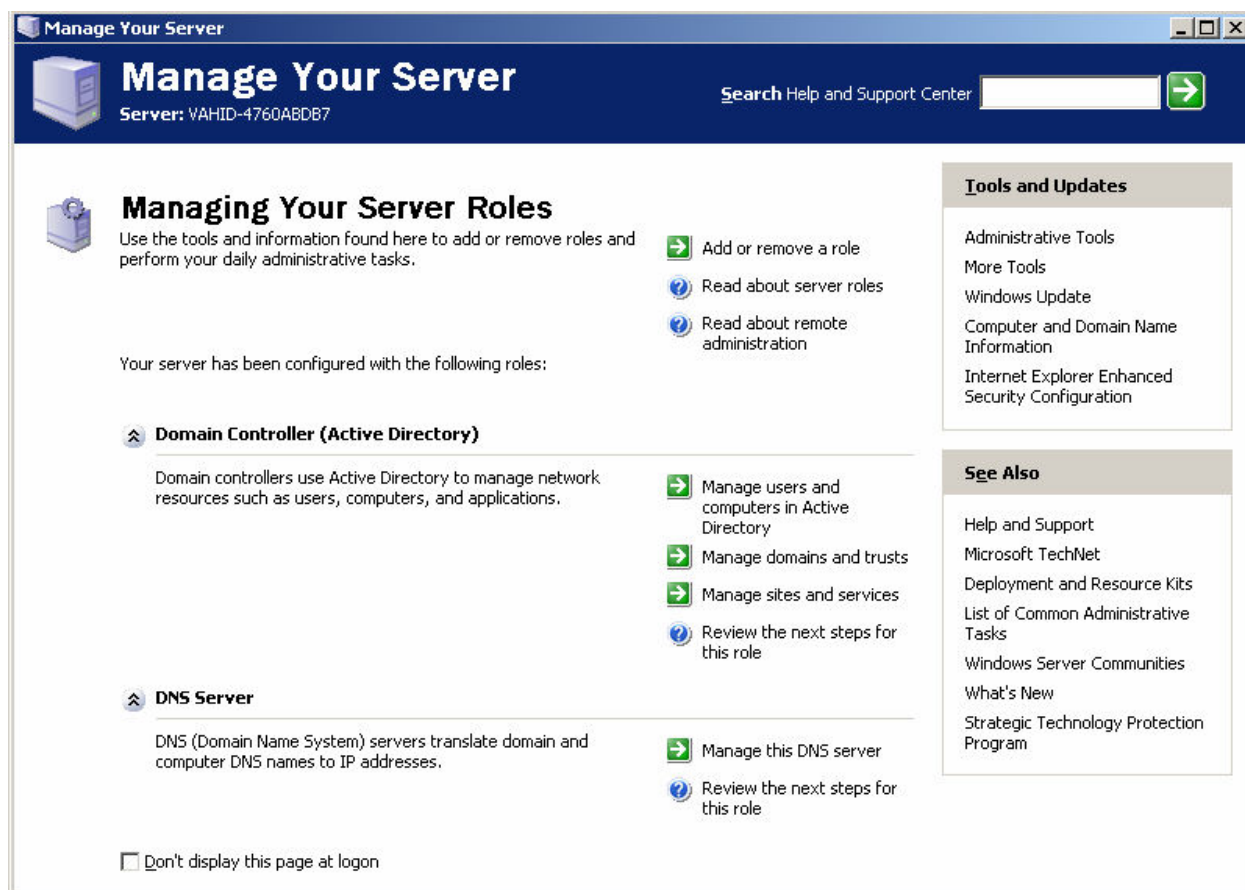
۹-۱-۱- بررسی تنظیمات سرور برای دستیابی از راه دور:

در مراحل زیر ما سرور را برای دستیابی از راه دور تنظیم می کنیم. برای این کار باید مراحل زیر را طی نماییم:

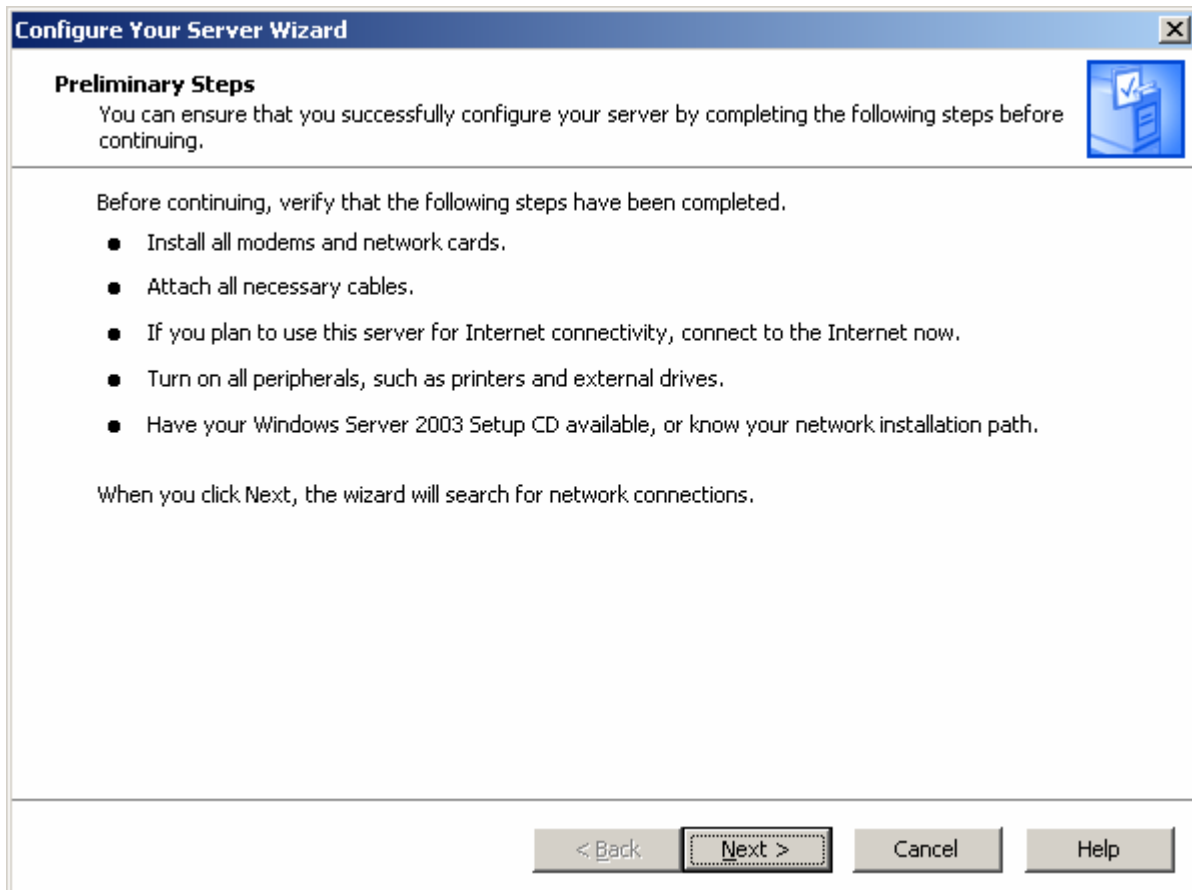
۱-۱-۹- دادن نقش Remote Access Server:

برای استفاده از سرویس راه دور باید اول نقش Remote Access /VPN Server به ویندوز سرور داده شود. برای دادن این نقش این مراحل را انجام دهید:

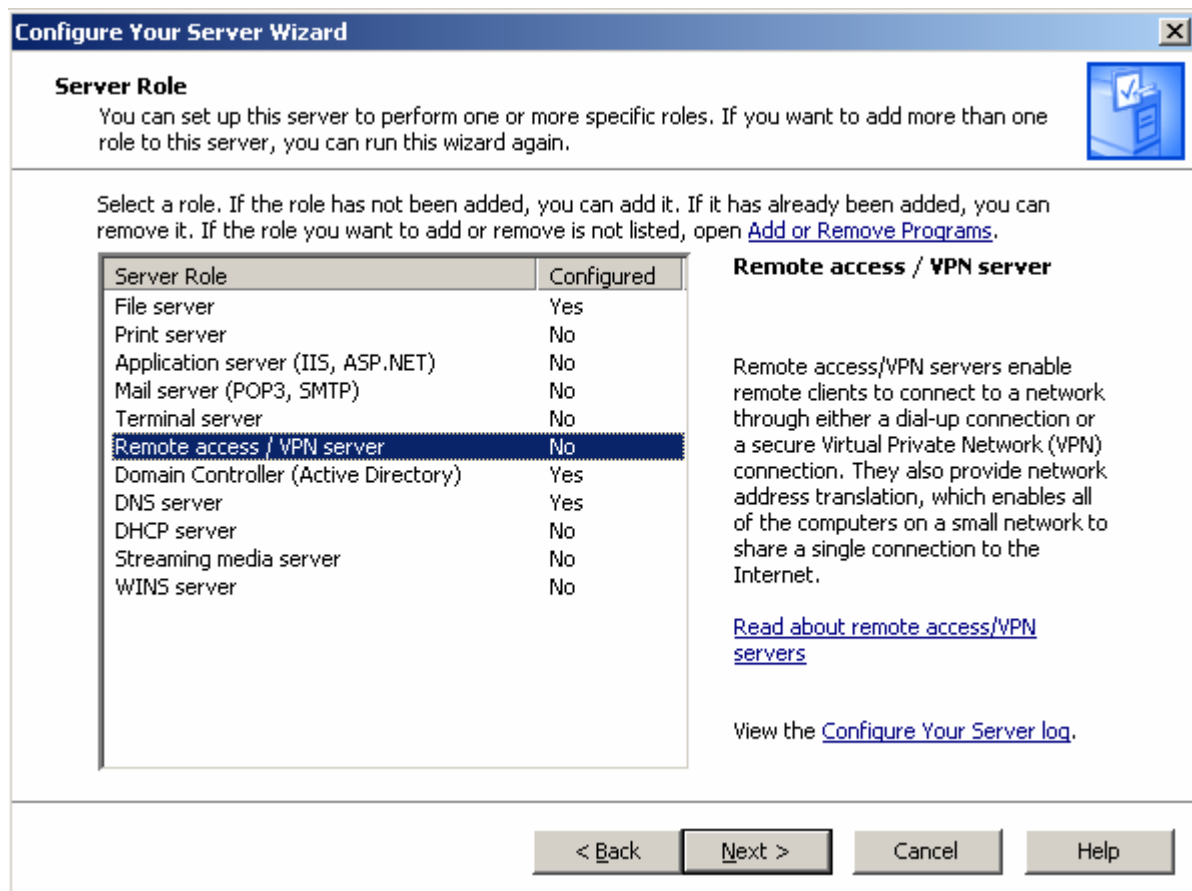
در پنجره Manage Your Server بر روی Add or remove a role کلیک کنید.



