

پیگر بندی و مدیریت

# ویندوز سرور 2008R2

- ✓ آموزش کامل آدرسدهی (IPv4 و IPv6) در شبکه و انجام سابنتینگ
- ✓ آموزش نصب و ارتقاء ویندوز سرور
- ✓ آموزش Server Core در ویندوز سرور 2008R2
- ✓ استفاده از دستورات در Cmd و PowerShell
- ✓ نصب و راه اندازی سرور DNS
- ✓ نصب و راه اندازی سرور DHCP
- ✓ آموزش Active Directory و Domain Controller
- ✓ ایجاد و مدیریت حسابهای کاربری، گروهها، و واحدهای سازمانی
- ✓ آموزش کار با سیاستها و Group Policy
- ✓ اشتراک گذاری فایل و ایجاد File Server
- ✓ اشتراک گذاری پرینتر و ایجاد Print Server
- ✓ آموزش Backup گیری از سرور و Active Directory
- ✓ اشتراک گذاری اینترنت و راه اندازی NAT Server در شبکه

مؤلف: اسماعیل یزدانی



**پیکربندی و مدیریت ویندوز سرور  
2008 R2**

**Configuring and Managing  
Windows Server 2008 R2**

مؤلف: اسماعیل یزدانی

سرشناسه	: یزدانی، اسماعیل، ۱۳۷۰
عنوان و نام پدیدآور	: پیکربندی و مدیریت ویندوز سرور R2 ۲۰۰۸ / مؤلف اسماعیل یزدانی.
مشخصات نشر	: اصفهان، آسمان نگار، ۱۳۹۲.
مشخصات ظاهری	: ۵۹۲ ص. مصور(رنگی)، جدول.
شابک	: ۹۷۸-۶۰۰-۶۵۹۶-۶۶-۲ : ۱۳۵۰۰۰ ریال
وضعیت فهرست نویسی	: فیپا
یادداشت	: کتابنامه: ص. ۵۷۳.
موضوع	: ویندوز مایکروسافت، سرور
موضوع	: سیستم‌های عامل (کامپیوتر)
رده بندی کنگره	: ۱۳۹۲ ی۴ ۹۴/س/۷۶ QA۷۶
رده بندی دیویی	: ۰۰۵/۴۴۷۶
شماره کتابشناسی ملی	: ۳۳۲۰۰۷۵

### انتشارات آسمان نگار (۰۹۱۳۱۱۷۲۶۴۲)

نام کتاب	: پیکربندی و مدیریت ویندوز سرور R2 ۲۰۰۸
مؤلف	: اسماعیل یزدانی
قیمت	: ۱۳۵۰۰ تومان
نوبت و سال چاپ	: اول/ ۱۳۹۲
تیراژ	: ۱۰۰۰ جلد
شماره استاندارد بین المللی کتاب	: ۹۷۸-۶۰۰-۶۵۹۶-۶۶-۲
ISBN	: 978-600-6596-66-2

کلیه حقوق مادی و معنوی این اثر محفوظ و متعلق به مؤلف آن می‌باشد.

تقدیم به

مادرم، آنکه آفتاب مهرش در آستانه قلمم، پمخنان پابرجاست و هرگز غروب نخواهد کرد.

كُلُّ وِعَاءٍ يَضِيقُ بِمَا جُعِلَ فِيهِ إِلَّا وِعَاءُ الْعِلْمِ فَإِنَّهُ يَتَّسِعُ بِهِ؛

فضای هر ظرفی در اثر محتوای خود تنگتر می‌شود مگر ظرف دانش که با تحصیل علوم، فضای آن بازتر می‌گردد.

شرح نهج البلاغه ابن ابی الحدید، ج ۱۹، ص ۲۵



**استفاده از این کتاب کاملاً رایگان است**

## پیش‌گفتار

ویندوز سرور 2008R2 دومین نسخه از ویندوز سرور 2008 و یکی از پرتعدادترین محصولات در زمینه سیستم عامل شبکه است که پس از انتشار توانست به سرعت جای خود را در انواع شبکه‌های کوچک و بزرگ باز نماید. با توجه به اینکه اکثر شرکت‌ها در سرتاسر دنیا جهت مدیریت شبکه و کاربران آن از این سیستم عامل استفاده می‌کنند، آشنایی با پیکربندی و مدیریت آن برای متخصصین فعال در این زمینه امری ضروری خواهد بود. در این کتاب تلاش شده است به زبانی ساده و گویا، مهمترین و ضروری ترین اقدامات پیکربندی جهت استفاده از ویندوز سرور 2008 و 2008R2 به صورت گام به گام و کاملاً مصور آموزش داده شوند.

خوانندگان عزیز پس از مطالعه این کتاب قادر خواهند بود انواع شبکه‌های مبتنی بر مایکروسافت را به راحتی راه اندازی نموده و به مدیریت آنها بپردازند. مواردی همچون آدرس‌های IPv4 و IPv6، سرویس‌های Active Directory، DNS، DHCP، Group Policy، File Server، NAT، Print Server، و همچنین مدیریت حساب‌های کاربری، گروه‌ها و واحدهای سازمانی از جمله مواردی هستند که به خوبی در این کتاب پوشش داده شده‌اند.

لازم می‌دانم از مسئولین محترم دانشگاه پیام نور مبارکه به‌ویژه جناب آقای مهدی بهرامی، و همچنین برادر عزیزم جناب آقای محمدحسین یزدانی بابت کمک‌هایی که در راستای چاپ این کتاب نموده‌اند کمال تشکر و قدردانی را داشته باشم.

اسماعیل یزدانی

پاییز ۱۳۹۲



## فهرست مطالب

فصل اول: آشنایی با مدل‌های مرجع، آدرس‌های IP، و سابنتینگ	۱
۱-۱ آشنایی با مدل هفت لایه‌ای OSI	۳
۱-۱-۱ پشته‌های پروتکل	۴
۱-۱-۲ لایه Physical	۶
۱-۱-۳ لایه Data Link	۷
۱-۱-۴ لایه Network	۸
۱-۱-۵ لایه Transport	۹
۱-۱-۶ لایه Session	۱
۱-۱-۷ لایه Presentation	۱
۱-۱-۸ لایه Application	۱۱
۱-۱-۹ ارتباط میان پشته‌ها در مدل OSI	۱۲
۲-۱ آشنایی با مدل TCP/IP	۱۴
۲-۱-۱ جزئیات مدل TCP/IP	۱۴
۲-۱-۲ برقراری ارتباط میان لایه‌های TCP/IP	۱۵
۳-۱ آشنایی با آدرس‌های IPv4	۱۶
۳-۱-۱ معرفی آدرس IPv4	۱۶
۳-۱-۲ ساختار آدرس IP	۱۷
۳-۱-۳ کلاس‌های آدرس IP	۱۷
۴-۱ انجام سابنتینگ در شبکه	۲۱
۴-۱-۱ پیاده‌سازی سابنتینگ	۲۲
۴-۱-۲ روشی ساده برای اعمال سابنتینگ	۳
۴-۱-۳ اعمال سابنتینگ به روش سنتی	۳۲
۵-۱ آدرس‌دهی بدون کلاس	۴۱
۵-۱-۱ شناسایی سریع مشخصات زیرشبکه با استفاده از CIDR	۴۱
۵-۱-۲ تعیین تعداد زیرشبکه‌ها و میزبان‌ها	۴۴
۶-۱ آشنایی با آدرس‌های IPv6	۴۴
۶-۱-۱ نمایش آدرس‌های IPv6	۴۴
۶-۱-۲ خلاصه نویسی آدرس‌های IPv6	۴۵
۶-۱-۳ انواع آدرس‌های IPv6	۴۶

<b>فصل دوم: نصب و ارتقاء به ویندوز سرور 2008R2</b>	<b>۵۵</b>
۱-۲ تغییرات نصب نسبت به ویندوز سرور 2000 و 2003	۵۷
۲-۲ نیازمندی‌های نصب ویندوز سرور 2008 و 2008R2	۵۸
۳-۲ نصب دستی سیستم عامل	۶۱
۴-۲ ارتقاء ویندوز سرور	۷۰
۵-۲ بررسی ابزارهای Initial Configuration Tasks	۷۶
۶-۲ پیکربندی سرور به کمک Server Manager	۷۷
۱-۶-۲ اقدامات پیکربندی متداول	۷۸
۲-۶-۲ افزودن و حذف کردن Role ها	۸۷
۳-۶-۲ افزودن و حذف کردن Feature ها	۱۰۴
۷-۲ نصب خودکار ویندوز	۱۰۶
۱-۷-۲ نصب WAIK	۱۰۷
۲-۷-۲ ایجاد فایل پاسخ	۱۱
۳-۷-۲ استفاده از فایل پاسخ	۱۲
<b>فصل سوم: آشنایی با Server Core</b>	<b>۱۲۲</b>
۱-۳ Server Core چیست؟	۱۲۵
۲-۳ نصب Server Core	۱۲۶
۳-۳ راهنمایی‌های ضروری در Server Core	۱۲۸
۱-۳-۳ دسترسی به Task Manager	۱۲۸
۲-۳-۳ دسترسی به Command Prompt	۱۲۹
۳-۳-۳ تغییر رمز عبور	۱۲۹
۴-۳-۳ دسترسی به فایل‌های اشتراکی	۱۳
۵-۳-۳ پیدا کردن دستورات خط فرمان به ترتیب حروف الفبا	۱۳۱
۶-۳-۳ پیدا کردن قالب دستورات به کمک علامت ؟	۱۳۱
۷-۳-۳ خواندن فایل‌های متنی به کمک Notepad	۱۳۱
۸-۳-۳ مهندسی معکوس	۱۳۲
۹-۳-۳ Restart و خاموش کردن Server Core	۱۳۲
۴-۳ پیکربندی مقدماتی Server Core	۱۳۲
۱-۴-۳ مرحله ۱: Provide Computer Information	۱۳۳
۲-۴-۳ مرحله ۲: Update This Server	۱۳۶
۳-۴-۳ مرحله ۳: Customize This Server	۱۳۷



۱۴۲	..... ۵-۳ پیکربندی Role ها و Feature ها در Server Core
۱۴۲	..... ۱-۵-۳ ایجاد Domain Controller و مدیریت DNS
۱۴۳	..... ۲-۵-۳ پیکربندی سرویس DHCP
۱۴۶	..... ۳-۵-۳ راه اندازی File Server

## فصل چهارم: DNS و نامگذاری ..... ۱۵۷

۱۵۹	..... ۱-۴ مفاهیم پایه DNS
۱۶۳	..... ۲-۴ نصب DNS Server
۱۶۷	..... ۳-۴ ایجاد Zone و مدیریت فضاهای نام
۱۶۷	..... Forward Lookup Zones ۱-۳-۴
۱۶۷	..... Reverse Lookup Zones ۲-۳-۴
۱۶۸	..... Primary Zones ۳-۳-۴
۱۷۴	..... Secondary Zones ۴-۳-۴
۱۷۸	..... Stub Zones ۵-۳-۴
۱۷۹	..... Zones های یکپارچه با اکتیو دایرکتوری ۶-۳-۴
۱۸۳	..... ۴-۴ یکپارچگی با سایر سرورهای DNS
۱۸۳	..... Iteration ۱-۴-۴
۱۸۴	..... Recursion ۲-۴-۴
۱۸۵	..... Delegation ۳-۴-۴
۱۸۶	..... Forwarding ۴-۴-۴
۱۸۸	..... ۵-۴ آشنایی با انواع رکوردها در DNS
۱۸۸	..... Host رکوردهای ۱-۵-۴
۱۹	..... Pointer رکوردهای ۲-۵-۴
۱۹	..... Alias رکوردهای ۳-۵-۴
۱۹۱	..... Mail Exchanger رکوردهای ۴-۵-۴
۱۹۲	..... Service Location رکوردهای ۵-۵-۴
۱۹۳	..... Start Of Authority رکوردهای ۶-۵-۴
۱۹۵	..... Name Server رکوردهای ۷-۵-۴
۱۹۵	..... Scavenging و Aging فرایندهای ۸-۵-۴
۱۹۷	..... ۶-۴ پیاده سازی DNS در Server Core
۱۹۸	..... DNS نصب ۱-۶-۴
۱۹۸	..... DNS پیکربندی سرور ۲-۶-۴
۲	..... ۳-۶-۴ افزودن Zone ها به DNS در Server Core

۲۲	..... Zone مدیریت رکوردها در ۴-۶-۴
----	------------------------------------

## فصل پنجم: مدیریت پروتکل DHCP ..... ۲۰۵

۲۰۷	..... معرفی پردازش DORA ۱-۵
۲۰۸	..... DHCP مزایا و معایب ۲-۵
۲۰۹	..... DHCP مزایای ۱-۲-۵
۲۰۹	..... DHCP معایب ۲-۲-۵
۲۱۰	..... DHCP Lease فرایند ۳-۵
۲۱۰	..... DHCP discovery :۱ مرحله ۱-۳-۵
۲۱۱	..... DHCP lease offer :۲ مرحله ۲-۳-۵
۲۱۱	..... DHCP lease Selection :۳ مرحله ۳-۳-۵
۲۱۱	..... DHCP lease Acknowledgment :۴ مرحله ۴-۳-۵
۲۱۲	..... DHCP Lease تمدید ۵-۳-۵
۲۱۳	..... DHCP Lease آزاد سازی ۶-۳-۵
۲۱۳	..... آشنایی با Scopeها ۴-۵
۲۱۳	..... Scope ۱-۴-۵
۲۱۴	..... Superscope ۲-۴-۵
۲۱۴	..... Exclusions و Reservations ۳-۴-۵
۲۱۵	..... Address Pool ۴-۴-۵
۲۱۵	..... DHCP Relay Agent ۵-۴-۵
۲۱۵	..... DHCP Role نصب ۵-۵
۲۲۱	..... DHCP Authorizing برای اکتیو دایرکتوری ۱-۵-۵
۲۲۲	..... DHCP ایجاد و مدیریت Scopeها در ۶-۵
۲۲۳	..... IPv4 در Scope ایجاد ۱-۶-۵
۲۲۸	..... IPv6 در Scope ایجاد ۲-۶-۵
۲۳۱	..... تغییر مشخصات Scopeها ۳-۶-۵
۲۳۳	..... Exclusion و Reservation مدیریت ۷-۵
۲۳۳	..... Exclusions افزودن و حذف کردن ۱-۷-۵
۲۳۴	..... Reservation افزودن و حذف کردن ۲-۷-۵
۲۳۵	..... IPv4 Scope Options تنظیمات برای ۸-۵
۲۳۵	..... Option با سطوح تخصیص Optionها ۱-۸-۵
۲۳۷	..... Option اختصاصها ۲-۸-۵
۲۳۸	..... DHCP سرور برای کلاسها ۳-۸-۵

۲۴۰	..... ۹-۵ ایجاد و حذف Superscope در IPv4
۲۴	..... ۱-۹-۵ ایجاد یک Superscope
۲۴۲	..... ۲-۹-۵ افزودن Scope به Superscope
۲۴۲	..... ۳-۹-۵ فعال و غیرفعال کردن Superscope
۲۴۲	..... ۱۰-۵ ایجاد Scope های Multicast برای IPv4
۲۴۳	..... ۱-۱-۵ آشنایی با پروتکل MADCAP
۲۴۳	..... ۲-۱-۵ ایجاد Multicast Scopes
۲۴۶	..... ۳-۱-۵ تنظیم مشخصات Multicast Scopes
۲۴۷	..... ۱۱-۵ یکپارچه سازی DDNS با DHCP
۲۴۷	..... ۱-۱۱-۵ بروز رسانی اطلاعات DNS در DHCP
۲۴۸	..... ۲-۱۱-۵ یکپارچه سازی DNS با DHCP
۲۴۹	..... ۱۲-۵ نظارت و عیب یابی DHCP
۲۴۹	..... ۱-۱۲-۵ نظارت بر Lease های DHCP
۲۵	..... ۲-۱۲-۵ ثبت فعالیت های DHCP
۲۵۲	..... ۳-۱۲-۵ کار با پایگاه داده های DHCP
۲۵۴	..... ۴-۱۲-۵ تطبیق دادن Scope های DHCP در IPv4

## ۲۵۷ ..... فصل ششم: اکتیو دایرکتوری

۲۵۹	..... ۱-۶ آشنایی با مفاهیم پایه اکتیو دایرکتوری
۲۵۹	..... ۱-۱-۶ Workgroup
۲۶	..... ۲-۱-۶ Domain
۲۶	..... ۳-۱-۶ Active Directory Domain Services (AD DS)
۲۶۱	..... ۴-۱-۶ Replication
۲۶۱	..... ۵-۱-۶ Objects
۲۶۲	..... ۶-۱-۶ Schema
۲۶۲	..... ۷-۱-۶ Organizational units
۲۶۳	..... ۸-۱-۶ Group Policy
۲۶۳	..... ۹-۱-۶ Default domain policy
۲۶۳	..... ۱-۱-۶ Default domain controllers policy
۲۶۳	..... ۱۱-۱-۶ Site
۲۶۴	..... ۱۲-۱-۶ Forest
۲۶۴	..... ۱۳-۱-۶ Global Catalog
۲۶۵	..... ۱۴-۱-۶ Tree

۲۶۵	۲-۶ جنگل تک دامنه‌ای
۲۶۶	۱-۲-۶ مزایای استفاده از یک دامنه
۲۶۷	۲-۲-۶ ایجاد جنگل تک دامنه‌ای
۲۸۲	۳-۶ افزودن DC ثانویه
۲۸۸	۴-۶ ایجاد واحدهای سازمانی (OU)، حساب‌های کاربری و گروه‌ها
۲۸۸	۱-۴-۶ ایجاد واحدهای سازمانی
۲۹۶	۲-۴-۶ ایجاد حساب‌های کاربری و کامپیوتری
۳	۳-۴-۶ ایجاد گروه‌ها
۳۰۵	۵-۶ اقدامات نگهداری از دامنه
۳ ۵	۱-۵-۶ پیوستن به یک دامنه
۳ ۷	۲-۵-۶ انهدام یک DC
۳ ۸	۳-۵-۶ عیب‌یابی ADI DNS
۳ ۹	۴-۵-۶ افزایش سطح عملکرد دامنه و جنگل
۳۱۲	۵-۵-۶ استفاده از NetDom
۳۱۳	۶-۶ ایجاد سیاست‌های دانه ریز رمز عبور
۳۱۴	۱-۶-۶ نیازمندی‌های سیاست‌های دانه ریز رمز عبور
۳۱۴	۲-۶-۶ ایجاد PSO

## فصل هفتم: ایجاد و مدیریت حساب‌های کاربری و گروه‌ها ..... ۲۲۱

۳۲۳	۱-۷ حساب‌های کاربری
۳۲۳	۱-۱-۷ ایجاد حساب‌های کاربری Local
۳۲۷	۲-۱-۷ ایجاد حساب‌های کاربری مبتنی بر دامنه
۳۳	۳-۱-۷ تغییر تنظیمات حساب‌های کاربری
۳۳۲	۴-۱-۷ مدیریت حساب‌های کاربری مبتنی بر دامنه در خط فرمان
۳۳۴	۲-۷ مدیریت گروه‌ها
۳۳۴	۱-۲-۷ گروه‌های Local
۳۴۱	۲-۲-۷ گروه‌های اکتیو دایرکتوری
۳۴۸	۳-۷ مدیریت حساب‌های کاربری و گروه‌ها به کمک ADAC
۳۴۸	۱-۳-۷ اقدامات پایه در ADAC
۳۵	۲-۳-۷ حرکت در ADAC
۳۵۵	۴-۷ مدیریت حساب‌های کاربری و گروه‌ها به کمک PowerShell
۳۵۶	۱-۴-۷ ایجاد کاربران
۳۵۷	۲-۴-۷ تعیین رمز عبور

۳۵۸	۳-۴-۷ ایجاد همزمان تعدادی کاربر
۳۶	۴-۴-۷ Unlock کردن حساب کاربری
۳۶۲	۵-۴-۷ فعال سازی و غیرفعال کردن حساب کاربری
۳۶۲	۶-۴-۷ ایجاد گروه
۳۶۶	۷-۴-۷ حذف گروه

## فصل هشتم: ایجاد و مدیریت سیاست‌های گروهی..... ۳۶۷

۳۶۹	۱-۸ ایجاد GPO ها
۳۷۵	۲-۸ تغییر عملکرد پیش فرض Group Policy
۳۷۵	۱-۲-۸ سیاست‌های Group Policy
۳۷۸	۲-۲-۸ Group Policy بروی لینک‌های کم سرعت
۳۷۹	۳-۸ استفاده از Group Policy
۳۸	۱-۳-۸ Group policy چگونه اعمال می‌شود
۳۸۲	۲-۳-۸ فیلتر کردن Group policy با استفاده از ACL
۳۸۴	۳-۳-۸ استفاده از فیلترهای WMI به همراه Group policy
۳۸۶	۴-۳-۸ مثال Group policy : انتخاب Password های پیچیده
۳۸۸	۴-۸ تنظیمات Group Policy
۳۸۹	۱-۴-۸ تنظیمات Computer/User Configuration
۴۵	۲-۴-۸ Group Policy Preferences

## فصل نهم: اشتراک‌گذاری فایل‌ها و ایجاد File Server..... ۴۰۹

۴۱۱	۱-۹ File Services Role
۴۱۲	۱-۱-۹ نصب File Services Role
۴۱۵	۲-۹ ایجاد Share
۴۱۵	۱-۲-۹ ایجاد Share با استفاده از Server Manager
۴۲	۲-۲-۹ ایجاد Share بروی کامپیوترهای Remote با استفاده از Server Manager
۴۲۱	۳-۲-۹ ایجاد Share با استفاده از Windows Explorer
۴۲۲	۴-۲-۹ ایجاد Share با استفاده از کنسول Computer Management
۴۲۵	۵-۲-۹ انتشار Share در اکتیو دایرکتوری
۴۲۶	۳-۹ مدیریت مجوزها
۴۲۷	۱-۳-۹ مجوزهای NTFS
۴۲۷	۲-۳-۹ مجوزهای Share
۴۲۸	۳-۳-۹ ایجاد و تغییر مجوزهای NTFS و Share



۴۳۳	۴-۹ اتصال به Share ها
۴۳۵	۵-۹ سرویس File Server Resource Manager
۴۳۵	۱-۵-۹ ایجاد Quota Policy
۴۴	۲-۵-۹ ایجاد یک Quota
۴۴۲	۳-۵-۹ ایجاد File Screen Policy
۴۴۵	۴-۵-۹ ایجاد گزارش ها
۴۴۷	۵-۵-۹ آپشن های File Server Resource Manager
۴۴۸	۶-۹ Distributed File System
۴۵	۱-۶-۹ آشنایی با اصطلاحات DFS
۴۵	۲-۶-۹ نصب DFS
۴۵۱	۳-۶-۹ ایجاد DFS Root
۴۵۴	۴-۶-۹ افزودن لینک ها به DFS Root
۴۵۵	۵-۶-۹ پیکربندی DFS Replications
۴۸۴	۷-۹ سرویس Network File System
۴۶۲	۱-۷-۹ نصب NFS
۴۶۳	۲-۷-۹ پیکربندی احراز هویت NFS و ایجاد NFS Share
۴۶۵	<b>فصل دهم: اشتراک گذاری پرینتر و ایجاد Print Server</b>
۴۶۷	۱-۱۰ نگاهی بر سرویس های چاپ
۴۶۸	۱-۱-۱ Print Spooler
۴۶۸	۲-۱-۱ درایور پرینتر
۴۶۹	۲-۱۰ نصب Print and Document Services Role
۴۷	۱-۲-۱ افزودن Print and Document Services Role
۴۷۱	۲-۲-۱ کار با کنسول Print Management
۴۷۹	۳-۱۰ استقرار پرینترها برای کاربران
۴۷۹	۱-۳-۱ افزودن دستی پرینتر برای کاربران
۴۸۱	۲-۳-۱ افزودن پرینتر با استفاده از ابزار Active Directory Search
۴۸۴	۳-۳-۱ استقرار پرینتر با استفاده از GPO
۴۸۷	۴-۱۰ انجام تنظیمات Print Server
۴۸۷	۱-۴-۱ Server Properties
۴۹	۲-۴-۱ Import و Export کردن پرینترها
۴۹۲	۵-۱۰ مدیریت تنظیمات پرینترها
۴۹۵	۶-۱۰ مدیریت Print Jobs

۷-۱۰ استفاده از Custom Filters ..... ۴۹۶

## **فصل یازدهم: اتصال کاربران به سرور و دامنه ..... ۴۹۹**

۱-۱۱ بررسی تنظیمات پیکربندی شبکه ..... ۵۰۱

۱-۱-۱۱ بررسی تنظیمات Local Area Connection ..... ۵۰۲

۲-۱-۱۱ تست ارتباط شبکه با دستور Ping ..... ۵۰۴

۳-۱-۱۱ بررسی تنظیمات Local Area Connection با استفاده از GUI ..... ۵۰۵

۲-۱۱ اتصال به دامنه ..... ۵۱۰

۱-۲-۱۱ اتصال به دامنه با استفاده از ویندوز ۷ ..... ۵۰۱

۲-۲-۱۱ اتصال به دامنه با استفاده از ویندوز XP ..... ۵۱۲

۳-۱۱ اتصال به منابع شبکه ..... ۵۱۳

۱-۳-۱۱ اتصال به منابع با استفاده از ویندوز ۷ ..... ۵۱۴

۲-۳-۱۱ اتصال به منابع با استفاده از ویندوز XP ..... ۵۲۴

## **فصل دوازدهم: Backup گیری از سرور، پوشه‌ها، و اکتیو دایرکتوری ..... ۵۲۱**

۱-۱۲ Backup گیری و بازگردانی ویندوز سرور ..... ۵۳۳

۱-۱-۱۲ نصب Windows Server Backup ..... ۵۳۴

۲-۱-۱۲ فعال‌سازی قابلیت Shadow Copy ..... ۵۳۵

۳-۱-۱۲ Backup گیری و بازگردانی کامل یک سرور ..... ۵۳۶

۴-۱-۱۲ Backup گیری و بازگردانی فایل‌ها و پوشه‌ها ..... ۵۴۶

۲-۱۲ Backup گیری و بازگردانی اکتیو دایرکتوری ..... ۵۵۱

۱-۲-۱۲ ایجاد Backup از اکتیو دایرکتوری ..... ۵۵۲

۲-۲-۱۲ بازگردانی Backup ایجاد شده از اکتیو دایرکتوری ..... ۵۵۳

## **فصل سیزدهم: اشتراک‌گذاری اینترنت و راه اندازی سرور NAT ..... ۵۵۷**

۱-۱۳ مفاهیم اولیه NAT ..... ۵۵۹

۲-۱۳ سرویس ICS ..... ۵۶۱

۱-۲-۱۳ راه اندازی NAT به کمک سرویس ICS ..... ۵۶۲

۲-۲-۱۳ تغییر تنظیمات کاربران ..... ۵۶۴

۳-۱۳ سرویس Routing And Remote Access ..... ۵۶۴

۱-۳-۱۳ نصب سرویس Routing And Remote Access ..... ۵۶۵

۲-۳-۱۳ پیکربندی NAT در کنسول Routing And Remote Access ..... ۵۶۶

۳-۳-۱۳ پیکربندی DHCP در NAT ..... ۵۶۸

۵۷ ..... NAT در DNS پیکربندی ۴-۳-۱۳

۵۷۱ ..... NAT نکاتی در رابطه با پیکربندی کاربران ۵-۳-۱۳

۵۷۲ ..... منابع و مآخذ

# « فصل ۱ »

آشنایی با مدل‌های مرجع، آدرس‌های IP و  
سابنتینگ

**Introduction to**

**Reference Models, IP Addresses**

**and Subnetting**





از زمان پیدایش شبکه‌های کامپیوتری و مخصوصاً اینترنت، مهندسین شبکه بر آن بوده‌اند که مدل‌های موثر و کارآمدی جهت پیاده‌سازی معماری شبکه ارائه نمایند. تلاش‌های انجام شده در این زمینه، منجر به ایجاد دو مدل OSI و TCP/IP شده که توانسته‌اند تحول عظیمی در شبکه‌های کامپیوتری و مخصوصاً شبکه جهانی اینترنت ایجاد نمایند. این مدل‌ها، دارای ساختاری چند لایه‌ای بوده و در هر لایه مجموعه‌ای از پروتکل‌ها به کارگیری شده است؛ در نهایت ارتباط و همکاری میان این لایه‌ها است که موجب برقراری ارتباط میان سیستم‌های مختلف در طول شبکه و یا اینترنت می‌گردد.

در این فصل قصد داریم به تشریح این دو مدل، لایه‌های تشکیل دهنده آن و پروتکل‌های استفاده شده در هر لایه بپردازیم. بطور کلی مهمترین مباحثی که در این فصل مورد بررسی قرار می‌گیرند عبارتند از:

- ♦ آشنایی با مدل مرجع OSI
- ♦ آشنایی با مدل TCP/IP
- ♦ آدرس‌دهی IP (IPv4 و IPv6) در شبکه
- ♦ روش‌های پیاده‌سازی سابنتینگ<sup>۲</sup>

### ۱-۱ آشنایی با مدل هفت لایه‌ای OSI

مدل مرجع OSI<sup>۱</sup> برای اولین بار توسط سازمان بین‌المللی استانداردسازی (ISO) در سال ۱۹۷۷ توسعه یافت. این مدل بطور گسترده‌ای برای درک ارتباطات شبکه مورد استفاده قرار می‌گیرد و آشنایی با آن می‌تواند نحوه پیاده‌سازی شبکه و برقراری ارتباط میان کامپیوترها را روشنتر سازد. زمانی که قصد دارید با شخص دیگری در شبکه ارتباط برقرار نمایید، باید از دو امکان برخوردار باشید: زبان ارتباط و رسانه ارتباط. اینکه در شبکه از چه سیستمی استفاده می‌کنید (ویندوز، لینوکس و ...) در برقراری ارتباط چندان مهم نیست بلکه موضوع مورد اهمیت، یکسان بودن زبان و رسانه ارتباط می‌باشد. مدل OSI (و سایر مدل‌های توسعه یافته توسط سازمان‌های دیگر) سعی می‌کند قوانینی را تعریف نموده که زبان و رسانه ارتباط را در سیستم‌های مختلف یکسان نموده و ارتباطی واضح و آشکار میان آنها برقرار نماید. در این مدل، جزئیات و کلیات مربوط به ارتباطات شبکه که در ادامه اشاره شده‌اند، تحت پوشش قرار می‌گیرد:

- ♦ نحوه برقراری ارتباط میان دو دستگاه چگونه است.

---

1. Transmission Control Protocol/Internet Protocol  
 2. Subnetting  
 3. Open Systems Interconnection

- ♦ چنانچه زبان دستگاه‌ها در شبکه متفاوت باشد از چه راهکارهایی جهت یکسان‌سازی زبان استفاده می‌شود.
- ♦ یک دستگاه در هنگام انتقال و یا دریافت داده‌ها از چه روش‌هایی استفاده می‌نماید.
- ♦ چگونه یک فرستنده از ارسال صحیح داده‌ها و تحویل آنها به مقصد آگاهی پیدا می‌کند.
- ♦ چگونه یک رسانه فیزیکی انتقال، جهت شرکت در ارتباط تنظیم شده و اتصال را برقرار می‌نماید.
- ♦ آیا وسایل انتقال دهنده، هنگام ارسال داده‌ها در شبکه از نرخ انتقال مناسبی برخوردار هستند و آیا گیرنده قادر به دریافت همزمان داده‌های ارسالی می‌باشد.
- ♦ چگونه بیت‌ها بر روی رسانه انتقال قرار گرفته و جابجا می‌شوند.

مدل OSI یک محصول واقعی نیست که بتوان آنرا در شبکه پیاده‌سازی نمود، بلکه یک چهارچوب مفهومی است که به کمک آن می‌توانید پیچیدگی ارتباط دستگاه‌ها در شبکه و انتقال داده میان آنها را راحت‌تر درک کنید. این مدل به سادگی بیان می‌کند که جهت برقراری ارتباط و انتقال داده‌ها چه کارهایی باید انجام شود و همچنین چه پروتکل‌هایی در هر لایه از مدل جهت انجام این کارها نیاز است. این مدل متشکل از هفت لایه می‌باشد که عبارتند از:

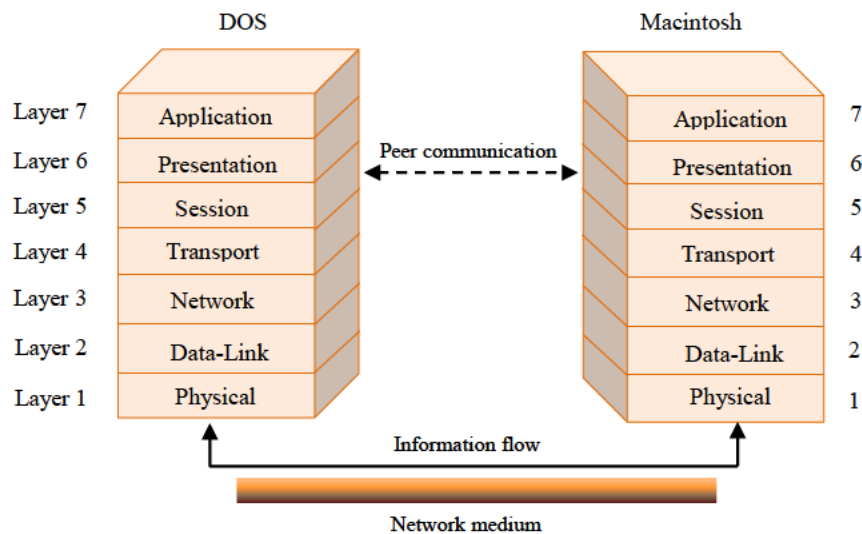
- ♦ لایه Application (لایه ۷)
- ♦ لایه Presentation (لایه ۶)
- ♦ لایه Session (لایه ۵)
- ♦ لایه Transport (لایه ۴)
- ♦ لایه Network (لایه ۳)
- ♦ لایه Data Link (لایه ۲)
- ♦ لایه Physical (لایه ۱)

هرکدام از این هفت لایه دارای عملکردهای متمایزی هستند که بطور مختصر آنها را مورد بررسی قرار خواهیم داد، اما اجازه دهید قبل از آن نگاهی به مفهوم “پشته پروتکل” بیندازیم.

### ۱-۱-۱ پشته‌های پروتکل<sup>۱</sup>

مدل OSI، وظایف انجام شده در برقراری ارتباطات را به قسمت‌های کوچکتری به نام زیروظیفه تقسیم می‌کند. این زیروظیفه‌ها توسط پروتکل‌های سازماندهی شده در هر لایه از مدل OSI قابل انجام می‌باشند. زمانی که این پروتکل‌ها با یکدیگر همکاری نموده تا یک وظیفه را انجام دهند، مجموعه آنها مفهومی به نام پشته پروتکل را ایجاد می‌کنند. در واقع هر پشته مجموعه‌ای از پروتکل‌ها است که در

لایه‌ها سازماندهی شده و فرایند برقراری ارتباط و انتقال داده‌ها را به انجام می‌رسانند. جهت درک پشته، پروتکل TCP/IP را در نظر بگیرید. این پروتکل شامل یک پشته از پروتکل‌های TCP و IP می‌باشد که هر کدام در لایه‌های متفاوتی قرار دارند ولی جهت برقراری یک ارتباط، با یکدیگر همکاری می‌نمایند. در پشته پروتکل، هر لایه خدماتی را از لایه زیرین خود دریافت نموده و آنها را (پس از پردازش) به لایه بالاتر تحویل می‌دهد. به عبارت دیگر شماره N، خدمات را از لایه شماره N-1 دریافت نموده و آنها را به لایه N+1 تحویل می‌دهد. برای برقراری ارتباط، هر کامپیوتر باید از یک پشته پروتکل استفاده نماید، البته به شرطی که این پشته‌ها برای دو طرف درگیر در ارتباط یکسان باشند. همچنین پروتکل‌های به کار رفته در هر لایه از یک پشته، باید با پروتکل‌های لایه متناظر در طرف دیگر یکسان باشد. با این کار، اگر دو طرف حتی از سیستم‌های متفاوتی استفاده نمایند، چون پشته‌های پروتکل در آنها یکسان است به راحتی می‌توانند با یکدیگر ارتباط برقرار نمایند. به عنوان مثال یک کامپیوتر با سیستم عامل DOS می‌تواند در یک ارتباط مبتنی بر IP با کامپیوتری که دارای سیستم عامل Macintosh است ارتباط برقرار نماید. به شکل زیر توجه نمایید.



شکل ۱-۱

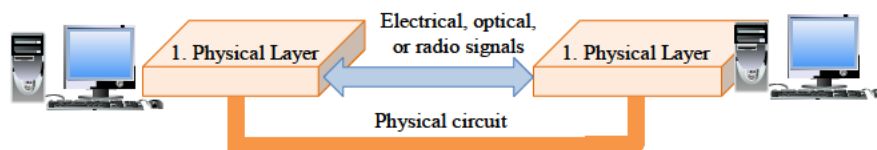
در زمان ارسال داده در شبکه، هر لایه طی فرایندی به نام «انکپسولیشن»<sup>۱</sup> اطلاعات خود (که شامل سرآیند<sup>۲</sup> و سایر اطلاعات کنترلی می‌باشد) را به پشته افزوده و به لایه بعد تحویل می‌دهد. زمانی که داده‌ها توسط گیرنده دریافت می‌شوند، پشته پروتکل از حالت انکپسولیشن خارج شده و با

1. Encapsulation
2. Header
3. Physical Layer

عبور از هر لایه، اطلاعات اضافه شده را در اختیار لایه‌های مرتبط قرار می‌دهد.

### ۲-۱-۱ لایه Physical

لایه Physical (فیزیکی) مسئول استفاده از سیگنال‌های الکتریکی (و در بعضی مواقع سیگنال‌هایی مثل نور و امواج رادیو) جهت انتقال بیت‌ها از یک کامپیوتر به دیگری می‌باشد. این لایه اهمیتی به ماهیت بیت‌ها نمی‌دهد و تنها وظیفه آن جابجایی بیت‌ها از نقطه‌ای به نقطه دیگر و با استفاده از رسانه‌هایی مانند فیبرنوری، کابل‌های مسی و یا امواج رادیویی، لیزر و ... (در ارتباطات بی‌سیم) می‌باشد. در این لایه جزئیات فیزیکی و الکتریکی ارتباط، مانند نوع بیت (۰ یا ۱)، تعداد پین‌های قابل استفاده در کانکتور<sup>۲</sup> شبکه، و جزئیاتی راجع به توانایی یا عدم توانایی کارت شبکه (NIC) در انتقال داده‌ها تعریف می‌شوند.



شکل ۲-۱

بطور کلی می‌توان گفت که کلیه جزئیات مربوط به اتصال فیزیکی میان دو کامپیوتر و رسانه ارتباطی بکار رفته در برقراری ارتباط میان آنها در لایه فیزیکی مشخص می‌شوند. این جزئیات شامل موارد زیر می‌باشد:

- نوع ارتباط شبکه (Point-to-Point یا Point-to-Multi Point)
- توپولوژی فیزیکی شبکه (خطی، ستاره‌ای یا حلقوی)
- نوع رسانه ارتباطی (کابل، امواج رادیو، لیزر، بلوتوث و ...)
- نوع سیگنال استفاده شده برای کد گذاری داده‌ها (آنالوگ یا دیجیتال)
- همگام‌سازی<sup>۳</sup> بیت‌ها جهت هماهنگی فرستنده و گیرنده در خواندن و نوشتن داده‌ها.
- مالتی پلکسینگ<sup>۴</sup> (پردازشی که باعث ترکیب چند کانال ارتباطی و تبدیل آن به یک کانال می‌شود).
- پایان‌دهی<sup>۵</sup> (این عمل مانع از منعکس شدن سیگنال‌ها پس از رسیدن به انتهای کابل می‌شود،

---

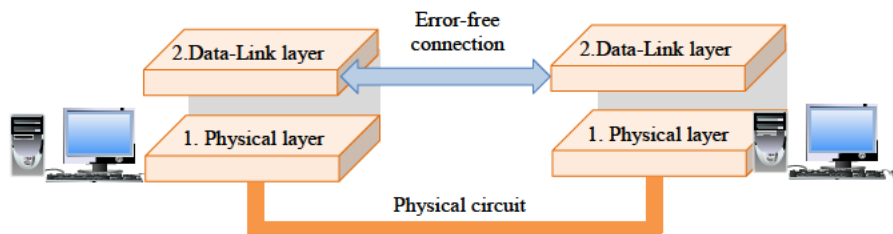
1. Connector  
2. Synchronization  
3. Multiplexing  
4. Termination

بنابراین از بروز خطا جلوگیری می‌نماید. همچنین آخرین گره در هر قسمت از شبکه را نیز مشخص می‌کند.

### ۳-۱-۱ لایه Data Link

لایه Data Link (پیوند داده)، وظیفه انتقال اطلاعات بر روی کانال ارتباطی میان دو دستگاه را برعهده دارد. این لایه، داده‌ها را از لایه شبکه دریافت نموده و آنها را در قالب واحدهایی به نام فریم<sup>۱</sup> بسته‌بندی می‌نماید و پس از افزودن اطلاعات کنترلی، آنها را به لایه Physical تحویل می‌دهد. لایه Data Link انتقال فریم‌ها از یک کامپیوتر به دیگری را به کمک مجموعه‌ای از اطلاعات کنترلی به نام CRC<sup>۲</sup> فراهم می‌نماید. از این اطلاعات جهت تشخیص فریم‌های آسیب دیده و ارسال مجدد آنها استفاده می‌گردد، بنابراین لایه Data Link در کامپیوتر مقصد می‌تواند با درخواست اطلاعات CRC وضعیت فریم‌ها را بررسی نموده و در صورت بروز خطا و یا از دست رفتن فریم‌ها، ارسال مجدد آنها را درخواست نماید.

در شبکه‌های چندپخش<sup>۳</sup> مانند Ethernet، همه دستگاه‌ها می‌توانند فریم‌های ارسالی توسط یک دستگاه را دریافت نمایند، بنابراین در این شبکه‌ها لایه Data Link فریم‌هایی که به یک دستگاه با آدرس مشخص شده فرستاده می‌شود را تشخیص داده و آنها را دریافت می‌کند، سپس بقیه این فریم‌ها را دور می‌ریزد. در شکل زیر برقراری یک اتصال بدون خطا بین دو دستگاه در شبکه توسط لایه Data Link نشان داده شده است.



شکل ۳-۱

در مجموعه استانداردهای IEEE 802.x که توسط مؤسسه IEEE<sup>۴</sup> گسترش یافته است، لایه Data Link به دو زیرلایه تقسیم می‌گردد که عبارتند از:

- زیرلایه LLC<sup>۵</sup>: در این زیرلایه لینک‌های ارتباط منطقی میان دو دستگاه شرکت‌کننده در یک ارتباط ایجاد و نگهداری می‌شود.

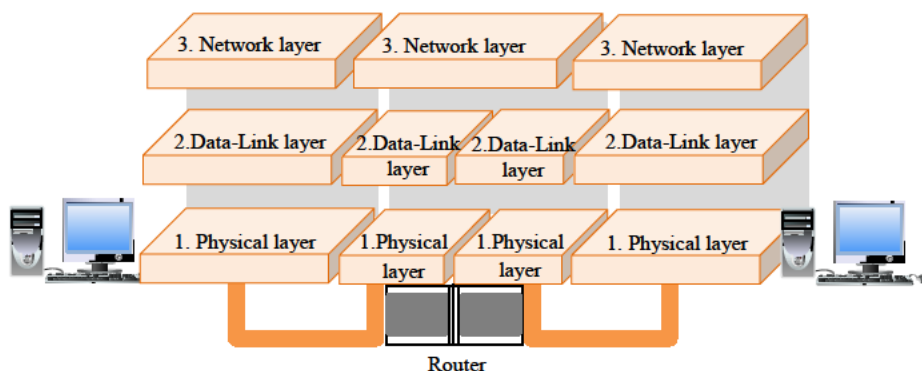
1. Frame  
2. Cyclic Redundancy Check  
3. Multicast  
4. Institute of Electrical and Electronics Engineers  
5. Logical Link Control



- زیر لایه MAC: این زیر لایه روشی جهت تنظیم ترافیک ارسال و دریافت اطلاعات توسط چندین دستگاه، زمانی که از یک کانال ارتباطی یکسان استفاده می‌کنند ارائه می‌دهد.

### ۱-۴ لایه Network

در لایه Network (شبکه) عملیات مربوط به حرکت بسته‌ها در بین دستگاه‌های مورد نظر و همچنین مسیریابی این بسته‌ها انجام می‌گیرد. در شبکه‌های بزرگ، ممکن است میان دو سیستم پایانی (در یک ارتباط)، تعدادی دستگاه واسطه و یا زیر شبکه وجود داشته باشد. لایه شبکه امکان ارسال بسته‌ها را بدون توجه به اینکه دو سیستم پایانی در یک شبکه کابلی و یا در شبکه‌هایی جداگانه که ممکن است در سطح یک کشور قرار داشته باشند فراهم نموده و این بسته‌ها را جهت ارسال، به لایه انتقال تحویل می‌دهد.



شکل ۱-۴

در لایه شبکه اقدامات مهمی جهت تحویل داده‌ها به مقصد انجام می‌گیرد که در میان آنها می‌توان به موارد زیر اشاره نمود:

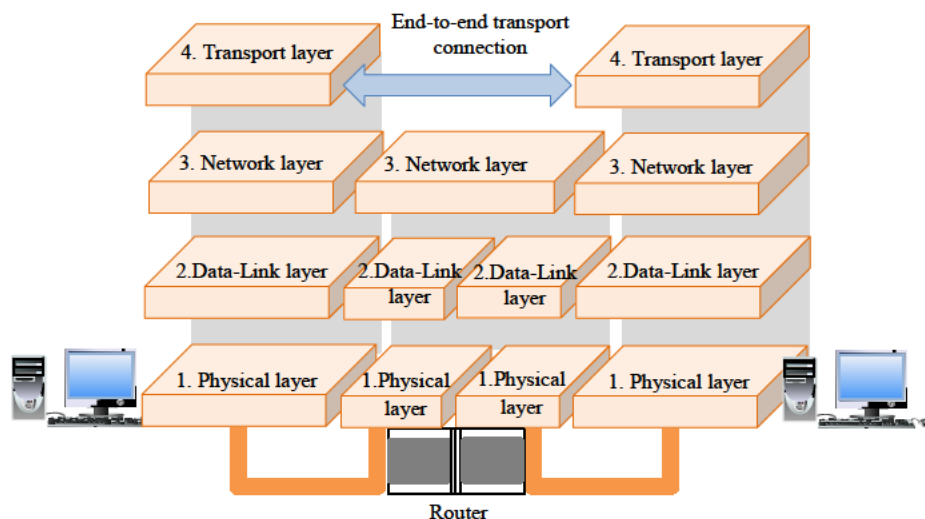
- تعیین آدرس جهت ارسال بسته‌ها به دستگاه مورد نظر.
- عملیات مسیریابی داده‌ها و انتخاب مسیر (در صورتی که میان دستگاه‌ها در شبکه چندین مسیر ارتباطی موجود باشد).
- شکست بسته‌ها به اندازه‌های کوچکتر در صورت لزوم (زمانی که اندازه آنها از اندازه قابل پذیرش توسط لایه Data Link بزرگتر باشد).
- انجام عملیات سوئیچینگ جهت ارسال بسته‌ها (سوئیچینگ مدار<sup>۲</sup>، پیام<sup>۳</sup> و بسته‌ای<sup>۴</sup>).

1. Media Access Control  
2. Circuit Switching  
3. Message Switching  
4. Packet Switching

- کنترل جریان و کنترل خطا در لایه و همچنین حفظ ترتیب ارسال بسته‌ها.
- برقراری ارتباط میان قسمت‌های منطقی در شبکه.
- سرویس‌های Gateway جهت ارسال داده‌ها از یک شبکه به شبکه دیگر.

### ۵-۱-۱ لایه Transport

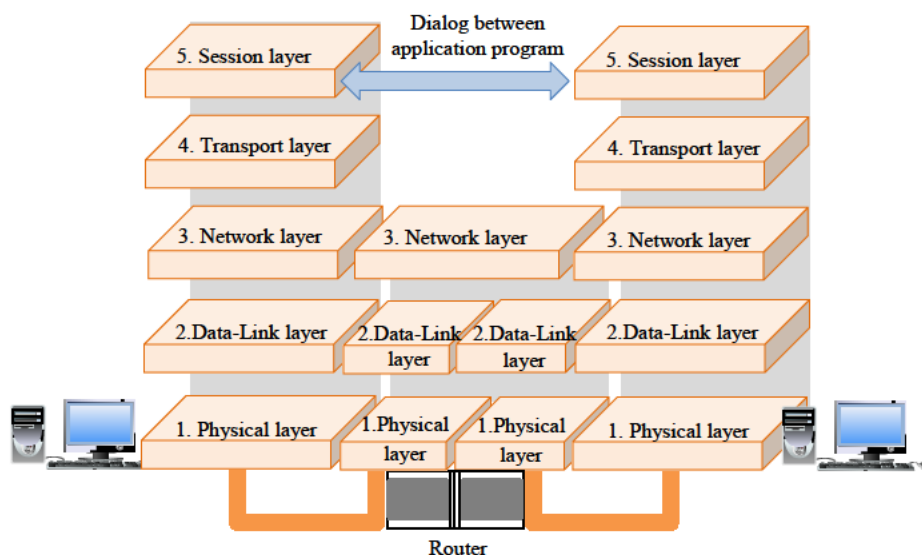
لایه Transport (انتقال) مسئول ارسال بدون خطا، به ترتیب، و بدون گم‌شدن یا تکرار شدن بسته‌ها می‌باشد. همچنین در صورتی که بسته‌های دریافتی از لایه Session (لایه بالایی آن) بزرگ باشند، آنها را به قسمت‌های کوچکتر تقسیم نموده و به لایه شبکه تحویل می‌دهد. این قسمت‌های کوچک پس از دریافت توسط گیرنده، مجدداً در لایه Network به یکدیگر متصل شده و پیغام اصلی را تشکیل می‌دهند، سپس به لایه Session در سمت گیرنده تحویل داده می‌شوند. لایه Transport هنگامی که پیغام‌ها با موفقیت دریافت می‌شوند، به فرستنده پیغام تصدیق دریافت<sup>۱</sup> (Ack) ارسال می‌نماید. البته در همه موارد ارسال پیغام‌های تصدیق نیاز نیست و در کل بستگی به این موضوع دارد که از چه پروتکلی جهت ارسال داده‌ها استفاده می‌شود (TCP یا UDP). چنانچه از پروتکل TCP (که پروتکلی اتصالگرا است) استفاده گردد، به ازای دریافت هر بسته یک پیغام تصدیق فرستاده می‌شود، اما چنانچه از پروتکل UDP (که غیر اتصالگرا است) استفاده شود، هیچ پیغام تصدیقی فرستاده نمی‌شود. در کل اینگونه می‌توان گفت که لایه انتقال خدمات را از لایه بالاتر (Session) دریافت نموده و آنها را به لایه شبکه تحویل می‌دهد. در شکل زیر جایگاه لایه انتقال در مدل OSI نشان داده شده است.



شکل ۵-۱

### ۱-۱-۶ لایه Session

لایه Session (نشست) به برنامه‌های کاربردی موجود در چند کامپیوتر مجزا اجازه می‌دهد که یک اتصال را بین خود به اشتراک گذارند. این اتصال، نشست یا جلسه نام دارد و طی آن کاربران قادر خواهند بود با یکدیگر ارتباط برقرار نمایند. علاوه بر این، در این لایه اقدامات همگام‌سازی نیز انجام می‌گیرد بنابراین در زمان وقوع یک شکست در ارسال داده‌ها، می‌توان ادامه فرایند ارسال را از سرگیری نمود. در لایه Session، گفتگوی میان دو پردازش نیز کنترل و مدیریت می‌شود، یعنی این لایه مشخص می‌کند که طی یک ارتباط کدام پردازش می‌تواند عمل ارسال و کدامیک می‌تواند عمل دریافت داده‌ها را انجام دهد (با این کار از انجام همزمان یک عمل بحرانی توسط دو طرف جلوگیری می‌شود). در شکل زیر، موقعیت این لایه در مدل OSI نشان داده شده است.

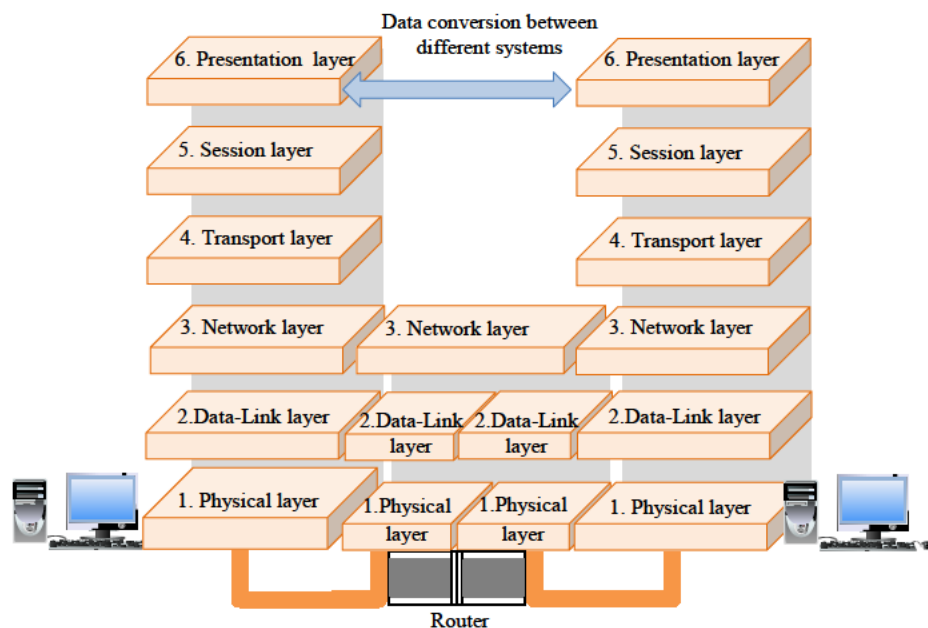


شکل ۱-۶

### ۱-۱-۷ لایه Presentation

لایه نمایش وظیفه ترجمه داده‌ها و کدگذاری آنها در فرمت‌های مختلف را برعهده دارد. در واقع چون فرمت داده‌های مورد استفاده توسط برنامه‌های کاربردی با فرمتی که توسط شبکه پذیرفته می‌شود متفاوت است، نیاز به راهکارهایی جهت یکسان‌سازی زبان گفتگو می‌باشد. این دقیقاً همان کاری است که در لایه Presentation انجام می‌شود. در این لایه اقداماتی مانند ترجمه داده‌ها، فشرده‌سازی، کدگذاری، تبدیل کاراکترها، و تفسیر و ترجمه دستورات گرافیکی انجام می‌پذیرد. به عنوان مثال، دو

فرمت برای نمایش تصاویر، فرمت‌های JPEG، MPEG می‌باشد. برای اینکه بتوان تصاویر را با این فرمت‌ها مشاهده نمود، ابتدا باید در مبدأ اقداماتی مانند کدگذاری، فشرده‌سازی و یا هر عملی که برای تفسیر شدن توسط مقصد نیاز باشد انجام شده، و پس از اینکه داده‌های انتقال یافته توسط مقصد دریافت شد مجدداً اقداماتی برای کدگشایی و تفسیر این داده‌ها صورت گیرد تا بتوان تصویر را به همان صورت اولیه مشاهده نمود.



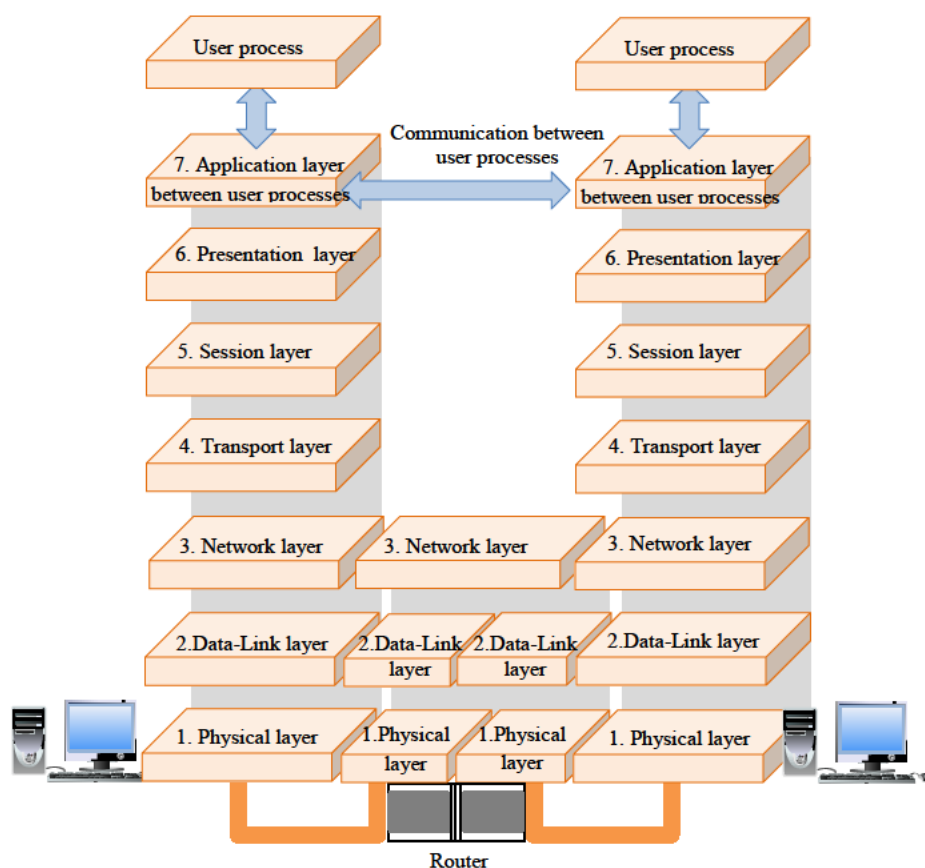
شکل ۷-۱

### ۸-۱-۱ لایه Application

لایه Application (کاربرد) بالاترین لایه در مدل OSI می‌باشد که کلیه برنامه‌های کاربردی تحت شبکه، مانند مرورگرهای وب، برنامه‌های انتقال فایل، برنامه‌های دسترسی به پایگاه داده و ... در آن بکار گرفته می‌شوند. در واقع این لایه محل قرارگیری واسطه‌های گرافیکی کاربر (GUI) می‌باشد و به برنامه‌های کاربردی اجازه می‌دهد که در محیط شبکه با یکدیگر ارتباط برقرار نمایند، مانند زمانی که همه آنها بر روی یک کامپیوتر قرار دارند.

یک برنامه پس از ایجاد شدن، تنها توسط این لایه قادر خواهد بود در محیط شبکه اجرا شود. به عنوان مثال زمانی که کاربر در برنامه Internet Explorer درخواستی جهت دسترسی به فایل‌ها یا

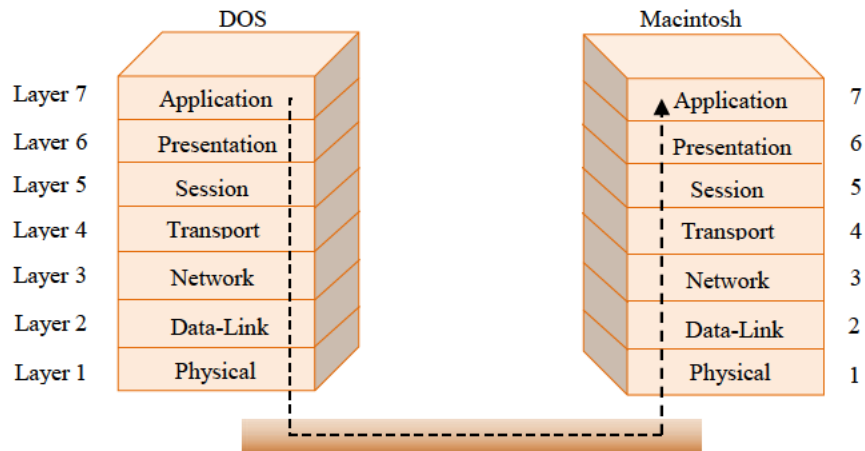
صفحات وب ارائه می‌دهد، این درخواست از موقعیت فعلی (لایه Application) به پشته پروتکل وارد شده و پس از عبور از کلیه لایه‌ها و پردازش توسط پاسخ دهنده، مجدداً در همین لایه و توسط برنامه Internet Explorer به کاربر تحویل داده می‌شود. پروتکل‌هایی مانند FTP، HTTP و SMTP در این لایه به کار گرفته می‌شوند. در شکل زیر، ارتباط و موقعیت هفت لایه در مدل OSI نشان داده شده است.



شکل ۸-۱

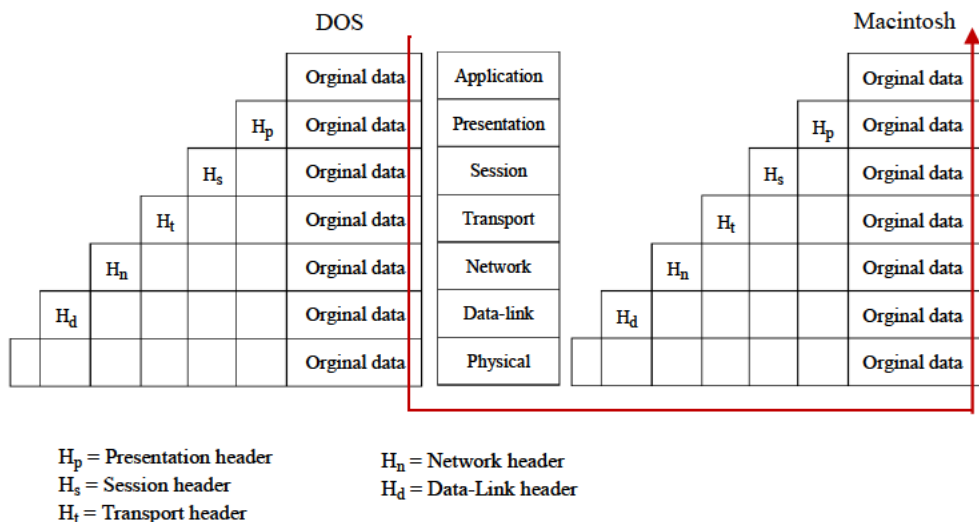
### ۹-۱-۱ ارتباط میان پشته‌ها در مدل OSI

زمانی که یک پیغام از ماشینی به ماشین دیگر فرستاده می‌شود، این پیغام در پشته فرستنده از لایه هفت به سمت لایه یک حرکت می‌کند تا به ماشین گیرنده تحویل داده شود. پس از تحویل به پشته گیرنده، مسیر حرکت عکس می‌شود، یعنی از لایه یک به سمت لایه هفت حرکت می‌نماید. در شکل ۹-۱ مسیر این حرکت نشان داده شده است.



شکل ۹-۱

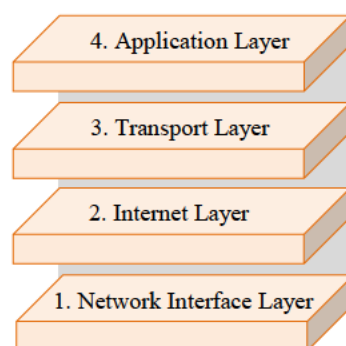
با عبور پیغام از هر لایه بجز لایه فیزیکی، یک سرایند به آن اضافه می‌گردد. این سرایند شامل اطلاعاتی کنترلی است که توسط لایه‌های متناظر در طرف دیگر خوانده شده و مورد پردازش قرار می‌گیرد. هنگامی که پیغام به سمت لایه‌های بالایی در ماشین مقصد حرکت می‌کند، هر لایه اطلاعات این سرایند را جهت آگاهی از محتویات آن مورد بررسی قرار داده و سپس سرایند را از پیغام حذف می‌نماید. در شکل زیر نحوه انجام این کار نشان داده شده است.



شکل ۱۰-۱

## ۲-۱-۲ آشنایی با مدل TCP/IP

TCP/IP<sup>۱</sup> مهمترین پروتکل بکار رفته در شبکه‌های مبتنی بر ویندوز می‌باشد که اولین بار توسط آژانس پروژه‌های تحقیقاتی وزارت دفاع آمریکا<sup>۲</sup> و در سال ۱۹۶۹ توسعه یافت. این پروتکل، از دو مجموعه پروتکل به نام‌های پروتکل کنترل انتقال (TCP) و پروتکل اینترنت (IP) تشکیل شده و قادر است میان سیستم‌های مختلف (مانند ویندوز، لینوکس و ...) در شبکه ارتباط برقرار نماید. بنابراین به عنوان یکی از مهمترین پروتکل‌ها در شبکه‌های کامپیوتری و مخصوصاً شبکه اینترنت مورد استفاده قرار می‌گیرد. این پروتکل‌ها در یک مدل چهار لایه‌ای همانند زیر قرار گرفته‌اند.



شکل ۱-۱۱

## ۱-۲-۱ جزئیات مدل TCP/IP

چهار لایه مدل TCP/IP به شرح زیر می‌باشند:

### لایه Application

این لایه، در واقع معادل با سه لایه Application، Presentation و Session در مدل OSI بوده و محل قرارگیری برنامه‌های کاربری می‌باشد. پروتکل‌هایی مانند انتقال فایل<sup>۳</sup> (FTP)، انتقال فایل جزئی<sup>۴</sup> (TFTP)، انتقال ساده پست الکترونیکی<sup>۵</sup> (SMTP)، انتقال ابر متن<sup>۶</sup> (HTTP)، پروتکل اداره پست<sup>۷</sup> (POP) و ... در این لایه به کار برده می‌شوند.

1. Transmission Control Protocol/Internet Protocol
2. Department of Defense's Advanced Research Projects Agency
3. File Transfer Protocol
4. Trivial File Transfer Protocol
5. Simple Mail Transfer Protocol
6. Hyper Text Transfer Protocol
7. Post Office Protocol

### لایه Transport

این لایه مسئول ارسال صحیح، به ترتیب و بدون گم شدن بسته‌ها در شبکه، و همچنین شکستن آنها به قطعات کوچکتر (در صورت نیاز) می‌باشد. در این لایه، دو پروتکل لایه انتقال یعنی TCP و UDP قرار گرفته‌اند.

TCP یک پروتکل اتصالگرا بوده و انتقال صحیح داده‌ها را تضمین می‌کند. UDP<sup>۱</sup>، پروتکلی بدون اتصال است که برای انتقال سریع پیام‌ها مناسب بوده ولی امنیت انتقال را تضمین نمی‌کند.

### لایه Internet

این لایه مسئول اتصال شبکه‌ها به یکدیگر و انجام اعمالی مانند مسیریابی بسته‌ها می‌باشد. در این لایه پروتکل‌هایی مانند پروتکل اینترنت (IP)، امنیت IP<sup>۲</sup> (IPsec)، پروتکل تحلیل آدرس<sup>۳</sup> (ARP)، پروتکل کنترل پیام‌های اینترنتی<sup>۴</sup> (ICMP)، پروتکل پیام‌های گروهی اینترنتی<sup>۵</sup> (IGMP) و ... قرار گرفته‌اند.

### لایه Network Interface

این لایه ترکیب دو لایه Data Link و Physical در مدل OSI بوده و وظیفه کدگذاری و ارسال داده‌ها بر روی رسانه ارتباطی میان دو دستگاه در شبکه را برعهده دارد. استانداردهایی مانند Ethernet و Token Ring در این لایه قرار دارند. این لایه با نام “لایه دسترسی شبکه”<sup>۶</sup> نیز شناخته می‌شود.

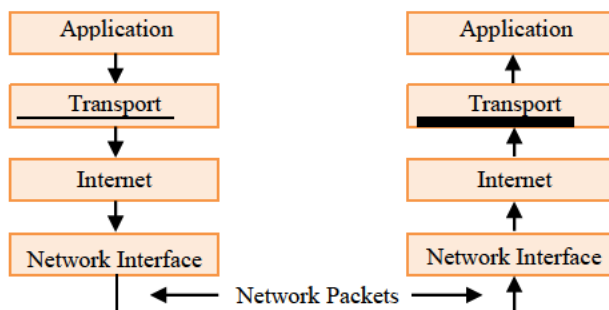
## ۱-۲-۲ برقراری ارتباط میان لایه‌های TCP/IP

برقراری ارتباط میان لایه‌ها در مدل TCP/IP مشابه مدل OSI می‌باشد. زمانی که یک کاربر از طریق برنامه‌های کاربردی مانند انتقال فایل (FTP) یا Email در لایه کاربرد (Application) درخواست خود را وارد می‌نماید، این درخواست به ترتیب لایه‌ها را به طرف پایین طی نموده تا به لایه Network Interface برسد؛ سپس با دریافت درخواست در طرف دیگر، لایه‌ها از پایین به بالا طی شده و به لایه کاربرد از ماشین پاسخ‌دهنده تحویل داده می‌شود. پس از اینکه درخواست پاسخ داده شد، این پاسخ مجدداً لایه‌ها را در جهت مخالف طی نموده و به لایه کاربرد از فرستنده تحویل داده می‌شود. توجه داشته باشید که در صورت استفاده از پروتکل TCP در لایه انتقال، به ازای دریافت هر بسته یک پیغام تصدیق (ACK) به فرستنده ارسال می‌شود، اما چنانچه از پروتکل UDP استفاده شود، هیچ پیغام تصدیقی فرستاده نخواهد شد.

---

1. User Datagram Protocol  
2. Internet Protocol Security  
3. Address Resolution Protocol  
4. Internet Control Message Protocol  
5. Internet Group Message Protocol  
6. Network Access Layer





شکل ۱-۱۲

### ۳-۱ آشنایی با آدرس‌های IPv4

آشنایی با آدرس‌های IP یکی از نکات کلیدی در درک نحوه عملکرد پروتکل IP می‌باشد. آدرس IP یک شناسه عددی است که به هر دستگاه در شبکه‌های IP اختصاص داده می‌شود. این نوع از آدرس‌ها، در واقع آدرس‌های منطقی هستند که برای تشخیص محل قرارگیری دستگاه‌ها به کار برده می‌شوند و با آدرس‌های فیزیکی (MAC Address) که به کارت واسط شبکه (NIC) اختصاص داده می‌شوند متفاوت هستند.



در این فصل، فرض بر این است که شما با نشانه‌گذاری اعداد در مبنای ۲ و نحوه تبدیل مبنای آشنا هستید. بنابراین تا حد امکان از ذکر جزئیات مربوط به تبدیل مبنای خودداری شده است.

### ۱-۳-۱ معرفی آدرس IPv4

یک آدرس IPv4 از ۳۲ بیت (۰ یا ۱) تشکیل شده است. این بیت‌ها به چهار قسمت (که Octet یا Quad نامیده می‌شود) تقسیم شده‌اند و هر قسمت حاوی یک بایت (۸ بیت) می‌باشد. سه روش رایج جهت نمایش یک آدرس IP وجود دارد:

- دهدهی<sup>۱</sup> (مبنای ده)، مانند 130.57.30.56
- دودویی<sup>۲</sup> (مبنای دو)، مانند 10000010.00111001.00011110.00111000
- شانزدهدهی<sup>۳</sup> (مبنای شانزده)، مانند 82 39 1E 38

همه مقادیری که در بالا مشاهده می‌نمایید، بیانگر آدرس IP یکسانی می‌باشند. با ۳۲ بیت موجود در آدرس‌های IPv4، مجموعاً تعداد  $2^{32} = 4,294,967,296$  آدرس از این نوع قابل ایجاد می‌باشد.

1. Decimal  
2. Binary  
3. Hexadecimal

### ۱-۳-۲ ساختار آدرس IP

بطور کلی آدرس‌های IP از دو شناسه تشکیل شده‌اند. یکی شناسه شبکه (NetworkID) و دیگری شناسه میزبان (HostID). هر کدام از این شناسه‌ها بسته به نوع کلاس آدرس IP تعیین می‌شوند.

#### شناسه شبکه

این شناسه، آدرس یک زیرشبکه را تعیین نموده و برای کلیه میزبان‌هایی که در یک زیرشبکه قرار دارند یکسان می‌باشد. شناسه شبکه در واقع یک ساختار سلسله مراتبی یا لایه‌ای به آدرس‌های شبکه می‌دهد. به عنوان مثال آدرس 130.57.30.56 را در نظر بگیرید. این آدرس از کلاس B بوده و دو قسمت اول آن به عنوان شناسه شبکه در نظر گرفته می‌شود، بنابراین کلیه کاربرانی که در زیرشبکه‌ای با این آدرس قرار داشته باشند دو قسمت اول آدرس IP آنها با 130.57 شروع می‌شود.

#### شناسه میزبان

آدرس یک دستگاه یا میزبان در شبکه است و برای هر میزبان عددی منحصر بفرد می‌باشد. در مثال قبل، دو قسمت دوم از آدرس متعلق به شناسه میزبان می‌باشد، بنابراین در آدرس‌هایی مانند 130.57.30.56، آدرس 30.56 بیانگر شناسه میزبان زیرشبکه‌ای با آدرس 130.57 می‌باشد.

### ۱-۳-۳ کلاس‌های آدرس IP

بطور کلی سه کلاس آدرس‌دهی قابل اختصاص به کاربران توسط طراحان اینترنت به کار گرفته شده است. این کلاس‌ها با نام‌های A، B و C شناخته می‌شوند. برای شبکه‌های خیلی بزرگ که متشکل از چندین زیرشبکه می‌باشند از کلاس A، و برای شبکه‌های بسیار کوچک از کلاس C استفاده می‌شود. شبکه‌های متوسط نیز از کلاس B جهت آدرس‌دهی به کاربران خود استفاده می‌نمایند. تقسیم‌بندی آدرس‌های IP به آدرس‌های شبکه و آدرس‌های میزبان (NetID و HostID) نیز بر اساس همین کلاس‌بندی‌ها انجام می‌شود. در جدول ۱-۱ خلاصه‌ای از مشخصات این سه کلاس آورده شده است.

جدول ۱-۱: خلاصه‌ای از مشخصات کلاس‌های A، B و C

کلاس	بیت‌های قاب زیر شبکه	الگوی بیتی راهنما	مقدار اولین اُکتت <sup>۱</sup> در آدرس	تعداد شبکه‌های قابل اختصاص	حداکثر میزبان‌ها در هر شبکه
A	8	0	1-126	126	16,777,214
B	16	01	128-191	16,384	65,534
C	24	110	192-223	2,097,152	254

1. Octet

همانطور که در جدول مشاهده می‌کنید، ستونی جهت نشان دادن الگوی بیت‌های راهنما برای هر کلاس در نظر گرفته شده است. این بیت‌ها در واقع بیت‌های شروع آدرس‌های هر کلاس را نشان می‌دهند. به عنوان مثال، آدرس  $126.x \times x$  را در کلاس A در نظر بگیرید. قسمت اول این آدرس عدد 126 است که معادل دودویی آن 01111110 می‌باشد، بنابراین در ستون مربوطه، الگوی شروع این آدرس‌ها با 0 نشان داده شده است. در کلاس‌های B و C نیز اکتت اول کلیه آدرس‌ها به ترتیب با الگوی 01 و 110 آغاز می‌شوند و با تغییر آدرس‌ها در هر کلاس، به غیر از بیت‌های ذکر شده، سایر بیت‌ها تغییر می‌کنند. استفاده از این الگوهای بیتی در مسیریاب‌ها بسیار پرکاربرد می‌باشد زیرا این دستگاه‌ها می‌توانند با خواندن قسمت اول این آدرس‌ها الگوی بیتی آنها را بدون نیاز به دانستن سایر بیت‌ها تشخیص داده و از کلاس آن آدرس و همچنین قاب زیرشبکه<sup>۱</sup> آن آگاهی یابند.

بعضی از آدرس‌های IP برای کاربردهای خاصی در نظر گرفته شده‌اند و قابل اختصاص به کاربران شبکه نمی‌باشند (البته به غیر از آدرس‌های خصوصی). در جدول ۱-۲ این آدرس‌ها به همراه کاربر آنها آورده شده است.

جدول ۱-۲: آدرس‌های IP با کاربردهای خاص

آدرس	کاربرد
آدرس 0.0.0.0	بسته به قاب زیرشبکه، بیانگر همین شبکه (شبکه یا زیرشبکه‌ای که در حال حاضر در آن قرار دارید) یا همین میزبان می‌باشد.
آدرس‌هایی که با 127 شروع می‌شوند	این آدرس‌ها برای تست‌های loopback استفاده می‌شوند و به یک میزبان اجازه می‌دهند تا پیغام‌های تست را بدون اینکه ترافیکی در شبکه ایجاد کند، برای خود ارسال نماید.
آدرس 255.255.255.255	این آدرس برای ارسال پیغام‌ها به تمام کاربران شبکه (Multicasting) استفاده می‌شود و با نام‌های limited broadcast و all-Is broadcast نیز شناخته می‌شود.
آدرس‌های 10.0.0.0 تا 10.255.255.255، 172.16.0.0 تا 172.31.255.255، 192.168.0.0 تا 192.168.255.255	این آدرس‌ها به عنوان آدرس‌های خصوصی/نامعتبر <sup>۲</sup> برای کلاس‌های A، B و C در نظر گرفته شده‌اند. آدرس‌های خصوصی در استاندارد RFC 1918 تعریف شده و قابل استفاده در اینترنت نمی‌باشند. از این آدرس‌ها در سرورهای NAT و شبکه‌های IP غیرمتصل به اینترنت (شبکه‌های داخلی یا همان شبکه‌های خصوصی) استفاده می‌شود.

1. Subnet mask  
2. Private/Invalid

این آدرس‌ها فقط در ارتباطات نقطه به نقطه میان دستگاه‌ها در یک شبکه به کار رفته و از قابلیت ارسال پیغام‌ها توسط مسیریاب برخوردار نمی‌باشند. به این آدرس‌ها، آدرس‌های APIPA <sup>۱</sup> گفته می‌شود.	آدرس‌های 169.254.0.0 با قاب زیر شبکه 255.255.0.0
---	---

در ادامه، آدرس‌های هر سه کلاس را به همراه شناسه‌های آنها برای شبکه و میزبان‌ها مورد بررسی قرار خواهیم داد.

### کلاس A

در کلاس A بایت اول (۸ بیت اول از سمت چپ) برای آدرس شبکه و سه بایت باقیمانده برای آدرس میزبان استفاده می‌شود و فرمت آدرس‌های این کلاس به صورت Network.Host.Host.Host می‌باشد. به عنوان مثال در آدرس 49.22.102.70 عدد 49 آدرس شبکه و 22.102.70 آدرس میزبان را نشان می‌دهند. در این مثال، هر دستگاه در شبکه دارای یک آدرس متمایز به همراه آدرس شبکه 49 می‌باشد.

در کلاس A می‌توان از ۱۲۶ زیر شبکه استفاده نمود. علت این است که آدرس شبکه در این کلاس یک بایت است و اولین بیت از آن (با صفر) رزرو شده است، بنابراین هفت بیت باقیمانده در این بایت قابل استفاده می‌باشند. این بدین معناست که بیت‌های تشکیل دهنده این کلاس حداکثر می‌توانند دارای مقدار ۱۲۸ باشند (هر کدام از این هفت بیت می‌توانند مقدار ۰ یا ۱ را اختیار کنند که در مجموع  $2^7$  یا ۱۲۸ موقعیت را فراهم می‌نمایند)، البته آدرس‌هایی که با ۰۰۰۰۰۰۰۰ (بایت اول با بیت‌های صفر) و ۰۱۱۱۱۱۱۱ (معادل با ۱۲۷ که آدرس‌های Loopback می‌باشند) شروع می‌شوند، رزرو شده هستند. بنابراین از ۱۲۸ موقعیت، دو موقعیت رزرو شده و در نهایت  $126 = 128 - 2$  موقعیت در دسترس است، پس تعداد زیر شبکه‌های قابل آدرس‌دهی در کلاس A برابر با ۱۲۶ می‌باشند.

در این کلاس سه بایت آخر آدرس (۲۴ بیت آخر) متعلق به آدرس میزبان می‌باشد، به این معنا که  $2^{24} = 16,777,216$  ترکیب متمایز از این ۲۴ بیت وجود دارد. چون آدرس‌های ۰.۰.۰.۰ و 255.255.255 رزرو شده هستند در نهایت تعداد  $16,777,214 = 2^{24} - 2$  آدرس قابل اختصاص به میزبان‌ها در کلاس A موجود می‌باشد.

### کلاس B

در کلاس B، دو بایت اول به عنوان آدرس شبکه و دو بایت باقیمانده به عنوان آدرس میزبان در نظر گرفته می‌شوند. فرمت آدرس‌های این کلاس به صورت Network.Network.Host.Host می‌باشد. به عنوان مثال در آدرس 130.57.30.56، آدرس شبکه برابر با 130.57 و آدرس میزبان نیز 30.56 می‌باشد.

1. Automatic Private IP Addressing

تعداد بیت‌های آدرس شبکه در کلاس A برابر ۱۶ بیت می‌باشد، بنابراین تعداد  $2^{16} = 65,536$  ترکیب متمایز از بیت‌ها وجود دارد. اما با توجه به نظر طراحان اینترنت مبنی بر اینکه آدرس‌های این کلاس باید با بیت‌های 01 شروع شوند، در نهایت ۱۴ بیت قابل استفاده است. بنابراین تعداد زیرشبکه‌ها در این کلاس برابر با  $2^{14} = 16,384$  می‌باشد.

در کلاس B دو بایت آخر به عنوان آدرس میزبان در نظر گرفته می‌شود، این دو بایت نیز از ۱۶ بیت تشکیل شده‌اند، بنابراین  $2^{16} = 65,536$  ترکیب متمایز برای آنها وجود دارد. چون آدرس‌های 0.0.255.255 (آدرس‌هایی که دو قسمت آخر آنها به شکل مذکور می‌باشد) رزرو شده هستند، تعداد میزبان‌های قابل آدرس‌دهی در این کلاس برابر با  $2^{16} - 2 = 65,534$  خواهد بود.

### کلاس C

در کلاس C سه بایت اول به عنوان آدرس شبکه و یک بایت باقیمانده به عنوان آدرس میزبان در نظر گرفته می‌شود. فرمت آدرس‌ها در این کلاس به صورت Network.Network.Network.Host می‌باشد. به عنوان مثال در آدرس 198.21.74.102، آدرس شبکه 198.21.74 و آدرس میزبان 102 می‌باشد.

آدرس‌های کلاس C با سه بیت 110 آغاز می‌شوند، بنابراین از ۲۴ بیتی که تشکیل‌دهنده آدرس شبکه در این کلاس هستند، ۳ بیت کسر شده و در نهایت تعداد ۲۱ بیت (قابل دستکاری) باقی می‌ماند. پس تعداد  $2^{21} = 2,097,152$  زیرشبکه در کلاس C قابل ایجاد می‌باشد. الگوی بیتی 110 نشان دهنده عدد ۱۹۲ (11000000) بوده و با دستکاری سایر بیت‌ها تا عدد ۲۲۳ (11011101) نیز قابل مقداردهی می‌باشد، بنابراین روشی ساده برای تشخیص آدرس‌های کلاس C این است که اکتت اول با اعداد بین ۱۹۲ تا ۲۲۳ شروع شده باشد صرفنظر از اینکه اکتت‌های دوم و سوم دارای چه مقادیری باشند.

در کلاس C بایت آخر به عنوان آدرس میزبان در نظر گرفته می‌شود. پس با داشتن ۸ بیت تعداد  $2^8 = 256$  آدرس متمایز وجود خواهد داشت. چون دو آدرس 0 و 255 رزرو شده هستند در نهایت تعداد ۲۵۴ آدرس قابل اختصاص به میزبان‌ها در کلاس C قابل دسترسی می‌باشد.



دو کلاس دیگر از آدرس‌های IP، کلاس‌های D و E هستند. آدرس‌های کلاس D به آدرس‌های Multicast یا چندپخش معروف هستند و برای موارد Multicasting یا ارسال پیغام‌ها به صورت همزمان به بیش از یک کاربر (چندپخشی) در شبکه استفاده می‌شوند. دامنه این آدرس‌ها از 224.0.0.0 تا 239.255.255.255 می‌باشد. آدرس‌های کلاس E نیز جهت استفاده در آینده رزرو شده‌اند و دامنه آنها از 240.0.0.0 تا 255.255.255.255 می‌باشد. آدرس‌های این کلاس جهت موارد آزمایشی مورد استفاده قرار می‌گیرد.

## ۴-۱ انجام سابنتینگ<sup>۱</sup> در شبکه

زمانی که در یک سازمان بزرگ با تعداد زیادی از کامپیوترها سروکار دارید و یا این کامپیوترها از لحاظ جغرافیایی جدا از یکدیگر قرار دارند، می‌توان شبکه را به چندین شبکه کوچکتر تقسیم کرده و آنها را از طریق مسیریاب‌ها به یکدیگر متصل نمود. به هر کدام از این شبکه‌های کوچکتر یک زیرشبکه<sup>۲</sup> گفته می‌شود. استفاده از زیرشبکه‌ها دارای مزایایی است که در ادامه آنها را بر می‌شماریم:

- ♦ کاهش ترافیک شبکه: زمانی که تعداد کامپیوترها در شبکه زیاد است، ارسال بسته‌ها به داخل شبکه می‌تواند موجب ایجاد ترافیک و در نتیجه مسدود شدن شبکه گردد. با استفاده از زیرشبکه و مسیریاب‌ها، بیشتر ترافیک در داخل هر زیرشبکه باقی مانده و بسته‌ها از طریق مسیریاب به سایر زیرشبکه‌ها ارسال می‌شوند. بنابراین با کاهش ترافیک، کارایی شبکه افزایش می‌یابد.
- ♦ مدیریت آسان: زمانی که بجای یک شبکه بسیار بزرگ، با تعدادی زیرشبکه کوچکتر مواجه باشید، مدیریت هر یک از این زیرشبکه‌های کوچک، بسیار ساده‌تر از مدیریت کل شبکه خواهد بود.

کلیه زیرشبکه‌ها در یک سازمان، دارای آدرس شبکه مشترکی می‌باشند که جهت شناسایی شبکه در این سازمان به کار می‌رود. اما علاوه بر آدرس شبکه، هر زیرشبکه باید دارای شماره‌ای باشد که بتوان آنرا از سایر زیرشبکه‌ها تشخیص داد. این شماره، آدرس زیرشبکه نامیده می‌شود.

استفاده از سابنتینگ و زیرشبکه‌ها، چندین مشکل را در انجام آدرس‌دهی به میزبان‌ها برطرف می‌کند:

- ♦ اگر یک سازمان فقط دارای یک آدرس IP باشد ولی به چندین زیرشبکه فیزیکی نیاز داشته باشد، می‌توان با استفاده از سابنتینگ و تقسیم این آدرس به چندین زیرشبکه، مشکل آدرس‌دهی در این سازمان را برطرف نمود.
- ♦ چون سابنتینگ اجازه می‌دهد که تعداد زیادی از شبکه‌ها با یکدیگر تشکیل گروه دهند، در مسیریاب‌ها جداول کوچکتری جهت نگهداری اطلاعات مسیریابی این زیرشبکه‌ها نیاز است و این مسئله باعث کاهش سربار شبکه می‌گردد.
- ♦ در مجموع، موارد ذکرشده در بالا عملکرد مناسب‌تری برای شبکه فراهم می‌نمایند.

طراحان پروتکل IP، در ابتدا یک شبکه اینترنت کوچک متشکل از ده‌ها شبکه و هزاران میزبان را پیش‌بینی می‌کردند. بنابراین در طرح آدرس‌دهی آنها برای هر زیرشبکه فیزیکی یک آدرس شبکه

1. Subnetting

2. Subnet

استفاده می‌شد. اما رشد پیش‌بینی نشده اینترنت، تعداد زیادی از مشکلات را برای مسئولین و طراحان اینترنت ایجاد نمود که در ادامه دو مورد از آنها آورده شده است:

- ♦ کمبود آدرس‌ها: زمانی که یک سازمان قصد داشت از چندین شبکه فیزیکی استفاده کند، باید برای هر کدام از آنها یک آدرس شبکه درخواست می‌کرد. بنابراین با افزایش تعداد شبکه‌ها دیگر آدرسی جهت اختصاص به آنها وجود نخواهد داشت.
- ♦ جداول مسیریابی بزرگ: اگر هر مسیریاب در اینترنت نیازمند نگهداری اطلاعات مسیریابی هر شبکه فیزیکی باشد، جدول مسیریابی آن بطور غیر ممکن افزایش خواهد یافت. این مسئله باعث ایجاد حجم طاقت فرسایی از سربار مدیریتی جهت نگهداری این جداول شده و در نتیجه سربار فیزیکی (مثل سربار CPU، فضای دیسک، حافظه و ...) برای این مسیریاب‌ها به دنبال خواهد داشت. حال چون هر مسیریاب اطلاعات مسیریابی خود را با سایر مسیریاب‌ها تبادل می‌کند، ترافیک شبکه را افزایش داده و در نتیجه موجب کاهش عملکرد شبکه می‌گردد.

یکی از راهکارهایی که جهت برخورد با این مشکلات استفاده می‌شود و در این کتاب نیز مورد بررسی قرار می‌گیرد استفاده از سابنتینگ می‌باشد. در واقع به کمک سابنتینگ می‌توان یک شبکه IP را بطور منطقی به زیرشبکه‌هایی تقسیم نمود. در قسمت بعد نحوه انجام این کار را شرح خواهیم داد.

#### ۱-۴-۱ پیاده‌سازی سابنتینگ

قبل از اقدام به اجرای سابنتینگ در یک شبکه، باید نیازمندی‌های این کار و همچنین طرحی مناسب برای پیاده‌سازی آن مشخص نمایید. در ادامه این موارد را مورد بررسی قرار می‌دهیم.

#### تعیین نیازمندی‌های سابنتینگ

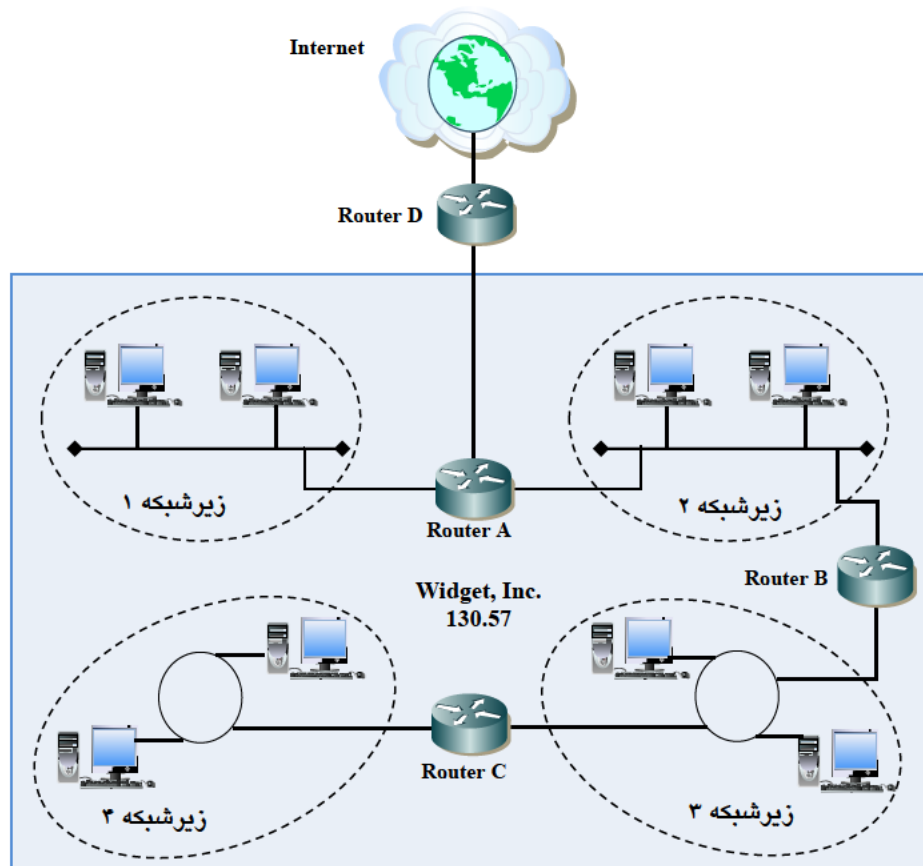
جهت تعیین نیازمندی‌های سابنتینگ، رهنمودهای زیر را دنبال کنید:

۱. شناسه شبکه (قاب زیرشبکه) را تعیین کنید. این شناسه با توجه به کلاسی که از آن استفاده می‌کنید مشخص می‌شود و برای همه میزبان‌ها مشترک خواهد بود.
۲. برای هر قسمت از شبکه (که به عنوان یک زیرشبکه در نظر گرفته می‌شود) شناسه‌ای متمایز مشخص کنید.
۳. به هر زیرشبکه ایجاد شده محدوده‌ای از شناسه‌ها را جهت شناسایی دستگاه‌های TCP/IP (شامل کامپیوترها، پرینترهای تحت شبکه و ...) اختصاص دهید.

#### نحوه پیاده‌سازی سابنتینگ

جهت پیاده‌سازی سابنتینگ باید به همه ماشین‌ها در یک زیرشبکه فیزیکی، آدرس زیرشبکه

یکسانی اختصاص داده شود. به عنوان مثال در شکل زیر کلیه ماشین‌هایی که در زیرشبکه ۱ قرار دارند، باید دارای آدرس زیرشبکه ۱ باشند.



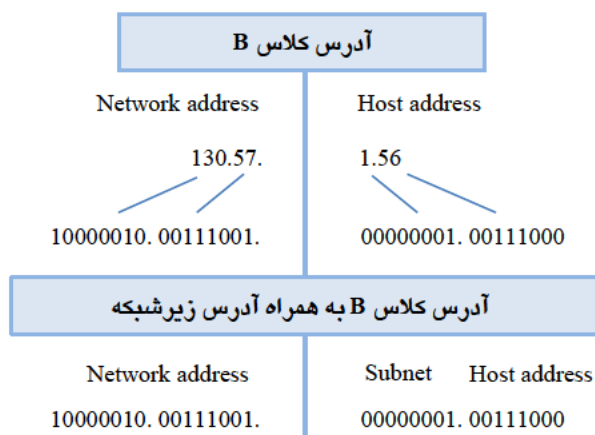
شکل ۱-۱۳

در هنگام پیاده‌سازی سابنتینگ، با توجه به کلاسی که جهت آدرس‌دهی انتخاب می‌شود، بخش شبکه از آدرس IP برای ماشین‌های موجود در همه زیرشبکه‌ها ثابت است. بنابراین نمی‌توان برای یک میزبان در این زیرشبکه‌ها آدرس شبکه را تغییر داد، مگر اینکه این آدرس برای همه میزبان‌ها تغییر کند (یا به عبارتی از آدرس دیگری استفاده شود). استفاده از آدرس شبکه یکسان موجب بهره‌مندی از حداکثر فضای آدرس‌دهی می‌گردد. همانطور که در شکل ۱-۱۳ مشاهده می‌کنید، همه میزبان‌های شرکت Widget دارای آدرس شبکه 130.57 می‌باشند بنابراین این آدرس برای همه آنها ثابت است. در واقع، طرح سابنتینگ به این صورت است که چون آدرس شبکه جهت شناسایی کل شبکه در یک



سازمان استفاده می‌شود بدون تغییر باقی می‌ماند اما با قرض‌گرفتن بیت‌های آدرس میزبان و در نتیجه ایجاد تغییر در بخش میزبان از آدرس، می‌توان زیرشبکه‌ها را ایجاد نموده و موقعیت قرارگیری میزبان‌ها در هر زیرشبکه را تعیین نمود.

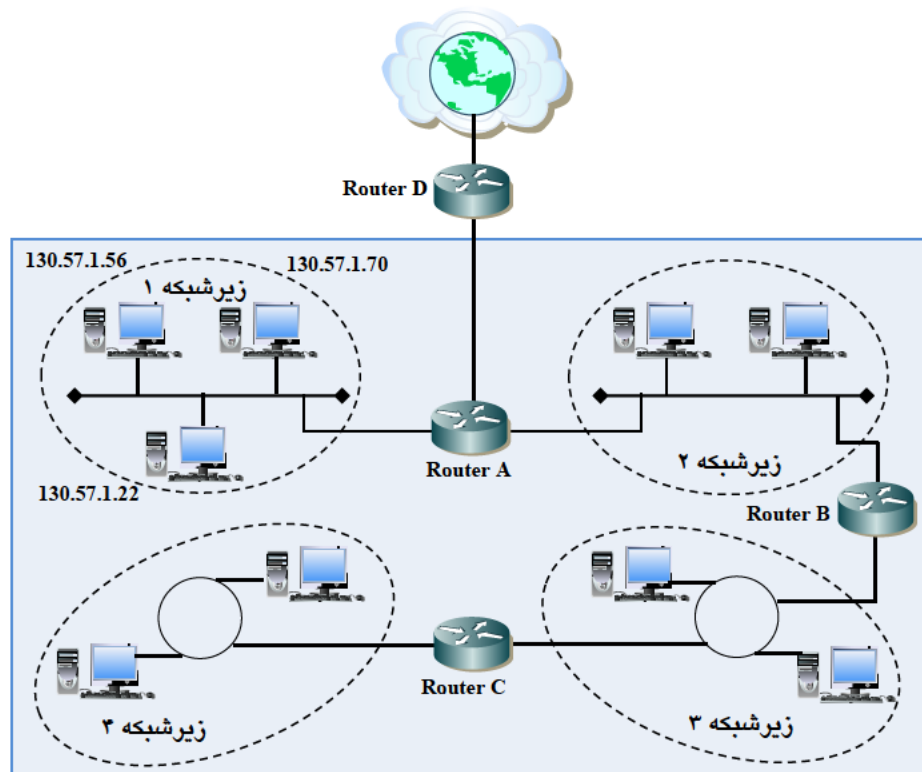
در مثال بالا چون آدرس شبکه در شرکت Widget از کلاس B می‌باشد، دو بایت اول آدرس در همه ماشین‌ها صرف‌نظر از اینکه در چه زیرشبکه‌ای قرار دارند یکسان است. در اینجا بایت سوم از آدرس هر ماشین به آدرس زیرشبکه اختصاص داده می‌شود. به عنوان مثال مقدار بایت سوم در زیرشبکه ۱ دارای مقدار 00000001 می‌باشد. در این آدرس‌ها، مقدار چهارمین بایت (به همراه مقدار سومین بایت که تعیین‌کننده محل قرارگیری میزبان‌ها در هر زیرشبکه می‌باشد) برای هر میزبان باید منحصر بفرد باشد. در شکل زیر، نحوه استفاده آدرس شبکه و آدرس میزبان با یکدیگر نشان داده شده است.



شکل ۱-۱۳

### نحوه استفاده از قاب زیرشبکه

به منظور عملکرد صحیح طرح آدرس زیرشبکه، هر ماشین باید از وضعیت بیت‌های شبکه، زیرشبکه و میزبان‌ها آگاه باشد. این کار با اختصاص قاب زیرشبکه به هر میزبان امکان‌پذیر است. در این مثال، مدیر شبکه یک قاب زیرشبکه ۳۲ بیتی متشکل از بیت‌های ۰ و ۱ ایجاد می‌نماید. دنباله بیت‌های ۱ در قاب زیرشبکه، بیانگر آدرس شبکه و زیرشبکه در آدرس IP می‌باشند. بیت‌های صفر نیز آدرس میزبان را مشخص می‌نمایند. در شکل‌های ۱-۱۵ و ۱-۱۶ مثالی (از کلاس B) در این رابطه آورده شده است.



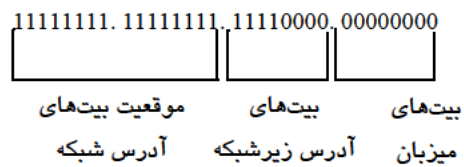
شکل ۱-۱۵

### وضعیت بیت‌ها

1ها: موقعیت‌هایی است که آدرس شبکه یا زیر شبکه را نشان می‌دهند.

0ها: موقعیت‌هایی است که آدرس میزبان را نشان می‌دهند.

### قاب زیر شبکه برای شرکت Widget



شکل ۱-۱۶

در مثال بالا دو بایت اول قاب زیر شبکه با بیت‌های ۱ مقداردهی شده است زیرا آدرس این شبکه

از نوع کلاس B بوده که دارای فرمت Network.Network.Host.Host می‌باشد. اگر بخاطر داشته باشید گفتیم جهت ایجاد زیرشبکه از بیت‌های میزبان استفاده می‌شود، بنابراین در اینجا بیت‌های موجود در بایت سوم به آدرس زیرشبکه اختصاص داده شده و با 11110000 که معادل شماره زیرشبکه ۲۲۰ می‌باشد مقداردهی شده است. در این مثال تنها چهارمین بایت به آدرس میزبان اختصاص داده شده است. توجه داشته باشید که ممکن است تعداد بیت‌های اختصاص داده شده به زیرشبکه و میزبان‌ها کمتر یا بیشتر از این مقدار باشد (مثلاً دو بیت، سه بیت و یا ...). در طول فصل با این موارد نیز آشنا خواهید شد.

قاب زیرشبکه را می‌توان با استفاده از معادل دهدهی (مبنای ده) بیت‌ها نیز نشان داد. الگوی دودویی 11110000 معادل عدد ۲۲۰ می‌باشد. بنابراین قاب زیرشبکه در مثال قبل می‌تواند به دو طریق زیر نشان داده شود:

قاب زیرشبکه بصورت دودویی: 11111111. 11111111. 11110000. 00000000  
قاب زیرشبکه بصورت دهدهی: 255 . 255 . 220 . 0

در همه زیرشبکه‌ها نیاز به استفاده از قاب‌های زیرشبکه سفارشی (قاب‌هایی که مقادیر اکتت‌های مربوط به زیرشبکه در آن عددی غیر از ۲۵۵ باشد) نمی‌باشد، بلکه می‌توان از همان مقادیر پیش‌فرض قاب زیرشبکه استفاده نمود. به عبارتی می‌توان در مورد این شبکه‌ها اینگونه تصور کرد که فاقد آدرس زیرشبکه می‌باشند. در جدول ۱-۳ مقادیر مختلف قاب زیرشبکه برای سه کلاس A، B و C (زمانی که هیچ تغییری در تعداد بیت‌های آن ایجاد نشده) آورده شده است.

جدول ۱-۳: قاب زیرشبکه برای سه کلاس A، B و C

کلاس	فرمت	قاب زیرشبکه پیش‌فرض
A	Network.Host.Host.Host	255.0.0.0
B	Network.Network.Host.Host	255.255.0.0
C	Network.Network. Network.Host	255.255.255.0

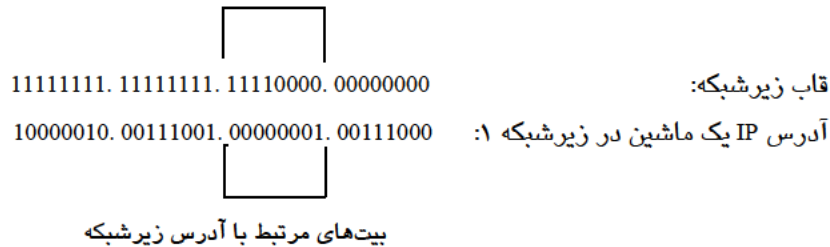
پس از ایجاد قاب زیرشبکه، آدرس IP باید از محل قرارگیری خود در زیرشبکه آگاه گردد. این کار با اعمال قاب زیرشبکه بر روی آدرس مورد نظر (توسط نرم افزار IP) انجام می‌شود. در واقع بیت‌هایی از آدرس IP که متناظر با بیت‌های تعیین‌کننده زیرشبکه در قاب زیرشبکه هستند، محل قرارگیری میزبان در زیرشبکه را مشخص می‌نمایند. برای روشنتر شدن این موضوع، در شکل ۱-۱۷ مثالی از آدرس IP و قاب زیرشبک آن آورده شده است.

## وضعیت بیت‌ها

1ها: موقعیت‌هایی است که آدرس شبکه یا زیرشبکه را نشان می‌دهند.

0ها: موقعیت‌هایی است که آدرس میزبان را نشان می‌دهند.

موقعیت‌های مرتبط با آدرس زیرشبکه



شکل ۱-۱۷

در این مثال، نرم افزار IP تشخیص می‌دهد که بایت سوم از قاب زیرشبکه به جای آدرس میزبان، برای آدرس زیرشبکه استفاده شده است. بنابراین به موقعیت بیت‌های متناظر با این بایت در آدرس IP که دارای مقدار 00000001 می‌باشد نگاه می‌کند.

در مرحله آخر نیز باید شماره زیرشبکه تعیین گردد. این کار با تبدیل مقادیر دودویی بایت سوم از آدرس IP به معادل دهدهی آن انجام می‌شود که در شکل زیر قابل مشاهده می‌باشد.

## تبدیل دودویی به معادل دهدهی آن

موقعیت/مقدار:	128	64	32	16	8	4	2	1
سومین بایت در مثال Widget:	0	0	0	0	0	0	0	1
معادل دهدهی:	$(128*0 + 64*0 + 32*0 + 16*0 + 8*0 + 4*0 + 2*0 + 1*1 = 1)$							1
آدرس زیر شبکه:								1

شکل ۱-۱۸

زمانی که در مواردی مانند مثال قبل، بایت سوم را به عنوان آدرس زیرشبکه قرار می‌دهید، به سادگی می‌توانید آدرس زیرشبکه برای میزبان‌ها را مشخص نمایید. به عنوان مثال اگر شرکت Widget قصد داشته باشد زیرشبکه‌ای با شماره ۶ داشته باشد، سومین بایت از همه ماشین‌ها در زیرشبکه برابر با مقدار 00000110 (معادل دودویی عدد ۶) خواهد بود. علاوه بر این، استفاده از همه

بیت‌های یک بایت جهت اختصاص به آدرس شبکه، تعداد نسبتاً مناسبی از آدرس‌های زیرشبکه را برای شما فراهم می‌نماید، زیرا این بایت تعداد ۸ موقعیت از بیت‌ها که هرکدام می‌تواند مقدار ۰ یا ۱ داشته باشد را در اختیار شما قرار می‌دهد؛ بنابراین طبق رابطه  $2^8 = 256$ ، تعداد ۲۵۶ زیرشبکه قابل اختصاص در این کلاس (B) موجود می‌باشد. پس در نهایت شرکت Widget می‌تواند مجموعاً ۲۵۶ زیرشبکه و هر کدام با ۲۵۴ میزبان در اختیار داشته باشد.

اگرچه استاندارد RFC 950 استفاده از آدرس‌های زیرشبکه که تمام بیت‌های آن ۰ و یا تماماً ۱ باشد را ممنوع کرده است ولی امروزه اکثر محصولات امکان استفاده از آنها را فراهم می‌نمایند که از جمله آنها می‌توان به پشته‌های TCP/IP در محصولات مایکروسافت و همچنین نرم افزار بیشتر مسیریاب‌ها اشاره نمود. به هر حال تا حصول اطمینان از اینکه نرم‌افزار شبکه شما این دو آدرس را به رسمیت می‌شناسد، نباید از آنها استفاده نمایید.

### محاسبه تعداد زیرشبکه‌ها

فرمول‌هایی که برای محاسبه حداکثر تعداد زیرشبکه‌ها و حداکثر تعداد میزبان‌ها در هر زیرشبکه استفاده می‌شوند بصورت زیر می‌باشد:

حداکثر تعداد زیرشبکه‌ها: (تعداد بیت‌های ماسک شده (۱) در قاب زیرشبکه)  $2^p$

حداکثر میزبان‌ها در هر زیرشبکه:  $2^q - 2$  (تعداد بیت‌های ماسک نشده ( ) در قاب زیرشبکه)  $2^q$

در فرمول‌های بالا، لفظ ماسک شده اشاره به بیت‌هایی با موقعیت ۱ و لفظ ماسک نشده نیز اشاره به بیت‌هایی با موقعیت ۰ دارند. هرچه تعداد بیت‌های صفر که به میزبان اختصاص داده می‌شود کمتر شود، تعداد آدرس‌های قابل ایجاد برای آنها نیز کاهش می‌یابد. به عنوان مثال در کلاس B زمانی که دو بایت به آدرس میزبان اختصاص داده می‌شود،  $2^{16} = 65,536$  آدرس میزبان را فراهم می‌نماید، اکنون چنانچه یک بایت به میزبان اختصاص داده شود، این تعداد آدرس به ۲۵۶ (با احتساب دو آدرس ۰ و ۲۵۵) کاهش پیدا می‌کند. در این صورت اگر در هر زیرشبکه به بیش از ۲۵۴ میزبان احتیاج داشته باشید، با مشکل روبرو خواهید شد. راه حلی که برای مقابله با این مشکل قابل استفاده می‌باشد، استفاده از تعداد بیت‌های کمتر (از یک بایت) برای آدرس زیرشبکه می‌باشد. البته این راه حل موجب کاهش تعداد زیرشبکه‌ها می‌شود ولی به دلیل نیاز به تعداد میزبان‌های بیشتر، چاره‌ای جز این نیست. مثالی که در ادامه آورده شده است، استفاده از تعداد بیت‌های کمتر از یک بایت را برای آدرس زیرشبکه نشان می‌دهد. در این مثال، شرکت Acme پیش‌بینی می‌کند که به ۱۴ زیرشبکه نیاز دارد. بنابراین با فرض گرفتن ۴ بیت از آدرس میزبان ( $2^4 = 16$ ) می‌تواند به این تعداد زیرشبکه دست یابد.

اکنون ۱۲ بیت برای استفاده در آدرس میزبان در اختیار دارد بنابراین در هر یک از این زیرشبکه‌ها می‌تواند تعداد  $2^{12} = 4096$  میزبان در اختیار داشته باشد که این تعداد برای یک زیرشبکه بسیار زیاد خواهد بود. در شکل زیر نحوه قرض گرفتن بیت‌ها و تعیین محل قرارگیری یک میزبان در زیرشبکه نشان داده شده است.

#### شرکت Acme

آدرس شبکه: 132.8 (کلاس B: Host.Host.Net)  
 آدرس IP نمونه: 10000100.00001000.00010010.00111100  
 معادل دهدهی: 132 . 8 . 18 . 60

#### وضعیت بیت‌ها

1ها: موقعیت‌هایی است که آدرس شبکه یا زیرشبکه را نشان می‌دهند.

0ها: موقعیت‌هایی است که آدرس میزبان را نشان می‌دهند.

#### قاب زیرشبکه

دودویی: 11111111.11111111.11110000.00000000  
 دهدهی: 255 . 255 . 240 . 0

#### موقعیت‌های مرتبط با آدرس زیرشبکه

قاب زیرشبکه: 11111111.11111111.11110000.00000000  
 آدرس IP ماشینی در Acme: 10000100.00001000.00010010.00111100

#### بیت‌های مرتبط با آدرس زیرشبکه

#### تبدیل دودویی به دهدهی برای آدرس زیرشبکه

موقعیت‌های قاب زیرشبکه: 1 1 1 1 0 0 0 0  
 موقعیت/مقدار: 128 64 32 16 8 4 2 1  
 سومین بایت از آدرس IP: 0 0 0 1 0 0 1 0  
 معادل دهدهی:  $(128*0 + 64*0 + 32*0 + 16*1 = 16)$  16

آدرس زیرشبکه برای این آدرس IP: 16

## ۱-۴-۲ روشی ساده برای اعمال سابنتینگ

اکنون که با اصول اولیه سابنتینگ آشنا شدید، قصد داریم روشی ساده جهت اعمال سابنتینگ در یک شبکه به شما معرفی کنیم. این روش با استفاده از یک جدول و یک نمودار عملیات سابنتینگ را انجام می‌دهد. شاید در آغاز کار مراحل کمی پیچیده به نظر برسند ولی با چند بار تکرار به سادگی آن پی خواهید برد. نمودار و جدول مربوطه را می‌توانید در ادامه مشاهده نمایید.

$2^{(8)}-2=Y$	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

0: میزبان‌ها 1: زیر شبکه

## نمودار ۱-۱

(توان) x					Y
2 <sup>x</sup>	3	=	8	-2	6
2 <sup>x</sup>	4	=	16	-2	14
2 <sup>x</sup>	5	=	32	-2	30
2 <sup>x</sup>	6	=	64	-2	62
2 <sup>x</sup>	7	=	128	-2	126
2 <sup>x</sup>	8	=	256	-2	254
2 <sup>x</sup>	9	=	512	-2	510
2 <sup>x</sup>	10	=	1024	-2	1022
2 <sup>x</sup>	11	=	2048	-2	2046
2 <sup>x</sup>	12	=	4096	-2	4094
2 <sup>x</sup>	13	=	8192	-2	8190
2 <sup>x</sup>	14	=	16384	-2	16382
2 <sup>x</sup>	15	=	32768	-2	32766
2 <sup>x</sup>	16	=	65536	-2	65534
2 <sup>x</sup>	17	=	131072	-2	131070

## جدول ۱-۴: اعمال سابنتینگ

در جدول بالا، اعدادی که در ستون Y نشان داده شده‌اند، تعداد آدرس‌های موجود را پس از حذف دو آدرس رزرو شده نشان می‌دهند. در ادامه، با استفاده از این روش تعدادی مثال در رابطه با سابنتینگ ارائه می‌دهیم.

**مثال ۱: کلاس C: ۱۰ میزبان در زیرشبکه**

فرض کنید یک آدرس از کلاس C در اختیار داشته و برای هر زیرشبکه به ۱۰ میزبان نیاز دارید:

۱. ابتدا مقدار \_\_\_\_ 255.255.255 را بنویسید. فضای خالی بیان‌کننده عددی است که باید بدست آورده و در قاب زیرشبکه قرار دهید.
۲. به ستون Y در جدول نگاه کرده و اولین عدد بزرگتر از ۱۰ (تعداد میزبان‌ها در زیرشبکه) را انتخاب کنید. این عدد ۱۴ می‌باشد.
۳. مجدداً به جدول مراجعه نموده و از ستون x (توان)، عدد توان را پیدا کنید. مقدار توان ۴ خواهد بود.
۴. به نمودار بالای جدول مراجعه نموده و سطری که دقیقاً چهار ۰ دارد را جستجو و عدد آغازین این سطر را پیدا کنید. این عدد برابر ۲۴۰ می‌باشد و دقیقاً همان پاسخی است که در قاب زیرشبکه باید قرار گیرد. بنابراین قاب زیرشبکه برابر با 255.255.255.240 خواهد بود.

**مثال ۲: کلاس C: ۲۰ میزبان در زیرشبکه**

یک آدرس از کلاس C در اختیار داشته و برای هر زیرشبکه به ۲۰ میزبان نیاز دارید:

۱. ابتدا مقدار \_\_\_\_ 255.255.255 را بنویسید.
۲. به ستون Y در جدول نگاه کرده و اولین عدد بزرگتر از ۲۰ را انتخاب کنید. این عدد ۳۰ می‌باشد.
۳. مجدداً به جدول مراجعه نموده و از ستون x (توان)، عدد توان را پیدا کنید. این عدد ۵ خواهد بود.
۴. به نمودار بالای جدول مراجعه نموده و سطری که دقیقاً پنج ۰ دارد را جستجو و عدد آغازین این سطر را پیدا کنید. این عدد برابر ۲۲۴ می‌باشد. بنابراین قاب زیرشبکه برابر با 255.255.255.224 خواهد بود.

**مثال ۳: کلاس C: ۵ زیرشبکه**

اکنون فرض کنید یک آدرس از کلاس C در اختیار داشته و نیازمند ۵ زیرشبکه می‌باشید. دقت داشته باشید که زیرشبکه‌ها با ۱۱ نشان داده شده‌اند.

۱. ابتدا مقدار \_\_\_\_ 255.255.255 را بنویسید.
۲. به ستون Y در جدول نگاه کرده و اولین عدد بزرگتر از ۵ را جستجو کنید (این عدد باید ۶ باشد).
۳. از ستون x (توان)، عدد توان را پیدا کنید. این عدد ۳ خواهد بود.
۴. به نمودار مراجعه نموده و سطری را که دقیقاً از چپ به راست دارای سه بیت ۱ می‌باشد جستجو کنید. پس از یافتن پاسخ، قاب زیرشبکه بصورت 255.255.255.224 خواهد بود.



**مثال ۴: کلاس B: ۱۵۰۰ میزبان در زیرشبکه**

این مثال کمی دشوارتر است، یک آدرس از کلاس B در اختیار داشته و نیازمند ۱۵۰۰ میزبان در هر زیرشبکه می‌باشید. چون آدرس شما از کلاس B می‌باشد در قالب زیرشبکه باید اکتت سوم را (برای آدرس زیرشبکه) مقداردهی کنید. اکتت چهارم با صفر (هشت بیت صفر) مقداردهی شده است.

۱. ابتدا مقدار 0. \_\_\_\_ 255.255 را بنویسید.
۲. به ستون Y در جدول نگاه کرده و اولین عدد بزرگتر از ۱۵۰۰ را جستجو کنید (این عدد باید ۲۰۴۶ باشد).
۳. از ستون x (توان)، عدد توان را پیدا کنید. این عدد ۱۱ خواهد بود.
۴. به خاطر داشته باشید که شما هشت بیت صفر در آخرین اکتت در اختیار دارید، بنابراین تنها به سه بیت (۰) دیگر نیازمندید. در نمودار، سطری که دقیقا سه بیت ۰ دارد را پیدا کنید. عدد بدست آمده در این سطر ۲۴۸ می‌باشد، بنابراین قالب زیرشکه شما بصورت 255.255.248.0 خواهد بود. معادل دودویی این قالب بصورت 11111111.11111111.11111000.00000000 می‌باشد که ۱۱ بیت صفر در آن قابل مشاهده است.

**مثال ۵: کلاس B: ۳۵۰۰ میزبان در زیرشبکه**

در این مثال، یک آدرس از کلاس B در اختیار داشته و نیازمند ۳۵۰۰ میزبان در هر زیرشبکه می‌باشید.

۱. ابتدا مقدار 0. \_\_\_\_ 255. 255 را بنویسید.
۲. به ستون Y در جدول نگاه کرده و اولین عددی که بزرگتر از ۳۵۰۰ است را جستجو کنید (این عدد باید ۴۰۹۴ باشد).
۳. از ستون x (توان)، عدد توان را پیدا کنید. این عدد ۱۲ خواهد بود.
۴. هشت بیت صفر در آخرین اکتت در اختیار دارید بنابراین تنها به چهار بیت (صفر) دیگر نیازمندید. در نمودار سطری که دقیقا چهار بیت صفر دارد را پیدا کنید. عدد بدست آمده در این سطر ۲۴۰ می‌باشد، بنابراین قالب زیرشکه شما بصورت 255.255.240.0 خواهد بود. معادل دودویی این قالب بصورت 11111111.11111111.11111000.00000000 می‌باشد که ۱۲ بیت صفر در آن قابل مشاهده است.

**۳-۴-۱ اعمال سابنتینگ به روش سنتی**

روش معرفی شده در مثال قبل، در عین سادگی می‌تواند کمی گیج کننده نیز باشد زیرا به خاطر

سپردن اعداد موجود در جدول و نمودار کمی دشوار است. در این قسمت قصد داریم روشی سنتی برای انجام سابنتینگ در سه کلاس A، B و C از آدرس‌های IP معرفی نماییم که در آن دیگر نیازی به به‌خاطر سپاری اعداد روش قبل نیست. در ادامه این روش را بر روی هر سه کلاس انجام می‌دهیم. به دلیل سادگی محاسبات در کلاس C، کار را با این کلاس آغاز می‌کنیم سپس در ادامه به دو کلاس دیگر خواهیم پرداخت.

### سابنتینگ در کلاس C

همانطور که قبلاً اشاره نمودیم، در کلاس C سه بایت به آدرس شبکه و تنها یک بایت به آدرس میزبان اختصاص داده می‌شود. ۸ بیت اختصاص داده شده به آدرس میزبان تنها ۲۵۴ آدرس در کل شبکه فراهم می‌نماید، بنابراین زمانی که می‌خواهید چندین زیرشبکه داشته باشید، با محدودیت فضای آدرس‌دهی مواجه خواهید بود و به همین‌رسان که تعداد زیرشبکه‌های شما افزایش می‌یابد، این ۲۵۴ آدرس در آنها تقسیم می‌شود.

تقسیم شبکه به چندین زیرشبکه و تعیین مواردی مثل قاب زیرشبکه، آدرس مسیریاب و همچنین آدرس پخش یا Broadcast (این آدرس به منظور ارسال پیغام به تمام کاربران زیرشبکه استفاده می‌شود) می‌تواند کاری گیج‌کننده باشد. بنابراین در اینجا تکنیک‌هایی را برای سادگی کار به شما معرفی خواهیم نمود (البته تکنیک‌های قسمت قبل نیز از کارایی خوبی برخوردار می‌باشند). در جدول ۵-۱ تقسیم یک شبکه در کلاس C به چندین زیرشبکه مختلف به همراه مواردی چون قاب زیرشبکه، شماره زیرشبکه، آدرس‌های مسیریاب و آدرس‌های پخش در هر زیرشبکه آورده شده است. سه بایت اول در هر آدرس با x.y.z. تعیین شده است و آدرس‌های دارای بیت‌های تماماً صفر یا تماماً ۱ نیز در نظر گرفته شده است.

جدول ۵-۱: تقسیم یک شبکه در کلاس C به چندین زیرشبکه مختلف

تعداد زیرشبکه‌ها	قاب زیرشبکه	شماره شبکه	آدرس مسیریاب	آدرس پخش	تعداد آدرس‌های باقیمانده
1	255.255.255.0	x.y.z.0	x.y.z.1	x.y.z.255	253
2	255.255.255.128 255.255.255.128	x.y.z.0 x.y.z.128	x.y.z.1 x.y.z.129	x.y.z.127 x.y.z.255	125 125
4	255.255.255.192 255.255.255.192 255.255.255.192 255.255.255.192	x.y.z.0 x.y.z.64 x.y.z.128 x.y.z.192	x.y.z.1 x.y.z.65 x.y.z.129 x.y.z.193	x.y.z.63 x.y.z.127 x.y.z.191 x.y.z.255	61 61 61 61

29	x.y.z.31	x.y.z.1	x.y.z.0	255.255.255.224	8
29	x.y.z.63	x.y.z.33	x.y.z.32	255.255.255.224	
29	x.y.z.95	x.y.z.65	x.y.z.64	255.255.255.224	
29	x.y.z.127	x.y.z.97	x.y.z.96	255.255.255.224	
29	x.y.z.159	x.y.z.129	x.y.z.128	255.255.255.224	
29	x.y.z.191	x.y.z.161	x.y.z.160	255.255.255.224	
29	x.y.z.223	x.y.z.193	x.y.z.192	255.255.255.224	
29	x.y.z.255	x.y.z.225	x.y.z.224	255.255.255.224	

جهت آشنایی بیشتر با این تکنیک، آدرس x 200.211.192 را که از کلاس C می‌باشد در نظر بگیرید. فرض کنید که به دو زیرشبکه نیازمندید. با توجه به جدول، باید از قاب زیرشبکه 255.255.255.128 برای هر زیرشبکه استفاده نمایید. اولین زیرشبکه دارای شماره 200.211.192.0، آدرس مسیریاب 200.211.192.1 و آدرس پخش 200.211.192.127 می‌باشد. می‌توانید آدرس‌های IP از 200.211.192.2 تا 200.211.192.126 را که ۱۲۵ آدرس مختلف می‌باشد به سایر میزبان‌ها اختصاص دهید.

دومین زیرشبکه در این مثال باید دارای شماره 200.211.192.128، آدرس مسیریاب 200.211.192.129 و آدرس پخش 200.211.192.255 باشد (در واقع این کلاس شامل تعداد ۲۵۶ آدرس است که از 192.0 شروع و به 192.255 خاتمه می‌یابد. چون دو زیرشبکه نیاز دارید، کل این تعداد آدرس را بر دو تقسیم نموده و به آنها اختصاص دهید. اولین آدرس قابل اختصاص در هر زیرشبکه را به مسیریاب یا همان Default Gateway، آخرین آدرس را به آدرس پخش و بقیه را به سایر ماشین‌ها اختصاص دهید).

### تعیین شماره برای یک زیرشبکه در کلاس C

اولین زیرشبکه همیشه دارای مقدار صفر در اکت‌های مربوط به آدرس زیرشبکه می‌باشد. به عنوان مثال در آدرس 200.211.192.0 مقدار چهارمین اکت برابر با ۰ است که نشان‌دهنده اولین زیرشبکه در شبکه مورد نظر می‌باشد. برای تعیین شماره سایر زیرشک‌ها مراحل زیر را دنبال نمایید:

۱. اکتی که در قاب زیرشبکه دارای مقداری غیر از ۰ یا ۲۵۵ می‌باشد را انتخاب نمایید. مقدار این اکت را از ۲۵۶ کسر کنید. نتیجه‌ای که از انجام این عمل بدست می‌آید، مقدار افزایشی در اکت مربوط به آدرس زیرشبکه را تعیین می‌نماید.

اگر بار دیگر از آدرس شبکه x 200.211.192 و قاب زیرشبکه 255.255.255.192 استفاده نمایید، حاصل انجام عملیات فوق بصورت  $256 - 192 = 64$  می‌باشد. بنابراین جهت تعیین شماره سایر زیرشبکه‌ها باید به مقدار زیرشبکه قبلی عدد ۶۴ افزوده شود.

۲. برای تعیین شماره زیرشبکه دوم، عدد ۶۴ (عدد افزایشی) را به مقدار ۰ در چهارمین اکتت از اولین زیرشبکه اضافه نمایید. در این مثال حاصل برابر با 200.211.192.64 خواهد بود.
۳. برای تعیین شماره زیرشبکه سوم، مجدداً عدد ۶۴ را به مقدار آخرین اکتت در زیرشبکه دوم اضافه نمایید. در اینجا حاصل برابر با 200.211.192.128 خواهد بود.
۴. این کار را تا رسیدن به مقدار قاب زیرشبکه تکرار نمایید.

در این مثال، شماره زیرشبکه اول برابر با ۰، زیرشبکه دوم  $64 = 64 + 0$ ، زیرشبکه سوم  $128 = 64 + 64$  و شماره زیرشبکه چهارم نیز برابر با  $192 = 64 + 64 + 64$  می‌باشد. چون در قاب زیرشبکه اکتت چهارم ۱۹۲ می‌باشد پس در اینجا کار به اتمام می‌رسد. اگر این کار را ادامه دهید به مقدار  $256 = 64 + 192$  خواهید رسید که مقداری غیر قابل استفاده می‌باشد. در این مثال شما چهار زیر شبکه با شماره‌های ۰، ۶۴، ۱۲۸ و ۱۹۲ در اختیار خواهید داشت.

اعدادی که بین شماره زیرشبکه‌ها قرار می‌گیرند، آدرس‌های میزبان و آدرس‌های پخش را مشخص می‌کنند. آدرس میزبان‌هایی که در زیرشبکه‌های مثال بالا قرار می‌گیرند در ادامه آورده شده است:

- ♦ میزبان‌های زیرشبکه ۰ (200.211.192.0) در دامنه آدرس‌های 200.211.192.1 تا 200.211.192.62 قرار دارند که ۶۲ میزبان در زیرشبکه را فراهم می‌نمایند. (آدرس 200.211.192.1 که اولین آدرس قابل اختصاص در زیرشبکه شماره ۰ است به مسیریاب و 200.211.192.63 به آدرس پخش اختصاص داده شده است)
- ♦ میزبان‌های زیرشبکه ۶۴ در دامنه آدرس‌های 200.211.192.65 تا 200.211.192.126 قرار دارند (آدرس 200.211.192.65 به مسیریاب و 200.211.192.127 به آدرس پخش اختصاص داده شده است)
- ♦ میزبان‌های زیرشبکه ۱۲۸ در دامنه آدرس‌های 200.211.192.129 تا 200.211.192.190 قرار دارند (آدرس 200.211.192.129 به مسیریاب و 200.211.192.191 به آدرس پخش اختصاص داده شده است)
- ♦ میزبان‌های زیرشبکه ۱۹۲ در دامنه آدرس‌های 200.211.192.193 تا 200.211.192.254 قرار دارند (آدرس 200.211.192.193 به مسیریاب و 200.211.192.255 به آدرس پخش اختصاص داده شده است)

مثال ۱: محاسبه مقادیر برای یک شبکه دارای ۸ زیرشبکه در کلاس C

فرض کنید در شبکه‌ای از کلاس C، به ۸ زیرشبکه نیاز داشته باشید. در این مورد می‌توانید با

استفاده از محاسبات  $2^x$ ، که در آن  $x$  تعداد بیت‌های زیرشبکه می‌باشد، تعداد زیرشبکه‌ها و شماره هر زیرشبکه را مشخص نمایید. مراحل کار بصورت زیر می‌باشد:

- برای ایجاد هشت زیرشبکه، به سه بیت نیاز است ( $2^3 = 8$ ). بنابراین مقدار دودویی اکتت چهارم در قاب زیرشبکه باید برابر با 11100000 باشد که این مقدار معادل عدد ۲۲۴ است. (مقدار این قاب باید در تمام ماشین‌ها یکسان باشد)
- عدد ۲۲۴ را از عدد ۲۵۶ تفریق کنید. حاصل برابر با ۳۲ می‌باشد. بنابراین مقدار اکتت چهارم در هر زیرشبکه باید به اندازه ۳۲ افزایش یابد. شماره زیرشبکه‌ها در این مثال به ترتیب برابر با ۰، ۳۲، ۶۴، ۹۶، ۱۲۸، ۱۶۰، ۱۹۲ و ۲۲۴ می‌باشد. آدرس‌های میزبان‌ها نیز اعداد بین شماره‌های زیرشبکه به جز اعدادی که دارای بیت‌های تماماً ۱ هستند، می‌باشند. این اعداد به ترتیب عبارتند از ۳۱، ۶۳، ۹۵، ۱۲۷، ۱۵۹، ۱۹۱، ۲۲۳ و ۲۵۵ که به منظور آدرس‌های Broadcast مورد استفاده قرار می‌گیرند. در جدول ۱-۶ زیرشبکه‌ها، میزبان‌ها و آدرس‌های پخش آنها آورده شده است.

جدول ۱-۶: مشخصات هشت زیرشبکه در کلاس C

زیرشبکه	میزبان‌ها	آدرس‌های پخش
0	1-30	31
32	33-62	63
64	65-94	95
96	97-126	127
128	129-158	159
160	161-190	191
192	193-222	223
224	225-254	255

#### مثال ۲: محاسبه مقادیر برای یک شبکه دارای ۱۶ زیرشبکه در کلاس C

فرض کنید که به تعداد بیت‌های زیرشبکه در مثال قبل، یکی اضافه می‌نمایید. در این حالت، مقدار اکتت چهارم در قاب زیرشبکه بصورت 11110000 که معادل با عدد ۲۴۰ است، می‌باشد. با استفاده از این چهار بیت تعداد ۱۶ زیرشبکه ( $2^4 = 16$ ) در اختیار خواهید داشت که در هرکدام از این زیر شبکه‌ها تنها ۱۴ میزبان قابل آدرس‌دهی می‌باشند ( $2^4 - 2 = 14$ ). همانطور که مشاهده می‌کنید، تنها با قرض گرفتن یک بیت بیشتر، تعداد میزبان‌ها در هر زیرشبکه تقریباً نصف می‌شوند.

برای تعیین شماره زیرشبکه‌ها همانند قبل، از ۰ شروع کنید. چون مقدار  $240 - 256 = 16$  است، مقدار افزایشی در اکتت چهارم برابر ۱۶ می‌باشد. بنابراین شماره زیرشبکه‌ها به ترتیب ۰، ۱۶، ۳۲، ۴۸،

۶۴، ۸۰، ۹۶، ۱۱۲، ۱۲۸، ۱۴۴، ۱۶۰، ۱۷۶، ۱۹۲، ۲۰۸، ۲۲۴ و ۲۴۰ خواهد بود. به خاطر داشته باشید که مقدار قاب زیرشبکه (۲۴۰)، بیانگر آخرین زیرشبکه دارای ارزش است، بنابراین شماره زیرشبکه‌ها نمی‌تواند از ۲۴۰ بیشتر باشد. آدرس میزبان‌ها اعداد بین شماره‌های شبکه، و آدرس‌های پخش نیز اعدادی هستند که تمام بیت‌های میزبان در آن ۱ می‌باشد (یا اعدادی که یک واحد از شماره زیرشبکه بعدی کوچکتر هستند). در جدول ۷-۱ زیرشبکه‌ها، میزبان‌ها و آدرس‌های پخش در هر زیرشبکه آورده شده است.

جدول ۷-۱: مشخصات ۱۶ زیرشبکه در کلاس C

زیرشبکه	میزبان‌ها	آدرس‌های پخش
0	1-14	15
16	17-30	31
32	33-46	47
48	49-62	63
64	65-78	79
80	81-94	95
96	97-110	111
112	113-126	127
128	129-142	143
144	145-158	159
160	161-174	175
176	177-190	191
192	193-206	207
208	209-222	223
224	225-238	239
240	241-254	255

### سابنتینگ در کلاس B

در کلاس B، ۱۶ بیت به آدرس شبکه و ۱۶ بیت نیز به آدرس میزبان تعلق دارد. ۱۶ بیت مربوط به آدرس میزبان‌ها می‌تواند تعداد زیادی از میزبان‌ها (۶۵،۵۳۴) را در اختیار شما قرار دهند. در این کلاس چنانچه شبکه را به تعداد زیادی از زیرشبکه‌ها تقسیم نمایید، باز هم در هر زیرشبکه تعداد مناسبی از میزبان‌ها را در اختیار خواهید داشت.

در کلاس B مقدار قاب زیرشبکه بصورت 11111111.11111111.00000000.00000000 می‌باشد.

بیت‌های ۱ بیانگر بیت‌های متناظر با آدرس شبکه و بیت‌های ۰ نیز بیانگر بیت‌های متناظر با آدرس میزبان در یک آدرس IP می‌باشند. برای ایجاد یک قاب زیرشبکه، بیت‌های میزبان از سمت چپ قرض گرفته شده و از ۰ به ۱ تبدیل می‌شوند. پس از قرض گرفته شدن بیت‌ها، آن دسته از بیت‌های ۰ که در قسمت میزبان باقی می‌مانند برای تولید آدرس میزبان‌ها مورد استفاده قرار می‌گیرد.

اگر تنها یک بیت برای ایجاد قاب زیرشبکه قرض گرفته شود، مقدار این قاب برابر 255.255.128.0، چنانچه دو بیت قرض گرفته شود، قاب زیرشبکه برابر 255.255.192.0 (11111111.11111111.11000000.00000000) و ... خواهد بود. اکنون قصد داریم سابنتینگ را برای کلاس B انجام دهیم. مراحل کار شبیه کلاس C می‌باشد فقط در کلاس B میزبان‌های بیشتری در هر زیرشبکه در اختیار خواهید داشت.

در مثال اخیر، با قرض گرفتن دو بیت، مقدار قاب زیرشبکه بصورت 255.255.192.0 خواهد بود. با این دو بیت تعداد  $2^2 = 4$  زیرشبکه در اختیار خواهید داشت. اکنون برای بدست آوردن مقدار افزایشی در اکتت سوم، عدد ۱۹۲ را از ۲۵۶ کسر نمایید. حاصل این عمل مقدار ۶۴ می‌باشد. پس شماره زیرشبکه‌ها به ترتیب برابر با ۰، ۶۴، ۱۲۸ و ۱۹۲ است. برای محاسبه تعداد میزبان‌ها در هر زیرشبکه، از ۱۴ بیت باقیمانده در قسمت میزبان از قاب زیرشبکه استفاده نمایید. با توجه به رابطه  $2^{14} = 16,384$  در هر زیرشبکه تعداد ۱۶,۳۸۴ میزبان قابل دسترسی می‌باشد. در جدول ۸-۱ مشخصات مربوط به این زیرشبکه‌ها آورده شده است.

جدول ۸-۱: مشخصات ۴ زیرشبکه در کلاس B

زیرشبکه	میزبان‌ها	آدرس‌های پخش
x.y.0.0	x.y.0.1 تا x.y.63.254	x.y.63.255
x.y.64.0	x.y.64.1 تا x.y.127.254	x.y.127.255
x.y.128.0	x.y.128.1 تا x.y.191.254	x.y.191.255
x.y.192.0	x.y.192.1 تا x.y.255.254	x.y.255.255

برای ایجاد ۸ زیرشبکه در کلاس B می‌توانید به قاب زیرشبکه مثال قبل یک بیت دیگر اضافه نموده تا مقدار آن به 11111111.11111111.11100000.00000000 یا 255.255.224.0 تبدیل شود. این مقدار، هشت زیرشبکه ( $2^3 = 8$ ) و ۸,۱۹۰ میزبان در هر زیرشبکه ( $2^{13} - 2 = 8,190$ ) در اختیار شما قرار می‌دهد. جهت تعیین شماره زیرشبکه‌ها، باید مقدار افزایشی در اکتت سوم را بدست آورید. این مقدار طبق رابطه  $224 - 256 = 32$  برابر با ۳۲ می‌باشد. بنابراین زیرشبکه‌ها به ترتیب ۰، ۳۲، ۶۴، ۹۶، ۱۲۸، ۱۶۰، ۱۹۲ و ۲۲۴ می‌باشند. در جدول ۹-۱ مشخصات این ۸ زیرشبکه آورده شده است.

جدول ۹-۱: مشخصات ۸ زیرشبکه در کلاس B

زیرشبکه	میزبان‌ها	آدرس‌های پخش
x.y.0.0	x.y.0.1 تا x.y.31.254	x.y.31.255
x.y.32.0	x.y.32.1 تا x.y.63.254	x.y.63.255
x.y.64.0	x.y.64.1 تا x.y.95.254	x.y.95.255
x.y.96.0	x.y.96.1 تا x.y.127.254	x.y.127.255
x.y.128.0	x.y.128.1 تا x.y.159.254	x.y.159.255
x.y.160.0	x.y.160.1 تا x.y.191.254	x.y.191.255
x.y.192.0	x.y.192.1 تا x.y.223.254	x.y.223.255
x.y.224.0	x.y.224.1 تا x.y.255.254	x.y.255.255

برای تمرین بیشتر در این رابطه، در ادامه استفاده از ۹ و ۱۴ بیت برای قاب زیرشبکه در کلاس B آورده شده است:

- اگر از ۹ بیت برای قاب زیرشبکه استفاده کنید، این قاب بصورت 255.255.255.128 یا 11111111.11111111.11111111.10000000 خواهد بود. با این ۹ بیت، تعداد  $2^9 = 512$  زیرشبکه خواهید داشت. با هفت بیت باقیمانده برای میزبان‌ها، ۱۲۶ میزبان در هر زیرشبکه ( $2^7 - 2 = 126$ ) قابل دسترسی می‌باشد.
- اگر از ۱۴ بیت برای قاب زیرشبکه استفاده کنید، این قاب بصورت 255.255.255.252 یا 11111111.11111111.11111111.11111100 خواهد بود. با این ۱۴ بیت، تعداد  $2^{14} = 16,384$  زیرشبکه خواهید داشت. با دو بیت باقیمانده برای میزبان‌ها، تنها دو میزبان در هر زیرشبکه ( $2^2 - 2 = 2$ ) قابل دسترسی می‌باشد.

#### ساب‌تینگ در کلاس A

در کلاس A تعداد بیت‌های بیشتری نسبت به دو کلاس B و C در اختیار خواهید داشت. در این کلاس، ۸ بیت به آدرس شبکه و ۲۴ بیت به آدرس میزبان تعلق دارد. بنابراین هم تعداد زیرشبکه‌های قابل ایجاد و هم تعداد میزبان‌ها در هر زیرشبکه بسیار زیاد می‌باشند. قاب زیرشبکه در کلاس A بصورت 255.0.0.0 یا 11111111.00000000.00000000.00000000 می‌باشد. قصد داریم به عنوان مثال تعداد زیرشبکه‌ها و تعداد میزبان‌ها را زمانی که ۸ و ۱۲ بیت از قسمت میزبان قرض گرفته می‌شود محاسبه نماییم. زمانی که ۸ بیت قرض گرفته شده و به آدرس زیرشبکه اختصاص داده می‌شود، تعداد



$2^{16} = 256$  زیر شبکه قابل ایجاد می‌باشد. با داشتن ۱۶ بیت باقیمانده برای میزبان، تعداد  $2^{16} = 65,536$  - آدرس میزبان در هر زیر شبکه قابل اختصاص می‌باشد.

اکنون حالتی را در نظر بگیرید که ۱۲ بیت به آدرس زیر شبکه اختصاص داده می‌شود. در این حالت قاب زیر شبکه بصورت 255.255.240.0 یا 11111111.11111111.11110000.00000000 می‌باشد. بنابراین تعداد زیر شبکه‌ها برابر با  $2^{12} = 4,096$  و تعداد میزبان‌ها در هر زیر شبکه برابر با  $2^4 = 16$  خواهد بود.

برای تعیین شماره زیر شبکه‌ها، باید توجه داشته باشید که اکتت دوم همواره مقداری بین ۰ و ۲۵۵ خواهد داشت و بنابراین باید به دنبال مقدار اکتت سوم باشید. چون سومین اکتت (در مثال ۱۲ بیت) دارای مقدار ۲۴۰ می‌باشد، طبق رابطه  $160 - 256$ ، مقدار افزایشی در این اکتت برابر با ۱۶ می‌باشد. شماره اولین زیر شبکه با ۰ شروع شده و با اضافه نمودن عدد ۱۶ به شماره هر زیر شبکه، شماره زیر شبکه بعدی بدست می‌آید. این کار تا رسیدن به عدد ۲۴۰ که قاب زیر شبکه است ادامه می‌یابد. مشخصات تعدادی از این زیر شبکه‌ها در جدول ۱-۱۰ آورده شده است (توجه داشته باشید که تعداد کل این زیر شبکه‌ها ۴۰۹۶ می‌باشد بنابراین مقادیر اکتت سوم در ستون زیر شبکه به ازای هر عددی بین ۰ و ۲۵۵ تکرار می‌شود).

جدول ۱-۱۰: مشخصات تعدادی از زیر شبکه‌ها در کلاس A

زیر شبکه	میزبان‌ها	آدرس‌های پخش
x.0-255.0.0	x.0-255.0.1 تا x.0-255.15.254	x.0-255.15.255
x.0-255.16.0	x.0-255.16.1 تا x.0-255.31.254	x.0-255.31.255
x.0-255.32.0	x.0-255.32.1 تا x.0-255.47.254	x.0-255.47.255
x.0-255.48.0	x.0-255.48.1 تا x.0-255.63.254	x.0-255.63.255
x.0-255.64.0	x.0-255.64.1 تا x.0-255.79.254	x.0-255.79.255
x.0-255.80.0	x.0-255.80.1 تا x.0-255.95.254	x.0-255.95.255
x.0-255.96.0	x.0-255.96.1 تا x.0-255.111.254	x.0-255.111.255
x.0-255.112.0	x.0-255.112.1 تا x.0-255.127.254	x.0-255.127.255
x.0-255.128.0	x.0-255.128.1 تا x.0-255.143.254	x.0-255.143.255
x.0-255.144.0	x.0-255.144.1 تا x.0-255.159.254	x.0-255.159.255
x.0-255.160.0	x.0-255.160.1 تا x.0-255.175.254	x.0-255.175.255
x.0-255.176.0	x.0-255.176.1 تا x.0-255.191.254	x.0-255.191.255

x.0-255.207.255	x.0-255.207.254 تا x.0-255.192.1	x.0-255.192.0
x.0-255.223.255	x.0-255.223.254 تا x.0-255.208.1	x.0-255.208.0
x.0-255.239.255	x.0-255.239.254 تا x.0-255.224.1	x.0-255.224.0
x.0-255.255.255	x.0-255.255.254 تا x.0-255.240.1	x.0-255.240.0

### ۱-۵ آدرس‌دهی بدون کلاس

مایکروسافت از یک روش ثانویه‌ای نیز جهت کار با آدرس‌های IP استفاده می‌کند که به روش CIDR<sup>۱</sup> (بخوانید سیدِر) معروف است. روشی جهت خلاصه‌نویسی قاب زیرشبکه می‌باشد. به عنوان مثال آدرس 131.107.2.3 به همراه قاب زیرشبکه 255.255.255.0 در روش CIDR بصورت 131.107.2.3/24 نشان داده می‌شود که عدد بعد از علامت “/” (Slash) بیانگر تعداد بیت‌های ۱ در قاب زیرشبکه می‌باشد. در این روش (به عنوان مثال) آدرسی که بصورت 141.10.32.0/19 نوشته می‌شود، دارای قاب زیرشبکه 255.255.224.0 است که ۱۹ بیت با مقدار ۱ در قاب زیرشبکه آن وجود دارد (11111111.11111111.11100000.00000000).

در جدول ۱-۱۱ لیست تمام اعداد CIDR به همراه قاب زیرشبکه متناسب با آنها آورده شده است.

جدول ۱-۱۱: لیست تمام اعداد CIDR

Mask	CIDR	Mask	CIDR	Mask	CIDR
255.255.255.128	/25	255.255.128.0	/17	255.0.0.0	/8
255.255.255.192	/26	255.255.192.0	/18	255.128.0.0	/9
255.255.255.224	/27	255.255.224.0	/19	255.192.0.0	/10
255.255.255.240	/28	255.255.240.0	/20	255.224.0.0	/11
255.255.255.248	/29	255.255.248.0	/21	255.240.0.0	/12
255.255.255.252	/30	255.255.252.0	/22	255.248.0.0	/13
255.255.255.254	/31	255.255.254.0	/23	255.252.0.0	/14
255.255.255.255	/32	255.255.255.0	/24	255.254.0.0	/15
				255.255.0.0	/16

### ۱-۵-۱ شناسایی سریع مشخصات زیرشبکه با استفاده از CIDR

در این قسمت قصد داریم با استفاده از نشانه‌گذاری CIDR روشی معرفی کنیم که به کمک آن

1. Classless Inter-Domain Routing

بتوانید به سرعت مشخصاتی مانند آدرس زیرشبکه، آدرس‌های پخش و محدوده آدرس‌های هر زیرشبکه را در سه کلاس A، B و C مشخص نمایید.

### شناسایی مشخصات زیرشبکه در کلاس C

آدرس میزبان 192.168.10.50/27 را در نظر بگیرید. جهت تعیین آدرس زیرشبکه‌ای که این میزبان در آن قرار دارد، مراحل زیر را دنبال نمایید:

۱. ابتدا قاب زیرشبکه معادل با عدد CIDR که بعد از آدرس IP آورده شده است را تعیین نمایید. در این مثال مقدار قاب زیرشبکه برای عدد 27/ برابر با 255.255.255.224 می‌باشد.
۲. مضربی از ۸ که بزرگتر یا مساوی عدد CIDR می‌باشد را تعیین نمایید. سپس آنرا بر ۸ تقسیم نموده تا اکتی که مقدار آن به ازای هر زیرشبکه افزایش می‌یابد تعیین گردد.
- در این مثال عدد CIDR برابر با ۲۷ است، بنابراین نزدیکترین مضرب ۸ که بزرگتر یا مساوی این عدد باشد، ۳۲ می‌باشد. با تقسیم ۳۲ بر ۸، عدد ۴ بدست می‌آید که به چهارمین اکت اشاره دارد.
۳. برای بدست آوردن مقدار افزایشی در اکت چهارم، عدد CIDR را از مضرب ۸ (که در این مثال ۳۲ است) تفریق کنید. حاصل برابر با ۵ خواهد بود ( $32 - 27 = 5$ ). اکنون ۲ را به توان این عدد برسانید تا مقدار افزایشی بدست آید ( $2^2 = 32$ ).
۴. برای تعیین شماره زیرشبکه‌ها، به جای عدد ۵۰ در آدرس اصلی، عدد ۰ را قرار داده و هر بار به شماره قبلی عدد ۳۲ را اضافه نمایید تا زمانی که مقدار آن از ۵۰ بیشتر شود. شماره‌های ۰، ۳۲ و ۶۴ برای زیرشبکه‌ها بدست می‌آیند.
۵. زیرشبکه‌ای که به دنبال آن هستید، بین دو شماره زیرشبکه که دارای نزدیکترین مقادیر بزرگتر و کوچکتر از مقدار فعلی هستند قرار دارد.
- در اینجا 192.168.10.50/27 بین دو زیرشبکه 192.168.10.32 (کوچکتر) و 192.168.10.64 (بزرگتر) قرار دارد.
۶. محدوده آدرس‌های قابل استفاده برای این زیرشبکه، از یک شماره بیشتر از شماره زیرشبکه شروع شده و تا قبل از آدرس پخش ادامه می‌یابد. در این مثال آدرس پخش 192.168.10.63 است بنابراین آدرس میزبان‌ها از 192.168.10.33 شروع و با 192.168.10.62 خاتمه می‌یابند. همانطور که مشاهده می‌کنید، آدرس 192.168.10.50/27 در زیرشبکه با شماره ۳۲ (192.168.10.32/27) قرار دارد.

### شناسایی مشخصات زیرشبکه در کلاس B

با استفاده از مراحل قسمت قبل، زیرشبکه‌ای که آدرس 172.16.76.12/20 در آن قرار دارد به

صورت زیر تعیین می‌شود:

۱. در این مثال، عدد CIDR برابر با 20/ (11111111.11111111.11110000) یا 255.255.240.0 می‌باشد.
۲. اولین مضرب از ۸ که بزرگتر یا مساوی ۲۰ باشد برابر است با ۲۴. چون حاصل تقسیم ۲۴ بر ۸ برابر با ۳ می‌باشد، مقدار اکتت سوم باید به ازای هر زیرشبکه افزایش یابد.
۳. برای بدست آوردن مقدار افزایشی در اکتت سوم، عدد CIDR را از مضرب ۸ (که در این مثال ۲۴ است) تفریق کنید. حاصل برابر با ۴ خواهد بود ( $24 - 20 = 4$ ). اکنون ۲ را به توان این عدد برسانید تا مقدار افزایشی بدست آید ( $2^4 = 16$ ).
۴. با شروع از ۰، شماره زیرشبکه‌ها به ترتیب برابر با ۰، ۱۶، ۳۲، ۴۸، ۶۴ و ۸۰ می‌باشد. عدد ۷۶ در اکتت سوم، بین دو زیرشبکه ۶۴ و ۸۰ قرار می‌گیرد. پس از قرار دادن صفر در اکتت چهارم (چنانچه اکتت افزایش یابنده غیر از اکتت چهارم باشد، باید تمام اکتت‌های بعد از آن را با ۰ مقداردهی نمود)، آدرس شروع زیرشبکه مورد نظر بصورت 172.16.64.0 خواهد بود که آدرس پخش در آن 172.16.79.255 (یکی کمتر از شروع زیرشبکه 172.16.80.0) می‌باشد.
۵. دامنه آدرس‌های قابل استفاده در این زیرشبکه از 172.16.64.1 شروع و با 172.16.79.254 خاتمه می‌یابند. همانطور که مشاهده می‌کنید، آدرس 172.16.76.12 در این زیرشبکه قرار دارد.

#### شناسایی مشخصات زیرشبکه در کلاس A

بار دیگر مراحل کار را برای آدرس 10.6.127.255/14 که از کلاس A است تکرار کنید:

۱. عدد CIDR برابر 14/ است (11111111.11111100.00000000) یا 255.252.0.0.
۲. اولین مضرب ۸ که بزرگتر یا مساوی ۱۴ باشد برابر است با ۱۶. چون حاصل تقسیم ۱۶ بر ۸ برابر با ۲ می‌باشد، مقدار اکتت دوم باید به ازای هر زیرشبکه افزایش یابد.
۳. برای بدست آوردن مقدار افزایشی در اکتت دوم، عدد CIDR را از مضرب ۸ (که در این مثال ۱۶ است) تفریق کنید. حاصل برابر با ۲ خواهد بود ( $16 - 14 = 2$ ). اکنون ۲ را به توان این عدد برسانید تا مقدار افزایشی بدست آید ( $2^2 = 4$ ).
۴. با شروع از ۰، شماره زیرشبکه‌ها به ترتیب برابر با ۰، ۴ و ۸ می‌باشد. عدد ۶ در اکتت دوم، بین دو زیرشبکه ۴ و ۸ قرار می‌گیرد. پس از قرار دادن صفر در اکتت‌های سوم و چهارم، آدرس شروع زیرشبکه مورد نظر بصورت 10.4.0.0 خواهد بود که آدرس پخش در آن 10.7.255.255 (یکی کمتر از شروع زیرشبکه 10.8.0.0) می‌باشد.
۵. دامنه آدرس‌های قابل استفاده در این زیرشبکه از 10.4.0.1 شروع و با 10.7.255.254 خاتمه می‌یابند. همانطور که مشاهده می‌کنید، آدرس 10.6.125.255 در این زیرشبکه قرار دارد.

### ۱-۵-۲ تعیین تعداد زیرشبکه‌ها و میزبان‌ها

با استفاده از روشی که در قسمت قبل معرفی نمودیم، می‌توانید تعداد زیرشبکه‌ها و تعداد میزبان‌ها در هر زیرشبکه را تعیین کنید. این کار به کمک تعداد بیت‌های پیش‌فرض در قاب زیرشبکه و تعداد بیت‌های تعیین شده بوسیله CIDR قابل انجام می‌باشد.

به عنوان مثال آدرس 172.16.0.0/23 (آدرسی از کلاس B) را در نظر بگیرید. قاب زیرشبکه برای این آدرس بصورت 255.255.254.0 بوده و قاب زیرشبکه پیش‌فرض در کلاس B نیز بصورت 255.255.0.0 است که دارای ۱۶ بیت ۱ می‌باشد. اکنون اگر تعداد بیت‌های قاب پیش‌فرض را از تعداد بیت‌های قاب زیرشبکه آدرس تفریق نمایید ( $16 - 23 = 7$ ) و ۲ را به توان حاصل این تفریق برسانید ( $2^7 = 128$ )، تعداد زیرشبکه‌ها برای یک آدرس با قاب داده شده بدست می‌آید. در اینجا ۱۲۸ زیرشبکه به ازای آدرسی از کلاس B که دارای قاب زیرشبکه 255.255.254.0 می‌باشد، بدست آمده است.

تعیین تعداد میزبان‌ها در هر کدام از این ۱۲۸ زیرشبکه نیز ساده است، چون همیشه با تفریق تعداد بیت‌های قاب زیرشبکه (که در اینجا ۲۳ است) از عدد ۳۲ (که تعداد کل بیت‌ها در یک آدرس IP می‌باشد) بدست می‌آید. در اینجا حاصل  $32 - 23 = 9$ ، که عدد ۹ بیانگر تعداد بیت‌های صفر باقیمانده در قاب زیرشبکه می‌باشد. زمانی که ۲ را به توان این عدد (۹) برسانید و از عدد ۲ تفریق کنید ( $2^9 - 2 = 510$ )، تعداد میزبان‌ها به ازای هر زیرشبکه با این قاب بدست می‌آید.

### ۱-۶-۱ آشنایی با آدرس‌های IPv6

IPv6 نسخه بازسازی شده IPv4 است که به دلیل مواجه شدن با مشکل کمبود آدرس‌های IPv4 ایجاد شد. در بحث IPv4 گفتیم که این آدرس‌ها از ۳۲ بیت تشکیل شده‌اند، بنابراین کل آدرس‌های موجود در این نوع برابر با  $2^{32} = 4,294,967,296$  می‌باشند.

در IPv6 تعداد بیت‌های تشکیل دهنده آدرس به ۱۲۸ بیت افزایش یافته است که با استفاده از آن می‌توان  $2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,656$  (یا  $10^{38} * 3.4$ ) آدرس مختلف ایجاد نمود. در ویندوزهای ویستا و سرور ۲۰۰۸ به بعد، از این آدرس‌ها به خوبی پشتیبانی می‌شود.

### ۱-۶-۱ نمایش آدرس‌های IPv6

آدرس‌های IPv4 بصورت چهار اکتت که دارای مقادیر ده‌دهی و یا مقادیر دودویی متناظر با آنها هستند نمایش داده می‌شوند. در IPv6 شیوه نمایش آدرس‌ها متفاوت خواهد بود. ۱۲۸ بیت تشکیل دهنده این آدرس‌ها به هشت قسمت ۱۶ بیتی تقسیم شده و هر قسمت با ترکیبی از اعداد ۰ تا ۹ و حروف A تا F ( $A = 10, B = 11, C = 12, D = 13, E = 14, F = 15$ ) نشان داده می‌شوند. در واقع این

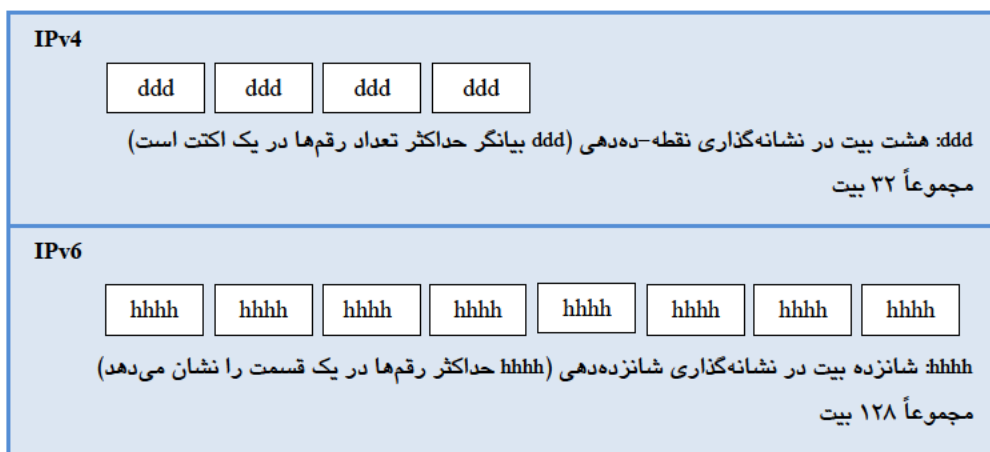
اعداد و حروف، آدرس IP را به صورت شانزده‌دهی (مبنای ۱۶) نشان می‌دهند. یک آدرس IPv6 به صورت زیر می‌باشد:

2001:0DB8:0000:0000:1234:0000:A9FE:133E

معادل دودویی هر قسمت از آدرس بالا به ترتیب (از چپ به راست) به صورت زیر نشان داده می‌شود:

0010 0000 0000 0001:0000 1101 1011 1000:0000 0000 0000 0000:0000 0000 0000 0001 0010  
0011 0100 :0000 0000 0000 0000:1010 1001 1111 1110:0001 0011 0011 1110

در شکل زیر مقایسه آدرس‌های IPv4 و IPv6 نشان داده شده است.



شکل ۲۰-۱

### ۱-۶-۲ خلاصه نویسی آدرس‌های IPv6

چندین قانون برای خلاصه نویسی آدرس‌های IP وجود دارد که لیست آنها در ادامه آورده شده است:

- استفاده از 0: به جای 0000:
- حذف صفرهای ابتدایی در یک قسمت ۱۶ بیتی (مثلاً دو کلمه DB8: و 0DB8: برابر هستند).
- استفاده از نماد :: زمانی که صفرها چندین بار تکرار می‌شوند. البته در هر آدرس تنها یکبار می‌توان از این نماد استفاده نمود (مثلاً آدرس 2001:DB8:3C4D:12:0:0:1234:56AB را می‌توان به صورت 2001:DB8:3C4D:12::1234:56AB نوشت).

به عنوان مثالی در این رابطه، آدرس 2001:0DB8:0000:0000:1234:0000:A9FE:133E را می‌توان بصورت زیر خلاصه نمود:

- ♦ 0000: را به 0: فشرده کنید: 2001:0DB8:0000:0000:1234:0:A9FE:133E
- ♦ صفرهای آغازین را حذف کنید: 2001:DB8:0000:0000:1234:0:A9FE:133E
- ♦ به جای چندین کلمه 0000: از نماد :: استفاده کنید: 2001:DB8::1234:0:A9FE:133E

### ۱-۶-۳ انواع آدرس‌های IPv6

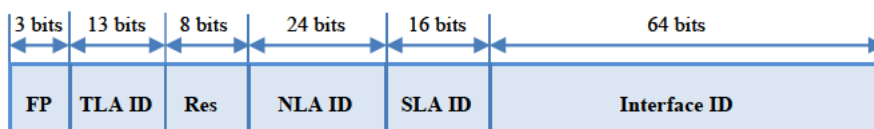
آدرس‌های IPv6 بطور کلی به سه دسته تقسیم می‌شوند که عبارتند از: آدرس‌های Unicast، Multicast و Anycast. در ادامه هر کدام را مورد بررسی قرار می‌دهیم.

#### آدرس‌های Unicast

آدرس‌های unicast تنها یک دستگاه (یا یک اینترفیس<sup>۱</sup>) را در شبکه مورد شناسایی قرار می‌دهند، بنابراین زمانی که بسته‌ای<sup>۲</sup> به یک آدرس unicast فرستاده می‌شود، این بسته تنها توسط آدرس مشخص شده دریافت می‌شود. آدرس‌های unicast خود به پنج دسته تقسیم می‌شوند که عبارتند از:

#### ۱. آدرس‌های global unicast/ Aggregatable global unicast

از این آدرس‌ها به دلیل برخورداری از قابلیت مسیریابی، در اینترنت استفاده می‌شود و معادل همان آدرس‌های IPv4 معتبر/عمومی<sup>۳</sup> می‌باشند. این آدرس‌ها با فرمت پیشوندی 001 (3/2000) آغاز می‌شوند و ساختار کلی آنها در شکل زیر نشان داده شده است.



شکل ۱-۲۱

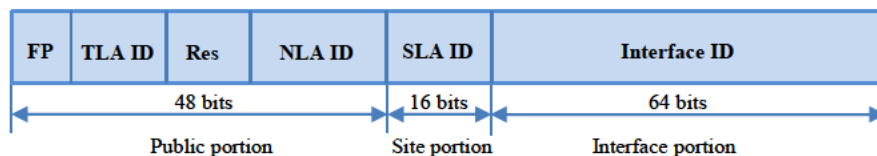
فیلدهای تشکیل‌دهنده این آدرس به شرح زیر می‌باشند:

- ♦ **FP:** این فیلد تعیین‌کننده نوع آدرس IPv6 است. در آدرس‌های global unicast، مقدار این فیلد و در واقع شروع آدرس‌های این نوع، برابر با 001 می‌باشد.

1. Interface  
2. Packet  
3. Valid/Public  
4. Format Prefix

- **TLA ID**<sup>۱</sup>: شناسه‌ای است که توسط سازمان تخصیص آدرس‌های اینترنت (IANA)<sup>۲</sup>، اختصاص داده می‌شود و به کمک آن می‌توان موقعیت جغرافیایی یک آدرس را تعیین نمود.
- **Res**<sup>۳</sup>: این فیلد در واقع فضایی کمکی است که برای دو فیلد TLA ID و NLA ID رزرو شده است. چنانچه این دو فیلد در آینده با مشکل کمبود فضا مواجه شوند، می‌توانند از ۸ بیت موجود در این فیلد (Res) استفاده کنند.
- **NLA ID**<sup>۴</sup>: این فیلد شناسه سطح بعد از فیلد TLA ID را برای آدرس مشخص می‌نماید و در مراکز ارائه دهنده خدمات اینترنت<sup>۵</sup> (ISP) مورد استفاده قرار می‌گیرد. ISPها به کمک این فیلد می‌توانند چندین سطح از ساختار آدرس‌دهی را ایجاد نموده و به سایت‌ها (مجموعه‌ای از چندین زیرشبکه) اختصاص دهند.
- **SLA ID**<sup>۶</sup>: این شناسه، در سطوح کوچکتری نسبت به شناسه NLA اختصاص داده می‌شوند. به عنوان مثال می‌توان برای مشخص نمودن زیرشبکه‌های موجود در یک سازمان از آن استفاده نمود. این شناسه از ۱۶ بیت تشکیل شده است بنابراین به کمک آن می‌توان تعداد ۶۵,۵۳۶ زیرشبکه یا سطح آدرس‌دهی را در یک سایت ایجاد نمود.
- **Interface ID**: از این شناسه برای مشخص نمودن یک اینترفیس منحصر بفرد در شبکه استفاده می‌شود و در واقع موقعیت آن در زیرشبکه را مشخص می‌کند.

اکنون پس از آشنایی با کلیه قسمت‌های این آدرس، می‌توان ساختار آنرا در قالب سه بخش نمایش داد. این ساختار در شکل زیر نشان داده شده است.

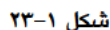


شکل ۱-۲۲

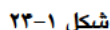
آدرس 2001:DB8:3C4D:0015:0000:0000:1A21:1A2B از نوع global در IPv6 است. معادل دودویی قسمت اول این آدرس برابر با 0010 0000 0000 0001 است که در آن سه بیت اول دارای مقدار 001 می‌باشند. با توجه به شکل بالا می‌توان سایر قسمت‌ها را بر روی آدرس مشخص نمود.

1. Top Level Aggregate Identifier
2. Internet Assigned Numbers Authority
3. Reserve
4. Next Level Aggregate Identifier
5. Internet Service Provider
6. Site Level Aggregate Identifier





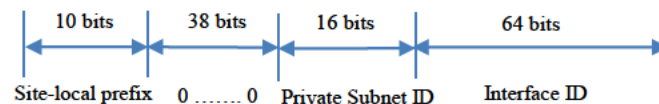
این آدرس‌ها فقط برای ارتباطات نقطه به نقطه در یک شبکه، زمانی که هیچ مسیریابی به‌کار گرفته نشده باشد استفاده می‌شود، زیرا قابلیت مسیریابی در آنها وجود ندارد. آدرس‌های Link-local IPv6 معادل با آدرس‌های 169.254.0.0/16 در IPv4 هستند (این آدرس‌ها APIPA نامیده شده و در واقع زمانی که در تنظیمات کارت شبکه بدون حضور سرویس DHCP تنظیم آدرس IP را بر روی دریافت خودکار قرار می‌دهید به میزبان‌ها اختصاص داده می‌شوند). مقدار پیشوند در این آدرس‌ها برابر با 10 1111 و شروع آدرس‌های آن نیز با FE80::/10 می‌باشد. به عنوان مثال آدرس FE80::A425:AB9D:7DA4:CCBA از نوع Link-local می‌باشد. ساختار این آدرس‌ها در تصویر زیر نشان داده شده است.



آدرس‌های Site-local در محدوده یک سایت قابل استفاده هستند. این آدرس‌ها معادل با آدرس‌های خصوصی در IPv4 (10.0.0.0/8، 172.16.0.0/12 و 192.168.0.0/16) می‌باشند. آدرس‌های

Site-local قابلیت مسیریابی ندارند بنابراین در شبکه‌هایی که ارتباط قسمت‌های آن با مسیریاب برقرار می‌شود (از جمله اینترنت) نمی‌توان از آنها استفاده نمود، اما در شبکه‌های داخلی یک سازمان (یک سایت) قابل استفاده هستند. مقدار پیشوند در این آدرس‌ها برابر با 1111 1110 11 می‌باشد و اولین ۴۸ بیت در این آدرس‌ها با FEC0::/48 شروع می‌شوند. پس از ۴۸ بیت مربوط به پیشوند، ۱۶ بیت برای تعیین زیرشبکه قرار می‌گیرد که با استفاده از این بیت‌ها می‌توان تعداد ۶۵,۵۳۶ زیرشبکه ( $2^{16} = 65,536$ ) در یک شبکه ایجاد نمود. پس از این ۱۶ بیت، ۶۴ بیت برای شناسایی اینترفیس شبکه آورده می‌شود که با این ۶۴ بیت می‌توان تعداد  $2^{64}$  اینترفیس را آدرس‌دهی نمود.

ساختار آدرس‌های Global unicast و Site-local unicast مشابه یکدیگر می‌باشند. در هر دوی این آدرس‌ها، از ۴۸ بیت ابتدایی برای تعیین پیشوند آدرس استفاده می‌شود. در آدرس‌های global، ۱۶ بیت مربوط به فیلد SLA ID برای شناسایی زیرشبکه در سازمان به کار می‌رود که معادل این فیلد در آدرس‌های Site-local، ۱۶ بیت مربوط به Subnet ID می‌باشد. ۶۴ بیت باقیمانده نیز برای تعیین اینترفیس شبکه به کار گرفته می‌شود. ساختار آدرس‌های Site-local در شکل زیر نشان داده شده است.



شکل ۱-۲۵

آدرس FEC0::2731:E2FF:FE96:C283/64 (۶۴، تعداد بیت‌ها تا قبل از رسیدن به بخش اینترفیس را مشخص می‌نماید) نمونه‌ای از آدرس global در IPv6 می‌باشد. معادل دودویی قسمت اول این آدرس 1111 1110 1100 0000 است که در آن ۱۰ بیت اول دارای مقدار 1111 1110 11 می‌باشند. دو آدرس زیر، نمونه دیگری در این رابطه می‌باشند.

FEC0::1111:2731:E2FF:FE96:C283/64

FEC0::2222:97A4:E2FF:FE1C:E2D1/64

#### ۴. آدرس‌های Special unicast

آدرس‌های Special دارای کاربردهای خاصی می‌باشند. این آدرس‌ها به دو دسته تقسیم می‌شوند:

• **Unspecified:** این آدرس بصورت 0:0:0:0:0:0:0:0 یا به اختصار :: نشان داده می‌شود و زمانی که

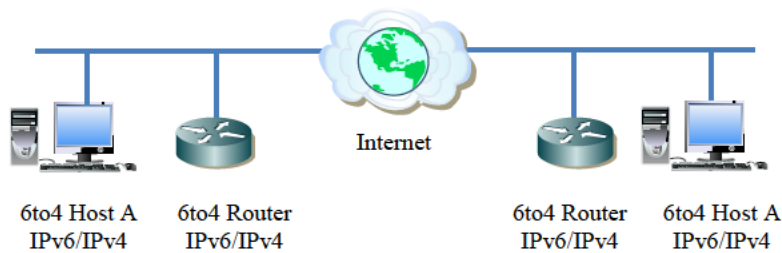
هیچ آدرسی به یک اینترفیس اختصاص داده نشود، از آن استفاده می‌گردد. در واقع این آدرس به معنای عدم وجود آدرس IP در یک اینترفیس می‌باشد. دقت داشته باشید که این آدرس را نمی‌توان به عنوان مقصد یک ارتباط در شبکه اختصاص داد (این آدرس معادل 0.0.0.0 در IPv4 است).

