Microsoft

MCTS EXAM
70-640

Configuring Windows Server® 2008 Active Directory®

Dan Holme
Nelson Ruest
Danielle Ruest

SELF-PACED

Training Kit

فصل ۱

نصب

Active Directory Domain Services و سرویسهای وابسته ، پایه و اساس شبکه‌های سازمانی مبتنی بر ویندوز می‌باشند که مجموعاً به عنوان ابزارهای ذخیره سازی اشیاء مانند حسابهای کاربری (User Account) ،کامپیوترها و سرویسها عمل می‌کنند . بطور مثال تایید هویت کاربران و کامپیوترها یا فراهم کردن مکانیزمی جهت دسترسی کاربران و کامپیوترها به منابع شبکه از وظایف این ابزارها می‌باشد.

در این فصل ورود به دنیای Active Directory در ویندوز سرور 2008 با نصب Active Directory Domain Services و ساخت یک Domain Controller یا به اختصار DC در یک forest در Active Directory آغاز می‌شود. شما در نتیجه کار کردن با Active Directory با مفاهیم و ویژگیهای بسیاری آشنا شده‌اید. پس از خواندن این متن متوجه خواهید شد که ویندوز سرور 2008 با ارتقاء آنها مسیر تکامل Active Directory را ادامه می دهد.

این فصل تمرکز را روی ساخت یک forest در Active Directory با یک دامنه روی یک DC می‌گذارد . تمرینهای عملی در این فصل شما را در ساخت یک DC با نام contoso.com یاری می‌کنند که در ادامه شما از این دامنه در تمام تمرینهای بعدی کتاب استفاده خواهید کرد. در فصل ۸ "Authentication" فصل ۱۰ "Domain Controllers" و فصل ۱۲ "Domains and Forests" پیاده سازی سناریوهای دیگری از جمله forest هایی با چند دامنه ، ارتقا forest موجود به ویندوز سرور 2008 و گزینه های نصب پیشرفته را یاد می‌گیرید . در فصل ۱۴ "Active Directory Lightweight Directory Services" ، فصل ۱۵ "Active Directory Certificate Services and Public Key Infrastructures" ، فصل ۱۶ "Active Directory Rights Management Services" و فصل ۱۷ "Active Directory Federation Services" جزئیات سرویسهای Active Directory مانند Active Directory Lightweight Directory ، Active Directory Certificate Services and Public Key Infrastructures ، Active Directory Rights Management Service و Active Directory Federated Services را یاد می گیرید

اهداف امتحانی در این فصل

- پیکر بندی زیرساخت Active Directory
  - پیکربندی یک forest یا یک دامنه

دروس این فصل

- درس ۱ : نصب Active Directory Domain Services
- درس ۲: Active Directory Domain Services روی Server Core

قبل از شروع

جهت تکمیل دروس این فصل موارد زیر باید اجرا گردد :

- دو دستگاه کامپیوتر برای نصب ویندوز سرور 2008 آماده شود . سیستمها می‌توانند سخت‌افزاری بوده و دارای حداقل امکانات برای نصب ویندوز سرور 2008 باشند . این حداقل‌ها را می‌توان از آدرس http://technet.microsoft.com/en-us/windowsserver/2008/bb414778.aspx استخراج کرد . حداقل میزان حافظه 512 MB ، فضای خالی دیسک 10 GB و پردازنده ۳۲ بیتی با سرعت ساعت 1 GHz یا پردازنده ۶۴ بیتی با حداقل سرعت ساعت 1.4 GHz مورد نیاز است . بجای سرور سخت افزاری امکان استفاده از ماشینهای مجازی با همین مشخصات وجود دارد .
- نسخه آزمایشی ویندوز سرور 2008 آماده گردد . در زمان نوشته شدن کتاب (زبان اصلی) از آدرس زیر قابل دانلود بوده است : http://www.microsoft.com/windowsserver2008

در دنیای واقعی

دن هلم

DC ها فرایندهای مدیریت Identity and Access را که در شبکه‌های ویندوزی از لحاظ صحت و امنیت حیاتی هستند اجرا می‌کنند . به همین دلیل بسیاری از سازمانها سروری را برای نقش DC انتخاب می‌کنند و نقش‌های دیگری را مانند سرویس فایل یا پرینت به آن سرور نمی‌دهند . در نسخه‌های قبلی ویندوز همزمان با ارتقا سرور به DC سرویسهای دیگری نصب می‌شد که ممکن بود نیازی به آن نداشته باشیم .این سرویسهای اضافی نیاز به نصب آپدیتها و وصله‌های امنیتی را افزایش می‌دهد و سرور را در معرض حمله هکرها قرار می‌دهد . ویندوز سرور 2008 این نگرانیها را از طریق معماری مبتنی بر نقشهای سروری از بین برده است . یعنی وقتی ویندوز روی سروری نصب می‌شود فقط نقشها و سرویسهای مرتبط افزوده می‌شود . بعلاوه نوع جدید نصب سرور بنام Server Core2008 (Server Core) نصب حداقلی از ویندوز است که حتی خط فرمان جایگزین رابط گرافیکی کاربر می‌شود . در این فصل در رابطه با این ویژگی‌های مهم سرورهای DC ویندوز سرور 2008 تجربیات جالبی بدست می‌آورید . این

تغییرات در معماری و ویژگی‌های DC ویندوز 2008 کمک زیادی به ارتقاء امنیت ، پایداری و مدیریت پذیری زیرساخت مدیریت identity and access می‌کند

درس ۱ : نصب Active Directory Domain Services

Active Directory Domain Services (AD DS) یک راه کار Identity and Access (IDA) را برای شبکه های سازمانی فراهم می‌کند. در این درس درباره AD DS و نقشهای دیگر Active Directory که توسط ویندوز سرور 2008 پشتیبانی می‌شود مطالبی را یاد می‌گیرید . همچنین با Server Manager ، ابزاری که با آن نقشهای سروری پیکربندی می‌شود، و ویزارد نصب پیشرفته Active Directory Domain Services آشنا می‌شوید. در این درس همچنین مفاهیم کلیدی IDA و Active Directory مرور می‌شود.

بعد از این درس شما می‌توانید :

- نقش Identity and Access را در یک شبکه سازمانی شرح بدهید .
- ارتباط بین سرویسهای Active Directory را درک کنید
- یک سرور DC را با نقش AD DS توسط رابط کاربری ویندوز پیکربندی کنید.

زمان تقریبی : ۶۰ دقیقه

Identity and Access ، Active Directory

همانطوریکه قبلاً اشاره شد Active Directory راه حل IDA را برای شبکه های سازمانی مبتنی بر ویندوز ارائه می‌دهد .IDA جهت تامین امنیت و نگهداری منابع شبکه از قبیل فایلها، e-mail ، برنامه های کاربردی و بانکهای اطلاعاتی ضروری است .زیر ساخت IDA باید بتواند :

- **اطلاعات کاربران ، گروهها ، کامپیوترها و دیگر هویتها را ذخیره کند** هویت به معنای عام معرف یک موجودیت می‌باشد که در شبکه کاری را انجام می‌دهد. بعنوان مثال یک کاربر می‌تواند سندی را از مسیر شبکه‌ای باز کند. امنیت سند بواسطه مجوزهای لیست کنترل دسترسی (ACL) تامین می‌شود. دسترسی به اسناد توسط زیرسیستم امنیت (Security Subsystem) سرور مدیریت می‌شود که هویت کاربر را با هویتهای موجود در ACL مقایسه کرده و مشخص می‌کند آیا کاربر می‌تواند به سند دسترسی داشته باشد یا خیر. کامپیوترها، گروهها، سرویسها و اشیاء دیگر هم عملیاتی را در شبکه انجام می‌دهند پس باید عنوان هویت را در موردشان بکار ببریم. از بین اطلاعاتی که درمورد یک هویت ذخیره می‌شود ویژگی‌هایی منحصر بفردی وجود دارد که هویت را مجزا می‌سازد . نمونه آن نام کاربری و مشخصه امنیتی (SID) و کلمه عبور می‌باشد. بنابراین انباره هویت (Identity Store) را می‌توان جزئی از اجزاء یک زیرساخت IDA به حساب آورد. انباره داده ی Active Directory با نام دیگر دایرکتوری یک انباره هویتی می‌باشد. دایرکتوری خود روی DC قرار دارد و توسط آن مدیریت می‌شود و DC سروری است که نقش AD DS را ایفا می‌کند.
- **تایید یک هویت** سرور تا زمانی که اعتبار هویت درخواست کننده را تایید نکند اجازه دسترسی به اسناد را صادر نمی کند. جهت سنجش اعتبار یک هویت ،کاربر رمزی را که فقط بین او و IDA شناخته شده است ارسال می کند. رمز ارسالی توسط کاربر و رمز موجود درانباره هویتی در پروسه ای با نام تایید هویت (Authentication) مقایسه می شود

تایید هویت از نوع Kerberos در یک دامنه Active Directory

در یک دامنه موجود در Active Directory پروتکلی با نام Kerberos جهت تایید هویت بکار می‌رود. زمانی که کاربری یا کامپیوتری وارد Domain می‌شود Kerberos اعتبار آنرا چک کرده و بسته اطلاعاتی با نام TGT (Ticket Granting Ticket) صادر می‌کند . قبل از اینکه کاربر جهت دریافت اطلاعات به سرور متصل شود یک درخواست Kerberos همراه TGT که معرف کاربر تایید هویت شده است به سمت DC ارسال می‌شود . DC بسته اطلاعاتی دیگری با نام Service Ticket برای کاربر صادر می‌کند. این بسته ،کاربر تایید هویت شده را به سرور معرفی می‌کند. کاربر Service Ticket را که تایید هویت کاربر را اثبات می‌کند به سرور ارائه می‌دهد

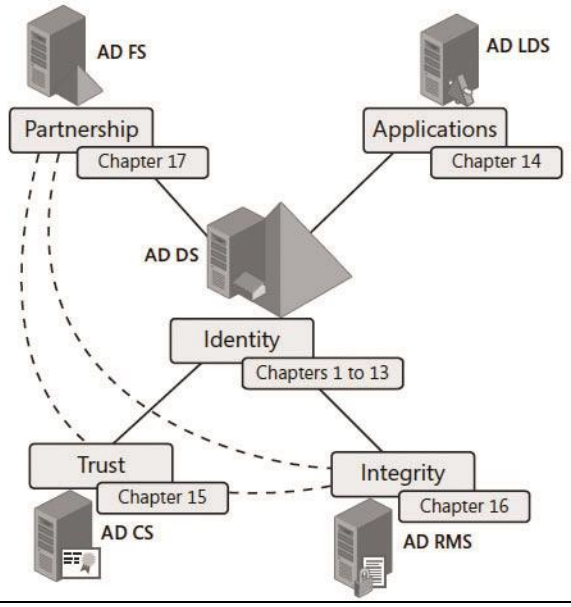
تراکنشهای Kerberos در شبکه باعث می‌شود کاربر فقط یکبار عملیات ورود به شبکه را انجام دهد . پس از ورود اولیه کاربر یا کامپیوتر به شبکه و دریافت TGT کاربر در کل دامنه دارای هویت خواهد بود و می تواند جهت معرفی به هر سرویسی Service Ticket دریافت کند . همه این مراحل توسط کلاینت Kerberos و سرویسهای موجود در ویندوز هدایت می‌شود و از چشم کاربر پنهان است.

- **کنترل دسترسی** زیر ساخت IDA مسئول حفاظت از اطلاعات محرمانه مانند اطلاعات موجود در اسناد می‌باشد. دستیابی به اطلاعات محرمانه بر اساس سیاستهای سازمانی مدیریت می‌گردد. ACLیک سند نشان‌دهنده سیاست امنیتی آن سند می‌باشد . سیاست امنیتی

ترکیبی از مجوزهایی است که سطح دسترسی یک هویت مشخص را به آن سند تعیین می‌کند . زیر سیستم امنیت سرور در این مثال اجرای عملکرد کنترل دسترسی در زیر ساخت IDA می‌باشد.

- **ممیزی** (Audit) در صورتی که سازمان مایل باشد تغییرات و فعل و انفعالات را در زیر ساخت IDA مانیتور کند باید مکانیزم ممیزی را فعال کند.

AD DS تنها کامپوننت IDA نیست که توسط ویندوز سرور 2008 پشتیبانی می‌شود. مایکروسافت با انتشار ویندوز سرور 2008 تعدادی کامپوننت را که قبلاً مجزا ارائه شده بودند در پلتفرم IDA بصورت مجتمع ارائه داد . خود Active Directory حالا شامل پنج تکنولوژی می‌باشد که هر کدام با یک کلید واژه شناخته می‌شود که مشخص کننده هدف تکنولوژی است . در شکل ۱-۱ این موضوع نشان داده شده است .



راهنما	
وابستگی تکنولوژی‌های Active Directory	———
ارتباطات ممکن	- - - - - - - -

شکل ۱-۱ یکپارچگی پنج تکنولوژی Active Directory

- **Active Directory Domain Services(Identity)** همانطور که قبلاً شرح داده شد AD DS مرکز اصلی مدیریت هویت در یک سازمان را تشکیل می‌دهد . وظیفه AD DS فراهم کردن سرویسهای تایید هویت و ارائه مجوز در شبکه بوده و از مدیریت اشیاء (Object Management) توسط Group Policy پشتیبانی می‌نماید . علاوه بر این AD DS با فراهم کردن سرویسهای به اشتراک گذاری و مدیریت اطلاعات به کاربر توانایی جستجوی دایرکتوری و پیدا کردن اجزایی مانند فایل سرورها ، پرینترها ، گروهها و کاربران دیگررا می‌دهد . بهمین دلیل از AD DS به عنوان یک سرویس دایرکتوری سیستم عامل شبکه یاد می‌شود . AD DS تکنولوژی پایه Active Directory بوده و نصب آن در تمامی شبکه های مبتنی بر ویندوز سرور 2008 الزامی است . فصلهای ۱ تا ۱۳ این کتاب درباره AD DS بحث می‌کند.

برای اطلاعات بیشتر در مورد طراحی Active Directory مقاله "Chapter 3:Designing the Active Directory" از آدرس http://www.reso-net.com/Documents/007222343x_ch03.pdf و مسیر Windows Server 2003 ، Best Practices for Enterprise Deployments دانلود کنید

اطلاعات بیشتر طراحی AD DS

برای اطلاعات بیشتر در مورد طراحی Active Directory Domain Services به کتاب Windows Server 2008: The Complete Reference نوشته Ruest و Ruest (McGraw-Hill Osborn) مراجعه نمایید .

- AD LDS Active Directory Lightweight Directory Services (Applications) اساساً یک نسخه مستقل از Active Directory می‌باشد که قبلاً با نام Active Directory Application Mode (ADAM) شناخته می‌شد .این کامپوننت از برنامه های کاربردی Directory-enabled پشتیبانی می‌کند . AD LDS زیر مجموعه AD DS به شمار می‌آید چراکه هردو بر پایه core code یکسان طراحی شده‌اند . دایرکتوری AD LDS تنها اطلاعات مرتبط با برنامه های کاربردی را ذخیره و تکثیر می‌کند . معمولاً برنامه‌هایی که نیاز به انباره دایرکتوری دارند ولی نیاز به تکثیر گسترده اطلاعات در همه DC ها ندارند از این کامپوننت استفاده می‌کنند . AD LDS این امکان را فراهم می‌کند که یک schema دلخواه جهت پشتیبانی از یک برنامه بدون تغییر schema در AD DS توزیع شود . نقش AD LDS بسیار سبک بوده و و از انباره داده ی چندگانه روی یک سیستم واحد پشتیبانی می‌کند بهمین دلیل همه برنامه‌ها با دایرکتوری ، schema ، Lightweight Directory Access Protocol (LDAP) ، پورتهای SSLو واقعه نگاری برنامه مختص خود می‌توانند توزیع شوند . AD LDS بدلیل عدم وابستگی به AD DS در محیطهای workgroup یا مستقل قابل استفاده می‌باشد . ولی در شبکه‌های مبتنی بر دامنه،AD LDS برای تایید هویت کاربران ، گروهها و کامپیوترها می‌تواند از AD DS استفاده کند . همچنین از AD LDS می توان در سرویسهای تایید هویت شبکه‌های خصوصی مانند اینترانت بهره برد . استفاده از AD LDS در این حالت خطر کمتری نسبت به AD DS دارد . AD LDS در فصل ۱۴ بررسی می‌شود .
- Active Directory Certificate Services (Trust) سازمانها از AD CS به منظور راه‌اندازی Certificate Authority (CA) بهره می‌برند . CA کار صدور گواهینامه دیجیتال را بعنوان بخشی از یک public key infrastructure (PKI) به عهده دارد بطوریکه هویت شخص ، دستگاه یا یک سرویس به private key متناظر آن پیوند می خورد . موارد استفاده گواهینامه‌ها عبارتند از تایید هویت کاربران و کامپیوترها ، تایید هویت مبتنی بر وب ، تایید هویت با کارت هوشمند ، پشتیبانی از برنامه‌ها ، شامل شبکه های بیسیم امن ، شبکه‌های خصوصی مجازی (VPN) ، IPSec ، EFS ، امضای دیجیتال و بسیاری دیگر . AD CS روشی کارآمد و مطمئن در صدور و مدیریت گواهینامه‌هاست.سرویسهای ارائه شده در AD CS را می‌توان در محیطهای خارج از شبکه خودمان نیز استفاده کرد . در این حالت باید ارتباط AD CS را با یک CA خارجی و شناخته شده برقرار کنیم تا ثابت شود هویت ما همانی است که ادعا می‌کنیم . AD CS آمده تا اعتماد را به دنیای غیر قابل اعتماد برگرداند . به خودی خود پروسه‌های آن باید اثبات شده و محکم بوده که بتواند تضمین کند شخص یا کامپیوتری که گواهی می‌گیرد بطور تمام وکمال مورد تایید است . AD CS در شبکه‌های داخلی می‌تواند با AD DS عجین شود تا کاربران و کامپیوترها را بصورت خودکار با گواهینامه‌ها مرتبط کند . AD CS در فصل ۱۵ بررسی می‌شود .
  جهت اطلاعات بیشتر در مورد PKI و چگونگی اعمال آنها در شبکه به آدرس زیر مراجعه کرده و بخش "Advanced Public Key Infrastructures" را مطالعه کنید

  http://www.reso-net.com/articles.asp?m=8
- **Active Directory Rights Management Services (Integrity)** در حالی که سرور ویندوزی می‌تواند مجوز دسترسی یا عدم دسترسی به یک سند را بر اساس ACL سند صادر کند راههایی وجود دارد که می‌توان تغییرات سند ومحتوای آنرا پس از استفاده کاربر کنترل کرد . Active Directory Rights Management Services (AD RMS) تکنولوژی حفاظت از اطلاعات می‌باشد که به ما امکان می‌دهد الگوهای امنیتی (Security Templates) محکمی را پیاده‌سازی کنیم . این الگوها مشخص می‌کند دسترسی در وضعیت آنلاین یا آفلاین و جلوی دیوار آتش یا پشت آن چگونه باشد . بعنوان مثال شما می‌توانید الگویی را پیکربندی کنید که به کاربر اجازه خواندن سند را می‌دهد اما اجازه کپی یا پرینت آنرا نمی‌دهد. بدینوسیله صحت داده تولید شده ، حفاظت از حق مالکیت معنوی ، و کنترل سطح دسترسی افراد به اسناد سازمانی تضمین می‌گردد. پیش نیازهای AD RMS یک دامنه در Active Directory با DC های ویندوز 2000 سرور با سرویس پک ۳ به بعد ، IIS ، یک سرور پایگاه داده نظیر Microsoft SQL Server 2008 ، کلاینت AD RMS که از سایت مایکروسافت قابل دانلود است و در ویندوز ویستا و سرور 2008 موجود می‌باشد ، یک مرورگر یا برنامه RMS-enabled نظیر IE ، Microsoft Office ، Microsoft Word ، Microsoft Outlook یا Microsoft Power Point می‌باشند . AD RMS می‌تواند برای تلفیق کردن گواهینامه ها در اسناد به همان ترتیب که در AD DS وجود دارد جهت مدیریت دسترسی‌ها متکی به AD CS باشد . AD RMS در فصل ۱۶ بررسی می‌شود .
- **Active Directory Federation Services (Partnership)**AD FS سازمان را در توسعه IDA بین پلت فرمهای مختلف شامل محیطهای ویندوزی و غیر ویندوزی و همچنین ارسال هویت و حق دسترسی از پشت مرزهای امنیتی به سمت شبکه های امن یاری می‌دهد . در یک محیط با چند شبکه مجتمع هر سازمان وظیفه تامین و مدیریت اشیاء خود را داراست ولی هر سازمان می‌تواند با امنیت کامل هویتها را به سایر سازمانها ارسال یا از آنها قبول کند . کاربر می‌تواند در یک شبکه تایید هویت شود ولی به منابع شبکه‌های دیگر دسترسی داشته باشد یعنی همان پروسه‌ای که به single sign-on(SSO) معروف است .AD FS از شراکت پشتیبانی می‌کند زیرا درحالی که جهت پروسه واقعی تایید هویت به ساختار AD DS داخلی شبکه خود متکی است به سازمانهای مختلف اجازه دسترسی به

برنامه‌های خارج از شبکه خود را می‌دهد . برای این منظور AD FS از طریق پورتهای TCP/IP نظیر 80(HTTP) و 443 (Secure HTTP یا (HTTPS) ساختار AD DS داخلی را به دنیای خارج بسط می‌دهد .AD FSدر حالت عادی در شبکه perimeter قرار دارد.AD FS می‌تواند جهت ایجاد سرورهای معتبر (Trusted) به AD CS و برای تامین حفاظت از حقوق مالکیت معنوی در برابر تهدیدات خارجی به AD RMS تکیه کند .AD FS در فصل ۱۷ بررسی می‌شود .

نقشهای Active Directory با هم یک راه حل IDA یکپارچه را ارائه می‌دهد. AD DS و AD LDS سرویسهای اساسی دایرکتوری را هم در شبکه‌های مدل دامنه وهم در شبکه های مستقل فراهم می‌کنند . AD CS در قالب گواهینامه‌های دیجیتال PKI گواهی‌نامه‌های معتبر صادر می‌کند . AD RMS صحت اطلاعات اسناد را تضمین می‌کند و AD FS از شراکت پشتیبانی می‌کند و این بدین معنی است که در محیطهای چند شبکه‌ای مجتمع دیگر نیازی نیست برای یک موجودیت واحد چند هویت مجزا ساخته شود .

آنسوی Identity and Access

Active Directory چیزی بیشتر از راهکار IDA است و مکانیزمهایی دارد که از مدیریت و پیکربندی منابع در محیطهای شبکه‌ای توزیع شده پشتیبانی می‌کند .

یکسری قواعد بنام schema کلاسهای اشیاء و صفات را که در دایرکتوری وجود دارند تعریف می‌کند . بعنوان مثال اگر Active Directory حاوی شیء user دارای نام کاربری و کلمه عبور می‌باشد به این دلیل است که schema برای کلاس user دو صفت دارد و ارتباط بین کلاس شیء و صفات را تعریف می‌کند .

مدیریت مبتنی بر سیاستهای کاری ، سنگینی بار مدیریتی حتی بزرگترین و پیچیده‌ترین شبکه‌ها را از بین می‌برد . این امر با یکبار پیکربندی و توزیع آن روی چند سیستم امکانپذیر است . مباحث Group Policy ، سیاستaudit ، و سیاستهای fine-grained password در فصل ۶ و Group Policy Infrastructure در فصل ۷ و Group Policy Settings در فصل ۸ پوشش داده می‌شود

سرویسهای تکثیر (Replication) ، داده ی دایرکتوری را در شبکه توزیع می‌کند .این داده هم شامل خود انباره داده و هم داده ی مورد نیاز برای پیاده سازی سیاستها و تنظیمات از جمله اسکریپتهای ورود (Logon Script) به شبکه می باشد . مبحث "Sites and Replication" در فصلهای ۸ و ۱۱ و تکثیر Active Directory در فصل ۱۰ بررسی می‌شود . البته بخش جداگانه‌ای از انباره داده با نام configuration موجود است که اطلاعاتی راجع به پیکربندی شبکه ، توپولوژی و سرویسها را نگهداری می‌کند .

کامپوننتها و تکنولوژیهای زیادی هستند که امکان پرس و جوی Active Directory را به ما می‌دهند تا بتوانیم اشیاء را در انباره داده محل‌یابی کنیم . بخشی از انباره داده بنام Global Catalog (نام دیگر آن Partial attribute set است) اطلاعاتی درباره همه اشیاء دایرکتوری را در خود نگه می‌دارد .اینکار با استفاده از نوعی اندیس‌گذاری انجام می‌شود که جهت محل‌یابی اشیاء در دایرکتوری استفاده می‌شود. رابط‌های کاربری همانند Active Directory Services Interface (ADSI) و پروتکل‌هایی نظیر LDAP به منظور خواندن و دستکاری انباره داده قابل استفاده می‌باشد . انباره داده ی Active Directory همچنین از برنامه‌ها و سرویس‌هایی هم که بطور مستقیم با AD DS ارتباط ندارند پشتیبانی می‌کند . بخش برنامه‌های کاربردی در بانک داده برای پشتیبانی از برنامه‌هایی که نیاز به داده ی تکثیر شده دارند داده را ذخیره می‌کنند . سرویس DNS روی ویندوز سرور 2008 اطلاعات خود را می‌تواند روی بانک اطلاعاتی بنام Active Directory integrated zone ذخیره کند که در AD DS بعنوان یک بخش برنامه در نظر گرفته می‌شود و با استفاده از Active Directory replication services تکثیر می‌شود .

کامپوننت‌های زیرساخت Active Directory

۱۳ فصل اول این کتاب روی نصب ، پیکربندی و مدیریت AD DS تمرکز دارد AD DS اساس و پایه IDA و مدیریت شبکه سازمان را تشکیل می‌دهد . در اینجا کامپوننت‌های زیر ساخت Active Directory را مرور می‌کنیم .

نکته

جزئیات Active Directory را کجا پیدا کنیم

برای مطالعه بیشتر در مورد Active Directory به مطالب کمکی نصب شده همراه ویندوز سرور 2008 و TechCenter ویندوز سرور 2008 واقع در آدرس http://technet.microsoft.com/en-us/windowsserver/2008/default.aspx مراجعه نمائید

- **انباره داده ی Active Directory**

همانطوریکه در بخش‌های پیشین به آن اشاره شد AD DS هویتها را در دایرکتوری ذخیره می‌کند که انباره داده ای روی DC ها می‌باشد . دایرکتوری خود یک فایل با نام Ntds.dit بوده که بطور پیش‌فرض در پوشه %SystemRoot%\Ntds روی DC قرار دارد . بانک اطلاعاتی به چند بخش تقسیم می‌شود .این بخشها عبارتند از : Schema ، Configuration ، global catalog و domain naming context که اطلاعاتی در مورد اشیاء domain مانند کاربران ، گروهها و کامپیوترها را نگه می دارد .

- **Domain Controllers**

که به اختصار به آن DC می‌گویند سرورهایی هستند که نقش AD DS را اجرا می‌کنند .بخشی از این نقش ،سرویس Kerberos Key Distribution (KDC) می‌باشد،که وظیفه تایید هویت و دیگر سرویسها را به عهده دارد. فصل ۱۰ جزئیات نقشهای DC را تشریح می‌کند.

- **Domain یا دامنه**

برای ایجاد یک دامنه نیاز به یک یا چند DC داریم . دامنه یک حوزه مدیریتی شبکه است که قابلیتها و خصوصیات در آن یکنواخت است . ابتدا همه DC ها بخش انباره دادهدامنه خود را تکثیر می‌کنند که شامل identity data برای کاربران ، گروهها و کامپیوترهای دامنه به همره اطلاعات دیگر می‌باشد .بدلیل اینکه همه DCها identity store مشترک دارند در دامنه می‌توانند همه موجودیتها را تایید هویت کنند. به تعبیر دیگردامنه یک محدوده سیاستهای مدیریتی مانند password complexity و account lockout policies می‌باشد. چنین سیاستهایی در یک دامنه پیکربندی می‌شوند و روی حسابهای همان دامنه تاثیر می‌گذارد و روی حسابهای دامنه‌های دیگر هیچ تاثیری ندارد. تغییرات روی اشیاء بانک اطلاعاتی Active Directory توسط یک DC ایجاد می‌شود و بر رویDCهای دیگر تکثیر می‌گردد .بنابراین در شبکه‌هایی که امکان تکثیر همه داده بین DCها وجود ندارد باید بیش از یک دامنه پیاده‌سازی گردد . مطالب بیشتر درباره دامنه در فصل ۱۲ ارائه می‌شود.

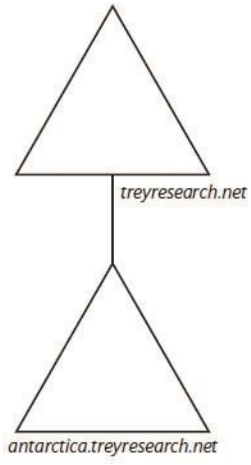
- **Forest**

به مجموعه یک یا چنددامنه در Active Directory یک forest گویند.اولین دامنه نصب شده در یک forest را forest root domain گویند . forest یک تعریف واحد از پیکربندی شبکه و یک instance واحد از directory schema ارائه می دهد. یک forest یک instance از دایرکتوری می‌باشد بطوریکه هیچ داده ای توسط Active Directory به خارج از مرزهای forest تکثیر نمی‌گردد. بنابراین forest مرزهای امنیتی را تعریف می‌کند . فصل ۱۲ مفهوم forest را دقیقاً تشریح می‌کند.

- **Tree**

فضای نام DNS دامنه‌ها در یک tree،forestها می‌سازد. اگر یک دامنه زیر دامنه دامنه دیگر باشد دو دامنه یک درخت را تشکیل می‌دهند. بعنوان مثال فرض کنیم forest ،treyresearch.net دارای دو دامنه است treyresearch.net و antarctica.treyresearch.net و چون این دامنه‌ها بخشهای متمادی از فضای اسمی DNS (namespace) را تشکیل می‌دهند می‌توان آنها را یک درخت تصور کرد. بالعکس دامنه‌های treyresearch.net و proseware.com که در یک فضای نام DNS نیستند در دو درخت متفاوت قرار دارند.درختها بر اساس اسامی DNS انتخاب شده برای دامنه‌ها در forest ایجاد می‌شوند .

شکل ۱-۲ یک Active Directory forest مربوط به موسسه تحقیقاتی Trey Research را نشان می‌دهد که در منطقه Antarctica (قطب جنوب) دارای شعبه می‌باشد . چون ارتباط بین مرکز و منطقه مذکور بسیار کند ، پرهزینه و غیرقابل‌اطمینان است منطقه Antarctica خود دارای یک دامنه مجزا می‌باشد . نام DNS مربوط به forest ، Treyresearch.net است . دامنه Antarctica در فضای اسمی Antarctica.treyresearch.net ، دامنه فرزند بوده بنابراین در درخت دامنه یک فرزند به حساب می‌آید .



شکل ۱-۲ یک forest با دو دامنه در Active Directory

- **Functional level**

که از این پس سطح عملیاتی خوانده می‌شود قابلیتهای عملیاتی را در یک Active Directory یا forest معین می‌کند . سطح عملیاتی یکی از تنظیمات AD DS بوده که ویژگی‌های پیشرفته AD DS را در سطح دامنه یا forest فعال می‌کند . سه سطح عملیاتی برای دامنه موجود است : Windows 2000 native ، Windows Server 2003 و Windows Server 2008 و دو سطح عملیاتی برای forest موجود می باشد : Microsoft Windows Server 2003 و Windows Server 2008 . هنگامی که سطح عملیاتی دامنه یا forest را ارتقا می دهیم ،

ویژگیهای ارائه شده توسط همان نسخه ویندوز برای AD DS قابل دسترس می‌شود .بعنوان مثال وقتی سطح عملیاتی دامنه به Windows Server 2008 ارتقا پیدا می‌کند یک صفت جدید اضافه می‌شود که مشخص می‌کند آخرین باری که کاربر بطور موفقیت‌آمیز به یک کامپیوتر وارد شده چه زمانی بوده یا کامپیوتری که آخرین بار کاربر با آن وارد شده است کدام بوده ویا تعداد دفعات خطای ورود از آخرین ورود موفقیت آمیز به بعد چقدر بوده است . نکته مهم اینست که سطح عملیاتی، نسخه‌های ویندوز مجاز برای نصب روی DC ها را مشخص می‌کند . قبل از اینکه سطح عملیاتی دامنه را به Windows Server 2008 ارتقا دهیم باید مطمئن شویم نسخه سیستم عامل همه DC ها Windows Server 2008 می‌باشد . فصل ۱۲ سطح عملیاتی دامنه و forest را تشریح می‌کند .

- **Organizational Unit**

Active Directory یک بانک اطلاعاتی سلسله مراتبی است . اشیاء انباره داده در container ها نگهداری می‌شوند .یک نوع container، کلاس شیء با نام *container* است . زمانی که ابزار (snap-in) ، Active Directory Users and Computers را باز می‌کنیم containerهای پیش‌فرض را مانند Users ، Computers و Builtin می‌توانیم ببینیم . نوع دیگر container ، OU می‌باشد. OUها نه تنها مزایای یک container را در جای دادن اشیاء دارند بلکه محدوده‌ای را جهت مدیریت اشیاء فراهم می‌کنند . این بدین خاطر است که OUها اشیائی دارند بنام Group policy objects (GPOs) که به آنها اعمال می‌شود . GPO ها مجموعه تنظیمات پیکربندی هستند که به کاربران و کامپیوترها در OUها اعمال می‌شوند . در فصل ۲ "Administration" با OUها و در فصل ۶ با GPO بیشتر آشنا می‌شوید .

- **Sites**

وقتی صحبت از توپولوژی شبکه سازمانی توزیع شده به میان می آید ناچاریم از سایت استفاده کنیم . سایت در Active Directory معنی خیلی خاصی دارد چراکه یک کلاس شیء با نام site موجود است . سایت شیئی است که تشکیل‌دهنده یک بخش شبکه با پهنای باند بالا می باشد . سایت مرزهای تکثیر و استفاده از سرویسها را مشخص می کند . DCهای یک سایت در عرض چند ثانیه تغییرات را تکثیر می‌کنند . تکثیر تغییرات بین سایتها با فرض بر اینکه ارتباط بین سایتها به نسبت ارتباطات داخل سایت کند ، گران یا غیرقابل‌اطمینان است بر اساس یک سیستم کنترل‌شده انجام می‌شود . بعلاوه کلاینتها ترجیح می‌دهند از سرویس سرورهای سایت خودشان یا نزدیکترین سایت استفاده کنند . بعنوان مثال زمانی که کاربری می‌خواهد به شبکه وارد شود ویندوز کلاینت سعی می‌کند برای تایید هویت با یک DC در داخل سایت خودش ارتباط برقرار کند . فقط زمانی که در سایت هیچ DC در دسترس نباشد کلاینت به DC های سایتهای دیگر مراجعه می‌کند . فصل ۱۱ پیکربندی و عملکرد سایتها را تشریح می‌کند .

هر کدام از کامپوننتهای اشاره شده در بالا به تفصیل بررسی خواهد شد . در این مقطع اگر شناخت خوبی از Active Directory ندارید کافی است یک درک ابتدایی از واژه‌شناسی ، اجزاء و ارتباطات کامپوننتها بدست آورید .

آماده سازی شرایط برای ساخت یک forest جدید در ویندوز سرور 2008

قبل از اینکه نقش AD DS را روی یک سرور نصب کنید زیرساخت Active Directory را طراحی کنید . بخشی از اطلاعات مورد نیاز برای ایجاد DC عبارتنداز:

- نام دامنه و نام DNS . دامنه باید دارای نام DNS منحصربفرد باشد مثلاً contoso.com ، همچنین نام اختصاری داشته باشد مانند contoso که به آن نام NetBIOS هم می‌گویند .NetBIOS یکی از پروتکل‌های شبکه می‌باشد که از اولین نسخه‌های ویندوز NT تاکنون استفاده شده است و هنوز هم توسط بعضی برنامه‌ها بکار برده می‌شود .
- آیا دامنه جدید قرار است از DC های دارای نسخه‌های قدیمی تر پشتیبانی کند یا خیر . وقتی forest جدیدی می‌سازیم باید سطح عملیاتی آنرا نیز پیکربندی کنیم . اگر دامنه فقط قرار است دارای DCهای ویندوز سرور 2008 باشد چه بهتر است سطح عملیاتی Windows Server 2008 را انتخاب کنیم تا از مزایای ویژگیهای پیشرفته آن بهره‌مند شویم .
- جزئیات در مورد پیاده‌سازی DNS برای پشتیبانی از Active Directory . بهترین حالت اینست که سرویس DNSویندوزی را برای دامنه خود پیاده سازی کنیم . درحالی که طبق توضیحات فصل ۹ "Integrating Domain Name System with AD DS" امکان استفاده از سرویس DNS نرم‌افزارهای غیرمایکروسافتی در دامنه ویندوزی وجود دارد.
- پیکربندی IP برای DC . IP در DC ها می‌بایست دستی(static) تنظیم شود. بعلاوه برای تحلیل نام باید آدرس سرور DNS در پیکربندی IP سیستم عامل DC درج شود .در صورتی که forest جدیدی ایجاد می‌کنید و تصمیم دارید سرویس DNS ویندوزی روی DC نصب کنید آدرس DNS را همان آدرس DC بگذارید .پس از نصب DNS ، سرور برای تحلیل نام به خودش مراجعه می‌کند .
- نام‌کاربری و کلمه عبور مربوط به یک حساب (Account) در گروه Administrators سرور .حساب باید حتماً دارای کلمه عبور باشد
- محل نصب انباره داده شامل(Ntds.dit) و system volume(SYSVOL) . بطور پیش‌فرض این فضاها در %SystemRoot% بطور مثال C:\Windows به ترتیب در پوشه‌های NTDS و SYSVOL ایجاد می شوند . هنگام ایجاد DC می‌توان این مسیرها را به درایوهای دیگر تغییر داد .

اطلاعات بیشتر **توزیع AD DS**

لیست حاضر از تنظیماتی تشکیل می‌شود که هنگام نصب DC پیکربندی شده‌اند. همچنین نکات دیگری در مورد تنظیمات شبکه در رابطه با توزیع AD DS اهمیت دارد. از آدرس http://technet2.microsoft.com/windowsserver2008/en/library/bab0f1a1-54aa-4cef-9164-139e8bcc44751033.mspx بخش Windows Server 2008 Technical Library را ببینید.

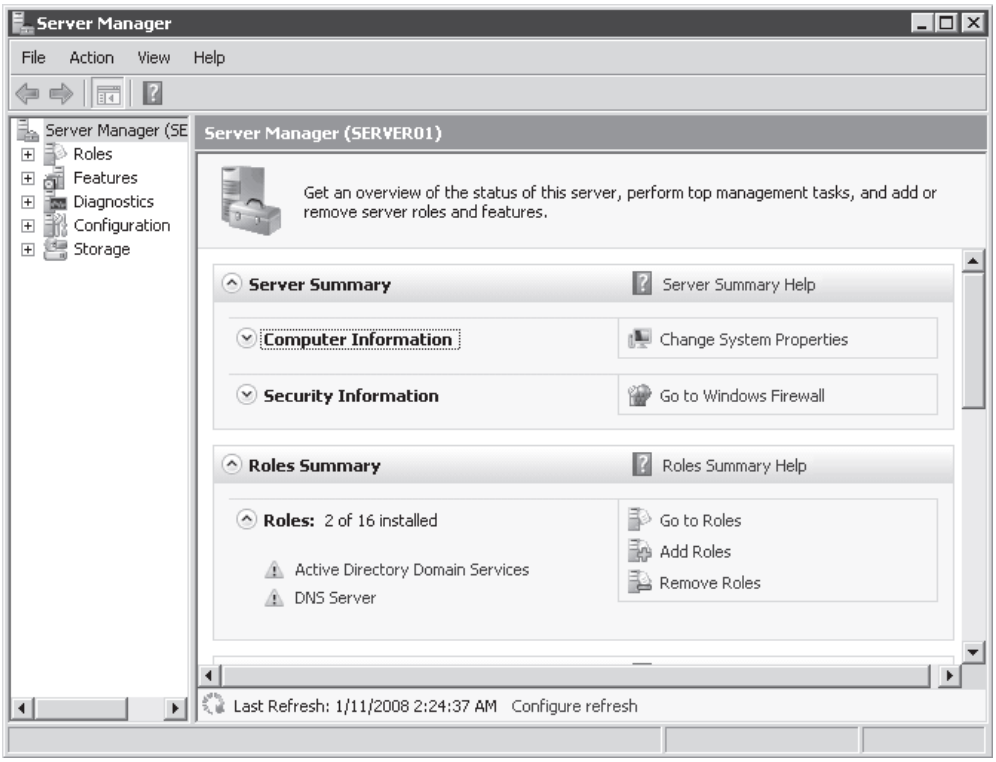
افزودن نقش AD DS با استفاده از رابط کاربری ویندوز

پس از جمع‌آوری اطلاعات پیش‌نیاز که قبلاً اشاره شد زمان افزودن نقش AD DS می‌رسد . راههای متعددی برای اینکار موجود است . در این درس یاد می‌گیریم این کار را از طریق رابط کاربری ویندوز انجام دهیم . در درس بعد روش اجرا از طریق خط فرمان را مرور می‌کنیم .

ویندوز سرور 2008 امکان پیکربندی سرور را بر اساس نقشها فراهم می‌کند بطوریکه فقط کامپوننتها و سرویسهای مورد نیاز برای نقشهایی را که سرور قرار است بازی کند نصب می‌کند . این شیوه مدیریت سرور مبتنی بر نقش‌های آن در کنسول مدیریتی جدید ویندوز بنام Server Manager مشهود است .شکل ۱-۳ تصویری از این کنسول را نشان می‌دهد . Server Manager اطلاعات ، ابزارها و منابع مورد نیاز برای پشتیبانی از نقشهای سروری را یکجا ارائه می‌دهد .

توسط پیوند Add Role (Link) در صفحه اصلی Server Manager می‌توان نقشی را به سرور اضافه کرد . راه دیگر آن راست کلیک روی گره Roles در ساختار درختی کنسول و انتخاب Add Roles می باشد .

ویزاردAdd Rolesلیستی از نقشهای قابل نصب را نمایش می‌دهد و مرحله به مرحله نصب نقش انتخابی را پیش می‌برد .



شکل ۱- ۳ پنجره Server Manager

ایجاد یک DC

پس از افزودن نقش AD DS فایلهای مورد نیاز برای اجرای نقش روی سرور نصب می‌گردد ولی همچنان سرور نمی‌تواند بعنوان یک DC عمل نماید . برای پیکربندی و راه‌اندازی Active Directory باید با فرمان Dcpromo.exe ویزارد Active Directory Domain Services Installation را اجرا کنیم .

تمرینات ایجادیک forest ویندوز سرور 2008

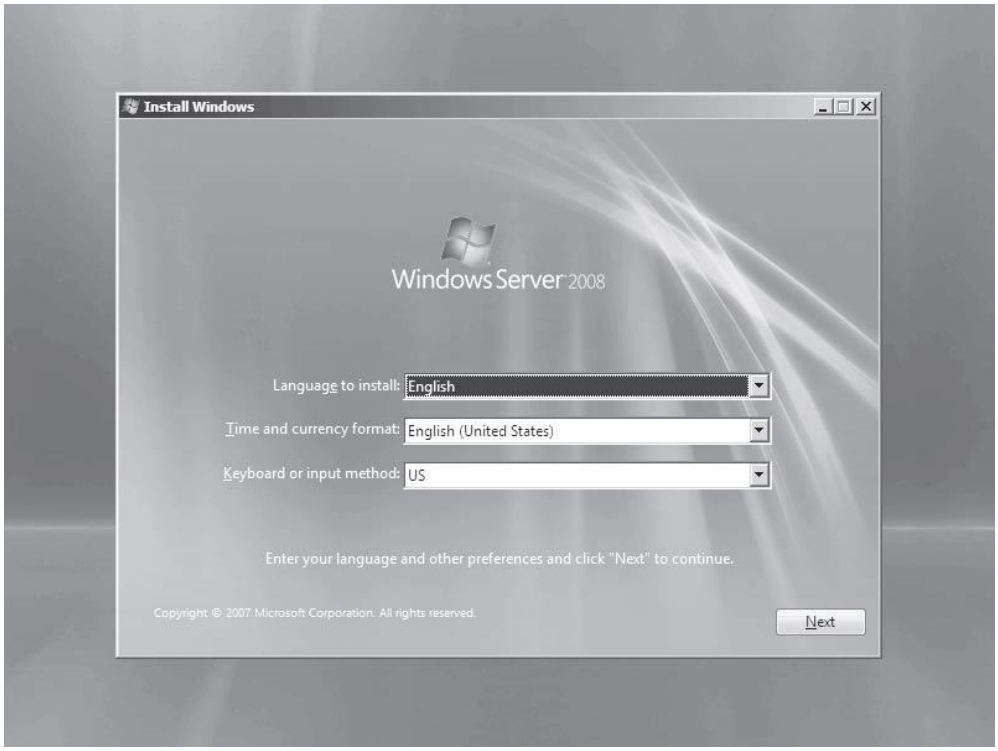
در این تمرینات یک AD DS forest جهت شرکت contoso ساخته می‌شود .این forest در تمامی تمرینهای کتاب استفاده خواهد شد . شروع تمرینات با نصب ویندوز سرور 2008 و اجرای پیکربندی پس از نصب خواهد بود .سپس نقش AD DS به سرور افزوده می‌شود و سرور با استفاده از ویزارد نصب Active Directory Domain Services به یک DC در forest مربوط به شرکت contoso.com ارتقاء می‌یابد .

تمرین ۱ : نصب ویندوز سرور 2008

در این تمرین قرار است ویندوز سرور 2008 روی کامپیوتر یا ماشین مجازی نصب شود .

۱. DVD نصب ویندوز سرور 2008 را درون درایو قرار می‌دهیم .اگر از ماشین مجازی استفاده می‌کنیم باید بدنبال گزینه‌ای برای سوار کردن فایل ISO که از روی DVD نصب تهیه شده بگردیم . برای اطلاعات بیشتر به مستندات نرم‌افزار ماشین مجازی رجوع شود .
۲. کامپیوتر را روشن می‌کنیم .

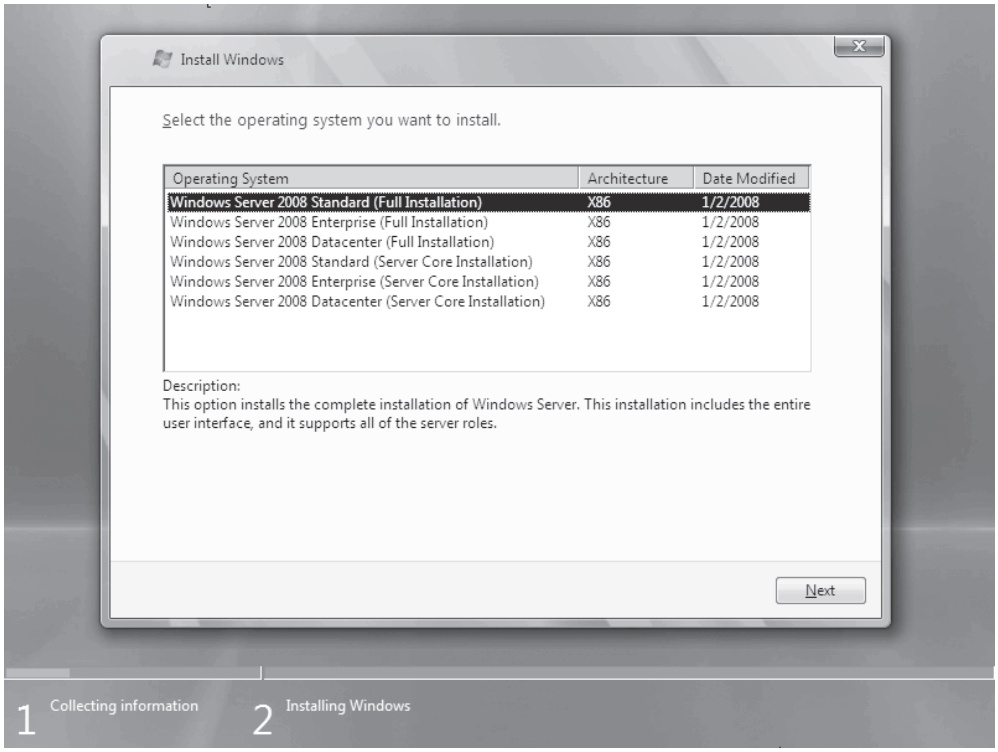
اگر هارد کامپیوتر خالی است سیستم از روی DVD راه اندازی می‌شود وگرنه پیغامی مبنی بر فشردن یک کلید برای راه‌اندازی سیستم از روی DVD دریافت می‌کنیم .اگر سیستم از روی DVD راه‌اندازی نشد یا منوی بوت ظاهر شد به تنظیمات BIOS سیستم رفته و ترتیب سخت‌افزارها طوری تعیین می‌کنیم که سیستم از روی DVD بوت شود . همانطور که در شکل ۱- ۴ نمایش داده شده است ویزارد نصب



ویندوز نمایان می‌شود .

شکل ۴- ۱ ویزارد نصب ویندوز

۳. گزینه‌های language ,regional setting و keyboard layout متناسب با شرایط خود انتخاب کرده و گزینه Next را کلیک می‌کنیم .
۴. کلید Install Now را می‌زنیم . همانند شکل ۱- ۵ لیستی از نسخه‌های مختلف نشان داده می‌شود . اگر سیستم ما ۶۴ بیتی باشد بجای نسخه‌های ۳۲ بیتی (x86) نسخه‌های ۶۴ بیتی (x64) نمایش داده می شود .



شکل ۵- ۱ صفحه Select The Operationg System You Want To Install

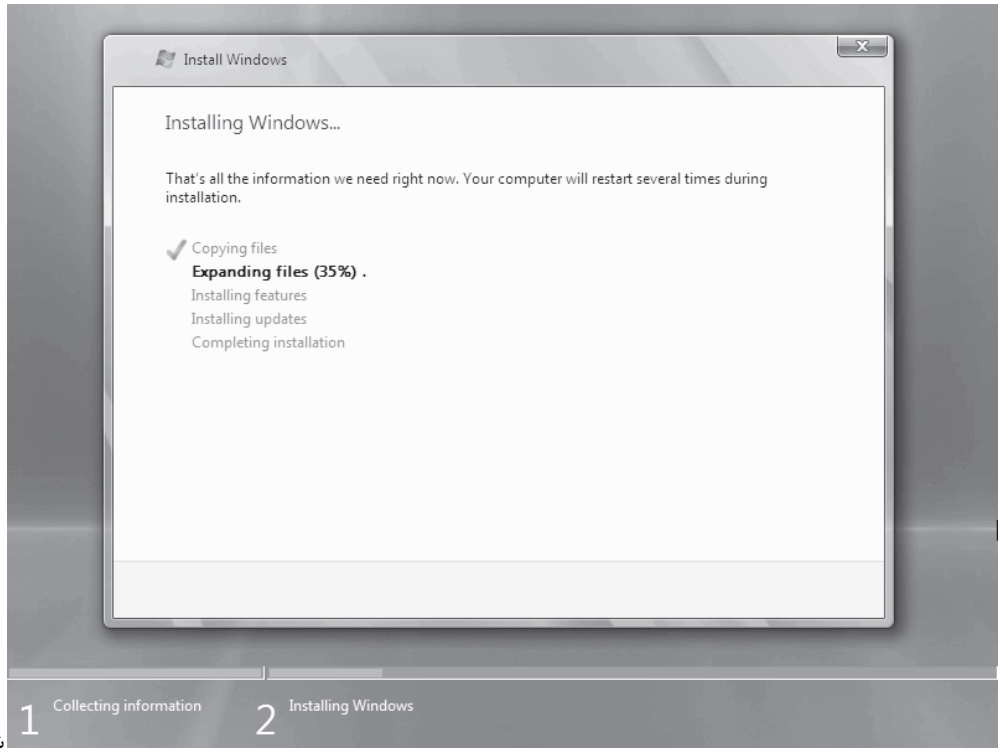
۵. گزینه Windows Server 2008 Standard (Full Installation) را انتخاب کرده و گزینه Next را کلیک می‌کنیم .

۶. کادر I Accept The License Terms را علامت زده و گزینه Next را کلیک می‌کنیم .

۷. گزینه Custom (Advanced) را کلیک می‌کنیم .

۸. در صفحه Where Do You Want To Install Windows دیسکی که می‌خواهیم روی آن ویندوز سرور 2008 را نصب کنیم انتخاب می‌کنیم .اگر نیاز به ساخت ،حذف ،توسعه (extend) یا فرمت پارتیشن‌ها و یا بارگذاری درایور یک دیسک داشته باشیم روی Driver Options (Advanced) کلیک می‌کنیم .

۹. کلید Next را می‌زنیم . مانند شکل ۱- ۶ کادر محاوره‌ای Installing Windows نمایان می‌شود . میزان پیشرفت مراحل نصب در صفحه نمایش داده می‌شود .نصب ویندوز سرور 2008 مانند ویستا مبتنی بر image است .بنابراین هرچند این نسخه از نسخه‌های قدیمی‌تر حجم بیشتری دارند ولی نصب آنها سریعتر است .



شکل ۶- ۱

صفحه ویندوز در حال نصب

کامپیوتر در طول نصب یکبار یا بیشتر راه‌اندازی مجدد می‌گردد .وقتی عملیات نصب کامل شد ویندوز از ما می‌خواهد کلمه عبور را قبل از اولین ورود به سیستم تغییر دهیم .

۱۰. گزینه OK را کلیک می‌کنیم .

۱۱. کلمه عبوری را برای کاربر Administrator هم در کادر New Password و هم در Confirm Password تایپ کرده و Enter را می زنیم .

طول کلمه عبور باید حداقل ۷ کاراکتر بوده و سه نوع از چهار نوع کاراکترهای زیر را داشته باشد :

- حروف بزرگ از A تا Z
- حروف کوچک از a تا z
- عدد از 0 تا 9
- علائم مانند $ ،#، @ و !

نکته کلمه عبور را فراموش نکنید

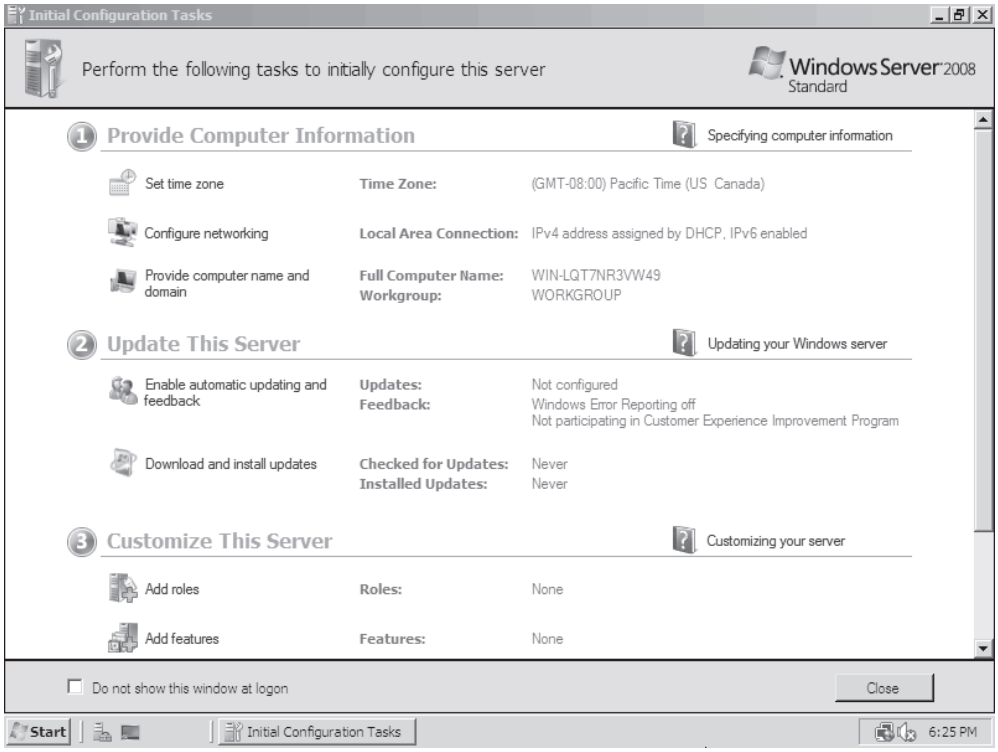
بدون کلمه عبور نمی‌توانیم وارد سرور شویم و تمرینات دیگر را انجام دهیم .

۱۲. گزینه OK را کلیک می‌کنیم .دسک‌تاپ کاربر Administrator ظاهر می‌شود .

تمرین ۲ پیکربندی پس از نصب

در این تمرین پس از نصب سرور ،پیکربندی نام و تنظیمات TCP/IP برای استفاده در تمرینات بعدی اجرا می‌گردد .

۱. منتظر می‌مانیم تا دسک‌تاپ کاربر Administrator ظاهر شود . بطوریکه در تصویر ۱- ۷ مشاهده می‌کنید پنجره Initial Configuration Tasks پدیدار می‌شود .این ابزار طراحی شده تا ما بتوانیم براحتی عملیات پیکربندی را انجام دهیم .



شکل ۷- ۱ پنجره Initial Configuration Tasks

۲. در ابتدا از این پنجره برای پیکربندی موارد زیر استفاده می‌کنیم :

- Time Zone : مناسب منطقه جغرافیایی خودمان
- Computer Name : SERVER01 . قبل از نمایان شدن پیغام راه‌اندازی مجدد آن را راه‌اندازی نمی‌کنیم .

۳. روی پیوند Configure Networking در پنجره کلیک می‌کنیم و تنظیمات IP سرور را متناسب با شبکه خود انجام می‌دهیم .

۴. اگر سرور به اینترنت متصل باشد اکیداً توصیه می‌شود پیوند Download And Install Updates را کلیک کنیم تا سرور آخرین آپدیت‌های امنیتی را از سایت مایکروسافت دانلود کند .

۵. پس از بروزرسانی ، سرور را راه‌اندازی مجدد می‌کنیم .

بقیه تمرینات کتاب دامنه‌ای را شامل می‌شود که محدوده آدرس آن از آدرس 10.0.0.11 تا آدرس 10.0.0.20 می‌باشد و subnet mask آن 255.255.255.0 است . اگر این آدرسها در شبکه جاری ما وجود دارند و سرور نیز به شبکه متصل است باید این آدرس‌ها را طوری تغییر دهیم تا دامنه contoso.com که در این تمرین ساخته می‌شود با شبکه جاری ما تداخلی نداشته باشد .

۶. در پنجره روی پیوند Configure Networking کلیک می‌کنیم. کادر محاوره‌ای Network Connections ظاهر می‌گردد .

۷. Local Area Connection را انتخاب می‌کنیم .

۸. روی نوار ابزار کلید Change Settings Of This Connection را کلیک می‌کنیم .

۹. Internet Protocol version 4 (TCP/IPv4) را انتخاب و Properties را کلیک می‌کنیم . ویندوز سرور 2008 از TCP/IPv6 نیز پشتیبانی می‌کند .

۱۰. Use The Following IP Address را کلیک می‌کنیم .تنظیمات زیر را انجام می‌دهیم :

- IP Address : 10.0.0.11
- Subnet Mask : 255.255.255.0
- Default Gateway : 10.0.0.1
- Preferred Dns Server : 10.0.0.11

۱۱. OK و بعد Close را کلیک کنید .

۱۲. به پیوندهای Add Roles و Add Features در پنجره توجه کنید .در تمرین بعدی از Server manager برای افزودن برخی نقش‌ها و ویژگی‌ها به SERVER01 استفاده خواهیم کرد .این پیوندها روش دیگر اجرای همین عملیات است .
هر بار پس از ورود به سرور ، پنجره Initial Configuration Tasks نمایش داده می‌شود

۱۳. برای ممانعت از نمایش دوباره پنجره کادر Do Not Show This Window At Logon را علامت می‌زنیم .در صورت نیاز می‌توان این پنجره را با اجرای فرمان oobe.exe باز کرد .

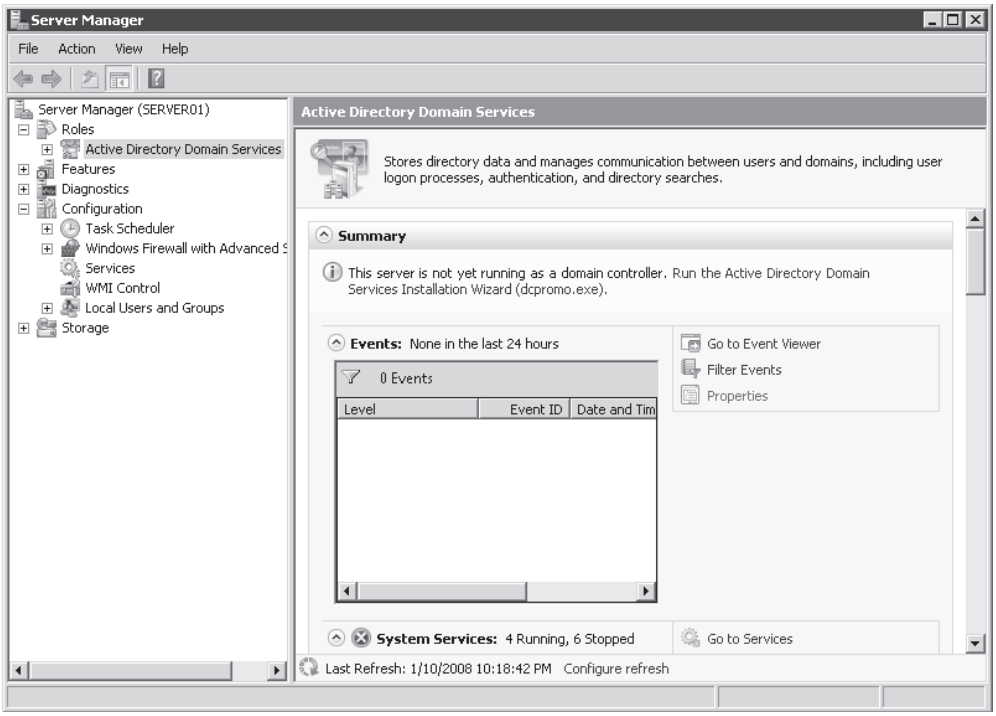
۱۴. دکمه Close را در انتهای پنجره کلیک می‌کنیم .
صفحه Server Manager باز می‌شود. در این صفحه می‌توانیم نقشها و ویژگی‌های سرور 2008 را پیکربندی کنیم. از این پنجره در تمرین بعدی استفاده می‌شود.

نکته از ماشین مجازی یک snapshot تهیه کنید.
اگر برای این تمرین از ماشین مجازی استفاده می‌کنید و نرم‌افزار امکان تهیه snapshot را از وضعیت کنونی می‌دهد در این مرحله این‌کار را انجام دهید. ویندوز سرور 2008 بشکل فعلی در تمرینهای بعدی همین فصل برای آزمایش روشهای مختلف افزودن نقش AD DS کاربرد دارد.

تمرین ۳ نصب یک forest ویندوز سرور 2008 با استفاده از رابط کاربری ویندوز

در این تمرین قرار است نقش AD DS به سرور نصب شده در تمرین ۱ و پیکربندی شده در تمرین ۲ افزوده شود.

۱. اگر پنجره Server Manager باز نیست، از طریق Administrative Tools آن را باز می‌کنیم.
۲. در بخش Roles Summary در صفحه اصلی دکمه Add Roles را کلیک می‌کنیم. ویزارد Add Roles ظاهر می‌شود.
۳. روی Next کلیک می‌کنیم.
۴. در صفحه Select Server Roles کادر Active Directory Domain Services را علامت زده و Next را می‌زنیم.
۵. در صفحه Active Directory Domain Services کلید Next را می‌زنیم.
۶. در صفحه Confirm Installation Selection کلید Install را می زنیم.
صفحه Installation Progress وضعیت نصب را گزارش می‌دهد.
۷. در صفحه Installation Page اتمام مراحل نصب را تایید می‌کنیم و روی Close کلیک می‌کنیم. در بخش Roles Summary در صفحه اصلی Server Manager پیغام خطایی بصورت دایره قرمز با علامت "x" داخل آن توجه ما را جلب خواهد کرد. همچنین پیغام دیگری در بخش Active Directory Domain Services خودنمایی خواهد کرد. هر دوی این خطاها که بصورت پیوند است ما را به صفحه نقش Active Directory Domain Services در Server Manager می‌برد ه در شکل ۱- ۸ نشان داده شده است. پیغام یادآوری می‌کند که اجرای Dcpromo.exe ضروری است که در تمرین بعدی اجرا خواهد شد.



شکل ۸- ۱ صفحه نقش‌های Active Directory Domain Services در کنسول Server Manager

تمرین ۴ نصب forest در ویندوز سرور 2008

در این تمرین از ویزارد Active Directory Domain Services Installation (Dcpromo.exe) برای ساخت forest ویندوز سرور 2008 استفاده می‌گردد.

۱. روی منوی استارت بعد Run کلیک کرده و فرمان Dcpromo.exe را تایپ می‌کنیم و سپس کلید OK را می‌زنیم
نکته فرمان dcpromo در صورت نیاز نقش AD DS را اضافه می‌کند
در تمرین قبل نقش AD DS را توسط Server Manager اضافه کردیم. بهرحال وقتی فرمان Dcpromo.exe را روی سروری که نقش AD DS را ندارد اجرا می‌کنیم بطور خودکار نقش اضافه خواهد شد.
ویزارد Active Directory Domain Services ظاهر می‌شود. در فصل ۱۰ درباره حالت پیشرفته ویزارد یاد می‌گیریم.

۲. روی Next کلیک می‌کنیم.

۳. در صفحه Operating System Compatibility هشدار مربوط به تنظیمات امنیتی پیش فرض DC های ویندوز سرور 2008 را مرور کرده و کلید Next را می‌زنیم.

۴. در صفحه Choose a Deployment Configuration گزینه Create A New Domain In A New Forest را انتخاب کرده و Next را می‌زنیم.

۵. در صفحه Name The Forest Root Domain تایپ می‌کنیم contoso.com و Next را کلیک می‌کنیم. سیستم بررسی می‌کند تا مطمئن شود نامهای DNS و NetBIOS در شبکه موجود نباشد.

۶. در صفحه Set Forest Functional Level ویندوز سرور 2008 را انتخاب کرده و کلید Next را می‌زنیم.
سطوح عملیاتی در کادر Details توصیف شده‌اند. انتخاب سطح عملیاتی forest به حالت ویندوز سرور 2008 تضمین می‌کند همه دامنه‌های forest در سطح عملیاتی ویندوز سرور 2008 قرار دارند و این یعنی استفاده از ویژگی‌های جدید بسیار در ویندوز سرور 2008 .در فصل ۱۲ سطوح عملیاتی شرح داده می‌شود.
صفحه Additional Domain Controller Options ظاهر می شود. DNS Server بطور پیش فرض انتخاب شده است. ویزارد Active Directory Domain Services Installation زیر ساخت DNS را طی نصب AD DS ایجاد می‌کند. اولین DC در forest باید global catalog(GC) باشد و نمی‌تواند DC فقط خواندنی (RODC) باشد.

۷. روی Next کلیک می‌کنیم.
پیغام هشداری مبنی بر دستی بودن آدرس IP ظاهر می شود. بدلیل اینکه بحث در مورد IPv6 خارج از محدوده کتاب است از آدرس IPv6 در تمرین ۲ استفاده نشد و آدرس IPv4 بصورت دستی تعیین گردید و در تمرینهای بعد نیز IPv4 استفاده خواهد شد. بنابراین از این هشدار چشم پوشی می‌کنیم.

۸. روی Yes کلیک می‌کنیم. سیستم از آدرس IP اتوماتیک استفاده خواهد کرد (پیشنهاد نمی‌شود)
هشداری مبنی بر عدم امکان تفویض اختیار سرور DNS ظاهر می‌شود. از این پیغام هم گذر می‌کنیم. تفویض اختیار دامنه‌هایDNS در فصل ۹ بحث می‌شود.

۹. روی Yes کلیک کرده تا پیغام هشدار بسته شود.

۱۰. در صفحات Location For Database، Log Files و SYSVOL مسیرهای پیش فرض را قبول می‌کنیم و کلید Next را می‌زنیم.
بهترین روش ذخیره این فایلها در سه درایو مجزاست که هیچ برنامه یا فایلی بدون ارتباط با AD DS روی آن موجود نباشد. این روش طراحی، کارایی را ارتقاء می‌دهد و باعث افزایش اثر بخشی در تهیه نسخه پشتیبان و بازیابی می‌گردد.

۱۱. در صفحه Directory Services Restore Mode Administrator Password کلمه عبوری پیچیده هم در کادر Password و هم در کادر Confirmed Password وارد می‌کنیم. کلید Next را می‌زنیم. این کلمه عبور را فراموش نکنید.

۱۲. در صفحه خلاصه تنظیمات انتخاب‌های خود را مرور می‌کنیم.
اگر تنظیمی اشتباه باشد با کلید Back می‌توان به عقب برگشت و آن را اصلاح کرد.

۱۳. روی Next کلیک کنید.
پیکربندی AD DS شروع می‌شود. پس از اتمام مراحل نصب سرور باید راه‌اندازی مجدد گردد. کادر Reboot On Completion را علامت می‌زنیم.

خلاصه درس

- سرویس‌های Active Directory راه حلی یکپارچه برای identity and access در شبکه‌های سازمانی ارائه می‌دهد.
- AD DS سرویس دایرکتوری و کامپوننت‌های تایید هویت IDA را فراهم می‌کند. بعلاوه AD DS مدیریت شبکه‌های بزرگ، پیچیده و توزیع شده را آسان می کند.

- سیستم‌های ویندوز سرور 2008 بر اساس نقش‌های خود پیکربندی می شوند. نقش AD DS با استفاده از Server Manager افزوده می‌شود.
- از Dcpromo.exe برای پیکربندی AD DS و ساخت DC استفاده می‌شود.

سئوالات پایان درس

از سئوالات زیر برای ارزیابی دانش خود در درس ۱ می‌توانید استفاده کنید. سئوالات همچنین از روی CD همراه کتاب بشکل الکترونیک قابل دستیابی است.

نکته جواب‌ها

جواب‌های این سئوالات در بخش "جواب‌ها" در آخر کتاب موجود است.

۱. کدامیک از موارد زیر برای ایجاد بدون اشکال DC ضروری است؟ (بیش از یک جواب دارد)
   A. نام DNS دامنه معتبر
   B. نام NetBIOS معتبر
   C. سرور DHCP برای اختصاص آدرس IP به DC
   D. سرور DNS

۲. شرکت Trey Research شرکت Litware را تصاحب می‌کند. بعلت مشکلات تکثیر تصمیم گرفته می‌شود یک دامنه فرزند در forest برای کاربران و کامپیوترهای Litware در نظر گرفته شود. Forest مربوط به Trey Research دارای DC های ویندوز سرور 2008 است. دامنه جدید روی DC ویندوز سرور 2008 ایجاد خواهد شد ولی ویندوزهای سرور 2003 که نقش DC را در دامنه Litware دارند باید حفظ شود. کدام سطح عملیاتی مناسب این وضعیت است؟
   A. سطح عملیاتی forest ویندوز سرور 2008 و سطح عملیاتی دامنه ویندوز سرور 2008 برای دامنه Litware
   B. سطح عملیاتی forest ویندوز سرور 2008 و سطح عملیاتی دامنه ویندوز سرور 2003 برای دامنه Litware
   C. سطح عملیاتی forest ویندوز سرور 2003 و سطح عملیاتی دامنه ویندوز سرور 2008 برای دامنه Litware
   D. سطح عملیاتی forest ویندوز سرور 2003 و سطح عملیاتی دامنه ویندوز سرور 2003 برای دامنه Litware

درس ۲ : Active Directory Domain Services روی Server Core

سازمانهای بسیاری مایلند بالاترین حد امنیت ممکن را در مورد سرورهای DC پیاده کنند چراکه حساسیت اطلاعات ذخیره‌شده مخصوصاً کلمات عبور کاربران بالاست . هرچند در ویندوز سرور 2008 پیکربندی مبتنی بر نقشهای سروری- که فقط سرویسها و کامپوننتهای مورد نیاز برای ایفای نقش مورد نظر نصب می‌گردد- سطح قابل نفوذ سرور را کاهش می‌دهد با نصب Server Core می‌توان این سطح را باز هم کاهش دهیم . نصب Server Core یک نصب حداقلی از ویندوز سرور است که حتی رابط گرافیکی Windows Explorer و Microsoft .NET Framework را حذف می‌کند . امکان مدیریت Server Core توسط ابزارهای رابط گرافیکی از راه دور وجود دارد . ولی برای پیکربندی و مدیریت یک سرور بصورت محلی (Local) مجبور هستیم از ابزارهای خط فرمان استفاده کنیم . در این درس چگونگی ایجاد یک DC از راه خط فرمان روی یک Server Core نصب شده را یاد می‌گیریم . همچنین یاد می‌گیریم که چطور یک DC را از دامنه حذف کنیم .

بعد از این درس باید بتوانید :

عملکرد و مزایای نصب Server Core را تشریح کنید.

Server Core را نصب و پیکربندی کنید.

AD DS را توسط ابزارهای خط فرمان افزوده و یا حذف کنید.

زمان تقریبی : ۶۰ دقیقه

درک Server Core

ویندوز سرور 2008 (نسخه Server Core) یک نصب حداقلی از ویندوز است که حدود ۳ گیگابایت از فضای دیسک و کمتر از ۲۵۶ مگابایت از فضای حافظه را اشغال می‌کند . نصب Server Core نقشها و ویژگیهای سرور را که می‌تواند اضافه شود محدود می‌کند ولی امنیت و قابلیت مدیریتی سرور را بواسطه کاهش سطح قابل نفوذ ، افزایش می‌دهد . تعداد سرویسها و کامپوننتهای اجرا شده روی سرور در لحظه خیلی کم بوده ،

بنابراین برای یک نفوذگر شانس اکتشاف در سرور کمتر است . Server Core همچنین بار مدیریتی کمتری را به همراه دارد که باعث کاهش نیاز به بروزرسانی و عملیات نگهداری می شود .

Server Core از ۹ نقش سروری پشتیبانی می‌کند .

- Active Directory Domain Services
- Active Directory Lightweight Directory Services (AD LDS)
- سرور Dynamic Host Configuration Protocole (DHCP)
- سرور DNS
- سرویسهای مربوط به فایلها
- پرینت سرور
- سرویسهای Streaming Media
- سرور وب (IIS) ایستا . سرویس پویا (Dynamic) وب مانند ASP.NET نصب نمی‌شود
- Hyper-V (Windows Server Virtualization)

همچنین ۱۱ ویژگی انتخابی دیگر را پشتیبانی می‌کند :

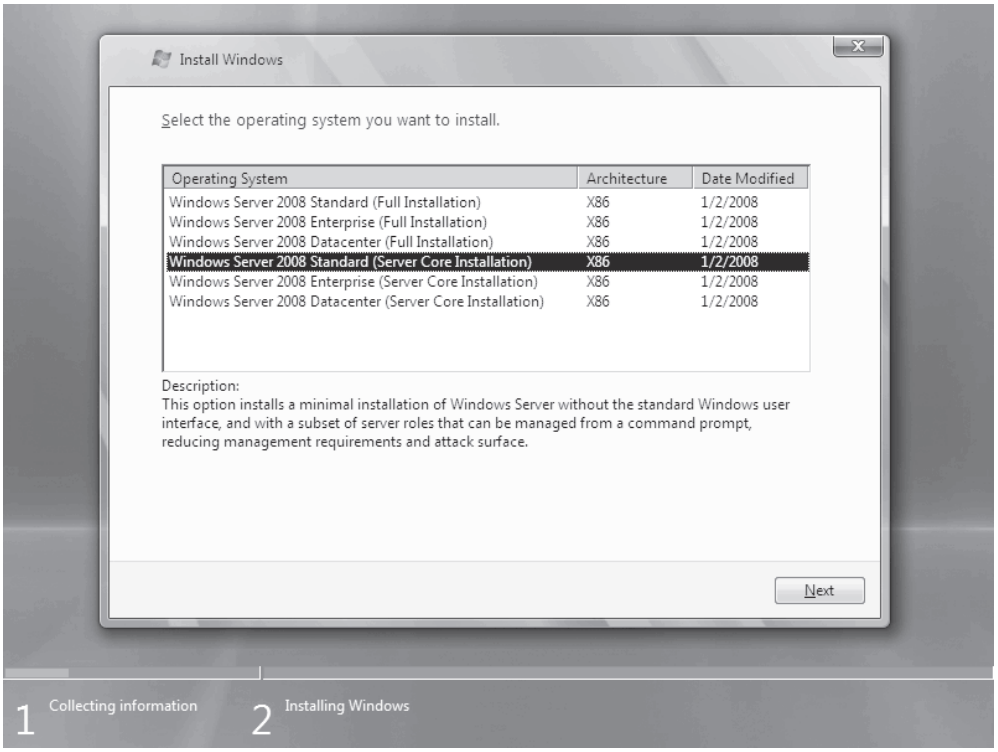
- Microsoft Failover Cluster
- Network Load Balancing
- زیر سیستم برنامه‌های مبتنی بر UNIX
- تهیه پشتیبان از ویندوزی
- Multipath I/O
- مدیریت دستگاههای ذخیره‌سازی قابل حمل (Removable Storage)
- رمزنگاری درایو در ویندوز (Bitlocker)
- Simple Network Management protocol(SNMP)
- Windows Internet Naming Service(WINS)
- کلاینت Telnet
- کیفیت سرویس‌دهی (QOS)

نصب Server Core

Server Core را طبق همان مراحل تمرین ۱ درس ۱ می توان نصب نمود . تفاوت نصب کامل و Server Core ، اول انتخاب گزینه Server Core در ویزارد نصب ویندوز می‌باشد (شکل ۱-۹) و دوم اینکه پس از نصب و ورود به ویندوز بجای رابط Windows Explorer خط فرمان دیده می‌شود .

نکته فقدان کلمه عبور اولیه برای کاربر Administrator

وقتی ویندوز سرور 2008 را از روی DVD نصب می‌کنید کاربر Administrator کلمه عبور ندارد . وقتی برای اولین بار به سیستم وارد می شوید از شما خواسته می شود کلمه عبور را تغییر دهید .



شکل ۹- ۱ صفحه انتخاب Operating Systems از ویزارد Install Windows

اجرای پیکربندی اولیه

در حالت نصب کامل ویندوز سرور 2008 پنجره Initial Configuration Tasks ظاهر می شود تا به ما در پیکربندی سرور کمک کند در حالی که Server Core هیچگونه رابط گرافیکی ندارد و باید پیکربندی را توسط ابزارهای خط فرمان انجام دهیم . جدول ۱-۱ عملیات پیکربندی رایج و دستور متناظر با آن را لیست می‌کند . برای دریافت اطلاعات بیشتر در مورد هر دستور دستور مربوط را در خط فرمان نوشته و علامت /? را به آن اضافه کنید .

جدول ۱-۱ دستورات پیکربندی Server Core

تغییر کلمه عبور Administrator	هنگام ورود با کلیدهای Ctrl+Alt+Del پیغام تغییرکلمه عبور ظاهر می‌شود . همچنین می‌توانید از دستور زیر استفاده کنید : Net user administrator
درج IP نسخه ۴ بصورت دستی	Netsh interface ipv4
فعال سازی (Activate) ویندوز سرور	Cscript c:\windows\system32\slmgr.vbs –ato
عضو دامنه کردن	Netdom
افزودن نقشها ،کامپوننتها یا ویژگیها به Server Core	بسته نرم‌افزاری یا ویژگی Ocsetup.exe توجه داشته باشید اسامی ویژگی حساس به حروف کوچک و بزرگ می‌باشد .
نمایش نقشها ، کامپوننتها و ویژگیهای نصب شده	Oclist.exe

فعال کردن Remote Desktop	Cscript c:\windows\system32\scregedit.wsf /AR 0
ارتقا سرور به DC	Dcpromo.exe
پیکربندی DNS	Dnscmd.exe
پیکربندی DFS	Dfscmd.exe

دستور Ocsetup.exe برای افزودن نقشها و ویژگیهای Server Core استفاده می‌گردد . AD DS از این قانون مستثنی است . برای افزودن یا حذف AD DS از Dcpromo.exe استفاده می‌شود .

افزودن نقش AD DS به Server Core

بدلیل اینکه هیچ‌نوع ویزارد نصب AD DS در Server Core موجود نیست برای پیکربندی AD DS باید دستور Dcpromo.exe را با پارامترهای مربوطه بکار گیریم .جهت دسترسی به راهنمای دستور در خط فرمان تایپ می‌کنیم Dcpromo.exe /? . همه سناریوهای پیکربندی اطلاعات جزئی‌تری هم دارد . مثلاً برای پارامترهای جزئی‌تر ارتقاء یک سرور به DC تایپ کنید :dcpromo.exe /?:promotion

اطلاعات بیشتر پارامترهای نصب غیرحضوری

لیستی از پارامترهای نصب غیرحضوری را در آدرس http://technt2.microsoft.com/windowsserver2008/en/library/bcd89659-402d-46fb-8535-8da1feb8d4111033.mspx می‌توانید بیابید .

اجرا کنید در تمرین ۳ آخر درس " یک DC با Server Core ایجاد کنید " روش افزودن AD DS به Server Core آموزش داده می شود .

حذف DC

گاهی‌اوقات ممکن است به هر دلیلی مجبور شویم DC را حذف کنیم . خیلی مهم است که DC را بطور صحیح حذف کنیم که اطلاعات مربوط به آن از Active Directory پاک شود . برای حذف DC از دستور Dcpromo.exe استفاده می کنیم .وقتی فرمان را با استفاده از رابط گرافیکی ویندوز روی یک DC اجرا کنید ویزارد نصب AD DS شما را به پیش می برد . اگر می‌خواهید از طریق خط فرمان اینکار را انجام دهید یا اصلاً DC شما Server Core است تایپ کنید dcpromo.exe /?:demotion تا اطلاعات دقیقتری راجع به پارامترهای عملیات حذف DC بدست آورید .

وقتی نقش AD DS را از روی یک سرور حذف می‌کنیم باید کلمه‌عبور کاربر Administrator محلی را مشخص کنیم تا پس از حذف DC بتوانیم با کاربر مذکور به وارد سیستم شویم .

تمرینات نصب DC بصورت Server Core

در این تمرینات قرار است یک DC به forest ، contoso.com که در تمرینات درس۱ ساخته شد افزوده شود. به منظور افزایش امنیت و کاهش بار مدیریتی DC جدید یک Server Core را به DC ارتقا می‌دهیم. قبل از اجرای تمرینات این درس باید تمرینات درس ۱ را کامل کرده باشیم.

تمرین ۱ نصب Server Core

در این تمرین Server Core روی یک کامپیوتر یا ماشین مجازی نصب می‌شود.

۱. DVD نصب ویندوز سرور 2008 را درون درایو قرار می‌دهیم .اگر از ماشین مجازی استفاده می‌کنیم باید بدنبال گزینه‌ای برای سوار کردن فایل ISO که از روی DVD نصب تهیه شده بگردیم . برای اطلاعات بیشتر به مستندات نرم‌افزار ماشین مجازی رجوع شود .
۲. کامپیوتر را روشن می‌کنیم .

اگر هارد کامپیوتر خالی است سیستم از روی DVD راه اندازی می‌شود وگرنه پیغامی مبنی بر فشردن یک کلید برای راه‌اندازی سیستم از روی DVD دریافت می‌کنیم .اگر سیستم از روی DVD راه‌اندازی نشد یا منوی بوت ظاهر شد به تنظیمات BIOS سیستم رفته و ترتیب سخت‌افزارها طوری تعیین می‌کنیم که سیستم از روی DVD بوت شود .

۳. گزینه‌های regional setting, language و keyboard layout متناسب با شرایط خود انتخاب کرده و گزینه Next را کلیک می‌کنیم .
۴. کلید Install Now را می‌زنیم .
۵. گزینه Windows Server 2008 Standard (Server Core Installation) را انتخاب کرده و گزینه Next را کلیک می‌کنیم .
۶. کادر I Accept The License Terms را علامت زده و گزینه Next را کلیک می‌کنیم .
۷. گزینه Custom (Advanced) را کلیک می‌کنیم .

۸. در صفحه Where Do You Want To Install Windows دیسکی که می‌خواهیم روی آن ویندوز سرور 2008 را نصب کنیم انتخاب می‌کنیم .اگر نیاز به ساخت ،حذف ،توسعه (extend) یا فرمت پارتیشن‌ها و یا بارگذاری درایور یک دیسک داشته باشیم روی Driver Options (Advanced) کلیک می‌کنیم .

۹. کلید Next را می‌زنیم .

۱۰. وقتی عملیات نصب کامل شد به سیستم وارد شوید. کاربر Administrator بدون کلمه عبور می‌باشد.

۱۱. پیغام تغییر کلمه عبور ظاهر می‌شود. کلمه عبوری را برای کاربر Administrator هم در کادر New Password و هم در Confirm Password تایپ کرده و Enter را می‌زنیم .

طول کلمه عبور باید حداقل ۷ کاراکتر بوده و سه نوع از چهار نوع کاراکترهای زیر را داشته باشد :

- حروف بزرگ از A تا Z
- حروف کوچک از a تا z
- عدد از 0 تا 9
- علائم مانند $ ،# ،@ و !

نکته کلمه عبور را فراموش نکنید

بدون کلمه عبور نمی‌توانیم وارد سرور شویم و تمرینات دیگر را انجام دهیم .

۱۲. گزینه OK را کلیک می‌کنیم. خط فرمان کاربر Administrator ظاهر می‌شود .

تمرین ۲ پیکربندی پس از نصب روی Server Core

در این تمرین پس از نصب سرور،پیکربندی نام و تنظیمات TCP/IP برای استفاده در تمرینات بعدی اجرا می‌گردد .

۱. نام سرور را با دستور netdom renamecomputer %computername% /newname:Server02 تغییر می‌دهیم. پیغام را با "Y" تایید می‌کنیم.

۲. آدرس Ipv4 سرور را با تایپ دستورات زیر پیکربندی می‌کنیم .

```
Netsh interface ipv4 set address name="Local Area Connection"
Source=static address=10.0.0.12 mask=255.255.255.0
Gateway=10.0.0.1

Netsh interface ipv4 set dns name="Local Area Connection"
Source=static address=10.0.011 primary
```

۳. پیکربندی IP وارد شده را با دستور ipconfig/all بررسی می‌کنیم.

۴. با استفاده از دستور shutdown –r –t 0سیستم را راه‌اندازی مجدد می‌کنیم.

۵. با کاربر Administrator وارد می‌شویم.

۶. با دستور netdom join %computername% /domain:contoso.com کامپیوتر را عضو دامنه می‌کنیم.

۷. با دستور shutdown –r –t 0 سیستم را راه‌اندازی مجدد می‌کنیم و با کاربر Administrator وارد می‌شویم.

۸. نقش‌های نصب شده سرور را با دستور oclist نمایش می‌دهیم.

به مشخصه بسته نرم‌افزاری برای نقش سروری DNS توجه کنید : DNS-Server-Core-Role.

۹. دستور ocsetup را تایپ کرده و کلید Enter را می‌زنیم.

عجب! ذره‌ای از رابط گرافیکی ویندوز در Server Core مشاهده می‌شود.

۱۰. روی OK کلیک می‌کنیم تا پنجره بسته شود.

۱۱. تایپ می‌کنیم ocsetup DNS-Server-Core-Role

مشخصه بسته نرم‌افزاری حساس به حروف بزرگ و کوچک است.

۱۲. دستور oclist را تایپ کرده و تایید نصب سرور DNS را کلیک می‌کنیم.

تمرین ۳ ایجاد DC با Server Core

در این تمرین با استفاده از دستور Dcpromo نقش AD DS را به Server Core اضافه می‌کنیم.

۱. دستور Dcpromo.exe /? را تایپ کرده و کلید Enter را می‌زنیم.

اطلاعات خروجی صفحه نمایش را مرور می‌کنیم.

۲. تایپ می‌کنیم dcpromo.exe /?:Promotion و کلید Enter را می‌زنیم.
اطلاعات خروجی صفحه نمایش را مرور می‌کنیم.
۳. دستور زیر را به منظور افزودن و پیکربندی نقش AD DS تایپ می‌کنیم :

```
Dcpromo /unattend /replicaOrNewDomain:replica
/replicaDomainDNSName:contoso.com /Confirmgc:Yes
/Username:CONTOSO\Administrator /Password:* /safeModeAdminPassword:P@sword
```

۴. هنگام ورود در پنجره کلمه عبور کاربر Administrator دامنه contoso را وارد کرده و OK را می‌زنیم.
نقش AD DS نصب و پیکربندی شده و سرور راه‌اندازی مجدد خواهد شد.

تمرین ۴ حذف DC

در این تمرین قرار است نقش AD DS از Server Core پاک شود.

۱. با کاربر Administrator به Server Core وارد شوید.
۲. تایپ می‌کنیمdcpromo /unattend /AdministratorPassword:passwordدر حالی که جای کلمه password کلمه عبور کاربر Administrator محلی را بصورت پیچیده (Strong) وارد می‌کنیم تا پس از حذف AD DS بتوانیم با کاربر مذکور وارد سیستم شویم. کلید Enter را می‌زنیم.

خلاصه درس

- ویندوز سرور 2008 نسخه Server Core یا همان Server Core نسخه حداقلی ویندوز 2008 می‌باشد که یک سری از ویژگی‌ها و نقشهای سروری را پشتیبانی می‌کند.
- Server Core امنیت و مدیریت پذیری سرورهای ویندوزی را افزایش می‌دهد.
- دستور Ocsetup.exe جهت افزودن و حذف نقش‌های Server Core جز AD DS بکار می‌رود. نقش AD DS با دستور Dcpromo.exe افزوده می‌شود.
- امکان خودکارسازی مراحل نصب یا حذف DC با دستور Dcpromo.exe /unattend به همراه پارامترهای مناسب دیگر وجود دارد.

سئوالات پایان درس

از سئوالات زیر برای ارزیابی دانش خود در درس ۲ می‌توانید استفاده کنید. سئوالات همچنین از روی CD همراه کتاب بشکل الکترونیک قابل دستیابی است.

۱. شما با کاربر Administrator وارد سیستم SERVER02شده‌اید. این سرور یکی از چهار DC در دامنه contoso.com است که سیستم عامل آنServer Core است. میخواهید نقش DC را از آن بگیرید. به کدام‌یک از موارد زیر نیاز دارید؟
   A. کلمه عبور کاربر Administrator محلی
   B. اعتبار یک کاربر عضو گروه Domain Admins
   C. اعتبار یک کاربر عضو گروه Domain Controllers
   D. آدرس سرور DNS
۲. SERVER02 دارای سیستم عامل Server Core است. نقش AD DS نیز قبلاً افزوده شده است. حال می‌خواهید سرویس Active Directory Certificate Services(AD CS) را اضافه کنید. چه باید بکنید؟
   A. نقش AD CS را نصب کنیم.
   B. نقش AD FS را اضافه کنیم.
   C. نقش AD RMS را اضافه کنیم.
   D. سرور را با حالت Windows Server 2008 (Full Installation) دوباره نصب کنیم.

فصل دوم

مدیریت

بیشتر مدیران شبکه اولین تجربه خود را با AD DS با Active Directory Users And Computers و ساخت اشیاء کاربر ، گروه و کامپیوتر در یک OU از دامنه شروع می‌کنند . اینها وظایف بسیار اساسی یک متخصص IT در محیط شبکه مبتنی بر Active Directory بوده بنابراین اکنون که طریقه ایجاد یک دامنه را در فصل ۱ " نصب " آموخته‌اید می‌توانید از ابزارها برای ساخت اشیاء استفاده کنید. در فصول بعدی هر کدام از این اشیاء را با جزئیات بیشتر بررسی خواهیم کرد .

در این فصل همچنین به دو موضوع مهم و سطحبالا در شبکه سازمانی نگاهی می‌اندازیم : اول اینکه چطور اشیاء را در دایرکتوری پیدا کنیم و دوم زمانی که نیروهای فنی را در انجام امور شبکه سهیم می‌کنیم چطور امنیت Active Directory را تامین کنیم .

قبل از شروع

برای اجرای تمرینات این فصل نیاز به یک ویندوز سرور 2008 نصب شده روی کامپیوتر فیزیکی یا ماشین مجازی داریم .نام ماشین SERVER01 باشد و DC دامنه contoso.com باشد . جزئیات روش ایجاد موارد فوق در فصل ۱ ارائه شده‌اند .