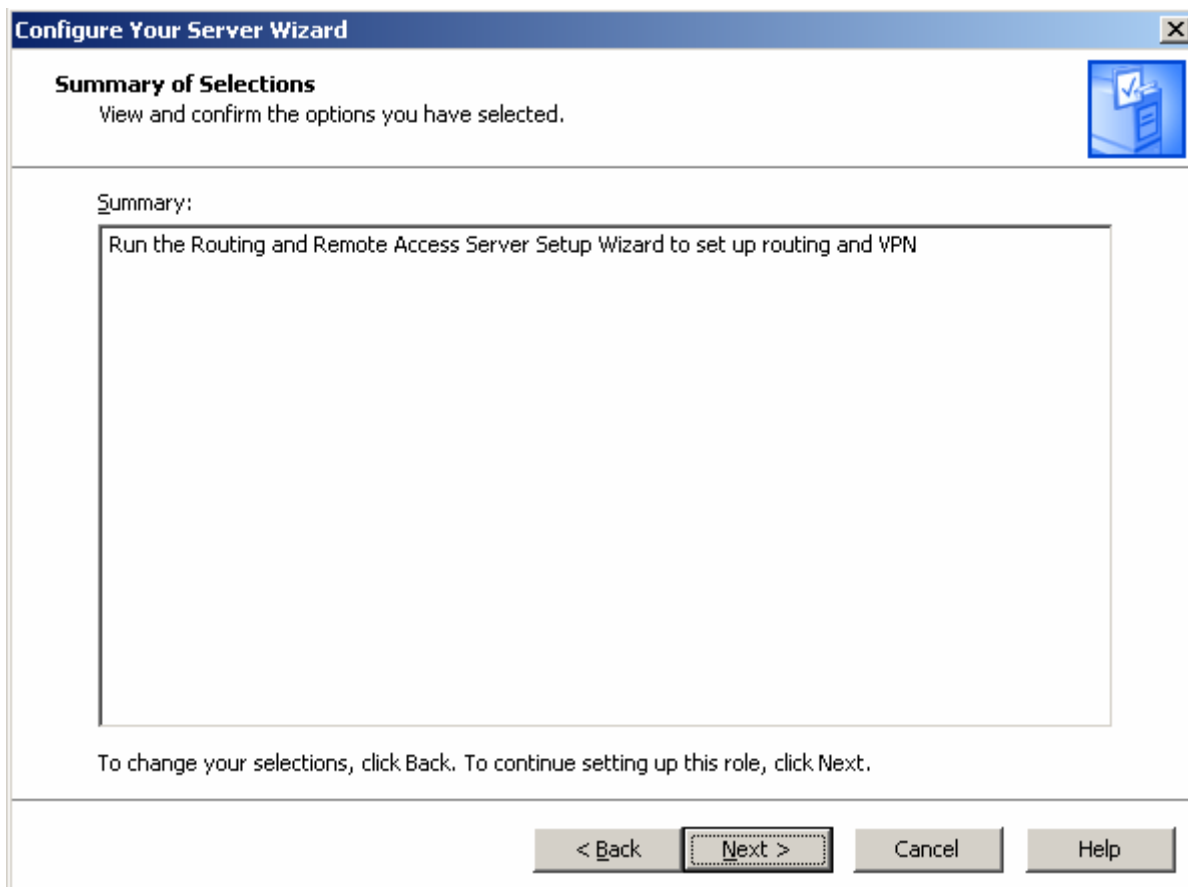
روی دکمه Next کلیک کنید.



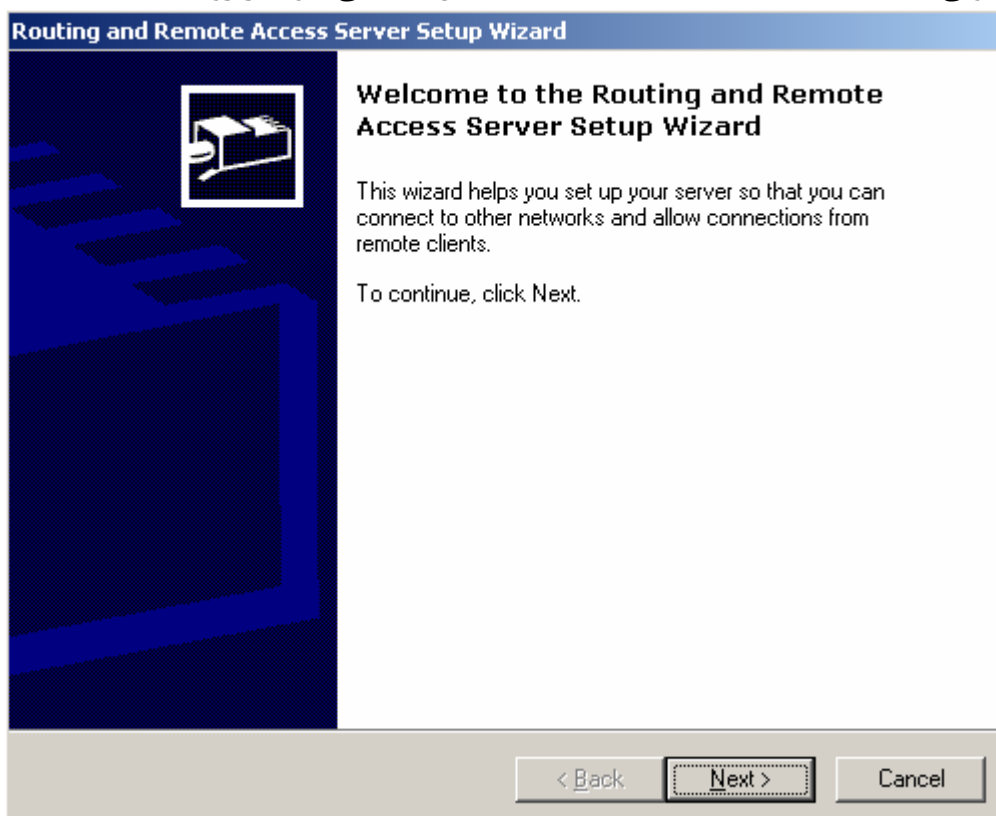
در این پنجره بر روی Remote access/ VPN server کلیک کرده سپس بر روی Next کلیک کنید.



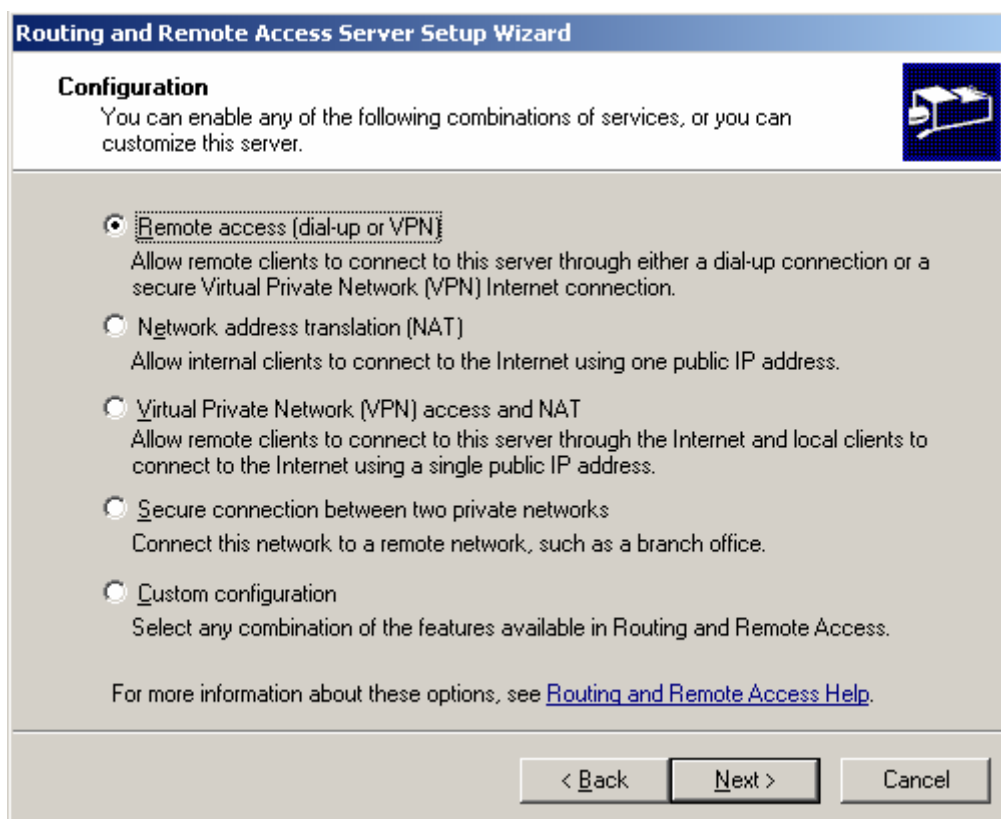
در این پنجره توضیح داده می شود که شما در حال نصب Remote access/ VPN server برای سرور می باشید. بر روی Next کلیک نمایید.



پنجره خوش آمد گویی نصب Remote Access Server نمایش داده می شود. بر روی Next کلیک نمایید.



در این پنجره انتخابهای مختلفی وجود دارد که برای دستیابی از راه دور استفاده می شود. در این پنجره چون ما می خواهیم دستیابی از راه دور را با استفاده از dial-up توضیح دهیم، گزینه اول را انتخاب و Next می کنیم.

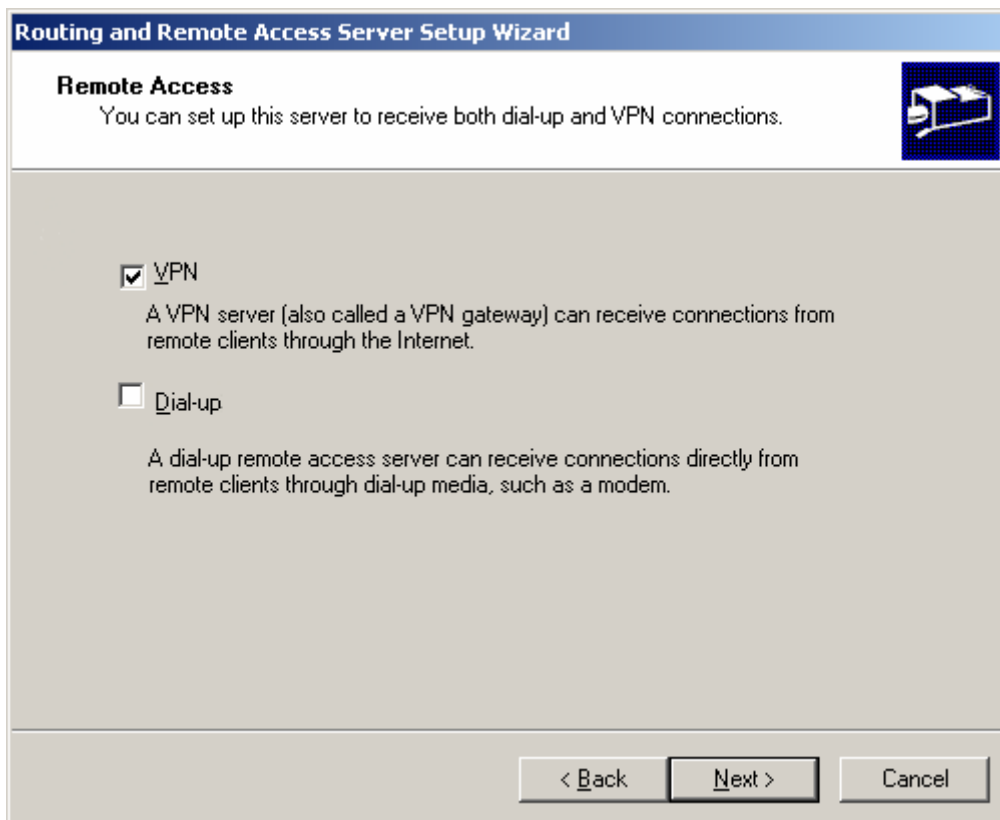


در این پنجره دو انتخاب وجود دارد:

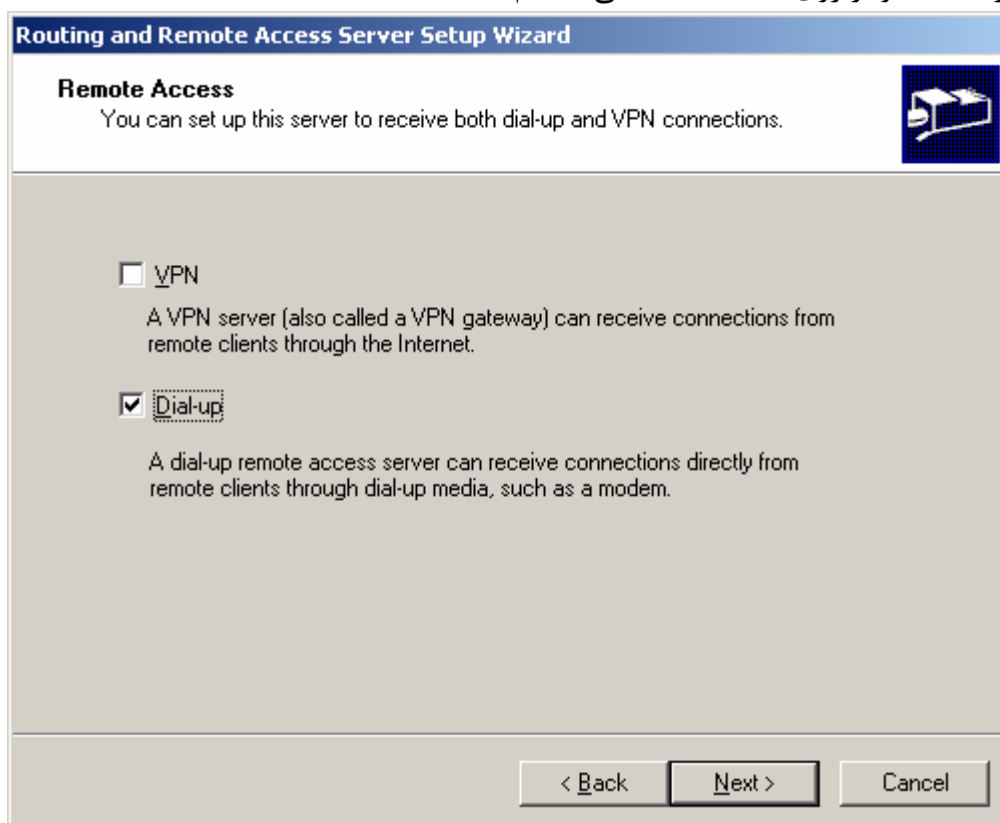
VPN: اگر بخواهیم از داخل شبکه دستیابی داشته باشیم از این گزینه استفاده می کنیم.

Dial-up: اگر بخواهیم خارج از شبکه از راه دور با خط تلفن به سرور دستیابی داشته باشیم از این گزینه استفاده می کنیم.

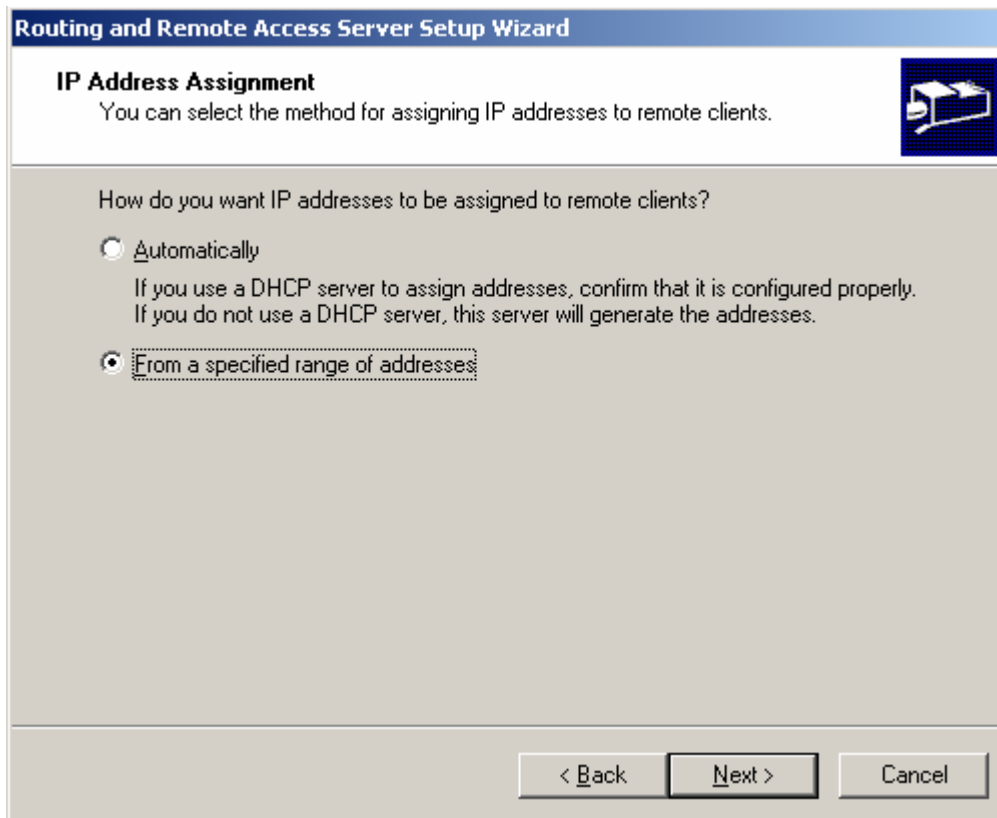
نکته: اگر بخواهید از VPN استفاده کنید باید سرور شما دارای دو کارت شبکه باشد در غیر اینصورت نمی توانید مراحل نصب را ادامه دهید. ما اول تیک گزینه VPN را قرار می دهیم تا پیغام خطایی را که برای کارت شبکه نمایش داده می شود را مشاهده نماییم.



گزینه Dial-up را انتخاب و بر روی Next کلیک می نمایم.



در این پنجره باید انتخاب کنیم که آدرس آپی که کلاینت بتواند با استفاده از آن وارد سرور شود به صورت اتوماتیک باشد. یا با استفاده از آدرس هایی که خودمان تعریف می کنیم، کلاینت فقط بتواند با استفاده از آن آدرس IP ها وارد سرور شود. گزینه دوم را انتخاب و بر روی Next کلیک می نماییم.



Routing and Remote Access Server Setup Wizard

IP Address Assignment
You can select the method for assigning IP addresses to remote clients.

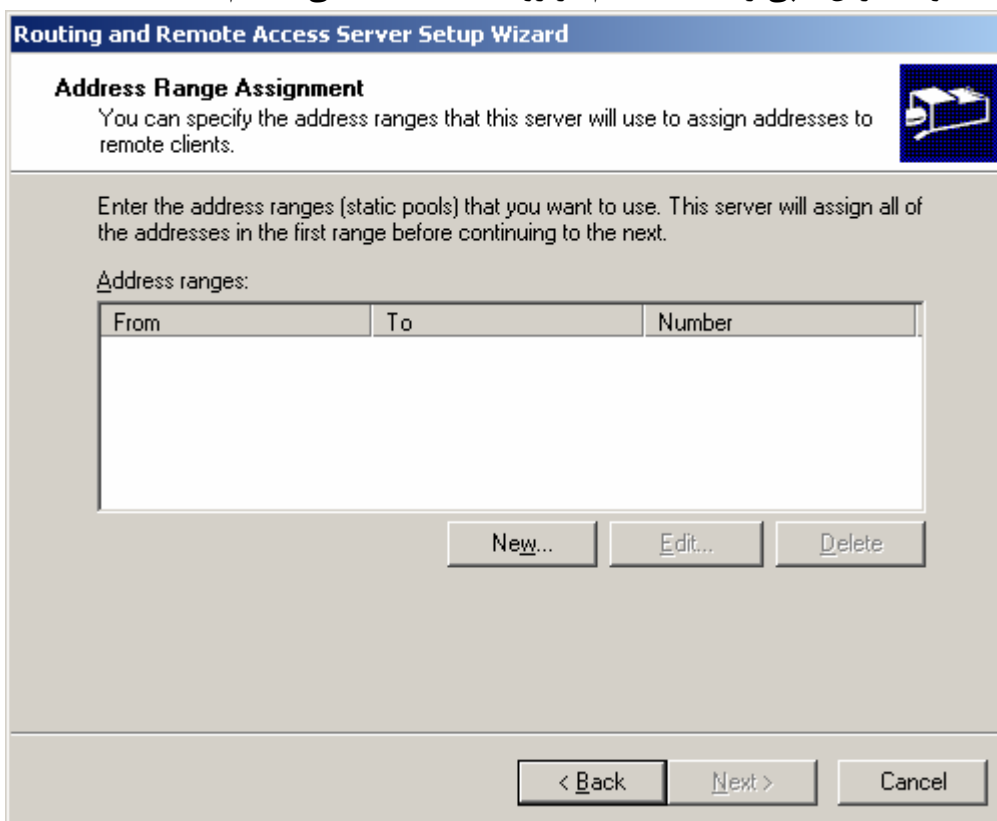
How do you want IP addresses to be assigned to remote clients?

☐ Automatically
If you use a DHCP server to assign addresses, confirm that it is configured properly.
If you do not use a DHCP server, this server will generate the addresses.

☒ From a specified range of addresses

< Back Next > Cancel

در این پنجره باید محدوده آدرس آپی را اضافه نماییم. بر روی Add کلیک می نماییم.



Routing and Remote Access Server Setup Wizard

Address Range Assignment
You can specify the address ranges that this server will use to assign addresses to remote clients.

Enter the address ranges (static pools) that you want to use. This server will assign all of the addresses in the first range before continuing to the next.

Address ranges:

From	To	Number

New... Edit... Delete

< Back Next > Cancel

در این پنجره باید محدوده آدرس IP را وارد کنیم.

New Address Range ? X

Type a starting IP address and either an ending IP address or the number of addresses in the range.

Start IP address: 0 . 0 . 0 . 0

End IP address: 0 . 0 . 0 . 0

Number of addresses: 0

OK Cancel

بعد از اینکه محدوده آدرس IP را وارد کردیم در قسمت Number تعداد آدرس IP که در آن محدوده می توان به سرور وصل شد، نمایش داده می شود.

New Address Range ? X

Type a starting IP address and either an ending IP address or the number of addresses in the range.

Start IP address: 192 . 168 . 0 . 2

End IP address: 192 . 168 . 0 . 6

Number of addresses: 5

OK Cancel

بر روی Next کلیک می نمایم.