- **Loopback address:** این آدرس بصورت 0:0:0:0:0:0:0:1 یا 1:: نشان داده می‌شود و برای انجام تست‌های loopback مورد استفاده قرار می‌گیرد. Loopback به یک اینترفیس اجازه می‌دهد که بسته‌های IP را به خود ارسال نماید (این آدرس معادل 127.0.0.1 در IPv4 می‌باشد).

#### ۵. آدرس‌های سازگار یا Compatible

ایده مهاجرت از IPv4 به IPv6 باعث شد تا آدرس‌هایی جهت وجود همزمان این دو نوع آدرس ایجاد شوند. این آدرس‌ها ترکیبی از هر دو نوع IPv4 و IPv6 می‌باشد و به سه دسته تقسیم می‌شوند:

- **IPv4-compatible:** این آدرس بصورت 0:0:0:0:0:w.x.y.z یا w.x.y.z:: بوده که در آن w.x.y.z معادل نقطه-دهدهی آدرس IPv4 می‌باشد. از این آدرس در مواردی که گره‌ها با استفاده از یک زیرساخت IPv4 با IPv6 ارتباط برقرار می‌کنند (که به این میزبان‌ها Dual-stack nodes) گفته می‌شود. در واقع این گره‌ها از هر دو پروتکل IPv4 و IPv6 در ارتباط خود استفاده می‌نمایند. زمانی که یک گره با IPv4 بسته‌ای را به میزبان دیگری با IPv6 در مقصد ارسال می‌نماید، ترافیک IPv6 بطور خودکار با سرآیند IPv4 کپسوله شده و به مقصد ارسال می‌شود.
- **IPv4-mapped:** این آدرس به صورت 0:0:0:0:FFFF:w.x.y.z یا FFFF:w.x.y.z:: بوده و برای نشان دادن ارتباط یک گره IPv4 به یک گره IPv6 استفاده می‌شود. این آدرس نمی‌تواند به عنوان یک مبدأ یا مقصد برای بسته‌های IPv6 قرار گیرند. در پروتکل IPv6 استفاده از این آدرس‌های IPv4-mapped پشتیبانی نمی‌شود.
- **6to4:** این آدرس برای برقراری ارتباط میان دو گره، یکی با IPv4 و دیگری با IPv6، در اینترنت مورد استفاده قرار می‌گیرد. فرمت این آدرس به صورت ترکیبی از پیشوند 2002::/16 با ۳۲ بیت از آدرس IPv4 (عمومی) گره می‌باشد که در مجموع یک آدرس ۴۸ بیتی را تشکیل می‌دهند. به عنوان مثال اگر آدرس میزبان به صورت 131.107.0.1 (مبنای دو: 1000 0011.0110 1011.0000 0000.0000 0001) باشد، آدرس 6to4 معادل با آن برابر است با 2002:836B:1::/48. ساختار شبکه‌هایی که از آدرس‌های 6to4 استفاده می‌کنند شبیه شکل ۱-۲۶ می‌باشد.



شکل ۱-۲۶

## ۶. آدرس‌های NSAP

قبل از ایجاد مدل TCP/IP، شبکه اولیه ARPANET از مدل OSI در ارتباطات خود استفاده می‌نمود. در این شبکه، به جای استفاده از آدرس‌های IP از آدرس‌هایی تحت عنوان NSAP<sup>۱</sup> استفاده می‌شد. به عنوان مثال آدرس 49.0002.1921.6800.1024.00 از نوع NSAP می‌باشد. در این آدرس عدد ۴۹ بیانگر نوع شبکه بوده و می‌تواند با اعداد ۰ تا ۹۹ مقداردهی شود. چهار رقم بعدی شماره زیرشبکه را مشخص می‌نمایند. رقم‌های هفت تا هجده مربوط به آدرس فیزیکی MAC و دو رقم آخر نیز بیانگر نوع دستگاه در شبکه می‌باشند (۰۰: مسیریاب، ۰۱: سوئیچ، ۰۲: فایروال). این آدرس‌ها دارای طول ثابتی نیستند و در بعضی موارد تا ۲۰ بایت یا ۱۶۰ بیت نیز مقداردهی می‌شوند.\*

## آدرس‌های Multicast

آدرس‌های multicast امکان ارسال بسته‌ها به تعداد مشخصی از میزبان‌ها در شبکه را فراهم می‌کنند. در IPv4 نوعی از آدرس‌ها با نام آدرس‌های Broadcast وجود دارد که به کمک آن می‌توان یک بسته را به تمام میزبان‌ها در شبکه ارسال نمود. این آدرس‌ها در IPv6 وجود ندارند ولی عملکرد آنها توسط آدرس‌های multicast پیاده‌سازی می‌شود. آدرس‌های multicast با نام “آدرس‌های یک به چند”<sup>۲</sup> نیز شناخته می‌شوند. پیشوند شروع آدرس‌های multicast به صورت FF می‌باشد، بنابراین مقدار فیلد FP در آنها برابر است با 1111 1111. دامنه این آدرس‌ها از FF00 تا FFFF می‌باشد و نمی‌توان آنها را به میزبان‌ها اختصاص داد. در شکل زیر، ساختار آدرس‌های multicast نشان داده شده است.



شکل ۱-۲۷

1. One-to-many
2. Network Service Access Point

\* جهت کسب اطلاعات بیشتر در این زمینه می‌توانید به RFC 1888 مراجعه نمایید.

فیلدهای تشکیل‌دهنده این آدرس به شرح زیر می‌باشند:

- ♦ **Flags (پرچم):** این فیلد حاوی یک سری اطلاعات کنترلی راجع به آدرس IP می‌باشد. همانطور که در RFC 2373 آمده است، تنها Flag ای که تا کنون در این فیلد تعریف شده است، Transient (T) می‌باشد. پرچم T از بیت کم ارزشتر (بیت سمت راست) فیلد Flag استفاده می‌نماید و می‌تواند دو مقدار اختیار کند. اگر مقدار این پرچم 0 باشد، آدرس Multicast بطور دائم و توسط سازمان IANA اختصاص داده شده است. چنانچه مقدار پرچم 1 باشد، به این معناست که آدرس multicast به صورت موقتی اختصاص داده شده و می‌تواند در آینده تغییر کند.\*
- ♦ **Scope:** در این فیلد، ناحیه‌ای که بسته‌های IPv6 به صورت multicast به آن فرستاده می‌شوند، تعیین می‌شود. مسیریاب‌ها، علاوه بر اطلاعاتی که توسط پروتکل‌های مسیریابی بدست می‌آورند، از اطلاعات این فیلد نیز جهت تعیین محدوده multicast و اینکه آیا این بسته‌ها باید به بیرون از شبکه فعلی انتقال داده شوند، استفاده می‌کنند. در جدول ۱-۱۲ محدوده‌های تعریف شده در RFC 2373 برای آدرس‌های multicast آورده شده است.

جدول ۱-۱۲: مقادیر فیلد Scope در آدرس‌های Multicast

مقدار	Scope (محدوده)
1	Node-local
2	Link-local
5	Site-local
8	Organization local
E	Global

- ♦ **Groupe ID:** این فیلد شناسه گروه multicast را مشخص نموده و برای هر Scope منحصر بفرد می‌باشد. طول این فیلد ۱۱۲ بیت است. در آدرس‌های multicast دائمی، شناسه گروه مستقل از شناسه Scope است ولی در آدرس‌های موقت، این شناسه با شناسه Scope در ارتباط است. آدرس‌های multicast از FF01:: تا FF0F:: رزرو شده هستند و نمی‌توان آنها را به اینترنتیسی اختصاص داد.

برای شناسایی تمام میزبان‌ها در یک ناحیه Node-local و Link-local، آدرس‌های multicast زیر تعریف شده‌اند:

\* جهت آگاهی از آدرس‌های اختصاص داده شده توسط IANA به وبسایت [www.iana.org](http://www.iana.org) مراجعه نمایید.

FF01::1 (node-local scope all-nodes address)

FF02::1 (link-local scope all-nodes address)

همچنین برای شناسایی تمام مسیرهای در ناحیه‌های Node-local، Link-local و Site-local آدرس‌های زیر تعریف شده است:

FF01::2 (node-local scope all-routers address)

FF02::2 (link-local scope all-routers address)

FF05::2 (site-local scope all-routers address)

### آدرس‌های Anycast

یک آدرس anycast به گروهی از اینترفیس‌ها در شبکه اختصاص داده می‌شود ولی هنگامی که بسته‌ای به این آدرس فرستاده می‌شود، تنها توسط یکی از آنها که نزدیکترین اینترفیس است دریافت می‌شود. برخلاف آدرس‌های multicast که در ارتباطات یک به چند استفاده می‌شوند، از آدرس‌های anycast در ارتباطات یک به یک استفاده شده و بسته IP از یک اینترفیس به دیگری ارسال می‌گردد. آدرس‌های anycast فقط به عنوان آدرس مقصد و در مسیرهای قابل استفاده می‌باشند. این آدرس‌ها، از آدرس‌های unicast گرفته می‌شوند و محدوده (Scope) تحت پوشش آنها نیز جزئی از محدوده آدرس unicast است که آدرس anycast از آن گرفته شده است.

جهت اختصاص یک آدرس anycast به مسیرهای موجود در قسمت پیشوند شبکه در مقدار فعلی خود ثابت مانده و تمام بیت‌های باقیمانده (SubnetID) با صفر جایگزین می‌شوند. به عنوان مثال اگر آدرس شبکه برابر با 2001:4375:0001:0015/64 باشد، آدرس anycastی که در آن استفاده می‌شود به صورت 2001:4375:0001:0015.0000.0000.0000.0000 یا 2001:4375:1:15:: خواهد بود. اکنون چنانچه این آدرس را بروی چندین مسیر تنظیم نمایید، اگر بسته‌ای به این آدرس فرستاده شود، نزدیکترین مسیر به آنرا دریافت می‌نماید. با این روش می‌توان یک مسیریابی کارآمد در اختیار داشت زیرا بسته ارسالی، به سرعت توسط نزدیکترین مسیر دریافت شده و مدت زیادی در شبکه سرگردان نمی‌ماند.



## « فصل ۲ »

نصب و ارتقاء به ویندوز سرور  
2008 R2

**Installing and Upgrading to  
Windows Server 2008 R2**





شاید اولین آزمون جهت فراگیری و کار با ویندوز سرور 2008 و 2008R2، نصب آن بر روی یک سیستم است که این سیستم می‌تواند یک ماشین فیزیکی و یا ماشینی مجازی<sup>۱</sup> باشد. عملیات نصب به دو روش دستی<sup>۲</sup> و خودکار قابل انجام است که البته انتخاب روش آن اختیاری است و به شرایط و محیط مورد نظر بستگی دارد.

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

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

## ۲-۱ تغییرات نصب نسبت به ویندوز سرور 2000 و 2003

عملیات نصب در ویندوز سرور 2008R2 بسیار راحت‌تر از نسخه‌های قبلی آن (2000 و 2003) شده است. بسیاری از افراد زمانی که عبارت “نصب ویندوز سرور” را می‌شنوند، عملیاتی پیچیده در ذهنشان مجسم می‌گردد در صورتی که اینگونه نخواهد بود. اگر این افراد قبلاً یکی از ویندوزهای ویستا یا ویندوز ۷ را نصب کرده باشند، آنگاه متوجه خواهند شد که نصب ویندوز سرور 2008R2 نه تنها پیچیده نیست، بلکه بسیار ساده و لذت بخش می‌باشد. در هنگام نصب ویندوز سرور 2000 و 2003 سؤالات زیادی به منظور انجام تنظیمات و یا راه اندازی قابلیت‌ها از شما پرسیده می‌شود، اما در نسخه 2008R2، این سؤالات به حداقل رسیده است که این امر به لحاظ ایجاد امنیت بیشتر در هنگام نصب می‌باشد.

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

---

1. Virtual Machine  
2. Manual

شاید سؤال دیگری که ممکن است برایتان پیش آید، این است که نصب سرویس‌ها و عملکردهای کمتر، به معنی انجام کار بیشتر پس از نصب ویندوز می‌باشد. اما جای نگرانی نیست زیرا به کمک Group Policyها و ابزار Server Manager، نصب و راه اندازی این قابلیت‌ها بسیار آسان شده است.

## ۲-۲ نیازمندی‌های نصب ویندوز سرور 2008 و 2008R2

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

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

جدول ۱-۲: نیازمندی‌های ویندوز سرور 2008

سخت افزار	حداقل	پیشنهاد شده	حداکثر
CPU	1GHz برای پردازنده‌های x86 و 1.4GHz برای پردازنده‌های x64	2 GHz	۴ پردازنده برای ویرایش Standard ۸ پردازنده برای ویرایش Enterprise ۳۲ پردازنده برای Datacenter (x84) ۶۴ پردازنده برای Datacenter (x64)
RAM	512 MB	2 GB یا بیشتر	4GB برای Standard (x86) 32GB برای Standard (x64) 64GB برای Enterprise و Datacenter (x84) 2TB برای Enterprise و Datacenter (x64) و Itanium

	40GB به اضافه فضایی برای برنامه‌ها و داده- ها	10GB	Disk
		به دلیل اینکه نصب از روی DVD انجام می‌شود نیاز است (از CD-ROM پشتیبانی نمی‌شود)	DVD-ROM
		Super-VGA (800-600) یا بالتر	Display
		صفحه کلید و ماوس	Input Devices

جدول ۲-۲: نیازمندی‌های ویندوز سرور 2008R2

سخت افزار	حداقل	پیشنهاد شده	حداکثر
CPU	1.4GHz	2 GHz	۴ پردازنده برای ویرایش Standard ۸ پردازنده برای ویرایش Enterprise ۶۴ پردازنده برای ویرایش Datacenter
RAM	512 MB	2 GB یا بیشتر	32GB برای ویرایش Standard 2TB برای ویرایش‌های Enterprise، Datacenter و Itanium
Disk	10GB	40GB به اضافه فضایی برای برنامه‌ها و داده‌ها	
DVD-ROM	به دلیل اینکه نصب از روی DVD انجام می‌شود نیاز است.		

		یا Super-VGA (800-600) بالتر	Display
		صفحه کلید و ماؤس	Input Devices



### پشتیبانی ۶۴ بیتی

اگر تا به حال با ویندوز ویندوز سرور 2003 و 2008 کار کرده باشید، حتماً شنیده‌اید که این دو ویندوز در دو نسخه ۳۲ و ۶۴ بیتی موجود می‌باشند. منظور از x64 نسخه‌های ۶۴ بیتی و منظور از x86 نسخه‌های ۳۲ بیتی از نرم‌افزارها (یا سیستم‌عامل‌ها) می‌باشند. سیستم عامل ویندوز سرور 2008R2 و برنامه‌هایی مانند Microsoft Exchange Server 2007 فقط به صورت ۶۴ بیتی یا x64 هستند.

لازم است نکاتی را در رابطه با راه‌اندازی سرورهای ۶۴ بیتی یادآور شویم:

- ♦ پشتیبانی سخت افزارها از x64 مسئله بزرگی نیست. بسیاری از تولید کنندگان، سال‌های زیادی است که پردازنده‌های x64 را به عنوان یکی از محصولات اصلی خود، تولید می‌کنند. بنابراین آگاهی از این موضوع که سخت افزار شما از ۶۴ بیت پشتیبانی می‌کند، کار سختی نیست.
- ♦ بسیاری از برنامه‌های ۳۲ بیتی قادرند بر روی ویندوز ویندوز سرور 2008R2 اجرا شوند. به کمک زیرسیستمی به نام WOW32 امکان شبیه‌سازی اکثر نرم‌افزارهای ۳۲ بیتی، و اجرای آنها بر روی ویندوز سرور 2008R2 فراهم شده‌است.
- ♦ امکان ارتقاء x86 به x64 وجود ندارد. در صورتی که سرور 2003 و یا 2008 شما، بر روی پردازنده‌های x86 قرار دارند، نمی‌توانید آنها را به 2008R2 ارتقاء دهید و باید سخت افزارهای x64 تهیه کنید.
- ♦ درایورهای سخت افزاری شما باید متناسب با سیستم عامل باشند. لازم است قبل از نصب سخت افزارها و درایورهای مربوط به آن، از سازگاری آنها با سیستم عامل جدید اطمینان حاصل کنید تا در استفاده از آنها با مشکل مواجه نشوید.

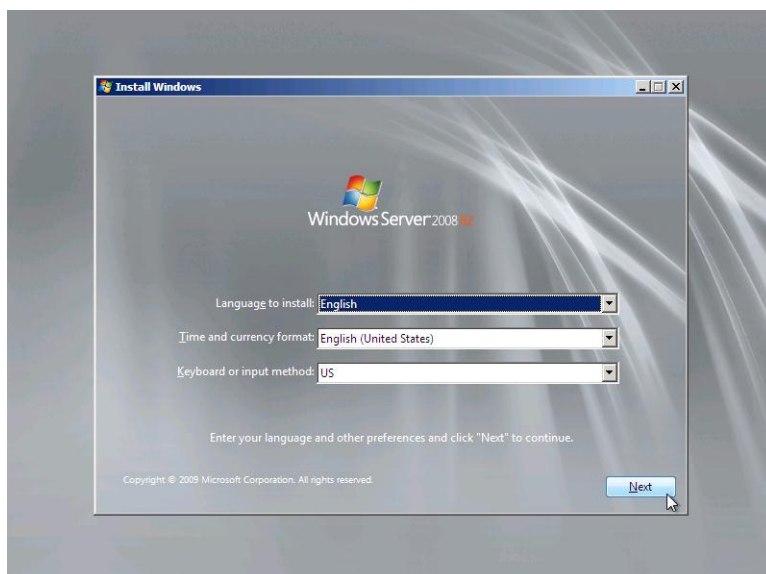
همانطور که قبلاً اشاره شد، نصب ویندوز سرور 2008 و 2008 R2 بسیار ساده است. بطور کلی عملیاتی که برای نصب باید انجام شود عبارتند از:

- ♦ بوت کردن سیستم از روی DVD ویندوز سرور 2008R2
- ♦ وارد نمودن کد License
- ♦ انتخاب ویرایش ویندوز
- ♦ انتخاب یکی از عملیات “نصب” یا “ارتقاء”<sup>۲</sup>
- ♦ پیکربندی فضای دیسک (هارد دیسک)
- ♦ تنظیم رمز عبور برای ورود مدیر
- ♦ ورود به سیستم

## ۲-۲ نصب دستی سیستم عامل

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

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



شکل ۱-۲

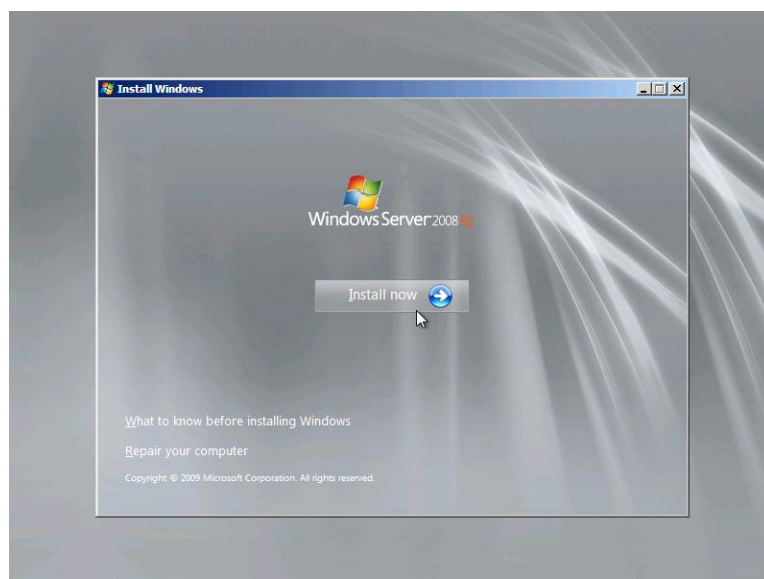
همانطور که در شکل ۲-۱ مشاهده می‌کنید، در این صفحه سه گزینه در اختیار شما قرار داده می‌شود:

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

پس از انجام تنظیمات مورد نظر، بر روی Next کلیک کنید.

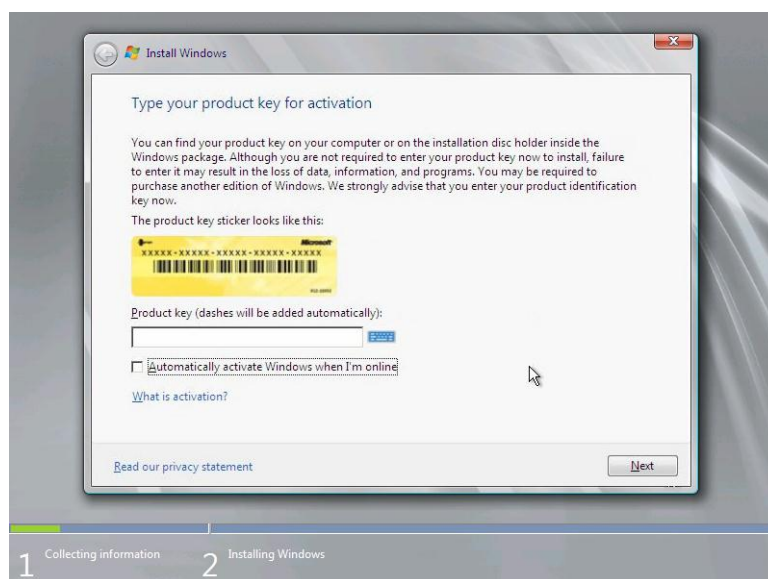
۲. با ورود به مرحله جدید، مجدداً با چند گزینه مواجه خواهید شد. این گزینه‌ها عبارتند از:

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



شکل ۲-۲

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

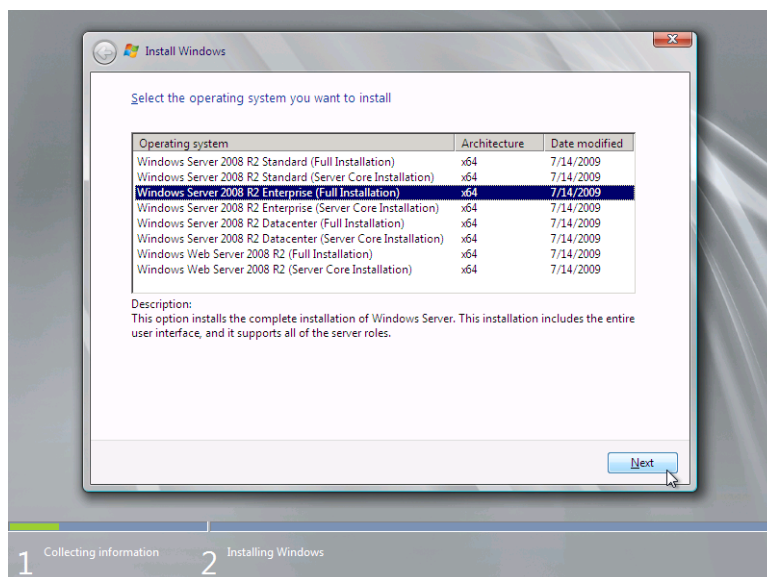


شکل ۲-۳

۴. در صفحه "Select the operating system you want to install" باید ویرایشی<sup>۱</sup> از ویندوز سرور 2008 R2 که قصد دارید آنرا بر روی سیستم نصب کنید، انتخاب نمایید. در اینجا، چهار ویرایش قابل انتخاب است که عبارتند از: Standard، Enterprise، Datacenter و Web Server. هر ویرایش از قابلیت‌ها و ویژگی‌های خاص برخوردار است و باید با توجه به عملکرد سرور و سخت‌افزارهای آن، ویرایش مورد نظر را انتخاب نمایید. دقت داشته باشید که هر ویرایش به دو دسته Full Installation و Server Core Installation تقسیم می‌شود. در دسته اول (Full Installation)، حجم زیادی از ابزارها و واسطه‌های گرافیکی در اختیار خواهید داشت که مدیریت ویندوز را برای شما آسانتر می‌کند، اما در دسته دوم (Server Core Installation) فرض بر این است که شما جزء کاربران خط فرمان<sup>۲</sup> هستید و بیشتر با کدها و دستورات، اعمال مدیریتی را انجام می‌دهید. بنابراین در این حالت، از واسطه‌های گرافیکی بسیار کمی استفاده شده است. یکی از ویرایش‌های Standard یا Enterprise (Full Installation) را انتخاب و بر روی Next کلیک کنید.

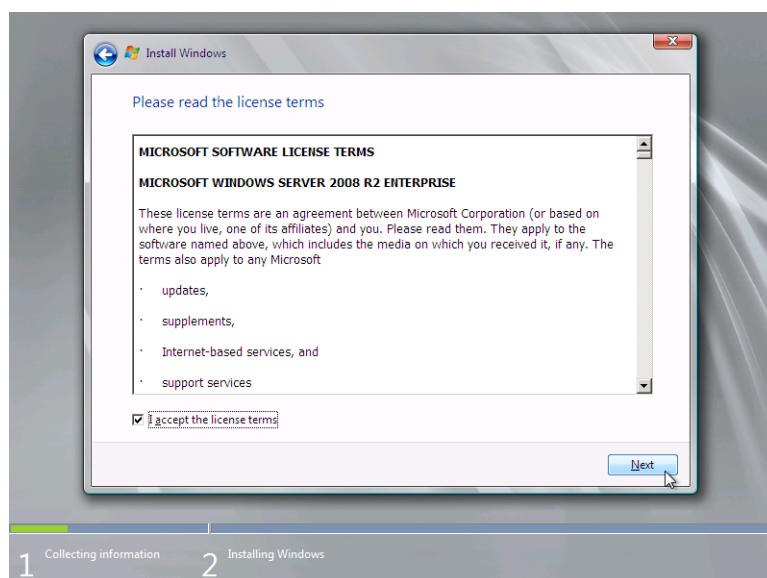
1. Edition





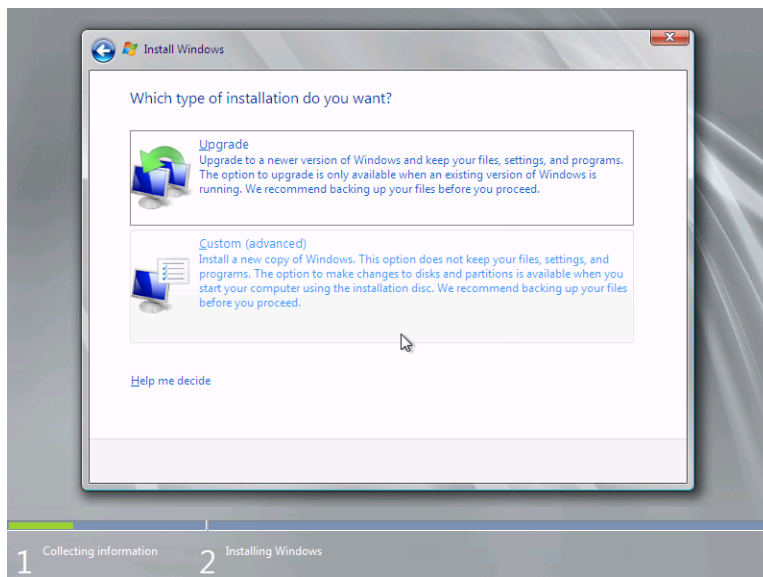
شکل ۲-۴

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



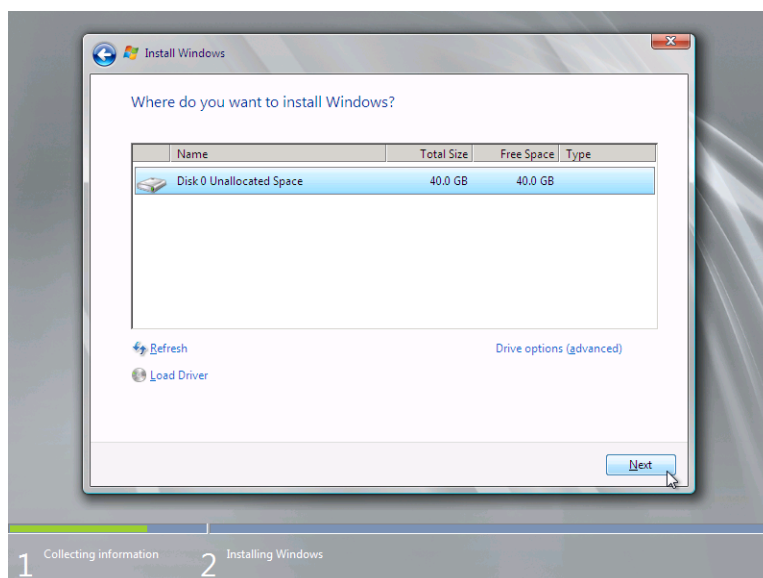
شکل ۲-۵

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



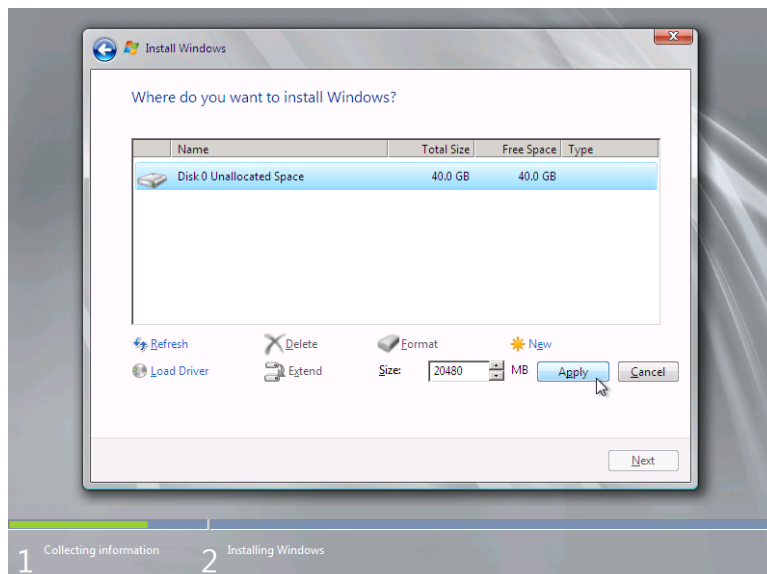
شکل ۶-۲

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



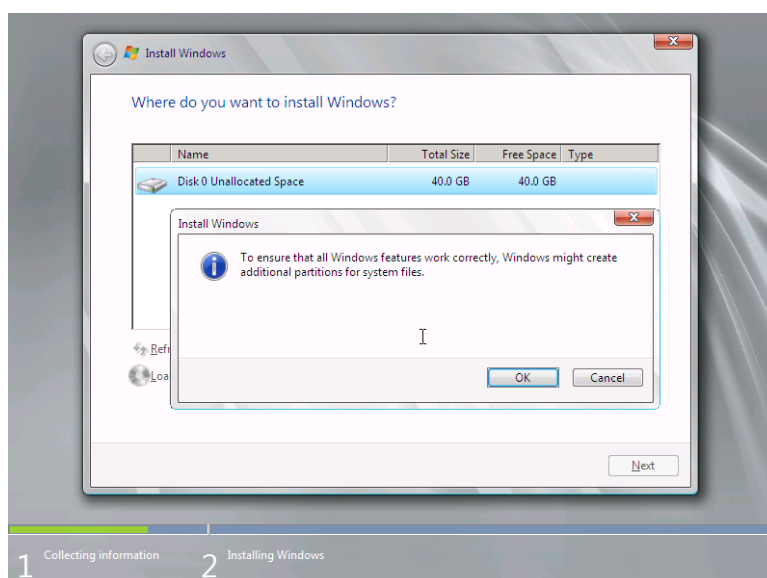
شکل ۷-۲

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



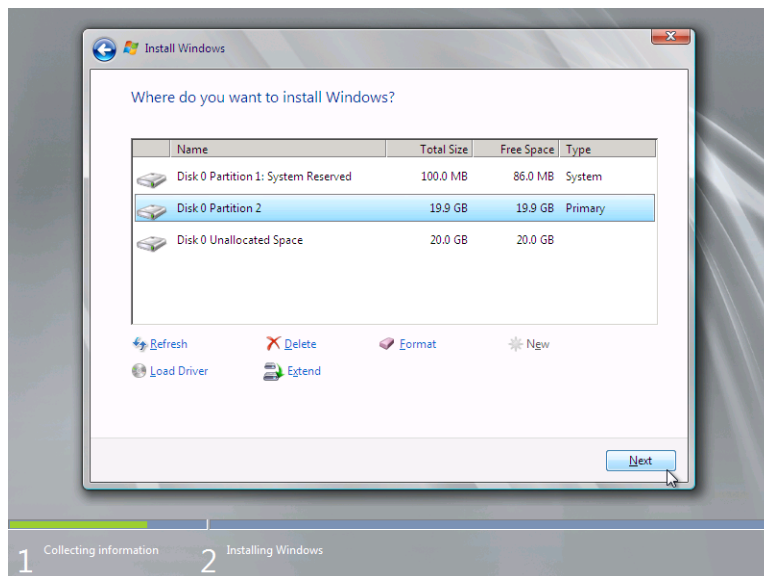
شکل ۸-۲

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



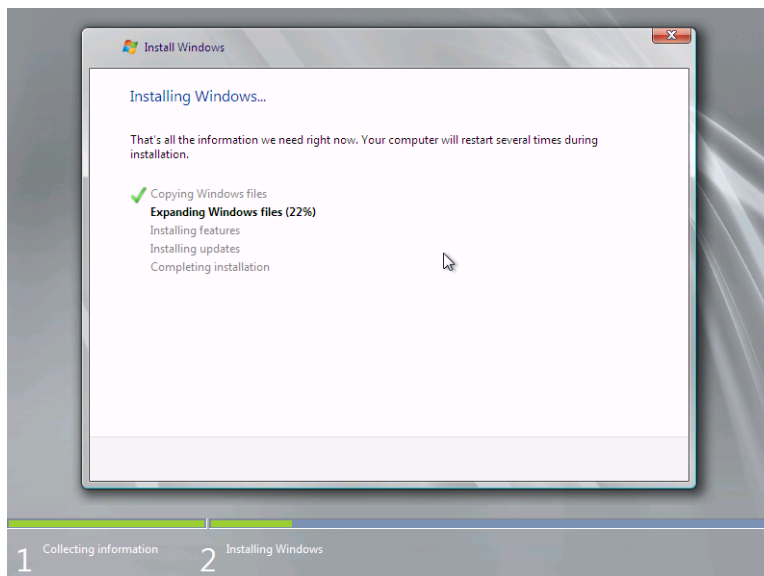
شکل ۹-۲

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



شکل ۱۰-۲

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



شکل ۱۱-۲

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



شکل ۱۲-۲

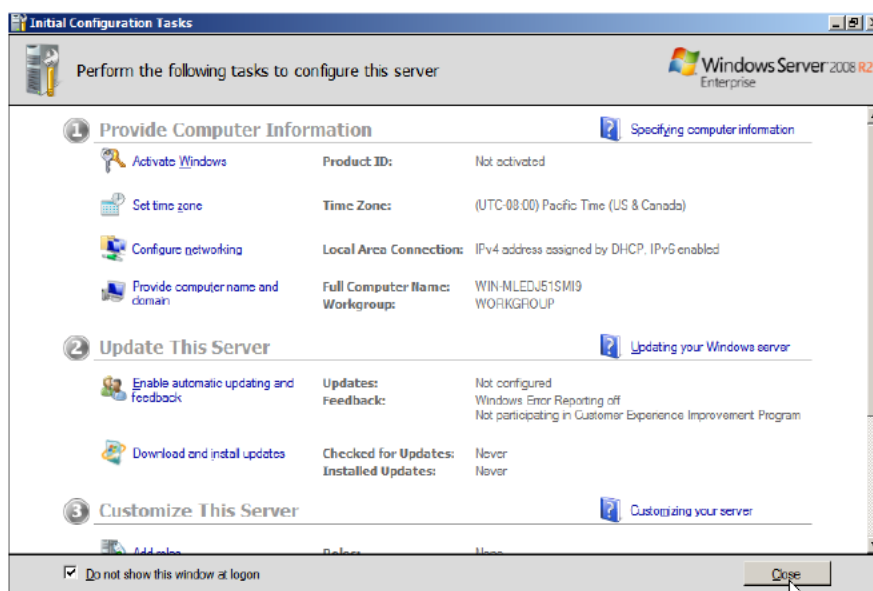
۱۳. با مشاهده صفحه زیر، در قسمت‌های مشخص شده رمز عبور یکسانی وارد نموده و بر روی دکمه جهتی (→) کلیک کنید. دقت کنید که رمز عبور باید حداقل ترکیبی از هشت یا نه کاراکتر و متشکل از حروف بزرگ، حروف کوچک و اعداد باشد (از کاراکترهایی مانند @ نیز می‌توان استفاده نمود).



شکل ۱۳-۲

۱۴. پس از انتخاب رمز عبور، قادر خواهید بود به عنوان مدیر<sup>۱</sup> وارد سیستم شوید. توجه داشته باشید که اولین ورود شما به داخل سیستم ممکن است کمی طول بکشد، این امر به دلیل آماده‌سازی تنظیمات شما و برخی از آیتم‌های موجود در Desktop می‌باشد.

۱۵. بعد از ورود کامل به سیستم و مشاهده دسکتاپ، پنجره‌ای تحت عنوان Initial Configuration Tasks نشان داده خواهد شد. در این پنجره، ابزارهایی جهت پیکربندی<sup>۲</sup> اولیه سرور قرار داده شده است و به کمک آنها می‌توانید سرور را به صورت ابتدایی پیکربندی کنید، اما پیشنهاد ما این است که این کار را به کمک Server Manager انجام دهید (این ابزار، از طریق منوی Start یا خط فرمان (Cmd) قابل دسترسی می‌باشد. در همین فصل، نحوه کار با Server Manager را شرح خواهیم داد).



شکل ۲-۱۳

محیط گرافیکی واسطه‌های موجود در ویندوز سرور 2008R2، متفاوت از ویندوز سرور 2008 می‌باشد. دلیل این امر، این است که محیط ویندوز سرور 2008، بر مبنای محیط ویندوز ویستا بوده، در حالی که محیط ویندوز سرور 2008R2 بر اساس ویندوز ۷ می‌باشد. این تفاوت با نگاهی ساده به آیکن‌های موجود در این سیستم عامل‌ها قابل مشاهده است (حتی می‌توان ظاهر ویندوز سرور 2008R2 را شبیه ویندوز ۷ نمود و برعکس).

1. Administrator
2. Configuration

## ۲-۴ ارتقاء ویندوز سرور

استفاده از ویندوز سرور، همیشه محدود به نصب کامل آن نیست، بلکه گاهی اوقات نیاز است تا یک سیستم عامل موجود را جهت سازگاری با برنامه‌ها و افزایش کارایی، ارتقاء دهیم. البته پیشنهاد مایکروسافت این است که سازمان‌ها تا جایی که امکان دارد، از ارتقاء سیستم عامل دوری کنند و سیستم‌عامل را بطور کامل نصب کنند. اما در بعضی شرایط، نصب کامل ویندوز، مشکل و یا پرهزینه است. مثلاً سازمانی کوچک را در نظر بگیرید که به دلیل نداشتن بودجه کافی، قادر به خرید یک سرور جدید نیست. یا حالتی را در نظر بگیرید که با یک سازمان مهم و حساس روبرو هستیم و از کار افتادن سرورها و برنامه‌های موجود بر روی آن، این سازمان را متحمل هزینه‌های زیادی خواهد نمود. بنابراین، کاری که این سازمان‌ها می‌توانند انجام دهند، ارتقاء سرور یا سرورهای فعلی می‌باشد. اما ارتقاء سرور به کمک ویندوز سرور 2008R2 چگونه امکان‌پذیر است؟ آیا می‌توان هر سروری را به 2008R2 ارتقاء داد؟ دانستن پاسخ چنین سؤالاتی مهم و ضروری است زیرا تعیین می‌کند که آیا امکان ارتقاء و کاهش هزینه‌ها وجود دارد یا خیر. قبلاً گفتیم که ویندوز سرور 2008R2، ویندوزی ۶۴ بیتی است و به سخت افزارهای ۶۴ بیتی (x64) نیاز دارد. بنابراین قبل از ارتقاء باید مطمئن شوید که سخت افزار شما از ۶۴ بیت پشتیبانی می‌کند. مسئله بعدی، در مورد نوع سیستم‌عامل و ویرایش‌هایی است که می‌توانند به یکدیگر ارتقاء پیدا کنند. به عنوان مثال، باید دید که آیا می‌توان ویرایش Standard از ویندوز سرور 2003 را به ویرایش استاندارد از 2008 یا 2008R2 ارتقاء داد یا خیر. در جداول ۲-۳ و ۲-۴، امکان ارتقاء ویرایش‌های مختلف از ویندوز سرور به یکدیگر نشان داده شده است.

جدول ۲-۳: امکان ارتقاء به ویندوز سرور 2008

سیستم عامل فعلی	ارتقاء پشتیبانی شده
Windows 2003 R2 Standard	Windows 2008 Standard
Windows 2003 Standard _ Service Pack 1	
Windows 2003 Standard _ Service Pack 2	
Windows 2003 R2 Enterprise	Windows 2008 Enterprise
Windows 2003 Enterprise _ Service Pack 1	
Windows 2003 Enterprise _ Service Pack 2	
Windows 2003 Standard _ Service Pack 1	
Windows 2003 Standard _ Service Pack 2	
Windows 2003 R2 Datacenter	Windows 2008 Datacenter
Windows 2003 Datacenter _ Service Pack 1	
Windows 2003 Datacenter _ Service Pack 2	
Windows 2003 Enterprise _ Service Pack 1	
Windows 2003 Enterprise _ Service Pack 2	

جدول ۲-۴: امکان ارتقاء به ویندوز سرور 2008 R2

سیستم عامل فعلی	ارتقاء پشتیبانی شده
Windows 2003 R2 Standard	Windows 2008 R2 Standard
Windows 2008 Standard _ Service Pack 1	
Windows 2008 Standard _ Service Pack 2	
Windows 2003 R2 Standard	Windows 2008 R2 Enterprise
Windows 2003 Standard _ Service Pack 2	
Windows 2003 R2 Enterprise	
Windows 2003 Enterprise _ Service Pack 2	
Windows 2008 Standard _ Service Pack 1	
Windows 2008 Standard _ Service Pack 2	
Windows 2008 Enterprise _ Service Pack 1	
Windows 2008 Enterprise _ Service Pack 2	
Windows 2003 R2 Datacenter	Windows 2008 R2 Datacenter
Windows 2003 Enterprise _ Service Pack 2	
Windows 2003 Datacenter _ Service Pack 2	
Windows 2008 Enterprise _ Service Pack 1	
Windows 2008 Enterprise _ Service Pack 2	
Windows 2008 Datacenter _ Service Pack 1	
Windows 2008 Datacenter _ Service Pack 2	

قبل از ارتقاء ویندوز سرور، لازم است نکاتی را یادآور شویم:

- ♦ ارتقاء از x86 به x64 و یا برعکس، امکان پذیر نیست.
- ♦ امکان ارتقاء مستقیم ویندوز سرور 2000 وجود ندارد. بنابراین باید ابتدا آنرا به 2003 و سپس به 2008 ارتقاء دهید.
- ♦ امکان ارتقاء از سرور 2003 به ویرایش هسته (Core Server) ویندوز سرور 2008R2 امکان پذیر نمی باشد.
- ♦ امکان مهاجرت از ویرایش های ویندوز سرور 2008R2 به ویرایش Server Core وجود ندارد.
- ♦ همیشه ارتقاء از ویرایش های پایین تر به ویرایش های بالاتر امکان پذیر است. ویرایش های قابل ارتقاء، به ترتیب از پایین به بالا: Standard « Enterprise « Datacenter).
- ♦ برای ارتقاء به هر نسخه از ویندوز، نیازمند خریداری کد License برای آن می باشید.
- ♦ قبل از ارتقاء به ویندوز سرور 2008R2، باید مطمئن شوید که برنامه های موجود بر روی سرور،

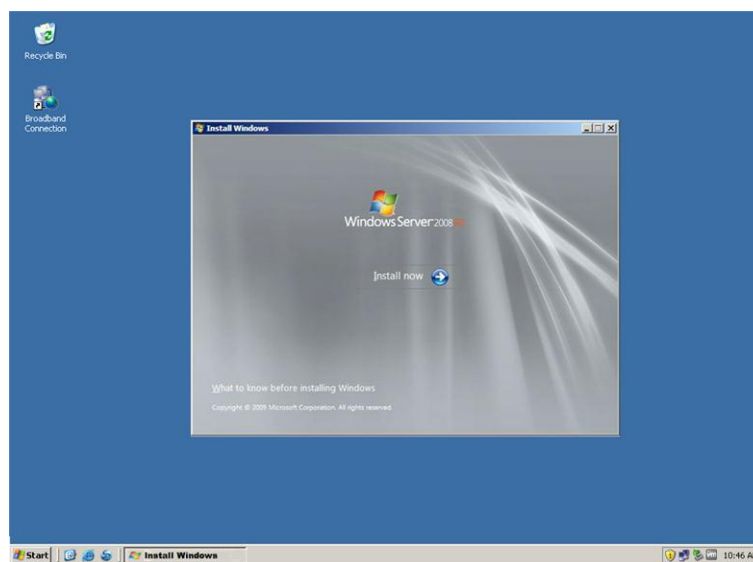


از آن پشتیبانی می‌کنند.

- از سالم بودن سخت‌افزارها قبل از انجام ارتقاء، اطمینان حاصل نمایید.
- اگر قصد ارتقاء یک سرور با داده‌ها و اطلاعات مهم را دارید، حتماً از آن Backup تهیه کنید.
- باید قبل از ارتقاء، Antivirus موجود بر روی سرور را غیر فعال و یا حذف نمایید، زیرا ممکن است سبب توقف عملیات در حین اجرا شود.

اکنون زمان آن رسیده است که مراحل کار را به صورت عملی نشان دهیم. در اینجا قصد داریم ویندوز سرور 2003 (x64) را به سرور 2008R2 ارتقاء دهیم. مراحل کار شبیه ارتقاء سرور 2003 (x86) به 2008 (x86) می‌باشد.

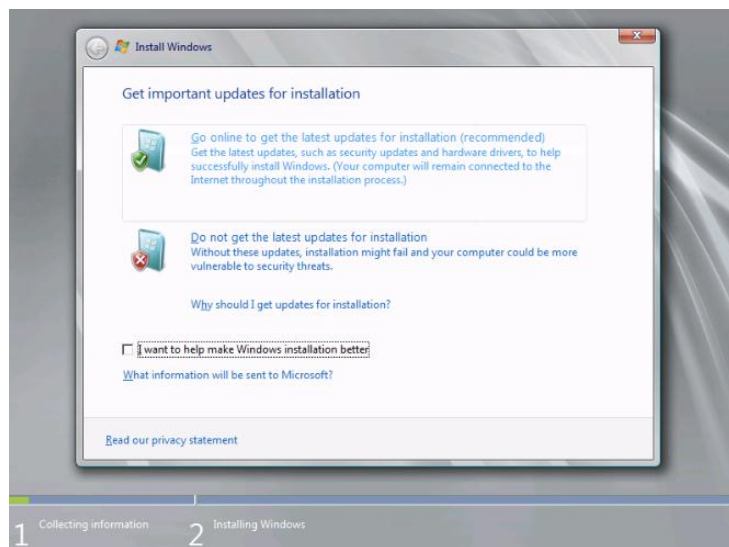
۱. ابتدا وارد سرور شده و سپس رسانه‌ای که قرار است عملیات از روی آن اجرا شود (معمولاً DVD) را قرار دهید. پس از قرار دادن رسانه مورد نظر، پنجره‌ای تحت عنوان “Install Windows” نمایش داده خواهد شد. در واقع این پنجره، همان پنجره ظاهر شده در هنگام نصب کامل ویندوز سرور 2008R2 می‌باشد با این تفاوت که گزینه Repair ویندوز از آن حذف شده است. دلیل این امر کاملاً واضح است، زیرا ویندوز را زمانی می‌توان با یک رسانه Repair نمود که از روی همان رسانه (یا نسخه‌ای یکسان) نصب شده باشد. در شکل زیر، این پنجره نشان داده شده است.



شکل ۲-۱۵

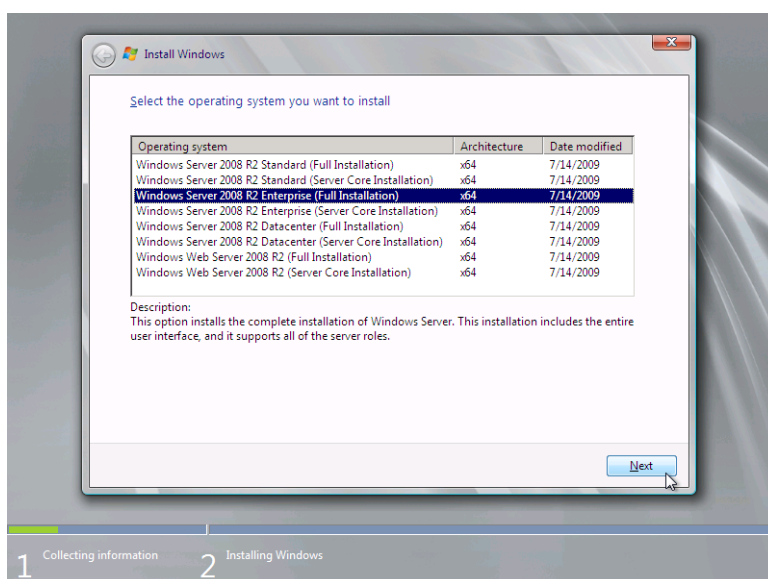
۲. بر روی “Install now” کلیک نموده تا به مرحله بعد وارد شوید. دقت داشته باشید که پس از کلیک بر روی این دکمه، محیط نصب، دوباره به همان محیط ویندوز سرور 2008R2 تبدیل می‌گردد.

۳. در صفحه "Get important updates for installation"، می‌توانید تعیین کنید که Update‌های جدید ویندوز از سایت مایکروسافت دریافت شوند یا خیر. گزینه دوم (Do not get the latest update ...) را انتخاب کنید.



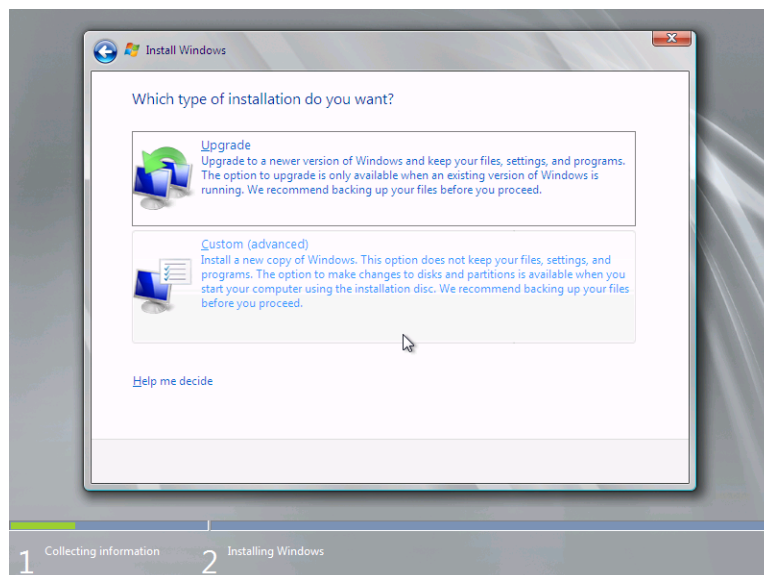
شکل ۲-۱۶

۴. در صفحه "Select the operating system you want to install" ویرایش ویندوز سرور 2008R2 را انتخاب (در اینجا Enterprise Full Installation) و بروی Next کلیک کنید.



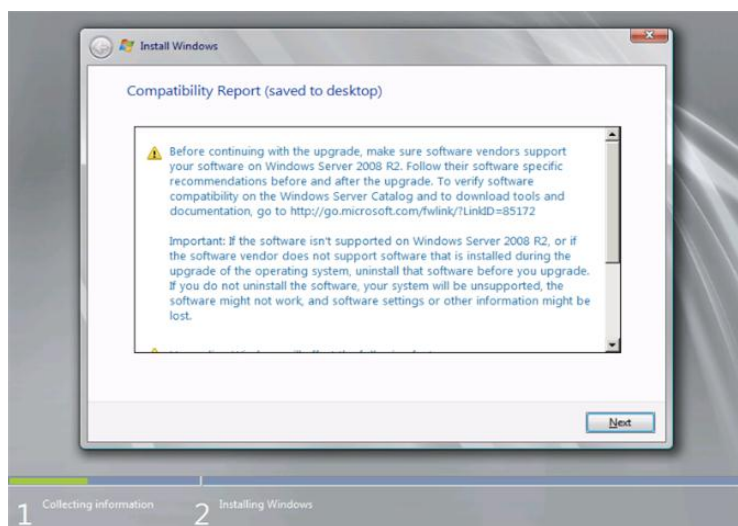
شکل ۲-۱۷

۵. در صفحه "Please read the license terms" گزینه I accept the license terms را انتخاب نموده و بر روی Next کلیک کنید (شکل ۲-۵).
۶. در صفحه "Which type of installation do you want" گزینه "Upgrade" را انتخاب کنید.



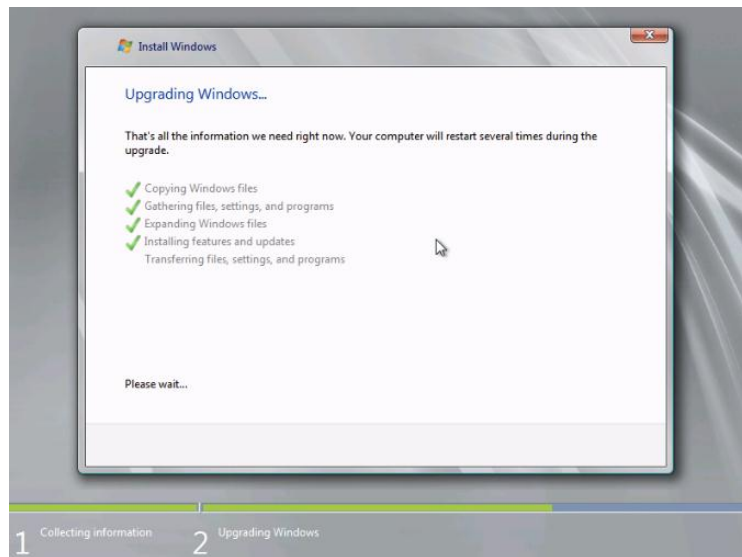
شکل ۲-۱۸

۷. در مرحله بعد، سازگاری سرور با ویندوز سرور 2008R2 بررسی شده و در صورتی که خطایی وجود داشته باشد، در صفحه "Compatibility Report" این خطاها به همراه توضیحاتی در مورد آن آورده می‌شود. بر روی Next کلیک کنید.



شکل ۲-۱۹

۸. با مشاهده صفحه "Upgrading Windows"، عملیات ارتقاء ویندوز آغاز می‌گردد. در طی این عملیات، ممکن است سیستم چند بار Restart شود، پس تا پایان عملیات منتظر بمانید.



شکل ۲-۲۰

۹. پس از اتمام عملیات و راه اندازی سرور، با صفحه زیر مواجه خواهید شد. سه کلید Alt, Ctrl, Delete را بطور همزمان فشار دهید تا به ویندوز وارد شوید.



شکل ۲-۲۱

در هنگام نصب کامل زمانی که اولین بار به ویندوز وارد می‌شوید، پنجره Initial Configuration Tasks نشان داده می‌شود، اما در هنگام ارتقاء به جای آن پنجره Server Manager نشان داده خواهد شد. در قسمت‌های قبل گفتیم که ویندوز سرور 2008R2 بطور پیش‌فرض هیچ سرویس و یا قابلیت را با خود نصب نمی‌کند. این موضوع در مورد ارتقاء نیز صدق می‌کند. اگر پس از ارتقاء ویندوز سرور، قابلیت نصب شده‌ای می‌بینید، اینها همان قابلیت‌هایی هستند که بر روی ویندوز سرور قبلی وجود داشته و مربوط به ویندوز جدید نمی‌باشند.

## ۲-۵ بررسی ابزارهای Initial Configuration Tasks

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

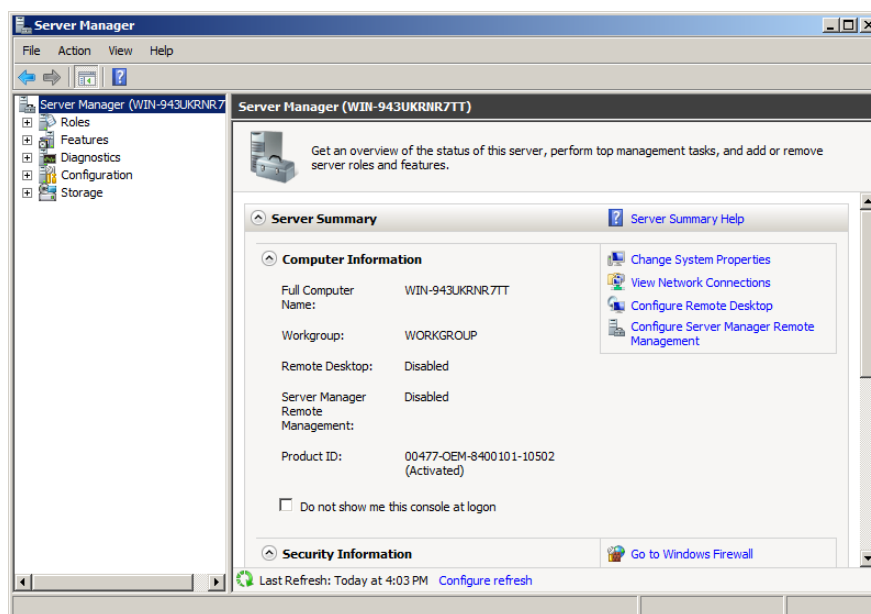
- ♦ **Active Windows:** هر نسخه از ویندوز، پس از نصب نیازمند فعال‌سازی<sup>۱</sup> می‌باشد. تا زمانی که ویندوز را فعال نکرده باشید، استفاده از تمام عملکردهای آن امکان‌پذیر نمی‌باشد (فعال‌سازی از طریق اینترنت، کد License و برنامه Genuine Microsoft امکان‌پذیر است).
- ♦ **Set time zone:** در این قسمت می‌توانید منطقه زمانی و تاریخ سرور را تنظیم کنید.
- ♦ **Configure networking:** به کمک این ابزار می‌توانید تنظیمات مربوطه جهت اتصال سرور به شبکه را انجام دهید.
- ♦ **Provide Computer Name and Domain:** این قسمت مربوط به انتخاب نام برای کامپیوترها و ایجاد Domain جهت اتصال کاربران شبکه به سرور می‌باشد.
- ♦ **Enable automatic updating and feedback:** در این قسمت می‌توانید امکان دریافت خودکار آپدیت‌های مهم و امنیتی مایکروسافت از طریق اینترنت را فعال کنید. البته این امکان به صورت دستی و یا به کمک Group Policy نیز امکان‌پذیر است.
- ♦ **Download and install updates:** به کمک این قسمت می‌توانید آپدیت‌ها را دریافت نموده و آنها را بر روی سرور نصب کنید.
- ♦ **Add roles:** امکان اضافه کردن سرویس‌ها و قابلیت‌های بیشتر به سرور را فراهم می‌نماید.
- ♦ **Add features:** این ابزار نیز جهت افزودن قابلیت‌ها به سرور استفاده می‌شود.
- ♦ **Enable Remote Desktop:** به کمک این ابزار قادر خواهید بود سرور خود را با استفاده از نرم افزار Remote Desktop کنترل کنید، البته به شرطی که سرور به شبکه متصل باشد.

1. Activation

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

## ۲-۶ پیکربندی سرور به کمک Server Manager

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



شکل ۲-۲۲

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

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

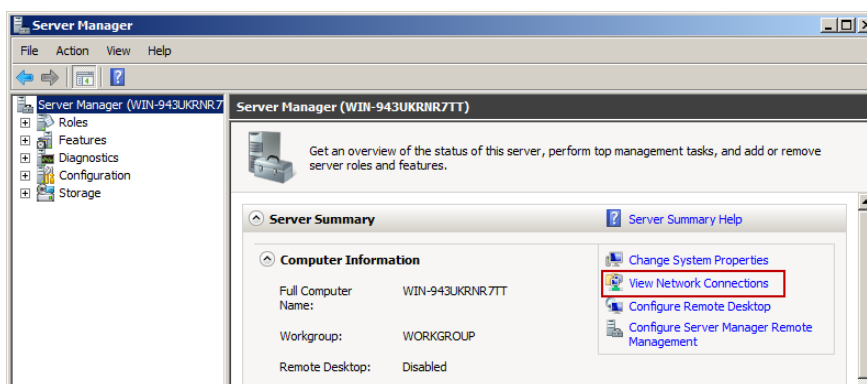
## ۲-۶-۱ اقدامات پیکربندی متداول

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

### تغییر تنظیمات شبکه

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

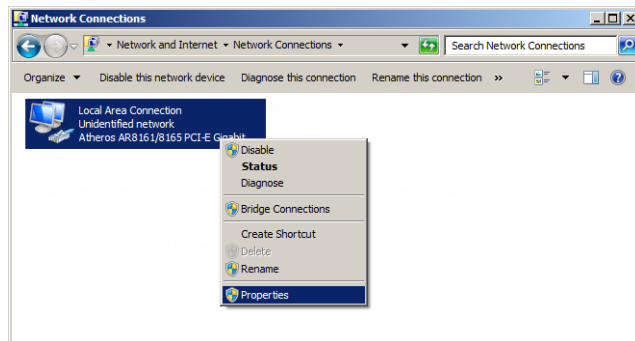
۱. کنسول Server Manager را باز نموده و از پنل سمت چپ، بر روی Server Manager کلیک کنید.
۲. در قسمت Server Summary، بر روی گزینه View Network Connections (که به صورت لینک آبی رنگ است) کلیک کنید.



شکل ۲-۲۲

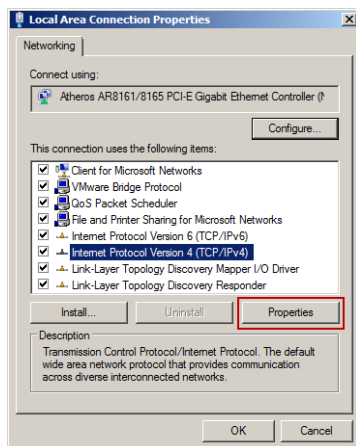
۳. پنجره‌ای تحت عنوان "Network Connection" نشان داده خواهد شد. (البته این پنجره از طریق Control Panel و یا نوشتن دستور `ncpa.cpl` در `cmd` نیز قابل دسترسی می‌باشد) در این پنجره، به ازای هر کارت شبکه (NIC)<sup>۱</sup> که بر روی سرور قرار دارد، یک کانکشن<sup>۲</sup> مشاهده می‌کنید. جهت اتصال به شبکه، باید کانکشنی را انتخاب کنید که قصد دارید از طریق آن به شبکه متصل شوید (ممکن است از کارت شبکه جهت اتصال به اینترنت نیز استفاده شود). در اینجا سرور ما ساده است و تنها دارای یک کارت شبکه می‌باشد. بر روی کانکشن Local Area Connection کلیک راست نموده و Properties را انتخاب کنید.

1. Network Interface Card  
2. Connection



شکل ۲-۲۳

۴. در پنجره “Local Area Connection Properties” گزینه “Internet Protocol Version 4 (TCP/IPv4)” را انتخاب و بروی Properties کلیک کنید.



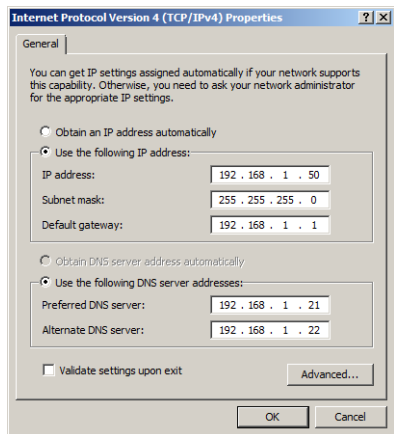
شکل ۲-۲۴

۵. در ویندوز سرور 2008R2، TCP/IP بطور پیش فرض پیکربندی نشده است و کارت شبکه آدرس IP خود را بطور خودکار از سرویس DHCP دریافت می کند (شکل ۲-۲۵). در اینجا قصد داریم، پیکربندی TCP/IP را بطور دستی انجام دهیم. بنابراین از تب General گزینه “Use the following IP address” را انتخاب کنید (شکل ۲-۲۶). پس از انتخاب گزینه ذکر شده، مکان هایی جهت وارد نمودن آدرس IP، قاب زیر شبکه<sup>۲</sup>، آدرس دروازه<sup>۳</sup>، و آدرس سرور DNS فعال می گردد. در این

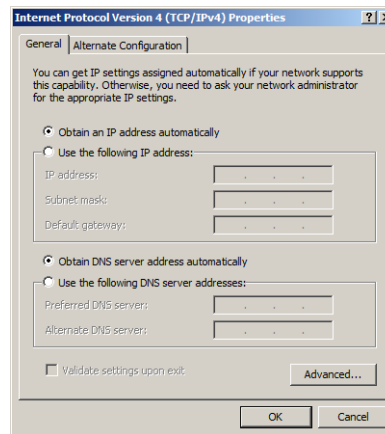
1. Network Interface Card
2. Connection
3. Subnet mask
4. Default Gateway



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



شکل ۲-۲۶



شکل ۲-۲۵

### تغییر تنظیمات شبکه در خط فرمان

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

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

بطور کلی، قالب دستور netsh به صورت زیر می‌باشد:

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

جهت انجام تنظیمات DNS، دستور زیر را تایپ کنید:

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

قالب کلی این دستور به صورت زیر می‌باشد:

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

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

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

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

```
C:\>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

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

Tunnel adapter Local Area Connection* 3:

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

Tunnel adapter Local Area Connection* 4:

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

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

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

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

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

Ping statistics for 192.168.1.2:
```

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

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

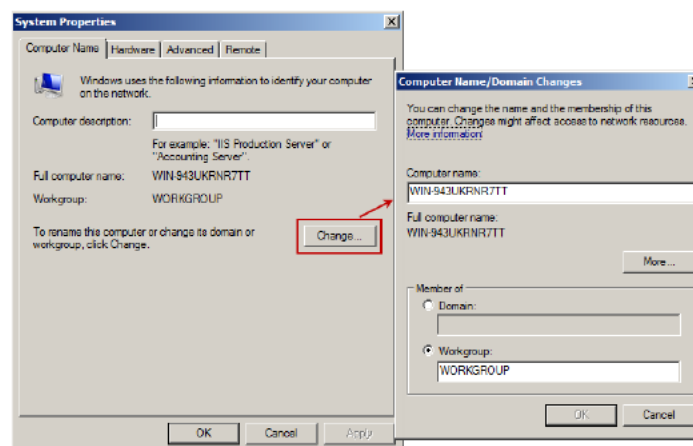


منظور از دروازه یا Gateway، وسیله‌ای است که امکان ارتباط یک شبکه را با خارج از آن فراهم می‌سازد. به عنوان مثال Router و Modem هر کدام می‌توانند به عنوان Gateway در نظر گرفته شوند.

### تغییر نام سرور

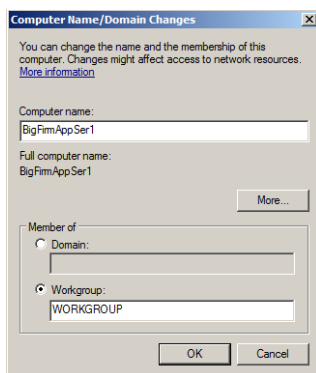
هر کامپیوتر در شبکه، باید دارای یک نام منحصر بفرد باشد تا بتواند توسط سایر کامپیوترها شناسایی شود. در بسیاری از موارد انتخاب این نام اختیاری است و کاربران می‌توانند با توجه به نظر خود آنرا انتخاب کنند، اما در مواردی استانداردهای سازمان تعیین‌کننده این نام می‌باشد (نام انتخابی می‌تواند ترکیبی از حروف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

۱. کنسول Server Manager را باز نموده و از قسمت Server Summary، گزینه Change Computer Setting را انتخاب کنید (این گزینه از مسیر «Computer Properties» Change setting نیز قابل دسترسی می‌باشد).
۲. در پنجره «System Properties»، از تب Computer Name/Domain Changes، بر روی دکمه Change کلیک کنید تا پنجره Computer Name/Domain Changes نشان داده شود.



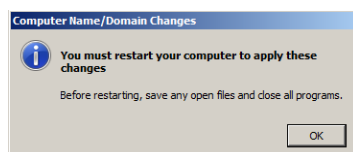
شکل ۲-۲۷

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



شکل ۲-۲۸

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



شکل ۲-۲۹

### تغییر نام سرور در خط فرمان

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

```
C:\Windows\system32>netdom /renamecomputer WIN-943UKRNR7TT
/newname:BIGFIRMAPPSE1
```

```
This operation will rename the computer WIN-943UKRNR7TT
to BIGFIRMAPPSE1.
Certain services, such as the Certificate Authority, rely on a fixed machine
name. If any services of this type are running on WIN-DCL9MRNLVOH,
then a computer name change would have an adverse impact.
```

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

```
Y
```

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

The command completed successfully.

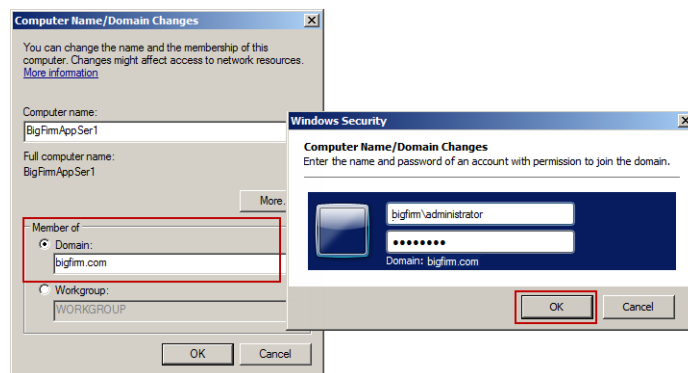
قالب کلی این دستور، به صورت زیر می‌باشد:

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

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

### اتصال سرور به یک دامنه<sup>۱</sup>

قبل از اینکه بتوانیم منابع موجود در سرور را با سایر اعضاء شبکه به اشتراک گذاریم، نیازمند اتصال آن به یک دامنه هستیم. در اینجا قصد داریم سرور را به دامنه‌ای با نام bigfirm.com متصل کنیم. جهت انجام این کار، در قسمت Member of از پنجره Computer Name گزینه Domain را انتخاب کنید. سپس نام دامنه را وارد نموده و بر روی OK کلیک کنید. پس از کلیک، از شما نام کاربری و رمز عبور یک حساب کاربری که اجازه افزودن سرور به دامنه را دارد، درخواست می‌شود. این کاربر ممکن است مدیر سرور (نام کاربری: bigfirm\administrator) و یا فردی باشد که در اکتیو دایرکتوری<sup>۲</sup> این مجوز به او داده شده باشد (به عنوان مثال bigfirm\user1). پس از وارد نمودن موارد درخواست شده تمام پنجره‌ها را ببندید و کامپیوتر را Restart کنید. پس از راه‌اندازی، این سرور از امکانات Group Policy، کاربران Active Directory، مدیریت مرکزی و ... برخوردار می‌گردد.



شکل ۲-۳۰

1. Domain
2. Active Directory

### اتصال سرور به دامنه در خط فرمان

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

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

Type the password associated with the domain user:\*\*\*\*\*

The computer needs to be restarted in order to complete the operation:

The command completed successfully.

قالب کلی این دستور به صورت زیر است:

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

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

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

### فعال‌سازی Remote Desktop بروی سرور

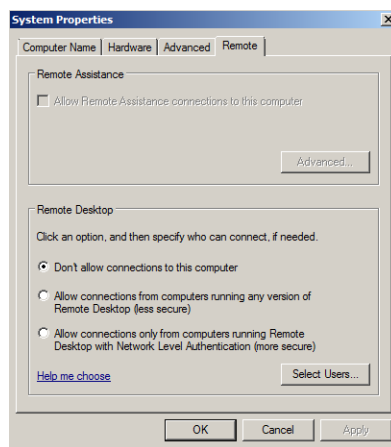
بسیاری از مدیران ویندوز تمایل دارند که سرور را از راه دور و از طریق کامپیوترهای شخصی خود کنترل کنند. این کار با فعال کردن سرویس Remote Desktop بروی سرور امکان‌پذیر است. پس از فعال‌سازی این سرویس، می‌توانید به کمک ابزار Remote Desktop که بروی کامپیوتر و یا لپ‌تاپ شما قرار دارد و همچنین از طریق یک اتصال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

جهت فعال‌سازی، مراحل زیر را دنبال کنید:

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

دارد. این گزینه‌ها عبارتند از:

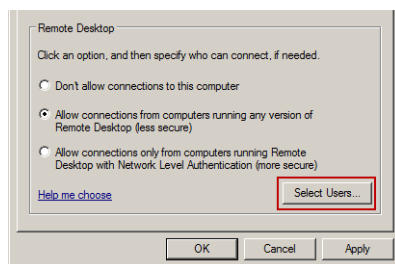
- ♦ **Do not allow connections to this computer**: این گزینه که به صورت پیش‌فرض نیز انتخاب شده است، استفاده از Remote Desktop را در حالت غیرفعال قرار می‌دهد.
- ♦ **Allow connections from computers running any version ...**: این گزینه، به نسخه‌هایی از برنامه Remote Desktop که پایین‌تر از نسخه ۶ در ویندوز سرور 2008R2 هستند اجازه می‌دهد تا به سرور متصل شوند. نسخه ۶، در ویندوز ویستا و بعد از آن به کار گرفته شده است و شامل قابلیت‌های امنیتی جدید می‌باشد. کاربرانی که از نسخه‌های پایین‌تر این برنامه در ویندوزهای XP و سرور 2003 استفاده می‌کنند، می‌توانند از طریق سایت مایکروسافت (به صورت رایگان) نسخه جدید این برنامه را دریافت کنند.
- ♦ **Allow connections only from computers running Remote Desktop with ...**: پیشنهاد مایکروسافت این است که جهت دسترسی به RDP، از این گزینه استفاده کنید. توجه داشته باشید که در این گزینه باید بر روی همه کامپیوترهای مورد نظر حداقل نسخه ۶ از برنامه Remote Desktop را داشته باشید.



شکل ۲-۳۱

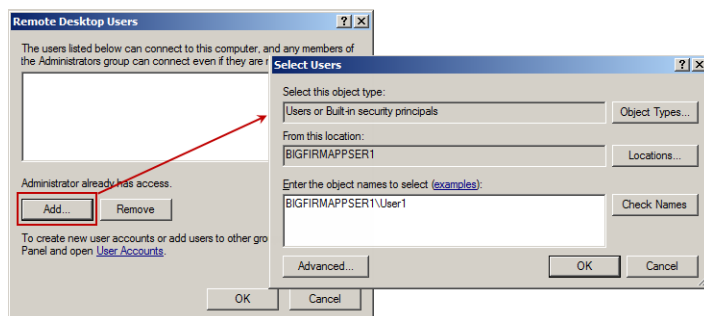
با توجه به نوع شبکه و کاربران خود، یکی از گزینه‌های مذکور را انتخاب کنید.

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



شکل ۲-۳۲

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



شکل ۲-۳۳

## ۲-۶-۲ افزودن و حذف کردن Role‌ها

قبل از پرداختن به این بحث، لازم است دو اصطلاح را تعریف کنیم:

- ♦ **Role:** نقش یا رُل (Role)، عملکردی است که بر روی یک سرور میزبانی می‌شود. در واقع هر Role، مجموعه‌ای از قابلیت‌ها است که می‌توانند بر روی سرور نصب شده و به آن اجازه دهد تا این قابلیت‌ها را اجرا نماید (مثل DNS Server و Web Server).
- ♦ **Feature:** ویژگی یا Feature، قطعه نرم‌افزاری خاصی است که قابلیت‌های کوچکی را به سرور اضافه می‌کند.

در ویندوز سرور 2008 و 2008R2، مجموعه‌ای از Role‌ها و Feature‌ها فراهم شده است که با استفاده از آنها می‌توانید عملکردهای زیادی را به سرور اضافه کنید. در ادامه، نحوه اضافه کردن و یا حذف کردن Role‌ها و Feature‌ها را شرح خواهیم داد.



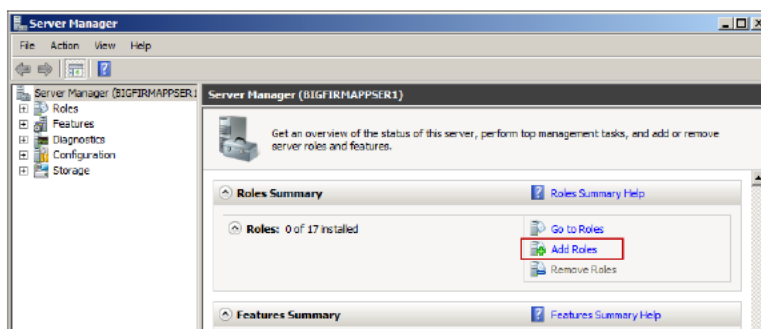


موقع نصب کامل ویندوز سرور 2008 و 2008R2، هیچ Role و یا Feature ای بطور پیش‌فرض نصب نخواهد شد. بنابراین نیاز است که پس از نصب ویندوز، آنها را با توجه به نیاز خود و عملکرد سرور نصب کنید. زمانی که ویندوز سرور 2003 را به 2008 یا 2008R2 ارتقاء می‌دهید، کلیه Role ها و Feature های موجود بر روی آن، به ویندوز جدید منتقل می‌شوند.

### اضافه کردن Role ها

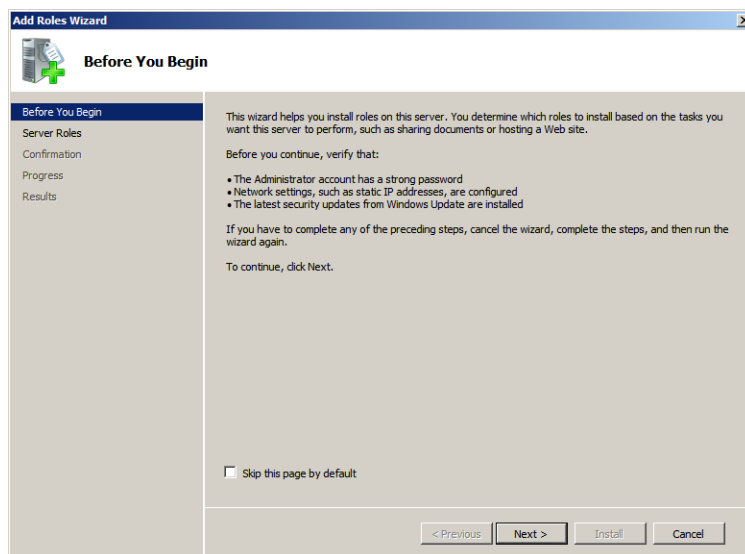
همانطور که اشاره نمودیم، Role ها مجموعه‌ای از قابلیت‌ها هستند، بنابراین با نصب یک Role در واقع مجموعه‌ای از قابلیت‌ها را بر روی سرور راه‌اندازی می‌کنید. هر Role، بطور پیش‌فرض دارای زیرمجموعه‌هایی است که می‌توانید آنها را با توجه به نیاز خود شخصی‌سازی کنید. در اینجا اضافه کردن Role را به کمک Server Manager و servermanagercmd.exe شرح می‌دهیم. البته دقت داشته باشید که از ذکر جزئیات مربوط به Role ها در این قسمت پرهیز نموده و در فصل‌های مربوطه به آنها خواهیم پرداخت.

۱. ابتدا Server Manager را اجرا نموده و به قسمت Roles Summery بروید. جهت افزودن Role، بر روی گزینه Add Roles کلیک کنید.



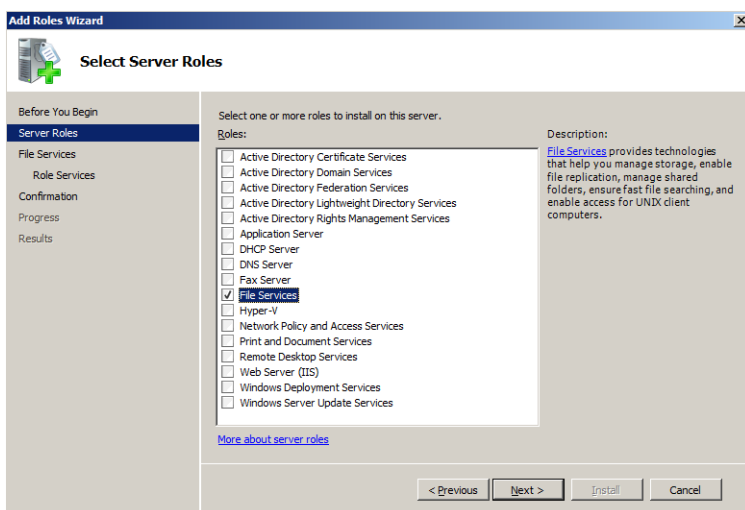
شکل ۲-۳۴

۲. ویزاردی به نام "Add Role Wizard" اجرا می‌شود. در صفحه "Before You Begin" توضیحاتی راجع به وظایف این ویزارد ارائه می‌شود. می‌توانید با برداشتن تیک مربوط به گزینه "Skip this page by default" از نمایش مجدد برای نصب سایر Role ها جلوگیری نمایید. بر روی Next کلیک کنید.



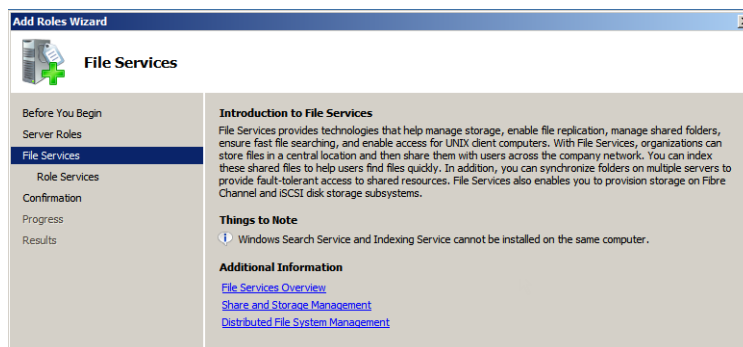
شکل ۳۵-۲

۳. در صفحه “Select Server Roles”، لیستی از Role‌های قابل نصب بر روی Server نمایش داده می‌شود. با کلیک بر روی هر Role، می‌توانید توضیحی مختصر راجع به آن مشاهده کنید. در اینجا قصد داریم سرور را به یک فایل‌سرور تبدیل کنیم، بنابراین گزینه File Services را انتخاب نموده و بر روی Next کلیک کنید.



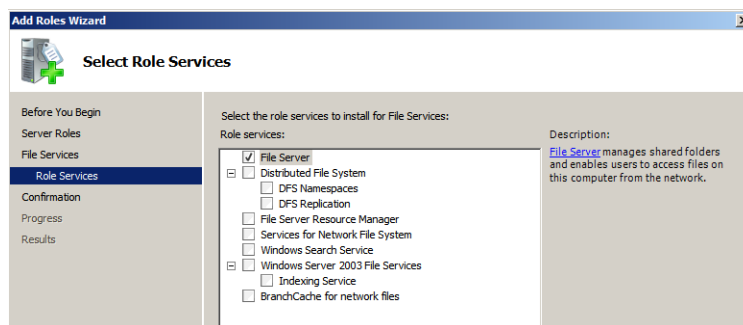
شکل ۳۶-۲

۴. در صفحه “File Services”، Role ای که انتخاب نموده‌اید، معرفی شده و توضیحاتی مختصر راجع به عملکرد آن ارائه می‌گردد. بر روی Next کلیک کنید.



شکل ۲-۳۷

۵. بعضی از Role ها ممکن است زیر مجموعه‌هایی نیز داشته باشند که به آنها Role Service گفته می‌شود. در صورتی که به ازای Role ها، Role Service هایی نیز موجود باشد، در صفحه “Select Role Services” Role Services لیست آنها نشان داده می‌شود و می‌توانید بر اساس نیاز خود، آنها را برای نصب شدن انتخاب کنید. در شکل ۲-۳۸ این وضعیت نشان داده شده است.

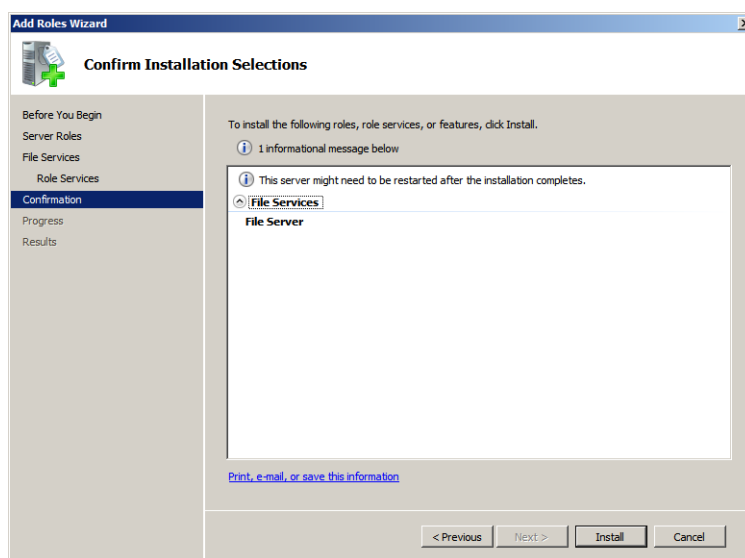


شکل ۲-۳۸

همانطور که در شکل مشاهده می‌کنید، در زمان انتخاب یک سرویس، کلیه سرویس‌های مرتبط با آن نیز به شما پیشنهاد می‌گردد. این موضوع باعث سادگی کار می‌شود، زیرا می‌توانید ارتباط و وابستگی میان سرویس‌ها را تشخیص داده و در صورت نیاز آنها را نصب نمایید. پس از انتخاب سرویس‌های مورد نظر، بر روی Next کلیک کنید. (دقت داشته باشید که در اینجا تنها File server به عنوان Role Service انتخاب شده است و بنابراین پس از این مرحله با مراحل بیشتری مواجه

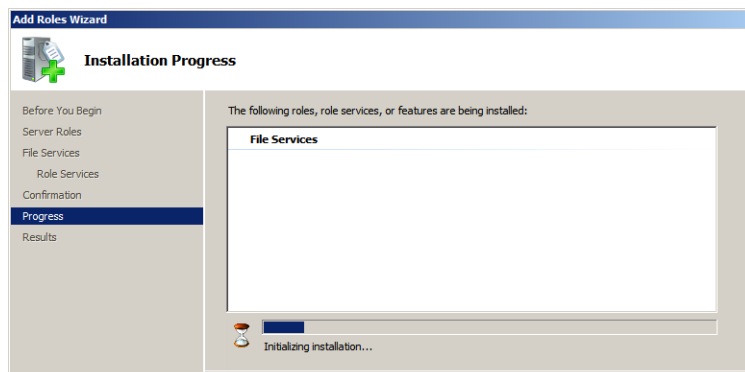
نخواهید شد. در فصل “راه‌اندازی فایل سرور” جزئیات این Role را بیشتر مورد بررسی قرار خواهیم داد).

۶. در صفحه “Confirm Installation Selections” خلاصه‌ای از تنظیمات انجام شده در مراحل قبل نشان داده می‌شود. در صورت نیاز می‌توانید به عقب بازگشته و آنها را اصلاح کنید. چنانچه تنظیمات انجام شده صحیح است بروی Install کلیک کنید تا عملیات نصب آغاز گردد.



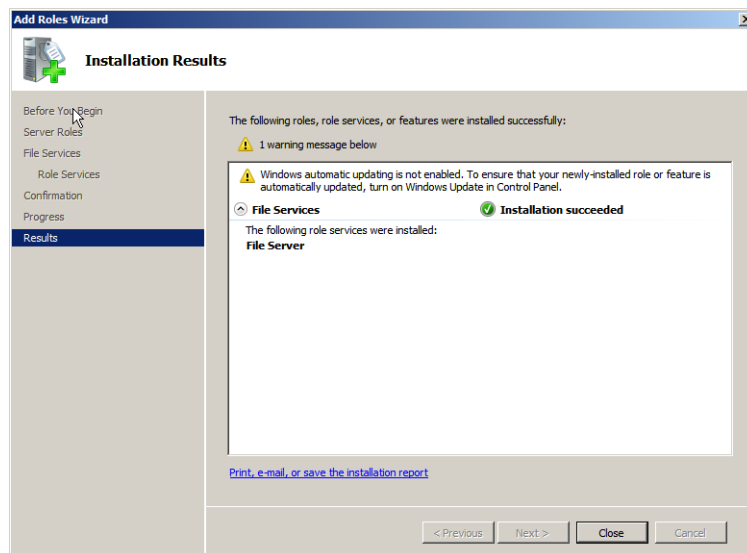
شکل ۲-۳۹

۷. فرایند نصب Role ها و Role Service ها ممکن است کمی زمان ببرد. پس منتظر بمانید تا فرایند کامل گردد. در شکل زیر، انجام فرایند نصب نشان داده شده است.



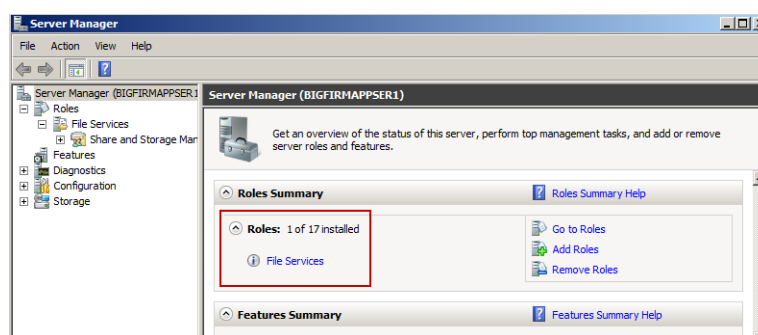
شکل ۲-۴۰

۸. پس از اتمام فرایند نصب، پیغامی مبنی بر انجام موفق آن نشان داده می‌شود. علاوه بر این، به شما تذکر داده می‌شود که آپدیت خودکار ویندوز غیرفعال است. این هشدار را نادیده گرفته و بر روی Close کلیک کنید.



شکل ۲-۴۱

۹. اکنون می‌توانید به Server Manager بازگشته و نتیجه عملیات را مشاهده نمایید.



شکل ۲-۴۲

### افزودن Role ها با استفاده از خط فرمان

در ویندوز سرور 2008 و 2008R2، اضافه کردن Role ها با استفاده از دستورات خط فرمان نیز امکان‌پذیر است. نوع دیگری از Server Manager وجود دارد که در خط فرمان اجرا شده و با دستور

servermanagercmd.exe استفاده می‌شود. در ویندوز سرور 2008R2، زمانی که از این دستور در Cmd استفاده می‌کنید، به شما هشدار داده و اعلام می‌کند که از PowerShell استفاده کنید. در اینجا، servermanagercmd.exe را در خط فرمان ویندوز سرور 2008 به کار می‌بریم و در ادامه استفاده از دستورات را در PowerShell شرح می‌دهیم.

در هنگام استفاده از دستور servermanagercmd.exe پارامترهایی نیز به همراه آن آورده می‌شود. یکی از این پارامترها query- می‌باشد و برای مشاهده وضعیت Roleها استفاده می‌گردد.

```
C:\Users\Administrator>servermanagercmd.exe -query

----- Roles -----

[ ] Active Directory Certificate Services [AD-Certificate]
[ ] Certification Authority [ADCS-Cert-Authority]
[ ] Certification Authority Web Enrollment [ADCS-Web-Enrollment]
[ ] Online Responder [ADCS-Online-Cert]
[ ] Network Device Enrollment Service [ADCS-Device-Enrollment]
.
.
.
[ ] File Services
[ ] File Server [FS-FileServer]
[ ] Distributed File System [FS-DFS]
    [ ] DFS Namespaces [FS-DFS-Namespaces]
    [ ] DFS Replication [FS-DFS-Replication]
[ ] File Server Resource Manager [FS-Resource-Manager]
[ ] Services for Network File System [FS-NFS-Services]
[ ] Windows Search Service [FS-Search-Service]
[ ] Windows Server 2003 File Services [FS-Win2003-Services]
    [ ] File Replication Service [FS-Replication]
    [ ] Indexing Service [FS-Indexing-Service]
.
.
.

----- Features -----

[ ] .NET Framework 3.0 Features [NET-Framework]
[ ] .NET Framework 3.0 [NET-Framework-Core]
[ ] XPS Viewer [NET-XPS-Viewer]
[ ] WCF Activation [NET-Win-CFAC]
    [ ] HTTP Activation [NET-HTTP-Activation]
    [ ] Non-HTTP Activation [NET-Non-HTTP-Activ]
[ ] BitLocker Drive Encryption [BitLocker]
[ ] BITS Server Extensions [BITS]
.
.
.

C:\Users\Administrator>
```

به دلیل طولانی بودن نتیجه، فقط قسمت‌های مهم را در اینجا آورده‌ایم. همانطور که مشاهده می‌کنید، قبل از هر Role یا Feature، از علامت [ ] استفاده شده است. زمانی که یک Role یا Feature

نصب می‌شود، داخل این علامت، با X نشانه‌گذاری می‌گردد.

اکنون قصد داریم File Service و File Server Resource Manager را از طریق خط فرمان نصب کنیم. در این محیط، File Service با FS-FileServer، و File Server Resource Manager با FS-Resource-Manager به کار برده می‌شوند. ترکیب این عبارات با پارامتر install- شما را قادر به نصب آنها می‌نماید.

```
C:\Users\Administrator>servermanagercmd.exe -install FS-FileServer
FS-Resource-Manager
..
Start Installation...
[Installation] Succeeded: [File Services] File Server.
[Installation] Succeeded: [File Services] File Server Resource Manager.
<100/100>
Success: Installation succeeded.
C:\Users\Administrator>
```

همانطور که مشاهده می‌کنید، عملیات نصب از طریق خط فرمان ساده‌تر از انجام آن از طریق کنسول Server Manager می‌باشد.

اکنون بار دیگر servermanagercmd.exe را به همراه پارامتر query- اجرا کنید:

```
C:\Users\Administrator>servermanagercmd.exe -query
..
----- Roles -----
[ ] Active Directory Certificate Services [AD-Certificate]
[ ] Certification Authority [ADCS-Cert-Authority]
[ ] Certification Authority Web Enrollment [ADCS-Web-Enrollment]
[ ] Online Responder [ADCS-Online-Cert]
[ ] Network Device Enrollment Service [ADCS-Device-Enrollment]
.
.
[X] File Services
[X] File Server [FS-FileServer]
[ ] Distributed File System [FS-DFS]
[ ] DFS Namespaces [FS-DFS-Namespaces]
[ ] DFS Replication [FS-DFS-Replication]
[X] File Server Resource Manager [FS-Resource-Manager]
[ ] Services for Network File System [FS-NFS-Services]
[ ] Windows Search Service [FS-Search-Service]
[ ] Windows Server 2003 File Services [FS-Win2003-Services]
[ ] File Replication Service [FS-Replication]
[ ] Indexing Service [FS-Indexing-Service]
.
.
----- Features -----
[ ] .NET Framework 3.0 Features [NET-Framework]
[ ] .NET Framework 3.0 [NET-Framework-Core]
[ ] XPS Viewer [NET-XPS-Viewer]
[ ] WCF Activation [NET-Win-CFAC]
```

```

[ ] HTTP Activation [NET-HTTP-Activation]
[ ] Non-HTTP Activation [NET-Non-HTTP-Activ]
.
.
.
[X] Remote Server Administration Tools [RSAT]
[X] Role Administration Tools [RSAT-Role-Tools]
    [ ] Active Directory Certificate Services Tools [RSAT-ADCS]
        [ ] Certification Authority Tools [RSAT-ADCS-Mgmt]
        [ ] Online Responder Tools [RSAT-Online-Responder]
    [ ] Active Directory Domain Services Tools [RSAT-ADDS]
        [ ] Active Directory Domain Controller Tools [RSAT-ADDC]
        [ ] Server for NIS Tools [RSAT-SNIS]
    [ ] Active Directory Lightweight Directory Services Tools [RSAT-ADLDS]
    [ ] Active Directory Rights Management Services Tools [RSAT-RMS]
    [ ] DHCP Server Tools [RSAT-DHCP]
    [ ] DNS Server Tools [RSAT-DNS-Server]
    [ ] Fax Server Tools [RSAT-Fax]
[X] File Services Tools [RSAT-File-Services]
    [ ] Distributed File System Tools [RSAT-DFS-Mgmt-Con]
[X] File Server Resource Manager Tools [RSAT-FSRM-Mgmt]
    [ ] Services for Network File System Tools [RSAT-NFS-Admin]
    [ ] Network Policy and Access Services Tools [RSAT-NPAS]
    [ ] Print Services Tools [RSAT-Print-Services]
    [ ] Terminal Services Tools [RSAT-TS]
        [ ] Terminal Server Tools [RSAT-TS-RemoteApp]
        [ ] TS Gateway Tools [RSAT-TS-Gateway]
        [ ] TS Licensing Tools [RSAT-TS-Licensing]
    [ ] UDDI Services Tools [RSAT-UDDI]
    [ ] Web Server (IIS) Tools [RSAT-Web-Server]
    [ ] Windows Deployment Services Tools [RSAT-WDS]
[ ] Feature Administration Tools [RSAT-Feature-Tools]
    [ ] BitLocker Drive Encryption Tools [RSAT-BitLocker]
    [ ] BITS Server Extensions Tools [RSAT-Bits-Server]
    [ ] Failover Clustering Tools [RSAT-Clustering]
    [ ] Network Load Balancing Tools [RSAT-NLB]
    [ ] SMTP Server Tools [RSAT-SMTP]
    [ ] WINS Server Tools [RSAT-WINS]
.
.
.
C:\Users\Administrator>

```

همانطور که در گزارش بالا مشاهده می‌کنید، Role ها و Role Service هایی که درخواست داده‌اید به همراه Feature های مورد نیاز آنها، نصب و با علامت X مشخص شده‌اند. جهت اطمینان از نصب می‌توانید از طریق Server Manager نیز آنها را مشاهده کنید.

### اسکرپت‌های نصب خودکار Role ها

این اسکرپت‌ها (که با نام اسکرپت‌های پاسخ شناخته می‌شوند) به شما امکان می‌دهند تا بدون نیاز به انجام پرسش و پاسخ بتوانید نصب Role ها، Role Service ها و Feature ها را در servermanagercmd.exe انجام دهید. این کار با قراردادن مجموعه‌ای از پاسخ‌ها در یک فایل، به



ازای هر پیکربندی سرور انجام می‌شود. به عنوان مثال پاسخی برای یک نصب Web Server به صورت زیر می‌باشد:

```
<?xml version="1.0" encoding="utf-8" ?>
<ServerManagerConfiguration Action="Install"
xmlns="http://schemas.microsoft.com/
sdm/Windows/ServerManager/Configuration/2007/1"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<Role Id="Application-Server" />
<RoleService Id="AS-Web-Support" />
<Role Id="Web-Server" />
</ServerManagerConfiguration>
```

کدهایی که در بالا مشاهده می‌کنید، یک فایل XML است. می‌توانید بدون نیاز به دانستن برنامه‌نویسی، پیکربندی سرور را در قالب این فایل‌ها ذخیره نموده و با یک فراخوانی ساده در Cmd آنها را اجرا کنید. تنها چیزهایی که از این فایل نیاز به دانستن دارید این است که دستور ServerManagerConfiguration Action جهت مشخص نمودن نوع عملیات است و با Install یا Remove مقدارگذاری می‌شود. جهت بدست آوردن عباراتی که بعد از ID نوشته شده‌اند، می‌توانید دستور servermanagercmd.exe -query در ادامه دستورات پیکربندی می‌توانید در یک فایل XML با نام FileServer.XML قرار دارند آورده شده است.

```
<?xml version="1.0" encoding="utf-8" ?>
<ServerManagerConfiguration Action="Install"
xmlns="http://schemas.microsoft.com/sdm/Windows/ServerManager/
Configuration/2007/1" xmlns:xs="http://www.w3.org/2001/XMLSchema">
<RoleService Id="FS-FileServer" />
<RoleService Id="FS-Resource-Manager" />
</ServerManagerConfiguration>
```

پس از ایجاد فایل‌های XML، می‌توانید آنها را از لحاظ صحیح بودن بررسی کنید. این کار با استفاده از servermanager.exe، پارامتر -whatif و آدرس فایل XML بر روی سرور، امکان‌پذیر است. در ادامه چگونگی انجام کار نشان داده شده است.

```
C:\Users\Administrator>servermanagercmd.exe -inputpath
C:\FileServer.xml -whatif
..
Note: Running in 'WhatIf' Mode.
Specified for installation: [File Services] File Server Resource Manager
Specified for installation: [File Services] File Server

This server may need to be restarted after the installation completes.
C:\Users\Administrator>
```

پس از بررسی فایل و اطمینان از صحیح بودن می‌توانید آنرا را اجرا کنید:

```
C:\Users\Administrator>servermanagercmd.exe -inputpath C:\FileServer.xml
.
Start Installation...
[Installation] Succeeded: [File Services] File Server.
[Installation] Succeeded: [File Services] File Server Resource Manager.
<100/100>
Success: Installation succeeded.
C:\Users\Administrator>
```

پس از اجرای این دستور، می‌توانید از طریق `servermanagercmd.exe -query` موفق بودن عملیات نصب را بررسی کنید.

### کار با دستورات در PowerShell

اکنون قصد داریم نحوه کار با دستورات در PowerShell ویندوز سرور 2008R2 را شرح دهیم. تعداد اشیاء موجود در PowerShell بسیار زیاد هستند و ما در اینجا تنها تعدادی از آنها که مربوط به مدیریت سرور هستند را شرح خواهیم داد (به دستوراتی که در PowerShell استفاده می‌شوند، `command-lets` یا `cmdlets` گفته می‌شود).

PowerShell، از طریق منوی پایین صفحه Desktop و یا از مسیر « Administrative Tools » Start « PowerShell Modules قابل دسترسی می‌باشد. دقت داشته باشید که شما باید به عنوان مدیر سرور از آن استفاده نمایید، بنابراین، بر روی آیکن آن کلیک راست نموده و گزینه « Run as administrator » را انتخاب کنید.

ماژول‌های PowerShell، بطور پیش‌فرض بارگذاری نشده‌اند. بنابراین باید با دستور زیر آنها را بارگذاری کنید:

```
PS C:\Users\Administrator> import-module Servermanager
```

پس از بارگذاری ماژول‌ها، برای نمایش Role‌ها و Feature‌هایی که نصب نموده‌اید، از دستور زیر استفاده نمایید:

```
PS C:\Users\Administrator> get-WindowsFeature
```

Display Name	Name
[ ] Active Directory Certificate Services	AD-Certificate
[ ] Certification Authority	ADCS-Cert-Authority
[ ] Certification Authority Web Enrollment	ADCS-Web-Enrollment
[ ] Online Responder	ADCS-Online-Cert
[ ] Network Device Enrollment Service	ADCS-Device-Enrollment

[ ] Certificate Enrollment Web Service	ADCS-Enroll-Web-Svc
[ ] Certificate Enrollment Policy Web Service	ADCS-Enroll-Web-Pol
[ ] Active Directory Domain Services	AD-Domain-Services
[ ] Active Directory Domain Controller	ADDS-Domain-Controller
[ ] Identity Management for UNIX	ADDS-Identity-Mgmt
[ ] Server for Network Information Services	ADDS-NIS
[ ] Password Synchronization	ADDS-Password-Sync
[ ] Administration Tools	ADDS-IDMU-Tools
[ ] Active Directory Federation Services	AD-Federation-Services
[ ] Federation Service	ADFS-Federation
[ ] Federation Service Proxy	ADFS-Proxy
[ ] AD FS Web Agents	ADFS-Web-Agents

هر Role Service، Role ای که نصب شده باشد، با علامت X مشخص می‌شود.

با استفاده از دستور زیر، می‌توانید نام کامل یک Role یا Feature را بدست آورید:

```
PS C:\Users\Administrator> get-windowsfeature AD-Certificate
```

Display Name	Name
[ ] Active Directory Certificate Services	AD-Certificate

در صورتیکه قصد دارید نتیجه اجرای دستورات را در یک فایل متنی ذخیره کنید، می‌توانید از دستور زیر استفاده نمایید:

```
PS C:\Users\Administrator> get-windowsfeature > C:\InstalledFeatures.txt
```

این دستور، نتایج حاصل از اجرای دستور get-windowsfeature را در فایلی به نام InstalledFeatures و با پسوند txt، ذخیره می‌کند.

نحوه اضافه‌کردن یک Role با استفاده از PowerShell: قالب کلی این دستور به صورت زیر می‌باشد:

**Add-WindowsFeature <Role Name>**

یکی از ویژگی‌های جالبی که در هنگام نصب Role‌ها می‌توانید از آن استفاده کنید، به کارگیری پارامتر -whatif می‌باشد. به کمک این پارامتر می‌توانید اتفاقی که در هنگام اضافه‌کردن یک Role رخ می‌دهد را بررسی نمایید. به مثال زیر توجه کنید:

```
PS C:\Users\Administrator> add-windowsfeature File-Services,FS-Resource-Manager -whatif
```

```
What if: Checking if running in 'WhatIf' Mode.
What if: Performing operation "Add-WindowsFeature" on Target "[File Services]
File Server Resource Manager".
What if: Performing operation "Add-WindowsFeature" on Target "[File Services]
File Server".
```

What if: This server may need to be restarted after the installation completes.

Success	Restart Needed	Exit Code	Feature Result
True	Maybe	Success	{ }

پس از بررسی اتفاقات و در صورت مطلوب بودن نتیجه می‌توانید Role را اضافه کنید. جهت انجام این کار دستور زیر را اجرا نمایید:

```
PS C:\Users\Administrator> add-windowsfeature File-Services,FS-Resource-Manager-concurrent
```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{File Server, File Server Resource Manager}

در صورتی که با حجم زیادی از Role ها و Role Service ها مواجه باشید می‌توانید نصب آنها را با کمترین تلاش و به کمک اسکریپت‌های PowerShell انجام دهید. برای این کار ابتدا نیاز به فعال‌سازی این اسکریپت‌ها دارید زیرا بطور پیش‌فرض غیرفعال هستند. جهت فعال‌سازی، دستور زیر را وارد کنید:

```
PS C:\Users\Administrator> set-executionpolicy unrestricted
```

```
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust.
Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic.
Do you want to change the execution policy?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
```

در صورتی که قصد داشته باشید این اسکریپت‌ها را غیرفعال کنید می‌توانید از دستور زیر استفاده نمایید:

```
PS C:\Users\Administrator> get-executionpolicy Unrestricted
```

اکنون، اسکریپت زیر را نوشته و با نام FileServer.PS1 ذخیره کنید:

```
import-module Servermanager
add-windowsfeature File-Services,FS-Resource-Manager -restart
```

پس از ذخیره فایل، بر روی آن کلیک‌راست نموده و آنرا در PowerShell اجرا کنید. اسکریپت شما اجرا شده و موارد مورد نظر نصب می‌شوند. پارامتر -restart در انتهای اسکریپت باعث می‌شود که سرور در صورت نیاز Restart گردد.

اجرای فایل بالا از طریق خط فرمان نیز امکان پذیر است. فقط کافی است دستور زیر را اجرا کنید:

```
C:\>powershell.exe c:\fileserver.ps1
```

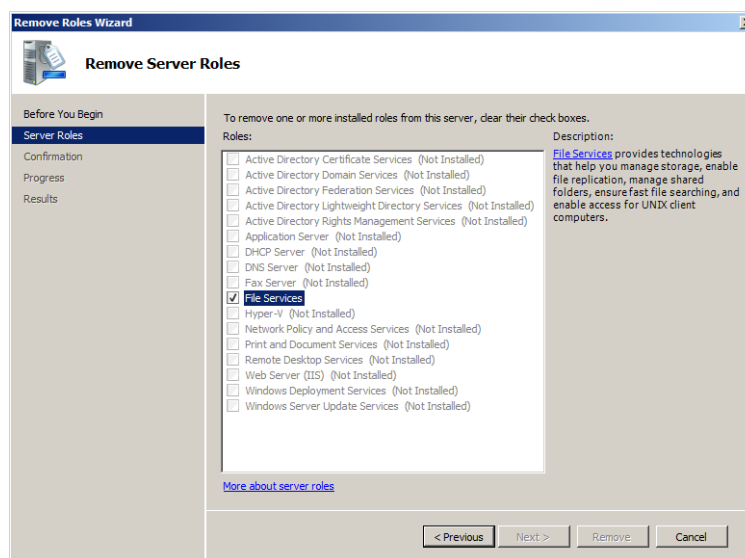
Success	Restart Needed	Exit Code	Feature	Result
True	No	Success	{File Server, File Server Resource Manager}	

با مشاهده مثال‌های بالا شاید اکنون به اهمیت استفاده از دستورات خط فرمان و PowerShell پی برده باشید. این دستورات را می‌توانید به صورت فایل‌ها ذخیره نموده و هر زمان که نیاز داشتید تنها با نوشتن دستوراتی کوچک (و یا حتی بدون نیاز به نوشتن)، آنها را بر روی سرور فراخوانی و اجرا نمایید.

### حذف کردن Role‌ها

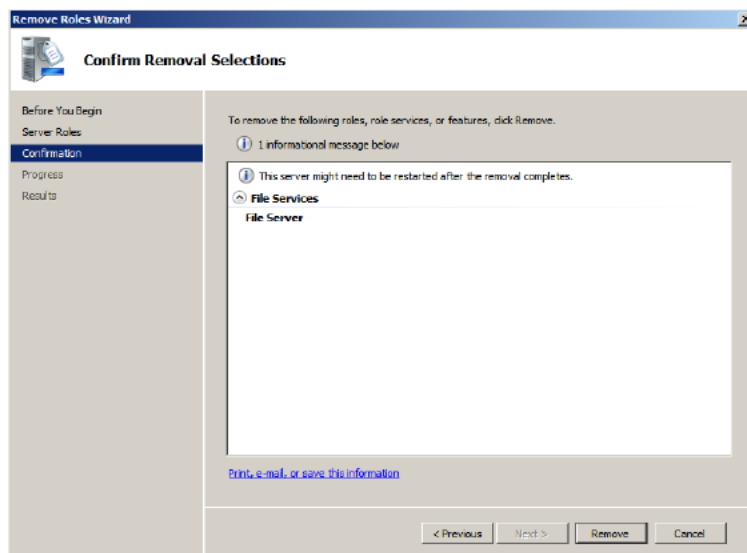
حذف کردن Role‌ها، تفاوت چندانی با اضافه کردن آنها ندارد. برای حذف کردن Role‌ها مراحل زیر را دنبال نمایید:

۱. در کنسول Server Manager و از قسمت Roles Summery، گزینه Remove Roles را انتخاب کنید.
۲. در صفحه “Remove Server Roles”، لیستی از Role‌ها نشان داده می‌شود، با این تفاوت که Role‌های نصب شده فعال، و Role‌های نصب نشده غیرفعال می‌باشند. با برداشتن تیک مربوط به Role‌های مورد نظر، آنها را انتخاب و بر روی Next کلیک کنید.



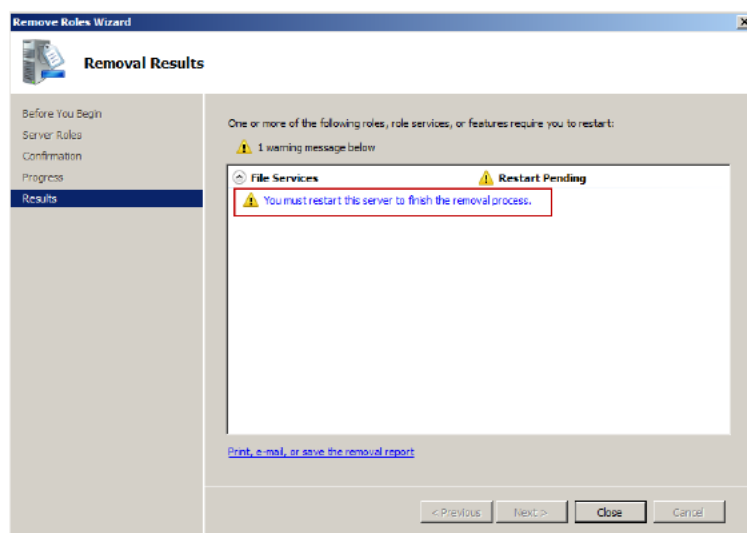
شکل ۲-۴۳

۳. در صفحه “Confirm Removal Selection” لیستی از Role های انتخاب شده و Role Service های مرتبط با آن نشان داده می شود. در صورت انتخاب صحیح موارد مورد نظر بر روی Remove کلیک کنید.



شکل ۲-۳۳

۴. پس از اتمام فرایند، “Removal Results” نشان داده می شود. در صورتی که Restart کردن سرور نیاز باشد، در این پنجره هشدار داده می شود. بر روی Close کلیک کنید.



شکل ۲-۳۵

## حذف Role ها در خط فرمان

حذف کردن Role ها از طریق Servermanagercmd.exe نیز امکان پذیر است. به مثال زیر توجه کنید:

```
C:\Users\Administrator>servermanagercmd -remove FS-FileServer FS-Resource-Manager
```

```
.
```

```
Start Removal...
```

```
Warning: [Removal] Succeeded: [File Services] File Server Resource Manager.
```

```
You
```

```
must restart this server to finish the removal process.
```

```
Warning: [Removal] Succeeded: [File Services] File Server. You must restart this server to finish the removal process.
```

```
<100/100>
```

```
Success: A restart is required to complete the removal.
```

```
C:\Users\Administrator>
```

پس از اجرای دستور، سرور را Restart نموده تا عملیات حذف تکمیل گردد. در صورتی که بخواهید سرور بعد از اجرای دستور بطور خودکار Restart شود، می توانید از دستور زیر استفاده کنید:

```
servermanagercmd -remove FS-FileServer FS-Resource-Manager -restart
```

شاید قصد داشته باشید جهت خودکارسازی فرایند، از یک فایل XML استفاده کنید. اگر به مثال های قبل بازگردید و در مقابل عبارت ServerManagerConfiguration Action مقدار Remove را قرار دهید همه چیز تمام است:

```
<?xml version="1.0" encoding="utf-8" ?>
<ServerManagerConfiguration Action="Remove"
xmlns="http://schemas.microsoft.com/sdm/Windows/ServerManager/
Configuration/2007/1" xmlns:xs="http://www.w3.org/2001/XMLSchema">
<RoleService Id="FS-FileServer" />
<RoleService Id="FS-Resource-Manager" />
</ServerManagerConfiguration>
```

دستورات بالا، مربوط به فایلی با نام RemoveFileServer.xml می باشد. حاصل اجرای این فایل به صورت زیر خواهد بود:

```
C:\Users\Administrator>servermanagercmd.exe -inputpath C:\RemoveFileServer.xml
..
```

```
Start Removal...
```

```
Warning: [Removal] Succeeded: [File Services] File Server Resource Manager.
You
must restart this server to finish the removal process.

Warning: [Removal] Succeeded: [File Services] File Server. You must restart
this server to finish the removal process.

<100/100>
Success: A restart is required to complete the removal.
```

### حذف کردن Role ها در PowerShell

در PowerShell هم می‌توان به سادگی و با دستور `Remove-WindowsFeature` عملیات حذف را انجام داد. قالب کلی این دستور به صورت زیر می‌باشد:

```
Remove-WindowsFeature <Role>,<RoleService>,<Feature> -restart -whatif
```

نتایج حاصل از اجرای پارامتر `-whatif` برای بررسی اتفاقاتی که با حذف کردن `File-Services` و `FS-Resource-Manager` می‌افتد، در ادامه آورده شده است:

```
PS C:\Users\Administrator> remove-windowsfeature File-Services,FS-Resource-Manager -whatif
```

```
What if: Checking if running in 'WhatIf' Mode.
What if: Performing operation "Remove-WindowsFeature" on Target "[File
Services]File Server Resource Manager".
What if: Performing operation "Remove-WindowsFeature" on Target "[File
Services]File Server".
What if: This server may need to be restarted after the removal completes.
```

```
Success Restart Needed Exit Code Feature Result
-----
True      Maybe          Success  {}
```

در صورتی که مشکلی در حذف وجود نداشت، می‌توانید دستورات زیر را اجرا کنید:

```
PS C:\Users\Administrator> remove-windowsfeature File-Services, FS-Resource-Manager
```

```
WARNING: [Removal] Succeeded: [File Services] File Server. You must restart
this server to finish the removal process.
WARNING: [Removal] Succeeded: [File Services] File Server Resource Manager.
You
must restart this server to finish the
removal process.
```

```
Success Restart Needed Exit Code Feature Result
-----
True      Yes              Succes   {File Server, File Server Resource Manager}
```

پس از اجرای موفق دستور باید سرور را Restart کنید. می‌توانید این کار را به صورت خودکار انجام دهید. فقط کافی است دستور زیر را وارد نمایید:



```
PS C:\Users\Administrator> remove-windowsfeature File-Services,FS-Resource-Manager -restart
```

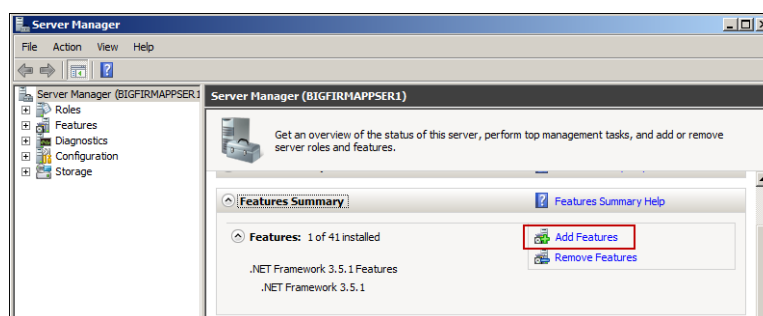
## ۲-۶-۳ افزودن و حذف کردن Feature ها

در این قسمت قصد داریم نحوه اضافه کردن Feature ها به فایل سروری که در قسمت های قبل ایجاد نمودید، و سپس حذف کردن آنها به کمک Server Manager، Servermanagercmd.exe و PowerShell را شرح دهیم. البته دقت داشته باشید که همه جزئیات را بیان نخواهیم کرد زیرا مراحل کار شبیه به اضافه و حذف کردن Role ها می باشد.

### اضافه کردن Feature

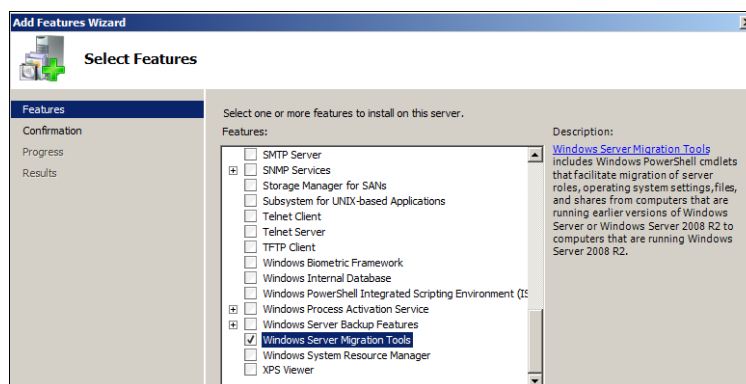
جهت اضافه کردن Feature ها مراحل زیر را دنبال کنید:

۱. Server Manager را اجرا نموده از قسمت Features Summery، گزینه Add Features را انتخاب کنید.



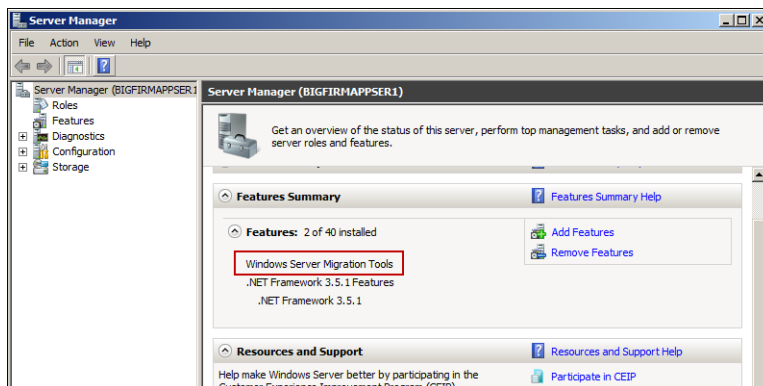
شکل ۲-۴۶

۲. ویزارد "Add Features Wizard" آغاز می گردد. در اینجا قصد داریم Feature ای با نام Windows Server Migration Tools را نصب کنیم، پس در صفحه "Select Features" آنرا انتخاب و بر روی Next کلیک کنید.



شکل ۲-۴۷

۳. پس از اتمام مراحل نصب، می توانید موفق بودن فرایند را در Server Manager مشاهده کنید.



شکل ۲-۴۸

### اضافه کردن Feature در خط فرمان

برای نصب Feature ها در خط فرمان نیز از ابزار `servermanagercmd.exe` استفاده می شود. به عنوان مثال برای نصب Feature قسمت قبل، دستور زیر را وارد کنید:

```
servermanagercmd.exe -install Migration
```

جهت ایجاد فایل پاسخ خودکار، دستورات زیر را در فایلی با نام `InstallFeature.XML` ذخیره کنید:

```
<?xml version="1.0" encoding="utf-8" ?>
<ServerManagerConfiguration Action="Install"
xmlns="http://schemas.microsoft.com/
sdm/Windows/ServerManager/Configuration/2007/1"
xmlns:xs="http://www.w3.org/2001/
XMLSchema">
<Feature Id="Migration" />
</ServerManagerConfiguration>
```

برای اجرا کردن فایل بالا می توانید از دستور زیر استفاده کنید:

```
servermanagercmd.exe -inputpath C:\InstallFeature.xml
```

در PowerShell نیز می توانید از طریق دستور زیر، فرایند نصب را انجام دهید:

```
PS C:\Windows\system32> add-windowsfeature migration
```

```
Success Restart Needed Exit Code Feature Result
```

```
-----
```

True	No	Success	{Windows Server Migration Tools}
------	----	---------	----------------------------------

## حذف کردن Featureها

کلیه مراحل در حذف Feature، همانند اضافه کردن آن می باشد.

- ♦ در Server Manager از گزینه Remove Features استفاده کنید.
- ♦ در خط فرمان ویندوز، از دستور `servermanagercmd.exe -remove <Feature Name>` استفاده کنید (برای مثال قبل: `servermanagercmd.exe -remove migration`).
- ♦ برای ایجاد فایل پاسخ خودکار، دستورات زیر را در فایلی به نام RemoveFeature.XML ذخیره کنید:

```
<?xml version="1.0" encoding="utf-8" ?>
<ServerManagerConfiguration Action="Remove"
xmlns="http://schemas.microsoft.com/
sdm/Windows/ServerManager/Configuration/2007/1"
xmlns:xs="http://www.w3.org/2001/
XMLSchema">
<Feature Id="Migration" />
</ServerManagerConfiguration>
```

جهت اجرای این فایل از دستور زیر استفاده کنید:

```
servermanagercmd.exe -inputpath C:\RemoveFeature.xml
```

- ♦ در نهایت با وارد نمودن دستور زیر در PowerShell، می توانید عملیات حذف را انجام دهید:

```
PS C:\Windows\system32> remove-windowsfeature migration

Success Restart Needed Exit Code Feature Result
-----
True      No                Success    {Windows Server Migration Tools}
```

۷-۲ نصب خودکار<sup>۱</sup> ویندوز

در سازمان های کوچک، مدیران شبکه ترجیح می دهند که سیستم عامل ها را بطور دستی بر روی کامپیوترها و یا سرورها نصب کنند. این کار با وجود تعداد کمی کامپیوتر شاید عملی لذت بخش باشد! اما زمانی که تعداد این کامپیوترها زیاد است، نصب سیستم عامل بر روی آنها عملی وقتگیر و خسته کننده می باشد، بخصوص زمانی که نیروی کمی جهت انجام این کار وجود داشته باشد.

فرایند نصب خودکار ویندوز از طریق ایجاد یک فایل پاسخ<sup>۲</sup> امکان پذیر است. افراد متخصصی که با نسخه های قدیمی ویندوز کار کرده باشند احتمالاً با این روش آشنا هستند. در گذشته با استفاده از ابزاری به نام Setup Manager، امکان ایجاد فایل های پاسخ و ویرایش آنها در برنامه Notepad وجود

1. Unattended Installation  
2. Answer File

داشت. با آغاز کار ویندوز ویستا، این روش دچار تغییراتی شد و به جای استفاده از Setup Manager، مجموعه‌ای به نام WAIK<sup>۱</sup> به کارگیری شد. در واقع WAIK مجموعه‌ای از ابزارهای قدرتمند است که قادر است یک DVD جهت Boot کردن ویندوز ایجاد کند. یکی از ابزارهای مهم در این مجموعه، WSIM<sup>۲</sup> است که جایگزین Setup Manager بوده و جهت ایجاد فایل‌های پاسخ در ویندوزهای ویستا، سرور 2008، ویندوز ۷ و سرور 2008R2 مورد استفاده قرار می‌گیرد.

از تغییرات دیگری که در این مجموعه می‌توان به آن اشاره نمود، فرمت فایل‌های پاسخ می‌باشد. فایل‌هایی که با Setup Manager ایجاد می‌شود، فایل‌های متنی (txt) هستند که در برنامه Notepad قابل ویرایش بوده و شخصی‌سازی آنها نیازمند انجام کارهای زیادی است. در WSIM، فایل‌ها با فرمت XML ایجاد می‌شوند و کار زیادی جهت شخصی‌سازی آنها لازم نیست. البته جای نگرانی وجود ندارد زیرا نیازی به دانستن برنامه‌نویسی ندارید، تنها کاری که شما در ویرایش این فایل انجام می‌دهید، پیدا کردن مواردی مثل Product Key و تغییر دادن آنها است.

در ادامه، توسعه ویندوز سرور 2008R2 را به روش نصب خودکار و همچنین چگونگی نصب مجموعه WAIK را برای ایجاد فایل پاسخ شرح خواهیم داد. البته توجه داشته باشید که مطالب تشریح شده، در مورد ویندوز ویستا، سرور 2008 و ویندوز ۷ هم قابل استفاده می‌باشد.

## ۲-۷-۱ نصب WAIK

در این قسمت قصد داریم نحوه نصب ویندوز سرور 2008R2 را با کمترین میزان دخالت شما در فرایند نصب آموزش دهیم. قبل از شروع کار باید مجموعه WAIK را در اختیار داشته باشید. جهت دریافت این مجموعه می‌توانید به آدرس [www.microsoft.com/downloads](http://www.microsoft.com/downloads) مراجعه نموده و عبارت WAIK را جستجو کنید. پس از جستجو، نسخه متناسب با سیستم عامل خود را پیدا نموده و آنرا دریافت کنید. فایل دریافتی دارای حجمی در حدود ۱.۶ گیگابایت و با فرمت ISO می‌باشد. بنابراین جهت استفاده می‌توانید آنرا بر روی DVD رایت نموده و یا از برنامه‌هایی مثل Virtual Clone Drive جهت باز کردن فایل ISO استفاده کنید.

در اینجا ما از سیستم عامل ویندوز ۷ جهت نصب WAIK استفاده می‌کنیم. شما نیز می‌توانید آن را بر روی سیستم عامل خود و یا سیستم عاملی که به کمک ماشین‌های مجازی (مثل VMware یا ...) ایجاد نموده‌اید، نصب کنید. فقط دقت داشته باشید که حداقل پیش‌نیازهای نصب WAIK: دارا بودن ویندوز XP SP2 و یا نسخه‌های بعد از آن، NET Framework 2.0 و MSXML 6 SP1 می‌باشد. این پیش‌نیازها بر روی مجموعه WAIK موجود است و می‌توانید آنها را از روی رسانه مورد نظر نصب کنید.

---

1. Windows Automated Installation Kit  
2. Windows System Image Manager

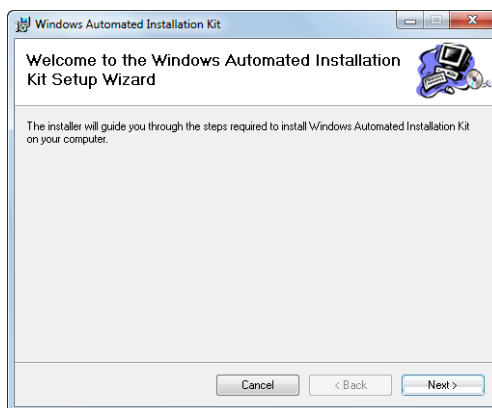
جهت نصب بسته WAIK مراحل زیر را دنبال کنید:

۱. پس از قراردادن رسانه مورد نظر که ممکن است DVD یا فایل ISO باشد، فایل StartCD.exe را از روی آن اجرا کنید. صفحه‌ای شبیه زیر نمایش داده می‌شود. از منوی سمت چپ، گزینه Windows AIK Setup را انتخاب کنید.



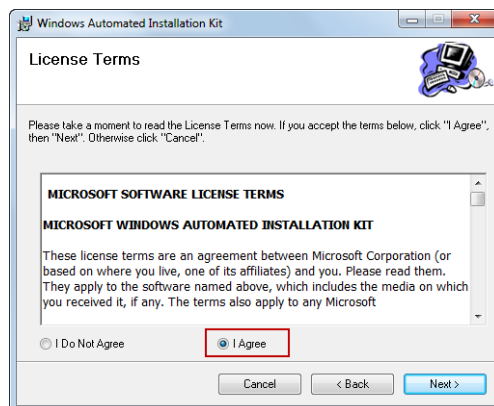
شکل ۲-۴۹

۲. با مشاهده صفحه “Welcome to the Windows Automated Installation Kit Setup Wizard” بروی Next کلیک کنید.



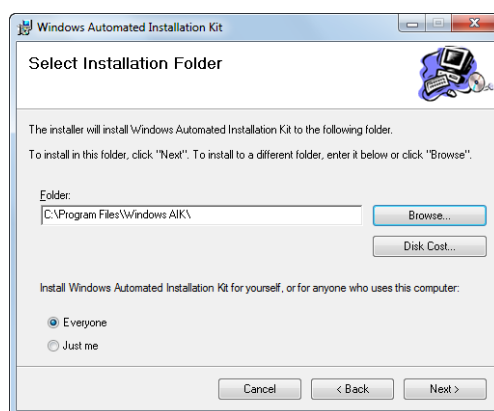
شکل ۲-۵۰

۳. در صفحه “License Terms”، گزینه “I Agree” را انتخاب و بروی Next کلیک کنید.



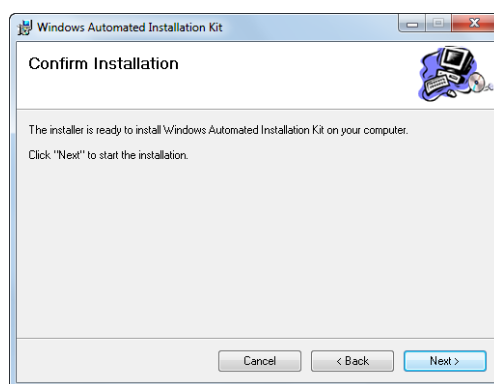
شکل ۵۱-۲

۴. در صفحه "Select Installation Folder" مسیر نصب را مشخص نموده و بر روی Next کلیک کنید.



شکل ۵۲-۲

۵. در صفحه "Confirm Installation" بر روی Next کلیک نموده تا عملیات نصب آغاز گردد.



شکل ۵۳-۲

۶. پس از اتمام مراحل نصب، بر روی Close کلیک نموده و کلیه پنجره‌ها را ببندید.

## ۲-۷-۲ ایجاد فایل پاسخ

قبل از ایجاد فایل پاسخ، اجازه دهید نگاهی به اتفاقاتی که هنگام نصب ویندوز و در پشت پرده رخ می‌دهند بیندازیم.

در ویندوز ویستا، ویندوز ۷، سرور 2008 و 2008R2، روال نصب از هفت گذرگاه<sup>۱</sup> پیکربندی عبور می‌کند. این گذرگاه‌ها، در جدول ۲-۵ نشان داده شده‌اند و به ترتیب از ۱ تا ۷ شماره‌گذاری می‌شوند. هر کدام از این گذرگاه‌ها، مسئول انجام وظایف خاصی هستند ولی در اصل، سه گذرگاه جهت اجرای عملیات نصب خودکار مورد نیاز می‌باشد (گذرگاه‌های ۱، ۴ و ۷).

جدول ۲-۵ گذرگاه‌های پیکربندی نصب ویندوز

شماره	گذرگاه	شرح
۱	windowsPE	راه‌اندازی محیط نصب windowsPE، پیکربندی Product Key، پیکربندی دیسک جهت نصب ویندوز بر روی آن، تنظیمات مربوط به مشخصات کاربر
۲	offlineServicing	اعمال آپدیت‌ها بر روی محتویات ویندوز، نرم افزارها و زبان
۳	Specialize	تنظیمات پیکربندی که بر روی هر سیستم به صورت شخصی می‌باشد، مانند تنظیمات شبکه، منطقه جغرافیایی و دامنه
۴	Generalize	عمومی کردن سیستم، مثلاً اضافه کردن نام کامپیوتر و یا منطقه زمانی
۵	auditSystem	انجام پردازش‌های مربوط به حساب‌های کاربری قبل از ورود کاربر
۶	auditUser	انجام پردازش‌های مربوط به حساب‌های کاربری بعد از ورود کاربر
۷	oobeSystem	اعمال تنظیمات قبل از ورود به صفحه Desktop

جهت ایجاد فایل پاسخ مراحل زیر را دنبال کنید:

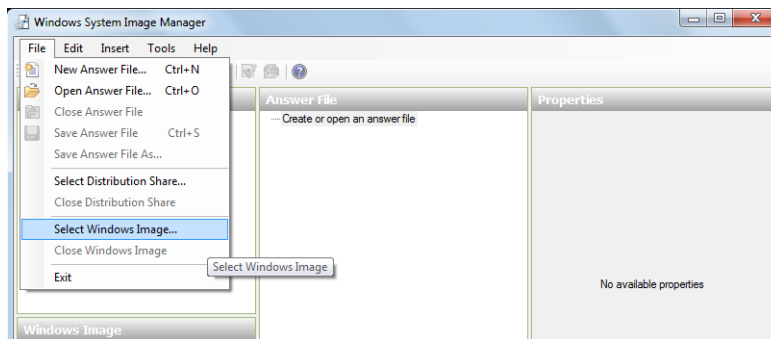
۱. ابتدا DVD یا فایل Image مربوط به ویندوز سرور 2008R2 را باز نموده و فایل Install.wim را از داخل پوشه‌ای به نام Sources، به مسیر C:\W2008R2\ (پوشه‌ای با نام W2008R2 در درایو C) بر روی کامپیوتر خود کپی کنید (حجم این فایل در حدود 2.5GB است).

1. Pass

۲. برنامه WSIM را از مسیر زیر اجرا کنید:

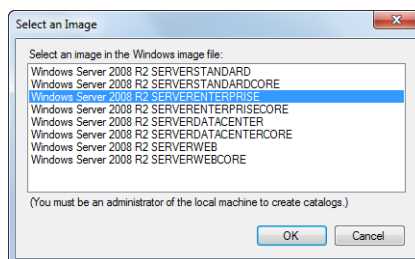
Start» All Programs» Microsoft Windows AIK» Windows System Image Manager

۳. از مسیر File «Select Windows Image، فایلی که در درایو C کپی نموده‌اید را انتخاب کنید:



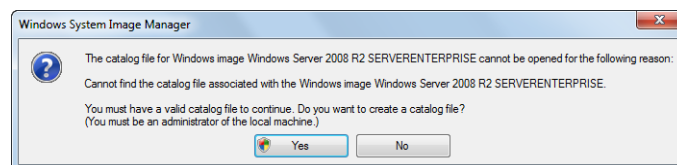
شکل ۲-۵۴

۴. پس از باز کردن فایل Install.wim، پنجره‌ای حاوی ویرایش‌های ویندوز سرور 2008R2 نشان داده می‌شود. ویرایش موردنظر (Enterprise) را انتخاب نموده و بر روی OK کلیک کنید.



شکل ۲-۵۵

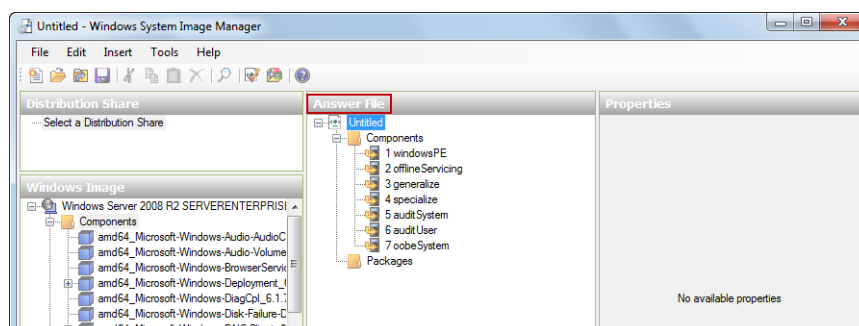
۵. پیغامی ظاهر شده و اعلام می‌کند که فایل کاتالوگ<sup>۱</sup> (فایلی که محتویات فایل Image را به صورت فهرست درآورده و جهت انجام عملیات از آن استفاده می‌کند) وجود ندارد. جهت ایجاد این فایل بر روی Yes کلیک کنید.



شکل ۲-۵۶

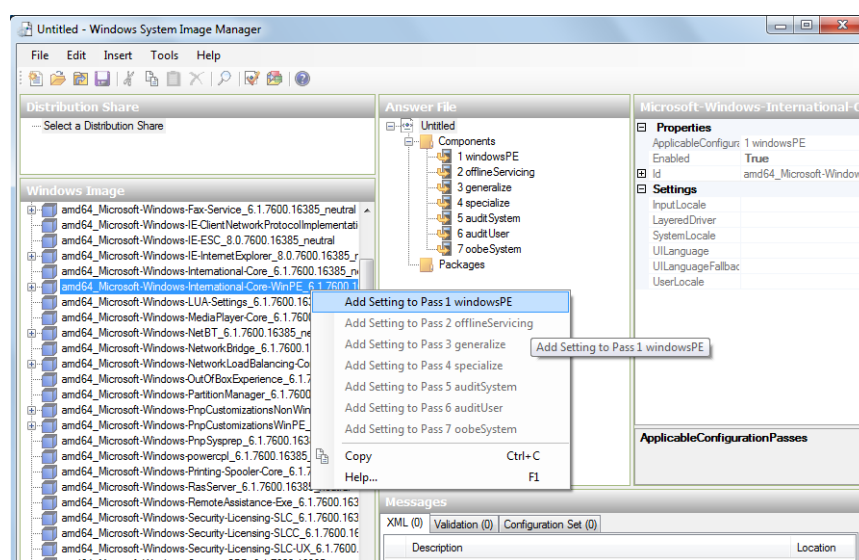


۶. ایجاد فایل کاتالوگ ممکن است چند دقیقه طول بکشد، بنابراین تا اتمام آن منتظر بمانید.
۷. پس از پایان عملیات می‌توانید فایل مورد نظر را از مسیر C:\W2008R2 مشاهده کنید.
۸. محتویات فایل کاتالوگی که ایجاد نموده‌اید، در پنل سمت راست (Windows Image) از پنجره WSIM قابل مشاهده می‌باشد. از منوی File، گزینه New Answer File را جهت ایجاد یک فایل پاسخ انتخاب کنید.
۹. فایل پاسخ ایجاد شده، در قسمت Answer File نمایش داده می‌شود.



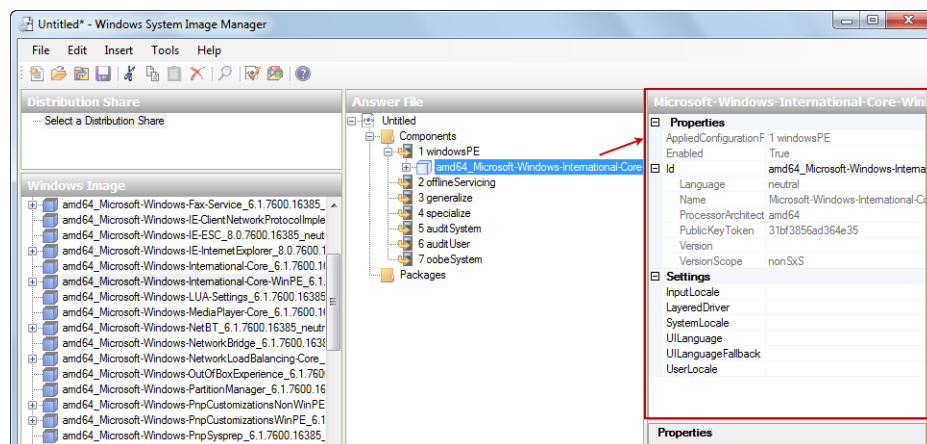
شکل ۲-۵۷

۱۰. از بین Component‌های موجود در قسمت Windows Images (Component «Windows Image») بروی amd64\_Microsoft-Windows-International-Core-WinPE کلیک‌راست نموده و گزینه Add Setting to Pass1 windowsPE را انتخاب کنید.



شکل ۲-۵۸

۱۱. پس از انتخاب گزینه مذکور، اگر بار دیگر به پنل Answer File بازگردید، مشاهده خواهید نمود که Component مورد نظر به فایل پاسخ اضافه شده است. با کلیک بر روی این Component می‌توانید از پنل سمت راست، مشخصات آنرا ویرایش کنید.



شکل ۲-۵۹

۱۲. طبق جدول ۲-۶، مشخصه‌های<sup>۱</sup> مورد نظر را با مقادیر داده شده، تکمیل کنید:

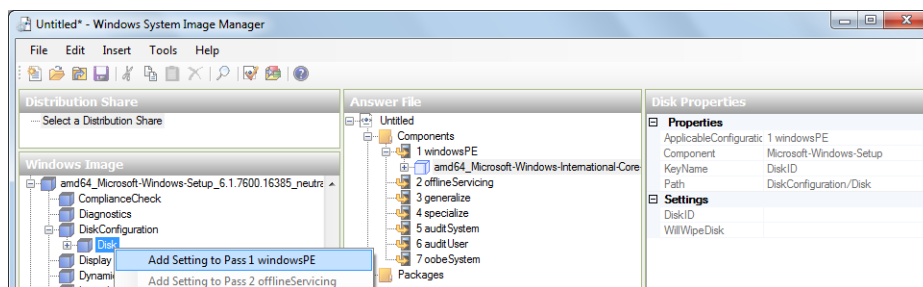
جدول ۲-۶ مشخصه‌های مربوط به Component زبان سیستم

مقدار	مشخصه	Component	PASS
en-us	InputLocale	amd64_Microsoft-Windows-International-Core-WinPE	۱
en-us	SystemLocale		
en-us	UILanguage		
en-us	UILanguageFallback		
en-us	SystemLocale		

تنظیمات بالا، زبان انگلیسی را برای صفحه کلید و سیستم انتخاب نموده و بر روی مشخصه‌های ذکر شده تنظیم می‌کند. دقت کنید که باید مقدار UILanguage را در SetupUILanguage که زیرمجموعه Component فعلی می‌باشد، به en-us تغییر دهید. البته می‌توانید با وارد نمودن مقدار fa-IR، زبان را بر روی فارسی نیز تنظیم کنید. با کلیک بر روی هر مشخصه و فشردن کلید F1 می‌توانید به زبان‌های پشتیبانی شده و همچنین اطلاعات بیشتر در مورد هر مشخصه دسترسی پیدا کنید.

1. Property

اکنون باید تعدادی Component دیگر (با همان روش قبلی) اضافه نموده و مشخصه‌های آنها را به مقادیری که در ادامه مشاهده می‌کنید، تغییر دهید.



شکل ۶۰-۲

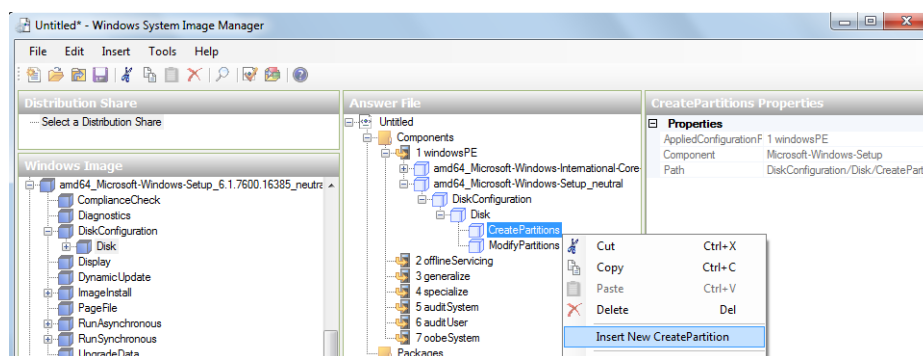
۱۳. Component بعدی مربوط به پیکربندی دیسک جهت نصب ویندوز بر روی آن می‌باشد.

جدول ۷-۲ مشخصه‌های مربوط به Component دیسک

مقدار	مشخصه	Component	PASS
0	DiskID	amd64_Microsoft-Windows-Setup\DiskConfiguration\Disk	۱
True	WillWipeDisk		

در جدول بالا، به Installer اعلام می‌کنید که عملیات نصب ویندوز را بر روی دیسک شماره صفر انجام دهد. توجه داشته باشید که دیسک شماره صفر، اولین دیسک موجود بر روی کامپیوتر می‌باشد (زمانی که چندین دیسک متصل به کامپیوتر یا سرور دارید).

در پنل Answer File، برای Component بالا دو SubComponent (زیرکامپوننت) به نام‌های CreatePartitions و ModifyPartitions وجود دارد. جهت اضافه کردن پارتیشن‌ها در دیسک شماره صفر، می‌توانید بر روی CreatePartitions کلیک راست نموده و گزینه Insert New را انتخاب کنید.



شکل ۶۱-۲

از مشخصه Size می‌توانید حجم هر پارتیشن را بر حسب مگابایت تعیین نمایید. به عنوان مثال، ۴۰ گیگابایت را با ۴۰۹۶۰ مقداردهی کنید. فقط دقت داشته باشید که به ازای هر زیرکامپوننت CreatePartitions، یک زیرکامپوننت ModifyPartitions جهت تنظیم مشخصات آن ایجاد کنید. پس از ایجاد پارتیشن، تنظیمات زیر را بر روی آن اعمال کنید:

جدول ۲-۸ مشخصه‌های مربوط به زیرکامپوننت CreatePartition

مقدار	مشخصه	Component	PASS
True	Extend	amd64_Microsoft-Windows-Setup\ DiskConfiguration\ Disk\ CreatePartitions\CreatePartition	۱
1	Order		
Primary	Type		

در صورتی که قصد دارید تنظیمات هر پارتیشن را تغییر دهید، می‌توانید از زیرکامپوننت ModifyPartitions استفاده کنید.

جدول ۲-۹ مشخصه‌های مربوط به زیرکامپوننت ModifyPartition

مقدار	مشخصه	Component	PASS
True	Active	amd64_Microsoft-Windows- Setup\ DiskConfiguration\Disk\ CreatePartitions\ModifyPartition	۱
NTFS	Format		
Windows	Label		
C	Letter		
1	Order		
1	PartitionsID		

در تنظیمات بالا، به کمک مشخصه PartitionId تعیین می‌کنید که اولین پارتیشن بر روی دیسک شما، پارتیشن فعلی باشد (با قراردادن مقدار ۱). در مشخصه Active، با قراردادن مقدار True اجرای عملیات Boot از روی آن پارتیشن را امکان‌پذیر می‌کنید. مشخصه Format، نحوه فرمت‌بندی پارتیشن را مشخص می‌کند. مشخصه‌های Label و Letter جهت برچسب زدن و نامگذاری پارتیشن استفاده می‌شوند.

۱۴. در Component بعد، ویرایش ویندوز سرور مشخص می‌گردد. جهت آگاهی از ویرایش‌های ویندوز، می‌توانید در ابزار Windows PE Tools Command Prompt (این ابزار از مسیر Start » All Programs » Microsoft Windows AIK قابل دسترسی می‌باشد) دستور زیر را وارد کنید:

**IMAGEX /info C:\W2008R2\INSTALL.WIM**

قالب کلی این دستور به صورت زیر می‌باشد:

**IMAGEX.EXE /info <.wim File Path>**

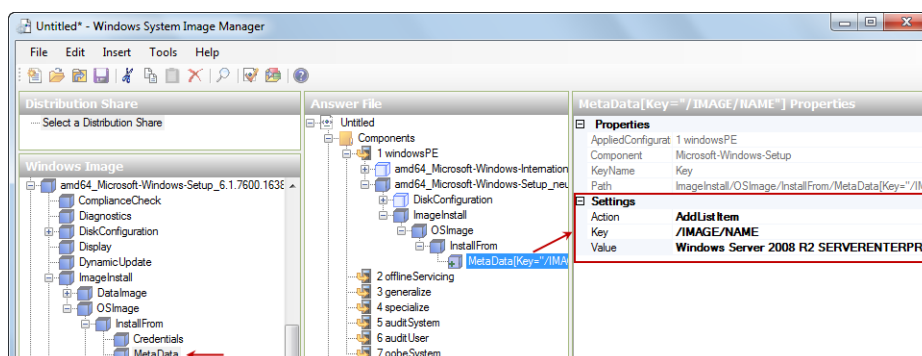
نتایج حاصل از اجرای این دستور، به صورت زیر می‌باشد:

```
.
.
<NAME>Windows Server 2008 R2 SERVERSTANDARD</NAME>
<DESCRIPTION> Windows Server 2008 R2 SERVERSTANDARD</DESCRIPTION>
<FLAGS>ServerStandard</FLAGS>
<WINDOWS>
.
.
<NAME>Windows Server 2008 R2 SERVERENTERPRISE</NAME>
<DESCRIPTION> Server 2008 R2 SERVERENTERPRISE</DESCRIPTION>
<FLAGS>ServerEnterprise</FLAGS>
<WINDOWS>
.
.
<NAME>Windows Server 2008 R2 SERVERDATACENTER</NAME>
<DESCRIPTION>Windows Server 2008 R2 SERVERDATACENTER</DESCRIPTION>
<FLAGS>ServerDatacenter</FLAGS>
<WINDOWS>
```

پس از انتخاب ویرایش ویندوز، مقادیر موجود در جدول ۲-۱۰ را جایگذاری کنید.

جدول ۲-۱۰ مشخصه‌های مربوط به Component ویرایش ویندوز

مقدار	مشخصه	Component	PASS
/IMAGE/NAME	Key	amd64_Microsoft-Windows-Setup\ImageInstall\OSImage\InstallFrom \Metadata	۱
Windows Server 2008 R2 SERVERENTERPRISE	Value		



شکل ۲-۶۲

۱۵. Component زیر مشخص می‌کند که ویندوز بر روی دیسک شماره صفر و پارتیشن شماره یک از آن دیسک، نصب گردد. پارتیشن شماره یک، اولین پارتیشن بر روی دیسک شما خواهد بود.

جدول ۱۱-۲ مشخصه‌های مربوط به Component دیسک و پارتیشن نصب ویندوز

مقدار	مشخصه	Component	PASS
0	DiskID	amd64_Microsoft-Windows- Setup \InstallImage\OSImage \InstallTo	۱
1	PartitionID		

۱۶. Component و SubComponent بعدی، مربوط به اطلاعات کاربر و Product Key می‌باشد.

جدول ۱۲-۲ مشخصه‌های مربوط به Component و SubComponent اطلاعات کاربر و Product Key

مقدار	مشخصه	Component	PASS
True	AcceptEula	amd64_Microsoft-Windows-Setup\ UserData	۱
Bigfirm	FullName		
Bigfirm	Organization		
HFG76-34GFT-O6ID9-MNBW-IYUSD	Key	amd64_Microsoft-Windows-Setup\UserData\ProductKey	

۱۷. Component زیر، مربوط به نام و منطقه زمانی کامپیوتر است و در گذرگاه ۴ تنظیم می‌شود. با قرار دادن مقدار \* در مشخصه ComputerName، یک نام تصادفی برای آن انتخاب می‌شود. از مشخصه TimeZone نیز می‌توانید منطقه زمانی را مشخص کنید. جهت اطلاع از منطقه زمانی می‌توانید بر روی فیلد مربوط به مشخصه آن کلیک نموده و کلید F1 را فشار دهید.

جدول ۱۳-۲ مشخصه‌های مربوط به Component تنظیمات عمومی سیستم

مقدار	مشخصه	Component	PASS
*	ComputerName	amd64_Microsoft-Windows-Shell-Setup	۴
Eastern Standard Time	TimeZone		

۱۸. Componen بعدی، مربوط به Active کردن ویندوز به صورت خودکار می‌باشد. پس از نصب، در صورت داشتن Product Key معتبر، ویندوز به صورت خودکار Active می‌شود. در ویندوز سرور

2008 این Component با نام Wow64\_Microsoft-Windows-Security-Licensing-SLC-UX شناخته می‌شود.

جدول ۲-۱۴ مشخصه مربوط به کامپوننت Active کردن خودکار ویندوز

مقدار	مشخصه	Component	PASS
False	SkipAutoActivation	wow64_Microsoft-Windows-Security-SPP-UX	۴

۱۹. SubComponent بعدی، در گذرگاه ۷ اضافه می‌گردد. در این SubComponent، فایروال با استفاده از تنظیمات شبکه پیکربندی می‌شود. در مشخصه Protect Your PC، با قراردادن مقدار ۱ تعیین می‌کنید که آپدیت خودکار ویندوز فعال باشد.

جدول ۲-۱۵ مشخصه‌های مربوط به کامپوننت تنظیمات شبکه و فایروال

مقدار	مشخصه	Component	PASS
True	HideEULAPage	amd64_Microsoft-Windows-Shell-Setup\OOBE	۷
Eastern Standard Time	NetworkLocation		
1	ProtectYourPC		

۲۰. پس از اضافه کردن Component‌های مورد نظر، می‌توانید فایل پاسخ را ایجاد کنید. جهت انجام این کار، از منوی File گزینه Save Answer File As را انتخاب نموده و فایل پاسخ را با نام autounattend.xml ذخیره کنید.

پس از ایجاد فایل، آنرا در برنامه Notepad باز کنید. محتویات فایل ایجاد شده شبیه زیر خواهد بود:

```
ml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
  <settings pass="windowsPE">
    <component name="Microsoft-Windows-International-Core-WinPE"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIconfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <SetupUILanguage>
        <UILanguage>en-us</UILanguage>
      </SetupUILanguage>
      <InputLocale>en-us</InputLocale>
      <SystemLocale>en-us</SystemLocale>
      <UILanguage>en-us</UILanguage>
```

---

```

        <UILanguageFallback>en-us</UILanguageFallback>
        <UserLocale>en-us</UserLocale>
    </component>
    <component name="Microsoft-Windows-Setup"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <DiskConfiguration>
            <Disk wcm:action="add">
                <CreatePartitions>
                    <CreatePartition wcm:action="add">
                        <Extend>true</Extend>
                        <Order>1</Order>
                        <Type>Primary</Type>
                    </CreatePartition>
                </CreatePartitions>
                <ModifyPartitions>
                    <ModifyPartition wcm:action="modify">
                        <Active>true</Active>
                        <Extend>true</Extend>
                        <Format>NTFS</Format>
                        <Label>Windows</Label>
                        <Letter>C</Letter>
                        <Order>1</Order>
                        <PartitionID>1</PartitionID>
                    </ModifyPartition>
                </ModifyPartitions>
                <DiskID>0</DiskID>
                <WillWipeDisk>true</WillWipeDisk>
            </Disk>
        </DiskConfiguration>
        <ImageInstall>
            <OSImage>
                <InstallFrom>
                    <MetaData wcm:action="add">
                        <Key>/IMAGE/NAME</Key>
                        <Value>Windows Server 2008 R2</Value>
                    </MetaData>
                </InstallFrom>
                <InstallTo>
                    <DiskID>0</DiskID>
                    <PartitionID>1</PartitionID>
                </InstallTo>
            </OSImage>
        </ImageInstall>
        <UserData>
            <ProductKey>
                <Key>HFG76-34GFT-06ID9-MNBW-IYUSD</Key>
            </ProductKey>
            <AcceptEula>true</AcceptEula>
            <FullName>Bigfirm</FullName>
            <Organization>Bigfirm</Organization>
        </UserData>
    </component>

```



```

        </UserData>
    </component>
</settings>
<settings pass="specialize">
    <component name="Microsoft-Windows-Shell-Setup"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIconfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <ComputerName>*</ComputerName>
        <TimeZone>Eastern Standard Time</TimeZone>
    </component>
</settings>
<settings pass="oobeSystem">
    <component name="Microsoft-Windows-Shell-Setup"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIconfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <OOBE>
            <HideEULAPage>true</HideEULAPage>
            <NetworkLocation>Work</NetworkLocation>
            <ProtectYourPC>1</ProtectYourPC>
        </OOBE>
    </component>
</settings>
<cpu:offlineImage cpu:source="wim:c:/w2008r2/install.wim#Windows Server
2008 R2 SERVERENTERPRISE" xmlns:cpu="urn:schemas-microsoft-com:cpu" />
</unattend>

```

## ۲-۷-۳ استفاده از فایل پاسخ

جهت استفاده از فایل پاسخ autounattend.xml که در مرحله قبل ایجاد نمودید، ابتدا باید آنرا در ریشه یک رسانه قابل حمل (مثل USB) ذخیره کنید. سپس در زمان بوت شدن سرور از روی DVD یا فایل ISO، رسانه فایل پاسخ را در سیستم قرار دهید.

در اینجا، فرض بر این است که از DVD جهت نصب ویندوز سرور 2008R2 استفاده می‌کنید. رسانه حاوی فایل پاسخ را همزمان با ویندوز قرار دهید. این رسانه می‌تواند یک USB و یا یک CD/DVD باشد. در صورتی که بخواهید از CD/DVD استفاده کنید، باید مجهز به دو دیسک خوان باشید، یکی برای اجرای ویندوز سرور و دیگری جهت اجرای فایل پاسخ. پیشنهاد ما این است که از USB استفاده کنید.

اگر از ماشین‌های مجازی استفاده می‌نمایید، کار کمی سخت‌تر می‌شود. ابتدا باید یک درایو CD/DVD ثانویه به ماشین مجازی خود اضافه نموده و سپس یک فایل ISO حاوی فایل پاسخ ایجاد نمایید. جهت ایجاد این فایل، می‌توانید دستور زیر را در ابزار Windows PE Tools command prompt

وارد کنید:

```
oscdimg -n C:\Answer C:\answer.iso
```

این دستور، محتویات پوشه Answer که در درایو C قرار دارد را به فایلی با نام answer.iso تبدیل می‌کند. قالب کلی این دستور به صورت زیر می‌باشد:

< محل و نام فایل ISO جدید > < پوشه‌ای که قصد دارید به فایل ایزو تبدیل کنید > -n oscdimg

توجه داشته باشید که رسانه فایل پاسخ باید همزمان با راه‌اندازی عملیات Boot از روی DVD ویندوز در دستگاه مربوطه قرارگیرد.



## « فصل ۳ »

آشنایی با Server Core

**Introduction to Server Core**  
INTRODUCTION TO SERVER CORE



مایکروسافت همواره به دنبال ارائه واسطه‌های گرافیکی جهت مدیریت بهتر سرورهای مبتنی بر ویندوز بوده است. اما با توجه به نیازهای بازار و اینکه تعداد زیادی از مدیران، خط فرمان را به عنوان واسطه خود و سرور به کار می‌گیرند، این شرکت تصمیم گرفت که ویرایش جدیدی از ویندوز سرور را با نام Server Core ایجاد نموده و توسعه دهد. این ویرایش که با انتشار ویندوز سرور 2008 ایجاد شد، قادر است دستورات مدیران را در محیط خط فرمان پذیرفته و آنها را به سرعت اجرا کند. در این فصل قصد داریم به نحوه مدیریت سرور در ویرایش Server Core از ویندوز سرور 2008 و 2008R2 بپردازیم. بطور کلی مهمترین مباحثی که در این فصل به آنها پرداخته خواهد شد عبارتند از:

- بررسی اهداف Server Core
- نصب و پیکربندی Server Core
- راه‌اندازی Server Core جهت توسعه در مراکز اداری
- مدیریت سرور از راه دور

### ۳-۱ Server Core چیست؟

اگر جزء افرادی باشید که اخبار مربوط به سیستم عامل‌های لینوکس و ویندوز را دنبال می‌کنند، حتماً به این مسئله پی برده‌اید که رقابت شدیدی میان این سیستم عامل‌ها و کاربران آن وجود دارد. با اینکه مایکروسافت واسطه‌های گرافیکی بسیاری را در اختیار کاربران قرار می‌دهد، اما هنوز لینوکس جزء سیستم عامل‌های پرطرفدار به شمار می‌رود. محبوبیت لینوکس در بین کاربران آن دلایل زیادی دارد که در ادامه، به تعدادی از آنها اشاره می‌کنیم:

- لینوکس، یک سیستم عامل منبع باز است و می‌توانید بدون پرداخت هیچ هزینه‌ای آنرا در اختیار داشته و حتی با توجه به نیازهای خود گسترش دهید.
- به همراه لینوکس، ابزارها و برنامه‌های اضافی نصب نمی‌شود. هنگام نصب ویندوز سرور 2000 و 2003 باید ابزارهایی را نصب کنید که ممکن است حتی برای یکبار هم مورد استفاده قرار نگیرند، مانند Windows Audio و Internet Explorer.
- از آنجایی که ابزارهای کمتری نصب می‌شود، مصرف منابعی مانند CPU نیز کاهش می‌یابد.
- نصب کمتر ابزارها مشکلاتی همچون اجرای ناموفق سیستم عامل، برنامه‌ها و ابزارها و همچنین نیاز به برطرف نمودن این مشکلات را کاهش می‌دهد.

مایکروسافت برای پاسخگویی به این نیازها ویرایش Server Core را با حداقل نیاز به منابع سخت افزاری، بر روی ویندوز سرورهای 2008 و 2008R2 گسترش داد. در این ویرایش، واسطه‌های گرافیکی

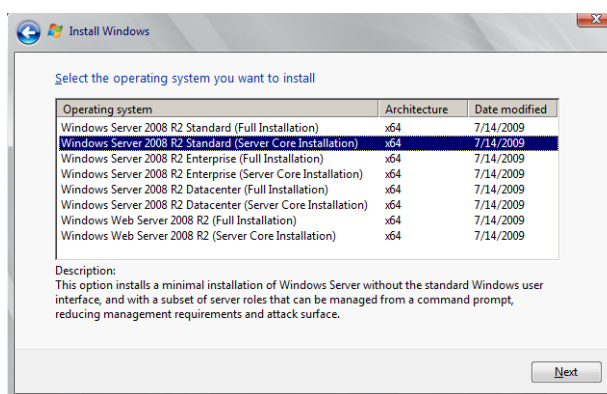
از جمله Windows Explorer، Internet Explorer و اجزاء وابسته به آنها حذف شده است. این مسئله بدین معناست که تنها واسطه اصلی جهت ارتباط با ویندوز و مدیریت آن، خط فرمان (Cmd) می باشد.

### ۲-۳ نصب Server Core

قبل از اقدام به نصب Server Core لازم است بدانید که فقط امکان نصب این ویرایش وجود دارد و نمی توان آنرا به سایر ویرایش ها ارتقاء داد. همچنین امکان ارتقاء سایر ویرایش ها به نسخه Server Core نیز وجود ندارد.

عملیات نصب Server Core همانند نصب سایر ویرایش ها می باشد. برای نصب، مراحل زیر را دنبال کنید:

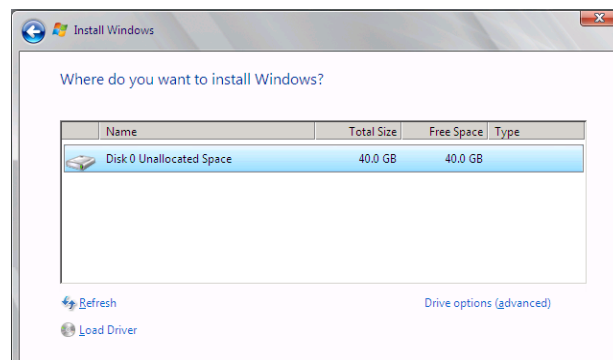
۱. رسانه (DVD) ویندوز سرور 2008R2 را قرار داده و اجازه دهید تا سرور از روی آن راه اندازی شود. ادامه عملیات را می توانید به صورت دستی و یا از طریق فایل پاسخی که توسط WAIK (به فصل قبل نگاه کنید) ایجاد نموده اید انجام دهید.
۲. تنظیمات زبان را انجام داده و بر روی Next کلیک کنید (شکل ۱-۳).
۳. بر روی دکمه Install now کلیک کنید (شکل ۲-۳).
۴. در صفحه "Type your product key for activation" کد License را وارد نموده (در صورتی که آنرا در اختیار دارید) و بر روی Next کلیک کنید (شکل ۳-۳).
۵. در صفحه "Select the operating system you want to install" یکی از ویرایش های Server Core را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۱-۳

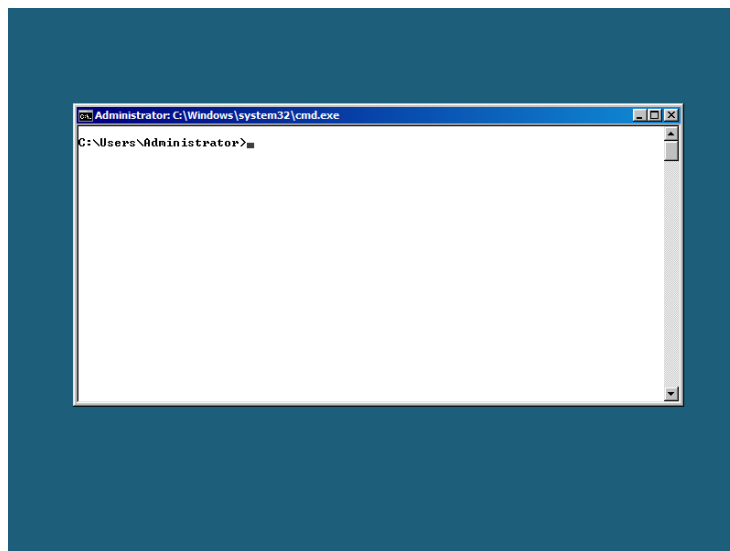
۶. در صفحه "Please read the license terms" گزینه I accept the license terms را انتخاب نموده و بر روی Next کلیک کنید (شکل ۵-۳).

۷. در صفحه "Where do you want to install Windows" باید محل نصب ویندوز را مشخص کنید. هنگام انتخاب محل نصب سیستم عامل، پیشنهاد می‌کنیم که فضای دیسک خود را به دو پارتیشن تقسیم کنید. یک پارتیشن با حجم 20GB برای سیستم عامل، و پارتیشن دیگر که حاوی فضای باقیمانده از دیسک می‌باشد برای نگهداری داده‌ها و برنامه‌ها. با این کار دیگر مجبور نیستید که در صورت نیاز از کل فضای دیسک Backup گیری کنید. البته انتخاب این فضا اختیاری بوده و میزان فضایی که جهت نصب Server Core به آن نیاز دارید حدوداً 3GB می‌باشد.



شکل ۲-۳

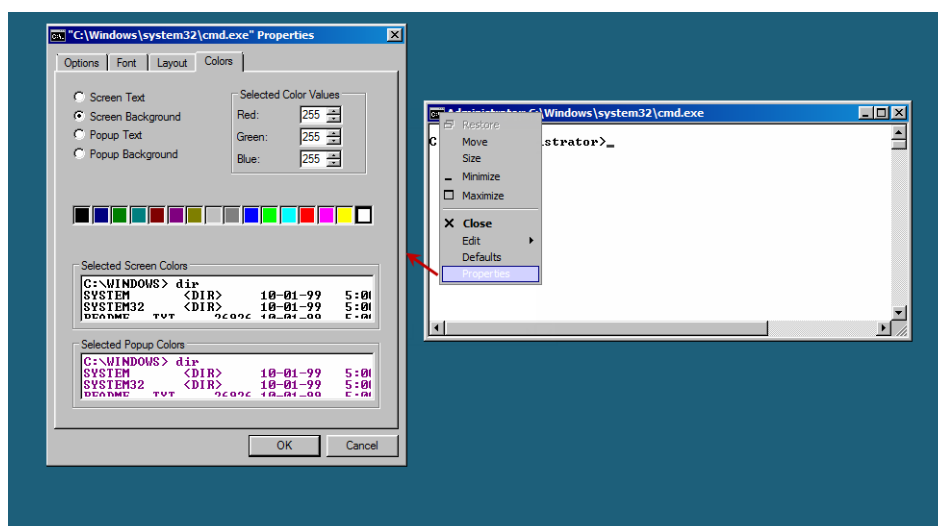
۸. پس از پایان نصب، رمز عبور جدیدی تعیین نموده و وارد سیستم شوید. اولین صفحه‌ای که مشاهده خواهید نمود به صورت زیر می‌باشد.



شکل ۳-۳



توجه داشته باشید که رنگ پس زمینه خط فرمان، با آنچه که در اینجا مشاهده می‌کنید متفاوت است زیرا در اینجا رنگ آنرا تغییر داده‌ایم. در صورتیکه قصد انجام چنین کاری را داشته باشید می‌توانید بر روی لبه بالا و سمت راست پنجره خط فرمان کلیک‌راست نموده و گزینه Properties را انتخاب کنید. در این پنجره امکاناتی جهت تغییر رنگ پس‌زمینه و متن وجود دارد.