دنیای واقعی

دن هلم

شما قطعاً با ابزاهای مدیریتی نظیر Active Directory Users and Computers snap-in و مهارتهای ابتدایی برای ساخت OU ها ، کاربران ، کامپیوترها و گروهها آشنا هستید . در این فصل ابزارها و مهارتهایی بررسی می شوند که می‌توانند نقاط تاریک اطلاعاتی ما را روشن کنند . از این مهمتر روشهایی را بررسی می‌کنیم که بهره‌وری و تاثیرگذاری ما را به عنوان مدیر شبکه افزایش می‌دهد . دیده‌شده بسیاری از مدیران شبکه برای انجام کارهایشان ، بجای باز کردن یک کنسول MMC (Microsoft Management Console) با تمام snap-in های مورد نیاز ، چندین کنسول را جداگانه باز می‌کنند . همچنین بعضی از مدیران شبکه بجای استفاده از مزایای پرس‌وجوی ذخیره‌شده برای جستجو و مدیریت اشیاء همیشه با صرف زمان زیاد در ساختار OUها به دنبال اشیاء مورد نظر خود می‌گردند . هرچند مطالب این فصل یک هدف را دنبال می‌کند "نگهداری و مدیریت حسابهای Active Directory " ، مطلب کمکی ارائه شده در گوشه کنار متن جزو باارزشترین بخشهای کتاب می باشد چراکه به شما کمک می‌کند همیشه بتوانید در شبکه سازمان خودتان موثرتر و ایمن‌تر کار کنید

درس ۱ : کار با snap-in های Active Directory

ابزارهای مدیریتی یا snap-in های Active Directory شرایط مورد نیاز جهت پشتیبانی از سرویس دایرکتوری را در اختیار می‌گذارد . در این درس با محل یابی و تشخیص مهم‌ترین snap-in های Active Directory اشنا می‌شوید . و یاد می‌گیرید چطور با استفاده از اعتبار جایگزین با آنها موثرتر کار کنید و چطور کنسولهای رایج و پرکاربرد ساخته و بین مدیران شبکه سازمان توزیع کنید .

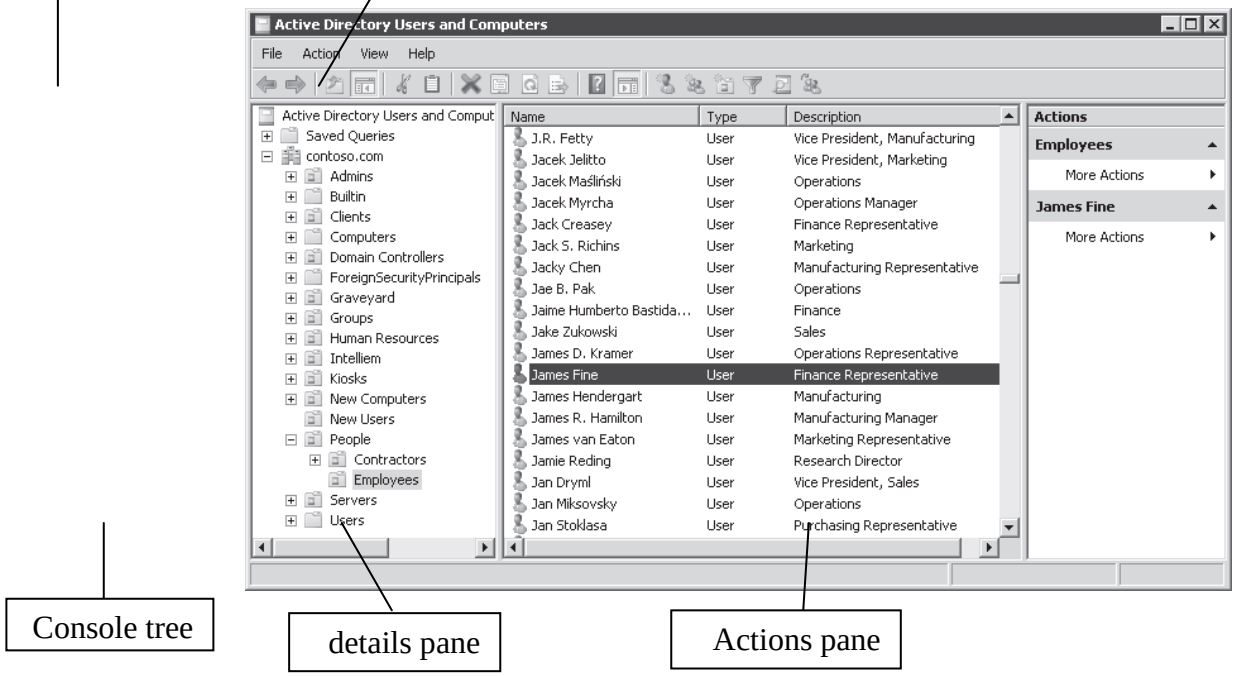
اشنایی با کنسول MMC

ابزار Administrative Tools در ویندوز بستری رابا نام MMC در اختیار کاربر قرار می‌دهد . این کنسول ابزارها را به شکل دلخواه نمایش می‌دهد . در سمت چپ پنل ساختار درختی کنسول (شبیه ساختار درختی Windows Explorer) و در وسط صفحه پنل جزئیات قرار دارد . در سمت راست ، پنل Actions دستوراتی در اختیار کاربر قرار می‌دهد . شکل ۲-۱ مثالی را در این زمینه نشان می‌دهد .

برای سفارشی کردن پنل‌های چپ و راست از تکمه‌های Show/hide Console Tree و Show/Hide Action Pane یا گزینه Customize از منوی View استفاده می شود .

ابزارهای مدیریتی که اینجا snap-in نامیده می‌شود از ساختار درختی و پنل جزئیات کنسول به منظور اجرای عملیات مدیریتی استفاده می‌کنند . MMC را می‌توان مانند یک کمربند ابزار در نظر گرفت که ابزارهای مختلف (snap-in) به آن متصل می‌شوند . ابزارها مستقیماً نمی‌توانند اجرا شوند و باید در محیط MMC قرار گیرند .بسیاری از ابزارهای پوشه Administrative Tools از یک کنسول با یک snap-in تشکیل می‌شوند . نمونه این ابزارها Event Viewer ، Services و Task Scheduler می باشد . ابزارهای دیگری مانند Computer Management کنسولهایی با چند ابزار هستند که خود این ابزارها به تنهایی می‌توانند کنسول مجزایی داشته باشند .مثلاً کنسول Computer Management شامل ابزارهای Event Viewer ، Services وTask Scheduler می باشد .

در حین کار با ابزارها در MMC می‌توان فرمانهایی بنام actions را اجرا کرد . این فرمانها هم از منوی Actions هم با کلیک راست و هم از پنل Action سمت راست کنسول قابل دسترسی است. بسیاری از مدیران باتجربه راحتتر هستند از منوی کلیک راست برای اجرای فرامین استفاده کنند . اگر شما هم از این منو استفاده می‌کنید بهتر است برای باز کردن فضای کنسول پنل Actions را ببندید .



شکل ۱- ۲ کنسول MMC و ابزارهای آن

دو نوع MMC وجود دارد : آماده و سفارشی . کنسولهای آماده زمانی که سرویس یا نقشی افزوده می شود برای مدیریت آن سرویس یا نقش بطور اتوماتیک نصب می‌شود .اینها در حالت user کار می‌کنند بنابراین نمی‌توانیم آنها را تغییر دهیم . کاربران می‌توانند کنسولهای سفارشی را دقیقاً با ابزارها و عملکرد مورد نیاز بسازند . در بخشهای بعدی از هر دو نوع کنسول استفاده می‌کنیم .

ابزارهای مدیریتی Active Directory

بسیاری از عملیات مدیریتی Active Directory در کنسولها و snap-inهای زیر اجرا می‌شود .

- **Active Directory Users and Computers** پرکاربردترین منابع شبکه را شامل کاربران ، گروهها ، پرینترها و پوشه‌های به‌اشتراک‌گذاشته شده مدیریت می‌کند . این کنسول احتمالاً پر مراجعه‌ترین ابزار مدیریتی Active Directory است .
- **Active Directory Site and Services** عملیات مدیریتی تکثیر ، توپولوژی شبکه و سرویسهای مرتبط را انجام می‌دهد .از این ابزار در فصل ۱۱ "Site and Replication"بسیار استفاده می شود .
- **Active Direcroty Domains and Trusts** در این کنسول روابط trust و سطوح عملیاتی forest و دامنه پیکربندی می‌شود . این ابزار در فصل ۱۳ "Domains and Forests" بررسی می‌شود .
- **Active Directory Schema** تست و تغییر تعریف خصوصیات و کلاسهای اشیاء Active Directory را انجام می‌دهد. این schema طرح Active Directory می‌باشد . بندرت دیده می شود یا تغییر می‌کند . به‌همین دلیل بطور پیش فرض نصب نمی شود .

کنسولها و ابزارهای Active Directory در زمان افزودن نقش AD DS به سرور نصب می شوند . از این بین دو ابزار پرکاربرد که به Server Manager اضافه می‌شوند یکی Active Directory Users and Computers است ودیگری Active Directory Sites and Services . اگر بخواهیم Active Directory را از یک سیستم دیگر که DC نیست مدیریت کنیم باید ویژگی RSAT را از طریق گره features در Server Manager ویندوز سرور 2008 نصب کنیم . این برنامه از سایت مایکروسافت قابل دانلود و نصب روی کلاینتهای ویستا سرویس‌پک ۱ می‌باشد .

جستجوی ابزارهای مدیریتی Active Directory

وقتی گره Roles and Active Directory Domain Services را در پنجره Server Manager باز می‌کنیم فقط دو ابزار می‌بینیم . همه ابزارها در پوشه Administrative Tools در کنترل پنل در دسترس می باشد . در نمایش کلاسیک کنترل پنل پوشه Administrative Tools جداگانه نشان داده می‌شود ولی در نمایش Home در پوشهSystem and Maintenance قابل دستیابی است .

افزودن Administrative Tools به منوی استارت

بطور پیش‌فرض Administrative Tools در منوی استارت ویندوز ویستا نمایش داده نمی‌شود .برای راحتی بیشتر می‌توانید آنرا به روش زیر به منو اضافه کنید .

۱. روی تکمه شروع کلیک راست کرده و Properties را انتخاب می‌کنیم .
۲. گزینه Customize را انتخاب می‌کنیم .

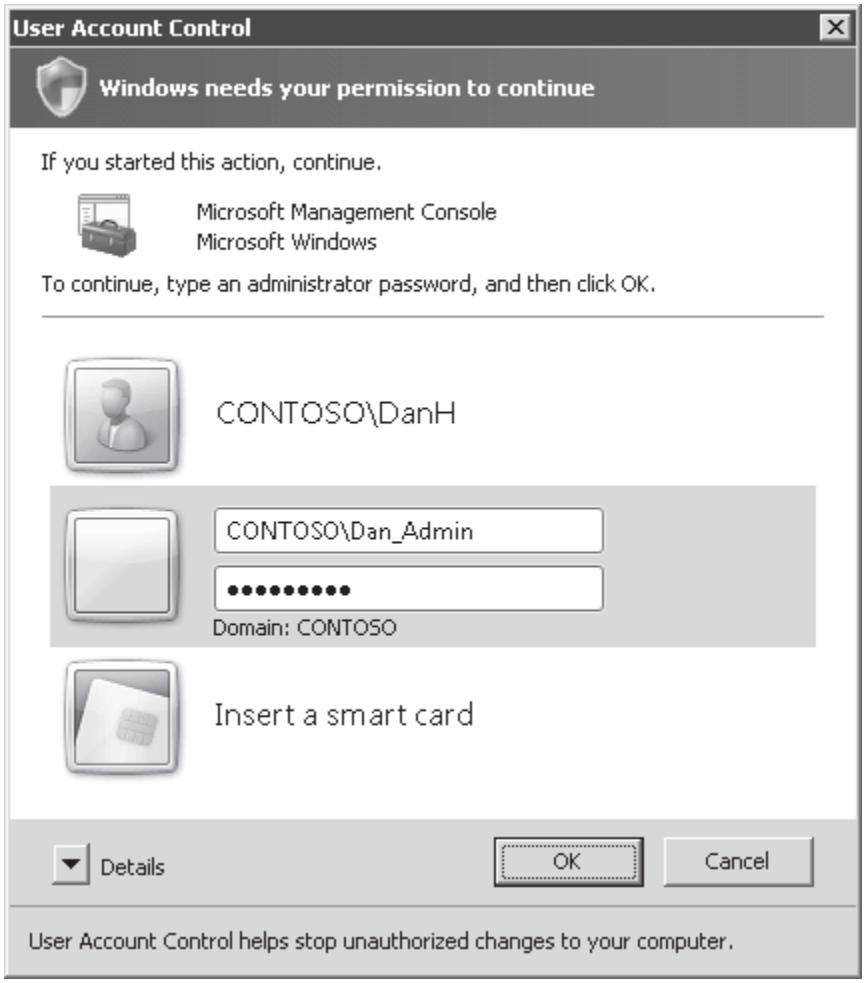
۳. اگر از منوی استارت پیش‌فرض استفاده می‌کنیم به System Administrative Tools اسکرول کرده و گزینه Display On The All Programs Menu And The Start Menu یا Display On The All Programs Menu را انتخاب می‌کنیم . ولی اگر از منوی استارت کلاسیک استفاده می‌کنیم گزینه Display Administrative Tools را انتخاب می‌کنیم .

۴. دوبار OK را می‌زنیم .

باز کردن ابزارهای مدیریتی با کاربر جایگزین

بسیاری از مدیران شبکه با حساب کاربری که توانائی مدیریت شبکه را دارد به کامپیوتر خود وارد می‌شوند . این کار بسیار خطرناک است چون حساب کاربری با اعتبار مدیریتی دسترسی بیشتری از یک حساب کاربری استاندارد دارد . بنابراین بدافزاری که با حساب کاربری مدیریتی اجرا شده می‌تواند صدمات بیشتری وارد کند . برای جلوگیری از این مشکل هیچگاه با حساب Administrator وارد نشوید . بجای آن بعنوان کاربر استاندارد وارد شده و برای اجرای ابزارهای مدیریتی با استفاده از ویژگی Run As Administrator از اعتبار مدیریتی لازم بهره‌مند شوید .

بر روی یک اپلت کنترل پنل یا MMC که می خواهید اجرا کنید کلیک راست کرده و گزینه Run As Administrator را کلیک کنید . اگر گزینه در منو وجود ندارد کلید Shift را نگهداشته و بعد کلیک راست کنید . همانطور که در شکل ۲-۲ می‌بینید کادر محاوره‌ای User Account Control ظاهر می شود .



شکل ۲-۲ کادر محاوره‌ای Account Control که اعتبار مدیریتی را وارد می‌کنیم.

۱. نام کاربری و کلمه عبور حساب کاربری با اعتبار مدیریتی را وارد کنید .

۲. کلید OK را بزنید .

اگر برنامه‌ای را مرتب با اعتبار مدیریتی اجرا می‌کنید میانبری را که با اعتبار مدیریتی پیکربندی شده بسازید . میانبر را ایجاد کرده و کادر محاوره‌ای properties میانبر را باز کنید .تکمه Advanced را بزنید و Run As Administrator را انتخاب کنید . از این به بعد هرزمان که میانبر را اجرا کنید کادر محاوره‌ای User Account Control ظاهر می شود .

ساخت کنسول سفارشی با Active Directory snap-in

مدیریت ویندوز زمانی ساده است که ابزارهای مورد نیاز همگی یکجا جمعند و بسته به نیاز ما سفارشی می شوند برای رسیدن به این مقصود می‌توان یک MMC سفارشی مدیریتی ساخت که بنا به تشبیه کمربند ابزارهای مورد نیاز ما بحساب می‌آید . با ساخت این کنسول می توانیم :

- ابزارهای متعددی را اضافه کنیم بطوریکه مجبور نباشیم برای اجرای وظایف دائماً بین کنسولها سوئیچ کنیم و اینکه فقط یک کنسول با اعتبار مدیریتی ساخته می‌شود .
- کنسولها را برای استفاده‌های بعدی ذخیره کنیم .
- کنسول را بین مدیران دیگر توزیع کنیم .
- کنسولها را به منظور مدیریت واحد و سفارشی شده در یک محل به اشتراک گذاشته شده متمرکز کنیم .

جهت ساخت یک MMC سفارشی یک MMC خالی باز کنید . برای اینکار از منوی استارت و کادر Start Search کلمه mmc.exe را تایپ کنید و کلید Enter را بزنید . برای افزودن ، حذف ، مرتب‌سازی و مدیریت ابزارهای کنسول از منوی File گزینه Add/Remove Snap-in را انتخاب کنید .

انجام دهید تمرین ۱ "ساخت یک MMC سفارشی" تمرین ۲ "افزودن یک ابزار به MMC" و تمرین ۳ "مدیریت ابزارهای یک MMC "

در آخر این درس شما را پله به پله با مهارتهای مرتبط با ساخت کنسول سفارشی چند ابزاره آشنا می‌کند .

ذخیره و توزیع کنسول سفارشی

اگر می‌خواهید کنسولی را توزیع کنید پیشنهاد می‌شود آنرا در حالی User ذخیره کنید .برای تغییر حالت کنسول از منوی File گزینه Option را انتخاب می‌کنیم . بطور پیش فرض کنسولها در حالت author ذخیره می‌شوند که امکان حذف و اضافه کردن ابزارها ، رویت همه بخشهای کنسول و ذخیره تغییرات را به کاربر می‌دهند . بالعکس حالت User عملکرد کنسول را محدود می کند تنظیمات کنسول تغییر نکند .حالت User خود سه نوع است. حالت User-Full Access معمولاً برای مدیران ارشد شبکه که از ابزارها بطور گسترده استفاده می‌کنند انتخاب می شود . حالت User-Limited Access(Multiple Window و Single Window) حالت دسترسی پایین است بنابراین برای کنسول مدیرانی انتخاب می‌شود که وظایف جزئی تری دارند .

بعد از اینکه کنسول را در حالت User ذخیره کردید برای انجام تغییرات در کنسول باید روی آن کلیک راست کرده و گزینه Author را انتخاب کنیم .

کنسولها با پسوند msc. ذخیره می شوند . محل پیش فرض ذخیره انها پوشه Administrative Tools می باشد ولی نه آن که در کنترل پنل موجود است . محل ذخیره آن پوشه Start Menu در پروفایل کاربر است :%userprofile%\AppData\Roaming\Microsoft\Windows\StartMenu

این مسیر مشکل دارد زیرا فقط کاربر آن پروفایل به کنسول دسترسی دارد . بهترین راه اینست که با یک کاربر با دسترسی محدود به کامپیوترتان وارد شوید و سپس ابزارهای مدیریتی مانند کنسول سفارشی را با حساب کاربری جایگزین که برای انجام وظایف مدیریتی اعتبار کافی دارد اجرا کنید . بدلیل اینکه هر دو حساب کاربری درگیر هستند ذخیره کنسول در پوشه Start Menu مربوط به پروفایل یکی از کاربران بدین معنی است که ما را به زحمت می‌اندازد و در بدترین حالت با خطای access-denied مواجه می شویم .

کنسول خود را در محلی ذخیره کنید که هم با کاربر معمولی وهم با کاربر دارای اعتبار مدیریتی قابل دسترس باشد . پیشنهاد می‌شود کنسولها را در یک پوشه به اشتراک‌گذاشته شده در شبکه ذخیره کنید تا زمانی که از سیستم‌های دیگر وارد شبکه می‌شوید به ابزارهای خود دسترسی داشته باشید . همچنین پوشه می‌تواند در دسترس همه مدیران دیگر قرار گیرد و همه کنسولهای سفارشی در این پوشه متمرکز شود . راه دیگر ذخیره کنسولها روی حافظه‌های قابل حمل مانند درایو USB و یا حتی ارسال آنها بعنوان پیوست یک نامه الکترونیکی می‌باشد .

به یاد داشته باشیم که کنسولها اساساً یک سری دستورالعمل هستندکه توسط mmc.exe تفسیر می‌شوند . دستورالعمل‌هایی که مشخص می‌کنند کدام ابزارها افزوده شوند و کدام کامپیوترها با آن ابزارها مدیریت شوند .خود ابزارها در کنسولها موجود نیستند بنابراین اگر ابزاری نصب نباشد حتی اگر snap-in آن به کنسول افزوده شده باشد کار نمی‌کند . پس snap-in های مناسب را از RSAT روی سیستم مورد نظر نصب کنید .

کاربر در حالت Author می تواند ابزارها را حذف یا اضافه کند و کنسول را بطور کامل سفارشی کند . حالت User از اعمال تغییر روی کنسول جلوگیری می‌کند .

تمرینات ساخت و مدیریت کنسول MMC سفارشی

در این تمرین یک کنسول سفارشی MMC می‌سازیم. بعد ابزارها را اضافه، حذف و مرتب می کنیم. سپس کنسول را برای استفاده مدیران دیگر شبکه توزیع می‌کنیم.

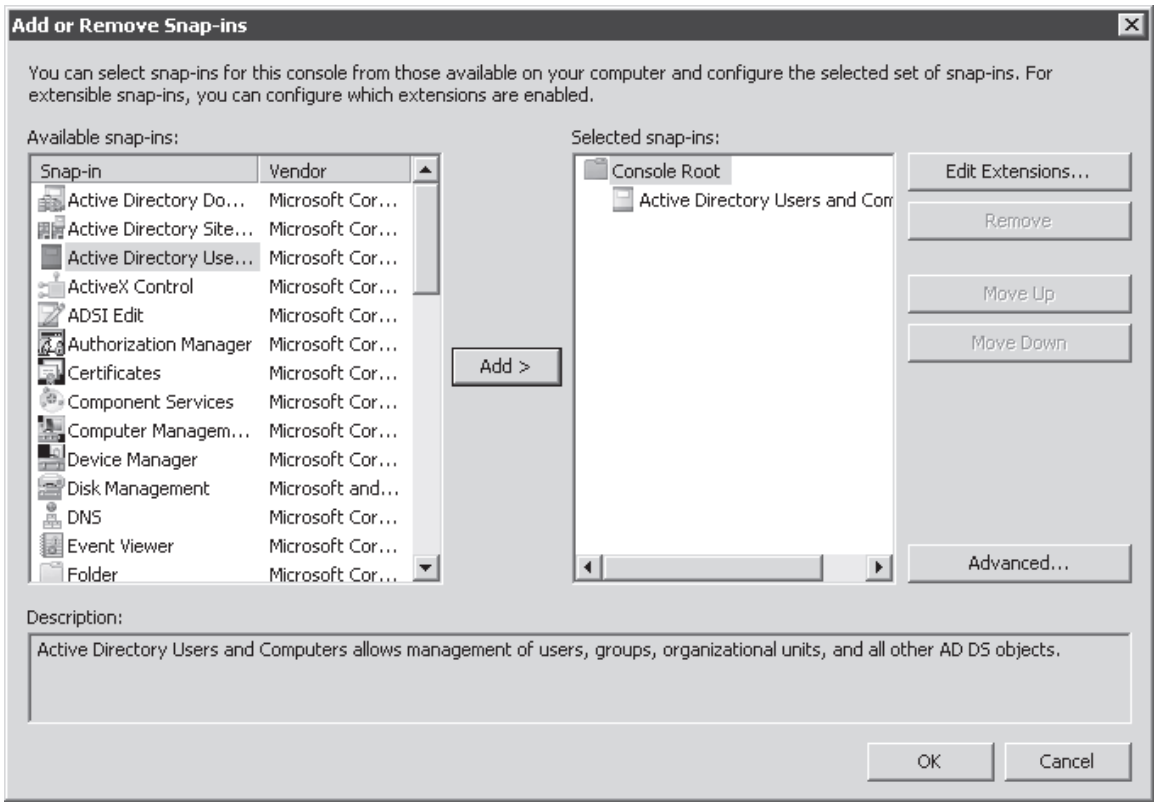
تمرین ۱ ساخت کنسول MMC سفارشی

در این تمرین با استفاده از ابزارهای Active Directory Users And Computers، Active Directory Schema و Computer Management کنسول سفارشی MMC می‌سازیم. این ابزارها برای مدیریت Active Directory و DC مفید می‌باشند.

۱. با کاربر Administrator به SERVER01 وارد می‌شویم.

۲. روی دکمه استارت کلیک کرده در کادر Start Search عبارت mmc.exe را تایپ کرده و کلید Enter را می‌زنیم. یک کنسول MMC خالی باز می‌شود.

۳. از منوی File ابزار Add/Remove را انتخاب می‌کنیم. کادر محاوره‌ای Add Or Remove Snap-ins طبق شکل ۳- ۲ ظاهر می‌شود.



شکل ۳- ۲ کادر محاوره‌ای Add Or Remove Snap-ins

اگر ابزار مورد نظر دیده نمی‌شود باید RSAT را نصب کنیم.

۴. در کادر محاوره‌ای Add Or Remove Snap-ins از لیست Available Snap-ins ابزار Active Directory Users And Computers را انتخاب می‌کنیم.

۵. روی دکمه Add کلیک می‌کنیم تا به لیست Selected Snap-ins افزوده شود. توجه داشته باشید که ابزار Active Directory Schema به همراه نقش AD DS با RSAT نصب می‌شود ولی رجیستر نمی‌شود بنابراین در لیست ظاهر نمی‌شود.

۶. روی OK کلیک می‌کنیم تا کادر بسته شود.

۷. منوی استارت را باز کرده و در کادر Start Search عبارت cmd.exe را تایپ می‌کنیم.

۸. در خط فرمان دستور regsvr32.exe schmmgmt.dll را اجرا می‌کنیم. این دستور باعث می‌شود DLL مربوط به ابزار Active Directory Schema رجیستر شود. این کار برای افزودن این ابزار به کنسول الزامی است.

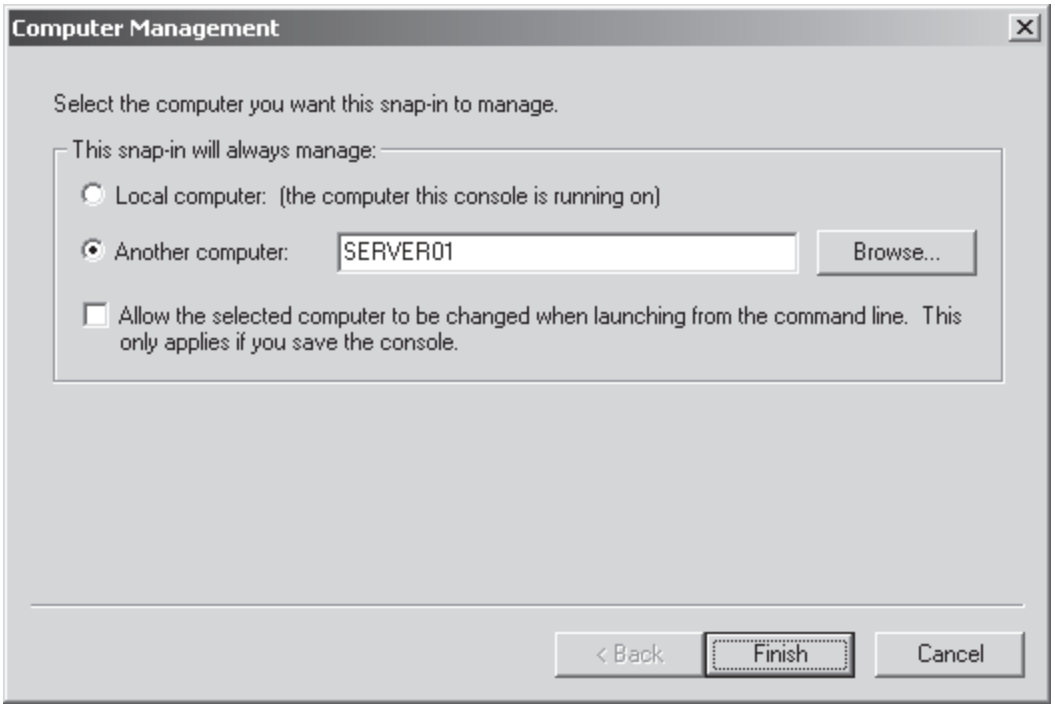
۹. پیغامی مبنی بر رجیستر شدن موفق نمایش داده می‌شود. روی OK کلیک می‌کنیم.

۱۰. به کنسول برمی‌گردیم و مراحل ۲ تا ۶ را برای افزودن ابزار Active Directory Schema تکرار می‌کنیم.

۱۱. از منوی File، Add/Remove Snap-in را انتخاب می‌کنیم.

۱۲. در کادر محاوره‌ای Add Or Remove Snap-ins و از لیست Available Snap-ins گزینه Computer Managenent را انتخاب می‌کنیم.

۱۳. روی دکمه Add کلیک می‌کنیم تا به لیست اضافه شود. اگر ابزاری از مدیریت راه دور پشتیبانی کند همانند شکل ۴- ۲ پیغامی مبنی بر انتخاب کامپیوتر مورد نظر ظاهر می‌شود.



شکل ۴- ۲ انتخاب کامپیوتر برای مدیریت توسط یک ابزار

- برای مدیریت کامپیوتری که کنسول روی آن اجرا می‌شود Local Computer را اجرا می‌کنیم.
- برای مشخص کردن یک کامپیوتر که ابزار کار مدیریت آنرا انجام می‌دهد Another Computer را انتخاب می‌کنیم. سپس نام کامپیوتر را وارد کرده یا روی Browse کلیک می‌کنیم و کامپیوتر را انتخاب می‌کنیم.

۱۴. Another Computer را انتخاب کرده و عبارت SERVER01 را به عنوان نام کامپیوتر تایپ می‌کنیم.

۱۵. روی Finish کلیک می‌کنیم.

۱۶. روی OK کلیک می‌کنیم.

۱۷. کنسول را با نام MyConsole.msc ذخیره می‌کنیم.

۱۸. کنسول را می‌بندیم.

تمرین ۲ افزودن یک ابزار به MMC

در این تمرین Event Viewer را به کنسولی که در تمرین ۱ ساختیم اضافه می‌کنیم که ابزار مفیدی برای مانیتور کردن فعالیت‌های روی DC می‌باشد.

۱. کنسول MyConsole.msc را باز می‌کنیم.

۲. از منوی File گزینه Add/Remove Snap-in را انتخاب می‌کنیم.

۳. در کادر محاوره‌ای Add Or Remove Snap-ins از لیست Available Snap-ins ابزار Event Viewer را انتخاب می‌کنیم.

۴. روی دکمه Add کلیک می‌کنیم تا به لیست اضافه شود.

۵. Another Computer را انتخاب کرده و عبارت SERVER01 را تایپ می‌کنیم.

۶. روی OK کلیک می‌کنیم.

۷. روی OK کلیک می‌کنیم تا کادر بسته شود.
۸. کنسول را ذخیره کرده و می‌بندیم.

تمرین ۳ مدیریت ابزارهای MMC

در این تمرین یاد می‌گیریم چطور ترتیب ابزارها را تغییر داده و یک ابزار را حذف کنیم. همچنین در مورد ابزارهای extension یاد می‌گیریم.

۱. MyCosole.msc را باز می‌کنیم.
۲. از منوی File گزینه Add/Remove Snap-in را انتخاب می‌کنیم.
۳. در لیست ابزارهای Selected گزینه Event Viewer را انتخاب می‌کنیم.
۴. روی دکمه Move Up کلیک می‌کنیم.
۵. Active Directory Schema را انتخاب می‌کنیم.
۶. روی دکمه Remove کلیک می‌کنیم.
۷. در لیست ابزارهای Selected گزینه Computer Management را انتخاب می‌کنیم.
۸. روی Edit Extensions کلیک می‌کنیم. Extension ها ابزارهایی هستند که در ابزارهای دیگر قرار دارند.
۹. Enable Only Selected Extensions را انتخاب می‌کنیم.
۱۰. Event Viewer را از حالت انتخاب خارج می‌کنیم.
۱۱. دو بار روی OK کلیک می‌کنیم تا کادرها بسته شوند.
۱۲. کنسول را ذخیره کرده و می‌بندیم.

تمرین ۴ آماده‌سازی کنسول برای ارائه به کاربران

در این تمرین کنسول خود را در حالت user ذخیره می‌کنیم تا کاربران نتوانند ابزارها را حذف و اضافه کنند یا تغییر دهند. به خاطر داشته باشید که کابران MMC خود مدیران شبکه هستند.

۱. MyConsole.msc را باز می‌کنیم.
۲. از منوی File گزینه Options را انتخاب می‌کنیم.
۳. در لیست بازشوی Cosole Mode گزینه User Mode – Full Access را انتخاب می‌کنیم.
۴. روی OK کلیک می‌کنیم.
۵. کنسول را ذخیره کرده و می‌بندیم.
۶. کنسول را باز می‌کنیم.
۷. منوی File را باز می‌کنیم. توجه کنید که گزینه Add/Remove Snap-in موجود نیست.
۸. کنسول را می‌بندیم.
۹. روی کنسول کلیک راست کرده و Author را انتخاب می‌کنیم.
۱۰. منوی File را باز کرده و می‌بینیم که در حالت author گزینه Add/Remove Snap-in ظاهر می‌شود.
۱۱. کنسول را می‌بندیم.

خلاصه درس

- ابزارهای مدیریتی ویندوز می‌توانند به کنسول MMC افزوده شوند. ابزار Active Directory Users And Computers و دیگر ابزارهای مدیریت Active Directory در کنسول Server Manager و کنسول‌های از پیش آماده Administrative Tools نیز حضور دارند.
- مدیران شبکه بهتر است به کامپیوترهایشان با کاربر مدیریتی وارد نشوند. در عوض بهتراست از یک کاربر استاندارد برای ورود استفاده کنند و برای اجرای ابزارهای مدیریتی از دستور Run As Administrator استفاده کنند.

- کنسول MMC سفارشی می‌سازیم که حاوی همه ابزارهای مورد نیاز ما باشد. این کنسول در جایی ذخیره می‌شود که ما و دیگر مدیران شبکه به آن دسترسی داشته باشند.
- پیشنهاد می‌شود کنسول را در حالت user ذخیره کنیم تا تغییرات ناخواسته اعمال نشود.

سئوالات پایان درس

۱. فرض کنید کارشناس نگهداری شبکه شرکت Contoso, Ltd هستیم. مدیران شبکه کنسولی با ابزار Active Directory Users and Computers توزیع کرده‌اند. وقتی کنسول را باز می‌کنیم تا کلمه عبور کاربری را ریست کنیم پیغام Access Denied دریافت می‌کنیم. مطمئن هستیم که مجوز مربوطه را داریم. بهترین راه حل مشکل چیست؟

A. کنسول را می‌بندیم و Server Manager را باز می‌کنیم و کار را با آن انجام می‌دهیم.

B. کنسول را می‌بندیم و در خط فرمان دستور dsa.msc را اجرا می‌کنیم.

C. کنسول را می‌بندیم و روی کنسول کلیک راست کرده و Run As Administrator را انتخاب می‌کنیم. نام کاربری و کلمه عبور و مدیریتی خود را وارد می‌کنیم.

D. کنسول را می‌بندیم و روی آن کلیک راست کرده و پنجره خط فرمان را باز می‌کنیم. دستور DSMOD USER را با سوئیچ P– به کار می‌گیریم.

درس ۲ : ساخت اشیاء در Active Directory

Active Directory یک سرویس دایرکتوری است و نقش یک سرویس دایرکتوری را با هدف نگهداری اطلاعات درباره منابع شبکه شامل کاربران ، گروهها و کامپیوترها بازی می‌کند . این منابع در OUها مختلف جای می‌گیرند تا کار مدیریت و جستجوی آنان ساده‌تر صورت گیرد . دراین درس یاد می‌گیریم چطور OU ، کاربر ، گروه و کامپیوتر بسازیم . همچنین مهارتهای خوبی در پیدا کردن اشیاء در زمان نیاز کسب می‌کنیم .

اگر تجربه کار با Active Directory را دارید می‌توانید چند بخش اول این درس را فقط مرور کنید ولی از بخشهای بعدی که عنوان آن با عبارت " اشیاء را در Active Directory پیدا کنید " شروع می‌شود سریع نگذرید چرا که به شما کمک می‌کند از ابزارهای Active Directory بهتر استفاده کنید .

تمرینهای انتهای درس را حتماً انجام دهید زیرا از اشیاء ساخته شده در این تمرینها در تمرینهای دروس بعد استفاده می‌شود .

بعد از اتمام این درس می‌توانید :

- کاربر ، گروه و OUها بسازید
- حفاظت از OUها را به منظور حذف آن غیر فعال کنید
- ابزار Active Directory Users and Computers را سفارشی کرده و از ویژگیهای آن برای کارکرد موثرتر با اشیاء دایرکتوری بهره مند شوید
- پرس‌و جوهای ذخیره شده بسازید تا نماهایی بر اساس قواعد خاص از اشیاء دایرکتوری داشته باشید

زمان درس : ۴۵ دقیقه

ساخت OU(Organizational Unit)

OUهاcontainerهایی در Active Directory هستند که اشیاء با نیازمندیهای مشابه را از نظر مدیریت ، پیکربندی و نمایش در خود جای می‌دهند .معنی این جمله زمانی روشن می‌شود که در مورد طراحی و مدیریت OUها بیشتر یاد بگیریم . الآن کافی است بدانیم OUها ساختار سلسله‌مراتبی مدیریتی مانند ساختار پوشه‌ها در دیسک درایو دارند. واژه مدیریت با تاکید استفاده می‌شود زیرا OUها برعکس گروهها برای دادن مجوز نسبت به منابع شبکه ساخته نمی‌شوند . کاربران در گروههایی قرار می‌گیرند که نسبت به منابع ، مجوزهای مشخصی دارند . OUهاcontainerهای مدیریتی هستند که کاربران و گروههای داخل آن توسط مدیران شبکه مدیریت می‌شوند .

برای ساخت یک OU :

۱. Active Directory Users and Computers snap-in را باز کنید
۲. روی گره Domain یا OU که داخل آن می‌خواهید OU جدید بسازیدکلیک راست کرده گزینه New و سپس Organizational Unit را انتخاب کنید
۳. نام OU را تایپ کنید . برای اینکار از قواعد نام‌گذاری سازمان تبعیت کنید
۴. گزینه Protect Container From Accidental Deletion را انتخاب کنید
۵. روی OK کلیک کنید . OUها خصوصیات دیگری دارند که می‌توان پیکربندی کرد . این خصوصیات بعد از ساخت شیء قابل تنظیم است .
۶. روی OU کلیک راست کرده و Properties را انتخاب کنید . از قواعد نام گذاری و دیگر استانداردها و رویه‌های سازمان پیروی کنید .از فیلد Description برای توضیح علت ساخت یک OU می‌توان استفاده کرد . اگر OU به یک محل فیزیکی مانند یک ساختمان از سازمان اختصاص دارد خصوصیت آدرس OU خیلی بدرد می‌خورد . زبانه Managed By به کاربر یا گروهی اشاره می‌کند که مسئولیت OU را به عهده دارد . تکمه Change را زیر کادر Name کلیک کنید . بطور پیش فرض کادر محاوره‌ای Select User,Contact,Or Group ظاهر می‌شود . برخلاف نامش در این کادر گروهها را نمی‌توان جستجو کرد . برای اینکار باید ابتدا روی تکمه Object Types کلیک کرده و Groups را انتخاب کنیم . درباره کادر محاوره‌ای Select User,Contact,Or Group در همین درس بیشتر یاد می‌گیریم .اطلاعات تماس باقی مانده از زبانه Managed By از کاربر مشخص شده در کادر Name درج می‌گردد. زبانه Managed By به تنهایی برای اطلاعات تماس استفاده می‌شود و به کاربر یا گروه درج شده هیچ نوع مجوز و دسترسی نسبت به OU اعطا نمی‌شود .
۷. روی OK کلیک کنید .

ابزارهای مدیریتی ویندوز سرور 2008 گزینه جدیدی را ارائه می‌دهد : Protect Container From Accidental Deletion . این گزینه OU را از حذف اتفاقی در امان نگه می‌دارد . دو مجوز به OU اعطا می‌گردد : Everyone::Deny::Delete و Everyone::Deny::Delete Subtree . نه کاربر و نه مدیر شبکه قادر نیستند بطور اتفاقی واحدسازمانی و محتویات آنرا پاک کنند .اکیداً توصیه می شود این نوع حفاظت را در مورد همه OUها جدید فعال کنید .

اگر تصمیم به حذف OU گرفتید باید این حفاظت را غیر فعال کنید . برای حذف OU حفاظت شده مراحل زیر را دنبال کنید :

۱. در Active Directory Users And Computers snap-in از منوی View گزینه Advanced Features را انتخاب کنید
۲. روی OU مورد نظر کلیک راست کرده Properties را انتخاب کنید
۳. زبانه Object را کلیک کنید . اگر زبانه Object را نمی‌بینید بخاطر اینست که در مرحله اول Advanced Features را فعال نکرده‌اید .
۴. علامت کادر Protect Container From Accidental Deletion را بردارید
۵. کلید OK را بزنید .
۶. روی OU کلیک راست کرده و delete را انتخاب کنید .
۷. پیغامی مبنی بر اطمینان از حذف OU دریافت می‌کنید . کلید Yes را کلیک کنید .
۸. اگر OU شامل اشیاء دیگر نیز باشد پیغام دیگری مبنی بر اطمینان از حذف خود OU و زیرمجموعه های آن در کادر محاوره‌ای Confirm Subtree Deletion دریافت می‌کنید . کلید Yes را بزنید .

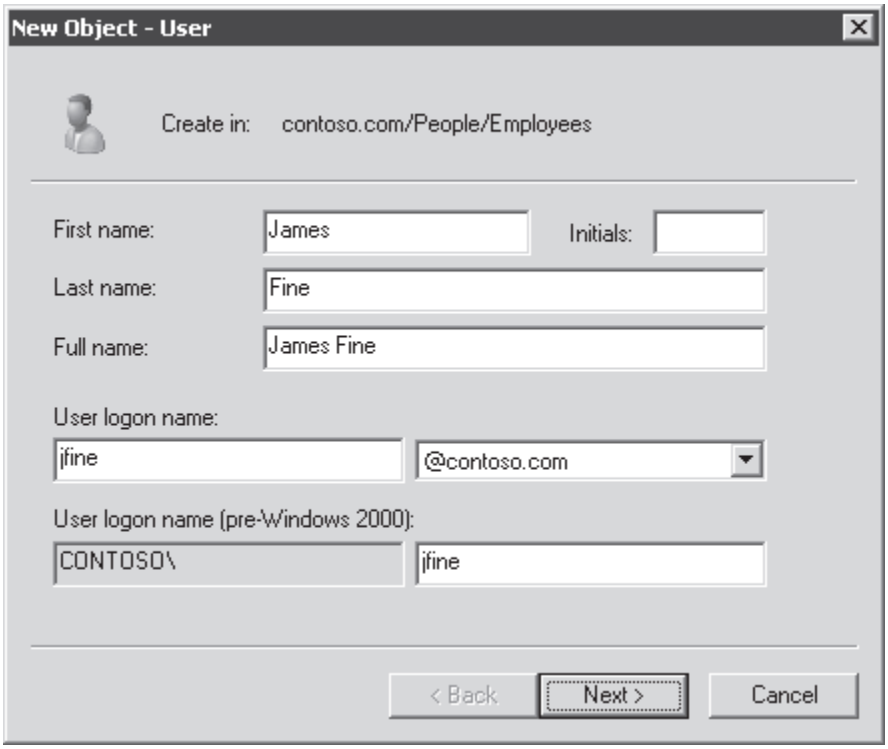
ساخت شیء کاربر

برای ساخت کاربر جدید در Active Directory مراحل زیر را انجام دهید . ضمناً قواعد نام‌گذاری و رویه‌های تعیین شده از سوی سازمان را رعایت کنید .

۱. Active Directory Users And Computer snap-in را باز کنید .

۲. در ساختار درختی کنسول گره مربوط به دامنه مورد نظر را باز کنید (بعنوان مثال contoso.com) و OU یا container ای را که حساب کاربری در آن ساخته می‌شود را پیدا کنید (مثلاً Users) .
۳. روی OU یا container گزینه New و بعد User را انتخاب کنید .
همانند شکل ۲-۵ کادر محاوره‌ای New Object-User پدیدار می‌شود .
۴. در کادر First Name نام کوچک کاربر را تایپ کنید .
۵. در کادر Initials نام middle کاربر را تایپ کنید .
۶. در کادر Last Name نام خانوادگی کاربر را تایپ کنید .

فیلد Full Name بطور اتوماتیک پر می‌شود در صورت نیاز آنرا تغییر دهید . فیلد Full Name برای ساخت صفات متعدد یک کاربر که نمونه بارز آن نام CN است و همچنین نمایش خصوصیت نام استفاده می‌شود . نام CN یک کاربر نامی است که درپنل وسط کنسول نمایش داده می‌شود . این نام در container یا OU باید منحصر بفرد باشد . بنابراین اگر کاربری را با نام مشابه کاربر موجود در همان container یا OU می‌سازید



باید اسمی منحصر بفرد را در فیلد Full Name وارد کنید .

شکل ۵- ۲ کادر محاوره‌ای New Object - User

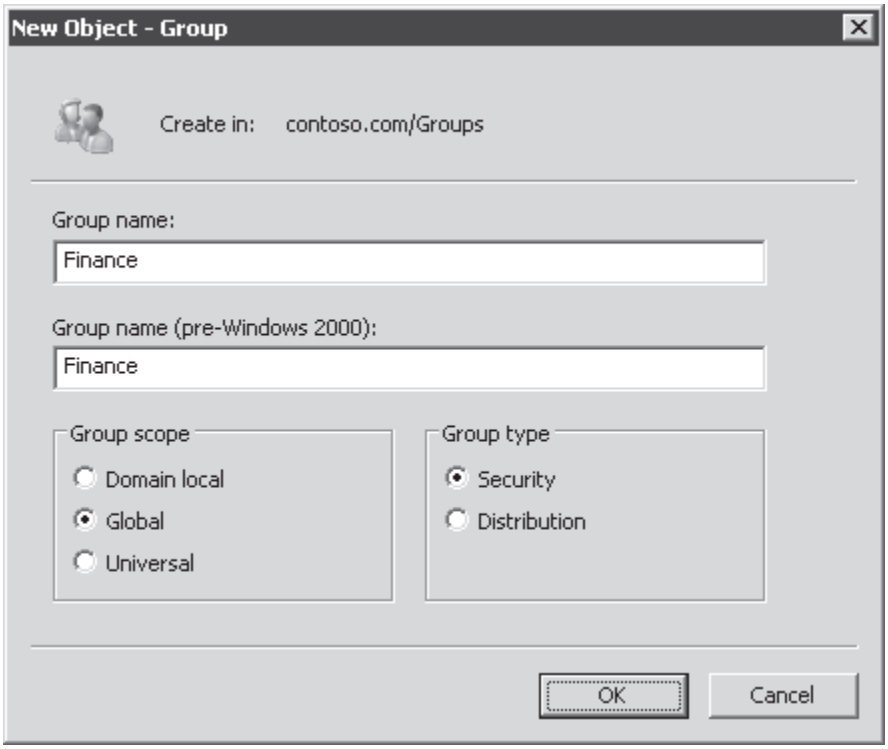
۷. در کادر User Logon Name نام کاربری را که جهت ورود به سیستم از آن استفاده می‌شود تایپ کنید و از لیست بازشو پسوند نام کامل کاربر (User Principle Name) یا UPN را انتخاب کنید که به نام کاربری همراه علامت @ اضافه خواهد شد . نام کاربری در Active Directory می‌تواند دارای بعضی کاراکترهای خاص باشد (مانند نقطه ، خط تیره و ') که امکان ثبت نامهای کاربری دقیق را مانند O'Hara و Smith-Bates می‌دهد . بهرحال نرم‌افزارهای خاصی ممکن است محدودیتهای دیگری داشته باشند بنابراین توصیه می شود از حروف استاندارد و اعداد استفاده شود مگر اینکه سازگاری نرم‌افزارهای سازمان با کاراکترهای خاص در نام کاربری اثبات شده باشد . لیست پسوندهای UPN موجود توسط ابزار Active Directory Domains And Trusts مدیریت می‌شود . روی ریشه snap-inActive Directory Domains And Trusts کلیک راست کنید و Properties را انتخاب کنید . سپس در زبانه UPN Suffixs پسوندها را حذف یا اضافه کنید . نام DNS دامنه Active Directory همیشه بعنوان پسوند وجود دارد و قابل پاک کردن نیست .
۸. در کادر User Logon Name (Pre-Windows 2000) نام کاربری قبل از ویندوز ۲۰۰۰ را وارد کنید که به آن اغلب نام کاربری سطح پایین نیز می‌گویند .
در فصل ۳ "کاربران" درباره تفاوتهای دو نوع نام کاربری بیشتر یاد می‌گیرید
۹. کلید Next را بزنید .

۱۰. یک کلمه عبور اولیه در کادرهای Password و Confirm Password برای کاربر وارد کنید .
۱۱. گزینه User Must Change Password At Next Logon را انتخاب کنید .
توصیه می‌شود همیشه این گزینه انتخاب گردد تا کاربر مجبورشود در اولین ورود کلمه عبورجدید بسازد و بدین ترتیب کارکنان بخش IT هم که برای کاربر نام کاربری و کلمه عبور ساخته‌اند از کلمه عبور جدید بی‌اطلاع خواهند بود . کارکنان پشتیبانی همیشه میتوانند کلمه عبور کاربر را تغییر داده و پس از ورود به سیستم به منابع کاربر دسترسی پیدا کنند . بهرجهت فقط خود کاربران باید کلمه عبور خود را بدانند .
۱۲. روی Next کلیک کنید .
۱۳. در صفحه آخر ورودی‌ها را چک کنید و روی finish کلیک کنید .
پنجره New Object – User امکان پیکربندی تعداد محدودی از خصلتهای حساب کاربری را مانند نام و کلمه عبور می‌دهد .در حالی که در Active Directory شیء کاربر امکان پیکربندی تعداد بیشتری از خصایص را امکانپذیر می‌کند .اینکار پس از ساخته شدن کاربر انجام می‌شود.
۱۴. روی شیء کاربر ساخته شده کلیک راست کرده و Properties را انتخاب کنید .
۱۵. خصوصیات کاربر را پیکربندی کنید .
از قوانین نام‌گذاری و دیگر استانداردهای سازمان پیروی کنید .درباره بسیاری از خصوصیات کاربر در فصل ۳ و ۸ "تایید هویت " بیشتر یاد می‌گیریم .
۱۶. روی OK کلیک کنید

ساخت شیء گروه

گروهها یک کلاس مهم ازاشیاءهستند زیرا کاربران ، کامپیوترها و گروههای دیگر را در بر می‌گیرند تا یک نقطه متمرکز مدیریتی ایجاد کنند . بیشترین استفاده از گروهها دادن مجوز به یک پوشه به اشتراک گذاشته شده می‌باشد . بعنوان مثال اگر به یک گروهی نسبت به یک پوشه دسترسی فقط خواندنی اعطا شود همه اعضاء گروه به آن پوشه دسترسی فقط خواندنی خواهند داشت . بنابراین نیاز نیست به تمامی اعضاء بطور جداگانه دسترسی بدهیم و براحتی با افزودن و حذف اعضاء به گروه دسترسی به پوشه را مدیریت می‌کنیم .
برای ساخت گروه :
۱. Active Directory Users And Computers snap-in را باز کنید .
۲. در ساختار درختی کنسول گره دامنه مورد نظر را باز کنید . (مثلاً contoso.com) و OU یا containerای را که گروه باید در آن ایجاد شود انتخاب کنید .
۳. روی container یا OU کلیک راست کرده و New ، سپس Group را انتخاب کنید .
۴. در کادر Group Name نام گروه جدید را تایپ کنید .
بسیاری از سازمانها قوانین نامگذاری خاصی دارند که باید رعایت شود .
بطور پیش فرض نامی که تایپ می‌شود بعنوان نام قبل از ویندوز 2000 هم درج می‌شود . اکیداً توصیه می‌شود نامها مشابه باشند .
۵. نام درج شده در کادر Group Nmae(Pre-Windows 2000) را دست نزنید .
۶. نوع گروه را انتخاب کنید .
   - گروه Security می‌تواند به منابع مجوز دسترسی داشته باشد . همچنین بعنوان لیست توزیع نامه‌های الکترونیکی استفاده شود .

گروه Distribution به منابع دسترسی ندارد ولی بعنوان لیست توزیع نامه‌ای الکترونیکی استفاده می‌شود .



شکل ۶- ۲ کادر محاوره‌ای New Object - Group

۷. حوزه گروه (Group Scope) را انتخاب کنید .

- گروه Global برای تعیین کاربرها بر اساس عملکرد شغلی ، محل و غیره بکار می‌رود
- گروه Domain Local برای در برگرفتن کاربران و گروههای دیگر که نیاز به دسترسی به منابع یکسان دارند استفاده می‌شود . بعنوان مثال همه کاربرانی که باید بتوانند گزارش کار یک پروژه را تغییر دهند در چنین گروهی قرار می‌گیرند .
- گروه Universal برای دربرگرفتن کاربران و گروههای دیگر از دامنه‌های مختلف استفاده می‌شود .

حوزه گروهها در فصل ۴ "گروهها" به تفصیل بررسی می‌شود .

توجه داشته باشید که اگر دامنه‌ای که گروه در آن ساخته می‌شود سطح عملیاتی Mixed یا Interim داشته باشد و گروه را از نوع Security تعیین کنید حوزه گروه را فقط می‌توان Domain Local یا Global انتخاب کرد . سطح عملیاتی دامنه در فصل ۱۳ "دامنه‌ها و Forests" بحث می شود .

۸. روی OK کلیک کنید .

اشیاء گروه ، خصوصیات مفیدی دارند که پس از ساخته شدن پیکربندی می‌شود .

۹. روی گروه کلیک راست کرده و Properties را انتخاب کنید .

۱۰. خصوصیات گروه را وارد کنید .

از قواعد نام‌گذاری و دیگر استانداردهای سازمان پیروی کنید .

زبانه‌های Members و Member Of گروه مشخص می‌کند به ترتیب چه کسانی به این گروه تعلق دارند و این گروه عضو چه گروه یا گروههای دیگری می‌باشد . عضویت گروهها در فصل ۴ بحث می‌شود .

با توجه به اینکه فیلد Description گروه در پنل وسط Active Directory Users And Computers snap-in نمایش داده می شود مکان خوبی برای درج هدف ساخت آن و آدرس شخص مسئول تعیین اعضاء گروه می‌باشد .

فیلد Notes گروه برای درج جزئیات بیشتر درباره گروه است .

زبانه Managed By برای مراجعه به کاربر یا کاربران مسئول گروه می‌باشد . تکمه Change را زیر کادر Name کلیک کنید . برای جستجوی یک گروه باید ابتدا روی تکمه Object Type کلیک کرده و Groups را انتخاب کنید . کادر محاوره‌ای Select User, Contact, Or Group در همین درس بررسی می‌شود .

باقی اطلاعات تماس در زبانه Managed By از اطلاعات حساب کاربری تعیین شده در کادر Name استخراج می‌شود . زبانه Managed By معمولاً اطلاعات تماس مسئول مدیریت گروه را مشخص می‌کند تا اگر کاربری درخواست عضویت در گروه را داشته

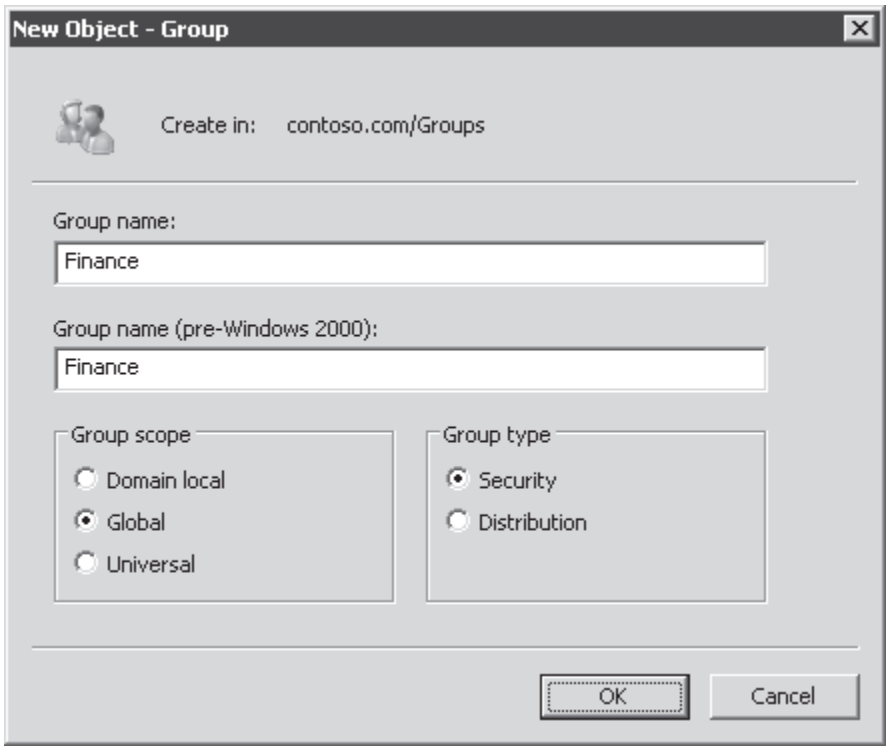
باشد بداند که باید با چه کسی تماس بگیرد . بهرحال اگر گزینه Manager Can Update Membership List را انتخاب کنید کاربر مشخص شده در کادر Name مجوز حذف و افزودن اعضاء به گروه را خواهد داشت . این یکی از روشهای واگذاری اختیار (Delegation) کنترل گروه می‌باشد . روشهای دیگر واگذاری اختیار در درس ۳ بحث می‌شود .

۱۱. روی OK کلیک کنید .

ساخت شیء کامپیوتر

کامپیوترها هم مانند کاربران در Active Directory یک حساب و شیء بحساب می‌آیند . در واقع کامپیوترها هم در پشت صحنه به دامنه وارد می‌شوند همانطور که کاربر وارد می‌شود . کامپیوتر نام کاربری دارد بدین صورت که نام کامپیوتر همراه علامت دلار نام کاربری آنرا تشکیل می‌دهد (مانند Desktop101$). و کلمه عبور آن در زمانی که کامپیوتر را عضو دامنه می‌کنیم (Join) ساخته می‌شود و هر سی روز یکبار یا بیشتر بطور اتوماتیک تغییر می‌کند . برای ساخت شیء کامپیوتر در Active Directory :

۱. Active Directory Users And Computers snap-in را باز کنید .
۲. در ساختار درختی کنسول گره دامنه مورد نظر را باز کنید . (مثلاً contoso.com) و OU یا containerای را که گروه باید در آن ایجاد شود انتخاب کنید (مثلاً Users) .
۳. روی container یا OU کلیک راست کرده و New ، سپس Computer را انتخاب کنید .
۴. در کادر Computer Name نام کامپیوتر جدید را تایپ کنید ..
بطور پیش فرض نامی که تایپ می‌شود در کادر Computer Name (Pre-Windows 2000) هم درج می‌شود .
۵. نام درج شده در کادر Computer Name(Pre-Windows 2000) را دست نزنید .
۶. حساب مشخص شده در فیلد User Or Group اجازه دارد کامپیوتر را عضو دامنه سازد . حساب پیش‌فرض Domain Admins می‌باشد .برای انتخاب کاربر یا گروه دیگر کلید Change را بزنید .
در اینجا عموماً گروهی انتخاب می‌شود که کار توزیع ویندوز یا پشتیبانی سیستم را انجام می‌دهد .همچنین کاربر صاحب کامپیوتر هم می‌تواند انتخاب شود . مباحث مربوط به join کامپیوتر به دامنه را در فصل ۵ "کامپیوترها" خواهید دید .
کادر Assign This Computer Account As A Pre-Windows 2000 Computer را انتخاب نکنید مگر اینکه حساب مربوط به کامپیوتر با سیستم عامل ویندوز NT 4.0 باشد .



شکل ۷- ۲ کادر محاوره‌ای New Object - Computer

۷. کلید OK را بزنید
اشیاء کامپیوتر ، خصوصیات مفیدی دارند که پس از ساخته شدن پیکربندی می‌شود .
۸. روی کامپیوتر کلیک راست کرده و Properties را انتخاب کنید .

۹. خصوصیات کامپیوتر را وارد کنید .

از قواعد نام‌گذاری و دیگر استانداردهای سازمان پیروی کنید .

فیلد Description کامپیوتر مشخص می‌کند که کامپیوتر به چه کسی منتسب است (بعنوان مثال واحد آموزش) یا اطلاعات توصیفی دیگر را ارائه می‌دهد .

با توجه به اینکه فیلد Description در پنل وسط Active Directory Users And Computers snap-in نمایش داده می شود مکان خوبی برای درج اطلاعات مفید درباره کامپیوتر می‌باشد .

خصوصیات متعددی وجود دارد که کامپیوتر را توصیف می‌کند . این خصوصیات شامل DNS Name ، DC Type ، Site ، Operating System Name ، Version و Service Pack می‌باشد .این خصوصیات زمانی کامپیوتر عضو دامنه می شود بطور اتوماتیک پر می شوند .

زبانه Managed By برای مراجعه به کاربر یا گروه مسئول کامپیوتر می‌باشد . تکمه Change را زیر کادر Name کلیک کنید . برای جستجوی یک گروه باید ابتدا روی تکمه Object Type کلیک کرده و Groups را انتخاب کنید . کادر محاوره‌ای Select User, Contact, Or Group در همین درس بررسی می‌شود . باقی اطلاعات تماس در زبانه Managed By از اطلاعات حساب کاربری تعیین شده در کادر Name استخراج می‌شود . در زبانه Managed By معمولاً اطلاعات تماس درج می‌شود . بعضی سازمانها از این زبانه برای تعیین تیم پشتیبانی مسئول کامپیوتر استفاده می‌کنند . بعضی دیگر اطلاعات کاربر کامپیوتر را وارد می‌کنند .

۱۰. روی OK کلیک کنید .

پیدا کردن اشیاء در Active Directory

تا حالا یاد گرفتیم که چطور اشیاء را در Active Directory بسازیم ولی اگر نتوانیم بخوبی به آن دسترسی پیدا کنیم هیچ فایده‌ای ندارد . بسیاری از مواقع مجبور هستیم اشیاء را در Active Directory پیدا کنیم . از جمله آنها به موارد زیر می‌توان اشاره کرد :

- اعطاء مجوز وقتی مجوزهای یک فایل یا پوشه را مشخص می‌کنید باید گروه یا کاربر گیرنده مجوز را انتخاب کنید .
- افزوده اعضاء به گروه اعضاء یک گروه از کاربران ، کامپیوترها ، گروههای دیگر یا ترکیبی از سه مورد مذکور تشکیل می شود . وقتی شیئی را بعنوان عضو گروه اضافه می‌کنیم باید شیء را انتخاب کنیم .
- ایجاد پیوند خصوصیات پیوندی (Linked Properties) خصوصیات یک شیء است که به شیء دیگر ارجاع می شود . در حقیقت عضویت گروهی یک خصوصیت پیوندی است .خصوصیات دیگر پیوندی مانند خصیصه Managed By که قبلاً بحث شد نیز از نوع پیوند می‌باشند . وقتی نام Managed By را تعیین می‌کنید باید کاربر یا گروه مورد نظر را انتخاب کنید .
- جستجوی شیء هر شیء را در دامنه Active Directory می‌توان جستجو کرد .

موقعیتهای متعدد دیگری نیز وجود دارند که مستلزم جستجوی Active Directory می‌باشند و در این ارتباط حتماً با رابطهای کاربری زیادی روبرو خواهید شد . در این قسمت با بعضی از تکنیکهای کار با آنها آشنا می‌شوید .

کنترل نحوه نمایش اشیاء در ابزار Active Directory Users And Computers

پنل وسط ابزار **Active Directory Users And Computers** را می‌توان به شکلی سفارشی کرد که امکان کار با اشیاء دایرکتوری را بطور موثرتری فراهم می‌کند . از دستور Add/Remove Columns از منوی View برای افزودن ستونهای دلخواه به پنل وسط استفاده می شود . هرچند همه خصلتها در پنجره نمایش داده نمی‌شود ولی تقریباً همه ستونهای پرکاربرد مانند User Logon Name یافت می‌شود . همچنین ستونهایی نیز وجود دارند که ممکن است به درد نخورند بعنوان مثال اگر OU فقط از یک نوع شیء تشکیل شده باشد (فقط کاربر یا فقط کامپیوتر) ستون Type بلااستفاده می‌ماند .

ترتیب ستونها را می‌توان با کشیدن سرتیتر آنها به سمت چپ و راست تغییر داد . همچنین نمای جزئیات از طریق کلیک کردن روی ستون مرتب می‌شود . درست مانند Windows Explorer کلیک اول منجر به ترتیب صعودی و کلیک دوم ترتیب نزولی می‌گردد . بهتر است ستون Last Name را به پنجره اضافه کنیم تا بتوانیم براساس آن پنجره را مرتب کنیم . بدلیل اینکه پیدا کردن کاربر توسط نام خانوادگی آن ساده‌تر از نام DN می‌باشد که معمولاً از مجموع نام کوچک و خانوادگی تشکیل می‌شود .

استفاده از پرس‌وجوهای ذخیره شده

ویندوز سرور 2003 گره Saved Queries را در ابزار Active Directory Users And Computers معرفی کرد . با این ابزار قدرتمند می‌توانیم دامنه را به شکلی که می‌خواهیم نمایش دهیم مثلاً اشیاء یک یا چند OU . برای ایجاد پرس و جوی ذخیره شده :

۱. ابزار Active Directory Users And Computers را باز می‌کنیم

پرس و جوهای ذخیره شده در ابزار Active Directory Users And Computers که بخشی از Server Manager باشد در

دسترس نخواهد بود . بنابراین باید از کنسول Active Directory Users And Computers یا یک کنسول سفارشی استفاده کرد

۲. روی Saved Queries کلیک راست کرده و گزینه New و سپس Query را انتخاب کنید
۳. برای پرس و جو اسمی انتخاب کنید
۴. در صورت نیاز توضیحات را در بخش Description وارد کنید .
۵. روی Browse کلیک کرده و محل ریشه پرس و جو را باز کنید

جستجو به دامنه یا OU که انتخاب کرده‌اید محدود می‌شود . پیشنهاد می‌شود جستجوی خود را تا حد امکان محدود کنید تا سرعت کار بالا رود .

۶. جهت تنظیم پرس و جو روی Define Query کلیک کنید
۷. در کادر محاوره‌ای Find Common Queries نوع شیء مورد نظر برای پرس و جو را انتخاب کنید

زبانه‌های موجود در کادر محاوره‌ای شامل تعدادی متغییر ورودی می‌باشند که با تغییر آنها پرس و جوی مناسب ساخته می‌شود .

۸. روی OK کلیک کنید .

پرس و جوی ساخته شده در ابزار Active Directory Users And Computers ذخیره می‌شود بنابراین وقتی کنسول را باز می‌کنید (dsa.msc) پرس و جو دفعه بعد که کنسول باز شود در دسترس خواهد بود . اگر پرس و جوی ذخیره شده در یک کنسول سفارشی ساخته شود در همان کنسول قابل دسترسی است . برای انتقال پرس و جوی ذخیره شده به کنسولها یا کاربران دیگر می‌توان پرس و جوی ذخیره شده را بعنوان فایل XML صادر(export) کرده و در مقصد به ابزار مورد نظر وارد (import) کرد

همانطور که پیشتر اشاره شد نحوه نمایش پرس و جوی ذخیره شده در پنل وسط با ستونها و مرتب سازی قابل سفارشی کردن است . نکته مهم پرسوجوهای ذخیره شده اینست که نحوه نمایش هرپرسوجوی ذخیره شده اختصاصی می‌باشد . وقتی ستونLast Name را به حالت نمایش نرمال یک OU اضافه می‌کنیم اینستون به نماهای همه OU ها اضافه می‌شود بنابراین یک ستون خالی حتی برای OU ها کامپیوترها گروهها اضافه می‌شود. باپرسوجوهای ذخیره شده می‌توانیم ستونLast Name را به یک پرسوجو برای اشیاء کاربر و ستونهای دیگر برای پرسوجوهای دیگر اضافه کنیم .

پرسوجوهای ذخیره شده روش قدرتمندی برای مجازی سازی دایرکتوری ومانیتورکردن مواردی مانند حسابهای قفل شده یا غیرفعال می‌باشد . یادگیری ساخت و مدیریت پرسوجوها به زحمتش می‌ارزد .

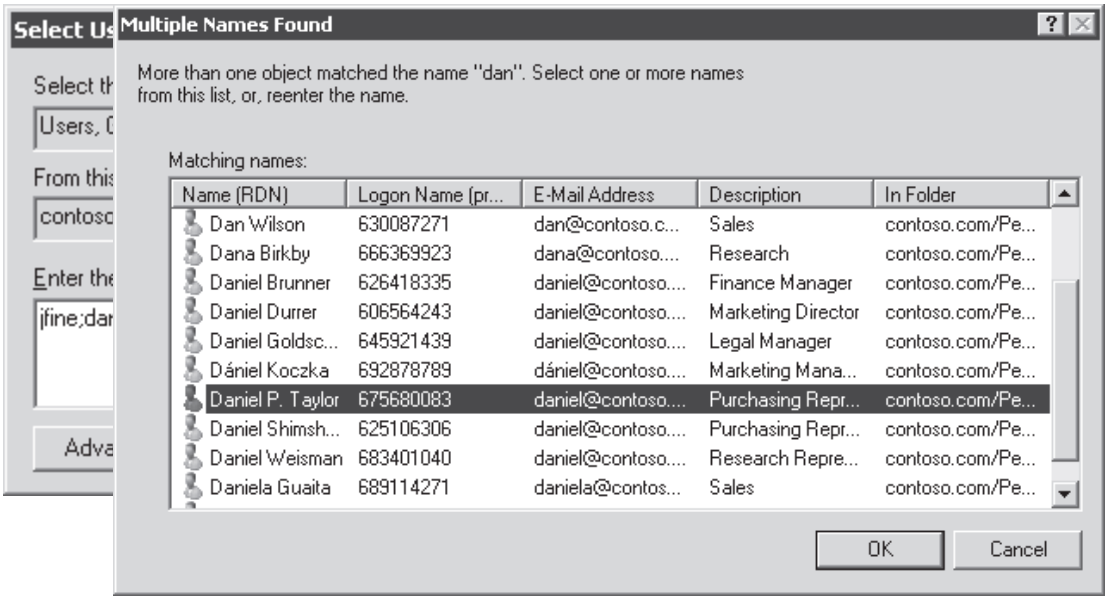
اطلاعات بیشتر پرسوجوهای ذخیره‌شده

سایت زیر برای دریافت جزئیات و مثالهای پرسوجوهای ذخیره‌شده اکیداً توصیه می‌شود .

http://www.petri.co.il/saved_queries_in_windows_2003_dsa.htm

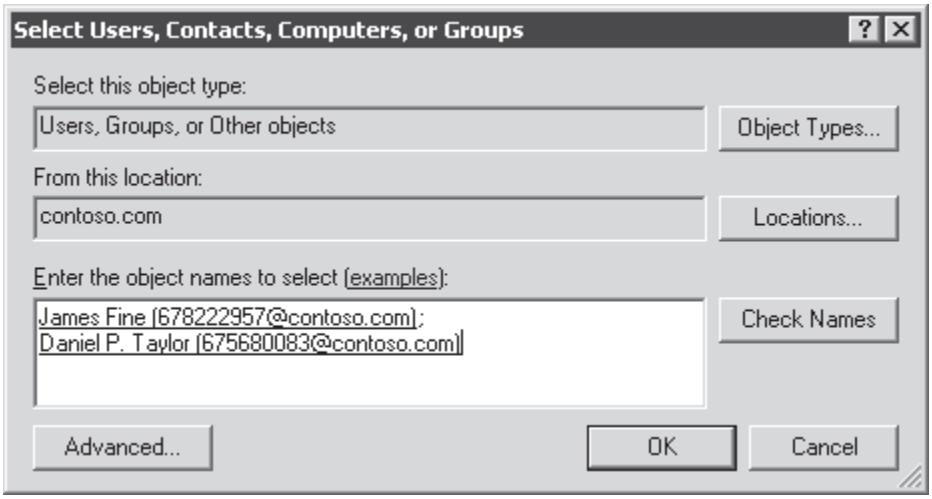
استفاده از کادر محاوره‌ای Select Users, Contacts, Computers, Or Groups

زمانیکه عضوی را به یک گروه اضافه می‌کنیم، مجوز اعطا می‌کنیم، یا یک خصیصه پیوندی می‌سازیم با کادر محاوره‌ای Select Users, Contacts, Computers, Or Groups در شکل ۲-۸ برخورد می‌کنیم. به این کادر محاوره‌ای از این به بعد در این کتاب کادر محاوره‌ای Select اطلاق می‌گردد . اگر مایل به دیدن یک مثال هستید Properties یک شیء گروه را باز کرده و زبانه Members را بزنید و سپس روی تکمه Add کلیک کنید .



شکل ۸- ۲ کادرمحاوره‌ایSelect Users, Contacts, Computers, Or Groups

اگرنام اشیاءرا می‌دانید مستقیماً می‌توانید آنرا در کادر متن Enter The Objects Names To Selectوارد کنید. اگرچندین نام مورد نظر باشد می‌توان همه آنها را با علامت جدا کننده نقطه ویرگول ";" همانند شکل ۲-۸ وارد کرد. وقتی روی OK کلیک می‌کنید ویندوز دنبال آیتمها در لیست می‌گردد و آنرا به یک پیوند به شیء مبدل می‌کند و کادر را می‌بندد . تکمه Check Names نیز نامها را به یک پیوند تبدیل می‌کند مانند شکل ۲-۹ ولی کادر را نمی‌بندد .



شکل ۹- ۲ نامهای مرتبط با لینکها با استفاده از دکمه Check Names

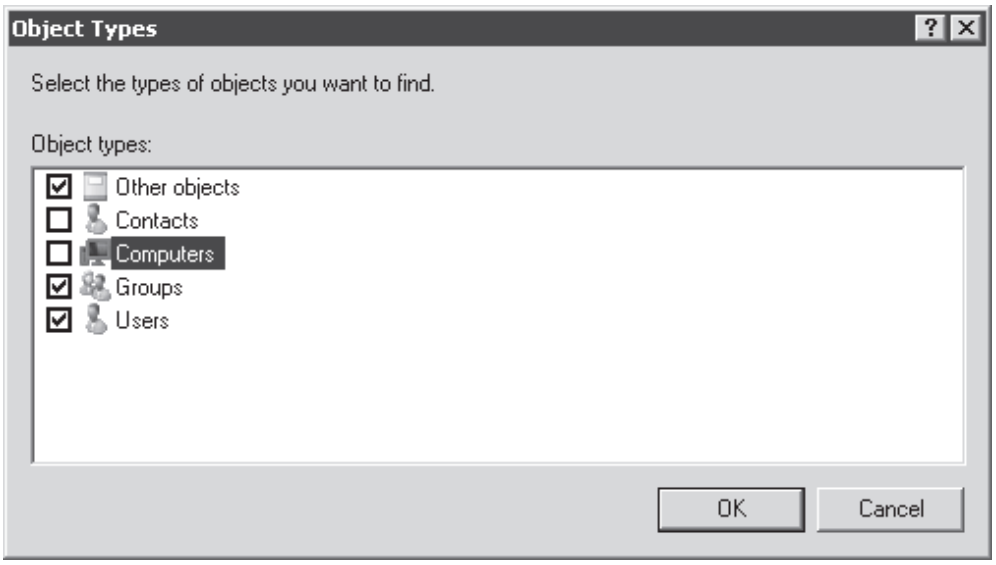
نیازی به ورود کامل نام شیء نیست و ورود قسمتی از نام هم ممکن است . مثلاً شکل ۲-۸ نامهای jfine و dan را نشان می‌دهد . وقتی روی OK یاCheck Names کلیک می‌کنید ویندوز نامهای ناقص درج شده را به نامهای صحیح تبدیل می‌کند. اگر نام ورودی فقط به یک شیء قابل تبدیل باشد مانند نام کاربری jfine، همانند شکل ۲-۹ مستقیماً تبدیل می‌شود. ولی اگر به چندین شیء قابل تبدیل باشد مانند Dan کادر Multiple Names Found همانند شکل ۲- ۱۰ ظاهر می‌شود. نامهای صحیح را انتخاب کرده و کلید OK را بزنید. نامهای انتخابی مانند شکل ۲- ۹ ظاهرمی‌شود.

شکل ۱۰- ۲ کادرمحاوره‌ایMultiple Names Found

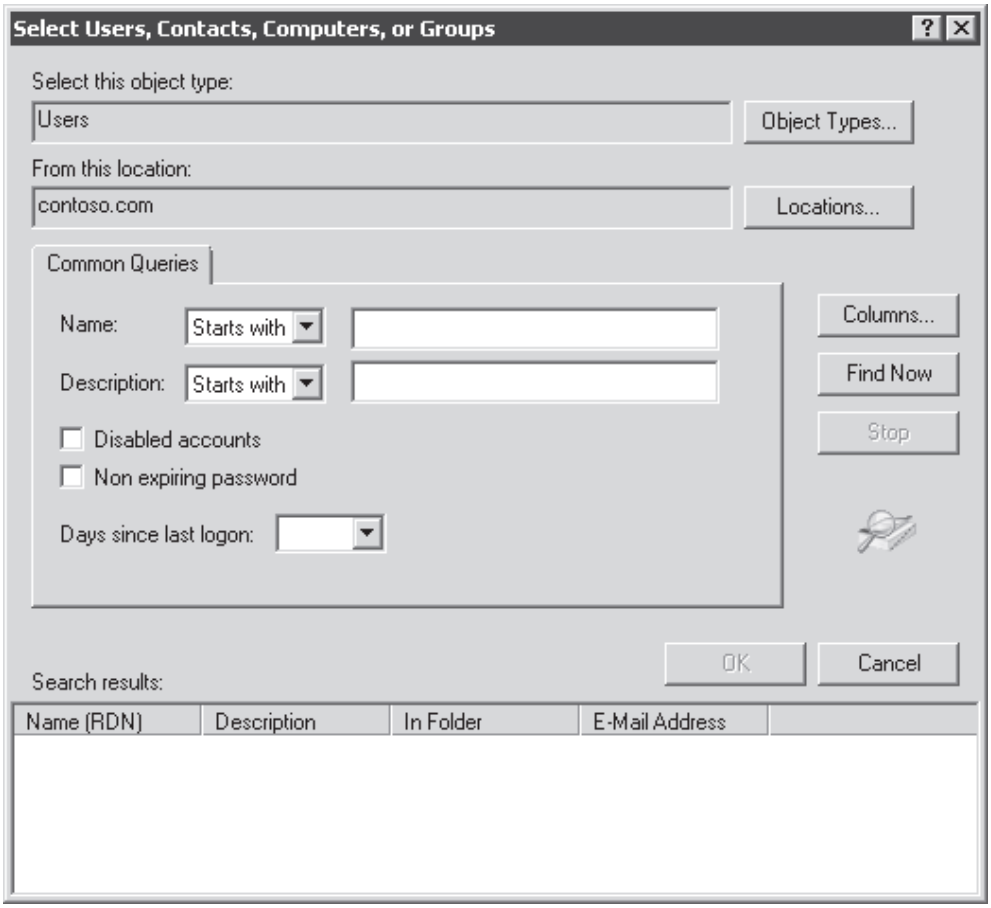
بطورپیش‌فرض کادر محاوره‌ای Select کل دامنه را جستجو می‌کند . اگر نتایج جستجو خیلی گسترده باشد یا نیاز به جستجوی دامنه‌های دیگر یا کاربران و گروههای محلی (Local) داشته باشیم تکمه Location را می‌زنیم .

بعلاوه کادر محاوره‌ای Select برخلاف نام کامل خود (Select Users, Contacts, Computers, Or Groups) بندرت همه چهارشیء را جستجو می‌کند . بعنوان مثال وقتی عضوی را به گروهی اضافه می‌کنیم، کامپیوترها بطور پیش‌فرض مورد جستجو قرار نمی‌گیرند. اگر نام کامپیوتری را وارد کنید به درستی تبدیل نمی‌گردد. وقتی نامی را در زبانه Managed By مشخص می‌کنید بصورت پیش فرض در گروهها جستجو انجام نمی‌گردد. به منظور جستجوی انواع اشیاء مورد نظر باید در کادر محاوره‌ای Select حوزه جستجو را مشخص کنیم. روی تکمه Object Types کلیک کرده و مانند شکل ۲- ۱۱ از کادر محاوره‌ایObjects Typesبرای انتخاب انواع صحیح اشیاء استفاده کرده و تکمه OK را کلیک کنیم .

اگربا محل‌یابی اشیاء مورد نظرتان مشکل دارید روی تکمه Advanced در کادر محاوره‌ای Select کلیک کنید. نمایش پیشرفته همانند شکل ۲- ۱۲ جستجوی فیلدهای نام و توضیحات را همچنین حسابهای غیرفعال، کلمات عبور بدون تاریخ انقضا و حسابهای بلااستفاده که در یک دوره زمانی کسی با آنها به سیستم وارد نشده امکانپذیر می‌کند. بعضی از فیلدهای زبانهCommon Queries بسته به نوع شیء مورد جستجو باید غیرفعال گردد. روی تکمه Object Types کلیک کرده و دقیقاً نوع شیء مورد نظر را مشخص کنید .



شکل ۱۱- ۲ کادرمحاوره‌ایObject Types

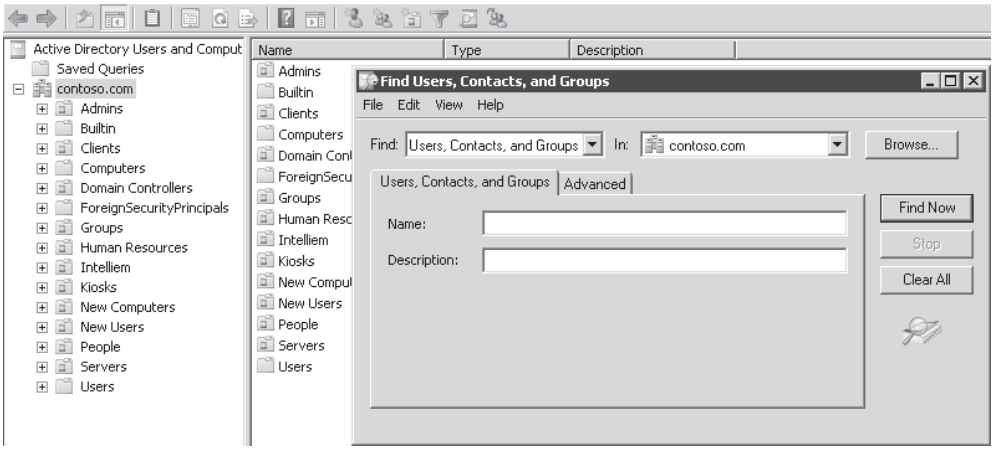


شکل ۱۲- ۲ نمایش کادر محاوره‌ایSelect

استفاده ازدستورFind

سیستمهای ویندوزی همچنین دارای ابزار پرسوجویActive Directory هستند که مدیران شبکه به آن کادر جستجو می‌گویند. یک روش بازکردن کادر جستجو کلیک روی تکمهFind Objects In Active Directory Domain Services در نوار ابزار Active Directory Users And Computers می‌باشد. تکمه مربوطه و کادر جستجو در شکل ۲- ۱۳ نمایش داده شده است .

ازلیست بازشوی Find جهت تعیین نوع یا انواع اشیاء موردنظر برای پرسوجو یا انتخاب پرسوجوهای متداول یا جستجوی سفارشی استفاده می‌شود . لیست بازشوی In حوزه جستجو را تعیین می‌کند. پیشنهاد می‌شود تا جایی که امکان دارد حوزه جستجو را کوچک کنید تا در شبکه‌های



گسترده از اتلاف وقت جلوگیری شود. لیست‌های Find و In با هم حوزه جستجو را مشخص می‌کنند.

شکل ۱۳- ۲ کادرFind

سپس معیارهای جستجو را مشخص می‌کنیم . بسته به نوع پرسوجویی که اجرا می‌کنیم فیلدهای پرکاربرد به عنوان معیارهای جستجو در پنجره ظاهر می‌شوند. برای کنترل پیشرفته و کامل پرسوجو از لیست بازشوی Find گزینه Custom Search را انتخاب کنید. اگر این گزینه را انتخاب کرده و روی زبانه Advanced کلیک کنید می‌توانید پرسوجوهای قدرتمند LDAP بسازید. بطورمثال پرسوجوی " OU=*main* " همه OU ها که حروف "main" را در نام خود دارد جستجو کرده و نتیجه رانشان می‌دهد. یکی از نتایج این پرسوجو OUDomain controllers خواهد بود چرا که حروف "main" در واژه Domain موجود است. بدون استفاده از جستجوی سفارشی، عبارت مورد جستجو حتماً باید قسمتی از ابتدای نام شیء را شامل شود درحالی که با جستجوی سفارشی امکان جستجو براساس قسمتهای ابتدایی وسط یا انتهایی شیء با استفاده از کاراکترهای جایگزین (wildcard) امکانپذیر است .

وقتی حوزه و معیارهای جستجو را مشخص کردیم روی Find Now کلیک می‌کنیم تا نتیجه را ببینیم. بعد می‌توانیم روی هر مورد از نتایج کلیک راست کرده و فرمانهایی نظیر Move، Delete و Properties را اجرا کنیم.

کادر جستجو در محلهای دیگری از ویندوز نیز به نمایش در می‌آید که نمونه آن Add Printer Wizard هنگام پیدا کردن پرینترهای شبکه است. پوشه به اشتراک گذاشته شده نیز دکمه Search Active Directory دارد. جهت سهولت بیشتر جستجو می‌توان یک میانبر در منوی استارت یا روی دسک‌تاپ ساخت. مقصد میانبر باید rundll dsquery یا OpenQueryWindow باشد.

پیداکردن اشیاء با استفاده از Dsquery

ویندوز دارای ابزارهای خط فرمانی است که عملکردی شبیه ابزارهای گرافیکی مانند ابزار Active Directory Users And Computers دارند بسیاری از این دستورات با حروف "DS" شروع می‌شود بنابراین به آنها دستورات DS نیز اطلاق می‌شود. دستور Dsquery مانند بقیه دستورات DS به قدر کافی اطلاعات راهنما دارد. دستور dsquery.exe /? را تایپ کنید تا ساختار و کاربرد آنرا ببینید. بیشتر دستورات DS به همراه شیئی بکار می‌رود که هدف دستور است. مثلاً با تایپ دستورات dsquery user،dsquery computer،dsquery group و dsquery ou به ترتیب کاربر، کامپیوتر، گروه و OU را جستجو می‌کند. بدنبال مشخصه نوع شیء می‌توان از سوئیچ‌هایی با هدف تعیین معیارهای پرسوجو استفاده کرد . هر شیئی توسط نامش قابل محل‌یابی است مثل سوئیچ name– . بیشتر اشیاء براساس خصیصه description قابل جستجو هستند (desc-). واحدهای امنیتی بر اساس نامهای قبل از ویندوز ۲۰۰۰ (samid-) قابل جستجو هستند . برای پیدا کردن اینکه کدام خصیصه می‌تواند مبنای جستجو باشد فرمان dsquery objecttype /?را تایپ کنید .

بعنوان مثال اگربخواهیم همه کاربرانی را که نامشان با "jam" شروع می‌شودپیدا کنیم باید دستور dsquery user –name jam* را وارد کنیم . بعد از سوئیچ خصیصه که در این مثال name بود معیار جستجو وارد می‌شود که حساس به بزرگ یا کوچک بودن حروف نیست وشامل کاراکترهای جایگزین مانند ستاره "*" می‌شود که جایگزین ۰ تاچندکاراکتراست. .. دستور dsquery بطور پیش‌فرض اشیاء یافت شده رامانند شکل ۲- ۱۴ باDN نمایش می‌دهد .

```
c:\>dsquery user -name jam*
"CN=James D. Kramer,OU=Employees,OU=People,DC=contoso,DC=com"
"CN=James Fine,OU=People,DC=contoso,DC=com"
"CN=James Hendergart,OU=Employees,OU=People,DC=contoso,DC=com"
"CN=James R. Hamilton,OU=Employees,OU=People,DC=contoso,DC=com"
"CN=James van Eaton,OU=Employees,OU=People,DC=contoso,DC=com"
"CN=Jamie Reding,OU=Employees,OU=People,DC=contoso,DC=com"
```

شکل ۲-۱۴ دستور Dsquery

اگر مایل نیستید نتایج را بصورت DN ببینید سوئیچ o– را به فرمان اضافه کنید . بعنوان مثال با اضافه کردن عبارت – o samid نتایج جستجو با نامهای قبل از ویندوز ۲۰۰۰ برگردانده می‌شود و اگر o upn– اضافه شود لیست نتایج با نامهای کاربری نمایش داده می‌شود .

مفاهیمDN،RDNوCN

DN نوعی مسیر رسیدن به یک شیء در Active Directory می‌باشد. هر شیء درActive Directory یک DN کاملاً انحصاری دارد. DN کاربر James Fine مساوی است باCN=James Fine,OU=People,DC=contoso,DC=com

DN مسیری است که با شیء شروع و به دامنه top-level در فضای اسمی DNS ختم می‌شود. همان‌طوری که گفته شد CN مخفف common name می‌باشد و وقتی کاربری ساخته می‌شود کادر Full Name برای ساخت CN شیء کاربر استفاده می‌شود. OU مشخص‌کننده OU است و DC به معنی اجزاء دامنه می‌باشد.

بخشی از DN که قبل از اولین OU یا container قرار می‌گیرد relative distinguished name (RDN) گویند در مثال فوق RDN می‌شود CN=James Fine. همیشه RDN از CN تشکیل نمی‌شود. DNOUPeople مساوی است با OU=People,DC=contoso,DC=com و RDN آن نیز می‌شود OU=People.

بدلیل اینکه DN یک شیء باید در سرویس دایرکتوری منحصر باشد RDN یک شیء باید در container خود منحصر باشد. به همین دلیل است که اگر کاربری همنام در یک OU موجود باشد به یکی از آنها باید CN متفاوت بدهیم. منطق مشابه آن در فایلهای یک پوشه هم صدق می‌کند : ما نمی‌توانیم دو فایل همنام در یک پوشه داشته باشیم.

ما در حین کار با Active Directory بطور مرتب با DNs سرو کارخواهیم داشت. درست مانند وقتی که با فایلها و پوشه‌ها کار می‌کنیم با مسیر فایل سروکارداریم. توانایی خواندن و تفسیر آنها الزامی است.

تمرینات ساخت و پیدا کردن اشیاء در Active Directory

در این تمرین در Active Directory شیء می‌سازیم و سپس آنرا جستجو می‌کنیم. اشیائی که می‌سازیم شامل OU، کاربر، گروه و کامپیوتر است. سپس پرس و جوی ذخیره شده ساخته و نمایش آنرا سفارشی می‌کنیم. اشیایی که در این تمرین ساخته می‌شود در تمرینات فصل‌های بعد استفاده می‌شود.

تمرین ۱ ساخت OU

Users and Computers container های پیش‌فرض به منظور سهولت کار با Actvie Directory توسط ویندوز ایجاد می‌شوند. پیشنهاد می‌گردد OU های مورد نیاز خود را با احتساب مدل مدیریتی سازمان بسازیم. در این تمرین قرار است OU هایی برای دامنه فرضی contoso.com بسازیم. این OU ها در تمرینات فصول بعدی مورد استفاده قرار می‌گیرند.

۱. با کاربر Administrator به SERVER01 وارد می‌شویم.
۲. ابزار Active Directory Users And Computers را باز می‌کنیم.
۳. گره Domain را باز می‌کنیم.
۴. روی گره Domian کلیک راست کرده و New و بعد Organizational Unit را انتخاب می‌کنیم.
۵. نام OU را People وارد می‌کنیم.
۶. گزینه Protect Container From Accidental Deletion را انتخاب می‌کنیم.
۷. روی OK کلیک می‌کنیم.
۸. روی OU کلیک راست کرده و Properties را انتخاب می‌کنیم.
۹. در فیلد Description عبارت Non-administrative user identities را تایپ می‌کنیم.
۱۰. روی OK کلیک می‌کنیم.
۱۱. مراحل ۲ تا ۱۰ را برای ساخت OU های زیر تکرار می‌کنیم.

نام OU	توضیحات OU
Clients	Client computers
Groups	Non-administrative groups
Admins	Administrative identities and groups
Servers	Servers

تمرین ۲ ساخت کاربر

حالا که OU مورد نظرمان را ساختیم نوبت به ساخت اشیاء کاربر در آنها می‌رسد.

۱. با کاربر Administrator به Server01 وارد شده و ابزار Active Directory Users And Computers را باز می‌کنیم.
۲. مراحل بخش "ساخت شیء کاربر " را در متن درس برای ساخت کاربران زیر در People OU به کار می‌گیریم. برای کاربران کلمات عبور پیچیده در نظر می‌گیریم.
۳. در ساختار درختی کنسول گره Domain را باز کرده (contoso.com) و People OU را انتخاب می‌کنیم.

۴. روی People OU کلیک راست کرده و New و بعد User را انتخاب می‌کنیم.
۵. در کادر First Name نام کاربر را Dan وارد می‌کنیم.
۶. در کادر Last Name نام فامیل کاربر را Holme وارد می‌کنیم.
۷. در کادر User Logon Name نام کاربری را dholme وارد می‌کنیم.
۸. در کادر User Logon Name (Pre-Windows 2000) عبارت dholme را وارد می‌کنیم.
۹. روی Next کلیک می‌کنیم.
۱۰. کلمه عبور را در کادرهای بعدی وارد می‌کنیم.
۱۱. کادر User Must Change Password At Next Logon را علامت می‌زنیم.
۱۲. روی Next کلیک می‌کنیم.
۱۳. صفحه خلاصه را مرور کرده و روی Finish کلیک می‌کنیم.
۱۴. روی شیء کاربر که ساختیم کلیک راست کرده و Properties را انتخاب می‌کنیم.
۱۵. خصیصه‌هایی که در کادر محاوره‌ای Properties پیکربندی کردیم بررسی می‌کنیم. هیچ خصوصیتی را اینجا تغییر نمی‌دهیم.
۱۶. روی OK کلیک می‌کنیم.
۱۷. مراحل ۳ تا ۱۲ را تکرار کرده و کاربران زیر را در People OU می‌سازیم.