Routing and Remote Access Server Setup Wizard

Address Range Assignment

You can specify the address ranges that this server will use to assign addresses to remote clients.

Enter the address ranges (static pools) that you want to use. This server will assign all of the addresses in the first range before continuing to the next.

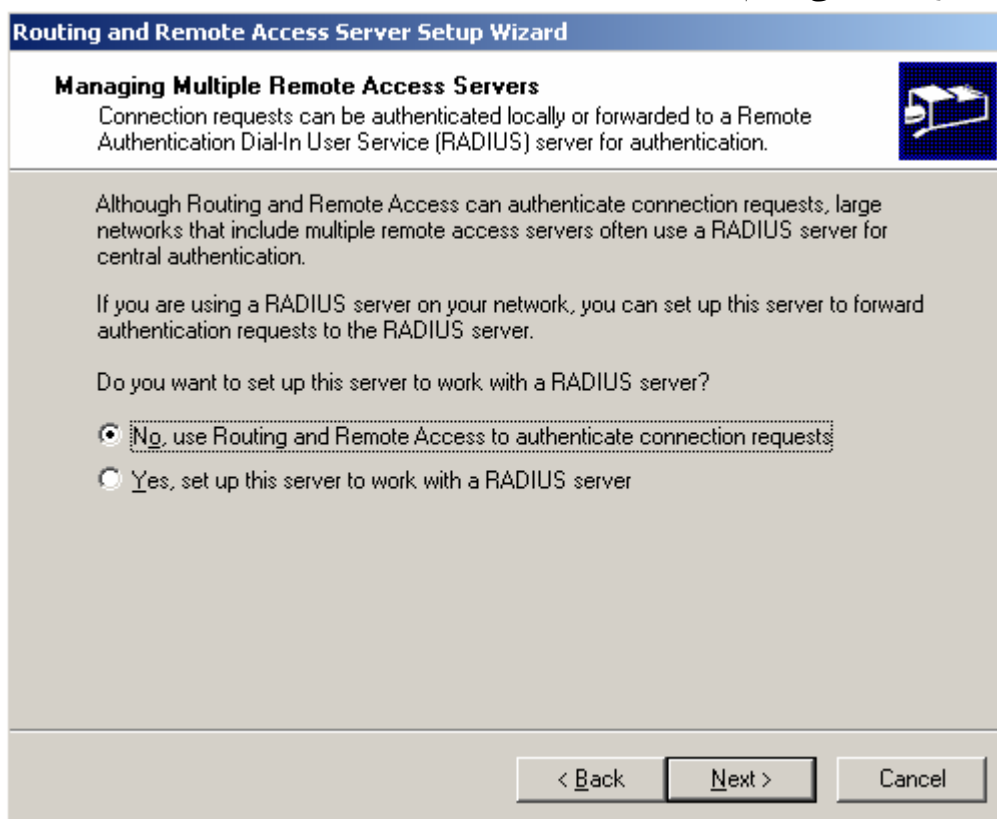
Address ranges:

From	To	Number
192.168.0.2	192.168.0.6	5

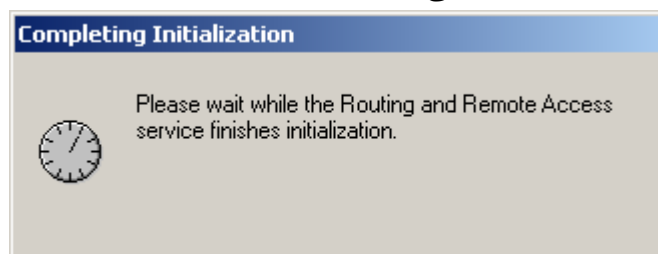
New... Edit... Delete

< Back Next > Cancel

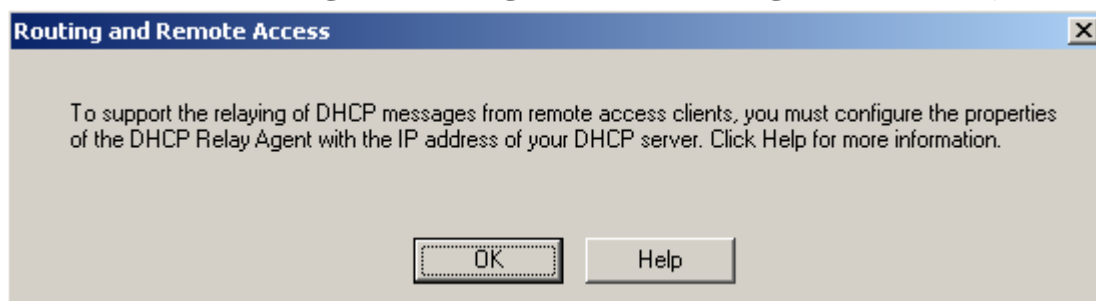
این پنجره مربوط به تنظیم RADIUS می باشد. RADIUS مربوط به اهراز هویت برای ورود به سرور می باشد که اگر گزینه Yes, set up this server to work with a RADIUS server را انتخاب کنیم در هر بار ورود به سرور از راه دور اهراز هیت صورت می گیرد ولی اگر بر روی No,... کلیک کنیم فقط یک بار اهراز هویت صورت خواهد گرفت. بر روی No,... کلیک و Next می کنیم.



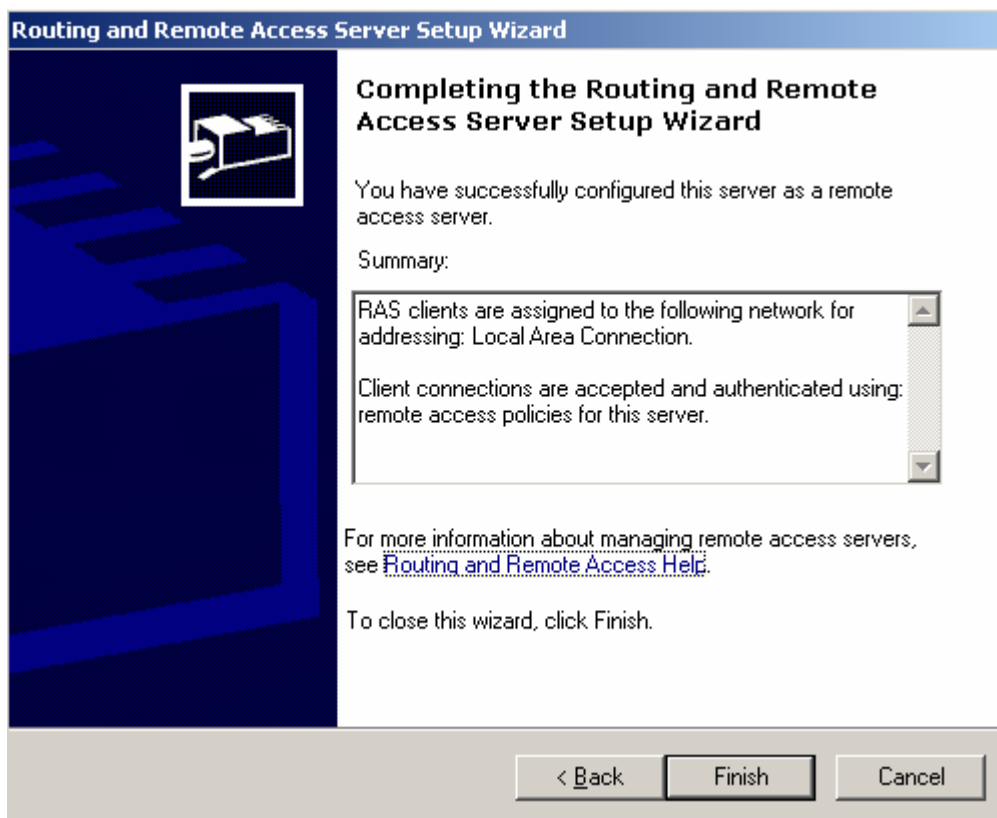
برنامه شروع به نصب Remot Access Server می کند.



بعد از اتمام نصب پیغام زیر نمایش داده می شود که برای پشتیبانی از DHCP می باشد که بر روی OK کلیک می کنیم.



در این پنجره چکیده مراحل که انجام دادیم نمایش داده شده است. بر روی Finish کلیک می کنیم.



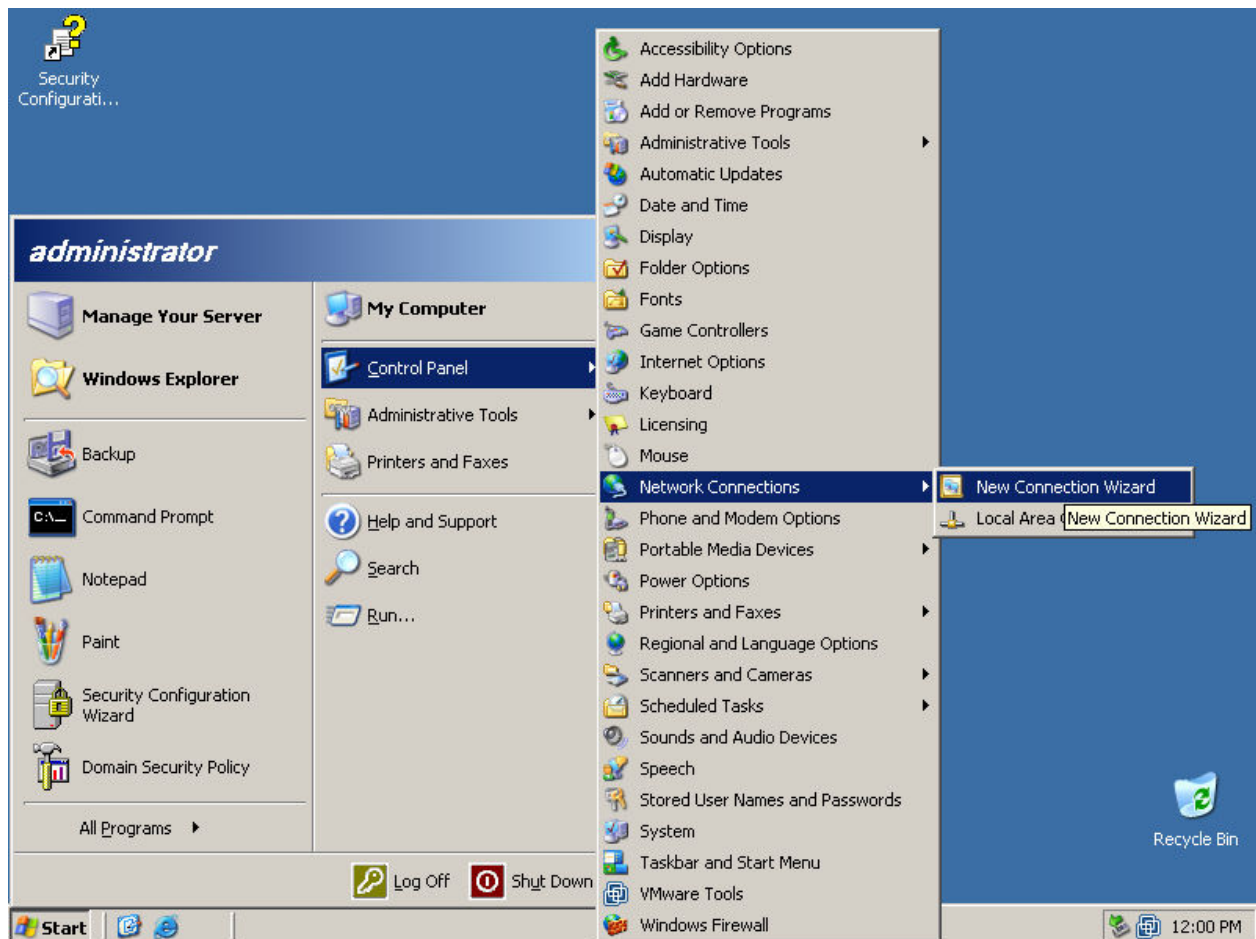
بعد از انجام این کار نقش Remote Access Server به سرور داده می شود.