شکل ۳-۴

### ۳-۳ راهنمایی‌های ضروری در Server Core

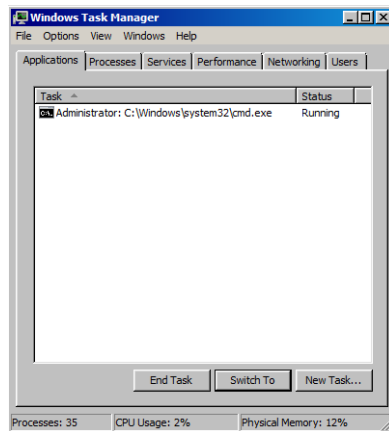
به دلیل کمبود واسطه‌های گرافیکی در این سیستم عامل، لازم است تعدادی راهنمایی در رابطه با دسترسی به عملکردهای آن ارائه دهیم.

#### ۱-۳-۳ دسترسی به Task Manager

در Server Core تعداد کمی از واسطه‌های گرافیکی به کار گرفته شده است که مهمترین آنها Task Manager می‌باشد. Task Manager همان ابزاری است که در سایر نسخه‌های ویندوز به کار رفته است و جهت مدیریت پردازش‌ها مورد استفاده قرار می‌گیرد. دو روش اصلی برای دسترسی به این ابزار وجود دارد:

- ♦ روش اول: نگه داشتن همزمان سه کلید Ctrl+Alt+Del.
- ♦ روش دوم: نگه داشتن سه کلید Ctrl+Shift+ESC

در شکل زیر، این پنجره نمایش داده شده است.

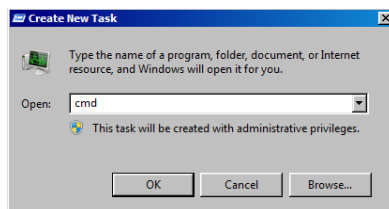


شکل ۳-۵

### ۳-۳-۲ دسترسی به Command Prompt (Cmd)

خط فرمان، ابزار اصلی مدیریت Server Core می‌باشد. جهت دسترسی به این ابزار (در صورتی که پس از ورود آنرا بسته باشید) مراحل زیر را دنبال کنید:

۱. Task Manager را به یکی از دو روش ذکر شده اجرا کنید.
۲. از منوی File، گزینه New Task را انتخاب کنید.
۳. در پنجره "Create New Task"، عبارت Cmd را تایپ و برروی OK کلیک کنید.



شکل ۳-۶

### ۳-۳-۳ تغییر رمز عبور

پس از اینکه برای اولین بار وارد محیط Server Core می‌شوید، شاید این سؤال برایتان پیش آید که "چگونه می‌توانم رمز عبور را تغییر دهم؟" پاسخ این سؤال، استفاده از دستور `net user` می‌باشد. به مثال زیر توجه کنید:

```
C:\Users\Administrator>net user administrator *
Type a password for the user:
Retype the password to confirm:
The command completed successfully.
```

در اینجا علامت \* موجب وارد کردن رمز عبور توسط شما می‌شود.

بسیاری از دستوراتی که در Server Core استفاده می‌شوند، با دستورات خط فرمان در ویندوزهای قبلی یکسان هستند. به عنوان مثال، دستور net از زمان ویندوز NT وجود داشته است. از این دستور جهت انجام وظایف زیر استفاده می‌شود:

- ♦ آغاز و پایان سرویس‌ها
- ♦ اضافه کردن کاربر
- ♦ مدیریت گروه‌ها
- ♦ ایجاد پوشه‌های اشتراکی

تعدادی از این خدمات بعداً در همین فصل مورد بررسی قرار خواهند گرفت.

### ۳-۳-۴ دسترسی به فایل‌های اشتراکی

از آنجایی که ویندوز سرور یک سیستم عامل شبکه است، باید به کمک آن بتوانید به فایل‌های اشتراک گذاشته شده دسترسی پیدا کنید. اگر به محیط گرافیکی و Windows Explorer وابسته شده باشید ممکن است هرگز نتوانید از طریق خط فرمان به این فایل‌ها دست پیدا کنید. در اینجا نحوه انجام این کار را شرح می‌دهیم.

۱. ابتدا جهت نمایش هر آنچه که در شبکه به اشتراک گذاشته شده است (در اینجا بر روی کامپیوتری به نام bf1 در شبکه)، دستور netview را به صورت زیر وارد کنید:

```
C:\Users\Administrator>net view \\bf1
```

```
Shared resources at \\bf1
```

```
Share name Type Used as Comment
```

```
-----
isos          Disk
netlogon      Disk
Public        Disk
Sysvol        Disk
temp          Disk
```

```
The command completed successfully.
```

۲. جهت دسترسی به یک پارتیشن از دیسک، دستور net use را به همراه نام آن پارتیشن وارد نموده تا به آن هدایت شوید:

```
C:\Users\Administrator>net use Z: \\bf1\temp
```

```
The command completed successfully
```

۳. با استفاده از دستورات MS-DOS می‌توانید عملیات مورد نظر را بر روی آن انجام دهید. به عنوان مثال جهت حذف درایو (پارتیشن) دستور زیر را وارد کنید:

```
C:\Users\Administrator>net use Z: /del
Z: was deleted successfully
```

### ۳-۳-۵ پیدا کردن دستورات خط فرمان به ترتیب حروف الفبا (A-Z)

دستورات خط فرمان بسیار ساده و کاربردی هستند. جهت دسترسی به این دستورات روش‌های زیادی وجود دارد، از جمله این روش‌ها، Help موجود در نسخه‌های Full از ویندوز سرور 2008R2 و همچنین از طریق سایت مایکروسافت و لینک زیر:

<http://technet.microsoft.com/en-us/library/cc778084.aspx>

### ۳-۳-۶ پیدا کردن قالب دستورات به کمک علامت ؟

زمانی که قصد دارید از نحوه نوشتن یک دستور به همراه پارامترهای آن آگاه شوید، می‌توانید آن دستور را به همراه علامت سؤال (?) تایپ کنید. پس از آن، کامپیوتر عملیات شما را حدس زده و راهنمایی‌های لازم را ارائه می‌دهد. البته از نمادهای -، / و یا دستور HELP نیز می‌توانید استفاده کنید.

در صورتی که قصد دارید اطلاعات مربوط به یک دستور را در فایلی ذخیره کنید، می‌توانید از نماد > استفاده کنید. به عنوان مثال جهت ذخیره کردن پارامترهای مورد استفاده در دستور ipconfig، دستور زیر را وارد نمایید:

```
C:\Users\Administrator>ipconfig ? > C:\ipconfigCommand.txt
```

این دستور، کلیه پارامترهای موجود در دستور ipconfig را در فایلی به نام ipconfigCommand.txt و در درایو C ذخیره می‌کند. جهت اضافه کردن پارامترهای مربوط به دستورات دیگر به انتهای این فایل می‌توانید بجای > از نماد >> استفاده کنید.

### ۳-۳-۷ خواندن فایل‌های متنی به کمک Notepad

پس از ایجاد یک فایل شاید بخواهید محتویات آنرا مشاهده کنید. خواندن فایل‌ها به کمک برنامه Notepad امکان‌پذیر می‌باشد. با در نظر گرفتن مثال قبل، از دستور زیر جهت خواندن فایل ipconfigCommand.txt استفاده کنید:

```
C:\Users\Administrator>C:\ipconfigCommand.txt
```

به کمک برنامه Notepad قادر خواهید بود دستورات خود را ایجاد و یا ویرایش نموده و تنها با

چند کلیک ساده، آنها را در خط فرمان کپی و اجرا نمایید. جهت انجام این کار، از گزینه‌های Copy و Paste در کلیک‌راست استفاده کنید.

### ۳-۳-۸ مهندسی معکوس<sup>۱</sup>

در اینجا منظور از مهندسی معکوس این است که تمام عملیات قابل انجام در خط فرمان Server Core به کمک ابزارهای گرافیکی در نصب استاندارد (Full Installation) نیز قابل انجام هستند؛ و بر عکس، تمام دستوراتی که در Server Core پشتیبانی می‌شوند، در نصب استاندارد نیز قابل استفاده می‌باشند. زمانی که قرار است در یک محیط نا آشنا مثل Server Core قرار بگیرید، بهترین کار این است که ابتدا تنظیمات پیکربندی را با استفاده از ابزارهای گرافیکی (در نسخه‌های گرافیکی ویندوز) انجام دهید تا از پیکربندی‌های مورد نیاز آگاه شوید. سپس این تنظیمات را در قالب فایل‌های Batch (bat). ذخیره نموده و در خط فرمان Server Core اجرا کنید.

### ۳-۳-۹ Restart و خاموش کردن Server Core

در Server Core دستوراتی جهت خاموش کردن سیستم و یا Restart آن در نظر گرفته شده است. با نوشتن دستور Shutdown در خط فرمان می‌توانید لیستی از پارامترهای استفاده شده با این دستور را مشاهده کنید. به عنوان مثال، با استفاده از دستور زیر می‌توانید سرور را Restart کنید:

```
C:\Users\Administrator>shutdown /r /m \\bfsc1 /t 30
```

سه پارامتر به کار رفته در این دستور عبارت‌اند از:

- ♦ /r: این پارامتر جهت Restart نمودن سرور استفاده می‌شود.
- ♦ /m: از این پارامتر جهت خاموش کردن ماشین‌هایی که به صورت Remote توسط این سرور کنترل می‌شوند (مانند bfsc1)، استفاده می‌گردد (در صورتیکه قصد دارید کامپیوتر فعلی را Restart کنید نیازی به استفاده از این پارامتر نمی‌باشد).
- ♦ /t: این پارامتر مدت زمان تأخیر (به ثانیه) جهت اجرای دستور را تعیین می‌کند.

از دستور زیر نیز می‌توانید جهت خاموش کردن سرور استفاده کنید:

```
C:\Users\Administrator>shutdown /s /t 30
```

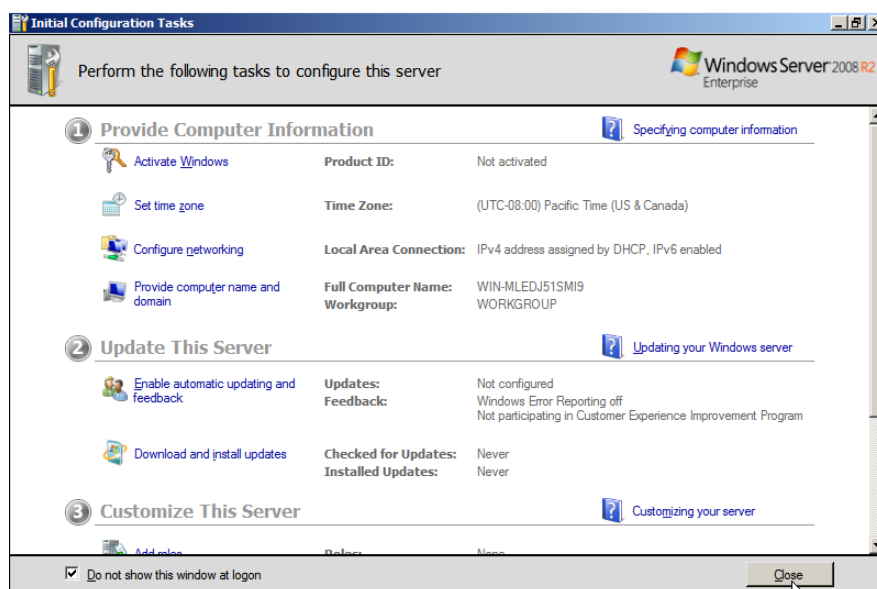
### ۳-۴ پیکربندی مقدماتی Server Core

زمانی که یکی از ویرایش‌های ویندوز را به صورت Full Installation نصب می‌کنید، پس از اتمام

---

1. Reverse Engineering

نصب و ورود به ویندوز، پنجره Initial Configuration Tasks به شما نشان داده می‌شود. به کمک این ابزار، می‌توانید مراحل ۱، ۲ و ۳ که در ادامه آمده است را به راحتی انجام دهید. متأسفانه این پنجره در Server Core وجود ندارد. بنابراین، جهت انجام این اقدامات کمی با دردسر مواجه خواهید بود. در این قسمت، قصد داریم این پیکربندی‌ها را به کمک خط فرمان انجام دهیم.



شکل ۷-۳

### ۳-۴-۱ مرحله ۱: Provide Computer Information

در پنجره Initial Configuration Tasks، مرحله ۱ شامل چهار اقدام پیکربندی ضروری می‌باشد. کلیه این اقدامات از طریق خط فرمان قابل اجرا هستند:

۱. اضافه کردن Product Key و Active کردن ویندوز
۲. تنظیم منطقه زمانی
۳. پیکربندی شبکه
۴. افزودن نام و دامنه به کامپیوتر

### اضافه کردن Product Key و Active کردن ویندوز

اگر توجه کرده باشید، ویندوز سرور 2008R2 بدون نیاز به Product Key بر روی سرور نصب می‌شود، اما لازم است بدانید که بدون این کد، استفاده از کلیه امکانات ویندوز فقط برای ۶۰ روز

امکان پذیر است. در حالت Full Installation اگر در مدت زمان ذکر شده کد را وارد نکنید، در حالتی به نام RFM قرار می‌گیرید که در آن، صفحه Desktop به رنگ سیاه درآمده و هشدارهای متوالی به شما داده می‌شود.

جهت فعال‌سازی و نصب Product Key، از اسکریپتی به نام slmgr.vbs استفاده می‌شود. نحوه استفاده از این اسکریپت، به صورت زیر می‌باشد:

```
C:\Users\Administrator>cscript c:\windows\system32\slmgr.vbs /ipk
q7y83-w4fvq-6mc6c-6qqtd-tpm88
```

```
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
Installed product key q7y83-w4fvq-6mc6c-6qqtd-tpm88 successfully.
```

فعال‌سازی از طریق اینترنت نیز توسط دستور زیر انجام می‌شود:

```
C:\Users\Administrator>cscript c:\windows\system32\slmgr.vbs -ato
```

### تنظیم منطقه زمانی

تعدادی از ابزارهای موجود در Control Panel ویندوز، در Server Core نیز وجود دارد. ابزار تنظیم تاریخ و زمان، یکی از آنها است. جهت دسترسی به این ابزار از دستور زیر استفاده کنید:

```
control timedate.cpl
```

برای اطمینان از اعمال شدن تنظیماتی که انجام داده‌اید، از دستور w32tm /tz استفاده کنید:

```
C:\Windows\system32>w32tm /tz
Time zone: Current:TIME_ZONE_ID_STANDARD Bias: -210min (UTC=LocalTime+Bias)
[Standard Name:"Iran Standard Time" Bias:0min Date:(M:9 D:3 DoW:1)]
[Daylight Name:"Iran Daylight Time" Bias:-60min Date:(M:3 D:3 DoW:6)]
```

### پیکربندی تنظیمات شبکه

مهمترین آیتمی که در این قسمت باید تغییر کند، آدرس IP سرور جهت قرارگرفتن در شبکه است. برای این کار ابتدا به نام کانکشنی که از طریق آن به شبکه متصل هستید نیاز دارید. دستور ipconfig /all نام تمامی کانکشن‌های شبکه را در اختیار شما قرار می‌دهد:

```
C:\Users\Administrator>ipconfig /all
```

```
Windows IP Configuration
```

```
Host Name . . . . . : WIN-AG6PVO 7DM2A
Primary Dns Suffix . . . . . :
```

---

1. Reduced Functionality Mode

```
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain
```

Ethernet adapter **Local Area Connection**:

```
Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-C9-F2-4B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b5a1:157f:7220:4f4c%3(Preferred)
IPv4 Address. . . . . : 192.168.1.136(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, May 19, 2013 1:42:26 PM
Lease Expires . . . . . : Tuesday, May 19, 2013 2:12:25 PM
Default Gateway . . . . . :
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 50334761
DHCPv6 Client DUID. . . . . : 00-01-00-01-11-A3-96-87-00-0C-29-C9-F2-4B
DNS Servers . . . . . : 192.168.1.254
NetBIOS over TcpiP. . . . . : Enabled
```

بطور پیش‌فرض، نام کانکشن ما Local Area Connection می‌باشد. از این نام در دستور netsh interface استفاده می‌کنیم:

```
C:\Users\Administrator>netsh interface ipv4 set address name="Local
Area Connection" source=static address=192.168.1.11
mask=255.255.255.0 gateway=192.168.1.254
```

جهت تغییر نام Connection (کانکشن)، از دستور زیر استفاده کنید (در اینجا، نام "Internal" برای Connection مذکور در نظر گرفته شده است):

```
netsh interface set interface name="local area connection" newname=
"Internal"
```

جهت تغییر آدرس سرور DNS، از دستور زیر استفاده کنید:

```
netsh interface ipv4 add dnsserver name="Internal" address=
192.168.1.10 index=1
```

جهت آگاهی از سایر پارامترهای دستور netsh interface، عبارت زیر را وارد کنید:

```
c:\Users\Administrator>netsh interface set interface /?
```

### افزودن نام و دامنه به کامپیوتر

هنگام نصب ویندوز، بطور پیش‌فرض نامی به کامپیوتر اختصاص داده می‌شود. جهت آگاهی از این نام، از دستور hostname استفاده کنید:



```
c:\Users\Administrator>hostname
WIN-AG6PVO7DM2A
```

همانطور که مشاهده می‌کنید، به خاطر سپاری این نام چندان ساده نیست، بنابراین با توجه به سیاست‌های نامگذاری سازمان می‌توان آنرا تغییر داد. به عنوان مثال قصد داریم نام این کامپیوتر را به Bfsc1 تغییر دهیم:

```
netdom renamecomputer WIN-AG6PVO7DM2A /NewName:Bfsc1 /reboot:5
```

چون فرایند تغییر نام نیازمند Restart سرور می‌باشد، از پارامتر /reboot استفاده شده است.

اکنون قصد داریم سرور را به دامنه Bigfirm.com متصل کنیم. جهت انجام این کار از دستور زیر استفاده کنید:

```
netdom join bfsc1 /domain:Bigfirm.com /user:Administrator
/password:P@ssw0rd /reboot:5
```

### ۳-۴-۲ مرحله ۲: Update This Server

در این مرحله فرایندهایی جهت Update کردن سرور به آخرین اصلاحیه‌ها و موارد امنیتی انجام می‌گیرد و شامل دو زیرمرحله است:

۱. فعال کردن Update خودکار
۲. دانلود و نصب Updateها

#### فعال کردن Update خودکار

جهت فعال سازی Update خودکار، از اسکریپت scregedit.wsf به همراه پارامتر /au استفاده می‌شود. این پارامتر یکی از مقادیر ۰ یا ۴ را پذیرا می‌باشد که مقدار ۴، Update را فعال و مقدار ۰ آنرا غیرفعال می‌نماید.

جهت فعال سازی این سرویس، دستور زیر را وارد کنید:

```
rem navigate to the System32 folder
cd c:\windows\system32\
```

```
rem enable automatic updates
cscript scregedit /au 4
```

```
net stop wuauserv
net start wuauserv
```

برای مشاهده تنظیمات اعمال شده از پارامتر /v استفاده کنید:

```
c:\Windows\System32>cscript scregedit.wsf /au /v
Microsoft (R) Windows Script Host Version 5.8

Copyright (C) Microsoft Corporation. All rights reserved.
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update AUOptions
View registry setting.
4
```

پس از مشاهده پیغام بالا، به Registry رفته (با نوشتن عبارت Regedit در خط فرمان) و کلیدی به نام AUOptions را جستجو کنید. پس از یافتن این کلید مشاهده خواهید نمود که با عدد ۴ مقداردهی شده است. این کلید از مسیر زیر قابل دسترسی می‌باشد:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ WindowsUpdate\
Auto Update
```

### دانلود و نصب Update ها

زمانی که از نسخه‌های گرافیکی ویندوز استفاده می‌کنید، می‌توانید با مراجعه به System Properties و از قسمت Windows Update، به سایت مایکروسافت متصل شده و آپدیت‌ها را دریافت کنید. در نسخه Server Core امکان استفاده از Internet Explorer وجود ندارد بنابراین باید دستوری قابل اجرا در خط فرمان وجود داشته باشد، بطوری که اجرای این عمل را امکان‌پذیر نماید. این دستور، wuauc1t /detectnow می‌باشد. قبل از اجرای این دستور لازم است Update خودکار را فعال کنید.

### ۳-۴-۳ مرحله ۳: Customize This Server

در این مرحله، اضافه کردن Role ها و Feature و همچنین تنظیمات مربوط به مدیریت از راه دور<sup>۲</sup> سرور انجام می‌شود و شامل چهار زیرمرحله است:

۱. اضافه کردن Role
۲. اضافه کردن Feature
۳. فعال‌سازی Remote Desktop
۴. پیکربندی فایروال

1. Remote Administration

### اضافه کردن Role و Feature

در فصل قبل گفتیم که به کمک کنسول Server Manager می‌توان Role ها و Feature ها را تنها با چند کلیک نصب نمود. در این فصل به دلیل استفاده از دستورات خط فرمان کار کمی سخت‌تر می‌شود. در ویندوز سرور 2008 با استفاده از دستور oc1ist امکان مشاهده Role ها، و با دستور ocsetup امکان نصب آنها وجود دارد. در ویندوز سرور 2008R2، برای مشاهده Role ها از دستور dism که برگرفته از عبارت "Deployment Image Servicing and Management Tool" است استفاده می‌گردد. در

این قسمت، به نصب Role‌های (Domain Controller (Active Directory Domain Services)، سرویس DNS، سرویس DHCP، سرویس Print و همچنین تعدادی Feature مانند Backup و PowerShell می‌پردازیم. اولین مرحله پیدا کردن لیست سرویس‌ها و اسامی آنها می‌باشد. بدین منظور دستور زیر را وارد کنید:

```
dism /online /get-features /format:table
```

نتیجه حاصل از اجرای دستور بالا به صورت زیر می‌باشد:

```
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385
```

```
Image Version: 6.1.7600.16385
```

```
Features listing for package : Microsoft-Windows-ServerCore-Package~
31bf3856ad364e35~amd64~~6.1.7600.16385
```

Feature Name	State
NetworkLoadBalancingHeadlessServer	Disabled
SUACore	Disabled
SUACore-WOW64	Disabled
WindowsServerBackup	Enabled
WindowsServerBackupCommandlet	Disabled
MultipathIo	Disabled
DNS-Server-Core-Role	Enabled
FRS-Infrastructure	Disabled
BitLocker	Disabled
BitLocker-RemoteAdminTool	Disabled
DirectoryServices-DomainController-ServerFoundation	Enabled
DirectoryServices-ADAM-ServerCore	Disabled
ActiveDirectory-PowerShell	Disabled
IIS-WebServerRole	Disabled
IIS-WebServer	Disabled
IIS-CommonHttpFeatures	Disabled
IIS-StaticContent	Disabled
IIS-DefaultDocument	Disabled
IIS-DirectoryBrowsing	Disabled
IIS-HttpErrors	Disabled
IIS-HttpRedirect	Disabled
IIS-WebDAV	Disabled
IIS-ApplicationDevelopment	Disabled
IIS-NetFxExtensibility	Disabled
IIS-ASPNET	Disabled
IIS-ASP	Disabled
IIS-CGI	Disabled
IIS-ISAPIExtensions	Disabled
IIS-ISAPIFilter	Disabled
IIS-ServerSideIncludes	Disabled
IIS-HealthAndDiagnostics	Disabled
IIS-HttpLogging	Disabled
IIS-LoggingLibraries	Disabled
IIS-RequestMonitor	Disabled

---



---

IIS-HttpTracing	Disabled
IIS-CustomLogging	Disabled
IIS-ODBCLogging	Disabled
IIS-Security	Disabled
IIS-BasicAuthentication	Disabled
IIS-WindowsAuthentication	Disabled
IIS-DigestAuthentication	Disabled
IIS-ClientCertificateMappingAuthentication	Disabled
IIS-IISCertificateMappingAuthentication	Disabled
IIS-URLAuthorization	Disabled
IIS-RequestFiltering	Disabled
IIS-IPSecurity	Disabled
IIS-Performance	Disabled
IIS-HttpCompressionStatic	Disabled
IIS-HttpCompressionDynamic	Disabled
IIS-WebServerManagementTools	Disabled
IIS-ManagementScriptingTools	Disabled
IIS-ManagementService	Disabled
IIS-IIS6ManagementCompatibility	Disabled
IIS-Metabase	Disabled
IIS-WMICompatibility	Disabled
IIS-LegacyScripts	Disabled
IIS-FTPServer	Disabled
IIS-FTPSvc	Disabled
IIS-FTPExtensibility	Disabled
WAS-WindowsActivationService	Disabled
WAS-ProcessModel	Disabled
WAS-NetFxEnvironment	Disabled
WAS-ConfigurationAPI	Disabled
IIS-HostableWebCore	Disabled
ClientForNFS-Base	Disabled
ServerForNFS-Base	Disabled
DFSR-Infrastructure-ServerEdition	Disabled
DHCPServerCore	Disabled
SNMP-SC	Disabled
DFSN-Server	Disabled
TelnetClient	Disabled
WINS-SC	Disabled
Printing-ServerCore-Role	Disabled
Printing-LPDPrintService	Disabled
Printing-ServerCore-Role-WOW64	Disabled
ServerCore-EA-IME	Enabled
ServerCore-EA-IME-WOW64	Disabled
QWAVE	Disabled
NetFx2-ServerCore	Enabled
NetFx2-ServerCore-WOW64	Disabled
NetFx3-ServerCore	Enabled
WCF-HTTP-Activation	Disabled
WCF-NonHTTP-Activation	Disabled
NetFx3-ServerCore-WOW64	Disabled
MicrosoftWindowsPowerShell	Disabled
MicrosoftWindowsPowerShell-WOW64	Disabled
ServerManager-PSH-Cmdlets	Disabled
BestPractices-PSH-Cmdlets	Disabled
PeerDist	Disabled
Microsoft-Hyper-V	Disabled
VmHostAgent	Disabled
CertificateServices	Disabled
SMBHashGeneration	Disabled
ServerMigration	Disabled
ServerCore-WOW64	Enabled

```
FSRM-Infrastructure-Core | Disabled
CoreFileServer | Disabled
LightweightServer | Disabled
Microsoft-Windows-Web-Services-for-Management-IIS-Extension | Disabled
```

The operation completed successfully.

صورت کلی فعال‌سازی سرویس‌ها به صورت زیر می‌باشد:

```
dism /online /enable-feature /featurename:<Service Name>
```

اکنون می‌توانید سرویس‌های مورد نظر را فعال کنید:

```
rem add DHCP role
dism /online /enable-feature /featurename:DHCPServerCore

rem add printer role
dism /online /enable-feature /featurename:Printing-ServerCore-Role

rem this printer role is for 32 bit drivers
dism /online /enable-feature /featurename:Printing-ServerCore-Role-WOW64

rem a prerequisite for NetFx3-ServerCore
dism /online /enable-feature /featurename:NetFx2-ServerCore

rem add ad domain services and DNS server roles
dism /online /enable-feature /featurename:NetFx3-ServerCore
dism /online /enable-feature /featurename:DNS-Server-Core-Role
dism /online /enable-feature /featurename:DirectoryServices
DomainController-ServerFoundation

rem add Windows Server Backup feature
dism /online /enable-feature /featurename:WindowsServerBackup

rem add powershell feature for the fun of it
dism /online /enable-feature /featurename:MicrosoftWindowsPowerShell
dism /online /enable-feature /featurename:ActiveDirectory-PowerShell
dism /online /enable-feature /featurename:WindowsServerBackupCommandlet
```

- ♦ جهت غیرفعال کردن سرویس‌ها، به جای `enable-feature` از `disable-feature` استفاده کنید.
- ♦ نام سرویس‌ها حساس به حروف کوچک و بزرگ می‌باشند، بنابراین طبق آنچه که در لیست مشاهده می‌کنید از آنها استفاده کنید.
- ♦ در ویندوز سرور 2008 جهت دسترسی به این سرویس‌ها از دستور `oclist` و جهت فعال‌سازی آنها از دستور `ocsetup` استفاده کنید.

## فعال‌سازی Remote Desktop

جهت فعال‌سازی Remote Desktop، از اسکریپت SCRegedit.wsf به همراه پارامترهای زیر استفاده کنید:

- ♦ **/ar**: این پارامتر مشخص‌کننده “مدیریت از راه دور دسکتاپ”<sup>۱</sup> می‌باشد و با مقادیر 0 (فعال) و 1 (غیرفعال) مقداردهی می‌شود. مثال:

```
c:\Windows\System32>cscript scregedit.wsf /ar 0
```

- ♦ **/v**: این پارامتر امکان مشاهده تنظیمات را فراهم می‌نماید. مثال:

*rem view remote desktop settings*

```
c:\Windows\System32>cscript scregedit.wsf /ar /v
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.
System\CurrentControlSet\Control\Terminal Server fDenyTSConnections
View registry setting.
0
```

- ♦ **/cs**: زمانی که قرار است برنامه Remote Desktop از روی سیستم عامل‌هایی مانند ویندوز XP به سرور متصل شود، از این پارامتر استفاده نموده و آنرا با 0 مقداردهی کنید. مثال:

```
c:\windows\system32>cscript scregedit.wsf /cs 0
```

## پیکربندی فایروال

فایروال، به شما اجازه می‌دهد تا بتوانید از طریق پروتکل‌های ارتباط از راه دور مانند RAP<sup>۲</sup> و RDP<sup>۳</sup> با سرور ارتباط برقرار نموده و آنرا مدیریت کنید. جهت پیکربندی فایروال تعدادی دستور باید اجرا شوند. اولین دستور مربوط به پروتکل‌های RAP است که اجازه برقراری ارتباط با “کنسول مدیریت مایکروسافت”<sup>۴</sup> یا MMC را فراهم نموده و گروهی از Role‌ها را جهت مدیریت از راه دور سرور فعال می‌کند (کنسول MMC با نوشتن دستور mmc.exe در خط فرمان قابل دسترسی می‌باشد):

```
netsh advfirewall firewall set rule group="Remote Administration"
new enable=yes
```

دستور بعدی جهت فعال‌سازی Remote Desktop است و اجازه دسترسی به سرور را از طریق برنامه Remote Desktop که بر روی کامپیوترهای شخصی قرار دارد فراهم می‌نماید:

---

1. Remote Desktop Administration  
2. Remote Administration Protocols  
3. Remote Desktop Protocols  
4. Microsoft Management Console

```
netsh advfirewall firewall set rule group="Remote Desktop" new
enable=yes
```

همچنین در صورتی که قصد دارید فایروال را از طریق یک کنسول MMC مدیریت کنید، می‌توانید از دستور زیر استفاده کنید:

```
netsh advfirewall set currentprofile settings remotemanagement enable
```

### ۳-۵ پیکربندی Role ها و Feature ها در Server Core

در این قسمت قصد داریم Server Core را جهت استفاده در یک ادره یا سازمان پیکربندی کنیم. بنابراین، راه‌اندازی سرویس‌هایی مانند Domain Controller، DHCP، DNS، File Service، و همچنین نحوه پشتیبان‌گیری از اطلاعات را شرح خواهیم داد.

### ۳-۵-۱ ایجاد Domain Controller و مدیریت DNS

در نسخه‌های گرافیکی ویندوز سرور، جهت راه‌اندازی Domain Controller می‌توانید از طریق کنسول Server Manager و یا نوشتن عبارت DCpromo.exe در Cmd، ویزارد مربوط به نصب را راه‌اندازی نموده و آنرا نصب کنید. در Server Core امکان استفاده از این ویزارد وجود ندارد بنابراین باید با استفاده از دستورات خط فرمان، عملیات نصب را انجام دهید. در اینجا جهت راه‌اندازی DC، از یک فایل پاسخ به صورت زیر استفاده کنید:

```
[DCInstall]
ReplicaDomainDNSName=bigfirm.com
ReplicaOrNewDomain=ReadOnlyReplica
SiteName=Default-First-Site-Name
InstallDNS=yes
ConfirmGC=yes
CreateDNSDelegation=No
UserDomain=bigfirm.com
UserName=bigfirm\Administrator
CriticalReplicationOnly=No
Password=P@ssw0rd
RebootOnCompletion=Yes
ReplicationSourceDC=bf1.bigfirm.com
SafeModeAdminPassword=P@ssw0rd
```

به کمک دستور ReplicaOrNewDomain=ReadOnlyReplica در فایل بالا مشخص نموده‌اید که سرور یک کنترل‌کننده دامنه فقط خواندنی<sup>۱</sup> (RODC) باشد. جهت استفاده از این فایل دستور زیر را وارد کنید:

```
dcpromo /unattend:c:\temp\RODCAnswerfile.txt
```

---

1. Read-Only Domain Controller

توجه داشته باشید که این دستور، فایلی به نام RODCanswerfile.txt را از مسیر C:\temp فراخوانی می‌کند.

DCpromo تنظیمات مربوط به DNS را نیز مدیریت کرده و سرور را به یک سرویس‌دهنده نام جهت درخواست‌های فقط خواندنی تبدیل می‌کند. پس از راه‌اندازی DC لازم است تنظیمات زیر را جهت پیکربندی مجدد DNS انجام دهید:

```
rem remove all IPV4 entries
netsh interface ipv4 delete dnsserver name=Internal address=all

rem add the assigned IP address as the DNS server
netsh interface ipv4 add dnsserver name=Internal address=
192.168.1.11 index=1

rem remove the IPV6 entry
netsh interface ipv6 delete dnsserver name=Internal address=::1
```

### ۳-۵-۲ پیکربندی سرویس DHCP

سرویس DHCP باید بطور خودکار راه‌اندازی شود تا در هنگام اختصاص آدرس IP به کاربران مشکلی بوجود نیاید. جهت پیکربندی این سرویس ابتدا با استفاده از دستور `sc query` وضعیت اجرا یا متوقف بودن آنرا بررسی کنید:

```
rem verify the service is running or not
sc query dhcpserver

SERVICE_NAME : dhcpserver
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1   STOPPED
        WIN32_EXIT_CODE     : 1077 (0x435)
        SERVICE_EXIT_CODE  : 0   (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

همانطور که در مثال بالا مشاهده می‌کنید، dhcpserver متوقف می‌باشد. با استفاده از دستور زیر می‌توانید راه‌اندازی این سرویس را بر روی خودکار تنظیم کنید:

```
rem configure the service to auto-start
sc config dhcpserver start= auto
[SC] ChangeServiceConfig SUCCESS
```

جهت راه‌اندازی سرویس، دستور زیر را وارد کنید:

```
rem start the service
sc start dhcpserver
```



```
SERVICE_NAME      : dhcpserver
TYPE               : 20 WIN32_SHARE_PROCESS
STATE              : 2 START_PENDING
                  (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
WIN32_EXIT_CODE     : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT         : 0x0
WAIT_HINT          : 0x7d0
PID                : 2564
FLAGS              :
```

پس از اجرای دستور بالا، بار دیگر وضعیت این سرویس را بررسی کنید:

```
rem query the service again
sc query dhcpserver
```

```
SERVICE_NAME      : dhcpserver
TYPE               : 20 WIN32_SHARE_PROCESS
STATE              : 4 RUNNING
                  (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE     : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT         : 0x0
WAIT_HINT          : 0x0
```

اکنون قصد داریم برای شعبه‌ای از اداره، یک ناحیه یا Scope تعریف کنیم. در واقع این Scope تعیین‌کننده مشخصات شبکه در شعبه می‌باشد. جهت تعریف Scope باید اطلاعاتی مانند Default Gateway، DNS Servers و DNS Domain Name را در تنظیمات آن وارد کنید. نحوه انجام این تنظیمات را در ادامه شرح خواهیم داد.

قبل از ایجاد تغییر در تنظیمات DHCP، باید از Active Directory مجوز داشته باشید یعنی سروری که قصد دارید Scope را در آن تعریف کنید، باید برای اکتیودایرکتوری شناخته شده باشد. جهت شناسایی سرور باید آنرا به اکتیودایرکتوری اضافه کنید. بدین منظور از دستور `add server` استفاده کنید:

```
netsh
netsh>dhcp
netsh dhcp>add server bfsc1.bigfirm.com 192.168.1.11

Adding server bfsc1.bigfirm.com, 192.168.1.11

Command completed successfully.
```

جهت بررسی اضافه شدن سرور به اکتیودایرکتوری، از دستور `show server` استفاده کنید:

```
netsh dhcp>show server

1 Servers were found in the directory service:

Server [bfsc1.bigfirm.com] Address [192.168.1.11] Ds location: c
```

```
n=bfsc1.bigfirm.com
Command completed successfully.
```

پس از اضافه کردن سرور می‌توانید Scope را تعریف کنید. برای شروع کار، حالت خط فرمان را به `netsh dhcp server` تغییر داده تا بتوانید از دستور `add scope` استفاده کنید. پارامترهایی که در این دستور نیاز دارید، آدرس Scope، آدرس قاب زیرشبکه و مشخصات Scope می‌باشد. به مثال زیر توجه کنید:

```
netsh dhcp>server
netsh dhcp server>add scope 192.168.1.0 255.255.255.0 "Branch Office
1" "Sample DHCP scope"
```

```
Command completed successfully.
```

```
netsh dhcp server>show scope
```

```
=====
Scope Address - Subnet Mask - State - Scope Name - Comment
=====
192.168.1.0 - 255.255.255.0 -Active -Branch Office 1 -Sample DHCP scope

Total No. of Scopes = 1
Command completed successfully.
```

Scope‌ای که ایجاد کردید باید محدوده‌ای از آدرس‌های IP را به خود اختصاص دهد. علاوه بر این باید دارای Default Gateway، DNS Server و DNS Domain Name باشد که هرکدام با یک شناسه سه کاراکتری مشخص می‌شوند. به عنوان مثال، تنظیمات زیر را برای یک Scope در نظر بگیرید:

- ♦ محدوده آدرس‌دهی: از 192.168.1.50 تا 192.168.1.100
- ♦ Default Gateway: با شناسه 003 و آدرس 192.168.1.254
- ♦ DNS Server: با شناسه 006 و آدرس 192.168.1.11
- ♦ DNS Domain Name: با شناسه 015 و نام bigfirm.com

جهت اختصاص موارد ذکرشده، ابتدا Scope‌ای که ایجاد نمودید را فراخوانی کنید. برای این کار، دستور زیر را وارد کنید:

```
netsh dhcp server>scope 192.168.1.0

Changed the current scope context to 192.168.1.0 scope.
```

جهت تعیین محدوده آدرس‌دهی، دستور زیر را وارد کنید:

```
netsh dhcp server scope>add iprange 192.168.1.50 192.168.1.100
```

Command completed successfully.

با دستور زیر، تنظیمات مربوط به Default Gateway را انجام دهید:

```
netsh dhcp server scope>set optionvalue 003 IPADDRESS 192.168.1.254
```

Command completed successfully.

دستور زیر، نام و شناسه DNS Server را تنظیم می‌کند:

```
netsh dhcp server scope>set optionvalue 006 IPADDRESS 192.168.1.11
```

Command completed successfully.

آخرین دستور نیز مربوط به اختصاص نام دامنه DNS می‌باشد:

```
netsh dhcp server scope>set optionvalue 015 STRING bigfirm.com
```

Command completed successfully.

پس از اتمام کار، جهت مشاهده تنظیمات از دستور زیر استفاده کنید:

```
netsh dhcp server scope>show optionvalue
```

Options for Scope 192.168.1.0:

```
DHCP Standard Options :
General Option Values:
OptionId : 51
Option Value:
    Number of Option Elements = 1
    Option Element Type = DWORD
    Option Element Value = 691200
OptionId : 3
Option Value:
    Number of Option Elements = 1
    Option Element Type = IPADDRESS
    Option Element Value = 192.168.1.254
OptionId : 6
Option Value:
    Number of Option Elements = 1
    Option Element Type = IPADDRESS
    Option Element Value = 192.168.1.11
OptionId : 15
Option Value:
    Number of Option Elements = 1
    Option Element Type = STRING
    Option Element Value = bigfirm.com
```

Command completed successfully.

### ۳-۵-۳ راه‌اندازی File Server

File Server، قابلیت‌هایی را جهت اشتراک فایل‌ها در اختیار شما قرار می‌دهد. در نسخه‌های گرافیکی

ویندوز سرور 2008R2، از طریق کنسول MMC و یا Server Manager می‌توانید File Server و سرویس‌های مرتبط با آن را نصب کنید. در اینجا قصد داریم راه‌اندازی این سرویس‌ها را به کمک دستورات خط فرمان شرح دهیم.

### ایجاد Primary Partition

Primary Partition، به پارتیشنی گفته می‌شود که امکان قرارگیری داده‌ها و یا سیستم‌عامل بر روی آن وجود داشته باشد. فرض کنید دیسکی با فضای ۷۰GB در اختیار دارید که ۲۰GB از این مقدار را به سیستم عامل اختصاص داده و مابقی آن (۵۰GB) آزاد است. قصد دارید یک پارتیشن ۱۰GB بر روی دیسک ایجاد کنید. جهت انجام این کار مراحل زیر را دنبال کنید:

۱. ابتدا از دستور diskpart استفاده کنید:

```
C:\Windows\system32>diskpart
Microsoft DiskPart version 6.1.7000
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: BFSC1
```

۲. جهت نمایش دیسک‌های متصل به سرور، دستور list disk را وارد کنید:

```
DISKPART>list disk

Disk ###  Status              Size       Free       Dyn Gpt
-----  -
Disk 0    Online              75 GB      55 GB
```

۳. پس از مشاهده دیسک(ها)، از دستور list volume جهت نمایش کلیه درایوهای موجود بر روی آن استفاده کنید:

```
DISKPART>list volume

Volume ###  Ltr Label          Fs      Type          Size      Status       Info
-----  -
Volume 0    D   GB1SXFRE_EN  UDF     CD-ROM        2850 MB  Healthy
Volume 1                      NTFS    Partition     200 MB  Healthy     System
Volume 2    C                      NTFS    Partition     19 GB   Healthy     Boot
```

۴. جهت انتخاب دیسک، از دستور select disk به همراه شماره آن استفاده کنید:

```
DISKPART>select disk 0

Disk 0 is now the selected disk.
```

۵. قبل از ایجاد پارتیشن بر روی دیسک انتخاب شده، لازم است اطلاعاتی راجع به نحوه انجام کار

بدست آورید. دستور `help create partition primary` در این زمینه به شما کمک خواهد کرد. فقط دقت داشته باشید که حجم دیسک برحسب MB (مگابایت) نشان داده می‌شود. یعنی ۵۵ گیگابایت معادل ۵۵۰۰۰ مگابایت می‌باشد:

```
DISKPART> help create partition primary
```

```
.....
```

```
Example:
```

```
CREATE PARTITION PRIMARY SIZE=1000  
rem size is in MB so 55 gb is 55000
```

۶. پارتیشن مورد نظر دارای حجم ۱۰GB یا ۱۰۰۰۰MB می‌باشد. برای ایجاد آن دستور زیر را وارد کنید:

```
DISKPART> create partition primary size=10000
```

```
DiskPart succeeded in creating the specified partition.
```

۷. جهت مشاهده کلیه پارتیشن‌های موجود بر روی دیسک، از دستور `list partition` استفاده کنید:

```
DISKPART>list partition
```

Partition ###	Type	Size	Offset
Partition 1	Primary	200 MB	1024 KB
Partition 2	Primary	19 GB	201 MB
*Partition 3	Primary	10 GB	20 GB

۸. پس از ایجاد پارتیشن، باید یک حرف به آن اختصاص داده، فرمت و نام آنرا مشخص کنید. برای انجام این کار، ابتدا آنرا انتخاب کنید:

```
DISKPART>select partition 3
```

```
Partition 3 is now the selected partition.
```

۹. با دستور `assign letter` حرف E را به آن اختصاص دهید:

```
DISKPART>assign letter=e
```

```
DiskPart successfully assigned the drive letter or mount point.
```

۱۰. جهت تعیین نام و فرمت پارتیشن، بار دیگر دستور `list volume` را اجرا کنید:

```
DISKPART> list volume
```

Volume ###	Ltr	Label	Fs	Type	Size	Status	Info
Volume 0	D	GB1SXFRE_EN	UDF	CD-ROM	2850 MB	Healthy	

---



---

Volume 1		NTFS	Partition	200 MB	Healthy	System
Volume 2	C	NTFS	Partition	19 GB	Healthy	Boot
*Volume 3	E	RAW	Partition	10 GB	Healthy	

---

۱۱. Volume مورد نظر، که همان Volume 3 می‌باشد را انتخاب نمایید:

```
DISKPART>select volume 3
Volume 3 is the selected volume.
```

۱۲. سرانجام، با دستور زیر می‌توانید فرمت، نام و نحوه فرمت کردن این Volume را مشخص کنید:

```
DISKPART>format fs=ntfs label="Data volume" quick
100 percent completed
DiskPart successfully formatted the volume.
```

### ایجاد پوشه و ویرایش مجوزها<sup>۱</sup>

در این قسمت قصد داریم دو پوشه در پارتیشن E ایجاد کنیم:

- ♦ Users: جهت قرارگیری داده‌های کاربران
- ♦ Sales: جهت دسترسی (به عنوان مثال) بخش فروش به آن

جهت ایجاد پوشه‌ها از دستور md که یکی از دستورات MS-DOS می‌باشد استفاده می‌شود:

```
E:\>md sales
E:\>md users
```

قصد داریم امنیت را برای دسترسی به این پوشه‌ها برقرارکنیم. در اکتیودایرکتوری، یک گروه از کاربران به نام “بخش فروش” ایجاد شده است که کنترل کاملی بر محتویات پوشه Sales دارند. پوشه Users محل نگهداری پوشه‌های کاربران اکتیودایرکتوری می‌باشد و بطور پیش‌فرض کلیه کاربران و گروه‌های کاربری به داده‌های آن دسترسی دارند. فرض کنید در اکتیو دایرکتوری گروهی از کاربران (Users group) هستند که نباید به این دو پوشه دسترسی داشته باشند. بنابراین باید مجوز خواندن یا نوشتن از این گروه گرفته شود.

بار دیگر به دستورات A-Z که در قسمت‌های قبل راجع به آن صحبت نمودیم باز گردید. دستوری به نام `cacls.exe` وجود دارد که به کمک آن می‌توان مجوز کاربران برای دسترسی به پوشه‌ها را تغییر داد. توسط این دستور، مجوزهای پوشه Sales را تغییر می‌دهیم. برای پوشه Users نیز می‌توانید به روش مشابهی عمل کنید.

۱. ابتدا مجوزهای اعمال شده بر روی این پوشه را با دستور زیر مشاهده کنید:

```
rem Display the permissions to the sales folder
caccls sales
E:\sales BUILTIN\Administrators:(OI)(CI)F
        NT AUTHORITY\SYSTEM:(OI)(CI)F
        BUILTIN\Administrators:F
        CREATOR OWNER:(OI)(CI)(IO)F
        BUILTIN\Users:(OI)(CI)R
        BUILTIN\Users:(CI)(special access:)
                FILE_APPEND_DATA

        BUILTIN\Users:(CI)(special access:)
                FILE_WRITE_DATA
```

۲. برای حذف مجوز داده شده به گروه کاربران (users group)، به روش زیر عمل کنید:

```
rem Remove the users group
caccls sales /E /R Users
processed dir: E:\sales
```

۳. جهت افزودن مجوز کنترل کامل بر روی پوشه Sales توسط بخش فروش، از دستور زیر استفاده کنید:

```
rem Add the Sales group with Full Control permissions
caccls sales /E /G bigfirm\sales:F
processed dir: E:\sales
```

۴. در نهایت برای مشاهده مجوزهای اعمال شده بر روی پوشه، بار دیگر از دستور زیر استفاده کنید:

```
rem View the Sales folder permissions
caccls sales
E:\sales BUILTIN\Administrators:(OI)(CI)F
        NT AUTHORITY\SYSTEM:(OI)(CI)F
        BUILTIN\Administrators:F
        CREATOR OWNER:(OI)(CI)(IO)F
        BIGFIRM\Sales:(OI)(CI)F
```

### اشتراک گذاری پوشه‌ها

اشتراک گذاری پوشه‌ها با استفاده از دستور net share امکان‌پذیر است. پوشه‌ای که در اینجا به اشتراک می‌گذاریم، Sales نام دارد:

```
rem create shares
E:\>net share SALES=e:\sales /grant:bigfirm\sales,FULL /Unlimited
Sales was shared successfully.
```

در دستور بالا، به منظور دادن مجوز به کاربران بخش فروش از پارامتر grant استفاده شده است و پارامتر Unlimited / نیز مشخص می‌کند که تعداد دسترسی‌ها به پوشه می‌تواند نامحدود

باشد.

دستور زیر جهت اشتراک گذاری پوشه Users بین کاربران دامنه bigfirm استفاده می‌شود:

```
E:\>net shareUsers=e:\users /grant:bigfirm\domain users,FULL /Unlimited
Users was shared successfully.
```

### استفاده از Backup Server

جهت پشتیبان‌گیری از داده‌های دیسک، مراحل زیر را دنبال کنید:

۱. ابتدا، رُل WindowsServerBackup را با دستور زیر فعال کنید:

```
dism /online /enable-feature /featurename:WindowsServerBackup
```

۲. با استفاده از دستور wbadmin می‌توانید عمل پشتیبان‌گیری را انجام دهید. جهت اطلاع از نحوه

به کار بردن این دستور، آنرا به صورت wbadmin /? وارد کنید:

```
c:\Windows\System32>wbadmin /?
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

---- Commands Supported ----

ENABLE BACKUP          -- Creates or modifies a daily backup schedule.
DISABLE BACKUP         -- Disables the scheduled backups.
START BACKUP           -- Runs a one-time backup.
STOP JOB               -- Stops the currently running backup or recovery
                        operation.
GET VERSIONS           -- List details of backups recoverable from a
                        specified location.
GET ITEMS              -- Lists items contained in a backup.
START RECOVERY         -- Runs a recovery.
GET STATUS             -- Reports the status of the currently running
                        operation.
GET DISKS              -- Lists the disks that are currently online.
START SYSTEMSTATE
RECOVERY              -- Runs a system state recovery.
START SYSTEMSTATE
BACKUP                -- Runs a system state backup.
DELETE SYSTEMSTATE
BACKUP                -- Deletes one or more system state backups.
```

همانطور که در بالا مشاهده می‌کنید، امکان پشتیبان‌گیری و بازگردانی داده‌های سیستم و کاربران وجود دارد که این امر جهت حفاظت از داده‌های Active Directory بسیار مفید خواهد بود.

۳. برای شروع کار، ابتدا یک USB را به سرور متصل کنید (F:\) تا عمل پشتیبان‌گیری و بازگردانی به کمک آن انجام شود. قصد داریم از درایو داده‌ها (E:\)، درایو سیستم عامل (C:\) و همچنین داده‌هایی که وضعیت سیستم را مشخص می‌کنند پشتیبان‌گیری کنیم.

۴. پس از قرار دادن USB دستور زیر را وارد کنید (پارامتر allcritical - جهت پشتیبان‌گیری از



درایو C:\ و پارامتر systemstate - جهت پشتیبان‌گیری از وضعیت سیستم می‌باشد. درایو F:\ نیز مشخص‌کننده مقصد است:

```
F:\WindowsImageBackup\BFSC1>wbadmin start backup -backupTarget:f: -
include:e: -allCritical -systemstate -quiet
```

```
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Retrieving volume information...
This will back up volume <Unlabeled Volume> (200.00 MB) (\\?\Volume{54a54ad2-43f9-11de-9b46-806e6f6e6963}\), Local Disk(C:), Data volume(E:) to f:.
The backup operation to F: is starting.
Creating a shadow copy of the volumes specified for backup...
...
Creating a backup of volume <Unlabeled Volume> (200.00 MB)
(\\?\Volume{54a54ad2-43f9-11de-9b46-806e6f6e6963}\), copied (38%).
The backup of volume <Unlabeled Volume> (200.00 MB) (\\?\Volume{54a54ad2-43f9-11de-9b46-806e6f6e6963}\) successfully completed.
Creating a backup of volume Local Disk(C:), copied (0%).
Creating a backup of volume Local Disk(C:), copied (1%).
...
Creating a backup of volume Local Disk(C:), copied (98%).
The backup of volume Local Disk(C:) successfully completed.
Creating a backup of volume Data volume(E:), copied (19%).
Creating a backup of volume Data volume(E:), copied (100%).
The backup operation successfully completed.
Summary of the backup operation:
-----
The backup of volume <Unlabeled Volume> (200.00 MB) (\\?\Volume{54a54ad2-43f9-11de-9b46-806e6f6e6963}\) successfully completed.
The backup of volume Local Disk(C:) successfully completed.
The backup of volume Data volume(E:) successfully completed.
```

♦ ممکن است در حین اجرای این دستور با سؤالاتی مواجه شوید. اول اینکه چگونه می‌توان نام USB را به F تغییر داد. پاسخ این سؤال در قسمت‌های قبل توضیح داده شده‌است. (مراحل کار: assign letter F « select partition « list partition « select disk « list volume « list disk « diskpart

♦ سوال بعدی ممکن است درمورد مسیر F:\WindowsImageBackup\BFSC1 باشد. این مسیر بیانگر پوشه‌ای به نام BFSC1 است که در پوشه WindowsImageBackup از درایو F قرار دارد. برای سادگی کار می‌توانید این فایل را در ریشه درایو F یعنی F:\ ذخیره کنید.

۵. پس از اجرای دستور بالا، جهت مشاهده محتویات پوشه BFSC1 از درایو F:\، دستور زیر را وارد کنید:

```
F:\WindowsImageBackup\BFSC1>dir
Volume in drive F is backup
Volume Serial Number is 0AF2-4B31
```

```

Directory of F:\WindowsImageBackup\BFSC1
05/24/2013 01:21 PM <DIR>          .
05/24/2013 01:21 PM <DIR>          ..
05/24/2013 01:21 PM <DIR>          Backup 2013-05-24 171141
05/24/2013 01:21 PM <DIR>          Catalog
05/24/2013 12:47 PM          16 MediaId
05/24/2013 01:21 PM <DIR>          SPPMetadataCache
          1 File(s)          16 bytes
          5 Dir(s) 74,138,492,928 bytes free

```

اکنون برای بازگردانی داده‌هایی که در قسمت قبل از آنها پشتیبان‌گیری نمودید مراحل زیر را دنبال کنید:

ابتدا از دستور `wbadmin get items` جهت مشاهده فایل‌های ایجاد شده در پشتیبان استفاده کنید. در این دستور، از پارامتر `-version` استفاده می‌شود که مقادیر انتصاب داده شده به آن، همان تاریخ و ساعت پشتیبان‌گیری می‌باشد (طبق آنچه که در نتیجه دستور قبل مشاهده می‌کنید):

```

wbadmin get items -version:05/24/2013-17:11
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Volume ID = {54a54ad2-43f9-11de-9b46-806e6f6e6963}
Volume '<Unlabeled Volume>', mounted at <not mounted> at the time the backup
was
created
Volume size = 200.00 MB
Can recover = Full volume

Volume ID = {54a54ad3-43f9-11de-9b46-806e6f6e6963}
Volume '<Unlabeled Volume>', mounted at C:
Volume size = 19.33 GB
Can recover = Full volume

Volume ID = {a8a658b4-454b-11de-9ff8-000c29c9f24b}
Volume 'Data volume', mounted at E:
Volume size = 9.76 GB
Can recover = Full volume

Application = FRS
Component = f95607bc-2b49-4b31-a0147ea3ee7f3545 (SYSVOL \f95607bc-2b49-4b31-
a0147ea3ee7f3545)

Application = AD
Component = ntds (C:\Windows_NTDS\ntds)

Application = Registry
Component = Registry (\Registry)

```

اگر به نتایج بالا دقت کنید، متوجه می‌شوید که پارامتر `-allcritical` موجب ذخیره شدن محتویات درایو C: (به حجم ۱۹.۳۳GB) و همچنین اطلاعات بازگردانی سیستم (به حجم ۲۰۰MB) شده است. پارامتر `-include` هم محتویات درایو E: را ذخیره نموده است. علاوه بر اینها، از سه برنامه دیگر به نام‌های FRS، Active Directory و Registry نیز پشتیبان گرفته شده است که اینها بیانگر

وضعیت سیستم یا همان System State هستند.

در ادامه، به شما نشان خواهیم داد که چگونه مشخصات (پروفایل) مدیر Bigfirm یا همان administrator.bigfirm را به یک مکان موقت بازگردانی کنید. بازگردانی داده‌ها با استفاده از دستور `wbadmin start recovery` امکان پذیر است. قبل از اجرای دستور، به موارد زیر توجه نمایید:

- ♦ از پشتیبانی که دارای تاریخ و زمان 05/24/2013-17:11 می‌باشد استفاده کنید.
- ♦ عمل بازگردانی فایل‌ها را انجام دهید.
- ♦ فایلی که قصد دارید آنرا بازگردانید، در مسیر `C:\users\administrator.bigfirm` قرار دارد.
- ♦ محتویات پوشه و زیرپوشه‌های آن و همچنین فایل‌های داخل آنها را بازگردانید.
- ♦ فایل‌ها را به جای مسیر اصلی، به مسیر `C:\temp` بازگردانید.

```
wbadmin start recovery -version:05/24/2013-17:11 -itemType:File -items
:c:\users\administrator.bigfirm -recursive -recoveryTarget:c:\temp
```

```
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.
```

```
Retrieving volume information...
You have chosen to recover the file(s) c:\users\administrator.bigfirm from
the
backup created on 5/24/2013 1:11 PM to c:\temp.
```

```
Do you want to continue?
[Y] Yes [N] No y
```

```
Successfully recovered c:\users\administrator.bigfirm to c:\temp.
The recovery operation completed.
Summary of the recovery operation:
-----
```

```
Recovery of c:\users\administrator.bigfirm to c:\temp successfully completed.
Total bytes recovered: 5.68 MB
Total files recovered: 116
Total files failed: 0
```

```
Log of files successfully recovered:
C:\Windows\Logs\WindowsServerBackup\FileRestore-24-05-2013_14-07-11.log
```

با مراجعه به مسیری که جهت بازگردانی تعیین نموده‌اید، موفق بودن عملیات را مشاهده کنید:

```
c:\temp\administrator.bigfirm>dir
Volume in drive C has no label.
Volume Serial Number is E0B3-709F

Directory of c:\temp\administrator.bigfirm

05/24/2013 02:07 PM <DIR>      .
05/24/2013 02:07 PM <DIR>      ..
05/19/2013 09:24 PM <DIR>      Contacts
```

```

05/19/2013 09:24 PM <DIR> Desktop
05/24/2013 11:50 AM <DIR> Documents
05/19/2013 09:24 PM <DIR> Downloads
05/19/2013 09:24 PM <DIR> Favorites
05/19/2013 09:24 PM <DIR> Links
05/19/2013 09:24 PM <DIR> Music
05/19/2013 09:24 PM <DIR> Pictures
05/19/2013 09:24 PM <DIR> Saved Games
05/19/2013 09:24 PM <DIR> Searches
05/19/2013 09:24 PM <DIR> Videos
                        0 File(s) 0 bytes
                  13 Dir(s) 15,841,628,160 bytes free

```

آخرین دستوری که در این قسمت به آن می‌پردازیم، `wbadmin enable backup` می‌باشد. این دستور شبیه `wbadmin start backup` است ولی هدف متفاوتی دارد: انجام پشتیبان‌گیری به صورت افزایشی<sup>۱</sup> و زمان‌بندی شده. در این روش پس از اجرای اولین عمل پشتیبان‌گیری، هر بار که طبق زمان‌بندی پشتیبان‌گیری انجام شود فایل‌های پشتیبان قبلی (که بر روی دیسک قرار دارد) حذف می‌گردد، سپس فایل‌های پشتیبان جدید جایگزین آن می‌شوند. مثال قبل را با روش پشتیبان‌گیری زمان‌بندی شده، که هر روز ساعت ۹ بعد از ظهر (P.M) عمل پشتیبان‌گیری را انجام می‌دهد اجرا می‌کنیم:

```

wbadmin enable backup -addtarget:F: -schedule:21:00 -include:e: -allCritical
-systemstate -vssFull -quiet

```

```

wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

```

```

Retrieving volume information...
The scheduled backup settings:

```

```

Bare metal recovery : Included
System state backup: Included
Volumes in backup: <Unlabeled Volume> (200.00 MB) (\\?\Volume{54a54ad2-43f9-
11de-
9b46-806e6f6e6963}\), Local Disk(C:), Data volume(E:)
Advanced settings: VSS Backup Option (FULL )
Location to store backup: F:
Times of day to run backup: 21:00
The scheduled backup is enabled.

```



## « فصل ۴ »

**DNS و نامگذاری**

**DNS and Naming**



برقراری ارتباط بین کامپیوترها در شبکه، از طریق آدرس IP که ممکن است IPv4 یا IPv6 باشد امکان پذیر است، بنابراین کاربران جهت دسترسی به سرویس‌هایی مثل File Server در شبکه و یا وبسایت مورد علاقه خود در اینترنت باید این آدرس را به خاطر بسپارند. برای برخی افراد، به خاطر سپاری این آدرس‌ها کار چندان آسانی نیست، بنابراین آنها ترجیح می‌دهند که جهت دسترسی به یک وبسایت مثلاً با آدرس 128.132.23.45، از آدرس [www.example.com](http://www.example.com) استفاده کنند. این دقیقاً همان کاری است که “سیستم نامگذاری دامنه”<sup>۱</sup> (DNS) در شبکه و یا اینترنت انجام می‌دهد. در ویندوز سرور 2008R2 از این سرویس به خوبی استفاده شده است و کاربران شبکه می‌توانند با ارائه درخواست‌های خود به سرور DNS، به سرویس‌های داخل و یا خارج از شبکه دسترسی پیدا کنند. در این فصل قصد داریم شما را با این سرویس و نحوه مدیریت آن آشنا کنیم. بطور کلی مهمترین مباحثی که در این فصل به آنها پرداخته خواهد شد عبارتند از:

- اجزاء و پردازش‌های اساسی در DNS
- پیکربندی DNS جهت پشتیبانی از محیط اکتیو دایرکتوری
- پیکربندی DNS در Server Core

#### ۴-۱ مفاهیم پایه DNS

قبل از اینکه وارد بحث اصلی DNS شویم، لازم است بطور خلاصه مفاهیمی که در طول این فصل مورد استفاده قرار می‌گیرند را تعریف کنیم:

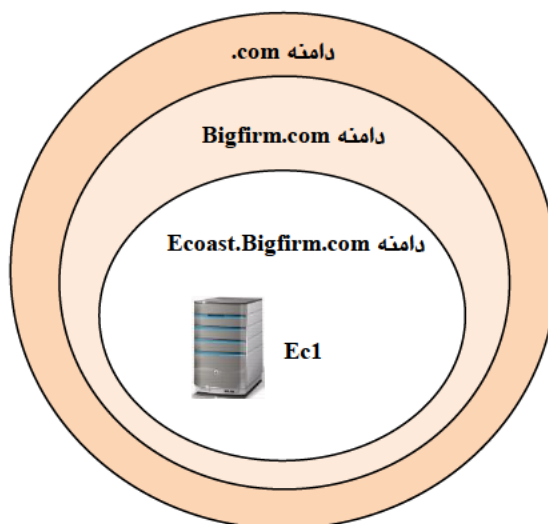
- **Hostname:** این مفهوم به معنای نام میزبان است و بیان کننده نام یک کامپیوتر در شبکه یا دامنه می‌باشد. بر طبق استانداردهای DNS، این نام می‌تواند حداکثر از ۲۵۵ کاراکتر تشکیل شود و معادل نام اولیه کامپیوتر<sup>۲</sup> می‌باشد.
- **Hosts file:** یک فایل متنی است که لیست Hostname‌ها و آدرس‌های IP متناظر با آنها را نگهداری می‌کند. در نصب ویندوز سرور 2008R2 به صورت Full Installation، این فایل از مسیر `c:\windows\system32\drivers\etc` قابل دسترسی می‌باشد.
- **Namespace (فضای نام):** بیان کننده نام یک دامنه است و به عنوان نام ثانویه (نام خانوادگی) میزبان‌های شبکه در نظر گرفته می‌شود. به عنوان مثال، [BigFirm.com](http://BigFirm.com) یک فضای نام برای میزبان‌هایی است که در دامنه [BigFirm.com](http://BigFirm.com) قرار دارند.
- **FQDN:** بیان کننده نام میزبان به همراه نام دامنه آن می‌باشد. به عنوان مثال [Bf1.Bigfirm.com](http://Bf1.Bigfirm.com)

---

1. Domain Name System  
2. Computer Name  
3. Fully Qualified Domain Name



- یک FQDN در دامنه BigFirm.com است و به ماشینی با نام Bf1 در این دامنه اشاره دارد.
- **Name Server** (سرور نام): همان سرور DNS است که FQDN ها را به آدرس های IP تبدیل می کند. این سرور همچنین مسئول کنترل فضای نام دامنه ها بوده و درخواست هایی که از طرف کاربران DNS در یک دامنه برای دسترسی به یک فضای نام داده می شود را به آدرس IP آن تبدیل می کند.
  - **ساختار نامگذاری سلسله مراتبی**<sup>۱</sup>: هر فضای نام از چندین قسمت تشکیل می شود که هر قسمت به ترتیب از سمت چپ، زیر مجموعه قسمت سمت راست خود می باشد. به عنوان مثال ماشینی با نام Ecl.Ecoast.Bigfirm.com را در نظر بگیرید. این نام، یک FQDN برای دامنه Ecoast.Bigfirm.com می باشد. حال، خود این دامنه نیز زیرمجموعه یا زیردامنه ای<sup>۲</sup> از دامنه Bigfirm.com است، به همین ترتیب، این دامنه نیز زیردامنه ای از دامنه سطح بالای com می باشد. همانطور که مشاهده می کنید، جهت دسترسی به یک ماشین (مثل Ec1) که در دامنه ای سطح پایین (مانند Ecoast.Bigfirm.com) قرار دارد، باید طی یک سلسله مراتب که از دامنه های سطح بالا شروع می شود حرکت کنید. به همین دلیل است که به این ساختار نامگذاری، ساختار سلسله مراتبی گفته می شود. به شکل زیر توجه کنید.



شکل ۱-۴

- **Recursion** (بازگشت): یک پردازش سمت سرور است که طی یک پرس و جوی بازگشتی، FQDN را به آدرس IP آن تبدیل می کند. اگر سرویس دهنده نام در یک دامنه، قادر به پیدا کردن یک FQDN

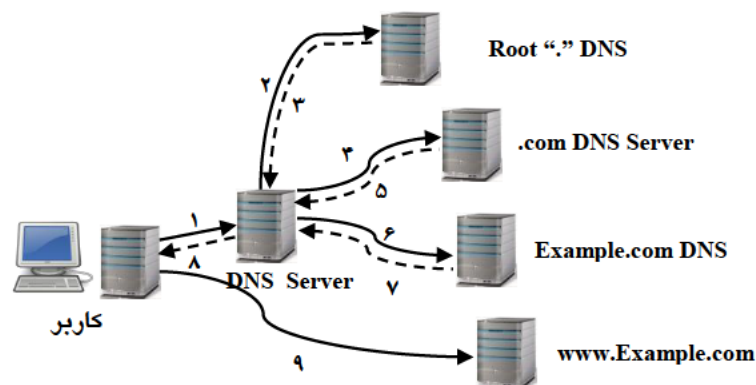
---

1. Hierarchical naming structure

در پایگاه داده خود نباشد، درخواستی را به سایر سرویس‌دهنده‌های نام می‌فرستد. این درخواست طی یک فرایند بازگشتی، آدرس FQDN را بدست آورده و آنرا به کاربری که درخواست را انجام داده است تحویل می‌دهد. فرایند بازگشت شامل سرورهای ریشه (Root) و سرورهای نام دامنه می‌باشد. سرورهای ریشه در بالاترین سطح از ساختار سلسله‌مراتبی نامگذاری قرار دارند و شامل لیستی از نام‌های دامنه سطح بالا مثل .com، .gov، .edu و ... می‌باشند. سرورهای دامنه سطح بالا، مسئول ثبت دامنه‌های سطح پایین‌تر می‌باشند. به عنوان مثال سرورهای نام .com، مسئول ثبت زیردامنه Example.com هستند.

زمانی که یک درخواست FQDN رخ می‌دهد، مراحل زیر انجام می‌گیرد:

۱. یک کاربر DNS، درخواست یک نام مثل www.example.com را به سرور DNS در دامنه خود ارائه می‌دهد.
  ۲. سرور DNS، طی یک فرایند بازگشتی درخواستی را به سرور ریشه جهت دسترسی به سرورهای نام دامنه .com می‌فرستد.
  ۳. سرور ریشه، لیستی از سرورهای نام برای دامنه .com را به سرور DNS باز می‌گرداند.
  ۴. سرور DNS، از سرورهای نام .com، دسترسی به example.com را درخواست می‌کند.
  ۵. سرورهای .com، لیست سرورهای نام دامنه example.com را به سرور DNS باز می‌گردانند.
  ۶. سرور DNS از بین نام‌های فراهم شده، FQDN با نام www.example.com را درخواست می‌کند.
  ۷. سرور example.com، آدرس IP مربوط به سرور www را به سرور DNS باز می‌گرداند.
  ۸. سرور DNS نیز آدرس را به کاربری که درخواست داده بود تحویل می‌دهد.
  ۹. به کمک این آدرس IP کاربر می‌تواند به وب‌سرور www.example.com متصل شود.
- در شکل زیر، کلیه این مراحل نشان داده شده است:



شکل ۲-۲



جدول ۴-۱: تعدادی از دامنه‌های سطح بالا به همراه موارد استفاده

نام دامنه	کاربرد	نام دامنه	کاربرد	نام دامنه	کاربرد
com	تجاری	info	اطلاع رسانی	au	
edu	مؤسسات آموزشی	aero	حمل و نقل هوایی	uk	
gov	دولتی	Biz	مؤسسات بازرگانی	ca	
int	سازمان‌های بین‌المللی	Coop	تعاونی‌ها	us	کشورها
mil	نظامی	Museum	موزه‌ها	jp	
net	ارائه‌دهنده خدمات شبکه	Name	افراد	ir	
org	سازمان‌های غیر انتفاعی	pro	حرفه‌ها و مشاغل	...	

- **Delegation**: این مفهوم به معنای دادن وکالت به سایر سرورهای نام جهت کنترل زیردامنه‌های یک فضای نام می‌باشد. به عنوان مثال سرور نام Bigfirm.com می‌تواند کنترل زیر دامنه‌های Ecoast.Bigfirm.com را به سایر سرورهای نام واگذار کند (می‌توانید به تنظیمات TCP/IP مربوط به کارت شبکه مراجعه نموده و از تنظیمات DNS این موضوع را مشاهده کنید).
- **Forwarding (ارسال)**: سروری که این عمل را انجام می‌دهد، می‌تواند به عنوان جایگزینی برای سرور درگیر در پردازش بازگشتی در نظر گرفته شود بطوری که درخواست را از کاربر پذیرفته و آنرا به سرور نام اصلی تحویل می‌دهد.
- **Iteration (از سرگیری)**: این عمل یک پردازش سمت مشتری برای تبدیل نام FQDN می‌باشد. زمانی که کاربر درخواستی را به یک سرور نام ارائه دهد ولی پاسخی دریافت نکند، درخواست خود را به سرویس‌دهنده دیگری ارسال می‌نماید.
- **NetBIOS naming system**: یک سیستم نامگذاری است که در ابتدا توسط نسخه‌های قدیمی ویندوز از جمله NT4.0 استفاده می‌شد ولی هم اکنون نیز جزئی از سیستم عامل‌های ویندوز است.
- **Service resource records (SRVs)**: یک رکورد در فضای نام DNS است که یک سرویس را به Hostname تبدیل می‌کند.
- **Dynamic DNS (DDNS) update**: پردازشی است که به کاربران اجازه می‌دهد تا Hostname‌های خود را در فضای نام مشخصی ثبت کنند. این کار، نیاز مدیران جهت وارد نمودن دستی

رکوردهای مربوط به Hostname را در پایگاه داده کاهش می‌دهد.

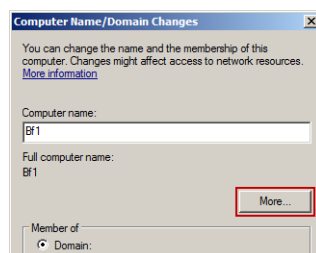
- ♦ **DNS Zone:** منظور از Zone (ناحیه)، پایگاه داده ای است که نام‌ها و آدرسهای IP مرتبط با آنها در یک دامنه نگهداری می‌شود. وجود این پایگاه‌های داده برای عملکرد DNS بسیار ضروری هستند زیرا برای پیدا کردن آدرس IP متناظر با یک نام، سرور DNS محتویات موجود در این پایگاه داده را مورد جستجو قرار می‌دهد.

## ۴-۲ نصب DNS Server

DNS Server یکی از Role‌هایی است که از زمان ویندوز 2000 در نسخه‌های ویندوز سرور قرار داده شده است، در واقع ویندوز 2000 اولین نسخه‌ای است که در اکتیو دایرکتوری آن از DNS پشتیبانی می‌شود. با انتشار نسخه‌های جدیدتر ویندوز سرور، بر قابلیت‌ها و توانایی‌های این سرویس افزوده شد بطوری که از نسخه 2008 به بعد، امکان استفاده از IPv6 نیز فراهم گردید و این به معنای یکپارچگی ویندوز سرور با سیستم‌هایی است که از IPv6 استفاده می‌کنند.

قبل از نصب DNS بر روی یک سرور، لازم است مراحل را جهت آماده‌سازی آن انجام دهید. بدین منظور ابتدا یک آدرس IP (که آدرس DNS Server شما می‌باشد) فراهم نموده و مراحل زیر را دنبال کنید:

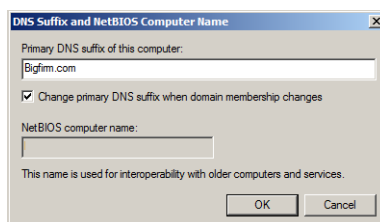
۱. از منوی Start، بر روی Computer کلیک راست نموده و گزینه Properties را انتخاب کنید.
۲. در پنجره باز شده، بر روی Change setting کلیک کنید.
۳. در پنجره "System Properties" بر روی دکمه Change کلیک کنید.
۴. در پنجره "Computer Name/Domain Changes" بر روی دکمه More کلیک کنید.



شکل ۴-۳

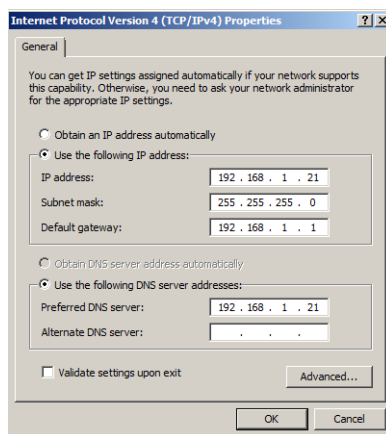
۵. در قسمت Primary DNS suffix، نام دامنه‌ای که از آن استفاده می‌کنید (به عنوان مثال Bigfirm.com) را وارد نموده و بر روی OK کلیک کنید (در مورد ایجاد دامنه در فصل اکتیو

دایرکتوری صحبت خواهیم نمود).



شکل ۴-۴

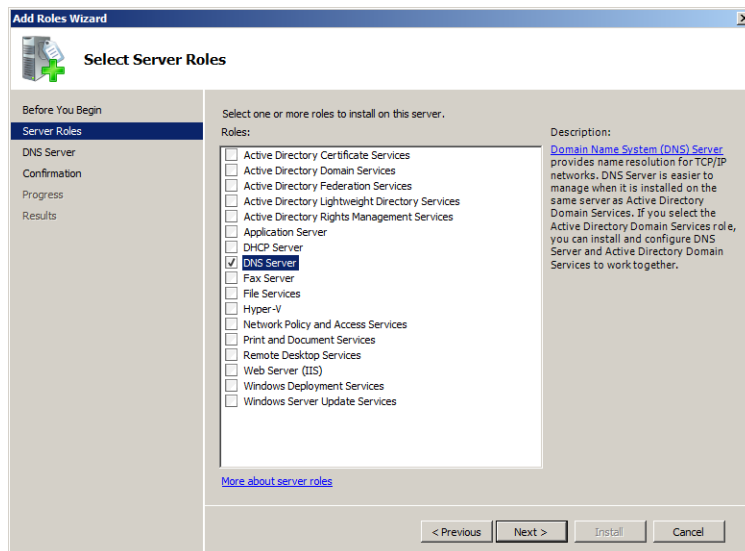
۶. در صورت نیاز، کامپیوتر را Restart نموده تا تنظیمات اعمال شوند.
۷. به تنظیمات کارت شبکه (TCP/IP) رفته و آدرس IP که قبلاً فراهم نموده‌اید را در قسمت‌های IP address و Preferred DNS Server وارد نمایید. با این کار تعیین می‌کنید که سرور DNS بر روی کامپیوتر شما قرار داشته باشد.



شکل ۴-۵

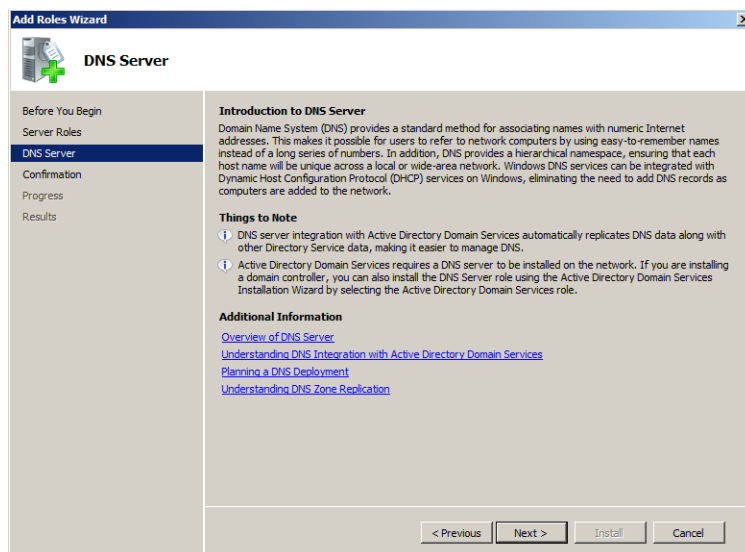
اکنون DNS آماده نصب می‌باشد. جهت نصب کافی است مراحل زیر را دنبال کنید:

۱. کنسول Server Manager را از مسیر Start «Administrative Tools» Server Manager اجرا کنید.
۲. در قسمت Roles Summary (یا با کلیک بر روی Roles در پنل سمت چپ از کنسول Server Manager) گزینه Add Roles را انتخاب کنید.
۳. در صفحه «Select Server Roles» گزینه DNS Server را انتخاب و بر روی Next کلیک کنید.



شکل ۴-۶

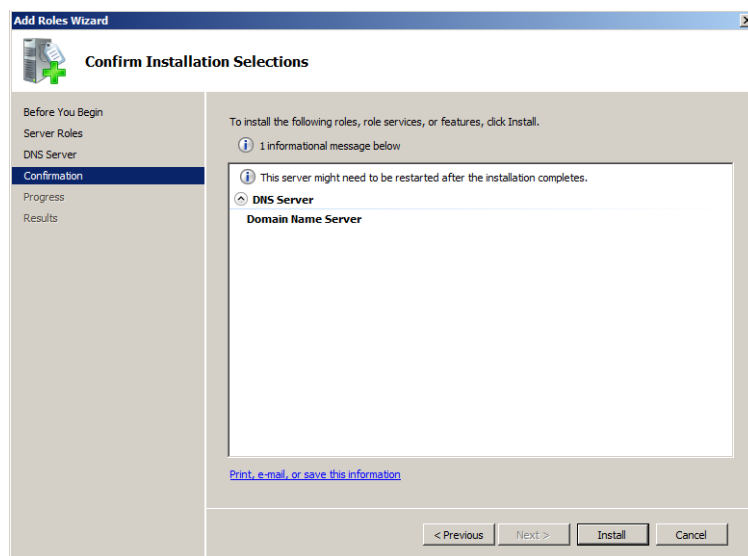
۴. در صفحه “DNS Server” توضیحاتی راجع به سرویس DNS ارائه می‌گردد. پس از مطالعه این توضیحات بر روی Next کلیک کنید.



شکل ۴-۷

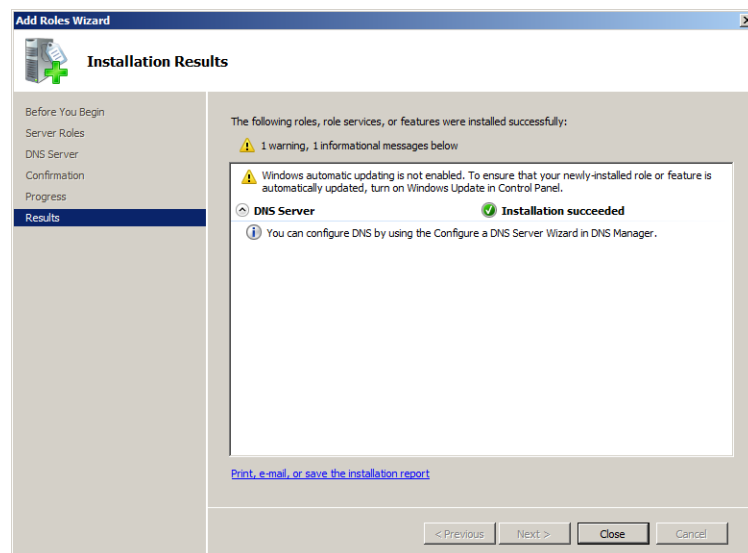
۵. در صفحه “Confirm Installation Selections” بر روی Install کلیک نموده و منتظر بمانید تا عملیات

نصب به اتمام برسد.



شکل ۴-۸

۶. پس از اتمام عملیات، در صفحه "Installation Results" بروی Close کلیک کنید.



شکل ۴-۹

### ۳-۴ ایجاد Zone و مدیریت فضاهای نام

منظور از Zone (ناحیه)، پایگاه داده‌ای است که محل نگهداری فضاهای نام می‌باشد. زمانی که درخواستی از طرف کاربر به یک سرور DNS فرستاده می‌شود، سرور، فضای نام درخواست شده را در پایگاه داده خود (Zone) جستجو نموده و در صورت پیدا شدن، آدرس IP معادل با آن را به کاربر باز می‌گرداند. در واقع این پایگاه داده، تمام اطلاعاتی است که سرور جهت پاسخگویی به درخواست‌های کاربران در یک دامنه به آن نیاز دارد و به عنوان یکی از مهمترین قسمت‌های DNS محسوب می‌شود. نکته ای که در مورد ایجاد Zone ها باید به آن توجه داشته باشید این است که در هنگام تبدیل سرور به Domain Controller (با استفاده از ویزارد DCPromo.exe) فرایند ایجاد Zone ها بصورت خودکار انجام می‌شود، اما در مواردی که نیاز به Zone های دیگری داشته باشید، باید آنها را به صورت دستی ایجاد نمایید.

Zone ها از لحاظ نحوه تبدیلاتی که در آنها انجام می‌شود (نام به IP، یا برعکس)، به دو دسته Forward Lookup Zones و Reverse Lookup Zones تقسیم می‌شوند. هر دسته نیز از لحاظ میزان اطلاعات موجود در آن و چگونگی دسترسی به این اطلاعات، به چهار نوع Primary Zones، Secondary Zones، Stub Zones و AD Integrated Zones تقسیم می‌گردد. هر نوع از این Zone ها دارای استفاده مشخصی هستند که در قسمت‌های بعد آنها را به صورت جداگانه مورد بررسی قرار خواهیم داد.

#### ۱-۳-۴ Forward Lookup Zones

این دسته از Zone ها وظیفه تبدیل نام ماشین‌ها به آدرس IP معادل با آنها را برعهده دارند. به عنوان مثال فرض کنید که کاربری با در اختیار داشتن فضای نام سرور BF4 به صورت Bf4.Bigfirm.com، درخواستی برای دسترسی به آن، به سرور DNS ارائه می‌دهد. از آنجایی که سرور DNS شامل Zone هایی است که نام (فضای نام) ماشین‌ها را به همراه آدرس IP آنها نگهداری می‌کنند، بنابراین با دریافت نام سرور از کاربر و جستجوی محتویات Zone ها، آدرس IP معادل با آن ماشین را پیدا نموده و در اختیار کاربر قرار می‌دهد. بنابراین این کاربر قادر خواهد بود با سرور مورد نظر ارتباط برقرار نماید.

#### ۲-۳-۴ Reverse Lookup Zones

Reverse Lookup Zones ها، دقیقاً عکس Forward Lookup Zones عمل می‌کنند. در Forward Lookup Zones، کاربران با داشتن یک فضای نام، آدرس IP آنرا از سرور DNS درخواست می‌کنند اما در Reverse Lookup Zones شیوه‌ای متفاوت به کار گرفته می‌شود. در اینجا، کاربر آدرس IP را در اختیار داشته و از سرور DNS فضای نام را درخواست می‌کند. شاید این سؤال برایتان پیش آید که چه



نیازی به این عمل می‌باشد؟ مهمترین دلیل استفاده از این روش، مسائل امنیتی است. فرض کنید یک هکر<sup>۱</sup> در حال گوش‌دادن به درخواست کاربران برای فضاهای نام که با “www” شروع می‌شوند (درخواست‌های دسترسی به وب‌سرور) باشد (با استفاده از یک سرویس‌دهنده که خود هکر راه‌اندازی نموده است). زمانی که سرویس‌دهنده این هکر درخواست شما را دریافت می‌کند، وب‌سرویس آن، از آدرس IP خود یک پاسخ جعلی به شما ارسال می‌کند. حال وب‌سایت موجود بر روی این وب‌سرویس قبل از اینکه کاربر متوجه شود انواع ویروس‌ها، تروجان‌ها<sup>۲</sup> و نرم افزارهای مخرب را اجرا نموده و امنیت کاربر و شبکه را به خطر می‌اندازد. اکنون حالتی را در نظر بگیرید که مرورگر وب کاربر به گونه‌ای پیکربندی شده که بتواند جستجوی معکوس<sup>۳</sup> برای آدرس IP بدست آمده را انجام دهد، بنابراین می‌تواند آدرس IP این وب‌سایت را با نام وب‌سروری که درخواست نموده مقایسه کند. اگر همخوانی نداشتند هرگز به آن وب‌سرور متصل نخواهد شد.

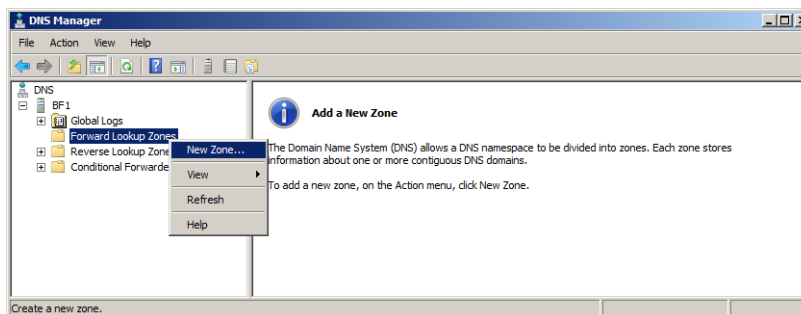
#### ۳-۳-۴ Primary Zones

مهمترین نوع Zone که در سرورهای DNS به کار برده می‌شود، Primary Zone (ناحیه اصلی) می‌باشد. این Zone، پایگاه‌داده‌ای شامل فضاهای نام و آدرس‌های IP آنها است که به عنوان اصلی‌ترین محل نگهداری این اطلاعات در نظر گرفته می‌شود. سایر Zone‌ها با استفاده از اطلاعات Primary Zone می‌توانند به درخواست‌های کاربران پاسخ دهند. در این Zone، امکان نوشتن و یا خواندن رکوردها به صورت کنترل‌شده وجود دارد.

#### ایجاد Forward Lookup Primary Zones

جهت ایجاد Primary Zone از نوع Forward Lookup مراحل زیر را دنبال کنید:

۱. کنسول DNS Manager «Start مسیر از مسیریاب» را اجرا نمایید.
۲. از زیرمجموعه نام سرور، بر روی پوشه Forward Lookup Zones کلیک راست نموده و New Zone را انتخاب کنید.



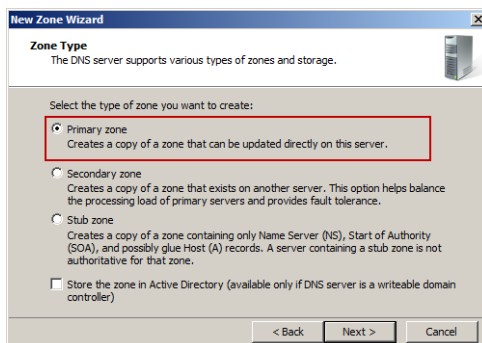
شکل ۴-۱۰

۳. پس از اجرای ویزارد "New Zone Wizard" با مشاهده صفحه "Welcom to New Zone Wizard"، بر روی Next کلیک کنید.



شکل ۴-۱۱

۴. در صفحه "Zone Type" باید نوع Zone را انتخاب کنید. گزینه Primary Zone را انتخاب نموده و بر روی Next کلیک کنید. دقت داشته باشید که گزینه Store the zone in Active Directory در این مرحله انتخاب نشده باشد (این گزینه مربوط به زمانی است که Zone در اکتیو دایرکتوری ذخیره می‌شود و تنها در صورت وجود اکتیو دایرکتوری قابل انتخاب می‌باشد. در این مورد بعداً توضیح خواهیم داد).



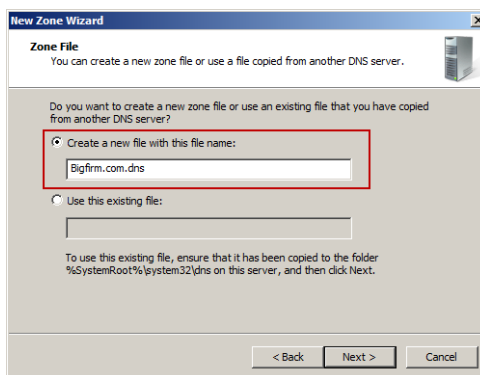
شکل ۴-۱۲

۵. در صفحه "Zone Name" یک نام برای Zone انتخاب نمایید. این نام می‌تواند متناسب با نام دامنه یا قسمتی از نام دامنه در سازمان انتخاب شود. (به عنوان مثال Bigfirm.com یا Primaryzone.bigfirm.com). در اینجا از نام Bigfirm.com برای Primary Zone استفاده شده است.



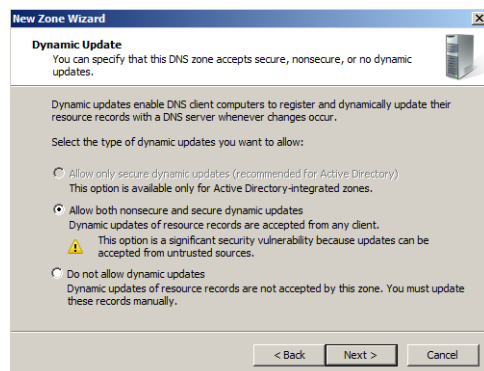
شکل ۴-۱۳

۶. در صفحه "Zone File" می‌توانید تعیین کنید که برای ذخیره سازی Zone، یک فایل جدید ایجاد شود و یا اینکه از فایل‌هایی که قبلاً ایجاد شده اند استفاده گردد. همچنین می‌توانید نام فایل Zone را تعیین کنید. گزینه Create a new file with this file name را انتخاب نموده و بر روی Next کلیک کنید (دقت داشته باشید که پسوند فایل ایجاد شده dns، بوده و در مسیر C:\Windows\System32\dns ذخیره می‌گردد).



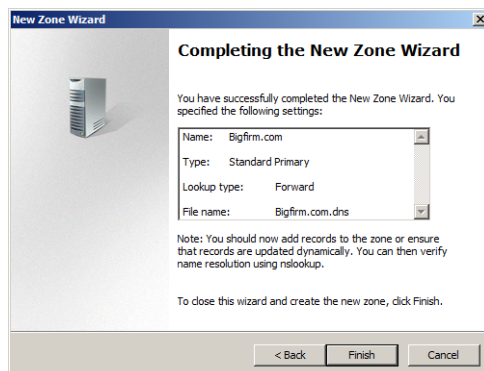
شکل ۴-۱۴

۷. در صفحه "Dynamic Update" باید نحوه ثبت hostname (نام میزبان‌ها) در DNS Zone را تعیین کنید. انجام این کار می‌تواند بصورت خودکار، و یا توسط مدیر سرور و به صورت دستی انجام شود. در اینجا فرض بر این است که رکوردها می‌توانند به صورت خودکار ثبت شوند، بنابراین گزینه allow both nonsecure and secure dynamic update را انتخاب نموده و بر روی Next کلیک کنید (البته می‌توانید با انتخاب گزینه آخر انجام این کار را به صورت دستی انجام دهید که در اینصورت با زحمت بیشتر و البته امنیت بیشتر مواجه خواهید بود).



شکل ۴-۱۵

۸. در صفحه “Completing the New Zone Wizard” پس از مشاهده تنظیمات انجام شده، بر روی Finish کلیک کنید.



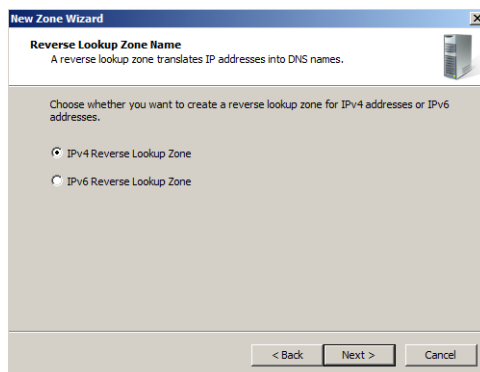
شکل ۴-۱۶

### ایجاد Reverse Lookup Primary Zones

جهت ایجاد Primary Zone از نوع Reverse Lookup مراحل زیر را دنبال کنید:

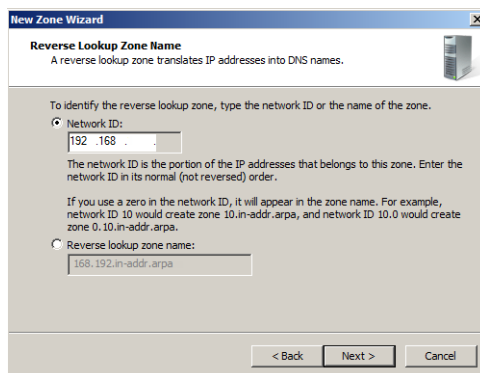
۱. کنسول DNS Manager را از مسیر Start «Administrative Tools» DNS اجرا نمایید.
۲. از زیرمجموعه نام سرور، بر روی پوشه Reverse Lookup Zones کلیک راست نموده و New Zone را انتخاب کنید.
۳. پس از اجرای ویزارد “New Zone Wizard” با مشاهده صفحه “Welcom to New Zone Wizard”، بر روی Next کلیک کنید (شکل ۴-۱۱).

۴. در صفحه "Zone Type" باید نوع Zone را انتخاب کنید. گزینه Primary Zone را انتخاب نموده و بر روی Next کلیک کنید. دقت داشته باشید که گزینه Store the zone in Active Directory در این مرحله انتخاب نشده باشد (شکل ۴-۱۲)
۵. در صفحه "Reverse Lookup Zone Name" نوع آدرس IP (IPv4 یا IPv6) که قرار است در DNS Server و Reverse Lookup Zone استفاده شود را تعیین نموده و بر روی Next کلیک کنید.

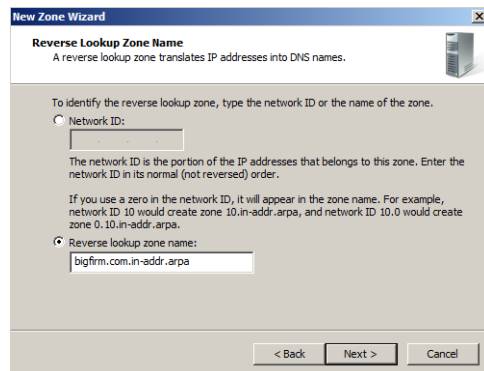


شکل ۴-۱۷

۶. در صفحه بعد جهت شناسایی Zone باید شناسه شبکه یا یک نام برای آن وارد نمایید. شناسه شبکه در واقع آدرس شبکه‌ای است که قرار است ماشین‌های موجود در آن، در این Zone قرار گیرند. در اینجا چون از آدرس‌های کلاس C استفاده کرده‌ایم، مقدار 192.168 را وارد کنید. البته انتخاب این آدرس و کلاس آن بستگی به شبکه شما دارد و ممکن است از کلاس A یا B نیز انتخاب گردد. دقت داشته باشید که با انتخاب گزینه Reverse lookup zone name می‌توانید به جای شناسه شبکه، از یک نام برای Zone استفاده نمایید. هر دو حالت مذکور در شکل‌های ۴-۱۸ و ۴-۱۹ نشان داده شده است.

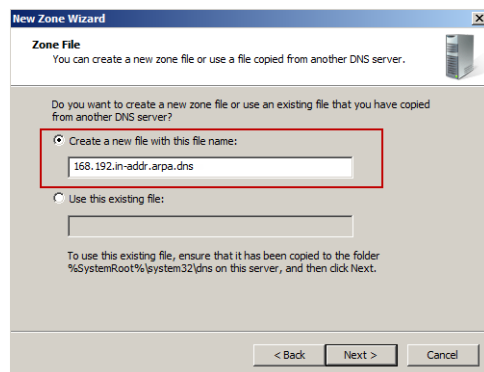


شکل ۴-۱۸



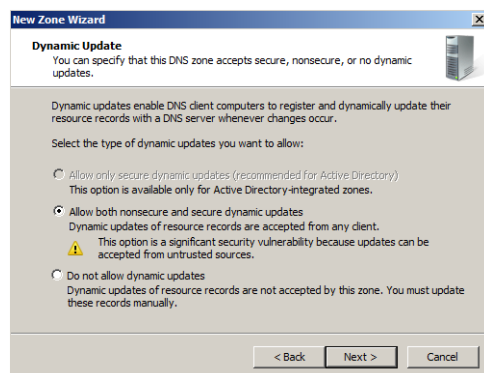
شکل ۱۹-۴

۷. در صفحه "Zone File" گزینه "Create a new file with this file name" را انتخاب نموده و بر روی Next کلیک کنید.



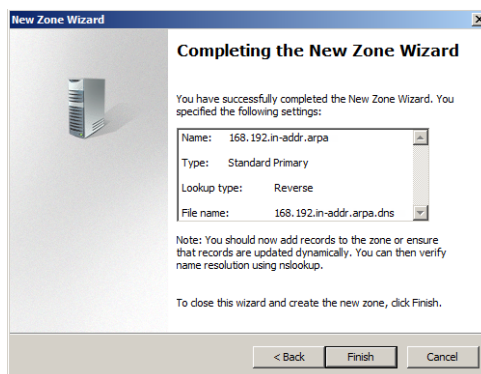
شکل ۲۰-۴

۸. در صفحه "Dynamic Update" گزینه "allow both nonsecure and secure dynamic update" (این انتخاب متناسب شرایط سازمان و کاربران آن می‌باشد) را انتخاب نموده و بر روی Next کلیک کنید.



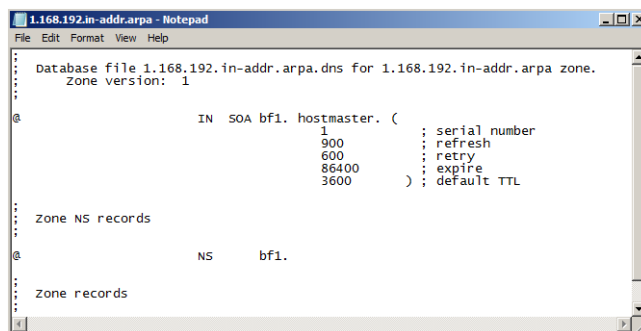
شکل ۲۱-۴

۹. در صفحه “Completing the New Zone Wizard” پس از مشاهده تنظیمات انجام شده، بر روی Finish کلیک کنید.



شکل ۴-۲۲

۱۰. پس از پایان مراحل می‌توانید فایل ایجاد شده را از مسیر C:\windows\system32\dns مشاهده کنید. پس از باز کردن این فایل، چیزی شبیه به شکل ۴-۲۳ مشاهده خواهید نمود.



شکل ۴-۲۳

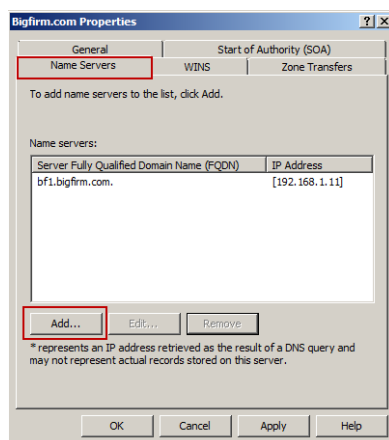
### Secondary Zones ۴-۳-۴

Secondary Zone (ناحیه ثانویه) یک نسخه فقط خواندنی از Primary Zone می‌باشد. بدین معنی که پس از ایجاد Primary Zone می‌توان یک کپی از اطلاعات آنرا که فقط امکان خواندن از آن وجود دارد در اختیار سایر سرورهای DNS قرار داد تا آنها بتوانند به درخواست‌هایی که از طرف کاربران داده می‌شود پاسخ دهند. استفاده از این Zone ها بیشتر در مواردی است که بار زیادی بر روی سرور DNS اصلی شبکه قرار داشته باشد. در این موارد می‌توان سرورهای DNS کمکی اضافه نموده و نسخه‌ای از Primary Zone را (با استفاده از Secondary Zone) در اختیار آنها قرار داد. با این کار، بار شبکه

برروی این سرورها توزیع می‌گردد.

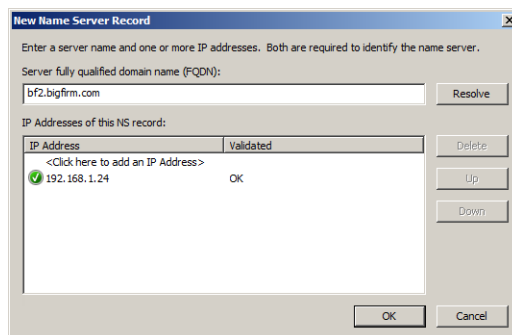
قبل از ایجاد Secondary Zone برروی یک سرور DNS، این سرور باید برای سرور اصلی (که Primary Zone را در اختیار دارد) شناخته شود. به عنوان مثال سرور Bf2.Bigfirm.com را در نظر بگیرید. برای اینکه یک نسخه از Primary Zone را در اختیار این سرور قرار دهید، باید آنرا به سرور اصلی (در اینجا Bf1.bigfirm.com) معرفی کنید. جهت شناساندن سرورهای DNS ثانویه به سرور اصلی، مراحل زیر را دنبال کنید:

۱. برروی Primary Zone که ایجاد نموده‌اید کلیک‌راست نموده و Properties را انتخاب کنید.
۲. با مراجعه به تب Name Server می‌توانید لیست سرورهای شناخته شده برای سرور اصلی را مشاهده کنید.
۳. برای اضافه کردن سرور، بر روی Add کلیک کنید.



شکل ۴-۲۴

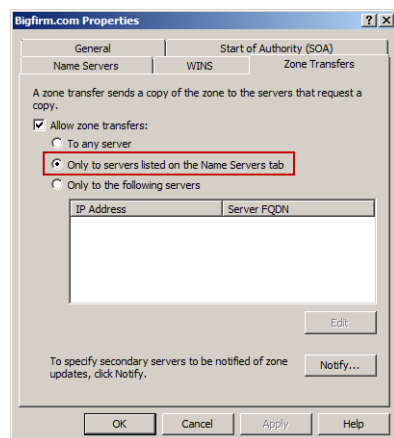
۴. در پنجره "New Name Server Record" نام و آدرس IP سرور DNS ثانویه را وارد نموده و برروی OK کلیک کنید.



شکل ۴-۲۵



۵. پس از تعریف سرورها، به تب Zone transfer رفته و گزینه Only to server listed on the Name Servers tab را انتخاب کنید. با این کار، تعیین می‌کنید که نسخه Primary Zone تنها به سرورهای اضافه شده در تب Name Server و تنها در زمان درخواست آنها فرستاده شود.



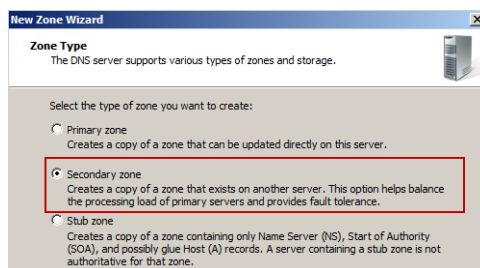
شکل ۴-۲۶

اکنون می‌توانید Secondary Zone را بر روی سرورهای DNS ثانویه که نام و آدرس IP آنها را در تب Name Server تعیین نمودید (مثل Ec1) ایجاد کنید. ایجاد Secondary Zone تقریباً شبیه Primary Zone می‌باشد. در ادامه نحوه انجام این کار را برای Forward Lookup Zones و Reverse Lookup Zones نشان می‌دهیم.

### ایجاد Forward Lookup Secondary Zones

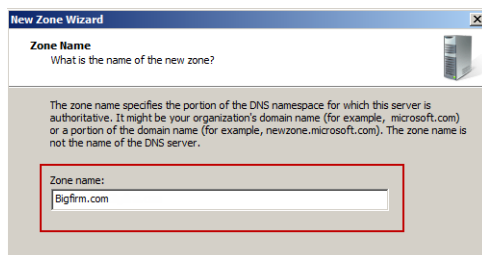
جهت ایجاد Secondary Zone از نوع Forward Lookup، مراحل زیر را دنبال کنید:

۱. در کنسول DNS Manager بر روی پوشه Forward Lookup Zones کلیک راست نموده و New Zone را انتخاب کنید.
۲. با مشاهده صفحه "Welcom to New Zone Wizard"، بر روی Next کلیک کنید.
۳. در صفحه "Zone Type" گزینه Secondary Zone را انتخاب نموده و بر روی Next کلیک کنید.



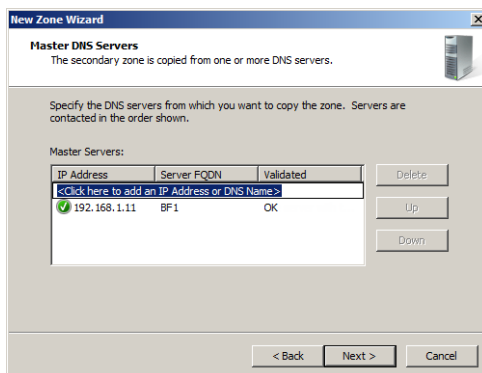
شکل ۴-۲۷

۴. در صفحه “Zone Name” نام Zone را وارد نموده و بر روی Next کلیک کنید. در اینجا چون قصد داریم یک نسخه از Bigfirm.com را بدست آوریم، از نام Bigfirm.com استفاده شده است.



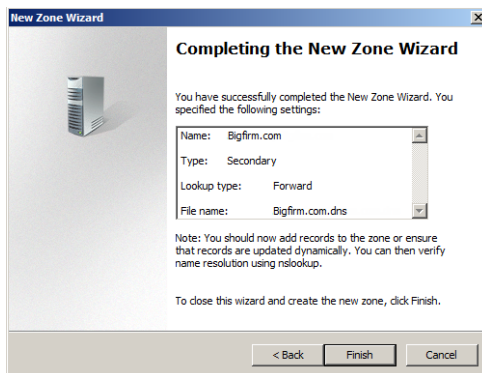
شکل ۴-۲۸

۵. در صفحه “Master DNS Servers” آدرس سرور یا سرورهای اصلی DNS که قرار است نسخه‌ای از Primary Zone آنها در اختیار سرور فعلی (ثانویه) قرار گیرد را وارد نموده و بر روی Next کلیک کنید.



شکل ۴-۲۹

۶. در صفحه “Completing the New Zone Wizard” بر روی Finish کلیک کنید.



شکل ۴-۳۰

### ایجاد Reverse Lookup Secondary Zones

جهت ایجاد Secondary Zone از نوع Reverse Lookup، مراحل زیر را دنبال کنید:

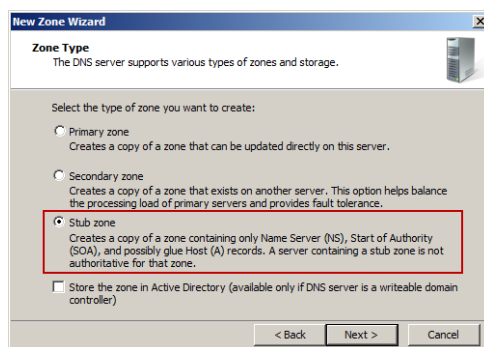
۱. در کنسول DNS Manager بروی پوشه Forward Lookup Zones کلیک راست نموده و New Zone را انتخاب کنید.
۲. با مشاهده صفحه "Welcom to New Zone Wizard"، بروی Next کلیک کنید (شکل ۴-۱۱).
۳. در صفحه "Zone Type" گزینه Secondary Zone را انتخاب نموده و بروی Next کلیک کنید (شکل ۴-۲۷).
۴. در صفحه "Reverse Lookup Zone Name" نوع آدرس IP (IPv4 یا IPv6) که قرار است در DNS Server و Reverse Lookup Zone استفاده شود را تعیین نموده و بروی Next کلیک کنید.
۵. در صفحه بعد جهت شناسایی Zone باید شناسه شبکه یا یک نام برای آن وارد نمایید. شناسه شبکه در واقع آدرس شبکه‌ای است که قرار است ماشین‌های موجود در آن، در این Zone قرار گیرند. انتخاب این آدرس و کلاس آن بستگی به شبکه شما دارد و ممکن است از کلاس A، B یا C انتخاب گردد. دقت داشته باشید که با انتخاب گزینه Reverse lookup zone name می‌توانید به جای شناسه شبکه، از یک نام برای Zone استفاده نمایید (شکل‌های ۴-۱۸ و ۴-۱۹).
۶. در صفحه "Master DNS Servers" آدرس سرور یا سرورهای اصلی DNS که قرار است نسخه‌ای از Primary Zone آنها در اختیار سرور فعلی (ثانویه) قرار گیرد را وارد نموده و بروی Next کلیک کنید (شکل ۴-۲۹).
۷. در صفحه "Completing the New Zone Wizard" بروی Finish کلیک کنید.

### Stub Zones ۵-۳-۴

نوع دیگری از Zone است که در واقع روشی برای یکپارچه شدن با سایر سرورهای DNS فراهم می‌نماید. این Zone ها فقط شامل لیستی از Name Server ها برای فضای نام داده شده می‌باشند و به عنوان یک سرور جانبی در کنار سرور DNS عمل می‌کنند. برای آشنایی بیشتر با این Zone ها فرض کنید که در شبکه، یک دامنه با نام Bigfirm.com و یک زیردامنه با نام Ecoast.Bigfirm.com در اختیار دارید. دامنه Bigfirm.com شامل یک سرور DNS اصلی به نام Bf1.bigfirm.com، و زیردامنه Ecoast.Bigfirm.com دارای دو سرور با نام‌های Dns1.Ecoast.Bigfirm.com و Dns2.Ecoast.Bigfirm.com می‌باشد. در ابتدا دو سرور Dns1 و Dns2 در زیردامنه، برای سرور Bf1 شناخته شده هستند و بنابراین این سرورها (Bf1، Dns1 و Dns2) می‌توانند با یکدیگر در ارتباط باشند. پس از مدتی، مدیر زیردامنه Ecoast دو سرور DNS دیگر به زیردامنه اضافه می‌کند اما سرور Bf1 از وجود آنها بی خبر است بنابراین هنوز با سرور جدید در ارتباط نمی‌باشد. برای حل این مشکل، می‌توان بروی سرور

DNS اصلی (Bf1)، یک Stub Zone در رابطه با زیردامنه Ecoast ایجاد نموده تا با استفاده از آن و طی فرایند Zone Transfer، سرور Bf1 بتواند سایر سرورهای اضافه شده به زیردامنه Ecoast را شناسایی نموده و با آنها ارتباط برقرار نماید.

ایجاد Stub Zone ها نیز با استفاده از ویزارد “New Zone Wizard” انجام می شود. مراحل کار شبیه به ایجاد Secondary Zone ها می باشد. فقط کافی است در صفحه “Zone Type” گزینه Stub Zone را انتخاب نموده و بقیه مراحل را همانند Secondary Zone انجام دهید.



شکل ۴-۳۱

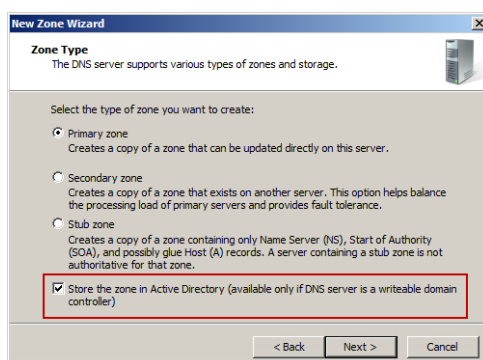
#### ۴-۳-۶ Zone های یکپارچه با اکتیو دایرکتوری

اگر بار دیگر به صفحه “Zone Type” از ویزارد “New Zone Wizard” نگاه کنید، گزینه ای به نام “Store the zone in Active Directory” را که در پایین صفحه قرار دارد مشاهده خواهید نمود. این گزینه تنها زمانی قابل استفاده می باشد که DNS به همراه اکتیو دایرکتوری نصب شده باشد و در واقع Domain Controller به عنوان سرور DNS در نظر گرفته شده باشد. Zone های یکپارچه با اکتیو دایرکتوری که با نام AD Integrated Zones نیز شناخته می شوند، یکی از برجسته ترین پیاده سازی ها در سرور DNS می باشند. این Zone ها با دو نوع قبلی تفاوت هایی دارند: اول اینکه پایگاه داده مربوط به فضاهای نام به جای قرارگیری در یک فایل متنی، داخل اکتیو دایرکتوری ذخیره می شود، و دوم اینکه این Zone ها به جای پاسخگویی به سرورهایی که در طی پردازش Zone Transfer تعیین کرده اید (تب Zone Transfer در قسمت Properties از Primary Zone)، به کلیه Domain Controller ها در اکتیو دایرکتوری پاسخگو می باشند. در واقع با وجود AD Integrated Zones دیگر نیازی با استفاده از فرایند Zone Transfer نمی باشد و به جای آن از فرایندی به نام AD Replication (تکثیر اکتیو دایرکتوری) استفاده می گردد. AD Replication به DC ها (که در اینجا نقش DNS نیز دارند) اجازه می دهد که اطلاعات موجود در Zone ها را میان خود تکثیر نموده و از آنها استفاده کنند.

ایجاد Active Directory Integrated Zones نیز با استفاده از ویزارد New Zone Wizard انجام می‌شود. در ادامه نحوه انجام کار را برای Forward Lookup Zones نشان خواهیم داد (باز هم تأکید می‌کنیم که استفاده از این قابلیت تنها در صورت وجود اکتیو دایرکتوری امکان‌پذیر می‌باشد. برای چگونگی استفاده از اکتیو دایرکتوری به فصل ۷ مراجعه نمایید).

### ایجاد Forward Lookup AD Integrated Zones

۱. در کنسول DNS Manager بر روی Forward Lookup Zones کلیک راست نموده و New Zone را انتخاب کنید.
۲. در صفحه آغازین ویزارد "New Zone Wizard" بر روی Next کلیک کنید.
۳. در صفحه "Zone Type" گزینه Primary Zone را انتخاب نموده و همچنین گزینه Store the zone in Active Directory را نیز فعال نمایید، سپس بر روی Next کلیک کنید.

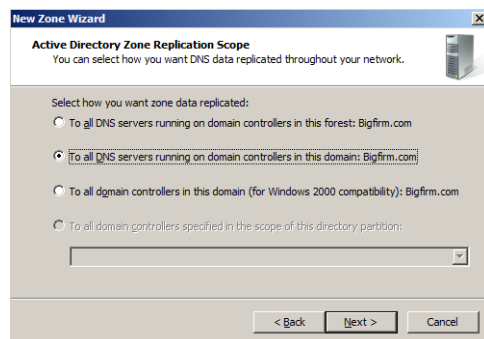


شکل ۴-۳۲

۴. در صفحه "Active Directory Zone Replication Scopes" باید ناحیه‌ای که اطلاعات این Zone مورد استفاده قرار می‌گیرد را تعیین کنید. در واقع باید مشخص کنید که اطلاعات Zone میان کدام DC ها و در چه سطحی (DC های موجود در یک دامنه، DC های موجود در یک Forest\_جنگل، و یا DC هایی که شما به صورت شخصی شده تعیین می‌کنید) تکثیر شوند. گزینه‌هایی که در این صفحه قابل انتخاب هستند عبارتند از:

- ♦ To all DNS servers running on domain controllers in this forest: این گزینه جهت تکثیر اطلاعات Zone میان تمام Domain Controller ها در یک جنگل (در اینجا Bigfirm.com) استفاده می‌شود.
- ♦ To all DNS servers running on domain controllers in this forest: این گزینه جهت تکثیر اطلاعات Zone میان تمام Domain Controller ها در یک دامنه (در اینجا Bigfirm.com) استفاده می‌شود.

- ♦ **To all domain controller in this domain(for Windows 2000 compability):** این گزینه همانند گزینه دوم بوده ولی برای دامنه‌هایی است که در آنها DC جزئی از ویندوز ۲۰۰۰ می‌باشد.

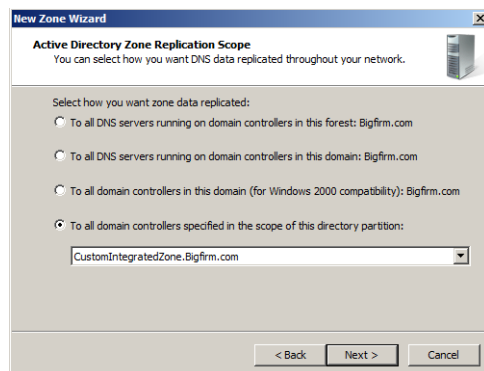


شکل ۴-۳۳

- ♦ **To all domain controllers specified in the scope of this directory partition:** این گزینه که بطور پیش‌فرض غیرفعال است زمانی استفاده می‌شود که قصد داشته باشید جهت استفاده تعداد مشخصی از DCها که خودتان تعیین می‌کنید، یک Zone (یکپارچه با اکتیو دایرکتوری) ایجاد کنید (به عبارت دیگر یک Directory Partition شخصی‌سازی شده ایجاد نمایید). برای استفاده از این گزینه باید ابتدا با استفاده از ابزار DnsCmd در خط فرمان یک Directory Partition شخصی‌سازی شده ایجاد کنید. برای انجام این کار، دستور زیر را در Cmd وارد نمایید:

```
dnscmd /createdirectorypartition CustomIntegratedZone.Bigfirm.com
```

این دستور یک Directory Partition با نام CustomIntegratedZone.Bigfirm.com در اکتیو دایرکتوری ایجاد می‌کند. پس از اجرای دستور بالا، صفحه "Active Directory Zone Replication Scopes" به صورت زیر خواهد بود.



شکل ۴-۳۴

دقت داشته باشید که Directory Partition های سفارشی زمانی ایجاد می‌شوند که قصد داشته باشید اطلاعات یک Zone تنها میان DC هایی که شما مشخص می‌کنید تکثیر شوند، بنابراین پس از ایجاد یک Directory Partition لازم است که سرورهای مورد نظر را در فهرست آن Partition قرار دهید. برای انجام این کار باید بار به ازای هر سروری که قصد دارید به Directory Partition اضافه کنید، از دستور زیر استفاده نمایید:

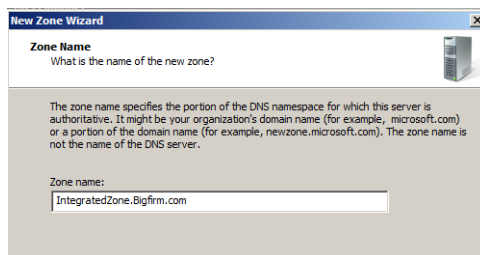
```
dnscmd <Server Name> /enlistdirectoryPartition CustomIntegratedZone.
Bigfirm.com
```

به عنوان مثال برای قرار دادن سرور Bf2 دستور زیر را وارد نمایید:

```
dnscmd Bf2 /enlistdirectoryPartition CustomIntegratedZone.Bigfirm.com
```

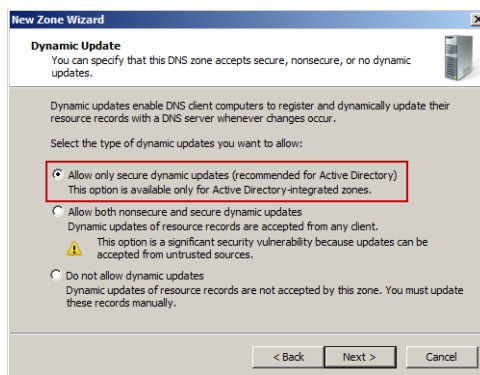
پس از انجام تنظیمات و انتخاب گزینه مورد نظر، بر روی Next کلیک کنید.

۵. در صفحه "Zone Name"، نام zone را وارد نموده و بر روی Next کلیک کنید. در اینجا از نام IntegratedZone.local استفاده شده است.



شکل ۴-۳۵

۶. در صفحه "Dynamic Update" گزینه Allow only secure dynamic updates را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۴-۳۶

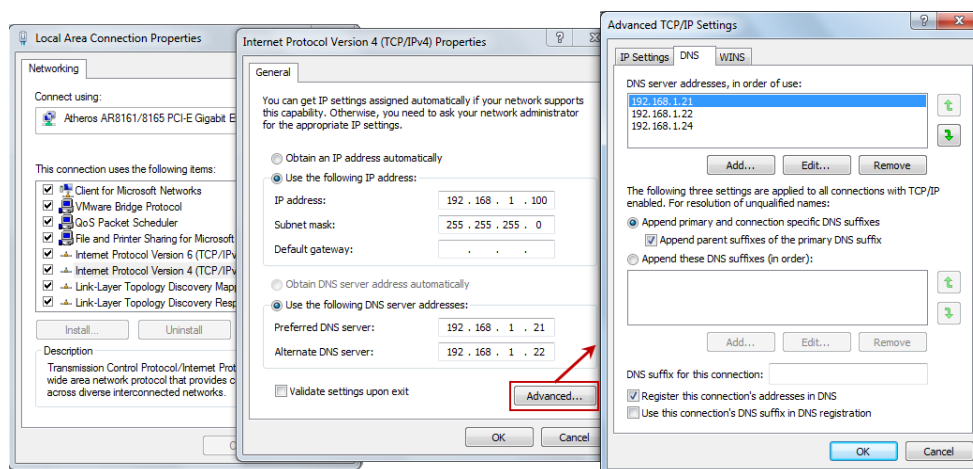
۷. در صفحه "Completing the New Zone Wizard" بروی Finish کلیک کنید.

#### ۴-۴ یکپارچگی با سایر سرورهای DNS

در قسمت مفاهیم پایه DNS، اصطلاحات Iteration، Recursion، Forwarding و Delegation را معرفی کردیم. این مفاهیم در واقع بیان‌کننده روش‌های تحلیل (تبدیل) نام هستند و در رابطه با یکپارچه سازی یک سرور با سایر سرورهای DNS به کار برده می‌شوند. منظور از یکپارچه سازی سرورها با یکدیگر، پیکربندی آنها بگونه‌ای است که قادر باشند با یکدیگر ارتباط برقرار نموده و چنانچه هر کدام از آنها قادر به پاسخگویی به درخواست‌هایی که از طرف کاربران داده می‌شود نباشند، بتوانند با کمک سایر سرورها درخواست‌های رسیده را پاسخ دهند. در این قسمت قصد داریم انواع روش‌هایی که در این زمینه مورد استفاده قرار می‌گیرند را مورد بررسی قرار دهیم.

#### ۴-۴-۱ Iteration

روش Iteration (از سرگیری) یکی از پردازش‌هایی است که در سمت کاربران قرار دارد و زمانی اتفاق می‌افتد که یک سرور DNS توانایی پاسخگویی به درخواست کاربر را نداشته باشد، بنابراین کاربر مجبور می‌شود به سرور DNS دیگری مراجعه کند. پیکربندی این روش بر روی کامپیوتر کاربران انجام می‌شود. بدین منظور لازم است در تنظیمات TCP/IP کاربر، به قسمت DNS رفته و آدرس IP سایر سرورهای DNS را وارد نمایید. در شکل زیر این وضعیت نشان داده شده است.



شکل ۴-۳۷



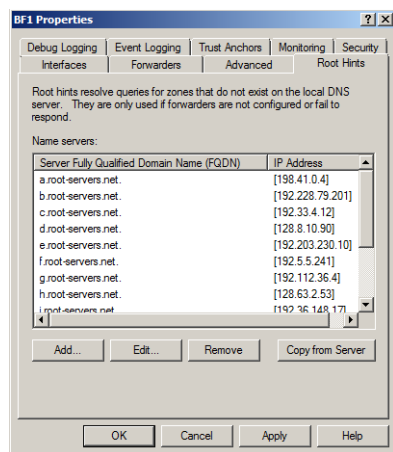
در شکل بالا چنانچه سرور DNS با آدرس 192.168.1.21 قادر به پاسخگویی نباشد، درخواست کاربر به سرور دیگری با آدرس 192.168.1.22 فرستاده می‌شود. به همین ترتیب، چنانچه سرور دوم قادر به پاسخگویی نباشد، این درخواست به سایر سرورهایی که آدرس آنها در تب DNS از شکل ۴-۳۷ تعیین نموده‌اید (به ترتیب از بالا به پایین) فرستاده می‌شود.

#### Recursion ۴-۴-۲

Recursion (بازگشت) مهمترین پردازشی است که در اینترنت اتفاق می‌افتد. درخواست یافتن یک آدرس با مراجعه به سرورهای سطح بالا شروع شده و به ترتیب تا رسیدن به سرور نام مورد نظر ادامه می‌یابد.

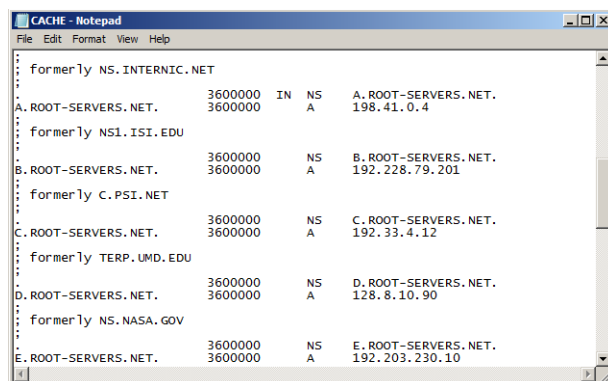
در ویندوز سرور، می‌توانید با مراجعه به کنسول DNS Manager این سرورهای سطح بالا را مشاهده کنید (این سرورها با نام Root Hints یا سرورهای ریشه شناخته می‌شوند). جهت مشاهده این سرورها مراحل زیر را دنبال کنید:

۱. در کنسول DNS Manager بروی نام سرور کلیک‌راست نموده و Properties را انتخاب کنید.
۲. در پنجره Server Properties تب Root Hints را انتخاب کنید.
۳. لیست Root Hint ها را از قسمت Name Servers مشاهده کنید.



شکل ۴-۳۸

لیست Root Hint ها در یک فایل متنی به نام CACHE.DNS و در مسیر C:\windows\system32\dns قرار دارد. پس از باز کردن این فایل، چیزی شبیه به شکل ۴-۳۹ مشاهده خواهید نمود.



شکل ۴-۳۹

#### Delegation ۳-۴-۴

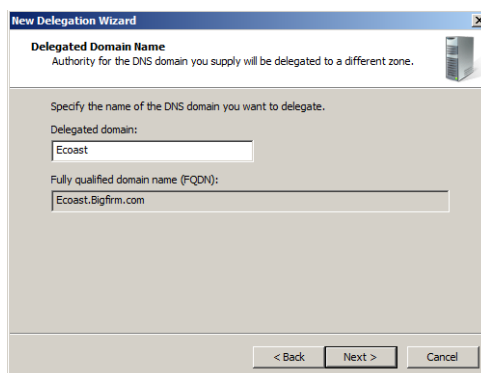
Delegation به معنای واگذاری اختیار به سایر سرورهای DNS می‌باشد. در حالی که سرورهای ریشه درخواست‌های رسیده از طرف سرورهای DNS در طی ساختار سلسله‌مراتبی را مدیریت می‌کنند، با استفاده از Delegation درخواست‌های روبه پایین را به سروهای سطح پایین‌تر واگذار می‌کنند. به عنوان مثال، سرورهای DNS که فضای نام com. را کنترل می‌کنند، ثبت زیردامنه‌هایی مثل example.com را به سرورهای سطح پایین‌تر واگذار می‌نمایند. طی فرایند Delegation، لیستی از سرورهای سطح پایین برای یافتن فضای نام example.com فراهم می‌شود، بنابراین سرور نام com. این لیست را به سرور DNS ای که به دنبال فضای نام مورد نظر می‌باشد ارسال می‌کند.

جهت درک موضوع، فرض کنید در اکتیو دایرکتوری، دامنه‌ای با نام Bigfirm.com وجود دارد. سرور DNS که برای این دامنه ایجاد می‌شود، وظیفه تحلیل نام برای کاربران آنرا برعهده دارد. حال فرض کنید دامنه دیگری با نام Ecoast.Bigfirm.com که زیردامنه Bigfirm.com می‌باشد ایجاد می‌کنید. بجای اینکه وظیفه تحلیل نام برای کاربران دامنه جدید را به همان سرور واگذار کنید، می‌توانید با تعریف یک Delegation بر روی این دامنه، این وظیفه را به سرور دیگری واگذار کنید.

اجازه دهید مراحل کار را با فرض اینکه دامنه‌ای به نام Ecoast.Bigfirm.com در اختیار دارید نشان‌دهیم:

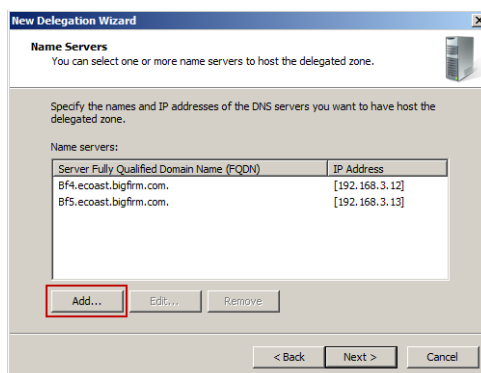
۱. در کنسول DNS Manager بر روی Forward Lookup Zone دابل کلیک نموده تا آیتم‌های زیرمجموعه آن نمایش داده شوند.
۲. بر روی Primary Zone که در قسمت‌های قبل با نام Bigfirm.com ایجاد کردید کلیک‌راست نموده و گزینه New Delegation را انتخاب کنید.

۳. در صفحه آغازین ویزارد "New Delegation Wizard" بر روی Next کلیک کنید.
۴. در صفحه "Delegate Domain Name" نام زیردامنه‌ای که قرار است به آن Delegation داده شود را وارد نموده و بر روی Next کلیک کنید.



شکل ۴-۴۰

۵. در صفحه "Name Servers" با استفاده از دکمه Add سرورهایی که قرار است Delegated Zone بر روی آنها میزبانی شود را اضافه کنید. پس از اضافه کردن، بر روی Next کلیک کنید.



شکل ۴-۴۱

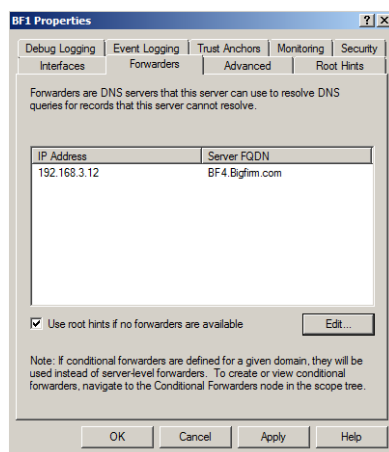
۶. در صفحه "Completing the New Delegation Wizard" بر روی Finish کلیک کنید.

#### Forwarding ۴-۴-۴

مفهوم بعدی، انجام Forwarding (ارسال) می‌باشد. Forwarder (انتقال‌دهنده) به عنوان یک سرور DNS کمکی برای سرور فعلی عمل می‌نماید. زمانی که یک سرور DNS نتواند عمل تحلیل نام را انجام دهد، بجای مراجعه به سرورهای ریشه، آنرا به یک سرور DNS دیگر ارسال می‌کند. به عنوان مثال،

فرض کنید سرور Bf1 در دامنه Bigfirm.com، و سرور Bf4 نیز در دامنه Ecoast.bigfirm.com وظیفه تحلیل نام را در هر دامنه برعهده دارند. گاهی اوقات ممکن است سرور Bf1 در تحلیل نام ناتوان باشد، بنابراین می‌توان این وظیفه را به سرور Bf4 (که در دامنه Ecoast.bigfirm.com قرار دارد) محول نمود. جهت تعریف Forwarder بروی یک سرور DNS، می‌توانید مراحل زیر را دنبال کنید:

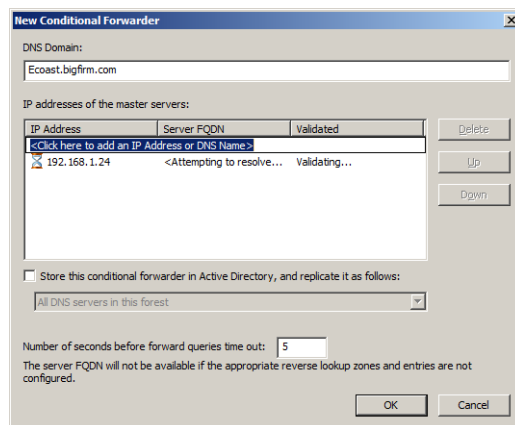
۱. در کنسول DNS Manager بروی نام سرور (Bf1) کلیک‌راست نموده و Properties را انتخاب کنید.
۲. در تب Forwarders بروی Edit کلیک کنید.
۳. آدرس IP سرور DNS که به عنوان Forwarder عمل می‌کند (در اینجا Bf4) را وارد نموده و بروی OK کلیک کنید.



شکل ۴-۴۲

نوع دیگری از Forwarder ها به نام **Conditional forwarders** (انتقال‌دهنده‌های شرطی) نیز وجود دارد که تمام درخواست‌های DNS را مطابق با نام دامنه‌ای که مشخص می‌کنید انتقال می‌دهند. به عنوان مثال می‌توانید مشخص کنید که درخواست‌های کاربران دامنه Ecoast.Bigfirm.com به یک یا چندین سرور DNS که تعیین نموده‌اید هدایت شوند. جهت افزودن Conditional forwarder مراحل زیر را دنبال کنید:

۱. در کنسول DNS Manager بروی پوشه Conditional forwarders کلیک‌راست نموده و گزینه New Conditional Forwarder را انتخاب کنید.
۲. در پنجره باز شده باید نام دامنه و آدرس IP سرور(های) DNS که قصد انتقال درخواست‌ها به آن(ها) را دارید وارد نمایید. این کارها به ترتیب از قسمت‌های DNS Domain (نام دامنه) و IP address of the master servers (نام و یا آدرس IP سرور DNS) امکان‌پذیر می‌باشد.



شکل ۴-۴۳

پس از یکپارچه کردن یک سرور DNS با سایر سرورها، اکنون می‌توانید آنرا در شبکه مورد استفاده قرار دهید. هر درخواستی که از طرف کاربران دامنه‌ها به سرور ارائه می‌شود، می‌تواند به کمک سایر سرورهای DNS پاسخ داده شود. این پاسخ‌ها برای مدتی (بطور پیش‌فرض یک ساعت) در حافظه سرور DNS باقی می‌ماند تا اگر سایر کاربران نیز آنرا درخواست نمودند، سرور بتواند به سرعت پاسخ دهد (دقت داشته باشید که تنظیمات معرفی شده در این قسمت برای شبکه‌های کوچک و متوسط الزامی نیستند اما در شبکه‌های بزرگ که بار پردازشی زیاد است می‌توانند مورد استفاده قرار گیرند).

#### ۴-۵ آشنایی با انواع رکوردها در DNS

پس از آنکه Zone را ایجاد نمودید، زمان آن می‌رسد که رکوردهایی<sup>۱</sup> را به آن اضافه کنید. در قسمت‌های قبل گفتیم که کاربران می‌توانند با استفاده از DNS پویا<sup>۲</sup>، به صورت خودکار رکوردها را ایجاد نموده و تغییر دهند، اما گاهی نیاز است که این رکوردها به صورت دستی وارد شوند و مورد ارزیابی قرار گیرند. بیش از ۲۵ نوع رکورد برای Zone های DNS وجود دارد که در اینجا تعدادی از مهمترین آنها که در ویندوز به کار گرفته شده است را معرفی خواهیم نمود.

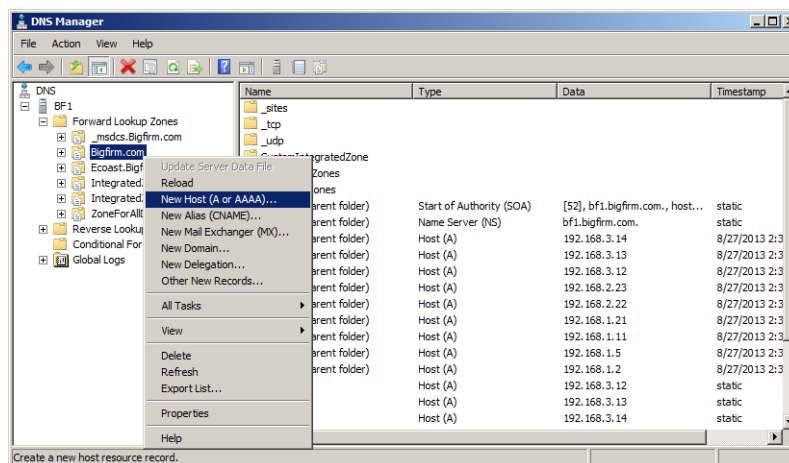
#### ۴-۵-۱ رکوردهای Host

رکوردهای Host(A) و Host(AAAA)، رایجترین رکوردهای به کار رفته در Forward Lookup Zone و Reverse Lookup Zone می‌باشند. به ترتیب، رکورد A در IPv4 یا AAAA در IPv6 شامل لیستی از نام کامپیوترها بوده و آدرس IP آنها را بدست می‌دهد، زمانی که قابلیت Dynamic Update در DNS

1. Records
2. Dynamic DNS

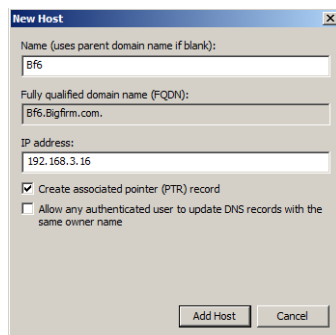
غیرفعال باشد، باید به ناچار از این رکوردها استفاده نمایید. به عنوان مثال فرض کنید یک سرور جدید به نام Bf6 به دامنه اضافه می‌کنید و قابلیت Dynamic Update در DNS نیز غیرفعال است. برای اینکه کاربران بتوانند با استفاده از نام این سرور (Bf6.bigfirm.com) به آن دسترسی پیدا کنند، باید یک رکورد Host(A) یا Host(AAAA) معادل با نام و آدرس IP (IPv4 یا IPv6) این سرور ایجاد کنید. به عنوان مثال برای ایجاد یک رکورد Host(A) برای ماشین Bf6 با آدرس 192.168.3.16 مراحل زیر را دنبال کنید:

۱. در کنسول Server Manager بروی Zone ای که قرار است سرور در آن قرار گیرد (در اینجا Bigfirm.com) کلیک راست نموده و New Host(A or AAAA) را انتخاب نمایید.



شکل ۴-۴۴

۲. در پنجره “New Host” نام و آدرس IP سرور را وارد نموده و بروی OK کلیک کنید.

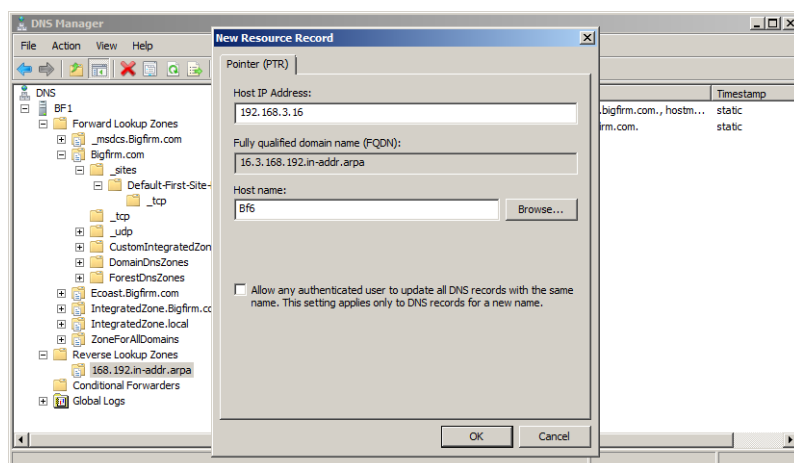


شکل ۴-۴۵

#### ۴-۵-۲ رکوردهای Pointer

رکوردهای Pointer (PTR) دارای عملکردی عکس رکوردهای Host هستند. این رکوردها برای تبدیل آدرس IP به نام FQDN به کار می‌روند. برای ایجاد رکوردهای PTR مراحل زیر را دنبال کنید:

۱. در زیر قسمت Reverse Lookup Zone بروی Zone مورد نظر کلیک‌راست نموده و New Pointer (PTR) را انتخاب کنید.
۲. در پنجره باز شده آدرس IP و نام متناظر با آنرا وارد نموده و بروی OK کلیک کنید.



شکل ۴-۴۶

#### ۴-۵-۳ رکوردهای Alias

رکورد Alias یا CNAME جهت ایجاد لیستی از نام‌های مستعار برای کامپیوترها به کار می‌رود و شامل فهرستی از نام‌ها و FQDN‌های متناظر با آنها می‌باشد. به عنوان مثال فرض کنید یک سرویس بروی سروری با نام AppService.bigfirm.com وجود داشته باشد. می‌توان جهت سهولت دسترسی کاربران به این سرویس، نام مستعار Application را برای آن انتخاب نمود. بنابراین زمانی‌که کاربران سرویسی با این نام را درخواست می‌کنند، به سرور (AppService.bigfirm.com) هدایت خواهند شد. برای ایجاد رکوردهای CNAME مراحل زیر را دنبال کنید:

۱. در قسمت Forward Lookup Zone بروی Zone مورد نظر کلیک راست نموده و New Alias (CNAME) را انتخاب نمایید.
۲. در پنجره باز شده، نامی که سرور با آن شناخته می‌شود و همچنین نام FQDN (نام کامل) سرور را وارد نموده و بروی OK کلیک کنید.

شکل ۴-۴۷

#### ۴-۵-۴ رکوردهای Mail Exchanger

رکورد MX آدرس سرویس‌دهنده پست الکترونیک (ایمیل) یک دامنه را مشخص می‌کند. به عنوان مثال فرض کنید کاربری در شبکه با آدرس ایمیل bill@Bigfirm.com وجود داشته باشد. اگر کسی قصد داشته باشد به این کاربر دسترسی پیدا کند ابتدا باید با سرویس‌دهنده ایمیل دامنه Bigfirm.com ارتباط برقرار نماید. اطلاعات این سرویس در رکورد MX ذخیره می‌شود. دقت داشته باشید که در صورت وجود چندین سرور ایمیل در دامنه، می‌توانید تعدادی رکورد MX ایجاد نموده و ب استفاده از اولویت‌هایی که برای آنها تعیین می‌کنید، آنها را در اختیار کاربران قرار دهید. برای ایجاد رکوردهای MX، بر روی Zone کلیک راست نموده و New Mail Exchanger را انتخاب کنید.

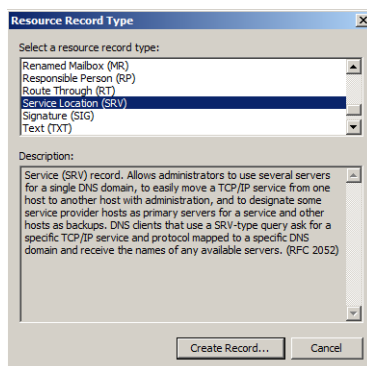
شکل ۴-۴۸



#### ۴-۵-۵ رکوردهای Service Location

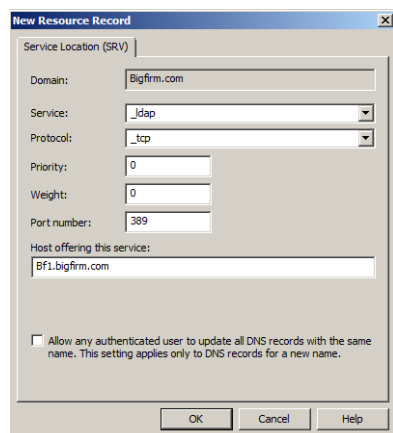
رکوردهای SRV یکی از جدیدترین رکوردهای سرویس DNS در ویندوز هستند. این رکوردها اجازه می‌دهند تا تعدادی از سرویس‌های خاص موجود بر روی سرورهای یک دامنه، مشخص شده و کاربرانی که اجازه استفاده از این رکوردها را دارند بتوانند از محل قرارگیری سرورهای میزبان این سرویس‌ها آگاهی یابند. رکوردهای SRV معمولاً بطور خودکار ایجاد می‌شوند، اما در مواردی که نیاز به ایجاد دستی آنها باشد می‌توانید مراحل زیر را دنبال کنید:

۱. بر روی نام Zone کلیک راست نموده و Other New Records را انتخاب نمایید.
۲. در پنجره "Resource Record Type" رکورد (SRV) Service location را انتخاب نموده و بر روی Create Record کلیک کنید.



شکل ۴-۴۹

۳. در پنجره باز شده، نوع سرویس و محل میزبانی آنرا تعیین نموده و بر روی OK کلیک کنید.



شکل ۴-۵۰

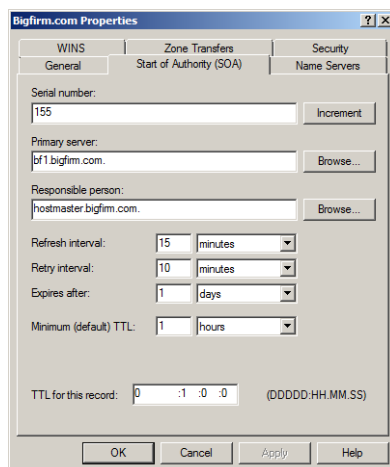
به عنوان مثالی در رابطه با این نوع از رکوردها، سرویس Net Logon در اکتیو دایرکتوری را در نظر بگیرید. این سرویس برای جستجوی LDAP و محل قرارگیری Domain Controllerها از رکوردهای SRV استفاده می‌نماید.

رکوردهای SRV دارای چندین پارامتر به شرح زیر می‌باشند:

- **Service name:** این مقدار بیانگر نام سرویس است و معمولاً قبل از آن از علامت “\_” استفاده می‌شود، مانند “\_gc” و “\_ldap”.
- **Server FQDN:** نام FQDN سروری است که یک سرویس را ارائه می‌دهد.
- **Port:** بیان کننده یکی از پورت‌های TCP یا UDP است که از طریق آنها یک سرویس قابل دسترسی می‌باشد. این پروتکل به صورت tcp یا udp مقداردهی می‌شود.
- **Priority:** این مقدار بیان کننده اولویت یک سرویس می‌باشد.
- **Weight:** این مقدار به عنوان معیاری برای اولویت در نظر گرفته می‌شود. در صورتی که از روابط سرویس‌ها و اولویت‌های آنها آگاهی ندارید، می‌توانید آنرا با صفر مقداردهی کنید.

#### ۴-۵-۶ رکوردهای Start Of Authority

در هر Zone یک رکورد SOA بطور پیش‌فرض ایجاد می‌شود. این رکورد اطلاعاتی در مورد چگونگی کنترل Zone و پارامترهای آن و همچنین نحوه برخورد سرور DNS با رکوردها را فراهم می‌نماید. در واقع زمانی که سرور DNS قصد استفاده از یک Zone را داشته باشد، به رکورد SOA موجود در آن مراجعه نموده و اطلاعات پایه از پیکربندی Zone (مانند نحوه تکثیر اطلاعات میان Zoneها) را بدست می‌آورد. برای ویرایش مقادیر رکوردهای SOA باید از تب Start Of Authority در قسمت Properties از Zone اقدام کنید. در شکل زیر، این تب نشان داده شده است.



شکل ۴-۵۱

فیلدهایی که در این تب وجود دارند عبارتند از:

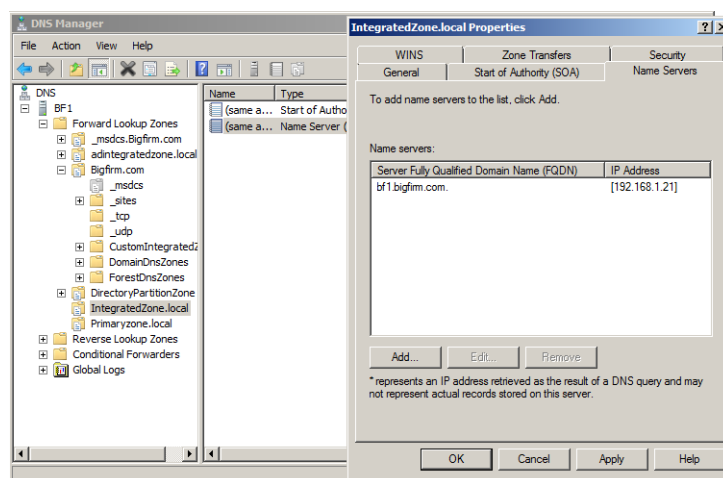
- ♦ **Serial Number**: این شماره بیانگر شماره تجدید نظر (اصلاح) در Zone می باشد. هرگاه که تغییر جدیدی در اطلاعات Zone رخ می دهد، این شماره یک واحد افزایش پیدا می کند. Primary Zone ها می توانند شماره خود را با این شماره در Secondary Zone ها مقایسه نموده و از بروز بودن اطلاعات Zone ها مطمئن شوند. دقت داشته باشید که شماره موجود در قسمت Serial Number برای انجام فرایند Zone Transfer مهم است زیرا تنها در صورت تغییر این شماره، فرایند Zone Transfer میان Primary Zone ها و Secondary Zone ها اتفاق خواهد افتاد. چنانچه شماره سریال Primary Zone بالاتر از Secondary Zone باشد (یعنی تغییرات بیشتری در Primary Zone رخ داده است)، درخواست Zone Transfer از طرف Secondary Zone فرستاده خواهد شد.
- ♦ **Primary Server**: نام کامل سروری است که فایل Zone بر روی آن قرار دارد.
- ♦ **Responsible person**: مقدار این فیلد به عنوان آدرس ایمیل فردی که Zone را مدیریت می کند در نظر گرفته می شود. دقت داشته باشید که در این آدرس علامت @ با نقطه (.) جایگزین شده است.
- ♦ **Refresh interval**: این مقدار بیان کننده مدت زمانی است که سرور حاوی Secondary Zone باید قبل از تلاش برای بررسی تغییرات رکوردهای Zone در سرور اصلی (Master)، منتظر بماند. پس از این مدت سرور حاوی Secondary Zone یک درخواست برای نسخه ای از رکورد SOA در سرور Master ارائه می دهد و پس از دریافت اطلاعات این رکورد، چنانچه شماره سریال Zone اصلی با Zone ثانویه متفاوت باشد، فرایند Zone Transfer رخ خواهد داد. بطور پیش فرض، این زمان ۱۵ دقیقه می باشد و در رکوردها برحسب ثانیه نشان داده می شود.
- ♦ **Retry interval**: چنانچه پس از ارائه درخواست Zone transfer توسط سرور Secondary، این فرایند با شکست مواجه شده باشد، مقدار موجود در فیلد Retry Interval مدت زمانی که سرور Secondary باید جهت ارائه درخواست مجدد برای بروزرسانی اطلاعات خود منتظر بماند را مشخص می نماید. این زمان بطور پیش فرض ۱۰ دقیقه بوده و مقدار آن در رکورد به صورت ثانیه می باشد.
- ♦ **Expires after**: مدت زمان اعتبار اطلاعات موجود در Secondary Zone را مشخص نموده و تا قبل از اتمام این زمان، سرور Secondary می تواند از اطلاعات خود برای پاسخگویی به درخواست های کاربران استفاده کند. بطور پیش فرض مقدار این زمان یک روز (۸۶۴۰۰ ثانیه) می باشد.
- ♦ **Minimum (default) TTL**: مدت زمان قرارگیری رکوردها در حافظه Cache سرور و در واقع مدت زمان عمر رکوردها را مشخص می کند. مقدار این زمان بطور پیش فرض یک ساعت (۳۶۰۰)

ثانیه) می باشد.

- ♦ **TTL for this record**: مدت زمان عمر رکورد SOA را مشخص می کند و مقدار پیش فرض آن نیز همانند گزینه قبلی یک ساعت (۳۶۰۰ ثانیه) می باشد. دقت داشته باشید که مدت زمان موجود در این قسمت بر سایر زمان های تعیین شده اولویت دارد.

#### ۷-۵-۴ رکوردهای Name Server

رکوردهای NS، لیست سرورهای پاسخگو به درخواست های یک Zone را نگهداری می کنند و حداقل یک رکورد از این نوع در هر Zone وجود دارد. همانند رکورد SOA، می توانید این رکورد را از قسمت Properties مربوط به Zone و از تب Name Servers مورد تغییر قرار دهید.



شکل ۴-۵۲

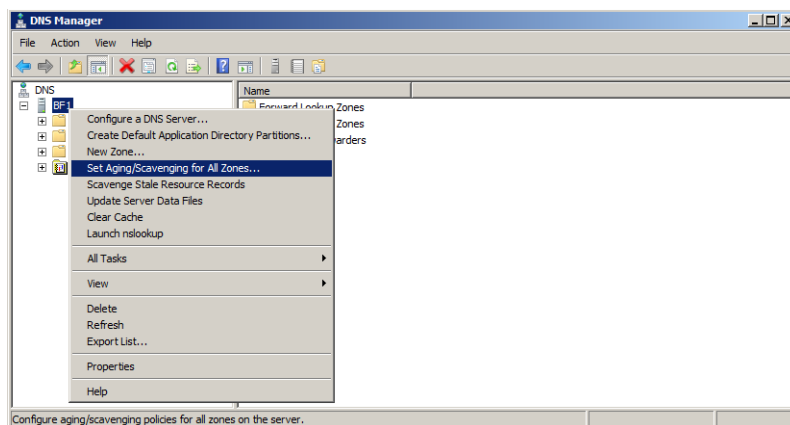
دقت داشته باشید چنانچه Zone های ایجاد شده در کنسول DNS Manager به صورت یکپارچه با اکتیو دایرکتوری نباشند، می توانید رکوردهایی که به صورت دستی در آنها ایجاد می کنید را در فایل حاوی Zone مشاهده کنید. برای انجام این کار لازم است به مسیر C:\Windows\System32\dns مراجعه نموده و فایل Zone را در برنامه Notepad باز کنید.

#### ۸-۵-۴ فرایندهای Aging و Scavenging

فرایند Aging اشاره به پروسه ای دارد که عمر رکوردهایی که از طریق Dynamic Update بدست آمده اند بررسی و مدیریت می شود. Scavenging نیز فرایندی است که از طریق آن رکوردهایی که عمر آنها به پایان رسیده است از داخل Zone حذف می شوند. این فرایندها برای نظم دهی به ساختار

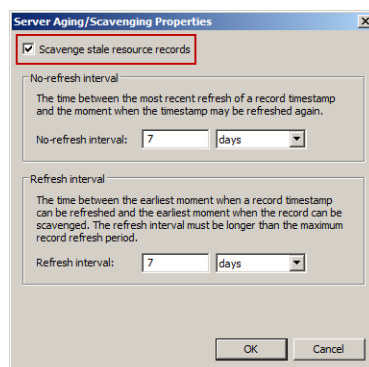
رکوردها در Zoneها بسیار پرکاربرد می‌باشند (دقت داشته باشید که فرایند مزکور در دوسطح Server و Zone انجام می‌شود). جهت فعال‌سازی Aging/Scavenging مراحل زیر را دنبال کنید:

۱. در کنسول DNS Manager بر روی نام سرور کلیک‌راست نموده و گزینه Set Aging/Scavenging for All Zones را انتخاب کنید.



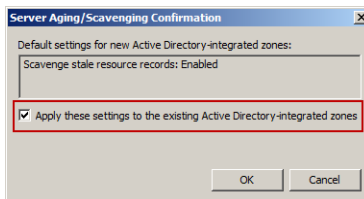
شکل ۴-۵۳

۲. در پنجره "Server Aging/Scavenging Confirmation"، گزینه Scavenging stale resource records را فعال کنید.



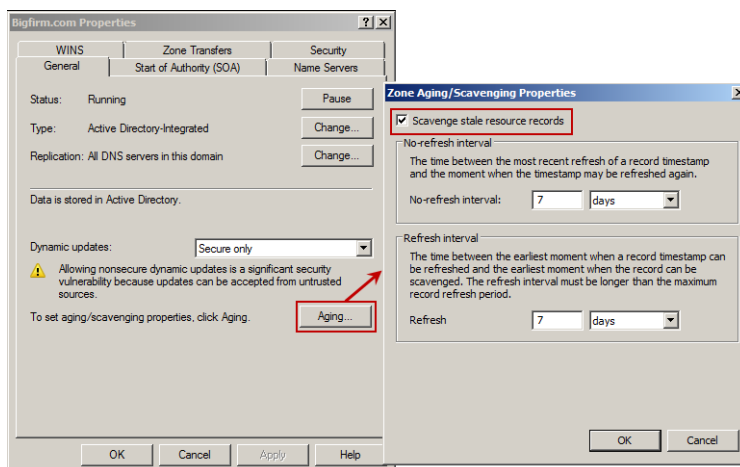
شکل ۴-۵۴

۳. در شکل ۴-۵۴ پس از کلیک بر روی OK، پنجره دیگری ظاهر می‌گردد. جهت اعمال این تنظیمات بر روی Zoneهای یکپارچه با اکتیو دایرکتوری، در این پنجره گزینه Apply this settings to the existing Active Directory-integrated zones را فعال کنید.



شکل ۴-۵۵

۴. اکنون بروی هر Zone کلیک راست نموده و Properties را انتخاب کنید.
۵. در صفحه Zone Properties، بروی دکمه Aging کلیک کنید.
۶. در پنجره "Zone Aging/Scavenging Properties" گزینه "Scavenging stale resource records" را فعال نموده و بروی OK کلیک کنید.



شکل ۴-۵۶

#### ۴-۶ پیاده‌سازی DNS در Server Core

در قسمت‌های قبل، چگونگی نصب و راه‌اندازی DNS با استفاده از کنسول Server Manager و همچنین پیکربندی آنرا با استفاده از کنسول DNS Manager شرح دادیم. در این قسمت قصد داریم نحوه پیاده‌سازی DNS در Server Core را شرح داده و مراحلی که در قسمت‌های قبل با استفاده از واسط‌های گرافیکی انجام دادیم را به کمک دستورات خط فرمان اجرا کنیم. یکی از دستوراتی که در این قسمت بسیار مورد استفاده قرار می‌گیرد، دستور DNSCmd است که اکثر تنظیمات و پیکربندی‌های DNS با استفاده از آن انجام می‌شود. در ادامه، به بررسی این دستور و پارامترهای آن می‌پردازیم.

## ۴-۶-۱ نصب DNS

جهت نصب DNS می‌توانید از دستور `dism` استفاده کنید. دو دستوری که در ادامه آورده‌شده، ابتدا فهرست Role‌های قابل نصب در Server Core را نمایش‌داده و سپس DNS را نصب می‌کند. فقط دقت داشته باشید که پارامتر `/featurename` نسبت به بزرگی و کوچکی حروف حساس می‌باشد.

```
rem list roles available
dism /online /get-features /format:table
```

```
rem install DNS role
dism /online /enable-feature /featurename:DNS-Server-Core-Role
```

در دستور بالا فقط یک سرور DNS راه‌اندازی می‌کنید و چون رل Active Directory Domain Services نصب نشده، هیچ سرویسی در رابطه با اکتیو دایرکتوری در اختیار نخواهید داشت.

## ۴-۶-۲ پیکربندی سرور DNS

جهت پیکربندی DNS از ابزار `DnsCmd` در خط فرمان استفاده می‌شود. برای مشاهده پارامترهای مورد استفاده در این ابزار، دو دستور زیر را وارد نموده تا آنها را در قالب یک فایل متنی ذخیره نمایید و سپس به کمک Notepad آنها را مشاهده کنید:

```
rem save to C drive
DnsCmd ? > C:\DnsCmd.txt
```

```
rem open in Notepad
C:\DnsCmd.txt
```

محتویات فایل ذخیره شده به صورت زیر می‌باشد:

```
Usage: DnsCmd <ServerName> <Command> [<Command Parameters>]
```

```
<ServerName>:
    IP address or host name    -- remote or local DNS server
    .                          -- DNS server on local machine

<Command>:
    /Info                      -- Get server information
    /Config                    -- Reset server or zone configuration
    /EnumZones                  -- Enumerate zones
    /Statistics                 -- Query/clear server statistics data
    /ClearCache                 -- Clear DNS server cache
    /WriteBackFiles             -- Write back all zone or root-hint datafile(s)
    /StartScavenging            -- Initiates server scavenging
    /IpValidate                 -- Validate remote DNS servers
    /ResetListenAddresses       -- Set server IP address(es) to serve DNS requests
    /ResetForwarders            -- Set DNS servers to forward recursive queries to
    /ZoneInfo                   -- View zone information
    /ZoneAdd                    -- Create a new zone on the DNS server
    /ZoneDelete                 -- Delete a zone from DNS server or DS
    /ZonePause                  -- Pause a zone
    /ZoneResume                 -- Resume a zone
```

---

```

/ZoneReload           -- Reload zone from its database (file or DS)
/ZoneWriteBack        -- Write back zone to file
/ZoneRefresh          -- Force refresh of secondary zone from master
/ZoneUpdateFromDs     -- Update a DS integrated zone by data from DS
/ZonePrint            -- Display all records in the zone
/ZoneResetType        -- Change zone type
/ZoneResetSecondaries -- Reset secondary\notify information for a zone
/ZoneResetScavengeServers -- Reset scavenging servers for a zone
/ZoneResetMasters     -- Reset secondary zone's master servers
/ZoneExport           -- Export a zone to file
/ZoneChangeDirectoryPartition -- Move a zone to another directory partition
/TrustAnchorsResetType -- Change zone type for a trust anchor zone
/EnumRecords          -- Enumerate records at a name
/RecordAdd            -- Create a record in zone or RootHints
/RecordDelete         -- Delete a record from zone, RootHints or cache
/NodeDelete           -- Delete all records at a name
/AgeAllRecords        -- Force aging on node(s) in zone
/TrustAnchorAdd       -- Create a new trust anchor zone on the DNS server
/TrustAnchorDelete    -- Delete a trust anchor zone from DNS server or DS
/EnumTrustAnchors     -- Enumerate records at a name
/EnumDirectoryPartitions -- Enumerate directory partitions
/DirectoryPartitionInfo -- Get info on a directory partition
/CreateDirectoryPartition -- Create a directory partition
/DeleteDirectoryPartition -- Delete a directory partition
/EnlistDirectoryPartition -- Add DNS server to partition replication scope
/UnenlistDirectoryPartition -- Remove DNS server from replication scope
/CreateBuiltinDirectoryPartitions -- Create built-in partitions
/ExportSettings       -- Output settings to DnsSettings.txt in the DNS
server database directory
/OfflineSign          -- Offline signing zone files, including key
generation/deletion

<Command Parameters>:
  DnsCmd <CommandName> /? -- For help info on specific Command

```

---

همانطور که قبلاً شرح دادیم، سرور DNS جهت تبادل اطلاعات باید با سایر سرورها در ارتباط باشد و با آنها یکپارچه شود. به کمک Forwarderها می‌توان درخواست‌های کاربران را دریافت نموده و آنها را به سرور DNS اصلی تحویل داد. جهت افزودن یک Forwarder به سرور از پارامتر `/resetforwarders` استفاده می‌شود. علاوه بر آن، دو پارامتر `/slave` و `/noslave` نیز معادل فعال نمودن تیک مربوط به گزینه “Use root hints if no forwarders are available” در تب Forwarders از قسمت Properties مربوط به سرور DNS می‌باشد. این گزینه بیان می‌کند که در صورت عدم دسترسی به Forwarderها، از سرورهای ریشه که فهرست آنها در تب Root Hints قرار دارد، جهت پاسخگویی به درخواست‌ها استفاده شود. بطور پیش‌فرض پارامتر `/noslave` به کار گرفته شده است و معادل فعال نمودن این گزینه می‌باشد. جهت اضافه نمودن Forwarder دستور زیر را که یک Forwarder با آدرس 192.168.1.22 به سرور DNS اضافه می‌نماید وارد نمایید:

```

rem add a forwarder
dnscmd /resetforwarders 192.168.1.22

```

پس از اجرای دستور، جهت بررسی ایجاد Forwarder می‌توانید از پارامتر `/info` استفاده کنید.



نتیجه اجرای این دستور (در مثال بالا) به صورت زیر می باشد:

```
rem verify forwarders
dnscmd /info
```

```
Forwarders:
Ptr          = 0000000000143CD0
MaxCount     = 1
AddrCount    = 1
Addr[0] => af=2, salen=16, [sub=0, flag=00000000] p=13568, addr=
192.168.1.22
forward timeout = 3
slave         = 0
```

در Server Core، امکان مشاهده فهرست Root Hints از طریق برنامه Notepad فراهم شده است. این اطلاعات در فایلی به نام `CACHE.dns` قرار دارد. جهت باز نمودن این فایل می توانید آدرس زیر را که محل قرارگیری آن می باشد وارد نمایید:

```
C:\Windows\system32\dns\cache.dns
```

پارامتر `/config` فهرستی از دستورات پیکربندی DNS را در اختیار شما قرار می دهد. جهت مشاهده این دستورات کافی است این پارامتر را به همراه یک علامت سؤال (?) وارد کنید. پیشنهاد می شود این دستورات را در یک فایل متنی ذخیره نموده تا بتوانید به راحتی دستورات پیکربندی خود را ایجاد نمایید. جهت انجام این کار از دستور زیر استفاده کنید:

```
Rem porting the help info to a text file
Dnscmd /config ? > "dnscmd_help.txt"
```

#### ۴-۶-۳ افزودن Zone ها به DNS در Server Core

در نسخه Server Core نیز همانند سایر نسخه ها امکان اضافه کردن انواع Zone ها به سرور DNS وجود دارد. قبل از شروع کار بد نیست از نحوه اضافه کردن Zone به سرور آگاه شوید. جهت انجام این کار دستور زیر را وارد کنید:

```
Dnscmd /zoneadd ?
```

جهت اضافه کردن Primary Zone و Secondary Zone، از پارامتر `/zoneadd` استفاده کنید. در اینجا نام Primary Zone، `Bigfirm.com` است و اطلاعات آن در فایلی به نام `bigfirm.com.dns` ذخیره می شود. نام Secondary Zone نیز `primaryzone.local` بوده و اطلاعات آن در فایل `primaryzone.local.dns` ثبت می شود.

```
rem create new zone for bigfirm.com
dnscmd /zoneadd bigfirm.com /primary /file bigfirm.com.dns
```

در Secondary Zone علاوه بر نام فایل، به آدرس IP سرور اصلی نیاز است:

```
rem create a secondary zone for PrimaryZone.local
dnscmd /zoneadd primaryzone.local /secondary 192.168.1.10 /file
primaryzone.local.dns
```

اکنون با دستور زیر می‌توانید وضعیت Zone‌های ایجاد شده را بررسی نمایید:

```
rem list zone
dnscmd /enumzones
Enumerated zone list:
Zone count = 3
```

Zone name	Type	Storage	Properties
.	Cache	File	
bigfirm.com	Primary	File	
primaryzone.local	Secondary	File	

با استفاده از پارامتر /zoneinfo می‌توانید مشخصات Zone را مشاهده کنید:

```
rem view properties of the zone
dnscmd /zoneinfo bigfirm.com
```

Zone query result:

```
Zone info:
ptr = 0000000000352700
zone name = bigfirm.com
zone type = 1 (1 = primary, 2 = secondary, 3 = stub)
shutdown = 0
paused = 0
update = 0 (0 = none, 1 = non and secure updates,
2 = secure only.)

DS integrated = 0 (0 = non AD integrated, 1 = AD integrated.)
read only zone = 0
data file = bigfirm.com.dns
using WINS = 0
using Ntstat = 0
aging = 0
refresh interval = 168
no refresh = 168
scavenge available = 0
Zone Masters NULL IP Array.
Zone Secondaries NULL IP Array.
secure secs = 1
Command completed successfully.
```

جهت مشاهده محتویات یک Zone نیز از پارامتر /zoneprint استفاده کنید:

```
rem list Bigfirm.com zone contents
```

```
dnscmd /zoneprint bigfirm.com
```

```
;
; Zone: bigfirm.com
; Server: BFSCl.bigfirm.com
; Time: Mon Jul 13 15:50:53 2009 UTC
;
@ 3600 NS bfsc1.bigfirm.com.
        3600 SOA bfsc1.bigfirm.com. hostmaster.bigfirm.com. 1 900
600 86400 3600
bfsc1 3600 A 192.168.1.11
```

```
;
; Finished zone: 2 nodes and 3 records in 0 seconds
;
```

```
rem list primaryzone.local zone contents
```

```
dnscmd /zoneprint primaryzone.local
```

```
;
; Zone: primaryzone.local
; Server: BFSCl.bigfirm.com
; Time: Mon Jul 13 16:17:11 2009 UTC
;
@ 3600 NS bf1.bigfirm.com.
        3600 NS 192.168.1.11.
        3600 NS 192.168.1.13.
        3600 SOA bf1.bigfirm.com. hostmaster.bigfirm.com . 9 900
600 86400 3600
cname 3600 CNAME hostrecord.primaryzone.local.
hostrecord 3600 A 192.168.1.21
```

```
;
; Finished zone: 3 nodes and 5 records in 0 seconds
```

#### ۴-۶-۴ مدیریت رکوردها در Zone

قبلاً انواع رکوردها و کاربرد آنها را معرفی کردیم. در این قسمت قصد داریم نحوه وارد کردن این رکوردها در Zone را به کمک دستورات خط فرمان نشان دهیم. دستور زیر، یک صورت کلی از وارد کردن رکوردها را نشان می‌دهد.

```
rem add records to bigfirm.com zone
```

```
DnsCmd <ServerName> /RecordAdd <Zone> <NodeName> [/Aging] [/OpenAcl]
[/CreatePTR] [<Ttl>] <RRType> <RRData>
```

مقادیر مورد نیاز برای این دستور، نام Zone، نام کامپیوتر، نوع رکورد (مانند A، CNAME یا MX) و اطلاعاتی در مورد داده‌های رکورد می‌باشد. دستور زیر، سه رکورد A، CNAME و MX را برای دامنه Bigfirm.com ایجاد می‌کند:

```
dnscmd /recordadd bigfirm.com webserver A 192.168.1.15
```

```

dnscmd /recordadd bigfirm.com vpn A 192.168.1.16
dnscmd /recordadd bigfirm.com mailserver A 192.168.1.17
dnscmd /recordadd bigfirm.com www cname webserver.bigfirm.com
dnscmd /recordadd bigfirm.com bigfirm.com. MX 10 mailserver.bigfirm.com

```

با استفاده از دستور زیر نیز می‌توانید رکوردی حاوی نام سرور اضافه کنید:

```

rem add a nameserver
dnscmd /recordadd bigfirm.com bfsc2 A 192.168.1.20
dnscmd /recordadd bigfirm.com bigfirm.com. NS bfsc2.bigfirm.com

```

اکنون اگر بار دیگر از پارامتر `/zoneprint` (جهت نمایش محتویات Zone) استفاده کنید نتایج حاصل از اجرای دستورات بالا را مشاهده خواهید نمود:

```

dnscmd /zoneprint bigfirm.com
;
; Zone: bigfirm.com
; Server: BFSC1.bigfirm.com
; Time: Mon Jul 13 16:09:58 2009 UTC
;
@ 3600 NS bfsc1.bigfirm.com.
      3600 NS bfsc2.bigfirm.com.
      3600 SOA bfsc1.bigfirm.com. hostmaster.bigfirm.com. 12 900 600
86400 3600
      3600 MX 10 mailserver.bigfirm.com.
bfsc1 3600 A 192.168.1.11
bfsc2 3600 A 192.168.1.20
mailserver 3600 A 192.168.1.17
vpn 3600 A 192.168.1.16
webserver 3600 A 192.168.1.15
www 3600 CNAME webserver.bigfirm.com.
;
; Finished zone: 7 nodes and 10 records in 0 seconds
;

```

جهت حذف رکوردها نیز می‌توانید از پارامتر `/recorddelete` استفاده کنید:

```

rem delete a record
dnscmd /recorddelete bigfirm.com vpn A 192.168.1.16

```

کلید اصلی مدیریت سرور DNS در محیط خط فرمان استفاده از دستور `DNSCmd` می‌باشد. به کمک این دستور قادر خواهید بود تمام تنظیمات قابل انجام در کنسول DNS Manager را توسط دستورات خط فرمان انجام دهید. به خاطر داشته باشید که بهترین کار جهت کار با دستورات خط فرمان ذخیره آنها در یک فایل متنی و ایجاد تنظیمات دلخواه در یک ویرایشگر متن می‌باشد. پس از آن فقط با چند کلیک‌راست در خط فرمان می‌توانید سرور خود را پیکربندی کنید.