- James Fine
  - First name: James
  - Last name: Fine
  - Full name: James Fine
  - User logon name: jfine
- Barbara Mayer
  - First name: Barbara
  - Last name: Mayer
  - Full name: Barbara Mayer
  - User logon name: bmayer
  - Pre-Windows 2000 logon name: bmayer
- Barbara Moreland
  - First name: Barbara
  - Last name: Moreland
  - Full name: Barbara Moreland
  - User logon name: bmoreland
  - Pre-Windows 2000 logon name: bmoreland

۱۸. مراحل ۳ تا ۱۲ را تکرار کرده و در همان People OU یک نام کاربری برای خود می‌سازیم. کلمه عبور پیچیده نیز برای حساب خود در نظر می‌گیریم.
۱۹. مراحل ۳ تا ۱۲ را تکرار می‌کنیم و در Admins OU یک حساب کاربری برای خود می‌سازیم. این حساب دارای اختیارات مدیریتی خواهد بود. در نام کاربری یک پسوند admin_ در نظر می‌گیریم که با نام کاربری قبلی خود اشتباه نشود.

تمرین ۳ ساخت کامپیوتر

اشیاء کامپیوتر بهتر است قبل از join کامپیوتر به دامنه ساخته شوند. در این تمرین اشیاء کامپیوتر متعددی در OU های ساخته شده در تمرین ۱ ایجاد شوند. این اشیاء کامپیوتر در تمرینات بعدی استفاده خواهد شد.

۱. با کاربر Administrator به Server01 وارد شده و ابزار Active Directory Users And Computers را باز می‌کنیم.
۲. در ساختار درختی کنسول گره Domain را باز کرده (contoso.com) و Servers OU را انتخاب می‌کنیم.
۳. روی Servers OU کلیک راست کرده و New و بعد Computer را انتخاب می‌کنیم.
۴. در کادر Computer Name نام کامپیوتر را FILESERVER01 تایپ می‌کنیم.
۵. کادر Computer Name (Pre-Windows 2000) را تغییر نمی‌دهیم.
۶. از حساب مشخص شده در کادر متنی User Or Group Field یادداشت برمی‌داریم. مقدار آنرا در اینجا تغییر نمی‌دهیم.
۷. روی OK کلیک می‌کنیم.
۸. روی کامپیوتر کلیک راست کرده و Properties را انتخاب می‌کنیم.
۹. خصوصیات کامپیوتر را بررسی می‌کنیم.
۱۰. روی OK کلیک می‌کنیم.
۱۱. مراحل ۳ تا ۸ را برای ساخت اشیاء کامپیوتر برای کامپیوترهای زیر تکرار می کنیم.
- SHAREPOINT02
- EXCHANGE03

۱۲. مراحل ۳ تا ۸ را برای ساخت کامپیوترهای زیر در Clients OU تکرار می‌کنیم.
- DESKTOP101
- DESKTOP102
- LAPTOP103

تمرین ۴ ساخت گروه

مدیریت اشیاء در گروهها بهتر از مدیریت تک تک آنهاست. در این تمرین گروههای متعددی در دو OU قبلی ایجاد می‌شود.

۱. با کاربر Administrator به Server01 وارد شده و ابزار Active Directory Users And Computers را باز می‌کنیم.
۲. در ساختار درختی کنسول گره Domain را باز کرده (contoso.com) و Groups OU را انتخاب می‌کنیم.
۳. روی Groups OU کلیک راست کرده و New و بعد Group را انتخاب می‌کنیم.
۴. در کادر Group Name نام گروه را Finance تایپ می‌کنیم.
۵. Group Type را Security انتخاب می‌کنیم.
۶. Group Scope را Global انتخاب می‌کنیم.
۷. روی OK کلیک می‌کنیم.
۸. روی گروه کلیک راست کرده و Properties را انتخاب می‌کنیم.
۹. خصوصیات گروه را بررسی می‌کنیم. هیچ تغییری در آنها ایجاد نمی‌کنیم.
۱۰. روی OK کلیک می‌کنیم.
۱۱. مراحل ۳ تا ۸ را برای ساخت گروههای امنیتی global در Groups OU ادامه می‌دهیم:
    - Finance Managers
    - Sales
    - APP_Office 2007
۱۲. مراحل ۳ تا ۸ را برای ساخت گروههای امنیتی global در Admins OU ادامه می‌دهیم:
    - Help Desk

- Windows Administrators

تمرین ۵ افزودن کاربران و کامپیوترها به گروهها

حالا که گروههای مورد نظر خود را ساختیم اشیاء و اعضاء را می‌توانیم به آنها اضافه کنیم. در این تمرین کاربران و کامپیوترها را به گروهها اضافه می‌کنیم. در طول تمرین با کادر محاوره‌ای Select آشنا خواهیم شد.

۱. با کاربر Administrator به Server01 وارد شده و ابزار Active Directory Users And Computers را باز می‌کنیم.
۲. پنجره Properties حساب کاربری خود را در Admins OU باز می‌کنیم.
۳. زبانه Member Of را باز می‌کنیم.
۴. روی دکمه Add کلیک می‌کنیم.
۵. در کادر محاوره‌ای Select Groups نام Domain Admins را تایپ می‌کنیم.
۶. روی OK کلیک می‌کنیم.
۷. دوباره روی OK کلیک می‌کنیم تا پنجره بسته شود.
۸. پنجره Properties گروه Help Desk را در Admins OU باز می‌کنیم.
۹. زبانه Members را باز می‌کنیم.
۱۰. روی دکمه Add کلیک می‌کنیم.
۱۱. در کادر محاوره‌ای Select عبارت Barb را تایپ می‌کنیم.
۱۲. روی Check Names کلیک می‌کنیم.
۱۳. Barbara Mayer را انتخاب کرده و روی OK کلیک می‌کنیم.
۱۴. روی OK کلیک کرده تا کادر بسته شود.
۱۵. روی OK کلیک کرده تا پنجره بسته شود.
۱۶. پنجره Properties گروه APP_Office 2007 را در Groups OU باز می‌کنیم.
۱۷. زبانه Members را باز می‌کنیم.
۱۸. روی دکمه Add کلیک می‌کنیم.
۱۹. در کادر محاوره‌ای Select عبارت DESKTOP101 را تایپ می‌کنیم.
۲۰. روی Check Names کلیک می‌کنیم.
۲۱. روی Cancel کلیک می‌کنیم تا کادر Name Not Found بسته شود.
۲۲. در کادر Select روی Object Types کلیک می‌کنیم.
۲۳. Computers را به عنوان یک نوع شیء انتخاب کرده و روی OK کلیک می‌کنیم.
۲۴. روی Check Names کلیک می‌کنیم.
۲۵. روی OK کلیک می‌کنیم.

تمرین ۶ پیدا کردن اشیاء در Active Directory

وقتی به دنبال اشیاء در سرویس دایرکتوری دامنه می‌گردیم معمولا جستجو از کارایی بالاتری نسبت به مرور تک به تک ساختار برخوردار است. در این تمرین از سه رابط برای جستجو استفاده می‌کنیم.

۱. با کاربر Administrator به Server01 وارد شده و ابزار Active Directory Users And Computers را باز می‌کنیم.
۲. روی دکمه Find Objects In Active Directory Domain Services کلیک می‌کنیم.
۳. بررسی می‌کنیم که لیست بازشوی In عبارت contoso.com را نشان می‌دهد.
۴. در کادر Name عبارت Barb را تایپ می‌کنیم.
۵. روی Find Now کلیک می‌کنیم.
۶. دو کاربر با نام‌های Barbara باید در نتیجه جستجو ظاهر شود.
۷. کادر را می‌بندیم.
۸. از منوی استارت Network را باز می‌کنیم.
۹. روی Search Active Directory کلیک می‌کنیم.
۱۰. مراحل ۳ تا ۷ را تکرار می‌کنیم.
۱۱. در ابزار Active Directory Users And Computers روی گره Saved Queries کلیک راست کرده و New و بعد Query را انتخاب می‌کنیم.
۱۲. در کادر Name عبارت All Users را تایپ می‌کنیم.
۱۳. در کادر Description عبارت Users for the entire domain را تایپ می‌کنیم.
۱۴. روی Define Query کلیک می‌کنیم.
۱۵. در زبانه Users در کادر Name عبارت Has A Value را انتخاب می کنیم.
۱۶. دو بار روی OK کلیک می‌کنیم تا کادرها بسته شوند.
۱۷. View را انتخاب کرده و روی Add/Remove Columns کلیک می‌کنیم.
۱۸. در لیست ستونهای Available ، Last Name را انتخاب کرده و روی دکمه Add کلیک می‌کنیم.
۱۹. در لیست ستونهای Displayed ، Type را انتخاب کرده و روی دکمه Remove کلیک می‌کنیم.
۲۰. روی OK کلیک می‌کنیم.
۲۱. سرستون Last Name را طوری می‌کشیم که بین Name و Description قرار گیرد.
۲۲. روی سرستون Last Name کلیک می‌کنیم تا کاربران به صورت الفبایی مرتب شوند.

خلاصه درس

- OU ها container های مدیریتی هستند که اشیاء همسان از نظر نیازمندی مدیریتی و پیکربندی را در بر می‌گیرند. این راهی برای دسترسی و مدیریت مجموعه کاربران، گروهها، کامپیوترها و دیگر اشیاء می‌باشد. به OU نمی‌توانیم مجوز دسترسی به منابعی مانند پوشه اشتراکی بدهیم.
- وقتی اشیائی نظیر کاربر، کامپیوتر یا گروه می‌سازیم قادر خواهیم بود فقط برخی از خصوصیات آنرا هنگام ساخت پیکربندی کنیم. پس از ساخت در پنجره Properties شیء می‌توانیم خصیصه‌های دیگر را نیز پیکربندی کنیم.
- خصوصیات شیء مانند Description، Managed By و Notes می‌تواند برای مستندسازی اطلاعات مهم شیء به کار رود.

- به طور پیش فرض OU در وضعیت محافظت شده ساخته می‌شود. برای غیرفعال کردن حفاظت باید از منوی View گزینه Advanced Features را روشن کنیم. سپس در پنجره Properties یک OU زبانه Object را باز کرده و محافظت را غیر فعال می‌کنیم.

سئوالات پایان درس

۱. فرض کنید پنجره خط فرمان را به صورت elevated باز کرده‌ایم. از دستور Dsrm به منظور حذف یک OU که به طور اتفاقی توسط یکی از مدیران شبکه با نام James ساخته شده استفاده می‌کنیم. جواب این است Dsrm Failed: Access Is Denied. علت خطا چیست؟

A. باید پنجره خط فرمان را با کاربر عضو گروه Administrators باز کنیم.

B. فقط گروه Administrators می‌تواند OU را حذف کند.

C. فقط مالک (owner) آن می‌تواند آنرا حذف کند.

D. OU از نظر حذف حفاظت شده است.

درس ۳: تفویض اختیار (Delegation) و امنیت اشیاء Active Directory

در دروس پیشین این فصل یاد گرفتیم که چگونه کاربر، گروه، کامپیوتر و OU بسازیم و چطور به خصوصیات آنها دسترسی پیدا کنیم. توانایی ما در اجرای این عملیات بستگی به عضویت ما در گروه Administrators دامنه داشت. برای انجام وظایفی مانند تغییر کلمه عبور کاربران و یا باز کردن قفل حسابهای کاربری نیازی نیست افراد تیم پشتیبانی را به گروه Administrators دامنه اضافه کنیم. بجای آن بهتر است به اعضاء تیم پشتیبانی بر حسب وظیفه‌ای که دارند دسترسی بدهیم و نه بیشتر. در این درس یاد می‌گیریم چگونه وظایف مدیریتی خاصی را واگذار کنیم . این مهم با تغییر لیست کنترل دسترسی (ACL) اشیاءActive Directory محقق می‌شود .

بعد از این درس شما می‌توانید :

- اهداف اجرایی واگذاری اختیار راشرح دهید
- نسبت به اشیاءActive Directory توسط رابطهای کاربری ویرایشگر امنیت و ویزارد واگذاری اختیار مجوز اعطا کنید.
- با استفاده از ابزارهای خط فرمان و رابط کاربری، مجوزهای اشیاءActive Directory را مشاهده کرده و از آنها گزارش تهیه کنید
- مجوزهای نهایی (effective) را برای کاربر یا گروه ارزیابی کنید
- مجوزهای یک شیء را به حالت اولیه خودش برگردانید
- رابطه بین واگذاری اختیار و طراحی OU ها را توصیف کنید

زمان : ۳۵ دقیقه

مفهوم تفویض اختیار

در بیشتر سازمانها بیش از یک مدیر شبکه وجود دارد و همزما ن با رشد سازمان وظایف مدیریتی شبکه بین مدیران مختلف شبکه یا واحدهای پشتیبانی توزیع می‌شود. بعنوان مثال در بسیاری از سازمانها نیروهای پشتیبان شبکه قادرند کلمه عبور کاربران را تغییر دهند و حساب کاربرانی را که قفل شده باز کنند. این توانایی نیروهای پشتیبانی نمونه واگذاری اختیار وظایف مدیریتی می‌باشد. آنها معمولاً نمی‌توانند کاربر جدید بسازند فقط می‌توانند تغییرات خاصی روی حسابهای کاربری موجود ایجاد کنند.

همه اشیاء Active Directory مانند کاربران، کامپیوترها و گروهها که در درس قبلی ساختید توسط لیستی از مجوزها می‌توانند ایمن گردند بنابراین می‌توانید به اعضاء گروه پشتیبانی مجوز تغییرکلمه عبور را نسبت به اشیاء کاربر اعطا کنید. مجوزهای اعطاشده نسبت به یک شیء را

access control entries (ACEs)می‌گویند و به کاربران، گروهها یا کامپیوترها (واحدهای امنیتی) اعطا می‌شوند. ACE ها در لیستی بنام discretionary access control list (DACL) مربوط به یک شیء ذخیره می‌شوند. DACL بخشی از ACL یک شیء است که شامل لیست کنترل دسترسی سیستم (SACL) نیزمی‌شود که دربرگیرنده تنظیمات ممیزی (Auditing) است . اگر مجوزهای فایل و پوشه را مطالعه کرده باشید متوجه می‌شوید واژه‌ها و مفهوم بکار رفته در آنجا با مبحث فعلی یکسان است.

واگذاری اختیار کنترل مدیریتی یا اختصاراً واگذاری اختیار یعنی اعطاء مجوزهایی که با آن می‌توان دسترسی به اشیاء و خصوصیات را در Active Directory مدیریت کرد. درست مانند زمانی که به گروهی امکان تغییر فایلها را در پوشه می‌دهیم می‌توانیم به یک گروه توانایی تغییرکلمه عبور اشیاء کاربر را بدهیم.

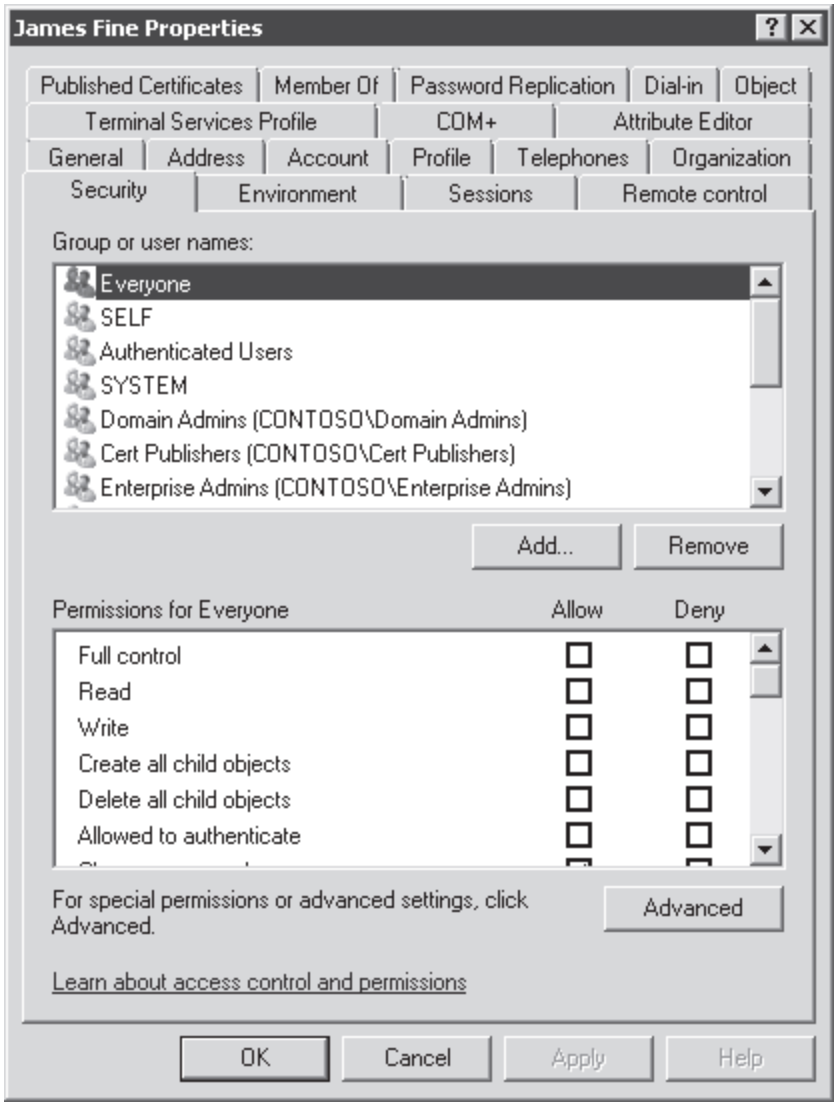
مشاهده ACL یک شیء در Active Directory

ACL یک شیء کاربر در Active Directory در پایین‌ترین سطح قرار دارد. برای مشاهده ACL یک شیء :

۱. ابزار Active Directory Users And Computers را باز کنید
۲. گزینه Advanced Features را از منوی View انتخاب کنید
۳. روی شیء مورد نظر کلیک راست کرده و Properties را انتخاب کنید
۴. زبانه Security را کلیک کنید

اگر Advanced Features فعال نباشد زبانه Security نیز در کادر محاوره‌ای Properties دیده نمی‌شود.

زبانه Security کادر محاوره‌ای Properties در شکل ۲- ۱۵ نشان داده شده است.



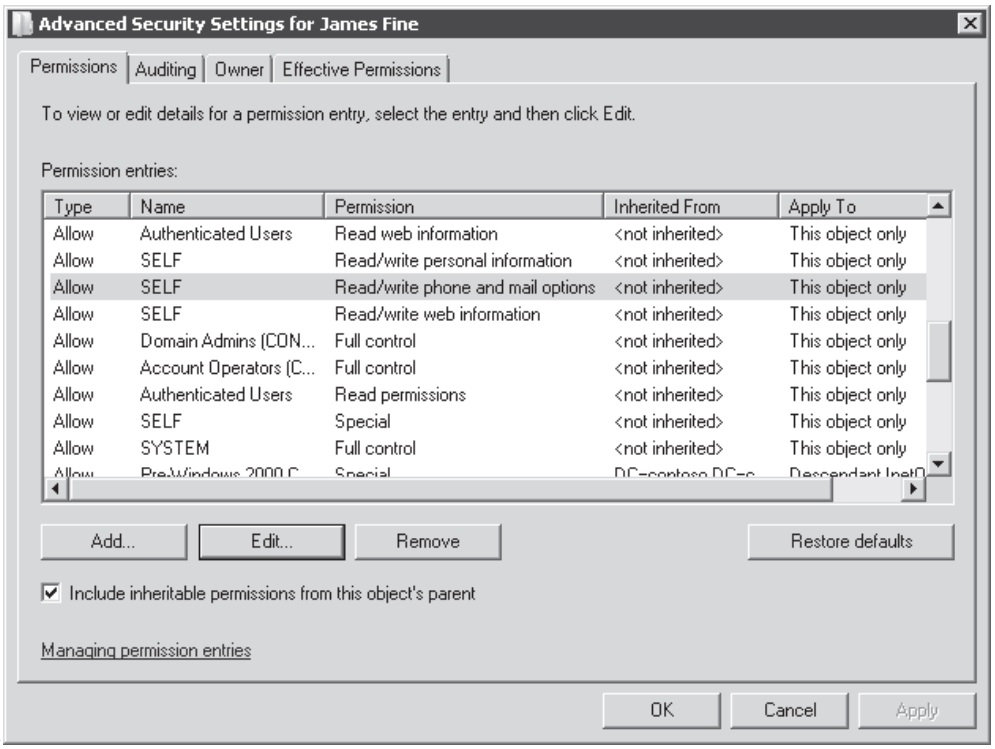
شکل ۱۵- ۲ زبانه Security مربوط به کادر محاوره‌ای Properties در Active Directory

۵. روی دکمه Advanced کلیک کنید

زبانه Security یک مرور کلی روی واحدهای امنیتی دارد که نسبت به شیء مجوز دارند ولی این زبانه جزئیات کافی درباره لیستهای

کنترل دسترسی Active Directory ارائه نمی‌دهد تا مدیر شبکه بتواند لیست را تفسیر یا مدیریت کند. برای همین باید روی Advanced کلیک کنیم تا کادر محاوره‌ای Advanced Security Settings باز شود.

شکل ۲- ۱۶ این کادر را نمایش می‌دهد

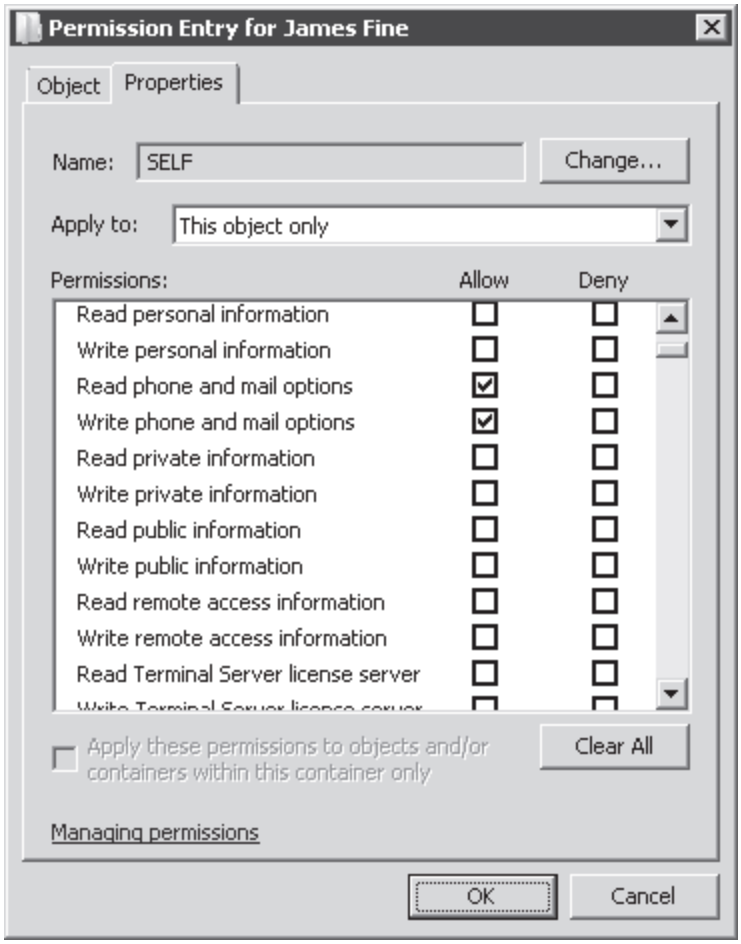


شکل ۲- ۱۶ کادر محاوره‌ای Advanced Security Settings برای یک شیء

زبانه Permission از کادر محاوره‌ای فوق لیست DACL شیء را نمایش می‌دهد. در شکل فوق بخوبی مشخص است که ACE ها در یک خط از لیست مجوزها خلاصه شده است. در این کادر ACE های تفکیک شده مربوط به DACL نمایش داده نمی‌شود. بعنوان مثال در شکل فوق خطی از مجوزها که انتخاب شده در واقع ترکیب دو ACE می‌باشد.

۶. برای مشاهده ACE های جزئی یک entry مجوز، entry را انتخاب و کلید Edit را بزنید .

کادر محاوره‌ای Permission Entry ظاهر شده جزئیات ACE های تشکیل دهنده entry مذکور را طبق شکل ۲- ۱۷ نمایش می‌دهد .



شکل ۱۷- ۲ کادر محاوره‌ای Permission Entry

شیء، خصیصه و حقوق دسترسی

DACL یک شیء، اعطاء مجوز نسبت به خصیصه مشخصی از یک شیء را امکانپذیر می‌کند. همانطوری که در شکل ۲- ۱۷ دیدیم می‌توانیم نسبت به تغییر شماره تلفن و پست الکترونیکی مجوز صادر کرده یا از آن جلوگیری کنیم. در حقیقت این فقط یک خصیصه نیست بلکه یک مجموعه خصیصه است که خصوصیات مشخص متعددی را در برمی‌گیرد. مدیریت خصوصیاتی که معمولاً بصورت گروهی استفاده می‌شوند با مجموعه‌های خصیصه ساده‌تراست. ولی ممکن است نیاز داشته باشیم باز هم مجوزهای جزئی‌تری را اعطا یا ممانعت کنیم. مثلاً اجازه تغییر فقط شماره همراه یا آدرس منزل را صادر کنیم.

صدور مجوز همچنین با هدف حقوق دسترسی نیز می‌تواند باشد. این حقوق به عمل خاصی مانند تغییر یا reset کلمه عبور اشاره می‌کند. تفاوت بین این دو حق بسیار مهم است. اگر کسی حق تغییر کلمه عبور را داشته باشد باید قبلا از تغییر کلمه عبور فعلی را وارد کند ولی اگر حق reset داشته باشد نیازی به دانستن کلمه عبور قبلی نیست.

در نهایت مجوزها نسبت به اشیاء اعطا می‌شوند. مثلاً توانایی تغییر مجوزهای یک شیء توسط ACE،Allow::Modify Permissions کنترل می‌شود . ساخت اشیاء فرزند (Child) نیز توسط مجوزهای شیء کنترل می‌شود. مثلاً می‌خواهیم به اعضای تیم پشتیبانی مجوز ساخت اشیاء کامپیوتر برای کامپیوترها و لپ‌تاپها را در OU اعطا کنیم. ACE،Allow::Create Computer Objects را باید برای تیم پشتیبانی در OU مربوطه در نظر بگیریم.

نوع و حوزه مجوزها در زبانه‌های Object و Properties و لیست بازشوی Apply To در هر زبانه مدیریت می‌شود .

اعطاء مجوز توسط کادر محاوره‌ای Advanced Security Settings

سناریویی را تصور کنید که می‌خواهیم به تیم پشتیبانی حق تغییر کلمه عبور کاربر James Fine را اعطا کنیم. در این بخش ابتدا یاد می‌گیریم از سخت‌ترین راه ممکن این کار را انجام دهیم یعنی توسط ایجاد ACE در DACL شیء کاربر. سپس یاد می‌گیریم با استفاده از ویزارد Delegation Of Control برای کل OUUsers واگذاری اختیار کنیم و خواهیم دید که چرا روش آخر توصیه می‌شود .

۱. ابزار ACTIVE DIRECTORY USERS AND COMPUTERS را باز کنید
۲. منوی View را باز کرده و Advanced Features را انتخاب کنید

۳. روی شیء دلخواه کلیک راست کرده Properties را انتخاب کنید
۴. زبانه Security را باز کنید
۵. دکمه Advanced را کلیک کنید
۶. دکمه Add را بزنید

اگر سرویس کنترل دسترسی کاربر ویندوز فعال باشد ممکن است مجبور شویم روی Edit کلیک کنیم و قبل از این که دکمه Add ظاهر شود اعتبار مدیریتی وارد کنیم.

۷. در کادر محاوره‌ای Select واحد امنیتی را که مجوز به آن اعطا می‌شود انتخاب کنید.

روش بهینه اعطاء مجوز به گروه است نه یک کاربر تنها. درمثال قبل بهتر است گروه پشتیبانی انتخاب شود.

۸. روی OK کلیک کنید.

کادر محاوره‌ای Permission Entry باز می‌شود.

۹. مجوزهای مورد نظر را پیکربندی کنید.

در این مثال در زبانه Object لیست مجوزها را اسکرول کرده و گزینه Allow::Reset Password را انتخاب کنید.

۱۰. روی OK کلیک کنید تا کادر بسته شود.

مفهوم مجوز موروثی و مدیریت آن

می‌توان تصور کرد که اعطاء مجوز تغییر کلمه عبور به تیم پشتیبانی برای هر شیء کاربر بصورت مجزا چه کار زمان‌بری خواهد بود. خوشبختانه اجباری برای این کار وجود ندارد. بجای آن می‌توان مجوز را نسبت به OU صادر کرد. مجوزی که نسبت به OU اعطا می‌شود توسط همه اشیاء آن به ارث برده می‌شود. بعنوان مثال اگر مجوز ریست کلمه عبور برای یک OU صادر گردد همه کاربران OU آنرا به ارث خواهند برد یعنی در یک مرحله اختیار مدیریتی واگذاری می‌شود .

وراثت مفهوم ساده وروشنی دارد. اشیاء فرزند مجوزهای container یا OU والد خود را به ارث می‌برند . OU یا container والد مجوزها را از والد خود به ارث می‌برد و اگر در بالاترین سطح باشد و والدین داشته باشد از دامنه به ارث می‌برد. دلیل اینکه شیء فرزند مجوزها را از والد خود به ارث می‌برد اینست که بطور پیش‌فرض شیء جدید هنگام ساخت دارای گزینه Include Inheritable Permissions From This Object's Parent فعال می‌باشد. این گزینه در شکل ۲- ۱۶ قابل مشاهده است

توجه داشته باشید که گزینه فقط روی مجوزهای با قابلیت وراثت عمل می‌کند در حالی که همه مجوزها قابلیت وراثت ندارند. مثلاً مجوز ریست کلمه عبور منتسب به یک OU توسط شیء گروه به ارث برده نمی‌شود چرا که گروهها اصلاً خصلت کلمه عبور ندارند . بنابراین وراثت به کلاسهای اشیاء خاصی قابلیت توسعه دارد بعنوان مثال کلمات عبور به شیء کاربر مربوط می‌شود نه به گروهها. بعلاوه کادر Apply To در کادر محاوره‌ای Permission Entry به منظور تعیین حد و مرز وراثت مجوز بکار می‌رود. این مبحث دارای پیچیدگی‌هایی است ولی چیزی که باید بدانیم اینست : بطورپیش‌فرض شیء جدید مجوزهای ممکن را از شیء والد خود (معمولاً OU یا container) به ارث می‌برد.

حالا این سئوال پیش می‌آید که اگر مجوز موروثی مناسب نباشد چه باید بکنیم؟ جواب اینست : برای تغییر مجوزهای موروثی دو کارمی‌توان انجام داد . اول : می‌توان علامت کادر Include Inheritable Permissions From This Object's Parent را در کادر محاوره‌ای Advanced Security Settings برداشت. با انجام اینکار شیء دیگر از والد خود ارث‌بری نمی‌کند و همه مجوزها مشخصاً برای شیء قابل تعریف خواهد بود . به جهت اینکه در قانون وراثت که از والد اعمال می‌گردد استثنا پیش می‌آید این روش مناسبی نمی‌تواند باشد .

روش دوم اینست که جلوی وراثت را نگیریم ولی با اعطای مجوزهای اختصاصی به شیء فرزند (مجوزexplicit) مجوزهای موروثی را بی‌اثر کنیم. مجوزهای explicit همیشه مجوزهای موروثی را بی‌اثر می‌کنند . نکته خیلی مهم اینست که اگر مجوز explicit اجازه دسترسی بدهد مجوز موروثی را که از دسترسی ممانعت (deny) می‌کند بی‌اثر می‌کند . شاید به نظر ضد و نقیض بیاید ولی می‌شود اینطور توجیه کرد که قانونی از طرف والد برای عدم دسترسی وضع شده ولی شیء فرزند بعنوان استثنا در نظر گرفته شده است (allow) .

نکته امتحانی مراقب سناریوهایی باشید که دسترسی یا واگذاری اختیار طبق انتظار اجرا نمی‌شوند . در این حالت یا وراثت شکسته شده است یعنی فرزند مجوزهای والد را به ارث نمی‌برد یا شیء فرزند مجوز explicit دارد که مجوز والد را بی اثر می‌کند .

واگذاری اختیار وظایف مدیریتی توسط ویزارد Delegation Of Control

تاکنون پیچیدگی DACL را دیدیم و به این نتیجه رسیدیم که مدیریت مجوزها با استفاده از کادر محاوره‌ای Permission Entry کار ساده‌ای نیست. خوشبختانه راه بهتری وجود دارد و آن ویزارد Delegation Control می‌باشد. رویه زیر جزئیات آنرا نشان می‌دهد .

۱. ابزار ACTIVE DIRECTORY USERS AND COMPUTERS را باز کنید .
۲. روی گره مورد نظر (دامنه یا OU) که می‌خواهید اختیارات مدیریتی را واگذاری کنید کلیک راست کرده و Delegation Control را انتخاب کنید. در این مثال می‌توانید OU متشکل از کاربران را انتخاب کنید. ویزارد ظاهر می‌شود.

۳. روی Next کلیک کنید. ابتدا گروه مدیریتی که قرار است وظایف به آنها محول شود در نظر بگیرید.
۴. در صفحه Users or Groups دکمه Add را کلیک کنید .
۵. از کادر محاوره‌ای Select برای انتخاب گروه استفاده کرده و OK را بزنید .
۶. Next را بزنید . سپس می‌توانید وظایف خاص مورد نظر را برای گروه مشخص کنید.
۷. در صفحه Tasks To Delegate وظایف را مشخص کنید. در این مثال وظایف Reset User Passwords و Force Password Change at Next Logon را انتخاب می‌کنیم.
۸. کلید Next را بزنید.
۹. خلاصه اطلاعات ورودی به ویزارد را مرور کرده و Finish را کلیک کنید . ویزارد فوق ACE های مورد نیاز برای اجرای وظایف تعریف شده گروههای منتخب را اعمال می‌کند.

گزارش‌گیری و مشاهده مجوزها

زمانی که نیاز است بدانیم چه کسی چه کاری می‌تواند انجام دهد راههای متعدد دیگری وجود دارند تا ما بتوانیم مجوزها را مشاهده کنیم و گزارش بگیریم. قبلا یاد گرفتیم که مجوزها را در DACL توسط کادر محاوره‌ای Advanced Security Settings and Permission Entry ببینیم. ابزار خط فرمان Dsacls.exe نیز از اشیاء دایرکتوری گزارش تهیه می‌کند. وقتی دستور را به همراه DN یک شیء تایپ کنید گزارشی از مجوزهای شیء را بعنوان خروجی دریافت می‌کنید. بعنوان مثال فرمان زیر گزارشی از مجوزهای منتسب بهOUPeople را ارائه می‌دهد :

Dsacls.exe "ou=people,dc=contoso,dc=com"

فرمان dsacls همچنین در اعطای مجوز برای واگذاری اختیار کاربرد دارد. برای اطلاعات کمکی syntaxو کاربرد فرمان تایپ کنید :

Dsacls.exe /?

حذف مجوزهای یک شیء

چطور می‌توان اختیارات واگذاری شده را برگرداند؟ متاسفانه دستوری در این ارتباط وجود ندارد . برای این منظور از کادر محاوره‌ای Advanced Security Settings و Permission Entry استفاده می‌شود. جهت برگرداندن مجوزها به حالت پیش‌فرض کادر محاوره‌ای Advanced Security Settings را باز کرده و Restore Default را می‌زنیم. مجوزهای پیش‌فرض کلاس شیء توسط schemaActive Directory مشخص می‌گردد. پس از انجام این کار می‌توانیم دوباره مجوزهای explicit را به DACL بیافزاییم. Dsaclsهمچنین سوئیچ /s دارد که می‌تواند مجوزها را به حالت پیش‌فرض درآورد و سوئیچ /tکه تغییرات را بروی شیء و تمام اشیاء فرزندش اعمال می‌کند. برای مثال جهت گرفتن مجوزهای OUPeople و اشیاء فرزندش تایپ می‌کنیم :

Dsacls "ou=people,dc=contoso,dc=com" /resetdefaultdacl

مفهوم مجوز نهایی (effective)

مجوز نهایی برآیند مجوزهای یک واحد امنیتی مانند کاربر یا گروه است که براساس مجموع تاثیرات ACE های موروثی یا explicit به دست می‌آید. بعنوان مثال توانایی تغییرکلمه عبورکاربر می‌تواند نتیجه عضویت در گروهی باشد که اجازه تغییر دادن کلمه عبور را روی یک OU، چند سطح بالاتر از شیءکاربر دارد . مجوز موروثی گروهی که عضو آن هستید باعث می‌شود مجوز نهایی Allow::Reset روی کلمه عبور داشته باشید. مجوز نهایی زمانی پیچیده خواهد شد که مجوزهای دسترسی و عدم دسترسی ACE های موروثی و explicit همزمان موجود باشد و ما عضو گروههای مختلفی باشیم که نسبت به اشیاء مجوزهای متفاوتی دارند

اینکه مجوز به حساب کاربری نسبت داده شود یا گروهی که کاربر عضو آن است فرقی نمی‌کند. در نهایت ACE به کاربر اشاره می‌کند. هر چند امکان نسبت دادن به یک کاربر یا کامپیوتر نیز موجود است ولی بهترین روش اینست که مجوزها به گروه نسبت داده شود. نسبت دادن یک مجوز مستقیماً به کاربر در مقایسه با حالتی که مجوز به گروهی که کاربر عضو آن است اعطا می‌شود نشانگر اهمیت بیشتر یا کمتر مجوز نیست.

مجوزهای دسترسی تجمعی هستند . مثلاً زمانی که کاربری عضو گروههای مختلفی است که هر گروه دارای مجوز عملیات مختلفی است درست مانند حالتی که همه وظایف به کاربر واگذاری شده است کاربر می‌تواند همه آن وظایف را انجام دهد .

مجوزهایی که دسترسی را منع می‌کنند (deny) مجوزهای معادل که اجازه دسترسی می‌دهند راخنثی می‌کنند . اگر کاربری عضو دو گروه باشد و یک گروه مجوز تغییرکلمه عبور داشته باشد و گروه دوم از این کار منع شده باشد کاربر اجازه تغییر کلمه عبور را نخواهد داشت .

نکته در استفاده از منع دسترسی احتیاط کنید .

عموماً نیازی به استفاده از منع دسترسی وجود ندارد . اگر مجوز دسترسی به کاربری اعطا نشود کاربر نمی‌تواند عملیات را انجام دهد . قبل از اعطا منع دسترسی بهتر است بررسی شود آیا با حذف یک مجوز دسترسی منظور حاصل می‌شود یا نه . نهایتاً توصیه می‌شود منع مجوز را با احتیاط و بندرت بکاربرید.

مجوزها همگی ذره‌ای هستند . حتی اگر کاربری از تغییر کلمه عبور منع شده باشد درصورت اعطاء مجوزهای دسترسی دیگر امکان تغییرنام کاربری یا آدرس پست الکترونیک را خواهد داشت

در نهایت یاد گرفتیم اشیاء فرزند بطور پیش‌فرض مجوزهای قابل وراثت را از اشیاء والد خود به ارث می‌برند و مجوزهای explicit مجوزهای موروثی را بی اثر می‌کنند . یعنی مجوز دسترسی explicit مجوز منع دسترسی را بی‌اثر می‌کند.

متاسفانه تعامل پیچیده انواع مجوزها از قبیل کاربر، گروه، explicit، موروثی، دسترسی و منع دسترسی محاسبه مجوزهای موثر را می‌تواند کمی سخت کند. البته زبانه Effective Permissions در کادر محاوره‌ای Advanced Security Settings مربوط به شیء موجود است ولی از آنجایی که جزئیات کافی در مورد مجوزها را ندارد عملاً غیرقابل استفاده می‌باشد. بهرحال گزارش مجوزها را هم از دستور Dsaclsو هم از زبانه مذکور می‌توانیم استخراج کنیم و از آن برای محاسبه مجوزهای نهایی بهره ببریم ولی این‌کار بصورت دستی انجام می‌گیرد.

اطلاعات بیشتر کنترل دسترسی مبتنی بر نقش

بهترین روش برای واگذاری اختیار در Active Directory کنترل دسترسی مبتنی بر نقش است. هرچند این رویکرد در امتحان مایکروسافت جایی ندارد درک آن در به پیاده‌سازی بهتر واگذاری اختیار در دنیای واقعی کمک می‌کند. برای اطلاعات بیشتر به منبع زیر مراجعه کنید : Windows Administration Resource Kit:Productivity Solutions for IT Professionalsتهیه شده توسط دن هلم (انتشارات مایکروسافت سال ۲۰۰۸).

طراحی ساختارOUبرای پشتیبانی ازتفویض اختیار

الآن می‌دانیم کهOUهاcontainerهای مدیریتی ودربرگیرنده اشیائی هستندکه نیازمندیهای مدیریتی،پیکربندی ونمایش‌پذیری (visibility)یکسان دارند. حالااولین نیازمندی رادرک می‌کنید: مدیریت. اشیائی که بطرزمشابهی توسط مدیران مشابه مدیریت می‌شوندبایددریکOUقرارگیرند. ازطریق جای دادن کاربران دریکOUبنامPeopleواعطاءیک مجوزبهOUعملاًواگذاری اختیارتغییرکلمه عبوررابه گروه پشتیبانی داده‌ایم. هرمجوزدیگری که روی عملکردمدیرشبکه نسبت به کاربرتاثیرمی‌گذاردمی‌تواندرویOUPeopleاعمال شود. بعنوان مثال می‌توانیم به مدیران منابع انسانی سازمان اجازه غیرفعال کردن حساب کاربری کاربران رابدهیم تادرپایان دوره کاری حساب آنهاغیرفعال گردد. این اختیاررانیزمی‌توان نسبت بهOUPeopleواگذاری کرد.

می‌دانیدکه به مدیران شبکه توصیه می‌شودباحساب کاربری سطح پایین به سیستم خودواردشوندوابزارهای مدیریتی راباعتباریک حساب سطح بالاکه برای اجرای وظایف مدیریتی مجوز لازم راداراست اجراکنند. این حسابهای ثانویه حسابهای مدیریتی شبکه میباشند. منطقی نیست که گروه پشتیبانی توانایی تغییرکلمه عبورروی چنین حسابهای سطح بالایی راداشته باشندوهمچنین مدیران منابع انسانی بتوانندآنهاراغیرفعال کنند. بنابراین مدیریت حسابهای مدیریتی باحسابهای غیرمدیریتی تفاوت دارد. به همین دلیل است کهOUجداگانه‌ای بنامAdminsبرای اشیاءکاربرمدیریتی ایجادشده است. واگذاری اختیارروی اینOUکاملاًباOUPeopleمتفاوت است.

بهمین ترتیب ممکن است بخواهیم به تیم پشتیبانی خوداختیارافزودن شیءکامپیوتررابهOUClientsواگذاریکنیم که شامل کامپیوترهای دسک‌تاپ ولپ‌تاپ میشودولی درموردOUServersفقط بایدگروهServer Administrationمجوزساخت ومدیریت اشیاءکامپیوترراداشته باشند.

نقش اصلیOUهاتعیین حوزه اختیاراتی است که به اشیاءدیگرواگذاری می‌گردد. شروع طراحی محیط Active Directoryطراحی ساختارOUخواهدبودکه مدل مدیریتی سازمان رامشخص می‌کند. بندرت پیش می‌آیدکه ساختارمدیریت اشیاءActive Directoryباچارت سازمانی مشابه باشند. عموماًکاربران عادی به یک روش وتوسط یک تیم پشتیبانی می‌شوندبنابراین اشیاءکاربردریکOUیاشاخه‌ای ازآن قرارداده می‌شوند. اغلب سازمانهایی که خدمات متمرکزدارندعملیات پشتیبانی متمرکزهم دارنددرچنین حالتی همه اشیاءکامپیوتردریکOUیاشاخه‌ای ازآن قرارمی‌گیرند. بهرصورت درحالتی که سیستم پشتیبانی مرکزیت نداردOUClientsبه چندشاخه تقسیم می‌شودکه هرکدام نماینده یک محل جغرافیایی می‌باشند. درهرمحل اختیارواحدبرای افزودن اشیاءکامپیوتربه دامنه به گروه پشتیبانی محلی سپرده می‌شود.

ابتداOUهارابه منظورواگذاری اختیارکافی نسبت به اشیاءدایرکتوری طراحی می‌کنیم. پس ازدستیابی به هدف اول طراحی راباهدف تسهیل در پیکربندی کامپیوترهاواشیاءازطریق سیاستهای گروهی که درفصل ۶ بحث میشودتصحیح می‌کنیم. طراحیActive Directoryیک هنروعلم است.

تمرینات واگذاری اختیارات مدیریتی

دراین تمرینات واگذاری اختیارات مدیریتی دردامنه contoso.comمدیریت می‌شودونتایج تغییرات رویACLهادراشیاء Active Directoryمشاهده می‌گردد. قبل ازاجرای تمرینات بایدتمرینات درس ۲ "ساخت وجستجوی اشیاءدرActive Directory" راانجام داده باشید. OUهاایجادشده درآن تمرینات برای تمرینات فعلی لازم می‌باشد.

تمرین ۱ واگذاری اختیارات برای پشتیبانی ازحسابهای کاربری

دراین تمرین قراراست گروه پشتیبانی اجازه ریست کلمه عبوروفعال کردن حساب‌های کاربری رادرOUPeopleدریافت کنند.

۱. بااعتبارAdministratorبهSERVER01واردشده وابزارActive Directory Users And Computersرااجراکنید.

۲. گرهDomainرابازمی‌کنیم (contoso.com) رویOUPeopleکلیک راست کرده وDelegate Controlراانتخاب می‌کنیم تاویزاردDelegation Of Controlاجراشود.
۳. روی Nextکلیک می‌کنیم.
۴. روی صفحهUsers Or GroupsدکمهAddرامی زنیم.
۵. درکادرمحاوره‌ایSelectتایپ می‌کنیمHelp DeskوOKرامی‌زنیم.
۶. رویNextکلیک می‌کنیم.
۷. درصفحهTask To DelegateگزینهReset User Passwords And Force Password Change At Next Logonراانتخاب می‌کنیم.
۸. روی Nextکلیک می‌کنیم.
۹. خلاصه تنظیمات رامرورکرده وFinishرامی‌زنیم.

تمرین ۲ مشاهده مجوزهای واگذارشده

دراین تمرین مجوزهای نسبت داده شده به گروه پشتیبانی رامشاهده می‌کنیم.

۱. بااعتبارکاربریAdministratorبهSERVER01واردمی‌شویم ابزارActive Direcotry Users And Computersرابازمی‌کنیم.
۲. رویOUPeopleکلیک راستکرده وPropertiesراانتخاب می‌کنیم.
توجه داشته باشیدکه زبانهSecurityقابل مشاهده نیست. وقتیAdvanced Featuresفعال نیست نمی‌توانیم زبانهSecurityرادرکادرمحاوره‌ایPropertiesیک شیءببینیم.
۳. رویOKکلیک می‌کنیم تاکادرمحاوره‌ایPropertiesبسته شود.
۴. منویViewرابازمی‌کنیم وگزینهAdvanced Featuresراانتخاب می‌کنیم.
۵. رویOUPeopleکلیک راست کرده وPropertiesراانتخاب می‌کنیم.
۶. روی زبانهSecurityکلیک می‌کنیم.
۷. دکمه Advanced رامی‌زنیم.
۸. درلیست Permission Entriesاولین مجوزاعطاشده بهHelp Deskراانتخاب می‌کنیم.
۹. دکمه Editرامی‌زنیم.
۱۰. درکادرمحاوره‌ای Permission Entryمجوزموردنظرراپیداکرده وروی‌OKکلیک می‌کنیم تاکادربسته شود.
۱۱. مراحل ۸ تا ۱۰ رابرای مجوزدومHelp Deskتکرارمی‌کنیم.
۱۲. برای مشاهدهACLیک کاربردرOUPeopleمراحل ۲ تا ۱۱ رابرای کاربرتکرارمی‌کنیم ومجوزهای موروثی اعطاشده به Help Deskراچک می‌کنیم.
۱۳. درخط فرمان عبارت dsacls "ou=people,dc=contoso,dc=com"راتایپ کرده وکلیدEnterرابزنید.
۱۴. مجوزهای اعطاشده به Help Deskراپیداکنید.

خلاصه درس

- واگذاری اختیاردرActive Directoryدر سازمان این امکان راایجادمی‌کندکه وظایف مدیریتی مشخصی به شخص یاگروههای مناسب محول شود.
- واگذاری اختیارنتیجه مجوزهایاACEهای مرتبط با DACLدر Active Directoryمی‌باشد.
- DACLازطریقAdvanced Security Settingsدر کادر محاوره‌ایPropertiesشیءقابل مشاهده وتغییراست.
- ویزارد Delegation of Controlپیچیدگی ذاتیACLاشیاءراازطریق اعطاءمجوزبه گروه‌هاازبین می‌برد.
- مجوزهای یک شیءبااستفاده ازکادرمحاوره‌ای Advanced Security SettingsیاDsaclsباسوئیچ /resetDefaultDACLقابل برگشت به حالت اولیه است.
- بهترین روش برای واگذاری اختیاراستفاده ازOUاست.اشیاءداخلOUمجوزهاراازOUوالدبه ارث می‌برند.
- وراثت قابل تغییراست چه باغیرفعال کردن آن روی شیءفرزندچه اعطای مجوزexplicitبه شیءفرزندکه باعث بی‌اثرشدن مجوزموروثی می‌شود.
- مجوزهای نهایی برآیندمجوزهای کاربر،گروه،دسترسی،عدم دسترسی،موروثی وexplicitمی‌باشد. مجوزهای عدم دسترسی مجوزهای دسترسی رابی‌اثرمی‌کنندومجوزهایexplicitمجوزهای موروثی رابی‌اثرمی‌کنند. بنابراین مجوزدسترسیexplicitمجوزعدم دسترسی موروثی رابی‌اثرمی‌کند.

سئوالات پایان درس

۱. می‌خواهید به گروه پشتیبانی خودامکانresetکلمه عبوروبازکردن قفل حسابهای کاربران رابدهید. ازکدام ابزارزیراستفاده می‌کنید؟

A. Delegation of Control Wizard
B. DSACLS
C. DSUTIL
D. کادر محاوره‌ای Advanced Security Settings

فصل ۳

کاربران

در فصل ۱ "نصب" Active Directory Domain Services(AD DS) به عنوان راه‌حل identity and access معرفی شد. حساب‌های ذخیره شده کاربران در دایرکتوری کامپوننتهای اساسی identity هستند. بخاطر اهمیت‌شان، دانش حساب‌های کاربری و عملیات مرتبط با پشتیبانی آنها در موفقیت مدیر شبکه سازمانی مبتنی بر ویندوز نقش حیاتی دارد.

توانایی شما در کارکرد موثر با حساب‌های کاربری می‌تواند در افزایش بهره‌وری تاثیر فراوان داشته باشد. مهارت‌هایی که در ساختن یا تغییر یک حساب کاربری موثر هستند مانند مواردی که در فصل ۲ "مدیریت" تشریح شد در مواجهه با تعداد زیاد کاربربی‌فایده خواهند بود. مثال آن ساختن حسابهای جدید برای کارمندان تازه استخدام شده سازمان است.

در این فصل یاد می‌گیریم چگونه از ابزارها و تکنیک‌ها برای خودکار سازی ایجاد و مدیریت کاربران و جستجو و تغییر اشیاء کاربر و خصوصیات‌شان استفاده کنیم. همزمان با Microsoft Windows PowerShell آشنا می‌شویم که آینده مدیریت خودکار و مبتنی بر خط فرمان برای تکنولوژی‌های ویندوزی است. همچنین گزینه‌های مختلفی را با هدف اجرای وظایف مدیریتی معمول یاد می‌گیریم.

در امتحان بین‌المللی انتظار می‌رود آشنایی مختصری با اهداف و شکل دستوری ابزارهای خط فرمان، Windows PowerShell و Microsoft Visual Basic Script (VBScript) داشته باشید. بهرحال در این فصل چیزی بیش از محدوده امتحان ارائه می‌گردد و خودکارسازی و اسکریپت نویسی را بطور کامل معرفی می‌کند. مطالبی را که در این فصل یاد می‌گیرید خوب تمرین کنید نه به خاطر امتحان بلکه هرچقدر وظایف مدیریتی تکراری خود را بصورت خودکار انجام دهید بهره‌وری و موفقیت شما بیشتر خواهد شد.

اهداف امتحانی در این فصل

- ساخت و پشتیبانی اشیاء Active Directory
  - خودکارسازی ساخت حساب‌های Active Directory
  - پشتیبانی حساب‌های Active Directory

دروس این فصل :

- درس ۱: خودکارسازی ساخت حساب‌های کاربری
- درس ۲: ساخت کاربر با Windows PowerShell و VBScript
- درس ۳: پشتیبانی از اشیاء کاربر و حسابها

قبل از شروع

برای اجرای تمرینات این فصل باید SERVER01 را به DC در دامنه contoso.com ارتقا داده باشید. برای مشاهده جزئیات این کار به فصل ۱ مراجعه کنید.

در دنیای واقعی

دن هلم

جالب خواهد بود اگر لحظه‌ای درنگ کنیم و ببینیم چه میزان از وقت ما بعنوان مدیر شبکه صرف اجرای عملیات ابتدایی مربوط به اشیاءکاربران می‌شود. همه روزه در یک شبکه سازمانی با یک سری موارد خاص در مورد مدیریت کاربران مواجه می‌شویم. مثلاً کارمندان استخدام می‌شوند، منتقل می‌شوند، ازدواج می‌کنند و عاقبت سازمان را ترک می‌کنند. بعنوان یک انسان اشتباهاتی دارند که نمونه آن فراموش کردن کلمه عبور یا قفل کردن حساب خودشان با تایپ کلمه عبور اشتباه می‌باشد.

مدیران شبکه باید به همه این مشکلات پاسخ دهند. از طرفی حسابهای کاربری خیلی پیچیده هستند چرا که خصوصیات زیادی دارند که حتی مدیران کارکشته نیز اغلب با این فرایندها و قوانین که خود وضع کرده‌اند سرگردان می‌شوند. به نظر اینجانب رمز داشتن مدیریت کاربران بصورت امن، کارامد و پیوسته افزایش سطح مهارت مدیران می‌باشد.

درس ۱ : خودکارسازی ساخت حساب‌های کاربری

در فصل ۲ یاد گرفتیم که چطور در ابزار Active Directory Users And Computers کاربر جدید تعریف کنیم. اگرچه روش ذکر شده در فصل ۲ برای تعداد کمی کاربر قابل اجراست ولی ما نیاز به روشهای پیشرفته‌تر داریم تا ساخت حساب کاربری را زمانی که تعداد کاربران زیاد است و باید به دامنه افزوده شوند بطور خودکار اجرا کنیم. دراین درس روشهای متعددی را از این دست یاد می‌گیریم.

بعد از این درس می‌توانید :

- از روی الگوهای (Templates)حساب کاربری کاربر جدید بسازیم.
- کاربران را با دستور CSVDE منتقل کنیم
- کاربران را با دستور LDIFDE منتقل کنیم

زمان تقریبی : ۳۰ دقیقه

ساخت کاربر با استفاده از الگو

کاربران در یک دامنه دارای خصیصه‌های مشابه بسیاری هستند. مثلاً همه نماینده‌های فروش در یک گروه قرار دارند، در ساعات مشابه به شبکه وارد می‌شوند و پروفایل سیار (roaming)و پوشه اختصاصی‌شان (home folders) روی یک سرور قرار دارد. وقتی کاربر جدیدی تعریف می‌شود براحتی امکان کپی حساب کاربری موجود وجود دارد بجای اینکه یک حساب خالی ایجاد شده و همه خصوصیات یکی یکی تعریف شود.

از زمان ویندوز NT 4.0 مفهوم الگوی حساب کاربری توسط ویندوز پشتیبانی می‌شود. الگوی حساب کاربری یک حساب کاربری عمومی است که خصوصیات معمول آن تنظیم شده است. مثلاً می‌توانیم یک حساب الگو برای نماینده‌های فروش با عضویت در گروه، ساعات ورود به شبکه ، پوشه اختصاصی و مسیر پروفایل سیار که همگی در الگو تعریف شده‌اند ایجاد کنیم.

نکته حساب کاربری الگو را غیرفعال کنید

حساب الگو بهتر است برای ورود به شبکه استفاده نشود بنابراین آنرا غیر فعال کنید.

برای تعریف کاربر جدید از روی الگو از منوی میانبر Copy را انتخاب کنید. ویزارد Copy Object User ظاهر می‌شود. نام، نام کاربری و تنظیمات کلمه عبور کاربر جدید باید مشخص شود. تعدادی از خصیصه‌های الگو به حساب کاربری جدید کپی می‌شود.پس از ساخت حساب خصوصیات آن به صورت گروهی در زبانه‌های مختلف در کادر محاوره‌ای Properties قابل مشاهده است. بعضی از زبانه‌ها و خصوصیات قابل انتقال در آنها را مرور می‌کنیم:

- General هیچ خصیصه‌ای از این زبانه کپی نمی‌شود.
- Address صندوق پستی، شهر، استان، کد پستی و کشور یا منطقه کپی می‌شود. توجه کنید که آدرس خیابان کپی نمی‌شود.
- Account ساعات ورود، کامپیوترهای مجاز برای ورود، درایو اختصاصی (home drive) و پوشه اختصاصی کپی می‌شود.
- Organization بخش، شرکت و مدیر کپی می‌شود.
- Member Of عضویت در گروهها و گروه اولیه کپی می‌شود.

نکته چیزی که می‌بینیم همه آن چیزی نیست که وجود دارد.

حساب‌های کاربری خصیصه‌های دیگری نیز دارند که در زبانه‌های استاندارد ابزار Active Directory Users And Computers قابل رویت نیستند. این خصلت‌های مخفی شامل خصیصه‌های مفیدی مانند assistant، division، نوع کاربر(employee type) و مشخصه کاربر(employee ID) می‌باشد. برای مشاهده این خصوصیات در ابزار Active Directory Users And Computers منوی View را باز کرده و گزینه Advanced Features را انتخاب می‌کنیم. سپس پنجره Properties یک کاربر و بعد زبانه Attribute Editor را باز می‌کنیم. بسیاری از این خصیصه‌ها مانند assistant، division، نوع کاربرو مشخصه کاربر از الگو به حساب کاربری جدید کپی می‌شود.

مواردی که کپی می‌شود کافی نیست

بسیاری از مدیران شبکه عقیده دارند خصیصه‌های کپی شده محدود است. بعنوان مثال لازم است عنوان شغل و نام خیابان نیز کپی شود. امکان تغییر Active Directory schema وجود دارد بطوری که در هنگام الگوبرداری خصیصه‌های بیشتری کپی شود. برای راهنمایی بیشتر مقاله Knowledge Base شماره 827832 را از آدرس http://support.microsoft.com/kb/827832 را ببینید.

در هر صورت امکان استفاده از روشهای پیشرفته خودکارسازی ساخت حساب کاربری وجود دارد. در این فصل یاد می‌گیریم چطور از دستورات سرویس دایرکتوری (DS) ، Comma-Seperated Values data Exchange(CSVDE) ، LDAP Data Interchange Format Data Exchange (LDIFDE) و Windows PowerShell به منظور خودکارسازی عملیات مدیریتی استفاده کنیم. با این ابزارها کنترل کاملی روی پروسه‌های ایجاد حسابهای جدید خواهیم داشت.

استفاده از ابزارهای خط فرمان Active Directory

در فصل ۲ با دستور Dsquery.exe آشنا شدیم. این دستور بخشی از ابزار موسوم به دستورات DS است. دستورات DS زیر در ویندوز سرور 2008 پشتیبانی می‌شود :

- Dsadd یک شیء در دایرکتوری می‌سازد
- Dsget خصصوصیات مشخصی از یک شئ را برمی‌گرداند
- Dsmod خصوصیات مشخصی از یک شیء را تغییر می‌دهد
- Dsmove یک شیء را به OU یا container جدید منتقل می‌کند
- Dsrm شیء، اشیاء داخل شیء یا هر دو را حذف می‌کند
- Dsquery پارامترهایی را برای پرس‌وجو در خط فرمان دریافت کرده و لیستی از اشیاء مرتبط را نمایش می‌دهد. بطور پیش فرض نتیجه بصورت DN هر شیء در خروجی ظاهر می‌شود ولی می‌توان از پارامتر o– با متغیرهایی نظیر dn, rdn, upn یا samid استفاده کرد تا نتیجه به ترتیب بصورت dn، user principle name(UPN)، dn مرتبط(rdn) یا pre-Windows 2000 logon names(security account manager ID) نمایش داده شود.

بیشتر دستورات DS پس از خود دستور دو متغیر دارند یکی نوع شیء و دیگری DN مربوط به شیء. بعنوان مثال دستور زیر یک حساب کاربری برای Mike Fitzmaurice می‌سازد:

```
Dsadd user "cn=Mike Fitzmaurice,ou=People,dc=contoso,dc=com"
```

نوع شیء یعنی user فوراً پس از شیء آمده است. پس از آن DN شیء قرار دارد. وقتی DN شیء جای خالی دارد (بین Mike و Fitzmaurice) کل DN را باید در گیومه قرار دهیم. دستور زیر همان کاربر را حذف می‌کند :

```
Dsrm user "cn=Mike Fitzmaurice,ou=People,dc=contoso,dc=com"
```

دستورات DS که خصوصیات اشیاء را می‌خواند یا دستکاری می‌کند شامل Dsquery.exe، Dsget.exe و Dsmod.exe می‌باشد. جهت تعیین یک خصیصه آن را بعد از DN بعنوان یک پارامتر اضافه می‌کنیم. بعنوان مثال دستور زیر پوشه اختصاصی کاربر مذکور را برمی‌گرداند.

```
Dsget user "cn=Mike Fitzmaurice,ou=People,dc=contoso,dc=com" -hmdir
```

نام پارامترهای دستور DS که یک خصیصه را برمی‌گرداند مانند hmdir همیشه همنام آن خصیصه در ابزار Active Directory Users And Computers نیستند.

ساخت کاربر با دستور Dsadd

از دستور فوق برای ساخت اشیاء در Active Directory استفاده می‌شود.دستور DSADD USER UserDN یک شیءکاربر جدید می‌سازد و پارامترهای مشخص کننده خصوصیات کاربر را قبول می‌کند. دستور زیر پارامترهای مهم برای ساخت حساب کاربری را نشان می‌دهد :

```
Dsadd user "user dn" -samid pre-windows 2000 logon name –pwd {password | *} -
mustchpwd yes
```

پارامتر pwd کلمه عبور را مشخص می‌کند. اگر بصورت ستاره "*" درج شود پیغام ورود کلمه عبور ظاهر می شود. پارامتر mustchpwd مشخص می‌کند که کاربر باید در هنگام ورود کلمه عبور خود را عوض کند.

DSADD USER تعدادی از پارامترهایی که مشخص کننده خصوصیات شیء کاربر هستند قبول می‌کند. نام بیشتر پارامترها بامسما هستند مانند email– ، profile- و company– . برای توضیحات کامل در مورد پارامترهای DSADD USER تایپ می‌کنیم: DSADD USER /? یا در Help And Support Center ویندوز سرور 2008 مستندات مربوطه را مرور می‌کنیم.

در مقادیر پارامترهای email– ، hmdir- ، profile- و webpg– عبارت %username% نماینده SAM ID است. بعنوان مثال برای پیکربندی پوشه اختصاصی یک کاربر در هنگام ساخت کاربر با دستور DSADD USER پارامتر زیر را اضافه کنید :

```
-hmdir \\server01\users\%username%\documents
```

انتقال کاربران با دستور CSVDE

این دستور ابزار خط فرمانی است که اشیاء دایرکتوری را از Active Directory به یک فایل متنی با جداکننده کاما (comma-delimited یا comma-separated با پسوند csv)و یا بالعکس منتقل می‌کند. این فایل‌ها با ابزارهای متداولی مانند Notepad و Microsoft Office Excel قابل باز شدن ایجاد و تغییر هستند. اگر اطلاعات کاربران در فایلهای Excel یا بانک اطلاعاتی Access موجود دارید دستور CSVDE ابزار قدرتمندی برای ساخت خودکار حساب‌های کاربران است.

شکل فرمان CSVDE به صورت زیر است :

```
Csvde [-i] [-f Filename] [-k]
```

پارامتر i جهت انتقال را تعیین می‌کند. بدون آن حالت پیش فرض دستور وضعیت انتقال از Active Directory به فایل است. پارامتر f– نام فایل را برای انتقال مشخص می‌کند. پارامتر k– هنگام عملیات انتقال از فایل بکار می‌آید زیرا دستور CSVDE را مجبور به چشم پوشی از خطاهایی مانند Object Already Exist، Constraint Violation و Attribute Or Value Already Exists می‌کند.

فایل انتقال خود فایل متنی با جداکننده کاما است (csv. یا txt.) که در آن خط اول مشخص کننده خصلت‌های انتقالی بر اساس نام خصلت مشخص شده در LDAP می‌باشد. هر شیء یک خط را به خود اختصاص می‌دهد و باید دقیقاً منطبق بر خصلت‌های خط اول باشد. نمونه فایل را در ادامه می‌بینیم :

```
DN,objectClass,SamAccountName,sn,givenName,userPrincipleNam
"cn=Lisa Andrews,ou=People,dc=contoso,dc=com",user,lisa.andrews ,
Lisa,Andrews,lisa.andrews@contoso.com
```

پس از انتقال اشیاء فایل توسط دستور CSVDE شیء کاربری با نام Lisa Andrews در People OU ساخته می‌شود. نام کاربری، نام و نام خانوادگی توسط فایل پیکربندی می‌شود. این دستور نمی‌تواند کلمات عبور را منتقل کند و بدون کلمه عبور حساب کاربری غیرفعال می‌گردد. پس از تغییر کلمه عبور می‌توان کاربر را فعال کرد.

در فصل ۴ "گروهها" و ۵ "کامپیوترها" از این دستور برای انتقال گروهها و کامپیوترها استفاده می‌کنیم. برای اطلاعات بیشتر درباره CSVDE شامل پارامترها و طریقه استفاده از آن برای انتقال اشیاء تایپ کنید csvde /? یا در Help and Support Center ویندوز سرور 2008 جستجو کنید.

انتقال کاربران با دستور LDIFDE

از این دستور نیز برای انتقال اشیاء Active Directory مانند کاربران استفاده می‌شود. LightWeight Directory Access Protocol Data Interchange Format (LDIF) استاندارد پیش‌نویس اینترنتی برای فرمت فایل است است که به منظور اجرای عملیات گروهی روی دایرکتوری‌هایی که با استاندارد LDAP تهیه شده‌اند بکار می‌رود. LDIF از عملیات دوطرفه انتقال و عملیات گروهی که اشیاء دایرکتوری را تغییر می‌دهد پشتیبانی می‌کند. دستور LDIFDE این عملیات گروهی را بااستفاده از فایل‌های LDIF پیاده‌سازی می‌کند.

فرمت فایل LDIF از یک بلوک خطی که با هم یک عملیات منفرد را تشکیل می‌دهند ساخته می‌شود. عملیات مختلف در یک فایل با یک خط خالی از هم جدا می‌شوند. هر خط شامل یک عملیات تشکیل شده از یک نام خصیصه همراه علامت ":" و مقدار خصیصه می‌باشد. مثلاً می‌خواهیم اشیاء کاربر را برای دو نماینده فروش بنام‌های April Stewart و Tony Krijnen منتقل کنیم. محتوای فایل LDIF چیزی شبیه به این خواهد بود :

```
Dn: CN=April Stewart,OU=People,DC=contoso,DC=com
ChangeType: add
CN: April Stewart
Objectclass: user
sAMAccountName: april.stewart
userPrincipleName: april.stewart@contoso.com
givenName: April
sn: Stewart
displayName: Stewart, April
mail: april.stewart@contoso.com
description: Sales Representative in the USA
Title: Sales Representative
Department: Sales
Company: Contoso, Ltd.

Dn: CN=Tony Krijnen,OU=People,DC=contoso,DC=com
ChangeType: add
CN: Tony Krijnen
Objectclass: user
sAMAccountName:tony.krijnen
userPrincipleName:  tony.krijnen@contoso.com
givenName: Tony
sn: krijnen
displayName: Krijnen, Tony
mail:  tony.krijnen@contoso.com
description: Sales Representative in the Netherlands
Title: Sales Representative
Department: Sales
Company: Contoso, Ltd.
```

هر عملیاتی با خصیصه DN شیء که مقصود عملیات است شروع می‌شود. خط بعدی ChangeType نوع عملیات را تعیین می‌کند :add (افزودن) ، modify (تغییر) و delete (حذف).

همانطور که مشاهده می‌شود فرمت فایل LDIF فرمت متنی با جداکننده کاما نیست ولی چون یک استاندارد است بسیاری از سرویس‌های دایرکتوری و بانک‌های اطلاعاتی می‌توانند از فایل‌های LDIF برای انتقال اشیاء استفاده کنند.

پس از ساخت یا تهیه فایل LDIF می‌توان عملیات تعریف شده در فایل را توسط دستور LDIFDE اجرا کرد. برای دریافت اطاعات کاربردی در این خصوص در خط فرمان تایپ کنید ldifde /? . دو تا از مهم‌ترین سوئیچ‌های فرمان عبارتند از:

- I- حالت انتقال از فایل را فعال می‌کند. بدون این پارامتر پیش فرض فرمان انتقال از Active Directory به سمت فایل است.
- f FileName- نام فایل LDIF را تعیین می‌کند.

برای مثال دستور زیر اشیاء را از فایل Newusers.ldf به Active Directory منتقل می‌کند.

```
Ldifde -I -f newusers.ldf
```

دستور تعداد زیادی از تغییرات را با استفاده از پارامترها قبول می‌کند. مفیدترین پارامترها در جدول ۳-۱ خلاصه شده‌اند.

جدول ۳- ۱ پارامترهای LDIFDE

دستور	کاربرد
پارامترهای عمومی	
-i	حالت انتقال از فایل
-f filename	نام فایل جهت انتقال اشیاء
-s servername	نام DC برای ارتباط
-c FromDN ToDN	رخداد FromDN را به ToDN تبدیل می‌کند زمانی به کار می‌اید که بعنوان مثال اشیاء را از دامنه دیگری منتقل کنیم
-v	حالت Verbose فعال می‌شود
-j path	محل فایل Log
-?	راهنما
پارامترهای انتقال به فایل	
-d RootDN	جستجوی ریشه LDAP . پیش فرض ریشه دامنه است
-r Filter	فیلتر جستجوی LDAP. پیش فرض همه اشیاء است (objectClass=*)
-p SearchScope	حوزه یا عمق جستجو. می‌تواند subtree (container و فرزندان آن)، base (اشیاء سطح اول container) یا onelevel (container و اشیاء سطح اول آن) باشد
-l list	لیست خصوصیات با جداکننده کاما برای درج در اشیاء نهایی . مفید برای زمانی که می‌خواهیم تعداد کمی خصلت را منتقل کنیم
-o list	لیست خصلت‌ها با جداکننده کاما برای حذف در اشیاء نهایی . مفید برای زمانی که بخواهیم همه خصلت‌ها را به استثنا چند تا منتقل کنیم
پارامترهای انتقال از فایل	
-k	از خطاها چشم‌پوشی می‌کند و روند ادامه می یابد وقتی خطای Constraint Violation یا Object Already Exists ظاهر می‌شود.

نکته امتحانی برای امتحان 70-640 باید بدانید هردو دستور CSVDE و LDIFDE کار انتقال اشیاء را با فرمت فایل خاص خودشان انجام می‌دهند. هردو در حالت پیش فرض کار انتقال را از Active Directory به فایل انجام می‌دهند و برای انتقال از فایل به Active Directory از پارامتر I– استفاده می شود.فقط LDIFDE قادر به تغییر اشیاء موجود یا حذف آنهاست. هیچ دستوری برای انتقال کلمه عبور موجود نیست. فقط در دستور Dsadd می‌توان کلمه عبور کاربر را

مشخص کرد .وقتی کاربری را با دستور CSVDE یا LDIFDE منتقل می‌کنیم حسابها غیر فعالند تا کلمات عبورشان وارد شده و آن زمن فعال می‌شود.

تمرینات خودکارسازی ساخت حساب‌های کاربری

در این تمرینات تعدادی کاربر با روشهای مطرح شده در این درس ساخته می‌شود. برای انجام تمرینات نیاز به اشیاء زیر در دامنه contoso.com داریم.

- OU سطح اول بنام People
- OU سطح اول بنام Groups
- یک گروه از نوع global security در Groups OU بنام Sales

تمرین ۱ ساخت کاربران با استفاده از یک الگوی حساب کاربری

در این تمرین یک الگوی حساب کاربری می‌سازیم که خصوصیات آن برای نمایندگان فروش آماده باشد. سپس یک حساب کاربری برای نماینده جدید فروش از طریق کپی الگو می‌سازیم.

۱. به SERCER01 با کاربر Administrator وارد می‌شویم.
۲. ابزار Active Directory Users And Computers و سپس گره دامنه را باز می‌کنیم.
۳. روی People OU کلیک راست کرده و New سپس User را انتخاب می‌کنیم.
۴. در کادر First Name عبارت Sales_ را تایپ می‌کنیم.
۵. در کادر Last Name عبارت Template را تایپ کنید.
۶. در کادر User Logon Name عبارت salestemlate_ را وارد کنید و کلید Next را می‌زنیم.
۷. یک کلمه عبور ترکیبی مطابق استاندارد مایکروسافت در کادرهای Password وConfirm Password وارد کنید.
۸. کادر Account Is Disabled را علامت بزنید. سپس Next و بعد Finish را کلیک کنید.

توجه کنید که علامت "_" قبل از نام حساب باعث می‌شود الگو در بالای لیست کاربران در People OU قرار گیرد. همچنین آیکن شیء کاربر علامت فلش به سمت پایین دارد که نشاندهنده غیرفعال بودن آن است.

۹. روی الگو دابل کلیک کنید تا کادر محاوره‌ای Properties باز شود.
۱۰. روی زبانه Organization کلیک کنید.
۱۱. در کادر Department تایپ کنید Sales.
۱۲. در کادر Company عبارت Contoso,Ltd را وارد کنید.
۱۳. روی زبانه Member Of کلیک کنید.
۱۴. کلید Add را می‌زنیم.
۱۵. تایپ می‌کنیم Sales و OK را می‌زنیم.
۱۶. روی زبانه Profile کلیک می‌کنیم.
۱۷. در کادر Profile Path عبارت \\Server01\profiles\%username% را تایپ می‌کنیم.
۱۸. OK می‌کنیم.

حالا یک حساب الگو برای ساخت کاربران جدید در واحد نمایندگان فروش داریم. حالا می‌خواهیم کاربر جدید را بر اساس الگو بسازیم.

۱۹. روی الگوی Sales_ کلیک راست کرده و copy را انتخاب می‌کنیم.

کادر محاوره‌ای Object-User ظاهر می‌شود.

۲۰. در کادر First Name تایپ می‌کنیم Jeff.
۲۱. در کادر Last Name تایپ می‌کنیم Ford.
۲۲. در کادر User Logon Name تایپ می‌کنیم jeff.ford و سپس کلید Next را می‌زنیم.
۲۳. یک کلمه عبور ترکیبی مطابق استاندارد مایکروسافت در کادرهای Password وConfirm Password وارد کنید.
۲۴. کادر Account Is Disabled را پاک کنید.

۲۵. Next و سپس Finish را کلیک می‌کنیم.

۲۶. پنجره properties حساب Jeff Ford را باز کرده و بررسی کنید آیا خصلتهای الگو در حساب جدید کپی شده است یا نه؟

تمرین ۲ ساخت کاربر با دستور Dsadd

در این تمرین با استفاده از دستور Dsadd حساب کاربری جدید برای Mike Fitzmaurice در OU People می‌سازیم.

۱. پنجره خط فرمان را باز می‌کنیم.

۲. دستورات زیر را در یک خط وارد کرده و کلید Enter را می‌زنیم:

```
Dsadd user "cn=Mike Fitzmaurice,ou=People,dc=contoso,dc=com" –samid mike.fitz –pwd * -mustchpwd yes -hmdir \\server01\users\%username%\documents -hmdrv u:
```

۳. در کادر باز شده دو بار کلمه عبور کاربر را وارد می‌کنیم. کلمه عبور ترکیبی با حداقل ۷ کاراکتر وارد می‌کنیم.

۴. ابزار Active Directory Users And Computers و سپس properties حساب Mike را باز می‌کنیم. بررسی می‌کنیم که آیا خصوصیات وارد شده در خط فرمان در حساب درج شده یا خیر.

تمرین ۳ انتقال کاربران با CSVDE

در دو تمرین قبلی هر بار یک کاربر ایجاد کردیم. در این تمرین از فایل متنی comma-delimited برای انتقال دو کاربر استفاده می‌کنیم.

۱. ابزار Notepad را باز کرده و سه خط زیر را وارد می‌کنیم. هر کدام از bullet ها نماینده یک خط است. Bullet ها را در فایل متنی وارد نمی‌کنیم.

- DN,objectClass,sAMAccountName,sn,givenName,userPrincipleName
- "cn=Lisa Andrews,ou=People,dc=contoso,dc=com",user,lisa.andrews,Lisa,Andrews,lisa.andrews@contoso.com
- "cn=David Jones,ou=People,dc=contoso,dc=com",user,david.jones,David,Jones,david.jones@contoso.com

۲. فایل را در پوشه Documents خود با نام Newusers.txt ذخیره کنید.

۳. پنجره خط فرمان را باز کنید.

۴. تایپ کنید cd %userprofile%\Documents و کلید Enter را بزنید.

۵. تایپ می‌کنیم csvde –I –f newusers.txt –k و Enter را می‌زنیم.

دو کاربر منتقل می‌شوند.اگر خطایی مشاهده شد در فایل متنی بدنبال غلط املایی می‌گردیم.

۶. ابزار Active Directory Users And Computers را باز می‌کنیم و وجود کاربران جدید را بررسی می‌کنیم.

اگر در طول اجرای تمرین ابزار مذکور باز بوده باشد برای مشاهده کاربران جدید صفحه را refresh می‌کنیم.

۷. حسابها را کنترل می‌کنیم و می‌بینیم آیا نام، نام خانوادگی، UPN و نام قبل از ویندوز 2000 مشابه ورودیهای ما در فایل NewUsers.txt هست یا نه.

تمرین ۴ انتقال کاربران با دستور LDIFDE

این دستور نیز مانند دستور قبلی برای انتقال کاربران استفاده می‌شود ولی یک فایل متنی جدا شونده نیست. در این تمرین برای ساخت دو کاربر از این دستور استفاده می شود.

۱. ابزار Notpad را باز کرده و خطوط زیر را تایپ می‌کنیم. افزودن یک خط خالی میان دو عملیات فراموش نشود.

```
Dn: CN=April Stewart,OU=People,DC=contoso,DC=com
ChangeType: add
CN: April Stewart
Objectclass: user
sAMAccountName: april.stewart
userPrincipleName: april.stewart@contoso.com
givenName: April
```

sn: Stewart
displayName: Stewart, April
mail: april.stewart@contoso.com
description: Sales Representative in the USA
Title: Sales Representative
Department: Sales
Company: Contoso, Ltd.

Dn: CN=Tony Krijnen,OU=People,DC=contoso,DC=com
ChangeType: add
CN: Tony Krijnen
Objectclass: user
sAMAccountName:tony.krijnen
userPrincipleName: tony.krijnen@contoso.com
givenName: Tony
sn: krijnen
displayName: Krijnen, Tony
mail: tony.krijnen@contoso.com
description: Sales Representative in the Netherlands
Title: Sales Representative
Department: Sales
Company: Contoso, Ltd.

۲. فایل را در پوشه Documents خود با نام Newusers.ldf ذخیره می‌کنیم. نام فایل را در گیومه قرار می‌دهیم تا Notepad پسوند .txt به آن اضافه نکند.

اگرچه امکان انتقال اشیاء داخل فایلهای LDIF با هر پسوندی وجود دارد ولی پسوند ldf بعنوان قرارداد پذیرفته شده است.

۳. پنجره خط فرمان را باز می‌کنیم.
۴. تایپ می‌کنیم cd %userprofile%\Documents و Enter را می‌زنیم.
۵. تایپ می‌کنیم ldifde –I –f newusers.ldf –k و Enter را می‌زنیم.

دو کاربر منتقل می‌شود. اگر خطایی مشاهده شد در فایل متنی بدنبال غلط املایی می‌گردیم

۶. ابزار Active Directory Users And Computers را باز می‌کنیم و وجود کاربران جدید را بررسی می‌کنیم.

اگر در طول اجرای تمرین ابزار مذکور باز بوده باشد برای مشاهده کاربران جدید صفحه را refresh می‌کنیم.

۷. حسابها را کنترل می‌کنیم و می‌بینیم آیا خصلتهای آنها مشابه ورودیهای ما در فایل NewUsers.ldf هست یا نه.

خلاصه درس

- برای ساخت کاربر جدید می‌توان از حساب کاربری در Active Directory کپی گرفت. در این پروسه یک سری از خصوصیات حساب کپی می‌شود. جهت ساخت الگوی حساب کاربری یک کاربر ساخته و خصوصیات آن را تعیین می‌کنیم. سپس حساب را غیرفعال می‌کنیم تا از آن برای ورود به شبکه استفاده نشود. از الگو کپی می‌گیریم و کاربر جدید ساخته می‌شود.
- دستور Dsadd جهت ساخت شیء کاربر از خط فرمان همراه پارامترهای مشخص کننده خصوصیات کاربر بکار می‌آید.
- امکان انتقال کاربران از فایل متنی comma-delimited و خصوصیات آنها با دستور CSVDE وجود دارد.
- از دستور LDIFDE برای اجرای عملیات ساخت، تغییر و حذف کاربر در Active Directory استفاده می‌شود. فایل LDIF که چنین عملیات را تعیین می‌کند دارای یک فرمت استاندارد است که امکان تبادل داده را بین دایرکتوری‌ها فراهم می‌کند.

سئوالات پایان درس

۱. شما مدیر شبکه یک دانشگاه بزرگ هستید و فایلی با فرمت Excel محتوی اطلاعات ۲۰۰۰ دانشجو به شما داده می‌شود. دو هفته بعد قرار است دانشجویان وارد دانشگاه شوند. شما باید در حداقل زمان حساب‌های کاربری جدید را برای دانشجویان بسازید. کدامیک از موارد زیر باید انجام شود؟

A. یک الگوی حساب کاربری ساخته و برای هر کاربر کپی می‌کنیم.
B. دستور LDIFDE –I را بکار می‌بریم.
C. دستور CSVDE –I را بکار می‌بریم
D. دستور DSADD USER را بکار می‌بریم.

۲. شما مدیر شبکه یک دانشگاه بزرگ هستید. کدام دستور برای حذف حساب‌های کاربری دانشجویان فارغ‌التحصیل کاربرد دارد؟

A. LDIFDE
B. Dsmod
C. DEL
D. CSVDE

درس ۲ : ساخت کاربر با استفاده از PowerShell ویندوز و VBScript

در درس ۱ یاد گرفتیم که چگونه از ابزارهای خط فرمان برای افزودن یا انتقال حسابهای کاربری استفاده کنیم. در این درس با دو ابزار قدرتمند در اجرا و خودکارسازی وظایف مدیریتی کار خواهیم کرد یکی PowerShell ویندوز و دیگری VBScript. هر دوی این ابزارها امکان ساخت اسکریپتهای خودکارسازی ساخت حساب‌های کاربری را فراهم می‌کنند. PowerShell ویندوز هم بعنوان یک محیط خط فرمان پیشرفته امکان ساخت کاربر را دارد.

بعد از این درس شما می‌توانید:

- ویژگی Windows PowerShell را روی ویندوز سرور 2008 نصب کنید.
- اجزاء کلیدی شکل دستوری PowerShell ویندوز را شامل cmdlets، variables، aliases و namespaces و providers تعیین کنید.
- در PowerShell ویندوز کاربر بسازید.
- در VBScript کاربر بسازید.

زمان تقریبی : ۷۵ دقیقه

معرفی PowerShell ویندوز

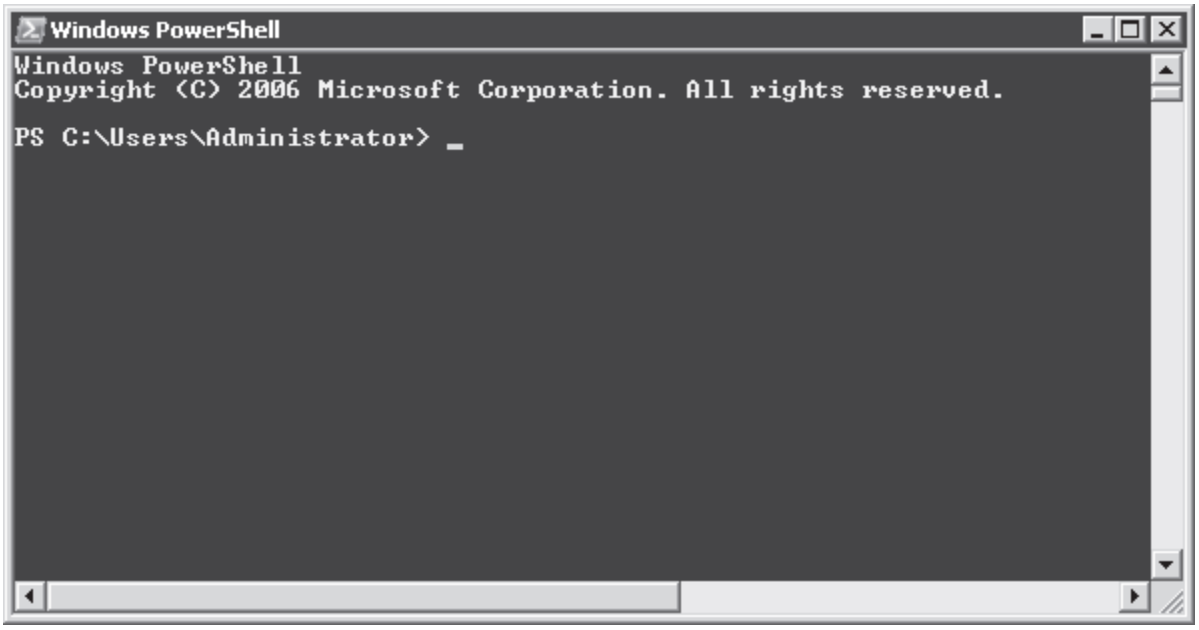
PowerShell ویندوز ابزاری است قدرتمند برای اجرا و خودکارسازی عملیات مدیریتی در ویندوز سرور 2008.

تکته امتحانی در این بخش ما با PowerShell ویندوز آشنا می شویم. در امتحان 70-640 از ما انتظار نمی رود بتوانیم اسکریپتهای PowerShell ویندوز را بسازیم ولی باید cmdlets (دستورات) مورد استفاده در کارکرد ابتدایی با Active Directory را مانند مواردی که در این کتاب بحث می‌شود بشناسیم. برای یادگیری کامل PowerShell ویندوز به Windows PowerShell Scripting Guide نوشته Ed Wilson (انتشارات مایکروسافت ، 2008) مراجعه نمایید.

PowerShell ویندوز هم یک پوسته خط فرمان و هم زبان اسکریپت نویسی با بیش از ۱۳۰ ابزار خط فرمان بنام cmdlet می باشد. این ابزارها از شکل فرمان و قواعد نام‌گذاری کاملاً سازگار تبعیت می‌کنند و با cmdlet های سفارشی قابل توسعه هستند. برخلاف command shell های قدیمی مانند cmd.exe در ویندوز یا BASH در یونیکس که با ارسال دستور متنی به یک پردازه یا برنامه مجزا و برگشت نتیجه دستور بصورت متن کار می‌کرد PowerShell ویندوز مستقیماً اشیاء Microsoft .NET Framework را در خط فرمان دستکاری می‌کند.

PowerShell ویندوز بعنوان یک ویژگی در ویندوز سرور 2008 نصب می‌شود. برای نصب آن Server Manager را باز کرده و روی پیوند Add Features کلیک می‌کنیم. پس از نصب آن را از منوی شروع باز می‌کنیم. برای دسترسی راحتتر به این پوسته

قدرتمند از آن یک میانبر می‌سازیم. برای اینکار روی Windows PowerShell در گروه برنامه Windows PowerShell کلیک راست کرده و گزینه Pin To Start Menu را انتخاب می‌کنیم. محیط PowerShell ویندوز خیلی شبیه به خط فرمان cmd.exe می‌باشد با این تفاوت که رنگ پیش‌زمینه آن آبی تیره بوده و prompt آن دارای عبارت PS است. شکل ۳- ۱ PowerShell ویندوز را نمایش می‌دهد.



شکل ۱- ۳ کنسول Windows PowerShell

توجه یک ویندوز ، یک shell PowerShell ویندوز به ما این امکان را می‌دهد که از دستورهای خط فرمان قدیمی استفاده کنیم. بنابراین PowerShell ویندوز سازگار با تکنولوژی‌های قدیمی نیز می باشد. اگر از PowerShell ویندوز استفاده کنیم برای انجام وظایف مدیریتی می‌توانیم دستورات قدیمی cmd.exe ویا دستورات PowerShell ویندوز را وارد کنیم.

شکل فرمان، cmdlet و اشیاء PowerShell ویندوز

در محیط‌های قدیمی مانند cmd.exe از دستوراتی نظیر dir یا copy استفاده می‌شود که به ابزارهای موجود دسترسی پیدا می‌کند و یا برنامه‌های اجرایی نظیر attrib.exe و xcopy را صدا می‌زنند. بسیاری از این‌ها پارامترهایی را از خط فرمان می‌گیرند و بازخورد آن را به شکل خروجی، خطا و کد خطا برمی‌گرداند.

در PowerShell ویندوز دستورات توسط cmdlets صادر می‌شوند. cmdlet یک دستور تک ویژگی است که شیء را دستکاری می‌کند. Cmdlet ها از شکل فعل- اسم استفاده می‌کنند یعنی یک فعل و یک اسم که با یک خط تیره از هم جدا می شوند. مثال‌ها شامل Get-Service و Start-Service هستند.

توجه cmdlet از ورود مستقیم و اسکریپت نویسی پشتیبانی می‌کند.

Cmdlets می‌تواند مستقیماً در PowerShell ویندوز تایپ شوند یا در فایلهای اسکریپت (*.PSL) ذخیره شوندکه بعداً توسط PowerShell ویندوز اجرا گردند.

شیء چیست؟

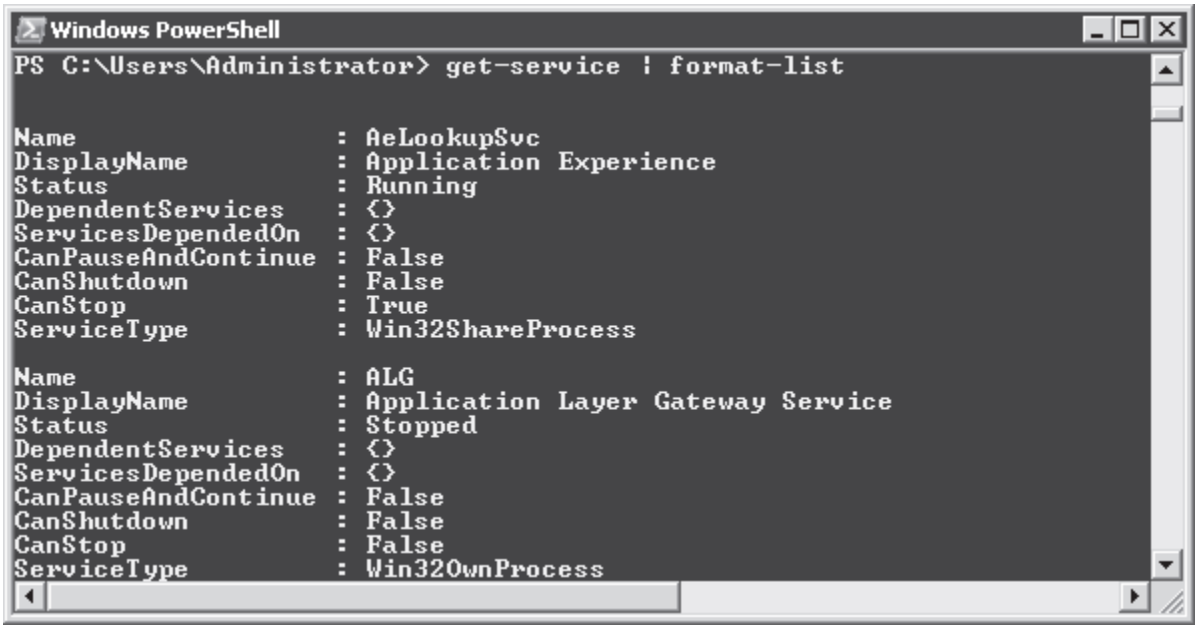
شیء یک ساختار برنامه‌نویسی است. از دیدگاه فنی شیء .NET یک instance از کلاس .NET است که شامل داده و عملکردهای مربوط به آن می‌باشد. در واقع به نوعی می‌توان شیء را نمایش مجازی از منابع در نظر گرفت. بعنوان مثال وقتی از Get-Service cmdlet در PowerShell ویندوز استفاده می‌کنیم، cmdlet یک یا چند شیء را که نماینده اشیاء هستند برمی‌گرداند. اشیاء می‌توانند properties داشته باشند که داده را نمایش می‌دهد و توسط منابع فراهم می‌شود. هر شیء نمایانگر یک سرویس است مثلاً خصوصیاتی برای نام سرویس و وضعیت startup آن دارد. وقتی یک خصیصه را دریافت می‌کنیم یعنی داده آن منبع را بدست می‌آوریم. وقتی یک خصیصه را پیکربندی می‌کنیم در واقع آن داده را در منبع رونویسی می‌کنیم.