۹-۱-۱-۲- بررسی ایجاد Connection برای دستیابی از راه دور در سرور :

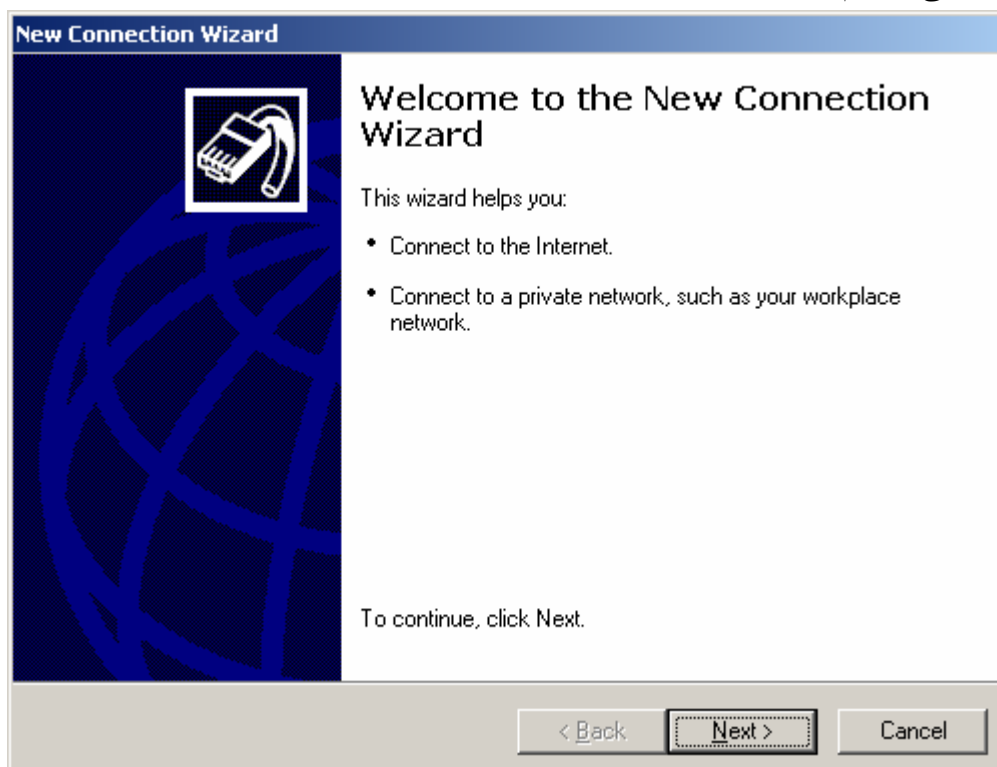
برای ایجاد Connection در سرور این مراحل را انجام می دهیم:

به مسیر زیر می رویم:

Start > Control Panel > Network Connections > New Connection Wizard



بر روی Next کلیک می نمایم.



گزینه دوم را برای استفاده از Dial-up انتخاب می کنیم.

New Connection Wizard

Network Connection Type
What do you want to do?

☐ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

☒ **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

☐ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

< Back Next > Cancel

در این پنجره نامی را برای Connection وارد کرده بر روی Next کلیک می کنیم.

New Connection Wizard

Connection Name
Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

Company Name

study

For example, you could type the name of your workplace or the name of a server you will connect to.

< Back Next > Cancel

در این پنجره شماره تلفنی را که از طریق آن به سرور وصل خواهیم شد را وارد می کنیم.

New Connection Wizard

Phone Number to Dial
What is the phone number you will use to make this connection?

Type the phone number below.

Phone number:
0452723394

You might need to include a "1" or the area code, or both. If you are not sure you need the extra numbers, dial the phone number on your telephone. If you hear a modem sound, the number dialed is correct.

< Back Next > Cancel

در این پنجره اگر گزینه **Anyone's use** را انتخاب کنیم از این connection همه کاربران استفاده خواهند کرد. ولی اگر گزینه **My use only** را انتخاب کنیم فقط کاربری که خودمان اجازه می دهیم می تواند دسترسی از راه دور داشته باشد.

New Connection Wizard

Connection Availability
You can make the new connection available to any user or only to yourself.

A connection that is created for your use only is saved in your user account and is not available unless you are logged on.

Create this connection for:

☐ Anyone's use

☒ My use only

< Back Next > Cancel

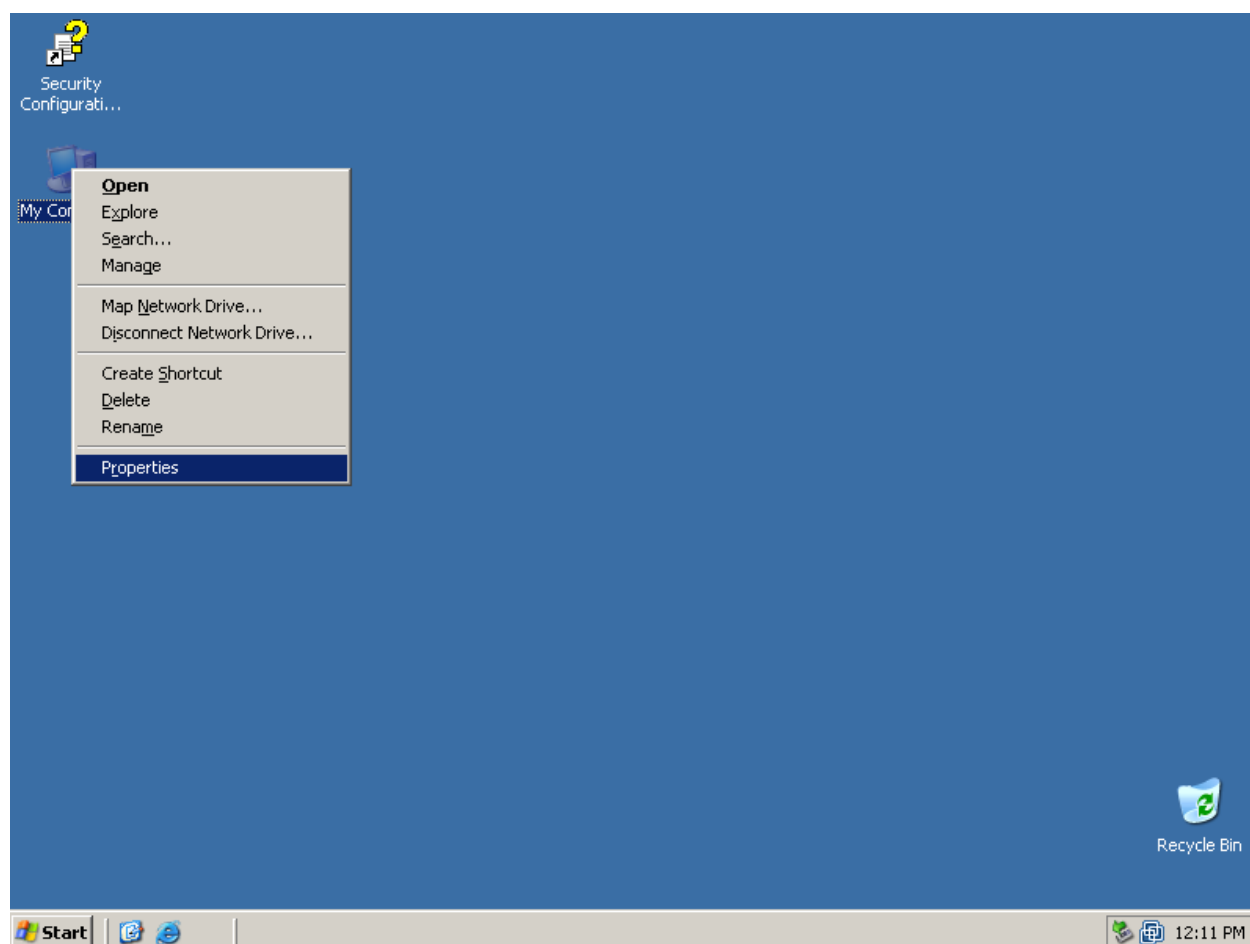
بعد از اتمام مراحل کار، این پنجره نمایش داده می شود که بر روی **Finish** کلیک می کنیم.



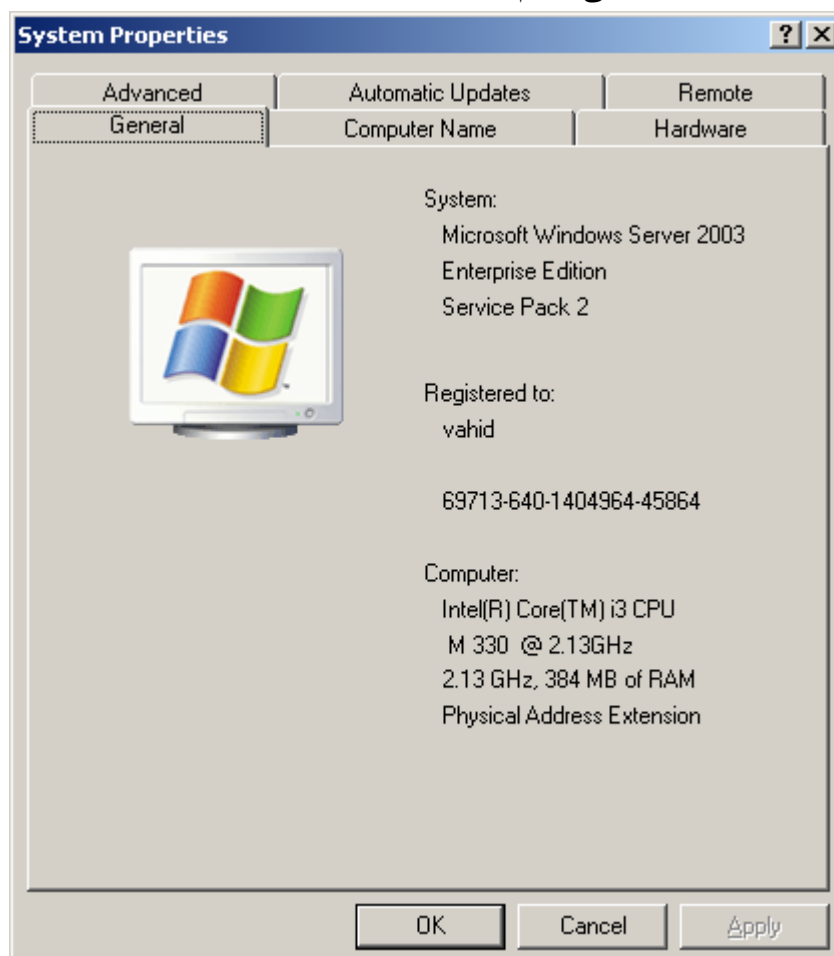
۳-۱-۱-۹- بررسی تعیین اجازه برای دستیابی از راه دور:

بعد از انجام این مراحل ما باید به عنوان مدیر اجازه دسترسی از راه دور به سرور را، به کاربر دهیم. برای این کار این مراحل را انجام می دهیم:

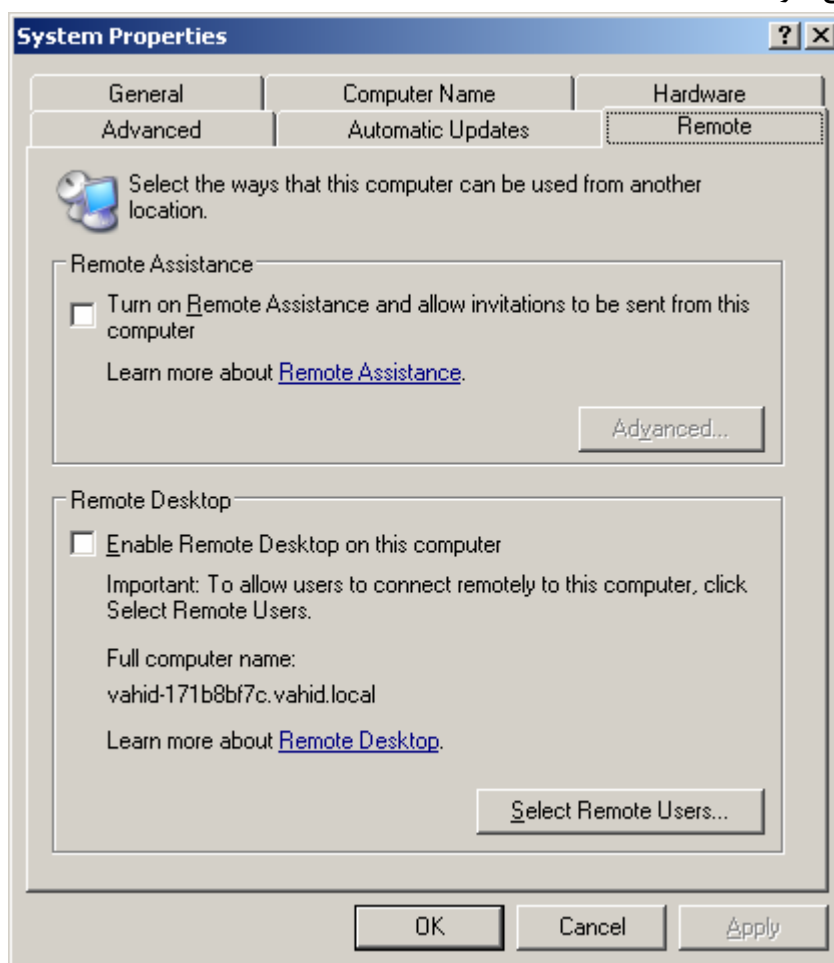
بر روی My Computer کلیک راست کرده و بر روی Properties کلیک می کنیم.



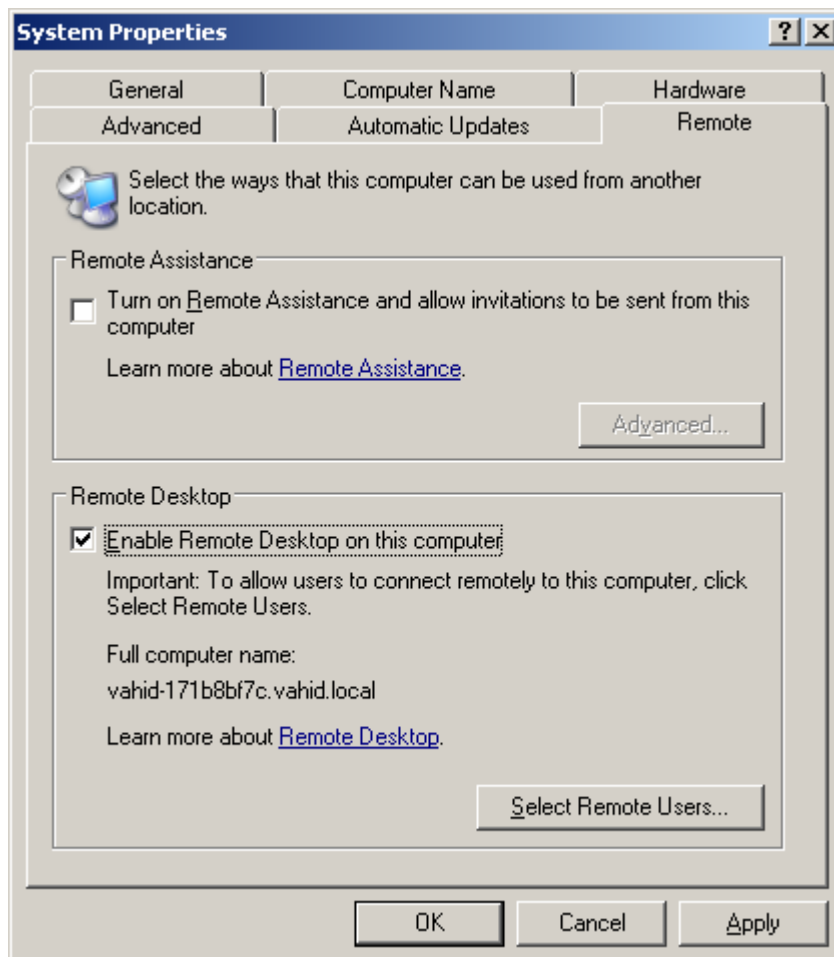
در این پنجره بر روی زبانه Remote کلیک می کنیم.



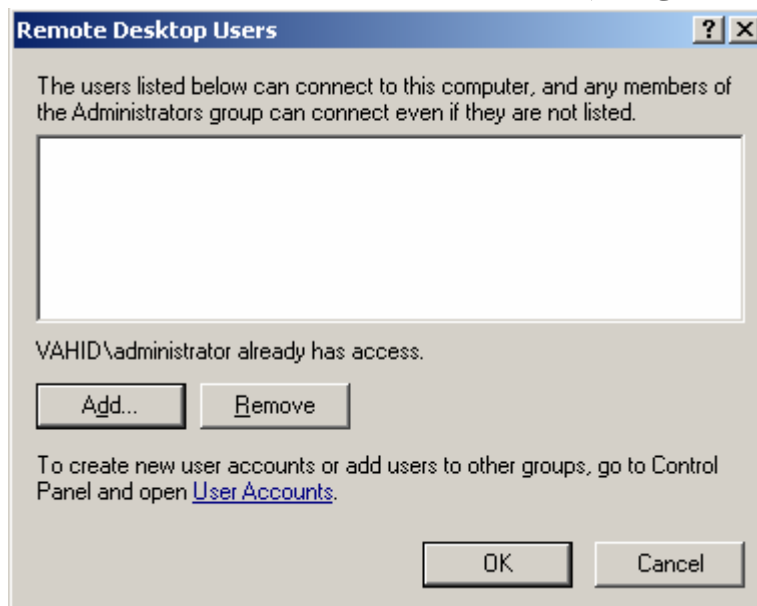
این پنجره نمایش داده می شود.



برای دادن دستیابی از راه دور به سرور، کادر **Enable Remote Desktop on this computer** را انتخاب می کنیم. حال می خواهیم به کاربر خاصی اجازه دستیابی از راه دور به سرور را بدهیم، برای این کار بر روی **Select Remote Users** کلیک می کنیم.



در این پنجره بر روی Add کلیک می کنیم.



بر روی Advanced کلیک می کنیم.

Select Users or Groups [?] [X]

Select this object type:

From this location:

Common Queries

Name:

Description:

☐ Disabled accounts
☐ Non expiring password

Days since last logon:

Search results:

Name (RDN)	E-Mail Address	In Folder
Administrator		vahid.local/Users
ashkan		vahid.local/Users
Guest		vahid.local/Users
krbtgt		vahid.local/Users
model		vahid.local/87intra
reza		vahid.local/87intra
SUPPORT_3...		vahid.local/Users

بر روی OK کلیک می کنیم.

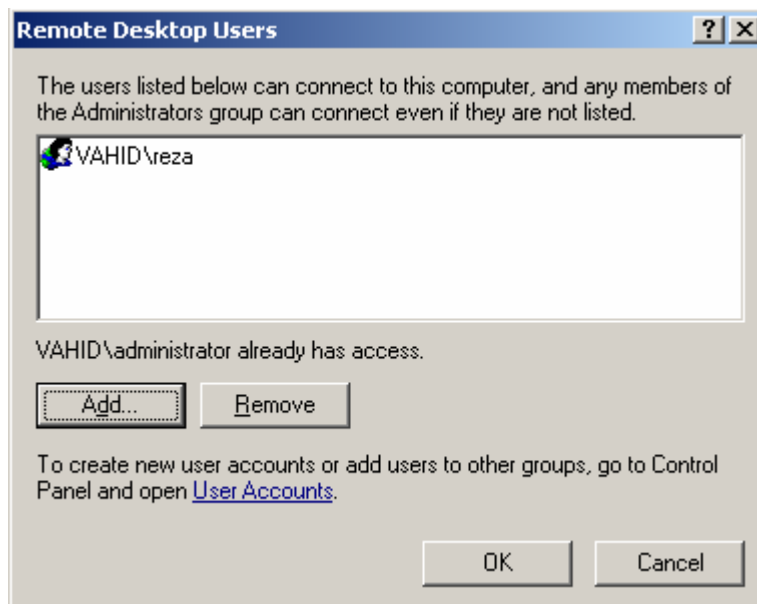
Select Users or Groups [?] [X]

Select this object type:

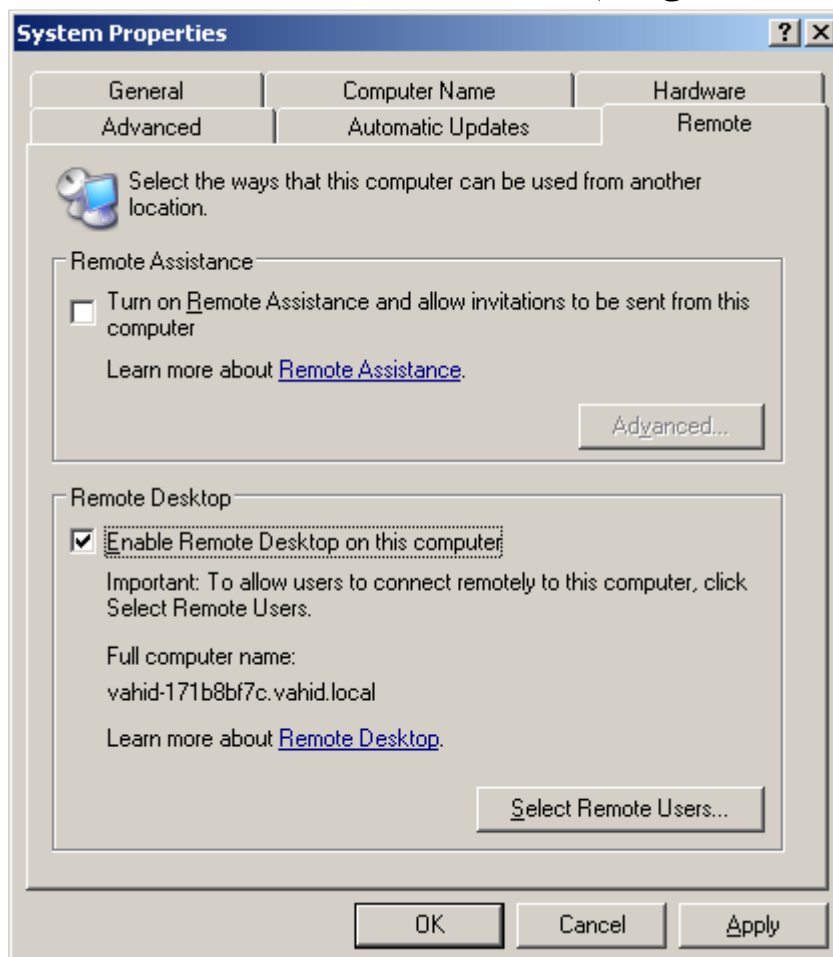
From this location:

Enter the object names to select (examples):

بر روی OK کلیک می کنیم.