## « فصل ۵ »

### مدیریت پروتکل DHCP

### Managing DHCP Protocol



TCP/IP یکی از پروتکل‌های پراهمیت در ویندوز سرور 2008 و 2008R2 می‌باشد. این پروتکل جهت برقراری ارتباط میان کاربران با استفاده از آدرس‌های IP مورد استفاده قرار می‌گیرد. جهت برخورداری کاربران و سرورها از آدرس‌های IP دو روش وجود دارد. روش اول وارد کردن آدرس‌ها به صورت دستی، و روش دوم دریافت آدرس به صورت خودکار می‌باشد. وارد کردن دستی آدرس‌های IP کار نسبتاً ساده‌ای است، مدیر شبکه به تنظیمات TCP/IP هریک از ماشین‌های متصل به شبکه رفته و یک آدرس به آن اختصاص می‌دهد. مشکل این روش زمانی آشکار می‌شود که تعداد ماشین‌ها در شبکه زیاد می‌شوند. تصور کنید که مدیر شبکه قرار است به ۵۰۰۰ ماشین در شبکه آدرس IP، Default Gateway، Subnet mask و آدرس‌های DNS را اختصاص دهد. در این مورد وارد کردن دستی آنها کار چندان ساده‌ای نخواهد بود.

به کمک سرویس DHCP<sup>۱</sup> می‌توانید محدوده‌ای از آدرس‌ها و اطلاعات مورد نیاز مثل Default Gateway، Subnet mask و تنظیمات DNS را فراهم نموده و به راحتی آنها را به ماشین‌ها اختصاص دهید. در این فصل قصد داریم نحوه راه‌اندازی این سرویس و مدیریت آنرا مورد بررسی قرار دهیم. بطور کلی مهمترین مباحثی که در این فصل به آنها پرداخته خواهد شد عبارتند از:

- ♦ نصب و راه‌اندازی سرویس DHCP
- ♦ پیکربندی سرور DHCP
- ♦ ایجاد و مدیریت Scope‌ها
- ♦ DHCP در اکتیو دایرکتوری

## ۵-۱ معرفی پردازش DORA

ساده ترین راه جهت آشنایی با طرز کار DHCP، آگاهی از فرایندی به نام DORA می‌باشد. DORA برگرفته از لغات Discover (کشف)، Offer (پیشنهاد)، Request (درخواست) و Acknowledge (تصدیق) می‌باشد. بطور خلاصه، فرایند DORA در DHCP به صورت زیر می‌باشد:

۱. **Discover**: در شبکه‌های مبتنی بر IP، زمانی که کاربران قصد دارند از سرویس DHCP استفاده کنند، ابتدا ماشین آنها یک پیغام خاص که DHCPDISCOVER (کشف DHCP) نامیده می‌شود، به داخل شبکه ارسال می‌کند.

۲. **Offer**: کلایه سرورهای DHCP که در حال گوش دادن به درخواست‌های کاربران هستند، پس از دریافت این پیغام، پایگاه داده داخلی خود را بررسی نموده و با یک پیغام که DHCPOFFER نامیده می‌شود و حاوی آدرس IP است به کاربر پاسخ می‌دهند. محتویات این پیغام بستگی به این دارد

1. Dynamic Host Configuration Protocol



- که سرور DHCP چگونه پیکربندی شده باشد. در ویندوز سرور 2008 و 2008R2 علاوه بر آدرس IP، Optiin های دیگری نیز جهت اختصاص به کاربران وجود دارد (مثل Default Gateway و ...).
۳. **Request:** پس از اینکه درخواست کاربر توسط سرورهای DHCP پاسخ داده شد، کاربر یک یا تعدادی از پیامهای DHCP OFFER را بسته به تعداد سرورهای DHCP که در زیرشبکه قرار دارد دریافت می‌کند، سپس یکی از آدرس‌ها را از میان OFFER ها انتخاب نموده و پیام DHCP REQUEST را به سرور انتخاب شده به منظور اعلام پذیرش سیگنال DHCP OFFER ارسال می‌کند. این پیام‌ها ممکن است پارامترهای پیکربندی اضافه‌تری را درخواست کنند.
۴. **Acknowledge:** زمانی که سرور DHCP یک DHCP REQUEST دریافت می‌کند، یک آدرس IP را به عنوان آدرس در حال استفاده علامت‌گذاری نموده، سپس یک DHCP ACK (تصدیق DHCP) به کاربر ارسال می‌کند. پیام تصدیق شامل پارامترهای درخواست شده در پیکربندی می‌باشد. اگر سرور به هر دلیلی قادر به پذیرفتن DHCP REQUEST نباشد، یک پیام DHCP NAK (عدم تصدیق DHCP) ارسال می‌کند. اگر کاربر این پیام را دریافت کند، فرایند درخواست آدرس را مجدداً آغاز می‌کند.
۵. زمانی که کاربر آدرس IP پیشنهاد شده (OFFER) را می‌پذیرد، این آدرس برای مدت زمانی محدود به او اختصاص پیدا می‌کند که این عمل Lease (اجاره) نامیده می‌شود. پس از دریافت DHCP ACK، کاربر یک بررسی نهایی پیرامون پارامترهای پیکربندی انجام داده و از مدت زمان Lease آگاه می‌شود. پس از آن، ماشین کاربر با تنظیمات دریافت‌شده از سوی سرور DHCP پیکربندی می‌گردد.

اگر کاربر متوجه شود که آدرس پیشنهاد شده از طرف سرور قبلاً به ماشین دیگری اختصاص داده شده است، یک پیام DHCP DECLINE (عدم پذیرش DHCP) برای سرور ارسال می‌کند. در صورتی که سرور DHCP با توجه به تعداد آدرس‌های موجود در پایگاه خود آدرس دیگری جهت اختصاص به کاربر در اختیار نداشته باشد قادر به ایجاد OFFER نمی‌باشد. اگر سایر سرورها نیز هیچ OFFER ای ایجاد نکنند، اختصاص آدرس IP به کاربر با شکست مواجه می‌شود.

## ۵-۲ مزایا و معایب DHCP

DHCP جهت ساده کردن مدیریت شبکه ایجاد شده است. این پروتکل از مزایای قابل توجهی برخوردار است اما اشکالاتی نیز در آن دیده می‌شود. در ادامه، این مزایا و معایب را مورد بررسی قرار می‌دهیم.

1. DHCP Acknowledgment
2. DHCP Negative Acknowledgment

## ۵-۲-۱ مزایای DHCP

مهمترین مزایای DHCP به شرح زیر می باشد:

- ♦ پیکربندی آدرس های IP برای شبکه های بسیار بزرگ را ساده می کند. به عنوان مثال اگر قرار باشد آدرس سرور DNS برای کاربران شبکه تغییر کند، مدیر شبکه لازم نیست این تغییر را در تک تک ماشین ها و بطور فیزیکی اعمال کند، بلکه کافی است آنرا از طریق سرور DHCP تغییر دهد.
- ♦ زمانی که تنظیمات پیکربندی را در یک محل (که همان سرور است) انجام می دهید، این تنظیمات به صورت خودکار میان کاربران شبکه توزیع شده و مشکلات ناشی از انجام تنظیمات اشتباه بر روی ماشین های کاربران و نیاز به رفع این اشتباهات حذف می گردد.
- ♦ به دلیل وجود مدیریت مرکزی، از هدر رفتن آدرس های IP جلوگیری می شود، زیرا این آدرس ها فقط در زمان درخواست کاربران به آنها اختصاص داده می شوند.
- ♦ پیکربندی IP در شبکه کاملاً خودکار انجام می شود. می توانید بدون نگرانی در رابطه با انتخاب آدرس IP، یک ماشین را به شبکه اضافه نموده و یا آنرا حذف کنید. به عنوان مثال زمانی که یک سرور DNS را در شبکه پیکربندی می کنید کافی است آدرس آنرا در تنظیمات سرور DHCP وارد کنید. پس از آن مشاهده خواهید نمود که این سرور بر روی کلیه کاربران پیکربندی می شود.
- ♦ به ماشین های کاربران اجازه می دهد که در محیطی به نام PXE<sup>۱</sup> اجرا شده و بتوانند آدرس های TCP/IP را از سرور DHCP دریافت کنند. کاربران PXE که کاربران "سرویس های نصب از راه دور ماکروسافت"<sup>۲</sup> یا RIS نیز نامیده می شوند، می توانند بدون نیاز به داشتن سیستم عامل بر روی کامپیوتر خود، آدرس های IP را دریافت کنند (به شبکه متصل شوند). این کار به کاربران RIS امکان می دهد تا از طریق پروتکل TCP/IP به سرور RIS متصل شده و به صورت Remote بتوانند سیستم عامل را دریافت کنند.

## ۵-۲-۲ معایب DHCP

متأسفانه، تعدادی مشکل نیز در DHCP وجود دارد که عبارتند از:

- ♦ سرور DHCP می تواند به یک مرکز شکست برای شبکه تبدیل شود. اگر در شبکه تنها یک سرور DHCP داشته باشید و این سرور در دسترس نباشد، کاربران نمی توانند از آن آدرس IP درخواست کنند.

---

1. Preboot Execution Environment  
2. Microsoft Remote Installation Services

- ♦ اگر سرور DHCP حاوی اطلاعات اشتباه باشد، این اطلاعات بطور خودکار بر روی همه کاربران آن اعمال می‌شود.
- ♦ اگر بخواهید سرور DHCP را در یک شبکه چندقسمتی<sup>۱</sup> استفاده کنید، باید برای هر قسمت یک سرور DHCP راه‌اندازی کنید؛ همچنین در صورتی که از مسیریاب<sup>۲</sup> بین دو قسمت از شبکه استفاده می‌کنید باید مطمئن شوید که مسیریاب شما قابلیت انتقال پیام‌ها از یک قسمت به قسمت دیگر را دارا می‌باشد.

### ۳-۵ فرایند DHCP Lease

فرایند DHCP Lease مراحل است که از زمان درخواست آدرس IP توسط یک کاربر تا زمان تحویل این آدرس توسط سرور DHCP باید طی شوند. این مراحل عبارتند از:

۱. DHCP discovery
۲. DHCP lease offer
۳. DHCP lease Selection
۴. DHCP lease acknowledgment

پس از پایان این مراحل، کاربر قادر خواهد بود آدرس IP و سایر تنظیمات پیکربندی که در سرور DHCP تعریف شده است را از آن دریافت کند. در ادامه این مراحل را شرح خواهیم داد.

#### ۳-۵-۱ مرحله ۱: DHCP discovery

اولین مرحله در فرایند DHCP Lease، پیدا کردن سرور DHCP می‌باشد. این مرحله زمانی اتفاق می‌افتد که کاربر DHCP برای اولین بار به شبکه متصل شده و درخواست پیکربندی آدرس IP می‌کند، و یا زمانی که یک آدرس IP درخواست می‌شود ولی در دسترس نیست.

در زمان درخواست Lease، کاربر از آدرس IP خود و آدرس سرور آگاهی ندارد بنابراین از آدرس 0.0.0.0 برای خود و 255.255.255.255 برای سرور استفاده می‌کند. پس از آن یک پیغام DHCPDISCOVER را در قالب بسته‌های UDP<sup>۳</sup> و از طریق پورت شماره ۶۸ (در مبدأ) به پورت شماره ۶۷ از مقصد می‌فرستد. این پیغام حاوی آدرس سخت افزار (MAC)<sup>۴</sup> کاربر می‌باشد. اگر این پیغام توسط سرور DHCP پاسخ داده نشود، درخواست مجدداً برای پنج بار و در فواصل زمانی ۰، ۴، ۸، ۱۶ و ۳۲ ثانیه تکرار می‌شود. اگر کاربر هنوز پاسخی دریافت نکرده باشد، از مکانیسمی به نام APIPA<sup>۵</sup> و یا از تنظیمات پیکربندی ثانویه برای ارسال پیغام‌های DHCPDISCOVER به سرور استفاده

---

1. Multisegment  
2. Router  
3. User Datagram Protocol  
4. Media Access Control Address  
5. Automatic Private IP Addressing

می‌کند. این پیغام‌ها هر پنج دقیقه یک بار فرستاده می‌شوند. با استفاده از APIPA، کاربر بجای انتظار برای دریافت پاسخ، آدرسی که فکر می‌کند مورد استفاده قرار نگرفته است را انتخاب می‌کند (این آدرس به صورت  $169.254 \times \times$  می‌باشد). با وجود اینکه پس از آن کاربر دارای آدرس IP می‌باشد، اما بازهم هر پنج دقیقه یک بار، به درخواست خود جهت اتصال به سرور DHCP ادامه می‌دهد. زمانی که سرور DHCP در دسترس قرار گرفت، کاربر آدرس خود را از آن دریافت خواهد نمود.

### ۵-۳-۲ مرحله ۲: DHCP lease offer

در مرحله دوم از فرایند DHCP Lease، هر سرور DHCP که در شبکه پیغام DHCPDISCOVER را دریافت کند، در صورت دارا بودن یک آدرس معتبر درخواست کاربر را با استفاده از یک پیغام OFFER پاسخ می‌دهد (این ویژگی به شما امکان می‌دهد که چندین سرور DHCP را در شبکه پیکربندی نموده و در صورتی که یک سرور قادر به پاسخگویی نباشد، سایر سرورها بتوانند به درخواست‌ها پاسخ دهند).

پیغام OFFER از سمت سرور به کاربر پیشنهاد می‌شود و حاوی اطلاعاتی مانند آدرس IP و معمولاً سایر اطلاعات مثل آدرس قاب زیرشبکه<sup>۱</sup>، مدت زمان Lease (به روز) و Default Gateway می‌باشد. هر پیغام OFFER فقط به یک کاربر فرستاده می‌شود و در واقع برای آن کاربر رزرو<sup>۲</sup> می‌شود، بنابراین امکان اختصاص یک آدرس به چندین کاربر وجود ندارد. این پیغام‌ها مستقیماً به آدرس سخت افزار کاربر (MAC) فرستاده می‌شوند.

### ۵-۳-۳ مرحله ۳: DHCP lease Selection

سومین مرحله از فرایند DHCP Lease زمانی آغاز می‌شود که کاربر حداقل یک OFFER دریافت می‌کند. در این مرحله، ماشین کاربر یکی از OFFERها را که معمولاً اولین OFFER دریافت شده است انتخاب می‌کند. پس از انتخاب، کاربر پیغام پذیرش (ACCEPT) که حاوی آدرس IP سرور انتخاب شده می‌باشد در شبکه ارسال (پخش) می‌کند. پخش این پیام در شبکه باعث می‌شود که سایر سرورها، OFFERهای فرستاده شده به کاربر را برای او رزرو نکنند.

### ۵-۳-۴ مرحله ۴: DHCP lease Acknowledgment

زمانی که سرور DHCP پیغام پذیرش را از طرف کاربر دریافت می‌کند، یک آدرس IP را به عنوان Lease علامت‌گذاری نموده و یک پیغام تصدیق که DHCPACK نامیده می‌شود برای کاربر ارسال می‌کند.

---

1. Subnet mask  
2. Reserve

اگر مشکلی وجود داشته باشد، سرور یک پیغام تصدیق منفی یا DHCPNACK به کاربر ارسال می‌کند. این پیغام‌ها بیشتر به دلایل زیر ایجاد می‌شوند:

- ♦ یک کاربر در حال تلاش جهت تمدید یک Lease برای آدرس IP سابق خود می‌باشد در حالی که آن آدرس به کاربر دیگری اختصاص داده شده است.
- ♦ کاربر دارای آدرس IP نادرستی می‌باشد زیرا مکان خود را بطور فیزیکی در شبکه تغییر داده است.

پیغام DHCPACK شامل همه تنظیمات مشخص شده توسط سرور DHCP به همراه آدرس IP و آدرس قاب زیر شبکه می‌باشد. زمانی که یک کاربر این پیغام را دریافت می‌کند، همه این پارامترها را در پشته IP ماشین خود یکپارچه می‌کند، درست مثل اینکه این پارامترها را به صورت دستی پیکربندی کرده باشد.

مراحل بالا اگرچه ممکن است کمی پیچیده به نظر برسند ولی وجود همگی آنها ضروری است. نتیجه فرایند DHCP Lease این است که دقیقاً یک سرور، یک آدرس IP را به یک کاربر اختصاص می‌دهد. اگر هریک از سرورهایی که پیغام‌های OFFER را ارسال می‌کنند عملکرد صحیحی نداشته باشند، به عنوان مثال سریعاً پس از درخواست یک کاربر آدرس را به او اختصاص دهند، طولی نمی‌کشد که دیگر آدرسی برای کاربران جدید وجود نداشته باشد. همچنین زمانی که یک کاربر در حال تصمیم‌گیری برای پذیرش و یا رد یک Lease می‌باشد، کاربران نمی‌توانند باعث شوند که سرور یک آدرس را به عنوان آدرس اختصاص داده نشده علامت‌گذاری نموده و سپس آنرا در جایی دیگر اختصاص دهد. این امر باعث می‌شود که به دو کاربر یک آدرس IP اختصاص داده شود.

### ۵-۳-۵ تمدید<sup>۱</sup> DHCP Lease

زمانی که یک Lease منقضی<sup>۲</sup> می‌شود و یا نیاز به تمدید دارد چه اتفاقی می‌افتد؟ هرگاه مدت Lease به بیش از نصف زمان تعریف شده می‌رسد (این زمان T1 نامیده می‌شود)، کاربر یک درخواست تمدید جدید به سرور DHCP ارسال می‌کند. اگر سرور به پیغام درخواست کاربر گوش دهد و دلیلی برای رد کردن آن وجود نداشته باشد، یک پیغام DHCPACK به کاربر ارسال می‌کند که مدت زمان Lease را Reset (بازنشانی) می‌کند. این کار مثل این است که یک راننده درخواست اجاره یک ماشین را تمدید نموده، و اجاره‌دهنده این درخواست را امضا کند.

اگر سرور DHCP در دسترس نباشد، کاربر متوجه می‌شود که امکان تمدید Lease وجود ندارد بنابراین از همان آدرس فعلی استفاده می‌کند. زمانی که ۸۷.۵ درصد از زمان Lease سپری شد (این

1. DHCP Lease Renewal

2. Expires

زمان T2 نامیده می‌شود)، کاربر درخواست تمدید دیگری به سرور ارسال می‌کند. در این نقطه زمانی، هر سرور DHCP که به پیغام درخواست گوش دهد، می‌تواند با استفاده از یک DHCPACK به کاربر پاسخ داده و Lease را تمدید کند. اگر در هر لحظه طی این پردازش، کاربر یک پیغام DHCPNACK دریافت کند باید سریعاً استفاده از آدرس IP را متوقف نموده و فرایند درخواست Lease را از ابتدا آغاز کند.

زمانی که کاربر با یک آدرس IP مقاردهی شد، در زمان‌های تعیین شده برای تمدید Lease تلاش می‌کند. در صورتی که پس از اتمام زمان Lease قصد نداشته باشد از آن استفاده کند، دیگر درخواستی جهت تمدید آن ارسال نمی‌کند. اگر کاربر قصد تمدید Lease را داشته باشد ولی قادر به انجام آن نباشد، کلیه عملکردهای مبتنی بر IP تا زمانی که یک آدرس معتبر بدست آورد متوقف خواهند شد.

### ۵-۳-۶ آزاد سازی DHCP Lease

اگرچه ممکن است درخواست تمدید Lease بارها تکرار شود اما گاهی پیش می‌آید که دیگر نیازی به استفاده از Lease نمی‌باشد و باید آدرس اختصاص داده شده به کاربر آزاد گردد. آزاد شدن Lease می‌تواند به دلیل لغو کردن آن توسط کاربر و یا سرور انجام شود. به عنوان مثال زمانی که کاربر قبل از منقضی شدن زمان Lease موفق به تمدید آن نشود، این فرایند را رها نموده و به APIPA مراجعه می‌کند. فرایند آزادسازی Lease از اهمیت زیادی برخوردار می‌باشد زیرا آدرس اشغال شده توسط سیستم را پس گرفته و به سرور تحویل می‌دهد.

### ۵-۴ آشنایی با Scopeها

اکنون که با فرایند Lease آشنا شدید، لازم است قبل از وارد شدن به بحث پیکربندی سرور DHCP، با مفاهیمی همچون Scope، Superscope، Exclusion، Reservation، Address Pool و Relay Agent آشنا شوید. در ادامه هریک از این مفاهیم را مورد بررسی قرار خواهیم داد.

#### ۵-۴-۱ Scope

Scope، محدوده‌ای پیوسته از آدرس‌های IP است. معمولاً برای هر زیرشبکه فیزیکی یک Scope وجود دارد که می‌تواند با آدرس‌های کلاس A، B، C از IPv4 و یا آدرس‌های IPv6 مقاردهی شود. سرور DHCP از این Scopeها جهت مدیریت و اختصاص آدرس‌های IP به کاربران استفاده می‌کند. هر Scope شامل مجموعه‌ای از پارامترها است که Scope option نامیده می‌شوند و می‌توانید آنها را بر روی ماشین‌های کاربران پیکربندی کنید. Scope optionها در واقع داده‌هایی که پس از اتمام فرایند درخواست آدرس، به کاربران DHCP تحویل داده می‌شوند را کنترل می‌کنند. به عنوان مثال

پارامترهایی مانند آدرس سرور DNS و آدرس Default Gateway گزینه‌هایی هستند که می‌توانند به صورت جداگانه در Scope تعریف شده و به کاربران اختصاص داده شوند.

### ۵-۴-۲ Superscope

Superscope ها به سرور DHCP اجازه می‌دهند که آدرس‌های موجود در بیش از یک Scope را برای کاربران یک زیرشبکه فیزیکی فراهم کنند. این کار زمانی مفید است که کاربران یک زیرشبکه، به بیش از یک شبکه مبتنی بر IP متصل هستند؛ بنابراین باید آدرس‌های IP خود را از بیش از یک Address Pool (حوض آدرس) بدست آورند. در کنسول مدیریت DHCP می‌توانید آدرس‌های اختصاص داده شده در Superscope را مدیریت کنید.

### ۵-۴-۳ Reservations و Exclusions

Scope ها تعیین می‌کنند که چه آدرس‌های IP می‌توانند به کاربران اختصاص داده شوند. دو روش دیگر جهت تعیین آدرس‌های اختصاص داده شده به کاربران، Exclusion و Reservation می‌باشد.

- ♦ **Exclusion:** محدوده‌ای از آدرس‌های IP است که قصد ندارید بطور خودکار به کاربران اختصاص داده شوند. این آدرس‌ها خارج از محدوده DHCP می‌باشند، بنابراین زمانی که نمی‌خواهید آدرس‌های IP مشخصی به کاربران اختصاص داده شوند می‌توانید آنها را در محدوده Exclusions تعریف کنید. آدرس‌هایی که در این محدوده تعریف می‌شوند معمولاً برای سرورها و کاربردهای ضروری در شبکه مورد استفاده قرار می‌گیرند.
- ♦ **Reservation:** محدوده‌ای از آدرس‌های IP است که می‌توانید بطور دائمی به فرایند DHCP Lease اختصاص دهید. این آدرس‌ها اساساً محدوده‌ای از آدرس‌های IP هستند که می‌توان آنها را برای تعدادی دستگاه مخصوص در شبکه رزرو کرد. اگر این دستگاه‌ها با اجرای فرایند DHCP Release (آزادسازی DHCP Lease) آدرس IP خود را به سرور تحویل دهند، پس از درخواست مجدد، همان آدرس قبلی را دریافت خواهند نمود.



آدرس‌های Exclusion زمانی استفاده می‌شوند که نخواهید یک محدوده از آدرس‌های IP در سرور DHCP استفاده شوند. آدرس‌های Reservation نیز زمانی استفاده می‌شوند که قصد داشته باشید محدوده‌ای از آدرس‌های IP را برای کاربران مشخصی اختصاص دهید تا این کاربران همیشه از آدرس‌های یکسانی استفاده کنند.

### ۴-۴-۵ Address Pool

محدوده‌ای از آدرس‌های IP است که می‌تواند در سرور DHCP مورد استفاده قرار گرفته و به کاربران یا سرورها اختصاص داده شود. فرض کنید که در یک سرور DHCP، یک Scope جدید ایجاد نموده که آدرس زیرشبکه در آن 192.168.1 می‌باشد. این Scope تعداد ۲۵۵ آدرس (از 192.168.1.1 تا 192.168.1.255) در اختیار شما قرار می‌دهد که این آدرس‌ها، Address Pool این Scope را تشکیل می‌دهند. پس از اضافه کردن این Address Pool می‌توانید به عنوان مثال آدرس‌های 192.168.1.240 تا 192.168.1.255 را به عنوان محدوده Exclusion تعریف کنید تا به کاربران اختصاص داده نشوند.

### ۵-۴-۵ DHCP Relay Agent

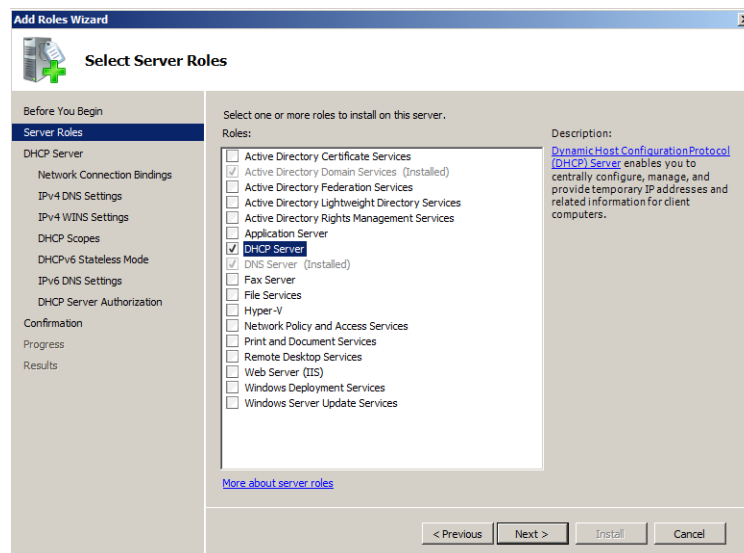
سرور DHCP، جهت برقراری ارتباط میان کاربران و سرورها در یک شبکه مبتنی بر IP طراحی شده است، اما در استانداردهای تعریف شده برای شبکه‌ها (RFC 1542) راهکارهایی جهت برقراری ارتباط میان کاربران و سرورها در شبکه‌های جداگانه که مبتنی بر IP می‌باشند ایجاد شده است. زمانی که هیچ سرور DHCP در شبکه قابل دسترسی نباشد، می‌توان با استفاده از DHCP Relay Agent (عامل تقویت‌کننده DHCP) پیغام‌های کاربران یک شبکه را دریافت نموده و آنرا به سرور DHCP منتقل نمود. Relay Agent به عنوان یک تقویت‌کننده عمل می‌کند یعنی اینکه به درخواست‌های کاربران DHCP در یک شبکه گوش داده و این درخواست‌ها را از طریق مسیریاب به سرور DHCP تحویل می‌دهد.

### ۵-۵ نصب DHCP Role

نصب DHCP با استفاده از ابزارهای جدید در ویندوز سرور 2008 و 2008R2 بسیار ساده شده است. کافی است قبل از شروع عملیات نصب، یک آدرس IP تهیه نموده و آنرا در تنظیمات TCP/IP سرور وارد کنید (آدرسی که فراهم کرده‌اید را باید به صورت دستی وارد کنید. چنانچه کارت شبکه آدرس را به صورت خودکار دریافت کند، قبل از نصب DHCP هشداری به شما داده خواهد شد). پس از وارد کردن آدرس IP می‌توانید مراحل زیر را دنبال کنید:

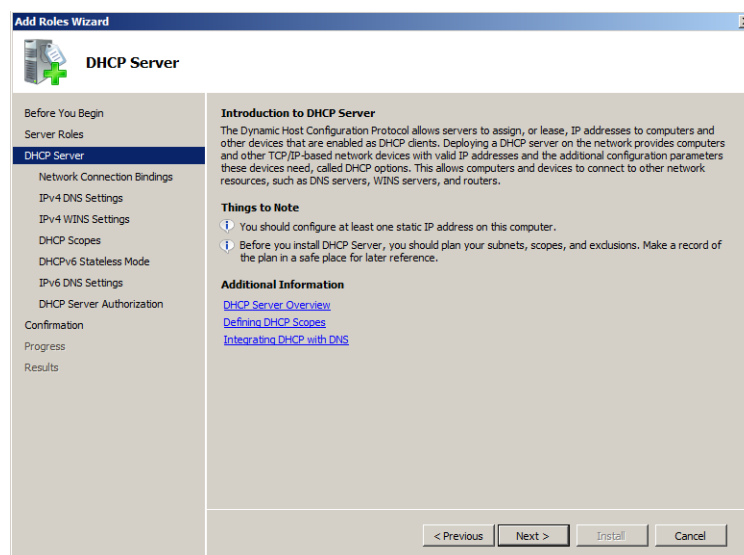
۱. کنسول Server Manager را از مسیر «Start» «Administrative Tools» «Server Manager» اجرا کنید.
۲. در قسمت Roles Summary، گزینه Add Roles را انتخاب نموده تا ویزارد «Add Roles Wizard» اجرا شود.
۳. در صفحه «Select Server Roles» گزینه DHCP Server را انتخاب نموده و بر روی Next کلیک کنید.





شکل ۵-۱

۴. در صفحه “DHCP Server”، توضیحاتی راجع به سرویس DHCP و عملکرد آن ارائه شده است. پس از مشاهده اطلاعات ارائه شده بر روی Next کلیک کنید.



شکل ۵-۲

۵. در صفحه “Select Network Connection Bindings”، Connection های مورد استفاده در سرویس DHCP را انتخاب کنید. با کلیک بر روی هر Connection، می‌توانید مشخصات آن از جمله نام و

MAC Address آنرا مشاهده کنید. پس از انتخاب Connection بروی Next کلیک کنید.

**Add Roles Wizard**

**Select Network Connection Bindings**

Before You Begin  
Server Roles  
DHCP Server  
**Network Connection Bindings**  
IPv4 DNS Settings  
IPv4 WINS Settings  
DHCP Scopes  
DHCPv6 Stateless Mode  
IPv6 DNS Settings  
DHCP Server Authorization  
Confirmation  
Progress  
Results

One or more network connections having a static IP address were detected. Each network connection can be used to service DHCP clients on a separate subnet.  
Select the network connections that this DHCP server will use for servicing clients.

IP Address	Type
<input checked="" type="checkbox"/> 192.168.1.2	IPv4

**Details**  
Name: Local Area Connection  
Network Adapter: Local Area Connection  
Physical Address: 00-0C-29-45-25-7D

< Previous   Next >   Install   Cancel

شکل ۳-۵

۶. در صفحه "Specify IPv4 DNS Server Settings" باید نام دامنه، آدرس سرور DNS اصلی و در صورت وجود، آدرس سرور DNS ثانویه را وارد کنید. پس از آن بروی Next کلیک کنید.

**Add Roles Wizard**

**Specify IPv4 DNS Server Settings**

Before You Begin  
Server Roles  
DHCP Server  
Network Connection Bindings  
**IPv4 DNS Settings**  
IPv4 WINS Settings  
DHCP Scopes  
DHCPv6 Stateless Mode  
IPv6 DNS Settings  
DHCP Server Authorization  
Confirmation  
Progress  
Results

When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of DNS servers and the parent domain name. The settings you provide here will be applied to clients using IPv4.

Specify the name of the parent domain that clients will use for name resolution. This domain will be used for all scopes you create on this DHCP server.

Parent domain:  
Bigfirm.com

Specify the IP addresses of the DNS servers that clients will use for name resolution. These DNS servers will be used for all scopes you create on this DHCP server.

Preferred DNS server IPv4 address:  
192.168.1.21   Validate

Alternate DNS server IPv4 address:  
192.168.1.22   Validate

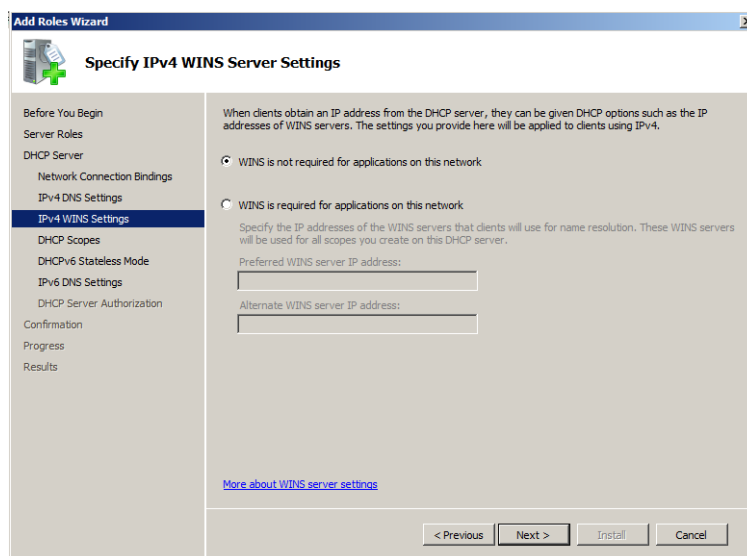
[More about DNS server settings](#)

< Previous   Next >   Install   Cancel

شکل ۴-۵

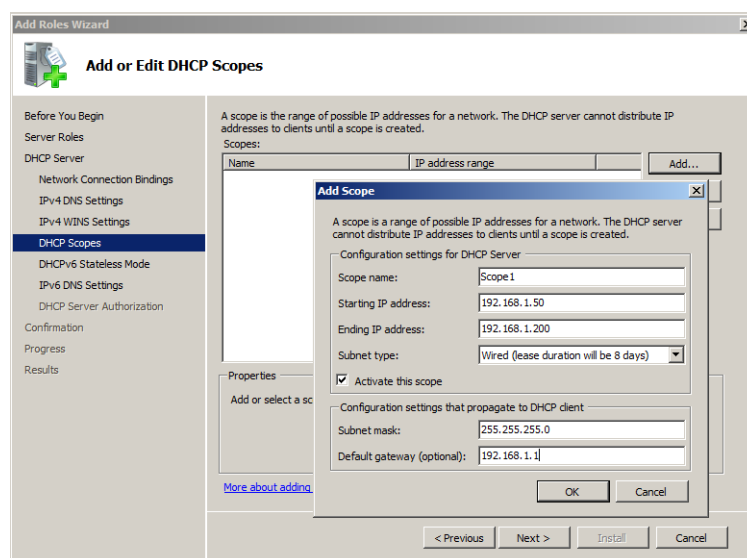
۷. در صفحه "Specify IPv4 WINS Server Settings" چنانچه از سرور WINS در شبکه استفاده

می‌کنید، با انتخاب گزینه دوم آدرس آنرا وارد نموده و در غیر اینصورت بر روی Next کلیک کنید.



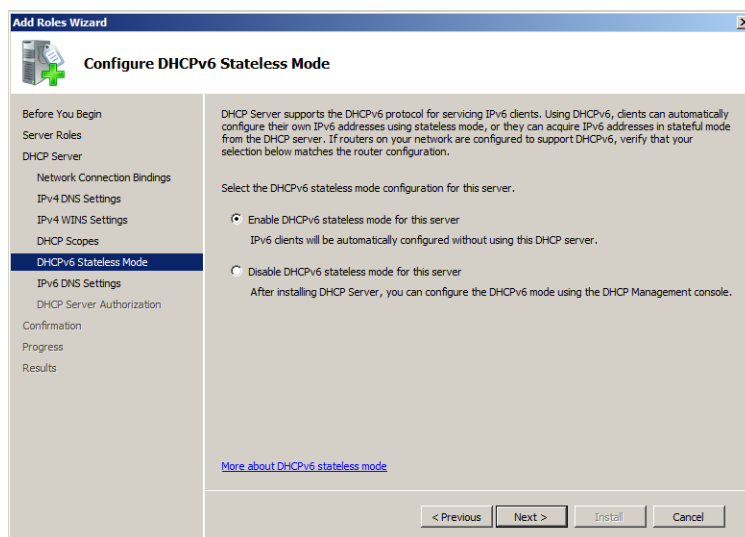
شکل ۵-۵

۸. در صفحه “Add or Edit DHCP Scopes” می‌توانید Scope های مورد نظر را ایجاد یا ویرایش کنید. جهت اضافه کردن Scope بر روی Add کلیک کنید نموده و در پنجره “Add Scope” مشخصات Scope را وارد کنید. (نام Scope، آدرس شروع و پایان، بستر ارتباطی شبکه (کابل یا بی‌سیم)، قاب زیرشبکه و Default Gateway). پس از تکمیل فیلدها بر روی OK و سپس بر روی Next کلیک کنید.



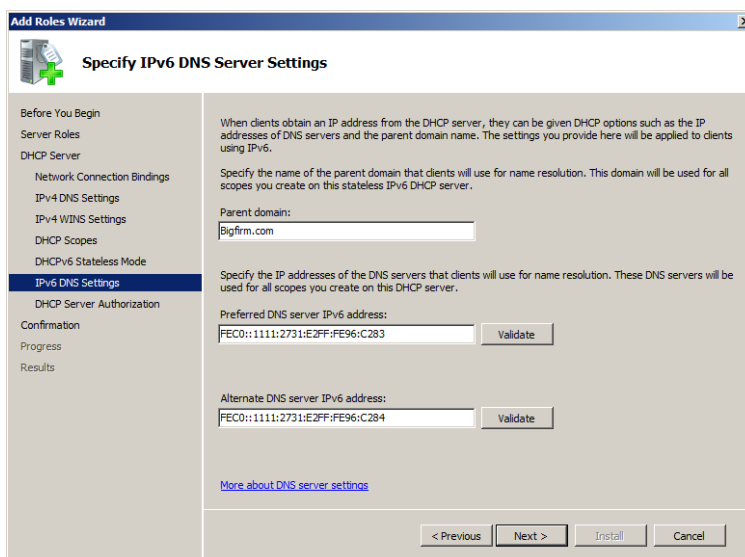
شکل ۵-۶

۹. در صفحه "Configure DHCPv6 Stateless Mode" می‌توانید تعیین کنید که امکان استفاده از آدرس‌های IPv6 وجود داشته باشد یا خیر. چنانچه قصد استفاده از IPv6 دارید گزینه "Enable DHCPv6 stateless mode" را انتخاب نموده و بر روی Next کلیک کنید.



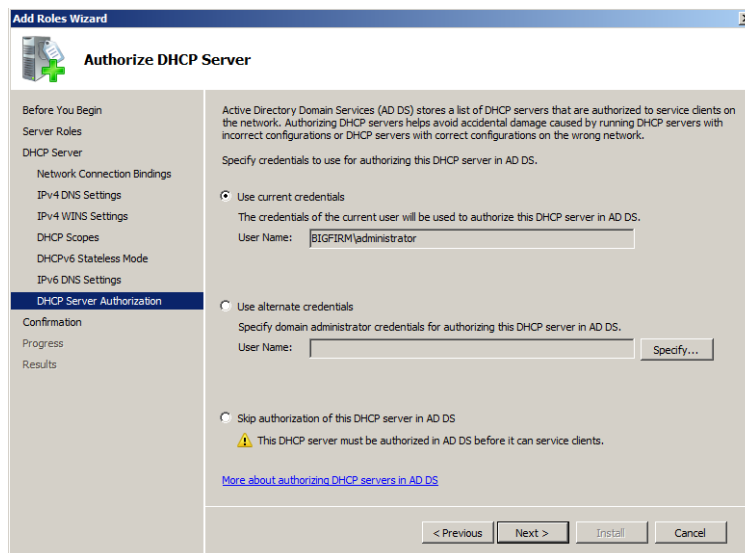
شکل ۷-۵

۱۰. در صفحه "Specify IPv6 DNS Server Settings" تنظیمات مربوط به آدرس IPv6 برای سرور DNS انجام می‌شود. آدرس IPv6 مربوط به سرور DNS را وارد نموده و بر روی Next کلیک کنید. (چنانچه آدرس IPv6 برای سرور DNS در اختیار ندارید در مرحله قبل گزینه دوم را انتخاب کنید)



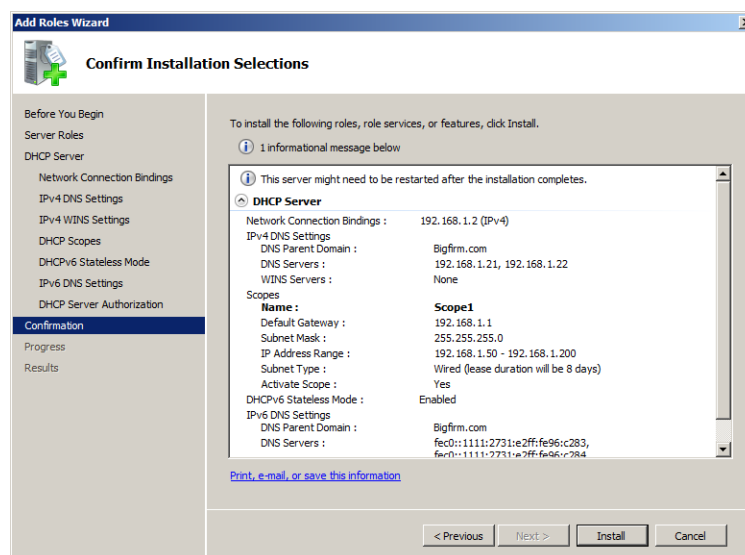
شکل ۸-۵

۱۱. در صفحه “Authorize DHCP Server” باید مدیر سرور را تعیین کنید. گزینه Use Current Credentials را انتخاب نموده و بر روی Next کلیک کنید (این گزینه کاربر فعلی که همان مدیر اصلی سرور است را به عنوان مدیر DHCP تعیین می‌کند).



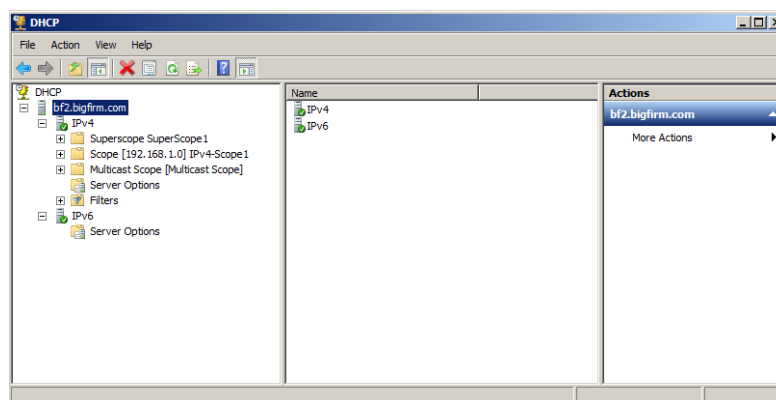
شکل ۵-۹

۱۲. در صفحه “Confirm Installation Selections” خلاصه‌ای از تنظیمات نشان داده می‌شود. پس از مشاهده این تنظیمات بر روی Install کلیک نموده و منتظر بمانید تا عملیات نصب به پایان برسد.



شکل ۵-۱۰

۱۳. پس از اتمام مراحل نصب، می‌توانید از مسیر Start « Administrative Tools » DHCP به کنسول مدیریت DHCP دسترسی پیدا کنید.



شکل ۵-۱۱

همانطور که در شکل ۵-۱۱ مشاهده می‌کنید، در پنل سمت چپ به ازای هر سرور DHCP دو قسمت IPv4 و IPv6 وجود دارد. با کلیک بروی علامت “+” در هر قسمت، گزینه‌هایی جهت ایجاد و مدیریت Scope وجود دارد. کلیه مفاهیمی که در ابتدای فصل معرفی کردیم، از این قسمت قابل دسترسی می‌باشند. در قسمت‌های بعد این موارد را مورد بررسی قرار خواهیم داد.

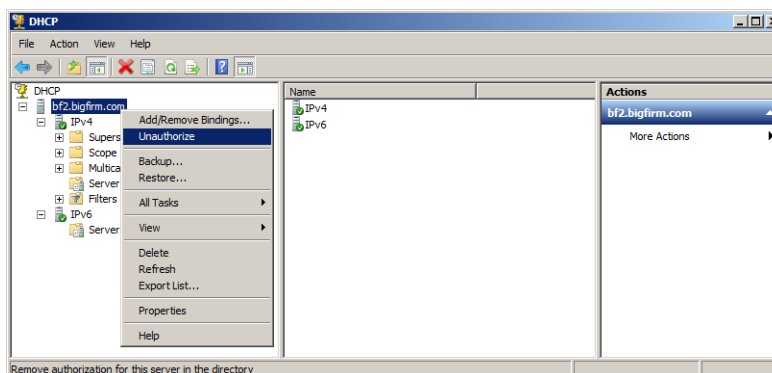
### ۵-۵-۱ DHCP Authorizing برای اکتیو دایرکتوری

DHCP Authorizing (تصویب DHCP) باعث می‌شود که این سرور در فهرست سرورهای مجاز در اکتیو دایرکتوری قرار گیرد و به کمک آن بتوانید شبکه را از دسترسی سرورهای بدون مجوز حفظ کنید. سرورهای بدون مجوز معمولاً دو مشکل در روند کار DHCP ایجاد می‌کنند: اول اینکه Lease‌های جعلی ایجاد نموده و آنرا به داخل شبکه می‌فرستند بنابراین ترافیک شبکه را افزایش می‌دهند. دوم اینکه ممکن است درخواست تمدید Lease که از طرف کاربران مجاز صادر می‌شود را باطل جلوه داده و آنها را رد کنند.

DHCP تا زمانی که برای اکتیو دایرکتوری مجاز نشده باشد نمی‌تواند به کاربران سرویس‌دهی کند. به عبارت دیگر، آدرس IP سرور DHCP باید در فهرست آدرس اشیاء مجاز در اکتیو دایرکتوری قرار داشته باشد. قبل از اینکه سرویس DHCP اجرا شود آدرس خود را در فهرست IP‌های مجاز در اکتیو دایرکتوری جستجو می‌کند، در صورتی که آدرس را پیدا نکند اجرای آن با شکست مواجه خواهد شد. تصویب یا عدم تصویب DHCP در اکتیو دایرکتوری به سادگی و با چند کلیک امکان‌پذیر می‌باشد. ابتدا با فرض اینکه سرور برای اکتیو دایرکتوری مجاز است، آنرا به حالت غیرمجاز انتقال می‌دهیم.

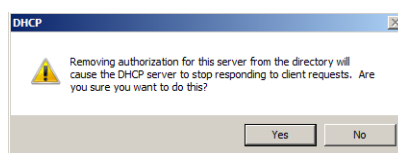
مراحل زیر را دنبال کنید:

۱. از مسیر Start « Administrative Tools » DHCP، کنسول مدیریت DHCP را اجرا کنید.
۲. بروی نام سرور کلیک راست نموده و گزینه Unauthorize را انتخاب کنید.



شکل ۵-۱۲

۳. هشداری مبنی بر متوقف شدن پاسخگویی به درخواست‌های کاربران ظاهر می‌شود. بروی Yes کلیک کنید.



شکل ۵-۱۳

۴. کمی منتظر بمانید تا عملیات انجام شود. جهت اطمینان از اجرای صحیح عملیات بار دیگر بروی نام سرور کلیک راست کنید. این بار باید بجای گزینه Unauthorize، گزینه authorize ظاهر شود.
۵. جهت Authorizing سرور نیز کافی است بروی نام سرور کلیک راست نموده و گزینه authorize را انتخاب کنید.

## ۵-۶ ایجاد و مدیریت Scope‌ها در DHCP

همانطور که قبلاً اشاره کردیم، Scope محدوده‌ای از آدرس‌های IP است که برای سرور DHCP تعریف می‌شود. در یک شبکه می‌توان چندین سرور DHCP قرار داده و برای هر کدام از آنها Scope‌هایی با تنظیمات و اطلاعات متفاوت ایجاد نمود. با این کار می‌توان شبکه را طوری پیکربندی کرد که کاربران بتوانند از سرورها و تجهیزات جداگانه‌ای استفاده کنند.

اقدامات مدیریتی زیر بروی Scope‌ها قابل انجام است:

- ♦ ایجاد Scope
- ♦ پیکربندی مشخصات Scope
- ♦ پیکربندی Exclusions و Reservations
- ♦ تنظیم Scope options
- ♦ فعال و غیرفعال کردن Scope
- ♦ ایجاد Superscope
- ♦ ایجاد Multicast Scope (Scope های چندپخش)
- ♦ یکپارچه سازی DHCP با Dynamic DNS

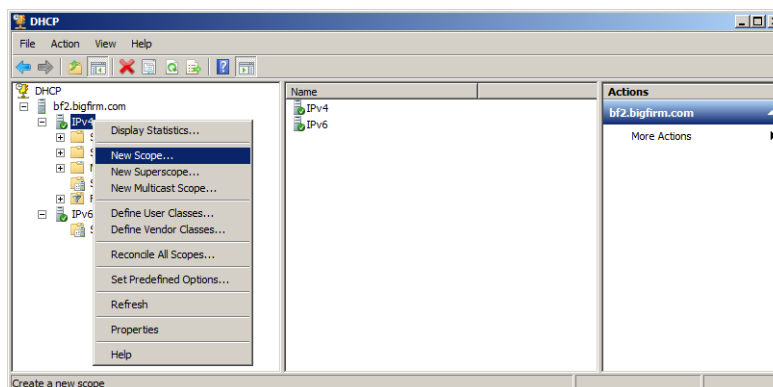
### ۵-۶-۱ ایجاد Scope در IPv4

ایجاد Scope با استفاده از ویزاردی به نام “New Scope Wizard” انجام می‌شود. اگرچه ممکن است در هنگام نصب DHCP یک Scope نیز ایجاد کرده باشید، اما گاهی اوقات داشتن یک Scope پاسخگو به نیازهای کاربران نخواهد بود. بنابراین لازم است که با توجه به شرایط بتوان Scope های جدیدی بر روی سرور ایجاد نمود. قبل از شروع کار، داشتن اطلاعاتی اضافی راجع به Scope می‌تواند کار را برایتان ساده‌تر کند. این اطلاعات عبارتند از:

- ♦ آدرس‌هایی که از لیست Address Pool مستثنی می‌کنید.
- ♦ آدرس‌هایی که برای اهداف خاصی رزرو می‌کنید.
- ♦ مقداری که باید به همراه Scope تنظیم کنید، مثل آدرس DNS، Default Gateway و ...

در اختیار داشتن این آیتم‌ها برای ایجاد Scope ضروری نیست ولی با داشتن آنها می‌توان یک Scope کامل و کارآمد ایجاد نمود. جهت ایجاد Scope مراحل زیر را دنبال کنید:

۱. در زیر نام سرور بر روی IPv4 کلیک‌راست نموده و گزینه New Scope را انتخاب کنید.



شکل ۵-۱۴



۲. در صفحه “Welcom to the New Scope Wizard” بر روی Next کلیک کنید.
۳. در صفحه “Scope Name”، نام Scope و توضیحی مختصر پیرامون آن وارد کنید.

شکل ۵-۱۵

۴. در صفحه “IP Address Range”، آدرس شروع و پایان Scope را وارد کنید. پس از وارد کردن آدرس‌ها، Subnet mask بطور خودکار محاسبه می‌شود. برای تغییر آن می‌توانید از قسمت Length تعداد بیت‌های آنرا تغییر داده تا mask مورد نظر ایجاد شود (جهت کسب اطلاعات بیشتر در مورد محاسبه Subnet nmask به فصل اول مراجعه کنید).

شکل ۵-۱۶

۵. در صفحه “Add Exclusions and Delay” می‌توانید از بین آدرس‌هایی که در مرحله قبل تعریف کرده‌اید، محدوده‌هایی را مستثنی نموده تا (با استفاده از سرویس DHCP) به کاربران و سرورها اختصاص داده نشوند. پس از وارد کردن آدرس شروع و پایان این محدوده‌ها، بر روی Add کلیک

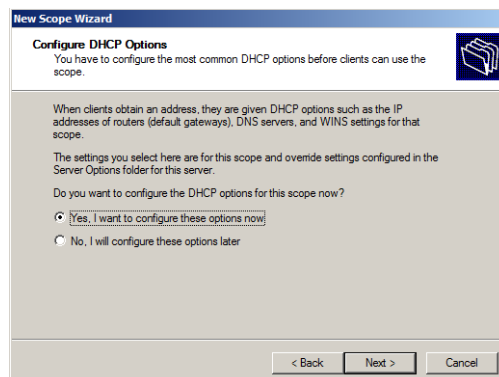
کنید تا به فهرست اضافه شوند. در این صفحه علاوه بر تعیین این محدوده‌ها می‌توانید مدت زمان تأخیر برای ارسال پیام‌های DHCP OFFER به زیرشبکه را مشخص کنید. پس از انجام تنظیمات بر روی Next کلیک کنید.

شکل ۱۷-۵

۶. در صفحه "Lease Duration" می‌توانید مدت زمان Lease (اجاره) را مشخص کنید. این زمان تعیین می‌کند که یک کاربر تا چه مدتی می‌تواند از آدرس IP استفاده کند. مقدار پیش‌فرض این زمان هشت روز است و می‌توانید آنرا برحسب روز، ساعت و دقیقه تنظیم کنید.

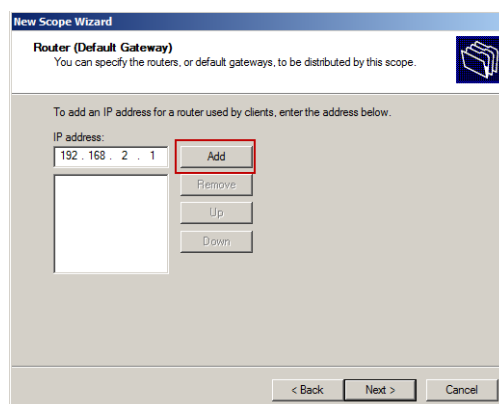
شکل ۱۸-۵

۷. در صفحه "Configure DHCP Options" جهت انجام پیکربندی DHCP Option‌ها در ادامه مراحل این ویزارد، گزینه اول (Yes, I want to configure this option now) را انتخاب نموده و بر روی Next کلیک کنید (با انتخاب گزینه دوم این تنظیمات را بعد از ایجاد Scope می‌توانید انجام دهید).



شکل ۵-۱۹

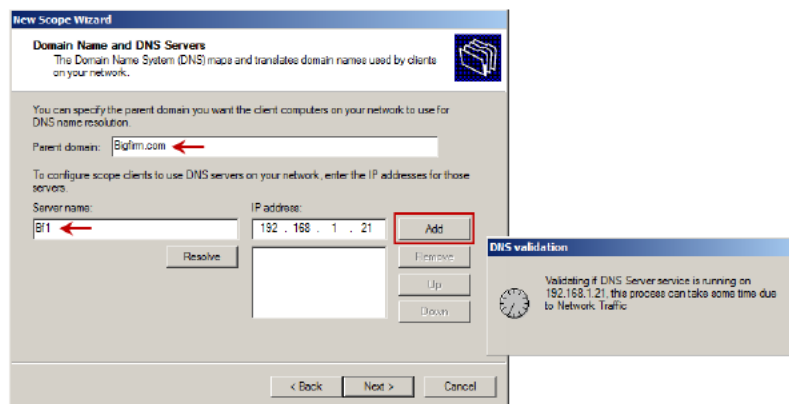
۸. در صفحه Router (Default Gateway)، آدرس Router یا Default Gateway هایی که در این Scope مورد استفاده قرار می‌گیرند را وارد کنید. پس از وارد کردن آدرس بر روی Add کلیک کنید تا به فهرست اضافه شود. با استفاده از دکمه‌های Up و Down نیز می‌توانید ترتیب و اولویت آنها را تعیین کنید. پس از انجام عملیات بر روی Next کلیک کنید.



شکل ۵-۲۰

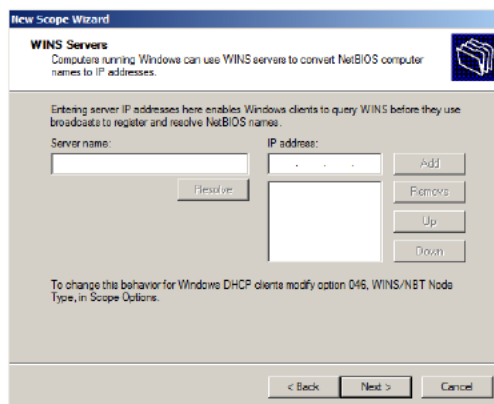
۹. در صفحه "Domain Name and DNS Servers" باید تنظیمات مربوط به نام دامنه و سرور DNS را انجام دهید. در قسمت Parent domain نام دامنه‌ای که کاربران از سرور DNS آن استفاده می‌کنند (در اینجا Bigfirm.com) را وارد کنید. در قسمت Server name و IP address نیز نام و آدرس IP سرور DNS را وارد نموده و بر روی Add کلیک کنید. پس از کلیک بر روی Add، سرور اعتبارسنجی شده و در صورت وجود به فهرست اضافه می‌گردد. چنانچه سروری با آن آدرس وجود نداشته باشد، پیغامی ظاهر شده و اعلام می‌کند که سرور وجود ندارد. با کلیک بر روی Yes

می‌توانید آنرا به فهرست اضافه کنید. پس از انجام تنظیمات بر روی Next کلیک کنید.



شکل ۵-۲۱

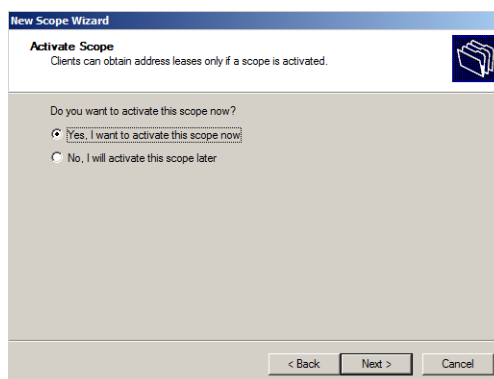
۱۰. چنانچه در شبکه از سرور WINS استفاده می‌کنید، در صفحه "WINS Servers" نام و آدرس IP آنرا وارد نموده و بر روی Add کلیک کنید (چنانچه چنین سروری ندارید بر روی Next کلیک کنید).



شکل ۵-۲۲

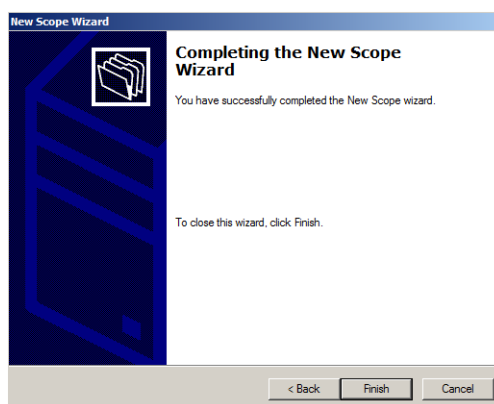
سرویس WINS (Windows Internet Name Service)، یک سرویس مبتنی بر پروتکل NetBIOS است که در ویندوزهای قبل از 2000 به کار گرفته می‌شود و تقریباً دارای عملکردی مشابه با DNS می‌باشد. در شبکه‌های مبتنی بر DNS، نام کامپیوترها در یک دامنه باید منحصر بفرد باشد ولی در کل شبکه می‌توان دو کامپیوتر با نام یکسان در اختیار داشت. به عنوان مثال، نام Ec1 می‌تواند در دو دامنه Bigfirm.com و Littlefirm.com یکسان باشد در حالی که در سرویس WINS تنها یک کاربر با نام Ec1 می‌تواند وجود داشته باشد. این سرویس برای شبکه‌های کوچک ممکن است مناسب باشد اما در شبکه‌های بزرگ و مخصوصاً اینترنت، استفاده از آن پیشنهاد نمی‌گردد.

۱۱. پس از پایان تنظیمات، در صفحه Active Scopes می‌توانید فعال یا غیرفعال بودن Scope را تعیین نمایید. گزینه اول را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۵-۲۳

۱۲. در صفحه "Completing the New Scope Wizard" بر روی Finish کلیک کنید.



شکل ۵-۲۴

### ۵-۶-۲ ایجاد Scope در IPv6

اکنون که با نحوه ایجاد Scope در IPv4 آشنا شدید، قصد داریم نحوه ایجاد آنرا در IPv6 نشان دهیم. جهت ایجاد Scope مراحل زیر را دنبال کنید:

۱. در زیر نام سرور بر روی IPv6 کلیک راست نموده و گزینه New Scope را انتخاب کنید.
۲. در صفحه "Welcom to the New Scope Wizard" بر روی Next کلیک کنید.
۳. در صفحه "Scope Name"، نام Scope و توضیحی مختصر پیرامون آن وارد نموده و بر روی Next کلیک کنید.

شکل ۵-۲۵

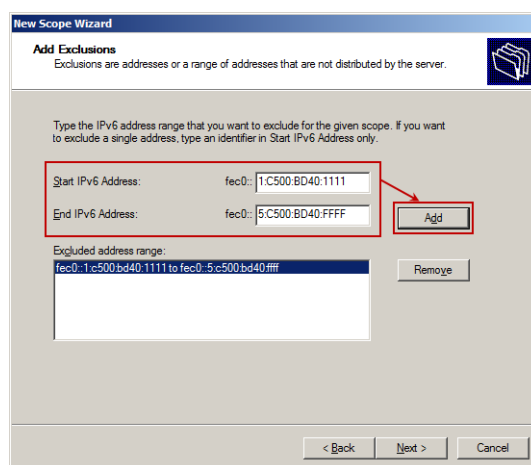
۴. در صفحه “Scope Prefix” باید پیشوند آدرس‌های IPv6 را وارد کنید. در فصل اول گفتیم که آدرس‌های IPv6 به چند نوع تقسیم شده و هر نوع با پیشوند خاصی شروع می‌شود. تعدادی از این پیشوندها عبارتند از:

- ♦ 2000::/3 برای آدرس‌های global unicast (قابل استفاده در اینترنت)
- ♦ FE80::/64 برای آدرس‌های Link-local unicast (استفاده در ارتباطات نقطه به نقطه)
- ♦ FEC0::/64 برای آدرس‌های Site-local unicast (قابل استفاده در محدوده یک سایت-معادل با آدرس‌های خصوصی در IPv4)
- ♦ FF00 تا FFFF برای آدرس‌های Multicast (استفاده در چندپخش)

در اینجا از پیشوند FEC0::1 یا FEC0:0:0:1 استفاده شده است (چون آدرس‌های IPv6 از هشت قسمت ۱۶ بیتی تشکیل شده‌اند و در این پیشوند چهار قسمت مقداردهی شده است، چهار قسمت بعدی برای تعیین آدرس‌های ماشین‌ها تغییر می‌کند). دقت داشته باشید که از قسمت Preference نیز می‌توانید اولویت این Scope را تعیین کنید.

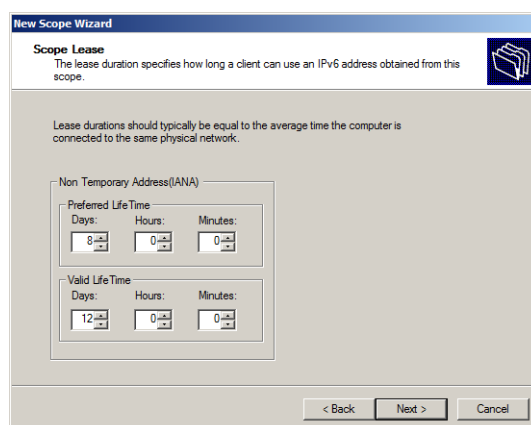
شکل ۵-۲۶

۵. در صفحه “Add Exclusions” می‌توانید محدوده‌ای از آدرس‌های IP را که نمی‌خواهید در سرویس DHCP استفاده شود، تعیین نمایید. آدرس شروع (در اینجا FEC0::1:C500:BD40:1111) و پایان (در اینجا FEC0::1:C500:BD40:FFFF) را وارد نموده و بر روی Add کلیک کنید تا به فهرست اضافه شوند. پس از آن بر روی Next کلیک کنید (دقت داشته باشید که در شکل ۵-۲۷ سه قسمت اول آدرس‌ها \_FEC0::\_ بطور پیش‌فرض در نظر گرفته شده‌اند و شما باید قسمت‌های بعدی را وارد کنید)



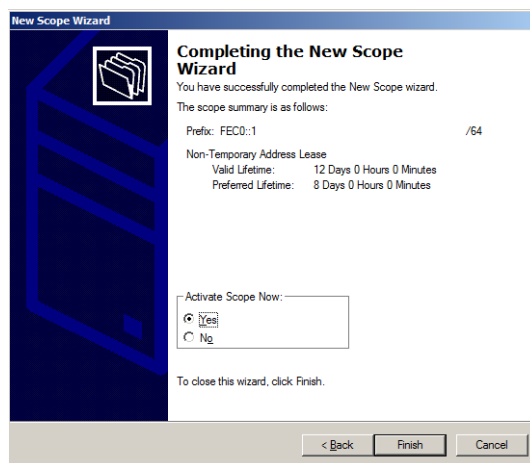
شکل ۵-۲۷

۶. در صفحه “Scope Lease” باید مدت زمان Lease (مدت زمان استفاده از آدرس IP توسط ماشین‌ها) را تعیین کنید. تنظیمات لازم را انجام داده و بر روی Next کلیک کنید.



شکل ۵-۲۸

۷. در صفحه "Completing the New Scope Wizard" پس از مشاهده خلاصه‌ای از تنظیمات می‌توانید فعال یا غیرفعال بودن Scope را تعیین کنید. در قسمت Active Scope Now گزینه Yes را انتخاب نموده و بر روی Finish کلیک کنید.



شکل ۵-۲۹

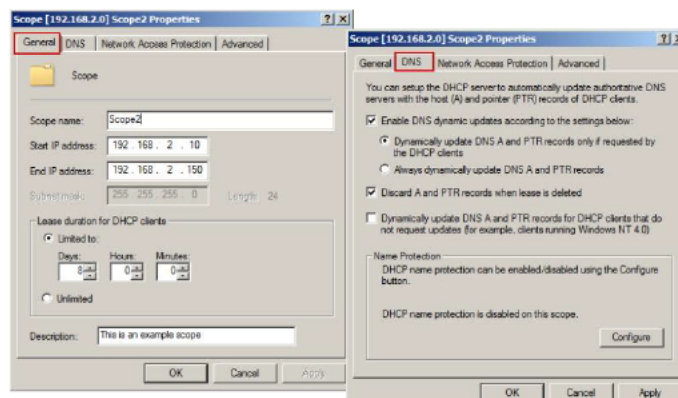
### ۵-۶-۳ تغییر مشخصات Scopeها

هر Scope شامل مجموعه‌ای از مشخصات است که با آن همراه شده‌اند. جهت دسترسی به مشخصات هر Scope می‌توانید بر روی نام آن کلیک راست نموده و Properties را انتخاب کنید. پنجره Scope Properties (بسته به نوع Scope) شامل تب‌هایی مانند General، DNS، Lease است که با استفاده از آنها می‌توانید تنظیمات Scopeها را تغییر دهید. تعدادی از مهمترین این تنظیمات در ادامه معرفی شده است:

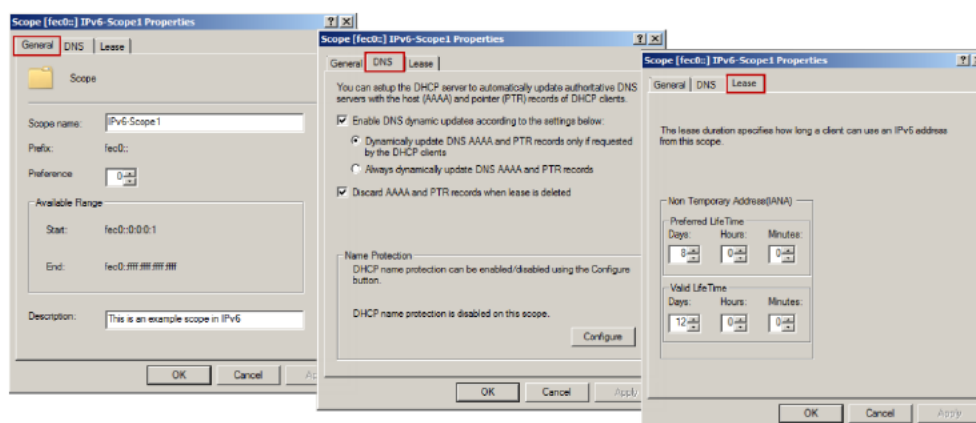
- ♦ Scope name: نام Scope را مشخص می‌کند.
- ♦ Start IP Address و End IP Address: آدرس‌های شروع و پایان Scope هستند که در حین ایجاد Scope آنها را تعیین کرده‌اید. می‌توانید آدرس‌های جدیدی در این فیلدها وارد نموده و محدوده آدرس‌ها را تغییر دهید.
- ♦ Lease duration for DHCP client: در Scopeهای IPv4، تنظیمات این قسمت مشخص می‌کنند که یک Lease چه مدت دارای ارزش می‌باشد. در Scopeهای IPv6 تب جداگانه‌ای جهت انجام تنظیمات Lease وجود دارد.
- ♦ Enable DNS dynamic update: با استفاده از این گزینه و آپشن‌های آن امکان انجام تنظیماتی پیرامون فعال‌سازی Dynamic DNS و رکوردهای Host و PTR فراهم گردیده است.



در شکل‌های ۳۰-۵ و ۳۱-۵ پنجره Scope Properties برای IPv4 و IPv6 نشان داده شده است.



شکل ۳۰-۵: IPv4 Scope Properties



شکل ۳۱-۵: IPv6 Scope Properties

زمانی که مشخصات یک Scope را تغییر می‌دهید، این تغییرات بر روی Lease که در حال اجرا می‌باشد تاثیری نمی‌گذارد. به عنوان مثال فرض کنید که یک Scope از آدرس 172.30.1.1 تا آدرس 172.30.1.199 در اختیار دارید و کاربران در حال استفاده از آن هستند. پس از انجام تغییرات، محدوده آدرس‌های این Scope را به 172.30.1.1 تا 172.30.1.150 تغییر می‌دهید. حال اگر کاربری از آدرس 172.30.1.180 که جزئی از Scope، قبل از تغییر می‌باشد استفاده کند، کاربر این آدرس را تا زمانی که اعتبار Lease به پایان نرسیده باشد استفاده خواهد کرد ولی قادر به تمدید آن نمی‌باشد.

## ۷-۵ Exclusion و Reservation

پس از تعریف Address Pool برای Scope، ممکن است نیاز به ایجاد آدرس‌های Reservation (رزرو) و Exclusion (مثثنی) داشته باشید. در نظر گرفتن این آدرس‌ها موجب کاهش تعداد کل آدرس‌های مورد استفاده توسط سرویس DHCP می‌گردد. در ادامه، نحوه افزودن و یا حذف کردن آدرس‌های Exclusion و Reservation را شرح خواهیم داد.

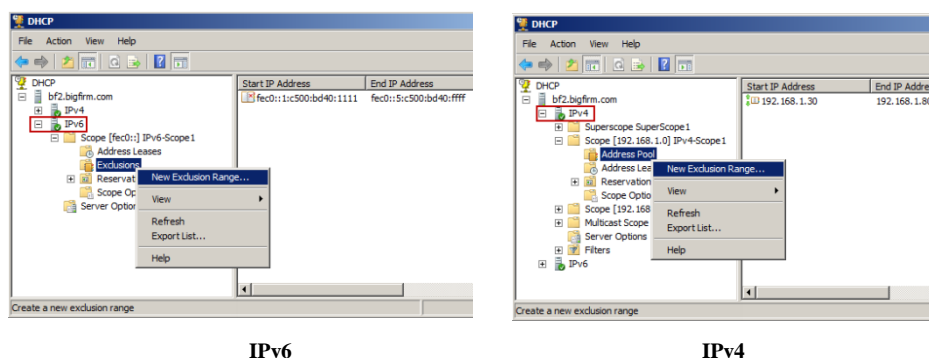
### ۷-۵-۱ افزودن و حذف کردن Exclusions

زمانی که قصد دارید محدوده‌ای از آدرس‌ها را از سرویس DHCP حذف کنید، باید آنها را به لیست آدرس‌های Exclusion اضافه کنید. بهتر است این کار قبل از فعال کردن یک Scope انجام شود مانع از اختصاص این آدرس‌ها به کاربران شده و بنابراین در زمان تمدید Lease با مشکلی مواجه نخواهند بود.

#### افزودن Exclusions

جهت افزودن آدرس‌ها به لیست Exclusions مراحل زیر را دنبال کنید:

۱. در کنسول مدیریت DHCP، نوع Scope مورد نظر جهت تعیین Exclusions را انتخاب کنید (IPv4 یا IPv6).
۲. برای Scope‌های IPv4، بر روی Address Pool کلیک‌راست نموده و گزینه New Exclusion Range را انتخاب کنید. برای IPv6 این گزینه با کلیک‌راست بر روی Exclusions قابل دسترسی می‌باشد.



شکل ۳۲-۵

۳. با مشاهده پنجره "Add Exclusion"، آدرس‌های شروع و پایان Exclusion را وارد نموده و بر روی Add کلیک کنید.

IPv6

IPv4

شکل ۳۳-۵

۴. پس از اتمام کار می‌توانید با کلیک برروی قسمت Exclusion در IPv4 یا IPv6 این آدرس‌ها را مشاهده کنید.

#### حذف Exclusions

جهت حذف یک Exclusion کافی است برروی آن کلیک راست نموده و Delete را انتخاب کنید. پس از حذف، آدرس‌هایی که در این دامنه قرار دارند بلافاصله به آدرس‌های قابل دسترسی افزوده می‌شوند.

#### ۵-۷-۲ افزودن و حذف کردن Reservation

زمانی که قصد دارید یک دستگاه همیشه از آدرس IP یکسانی استفاده کند می‌توانید آنرا به فهرست Reservation اضافه کنید. این روش جهت سهولت دسترسی به ماشین‌های پرکاربرد و مهم در شبکه استفاده شده و بیشتر جهت اختصاص آدرس IP به دستگاه‌هایی مانند سرورها، پرینتر و ... به کار می‌رود.

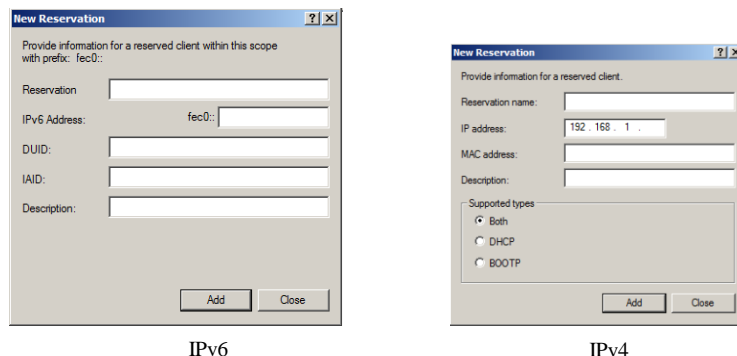
#### افزودن Reservation

اضافه کردن Reservation بسیار ساده است. کافی است آدرس سخت افزار یک دستگاه (MAC Address) و یا شناسه آن را در اختیار داشته و مطابق مراحل زیر اقدام کنید:

۱. Scope مورد نظر را انتخاب کنید.
۲. برروی Reservations کلیک راست نموده و گزینه New Reservation را انتخاب کنید.
۳. در پنجره "New Reservation" آدرس سخت افزار (MAC) یا شناسه آنرا به همراه آدرس IP که قصد دارید به آن اختصاص دهید وارد کنید (شکل ۵-۳۴).



برای پیدا کردن آدرس MAC می‌توانید از دستور ipconfig در خط فرمان استفاده کنید. چنانچه قصد دارید آدرس MAC را برای یک ماشین Remote (راه دور) پیدا کنید، می‌توانید از دستور nbtstat -a computername استفاده کنید (بجای computername نام ماشین مورد نظر را وارد نمایید).



شکل ۳۴-۵

۴. در صورت تمایل می‌توانید نام و توضیحی نیز راجع به Reservations وارد کنید.
۵. برای IPv4 می‌توانید از قسمت Supported Types تعیین کنید که انجام رزرو برای DHCP، BOOTP (قابل استفاده برای دستگاه‌های Remote) و یا هر دو باشد.

### حذف Reservation

جهت حذف یک Reservation کافی است بر روی آن کلیک راست نموده و گزینه Delete را انتخاب کنید. دقت داشته باشید که حذف Reservation تاثیری بر ماشین کاربر نخواهد داشت.

## ۵-۸ تنظیمات Scope Options برای IPv4

پس از راه اندازی سرور DHCP، تصویب<sup>۱</sup> آن در اکتیو دایرکتوری، و ایجاد Scope، نوبت به انجام تنظیمات Scope Options می‌رسد. تنظیمات مربوط به Option ها، امکاناتی جهت دسترسی کاربران به یکدیگر و یا به سرورها فراهم می‌کنند. این تنظیمات شامل مواردی مانند تنظیم DNS، Default Gateway و ... می‌باشند. تنظیمات Scope Option باید قبل از فعال‌سازی یک Scope پیکربندی شوند زیرا ثبت کاربران در Scope بدون استفاده از این Option ها عملاً کاری بی‌فایده می‌باشد. Scope Options به همراه آدرس IP و قاب زیرشبکه که در قسمت‌های قبل پیکربندی نمودید، تنظیمات TCP/IP را برای کاربران تکمیل خواهند نمود. در ادامه نحوه پیکربندی Option ها بر روی سرور DHCP را شرح خواهیم داد.

### ۵-۸-۱ آشنایی با سطوح تخصیص Option ها

Option های DHCP در پنج سطح قابل اختصاص به میزبان‌های شبکه می‌باشند:

1. Authorizing

### Predefined Options

Predefined Options، الگوهایی<sup>۱</sup> هستند که بطور پیش فرض در پنجره‌های مربوط به Option‌های Server، Scope و Client تنظیم شده‌اند.

### Server Options

این Option‌ها به کلیه Scope‌ها و کاربران یک سرور اختصاص داده می‌شوند. این بدان معناست که بهترین روش برای اختصاص یک Option به همه کاربران (یک سرور)، بدون توجه به Scope‌ها استفاده از تنظیمات سطح سرور می‌باشد.

### Scope Options

اگر قصد دارید Option‌هایی را به کاربران یک زیرشبکه اختصاص دهید، بهترین گزینه استفاده از تنظیمات سطح Scope می‌باشد. به عنوان مثال یکی از کارهای رایج در شبکه‌ها این است که تعدادی مسیریاب را برای زیرشبکه‌های فیزیکی متفاوت مشخص می‌کنند. حال اگر شما به ازای یک زیرشبکه دو Scope داشته باشید می‌توانید به هرکدام از Scope‌ها آدرس یکی از مسیریاب‌ها را اختصاص دهید، بنابراین کاربران زیرشبکه می‌توانند از هر دو مسیریاب استفاده کنند.

### Class Options

Option‌های سطح Class می‌توانند به کاربران متفاوتی در شبکه اختصاص داده شوند. همیشه کاربران شبکه از سیستم‌های مشابهی استفاده نمی‌کنند، به عنوان مثال ممکن است کاربران از ویندوزهای 2000، XP، Vista، Server 2003، Server 2008 و 2008R2 استفاده نمایند که Option‌های تحت پوشش این سیستم‌عامل‌ها (در DHCP)، برای سیستم‌عامل‌های Windows 98، Windows NT و Mac OS ناشناخته هستند (و برعکس). با تعریف کلاس‌های نوع Windows 2000 یا Windows 98 می‌توانید این Option‌ها را دسته‌بندی نموده و با توجه به نوع کاربران به آنها اختصاص دهید.

### Client Options

این option‌ها می‌توانند در سطح کاربر اختصاص داده شوند. به عنوان مثال زمانی که کاربران از آدرس‌های رزرو شده استفاده می‌کنند، می‌توانید Option‌هایی را به این آدرس‌ها پیوست نموده و به کاربران اختصاص دهید. تنظیمات سطح کاربر، کلیه تنظیمات سطح Server، Class و Scope را لغو می‌کنند.



Option‌های سطح پایین (مثل سطح کاربر) می‌توانند Option‌های سطوح بالاتر را لغو کنند. به عبارت دیگر اگر کاربران را با استفاده از Option‌های سطوح بالا تنظیم نموده، سپس بروی تعدادی از آنها Option‌های سطح پایین را پیکربندی کنید، تنظیمات قبلی لغو خواهند شد. ترتیب لغو شدن Option‌ها بصورت روبرو می‌باشد: Client Options « Class Options « Scope Options « Server Options

## ۵-۸-۲ اختصاص Option ها

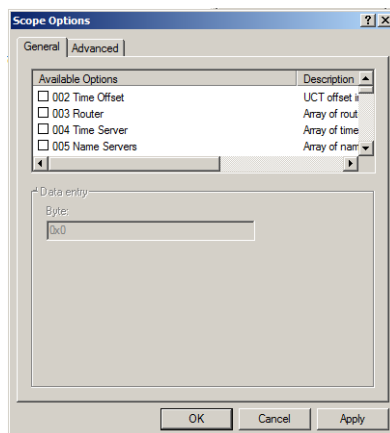
با استفاده از کنسول مدیریت DHCP می‌توانید Option ها را به Scope، سرور، آدرس‌های رزرو شده و یا کلاس‌ها اختصاص دهید. روش انجام کار در همه سطوح یکسان است و تنها تفاوت آن در محلی است که Option اختصاص داده می‌شود.

زمانی که یک Option را اختصاص می‌دهید بخاطر داشته باشید که این Option به همه کاربران در آن سرور یا Scope اختصاص داده می‌شود. این Option ها قابل انتقال از یک Scope و یا سرور به دیگری نمی‌باشند.

### ایجاد و اختصاص یک Option جدید

جهت ایجاد و اختصاص یک Option مراحل زیر را دنبال کنید:

۱. ابتدا سطح اختصاص Option را تعیین کنید:
  - ♦ جهت اختصاص Option به سرور، بر روی آن کلیک کنید تا زیرشاخه‌های آن نمایش داده شوند. در فهرست زیرشاخه‌ها، بر روی آیتم Server Options کلیک‌راست نموده و گزینه Configure Options را انتخاب کنید.
  - ♦ جهت اختصاص Option به Scope، بر روی آن کلیک نموده و از بین آیتم‌های موجود، Scope Options را انتخاب کنید. بر روی Scope Options کلیک‌راست نموده و گزینه Configure Options را انتخاب کنید.
  - ♦ جهت اختصاص Option به آدرس‌های Reservation نیز بر روی Reservation کلیک‌راست نموده گزینه Configure Options را انتخاب کنید.
۲. پس از انتخاب گزینه موردنظر، پنجره Server/Scope/Reservation Options نمایش داده می‌شود. در این پنجره تمام Option های قابل اختصاص فهرست شده است.



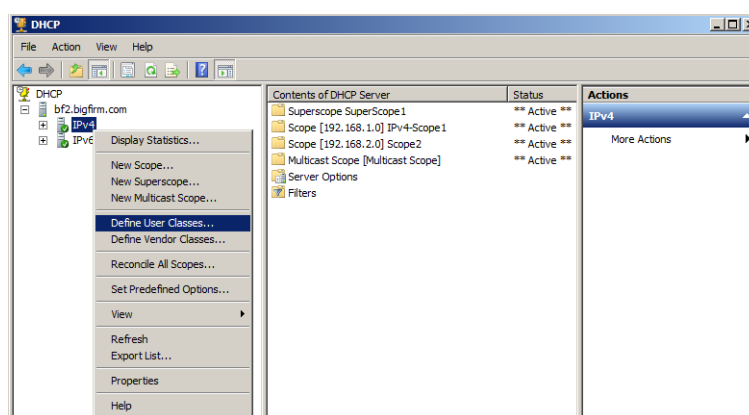
شکل ۵-۳۵

۳. جهت انتخاب یک Option، تیک مربوط به آن را فعال نموده و از قسمت پایین پنجره (Data Entry) مقادیر مورد نظر را اختصاص دهید. در نهایت بر روی OK کلیک کنید.

### ۵-۸-۳ پیکربندی سرور DHCP برای کلاس‌ها

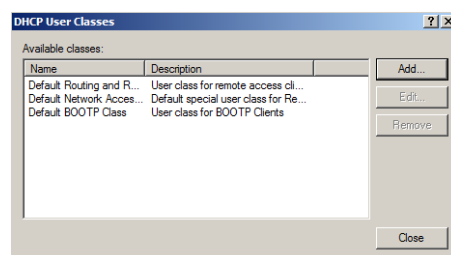
با استفاده از Class، مدیر شبکه می‌تواند کاربران را گروه‌بندی نموده و Option‌های یکسانی روی کامپیوترهای هر گروه اعمال کند. در این قسمت قصد داریم نحوه ایجاد کلاس در سرور DHCP و همچنین اختصاص Option‌ها به آنرا شرح دهیم. برای انجام این کار مراحل زیر را دنبال کنید:

۱. از مسیر «Start» «Administrative Tools» DHCP، کنسول مدیریت DHCP را اجرا کنید.
۲. بر روی آیتم IPv4 کلیک‌راست نموده و گزینه Define User Classes را انتخاب کنید.



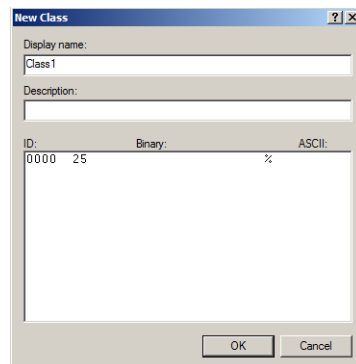
شکل ۳۶-۵

۳. در پنجره “DHCP User Classes”، بر روی دکمه Add کلیک کنید.



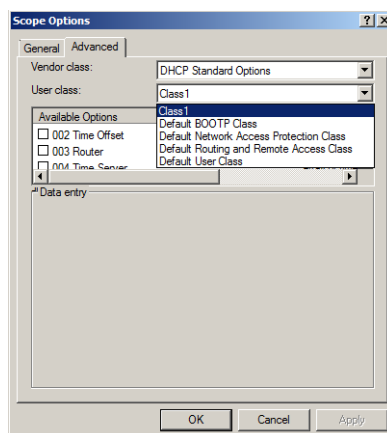
شکل ۳۷-۵

۴. در پنجره New Class، از قسمت Display Name و ID، نام و شناسه کلاس را وارد نموده و بر روی OK کلیک کنید. همچنین می‌توانید از قسمت Description توضیحاتی نیز راجع به آن ارائه دهید.



شکل ۵-۳۸

۵. پس از کلیک بر روی OK، کلاسی که ایجاد نموده‌اید در پنجره "DHCP User Classes" نشان داده می‌شود. بر روی Close کلیک کنید.
۶. در کنسول مدیریت DHCP، بر روی Scope Options کلیک راست نموده و گزینه Configure Options را انتخاب کنید.
۷. در تب Advanced و از قسمت User Class، کلاسی که تعریف نمودید را انتخاب کنید.



شکل ۵-۳۹

۸. Option‌های مورد نظر را به کلاس اختصاص داده و در نهایت بر روی OK کلیک کنید.
- جهت اختصاص شناسه کلاس به کاربران می‌توانید از دستور ipconfig به همراه پارامتر /setclassid استفاده کنید. این دستور به صورت زیر می‌باشد:

```
Ipconfig /setclassid <adapter name> <Class ID>
```



چنانچه بر روی یک کامپیوتر از چندین کارت شبکه استفاده می‌کنید، جهت اختصاص ID یکسان به آنها می‌توانید از دستور زیر استفاده کنید:

```
Ipconfig /setclassid * <Class ID>
```

همچنین در صورتی که قصد دارید به کارت‌های شبکه‌ای که نام آنها با عبارت خاصی آغاز می‌شود ID اختصاص دهید، آن عبارت را به همراه یک ستاره (\*)، و چنانچه شامل عبارت خاصی می‌باشد آن عبارت را بین دو ستاره به صورت زیر وارد کنید:

```
rem start name with "Local"
Ipconfig /setclassid Local* <Class ID>
```

```
rem name Include "Con"
Ipconfig /setclassid *Con* <Class ID>
```

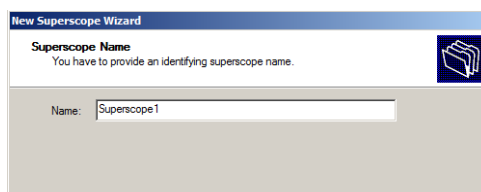
## ۹-۵ ایجاد و حذف Superscope در IPv4

Superscope، به سرور DHCP اجازه می‌دهد که آدرس‌های چندین زیرشبکه منطقی را در اختیار کاربران یک شبکه فیزیکی قرار دهد. ایجاد Superscope با استفاده از گزینه New Superscope در کنسول مدیریت DHCP انجام می‌شود.

### ۹-۵-۱ ایجاد یک Superscope

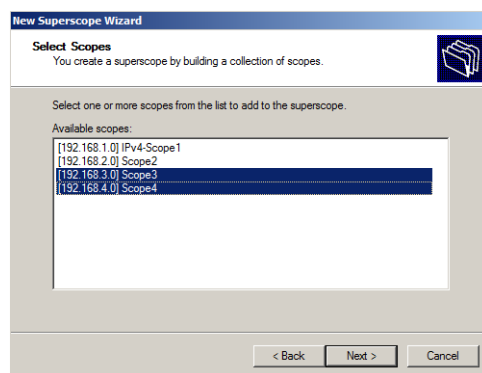
جهت ایجاد Superscope مراحل زیر را دنبال کنید:

۱. کنسول مدیریت DHCP را از مسیر «Start» «Administrative Tools» DHCP اجرا کنید.
۲. با استفاده از گزینه New Scope (قسمت ۵-۶-۱) دو Scope با محدوده‌های 192.168.3.2 تا 192.168.3.127 و 192.168.4.2 تا 192.168.4.127 ایجاد کنید.
۳. بر روی IPv4 کلیک‌راست نموده و گزینه New Superscope را انتخاب کنید.
۴. در صفحه «Welcom to the New Superscope Wizard» بر روی Next کلیک کنید.
۵. در صفحه «Superscope Name» نام Superscope را وارد نموده و بر روی Next کلیک کنید.



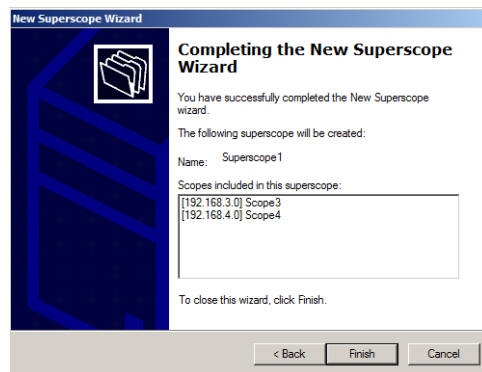
شکل ۴۰-۵

۶. در صفحه Select Scopes لیست Scope های موجود نشان داده شده است. دو Scope که ایجاد کردید را انتخاب نموده و بر روی Next کلیک کنید.



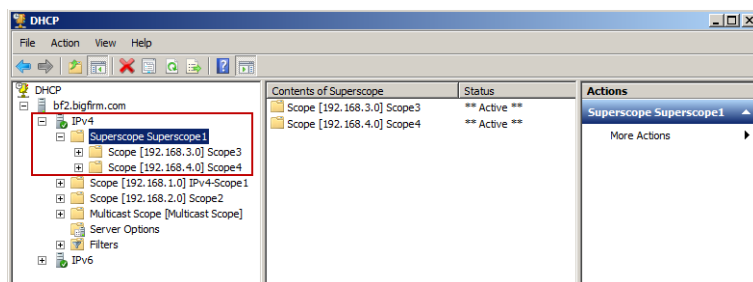
شکل ۴۱-۵

۷. در صفحه "Completing the New Super Scope Wizard" خلاصه ای از تنظیمات انجام شده نشان داده می شود. بر روی Finish کلیک کنید.



شکل ۴۲-۵

۸. در کنسول مدیریت DHCP می توانید Superscope که ایجاد نموده اید را مشاهده کنید.



شکل ۴۳-۵

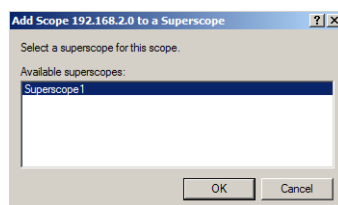
### حذف Superscope

جهت حذف یک Superscope، بر روی آن کلیک راست نموده و گزینه Delete را انتخاب کنید. دقت داشته باشید که حذف یک Superscope تأثیری بر Scope های اصلی ندارد.

### ۵-۹-۲ افزودن Scope به Superscope

جهت افزودن Scope به یک Superscope مراحل زیر را دنبال کنید:

۱. بر روی Scope مورد نظر کلیک راست نموده و گزینه Add to Superscope را انتخاب کنید.
۲. لیست تمام Superscope های شناخته شده برای سرور نشان داده می شود. Superscope مورد نظر را انتخاب نموده و بر روی OK کلیک کنید.



شکل ۵-۴۴

### حذف Scope از Superscope

جهت حذف Scope از یک Superscope، در زیرمجموعه Superscope بر روی Scope مورد نظر کلیک راست نموده و گزینه Remove From Superscope را انتخاب کنید.

### ۵-۹-۳ فعال و غیرفعال کردن Superscope

جهت فعال سازی یا غیرفعال کردن یک Scope و یا Superscope، بر روی آن کلیک راست نموده و گزینه Active یا Deactive را انتخاب کنید. توجه داشته باشید که با غیرفعال کردن Scope یا Superscope، کاربران Lease های فعلی خود را از دست خواهند داد و باید مجدداً درخواست Lease نمایند.

### ۵-۱۰ ایجاد Scope های Multicast برای IPv4

Multicasting (چند پخش) زمانی اتفاق می افتد که یک ماشین بجای برقراری ارتباط با تک تک کامپیوترها در شبکه، با شبکه ای از کامپیوترها ارتباط برقرار نماید. این کار بیشتر زمانی مفید است که بخواهید یک ویدئو یا صدا را به تعدادی از کاربران در شبکه ارسال کنید. در ادامه با پروتکلی به نام MADCAP که انجام Multicasting را کنترل می کند آشنا خواهید شد و سپس نحوه ایجاد و

پیکربندی یک Scope از نوع Multicast را شرح خواهیم داد.

### ۵-۱۰-۱ آشنایی با پروتکل MADCAP<sup>۱</sup>

سرویس DHCP معمولاً برای اختصاص آدرس‌های IP و سایر اطلاعات پیکربندی در ارتباطات شبکه‌ای تک‌پخش<sup>۲</sup> (یک به یک) استفاده می‌شود. با استفاده از Multicasting چندین نوع فضای آدرس‌دهی جداگانه از آدرس 224.0.0.0 تا 239.255.255.255 وجود دارد. آدرس‌هایی که در این دامنه قرار می‌گیرند، آدرس‌های کلاس D (Class D) یا آدرس‌های Multicast شناخته می‌شوند. کاربران تنها با دانستن و استفاده از این آدرس‌ها می‌توانند (جهت دریافت محتوا) در یک Multicast شرکت کنند، اگرچه به آدرس‌های IP معمولی نیز نیاز دارند.

اما کاربران چگونه می‌توانند از آدرسی که باید استفاده کنند مطلع شوند؟ DHCP در این زمینه کمکی نخواهد کرد زیرا این سرویس جهت اختصاص آدرس‌های IP و سایر اطلاعات به یک کاربر در هر لحظه طراحی شده است. برای تحقق بخشیدن به این موضوع، گروه مهندسين اينترنت (IETF)<sup>۳</sup> پروتکلی به نام MADCAP را طراحی کرده‌اند. این پروتکل در کاربردهای Multicast مورد استفاده قرار می‌گیرد و شبیه پروتکل DHCP می‌باشد. با استفاده از این پروتکل، کاربران MADCAP زمانی که قصد مشارکت در یک Multicast داشته باشند می‌توانند Lease‌هایی از نوع Multicast را از سرور درخواست نمایند.

DHCP و MADCAP دارای چندین تفاوت مهم هستند: این دو پروتکل کاملاً از یکدیگر جدا هستند. یک سرور می‌تواند به عنوان سرور DHCP یا سرور MADCAP و یا هر دو به کار گرفته شود، اما هیچ رابطه ضمنی و یا واقعی میان این دو وجود ندارد. علاوه بر این، کاربران می‌توانند بطور همزمان از DHCP و/یا MADCAP استفاده کنند، کافی است کاربران MADCAP یک آدرس Unicast را از جایی دریافت کنند.



توجه داشته باشید که DHCP می‌تواند طی فرایند Lease، اطلاعات Option‌ها را به کاربران اختصاص دهد، در حالی که MADCAP قادر به انجام چنین کاری نیست و فقط می‌تواند آدرس‌های Multicast را به صورت پویا به کاربران اختصاص دهد.

### ۵-۱۰-۲ ایجاد Multicast Scopes

جهت ایجاد Multicast Scopes مراحل زیر را دنبال کنید:

1. Multicast Address Dynamic Client Allocation Protocol
2. Unicast
3. Internet Engineering Task Force

۱. در کنسول مدیریت DHCP بر روی IPv4 کلیک راست نموده و گزینه New Multicast Scope را انتخاب کنید.
۲. در صفحه "Welcom to the New Multicast Scope Wizard" بر روی Next کلیک کنید.
۳. در صفحه "Multicast Scope Name"، نام و توضیحی راجع به Scope وارد نموده و بر روی Next کلیک کنید.

شکل ۴۵-۵

۴. صفحه "IP Address Range" نشان داده می شود. در قسمت Start IP address، آدرس 224.0.0.0 و در قسمت End IP address آدرس 224.255.0.0 را وارد کنید. در قسمت TTL<sup>۱</sup> نیز عدد ۱ را وارد نموده تا مطمئن شوید که هیچ پکت Multicast از شبکه خارج نمی گردد (در واقع این عدد تعداد مسیریاب هایی که در فرایند Multicast مورد استفاده قرار می گیرند را مشخص می نماید).

شکل ۴۶-۵

۵. در صفحه "Add Exclusions" می توانید محدوده آدرس های Exclusions را تعیین نمایید. بر روی Next کلیک کنید.

---

1. Time to Live

شکل ۴۷-۵

۶. در صفحه "Lease Duration" می‌توانید مدت زمان Lease را تعیین کنید. این زمان بطور پیش‌فرض ۳۰ روز می‌باشد. پس از تنظیم مدت زمان، بر روی Next کلیک کنید.

شکل ۴۸-۵

۷. در صفحه "Active Multicast Address" می‌توانید فعال یا غیرفعال بودن Scope را تعیین کنید. گزینه No را انتخاب نموده و بر روی Next کلیک کنید.

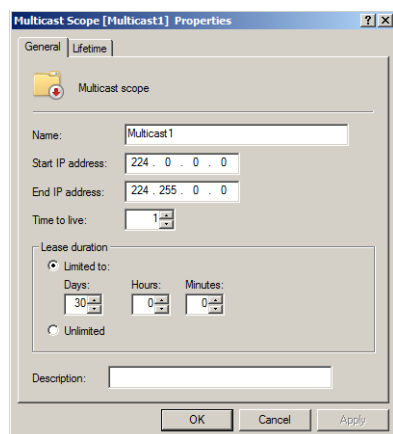
شکل ۴۹-۵

۸. در صفحه "Completing the New Multicast Scope Wizard" بر روی Finish کلیک کنید.

### ۵-۱۰-۳ تنظیم مشخصات Multicast Scopes

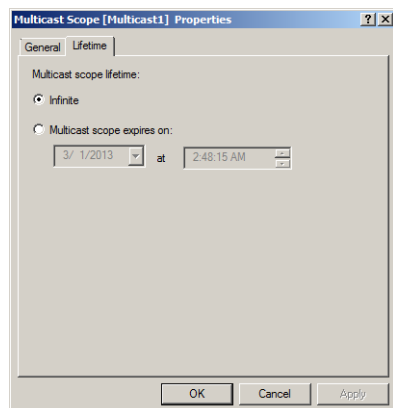
همانند سایر Scope ها، می‌توانید مشخصات Scope های Multicast را تغییر داده و یا تنظیم نمایید. برای انجام این کار مراحل زیر را دنبال کنید:

۱. بروی Multicast Scope مورد نظر کلیک‌راست نموده و Properties را انتخاب کنید.
۲. پنجره "Multicast Scope [Scope name] Properties" نشان داده می‌شود. در تب General از این پنجره می‌توانید تنظیماتی مانند نام Scope، آدرس‌های شروع و پایان Scope، مدت زمان عمر بسته‌ها (TTL)، مدت زمان Lease و توضیحاتی راجع به Scope را انجام دهید.



شکل ۵-۵۰

۳. در تب lifetime نیز می‌توانید مدت زمان فعال بودن Scope را تعیین کنید. بطور پیش‌فرض، Scope برای همیشه فعال است اما چون این Scope ها برای رویدادهای خاصی ایجاد می‌شوند می‌توانید مدت زمان فعال بودن آنها را به صورت دلخواه تنظیم کنید. جهت انجام این کار باید گزینه Multicast scope expires on را انتخاب نموده و تاریخ و ساعت غیرفعال شدن آنرا تعیین نمایید.



شکل ۵-۵۱

## ۵-۱۱ یکپارچه سازی DDNS با DHCP

اطلاعات سرور DNS به دو روش می‌تواند بروز رسانی شود. روش اول زمانی است که کاربران DHCP آدرس خود را به سرور DNS اعلام می‌کنند، و روش دوم زمانی است که سرور DHCP هنگام ثبت یک کاربر جدید، آدرس آنرا به سرور DNS اعلام می‌کند. هیچکدام از این بروز رسانی‌ها تا وقتی که سرور DNS را برای استفاده از DNS پویا<sup>۱</sup> (DDNS) پیکربندی نکنید انجام نخواهد شد. پیکربندی DDNS در دو سطح قابل انجام است:

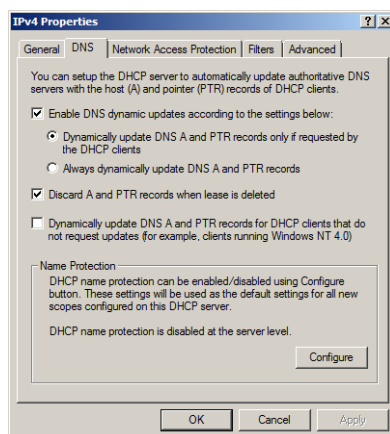
- سطح Scope: اگر پیکربندی در سطح یک Scope انجام شود، تنظیمات آن تنها بر روی کاربران همان Scope اعمال خواهند شد.
- سطح Server: پیکربندی سطح سرور، تنظیمات را بر روی کلیه Scope ها و Superscope ها اعمال می‌کند.

انتخاب سطح پیکربندی بستگی به محدوده‌ای دارد که قرار است از DDNS پشتیبانی کند. به عنوان مثال بیشتر وبسایت‌هایی که بر روی اینترنت مشاهده می‌کنید، بروز رسانی DNS را در سطح سرور انجام می‌دهند.

## ۵-۱۱-۱ بروز رسانی اطلاعات DNS در DHCP

برای بروز رسانی تنظیمات چه در سطح Scope و یا سطح سرور، مراحل زیر را دنبال کنید:

۱. بر روی Scope یا سرور مورد نظر کلیک راست نموده و properties را انتخاب کنید.
۲. در پنجره IPv4 Properties/Scope Properties، تب DNS را انتخاب کنید.



شکل ۵-۵۲



- همانطور که در شکل ۵-۵۲ مشاهده می‌کنید تب DNS شامل موارد زیر می‌باشد:
- ♦ **Enable DNS Dynamic Updates According To The Settings Below**: این گزینه فعال یا غیرفعال کردن توانایی سرور DHCP جهت ثبت اطلاعات Lease به همراه سرور DNS را کنترل می‌کند. جهت فعال‌سازی DDNS این گزینه باید تیک خورده باشد.
  - ♦ **Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients**: این گزینه به سرور DHCP اعلام می‌کند که فقط در صورت درخواست کاربران برای ثبت نام در DNS، بروز رسانی را انجام دهد. زمانی که این گزینه فعال باشد، کاربران DHCP که به DDNS متصل نباشند نمی‌توانند بروز رسانی رکوردهای DNS را در اختیار داشته باشند. با این حال، کاربران ویندوزهای 2000، XP، Vista، Server 2003، Server 2008 و Server 2008R2 به اندازه‌ای هوشمند هستند که برای این بروز رسانی درخواست دهند.
  - ♦ **Always Dynamically Update DNS A And PTR Records**: این گزینه سرور DHCP را مجبور می‌کند که بروز رسانی را برای تمام کاربران انجام دهد. اگرچه این ویژگی باعث می‌شود که اطلاعات بروز رسانی برای دستگاه‌هایی که DHCP بر روی آنها فعال بوده ولی نیاز به این اطلاعات ندارند (مثل Print Server) ارسال شود، اما به سایر کاربران (کاربران ماشین‌های Mac، OS، Windows NT و Linux) اجازه می‌دهد که بروز رسانی خودکار اطلاعات DNS را در اختیار داشته باشند.
  - ♦ **Discard A And PTR Records When Lease Is Deleted**: این گزینه اتفاقی که برای اطلاعات DNS مرتبط با یک Lease در زمان اتمام آن رخ می‌دهد را مشخص می‌نماید. چنانچه این گزینه فعال باشد (تیک خورده باشد) اطلاعات DNS در زمان اتمام Lease حذف خواهند شد ولی در صورتی که این گزینه غیرفعال باشد، پس از اتمام اعتبار Lease نیز اطلاعات DNS برای آن نگهداری خواهد شد.
  - ♦ **Dynamically Update DNS A And PTR Records For DHCP Clients That Do Not Request Updates**: این گزینه باعث فراهم شدن اطلاعات بروز رسانی DNS برای کاربرانی می‌شود که آن اطلاعات را درخواست نکرده‌اند (البته فعال‌سازی این ویژگی لطفی است که در حق این کاربران انجام می‌شود!)

## ۵-۱۱-۲ یکپارچه سازی DNS با DHCP

جهت یکپارچه سازی DNS با DHCP مراحل زیر را دنبال کنید:

۱. در کنسول مدیریت DHCP بر روی IPv4 کلیک‌راست نموده و Properties را انتخاب کنید.

۲. در پنجره "IPv4 Properties" تب DNS را انتخاب کنید.
۳. گزینه Enable DNS Dynamic Updates According To The Settings Below را فعال نموده و سپس گزینه Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients را انتخاب کنید.
۴. مطمئن شوید که گزینه Discard A And PTR Records When Lease Is Deleted نیز فعال است (در غیر اینصورت آنرا فعال کنید).
۵. بر روی OK کلیک کنید تا تنظیمات اعمال گردد.
۶. پنجره "IPv4 Properties" را ببندید.

## ۵-۱۲ نظارت و عیب‌یابی DHCP

DHCP به مراقبت زیاد و مداوم نیاز ندارد، با این حال دانستن نحوه نظارت<sup>۱</sup> و عیب‌یابی<sup>۲</sup> آن در مواردی که کارهای نادرستی انجام می‌شود، می‌تواند مفید واقع گردد. در ادامه به مباحثی مثل نظارت بر Leaseهای DHCP، ثبت<sup>۳</sup> فعالیت‌های DHCP، کارکردن با فایل‌های ثبت وقایع و پایگاه‌داده‌های DHCP و تطبیق‌دادن<sup>۴</sup> Scopeها در DHCP خواهیم پرداخت.

### ۵-۱۲-۱ نظارت بر Leaseهای DHCP

با استفاده از کنسول مدیریت DHCP، امکان مدیریت و نظارت بر Leaseها بسیار ساده شده است. جهت مشاهده Leaseها می‌توانید از زیرشاخه هر Scope، بر روی Address Leases کلیک نموده و لیست Leaseها را مشاهده کنید.

چنانچه قصد داشته باشید Lease مرتبط با یک کاربر را حذف کنید، کافی است در قسمت Address Leases بر روی Lease کلیک‌راست نموده و Delete را انتخاب کنید. این کار باعث لغو شدن و حذف Lease می‌گردد. معمولاً بهترین کار این است که بجای حذف دستی Lease، اجازه دهید مدت زمان آن به پایان برسد، اما گاهی اوقات و با توجه به شرایط، حذف دستی آنها لازم است. در ادامه قصد داریم نحوه بررسی Leaseها را با ذخیره کردن آنها به صورت یک فایل متنی شرح دهیم. قبل از این کار لازم است حداقل یک یا دو Lease در حال اجرا باشند. جهت انجام این کار مراحل زیر را دنبال کنید:

۱. در کنسول مدیریت DHCP بر روی IPv4 کلیک کنید تا آیتم‌های زیرشاخه آن نشان داده شوند.

---

1. Monitoring  
2. Troubleshooting  
3. Log  
4. Reconcile

۲. Scope مورد نظر را انتخاب کنید.
۳. بر روی Scope کلیک راست نموده و گزینه Export List را انتخاب کنید.
۴. در پنجره "Save As" محل ذخیره و نام فایل Export را مشخص نموده و بر روی Save کلیک کنید.
۵. فایل را در یکی از برنامه‌های Notepad، WordPad، Word، Excel و یا ... باز کنید. توجه داشته باشید که محتویات این فایل همان چیزی است که در کنسول DHCP مشاهده نمودید. چنانچه هیچ Lease ای اختصاص داده نشده باشد، شما تنها یک سطر حاوی عنوان هر ستون مشاهده خواهید نمود.

### ۵-۱۲-۲ ثبت فعالیت‌های DHCP

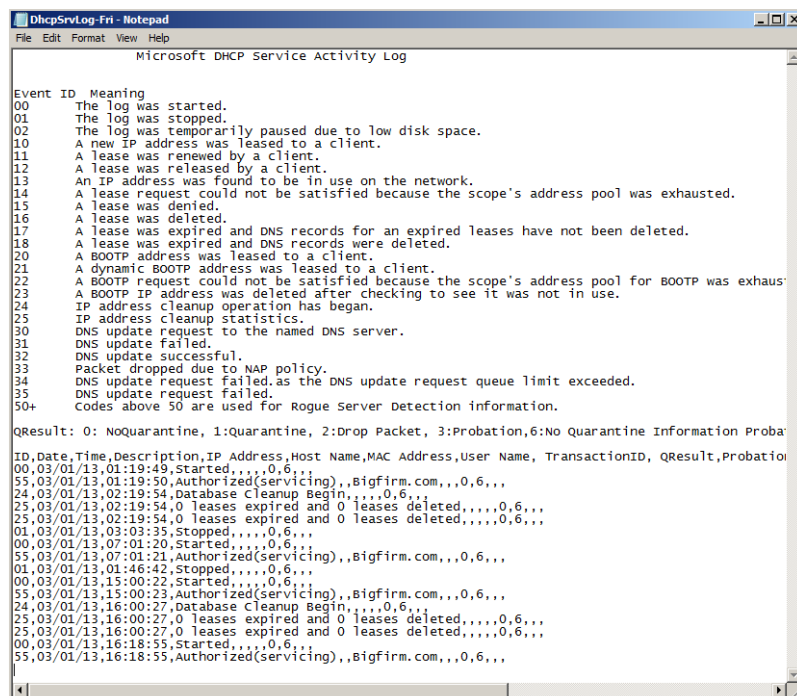
سرور DHCP به طور خودکار تمام فعالیت‌های DHCP را در یک فایل ثبت وقایع (log) به صورت روزانه ثبت می‌کند. این فایل در پوشه C:\Windows\System32\dhcp و با نام DhcpSrvLog-Day قرار دارد که Day یک مخفف سه حرفی و نمایانگر روزهای هفته می‌باشد. فایل‌های Log در DHCP، یک سری از فایل‌های متنی هستند که در آن هر مدخل<sup>۱</sup> (ورودی) در یک سطر جداگانه آورده می‌شود. تعدادی از فیلدهایی که برای مدخل‌های این فایل‌ها وجود دارد، در جدول ۵-۱ شرح داده شده است

جدول ۵-۱: فیلدهای موجود در فایل‌های Log در سرور DHCP

نام فیلد	شرح
ID	شناسه مربوط به رویداد در سرور DHCP (00، 01 و ...)
Date	تاریخی که یک رویداد در سرور DHCP اتفاق می‌افتد
Time	زمانی که یک رویداد در سرور DHCP اتفاق می‌افتد
Description	نوع رویدادی که در سرور DHCP رخ می‌دهد
IP Address	آدرس IP کاربر DHCP
Host Name	نام میزبان (نام ماشین) کاربر DHCP
MAC Address	آدرس سخت افزار کاربر که همان آدرس فیزیکی کارت شبکه می‌باشد
User Name	نام کاربر DHCP

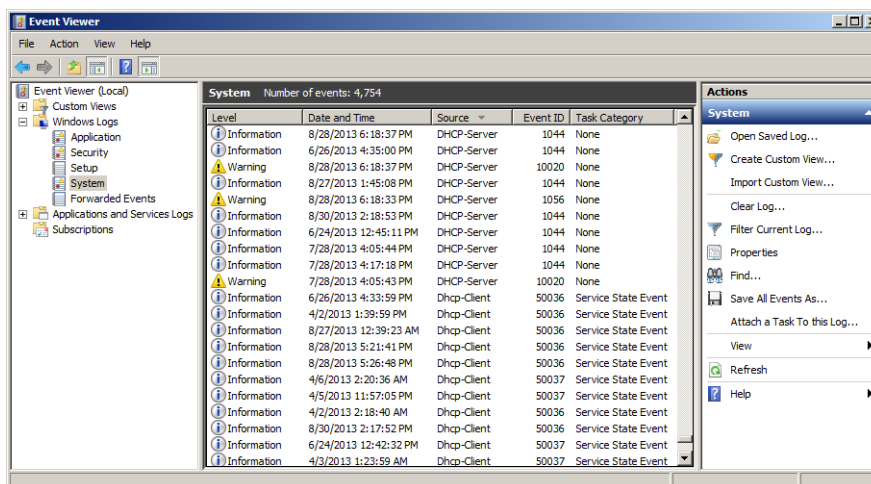
در شکل ۵-۳ می‌توانید محتویات یکی از فایل‌های Log را مشاهده کنید.

1. Entry



شکل ۵-۵۳

دقت داشته باشید که این رویدادها را می‌توان از ابزار Event Viewer نیز مشاهده نمود. این ابزار از مسیر «Start» «Administrative Tools» Event Viewer قابل دسترسی می‌باشد. در Logهای این ابزار باید به دنبال مدخل‌های مرتبط با DHCP بگردید (شکل ۵-۵۴).



شکل ۵-۵۴

### ۵-۱۲-۳ کار با پایگاه داده های DHCP

DHCP جهت نگهداری اطلاعات مربوط به Scope ها، Superscope ها و Lease های کاربران، از چند پایگاه داده استفاده می کند. این فایل ها در مسیر C:\Windows\System32\dhcp قرار دارند و در زمان اجرای سرویس DHCP مورد استفاده قرار می گیرند. مشاهده محتویات و ایجاد تغییرات در این فایل ها تا زمانی که سرویس DHCP در حال اجرا می باشد امکان پذیر نیست، بنابراین قبل از ایجاد تغییرات باید این سرویس را متوقف کنید.

فایل اصلی مربوط به پایگاه داده DHCP با نام dhcp.mdb و در مسیر ذکر شده قرار دارد و حاوی اطلاعات تمام Scope ها می باشد. تعدادی دیگر از فایل های مرتبط با پایگاه داده DHCP که در این مسیر قرار دارند عبارتند از:

- ♦ **Dhcp.tmp**: این فایل یک کپی از فایل Backup پایگاه داده DHCP می باشد که در زمان شاخص دهی مجدد<sup>۱</sup> پایگاه داده ایجاد می شود.
- ♦ **J50 log** (به اضافه تعدادی از فایل ها با نام J50xxxxx.log که xxxxx مقادیر 00001 و 00002 و 00003 و مشابه آن می باشند): این فایل هرگونه تغییری را قبل از نوشته شدن برروی پایگاه داده ذخیره می کند. موتور<sup>۲</sup> پایگاه داده DHCP، در هنگام راه اندازی سرور از این فایل ها جهت بازیابی تعدادی از تغییرات استفاده می کند.
- ♦ **J50.chk**: یک فایل Checkpoint (نقطه بررسی) می باشد و به موتور DHCP اعلام می کند که کدامیک از فایل های Log نیازمند بازیابی می باشند.

#### حذف فایل های پایگاه داده

گاهی اوقات ممکن است در هنگام کار با پایگاه داده متوجه شوید که اطلاعات مربوط به Lease ها با آنچه که در شبکه باید وجود داشته باشد ناسازگار است. یکی از راه حل هایی که جهت برطرف کردن این مشکل به کار گرفته می شود، حذف فایل پایگاه داده و راه اندازی سرور با استفاده از یک فایل بدون محتوا می باشد. برای انجام این کار مراحل زیر را دنبال کنید:

۱. سرویس DHCP را با استفاده از دستور `net stop dhcpserver` و یا با کلیک راست برروی نام سرور در کنسول مدیریت DHCP و انتخاب «All Tasks» Stop متوقف کنید.
۲. کلیه فایل های موجود در پوشه C:\Windows\System32\dhcp را حذف کنید.
۳. سرور را Restart کنید.
۴. Scope (ها) را با سرور تطبیق دهید تا محتویات پایگاه داده مجدداً ایجاد شوند.

1. Reindexing  
2. Engine

### تغییر بازه زمانی Backup گیری از پایگاه داده

بطور پیش فرض، DHCP هر ۶۰ دقیقه یکبار از پایگاه داده خود Backup گیری می کند. می توانید این زمان را با استفاده از مقدار Backup Interval در رجیستری تغییر دهید. این مقدار از مسیر زیر قابل دسترسی می باشد:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DhcpServer\Parameter

### جابجایی فایل های پایگاه داده DHCP

گاهی اوقات لازم است که سرور DHCP و عملکردهای مرتبط با آنرا به کامپیوتر دیگری انتقال دهید. در این مواقع بهترین کار این است که فایل های پایگاه داده DHCP را کپی نموده و آنرا مستقیماً به کامپیوتر جدید منتقل کنید. با این روش دیگر نیازی به ایجاد مجدد فایل ها و همچنین برطرف کردن خطاهایی که در هنگام ایجاد آنها ممکن است رخ دهد نخواهید داشت.

در این قسمت قصد داریم نحوه انتقال فایل پایگاه داده DHCP از یک ویندوز 2000، سرور 2003 و سرور 2008 را به دیگری نشان دهیم. جهت جابجایی پایگاه داده مراحل زیر را دنبال کنید:

۱. سرور DHCP را با دستور `net stop dhcpserver` در خط فرمان متوقف کنید.
۲. پوشه `C:\Windows\System32\dhcp` را به یک پوشه موقت در سرور مقصد کپی کنید.
۳. با نوشتن دستور `Regedit.exe` در `Cmd`، رجیستری را اجرا نموده و کلید `Configuration` را از مسیر `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DhcpServer` پیدا کنید. آنرا انتخاب نموده و از منوی بالای پنجره رجیستری، گزینه `File » Export` را انتخاب کنید.
۴. سرویس DHCP را بروی سرور مقصد نصب نموده با دستور `net stop dhcpserver` آنرا متوقف کنید.
۵. فایل `System.mdb` را از پوشه موقت انتخاب نموده و نام آنرا به `System.src` تغییر دهید.
۶. تمام محتویات پوشه `C:\Windows\System32\dhcp` را در کامپیوتر مقصد حذف کنید.
۷. رجیستری را در کامپیوتر مقصد اجرا نموده و مجدداً کلید `Configuration` را از مسیر `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DhcpServer` پیدا کنید. این کلید را انتخاب نموده و از منوی بالای پنجره رجیستری، گزینه `File » Import` را انتخاب کنید.
۸. فایلی که اخیراً ذخیره نموده اید را انتخاب نموده و بروی `Yes` کلیک کنید تا جایگزین تنظیمات فعلی گردد.
۹. سرویس DHCP را در کامپیوتر مقصد با دستور `net start dhcpserver` در خط فرمان راه اندازی کنید.
۱۰. در آخرین مرحله نیز باید سرور را در اکتیو دایرکتوری مجاز کنید. جهت انجام این کار بروی

نام سرور کلیکراست نموده و گزینه Authority را انتخاب کنید.

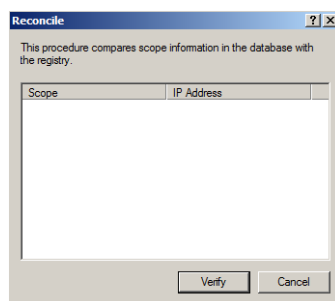
#### ۵-۱۲-۴ تطبیق دادن Scope های DHCP در IPv4

با گذشت زمان ممکن است متوجه شوید که اطلاعات پایگاه داده DHCP با اطلاعات اصلی در شبکه سازگار نمی باشد و بنابراین دیگر از کارایی لازم برخوردار نخواهند بود. راه حل این مشکل، حذف پایگاه داده و ایجاد مجدد آن می باشد. برای انجام این کار باید Scope های خود را با پایگاه داده تطبیق دهید.

#### تطبیق دادن یک Scope

جهت تطبیق دادن یک Scope مراحل زیر را دنبال کنید:

۱. کنسول مدیریت DHCP را اجرا کنید.
۲. بر روی IPv4 کلیک کنید تا آیتم های زیرشاخه آن نشان داده شود.
۳. بر روی Scope موردنظر کلیکراست نموده و گزینه Reconcile را انتخاب کنید.
۴. در پنجره "Reconcile" بر روی دکمه Verify کلیک کنید تا عمل تطبیق آغاز شود.



شکل ۵-۵۵

۵. اگر پایگاه داده با Scope سازگار بود، پنجره ای ظاهر شده و سازگاری آنرا اعلام می نماید. در صورتی که هرگونه ناسازگاری وجود داشته باشد، پنجره ای حاوی فهرست آنها نشان داده می شود و به شما اجازه می دهد تا این ناسازگاری ها را برطرف کنید.

#### تطبیق دادن همه Scope ها

برای تطبیق دادن همه Scope ها با پایگاه داده نیز فرایند مشابهی اجرا می گردد:

۱. پنجره مدیریت DHCP را اجرا کنید.
۲. بر روی IPv4 کلیکراست نموده و گزینه Reconcile All Scopes را انتخاب کنید.
۳. بر روی دکمه Verify کلیک کنید.

**بازگردانی یک سرور ناموفق**

روش پیشنهادی برای بازگردانی یک سرور ناموفق به صورت زیر می باشد:

۱. حذف فایل پایگاه داده
۲. Reconcile کردن همه Scope ها در سرور برای بازسازی پایگاه داده.





## « فصل ۶ »

اكتيو دايركتورى

**Active Directory**  
VCLIA6 DILGCLOLA



اکتیو دایرکتوری یک پایگاه داده مرکزی در ویندوز سرور است که تمامی اطلاعات مربوط به اشیاء متصل به شبکه را در خود نگهداری می‌کند. با اینکه تاکنون مطالب زیادی در مورد ساختار پیچیده اکتیو دایرکتوری نوشته شده است، بسیاری از سازمان‌ها ترجیح می‌دهند که به دلیل سهولت کار، از ساختار مبتنی بر یک دامنه استفاده کنند. پیاده‌سازی ساختار تک‌دامنه‌ای بسیار ساده است، ولی در مواردی که تعداد کاربران بیش از ۵۰۰۰ باشند و یا به دلایل خاصی دامنه‌های بیشتری نیاز باشد، این ساختار توصیه نمی‌گردد.

ایجاد یک دامنه نسبتاً ساده است. کافی است یک نام برای آن انتخاب نموده و با راه‌اندازی ویزارد نصب کنترل‌کننده دامنه یا DCPromo، سرور خود را به یک کنترل‌کننده دامنه<sup>۱</sup> (DC) تبدیل کنید. مهمترین ابزاری که در مدیریت دامنه‌ها به کار خواهید برد، ابزاری بنام Active Directory Users and Computers می‌باشد. به کمک این ابزار می‌توانید کاربران و اشیاء کامپیوتری را در دامنه ایجاد نموده و آنها را در قالب یک واحد سازمانی<sup>۲</sup> (OU) سازماندهی کنید. البته ایجاد اشیاء اکتیو دایرکتوری از طریق خط فرمان نیز امکان‌پذیر می‌باشد.

مهمترین مباحثی که در این فصل به آنها پرداخته خواهد شد عبارتند از:

- ♦ ایجاد جنگل تک‌دامنه‌ای<sup>۳</sup>
- ♦ افزودن یک DC ثانویه به دامنه
- ♦ ایجاد حساب‌های کاربری
- ♦ ایجاد سیاست‌های دانه‌ریز رمز عبور<sup>۴</sup>

## ۶-۱ آشنایی با مفاهیم پایه اکتیو دایرکتوری

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

### Workgroup ۱-۱-۶

یک شبکه Workgroup گروهی از کاربران هستند که به یک شبکه محلی<sup>۵</sup> (LAN) متصل شده و در آن هر کامپیوتر دارای حساب‌های کاربری مجزایی می‌باشد. کاربری که با استفاده از یک حساب

---

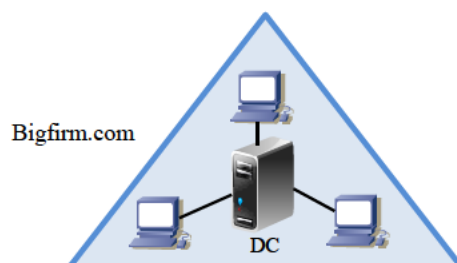
1. Domain Controller  
2. Organizational Unit  
3. Single-domain forest  
4. Fine-Grained Password Policies  
5. Local Area Network

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

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

### Domain ۲-۱-۶

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



شکل ۱-۶

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

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

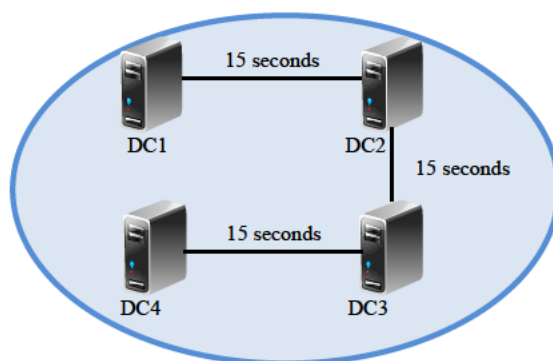
کپی‌هایی از اکتیو دایرکتوری بر روی DCها نگهداری می‌شوند. معمولاً برای اهداف افزونگی<sup>۱</sup>، حداقل از دو DC استفاده می‌شود تا در مواقع از کار افتادن یکی از آنها بتوان از دیگری استفاده نمود.

1. Domain Controller Promotion  
2. Redundant

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

#### ۴-۱-۶ Replication

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



شکل ۴-۶

#### ۵-۱-۶ Objects

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

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

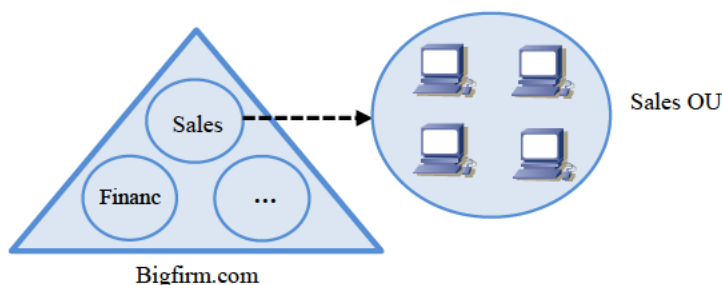
#### Schema ۶-۱-۶

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

#### Organizational units ۷-۱-۶

واحدهای سازمانی (OU)، برای سازماندهی اشیاء در اکتیو دایرکتوری استفاده می‌شوند. در واقع OUها مانند کانتینترهایی<sup>۱</sup> هستند که جهت نگهداری اشیاء مورد استفاده قرار می‌گیرند. با قرار دادن اشیاء در این کانتینترها مدیریت آنها آسانتر می‌شود. به عنوان مثال می‌توانید یک OU با نام Sales (فروش) ایجاد نموده و تمام کاربران و کامپیوترهای بخش فروش را در آن قرار دهید.

OUها دو مزیت ممتاز دارند: اول، می‌توان بر روی آنها مجوزهایی<sup>۲</sup> برای دسترسی اشیاء تعیین نمود. دوم، می‌توان انواع Group Policyها را ایجاد نموده و به آنها پیوند داد. به عنوان مثال Maria مسئول تمام کاربران و کامپیوترها در بخش فروش است. اگر این اشیاء در یک OU به نام Sales قرار داده شوند، Maria برای مدیریت آنها می‌تواند بر روی آن OU مجوزی اعمال نموده تا بر روی تمام کاربران و کامپیوترها اعمال شود. بطور مشابه می‌تواند با استفاده از اشیاء Group Policy (GPO) تنظیمات و پیکربندی‌های گوناگونی را بر روی کاربران و کامپیوترهای این OU اعمال کند.



شکل ۳-۶

1. Containers
2. Permissions

**Group Policy ۸-۱-۶**

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

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

**Default domain policy ۹-۱-۶**

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

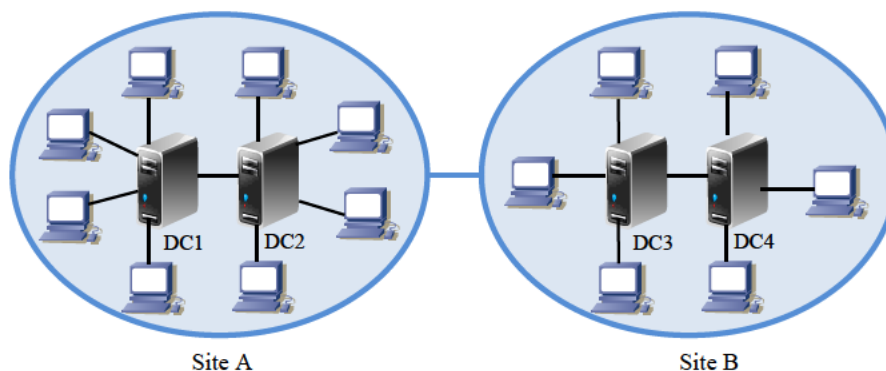
**Default domain controllers policy ۱۰-۱-۶**

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

**Site ۱۱-۱-۶**

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

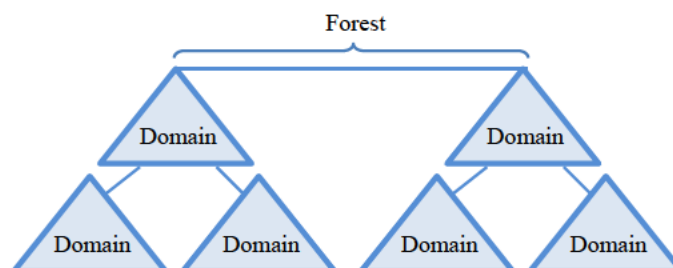




شکل ۴-۶

## Forest ۱۲-۱-۶

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



شکل ۵-۶

## Global Catalog ۱۳-۱-۶

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

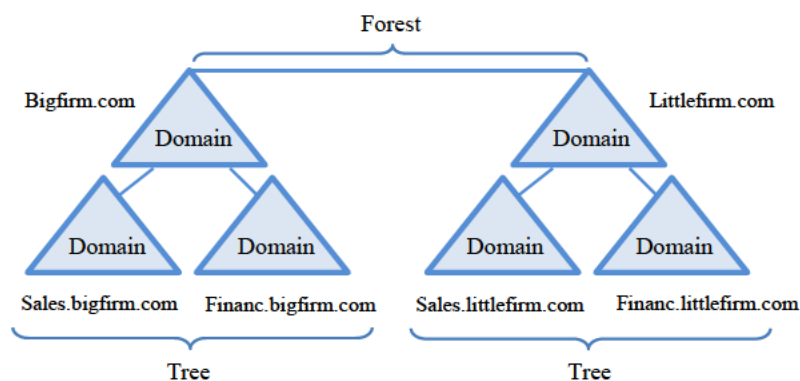
از آنجایی که تنها یک GC می‌تواند در یک جنگل وجود داشته باشد و هر جنگل می‌تواند شامل چندین دامنه باشد، بنابراین حجم فایل GC می‌تواند کمی بزرگ باشد. برای محدود کردن حجم آن، اشیاء داخل GC تنها می‌توانند دارای زیرمجموعه‌ای از مشخصات اصلی باشند. به عنوان مثال اگر یک حساب کاربری دارای ۱۰۰ مشخصه برای توصیف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

می‌شود.

### Tree ۱۴-۱-۶

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

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



شکل ۶-۶

### ۲-۶ جنگل تک دامنه‌ای

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

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

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

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

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

از لحاظ فنی، یک دامنه یک جنگل نیز می‌باشد. اولین دامنه در جنگل، دامنه ریشه<sup>۱</sup> است و یک جنگل تک دامنه‌ای تنها شامل دامنه ریشه می‌باشد. در سازمان‌های خیلی بزرگ ممکن است چندین جنگل به منظور فعال‌سازی Schemaها، مدیریت منابع مختلف، تقسیم‌بندی دسترسی مدیر شبکه و یا حتی به دلایل جغرافیایی یا سیاسی ایجاد شود. مدیریت و ایجاد تغییر در دامنه‌های موجود در جنگل‌های چند دامنه‌ای نیازمند دقت و اطمینان زیادی می‌باشد زیرا سایر دامنه‌ها نیز باید لحاظ گردند. اما مدیریت جنگل‌های تک دامنه‌ای به دلیل عدم وجود دامنه‌های دیگر کار نسبتاً ساده‌ای می‌باشد.

## ۶-۲-۱ مزایای استفاده از یک دامنه

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

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

1. Root Domain

- ♦ **مدیریت آسانتر:** هر دامنه‌ای که ایجاد می‌شود، به دنبال آن حساب‌های کاربری، گروه‌ها، انواع سیاست‌های گروهی و ... نیز باید ایجاد شوند. زمانی که از یک دامنه استفاده شود با حجم کمتری از این اشیاء روبرو خواهید بود و بنابراین (نسبت به زمانی که چندین دامنه در اختیار دارید) به آسانی می‌توانید آنها را مدیریت کنید.
- ♦ **بازیابی فاجعه<sup>۱</sup> ساده‌تر:** اغلب دیده می‌شود که سرورهای موجود در شبکه ناموفق عمل کرده و یا بطور ناگهانی از کار می‌افتند. برای رفع چنین مشکلاتی باید از اطلاعات این سرورها Backup تهیه نموده و در صورت نیاز آنها را بازگردانی کرد. زمانی که از یک دامنه استفاده می‌کنید، تعداد سرورهای کمتری مورد استفاده قرار می‌دهید بنابراین بازگردانی این سرورها در صورت از کار افتادن و یا وقوع هر مشکلی ساده‌تر خواهد بود.
- یکی از دلایلی که در گذشته مدیران شبکه‌ها را مجبور به ایجاد چندین دامنه می‌کرد، اعمال سیاست‌های رمزعبور مختلف بر روی یک دامنه بود. از ویندوز سرور 2008 به بعد، این مسئله برطرف شده و به کمک سیاست‌های دانه‌ریز رمز عبور می‌توان چندین Password Policy بر روی یک دامنه ایجاد کرد (بعداً در همین فصل به این موضوع خواهیم پرداخت).

## ۶-۲-۲ ایجاد جنگل تک دامنه‌ای

زمانی که ویندوز سرور 2008R2 را برای اولین بار نصب می‌کنید، ایجاد دامنه در آن بسیار ساده خواهد بود. کافی است ویزارد Domain Controller Promotion یا همان DCPromo را اجرا نموده و سرور خود را به یک DC تبدیل کنید. این ویزارد، سرویس‌های مربوط به دامنه در اکتیو دایرکتوری یا Active Directory Domain Services را بر روی سرور راه‌اندازی (یا حذف) می‌کند. ویزارد DCPromo بر روی هر نسخه از ویندوز سرور (مثل 2000، 2003، 2008 و ...) قابل اجرا است اما قابلیت‌های دامنه در این نسخه‌ها متفاوت می‌باشد.

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

- ♦ پیکربندی سرور
- ♦ بررسی سازگاری سیستم‌عامل<sup>۲</sup>
- ♦ پیکربندی توسعه<sup>۳</sup>

---

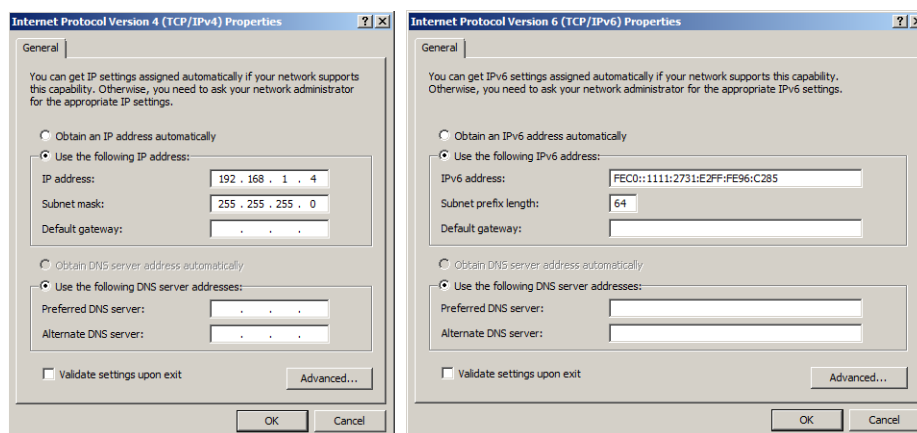
1. Disaster recovery  
2. Operating System Compatibility  
3. Deployment Configuration

- ♦ نام دامنه
- ♦ سطح عملکرد جنگل<sup>۱</sup>
- ♦ سطح عملکرد دامنه<sup>۲</sup>
- ♦ پیکربندی DNS
- ♦ محل قرارگیری فایل‌ها
- ♦ رمز عبور مدیر DSRM<sup>۲</sup>

### قبل از اجرای DCPromo (پیکربندی سرور)

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

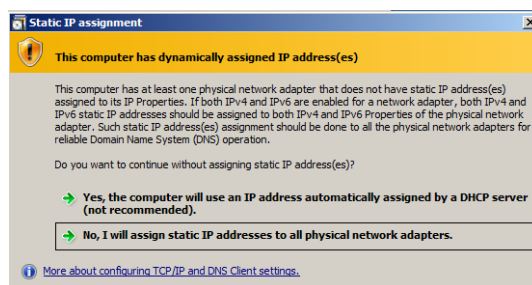
- ♦ نام سرور: قبل از اینکه سرور را به یک DC تبدیل کنید، بهتر است یک نام برای آن انتخاب نموده و بر روی آن اعمال کنید. معمولاً سازمان‌ها از نام‌های DC1، DC2 و مانند آن استفاده می‌کنند. انتخاب این نام بستگی به نظر مدیر شبکه و سیاست‌های سازمان دارد. جهت تنظیم نام بر روی سرور می‌توانید مسیر Computer Properties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



شکل ۶-۷

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

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



شکل ۶-۸

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

### سازگاری سیستم عامل (Operating System Compatability)

طی سال‌های گذشته، در رابطه با استفاده از کامپیوتر و سیستم‌های کامپیوتری چیزی که زیاد شنیده می‌شد و یا مطالب زیادی در مورد آن انتشار پیدا می‌کرد، این بود که این سیستم‌ها توسط ویروس‌ها و به دلایل سرگرمی مورد حمله قرار می‌گرفتند. امروزه وضعیت فرق کرده است و این حملات بیشتر بجای سرگرمی برای سرقت اطلاعات و دریافت پول از سازمان مورد حمله انجام می‌شوند. مدیران شبکه باید از فعال‌سازی هر حفره امنیتی که موجب باز نمودن راه نفوذ به شبکه می‌شود پیشگیری کنند. یکی از این حفره‌ها این است که کاربران ویندوز NT 4.0 و کاربرانی که از سیستم‌های غیر مایکروسافت SMB<sup>۱</sup> (مثل لینوکس) استفاده می‌کنند، سعی می‌کنند توسط DCها تأیید هویت شوند.

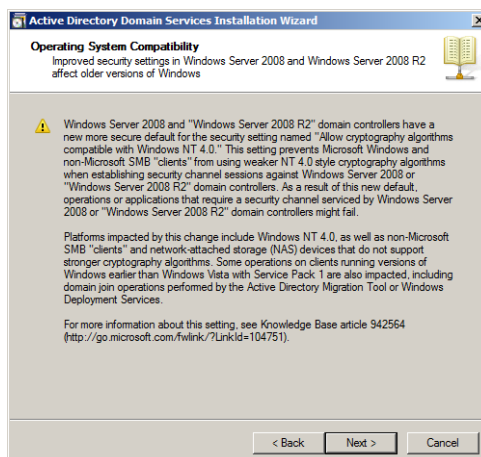
شیوه کدگذاری که در ویندوز NT 4.0 به کار می‌رود امروزه به عنوان یک شیوه فاقد امنیت به شمار رفته و قابل استفاده نیست. به منظور تقویت این شیوه، مایکروسافت نصب پیش‌فرض دامنه در ویندوز سرور 2008 و 2008R2 را امن‌تر نموده است. یکی از اقداماتی که در این زمینه انجام شده، تنظیماتی تحت عنوان “Allow cryptography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

1. Server Message Block

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

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

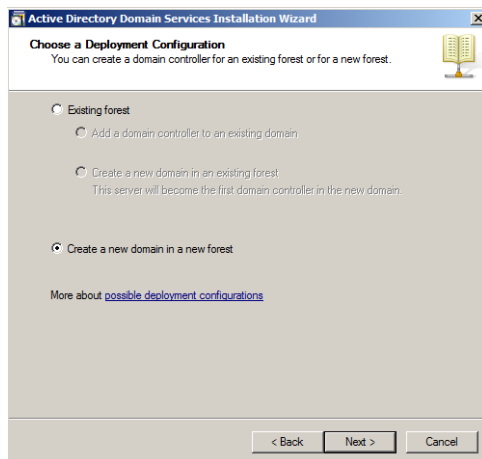
ویزارد DCPromo امکان ایجاد تغییرات در این تنظیمات را فراهم نمی‌کند ولی در صفحه "Operating System Compatibility" هشدارهایی را در این رابطه متذکر می‌شود. در شکل ۶-۹ این صفحه نمایش داده شده است.



شکل ۶-۹

### پیکربندی‌های توسعه (Deployment Configuration)

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

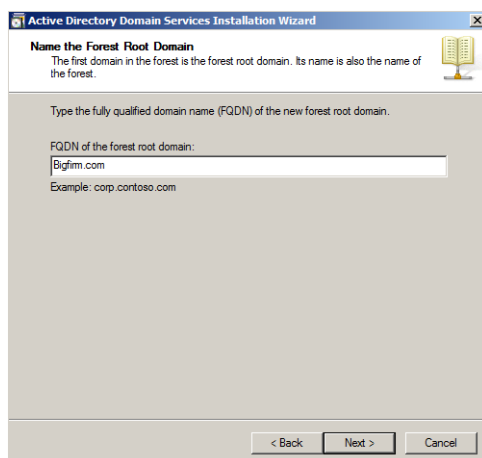


شکل ۱۰-۶

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

اولین دامنه در هر جنگل، به دامنه ریشه اشاره دارد. در زمان ایجاد یک دامنه ریشه باید از یک FQDN<sup>۱</sup> برای آن استفاده کنید. این FQDN از دو جزء تشکیل می‌شود، مانند Bigfirm.com یا Mydomain.net که دومین قسمت در این FQDN ها (.com و .net در این مثال) اشاره به نام دامنه سطح بالا دارد. تعدادی از دامنه‌های سطح بالا که ممکن است در اینترنت مشاهده کنید عبارت‌اند از: .tv، .org، .gov، .biz، .ir و ...

در شکل ۱۱-۶ (و مثال ما) نام FQDN انتخاب شده برای دامنه به صورت Bigfirm.com است.



شکل ۱۱-۶

---

1. Fully Qualified Domain Name



در این صفحه باید از FQDN های دو قسمتی استفاده کنید اما توجه داشته باشید که نام انتخابی شما با نام های معتبری که در اینترنت وجود دارند یکسان نباشد.

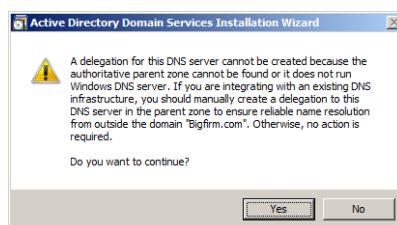
### اکتیو دایرکتوری و DNS

در فصل ۵ راجع به رابطه اکتیو دایرکتوری و DNS صحبت کردیم. چیزی که بطور مختصر لازم است بدانید این است که DNS یکی از نیازمندی های اکتیو دایرکتوری می باشد. رکوردهای SRV در DNS محل نگهداری DC هایی هستند که سرویس های خاصی را اجرا می کنند.

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

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

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



شکل ۶-۱۲

پس از دریافت این پیغام، بر روی Yes کلیک کنید تا فرایند نصب ادامه یابد و DNS، DCPromo را پیکربندی کند. این ویزارد، Zone مربوط به DNS را به صورت “Zone یکپارچه با اکتیو دایرکتوری”<sup>۱</sup> ایجاد می کند.

1. Active Directory Integrated Zone

### سطح عملکرد جنگل (Set Forest Functional Level)

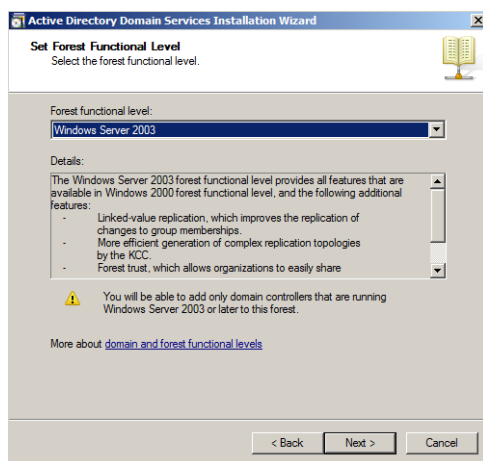
این سطح قابلیت‌های یک جنگل را مشخص می‌کنند. بخاطر داشته باشید که سطح عملکرد دامنه باید منطبق با قدیمی‌ترین سیستم عامل اجرا شونده بر روی DC در دامنه باشد. بطور مشابه، سطح عملکرد جنگل نیز باید منطبق با قدیمی‌ترین سیستم عامل اجرا شونده بر روی DC در جنگل باشد. به عنوان مثال اگر سطح Windows Server 2008 را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

موارد زیر برای سطوح عملکرد جنگل توسط DCPromo پیشنهاد می‌شوند:

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

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

با اجرای DCPromo در پنجره‌ای همانند شکل ۶-۱۳ می‌توانید سطح عملکرد جنگل را تعیین کنید. برای انجام این کار کافی است سطح عملکرد یکسان با آنچه در سطح عملکرد دامنه تعیین نمودید را انتخاب کنید. به عنوان مثال اگر سطح عملکرد دامنه Windows Server 2008 R2 بود سطح عملکرد جنگل نیز باید Windows Server 2008 R2 انتخاب شود.



شکل ۶-۱۳

### تنظیم سطح عملکرد دامنه ( Set Domain Functional Level )

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

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

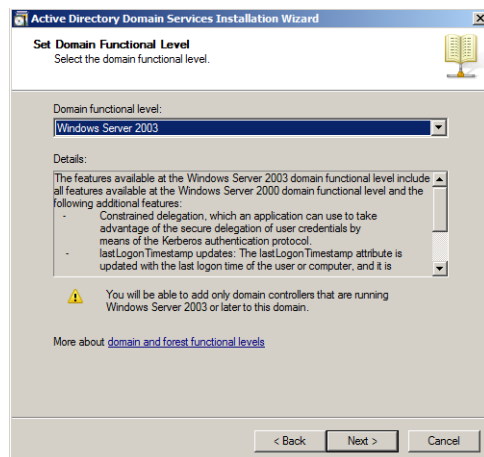
با انتخاب هر سطح می‌توان از DCهایی که دارای نسخه‌های بالاتر و یا یکسان با سطح مورد نظر هستند استفاده کرد. به عنوان مثال با انتخاب سطح Windows Server 2008 می‌توان از سیستم‌عامل‌های ویندوز سرور 2008 و 2008R2 به عنوان DC استفاده نمود.

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

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

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

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

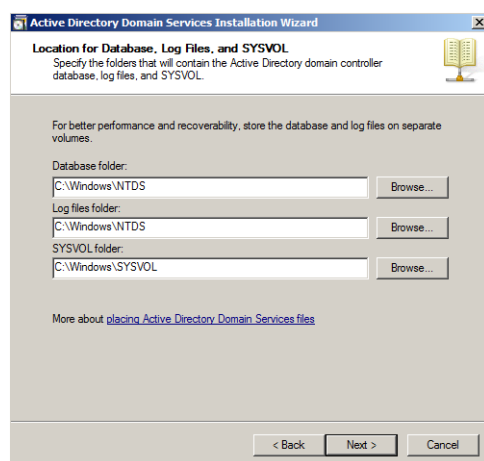


شکل ۶-۱۴

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

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

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



شکل ۶-۱۵

در اصل، اکتیو دایرکتوری یک پایگاه داده عظیم است که شامل فایل داده اصلی و یک فایل مربوط به تراکنش های Log (ورود) می باشد. تغییراتی که در این پایگاه داده اعمال می شوند، ابتدا بر روی فایل تراکنش Log نوشته شده و سپس این فایل ها به صورت دوره ای مورد بررسی قرار می گیرند. این کار در واقع روشی برای اعلام ایجاد تغییرات بر روی پایگاه داده می باشد.

تراکنش های Log، امکان تحمل خطا و قابلیت بازیابی مطمئنی را برای پایگاه داده اکتیو دایرکتوری فراهم می کنند. زمانی که سرور در اثر ایجاد یک تغییر در اکتیو دایرکتوری عملکردش را از دست می دهد، با استفاده از Log و بررسی موفق یا عدم موفق بودن اعمال یک تغییر می تواند مطمئن شود که پایگاه داده در زمان Boot شدن سرور در وضعیت مناسب و سازگاری قرار دارد.

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

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

در این پیکربندی هر درایو نیازمند یک دیسک فیزیکی می باشد، زیرا استفاده از یک درایو با سه پارتیشن بهبود چندانی در کارایی ایجاد نمی کند. چنانچه دیسک های انتخابی شما از سرعت های متفاوتی برخوردار هستند باید سریع ترین دیسک را به سیستم عامل، دیسکی که سرعت کمتری دارد را به فایل تراکنش log، و کندترین دیسک را نیز به فایل پایگاه داده اکتیو دایرکتوری و SYSVOL اختصاص دهید. علت این کار این است که سیستم عامل و فایل تراکنش log از عملکرد سنگین تری برخوردار هستند.

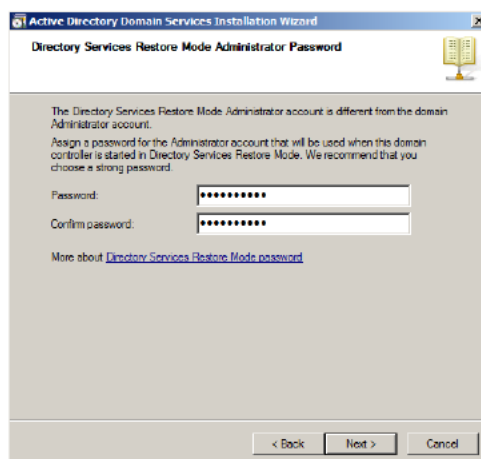
اجازه دهید مثالی در این رابطه ارائه دهیم. فرض کنید تعداد کاربران دامنه شما ۱۰۰ کاربر هستند. در این صورت می توانید فایل پایگاه داده و log را در همان دیسک سیستم عامل (C:\) قرار دهید بدون اینکه مشکلی در کارایی بوجود آید. اما حالتی را در نظر بگیرید که تعداد کاربران ۵۰,۰۰۰ کاربر باشند. در این صورت باید برای کاهش فشار و بهینه سازی عملکرد، فایل های log و پایگاه داده را در درایوهای متفاوتی ذخیره کنید.



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

### رمز عبور مدیر Directory Services Restore Mode

اگر نیاز به نگهداری یا بازسازی اکتیو دایرکتوری داشته باشید، باید این کار را با استفاده از Directory Services Restore Mode (DSRM) انجام دهید. برای دسترسی به این حالت باید در هنگام راه‌اندازی سرور کلید F8 را فشار دهید تا به منوی تنظیمات پیشرفته<sup>۱</sup> هدایت شوید. سپس در این منو باید گزینه Directory Services Restore Mode را انتخاب نموده و enter را فشار دهید. با ورود به حالت DSRM چون هنوز اکتیو دایرکتوری اجرا نشده است، نمی‌توانید با یک حساب کاربری به آن وارد شوید. در عوض می‌توانید برای مدیریت، از یک حساب کاربری مخصوص با رمز عبوری متفاوت استفاده کنید. در DCPromo باید رمز عبور این حساب کاربری را مشخص کنید. در شکل زیر پنجره مربوطه ("Directory Services Restore Mode Administrator Password") نشان داده شده است.



شکل ۶-۱۶

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



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

### اجرای DCPromo

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

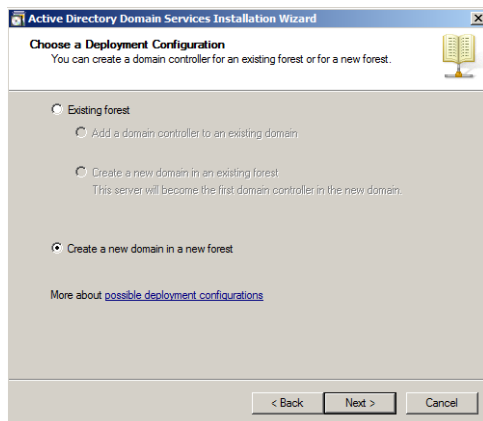
قبل از اجرای DCPromo لازم است تمام Role‌هایی که نصب کرده‌اید را حذف کنید، زیرا این ویزارد باید قبل از نصب هر Role دیگری اجرا شود. جهت تبدیل سرور به DC (و ایجاد جنگل تک دامنه‌ای) مراحل زیر را دنبال کنید:

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



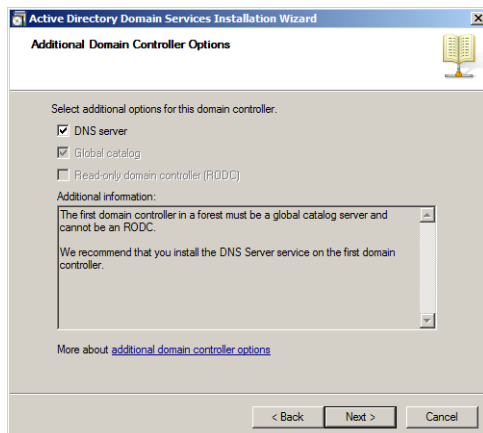
شکل ۶-۱۷

۴. در صفحه “Operating System Capability”، اطلاعات مربوط به سازگاری سیستم عامل‌های قابل اتصال به DC را مشاهده نموده و بروی Next کلیک کنید (شکل ۶-۹).
۵. در صفحه “Choose a Deployment Configuration” گزینه Create a new domain in a new Forest را انتخاب نموده و بروی Next کلیک کنید.



شکل ۶-۱۸

۶. در صفحه "Name the Forest Root Domain" (شکل ۶-۱۱)، نام FQDN دامنه را وارد نموده و بر روی Next کلیک کنید (در اینجا از Bigfirm.com استفاده شده است).
۷. در صفحه "Set Forest Functional Level"، گزینه Windows Server 2003 را انتخاب و بر روی Next کلیک کنید (شکل ۶-۱۳).
۸. در صفحه "Set Domain Functional Level"، گزینه Windows Server 2003 را انتخاب و بر روی Next کلیک کنید (شکل ۶-۱۴).
۹. در صفحه "Additional Domain Controller Options"، مطمئن شوید که گزینه DNS انتخاب شده است. با انتخاب این گزینه DCPromo سرویس DNS را به همراه خود نصب می‌کند. دقت داشته باشید که گزینه Global Catalog بطور پیش‌فرض انتخاب شده است ولی قابل تغییر نیست. علت این است که اولین DC در دامنه به عنوان Global Catalog Server (GC Server) در نظر گرفته می‌شود.



شکل ۶-۱۹



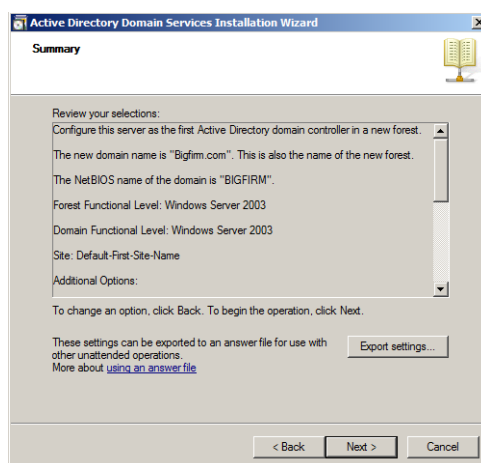
۱۰. اگر در تنظیمات TCP/IP دریافت آدرس IP (IPv4 یا IPv6) از سرور DHCP و به صورت خودکار باشد، پیغامی ظاهر شده و اعلام می‌کند که کارت شبکه سرور دارای آدرس IP ایستا<sup>۱</sup> (ثابت) نیست. پیشنهاد می‌شود که یک آدرس ایستا (با انتخاب گزینه No, I will assign static IP addresses) به آن اختصاص دهید. در صورتی که این آدرس IPv4 را در اختیار دارید وارد نموده و همچنین IPv6 را نیز فعال کنید. در غیر اینصورت بر روی Yes, the computer will use an IP address automatically assigned by DHCP server کلیک کنید تا فرایند نصب ادامه یابد (شکل ۶-۸).

۱۱. DCPromo سعی می‌کند که یک سرور DNS را موقعیتیابی کند. چنانچه سروری وجود نداشته باشد، پیغامی ظاهر شده و اعلام می‌کند که برای دامنه هیچ Zone ای ایجاد نشده است. این پیغام عادی است. DCPromo، سرور DNS را پیکربندی خواهد نمود. بر روی Yes کلیک کنید تا فرایند نصب ادامه پیدا کند (شکل ۶-۱۲).

۱۲. در صفحه “Location for Database, Log Files, and SYSVOL” باید محل قرارگیری فایل‌های پایگاه داده، فایل‌های log و همچنین SYSVOL را تعیین کنید. بهتر است از همین مسیرهای پیش فرض استفاده کنید. بر روی Next کلیک کنید (شکل ۶-۱۵).

۱۳. در صفحه “Directory Services Restore Mode Administrator Password”، رمز عبور مدیر DSRM را وارد کنید. برای امنیت بیشتر این رمز را ترکیبی از حروف، اعداد و علائم انتخاب کنید (مانند P@ssw0rd). بر روی Next کلیک کنید (شکل ۶-۱۶).

۱۴. در صفحه “Summary” خلاصه‌ای از تنظیمات انجام شده نشان داده می‌شود. این تنظیمات چیزی شبیه شکل ۶-۱۹ خواهد بود.



شکل ۶-۲۰

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



شکل ۶-۲۱

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

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

۱. در صفحه "Summary" از DCPromo، بر روی دکمه Export Setting کلیک کنید. این دکمه تنظیمات انجام شده توسط شما را در قالب یک فایل پاسخ ذخیره می‌کند.
  ۲. پنجره "Save unattend file" ظاهر می‌شود. نام DCPromoexport و مسیر C:\ (ریشه درایو C) را جهت ذخیره فایل انتخاب نموده و بر روی Save کلیک کنید.
  ۳. از مسیر « Start » Comand Prompt خط فرمان (Cmd) را اجرا کنید.
  ۴. در Cmd، عبارت cd\ را تایپ نموده و enter را فشار دهید.
  ۵. عبارت notepad DCPromoexport.txt را تایپ نموده و enter را فشار دهید. برنامه Notepad اجرا شده و محتویات فایل پاسخی که ایجاد نموده‌اید را نشان می‌دهد. در این فایل خطوطی که با علامت (;) شروع می‌شوند جنبه توضیحی داشته و نادیده گرفته می‌شوند.
- توجه داشته باشید که در مقابل عبارت SafeModeAdminPassword هیچ رمز عبوری وجود ندارد. پس از علامت مساوی (=) در این خط، یک رمز عبور مانند P@ssw0rd وارد کنید. این خط باید چیزی شبیه زیر باشد:

**SafeModeAdminPassword=P@ssw0rd**

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

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

### ۳-۶ افزودن DC ثانویه

گاهی اوقات نیاز است که یک DC ثانویه به دامنه اضافه کنید. افزودن DC ثانویه ممکن است به دلایلی مثل ایجاد پشتیبان برای DC اصلی انجام شود. زمانی که از یک DC در شبکه استفاده می‌کنید، چنانچه در عملکرد این DC اختلالی بوجود آید یا از کار بیفتد، عملکرد کل شبکه با مشکل مواجه می‌شود، بنابراین این DC می‌تواند به یک نقطه شکست در شبکه تبدیل شود. اکنون حالتی را در نظر بگیرید که از یک DC ثانویه نیز به عنوان پشتیبانی برای DC اصلی استفاده می‌شود. اگر DC اصلی از کار بیفتد، هنوز می‌توان از DC ثانویه استفاده کرد و در واقع عملکرد شبکه بر دوش این DC قرار داده می‌شود. کاربران به راحتی می‌توانند درخواست‌های خود را برای سرویس‌های مختلف ارائه داده و بدون احساس هیچگونه تغییر در روند پاسخگویی، به سرویس مورد نظر دسترسی پیدا کنند. بازگردانی DC از کار افتاده نیز در این حالت ساده خواهد بود، کافی است آخرین پشتیبانی که از اکتیو دایرکتوری گرفته شده است را بر روی این DC اجرا نموده و وضعیت آنرا به حالت اولیه بازگردانید. بطور کلی هیچ نگرانی در رابطه با توقف شبکه زمانی که از دو DC استفاده می‌کنید وجود نخواهد داشت.

برای ایجاد DC ثانویه باید ابتدا DC اولیه را ایجاد و پیکربندی نموده و سپس با اجرای DCPromo بر روی سروری که قرار است به عنوان DC ثانویه استفاده شود، آنرا به DC تبدیل کنید. برای ایجاد DC ثانویه باید یک حساب کاربری که دارای مجوز مدیر دامنه می‌باشد تهیه نموده و با در نظر گرفتن موارد زیر ویزارد DCPromo را اجرا کنید.

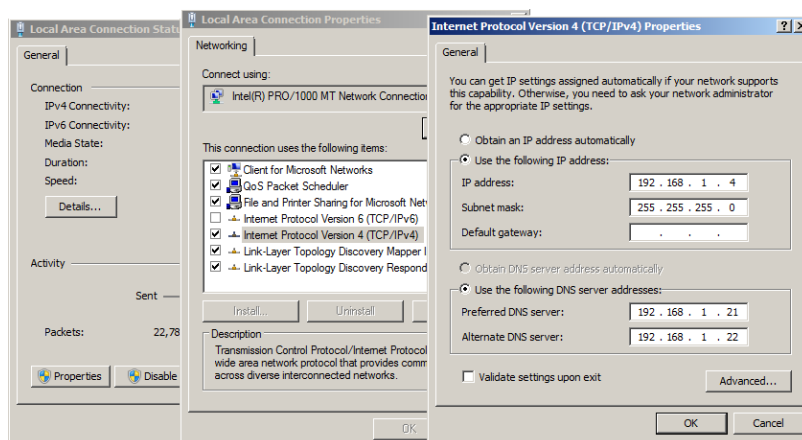
- ♦ Deployment Configuration
- ♦ پیکربندی DNS
- ♦ Global Catalog

در ادامه این موارد را مورد بررسی قرار می‌دهیم.

### قبل از اجرای DCPromo

کامپیوتری که قصد دارید آنرا به DC تبدیل کنید، نیازمند تنظیمات پیکربندی DNS در دامنه می‌باشد. همانند اولین DC که نیازمند آدرس IP ایستا بود، دومین DC نیز به آدرس IP ایستا نیاز دارد. برای اختصاص این آدرس IP به DC، باید به تنظیمات TCP/IP وارد شوید. برای دسترسی به این تنظیمات مراحل زیر را دنبال کنید:

۱. از منوی Start بروی Network کلیک‌راست نموده و Properties را انتخاب کنید.
۲. بروی Local Area Connection کلیک نموده و گزینه Properties را انتخاب کنید.
۳. گزینه Internet Protocol Version 4 (TCP/IPv4) را انتخاب نموده و بروی Properties کلیک کنید.
۴. گزینه Use the following IP address را انتخاب نموده و آدرس IP مورد نظر را وارد کنید. همچنین با انتخاب گزینه Use the following DNS server address آدرس سرور DNS در دامنه را وارد نمایید. در این مثال آدرس سرور DNS در شبکه 192.168.1.21 می‌باشد.



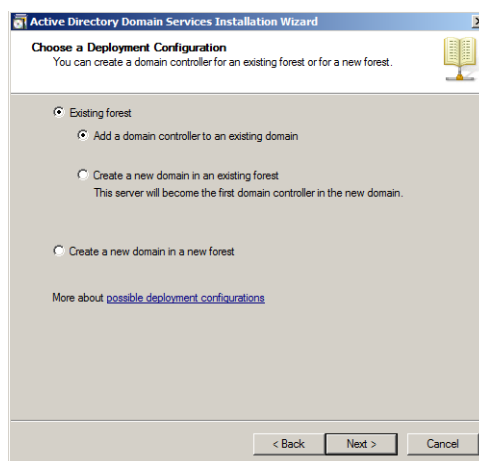
شکل ۶-۲۲

۵. بروی OK کلیک نموده و تمام پنجره‌ها را ببندید.
- چنانچه سرور شما عضوی از دامنه نباشد، طی فرایند DCPromo به دامنه مورد نظر متصل می‌شود، بنابراین نیازی نیست که قبل از اجرای DCPromo آنرا به دامنه متصل کنید.

### Deployment Configuration برای DC ثانویه

زمانی که در حال اجرای DCPromo بروی DC ثانویه هستید، گزینه‌های “Existing forest” و “Add a domain controller to an existing domain” را طبق شکل زیر انتخاب کنید. برای هر DC ای که قصد

دارید اضافه کنید، باید همین گزینه‌ها را در طی فرایند DCPromo برای آنها انتخاب نمایید. چنانچه قصد دارید در جنگل دامنه‌های فرزند<sup>۱</sup> ایجاد کنید، باید گزینه “Create a new domain in an existing forest” را انتخاب کنید.