اشیاء متد (method) هم دارند. متدها عملکرد اجرایی روی شیء هستند. بعنوان مثال شیء سرویس متدهای start و stop دارد. وقتی متدی روی شیء که نماینده منبع است اجرا می‌شود در اصل اتفاق روی خود منبع می‌افتد.

این cmdlet ها فرامین یا پارامترها را به ابزارها و برنامه‌های دیگر نمی‌فرستند و در عوض آنها را روی اشیاء .NET اجرا می‌کنند. وقتی cmdlet Get-Service را تایپ می‌کنیم PowerShell ویندوز مجموعه‌ای از اشیاء را برای تمام سرویسها برمی‌گرداند. نتیجه cmdlet به صورت جدول سرویسها و نام آنها همانند شکل ۳- ۲ نمایش داده می‌شود.

شکل ۲- ۳ Get-Service cmdlet

با ترکیب این دستورات ساده می‌توان دستورات پیچیده ساخت. بعنوان مثال ترکیب Get-Service با Format-List همانند شکل ۳- ۳ نتیجه‌ای متفاوت بدست می‌دهد.



شکل ۳- ۳ Format-List cmdlet که روی مجموعه ساخته شده توسط Ger-Service اجرا می‌شود.

توجه داشته باشید که Format-List cmdlet جزئیات بیشتری را از خروجی پیش فرض Get-Service cmdlet نمایش می‌دهد. این حاوی نکته مهمی است. Get-Service cmdlet فقط لیستی از سه خصیصه مربوط به سرویسها را برنمی‌گرداند. این cmdlet اشیاء نمایانگر سرویسها را برمی‌گرداند. وقتی اشیاء به Format-List cmdlet ارسال می‌شوند این cmdlet می‌تواند به طور مستقیم با آنها کارکند و تمام خصیصه‌های آنها را نمایش دهد.

نکته دقیق ولی متفاوت

این محیط با محیط دستوری استاندارد ویندوز کاملاً متفاوت است. در آن محیط خروجی یک دستور درحالی که با دستور دیگر ترکیب شده است فقط می‌تواند متنی باشد. اگر فرضاً مثالهای بالا در محیط cmd.exe اجرا می‌شد دستور "formt list" فقط می‌توانست سه بخش از اطلاعات را که از دستور "get-service" گرفته با قالبی متفاوت نمایش دهد.

Format-List cmdlet تصمیم می‌گیرد که کدام خصیصه‌ها را نمایش دهد. ما می‌توانیم با افزودن پارامتر با یک مقدار "*" آنرا طوری هدایت کنیم تا مانند مثال زیر همه خصوصیات همه سرویسها را لیست کند.

```
Get-service |  format-list  -property *
```

استفاده از راهنما

Get-Help cmdlet از PowerShell ویندوز بهترین محل برای شروع بررسی اطلاعات خصوصاً برای کسانی است که کار با PowerShell ویندوز را تازه شروع کرده‌اند. ساده‌ترین شکل راهنما تایپ Get-Help cmdlet به همراه نام cmdlet مورد نظر است برای مثال :

```
Get-help get-service
```

با افزودن پارامترهای detailed یا full امکان دریافت راهنمایی بیشتر وجود دارد. مثلاً get-help get-command –detailed یا get-help get-command –full .

استفاده از متغیرها

وقتی با تعریف شیء یا مسیر تکراری مواجه هستیم می‌توانیم از متغیر استفاده کنیم. متغیرها در PowerShell ویندوز همیشه با علامت دلار ($) شروع می‌شوند. برای مثال می‌توانیم متغیر $DNS را به عنوان جایگزین شیء بدست آمده از Get- cmdlet Service DNS استفاده کرد :

```
$DNS=get-service DNS
```

وقتی یک شیء به متغیر نسبت داده می‌شود یک object reference ساخته می‌شود. خصوصیات این شیء توسط علامت نقطه قبل از نام خصیصه قابل دستیابی است. برای مثال جهت دستیابی به وضعیت (status) سرویس cmdlet DNS زیر را تایپ کنید :

```
$DNS.status
```

یک pipeline variable خاص بعنوان یک نگهدارنده فضای شیء فعلی در pipeline فعلی بکار می رود. این pipeline variable علامت "$_" می باشد. مثلاً برای بدست آوردن لیست همه سرویسهای جاری دستور زیر بکار می رود :

```
Get-services- | where=object { $_.status –eq "Running"}
```

این دستور همه سرویسها را برمیگرداند و اشیاء را به Where-Object cmdlet می‌فرستد. خصیصه وضعیت همه اشیاء ارائه شده توسط pipeline variable بررسی می شود آنهایی که خصیصه وضعیتشان مساوی با Running است نمایش داده می شوند.

استفاده از نامهای مستعار

نام مستعار روش جایگزین ارجاع به cmdlet می‌باشد. مثلاً where-object cmdlet که قبلاً استفاده شد نام مستعاری دارد بنام where . شکل خلاصه کد قبلی به شکل زیر است:

```
Get-service | where {$_.status –eq "Running"}
```

بسیاری از cmdlet های PowerShell ویندوز دارای اسامی مستعار هستند. بعنوان مثال cmdletی که محتوای پوشه را روی یک دیسک نشان می‌دهد Get-ChildItem نام دارد. این cmdlet نام مستعارِ Dir را دارد که همنام دستور محیط فرمان قدیمی ویندوز و Ls نام مستعار دیگر آن است که برای کاربران آشنا به UNIX طاحی شده است.

چطور می‌توان فهمید کدام cmdlet به کدام نام مستعار تعلق دارد؟ مانند مثال دستور alias را تایپ می‌کنیم

```
Alias  dir
```

خروجی مشخص می‌سازد که Dir نام مستعار Get-Children است.

اگرچه PowerShell ویندوز نام‌های مستعار را در محیط دستوری فراهم می‌کند ولی cmdlet ها، پارامترهای مشابه دستورات Cmd.exe را قبول نمی‌کند. برای مثال برای نمایش لیست پوشه‌ها و تمام محتویات آنها در خط فرمان عبارت dir/s را تایپ می‌کنیم و در PowerShell ویندوز عبارت dir –recurse را تایپ می‌کنیم.

فضای اسمی، Provider و PSDrive

Cmdlet ها در فضای اسمی روی اشیاء عمل می‌کنند. یک پوشه روی دیسک مثالی از یک فضای اسم است. فضای اسم یک ساختار سلسله مراتبی بوده که قابل پیمایش است. فضاهای اسمی توسط provider ها ساخته می‌شود. که می‌توان آنها را درایور در نظر گرفت. مثلاً فایل سیستم یک PowerShell provider دارد همانطور که رجیستری دارد بنابراین PowerShell ویندوز می‌تواند مستقیماً به اشیاء در فضای اسمی آن provider ها دسترسی داشته باشد و آنها را دستکاری کند.

شما قطعاً با مفهوم نمایش فضای اسم درایو دیسک با یک drive letter یا نمایش یک فضای نام پوشه به اشتراک گذاشته شده بعنوان درایو map شده آشنا هستید. در powerShell ویندوز فضاهای اسمی از هر provider بعنوان PSDrive قابل نمایش است. PowerShell ویندوز بطور خودکار یک PSDrive از قبل تعریف شده برای هر drive letter می‌سازد.

PowerShell ویندوز این مفهوم را با ساخت PSDrive های دیگر به یک سطح بالاتر منتقل می‌کند. برای مثال دو درایو با نامهای HKCU و HKLM به ازای Hive های رجیستری HKEY_CURRENT_USER و HKEY_LOCAL_MACHINE می‌سازد. حالا ما می‌توانیم در رجیستری جولان بدهیم و همانند یک سیستم فایل آنها را دستکاری کنیم. در PowerShell ویندوز تایپ می‌کنیم :

```
Cd hklm:\software
Dir
```

برای نامهای مستعار، environment، گواهینامه‌ها، عملیات و متغیرها نیز درایو ساخته می‌شود. برای مشاهده لیست PSDrive ها تایپ می‌کنیم get-psdrive .

ساخت کاربر با PowerShell ویندوز

حالا یاد می‌گیریم که چطور از PowerShell ویندوز برای ساخت کاربر در Active Directory استفاده کنیم. ابتدایی‌ترین اسکریپت PowerShell ویندوز برای ساخت یک کاربر چیزی شبیه به این است :

```
$objOU=[ADSI]"LDAP://OU=People,DC=contoso.com"
$objUser=$objOU.Create("user",CN=Mary North")
$objUser.Put("sAMAccountName","mary.north")
$objUser.SetInfo()
```

این مثال چهار مرحله ابتدایی ساخت یک شیء را در Active Directory با PowerShell ویندوز نشان می‌دهد:

۱. به container متصل می‌شویم مثلاً OU که شیء در آن ساخته می‌شود.
۲. متد Create container را با پارامترهای کلاس شیء و RDN شیء جدید اجرا می‌کنیم.
۳. خصلت‌های شیء را با متد Put تعیین می‌کنیم.
۴. تغییرات را با متد SetInfo در Active Directory اعمال می‌کنیم.

هر کدام از این مراحل در بخش‌های زیر شرح داده می‌شود.

اتصال به یک container در Active Directory

جهت ساخت یک شیء مانند کاربر container مورد نظر را پیدا می‌کنیم و متد مربوطه را اجرا می‌کنیم. پس مرحله اول اتصال به container است. PowerShell ویندوز ازمبدل نوع Active Directory Services Interface (ADSI) برای برقراری ارتباط با اشیاء Active Directory استفاده می‌کند. مبدل نوع (type adapter) مبدلی است بین ذات پیچیده یا گاهی عجیب و غریب اشیاء .NET Framework. و ساختار ساده PowerShell ویندوز. برای اتصال به یک شیء Active diectory یک رشته پرس و جوی LDAP ارسال می‌گردد که در واقع یک نام پروتکل LDAP:// به همراه DN شیء می‌باشد. بنابراین اولین خط کد زیر است:

```
$objOU=[ADSI]"LDAP://OU=People,DC=contoso.com"
```

PowerShell ویندوز از نوع مبدل ADSI برای ساخت یک مرجع شیء به People OU استفاده می‌کند و آن را به یک متغیر نسبت می‌دهد. نام متغیر objOU استانداردهای برنامه‌نویسی را منعکس می‌کند که یک پیشوند سه حرفی نوع متغیر را تعیین می‌کند ولی نام متغیر می‌تواند هر چیزی باشد به شرطی که با "$" شروع شود.

اجرای متد Create

در این جا متغیر $objOU یک مرجع به People OU است. حالا می‌توانیم از container بخواهیم تا با متد Create شیء را بسازد. این متد دو پارامتر را به عنوان آرگومان ارسال می‌کند: یکی کلاس شیء و دیگری RDN شیء. RDN شیء قسمتی از نام

است که قبل از container والد می‌آید. بیشتر کلاسهای شیء از شکل CN=object name بعنوان RDN استفاده می‌کنند.
RDN یک OU بصورت OU=organizational unit name و RDN یک دامنه بشکل DC=domain name می‌باشد.
بنابراین خط زیر یک شیء کاربر با RDN ، CN=Mary North می‌سازد.

```
$objUser=$objOU.Create("user",CN=Mary North")
```

شیء ایجاد شده به متغیر $objUser نسبت داده می‌شود که نماینده شیء بوده و امکان دستکاری آن را به ما می دهد.

تعیین خصوصیات کاربر

به خاطر داشته باشید که شیء جدید و تغییرات تا اعمال نشود ذخیره نمی‌شود و تا همه خصلت‌های مورد نیاز تعیین نشود تغییرات اعمال نمی‌شود. خصیصه ضروری برای شیء کاربر نام کاربری قبل از 2000 است. نام LDAP این خصیصه sAMAccountName می‌باشد. بنابراین در خط بعدی، sAMAccountName با استفاده از متد Put به شیء نسبت داده می‌شود. Put یک متد استاندارد برای ثبت خصیصه در یک شیء می‌باشد. کد نهایی بصورت زیر خواهد شد:

```
$objUser.Put("sAMAccountName","mary.north")
```

خصیصه‌های اجباری دیگری نیز برای شیء کاربر وجود دارد مانند Security Identifier (SID) ولی بطور خودکار توسط Active Directory هنگام اعمال تغییرات ساخته می‌شود.

اعمال تغییرات با متد SetInfo

برای اعمال تغییرات از متد SetInfo بشکل زیر استفاده می‌شود :

```
$objUser.SetInfo()
```

ثبت خصوصیات اضافی برای کاربر

دستورات قبلی فقط خصیصه اجباری sAMAccountName را پیکربندی می‌کند. می‌توانیم خصیصه‌های دیگری را هنگام ساخت کاربر مشخص کنیم. حالا یاد می‌گیریم از متد Put برای اینکار استفاده کنیم. فقط کافی است همان متد را برای خصیصه‌های مورد نظر تکرار کنیم:

```
$objUser.put("sAMAccountName",$samAccountName)
$objUser.put("userPrincipalName",$userPrincipleName)
$objUser.put("displayName",$displayName)
$objUser.put("givenName",$givenName)
$objUser.put("sn",$sn)
$objUser.put("description",$description)
$objUser.put("company",$company)
$objUser.put("department",$department)
$objUser.put("title",$title)
$objUser.put("mail",$mail)
$objUser.SetInfo()
```

دستورات بالا هر کدام مقدار ذخیره شده در متغیر را به عنوان مقدار خصیصه درج می‌کند. متد SetInfo را برای اعمال تغییرات فراموش نکنید. تا زمانی که این دستور را بکار نبریم تغییرات ذخیره نمی‌شود. این متد صحت مقادیر ورودی را بررسی می‌کند. اگر مقدار اشتباه برای یک خصیصه مشخص شده باشد در خط SetInfo() با خطا مواجه می‌شویم. متد GetInfo() تغییرات را بی‌اثر می‌کند.
اگر نام LDAP یک خصیصه را نمی‌دانیم روی زبانه Attribute Editor در ابزار Active Directory Users And Computers کلیک می‌کنیم. این زبانه وقتی دیده می‌شود که Advanced Features از منوی View انتخاب شده باشد. Attribute Editor همه خصیصه‌های شیء را شامل نام LDAP و مقدار آنها را نمایش می‌دهد. همچنین می‌توان از دستورات زیر برای اینکار استفاده کرد:

```
$objUser.psbase.properties
$objUser | get-mamber
```

نکته خصلتهای چند مقداره وضعیتی متفاوت دارند

اگرچه بیشتر خصلتهای کاربر تک مقدار هستند ولی بعضی نیز چند مقداره هستند. وقتی یک خصلت چند مقدار داشته باشد از متد PutEx() استفاده می‌کنیم. با جستجوی کلیدواژه زیر در اینترنت منابع متعددی را برای راهنمایی در مورد خصلتهای چند مقداره پیدا خواهید کرد

PowerShell user array PutEx

ما نمی‌توانیم با استفاده از متد Put کلمه عبور کاربر را تعیین کنیم و بجای آن از متد SetPassword طبق دستور زیر استفاده می‌کنیم:

```
$objUser.SetPassword("C0mp!exP@ssw0rd")
```

متاسفانه این متد پس از ساخت کاربر و اعمال تغییرات کاربرد دارد یعنی ساخت کاربر قبل از تنظیم کلمه عبور انجام می‌شود. این یک ایراد یا محدودیت PowerShell ویندوز نیست واقعیت Kerberos و LDAP است. بهرحال به اندازه کافی امن است چون کاربر پس از ساخت غیر فعال است.

حالا باید حساب را فعال کنیم. وضعیت یک حساب را یک پرچم (flag) مشخص می‌کند که با دستور Put دستکاری نمی‌شود. بجای آن از دستور زیر استفاده می‌کنیم:

```
$objUser.psbase.invokeSet("AccountDisabled",$false)
$objUser.SetInfo()
```

انتقال کاربران از بانک اطلاعاتی با PowerShell ویندوز

اگرچه یاد گرفتن انتقال اشیاء از بانک اطلاعاتی در آزمون 70-640 ضروری نیست ولی در خودکارسازی ساخت کاربر به ما کمک می‌کند. همانطور که خواهید دید فقط با چند خط کد اضافی با cmdlet های قدرتمند PowerShell ویندوز این کار را انجام می‌دهیم.

فرض می‌کنیم یک فایل Excel از بخش منابع انسانی محتوی کارمندان تازه استخدام شده تحویل گرفته‌ایم. Excel می‌تواند فایل را بصورت comma-delimited متنی (.CSV) ذخیره کند که با PowerShell ویندوز قابل انتقال است. خط اول فایل CSV. باید دارای نام فیلدها و سپس اطلاعات کاربران باشد. بعنوان یک مثال ساده فایل csv. زیر را با نام Newusers.csv در نظر بگیرید:

Newusers.csv

```
Cn,sAMAccountName,FirstName,LastName
John Woods,john.woods,Johnathan,Woods
Kim Akers,kim.akers,Kimberly,Akers
```

توجه کنید که نیازی نیست نام فیلدها با نام خصیصه‌ها در LDAP یکی باشد. قرار است آنها توسط اسکریپت به نام خصیصه ها نگاشت شوند.

PowerShell ویندوز می‌تواند این منبع داده را با یک دستور منتقل کند:

```
$dataSource=import-csv "newusers.csv"
```

پس از انتقال منبع داده باید رکوردها را در حلقه قرار دهیم. این کار به شکل زیر با یک بلوک foreach انجام می‌شود:

```
Foreach($dataRecord in $datasource)
{
    # do whatever you want to do
}
```

یک Cmdlet با نام ForEach حلقه را ایجاد می‌کند و شیء حاضر را به متغیر $dataRecord نسبت می‌دهد بنابراین متغیر $dataRecord نماینده رکورد جاری است. ما می‌توانیم فیلدهای واقعی در هر رکورد مشاهده کنیم که خصوصیات متغیر $dataRecord را تشکیل می‌دهد. برای مثال نام اولین کاریر هست:

```
$dataRecord.FirstName
```

می‌توانیم آن را به یک متغیر نسبت دهیم:

```
$givenName=$datarecord.FirstName
```

باز هم نیازی نیست نام فیلد یا متغیر با نام خصیصه در LDAP یکی باشد. وقتی ما متغیر حاوی مقدار را در خصیصه خودش ثبت می‌کنیم عمل نگاشت انجام می‌شود:

```
$objUser.Put("givenName",$givenName)
```

خصلت LDAP با نام givenName در گیومه قرار می‌گیرد. فقط زمانی که به خصوصیت واقعی یک شیء ارجاع می‌دهیم باید از نام واقعی استفاده کنیم. بهرحال وقتی نام فیلدهای منبع داده و نام متغیرها نام خصیصه‌ها را منعکس می‌کند راحت‌تر اینست که از کد پیروی کنیم.

با کنار هم گذاشتن این مطالب می‌توانیم اسکریپت انتقال کاربر را بنویسیم:

Userimport.psl

```
$objOU=[ADSI]"LDAP://OU=People,DC=contoso,DC=com"
$dataSource=import-csv "NewUsers.csv"
Foreach($dataRecord in $datasource) {
        #map variables to data source
        $cn=$dataRecord.cn
        $sAMAccountName=$dataRecord.sAMAccountName
        $givenName=$dataRecord.FirstName
        $sn=$dataRecord.LastName
        $displayName=$sn + ", " + $givenName
        $userPrincipleName=$givenName + "." + $sn + "@contoso.com"

        #create the user object
        $objUser=$objOU.Create("user","CN="+$cn)
        $objUser.Put("sAmaccountName",$sAMAccountName)
        $objUser.Put("userPrincipleName",$userPrincipleName)
        $objUser.Put("displayName",$displayName)
        $objUser.Put("givenName",$givenName)
        $objUser.Put("sn",$sn)
        $objUser.SetInfo()
        $objUser.SetPassword("C0mp!P@ssw0rd")
        $objUser.psbase.InvokeSet("AccountDisabled",$False)
        $objUser.SetInfo()
}
```

خط اول اسکریپت اتصال به containerای را ایجاد می‌کند که کاربران جدید در آن ساخته می‌شوند. دو خط بعدی اتصال به منبع داده و حلقه را برقرار می‌کند تا هر رکورد به یک متغیر $dataRecord نسبت داده شود. بلوک foreach دو کار را انجام می‌دهد . اول فیلدهای منبع داده را به متغیرها نگاشت می‌کند. سپس کاربر را می‌سازد.

توجه داشته باشید که بعضی متغیرها با ترکیب دو فیلد ساخته می‌شود. متغیر $displayName قالب LastName, FirstName را بخود می‌گیرد و متغیر $userPrincipleName قالب FirstName.LastName@contoso.com را به خود می‌گیرد.

کاربر با اعمال متد Create از متدهای OU ساخته می‌شود. خصیصه‌های کاربر تعیین و اعمال شده و سپس کلمه عبور تعیین و حساب فعال می‌شود.

اجرای اسکریپت PowerShell ویندوز

بطور پیش‌فرض PowerShell ویندوز از اجرای اسکریپت‌ها به دلایل امنیتی جلوگیری می‌کند. برای اجرای یک اسکریپت که خود ساخته‌اید باید با دستور زیر سیاست اجرایی PowerShell ویندوز را تغییر دهید:

```
Set-executionpolicy remotesigned
```

سیاست اجرایی مشخص می‌کند کدام اسکریپت‌ها اجرا شوند. دستور فوق PowerShell ویندوز را طوری پیکربندی می‌کند اسکریپتهای محلی اجرا شود ولی اسکریپت‌های دیگر نیاز به ثبت داشته باشند. تغییر سیاستهای اجرایی بار امنیتی دارد بنابراین بهتر است اطلاعات مربوط به اجرای اسکریپت‌های PowerShell ویندوز را در آدرس http://www.microsoft.com/technet/scriptcenter/topics/winpsh/manual/run.mspx#EXC مطالعه کنید.

پس از تنظیم سیاستهای اجرایی می‌توانیم اسکریپت را اجرا کنیم. ولی اجرای آن با نام تنها خطایی به همراه دارد. باید مسیر اسکریپت را مشخص کنیم. میانبری وجود دارد که از نماد .\scriptname استفاده می‌کند که دایرکتوری جاری را نشان می‌دهد بنابراین دستور زیر اسکریپت انتقال کاریر را اجرا می‌کند:

```
.\UserImport.psl
```

معرفی VBScript

VBScript یک زبان اسکریپت نویسی می‌باشد که خودکارسازی وظایف مدیریتی را روی تمام نسخه‌های جاری ویندوز پشتیبانی می‌کند. فایل‌های VBScript متنی هستند و عموما با Notepad یا ویرایشگر اسکریپت ویرایش و با پسوند vbs ذخیره شده‌اند. برای اجرای یک اسکریپت روی آن دابل کلیک می‌کنیم تا با Wscript.exe باز شود بجای آن می‌توان از خط فرمان اسکریپت را بشکل زیر اجراکرد:

```
Cscript.exe  scriptname
```

هم Wscript.exe و هم Cscript.exe کامپوننتهای Windows Scripting Host (WSH) هستند که automation framework نصب شده روی تمام نسخه‌های جاری ویندوز می‌باشند و از زبان‌های اسکریپت‌نویسی متعددی از جمله VBScript پشتیبانی می‌کنند.

ساخت کاربر با VBScript

چون VBScript از رابط ADSI برای دستکاری Active Directory استفاده می‌کند مراحل ساخت کاربر در VBScript دقیقا مشابه PowerShell ویندوز است. کد زیر یک اسکریپت ساده ساخت کاربر است:

```
Set  obj=Getobject("LDAP://OU=People,DC=contoso,DC=com")
Set  objUser=objOU.Create("user","CN=Mary North")
objUser.Put "sAMAccountName","mary.north"
objUser.SetInfo()
```

ابتدا اتصال به container که همان OU مقصد است ایجاد می‌شود. VBScript از عبارت GetObject برای اتصال به یک شیء ADSI با DN استفاده می‌شود. وقتی در VBScriptیک شیء به یک متغیر منتسب می‌شود برای ایجاد مرجع شیء از عبارت Set استفاده می‌گردد.

خط دوم کد متد OU Create را به منظور ساخت شیء از یک کلاس مشخص و با DN مشخص اجرا می‌کند درست مانند مثال PowerShell ویندوز . چون نتیجه متد یک شیء است باید از عبارت Set برای نسبت دادن مرجع شیء به متغیر استفاده کنیم.

خط سوم از متد Put استفاده می‌کند ولی VBScript از پرانتز برای فرستادن پارامترها به آرگومان استفاده نمی‌کند. خط چهارم مانند PowerShell ویندوز تغییرات را اعمال می‌کند. اسکریپت را با نام Newuser.vbs ذخیره کرده و از خط فرمان یا PowerShell ویندوز آن را اجرا کنید به این صورت :

```
Cscript.exe  newusers.vbs
```

مقایسه VBScript و PowerShell ویندوز

VBScript نسبت به PowerShell ویندوز دو مزیت دارد. اول اینکه اسکریپت‌های VBScript توسط WSH روی تمام نسخه‌های ویندوز قابل اجراست در حالی که PowerShell ویندوز باید دانلود و روی نسخه‌های ویندوز قبل از 2008 نصب شود. از طرفی نیاز به NET Framework. نسخه ۲ یا بالاتر دارد. مزیت دوم استفاده مستمر طی سالیان بسیار می‌باشد. در نتیجه تجربیات و دانش بسیاری در این زمینه موجود است.

از طرفی WSH نمی‌تواند محیطی را برای اجرای مستقیم دستورات فراهم کند. بعلاوه VBScript بعنوان یک زبان آن قدر قوی نیست و بطور کامل از NET Framework. استفاده نمی‌کند. اگرچه WSH روی ویندوز 2008 و VBScript هنوز پشتیبانی می‌شود ولی راه آینده PowerShell ویندوز است. به همین دلیل در این درس اول ارائه شد.

معایب PowerShell ویندوز درست معکوس مزایای VBScript است. تازگی PowerShell ویندوز بدین معنی است که در حال توسعه است. در بخش‌های پیشین یاد گرفتیم با PowerShell ویندوز کاربر بسازیم. تکنیک‌ها و کدهایی که یاد گرفتیم انصافا پیچیده بودند. در حقیقت آنها تقریبا شبیه VBScript هستند.

بهمین علت در نسخه‌های فعلی PowerSell ویندوز از مدیریت Active Directory بصورت محدود پشتیبانی می‌شود. برخلاف Windows Management PowerShell (WMI) و Microsoft Exchange Server که دارای PowerShell provider های قدرتمندی هستند پشتیبانی از Active Directory به مبدل نوع ADSI محدود می‌شود که پیچیده و عجیب غریب است و مانند VBScript به ADSI متکی است. در نسخه‌های بعدی PowerShell ویندوز نوعی Active Directory provider معرفی خواهد شد که کار کردن با اشیاء Active Directory را همانند کار کردن با فایلها در فایل سیستم آسان می‌سازد.

بخاطر داشته باشید که در امتحان 70-640 انتظار نمی‌رود در PowerShell ویندوز یا VBScript بتوانید اسکریپت بسازید بلکه باید بتوانید مراحل تکمیل یک اسکریپت را برشمارید: اتصال به OU، ساخت شیء، تعیین خصوصیات و نهایتا اعمال تغییرات.

تمرینات ساخت کاربر با PowerShell ویندوز و VBScript

در این تمرینات قرار است با استفاده از متدهای خودکارسازی که تشریح شد تعدادی کاربر بسازیم. برای انجام این تمرینات نیاز به شیء واحدسازمانی به‌نام People در دامنه contoso.com داریم.

تمرین ۱ نصب PowerShell ویندوز

برای انجام تمارین که از PowerShell ویندوز برای انجام وظایف مدیریتی استفاده می‌کند در این تمرین ویژگی PowerShell ویندوز را نصب می‌کنیم.

۱. Server Manager را باز می‌کنیم.
۲. گره Features را در کنسول باز می‌کنیم.
۳. روی پیوند Add Features کلیک کنید.
۴. PowerShell ویندوز را از لیست Features انتخاب می‌کنیم و Next را می‌زنیم.
۵. روی دکمه Install کلیک می‌کنیم.
۶. وقتی نصب تمام شد Close را می‌زنیم.
۷. در گروه برنامه PowerShell ویندوز روی Windows PowerShell کلیک راست می‌کنیم و گزینه Pin To Start Menu را انتخاب می‌کنیم.

تمرین ۲ ساخت کاربر با PowerShell ویندوز

حالا که PowerShell ویندوز نصب شده از آن برای ساخت کاربر در Active Directory استفاده می‌کنیم.

۱. PowerShell ویندوز را باز کنید.
۲. با درج دستور زیر به OU People متصل می‌شویم:
```
$objOU=[ADSI]"LDAP://OU=People,DC=contoso,DC=com"
```
۳. توسط دستور زیر یک شیء کاربر در OU می‌سازیم:
```
$objUser=$objOU.Create("user","CN=Mary North")
```
۴. خصیصه اجباری یعنی نام کاربری قبل از ویندوز 2000 را طبق دستور زیر تعیین می‌کنیم:
```
$objUser.Put("sAMAccountName""mary.north")
```
۵. با تایپ دستور زیر تغییرات را به Active Directory اعمال می‌کنیم:
```
$objUser.SetInfo()
```
۶. با تایپ دستور زیر مطمئن می‌شویم که شیء ساخته شده است:
```
$objUser.distinguishedName
```
DN کاربر باید نمایش داده شود.
۷. خصیصه‌هایی را که Active Directory بطور خودکار پیکربندی می‌کند با دستور زیر بررسی می‌کنیم:
```
$objUser | get-member
```
این دستور شیء نماینده کاربر را به Get-Member cmdlet می‌فرستد تا لیست خصیصه‌های تعیین شده نمایش داده شود.

تمرین ۳ ساخت کاربر با اسکریپت PowerShell ویندوز

در تمرین ۲ با درج دستور در PowerShell ویندوز بطور مستقیم کاربری را ساختیم. در این تمرین یک اسکریپت PowerShell ویندوز ساخته می‌شود تا ساخت کاربر را بطور خودکار انجام دهد.

۱. برنامه Notepad را باز کنید.

کد زیر را وارد کنید:
```
$objOU=[ADSI]"LDAP://OU=People,DC=contoso,DC=com"
$objUser=$objOU.Create("user","CN=Scott Mitchell")
```

```
$objUser.Put("sAMAccountName","scott.mitchell")
$objUser.SetInfo()
```

۲. اسکریپت را با نام "Newuser.psl" داخل گیومه ذخیره می‌کنیم تا Notepad پسوند txt به آن اضافه نکند.

۳. PowerShell ویندوز را باز می‌کنیم.

۴. تایپ می‌کنیم get-childitem و Enter را می‌زنیم.

Get-ChildItem cmdlet همه اشیاء فرزند شیء را برمی‌شمارد. در خط فرمان PowerShell ویندوز دایرکتوری جاری، پیش‌فرض است.

۵. Dir و سپس Enter را بزنید.

نام مستعار dir به Get-ChildItem ارجاع می‌دهد.

۶. عبارت cd documents راتایپ کرده و Enter را بزنید.

الان باید در پوشه Documents خود باشید.

۷. اجرای اسکریپت را با دستور زیر فعال می‌کنیم:

```
set-executionpolicy remotesigned
```

۸. اسکریپت را با تایپ عبارت .\newuser.psl اجرا می‌کنیم.

علامت .\ مسیر جاری را به عنوان مسیر اسکریپت معرفی می‌کند. بدون آن با خطا مواجه می‌شویم.

۹. بررسی می‌کنیم تا ببینیم کاربر در Active Directory ایجاد شده است یا نه.

تمرین ۴ ساخت کاربر با اسکریپت VBScript

در این تمرین اسکریپت VBScript برای خودکارسازی ساخت کاربر ایجاد می‌شود.

۱. برنامه Notepad را باز می‌کنیم.

۲. کد زیر را وارد می‌کنیم:

```
Set objOU=GetObject("LDAP://OU=People,DC=contoso,DC=com")
Set objUser=objOU.Create("user","CN=Linda Mitchell")
objUser.Put("sAMAccountName","linda.mitchell")
objUser.SetInfo()
```

۳. اسکریپت را با نام "Newuser.vbs" داخل گیومه در پوشه Documents ذخیره می‌کنیم تا Notepad پسوند txt به آن اضافه نکند.

۴. پنجره خط فرمان را باز می‌کنیم.

۵. عبارت cd %userprofile%\documents را تایپ کرده و Enter را می‌زنیم.

۶. اسکریپت را با تایپ دستور cscript.exe newuser.vbs اجرا می‌کنیم.

۷. بررسی می‌کنیم تا مطمئن شویم کاربر به درستی در Active Directory ایجاد شده است.

خلاصه درس

- PowerShell ویندوز از اجرای وظایف مدیریتی هم از خط فرمان و هم از طریق اسکریپت پشتیبانی می‌کند. PowerShell ویندوز یک ویژگی از ویژگی‌های ویندوز سرور 2008 بوده و برای نصب روی ویندوز سرور 2003، ویندوز ویستا و ویندوز XP قابل دانلود است.
- VBScript یک زبان اسکریپت نویسی است که توسط Windows Scripting Host کامپوننتی که روی همه نسخه‌های ویندوز وجود دارد پردازش می‌شود.
- برای ساخت یک شیء Active Directory توسط VBScript یا PowerShell ویندوز به container متصل می‌شویم مثلا OU و سپس شیء را می‌سازیم خصوصیات آن را مشخص می‌کنیم و تغییرات را در Active Directory با متد SetInfo اعمال می‌کنیم.

سئوالات پایان درس

۱. می‌خواهید یک شیء کاربری با PowerShell ویندوز بسازید. کدام‌یک از موارد زیر باید اجرا شود؟
   a. از Create-User cmdlet استفاده کنیم.
   b. از متد NewUser از ADSI استفاده کنیم.
   c. متد Create یک OU را اجرا کنیم.
   d. از عبارت set objUser=CreateObject استفاده کنیم.
۲. می‌خواهید یک شیء کاربر با یک دستور تنها بسازید. کدام‌یک از موارد زبر باید اجرا گردد؟
   a. از Create-Item cmdlet استفاده کنیم.
   b. از متد SetInfo استفاده کنیم.
   c. از متد Create یک OU استفاده کنیم.
   d. از دستور Dsadd استفاده کنیم.
۳. کدام‌یک از خطوط PowerShell ویندوز برای ساخت شیء کاربر در People OUضروری است؟ (بیش از یک جواب دارد. هر جواب بخشی از راه حل است.)
   a. $objUser=$objOU.Create("user","CN=Jeff Ford")
   b. $objUser.SetInfo()
   c. $objUser=CreateObject("LDAP://CN=Jeff Ford,OU=People,DC=contoso,DC=com")
   d. $objOU=[ADSI]"LDAP://OU=People,DC=contoso,DC=com"

درس ۳ : نگهداری از اشیاء و حساب‌های کاربر

دو درس اول این فصل متدهای ساخت حساب‌های کاربری را تشریح کردند. این فقط چرخه اول زندگی یک کاربر در دامنه محسوب می‌شود. پس از ساخت کاربر ما باید خصوصیاتی را که مربوط به واحد امنیتی (حساب) می‌شود و خصلت‌هایی را که کاربر را مدیریت می‌کند پیکربندی کنیم. همچنین باید بدانیم چطور و چه زمانی حساب را مدیریت کنیم مثلا برای تغییر کلمه عبور یا باز کردن قفل حساب. در نهایت باید بتوانیم کاربر را به OU ها دیگر منتقل کنیم یا گاهی اوقات آن را غیر فعال یا حذف کنیم. در این درس یاد می‌گیریم از کاربران نگهداری کنیم وظایفی که هم از طریق رابط کاربری ویندوز و هم از طریق ابزارهای خط فرمان انجام می‌شود.

بعد از این درس باید بتوانیم:

- هدف و نیازمندی‌های خصیصه‌های حساب کاربری و خصوصیات نام کاربری را بدانیم.
- خصوصیات مخفی یک شیء کاربر را مشاهده کنیم و تغییر دهیم.
- خصوصیات کاربران را با هم و همزمان تغبیر دهیم.
- کاربران را با ابزار Active Directory Users And Computers، دستورات DS، PowerShell ویندوز و VBScript مدیریت کنیم.
- وظایف مدیریتی معمول را برای نگهداری از حساب‌های کاربری اجرا کند.

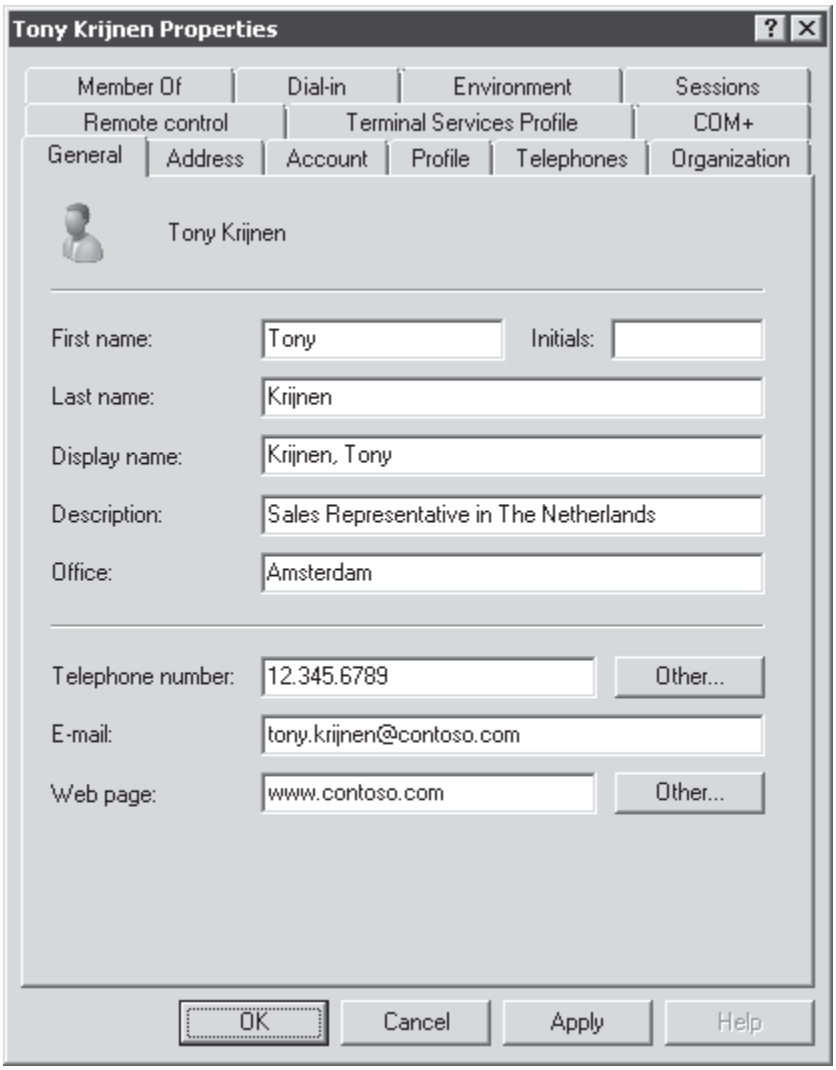
زمان تقریبی : ۹۰ دقیقه

مدیریت خصیصه‌های کاربر توسط Active Directory Users And Computers

وقتی یک کاربر را با استفاده از ویزارد New Object-User از ابزار Active Directory Users And Computers می‌سازیم باید در ویزارد نام کاربر کلمه عبور و نام و نام خانوادگی کاربر را واردکنیم. یک کاربر در Active Directory دهها خصیصه دیگر دارد که در زمان مقتضی با ابزار **Active Directory Users And Computers** می‌توان آن را پیکربندی کرد.

برای مشاهده و تغییر خصیصه‌های کاربر روی آن کلیک راست کرده و Properties را انتخاب می‌کنیم. کادر محاوره‌ای Properties کاریر ظاهر می‌شود مانندشکل ۳- ۴ . خصیصه‌های شیء کاربر در گروه‌های متعددی قرار می‌گیرد که در زبانه‌های کادر محاوره‌ای ظاهر

می‌شود:



شکل ۴- ۳ کادر محاوره‌ای Properties کاربر

- خصیصه‌های حساب کاربری: زبانه Account این خصیصه‌ها شامل نام کاربری، کلمه عبور و پرچم‌های (flag) حساب می‌باشد. بسیاری از این خصیصه‌ها در زمان ساخت کاربر می‌تواند پیکربندی شود. بخش "Account Properties" جزئیات آن را شرح می‌دهد.
- اطلاعات شخصی : زبانههای General، Address، Telephones و Organization زبانه General خصوصیات مربوط به نام را که هنگام ساخت شیء کاربر پیکربندی می‌شود و همچنین اطلاعات کلی و تماس کاربر را نشان می‌دهد. زبانه Address و Telephone جزئیات اطلاعات تماس را نمایش می‌دهد. زبانه Telephone جایی است که مایکروسافت فیلد Notes را در آن قرار داده که به خصیصه Info اشاره می‌کند و بسیار پرکاربرد است. زبانه Organization عنوان شغلی، بخش، شرکت و ارتباطات سازمانی را نمایش می‌دهد.
- پیکربندی کاربر : زبانه Profile مسیر پروفایل کاربر، logon script و home folder در این زبانه پیکربندی می‌شود.
- عضویت در گروهها : زبانه Member Of کاربر را می‌توان به گروه اضافه یا از گروه حذف کرد و گروه اولیه (Primary Group)کاربر را تغییر داد. عضویت در گروهها و گروه اولیه در فصل ۵ "کامپیوترها" بحث می‌شود.

- Terminal services : زبانه‌های Terminal Services Profile، Remote Control و Sessions این چهار زبانه پیکربندی و مدیریت کاربر را هنگام ایجاد Terminal Services session انجام می‌دهند.

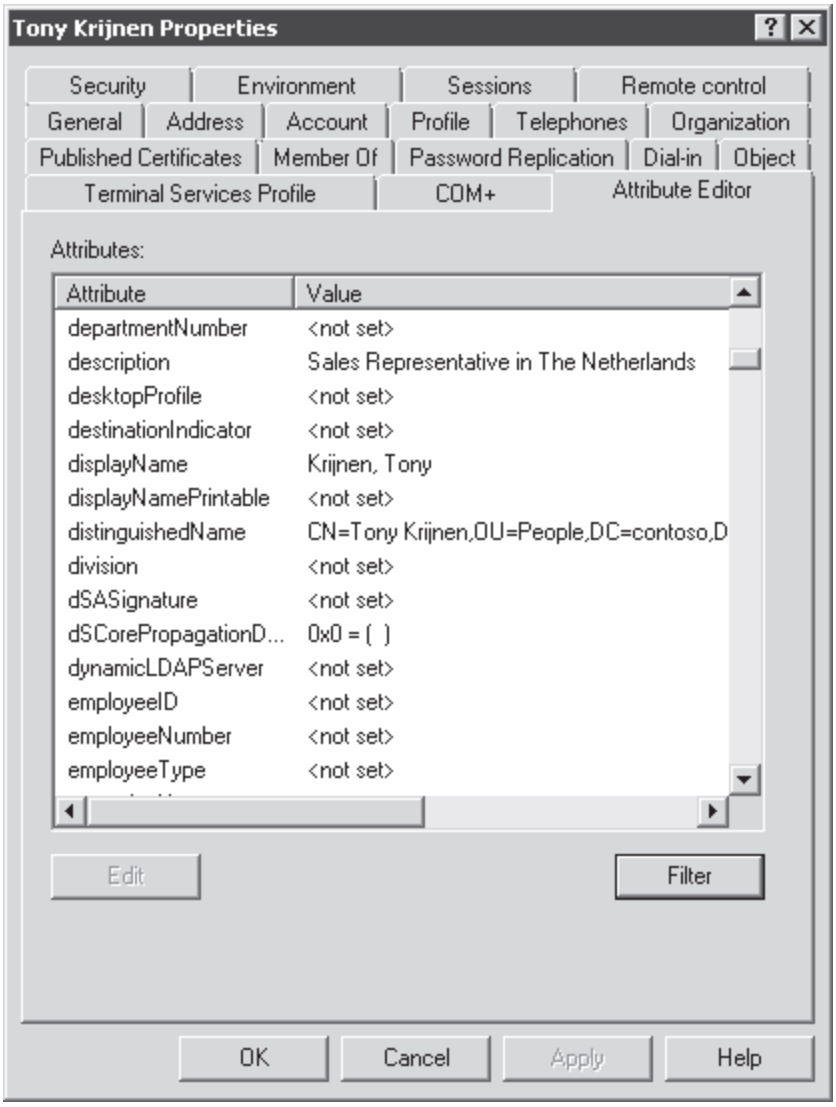
اطلاعات بیشتر تنظیمات Terminal Services

برای اطلاعات بیشتر در مورد تنظیمات Terminal Services به کتاب MCTS: Configuring Windows Server 2008 Applications Infrastructure اثر J.C. Mackin و Anil Desai از انتشارات Microsoft Press در سال ۲۰۰۸ مراجعه کنید.

- ارتباط از راه دور : زبانه Dial-in در این زبانه می‌توانیم مجوز ارتباط از راه دور را پیکربندی کنیم.
- برنامه‌های کاربردی : زبانه COM+ در این زبانه می‌توان کاربران را به یک Active Directory COM+ partition set منتسب کرد. این ویژگی مدیریت برنامه‌های کاربردی توزیع شده را تسهیل می‌کند که البته خارج از مباحث امتحانی 70-640 است.

نمایش همه خصیصه‌ها

خصیصه‌های نمایش داده شده در کادر محاوره‌ای Properties همه خصیصه‌های شیء کاربر نیست. بعضی از خصیصه‌های اصطلاحا مخفی می‌توانند برای سازمان بسیار مفید باشند. برای خارج کردن این خصیصه‌ها از حالت مخفی باید ویژگی جدید ویندوز سرور 2008 را به‌نام Attribute Editor فعال کنیم. منوی View را باز کرده و گزینه Advanced Features را انتخاب می‌کنیم. سپس کادر محاوره‌ای Properties کاربر را باز می‌کنیم و همانند شکل ۳- ۵ زبانه Attribute Editor را می‌بینیم.



شکل ۵- ۳ زبانه Attribute Editor

در این زبانه همه خصیصه‌های موجود شیء مورد نظر نمایش داده می‌شود. با استفاده از دکمه Filter حتی می‌توان خصیصه‌های بیشتری را مانند خصیصه‌های backlink و constructed مشاهده کرد. Backlink ها خصیصه‌هایی هستند که از ارجاع اشیاء به یک شی حاصل می‌شوند. بهترین راه درک این نوع از خصیصه‌ها فهم مثالی در این مورد است : خصیصه memberOf را در نظر بگیرید. ***** وقتی کاربری به یک گروه اضافه می‌شود خصیصه member گروه است که تغییر می‌کند یعنی DN کاربر به خصیصه چند مقداری member افزوده می‌شود. بنابراین خصیصه member گروه خصیصه forward link نام خواهد گرفت. وقتی کاربر توسط خصیصه member یک گروه ارجاع می‌شود خصیصه memberOf کاربر بطور خودکار توسط Active Directory بروزرسانی می‌گردد. در حالی که ما مستقیما خصیصه memberOf کاربر را تغییر نمی‌دهیم و Active Directory خود این کار را انجام می‌دهد.

خصیصه Constructed یکی از نتایج محاسبه توسط Active Directroy می‌باشد. مثال آن خصیصه tokenGroups است. این خصیصه لیستی از SID های همه گروههایی است از جمله گروههای تودرتو (Nested Group) که کاربر عضو آن است. برای تعیین مقدار tokenGroups ، Active Directory باید عضویت نهایی کاربر را محاسبه کند که چند سیکل کاری پردازنده را به خود اختصاص می‌دهد. بنابراین خصیصه بعنوان بخشی از شیء کاربر ذخیره نمی‌گردد. در عوض هنگام نیاز محاسبه می‌شود. چون برای نمایش خصیصه‌های Constructed نیاز به پردازش می‌باشد Attribute Editor آن‌ها را بطور پیش‌فرض نمایش نمی‌دهد. همچنین در پرس‌و جوهای LDAP نیز نمی‌توانند استفاده شوند.

همانطور که در شکل ۳- ۵ مشاهده می‌کنید برخی خصیصه‌های شیء کاربر نظیر division، employeeID، employeeNumber و employeeType می‌توانند خیلی مفید باشند. اگرچه این خصیصه‌ها در زبانه‌های استاندارد شیء کاربر نمایش داده نمی‌شدند الان از طریق Attribute Editor در دسترس هستند و توسط PowerShell ویندوز و VBScript قابل استفاده می‌باشند.

اطلاعات بیشتر خصیصه‌های مخفی اشیاء

برای اطلاعات بیشتر درباره استفاده از خصیصه‌های مخفی اشیاء و توسعه schema با خصیصه‌های سفارشی به Windows Administration Resource Kit: Productivity Solutions for IT Professionals نوشته Dan Holme از انتشارات Microsoft Press سال ۲۰۰۸ مراجعه کنید.

مدیریت خصیصه‌های چند کاربر

ابزار Active Directory Users And Computers اجازه تغییر همزمان چند کاربر را می‌دهد. با نگه‌داشتن کلید Ctrl و کلیک روی کاربر و یا دیگر روشهای انتخاب گروهی کاربران را انتخاب می‌کنیم. این انتخاب باید فقط شامل یک کلاس از اشیاء باشد مثلا کاربر. سپس روی یکی از اشیاء انتخابی کلیک راست کرده و Properties را انتخاب می‌کنیم.

در حالت انتخاب گروهی بعضی از خصیصه‌ها برای تغییر در دسترس قرار می‌گیرند.

- **General** Description، Office، telephon Number، Fax، Web Page و E-mail
- **Account** UPN Suffix، Logon Houres، Logon Computer Restrictions (logon workstations)، همه Account Options و Account Expires
- **Address** Street، P.O.Box، City، State/Province، ZIP/Postal Code و Country/Region
- **Profile** Profile Path، Logon Script و Home Folder
- **Organization** Title، Department، Company و Manager

نکته امتحانی برای امتحان باید بدانید کدام خصیصه‌ها در انتخاب گروهی قابل تغییر هستند. سناریوهای امتحان و شبیه‌سازی‌هایی که نیاز به تغییر خصیصه‌های چند کاربر را دارند درک شما را از انتخاب گروهی آزمایش می‌کنند. در دنیای واقعی بخاطر داشته باشید شما می‌توانید و باید از ابزارهایی نظیر Dsmod، PowerShell ویندوز و VBScript استفاده کنید.

درک خصیصه‌های نام و حساب

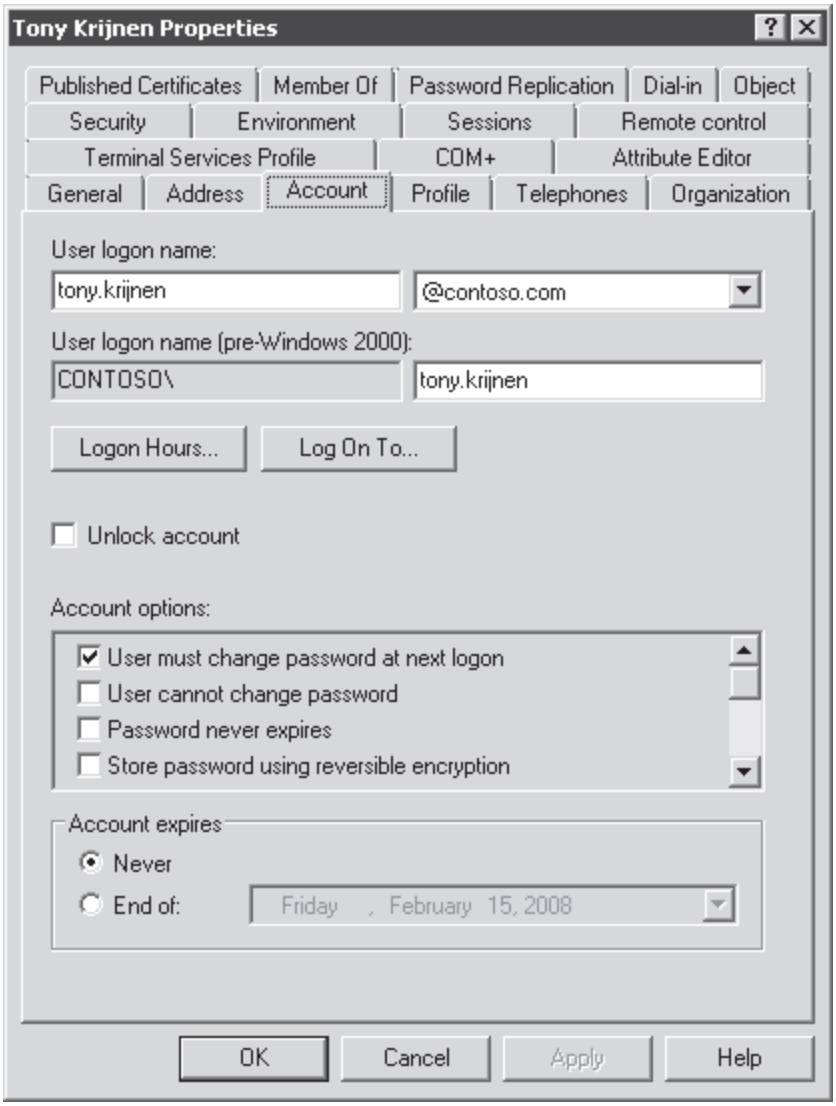
دو گروه از خصیصه‌ها در امتحان بین‌المللی حضور خواهند شد و چالشی برای مدیران شبکه بحساب می‌آید : خصیصه‌های نام و حساب نام شیء کاربر

خصیصه‌های متعددی با با نام شیء و حساب مرتبط هستند. دانستن تفاوت‌های آنان اهمیت زیادی دارد.

- خصیصه sAMAccountName کاربر (نام کاربری قبل از ویندوز 2000) باید در کل دامنه واحد باشد. بسیاری از سازمانها از نام middle یا ترکیبی از نام و نام خانوادگی برای ساخت sAMAccountName استفاده می‌کنند. این رویکرد می‌تواند مسئله ساز باشد چون یک سازمان با هر اندازه می‌تواند کاربرانی با نامهای مشابه داشته باشد و sAMAccountName ساخته شده تکراری خواهد بود. در این حالت باید استثنا قایل شد و این استثنا قانون را خراب می‌کند. این مسئله با انتخاب شماره کارمندی یا دیگر خصیصه‌های واحد کاربران به عنوان sAMAccountName قابل است. اگر توانایی تغییر قواعد نام‌گذاری را در سازمان دارید قاعده نام‌گذاری مستقل از نام پیشنهاد می‌شود.
- خصیصه userPrincipalName یا UPN از نام کاربری و یک پسوند UPN که بطور پیش‌فرض نام DNS دامنه که کاربر در آن ایجاد شده تشکیل می‌شود.UPN در کل forest باید واحد باشد. آدرس‌های پست الکترونیکی که باید در دنیا واحد باشد از این قانون پیروی می‌کنند. فرض کنید می‌خواهیم از آدرس E-mail به‌عنوان UPN کاربران استفاده کنیم. وقتی دامنه Active Directory با نام دامنه آدرس E-mail یکی نیست باید دامنه E-mail را به عنوان پسوند UPN اضافه کنیم. برای این کار ابزار Active Directory Domains And Trusts را باز کرده و روی ریشه ابزار کلیک راست کرده و Properties را انتخاب می‌کنیم.
- RDN در OU باید منحصربه فرد باشد. برای کاربران این یعنی خصیصه cn باید در OU منحصر باشد. این وضعیت می‌تواند کمی مزاحم باشد. وقتی در سازمان فقط یک OU برای کاربران موجود است و کاربری به‌نام Scott Miller داریم و کارمند دیگری با همین نام استخدام می‌شود. بهرحال cn کاربر نمی‌تواند تکراری باشد. متاسفانه راه حل مناسبی برای این مسئله وجود ندارد. باید قوانین نام‌گذاری را طوری طراحی کنیم که برای همه CN ها یک قانون موجود باشد. شاید بهتر باشد شماره کارمندی در ایجاد CN دخیل باشد مثلا Scott Miller (645928). وقتی ساختار OU صاف و بدون شاخه باشد باید منتظر چنین مشکلاتی باشیم.
بعلاوه بسیاری از سازمانها خصیصه cn را به صورت LastName,FirstName انتخاب می‌کنند که در ابزار Active Directory Users And Computers براحتی می‌توان کاربران را مرتب کرد. برای چنین هدفی این کار توصیه نمی‌شود. بجای این‌کار بهتر است ستون Last Name را با کلیک منوی View و انتخاب Add/Remove Columns به ابزار اضافه کنیم. سپس روی سرستون Last Name کلیک می‌کنیم تا براساس نام خانوادگی مرتب شود.
- خصیصه displayName در لیست Exchange global address list (GAL) ظاهر می‌شود. وقتی کاربران برحسب نام خانوادگی مرتب می‌شوند پیدا کردن آن‌ها در GAL راحت تر است. بنابراین می‌توان یک قاعده نام‌گذاری برای سازمان تعیین کرد که خصیصه displayName را از LastName,FirstName بگیرد.

خصوصیات حساب

در زبانه Account کادر محاوره‌ای Properties کاربر که در شکل ۳- ۶ می‌بینید خصیصه‌هایی وجود دارند که نشان می‌دهد کاربر یک واحد امنیتی است. یعنی هویتی است که حقوق و مجوز نسبت به آن اختصاص داده می‌شود. دیگر واحدهای امنیتی شامل کامپیوترها، گروهها و کلاس شیء inetOrgPerson می‌باشند.



شکل ۶- ۳ خصوصیات Account یک شیء کاربر

بسیاری از خصیصه‌های حساب باید شرح داده شوند چون کمی مبهم هستند. جدول ۳- ۲ این خصیصه‌ها را شرح می‌دهد.

خصیصه	شرح
Logon Houres	با کلیک روی آن ساعاتی را که کاربر مجاز به ورود به شبکه است مشخص می‌کند.
Log On To	برای محدود کردن کامپیوترهایی است که کاربر مجاز است از آن‌ها به شبکه وارد شود. در بخش‌های دیگر رابط کاربری Computer Restrictions نامیده می‌شود و به خصیصه userWorkstations نگاشت می‌شود. برای استفاده از این ویژگی پروتکل NetBIOS باید فعال باشد زیرا از نام کامپیوتر به‌جای آدرس Media Access Controll (MAC) استفاده می‌کند.
User Must Change Password At Next Logon	اگر بخواهیم کاربر در اولین ورود کلمه عبور خود را تغییر دهد از این گزینه استفاده می‌کنیم. اگر گزینه Password Never Expires انتخاب شود از این گزینه نمی‌توانیم استفاده کنیم. انتخاب این گزینه باعث می‌شود گزینه User Cannot Change Password از انتخاب خارج شود.
User Cannot Change Password	این کادر را علامت بزنید اگر بیش از یک نفر از این حساب استفاده می‌کنند (مانند Guest) یا بخواهیم نظارت دقیقی روی کلمات عبور داشته باشیم. این

	گزینه معمولا برای مدیریت کلمات عبور حساب‌های خاص به‌کار می‌رود. وقتی گزینه User Must Change Password At Next Logon انتخاب شود این گزینه قابل انتخاب نخواهد بود.
Password Never Expires	این گزینه زمانی انتخاب می‌شود که بخواهیم کلمه عبور تاریخ انقضاء نداشته باشد. انتخاب این گزینه باعث می‌شود گزینه User Must Change Password At Next Logon از انتخاب خارج شود چون هر دو را باهم نمی‌توان انتخاب کرد. این گزینه معمولا برای مدیریت کلمات عبور حساب‌های خاص به‌کار می‌رود
Account Is Disabled	انتخاب این گزینه باعث غیرفعال شدن حساب کاربری می‌شود. بعنوان مثال وقتی کارمندی استخدام می‌شود حساب کاربری برای او ساخته می‌شود و تا زمانی که نیاز به دسترسی به منابع شبکه ندارد حسابش غیرفعال می‌ماند.
Store Password Using Reversible Encryption	این گزینه باعث می‌شود کلمه عبور در Active Directory بدون استفاده از الگوریتم رمزنگاری غیرقابل برگشت و قدرتمند Active Directory ذخیره گردد. این گزینه برای برنامه‌هایی طراحی شده که نیاز دارند کلمه عبور کاربر را بدانند. تا جایی که می‌توانید از این گزینه استفاده نکنید چون بشدت باعث تضعیف امنیت می‌شود. کلمه عبور ذخیره شده با این گزینه مانند ذخیره کلمه عبور به صورت متن ساده است. کلاینتهای Macintosh که از پروتکل AppleTalk استفاده می‌کنند نیاز به دانستن کلمه عبور دارند. وقتی کاربری از یک سیستم Macintosh به شبکه وارد می‌شود باید این گزینه را برای او فعال کنیم.
Smart Card Is Required For Interactive Logon	کارت‌های هوشمند سخت‌افزارهای قابل حملی هستند که اطلاعات هویتی انحصاری مربوط به کاربر را ذخیره می‌کند. این ادوات به سیستم متصل می‌شوند و کار تایید هویت را انجام می‌دهند.
Account Is Trusted For Delegation	این گزینه به یک حساب خاص امکان می‌دهد تا بجای کاربر به منابع شبکه دسترسی پیدا کند.
Account Expires	از این گزینه برای تعیین زمان انقضاء حساب استفاده می‌شود.

نکته برای حساب‌های خاص کلمه عبور پیچیده پیکربندی کنید

سرویس‌ها نیاز به اعتبار برای دسترسی به منابع سیستم دارند. بسیاری از سرویس‌ها به حساب کاربری دامنه برای تایید هویت احتیاج دارند و معمولا این حساب بدون تاریخ انقضاء پیکربندی می‌شود. در چنین شرایطی از کلمه عبور پیچیده و طولانی استفاده کنید. اگر حساب مذکور توسط سرویسی استفاده می‌شود که روی تعداد محدودی سیستم اجرا می‌شود می‌توان با پیکربندی خصیصه Log On To با لیست سیستم‌ها امنیت را ارتقاء داد.

مدیریت خصلت‌های کاربر با Dsmod و Dsget

این دستورات ابزارهای خط فرمان Active Directory هستند که دستورات DS نامیده می‌شوند. در فصل ۲ Dsquery و در درس ۱ همین فصل Dsadd را بررسی کردیم.

Dsmod

این دستور خصیصه‌های اشیاء موجود را تغییر می‌دهد. دستورات DS در درس ۱ معرفی شدند. مانند بقیه دستورات DS شکل فرمان Dsmod به‌صورت زیر است:

Dsmod user UserDn . . . parameters

پارامتر UserDn DN کاربر را مشخص می‌کند. بقیه پارامترها خصیصه و مقدار جدیدش را تعیین می‌کند. به‌عنوان مثال دستور زیر خصیصه Office کاربر Tony Krijnen را تغییر می‌دهد:

Dsmod user "cn=Tony Krijnen,ou=People,dc=contoso,dc=com" –Office "Amsterdam"

پارامترهای خصیصه دقیقاً مشابه اسامی خصیصه LDAP شیء کاربر نیستند. برای مثال پارامتر dept دستور DSMOD USER خصیصه department شیء کاربر را تغییر می‌دهد. به‌علاوه DSMOD USER فقط یک سری از خصیصه‌ها را می‌تواند تغییر دهد. برای اطلاعات بیشتر در مورد پارامترها و کاربرد آن‌ها دستور DSMOD USER را اجرا کنید.

انتقال چند DN به دستور Dsmod

پارامتر UserDn دستور Dsmod حتماً لازم نیست در خط فرمان درج شود. دو راه دیگر برای انتقال DN ها به دستور وجود دارد. راه اول اینست که DN ها را در کنسول وارد کنیم. فرض کنید می‌خواهیم خصیصه office دو کاربر را به علت انتقال به دفتر سیدنی تغییر دهیم. دستورات زیر این کار را انجام می‌دهد:

Dsmod user -office "Sydney"

پارامتر UserDn مشاهده نمی‌شود. بعد از اجرای دستور بالا خط فرمان منتظر ورود DN کاربران می‌ماند. هر کدام از DN ها در گیومه قرار گرفته و پس از هر DN کلید Enter را می‌زنیم. پس از ورود آخرین DN و زدن کلید Enter کلیدهای Ctrl+Z را فشار می‌دهیم و باز Enter را می‌زنیم. دستورات اجرا می‌شوند.

روش پیچیده‌تر برای انتقال DN ها به دستور Dsmod انتقال نتیجه دستور Dsquery می‌باشد. این دستور در فصل ۲ بررسی شده است. این دستور Active Directory را بر حسب شرایط تعیین شده جستجو می‌کند و DN اشیاء را برمی‌گرداند. مثلاً برای تغییر خصیصه office مربوط به Linda و Scott Mitchell به Sydney دستور زیر به‌کار می‌رود:

Dsquery user -name "* Mitchell" | dsmod user -office "Sydney"

دستور Dsquery در Active Directory به دنبال کاربرانی می‌گردد که نام‌هایشان با Mitchell تمام می‌شود. DN اشیاء بدست آمده سپس به دستور DSMOD USER ارسال می‌شود که خصیصه office آن‌ها را به Sydney تغییر بدهد.

به‌عنوان مثالی دیگر فرض کنید می‌خواهیم برای همه کاربران پوشه اختصاصی روی SERVER01 بسازیم. دستور زیر خصیصه‌های homeDirectory و homeDrive شیء کاربر را در People OU تغییر می‌دهد:

Dsquery user "ou=People,dc=contoso,dc=com" | dsmod user –hmdir "\\server01\users\%username%\documents" –hmdrv "U:"

همانطوریکه در درس ۱ اشاره شد عبارت %username% وقتی برای پیکربندی مقادیر پارامترهای email–، hmdir-، profile- و webpg– از دستور DS استفاده می‌کنیم به sAMAccountName کاربر اشاره می‌کند

Dsget

این دستور خصیصه‌های انتخاب شده یک یا چند شیء را در خروجی نمایش می‌دهد. شکل دستور مشابه Dsmod و به صورت زیر است:

Dsget user UserDN . . . parameters

DN شیء یا اشیاء را می‌توان در خط فرمان با در نظر گرفتن فاصله خالی بین آن‌ها وارد کرد یا نتیجه دستور DSQUERY USER را به دستور منتقل کرد. برخلاف Dsadd و Dsmod این دستور فقط یک پارامتر را آن‌هم بدون مقدار می‌گیرد. در عوض مقدار جاری خصیصه را گزارش می‌دهد. برای مثال جهت نمایش نام کاربری قبل از ویندوز 2000 کاربر Jeff Ford در People OU دستور زیر به‌کار می‌رود:

Dsget user "cn=Jeff Ford",ou=People,dc=contoso,dc=com" -samid

جهت نمایش نام کاربری قبل از ویندوز 2000 همه کاربران دفتر سیدنی این دستور به‌کار می‌رود:

Dsquery user -office "Sydney" | dsget user -samid

مدیریت خصیصه‌های کاربر با PowerShell ویندوز و VScript

برای مشاهده یک خصیصه شیء کاربر با PowerShell ویندوز یا VBScript از ADSI برای اتصال به شیء کاربر استفاده می‌کنیم که به این پروسه binding نیز گویند. در درس ۲ برای ساخت کاربر به یک OU متصل شدیم. بعد از ایجاد شیء به خود شیء متصل می‌شویم. یک روش برای انجام این‌کار استفاده از Active Directory services path(aDSPath) شیء می‌باشد که مشخصه پروتکل "LDAP://" به همراه DN شیء می‌باشد.

دستور PowerShell ویندوز برای اتصال به کاربر Jeff Ford در People OU عبارت است از :

```
$objUser=[ADSI]”LDAP://cn=Jeff Ford,ou=People,dc=contoso,dc=com”
```

معادل VBScript آن به‌صورت زیر است:

```
Set objUser=GetObject(”LDAP://cn=Jeff Ford,ou=People,dc=contoso,dc=com”
```

به خاطر داشته باشید که PowerShell ویندوز مبدل نوع ADSI را مشخص می‌کند و VBScript از GetObject استفاده می‌کند. VBScript از عبارت Set برای منتسب کردن ارجاع یک شیء به یک متغیر استفاده می‌کند. PowerShell ویندوز از عبارت Set استفاده نمی‌کند و ابتدای همه متغیرها علامت $ قرار می‌دهد.

وقتی صاحب متغیری شدیم که به شیء برمی‌گردد می‌توانیم خصوصیات آن را بدست آوریم. مثلاً در PowerShell ویندوز عبارت زیر را وارد کنید تا خصیصه sAMAccountName کاربر نمایش داده شود:

```
$objUser.Get(“sAMAccountName”)
```

در VBScript باید نشان دهیم که می‌خواهیم خصیصه را در خروجی نمایش دهیم. راه معمول برای این‌کار استفاده از عبارت WScript.Echo می‌باشد به صورت زیر:

```
WScript.Echo  objUser.Get(“sAMAccountName”)
```

شکل خلاصه دستور به نام property. وجود دارد و instance آن $objUser.sAMAccountName در PowerShell ویندوز و objUser.sAMAccountName در VBScript می‌باشد. اگرچه این روش در بیشتر موارد کار می‌کند پیشنهاد می‌شود از متد Get استفاده شود مخصوصاً وقتی در PowerShell ویندوز با اشیاء Active Directory کار می‌کنیم.

وقتی می‌خواهیم یک خصیصه را تغییر دهیم سه کار را باید انجام دهیم:

۱. به شیء کاربر متصل شویم.
۲. خصیصه را تغییر دهیم.
۳. تغییرات را اعمال کنیم.

قبلاً دیدیم که چطور می‌توان به شیء متصل شد. مرحله دوم تغییر خصیصه است. بیشتر خصیصه‌ها تک مقداره و ساده هستند و با متد Put شیء تغییر می‌کنند. برای مثال در PowerShell ویندوز:

```
$objUser.put(“company”,”contoso, Ltd.”)
```

و در VBScript:

```
objUser.put “company”,”contoso, Ltd.”
```

تنها تفاوت این است که در VBScript در متد Put پرانتز استفاده نمی‌شود.

ما می‌توانیم در این مرحله چند خصیصه را مشخص کنیم. پس از این که همه خصیصه‌ها مشخص شدند باید تغییرات را با دستور SetInfo اعمال کنیم. در PowerShell ویندوز وارد می‌کنیم:

```
$objUser.SetInfo()
```

و در VBScript وارد می‌کنیم:

```
objUser.SetInfo()
```

از قرار دادن سه مرحله فوق اسکریپت PowerShell ویندوز حاصل می‌شود:

```
$objUser=[ADSI]”LDAP://cn=Jeff Ford,ou=People,dc=contoso,dc=com”
$objUser.put(“company”,”contoso, Ltd.”)
$objUser.SetInfo()
```

در VBScript کد به صورت زیر است:

```
Set objUser=GetObject(”LDAP://cn=Jeff Ford,ou=People,dc=contoso,dc=com”
objUser.put “company”,”contoso, Ltd.”
objUser.SetInfo()
```

اگر بخواهیم خصیصه را حذف کنیم چه باید بکنیم؟ باید ابتدا به شیء متصل شویم. سپس خصیصه را با مقدار خالی "" مشخص کنیم وقتی خصیصه از نوع رشته کاراکتر است. اگر خصیصه از نوع عددی است با عدد صفر پر می‌کنیم. و اگر صفر نمایانگر مقدار خالی است از آن استفاده می‌کنیم. همچنین می‌توان یک خصیصه را به طور کامل حذف کرد البته این زمانی ممکن است که خصیصه اجباری نباشد.

برای این کار از متد PutEX استفاده می‌کنیم. به عنوان مثال برای حذف خصیصه office در PowerShell ویندوز از کد زیر استفاده می‌کنیم:

```
$objUser.PutEX(1, “office”, 0)
$objUser.SetInfo()
```

در VBScript از کد زیر استفاده می‌کنیم:

```
objUser.PutEX 1, “office”, 0
objUser.SetInfo()
```

مدیریت حساب‌های کاربری

هدف اولیه شیء کاربر در Active Directory تایید هویت یک کارمند یا یک سرویس است. حساب‌ها ساخته می‌شوند مدیریت می‌شوند و گاهی حذف می‌شوند. پرکاربردترین وظایف مدیریتی مربوط به حساب‌های کاربری تغییر کلمه عبور باز کردن قفل حساب کاربر غیرفعال کردن فعال کردن حذف انتقال و تغییر نام اشیاء کاربر می‌باشد.

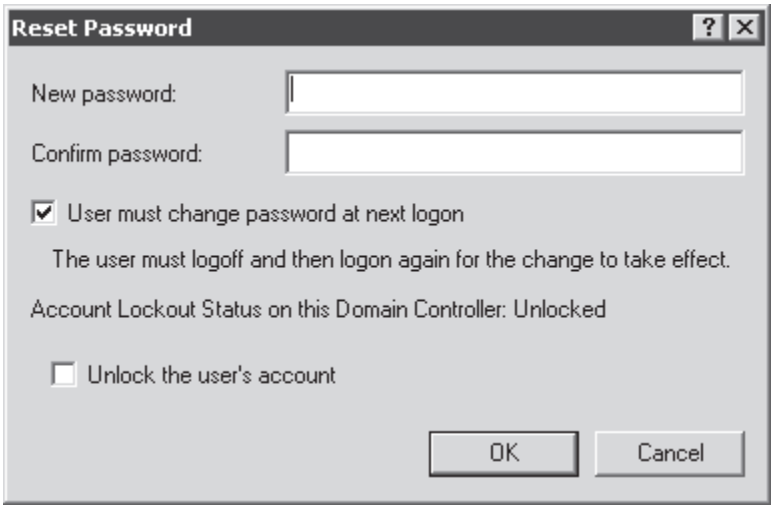
در بخش‌های بعدی این وظایف بررسی شده و در محیط‌های رابط کاربری ویندوز، PowerShell ویندوز ، VBScript و خط فرمان اجرا می‌گردد. هر کدام از این وظایف نیاز به داشتن مجوزهای مناسب نسبت به اشیاء کاربر دارند. واگذاری مجوزهای مدیریتی در فصل ۲ بحث شده است.

ریست کلمه عبور کاربر

اگر کاربری کلمه عبور خود را فراموش کند و سعی کند به سیستم وارد شود پیغامی طبق شکل ۳- ۷ دریافت می‌کند.

در این حالت برای اینکه کاربر بتواند به سیستم وارد شود باید کلمه عبور را ریست کرد. برای این کار نیاز نیست کلمه عبور قبلی را بدانیم. به سادگی روی شیء کاربر در Active Directory کلیک راست کرده و Reset Password را انتخاب می‌کنیم. کادر محاوره‌ای Reset Password همانند شکل ۳- ۸ باز می‌شود. کلمه عبور جدید را در کادرهای New Password و Confirm Password وارد می‌کنیم. بهتر است گزینه User Must Change Password At Next Logon را انتخاب کنیم تا کاربر کلمه عبوری را وارد کند که فقط خودش بداند.

شکل ۷- ۳ پیغام هنگام ورود که به کاربر اطلاع می‌دهد نام کاربری یا کلمه عبور اشتباه است



شکل ۸- ۳ کادر محاوره‌ای Reset Password

همچنین می‌توان از دستور DS برای این‌کار بهره برد. دستور زیر برای این منظور به کار می‌رود:

```
Dsmod user UserDN –pwd NewPassword –mustchpwd yes
```

یا در محیط PowerShell ویندوز تایپ می‌کنیم:

```
$objUser=[ADSI]”LDAP://UserDN”
$objUser.SetPassword(“NewPassword”)
```

توجه داشته باشید که برخلاف دیگر خصیصه‌ها بعد از دستور SetPassword نباید از SetInfo استفاده کنیم. اگر بخواهیم کاربر در اولین ورود کلمه عبور خود را عوض کند از روش زیر بهره می‌گیریم:

```
$objUser.Put (“pwdLastSet”,0)
$objUser.SetInfo()
```

در VBScript کد مشابه قبل و به صورت زیر می‌باشد:

```
Set  objUser=GetObjecy("LDAP://UserDN")
objUser.SetPassword "NewPassword"
objUser.Put "pwdLastSet",0
objUser.SetInfo
```

همچنین امکان انتقال کلمات عبور با استفاده از دستور LDIFDE وجود دارد. این دستور در درس ۱ معرفی شد. برای اطلاعات بیشتر به مقاله 263991 در آدرس http://support.microsoft.com/default.aspx?scid=kb;en-us;263991 مراجعه کنید.

باز کردن قفل حساب کاربری

در فصل ۸ "تایید هویت" یاد خواهید گرفت که چطور سیاست‌های مربوط به قفل حساب‌های کاربری (Lockout Policies) را پیکربندی کنید. سیاست قفل کردن حساب کاربری برای جلوگیری از موفقیت یک نفوذگر که به دفعات کلمات عبور مختلف را برای پیدا کردن کلمه عبور کاربر امتحان می‌کند طراحی می‌شود. وقتی کسی کلمه عبور را اشتباه وارد می‌کند پیغام خطای ورود ظاهر می‌شود. وقتی در یک بازه زمانی مشخص که توسط سیاست قفل‌کردن حساب‌های کاربری مشخص می‌شود چند بار کلمه عبور به اشتباه وارد شود حساب قفل می‌شود. دفعه بعد که کاربر بخواهد به سیستم وارد شود با پیغامی مبنی بر قفل بودن حساب مواجه می‌شود.

نکته مواظب درایوهای نگاشت شده با حساب کاربری ثانویه باشید

یکی از دلایل قفل شدن حساب درایوهای نگاشت شده با حساب کاربری ثانویه می‌باشد. وقتی کلمه عبور حساب کاربری ثانویه عوض می‌شود ویندوز سعی می‌کند به درایو نگاشت شده متصل شود و در نتیجه حساب قفل می‌شود.

سیاست قفل شدن حساب کاربری تعیین می‌کند که حساب قفل شده پس از چه مدت زمانی باز شود. ولی وقتی کاربر با چنین وضعیتی روبرو می‌شود احتمالا با بخش پشتیبانی تماس می‌گیرد. ما می‌توانیم با کلیک راست روی حساب کاربری، انتخاب Properties، کلیک روی زبانه Account و علامت زدن کادر Unlock Account قفل حساب را باز کنیم.

وقتی کلمه عبور کاربری را ریست می‌کنیم ویندوز سرور 2008 گزینه‌ای را برای باز کردن قفل حساب در اختیار قرار می‌دهد. کادر Unlock The User's Account را که در شکل ۳- ۸ نشان داده شده علامت بزنید. این روش زمانی به‌درد می‌خورد که کاربر به

علت فراموش کردن کلمه عبور خود باعث قفل شدن حسابش شده باشد. در این حالت کلمه عبور جدیدی برایش وارد می‌کنیم و کاربر را مجبور می کنیم در هنگام اولین ورود کلمه عبور خود را عوض کند. سپس قفل حساب کاربر را باز می‌کنیم.
متاسفانه نه خط فرمان و نه PowerShell ویندوز ابزار آماده‌ای برای باز کردن قفل حساب ندارد. برای باز کردن قفل حساب در VBScript از تکه کد زیر استفاده می‌کنیم:

```
Set objUser = GetObject("Ldap://UserDn")
objUser.IsAccountLocked = False
objUser.SetInfo
```

فعال و غیرفعال کردن حساب کاربری

حساب‌های کاربری واحدهای امنیتی هستند. یعنی هویت‌هایی که می‌توانند به منابع شبکه دسترسی داشته باشند. چون هر کاربر عضوی از کاربران دامنه است و دارای هویت تایید اعتبار شده می‌باشد هر کاربر حداقل دسترسی فقط خواندنی به طیف وسیعی از اطلاعات Active Directory دارد مگر اینکه ACL منابع را بطور جدی محدود کنیم.
بنابراین مهم است که حساب‌های کاربری را باز رها نکنیم. یعنی باید سیاست‌های کلمه عبور و ممیزی را پیکربندی کنیم که هر دو در فصل ۸ بررسی می‌شود و همچنین پروسه‌هایی را که تضمین کند حساب‌های کاربری به درستی استفاده می‌شود. وقتی حساب کاربری بلا استفاده می‌ماند مثلا کاربری برای مدتی در محل کار حضور ندارد حساب را غیرفعال می‌کنیم.
برای غیرفعال کردن حساب در ابزار Active Directory Users And Computers روی کاربر کلیک راست می‌کنیم. در خط فرمان از دستور Dsmod.exe بصورت زیر استفاده می‌کنیم:

```
Dsmod user UserDn -disabled yes
```

در PowerShell ویندوز همانطور که در درس ۲ دیدیم باید از متد پیچیده برای این کار استفاده کنیم:

```
$objUser=[ADSI]"LDAP://UserDn"
$objUser.psbase.InvokeSet('Account Disabled' , $true)
$objUser.SetInfo()
```

در VBScript کار ساده‌تر است:

```
Set objUser = GetObject("LDAP://UserDN")
objUser.AccountDisabled=TRUE
```

برای فعال کردن حساب در دستور Dsmod فقط باید Yes را با No عوض کنیم:

```
Dsmod user UserDn -disabled no
```

در PowerShell ویندوز $true را با $false و در VBScript باید TRUE را با FALSE عوض کنیم.

حذف حساب کاربری

وقتی از یک حساب استفاده نمی‌شود می‌توانیم آن را از دایرکتوری حذف کنیم. نکته حیاتی این است که پس از حذف کاربر ، حساب به طور کل از دایرکتوری پاک می‌شود. در واقع ما نمی‌توانیم حساب جدیدی با همان نام بسازیم و امیدوار باشیم عضویت در گروهها و دسترسی به منابع مانند کاربر قبلی باشد. از دست رفتن SID کاربر و به تبع آن عضویت در گروه مشکلات جدی را باعث می‌شود اگر بعداً به آن نیاز پیدا کنیم.
به همین دلیل بسیاری از سازمان‌ها حذف کاربر را در دو مرحله انجام می‌دهند. ابتدا حساب را غیرفعال می‌کنند و بعد از مدتی حذف می‌کنند. Active Directory یک سری از خصوصیات حساب از همه مهمتر SID را برای مدتی که پیش‌فرض آن ۶۰ روز است نگه می‌دارد که به آن tombstone lifetime گویند. بعد از آن حساب از دایرکتوری حذف می‌شود.
امکان بازیابی حساب کاربری نیز وجود دارد. وقتی کاربری سازمان را ترک می‌کند احتمالا جایگزینی برای او استخدام می‌شود که نیاز به دسترسی به منابع، عضویت در گروهها و حقوق کاربری مشابه کاربر قبلی دارد. بهتر است حساب کاربری تا زمانی که نیروی جدید استخدام شود غیرفعال باقی بماند و پس از استخدام نیروی جدید نام حساب را برای کاربر جدید تغییر داده و آن را فعال کنیم. با این روش SID ، عضویت در گروه و دسترسی به منابع مربوط به کاربر قبلی به کاربر جدید منتقل می‌شود.
برای حذف کاربر در Active Directory کافی است کاربر را انتخاب کرده و کلید Delete را می‌زنیم یا از منوی کلیک راست Delete را انتخاب می‌کنیم. بعلت اهمیت عملیات حذف کادری برای تایید عملیات حذف باز می‌شود.

با استفاده از دستور Dsrm ، یکی دیگر از دستورات DS، هم می‌توان اشیاء Active Directory را حذف کرد. دستور به شکل زیر استفاده می‌شود:

Dsrm UserDN

توجه داشته باشید که برخلاف دیگر دستورات DS در این دستور نیازی به مشخص کردن کلاس شیء نیست.

برای حذف کاربر با استفاده از PowerShell ویندوز باید به container والد کاربر – OU – متصل شویم و از متد Delete container استفاده کنیم. ممکن است کمی عجیب به نظر برسد ولی مشابه ساخت کاربر است که از متد container Create برای ساخت کاربر استفاده می‌کردیم. دو دستور PowerShell ویندوز کاربر را حذف می‌کند:

```
$objUser = [ADSI]"LDAP://organizational unit's DN"
$objOU.Delete("user","CN=UserCN")
```

VBScript نیز رویکردی این‌چنینی دارد:

```
Set objOU = GetObject(LDAP://organizational unit's DN)
objOU.Delete "user", "CN=UserDN"
```

انتقال حساب کاربری

وقتی بخواهیم شیء کاربری را در Active Directory جابجا کنیم بسادگی آن را با کشیدن و رها کردن انجام می دهیم. ولی بهتر است از منوی کلیک راست و انتخاب گزینه Move این کار را انجام دهیم. به خاطر داشته باشید که وقتی کاربری را منتقل می‌کنیم باید اشیاء سیاست‌های گروهی (GPOs) را که به کاربر اعمال می‌شود عوض کنیم. GPO در فصل ۶ "زیر ساخت سیاست‌های گروهی " بحث می‌شود.

برای انتقال کاربر با ابزار خط فرمان از دستور Dsmove استفاده می شود. شکل فرمان به صورت زیر است:

```
Dsmove UserDN -newparent TargetOUDN
```

این دستور از کلاس شیء کاربر استفاده نمی‌کند. در عوض DN کاربر و در محل TargetOUDN، OU DN را که کاربر به آن منتقل می‌شود مشخص می‌کنیم.

برای انتقال کاربر در PowerShell ویندوز باید از متد psbase.MoveTo استفاده کنیم. دو خط زیر کاربر را منتقل می‌کند:

```
$objUser = [ADSI] "LDAP://UserDN"
$objUser.psbase.MoveTo("LDAP://TargetOUDN")
```

این مثالی دیگر از یک workaround مورد نیاز است که علت آن نسخه PowerShell ویندوز است که یک Active Directory provider ارائه نمی‌کند. در آینده می‌توانیم از Move-Item cmdlet استفاده کنیم همانطوری که برای provider های سیستم فایل و رجیستری استفاده می‌کنیم.

در VBScript از رویکرد ظاهراً قدیمی‌تری استفاده می‌کنیم. به این صورت که به container مقصد متصل می‌شویم و شیء کاربر را گرفته و به container جدید منتقل می‌کنیم. دو خط زیرین مثالی از این کد است:

```
Set objOU = GetObject("LDAP://TargetOUDN")
objOU.MoveHere "LDAP://UserDN" , vbNullString
```

ثابت vbNullString مقدار Null را به متد MoveHere برمی‌گرداند و معنی آن اینست که کاربر با همان CN قبلی به جای جدید منتقل شود.

تغییر نام حساب کاربری

در بخش "نام‌های حساب کاربری" درباره بسیاری از نام‌های مرتبط با یک حساب کاربری یاد گرفتیم. اگر نام بخواهیم کاربری را تغییر دهیم باید یک یا چند خصیصه را تغییر دهیم. برای تغییر نام کاربر روی آن کلیک راست کرده و Rename را انتخاب می‌کنیم. CN جدید را برای کاربر وارد کرده و Enter را می‌زنیم. کادر محاوره‌ای Rename User ظاهر می‌شود و از ما می‌خواهد که Full Name (که ترکیب CN و خصیصه Name کاربر است) ، First Name، Last Name، Display Name، User Logon Name، User Logon Name (Pre-Windows 2000) را وارد کنیم

در خط فرمان از دستور Dsmod.exe به شکل زیر استفاده می‌کنیم:

```
Dsmod user UserDN [-upn UPN][-fn FirstName][-mi Initial][-ln LastName][-dn DisplayName][-email EmailAddress]
```

امکان تغییر خصیصه samAccountName و CN با دستور Dsmod.exe وجود ندارد.

برای تغییر CN یک شیء از طریق خط فرمان باید از PowerShell ویندوز یا VBScript استفاده کنید. در powerShell ویندوز دو خط زیر این کار را انجام می‌دهد:

```
$objUser = [ADSI]"LDAP://UserDN"
$objUser.psbase.rename("CN=New CN")
```

از متد Put شیء کاربر برای تغییر دیگر خصیصه‌های نام استفاد می‌شود.

برای تغییر نام کاربر با VBScript از متد MoveHere مانند زیر استفاده می‌کنیم:

```
Set objOU = GetObject("LDAP://CurrentOUDN")
objOU.MoveHere "LDAP"//UserDN" , "CN=Nrew CN"
```

در این دو خط به OU فعلی کاربر متصل شده و از متد OU MoveHere برای تغییر CN کاربر استفاده می‌کنیم.

تمرینات نگهداری از حساب‌ها و اشیاء کاربر

در این تمرین پروسه‌هایی اجرا می‌شود که در اجرای عملیات نگهداری حساب‌های کاربری در یک شبکه سازمانی به ما کمک می‌کند.

برای اجرای تمرینات باید تمرینات درس ۱ و ۲ را اجرا کرده باشید و کاربران زیر در People OU ایجاد شده باشند:

- Tony Krijnen
- Linda Mitchell
- Scott Mitchell
- April Stewart

تمرین ۱ دیدن تمام خصیصه‌های کاربر

در این تمرین از Attribute Editor برای مشاهده و تغییر خصیصه‌های کاربر که در ابزار Active Directory Users And Computers قابل مشاهده نیستند استفاده می‌شود.

۱. با کاربر Administrator به SERVER01 وارد شده و ابزار Active Directory Users And Computers را باز کنید.
۲. در People OU روی Tony Krijnen کلیک راست کرده و Properties را انتخاب می‌کنیم.
۳. زبانه‌های کادر محاوره‌ای Properties را چک می‌کنیم.
چه خصیصه‌هایی قابل مشاهده هستند؟ آیا موردی که قبلا ندیده‌اید می‌بینید؟ آیا خصیصه‌ای که اطلاعات مفیدی راجع به سازمان ارائه دهد می‌بینید؟
۴. زبانه Telephone را باز کرده و اطلاعاتی را در فیلد Notes وارد کنید. OK را می‌زنیم.
۵. منوی View را باز کرده و Advanced Features را انتخاب می‌کنیم.
۶. پنجره Properties مربوط به کاربر Tony Krijnen را دوباره باز کرده و زبانه Attribute Editor را کلیک می‌کنیم.
۷. اسکرول می‌کنیم تا خصیصه info را ببینیم. آنجا چه می‌بینید ؟
۸. خصیصه division را پیدا کرده، دوبار کلیک می‌کنیم و تایپ می‌کنیم . Subsidiary
۹. خصیصه employeeID را پیدا کرده و دوبار کلیک کرده و عدد 104839 را تایپ می‌کنیم.
۱۰. خصیصه‌های دیگری که در Attribute Editor قابل مشاهده هستند بررسی کنید.
چه خصیصه‌هایی آن‌جا می‌بینید که در ابزار Active Directory Users And Computers قابل مشاهده نیست؟ آیا هیچ خصیصه پنهانی وجود دارد که اطلاعات مفیدی راجع به شرکت ارائه کند؟
۱۱. روی OK کلیک کرده تا کادر Properties بسته شود.

تمرین ۲ خصیصه‌های چند شیء را با هم مدیریت کنید

در این تمرین چند شیء انتخاب شده و خصوصیات اشیاء پیکربندی می‌شود.

۱. در People OU ، Scott Mitchell را انتخاب کنید.

۲. کلید CTRL را نگه دارید و Linda Mitchell و April Stewart را هم انتخاب کنید.
الان باید سه کاربر انتخاب شده باشد.
۳. روی یکی از کاربران انتخاب شده کلیک راست کرده و Properties را انتخاب کنید.
کادر محاوره‌ای Properties با یک سری از خصوصیات کاربری که همزمان برای چند کاربر قابل انتخاب است باز می‌شود.
۴. در زبانه General کادر Office را انتخاب کرده و کلمه Miami را در کادر تایپ می‌کنیم.
۵. زبانه Account را کلیک می‌کنیم.
در این سناریو این سه کاربر در طول هفته کار می‌کنند و اجازه ندارند در آخر هفته به شبکه وارد شوند.
۶. کادر Logon Houres را انتخاب می‌کنیم و دکمه Logon Houres را می‌زنیم.
۷. روی Sunday کلیک می‌کنیم و دکمه Logon Denied را کلیک می‌کنیم.
۸. روی Saturday کلیک می‌کنیم و دکمه Logon Denied را کلیک می‌زنیم. بعدOK می‌کنیم.
به علاوه سه کاربر اجازه ورود به شبکه را از طریق کامپیوترهای مشخصی دارند.
۹. کادر Computers Restrictions را انتخاب کرده و دکمه Logon To را کلیک می‌کنیم.
۱۰. گزینه Following Computers را انتخاب می‌کنیم.
۱۱. در کادر Computer Name کلمه DESKTOP101 را وارد می‌کنیم.
۱۲. مراحل را برای DESKTOP102 و DESKTOP103 تکرار می‌کنیم. سپس OK را می‌زنیم.
۱۳. در زبانه Address کادرهای Street، City، State/Provine و ZIP/Postal Code را علامت بزنید. در این کادرها اطلاعات فرضی وارد کنید.
۱۴. روی زبانه Profile کلیک کرده و home folder را با عبارت \\server01\%username%\documents پیکربندی کنید.
۱۵. روی زبانه Organizational کلیک کرده و نام شرکت را پیکربندی کنید Contoso, Ltd .
۱۶. روی OK کلیک کنید.
۱۷. اشیاء کاربر را بررسی کنید تا مطمئن شوید تغییرات اعمال شده است.