در این پنجره نیز بر روی OK کلیک می کنیم.



بعد از انجام این مراحل سرور برای دستیابی از راه دور تنظیم شده است. حال باید کلاینت نیز برای دستیابی به سرور تنظیم شود.

۲-۱-۹- بررسی تنظیمات کلاینت برای دستیابی از راه دور:

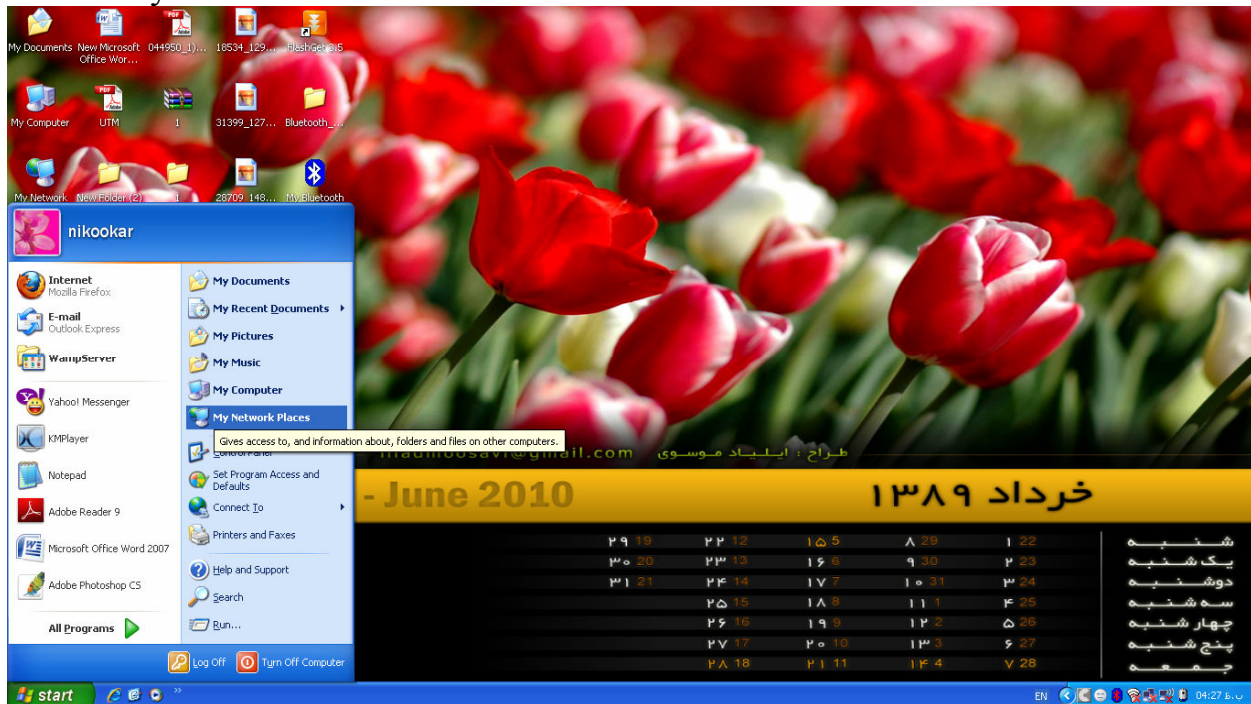
بعد از اینکه سرور را برای دستیابی از راه دور تنظیم کردیم، باید تنظیماتی را در کامپیوتری که می خواهیم به وسیله آن از راه دور به سرور دستیابی داشته باشیم، را انجام دهیم برای این کار مراحل زیر را طی می کنیم:

۱-۲-۹- بررسی ایجاد Connection برای دستیابی از راه دور در کلاینت:

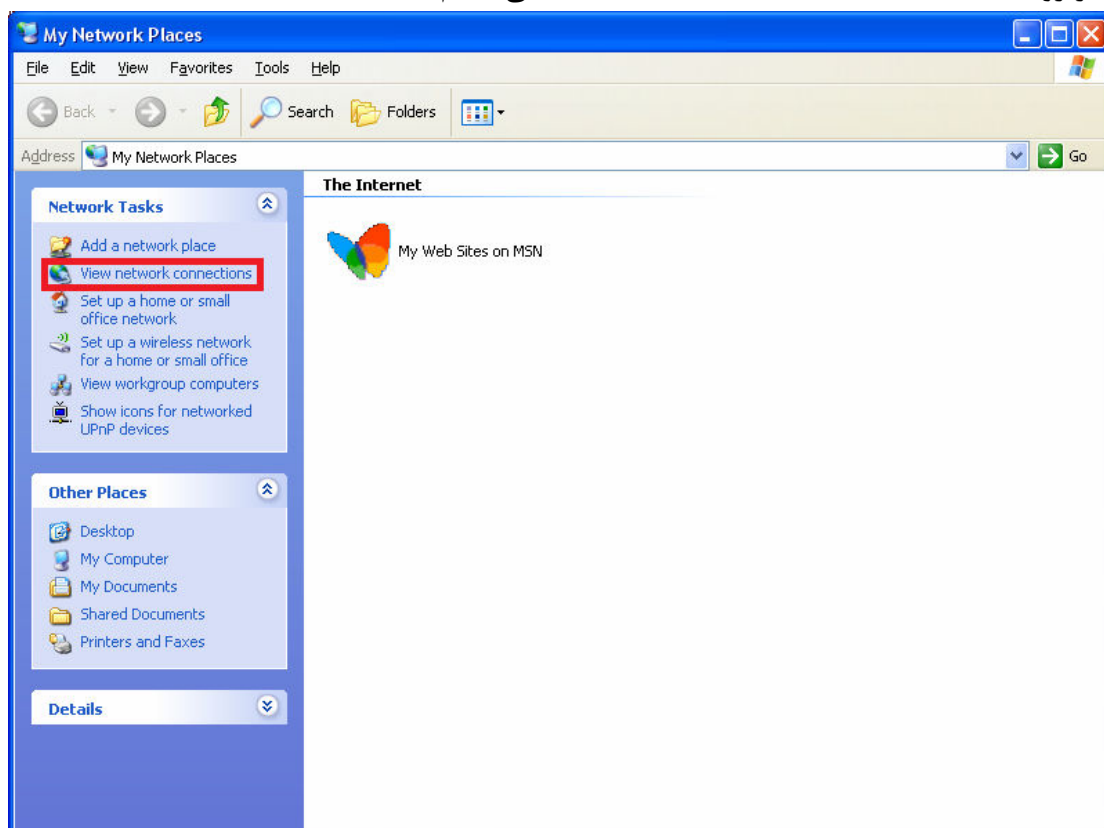
برای ایجاد Connection در کلاینت این مراحل را انجام می دهیم:

به مسیر زیر می رویم:

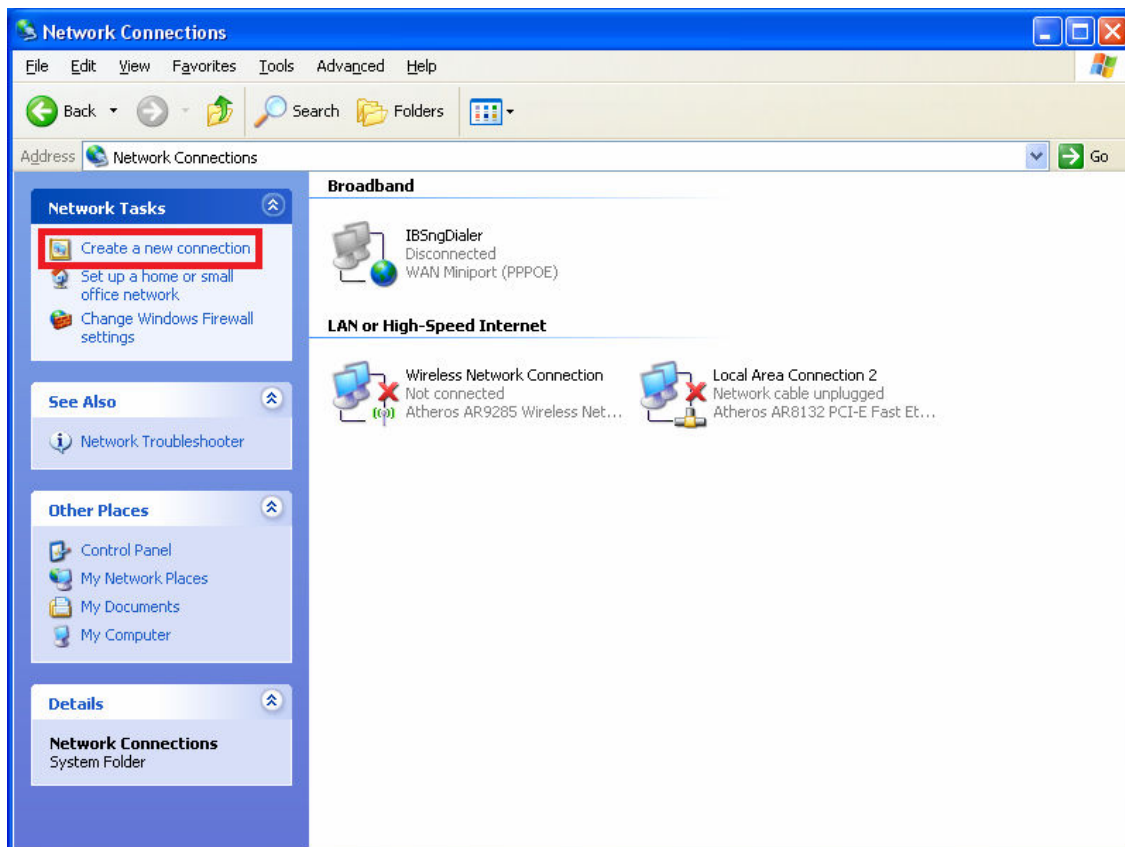
Strat > My Network Places



در این پنجره بر روی View network connection کلیک می کنیم.