شکل ۶-۲۳

### پیکربندی DNS برای DC ثانویه

همانند DC اولیه، پیکربندی DNS برای DC ثانویه نیز ضروری می‌باشد. چنانچه DC اولیه سرور DNS را اجرا کند، DC ثانویه نیز باید از سرور DNS استفاده کند. این کار با استفاده از Zone‌های یکپارچه با اکتیو دایرکتوری (ADI Zones) که در DC اول ایجاد می‌شود، انجام می‌شود. با افزودن سرور DNS به DC ثانویه، مقداری سربار برای سرور DNS ایجاد می‌شود. برای حفظ تعادل می‌توانید یک سرور DNS دیگر نیز اضافه کنید.

بخاطر داشته باشید که اکتیو دایرکتوری به شدت وابسته به DNS می‌باشد. سرویس‌ها برای یافتن DC و کاربران در طول شبکه، از رکوردهای SRV در سرور DNS استفاده می‌کنند. چنانچه DNS را به DC اول اضافه نموده ولی به DC ثانویه اضافه نکنید، اگر DC اول با شکست مواجه شود، چون DC دوم نمی‌تواند از DNS استفاده کند بنابراین کل شبکه نمی‌تواند از DNS استفاده کند و در نتیجه با شکست مواجه می‌شود. وجود یک DC بدون سرور DNS ای که بتواند موقعیت آنرا تشخیص دهد مثل این است که در اصل هیچ DC در شبکه وجود ندارد.

با وجود دو سرور DNS، همه کاربران می‌توانند از این دو سرور استفاده کنند. بدین منظور باید بر روی کامپیوترهای آنها هر دوی این سرورها پیکربندی شوند. بنابراین یکی از آنها به عنوان

1. Child Domain

Preferred DNS (اصلی) و دیگری به عنوان Alternate DNS (جایگزین) در نظر گرفته می‌شوند. کاربران تنها زمانی می‌توانند از سرور جایگزین استفاده کنند که سرور اصلی با شکست مواجه شده و یا قادر به پاسخگویی نباشد.

فرض کنید در شبکه دو سرور با نام‌های BF1 و BF2 به عنوان DC، با استفاده از ADI DNS پیکربندی نموده‌اید. می‌توانید نیمی از کاربران را با تنظیمات زیر:

- ◆ Preferred DNS server: BF1
- ◆ Alternate DNS server: BF2

و نیمه دیگر را با تنظیمات زیر پیکربندی کنید:

- ◆ Preferred DNS server: BF2
- ◆ Alternate DNS server: BF1

(Preferred DNS server: BF1 یعنی اینکه کاربران یک DC با نام BF1 از سرور DNS اصلی استفاده کنند)

### Global Catalog برای DC ثانویه

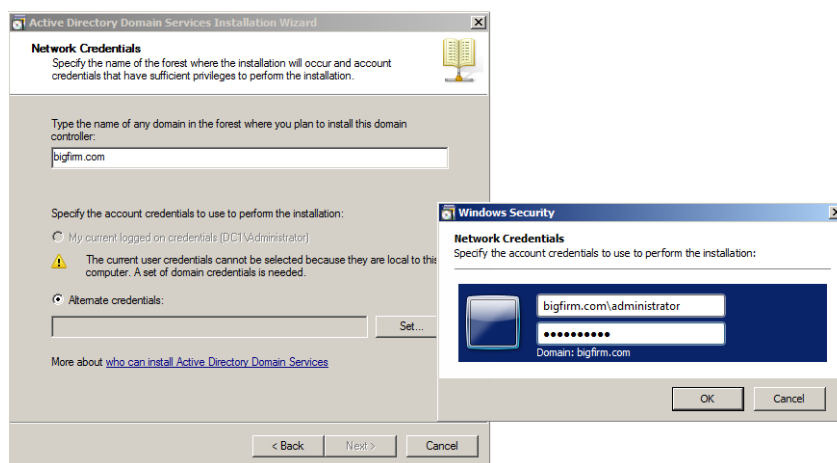
همانند DC اول، DC ثانویه نیز باید یک سرور GC باشد. زمانی که یک جنگل تک دامنه‌ای ایجاد می‌کنید، باید تمام DC‌های شما یک سرور GC نیز باشند. این سرورها به شما اطمینان می‌دهند که در صورت شکست یک DC می‌توان از تمام قابلیت‌های سایر DC‌ها استفاده نمود (دقت داشته باشید که ایجاد سرورهای GC هیچ هزینه اضافی ندارد).

### اجرای DCPromo برای DC ثانویه

برای تبدیل یک سرور به DC ثانویه مراحل زیر را دنبال کنید (در این مراحل فرض بر این است که سرور عضو هیچ دامنه‌ای نیست. اگر سرور شما عضو دامنه باشد ممکن است مراحل کمی متفاوت‌تر باشند):

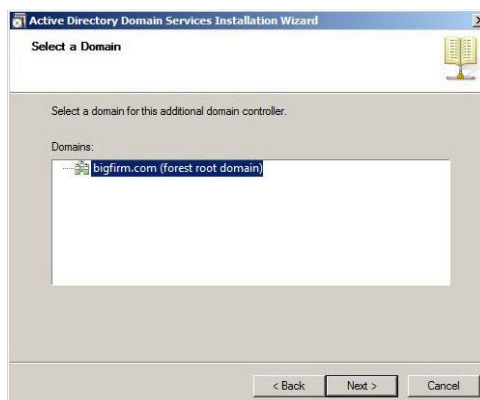
۱. ابتدا با حساب کاربری که دارای مجوز مدیریت سرور (Administrator) است وارد شوید.
۲. در قسمت جستجوی منوی Start، عبارت DCPromo را وارد نموده و enter را فشار دهید.
۳. با مشاهده صفحه خوشامدگویی، بر روی Next کلیک کنید.
۴. در صفحه "Operating System Compatibility" بر روی Next کلیک کنید.
۵. در صفحه "Choose a Deployment Configuration" گزینه Existing forest را انتخاب نموده و مطمئن شوید که گزینه Add a domain controller to an existing domain انتخاب شده است. بر روی Next کلیک کنید.
۶. در صفحه "Network Credentials" نام دامنه فعلی (دامنه‌ای که وجود دارد) را وارد کنید (در اینجا از نام bigfirm.com استفاده شده است).

۷. چنانچه سرور شما عضو دامنه نباشد، باید آنرا به دامنه مورد نظر متصل کنید. برای این کار بر روی دکمه Set کلیک کنید. در پنجره باز شده، مشخصات حساب کاربری که دارای مجوز مدیریت دامنه (در اینجا bigfirm.com) است را وارد نموده و بر روی OK کلیک کنید. در نهایت بر روی Next کلیک کنید.



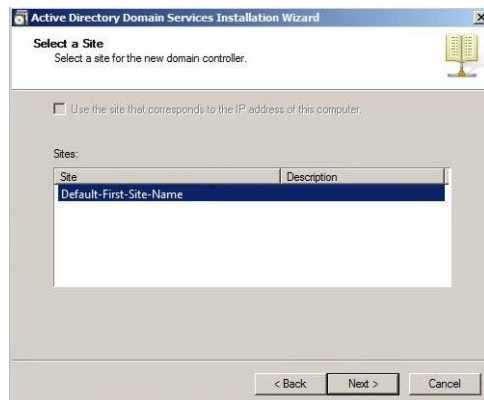
شکل ۶-۲۴

۸. در صفحه "Select a Domain" مطمئن شوید که دامنه مورد نظر انتخاب شده است و بر روی Next کلیک کنید.



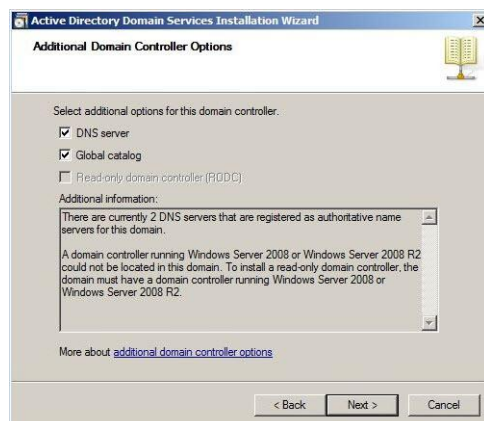
شکل ۶-۲۵

۹. در صفحه "Select a Site"، سایت پیش فرض را انتخاب نموده و بر روی Next کلیک کنید (زمانی که چند سایت وجود داشته باشد، سایت مورد نظر برای DC بطور خودکار انتخاب می شود).



شکل ۶-۲۶

۱۰. در صفحه “Additional Domain Controller Options”، هر دو گزینه DNS و Global Catalog را انتخاب کنید.



شکل ۶-۲۷

۱۱. اگر با هشدار مربوط به Delegation در DNS مواجه شدید، بر روی Yes کلیک کنید.

۱۲. در صفحه “Location for Database, Log Files, and SYSVOL” بر روی Next کلیک کنید تا مسیرهای پیش فرض برای قرارگیری فایل ها انتخاب شوند.

۱۳. در صفحه “Directory Services Restore Mode Administrator Password”، رمزعبور DSRM را وارد نموده و بر روی Next کلیک کنید.

۱۴. در صفحه “Summary” خلاصه ای از تنظیمات انجام شده را مشاهده نموده و بر روی Next کلیک کنید. همانند ایجاد DC اولیه، می توان با استفاده از دکمه Export Settings یک فایل پاسخ برای DCPromo ایجاد نمود.



۱۵. با مشاهده صفحه زیر، فرایند نصب DC بر روی سرور آغاز شده است. با فعال کردن گزینه Reboot on completion سرور پس از اتمام عملیات Restart می‌شود.



شکل ۶-۲۸

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

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

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

#### ۶-۴-۱ ایجاد واحدهای سازمانی

واحدهای سازمانی به منظور سازماندهی اشیاء در اکتیو دایرکتوری مورد استفاده قرار می‌گیرند. هر شیء (مانند کاربر، کامپیوتر، گروه و ...) جهت مدیریت آسانتر می‌تواند در OU قرار گیرد. معمولاً OUها بر طبق بخش‌های سازمان ایجاد می‌شوند. مثلاً (بخش فروش و ...) اما دو دلیل فنی که مدیران برای ایجاد OUها به کار می‌گیرند عبارتند از:

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

#### مدیریت گروه‌ها از طریق Group Policy

امکان پیوند اشیاء Group Policy (GPO) به سایت‌ها، دامنه‌ها و OUها وجود دارد. بنابراین اگر قصد دارید بر روی تعدادی از کاربران سیاست‌های خاصی را اعمال کنید می‌توانید حساب‌های آنها را در

یک OU قرار داده و سپس GPO را به این OU پیوند دهید.

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

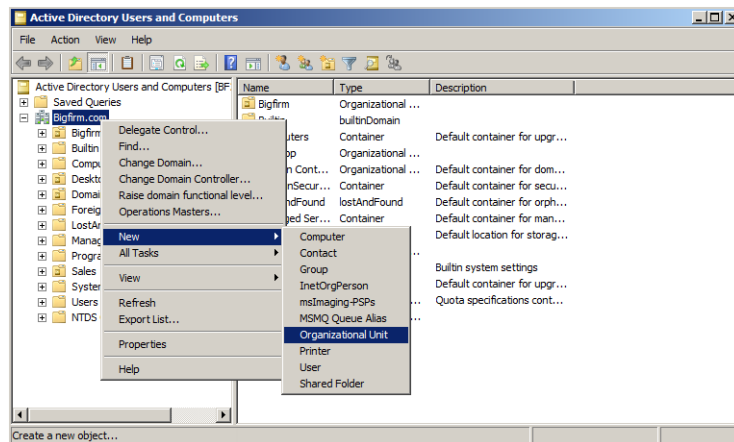
### مدیریت گروه‌ها از طریق Delegation (واگذاری)

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

### ایجاد OUها به کمک ADUC

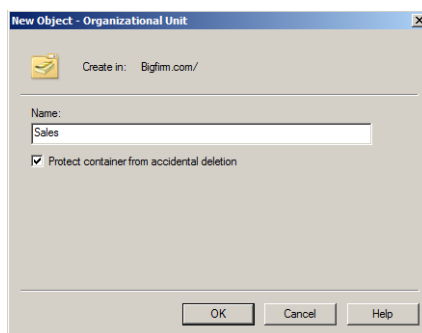
برای ایجاد OU با استفاده از ADUC مراحل زیر را دنبال کنید:

۱. ADUC را از مسیر «Start» «Administrative Tools» «Active Directory Users and Computers» اجرا کنید.
۲. بر روی نام دامنه کلیک‌راست نموده و «New» «Organizational Unit» را انتخاب کنید.



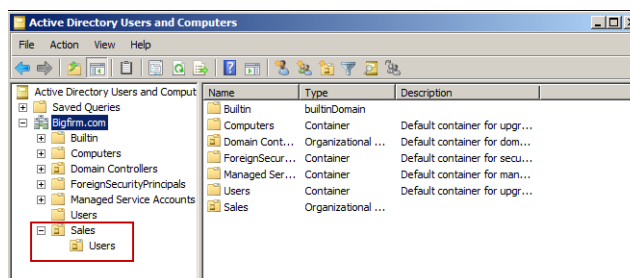
شکل ۶-۲۹

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



شکل ۳۰-۶

۴. چنانچه قصد داشته باشید در داخل یک OU (در اینجا Sales)، OU دیگری (OU فرزند) ایجاد کنید، کافی است بر روی نام OU کلیک راست نموده و «New Organization Unit» را انتخاب کنید. سپس نام آنرا وارد نموده (در اینجا Users) و بر روی OK کلیک کنید. نام این OU در زیر نام OU اصلی قابل مشاهده می باشد.



شکل ۳۱-۶

### نام‌های ممتاز LDAP

اکتیو دایرکتوری برای برقراری ارتباط از پروتکلی با نام LDAP<sup>۱</sup> استفاده می کند. این پروتکل برای متمایز کردن اشیاء اکتیو دایرکتوری از یک سری نام‌های ممتاز<sup>۲</sup> (DN) استفاده می کند که آشنایی با اجزای آن جهت ایجاد اشیاء به کمک خط فرمان ضروری می باشد.

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

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

چندین نوع شیء است که بوسیله کاما از یکدیگر جدا شده‌اند. به عنوان مثال نام دامنه Bigfirm.com از دو جزء bigfirm و com تشکیل شده است که به صورت `dc=bigfirm,dc=com` شناخته می‌شود. واحدهای سازمانی دارای نوع `ou`، و کانتینر `Users` و `Computers` نیز دارای نوع `cn` می‌باشند، بدین ترتیب DN مربوط به واحد سازمانی Sales در دامنه Bigfirm.com به صورت زیر نمایش داده می‌شود:

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

کانتینر `Users` نیز دارای DN زیر می‌باشد:

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

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

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

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

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

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

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

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

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

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

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

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

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

`CN=maria,OU=users,OU=sales,DC=BigFirm,DC=Com`

## ایجاد OUها به کمک DSAdd (خط فرمان)

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

- ♦ OU
- ♦ User
- ♦ Computer
- ♦ Group
- ♦ Contact

دستوراتی که برای ایجاد هریک از این اشیاء استفاده می‌شود، در جدول ۶-۱ آورده شده است.

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

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

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

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

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

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

```
notepad DSAddhelp.txt
```

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

```
DSAdd ou DN
```

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

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

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

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

### ایجاد OUها به کمک WSH

در ویندوز، برنامه‌ای به نام “میزبان اسکریپ نویسی ویندوز”<sup>۱</sup> یا WSH فراهم شده است که به کمک آن می‌توان اشیائی مانند OU را ایجاد نمود. در استفاده از این اسکریپت‌ها جای نگرانی نیست زیرا نیازی به دانستن برنامه نویسی حرفه‌ای ندارید. کافی است اسکریپت‌های مورد نظر را پیدا نموده و با کمی تغییرات در آن مورد استفاده قرار دهید. اسکریپت نویسی در ویندوز فراتر از آن است که بتوان در قالب یک پاراگراف آنرا شرح داد ولی یکی از منابعی که در این زمینه می‌توانید از آن استفاده نمایید، سایت شرکت مایکروسافت و لینک <http://technet.microsoft.com/en-us/scriptcenter/default.aspx> می‌باشد. با کمی جستجو در این سایت قادر خواهید بود به اسکریپت‌های مورد نظر دست پیدا کنید. برای ایجاد این دسته از فایل‌ها می‌توانید اسکریپت‌های مورد نظر را در برنامه Notepad وارد نموده و سپس با پسوند vbs ذخیره کنید. پس از آن می‌توانید فایل را در خط فرمان اجرا کنید. به عنوان مثال دستورات زیر را در Notepad وارد نموده و با نام CreateOU.vbs ذخیره نمایید:

```
Set objDom = GetObject("LDAP://dc=bigfirm,dc=com")
Set objOU = objDom.Create("OrganizationalUnit","ou=SalesWSH")
objOU.SetInfo
Msgbox "Creating an OU", vbInformation, "Woo Hoo!"
```

♦ اولین خط این دستور، متغیری به نام objDom (که مخفف “object of type domain” است) را ایجاد می‌کند. نام دامنه با استفاده از دستور GetObject بازیابی شده و در این متغیر ذخیره می‌شود.

دقت داشته باشید که WSH حساس به حروف است بنابراین LDAP باید با حروف بزرگ نوشته شود. برای دامنه‌های مختلف می‌توانید مقادیر مقابل dc را تغییر دهید. به عنوان مثال چنانچه دامنه شما به صورت test.com باشد، عبارت داخل پرانتز به صورت "LDAP://dc=test,dc=com" خواهد بود.

- ♦ خط دوم، متغیری به نام objOU (که مخفف "object of type OU" است) را ایجاد نموده، سپس با استفاده از متد objDom، آنچه که قصد دارید ایجاد کنید را شناسایی می‌کند. متغیرهای داخل پرانتز با مقادیر "OrganizationalUnit", "ou=SalesWSH" نیز برای شناساندن نام ممتاز OU=SalesWSH (DN) استفاده می‌شوند.
- ♦ در خط سوم، SetInfo متدی است که در حقیقت شیئی که در متد Create در خط دوم شناخته شد را ایجاد می‌کند. در این لحظه ایجاد OU به اتمام می‌رسد.
- ♦ چهارمین خط، یک پنجره پیغام نشان داده و تعدادی بازخورد<sup>۲</sup> به شما ارائه می‌دهد. متنی که در میان علامت نقل قول اول قرار دارد، پیغامی است که پس از ایجاد OU نشان داده می‌شود. عبارت vbInformation نیز مشخص می‌کند که علامت اطلاعات (که با یک i در داخل دایره‌ای آبی رنگ) نشان داده شود. متنی که در علامت نقل قول دوم قرار دارد نیز عنوان پنجره پیغام را مشخص می‌کند.

### ایجاد OU به کمک PowerShell

امکان ایجاد OUها با استفاده از PowerShell نیز وجود دارد. این ابزار بطور پیش‌فرض در ویندوز سرور 2008R2 نصب شده است و از مسیر Start « All Programs « Accessories « Windows PowerShell « Windows PowerShell قابل دسترسی می‌باشد.

زمانی که PowerShell را اجرا می‌کنید، عبارت PS C:\Users\Administrator> را قبل از نوشتن هر دستور مشاهده می‌کنید (با فرض اینکه به صورت مدیر یا Administrator وارد شده باشید). با وارد کردن دستورات زیر در این ابزار می‌توانید یک OU با نام PS\_OU ایجاد کنید. برای دامنه‌های مختلف ممکن است نیاز داشته باشید که در خط اول تغییراتی ایجاد کنید. فقط دقت داشته باشید که بعضی از دستورات نسبت به کوچک یا بزرگی حروف حساس هستند و باید با دقت نوشته شوند. به عنوان مثال LDAP در دستورات زیر باید با حروف بزرگ نوشته شود:

```
$DCCon = "LDAP://Bf1/DC=BigFirm,DC=Com"
$AD = [adsis] $DCCon
$OU = $AD.Create("OrganizationalUnit", "OU=PS_OU")
$OU.SetInfo()
```

---

1. Method  
2. Feedback

در این دستورات حتی نباید یک کاما یا پرانتز اشتباه نوشته شود زیرا باعث می‌شود که دستورات به درستی عمل نکرده و یا نتایج متفاوت‌تری بدست آید.

- خط اول در دستورات بالا با متغیر \$DCCon شروع شده است. در این خط BF1 نام DC است که بر روی دامنه Bigfirm.com قرار دارد. این نام در متغیر \$DCCon ذخیره می‌شود.
- دومین خط متغیری به نام \$AD ایجاد نموده و از “اینترفیس خدمات اکتیو دایرکتوری”<sup>۱</sup> (ADSI) به منظور ارتباط با نمونه مشخص شده در متغیر \$DCCon استفاده می‌کند.
- پس از آن، متغیر \$OU ایجاد شده و از متد Create در ADSI، برای نشان دادن OU ای که دارای نام PS\_OU بوده و قصد دارید آنرا ایجاد کنید، استفاده می‌کند. در این مرحله هنوز OU ایجاد نشده است و فقط مشخص می‌شود که شما قصد دارید چه چیزی را ایجاد کنید.
- متد SetInfo() در خط آخر، OU را ایجاد می‌کند.

شاید از نظر شما استفاده از این دستورات جهت ایجاد اشیاء در حالی که می‌توان با استفاده از چندین کلیک در Active Directory Users and Computers به راحتی آنها را ایجاد نمود، کار خوشایندی نباشد. اما باید به این نکته توجه داشته باشید که با استفاده از این دستورات در PowerShell می‌توان فرایند ایجاد OU یا هر شیء دیگری را خودکارسازی نمود. بنابراین می‌توانید ده‌ها OU را بدون اینکه نیاز به انجام کار خاصی داشته باشید و تنها با استفاده از اسکریپت‌هایی که از قبل آماده نموده‌اید ایجاد کنید.

جهت ایجاد و اجرای اسکریپت‌ها در PowerShell مراحل زیر را دنبال کنید:

۱. ابزار PowerShell را اجرا کنید.
۲. دستور زیر را وارد نموده و enter را فشار دهید تا فایل متنی ایجاد شده و در برنامه Notepad اجرا گردد:

**Notepad CreateOU.ps1**

۳. دستورات زیر را در این فایل وارد کنید. دقت داشته باشید که در اینجا دو OU با نام‌های Script\_OU1 و Script\_OU2 ایجاد می‌شود. چنانچه قصد دارید OUهای بیشتری ایجاد کنید، کافی است خطوط سوم و چهارم را Copy و Paste نموده و نام‌های OU را در آنها تغییر دهید:

```
$DCCon = "LDAP://BF1/DC=Bigfirm,DC=Com"
$AD = [adsis] $DCCon
$OU = $AD.Create("OrganizationalUnit", "OU=Script_OU1")
$OU.SetInfo()
$OU = $AD.Create("OrganizationalUnit", "OU=Script_OU2")
$OU.SetInfo()
```

1. Active Directory Services Interface



۴. کلیدهای Ctrl+S را فشار دهید تا فایل ذخیره شود.
- در این لحظه شما یک اسکریپت PowerShell دارید که می‌توانید آنرا اجرا کنید، اما این اسکریپت‌ها بدون دستکاری خطوط اول و دوم قادر به اجرا در هر محیطی نیستند.
۵. به PowerShell بازگشته و عبارت Get-ex را وارد کنید، سپس کلید tab را بر روی صفحه کلید فشار داده تا این عبارت به دستور Get-ExecutionPolicy تبدیل شود. کلید enter را فشار دهید.
- در نصب پیش‌فرض هنگام وارد کردن دستور بالا و فشردن enter، نتیجه Restricted ظاهر می‌شود که این به معنای محدود بودن مجوز اجرای دستورات در محیط PowerShell می‌باشد.
۶. برای تغییر سیاست اجرای دستور، عبارت زیر را وارد کنید:

**Set-ExecutionPolicy RemoteSigned**

- هنگامی که با پرسش Do you want to change the execution policy ? مواجه شدید، کلید Y را فشار دهید. با این کار امکان اجرای اسکریپت‌ها فعال می‌گردد.
۷. اکنون می‌توانید اسکریپت خود را اجرا کنید. چنانچه مسیر ذخیره شدن فایل را تغییر داده‌اید باید آنرا مشخص کنید که این کار با استفاده از نماد \ قابل انجام است. در اینجا مسیر فایل تغییر نکرده است پس برای اجرای آن دستور زیر را وارد کنید:

**\CreateOU.ps1**

(در صورتی که در مسیر اجرای این دستور مشکلی بوجود آمد از مسیر .\CreateOU.ps1 استفاده کنید.)

اکنون اگر به ADUC مراجعه کنید OUهای ایجاد شده قابل مشاهده می‌باشند. در صورت وقوع هر گونه خطا، به پیغامی که داده می‌شود توجه کنید. همانطور که گفتیم حتی یک کاما می‌تواند مانع از اجرای دستور شود.

## ۶-۴-۲ ایجاد حساب‌های کاربری و کامپیوتری

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

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

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

**Redircmp <DN>**

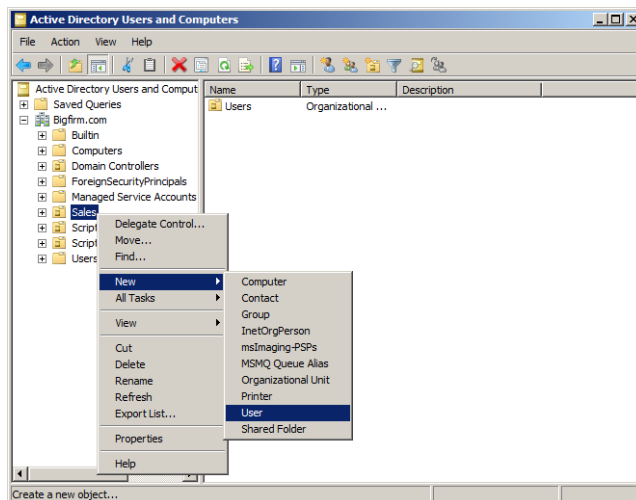
به عنوان مثال زمانی که یک کامپیوتر به دامنه متصل می‌شود، در صورتی که بخواهید حساب آن کامپیوتر در واحد سازمانی Sales ایجاد شود می‌توانید دستور زیر را وارد کنید:

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

### ایجاد حساب‌ها به کمک ADUC

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

۱. ADUC را از مسیر Start « Administrative Tools « Active Directory Users and Computers اجرا کنید.
۲. بروی واحد سازمانی Sales که اخیراً ایجاد کردید کلیک راست نموده و New « User را انتخاب کنید.



شکل ۶-۳۲

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

شکل ۳۳-۶

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

شکل ۳۴-۶

- ♦ چنانچه حساب کاربری توسط چندین کاربر مختلف استفاده می‌شود، گزینه "User cannot change password" را فعال کنید.
- ♦ در صورتی که قصد ندارید رمز عبور تعیین شده هرگز منقضی شود، گزینه "Password never expires" را فعال کنید.
- ♦ چنانچه فعلاً قصد فعال‌سازی این حساب کاربری را ندارید می‌توانید گزینه "Account is disabled" را فعال کنید.
- ۵. پس از انجام تنظیمات برروی Next کلیک کنید.
- ۶. در صفحه "Summary" خلاصه‌ای از تنظیمات انجام شده قابل مشاهده می‌باشد. برروی Finish

کلیک کنید.

### ایجاد حساب به کمک DSAdd (خط فرمان)

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

**DSAdd user <DN>**

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

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

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

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

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

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

شکل ۶-۳۵

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

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

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

```
dsadd user "cn=Maria Smith,OU=Sales,dc=Bigfirm,dc=Com" -samid "Maria.Smith" -upn "Maria.Smith@bigfirm.com" -fn "Maria" -ln "Smith" -display "Maria Smith" -pwd "p@ss0000" mustchpwd Yes
```

### ۳-۴-۶ ایجاد گروه‌ها

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

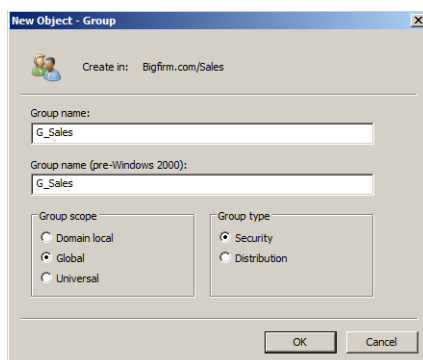
- دو نوع کلی برای گروه‌ها وجود دارد: Distribution (توزیع) و Security (امنیت). گروه‌های نوع Distribution برای ایمیل، و گروه‌های Security برای اعمال مجوزها و همچنین ایمیل استفاده می‌شوند. گروه‌ها علاوه بر نوع، دارای ناحیه<sup>۱</sup> نیز می‌باشند. این نواحی به سه دسته تقسیم می‌شوند:
- ♦ Global: متداول‌ترین نوع از گروه‌ها هستند که به منظور سازماندهی کاربران استفاده می‌شوند. می‌توان کاربران را در این گروه‌ها قرار داده و مجوزهای لازم را بر روی گروه اعمال نمود.

1. Scope

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

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

۱. ADUC را اجرا کنید.
۲. بر روی واحد سازمانی Sales کلیک‌راست نموده و «New Group» را انتخاب کنید.
۳. در فیلد "Group name" نام G\_Sales را وارد نموده و بر روی OK کلیک کنید.



شکل ۶-۳۶

۴. مجدداً بر روی واحد سازمانی Sales کلیک‌راست نموده و «New Group» را انتخاب کنید. این بار نام G\_SalesAdmins را وارد نموده و بر روی OK کلیک کنید. با استفاده از این گروه می‌توانید مجوزهای لازم را به مدیر واحد سازمانی OU بدهید.

### واگذاری<sup>۱</sup> کنترل

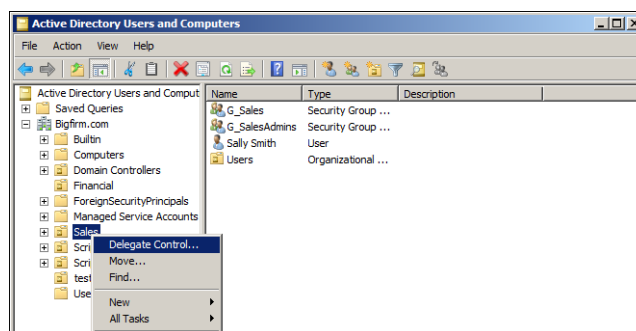
یکی از دلایل ایجاد OUها واگذاری کنترل تعدادی از کاربران به فرد (یا افرادی) می‌باشد. به عنوان مثال فرض کنید که کلیه اقدامات مدیریت IT در بخش فروش به دو کاربر واگذار شده است. این دو

1. Delegating

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

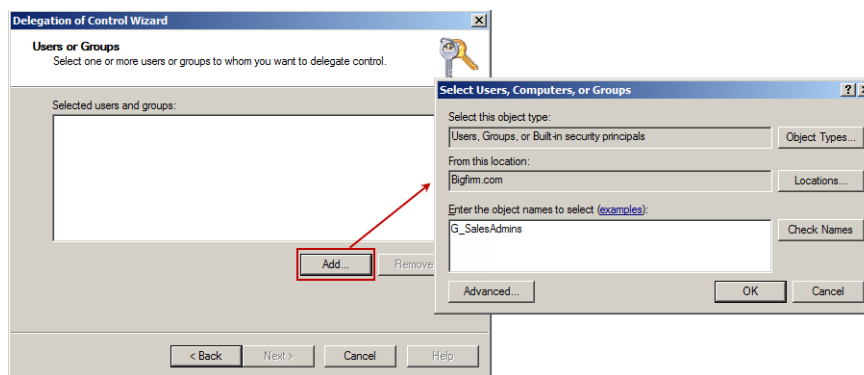
برای انجام این کار باید ابتدا یک واحد سازمانی با نام Sales ایجاد نموده و تمام کاربران و کامپیوترهای بخش فروش را در آن قرار دهید. همچنین باید یک گروه Global (مثلاً G\_SalesAdmins) ایجاد نموده و حساب کاربری مدیر IT بخش فروش را در آن قرار دهید. پس از انجام این اقدامات می‌توانید مراحل زیر را برای دادن مجوز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

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



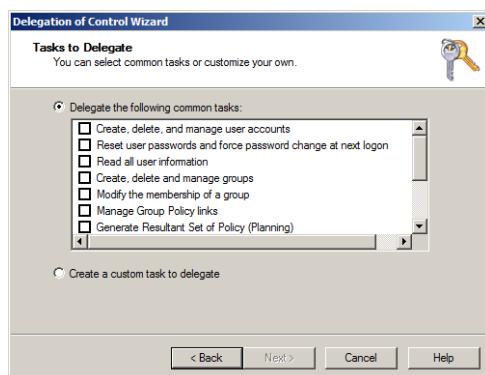
شکل ۶-۳۷

۳. در صفحه "Welcom to the Delegation of Control Wizard" بروی Next کلیک کنید.
۴. در صفحه "Users or Groups" بروی دکمه Add کلیک کنید.
۵. در قسمت "Enter the object names to select" نام G\_SalesAdmins را وارد نموده و بروی OK کلیک کنید.



شکل ۶-۳۸

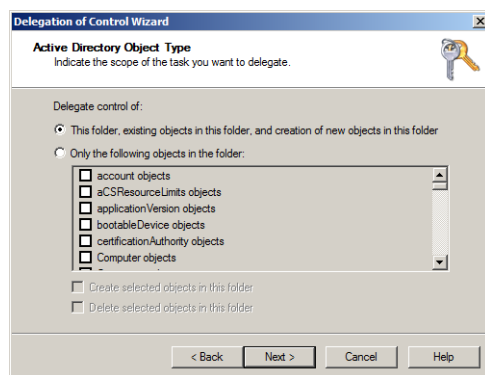
۶. بر روی Next کلیک کنید تا به صفحه "Tasks to Delegate" هدایت شوید. در این صفحه دو گزینه قابل انتخاب است. با انتخاب گزینه اول (Delegate the following common tasks) می‌توانید به لیستی از مجوزهای قابل اعمال بر روی گروه دسترسی پیدا کنید. با فعال کردن هر مجوز می‌توانید آنرا برای اختصاص دادن انتخاب کنید.



شکل ۳۹-۶

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

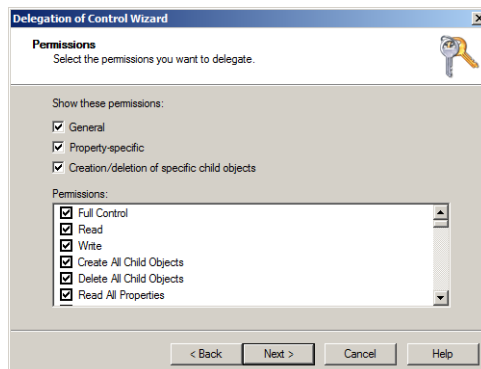
۸. در صفحه "Active Directory Object Type" نیز تعدادی گزینه وجود دارد. با استفاده از این گزینه‌ها می‌توانید مجوزها را به اشیاء خاصی مثل کاربران، کامپیوترها و ... محدود کنید. گزینه This folder, existing objects in this folder ... را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۴۰-۶

۹. در صفحه "Permissions" مجوز Full Control را در قسمت Permissions انتخاب نموده و سپس بر روی Next کلیک کنید.



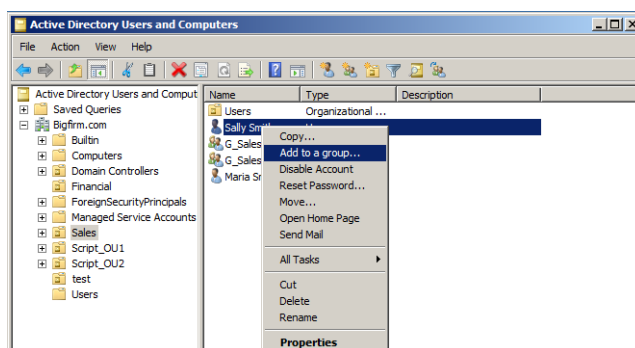


شکل ۴۱-۶

۱۰. در صفحه “Completing the Delegation”، خلاصه‌ای از تنظیمات را مشاهده نموده و بر روی Finish کلیک کنید.

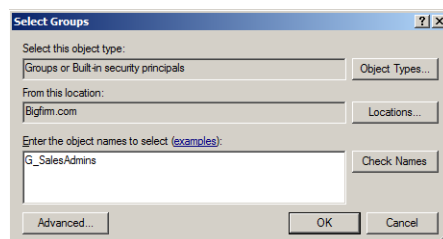
اکنون پس از ایجاد گروه لازم است که کاربران را به آن اضافه کنید. جهت افزودن کاربران به گروهی که اخیراً ایجاد نمودید مراحل زیر را دنبال کنید:

۱۱. در کنسول ADUC بر روی کاربر کلیک راست نموده و گزینه Add to a group را انتخاب کنید.



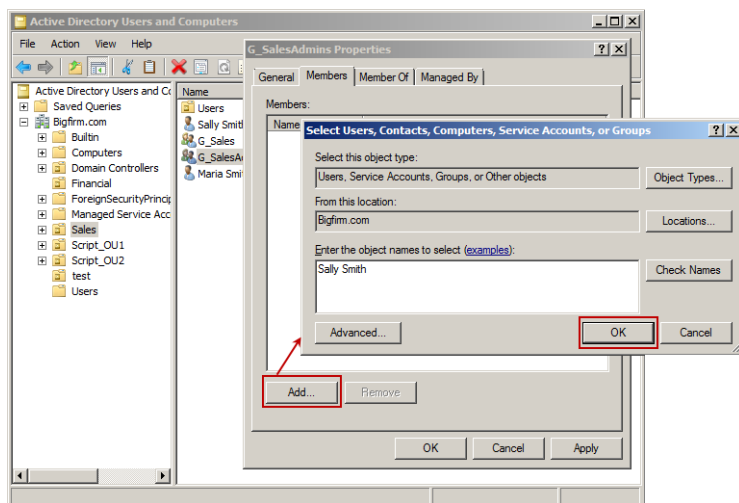
شکل ۴۲-۶

۱۲. در صفحه “Select Groups” نام گروه را وارد نموده و بر روی OK کلیک کنید.



شکل ۴۳-۶

افزودن کاربر به گروه از طریق تب Members در Properties گروه نیز امکان پذیر می باشد. در این تب باید پس از کلیک بر روی Add، نام کاربر را وارد نموده و بر روی OK کلیک کنید.



شکل ۴۴-۶

## ۵-۶ اقدامات نگهداری از دامنه

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

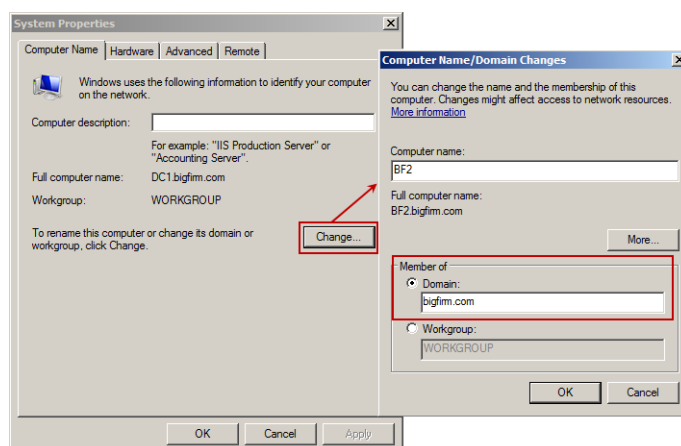
- ♦ پیوستن به یک دامنه
- ♦ انهدام یک DC
- ♦ عیب یابی ADI DNS
- ♦ افزایش سطح عملکرد دامنه و جنگل
- ♦ استفاده از NetDom

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

### ۵-۶-۱ پیوستن به یک دامنه

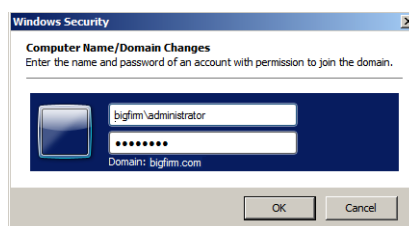
برای اتصال ویندوز سرور 2008R2 به یک دامنه، مراحل زیر را دنبال کنید (دقت داشته باشید زمانی که یک سرور به دامنه متصل می شود، از آن لحظه به بعد با مفهوم Member Server شناخته می شود):

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



شکل ۴۵-۶

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



شکل ۴۶-۶

۷. پس از مدت کوتاهی، پنجره خوشامدگویی نشان داده می‌شود. بر روی OK کلیک کنید.
۸. از شما خواسته می‌شود که کامپیوتر را Restart کنید. مجدداً بر روی OK کلیک کنید.
۹. بر روی Close کلیک نموده و پنجره "System Properties" را ببندید. بار دیگر به شما اعلام می‌شود

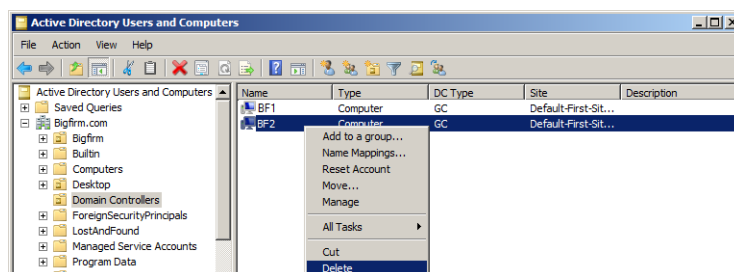
که سرور باید Restart شود. بر روی Restart Now کلیک کنید. پس از Restart، سرور به دامنه مورد نظر متصل شده و به عنوان یک Member Server شناخته می‌شود.

### ۶-۵-۲ انهدام یک DC

گاهی اوقات نیاز است که یکی از DCها را از حالت سرویس‌دهی خارج نمود. به این عمل "انهدام"<sup>۱</sup> گفته می‌شود. زمانی که یک DC را منهدم می‌کنید، کلیه اجزاء اکتیبو دایرکتوری در آن را حذف نموده و آنرا به یک Member Server تبدیل می‌کنید.

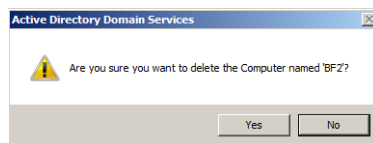
ساده‌ترین راه برای انهدام یک DC، راه‌اندازی DCPromo بر روی آن می‌باشد. البته پس از انهدام، سرور هنوز قادر به اجرا است ولی عملکردهای مورد انتظار (از یک DC) را نخواهد داشت. چنانچه به دلیل شکست سرور DC نتوان DCPromo را برای حذف آن اجرا نمود، می‌توانید از طریق اکتیبو دایرکتوری آنرا حذف کنید. با استفاده از ابزار Active Directory Users and Computers سادگی می‌توان عمل حذف یک DC را انجام داد. برای انجام این کار مراحل زیر را دنبال کنید:

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



شکل ۶-۴۷

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



شکل ۶-۴۸

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

شکل ۶-۴۹

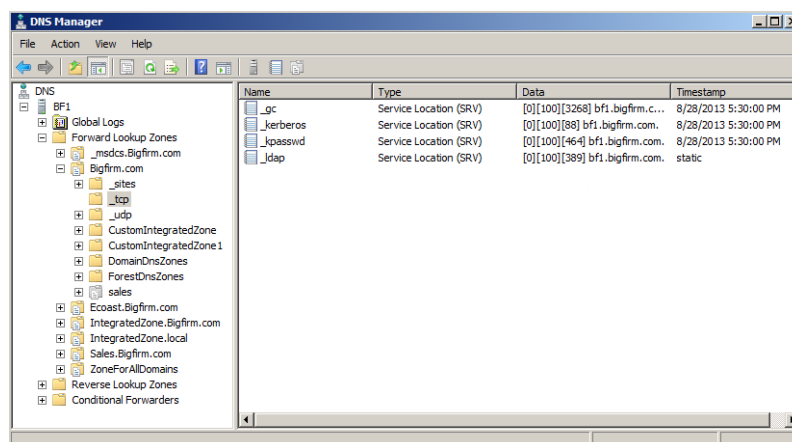
6. اگر بروی سرور، اقدامات اصلی (Operations Master Roles) نگهداری می‌شوند از شما خواسته می‌شود که آنها را به DC دیگری انتقال دهید. بروی OK کلیک کنید. پس از آن عملکرد این DC متوقف خواهد شد.

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

### ۳-۵-۶ عبیایی ADI DNS

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

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



شکل ۵۰-۶

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

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

سرویس NetLogon رکوردها را مجدداً ایجاد نموده و پس از آن می‌توانید از سرور DNS استفاده کنید.

### ۴-۵-۶ افزایش سطح عملکرد دامنه و جنگل

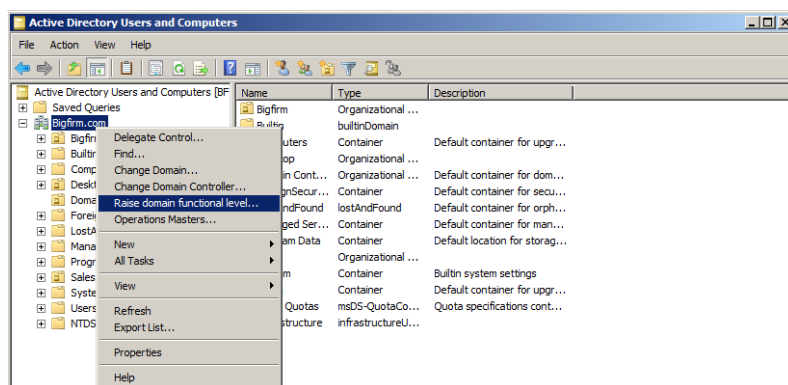
پس از ایجاد جنگل (Forest) ممکن است بخواهید سطح دامنه و یا جنگل را افزایش دهید. مهمترین دلیل انجام این کار استفاده از قابلیت‌ها و ویژگی‌های سطوح بالاتر می‌باشد. دقت داشته باشید زمانی که سطح عملکرد را افزایش می‌دهید امکان بازگرداندن آن وجود ندارد. به عنوان مثال اگر سطح عملکرد دامنه را از Windows Server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

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

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

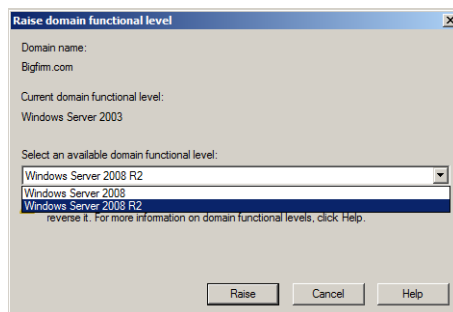
برای افزایش سطح عملکرد دامنه مراحل زیر را دنبال کنید:

۱. ADUC را اجرا کنید.
۲. بروی نام دامنه کلیک راست نموده و گزینه Raise Domain Functional Level را انتخاب کنید.



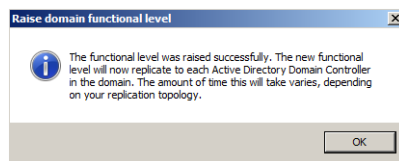
شکل ۶-۵۱

۳. در صفحه "Raise Domain Functional Level" می‌توانید اطلاعات مربوط به سطح عملکرد فعلی را مشاهده کنید. از قسمت Select an available domain functional level که قصد دارید به آن افزایش دهید (در اینجا Windows Server 2008 R2) را انتخاب کنید.



شکل ۶-۵۲

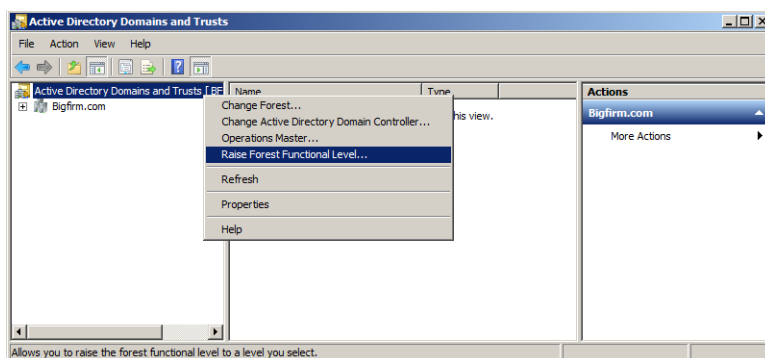
۴. پیغامی مبنی بر اینکه تغییرات انجام شده قابل بازگشت نمی‌باشند دریافت خواهید نمود. بروی OK کلیک کنید.
۵. پس از گذشت مدت زمان کوتاهی، پنجره‌ای ظاهر شده و موفقیت آمیز بودن افزایش سطح دامنه را اعلام می‌نماید. بروی OK کلیک کنید.



شکل ۵۳-۶

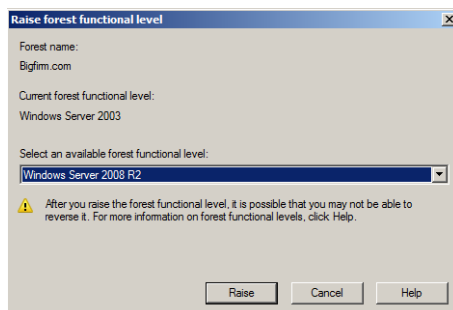
جهت افزایش سطح عملکرد جنگل نیز مراحل زیر را دنبال کنید:

۱. ADDT را از مسیر Start « Administrative Tools « Active Directory Domains and Trusts اجرا کنید.
۲. بروی Active Directory Domains and Trusts کلیک راست نموده و گزینه Raise Forest Functional Level را انتخاب کنید.



شکل ۵۴-۶

۳. در صفحه "Raise Forest Functional Level"، می‌توانید اطلاعات مربوط به سطح عملکرد فعلی را مشاهده کنید. از قسمت Select an available forest functional level سطحی که قصد دارید به آن افزایش دهید (در اینجا Windows Server 2008 R2) را انتخاب کنید.



شکل ۵۵-۶



۴. پیغامی مبنی بر اینکه تغییرات انجام شده قابل بازگشت نمی باشند دریافت خواهید نمود. برروی OK کلیک کنید.
۵. پس از گذشت مدت زمان کوتاهی پنجره‌ای ظاهر شده و موفقیت آمیز بودن افزایش سطح عملکرد جنگل را اعلام می نماید. برروی OK کلیک کنید.

### ۵-۵-۶ استفاده از NetDom

یکی از ابزارهای بسیار مفید در خط فرمان، NetDom (برگرفته از Domain Manager) می باشد. این ابزار در خط فرمان هر سروری که به DC تبدیل شده باشد وجود دارد. در ادامه تعدادی از کاربردهای این ابزار را مورد بررسی قرار خواهیم داد.

#### تغییر نام کامپیوترها (سرورهای DC)

با استفاده از دستور `netdom computername` می توان نام DC ها و Member Server ها را مورد تغییر قرار داد.

قبل از اینکه تغییر نام یک DC انجام شود ابتدا باید یک نام جایگزین به آن اختصاص دهید، سپس این نام جایگزین به عنوان نام اصلی سرور DC اختصاص داده می شود. به عنوان مثال اگر یک DC با نام Server9 در دامنه Bigfirm.com داشته باشید و بخواهید نام آنرا به BF2 تغییر دهید، ابتدا باید نام جایگزین BF2 را به آن اختصاص دهید. بدین منظور می توانید از دستور زیر استفاده کنید:

```
Netdom computername Server9 /add:bf2.bigfirm.com
```

قبل از اقدام به اجرای دستور بعدی، نیاز به Reboot کردن سرور دارید. این کار اطمینان می دهد که نام جایگزین در سرور DNS و برروی سیستم ثبت می شود. در این لحظه سرور دو نام (یکی نام اصلی و دیگری نام جایگزین) در اختیار دارد.

پس از Reboot شدن سرور می توانید نام جایگزین را با استفاده از دستور زیر به عنوان نام اصلی سرور اختصاص دهید:

```
Netdom computername Server9 /makeprimary:bf2.bigfirm.com
```

پس از اجرای این دستور، NetDom موفقیت آمیز بودن عملیات را اعلام نموده و شما را مجبور به Reboot کردن سرور می کند. پس از آن، نام قبلی حذف شده و سرور تنها با یک نام (bf2) شناخته می شود.

#### اتصال کامپیوتر به یک دامنه

جهت اتصال کامپیوتر به یک دامنه با استفاده از خط فرمان و یا اسکریپت ها می توان از ابزار

NetDom استفاده نمود. به مثال زیر توجه کنید:

```
Netdom join bf2 /d:bigfirm.com /reboot
```

دستور بالا، کامپیوتری با نام bf2 را به دامنه Bigfirm.com متصل نموده و سپس آنرا Reboot می‌کند. در حالت عادی حساب کامپیوتری که به دامنه متصل شده است در کانتینر Computers قرار می‌گیرد. همانطور که اخیراً شرح دادیم، با استفاده از دستور redircmp می‌توانید مسیر قرارگیری این حساب را تغییر دهید. به عنوان مثال برای تغییر مسیر حساب کامپیوتر bf2 از کانتینر Computers به واحد سازمانی Sales می‌توانید از دستور زیر استفاده کنید:

```
Dsmove "cn=bf3,cn=computers,dc=bigfirm,dc=com" -newparent "ou=sales,dc=bigfirm,dc=com"
```

### دستورات دیگر در NetDom

ابزار NetDom شامل دستورات بسیاری برای مدیریت دامنه می‌باشد. جهت دسترسی به لیست کامل این دستورات می‌توانید به آدرس <http://technet.microsoft.com/library/cc772217.aspx> مراجعه کنید. در ادامه تعدادی از این دستورات آورده شده است:

- ♦ **NetDom Reset**: گاهی اوقات ممکن است در اثر از دست رفت یک حساب کامپیوتری قادر نباشید به یک دامنه وارد شوید. برای برطرف نمودن این مشکل می‌توانید حساب مورد نظر را با استفاده از دستور بالا بازنشانی کنید.
- ♦ **NetDom ResetPwd**: از این دستور به منظور بازنشانی رمز عبور برای یک حساب کامپیوتری در دامنه استفاده می‌شود. اگر یک حساب برای مدت طولانی به دامنه متصل نشود ممکن است رمز عبور آن منقضی گردد. برای حل این مشکل می‌توانید از این دستور استفاده کنید.
- ♦ **NetDom Remove**: این دستور یک سیستم را از دامنه حذف می‌کند.

### ۶-۶ ایجاد سیاست‌های دانه ریز رمز عبور<sup>۱</sup>

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

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

1. Fine-Grained Password Policies

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

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

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

پیاده‌سازی Password Policy ها از طریق موارد زیر امکان‌پذیر می‌باشد:

- ♦ ایجاد “شیء تنظیمات رمز عبور”<sup>۱</sup> (PSO) و ذخیره آن در “کانتینر تنظیمات رمز عبور”<sup>۲</sup> (PSC)
- ♦ اعمال PSO بر روی کاربر یا گروه Global Security

## ۶-۶-۱ نیازمندی‌های سیاست‌های دانه ریز رمز عبور

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

## ۶-۶-۲ ایجاد PSO

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

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

1. Password Settings Object  
2. Password Settings Container

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

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



فرمت مدت زمان عمر رمز عبور به صورت d:hh:mm:ss می‌باشد که در آن، d بیانگر تعداد روزها، h بیانگر تعداد ساعات، m بیانگر تعداد دقیقه‌ها و s بیانگر تعداد ثانیه‌ها می‌باشد. به عنوان مثال مقدار 1:05:30:45 بیانگر مدت عمر یک روز و ۵ ساعت و ۳ دقیقه و ۴۵ ثانیه می‌باشد.

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

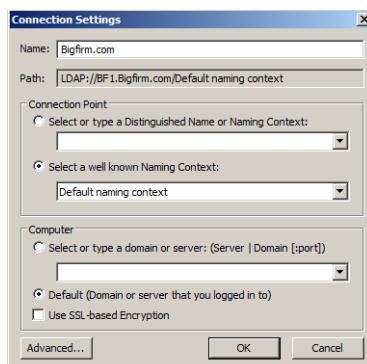
۶۵۵۳۵ باشد.

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

♦ **msDS-LockoutDuration**: این مشخصه تعیین می‌کند که حساب یک کاربر در اثر وارد کردن رمز عبورهای اشتباه (بیش از تعداد دفعات مجاز) چه مدت بسته باشد. یا به عبارت دیگر، کاربر چه مدتی باید برای وارد کردن مجدد رمز عبور منتظر بماند.

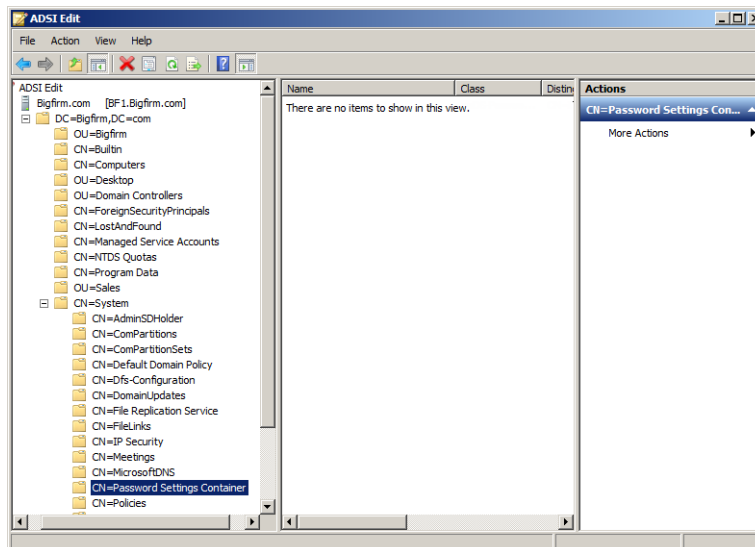
با کمی آگاهی راجع به تنظیمات PSOها، اکنون می‌توانید یکی از آنها را ایجاد کنید. برای ایجاد PSO بر روی یک گروه (به عنوان مثال G\_ITAdmins) مراحل زیر را دنبال کنید:

۱. ADUC را اجرا نموده و یک گروه با نام G\_ITAdmins در کانتینر Users ایجاد کنید.
۲. ADSI Edit را از مسیر Start » Administrative Tools (یا از طریق جستجو در منو Start) اجرا کنید.
۳. در کنسول ADSI Edit، بر روی ADSI Edit کلیک‌راست نموده و گزینه Connect To را انتخاب کنید.
۴. در صفحه "Connection Settings"، در فیلد Name نام FQDN دامنه (در اینجا Bigfirm.com) را وارد نموده و بر روی OK کلیک کنید.



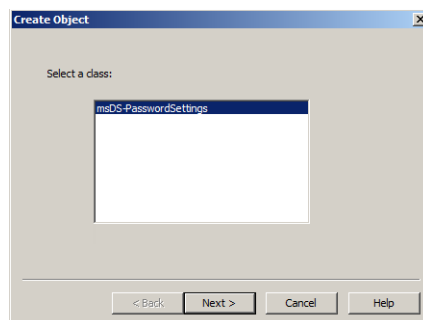
شکل ۶-۵۶

۵. از آیتم CN=System، مقدار CN=Password Settings Container را پیدا کنید.



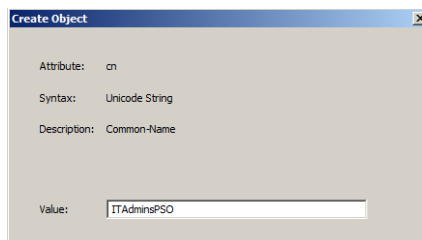
شکل ۵۷-۶

۶. بروی CN=Password Settings Container کلیک راست نموده و «New» Object را انتخاب کنید.
۷. در صفحه «Create Object» تنها شیء موجود، msDS-PasswordSettings می باشد که بطور پیش فرض انتخاب شده است. بروی Next کلیک کنید.



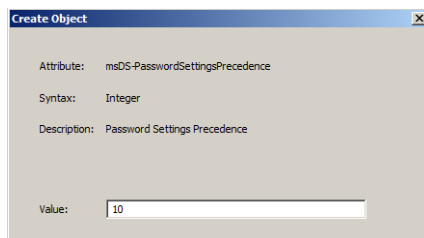
شکل ۵۸-۶

۸. در قسمت Value، نام ITAdminsPSO را برای PSO وارد نموده و بروی Next کلیک کنید.



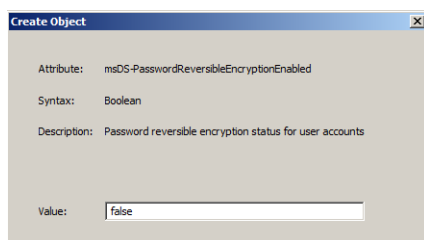
شکل ۵۹-۶

۹. برای مشخصه msDS-PasswordSettingsPrecedence در قسمت Value عدد ۱۰ را وارد نموده و برروی Next کلیک کنید.



شکل ۶-۶۰

۱۰. برای مشخصه msDS-PasswordReversibleEncryptionEnabled مقدار False را وارد نموده و برروی Next کلیک کنید.



شکل ۶-۶۱

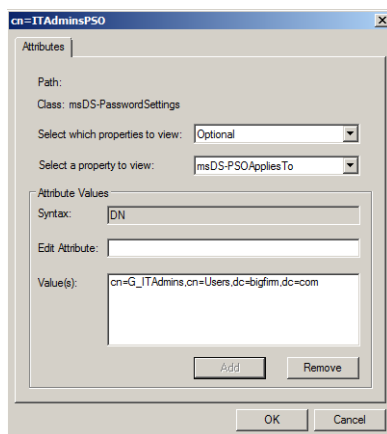
۱۱. برای مشخصه msDS-PasswordHistoryLength مقدار ۲۴ را وارد نموده و برروی Next کلیک کنید.
۱۲. برای مشخصه msDS-PasswordComplexityEnabled مقدار True را وارد نموده و برروی Next کلیک کنید.
۱۳. برای مشخصه msDS-MinimumPasswordLength مقدار ۱۵ را وارد نموده و برروی Next کلیک کنید.
۱۴. برای مشخصه msDS-MinimumPasswordAge مقدار 1:00:00:00 (یک روز) را وارد نموده و برروی Next کلیک کنید.
۱۵. برای مشخصه msDS-MaximumPasswordAge مقدار 30:00:00:00 (۳۰ روز) را وارد نموده و برروی Next کلیک کنید.
۱۶. برای مشخصه msDS-LockoutThreshold مقدار ۵ را وارد نموده و برروی Next کلیک کنید.
۱۷. برای مشخصه msDS-LockoutObservationWindow مقدار 0:00:30:00 (۳۰ دقیقه) را وارد نموده و برروی Next کلیک کنید.

۱۸. برای مشخصه msDS-LockoutDuration مقدار 0:00:30:00 (۳۰ دقیقه) را وارد نموده و برروی Next کلیک کنید.

۱۹. بجای کلیک برروی Finish، برروی دکمه More Attributes کلیک کنید.

۲۰. در قسمت "Select a property to view" گزینه msDS-PSOAppliesTo را انتخاب کنید.

۲۱. در قسمت Edit Attribute، نام DN برای گروه G\_ITAdmins را وارد نموده و برروی Add کلیک کنید. سپس برروی OK کلیک کنید.



شکل ۶-۶۲

۲۲. در نهایت برروی Finish کلیک کنید. چنانچه در هر زمانی قصد داشته باشید مشخصات این PSO را مشاهده نموده و یا مورد تغییر قرار دهید، می‌توانید به CN=Password Settings Container در ADSI Edit بازگشته و با دابل‌کلیک برروی PSO، مشخصات آنرا مشاهده کنید. تنها امکان تغییر تعدادی از مشخصات وجود دارد و بقیه فقط قابل مشاهده هستند.

۲۳. تمام پنجره‌ها را ببندید.

پس از ایجاد PSO می‌توانید آنرا با استفاده از ADUC برروی کاربران یا گروه‌ها اعمال کنید. بدین منظور مراحل زیر را دنبال کنید:

۱. ADUC را اجرا کنید.

۲. از منوی View، گزینه Advanced Features را انتخاب کنید.

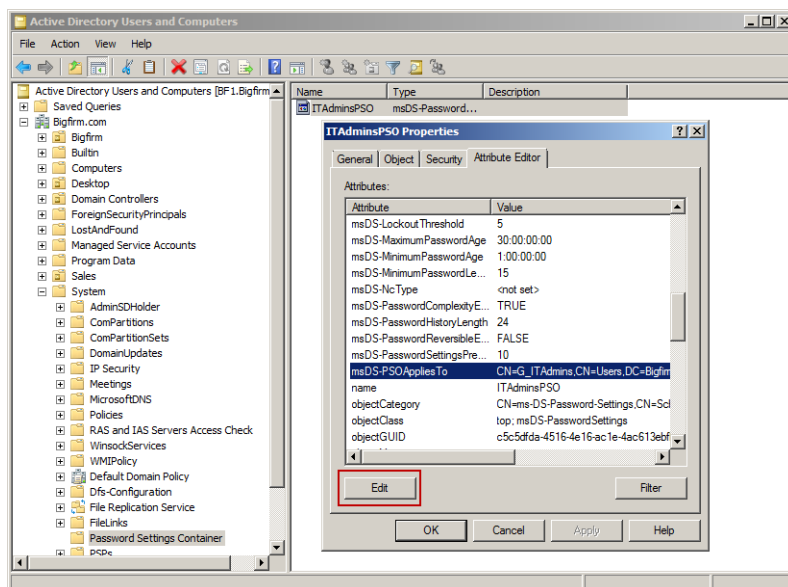
۳. در زیر نام دامنه، برروی System «Password Settings Container» کلیک کنید.

۴. برروی PSO کلیک‌راست نموده و Properties را انتخاب کنید.

۵. در پنجره PSO Properties تب Attribute Editor را انتخاب کنید.

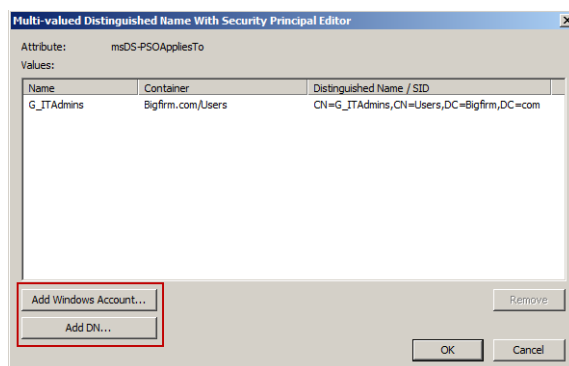


۶. مشخصه msDS-PSOAppliesTo را انتخاب نموده و بر روی Edit کلیک کنید.



شکل ۶-۶۳

۷. در پنجره باز شده می‌توانید با کلیک بر روی یکی از دکمه‌های Add Windows Account (برای وارد نمودن نام کاربر، گروه و ...) یا Add DN (برای افزودن نام DN)، اشیاء موردنظر را اضافه نموده و PSO را بر روی آن اعمال کنید.



شکل ۶-۶۴

## « فصل ۷ »

ایجاد و مدیریت  
حسابهای کاربری و گروهها

**Creating and Managing**  
**User Accounts and Groups**



شاید یکی از مهمترین اقداماتی که مدیران در طول حیات شبکه‌ها انجام می‌دهند، ایجاد و مدیریت حساب‌های کاربری می‌باشد. با اینکه ایجاد این حساب‌ها ساده به نظر می‌رسد ولی مدیریت زمان و پیاده‌سازی امنیت برای آنها بسیار مهم است. در بسیاری از شبکه‌ها، تنها اقداماتی اولیه برای ایجاد حساب‌ها انجام می‌شود و مدیر شبکه برطبق تعداد کارکنان و یا افراد متصل به شبکه، واحدهای سازمانی، گروه‌ها و کاربران را ایجاد می‌نماید. پس از آن مدیریت هر یک از این بخش‌ها به افراد خاصی که ممکن است از بین کارکنان سازمان انتخاب شده باشند واگذار می‌شود، بنابراین برای این مدیران ایجاد حساب‌های کاربری و مدیریت آنها در هر بخش از اهمیت ویژه‌ای برخوردار می‌باشد.

در این فصل قصد داریم بطور جامع به بحث ایجاد و مدیریت حساب‌ها با استفاده از ابزارهای گرافیکی و همچنین ایجاد و مدیریت آنها با استفاده از دستورات خط فرمان (برای Server Core) بپردازیم. کلیه مباحثی که در این فصل بیان می‌شوند، برای ویندوز سرور 2008 و 2008R2 قابل استفاده است اما ممکن است تفاوت‌هایی جزئی در آنها دیده شود.

بطور کلی مهمترین مباحث این فصل عبارتند از:

- ♦ مدیریت کاربران و گروه‌های محلی
- ♦ مدیریت کاربران و گروه‌ها در اکتیو دایرکتوری
- ♦ مدیریت کاربران و گروه‌ها در ویندوز سرور 2008R2
- ♦ واگذاری مجوز مدیریت گروه

## ۷-۱ حساب‌های کاربری

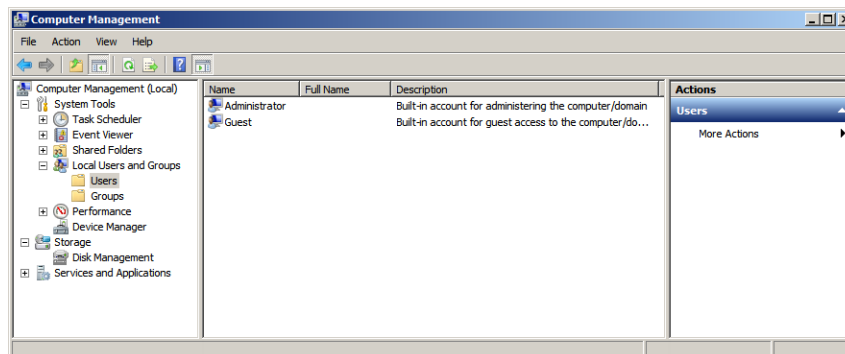
در این قسمت قصد داریم نحوه ایجاد، مدیریت و حذف حساب‌های کاربری در سطح محلی (Local) و دامنه را با استفاده از ابزارهای گرافیکی، دستورات خط فرمان و PowerShell شرح دهیم. برای انجام کار، از یک DC به نام bf1.bigfirm.com و یک Member Server به نام bf2.bigfirm.com استفاده می‌کنیم.

### ۷-۱-۱ ایجاد حساب‌های کاربری Local

برای ایجاد حساب‌های کاربری Local، از دو ابزار گرافیکی به نام‌های Server Manager و Computer Management استفاده می‌شود. این ابزارها از طریق «Start Administrative Tools» دسترسی هستند.

جهت افزودن حساب کاربری Local مراحل زیر را دنبال کنید:

۱. با حساب مدیر به bf2.bigfirm.com وارد شده و پس از اجرای Computer Management به مسیر Local Users and Groups\Users حرکت کنید.



شکل ۷-۱

همانطور که در شکل ۷-۱ مشاهده می‌کنید، دو حساب کاربری در این مسیر وجود دارد:

- ♦ **Administrator:** حساب کاربری پیش‌فرض برای مدیریت است و از طریق آن می‌توان کلیه اقدامات سرور را مدیریت نمود (دقت داشته باشید که حساب کاربری مدیریت دامنه برای مدیریت کل سرورها در یک دامنه است و با این حساب متفاوت است).
- ♦ **Guest:** این حساب به کاربرانی که حساب کاربری واقعی ندارند اجازه می‌دهد که به کامپیوتر Local وارد شوند. این حساب‌ها زمانی استفاده می‌شوند که تعداد زیادی از کاربران قصد وارد و خارج شدن به/از سرور را داشته باشند. بر روی آیکن مربوط به حساب کاربری Guest، یک علامت ↓ قرار دارد. این علامت بدین معناست که این حساب باید غیر فعال شود. مایکروسافت این حساب را بطور پیش‌فرض غیر فعال کرده است و به دلیل اینکه نیاز چندانی به آن نیست ممکن است هرگز آنرا فعال نکنید.

۲. جهت افزودن یک حساب کاربری برای کارمندی به نام Joe Bloggs در پنل سمت چپ بر روی «Local Users and Groups» کلیک راست نموده و New User را انتخاب کنید.

۳. در پنجره «New User» تعدادی فیلد برای تکمیل مشخصات کاربر وجود دارد. این فیلدها عبارتند از:

- ♦ **User Name:** نامی است که کاربر در هر بار ورود به سرور باید از آن استفاده کند. بهتر است که این نام طبق یک استاندارد در سازمان مشخص شود. به عنوان مثال اگر برای این کاربر نام کاربری JBloggs انتخاب شود و مدتی بعد، کاربر دیگری با نام John Bloggs نیز به سازمان اضافه شود، می‌توان نام کاربری JBloggs1 (یا JBloggs01) را برای آن انتخاب نمود. البته انتخاب نام بستگی به سازمان‌ها دارد. برخی از سازمان‌ها از شماره استخدامی و یا مشخصات فردی کاربران نیز به عنوان نام کاربری آنها استفاده می‌کنند.

- ♦ **Full Name:** نام کامل کاربری است که از این حساب استفاده می‌کند.
  - ♦ **Password:** این فیلد جهت تعیین رمز عبور برای حساب کاربری می‌باشد.
- علاوه بر فیلدهای ذکر شده، تعدادی گزینه نیز به شرح زیر وجود دارد:
- ♦ **User must change password at next logon:** با فعال کردن این گزینه کاربر زمانی که برای اولین بار به سیستم وارد می‌شود باید رمز عبور خود را تغییر دهد.
  - ♦ **User cannot change password:** کاربرد این گزینه زمانی است که چندین کاربر از یک حساب کاربری مشترک استفاده می‌کنند. با فعال کردن این گزینه کاربران نمی‌توانند رمز عبور خود را تغییر دهند.
  - ♦ **Password never expires:** فعال کردن این گزینه باعث می‌شود که رمز عبور هیچگاه منقضی نشده و به صورت دائمی مورد استفاده قرار گیرد.
  - ♦ **Account is disabled:** چنانچه قصد دارید حساب کاربری را در زمان دیگری فعال کنید می‌توانید از این گزینه استفاده نمایید.

پس از انجام تنظیمات مورد نظر، بر روی **Create** کلیک کنید تا حساب کاربری با نام JBloggs ایجاد شود. دقت داشته باشید که پنجره ایجاد حساب کاربری بسته نخواهد شد و فقط مقادیر فیلدهای آن پاک می‌شوند. این کار باعث می‌شود که به سرعت بتوانید حساب‌های کاربری خود را ایجاد کنید.

شکل ۷-۲

### ایجاد حساب‌های کاربری محلی از طریق خط فرمان

ایجاد کاربرن با استفاده از خط فرمان نیز امکان‌پذیر است. انجام این کار در زمان استفاده از Server Core و یا ایجاد اسکریپت‌ها بسیار مفید خواهد بود. با استفاده از دستور زیر می‌توانید کاربری

با نام JBloggs ایجاد کنید:

```
C:\Users\administrator>net user JBloggs mydogisbrown /ADD
The command completed successfully.
```

قالب کلی این دستور به صورت زیر می‌باشد:

```
net user <User Name> <Password> /ADD
```

این دستور یک کاربر بر روی کامپیوتر Local ایجاد می‌کند. دقت داشته باشید که می‌توانید در رمز عبور خود فاصله نیز قرار دهید. این کار با قرار داده رمز عبور در داخل علامت " امکانپذیر می‌باشد. به مثال زیر توجه کنید:

```
net user JBloggs "My d0g is yellow" /ADD
```

امکان افزودن گزینه‌های بیشتر برای ایجاد کامل یک کاربر نیز وجود دارد. با دستور زیر یک کاربر همانند آنچه که با استفاده از Computer Manager ایجاد نمودید، ایجاد می‌شود:

```
net user JBloggs Myd0giswhite /fullname:"Joe Bloggs" /comment:"A member of the Server Management Team" /logonpasswordchg:yes /add
```

پارامترهایی که می‌توان در این دستور به کار برد عبارتند از:

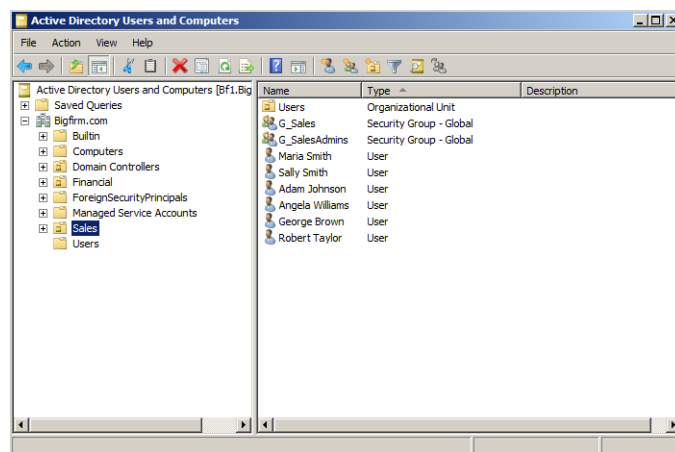
- ♦ **/fullname**: نام کامل کاربر است.
- ♦ **/comment**: توضیحی راجع به کاربر اضافه می‌کند و معادل فیلد Description در Computer Management می‌باشد.
- ♦ **/logonpasswordchg:yes**: از این پارامتر برای تغییر رمز عبور کاربر پس از اولین ورود به سیستم استفاده می‌شود.
- ♦ **/passwordchg**: این پارامتر برای تعیین اینکه کاربر توانایی تغییر رمز عبور را داشته باشد استفاده می‌شود. مقدار Yes بیانگر توانایی تغییر رمز و No به معنای عدم توانایی تغییر آن می‌باشد.
- ♦ **/expires**: جهت تعیین زمان منقضی شدن رمز عبور استفاده می‌شود و مقدار قابل اختصاص به آن یک تاریخ به صورت mm/dd/yy (سال/روز/ماه) یا Never می‌باشد.
- ♦ **/active**: جهت تعیین فعال یا غیرفعال بودن حساب کاربری استفاده می‌شود.

جهت کسب اطلاعات بیشتر پیرامون این دستور می‌توانید از دستور `net help user` استفاده کنید.

## ۷-۱-۲ ایجاد حساب‌های کاربری مبتنی بر دامنه

حساب‌های کاربری که به صورت Local ایجاد می‌شوند فقط برای ورود کاربر به یک سرور در نظر گرفته شده‌اند. به عنوان مثال کاربری که در قسمت قبل ایجاد نمودید (Joe Bloggs) فقط قادر است به Member Server با نام bf2.bigfirm.com وارد شود. اکنون فرض کنید که این کاربر باید به سایر سرورها نیز دسترسی داشته باشد. در این موارد بجای ایجاد یک حساب کاربری بر روی هر سرور (به صورت Local)، می‌توان یک حساب مبتنی بر دامنه برای او ایجاد نموده تا این کاربر با استفاده از یک نام کاربری و رمز عبور بتواند به سایر سرورها (در صورت داشتن مجوز) وارد شود. برای ایجاد حساب‌های کاربری مبتنی بر دامنه، به DC وارد شوید (در اینجا bf1.bigfirm.com) و از طریق ابزار Active Directory Users and Computers (ADUC) در Administrative Tools نسبت به ایجاد آن اقدام کنید. برای دسترسی Remote (از راه دور) به سرور و مدیریت آن از طریق ویندوز ویستا یا ویندوز ۷ می‌توانید نرم افزار رایگان Remote Server Administration Tools را دانلود نموده و بر روی این سیستم عامل‌ها نصب کنید.

در تصویر زیر، نمایی از ابزار ADUC به همراه تعدادی از کانتینرها (Containerها) و واحدهای سازمانی (OU) نشان داده شده است. با کلیک بر روی هر OU می‌توانید لیستی از کاربرانی که در آن قرار گرفته و از مشخصه‌های آن استفاده می‌کنند را مشاهده کنید.

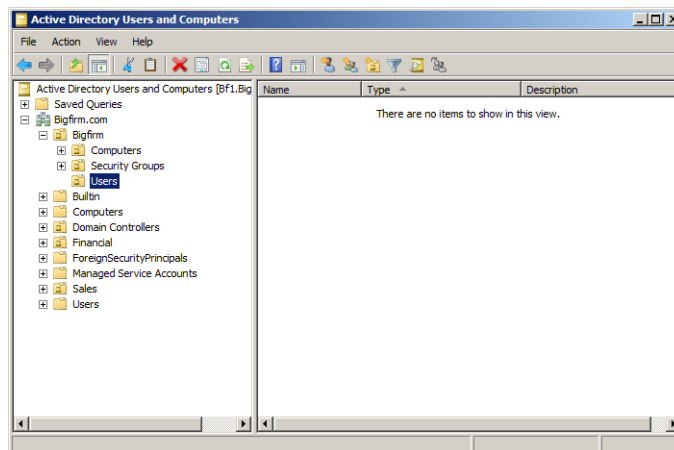


شکل ۷-۳

۱. قبل از اینکه به نحوه ایجاد حساب‌های کاربری در این ابزار بپردازیم، لازم است تعدادی OU ایجاد کنید. با فرض اینکه سازمان شما از یک سایت تشکیل شده است، یک OU با نام Bigfirm ایجاد نموده و سپس سه OU دیگر جهت قرارگیری کاربران، کامپیوترها و گروه‌های نوع Security ایجاد کنید. این OUها را به ترتیب، Users، Computers و Security Groups نامگذاری کنید. در تصویر زیر

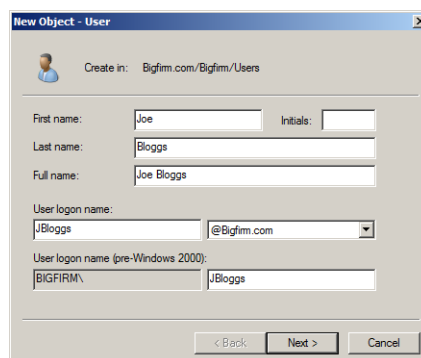


این وضعیت نشان داده شده است (دقت داشته باشید OU ای که با نام Users ایجاد می‌کنید، به این دلیل است که با کانتینر Users در ADUC تداخل پیش نیاید زیرا این کانتینر محل نگهداری اشیاء مهم برای اکتیو دایرکتوری می‌باشد).



شکل ۴-۷

۲. اکنون برای ایجاد کاربر در هر یک از OU های ایجاد شده، بر روی آن کلیک راست نموده و Users را انتخاب نمایید. ویزاردی تحت عنوان New Object – User راه اندازی می‌گردد. با استفاده از این میزبان به راحتی می‌توانید کاربر مورد نظر را ایجاد کنید. کافی است در فیلدهای First name و Last name، نام و نام خانوادگی کاربر را وارد کنید. فیلد Full name بطور خودکار تکمیل می‌شود. در فیلد User logon name نیز نام کاربری را وارد کنید (به عنوان مثال برای Joe Bloggs می‌توانید از نام کاربری JBloggs استفاده کنید).



شکل ۵-۷

بد نیست در اینجا دو اصطلاح را در که در هنگام ایجاد کاربران با آن مواجه می‌شوید معرفی کنیم:

- **User logon name:** این همان نامی است که شما به عنوان نام کاربری وارد می‌کنید و با آن آشنا هستید.
- **User principal name:** این نام با عنوان UPN در ویندوز 2000 شناخته می‌شود و همانند یک آدرس ایمیل برای کاربر عمل می‌کند. به عنوان مثال UPN که برای JBloggs ایجاد می‌شود به صورت JBloggs@bigfirm.com می‌باشد که در آن پسوند UPN (bigfirm.com) از نام دامنه گرفته شده است.



جهت تغییر پسوند UPN و افزودن پسوندهای جدید، ADDT را از مسیر Start Administrative Tools «Active Directory Domain and Trusts» اجرا کنید. در پنل سمت چپ بر روی Domains and Trusts کلیک راست نموده و Properties را انتخاب نمایید. در پنجره باز شده در قسمت Alternative UPN suffixes پسوند مورد نظر را وارد نموده و بر روی Add کلیک کنید.

۳. بر روی Next کلیک کنید تا به صفحه بعد هدایت شوید. در فیلدهای Password و Confirm Password رمز عبور یکسانی را وارد کنید. همچنین با فعال یا غیر فعال نمودن چهار گزینه موجود می‌توانید تنظیماتی مانند: تغییر رمز عبور کاربر پس از اولین ورود به سیستم، عدم تغییر رمز عبور توسط کاربر، عدم منقضی شدن رمز عبور، و فعال یا غیر فعال بودن حساب کاربری را انجام دهید.

شکل ۶-۷

ایجاد حساب‌های کاربری مبتنی بر دامنه با استفاده از خط فرمان

ایجاد حساب‌های کاربری در دامنه با استفاده از خط فرمان نیز امکان‌پذیر است. اولین دستوری

که در این زمینه استفاده می‌شود، DsAdd می‌باشد. با استفاده از دستور زیر می‌توانید کاربری را که به کمک ADUC ایجاد کردید اکنون با استفاده از خط فرمان ایجاد کنید:

```
dsadd user "CN=Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com" -
samid JBloggs -upn JBloggs@bigfirm.com -fn Joe -ln Bloggs -display
"Joe Bloggs" -pwd Mydogisblu3 -mustchpwd yes
```

قالب کلی این دستور به صورت زیر می‌باشد:

```
dsadd user <Distinguished Name of the user> -samid <user logon name>
-upn <user principal name> -fn <firstname> -ln <surname (Last name)>
-display <full name> -pwd <password> -mustchpwd <the user must
change their password on first logon: yes or no>
```

قسمت‌های تشکیل دهنده نام DN در دستور قبل به شرح زیر می‌باشند:

- **Component name (CN):** نام شیء (که در اینجا یک حساب کاربری است) را مشخص می‌کند.
- **Organization unit (OU):** واحد سازمانی که شیء مورد نظر در آن قرار گرفته است را مشخص نموده و چنانچه از OUهای تو در تو استفاده شده باشد، نام داخلی ترین OU و سپس OUهای خارجی آن به ترتیب نوشته می‌شوند. به عنوان مثال در CN=Joe Bloggs,OU=Users,OU=BigFirm ابتدا نام Users نوشته شده است که این OU خود در OU با نام Bigfirm قرار دارد.
- **Domain component (DC):** نام دامنه را مشخص می‌کند (مانند bigfirm.com).

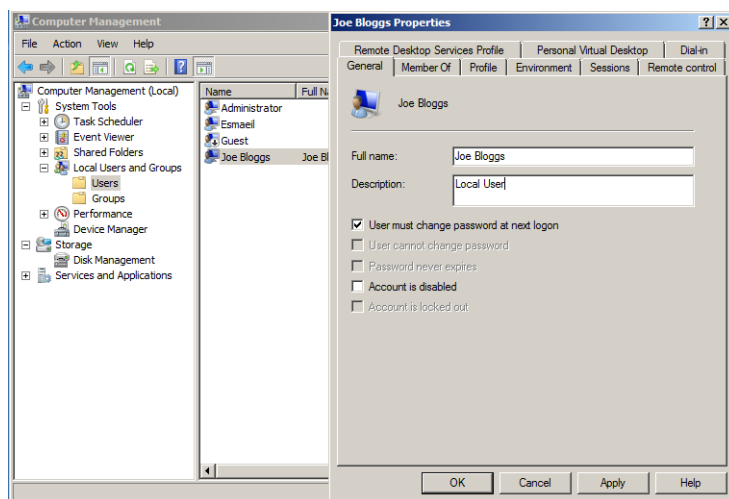
جهت کسب اطلاعات بیشتر در این زمینه می‌توانید از دستور dsadd user /? استفاده کنید.

### ۳-۱-۷ تغییر تنظیمات حساب‌های کاربری

پس از ایجاد حساب‌های کاربری ممکن است قصد داشته باشید تنظیمات مربوط به آنها را تغییر دهید. در این قسمت نحوه انجام این کار را برای حساب‌های Local، مبتنی بر دامنه و همچنین تغییر همزمان تعدادی از حساب‌ها را شرح می‌دهیم.

#### تغییر تنظیمات حساب‌های کاربری Local

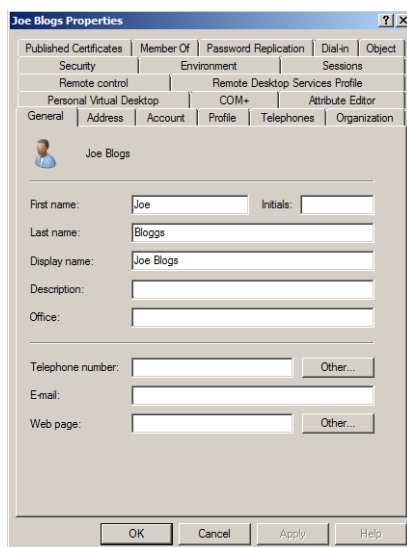
برای دسترسی به تنظیمات یک حساب کاربری Local و تغییر آنها، در کنسول Computer Management کاربر موردنظر را انتخاب نموده و سپس بر روی آن کلیک‌راست کنید. گزینه Properties را انتخاب نموده تا پنجره تنظیمات حساب کاربری نشان داده شود. در این پنجره با توجه به تب‌های موجود می‌توانید کلیه تنظیمات مربوط به کاربر را مشاهده و در صورت نیاز آنها را مورد تغییر قرار دهید. در شکل زیر این پنجره نشان داده شده است.



شکل ۷-۷

### تغییر تنظیمات حساب‌های کاربری مبتنی بر دامنه

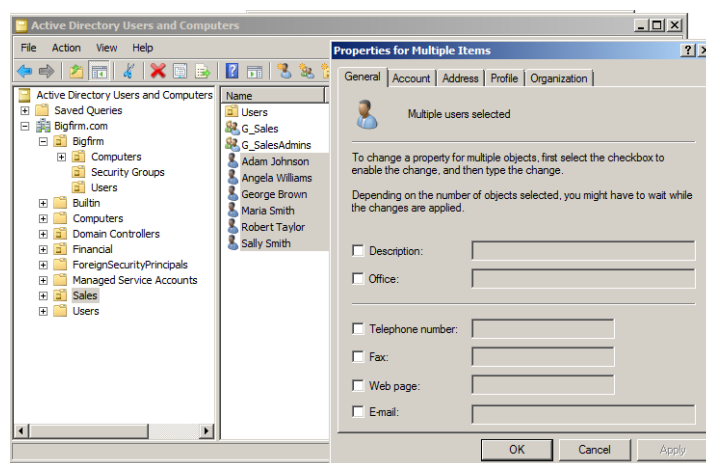
همانند حساب‌های کاربری Local، امکان دسترسی به تنظیمات حساب‌های کاربری مبتنی بر دامنه نیز وجود دارد. کافی است بر روی هر کاربر کلیک راست نموده و با انتخاب گزینه Properties به پنجره تنظیمات آن کاربر دسترسی پیدا کنید. تصویر این پنجره در شکل زیر نشان داده شده است.



شکل ۷-۸

### تغییر همزمان تنظیمات مربوط به گروهی از کاربران

همانطور که در قسمت‌های قبل مشاهده کردید، با استفاده از پنجره Properties مربوط به هر حساب کاربری می‌توان تنظیمات آن کاربر را تغییر داد. اکنون حالتی را در نظر بگیرید که قصد دارید تنظیمات مربوط به تعدادی از حساب‌های کاربری را به صورت همزمان تغییر دهید. روش انجام این کار همانند قسمت‌های قبل است با این تفاوت که بجای یک کاربر، همه کاربران مورد نظر انتخاب می‌شوند و سپس با کلیک راست بر روی آنها و انتخاب گزینه Properties می‌توان به پنجره تنظیمات آنها دسترسی پیدا نمود. در شکل زیر این پنجره نشان داده شده است.



شکل ۷-۹

همانطور که مشاهده می‌کنید، تعداد تب‌های موجود در این حالت نسبت به حالتی که یک حساب کاربری انتخاب می‌شود کمتر است. این مسئله به آن دلیل است که حساب‌ها دارای تنظیمات منحصر بفردی بوده که ممکن است برای سایر کاربران متفاوت باشد و بنابراین باید به صورت تکی تنظیم گردند.

### ۴-۱-۷ مدیریت حساب‌های کاربری مبتنی بر دامنه در خط فرمان

حساب‌های کاربری را از طریق خط فرمان نیز می‌توان مدیریت نمود. دستوری که در این زمینه مورد استفاده قرار می‌گیرد، دستور dsmod به همراه user می‌باشد. برای اطلاع از نحوه کاربرد این دستور می‌توانید از دستور زیر استفاده نمایید:

```
dsmod user /?
```

دقت داشته باشید که برای استفاده از این دستور به DN مربوط به کاربران نیاز دارید. جهت

آگاهی از DN هر کاربر (با استفاده از ADUC) می‌توانید به تب Attribute Editor در Properties آن کاربر مراجعه کنید. در خط فرمان نیز می‌توانید با در اختیار داشتن UPN کاربر و با استفاده از دستور `dsquery` نام DN آن کاربر را جستجو کنید:

```
dsquery user -upn jbloggs@bigfirm.com
"CN=Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

همچنین بدست آوردن DN با استفاده از شناسه SAM نیز امکان‌پذیر است. به مثال زیر توجه کنید:

```
dsquery user -samid jbloggs
"CN=Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

با استفاده از دستور `dsquery /?` می‌توانید از سایر قابلیت‌های این دستور آگاه شوید.

پس از بدست آوردن DN کاربر می‌توانید کار با دستور `dsmod` را آغاز کنید. در ادامه تعدادی مثال در رابطه با استفاده از دستور `dsmod` ارائه می‌دهیم:

تغییر رمز عبور یک کاربر و اجبار آن برای تغییر دادن رمز عبور:

```
dsmod user "CN=Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
-pwd A1b2C3d4 -mustchpwd yes
```

تعیین رمز عبور مشترک برای چندین کاربر و اجبار آنها برای تغییر دادن آن:

```
dsmod user "CN=Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
"CN=John Doe,OU=Users,OU=BigFirm,DC=bigfirm,DC=com" -pwd A1b2C3d4
-mustchpwd yes
```

تغییر نامی که کاربر با آن نمایش داده می‌شود (نام کامل):

```
dsmod user "CN=Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
-display "Joe Bloggs"
```

افزودن آدرس ایمیل برای کاربر:

```
dsmod user "CN=Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
-email JoeBloggs@yahoo.com
```

همانطور که اشاره کردیم، با استفاده از دستور `dsmod user /?` می‌توانید از سایر پارامترهای قابل استفاده در این دستور آگاهی پیدا کنید.

دستور دیگری که در رابطه با مدیریت حساب‌های کاربری مورد استفاده قرار می‌گیرد، `dsrm` می‌باشد. از این دستور جهت حذف اشیاء اکتیو دایرکتوری (در اینجا حساب‌های کاربری) استفاده

شود. به مثال زیر توجه کنید:

```
dsrm "CN=Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

با استفاده از دستور بالا، کاربر Joe Bloggs از اکتیو دایرکتوری حذف می‌گردد. جهت آگاهی از سایر قابلیت‌های این دستور می‌توانید آنرا به صورت `dsrm /?` وارد کنید.

جهت حذف کاربران Local (کاربرانی که بروی خود کامپیوتر قرار دارند) نیز می‌توانید از دستور زیر استفاده کنید:

```
net user <username> /delete
```

به عنوان مثال جهت حذف حساب کاربری Joe Bloggs (که به صورت Local است) می‌توانید دستور زیر را وارد کنید:

```
net user JBloggs /delete
```

## ۲-۷ مدیریت گروه‌ها

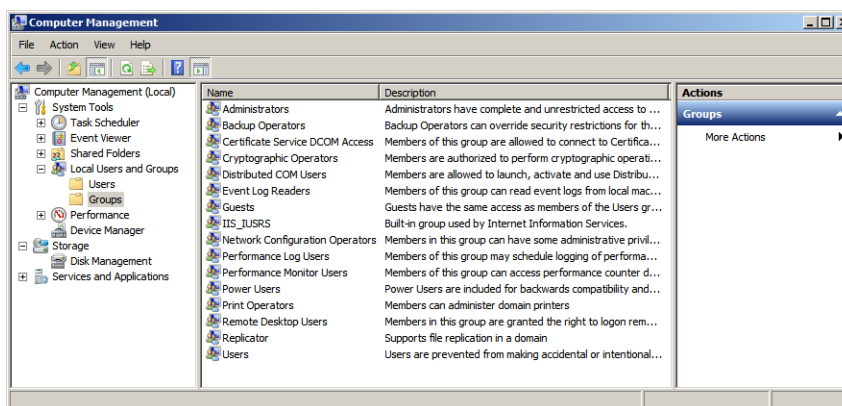
انجام اقدامات مشابه برای تعداد زیادی از کاربران می‌تواند کاری خسته کننده و وقت‌گیر باشد. به عنوان مثال فرض کنید برای دسترسی ۲۰۰ کاربر به تعداد مشخصی از منابع شبکه باید مجوزهایی تعیین شود. بجای اینکه این مجوزها بروی هر کاربر به صورت جداگانه اعمال شود، می‌توان آنها را در یک گروه قرار داده و سپس مجوزهای لازم را بروی آن گروه اعمال نمود. در این حالت، بجای تعداد زیادی از کاربران، تنها با یک (یا تعدادی) گروه سروکار خواهید داشت.

استفاده و مدیریت گروه‌ها نیازمند آشنایی شما با مسائلی مانند ایجاد گروه‌ها، انجام تغییرات بروی اعضا و حذف گروه‌ها می‌باشد. بنابراین در ادامه نحوه انجام این اقدامات را برای گروه‌های Local و گروه‌های مبتنی بر دامنه با استفاده از ابزار Active Directory Users and Computers و همچنین دستورات خط فرمان شرح خواهیم داد.

## ۱-۲-۷ گروه‌های Local

همانند کاربران Local، گروه‌های Local نیز بروی کامپیوترهای متصل به دامنه (Member Computers) و یا کامپیوترهای مستقل که می‌توانند یک سرور، لپ تاپ و یا کامپیوتری رومیزی باشند وجود دارد. دقت داشته باشید که حساب‌های کاربری و گروه‌های موجود بروی این کامپیوترها تنها محدود به کاربران و یا گروه‌های Local نیست و ممکن است شامل کاربران و گروه‌های اکتیو دایرکتوری باشد که سرور فعلی عضوی از آن می‌باشد. ابزار گرافیکی که جهت مدیریت گروه‌های

Local مورد استفاده قرار می‌گیرد، Computer Management می‌باشد. این ابزار از طریق کلیک راست بر روی Computer و انتخاب گزینه Manage، یا از مسیر Start « Administrative Tools « Computer Management قابل دسترسی می‌باشد. جهت دسترسی به گروه‌ها می‌توانید از زیر آیتم Local Users and Groups (شکل ۷-۱۰) را انتخاب کنید.



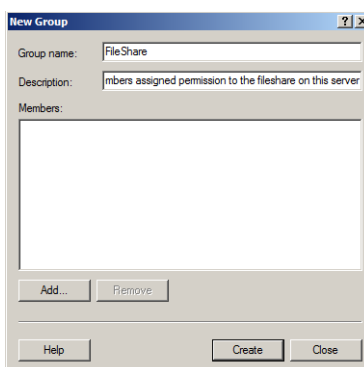
شکل ۷-۱۰

### ایجاد یک گروه

در این قسمت یک گروه با نام FileShare ایجاد نموده و از آن جهت اختصاص مجوز به کاربران این گروه به منظور دسترسی به فایل‌ها که بر روی سرور به اشتراک گذاشته شده است استفاده می‌کنیم.

۱. جهت ایجاد گروه، از منوی Action و یا انجام کلیک راست بر روی پنل وسط پنجره Computer Management (در قسمت Groups) گزینه New Groups را انتخاب کنید.

۲. با مشاهده پنجره "New Group"، نام و توضیحی پیرامون گروه وارد کنید.

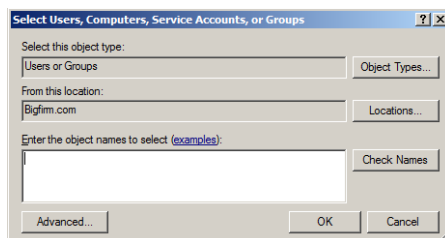


شکل ۷-۱۱



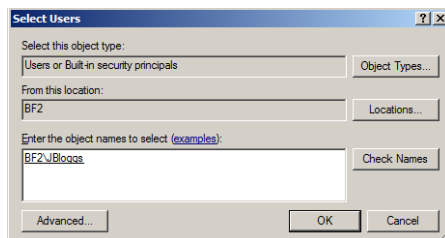
۳. چنانچه قصد دارید گروه را بدون افزودن هیچ کاربری به آن ایجاد کنید، بر روی دکمه Create کلیک کنید. در غیر اینصورت می‌توانید با انتخاب دکمه Add، کاربران مورد نظر را به آن اضافه کنید.

۴. در صورتی که سرور به یک دامنه متصل باشد، امکان اضافه کردن اشیاء موجود در اکتیو دایرکتوری به گروه فعلی وجود دارد. برای انجام این کار می‌توانید با کلیک بر روی دکمه Location، دامنه مورد نظر را انتخاب نموده و سپس با کلیک بر روی دکمه Object type نوع اشیاء را مشخص کنید. در نهایت با وارد کردن نام شیء در قسمت Enter the object name to select و فشردن دکمه Chek Names می‌توانید نام را جستجو نموده و به گروه اضافه کنید.



شکل ۷-۱۲

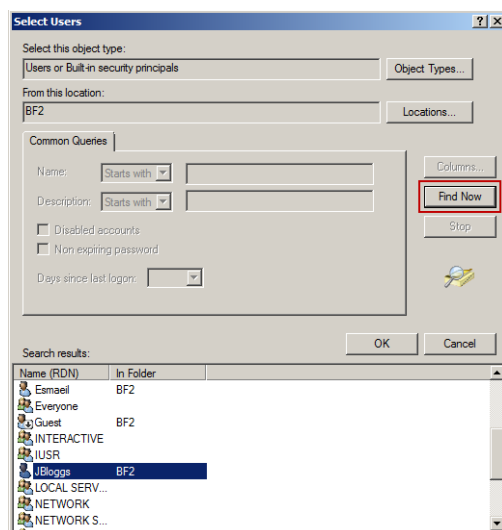
۵. اکنون حالتی را در نظر بگیرید که قصد داریم کاربری به نام JBloggs را بر روی کامپیوتر (سرور) فعلی که دارای نام BF2 است جستجو نموده و به گروه اضافه کنیم. برای انجام این کار لازم است پس از انتخاب نوع شیء و محل قرارگیری آن (سرور BF2) نام آنرا در قسمت Enter the object name to select وارد نموده و بر روی دکمه Chek Names کلیک کنید. پس از جستجو شدن می‌توانید بر روی Ok کلیک کنید.



شکل ۷-۱۳

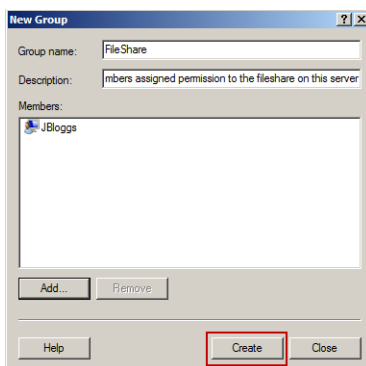
۶. گاهی اوقات حالاتی پیش می‌آید که نام اشیاء را به صورت کامل در اختیار ندارید. در این حالت می‌توانید از دکمه Advanced به منظور انجام جستجوی پیشرفته استفاده کنید. با کلیک بر روی این دکمه پنجره شکل ۷-۱۴ نمایش داده خواهد شد. با کلیک بر روی دکمه Find Now می‌توانید کلیه

اشیائی که نوع آنها را تعیین نموده‌اید مورد جستجو قرار دهید.



شکل ۷-۱۴

۷. پس از انتخاب شیء مورد نظر (در اینجا کاربری به نام JBloggs) بر روی Ok کلیک کنید.
۸. اکنون شیء مورد نظر به گروه FileShare اضافه شده است و می‌توانید با فشردن دکمه Create مراحل ایجاد گروه و افزودن کاربر به آن را تکمیل کنید.



شکل ۷-۱۵

### ایجاد گروه در خط فرمان

جهت ایجاد گروه با استفاده از خط فرمان، از دستور net localgroup استفاده می‌شود. برای آشنایی با این دستور می‌توانید عبارت زیر را در خط فرمان وارد کنید:

```
net help localgroup
```

اکنون گروه ایجاد شده با استفاده از Computer Management را می‌توانید با استفاده از دستور زیر در خط فرمان ایجاد کنید:

```
net localgroup Fileshare /add /comment:"Members assigned permission to the fileshare on this server"
```

قالب این دستور به صورت زیر می‌باشد:

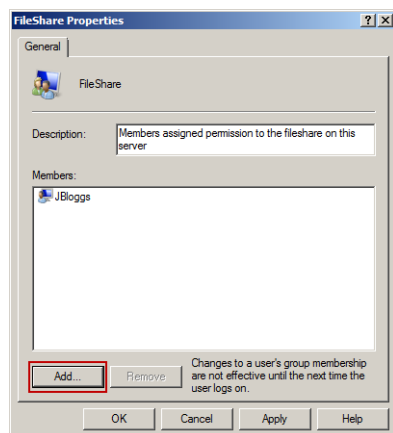
```
net localgroup <name of the new group> /add /comment:"<a description for the group>"
```

توجه داشته باشید که همزمان با ایجاد یک گروه با استفاده از خط فرمان نمی‌توانید کاربران را به آن اضافه کنید.

### افزودن کاربر به گروه با استفاده از Computer Management

جهت افزودن کاربران به گروه لازم است ابتدا به قسمت Properties گروه مراجعه کنید، بنابراین می‌توانید مراحل زیر را دنبال کنید:

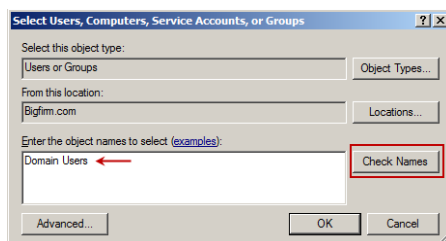
۱. بروی نام گروه کلیک راست نموده و گزینه Properties را انتخاب نمایید. در پنجره باز شده، بروی Add کلیک کنید.



شکل ۷-۱۶

۲. افزودن کاربران به گروه همانند قسمت قبل انجام می‌شود. در اینجا فرض کنید قرار است کلیه کاربران دامنه bigfirm.com به گروه FileShare Local افزوده شوند. بدین منظور لازم است ابتدا

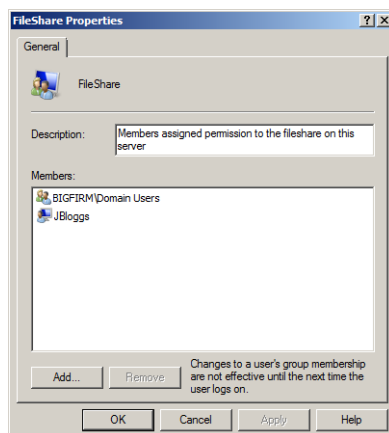
این کاربران را جستجو نمایید. عبارت “Domain Users” را در قسمت Enter the object name وارد نموده و دکمه Check Names را کلیک کنید.



شکل ۷-۱۷

۳. بر روی Ok کلیک کنید.

۴. چنانچه در شکل زیر مشاهده می‌کنید، BIGFIRM\Domain Users (کاربران دامنه Bigfirm) به لیست اشیاء موجود در گروه اضافه می‌شود. بر روی OK کلیک کنید.



شکل ۷-۱۸

۵. در نهایت بر روی Ok کلیک کنید.

افزودن کاربر به گروه با استفاده از خط فرمان

جهت افزودن کاربران به یک گروه و با استفاده از خط فرمان، لازم است بار دیگر از دستور net localgroup استفاده کنید:

```
net localgroup Fileshare jbloggs /add
```

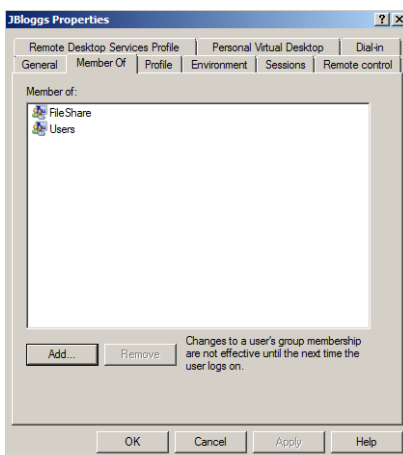
قالب کلی این دستور به صورت زیر می‌باشد:

```
net localgroup Fileshare <name of object to add to the group> /add
```

اکنون جهت افزودن کاربران دامنه (Domain Users) به گروه می‌توانید از دستور زیر استفاده کنید:

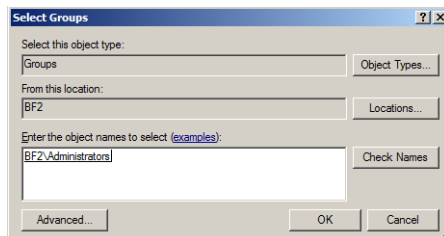
```
net localgroup Fileshare "bigfirm\domain users" /add
```

برای اطمینان از اینکه کاربر به گروه مورد نظر اضافه شده است می‌توانید به تب Member Of قسمت Properties کاربر مراجعه کنید. در این تب باید نام گروه (یا گروه‌هایی) که کاربر به آن اضافه شده است نمایش داده شود. در شکل ۷-۱۹ این وضعیت نشان داده شده است.



شکل ۷-۱۹

جهت افزودن کاربر به سایر گروه‌ها می‌توانید از دکمه Add در این پنجره استفاده کنید. پس از کلیک بر روی این دکمه باید نام گروه را وارد نموده و یا از دکمه Advanced به منظور انجام جستجوی پیشرفته استفاده کنید. در نهایت بر روی Ok کلیک کنید تا کاربر به گروه اضافه گردد. توجه داشته باشید که امکان افزودن کاربران Local به گروه‌های موجود در دامنه وجود ندارد و این دسته از کاربران تنها قابل افزودن به گروه‌های Local می‌باشند.



شکل ۷-۲۰

### حذف کاربر از گروه

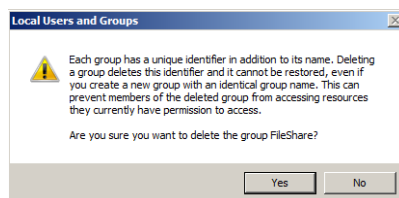
حذف کاربران از گروه‌های Local بسیار ساده است. برای انجام این کار کافی است به Properties گروه مراجعه نموده و پس از انتخاب کاربر (کاربران) موردنظر، بر روی دکمه Remove کلیک کنید. به عنوان مثال جهت حذف کاربر JBloggs از گروه FileShare می‌توانید طبق مراحل زیر اقدام کنید:

- ♦ بر روی گروه FileShare کلیک‌راست نموده و گزینه Properties را انتخاب کنید.
- ♦ در پنجره باز شده کاربر JBloggs را انتخاب کنید.
- ♦ جهت انتخاب همزمان تعدادی از کاربران از کلیدهای Shift یا Ctrl استفاده کنید.
- ♦ بر روی دکمه Remove کلیک کنید.

جهت حذف کاربر از گروه با استفاده از خط فرمان نیز می‌توانید از دستور زیر استفاده کنید:

```
net localgroup fileshare jbloggs /delete
```

در صورتی که قصد دارید کل یک گروه را حذف نمایید باید بر روی آن کلیک‌راست نموده و Delete را انتخاب کنید. با مشاهده پیغام زیر بر روی Yes کلیک کنید.



شکل ۷-۲۱

همچنین جهت حذف گروه با استفاده از خط فرمان نیز می‌توانید از دستور زیر استفاده کنید:

```
net localgroup fileshare /delete
```

### ۲-۲-۷ گروه‌های اکتیو دایرکتوری

مفاهیم پایه در گروه‌های اکتیو دایرکتوری یا مبتنی بر دامنه، تفاوت چندانی با گروه‌های Local ندارند. این دسته از گروه‌ها نیز جهت اجتماع مجموعه‌ای از اشیاء به کار برده می‌شوند. با این حال، گروه‌های اکتیو دایرکتوری به دلیل قرارگیری در کنترل‌کننده دامنه (DC) و سروکار داشتن با زیرمجموعه‌ای از دامنه‌ها و DCها، از قابلیت‌های بیشتری برخوردار می‌باشند. این قابلیت‌ها گروه را قادر می‌سازند تا اصول امنیتی مشخصی را برای مجموعه‌ای از اشیاء مانند کاربران و کامپیوترهایی

که در آن قرار داده می‌شوند تامین نموده و در سرتاسر دامنه آنها را اجرا نماید. در واقع می‌توانید از این گروه‌ها در خارج از محدوده اصلی خود استفاده کنید و حتی نوعی از گروه‌ها وجود دارند بطوری که اعضای آن از هر دامنه‌ای در یک جنگل می‌توانند انتخاب شوند.

توجه داشته باشید که در این قسمت ما بر روی گروه‌های اکتیو دایرکتوری تمرکز می‌کنیم، بنابراین هرجا صحبت از گروه نمودیم، منظور گروه اکتیو دایرکتوری می‌باشد.

گروه‌های اکتیو دایرکتوری در دو نوع پایه دسته‌بندی می‌شوند که عبارتند از:

- ♦ **Distribution group**: از این گروه‌ها به منظور دسته‌بندی تعدادی از اشیاء با یکدیگر بطوری که به صورت جمعی مورد خطاب قرار گیرند استفاده می‌گردد. سرور E-Mail می‌تواند به عنوان یک Distribution group در نظر گرفته شود. زمانی که یک کاربر قصد دارد به یک گروه Distribution ایمیلی ارسال کند، سرور mail (مانند Microsoft Exchange) تلاش می‌کند که این ایمیل را به تمام اعضاء گروه (در صورتی که پست الکترونیکی برای آنها پیکربندی شده باشد) ارسال نماید.

- ♦ **Security group**: این گروه نیز می‌تواند عملکرد ایمیل در گروه Distribution را داشته باشد اما هدف اصلی آن همانطور که از نامش مشخص است برقراری امنیت است. با استفاده از این گروه‌ها می‌توانید مجوز یا حقوقی را به یک یا مجموعه‌ای از اشیاء مانند واحدهای سازمانی، پوشه‌ها و یا قسمتی از یک برنامه اختصاص دهید. یک کاربر زمانی که در گروه امنیتی قرار داده می‌شود دیگر نیازی به داشتن حساب‌های کاربری متفاوت به ازای دامنه‌های مختلف ندارد و می‌تواند تنها با یک حساب کاربری (در صورت داشتن مجوز) از منابع در سراسر یک Forest استفاده کند.

برای هر کدام از گروه‌های مذکور سه محدوده یا Scope وجود دارد:

- ♦ **Domain local group**: این دسته از گروه‌ها تنها در دامنه‌ای که در آن ایجاد می‌شوند مورد استفاده قرار می‌گیرند. این گروه‌ها شامل حساب‌های کاربری/کامپیوتر، گروه‌های Global و گروه‌های Universal از هر دامنه‌ای در جنگل و شامل گروه‌های Domain local از دامنه فعلی می‌باشند.

- ♦ **Global group**: این گروه‌ها که در هنگام ایجاد گروه به صورت پیش‌فرض نیز انتخاب شده‌اند می‌توانند توسط کامپیوترهایی که جزء دامنه فعلی هستند و همچنین کامپیوترهای عضو سایر دامنه‌ها در جنگل اکتیو دایرکتوری مورد استفاده قرار گیرند. این گروه‌ها می‌توانند شامل حساب‌های کاربری/کامپیوتری دامنه‌ای باشند که گروه Global در آن ایجاد شده است.

- ♦ **Universal group**: مسئله‌ای که موجب تمایز این دسته از گروه‌ها با دو نوع قبلی می‌شود این است

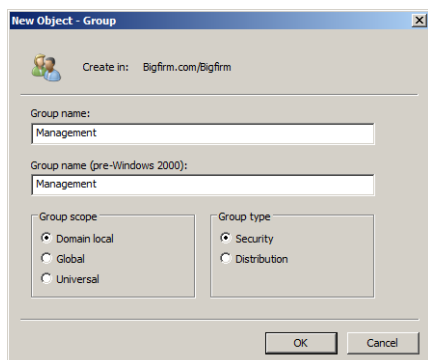
که گروه‌های global و Domain local در DC‌های دامنه‌ای که ایجاد شده‌اند ذخیره شده و جهت پاسخگویی به DC‌ها در همین دامنه استفاده می‌شوند. اما گروه‌های Universal بر روی DC‌هایی که به عنوان Global Catalog پیکربندی شده‌اند ذخیره می‌شوند. این بدین معنا است که این گروه‌ها جهت پاسخگویی به تمام DC‌ها در یک جنگل مورد استفاده قرار می‌گیرند. این امر موجب می‌شود که این گروه‌ها نه تنها توسط تمام کامپیوترها در جنگل مورد استفاده قرار گیرند بلکه شامل اعضای هر دامنه از داخل جنگل نیز باشند.

در هنگام طراحی گروه‌های global در محیط‌های بزرگ باید دقت نمود، زیرا به دلیل استفاده در تمام یک جنگل ایجاد تغییرات در آن بار زیادی در شبکه ایجاد خواهد نمود. همچنین باید مطمئن باشید که Global Catalogی که بر روی DC‌ها فعال است نزدیک به خدماتی باشد که به شدت به آن وابسته هستند. شبکه‌های کوچک و تک‌دامنه‌ای نیازی به نگرانی در این زمینه ندارند. گروه‌های global می‌توانند شامل حساب‌های کاربری/کامپیوتری، گروه‌های global و سایر گروه‌های universal از هر دامنه‌ای در جنگل باشند.

### ایجاد گروه‌های اکتیو دایرکتوری

فرض کنید قرار است که یک گروه به منظور اختصاص مجوز به مدیران در یک واحد سازمانی به نام Bigfirm ایجاد کنید بطوری که این گروه فقط در دامنه فعلی قابل استفاده باشد. برای انجام این کار لازم است که گروه شما از نوع Security و ناحیه آن نیز Domain local باشد. بنابراین مراحل زیر را دنبال کنید:

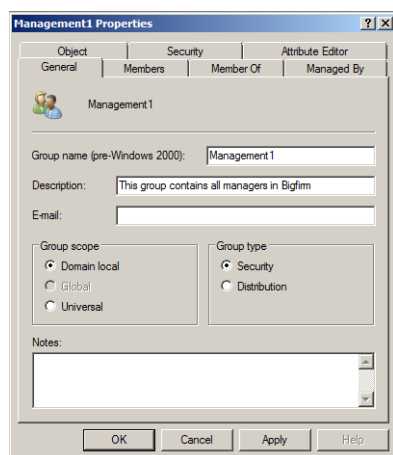
۱. در کنسول ADUC به مسیر Bigfirm.com/Bigfirm رفته و بر روی آن کلیک راست کنید.
۲. گزینه « New Group » را انتخاب کنید.
۳. در پنجره باز شده نام گروه (Management)، نوع گروه (Security) و نوع (Domain local) Scope را مشخص نموده و بر روی Ok کلیک کنید.



شکل ۷-۲۲



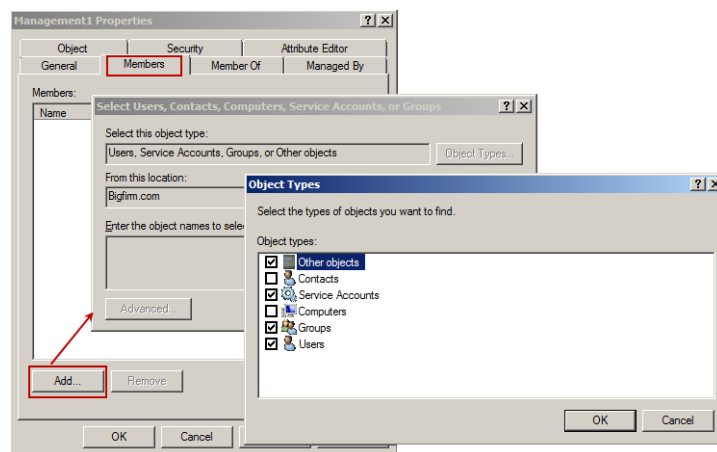
۴. جهت دسترسی به تنظیمات این گروه می‌توانید بر روی آن کلیک‌راست نموده و Properties را انتخاب کنید. پنجره زیر نشان داده خواهد شد.



شکل ۲۳-۷

۵. همانطور که در شکل ۲۳-۷ مشاهده می‌کنید تعدادی تب در این پنجره وجود دارد که در اینجا به اختصار آنها را مورد بررسی قرار می‌دهیم:

- **General:** در این تب امکان تغییر نام، افزودن توضیح، پست الکترونیکی برای گروه و همچنین تغییر نوع گروه وجود دارد. دقت داشته باشید که تغییر نوع گروه از Security به Distribution باعث می‌شود که نتوانید مجوزها را بر روی کاربران اعمال کنید.
- **Members:** در این تب می‌توانید اشیاء مورد نظر را به گروه اضافه کنید. جهت انجام این کار بر روی دکمه Add کلیک کنید.

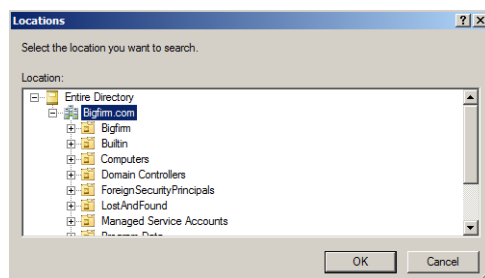


شکل ۲۴-۷

گزینه‌هایی که در پنجره “Object Types” قابل افزودن هستند عبارتند از:

- Other objects: این گزینه یک راه حل انعطاف‌پذیر جهت افزودن اعضای است که توسط برنامه‌های کاربردی ساخته می‌شوند. این اعضاء شامل کاربران، کامپیوترها و یا گروه‌های معمولی نیستند.
- Contacts: این اشیاء در اکتیو دایرکتوری به منظور نگهداری اطلاعات تماس مربوط به افراد یا سازمانها ایجاد شده و در گروه‌های distribution مورد استفاده قرار می‌گیرند.
- Service accounts: یکی از ویژگی‌های جدید در ویندوز سرور 2008R2 است که با استفاده از آن می‌توانید بجای ایجاد حساب‌های کاربری، حساب‌های مربوط به سرویس‌ها را ایجاد نموده و به آنها اختصاص دهید.
- Computers/Users: همان حساب‌های کاربری و کامپیوترهای معمولی هستند که در اکتیو دایرکتوری موجود می‌باشند.

با استفاده از دکمه Location در این پنجره نیز می‌توانید محل قرارگیری اشیاء را تعیین کنید.



شکل ۷-۲۵

- ♦ **Member Of**: زمانی که گروه فعلی عضوی از یک گروه دیگر باشد، نام آن گروه در این تب نشان داده می‌شود. به این حالت گروه‌های تو در تو<sup>۱</sup> گفته می‌شود.
- ♦ **Managed By**: با استفاده از این تب می‌توانید فرد یا گروهی را به عنوان مسئول این گروه تعیین کنید.
- ♦ **Object**: در این تب توضیحاتی راجع به نوع شیء (Group) و اطلاعاتی مانند تاریخ ایجاد نشان داده شده است که البته اطلاعات این تب قابل تغییر نمی‌باشد.
- ♦ **Security**: در این تب مجوزهایی که قرار است به کاربران گروه داده شود تعیین می‌گردند.

- ♦ **Attribute Editor:** در این تب می‌توانید نام CN گروه و سایر پارامترهای اختصاص داده شده به آن را مشاهده نموده و در صورت امکان مورد تغییر قرار دهید.

### ایجاد گروه در خط فرمان

ایجاد گروه در خط فرمان با استفاده از دستور `dsadd group` انجام می‌شود. در ابتدا برای آشنایی با ساختار آن از دستور زیر استفاده کنید:

```
dsadd group /?
```

دستوری که در ادامه آورده شده است، جهت ایجاد گروهی است که در قسمت قبل با استفاده از ابزار ADUC ایجاد کردید:

```
dsadd group "CN=Management,OU=BigFirm,DC=bigfirm,DC=com" -scope 1
```

قالب این دستور به صورت زیر می‌باشد:

```
dsadd group <distinguished name of the new group> -scope <Domain  
Local= 1 | Global = g | Universal = u>
```

این دستور بطور پیش‌فرض یک گروه Security ایجاد می‌نماید. برای ایجاد گروه‌های Distribution لازم است مقدار پارامتری به نام `-secgrp` را برابر با `no` قرار دهید. به دستور زیر توجه کنید:

```
dsadd group "CN=Management,OU=BigFirm,DC=bigfirm,DC=com" -secgrp no  
-scope g
```

تغییر نوع گروه با استفاده از عبارت زیر روشنتر می‌شود:

```
-secgrp <security group = yes | distribution group = no>
```

اکنون قصد داریم یک گروه به نام Senior Managers (مدیران ارشد) در گروه Management ایجاد نموده و سپس دو کاربر با نام‌های Joe Bloggs و Alexandra Garcia را به آن اضافه کنیم (البته فرض بر این است که قبلاً این کاربران ایجاد شده‌اند). دستور زیر این عملیات را برای شما انجام می‌دهد:

```
dsadd group "CN=Senior Management, OU=Security Groups,OU=BigFirm,  
DC=bigfirm,DC=com" -scope g -desc "This group contains senior  
managers" -memberof "CN=Management,OU=BigFirm,DC=bigfirm,DC=com"  
-members "CN=Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com" "CN=  
Alexandra Garcia,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

دقت داشته باشید که این دو کاربر در یک واحد سازمانی به نام Users که خود نیز در واحد

سازمانی Bigfirm قرار دارد ایجاد شده‌اند (فراموش نکنید که کل این دستور باید به صورت یک دستور نوشته شود و فاصله‌ها نیز در آن رعایت گردد).

جهت ایجاد تغییرات در گروه نیز می‌توانید از دستور `dsmod group` استفاده کنید. ابتدا برای آشنایی با ساختار دستور عبارت زیر را وارد کنید:

`dsmod group /?`

دستور زیر، دو کاربر Joe Bloggs و Alexandra Garcia را به گروه Management اضافه می‌کند:

```
dsmod group "CN=Management,OU=BigFirm,DC=bigfirm,DC=com" -addmbr
"CN=Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com" "CN= Alexandra
Garcia,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

قالب این دستور به صورت زیر می‌باشد:

```
dsmod group <DN of the group to manage> -addmbr <DN's of the users
to add to the group>
```

اکنون برای حذف Joe Bloggs از گروه می‌توانید دستور زیر را وارد کنید:

```
dsmod group "CN=Management,OU=BigFirm,DC=bigfirm,DC=com" -rmmbr "CN=
Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

با استفاده از دستور زیر می‌توانید لیست اعضاء گروه را حذف نموده و سپس اعضاء جدیدی را جایگزین آن کنید:

```
dsmod group "CN=Management,OU=BigFirm,DC=bigfirm,DC=com" -chmbr
"CN=Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

برای تغییر Scope گروه به Universal از دستور زیر استفاده کنید:

```
dsmod group "CN=Management,OU=BigFirm,DC=bigfirm,DC=com" -scope u
```

مقادیر قابل استفاده در پارامتر `-scope` به صورت زیر می‌باشند:

```
-scope <Domain Local = l | Global = g | Universal = u>
```

برای حذف گروه نیز می‌توانید از دستور زیر استفاده کنید:

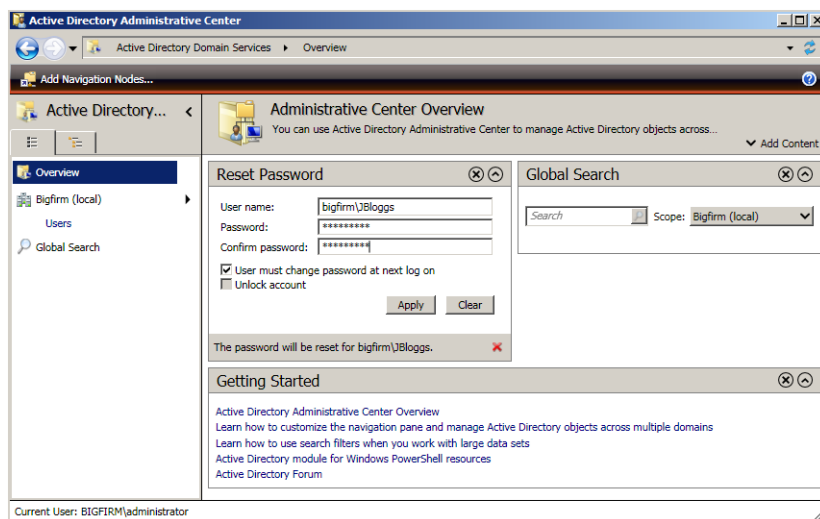
```
dsrm "CN=Management,OU=BigFirm,DC=bigfirm,DC=com"
```

### ۳-۷ مدیریت حساب‌های کاربری و گروه‌ها به کمک ADAC

ADAC یکی از ابزارهای جدید مدیریتی مایکروسافت است که برای دسترسی سریع و آسان به اقداماتی است که معمولاً تکرار می‌شوند (مثل کار با حساب‌های کاربری). در این قسمت قصد داریم نحوه مدیریت کاربران و گروه‌ها را با استفاده از این ابزار شرح دهیم. این ابزار از مسیر Administrative tools « Administrative Center » Active Directory Administrative Center در کنترل کننده دامنه ویندوز سرور 2008R2 قابل دسترسی می‌باشد.

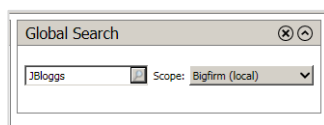
#### ۱-۳-۷ اقدامات پایه در ADAC

قبل از اینکه وارد بحث اصلی شویم اجازه دهید مروری سریع در این کنسول داشته باشیم. هنگامی که ADAC را اجرا می‌کنید، در پنل مرکزی آن انجام اقداماتی مانند بازنشانی رمز عبور کاربران و یا Unlock (بازکردن قفل) حساب‌ها امکان‌پذیر می‌باشد. این اولین مورد از دسترسی سریع به اقدامات مدیریتی می‌باشد زیرا بدون نیاز به انجام کار زیاد می‌توانید کار با حساب‌های کاربری را آغاز کنید.



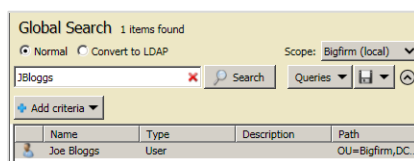
شکل ۲۶-۷

همانطور که در شکل بالا مشاهده می‌کنید، قسمتی با عنوان Global Search تعبیه شده است. این قسمت به شما امکان می‌دهد تا اشیاء موجود در اکتیو دایرکتوری را مورد جستجو قرار دهید. به عنوان مثال در شکل ۲۷-۷ کاربری با نام JBloggs مورد جستجو قرار گرفته است.



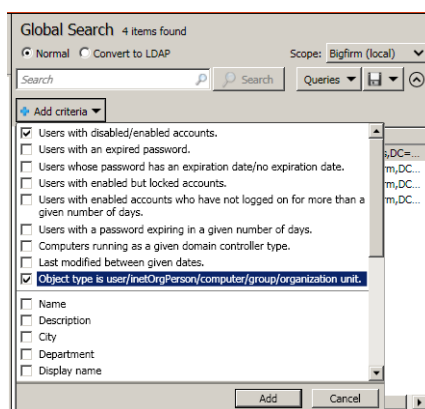
شکل ۲۷-۷

نتیجه حاصل از جستجوی بالا در شکل ۲۸-۷ نشان داده شده است.



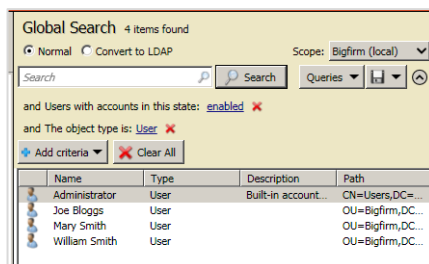
شکل ۲۸-۷

یکی از امکانات قدرتمند در زمینه جستجوی اشیاء در ADAC، دکمه Add Criteria می‌باشد. با کلیک بر روی این دکمه گزینه‌هایی نشان داده می‌شوند که با انتخاب آنها می‌توانید جستجو را بر اساس شرایط خاصی انجام دهید.



شکل ۲۹-۷

همانطور که در شکل ۲۹-۷ مشاهده می‌کنید، در قسمت شرایط جستجو دو گزینه انتخاب شده است که با استفاده از آنها می‌توان جستجو را بر اساس فعال/غیرفعال بودن حساب‌ها و همچنین تعیین نوع اشیاء انجام داد. نتایج حاصل از اجرای این جستجو در شکل ۳۰-۷ نشان داده شده است.



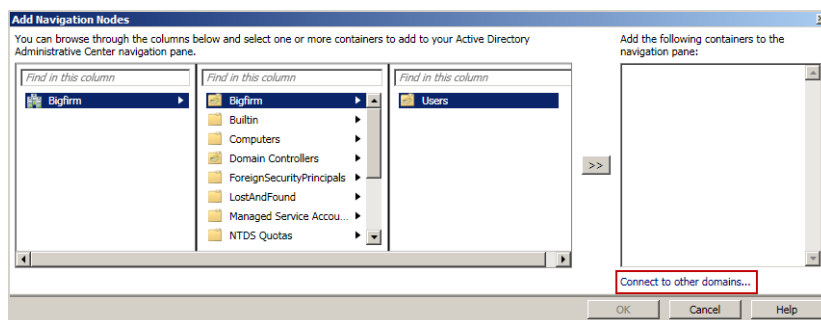
شکل ۷-۳۰

### ۷-۳-۲ حرکت در ADAC

اکنون که با مفاهیم پایه ADAC آشنا شدید اجازه دهید تا مروری در آن داشته باشیم. برای انجام این کار از پنل سمت چپ استفاده می‌شود. این پنل شامل موارد زیر می‌باشد:

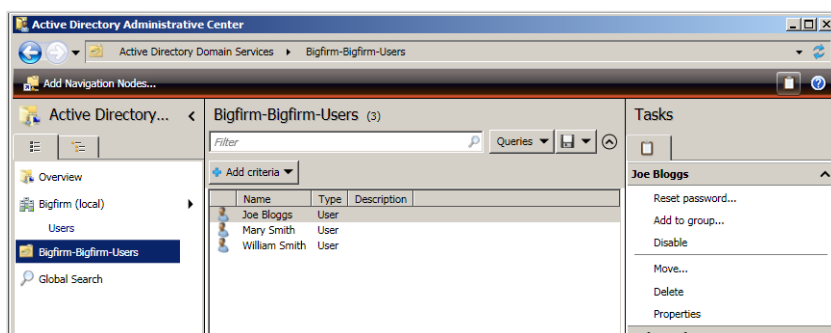
- ♦ **Overview:** این قسمت برای آغاز کار سریع با حساب‌های کاربری و همچنین انجام جستجوی ساده مورد استفاده قرار می‌گیرد.
- ♦ **Domain:** این قسمت همان نام دامنه است که از طریق آن می‌توانید به OUها و Containerها دسترسی پیدا کنید.
- ♦ **Global Search:** از این ابزار برای انجام جستجوی پیشرفته استفاده می‌شود که در قسمت قبل آن راجع به آن صحبت کردیم.

جهت افزودن گزینه‌های بیشتر به این پنل می‌توانید بر روی آن کلیک راست نموده و گزینه Add Navigation Nodes را انتخاب کنید. در پنجره “Add Navigation Nodes” ساختار اکتیو دایرکتوری شما نشان داده می‌شود. چنانچه قصد دارید گزینه‌هایی را از سایر دامنه‌ها انتخاب نمایید می‌تواند از گزینه Connect to other Domain استفاده کنید.



شکل ۷-۳۱

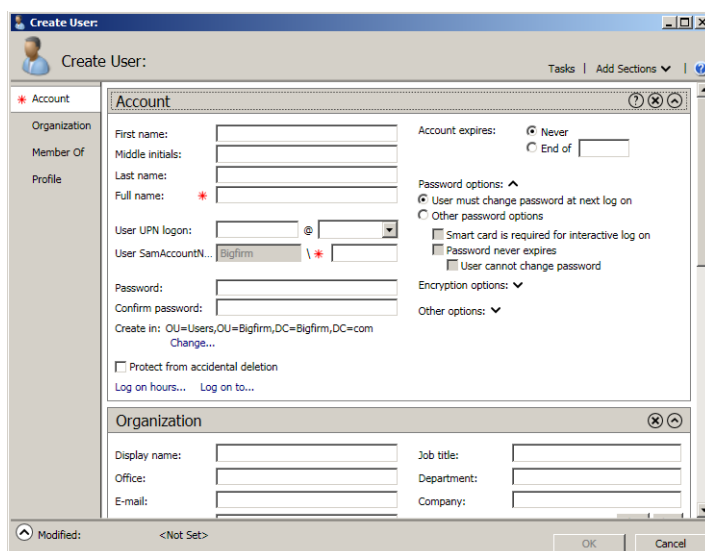
از بین آیتم‌های موجود در پنجره “Add Navigation Nodes” مواردی که قصد دارید به پنل سمت چپ ADAC اضافه کنید را انتخاب نموده و پس از انتخاب هر گزینه بر روی علامت >> کلیک کنید تا به فهرست سمت راست اضافه گردند. در نهایت با کلیک بر روی Ok می‌توانید آنها را به فهرست اصلی (پنل سمت چپ ADAC) اضافه کنید.



شکل ۳۲-۷

### ایجاد حساب کاربری

پس از افزودن واحد سازمانی Users به پنل سمت چپ، قصد داریم کاربری در آن ایجاد کنیم. برای انجام این کار بر روی Bigfirm-Users کلیک راست نموده و گزینه «New User» را انتخاب کنید. پنجره Create User نشان داده می‌شود.



شکل ۳۳-۷



همانطور که مشاهده می‌کنید در این پنجره فیلدهای زیادی جهت وارد کردن مشخصات کاربر جدید تعبیه شده است. اما تکمیل همه این فیلدها ضروری نیست و فقط می‌توانید آنهایی را که با علامت \* تعیین شده اند تکمیل کنید. با توجه به شکل بالا مشخص است که فیلدهای مربوط به Password فاقد علامت \* می‌باشند یعنی ضرورتی برای تکمیل آن وجود ندارد اما دقت داشته باشید که اگر این فیلدها خالی رها شوند، حساب کاربری پس از ایجاد شدن غیر فعال می‌شود بنابراین بهتر است رمز عبور را نیز وارد کنید.

با توجه به مطالب بالا، موارد زیر را برای ایجاد کاربر انجام دهید:

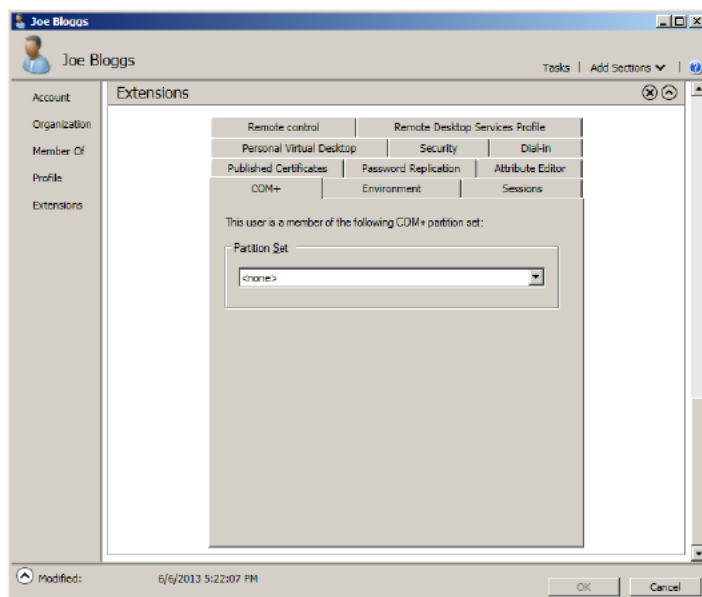
- وارد کردن مشخصات نام کاربری
- تعیین رمز عبور
- افزودن کاربر به گروه

در شکل زیر این وضعیت نشان داده شده است. با کلیک برروی Ok عملیات ساخت کاربر به پایان می‌رسد.

شکل ۷-۳۴

پس از ایجاد کاربر احتمالاً قصد دارید تنظیمات آنرا مشاهده کنید. در ADUC با مراجعه به Properties کاربر می‌توانید به تنظیمات آن دسترسی پیدا کنید بنابراین لازم است برروی نام کاربر

کلیک راست نموده و گزینه Properties را انتخاب کنید.



شکل ۷-۳۵

### ایجاد گروه

برای ایجاد گروه، ابتدا یک واحد سازمانی به نام Security Groups و سپس گروهی به نام Helpdesk را در آن ایجاد می‌کنیم.

۱. برای ایجاد OU، بار دیگر بر روی پنل سمت چپ کلیک راست نموده و گزینه Add Navigation Nodes را انتخاب کنید.

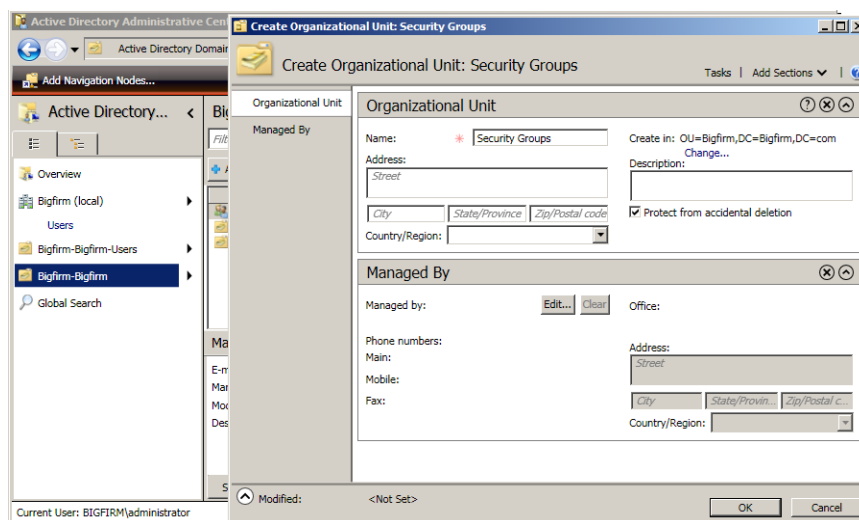
۲. در پنجره باز شده، بر روی آیتم Bigfirm دابل کلیک نموده و سپس بر روی Ok کلیک کنید تا به فهرست اضافه گردد.

۳. پس از افزوده شدن به فهرست، بر روی Bigfirm-Bigfirm کلیک راست نموده و «New Organizational Unit» را انتخاب کنید.



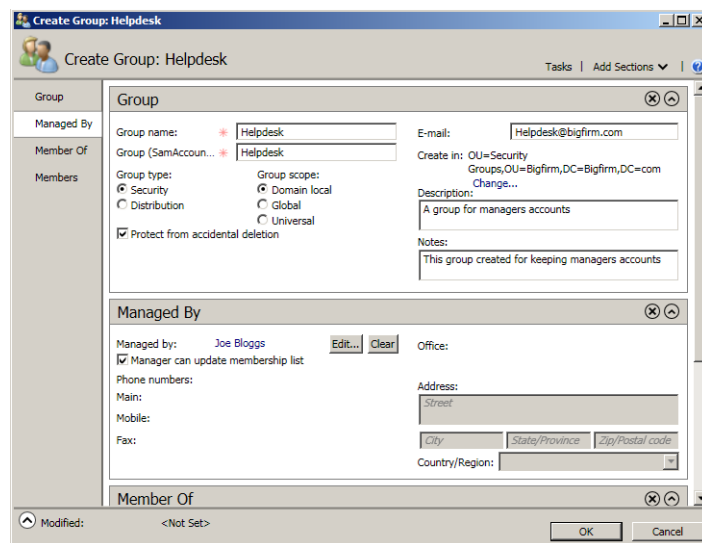
دقت داشته باشید که منظور از Bigfirm-Bigfirm، واحد سازمانی با نام Bigfirm است که در داخل دامنه Bigfirm قرار دارد. OU و گروهی که در ادامه ایجاد می‌کنید، داخل این OU (Bigfirm) ایجاد می‌شود.

۴. در پنجره باز شده نام OU را وارد نموده و بر روی Ok کلیک کنید.



شکل ۷-۳۶

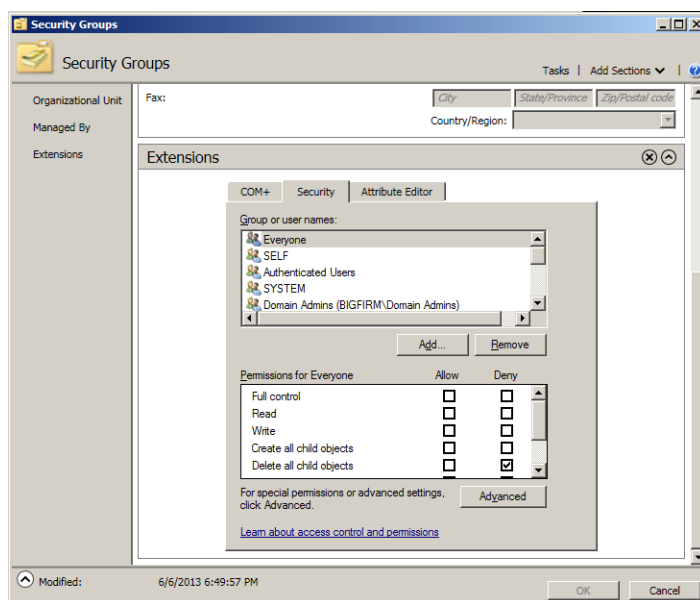
۵. بر روی OU ایجاد شده (Security Groups) کلیک راست نموده و « New Group » را انتخاب کنید.
۶. در پنجره « Create Group » موارد خواسته شده را تکمیل نمایید:



شکل ۷-۳۷

♦ نام گروه و SAM Account

- ♦ نوع و Scope گروه
  - ♦ فعال کردن گزینه Protect from accidental deletion (برای جلوگیری از امکان حذف شدن تصادفی)
  - ♦ وارد کردن آدرس ایمیل (البته این گزینه نیازمند سرویس Mail می‌باشد).
  - ♦ وارد کردن توضیحاتی در فیلدهای Description و Notes
  - ♦ تعیین مدیر گروه
۷. بر روی Ok کلیک کنید تا گروه ایجاد شود. اکنون برای دسترسی به تنظیمات آن و انجام اعمالی مانند اعمال مجوزها می‌توانید به قسمت Properties گروه مراجعه نمایید.



شکل ۷-۳۸

## ۴-۷ مدیریت حساب‌های کاربری و گروه‌ها به کمک PowerShell

PowerShell به شما امکان می‌دهد تا اقدامات مدیریتی را با استفاده از دستورات خط فرمان و اسکریپت‌ها انجام دهید. این ابزار همانند ADAC فقط در سیستم عامل‌های ویندوز سرور 2008R2، ویندوز ۷ و بعد از آن مورد استفاده قرار گرفته است. همچنین برای استفاده از این ابزار همانند ADAC لازم است که رل Directory Web Services حداقل بر روی یکی از DCها بر روی دامنه ای که تحت مدیریت قرار گرفته است نصب شده باشد. در این قسمت نحوه مدیریت کاربران و گروه‌ها را به کمک PowerShell مورد بررسی قرار می‌دهیم. برای اجرای دستورات لازم است PowerShell را از

مسیر Administrative Tools « Active Directory Module for Windows PowerShell را اجرا کنید (دقت داشته باشید که دستورات PowerShell با نام Cmdlet شناخته می‌شوند).

### ۷-۴-۱ ایجاد کاربران

برای ایجاد کاربران از دستور New-Aduser استفاده می‌شود. به مثال زیر توجه کنید:

```
PS C:\Users\Administrator> new-aduser "Boomer Moon"
```

همانند دستورات خط فرمان، امکان استفاده از help برای Cmdlet‌ها نیز وجود دارد. برای راهنمایی در زمینه دستور بالا عبارت زیر را وارد کنید:

```
PS C:\Users\Administrator> help new-aduser
```

قابلیت دیگری که در این ابزار وجود دارد، امکان استفاده از مثال‌ها در رابطه با هر دستور می‌باشد. برای دسترسی به این قابلیت از دستور زیر استفاده کنید:

```
PS C:\Users\Administrator> get-help new-aduser -examples
```

سر انجام برای دریافت جزئیات بیشتر در رابطه با دستور بالا می‌توانید از دستور زیر استفاده کنید:

```
PS C:\Users\Administrator> get-help new-aduser -detailed
```

تعدادی نکته کاربردی دیگر در این زمینه وجود دارد که آنها را شرح می‌دهیم. با استفاده از پارامتر -whatif می‌توانید مشاهده کنید که با اجرای یک دستور چه اتفاقی رخ خواهد داد. به مثال زیر توجه کنید:

```
PS C:\Users\Administrator> new-aduser BMoon -whatif
```

```
What if: Performing operation "New" on Target "CN=BMoon,CN=Users, DC=bigfirm, DC=com".
```

پارامتر بعدی -confirm است. با استفاده از این پارامتر می‌توانید یک دستور را تنها در صورت تأیید از طرف شما اجرا کنید. مثال زیر این موضوع را نشان می‌دهد:

```
PS C:\Users\Administrator> new-aduser BMoon -confirm
```

```
Confirm
Are you sure you want to perform this action?
Performing operation "New" on Target "CN=BMoon,CN=Users,DC= bigfirm,DC=com".
```

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y") :

امکان استفاده از دو پارامتر `-whatif` و `-confirm` در همه Cmdlet ها وجود دارد. استفاده از آنها به شما اطمینان می‌دهد که اقدامی که در حال انجام دادن آن هستید دقیقاً منطبق با خواسته شما می‌باشد.

در اولین دستور این بخش کاربری به نام Boomer Moon ایجاد نمودید اما این کاربر فاقد تنظیمات لازم می‌باشد. بنابراین در دستوری که در ادامه آورده می‌شود کاربر را با پیکربندی تعدادی از تنظیمات برای آن ایجاد می‌کنیم:

```
PS C:\Users\Administrator> new-ADUser "Boomer Moon" SamAccountName
"BMoon" -GivenName "Boomer" -Surname "Moon" -DisplayName "Boomer
Moon" -Path 'OU=Users,OU=BigFirm,DC=bigfirm,DC=com'
-UserPrincipalName BMoon@bigfirm.com
```

اکنون به تشریح پارامترهای به کار رفته در این دستور می‌پردازیم:

- ♦ **SamAccountName**:- این پارامتر معادل نام ورود کاربر (pre-Windows 2000) می‌باشد. بنابراین زمانی که نام BMoon را برای کاربری انتخاب می‌کنید، این کاربر با نام دامنه BigFirm\BMoon می‌تواند به دامنه وارد شود.
- ♦ **GivenName**:- نام یا First Name است.
- ♦ **Surname**:- نام خانوادگی یا Last Name می‌باشد.
- ♦ **DisplayName**:- نام کامل کاربر یا Full Name می‌باشد.
- ♦ **Path**:- نام DN واحد سازمانی که کاربر در آنجا ساخته می‌شود را تعیین می‌کند. در این مثال، کاربر در مسیر BigFirm\Users از دامنه Bigfirm.com ایجاد می‌شود.
- ♦ **UserPrincipalName**:- این پارامتر (UPN) همان نام کاربری مربوط به کاربر است که به همراه نام دامنه آورده می‌شود و معادل با آدرس ایمیل کاربر در دامنه می‌باشد.

پس از اجرای دستور بالا کاربر ایجاد می‌شود اما باید توجه داشته باشید که هنوز Password برای این کاربر تعیین نشده و بنابراین غیر فعال است. در ادامه نحوه تعیین رمز عبور و فعال‌سازی کاربران را شرح خواهیم داد.

#### ۷-۴-۲ تعیین رمز عبور

اختصاص رمز عبور به کاربران با استفاده از پارامتر `AccountPassword` انجام می‌شود. قبل از استفاده از این پارامتر حالتی را در نظر بگیرید که قرار است به ۱۰ کاربر رمز عبور یکسانی

اختصاص دهید. با استفاده از دستور زیر می‌توانید این رمز عبور را تعریف نموده و سپس در زمان ایجاد هر کاربر از آن استفاده کنید:

```
PS C:\Users\Administrator> $pw = read-host "Please Enter The Password" -AsSecureString
```

```
Please Enter The Password: *****
```

```
PS C:\Users\Administrator> new-ADUser "Boomer Moon" -SamAccountName "BMoon" -GivenName "Boomer" -Surname "Moon" -DisplayName "Boomer Moon" -Path 'OU=Users,OU=BigFirm,DC=bigfirm,DC=com' -UserPrincipalName "BMoon@bigfirm.com" -AccountPassword $pw -Enabled 1 -ChangePasswordAtLogon 1
```

♦ در دستور اول، متغیری به نام \$pw تعریف شده تا مقدار رمز عبور در آن ذخیره شود. مقدار Read-Host شما را وادار می‌کند که مقداری را برای رمز عبور تعیین کنید. پارامتر -AsSecureString نیز رمز عبور شما را به یک رشته امن تبدیل می‌کند. مقدار ذخیره شده در \$pw تا زمانی که PowerShell را ببندید و یا مقدار جدید تعریف کنید در حافظه PowerShell باقی می‌ماند.

♦ در دستور دوم پارامتر AccountPassword با مقدار \$pw مقداردهی شده که به معنای استفاده از رمز عبور ذخیره شده در این متغیر می‌باشد. پارامتر Enable با دو مقدار ۱ (فعال) و ۰ (غیرفعال) مقداردهی می‌شود. در پارامتر ChangePasswordAtLogon نیز مقدار ۱ بیانگر اجبار کاربر برای تغییر رمز عبور و ۰ به معنای عدم اجبار او می‌باشد.

چنانچه تنها قصد ایجاد یک کاربر دارید، می‌توانید از رمز عبور جداگانه‌ای استفاده کنید. در دستور زیر با استفاده از پارامتر read-host می‌توانید پس از اجرای دستور، رمز عبور خود را وارد کنید:

```
PS C:\Users\Administrator> new-ADUser "Boomer Moon" -SamAccountName "BMoon" -GivenName "Boomer" -Surname "Moon" -DisplayName "Boomer Moon" -Path 'OU=Users,OU=BigFirm,DC=bigfirm,DC=com' -UserPrincipalName "BMoon@bigfirm.com" -AccountPassword (read-host "Please Enter The Password" -AsSecureString) -Enabled 1 -ChangePasswordAtLogon 1
```

```
Please Enter The Password: *****
```

### ۳-۴-۷ ایجاد همزمان تعدادی کاربر

برای ایجاد همزمان تعدادی از کاربران لازم است تا دستورات آنها در یک فایل ذخیره شوند. فایل‌هایی که دستورات PowerShell در آن ذخیره می‌شوند دارای پسوند csv می‌باشند. نمونه‌ای از این

فایل‌ها که در ادامه آورده شده است، شامل دستورات ایجاد سه کاربر می‌باشد. محتویات این فایل که نام آن users.csv می‌باشد به صورت زیر است:

Name	SamAccountName	GivenName	SurName
Rachel Kelly	RKelly	Rachel	Kelly
Ulrika Gerhardt	UGerhardt	Ulrika	Gerhardt
Tomasz Kozlowski	TKozlowski	Tomasz	Kozlowski
DisplayName	Path	UserPrincipalName	AccountPassword
Rachel Kelly	OU=Users, OU=BigFirm, DC=bigfirm, DC=com	RKelly@bigfirm.com	NewPassw0rd
Ulrika Gerhardt	OU=Users, OU=BigFirm, DC=bigfirm, DC=com	UGerhardt@bigfirm.com	NewPassw0rd
Tomasz Kozlowski	OU=Users, OU=BigFirm, DC=bigfirm, DC=com	TKozlowski@bigfirm.com	NewPassw0rd

چنانچه فایل بالا را در Notepad اجرا کنید، با چیزی شبیه زیر مواجه خواهید شد:

```
Name,SamAccountName,GivenName,Surname,DisplayName,Path,UserPrincipal
Name,AccountPassword
Rachel Kelly,RKelly,Rachel,Kelly,RachelKelly,"OU=Users, OU=BigFirm
,DC=bigfirm,DC=com",RKelly@bigfirm.com,NewPassw0rd
Ulrika Gerhardt,UGerhardt,Ulrika,Gerhardt,Ulrika Gerhardt, "OU=Users
,OU=BigFirm,DC=bigfirm,DC=com",UGerhardt@bigfirm.com,NewPassw0rd
Tomasz Kozlowski,TKozlowski,Tomasz,Kozlowski,Tomaz Kozlowski, "OU=
Users,OU=BigFirm,DC=bigfirm,DC=com",TKozlowski@bigfirm.com,
NewPassw0rd
```

اکنون برای اجرای همه سطرهای این فایل در PowerShell، با فرض اینکه مسیر فایل درایو C است، از دستور زیر استفاده کنید:

```
PS C:\Users\Administrator> Import-CSV c:\users.csv | foreach
{New-ADUser -Name $_.Name -SamAccountName $_.SamAccountName
-GivenName $_.GivenName -Surname $_.Surname -DisplayName
$_.DisplayName -Path $_.Path -UserPrincipalName $_.UserPrincipalName
-AccountPassword (ConvertTo-SecureString -AsPlainText
$_.AccountPassword -Force) -Enabled $true -ChangePasswordAtLogon 1}
```

پارامترهای به کار رفته در این دستور عبارتند از:



- ♦ **IMPORT-CSV**: از این پارامتر به منظور فراخوانی فایل از مسیر موردنظر استفاده می‌شود.
- ♦ |: این نماد برای استفاده کردن از یک پارامتر به همراه پارامتر دیگر مورد استفاده قرار می‌گیرد و با فشردن کلیدهای ترکیبی Shift و \ نوشته می‌شود.
- ♦ **FOREACH**: این پارامتر تک تک سطرها را موجود در فایل را بررسی و اجرا می‌کند.
- ♦ **NEW-ADUSER**: برای تعیین اینکه کاربر در حال ایجاد شدن است مورد استفاده قرار می‌گیرد.
- ♦ **\$\_**: زمانی که از این علامت به همراه پارامترهای موجود در دستور New-User استفاده می‌شود، مقادیر موجود در هریک از سرایندهای سطرها را به پارامترها اختصاص می‌دهد. مثلاً پارامتر **\$\_Name** به سرایند **Name** در فایل CSV اشاره نموده و مقدار آن را در این پارامتر وارد می‌کند.
- ♦ **AccountPassword**: این پارامتر نیز جهت اختصاص رمز عبور به کاربر مورد استفاده قرار می‌گیرد.

#### ۷-۴-۴ Unlock کردن حساب کاربری

برای Unlock کردن یک حساب کاربری از دستور **Unlock-ADAccount** استفاده می‌شود. به مثال زیر توجه کنید:

```
PS C:\Users\Administrator> Unlock-ADAccount -identity JBloggs
```

در دستور بالا پارامتر **-identity** نام کاربر را گرفته و آنرا بازگشایی (Unlock) می‌نماید. در این دستور ما از نام معمولی کاربر استفاده کردیم اما امکان استفاده از DN کاربر نیز وجود دارد. در ادامه، دستور بالا را با استفاده از نام DN کاربر به کار برده‌ایم:

```
PS C:\Users\Administrator> Unlock-ADAccount -identity "CN=Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com"
```

امکان بازنشانی رمز عبور کاربر با استفاده از این دستور نیز وجود دارد:

```
PS C:\Users\Administrator> set-adaccountpassword -identity jbloggs -reset -newpassword (read-host "Please Enter The New Password" -AsSecureString)
```

```
Please Enter The New Password: *****
```

در دستور **Set-Adaccountpassword**، از پارامتر **-identity** به منظور تعیین شیء تحت مدیریت و از پارامتر **-reset** نیز برای تعیین اینکه عمل تغییر رمز عبور به صورت عادی نبوده و بدون داشتن رمز عبور قبلی می‌باشد. علت استفاده از این پارامتر این است که کاربر رمز عبور خود را فراموش نموده و چاره‌ای جز بازنشانی آن نیست. از عبارت **Read-Host** در پارامتر

newpassword- نیز برای دریافت رمز عبور و تبدیل آن به یک رشته امن استفاده می‌شود.

دستور دیگری که مورد استفاده قرار می‌دهیم، Get-ADuser می‌باشد. از این دستور به منظور بازیابی مشخصات کاربر استفاده می‌گردد:

```
PS C:\Users\Administrator> get-aduser jbloggs
```

```
DistinguishedName: CN=JoeBloggs,OU=Users,OU=BigFirm,DC=bigfirm,DC=com
Enabled           : True
GivenName        : Joe
Name             : Joe Bloggs
ObjectClass      : user
ObjectGUID       : 5fa7f3ac-93ec-4cf8-bf80-21368f8b3a8d
SamAccountName   : JBloggs
SID              : S-1-5-21-3625881918-2577536232-3089104624-1108
Surname          : Bloggs
UserPrincipalName: JBloggs@bigfirm.com
```

این دستور بطور پیش‌فرض دسته کوچکی از مشخصات کاربر را بازیابی می‌کند. برای نمایش کلیه مشخصات کاربر می‌توانید از دستور زیر استفاده کنید:

```
PS C:\Users\Administrator> get-aduser jbloggs -properties * | more
```

برای تغییر مشخصات یک کاربر می‌توانید از دستور Set-ADuser استفاده کنید. به عنوان مثال دستور زیر توضیحی را به کاربر با نام AGarcia اضافه می‌کند:

```
PS C:\Users\Administrator> Set-ADUser AGarcia -Description "IT Manager"
```

برای دسترسی به لیست پارامترهای قابل استفاده در این دستور می‌توانید از عبارت زیر استفاده کنید:

```
PS C:\Users\Administrator> Help Set-ADUser
```

به عنوان آخرین دستور در این بخش، نحوه تغییر مشخصات تعدادی از کاربران به صورت همزمان را شرح می‌دهیم. به عنوان مثال فرض کنید قصد دارید مشخصات تمام اشیاء موجود در واحد سازمانی Users که در Bigfirm قرار دارد (Bigfirm.cim/Bigfirm/Users) را تغییر دهید. برای انجام این کار می‌توانید از دستور زیر استفاده کنید:

```
PS C:\Users\Administrator> Get-ADUser -Filter 'Name -like "*"\'
-SearchBase "OU=Users,OU=BigFirm,DC=bigfirm,DC=com" | Set-ADUser
-Description "Member of IT"
```

### ۷-۴-۵ فعال‌سازی و غیرفعال کردن حساب کاربری

جهت فعال‌سازی حساب کاربری از دستور `Enable-ADAccount` استفاده می‌شود. دستور زیر حساب کاربری کاربر `BMoon` را فعال می‌نماید:

```
PS C:\Users\Administrator> Enable-ADAccount -Identity BMoon
```

دستور زیر نیز جهت غیرفعال کردن حساب کاربری بالا استفاده می‌شود:

```
PS C:\Users\Administrator> Disable-ADAccount -Identity BMoon
```

همچنین برای حذف حساب کاربری نیز می‌توانید از دستور زیر استفاده کنید:

```
PS C:\Users\Administrator> remove-aduser -Identity BMoon -confirm
```

```
Confirm
Are you sure you want to perform this action?
Performing operation "Remove" on Target "CN=BMoon,CN=Users,DC=bigfirm,DC=com".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):
```

### ۷-۴-۶ ایجاد گروه

برای ایجاد گروه از دستور `New-ADGroup` استفاده می‌شود. یکی از ویژگی‌های جالب دستورات در PowerShell این است که به راحتی می‌توان کاربرد هر دستور را از نام آن تشخیص داد. به عنوان مثال در اینجا دستور `New` مشخص می‌کند که در حال ایجاد یک شیء جدید هستیم. یا مثلاً دستور `Set` تعیین کننده تنظیم چیزی (مثل مشخصات) است. قطعه کدی که در ادامه آورده شده است، گروهی با نام `IT Administrators` در مسیر `Bigfirm.com/Bigfirm/Security Groups` ایجاد می‌کند:

```
PS C:\Users\Administrator> New-ADGroup -Name "IT Administrators"
-SamAccountName "IT Administrators" -GroupCategory Security
-GroupScope DomainLocal -DisplayName "IT Administrators" -Path "OU=Security Groups,OU=BigFirm,DC=bigfirm,DC=com" -Description "Members of this group are in IT"
```

پارامترهایی که در این دستور به کار گرفته شده‌اند عبارتند از:

- ♦ `Name`: نام گروه را مشخص می‌کند.
- ♦ `SamAccountName`: نام کاربری یا همان `pre-Windows 2000` است.

- ♦ GroupCategory: نوع گروه را مشخص می‌کند و با مقادیر Security (یا ۱) و Distribution (یا ۰) تعیین می‌شود.
- ♦ GroupScope: نوع Scope گروه را تعیین نموده و با یکی از مقادیر DomainLocal (یا ۰)، Global (یا ۱) و Universal (یا ۲) مقداردهی می‌شود.
- ♦ DisplayName: نامی است که گروه با آن نشان داده می‌شود.
- ♦ Path: محل قرارگیری گروه را تعیین می‌کند.
- ♦ Description: توضیحی راجع به گروه ارائه می‌دهد.

پس از ایجاد گروه، لازم است تعدادی کاربر به آن افزوده شود. برای انجام این کار از دستور `Add-ADGroupMember` استفاده می‌شود. به مثال زیر توجه کنید:

```
PS C:\Users\Administrator> Add-ADGroupMember "IT Administrators"
-Member JBloggs
```

دستور بالا تنها یک کاربر با نام JBloggs را به گروه IT Administrators اضافه می‌کند، اما شاید بخواهید تعدادی از کاربران را به گروه اضافه کنید. برای انجام این کار می‌توانید دستور بالا را به صورت زیر به کار ببرید:

```
PS C:\Users\Administrator> add-adgroupmember "IT Administrators"
```

نتیجه حاصل از اجرای این دستور به صورت زیر می‌باشد که در آن نام هر کاربر به ترتیب وارد می‌شود:

```
cmdlet Add-ADGroupMember at command pipeline position 1
Supply values for the following parameters:
Members[0]:AGarcia
Members[1]:JElway
Members[2]:
```

این دستور دو کاربر با نام‌های AGarcia و JElway را به گروه اضافه نموده و تا زمانی که دستور به پایان نرسیده است می‌توانید نام سایر کاربران را در آن وارد کنید.

دستور بالا را می‌توان به صورت زیر نیز مورد استفاده قرار داد:

```
PS C:\Users\Administrator> Add-ADGroupMember "IT Administrators"
-Member JBloggs,AGarcia
```

برای افزودن تعداد زیادی از کاربران به گروه می‌توانید از دستور زیر استفاده کنید:

```
PS C:\Users\Administrator> Add-ADGroupMember "IT Administrators"
-Member (Get-ADUser -Filter 'Name -like "*" -SearchBase "OU=Users,
OU=BigFirm,DC=bigfirm,DC=com")
```

این دستور ابتدا با استفاده از Get-ADuser همه کاربران موجود در واحد سازمانی Users را مورد جستجو قرار داده سپس آنها را به گروه IT Administrators اضافه می‌کند.

جهت افزودن یک گروه به گروه دیگر می‌توانید از دستور زیر استفاده کنید:

```
PS C:\Users\Administrator> add-adgroupmember "IT Administrators"
"Helpdesk"
```

این دستور گروه Helpdesk را به گروه IT Administrators اضافه می‌کند.

اکنون جهت مشاهده کلیه اعضاء گروه IT Administrators می‌توانید از دستور زیر استفاده کنید:

```
PS C:\Users\Administrator> Get-ADGroupMember "IT Administrators"
```

```
distinguishedName: CN=Helpdesk,OU=Security Groups,OU=BigFirm,DC=
bigfirm,DC=com
name              : Helpdesk
objectClass       : group
objectGUID       : 93e9b21b-023a-4e46-88b5-3c4cbf71f218
SamAccountName    : Helpdesk
SID              : S-1-5-21-3625881918-2577536232-3089104624-1115
distinguishedName: CN=Joe Bloggs,OU=Users,OU=BigFirm,DC=bigfirm, DC=com
name              : Joe Bloggs
objectClass       : user
objectGUID       : 5fa7f3ac-93ec-4cf8-bf80-21368f8b3a8d
SamAccountName    : JBloggs
SID              : S-1-5-21-3625881918-2577536232-3089104624-1108
```

چنانچه قصد دارید تنها مشخصات خاصی برای شما نمایش داده شوند، می‌توانید آنها را فیلتر کنید. به عنوان مثال در دستور زیر نمایش مشخصات برحسب مقدار نام و نوع شیء فیلتر شده است:

ObjectClass	Name
-----	----
group	Helpdesk
user	Joe Bloggs

برای حذف کاربران از گروه می‌توانید از دستور Remove-ADGroupMember استفاده نمایید. به مثال زیر توجه کنید:

```
PS C:\Users\Administrator> Remove-ADGroupMember "IT Administrators"
-Member JBloggs
```

```
Confirm
Are you sure you want to perform this action?
```

```
Performing operation "Set" on Target "CN=IT Administrators,OU= Security
Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```

جهت حذف همزمان تعدادی از کاربران نیز می‌توانید از دستور زیر استفاده کنید:

```
PS C:\Users\Administrator> Remove-ADGroupMember -Identity "IT
Administrators" -Member AGarcia,JBloggs
```

```
Confirm
Are you sure you want to perform this action?
Performing operation "Set" on Target "CN=IT Administrators,OU= Security
Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is
"Y"):
```

دستور بالا دو کاربر AGarcia و JBloggs را از گروه حذف می‌کند.

همانند افزودن کاربر، حذف تعدادی از کاربران با استفاده از نتیجه جستجوی آنها امکان‌پذیر است. به مثال زیر توجه کنید:

```
PS C:\Users\Administrator> Remove-ADGroupMember "IT Administrators"
-Member (Get-ADUser -Filter 'Name -like "*" -SearchBase "OU=Users
,OU=BigFirm,DC=bigfirm,DC=com")
```

```
Confirm
Are you sure you want to perform this action?
Performing operation "Set" on Target "CN=IT Administrators,OU= Security
Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```

جهت حذف همه اشیاء موجود در گروه می‌توانید از دستور زیر استفاده کنید:

```
PS C:\Users\Administrator> Remove-ADGroupMember "IT Administrators"
-Member (Get-ADGroupMember "IT Administrators")
```

```
Confirm
Are you sure you want to perform this action?
Performing operation "Set" on Target "CN=IT Administrators,OU= Security
Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```

این دستور ابتدا همه اعضاء گروه را مورد جستجو قرار داده (Get-ADGroupMember) و سپس آنها را حذف می‌کند.