تمرین ۳ خصیصه‌های کاربر را با دستور DS مدیریت کنید.

در این سناریو Linda و Scott Mitchell از میامی به سیدنی منتقل می‌شوند. آنها سه هفته فرصت دارند تا نقل مکان کنند. حساب آنها باید تغییر کند.

۱. PowerShell ویندوز را باز کنید.
PowerShell ویندوز دستورات اجرایی را اجرا می‌کند.
۲. فکر کنید چطور می‌توان با یک دستور خصیصه office دو کاربر را به Sydney تغییر داد و حساب‌های کاربری را در زمانی که کاربران در حین انتقال هستند غیرفعال کرد.
۳. دستور زیر را تایپ کرده و Enter را بزنید:

```
Dsquery user –name “* Mitchell” | dsmod user -office “Sydney” -disabled yes
```

۴. در ابزار Active Directory Users And Computers حساب‌های کاربری را چک کنید تا مطمئن شوید تغییرات اعمال شده است.
۵. حالا باید رکوردی شامل نام کاربری قبل از ویندوز 2000 و UPN بسازیم. چه دستوری به تنهایی این اطلاعات را نمایش می‌دهد؟
۶. دستور زیر را تایپ کرده و Enter را بزنید:

```
Dsquery user -name “* Mitchell” | dsget user -samid -upn
```

خانواده Mitchell به سیدنی می‌رسند. الان موقع فعال کردن حساب آن‌هاست.
۷. در PowerShell ویندوز خطوط زیر را تایپ کنید:

```
$objUser = [ADSI]”LDAP”//CN=Linda Mitchell,OU=People,DC=contoso,DC=com”
```

```
$objUser.psbase.InvokeSet('AccountDisabled',$false)
$objUser.SetInfo()
```

۸. در ابزار Active Directory Users And Computers حساب Linda Mitchell را چک کنید تا مطمئن شوید فعال شده است.

۹. روی حساب Scott Mitchell کلیک راست کنید و Enable Account را انتخاب کنید.

تمرین ۴ ریست کلمه عبور و باز کردن قفل حساب کاربری

فرض کنید در حین انتقال از میامی به سیدنی Scott Mitchell کلمه عبور خود را فراموش کرده است. پس از این‌که حسابش فعال شد چند بار سعی می‌کند با کلمه عبور اشتباه به سیستم وارد شود و در نتیجه حساب قفل می‌شود. در این تمرین قرار است کلمه عبور Scott ریست شده و قفل حساب او باز شود.

۱. در ابزار Active Directory Users And Computers OU People را انتخاب کنید.

۲. در پنل وسط روی حساب Scott Mitchell کلیک راست کرده و گزینه Reset Password را اننتخاب کنید.

۳. کلمه عبور جدید را برای Scott در کادرهای New Password و Confirm Password وارد می‌کنیم.

۴. علامت کادر User Must Change Password At Next Logon را بزنید.

۵. کادر Unlock The User's Account را علامت بزنید.

۶. OK را بزنید.

خلاصه درس

- از Attribute Editor برای مشاهده و تغییر همه خصیصه‌های شیء کاربر استفاده می‌شود.
- خصیصه‌های حساب کاربری می‌تواند طوری پیکربندی شود که ورود کاربر را از روی برخی کامپیوترها محدود کند، ساعات ورود کاربر را محدود کند و برای حساب تاریخ انقضاء مشخص کند.
- امکان تغییر خصیصه‌های کاربران بصورت گروهی توسط دستور Dsmod.exe یا با انتخاب چند شیء در ابزار Active Directory Users And Computers وجود دارد. بهرحال خصوصیات قابل تغییر با هر متدی محدود خواهد بود. همچنین می‌توان از اسکریپت‌هایی نظیر VBScript و PowerShell ویندوز برای تغییر خصیصه‌های کاربر استفاده کرد.
- وقتی حساب کاربری حذف می‌شود و حسابی با همان نام ساخته می‌شود حساب جدید به گروهی که کاربر قبلی عضو آن بوده تعلق نخواهد داشت و به همان منابع دسترسی پیدا نخواهد کرد. بنابراین باید دسترسی‌ها و گروه‌بندی‌ها دوباره تعیین شود.

سئوالات پایان درس

۱. می‌خواهیم خصیصه Office ده کاربر را در دو OU مختلف مشخص کنیم. خصیصه Office فعلی کاربران Miammi می‌باشد. شما اخیرا متوجه اشتباه تایپی شده‌اید و می‌خواهید آن را به Miami تغییر دهید. چکار می‌کنید؟ (ممکن است بیش از یک جواب داشته باشد)

A. همه ده کاربر را با نگه داشتن کلید Ctrl انتخاب کرده و پنجره Properties را باز می‌کنیم.
B. از Dsget و Dsmod استفاده می‌کنیم.
C. از Dsquery و Dsmod استفاده می‌کنیم.
D. از Get-Item و Move-Item استفاده می‌کنیم.

۲. می‌خواهیم کاربری را از Paris OU به Moscow منتقل کنیم. از کدام ابزار استفاده می‌کنیم؟ (ممکن است بیش از یک جواب داشته باشد)

A. Move-Item
B. متد MoveHere از Moscow OU
C. Dsmove
D. Redirusr.exe
E. Active Directory Migration Tool

۳. کاربری گزارش می‌دهد که پیغامی دریافت کرده که متن آن به این شکل است "Your Account Is Configured To Prevent You From Using The Computer.Please Try Another Computer" چه باید بکنیم تا کاربر بتواند به کامپیوتر وارد شود.

A. روی دکمه Log On To در زبانه Account حساب کاربریش کلیک می‌کنیم.
B. روی دکمه Allowed To Join Domain در کادر محاوره‌ای New Computer کلیک کنید.
C. از دستور Dsmove استفاده کنید.
D. با استفاده از Local Security Policy به کاربر حق Log On Locally می‌دهیم.

فصل ٤

گروهها

هرچند کاربران، کامپیوترها و حتی سرویس‌ها در طول زمان تغییر می‌کنند نقش‌ها و قوانین کمتر دستخوش تحول می‌شوند. احتمالا یک شرکت دارای نقش مالی می‌باشد که نیازمند توانایی‌های خاصی در سازمان است. کاربر یا کاربرانی که این نقش را اجرا می‌کنند جابجا می‌شوند ولی نقش آنان باقی می‌ماند. به همین دلیل انتساب حقوق و مجوزها برای هویت‌هایی نظیر کاربرها، کامپیوترها یا سرویس‌ها درست نیست. وظایف مدیریتی بهتر است به گروهها محول شوند. در این درس از گروهها برای تعیین نقش‌های کاربری و مدیریتی، فیلتر کردن سیاست‌های گروهی، تعیین سیاست‌های کلمه عبور یکتا، اعطا حقوق و مجوزهای دسترسی و بسیاری موارد دیگر استفاده می‌کنیم. در این درس یاد می‌گیریم که چطور برای این وظایف شیء گروه در AD DS دامنه بسازیم، تغییر دهیم و حذف کنیم.

اهداف امتحانی در این فصل:

- ساخت و نگهداری اشیاء Active Directory
  - خودکارسازی ساخت اشیاء در Active Directory
  - نگهداری حساب‌های Active Directory

دروس این فصل:

- درس ۱ : ساخت و مدیریت گروهها
- درس ۲: خودکارسازی ساخت و مدیریت گروهها
- مدیریت گروهها در سازمان

قبل از شروع

در این فصل از PowerShell ویندوز، Microsoft VBScript، CSVDE و LDIFDE برای خودکارسازی ساخت گروهها استفاده می‌شود. قبل از شروع این فصل درس ۱ و ۲ از فصل ۳ باید مطالعه شود.

به علاوه برای اجرای تمرینات در این فصل نیاز به DC با نام SERVER01 داریم . برای مرور جزئیات این کار به فصل ۱ مراجعه کنید.

در دنیای واقعی

دن هلم

مدیریت موثر و مناسب گروهها باعث افزایش امنیت، تداوم و بهره‌وری در فضای IT می‌گردد. من به عنوان مشاور زمان زیادی را با کاربران جهت سازگار کردن تکنولوژی با نیازهای کاری آنان صرف کرده‌ام. در مورد تکنولوژی‌های ویندوزی باید گفت که تعریف و پیاده‌سازی نقش‌های کاری و قوانین را به دنبال دارد بطوریکه مدیریت تعریف شده مستند و خودکار انجام می‌گیرد. این پروسه اغلب نیازمند ارتقاء دانش، تکنولوژی و پروسه‌های مدیریت گروه‌های کاربری می‌باشد. بسیاری از متخصصین IT هنگام کار با ویندوز سرور 2008 از تکنیک‌های قدیمی استفاده می‌کنند که از مزایای گروهها به طور کامل بهره نمی‌گیرد. در حقیقت موارد بسیاری دیده شده که به علت مدیریت ضعیف گروه‌ها بهره‌وری و امنیت به شدت کاهش یافته و من ترجیح دادم دو بخش از کتاب خود را (Windows Administration resource Kit: Productivity Solutions for IT Professionals-Microsoft Press,2008) به آن اختصاص دهم که مربوط به ارتقاء و خودکارسازی مدیریت گروه است. در این درس آن چیزی را یاد می‌گیرید که برای امتحان نیاز است و تعدادی از نکته‌ها و عملیاتی را که برای کار با گروهها در سازمان نیاز دارید. اکیدا توصیه می‌شود برای اطلاعات بیشتر و آشنایی با ابزارهای جالب در رابطه با مدیریت گروه به resource kit مراجعه کنید.

درس ۱ : ساخت و مدیریت گروه‌ها

شما مطمئنا با اهداف گروهها آشنا هستید جمع کردن آیتم‌ها و مدیریت آنها به عنوان یک موجودیت. پیاده سازی مدیریت گروهها در Active Directory ، ذاتی نیست چون Active Directory برای پشتیبانی از شبکه‌های بزرگ و توزیع شده طراحی شده و هفت نوع گروه را شامل می‌شود: دو نوع گروه تحت دامنه هر کدام سه scope و گروههای امنیتی محلی. در این درس اهداف هر کدام از این گروهها را یاد می‌گیریم و اینکه چطور نیازمندیهای کاری را با گزینه‌های پیچیده که Active Directory سر راه ما می‌گذارد تطبیق دهیم.

بعد از این درس می‌توانید:

- با استفاده از ابزار Active Directory Users and Computers گروه بسازید.
- نوع و حوزه گروه را مدیریت کرده و به یکدیگر تبدیل کنید.
- انواع گروهها را که می‌توانند عضو گروههای حوزه‌های مختلف شوند تعیین کنید.
- اعضاء گروهها را مدیریت کنید.
- یک استراتژی مدیریت گروه ایجاد کنید.

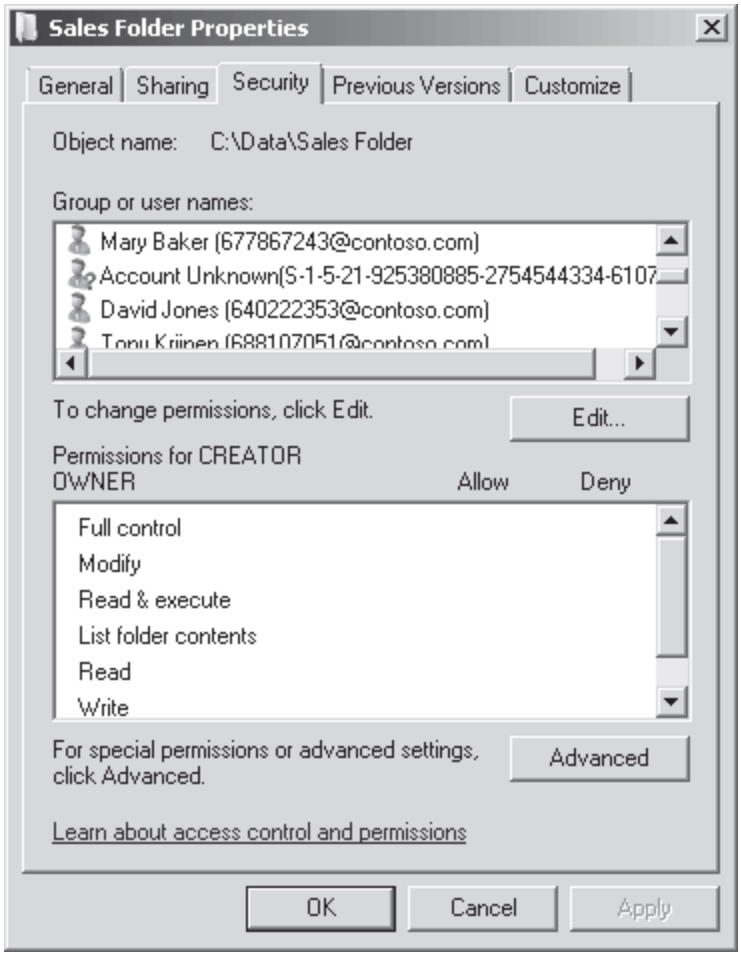
زمان درس : ۴۵ دقیقه

مدیریت یک شبکه با گروهها

گروهها واحدهایی با یک مشخصه امنیتی (SID) هستند که به واسطه خصیصه member و به منظور تسهیل مدیریت، دیگر واحدهای امنیتی را شامل می‌شوند (کاربران، کامپیوترها، اطلاعات تماس و دیگر گروهها)

تصور کنید همه ۱۰۰ کاربر در بخش فروش نیاز به دسترسی خواندن به یک پوشه روی سرور دارند. اعطاء مجوز به تک تک کاربران به طور اختصاصی منطقی به نظر نمی‌آید. وقتی فروشنده جدیدی استخدام می‌شود باید حساب جدید را به ACL پوشه اضافه کنید. وقتی حسابی حذف می‌شود باید مجوزهای آن را از ACL حذف کنید یا ACL را همانطوری که در شکل ۴- ۱ نمایش می‌دهد با SID مربوط به کاربر حذف شده رها کنید. حالا فرض کنید ۱۰۰ کاربر باید به ۱۰ پوشه روی سه سرور دسترسی داشته باشند. مشکلات مدیریتی به شدت افزایش پیدا می‌کند.

بی شک می‌دانید که هرچند امکان اعطاء مجوز نسبت به منابع به صورت تک تک (کاربر یا کامپیوتر) وجود دارد راه حل مناسب اعطاء یک مجوز به یک گروه بوده و برای مدیریت دسترسی ها به منابع عضویت گروه را تغییر می‌دهیم.



شکل ۱- ۴ یک ACL با یک SID که به یک حساب حذف شده منتسب است.

در ادامه تمرین گروهی به نام Sales ساخته می‌شود و به آن دسترسی فقط خواندنی نسبت به ده پوشه روی سه سرور داده می‌شود. با این کار یک نقطه مرکزی مدیریتی ایجاد می‌شود. گروه مذکور دسترسی به پوشه مشترک را به طور موثر مدیریت می‌کند. از این پس با اضافه کردن کاربران جدید بخش فروش به گروه Sales دسترسی به ده پوشه مشترک را برای آنان امکانپذیر می‌کنیم. وقتی حسابی حذف می‌شود بطور خودکار از گروه حذف می‌شود بنابرین SID آنان دیگر در ACL وجود نخواهد داشت. همچنین مزیت دیگری نیز وجود دارد به این ترتیب که چون ACL برای گروه Sales که مجوز خواندن دارند ثابت است مراحل پشتیبان گیری ساده‌تر می‌شود. وقتی ACL پوشه‌ای عوض می‌شود ACL جدید به همه پوشه‌ها و فایل‌ها دیکته می‌شود و پرچم آرشیو آنها ست شده و در پشتیبان گیری بعدی لحاظ می‌گردد حتی اگر فایل‌ها تغییری نکرده باشد.

فرض کنید کارمندان بخش فروش تنها کسانی نیستند که باید به پوشه‌ها دسترسی خواندن داشته باشند. کارکنان بخش بازاریابی و مشاوران فروش استخدام شده نیز نیاز به دسترسی مشابه دارند. برای این کار می‌توان این گروهها را به سرعت به ACL پوشه اضافه کرد. برای ایجاد دسترسی سه گروه نسبت به ده پوشه‌ای که روی سه سرور وجود دارند باید سی بار عملیات اعطاء مجوز را تکرار کنیم. اگر بخواهیم گروهی را به این‌ها اضافه کنیم باید مراحل را ده بار دیگر تکرار کنیم. حالا اگر هشت کاربر دیگر که عضو گروههای بالا نیستند نیاز به پوشه‌ها داشته باشند چه باید کرد؟ ایا باید آنها را تک تک به ACL اضافه کنیم؟

خیلی زود متوجه شدیم که استفاده از یک نوع گروه ، گروهی که نقش‌های کاری کاربران را تبیین می‌کند، مدیریت موثری را روی ده پوشه اعمال نمی‌کند. راه حل این است که دو نوع گروه را برای مدیریت بهتر انتخاب کنیم. کاربران را باید بر اساس نقش کاری‌شان به عنوان مجموعه در نظر گرفت و دسترسی به ده پوشه را مدیریت کنیم. این ده پوشه نیز مجموعه‌ای از آیتم ها به حساب می‌آیند. آنها منبع واحدی هستند که به منظور توزیع بین ده پوشه روی سه سرور ایجاد شده‌اند. ما داریم تلاش می‌کنیم دسترسی خواندن به مجموعه را مدیریت کنیم. ما به یک نقطه مدیریتی واحد نیاز داریم تا بتوانیم دسترسی به منابع را مدیریت کنیم.

برای این کار به یک گروه نیاز داریم که دسترسی فقط خواندنی به ده پوشه روی سه سرور داشته باشد. در نظر بگیرید پوشه‌ای با نام ACL_Sales Folders_Read ایجاد شود و دسترسی فقط خواندنی به ده پوشه را به آن اعطاء کنیم. بعد گروههای Sales،

Marketting و Consultants را به همراه هشت کاربر دیگر عضو گروه ایجاد شده می‌کنیم. وقتی بخواهیم به کاربری یا گروهی دسترسی فقط خواندنی نسبت به پوشه‌ها اعطاء کنیم آن را عضو همین گروه می‌کنیم. از این راه به راحتی می‌توان گزارش گرفت که چه کسانی به پوشه‌ها دسترسی دارند. بدین ترتیب به جای این که ACL ده پوشه را بررسی کنیم کافی است اعضاء گروه ACL_Sales Folders_Read را بررسی کنیم.

رویکرد مدیریت شبکه بر اساس گروهها مدیریت مبتنی بر نقش (role-based management) نام دارد. در این رویکرد نقش کاربران بر اساس وضعیت کاری آنان مشخص می‌شود. برای مثال بخش کاری یا دپارتمان مانند فروش بازاریابی و مشاوره مشخص شده و قوانین کاری روی آن پیاده می‌شود. مثلا مشخص می‌کنیم که کدام نقش‌ها به پوشه‌ها دسترسی داشته باشند.

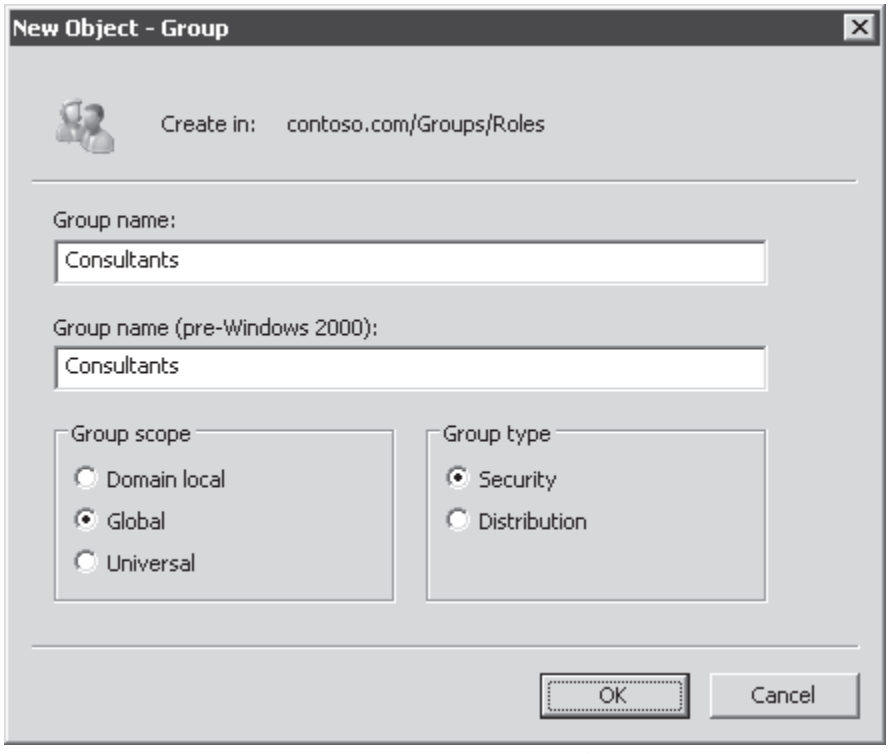
با استفاده از گروهها به هر دو وظیفه مدیریتی در دایرکتوری دست پیدا می‌کنیم. گروهها نماینده نقش‌ها خواهند بود که کاربران، کامپیوترها و نقش های دیگر را در بر می‌گیرند. بله نقش‌ها هم می‌توانند نقش‌های دیگر را در برگیرند. برای مثال نقش مدیریت نقش‌های مدیران فروش مالی و تولید را دربر می‌گیرد. قوانین نظیر قانون دسترسی به پوشه‌ها توسط گروهها نمایندگی می‌شود. گروههای قوانین گروههای نقش و گاهی کاربران یا کامپیوترهای خاصی مانند همان هشت کاربر مثال ما را شامل می‌شوند.

برای دستیابی به مدیریت پذیری شبکه سازمانی در هر اندازه و پیچیدگی باید گروهها را به طور موثر مدیریت کنیم و زیرساخت گروه را طوری پایه‌ریزی کنیم که فقط یک نقطه مدیریتی واحد برای قوانین و نقش‌ها داشته باشیم. از لحاظ فنی یعنی یه گروههایی نیاز داریم که اعضاء کاربر کامپیوتر گروههای دیگر و حتی واحدهای امنیتی را از دامنه‌های دیگر در برگیرد.

برای اطلاعات بیشتر درباره مدیریت مبتنی بر نقش‌ها به منبع Windows Administration Resource Kit: Productivity Solutions for IT Professional

تعریف قواعد نام‌گذاری گروه

برای ساخت گروه با ابزار Active Directory Users And Computers روی OU که می‌خواهید گروه در آن ایجاد شود کلیک راست کرده و New بعد Group را انتخاب کنید. کادر محاوره‌ای New Object – Group طوری که در شکل ۴- ۲ نشان می‌دهد امکان تعریف خصوصیات اساسی گروه جدید را به ما می‌دهد.



شکل ۴- ۲ کادر محاوره‌ای Object - Group

اولین خصیصه‌ای که باید پیکربندی شود نام گروه است. گروه همانند کاربر یا کامپیوتر اسامی متعددی دارد. اول اسمی است که در کادر Group Name در شکل ۴- ۲ نشان داده شده است و توسط ویندوز 2000 و سیستم‌های قدیمی‌تر برای تشخیص شیء استفاده می‌شود و خصیصه‌های CN و Name شیء را می‌سازد. دوم نام قبل از ویندوز 2000 است که خصیصه sAMAccountName را

می‌سازد که توسط کامپیوترهای ویندوز NT 4.0 و بعضی دستگاه‌های خاص مورد استفاده در شبکه نظیر NAS که سیستم عامل غیر مایکروسافتی دارند برای تشخیص گروه استفاده می‌شود. خصیصه CN و Name باید در container یا OU که گروه در آن ساخته می‌شود منحصر باشد. sAMAccountName باید در کل دامنه منحصر باشد. از لحاظ فنی sAMAccountName باید از لحاظ مقداری با CN و Name تفاوت داشته باشد ولی توصیه می‌شود این کار را نکنید. نامی را که در دامنه منحصر است انتخاب کرده و آن را در هر دو فیلد نام کادر محاوره‌ای New Object – Group وارد کنید.

نامی که انتخاب می‌کنیم باید ما را در مدیریت گروه و شبکه به صورت روزمره کمک کند. پیشنهاد می‌شود قوانین نام‌گذاری گروه طوری تعیین شود که نمایانگر نوع و هدف گروه باشد. در مثال قبل نام گروه ACL_Sales Folder_Read بود. پیشوند نام نشان می‌دهد که گروه برای اعطاء مجوز به یک پوشه استفاده می‌شود در اینجا ACL. بخش اصلی نام منبع را که با استفاده از گروه مدیریت می‌شود مشخص می‌کند در اینجا Sales Folder. پسوند مشخص می‌کند با این گروه چه چیزی مدیریت می‌شود یعنی دسترسی فقط خواندنی. یک جداکننده در این جا "_" برای جداسازی بخش‌های نام به کار می‌رود. توجه کنید که کاراکتر جداکننده بین کلمات Sales و Folders به کار نمی‌رود. در نام‌گذاری گروهها استفاده از فاصله مجاز است. در عوض باید در صورت استفاده از فاصله در نام گروه اگر بخواهیم از آن در دستورات استفاده کنیم باید آن را در گیومه قرار دهیم. می‌توانیم اسکریپت‌هایی بسازیم که از جداکننده‌ها برای deconstruct کردن نام گروهها استفاده می‌کنند تا گزارش گیری و ممیزی راحت‌تر انجام شود. به خاطر داشته باشید که گروههای نقش که نقش‌های کاربران را تعریف می‌کنند اغلب توسط کاربران غیرفنی استفاده می‌شوند. به عنوان مثال می‌توانیم e-mail گروه Sales را فعال کنیم تا به عنوان لیست توزیع e-mail استفاده شوند. بنابراین پیشنهاد می‌شود از پیشوند در نام گروه استفاده نکنیم تا نام گروه برای کاربران ملموس‌تر شود.

برای اطلاعات بیشتر درباره مدیریت گروهها به طور موثر به منبع Windows Administration Resource Kit: Productivity Solutions for IT Professionals.

انواع گروه‌ها

دو نوع گروه موجود است : امنیتی (Security) و توزیع (Distribution). وقتی گروهی ساخته می‌شود باید نوع آن را در کادر محاوره‌ای New Object – Group مشخص کنیم.

گروههای توزیع توسط برنامه‌های پست الکترونیک استفاده می‌شود. این گروهها قابلیت امنیتی ندارند. چون SID ندارند بنابراین به آنها نمی‌توان مجوز اعطا کرد. با ارسال پیام به یک گروه توزیع پیام مذکور به همه اعضای گروه ارسال می‌شود.

گروههای امنیتی واحدهای امنیتی دارای SID هستند. و SID آنها می‌تواند برای کنترل دسترسی به منابع در ACL آن منبع قرار گیرد. همچنین این گروهها می‌توانند به عنوان گروههای توزیع استفاده شوند. هرگاه بخواهیم از گروهی در مدیریت امنیت استفاده کنیم آن گروه باید امنیتی باشد.

بدلیل اینکه گروههای امنیتی قابلیت گروههای توزیع را نیز دارد بسیاری از شرکت‌ها ترجیح می‌دهند همیشه از این نوع گروه استفاده کنند. ولی توصیه می‌شود اگر منظور فقط ارسال e-mail است از گروه توزیع استفاده شود. در غیر این صورت به گروه SID تعلق می‌گیرد و این SID به توکن دسترسی امنیتی کاربر اضافه می‌شود که باعث افزایش بی‌رویه حجم توکن می‌شود.

حوزه گروه

اعضای گروه شامل کاربران، کامپوترها و گروههای دیگر است. یک گروه می‌تواند عضو گروه دیگر باشد. می‌توان به گروه توسط ACL، فیلترهای GPO و دیگر کامپوننت‌های مدیریتی رجوع کرد. حوزه گروه روی همه ویژگی‌های مذکور تاثیر می‌گذارد. گروهها چه چیزهایی را دربر می‌گیرند و کجا می‌توان از آن‌ها استفاده کرد. چهار حوزه برای گروهها موجود است : global، domain local، local و universal .

ویژگی‌های تعریف شده در هر حوزه در این دسته‌ها قرار می‌گیرند:

- **تکثیر** گروه کجا تعریف می‌شود و به کدام سیستم‌ها تکثیر می‌شود.
- **عضویت** چه نوع واحد امنیتی می‌تواند عضو گروه باشد؟ آیا واحدهای امنیتی از دامنه‌های مورد اعتماد (Trusted) دیگر می‌توانند عضو این گروه شوند؟

در فصل ۱۲ "دامنه و Forest" درباره ارتباطات trust بحث می‌شود. Trust دامنه را قادر می‌سازد برای تایید هویت به دامنه دیگر مراجعه کند و واحدهای امنیتی را از دامنه دیگر به عنوان عضو گروه اضافه کند و به واحدهای امنیتی دامنه‌های دیگر مجوز اعطاء کند. اصطلاح مورد استفاده در این مبحث کمی گیج‌کننده است. وقتی دامنه A ارتباط trust با دامنه B برقرار می‌سازد دامنه A دامنه اعتمادکننده (trusting) و دامنه B دامنه مورد اعتماد (trusted) خواهد بود. دامنه A اعتبار کاربران دامنه B را قبول می‌کند. دامنه A برای تایید هویت درخواست‌های کاربران دامنه B را به DC دامنه B می‌فرستد چون به انباره هویت و سرویس تایید هویت دامنه B اعتماد دارد. دامنه A می‌تواند واحدهای امنیتی دامنه B را به گروهها و ACL های دامنه A اضافه کند. برای جزئیات بیشتر به فصل ۱۲ مراجعه کنید.

نکته امتحانی در مورد عضویت گروهها به خاطر داشته باشید وقتی دامنه A به دامنه B اعتماد می‌کند دامنه B دامنه مورد اعتماد است و کاربران و گروههای Global آن می‌توانند عضو گروههای domain local دامنه A شوند. به علاوه به کاربران و گروههای global دامنه B می‌توان مجوز برای دسترسی به منابع دامنه A اعطاء کرد.

- **دسترسی پذیری** از گروه در کجا می‌توان استفاده کرد؟ آیا می‌توان آن را عضو گروه دیگر کرد؟ آیا می‌توان آن را به ACL اضافه کرد؟

این ویژگی‌ها را به خاطر داشته باشید که در هر حوزه گروه جزئیات آن بررسی می‌شود.

گروههای محلی (Local)

این گروهها به معنی واقعی کلمه محلی هستند. روی یک سیستم خاص ساخته می‌شوند و روی همان سیستم به کار گرفته می‌شوند. گروههای محلی در بانک اطلاعاتی SAM یک کامپیوتر عضو دامنه ساخته می‌شوند. سیستم‌های عضو workgroup و دامنه هر دو گروههای محلی دارند. در شبکه workgroup از گروههای محلی برای مدیریت امنیت منابع سیستم استفاده می‌شود. در شبکه‌های مبتنی بر دامنه مدیریت گروههای محلی کامپیوترها محدود شده و در بیشتر موارد غیرضروری به نظر می‌رسند. ساخت گروههای محلی سفارشی در سیستم‌های عضو دامنه پیشنهاد نمی‌گردد. در حقیقت گروههای محلی Users و Administrators تنها گروههایی هستند که باید در مدیریت دامنه در نظر گرفته شوند. به طور خلاصه :

- تکثیر گروه محلی فقط روی SAM سیستم عضو دامنه ساخته می‌شود. گروه و عضویت به سیستم دیگری تکثیر نمی‌شود.
- عضویت یک گروه محلی می‌تواند اعضاء زیر را داشته باشد:
  - هر واحد امنیتی از دامنه مانند کاربران کامپیوترها گروههای global یا domain local.
  - کاربران کامپیوترها و گروههای global از هر دامنه‌ای در forest .
  - کاربران کامپیوترها و گروههای global از هر دامنه مورد اعتماد.
  - گروههای universal تعریف شده در هر دامنه در forest .
- دسترسی پذیری گروه محلی فقط در حوزه کامپیوتر خود اعتبار دارد و فقط در ACL های کامپیوتر خود قابل استفاده است. این نوع گروه نمی‌تواند عضو هیچ گروه دیگری باشد.

گروههای domain local

این گروهها برای مدیریت مجوزها استفاده می‌شود. برای مثال گروه ACL_Sales Folder_Read که قبلا بحث شد می‌تواند به عنوان گروه domain local ایجاد شود. این گروهها ویژگی‌های زیر را دارد:

- **تکثیر** این نوع از گروه در حوزه نام دامنه تعریف می‌شود. شیء گروه و اعضاء آن (خصیصه member) به تمام DC های دامنه تکثیر می‌شود.

- **عضویت** این نوع گروه می‌تواند دارای اعضاء زیر باشد:
  - همه واحدهای امنیتی دامنه شامل کاربران کامپیوترها گروههای global یا دیگر گروههای domain local
  - کاربران کامپیوترها و گروههای global از همه دامنه‌های forest
  - کاربران کامپیوترها و گروههای global از همه دامنه‌های مورد اعتماد
  - گروههای universal تعریف شده در همه دامنه‌های forest
- **دسترسی‌پذیری** این نوع گروه می‌تواند به ACL هر منبعی روی همه اعضاء دامنه اضافه شود. به علاوه می‌تواند عضو گروههای domain local دیگر یا گروههای محلی کامپیوتر شود.

وضعیت عضویت گروه domain local دقیقاً مشابه گروههای محلی می‌باشد ولی تکثیر و در دسترس بودن گروه domain local در کل دامنه آن را از نوع محلی متمایز می‌کند. بنابراین این نوع از گروهها برای تعریف قوانین مدیریت کاری مانند قوانین دسترسی کاملا مناسب هستند چون در هر جای دامنه کار می‌کنند و می‌توانند اعضاء را از هر نوعی در دامنه خود و یا از دامنه‌های مورد اعتماد دیگر در بر گیرند.

گروههای global

این گروهها برای تعریف مجموعه‌های اشیاء دامنه بر اساس نقش‌های کاری استفاده می‌شوند. گروههای نقش مانند sales و marketing که قبلا ساختیم و همچنین نقش‌های کامپیوتر مانند گروه Sales Laptop به عنوان گروههای global ساخته می‌شوند. مشخصات این گروهها به شرح زیر است:

- **تکثیر** این گروه در حوزه نام دامنه تعریف شده است. شیء گروه شامل خصیصه member به همه DCهای دامنه تکثیر می‌شود.
- **عضویت** این نوع گروه می‌تواند اعضاء کاربر ، کامپیوتر و گروههای global دیگر را فقط در همان دامنه در بر گیرد.
- **قابلیت‌دسترسی** این نوع گروه توسط همه اعضاء دامنه خود و دامنه‌های دیگر در forest و همچنین دامنه‌های خارجی مورداعتماد قابل استفاده است. این نوع گروه می‌تواند عضو یک گروه domain local یا universal در دامنه یا forest باشد. همچنین می‌تواند عضو هر گروه domain local در دامنه مورد اعتماد باشد. در نهایت یک گروه global می‌تواند به ACL های دامنه ، forest یا دامنه‌های دیگر مورد اعتماد افزوده شود.

همانطور که می‌بینید گروههای global بیشترین محدودیت گیری را دارند. (فقط کاربران کامپیوترها و گروههای global همان دامنه) ولی بیشترین وسعت دسترسی را در سطح دامنه، forest و دامنه‌های خارجی مورد اعتماد دارند. به خاطر همین برای تعریف نقش‌ها کاملا مناسب هستند. چون نقش‌ها مجموعه‌های اشیاء همان دایرکتوری هستند

گروههای universal

این گروهها در forest هایی با چند دامنه مفید هستند و امکان تعریف نقش‌ها یا مدیریت منابع را که بین چنددامنه در گردش است می‌دهد. بهترین راه درک این نوع گروه ذکر مثال است. فرض کنید موسسه Trey Research دارای یک forest با سه دامنه به نامهای Americas، Asia و Europe می‌باشد. هر دامنه حساب‌های کاربری و یک گروه global به نام Regional Managers را داراست که حساب کاربری مدیران همان منطقه را شامل می‌شود. به خاطر دارید که گروههای global فقط می‌توانند کاربران را از همان دامنه در بر گیرند. یک گروه universal به نام Trey Research

Regional Managers ساخته می‌شود و سه گروه Regional Managers به عنوان عضو به این گروه اضافه می‌شوند. بنابراین گروه ساخته شده نقشی را برای کل forest تعریف می‌کند. همانطوریکه کاربران عضو هر کدام از گروههای محلی شوند عضو گروه Trey Research Regional Managers نیز خواهند شد. شرکت تصمیم می‌گیرد محصول جدیدی تولید کند که نیازمند تعامل بین مناطق مختلف می‌باشد. منابع مربوط به پروژه روی فایل سرورها در هر دامنه ذخیره می‌شود. برای تعریف اینکه چه کسی بتواند فایلهای مربوط به محصول جدید را تغییر دهد یک گروه UNIVERSAL به نام ACL_New Product_Modify ایجاد می‌شود. به این گروه مجوز Allow Modify نسبت به پوشه‌های مشترک هر کدام از فایل‌سرورهای هر دامنه اعطاء می‌شود. گروه Trey Research Regional Managers عضوی از گروه نام ACL_New Product_Modify شده همانطوریکه گروههای global و چند کاربر هر منطقه عضو این گروه هستند.
همانطوریکه می‌بینید گروههای universal به ما این امکان را می‌دهد که گروههایی را که در دامنه‌های یک forest در گردش هستند یکپارچه کند و قوانینی را که در سطح forest اعمال می‌شود تعریف کنیم . گروههای universal ویژگی‌های زیر را دارند:

- **تکثیر** در یک دامنه در forest تعریف می‌شود. ولی به global catalog تکثیر می‌شود. در فصل ۱۰ "Domain Controllers" مطالب بیشتری درباره global catalog یاد می‌گیرید. اشیاء global catalog در سطح forest قابل دسترس است.

- **عضویت** این نوع گروه می‌تواند عضوهای کاربر، گروه global و دیگر گروههای universal هر دامنه از forest را داشته باشد.

- **قابلیت‌دسترسی** این نوع گروه می‌تواند عضو یک گروه universal دیگر یا domain local در سطح forest باشد. به علاوه یک گروه universal برای مدیریت منابع به عنوان مثال اعطاء مجوز در سطح forest می‌تواند استفاده شود.

خلاصه امکانات عضویت گروه

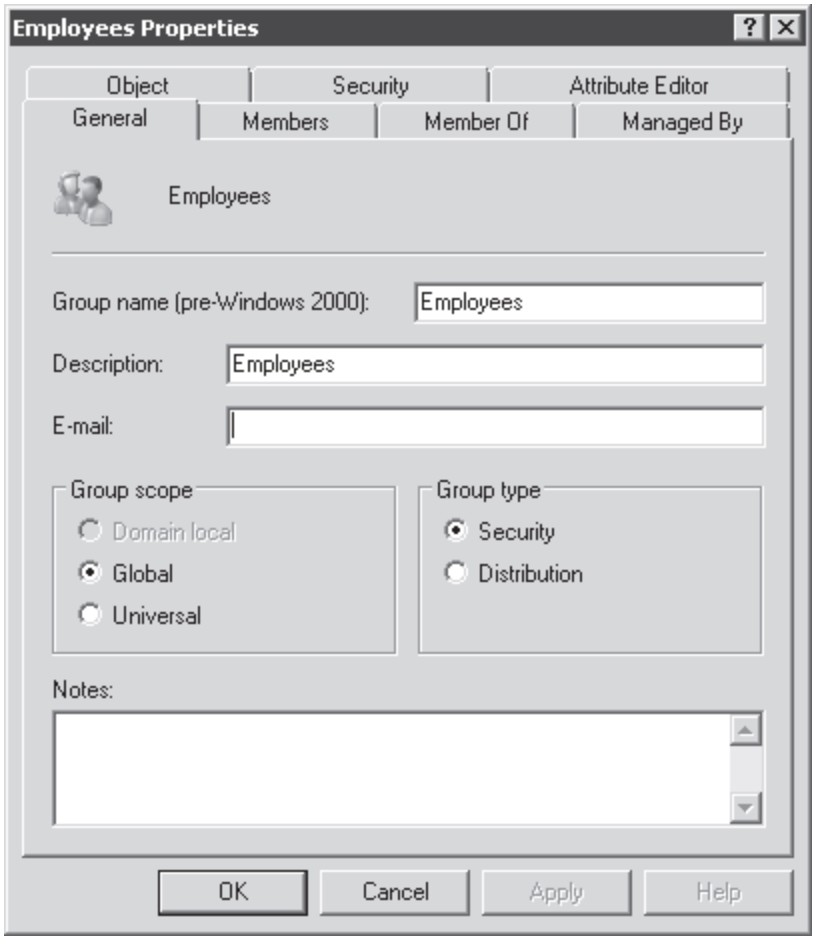
هم در امتحان 70-640 و هم در مدیریت روزمره شبکه مهم است که به طور کامل با خصوصیات عضویت همه حوزه‌های گروهها آشنا شویم.
جدول ۱- ۴ اشیایی را که می‌تواند عضو هر حوزه از گروههای مختلف شود خلاصه می‌کند.
جدول ۱- ۴ حوزه گروه و اعضاء

حوزه گروه	اعضاء از همان دامنه	اعضاء از دامنه‌های دیگر همان forest	اعضاء از یک دامنه خارجی مورد اعتماد
Local	کاربران کامپیوترها گروههای global گروههای universal گروههای domain local کاربران محلی تعریف شده روی همان کامپیوتر به عنوان گروه محلی	کاربران کامپیوترها گروههای global گروههای universal	کاربران کامپیوترها گروههای global
Domain Local	کاربران کامپیوترها	کاربران کامپیوترها	کاربران کامپیوترها

	گروههای global گروههای universal گروههای domain local	گروههای global گروههای universal	گروههای global
Universal	کاربران کامپیوترها گروههای global گروههای universal	کاربران کامپیوترها گروههای global گروههای universal	-
Global	کاربران کامپیوترها گروههای global	-	-

تبدیل نوع و حوزه گروه

پس از ایجاد گروه ممکن است متوجه شوید که باید گروه عوض شود. برای این‌کار کادر محاوره‌ای Properties گروه موجود را باز کرده و در زبانه General که در شکل ۳- ۴ مشاهده می‌کنید نوع و حوزه فعلی را می‌بینید. حداقل یک نوع و حوزه برای انتخاب آماده است.



شکل ۳- ۴ زبانه General مربوط به کادر محاوره‌ای Properties گروه

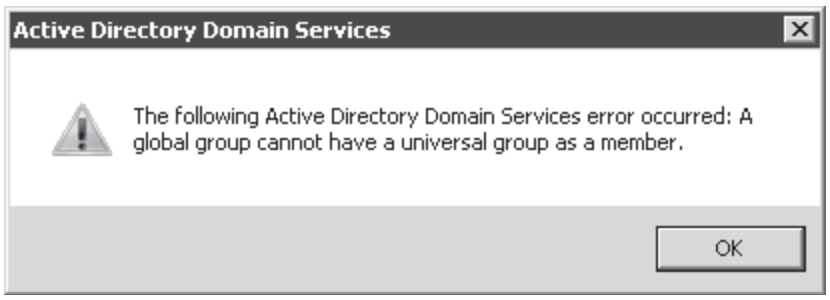
در هر زمانی با تغییر انتخاب نوع گروه در پنجره مربوطه می‌توان آن را تغییر داد. باید مراقب بود چون وقتی گروهی را از نوع امنیتی به توزیع تغییر می‌دهیم منابعی که گروه به آن مجوز دسترسی دارد به شکل سابق در دسترس نخواهد بود. وقتی گروه به توزیع تبدیل می‌شود کاربرانی که به دامنه وارد می‌شوند SID گروه را در توکن دسترسی امنیتی خود نخواهند داشت.

حوزه گروه را به یکی از اشکال زیر می‌توانیم تغییر دهیم:

- Global به Universal
- Universal به Domain Local
- Universal به Global
- Universal به Domain Local

تنها تبدیلی که امکانپذیر نیست Domain Local به Global و بالعکس است. البته امکان تبدیل غیرمستقیم وجود دارد. بدین ترتیب که ابتدا گروه به Universal تبدیل شده و سپس به حوزه موردنظر تبدیل شود. پس نهایتا امکان تبدیل همه حوزه‌ها به یکدیگر وجود دارد.

به خاطر داشته باشید که حوزه گروه انواع اشیایی را که می‌تواند عضو آن شود تعیین می‌کند. اگر گروه قبلا دارای عضو باشد یا عضو گروه دیگری باشد از تبدیل حوزه آن گروه ممانعت به عمل می‌آید. مثلا اگر یک گروه global عضو گروه global دیگری باشد گروه اول را نمی‌توانیم به universal تبدیل کنیم. چون گروه universal نمی‌تواند عضو گروه global باشد و در نتیجه خطایی مشابه شکل ۴- ۴ ظاهر می‌شود. در این حالت تداخل بین گروهها را برطرف کرده و بعد حوزه گروه را تغییر می‌دهیم.



شکل ۴- ۴ خطای تولید شده زمانی که عضویت یک گروه اجازه تغییر حوزه گروه را نمی‌دهد.

دستور Dsmod که در فصل ۳ معرفی شده جهت تغییر نوع و حوزه گروه به شکل زیر قابل استفاده است:

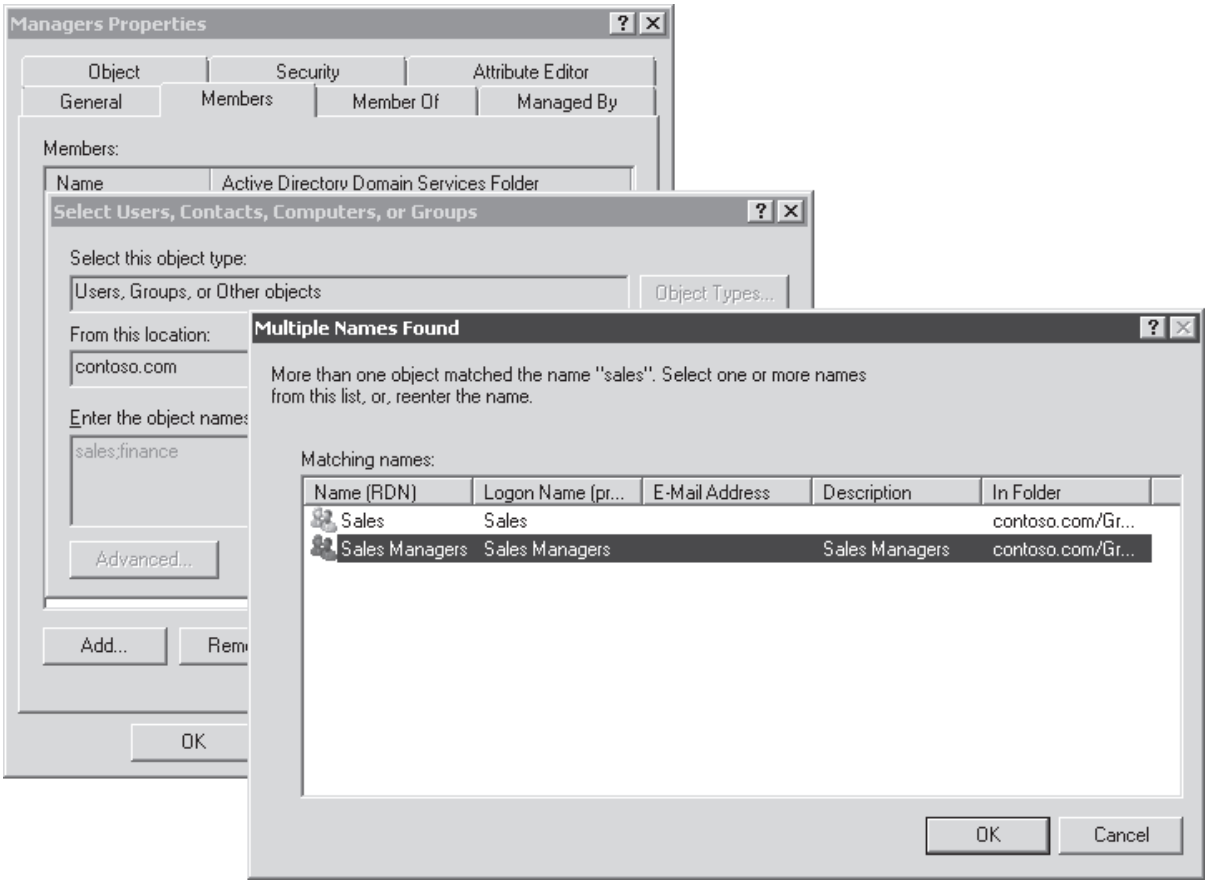
Dsmod group GroupDN -secgrp {yes | no} -scope {l|g|u}

GroupDN ، DN گروه است که تغییر می‌کند. دو پارامتر زیر روی نوع و حوزه گروه تاثیر می‌گذارد.

- -secgrp {yes|no} نوع گروه را تعیین می‌کند. برای امنیتی yes و برای توزیع no انتخاب می‌شود.
- -Scope {l|g|u} حوزه گروه را تعیین می‌کند. L برای domain local ، g برای global و u برای universal

مدیریت عضویت گروهها

وقتی نیاز داریم عضوی را به گروه اضافه و یا از آن حذف کنیم راههای متعددی پیش روی ما قرار دارد. اول کادر محاوره‌ای Properties گروه را باز کرده و زبانه Members را انتخاب می‌کنیم. برای حذف یک عضو آن را انتخاب کرده و دکمه Remove را کلیک می‌کنیم. برای افزودن عضو دکمه Add را کلیک می‌کنیم. کادر محاوره‌ای Select Users, Computers, Or Groups همانند شکل ۵- ۴ ظاهر می‌شود.



شکل ۵- ۴ افزودن عضو به گروه

نکاتی که در این پروسه به آن باید اشاره کرد به ترتیب زیر است:

- در کادر محاوره‌ای Select در کادر Enter Th

- e Object Names امکان تایپ چند حساب مجزا با درج علامت ";" بین آن‌ها وجود دارد. مثلا در شکل ۵- ۴ هم sales و هم finance وارد شده‌اند و با علامت ";" از هم جدا گشته‌اند.

- می‌توانیم بخشی از نام حساب را تایپ کنیم نه همه آن را. ویندوز در Active Directory به دنبال حساب‌هایی که با نام وارد شده شروع می‌شوند می‌گردد. اگر تنها یک مورد یافت شود ویندوز آن را انتخاب می‌کند. اگر بیش از یک مورد پیدا شود کادر محاوره‌ای Multiple Names Found ظاهر می‌شود و می‌توانیم شیء مورد نظر را از بین آن‌ها انتخاب کنیم. با استفاده از این روش هم زمان کمتری صرف می‌کنیم و هم وقتی نام دقیق کاربر را نمی‌دانیم از این روش سود می‌بریم.

- به طور پیش فرض ویندوز نام وارد شده را در بین کاربران و گروهها جستجو می‌کند. اگر بخواهیم کامپیوترها را به گروه اضافه کنیم باید دکمه Options را زده و Computers را انتخاب کنیم.

- به طور پیش فرض ویندوز نام وارد شده را در بین گروههای دامنه جستجو می‌کند. اگر بخواهیم حساب‌های محلی را به آن اضافه کنیم دکمه Location را در کادر محاوره‌ای Select کلیک می‌کنیم.

- اگر عضو مورد نظر پیدا نشد دکمه Advanced را در کادر محاوره‌ای Select کلیک می‌کنیم. پنجره قدرتمندتری ظاهر می‌شود که انتخاب بیشتری را برای جستجوی Active Directory میسر می‌کند.

همچنین می‌توان یک شیء را در ابزار Active Directory Users And Computers به یک گروه اضافه کرد. برای این کار در پنجره Properties شیء زبانه MemberOf را کلیک می‌کنیم. دکمه Add را زده و گروه مورد نظر را انتخاب می‌کنیم. روش دیگر این است که یک یا چند شیء را انتخاب کرده و روی آن کلیک راست می‌کنیم و سپس از دستور Add To Group استفاده می‌کنیم.

خصیصه Member و MemberOf

وقتی عضوی به گروه اضافه می‌شود در واقع خصیصه member گروه تغییر می‌کند. این خصیصه یک خصیصه چند مقداره است. هر عضو مقداری است که توسط DN عضو نمایش داده می‌شود. وقتی عضو منتقل می‌شود یا تغییر نام می‌دهد Active Directory به طور خودکار خصیصه‌های member گروهها را که شامل عضو مورد نظر است به روزرسانی می‌کند. وقتی عضوی به گروه اضافه می‌شود خصیصه memberOf عضو نیز به طور غیرمستقیم به روز می‌شود. خصیصه memberOf نوع خاصی از خصیصه به نام back link می‌باشد. این خصیصه وقتی یک خصیصه forward link مانند member به شیء ارجاع داده می‌شود توسط Active Directory به روز می‌شود. وقتی عضوی به یک گروه اضافه می‌شود خصیصه member تغییر می‌کند. بنابراین وقتی از زبانه memberOf یک شیء برای افزودن به گروه استفاده می‌شود در واقع خصیصه member گروه است که تغییر می‌کند. Active Directory خصیصه memberOf را به طور خودکار به روز می‌کند.

تسریع اعمال تغییرات عضویت

وقتی کاربری به یک گروه اضافه می‌شود عضویت فورا اعمال می‌شود. عضویت گروه هنگام ورود کاربر به سیستم ارزیابی می‌گردد بنابراین کاربر مجبور است از سیستم خارج شده و دوباره وارد شود تا تغییر عضویت در توکن کاربر درج گردد.

به علاوه هنگام تکثیر عضویت گروهها ممکن است تاخیر دیگری به وجود آید. بحث تکثیر در فصل ۱۱ "سایت‌ها و تکثیر" بحث خواهد شد. این مساله زمانی پیش می‌آید که شبکه بیش از یک سایت داشته باشد. برای اعمال سریع‌تر تغییرات برای کاربر می‌توانیم تغییر را روی DC در سایت کاربر انجام دهیم. روی دامنه در ابزار Active Directory Users And Computers کلیک راست کرده و Change Domain Controller را انتخاب می‌کنیم.

توسعه استراتژی مدیریت گروه

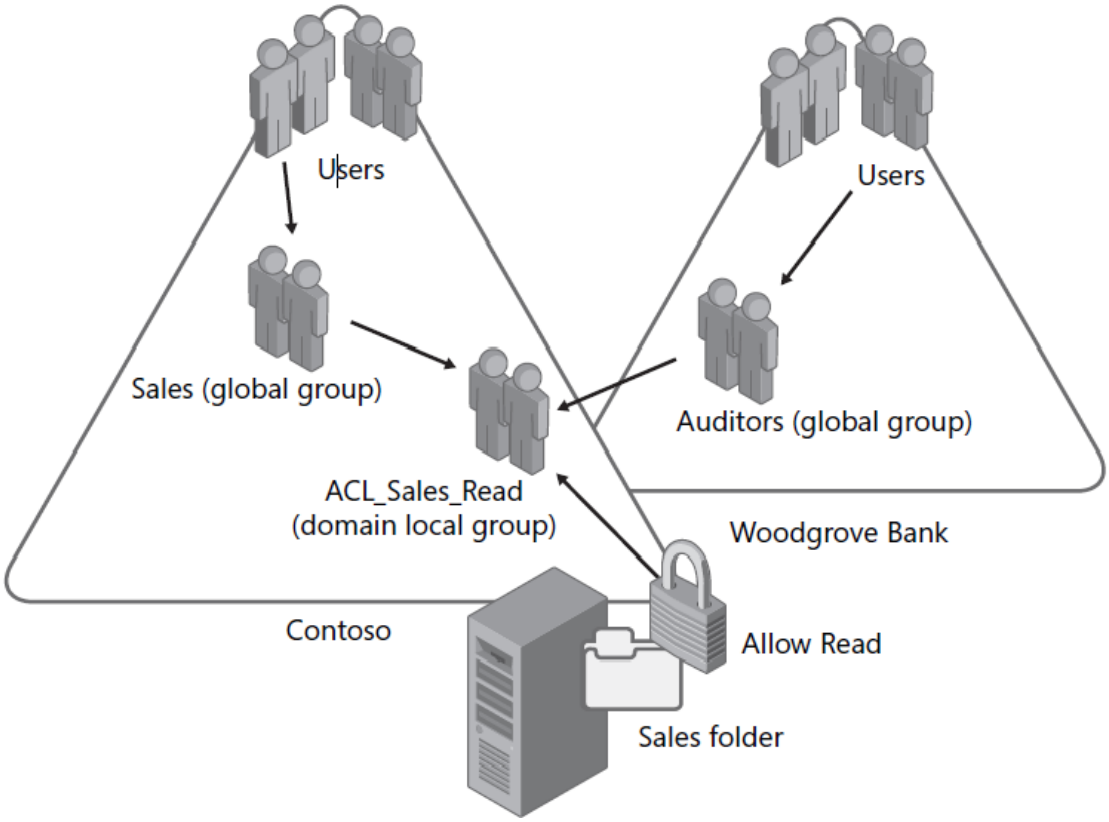
افزودن گروهها به یکدیگر که تودرتو (nesting) نام دارد ساختار سلسله مراتبی گروهها را ایجاد می‌کند. این ساختار نیز نقش‌ها و قوانین کاری را حمایت می‌کند. حالا که اهداف کاری و خصوصیات فنی گروهها را یاد گرفتیم زمان بررسی دومین استراتژی مدیریت گروه‌ها فرا رسیده است.

قبلا درهمین درس یاد گرفتیم که چه نوع شیء می‌تواند عضو هر حوزه گروه شود. حالا باید مشخص کنیم کدام نوع از اشیاء باید عضو هر حوزه گروه شود. برای درک مسئله بهترین روش برای گروههای تودرتو یعنی AGDLA ارائه می‌گردد.

- Accounts (هویت‌های کاربر و کامپیوتر) عضوهای
- گروههای global هستند که نقش‌های کاری را نشان می‌دهند. این گروههای نقش عضوهای
- گروههای domain local هستند که نمایانگر قوانین کاری هستند که به طور مثال مجوز فقط خواندنی به یک گروه از پوشه‌ها دارند. این گروههای قوانین (گروههای domain local) به
- ACL ها اضافه می‌شوند که سطح دسترسی مورد نیاز توسط یک قاعده را فراهم می‌کند.

در یک forest با چند دامنه گروههای universal هم وجود دارند که بین گروههای global و domain local حضور دارند. گروههای global دامنه‌های مختلف اعضاء یک گروه universal می‌باشند. این گروه universal عضو گروههای domain local در دامنه‌های مختلف است. گروههای تودرتو را می‌توان معادل AGUDLA در نظر گرفت. این تمرین مناسب برای پیاده سازی گروههای تودرتو حتی در سناریوهای دارای چند دامنه می‌باشد. شکل ۶- ۴ را در نظر بگیرید که

پیاده سازی یک گروه را که نه تنها نمای فنی بهترین روش مدیریت گروه را (AGDLA) بلکه نمای مدیریت مبتنی بر نقش و قواعد را منعکس می‌کند نمایش می‌دهد.



شکل ۶- ۴ پیاده سازی مدیریت یک گروه

سناریوی زیر را در نظر بگیرید. کارکنان فروش در شرکت Contoso,Ltd. اخیرا سال مالی را به پایان رسانده‌اند. فایل‌های فروش از سال قبل در یک پوشه به نام Sales قرار دارد. نیروهای فروش نیاز به دسترسی خواندن پوشه Sales دارند. به علاوه یک گروه از ممیزین از بانک Woodgrove به عنوان سرمایه گذار نیاز به دسترسی خواندن پوشه Sales دارند تا بتوانند عملیات ممیزی را انجام دهند. مراحل پیاده‌سازی امنیت مورد نیاز این سناریو به ترتیب زیر است:

۱. کاربران با مسئولیت‌های کاری یا دیگر خصوصیات کاری مشترک را به گروههای نقش از نوع گروه امنیتی global تعریف کنید. این کار در هر دامنه به طور مجزا اتفاق می‌افتد. کارکنان بخش فروش در شرکت به گروه نقش Sales اضافه می‌شوند. ممیزین بانک Woodgrove به گروه نقش Auditors اضافه می‌شوند.

۲. گروهی برای ارائه قواعد کاری بسازید که مشخص کند چه کسی به پوشه Sales دسترسی خواندنی داشته باشد. این روش در دامنه‌هایی پیاده سازی می‌شود که قواعد به منابع دامنه اعمال می‌شود. در این مثال دامنه Contoso است که پوشه Sales در آن قرار دارد. گروه قواعد به عنوان گروه domain local ساخته می‌شود.

۳. گروههای مبتنی بر نقش را به گروههایی که قوانین سازمان به آنها اعمال می‌شود اضافه کنید. این گروهها می‌توانند از هر دامنه‌ای در forest یا از دامنه‌های مورد اعتماد دیگر مانند Woodgrove Bank بیایند. گروههای global از دامنه‌های خارجی مورد اعتماد یا از هر دامنه‌ای در همان forest می‌تواند عضو گروه domain local شود.

۴. مجوزی که سطح دسترسی مورد نیاز را پیاده سازی می‌کند نسبت دهید.

در این مثال مجوز خواندن به گروه domain local اعطاء کنید.

این استراتژی باعث ایجاد یک نقطه مدیریتی واحد و کاهش عملیات مدیریتی می‌شود. فقط یک نقطه مدیریتی وجود دارد که مشخص می‌کند چه کسی در گروه Sales یا Auditor عضو است. این نقش‌ها مجوزهای متعددی را بیش از یک پوشه Sales نسبت به منابع مختلف داراست. نقطه مرکزی مدیریت دیگری برای تعیین حساب‌های دارای دسترسی خواندن به پوشه Sales وجود دارد. پوشه Sales می‌تواند فقط یک پوشه روی یک سرور نباشد و مجموعه‌ای از پوشه‌های روی سرورهای متعدد باشد که هر کدام مجوز خواندن به گروه domain local منفرد اعطاء کند.

تمرینات ساخت و مدیریت گروهها

در این تمرینات قرار است گروه‌ها ساخته شوند، با عضویت گروهها کار شود و نوع و حوزه گروه تغییر کند. قبل از انجام تمرینات باید اشیاء زیر در دامنه contoso.com ساخته شده باشند:

- OU سطح اول به نام Groups
- OU سطح اول به نام People
- اشیاء کاربر در OU People برای Linda Mitchell، Scott Mitchell، Jeff Ford، Mike Fitzmaurice، Mike Danseglio و Tony Krijnen

تمرین ۱ ساخت گروهها

در این تمرین گروهها با انواع مختلف و حوزه‌های مختلف ساخته می‌شوند.

۱. به سرور SERVER01 با کاربر Administrator وارد شده و ابزار ACTIVE DIRECTORY USERS AND COMPUTERS را باز می‌کنیم. در ساختار درختی Groups OU را انتخاب می‌کنیم.

۲. روی Groups OU کلیک راست کرده و New و سپس Group را انتخاب می‌کنیم.

۳. در کادر Group Name عبارت Sales را تایپ می‌کنیم.

۴. نوع گروه را Security و حوزه آن را Global تعیین می‌کنیم.

۵. روی گروه Sales کلیک راست کرده و Properties را انتخاب می‌کنیم.

۶. روی زبانه Members کلیک می‌کنیم.

۷. روی دکمه Add کلیک می‌کنیم.

۸. عبارت Jeff;Tony را تایپ کرده و OK می‌کنیم.

۹. OK را کلیک می‌کنیم تا کادر محاوره‌ای Properties بسته شود.

۱۰. مراحل ۲ تا ۴ را برای دو گروه با نام‌های Marketing و Consultants تکرار می‌کنیم.

۱۱. مراحل ۲ تا ۴ را برای ساخت گروه امنیتی domain local به نام ACL_Sales Folder_Read تکرار می‌کنیم.

۱۲. پنجره Properties گروه ACL_Sales Folder_Read را باز می‌کنیم.

۱۳. زبانه Member را کلیک می‌کنیم.

۱۴. دکمه Add را کلیک می‌کنیم.

۱۵. تایپ می‌کنیم Sales;Marketing;Consultants و OK می‌کنیم.

۱۶. دکمه Add را کلیک می‌کنیم.

۱۷. عبارت Linda را تایپ کرده و OK را کلیک می‌کنیم.

۱۸. OK را کلیک می‌کنیم تا کادر محاوره‌ای Properties بسته شود.

۱۹. کادر محاوره‌ای Properties گروه Marketing را باز می‌کنیم.

۲۰. روی زبانه Member و سپس Add کلیک می‌کنیم.

۲۱. عبارت ACL_Sales Folder_Read را تایپ کرده و OK را کلیک می‌کنیم.

امکان افزودن گروه domain local به گروه global وجود ندارد.

۲۲. همه کادرهای محاوره‌ای باز را Cancel می‌کنیم.

۲۳. پوشه‌ای با نام Sales در درایو C می‌سازیم.

۲۴. روی پوشه Sales کلیک راست می‌کنیم و Properties و سپس زبانه Security را کلیک می‌کنیم.

۲۵. Editو سپس Add را کلیک می‌کنیم.

۲۶. دکمه Advanced و سپس Find Now را کلیک می‌کنیم.

توجه داشته باشید که افزودن یک پیشوند به نام گروه مانند ACL_ برای گروههای دسترسی به منابع باعث می‌شود به راحتی آن‌ها را پیدا کنیم.

۲۷. همه کادرهای محاوره‌ای باز را Cancel می‌کنیم.

۲۸. روی Groups کلیک راست کرده و New و سپس Group را انتخاب می‌کنیم.

۲۹. در کادر Group Name عبارت Employees را تایپ می‌کنیم.

۳۰. حوزه گروه را domain local و نوع گروه را distribution انتخاب می‌کنیم.

تمرین ۲ تبدیل نوع و حوزه گروه

در این تمرین یاد می‌گیریم نوع و حوزه گروه را تغییر دهیم.

۱. روی گروه Employees کلیک راست کرده و Properties را انتخاب می‌کنیم.

۲. نوع گروه را به Distribution تغییر می‌دهیم.

۳. Apply را کلیک می‌کنیم.

آیا می‌توانیم حوزه گروه را از domain local به global تغییر دهیم؟ چطور؟

۴. حوزه گروه را به universal تغییر می‌دهیم. دکمه Apply را کلیک می‌کنیم.

۵. حوزه گروه را به global تغییر می‌دهیم. دکمه Apply را کلیک می‌کنیم.

۶. دکمه OK را کلیک کرده تا کادر محاوره‌ای Properties بسته شود.

خلاصه درس

- دو نوع گروه موجود است: امنیتی و توزیع. گروههای امنیتی قابلیت اعطاء مجوز دارند و گروههای توزیع به عنوان لیست‌های توزیع استفاده می‌شوند.
- به علاوه گروههای محلی که فقط در بانک اطلاعاتی SAM سیستم ذخیره می‌شود سه حوزه گروههای دامنه به نام‌های domain local، global و universal وجود دارند.
- حوزه گروه روی تکثیر آن، نوع اشیاء که می‌توانند عضو گروه باشند و امکان افزودن آن به گروه دیگر یا استفاده برای مدیریت وظایفی مانند اعطاء مجوز تاثیر می‌گذارد
- امکان تبدیل نوع گروه و حوزه آن پس از ساخت وجود دارد.

سئوالات پایان درس

برای آزمایش دانش خود در درس ۱ "ساخت و مدیریت گروهها" از سئوالات زیر استفاده کنید. سئوالات همچنین در CD همراه کتاب موجود می‌باشد.

۱. یک پروژه جدید نیاز دارد که که کاربران در دامنه شما و دامنه یک سازمان دیگر که شریک شماست به یک پوشه مشترک روی یک فایل سرور دسترسی داشته باشند. چه نوع گروهی باید ایجاد گردد؟

A. گروه Universal Security

B. گروه Domain Local Security

C. گروه Global Security

D. گروه Domain Local Security

۲. گروه توزیعی با حوزه global و نام Company Update در دامنه شما وجود دارد که برای ارسال اخبار شرکت به اعضاء از طریق پست الکترونیک به کار می‌رود. شما تصمیم دارید به همه اعضاء اجازه دهید از طریق ساخت پوشه مشترک روی سرور در اخبار شرکت سهیم شوند. چه کاری باید انجام شود تا اعضاء گروه اجازه این کار را پیدا کنند؟

A. حوزه گروه را به domain local تغییر می‌دهیم

B. حوزه گروه را به universal تغییر می‌دهیم.

C. گروه را به گروه Domain Users اضافه می‌کنیم.

D. از دستور Dsmod با سوئیچ secgrp yes– استفاده می‌کنیم.

۳. شما یک گروه امنیتی global در دامنه contoso.com با نام Corporate Managers ساخته‌اید. کدام اعضاء می‌توانند به گروه اضافه شوند؟ (بیش از یک جواب دارد)

A. Sales Managers یک گروه global در دامنه fabrikam.com که یک دامنه مورد اعتماد از شرکاء می‌باشد.

B. Sales Managers یک گروه global در دامنه tailspintoys.com که یک دامنه در forest ، contoso.com می‌باشد.

C. Linda Mitchell کاربری در دامنه tailspintoys.com که یک دامنه در forest ، contoso.com می‌باشد

D. Jeff Ford کاربری در دامنه fabrikam.com که یک دامنه مورد اعتماد از شرکاء می‌باشد.

E. Mike Danseglio کاربری در دامنه contoso.com

F. Sales Executives گروهی global در دامنه contoso.com

G. Sales Directors یک گروه domain local در دامنه contoso.com

H. European Sales Managers یک گروه universal در forest، contoso.com

درس ۲: خودکارسازی ساخت و مدیریت گروهها

در درس ۱ مراحل ساخت گروه، انتخاب نوع و حوزه گروه و پیکربندی عضویت گروه را با ابزار Active Directory Users And Computers یاد گرفتیم. وقتی نیاز به ساخت بیش از یک گروه در یک زمان داریم یا وقتی بخواهیم ساخت گروه را خودکار کنیم باید به ابزارهای دیگر رجوع کنیم. در فصل ۳ با ابزارهای خودکارسازی و خط فرمان مانند CSVDE، LDIFDE، Dsadd، windows PowerShell و VBScript آشنا شدیم. این ابزارها در خودکارسازی ساخت و مدیریت اشیاء گروه استفاده می‌شود. در این درس یاد می‌گیریم که با استفاده از خط فرمان و ابزارهای خودکارسازی دوره حیات گروه‌ها را مدیریت کنیم.

بعد از این درس یاد می‌گیریم:

- با استفاده از Dsadd، LDIFDE و CSVDE گروه بسازیم
- عضویت گروهها را با Dsmod، LDIFDE، windows PowerShell و VBScript تغییر دهیم
- بررسی عضویت گروهها با Dsget
- انتقال و حذف گروهها با دستورات Dsmove و Dsrm

زمان تقریبی : ۴۵ دقیقه

ساخت گروه‌ها با دستور Dsadd

دستور Dsadd که در فصل ۳ معرفی شد امکان افزودن اشیاء را به Active Directory میسر می‌کند. برای افزودن گروه دستور dsadd group GroupDN را تایپ کنید که GroupDN تعیین کننده DN گروه است مانند " CN=Finance Managers,OU=Groups,DC=contoso,DC=com". اگر در DN فاصله خالی وجود دارد حتماً از گیومه استفاده کنید. برای مثال برای ساخت یک گروه امنیتی global با نام Marketing در Groups OU از دامنه contoso.com دستور زیر را به کار برید:

Dsadd group "CN=Marketing,OU=Groups,DC=contoso,DC=com"
-samid Marketing –secgrp yes -scope g

همچنین پارامتر GroupDN از راههای زیر نیز قابل تعیین است:

- از طریق انتقال لیستی از DN ها از دستور دیگری مانند Dsquery
- با تایپ هر DN جداگانه در خط فرمان هر کدام با فاصله
- با خالی گذاشتن پارامتر DN در دستور و درج DN در هر خط و زدن کلید Enter بعد از هر DN. در نهایت فشردن کلیدهای Ctrl+Z و زدن کلید Enter پس از آخرین DN.

به دلیل اینکه می‌توان بیش از یک DN را در خط فرمان با درج فضای خالی بین آن‌ها وارد کرد امکان ساخت چند گروه با دستور Dsadd وجود دارد. این دستور می‌تواند همچنین با استفاده از پارامترهای زیر خصیصه‌های گروه را پیکربندی کند:

- -secgrp {yes | no } نوع گروه را تعیین می‌کند امنیتی (yes) یا توزیع (no)
- -scope { l | g | u } حوزه گروه را تعیین می‌کند l برای domain local، g برای global و u برای universal
- -samid Name مشخص کننده sAMAccountName گروه است. وقتی تعیین نمی‌شود نام گروه از DN گرفته می‌شود. توصیه می‌شود نام گروه با sAMAccountName یکی باشد تا هنگام استفاده از دستور Dsadd نیازی به وارد کردن آن نباشد.
- -desc Description برای گروه توضیحات درج می‌کند.
- -members MemberDN اعضاء را به گروه اضافه می‌کند. اعضاء با DN خود در لیست که بین آن‌ها فاصله وجود دارد مشخص می‌شوند.
- -memberof GroupDN گروه جدید را عضو یک یا چند گروه موجود می‌کند. گروهها با DN خود در لیست که بین آن‌ها فاصله وجود دارد مشخص می‌شوند

انتقال گروهها با CSVDE

در فصل ۳ با این دستور که داده را از فایل‌های CSV. منتقل می‌کرد آشنا شدیم. این دستور به همان ترتیب می‌تواند داده را به درون فایل CSV. منتقل کند. مثال زیر یک فایل CSV. را که گروه Marketing را می‌سازد و دو عضو اولیه به نام‌های Linda Mitchell و Scott Mitchell را اضافه می‌کند نشان می‌دهد.

objectClass,sAMAccountName,DN,Member
group,Marketing, "CN=Marketing,OU=Groups,DC=contoso,DC=com",
"CN=Linda Mitchell,OU=People,DC=contoso,DC=com;CN=Scott Mitchell,
OU=People,DC=contoso,DC=com"

اشیاء لیست شده در خصیصه member باید قبلا در سرویس دایرکتوری موجود باشد. DN آن‌ها در ستون member با نقطه ویرگول از هم جدا می‌شوند.

این فایل را می‌توان با دستور زیر به Active Directory منتقل کرد:

```
Csvde  -I  -f  “Filename” [-k]
```

پارامتر I– مد دستور را به حالت import تعیین می‌کند. حالت پیش فرض دستور export است. پارامتر f– قبل از نام فایل می‌آید و پارامتر k– باعث ادامه پردازش دستور می‌گردد حتی اگر خطایی بروز کند.

نکته امتحانی دستور CSVDE برای ساخت اشیاء به کار می‌رود نه برای تغییر آن‌ها بنابراین امکان انتقال اعضاء به گروه موجود با این دستور وجود ندارد.

مدیریت گروهها با LDIFDE

همانطور که در فصل ۳ یاد گرفتیم این دستور ابزاری برای انتقال فایل‌ها در فرمت LDIF است. فایل‌های LDIF فایل‌های متنی هستند که در آن‌ها هر عملیاتی در یک بلوک مجزا و با یک خط خالی قبل از آن مشخص می‌شود. هر عملیاتی با خصیصه DN شیء هدف عملیات آغاز می‌شود. خط بعدی یعنی changeType نوع عملیات را مشخص می‌کند : افزودن، تغییر یا حذف.

فایل LDIF زیر دو گروه با نام‌های Finance و Research در Groups OU از دامنه contoso.com می‌سازد:

```
DN: CN=Finance,OU=Groups,DC=contoso,DC=com
ChangeType: add
CN: Finance
Description: Finance Users
objectClass: group
sAMAccountName: Finance

DN: CN=Research,OU=Groups,DC=contoso,DC=com
ChangeType: add
CN:  Research
Description: Research Users
objectClass: group
sAMAccountName: Research
```

به طور پیش فرض فایل با پسوند ldf. ذخیره می‌شود مثلا Groups.ldf. برای انتقال گروه به دایرکتوری از دستور ldifde.exe به صورت زیر استفاده می‌کنیم:

```
Ldifde  -I  -f  groups.ldf
```

تغییر عضویت گروهها با دستور LDIFDE

از این دستور همچنین برای تغییر اشیاء در Active Directory با استفاده از عملیات LDIF با modify changeType نیز استفاده می‌شود. جهت افزودن دو عضو به گروه Finance فایل LDIF مربوطه به صورت زیر است:

```
Dn:  CN=Finance,OU=Groups,DC=contoso,DC=com
Changetype: modify
Add: member
Member: CN=April Stewart,OU=People,dc=contoso,dc=com
Member: CN=Mike Fitzmaurice,OU=People,dc=contoso,dc=com
-
```

ابتدا changeType به حالت modify تنظیم شده و سپس عملیات تغییر که افزودن شیء به خصیصه member است مشخص شده است. هر عضو جدید در خط مجزا که با نام خصیصه member شروع می‌شود قرار می‌گیرد. عملیات تغییر با یک خط که فقط علامت "-" دارد خاتمه می‌یابد. تغییر خط سوم به خطوط زیر باعث حذف دو عضو از گروه می‌شود:

```
Delete:  member
```

مشاهده عضویت گروهها با دستور Dsget

دستورات Dsmod و Dsget که در فصل ۳ بحث شدند برای مدیریت عضویت گروهها به کار می‌آیند. در ابزار Active Directory Users And Computers هیچ گزینه‌ای برای نمایش همه اعضای گروه شامل گروههای تودرتو وجود ندارد. فقط عضویت‌های مستقیم در زبانه Members یک گروه قابل مشاهده است. همچنین راهی برای لیست کردن همه گروههایی که یک کاربر عضو آن‌هاست از جمله گروههای تودرتو وجود ندارد. در زبانه MemberOf کاربر یا کامپیوتر فقط عضویت‌های مستقیم قابل مشاهده است.

دستور Dsget ما را قادر می‌سازد لیست کاملی از عضویت گروه شامل اعضاء تودرتو را ببینیم. دستور آن به شکل زیر است:

```
Dsget group “GroupDn” -members [-expand]
```

گزینه expand اعضاء گروههای تودرتو را در یک سطح نمایش می‌دهد.

به طور مشابه دستور Dsget برای تهیه لیست کاملی از گروههایی که کاربر یا کامپیوتر به آن تعلق دارد به کار می‌رود و گزینه expand اینجا هم همان کار را انجام می‌دهد به صورت زیر:

```
Dsget user "userDN" -memberof [-expand]
Dsget computer "computerDN" -memberof [-expand]
```

گزینه memberof با نمایش گروههایی که شیء مستقیما به آن‌ها تعلق دارد در واقع مقدار خصیصه memberOf کامپیوتر یا کاربر را برمی‌گرداند. با افزودن گزینه expand این گروهها به طور معکوس جستجو شده و لیست کاملی از همه گروههایی که کاربر به آن‌ها تعلق دارد ارائه می‌شود.

تغییر عضویت گروهها با دستور Dsmod

دستور Dsmod که در درس ۱ بررسی شده برای تغییر حوزه و نوع گروه استفاده می‌شود. شکل ابتدایی دستور به صورت زیر است:

```
Dsmod group "GroupDN" [options]
```

امکان استفاده از گزینه‌هایی مانند samid و desc برای تغییر خصیصه‌های sAMAccountName و description گروه وجود دارد. خصیصه مفیدتری که می‌توان تغییر داد عضویت گروه می‌باشد:

- -addmbr "Member DN" اعضاء را به گروه اضافه می‌کند
- -rmmbr "Member DN" اعضاء را از گروه حذف می‌کند.

امکان اضافه کردن چند Member DN با درج فضای خالی بین آن‌ها وجود دارد. مثلا برای افزودن Mike Danseglio به گروه Research دستور Dsmod به شکل زیر استفاده می‌شود:

```
Dsmod group "CN=Research,OU=Groups,DC=contoso,DC=com" -addmbr "CN=Mike
Danseglio,OU=People,DC=contoso,DC=com"
```

همچنین می‌توان دستور Dsget را در ترکیب با Dsmod برای کپی کردن اعضاء گروه استفاده کرد. در مثال زیر دستور Dsget برای دریافت اطلاعات همه اعضاء گروه Sales و انتقال آن به دستور Dsmod برای عضویت در گروه Marketing به کار می‌رود:

```
Dsget group "CN=Sales,OU=Groups,DC=contoso,DC=com" –mambers | dsmod group
"CN=Marketing,OU=Groups,DC=contoso,DC=com" -addmbr
```

انتقال و تغییر نام گروهها با Dsmove

این دستور که در فصل ۳ بررسی شد ما را قادر می‌سازد شیء را در یک domain جابجا کنیم یا نامش را تغییر دهیم. از این دستور برای انتقال شیء بین domain ها نمی‌توان استفاده کرد. شکل اولیه فرمان به ترتیب زیر است:

```
Dsmove objectDN [-newname NewName] [-newparent TargetOUDN]
```

شیء مورد نظر با DN در پارامتر ObjectDN مشخص می‌شود برای تغییر نام CN جدید را به‌جای newname وارد کنید. برای انتقال شیء به مکان جدید DN مربوط به container مقصد را به جای پارامتر newparent وارد کنید. مثلا برای تغییر نام گروه Marketing به Public Relations تایپ می‌کنیم:

```
Dsmove "CN=Marketing,OU=Groups,DC=contoso,DC=com" –newparent
"OU=Marketing,DC=contoso,DC=com"
```

نکته خط فرمان تنها راه نیست

امکان انتقال یا تغییر یک گروه در ابزار Active Directory Users And Computers با کلیک راست روی گروه و انتخاب گزینه Move یا Rename نیز موجود است.

حذف گروه با دستور Dsrm

این دستور برای حذف گروه یا دیگر اشیاء به کار می‌رود. شکل ابتدایی دستور به صورت زیر است:

Dsrm ObjectDN … [-subtree [-exclude]] [-noprompt] [-c]

شیء با DN خود در پارامتر ObjectDN مشخص می‌گردد. در صورت استفاده از گزینه noprompt پنجره‌ای برای تایید حذف شیء باز می‌شود. سوئیچ c– دستور را در حالت اجرای بدون وقفه قرار می‌دهد و خطاهای تولید شده گزارش می‌شود ولی باعث قطع عملیات نمی‌شود. بدون این سوئیچ با اولین خطا پروسه متوقف می‌شود.

برای حذف گروه Public Relations به ترتیب زیر عمل می‌کنیم:

Dsrm "CN=Public Relations,OU=Marketing,DC=contoso,DC=com"

همچنین می‌توان یک گروه را در ابزار Active Directory Users And Computers با کلیک راست روی آن و انتخاب گزینه Delete حذف کرد.

نکته عواقب حذف گروه

با حذف گروه یک نقطه مدیریتی در سازمان حذف می‌شود. بنابراین قبل از حذف بررسی می‌کنیم که هیچ مجوز یا منبعی در شبکه متکی به گروه نباشد. حذف گروه اقدامی جدی با عواقب مهم می‌باشد. پیشنهاد می‌شود قبل از حذف گروه ابتدا اعضاء را در جایی ثبت و سپس برای مدتی از گروه حذف کنیم تا ببینیم دسترسی کاربران با مشکل مواجه می‌شود یا نه. در صورت بروز مشکل اعضاء را دوباره اضافه می‌کنیم در غیر این‌صورت گروه را حذف می‌کنیم.

مدیریت عضویت گروهها با PowerShell ویندوز و VBScript

بعید به نظر می‌رسد که برای آزمون 70-640 به درک پیچیدگی‌های مدیریت گروه نیاز داشته باشید. بهرحال بحث مفصل راجع به اسکریپت‌نویسی گروهها از حوزه کتاب حاضر خارج است. برای اطلاعات بیشتر درباره خودکارسازی مدیریت گروهها با VBScript به Windows Administratio Resource Kit: Productivity Solutions for IT Professionals مراجعه کنید.

البته داشتن اطلاعات اولیه درباره آن ضرری ندارد. در PowerShell ویندوز و VBScript برای دستکاری عضویت گروهها راههای متعددی وجود دارد (خصیصه member گروه) ولی رایج‌ترین و موثرترین آن‌ها به شکل زیر است:

۱. aDSPath عضو را مشخص می‌کنیم. شکل آن به صورت LDAP://<DN of member> می‌باشد.

۲. به گروه متصل می‌شویم.

۳. از متد Add یا Remove شیء گروه با تعیین aDSPath عضو استفاده می‌کنیم.

اسکریپت PowerShell ویندوز که کاربر Mike Danseglio را به گروه Research اضافه می‌کند خواهد شد:

```
$MemberADSPath = "LDAP://CN=Mike Danseglio,OU=People,DC=contoso,DC=com"
$objGroup = [ADSI] "LDAP://CN=Research,OU=Groups,DC=contoso,DC=com"
$objGroup.Add ($MemberADSPath)
```

در VBScript دستور به شکل زیر خواهد شد:

```
MemberADSPath = "LDAP://CN=Mike Danseglio,OU=People,DC=contoso,DC=com"
Set objGroup =GetObject("LDAP://CN=Research,OU=Groups,DC=contoso,DC=com"
objGroup.Add  MemberADSPath
```

برای حذف اعضاء از متد Remove به جای Add استفاده می‌شود. باقی کدها مشابه حالت قبل است.

تمرینات خودکارسازی ساخت و مدیریت گروهها

در این تمرین از دستورات CSVDE و LDIFDE برای اجرای وظایف مدیریتی گروه استفاده می‌شود. برای اجرای تمرینات اشیاء زیر در دامنه contoso.com مورد نیاز است:

- OU سطح اول با نام Groups

- OU سطح اول با نام People
- اشیاء کاربر در People OU برای Linda Mitchell، Scott Mitchell، Jeff Ford، Mike Fitzmaurice، Mike Danseglio، April Stewart و Tony Krijnen

به علاوه همه گروهها با نام‌های Finance و Accounting را حذف کنید.

تمرین ۱ ساخت گروه با دستور Dsadd

با این دستور می‌توان گروه ساخت و در یک خط اعضاء را اضافه کرد.

۱. با کاربر Administrator وارد می‌شویم.

۲. پنجره خط فرمان را باز کرده و دستور زیر را در یک خط تایپ می‌کنیم:

```
Dsadd group "CN=Finance,OU=Groups,DC=contoso,DC=com" –samid Finance –secgrp yes –scope g
```

۳. ابزار Active Directory Users And Computers را باز کرده و از وجود گروه ساخته شده مطمئن می‌شویم

تمرین ۲ انتقال گروه با دستور CSVDE

۱. با کاربر Administrator وارد می‌شویم.

۲. پنجره Notepad را باز کرده و خطوط زیر را تایپ می‌کنیم. هر بالت نشان‌دهنده یک خط در Notpad است و نباید آن را به دستور اضافه کنیم:

1. objectClass,sAMAccountName,DN,member
2. group,Accounting,"CN=Accounting,OU=Groups,DC=contoso,DC=com", "CN=Linda Mitchell,OU=People,DC=contoso,DC=com; CN=Scott Mitchell,OU=People,DC=contoso,DC=com"

۳. فایل را در My Document با نام Importgroups.csv ذخیره می‌کنیم.

۴. خط فرمان را باز کرده و دستور زیر را تایپ می‌کنیم:

```
Csvde -i -f "%userprofile%\importgroups.csv"
```

تمرین ۳ تغییر عضویت گروه را با دستور LDIFDE

دستور CSVDE قادر به تغییر عضویت گروههای موجود نیست بنابراین در این تمرین از دستور LDIFDE برای تغییر عضویت گروه Accounting که در تمرین ۲ منتقل کردیم استفاده می‌کنیم.

۱. پنجره Notpad را باز کرده و خطوط زیر را تایپ می‌کنیم:

```
Dn: CN=Accounting,OU=Groups,DC=contoso,DC=com
Changetype: modify
Add: member
Member: CN=April Stewart,OU=People,dc=contoso,dc=com
Member: CN=Mike Fitzmaurice,OU=People,dc=contoso,dc=com
-

Dn: CN=Accounting,OU=Groups,DC=contoso,DC=com
```

```
Changetype: modify
delete: member
Member: CN=Linda Mitchell,OU=People,dc=contoso,dc=com
-
```

بین دو بلوک باید خط خالی و بعد از هر بلوک خط تیره الزامی است.

۲. فایل را با نام Membershipchange.ldf در My Document ذخیره می‌کنیم.

۳. خط فرمان را باز می‌کنیم.

۴. دستور زیر را وارد کرده و Enter را می‌زنیم:

```
Ldifde  -i –f  "%userprofile%\documents\membershipchange.ldf"
```

تمرین ۴ تغییر عضویت گروه با دستور Dsmod

در این تمرین با استفاده از دستور Dsmod یک کاربر و یک گروه به اعضای گروه Finance افزوده می‌شود

۱. پنجره خط فرمان را باز می‌کنیم.

۲. دستور زیر را تایپ می‌کنیم

```
Dsmod group  "CN=Finance,OU=Groups,DC=contoso,DC=com"  -addmbr  "CN=Tony
Krijnen,OU=People,DC=contoso,DC=com"
"CN=Accounting,OU=Groups,DC=contoso,DC=com"
```

تمرین ۵ تایید عضویت گروه با دستور Dsget

ارزیابی عضویت نهایی در ابزار Active Directory Users And Computers بسیار مشکل بوده به همین دلیل از دستور Dsget برای این کار استفاده می‌کنیم. در این تمرین هم عضویت کامل یک گروه و هم عضویت یک کاربر در گروههای مختلف بررسی می‌شود.

۱. پنجره خط فرمان را باز می‌کنیم.

۲. اعضاء مستقیم گروه Accounting را با دستور زیر لیست می‌کنیم:

```
Dsget  group  "CN=Accounting,OU=Groups,DC=contoso,DC=com"  -members
```

۳. اعضاء مستقیم گروه Finance را با دستور زیر لیست می‌کنیم:

```
Dsget  group  "CN=Finance,OU=Groups,DC=contoso,DC=com"  -members
```

۴. اعضاء کامل گروه Finance را با دستور زیر لیست می‌کنیم:

```
Dsget  group  "CN=Finance,OU=Groups,DC=contoso,DC=com"  -members  -expand
```

۵. عضویت‌های مستقیم کاربر Scott Mitchell را با دستور زیر لیست می‌کنیم:

```
Dsget  user  "CN=Scott Mitchell,OU=People,DC=contoso,DC=com"  -memberof
```

۶. عضویت‌های کامل کاربر Scott Mitchell را با دستور زیر لیست می‌کنیم:

```
Dsget  user  "CN=Scott Mitchell,OU=People,DC=contoso,DC=com"  -memberof  -expand
```

خلاصه درس

- با دستورات Dsadd، CSVDE و LDIFDE می‌توان گروه ساخت.
- دستورات LDIFDE و Dsmod قادرند عضویت گروههای موجود را تغییر دهند.

- دستور Dsget می‌تواند اعضاء کامل یک گروه و لیست گروههایی را که کاربر عضو آن است نشان دهد.

سئوالات پایان درس

۱. کدام یک از دستورات زیر برای حذف عضو گروه استفاده می‌شود؟(بیش از یک جواب دارد)

A. Remove-Item

B. Dsrm

C. Dsmod

D. LDIFDE

E. CSVDE

۲. شما در حال افزودن یک گروه domainlocal با نام GroupA به یک گروه global با نام GroupB با استفاده از دستور Dsmod هستید. خطایی بروز می‌کند. کدام دستور مشکل را برطرف می‌کند ؟(بیش از یک جواب دارد)

A. Dsrm.exe

B. Dsmod.exe

C. Dsquery.exe

D. Dsget.exe

۳. مدیر شما از شما می‌خواهد لیستی از همه کاربران که به گروه Special Project تعلق دارند از جمله کاربرانی که در گروههای تودرتو در داخل گروه Special Project قرار دارند داشته باشد. از کدام دستور استفاده می‌کنید؟

A. Get-Members

B. Dsquery.exe

C. LDIFDE

D. Dsget.exe

درس ۳ مدیریت گروهها در یک شبکه سازمانی

درس ۱ و ۲ ما را برای انجام وظایف مدیریتی روزمره آماده کرد. یاد گرفتیم با استفاده از چند ابزار گروه بسازیم تغییر دهیم و حذف کنیم. در این درس یاد می‌گیریم از خصیصه‌های ویژه گروهها برای مستندسازی گروهها، تفویض اختیار مدیریت عضویت گروهها به کاربران یا تیم‌ها و خروج از بعضی چهارچوب‌های پیش فرض Active Directory استفاده کنیم.

بعد از این درس می‌توانیم:

- اهداف گروه را با استفاده از خصیصه‌های گروه مستند کنیم.