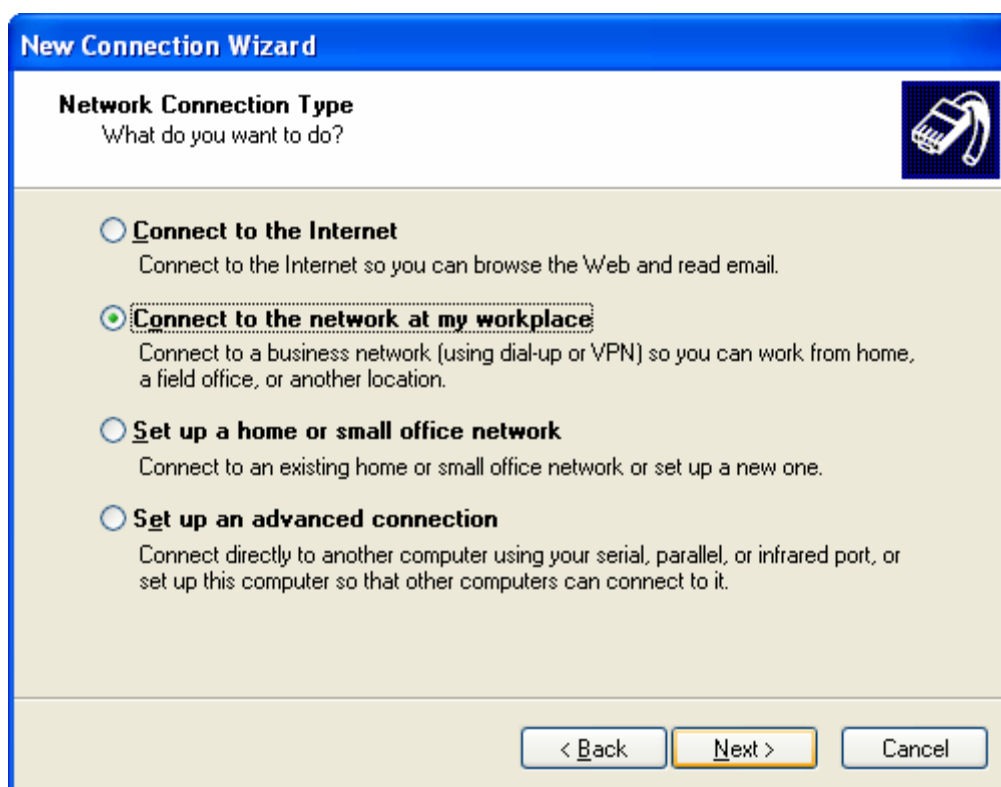
بر روی Create a new connection کلیک می کنیم.



پنجره خوش آمد گویی New Connection نمایش داده می شود. بر روی Next کلیک می کنیم.



در این پنجره چون ما با استفاده از Dial-up می خواهیم از راه دور به سرور وصل شویم بر روی گزینه دوم را انتخاب و بر روی Next کلیک می کنیم.



در این پنجره گزینه Dial-up connection را انتخاب و بر روی Next کلیک می نماییم.



در این پنجره نامی را برای Connection وارد کرده و Next می کنیم.

New Connection Wizard

Connection Name
Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

Company Name

conrt

For example, you could type the name of your workplace or the name of a server you will connect to.

< Back Next > Cancel

New Connection Wizard

Public Network
Windows can make sure the public network is connected first.

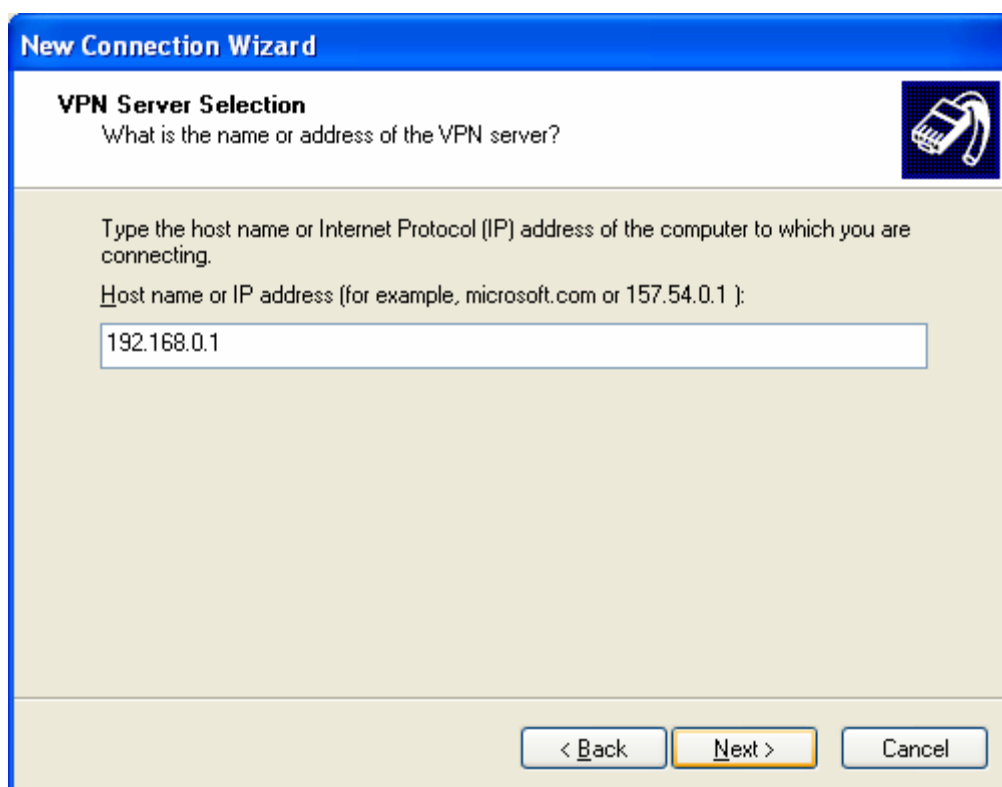
Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.

☒ Do not dial the initial connection:

☐ Automatically dial this initial connection:

< Back Next > Cancel

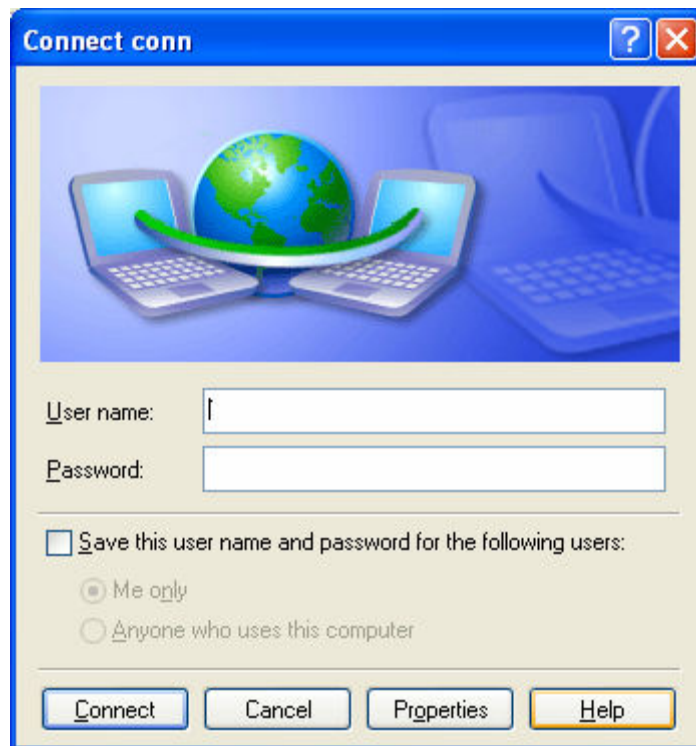
در این پنجره باید IP سرور را وارد کنیم.



بر روی Finish کلیک می کنیم.



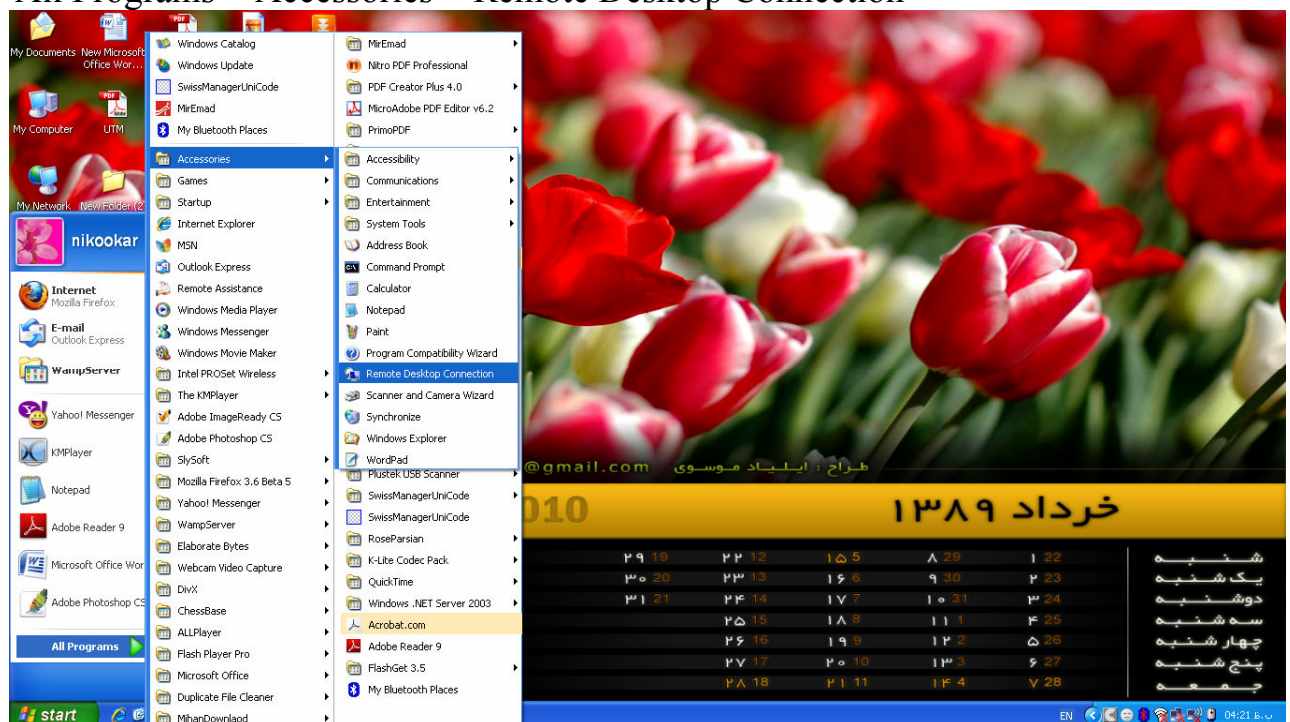
حال Connection ایجاد شده است.



۲-۱-۹- وصل شدن به سرور از راه دور:

برای وصل شدن به سرور به مسیر زیر می رویم:

Start > All Programs > Accessories > Remote Desktop Connection



پنجره زیر ظاهر می شود که برای وصل شدن باید نام کامپیوتر را وارد نماییم.



اگر بر روی Options کلیک کنیم تنظیمات پیش فرض Remote Desktop Connection را می توانیم ر صورت نیاز تغییر دهیم.