در کلیه مثال‌هایی که در بالا آورده شد، چنانچه با عبارت "OU=Security Groups,OU=Bigfirm"

مواجهه شدید منظور اشیائی است که در واحد سازمانی Security Groups قرار گرفته‌اند که البته این OU نیز در واحد سازمانی Bigfirm قرار دارد (یعنی در مسیر Bigfirm.com/Bigfirm/Security Groups)

#### ۷-۴-۷ حذف گروه

جهت حذف گروه از دستور Remove-ADGroup استفاده می‌شود. به عنوان مثال دستور زیر گروهی به نام IT Administrators را از واحد سازمانی Security Groups که در واحد Bigfirm قرار دارد (Bigfirm.com/Bigfirm/Security Groups) حذف می‌کند:

```
PS C:\Users\Administrator> Remove-ADGroup "IT Administrators"

Confirm
Are you sure you want to perform this action?
Performing operation "Remove" on Target "CN=IT Administrators,OU= Security
Groups,OU=BigFirm,DC=bigfirm,DC=com".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is
"Y"):
```

در نهایت لازم به ذکر است که اگرچه در ابتدا کار با دستورات PowerShell ممکن است کمی دشوار به نظر برسد اما کمی کار کردن با آنها می‌تواند استفاده از این دستورات را لذت بخش نماید. البته این نکته فراموش نشود که در سازمان‌های کوچک نیازی به استفاده از PowerShell نیست زیرا کارهای زیادی برای انجام دادن وجود ندارد. اما در سازمان‌های بزرگ که بسیاری از اقدامات (مثل ایجاد یا تغییر کاربران) به دفعات زیاد تکرار می‌شوند خودکارسازی آنها با استفاده از این دستورات می‌تواند سربار مدیریتی را به شدت کاهش دهد.

## « فصل ۸ »

ایجاد و مدیریت سیاست‌های گروهی

**Creating and Managing**  
CREATING AND MANAGING

**Group Policies**  
GROUP POLICIES





زمانی که صحبت از اکتیو دایرکتوری به میان می‌آید، لازم است که در مورد Group Policy (GP) نیز صحبت شود. Group Policy در واقع به سیاست‌هایی گفته می‌شود که بر روی اشیاء اکتیو دایرکتوری اعمال شده و نحوه عملکرد آنها را در شبکه تعیین می‌کند. Group Policy یک فناوری جدید برای اکتیو دایرکتوری در ویندوز سرور 2008R2 به شمار نمی‌آید زیرا از زمان ویندوز 2000 وجود داشته است، اما با انتشار هر نسخه یا Service Pack جدید از ویندوز سرور (و اکتیو دایرکتوری) این فناوری نیز دست‌خوش پیشرفت‌ها و بهبودهای قابل توجهی شده است. این پیشرفت‌ها به ویژه از زمان ویندوز سرور 2008 در مواردی همچون مدیریت Group Policy (با استفاده از ابزارهایی همچون Group Policy Management Console و Group Policy Management Editor)، مدیریت تنظیمات (بیش از ۵۰۰۰ مشخصه قابل تنظیم)، کنترل اشیاء و همچنین عیب‌یابی زیرساخت Group Policy حاصل شده است. پیکربندی و توسعه Group Policy به کمک Group Policy objects (GPOs) انجام می‌شود. GPOها کانتینترها یا گروه‌هایی از تنظیمات (Policy Setting) هستند که می‌توانند به حساب‌های کاربری و کامپیوترهای یک اکتیو دایرکتوری در طول شبکه اعمال شوند. اشیاء Policy با استفاده از Group Policy Management Editor یا به اختصار GPME ایجاد می‌شوند و در این ابزار قابل ویرایش می‌باشند. با استفاده از GPOها می‌توان اعمالی مانند مشخص نمودن تعدادی برنامه برای نصب بر روی Desktop کاربران، تعیین نحوه انتخاب رمز عبور کاربران، محدود کردن سهمیه<sup>۱</sup> استفاده از دیسک برای کاربران و ... را انجام داد. امکان ایجاد یک GPO همه جانبه به منظور اعمال تعدادی از سیاست‌ها و یا ایجاد تعدادی GPO هریک برای یک عمل خاص وجود دارد.

در این فصل قصد داریم به نحوه ایجاد و مدیریت Group Policyها با استفاده از ابزارهای مدیریتی آن بپردازیم. بطور کلی مهمترین مباحثی که در این فصل مورد بررسی قرار می‌گیرند عبارتند از:

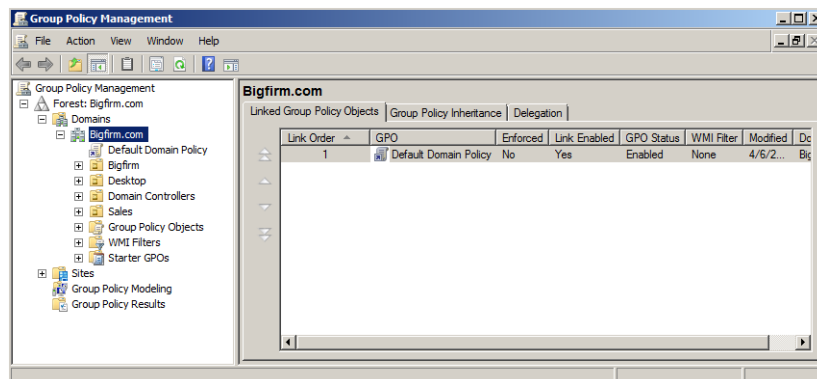
- ♦ آشنایی با سیاست‌های Local و اشیاء Group Policy<sup>۲</sup> (GPO)
- ♦ ایجاد GPOها
- ♦ مدیریت و عیب‌یابی Group Policyها

## ۸-۱ ایجاد GPOها

برای ایجاد Group Policy مبتنی بر دامنه لازم است ابزاری به نام Group Policy Management را اجرا کنید. این ابزار از مسیر «Start Administrative Tools» Group Policy Management و یا از طریق کنسول Server Manager قابل دسترسی می‌باشد.

1. Quota

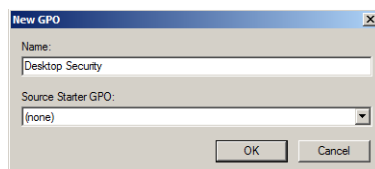
2. Group Policy Objects



شکل ۸-۱

جهت ایجاد یک GPO ابتدا بر روی نام جنگل (Forest: Bigfirm.com) کلیک کرده تا آیتم‌های زیرمجموعه آن نشان داده شوند. سپس از زیر نام دامنه (Bigfirm.com) آیتم Group Policy Objects را پیدا نموده و مراحل زیر را دنبال کنید:

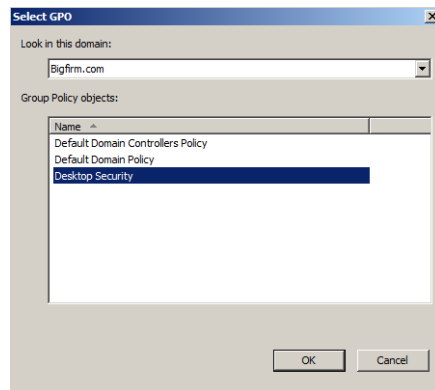
۱. بر روی Group Policy Objects کلیک راست نموده و New را انتخاب کنید.
۲. در پنجره "New GPO" نام انتخابی برای GPO (در اینجا Desktop Security) را وارد نموده و بر روی OK کلیک کنید.



شکل ۸-۲

پس از انجام مراحل بالا، GPO ای با نام Desktop Security ایجاد می‌شود ولی این GPO به هیچ کانتینری در دامنه پیوند نشده است، بنابراین شاید قصد داشته باشید که تنظیماتی را برای این GPO پیکربندی نموده و آنرا به یک سایت، دامنه و یا OU پیوند دهید. برای انجام این کار (با فرض اینکه قبلاً یک OU با نام Desktop در ADUC ایجاد کرده‌اید)، مراحل زیر را دنبال کنید:

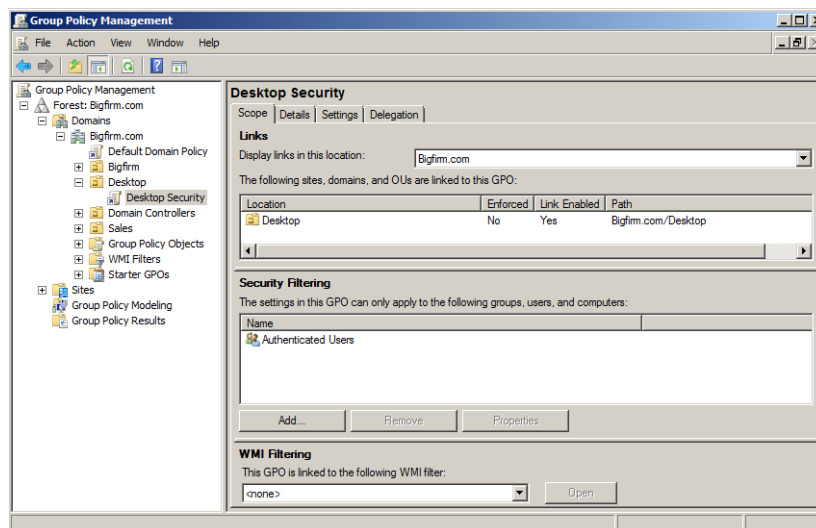
۱. بر روی Desktop OU کلیک راست نموده و گزینه Link an Existing GPO را انتخاب کنید.
۲. در پنجره "Select GPO" لیستی از GPO های موجود نشان داده می‌شود. GPO با نام Desktop Security را انتخاب نموده و بر روی OK کلیک کنید.



شکل ۳-۸

۳. برای ایجاد و پیوند دادن GPO به یک دامنه نیز کافی است بر روی نام آن دامنه کلیک راست نموده و گزینه “Create a GPO in this domain, and link it here” را انتخاب کنید.

پس از ایجاد GPO و پیوند آن به Desktop OU، بر روی OU کلیک کنید. در پنل سمت راست تعدادی تب ظاهر می‌شود. این تب‌ها عبارتند از: Scope، Details، Settings و Delegation.



شکل ۴-۸

### تب Scope

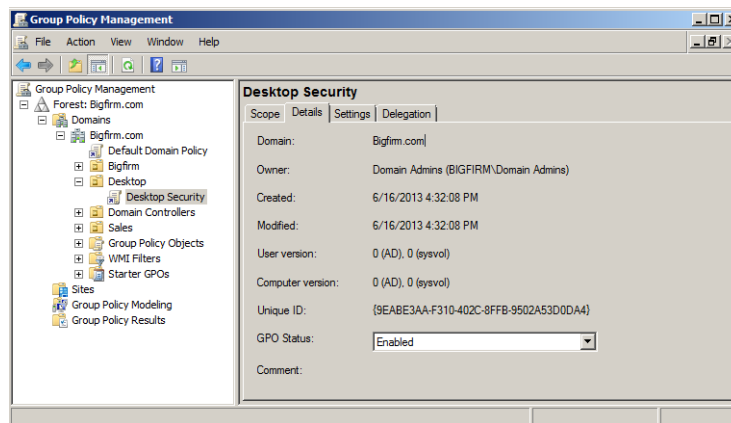
تب Scope کمک می‌کند تا بسیاری از جنبه‌های GPO را پیگیری کنید. مهمترین جزئیات قابل

مشاهده در این تب، نام گره‌ای از اکتیو دایرکتوری است که GPO به آن پیوند شده است.

- در قسمت **Link** می‌توان نام OU، دامنه و یا سایتی که GPO به آن پیوند شده را مشاهده نمود.
- قسمت **Security Filtering** مشخص می‌کند که کدام کاربران و یا گروه‌ها می‌توانند تنظیمات را بر روی GPO اعمال کنند. انجام فیلترینگ برای دادن مجوز یا حذف آن تنها با اضافه کردن و یا حذف کردن کاربران و گروه‌ها از این لیست قابل انجام می‌باشد.
- سومین قسمت موجود در این تب، **WMI Filtering**<sup>۱</sup> می‌باشد. WMI یک زیرساخت مدیریتی است که مدیران شبکه را قادر می‌سازد تا بتوانند اشیاء روی یک شبکه را نظارت و کنترل کنند. برای خودکار کردن فرایندهای امنیتی، می‌توان یک برنامه یا اسکریپت WMI نوشت و آن را به صورت Remote یا Local به کار برد. با یک WMI Query می‌توان سیستم‌های موجود در شبکه را بر حسب مشخصه خاصی از آنها فیلتر نمود، مانند مقدار فضای RAM آزاد آنها، سیستم عامل، Service Pack، نرم افزارهای نصب شده و تنظیمات پرینتر. جهت کسب اطلاعات بیشتر در این زمینه به آدرس [http://technet.microsoft.com/en-us/library/cc779036\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc779036(v=ws.10).aspx) مراجعه کنید.

### تب Details

در این تب اطلاعاتی راجع به GPO و وضعیت آن ارائه شده است. همچنین امکان فعال یا غیر فعال کردن تنظیمات GPO برای کامپیوترها یا کاربران نیز در این تب امکان پذیر می‌باشد.

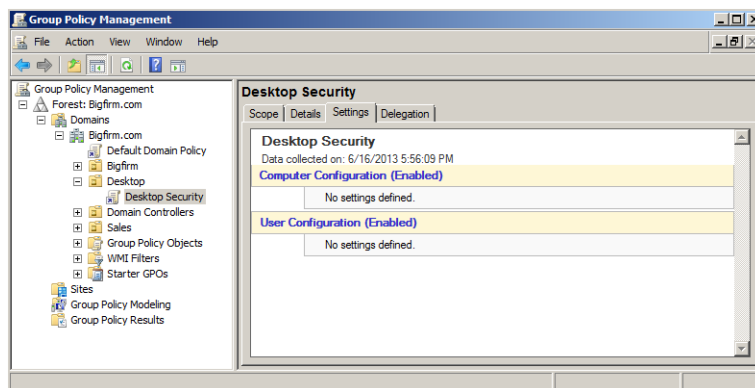


شکل ۵-۸

### تب Settings

این تب شامل داده‌های پویای مرتبط با تنظیمات پیکربندی شده برای GPO می‌باشد.

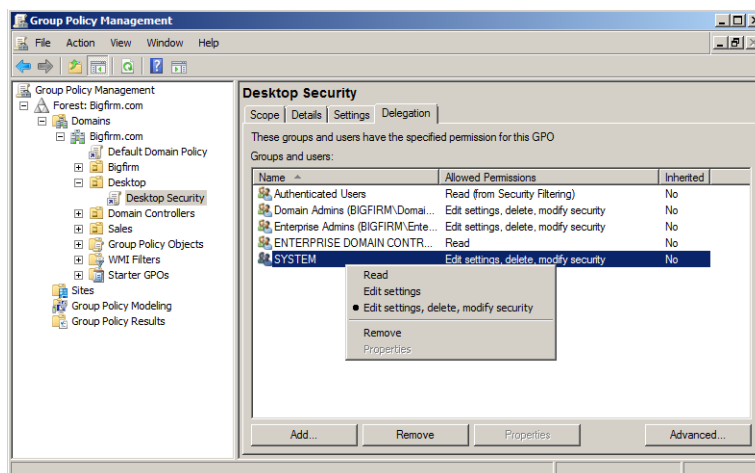
1. Windows Management Instrumentation Filters



شکل ۸-۶

### تب Delegation

در این تب لیست افراد و یا گروه‌های مجاز جهت مدیریت GPO آورده شده است. سه سطح مدیریتی برای GPO تعریف شده است که سطح اول (Read) تنها مجوز خواندن و دو سطح بعدی مجوز ویرایش GPO را به کاربران و یا گروه‌ها واگذار می‌کنند. در شکل زیر این سطوح قابل مشاهده هستند.

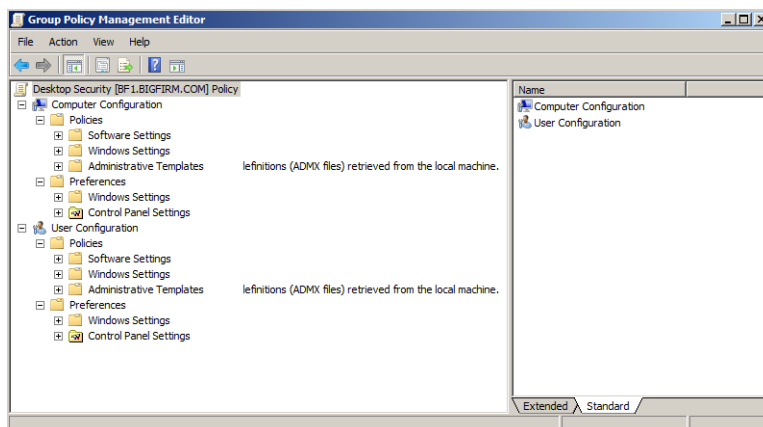


شکل ۸-۷

### تنظیمات GPO

پس از ایجاد GPO اجازه دهید نحوه ایجاد تغییرات در آن را نیز مورد بحث قرار دهیم. به گره

Group Policy Objects در GPMC باز گشته و بر روی GPO کلیک راست کنید. با انتخاب گزینه Edit پنجره GPME اجرا می شود.



شکل ۸-۸

دو دسته کلی از تنظیمات در این پنجره قابل انجام هستند. دسته اول **Computer Configuration** است که مربوط به تنظیمات حساب های کامپیوتری و دسته دوم **User Configuration** تنظیمات مربوط به حساب های کاربری می باشد. در این قسمت تعدادی تنظیمات قابل اعمال بر روی حساب ها را معرفی نموده و در قسمت های بعد مثال هایی در این زمینه ارائه می دهیم.

- ♦ برای مشخص کردن یک بسته نرم افزاری (جهت نصب از طریق Group Policy) پوشه Policies\Software Settings\Software Installation را انتخاب نموده و بر روی آن کلیک راست کنید. گزینه «New Package» را انتخاب نموده و در پنجره باز شده مسیر برنامه مورد نظر را تعیین و سپس آنرا نصب کنید. پس از نصب می توانید مشخصات آنرا تنظیم کنید.

- ♦ برای تنظیم مدت زمانی که کاربران باید برای تغییر رمز عبور خود منتظر بمانند، به مسیر Computer Configuration\Policies\ Windows Settings\Security Settings\Account Policies>Password Policy رفته و سپس با دابل کلیک بر روی هر یک از گزینه ها، تنظیمات مربوط به رمز عبور کاربران را مشخص کنید.

- ♦ برای تنظیم سیاستی که اعضای یک گروه را محدود می کند، به مسیر Computer Configuration\Policies\ Windows Settings\ Security Settings Restricted Groups رفته و انتخاب کنید. بر روی این آیتم کلیک راست نموده و Add Group را انتخاب کنید. پس از انتخاب گروه بر روی نام آن دابل کلیک نموده و کاربران یا گروه هایی که در این گروه باید قرار گیرند را تعیین

نمایید.

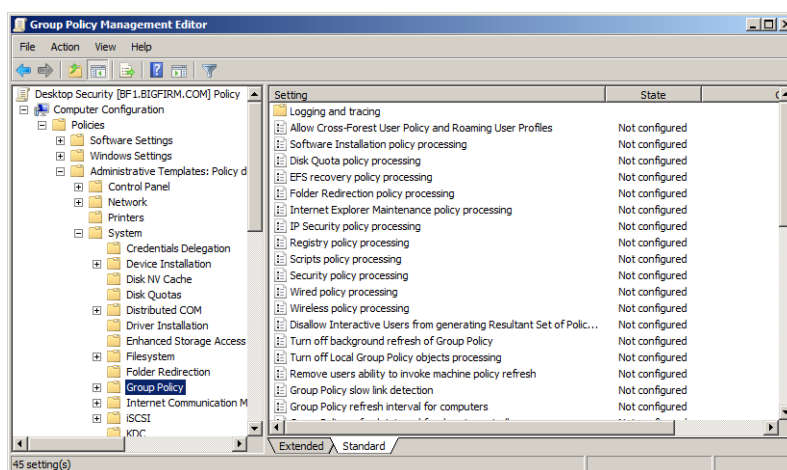
- ♦ برای تنظیم تغییر مسیر یک پوشه، به مسیر \User Configuration\Policies\Windows Settings\Folder Redirection رفته و سپس یک پوشه (به عنوان مثال Start Menu) را انتخاب کنید. در پنل سمت راست، کلیک‌راست نموده و Properties را انتخاب کنید. در صفحه باز شده می‌توانید تنظیمات مربوط به محل قرار گیری محتویات پوشه مورد نظر را انجام دهید.

## ۲-۸ تغییر عملکرد پیش‌فرض Group Policy

Group Policy بطور ذاتی یک امکان فوق‌العاده به شمار می‌آید اما برخی عملکردها در آن وجود دارند که ممکن است بخواهید تغییر دهید و یا کنترل کنید. تغییر این عملکردها با استفاده از GPOها و تنظیمات آنها قابل انجام است. بسیاری از این تنظیمات نیازی به پیکربندی ندارند اما در مواردی که نیازمند ایجاد برخی از تنظیمات جزئی هستید، این کار لازم است.

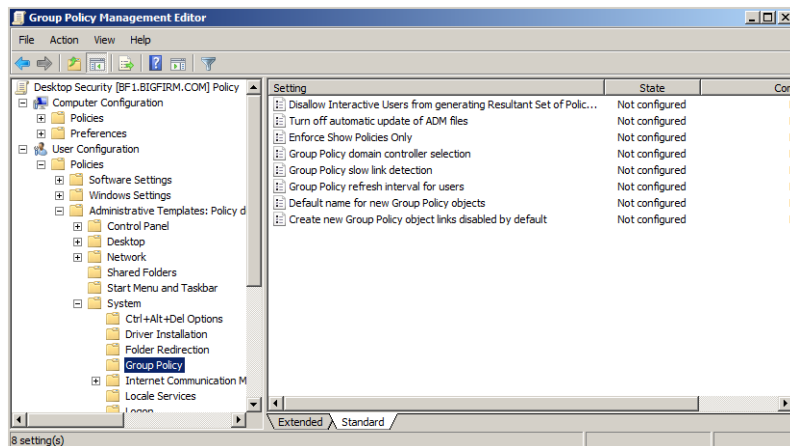
## ۱-۲-۸ سیاست‌های Group Policy

تنظیمات GPO از زیرمجموعه Administrative Templates در گره‌های User Configuration و Computer Configuration قابل دسترسی می‌باشد. (Policies\Administrative Templates\System\Group Policy). در شکل‌های ۸-۹ و ۸-۱۰ به ترتیب آپشن‌های Group Policy برای هر دو گره Computer Configuration و User Configuration نشان داده شده است. در ادامه مهمترین آپشن‌های پیکربندی را مورد بررسی قرار می‌دهیم.



شکل ۸-۹: آپشن‌های Computer Configuration



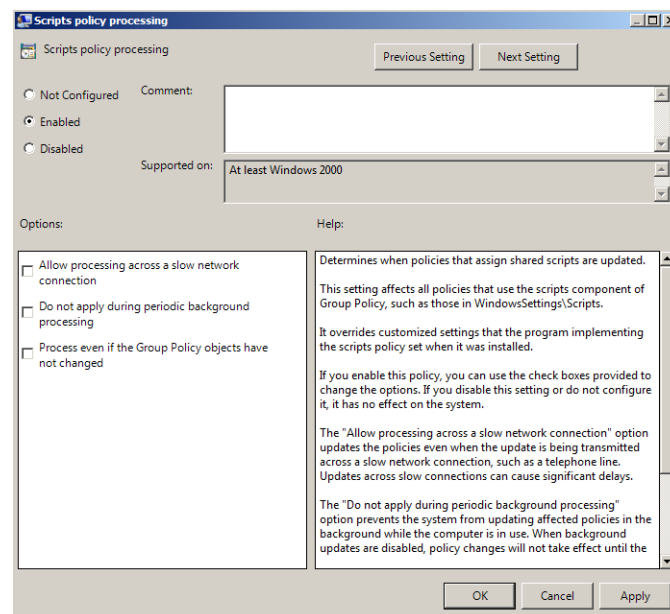


شکل ۸-۱۰: آپشن‌های User Configuration

- ♦ **Group Policy refresh intervals for users/computers/domain controller**: این سیاست‌ها چگونگی Refresh شدن GPOها را زمانی که کاربران و کامپیوترها در حال کارکردن هستند مشخص می‌کند. این پارامترها اجازه تغییر Refresh شدن پیش‌فرض و تنظیم بازه‌های زمانی برای Refresh شدن را مشخص می‌کنند.
- ♦ **Turn off background refresh of Group Policy**: چنانچه این گزینه را فعال کرده باشید، سیاست‌ها تنها در زمان راه اندازی سیستم و logon کردن کاربران Refresh می‌شوند. این امکان برای دلایل بهبود کارایی در شعبه‌های سازمان زمانی که دارای ۱۵۰۰ کامپیوتر که هر ۹۰ دقیقه Refresh شده و باعث ایجاد ازدحام در یک ارتباط WAN می‌شوند مفید است.
- ♦ **Policy processing options**: این سیاست‌ها با نام‌هایی مثل **Policy Processing** Registry و Folder Redirection **Policy Processing** به منظور شخصی‌سازی عملکرد GPOهای مختلف در دسترس هستند. این تنظیمات در زیرمجموعه گره Computer Configuration موجود بوده و هر سیاست حداقل دو مورد از سه آپشن زیر را ارائه می‌دهند:
  - **Allow processing across a slow network connection**: در ارتباطات کند تعدادی از سیاست‌ها به منظور افزایش کارایی می‌توانند غیرفعال شوند. (امکان تعریف ارتباط کند از طریق سیاست Group Policy Slow Link Detection امکان‌پذیر می‌باشد). البته دقت داشته باشید که تنظیمات امنیتی و Registry Policy Processing همیشه اعمال شده و امکان خاموش کردن آنها وجود ندارد.
  - **Do not apply during periodic background processing**: این گزینه تعیین می‌کند چنانچه

کامپیوتر در حال اجرا است، سیاست‌هایی که آپدیت شده و قرار است در عملکرد سیستم تغییری ایجاد کنند نتوانند بر روی کامپیوتر اعمال شوند. اعمال تغییرات ایجاد شده در زمان ورود بعدی کاربر و یا Restart شدن کامپیوتر انجام خواهد شد.

- **Process even if the Group Policy objects have not changed**: برای افزایش امنیت و جلوگیری از ایجاد تغییر در تنظیمات Policy توسط یک کاربر، فعال‌سازی این سیاست اطمینان می‌دهد که در هر بار Refresh شدن، تمام تنظیمات مجدداً تکرار می‌شوند. دقت داشته باشید که فعال‌سازی این سیاست ممکن است بطور قابل توجهی باعث کاهش کارایی گردد.

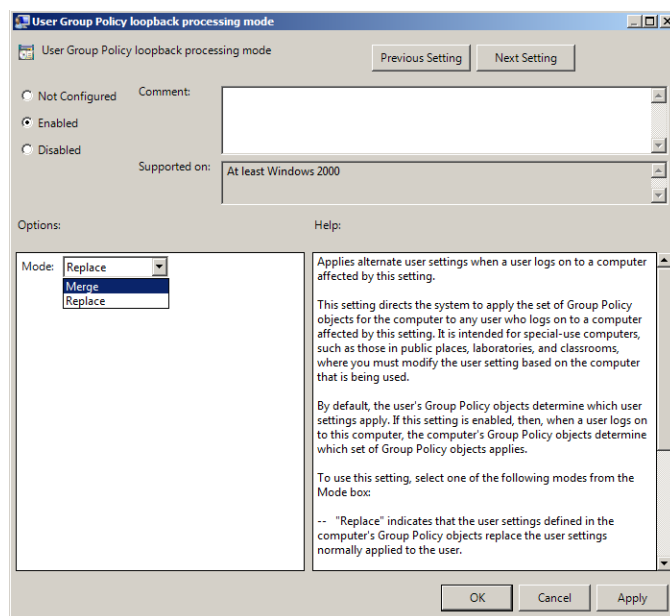


شکل ۸-۱۱

- **Loopback processing mode**: بطور پیش‌فرض تنظیمات User Policy بعد از سیاست‌های Computer Configuration پردازش می‌شوند. همچنین کاربران تنظیمات Policy را بدون در نظر گرفتن ماشینی که به آن وارد می‌شوند دریافت می‌کنند. به عنوان مثال فرض کنید که با استفاده از User Policy تعریف شده است که در هنگام ورود کاربران به دامنه، تعدادی برنامه کاربردی برای آنها نصب شود. زمانی که شما به منظور انجام اقدامات مدیریتی به سرور وارد می‌شوید، دیگر نیازی به نصب شدن این برنامه‌ها نخواهید داشت بنابراین لازم است که این Policy‌ها بجای کاربر، مطابق با کامپیوتری که به آن وارد می‌شوید اعمال شوند (Loopback processing). به عنوان مثالی دیگر می‌توان حالتی را در نظر گرفت که لازم است سیاست‌های کامپیوتر،

سیاست‌های مربوط به کاربران را نادیده بگیرند. این حالت زمانی است که از کامپیوتر در مکان‌های عمومی مانند کتابخانه‌ها، آزمایشگاه‌های کامپیوتر در دانشگاه‌ها، و ... استفاده می‌شود. دو حالت برای کنترل عملکرد این سیاست وجود دارد:

- **Merge mode:** این گزینه تنظیمات معمولی کاربر و تنظیمات GPOهای کامپیوتر را با یکدیگر ترکیب می‌کند. چنانچه در این تنظیمات تضادی وجود داشته باشد، تنظیمات کاربر در GPOهای کامپیوتر نسبت به تنظیمات معمولی کاربر اولویت پیدا می‌کنند.
- **Replace mode:** این گزینه تنظیمات GPOهای کامپیوتر را جایگزین تنظیمات معمولی کاربر می‌نماید.

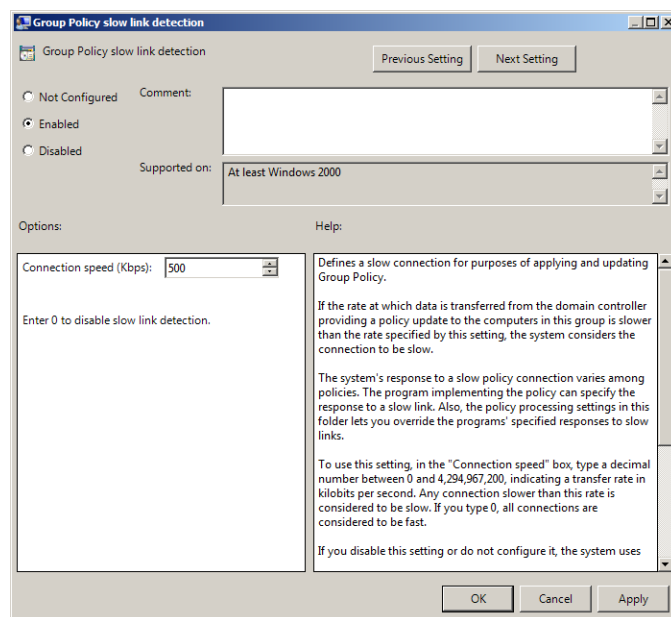


شکل ۸-۱۲

## ۸-۲-۲ Group Policy بروی لینک‌های کم سرعت

Group Policy هنوز هم در طول لینک‌های کم سرعتی مانند Dial\_Up عمل می‌کنند (این لینک‌ها ممکن است در بین سایت‌هایی که شعبه‌های سازمان را به یکدیگر و یا شعبه مرکزی متصل می‌کنند برقرار باشد). به دلیل اینکه استفاده از لینک‌های کم سرعت باعث ایجاد مسائل کارایی می‌شود، در Group policy برای آنها تنظیماتی جهت تعریف سرعت لینک و همچنین چگونگی اعمال سیاست‌ها بروی این لینک‌ها وجود دارد. برای انجام تنظیمات لینک‌های کم سرعت می‌توانید از مسیر

Group Policy Computer Configuration\ Policies\Administrative Templates\System\Group Policy slow link detection را پیدا نموده و با فعال‌سازی آن، سرعت مورد نظر برای لینک کم سرعت را تعیین کنید. زمانی که این Policy را فعال می‌کنید بطور پیش‌فرض عدد ۵۰۰ در آن درج شده است که می‌توانید با توجه به نوع ارتباط خود آنرا تغییر دهید. (به عنوان مثال سرعت ۵۶ کیلو بیت/ثانیه برای ارتباط Dial\_Up).



شکل ۸-۱۳

توجه داشته باشید که پس از تعریف لینک کم سرعت باید امکان ارتباط از طریق این لینک را فعال کنید. این کار با فعال کردن گزینه “Allow processing across a slow network connection” در Policyها امکان‌پذیر می‌باشد.

### ۸-۳ استفاده از Group Policy

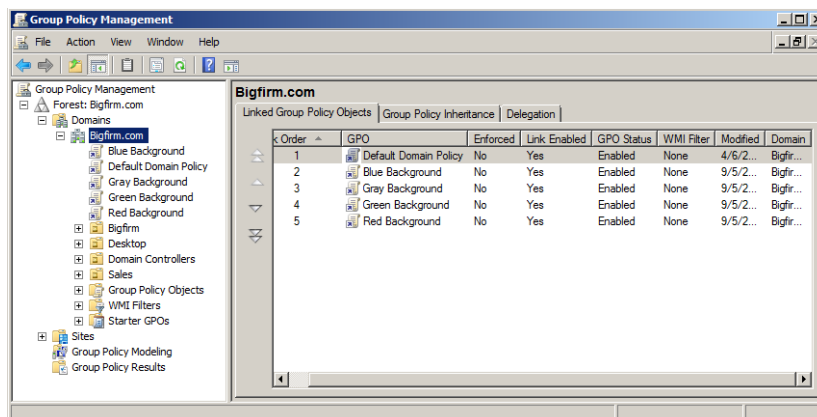
هنگام استفاده از Group Policy باید مطمئن شوید که سیاست‌ها به روش قابل اطمینانی اعمال می‌شوند. بیشتر اوقات استفاده از Group Policy ساده است و تنها زمانی که در هنگام استفاده از آن با تضاد مواجه می‌شوید یا قصد دارید عملکرد پیش‌فرض آنرا تغییر دهید ممکن است کار برایتان کمی پیچیده‌تر شود. با این وجود زمانی که در حال طراحی و پیاده‌سازی تنظیمات Policy هستید باید درک کاملی از نتیجه اجرای آنها بر روی کاربران و کامپیوترها داشته باشید.

### ۸-۳-۱ Group policy چگونه اعمال می‌شود

اکنون با داشتن یک یا دو GPO بزودی با بخش دردرس ساز Group policy مواجه می‌شوید: دانستن این مطلب که نتیجه نهایی برای کاربران و کامپیوترها چه خواهد بود. به عنوان مثال فرض کنید یک کاربر سؤال می‌کند که “چرا پس زمینه<sup>۱</sup> من بنفش است؟”، بعد از آن متوجه می‌شوید که سیستم این کاربر از جاهای زیادی سیاست‌های خود را دریافت می‌کند و ممکن است این سیاست‌ها در مسائلی مانند رنگ پس زمینه متفاوت باشند. بنابراین کدامیک سیاست دارای اولویت خواهد بود؟

### سیاست‌ها از پایین به بالا در GUI اجرا می‌شوند

اجازه دهید کار را با یک وضعیت ساده آغاز کنیم: حالتی که Policyها تنها از یک دامنه دریافت می‌شوند. فرض کنید که در حال جستجوی یک گره در پنجره GPMC هستید و پس از پیدا کردن آن مشاهده می‌کنید که تعدادی GPO به آن پیوند شده است. این وضعیت در شکل ۸-۱۴ نشان داده شده است.



شکل ۸-۱۴

در این وضعیت (مسلماً خیالی) دامنه دارای پنج Group policy است که چهارتای آن برای تنظیم رنگ پس زمینه ایستگاه‌های کاری به خاکستری، سبز، قرمز یا آبی است. برای مشاهده اینکه کدامیک از GPOها دارای اولویت است، بروی گره دامنه (Bigfirm.com) کلیک نموده و در پنل سمت راست تب Linked Group Policy Objects را انتخاب کنید. با توجه به Policyهای موجود در این تب حدس می‌زنید کدامیک برنده خواهند شد؟ خاکستری، قرمز، سبز یا آبی؟

پاسخ به این سوال در دو قاعده برای حل تعارض GPOها نهفته است:

- ♦ قاعده اول: توجه به آخرین سیاستی که بر روی گره اعمال شده است.
- ♦ قاعده دوم: اجرای سیاست‌ها از پایین به بالا انجام می‌شود همانگونه که در GUI (منظور همان پنجره گرافیکی است) ظاهر شده‌اند.

با خواندن سیاست‌ها از پایین صفحه به بالای آن مشاهده می‌کنید که سیستم ابتدا به Policy که رنگ پس زمینه را به قرمز تنظیم می‌کند توجه می‌نماید. پس از آن به سیاستی که رنگ را به سبز، پس از آن سیاست تنظیم رنگ به خاکستری و در آخر نیز به سیاست رنگ آبی نگاه می‌کند. از آنجایی که آبی آخرین سیاست اعمال شده است بنابراین برنده است و تاثیر رنگ سه سیاست قبلی را خنثی می‌نماید.

چنانچه قصد داشته باشید اولویت این سیاست‌ها را تغییر دهید، می‌توانید از دکمه‌های جهتی که در این تب تعبیه شده است استفاده کنید. دقت داشته باشید که هر سیاستی که به بالا انتقال داده شود اولویت بالاتری اتخاذ می‌کند و تأثیر سیاست‌های پایین‌تر از خود را خنثی می‌نماید.

#### ترتیب استفاده از Group Policy

مثالی که در قسمت قبل ارائه شد، تنها حالتی را در نظر گرفته بود که GPO ها به دامنه پیوند شده‌اند، اما می‌توانید GPO ها را به سایر گره‌ها در اکتیو دایرکتوری نیز پیوند دهید:

- ♦ GPO ها می‌توانند به سایت‌ها نیز پیوند شده بدون اینکه به ماشین‌ها و کاربرانی که در آن قرار گرفته‌اند توجهی داشته باشند.
- ♦ OU ها نیز می‌توانند شامل پیوندهای GPO باشند. توجه داشته باشید که هر OU می‌تواند شامل تعدادی OU دیگر باشد، بنابراین هر یک از OU های موجود در طی این زنجیره (OU های داخل سایر OU ها) می‌توانند شامل GPO هایی باشند که به آنها پیوند شده است.
- ♦ Policy ها به صورت Local نیز قابل اعمال بر روی ماشین‌ها و کاربران می‌باشند.

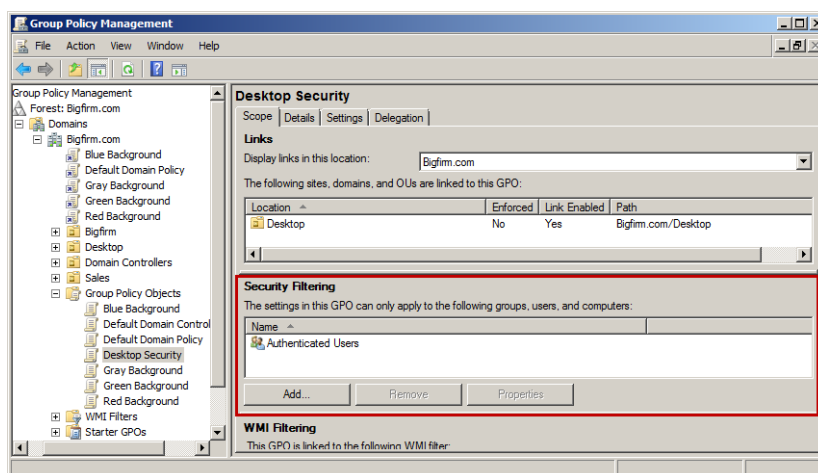
با توجه به موارد بالا چنانچه مجدداً بخواهید سوال “کدام Policy برنده است؟” را پاسخ دهید باید ترتیب زیر را دنبال کنید:

- ♦ Local های Policy
- ♦ Policy های اعمال شده بر روی سایت‌ها
- ♦ Policy های اعمال شده بر روی دامنه‌ها
- ♦ Policy های اعمال شده بر روی OU ها
- ♦ Policy های اعمال شده بر روی Child OU ها

اگر سیاست دامنه بگوید که “قبل از خاموش کردن سیستم باید به آن Login کنید” و سیاست OU بگوید که “اجازه خاموش کردن سیستم را قبل از Login کردن دارید” سیاست OU دارای اولویت خواهد بود زیرا آخر از همه اعمال شده است. اگر یک Policy بگوید که “آنها قفل کن” و سیاست بعدی بگوید “پیکربندی نشده”، تنظیمات پیکربندی نشده باقی می ماند. بر عکس، زمانی که یک سیاست “پیکربندی نشده” است و سیاست بعدی “قفل کردن باشد” تنظیمات به صورت قفل کردن باقی خواهد ماند. به همین ترتیب اگر چندین سیاست به صورت متوالی آورده شده باشند، آن سیاستی برنده خواهد بود که آخر از همه (از پایین به بالا) خوانده می شود.

### ۸-۳-۲ فیلتر کردن Group policy با استفاده از ACL

لیست کنترل دسترسی<sup>۱</sup> (ACL) به فهرستی از کاربران گفته می شود که برای خواندن و یا ایجاد تغییر در GPOها مجوزدهی می شوند. برای دسترسی به این لیست، بروی یکی از GPOها در GPMC کلیک نموده (به عنوان مثال GPO با نام Desktop Security) و سپس تب Scope را از پنل سمت راست مشاهده کنید. در قسمت Security Filtering لیست ACL برای GPO قابل مشاهده می باشد.

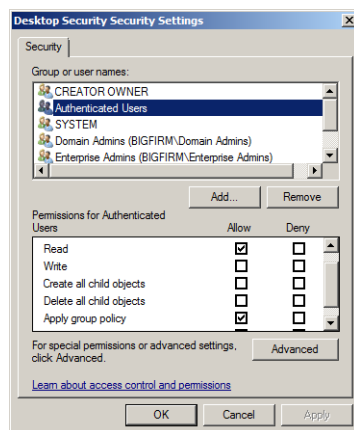


شکل ۸-۱۵

مدیران دامنه<sup>۲</sup> و مدیران سازمانی<sup>۳</sup> باید مجوز خواندن و ایجاد تغییر، و کاربران مجاز<sup>۴</sup> باید مجوز خواندن و اعمال Group policy ها را داشته باشند. با این وجود، در شکل ۸-۱۶ شما تنها کاربران مجاز را در لیست مشاهده خواهید نمود. علت این است که این لیست تنها برای کاربران، کامپیوترها و

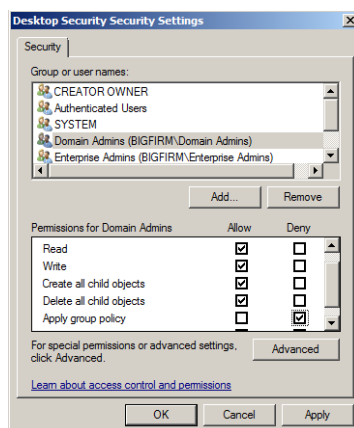
1. Access Control List
2. Domain Admins
3. Enterprise Admins
4. Authenticated Users

گروه‌هایی است که دارای مجوز اعمال تنظیمات GPO می‌باشد. برای مشاهده لیست کامل ACL به تب Delegation بروید. در این تب بر روی دکمه Advanced کلیک کنید تا پنجره زیر نمایش داده شود.



شکل ۸-۱۶

ممکن است اتفاق افتد که شما یک GPO برای محدود کردن Desktop کاربران ایجاد نموده و نخواهید که بر روی گروه خاصی از افراد اعمال شود. گروه Authenticated Users (کاربران مجاز) شامل همه افراد (حساب‌های کاربری و کامپیوتری) بجز مهمانان (guests) می‌باشد. بنابراین بطور پیش‌فرض GPO بر روی تمام افراد به غیر از مهمانان اعمال می‌شود. این بدین معناست که Domain Admins و Enterprise Admins نیز تنظیمات Policy را دریافت می‌کنند. برای اجتناب از دریافت این تنظیمات توسط Domain Admins و Enterprise Admins، باید گزینه Apply Group Policy را برای آنها با Deny تنظیم کنید. در شکل ۸-۱۷ این وضعیت قابل مشاهده می‌باشد.



شکل ۸-۱۷



چنانچه قصد دارید افراد دیگری را نیز از این تنظیمات معاف کنید، می‌توانید آنها را به صورت تک تک اضافه نموده (با استفاده از دکمه Add) و یا یک گروه (به عنوان مثال Security Group) ایجاد نموده و این افراد را در آن قرار دهید. سپس گروه مورد نظر را به لیست ACL اضافه کنید. چون این گروه جزء Authenticated Users به شمار می‌رود، پس مجوزهای Read و Apply Group Policy به آنها داده شده است. اما لازم است برای معاف کردن آنها از دریافت تنظیمات Policy، گزینه Apply Group Policy را برای آنها با Deny تنظیم کنید.

جهت حذف کاربران یا گروه‌ها از لیست ACL نیز می‌توانید ابتدا آن کاربر و یا گروه را انتخاب نموده و سپس بر روی دکمه Remove کلیک کنید.

### ۳-۳-۸ استفاده از فیلترهای WMI به همراه Group policy

ویندوز سرور 2003، سرور 2008 و سرور 2008R2 نوعی از فیلترینگ به نام WMI را ارائه می‌کنند که در ویندوز 2000 وجود ندارد. فیلترهای WMI پرس و جوهای<sup>۱</sup> که به زبان WQL<sup>۲</sup> ایجاد شده‌اند را اجرا نموده و از آنها به منظور تعیین اینکه همه تنظیمات در یک GPO اعمال شوند استفاده می‌کنند. در این فیلترها امکان انتخاب تنظیمات Policy از میان سایر تنظیمات وجود ندارد.

برای استفاده از فیلترهای WMI ابتدا بر روی GPO کلیک نموده و سپس از تب Scope به قسمت WMI Filtering مراجعه کنید. با استفاده از drop-down لیستی که در این قسمت قرار دارد می‌توانید فیلترهای مورد نظر را انتخاب نموده و به GPO پیوند دهید.

امکان انتخاب از میان هزاران فیلتر WMI وجود دارد. به عنوان مثال فرض کنید که قصد دارید تنظیمات Policy شما تنها بر روی لپ‌تاپ‌ها اعمال شوند. برای انجام این کار ابتدا باید ساخت و مدل لپ‌تاپ‌ها را مشخص نموده و سپس Query شبیه زیر ایجاد کنید:

```
Root\CimV2; Select * from Win32_ComputerSystem where manufacturer = "Toshiba"
and Model = "Tecra 800" OR Model = "Tecra 810"
```

سایر شرایطی که برای WMI (در این مثال) می‌تواند تعیین شود، فضای دیسک و نسخه سیستم عامل است که در دو Query زیر آورده شده‌اند:

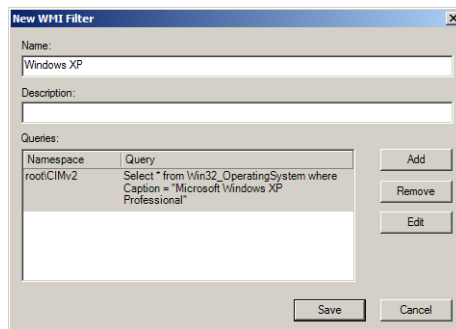
```
Root\CimV2; Select * from Win32_LogicalDisk where FreeSpace > 629145600 AND
FileSystem = " NTFS"
```

```
Root\CimV2; Select * from Win32_OperatingSystem where Caption = "Microsoft
Windows XP Professional"
```

قبل از اقدام به استفاده از فیلترهای WMI ابتدا باید آنها را ایجاد کنید. برای انجام این کار، در

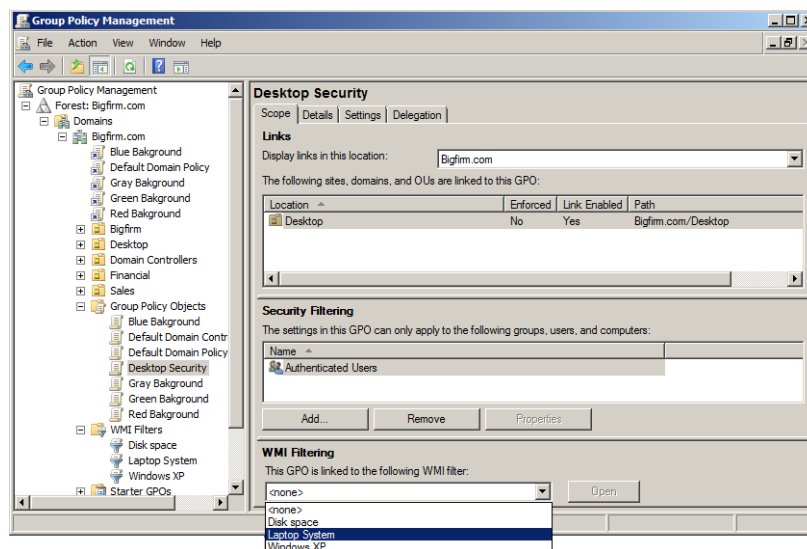
1. Query
2. WMI Query Language

پنجره GPMC بر روی گره WMI Filters کلیک‌راست نموده و گزینه New را انتخاب کنید. در پنجره “New WMI Filter” نام فیلتر را وارد نموده و سپس با کلیک بر روی Add، نوع فیلتر و Query آن را وارد کنید.



شکل ۸-۱۸

به عنوان مثال سه Query که در صفحه قبل آورده شده است را به صورت جداگانه وارد نموده و سه فیلتر ایجاد کنید. سپس با مراجعه به قسمت WMI Filtering زمانی‌که بر روی GPO کلیک می‌کنید، فیلترها را انتخاب نموده و به GPO پیوند دهید.



شکل ۸-۱۹

جهت کسب اطلاعات بیشتر در زمینه استفاده از فیلترهای WMI می‌توانید به آدرس

<http://technet.microsoft.com> مراجعه نموده و سپس عبارت WMI Filters را جستجو کنید.

### ۸-۳-۴ مثال Group policy: انتخاب Password های پیچیده

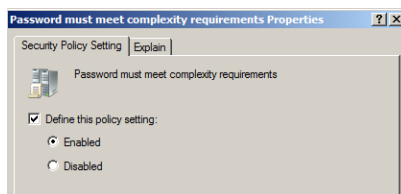
اکنون پس از توضیحات بالا، قصد داریم مثالی در رابطه با ایجاد Group Policy برای رمز عبور کاربران ارائه دهیم. اما قبل از آن لازم است فاکتورهایی را که در برنده شدن یک policy مؤثر است بیان کنیم:

- آزمودن Policy ها به ترتیب روبرو می‌باشد: GPO های Local، GPO های سایت، GPO های دامنه، GPO های OU، GPO های Child OU و به همین ترتیب.
  - برای هر گره در اکتیو دایرکتوری (سایت، دامنه، OU) ترتیب آزمودن Policy ها از پایین به بالای GUI می‌باشد.
  - در صورت مشاهده تضاد در Policy ها، باید آخرین GPO آزموده شده را مورد بررسی قرار دهید، مگر اینکه اجرای یک Policy به صورت اجباری باشد که در این صورت باید تناقض را نادیده گرفت.
  - قبل از اعمال کردن یک GPO، لیست ACL آن را بررسی کنید. اگر کاربران و کامپیوترهای این لیست دارای مجوز Read و Apply Group Policy نباشند، GPO قابل اعمال بر روی آنها نیست.
- اکنون به مثال رمز عبور باز می‌گردیم. فرض کنید قصد ایجاد یک سیاست رمز عبور بسیار امن برای کاربران دامنه دارید بطوری که GPO ایجاد شده برای این کار از دو شرایط زیر برخوردار باشد:
- وجود پیچیدگی در رمز عبور.
  - وجود حداقل ۱۲ کاراکتر در رمز عبور.

برای پیاده‌سازی این سیاست مراحل زیر را دنبال کنید:

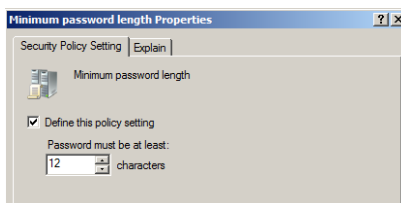
۱. کنسول Group Policy Management را اجرا کنید.
۲. بر روی گره دامنه (در اینجا Bigfirm.com) کلیک راست نموده و گزینه Create a GPO in this domain, and Link it here را انتخاب کنید.
۳. نام GPO را New Password Policy قرار داده و بر روی OK کلیک کنید.
۴. بر روی GPO ایجاد شده (New Password Policy) کلیک راست نموده و Edit را انتخاب کنید.
۵. در پنجره GPME به مسیر Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy بروید.
۶. بر روی سیاست Password must meet complexity requirements دابل کلیک نموده و آنرا در

وضعیت Enable (فعال) قرار دهید.



شکل ۸-۲۰

۷. سیاست Minimum password length را نیز فعال نموده و آنرا با عدد ۱۲ پیکربندی کنید.



شکل ۸-۲۱

۸. پنجره GPME را ببندید.

اکنون Policy ایجاد شده است ولی به سرعت بر روی حساب‌ها اعمال نخواهد شد. Domain Controller ها، بطور پیش‌فرض تغییرات ایجاد شده در Policy را هر ۱۵ ثانیه یکبار و در صورتی که نسبت به این تغییرات آگاه باشند اعمال خواهند نمود، بنابراین چنانچه در دامنه چندین DC وجود داشته باشد باید منظر بمانید تا اطلاعات Policy به سایر DC ها ارسال شود (واضح است که اگر تنها یک DC داشته باشید با مسئله انتظار روبرو نخواهید بود).

اکنون سعی کنید یک حساب کاربری با رمز عبور ۷ کاراکتری ایجاد کنید، احتمالاً منتظر دریافت پیغام خطایی خواهید بود اما هیچ پیغامی دریافت نخواهید کرد. سیستم رمز عبور ۷ کاراکتری شما را برخلاف GPO که ایجاد نمودید (New Password Policy) می‌پذیرد. حتی اگر از دستور gpupdate در خط فرمان نیز استفاده کنید (این دستور جهت آپدیت سریع Policy ها می‌باشد)، باز هم رمز عبور ۷ کاراکتری شما پذیرفته می‌شود. شاید بپرسید که علت این امر چیست؟ اگر بخاطر داشته باشید در قسمت‌های قبل گفتیم که GPO ها به ترتیب از پایین به بالا در GUI اجرا می‌شوند. زمانی که شما GPO مورد نظر (New Password Policy) را ایجاد می‌کنید، این GPO در زیر Default Domain Policy قرار می‌گیرد. Default Domain Policy بطور پیش‌فرض همراه اکتیو دایرکتوری قرار دارد بنابراین تا زمانی که در بالای GPO شما قرار داشته باشد، سیاست‌های موجود در آن نسبت به سیاست‌های شما

اولویت خواهد داشت. راه حل این مشکل، انتقال GPO های ایجاد شده به بالای Default Domain Policy می باشد. پس از انجام این انتقال اگر بار دیگر اقدام به ایجاد یک حساب کاربری با رمز عبور ۷ کاراکتری نمایید پیغامی ظاهر شده و به شما اعلام می کند که رمز عبوری با حداقل ۱۲ کاراکتر وارد کنید.

نکته ای که در این زمینه نباید فراموش کنید اولویت GPO ها در سطوح مختلف می باشد. به عنوان مثال فرض کنید که GPO بالا را ایجاد نموده اید تا به کاربران یک OU اعمال شوند. اما مشاهده می کنید که مشکلی در این روند وجود دارد. علت این است که این GPO به دامنه پیوند شده است و چنانچه GPO دیگری به OU مورد نظر شما پیوند شده باشد، سیاست های GPO دامنه را نادیده می گیرد.

#### ۴-۸ تنظیمات Group Policy

با استفاده از تنظیمات Group policy امکان انجام بسیاری از اقدامات پیکربندی برای سیستم ها وجود دارد. تعدادی از این اقدامات عبارتند از:

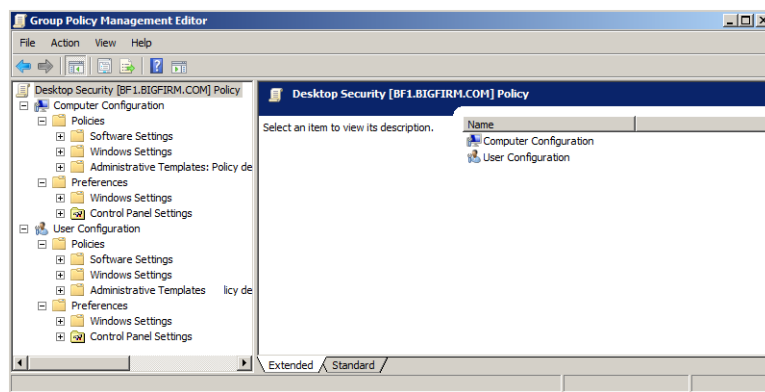
- استقرار نرم افزار: می توانید تمام فایل های مورد نیاز برای نصب یک نرم افزار را با یکدیگر به صورت یک بسته (Package) در آورده و سپس این بسته را در جایی از سرور قرار داده و نصب کنید. سپس با استفاده از Desktop, Group Policy کاربران را به آن اشاره دهید. مشاهده خواهید نمود با وجود اینکه این نرم افزار تنها بر روی سرور قرار دارد و همانجا نیز نصب شده، اما بر روی Desktop تمام کاربران نیز موجود است. زمانی که کاربر برای اولین بار سعی در اجرای این برنامه می کند، نرم افزار بطور خودکار شروع به نصب شدن نموده بدون اینکه کاربر در آن دخالتی داشته باشد.
- تنظیم حقوق کاربر: احتمالاً می دانید که کلمه "Right" اشاره به حقوق و یا توانایی کاربر برای انجام عملکردهای خاص می باشد. این عملکردها شامل Logon شدن به صورت Local و یا از طریق سرویس های Terminal (در ویندوز NT4) و مانند اینها می باشد. با استفاده از GPO ها می توان این حقوق را برای کاربران و یا ماشین ها به راحتی تعریف نموده و دیگر نگرانی در این زمینه وجود نخواهد داشت.
- محدود کردن برنامه هایی که کاربر می تواند اجرا نماید: با استفاده از GPO ها می توانید برنامه ها و قابلیت هایی که یک کاربر می تواند به آنها دسترسی داشته باشد را مشخص کنید. به عنوان مثال برنامه هایی مانند Word, Outlook, Internet Explorer.
- کنترل تنظیمات سیستم: یک روش آسان برای کنترل سهمیه بندی فضای دیسک، استفاده از GPO ها است. بسیاری از سیستم های ویندوز به آسانی توسط تنظیمات Policy ها کنترل می شوند.

- برای برخی از سیستم‌ها، استفاده از Policy ها تنها روش کنترل تنظیمات سیستم است.
- ♦ تنظیم اسکرین‌های Startup, Logoff, Logon و Shutdown: GPO ها اجازه می‌دهند که همه این چهار رویداد به صورت اسکرین ایجاد نموده و تعیین کنید که کدام اسکرین اجرا گردد.
  - ♦ ساده سازی و محدود کردن برنامه‌ها: با استفاده از GPO ها امکان حذف بسیاری از ویژگی‌ها از برنامه‌هایی مثل Internet Explorer, Windows Explorer و سایر برنامه‌ها وجود دارد.
  - ♦ محدود کردن Desktop: با استفاده از GPO ها می‌توانید همه یا بخشی از آیتم‌های منوی Start کاربران را حذف نموده، مانع از اضافه کردن پرینتر توسط آنها شده، و یا به آنها اجازه خروج از سیستم و تغییر پیکربندی Desktop را ندهید.
- اقدامات قابل انجام بسیاری توسط Policy ها وجود دارد، اما در اینجا تنها مقدمه‌ای برای شروع کار آورديم.

#### ۸-۴-۱ تنظیمات Computer/User Configuration

ویندوز سرور ۲۰۰۸، سرور ۲۰۰۸R2، ویندوز ویستا SP1 و بعد از آن با یک نگاه کاملاً جدید نسبت به تنظیمات Computer/User Configuration در GPME آمده‌اند. مایکروسافت در این سیستم عامل‌ها بیش از ۳۰۰۰ تنظیم GPO معرفی نموده است که به منظور انجام بهتر تنظیمات توسط مدیران Group Policy است.

در شکل ۸-۲۳ دو گره اصلی در واسط GPME قابل مشاهده هستند: User Configuration و Computer Configuration. هر دوی این گره‌ها دارای زیرگره‌های Policies و Preferences می‌باشند. زیرگره policies خود به سه زیرگره Software Settings, Windows Settings و Administrative Templates شکسته می‌شود. زیرگره Preferences نیز به زیرگره‌های Control Panel و Windows Settings تقسیم می‌شود.



شکل ۸-۲۲

تفاوت میان این گره‌های اصلی در این است که تنظیمات User Configuration بر روی حساب‌های کاربری و تنظیمات Computer Configuration بر روی حساب‌های کامپیوتر اعمال می‌شوند. به عنوان مثال تنظیمات Registry را در نظر بگیرید. تنظیمات Registry برای Computer Configuration در کلیدی به نام HKEY\_LOCAL\_MACHINE و تنظیمات User Configuration در کلیدی به نام HKEY\_CURRENT\_USER (HKCU) ذخیره می‌شوند. چنانچه دو GPO یکی در Computer Configuration و دیگری در User Configuration ایجاد نموده و تنظیمات یکسانی را در آن قرار دهید، تنظیمات Computer Configuration نسبت به تنظیمات User Configuration دارای اولویت خواهند بود.

بیشتر از ۵۰۰۰ تنظیم برای GPO در ویندوز سرور 2008 موجود است که در زمینه‌های مختلفی تدوین شده‌اند. در ادامه تعدادی از مفیدترین این سیاست‌ها را مورد بررسی قرار می‌دهیم.

### مشخص کردن اسکریپت‌ها با استفاده از Group Policy

اسکریپت‌ها کدهایی هستند که در زمان Logon یا Logoff شدن کاربران و همچنین در زمان Startup یا Shutdown شدن سیستم اجرا می‌شوند. این اسکریپت‌ها می‌توانند به هر زبان ActiveX Script مانند VBScript، JScript و یا در قالب فایل‌های Batch (\*.bat یا \*.cmd) می‌توانند مورد استفاده قرار گیرند. به عنوان مثال با استفاده از اسکریپت زیر که به زبان Visual Basic نوشته شده است می‌توانید یک پیغام در هنگام ورود کاربر به سرور ایجاد کنید:

```
MsgBox "Welcome to your server!", vbExclamation, "Logon Script"
```

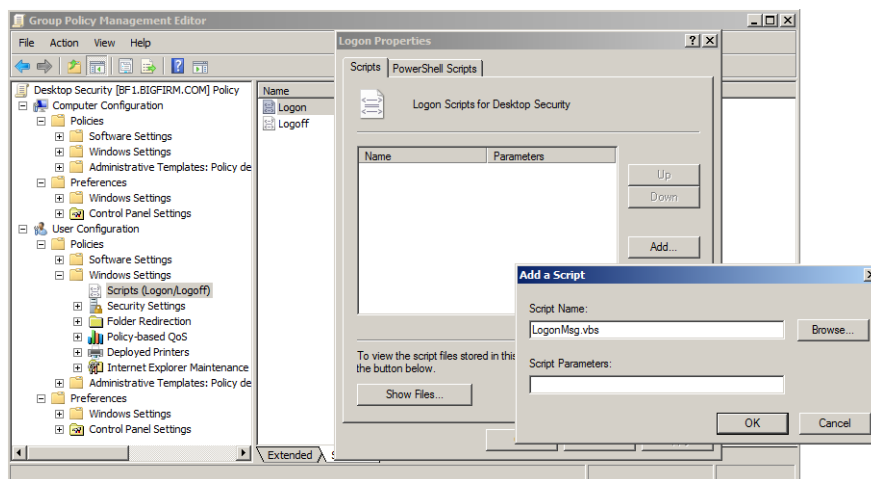
برای استفاده از اسکریپت‌ها ابتدا باید آنها بر روی سرور ایجاد شوند. بدین منظور می‌توانید مراحل زیر را دنبال کنید:

۱. کنسول GPMC را اجرا کنید.
۲. بر روی یکی از GPOها کلیک راست نموده و Edit را انتخاب کنید تا پنجره GPME اجرا شود.
۳. به مسیر User Configuration\Policies\Windows Settings\Scripts(Logon/Logoff) بروید.
۴. در پنل سمت راست بر روی Logon کلیک راست نموده و Properties را انتخاب کنید.
۵. در پنجره "Logon Properties" بر روی Show Files کلیک کنید.
۶. کد زیر را در برنامه Notepad وارد نموده و آنرا با نام و پسوند LogonMsg.vbs ذخیره کنید:

```
MsgBox "Welcome to your server!", vbExclamation, "Logon Script"
```

۷. فایل ذخیره شده را در محلی که با کلیک بر روی Show Files باز می‌شود کپی نموده و پنجره را ببندید.

۸. اکنون بر روی دکمه Add کلیک کنید.
۹. در پنجره "Add a Script" نام LogonMsg.vbs را وارد نموده و بر روی Ok کلیک کنید. اکنون زمانی که کاربران به سیستم وارد می‌شوند، پیغام "Welcome to your server!" در یک پنجره پیغام به آنها نشان داده می‌شود.
۱۰. ایجاد اسکریپت‌ها برای Startup، Shutdown و Logoff نیز به همین صورت می‌باشد.



شکل ۸-۲۳

برای دسترسی به محل ذخیره سازی فایل‌های اسکریپت می‌توانید به مسیر زیر مراجعه کنید:

C:\Windows\SYSTEM32\sysvol\Bigfirm.com\Policies\{GUID for example: 366FADC5-051F-4C97-965A-8E0F62958FB3}

در این مسیر دو پوشه با نام های Machine و User قابل مشاهده است که اسکریپت‌های Computer Configuration و User Configuration در آن ذخیره می‌شوند.

### Folder Redirection

یکی از موارد پر اهمیت در تنظیمات User Configuration در Group policy، امکان تعیین مکانی مشخص در شبکه جهت قرارگیری پوشه‌هایی همچون Desktop، Start Menu، AppData، Documents، Favorites و سایر پوشه‌های پر اهمیت برای کاربر است. این پوشه‌ها از این نظر مورد اهمیت کاربران هستند که محیط عملکرد آنها به این پوشه‌ها وابسته می‌باشد. پوشه AppData محل نگهداری اطلاعات مرتبط با برنامه‌ها مانند Internet Explorer، Desktop، محل نگهداری پوشه‌های مهم و میانبرهایی<sup>۱</sup> است

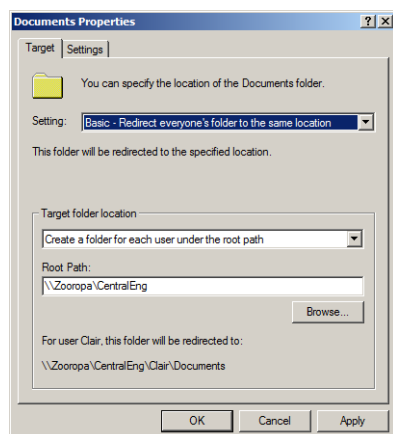
1. Shortcuts



که تنها با یک کلیک قابل دسترسی هستند، پوشه Start Menu شامل گروه‌هایی از برنامه‌ها و میانبرهای آنها است، My Documents محل پیش‌فرض ذخیره و بازیابی اطلاعات کاربران است و ... . دلایل زیادی برای استفاده از Folder Redirection (تغییر مسیر پوشه‌ها) وجود دارد. یکی از این دلایل، راحتی کاربرانی است که از چندین کامپیوتر در شبکه استفاده می‌کنند. زمانی که این کاربران دارای مکان مشخصی در شبکه جهت نگهداری برنامه‌ها و اطلاعات خود باشند، بدون نیاز به داشتن برنامه‌ها بر روی همه این ماشین‌ها می‌توانند به داده‌های خود دسترسی پیدا کنند.

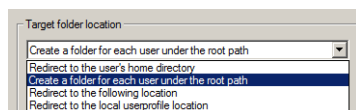
برای تنظیم مکانی از شبکه برای پوشه‌ها، به مسیر User Configuration\Policies\Windows Settings\Folder Redirection بروید. لیستی از پوشه‌های قابل انتقال نمایش داده می‌شود. برای تغییر مسیر هر یک می‌توانید بر روی آن پوشه کلیک‌راست نموده و Properties را انتخاب کنید. سپس با تعیین مسیری جهت قرار گیری پوشه، مسیر آنرا برای کاربران در شبکه تغییر دهید. به عنوان مثال برای تغییر مسیر پوشه Documents در Group Policy، مراحل زیر را دنبال کنید:

۱. به مسیر User Configuration\Policies\Windows Settings\Folder Redirection\Documents رفته و بر روی پوشه Documents کلیک‌راست کنید.
۲. پس از انتخاب گزینه Properties، مشاهده می‌کنید که این تنظیمات بطور پیش‌فرض بر روی Not Configured قرار دارد. از داخل لیست Drop-Down، گزینه Basic را انتخاب کنید.
۳. فیلدهایی جهت تعیین محل قرار گیری پوشه و ریشه آن (سرور شبکه) ظاهر می‌شود. از لیست Target folder location گزینه Create a folder for each user را انتخاب کنید.
۴. پوشه در آن قرار می‌گیرد (در اینجا سروری با نام Zooropa) را وارد کنید.
۵. با استفاده از دکمه Browse می‌توانید هر مکان از سرور فعلی یا سروری در شبکه را جستجو نموده و انتخاب کنید.



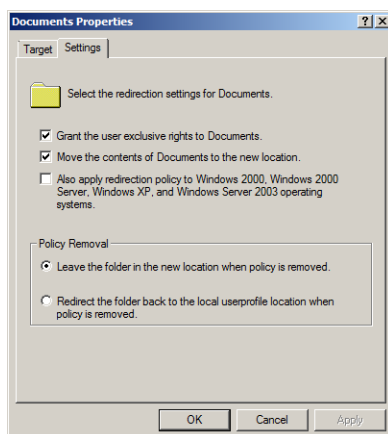
شکل ۸-۲۴

۵. دقت داشته باشید که در قسمت Target folder location گزینه‌های دیگری نیز وجود دارد. می‌توانید با توجه به مکانی که جهت تغییر مسیر در نظر گرفته‌اید، یکی از این گزینه‌ها را انتخاب کنید.



شکل ۸-۲۵

علاوه بر تب Target در این پنجره، تب دیگری نیز با نام Settings وجود دارد. در این تب تنظیماتی پیرامون انتقال فایل به مکان جدید وجود دارد. می‌توانید این تنظیمات را با فعال/غیر فعال کردن هر گزینه تغییر دهید.



شکل ۸-۲۶

## Security Settings

Security Settings به همراه Administrative Templates بخش قابل توجهی از Group policy را تشکیل می‌دهند. تنظیمات پیش‌فرض در این دو گره به منظور راحتی کار در نظر گرفته شده‌اند. افزایش امنیت به معنی افزایش محدودیت‌ها بوده و دارای رابطه‌ای معکوس با راحتی می‌باشد. تنظیمات امنیتی در چند گروه دسته‌بندی شده و از مسیر Computer Configuration\Policies\Windows Settings\Security Settings قابل دسترسی می‌باشند. عمده‌ترین دسته از این تنظیمات عبارتند از:

- ♦ **Account Policies:** این سیاست‌ها محدودیت‌های رمزعبور، سیاست‌های قفل شدن سیستم و سیاست‌های Kerberos را مشخص می‌کنند.
- ♦ **Local Policies:** این سیاست‌ها مربوط به حقوق کاربران و حسابرسی آنها می‌باشد.

- ♦ **Event Log**: متمرکز نمودن پیکربندی‌ها برای ثبت وقایع سیستم.
- ♦ **Restricted Groups**: وادار نمودن و کنترل کردن کاربران گروه‌ها برای گروه‌های خاصی مانند Administrators group.
- ♦ **System Services**: استانداردسازی پیکربندی سیستم و جلوگیری از ایجاد تغییر در آن.
- ♦ **Registry**: ایجاد قالب‌های امنیتی برای Key‌های رجیستری به منظور کنترل Key‌هایی که می‌توانند تغییر کنند و همچنین کنترل دسترسی به بخش‌های رجیستری.
- ♦ **File System**: ایجاد قالب‌های امنیتی برای مجوزهای فایل‌ها و پوشه‌ها به منظور اطمینان از اینکه فایل‌ها و مسیرها دارای مجوزهای مورد نظر می‌باشند.
- ♦ **Public Key Policies**: مدیریت تنظیمات برای سازمان‌ها با استفاده از زیرساخت‌های کلید عمومی<sup>۱</sup>.
- ♦ **Software Restrictions Policies**: قرار دادن محدودیت برای اجرای برنامه‌ها بر روی سیستم. این یکی از ویژگی‌های جدید است که مانع از اجرای ویروس‌ها و نرم افزارهای مخرب بر روی سیستم می‌شود.

### کار با Template‌ها

Template‌ها قالب‌های امنیتی هستند که توسط مدیران ایجاد شده و می‌توان تنظیمات دلخواه را برای همیشه در آن جای داد. برای آشنایی با طرز کار Template‌ها اجازه دهید مثالی ارائه دهیم. قصد داریم Template‌ای برای انجام سه اقدام زیر ایجاد کنیم:

- ♦ حصول اطمینان از اینکه فردی در گروه محلی Power users قرار ندارد.
- ♦ تنظیم مجوز NTFS برای مسیر C:\SECRET که تنها توسط گروه محلی Administrators قابل دسترسی است.
- ♦ خاموش کردن سرویس IIS<sup>۲</sup> که به نظر می‌رسد بر روی هر سیستم عامل میکروسافت خود را نصب نموده و برای Web server ایجاد مزاحمت می‌کند.

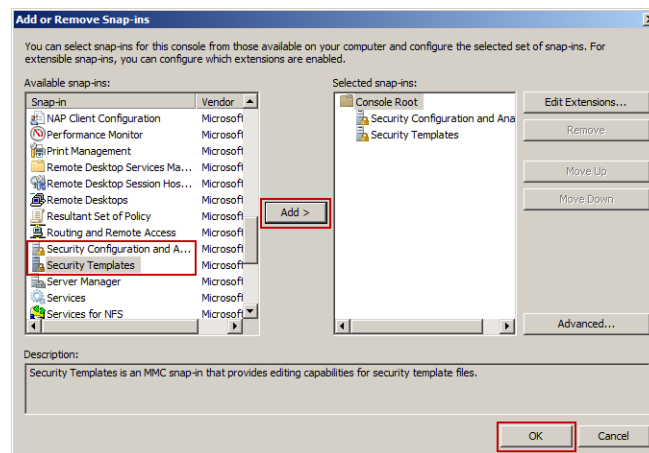
در ابتدا به تعدادی ابزار نیازمندید. یکی از این ابزارها کنسول MMC<sup>۳</sup> می‌باشد. در این کنسول به دو Snap-in با نام‌های Security Templates و Security Configuration and Analysis نیاز است. این ابزار را به صورت زیر راه اندازی نمایید:

۱. در قسمت Search از منوی Start، عبارت mmc /a را وارد نموده و Enter را فشار دهید تا کنسول MMC اجرا گردد.

---

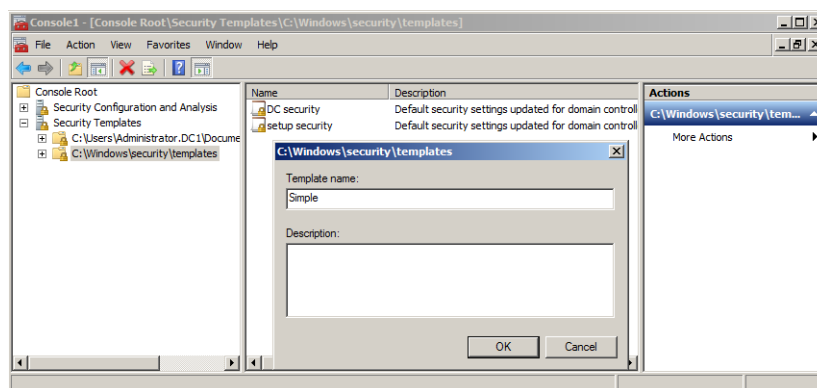
1. Public Key infrastructures  
2. Internet Information Service  
3. Microsoft Management Console

۲. از منوی File گزینه Add/Remove Snap-in را انتخاب کنید.
۳. در صفحه "Add or Remove Snap-ins" گزینه‌های Security Configuration and Analysis و Security Templates را انتخاب نموده و بر روی Add کلیک کنید تا به فهرست Selected snap-ins اضافه شوند. در نهایت بر روی Ok کلیک کنید.



شکل ۸-۲۷

۴. اکنون به منظور اضافه کردن یک مسیر برای Template (در کنسول MMC) بر روی گره Security Templates کلیک راست نموده و گزینه New Template Search Path را انتخاب کنید. مسیری که باید اضافه شود به صورت C:\Windows\Security\Templates خواهد بود. این مسیر شامل Template از پیش ساخته‌ای به نام DC Security می‌باشد، اما در اینجا قصد داریم یک Template را از ابتدا ایجاد کنیم بنابراین بر روی مسیری که اضافه نمودید کلیک راست نموده و New Template را انتخاب کنید. سپس نام آنرا (در اینجا Simple) را وارد نمایید.



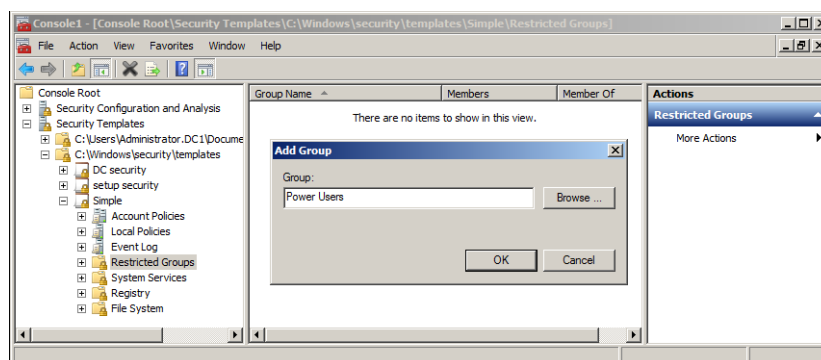
شکل ۸-۲۸

هر Security Templates شامل تعدادی زیرمجموعه است که عبارتند از:

- ♦ Account Policies: برای تنظیم Passwordها، قفل کردن حسابها و سیاستهای Kerberos استفاده می‌شود.
- ♦ Local Policies: جهت کنترل تنظیمات حسابرسی، حقوق کاربر و تنظیمات امنیتی می‌باشد.
- ♦ Event Log settings: پارامترهای مربوط به نحوه ذخیره‌سازی وقایع سیستم را ذخیره می‌نماید.
- ♦ Restricted Groups: اعضای وارد شده و خارج شده از یک گروه Local را کنترل می‌نماید.
- ♦ System Services: روشن و خاموش کردن سرویس‌ها و کنترل افرادی که مجوز انجام این کار را دارند.
- ♦ Registry security: تنظیم و کنترل مجوزها برای مشاهده و تغییر Keyهای رجیستری.
- ♦ File System: کنترل مجوزهای NTFS برای فایل‌ها و پوشه‌ها.

اکنون به سراغ گروه Power Users (اقدام اول) رفته و آنرا تشریح می‌کنیم:

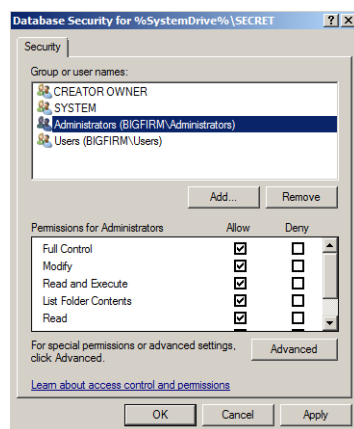
۱. Simple (Template ایجاد شده) را باز کنید.
۲. از زیرگره‌های آن بروی Restricted Groups کلیک‌راست نموده Add Group را انتخاب کنید.
۳. نام Power Users را وارد نموده و یا با استفاده از دکمه Browse آنرا جستجو کنید (به شرطی که از قبل این گروه را ایجاد کرده باشید).



شکل ۸-۲۹

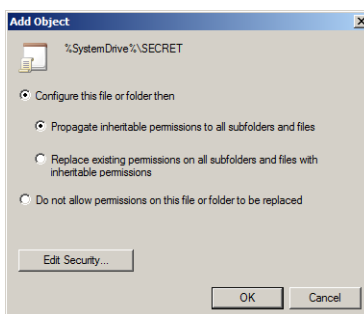
بطور پیش‌فرض، اگر گروهی در Security Template قرار گیرد اعضای آن از گروه حذف می‌شوند. بنابراین چنانچه با پنجره‌ای تحت این موضوع مواجه شدید، بروی Ok کلیک کنید. چنانچه تمایل دارید افرادی را در این گروه قرار دهید می‌توانید بروی گروه کلیک‌راست نموده و با ورود به بخش Properties، افراد مورد نظر را به آن اضافه کنید.

- اکنون قصد داریم برای مسیر C:\SECRET مجوز NTFS تنظیم نموده (اقدام دوم) بطوری که تنها توسط گروه محلی Administrators قابل دسترسی باشد. برای انجام این کار مراحل زیر را دنبال کنید:
۱. به پنل سمت چپ باز گردید. بر روی File System کلیک راست نموده و Add Files را انتخاب کنید.
  ۲. در پنجره "Add a File or Folder" مسیر مورد نظر (C:\SECRET) را وارد نموده و یا با استفاده از دکمه Browse آنرا تعیین کنید.
  ۳. پس از کلیک بر روی Ok، پنجره مجوز NTFS ظاهر می‌شود. مجوزهای داده شده به تمام گروه‌ها و کاربران را به غیر از گروه Administrators حذف نموده و مجوز Full Control را برای گروه Administrators فعال کنید.



شکل ۸-۳۰

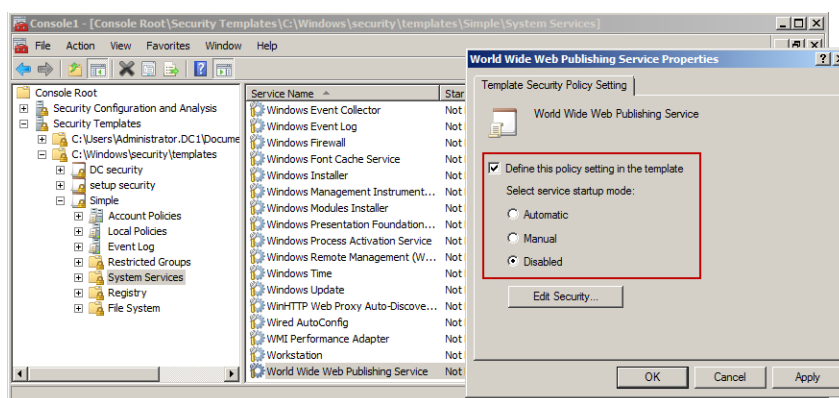
۴. پنجره "Add Object" ظاهر شده و از شما می‌پرسد که این مجوز تنها بر روی همین پوشه اعمال شود یا زیر پوشه‌های آنرا نیز شامل شود. با توجه به نظر خود آنرا تنظیم نموده و بر روی Ok کلیک کنید.



شکل ۸-۳۱

سرانجام نوبت به خاموش نمودن IIS (اقدام سوم) می‌رسد.

۱. بروی System Services کلیک کنید.
۲. در پنل سمت راست بروی World Wide Web Publishing Services کلیک راست نموده و Properties را انتخاب کنید.
۳. گزینه Define This Policy Setting in the Template را فعال نموده و Disabled را انتخاب کنید.
۴. بروی Ok کلیک کنید.



شکل ۸-۳۲

اکنون می‌توانید Template ایجاد شده را ذخیره کنید. برای انجام این کار بروی Simple کلیک راست نموده و Save را انتخاب کنید. اکنون شما یک فایل با نام Simple.inf در مسیر \Windows\Security\Templates در اختیار دارید.

### ایجاد یک Security Database

پس از ایجاد Template، برای اینکه ببینید چگونه این Template سیستم را مورد تغییر قرار می‌دهد و یا برای آگاهی از اینکه چگونه تنظیمات آن با استفاده از Snap-in های MMC اعمال می‌شوند، باید یک Security Database ایجاد کنید. در واقع باید Template را از فرم ASCII به فرم Binary که Database نامیده می‌شود کامپایل (ترجمه) کنید. این کار با استفاده از Snap-in اول یعنی Security Configuration and Analysis قابل انجام است.

۱. در کنسول MMC بروی Security Configuration and Analysis کلیک راست نموده و Open Database را انتخاب کنید.
۲. در پنجره "Open Database" باید یک Database جدید ایجاد کنید اما آپشنی برای این کار وجود

- ندارد. بنابراین می‌توانید در قسمت File name نام Database جدید را وارد کنید. در این مثال نام Simple را وارد نموده و Enter را فشار دهید.
۳. در پنجره باز شده از شما خواسته می‌شود که فایلی با پسوند .inf را باز کنید. می‌توانید از مسیر C:\Windows\Security\Templates فایل Simple.inf را انتخاب نموده و بر روی Open کلیک کنید.
۴. بر روی Security Configuration and Analysis کلیک‌راست کنید. دو گزینه قابل مشاهده است: Analyze Computer Now و Analyze Computer Now. در کامپیوتر تغییری ایجاد نمی‌کند و فقط نشان می‌دهد که سیستم شما چگونه تغییر خواهد کرد. با اجرای این گزینه یک فایل log در مسیر Documents\Security\Logs ایجاد می‌شود.
۵. گزینه Analyze Computer Now را انتخاب نموده تا سیستم شما با تنظیمات Database سنجیده شود. چنانچه تصمیم به اعمال این تنظیمات گرفتید، گزینه Configure Computer Now را انتخاب نموده (از منوی کلیک‌راست) تا تغییرات بر روی سیستم شما اعمال گردد.

این عمل عالی به نظر می‌رسد. اما اگر بخواهید آنرا بر روی ده‌ها کامپیوتر اعمال کنید چطور؟ راه حل ساده است. می‌توانید با استفاده از ابزاری به نام `secedit.exe` در خط فرمان ابتدا Template را به یک Database تبدیل نموده و سپس Database را اعمال کنید. برای خواندن یک Template، اعمال نمودن آن و سپس ایجاد Database از قالب دستوری زیر استفاده کنید:

```
Secedit /configure /cfg templatefilename /db databasefilename/  
overwrite /log logfilename
```

برای اعمال این دستور بر روی ایستگاه‌های کاری مختلف می‌توانید آنرا با استفاده از Logon Scripts یا فایل‌های Batch تعریف نموده تا در هر بار ورود به سیستم مجدداً اعمال گردد.

#### *استفاده از Group policy های مبتنی بر دامنه برای اعمال Template ها*

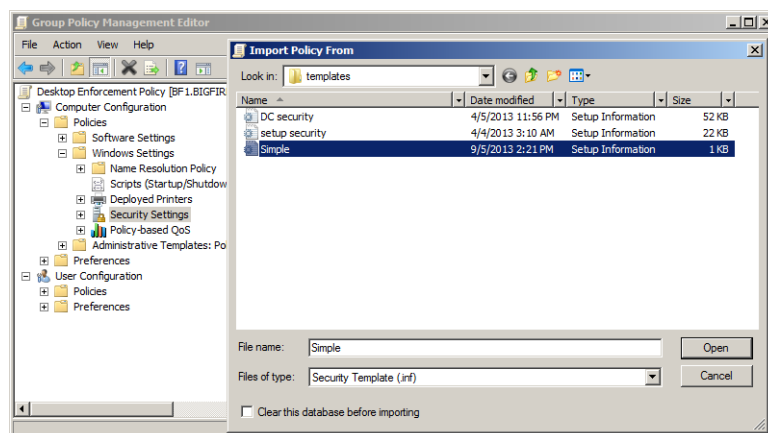
اگرچه استفاده از Logon Script برای اعمال Template ها مناسب است اما باید توجه داشته باشید که این اسکریپت‌ها تنها در زمان وارد شدن کاربر قادر به اجرا هستند و در بقیه موارد نمی‌توان آنها را اجرا نمود. برای حل این مشکل می‌توان از GPO های مبتنی بر دامنه استفاده نمود. GPO های مبتنی بر دامنه در طول روز قابل اعمال هستند و کنترل کردن آنها نیز نسبت به فایل‌های Batch ساده‌تر است.

#### *Import کردن Security Templates*

Template ایجاد شده در قسمت قبل (Simple.inf) را در نظر بگیرید. قصد داریم آنرا با استفاده از GPO بر روی سیستم مستقر کنیم. مراحل زیر را برای Import کردن Template ها دنبال کنید:



۱. کنسول GPMC را اجرا کنید.
۲. OU ای که شامل کامپیوترهای مورد نظر جهت اعمال تنظیمات امنیتی است را انتخاب کنید (به عنوان مثال Desktop).
۳. بر روی OU کلیک راست نموده و گزینه Create a GPO in this domain, and Link it here را انتخاب کنید.
۴. نام GPO را وارد نمایید. در اینجا ما از نام Desktop Enforcement Policy استفاده کرده ایم.
۵. بر روی GPO ایجاد شده کلیک راست نموده و Edit را انتخاب کنید.
۶. در پنجره GPME به مسیر Computer Configuration\Policies\Windows Settings Security Settings را انتخاب کنید.
۷. بر روی Security Settings کلیک راست نموده و گزینه Import Policy را انتخاب کنید.
۸. Template مورد نظر (Simple.inf) را انتخاب نموده و بر روی Open کلیک کنید.



شکل ۸-۳۳

۹. به گره Security Settings و سپس Restricted Groups بروید و مطمئن شوید که سیاست Power Users در آن قرار دارد.

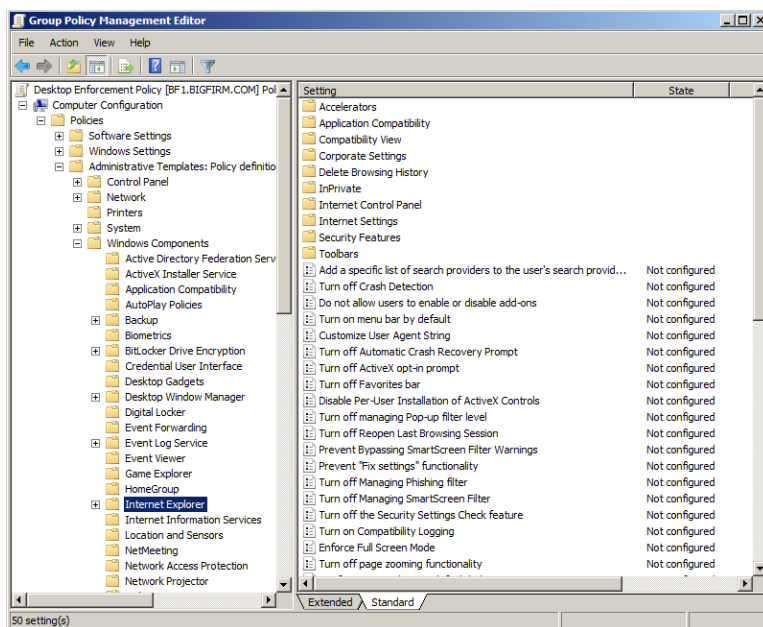
شاید این سؤال برایتان پیش آمده باشد که در حال حاضر باید چه اقدامی انجام دهید؟ پاسخ انتظار به مدت ۹۰ دقیقه است. نیاز به انجام کار خاصی نیست فقط اجازه دهید تا سیاست‌ها Refresh شده و تنظیمات شما بر روی تمام کاربران موجود در OU Desktop اعمال شوند (البته فراموش نشود که با استفاده از دستور gpupdate می‌توانید عملیات Refresh شدن را در هر زمان انجام دهید).

**(ADMX /ADML ) Administrative Templates**

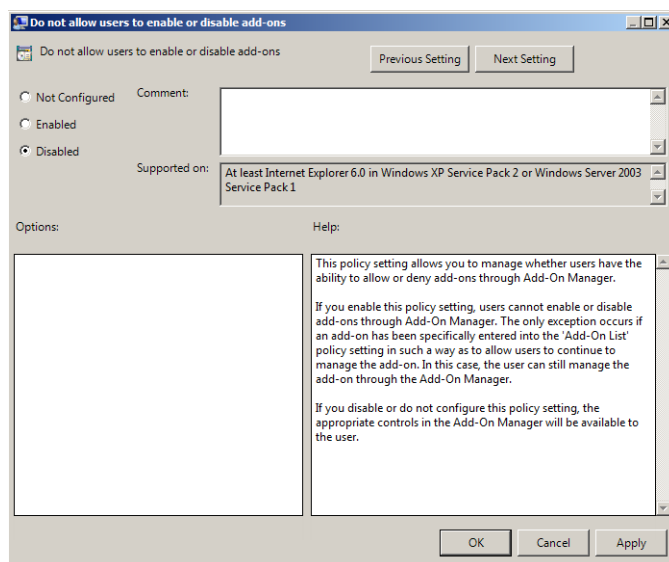
Administrative Templates تنظیماتی هستند که بسیاری از جنبه‌های محیط عملکرد کاربر و پیکربندی ماشین‌ها را مشخص می‌کنند. از معروف‌ترین این تنظیمات می‌توان محدود کردن Desktop کاربران برای اجرای محدوده‌ای از برنامه‌ها می‌باشد. این تنظیمات برای کاربران در مسیر HKEY\_CURRENT\_USER\Software\Policies و برای ماشین‌ها در مسیر HKEY\_LOCAL\_MACHINE\Software\Policies نوشته می‌شوند. در ادامه تعدادی از عملکردهای این Template‌ها را ارائه می‌دهیم.

**محدود کردن Internet Explorer**

به نظر می‌رسد برای هر امکان در Internet Explorer یک Policy به منظور غیر فعال کردن آن امکان در نظر گرفته شده است. برای دسترسی به این Policy‌ها می‌توانید به مسیر Computer Configuration/Policies/Administrative Templates/ Windows Components/Internet Explorer مراجعه نموده و سپس از میان Policy‌های موجود، آنهایی را که در نظر دارید انتخاب نموده و با کلیک راست بر روی آن و انتخاب گزینه Edit، امکان استفاده از آنرا توسط کاربران فعال/غیر فعال کنید. در شکل ۸-۳۵ Policy‌های مربوط به Internet Explorer و در شکل ۸-۳۶ نمونه‌ای از این Policy‌ها که غیر فعال شده نشان داده شده است.



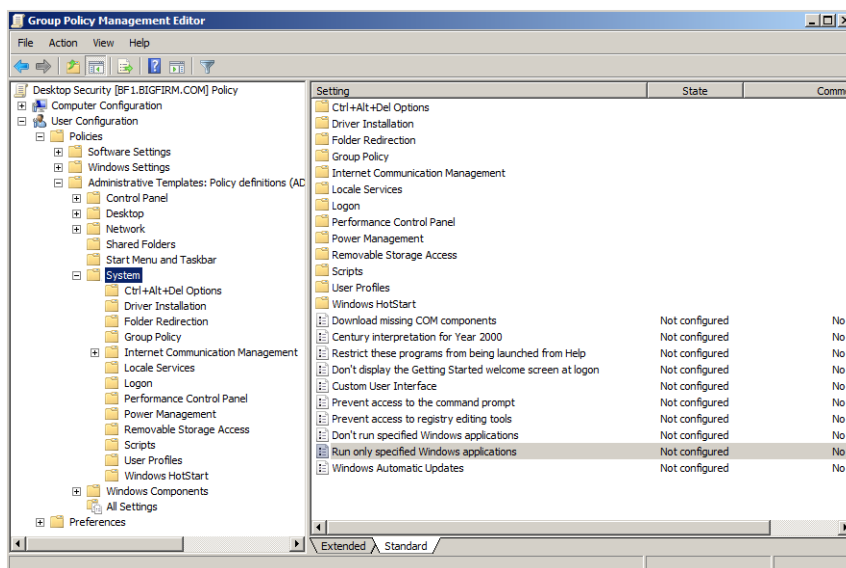
شکل ۸-۳۶



شکل ۸-۳۵

### ممنوعیت کاربران از نصب و اجرای نرم افزارهای غیر مجاز

برای جلوگیری از انجام نصب نرم افزارها توسط کاربران باید Policy به نام "Prevent Removable Media Source for Any Install" در مسیر User Configuration/.../ Windows Components/Windows Installer قرار دارد را فعال کنید. با فعال سازی این Policy کاربران قادر نخواهند بود با استفاده از رسانه هایی مانند CD-ROM یا Floppy ها فرایند نصب نرم افزارها را راه اندازی کنند. همچنین باید Policy دیگری به نام "Add a Program from CD-ROM or floppy disk" را نیز در مسیر User Configuration/.../Control Panel/Add or Remove Programs فعال کنید. در گره Control Panel تعدادی از آپشن ها به منظور غیرفعال کردن و یا حذف قسمت هایی از آپلت های Add/Remove Programs در نظر گرفته شده است. دقت داشته باشید که تنها استفاده از این سیاست ها جهت جلوگیری از نصب برنامه ها توسط کاربران کافی نیست زیرا امکان انجام آن با استفاده از خط فرمان نیز امکان پذیر است. بنابراین دسترسی به Command Line نیز باید غیر فعال گردد. این کار با فعال نمودن سیاست "Prevent access to the command prompt" امکان پذیر می باشد. البته توجه داشته باشید که Policy دیگری برای اجرای برنامه ها وجود دارد که نام آن "Run only specified windows application" می باشد. در هنگام استفاده از این Policy باید مراقب باشید زیرا فعال سازی آن باعث اجرای تنها برنامه های مشخصی خواهد شد. می توانید لیست این برنامه های قابل اجرا را در این سیاست مشخص کنید. در شکل ۸-۳۶ محل قرارگیری این Policy ها نشان داده شده است.



شکل ۸-۳۶

به عنوان آخرین نکته در رابطه با اجرای برنامه‌ها اشاره می‌کنیم که کاربران می‌توانند برنامه‌ها را از طریق Task Manager نیز اجرا کنند، بنابراین لازم است که سیاست Ctrl+Alt+Delete را نیز غیرفعال نمایید.

### استفاده از Group Policy به منظور تنظیم سیاست Password و Account Lockout

شاید یکی از مهمترین کاربردهای Group policy، استفاده از آن به منظور تعیین سیاست‌های رمز عبور برای کاربران می‌باشد. به همین دلیل در این قسمت سیاست‌های مرتبط با رمز عبور را مورد بررسی قرار می‌دهیم. قبل از شروع کار لازم است بار دیگر محل قرارگیری این سیاست‌ها را یادآور شویم. سیاست‌های مرتبط با رمز عبور و حساب‌های کاربران در مسیر Computer Configuration/ Policies/Windows Settings/Security Settings قرار دارند. اکنون به بررسی هریک از آپشن‌های موجود در این مسیر می‌پردازیم.

#### سیاست‌های Password

این سیاست‌ها مرتبط با رمز عبور کاربران هستند:

- **Enforce password history**: فعال‌سازی این گزینه، تعداد دفعاتی را که باید رمزهای عبور متمایز برای یک حساب کاربری وارد شده تا بتوان مجدداً یک رمز عبور را مورد استفاده قرار داد مشخص می‌نماید.

- ♦ **Maximum password age**: حداکثر مدت زمانی را که یک رمز عبور قبل از اینکه کاربر بتواند آنرا تغییر دهد مشخص می‌نماید.
- ♦ **Minimum password age**: مدت زمانی است که یک رمز عبور باید استفاده شود تا کاربر بتواند آنرا مجدداً تغییر دهد.
- ♦ **Minimum password length**: حداقل تعداد کاراکترهای استفاده شده در رمز عبور را مشخص می‌نماید. تعداد ۷ یا ۸ کاراکتر برای این آپشن مناسب می‌باشد. تنظیم این گزینه مانع از انتخاب رمز عبور خالی می‌شود.
- ♦ **Passwords must meet complexity requirements**: این آپشن تعیین می‌کند که رمز عبور باید دارای پیچیدگی باشد. پیچیدگی رمز عبور شامل سه مورد می‌باشد:
  - حداقل دارای ۶ کاراکتر باشد.
  - نباید شامل نام کاربری یا قسمتی از آن باشد.
  - باید شامل سه دسته از ۶ نوع کاراکتر روبرو باشد: حروف بزرگ (A-Z)، حروف کوچک (a-z)، اعداد (0-9)، کاراکترهای ویژه (@, %, &, #)
- ♦ **Store passwords using reversible encryption**: این آپشن باعث می‌شود که اکتیو دایرکتوری رمز عبور را با استفاده از روش رمزگذاری بازگشتی ذخیره نماید. فعال‌سازی این گزینه برای دسترسی‌های Remote و سرویس‌های Internet Authentication Services مناسب است.

#### سیاست‌های Account Lockout

- سیاست‌های مرتبط با قفل شدن حساب کاربری به دلیل وارد نمودن تعداد مشخصی از رمزهای عبور نادرست در این قسمت قرار دارند:
- ♦ **Account lockout duration**: مدت زمانی است که کاربر پس از قفل شدن یک حساب کاربری باید منتظر مانده تا بتواند مجدداً رمز عبور خود را وارد کند. اگر این آپشن فعال شود ولی فیلد minutes با صفر تنظیم گردد، حساب کاربری باید توسط مدیر از حالت Lokout خارج گردد. بنابراین منتظر ماندن برای مدت مشخص بی‌فایده خواهد بود.
  - ♦ **Account lockout threshold**: این آپشن تعداد دفعات مجاز تا لحظه وارد نمودن رمز عبور صحیح جهت ورود به سیستم را قبل از قفل شدن آن مشخص می‌نماید. چنانچه این گزینه با صفر تنظیم گردد حساب کاربری هرگز قفل نخواهد شد.
  - ♦ **Reset account lockout counter after**: این گزینه تعیین می‌کند که قبل از آخرین تلاش برای وارد نمودن رمز عبور صحیح (در صورتی که رمزهای وارد شده در دفعات قبلی اشتباه باشند) چه

مدت باید منتظر مانده تا شمارنده مجدداً به صفر بازگردد. به عنوان مثال اگر Reset account lockout counter را بر روی ۲ دقیقه و Account lockout threshold را بر روی ۳ بار تنظیم نموده باشید، اگر دوبار رمز عبور را اشتباه وارد کنید، باید دو دقیقه منتظر مانده تا بتوانید مجدداً از سه فرصت خود استفاده کنید.

### ۸-۴-۲ Group Policy Preferences

Group Policy Preferences (GPP) یکی از جنبه‌های تاثیرگذار در ویندوز سرور 2008 است که بیش از ۳۰۰۰ تنظیم Policy به GPOها اضافه می‌نماید. در ادامه با این تنظیمات بیشتر آشنا خواهید شد.

#### تنظیمات GPP

تنظیمات GPP کمی متفاوت‌تر از سایر تنظیمات Group Policy هستند. در درجه اول به این دلیل که آنها در هر دو محیط Computer Configuration و User Configuration از GPO قرار دارند. این امکان قدرت و انعطاف‌پذیری بیشتری به منظور انجام تنظیمات بر روی Desktopها و کاربران در اختیار شما قرار می‌دهد. در جدول ۸-۱ لیستی از تنظیمات GPP آورده شده است.

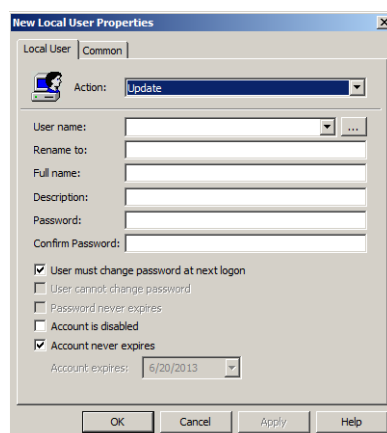
جدول ۸-۱ تنظیمات GPP

قابل دسترسی در		تنظیمات
User Configuration	Computer Configuration	Group Policy Preferences
Yes	No	Applications
Yes	No	Drive Maps
Yes	Yes	Environment
Yes	Yes	Files
Yes	Yes	Folders
Yes	Yes	Ini Files
No	Yes	Network Shares
Yes	Yes	Registry
Yes	Yes	Shortcuts
Yes	Yes	Data Sources
Yes	Yes	Devices
Yes	Yes	Folder Options
Yes	No	Internet Settings
Yes	Yes	Local Users and Groups
Yes	Yes	Network Options
Yes	Yes	Power Options

Yes	Yes	Printers
Yes	No	Regional Options
Yes	Yes	Scheduled Tasks
No	Yes	Services
Yes	No	Start Menu

بیشتر تنظیمات موجود در جدول ۸-۱ واضح بوده و نیاز به توضیح ندارند. با این وجود نحوه کار با تعدادی از این تنظیمات را که ممکن است مورد استفاده قرار گیرند شرح می‌دهیم.

همواره امنیت یکی از مسائل مهم در ذهن مدیران IT بوده است اما همیشه زمان کافی برای اعمال آن وجود ندارد. به عنوان مثال بازنشانی رمز عبور برای مدیر Local (Local Administrator) در هر کامپیوتر رومیزی سازمان را در نظر بگیرید. آخرین باری که این رمز عبورها را تغییر داده‌اید چه زمانی بوده است؟ زمان نصب؟ دو سال پیش؟ شاید هر کدام از شما پاسخ‌هایی در این زمینه داشته باشید، اما استفاده از GPP شما را قادر می‌سازد تا این کار را هر زمان که تمایل داشته باشید انجام دهید. برای انجام این کار لازم است یک GPO ایجاد نموده و آنرا به یک OU که شامل تمام کامپیوترهای رومیزی سازمان شما می‌باشد پیوند دهید. زمانی که GPME را برای این GPO اجرا می‌کنید، به مسیر Computer Configuration\Preferences\Control Panel\Local Users and Groups رفته و بر روی گروه Local Users and Groups کلیک راست کنید. گزینه «New Local User» را انتخاب نموده تا پنجره «New Local User Properties» اجرا گردد.



شکل ۸-۳۷

در قسمت User name، نام کاربری که قصد کنترل کردن آنرا دارید (در اینجا Administrator) وارد

کنید. سپس در فیلدهای Password و Confirm Password نیز رمز عبور جدیدی جهت بازنشانی وارد نمایید. اکنون رمز عبور کاربر Administrator در هر کامپیوتر که به دامنه و شبکه متصل است پس از مدت ۲ ساعت بازنشانی خواهد شد.

مشاهده نمودید که استفاده از GPP ها بسیار ساده است. برای درک چگونگی عملکرد سایر GPP ها، اعمالی که توسط آنها قابل انجام است را شرح می‌دهیم:

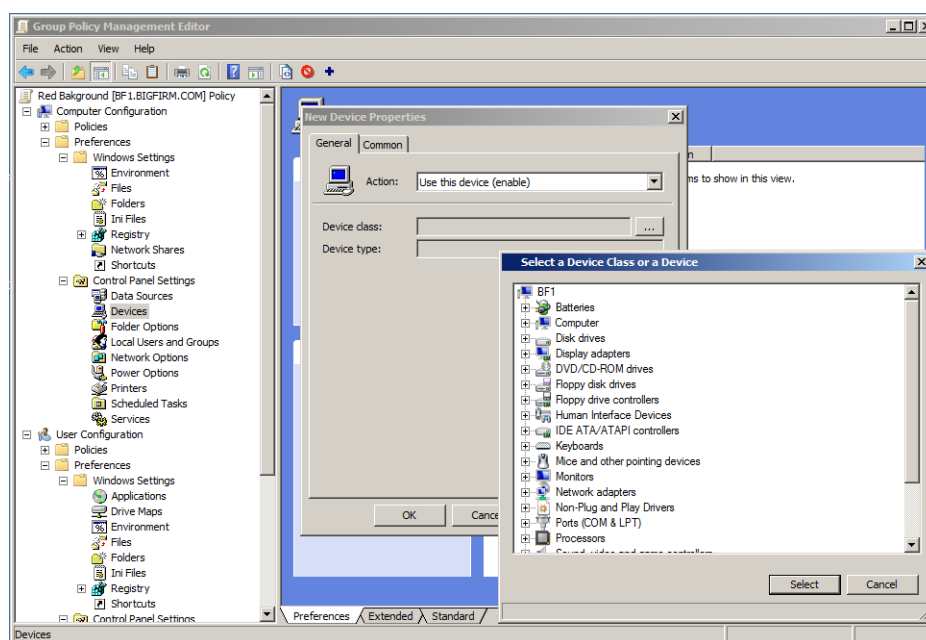
- ♦ **Applications:** انجام اقداماتی مانند فعال‌سازی غلط یاب املایی (spell checker) برای Microsoft Word، پیکربندی قابلیت بایگانی خودکار برنامه Outlook، پیکربندی امضاء "company-approved" and consistent" برای ایمیل‌های Outlook.
- ♦ **Drive maps:** جایگزینی تمام نگاشت‌های درایو تعریف شده در logon script با تنظیمات Group Policy preferences
- ♦ **Environment:** ایجاد متغیرهای محیطی جهت استفاده با سایر تنظیمات Group Policy preferences (به عنوان مثال تعریف فضای مشخصی از RAM یا سرعت مشخصی از CPU به منظور استفاده یک برنامه)
- ♦ **Files:** استقرار فایل‌های پیکربندی برنامه‌ها روی کامپیوترهای رومیزی.
- ♦ **Folders:** ایجاد پوشه‌ها به منظور استفاده سایر برنامه‌های کاربردی، و یا حذف محتویات از پوشه‌ها و ... .
- ♦ **Network shares:** کنترل اشتراک گذاری‌های شبکه بر روی سرور.
- ♦ **Registry:** ایجاد و کنترل تنظیمات مربوط به Registry.
- ♦ **Data sources:** ایجاد یک منبع داده متمرکز برای کارمندان و فروشندگان.
- ♦ **Devices:** افزودن دستگاه‌های سخت افزاری و فعال/غیرفعال نمودن دستگاه‌های موجود.
- ♦ **Folder options:** پیکربندی تنظیمات فایل‌ها بر روی Windows Explorer و Desktop توسط مدیران و کاربران.
- ♦ **Internet settings:** پیکربندی تنظیمات مرتبط با اینترنت و برنامه Internet Explorer.
- ♦ **Local users and groups:** مدیریت کاربران و گروه‌ها بر روی سرور و کامپیوترها
- ♦ **Power options:** کنترل و مدیریت تنظیمات مرتبط با منبع برق کامپیوترها (مانند حالت Standby و ...).
- ♦ **Printers:** انجام تنظیمات مرتبط با افزودن و یا مدیریت پرینترها (Local و تحت شبکه).
- ♦ **Scheduled tasks:** ایجاد برنامه‌های زمانبندی شده به منظور انجام اقداماتی مشخص (مانند اجرای



برنامه‌ها و ...).

- ♦ **Services:** پیکربندی و مدیریت سرویس‌ها به منظور افزایش امنیت و ... .
- ♦ **Start Menu:** مدیریت منوی Start و افزودن/حذف کردن آیتم‌های موجود در آن.

در شکل ۸-۳۹ نحوه استفاده از آپشن Devices (پس از کلیک راست بر روی Devices و انتخاب New Device « Device نشان داده شده است).



شکل ۸-۳۸

## « فصل ۹ »

اشتراک‌گذاری فایل‌ها و ایجاد

**File Server**

**Sharing Files and Setup**

**File Server**



یکی از وظایف اصلی هر سرور، انجام خدمات مرتبط با نگهداری و اشتراک منابع به منظور استفاده توسط سایر ماشین‌ها و یا سرویس‌ها می‌باشد. در ویندوز سرور 2008R2 یکی از Role‌های کلیدی در این زمینه، File Services می‌باشد. این Role شامل سرویس‌های دیگری از جمله سرویس FSRM<sup>۱</sup>، سرویس NFS<sup>۲</sup> (برای پشتیبانی از کاربران Unix)، سرویس Windows Search، و سرویس BranchCache (برای شعبه‌های Remote) بوده که همگی به منظور خدمت‌رسانی در زمینه استفاده از فایل‌های موجود بر روی سرور به کار می‌روند.

در زمان اشتراک‌گذاری فایل‌ها یا پوشه‌ها، شاید مهمترین مسئله‌ای که باید نسبت به آن آگاهی داشته باشید نحوه اشتراک‌گذاری باشد اما فراموش نکنید که محافظت از آنها توسط مجوزهای NTFS<sup>۳</sup> و همچنین مجوزهای اشتراک‌گذاری نیز از اهمیت بالایی برخوردار می‌باشد. علاوه بر این امکان ایجاد امنیت برای هارد درایورها با استفاده از رمزگذاری BitLocker Drive Encryption نیز می‌تواند به عنوان اقدام امنیتی دیگر به شمار رود.

در ویندوز سرور 2008 استفاده از سرویس‌هایی مانند NFS که امکان اشتراک‌گذاری فایل‌ها را میان سیستم عامل‌های مختلف مانند Windows، Linux، Unix و Mac OS در یک سازمان فراهم نموده و همچنین استفاده از تکنولوژی DFS<sup>۴</sup> که امکان دسترسی به فایل‌هایی که از لحاظ جغرافیایی (در شبکه) پراکنده هستند را فراهم می‌نماید، توانسته است این سیستم عامل و نسخه‌های بعد از آن را به سیستم عاملی قدرتمند جهت ارائه سرویس‌های اشتراک‌گذاری فایل‌ها تبدیل کند.

در این فصل قصد داریم مباحث مرتبط با اشتراک‌گذاری فایل‌ها، پوشه‌ها و همچنین برقراری امنیت برای آنها را مورد بررسی قرار دهیم. بطور کلی مهمترین مباحث مطرح شده در این فصل عبارتند از:

- ♦ نصب File Services بر روی سرور
- ♦ مجوزهای Share و NTFS
- ♦ استفاده از تکنولوژی DFS برای اشتراک‌گذاری پوشه‌ها
- ♦ افزودن پوشه‌های اشتراکی با استفاده از NFS

## ۹-۱ File Services Role

در Server Manager تعدادی کنسول جهت مدیریت Role‌های مختلف از جمله File Services در نظر گرفته شده است. در ویندوز سرور 2008R2، File Services خدماتی بیش از اشتراک‌گذاری پوشه‌ها

---

1. File Server Resource Manager  
 2. Network File System  
 3. New Technology File System  
 4. Distributed File System

را فراهم می‌نماید. این Role شامل تعدادی Role Service به شرح زیر می‌باشد:

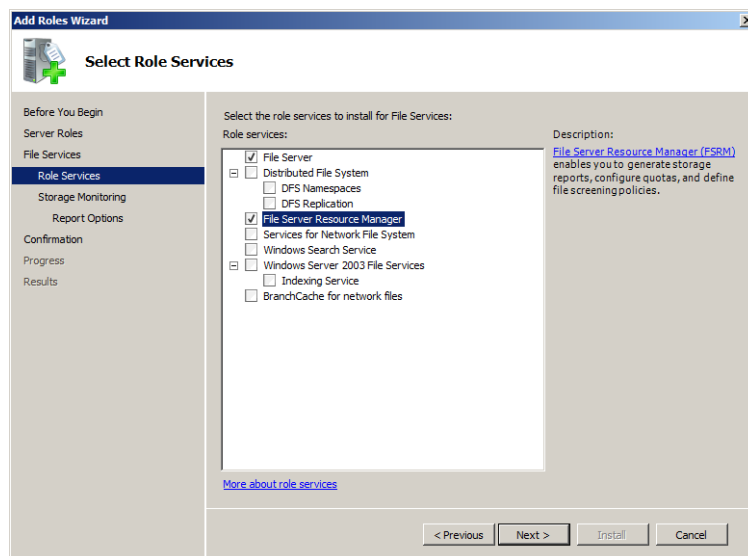
- **File Server:** Role Service اصلی که جهت پشتیبانی از File Services Role مورد نیاز است. این سرویس زمانی که یک پوشه به اشتراک گذاشته می‌شود بطور خودکار اضافه می‌گردد.
  - **Distributed File System (DFS):** DFS (سیستم فایل توزیع شده) سرویسی است که به منظور نگهداری و همگام‌سازی فایل‌های اشتراک گذاشته شده میان سرورهای مختلف مورد استفاده قرار می‌گیرد.
  - **File Server Resource Manager (FSRM):** مجموعه‌ای غنی از ابزارهای اضافی فراهم نموده که به منظور مدیریت ذخیره‌سازی داده‌ها بر روی سرورها مورد استفاده قرار می‌گیرد.
  - **Services for Network File System (NFS):** این سرور امکان دسترسی کاربران سیستم‌های Unix به فایل‌های موجود در ویندوز را فراهم می‌نماید.
  - **Windows Search Service:** این سرویس به منظور شاخص‌دهی جهت جستجوی سریع‌تر فایل‌ها بر روی File Server های کوچک در نظر گرفته شده است و می‌تواند عملکرد فایل سرورهای بزرگ در سازمان را تحت تاثیر قرار دهد.
  - **Windows Server 2003 File Services:** این سرویس شامل یک سرویس شاخص‌دهی بوده که به منظور سازگاری با File Service در ویندوز سرور 2003 در نظر گرفته شده است.
  - **BranchCache for Network Files:** این سرویس در محیط‌های چند سایتی استفاده شده و به شعبه‌های یک سازمان اجازه می‌دهد فایل‌های دانلود شده رایج را Cache نمایند. جهت استفاده از این سرویس لازم است BranchCache بر روی پوشه اشتراک گذاشته شده فعال گردد.
- در طول فصل با برخی از این سرویس‌ها و چگونگی استفاده از آنها آشنا خواهید شد.

## ۹-۱-۱ نصب File Services Role

جهت افزودن File Service Role به سرور، مراحل زیر را دنبال کنید:

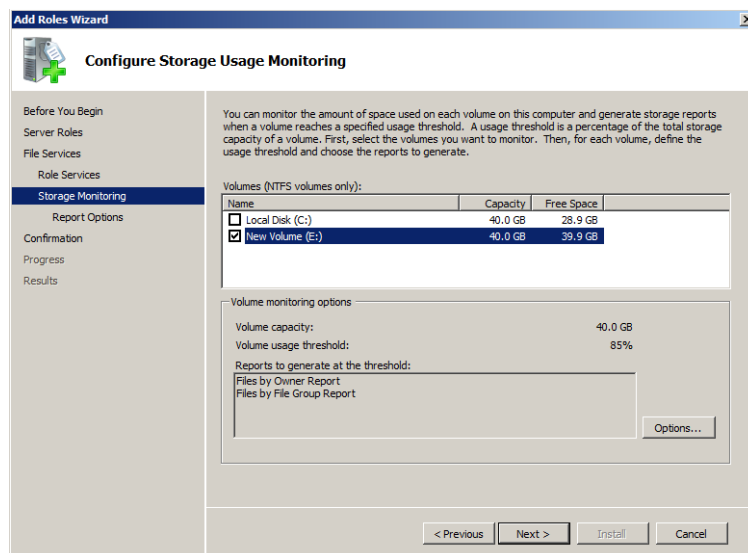
۱. در کنسول Server Manager به قسمت Roles رفته و پیوند Add Roles را انتخاب کنید.
۲. در صفحه “Before You Begin” اطلاعاتی راجع به نصب Role ها ارائه شده است. بر روی Next کلیک کنید.
۳. در صفحه “Select Server Roles” رل File Services را انتخاب نموده و بر روی Next کلیک کنید.
۴. در صفحه “File Services” اطلاعات مرتبط با File Services Role را مشاهده نموده و بر روی Next کلیک کنید.

۵. در صفحه "Select Role Services"، Role Service‌های مورد نظر را انتخاب نموده و بر روی Next کلیک کنید (در اینجا File Server Resource Manager و File Server Resource Manager انتخاب شده است).



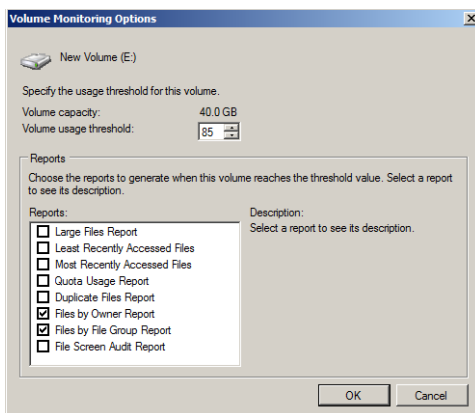
شکل ۹-۱

۶. در صفحه "Configure Storage Usage Monitoring"، درایوی که قصد اشتراک‌گذاری اطلاعات در آنرا دارید انتخاب نموده و بر روی Next کلیک کنید.



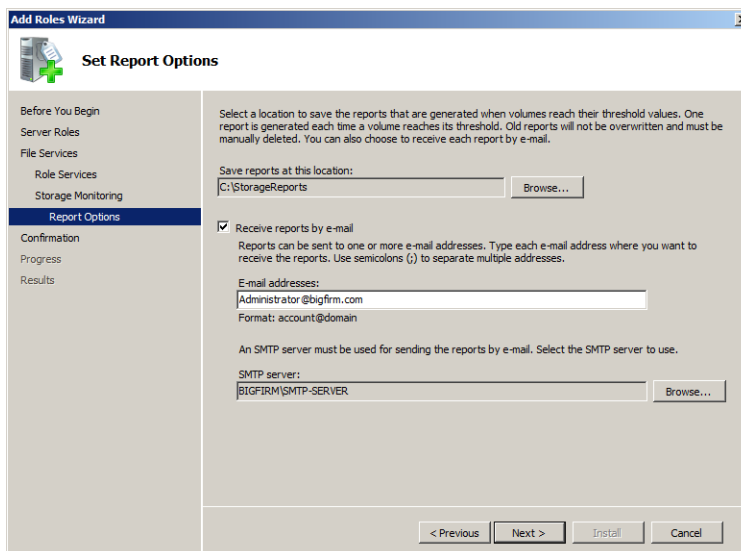
شکل ۹-۲

با استفاده از دکمه Options می‌توانید شرایطی را که در صورت وقوع آنها باید به مدیر سرور گزارش داده شود تعیین کنید. به عنوان مثال در قسمت Volume usage threshold می‌توانید تعیین کنید چنانچه فضای دیسک از درصد مشخصی تجاوز نمود برای مدیر هشدار ارسال گردد.



شکل ۳-۹

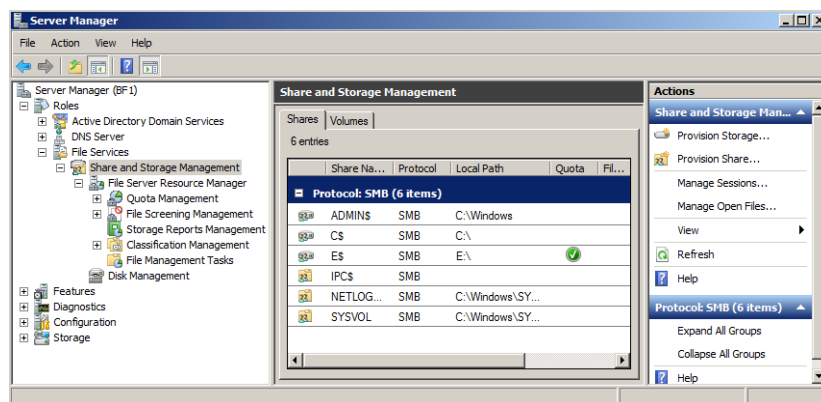
۷. در صفحه “Set Report Options” محلی را جهت قرارگیری گزارش‌ها تعیین کنید. همچنین با فعال‌سازی گزینه Recive reports by e-mail نیز می‌توانید گزارش‌های مربوط به این سرویس را از طریق ایمیل دریافت کنید (البته به شرطی که سرور SMTP در شبکه پیکربندی شده باشد). پس از انجام تنظیمات بر روی Next کلیک کنید.



شکل ۴-۹

۸. در صفحه “Confirm Installation Selections” خلاصه‌ای از تنظیمات انجام شده را مشاهده نموده و بر روی Install کلیک کنید. کمی منتظر بمانید تا عملیات نصب به اتمام رسد.

چنانچه Server Manager را مجدداً اجرا کنید، مشاهده خواهید نمود که گره Share and Storage Management به همراه تعدادی گره دیگر به قسمت Roles «File Services» اضافه شده است.



شکل ۵-۹

## ۹-۲ ایجاد Share

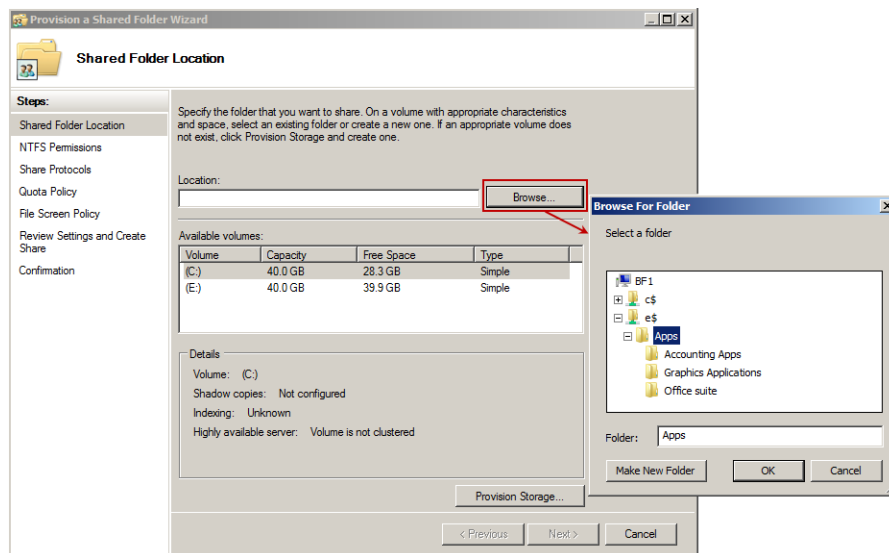
در این قسمت چندین روش برای اشتراک‌گذاری معرفی می‌کنیم. پس از اینکه یک Share ایجاد شد لازم است در اکتیو دایرکتوری منتشر شده تا دسترسی به آن توسط سایر کاربران آسان گردد.

### ۹-۲-۱ ایجاد Share با استفاده از Server Manager

ایجاد Share با استفاده از Server Manager بسیار ساده است. گره Share and Storage Management شامل ویزاردی به نام “Provision a Shared Folder Wizard” است که به کمک آن و طبق مراحل زیر می‌توانید Share را ایجاد کنید:

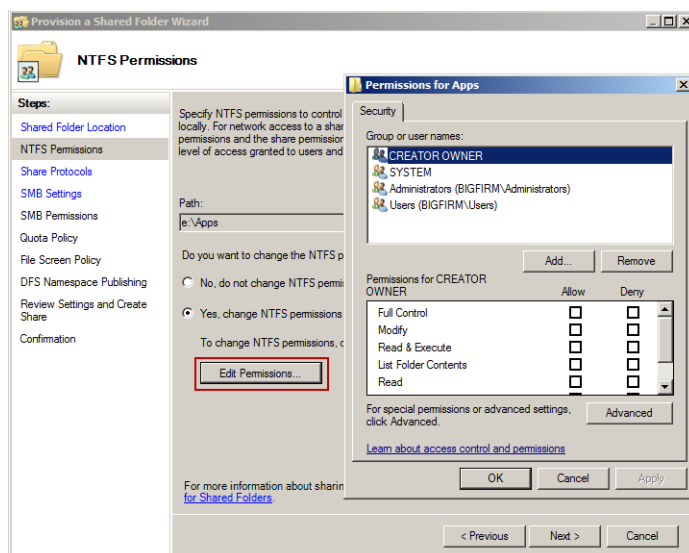
۱. از مسیر Administrative Tools «Start» کنسول Server Manager را اجرا کنید.
۲. به گره Roles «File Services» «Share and Storage Management» رفته و بر روی آن کلیک‌راست نمایید. سپس گزینه Provision Share را انتخاب کنید.
۳. در صفحه “Shared Folder Location” بر روی Browse کلیک کنید. پوشه‌ای که قصد دارید به اشتراک گذارید را انتخاب نموده و بر روی Ok کلیک کنید (ما در اینجا پوشه Apps را در درایو E انتخاب کرده‌ایم).





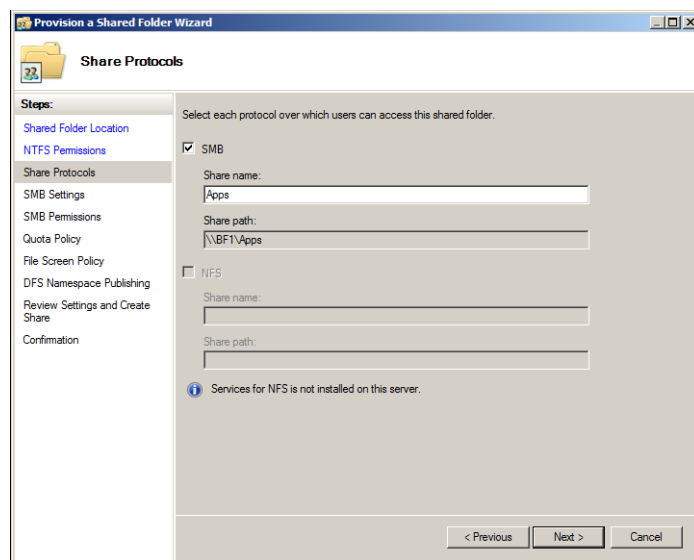
شکل ۹-۶

۴. در صفحه "NTFS Permissions" می‌توانید مجوزهای داده شده به افراد یا گروه‌ها را برای دسترسی به پوشه مشخص کنید. با انتخاب گزینه No, do not change permissions تنظیمات پیش‌فرض پذیرفته می‌شود. چنانچه قصد دارید این تنظیمات را مورد تغییر قرار دهید، می‌توانید از گزینه Yes, change NTFS permissions استفاده کنید. پس از انجام تنظیمات بر روی Next کلیک کنید.



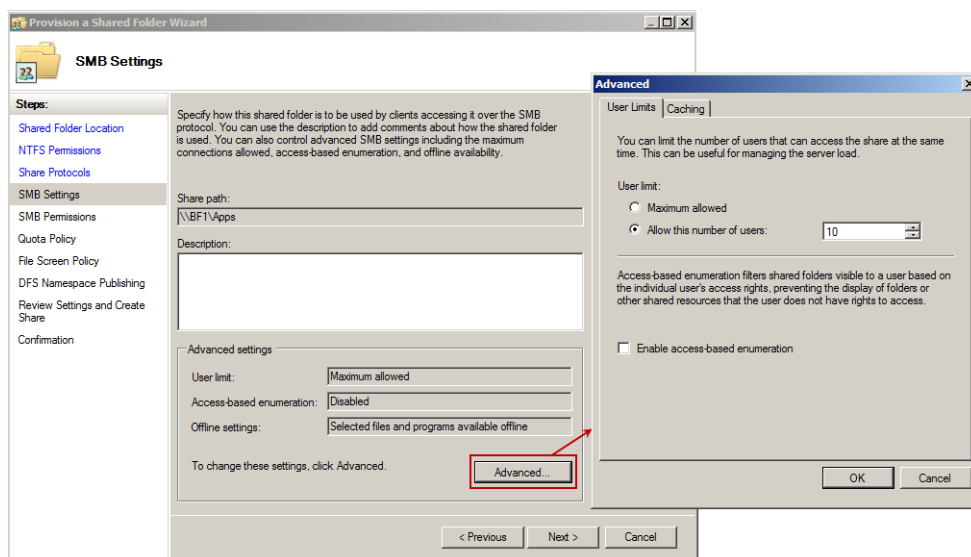
شکل ۹-۷

۵. در صفحه “Share Protocols”، پروتکل SMB (پروتکل انتقال پیغام در ویندوز) و یک نام جهت نمایش پوشه اشتراک‌گذاشته شده انتخاب کنید. سپس بر روی Next کلیک کنید.



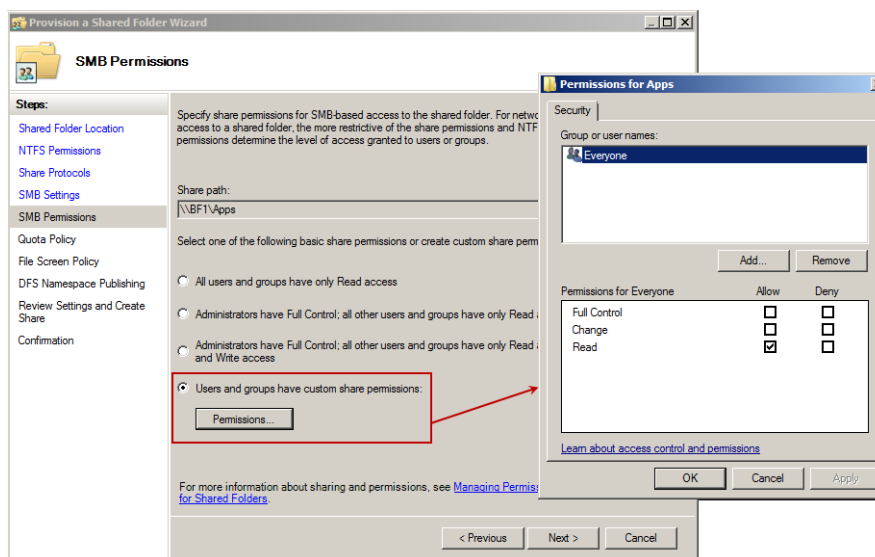
شکل ۸-۹

۶. در صفحه “SMB Settings” می‌توانید با استفاده از دکمه Advanced بعضی از تنظیمات پیشرفته مانند User Limit (جهت تعیین تعداد دسترسی همزمان به Share) و Access-based Enumeration (مربوط به تنظیمات DFS) را مشخص کنید. پس از انجام تنظیمات بر روی Next کلیک کنید.



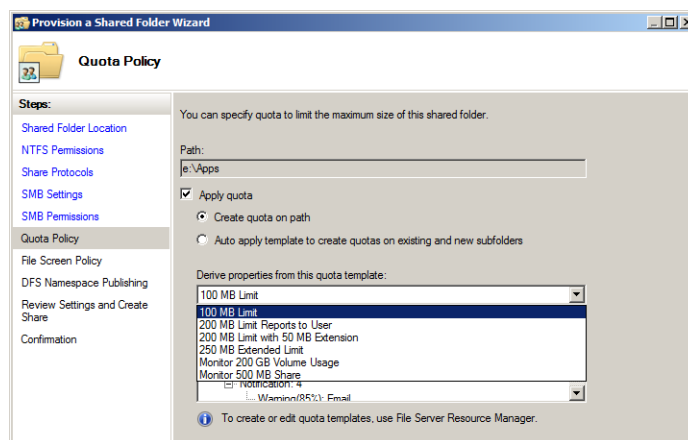
شکل ۹-۹

۷. در صفحه "SMB Permissions" می‌توانید تنظیمات پیش‌فرض برای مجوز اشتراک (Share) را انتخاب نموده و یا آنها را تغییر دهید. برای تغییر مجوزها ابتدا گزینه "Users and groups have custom share permissions" را انتخاب کنید. پس از انجام تنظیمات و انتخاب گزینه مورد نظر بر روی Next کلیک کنید.



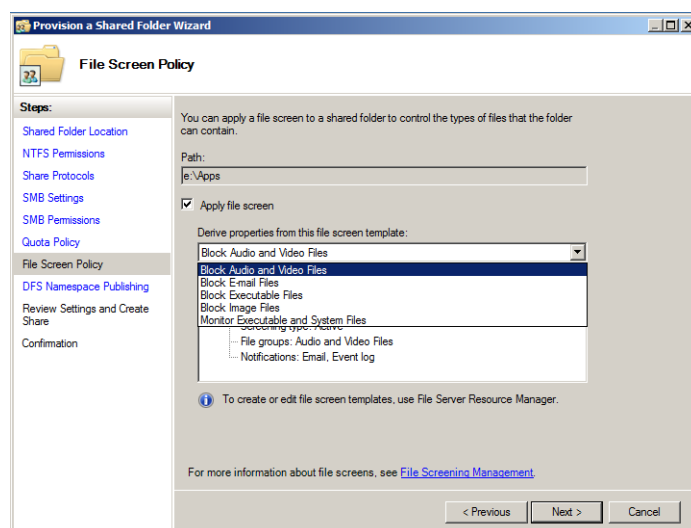
شکل ۹-۱۰

۸. در صفحه "Quota Policy" می‌توانید سهمیه‌بندی مورد نظر برای اشتراک را تعیین کنید. به عنوان مثال اگر می‌خواهید که کاربران را به فضای ذخیره‌سازی مشخصی محدود کنید، می‌توانید با استفاده از قسمت Drive properties from this quota template فضای مورد نظر را برای او تعیین نمایید (بعداً در این مورد بیشتر صحبت خواهیم نمود). بر روی Next کلیک کنید.



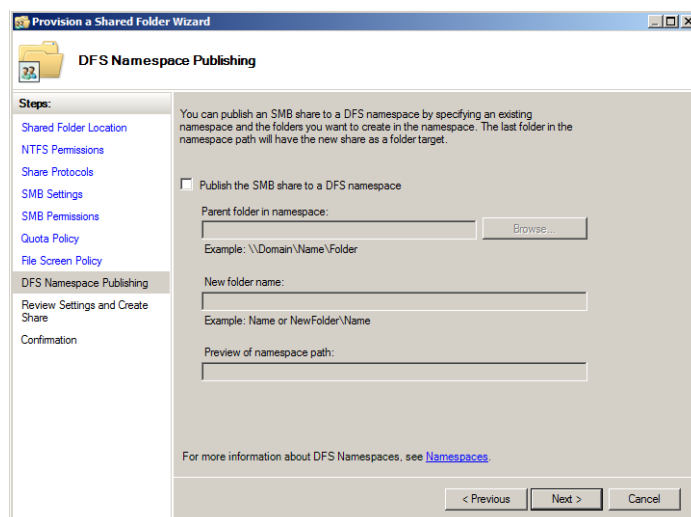
شکل ۹-۱۱

۹. در صفحه “File Screen Policy” می‌توانید انواعی از فایل‌ها را که قصد ندارید توسط دیگران در پوشه اشتراک گذاشته شده ذخیره شوند، مسدود کنید. به عنوان مثال برای اطمینان از اینکه کاربران نمی‌توانند فایل‌های صوتی و ویدئویی را بروی پوشه اشتراکی ذخیره نمایند، می‌توانید گزینه Block Audio and Video Files را انتخاب کنید. بروی Next کلیک کنید.



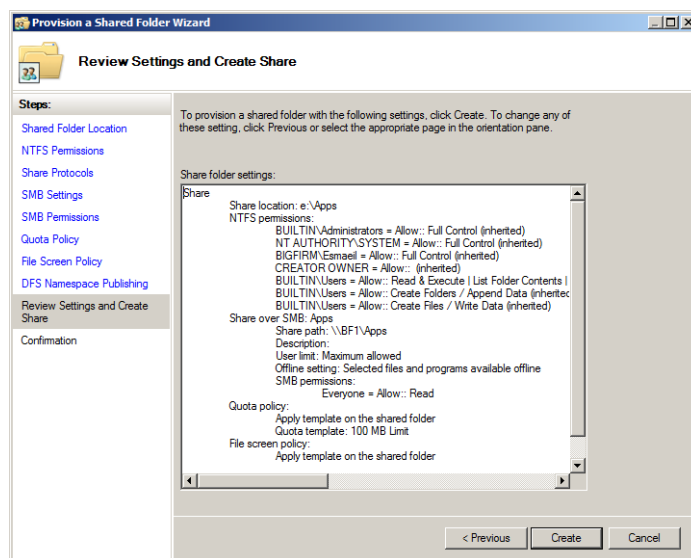
شکل ۹-۱۲

۱۰. در صفحه “DFS Namespace Publishing” می‌توانید اشتراک SMB را به فضای نام DFS انتشار دهید (DFS بعداً در همین فصل مورد بررسی قرار خواهد گرفت). بروی Next کلیک کنید.



شکل ۹-۱۳

۱۱. در صفحه "Review Settings and Create Share" خلاصه‌ای از تنظیمات انجام شده را مشاهده نموده و بر روی Create کلیک کنید.



شکل ۹-۱۴

۱۲. پس از اتمام عملیات ایجاد Share بر روی Close کلیک کنید.

## ۹-۲-۲ ایجاد Share بر روی کامپیوترهای Remote با استفاده از Server Manger

پروسه قبلی، برای ایجاد Share بر روی کامپیوترهای Remote با استفاده از کنسول Server Manager نیز امکان پذیر می‌باشد. برای انجام این کار باید اطمینان پیدا کنید که کامپیوترهای Remote بطور صحیح پیکربندی شده‌اند. این کار با استفاده از سه دستور زیر امکان‌پذیر است:

۱. Cmd را بر روی کامپیوتری که قصد دارید به صورت Remote کنید اجرا نموده و دستور زیر را جهت فعال‌سازی WinRM وارد کنید:

```
winrm qc
```

۲. مطمئن شوید که سرویس Virtual Disk بر روی کامپیوتر Remote فعال است. برای انجام این کار دستور زیر را در خط فرمان (Cmd) وارد کنید:

```
sc config vds start= auto
net start vds
```

۳. در نهایت لازم است تنظیمات مربوط به فایروال را بر روی کامپیوتر Remote انجام دهید. به این

منظور دستور زیر را وارد کنید:

```
netsh advfirewall firewall set rule group="Remote Volume Management"
new enable=yes
```

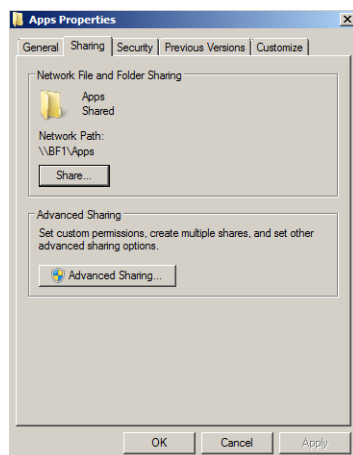
اکنون پس از پیکربندی کامپیوتر Remote می‌توانید فایل را بر روی آن به اشتراک گذارید. برای انجام این کار مراحل زیر را دنبال کنید:

۱. Server Manager را بر روی سرور Local اجرا کنید.
۲. بر روی گره Server Manager کلیک‌راست نموده و گزینه Connect to Another Computer را انتخاب کنید.
۳. نام کامپیوتر Remote را وارد نموده و بر روی Ok کلیک کنید.
۴. پس از اتصال سرور به کامپیوتر Remote می‌توانید فرایندی مشابه با قسمت قبل را جهت اشتراک گذاری فایل بر روی آن اجرا کنید.

### ۳-۲-۹ ایجاد Share با استفاده از Windows Explorer

برای ایجاد Share با استفاده از Windows Explorer، مجدداً پوشه E:\Apps را در نظر بگیرید. برای قرار دادن آن در شبکه مراحل زیر را دنبال کنید:

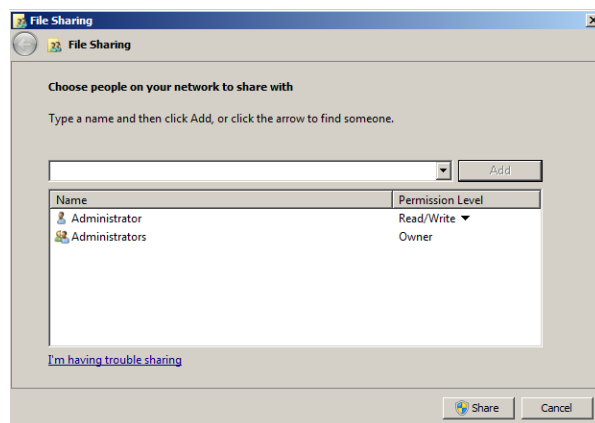
۱. بر روی پوشه Apps کلیک‌راست نموده و Properties را انتخاب کنید.
۲. به تب Sharing رفته و بر روی دکمه Share کلیک کنید.



شکل ۹-۱۵

۳. در پنجره "File Sharing" افرادی که قصد اشتراک‌گذاری پوشه با آنها را دارید به لیست اضافه

نموده و بر روی Share کلیک کنید.



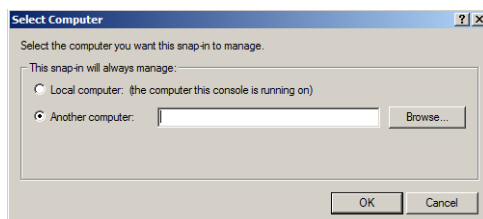
شکل ۹-۱۶

۴. بر روی Done کلیک کنید.
۵. برای مشاهده لیست پوشه‌های اشتراک گذاشته شده توسط افراد می‌توانید در پنجره Computer به قسمت Network مراجعه کنید.

#### ۹-۲-۴ ایجاد Share با استفاده از کنسول Computer Management

با استفاده از کنسول Computer Management امکان اشتراک‌گذاری پوشه‌ها به صورت Local و Remote وجود دارد. مزیت استفاده از Computer Management در این است که می‌توان پوشه‌های اشتراک‌گذاشته شده بر روی سایر سرورها را نیز کنترل نمود. برای انجام این کار لازم است به سرور Remote متصل شوید، بنابراین می‌توانید مراحل زیر را دنبال کنید:

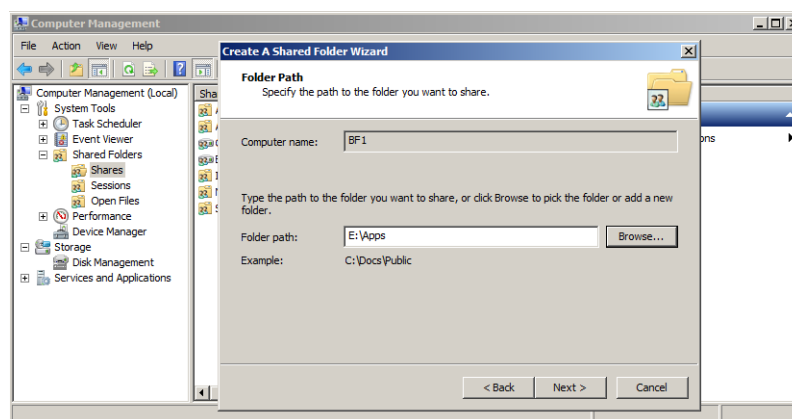
۱. از مسیر Start » administrative Tools، Computer Management را اجرا کنید.
۲. بر روی گره Computer Management (Local) کلیک راست نموده و گزینه Connect to Another Computer را انتخاب کنید.
۳. در پنجره "Select Computer" نام سرور مورد نظر را وارد نموده و یا آنرا در شبکه جستجو کنید.



شکل ۹-۱۷

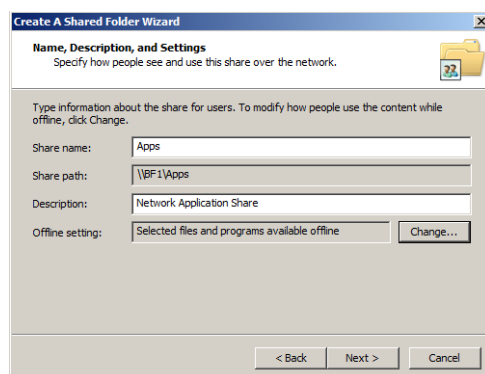
برای اشتراک‌گذاری پوشه‌ها با استفاده از این کنسول لازم است مراحل زیر را دنبال کنید:

۱. به مسیر Computer Management\SystemTools\Shared Folders\Shares بروید.
۲. بر روی گروه Shares کلیک‌راست نموده و New Share را انتخاب کنید. ویزارد “Create a Shared a Folder Wizard” اجرا می‌گردد.
۳. در صفحه “Welcom to Create A Shared Folder Wizard” بر روی Next کلیک کنید.
۴. در صفحه “Folder Path” پوشه مورد نظر برای Share را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۹-۱۸

۵. در صفحه “Name, Description, and Settings” نام و توضیحی برای پوشه اشتراک‌گذاشته شده وارد نموده و بر روی Next کلیک کنید.



شکل ۹-۱۹

۶. در صفحه “Shared Folder Permissions” تعدادی گزینه جهت تعیین مجوزهای پوشه ارائه شده است. این گزینه‌ها عبارتند از:



- ♦ **All users have read-only access:** این گزینه به گروه Everyone (همه کاربران) مجوز فقط خواندنی (Read-Only) می‌دهد.
- ♦ **Administrators have full access; other users have read-only access:** این گزینه به مدیران مجوز کنترل کامل پوشه و به کاربران تنها مجوز خواندن از پوشه را می‌دهد.
- ♦ **Administrators have full access; other users have no access:** با انتخاب این گزینه تنها مدیران قادر خواهند بود به پوشه دسترسی پیدا کنند.
- ♦ **Customize permissions:** این گزینه امکانات بیشتری جهت تعیین مجوزها برای کاربران و گروه‌ها در اختیار شما قرار می‌دهد و به کمک آن می‌توانید مجوزهای شخصی‌سازی شده بر روی آنها اعمال کنید (اعمال این مجوزها با استفاده از دکمه Customize امکان‌پذیر می‌باشد).



شکل ۹-۲۰

پس از انتخاب گزینه مورد نظر و انجام تنظیمات لازم بر روی Next کلیک کنید.

۷. در صفحه "Sharing was Successful" خلاصه‌ای از تنظیمات به همراه موفقیت آمیز بودن Share نشان داده می‌شود. بر روی Finish کلیک کنید.



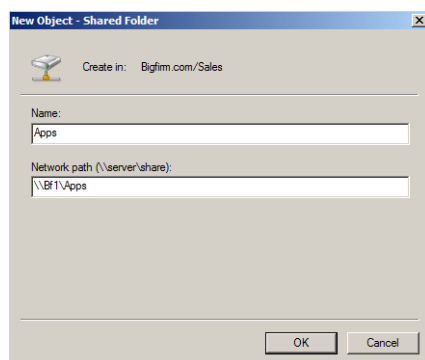
شکل ۹-۲۱

## ۹-۲-۵ انتشار Share در اکتیو دایرکتوری

یکی از مزیت‌های مهم اکتیو دایرکتوری، یکپارچه‌سازی منابع سازمان از جمله پرینترها، کاربران، گروه‌ها، واحدهای سازمانی و ... می‌باشد. این منابع یکپارچه شامل Shareها نیز می‌شود. دلیل اصلی انتشار Share در اکتیو دایرکتوری این است که کاربران به راحتی بتوانند آنرا پیدا نموده و مورد استفاده قرار دهند. به عنوان مثال چنانچه پوشه اشتراکی Apps که در درایو E قرار داشت را در اکتیو دایرکتوری منتشر کنید، کاربران که به دامنه متصل هستند می‌توانند به راحتی آنرا جستجو نموده و در صورت داشتن مجوز از آن استفاده کنند.

جهت انتشار Share در اکتیو دایرکتوری مراحل زیر را دنبال کنید:

۱. کنسول Active Directory Users and Computers را اجرا کنید.
۲. بروی یکی از OUها (مانند Share) کلیک‌راست نموده و New Shared Folder را انتخاب کنید.
۳. نام و مسیر قرارگیری Share در شبکه را مشخص نموده و بروی OK کلیک کنید.

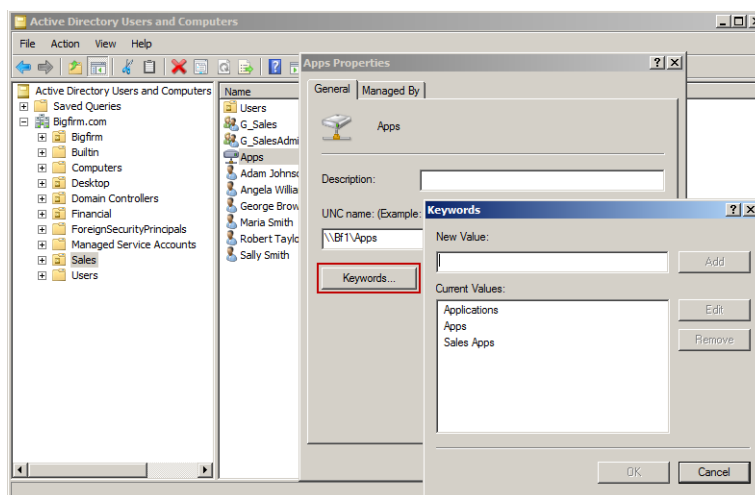


شکل ۹-۲۲

اکنون پوشه تعیین شده در AD انتشار یافته است. می‌توانید برای سهولت کار تعدادی کلمه کلیدی<sup>۱</sup> نیز برای جستجوی آن اضافه نمایید. برای انجام این کار مراحل زیر را دنبال کنید:

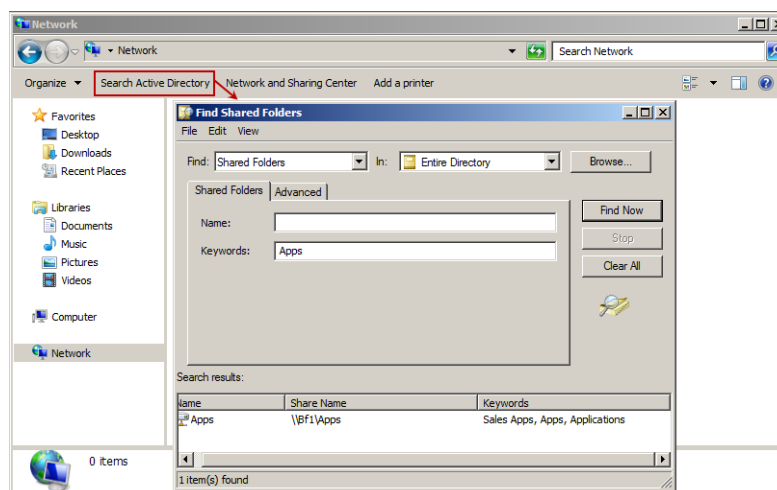
۱. در کنسول ADUC بروی اشتراکی که ایجاد کردید (Apps) کلیک‌راست نموده و Properties را انتخاب کنید.
۲. در تب General بروی دکمه Keywords کلیک کنید.
۳. در قسمت New Value کلمات کلیدی را وارد نموده و بروی OK کلیک کنید.

1. KeyWords



شکل ۹-۲۳

۴. جهت جستجوی این پوشه در اکتیو دایرکتوری می‌توانید به کامپیوتر یکی از کاربران رفته و در قسمت Network از پنجره Computer، بر روی Search Active Directory کلیک نمایید. در صفحه باز شده می‌توانید جستجو را با استفاده از نام پوشه و یا کلمات کلیدی آن انجام دهید.



شکل ۹-۲۴

### ۳-۹ مدیریت مجوزها

یکی از مزیت‌های قابل توجه فرمت NTFS برای درایوها، امکان اختصاص مجوز به فایل‌ها و

پوشه‌ها و کنترل افرادی است که می‌توانند به آنها دسترسی داشته باشند. بین مجوزهای Share و مجوزهای NTFS شباهت‌های زیادی وجود دارد که در این قسمت آنها را مورد بررسی قرار می‌دهیم. نکته قابل توجه این است که باید از نتیجه اعمال همزمان این دو نوع مجوز بر روی پوشه‌ها آگاهی داشته باشید چراکه اعمال مجوزهای نادرست موجب عدم دسترسی افراد به این پوشه‌ها خواهد شد.

### ۹-۳-۱ مجوزهای NTFS

مجوزهای NTFS بر روی فایل‌ها و پوشه‌های موجود در یک دیسک که با استفاده از قالب NTFS فرمت‌بندی شده است قابل اعمال است. این مجوزها به صورت زیر می‌باشند:

- ♦ **Read:** این مجوز تنها امکان خواندن محتویات، مجوزها و مشخصه‌های یک فایل یا پوشه را فراهم می‌نماید.
- ♦ **Read and Execute:** با استفاده از این مجوز کاربران می‌توانند علاوه بر خواندن فایل‌ها، آنها را اجرا نمایند. فایل‌هایی مانند .exe، .bat و .com از جمله فایل‌های قابل اجرا به شمار می‌روند.
- ♦ **List Folder Contents:** این مجوز به کاربران امکان می‌دهد که تنها بتوانند از این که پوشه‌ای دارای محتویات هست یا خیر آگاهی پیدا کنند. با استفاده از این مجوز امکان خواندن محتویات پوشه وجود ندارد.
- ♦ **Write:** با استفاده از این مجوز، امکان ایجاد تغییر در فایل یا پوشه فراهم می‌گردد. این تغییرات شامل اضافه کردن فایل یا پوشه درون پوشه فعلی و یا ایجاد تغییر در آن می‌باشد. دقت داشته باشید که امکان حذف فایل از یک پوشه با استفاده از این مجوز وجود ندارد.
- ♦ **Modify:** این مجوز، علاوه بر دادن مجوزهای Read، Write، Read and Execute، امکان حذف فایل از پوشه را نیز فراهم می‌نماید.
- ♦ **Full Control:** این مجوز امکان انجام هر عملی را بر روی فایل‌ها و پوشه‌ها امکان پذیر می‌نماید. با استفاده از این مجوز حتی امکان تغییر مجوز سایر افراد نیز فراهم می‌گردد.

### ۹-۳-۲ مجوزهای Share

این مجوزها تنها زمانی که یک پوشه در شبکه به اشتراک گذاشته می‌شود قابل اعمال هستند و به سه دسته تقسیم می‌شوند:

- ♦ **Read:** با این مجوز افراد قادر خواهند بود فایل‌ها یا پوشه‌های اشتراک گذاشته شده را مشاهده نمایند.
- ♦ **Change:** مجوز Change، اختیاراتی همچون خواندن، اجرا کردن، ایجاد تغییر و حذف فایل‌ها از درون پوشه را به افراد واگذار می‌نماید.

- ♦ **Full Control:** این مجوز کلیه اختیارات برای انجام اقدامات بر روی پوشه اشتراکی را در اختیار افراد قرار می‌دهد.

دقت داشته باشید که در هر دو نوع مجوز NTFS و Share، انتخاب Allow به معنی دادن مجوز و انتخاب Deny به معنی گرفتن مجوز از افراد می‌باشد. چنانچه فرد یا گروهی دارای بیش از یک مجوز باشد (Read، Write و ...)، مجوز این کاربر یا گروه از نوع ترکیبی می‌باشد.

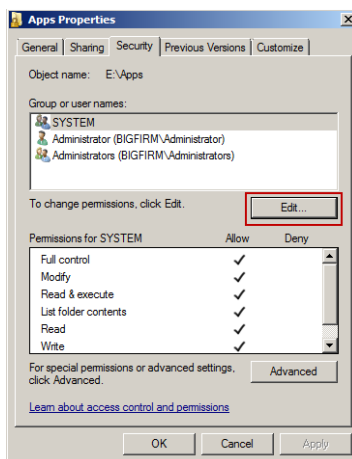
### ۳-۳-۹ ایجاد و تغییر مجوزهای NTFS و Share

ایجاد و تغییر هر دو نوع مجوز NTFS و Share با استفاده از کنسول Server Manager و یا Windows Explorer امکان‌پذیر می‌باشد. در ادامه انجام این کار را به هر دو روش شرح خواهیم داد.

#### ایجاد مجوز با استفاده از Windows Explorer

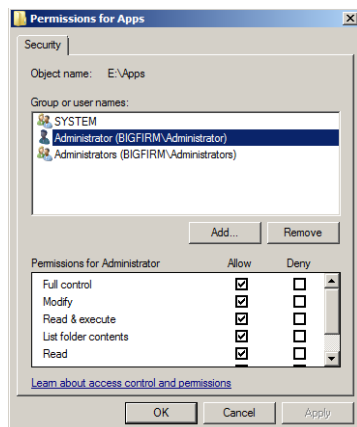
برای ایجاد مجوزهای NTFS بر روی پوشه‌ها (چه اشتراکی و چه غیر اشتراکی) مراحل زیر را دنبال کنید:

۱. بر روی پوشه مورد نظر کلیک راست نموده و Properties را انتخاب کنید.
۲. در پنجره "Folder Properties" تب Security را انتخاب کنید.
۳. در تب Security لیستی از کاربران و گروه‌ها به همراه مجوزهای داده شده به آنها نمایش داده شده است. برای ایجاد تغییر در مجوزها، بر روی دکمه Edit کلیک کنید.



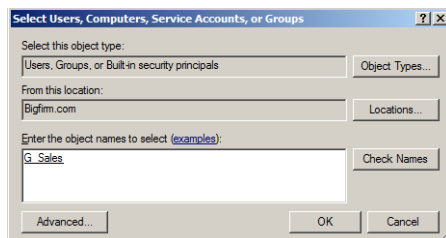
شکل ۹-۲۵

۴. در پنجره باز شده، کاربر یا گروه مورد نظر را انتخاب نموده و از قسمت Permission for... مجوزهای لازم را با انتخاب Allow یا Deny به کاربر یا گروه مورد نظر اختصاص دهید.



شکل ۹-۲۶

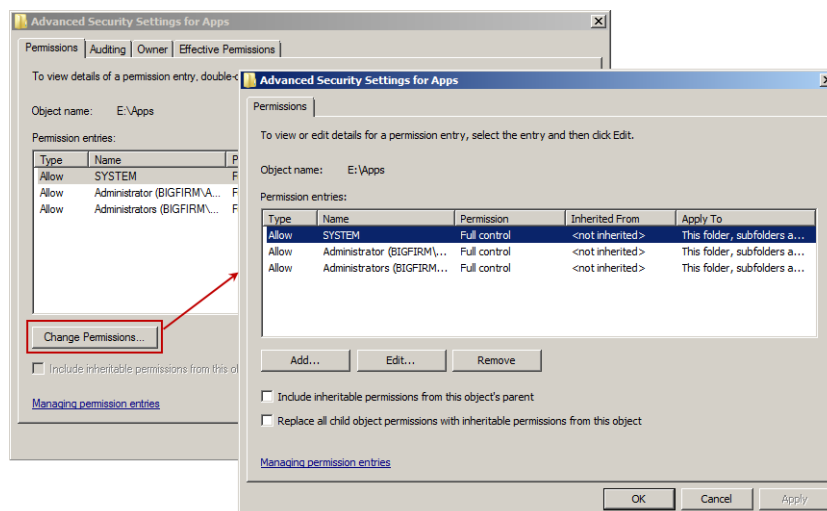
۵. جهت افزودن کاربر و یا گروه به این لیست بر روی دکمه Add در این پنجره کلیک کنید.
۶. در پنجره "Select Users, Computers, Service Accounts, or Groups" می‌توانید نام کاربر و یا گروه را وارد نموده و یا با استفاده از دکمه Advanced آنرا جستجو کنید.



شکل ۹-۲۷

۷. پس از افزودن کاربران یا گروه‌ها و اختصاص مجوز به آنها بر روی کلیه دکمه‌های OK کلیک نموده و پنجره‌ها را ببندید.

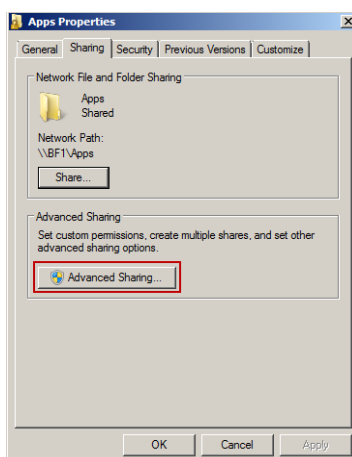
چنانچه بار دیگر به مرحله ۳ (شکل ۹-۲۵) باز گردید، مشاهده می‌کنید که دکمه‌ای به نام Advanced نیز وجود دارد. از این دکمه در مواردی که قصد دارید مجوزهای بیشتری به افراد یا گروه‌ها اختصاص دهید استفاده می‌شود. تعداد آپشن‌هایی که دکمه Advanced فراهم می‌کند نسبت به حالت تعریف شده با استفاده از دکمه Edit بیشتر بوده و بنابراین به شما امکان می‌دهد که دقت بیشتری در اختصاص مجوزها داشته باشید. در شکل ۹-۲۸ پنجره‌ای که با کلیک بر روی دکمه Advanced اجرا می‌شود نشان داده شده است. در این پنجره با کلیک بر روی دکمه Change Permissions و سپس دکمه‌های Add و Edit می‌توانید تنظیمات کاربران، گروه‌ها و مجوزهای آنها را انجام دهید.



شکل ۹-۲۸

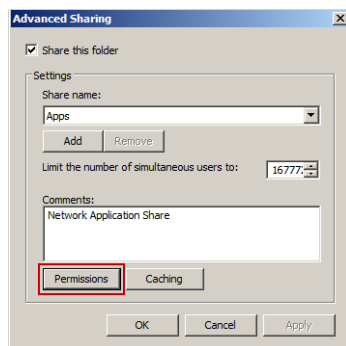
پس از تشریح نحوه ایجاد مجوزهای NTFS، اکنون مراحل کار را برای ایجاد مجوزهای Share شرح می‌دهیم. پوشه اشتراکی Apps در درایو E را در نظر بگیرید. برای تغییر مجوزهای پیش‌فرض آن می‌توانید مراحل زیر را دنبال کنید:

۸. بروی پوشه اشتراکی کلیک راست نموده و Properties را انتخاب کنید.
۹. در پنجره باز شده، تب Sharing را انتخاب نموده و بروی دکمه Advanced Sharing کلیک کنید.



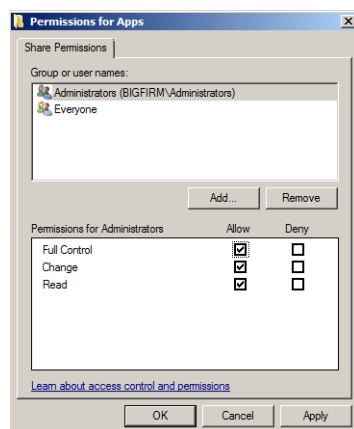
شکل ۹-۲۹

۱۰. در پنجره "Advanced Sharing" بروی دکمه Permissions کلیک کنید.



شکل ۹-۳۰

۱۱. کاربر و یا گروه مورد نظر را انتخاب نموده و مجوزهای لازم را به او اختصاص دهید. جهت افزودن کاربر و یا گروه به این لیست می‌توانید از دکمه Add استفاده کنید.



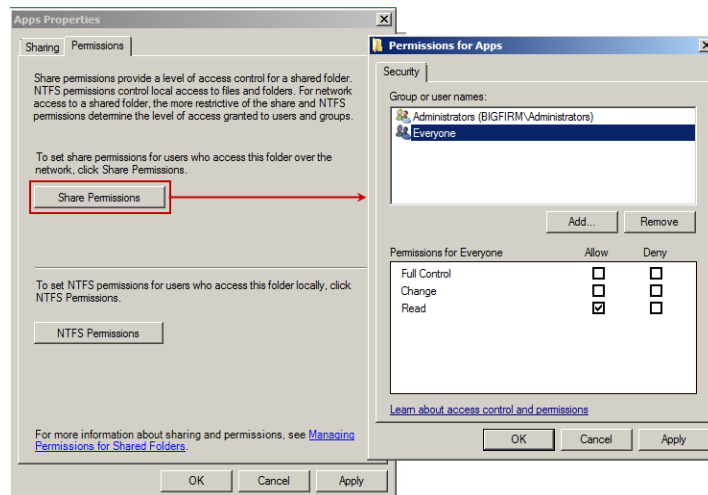
شکل ۹-۳۱

### ایجاد مجوز با استفاده از Server Manager

مجوزهای ایجاد شده در این روش نیز همانند مجوزهای قبل هستند. تنها تفاوت در این است که مراحل ایجاد و یا تغییر مجوزها با استفاده از کنسول Server Manager انجام می‌شود:

۱. Server Manager را اجرا نموده و به مسیر «Roles» «File Services» «Share and Storage Management» بروید.
۲. بر روی فایل Share (در اینجا Apps) کلیک راست نموده و Properties را انتخاب کنید.
۳. به تب Permission رفته و بر روی دکمه Share Permissions کلیک کنید تا پنجره «Permissions for Apps» نمایش داده شود.



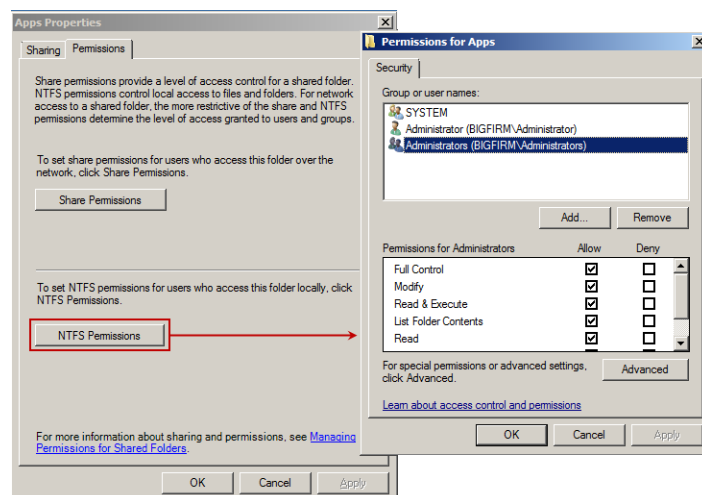


شکل ۹-۳۲

۴. جهت افزودن کاربران و یا گروه‌ها از دکمه Add، جهت حذف آنها از دکمه Remove، و جهت اختصاص مجوز از گزینه‌های Allow و Deny استفاده کنید.
۵. برروی OK کلیک نموده و پنجره‌ها را ببندید.

جهت ایجاد و تغییر مجوزهای NTFS برروی این پوشه نیز می‌توانید مراحل زیر را دنبال کنید:

۱. برروی فایل Share (در اینجا Apps) کلیک‌راست نموده و Properties را انتخاب کنید.
۲. به تب Permission رفته و برروی دکمه NTFS Permissions کلیک کنید.