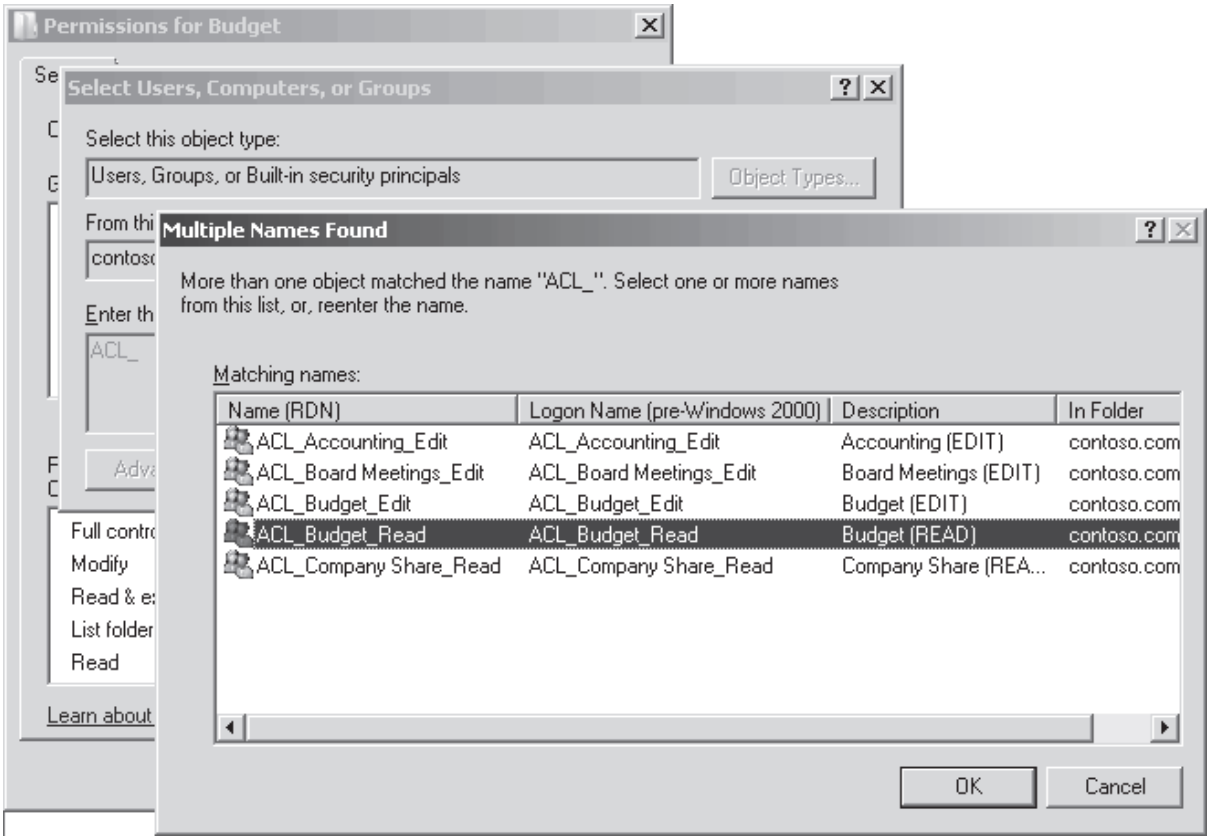
- از حذف ناگهانی گروه جلوگیری کنیم.
- مدیریت عضویت گروهها را واگذار کنیم.
- گروه shadow بسازیم.
- گروههای پیش فرض دامنه را تشخیص دهیم و مدیریت کنیم.
- به هویت‌های خاص مجوز بدهیم.

زمان تقریبی : ۴۵ دقیقه

بهترین تصمیم درباره خصیصه‌های گروه

هرچند ساخت یک گروه ساده است ولی ساخت گروه به طوری که در طول زمان قابل استفاده باشد کار آسانی نیست. ما می‌توانیم با مستندسازی اهداف ساخت گروه مدیریت و استفاده از آن را تسهیل کنیم. راههای متعددی در این مورد وجود دارد که اگرچه برای امتحان کاربردی ندارند برای مدیریت گروهها در سازمان نقش مهمی ایفا می‌کنند:

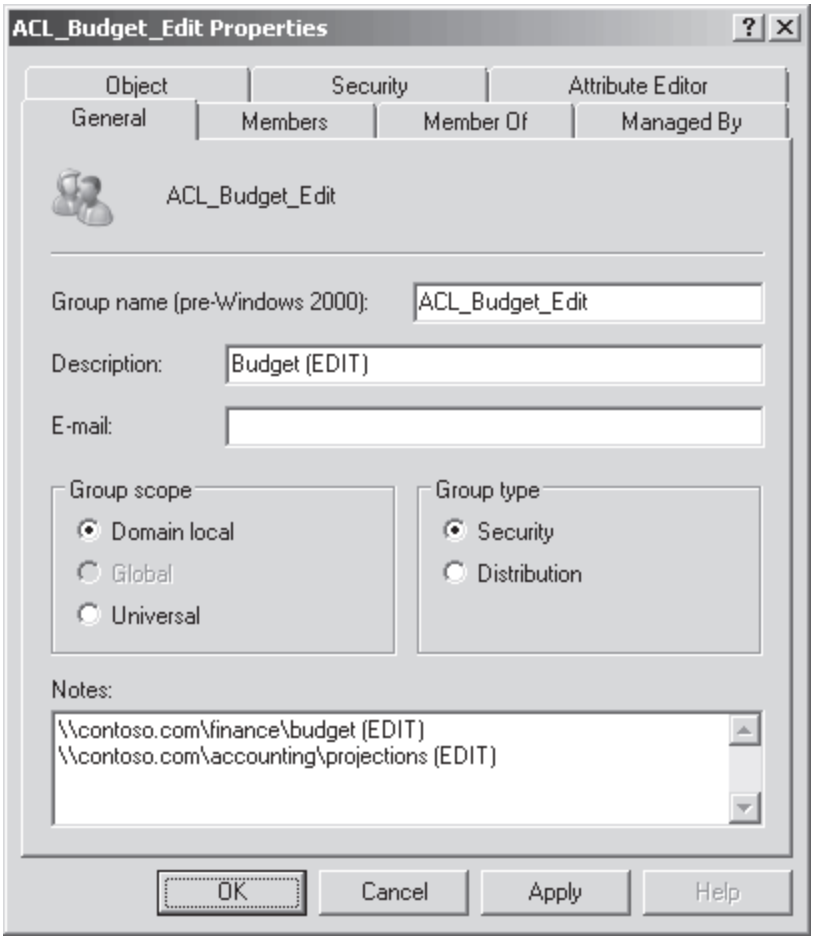
- **وضع قانون نام‌گذاری و وفاداری به آن** در درس ۱ پیشنهادی برای قانون نام‌گذاری گروهها ارائه شد. تعیین و پیروی از استانداردهای نام‌گذاری گروه بهره‌وری مدیریتی را افزایش می‌دهد. استفاده از پیشوند نشان‌دهنده هدف از ساخت گروه و استفاده از جداکننده مشخص بین پیشوند و بخش توصیفی نام گروه می‌توان گروه را بهتر محل‌یابی کرد. برای مثال پیشوند APP را می‌توان برای گروههایی که کار مدیریت برنامه‌ها را به عهده دارند در نظر گرفت و پیشوند ACL در نام گروههایی به کار گرفت که مجوز به آن‌ها اعطاء شده است. با این پیشوندها پیدا کردن و تفسیر اهداف گروهها با نام‌های APP_Accounting و ACL_Accounting_Read ساده‌تر است. اولی برای مدیریت توزیع نرم‌افزارهای حسابداری و دومی برای دسترسی خواندن به پوشه حسابداری ساخته شده است. پیشوندها همچنین درگروه‌بندی نام گروهها در رابط کاربری کاربرد دارد. شکل ۷- ۴ مثالی را در این مورد نشان می‌دهد. وقتی بخواهیم گروهی را برای اعطاء مجوز ساخته شده پیدا کنیم در کادر محاوره‌ای Select عبارت _ACL را تایپ می‌کنیم. کادر محاوره‌ای Multiple Names Found با نمایش گروههای _ACL در دایرکتوری ظاهر می‌شود.



شکل ۷- ۴ انتخاب یک گروه با استفاده از پیشوند گروه برای سهولت جستجو و انتخاب

- **اهداف گروه را در خصیصه description خلاصه کنید**از خصیصه description گروه برای خلاصه کردن اهداف گروه استفاده کنید. چون ستون Description در پنل وسط ابزار Active Directory Users And Computers به طور پیش فرض فعال است هدف گروه براحتی برای مدیران شبکه قابل رویت است.

- **جزئیات هدف گروه را در Notes وارد کنید** وقتی کادر محاوره‌ای Properties گروه را باز می‌کنیم فیلد Notes در پایین زبانه General برای مستندسازی هدف گروه به کار می‌رود. برای مثال می‌توان پوشه‌هایی را که گروه به آن مجوز دارد مانند شکل ۸- ۴ لیست کرد.



شکل ۸- ۴ کادر محاوره‌ای Properties گروه که فیلد Notes را نمایش می‌دهد.

حفاظت از گروهها در مقابل حذف ناگهانی

حذف یک گروه تاثیر زیادی در کار مدیریت و در امنیت می‌گذارد. گروهی را در نظر بگیرید که برای مدیریت دسترسی به منابع استفاده می‌شود. وقتی گروه حذف می‌شود دسترس به آن منابع تغییر می‌کند. کاربرانی که به واسطه گروه به منابع دسترسی داشتند دیگر امکان استفاده از آن منابع را نخواهند داشت یا اگر برای گروه عدم دسترسی به منابع خاصی در نظر گرفته شده باشد اعضای گروه پس از حذف به آن منابع دسترسی خواهند داشت.

به علاوه اگر گروه را دوباره بسازیم شیء گروه جدید دارای SID جدید خواهد بود که با SID قبلی که روی ACL منابع ثبت شده یکی نیست و بنابراین گروه جدید هرچند دارای نام یکسان با گروه حذف شده باشد از نظر سیستم گروه جدیدی به شمار می‌آید. به جای ساخت گروه باید قبل از سررسیدن زمان حذف نهایی گروه عملیات بازیابی را انجام دهیم. وقتی گروهی حذف می‌شود پس از دوره‌ای موسوم به tombstone که پیش فرض آن ۶۰ روز است گروه و SID آن به طور کل از Active Directory حذف می‌شود. در این دوره پس از بازیابی شیء حذف شده مجبور هستیم بسیاری از خصیصه‌ها را درباره تعریف کنیم. مهم‌ترین این خصیصه‌ها member گروه است. یعنی پس از بازیابی گروه باید عضویت گروه را دوباره از ابتدا تعریف کنیم. راه دیگر بازیابی گروه حذف شده بازیابی Authoritative یا در ویندوز سرور 2008 برگرداندن به Active Directory snapshot است که عضویت را نیز برمی‌گرداند و دیگر نیازی به تعریف مجدد کاربران گروه نداریم. بازیابی Authoritative و snapshot در فصل ۱۳ "نگهداری، پشتیبان گیری و بازیابی " بررسی می‌شود.

اطلاعات بیشتر بازیابی گروههای حذف شده

برای اطلاعات بیشتر در این زمینه به مقاله Knowledge Base شماره 840001 در آدرس
http://support.microsoft.com/kb/840001/en-us

در هر شرایطی باید متذکر شویم بازیابی گروه حذف شده مهارتی است که در شرایط بحرانی به کار گرفته می‌شود نه در شرایط عادی. بنابراین باید خودمان را در برابر نتایج مخرب حذف اشتباهی گروه محافظت کنیم. برای این کار گروه ساخته شده را در برابر حذف

ناگهانی محافظت می‌کنیم. ویندوز سرور 2008 امکان حفاظت از همه اشیاء را به آسانی در اختیار ما قرار داده است. برای انجام این کار مراحل زیر را انجام دهید:

۱. در ابزار Active Directory Users And Computers روی منوی View کلیک کرده و گزینه Advanced Features را علامت می‌زنیم.

۲. کادر محاوره Properties گروه را باز می‌کنیم.

۳. در زبانه Object کادر Protect Object From Accidental Deletion را علامت می‌زنیم.

۴. دکمه OK را کلیک می‌کنیم.

اینجا یکی از معدود جاهایی از ویندوز است که باید حتما روی OK کلیک کنیم. با کلیک کردن Apply تغییری ایجاد نمی‌کند. گزینه Protect Object From Accidental Deletion یک رکورد دسترسی به ACL شیء اضافه می‌کند که به طور کامل مجوز حذف خود شیء و زیرشاخه‌های آن را از گروه Everyone می‌گیرد. وقتی واقعا بخواهیم گروه را حذف کنیم باید به زبانه Object کادر محاوره‌ای Properties شیء مراجعه کرده و علامت کادر Protect Object From Accidental Deletion

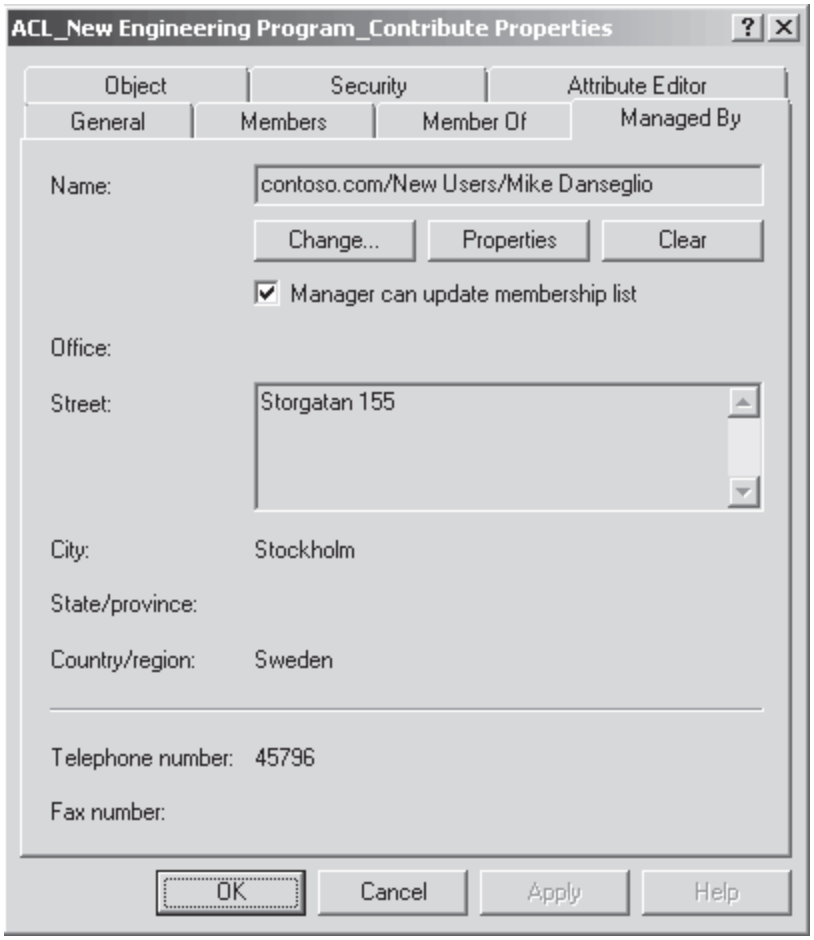
تفویض اختیار مدیریت عضویت گروه

بعد از ساخت گروه شاید بخواهیم مدیریت عضویت گروه را به یک تیم یا فرد خاصی واگذار کنیم که نسبت به منابع مورد استفاده گروه مسئولیت داشته باشد. برای مثال فرض کنید مدیر مالی شرکت مسئول ایجاد بودجه سال بعد است. شما پوشه‌ای را برای بودجه به اشتراک می‌گذارید و به گروهی موسوم به ACL_Budget_Edit دسترسی Write می‌دهید. وقتی کاربری نیاز دارد به پوشه دسترسی داشته باشد با تیم پشتیبانی تماس گرفته و درخواست خود را اعلام می‌کند. تیم پشتیبانی با مدیر مالی تماس می‌گیرد و پس از تایید ایشان کاربر به گروه اضافه می‌شود. ما با دادن مجوز تغییر عضویت به مدیر مالی کیفیت مدیریتی شبکه را ارتقاء می‌دهیم. از این به بعد کاربران درخواست عضویت گروه را به مدیر مالی ارائه می‌کنند. برای تفویض اختیار مدیریت عضویت گروه باید به مدیر مالی مجوز Allow Write Member نسبت به گروه اعطاء شود. خصیصه member خصیصه‌ای چند مقداره است. راههای متعددی برای تفویض اختیار وجود دارد. دو تا از آن‌ها در ادامه بررسی می‌شود.

تفویض اختیار مدیریت عضویت گروه از طریق Managed By

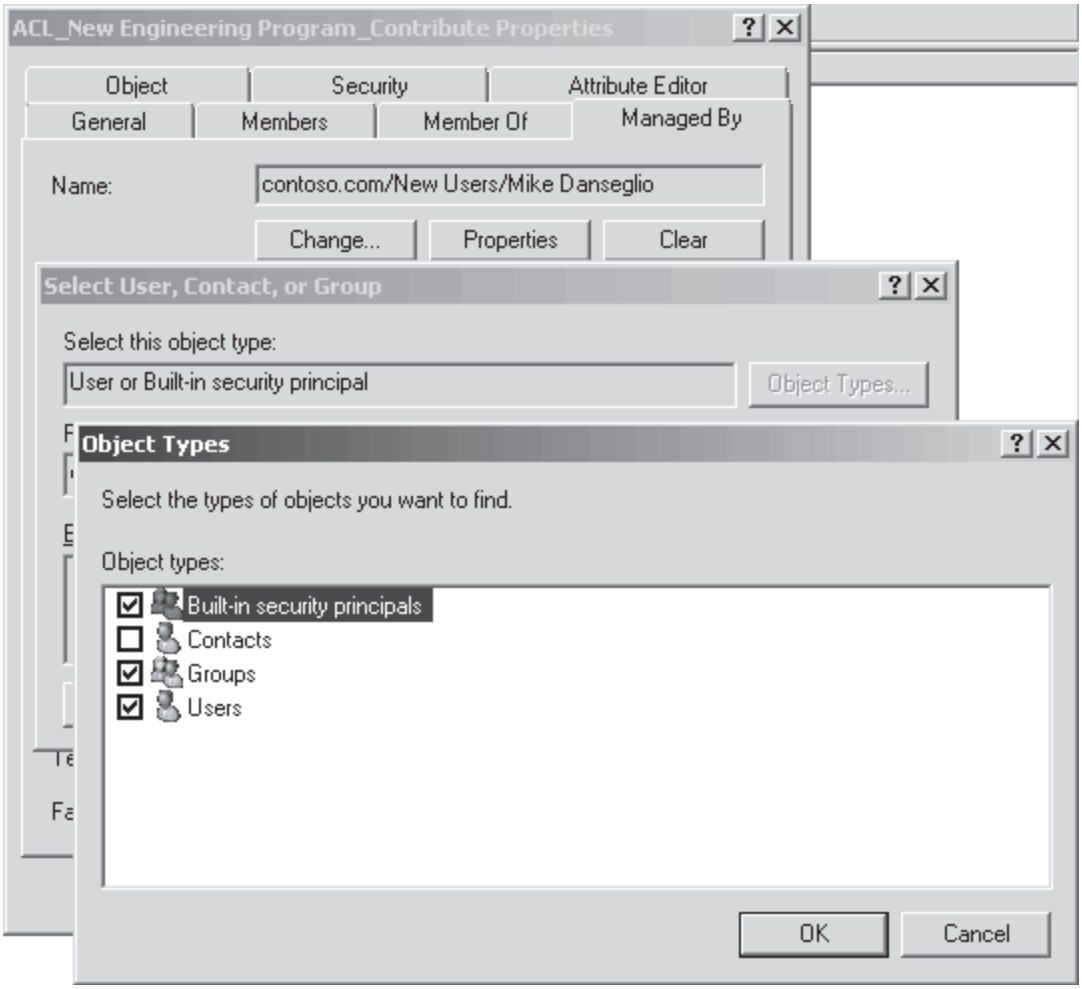
ساده ترین راه برای تفویض اختیار مدیریت گروه از طریق زبانه Managed By می‌باشد. این زبانه همان طوری که در شکل ۹- ۴ نشان داده شده است در کادر محاوره‌ای Properties گروه می‌باشد و دو هدف را دنبال می‌کند. اول فراهم کردن اطلاعات تماس مدیر گروه است. از این اطلاعات برای تماس با مسئول گروه استفاده می‌شود تا قبل از افزودن کاربر به گروه با او هماهنگی شود.

هدف دوم تفویض اختیار خصیصه member گروه است. به کادر نشان داده شده در شکل ۹- ۴ توجه کنید. عنوان کادر اینست Manager Can Update Membership List. اگر این کادر را علامت بزنیم کاربر یا گروه مشخص شده در کادر Name مجوز Write Member نسبت به گروه خواهند داشت. هر تغییری در این کادر روی ACL گروه تاثیر می‌گذارد.



شکل ۹- ۴ زبانه Managed By از کادر محاوره‌ای Properties گروه

البته درج یک گروه در زبانه Managed By گروه دیگر به همین سادگی نیست. وقتی روی کلید Change کلیک می‌کنیم کادر محاوره‌ای Select User, Contact, Or Group همانند شکل ۱۰- ۴ ظاهر می‌شود. اگر نام گروه را وارد و OK کنیم خطایی بروز می‌کند. دلیل آن اینست که این کادر برای قبول گروه به عنوان نوع شیء معتبر پیکربندی نشده است. برای از بین بردن این محدودیت روی دکمه Object Types کلیک می‌کنیم و کادر Groups را علامت می‌زنیم. کلید OK را کلیک می‌کنیم تا پنجره‌ها بسته شوند. اگر بخواهیم دسترسی WriteMember به گروه اعطاء کنیم کادر Manager Can Update Membership List را علامت می‌زنیم. وقتی به گروهی دسترسی فوق را اعطاء می‌کنیم هیچ اطلاعات تماسی در زبانه Managed By درج نمی‌شود چون گروهها چنین خصایصی ندارند.



شکل ۱۰- ۴ انتخاب یک گروه در زبانه Managed By

تفویض اختیار مدیریت گروه از طریق Advanced Security Settings

از این کادر محاوره‌ای برای اعطاء مجوز Allow Write Member به صورت مستقیم استفاده می‌شود. امکان تعیین مجوز برای یک گروه خاص یا همه گروههای یک OU وجود دارد.

تفویض اختیار مدیریت عضویت گروه برای یک گروه خاص

۱. در ابزار ACTIVE DIRECTORY USERS AND COMPUTERS روی منوی View کلیک کرده و گزینه Advanced Features را علامت می‌زنیم.

۲. روی گروه کلیک راست کرده و Properties را انتخاب می‌کنیم.

۳. زبانه Security را انتخاب می‌کنیم.

۴. دکمه Advanced را کلیک می‌کنیم.

۵. در کادر محاوره‌ای Advanced Security Settings دکمه Add را کلیک می‌کنیم.

اگر دکمه Add قابل رویت نیست دکمه Edit را کلیک کرده و بعد کلید Add را کلیک می‌کنیم.

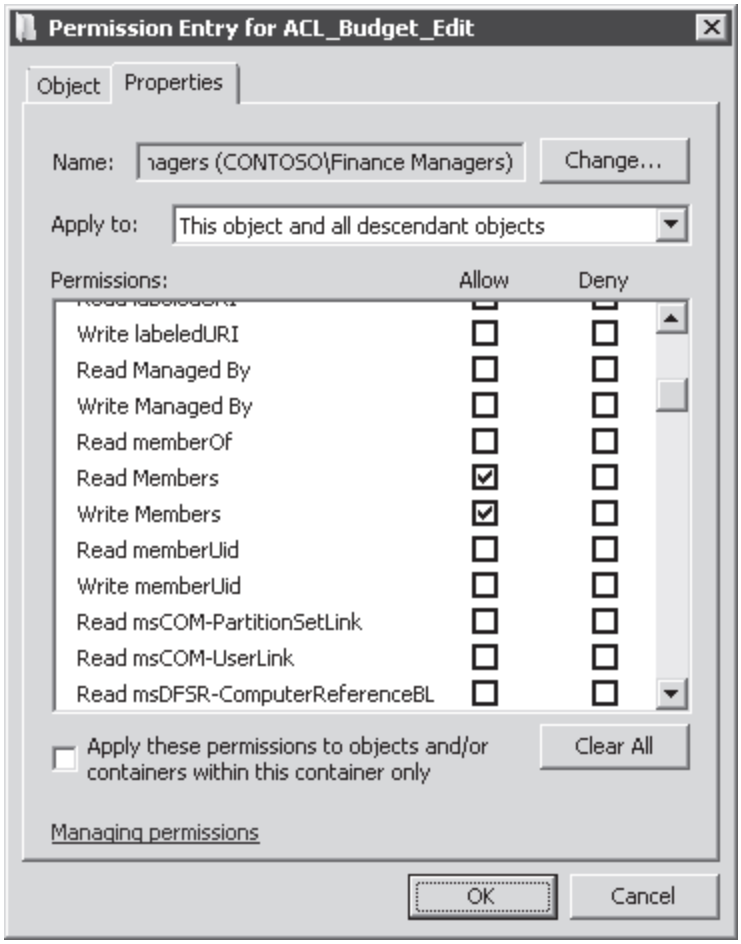
۶. در کادر محاوره‌ای Select نام گروهی را که قرار است به آن مجوز اعطاء شود انتخاب کرده و کلید OK را کلیک می‌کنیم.

۷. روی زبانه Properties کلیک می‌کنیم.

۸. در لیست بازشوی Apply To گزینه This Object And All Descendant Objects را کلیک می‌کنیم.

۹. در لیست مجوزها کادر Allow را کنار Read Members و Write Members علامت می‌زنیم.

به طور پیش فرض همه کاربران مجوز Read Members دارند بنابراین این مجوز را نیازی نیست انتخاب کنیم. به هرحال کنترل دسترسی مبتنی بر نقش زمانی به تحقق می‌پیوندد که همه مجوزها بر اساس نیازهای کاری ارائه شود نه از طریق مجوزهای غیر مستقیم.



شکل ۱۱- ۴ کادر محاوره‌ای Permission Entry را نمایش می‌دهد.

شکل ۱۱- ۴ کادر محاوره‌ای Permission Entry تفویض اختیار مدیریت عضویت گروه را نشان می‌دهد.

۱۰. روی دکمه OK کلیک می‌کنیم تا کادرهای محاوره‌ای بسته شوند.

تفویض اختیار مدیریت عضویت همه گروههای یک OU

۱. در ابزار ACTIVE DIRECTORY USERS AND COMPUTERS روی منوی View کلیک کرده و گزینه Advanced Features را علامت می‌زنیم.

۲. روی OU شامل گروهها کلیک راست کرده و Properties را انتخاب می‌کنیم.

۳. زبانه Security را انتخاب می‌کنیم.

۴. دکمه Advanced را کلیک می‌کنیم.

۵. در کادر محاوره‌ای Advanced Security Settings دکمه Add را کلیک می‌کنیم.

اگر دکمه Add قابل رویت نیست دکمه Edit را کلیک کرده و بعد کلید Add را کلیک می‌کنیم.

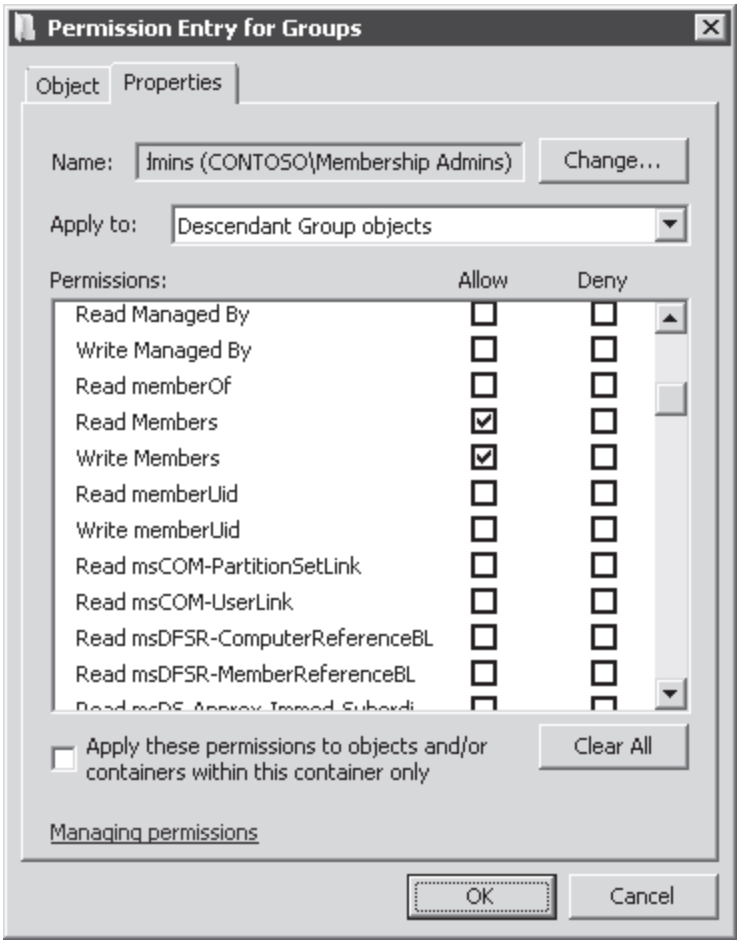
۶. در کادر محاوره‌ای Select نام گروهی را که قرار است به آن مجوز اعطاء شود انتخاب کرده و کلید OK را کلیک می‌کنیم.

۷. روی زبانه Properties کلیک می‌کنیم.

۸. در لیست بازشوی Apply To گزینه Descendant Group Objects را کلیک می‌کنیم. اگر از ابزارهای قدیمی ACTIVE DIRECTORY USERS AND COMPUTERS استفاده می‌کنیم گزینه Group Objects انتخاب می‌کنیم

۹. در لیست مجوزها کادر Allow را کنار مجوزهای Read Members و Write Members علامت می‌زنیم.

به طور پیش فرض همه کاربران مجوز Read Members دارند بنابراین این مجوز را نیازی نیست انتخاب کنیم. به هرحال کنترل دسترسی مبتنی بر نقش زمانی به تحقق می‌پیوندد که همه مجوزها بر اساس نیازهای کاری ارائه شود نه از طریق مجوزهای غیر مستقیم.
شکل ۱۲- ۴ کادر محاوره‌ای Permission Entry را نمایش می‌دهد.



شکل ۱۲- ۴ کادر محاوره‌ای Permission Entry تفویض اختیار مدیریت عضویت همه گروههای OU با نام Groups را نشان می‌دهد.

۱۰. روی دکمه OK کلیک می‌کنیم تا کادرهای محاوره‌ای بسته شوند.

گروههای سایه (Shadow)

عمده مدیریت یک شبکه سازمانی همراه گروهها ارائه می‌شود. به گروهها نسبت به منابع مجوز اعطاء می‌شود. همچنین می‌تواند برای فیلتر کردن حوزه اشیاء Group Policy استفاده شود. به گروهها سیاست‌های کلمه عبور نسبت داده می‌شود. گروهها به عنوان مجموعه‌هایی برای ابزارهای مدیریت پیکربندی مانند Microsoft System Configuration Manager می‌توانند استفاده شوند. این قابلیت‌ها ادامه دارند. OU ها به این گستردگی در مدیریت شبکه نقش ندارند و در بعضی موارد قابل استفاده نیستند. برای مثال به OU نمی‌توان مجوز دسترسی به منابع یا سیاست‌های کلمه عبور fine-grained اعطاء کرد (در فصل ۸ "تایید هویت" بررسی می‌شود). در عوض هدف اولیه OU فراهم کردن محدوده‌ای از مدیریت است که برای تفویض اختیار اشیاء داخل آن استفاده می‌شود. به عبارت دیگر OU با نام users به ما امکان می‌دهد به تیم پشتیبانی شبکه اجازه ریست کلمه عبور کاربران داخل OU را بدهیم. از این رو می‌توان گفت OU ها container های مدیریتی هستند.
دلیل تفاوت هدف OU ها و گروهها در این است که OU ها به اندازه گروهها منعطف نیستند. یک کامپیوتر یا کاربر (یا اشیاء دیگر) فقط می‌تواند در یک OU قرار گیرند ولی در عوض عضو گروههای متعددی باشند. بنابراین گروهها به منظور مرتب سازی هویت‌ها با نیازهای مشابه استفاده می‌شود. بعضی مواقع ممکن است بخواهیم با استفاده از OU کاری غیرممکن انجام دهیم. مثلا اگر بخواهیم به همه کاربران در یک OU نسبت به یک پوشه دسترسی بدهیم. یا یک سیاست کلمه عبور منحصر برای کاربران یک OU در نظر بگیریم. این کارها را به طور مستقیم نمی‌توانیم انجام دهیم ولی با ساخت گروههای سایه این کار امکانپذیر است. گروه سایه گروهی با همه کاربران یک OU است. به عبارت صحیح تر گروه سایه شامل کاربرانی با معیارهای معین می‌باشند.

ساده ترین راه برای ساخت گروه سایه این است که ابتدا گروهی بسازیم و سپس در OU که شامل کاربران است کلیدهای Ctrl+A را گرفته تا همه کاربران انتخاب شوند. روی یکی از کاربران انتخاب شده کلیک راست کرده و گزینه Add To Group را انتخاب می‌کنیم. نام گروه را تایپ کرده و OK را می‌زنیم.

نکته امتحانی در امتحان 70-640 باید با گروههای سایه آشنایی داشته باشید و بدانید که گروه سایه گروهی است که شامل همه اعضاء موجود در یک OU می‌باشد.

متاسفانه هنوز راهی برای تعیین عضویت یک گروه سایه به صورت اتوماتیک وجود ندارد. وقتی کاربری از OU حذف یا به آن اضافه می‌شود باید تغییر را در گروه سایه نیز دستی انجام دهیم.

اطلاعات بیشتر نگهداری گروههای سایه به طور خودکار

برای دسترسی به اسکریپت‌هایی که کار نگهداری گروههای سایه را به طور خودکار انجام می‌دهند به منبع Windows Resource Kit: Productivity Solutions for IT Professionals مراجعه کنید.

گروههای پیش فرض

تعدادی گروه هنگام نصب ویندوز سرور 2008 به طور خودکار ایجاد می‌شود که به آن ها گروههای پیش فرض محلی (default local groups) گویند و شامل گروههای معروف مانند Administrators، Backup Operators و Remote Desktop Users می‌باشد. گروههای دیگری نیز در یک دامنه در container های Users و Builtin ایجاد می‌شود که شامل Domain Admins، Enterprise Admins و Schema Admins است. لیست زیر خلاصه‌ای از قابلیت‌های گروههای پیش فرض را که دارای مجوزها و حقوق دسترسی مهم برای مدیریت Active Directory است نشان می‌دهد:

- **Enterprise Admins** (موجود در Users container در دامنه ریشه forest) این گروه عضوی از گروه Administrator در هر دامنه forest است که به آن اجازه دسترسی کامل به تمام تنظیمات همه DC ها را می‌دهد. همچنین دارای بخش پیکربندی دایرکتوری بوده و کنترل کامل روی محدوده نام دامنه در همه دامنه‌های forest دارد.

- **Schema Admins** (موجود در Users container دامنه ریشه forest) این گروه کنترل کامل روی Active Directory schema دارد.

- **Administrators** (موجود در Builtin container هر دامنه) این گروه کنترل کاملی روی همه DC ها و داده محدوده نام دامنه دارد. این گروه می‌تواند عضویت همه گروههای مدیریتی دیگر دامنه را تغییر دهد و گروه Administrators دامنه ریشه forest می‌تواند عضویت Enterprise Admins، Schema Admins و Domain Admins را تغییر دهد. گروه Administrators دامنه ریشه forest قدرتمندترین گروه مدیریتی در forest است.

- **Domain Admins** (موجود در Users container هر دامنه) این گروه به گروه Administrators همان دامنه افزوده می‌شود بنابراین همه قابلیت‌های گروه Administrators را به ارث می‌برد. همچنین به طور پیش فرض به گروه Administrators محلی همه کامپیوترهای عضو دامنه اضافه می‌شود و کامپیوترهای دامنه را در تصاحب این گروه در می‌آورد.

- **Server Operators** (موجود در Builtin container هر دامنه) این گروه می‌تواند وظایف نگهداری DC ها را انجام دهد. می‌تواند به سرور DC وارد شود، سرویس‌ها را شروع یا متوقف کند، عملیات پشتیبان‌گیری و بازیابی اطلاعات را اجرا کند، دیسکهای سرور را فرمت کند، پوشه‌ها را به اشتراک گذاشته یا از اشتراک در آورد و سرور را خاموش کند. به طور پیش فرض عضوی ندارد.

- **Account Operators** (موجود در Builtin container هر دامنه) این گروه می‌تواند در OU های دامنه و container های Users و Computers حساب‌های کاربران گروهها و کامپیوترها را بسازد تغییر دهد و حذف کند (به استثناء Domain Controllers OU). این گروه نمی‌تواند حساب‌های عضو گروههای Administrators یا Domain Admins و خود گروهها را تغییر دهند. اعضای این گروه می‌توانند به DC ها وارد شوند. به طور پیش فرض هیچ عضوی ندارند.

- **Backup Operators** (موجود در Builtin container هر دامنه) این گروه می‌تواند عملیات پشتیبان گیری و بازیابی را روی DC ها انجام دهد و به DC وارد شده و آن را خاموش کند. به طور پیش فرض هیچ عضوی ندارند.

- **Print Operators** (موجود در Builtin container هر دامنه) این گروه می‌تواند صف‌های چاپ را روی DC ها نگهداری کنند و به DC ها وارد شده و آن را خاموش کنند.

گروههای پیش فرض که دسترسی‌های مدیریتی را فراهم می‌کنند باید با احتیاط مدیریت شوند زیرا در بیشتر موارد بیش از حد نیاز اختیار دارند.
گروه Account Operators مثال کاملی در این مورد است. اگر قابلیت‌های این گروه را لیست کنیم می‌بینیم که حقوق این گروه خیلی وسیع است. این گروه حتی می‌تواند به DC وارد شود. در سازمان‌های کوچک چنین حقی احتمالا برای یک یا دو فرد خاص که مدیر شبکه هستند مناسب است. در شبکه‌هایی با هر اندازه حقوق و مجوزهای اعطاء شده به گروه Account Operators خیلی وسیع است.
به علاوه این گروه مانند گروههای مدیریتی که قبلا لیست شد یک گروه حفاظت شده (protected) است. گروههای حفاظت شده توسط سیستم عامل تعریف می‌شود و غیر قابل حذف هستند. اعضاء این گروه محافظت می‌شوند. نتیجه این محافظت مجوزهای (ACL ها) گروههاست که طوری تغییر می‌کنند که دیگر مجوزهای OU خود را به ارث نمی‌برد به جای آن یک کپی از یک ACL که کاملا محدود است دریافت می‌کند. مثلا اگر Jeff Ford به گروه Account Operators اضافه شود حساب او محافظت می‌شود و اعضای گروه پشتیبانی که می‌توانند کلمات عبور همه کاربران را در People OU ریست کنند دیگر قادر به ریست کردن کلمه عبور Jeff Ford نخواهند بود.

اطلاعات بیشتر حساب‌های محافظت شده

برای اطلاعات بیشتر درباره حساب‌های محافظت شده مقاله Knoeledge Base شماره 817433 را در آدرس http://support.microsoft.com/?kbid=817433 . اگر بخواهیم در اینترنت دنبال منابع بگردیم از واژه adminSDHolder استفاده می‌کنیم.
به همین دلایل (حقوق وسیع و محافظت) باید سعی کنیم از افزودن کاربران به گروههای لیست شده که به طور پیش فرض هیچ عضوی ندارند تا حد امکان پرهیز کنیم : یعنی Account Operators، Backup Operators، Server Operators و Print Operators. در عوض گروههایی بسازیم و به آن مجوزها و حقوق لازم برای انجام کارها را بدهیم. برای مثال اگر Scott Mitchell باید بتواند عملیات پشتیبان‌گیری روی DC را انجام دهد ولی نباید عملیات بازیابی یا خاموش کردن سرور را انجام دهد Scott Mitchell را در گروه Backup Operators قرار نمی‌دهیم. به جای آن یک گروه ساخته و به آن فقط حق Backup Files And Directories می‌دهیم. سپس Scott را عضو گروه می‌کنیم.

اطلاعات بیشتر اطلاعات قابلیت‌های گروههای پیش‌فرض

یک مرجع کامل درباره گروههای پیش‌فرض در دامنه و گروههای محلی پیش‌فرض در Microsoft TechNet موجود است. اگر با گروههای پیش‌فرض و قابلیت‌های آن‌ها آشنا نیستید باید برای امتحان آن را مرور کنید. مرجع گروههای پیش‌فرض دامنه در آدرس http://technet2.microsoft.com/WindowsServer/en/library/1631acad-ef34-4f779c2e-94a62f8846cf1033.mspx و مرجع گروههای محلی پیش‌فرض در آدرس http://technet2.microsoft.com/WindowsServer/en/library/f6e01e51-14ea-97fc-5288a9a4a9b11033.mspx

هویتهای خاص (Special Identities)

ویندوز و Active Directory همچنین از هویت‌های خاص پشتیبانی می‌کنند. این هویت‌ها در واقع گروههایی هستند که عضویت آن‌ها توسط سیستم عامل کنترل می‌شود. ما نمی‌توانیم گروهها را در قالب یک لیست مثلا در ابزار Active Directory Users And Computers مشاهده کنیم. همچنین نمی‌توانیم عضویت این گروهها را ببینیم یا آن‌ها را تغییر دهیم و عضو گروههای دیگر کنیم. فقط می‌توان از این گروهها برای اعطاء مجوز استفاده کرد. مهم‌ترین هویت‌های خاص که اغلب برای راحتی به صورت گروه به آن اشاره می‌شود در لیست زیر بررسی می‌شود:

- **Anonymous Logon** اتصالات به یک کامپیوتر و منابعی را که در اختیار کاربر بدون ارائه نام کاربری و کلمه عبور قرار می‌دهد کنترل می‌کند. قبل از ویندوز سرور 2003 این گروه عضو گروه Everyone بود ولی از ویندوز سرور 2003 به بعد دیگر عضو این گروه قرار نمی‌گیرد.
- **Authenticated Users** نمایانگر هویت‌هایی است که تایید هویت شده اند. این گروه شامل Guest نمی‌شود حتی اگر حساب Guest کلمه عبور داشته باشد.
- **Everyone** شامل گروه Authenticated Users و Guest می‌باشد. در سیستم‌های قبل از ویندوز سرور 2003 این گروه شامل Anonymous Logon می‌باشد.
- **Interactive** نمایانگر کاربرانی است که هنگام ورود به سیستمی که دارای منابع است به آن منابع دسترسی پیدا می‌کنند. این گروه در مقابل گروهی است که از راه دور به منابع دسترسی پیدا می‌کنند. وقتی کاربری به سیستمی وارد شده و به منابع آن دسترسی پیدا می‌کند به صورت خودکار کاربر به گروه Interactive آن منبع اضافه می‌شود. همچنین کاربرانی که از طریق ارتباط remote desktop وارد سیستم شوند عضو این گروه خواهند شد.
- **Network** نمایانگر کاربرانی است که از طریق شبکه به منابع دسترسی پیدا می‌کنند. وقتی کاربری به منابع سیستمی از طریق شبکه دسترسی پیدا می‌کند به صورت خودکار کاربر به گروه Network آن منبع اضافه می‌شود.

اهمیت این گروهها این است که ما را قادر می‌سازند بر اساس نوع تایید هویت یا طریقه اتصال به منابع دسترسی‌ها را مدیریت کنیم نه بر اساس حساب‌های کاربری. برای مثال می‌توانیم پوشه‌ای ایجاد کرده و به کاربران وقتی به سیستم وارد می‌شوند اجازه مشاهده محتویات را بدهیم و به همان کاربران وقتی از طریق شبکه وارد می‌شوند این اجازه را ندهیم. این کار با اعطاء مجوز به گروه Interactive قابل انجام است.

تمرینات مدیریت گروهها در یک شبکه سازمانی

در این تمرینات قرار است بهترین روش‌های مدیریت گروه در دامنه contoso.com انجام شود. برای اجرای این تمرینات باید اشیاء زیر در دامنه contoso.com موجود باشد:

- OU سطح اول با نام Groups
- یک گروه امنیتی global با نام Finance در OU با نام Groups
- OU سطح اول با نام People
- یک حساب کاربری با نامMike Danseglio در OU با نام People . اطلاعات تماس را به شکل فرضی وارد کنید. گزینه مربوط به تغییر کلمه عبور در اولین ورود کاربر را خالی بگذارید.

به علاوه گروه Domain Users را عضو گروه Print Operators کنید که در container با نام Builtin موجود است تا کاربران نمونه در این تمرین بتوانند به DC با نام SERVER01 وارد شوند. در این تمرینات ما این کار را انجام می‌دهیم ولی در دنیای واقعی نباید کاربران عادی اجازه ورود به DC را داشته باشند بنابراین گروه Domain Users را نباید عضو گروه Print Operators کنیم.

تمرین ۱ یک گروه با مستندات کامل بسازیم

در این تمرین گروهی برای مدیریت دسترسی به پوشه Budget ایجاد می‌شود و بهترین روش را در این درس دنبال می‌کنیم.

۱. با کاربر Administrator به SERVER01 وارد شده و ابزار ACTIVE DIRECTORY USERS AND COMPUTERS را اجرا می‌کنیم.

۲. OU با نام Groups را در ساختار درختی کنسول انتخاب می‌کنیم.

۳. روی OU با نام Groups کلیک راست کرده و New و سپس Group را انتخاب می‌کنیم. کادر محاوره‌ای New Object – Group ظاهر می‌شود.

۴. در کادر Group Name عبارت ACL_Budget_Edit را تایپ می‌کنیم.

۵. نوع گروه را امنیتی و حوزه را Domain Local انتخاب کرده و OK می‌کنیم.

۶. منوی View را باز کرده و گزینه Advanced Features را انتخاب می‌کنیم.

۷. روی گروه ACL_Budget_Edit کلیک راست کرده و Properties را انتخاب می‌کنیم.

۸. زبانه Object را باز می‌کنیم.

۹. کادر Protect Object From Accidental Deletion را علامت زده و OK می‌کنیم.

۱۰. پنجره Properties گروه را دوباره باز می‌کنیم.

۱۱. در کادر Description تایپ می‌کنیم (BUDGET(EDIT) .

۱۲. در فیلد Notes مسیر زیر را تایپ می‌کنیم تا پوشه‌هایی که این گروه به آن دسترسی دارند مشخص شود:

\\server23\data$\finance\budget
\\server32\data$\finance\revenue projections

۱۳. روی OK کلیک می‌کنیم.

تمرین ۲ تفویض مدیریت عضویت گروه

در این تمرین به Mike Danseglio امکان مدیریت عضویت گروه ACL_Budget_Edit را می‌دهیم.

۱. کادر محاوره‌ای Properties گروه ACL_Budget_Edit را باز می‌کنیم.

۲. زبانه Managed By را باز می‌کنیم.

۳. دکمه Change را کلیک می‌کنیم.

۴. نام کاربری Mike Danseglio را تایپ کرده و OK می‌کنیم.

۵. کادر Manager Can Update Membership List را علامت زده و OK می‌کنیم.

تمرین ۳ ارزیابی تفویض مدیریت عضویت

در این تمرین تفویض مدیریت که در تمرین ۲ انجام شد با تغییر عضویت گروه با استفاده از کاربر Mike Danseglio تست می‌شود.

۱. پنجره خط فرمان را باز می‌کنیم.

۲. دستور زیر را اجرا می‌کنیم: runas /user:Username cmd.exe و به جای Username نام کاربری Mike Danseglio را تایپ می‌کنیم.

۳. در صورت نیاز کلمه عبور کاربر مربوطه را وارد می‌کنیم. پنجره خط فرمان جدیدی با حساب کاربری Mike Danseglio باز می‌شود.

۴. دستور زیر را تایپ کرده و کلید Enter را می‌زنیم:

```
Dsmod group “CN=ACL_Budget_Edit,OU=Groups,DC=contoso,DC=com” –addmbr
“CN=Finance,OU=Groups,DC=contoso,DC=com”
```

۵. پنجره خط فرمان را می‌بندیم.

۶. در ابزار ACTIVE DIRECTORY USERS AND COMPUTERS عضویت گروه ACL_Budget_Edit را چک کرده و اطمینان حاصل می‌کنیم که گروه Finance به آن افزوده شده است.

خلاصه درس

- از فیلدهای Description و Notes در کادر محاوره‌ای Properties گروه برای مستند سازی اهداف گروه استفاده می‌کنیم.
- زبانه Managed By ما را قادر می‌سازد کاربر یا گروهی را که مسئول گروه است مشخص کنیم. همچنین می‌توان اجازه مدیریت عضویت گروه را به کاربر یا گروهی دیگر صادر کرد. برای این کار کادر Manager Can Update Membership List را علامت می‌زنیم.
- برای تفویض مدیریت عضویت گروه مجوز Allow Write Members را اعطاء می‌کنیم.
- برای جلوگیری از حذف تصادفی گروه کادر Protect Object From Accidental Deletion را علامت می‌زنیم.
- ویندوز سرور 2008 و Active Directory دارای گروههای پیش فرض با مجوزها و حقوق مهمی هستند. بهتر است به گروههای پیش فرض که عضوی ندارند عضوی اضافه نکنیم (Account Operators، Backup Operators ، Print Operators و Server Operators) و عضویت گروههای مدیریتی دیگر را به شدت محدود کنیم (Enterprise Admins، Domain Admins، Schema Admins و Administrators).
- هویت‌های خاص مانند Authenticated Users، Everyone، Interactive و Network می‌توانند برای اعطاء مجوز و حقوق به کار روند. عضویت آن‌ها توسط سیستم عامل تعیین می‌شود و قابل تغییر نیست.

سئوالات پایان درس

۱. شرکت شما در حال تدارک جلسه‌ای برای پروژه‌ای خاص می‌باشد. داده تا حدی محرمانه می‌باشد. جلسه در اتاق کنفرانس تشکیل می‌شود و شما یک پوشه روی کامپیوتر اتاق کنفرانس ساخته و به اعضاء تیم دسترسی داده‌اید. می‌خواهید مطمئن شوید اعضاء فقط زمانی که به کامپیوتر وارد می‌شوند به داده دسترسی داشته باشند نه زمانی که از طریق شبکه متصل می‌شوند. چه کار باید انجام دهید؟

A. مجوز Allow Read به گروه Interactive اعطاء می‌کنید.

B. مجوز Allow Read به گروه team اعطاء می‌کنید.

C. مجوز Deny Traverse Folders به گروه team اعطاء می‌کنید.

D. مجوز Deny Full Controll به گروه Network اعطاء می‌کنید.

۲. می‌خواهید به یک کاربر به نام Mike Danseglio اجازه افزودن کاربران به یا حذف کاربران را از گروهی به نام Special Project بدهید. چطور این مجوز را پیکربندی می‌کنید؟

A. زبانه Members گروه

B. زبانه Security شیء کاربر Mike Danseglio

C. زبانه Member Of شیء کاربر Mike Danseglio

D. زبانه Managed By گروه

۳. کدام یک از گروههای زیر می‌توانند DC را خاموش کنند؟ (ممکن است بیش از یک جواب داشته باشد.)

A. Account Operators

B. Print Operators

C. Backup Operators

D. Server Operators

E. Interactive

فصل ۵

کامپیوترها

کامپیوترها هم مانند کاربران در دامنه واحدهای امنیتی به حساب می‌آیند. آن‌ها یک حساب با یک نام و کلمه عبور دارند که ویندوز به طور خودکار هر ۳۰ روز کلمه عبور را عوض می‌کند. آن‌ها با دامنه تایید هویت می‌شوند. می‌توانند به گروهها تعلق داشته باشند، به منابع دسترسی داشته باشند و توسط Group Policy پیکربندی شوند. کامپیوترها نیز مانند کاربران گاهی کلمه عبور خود را گم می‌کنند و نیاز به ریست دارند یا حسابی دارند که باید فعال یا غیرفعال شود.

مدیریت کامپیوترها چه اشیاء موجود در Active Directory Domain Services (AD DS) و چه دستگاههای فیزیکی، بخشی از کار روزمره متخصصین IT به شمار می‌آید. سیستم‌های جدید به سازمان افزوده می‌شوند کامپیوترها برای تعمیر از کار باز می‌ایستند کامپیوترها بین کاربران دست به دست می‌شوند و کامپیوترهای قدیمی از رده خارج یا ارتقا داده می‌شوند. هر کدام از این فعالیت‌ها نیاز به مدیریت هویت کامپیوتر دارد که توسط شیء یا حساب در Active Directory ارائه می‌شود.

متاسفانه بیشتر سازمان‌ها به اندازه‌ای که روی حساب‌های کاربری سرمایه‌گذاری می‌کنند روی کامپیوترها سرمایه‌گذاری نمی‌کنند هر چند هر دو واحدهای امنیتی به شمار می‌آیند. در این فصل یاد می‌گیریم اشیاء کامپیوتر بسازیم. این اشیاء شامل خصیصه‌هایی است که با آن‌ها شیء به عنوان یک حساب جلوه می‌کند. یاد می‌گیریم چطور از حساب‌های کامپیوتر نگهداری کنیم که شامل پیکربندی، رفع عیوب، تعمیر و حذف اشیاء می‌باشد. همچنین می‌توانیم درک خود را در مورد مراحلی که توسط آن یک کامپیوتر عضو دامنه می‌شود (یعنی join می‌شود) عمق ببخشیم به طوری که بتوانیم از خطاهای بالقوه جلوگیری کنیم.

اهداف امتحان در این فصل:

- ساخت و نگهداری اشیاء Active Directory
  - خودکارسازی ساخت حساب‌های Active Directory
  - نگهداری حساب‌های Active Directory
- دروس این فصل:
  - درس ۱: ساخت کامپیوتر و join کردن آن به دامنه
  - درس ۲: خودکارسازی ساخت اشیاء کامپیوتر
  - درس ۳: پشتیبانی از اشیاء و حساب‌های کامپیوتر

قبل از شروع

در این فصل از PowerShell ویندوز، VBScript، CSVDE و LDIFDE برای خودکارسازی ساخت حساب کامپیوتر استفاده می‌شود. قبل از مطالعه این فصل درس ۱و۲ را از فصل ۳ مرور کنید.

دنیای واقعی

دن هلم

کامپیوترها حداقل در Active Directory مانند کاربر هستند. مانند کاربران حساب دارند. می‌توانند کلمه عبور را فراموش کنند. چون کامپیوترها واحدهای امنیتی بوده و در حوزه Group Policy (در فصل بعد بررسی می‌شود) قابل استفاده هستند مهم است که با آن‌ها مشابه حساب‌های کاربری رفتار شود.

مطمئنا تا کنون با وضعیتی روبرو شده‌اید که مجبور شوید کامپیوتری را از دامنه حذف کرده و دوباره آن را به دامنه join کنید. همانطوریکه در درس ۳ خواهید دید این راه درست نیست و مانند این است که کاربری را به دلیل فراموشی کلمه عبور حذف و دوباره بسازیم. این فقط یک مثال از سناریوهایی است که مرتبا مشاهده می‌شود و در آنها مدیران شبکه کمی با حساب‌های کامپیوتر بی‌احتیاطی می‌کنند.

در این درس یاد می‌گیریم که از حساب‌های کامپیوتر نیز مانند بقیه واحدهای امنیتی (کاربران و گروهها) در دامنه نگهداری کنیم. همچنین یاد می‌گیریم از ابزارهای خط فرمان، VBScript و PowerShell ویندوز برای خودکارسازی ساخت و مدیریت اشیاء کامپیوتر استفاده کنیم. تشابهات زیادی را بین مراحل اجرایی این فصل با فصل ۳ خواهیم دید.

درس ۱: ساخت کامپیوترها و عضویت در دامنه

پیکربندی پیش فرض ویندوز سرور 2008 هم مانند 2003، ویستا، XP و 2000 این است که کامپیوتر به یک workgroup تعلق دارد. برای اینکه بتوانیم با حساب کاربری دامنه به کامپیوتر وارد شویم آن کامپیوتر باید عضو دامنه باشد. کامپیوتر برای عضویت باید یک حساب در دامنه داشته باشد که مانند حساب کاربری شامل نام (sAMAccountName)، کلمه عبور و SID باشد. SID انحصاری بوده و کامپیوتر را به عنوان یک واحد امنیتی در دامنه معرفی می‌کند. این حساب کامپیوتر را قادر می‌سازد در دامنه تایید هویت شده و ارتباط امنی برقرار شود که از این طریق کاربران بتوانند با حساب‌های دامنه خود به سیستم وارد شوند. همچنین مراحلی را می‌بینیم که از طریق آن کامپیوتر عضو دامنه می‌شود.

بعد از این درس می‌توانیم:

- ساختار OU برای کامپیوترها طراحی کنیم.
- در دامنه اشیاء کامپیوتر بسازیم.

- مجوز ساخت اشیاء کامپیوتر را واگذار کنیم.
- کامپیوترها را به دامنه join کنیم.
- مسیر Container پیش فرض computer را تغییر دهیم.
- از ساخت شیء کامپیوتر و join کردن کامپیوترها توسط کاربران عادی جلوگیری کنیم.

زمان تقریبی : ۴۵ دقیقه

Workgroup، دامنه و Trust

در یک شبکه Workgroup هر سیستمی دارای یک انباره هویت حساب‌های کاربران و گروهها می‌باشد که با آن کاربران تایید هویت شده و دسترسی‌ها امکانپذیر می‌شود. انباره هویت محلی روی هر کامپیوتر، بانک اطلاعاتی Security Accounts Manager (SAM) نامیده می‌شود. وقتی کاربری به شبکه workgroup وارد می‌شود سیستم تایید هویت کاربر را بر اساس بانک اطلاعاتی SAM محلی انجام می‌دهد. اگر کاربر به سیستم دیگری متصل شود مثلا برای دسترسی به یک فایل دوباره کاربر باید در انباره هویت سیستم مقصد تایید هویت گردد. از منظر امنیت، کامپیوتر موجود در workgroup همیشه یک سیستم انفرادی است.

وقتی کامپیوتری عضو دامنه می‌شود وظیفه تایید هویت کاربران را به دامنه واگذار می‌کند. اگرچه کامپیوتر بانک SAM را برای پشتیبانی از کاربران و گروههای محلی نگه می‌دارد حساب‌های کاربری به طور معمول در دایرکتوری مرکزی دامنه ساخته می‌شوند. وقتی کاربری با حساب دامنه به کامپیوتر وارد می‌شود کاربر به جای SAM توسط DC تایید هویت می‌شود. به عبارت دیگر حالا کامپیوتر به یک منبع دیگر برای تایید هویت کاربر اعتماد می‌کند. ارتباطات Trust معمولا در محدوده دو دامنه بررسی می‌شود که در فصل ۱۲ به آن می‌پردازیم ولی بین اعضاء دامنه و کامپیوترها زمانی که کامپیوتر عضو دامنه می‌شود trust برقرار می‌شود.

تعیین نیازمندی‌های join شدن یک کامپیوتر به دامنه

برای join کردن یک کامپیوتر به دامنه سه شرط وجود دارد:

- یک شیء کامپیوتر باید در سرویس دایرکتوری ساخته شود.
- ما باید مجوز لازم به شیء کامپیوتر را داشته باشیم. مجوز به ما امکان می‌دهد کامپیوتر را با همان نام به عنوان شیء به دامنه join کنیم.
- ما باید عضو گروه Administrators محلی روی کامپیوتر باشیم تا بتوانیم عضویت دامنه یا workgroup را عوض کنیم.

در بخش‌های بعدی هر کدام از این شرایط بررسی می‌شود.

Computers Container

قبل از ساخت شیء کامپیوتر در سرویس دایرکتوری (اولین شرط عضو شدن کامپیوتر به دامنه) باید جایی برای آن در نظر بگیریم. وقتی دامنه ایجاد می‌شود به طور پیش فرض Computers container ساخته می‌شود (CN=Computers, . . .). این container یک OU نیست بلکه یک شیء از کلاس container است. چند تفاوت ظریف و مهم بین یک container و OU وجود دارد. ما نمی‌توانیم داخل container یک OU بسازیم پس نمی‌توانیم Computers OU را تقسیم کنیم و شیء Group Policy را به یک container پیوند کنیم. بنابراین اکیدا توصیه می‌شود به جای Computers container از یک OU سفارشی برای نگهداری اشیاء کامپیوتر استفاده کنیم.

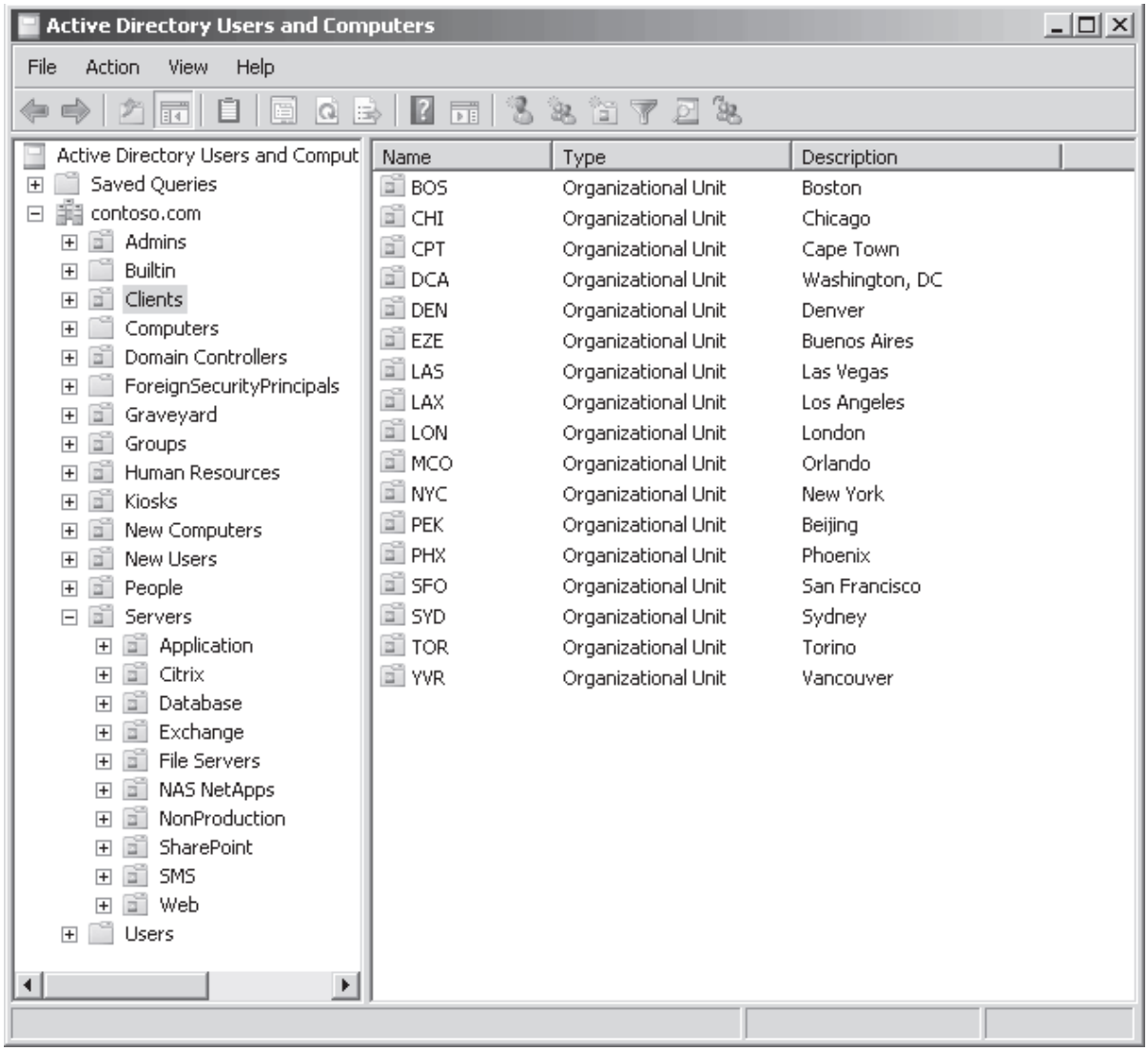
ساخت OU برای کامپیوترها

بسیاری از سازمان‌ها حداقل دو OU برای اشیاء کامپیوتر می‌سازند. یکی برای کلاینت‌ها یعنی دسک‌تاپ، لپ‌تاپ و دیگر سیستم‌ها و دیگری برای سرورها. این دو OU اضافه بر Domain controllers OU است که به طور پیش فرض هنگام نصب Active Directory ساخته می‌شود. در هر کدام از این OU ها اشیاء کامپیوتر ساخته می‌شوند. اشیاء کامپیوتر، اشیاء کامپیوتر هستند و فرقی

بین یک شیء کامپیوتر در OU کلاینت‌ها و OU سرورها یا Domain Controller ها وجود ندارد. ولی OU های مجزا به منظور ایجاد محدوده مدیریتی ساخته می‌شوند به طوری‌که بتوانیم مدیریت اشیاء کلاینت را به یک تیم و اشیاء سرور را را به تیم دیگری واگذار کنیم.

مدل مدیریتی ما ممکن است نیاز به تعمیق بیشتری داشته باشد. بسیاری از سازمان‌ها داخل OU سرور OU های فرعی می‌سازند تا انواع خاصی از سرورها را جمع‌آوری و مدیریت کنند مثلا یک OU برای سرورهای فایل و پرینت و یک OU برای سرورهای بانک اطلاعاتی. به این ترتیب مجوزهای مدیریت اشیاء کامپیوتر در OU مربوطه به تیم مدیران شبکه برای هر نوع سرور داده می‌شود. به طرز مشابهی سازمان‌های با توزیع جغرافیایی گسترده با تیم پشتیبانی محلی اغلب OU اصلی مربوط به کلاینت‌ها را به چند OU هر کدام برای یک منطقه تقسیم می‌کنند. این رویکرد تیم پشتیبانی محلی را قادر می‌سازد در سایت خود برای کلاینت‌های کامپیوتر شیء بسازند و کامپیوترها را به دامنه join کنند. این فقط یک مثال است. چیزی که از همه مهم‌تر است این است که ساختار OU ما منعکس کننده مدل مدیریتی سازمان ماست به طوری که OU های ما نقطه مرکزی مدیریتی برای تفویض وظایف مدیریتی به‌شمار می‌آیند.

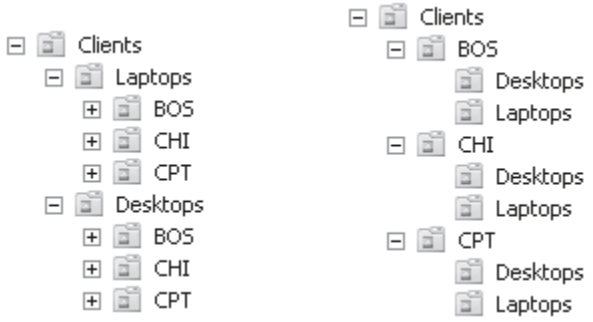
شکل ۱- ۵ یک طرح رایج OU برای یک سازمان است که تیم مدیران سرورها روی انواع خاصی از سرورها تمرکز دارند و تیم پشتیبانی روی کلاینت‌های مناطق مشخص کار می‌کنند.



شکل ۱- ۵ طرح رایج OU که مدیریت کلاینت‌ها بر اساس سایت و مدیریت سرورها بر اساس نقش سروری طراحی شده است.

به علاوه، OU های مجزا ما را قادر می‌سازند با استفاده از اشیاء Group Policy (GPOs) مختلف پیکربندی‌های پایه متفاوتی ساخته و به OU های سرور و کلاینت پیوند دهیم. جدا کردن کلاینت‌ها به دو OU با نام Laptop و Desktop نیز رایج است. GPO های تعریف کننده پیکربندی لپ‌تاپ‌ها و دسک‌تاپ‌ها به OU های مربوطه پیوند می‌شوند.

وقتی سازمانی مدیریت غیرمتمرکز و مبتنی بر سایت دارد و می‌خواهد پیکربندی مجزا برای لپ‌تاپ‌ها و دسک‌تاپ‌هایش داشته باشد ما با معمایی روبرو می‌شویم. آیا باید OU کلاینت‌ها را بر اساس منطقه تقسیم کرده و سپس آن‌ها را به دو قسمت لپ‌تاپ و دسک‌تاپ تقسیم کنیم و یا OU کلاینت‌ها را به لپ‌تاپ و دسک‌تاپ تقسیم کرده و بر اساس منطقه تقسیم بندی را کامل کنیم؟ دو حالت در شکل ۲- ۵ شرح داده شده است. به دلیل اینکه در طرح سمت چپ واگذاری اختیارات مدیریتی روی OU ها بر اساس منطقه جغرافیایی ساده‌تر انجام می‌شود این مدل بهتر از مدل سمت راست است.



شکل ۲- ۵ انواع طراحی OU

واگذاری اختیار ساخت اشیاء کامپیوتر

به طور پیش‌فرض گروههای Enterprise Admins، Domain Admins، Administrators و Account Operators مجوز ساخت شیء کامپیوتر در OU جدید را دارند. به هر حال همان‌طوریکه در فصل ۴ بحث شد توصیه می‌شود عضویت گروه‌های سه گانه فوق به شدت محدود شود و نیز مدیران شبکه عضو گروه Account Operators نشوند.

در عوض به مدیران یا کارکنان پشتیبانی مربوطه مجوز ساخت شیء کامپیوتر داده می‌شود. مجوز مورد نیاز برای ساخت شیء کامپیوتر Create Computer Object است. این مجوز به اعضاء گروه نسبت به یک OU داده می‌شود و به اعضاء گروه اجازه می‌دهد در آن OU شیء کامپیوتر بسازند. مثلا ممکن است بخواهیم به تیم پشتیبانی مجوز ساخت شیء کامپیوتر در OU کلاینت و به مدیران فایل سرورها مجوز ساخت شیء کامپیوتر در OU سرور را بدهیم

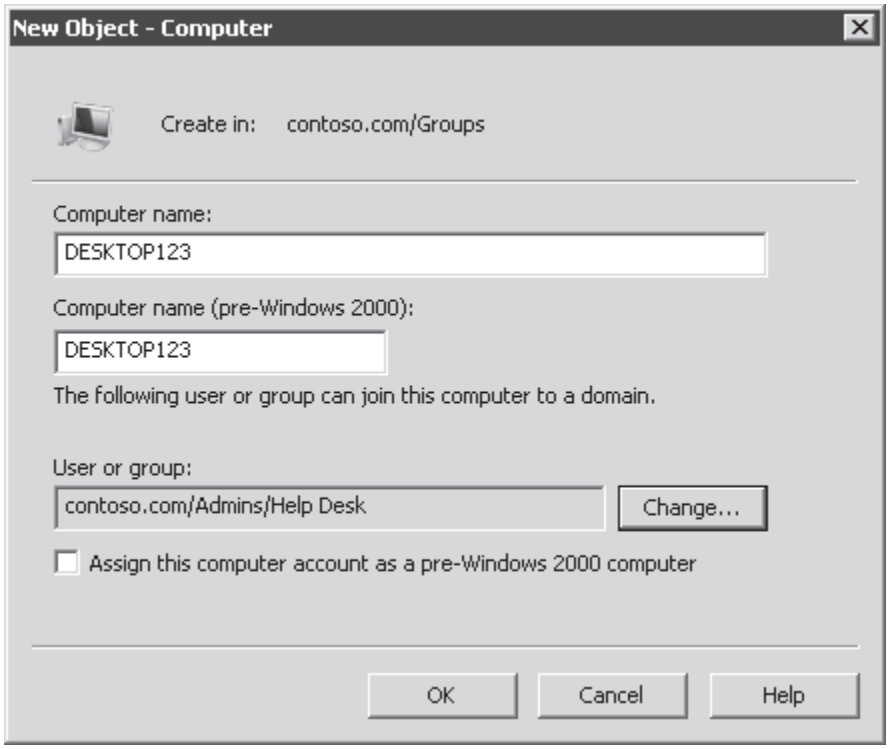
ساخت حساب کامپیوتر با روش Prestaging

پس از گرفتن مجوز ساخت شیء کامپیوتر، روی OU کلیک راست کرده و از منوی New گزینه Computers را انتخاب می‌کنیم. کادر محاوره‌ای New Object – Computer مانند شکل ۳- ۵ ظاهر می‌شود.

طبق قواعد نام گذاری سازمان نام کامپیوتر را وارد می‌کنیم و کاربر یا گروهی که اجازه دارد کامپیوتر را با این حساب join دامنه کند انتخاب می‌کنیم. نام‌های وارد شده برای Computer Name و Computer Name (Pre-Windows 2000) باید مشابه باشند. به ندرت می‌توان توجیهی برای متفاوت بودن دو نام پیدا کرد.

نکته ویزارد New Object – Computer دسترسی بیش از نیاز اعطاء می‌کند

کاربر یا گروهی که در این ویزارد مجوز می‌گیرند قابلیت تغییر شیء کامپیوتر را نیز خواهند داشت. برای راهنمایی در مورد اعطاء حداقل مجوز برای join کردن کامپیوتر به دامنه به منبع Windows Administration Resource Kit: Productivity Solutions for IT Professionals نوشته دن هلم (انتشارات مایکروسافت 2008) مراجعه کنید.



شکل ۳- ۵ کادر محاوره‌ای New Object – Computer

پروسه ساخت حساب کامپیوتر قبل از اینکه کامپیوتر عضو دامنه شود Prestaging نام دارد. مزیت این روش در این است که حساب در OU مورد نظر ساخته می‌شود و بنابراین بر اساس سیاست امنیتی تعریف شده توسط ACL مربوط به OU مجوز دریافت می‌کند و قبل از این که عضو دامنه شود در حوزه GPOs مربوط به OU قرار می‌گیرد. این روش به دلایل عنوان شده در بخش "اهمیت افزودن شیء کامپیوتر به روش Prestaging" اکیدا توصیه می‌شود

Join کردن کامپیوتر به دامنه

با روش Prestaging دو نیاز اول عضویت کامپیوتر در دامنه مرتفع می‌شود. شیء کامپیوتر ایجاد می‌شود و مشخص می‌شود چه کسی مجوز دارد کامپیوتر را عضو دامنه کند. حالا یک کاربر عضو گروه Administrators همین کامپیوتر می‌تواند کامپیوتر را با وارد کردن اعتبار دامنه‌ای مورد نیاز به دامنه join کند. برای اینکه کامپیوتر عضو دامنه شود مراحل زیر باید انجام شود:

۱. با اعتبار مدیریتی سیستم به کامپیوتر وارد می‌شویم.

فقط کاربران عضو گروه Administrators سیستم می‌توانند عضویت کامپیوتر را بین دامنه و workgroup تغییر دهند.

۲. با یکی از روش‌های زیر پنجره System Properties را باز می‌کنیم:

- در ویندوزهای XP و 2003 : روی Computer کلیک راست کرده و Properties را انتخاب می‌کنیم.
- در ویندوزهای ویستا و سرور 2008 : روی Computer کلیک راست و انتخاب Properties و سپس در بخش Computer Name, Domain, And Workgroup Settings روی Change Settings کلیک می‌کنیم.

۳. زبانه Computer Name را کلیک می‌کنیم.

۴. دکمه Change را کلیک می‌کنیم.

۵. در زیر Member Of گزینه Domain را انتخاب می‌کنیم.

۶. نام دامنه‌ای که قرار است کامپیوتر عضو آن شود تایپ می‌کنیم.

نکته از نام کامل DNS دامنه استفاده کنید
نه تنها این کار صحیح‌تر بوده و احتمال موفقیت بیشتر است بلکه در صورت عدم موفقیت مشکل احتمالی DNS را به ما گوشزد می‌کند.

۷. روی دکمه OK کلیک می‌کنیم.

۸. ویندوز اعتبار(credential) مورد نیاز برای انجام این کار را درخواست می‌کند.

دامنه چک می‌کند که شیء کامپیوتری با این نام قبلا ساخته نشده باشد. یکی از سه حالت زیر اتفاق می‌افتد:

- اگر شیء موجود باشد یعنی کامپیوتری با آن نام قبلا عضو دامنه شده باشد پیغام خطایی ظاهر می‌شود و اجازه عضویت صادر نمی‌شود.

- اگر شیء با روش Prestage ایجاد شده باشد یعنی کامپیوتری با این نام عضو شبکه نشده باشد دامنه اعتبار کاربری را که وارد می‌کنیم چک می‌کند تا ببیند مجوز join کردن کامپیوتر را دارد یا نه. این مجوزها در بخش "ایجاد حساب کامپیوتر با روش Prestaging" بررسی می‌شود.

- اگر حساب کامپیوتر ساخته نشده باشد ویندوز مجوزهای ما را برای ساخت شیء کامپیوتر جدید در container کامپیوتر پیش فرض بررسی می‌کند. اگر مجوزها کافی بود شیء با نام کامپیوتر ساخته می‌شود. این روش join کردن به منظور پشتیبانی از تکنولوژی‌های قدیمی‌تر وجود دارد و توصیه نمی‌شود. پیشنهاد می‌شود برای join کردن کامپیوتر از روش Prestaging استفاده شود که در بخش بعدی به جزئیات آن پرداخته می‌شود.

پذیرفته شدن شیء کامپیوتر در Active Directory به معنی عضویت کامپیوتر در دامنه است. SID کامپیوتر توسط خود کامپیوتر طوری پیکربندی می‌شود که با SID حساب کامپیوتر در دامنه هم‌خوانی داشته باشد و کلمه عبوری برای ارتباط با دامنه ساخته می‌شود. سپس کامپیوتر وظایف دیگر مربوط به عضویت دامنه را انجام می‌دهد. گروه Domain Admins به گروه Administrators محلی افزوده شده و گروه Domain Users به گروه Users محلی اضافه می‌شوند.

۹. پیغام راه اندازی مجدد کامپیوتر ظاهر می‌شود. OK می‌کنیم تا کادر پیغام بسته شود.

۱۰. روی Close (در ویندوز ویستا) یا OK (در ویندوز XP) کلیک می‌کنیم تا کادر محاوره‌ای System Properties بسته شود.

۱۱. دوباره پیغام راه اندازی مجدد ظاهر می‌شود. پس از راه اندازی مجدد سیستم به طور کامل عضو دامنه شده و می‌توان با حساب کاربری دامنه وارد سیستم شد.

دستور Netdom.exe به ما امکان می‌دهد از طریق خط فرمان کامپیوتر را عضو دامنه کنیم. شکل ساده فرمان به صورت زیر است:

```
Netdom join MachinName /Domain:DomainName [/OU:"DN of OU"]
[/Usero:LocalUsername] [/Passwordo:{LocalPassword|*} ]
[/UserD:DomainUsername] [/PasswordD:{DomainPassword|*} ]
[/SecurePasswordPrompt] [/REBoot[:TimeInSeconds]]
```

استفاده از این دستور برای join کردن کامپیوتر به دامنه توصیه می‌شود به این دلیل که اولا درکنار این کار می‌توان عملیات دیگری نیز به اسکریپت اضافه کرد. دوم دستور Netdom.exe از راه دور نیز قابل استفاده است سوم این دستور امکان تعیین OU را برای شیء کامپیوتر فراهم می‌کند. از نام پارامترهای دستور براحتی می‌توان کارکردشان را حدث زد. UserO و PasswordO اعتبار عضو گروه Administrators محلی کامپیوتر workgroup هستند. تعیین * برای کلمه عبور دستور Netdom را وادار می‌کند هنگام اجرا کلمه عبور را دریافت کند. UserD و PasswordD اعتباری از دامنه می‌باشد که دو حالت دارد. اول این که اگر شیء کامپیوتر با

روش Prestaging ساخته نشده باشد این اعتبار باید دارای مجوز ساخت شیء کامپیوتر در دامنه باشد. حالت دوم این است که شیء با روش Prestaging ایجاد شده باشد پس فقط کافی است اعتبار وارد شده مجوز join کردن یک کامپیوتر Prestaged را داشته باشد. پارامتر REBoot باعث راه اندازی مجدد سیستم پس از اتمام کار می‌شود. زمان پیش فرض ۳۰ ثانیه است. وقتی برای PasswordO یا PasswordD کاراکتر "*" تعیین شده باشد پارامتر SecurePasswordPrompt صفحه‌ای را برای ورود کلمه عبور ظاهر می‌کند

اهمیت join کردن اشیاء کامپیوتر با روش Prestaging

بهترین کار استفاده از روش Prestaging قبل از عضویت کامپیوتر به دامنه است. متاسفانه ویندوز اجازه عضویت کامپیوتر را بدون استفاده از این روش می‌دهد. می‌توانیم با کاربر دارای اعتبار مدیریتی یه یک کامپیوتر عضو workgroup وارد شده و عضویت آن را به دامنه تغییر دهیم. سپس در صورت نیاز ویندوز یک شیء کامپیوتر در container پیش فرض کامپیوتر ساخته و مجوز عضویت کامپیوتر به دامنه را اعطاء کرده و سیستم را عضو دامنه می‌کند.

سه مشکل در این رفتار ویندوز مشاهده می‌شود. اول حساب کامپیوتر به طور خودکار در container پیش فرض کامپیوتر ساخته می‌شود که در بسیاری از موارد جایگاه نهایی آن نیست. دوم باید کامپیوتر را از این محل به OU خود منتقل کنیم که یک مرحله اضافی بوده و اغلب فراموش می‌شود. سوم هر کاربری می‌تواند کامپیوتر را عضو دامنه کند چون هیچ مجوز مدیریتی در سطح دامنه مورد نیاز نیست. چون شیء کامپیوتر یک واحد امنیتی محسوب می‌شود و چون سازنده شیء کامپیوتر صاحب شیء است و می‌تواند خصیصه‌های خود را تغییر دهد این خود نفوذپذیری امنیتی بالقوه به شمار می‌آید. بخش بعدی این معایب را با جزئیات بیشتر توصیف می‌کند.

پیکربندی container پیش فرض کامپیوتر

وقتی کامپیوتری عضو دامنه می‌شود و شیء کامپیوتر نیز قبلا در Active Directory حضور ندارد ویندوز یک حساب کامپیوتر در container پیش فرض کامپیوتر می‌سازد که نام این container ، Computers می‌باشد (CN=Computers,DC=domain).

مشکل این است که اگر از روش‌های بهینه برای مدیریت اشیاء کامپیوتر در OU مشخص به طور مجزا استفاده شده باشد این روش، طراحی OU را بهم می‌زند. به علاوه ممکن است GPO ها را به این OU ها پیوند داده باشیم. بنابراین اگر شیء کامپیوتر جدید در بیرون از این OU ها ساخته شود پیکربندی آن که از container والد به ارث می‌رسد با چیزی که ما در نظر گرفته‌ایم متفاوت می‌شود. پس باید به خاطر داشته باشیم که شیء را از محل پیش فرض به OU مناسب منتقل کنیم.

برای جلوگیری از بروز این مشکل دو کار پیشنهاد می‌شود. اول باید سعی کنیم از روش Prestaging استفاده کنیم. اگر یک شیء با روش Prestaging در OU مناسب ساخته شود پس از عضویت دامنه، پیکربندی مناسب خود را دریافت خواهد کرد. دوم برای کاهش تاثیرات منفی عضویت شیء کامپیوتر به دامنه بدون Prestaging بهتر است container پیش فرض کامپیوتر را طوری تغییر دهیم که شیء در OU مناسب ساخته شود. برای مثال اگر OU با نام Clients داریم می‌توانیم ویندوز را مجبور کنیم که اشیاء کامپیوتر را در این OU بسازد.

دستور Redircmp.exe که روی DC ها قابل اجراست به شکل زیر مسیر ساخت اشیاء کامپیوتر را تغییر می‌دهد:

Redircmp “DN of OU for new computer objects”

حالا اگر کامپیوتری بدون Prestaging عضو دامنه شود شیء آن در OU مناسب که در دستور مشخص شده ساخته می‌شود.

تغییر محل container پیش فرض کاربر

همین روش برای ساخت کاربر هم صادق است. به طور پیش فرض وقتی کاربری با روشی که مشخص کننده OU کاربر نیست ساخته می‌شود شیء کاربر در container پیش فرض کاربر ایجاد می‌شود.(CN=Users,DC=domain). دستور Redirusr.exe که روی DC قابل اجراست می‌تواند container پیش فرض را به یک OU مشخص تغییر دهد. این دستور نیز مانند دستور Redircmp.exe یک پارامتر واحد می‌گیرد: DN مربوط به OU مقصد.

محدود کردن کاربران در ساخت اشیاء کامپیوتر

وقتی از روش Prestaging در ساخت شیء استفاده می‌شود مجوزهای حساب مشخص می‌کند چه کسی اجازه دارد کامپیوتر را عضو دامنه کند. وقتی از Prestaging استفاده نمی‌شود ویندوز به طور پیش فرض به همه کاربران گروه Authenticated Users اجازه ساخت شیء کامپیوتر را در container پیش فرض کامپیوتر می‌دهد. در حقیقت ویندوز به این کاربران اجازه ساخت حداکثر ۱۰ شیء

را می‌دهد. به طور پیش فرض سازنده یک شیء مجوز join کردن آن را به دامنه خواهد داشت. از طریق این مکانیزم است که کاربران Authenticated می‌توانند تا ۱۰ کامپیوتر را بدون هیچ مجوز اضافه‌ای عضو دامنه کنند.
سهمیه ۱۰ تایی توسط خصیصه ms-DS-MachineAccountQuota دامنه تعیین شده است. این خصیصه بدون هیچ پرسشی اجازه join کردن کامپیوتر را به کاربر Authenticated می‌دهد. این یک مشکل امنیتی است چرا که کامپیوترها واحدهای امنیتی هستند و سازنده یک واحد امنیتی اجازه مدیریت آن خصیصه کامپیوتر را دارد. این سهمیه مانند این است که یک کاربر دامنه بدون هیچ کنترلی بتواند ۱۰ کاربر بسازد.
اکیدا توصیه می‌شود این نقیصه را با تغییر خصیصه ms-DS-MachineAccountQuota به شکل زیر برطرف کنیم:

۱. از پوشه Administrative Tools گزینه ADSI Edit را باز می‌کنیم.

۲. روی آن کلیک راست کرده و Connect To را انتخاب می‌کنیم.

۳. در بخش Connection Point گزینه Select A Well Known Naming Context و از لیست پایین افتادنی گزینه Default Naming Context را انتخاب می‌کنیم.

۴. OK را کلیک می‌کنیم.

۵. گره Default Naming Context را باز می‌کنیم.

۶. روی پوشه dc=contoso,dc=com کلیک راست کرده و Properties را انتخاب می‌کنیم.

۷. ms-DS-MachineAccountQuota را انتخاب کرده و Edit را کلیک می‌کنیم.

۸. عدد 0 را تایپ می‌کنیم.

۹. OK می‌کنیم.

گروه Authenticated Users حق افزودن کامپیوتر را هم به دامنه دارند ولی تغییر مقدار پیش فرض ms-DS-MachineAccountQuota این حق را هم از آن‌ها می‌گیرید
پس از تغییر مقدار فوق به صفر می‌توان مطمئن بود که هیچ کاربری بدون دریافت مجوز نمی‌تواند شیء کامپیوتر Prestaged را عضو دامنه کند یا یک شیء جدید ساخته و آنرا عضو دامنه کند.
پس از بر برطرف کردن این حفره امنیتی باید به کاربر یا گروه مشخص اجازه ساخت اشیاء را در OU های مناسب اعطاء کنیم در غیر این صورت پیغامی مشابه شکل ۴- ۵ ظاهر می‌شود.
شکل ۴- ۵

تمرینات ساخت شیء کامپیوتر و join کردن به دامنه

در این تمرینات بهترین راهها برای ساخت شیء کامپیوتر و Join به دامنه بررسی می‌شود. کار با ایجاد ساختار OU برای نگهداری اشیاء کامپیوتر جدید شروع می‌شود. سپس اشیاء کامپیوتر به روش prestaging ساخته شده و برای join کردن کامپیوترها مجوز لازم اعطاء می‌شود. مجوز ساخت شیء کامپیوتر با استفاده از دستور Dsacls.exe اعطاء می‌شود و container پیش فرض کامپیوتر تغییر می‌کند. قبل از شروع تمرینات باید اشیاء زیر در دامنه contoso.com ساخته شده باشند:

- OU سطح اول با نام Admins با OU فرعی با نام Groups
- یک گروه امنیتی global در Admins\Groups OU با نام Server Admins.

- یک گروه امنیتی global در Admins\Groups OU با نام Help Desk.
- OU سطح اول با نام People.
- یک کاربر در People OU با نام Jeff Ford و عضو گروههای Domain Users و Server Admins باشد.
- یک کاربر در People OU با نام Linda Mitchell و عضو گروههای Domain Users و Help Desk باشد.

همچنین باید گروه Domain Users عضو گروه Print Operators باشد که در Builtin container وجود دارد. این باعث می‌شود همه کاربران در تمرینات بتوانند به SERVER01 که domain controller است وارد شوند. این کار برای اجرای تمرینات انجام می‌شود و در دنیای واقعی نباید اتفاق بیافتد.

تمرین ۱ ساخت OU برای اشیاء کامپیوتر کلاینت و سرور

قبل از ساخت حساب‌های کامپیوتر باید OU ها را بسازیم. در این تمرین برای اشیاء سرور و کلاینت OU می‌سازیم.

۱. با کاربر Administrator به SERVER01 وارد می‌شویم.
۲. ابزار Active Directory Users And Computers را باز کرده و گره دامنه را باز می‌کنیم.
۳. روی دامنه contoso.com کلیک راست می‌کنیم و New و سپس Organizational Unit را انتخاب می‌کنیم.
۴. تایپ می‌کنیم Clients و OK می‌کنیم.
۵. روی دامنه contoso.com کلیک راست کرده و New و سپس Organizational Unit را انتخاب می‌کنیم.
۶. تایپ می‌کنیم Servers و OK می‌کنیم.

تمرین ۲ ساخت اشیاء کامپیوتر

پس از ساخت OU برای اشیاء کامپیوتر می‌توان اشیاء کامپیوتر را به روش Prestaging ایجاد کرده و به دامنه join کرد. در این تمرین با این روش یک شیء برای کلاینت و یک شیء برای سرور ساخته می‌شود و توانایی join کردن کامپیوتر اعطاء می‌گردد.

۱. روی Clients OU کلیک راست کرده و New و سپس Computer را انتخاب می‌کنیم.
۲. کادر محاوره‌ای New Object – Computer طبق شکل ۳- ۵ ظاهر می‌شود.
۳. نام کامپیوتر را در کادر Computer Name تایپ می‌کنیم : DESKTOP101
۴. دکمه Change نزدیک کادر User Or Group را کلیک می‌کنیم.
۵. در کادر محاوره‌ای Select User Or Group که ظاهر می‌شود نام کاربر یا گروهی که باید اجازه join کردن کامپیوتر به دامنه را داشته باشد تایپ می‌کنیم در این تمرین یعنی Help Desk سپس OK می‌کنیم.
۶. OK می‌کنیم تا کادر بسته شود.
۷. روی Servers OU کلیک راست کرده New و سپس Computer را انتخاب می‌کنیم.
۸. کادر محاوره‌ای New Object – Computer طبق شکل ۳- ۵ ظاهر می‌شود.

۹. در کادر Computer Name نام کامپیوتر را تایپ می‌کنیم.

۱۰. دکمه Change کنار کادر User Or Group را کلیک می‌کنیم.

۱۱. در کادر محاوره‌ای Select User Or Group نام کاربر یا گروهی که باید اجازه join کردن کامپیوتر به دامنه را داشته باشد وارد می‌کنیم در این تمرین یعنی Server Admins و OK می‌کنیم.

۱۲. OK می‌کنیم تا کادر بسته شود.

تمرین ۳ واگذاری مجوز ساخت اشیاء کامپیوتر

همان طوری که در تمرین ۲ دیدیم برای ساخت اشیاء کامپیوتر نیاز به مجوز داریم. کاربر Administrator چنین مجوزی را دارد ولی شاید بخواهیم این توانایی را به گروههای دیگر واگذار کنیم. در این تمرین حداقل دسترسی برای ساخت شیء کامپیوتر اعطاء می‌شود.

۱. ابزار Active Directory Users And Computers را روی Server01 باز می‌کنیم.

۲. منوی View را باز کرده و گزینه Advanced Features را علامت دار می‌کنیم.

۳. روی Clients کلیک راست کرده و Properties را انتخاب می‌کنیم.

۴. زبانه Security را کلیک می‌کنیم.

۵. روی Advanced کلیک می‌کنیم.

۶. Add را کلیک می‌کنیم.

۷. Help Desk را تایپ کرده و OK می‌کنیم.

۸. زبانه Object را باز می‌کنیم.

۹. در لیست پایین افتادنی Apply To گزینه This Object And All Descendant Objects را انتخاب می‌کنیم.

۱۰. در لیست Permissions کادر Allow گزینه Create Computer Objects را علامت می‌زنیم.

۱۱. سه بار کلید OK را می‌زنیم تا کادرها بسته شوند.

تمرین ۴ تغییر container پیش فرض کامپیوتر

پیشنهاد می‌شود container پیش فرض کامپیوتر را تغییر دهیم تا اشیاء کامپیوتر جدید که با روش prestaging ایجاد نمی‌شوند در محل برنامه‌ریزی شده ساخته شوند. در این تمرین از دستور Redircmp.exe برای تغییر container پیش فرض کامپیوتر استفاده می‌شود.

۱. پنجره خط فرمان را روی SERVER01 باز می‌کنیم.

۲. دستور زیر را تایپ کرده و Enter را می‌زنیم:

```
Redircmp  “OU=Clients,DC=contoso,DC=com”
```

تمرین ۵ اختیاری **join کردن کامپیوتر به دامنه**

در این تمرین یک کامپیوتر را به دامنه join می‌کنیم. برای این کار سیستم دومی نیاز داریم که سروری با نام SERVER02 با ویندوز سرور 2008 یا کلاینت با نام DESKTOP101 با ویندوز ویستا می‌باشد. اگر کامپیوتر نام دیگری دارد یا باید آن را معادل شیء کامپیوتر در OU تغییر دهیم و یا یک شیء کامپیوتر با نام آن در OU بسازیم.