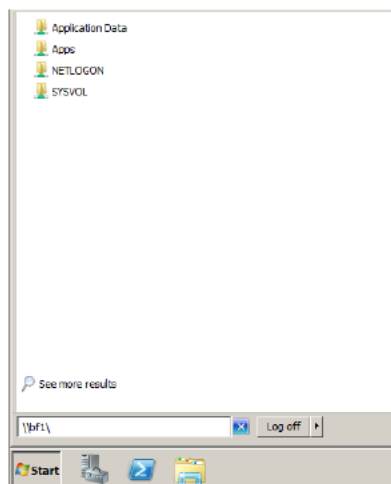
شکل ۹-۳۳

۳. جهت افزودن، حذف کردن و یا اختصاص مجوز به کاربران و گروه‌ها همانند قبل اقدام کنید.

در هنگام اختصاص مجوزها حتماً به این نکته توجه داشته باشید که مجوزهای Share و NTFS را طوری اختصاص ندهید که در آن تداخلی ایجاد شود. به عنوان مثال چنانچه به کاربری مجوز Full Control را در NTFS داده باشید و سپس برای همین گروه در Share مجوز Full Control را Deny کرده باشید، نباید انتظار داشته باشید که این کاربر بتواند در استفاده از پوشه اشتراکی در شبکه کنترل کاملی داشته باشد زیرا مجوز این کار در شبکه از او گرفته شده است.

#### ۹-۴ اتصال به Shareها

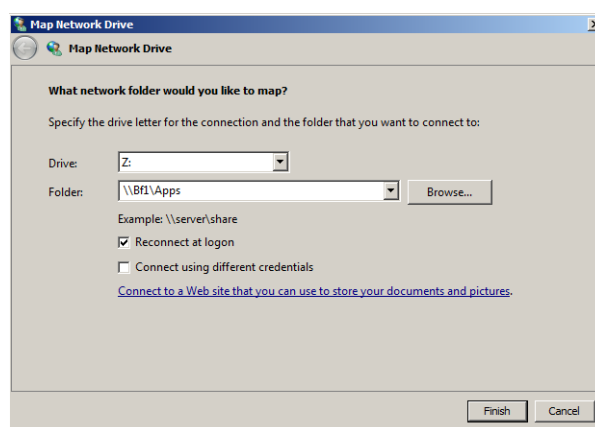
جهت اتصال به پوشه‌های اشتراکی از نام UNC آنها به صورت \\ServerName\ShareName استفاده می‌شود، به عنوان مثال برای دسترسی به فایل‌ها و پوشه‌های اشتراک گذاشته شده در سرور Bf1 باید از نام \\BF1\ استفاده شود. بدین منظور به قسمت جستجوی منوی Start رفته و عبارت \\BF1\ را وارد کنید. تمام اشتراک‌های موجود بر روی این سرور نمایش داده خواهد شد. با کلیک بر روی هر Share می‌توانید در صورت داشتن مجوز به محتویات آن دسترسی پیدا کنید.



شکل ۹-۳۳

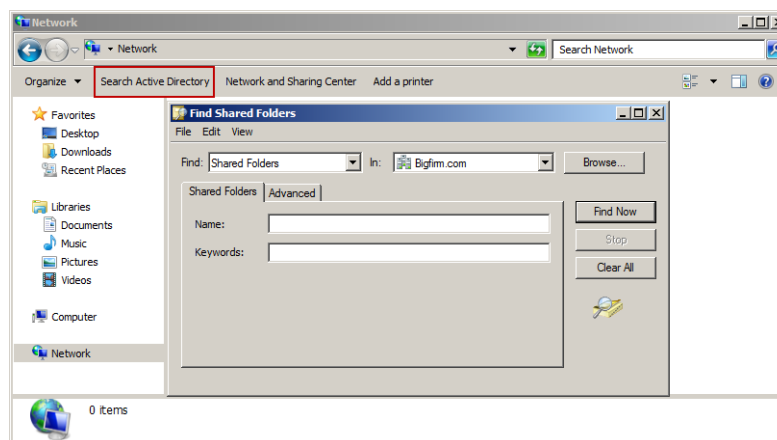
در سیستم عامل‌هایی مانند Windows XP که قسمت Search در منوی Start آنها وجود ندارد، می‌توانید از ابزار Run استفاده نموده و نام UNC را در آن وارد کنید.

- برای دسترسی به فایل‌های اشتراک گذاشته شده روش‌های دیگری نیز وجود دارد که عبارتند از:
- ♦ استفاده از گزینه **Map Network Drive**: این گزینه زمانی استفاده می‌شود که قصد دارید کاربران در هنگام Logon شدن به سیستم، به Share‌ها دسترسی پیدا کنند. برای استفاده از این امکان، در منوی Start بروی Computer یا Network کلیک‌راست نموده و گزینه Map Network Drive را انتخاب کنید (در فصل ۱۳ به این موضوع خواهیم پرداخت).



شکل ۹-۳۵

- ♦ جستجوی اکتیو دایرکتوری: اگر کاربران عضوی از یک دامنه باشند، در کنسول Network (Computer «Network») از آنها گزینه‌ای به نام Search Active Directory ظاهر می‌شود که با استفاده از آن می‌توانند پوشه‌های اشتراک گذاشته را جستجو کنند.



شکل ۹-۳۶

- ♦ استفاده از دستور **net use** با استفاده از دستور **net use** در خط فرمان نیز امکان دسترسی به Shareها وجود دارد. این دستور به صورت زیر استفاده می‌شود:

```
net use driveletter \\servername\sharename
```

به عنوان مثال برای جستجوی پوشه Apps در سرور BF1 که نام درایو اشتراک نیز Z می‌باشد از دستور زیر استفاده می‌شود:

```
net use Z: \\BF1\apps
```

چنانچه بعداً تصمیم گرفتید که این نگاشت را حذف کنید می‌توانید از دستور زیر استفاده نمایید:

```
net use Z: /delete
```

امکان استفاده از دستور **net use** در ارتباطات WAN نیز امکان‌پذیر می‌باشد. به عنوان مثال چنانچه آدرس IP سرور BF1 برابر با 134.81.12.4 باشد، می‌توانید از دستور زیر برای دسترسی به پوشه Apps در آن استفاده کنید:

```
net use \\134.81.12.4\apps
```

## ۹-۵ سرویس File Server Resource Manager

FSRM سرویسی اضافی است که می‌توانید به همراه رل File Service اضافه کنید. این سرویس تعدادی قابلیت‌هایی را به File Server اضافه نموده و مدیریت آنرا ساده‌تر می‌کند. این قابلیت‌ها عبارتند از:

- ♦ ایجاد و مدیریت Quota Policy
- ♦ ایجاد و مدیریت File Screen Policy
- ♦ مشاهده گزارش‌ها

### ۹-۵-۱ ایجاد Quota Policy

در فرمت NTFS، امکاناتی برای مدیریت سهمیه‌بندی<sup>۱</sup> دیسک وجود دارد اما با این حال قابلیت‌های بیشتر و کاملتری را در FSRM مشاهده خواهید نمود. Quota امکان نظارت و محدود کردن فضای کاربران در استفاده از یک درایو یا پوشه را در اختیار شما قرار می‌دهد.

---

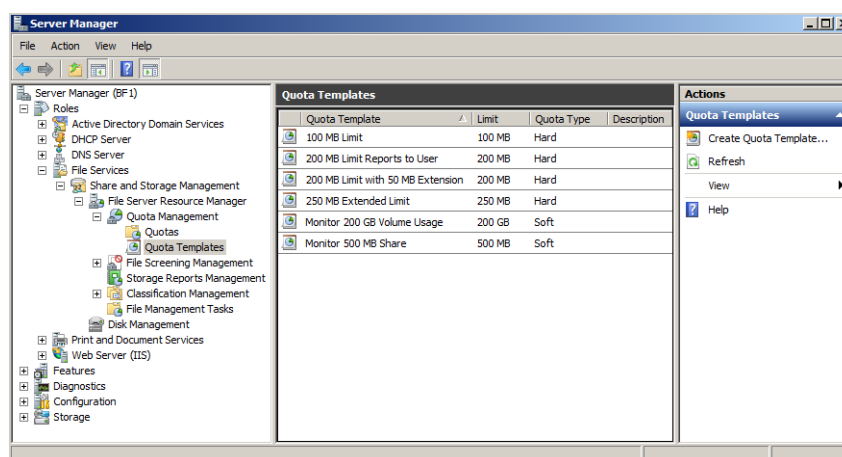
1. Quota  
2. Monitor

با استفاده از Quota، امکاناتی مانند تنظیم هشدارهای محدودیت‌ها، دریافت اطلاعات مربوط به محدودیت از طریق Email یا مدخل‌های Log، و حتی اجرای دستورات در پاسخ به هر گونه محدودیت فراهم می‌گردد.

Quotaها می‌توانند بر روی هر Share و یا مسیر خاصی بر روی سرور تنظیم شوند. همچنین می‌توانند برای نظارت بر ذخیره‌سازی داده‌ها بر روی File Server نیز مفید واقع شوند. به عنوان مثال فرض کنید که فضای ذخیره‌سازی File Server برابر با ۲TB (معادل 2048GB) باشد. شاید این فضا از نظر شما کافی باشد اما چنانچه کاربران فایل‌های صوتی و ویدیویی را بر روی سرور ذخیره کنند، این فضا به سرعت پر خواهد شد، بنابراین با استفاده از Quota Policyها می‌توانید کاربران را در مقدار مشخصی از این فضا محدود کنید. حالت دیگری را در نظر بگیرید که فایل‌های صوتی و ویدیویی جزء جدایی‌ناپذیر تجارت شما باشند. بنابراین ممکن است نخواهید فضای ذخیره‌سازی را محدود کنید اما بجای آن چنانچه فضای ذخیره‌سازی به یک آستانه مشخص رسید از آن مطلع شوید. در این حالت می‌توانید از Quota Policyها بجای اعمال محدودیت، تنها برای نظارت بر فضای مصرف شده استفاده کنید. در ادامه این policyها را بیشتر مورد بررسی قرار خواهیم داد.

### Quota Templates

مایکروسافت تعدادی Quota Templates در FSRM قرار داده است که می‌توانید از آنها به راحتی استفاده نموده و یا با توجه به نیاز خود آنها را تغییر دهید. همچنین در صورت نیاز می‌توانید Templateهای خود را ایجاد کنید. در شکل ۹-۳۷، Templateهای پیش‌فرض که در Quota Templates از FSRM قرار دارد نشان داده شده است.

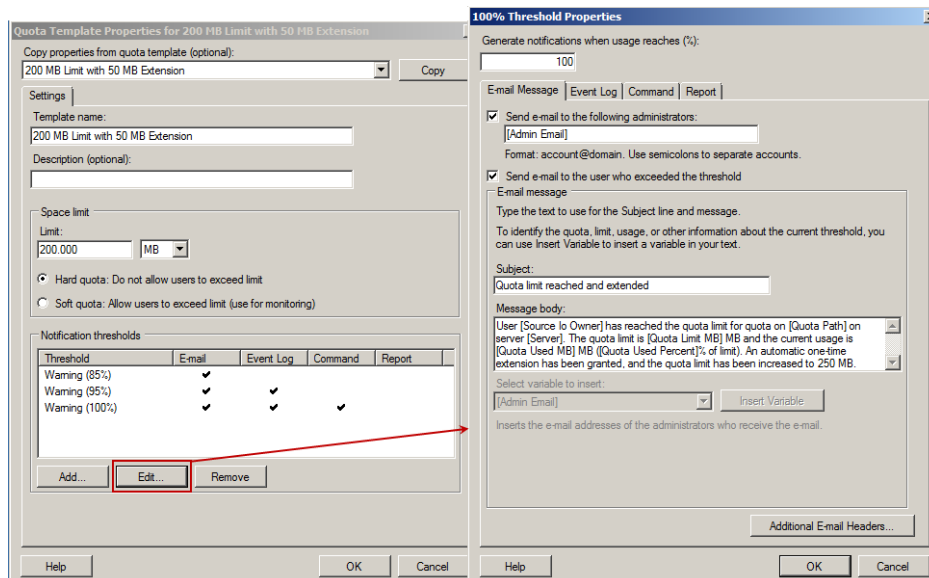


شکل ۹-۳۷

جهت آشنایی با طرز کار Quota ها، اطلاعات ارائه شده در شکل ۹-۳۷ می‌تواند مفید واقع گردد. به عنوان مثال یکی از اطلاعات موجود در این صفحه، Quota Type است که نوع سهمیه‌بندی را مشخص نموده و به دو دسته Soft و Hard تقسیم می‌شود. Soft Quota ها تنها به منظور نظارت و فراهم نمودن هشدارها مورد استفاده قرار می‌گیرند و کاری با محدود کردن فضای کاربران ندارند. برعکس، Hard Quota ها جهت ایجاد محدودیت در فضای دیسک استفاده می‌شوند.

### ویرایش مشخصات یک Quota Template

برای مشاهده و ویرایش مشخصات یک Template کافی است بر روی آن کلیک‌راست نموده و گزینه Edit Template Properties را انتخاب کنید. در شکل ۹-۳۸ پنجره Properties مربوط به Quota Template با نام "200 MB Limit with 50 MB extension" نشان داده شده است. همانطور که در پنجره سمت چپ مشاهده می‌کنید، در پایین این پنجره و در قسمت Notification thresholds سه آستانه اطلاع رسانی پیکربندی شده است: ۸۵٪، ۹۵٪ و ۱۰۰٪. آستانه ۸۵٪ تنها یک ایمیل ارسال نموده، آستانه ۹۵٪ یک ایمیل فرستاده و آنرا به عنوان یک رویداد (log) ثبت می‌کند، و آستانه ۱۰۰٪ نیز علاوه بر ارسال ایمیل و ثبت رویداد، یک دستور را نیز اجرا می‌نماید. پنجره سمت راست، با انتخاب یکی از Notification thresholds و کلیک بر روی دکمه Edit حاصل می‌شود. در این پنجره چهار تب برای انجام تنظیمات مربوط به هر Quota فراهم شده است.



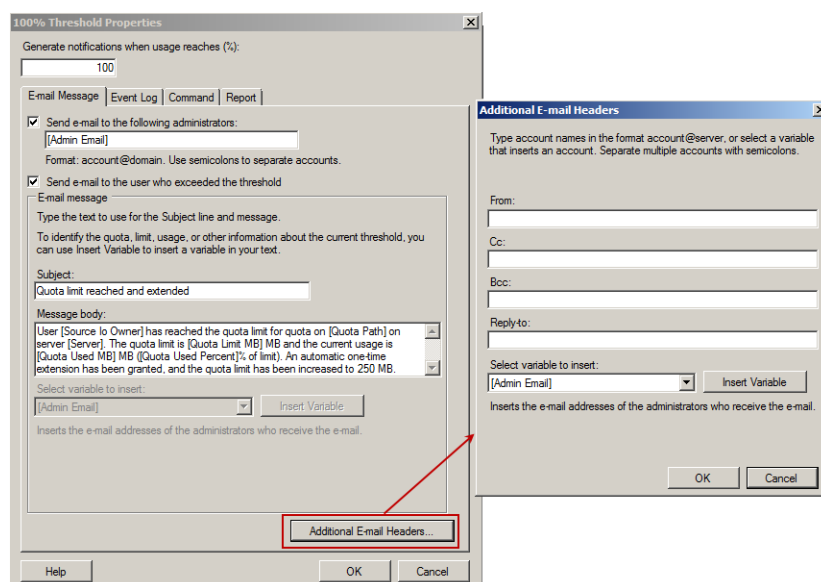
شکل ۹-۳۸

## تب E-mail Message

این تب امکان پیکربندی آدرس ایمیل برای ارسال هشدارهای محدودیت فضا را فراهم می‌نماید. چنانچه قصد دارید این ایمیل‌ها به مدیران (و یا گروهی از آنها ارسال شود) می‌توانید آدرس ایمیل آنها را به صورت account@domain در قسمت Send e-mail to following administrators وارد نمایید، مانند ITAdmins@bigfirm.com. همچنین ارسال ایمیل برای کاربرانی که فضای آنها در حال پرشدن می‌باشد نیز با استفاده از گزینه Send e-mail to the user who exceeded the threshold امکان‌پذیر می‌باشد. FSRM از Active Directory به منظور جستجوی آدرس‌های ایمیل استفاده می‌نماید.

Subject و Message body در Template‌ها (در هشدارهایی که فرستاده می‌شوند) به صورت پیش‌فرض پیکربندی شده‌اند ولی می‌توانید آنها را مورد تغییر قرار دهید. چنانچه به شکل ۹-۳۸ توجه کنید، متن پیغامی که فرستاده می‌شود شامل چندین متغیر است: Quota Path, Source I/O Owner, Server و .... با کلیک بر روی این متن یا متن موجود در قسمت Subject، یک لیست Drop-Down در پایین پنجره فعال می‌گردد. می‌توانید هر کدام از متغیرها را از این لیست انتخاب نموده و توضیح مختصری که راجع به عملکرد آن ارائه می‌شود مشاهده کنید. همچنین با استفاده از دکمه Insert Variable می‌توانید انواع متغیرها را به متن پیغام اضافه نمایید.

علاوه بر موارد بالا، دکمه Additional E-mail Headers نیز به شما امکان می‌دهد یک سرایند اضافی به ایمیل اضافه کنید. در ۹-۳۹ فیلدهای این سرایند قابل مشاهده می‌باشد.



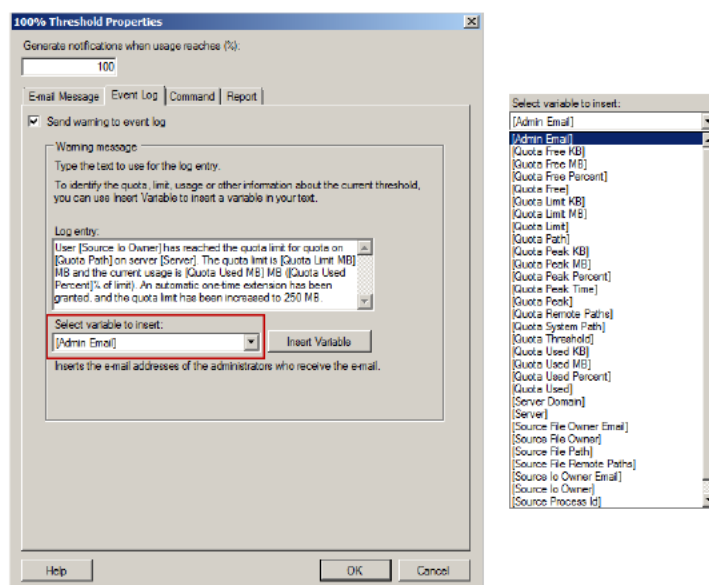
شکل ۹-۳۹



برای ارسال ایمیل توسط FSRM لازم است که سرور SMTP در شبکه پیکربندی شده باشد. این سرور به منظور پذیرش آدرس‌های ایمیلی که ارسال می‌شوند مورد استفاده قرار می‌گیرد. برای استفاده از SMTP باید نام و یا آدرس IP این سرور در تنظیمات FSRM تعیین گردد.

### تب Event Log

در این تب می‌توانید ایمیل‌های ارسالی را به صورت رویدادهایی در log مربوط به سرویس ثبت کنید. همانند آدرس ایمیل، می‌توانید با استفاده از لیست Drop-Down موجود، متغیرهایی که نیاز به ثبت شدن در مدخل‌های log دارید را تعیین نمایید.

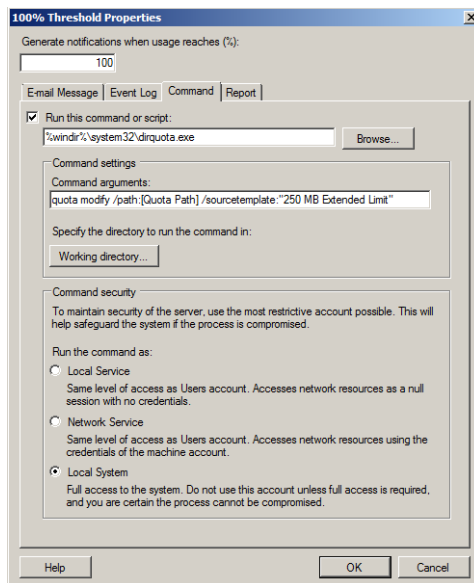


شکل ۹-۴۰

### تب Command

تنظیمات این تب زمانی استفاده می‌شود که قصد داشته باشید در صورت رسیدن به آستانه مشخصی از فضای استفاده شده، دستور خاصی برای ایجاد تغییر در Quota اجرا شود. در این Template، از ابزار dirquota.exe به منظور تغییر فضا از ۲۰۰ MB به ۲۵۰ MB استفاده شده است. همچنین امکان ایجاد بسترهای امنیتی نیز با توجه به مجوزهایی که دستور برای اجرا شدن نیاز دارد فراهم شده است.

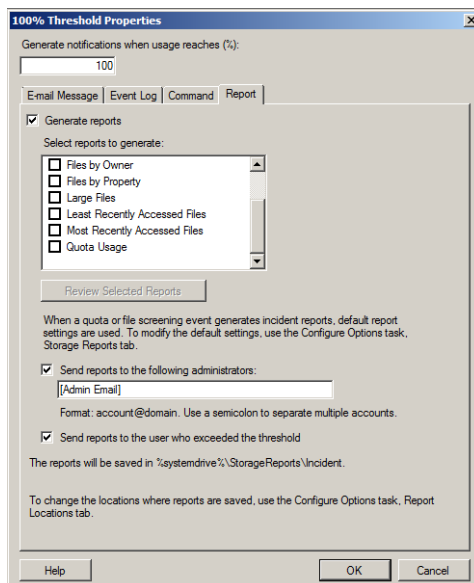




شکل ۹-۴۱

### تب Report

در این تب امکان ایجاد انواع گزارش‌ها و ارسال خودکار آنها به مدیران فراهم شده است. برای انجام این کار کافی است نوع گزارش را از قسمت Select reports to generate انتخاب کنید.



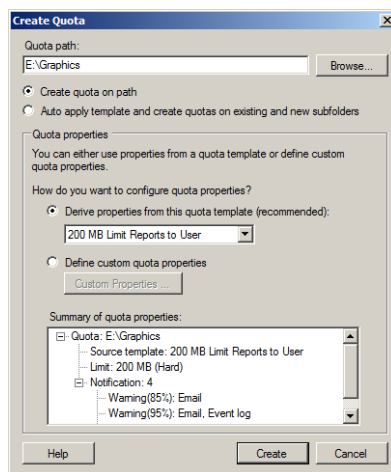
شکل ۹-۴۲

## ۹-۵-۲ ایجاد یک Quota

اکنون که با مفاهیم Quota آشنا شدید، به نحوه ایجاد آن می‌پردازیم. فرض کنید می‌خواهید بر میزان داده‌هایی که در فایل‌ی به نام Graphics ذخیره شده و بر روی سیستم شما قرار دارد نظارت کنید. بطور خاص می‌خواهید بدانید که آیا حجم داده‌های ذخیره شده در این پوشه نزدیک به ۵۰۰ MB هست یا خیر. اگر به حجم مورد نظر نزدیک بود، باید گزارشی به کاربر ارسال نموده تا او از فایل‌های تکراری، فایل‌های حجیم، و فایل‌هایی تا کنون استفاده نشده‌اند اطلاع پیدا کند.

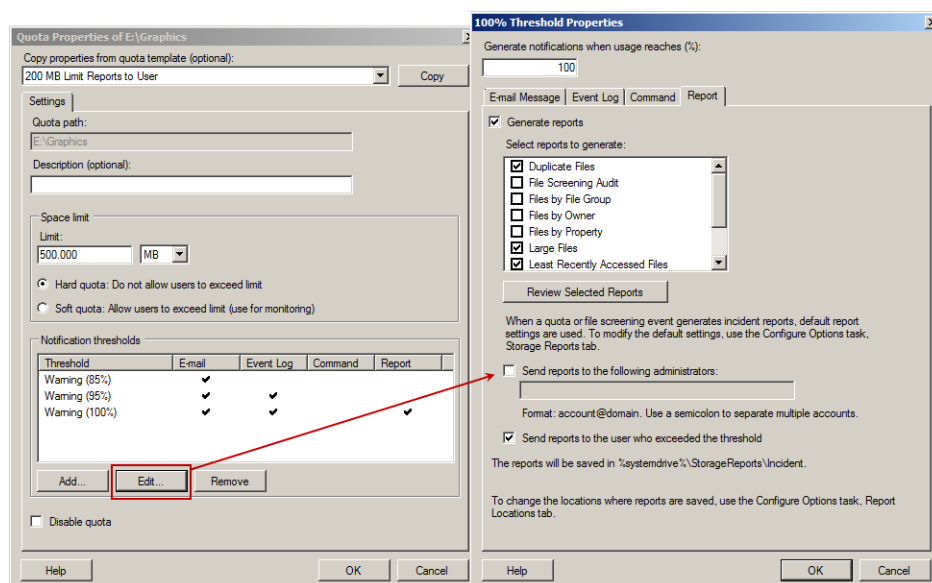
برای ایجاد این Quota مراحل زیر را دنبال کنید:

۱. Server Manager را اجرا نموده و به گره «File Services» «Share and Storage Management» «Quota Management» «Quota Templates» حرکت کنید.
۲. بر روی Quota با نام «200 MB Limit Reports to User» کلیک‌راست نموده و گزینه Create Quota from Template را انتخاب کنید.
۳. در قسمت Quota Path مسیری پوشه‌ای که قصد نظارت بر آن دارید را وارد نموده (مانند E:\Graphics) و یا با استفاده از دکمه Browse مسیر آنرا مشخص کنید.
۴. بر روی Create کلیک کنید.



شکل ۹-۴۳

۵. در پنل سمت راست Server Manager، زیرگره Quotas از گره Quota Templates را انتخاب نمایید.
۶. بر روی Quota ای که ایجاد کردید کلیک‌راست نموده و گزینه Edit Quota Properties را انتخاب کنید.
۷. در قسمت Space Limit، میزان فضا را از ۲۰۰ MB به ۵۰۰ MB تغییر دهید.
۸. آستانه Warning (100%) را انتخاب نموده و بر روی Edit کلیک کنید.



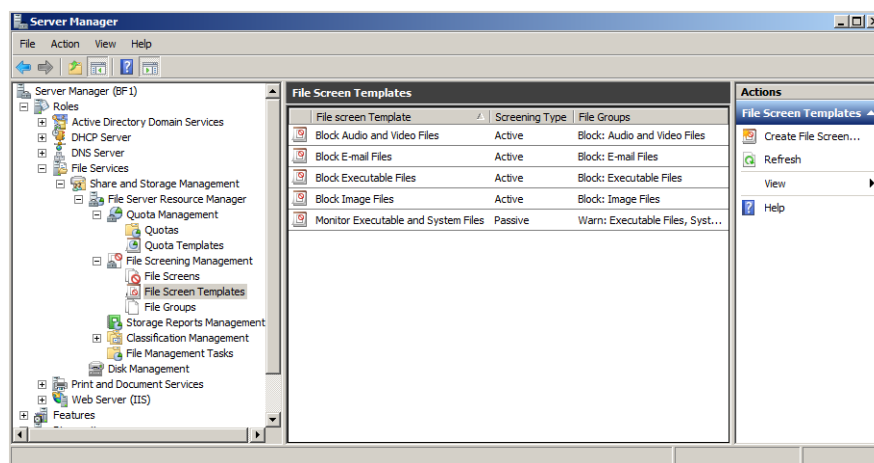
شکل ۹-۴۴

۹. اطلاعات موجود در تب‌های E-mail Message، Event Log و Command را مشاهده کنید. چنانچه با پیغامی مبنی بر پیکربندی نشدن سرور SMTP روبرو شدید، بر روی Yes کلیک کنید. SMTP را بعداً می‌توانید پیکربندی کنید.
۱۰. تب Report را انتخاب کنید.
۱۱. همانطور که در شکل ۹-۴۴ مشاهده می‌کنید، گزینه Generate Reports فعال بوده و سه گزارش Duplicate Files، Large Files و Least Recently Accessed Files انتخاب شده‌اند. علاوه بر این، ارسال گزارش از طریق ایمیل نیز برای کاربران پیکربندی شده است. بر روی OK کلیک کنید تا صفحه "100% Threshold Properties" بسته شود.
۱۲. در نهایت برای بستن صفحه "Quota Properties" نیز بر روی OK کلیک کنید.

### ۹-۵-۳ ایجاد File Screen Policy

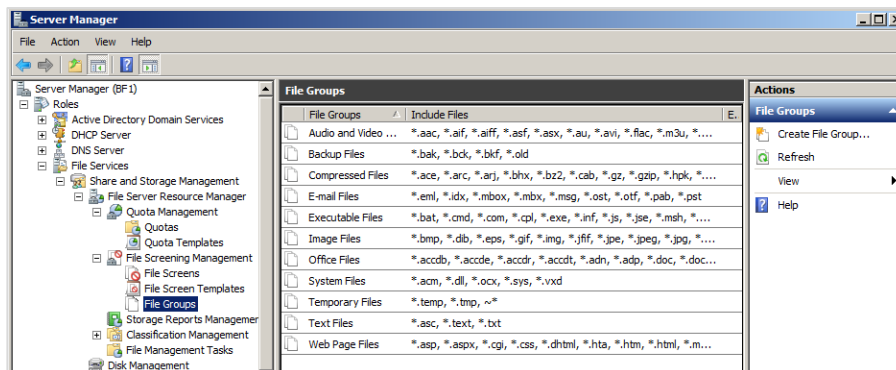
File Screen ها به منظور فیلتر کردن داده‌هایی که بر روی سرور ذخیره می‌شوند و اطمینان از اینکه انواع خاصی از داده‌ها قابلیت ذخیره شدن بر روی سرور را ندارند مورد استفاده قرار می‌گیرد. فرض کنید پس از اینکه Quota Policy ها را ایجاد نمودید، مدت زیادی طول نمی‌کشد که گزارش‌هایی مبنی بر رو به اتمام بودن ظرفیت ذخیره‌سازی دریافت می‌کنید که دلیل آن می‌تواند فایل‌های حجیم Backup هایی باشد که کاربران از فایل‌های MP3 خود ایجاد نموده و بر روی سرور ذخیره کرده‌اند.

ممکن است تمایل نداشته باشید که کاربران این فایل‌های MP3 و یا هر نوع داده صوتی و ویدئویی دیگر را بر روی سرور ذخیره کنند، بنابراین می‌توانید با ایجاد File Screen ها مانع از ذخیره انواع مشخصی از داده‌ها شده و زمانی که کاربری قصد ذخیره چنین داده‌هایی دارد، برای او پیغام هشدار ارسال کنید. File Screen ها می‌توانند بر روی درایوها و یا پوشه‌ها اعمال شده و همانند Quota دارای Template می‌باشند. در شکل زیر Template های مربوط به File Screen ها در کنسول Server Manager نشان داده شده است.



شکل ۹-۴۵

دقت داشته باشید که برای مشاهده لیست کامل فایل‌های قابل فیلتر شدن توسط File Screen می‌توانید به گره File Groups مراجعه کنید. در این گره، انواع فایل‌ها با پسوندهای مورد استفاده در هر نوع نشان داده شده است.

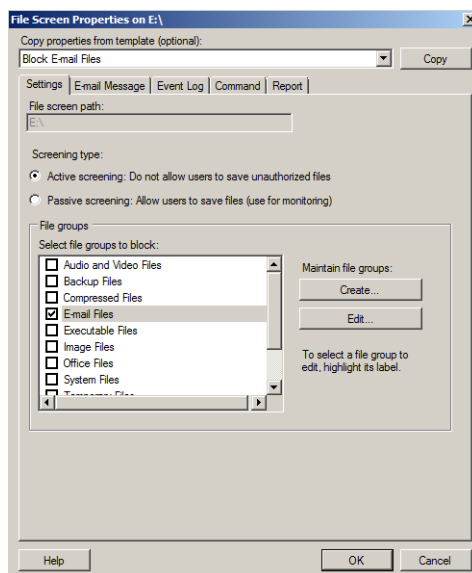


شکل ۹-۴۶

فرض کنید شرکت شما به تازگی متوجه شده است که بسیاری از کاربران آن فایل‌های Outlook که دارای پسوند .pst هستند را بر روی سروری که دارای ۱GB فضا بوده و در حال پر شدن است ذخیره می‌کنند. شرکت بیان می‌کند که فایل‌های Outlook نمی‌توانند بر روی Server ذخیره شوند بنابراین شما باید این دسته از فایل‌ها را فیلتر کنید.

برای اجرای طرح بالا مراحل زیر را دنبال کنید:

۱. کنسول Server Manager را اجرا نموده و به گره File Screen Templates حرکت کنید.
۲. بر روی Template با نام “Block E-mail Files” کلیک راست نموده و گزینه Create File Screen from Template را انتخاب کنید.
۳. در قسمت File Screen Path، نام Volume مورد نظر جهت فیلتر کردن را وارد نموده (مانند E:\) و بر روی Create کلیک کنید.
۴. زیرگروه File Screens را از زیرمجموعه File Screen Templates انتخاب کنید. بر روی File Screen که ایجاد کردید کلیک راست نموده و گزینه Edit File Screen Properties را انتخاب کنید.
۵. در پنجره “File Screen Properties” می‌توانید یکی از گزینه‌های Active Screening یا Passive Screening را انتخاب کنید. گزینه اول عدم امکان ذخیره فایل‌ها، و گزینه دوم امکان ذخیره فایل‌های تعیین شده را فراهم می‌نماید. گزینه Active Screening را انتخاب کنید.



شکل ۹-۴۷

۶. تب‌های Email Message، Event Log، Command، و Report را مشاهده کنید. چنانچه با پیغامی مبنی

بر عدم پیکربندی SMTP مواجه شدید، بر روی Yse کلیک کنید. اطلاعات این تب‌ها مشابه قسمت Quota می‌باشد فقط محتویات پیغام‌ها تغییر کرده است.

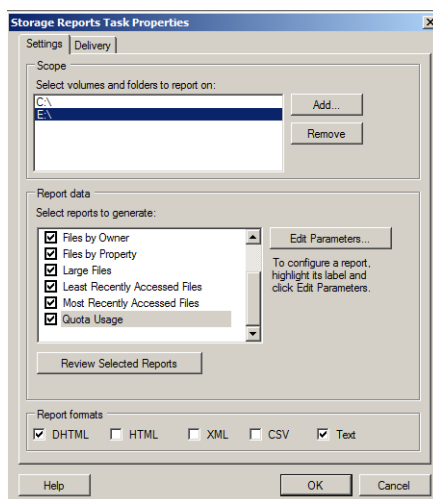
۷. بر روی OK کلیک کنید.

### ۹-۵-۴ ایجاد گزارش‌ها

در سرویس FSRM انواع مختلفی از گزارش‌ها وجود دارد که می‌توان آنها را به عنوان بخشی از Quota policy یا File Screen ایجاد نمود. با نگاهی ساده به نام گزارش، می‌توانید آنها را مورد شناسایی قرار داده و از عملکرد آنها آگاهی پیدا کنید. انواع گزارشهای موجود عبارتند از: Duplicate Files، File Screening Audit، Files by File Group، Files by Owner، Files by Property، Large Files، Least Recently Accessed Files، Recently Accessed Files، Most Recently Accessed Files، و Quota Usage. گزارش‌ها را می‌توان در فرمت‌های گوناگونی مانند DHTML، HTML، XML، CSV، و TXT ذخیره نمود.

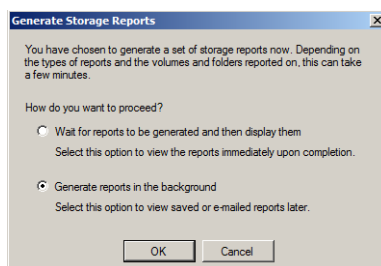
برای دسترسی به گزارش‌ها مراحل زیر را دنبال کنید:

۱. در کنسول Server Manager، به گره File Server Resource Manager حرکت نموده و زیرگره Storage Reports Management را انتخاب کنید. بر روی آن کلیک راست نموده و گزینه Generate Reports Now را کلیک کنید.
۲. در پنجره "Storage Reports Task Properties" بر روی دکمه Add کلیک کنید.
۳. درایو یا پوشه (یا تعدادی از آنها) که قصد ایجاد گزارش از آن دارید را انتخاب نموده و بر روی OK کلیک کنید.



شکل ۹-۴۸

۴. در قسمت Select reports to generate نوع گزارش را تعیین کنید. البته امکان انتخاب همه موارد بطور همزمان نیز وجود دارد اما ایجاد گزارش از آنها کاری زمان‌گیر خواهد بود. برخی از این گزارش‌ها شامل آپشن‌هایی هستند که باید تنظیم شوند. به عنوان مثال برای Quota Usage می‌توانید دکمه Edit Parameters را کلیک نموده و حداقل استفاده از Quota (به درصد) را تعیین کنید.
۵. پس از انتخاب نوع گزارش‌ها، از قسمت Report formats فرمت ذخیره‌سازی آنها را نیز تعیین نموده و بر روی OK کلیک کنید.
۶. جهت دریافت گزارش از طریق ایمیل می‌توانید به تب Delivery رفته و پس از فعال‌سازی گزینه Send reports to the following administrators، آدرس ایمیل مدیرانی که این گزارش‌ها را باید دریافت کنند وارد نمایید. پس از انجام تنظیمات بر روی OK کلیک کنید.
۷. در پنجره “Generate Storage Reports” گزینه Generate Reports in the Background را انتخاب نموده و بر روی OK کلیک کنید.



شکل ۹-۴۹

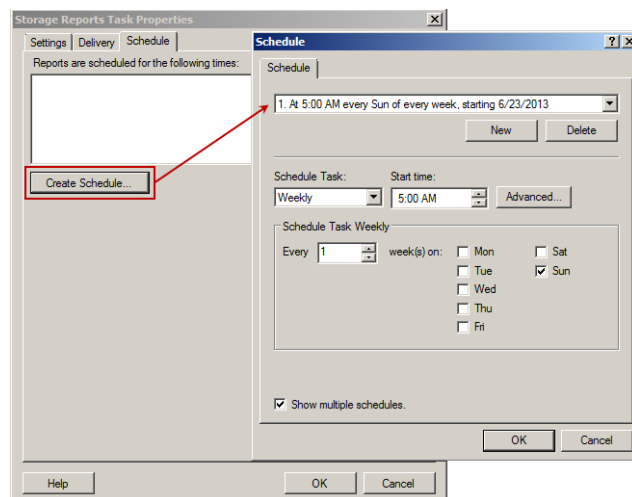
با توجه به نوع گزارش‌ها و تعداد پوشه‌هایی که انتخاب نمودید، ایجاد گزارش چند دقیقه طول خواهد کشید.

### ایجاد گزارش زمان‌بندی شده

برای ایجاد یک گزارش زمان‌بندی شده مراحل زیر را دنبال کنید:

۱. بر روی Storage Reports Management کلیک راست نموده و Schedule a New Report Task را انتخاب کنید.
۲. در پنجره “Storage Reports Task Properties” بر روی دکمه Add کلیک کنید. درایو یا پوشه مورد نظر را انتخاب نموده و بر روی OK کلیک کنید.
۳. نوع گزارش‌ها و فرمت ذخیره‌سازی آنها را تعیین کنید.
۴. تب Schedule را انتخاب نموده و بر روی دکمه Create Schedule کلیک کنید.

۵. در پنجره "Schedule" بر روی دکمه New کلیک کنید.
۶. با استفاده از آپشن‌های موجود، نوع زمان‌بندی برای ایجاد گزارش را مشخص نموده و بر روی OK کلیک کنید.



شکل ۹-۵۰

۷. گزارشی که ایجاد می‌کنید در مسیر `%systemdrive%\StorageReports\Interactive` قرار دارد. پس از باز کردن فایل‌های HTML، TXT و یا هر فایل‌ای که ایجاد نموده‌اید می‌توانید گزارش‌های ایجاد شده را مشاهده کنید.

#### ۵-۵-۹ آپشن‌های File Server Resource Manager

امکان ایجاد تغییر در آپشن‌های FSRM وجود دارد. برای دسترسی به این آپشن‌ها می‌توانید بر روی گره File Server Resource Manager در Server Manager کلیک راست نموده و Configure Options را انتخاب کنید. پنجره "File Server Resource Manager" دارای تعدادی تب می‌باشد که بطور مختصر آنها را معرفی می‌کنیم:

- ♦ **Email Notifications:** چنانچه بخواهید هشدارها و گزارش‌ها مربوط به فایل‌ها را از طریق ایمیل دریافت کنید، می‌توانید تنظیمات لازم را در این تب انجام دهید. این تنظیمات عبارتند از: آدرس IP یا نام سرور SMTP که ایمیل‌های ارسالی از سرور شما را دریافت می‌کند، و همچنین آدرس ایمیل مدیران.
- ♦ **Notification Limits:** در این تب می‌توانید تعیین کنید که پس از ارسال هشدارهای مربوط به



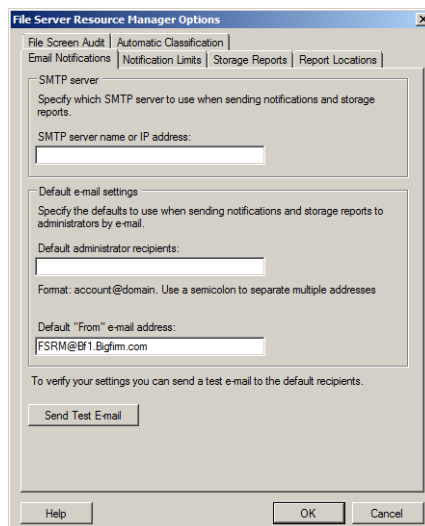
Quota یا File Screen، چه مدت طول می‌کشد تا مجدداً هشدار ارسال گردد. این زمان به دقیقه بوده و برای انواع هشدارها بطور پیش‌فرض با ۶۰ دقیقه تنظیم شده است.

- ♦ **Storage Reports:** در این تب تنظیمات مربوط به مقادیر مقادیر پیش‌فرض گزارش‌ها انجام می‌شود. برای تنظیم این مقادیر، پس از انتخاب نوع گزارش می‌توانید بر روی دکمه Edit Parameters کلیک کنید.

- ♦ **Report Locations:** در این تب تنظیمات مربوط به محل ذخیره‌سازی گزارش‌ها انجام می‌شود. با استفاده از دکمه Browse می‌توانید مسیر پیش‌فرض ذخیره گزارش‌ها را تغییر دهید.

- ♦ **File Screen Audit:** این تب تنها داری یک گزینه با نام Record file screening activity in an auditing database بوده که اگر انتخاب شود، اقدامات مربوط به فیلترکردن فایل‌ها در یک فایل پایگاه‌داده ثبت می‌شود.

- ♦ **Automatic Classification:** این تب تنظیمات مربوط به ایجاد گزارش‌ها را زمانی که مدیریت فایل‌ها، با استفاده از خصوصیات و قوانین طبقه‌بندی شده (Classification /Classification Properties) انجام می‌شود، فراهم می‌نماید.



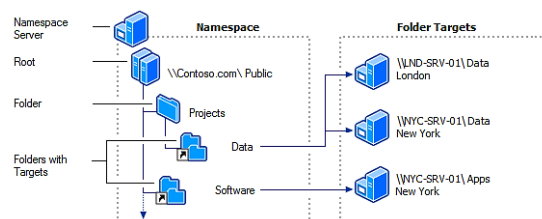
شکل ۹-۵۱

## ۹-۶ Distributed File System

DFS سرویسی است که با استفاده از آن می‌توانید یک Share که شامل کلیه فایل‌های اشتراک

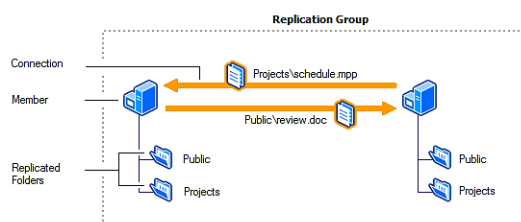
گذاشته شده در شبکه است ایجاد کنید. در واقع DFS یک محل برای نگهداری فایل‌های اشتراک‌گذاشته شده، به همراه یک صفحه “Links” است که کاربران را به یک سرور خاص یا سرورهایی که محل نگهداری فایل‌های اشتراک‌گذاشته هستند هدایت می‌کند. در ویندوز سرور 2008 از دو تکنولوژی جدید در این سرویس استفاده می‌شود:

- **DFS Namespaces:** فضاهای نام DFS، شما را قادر می‌سازند تا پوشه‌های اشتراک‌گذاشته بر روی سرورهای مختلف که در یک یا بیشتر از یک ساختار منطقی از فضای نام قرار گرفته‌اند گروه‌بندی کنید. هر فضای نام به صورت یک پوشه اشتراکی به همراه مجموعه‌ای از زیرپوشه‌ها برای کاربران نمایش داده می‌شود. این ساختار، دسترس‌پذیری را افزایش داده و کاربران را بطور خودکار به پوشه‌های اشتراک‌گذاشته شده در یک سایت Active Directory Domain Services زمانی که در دسترس باشند، متصل می‌نماید.



شکل ۹-۵۲

- **DFS Replication:** تکثیرهای DFS، پروسه‌ای است که با استفاده از آن می‌توانید پوشه‌ها را میان سرورهای مختلف در میان ارتباطات شبکه‌ای با پهنای باند محدود هماهنگ کنید. در واقع می‌توانید با استفاده از DFS Namespace پوشه‌های اشتراکی را ایجاد نموده و سپس به کمک DFS Replication آنها را میان سرورهای مختلف تکثیر کنید. این بدین معناست که ایجاد هرگونه تغییر می‌تواند طی پروسه Replication در میان سایر سرورها تکثیر شده و در نتیجه هماهنگی آنها را در پی خواهد داشت.



شکل ۹-۵۳

### ۹-۶-۱ آشنایی با اصطلاحات DFS

قبل از پرداختن به مبحث اصلی، لازم است با مجموعه‌ای از اصطلاحات به کار رفته در DFS آشنا شوید. در ادامه این اصطلاحات معرفی شده‌اند:

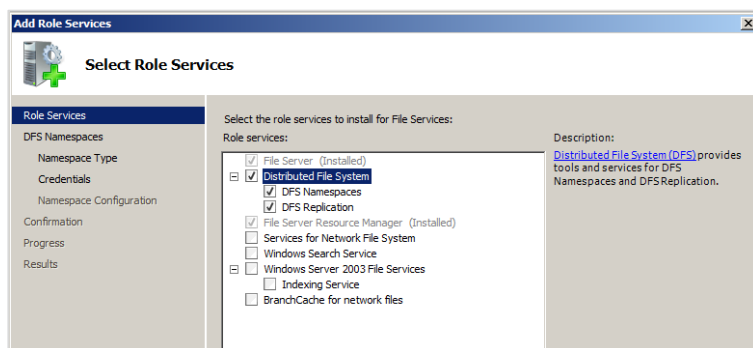
- ♦ **Root:** اصطلاح Root، تقریباً به اشتراک گذاری در شبکه گفته می‌شود. به عنوان مثال پوشه اشتراکی Apps را در نظر بگیرید. این پوشه یک Root به شمار رفته و همانند سایر Share ها در شبکه عمل می‌کند. Root ها می‌توانند شامل فایل‌ها و پوشه‌هایی اضافه نیز باشند.
- ♦ **DFS links:** DFS link ها، به اشتراک گذاری‌هایی در شبکه اطلاق می‌شود که در جایی دیگر قرار داشته ولی در زیر قسمت Root قرار می‌گیرند. لینک‌ها در DFS همانند ابر لینک‌ها<sup>۱</sup> در اینترنت عمل می‌کنند، بنابراین با استفاده از آنها می‌توان کاربران را به قسمت‌های مختلف از شبکه (که پوشه‌های اشتراکی در آن قرار دارند) هدایت نمود. شما به عنوان یک کاربر نیازی به دانستن اینکه لینک‌ها تا زمان باز شدن صفحه مورد نظر چه پروسه‌ای را طی می‌کنند نخواهید داشت. زمانی که به صفحه اصلی (DFS root) هدایت می‌شوید، با استفاده از DFS link ها می‌توانید به سایر Share ها دسترسی پیدا کنید.
- ♦ **Target or Replica:** این اصطلاح به یک Root یا Link اشاره می‌کند. اگر دو Share یکسان در شبکه که روی سرورهای مختلف قرار دارند داشته باشید، می‌توانید آنها را با استفاده از لینک یکسان به عنوان DFS Targets گروه‌بندی کنید.
- ♦ **Root Replica Member:** به هریک از Root های ورودی در جدول محتویات گفته می‌شود. زمانی که Target ها برای Replication (تکثیر) پیکربندی می‌شوند، سرویس File Replication محتویات Root ها را هماهنگ می‌سازد.

### ۹-۶-۲ نصب DFS

قبل از اینکه بتوانید از تکنولوژی‌های جدید DFS استفاده کنید، ابتدا باید سرویس آنرا به File Server اضافه نمایید. جهت افزودن DFS مراحل زیر را دنبال کنید:

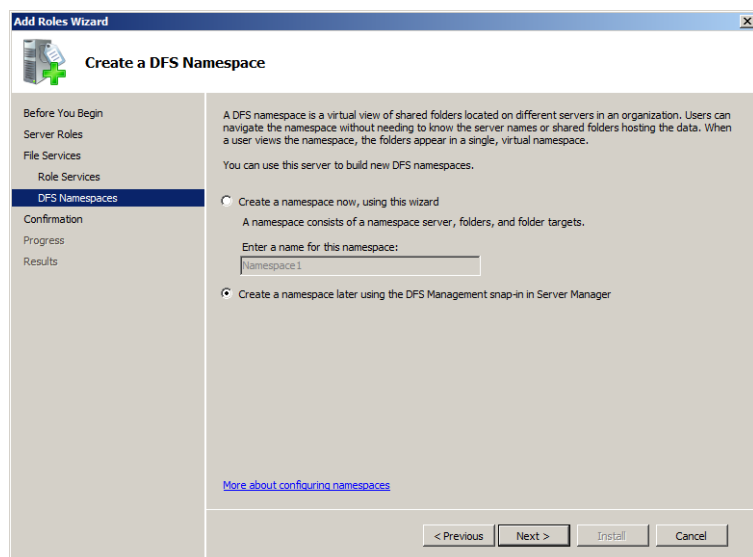
۱. Server Manager را اجرا نموده و به مسیر «Roles» File Services حرکت کنید.
۲. بر روی File Services کلیک راست نموده و گزینه Add Role Services را انتخاب کنید.
۳. در صفحه «Select Role Services» گزینه Distributed File System را به همراه زیرمجموعه‌های DFS Namespaces و DFS Replication انتخاب نموده و بر روی Next کلیک کنید.

1. Hyperlinks



شکل ۹-۵۴

۴. در صفحه “Create a DFS Namespace”، گزینه “Create a namespace later using the DFS management” را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۹-۵۵

۵. در صفحه “Confirm Installation Selections” خلاصه‌ای از تنظیمات را مشاهده نموده و بر روی Install کلیک کنید.

### ۹-۶-۳ ایجاد DFS Root

بطور کلی امکان ایجاد دو نوع Root وجود دارد: Domain Root و Stand-Alone Root. Root‌های نوع

Domain، خود را در اکتیو دایرکتوری منتشر می‌کنند در حالی که Root های Stand-Alone قادر به انجام چنین کاری نیستند. توجه داشته باشید که Domain Root ها بر روی DC ها قرار می‌گیرند بنابراین برای عملکرد آنها از Active Directory استفاده می‌شود. یکی از مزایای مهم منتشر شدن Root در اکتیو دایرکتوری این است که Domain Root ها می‌توانند Root های المثنی داشته باشند. Root المثنی اجازه می‌دهد که هر DC در دامنه از Root نگهداری کند، در نتیجه تا حد زیادی تحمل خطا بهبود پیدا می‌کند. از آنجایی که Root های المثنی به اکتیو دایرکتوری نیاز دارند، Stand-Alone Root ها نمی‌توانند و نباید المثنی داشته باشند.

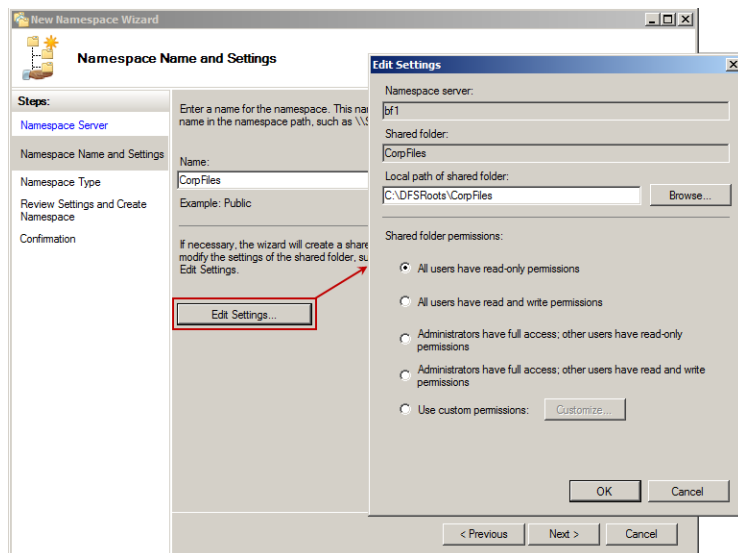
جهت ایجاد DFS Root مراحل زیر را دنبال کنید:

۱. از مسیر Start » Administrative Tools، کنسول DFS Management را اجرا کنید.
۲. در پنل سمت راست، بر روی Namespaces کلیک راست نموده و گزینه New Namespace را انتخاب کنید. ویزارد "Namespace Server Wizard" اجرا می‌گردد.
۳. در صفحه "Namespace Server"، نام سروری که Namespace را نگهداری می‌کند وارد نموده و بر روی Next کلیک کنید (در اینجا از سروری به نام Server2008-02 که یک سرور Stand-Alone است استفاده شده است).



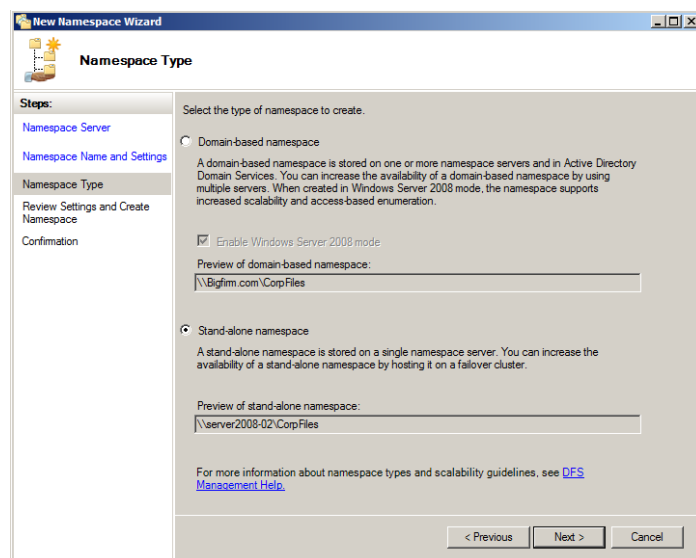
شکل ۹-۵۶

۴. در صفحه "Namespace Name and Settings" نام Namespace را تعیین کنید. این نام پس از نام سرور نمایش داده می‌شود و به عنوان نام مجموعه فایل‌ها و پوشه‌های اضافه شده به Namespace استفاده می‌گردد. به عنوان مثال چنانچه یک Namespace با نام CorpFiles بر روی سرور Server2008-02 ایجاد می‌کنید، می‌توانید جهت دسترسی به پوشه‌های اشتراکی این سرور، آنها را در مسیر //Server2008-02/CorpFiles/Folder نام قرار دهید تا سایر افراد بتوانند به آن دسترسی پیدا کنند. با استفاده از دکمه Edit Settings نیز می‌توانید تنظیماتی مانند محل قرار گیری Namespace و مجوزهای دسترسی به آن را انجام دهید. بر روی Next کلیک کنید.



شکل ۹-۵۷

۵. در صفحه “Namespace Type”، نوع Namespace مشخص کنید. در این صفحه، انتخاب شما یکی از گزینه‌های Domain-Based Namespace یا Stand-Alone Namespace خواهد بود. Domain-Based Namespace به شما اجازه می‌دهد که Namespace را بر روی یک یا بیشتر از یک سرور ذخیره کنید در حالی که Stand-Alone Namespace تنها اجازه ذخیره Namespace بر روی یک سرور را فراهم می‌نماید. ما در اینجا از Stand-Alone Namespace استفاده می‌کنیم.

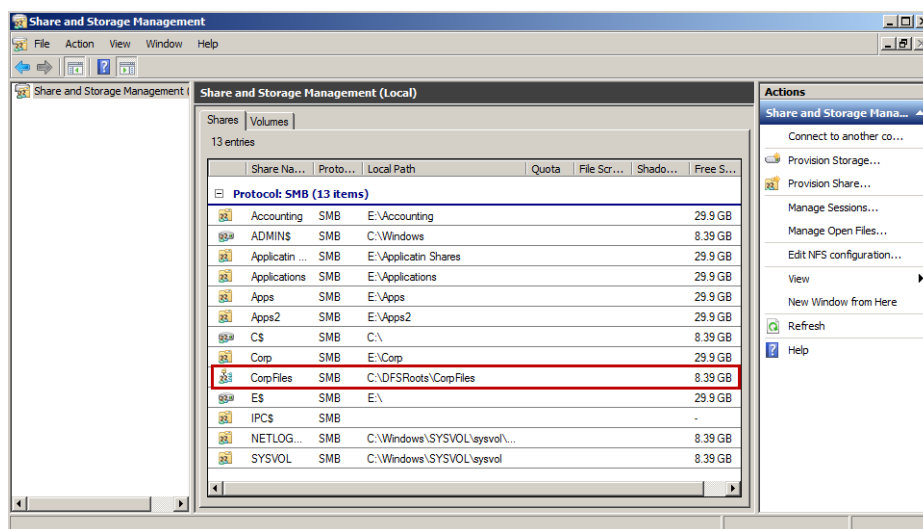


شکل ۹-۵۸

۶. در صفحه “Review Settings and Create Namespaces” خلاصه‌ای از تنظیمات را مشاهده نموده و بر روی Create کلیک کنید.

۷. فرایند ایجاد Namespace ممکن است مدتی طول بکشد، پس تا اتمام آن منتظر بمانید. با ایجاد Namespace، روشی برای در اختیار داشتن فایل‌ها و پوشه‌های اشتراک گذاشته شده در سراسر محیط سرور، به همراه یک نام برای دسترسی آسان به آنها خواهید داشت.

در کنسول Share and Storage Management می‌توانید پوشه (یا همان Namespace) CorpFiles ایجاد نمودید را مشاهده کنید. مسیر قرارگیری این پوشه C:\DFSRoots\CorpFiles می‌باشد و فضای پیش‌فرض آن نیز در مثال ما برابر با ۸.۳۹GB است.



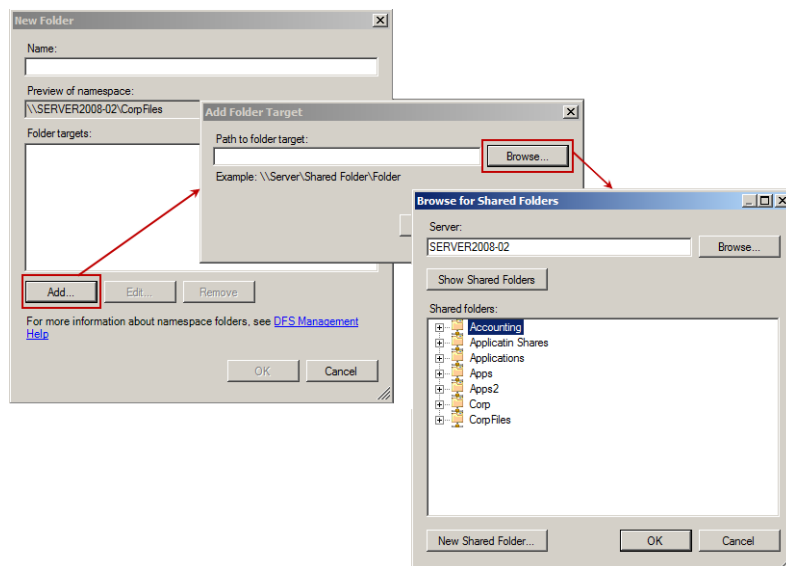
شکل ۹-۵۹

## ۹-۶-۴ افزودن لینک‌ها به DFS Root

در زیر Root Share که ایجاد نمودید، می‌توانید Linkها یا همان فایل‌ها و پوشه‌ها را اضافه کنید. انجام این کار را با مثال قبل دنبال می‌کنیم:

۱. در کنسول DFS Management بر روی فضای نام CorpFiles کلیک راست نموده و New Folder را انتخاب کنید.

۲. در پنجره “New Folder”، بر روی Add و سپس بر روی Browse کلیک کنید. لیستی از پوشه‌های اشتراک گذاشته شده نمایش داده می‌شود. پوشه مورد نظر (در اینجا Accounting) را انتخاب نموده و بر روی OK کلیک کنید.



شکل ۹-۶۰

۳. در قسمت Name از پنجره "New Folder" نام پوشه را وارد نموده و بر روی OK کلیک کنید.
۴. جهت افزودن Targetها به پوشه‌ای که ایجاد نمودید می‌توانید بر روی آن کلیک‌راست نموده و Add Folder Target را انتخاب کنید.

دقت داشته باشید که DFS فایل اشتراکی ایجاد نمی‌کند بنابراین باید ابتدا فایل‌ها و پوشه‌های اشتراکی را بر روی سرورهای مختلف ایجاد نموده و سپس با استفاده از DFS آنها را در یک محل مشترک قرار دهید. در واقع با این کار یک فهرست محتویات برای اشاره به این فایل‌ها ایجاد می‌کنید. استفاده از DFS در اکتیو دایرکتوری، یک مزیت قابل توجه دارد؛ زمانی که پوشه‌های اشتراک گذاشته شده در سرورهای فیزیکی مختلف، در اکتیو دایرکتوری ذخیره می‌شوند، چون AD بین DCهای مختلف نگهداری می‌شود، اگر هر کدام از سرورهایی که Rootها را نگهداری می‌کنند با مشکلی مواجه شوند، کاربران بطور خودکار و بدون حتی یک وقفه به محل دیگری برای بازیابی اطلاعات Root هدایت می‌شوند.

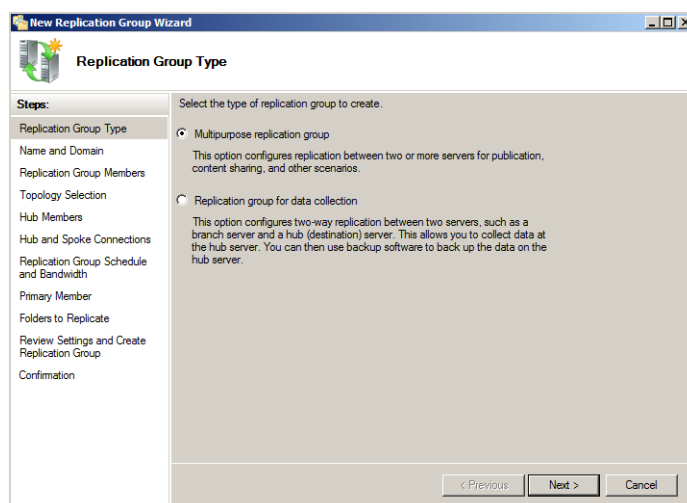
### ۹-۶-۵ پیکربندی DFS Replications

تا اینجا توانستید DFS را راه‌اندازی نموده و پس از ایجاد Namespaceها، Fileها و پوشه‌های اشتراکی را متمرکز کنید. اما حفاظت از این فایل‌ها و پوشه‌های اشتراک گذاشته شده و داده‌های آنها در مواقع وقوع خطاها چگونه امکان‌پذیر است؟ این کار با استفاده از قسمت Replication در پنجره



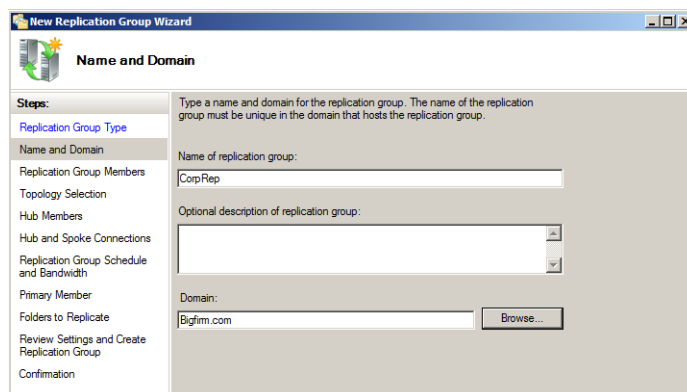
DFS Management قابل انجام می‌باشد. مراحل زیر نحوه انجام کار را نشان می‌دهند:

۱. بر روی گروه Replication کلیک‌راست نموده و New Replication Group را انتخاب کنید.
۲. در صفحه "Replication Group Type" دو انتخاب در اختیار خواهید داشت: Multipurpose Replication group و replication group for data collection. گزینه اول امکان پیکربندی Replication میان دو یا چندین سرور، و گزینه دوم امکان Backup گیری و جمع‌آوری داده‌ها بر روی سرور اصلی که Hub Server شناخته می‌شود (زمانی که یک سرور دیگر \_Branch Server\_ نیز به عنوان شعبه‌ای از سازمان وجود داشته باشد) فراهم می‌کند. در اینجا گزینه اول را انتخاب نموده و بر روی Next کلیک کنید.



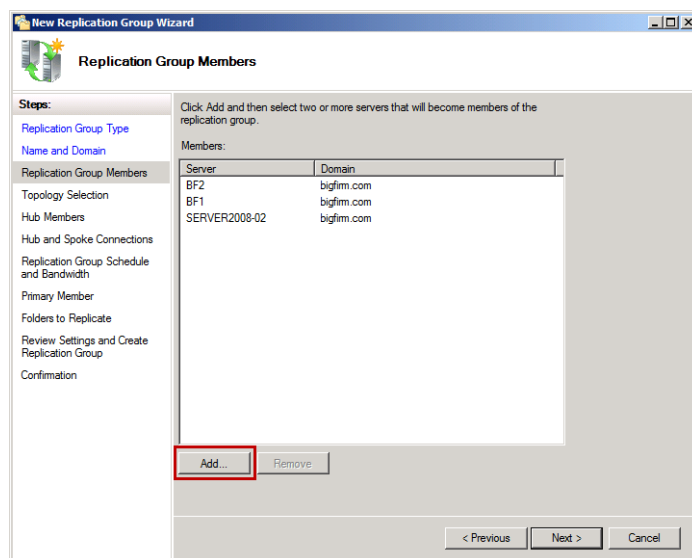
شکل ۹-۶۱

۳. در صفحه بعد نام گروه Replication را وارد نموده (در اینجا CorpRep) و بر روی Next کلیک کنید.



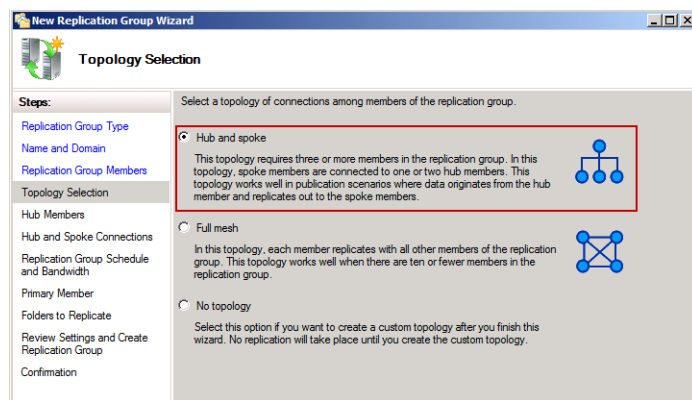
شکل ۹-۶۲

۴. در صفحه “Replicatin Group Members”، با استفاده از دکمه Add می‌توانید سرورهایی که قرار است Replication میان آنها انجام شود را به گروه اضافه کنید. دقت داشته باشید که باید حداقل دو سرور به گروه اضافه شوند.



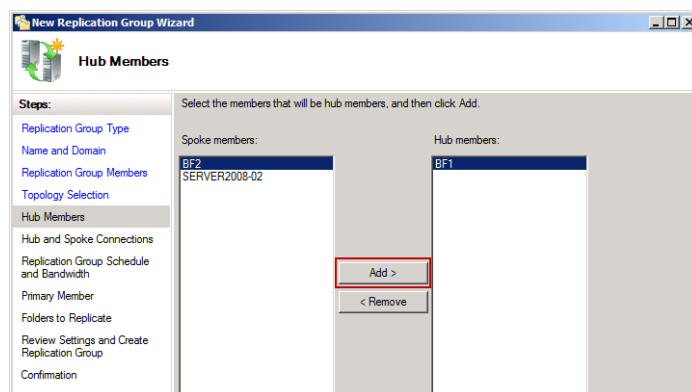
شکل ۹-۶۳

۵. در صفحه “Topology Selection” نوع توپولوژی که اعضاء گروه Replication در آن قرار گرفته‌اند را تعیین کنید. این توپولوژی در واقع نحوه ارتباط اعضاء با یکدیگر را مشخص می‌کند. در اینجا از توپولوژی Hub and Spoke استفاده شده است که در آن می‌توان سرور (سرورهایی) را به عنوان سرور اصلی (Hub) و سرورهایی را به عنوان سرورهایی که به Hub متصل هستند (Spoke) تعیین نمود. پس از انتخاب توپولوژی، بر روی Next کلیک کنید.



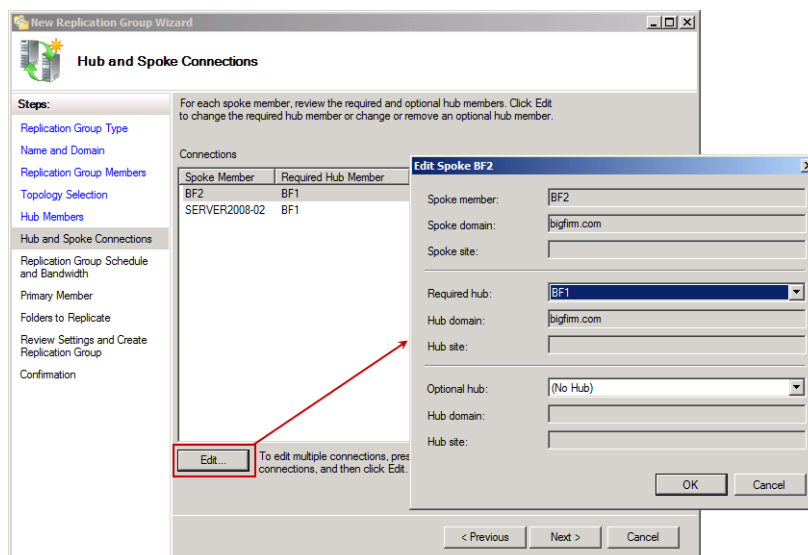
شکل ۹-۶۴

۶. در صفحه "Hub Members" لیست تمام سرورها نشان داده می‌شود. از این لیست می‌توانید تعدادی را انتخاب نموده و با کلیک بر روی دکمه Add به فهرست سرورهای Hub اضافه کنید. آن دسته از سرورهایی که در این لیست باقی می‌مانند به عنوان سرورهای Spoke در نظر گرفته می‌شوند. پس از افزودن سرور (ها) به لیست، بر روی Next کلیک کنید.



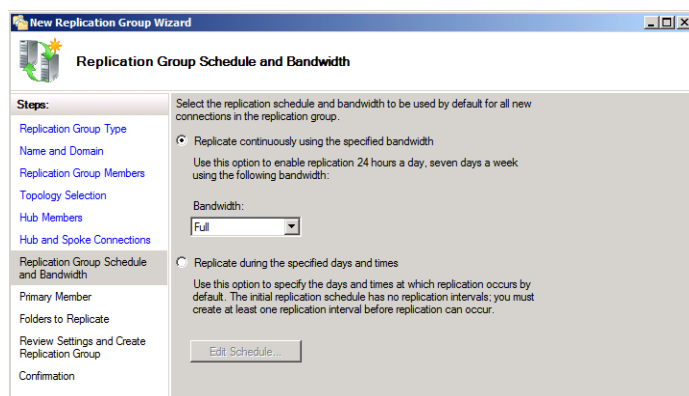
شکل ۹-۶۵

۷. در صفحه "Hub and Spoke Connections" می‌توانید پس از انتخاب سرورهای Spoke، بر روی دکمه Edit کلیک نموده تا در صورت نیاز، تنظیمات Hub را برای آنها تغییر دهید. بر روی Next کلیک کنید.



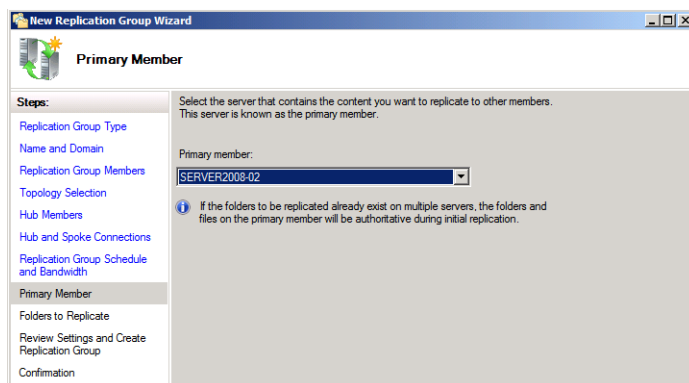
شکل ۹-۶۶

۸. در صفحه “Replication Group Scheduled and Bandwidth” دو گزینه قابل انتخاب است. گزینه Replicated continuously using the specified bandwidth امکان انتخاب پهنای باند استفاده شده در ارتباط را به صورت ثابت، و گزینه Replicated during the specified days and times امکان تنظیم پهنای باندی متغیر به ازای روزهای هفته را فراهم می‌نماید. گزینه اول را انتخاب نموده و پهنای باند لازم را برای آنرا تنظیم کنید (در اینجا Full). سپس بر روی Next کلیک کنید.



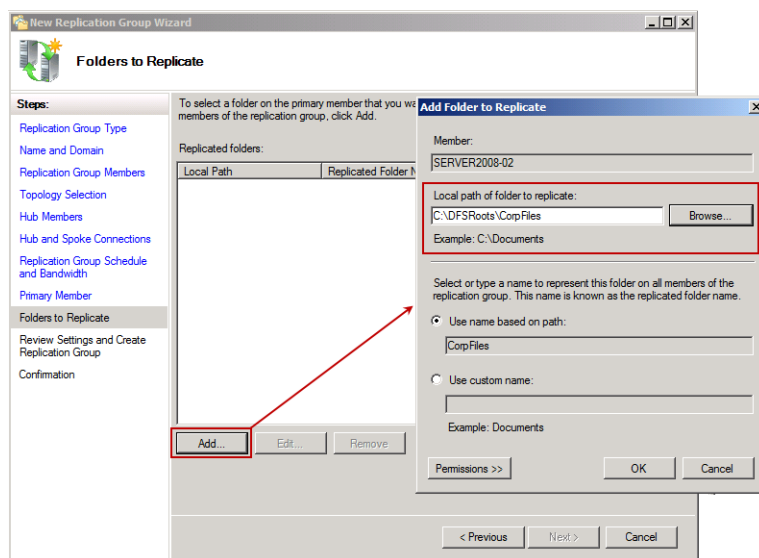
شکل ۹-۶۷

۹. در صفحه “Primary Member” سرور اصلی در ارتباط Replication (سروری که پوشه‌های اشتراکی اصلی بر روی آن قرار دارد) را تعیین نموده و بر روی Next کلیک کنید.



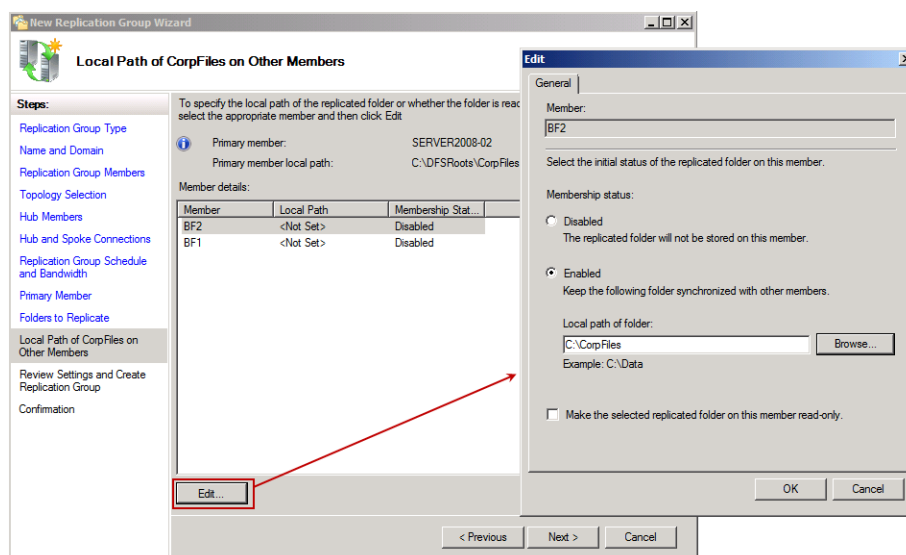
شکل ۹-۶۸

۱۰. در صفحه “Folders to Replicate” با استفاده از دکمه Add، پوشه‌هایی که قرار است طی فرایند Replication میان سرورها تکثیر شود را تعیین نموده و در نهایت بر روی Next کلیک کنید (در اینجا پوشه CorpFiles انتخاب شده است).



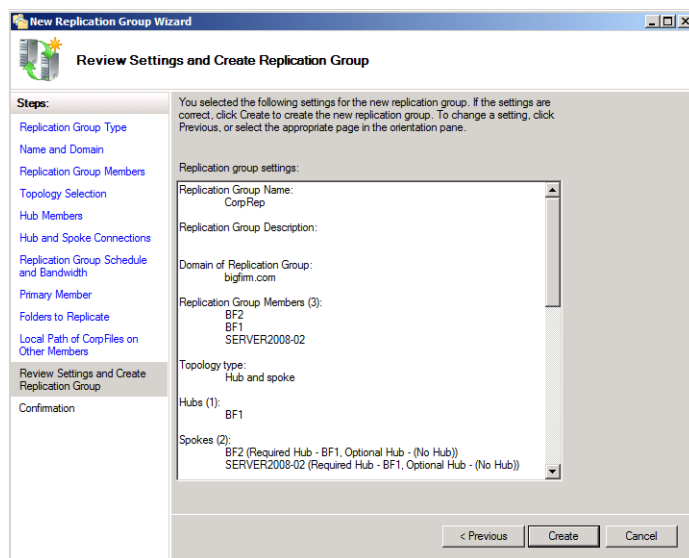
شکل ۹-۶۹

۱۱. در صفحه “Local Path of CorpFiles on Other Members” باید محل قرارگیری پوشه CorpFiles که توسط سرور اصلی به اشتراک گذاشته شده است را بر روی سایر سرورها تعیین کنید. با انتخاب هر سرور و کلیک بر روی دکمه Add، پوشه‌ای را جهت نگهداری محتویات پوشه اشتراکی اصلی تعیین نموده و بر روی OK کلیک کنید. در نهایت بر روی Next کلیک کنید.



شکل ۹-۷۰

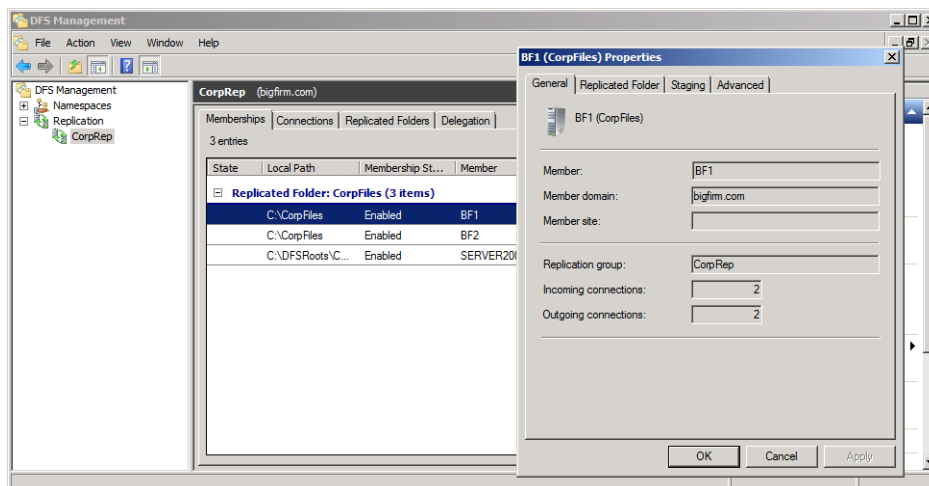
۱۲. در صفحه “Review Settings and Create Replication Group” خلاصه‌ای از تنظیمات را مشاهده نموده و بر روی Create کلیک کنید.



شکل ۹-۷۱

۱۳. پس از اتمام عملیات، در صفحه “Confirmation” بر روی Close کلیک کنید.

۱۴. با مراجعه به کنسول DFS Management و حرکت به گره Replication، می‌توانید Replication ایجاد شده را مشاهده کنید. برای مشاهده و یا تغییر تنظیمات هر یک از سرورها (در صورت امکان) کافی است بر روی آن کلیک‌راست نموده و Properties را انتخاب کنید.



شکل ۹-۷۲

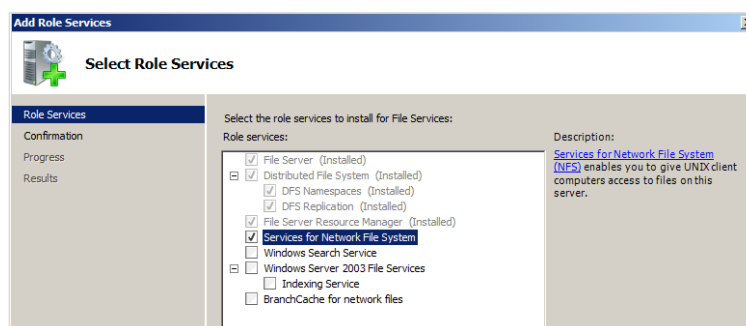
## ۷-۹ سرویس Network File System

سرویس NFS زمانی استفاده می‌شود که قصد داشته باشید فایل‌ها و پوشه‌ها را میان سیستم‌های ویندوز و سایر سیستم‌ها مانند Mac OS، لینوکس، یونیکس و ... به اشتراک گذارید. همانطور که می‌دانید، فایل‌های استفاده شده در سیستم‌های لینوکس و ویندوز با یکدیگر متفاوت هستند بنابراین اگر فایلی در یک سیستم با سیستم عامل ویندوز به اشتراک گذاشته شود و در سیستمی که دارای سیستم عامل لینوکس است بخواند استفاده شود، باید راهکارهایی برای انجام این کار فراهم گردد. سرویس NFS این وظیفه را در طی شبکه ایفا نموده و اشتراک گذاری فایل‌ها میان این سیستم‌ها را امکان‌پذیر می‌نماید.

### ۷-۹-۱ نصب NFS

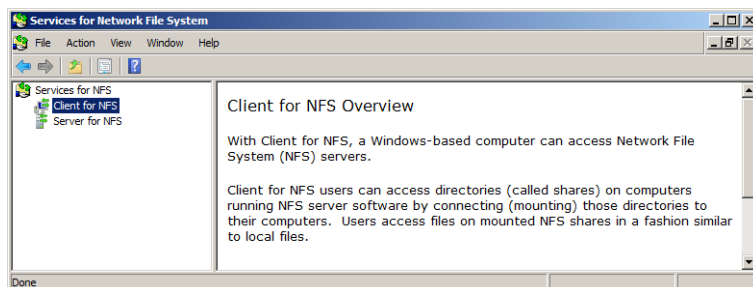
NFS یکی از Role Service‌هایی است که به File Server Role اضافه می‌گردد. بنابراین همانند نصب DFS لازم است از طریق کنسول Server Manager نسبت به افزودن آن اقدام کنید:

۱. در کنسول Server Manager، به مسیر «Roles» File Services حرکت کنید.
۲. بروی File Services کلیک راست نموده و «Add Role Services» را انتخاب کنید.
۳. در صفحه «Select Role Services»، گزینه «Services for Network File System» را انتخاب نموده و بروی «Next» کلیک کنید.



شکل ۷۳-۹

۴. در صفحه «Confirm Installation Selections» بروی «Install» کلیک کنید.
۵. از مسیر «Start» «Administrative Tools» «Services for Network File System» می‌توانید به کنسول NFS دسترسی پیدا کنید.

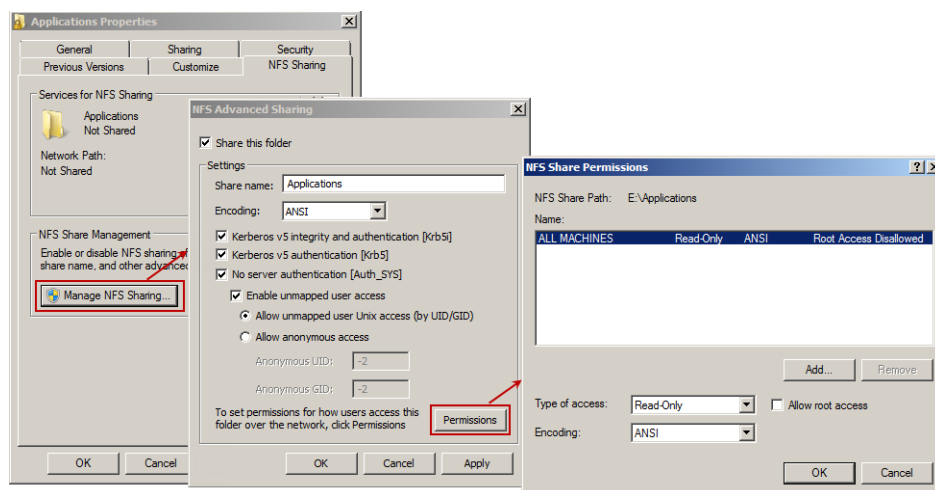


شکل ۷۴-۹

### ۲-۷-۹ پیکربندی احراز هویت NFS و ایجاد NFS Share

برای اینکه یک پوشه اشتراک گذاشته شده بتواند میان سایر سیستم‌ها استفاده گردد باید توسط NFS به اشتراک گذاشته شود. بدین منظور می‌توانید مراحل زیر را دنبال کنید:

۱. بر روی کامپیوتری که به عنوان سرور NFS استفاده می‌شود، پوشه‌ای ایجاد کنید.
۲. بر روی پوشه کلیک‌راست نموده و Properties را انتخاب کنید.
۳. تب NFS Sharing را انتخاب نموده و بر روی دکمه Manage NFS Sharing کلیک کنید.
۴. در پنجره "NFS Advanced Sharing"، گزینه Share this folder را فعال کنید.
۵. به کمک آپشن‌های موجود، تنظیمات مربوط به اشتراک‌گذاری NFS را برای این پوشه انجام دهید.
۶. با استفاده از دکمه Permissions مجوزهای لازم برای دسترسی به این پوشه را تعیین کنید.
۷. بر روی کلیه OK‌ها کلیک نموده و پنجره‌ها را ببندید.



شکل ۷۵-۹





## « فصل ۱۰ »

اشتراک‌گذاری پرینتر و ایجاد

**Print Server**

**Sharing Printer and Setup**

**Print Server**



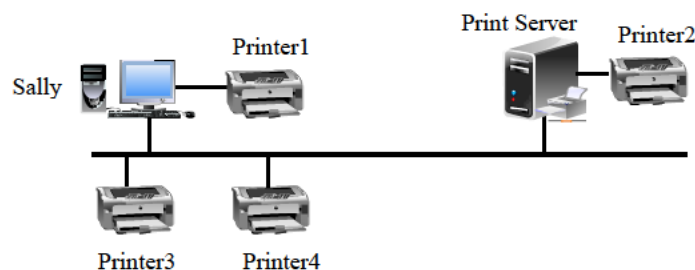
اشتراک‌گذاری پرینتر تکنیکی است که بوسیله آن می‌توان امکان استفاده از پرینترها را در اختیار کاربران شبکه قرار داد بدون اینکه نیاز به فراهم کردن تعداد زیادی پرینتر در شبکه باشد. فرض کنید در شرکتی با ۵۰۰۰ کامپیوتر قرار است امکان استفاده از پرینتر فراهم شود. در این حالت، چنانچه بخواهید به ازای هر کامپیوتر یک پرینتر خریداری کنید به ۵۰۰۰ پرینتر نیاز خواهید داشت. مسلماً اجرای این طرح ایده مناسبی نخواهد بود زیرا هزینه‌های بسیاری صرف آن خواهد شد. اکنون حالتی را در نظر بگیرید که به ازای تعداد مشخصی از افراد، مثلاً ۵، ۱۰ یا ۲۰ نفر، یک دستگاه پرینتر خریداری نموده و در اختیار آنها قرار می‌دهید. این کار نه تنها هزینه خرید پرینترها را کاهش می‌دهد بلکه در مصرف برق و نگهداری از آنها نیز صرفه‌جویی خواهد شد.

اشتراک‌گذاری تعداد زیادی پرینتر در یک شبکه، نیازمند مدیریتی مؤثر و کارآمد است. روش ارائه شده برای پاسخگویی به این وضعیت، استفاده از Print Server یا همان سرور چاپ است. در ویندوز سرور 2008R2 امکان ایجاد Print Server با استفاده از Print and Document Services Role فراهم شده است. با استفاده از این Role، یک کنسول مدیریتی به نام Print Management در اختیار خواهید داشت که به کمک آن می‌توانید وظایف انجام شده توسط پرینترهای شبکه و همچنین در صورت نیاز، چندین Print Server را از یک نقطه مرکزی مدیریت کنید. در این فصل قصد داریم به نحوه ایجاد و مدیریت Print Server بپردازیم، بنابراین مهمترین مباحث مورد بررسی به شرح زیر خواهد بود:

- افزودن Print and Document Services Role
- مدیریت پرینترها با استفاده از کنسول Print Management
- مدیریت تنظیمات پرینترها و Print Server

### ۱-۱۰ نگاهی بر سرویس‌های چاپ

قبل از اینکه وارد بحث راه‌اندازی Print Server شویم، اجازه دهید به روش‌های استفاده از پرینترها در شبکه بپردازیم. فرض کنید در کل سازمان چهار پرینتر با نام‌های Printer1، Printer2، Printer3 و Printer4 در اختیار دارید که طبق شکل ۱-۱۰ در شبکه قرار گرفته‌اند.



شکل ۱-۱۰

در شکل بالا Printer1 با استفاده از پورت USB به کامپیوتر کاربری به نام Sally متصل شده است. این پرینتر، یک پرینتر شبکه محسوب نمی‌شود مگر اینکه توسط Sally به اشتراک گذاشته شود. در این وضعیت کامپیوتر Sally حتی اگر از یک سیستم عامل سمت کاربر مانند ویندوز ۷ هم استفاده کند باز به عنوان یک Print Server در نظر گرفته می‌شود (دقت داشته باشید که این پرینتر نمی‌تواند توسط Print server تعیین شده در شبکه اشتراک گذاشته شود).

Printer2 مستقیماً به Print Server متصل است بنابراین به عنوان پرینتر شبکه در نظر گرفته می‌شود. از آنجایی که Printer3 و Printer4 بطور مستقیم به شبکه متصل هستند، بنابراین آنها به عنوان پرینتر شبکه در نظر گرفته می‌شوند. نکته قابل ذکر این است که این دو پرینتر حتماً باید مجهز به کارت شبکه (NIC) باشند تا بتوانند با استفاده از آدرس IP در شبکه شناخته شوند.

اما در مورد Print Server نیز باید گفت زمانی که با استفاده از ویندوز سرور 2008 R2 Print and Document Services را نصب و پیکربندی می‌کنید، در واقع آنرا به یک Print Server تبدیل نموده‌اید.

#### ۱-۱-۱۰ Print Spooler

کامپیوترها دارای سرعت بیشتری نسبت به پرینترها هستند، بنابراین زمانی که چندین کامپیوتر بطور همزمان درخواست‌های خود را به پرینترها می‌فرستند، به دلیل اینکه پرینترها نمی‌توانند با سرعت بالا (مانند کامپیوتر) آنها را پردازش و چاپ کنند، هر کامپیوتر باید مدت زمانی منتظر بماند. Print Spooler به منظور پاسخگویی به این مشکل توسعه داده شده است. زمانی که کاربران درخواست‌های چاپ را به پرینتر می‌فرستند، سرویس Print Spooler آنها را دریافت نموده و در هارد درایو کامپیوتر (سرور) ذخیره می‌کند. سپس به ترتیب این درخواست‌ها را به پرینتر فرستاده و آنها را چاپ می‌کند. در طی این عملیات ممکن است بعضی از کاربران پس از ارسال درخواست خود مدت زیادی منتظر بمانند زیرا تا اتمام انجام یک درخواست، پردازش درخواست بعدی امکان‌پذیر نمی‌باشد. در صورت استفاده از Print Server، دو Spooler درگیر خواهند شد. ابتدا درخواست چاپ توسط Spooler موجود در کامپیوتر کاربر دریافت شده و در حافظه ذخیره می‌شود. سپس این درخواست به Spooler موجود در Print Server فرستاده شده و در Spooler آن قرار می‌گیرد. در این مدت ممکن است Print Server در حال پرداختن به سایر درخواست‌ها باشد. معمولاً درخواست‌های رسیده به سرور بر روی هارد درایو آن ذخیره می‌شوند. مسیر پیش‌فرض ذخیره این درخواست‌ها C:\Windows\System32\Spool\Printers می‌باشد.

#### ۲-۱-۱۰ درایور پرینتر

درایور پرینتر نرم افزاری است که سیستم عامل را قادر می‌سازد تا با دستگاه پرینتر تعامل داشته

باشد و نهایتاً امکان ارسال درخواست‌ها به پرینتر را فراهم می‌کند. سه دسته اصلی از درایورهای پرینتر که در ویندوز سرور 2008R2 آورده شده عبارتند از: x64، x86 و هر سه دسته دارای نوع Type 3 – User Mode هستند به این معنا که تنها در حالت کاربر اجرا شده و از سیستم عامل جدا هستند. تا قبل از ویندوز 2000 نوعی از درایورها به نام version 2 Kernel mode استفاده می‌شدند که این درایورها با هسته سیستم عامل تعامل داشتند. بنابراین چنانچه مشکلی در درایور رخ می‌داد سیستم را تحت تاثیر قرار داده و در مواردی موجب هنگ کردن<sup>۱</sup> سیستم می‌شد. درایورهای Itanium یک معماری ویژه ۶۴ بیتی هستند که در سرورها مورد استفاده قرار می‌گیرند. درایورهای x64 و x86 نیز به ترتیب نشان دهنده معماری‌های ۶۴ بیتی (برای سیستم عامل ۶۴ بیتی) و ۳۲ بیتی (برای سیستم عامل ۳۲ بیتی) می‌باشند. زمانی که یک کاربر به سرور متصل می‌شود، با توجه به نوع سیستم عامل بطور خودکار درایور را دریافت نموده و مورد استفاده قرار می‌دهد. البته قبل از آن باید از وجود این درایورها بر روی سیستم اطمینان حاصل شود.

## ۱۰-۲ نصب Print and Document Services Role

برای اینکه سرور خود را به Print Server تبدیل کنید، باید Print and Document Services Role را نصب نمایید. در زمان نصب، به همراه این Role مجموعه‌ای از سرویس‌ها نیز قابل نصب می‌باشند. این سرویس‌ها عبارتند از:

- ♦ **Print Server:** سرویس Print Server شامل کنسول Print Management است که از طریق آن می‌توانید بسیاری از اقدامات مدیریتی را بر روی Print Server انجام دهید. با استفاده از این کنسول امکان مدیریت چندین پرینتر و حتی چندین Print Server فراهم می‌گردد. این سرویس، اصلی‌ترین سرویسی است که در این فصل مورد بررسی قرار می‌گیرد.
- ♦ **LPD Service:** چنانچه سازمان شما دارای کامپیوترهای مبتنی بر لینوکس و یا کامپیوترهایی که از سرویس LPR<sup>۲</sup> استفاده می‌کنند بوده، و این کامپیوترها نیازمند استفاده از Print Server (مبتنی بر ویندوز) باشند از این سرویس استفاده می‌شود.
- ♦ **Internet Printing: IPP:** به کاربران اجازه می‌دهد که با استفاده از مرورگرهای وب به پرینترهای اشتراک گذاشته شده در سرور متصل شده و از آنها استفاده نمایند. نصب این سرویس همچنین یک وبسایت ایجاد نموده که در آنجا کاربران می‌توانند درخواست‌های چاپ را مدیریت کنند.

---

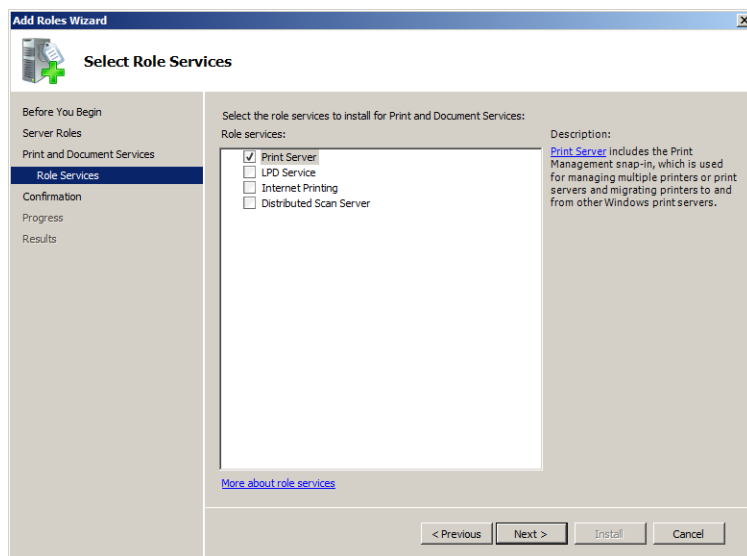
1. Crashing  
 2. Line Printer Daemon Service  
 3. Line Printer Remote  
 4. Internet Printing Protocol

- ♦ **Distributed Scan Server**: این سرویس، اسناد اسکن شده توسط اسکنرهای شبکه را دریافت نموده و آنها را به مقصد مورد نظر هدایت می‌کند. زمانی که این سرویس را اضافه می‌کنید، کنسولی به نام Scan Management نیز اضافه می‌گردد.

### ۱۰-۲-۱ افزودن Print and Document Services Role

نصب Print and Document Services با استفاده از Server Manager بسیار ساده است. تنها انتخاب شما در زمان نصب این است که چه سرویسی برای نصب شدن به همراه این Role نیاز دارید. جهت نصب Role مراحل زیر را دنبال کنید:

۱. از مسیر «Start» «Server Manager» «Administrative Tools»، کنسول Server Manager را اجرا کنید.
۲. از قسمت Roles، بر روی Add Roles کلیک کنید.
۳. در صفحه «Before You Begin» بر روی Next کلیک کنید.
۴. در صفحه «Select Server Roles»، Print and Document Services را انتخاب نموده و بر روی Next کلیک کنید.
۵. در صفحه «Introduction to Print and Document Services» اطلاعات مربوط به این Role را مشاهده نموده و بر روی Next کلیک کنید.
۶. در صفحه «Select Role Services» مطمئن شوید که سرویس Print Server انتخاب شده است. در صورت نیاز سایر Role Service ها را نیز انتخاب نموده و بر روی Next کلیک کنید.



شکل ۱۰-۲

۷. در صفحه "Confirm Installation Selections" بر روی Install کلیک کنید.

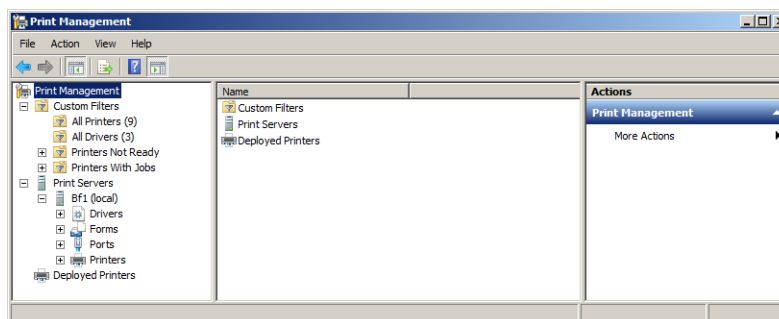
۸. پس از اتمام عملیات نصب، در صفحه "Installation Results" بر روی Close کلیک کنید.

### ۱۰-۲-۲ کار با کنسول Print Management

کنسول Print Management (PMC) که اولین بار در ویندوز سرور 2003R2 معرفی شد، شما را قادر می‌سازد کلیه اقدامات مربوط به چاپ را با استفاده از یک کنسول انجام دهید. در این کنسول اقدامات زیر قابل انجام می‌باشد:

- ♦ افزودن درایورهای جدید
- ♦ مشاهده پرینترها با استفاده از فیلترهای مورد نظر
- ♦ مدیریت تنظیمات پرینترها و درایورها
- ♦ نظارت بر وضعیت پرینتر و پیکربندی هشدارها<sup>۱</sup>
- ♦ اتصال به Print Server های راه دور

پس از افزودن رل Print and Document Services می‌توانید کنسول Print Management (PMC) را از مسیر Start «Administrative Tools» Print Management اجرا کنید. این کنسول همچنین از طریق گره Roles در کنسول Server Manager نیز قابل دسترسی می‌باشد.



شکل ۱۰-۳

کنسول PMC به سه قسمت اصلی تقسیم شده است:

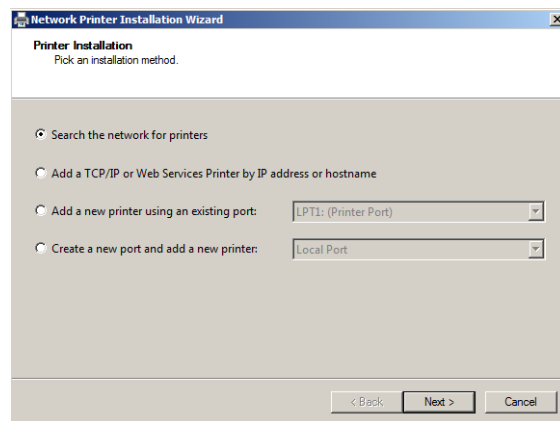
- ♦ **Custom Filters:** فیلترها امکان مشاهده کلیه پرینترهای مدیریت شده توسط کنسول PMC را بدون توجه به متصل بودن آنها به سرور فراهم می‌کنند. اگر تعداد پرینترهای موجود در یک Print Server کم باشند مشاهده آنها کار سختی نخواهد بود. اما اگر هزاران پرینتر در شبکه داشته باشید، می‌توانید با استفاده از فیلترها آنها را به راحتی جستجو کنید.



- ♦ **Print Servers:** در این گره لیست Print Server های اضافه شده به سازمان قابل مشاهده می‌باشد. در مثال ما تنها از یک Print Server به نام Bf1 استفاده شده است اما چنانچه Print Server های بیشتری در سازمان داشته باید می‌توانید از طریق کنسول PMC به آنها متصل شده و آنها را مدیریت کنید.
  - ♦ **Deployed Printers:** در این گره، پرینترهایی که با استفاده از Group policy بر روی سرور مستقر شده‌اند نمایش داده می‌شود. بعداً در مورد نحوه انجام این کار صحبت خواهیم نمود.
- علاوه بر سه مورد ذکر شده در بالا، به ازای هر Print Server چهار گره اصلی در اختیار خواهید داشت. این گره‌ها به منظور مدیریت پرینترهای مختلف که توسط Print Server رزرو شده‌اند مورد استفاده قرار می‌گیرد:
- ♦ **Drivers:** با استفاده از این گره می‌توانید درایورهای مورد نیاز برای پرینترها را اضافه کنید. درایورها به سه دسته اصلی تقسیم می‌شوند: Itanium برای سرورها، x64 برای سیستم عامل‌های ۶۴ بیتی، و x86 برای سیستم عامل‌های ۳۲ بیتی.
  - ♦ **Forms:** این گره سطوح مختلفی که یک پرینتر نصب شده می‌تواند از آنها پشتیبانی کند را مشخص نموده و شامل مواردی چون اندازه کاغذ و حاشیه‌های پرینتر می‌باشد. فرم‌ها بر پایه سرورها نشان داده می‌شوند نه پرینترها.
  - ♦ **Ports:** این گره پورتهایی که برای اتصال پرینتر به سرور استفاده می‌شوند را مشخص می‌کند. مثال‌هایی از این پورته‌ها، پورت‌های سریال COM1 تا COM4، پورت‌های موازی LPT1 تا LPT3 و FILE می‌باشد. چنانچه پرینتری را از طریق پورت USB به سرور متصل کنید، این پورت نیز بطور خودکار اضافه می‌گردد. پورت‌های دیگری مانند XPSPort (برای ایجاد اسناد در قالب Microsoft XPS) و TCP/IP (برای افزودن پرینترهای تحت شبکه) نیز قابل افزودن می‌باشند.
  - ♦ **Printers:** در این گره، لیست پرینترهای افزوده شده به Print Server نشان داده می‌شود. بخاطر داشته باشید که در این گره، پرینترها واسط‌های نرم افزاری قابل مدیریت بر روی Print Server هستند که درخواست‌های چاپ را به دستگاه‌های پرینتر می‌فرستند. می‌توانید برای هر دستگاه چندین پرینتر (نرم افزاری) داشته باشید.

### افزودن پرینتر جدید

با استفاده از کنسول PMC امکان افزودن پرینترها و همچنین شناسایی خودکار پرینترهای موجود در زیرشبکه‌ای که Print Server قرار گرفته، فراهم شده است. برای انجام این کار بر روی گره Printers کلیک راست نموده و گزینه Add Printer را انتخاب کنید. شکل ۱۰-۴ نشان داده می‌شود.



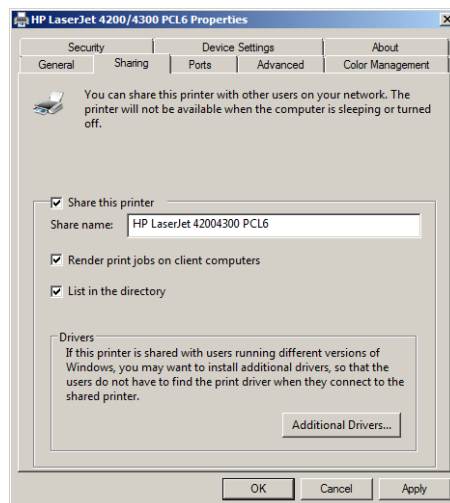
شکل ۱۰-۴

همانطور که مشاهده می‌کنید در این صفحه چهار انتخاب خواهید داشت:

- ♦ **Search the network for printers:** با استفاده از این گزینه می‌توانید پرینترهایی را که در زیرشبکه یکسان با Print Server قرار دارند بطور خودکار شناسایی نموده به PMC اضافه کنید.
- ♦ **Add a TCP/IP or Web Services Printer by IP address or hostname:** چنانچه پرینترهای شما در زیرشبکه متفاوتی قرار داشته و یا به عنوان پرینترهای مبتنی بر سرویس وب پیکربندی شده باشند می‌توانید از این گزینه برای افزودن دستی نام یا آدرس IP آن استفاده کنید. چنانچه از نام برای جستجو استفاده می‌کنید باید مطمئن شوید که سرور DNS جهت تحلیل نام در شبکه پیکربندی شده است.
- ♦ **Add a new printer using an existing port:** اگر سرور شما مجهز به پورت‌های موجود در این گزینه است، می‌توانید از طریق آن پرینترهای خود را اضافه کنید. چنانچه سرویس Printer Pooling فعال باشد می‌توانید به ازای هر پرینتر (نرم افزاری) چندین پورت داشته باشید که در اینصورت هر پورت به یک دستگاه پرینت متصل می‌شود.
- ♦ **Create a new port and add a new printer:** با استفاده از این گزینه می‌توانید یک پورت جدید ایجاد نموده و پرینتر را به آن اضافه کنید. با توجه به اینکه این گزینه انتخاب‌های زیادی در اختیار شما قرار نمی‌دهد ممکن است هرگز از آن استفاده نکنید.

پرینترهایی که با استفاده از پورت USB به سرور متصل می‌شوند، نیاز به انجام کار اضافه نداشته و پس از اتصال فیزیکی بطور خودکار به Print Server افزوده می‌شوند. این پرینترها بطور پیش فرض اشتراک گذاشته نشده‌اند، بنابراین می‌توانید با مراجعه به بخش Properties از تنظیمات آنها

و انتخاب تب Sharing، آنرا در شبکه به اشتراک گذارید.



شکل ۱۰-۵

### حذف یک پرینتر

گاهی اوقات نیاز است که یک پرینتر را از Print Server حذف کنید. قبل از حذف پرینتر باید اطمینان حاصل کنید که در حال استفاده برای چاپ نمی باشد زیرا در اینصورت با پیغام خطایی مواجه خواهید شد. با فرض اینکه پرینتر انتخابی در حال استفاده است، مراحل زیر را جهت متوقف کردن و حذف پرینتر دنبال کنید:

۱. در کنسول Print Management، گره Printers را انتخاب کنید.
۲. بر روی پرینتر مورد نظر کلیک راست نموده و گزینه Open Printer Queue را انتخاب کنید.
۳. در پنجره باز شده کلیک راست نموده و گزینه Cancel All Documents را انتخاب کنید. سپس پنجره مذکور را ببندید.
۴. مجدداً بر روی پرینتر کلیک راست نموده و این بار گزینه Delete را انتخاب کنید. بر روی Yes کلیک کنید.

### شناسایی خودکار پرینترهای شبکه

در شکل ۱۰-۴ گزینه "Search the network for printers" برای شناسایی خودکار و افزودن پرینترهای موجود در شبکه استفاده می شود ولی این روش کمی گمراه کننده است. در این روش تنها زیر شبکه ای که Print Server در آن قرار گرفته است جستجو می شود و با بقیه زیر شبکه ها در شبکه

LAN کاری ندارد.

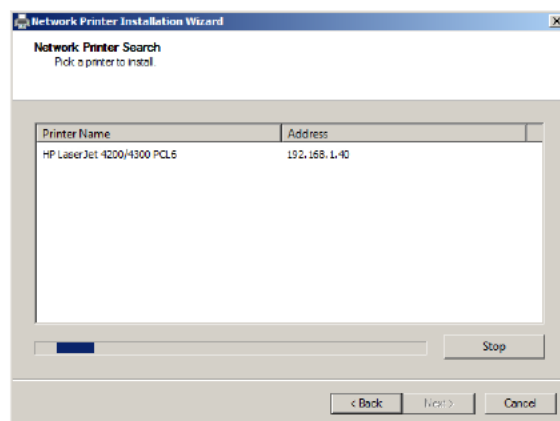
در صورت داشتن پرینترهای تحت شبکه، مراحل زیر را جهت افزودن آنها به سرور دنبال کنید:

۱. کنسول Print Management را اجرا نموده و Print Server خود را انتخاب کنید.
۲. بر روی گره Printers کلیک راست نموده و گزینه Add Printers را انتخاب کنید.



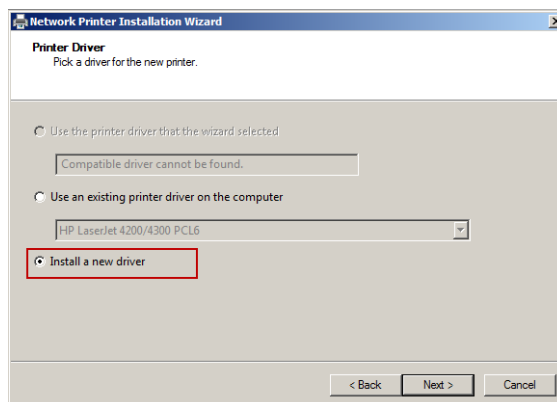
چنانچه شبکه از نوع Public یا عمومی باشد نمی‌توانید از این گزینه برای پیدا کردن پرینترهای شبکه استفاده کنید. بنابراین ابتدا شبکه را به صورت Private یا خصوصی پیکربندی نموده و سپس نسبت به این کار اقدام کنید.

۳. گزینه Search the network for printers را انتخاب نموده و بر روی Next کلیک کنید.
۴. پس از آغاز عملیات جستجو، چنانچه پرینتری در شبکه موجود باشد در صفحه "Network Printer Search" Search نشان داده می‌شود.



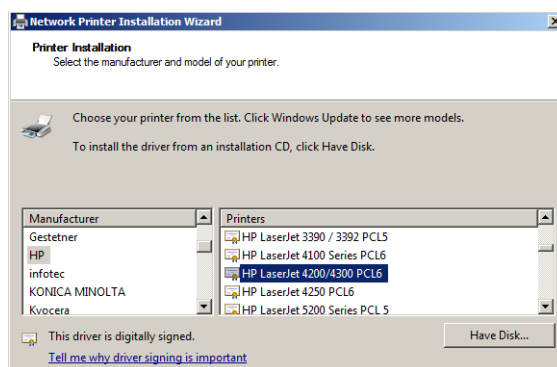
شکل ۶-۱۰

۵. پس از پایان جستجو، در صورت پیدا شدن پرینتر مورد نظر آنرا انتخاب نموده و بر روی Next کلیک کنید. در حین این عملیات، یک پورت TCP/IP استاندارد با آدرس IP پرینتر ایجاد می‌شود و نیازی به ایجاد پورت در مرحله‌ای جداگانه نمی‌باشد.
۶. در صفحه "Print Driver" چنانچه درایوری برای پرینتر مورد نظر وجود داشت آنرا انتخاب کنید، در غیر اینصورت گزینه Install a new driver را انتخاب نموده و بر روی Next کلیک کنید.



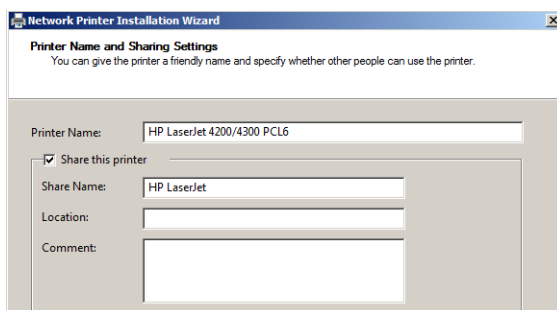
شکل ۷-۱۰

۷. در صفحه “Printer Installation” نوع و مدل پرینتر را انتخاب نموده و بر روی Next کلیک کنید. چنانچه مدل پرینتر در فهرست وجود نداشت می‌توانید با استفاده از دکمه Have Disk و قرار دادن دیسک حاوی درایور، آنرا به فهرست اضافه کنید.



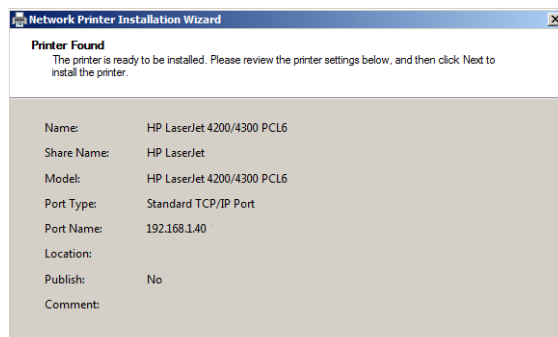
شکل ۸-۱۰

۸. پس از Load شدن درایور، در صفحه “Printer Name and Sharing Settings” تنظیمات مربوط به نام و اشتراک‌گذاری پرینتر را انجام داده و بر روی Next کلیک کنید.



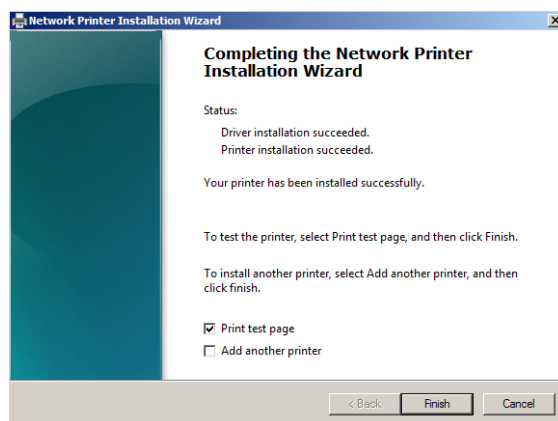
شکل ۹-۱۰

۹. در صفحه “Printer Found” تنظیمات انجام شده نمایش داده می‌شود. بر روی Next کلیک کنید.



شکل ۱۰-۱۰

۱۰. در صفحه “Completing the Network Printer Installation Wizard” سیستم تلاش می‌کند که ابتدا درایور و سپس پرینتر را نصب کند. اگر ناسازگاری بین درایور و پرینتر وجود داشته باشد پیغام خطایی به شما نشان داده خواهد شد. در غیر اینصورت پرینتر با موفقیت نصب خواهد شد. در نهایت می‌توانید با انتخاب گزینه Print test page موفقیت آمیز بودن عملیات و اضافه شدن پرینتر را تست کنید.



شکل ۱۱-۱۰

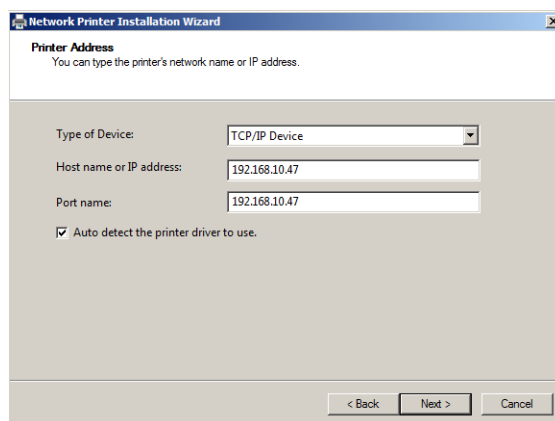
### نصب دستی یک پرینتر جدید

جهت افزودن پرینتری که در شبکه موجود بوده ولی در زیرشبکه شما قرار ندارد مراحل زیر را دنبال کنید:

۱. در کنسول PMC بر روی گره Printers کلیک‌راست نموده و گزینه Add Printers را انتخاب کنید.

۲. گزینه Add a TCP/IP or Web Service Printer by IP address or hostname را انتخاب و بر روی Next کلیک کنید.

۳. در صفحه "Printer Address"، نوع دستگاه (TCP/IP) را انتخاب نموده و آدرس IP یا نام آنرا (در صورتی که از DNS استفاده می‌شود) وارد کنید. همچنین مطمئن شوید که گزینه Auto detect the printer driver to use نیز انتخاب شده است. در نهایت بر روی Next کلیک کنید.



شکل ۱۰-۱۲

در این لحظه ویزارد "Network Printer Installation Wizard" به اتمام رسیده و عملیات جستجوی پرینتر آغاز می‌گردد.

۴. در صفحه "Print Driver" چنانچه درایوری برای پرینتر مورد نظر وجود داشت آنرا انتخاب کنید، در غیر اینصورت گزینه Install a new driver را انتخاب نموده و بر روی Next کلیک کنید.

۵. در صفحه "Printer Installation" نوع و مدل پرینتر را انتخاب نموده و بر روی Next کلیک کنید.

۶. در صفحه "Printer Name and Sharing Settings" تنظیمات مربوط به نام و اشتراک‌گذاری پرینتر را انجام داده و بر روی Next کلیک کنید.

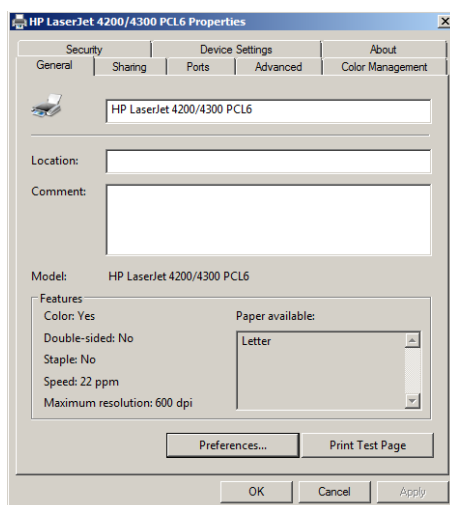
۷. در صفحه "Printer Found" تنظیمات انجام شده نمایش داده می‌شود. بر روی Next کلیک کنید.

۸. در صفحه "Completing the Network Printer Installation Wizard" بر روی Finish کلیک کنید.

همانطور که مشاهده نمودید، تنها تفاوت میان روش دستی و خودکار، وارد کردن آدرس IP پرینتر می‌باشد. بخاطر داشته باشید که روش دستی (Add a TCP/IP or Web Service...) زمانی که پرینتر در زیر شبکه مجزایی نسبت به Print Server قرار داشته باشد مورد استفاده قرار می‌گیرد.

### تغییر تنظیمات پرینتر

پس از افزودن پرینتر می‌توانید تنظیمات آنرا با استفاده از کنسول PMC تغییر دهید. برای انجام این کار لازم است در کنسول PMC پس از انتخاب گره Printers، بروی پرینتر مورد نظر کلیک‌راست نموده و Properties را انتخاب کنید. در پنجره باز شده می‌توانید مشخصات و تنظیماتی مانند تنظیمات اشتراک‌گذاری، اندازه کاغذها، تنظیمات رنگ، تنظیمات پورت، تنظیمات درایور، مجوزهای دسترسی به پرینتر و تنظیماتی از این دست را انجام دهید.



شکل ۱۰-۱۳

### ۱۰-۳ استقرار پرینترها برای کاربران

پس از افزودن پرینتر به سرور می‌توانید آنرا در دسترس کاربران قرار دهید. این کار به سه روش قابل انجام است:

- ♦ به صورت دستی
- ♦ با استفاده از ابزار Active Directory Search
- ♦ با استفاده از Group Policy

استفاده از گزینه‌های دوم و سوم زمانی که کامپیوترها در یک دامنه اکتیو دایرکتوری قرار دارند امکان‌پذیر می‌باشد. در ادامه مراحل کار را برای هر سه روش شرح می‌دهیم.

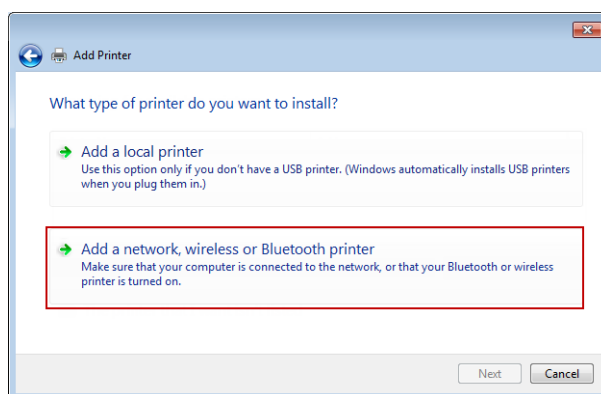
### ۱۰-۳-۱ افزودن دستی پرینتر برای کاربران

پس از افزودن پرینتر به Print Server، افزودن آن برای کاربران نیز ساده است. کافی است مراحل



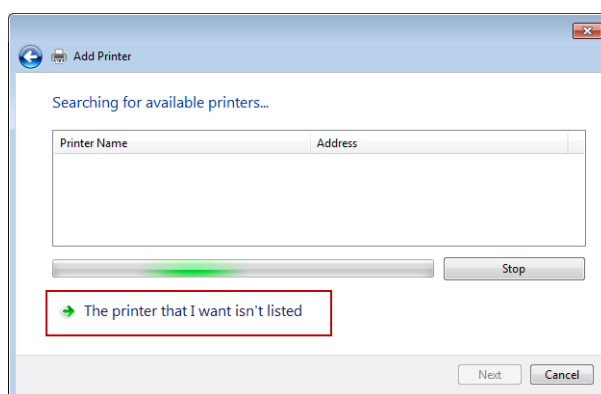
زیر را برای کاربران ویندوز ۷ دنبال کنید:

۱. به مسیر Start » Devices and Printers بروید.
۲. در قسمت سفیدی از صفحه باز شده کلیک راست نموده و Add a printer را انتخاب کنید.
۳. در صفحه "Add Printers"، گزینه Add a network, wireless, or Bluetooth printer را انتخاب کنید.



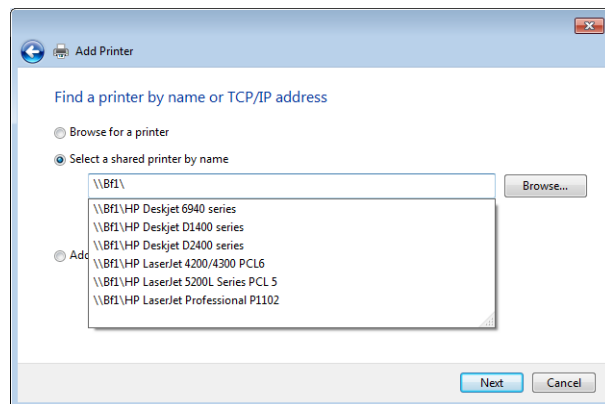
شکل ۱۰-۱۴

۴. سیستم شروع به جستجوی پرینترها در شبکه می‌نماید. گزینه The printer that I want isn't listed را انتخاب کنید.



شکل ۱۰-۱۵

۵. در صفحه "Find a printer by name or TCP/IP address" گزینه Select a shared printer by name را انتخاب نموده و جهت مشاهده پرینترهای اشتراک گذاشته شده در سرور، نام آنرا به صورت \\ServerName\ وارد کنید (مانند \\Bf1).
۶. پرینتر مورد نظر را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۱۰-۱۶

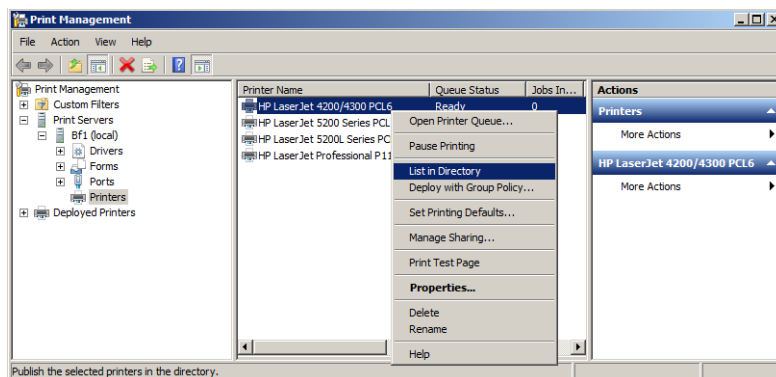
۷. درایور نصب شده بر روی سرور، بطور خودکار برای کاربر دانلود و نصب می‌شود. نام پرینتر همان نامی است که با آن به اشتراک گذاشته شده است. بر روی Next و سپس Finish کلیک کنید.

### ۱۰-۳-۲ افزودن پرینتر با استفاده از ابزار Active Directory Search

اکتیو دایرکتوری پایگاه‌داده‌ای عظیم از اشیاء است که می‌توانند توسط کاربران و مدیران مورد جستجو قرار گیرند. بسیاری از این اشیاء (مانند Users، Groups و Shares) بطور خودکار در اکتیو دایرکتوری منتشر می‌شوند و به کاربران اجازه می‌دهند که به سادگی آنها را مورد جستجو قرار دهند، با این وجود پرینترها بطور پیش‌فرض در اکتیو دایرکتوری منتشر نمی‌شوند، بنابراین لازم است که انتشار آنها را بطور دستی انجام دهید. برای انجام این کار مراحل زیر را دنبال کنید:

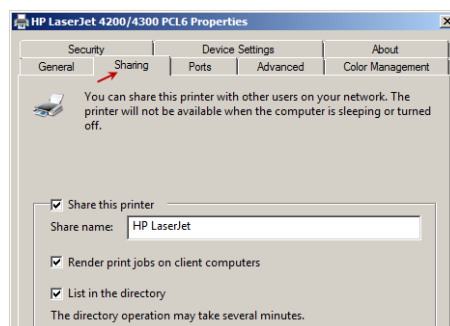
۱. در کنسول PMC به گره Printers رفته و پرینتر مورد نظر را انتخاب کنید.

۲. بر روی پرینتر کلیک راست نموده و گزینه List in Directory را انتخاب کنید.



شکل ۱۰-۱۷

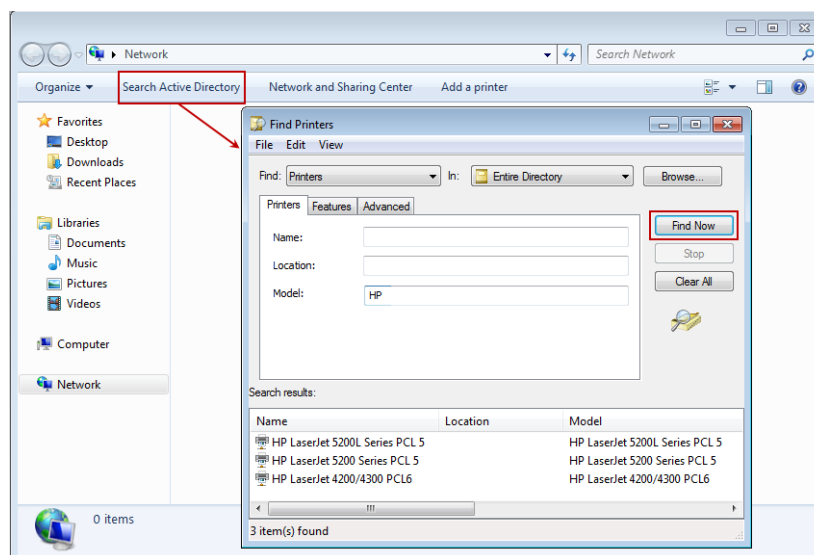
۳. چنانچه گزینه List in Directory وجود نداشت، ممکن است پرینتر به اشتراک گذاشته نشده باشد. جهت اشتراک‌گذاری بر روی Printer کلیک‌راست نموده و Properties را انتخاب کنید.
۴. به تب Sharing رفته و گزینه Share this printer را فعال کنید. دقت داشته باشید که امکان انتخاب گزینه List in Directory در این تب نیز وجود دارد.



شکل ۱۰-۱۸

تا اینجا امکان جستجوی پرینتر توسط کاربران فراهم شده است. اکنون مراحل زیر را جهت افزودن پرینتر بر روی سیستم کاربران دنبال کنید:

۱. به مسیر Start » Network بروید.
۲. بر روی گزینه Search Active Directory کلیک کنید.
۳. در قسمت Find گزینه Printers را انتخاب نموده و بر روی Find Now کلیک کنید.



شکل ۱۰-۱۹

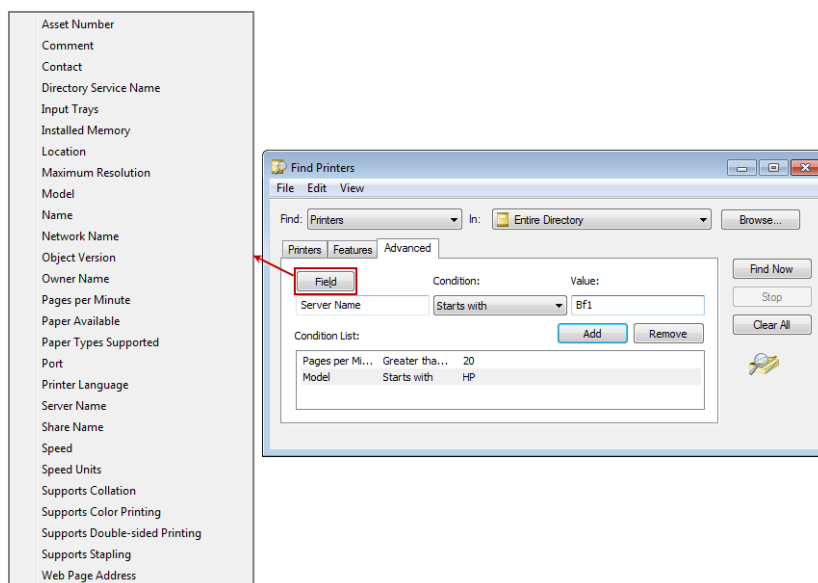
۴. پس از اینکه پرینتر مورد نظر جستجو شد، بر روی آن دابل‌کلیک نموده تا پرینتر بر روی سیستم نصب گردد.

در ابزار Active Directory search امکان جستجوی پرینترها (یا سایر اشیاء) بر اساس شرایط دیگر نیز وجود دارد. اعمال این شرایطها با استفاده از تب‌های موجود در این ابزار امکان‌پذیر می‌باشد. در جدول زیر فهرستی از این شرایط به همراه تب محل قرار گیری آنها آورده شده است.

جدول ۱۰-۱: شرایط قابل اعمال در جستجوی پرینترها

محل قرار گیری (نام Tab)	مشخصه‌های پرینتر
Printers	Name (نام)
Printers	Location (محل قرارگیری)
Printers	Model (مدل)
Features	Double-sided printing (امکان چاپ پشت و رو)
Features	Color printing (چاپ رنگی)
Features	Can staple (چاپ عمده - عمودی)
Advanced	جستجو بر اساس مشخصات ویژه

در تب‌های Printers و Features کافی است مشخصه‌های مورد نظر را وارد نموده و یا آنها را علامت گذاری کنید. در تب Advanced باید این مشخصه‌ها را با استفاده از قسمت Field انتخاب نموده و سپس عمل جستجو را انجام دهید.

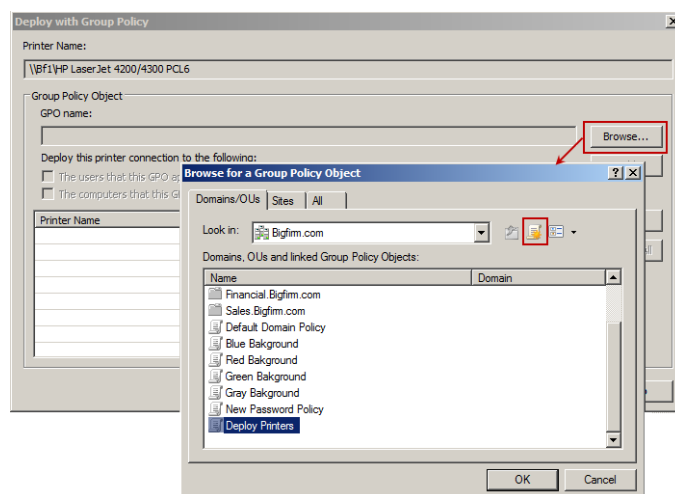


شکل ۱۰-۲۰

### ۳-۳-۱۰ استقرار پرینتر با استفاده از GPO

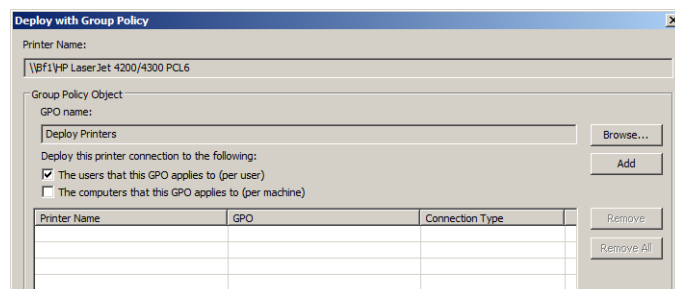
امکان استقرار پرینتر با استفاده از Group policy و GPO ها نیز میسر می‌باشد. جهت انجام این کار می‌توانید مراحل مراحل زیر را دنبال کنید:

۱. بروی سروری که به عنوان Print Server استفاده می‌شود، کنسول PMC را اجرا نموده و به گره Printers حرکت کنید.
۲. بروی پرینتر مورد نظر کلیک‌راست نموده و گزینه Deploy with Group Policy را انتخاب کنید.
۳. در صفحه "Deploy with Group Policy" بروی دکمه Browse کلیک کنید.
۴. بروی آیکن Create a New Group Policy Object کلیک نموده و سپس عبارت Deploy Printers را جهت تخصیص به نام GPO وارد کنید.



شکل ۱۰-۲۱

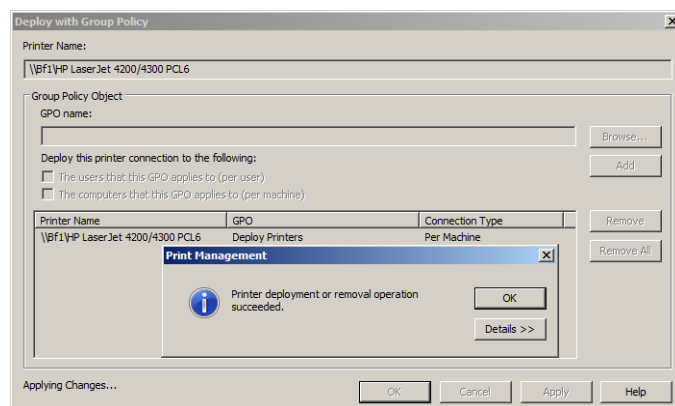
۵. GPO که ایجاد نمودید (Deploy Printers) را انتخاب و بروی OK کلیک کنید.
۶. گزینه The computers that this GPO applies to (per machine) را فعال کنید.



شکل ۱۰-۲۲

چنانچه قصد دارید پرینتر را برای کاربران و بدون در نظر گرفتن اینکه چه کسی به کامپیوتر وارد می‌شود و یا برای کاربرانی که مهم نیست از کجا وارد می‌شوند مستقر کنید، باید گزینه The users that this GPO applies to (per user) را نیز انتخاب کنید.

۷. بر روی دکمه Add کلیک کنید تا تنظیمات انتخاب شده توسط شما بر روی GPO اعمال شوند. در نهایت بر روی OK کلیک کنید. پس از چند ثانیه پنجره‌ای ظاهر شده و موفقیت آمیز استقرار پرینتر را نشان می‌دهد. مجدداً بر روی OK کلیک کنید.



شکل ۱۰-۲۳

اگر به کنسول Group Policy Management مراجعه کنید، مشاهده خواهید نمود که این GPO در زیرمجموعه Group Policy Objects قرار گرفته است. همچنین پرینتر مورد نظر در مسیر Computer Configuration\ Policies\Windows Settings\Deployed Printers (Right Click «GPO») GPME اضافه می‌گردد.

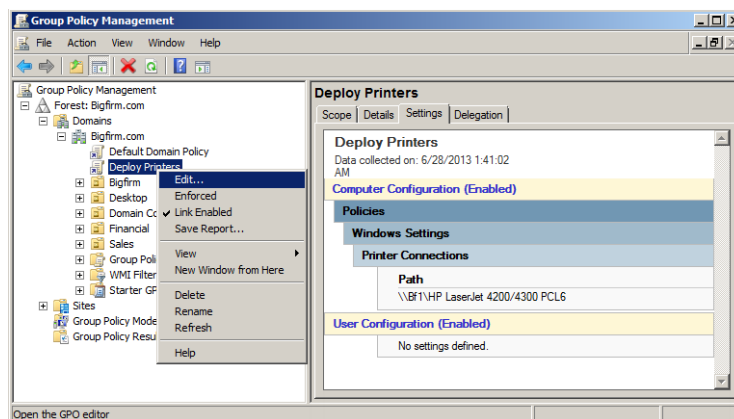
پس از انجام مراحل بالا، به کامپیوترهای ویندوز ۷ و ویندوز سرور 2008R2 در دامنه مراجعه نموده و در داخل خط فرمان آنها (Cmd) دستور زیر را جهت اعمال شدن Policy وارد کنید:

**gpupdate /force**

پس از اجرای این دستور، پرینتر بطور خودکار در فهرست پرینترهای موجود بر روی کامپیوتر قرار می‌گیرد. مسئله‌ای که در اینجا باید به آن توجه داشته باشید این است که اگر تمام کاربران از ویندوز سرور 2008R2 یا ویندوز ۷ استفاده کنند، دستور بالا به خوبی انجام خواهد شد، اما چنانچه در دامنه کاربرانی با ویندوز سرور 2008 یا ویندوز ویستا داشته باشید، دستور بالا قابل اجرا نیست و باید از ابزار PushPrinterConnection.exe جهت استقرار پرینتر بر روی کامپیوترهای آنها استفاده کنید. در این دو سیستم عامل، این ابزار در پوشه Windows\System32 قابل مشاهده می‌باشد.

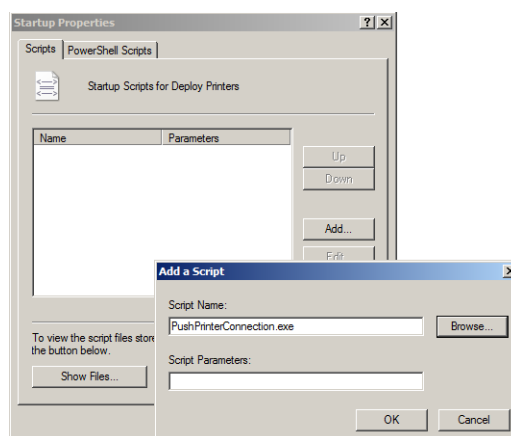
جهت استقرار پرینتر بر روی کاربران ویستا و سرور 2008 مراحل زیر را دنبال کنید:

۱. کنسول Group Policy Management را از مسیر «Start Administrative Tools اجرا کنید.
۲. بر روی GPO با نام Deploy Printers کلیک راست نموده و Edit را انتخاب کنید.



شکل ۱۰-۲۴

۳. به گره Computer Configuration\Policies\Windows Settings\Scripts (Startup/ Shutdown) بروید.
۴. بر روی Startup دابل کلیک نموده و سپس در پنجره "Startup Properties" بر روی دکمه Show Files کلیک کنید.
۵. در پنجره بازشده، باید ابزار PushPrinterConnection.exe را که در داخل پوشه Windows\System32 از ویندوز ویستا و سرور 2008 قرار دارد به داخل این پنجره کپی نمایید.
۶. بر روی دکمه Add و سپس Brows کلیک کنید. اسکرپت PushPrinterConnection.exe را انتخاب نموده و بر روی Open کلیک کنید. نام ابزار در پنجره "Add a Script" ظاهر می شود.



شکل ۱۰-۲۵

۷. در صورت تمایل می‌توانید پارامتر log- را در قسمت Script Parameters وارد کنید. بر روی OK کلیک نموده تا پنجره “Add a Script” بسته شود. مجدداً برای بسته شدن پنجره “Startup Properties” نیز بر روی OK کلیک کنید.

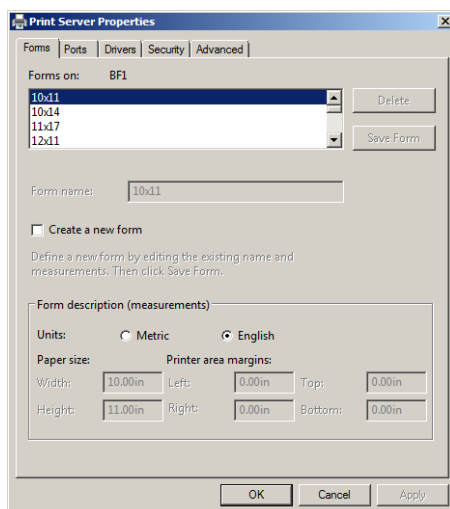
در نهایت لازم به ذکر است که برای مشاهده پرینترهای استقرار یافته توسط Group policy می‌توانید در کنسول Print Management به کانتینر Deployed Printers مراجعه کنید. در زمان مراجعه، اکتیو دایرکتوری مورد جستجو قرار گرفته و فهرست پرینترهای Deploy شده نمایش داده می‌شود.

## ۱۰-۴ انجام تنظیمات Print Server

تعدادی از تنظیمات وجود دارند که در سطح سرور انجام شده و می‌توانند به یکباره بر روی تمام منابعی (Ports, Forms, Drivers, Printers) که توسط آن سرور مدیریت می‌شود پیکربندی گردد. همچنین تنظیمات دیگری مانند امکان Export و Import کردن پرینترها به/از داخل فایل‌ها و تنظیم هشدارها (Notifications) نیز برای Print Server قابل انجام می‌باشد. کلیه این تنظیمات با کلیک‌راست بر روی نام سرور در کنسول Print Management قابل دسترسی هستند. در ادامه این تنظیمات را مورد بررسی قرار می‌دهیم.

### ۱۰-۴-۱ Server Properties

زمانی که پس از کلیک‌راست بر روی نام سرور (در اینجا Bf1)، گزینه Properties را انتخاب کنید، پنجره “Print Server Properties” نمایش داده می‌شود. دقت داشته باشید که این پنجره با کلیک‌راست بر روی گره Forms و انتخاب Manage Forms نیز قابل دسترسی می‌باشد.



شکل ۱۰-۲۶

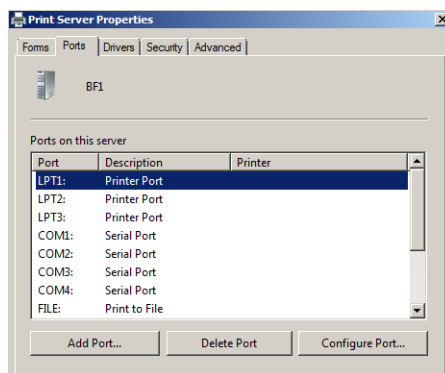


### تب Forms

Form ها، الگوهای پیش فرضی هستند که متن کاغذها برای چاپ شدن در اندازه‌های آنها تنظیم می‌شود. در این تب لیستی طولانی از Form های قابل انتخاب برای چاپ آورده شده است و امکان افزودن Form جدید و یا ایجاد تغییر در تنظیمات Form های ایجاد شده نیز فراهم شده است. اندازه استاندارد کاغذ در این فرم ها 8.5×11 است که می‌توانید آنرا از لیست پیدا نموده و انتخاب کنید. برای ایجاد Form جدید نیز می‌توانید از گزینه Create a new form در این تب استفاده نمایید. دقت داشته باشید که امکان حذف Form های از پیش تعریف شده وجود ندارد ولی می‌توانید Form هایی که خودتان ایجاد می‌کنید را حذف نمایید.

### تب Ports

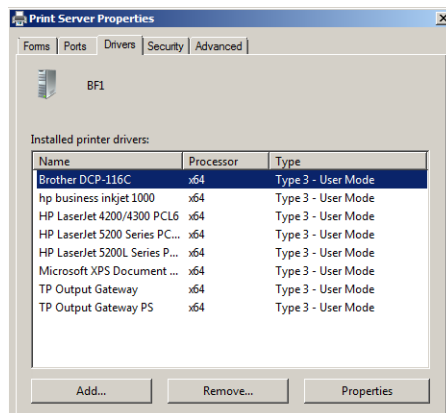
اگر بخاطر داشته باید گفتیم که پرینترها با استفاده از پورت‌ها به سرور متصل می‌شوند. در تب Ports لیست کلیه پورت‌های موجود بر روی سرور نمایش داده شده است. امکان افزودن پورت‌ها، حذف پورت‌ها و پیکربندی آنها در این تب وجود دارد. دسترسی به این تب همچنین از طریق کلیک راست بر روی گره Ports و انتخاب Manage Ports نیز امکان پذیر می‌باشد.



شکل ۱۰-۲۷

### تب Drivers

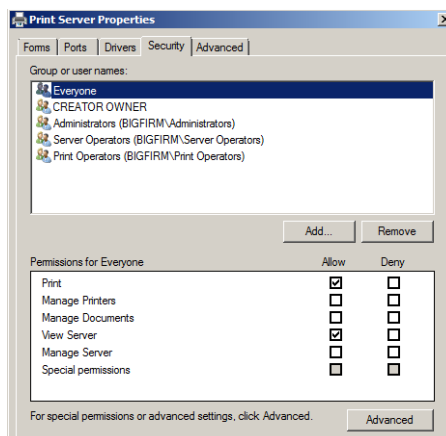
قبلاً نحوه افزودن Driver ها را شرح دادیم و گفتیم که درایورها نرم افزارهایی هستند که برای استفاده از پرینتر نصب می‌شوند. می‌توانید با استفاده از این تب پروسه مشابهی را برای افزودن درایورها (برای پشتیبانی از کاربران مختلف) دنبال کنید. دقت داشته باشید که هر درایور دارای تنظیمات مشخصی است و می‌توانید با انتخاب دکمه Properties به این تنظیمات دسترسی پیدا کنید.



شکل ۱۰-۲۸

### تب Security

در این تب امکان مدیریت دسترسی به Print Server فراهم شده است. جهت اختصاص مجوزها می‌توانید از گزینه‌های Allow (دادن مجوز) و Deny (گرفتن مجوز) استفاده کنید. جهت اعمال مجوزها بر روی سرور، ابتدا از قسمت Group or user names فرد یا گروه مورد نظر را انتخاب نموده و سپس در قسمت Permissions for... مجوزهای لازم را برای او Allow یا Deny کنید.

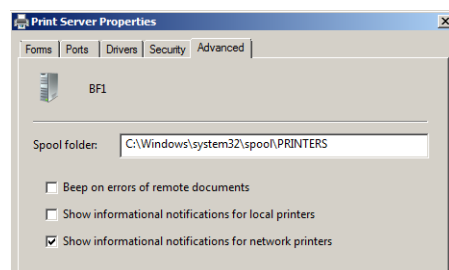


شکل ۱۰-۲۹

### تب Advanced

در این تب نیز تنظیماتی جهت تعیین مسیر قرارگیری پوشه Spool (پوشه ذخیره‌سازی اسناد انتقالی به پرینترها) و همچنین گزینه‌هایی برای نمایش هشدارهای مربوط به پرینترهای Local و

پرینترهای شبکه تعبیه شده است. برای تغییر مسیر قرارگیری Spooler می‌توانید آدرس مورد نظر را در فیلد Spool folder وارد نمایید.

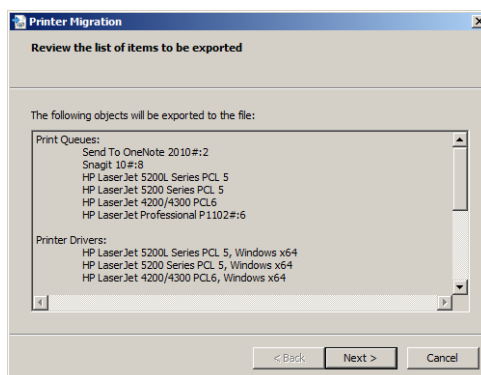


شکل ۱۰-۳۰

#### ۱۰-۴-۲ Import و Export کردن پرینترها

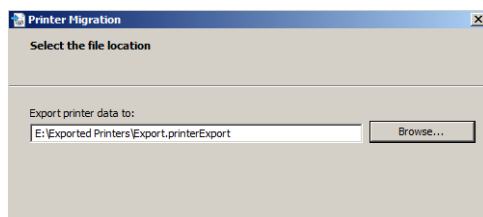
گاهی اوقات ممکن است به دلایل خاصی نیاز به توقف عملکرد یک Print Server و انتقال تنظیمات آن به سرور دیگر باشد. انتقال دستی این تنظیمات برای تعداد کمی از پرینترها ساده است ولی وقتی تعداد آنها زیاد است کار کمی سخت‌تر می‌شود بنابراین می‌توان از روش‌های ساده‌ای جهت انجام آن استفاده نمود. روش پیشنهادی برای انتقال عملکرد Print Server به این صورت است که ابتدا پرینترها را در پوشه‌ای از سرور اصلی Export نموده و سپس این پوشه را به سرور جدید منتقل می‌کنید. در سرور جدید، با Import کردن فایل‌های موجود در این پوشه می‌توانید پرینترها را به آن منتقل نمایید. برای انجام این کار مراحل زیر را دنبال کنید:

۱. در کنسول Print Management بروی Print Server مورد نظر (Bf1) کلیک‌راست نموده و گزینه Export printers to a file را انتخاب کنید.
۲. در صفحه "Review the list of items to be exported" پس از مشاهده لیست پرینترهای موجود، بروی Next کلیک کنید.



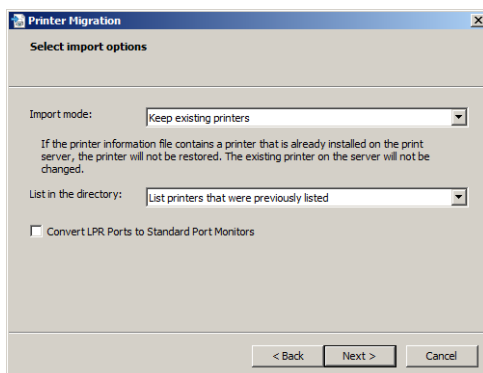
شکل ۱۰-۳۱

۳. در صفحه "Select the File Location" با استفاده از دکمه Browse محل ذخیره‌سازی فایل Export را به همراه نام آن تعیین نموده و سپس بر روی Next کلیک کنید.



شکل ۱۰-۳۲

۴. کمی منتظر بمانید تا عملیات به اتمام برسد. سپس بر روی Finish کلیک کنید.
۵. پس از اتمام فرایند، فایل ایجاد شده را به سرور جدید منتقل کنید.
۶. در کنسول Print Management از سرور جدید، بر روی سرور مورد نظر کلیک راست نموده و گزینه Import printers from a file را انتخاب کنید.
۷. در صفحه "Select the File Location" آدرس فایلی که به سرور انتقال داده‌اید را وارد نموده و بر روی Next کلیک کنید.
۸. در صفحه "Review the list of items to be exported" لیست پرینترها و درایورهای انتقالی به سرور جدید را مشاهده نموده و بر روی Next کلیک کنید.
۹. در صفحه "Select Import options" نوع انتقال را مشخص نموده و بر روی Next کلیک کنید.



شکل ۱۰-۳۳

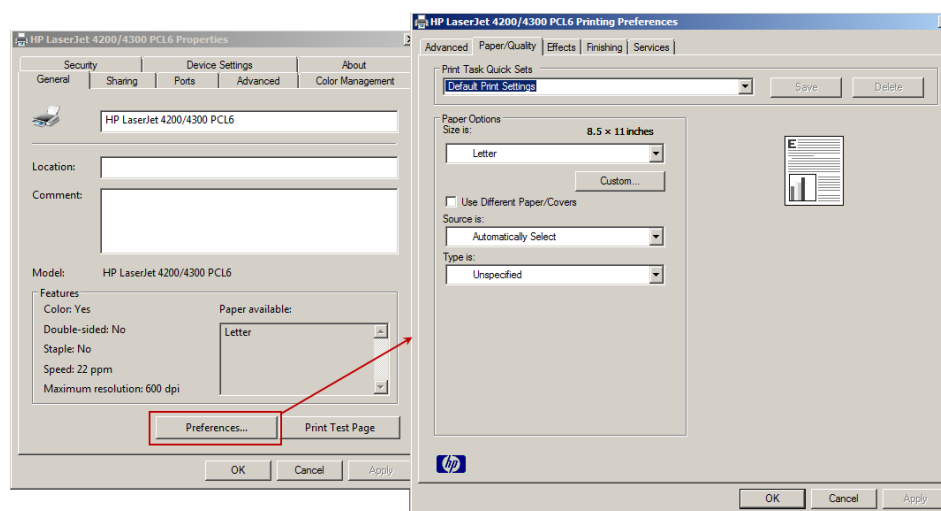
۱۰. پس از اتمام عملیات بر روی Finish کلیک کنید.

### ۵-۱۰ مدیریت تنظیمات پرینترها

تنظیماتی که در قسمت قبل معرفی کردیم، در سطح سرور قابل انجام هستند. در این قسمت قصد داریم به تنظیمات سطح پرینتر بپردازیم. برای دسترسی به تنظیمات هریک از پرینترها به کانتینر Printers رفته، بروی پرینتر مورد نظر کلیک راست نموده و Properties را انتخاب کنید. پنجره Printer Properties شامل هشت تب است که در ادامه مهمترین آنها را مورد بررسی قرار می‌دهیم.

#### تب General

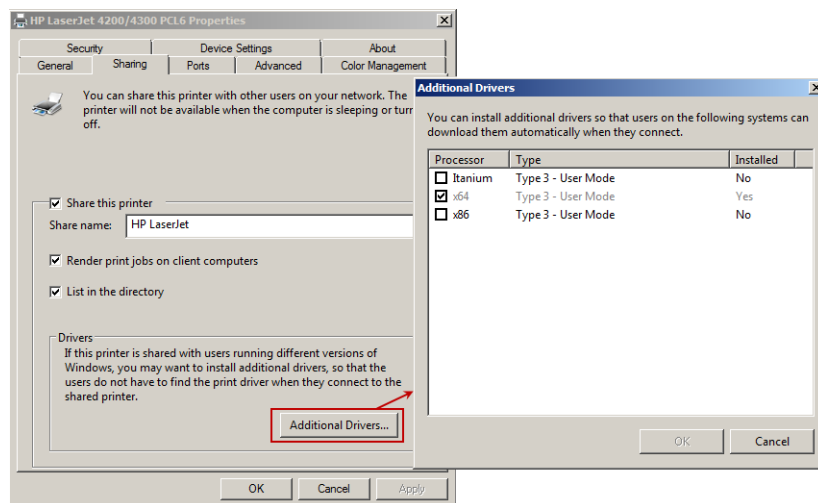
همانطور که در شکل ۱۰-۳۴ مشاهده می‌کنید، در این تب تنظیماتی از قبیل نام پرینتر، محل قرارگیری آن، و توضیحاتی راجع به پرینتر قابل انجام است. همچنین با استفاده از دکمه Preferences امکان انجام تنظیمات مربوط به چاپ نیز فراهم گردیده است.



شکل ۱۰-۳۴

#### تب Sharing

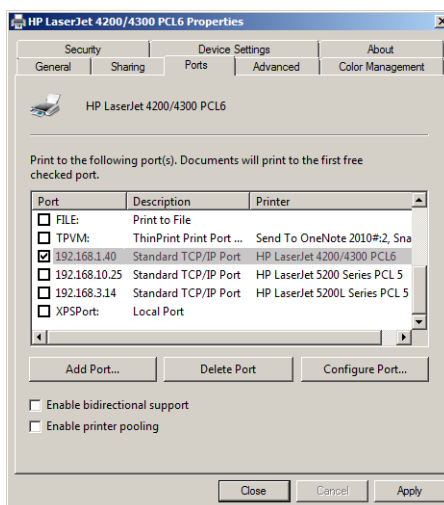
در این تب همانطور که از نام آن نیز مشخص است، تنظیمات مربوط به اشتراک‌گذاری پرینتر انجام می‌شود. این تنظیمات شامل مواردی همچون نام اشتراک پرینتر جهت نمایش برای کاربران، و قرار دادن پرینتر در اکتیو دایرکتوری می‌باشد. علاوه بر این، با استفاده از دکمه Additional Drivers می‌توان درایورهای جدیدی برای پرینتر اضافه نمود. قبلاً در مورد نوع درایورها توضیح داده شده است.



شکل ۱۰-۳۵

### تب Ports

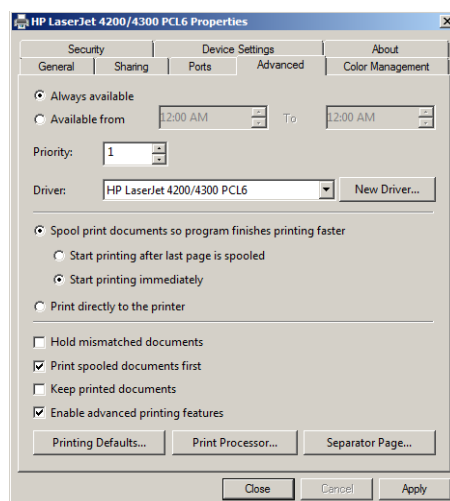
در تب Ports امکان افزودن، حذف کردن و پیکربندی پورتهایی که توسط پرینتر استفاده می‌شوند فراهم گردیده است. همچنین با انتخاب گزینه Enable bidirectional support می‌توانید چندین دستگاه پرینتر را برای پرینتر فعلی پیکربندی کنید. با پیکربندی این گزینه، زمانی که تعداد درخواست‌ها برای یک پرینتر زیاد است، این پرینتر درخواست‌ها را به دستگاهی که آزاد است (از بین چند دستگاه متصل به پرینتر) ارسال می‌کند بنابراین از انتظار بیش از حد کاربران جلوگیری می‌شود.



شکل ۱۰-۳۶

## تب Advanced

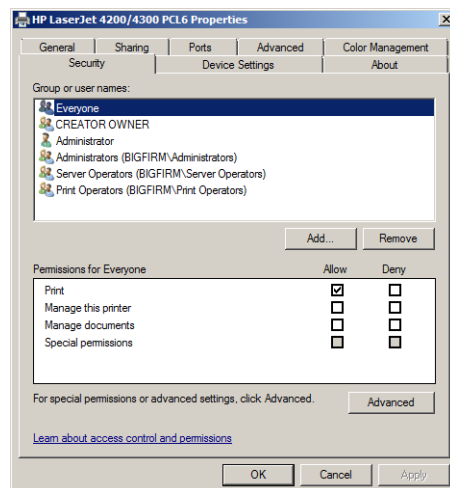
در این تب، تنظیم و پیکربندی تعداد زیادی از اقدامات از جمله ایجاد بازه زمانی برای استفاده از پرینتر، تنظیم اولویت (Priority) پرینتر، آپدیت درایور، زمان شروع عملیات پرینت، و انجام بعضی از ویژگی‌ها و وظایف متفرقه در رابطه با مدیریت پرینت‌ها امکان‌پذیر می‌باشد.



شکل ۱۰-۳۷

## تب Security

در این تب تنظیمات مربوط به دسترسی افراد یا گروه‌ها به پرینتر انجام می‌شود و با استفاده از مجوزهای موجود در آن می‌توان میزان دسترسی و استفاده افراد از پرینتر را محدود نمود.

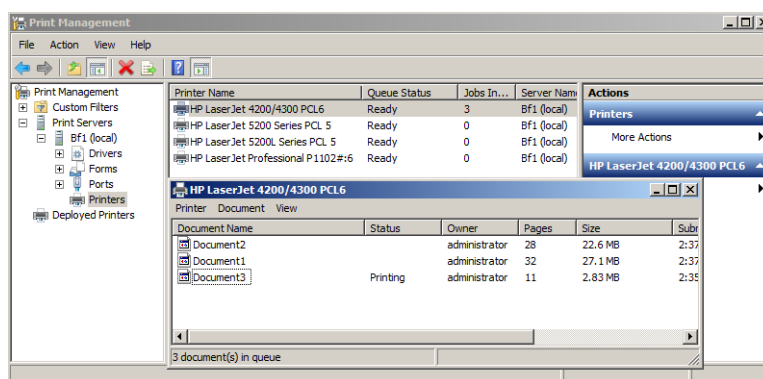


شکل ۱۰-۳۸

## ۱۰-۶ مدیریت Print Jobs

برای مدیریت Print Job می‌توانید از کنسول Print Management استفاده کنید. منظور از Print Jobs درخواست‌های چاپی است که برای اجرا شدن به پرینتر فرستاده شده و در صف قرار می‌گیرند. برای دسترسی به این صف کافی است بروی نام پرینتر کلیک‌راست نموده و Open Printer Queue را انتخاب کنید.

در شکل زیر، صف پرینت برای پرینتر HP LaserJet 4200/4300 PCL6 (در مثال ما) که دارای سه سند برای پرینت است نشان داده شده است.



شکل ۱۰-۳۹

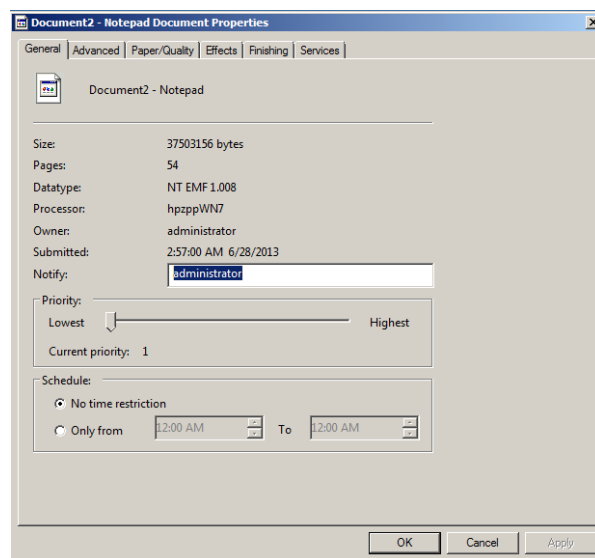
در این پنجره، اطلاعاتی راجع به اسناد قرارگرفته در صف پرینت ارائه شده است. این اطلاعات عبارتند از:

- **File Name:** نام سند یا فایلی است که در صف قرار گرفته است.
- **Status:** وضعیت فعلی فایل را نشان می‌دهد که یکی از حالات `printing`, `spooling`, `paused` و یا خالی می‌باشد.
- **Owner:** نام فردی است که فایل را برای پرینت فرستاده است.
- **Pages:** تعداد صفحات فایل ارسالی برای پرینت را نشان می‌دهد.
- **Size:** بیانگر حجم فایل می‌باشد.
- **Submitted:** تاریخ و زمانی است که فایل برای پرینت فرستاده شده است.
- **Port:** پورتهی است که فایل برای پرینت به آن فرستاده می‌شود.

زمانی که فایل‌ها برای پرینت فرستاده شده و در صف قرار می‌گیرند، در منوی بالای پنجره مربوط به صف، انجام اقداماتی مانند توقف، Restart و Cancel کردن عملیات پرینت وجود دارد.



همچنین آپشنی به نام Properties نیز وجود دارد که با استفاده از آن می‌توانید تنظیمات مربوط به فایل ارسالی برای چاپ را مشخص کنید.



شکل ۱۰-۴۰

## ۷-۱۰ استفاده از Custom Filters

Custom Filterها، فیلترهایی هستند که به منظور انجام جستجو میان پرینترها و درایورها زمانی که تعداد آنها بسیار زیاد است مورد استفاده قرار می‌گیرند. به عنوان مثال حالتی را در نظر بگیرید که دارای بیست Print Server، هر کدام با ۱۰۰ پرینتر هستید. مسلماً جستجوی یک پرینتر در میان این پرینترها کار ساده‌ای نخواهد بود.

زمانیکه در کنسول PMC به کانتینتر Custom Filters مراجعه می‌کنید، بطور پیش‌فرض چهار Template برای فیلترها موجود می‌باشد:

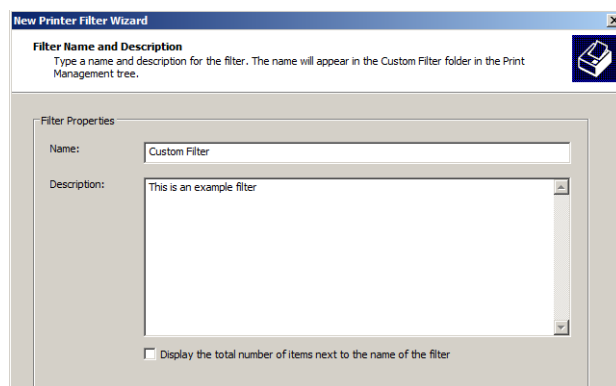
- ♦ **All Printers**: این گزینه تمام پرینترهایی که توسط کلیه سرورهای مدیریت شده در کنسول PMC استفاده می‌شوند را نمایش می‌دهد.
- ♦ **All Drivers**: این گزینه تمام درایورهای مدیریت شده در کنسول PMC استفاده می‌شوند را نمایش می‌دهد.
- ♦ **Printers Not Ready**: زمانی که هر کدام از پرینترها در حالت توقف باشند یا آماده اجرای پرینت نباشند، در این فیلتر قرار می‌گیرند.
- ♦ **Printers with Jobs**: پرینترهایی که در حال اجرای درخواست چاپ بوده و یا دارای درخواست‌های

قرار گرفته در صف باشند، در این فیلتر قرار می‌گیرند.

امکان ایجاد فیلترها با استفاده از تنظیمات و مشخصه‌های دیگر نیز وجود دارد. برای انجام این کار کافی است مراحل زیر را دنبال کنید:

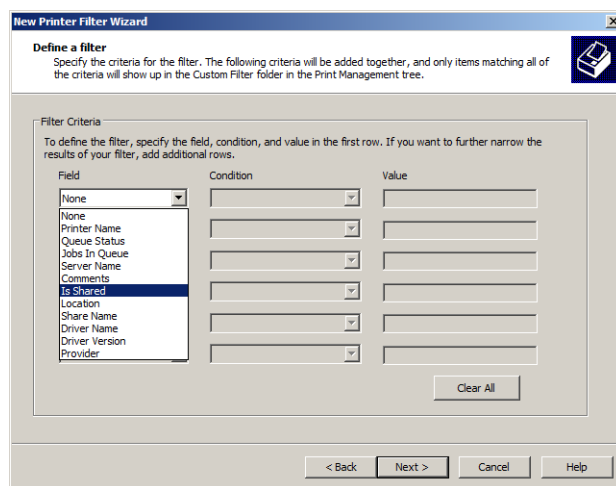
۱. بروی کانتینر Custom Filters کلیک‌راست نموده و یکی از گزینه‌های Add New Printer Filter یا Add New Driver Filter را انتخاب کنید.

۲. در صفحه "Filter Name and Description" نام و توضیحی راجع به فیلتر وارد نموده و بروی Next کلیک کنید.



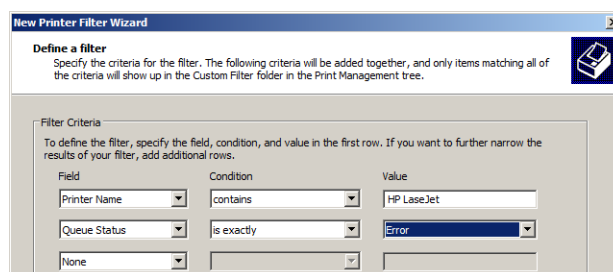
شکل ۱۰-۴۱

۳. در صفحه "Define a filter" می‌توانید با استفاده از قسمت Field، فیلترها را با توجه به موارد ارائه شده ایجاد کنید.



شکل ۱۰-۴۲

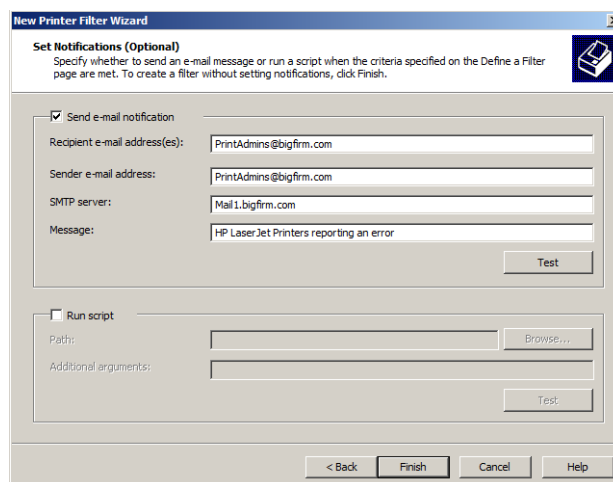
۴. بسته به نوع فیلترهای انتخابی، مجموعه‌ای از شرایط در اختیار شما قرار داده می‌شود (مانند "is exactly" یا "is not exactly"). پس از آن می‌توانید مقادیری (مانند true یا false) را برای این شرایط انتخاب کنید. به عنوان مثال در شکل زیر دو فیلتر Printer Name و Queue Status به همراه مقادیر مورد نظر برای شرایط آنها انتخاب شده است.



شکل ۱۰-۴۳

۵. پس از انتخاب فیلترها و شرایط مورد نظر، بر روی Next کلیک کنید.

۶. در صفحه "Set Notification" آپشنی به نام Send e-mail notification وجود دارد که با فعال‌سازی آن می‌توانید هشدارهایی را برای افراد یا گروهی که آدرس ایمیل آنها را در فیلدهای ارد می‌نمایید ارسال کنید. پس از انجام تنظیمات بر روی Finish کلیک کنید.



شکل ۱۰-۴۴

دقت داشته باشید که با فعال‌سازی گزینه Run script نیز می‌توانید در صورت وقوع شرایط مورد نظر، اسکریپتی را اجرا کنید.

## « فصل ۱۱ »

اتصال کاربران به سرور و دامنه

**Connecting Clients to Server and  
Domain**



پس از راه‌اندازی سرور، ایجاد کاربران و اشتراک‌گذاری منابع، لازم است که کامپیوترهای کاربران برای استفاده از این منابع پیکربندی شوند. ایجاد این اتصال باعث می‌شود که کاربران و کامپیوترهای آنها به عنوان جزئی از اکتیو دایرکتوری محسوب شوند، بنابراین می‌توانند اشیاء موجود در این پایگاه داده را مورد جستجو قرار داده و در صورت نیاز (و داشتن مجوز) از این اشیاء و سایر منابع استفاده کنند.

در این فصل قصد داریم نحوه اتصال کاربران و انجام تنظیمات مرتبط با این کار را مورد بررسی قرار داده و چگونگی جستجوی اشیاء و منابع اشتراک گذاشته شده و پس از آن استفاده از این منابع را شرح دهیم. با نگاهی به فصل‌های گذشته مشاهده خواهید نمود که اکثر تنظیمات در سمت سرور قرار دارند، اما در این فصل تنها به تنظیمات سمت کاربران پرداخته می‌شود. بطور کلی مهمترین مباحث مورد بررسی در این فصل عبارتند از:

- ♦ بررسی تنظیمات پیکربندی شبکه
- ♦ اتصال کاربر به یک دامنه
- ♦ اتصال به منابع شبکه

### ۱-۱۱ بررسی تنظیمات پیکربندی شبکه

اولین قدم در اتصال کاربران به یک شبکه مبتنی بر آدرس IP، بررسی این موضوع است که آنها قادر به برقراری ارتباط با آن شبکه باشند. برقراری این ارتباط برای همه کاربرانی که در این فصل در مورد آنها صحبت می‌کنیم با دو اقدام زیر قابل انجام می‌باشد:

- ♦ نصب یک کارت رابط شبکه (NIC) و درایور مربوط به آن بر روی کامپیوتر کاربر
- ♦ پیکربندی تنظیمات برای برقراری ارتباط با شبکه

پس از قرار دادن کارت شبکه بر روی کامپیوتر و نصب درایور مربوطه، برای اطمینان از قابلیت استفاده از آن می‌توانید مراحل زیر را دنبال کنید:

۱. بر روی Computer کلیک راست نموده و Manage را انتخاب کنید.
۲. در کنسول "Computer Management"، از پنل سمت چپ Device Manager را انتخاب کنید.
۳. در پنل سمت راست، بر روی Network Adapters کلیک کنید. در زیر مجموعه‌های Network Adapters باید نام کارت شبکه (نام درایور کارت شبکه) که نصب نموده‌اید مشاهده شود.

پس از حصول اطمینان از نصب صحیح کارت شبکه، می‌توانید کامپیوتر را برای انجام تنظیماتی که در ادامه به آنها پرداخته می‌شود آماده کنید.

### ۱-۱-۱۱ بررسی تنظیمات Local Area Connection

پس از نصب NIC بر روی کامپیوتر، یک نمایش نرم افزاری از کارت شبکه تحت عنوان Local Area Connection در Control Panel ایجاد می‌شود. علاوه بر آن دو Component دیگر به شرح زیر به این نمایش نرم افزاری اضافه می‌گردد:

- پروتکل TCP/IP که با استفاده از آن می‌توانید با سایر گره‌ها در شبکه ارتباط برقرار کنید.
- Client for Microsoft Networks که به شما اجازه می‌دهد از منابع موجود در شبکه‌های مبتنی بر مایکروسافت استفاده کنید.

بطور پیش فرض، Local Area Connection برای دریافت تنظیمات زیر از سرور DHCP پیکربندی شده است:

- **IP Address:** آدرس منطقی است که به هر کامپیوتر (یا دستگاه تحت شبکه) اختصاص داده شده و برای هر دستگاه در یک شبکه منحصر بفرد می‌باشد.
- **Subnet Mask:** شماره‌ای است که بطور منطقی شبکه‌های بزرگ را به زیر شبکه‌های کوچکتر تقسیم می‌کند (به فصل اول مراجعه نمایید).
- **Default Gateway:** آدرس Router است که ارتباط میان گره‌های موجود در زیر شبکه‌ها و یا شبکه‌های مختلف را برقرار می‌کند.
- **Domain Name System (DNS) Server:** آدرس سرور DNS شبکه است.
- **DNS Suffix:** (اختیاری): نام دامنه اکتیو دایرکتوری است که کامپیوتر به آن متصل می‌گردد.

سریع‌ترین راه جهت آگاهی از تنظیمات دریافت شده توسط کارت شبکه استفاده از دستور `ipconfig /all` در خط فرمان می‌باشد. اجرای این دستور نتیجه‌ای شبیه زیر در پی خواهد داشت.

```

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

C:\Users\Yazdani>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Win7Client
Primary Dns Suffix . . . . . : bigfirm.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : bigfirm.com

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . : 
Description . . . . . : Atheros AR8161/8165 PCI-E Gigabit Ethernet Con
Physical Address. . . . . : 00-15-5D-02-15-01
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Site-local IPv6 Address . . . . . : fec0::1111:2731:e2ff:fe96:c311%1(Preferred)
Link-local IPv6 Address . . . . . : fe80::b845:5803:fc1f:8ced%11(Preferred)
IPv4 Address. . . . . : 192.168.1.193(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, September 10, 2013 6:51:03 PM
Lease Expires . . . . . : Wednesday, September 11, 2013 6:50:59 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.2
DHCPv6 Iaid . . . . . : 234886493
DHCPv6 Client DUID. . . . . : 00-01-00-01-19-06-55-BD-00-15-5D-02-15-01
DNS Servers . . . . . : fec0::1111:2731:e2ff:fe96:c283%1
192.168.1.21
NetBIOS over Tcpip. . . . . : Enabled
  
```

شکل ۱-۱۱

در شکل بالا، خطوطی که در قسمت Ethernet Adapter Local Area Connection قرار دارند، تنظیمات دریافت شده برای کارت شبکه را نشان می‌دهند:

- ♦ **DHCP Enabled**: چنانچه این گزینه با Yes تنظیم شده باشد، کارت شبکه تنظیمات خود را از سرور DHCP دریافت می‌کند. اگر این گزینه با No مقداردهی شود، کارت شبکه باید به صورت دستی برای دریافت تنظیمات پیکربندی گردد.
  - ♦ **Autoconfiguration Enabled**: این گزینه با Yes مقداردهی شده و زمانی نشان داده می‌شود که کارت شبکه اطلاعات خود را از سرور DHCP دریافت می‌کند.
  - ♦ **Lease Obtained**: نشان‌دهنده Lease (اجاره) است که توسط سرویس DHCP به کاربر اختصاص داده می‌شود.
  - ♦ **Lease Expires**: تاریخ اتمام Lease را نشان می‌دهد.
  - ♦ **IPv4 Address**: آدرس IP منحصر بفردی است که به Local Area Connection اختصاص داده شده است.
  - ♦ **Subnet Mask**: آدرس قاب زیرشبکه‌ای است که گره مورد نظر در آن قرار گرفته است.
  - ♦ **Default Gateway**: آدرس Router ای است که میان شبکه فعلی و سایر زیرشبکه‌ها/شبکه‌ها ارتباط برقرار می‌کند.
  - ♦ **DNS Servers**: آدرس DNS سرور شبکه می‌باشد. چنانچه قصد داشته باشید به یک دامنه متصل شوید، حتما باید برای تحلیل آدرس‌های IP به نام کامپیوترها از سرور DNS استفاده کنید.
- در صورتی که گزینه‌های بالا با No مقداردهی شده و یا در این تنظیمات نمایش داده نشوند، ممکن است از سرور DHCP استفاده نشده باشد. در این حالت می‌توانید تنظیمات NIC را به صورت دستی انجام دهید.

#### ۱۱-۲-۱ تست ارتباط شبکه با دستور Ping

پس از اینکه کارت شبکه را بروی کامپیوتر خود نصب نموده و تنظیمات مربوط به آنرا پیکربندی نمودید، می‌توانید برای اطمینان از انجام صحیح این تنظیمات از دستور Ping استفاده کنید. با استفاده از این دستور می‌توان از برقراری ارتباط با یک کاربر، یک ماشین (یا سرور)، آدرس IP، و یا یک سایت اینترنتی (مانند yahoo.com) اطمینان حاصل نمود.

برای استفاده از دستور Ping کافی است آدرس IP، نام ماشین و یا آدرس سایت اینترنتی را پس از این دستور وارد کنید. در شکل ۱۱-۲ دو مثال در این زمینه نشان داده شده است.



```

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

C:\Users\Vazdani>ping 192.168.1.101

Pinging 192.168.1.101 with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Vazdani>ping yahoo.com

Pinging yahoo.com [206.190.36.45] with 32 bytes of data:
Reply from 206.190.36.45: bytes=32 time=419ms TTL=36
Reply from 206.190.36.45: bytes=32 time=425ms TTL=37
Reply from 206.190.36.45: bytes=32 time=469ms TTL=36
Reply from 206.190.36.45: bytes=32 time=483ms TTL=36

Ping statistics for 206.190.36.45:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 419ms, Maximum = 483ms, Average = 449ms

```

شکل ۲-۱۱



برای تست ارتباط میان ماشین خود و سرورهای شبکه می‌توانید دستور Ping را به صورت Ping bfl.bigfirm.com که در آن نام ماشین به همراه نام دامنه قرارگیری آن می‌باشد وارد کنید. همچنین برای تست ارتباط با خود نیز می‌توانید از دستورات Ping localhost و Ping 127.0.0.1 استفاده کنید.

دقت داشته باشید که در دستور Ping ممکن است با پیغام‌های "Request timed out" و "Destination host unreachable" نیز مواجه شوید. این پیغام‌ها به دلیل عدم برقراری ارتباط میان دو ماشین تست شونده، و یا عدم پذیرش دستور Ping توسط مقصد می‌باشد (به عنوان مثال سایت Microsoft.com دستور Ping را قبول نمی‌کند). این مشکل ممکن است به دلایلی مانند عدم پیکربندی صحیح سرور DNS و یا فعال بودن فایروال و یا حتی وجود مشکلات سخت افزاری در ارتباط باشد. در شکل ۳-۱۱ عدم برقراری ارتباط و همچنین عدم پذیرش دستور Ping نشان داده شده است.

```

C:\Windows\system32\cmd.exe
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Vazdani>ping 192.168.1.107

Pinging 192.168.1.107 with 32 bytes of data:
Reply from 192.168.1.101: Destination host unreachable.
Reply from 192.168.1.101: Destination host unreachable.
Reply from 192.168.1.101: Destination host unreachable.
Reply from 192.168.1.101: Destination host unreachable.

Ping statistics for 192.168.1.107:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Vazdani>ping microsoft.com

Pinging microsoft.com [65.55.58.201] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 65.55.58.201:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

شکل ۳-۱۱

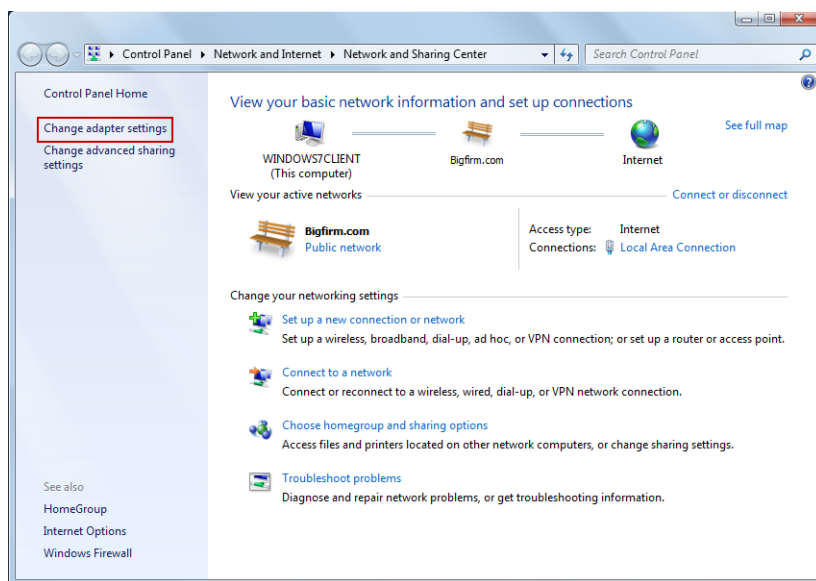
### ۱۱-۳ بررسی تنظیمات Local Area Connection با استفاده از GUI

بازبینی و پیکربندی تنظیمات Local Area Connection با استفاده از واسطه‌های گرافیکی نیز امکان‌پذیر می‌باشد. استفاده از این ابزارهای گرافیکی به این دلیل مهم هستند که در صورت عدم وجود DHCP (برای پیکربندی خودکار تنظیمات) بتوانید NIC را برای برقراری ارتباط با شبکه پیکربندی کنید.

#### پیکربندی دستی تنظیمات Local Area Connection در ویندوز ۷

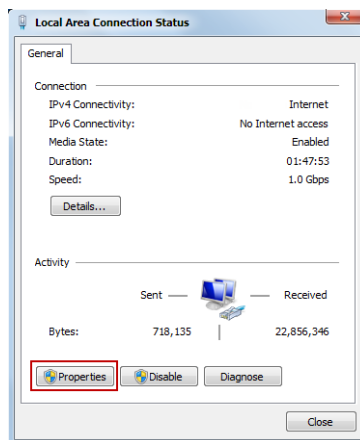
در ویندوز ۷ برای دسترسی به Local Area Connections و پیکربندی تنظیمات شبکه برروی آن مراحل زیر را دنبال کنید:

۱. به مسیر «Control Panel» «Network and Internet» «Network and Sharing Center» بر روی کلیک کنید.
۲. در پنجره باز شده بر روی Change Adapter Settings کلیک کنید.



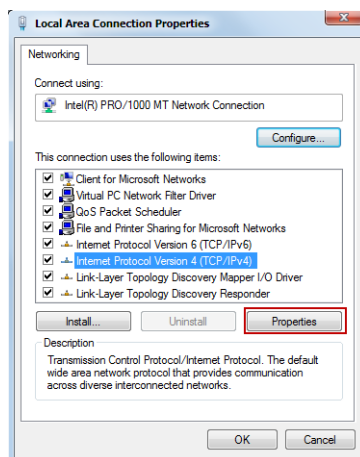
شکل ۱۱-۴

۳. در پنجره «Network Connections» بر روی Local Area Connection کلیک راست نموده و Status را انتخاب کنید.
۴. در پنجره «Local Area Connection Status» جهت مشاهده اطلاعات پیکربندی کارت شبکه، بر روی Details کلیک کنید.
۵. پس از مشاهده، جهت پیکربندی تنظیمات در همان پنجره بر روی Properties کلیک کنید.



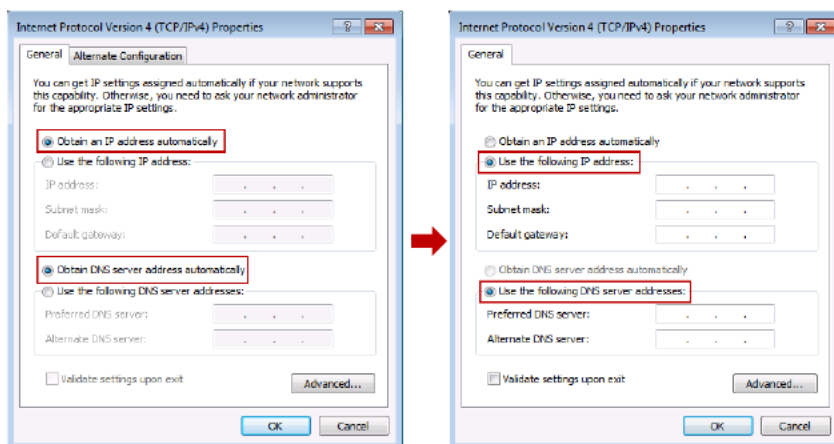
شکل ۱۱-۵

۶. در پنجره “Local Area Connection Properties” گزینه Internet Protocol Version 4 (TCP/IPv4) را انتخاب نموده و بر روی Properties کلیک کنید.



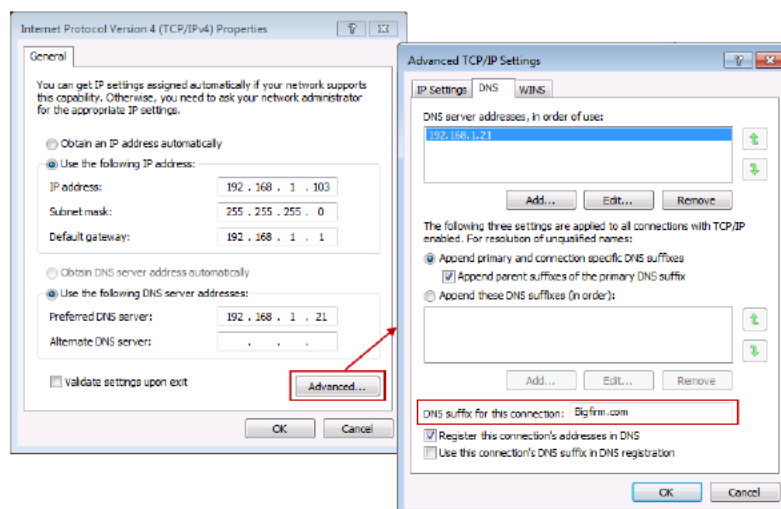
شکل ۱۱-۶

۷. کارت شبکه بطور پیش فرض تنظیمات خود را از سرویس DHCP در یافت می کند. برای پیکربندی دستی این تنظیمات لازم است گزینه های Obtain an IP address automatically و Obtain DNS server address را به ترتیب به گزینه های Use the following IP address و Use the following DNS server address تغییر دهید. در شکل ۱۱-۷ این وضعیت نشان داده شده است.



شکل ۷-۱۱

۸. در قسمت‌های IP address، Subnet mask، Default gateway و Preferred DNS server، به ترتیب مقادیر آدرس IP میزبان، قاب زیرشبکه، آدرس Router و آدرس سرور DNS را وارد کنید.
۹. با کلیک بر روی دکمه Advances و انتخاب تب DNS می‌توانید نام دامنه (Bigfirm.com) را به عنوان DNS Suffix اضافه کنید.



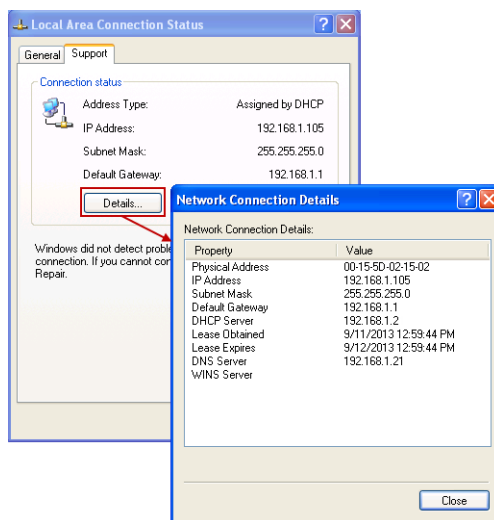
شکل ۸-۱۱

۱۰. پس از انجام تنظیمات بر روی OK کلیک نموده و پنجره‌ها را ببندید.

### پیکربندی دستی تنظیمات Local Area Connection در ویندوز XP

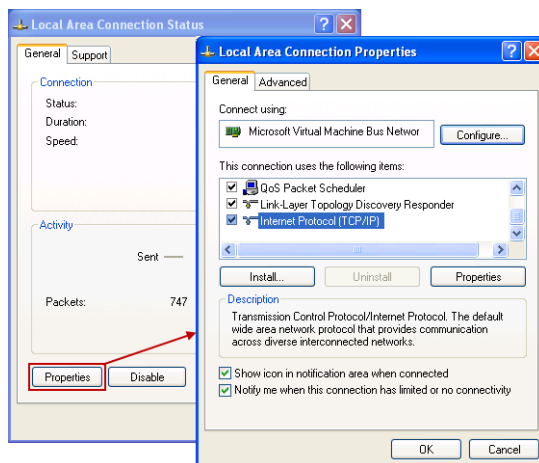
برای دسترسی به تنظیمات کارت شبکه در ویندوز XP مراحل زیر را دنبال کنید:

۱. به مسیر «Start» «Control Panel» «Network Connections» حرکت کنید.
۲. در پنجره «Network Connections» بروی Local Area Connection کلیک راست نموده و Status را انتخاب کنید.
۳. در پنجره «Local Area Connection Status» جهت مشاهده اطلاعات پیکربندی کارت شبکه، تب Support را انتخاب نموده و بروی Details کلیک کنید.



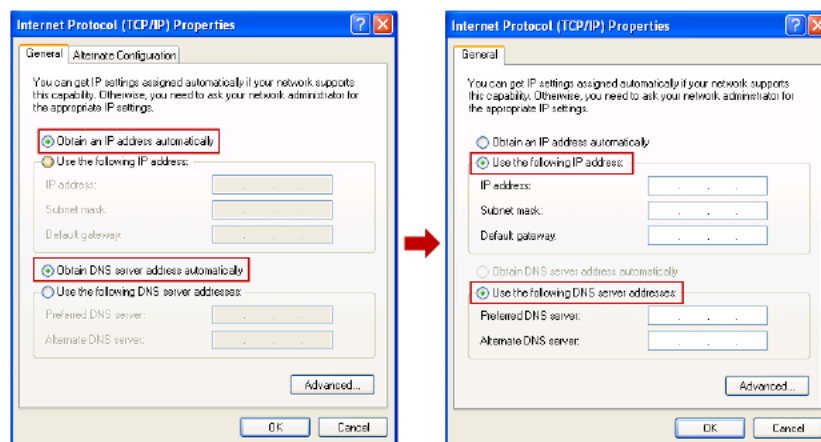
شکل ۹-۱۱

۴. پس از مشاهده تنظیمات، به تب General بروی Properties کلیک کنید.



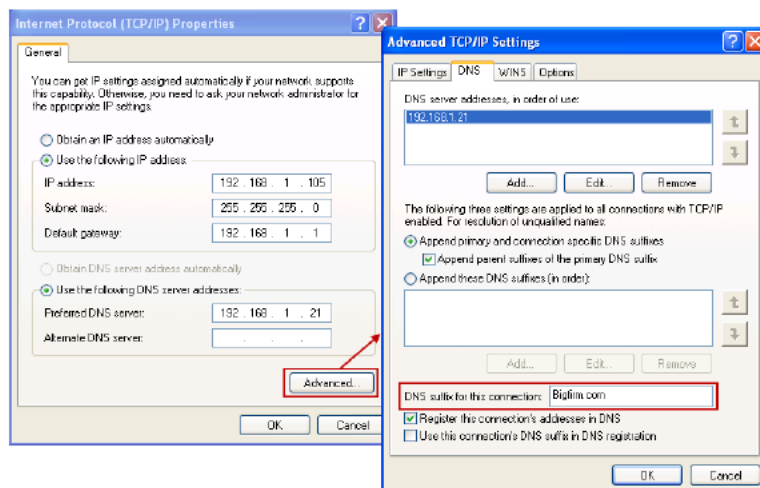
شکل ۱۰-۱۱

۵. در پنجره "Local Area Connection Properties" گزینه Internet Protocol (TCP/IP) را انتخاب نموده و بر روی Properties کلیک کنید.
۶. برای پیکربندی دستی تنظیمات، گزینه‌های Obtain an IP address automatically و Obtain DNS server address automatically را به ترتیب به گزینه‌های Use the following IP address و Use the following DNS server address تغییر دهید.



شکل ۱۱-۱۱

۷. در قسمت‌های IP address، Subnet mask، Default gateway و Preferred DNS server، به ترتیب مقادیر آدرس IP میزبان، قاب زیرشبکه، آدرس Router و آدرس سرور DNS را وارد کنید. همچنین با کلیک بر روی دکمه Advances و انتخاب تب DNS نیز می‌توانید نام دامنه (Bigfirm.com) را به عنوان DNS Suffix وارد کنید.



شکل ۱۱-۱۲

۸. پس از انجام تنظیمات بر روی Ok کلیک کنید.

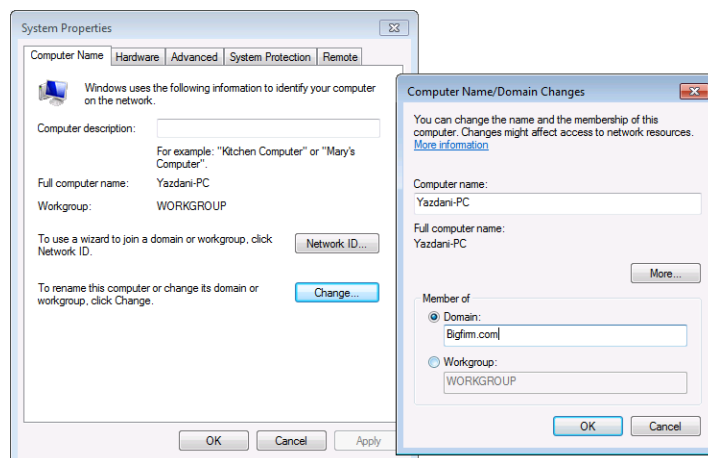
## ۱۱-۲ اتصال به دامنه

پس از پیکربندی تنظیمات شبکه بر روی کامپیوترهای کاربران، می‌توانید آنها را به دامنه متصل نموده تا از منابع اشتراک گذاشته شده در داخل دامنه و اکتیو دایرکتوری استفاده کنند. قبل از پرداختن به این موضوع، لازم است متذکر شویم که جهت اتصال کاربران به دامنه، داشتن یک حساب کاربری با مجوز مدیر دامنه و یا مجوز اتصال کاربران به دامنه ضروری می‌باشد. بنابراین می‌توانید با استفاده از حساب کاربری Administrator (مدیر دامنه) و یا حساب کاربری مانند BigfirmAdmin که آنرا در گروه Domain Admins (گروه پیش‌فرض جهت قرارگیری حساب‌های کاربری مدیران دامنه) ایجاد کرده‌اید نسبت به انجام اتصال کاربران به دامنه اقدام کنید.

## ۱۱-۲-۱ اتصال به دامنه با استفاده از ویندوز ۷

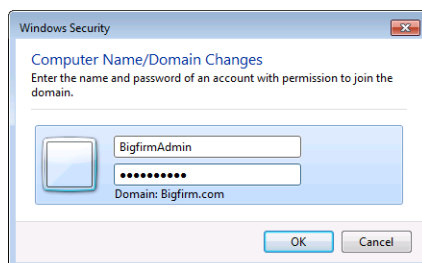
برای اتصال به دامنه با استفاده از GUI مراحل زیر را دنبال کنید:

۱. از منوی Start بر روی Computer کلیک‌راست نموده و Properties را انتخاب کنید.
۲. در پنجره "System Properties" بر روی Change Settings کلیک کنید.
۳. در تب Computer Name بر روی دکمه Change کلیک کنید.
۴. در قسمت Member of از پنجره "Computer Name/Domain Changes"، گزینه Domain را انتخاب نموده و نام دامنه‌ای که قصد دارید به آن متصل شوید (در اینجا Bigfirm.com) را وارد کنید، سپس بر روی Ok کلیک کنید.



شکل ۱۱-۱۳

۵. در پنجره "Windows Security" مشخصات حساب کاربری که دارای مجوز اتصال به دامنه است را وارد نموده (در اینجا BigfirmAdmin یا Administrator) و بر روی OK کلیک کنید.

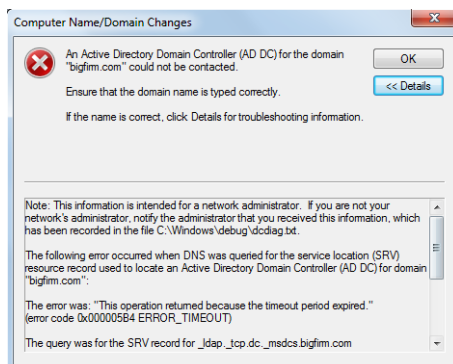


شکل ۱۱-۱۴

۶. پیغامی ظاهر شده و ورود شما به دامنه را خوشامد می‌گوید. بر روی OK کلیک کنید.
۷. مجدداً پیغامی ظاهر شده و اعلام می‌کند که کامپیوتر باید Restart شود. بر روی OK کلیک نموده و کامپیوتر را Restart کنید.

چنانچه در هنگام اتصال کاربر به دامنه با مشکل و یا خطایی مواجه شدید، موارد زیر را بررسی کنید:

- حساب کاربری که از آن جهت اتصال کاربر به دامنه استفاده می‌شود بطور صحیح وارد شده باشد.
- وارد نمودن صحیح نام دامنه و همچنین حصول اطمینان از امکان برقراری ارتباط میان کاربر و سرور DNS در دامنه. چنانچه با این مشکل مواجه شوید خطای زیر نمایش داده می‌شود و برای رفع آن باید پیکربندی و اتصال سرور DNS را بررسی نمایید.



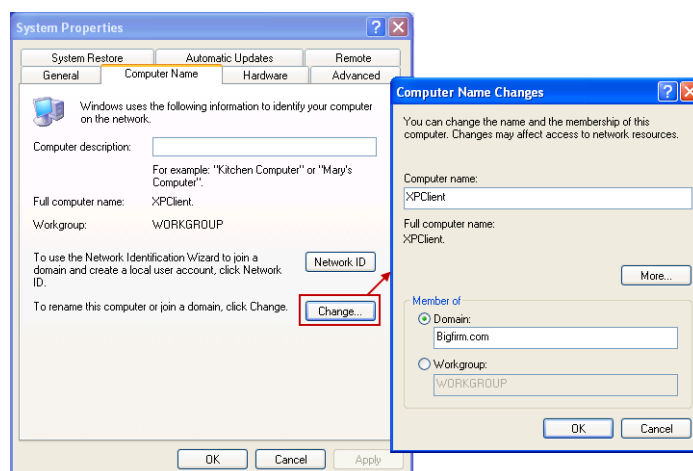
شکل ۱۱-۱۵



## ۱۱-۲-۲ اتصال به دامنه با استفاده از ویندوز XP

برای پیوستن به دامنه با استفاده از ویندوز XP مراحل زیر را دنبال کنید:

۱. از منوی Start بروی My Computer کلیک راست نموده و Properties را انتخاب کنید.
۲. در صفحه "System Properties" تب Computer Name را انتخاب نموده و بر روی دکمه Change کلیک کنید.
۳. در قسمت Member of از پنجره "Computer Name Changes"، گزینه Domain را انتخاب نموده و سپس نام دامنه (Bigfirm.com) را وارد کنید. سپس بر روی OK کلیک کنید.



شکل ۱۱-۱۶

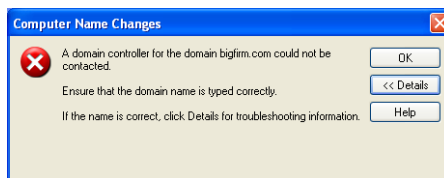
۴. مشخصات حساب کاربری دارای مجوز اتصال به دامنه را وارد نموده و بر روی OK کلیک کنید.



شکل ۱۱-۱۷

۸. با مشاهده پیغام خوشامدگویی بر روی OK کلیک نموده و سپس کامپیوتر را Restart کنید.
۹. چنانچه در حین اتصال با پیغام زیر مواجه شدید، باید تنظیمات سرور DNS و همچنین نام دامنه

را بررسی نموده و در صورت وجود هرگونه مغایرت، نسبت به برطرف نمودن آن اقدام کنید.



شکل ۱۱-۱۸

### ۱۱-۳ اتصال به منابع شبکه

یکی از بزرگترین دلایل اتصال کاربران به دامنه، استفاده از منابع موجود در دامنه مانند پرینتر است. مزیت دسترسی به منابع شبکه و استفاده از آنها در این است که می‌توانید به انواع فایل‌های صوتی، تصویری و ... دسترسی پیدا نموده و آنها را مورد استفاده قرار دهید، بدون اینکه نیازی به ذخیره‌سازی آنها بر روی کامپیوتر خود داشته باشید. همچنین با استفاده از ارتباطات شبکه‌ای دسترسی به منابع نیز امن‌تر می‌شود زیرا شبکه از طریق یک نقطه مرکزی مورد کنترل قرار می‌گیرد. نمونه‌هایی از منابع شبکه عبارتند از:

- ♦ پرینترها
- ♦ فایل‌ها و پوشه‌های اشتراک گذاشته شده
- ♦ دستگاه‌های بیسیم (مانند پرینتر بیسیم)
- ♦ سرویس‌ها
- ♦ سایر کامپیوترها

با استفاده از Network Discovery و Active Directory دسترسی به منابع شبکه بسیار آسان شده است. Network Discovery تنظیماتی است که به کاربران اجازه می‌دهد منابع اشتراک گذاشته شده در شبکه را به سادگی پیدا نموده و مورد استفاده قرار دهند. همچنین به سایر کامپیوترها در شبکه امکان می‌دهد تا کاربران موجود در کامپیوتر شما را مشاهده نموده و قادر باشند منابع اشتراک گذاشته بر روی کامپیوتر را به آسانی پیدا کنند. تنظیمات Network Discovery از مسیر «Start» «Control Panel» «Network and sharing Center» «Change advanced sharing settings» قابل دسترسی می‌باشند.

علاوه بر Network Discovery، می‌توان با استفاده از ابزار Search Active Directory نیز به منابع انتشار یافته در شبکه (دامنه) دسترسی پیدا نمود، بنابراین دیگر نیازی به دانستن محل قرارگیری دستگاه‌ها، پوشه‌ها و یا پرینترهای اشتراک گذاشته شده در شبکه وجود نخواهد داشت و تنها با

جستجویی ساده در اکتیو دایرکتوری می‌توان به همه این منابع دسترسی پیدا کرد. تعدادی روش جهت دسترسی به منابع اشتراک گذاشته شده در شبکه استفاده می‌شود که از جمله می‌توان به: استفاده از ابزار Search Active Directory، استفاده از خط فرمان، استفاده از مسیر قرار گیری پوشه اشتراکی (مانند \\ComputerName\ShareName) اشاره نمود. به عنوان تعدادی مثال، در جدول زیر دسترسی به منابع قرارگرفته شده بر روی دامنه Bigfirm.com نشان داده شده است.

جدول ۱-۱۱: مثال‌هایی در رابطه با دسترسی به منابع شبکه

نوع منابع شبکه	مسیر قرار گیری در شبکه	ماشین قرار گیری منابع
فایل اشتراکی Finance	\\bfl\BF_Finance	bfl.bigfirm.com
فایل اشتراکی Marketing	\\bfl\BF_Marketing	bfl.bigfirm.com
فایل اشتراکی HR	\\bfl\BF_HR	bfl.bigfirm.com
پرینتر سیاه و سفید	\\bfl\BF_Main_Printer	bfl.bigfirm.com
پرینتر رنگی	\\windows7client\HP_LJ_2800	windows7client.bigfirm.com



همانطور که اطلاع دارید، جهت مشاهده دستگاه‌های متصل به شبکه و منبع اشتراک گذاشته شده بر روی آنها، از پنجره "Network" استفاده می‌شود. برای سادگی و دسترسی آسان به این پنجره می‌توانید آیکن Network را به صفحه Desktop اضافه نمایید. جهت انجام این کار مراحل زیر را در ویندوز ۷ دنبال کنید:

۱. در صفحه Desktop کلیک راست نموده و Personalize را انتخاب کنید.
۲. در پنل سمت چپ بر روی Change Desktop Icons کلیک کنید.
۳. گزینه Network را انتخاب نموده و بر روی OK کلیک کنید.

همچنین جهت افزودن این دکمه به منوی Start نیز می‌توانید مراحل زیر را دنبال کنید:

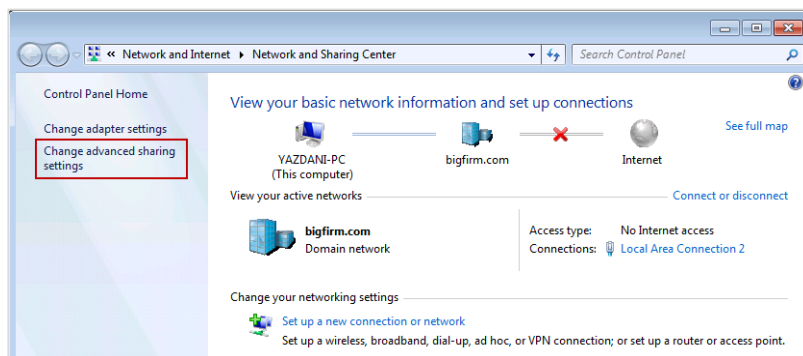
۱. بر روی منوی Start کلیک راست نموده و Properties را انتخاب کنید.
۲. تب Start Menu را انتخاب نموده و بر روی Customize کلیک کنید.
۳. در پنجره "Customize Start Menu" گزینه Network را انتخاب نموده و بر روی OK کلیک کنید.

### ۱-۳-۱۱ اتصال به منابع با استفاده از ویندوز ۷

در ویندوز ۷ آپشن Network Discovery بطور پیش فرض غیرفعال است بنابراین کامپیوتر شما و منابع اشتراک گذاشته شده در آن برای سایر کامپیوترها قابل مشاهده نمی‌باشد. برای فعال کردن این

گزینه مراحل زیر را دنبال کنید:

۱. از مسیر «Start» «Control Panel» «Network and Internet»، گزینه Network and Sharing Center را انتخاب کنید.
۲. در پنل سمت چپ از پنجره باز شده، بروی Change Advanced Sharing Settings کلیک کنید.



شکل ۱۱-۱۹

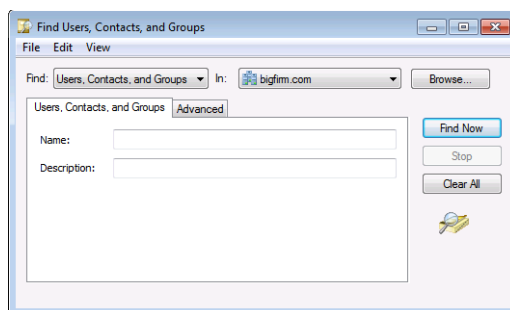
۳. چون کامپیوتر شما به دامنه متصل است، Advanced Sharing Settings برای پروفایل دامنه باز می‌شود. در قسمت Network Discovery آپشن “Turn on network discovery” را انتخاب کنید.
۴. سایر گزینه‌های موجود در Advanced Sharing Settings به شما کمک می‌کنند که فایل‌ها و پرینترهای قرارگرفته بروی کامپیوتر خود را با کاربران و کامپیوترها در دامنه به اشتراک گذارید. بنابراین با توجه به نیاز خود، تنظیمات مورد نظر را انجام داده و بروی Save Changes کلیک کنید.

### جستجو در اکتیو دایرکتوری

اکنون که گزینه Network Discovery فعال است، کاربران به راحتی می‌توانند همدیگر را در شبکه جستجو کنند. یکی از سریعترین راه‌هایی که برای آگاهی از منابع اشتراک گذاشته شده در شبکه مورد استفاده قرار می‌گیرد، استفاده از ابزار Search Active Directory است که با استفاده از آن می‌توانید انواع اشیاء و منابع شبکه را جستجو کنید. برای دسترسی به این ابزار در ویندوز ۷ مراحل زیر را دنبال کنید:

۱. در پنجره “Computer”، بروی گزینه Network که در پنل سمت چپ قرار دارد کلیک کنید.
۲. پس از بازشدن پنجره، در نوار بالای آن بروی بروی دکمه Search Active Directory کلیک کنید.
۳. پنجره “Find Users, Groups, and Contacts” ظاهر می‌شود. در این پنجره امکان دسترسی به منابع

اشتراک گذاشته شده (و قابل جستجو) در اکتیو دایرکتوری از جمله کامپیوترها، پوشه‌های اشتراکی، پرینترها و مواردی مانند کاربران و گروه‌ها فراهم می‌گردد. جهت جستجوی یک شیء کافی است در قسمت Find نوع شیء را مشخص نموده و بر روی دکمه Find Now کلیک کنید.



شکل ۱۱-۲۰

### افزودن پرینتر شبکه

برای افزودن پرینتر شبکه، به سه روش می‌توان اقدام نمود: جستجو در اکتیو دایرکتوری، استفاده از خط فرمان و استفاده از آپلت<sup>۱</sup> Network.

### جستجو در اکتیو دایرکتوری

برای افزودن پرینتر در این روش از ابزار Search Active Directory استفاده می‌شود. بدین منظور در قسمت Find از پنجره "Find Users, Groups, and Contacts" گزینه Printers را انتخاب نموده و بر روی Find Now کلیک کنید. پس از کلیک، لیستی از پرینترهای منتشر شده در اکتیو دایرکتوری ظاهر می‌شود. برای افزودن پرینتر مورد نظر، بر روی آن کلیک‌راست نموده و گزینه Connect را انتخاب نمایید. پس از آن پرینتر نصب شده و می‌توانید از آن استفاده کنید.

### افزودن پرینتر با استفاده از خط فرمان

جهت افزودن پرینتر با استفاده از خط فرمان، به نام پرینتر نیاز است. پس از اینکه از نام پرینتر آگاهی پیدا نمودید، با استفاده از دستور Start می‌توانید آنرا به کامپیوتر خود اضافه کنید. به عنوان مثال برای افزودن پرینتری با نام bf\_main\_printer که بر روی سرور bf1 قرار دارد، می‌توانید از دستور زیر استفاده کنید:

```
start \\bf1\bf_main_printer
```

پس از افزوده شدن و نصب پرینتر می‌توانید آنرا در قسمت Devices and Printers که در منوی

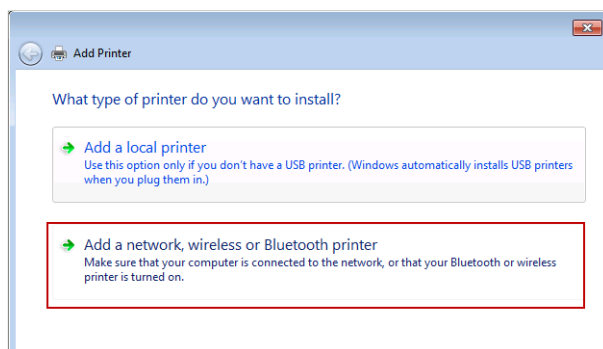
1. Applet

Start قرار دارد مشاهده کنید.

### افزودن پرینتر با استفاده از اپلت Network

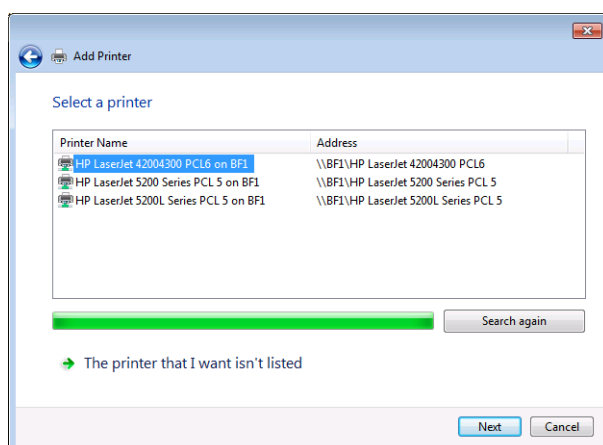
امکان افزودن پرینتر شبکه با استفاده از اپلت Network نیز فراهم گردیده است. برای استفاده از این ابزار مراحل زیر را دنبال کنید:

۱. پس از باز کردن پنجره «Network»، بروی Add a Printer کلیک کنید (این گزینه از مسیر «Start» «Device and Printers» «Add a Printer» نیز قابل دسترسی می‌باشد).
۲. پس از اجرای ویزارد «Add Printer»، بروی گزینه دوم یعنی Add a network, wireless or Bluetooth printer کلیک کنید.



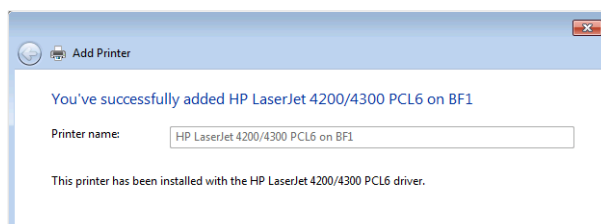
شکل ۱۱-۲۱

۳. پس از اتمام جستجو، در صفحه «Select Printer» پرینتر مورد نظر را انتخاب نموده و بروی Next کلیک کنید.



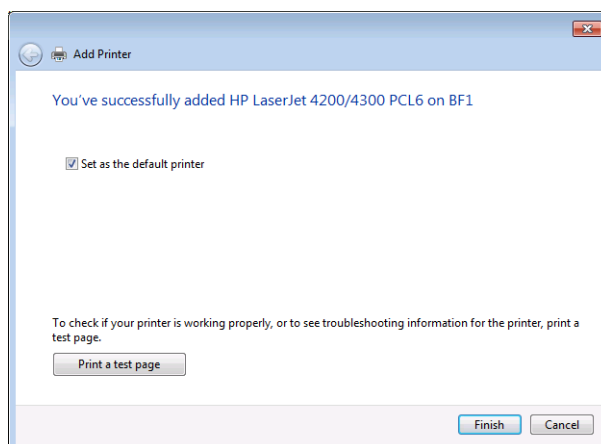
شکل ۱۱-۲۲

۴. در صفحه بعد نام پرینتر به همراه موفقیت آمیز بودن نصب درایور آن اعلام می‌شود. برروی Next کلیک کنید.



شکل ۱۱-۲۳

۵. در آخر نیز برای قرار دادن پرینتر به عنوان پرینتر پیش‌فرض، گزینه Set as default printer را فعال نمایید. با کلیک برروی Print a test page نیز می‌توانید امکان استفاده از آنرا امتحان کنید. در نهایت برروی Finish کلیک کنید.

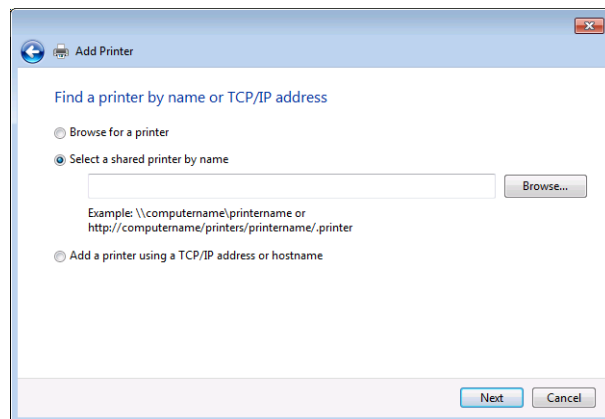


شکل ۱۱-۲۴

ممکن است در طی ویزارد "Add Printer" پرینتر مورد نظر شما در فهرست پرینترها قرار نداشته باشد. در اینصورت می‌توانید در مرحله ۳ (شکل ۱۱-۲۲) گزینه The printer that I want isn't listed را انتخاب کنید. انتخاب این گزینه، سه آپشن برای پیدا کردن پرینتر در اختیار شما قرار می‌دهد:

- ♦ جستجوی اکتیو دایرکتوری برای افزودن پرینتر
- ♦ وارد کردن نام پرینتر و محل قرارگیری آن (به صورت \\ServerName\PrinterName)
- ♦ وارد کردن آدرس IP پرینتر (که این نوع پرینتر با نام TCP/IP printer شناخته می‌شود).

با توجه به گزینه انتخابی، مراحل را پیش رفته و پرینتر مورد نظر را اضافه کنید.

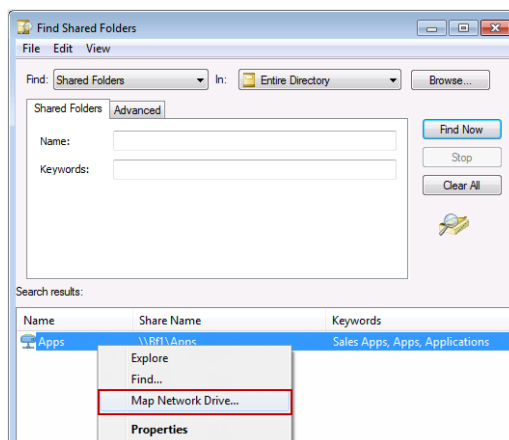


شکل ۱۱-۲۵

### نگاشت یک درایو برای پوشه‌های اشتراک گذاشته شده

گاهی اوقات استفاده از یک درایو بجای استفاده از مسیرهای UNC، جهت اتصال به پوشه‌های اشتراک گذاشته شده در شبکه ساده‌تر است. درایوهایی که به این منظور ایجاد می‌شوند، در کنار سایر درایوهای کامپیوتر قرار می‌گیرند اما تنها جهت دسترسی به پوشه‌های اشتراک گذاشته شده در شبکه استفاده می‌شوند. درایوهای شبکه در ویندوز ۷ با استفاده از ویژگی‌های به نام «Map Network Drive» ایجاد می‌شوند. جهت راه‌اندازی این ویژگی در ویندوز ۷ می‌توانید مراحل زیر را دنبال کنید:

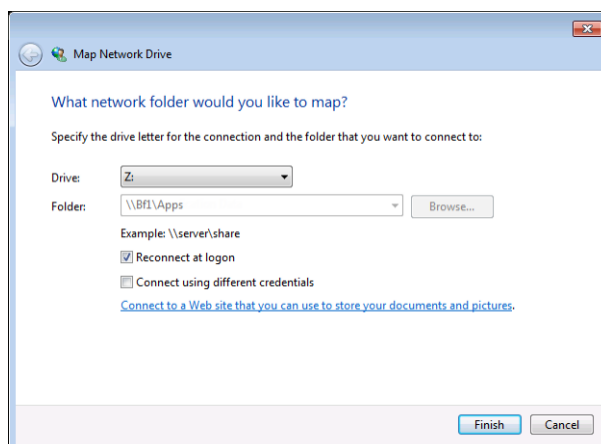
۱. اپلت Network را باز نموده (Start «Network») و بروی Search Active Directory کلیک کنید.
۲. در قسمت Find، گزینه Shared Folders را انتخاب نموده و بروی Find Now کلیک کنید.
۳. بروی پوشه مورد نظر (در اینجا Apps) کلیک راست نموده و Map Network Drive را انتخاب کنید.



شکل ۱۱-۲۶



۴. هر درایوی که برای پوشه‌های اشتراکی نگاشت می‌شود باید دارای یک نام منحصر بفرد باشد (مانند X، Z و ...)، بنابراین در صفحه "What network folder would you like to map?" یک نام برای درایو انتخاب نموده و همچنین گزینه Reconnect at logon را نیز فعال کنید (این گزینه باعث می‌شود که کاربر در هنگام ورود به شبکه بتواند به درایو متصل شود). در نهایت بر روی Finish کلیک کنید.

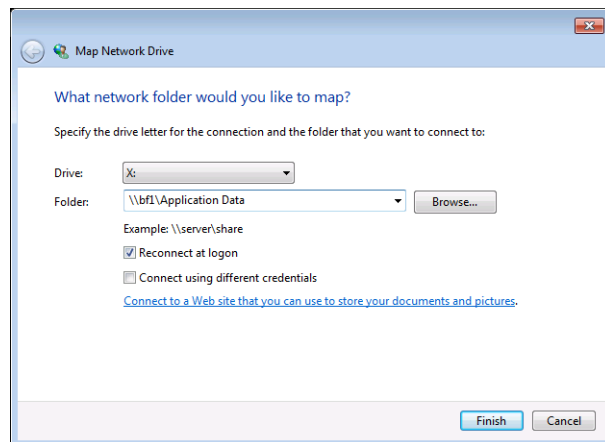


شکل ۱۱-۲۷

۵. پس از ایجاد درایو، جهت دسترسی به آن می‌توانید به مسیر «Start Computer» رفته و سپس بر روی نام درایوی که ایجاد نموده‌اید دابل‌کلیک کنید. برای قطع ارتباط با این درایو نیز می‌توانید بر روی آن کلیک‌راست نموده و Disconnect را انتخاب کنید.

دقت داشته باشید که بعضی از پوشه‌های اشتراکی در فهرست اکتیو دایرکتوری قرار نمی‌گیرند، بنابراین برای نگاشت درایو به آنها ممکن است کمی با زحمت مواجه شوید. اما جای نگرانی در این زمینه نیست زیرا می‌توانید با کمی تغییر در مراحل قبل، درایو مورد نظر را به پوشه اشتراکی نگاشت کنید:

۱. از منوی Start بر روی Computer کلیک‌راست نموده و Map Network Drive را انتخاب کنید.
۲. یکی از حروفی که تاکنون انتخاب نشده است را از لیست حروف انتخاب کنید.
۳. مسیر قرارگیری پوشه اشتراکی را وارد نموده (مانند \\bf1\Application Data) و یا با استفاده از دکمه Browse آنها در شبکه جستجو کنید، سپس بر روی Finish کلیک کنید. دقت داشته باشید که این پوشه‌ها باید توسط سرویس Share and Storage Management در File Service به اشتراک گذاشته شده باشند.



شکل ۱۱-۲۸

### نگاشت درایو شبکه در خط فرمان

نگاشت درایو برای پوشه‌های اشتراک گذاشته شده با استفاده از خط فرمان نیز امکان‌پذیر است. مثال زیر با استفاده از دستور `net use` یک درایو به نام Z برای پوشه اشتراکی Apps ایجاد می‌کند:

```
net use Z: \\bf1\\Apps /PERSISTENT:YES
```

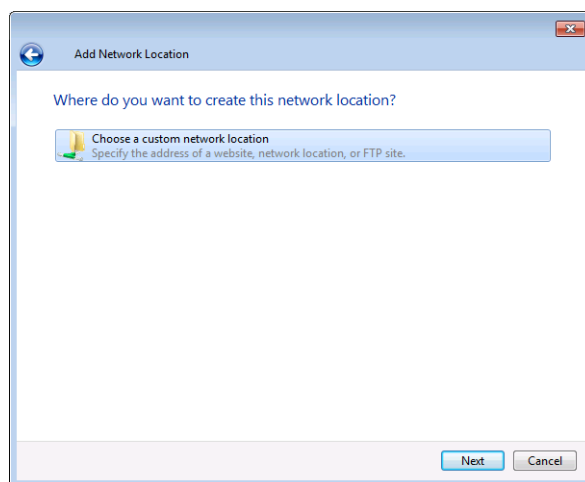
در دستور بالا عبارت `PERSISTENT:YES` معادل با انتخاب گزینه `Reconnect at logon` است که بطور خودکار کاربر را در هنگام ورود به کامپیوتر به این درایو متصل می‌کند. برای دسترسی به لیست کلیه پارامترهای قابل استفاده در دستور `net use` می‌توانید از دستور `net use /?` استفاده کنید.

در آخر نیز چنانچه از منابع اشتراک گذاشته شده بر روی سرور اطلاع ندارید، می‌توانید از دستور `net view` استفاده کنید. این دستور لیست منابع اشتراک گذاشته شده بر روی سرور را به شما نشان خواهد داد. برای استفاده از دستور آنرا به صورت `Net view \\computername` وارد کنید (مانند `Net view \\bf1`).

### Network Folder

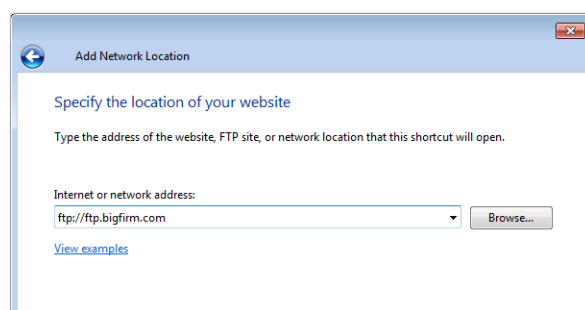
یکی دیگر از روش‌هایی که برای ایجاد درایو نگاشت شده به منابع شبکه استفاده می‌شود، ایجاد Network Folder (پوشه شبکه) است. تفاوت این روش با Map Network Drive در این است که Map Network Drive برای منابع محلی شبکه ایجاد می‌شود اما با استفاده از Network Folder می‌توان علاوه بر منابع موجود در شبکه، برای منابع موجود در اینترنت (مانند سایت‌های http و ftp) نیز درایو ایجاد نمود. جهت ایجاد Network Folder مراحل زیر را دنبال کنید:

۱. در قسمتی از صفحه "Computer" کلیک راست نموده و Add a Network Location را انتخاب کنید.
۲. در صفحه "Welcom to Add Network Location Wizard" بروی Next کلیک کنید.
۳. در صفحه "Where do you want to create network location" بروی گزینه "Choose a custom network location" کلیک کنید.



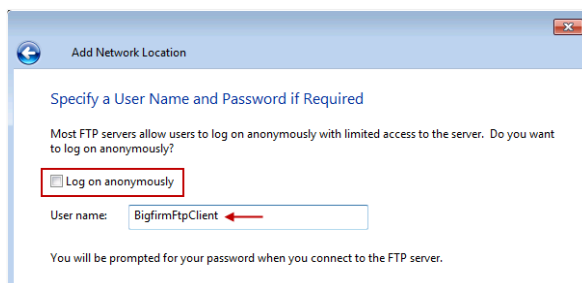
شکل ۱۱-۲۹

۴. در صفحه "Specify the location of your website" آدرس سایت ftp یا http مورد نظر را وارد نموده و بروی Next کلیک کنید (در اینجا از آدرس ftp://ftp.bigfirm.com استفاده شده است).



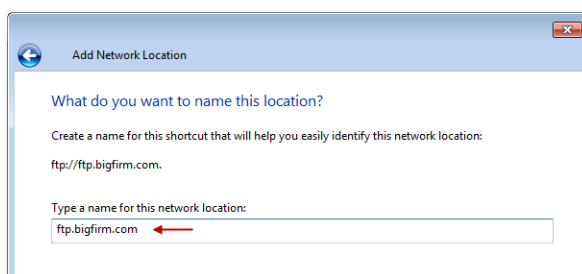
شکل ۱۱-۳۰

۵. ویزارد "Add Network Location" بطور پیش فرض اجازه دسترسی به سایت ftp را بدون استفاده از نام کاربری می دهد. برای تغییر این آپشن ابتدا در صفحه "Specify a User Name and Password" گزینه "Log on anonymously" را غیرفعال نموده و سپس نام کاربری جهت ورود به سایت را وارد کنید. در نهایت بروی Next کلیک کنید.



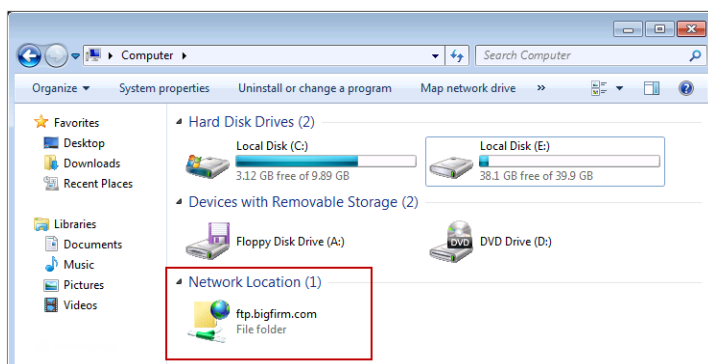
شکل ۱۱-۳۱

۶. در صفحه "What do you want to name this location?" یک نام برای نمایش Network Folder انتخاب نموده (مانند ftp.bigfirm.com) و بروی Next کلیک کنید.



شکل ۱۱-۳۲

۷. در صفحه "Completing the Add Network Location Wizard" بروی Finish کلیک کنید.  
۸. پس ایجاد این پوشه می‌توانید آنرا از مسیر Computer «Network Location» مشاهده کنید.

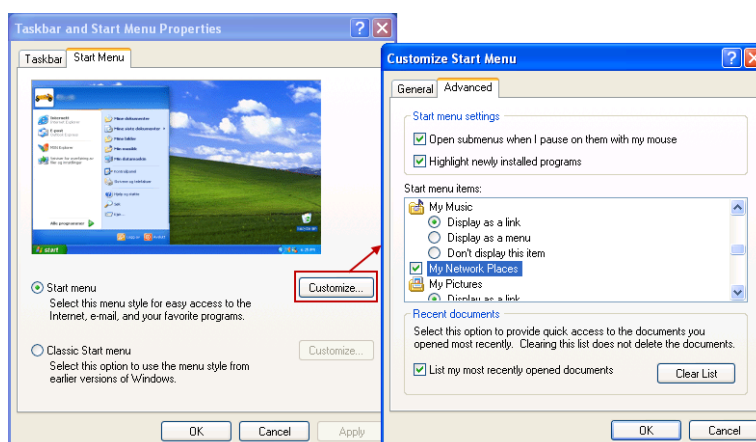


شکل ۱۱-۳۳

### ۱۱-۳-۲ اتصال به منابع با استفاده از ویندوز XP

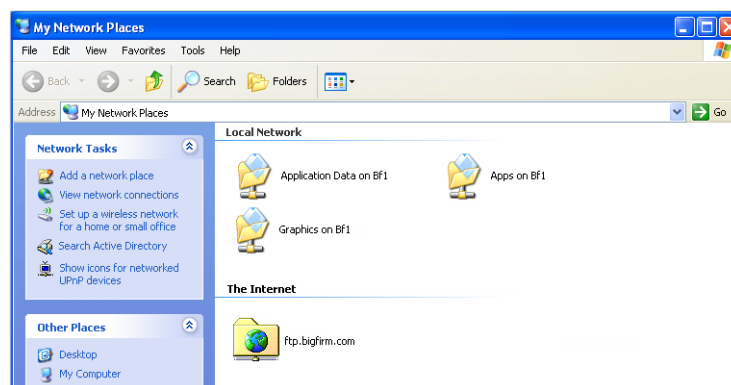
در ویندوز XP برای پیدا کردن منابع اشتراک گذاشته شده در شبکه از اپلتی به نام My Network Places استفاده می‌شود. این اپلت بطور پیش‌فرض در منوی Start قرار نگرفته است و شما می‌توانید با دنبال کردن مراحل زیر آنرا به منوی Start اضافه کنید:

۱. بر روی دکمه Start کلیک‌راست نموده و Properties را انتخاب کنید.
۲. در صفحه "Taskbar and Start Menu Properties"، تب Start Menu را انتخاب نموده و بر روی دکمه Customize کلیک کنید.
۳. در صفحه "Customize Start Menu"، تب Advanced را انتخاب نموده و در قسمت Start Menu items گزینه My Network Places را انتخاب کنید. سپس بر روی OK کلیک کنید.



شکل ۱۱-۳۴

۴. اکنون از مسیر Start «My Network Places» می‌توانید منابع اشتراک گذاشته شده را مشاهده کنید.



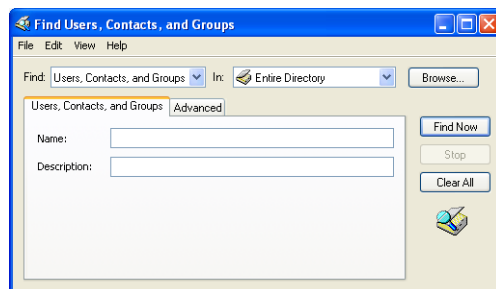
شکل ۱۱-۳۵

همانطور که در شکل ۱۱-۳۵ مشاهده می‌کنید، در پنجره “My Network Places” سه آپشن برای پیدا کردن و اتصال به منابع اشتراک گذاشته شده وجود دارد:

- استفاده از ویزارد “Add a Network Place” برای ایجاد میانبر به یک منبع شبکه. در این ویزارد می‌توانید با استفاده از نام UNC (\\servername\sharename) منبع اشتراک گذاشته شده، یک میانبر برای آن ایجاد کنید.
- استفاده از ابزار Search Active Directory برای جستجوی پوشه‌ها یا پرینترهای انتشار یافته در اکتیو دایرکتوری
- جستجوی شبکه با استفاده از گزینه Entire Network در قسمت Other Places

### جستجو در اکتیو دایرکتوری

برای جستجوی اکتیو دایرکتوری، در پنجره My Network Places بر روی لینک Search Active Directory کلیک کنید. پنجره “Find Users, Contacts, and Groups” نشان داده می‌شود. در این پنجره کافی است در قسمت Find نوع اشیاء را انتخاب نموده و بر روی دکمه Find Now کلیک کنید (البته می‌توانید با استفاده از امکانات تب Features شرایط جستجو را محدودتر کنید).



شکل ۱۱-۳۶

### افزودن پرینتر شبکه

جهت افزودن پرینتر شبکه، به سه روش می‌توان اقدام نمود: جستجو در اکتیو دایرکتوری، استفاده از خط فرمان و استفاده از اپلت Network.

### جستجو در اکتیو دایرکتوری

جهت افزودن پرینتر در این روش، از ابزار Search Active Directory استفاده می‌گردد. کافی است در قسمت Find از پنجره “Find Users, Groups, and Contacts”، گزینه Printers را انتخاب نموده و بر روی Find Now کلیک کنید. پس از کلیک، لیستی از پرینترهای منتشر شده در اکتیو دایرکتوری ظاهر

می‌گردد. برای افزودن پرینتر مورد نظر، بر روی آن کلیک‌راست نموده و گزینه Connect را انتخاب کنید. پس از آن پرینتر نصب شده و می‌توانید از آن استفاده نمایید.

#### افزودن پرینتر با استفاده از خط فرمان

چنانچه از نام پرینتری که قصد دارید اضافه کنید مطلع هستید، می‌توانید از دستور Start در خط فرمان استفاده کنید. به عنوان مثال برای افزودن پرینتری با نام bf\_main\_printer که بر روی سرور bf1 قرار دارد، از دستور زیر استفاده کنید:

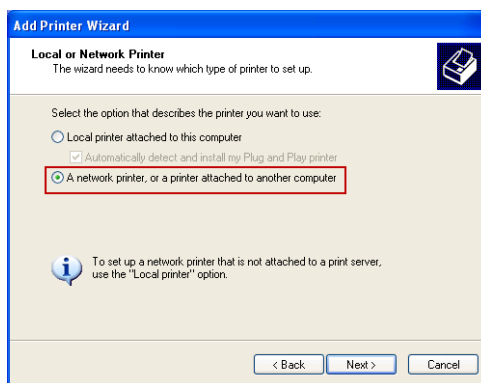
```
Start \\bf1\bf_main_printer
```

پس از افزوده شدن و نصب پرینتر می‌توانید آنرا از مسیر «Start Printers and Faxes» مشاهده کنید.

#### افزودن پرینتر با استفاده از اپلت Printers and Faxes

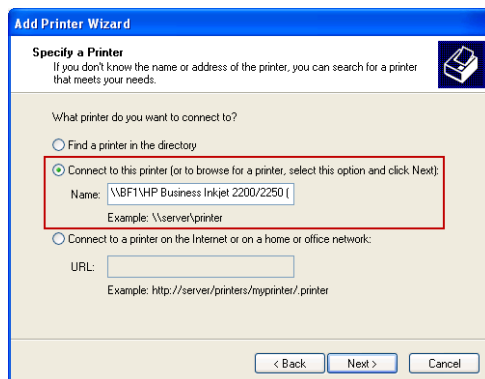
افزودن پرینتر شبکه با استفاده از اپلت Printers and Faxes نیز امکان‌پذیر می‌باشد. برای استفاده از این ابزار مراحل زیر را دنبال کنید:

۱. اپلت Printers and Faxes را از مسیر «Start» اجرا کنید.
۲. بر روی گزینه Add a Printer کلیک نموده تا ویزارد «Add Printer Wizard» اجرا شود.
۳. در صفحه «Welcome to the Add Printer Wizard» بر روی Next کلیک کنید.
۴. در صفحه «Local or Network Printer»، گزینه «A network printer, or a printer attached to another computer» را انتخاب نموده و بر روی Next کلیک کنید.



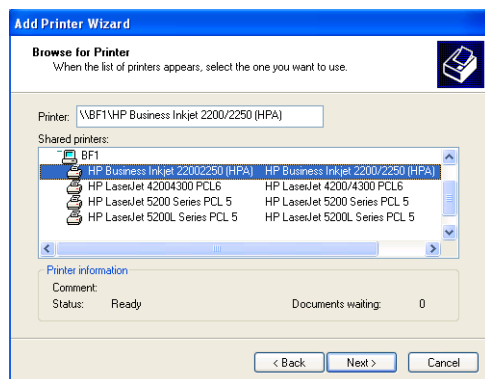
شکل ۱۱-۳۷

۵. در صفحه «Specify a Printer» گزینه Connect to this printer را انتخاب نموده و مسیر قرارگیری پرینتر را به صورت \\Servername\Printername وارد نمایید. سپس بر روی Next کلیک کنید.



شکل ۱۱-۳۸

۶. در مرحله قبل، چنانچه از نام پرینتر اطلاع نداشتید می‌توانید فیلد Name را رها نموده و بر روی Next کلیک کنید. سپس پرینتر را در داخل شبکه مورد جستجو قرار دهید.



شکل ۱۱-۳۹

۷. ممکن است در حین عملیات از شما خواسته شود که دیسک مربوط به درایور پرینتر را قرار دهید. این حالت زمانی اتفاق می‌افتد که کامپیوتر کاربر نتواند درایور مربوط به پرینتر اشتراک گذاشته شده توسط سرور را نصب کند. در صورت وقوع چنین وضعیتی، درایور پرینتر را از روی دیسک نصب کنید.
۸. پس از نصب پرینتر، در صفحه "Default Printers" می‌توانید با انتخاب گزینه Yes، این پرینتر را به عنوان پرینتر پیش‌فرض قرار دهید. بر روی Next کلیک کنید.
۹. در صفحه "Completing the Add Printer Wizard" بر روی Finish کلیک کنید.



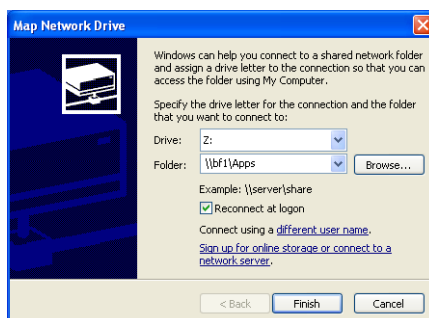
### نگاشت یک درایو برای پوشه‌های اشتراک گذاشته شده

همانطور که برای ویندوز ۷ شرح دادیم، هدف از ایجاد درایو شبکه، سهولت دسترسی به منابع اشتراک گذاشته شده در شبکه می‌باشد. در ویندوز XP هم می‌توان همانند ویندوز ۷ و با استفاده از ویزارد "Map Network Drive" نسبت به ایجاد درایو شبکه اقدام نمود. برای انجام این کار مراحل زیر را دنبال کنید:

۱. پنجره "My Network Places" را باز نموده و بر روی لینک Search Active Directory کلیک کنید.
۲. در قسمت Find، گزینه Shared Folders را انتخاب نموده و بر روی Find Now کلیک کنید.
۳. بر روی پوشه مورد نظر کلیک راست نموده و Map Network Drive را انتخاب کنید.
۴. در پنجره "Map Network Drive" یک نام برای درایو انتخاب نموده و همچنین گزینه Reconnect at logon را نیز فعال نمایید. سپس بر روی Finish کلیک کنید.
۵. جهت دسترسی به درایو ایجاد شده می‌توانید به مسیر Start » My Computer رفته و سپس بر روی نام درایوی که ایجاد نموده‌اید دابل کلیک کنید. برای قطع ارتباط با این درایو نیز می‌توانید بر روی آن کلیک راست نموده و Disconnect را انتخاب نمایید.

بعضی از پوشه‌های اشتراکی در فهرست اکتیو دایرکتوری قرار نگرفته اند. برای نگاشت درایور به این پوشه‌ها، مراحل زیر را دنبال کنید:

۱. از منوی Start بر روی My Computer کلیک راست نموده و Map Network Drive را انتخاب کنید.
۲. در قسمت Drive از صفحه "Map Network Drive" یکی از حروف را از لیست انتخاب کنید.
۳. مسیر قرارگیری پوشه اشتراکی را وارد نموده (مانند \\bf1\apps) و یا با استفاده از دکمه Browse آنرا در شبکه جستجو کنید.



شکل ۱۱-۴۰

۴. پس از انجام تنظیمات بر روی Finish کلیک کنید.

## نگاشت درایو شبکه در خط فرمان

نگاشت درایو برای پوشه‌های اشتراک گذاشته شده با استفاده از خط فرمان ویندوز XP نیز امکان‌پذیر می‌باشد. در مثال زیر با استفاده از دستور `net use` یک درایو به نام Z برای پوشه اشتراکی Apps ایجاد می‌شود:

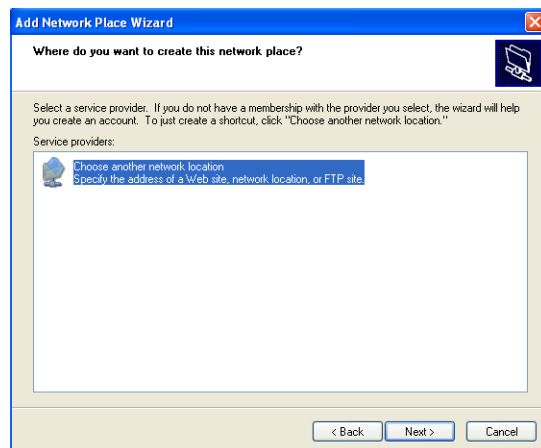
```
net use Z: \\bf1\Apps /PERSISTENT:YES
```

همانطور که قبلاً نیز اشاره نمودیم، در دستور بالا عبارت `PERSISTENT:YES` معادل با انتخاب گزینه `Reconnect at logon` می‌باشد.

## ایجاد میانبرهای Network Location

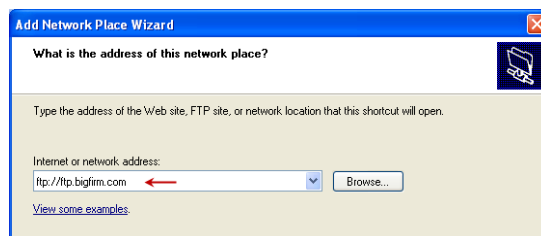
همانطور که در قسمت Network Location از ویندوز ۷ شرح دادیم، میانبرهای Network Location می‌توانند برای پوشه‌های اشتراک گذاشته شده در یک شبکه محلی و یا در سایت‌های `http` و `ftp` ایجاد شوند. برای ایجاد این میانبرها در ویندوز XP مراحل زیر را دنبال کنید.

۱. در پنجره "My Network Places" بر روی لینک `Add a network place` کلیک کنید.
۲. در صفحه "Welcom to the Add Network Place Wizard" بر روی `Next` کلیک کنید.
۳. در صفحه "What do you want to create this network place?" گزینه `Choose another network location` را انتخاب نموده و بر روی `Next` کلیک کنید.



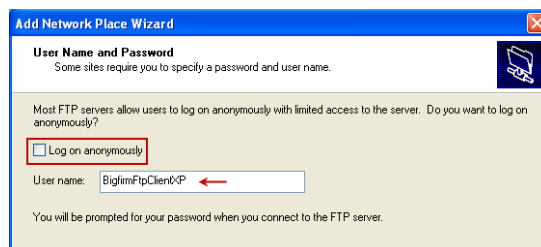
شکل ۱۱-۴۱

۴. در صفحه "What is address of this network place?" آدرس سایت `ftp` یا `http` را وارد نموده و بر روی `Next` کلیک کنید. (ftp://ftp.bigfirm.com)



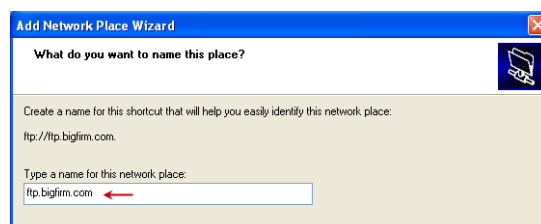
شکل ۱۱-۴۲

۵. در صفحه "User Name and Password" گزینه Log on anonymously را غیرفعال نموده و نام کاربری جهت ورود به سایت را وارد کنید. سپس بر روی Next کلیک کنید.



شکل ۱۱-۴۳

۶. یک نام جهت اختصاص به محل (مانند ftp.bigfirm.com) انتخاب نموده و بر روی Next کلیک کنید.



شکل ۱۱-۴۴

۷. در صفحه "Completing the Add Network Location Wizard" بر روی Finish کلیک کنید.
۹. اکنون با مراجعه به پنجره "My Network Places" می‌توانید میانبر ایجاد شده را مشاهده کنید.

## « فصل ۱۲ »

**Backup** گیری از سرور، پوشه‌ها، و  
اکتیو دایرکتوری

**Backup from Server, Folders, and**  
**Active Directory**



Backup گیری و بازگردانی، دو اقدام بسیار آشنا برای مدیران سرورها هستند. با استفاده از این اقدامات می‌توان از داده‌ها و کاربردهایی که بر روی سرور قرار دارند محافظت نمود. اهمیت این اقدامات زمانی مشخص می‌شود که داده‌های موجود بر روی سرور و یا اشیاء اکتیو دایرکتوری به نحوی از دست بروند، در اینصورت چنانچه فایل‌های Backup از آنها تهیه نکرده باشید، تقریباً می‌توان گفت که با در دستر بزرگی مواجه خواهید شد، مخصوصاً زمانی که این داده‌ها قابل جایگزینی نباشند. اکنون حالتی را در نظر بگیرید که فایل‌های Backup به صورت روزانه یا هفتگی تهیه می‌شوند. چنانچه هر اتفاقی برای سرور و داده‌های آن رخ دهد، کافی است این فایل‌ها را بر روی آن بازگردانی نموده و همه چیز را به وضعیت عادی خود بازگردانید. این کار حتی در زمانی که سخت افزارهای سرور در زمان خرابی به کلی تعویض می‌شوند نیز می‌تواند به نیازهای شما پاسخگو باشد.

در این فصل قصد داریم نحوه انجام Backup گیری و Restore کردن (بازگردانی) داده‌ها را برای سرور و همچنین اشیاء اکتیو دایرکتوری شرح دهیم. بطور کلی مهمترین مباحثی که در این فصل مورد بررسی قرار می‌گیرد عبارتند از:

- ♦ Backup گیری و بازگردانی کل سرور با استفاده از ابزار Windows Server Backup
- ♦ Backup گیری از فایل‌ها و پوشه‌ها
- ♦ Backup گیری و بازگردانی اکتیو دایرکتوری

## ۱۲-۱ Backup گیری و بازگردانی ویندوز سرور

Backup گیری از ویندوز سرور با استفاده از ابزاری به نام Windows Server Backup که به صورت رایگان در خود ویندوز سرور 2008/2008R2 قرار دارد قابل انجام است. در ویندوز سرور 2008R2 این ابزار با بهبودهایی همراه شده است که از جمله می‌توان به موارد زیر اشاره نمود:

- ♦ Backup گیری و بازگردانی وضعیت سیستم<sup>۱</sup> با استفاده از ابزار Windows Server Backup در کنسول Server Manager قابل انجام است. همچنین پس از ایجاد Backup از وضعیت سیستم می‌توان بعداً داده‌های بیشتری به آن اضافه نمود. Backup ای که از وضعیت سیستم تهیه می‌شود، شامل تمام داده‌های مورد نیاز برای بازگردانی سیستم عامل به وضعیتی است که در زمان Backup گیری داشته است
- ♦ ابزار Windows Server Backup دارای قابلیت عملکرد از طریق Command Line و PowerShell است، بنابراین می‌توانید هر اقدامی را که با استفاده از Snap-in مربوط به Windows Server Backup در Server Manager قابل انجام است، از طریق دستورات خط فرمان یا اسکریپت‌ها نیز انجام دهید.

1. System State

- می‌توانید Backup‌های ذخیره شده را بطور خودکار مدیریت کنید. Windows Server Backup بطور خودکار Backup‌های قدیمی‌تر را حذف نموده و Backup‌های جدید را جایگزین آنها می‌نماید.
- آپشن Remote Storage برای Backup‌هایی که شامل پوشه‌های اشتراکی و درایوهای Remote (مانند iSCSI و کانال‌های فیبر نوری) و همچنین دیسک‌های مجازی<sup>۱</sup> هستند اضافه گردیده است.

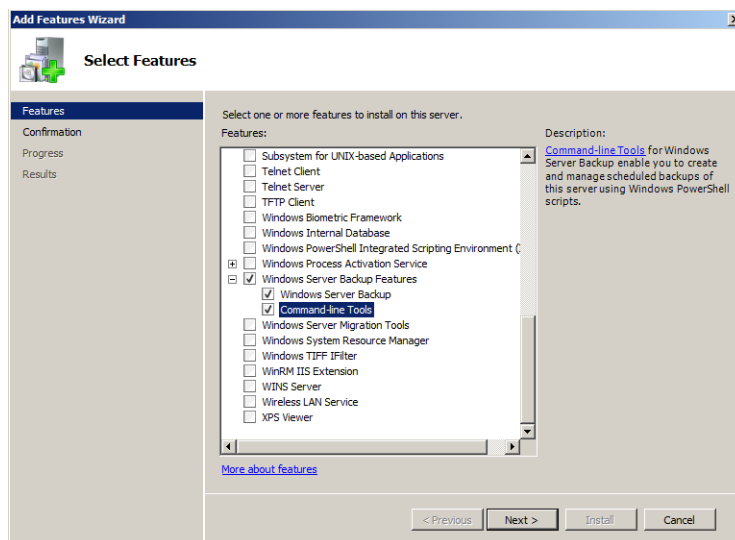
### ۱-۱۲ نصب Windows Server Backup

Windows Server Backup یک Feature به همراه رل File Service در ویندوز سرور 2008R2 است که از دو قسمت مجزا تشکیل شده است:

- ابزار گرافیکی Windows Server Backup: این ابزار جهت انجام Backup‌گیری با استفاده از کنسول Server Manager استفاده می‌شود.
- Command-Line Tools: ابزارهای مربوط به خط فرمان که شامل Cmd و PowerShell هستند را فراهم می‌نماید.

Windows Server Backup بطور پیش‌فرض بر روی ویندوز سرور 2008R2 نصب نشده است بنابراین جهت نصب آن می‌توانید طبق مراحل زیر اقدام کنید:

۱. در کنسول Server Manager بر روی Features کلیک‌راست نموده و Add Features را انتخاب کنید.
۲. در صفحه “Select Features” گزینه Windows Server Backup Features را به همراه آیتم‌های زیرمجموعه آن انتخاب نموده و بر روی Next کلیک کنید.



شکل ۱-۱۲

۳. در صفحه “Confirm Installation Selections” بروی Install کلیک نموده و منتظر بمانید تا عملیات نصب به اتمام رسد.

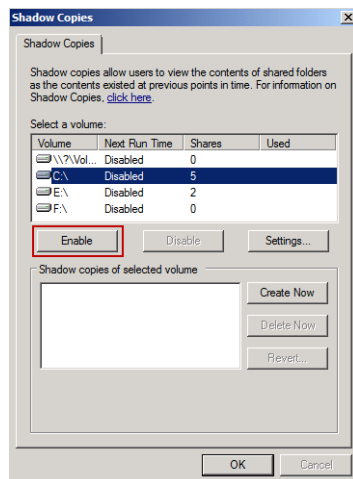
۴. در صفحه “Installation Results” بروی Close کلیک کنید.

## ۲-۱-۱۲ فعال‌سازی قابلیت Shadow Copy

قابلیت Shadow Copy امکان Backup گیری از فایل‌های باز که در برنامه‌های ویندوز در حال استفاده هستند را فراهم می‌نماید. با استفاده از این قابلیت دیگر نیازی به متوقف نمودن برنامه‌ها جهت آزادسازی فایل‌ها نمی‌باشد و به راحتی می‌توانید از فایل‌هایی که در برنامه‌ها باز هستند Backup تهیه نمایید. قبل از اقدام به Backup گیری از فایل‌ها (چنانچه در وضعیت ذکر شده قرار دارید) لازم است که این قابلیت بر روی درایوهای ویندوز (یا همان Volume ها) فعال گردد. جهت فعال‌سازی مراحل زیر را دنبال کنید:

۱. در پنجره “Computer” بروی درایوی که فایل مورد نظر در آن قرار دارد کلیک‌راست نموده و گزینه Configure Shadow Copies را انتخاب کنید.

۲. در پنجره “Shadow Copie” درایو مورد نظر را انتخاب نموده و بر روی دکمه Enable کلیک کنید.



شکل ۲-۱۲

۳. در پیغام ظاهر شده بر روی Yes کلیک کنید تا فایل Shadow ایجاد شود. در نهایت بر روی OK کلیک کنید.

۴. جهت غیر فعال کردن این قابلیت می‌توانید درایو فعال شده را انتخاب نموده و بر روی Disable کلیک کنید.



### ۳-۱-۱۲ Backup گیری و بازگردانی کامل یک سرور

Backup گیری کامل از سرور ساده‌ترین راه Backup گیری و در عین حال بهترین گزینه برای بازگردانی سرور است. یک Backup کامل از سرور شامل موارد زیر می‌باشد:

- ♦ تمام Volume های Local سیستم (دیسک‌های مجازی که بر روی Volume های محلی قرار گرفته‌اند در صورت Online بودن نمی‌توانند Backup گیری شوند).
- ♦ Volume های حساس و حیاتی
- ♦ وضعیت سیستم (System State)

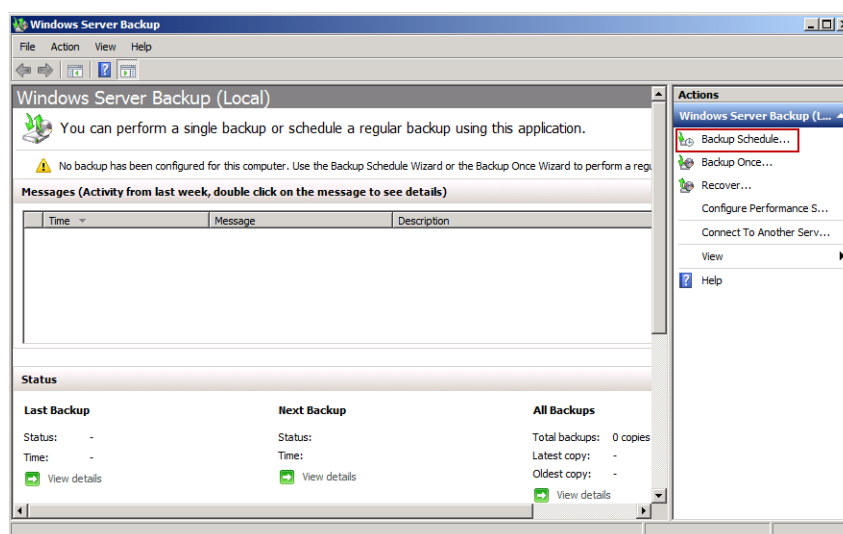
در یک Backup گیری کامل می‌توانید هر کدام از فایل‌ها و پوشه‌ها را در صورت وقوع خطا در دیسک بازگردانی کنید. همچنین امکان یک بازگردانی "bare-metal" نیز وجود دارد که با استفاده از آن می‌توانید یک کامپیوتر که بر روی آن سیستم عاملی نصب نشده است (یا حداقل هارد دیسک‌های شامل سیستم عامل و وضعیت سیستم) را جایگزین کنید.

#### انجام Backup گیری کامل از سرور

در مراحل زیر چگونگی Backup گیری کامل از سرور بر روی یک دیسک Local و همچنین تنظیم زمانبندی برای Backup گیری خودکار نشان داده شده است:

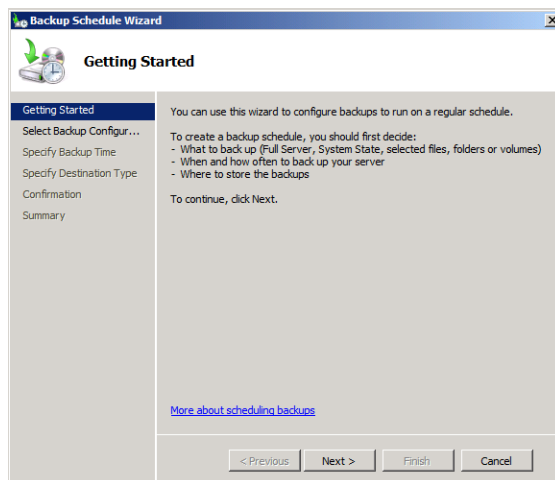
۱. کنسول Windows Server Backup را از مسیر Start Administrative Tools اجرا کنید.

۲. در پنل Action (سمت راست) بر روی Backup Schedule کلیک کنید.



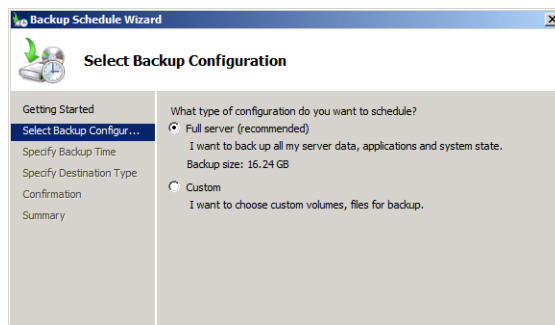
شکل ۳-۱۲

۳. در صفحه “Getting Started” بروی Next کلیک کنید.



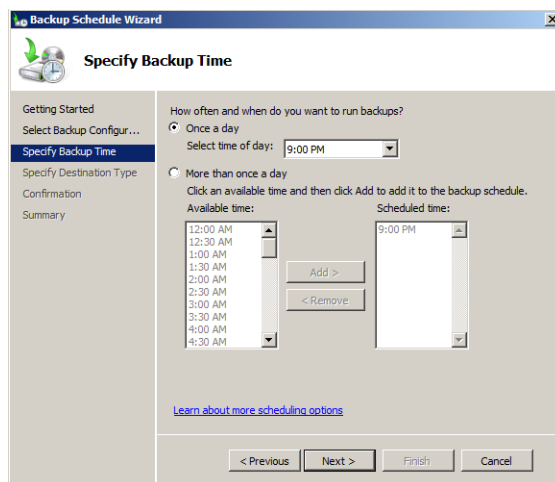
شکل ۱۲-۴

۴. در صفحه “Select Backup Configuration” گزینه Full server را انتخاب نموده و بروی Next کلیک کنید.



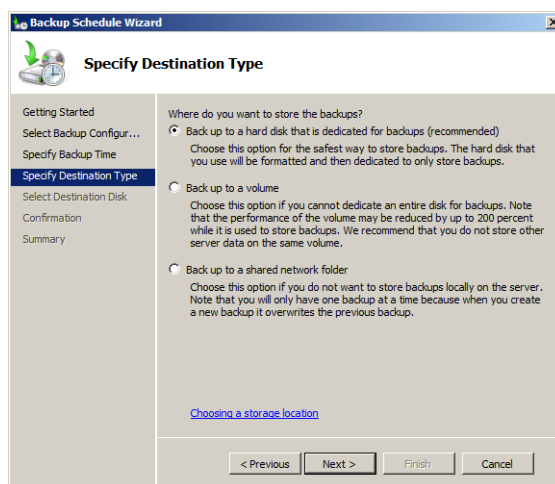
شکل ۱۲-۵

۵. در صفحه “Specify Backup Time”، باید تعداد دفعاتی که عمل Backup گیری در طول روز انجام می‌شود را تعیین نمایید. گزینه Once a day برای انجام Backup گیری تنها یکبار در روز و گزینه More than once a day برای انجام Backup گیری به تعداد دفعات بیشتر و در ساعات مشخص شده می‌باشد. با افزودن ساعات تعیین شده به فهرست Scheduled time، Backup گیری به صورت خودکار در آن زمان‌ها انجام می‌شود. پس از انجام تنظیمات بروی Next کلیک کنید.



شکل ۱۲-۶

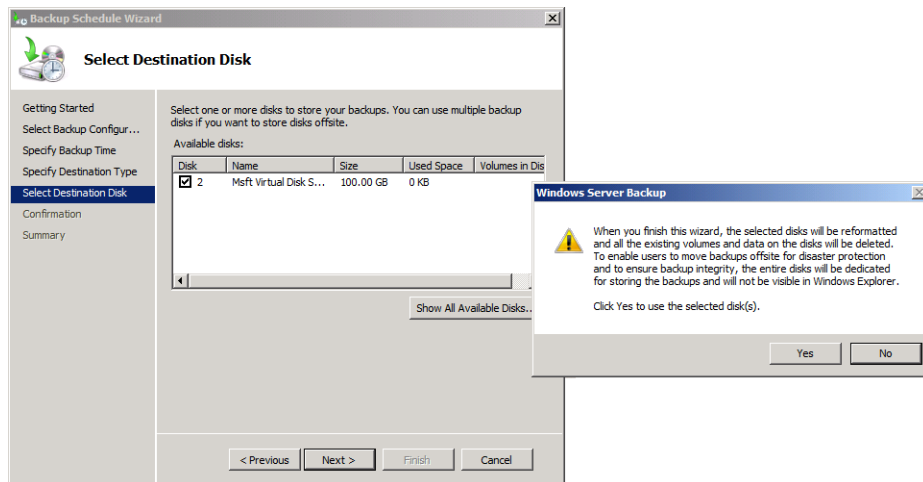
۶. در صفحه "Specify Destination Type" در صورت داشتن یک دیسک جداگانه برای ذخیره Backup ها گزینه "Back up to a hard disk that is dedicated for backups" و در غیر اینصورت گزینه "Backup to a Volume" را انتخاب نموده و بر روی Next کلیک کنید. دقت داشته باشید که دیسک جداگانه‌ای که به سرور متصل می‌کنید باید فاقد پارتیشن یا فایل سیستمی باشد. همچنین نوع دیسک نیز باید باید Raw باشد.



شکل ۱۲-۷

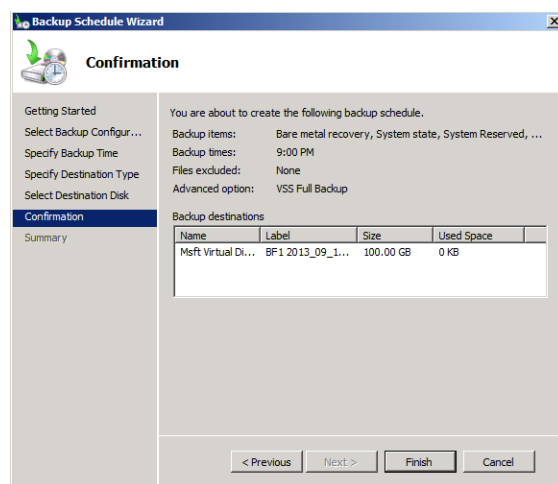
۷. در صفحه "Specify Destination Disk" دیسک مورد نظر برای ذخیره فایل Backup را انتخاب

نموده و بر روی Next کلیک کنید. دقت داشته باشید که در طی این فرایند هشدار مبنی بر فرمت شدن دیسک و از بین رفتن داده‌های آن دریافت خواهید نمود. چنانچه قصد دارید از همان دیسک استفاده کنید بر روی Yes کلیک کنید.



شکل ۸-۱۲

۸. در صفحه "Confirmation" بر روی Finish کلیک کنید.



شکل ۹-۱۲

۹. پس از اتمام عملیات و ایجاد فایل Backup، در صفحه "Summary" بر روی Close کلیک کنید.

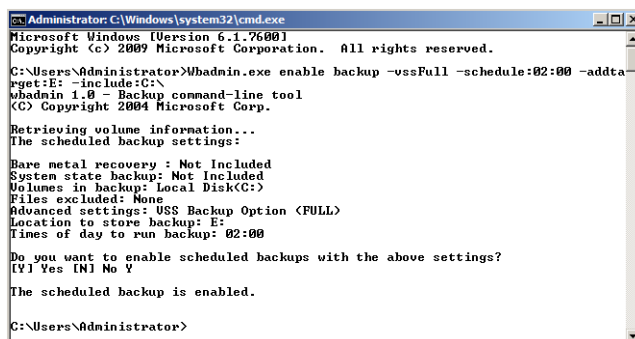
### انجام Backup گیری کامل از سرور با استفاده از خط فرمان

Backup گیری در خط فرمان با استفاده از ابزار Wbadmin.exe انجام می‌شود. دستور زیر یک Backup گیری زمانبندی شده در ساعت ۲:۰۰ انجام می‌دهد:

```
Wbadmin.exe enable backup -vssFull -schedule:02:00 -addtarget:E: -include:C:\
```

در دستور بالا تعدادی پارامتر مورد استفاده قرار گرفته است:

- ♦ -vssFull : تعیین می‌کند که Backup گیری کامل از سرور انجام می‌شود.
- ♦ -schedule : زمانبندی انجام Backup گیری را تعیین می‌نماید.
- ♦ -addtarget : محل ذخیره‌سازی فایل Backup را تعیین می‌کند که در اینجا درایو E است.
- ♦ -include:C:\ : نیز مشخص می‌کند که از درایو C نیز باید Backup گرفته شود.



شکل ۱۲-۱۰

پس از اجرای دستور بالا، برای شروع Backup گیری دستور زیر را وارد کنید:

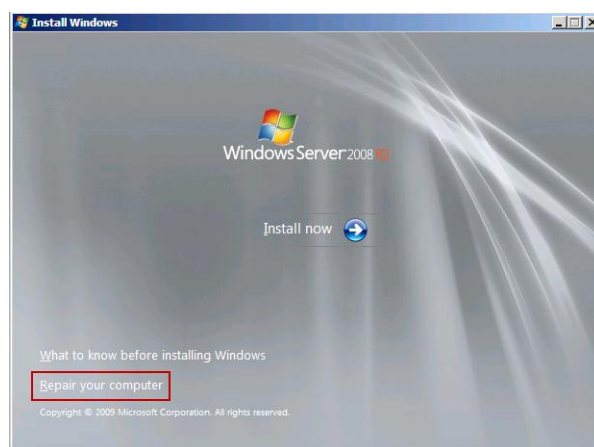
```
Wbadmin.exe start backup
```

### بازگردانی کامل سرور

جهت بازگردانی فایل‌های Backup گرفته شده، روش‌های مختلفی وجود دارد. انتخاب این روش به حجم داده‌ها و زمان موجود برای بازگردانی بستگی دارد. به عنوان مثال فرض کنید که سیستم به دلایلی مانند کل داده‌های نقص سخت افزاری از بین رفته است. در این حالت شما می‌توانید ویندوز سرور 2008R2 را مجدداً نصب نموده و کل سرور را با استفاده از Windows Server Backup بازگردانی کنید. یا می‌توانید با استفاده از DVD نصب ویندوز سرور 2008R2 و انجام یک بازگردانی bare-metal، کل سرور را بازگردانی نمایید.

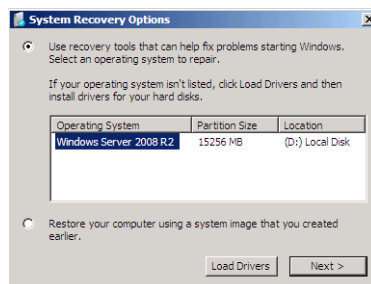
مراحل زیر بازگردانی کل سرور را زمانی که داده‌های آن به دلیل نقص سخت افزاری (هارد دیسک) از بین رفته‌اند نشان می‌دهد. در این سناریو، یک هارد دیسک جدید جایگزین هارد دیسک قبلی شده است:

۱. سرور را با استفاده از DVD نصب ویندوز سرور 2008R2 بوت کنید.
۲. در صفحه “Install Windows” زبان مورد نظر را انتخاب نموده و بر روی Next کلیک کنید.
۳. گزینه “Repair your computer” را انتخاب نمایید.



شکل ۱۱-۱۲

۴. در صفحه “System Recovery Option” چنانچه سیستم عامل فعلی شما بر روی سرور شناسایی شود، پیشنهاد می‌کند که آنرا Repair کنید. در صورتی که از یک هارد دیسک جدید استفاده کنید، این گزینه وجود نخواهد داشت. بر روی Next کلیک کنید.



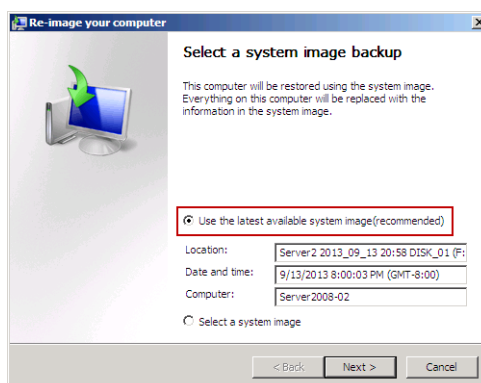
شکل ۱۲-۱۲

۵. در صفحه “Choose a Recovery Tool” بر روی System Image Recovery کلیک کنید.



شکل ۱۲-۱۳

۶. در "Select a system image backup" یکی از گزینه‌های Use the latest available system image یا Restore a different backup را انتخاب کنید. با انتخاب Restore a different backup باید از بین Backup‌های موجود یکی را انتخاب نموده و یا یک مسیر شبکه جهت فراهم کردن Backup تعیین کنید.

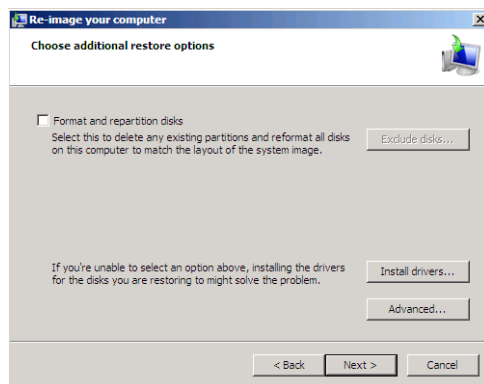


شکل ۱۲-۱۴

۷. در صفحه "Choose additional restore options" آپشن‌های مورد نظر را با توجه به موارد زیر انتخاب نموده و بر روی Next کلیک کنید:

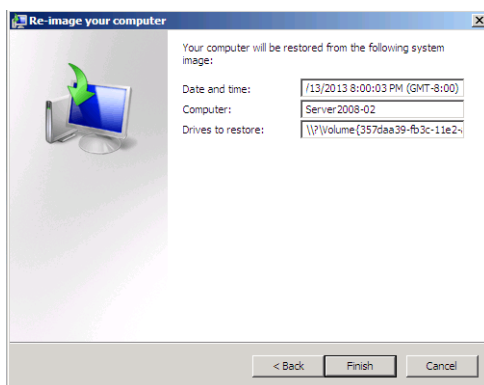
- ♦ گزینه "Format and repartition disks" برای فرمت کردن و پارتیشن‌بندی مجدد دیسک استفاده می‌شود. زمانی که این آپشن را انتخاب می‌کنید، آپشن Exclude disks در دسترس قرار می‌گیرد و می‌توانید تعدادی از دیسک‌ها را برای ممانعت از فرمت شدن آنها انتخاب کنید. این آپشن زمانی مفید است که بخواهید دیسک قرارگیری ویندوز را بازگردانی نموده بدون اینکه داده‌های سایر Volume‌ها دچار تغییر شوند.
- ♦ چنانچه قصد دارید فقط سیستم عامل را بازگردانی کنید، گزینه Only restore system drives را انتخاب کنید.
- ♦ چنانچه تمام دیسک‌های نصب شده بر روی کامپیوتر قابل مشاهده نباشند باید درایور آنرا نصب

- کنید، بنابراین می‌توانید بر روی Install drivers کلیک کنید.
- ♦ با استفاده از دکمه Advanced نیز می‌توانید تعیین کنید که کامپیوتر بطور خودکار Restart گردد و در هنگام Restart خطاهای دیسک را بررسی نماید.



شکل ۱۲-۱۵

۸. در آخرین صفحه از ویزارد "Re-image your computer" بر روی Finish کلیک کنید تا عملیات Recovery آغاز گردد. این عملیات ممکن است کمی طول کشد بنابراین تا اتمام آن منتظر بمانید.



شکل ۱۲-۱۶

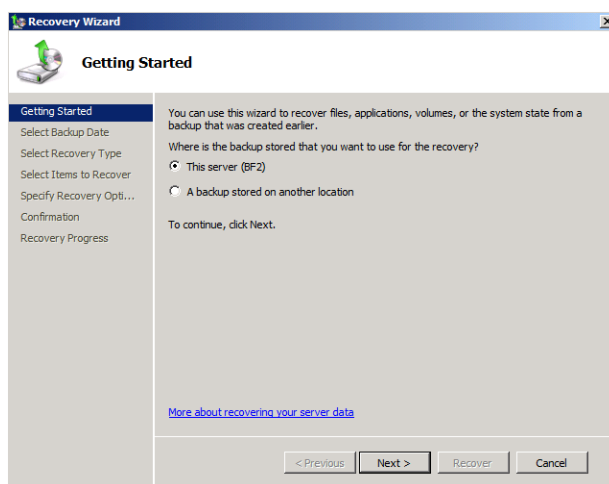
### بازگردانی وضعیت سیستم (System State)

جهت بازگردانی وضعیت سیستم مراحل زیر را دنبال کنید:

۱. در کنسول Windows Server Backup به پنل Action مراجعه نموده و بر روی Recover کلیک کنید.
۲. در صفحه "Getting Started page" باید سرور مورد نظر برای بازگردانی را انتخاب نمایید:

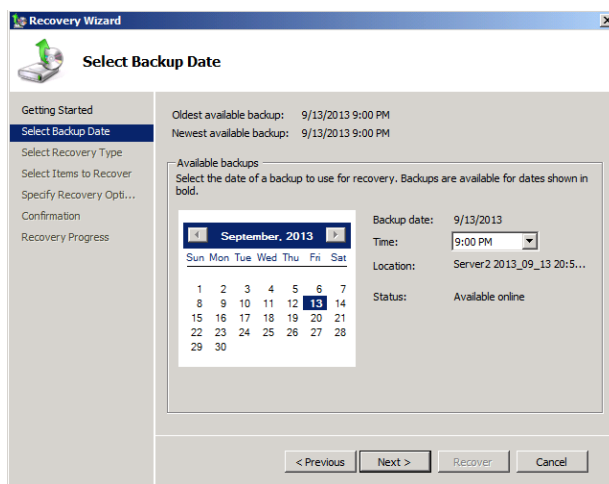


- ♦ This server: سرور فعلی را بازگردانی می‌کند.
- ♦ Another server: برای بازگردانی داده‌ها بر روی یک سرور Remote استفاده می‌شود. با انتخاب این گزینه باید محل قرارگیری فایل‌های Backup را بر روی کامپیوتر Local و یا پوشه اشتراکی شبکه تعیین کنید.



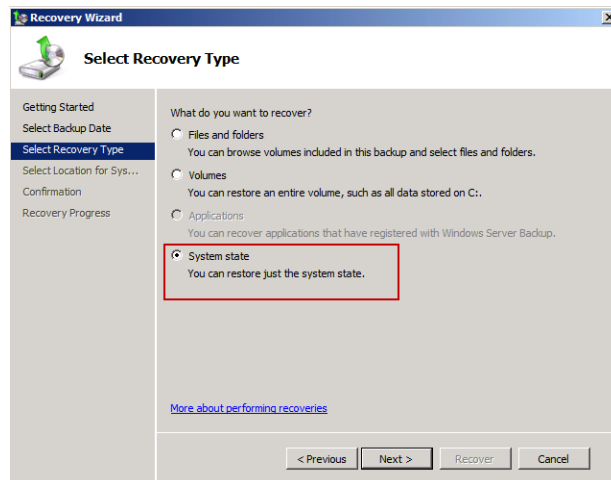
شکل ۱۲-۱۷

۳. در صفحه "Select Backup Date" تاریخ و زمان فایل Backup جهت بازگردانی تعیین نموده و بر روی Next کلیک کنید.



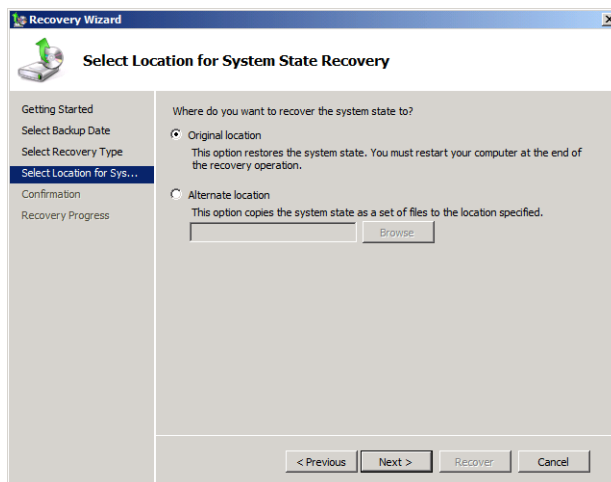
شکل ۱۲-۱۸

۴. در صفحه “Select Recovery Type” گزینه System State را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۱۲-۱۹

۵. در صفحه “Select Location for System State Recovery” گزینه Original location را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۱۲-۲۰

۶. در صفحه “Confirmation” بر روی Recover کلیک کنید تا عملیات بازگردانی آغاز گردد. پس از اتمام عملیات سیستم Restart خواهد شد.

### بازگردانی وضعیت سیستم در خط فرمان

برای بازگردانی وضعیت سیستم با استفاده از خط فرمان در ویندوز سرور 2008R2 می‌توانید از دستور زیر استفاده کنید:

```
Wbadmin.exe start systemstate recovery -version -backupTarget -machine recoveryTarget -authsysvol -autoreboot
```

پارامترهای به کار رفته در این دستور عبارتند از:

- ♦ **-version**: تاریخ و زمان Backup را مشخص می‌نماید. به عنوان مثال برای تعیین Backup ای که در تاریخ ۱۰ ژوئن ۲۰۱۲ ساعت ۱۱ بعد از ظهر ایجاد شده است می‌توانید از مقدار `-version:06/10/2012-23:00` استفاده کنید.
- ♦ **-backupTarget**: محلی که فایل Backup در آن ذخیره شده است را مشخص می‌کند، مانند: `-backupTarget:\\server1\share`
- ♦ **-machine**: نام کامپیوتری است که بازگردانی می‌شود، مانند: `-machine:BF1`
- ♦ **-recoveryTarget**: مقصد Backup را چنانچه بر روی کامپیوتر Local نباشد تعیین می‌کند.
- ♦ **-authsysvol**: نشان می‌دهد که عمل بازگردانی باید به صورت یک بازگردانی معتبر از پوشه Sysvol انجام شود.
- ♦ **-autoreboot**: این پارامتر سیستم را پس از بازگردانی بطور خودکار Restart می‌نماید.

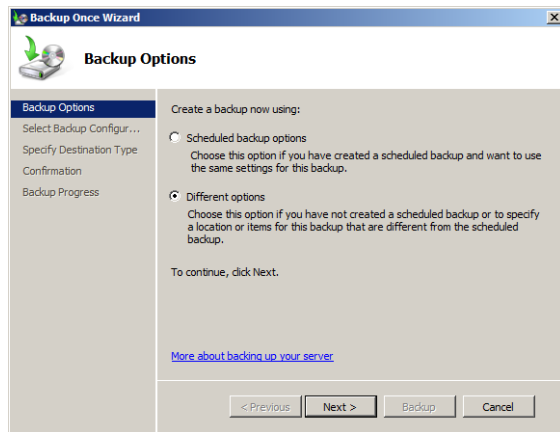
### ۱۲-۴ Backup گیری و بازگردانی فایل‌ها و پوشه‌ها

علاوه بر امکان Backup گیری از کل سرور و وضعیت سیستم، Windows Server Backup اجازه می‌دهد که از تک تک فایل‌ها و پوشه‌ها و همچنین Volume‌ها Backup گیری نمایید. این قابلیت در زمانی که بنا به دلایلی داده‌های موجود بر روی هارد دیسک‌ها از بین می‌روند، بسیار مفید می‌باشد.

#### انجام Backup گیری دستی از فایل‌ها و پوشه‌ها

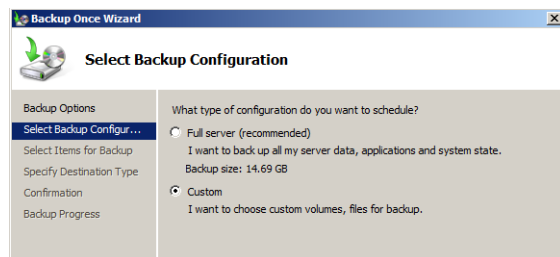
در Windows Server Backup انجام Backup گیری از فایل‌ها و پوشه‌ها به دو صورت زمانبندی شده و دستی قابل انجام است. مراحل زیر نحوه Backup گیری از فایل‌ها و پوشه‌ها را با فرض اینکه Windows Server Backup نصب شده است نشان می‌دهد:

۱. Windows Server Backup را اجرا کنید.
۲. در پنل Action (سمت راست) بر روی Backup Once کلیک کنید.
۳. در صفحه "Backup Options" گزینه Differenet Options را انتخاب نموده و بر روی Next کلیک کنید.



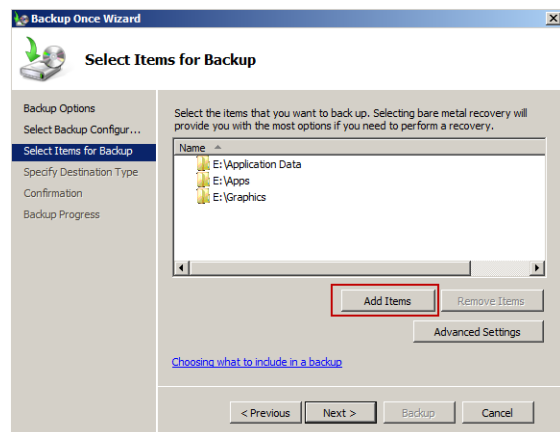
شکل ۱۲-۲۱

۴. در صفحه “Select Backup Configuration”، Custom را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۱۲-۲۲

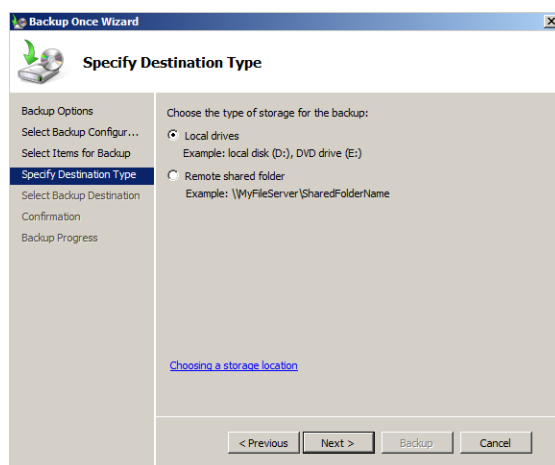
۵. در صفحه “Select Item for Backup”، با استفاده از دکمه Add Item، فایل‌ها و پوشه‌های مورد نظر را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۱۲-۲۳

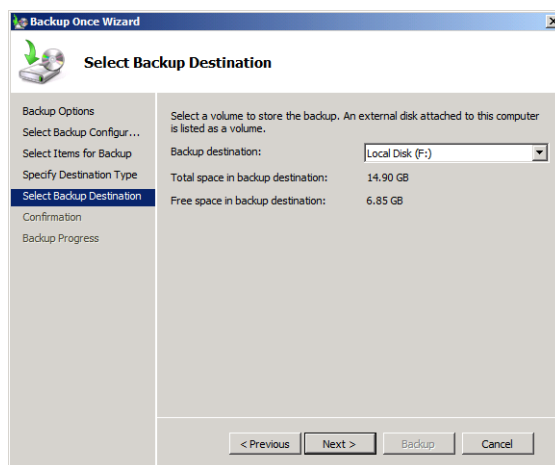
چنانچه قصد دارید از فایل‌های مشخصی Backup گیری نشود (مانند فایل‌های موقت) ، می‌توانید بر روی دکمه Advanced Settings کلیک نموده و تب Exclusions را انتخاب نمایید. در این تب باید فایل‌های مورد نظر را علامت‌گذاری کنید.

۶. در صفحه “Specify Destination Type” نوع محل ذخیره‌سازی فایل Backup (هارد دیسک یا محلی بر روی شبکه) را تعیین نموده و بر روی Next کلیک کنید.



شکل ۱۲-۲۴

۷. در صفحه “Select Backup Destination” محل ذخیره‌سازی فایل Backup را تعیین نموده و بر روی Next کلیک کنید.



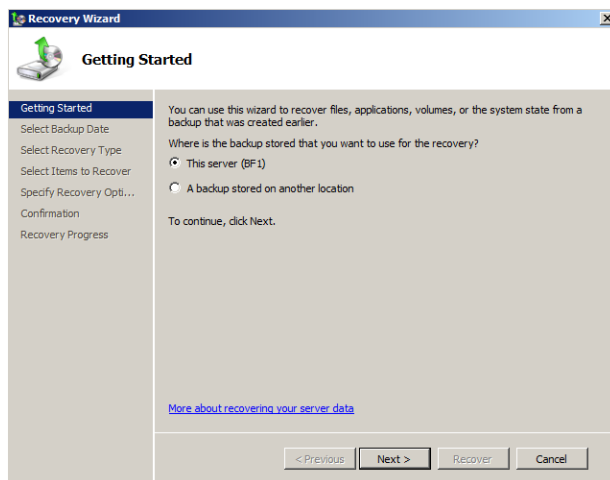
شکل ۱۲-۲۵

۸. بر روی دکمه Backup کلیک کنید تا عملیات آغاز گردد. پس از اتمام کار بر روی Close کلیک کنید.

### بازگردانی یک پوشه از فایل Backup

اکنون برای بازگردانی پوشه‌ها، زمانی که به دلایلی مانند حذف نادرست و ... از بین رفته‌اند می‌توانید مراحل زیر را دنبال کنید:

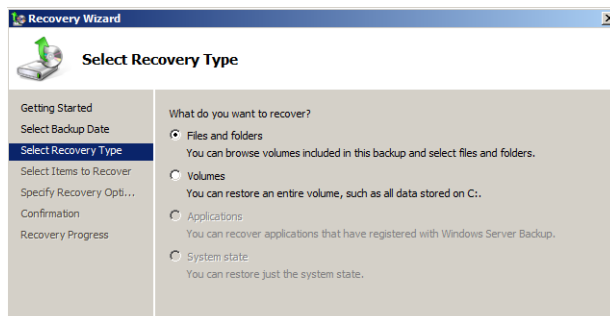
۱. در پنل Action بر روی Recover کلیک کنید.
۲. در صفحه "Getting Start" محل قرارگیری فایل Backup را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۱۲-۲۶

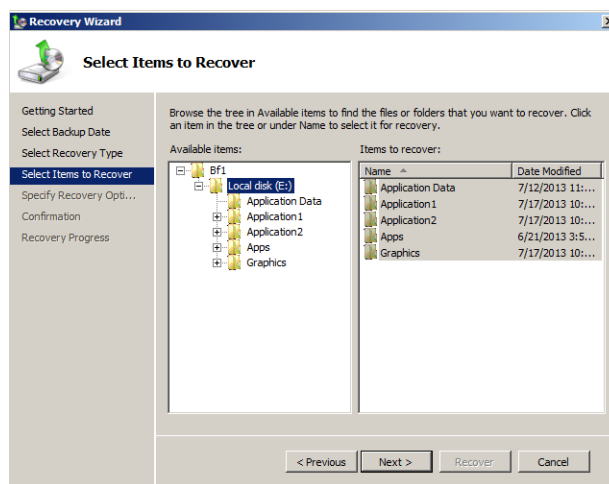
۳. در صفحه "Select Backup Date" تاریخ و زمان ایجاد فایل Backup که قصد بازگردانی پوشه از آن دارید را تعیین نموده و بر روی Next کلیک کنید (رجوع کنید به شکل ۱۲-۱۸).

۴. در صفحه "Select Recovery Type" باید نوع Backup را تعیین کنید. گزینه Files and Folders را انتخاب نموده و بر روی Next کلیک کنید.



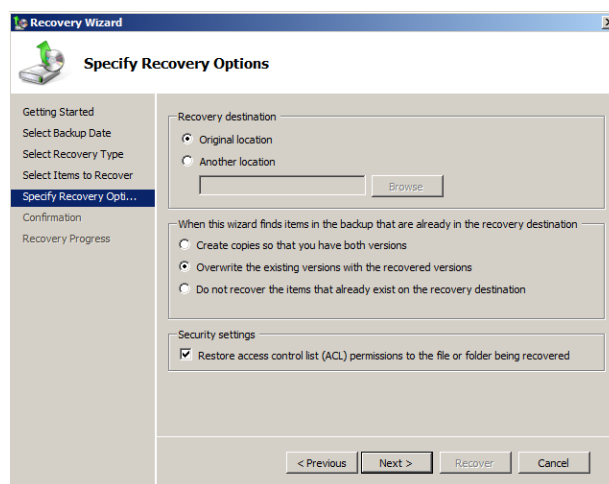
شکل ۱۲-۲۷

۵. در صفحه "Select Items to Recover"، فایل‌ها و پوشه‌های مورد نظر جهت بازگردانی را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۱۲-۲۸

۶. در صفحه "Specify Recovery Options" تنظیماتی جهت بازگردانی باید انجام شود. این تنظیمات عبارتند از: محل بازگردانی فایل‌ها و پوشه‌ها، عملیاتی که در صورت وجود فایل‌های تکراری در مقصد باید انجام شود، و بازگردانی مجوزهایی که قبلاً بر روی پوشه‌ها وجود داشتند. پس از انجام تنظیمات بر روی Next کلیک کنید.



شکل ۱۲-۲۹

۷. در صفحه "Confirmation" بروی Recover کلیک نموده و منتظر بمانید تا عملیات به اتمام رسد.

#### بازگردانی یک پوشه از فایل Backup در خط فرمان

بازگردانی پوشه‌های تکی با استفاده از خط فرمان نیز امکان‌پذیر است. مثال زیر، پوشه موجود در مسیر C:\Library را بازگردانی می‌نماید:

```
Wbadmin.exe START RECOVERY -version:07/20/2013-18:39 -items:C:\Library -itemtype:File -backupTarget:E: -recursive
```

پارامترهای به کار رفته در این دستور عبارتند از:

- ♦ **START RECOVERY**: این پارامتر به Wbadmin.exe اعلام می‌کند که عملیات Recovery را آغاز نماید.
- ♦ **-version**: تاریخ و زمان ایجاد فایل Backup را مشخص نموده و به صورت MM/DD/YYYY-HH:MM می‌باشد.
- ♦ **-items**: جهت تعیین آیتم‌هایی که باید بازگردانی شوند استفاده می‌گردد. می‌توان با استفاده از کاما (,) این آیتم‌ها را به صورت جداگانه تعیین نمود.
- ♦ **-itemtype**: نوع شیئی که قرار است با استفاده از پارامتر **-items** بازگردانی شود را مشخص نموده و می‌تواند یکی از موارد **APP**، **FILE**، و **VOLUME** باشد. برای تعیین انواع مختلف اشیاء می‌توانید این پارامتر را به همراه نوع شیء و به صورت جداگانه (برای هر نوع) استفاده نمایید.
- ♦ **-backupTarget**: محل بازگردانی فایل‌ها را مشخص می‌نماید.

## ۱۲-۲ Backup گیری و بازگردانی اکتیو دایرکتوری

زمانی که با استفاده از ابزارهای Windows Server Backup یا Wbadmin.exe اقدام به Backup گرفتن از سرور می‌کنید، از اکتیو دایرکتوری به عنوان بخشی از System State در کنترل‌کننده دامنه (DC)، Backup گرفته می‌شود. نوع Backup که از DC گرفته می‌شود به فرکانس تغییراتی که در اکتیو دایرکتوری، داده‌ها، یا Application‌هایی که بر روی DC نصب شده است بستگی دارد. حداقل نیاز شما برای Backup گیری از اکتیو دایرکتوری (یا همان ADDS) بر روی یک DC، System State است که بسته به Role‌های نصب شده بر روی آن شامل مواردی چون: پایگاه‌داده اکتیو دایرکتوری (ntds.dit)، Registry، پایگاه‌داده ثبت COM+، پایگاه‌داده سرویس‌های Active Directory Certificate Services، پوشه SYSVOL، کلیه فایل‌های سیستمی که توسط سرویس Windows Resource protection محافظت می‌شوند، و مواردی از این دست می‌باشد.

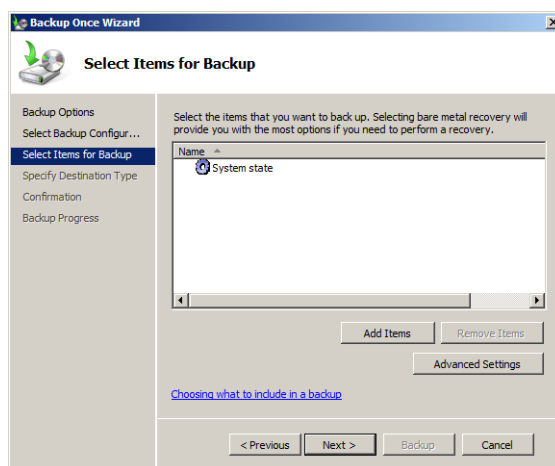


برای ایجاد این نوع از Backup، همانطور که در قسمت‌های قبل شرح داده شد می‌توانید از دو روش دستی و زمانبندی شده و یا از ابزار Wbadmin.exe استفاده نمایید.

## ۱۲-۲-۱ ایجاد Backup از اکتیو دایرکتوری

جهت ایجاد Backup از اکتیو دایرکتوری، بر روی سرورهایی که به عنوان DC استفاده می‌شوند، مراحل زیر را دنبال کنید:

۱. کنسول Windows Server Backup را اجرا کنید.
۲. در پنل Action، بر روی Backup Once کلیک کنید.
۳. در صفحه "Backup Options" بر روی "Differenet Options" کلیک کنید.
۴. در صفحه "Select Backup Configuration"، Custom را انتخاب نموده و بر روی Next کلیک کنید.
۵. بر روی دکمه Add Items کلیک نموده و و پس از افزودن System state، بر روی Next کلیک کنید.



شکل ۱۲-۳۰

۶. در صفحه "Specify Destination Type" نوع محل ذخیره‌سازی فایل Backup (هارد دیسک یا محلی بر روی شبکه) را تعیین نموده و بر روی Next کلیک کنید.
۷. در صفحه "Select Backup Destination" محل ذخیره‌سازی فایل Backup را تعیین نموده و بر روی Next کلیک کنید.
۸. در صفحه "Confirmation" بر روی دکمه Backup کلیک کنید تا عملیات آغاز گردد. پس از اتمام کار بر روی Close کلیک کنید.

## ایجاد Backup در خط فرمان

جهت ایجاد Backup از System State با استفاده از خط فرمان می‌توانید از دستور زیر استفاده کنید:

```
Wbadmin.exe start systemstatebackup -target <volumename>
```

دقت داشته باشید که در دستور بالا، <volumename> نام Volume ای است که فایل Backup بر روی آن ذخیره می‌شود (مانند F:).

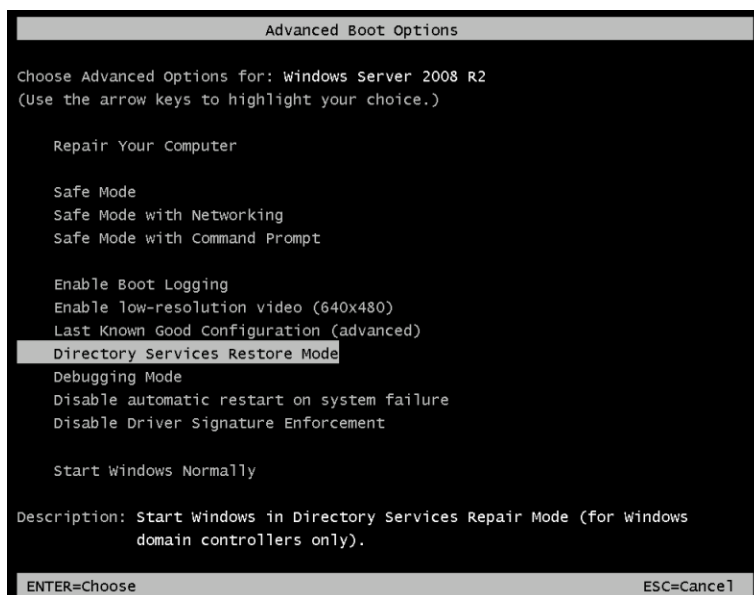
## ۲-۲-۱۲ بازگردانی Backup ایجاد شده از اکتیو دایرکتوری

دو نوع اقدام جهت بازگردانی Backup که از اکتیو دایرکتوری گرفته می‌شود وجود دارد:

- ♦ **Nonauthoritative**: این روش جهت بازگردانی Backup که از System State گرفته شده (که شامل اکتیو دایرکتوری نیز هست)، استفاده می‌گردد.
- ♦ **Authoritative**: این روش جهت بازگردانی اشیاء موجود در اکتیو دایرکتوری استفاده می‌شود.

جهت انجام یک بازگردانی Nonauthoritative لازم است حداقل یک Backup از System State (که از روی یک DC گرفته شده) و همچنین رمز عبور DSRM (که در زمان تبدیل سرور به DC تعیین شده) را در اختیار داشته باشید. پس از فراهم نمودن موارد ذکر شده، مراحل زیر را دنبال کنید:

۱. سرور را Restart نموده و کلید F8 را فشار دهید تا به منوی Advanced Boot Options وارد شوید.
۲. گزینه Directory Services Restore Mode را انتخاب نموده و Enter را فشار دهید.



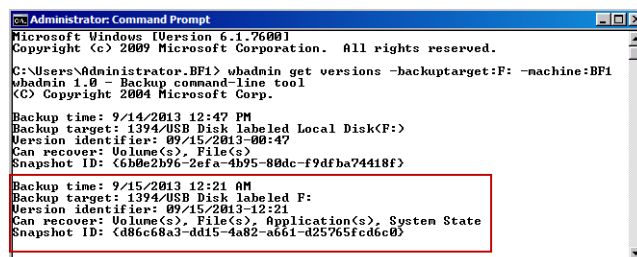
شکل ۳۱-۱۲

۳. مشخصات حساب کاربری مدیر DSRM را وارد نموده و به محیط DSRM وارد شوید.
۴. از منوی Start، بروی Command Prompt کلیک راست نموده و Run as Administrator را انتخاب کنید.
۵. جهت مشاهده Backup‌هایی که بروی سرور قرار دارند از دستور کلی زیر استفاده می‌شود:

```
wbadmin get versions -backuptarget:<drive>:-machine:<computername>
```

در دستور بالا، <drive> نام درایوی است که Backup در آن ذخیره شده و <computername> نیز نام کامپیوتر/سروری است که درایو مورد نظر بروی آن قرار دارد. پارامتر -machine تنها زمانی که فایل‌های Backup از چندین ماشین بروی دیسک قرار دارند استفاده می‌گردد. به عنوان مثال با فرض اینکه Backup‌های ایجاد شده از System State در درایو F از سرور BF1 قرار دارند، جهت مشاهده آنها دستور زیر را وارد نمایید:

```
wbadmin get versions -backuptarget:F: -machine:BF1
```



شکل ۱۲-۳۲

۶. پس از مشاهده Backup‌ها، ورژن Backup مورد نظر (که شامل System State است) را در عبارت زیر جایگذاری کنید:

```
wbadmin start systemstaterecovery -version:<MM:DD:YYYY-HH:MM>  
-backuptarget:<drive>:-machine:<computername> -quiet
```

در دستور بالا، پارامتر -quiet اعلام می‌کند که قصد دارید عمل بازگردانی را انجام دهید و همچنین SYSVOL نیز تغییر نکرده است. دستوری که وارد می‌کنید باید چیزی شبیه به زیر باشد:

```
wbadmin start systemstaterecovery -version:<09:15:2013-12:21>  
-backuptarget:F: -machine:BF1 -quiet
```

چنانچه قصد دارید پس از اتمام یک بازیابی Nonauthoritative، بازیابی Authoritative انجام دهید،

کامپیوتر را Restart نکنید. زمانی که DC را Restart می‌کنید AD DS و Active Directory Certificate Services تشخیص می‌دهند که عمل Restore رخ داده و بطور خودکار یکپارچگی پایگاه‌داده‌های خود را بررسی می‌کنند.

### بازگردانی Authoritative

هدف از بازگردانی Authoritative، بازگردانی اشیاء یا کانتینری از اشیاء حذف شده (مثل OU) به وضعیتی است که در هنگام Backup گیری قبل از حذف شدن داشته‌اند. زمانی که Backup های ایجاد شده از اکتیو دایرکتوری را با روش Nonauthoritative بازگردانی می‌کنید، اشیائی مانند OU ها بازگردانی نمی‌شوند، بنابراین لازم است که با انجام بازگردانی Authoritative، و قبل از اینکه عمل تکثیر انجام شود، هرکدام از اشیاء مورد نظر به وضعیت قبلی خود بازگردانیده شوند. برای انجام یک بازگردانی Authoritative، قبل از تکثیر تغییرات در دامنه، مراحل زیر را دنبال نمایید:

۱. ابتدا سرور را به یکی از روش‌های روبرو ایزوله نمایید: جدا کردن کابل شبکه، یا وارد نمودن دستور `Repadmin /options <servername> +DISABLE_INBOUND_REPL`
۲. AD DS را به یکی از روش‌های روبرو متوقف نمایید: سرویس آن را در Server Manager و در قسمت Services متوقف نموده، یا دستور `net stop ntds` را در خط فرمان وارد کنید.
۳. عبارت `ntdsutil` را در خط فرمان وارد نموده و Enter را فشار دهید.
۴. عبارت `authoritative restore` را وارد نموده و Enter را فشار دهید.
۵. برای بازگردانی اشیاء مانند OU، عبارت `restore subtree <DN>` که در آن <DN> نام DN مربوط به شیء در حال بازگردانی است را وارد نمایید. به عنوان مثال برای OU با نام HR داریم:  
`restore object "OU=HR,DC=bigfirm,DC=com"`
۶. برای بازگردانی یک شیء تنها مانند حساب کاربری، عبارت `restore object <DN>` که در آن <DN> نام DN مربوط به شیء در حال بازگردانی است را وارد نمایید.
۷. عبارت `quit` را یکبار برای خروج از حالت بازگردانی authoritative و سپس برای خروج از حالت Ntdsutil وارد کنید.
۸. سرور را به صورت معمولی Restart نمایید.



## « فصل ۱۳ »

اشتراک‌گذاری اینترنت و راه‌اندازی سرور  
NAT

**Sharing Internet and Setup NAT**  
**Server**



یکی از مسائلی که همواره در شبکه‌های داخلی وجود دارد، امکان دسترسی کاربران به اینترنت می‌باشد. همانطور که اطلاع دارید، اکثر شبکه‌های داخلی از آدرس‌های IP خصوصی (Invalid) برای ارتباط میان کاربران استفاده می‌کنند. آدرس‌های خصوصی در اینترنت قابل شناسایی نیستند زیرا در ارتباطات تحت اینترنت، از آدرس‌های عمومی یا معتبر (Valid) استفاده می‌شود. سرویس NAT<sup>۱</sup>، راه حلی است که برای برطرف نمودن این مشکل ایجاد شده است. با استفاده از این سرویس، تنها با داشتن یک یا تعدادی محدود از آدرس‌های IP معتبر، می‌توان دسترسی کاربران به محیط اینترنت را فراهم نمود.

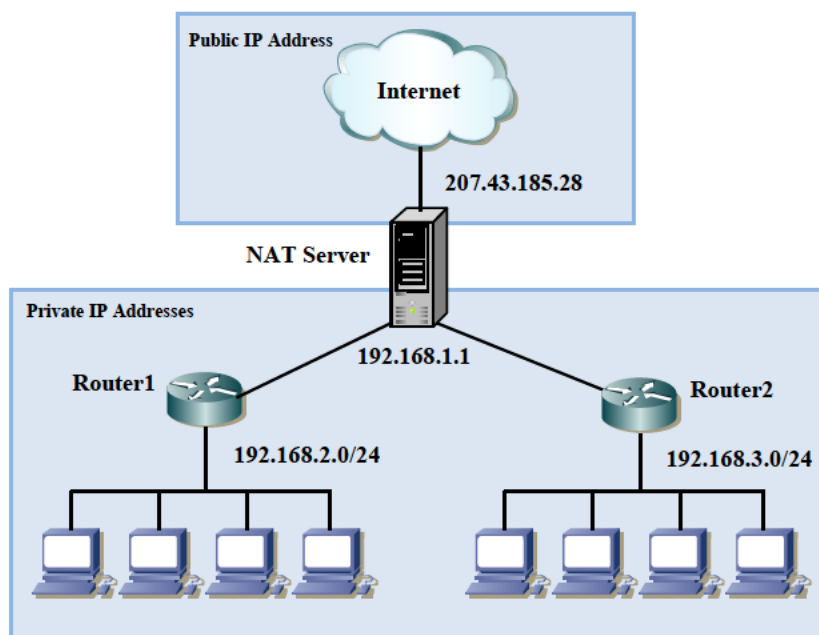
در این فصل قصد داریم نحوه راه‌اندازی یک سرور NAT و روش‌هایی که به این منظور مورد استفاده قرار می‌گیرند را شرح دهیم. بطور کلی مهمترین مباحث این فصل عبارتند از:

- ♦ آشنایی با مفاهیم اولیه NAT
- ♦ برپایی NAT با استفاده از سرویس ICS
- ♦ نصب و پیکربندی NAT به کمک Server Manager

### ۱۳-۱ مفاهیم اولیه NAT

سرویس NAT برگرفته از عبارت Network Address Translation و به معنای ترجمه آدرس شبکه می‌باشد. همانطور که اشاره کردیم در اینترنت کلیه ماشین‌ها باید دارای آدرس IP معتبر باشند، بنابراین با استفاده از آدرس‌های IP خصوصی امکان برقراری ارتباط تحت اینترنت وجود نخواهد داشت. فرض کنید شبکه شما دارای ۱۰۰۰ ماشین باشد که همگی قرار است به اینترنت متصل شوند. در این حالت خرید ۱۰۰۰ آدرس IP از نوع Valid کار عاقلانه‌ای نیست زیرا علاوه بر بحث هزینه بالای خرید این آدرس‌ها، با محدودیت خرید این تعداد نیز روبرو خواهید بود، زیرا به دلیل گسترش چشمگیر کاربران اینترنت مشکل کمبود آدرس‌های IPv4 و در نتیجه محدودیت در اختصاص این آدرس‌ها بوجود آمد. به عنوان مثال شما برای شرکت خود که دارای ۱۰۰۰ ماشین است، ممکن است قادر باشید تنها بین ۱ تا ۴ آدرس IP از مرکز ISP خریداری کنید. اما جای نگرانی نیست زیرا به لطف سرویس NAT و با داشتن همین تعداد از آدرس‌های IPv4 (از نوع Valid) قادر خواهید بود تمام کاربران خود را به اینترنت متصل کنید. در واقع هر کاربر قبل از اینکه بتواند به اینترنت متصل شود، ابتدا به سرور NAT وصل شده و پس از تغییر آدرس او از Invalid (آدرس‌های داخلی) به Valid (آدرس‌های عمومی) می‌تواند به شبکه اینترنت متصل گردد. برای درک بهتر این موضوع به تصویر زیر دقت نمایید:





شکل ۱-۱۳

همانطور که مشاهده می‌کنید، شبکه‌های داخلی با آدرس‌های خصوصی 192.168.2.0/24 و 192.168.3.0/24 به سرور NAT با آدرس 192.168.1.1 متصل شده و چون در این سرور آدرس عمومی 207.43.185.28 قرار داده شده است، ابتدا کلیه آدرس‌های خصوصی در این سرور به آدرس 207.43.185.28 تبدیل شده و سپس کامپیوترها می‌توانند از طریق آن به اینترنت متصل شوند.



متذکر می‌شویم که دامنه آدرس‌های Private برای سه کلاس A، B و C به صورت زیر می‌باشد:

Class A: 10.0.0.0 to 10.255.255.255

Class B: 172.16.0.0 to 172.31.255.255

Class C: 192.168.0.0 to 192.168.255.255

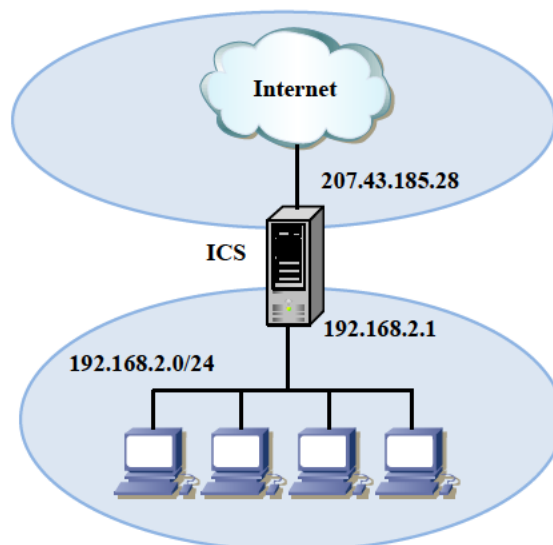
هر آدرسی به غیر از آدرس‌های بالا به عنوان آدرس‌های Public یا Valid شناخته می‌شود.

جهت راه‌اندازی سرویس NAT در ویندوز سرور 2008 و 2008R2 به دو طریق می‌توان اقدام نمود:

- استفاده از سرویس ICS (Internet Connection Sharing)
- استفاده از سرویس Routing And Remote Access Services

## ۱۳-۲ سرویس ICS

سرویس ICS<sup>۱</sup> امکان اشتراک گذاری اینترنت در شبکه را فراهم می‌نماید. با استفاده از این سرویس می‌توانید اینترنت را توسط سرور شبکه دریافت نموده و در میان کاربران شبکه اشتراک گذاری، بنابراین همگی قادر خواهند بود به اینترنت متصل شوند. این سرویس بیشتر در شبکه‌های کوچک مورد استفاده قرار می‌گیرد زیرا امکانات محدودی را جهت مدیریت در اختیار قرار می‌دهد. به عنوان مثالی در این رابطه فرض کنید که در یک شبکه، ۱۵۰ کامپیوتر در اختیار دارید که قصد دارید همگی آنها از اینترنت استفاده کنند. در چنین شرایطی می‌توانید با راه اندازی سرویس ICS بر روی سرور شبکه (البته به شرطی که سرور به اینترنت متصل باشد) امکان اشتراک گذاری اینترنت در شبکه را فراهم نموده و کاربران قادر باشند به اینترنت متصل شوند. در شکل زیر مثالی در این رابطه نشان داده شده است.



شکل ۱۳-۲

همانطور که در شکل بالا مشاهده می‌کنید کاربران شبکه 192.168.2.0 به سرور موجود در این شبکه با آدرس 192.168.2.1 متصل شده‌اند. چنانچه این سرور به اینترنت متصل باشد و سرویس ICS بر روی آن راه اندازی گردد، کاربران می‌توانند با آدرس IP عمومی سرور به اینترنت متصل شوند. نکته‌ای که لازم است به آن توجه داشته باشید این است که آدرس IP کاربران باید در محدوده 192.168.0.0/24 باشد. این آدرس‌ها معمولاً در شبکه‌های داخلی متصل به اینترنت استفاده می‌شوند.

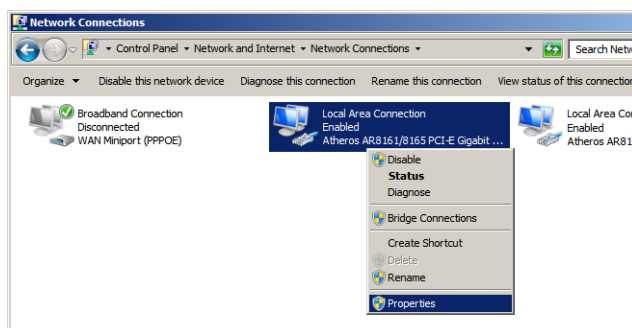
### ۱۳-۲-۱ راه اندازی NAT به کمک سرویس ICS

اکنون که با مفهوم ICS آشنا شدید اجازه دهید نحوه راه اندازی آنرا نیز شرح دهیم. قبل از اقدام به راه اندازی این سرویس باید موارد زیر را فراهم نمایید:

- ♦ دو عدد کارت شبکه، یکی برای ارتباط با شبکه و دیگری جهت اتصال به اینترنت. کارت شبکه‌ای که به شبکه داخلی متصل است دارای آدرس Private و کارتی که به اینترنت متصل است دارای آدرس Public می‌باشد (این آدرس توسط مراکز ISP تعیین می‌شود).
- ♦ دریافت اینترنت از مرکز ISP جهت اشتراک گذاری.
- ♦ غیرفعال کردن سرویس Routing And Remote Access در صورتی که قبلاً اقدام به فعال‌سازی آن نموده باشید.

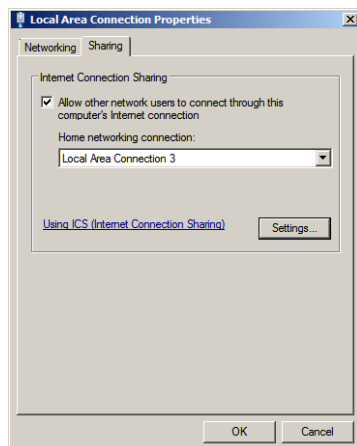
پس از فراهم نمودن موارد بالا، مراحل زیر را جهت فعال‌سازی ICS دنبال کنید:

۱. به مسیر «Start» «Control Panel» «Network and Sharing Center» بروید.
۲. بروی کارت شبکه‌ای که از طریق آن به اینترنت متصل می‌شوید کلیک‌راست نموده و Properties را انتخاب کنید



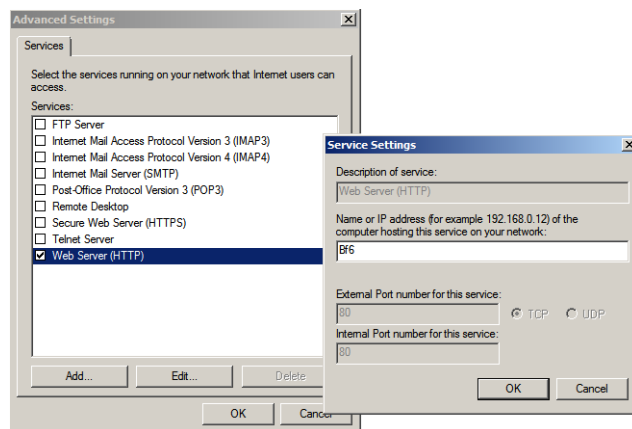
شکل ۱۳-۳

۳. در پنجره «Local Area Connection Properties» تب Sharing را انتخاب نمایید (چنانچه برای اتصال به اینترنت Connection ایجاد نموده باشید، می‌توانید جهت دسترسی به تب Sharing، از طریق کلیک‌راست بروی این Connection و انتخاب Properties نیز اقدام کنید).
۴. گزینه Allow other network users to connect through this computer's internet connection را فعال نموده و در قسمت Home Networking Connection کارت شبکه‌ای که از طریق آن به شبکه داخلی متصل هستید را انتخاب نمایید.



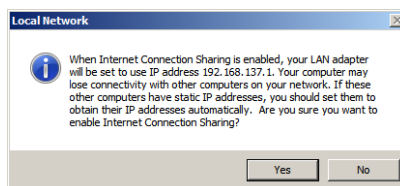
شکل ۱۳-۴

۵. با انتخاب دکمه Settings می‌توانید سرویس‌های فعال بر روی شبکه، که کاربران با استفاده از اینترنت می‌توانند به آنها دسترسی داشته باشند را تعیین کنید. جهت انجام این کار پس از کلیک بر روی سرویس مورد نظر، نام یا آدرس IP کامپیوتری که این سرویس بر روی آن اجرا می‌شود را وارد نموده و بر روی OK کلیک کنید. چنانچه سرویس مورد نظر در فهرست وجود نداشت می‌توانید با کلیک بر روی دکمه Add آنها اضافه کنید. پس از تعیین این سرویس‌ها بر روی OK کلیک کنید.



شکل ۱۳-۵

۶. در صفحه "Local Area Connection Properties" بر روی OK کلیک کنید. پیغامی ظاهر شده و اعلام می‌کند که آدرس IP کارت شبکه (داخلی) به 192.168.137.1 تغییر پیدا می‌کند. بر روی Yes کلیک کنید.



شکل ۱۳-۶

### ۱۳-۲-۲ تغییر تنظیمات کاربران

پس از اینکه سرویس ICS فعال شد، به دلیل تغییر آدرس کارت شبکه موجود بر روی سرور، ممکن است ارتباط کاربران با آن قطع گردد. برای رفع این مشکل لازم است به تنظیمات کارت شبکه کاربران رفته و نحوه دریافت آدرس IP را به صورت "Obtain an IP address automatically" (سرویس DHCP) تنظیم کنید. منظور از سرویس DHCP در این قسمت، سرویس موجود بر روی ویندوز است که با DHCP Server Role متفاوت است. این سرویس قابلیت‌های محدودی را جهت اختصاص آدرس IP به کاربران فراهم می‌نماید. دقت داشته باشید که با فعال‌سازی سرویس ICS، آدرس‌های IP قابل اختصاص به کاربران از محدوده 192.168.0.0/24 (255.255.255.0) خواهد بود و همچنین Default Gateway این کاربران برابر با آدرس IP کارت شبکه‌ای است که سرور از طریق آن به شبکه متصل است (به عنوان مثال ۱۹۲.۱۶۸.۱۳۷.۱).

### ۱۳-۳ سرویس Routing And Remote Access

سرویس Routing And Remote Access دیگر سرویسی است که با استفاده از آن می‌توان یک سرور NAT ایجاد نمود. این سرویس در مقایسه با ICS امکانات و قابلیت‌های بیشتری جهت پیکربندی و مدیریت NAT فراهم می‌کند که از جمله می‌توان به موارد زیر اشاره نمود:

- ♦ استفاده از قابلیت Routing در صورت وجود چندین شبکه داخلی
- ♦ امکان استفاده از آدرس‌های IP با محدوده‌ای غیر از 192.168.0.0/24 در شبکه‌های داخلی
- ♦ امکان استفاده از سرویس DHCP Server Role جهت پیکربندی کامل تنظیمات IP

نکته‌ای که باید به آن دقت داشته باشید این است که نمی‌توانید بطور همزمان سرویس ICS و سرویس Routing And Remote Access را بر روی یک کامپیوتر فعال کنید. بنابراین قبل از اقدام به راه‌اندازی هر سرویس، از غیرفعال بودن دیگر سرویس مطمئن شوید.

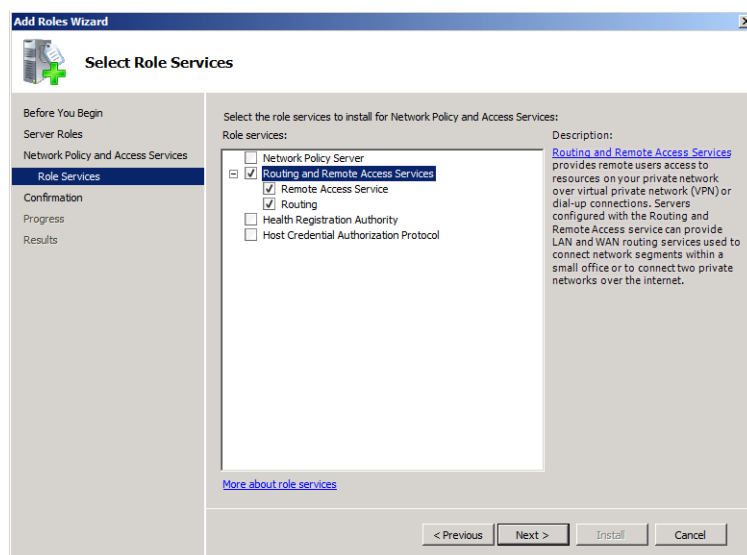
### ۱۳-۳-۱ نصب سرویس Routing And Remote Access

همانند سرویس ICS، قبل از اقدام به راه اندازی NAT باید موارد زیر را فراهم نمایید:

- ♦ دو عدد کارت شبکه، یکی برای ارتباط با شبکه و دیگری جهت اتصال به اینترنت.
- ♦ دریافت اینترنت از مرکز ISP جهت استفاده در سرویس Routing And Remote Access.
- ♦ غیرفعال کردن سرویس ICS در صورتی که قبلاً اقدام به فعال سازی آن نموده باشید.

اکنون پس از فراهم نمودن موارد بالا می‌توانید مراحل زیر را دنبال کنید:

۱. در کنسول Server Manager به قسمت Roles رفته و Add Roles را انتخاب کنید.
۲. در صفحه "Select Server Roles"، گزینه Network Policy and Access Services را انتخاب نموده و بر روی Next کلیک کنید.
۳. در صفحه "Introduction to Network Policy and Access Services"، اطلاعات ارائه شده در مورد این Role را مشاهده نموده و بر روی Next کلیک کنید.
۴. در صفحه "Select Role Services" رل سرویس Routing And Remote Access را به همراه زیرشاخه‌های آن انتخاب نموده و بر روی Next کلیک کنید.



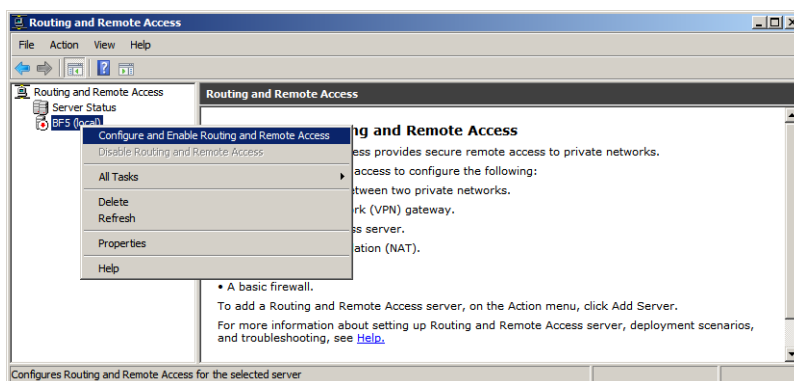
شکل ۱۳-۷

۵. در صفحه "Confirm Installation Selections" بر روی Install کلیک نموده و منتظر بمانید تا عملیات نصب به اتمام برسد. در نهایت بر روی Close کلیک کنید.

### ۱۳-۲ پیکربندی NAT در کنسول Routing And Remote Access

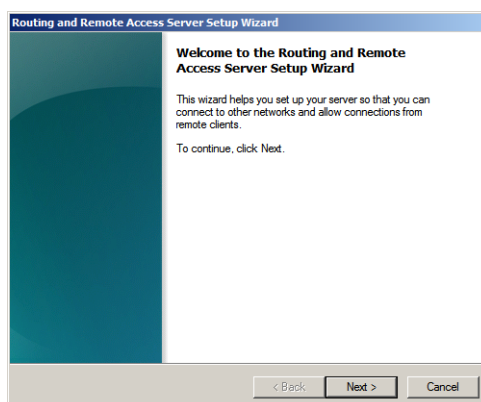
پس از نصب سرویس Routing And Remote Access، باید آنرا جهت دسترسی کاربران پیکربندی نمایید. جهت پیکربندی مراحل زیر را دنبال کنید:

۱. کنسول Routing And Remote Access را از مسیر «Start» «Administrative Tools» Routing And Remote Access اجرا کنید.
۲. بروی نام سرور کلیک راست نموده و گزینه Configure and Enable Routing and Remote Access را انتخاب کنید.



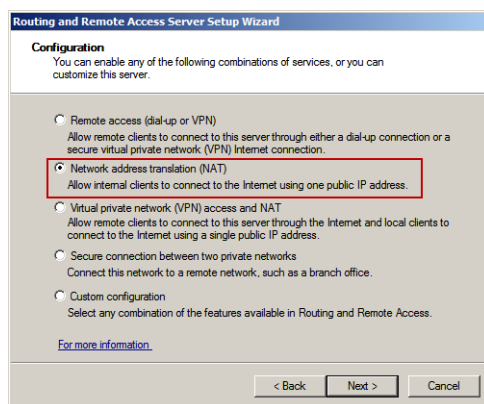
شکل ۱۳-۸

۳. در صفحه «Welcome to the Routing and Remote Access Server Setup Wizard» بروی Next کلیک کنید.



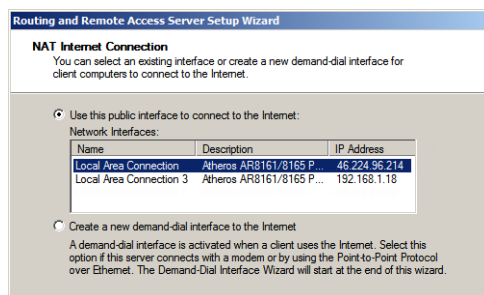
شکل ۱۳-۹

۴. در صفحه “Configuration”، گزینه (NAT) Network address translation را انتخاب نموده و بر روی Next کلیک کنید.



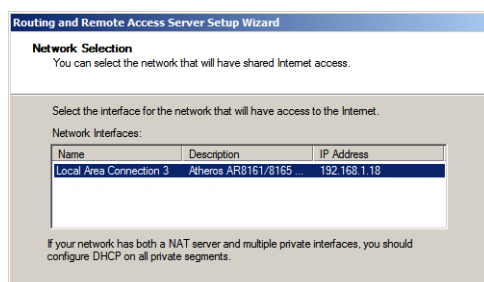
شکل ۱۰-۱۳

۵. در صفحه “NAT Internet Connection” کارت شبکه‌ای که با آن به اینترنت متصل هستید را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۱۱-۱۳

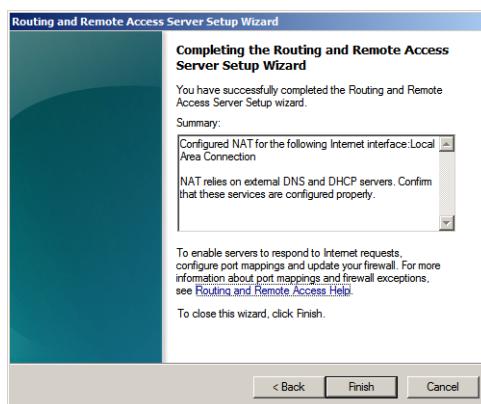
۶. در صفحه “Network Selection” کارت شبکه‌ای که با استفاده از آن به شبکه متصل می‌شوید را انتخاب نموده و بر روی Next کلیک کنید.



شکل ۱۲-۱۳



۷. در صفحه "Completing the Routing and Remote Access Server Setup Wizard" بر روی Finish کلیک کنید.



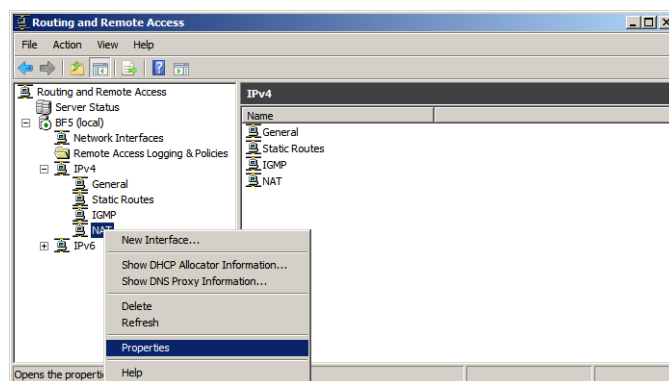
شکل ۱۳-۱۳

### ۳-۳-۱۳ پیکربندی DHCP در NAT

پس از نصب و پیکربندی سرویس Routing And Remote Access، می‌توانید سرویس DHCP را جهت اختصاص آدرس IP و تنظیمات مرتبط با آن پیکربندی کنید. برای پیکربندی سرویس DHCP، می‌توانید هم از رل DHCP Server و هم از سرویس NAT DHCP Server که در سرویس NAT فراهم شده است استفاده نمایید. نحوه استفاده از رل DHCP در فصل‌های قبل شرح داده شده است، بنابراین در اینجا نحوه استفاده از DHCP موجود در NAT را شرح می‌دهیم.

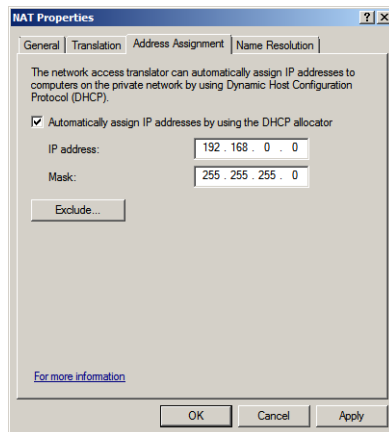
برای پیکربندی NAT DHCP مراحل زیر را دنبال نمایید:

۱. در کنسول Routing And Remote Access بر روی IPv4، NAT کلیک راست نموده و Properties را انتخاب کنید.



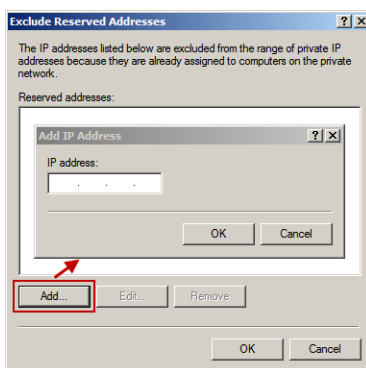
شکل ۱۴-۱۳

۲. در تب Address assignment گزینه Automatically assign IP address by using the DHCP allocator را فعال کنید. در قسمت IP address محدوده آدرس‌های IP جهت اختصاص به کاربران شبکه داخلی، و در قسمت mask نیز قاب زیر شبکه متناظر با آنرا تعیین کنید.



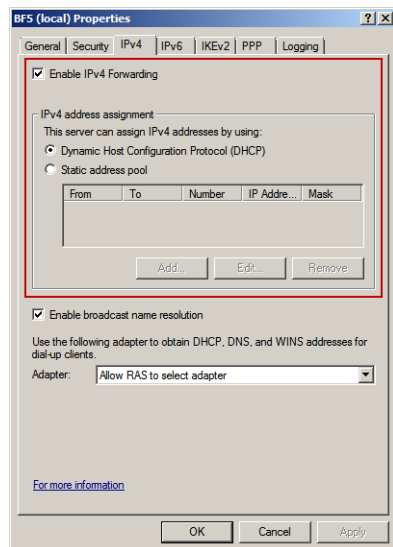
شکل ۱۳-۱۵

۳. چنانچه قصد دارید آدرس‌هایی را جهت استفاده نشدن در DHCP تعیین کنید، دکمه Exclusion را انتخاب نموده و پس از کلیک بر روی دکمه Add آدرس مورد نظر را وارد نمایید.



شکل ۱۳-۱۶

۴. در هر پنجره بر روی OK کلیک نموده و سپس پنجره‌ها را ببندید.  
دقت داشته باشید که برای دسترسی به تنظیمات DHCP یا سایر تنظیمات NAT می‌توانید از طریق کلیک راست بر روی نام سرور و انتخاب Properties نیز اقدام نمایید.



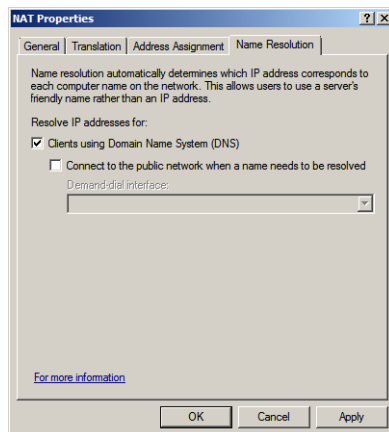
شکل ۱۳-۱۷

### ۱۳-۳-۴ پیکربندی DNS در NAT

همانطور که قبلاً شرح داده‌ایم، از سرور DNS جهت تحلیل نام میزبان به آدرس IP و برعکس (تحلیل آدرس IP به نام) استفاده می‌گردد. زمانی که سرور NAT را فعال می‌کنید، لازم است سرویس DNS را نیز برای این آن پیکربندی نمایید زیرا کاربران باید با خارج از شبکه ارتباط برقرار نمایند. چنانچه قبلاً DNS Role را نصب نکرده‌اید، لازم است جهت استفاده از NAT نسبت به نصب و پیکربندی آن در Server Manager اقدام کنید.

علاوه بر DNS Role، در سرویس NAT نیز قابلیت وجود دارد که با استفاده از آن می‌توانید این تحلیل‌ات نام را انجام دهید. این قابلیت برای شبکه‌های کوچک مناسب است و پیغام‌های DNS کاربران داخلی شبکه را به سمت سرورهای DNS موجود در خارج از شبکه هدایت می‌نماید. برای پیکربندی این سرویس مراحل زیر را دنبال کنید:

۱. در کنسول Routing And Remote Access بر روی «IPv4» NAT کلیک‌راست نموده و Properties را انتخاب کنید.
۲. در پنجره «NAT Properties»، تب Name Resolution را انتخاب نموده و گزینه Client Using Domain Name System را فعال کنید.



شکل ۱۳-۱۸

۳. چنانچه سرور NAT با استفاده از اتصالات Dial-up یا VPN به اینترنت متصل می‌گردد، گزینه Connect to public network when a name need to be resolved را فعال کنید.
۴. بر روی OK کلیک کنید.

### ۱۳-۳-۵ نکاتی در رابطه با پیکربندی کاربران NAT

در رابطه با پیکربندی کاربران NAT لازم است موارد زیر را لحاظ نمایید:

۱. چنانچه تنظیمات کاربران را به صورت دستی پیکربندی می‌نمایید، آدرس Default Gateway آنها را برابر با آدرس IP کارت شبکه‌ای که سرور از طریق آن با شبکه داخلی ارتباط برقرار می‌کند قرار دهید.
۲. چنانچه شبکه متشکل از چندین قسمت مجزا بوده بطوری که در هر قسمت از Router استفاده می‌شود، باید این Routerها طوری پیکربندی شوند که ترافیک خروجی آنها به سمت کارت شبکه داخلی سرور باشد.
۳. تنظیمات سرویس DNS و DHCP را برای سرور بررسی کنید. چنانچه از سرور فعلی به عنوان سرور DNS و DHCP استفاده می‌کنید، از انجام صحیح تنظیمات بر روی آنها اطمینان حاصل نمایید.
۴. جهت اطلاع از چگونگی پیکربندی سرورهای DNS و DHCP در شبکه، به فصل‌های مربوطه در کتاب مراجعه کنید.



تا قبل از ویندوز سرور 2008، به این دلیل که آدرس‌های IPv4 به صورت گسترده در سطح اینترنت مورد استفاده قرار می‌گرفتند، سرویس NAT از اهمیت زیادی برخوردار بود. با پیدایش IPv6 و توسعه آن در سطح اینترنت، شاید در آینده‌ای نه چندان دور، دیگر مفهوم NAT چندان پر اهمیت نباشد زیرا تعداد آدرس‌های IPv6 آنقدر زیاد است که هرگز با کمبود آن مواجه نخواهید شد. بنابراین می‌توانید به هر کامپیوتر در شبکه یک آدرس IPv6 اختصاص دهید و با آن به راحتی به اینترنت متصل شوید. البته استفاده از IPv6 می‌تواند هزینه‌هایی را نیز متحمل شبکه‌ها نماید ولی چاره‌ای جز استفاده از آنها نخواهد بود!

## منابع و مأخذ:

1. Mark Minasi, Darril Gibson, Aidan Finn, Wendy Henry, Biron Hynes, Mastering Windows Server 2008 R2, Wiley, 2010, ISBN: 978-0-470-53286-7
2. Rand Morimoto, Michael Noel, Omar Droubi, Ross Mistry, Chris Amaris, Windows Server 2008 Unleashed, Sams, 2008, ISBN-13: 978-0-672-32930-2
3. Mark E Russinovich, David A Solomon, Alex Ionescu, Windows Internals, Part 2, 6th Edition, Microsoft Press, 2012, ISBN: 978-0-7356-6587-3
4. Orin Thomas, Windows Server 2008 R2 Secrets, John Wiley & Sons, Inc, 2011, ISBN: 978-0-470-88658-8
5. Dan Holme, Nelson Ruest, Danielle Ruest, Jason Kellington, Configuring Windows Server 2008 Active Directory (70-640), 2nd Edition, Microsoft Press, 2011, ISBN: 978-0-7356-5193-7
6. Will Panek, Tylor Wentworth, James Chellis, MCTS: Windows Server 2008 Network Infrastructure Configuration Study Guide (70-642), Wiley, 2008, ISBN: 978-0-470-26169-9
7. Tony Northrup, J.C Mackin, MCTS Self-Paced Training Kit (Exam 70-642): Configuring Windows Server 2008 Network Infrastructure, 2nd Edition, Microsoft Press, 2008, ISBN: 978-0-7356-5160-9
8. J.C Mackin, Anil Desai, Configuring Windows Server 2008 Application Infrastructure (70-643), Microsoft Press, 2008,
9. Derek Melber, Windows Group Policy Windows Server 2008 and Windows Vista, Microsoft Press, 2008
10. Joe Habraken, Teach Yourself Windows Server 2008 in 24 Hours, Sams, 2008, ISBN: 978-0-672-33012-4
11. William R Stanek, Windows Server 2008 Inside Out, Microsoft Press, 2008, ISBN: 978-0-7356-2438-2
12. Charlie Russel, Craig Zacker, Introducing Windows Server 2008 R2, Microsoft Press, 2010
13. Anderson Christa, Griffin Kristin L, Windows Server 2008 R2 Remote Desktop Services, Microsoft Press, 2010