۱. با یک کاربر عضو گروه Administrators محلی به کامپیوتر workgroup وارد می‌شویم.

۲. با یکی از روش‌های زیر پنجره properties سیستم را باز می‌کنیم:

- از کنترل پنل System را باز می‌کنیم
- روی Computer در منوی start کلیک راست می‌کنیم
- کلید Windows و Pause را فشار می‌دهیم.

۳. در بخش Computer Name,Domain, And Workgroup Settings کلید Change Settins را می‌زنیم. سپس کلید Continue را می‌زنیم.

۴. زبانه Computer Name را کلیک می‌کنیم.

۵. کلید Change را می‌زنیم.

۶. در قسمت Member Of گزینه Domain را انتخاب می‌کنیم.

۷. نام Domain را تایپ می‌کنیم. در این جا contoso.com دامنه ماست.

۸. OK می‌کنیم.

کامپیوتر تلاش خود را برای ارتباط با دامنه شروع می‌کند. پنجره‌ای برای ورود مشخصات کاربر دامنه باز می‌شود.

۹. مشخصات کاربر دامنه را وارد و OK می‌کنیم.

- اگر SERVER02 را به دامنه join می‌کنیم مشخصات کاربر Jeff Ford را وارد می‌کنیم که عضو گروه Server Admins است.
- اگر DESKTOP101 را به دامنه join می‌کنیم مشخصات کاربر Linda Mitchell را وارد می‌کنیم که عضو گروه Help Desk است.

۱۰. حالا OK می‌کنیم تا سیستم راه اندازی مجدد شود.

۱۱. کلید Close را می‌زنیم تا کادر System Properties بسته شود.

۱۲. دوباره پیغام راه اندازی مجدد ظاهر می‌شود.

خلاصه درس

- امکان پیوند اشیاء Group Policy به Computers Container یا ساخت OU های فرعی در آنها وجود ندارد. برای شکل گیری مدل مدیریتی سازمان، باید ساختار OU مناسبی پیاده سازی کرد.

- همیشه با روش Prestaging اشیاء را بسازید یعنی شیء کامپیوتر قبل از join سیستم به دامنه در Active Directory ساخته شود.
- برای join کردن کامپیوتر کاربر، باید عضو گروه Administrators محلی سیستم باشد، شیء کامپیوتر باید ساخته شده باشد و باید از اعتبار کاربر دامنه که مجاز به join کردن است استفاده شود.
- برای تغییر container پیش فرض کامپیوتر به یک OU از دستور Redircmp.exe استفاده می‌شود.
- ms-DS-MachineAccountQuota به همه کاربران گروه Authenticated Users اجازه join کردن تا سقف ۱۰ سیستم را می‌دهد. ویندوز اشیاء کامپیوتر را در container پیش فرض کامپیوتر می‌سازد. این سهمیه را به صفر کاهش دهید تا کاربران عادی نتوانند شیء بسازند.

سئوالات پایان درس

۱. می‌خواهیم همه حساب‌های کامپیوتر جدید هنگام join در Clients OU قرار گیرند. از کدام دستور باید استفاده کنیم؟

A. Dsmove

B. Move-Item

C. Netdom

D. Redircmp

۲. می‌خواهیم اجازه join کردن کامپیوترها را از کاربران عادی بگیریم. چه باید بکنیم؟

A. سهمیه ms-DS-MachineAccountQuota را به صفر کاهش دهیم.

B. سهمیه ms-DS-DefaultQuota را به صفر کاهش دهیم.

C. حق Add Workstations To Domain را از گروه Authenticated Users بگیریم.

D. در دامنه مجوز گروه Authenticated Users را برای Create Computer Objects ، deny کنیم.

۳. می‌خواهیم کامپیوتر راه دوری را join کنیم. از کدام دستور استفاده می‌کنیم؟

A. Dsadd.exe

B. Netdom.exe

C. Dctest.exe

D. System.cpl

درس ۲: خودکارسازی ساخت اشیاء کامپیوتر

وقتی قرار است دهها یا صدها شیء کامپیوتر در یک زمان ساخته شود استفاده از روش‌های مطرح شده در درس ۱ خیلی ملال آور خواهد بود. دستوراتی مانند CSVDE، LDIFDE و Dsadd درکنار اسکریپت‌های PowerShell ویندوز و VBScript می‌تواند ساخت اشیاء کامپیوتر را خودکار کند یا از جایی به جای دیگر منتقل کند. اسکریپت‌ها همچنین به ما امکان می‌دهند اشیاء کامپیوتر را بر اساس قوانین نام‌گذاری کنیم که این یعنی اجرای قواعد کاری . در این درس انتقال، خودکارسازی اشیاء کامپیوتر را یاد می‌گیریم. ما دانش خود را در این زمینه در ادامه مطالب مطرح شده در درس‌های ۱و۲ از فصل ۳ که پیش‌نیاز این درس هستند ارتقا می‌دهیم.

بعد از این درس یاد می‌گیریم:

- از دستورات CSVDE و LDIFDE برای انتقال اشیاء کامپیوتر استفاده کنیم.
- با دستور Dsadd شیء کامپیوتر بسازیم.
- با دستور Netdom شیء کامپیوتر بسازیم.
- با PowerShell ویندوز شیء کامپیوتر بسازیم.
- با VBScript شیء کامپیوتر بسازیم.

زمان تقریبی : ۳۰ دقیقه

انتقال اشیاء کامپیوتر با دستور CSVDE

در درس ۱ از فصل ۳ با دستور CSVDE آشنا شدیم. این دستور یک ابزار خط فرمان است که اشیاء Active Directory را از یک فایل متنی comma-delimited (همچنین فایل متنی comma-separated یا فایل csv. نامیده می‌شود) می‌خواند یا به آن منتقل می‌کند. شکل ساده دستور به صورت زیر است:

Csvde [-i] [-f “Filename”] [-k]

پارامتر i– حالت انتقال را مشخص می‌کند. حالت پیش فرض انتقال به فایل است. پارامتر f– نام فایل را برای انتقال مشخص می‌کند. پارامتر k– هنگام عملیات انتقال کاربرد دارد بدین ترتیب که در صورت بروز خطاهایی از قبیل Already Exists، Constraint Vilolation یا Attribute Or Value Already Exists کار ادامه پیدا می‌کند.

فایل‌های comma-delimited با ابزارهایی از قبیل Notepad و Excel قابل ساخت، تغییر و مشاهده است. خط اول این فایل خصیصه‌ها را با نام‌های استاندارد LDAP مشخص می‌کند. هر شیء در یک خط درج می‌شود و باید دقیقا شامل خصیصه‌های مشخص شده در خط اول باشد. یک فایل نمونه Excel در شکل ۵- ۵ نشان داده شده است.

هنگام انتقال اشیاء کامپیوتر از وجود خصیصه userAccountControl و مقدار 4096 برای آن مطمئن شوید. این خصیصه تضمین می‌کند که کامپیوتر قادر به join شدن است. همچنین مطمئن شوید که نام کاربری pre-Windows 2000 (خصیصه sAMAccountName) را که انتهای آن علامت "$" دارد اضافه شده است.

	A	B	C	D	E
1	DN	objectClass	name	userAccountControl	sAMAccountName
2	CN=DESKTOP103,OU=Clients,DC=contoso,DC=com	computer	DESKTOP103	4096	DESKTOP103$
3	CN=DESKTOP104,OU=Clients,DC=contoso,DC=com	computer	DESKTOP104	4096	DESKTOP104$
4	CN=SERVER02,OU=Servers,DC=contoso,DC=com	computer	SERVER02	4096	SERVER02$

شکل ۵- ۵ یک فایل csv. که در Excel باز شده و سه شیء کامپیوتر را ایجاد می‌کند.

اطلاعات بیشتر در فصل ۳ و ۴ از دستور CSVDE برای انتقال کاربران و گروهها استفاده کردیم. برای اطلاعات بیشتر شامل جزئیات پارامترها و انتقال اشیاء دایرکتوری تایپ کنید csvde/? یا Help and Support Center ویندوز سرور 2008 را جستجو کنید.

انتقال اشیاء کامپیوتر با دستور LDIFDE

در فصل ۳ دستور Ldifde.exe نیز بررسی شد که داده را از فایل‌های با فرمت LDIF منتقل می‌کرد. این فایل‌ها فایل‌های متنی هستند که در آن عملیات مختلف در بلوک‌های مستقل با یک خط خالی فاصله قرار می‌گیرند. هر عملیات با خصیصه DN شیء مقصد شروع می‌شود. خط بعدی، ChangeType ، نوع عملیات را مشخص می‌کند: Add، modify یا delete
لیست زیر یک فایل LDIF را که دو شیء کامپیوتر ایجاد می‌کند نشان می‌دهد:

```
Dn: CN=SERVER10,OU=Servers,DC=contoso,DC=com
Changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
objectClass: computer
cn: SERVER10
userAccountControl: 4096
sMAccountName: SERVER10$

Dn: CN=SERVER11,OU=Servers,DC=contoso,DC=com
Changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
objectClass: computer
cn: SERVER11
userAccountControl: 4096
sMAccountName: SERVER11$
```

شکل ظاهری دستور LDIFDE شبیه دستور CSVDE است:

```
Ldifde [-i] [-f “Filename”] [-k]
```

به صورت پیش فرض دستور LDIFDE در حالت "انتقال به فایل" کار می‌کند یعنی اشیاء را از Active Directory به یک فایل کپی می‌کند. پارامتر i– حالت آن را به "انتقال از فایل" تغییر می‌دهد. ما باید با پارامتر f– نام فایل را تعیین کنیم. پارامتر k– نیز در هنگام بروز خطا اجازه توقف عملیات را از فرمان می‌گیرد.
نکته امتحانی به خاطر داشته باشید که حالت پیش فرض دستورات CSVDE و LDIFDE "انتقال به فایل" است. ما باید از پارامتر i– برای تغییر حالت دستور به "انتقال از فایل" استفاده کنیم.

ساخت اشیاء کامپیوتر با دستور Dsadd

دستور Dsadd را در فصل‌های قبلی برای ساخت اشیاء در Active Directory به کار می‌بردیم. برای ساخت شیء کامپیوتر به سادگی تایپ می‌کنیم dsadd computer ComputerDN در حالی که ComputerDN به DN کامپیوتر اشاره دارد مانند:
CN=Desktop123,OU=Desktop,DC=contoso,DC=com
اگر DN شیء دارای فاصله باشد کل DN باید در گیومه قرار گیرد. پارامتر ComputerDN می‌تواند شامل DN بیش از یک شیء باشد. در این صورت ورود پارامترها به یکی از روش‌های زیر باید انجام شود:

- با انتقال لیست DN ها از دستور دیگری مانند Dsquery
- با تایپ DN در خط فرمان با درج فاصله خالی بین آنها
- با خالی گذاشتن پارامتر DN دستور و ورود DN ها هر بار یکی و پس از هر کدام کلید Enter را می‌زنیم. بعد از ورود همه Dn ها کلیدهای Ctrl+Z و Enter را می‌زنیم.

دستور Dsadd computer پارامترهای دیگری هم بعد از پارامتر DN دارد که می‌توانیم از آنها استفاده کنیم:

- -samid SAMName
- -desc Description
- -loc Location

ساخت شیء کامپیوتر با دستور Netdom

این دستور قادر به اجرای وظایف متعددی در دامنه می‌باشد. در درس ۱ یاد گرفتیم از Netdom برای join کردن کامپیوتر به دامنه استفاده کنیم. از این دستور همچنین می‌توان برای ساخت شیء کامپیوتر به شکل زیر استفاده کرد:

```
Netdom add ComputerName /domain:DomainName [/ou:OUDN]
[/userd:User /PasswordD:Password]
```

این دستور برای کامپیوتری که نامش در پارامتر ComputerName جای می‌گیرد در دامنه حساب ایجاد می‌کند. اعتبار مورد نیاز برای این کار نیز در پارامترهای UserD و PasswordD مشخص می‌شود. پارامتر OU باعث ساخت شیء در OU مشخص شده توسط OUDN می‌شود. اگر OUDN مشخص نشود شیء در container پیش فرض کامپیوتر ساخته می‌شود. اعتبار کاربر باید مجوز ساخت شیء کامپیوتر را داشته باشد.

ساخت شیء کامپیوتر با PowerShell ویندوز

در فصل ۳ PowerShell ویندوز معرفی شد. یک shell جدید مدیریتی و خودکارسازی در ویندوز. در این درس یاد گرفتیم چطور کاربر بسازیم. مانند شیء کاربر می‌توان شیء کامپیوتر هم ساخت. مراحل کلی ساخت شیء کامپیوتر به ترتیب زیر است:

۱. به container (OU) که می‌خواهیم در آن شیء بسازیم متصل می‌شویم.

۲. از متد Create برای ساخت شیء کامپیوتر استفاده می‌کنیم.

۳. خصیصه‌های اجباری را مقدار دهی می‌کنیم.

۴. تغییرات را اعمال می‌کنیم.

برای اتصال به یک OU در خط فرمان PowerShell تایپ می‌کنیم:

```
$objOU=[ADSI]"LDAP://DN of OU"
```

این دستور یک مرجع شیء در متغیر $objOU می‌سازد که نماینده OU خواهد بود. حالا می‌توانیم متد مربوطه را فراخوانی کنیم که از متغیر $objOU استفاده کند. برای ساخت شیء از متد Create به شکل زیر استفاده می‌کنیم:

```
$objComputer=$objOU.Create("computer","CN=Computer CN")
```

سپس باید دو خصیصه را پیکربندی کنیم. اول نام کاربری pre-Windows 2000 (خصیصه sAMAccountName) که نام کامپیوتر با علامت $ در انتهای آن می‌باشد. دوم خصیصه userAccountControl است که باید با مقدار 4096 (0x1000 در سیستم هگزادسیمال) پر شود. این خصیصه یک سری پرچم است که تک بیتی هستند. این بیت‌ها مشخص می‌کنند که حساب، مربوط به یک عضو دامنه می‌باشد. بدون آن با این حساب کامپیوتر نمی‌تواند به دامنه join شود. برای مقداردهی به این دو خصیصه دستورات زیر را تایپ کنید:

```
$objComputer.Put("sAMAccountName","ComputerName$")
$objComputer.Put("userAccountControl", 4096)
```

دیگر خصیصه‌ها را هم در این جا می‌توان مقداردهی کرد. مثلا خصیصه‌های description یا info. وقتی پیکربندی خصیصه‌ها تمام شد باید تغییرات را با کد زیر اعمال کنیم:

```
$objComputer.SetInfo()
```

انتقال اشیاء کامپیوتر از بانک اطلاعاتی توسط PowerShell ویندوز

در امتحان 70-640 نیازی نیست بدانید که چطور به بانک اطلاعاتی متصل می‌شویم و با استفاده از PowerShell ویندوز شیء کامپیوتر می‌سازیم. این دانش در محیط کاری به کار می‌آید. فرض کنید لیستی از کامپیوترهایی را دریافت کرده‌اید که سازمان خریداری کرده است. حالا باید اشیاء کامپیوتر را برای آنها به روش prestaging بسازید. به راحتی می‌توان با اسکریپت PowerShell ویندوز این کار را انجام داد. با اسکریپت همچنین می‌توان قواعد کاری از جمله استانداردهای نام‌گذاری را اعمال کرد. در این بخش موارد ذکر شده را یاد می‌گیریم.

PowerShell ویندوز می‌تواند به یک منبع داده مانند فایل csv. که در Excel می‌تواند ساخته شود متصل شده و آن را باز کند. برای مثال می‌توان بر حسب لیست ارسالی از فروشنده کامپیوتر شماره اموال را در صفحه Excel درج کرده و فایلی با نام Assets.csv بسازیم.

	A	B
1	**AssetTag**	**Type**
2	A849XD	Desktop
3	D82KE8	Desktop
4	ELW938	Laptop
5	XKD8G0	Laptop
6	93JX9D	Laptop
7	SJ0GJ3	Laptop

شکل ۶- ۵ یک منبع داده ساده Excel از شماره‌های اموال کامپیوتر

فرض کنید می‌خواهیم این کامپیوترها را به دامنه منتقل کنیم و دو قاعده باید رعایت شود. اول لپ‌تاپ‌ها و دسک‌تاپ‌ها در OU های مجزا و زیرمجموعه Clients OU باشند. دوم قواعد نام‌گذاری کامپیوتر به این ترتیب باشد که لپ‌تاپ‌ها دارای پیشوند L و دسک‌تاپ‌ها دارای پیشوند D باشند. برای مثال نام کامپیوتر اول در لیست شکل ۶- ۵ خواهد شد DA849XD . این دو قانون ساده مثالهایی از قواعد نام‌گذاری در حوزه برنامه‌نویسی می‌باشد که در اینجا از آن استفاده می‌شود.

اسکریپتی که کامپیوترها را از فایل منتقل می‌کند در زیر آورده شده است. شماره خطوط برای راحتی اضافه شده است و در کد اصلی وجود ندارد.

```
1.  $dataSource=import-csv  "Assets.csv"
2.  Foreach($dataRecord in $datasource) {
3.      #map  variables  to  data  source
4.      $AssetTag = $dataRecord.AssetTag
5.      $Type = $dataReacord.Type

6.      #determine  name
7.      $ComputerName = $Type.substring(0,1) + $AssetTag
8.      $sAMAccountName=$ComputerName + "$"
9.      #determine  OU
10.         $strOUADsPath = "LDAP://OU=" + $TYPE + "S" + '
11.             ",ou=Clients,DC=contoso,DC=com"

12.         #create  the  computer  object
```

```
13.     $objOU=[ADSI]$strOUADsPath
14.     $objComputer=$objOU.Create("computer","CN="+$ComputerName)
15.     $objComputer.Put("sAMAccountName",$sAMAccountName)
16.     $objComputer.Put("userAccountControl",4096)
17.      $objComputer.SetInfo()
18. }
```

خطوط ۱۳ تا ۱۷ مشابه دستورات بخش قبلی است به جز خط ۱۳ که به جای مسیر OU از متغیر آن استفاده شده است. این خطوط بخشی از بلوک کد هستند که در محدوده خطوط ۲ تا ۱۸ قرار دارند و برای هر رکورد در منبع داده تکرار می‌شوند. منبع داده در خط ۱ با استفاده از همان Import-Csv cmdlet که در فصل ۳ بررسی شد تعریف می‌شود. در خط ۲ از مجموعه foreach (نام دیگر آن ForEach-Object است) برای ایجاد حلقه استفاده می‌شود.

خط ۴ و ۵ در هر رکورد دو فیلد را به متغیر نسبت می‌دهد. خطوط ۶ تا ۱۱ قواعد نام‌گذاری را اجرا می‌کند. خط ۷ نام کامپیوتر را همراه پیشوند نام (D یا L) می‌سازد. خط ۸ خصیصه sAMAccountName را با افزودن علامت $ به نام کامپیوتر ایجاد می‌کند. خط ۱۰ مسیر OU را برای انتقال شیء مشخص می‌کند. علامت درج شده در انتهای خط ۱۰ به ما می‌گوید که خط تمام نشده و در خط بعدی ادامه پیدا می‌کند. در واقع خطوط ۱۰ و ۱۱ یک خط واحد هستند. طبق قواعد نام‌گذاری باید حرف "S" در انتهای Desktop OU اضافه شود تا نام OU به Desktops تغییر کند.

همان‌طور که از اسکریپت پیداست ساخت یک سیستم خودکار اشیاء کامپیوتر کار خیلی سختی نیست. منبع داده و قواعد نام‌گذاری را ما تعیین می‌کنیم و اسکریپت PowerShell ویندوز کار را انجام می‌دهد.

ساخت اشیاء کامپیوتر با استفاده از VBScript

VBScript برای دست‌کاری اشیاء دایرکتوری از همان ADSI استفاده می‌کندکه PowerShell ویندوز استفاده می‌کند بنابراین مراحل کار مشابه است. به container متصل می‌شویم، شیء را ایجاد می‌کنیم، خصیصه‌ها را مقداردهی می‌کنیم و تغییرات را اعمال می‌کنیم. قطعه کد زیر شیء کامپیوتری را در دامنه می‌سازد:

```
Set  objOU = GetObject("LDAP://DN of OU")
Set  objComputer = objOU.Create("computer","CN=Computer CN")
objComputer.Put "sAMAccountName","ComputerName$"
objComputer.Put "userAccountControl", 4096
objComputer.SetInfo()
```

کد خیلی شبیه دستور PowerShell ویندوز است که در خطوط ۱۳ تا ۱۷ اسکریپت در بخش قبلی دیدیم.

نکته VBScript نیز می‌تواند از بانک اطلاعاتی استفاده کند

در بخش قبلی دیدیم که چطور می‌توان از فایل csv. به عنوان منبع داده در اسکریپت PowerShell ویندوز استفاده کرد. VBScript هم می‌تواند داده را از این فایل‌ها بارگذاری کند ولی نه به آن خوبی که PowerShell Import-Csv cmdlet انجام می‌دهد.

تمرینات ساخت و مدیریت یک کنسول MMC

در این تمرینات خودکارسازی انتقال و ساخت اشیاء کامپیوتر در دامنه تمرین می‌شود. برای اجرای این تمرینات اشیاء زیر در دامنه contoso.com باید ساخته شده باشند.

- OU سطح اول با نام Clients
- OU سطح اول با نام Servers

همچنین باید ویژگی PowerShell ویندوز نصب شده باشد. تمرین فصل ۳ درس ۲ روش کار را نشان داده است.

تمرین ۱ ساخت شیء کامپیوتر با دستور Dsadd

این دستور به ما امکان می‌دهد شیء کامپیوتر را از طریق خط فرمان ایجاد کنیم. مزیت این دستور این است که فقط نیاز به DN کامپیوتر دارد. این دستور به طور خودکار خصیصه‌های userAccountControl و sAMAccountName را مقداردهی می‌کند. در این تمرین با دستور Dsadd.exe شیء کامپیوتر می‌سازیم.

۱. با کاربر Administrator به SERVER01 وارد می‌شویم.

۲. پنجره خط فرمان را باز می‌کنیم.

۳. دستور زیر را تایپ کرده و دکمه Enter را می‌زنیم.

```
Dsadd computer "CN=DESKTOP!%@,OU=Clients,DC=contoso,DC=com"
```

تمرین ۲ انتقال اشیاء کامپیوتر با دستور CSVDE

اگر بخواهیم تعداد زیادی شیء کامپیوتر بسازیم بهتر است اشیاء را از یک منبع داده از قبیل فایل csv. منتقل کنیم. در این تمرین از دستور CSVDE برای این کار استفاده می‌شود.

۱. Notpad را باز می‌کنیم.

۲. خطوط زیر را در آن وارد می‌کنیم. هر بالت نشان دهنده یک خط می‌باشد. بالت‌ها را در فایل Notpad وارد نکنید.

- DN,objectClass,name,userAccountControl,sAMAccountName
- "CN=DESKTOP103,OU=Clients,DC=contoso,DC=com",computer,DESKTOP103,4096,DESKTOP103$
- "CN=DESKTOP104,OU=Clients,DC=contoso,DC=com",computer,DESKTOP104,4096,DESKTOP104$
- "CN=SERVER02,OU=Servers,DC=contoso,DC=com",computer,SERVER02,4096,SERVER02$

۳. فایل را در پوشه Documents با نام "Computers.csv" ذخیره می‌کنیم. نام فایل را در داخل گیومه قرار می‌دهیم تا Notpad پسوند txt. به آن اضافه نکند.

۴. پنجره خط فرمان را باز می‌کنیم.

۵. دستور زیر را تایپ کرده و کلید Enter را می‌زنیم:

```
Csvde -i -f "%username%\documents\computers.csv"
```

تمرین ۳ انتقال اشیاء کامپیوتر از یک فایل LDIF

فایل‌های LDIF به اندازه فایل‌های csv. برای مدیران شبکه آشنا نیستند ولی خیلی قدرتمند و ساده هستند. در این تمرین یک فایل LDIF می‌سازیم و با دستور Ldifde.exe آن را منتقل می‌کنیم.

۱. Notpad را باز می‌کنیم.

۲. خطوط زیر را در برنامه تایپ کرده و بین دو عملیات یک خط خالی درج می‌کنیم (قبل از خط dn برای SERVER11)

```
Dn: CN=SERVER10,OU=Servers,DC=contoso,DC=com
Changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
objectClass: computer
cn: SERVER10
userAccountControl: 4096
sMAccountName: SERVER10$

Dn: CN=SERVER11,OU=Servers,DC=contoso,DC=com
Changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
objectClass: computer
cn: SERVER11
userAccountControl: 4096
sMAccountName: SERVER11$
```

۳. فایل را در پوشه Documents با نام "Computers.ldf" ذخیره می‌کنیم. نام فایل را داخل گیومه قرار می‌دهیم.

۴. پنجره خط فرمان را باز می‌کنیم.

۵. دستور زیر را تایپ کرده و کلید Enter را می‌زنیم:

```
Ldifde  -i  -f  “%userprofile%\documents\computers.ldf”
```

تمرین ۴ ساخت شیء کامپیوتر با PowerShell ویندوز

PowerShell ویندوز امکان ساخت و دستکاری اشیاء Active Directory را با استفاده از ADSI می‌دهد که در این تمرین اجرا می‌شود.

۱. PowerShell ویندوز را باز می‌کنیم.

۲. دستورات زیر را تایپ کرده و بعد از هر کدام کلید Enter را می‌زنیم:

```
$objOU=[ADSI]”LDAP://OU=Clients,DC=contoso,DC=com”
$objComputer=$objOU.Create("computer","CN=DESKTOP154”)
$objComputer.Put("sAMAccountName", “DESKTOP154$”)
$objComputer.Put("userAccountControl",4096)
 $objComputer.SetInfo()
```

۳. حالا Active Directory را چک می‌کنیم و از ساخت شیء کامپیوتر مطمئن می‌شویم.

تمرین ۵ ساخت شیء کامپیوتر با VBScript

در این تمرین با نوشتن VBScript و اجرای آن یک شیء کامپیوتر ساخته می‌شود.

۱. Notpad را باز می‌کنیم.

۲. خطوط زیر را در برنامه تایپ می‌کنیم:

```
Set objOU = GetObject(”LDAP://OU=Clients,DC=contoso,DC=com”)
Set objComputer=objOU.Create("computer","CN=DESKTOP155”)
objComputer.Put  "sAMAccountName", “DESKTOP155$”
objComputer.Put  "userAccountControl" , 4096
objComputer.SetInfo
```

۳. فایل را در پوشه Documents با نام "CreateComputer.vbs" ذخیره می‌کنیم. نام فایل را داخل گیومه قرار می‌دهیم.

۴. پنجره خط فرمان را باز کرده و دستور زیر را تایپ می‌کنیم:

```
Cscript  “%userprofile%\documents\createcomputer.vbs”
```

۵. با چک کردن Active Directory از ساخت شیء کامپیوتر مطمئن می‌شویم.

خلاصه درس

- از CSVDE به منظور انتقال اشیاء کامپیوتر از فایل‌های متنی comma-delimited بهره می‌بریم. این فایل‌ها با ابزارهایی نظیر Notpad یا Excel ویرایش می‌شود.
- از LDIFDE برای انتقال فایل‌های LDIF که شامل دستورات افزودن کامپیوتر می‌باشد استفاده می‌شود.
- دستور Dsadd با یک خط دستور می‌تواند در دامنه شیء کامپیوتر بسازد.
- VBScript و PowerShell ویندوز با استفاده از ADSI می‌توانند شیء کامپیوتر به دامنه اضافه کنند.

سئوالات پایان درس

۱. مدیر ما دستور ساخت یک حساب برای کامپیوتر DESKTOP234 را صادر کرده است. کدام‌یک از گزینه‌های زیر در اجرای این درخواست به ما کمک می‌کند؟

A. CDVDE

B. LDIFDE

C. Dsadd

D. PowerShell ویندوز

E. VBScript

۲. فروشنده دستگاههای کامپیوتر یک فایل Excel شامل شماره اموال (asset tag) کامپیوترهایی که قرار است هفته بعد تحویل دهد ارسال می‌کند. می‌خواهیم برای دستگاهها اشیاء کامپیوتر بسازیم. قواعد نام‌گذاری سازمان ایجاب می‌کند از شماره اموال برای نام کامپیوترها استفاده کنیم. کدام یک از گرینه‌های زیر برای این کار مناسب می‌باشد؟ (ممکن است بیش از یک جواب داشته باشد)

A. CSVDE

B. LDIFDE

C. Dsadd

D. PowerShell ویندوز

E. VBScript

درس ۳ نگهداری از حساب‌ها و اشیاء کامپیوتر

حساب کامپیوتر زمانی که ساخته می‌شود و به دامنه join می‌شود حیات خود را شروع می‌کند. وظایف روزمره مدیریتی کارهایی از قبیل پیکربندی خصیصه‌های کامپیوتر، انتقال کامپیوترها بین OU ها، مدیریت کامپیوترها، تغییر نام، غیرفعال کردن، فعال کردن و حذف اشیاء کامپیوتر می‌باشد. در این درس به خصیصه‌های کامپیوتر و روندهایی که به این وظایف مربوط می‌شود و ما را در مدیریت کامپیوترها یاری می‌دهد پرداخته می‌شود.

بعد از این درس ما می‌توانیم:

- خصیصه‌های یک کامپیوتر را پیکربندی کنیم.
- کامپیوترها را بین OU ها جابجا کنیم.
- نام کامپیوتر را تغییر دهیم.
- حساب‌های کامپیوتر را فعال و غیر فعال کنیم.
- کانال ارتبایی امن کامپیوتر عضو دامنه را ریست کنیم.
- وظایف مدیریتی را با ابزار Active Directory Users And Computers ، دستورات خط فرمان، VBScript و PowerShell ویندوز اجرا کنیم.

زمان تقریبی : ۴۵ دقیقه

پیکربندی خصیصه‌های کامپیوتر

وقتی شیء کامپیوتر ساخته می‌شود فقط پیکربندی اساسی‌ترین خصیصه‌ها از قبیل نام کامپیوتر و مجوز join کردن آن به دامنه ضروری است. کامپیوترها خصیصه‌های متعددی دارند که هنگام ساخت قابل رویت نیستند و باید آنها را در پروسه‌های نگهداری پیکربندی کنیم.

کادر محاوره‌ای Properties شیء کامپیوتر را باز کنید و location و description، عضویت گروه و مجوزهای dial-in آن را پیکربندی کنید و آن را به شیء کاربر صاحب کامپیوتر پیوند دهید. زبانه Operating System فقط خواندنی است. اطلاعات تا زمانی که کامپیوتر به دامنه join نشود خالی خواهد ماند

کلاس‌های شیء متعددی در Active Directory از خصیصه managedBy پشتیبانی می‌کنند که در زبانه Managed By قرار دارد. این خصیصه پیوندی یک cross-reference به شیء کاربر می‌سازد. همه خصیصه‌های دیگر مثل آدرس و شماره تلفن مستقیما در شیء کاربر نمایش داده می‌شوند ولی به عنوان بخشی از شیء کامپیوتر ذخیره نمی‌شوند.

در زبانه Member Of کادر محاوره‌ای Properties کامپیوتر می‌توانیم کامپیوتر را به گروه اضافه کنیم. قابلیت مدیریت کامپیوترها در گروهها ویژگی مهمی است. گروهی که کامپیوتر به آن تعلق دارد می‌تواند برای اعطاء مجوز دسترسی به منابع کامپیوتر یا فیلتر کردن برنامه یک GPO به کار رود.

مانند کاربران و گروهها انتخاب گروهی اشیاء کامپیوتر و مدیریت یا تغییر خصوصیات همه اشیاء انتخاب شده به صورت همزمان امکانپذیر است.

پیکربندی خصیصه‌های کامپیوتر با دستور Dsmod

دستور Dsmod که در فصل ۳ و ۴ با آن آشنا شدیم قادر است فقط خصیصه‌های location و description را تغییر دهد. شکل فرمان به صورت زیر است:

Dsmod computer "DN of computer" [-desc Description] [-loc Location]

پیکربندی خصیصه‌های کامپیوتر با PowerShell ویندوز یا VBScript

در PowerShell ویندوز و VBScript می‌توانیم خصیصه‌های کامپیوتر را در سه مرحله تغییر دهیم:

۱. ابتدا با استفاده از ADSI و خصیصه aDSPath کامپیوتر و به شکل "LDAP://DN of Computer" به آن متصل می‌شویم.

۲. از متد Put شیء کامپیوتر برای مقداردهی خصیصه‌های تک مقداره استفاده می‌کنیم.

۳. از متد SetInfo برای اعمال تغییرات به شیء استفاده می‌کنیم.

دستورات PowerShell ویندوز به صورت زیر است:

```
$objComputer= [ADSI]"LDAP://DN of Computer"
$objComputer.Put("property",value)
$objComputer.SetInfo()
```

و کد VBScript آن به شکل زیر است:

```
Set objComputer= GetObject("LDAP://DN of Computer"
objComputer.Put "property"
Value objComputer.SetInfo
```

در هر دو مورد اگر مقدار متنی باشد باید در گیومه قرار گیرد.

انتقال شیء کامپیوتر

بسیاری از سازمان‌ها برای اشیاء کامپیوتر چند OU دارند. به عنوان مثال همان طور که در شکل ۲- ۵ نشان داده شده است بعضی دامنه‌ها OU هایی بر اساس سایت‌های جغرافیایی برای کامپیوتر دارند. اگر بیش از یک OU برای کامپیوتر داشته باشیم ممکن است روزی بخواهیم کامپیوتری را بین OUها جابجا کنیم.

برای انتقال شیء کامپیوتر در ابزار Active Directory Users And Computers کافی است شیء را کشیده و در OU جدید رها کنیم یا روی شیء کلیک راست کرده و دستور Move را کلیک کنیم.

برای این جابجایی باید مجوزهای لازم را داشته باشیم. به طور پیش فرض گروه Account Operators می‌توانند اشیاء کامپیوتر را بین container ها جابجا کنند به غیر از Domain Controllers OU . گروه Administrators که گروههای Domain Admins و Enterprise Admins را در بر می‌گیرد می‌تواند اشیاء را در همه جا بدون محدودیت جابجا کند. هیچ راهی برای اعطاء مجوز خاص انتقال شیء در Active Directory وجود ندارد. در عوض قابلیت انتقال شیء از قابلیت حذف یک شیء در مبدا و ساخت آن در مقصد ناشی می‌شود. وقتی شیئی جابجا می‌شود در واقع حذف و بازسازی انجام نمی‌شود بلکه مجوزهای حذف و بازیابی هستند که برای انجام عمل انتقال ارزیابی می‌گردند.

دستور Dsmove امکان انتقال اشیاء را فراهم می‌کند. شکل فرمان به صورت زیر است:

Dsmove ObjectDN [-newname NewName] [-newparent ParentDN]

پارامتر newname امکان تغییر نام شیء را فراهم می‌کند. پارامتر newparent ما را قادر می‌سازد شیء را منتقل کنیم. برای تغییر نام کامپیوتر با نام DESKTOP153 از Computers container به Clients OU باید دستورات زیر را وارد کنیم:

```
Dsmove "CN=DESKTOP153,CN=Computers,DC=contoso,DC=com" –newparent
"OU=Clients,DC=contoso,DC=com"
```

برای انتقال یک کامپیوتر در PowerShell ویندوز باید از متد psbase.MoveTO استفاده کنیم. دو خط زیر یک کامپیوتر را منتقل می‌کند:

```
$objUser=[ADSI]"LDAP://ComputerDN"
$objUser.psbase.MoveTo("LDAP://TargetOUDN")
```

با VBScript ما به container مبداء متصل می‌شویم و از متد MoveHere آن استفاده می‌کنیم:

```
Set objOU = GetObject(“LDAP://TargetOUDN”)
objOU.MoveHere “LDAP://ComputerDN” , vbNullString
```

قبل از انتقال شیء کامپیوتر موارد تفویض اختیار و پیکربندی را باید در نظر بگیریم. OU مقصد ممکن است مجوزهای متفاوتی نسبت به OU مبداء داشته باشد. در این حالت شیء، مجوزهای جدید را به ارث می‌برد که مشخص می‌کند چه کسی می‌تواند شیء را مدیریت کند. OU مقصد ممکن است در حوزه GPO های متفاوتی قرار داشته باشد که خود باعث تغییر پیکربندی سیستم خواهد شد.

مدیریت کامپیوتر توسط ابزار Active Directory Users And Computers

یکی از ویژگی‌های سودمند و کمتر مورد توجه ابزار Active Directory Users And Computers دستور Manage است. روی کامپیوتری در این ابزار کلیک راست کرده و Manage را انتخاب می‌کنیم. کنسول Computer Management باز می‌شود و درباره کامپیوتر انتخابی کلیاتی راجع به event log ، گروهها و کاربران محلی، پیکربندی پوشه‌های به اشتراک گذاشته شده و دیگر ابزارهای مدیریتی ارائه می‌شود. این ابزار با اعتبار موجود برای اجرای Active Directory Users And Computers اجرا می‌شود بنابراین باید ابزار Active Directory Users And Computers را با کاربر عضو گروه Administrators کامپیوتر مقصد اجرا کنیم تا حداکثر کارایی را در کنسول Computer Management داشته باشیم.

ورود به کامپیوتر و کانال ارتباطی امن

همه کامپیوترها در دامنه درست مانند حساب کاربر دارای حساب با نام کاربری (sAMAccountName) و کلمه عبور هستند. کامپیوتر کلمه عبور خود را به شکل رمز local security authority (LSA) ذخیره می‌کند و کلمه عبور خود را با دامنه تقریبا هر ۳۰ روز یکبار تغییر می‌دهد. سرویس Netlogon از این حساب برای ورود به دامنه استفاده می‌کند و یک کانال ارتباط امن با DC برقرار می‌کند.

تشخیص مشکلات حساب کامپیوتر

حساب‌های کامپیوتر و ارتباطات امن بین آنها و دامنه خیلی قوی است. ولی شرایطی ممکن است پیش آید که کامپیوتر دیگر نتواند توسط دامنه تایید هویت شود. نمونه‌هایی از این شرایط را بررسی می‌کنیم:

- ***پس از نصب سیستم عامل کلاینت سیستم حتی اگر با نام قبلی نصب شده باشد دیگر تایید هویت نمی‌شود.*** چون سیستم عامل جدید SID جدید هم می‌سازد و چون سیستم عامل جدید کلمه عبور حساب کامپیوتر را در دامنه نمی‌داند به دامنه تعلق نخواهد داشت و تایید هویت نمی‌شود.

- ***کامپیوتر از یک پشتیبان به طور کامل بازیابی شده ولی تایید هویت نمی‌شود.*** احتمالا کلمه عبور کامپیوتر بعد از عملیات بازیابی عوض شده است. کامپیوترها هر ۳۰ روز یکبار کلمه عبور خود را عوض می‌کنند و Active Directory کلمه عبور جاری و قبلی را ذخیره می‌کند. اگر عملیات بازیابی، کامپیوتر را با کلمه عبور منقضی شده برگرداند کامپیوتر دیگر تایید هویت نمی‌شود.

- ***رمز LSA یک کامپیوتر با کلمه عبور ثبت شده در دامنه همخوانی ندارد.***می‌توان فرض کرد کامپیوتر کلمه عبور خود را فراموش کرده است. در واقع کلمه عبور کامپیوتر در دامنه اعتبار ندارد و به همین دلیل تایید هویت نمی‌شود.

مهم‌ترین عوارض مشکلات حساب کامپیوتر به ترتیب زیر است:

- پیغامی هنگام ورود به سیستم مبنی بر اینکه domain controller در دسترس نیست ظاهر می‌شود و اینکه حساب کامپیوتر وجود ندارد، کلمه عبور حساب کامپیوتر صحیح نیست یا trust (به بیان دیگر ارتباط امن) بین کامپیوتر و دامنه ایجاد نمی‌شود. مثالی از این مورد در شکل ۷- ۵ نشان داده شده است.

شکل ۷- ۵ پیغام خطایی که نشان دهنده خطای کانال ارتباطی امن است

- خطاها یا وقایع ثبت شده در event log نشان می‌دهد که مشکلات مشابه اتفاق افتاده یا کلمات عبور، trust ها، کانال‌های ارتباطی امن یا ارتباطات با دامنه یا domain controller به مشکل خورده است.
- حساب کامپیوتر در Active Directory وجود ندارد.

ریست حساب کامپیوتر

وقتی کانال امن به مشکل برخورد می‌کند باید آن را ریست کنیم. بسیاری از مدیران شبکه این کار را با حذف کامپیوتر از دامنه، قرار دادن آن در یک workgroup و سپس join کردن آن انجام می‌دهند. این روش مناسبی نیست زیرا SID کامپیوتر و از آن مهم‌تر عضویت گروه‌ها از دست می‌رود. وقتی کامپیوتر را دوباره join می‌کنیم حتی اگر نام کامپیوتر را مانند قبل تعیین کنیم SID آن جدید خواهد بود و همه عضویت گروههای شیء کامپیوتر قبلی باید دوباره ساخته شود. راه بهتر این است که کانال امن را ریست کنیم.

برای ریست کانال امن بین عضو دامنه و خود دامنه از ابزار Active Directory Users And Computers ، Dsmod.exe یا Nttest.exe استفاده می‌شود. با ریست حساب، SID کامپیوتر به همان شکل باقی می‌ماند و بنابراین عضویت گروهها تغییر نمی‌کند. در این قسمت روش کار با ابزارهای نام‌برده بررسی می‌شود:

- **ابزار Active Directory Users And Computers** روی کامپیوتر کلیک راست کرده و Reset Account را انتخاب می‌کنیم. سپس Yes را می‌زنیم. حالا کامپیوتر را باید دوباره join می‌کنیم که البته به راه اندازی مجدد سیستم نیاز داریم.
- **Dsmod** دستور dsmod computer "Computer DN" –reset را اجرا می‌کنیم. حالا کامپیوتر را باید دوباره join کنیم که البته سیستم را باید راه اندازی مجدد کنیم.
- **Netdom** دستور netdom reset MachineName /domain DomainName/UserO {Password|*}/PasswordO:UserName را روی سرور اجرا می‌کنیم. در حالی که اعتبار کاربر، مربوط به گروه Administrators محلی کامپیوتر می‌باشد. این دستور کانال امن بین کامپیوتر و دامنه را با ریست کردن هر دو کلمه عبور تجدید می‌کند. بنابراین نیازی به join دوباره و راه اندازی مجدد سیستم نیست.
- **Nltest** روی کامپیوتری که کانال را از دست داده دستور nltest /server:ServerName /sc_reset:DOMAIN\DomainController را اجرا می‌کنیم. برای مثال دستور nltest /server:SERVER02 /sc_rest:CONTOSO\SERVER01 یک نمونه از آن می‌باشد. این دستور نیز مانند دستور Netdom کلمه عبور کامپیوتر و دامنه را ریست می‌کند و نیازی به join دوباره و راه اندازی مجدد سیستم نمی‌باشد.

چون Nltest.exe و Netdom.exe کانال امن را بدون نیاز به راه اندازی مجدد انجام می‌دهند اول این دستورات را امتحان می‌کنیم. اگر جواب نگرفتیم از دستور Dsmod یا Reset Account استفاده می‌کنیم.

تغییر نام کامپیوتر

تغییر نام کامپیوتر باید با احتیاط صورت گیرد. نام کامپیوتر در تایید هویت آن در دامنه مورد استفاده قرار می‌گیرد بنابراین اگر نام شیء کامپیوتر را فقط در دامنه یا فقط خود کامپیوتر تغییر دهیم ارتباط این دو قطع خواهد شد. نام کامپیوتر باید به گونه‌ای تغییر یابد که در هر دو طرف تغییر انجام شود

نام کامپیوتر را با ورود به سیستم به صورت محلی یا remote desktop می‌توان تغییر داد. پنجره System Properties را از طریق کنترل پنل باز می‌کنیم و در بخش Computer Name, Domain, And Workgroup Settings دکمه Change Settings را کلیک می‌کنیم. اگر پیغام ظاهر شد Continue را کلیک می‌کنیم و دکمه Change را در زبانه Computer Name می‌زنیم.

از پنجره خط فرمان دستور Netdom را به شکل زیر می‌توانیم استفاده کنیم:

```
Netdom renamecomputer MachineName /NewName:NewName
    [/UserO:LocalUsername] [/PasswordO:{LocalPassword|*} ]
    [/UserD:DomainUsername] [/PasswordD:{DomainPassword|*} ]
    [/SecurePasswordPrompt] [/REBoot[:TimeInSeconds] ]
```

به علاوه تعیین کامپیوتر (MachineName) برای تغییر نام و نام جدید (NewName) ما باید از اعتبار کاربر عضو گروه Administrators محلی کامپیوتر و اعتبار دارای مجوز تغییر نام شیء کامپیوتر دامنه استفاده کنیم. به طور پیش فرض دستور Netdom.exe از اعتباری که با آن دستور اجرا شده استفاده می‌کند. ما می‌توانیم با استفاده از پارامترهای UserO و PasswordO از اعتبار کاربر عضو گروه Administrators محلی و پارامترهای UserD و PasswordD از اعتبار کاربر دامنه با مجوز تغییر نام شیء کامپیوتر استفاده کنیم. تعیین علامت "*" برای کلمه عبور باعث باز شدن پنجره برای ورود کلمه عبور خواهد شد. پارامتر SecurePasswordPropmpt وقتی هم به جای PasswordO و هم PasswordD علامت * قرار می‌گیرد پنجره‌ای را برای ورود نام کاربری و کلمه عبور باز می‌کند. پس از تغییر نام کامپیوتر باید سیستم را راه‌اندازی مجدد کنیم. پارامتر REBoot باعث راه‌اندازی مجدد سیستم پس از ۳۰ ثانیه می‌شود مگر اینکه با پارامتر TimeInSeconds دقیقا تعیین شود.

وقتی نام کامپیوتری تغییر می‌کند باید سرویس‌های وابسته به نام روی آن نیز تغییر کند. برای مثال Active Directory Certificate Services (AD CS) وابسته به نام سرور می‌باشد. قبل از تغییر نام سرور به عواقب آن توجه کنید. ضمنا از این روش‌ها برای تغییر نام domain controller نمی‌توان استفاده کرد.

فعال و غیرفعال کردن حساب کامپیوتر

وقتی کامپیوتری برای مدتی از شبکه خارج می‌شود باید حساب آن را غیرفعال کنیم. این کار امنیت را ارتقا می‌دهد چون هرچه تعداد حسابهای فعال در انباره هویت کمتر باشد امنیت بالاتر است.

غیرفعال کردن حساب، SID یا عضویت گروه را تغییر نمی‌دهد بنابراین وقتی حساب را فعال می‌کنیم به وضعیت سابق برمی‌گردیم.

با راست کلیک کردن روی کامپیوتر و انتخاب گزینه Disable Account آن را غیرفعال می‌کنیم. آیکن حساب غیرفعال همانند شکل ۸- ۵ با یک علامت فلش روبه‌پایین در ابزار Active Directory Users And Computers مشخص می‌شود.

شکل ۸- ۵ یک حساب کامپیوتر غیرفعال

تا زمانی که حساب غیرفعال است کامپیوتر نمی‌تواند کانال امن با دامنه ایجاد کند. نتیجه این می‌شود که کاربرانی که تاکنون به کامپیوتر وارد نشده‌اند و بنابراین اعتبار آنان روی کامپیوتر cashe نشده است تا زمانی که حساب فعال نشود نمی‌توانند به سیستم وارد شوند.

برای فعال کردن حساب، کامپیوتر را انتخاب کرده و دستور Enable Account را از منوی کلیک راست انتخاب می‌کنیم.

برای فعال کردن حساب کامپیوتر از طریق خط فرمان از دستور Dsmod استفاده می‌کنیم. شکل فرمان به صورت زیر است:

```
DSMOD        COMPUTER  ComputerDN  -DISAABLED  YES
```

DSMOD COMPUTER ComputerDN -DISAABLED NO

حذف شیء کامپیوتر

دیدیم که حساب‌های کامپیوتر مانند کاربر دارای یک SID منحصر می‌باشد که به مدیر شبکه امکان اعطاء مجوز به کامپیوترها را می‌دهد. همچنین مانند حساب‌های کاربر، کامپیوترها می‌توانند عضو گروه شوند. بنابراین مانند حساب‌های کاربر باید مواظب تاثیرات حذف حساب کامپیوتر باشیم. وقتی حساب کامپیوتری حذف می‌شود عضویت گروه و SID آن حذف می‌گردد. اگر حذف تصادفی باشد و کامپیوتری با همان نام ساخته شود به هر حال حساب جدید SID جدید خواهد داشت. عضویت گروهها و مجوزها برای کامپیوتر جدید باید دوباره تنظیم شود. فقط زمانی باید کامپیوتر را حذف کرد که به خصیصه‌های امنیتی آن شیء نیازی نداشته باشیم.

برای حذف کامپیوتر با استفاده از Active Directory Users And Computers روی شیء کامپیوتر کلیک راست کرده و از منو دستور Delete را انتخاب می‌کنیم. در تاییدیه حذف دکمه Yes را می‌زنیم و شیء حذف می‌شود.

دستور Dsrm که در فصل ۳ معرفی شد قادر به حذف اشیاء از طریق خط فرمان است. برای این کار تایپ می‌کنیم:

DSRM ObjectDN

در حالی که ObjectDN در واقع DN کامپیوتر است. دوباره پیغام تایید را OK می‌کنیم.

بازیابی کامپیوتر

وقتی بخواهیم کامپیوتری را به سیستم با سخت افزار جدیدتر ارتقا دهیم چه باید بکنیم؟ این سناریوی دیگری است که در آن می‌توانیم حساب کامپیوتر را ریست کنیم.

ریست حساب کامپیوتر کلمه عبور آن را ریست می‌کند ولی همه خصیصه‌ها به همان شکل باقی می‌ماند. پس از این کار باید کامپیوتر ارتقا یافته را دوباره به دامنه join کرد. با این روش حساب کامپیوتر به کامپیوتر جدید تعلق می‌یابد. همچنین می‌توانیم نام حساب را تغییر دهیم که عضویت گروه و SID به همان شکل باقی می‌ماند.

همانطور که پیش‌تر در این درس گفته شد دستور Reset Account در منوی کلیک راست موجود است. دستور Dsmod همچنین برای ریست کردن حساب کامپیوتر استفاده می‌شود:

Dsmod computer "ComputerDN" –reset

تمرینات نگهداری حساب‌ها و اشیاء کامپیوتر

در این تمرینات ما با مهارت‌هایی که در این درس آموختیم حساب‌های کامپیوتر را پشتیبانی و عیب‌یابی می‌کنیم. برای انجام تمرینات درس باید اشیاء زیر در دامنه contoso.com موجود باشد.

- OU سطح اول با نام Clients
- دو شیء کامپیوتر به نام DESKTOP154 و DESKTOP155 در Clients OU
- یک OU با نام Desktop و یک OU با نام Laptops در Clients OU.
- OU سطح اول با نام People
- حساب‌های کاربری در People OU برای Linda Mitchell و Scott Mitchell. خصیصه‌های اطلاعات تماس را برای آن‌ها مقداردهی کنید: آدرس، تلفن و e-mail
- OU سطح اول با نام Groups
- یک گروه در Groups OU به نام Sales Desktops

تمرین ۱ مدیریت اشیاء کامپیوتر

در این تمرین ما چند وظیفه مدیریتی رایج را مربوط به کامپیوترها را انجام می‌دهیم.

۱. با کاربر Administrator به SERVER01 وارد می‌شویم.

۲. ابزار Active Directory Users And Computers را باز می‌کنیم.

۳. Clients OU را انتخاب می‌کنیم.

۴. در پنل وسط روی DESKTOP154 کلیک راست کرده و Properties را انتخاب می‌کنیم.

۵. زبانه Managed By را باز می‌کنیم.

۶. دکمه Change را کلیک می‌کنیم.

۷. نام کاربری Scott Mitchell را تایپ کرده و OK می‌کنیم.

زبانه Managed By اطلاعات تماس شیء کاربر Scott Mitchell را منعکس می‌کند.

۸. دکمه Properties را کلیک می‌کنیم.

این دکمه ما را به خصیصه managedBy شیء کاربر می‌برد

۹. دکمه OK را کلیک می‌کنیم تا کادرها بسته شوند.

۱۰. مراحل ۴ تا ۹ برای DESKTOP155 و Linda Mitchell تکرار می‌کنیم.

۱۱. در پنل وسط Clients OU هر دو کامپیوتر DESKTOP154 و DESKTOP155 را انتخاب می‌کنیم.

۱۲. هر دو شیء را به Desktop OU می‌کشیم. Yes را برای تایید کلیک می‌کنیم.

۱۳. در ساختار درختی کنسول Desktop OU را انتخاب می‌کنیم.

۱۴. در پنل وسط هر دو کامپیوتر را انتخاب می‌کنیم.

۱۵. روی کامپیوترهای انتخاب شده کلیک راست کرده و Properties را انتخاب می‌کنیم.

کادر محاوره‌ای Properties For Multiple Items باز می‌شود.

۱۶. کادر Change The Description Text For All Selected Objects را علامت زده و عبارت Sales Desktop را تایپ می‌کنیم و دکمه OK را کلیک می‌کنیم.

۱۷. وقتی هر دو در حالت انتخاب قرار دارند روی یکی از کامپیوترها کلیک راست کرده و Add To A Group را انتخاب می‌کنیم.

۱۸. Sales Desktop را تایپ کرده و OK می کنیم.

۱۹. پیغام موفقیت عملیات ظاهر می‌شود.

۲۰. دکمه OK را کلیک می‌کنیم.

۲۱. در ساختار درختی کنسول Domain Controllers OU را انتخاب می‌کنیم.

۲۲. در پنل وسط روی SERVER01 کلیک راست کرده و Manage را انتخاب می‌کنیم

۲۳. کنسول Computer Management مربوط به SERVER01 ظاهر می‌شود

تمرین ۲ عیب یابی حساب کامپیوتر

در این تمرین ریست کانال امن روی عضوی از دامنه شبیه‌سازی می‌شود. اگر کامپیوتر دومی وجود دارد که عضو دامنه contoso.com است می‌توانیم از نام آن در مرحله ۴ این تمرین برای اجرای واقعی ریست کانال امن استفاده کنیم.

۱. پنجره خط فرمان را باز می‌کنیم.

۲. دستور Nltest می‌تواند کانال ارتباطی و چند مورد دیگر مربوط به دامنه را تست کند. دستور nltest /? را تایپ کرده و گزینه‌های مختلف دستور را مرور می‌کنیم.

۳. دستور Netdom چندین کار را هم برای کامپیوتر و هم برای دامنه انجام می‌دهد. دستور netdom /? را تایپ کرده و گزینه‌های دستور را مرور می‌کنیم.

۴. ریست کانال ارتباطی را با تایپ netdom reset desktop154 شبیه‌سازی می‌کنیم. پیغام خطایی با بیان RPC Server Is Not Available ظاهر می‌شود چون سیستم آنلاین نمی‌باشد.

خلاصه درس

- می‌توانیم خصیصه‌های کامپیوتر را با ابزار Active Directory Users And Computers ، Dsmod، PowerShell ویندوز و VBScript پیکربندی کنیم.
- کامپیوترها هم مانند کاربران دارای حساب هستند و به آنها SID و عضویت گروه تعلق می‌گیرد. هنگام حذف شیء کامپیوتر مواظب عواقب آن باشید. غیرفعال کردن شیء کامپیوتر به ما امکان می‌دهد در صورت نیاز حساب را به صورت اول درآوریم.
- وقتی کانال امن کامپیوتری از بین می‌رود با دستور Reset Account در ابزار Active Directory Users And Computers، دستور Dsmod، Netdom.exe یا nltest.exe می‌توان آنرا ریست کرد.

سئوالات پایان درس

۱. مدیر سروری گزارش می‌دهد که یک event با مضمون Failed To Authenticate در event log فایل سرور مشاهده شده است. چه کار باید کرد؟

A. حساب سرور را ریست کنیم.

B. کلمه عبور کاربر مدیر سرور را ریست کنیم.

C. حساب سرور را غیرفعال و سپس فعال کنیم.

D. حساب کاربری مدیر سرور را حذف کنیم.

۲. کامپیوتری دارای مجوزهایی است که با آن سرویس سیستم را پشتیبانی می‌کند. این کامپیوتر عضو ۱۵ گروه مختلف می‌باشد. کامپیوتر با سخت افزار جدید جایگزین می‌شود. سخت افزار جدید asset tag جدید دارد و قواعد نام گذاری asset tag را

به عنوان نام کامپیوتر تعیین کرده است. چه باید بکنیم؟ (درصورت نیاز همه را انتخاب کنید. هر جواب صحیح بخشی از جواب است)

A. حساب کامپیوتر سیستم قبلی را حذف کنیم.

B. یک حساب کامپیوتر برای سیستم جدید بسازیم.

C. حساب کامپیوتر قبلی را ریست کنیم.

D. نام حساب کامپیوتر سیستم قبلی را تغییر دهیم.

E. سیستم جدید را به دامنه join کنیم.

۳. اخیرا دامنه فرزندی برای پشتیبانی از یک پروژه تحقیقاتی در محلی دور ساخته شده است. حساب‌های کامپیوتر برای محققین به دامنه جدید منتقل شده‌اند. وقتی ابزار Active Directory Users And Computers را باز می‌کنیم اشیاء این کامپیوترها با آیکن فلش رو به پایین نشان داده می‌شود. بهترین راه برای حل مشکل کدام است؟

A. حساب‌ها را ریست کنیم.

B. حساب‌ها را غیرفعال کنیم.

C. حساب‌ها را فعال کنیم.

D. حساب‌ها را حذف کنیم.

فصل ۶

زیرساخت Group Policy

در فصل ۱ یاد گرفتیم Active Directory Domain Services (AD DS) سرویس‌های اساسی identity and Access را برای شبکه‌های سازمانی که مبتنی بر ویندوز هستند فراهم می‌کند و اینکه فراتر از آن AD DS از مدیریت و پیکربندی حتی بزرگترین و پیچیده‌ترین شبکه‌ها پشتیبانی می‌کند. در فصل ۲، ۳، ۴ و ۵ تمرکز روی مدیریت واحدهای امنیتی AD DS یعنی کاربران گروهها و کامپیوترها بود. حالا باید با استفاده از Group Policy مدیریت و پیکربندی کاربران و کامپیوترها را انجام دهیم. Group Policy زیرساختی را فراهم می‌کند که در آن تنظیمات می‌توانند به صورت مرکزی تعریف شوند و به کاربران و کامپیوترها در سازمان اعمال شوند.

در سازمانی با زیرساخت مناسب Group Policy به ندرت پیش می‌آید که نیاز به پیکربندی مستقیم روی دستگاه پیدا کنیم. همه پیکربندی‌ها از طریق تنظیمات Group Policy (GPOs) تعریف، اعمال و به روز رسانی می‌شود. این تنظیمات روی بخشی از سازمان به اندازه یک سایت، دامنه، OU یا گروه تاثیر می‌گذارد. در این فصل با Group Policy ، نحوه کارکرد و بهترین روش پیاده سازی در سازمان آشنا می‌شویم. در فصل‌های بعدی از Group Policy در وظایف مدیریتی خاصی مانند پیکربندی امنیتی، توزیع نرم‌افزار، سیاست کلمه عبور و ممیزی استفاده می‌کنیم.

اهداف امتحانی در این فصل:

- ساخت و نگهداری اشیاء Active Directory

- ساخت و اعمال اشیاء Group Policy
- پیکربندی الگوهای GPO

- نگهداری Active Directory
- مانیتور کردن Active Directory

دروس این فصل:

- درس ۱: پیاده‌سازی Group Policy
- درس ۲: مدیریت حوزه Group Policy
- درس ۳: پشتیبانی از Group Policy

قبل از شروع

برای انجام تمرینات این فصل باید یک DC با نام SERVER01 در دامنه‌ای با نام contoso.com ساخته باشیم. برای جزئیات ساخت آن به فصل ۱ مراجعه کنید.

دنیای واقعی

دن هلم

بسیاری از مشتریان من همه چیز را با صرف کمترین انرژی می‌خواهند. افزایش امنیت، کاهش هزینه‌ها و افزایش بهره‌وری. اگر بتوانیم تغییرات و پیکربندی را در سازمان مدیریت کنیم رسیدن به این اهداف ساده می‌شود. وقتی یک مشکل امنیتی بروز می‌کند می‌خواهیم خیلی سریع حفره امنیتی را پر کنیم. وقتی تیم پشتیبانی گزارش می‌دهند که درخواست‌های کاربران برای پیکربندی خاصی روی سیستم‌شان زیاد است باید تغییرات را به صورت مرکزی توزیع کنیم که به‌طور موثرتری کار می‌کندو یا اگر نیاز باشد تکه کدی روی همه سیستم‌ها نصب می‌کنیم. اینها چند نمونه از انواع پیکربندی می‌باشد که روزانه در شبکه‌های کوچک و بزرگ اتفاق می‌افتد. Group Policy یک فن‌آوری فوق العاده است که به شبکه ارزش زیادی می‌دهد. بعضی مواقع در بعضی سازمان‌ها Group Policy با طراحی ضعیف دیده می‌شود.

درس ۱ پیاده سازی Group Policy

زیرساخت Group Policy بخش‌های قابل انتقال زیادی دارد. باید بدانیم هر بخشی چیست و این بخش‌ها چگونه با هم کار می‌کنند. همچنین چرا ترکیب اینها در پیکربندی های مختلف استفاده می‌شود. در این درس اطلاعات کاملی از اجزاء و عملکرد Group Policy ارائه می‌شود.

بعد از این درس ما می‌توانیم:

- اجزاء Group Policy را تشخیص دهیم.
- اساس پردازش Group Policy را تشریح کنیم.
- اشیاء Group Policy را بسازیم ویرایش کنیم و لینک دهیم.
- انباره مرکزی برای الگوهای مدیریتی بسازیم.
- تنظیمات policy خاصی را در GPO جستجو کنیم.

- از یک Starter GPO یک GPO دیگر بسازیم.

زمان تقریبی: ۹۰ دقیقه

مروری بر Group Policy

Group Policy یک ویژگی از ویندوز است که به ما امکان می‌دهد تغییرات و پیکربندی کاربران و کامپیوترها را از یک نقطه مرکزی مدیریت کنیم. اگر با مفهوم Group Policy آشنا نیستید دانستن این نکته مفید است که Group Policy همه چیز درباره پیکربندی و تنظیمات یک یا چند کامپیوتر یا کاربر می‌باشد. هزاران مورد تنظیم پیکربندی وجود دارد که با Group Policy مدیریت می‌شود.

تنظیمات Policy

ریزترین جزء Group Policy تنظیم policy منحصربه‌فردی است که به آن اختصارا policy نیز می‌گویند که یک تغییر پیکربندی خاص را تعریف می‌کند. برای مثال تنظیم policy را در نظر می‌گیریم که از دسترسی کاربر به ابزار ویرایش رجیستری جلوگیری می‌کند اگر این policy تعریف شود و به کاربر نیز اعمال شود کاربر دیگر نمی‌تواند از ابزارهایی نظیر Regedit.exe استفاده کند. policy دیگری را در نظر بگیرید که حساب Administrator محلی را غیرفعال می‌کند. این policy را می‌توانید روی همه کامپیوترها و لپ‌تاپ‌ها اعمال کنید.

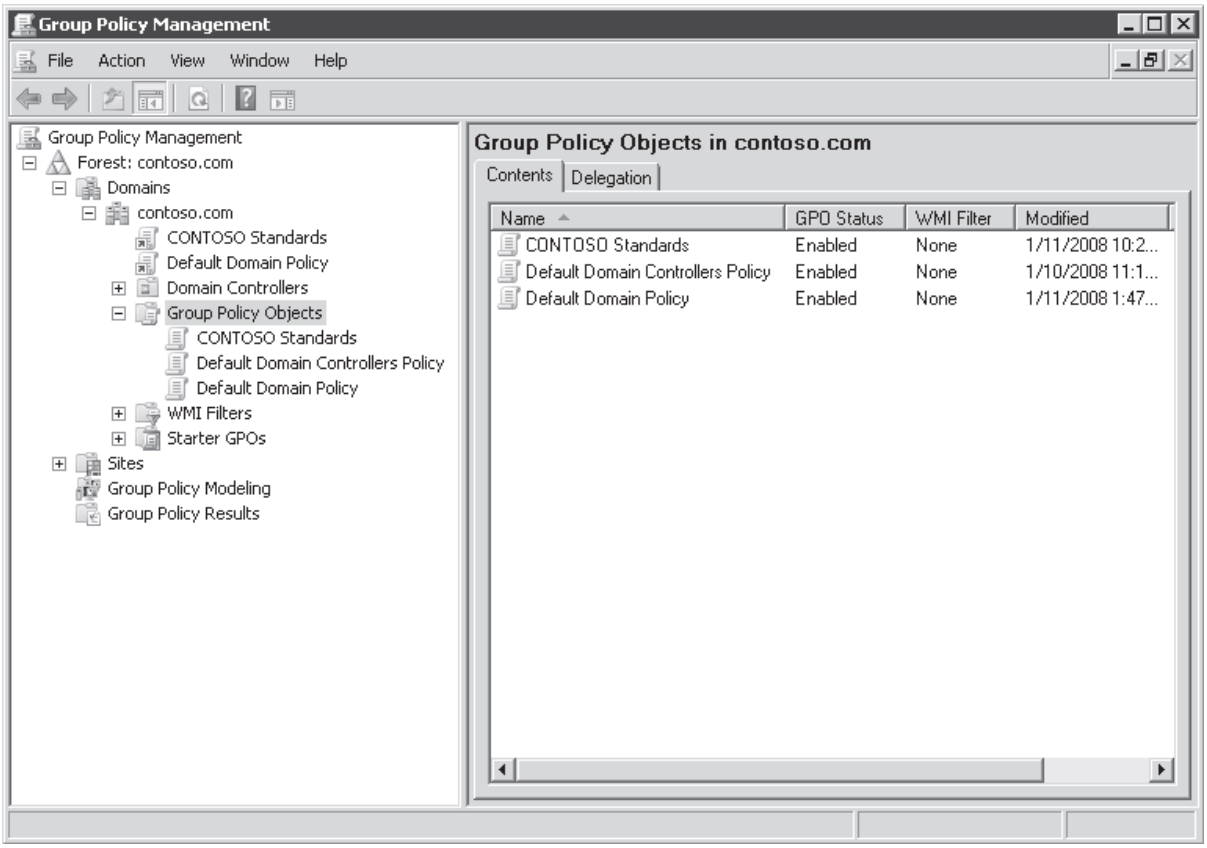
این دو مثال یک نکته مهم را نشان می‌دهد که بعضی از policy ها روی کاربر تاثیر می‌گذارند صرف نظر اینکه کاربر به چه کامپیوتری وارد شده است. برخی دیگر روی کامپیوتر اعمال می‌شوند صرف نظر از اینکه کدام کاربر به آن وارد شده است. عدم دسترسی کاربر به ابزار ویرایش رجیستری مثال حالت اول است که به آن تنظیمات پیکربندی کاربر یا به اختصار تنظیمات کاربر گفته می‌شود. غیرفعال کردن حساب Administrator نیز مثالی از حالت دوم است که به آن تنظیمات پیکربندی کامپیوتر یا تنظیمات کامپیوتر گفته می‌شود.

اشیاء Group Policy (GPOs)

تنظیمات policy در یک شیء Group Policy (GPO) تعریف و نگهداری می‌شود. GPO شیئی است که شامل یک یا چند تنظیم policy است و در نتیجه یک یا چند تنظیم را به روی کاربر یا کامپیوتر اعمال می‌کند.

ساخت ومدیریت GPO ها

GPO ها می‌توانند در Active Directory توسط کنسول Group Policy Management Console (GPMC)که در شکل ۱- ۶ نشان داده شده مدیریت شود. اینها در یک container به نام Group Policy Objects نمایش داده می‌شوند. روی آن کلیک راست کرده و گزینه New را برای ساخت یک GPO انتخاب می‌کنیم.

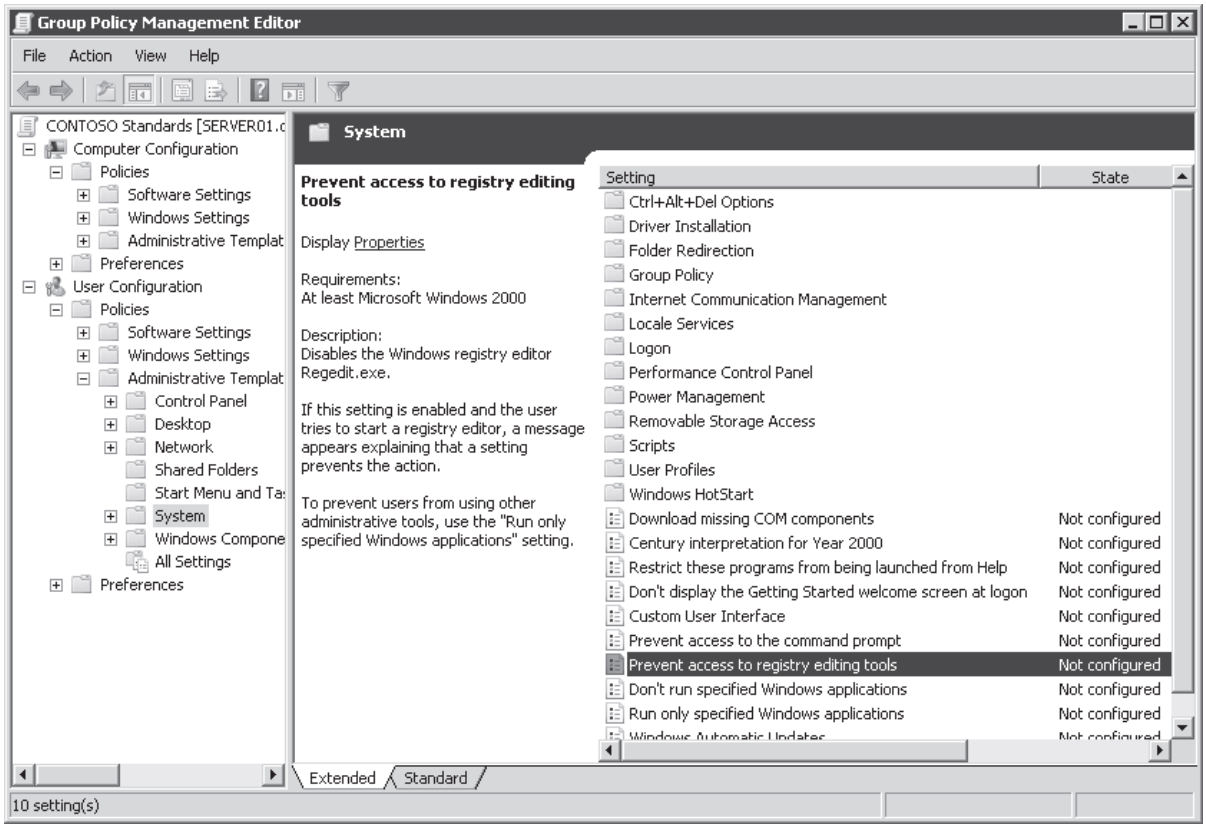


شکل ۱- ۶ کنسول Group Policy Management

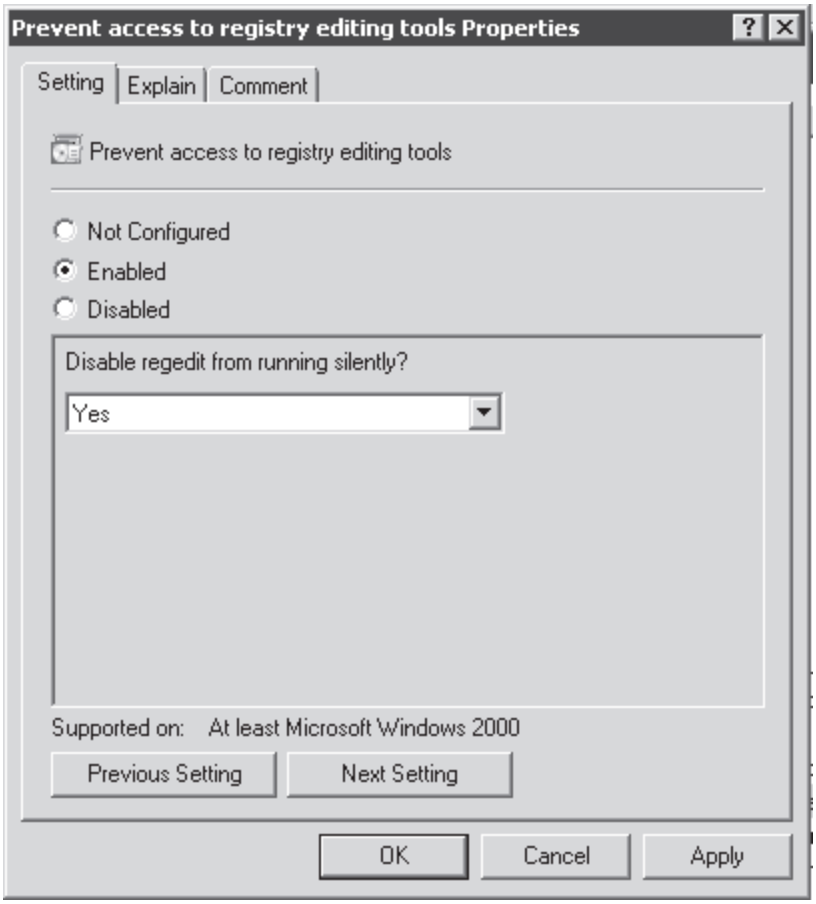
ویرایش GPO

جهت تغییر تنظیمات GPO روی آن کلیک راست کرده و Edit را انتخاب می‌کنیم. GPO همان‌طور که در شکل ۲- ۶ نشان داده شده است در ابزار Goup Policy Management Editor (GPME) باز می‌شود که قبلا به نام Group Policy Object Editor (GPO Editor) شناخته می‌شد.

GPME هزاران تنظیم policy را که در یک GPO موجود است در ساختار سلسله مراتبی نمایش می‌دهد که ابتدا آنها را به دو گروه تنظیمات کامپیوتر و تنظیمات کاربر تقسیم می‌کند. نام این دو گروه در کنسول Computer Configuration و User Configuration می‌باشد. سطح بعدی سلسله مراتب دو گره به نام‌های Policies و Preferences می‌باشد. هر چه در این درس جلوتر می‌رویم بیشتر در مورد تفاوت‌های این دو گروه یاد می‌گیریم. با عمق گرفتن بیشتر در ساختار، پوشه‌های GPME ظاهر می‌شوند که با نام گره یا گروه تنظیمات policy شناخته می‌شوند. در داخل پوشه‌ها تنظیمات Policy مربوط به گروه قرار دارند. تنظیم Prevent Access To Registry Editing Tools در شکل ۲- ۶ انتخاب شده است. برای تعریف یک Policy خاص روی تنظیم دوبار کلیک می‌کنیم. کادر محاوره‌ای Properties همان تنظیم مانند شکل ۳- ۶ ظاهر می‌شود.



شکل ۲- ۶ پنجره Group Policy Management Editor



شکل ۳- ۶ کادر محاوره‌ای Properties یک تنظیم Policy

پیکربندی تنظیم Policy

تنظیم policy سه حالت دارد. Not Configured، Enabled و Disabled. همان طور که در شکل ۲- ۶ می‌بینیم در یک GPO جدید همه تنظیمات در حالت Not Configured قرار دارند. این یعنی GPO تغییری در پیکربندی موجود آن تنظیم policy برای کاربر یا کامپیوتر ایجاد نخواهد کرد. وقتی تنظیم را فعال یا غیرفعال می‌کنیم تغییری در پیکربندی کاربران و کامپیوترهایی که GPO به آنها اعمال می‌شود به وجود می‌آید. تاثیر آن بستگی به خود تنظیم policy دارد. برای مثال اگر تنظیم Prevent Access To Registry Editing Tools را فعال کنیم کاربران قادر به اجرای ویرایشگر رجیستری Regedit.exe نخواهند بود. اگر همین تنظیم را غیرفعال کنیم مطمئن می‌شویم کاربران می‌توانند ویرایشگر رجیستری را اجرا کنند. به تاثیر دو عبارت منفی توجه کنید که برایند آنها مثبت خواهد شد یعنی وقتی عدم دسترسی به چیزی را غیرفعال می‌کنیم در واقع دسترسی را اعطاء می‌کنیم.

نکته همه تنظیمات را تست کرده و یاد بگیرید

بسیاری از تنظیمات پیچیده بوده و نتیجه فعال یا غیرفعال کردن آنها فورا مشخص نمی‌شود. همچنین برخی از تنظیمات روی نسخه‌های خاصی از ویندوز عمل می‌کنند. حتما متن توضیحی تنظیم را در پنل وسط که در شکل ۲- ۶ مشاهده می‌شود یا در زبانه Explain در کادر محاوره‌ای Properties تنظیم policy همانند شکل ۳- ۶ مرور کنید. به علاوه همیشه تاثیرات یک تنظیم policy و تعامل آن با تنظیمات دیگر را قبل از ایجاد تغییر در سازمان تست کنید.

بعضی تنظیمات مجموعه‌ای از تنظیم را دربر می‌گیرند و ممکن است نیاز به تنظیم پارامترهایی داشته باشند. در شکل ۳- ۶ می‌توانیم مشاهده کنیم که با فعال کردن تنظیم policy ممانعت از اجرای رجیستری که قبلا گفته شد همچنین می‌توان پارامتر دیگری را تنظیم کرد.

حوزه

پیکربندی توسط تنظیمات policy در اشیاء Group Policy تعریف می‌شود. تغییر پیکربندی در یک GPO تا زمانی که کامپیوترها و کاربرانی که GPO به آنها باید اعمال شود مشخص نشوند تاثیری ندارد. این یعنی تعیین حوزه GPO . حوزه یک GPO مجموعه کاربران و کامپیوترهایی است که تنظیمات GPO روی آنها اعمال می‌شود.

از روشهای زیادی برای مدیریت حوزه GPOs می‌توان استفاده کرد. اول لینک GPO است. GPO می‌تواند به سایت، دامنه و OU لینک شود. سایت، دامنه یا OU نهایت حوزه GPO خواهد شد. همه کامپیوترها و کاربران در سایت، دامنه یا OU شامل OU های فرزند تحت تاثیر پیکربندی‌های تعریف شده توسط تنظیمات GPO قرار می‌گیرند. یک GPO می‌تواند به یک یا چند سایت یا OU لینک شود.

در ادامه می‌توان حوزه GPO را با یکی از دو نوع فیلتر محدود کرد. یکی فیلترهای امنیتی که گروههای امنیتی global را که GPO باید یا نباید به آن اعمال شود مشخص می‌کند. دیگری فیلترهای Windows Management Instrumentation (WMI) که با استفاده از خصوصیات مشخص سیستم مانند نسخه سیستم عامل یا فضای خالی دیسک یک حوزه را تعیین می‌کند. از این دو فیلتر برای تعیین حوزه‌های کوچکتر در حوزه بزرگتر که توسط لینک GPO ساخته شده استفاده می‌شود. جزئیات حوزه‌بندی GPO ها در درس ۲ بررسی می‌شود.

برایند Policy ها (RSoP)

کامپیوترها و کاربران در حوزه یک GPO تنظیماتی را که در GPO مشخص می‌شود اعمال می‌کنند. یک کاربر یا کامپیوتر خاص ممکن است در حوزه‌های مختلف GPO های لینک شده به سایت‌ها، دامنه‌ها یا OU ها که شیء عضو آنهاست قرار بگیرد. از طرفی ممکن است تنظیمات در GPO های مختلف متفاوت باشد و ما باید بتوانیم برایند این تنظیمات را محاسبه و ارزیابی کنیم. RSoP در درس ۳ تشریح می‌شود.

اعمال تنظیمات Group Policy

تنظیمات policy کی اعمال می‌شود؟ تنظیمات policy در Computer Configuration موقع بوت شدن سیستم و پس از آن هر ۹۰ تا ۱۲۰ دقیقه یک بار و تنظیمات User Configuration هنگام ورود به سیستم و پس از آن هر ۹۰ تا ۱۲۰ دقیقه یک بار اعمال می‌شود. اعمال این تنظیمات را Group Policy refresh گویند.

اعمال تغییرات Group Policy به صورت دستی توسط دستور GPUpdate

وقتی با Group Policy کار می‌کنیم ممکن است بخواهیم به جای انتظار کشیدن برای اعمال تغییرات به طور خودکار ، سریعا نتیجه تغییرات را ببینیم. دستور Gpupdate.exe این کار را انجام می‌دهد. این دستور هم پیکربندی کامپیوتر و هم پیکربندی کاربر را اعمال می‌کند. برای اعمال تغییرات فقط کامپیوتر از سوئیچ /target:computer و فقط کاربر از /target:user می‌توان استفاده کرد. اعمال پیکربندی خودکار سیستم فقط زمانی اتفاق می‌افتد که GPO تغییر کرده باشد. سوئیچ /force باعث اعمال دوباره همه GPO ها می‌شود چه تغییر کرده باشد چه نکرده باشد. بعضی تنظیمات Policy حتما نیاز به خروج یا راه‌اندازی مجدد برای اعمال تغییرات دارند. در این موارد از سوئیچ /logoff و /boot به ترتیب برای خروج و راه‌اندازی مجدد سیستم در دستور Gpupdate.exe استفاده می‌شود. در ویندوز 2000 برای اعمال تغییرات از دستور Secedit.exe استفاده می‌شد که دانستن آن برای امتحان لازم است.

کلاینت Group Policy و Extension های سمت کلاینت

تنظیمات policy چگونه اعمال می‌شوند؟ وقتی اعمال تغییرات Group policy شروع می‌شود سرویسی روی همه سیستم‌ها (در ویندوز ویستا و سرور 2008 کلاینت Group policy نامیده می‌شود) اجرا می‌شود که تعیین می‌کند کدام GPO ها باید روی کامپیوتر یا کاربر اعمال شود. سپس GPO هایی را که در cache موجود نیست دانلود می‌کند. بعد یک سری پروسه به نام Extension های سمت کلاینت (CSE) کار تفسیر تنظیمات GPO و ایجاد تغییرات لازم را روی کامپیوتر محلی یا کاربر تازه وارد شده به سیستم انجام می‌دهند. برای هر گروه اصلی تنظیمات policy یک CSE موجود است. برای مثال یک CSE تغییرات امنیتی را اعمال می‌کند، یک CDE اسکریپت‌های logon و startup را اجرا می‌کند، یک CSE نرم‌افزار نصب می‌کند و یک CSE مقادیر و کلیدهای رجیستری را تغییر می‌دهد. ویندوز نسخه به نسخه CSE ها را برای عملیات Group policy توسعه بخشیده است. حالا در ویندوز سرور 2008 دهها CSE وجود دارد. یکی از مهم‌ترین مفاهیمی که باید بدانیم این است که Group policy در اصل یک پروسه سمت کلاینت است. GPO از سمت سرور به کلاینت ارسال (push) نمی‌شود بلکه کلاینت Group policy خود از دامنه GPO را دریافت (pull) و CSE ها را برای اعمال آن اجرا می‌کند.

رفتار CSE ها در واقع می‌تواند توسط Group Policy پیکربندی شود. بیشتر CSE ها تنظیمات GPO را فقط زمانی که تغییر می‌کند اعمال می‌کنند. این رفتار با حذف برنامه‌های تکراری با تنظیمات یکسان باعث بهینه شدن پردازش تنظیمات می‌شود. بیشتر policy ها طوری اعمال می‌شود که کاربران استاندارد نتوانند تنظیمات سیستم‌شان را تغییر دهند و همیشه پیکربندی Group Policy اجباری باشد. برخی از تنظیمات توسط کاربر استاندارد قابل تغییر هستند و بسیاری نیز فقط توسط کاربران گروه Administrator سیستم تغییر می‌یابند. وقتی کاربران شبکه روی سیستم خودشان در سطح Administrator هستند CSE ها را باید طوری پیکربندی کنیم که تنظیمات policy حتی اگر GPO تغییر نکند دوباره اعمال شوند. با این کار اگر کاربر پیکربندی سیستم خودش را تغییر دهد به صورتی که دیگر از Group Policy تبعیت نکند پیکربندی در اعمال Group Policy در زمان‌های پیش فرض به حالت اولیه خود برمی‌گردد.

نکته CSE ها را طوری پیکربندی کنیم که حتی اگر GPO تغییر نکند تنظیمات دوباره اعمال شود.

برای این کار یک GPO را در حوزه کامپیوترهای مورد نظر پیکربندی کرده و تنظیمات گره Computer Configuration\Policies\Administrative Templates\System\ Group Policy را تعریف می‌کنیم. هر CSE را که می‌خواهیم پیکربندی کنیم تنظیم مربوط به همان policy را باز می‌کنیم. مثلا Registry Policy Processing برای Registry CSE . دکمه Enabled را کلیک کرده و کادر Process Even If The Group Policy Objects Have Not Changed را علامت می‌زنیم.

یک استثنا مهم برای تنظیمات policy processing پیش فرض، تنظیمات تعیین شده توسط Security CSE است. تنظیمات امنیتی هر ۱۶ ساعت یکبار حتی اگر GPO تغییرنکند دوباره اعمال می‌شود.

نکته تنظیم The Always Wait For Network At Startup And Logon

اکیدا توصیه می‌شود که این گزینه برای ویندوزهای XP و ویستا فعال شود. بدون این تنظیم به طور پیش فرض ویندوز اعمال تغییرات را در پشت صحنه انجام می‌دهد یعنی بدون دریافت آخرین policy ها از دامنه کلاینت می‌تواند بوت شده و کاربر می‌تواند به سیستم وارد شود. تنظیم در Computer Configuration\Policies\Administrative Templates\System\Logon واقع شده است. متن توضیحی تنظیم را حتما بخوانید.

ارتباطات کند و سیستم‌های خارج از شبکه

یکی از کارهایی که با Group Policy می‌تواند خودکارسازی و مدیریت شود نصب نرم‌افزار است. Group Policy Software Installation (GPSI) توسط CSE نصب نرم‌افزار پشتیبانی می‌شود. می‌توانیم یک GPO را برای نصب یک یا چند بسته نرم‌افزاری پیکربندی کنیم. تصور کنید اگر ارتباط کاربری با شبکه کند باشد نمی‌توانیم نرم‌افزارهای سنگین را روی شبکه برای آن کاربر ارسال کنیم.

کلاینت Group Policy این مشکل را حل کرده است به طوری که سرعت ارتباط به دامنه را چک می‌کند و تشخیص می‌دهد که ارتباط کند است. این تحقیق توسط همه CSE ها مورد استفاده قرار می‌گیرد تا در مورد اعمال تنظیمات تصمیم‌گیری کنند. برای مثال CSE نصب نرم‌افزار پیکربندی شده که اگر سرعت ارتباط پایین بود نرم‌افزار نصب نشود. به طور پیش فرض سرعت ارتباط کمتر از 500 Kbps کند محسوب می‌شود.

اگر کاربری بدون اتصال به شبکه شروع به کار کند آخرین تنظیماتی که توسط Group Policy اعمال شده باز اعمال می‌شود بنابراین کاربر متوجه تغییری در این زمینه نمی‌شود. برای این قانون چند استثنا وجود دارد. مهم‌ترین آنها اسکریپت‌های logon، logoff، startup و shutdown است که وقتی کاربر به شبکه متصل نیست اجرا نمی‌شوند.

وقتی کاربر راه دور از طریق ویندوز ویستا یا سرور 2008 دوباره به شبکه متصل شود کلاینت Group Policy فعال شده و تعیین می‌کند که آخرین بار دریافت Group Policy با مشکل مواجه شده و بنابراین آخرین GPO را از دامنه دریافت می‌کند. سپس CSE ها اعمال تنظیمات را در این GPO ها چک می‌کنند.

اشیاء Group Policy

حالا که آشنایی خوبی با Group Policy و اجزاء آن پیدا کردیم نگاهی دقیق‌تر به اجزاء آن می‌اندازیم. در این بخش جزئیات GPO ها بررسی می‌شود. ما برای مدیریت پیکربندی کاربران و کامپیوترها GPO هایی می‌سازیم که تنظیمات مورد نظر ما را در خود دارد. تمام کامپیوترها GPO های متعددی دارند که روی خود سیستم ذخیره می‌شوند و می‌توانند در حوزه هر تعداد از GPO های بر دامنه قرار گیرند.

GPO های محلی

کامپیوترهایی که سیستم عامل ویندوز 2000، XP و سرور 2003 دارند دارای GPO محلی هستند که پیکربندی سیستم را مدیریت می‌کند. GPO های محلی صرف نظر از اینکه کامپیوتر عضو دامنه باشد یا workgroup یا حتی در شبکه نباشد حضور دارند. محل ذخیره آنها %SystemRoot%\System32\GroupPolicy می‌باشد. تنظیمات آن فقط روی خود کامپیوتر تاثیرگذار است. به طور پیش فرض فقط تنظیمات امنیتی روی GPO محلی سیستم پیکربندی می‌شود و بقیه تنظیمات به حالت Not Configured باقی می‌ماند.

وقتی کامپیوتری عضو دامنه نیست policy محلی برای پیکربندی مفید واقع می‌شود. در دامنه تنظیمات در GPO ها که به سایت، دامنه یا OU لینک می‌شود بر تنظیمات GPO محلی غلبه می‌کند و البته مدیریت آن راحت‌تر از GPO محلی اختصاصی برای هر کامپیوتر است.

ویندوز ویستا و سرور 2008 تعداد زیادی GPO محلی دارند. این GPO ها نظیر همتاهایشان در نسخه‌های قدیمی ویندوز است. در گره Computer Configuration همه تنظیمات مرتبط با کامپیوتر را پیکربندی می‌کنیم. در گره User Configuration تنظیماتی که می‌خواهیم به همه کاربران کامپیوتر اعمال شود پیکربندی می‌کنیم. تنظیمات کاربر در Local Computer GPO توسط تنظیمات کاربر در دو GPO محلی جدید قابل تغییر است. یکی Administrators و دیگری Non-Administrators . اولی تنظیمات کاربر را روی کاربر وارد شده به سیستم که عضو گروه Administrators است اعمال می‌کند و دومی روی کاربری که عضو این گروه نیست. همچنین می‌توانیم تنظیمات دقیق‌تری را با GPO محلی که روی یک کاربر خاص اعمال می‌شود انجام دهیم. GPO های محلی مخصوص کاربر با کاربران محلی عجین شده است نه با کاربران دامنه.

RSoP برای تنظیمات کامپیوتر ساده است چون Local Computer GPO تنها GPO محلی است که می‌تواند تنظیمات کامپیوتر را اعمال کند. تنظیمات کاربر در یک GPO مخصوص کاربر بر تنظیمات موجود در GPO های Administrative و Non-

Administrative غلبه می‌کند در حالی که خودشان بر تنظیمات Local Computer GPO برتری دارند. مفهوم ساده است: هرچه GPO محلی خاص‌تر باشد اولویت آن بالاتر است.

به منظور ساخت و ویرایش GPO های محلی روی منوی start کلیک می‌کنیم و در کادر Start Search تایپ می‌کنیم mmc.exe . یک کنسول خالی باز می‌شود. منوی File را باز کرده و Add/Remove Snap-in را انتخاب می‌کنیم. Group Policy Object Editor را انتخاب کرده و Add را کلیک می‌کنیم. کادر محاوره‌ای باز می‌شود که امکان انتخاب GPO را برای ویرایش می‌دهد. به طور پیش فرض Local Computer GPO انتخاب شده است. اگر بخواهیم GPO محلی دیگری را ویرایش کنیم دکمه Browse را کلیک می‌کنیم. در زبانه Users می‌توانیم GPO های Non-Administrative و Administrative و یک GPO برای هر کاربر محلی را پیدا کنیم. GPO را انتخاب و OK می‌کنیم. دکمه Finish و سپس OK را کلیک می‌کنیم تا همه کادرها بسته شوند. ویرایشگر Group Policy Object با تمرکز روی GPO انتخاب شده به کنسول افزوده می‌شود.

به خاطر داشته باشید GPO های محلی برای محیط‌های دامنه طراحی نمی‌شوند. این اشیاء در کامپیوتر خانگی برای مدیریت تنظیمات استفاده می‌شود. تنظیمات GPO های دامنه که با GPO های محلی تداخل دارند بر آنها غلبه می‌کنند و بنابراین راه مناسبی برای مدیریت تنظیمات می‌باشد.

GPO های مبتنی بر دامنه

این نوع از GPO ها در Active Directory ساخته شده و روی DC ها ذخیره می‌شوند. این اشیاء به منظور مدیریت پیکربندی کاربران و کامپیوترهای دامنه به طور متمرکز استفاده می‌شوند. در ادامه کتاب هر جا نوع GPO ذکر نشود منظور نوع دامنه‌ای آن است. وقتی AD DS نصب می‌شود دو GPO پیش فرض ساخته می‌شود:

- **Default Domain Policy** این GPO به دامنه لینک می‌شود و هیچ فیلتری اعم از گروه امنیتی یا WMI ندارد. بنابراین روی همه کاربران و کامپیوترهای دامنه (حتی DC ها) تاثیر می‌گذارد. این GPO دارای تنظیماتی می‌باشد که policy های مربوط به کلمه عبور، account lockout و Kerberos را تعیین می‌کند. همانطور که در فصل ۸ "تایید هویت" بحث می‌شود تنظیمات فعلی را برای همسو کردن سیاست‌های کلمه عبور و account lockout policy تغییر می‌دهیم ولی تنظیمات غیرمرتبط را به این GPO اضافه نمی‌کنیم. اگر بخواهیم تنظیمات دیگری را برای حوزه وسیع‌تری پیکربندی کنیم یک GPO ساخته و آنرا به دامنه لینک می‌دهیم.

- **Default Domain Controllers Policy** این GPO به Domain Controllers OU لینک می‌شود چون حساب کامپیوترهای DC به طور اختصاصی در Domain Controllers OU و دیگر کامپیوترها در OU های دیگر نگهداری می‌شوند این GPO روی DC ها تاثیر می‌گذارد. GPO پیش فرض DC ها برای پیاده‌سازی سیاست‌های ممیزی که در فصل ۷ و ۸ بررسی خواهد شد بهتر است تغییر یابند. همچنین این GPO می‌تواند برای اعطاء حقوق مورد نیاز کاربر روی DC ها تغییر یابد.

ساخت، لینک دادن و ویرایش GPO

برای ساخت GPO روی Group Policy Object container کلیک راست کرده و New را انتخاب می‌کنیم. البته باید مجوز ساخت GPO را در این container داشته باشیم.

به طور پیش فرض گروههای Domain Admins و Group Policy Creator Owners دارای مجوز ساخت GPO هستند. به منظور اعطاء این مجوز به گروههای دیگر Group Policy Objects container در کنسول GPME را انتخاب می‌کنیم و زبانه Delegation را در پنل وسط کنسول کلیک می‌کنیم.

پس از ساخت GPO می‌توانیم حوزه اولیه آنرا با لینک کردن آن به یک سایت، دامنه یا OU مشخص کنیم. برای لینک کردن GPO روی container کلیک راست کرده و گزینه Link An Existing GPO را انتخاب می‌کنیم. توجه داشته باشید که سایت‌ها در گره Sites نمایش داده نمی‌شود مگر اینکه روی Sites کلیک راست کرده و Show Sites را انتخاب کنیم. بعد می‌توانیم سایت مورد نظر

را کلیک کنیم. همچنین می‌توان با یک مرحله یک GPO ساخته و آنرا لینک کنیم. این کار با کلیک راست روی سایت، دامنه یا OU و انتخاب Create A GPO In This Domain And Link It Here انجام می‌شود.

برای لینک کردن GPO ما باید مجوز لازم را داشته باشیم. در کنسول GPMC در ساختار درختی کنسول container مورد نظر را انتخاب کرده و در پنل وسط کنسول زبانه Delegation را کلیک می‌کنیم. از لیست بازشوی Permission گزینه Link GPOs را انتخاب می‌کنیم.کاربران و گروههای دارای مجوز OU انتخاب شده را نشان می‌دهد. دکمه‌های Add یا Remove را برای تغییر مجوزها کلیک می‌کنیم.

برای ویرایش GPO در Group Policy Objects container روی GPO کلیک راست کرده و Edit را انتخاب می‌کنیم. GPO در GPME باز می‌شود. برای باز کردن GPO حداقل دسترسی Read مورد نیاز است. برای ایجاد تغییرات باید مجوز Write به GPO داشته باشیم. مجوزهای GPO با انتخاب آن در Group Policy Objects container و سپس کلیک روی زبانه Delegation در پنل وسط می‌تواند تنظیم شود.

GPME نام GPO را به عنوان گره ریشه نمایش می‌دهد. GPME همچنین دامنه‌ای که GPO در آن تعریف شده و سروری که از روی آن GPO باز شده و تغییرات روی آن ذخیره می‌شود نشان می‌دهد. گره ریشه به شکل GPOName[ServerName] نمایش می‌یابد. در شکل ۲- ۶ گره ریشه CONTOSO Standards[SERVER01.contoso.com] Policy می‌باشد. نام GPO، CONTOSO Standards بوده و از سرور Server01.contoso.com باز شده به این معنی که GPO در دامنه contoso.com تعریف شده است.

انباره GPO

تنظیمات Group Policy در ابزار Active Directory به عنوان GPO حضور دارند ولی GPO در واقع دو جزء دارد: Group Policy Container (GPC) و Group Policy Template (GPT). GPC یک شیء است که در Group Policy Objects container در فضای نام دامنه ذخیره می‌شود. همانند دیگر اشیاء GPC خصیصه globally unique identifier (GUID) دارند که مشخصه انحصاری اشیاء در دایرکتوری می‌باشند. GPC خصیصه‌های اساسی GPO را تعریف می‌کند ولی هیچ کدام از تنظیمات را دربر نمی‌گیرد. تنظیمات در GPT ذخیره می‌شوند و مجموعه‌ای از فایل‌های ذخیره شده در پوشه SYSVOL همه DC ها در مسیر %SystemRoot%\SYSVOL\Domain\Policies\GPO GUID می‌باشد که GPO GUID در واقع GUID مربوط به GPO است. وقتی تنظیمات GPO را تغییر می‌دهیم تغییرات در GPT سروری که GPO از روی آن باز شده ذخیره می‌شود.

به طور پیش فرض CSE ها تنظیمات GPO را زمانی اعمال می‌کنند که تغییر کرده باشد. کلاینت Group Policy از روی شماره نسخه GPO متوجه تغییرات می‌شود. هر GPO شماره نسخه‌ای دارد که پس از هر تغییری یک شماره افزایش می‌یابد. شماره نسخه به عنوان یک خصیصه GPC در یک فایل متنی به نام GPT.ini در پوشه GPT ذخیره می‌شود. کلاینت Group Policy شماره نسخه GPO که آخرین بار اعمال شده می‌داند. در زمان به روز رسانی Group Policy، کلاینت تشخیص می‌دهد که شماره نسخه تغییر کرده و CSE ها را متوجه خواهد کرد.

تکثیر GPO

هر دو بخش GPO توسط مکانیزم‌های جداگانه‌ای روی DC ها تکثیر می‌شوند. GPC در Active Directory توسط Directory Replication Agent (DRA) با استفاده از توپولوژی که توسط Knowledge Consistency Checker (KCC) ساخته می‌شود تکثیر می‌شود. در فصل ۱۱ درباره این سرویس‌ها بیشتر یاد می‌گیریم. نتیجه این می‌شود که GPC در عرض چند ثانیه روی همه DC ها در سایت و بین سایت‌ها بسته به پیکربندی تکثیر بین سایتی موجود تکثیر می‌شود. این بحث نیز در فصل ۱۱ مطرح می‌شود.

GPT موجود در SYSVOL با یکی از روش‌ها تکثیر می‌شود. سرویس File Replication Service (FRS) برای تکثیر SYSVOL در دامنه‌های ویندوز سرور 2008 ، 2003 و 2000 استفاده می‌شود. وقتی سیستم عامل همه DC ها ویندوز سرور 2008 است مکانیزم موثرتر و قوی‌تری به نام Distributed File System Replication (DFS-R) می‌تواند برای تکثیر SYSVOL استفاده شود.

به دلیل اینکه GPT و GPC به طور جداگانه تکثیر می‌شوند این احتمال پیش می‌آید که برای مدت کوتاهی بین این دو ناهماهنگی به وجود آید. وقتی این اتفاق می‌افتد GPC ابتدا روی DC تکثیر می‌شود. سیستم‌هایی که لیست مرتب شده GPO های خود را از آن DC دریافت می‌کنند GPC جدید را تشخیص می‌دهند و سپس GPT را دانلود کرده و خواهند دید که شماره نسخه‌ها مساوی نیستند. در این حالت خطایی در event logs ثبت می‌شود. بالعکس اگر GPO قبل از GPC به دامنه تکثیر شود کلاینت‌هایی که لیست مرتب شده GPO ها را از DC دریافت می‌کنند از نسخه جدید GPO آگاه نمی‌شوند مگر GPC تکثیر شود.

ابزار Group Policy Verification Tool (Gpotool.exe) که بخشی از Windows Resource Kits می‌باشد از Microsoft Download Center قابل دانلود است. این ابزار وضعیت GPO را در دامنه را گزارش می‌دهد و می‌تواند تفاوت نسخه‌های GPT و GPC را تشخیص دهد. برای اطلاعات بیشتر درباره Gpotool.exe دستور gpotool /? را در خط فرمان تایپ می‌کنیم.

نکته امتحانی دستور Gpotool.exe برای عیب‌یابی وضعیت GPO استفاده می‌شود. از جمله ایرادات آن می‌توان به عدم تطابق نسخه‌های GPC و GPT اشاره کرد که دلیل آن تکثیر GPO ها به صورت مجزا می‌باشد.

تنظیمات Policy

تنظیمات Group Policy یا همان Policies در GPO قرار دارند و با GPME قابل رویت و تغییر می‌باشند. در این بخش نگاه دقیق‌تری به انواع تنظیمات در GPO می‌اندازیم.

تنظیمات کامپیوتر و تنظیمات کاربر

دو بخش اصلی تنظیمات Policy، تنظیمات کامپیوتر و تنظیمات کاربر هستند. این دو به ترتیب در گره‌های Computer Configuration و User Configuration هستند. تنظیمات Computer Configuration صرف نظر از اینکه چه کسی به سیستم وارد می‌شود روی کامپیوترها اعمال می‌شود. زمان اعمال این تنظیمات بوت شدن سیستم عامل بوده و پس از آن در پشت صحنه هر ۹۰ تا ۱۲۰ دقیقه یک بار به روز می‌شود. گره User Configuration تنظیماتی را شامل می‌شود که هنگام ورود کاربر به کامپیوتر اعمال می‌شود و پس از آن هر ۹۰ تا ۱۲۰ دقیقه به روز می‌شود.

در هر دو گره، گره‌های دیگری با نام‌های Policies و Preferences قرار دارند. Policies تنظیماتی است که پیکربندی شده و رفتار آن شبیه تنظیمات Policy ویندوزهای قبلی است. Preferences در ویندوز سرور 2008 معرفی شده است. بخش‌های بعدی این گره‌ها را بررسی می‌کند.

گره Software Settings

در گره‌های Policies در Computer Configuration و User Configuration ساختار پوشه‌ای سلسله مراتبی در برگیرنده تنظیمات policy قرار دارد. به دلیل وجود هزاران تنظیم عملا امکان تست همه تنظیمات در این کتاب وجود ندارد و فقط گروههای مهم تنظیمات در پوشه‌ها بررسی می‌شود. اولین آنها گره Software Settings است که فقط شامل Software Installation Extension است. این بخش به ما امکان می‌دهد مشخص کنیم برنامه‌ها چطور نصب و نگهداری شوند. همچنین مکانی برای تولیدکنندگان نرم‌افزار مستقل فراهم می‌کند تا تنظیمات خود را اضافه کنند. توزیع نرم‌افزار توسط Group Policy در فصل ۷ بحث می‌شود.

گره Windows Settings

در هر دو گره Computer Configuration و User Configuration گره Policies شامل گره Windows Settings است که گره‌های Scripts، Security Settings و Policy-Based Qos را دربر می‌گیرد.

گره Scripts امکان تعیین دو نوع اسکریپت را محیا می‌کند: یکی startup/shutdown در گره Computer Configuration و دیگری logon/logoff در گره User Configuration . اسکریپت‌های startup/shutdown هنگام بوت و خاموش شدن کامپیوتر اجرا می‌شوند و اسکریپت‌های logon/logoff وقتی کاربر به سیستم وارد یا از آن خارج می‌شود اجرا می‌شود. وقتی چند اسکریپت را به کاربر یا کامپیوتر انتساب می‌دهیم scripts CSE آنها را از بالا به پایین اجرا می‌کند. امکان تعیین ترتیب اجرای اسکریپت‌های متعدد در کادر محاوره‌ای Properties وجود دارد. وقتی کامپیوتری خاموش می‌شود ابتدا CSE اسکریپت‌های logoff را پردازش می‌کند و سپس اسکریپت‌های shutdown را اجرا می‌کند. به طور پیش فرض مقدار انتظار (timeout) پردازش اسکریپت ۱۰ دقیقه است. اگر

اسکریپت‌های مذکور به بیش از ۱۰ دقیقه زمان نیاز داشته باشند باید مقدار انتظار را در policy تنظیم کنیم. ما می‌توانیم از هر زبان اسکریپت‌نویسی Activex برای نوشتن اسکریپت استفاده کنیم. برخی از این زبان‌ها Microsoft Visual Basic، Scripting Edition (VBScript)، Microsoft Jscript، Perl و فایل‌های دسته‌ای (batch files) تحت DOS (bat. و cmd.) می‌باشند.
اسکریپت‌های logon روی یک دایرکتوری به اشتراک‌گذاشته شده در forest می‌تواند از forest های دیگر اجرا شود.
گره Security Settings به مدیر امنیت امکان پیکربندی امنیتی با استفاده از GPO را فراهم می‌کند. این کار به جای یا بعد از اعمال الگوی امنیتی انجام می‌شود. جزئیات بیشتر درباره امنیت سیستم و گره Security Settings به فصل ۷ مراجعه کنید.
گره Policy-Based QoS تنظیماتی را تعریف می‌کند که ترافیک شبکه را مدیریت می‌کند. برای مثال ممکن است بخواهیم کاربران بخش مالی در اجرای یک برنامه ضروری تحت شبکه اولویت بالاتری نسبت به بقیه کارکنان داشته باشند.
فقط در گره User Configuration پوشه Windows Settings شامل گره‌های دیگری چون Remote Installation Services، Folder Redirection و Internet Explorer Maintenance می‌باشد.
Policy های Remote Installation Services (RIS) رفتار نصب از راه دور سیستم عامل را که توسط RIS انجام می‌شود کنترل می‌کند. Folder Redirection به ما امکان می‌دهد مسیر ذخیره پوشه های تنظیمات و داده کاربر را (برای مثال AppData,Desktop,Documents,Pictures,Music,Favorites) از محل پروفایل پیش فرض کاربر به محلی دیگر در شبکه تغییر دهیم جایی که بتوانیم به صورت مرکزی آنها را کنترل کنیم. Internet Explorer Maintenance امکان مدیریت و سفارشی کردن Internet Explorer را فراهم می‌کند.

گره Administrative Templates

این گره هم در Computer Configuration و هم در User Configuration دارای تنظیمات Group Policy مبتنی بر رجیستری می‌باشد.این تنظیمات به چند هزار عدد می‌رسد. به عنوان یک مدیر شبکه ما بیشتر با این سری تنظیمات کار داریم. برای راهنمایی درباره هر تنظیم توضیح هر تنظیم در دو محل در دسترس است:

- در زبانه Explain کادر محاوره‌ای Properties هر تنظیم. به علاوه زبانه Settings در کادر محاوره‌ای Properties هر تنظیم، سیستم عامل یا برنامه مورد نیاز تنظیم را لیست می‌کند
- در زبانه Extended از GPME. این زبانه در پایین و سمت راست پنل وسط جای دارد و توضیح هر تنظیم را در ستونی بین ساختار درختی کنسول و پنل تنظیمات فراهم می‌کند. سیستم عامل یا نرم‌افزار مورد نیاز تنظیم هم لیست می‌شود.

گره Administrative Templates به تفصیل در بخش دیگری بحث می‌شود.

گره Preferences

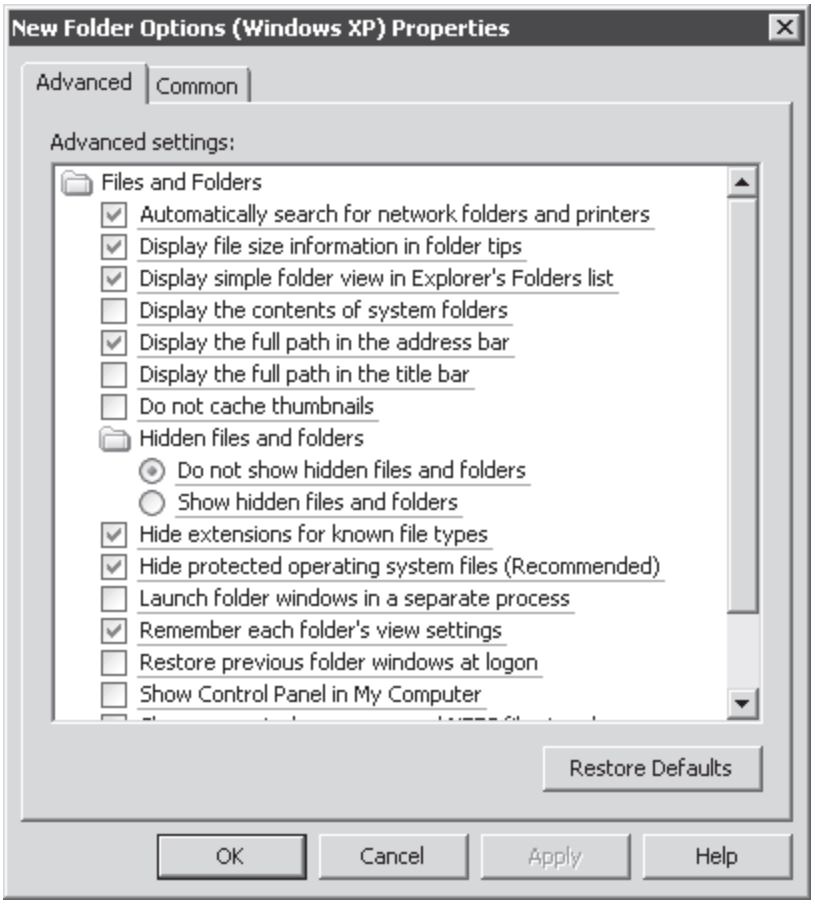
زیر گره‌های Computer Configuration و User Configuration گره Preferences حضور دارد. در ویندوز سرور 2008 این بخش بیش از ۲۰ CSE را برای کمک به ما در مدیریت هر تعداد تنظیمات فراهم می‌کند. تعدادی از این تنظیمات لیست شده اند:

- برنامه‌هایی نظیر Microsoft Office 2003,2007
- درایوهای نگاشت شده (Mapped drives)
- تنظیمات رجیستری
- Power Options
- Folder Options
- Regional Options
- گزینه‌های منوی شروع

Preferences همچنین ما را در توزیع موارد زیر یاری می‌کند:

- فایل‌ها و پوشه‌ها
- پرینترها
- وظایف زمان‌بندی شده
- اتصالات شبکه

بسیاری از سازمان‌ها به دلیل امکان فعال یا غیرفعال کردن قطعات سخت‌افزاری در این بخش از آن استفاده می‌کنند. برای مثال از Preferences می‌توان برای جلوگیری از اتصال Player ها و هارد دیسک‌های USB به کامپیوتر بهره برد.
نسخه جدید GPME برای ویندوز ویستا سرویس پک ۱ که از پیکربندی Preferences پشتیبانی می‌کند از آدرس http://www.microsoft.com/downloads قابل دانلود است. سیستم‌ها برای اعمال Preferences به preferences CSE ها نیاز دارند که در ویندوز سرور 2008 موجود است. CSE های ویندوز XP، ویندوز سرور 2003 و ویندوز ویستا از Microsoft Download Center قابل قابل دانلود است.
رابط کاربری که ما برای پیکربندی preferences استفاده می‌کنیم شبیه رابط کاربری ویندوز است که در آن به صورت دستی تغییرات را انجام می‌دهیم. شکل ۴- ۶ آیتم Folder Options preference را در ویندوز XP نشان می‌دهد که در واقع مجموعه‌ای از تنظیماتی است که توسط preferences CSE پردازش می‌شود. تشابه این پنجره با برنامه Folder Options در Control Panel مشهود است.



شکل ۴- ۶ یک آیتم Folder Options preference

گره Administrative Templates

Policy ها در گره Administrative Templates در گره Computer Configuration مقادیر رجیستری را در کلید HKEY_LOCAL_MACHINE (HKLM) تغییر می‌دهند و Policy ها در گره Administrative Templates در گره User Configuration مقادیر رجیستری را در کلید HKEY_CURRENT_USER (HKCU) تغییر می‌دهند. بیشتر مقادیر رجیستری که توسط POLICY های پیش فرض تغییر می‌کنند در یکی از چهار شاخه زیر واقع شده‌اند:

- HKLM\Software\Policies (تنظیمات کامپیوتر)
- HKCU\Software\Policies (تنظیمات کاربر)
- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies (تنظیمات کامپیوتر)
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies (تنظیمات کاربر)

یک الگوی مدیریتی (administrative template) فایلی متنی است که تغییر مورد نیاز رجیستری را مشخص می‌کند و رابط کاربری را برای پیکربندی تنظیمات الگوی مدیریتی در GPME می‌سازد. شکل ۳- ۶ کادر محاوره‌ای properties مربوط به Prevent Access To Registry Editing Tools را نشان می‌دهد. تنظیمات از قبل موجود است و فقط لیست بازشو انتخاب می‌شود. این تنظیم رجیستری در الگوی مدیریتی نیز تعریف می‌شود.

با کلیک راست روی گره Administrative Templates و انتخاب Add/Remove Templates می‌توانیم یک الگوی مدیریتی جدید به GPME اضافه کنیم. برخی از تولیدکنندگان نرم‌افزار الگوهای مدیریتی را به عنوان روشی برای مدیریت متمرکز نرم‌افزار فراهم می‌کنند. به عنوان مثال می‌توانیم الگوهای مدیریتی را برای همه نسخه‌های آفیس از مرکز دانلود مایکروسافت دانلود کنیم. همچنین می‌توانیم الگوی سفارشی خود را بسازیم. آموزش ساخت این الگوهای سفارشی از حوزه این کتاب خارج است.

در نسخه‌های قبل از ویندوز ویستا الگوهای مدیریتی دارای پسوند adm. بودند. فایل‌های ی ADM دارای اشکالات زیادی می‌باشد. مثلا وقتی بخواهیم یک فایل ADM برای توزیع پیکربندی در یک سازمان چند زبانی بسازیم به فایل‌های ADM جداگانه برای هر زبان نیاز داریم تا رابط کاربری مدیران را که با زبان‌های مختلف صحبت می‌کنند فراهم کنیم. بعدا اگر بخواهیم در تنظیمات رجیستری که با الگوها مدیریت می‌شوند تغییراتی دهیم باید این تغییرات را در همه فایل‌های ADM اعمال کنیم.

مشکل دیگر در مورد این فایل‌ها روش ذخیره شدن آنهاست. فایل ADM به عنوان بخشی از GPT در SYSVOL ذخیره می‌شود. وقتی یک فایل ADM در GPO های مختلف استفاده می‌شود چندین بار ذخیره می‌شود که خود باعث حجیم شدن SYSVOL می‌شود. همچنین مشکلاتی در مورد نسخه فایل‌های ADM وجود داشت.

در ویندوز ویستا و سرور 2008 یک الگوی امنیتی دو عد فایل XML است که یکی دارای پسوند admx. و دیگری adml. می‌باشد. فایل اول تغییرات مورد نظر روی رجیستری را مشخص می‌کند و دومی رابط کاربری با زبان مشخص را در GPME فراهم می‌کند. وقتی نیاز به تغییرات روی تنظیمات اعمال شده توسط الگوی مدیریتی داریم این تغییرات را روی یک فایل ADMX انجام می‌دهیم. هر مدیر شبکه‌ای که یک GPO را که از الگو استفاده می‌کند تغییر می‌دهد به همان فایل ADMX دسترسی پیدا می‌کند و فایل ADML مناسب را برای فراهم کردن رابط کاربری فراخوانی می‌کند.

تکته نیازی به جدا کردن نیست

الگوهای ADM و ADMX/ADML در کنار هم کار می‌کنند.

انباره مرکزی (central store)

همان‌طوریکه قبلا اشاره شد فایل‌های ADM به عنوان بخشی از خود GPO ذخیره می‌شوند. وقتی یک GPO را که از الگوهای مدیریتی با فرمت ADM استفاده می‌کند ویرایش می‌کنیم GPME، ADM را از GPC بارگذاری می‌کند تا رابط کاربری آماده شود. زمانی که فایل‌های ADMX/ADML به عنوان الگوهای مدیریتی به کار می‌رود GPO فقط دادهی را شامل می‌شود که کلاینت به منظور پردازش Group Policy به آن نیاز دارد . وقتی GPO ویرایش می‌شود GPME فایل‌های ADMX و ADML را از کلاینت بیرون می‌کشد.

این روش در سازمان‌های کوچک عملی است ولی در محیط‌های پیچیده و بزرگ که دارای الگوهای مدیریتی سفارشی هستند یا نیاز به کنترل مرکزی دارند ویندوز سرور 2008 انباره مرکزی را معرفی می‌کند. انباره مرکزی یک پوشه منفرد در SYSVOL است که همه فایل‌های ADMX و ADML مورد نیاز را نگهداری می‌کند. بعد از نصب این انباره، GPME آنرا تشخیص می‌دهد و همه الگوهای مدیریتی را به جای کامپیوتر مقصد از انباره مرکزی بارگذاری می‌کند.

برای ساخت یک انباره مرکزی پوشه‌ای به نام PolicyDefinitions در مسیر \\FQDN\SYSVOL\FQDN\Policies می‌سازیم. برای مثال انباره مرکزی برای دامنه contoso.com می‌شود :

\\contoso.com\SYSVOL\contoso.com\Policies\PolicyDefinitions . سپس همه فایل‌ها را از پوشه %SystemRoot%\PolicyDefinitions در سرور 2008 به پوشه جدید SYSVOL PolicyDefinition کپی می‌کنیم. این شامل فایل‌های admx. و adml. که در پوشه با نام زبان خود موجود هستند نیز می‌شود. برای مثال فایل‌های انگلیسی ADML (ایالات متحده) در مسیر %SystemRoot%\PolicyDefinitions\en-us موجود هستند. این فایل‌ها نیز باید به مسیر \\FQDN\SYSVOL\FQDN\Policies\PolicyDefinitions\en-us کپی شوند. اگر زبان‌های دیگری نیز مورد نیاز باشند پوشه محتوی فایل‌های ADML را به انباره مرکزی کپی می‌کنیم. وقتی همه فایل‌ها کپی شد پوشه PolicyDefinitions در DC باید حاوی فایل‌های ADMX و یک یا چند پوشه حاوی فایل‌های ADML با نام زبان خود باشد.

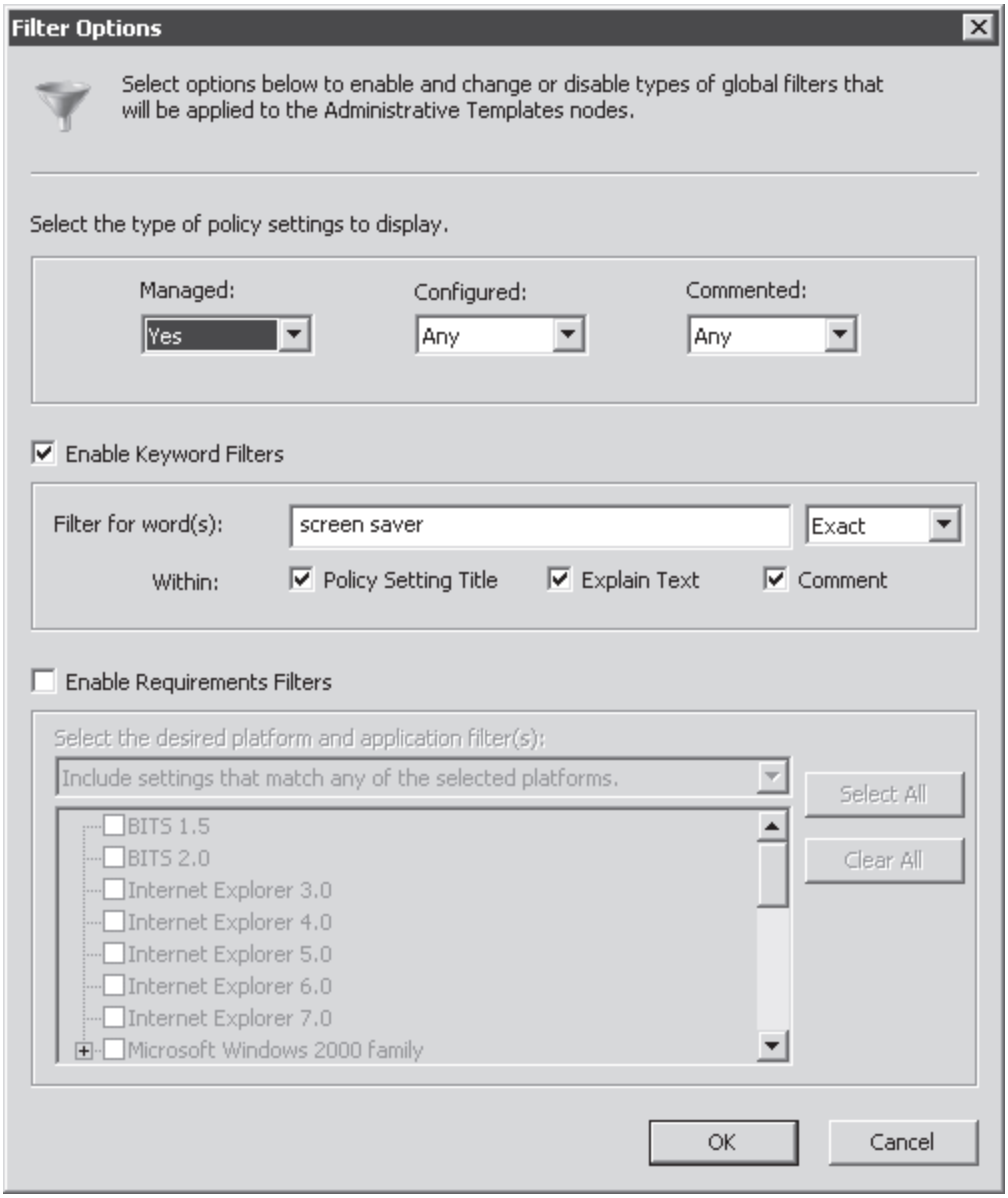
نکته امتحانی اگر به یک DC وارد شوید چه از پشت سرور چه از راه دور مسیر پوشه PolicyDefinitions به صورت زیر خواهد بود: %SystemRoot\SYSVOL\domain\Policies\PolicyDefinitions .

فیلتر کردن تنظیمات Policy الگوی مدیریتی

ضعف ابزارهای ویرایش Group Policy در نسخه‌های قبلی ویندوز عدم امکان جستجوی یک تنظیم خاص بود. با وجود هزاران policy پیدا کردن تنظیم مورد نظر خیلی مشکل می‌شود. GPME جدید در ویندوز سرور 2008 این مشکل را حل می‌کند. ما الان می‌توانیم فیلترهایی را برای پیدا کردن تنظیمی خاص بسازیم.

برای ساخت یک فیلتر روی Administrative Templates کلیک راست کرده و Filter Options را انتخاب می‌کنیم. برای پیدا کردن policy خاص Enable Keyword Filters را انتخاب می‌کنیم و کلمات مورد نظر را وارد می‌کنیم. سپس فیلدهای جستجو را انتخاب می‌کنیم. شکل ۵- ۶ یک مثال از یک جستجو در مورد تنظیمات مربوط به screen saver را نشان می‌دهد.

در بخش بالایی کادر محاوره‌ای Filter Options در شکل ۵- ۶ می‌توانیم نمایش را به فقط به تنظیمات پیکربندی شده محدود کنیم به طوری که تنظیمات پیش فرض نمایش داده نشود. این مساله به ما کمک می‌کند تا تنظیماتی را که قبلا در GPO تعیین شده پیدا کرده و تغییر دهیم.



شکل ۵- ۶ فیلتر کردن تنظیمات policy الگوهای مدیریتی

درج توضیحات

ما می‌توانیم جستجو را بر اساس توضیحات تنظیم policy انجام دهیم. ویندوز سرور 2008 این امکان را به ما می‌دهد که توضیحی را به تنظیم policy در گره Administrative Templates اضافه کنیم. روی تنظیم policy دوبار کلیک کرده و زبانه Comment را کلیک می‌کنیم. توصیه می‌شود به تنظیم policy پیکربندی شده به منظور مستندسازی و تعیین هدف آن توضیحی اضافه کنیم. در ویندوز سرور 2008 این توضیحات به خود GPO نیز می‌توانند اضافه شوند. در GPME روی گره ریشه کلیک راست کرده و Properties را انتخاب می‌کنیم و بعد زبانه Comment را کلیک می‌کنیم.

Starter GPOs

ویژگی جدید دیگر Group Policy در ویندوز سرور 2008 ، starter GPOs می‌باشد. این نوع GPO تنظمات Administrative Template را در بر می‌گیرد. ما می‌توانیم یک GPO جدید از یک starter GPO بسازیم که در این حالت GPO جدید تنظیماتی مشابه starter GPO خواهد داشت. در واقع Starter GPO یک الگو (template) می‌باشد. متاسفانه مایکروسافت از واژه template در administrative templates استفاده کرده و بنابراین باید نام دیگری برای آن انتخاب می‌کرد و انتخاب مایکروسافت starter بود. وقتی GPO جدید می‌سازیم می‌توانیم مشخص کنیم به صورت یک GPO خالی یا یک starter GPO موجود در ویندوز یا سفارشی آغاز شود.

نکته وقتی تنظیمات الگوی مدیریتی کفاف نیاز ما را نمی‌دهد

Starter GPO ها فقط حاوی تنظیمات Administrative Templates هستند. امکان کپی و درج کل GPO ها در Group Policy Objects container از کنسول Group Policy Management وجود دارد به طوری که GPO جدیدی با همه تنظیمات GPO مبدا خواهیم داشت. به منظور انتقال تنظیمات بین GPO ها در دامنه‌ها یا forest های مختلف روی یک GPO کلیک راست کرده و Back Up را انتخاب می‌کنیم. در دامنه هدف یک GPO جدید می‌سازیم، روی آن کلیک راست کرده و Import Settings را انتخاب می‌کنیم. حالا مسیر فایل پشتیبان را وارد کرده و عملیات را به پایان می‌رسانیم.

تنظیمات managed policy و unmanaged policy

در بحث تنظیمات رجیستری که توسط گره Administrative Templates پیکربندی شده است نکته ظریفی وجود دارد که دانستن آن اهمیت دارد و آن تفاوت بین تنظیمات policy به صورت managed و unmanaged می‌باشد. تنظیمات policy رجیستری که بررسی شد و در تمرینات هم کار می‌شود نمونه ای از تنظیمات managed policy می‌باشد. یک managed policy وقتی تنظیمات توسط GPO اعمال می‌شود به نوعی روی یک تغییر پیکربندی تاثیرگذار است وقتی کامپیوتر یا کاربری از حوزه GPO خارج می‌شود پیکربندی به طور خودکار به وضعیت اصلی خود برمی‌گردد. برای مثال وقتی GPO دسترسی به ابزارهای ویرایش رجیستری را منع می‌کند و سپس GPO حذف یا غیرفعال می‌شود، پس از به‌روز رسانی policy، کاربران دوباره به این ابزارها دسترسی خواهند داشت.

بالعکس یک unmanaged policy تغییری دائمی در رجیستری ایجاد می‌کند. وقتی GPO حذف شود تنظیمات باقی خواهد ماند. به این وضعیت خالکوبی (tatto) رجیستری نیز می‌گویند. برای برگرداندن تاثیرات policy باید تغییر جدید را در شبکه توزیع کنیم. به طور پیش فرض GPME تنظیمات unmanaged را مخفی می‌کند تا ما به این نوع از تغییر که برگشت آن مشکل است تشویق نشویم. بهرحال تغییرات مفید زیادی توسط تنظیمات unmanaged قابل اجراست مخصوصا برای الگوهای مدیریتی سفارشی به منظور پیکربندی برنامه‌ها. برای کنترل نمایش تنظیمات روی Administrative Templates کلیک راست کرده و Filter Options را انتخاب می‌کنیم. گزینه‌ای را از لیست بازشوی Managed انتخاب می‌کنیم.

تمرینات پیاده سازی Group Policy

در این تمرینات ما پیکربندی دامنه contoso.com را توسط Group Policy پیاده سازی می‌کنیم. ما باید GPO ها را بسازیم، پیکربندی کنیم و حوزه آنها را مشخص کنیم. همچنین نسبت به ویژگیهای جدید Group Policy در ویندوز سرور 2008 تجربیات عملی به دست می‌آوریم.

تمرین ۱ ساخت، ویرایش و تعیین حوزه شیء Group Policy

در این تمرین یک GPO می‌سازیم که تنظیمات اجباری شرکت Contoso را پیاده می‌کند و آن را به روی همه کاربران و کامپیوترها در دامنه اعمال می‌کند.

۱. با اعتبار Administrator به SERVER01 وارد می‌شویم.

۲. کنسول Group Policy Management را از پوشه Administrative Tools باز می‌کنیم.

۳. گره‌های Forest، Domains، دامنه contoso.com و Group Policy Objects container را باز می‌کنیم.

۴. در ساختار درختی روی Group Policy Container کلیک راست کرده و New را انتخاب می‌کنیم.

۵. در کادر Name عبارت CONTOSO Standards را تایپ کرده و OK می‌کنیم.

۶. روی CONTOSO Standards GPO کلیک راست کرده و Edit را انتخاب می‌کنیم.

پنجره Group Policy Management Editor ظاهر می‌شود.

۷. روی گره ریشه کنسول یعنی CONTOSO Standards کلیک راست کرده و Properties را انتخاب می‌کنیم.

۸. زبانه Comment را باز کرده و عبارت زیر را تایپ می‌کنیم :

"تنظیمات استاندارد شرکت Contoso. تنظیمات روی همه کاربران و کامپیوترها در دامنه اعمال می‌شود. شخص مسئول این GPO . . . . . می‌باشد." به جای نقطه چین نام خود را می‌نویسیم. سپس OK می‌کنیم.
در این سناریو policy امنیتی شرکت مشخص می‌کند که کامپیوترها نباید به مدت بیش از ۱۰ دقیقه بدون کاربر بمانند. برای این کار می‌توان زمان screen saver و policy ورود کلمه عبور برای خارج شدن از screen saver را پیکربندی کرد. قابلیت جستجوی جدید Windows Server 2008 Group Policy به پیدا کردن تنظیم مربوطه کمک می‌کند.

۹. گره User Configuration\Policies\Administrative Templates را باز می‌کنیم.

۱۰. بد نیست چند لحظه‌ای را به مرور تنظیمات زیر این گره بپردازیم. متن توضیح هر تنظیم می‌تواند برای ما جالب باشد. هیچ تغییری در تنظیمات ایجاد نمی‌کنیم.

۱۱. در گره User Configuration روی Administrative Templates کلیک راست می‌کنیم و Filter Options را انتخاب می‌کنیم.

۱۲. کادر Enable Keyword Filters را علامت می‌زنیم.

۱۳. در کادر متنی Filter for Word(s) عبارت screen saver را تایپ می‌کنیم.

۱۴. در لیست بازشوی نزدیک کادر متنی Exact را انتخاب می‌کنیم.

۱۵. دکمه OK را کلیک می‌کنیم.

تنظیمات Administrative Templates فقط عباراتی را که شامل کلمه screen saver است نشان می‌دهد.

۱۶. تنظیمات screen saver پیدا شده را بررسی می‌کنیم.

۱۷. در گره Control Panel\Display روی تنظیم Screen Saver Timeout کلیک می‌کنیم. به متن توضیحی در حاشیه سمت چپ کنسول توجه کنید.

۱۸. روی تنظیم Screen Saver Timeout دوبار کلیک می‌کنیم.

۱۹. متن توضیحی را در زبانه Explain مرور می‌کنیم.

۲۰. زبانه Setting را باز کرده و Enabled را انتخاب می‌کنیم.

۲۱. در کادر Seconds عدد ۶۰۰ را تایپ می‌کنیم.

۲۲. در زبانه Comment عبارت زیر را تایپ می‌کنیم:

"سیاست امنیتی شرکت در ترکیب با تنظیم Password Protect the Screen Saver پیاده سازی می‌شود."

۲۳. دکمه OK را کلیک می‌کنیم.

۲۴. تنظیم Password Protect The Screen Saver را دوبار کلیک می‌کنیم.

۲۵. Enabled را انتخاب می‌کنیم.

۲۶. در زبانه Comment عبارت "سیاست امنیتی شرکت در ترکیب با تنظیم Screen Saver Timeout پیاده سازی می‌شود." را تایپ می‌کنیم

۲۷. دکمه OK را کلیک می‌کنیم.

۲۸. پنجره GPME را می‌بندیم.

تغییرات انجام شده در GPME به صورت لحظه‌ای ذخیره می‌شود و نیازی به دستور Save نیست.

۲۹. در کنسول Group Policy Management روی دامنه contoso.com دوبار کلیک کرده و Link An Existing GPO را انتخاب می‌کنیم.

۳۰. CONTOSO Standards GPO را انتخاب کرده و OK می‌کنیم.

تمرین ۲ مشاهده تاثیرات Group Policy

در این تمرین تاثیرات تنظیمات Group Policy را که در تمرین ۱ پیکربندی کردیم تجربه می‌کنیم و با استفاده از دستور Gpupdate.exe به صورت دستی تغییرات را اعمال می‌کنیم.

۱. در SERVER01 روی دسک‌تاپ کلیک راست کرده و Personalize را انتخاب می‌کنیم.

۲. Screen Saver را کلیک می‌کنیم.

۳. توجه کنید که امکان تغییر زمان screen saver و انتخاب گزینه نمایش پنجره logon screen وجود دارد. کادر را می‌بندیم.

۴. پنجره خط فرمان را باز می‌کنیم و تایپ می‌کنیم :gpupdate.exe /force /boot /logoff

این سوئیچ‌ها در دستور Gpupdate.exe باعث به روز شده کامل Group Policy می‌شود. منتظر می‌مانیم تا هم تنظیمات کاربر و هم کامپیوتر به روز شوند.

۵. به کادر محاوره‌ای Screen Saver Settings برمی‌گردیم. توجه کنید که دیگر نمی‌توانیم زمان screen saver را تغییر دهیم یا گزینه resume را انتخاب کنیم.

تمرین ۳ بررسی دقیق یک GPO

حالا که عملکرد GPO را دیدیم می‌خواهیم خود GPO را دقیق‌تر بررسی کنیم.

۱. در کنسول Group Policy Management و داخل Group Policy Object container گزینه CONTOSO Standards GPO را انتخاب می‌کنیم.

۲. توجه کنید که GPO در زبانه Scope در بخش Links، پیوند خود را گزارش می‌دهد.

۳. برای مشاهده گزارش تنظیمات در GPO روی زبانه Settings کلیک می‌کنیم.

اگر ویژگی Internet Explorer Enhanced Security Configuration (ESC) فعال باشد پیغامی برای تایید افزودن about:security_mmc.exe به Trusted Sites zone مشاهده می‌کنیم

۴. در بالای این گزارش روی لینک Show All کلیک می‌کنیم تا همه بخش‌های گزارش باز شود. توجه کنید که توضیحات درج شده به عنوان بخشی از گزارش نمایش داده می‌شود.

۵. اگر به متن Screen Saver Timeout اشاره کنیم می‌بینیم که در واقع یک لینک فرامتنی است. با کلیک کردن روی آن متن توضیحی راجع به تنظیم را مشاهده می‌کنیم.

۶. زبانه Details را باز می‌کنیم. توجه کنید که در این زبانه توضیحات GPO به همراه نسخه GPO نمایش داده می‌شود.

۷. Unique ID نمایش داده شده در زبانه Details را یادداشت می‌کنیم.

۸. پوشه \\contoso.com\SYSVOL\contoso.com\Policies را باز می‌کنیم.

۹. پوشه هم‌نام Unique ID نوشته شده را باز می‌کنیم. این همان GPT مربوط به GPO است.

تمرین ۴ بررسی دقیق‌تر Administrative Template

Administrative Template دستوراتی را مهیا می‌کند که با آن GPME یک رابط کاربری برای پیکربندی تنظیمات Administrative Template می‌سازد و تغییراتی را که باید براساس آن تنظیمات روی رجیستری اعمال شود تعیین می‌کند. در این تمرین یک الگوی مدیریتی می‌سازیم.

۱. پوشه %SystemRoot%\PolicyDefinitions را باز می‌کنیم.

۲. پوشه en-us یا پوشه با نام زبان منطقه خود را باز می‌کنیم.

۳. روی ControlPanelDisplay.adml دوبار کلیک می‌کنیم. گزینه Select A Program From A List Of Installed Programs انتخاب کرده و OK می‌کنیم. فایل را با Notepad باز می‌کنیم.

۴. Word Wrap را از منوی Format فعال می‌کنیم.

۵. متن ScreenSaverIsSecure را جستجو می‌کنیم.

۶. به برچسب تنظیم و در خط بعدی متن توضیحی توجه کنید.

۷. فایل را بسته و به پوشه PolicyDefinitions بازمی‌گردیم.

۸. روی ControlPanelDisplay.admx دوبار کلیک می‌کنیم. فایل را با برنامه Notepad باز می‌کنیم.

۹. عبارت زیر را در متن جستجو می‌کنیم:

```
<policy name=”ScreenSaverIsSecure” class=”user”
displayName=”$(string.ScreenSaverIsSecure)”
explainText=”$(string.ScreenSaverIsSecure_Help)”
key=”Software\Policies\Microsoft\Windows\Control Panel\Desktop”
valueName=”ScreenSaverIsSecure”>
        <parentCategory ref=”Display” />
        <supportedon ref=”windows:SUPPORTED_Win2kSP1” />
        <enabledValue>
```

```
      <string>1</string>
    </enabledValue>
    <disabledValue>
      <string>0</string>
    </disabledValue>
</policy>
```

۱۰. بخش‌هایی از این الگو را که موارد زیر را تعریف می‌کند پیدا می‌کنیم:

- نام تنظیمی که در GPME ظاهر می‌شود
- متن توضیحی برای تنظیم
- کلید رجیستری و مقدار آن که تحت تاثیر تنظیم policy قرار گرفته‌اند
- داده‌هایی که در رجیستری قرار گرفته‌اند زمانی که policy فعال باشد
- داده‌هایی که در رجیستری قرار گرفته‌اند زمانی که policy غیرفعال باشد

تمرین ۵ ساخت انباره مرکزی

در این تمرین یک انباره مرکزی از الگوهای مدیریتی می‌سازیم تا بتوانیم مدیریت الگوها را متمرکز کنیم.

۱. در کنسول Group Policy Management روی CONTOSO Standards کلیک راست کرده و Edit را انتخاب می‌کنیم.

۲. گره User Configuration\Policies\Administrative Template را باز می‌کنیم.

۳. توجه کنید که گره باز شده Policy Definitions (ADMX Files) Retrived From The Local Machine را نمایش می‌دهد.

۴. ابزار GPME را می‌بندیم.

۵. پوشه \\contoso.com\SYSVOL\contoso.com\Policies را باز می‌کنیم.

۶. پوشه‌ای با نام PolicyDefinition می‌سازیم.

۷. محتویات آدرس %SystemRoot%\PolicyDefinitions را به پوشه ساخته شده کپی می‌کنیم.

۸. در کنسول Group Policy Management روی CONTOSO Standards کلیک راست کرده و Edit را انتخاب می‌کنیم.

۹. گره User Configuration\Policies\Administrative Template را باز می‌کنیم.

۱۰. توجه کنید که گره باز شده Policy Definitions (ADMX Files) Retrived From The Central Store را نمایش می‌دهد.

خلاصه درس

- GPO ها تنظیمات policy را در بر می‌گیرند. وقتی کاربران، کامپیوترها، OU و سایت در حوزه GPO قرار می‌گیرند تنظیمات GPO را به خود می‌گیرند.
- پردازش‌هایی که روی ویندوز کلاینت اجرا می‌شود مشخص می‌کند کدام GPO ها باید دانلود و اعمال شود. این پردازش‌ها برای تنظیمات کامپیوتر در زمان بوت شدن و بعد از آن هر ۹۰ تا ۱۲۰ دقیقه یکبار و برای تنظیمات کاربر در زمان ورود به ویندوز و بعد از آن هر ۹۰ تا ۱۲۰ دقیقه یکبار اجرا می‌شود.
- به طور پیش فرض CSE ها تنظیمات را فقط زمانی اعمال می‌کنند که GPO تغییر کرده باشد. تنظیمات امنیتی از این قاعده مستثنی هستند که هر ۱۶ ساعت یکبار اتفاق می‌افتد چه تغییر کرده باشد چه نکرده باشد. CSE ها می‌توانند برای اعمال دوباره تنظیمات در هر به روز آوری پیکربندی شوند و در موارد ارتباط ضعیف شبکه‌ای از نصب برنامه که توسط Group Policy توزیع شده جلوگیری کنند.
- ویندوز سرور 2008، Group Policy Preferences را معرفی کرده که بیش از ۲۰ CSE را برای مدیریت تنظیمات کاربران و کامپیوترها به تعداد زیاد، افزوده است.
- الگوهای مدیریتی (فایل‌های adm. یا admx.) رابط کاربری و تغییرات رجیستری را برای تنظیمات policy در گره Administrative Templates مربوط به GPO تعریف می کند.
- می‌توانیم الگوهای مدیریتی را با یک انباره مرکزی به صورت متمرکز مدیریت کنیم.
- ویندوز سرور 2008 قابلیت درج توضیح را در GPO و تنظیمات policy داراست و می‌تواند GPO های جدید را بر اساس starter GPO که دارای تنظیمات اولیه می‌باشد ایجاد کند

سئوالات پایان درس

۱. شرکت Litware سه واحد تجاری دارد که هر OU در دامنه litwareinc.com نماینده یکی از آنهاست. مدیران شبکه واحدها باید بتوانند Group Policy کاربران و کامپیوترها را در OU خود مدیریت کنند. برای اعطاء این قابلیت چه کاری باید انجام گیرد؟ (ممکن بیش از یک جواب داشته باشد. هرجواب صحیح بخشی از راه حل نهایی است)

A. الگوهای مدیریتی را از انباره مرکزی در پوشه PolicyDefinitions در کلاینت‌های ویندوز ویستا مدیران شبکه کپی می‌کنیم.

B. مدیران شبکه واحدهای تجاری را به گروه Group Policy Creator Owners اضافه می‌کنیم.

C. مجوز Link GPOs را به مدیران شبکه در دامنه litwareinc.com اعطاء می‌کنیم.

D. مجوز Link GPOs را به مدیران شبکه در هر واحد تجاری نسبت به OU همان واحد اعطاء می‌کنیم.

۲. شما یکی از مدیران شبکه شرکت Contoso هستید. دامنه contoso.com دارای دامنه فرزندی به نام es.contoso.com برای شعبه اسپانیا می‌باشد. مدیران این دامنه از شما درخواست می‌کنند یک رابط کاربری با زبان اسپانیایی برای Group Policy Management Editor برایشان فراهم کنید. چطور این کار را انجام می‌دهید؟

A. به یک DC در دامنه es.contoso.com وارد می‌شویم و پوشه %SystemRoot%\SYSVOL\domain\Policies\PolicyDefinitions را باز کرده و فایل‌های ADM را به پوشه ES کپی می‌کنیم.

B. فایل‌های ADML را به پوشه \\es.contoso.com\SYSVOL\es.contoso.com\policies\PolicyDefinitions\es کپی می‌کنیم.

C. به یک DC در دامنه es.contoso.com وارد می‌شویم و پوشه %SystemRoot%\SYSVOL\domain\Policies\PolicyDefinitions را باز کرده و فایل‌های ADMX را به پوشه ES کپی می‌کنیم.

D. فایل Boot.wim را از سی‌دی ویندوز سرور 2008 روی یک DC در دامنه فرزند نصب می‌کنیم.

۳. شما یکی از مدیران شبکه شرکت Contoso هستید. در آخرین همایش طی صحبتی که با مدیران شبکه شرکت Fabrikam داشته‌اید راجع به اعمال موفقیت‌آمیز تنظیمات GPO شرکت صحبت کرده‌اید. مدیران آن شرکت از شما خواسته‌اند یک کپی از GPO خود را به دامنه آنها کپی کنید. کدام روش ما را به هدف می‌رساند؟

A. روی Contoso GPO کلیک راست کرده و Save Report را انتخاب می‌کنیم. یک GPO را در دامنه Fabrikam می‌سازیم روی آن کلیک راست کرده و Import را انتخاب می‌کنیم.

B. روی Contoso GPO کلیک راست کرده و Backup را انتخاب می‌کنیم. روی Group Policy Objects container در دامنه Fabrikam کلیک راست کرده و گزینه Restore From Backup را انتخاب می‌کنیم.

C. روی Contoso GPO کلیک راست کرده و Backup را انتخاب می‌کنیم. یک GPO را در دامنه Fabrikam می‌سازیم روی آن کلیک راست کرده و Paste را انتخاب می‌کنیم.

D. روی Contoso GPO کلیک راست کرده و Backup را انتخاب می‌کنیم. یک GPO را در دامنه Fabrikam می‌سازیم روی آن کلیک راست کرده و Import Settings را انتخاب می‌کنیم.

درس ۲ : مدیریت حوزه Group Policy

یک GPO فقط یک مجموعه تنظیمات است که توسط CSE های کامپیوتر پردازش می‌شوند. تا زمانی که حوزه آن مشخص نشود به هیچ کاربر یا کامپیوتری اعمال نمی‌شود. حوزه GPO مشخص می‌کند کدام کامپیوترها باید GPO را دریافت و پردازش کنند و فقط کامپیوترها یا کاربران در حوزه GPO تنظیمات را اعمال می‌کنند. راههای متعددی برای تعیین حوزه یک GPO استفاده می‌شود:

- لینک GPO به یک سایت، دامنه یا OU و فعال کردن آن لینک
- گزینه Enforce یک GPO
- گزینه Block Inheritance مربوط به یک OU
- فیلترکردن گروه امنیتی

- فیلتر کردن WMI
- فعال یا غیرفعال کردن گره Policy
- Preferences targeting
- پردازش Loopback policy

ما باید بتوانیم کاربران و کامپیوترهایی را که تنظیمات به آنها باید اعمال شود مشخص کنیم. در این درس همه روش‌های تعیین حوزه GPO را یاد می‌گیریم و مفاهیم Group Policy application ، وراثت و تقدم را درک می‌کنیم.
بعد از این درس ما می‌توانیم:

- لینک‌های GPO را مدیریت کنیم
- وراثت و تقدم GPO را ارزیابی کنیم
- گزینه‌های لینک Block Inheritance و Enforced را درک کنیم
- از فیلتر کردن امنیتی برای محدود کردن حوزه GPO استفاده کنیم
- یک فیلتر WMI را به GPO اعمال کنیم
- Loopback policy preferences را پیاده‌سازی کنیم

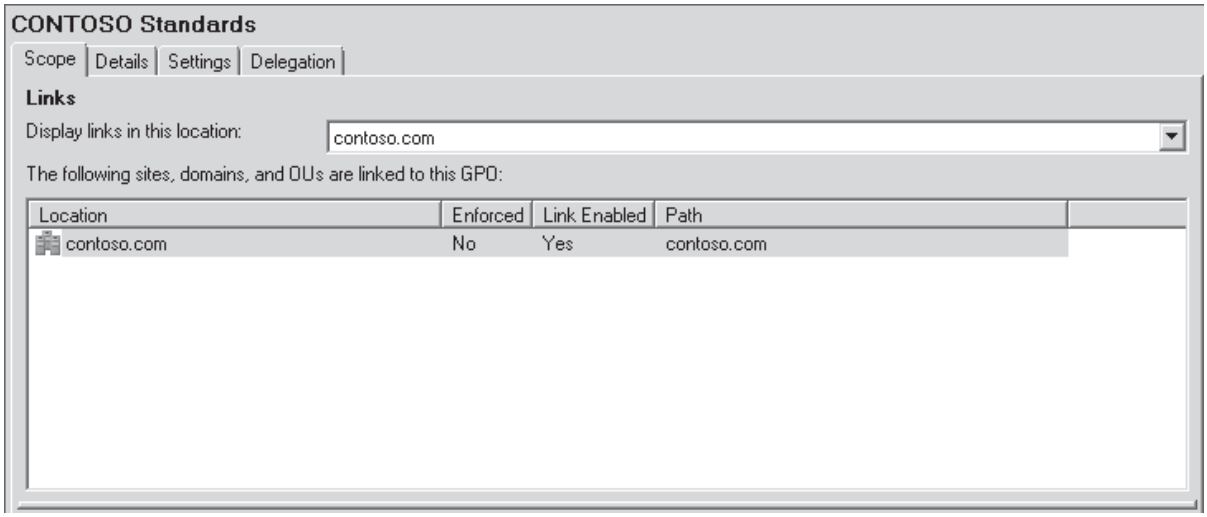
زمان تقریبی : ۹۰ دقیقه

لینک‌های GPO

یک GPO می‌تواند به بیش از یک سایت، دامنه یا OU لینک شود. وقتی policy به یک container لینک می‌شود کاربران یا کامپیوترها و کاربران آن container و OU های فرزند در حوزه GPO قرار خواند گرفت.
همان‌طوری که در درس ۱ یاد گرفتیم ما می‌توانیم یک GPO را به دامنه یا OU لینک کنیم. بدین ترتیب که روی دامنه یا OU کلیک راست کرده و Link An Existing GPO را انتخاب می‌کنیم. اگر هنوز هیچ GPO درست نکرده باشیم می‌توانیم Create A GPO In This Domain, And Link It Here را انتخاب کنیم. از دستورات مشابه برای لینک کردن یک GPO به یک سایت می‌توان استفاده کرد ولی به طور پیش فرض سایت‌های دایرکتوری در GPME قابل مشاهده نیستند و ابتدا باید روی Sites کلیک راست کرده و Show Sites را انتخاب کنیم.

GPO های لینک شده به سایت (Site-Linked) و محل DC

GPO لینک شده به یک سایت روی همه کامپیوترهای سایت صرف‌نظر از اینکه در کدام دامنه قرار دارند تاثیر می‌گذارد (به شرطی که در یک forest قرار داشته باشند). بنابراین با لینک کردن GPO به یک سایت آن GPO می‌تواند به چند دامنه در forest اعمال شود.
GPO های لینک شده به سایت روی DC در دامنه‌ای که GPO در آن ساخته شده ذخیره می‌شود. بنابراین برای اینکه این GPO ها به درستی اعمال شوند DC های آن دامنه باید در دسترس باشند. در هنگام برنامه‌ریزی زیرساخت شبکه اگر بخواهیم از policy های سایت استفاده کنیم باید policy application را در نظر بگیریم. یا یک DC از دامنه GPO در سایتی که GPO به آن لینک شده قرار می‌دهیم یا از ارتباط WAN مربوط به DC در دامنه GPO اطمینان حاصل می‌کنیم.
وقتی یک GPO را به یک سایت، دامنه یا OU لینک می‌کنیم حوزه اولیه GPO را نیز تعریف می‌کنیم. GPO را انتخاب کرده و زبانه Scope را باز می‌کنیم تا container هایی که GPO به آنها لینک می‌شود مشخص کنیم. در پنل وسط GPMC لینک‌های GPO در بخش اول زبانه Scope همانند شکل ۶- ۶ نشان داده می‌شود.



شکل ۶- ۶ لینک‌های یک GPO در زبانه Scope از پنجره GPMC

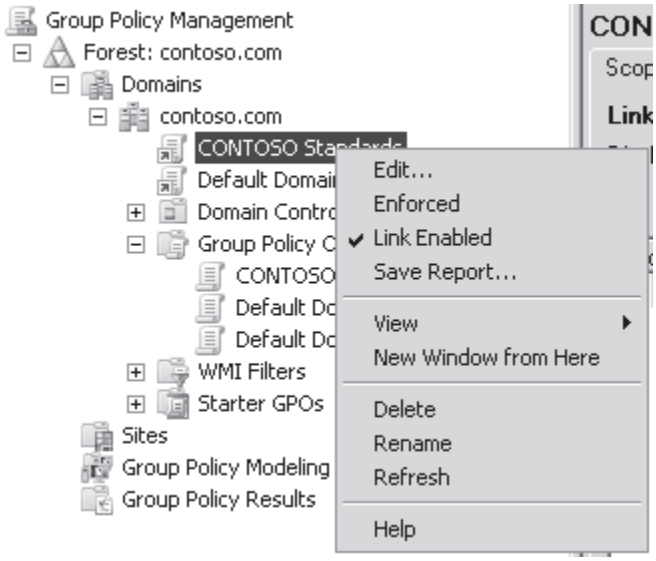
نکته مهم در مورد لینک‌های GPO این است که کلاینت Group Policy زمانی GPO را دانلود می‌کند که اشیاء کامپیوتر یا کاربر در حوزه لینک واقع شده باشد. GPO زمانی دانلود می‌شود که تغییر کرده باشد. کلاینت Group Policy برای به روز رسانی سریع‌تر GPO را در حافظه نهانی (cache) خود ذخیره می‌کند.

لینک کردن یک GPO به چندین OU

ما می‌توانیم یک GPO را به بیش از یک سایت، دامنه یا OU لینک کنیم. به عنوان مثال اعمال تنظیمات به کامپیوترهای چند OU بسیار بدیهی است. ما می‌توانیم تنظیمات را درون یک GPO منفرد ذخیره کنیم و آن GPO را به هر OU که می‌خواهیم لینک کنیم. وقتی بعدها تنظیمات GPO را تغییر می‌دهیم این تغییرات به همه OU ها که GPO به آنها لینک شده است اعمال می‌شود.

حذف یا غیرفعال کردن یک لینک GPO

بعد از لینک کردن GPO، این لینک در زیر سایت، دامنه یا OU در پنجره GPMC نمایان می‌شود. آیکن لینک GPO یک فلش میانبر کوچک دارد. وقتی روی لینک GPO کلیک راست می‌کنیم یک منو مطابق شکل ۶- ۷ باز می‌شود.



شکل ۶- ۷ منوی کلیک راست لینک GPO

ما می‌توانیم یک لینک GPO را با انتخاب Delete از منوی کلیک راست حذف کنیم. حذف لینک GPO به معنای حذف خود GPO نیست. حذف لینک باعث تغییر حوزه GPO می‌شود به این صورت که کامپیوترها یا کاربرانی که قبلا در حوزه این GPO قرار می‌گرفتند پس از حذف لینک دیگر در این حوزه نخواهند بود.

تغییر لینک GPO با غیرفعال کردن آن نیز ممکن است. روی آن کلیک راست کرده و گزینه Enabled را از حالت انتخاب خارج می‌کنیم. تغییر ایجاده شده مانند حذف لینک است با این تفاوت که امکان فعال کرده دوباره آن موجود است.

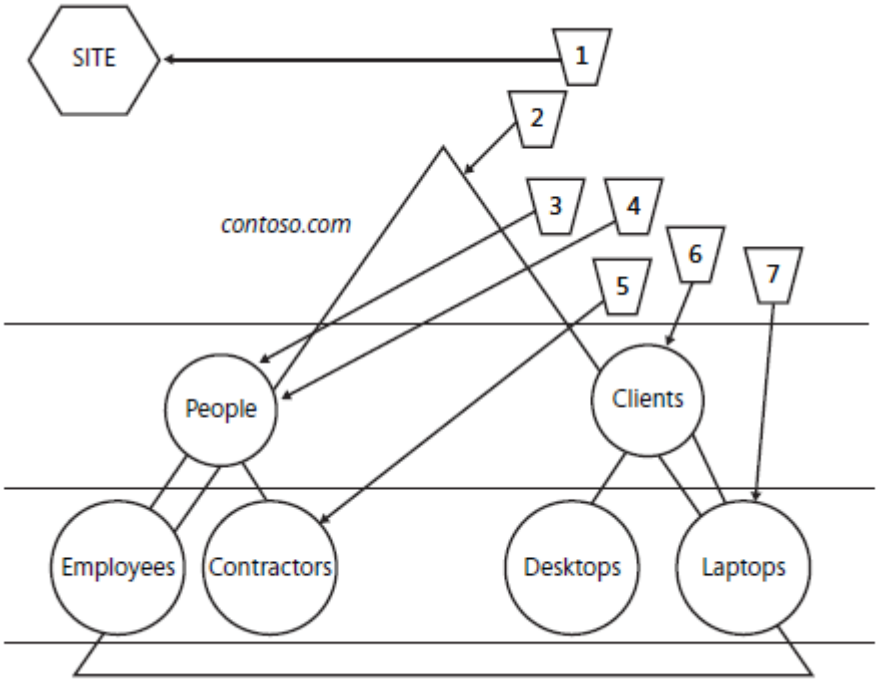
وراثت و اولویت GPO

یک تنظیم policy می‌تواند در بیش از یک GPO پیکربندی شود و GPO ها می‌توانند در تداخل با یکدیگر باشند. به عنوان مثال یک تنظیم policy می‌تواند در یک GPO فعال باشد و در دیگری غیرفعال و در سومی تنظیم نشده باشد. در این وضعیت اولویت (precedence) GPO ها مشخص می‌کند کدام تنظیم را کلاینت اعمال کند. GPO با اولویت بالاتر بر GPO با اولویت پایین‌تر غلبه می‌کند. اولویت در GPMC به عنوان یک شماره نمایش داده می‌شود. هرچه عدد کوچکتر باشد یعنی به عدد یک نزدیک‌تر باشد اولویت آن بالاتر است. بنابراین GPO با اولویت ۱ بر GPO های دیگر غلبه خواهد کرد. دامنه یا OU را انتخاب کرده و زبانه Group Policy Inheritance را باز می‌کنیم تا اولویت هر GPO را ببینیم.

وقتی یک تنظیم policy در یک GPO با اولویت بالاتر فعال یا غیرفعال است این تنظیم اعمال می‌شود. به خاطر داشته باشید تنظیمات policy به طور پیش فرض در حالت Not Configured قرار دارد. وقتی یک تنظیم در GPO با اولویت بالاتر پیکربندی نمی‌شود آن تنظیم (فعال یا غیرفعال) در GPO با اولویت پایین‌تر اعمال می‌شود.

به یک سایت، دامنه یا OU می‌توان بیش از یک GPO لینک کرد. ترتیب لینک‌های GPO اولویت را در این وضعیت مشخص می‌کند. GPO هایی که در لیست بالاتر از بقیه قرار می‌گیرند اولویت بالاتری دارند. اگر یک OU را در GPMC انتخاب کنیم زبانه Linked Group Policy Objects ترتیب لینک‌های GPO لینک شده به آن OU را نمایش می‌دهد.

رفتار پیش فرض Group Policy به این شکل است که GPO های لینک شده به container سطح بالاتر توسط container های سطح پایین‌تر به ارث می‌رسند. وقتی کامپیوتری بوت شده یا کاربری وارد می‌شود کلاینت Group Policy محل شیء کامپیوتر یا کاربر را در Active Directory چک می‌کند و GPO ها را به همراه حوزه آنان که کامپیوتر یا کاربر را در بر می‌گیرند ارزیابی می‌کند. سپس پروسه‌های سمت کلاینت تنظیمات policy را از این GPO ها اعمال می‌کنند. Policy ها به ترتیب اعمال می‌شوند. ابتدا policy های لینک شده به سایت سپس دامنه بعد OU از OU های سطح بالا به سطح پایین که کاربران و کامپیوترها را در بر می‌گیرند. به این تنظیمات چندلایه گویند به طوری که GPO که آخر پردازش می‌شود اولویت بالاتری دارد و بر همه تنظیماتی که زودتر پردازش می‌شود غلبه می‌کند. این ترتیب پیش فرض اعمال GPO در شکل ۸- ۶ نمایش داده شده است.



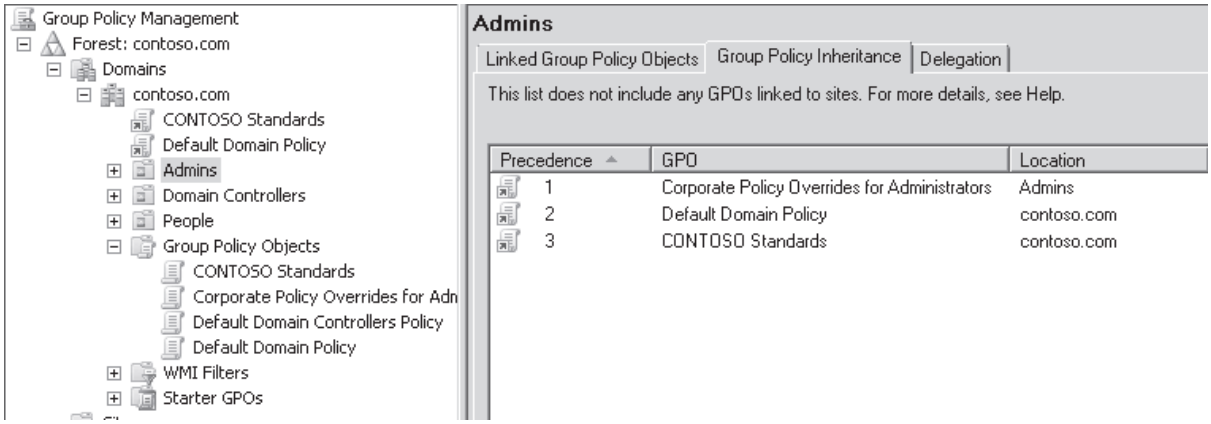
ترتیب پردازش GPO برای Contractors OU = ۱-۲-۳-۴-۵

ترتیب پردازش GPO برای Laptops OU = ۱-۲-۶-۷

شکل ۸- ۶ پردازش پیش فرض GPO های سایت، دامنه یا OU

نکته امتحانی ترتیب پردازش policy را به خاطر داشته باشید: سایت، دامنه و OU . به خاطر داشته باشید که تنظیمات policy های دامنه بعد از تنظیمات محلی اعمال می‌شوند پس دارای اولویت بالاتری هستند.

این روش ترتیبی GPO ها پدیده‌ای به نام وراثت policy را خلق می‌کند. در یک مثال عملی ممکن است تنظیمی را در یک GPO لینک شده به دامنه پیکربندی کنیم که استفاده از ابزارهای ویرایش رجیستری را برای همه کاربران غیرفعال کند. این GPO و تنظیماتش توسط همه کاربران دامنه به ارث برده می‌شود. بهرحال ممکن است بخواهیم مدیران شبکه را از این قاعده مستثنی کنیم. چون GPO لینک شده به OU مدیران شبکه اولویت بالاتری از GPO به ارث رسیده دارد مدیران امکان تغییر رجیستری را پیدا خواهند کرد.

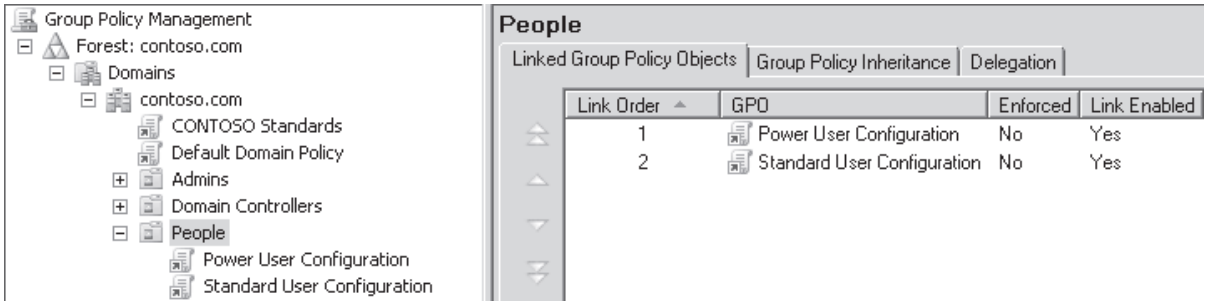


شکل ۹- ۶ زبانه Group Policy Inheritance

شکل ۹- ۶ این مسئله را نمایش می‌دهد. تنظیمی که ابزار ویرایش رجیستری را محدود می‌کند در CONTOSO Standards GPO که به دامنه contoso.com لینک شده تعریف می‌شود. تنظیمی به طور خاص در Corporate Policy Overrides For Administrators GPO اجازه دستکاری رجیستری را به مدیران شبکه می‌دهد. در کنسول GPMC وقتی یک OU را مانند Admins OU انتخاب می‌کنیم زبانه‌ای با نام Group Policy Inheritance نمایش داده می‌شود که در آن اولویت GPO برای آن OU قابل مشاهده است. در این جا به خوبی مشخص است که Corporate Policy Overrides For Administrators GPO دارای اولویت بالاتری است. هر تنظیمی در این GPO که با تنظیمی در CONTOSO Standards تداخل دارد از GPO مدیران تنظیم را اعمال می‌کند. بنابراین کاربران در Admins OU قادرند از ابزارهای ویرایش رجیستری استفاده کنند اگرچه کاربران دیگر در دامنه نمی‌توانند. همان طوری که از این مثال ساده دریافتیم ترتیب پیش فرض باعث می‌شود نزدیک‌ترین Policy به کاربر یا کامپیوتر بر بقیه غلبه می‌کند.

اولویت اشیاء Group Policy لینک شده

به یک OU، دامنه یا سایت می‌تواند بیش از یک GPO لینک شود. در این حالت ترتیب لینک (order link) مربوط به شیء اولویت آنها را مشخص می‌کند. در شکل ۱۰- ۶ دو GPO به People OU لینک شده است. شیء بالاتر در لیست با شماره لینک ۱ بالاترین اولویت را دارد. بنابراین تنظیماتی که در Power User Configuration GPO فعال یا غیرفعال است بر همین تنظیمات در Standard User Configuration GPO غلبه می‌کند.



شکل ۱۰- ۶ ترتیب لینک‌های GPO

جلوگیری از وراثت

می‌توانیم OU یا دامنه را طوری پیکربندی کنیم که از وراثت تنظیمات policy جلوگیری شود. برای این کار روی دامنه یا OU در GPME کلیک راست کرده و Block Inheritance را انتخاب می‌کنیم.

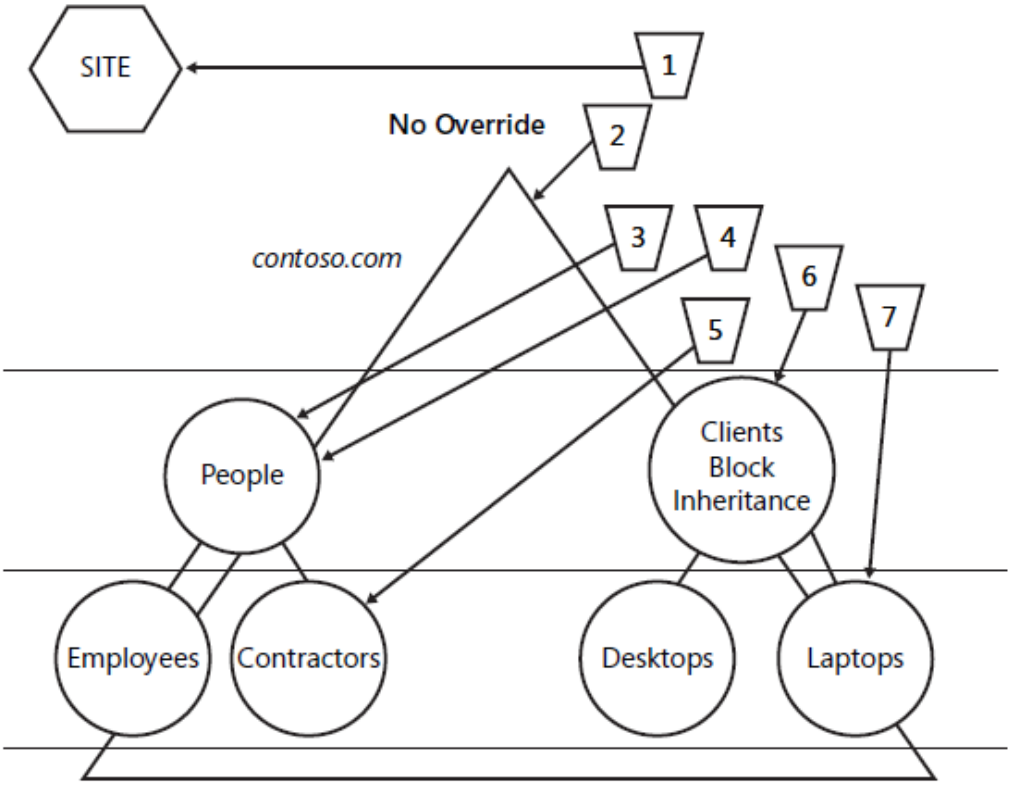
این گزینه یک خصیصه از دامنه یا OU می‌باشد بنابراین از وراثت همه تنظیمات Group Policy لینک شده به والد شیء جلوگیری می‌کند. وقتی از وراثت جلوگیری می‌شود برنامه GPO از اعمال تنظیمات GPO های لینک شده به طور مستقیم به OU کار را شروع می‌کند و GPO های لینک شده به OU، دامنه یا سایت سطح بالاتر هیچ‌گاه اعمال نمی‌شوند.

گزینه Block Inheritance بهتر است به ندرت استفاده شود. جلوگیری از وراثت ارزیابی اولویت و وراثت Group Policy را بسیار مشکل می‌کند. در بخش "استفاده از فیلتر امنیتی برای تغییر حوزه GPO" یاد می‌گیریم چطور حوزه یک GPO را طوری تعیین کنیم که فقط به یک زیرمجموعه از اشیاء اعمال شود یا نشود. با فیلتر کردن گروه امنیتی می‌توان حوزه یک GPO را طوری تعیین کرد تا فقط به کاربران و کامپیوترهای مورد نظر ما اعمال شود و ما را از گزینه Block Inheritance بی‌نیاز کند.

اعمال اجباری یک لینک GPO

لینک GPO می‌تواند به صورت اجباری پیکربندی شود. برای این کار روی لینک کلیک راست کرده و مطابق شکل ۷- ۶ از منو گزینه Enforced را انتخاب می‌کنیم. در این حالت GPO بالاترین اولویت را خواهد داشت و تنظیمات policy در این GPO بر همه تنظیمات GPO های دیگر که با آن تداخل دارند غلبه می‌کند. به علاوه چنین لینکی به container های فرزند خود اعمال می‌شود حتی اگر این container ها به حالت Block Inheritance پیکربندی شده باشند. گزینه Enforced باعث می‌شود policy به همه اشیاء در حوزه اعمال گردد. گزینه Enforced باعث می‌شود policy ها بر همه policy هایی که با آن تداخل دارند غلبه کند و صرف نظر از اینکه گزینه Block Inheritance انتخاب شده یا نه اعمال شود.

در شکل ۱۱- ۶ Block Policy Inheritance به Clients OU اعمال شده است. در نتیجه GPO1 که به سایت اعمال می‌شود بلوکه شده و به Clients OU اعمال نمی‌شود. GPO2 که با گزینه Enforced به دامنه لینک شده اعمال خواهد شد. در حقیقت این GPO آخر پردازش می‌شود یعنی تنظیمات آن بر GPO6 و GPO7 غلبه می‌کند.



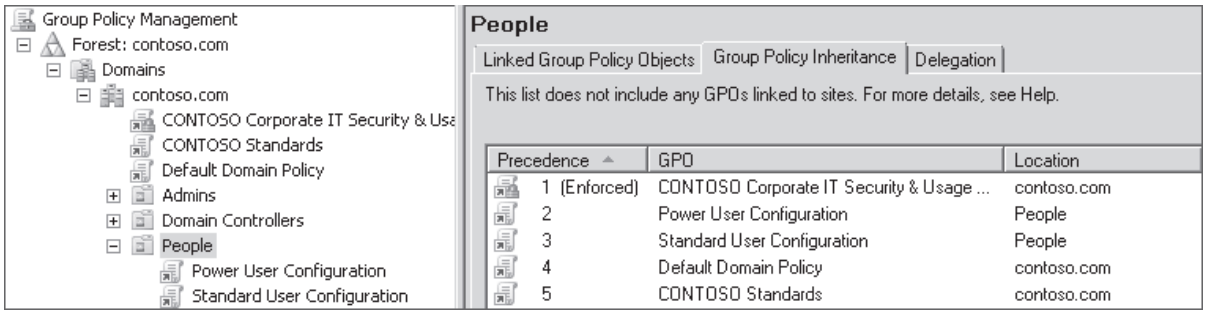
ترتیب پردازش GPO برای Contractors OU = ۱-۳-۴-۵-۲

ترتیب پردازش GPO برای Laptops OU = ۶-۷-۲

شکل ۱۱- ۶ پردازش policy با گزینه‌های Block Inheritance و Enforced

وقتی یک GPO را پیکربندی می‌کنیم که تنظیمات اجباری دیکته شده از طرف سازمان را تعریف کند باید مطمئن شویم تنظیمات دیگری از GPO های دیگر بر آن غلبه نکند. این کار با گزینه Enforced انجام می‌شود. شکل ۱۲- ۶ این سناریو را نمایش می‌دهد. تنظیمات دیکته شده توسط سیاست‌های سازمان در CONTOSO Corporate IT Security & Usage GPO که به صورت Enforced به دامنه contoso.com لینک شده پیکربندی شده است. آیکن لینک GPO دارای یک قفل می‌باشد که مشخص کننده لینک Enforced است. در People OU زبانه Group Policy Inheritance نشان می‌دهد که این GPO بر همه GPO ها حتی GPO های لینک شده مستقیم به خود OU غلبه می‌کند.

برای سهولت ارزیابی اولویت GPO به سادگی OU (یا دامنه) را انتخاب می‌کنیم و زبانه Group Policy Inheritance را باز می‌کنیم. این زبانه برآیند اولویت GPO ها، لینک‌های GPO، ترتیب لینک‌ها، جلوگیری از وراثت و Enforced شدن لینک را نمایش می‌دهد. این زبانه نه policy های لینک شده به سایت را و نه فیلتر امنیتی یا WMI را گزارش نمی‌کند



شکل ۱۲- ۶ اولویت GPO با لینک Enforced

نکته امتحانی هرچند جلوگیری از وراثت و گزینه Enforced توصیه نمی‌شود ولی در امتحان 70-640 انتظار می‌رود تاثیر این دو را یاد بگیرید.

استفاده از فیلتر امنیتی برای تغییر حوزه GPO

تا حالا یاد گرفتیم یک GPO را به یک سایت دامنه یا OU لینک دهیم. بهرحال ممکن است نیاز داشته باشیم GPO را فقط به گروههایی از کاربران یا کاپیوترهای مشخصی اعمال کنیم تا همه کاربران یا کامپیوترهای حوزه GPO . هرچند به طور مستقیم نمی‌توان یک GPO را به یک گروه امنیتی لینک کرد ولی راهی برای اعمال GPO به گروه وجود دارد. Policy های یک GPO فقط به کاربرانی که مجوز Allow Read و Allow Apply Group Policy به GPO دارند اعمال می‌شود.

هر GPO دارای ACL است که مجوزهای GPO را تعریف می‌کند. دو مجوز Allow Read و Allow Apply Group Policy برای اعمال یک GPO به کاربر یا کامپیوتر مورد نیاز است. برای مثال اگر کامپیوتری به واسطه لینک یک GPO به Computers OU در حوزه آن GPO قرار گیرد ولی مجوزهای نام برده را نداشته باشد قادر به دانلود و اعمال GPO نخواهد بود. بنابراین با تنظیم مجوزهای مناسب برای گروههای امنیتی می‌توان یک GPO را طوری فیلتر کرد که تنظیمات فقط به کامپیوترها و کاربران مورد نظر ما اعمال شود.

به طور پیش فرض گروه Authenticated Users مجوز Allow Apply Group Policy را روی GPO جدید دارند. این بدین معنی است که همه کاربران و کامپیوتر ها تحت تاثیر GPO های لینک شده به دامنه، سایت یا OU قرار می‌گیرند صرف نظر از گروههای دیگری که عضوی از آن باشند. بنابراین دو راه برای فیلترکردن حوزه GPO وجود دارد:

- مجوز Apply Group Policy را از گروه Authenticated Users حذف می‌کنیم ولی این مجوز را deny نمی‌کنیم. سپس گروههایی که GPO باید به آنها اعمال شود پیدا کرده و مجوز Read و Apply Group Policy را برای آنها Allow می‌کنیم.

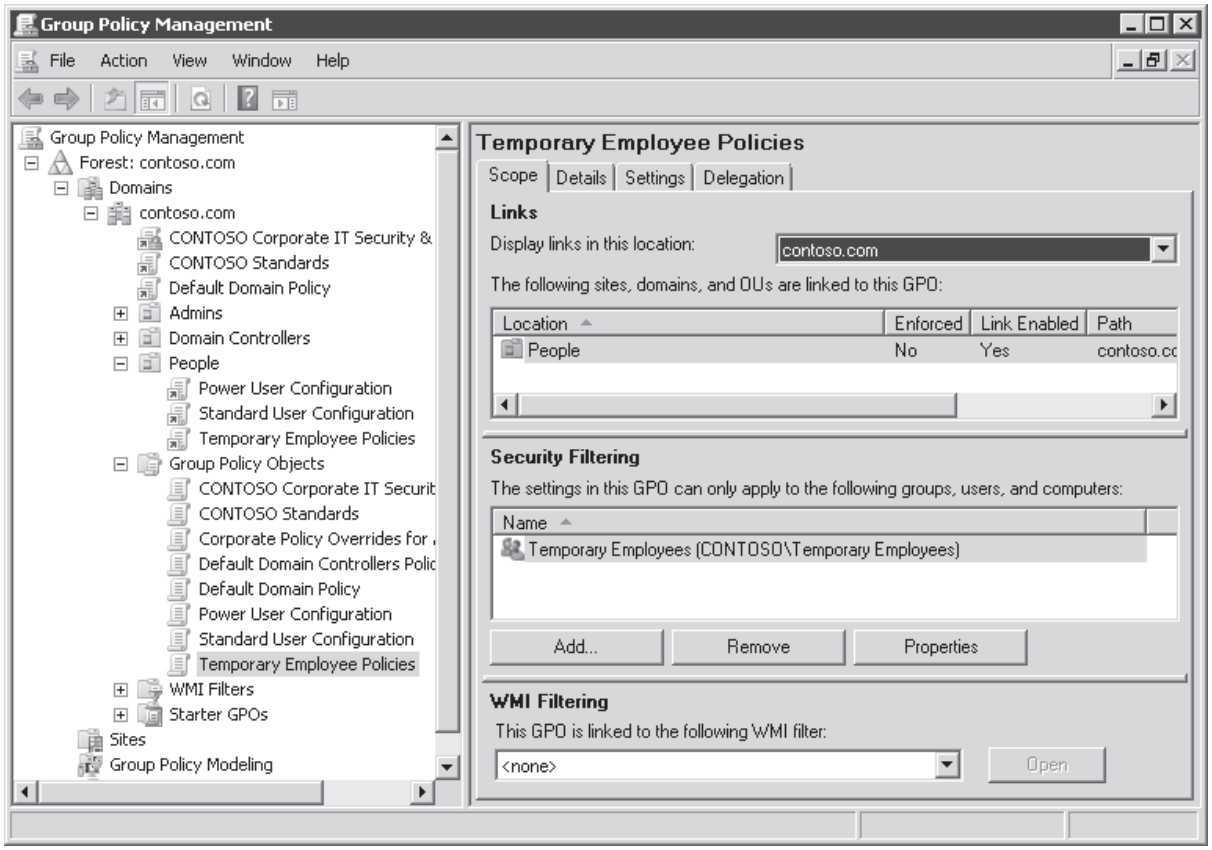
- گروههایی که GPO نباید به آنها اعمال شود را مشخص کرده و مجوز Apply Group Policy را برای آنان deny می‌کنیم. با این کار کاربر یا کامپیوتر نمی‌تواند تنظیمات GPO را اعمال کند حتی اگر کاربر یا کامپیوتر عضو گروه دیگری باشد که دسترسی‌های لازم را داشته باشد.

فیلتر کردن یک GPO برای اعمال به گروههای مشخص

برای اعمال یک GPO به یک گروه امنیتی مشخص در Group Policy Objects container واقع در GPMC ، GPO مورد نظر را انتخاب می‌کنیم. در بخش Security Filtering گروه Authenticated Users را انتخاب کرده و Remove را کلیک می‌کنیم. OK را برای تایید کلیک می‌کنیم و سپس Add را می‌زنیم. گروهی را که می‌خواهیم policy به آن اعمال شود انتخاب کرده و OK می‌کنیم. نتیجه چیزی شبیه به شکل ۱۳- ۶ خواهد بود که گروه Authenticated Users لیست نشده و گروهی که policy باید به آن اعمال شود لیست شده است.

نکته استفاده از گروههای امنیتی global برای فیلتر کرده GPO ها

GPO ها فقط با گروههای امنیتی global فیلتر می‌شوند نه با domain local

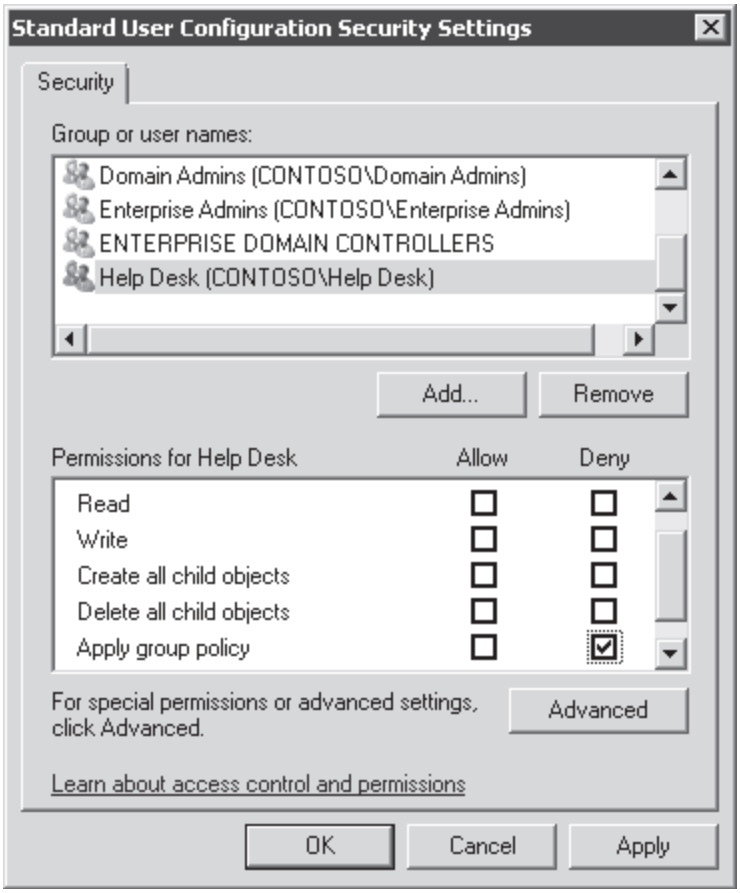


شکل ۱۳- ۶ فیلتر امنیتی یک GPO

فیلتر کردن یک GPO برای مستثنی کرده گروههای خاص

متاسفانه زبانه Scope مربوط به GPO اجازه مستثنی کردن (exclude) گروه‌ها را نمی‌دهد. برای این کار که به معنی deny کردن مجوز Apply Group Policy می‌باشد باید زبانه Delegation را باز کنیم. دکمه Advdnced را کلیک کنیم که کادر محاوره‌ای Security Settings ظاهر می‌شود. روی دکمه Add کلیک می‌کنیم و گروهی که می‌خواهیم مستثنی کنیم انتخاب و OK می‌کنیم. گروه به طور پیش فرض مجوز Allow Read دارد. علامت کادر مربوط به این مجوز را برداشته و Deny Apply Group Policy را انتخاب می‌کنیم. شکل ۱۴- ۶ مثالی را نشان می‌دهد که در آن مجوز Apply Group Policy مربوط به گروه HelpDesk را deny کرده‌اند بنابراین گروه از حوزه GPO مستثنی شده است.

وقتی درکادر Security Settings روی دکمه OK کلیک می‌کنیم پیغامی به ما هشدار می‌دهد که مجوز Deny بر مجوزهای دیگر غلبه می‌کند. برای همین پیشنهاد می‌شود تا حد امکان از Deny استفاده نشود. استفاده از این روش نسبت به روش اضافه کردن گروه در بخش Security Filtering از زبانه Scope بسیار سخت‌تر است.



شکل ۱۴- ۶ مستثنی کردن یک گروه از حوزه GPO با deny کردن مجوز Apply Group Policy

نکته مجوز deny شده در زبانه Scope نشان داده نمی‌شود.

متاسفانه وقتی گروهی مستثنی می‌شود این استثنا در بخش Security Filtering از زبانه Scope نمایش داده نمی‌شود. این یک دلیل دیگری است برای اینکه مجوز را deny نکنیم.

فیلترهای WMI

Windows Management Instrumentation (WMI) یک فن‌آوری زیرساخت مدیریتی است که مدیران شبکه را قادر می‌کند اشیاء managed را در شبکه مانیتور و کنترل کنند. یک پرس و جوی WMI بسته به خصوصیاتی نظیر RAM، سرعت CPU، ظرفیت دیسک، آدرس IP، نسخه سیستم عامل و سرویس پک، برنامه‌های نصب شده و ویژگی‌های چاپگر قادر به اجرای سیستم‌های فیلترینگ می‌باشد. چون WMI تقریبا همه خصوصیات اشیاء را در کامپیوتر آشکار می‌کند لیست خصیصه‌هایی که در پرس و جوی WMI استفاده می‌شود تقریبا نامحدود است. پرس و جوی WMI با زبان WMI query language (WQL) نوشته می‌شود. ما می‌توانیم از پرس و جوی WMI برای ساخت فیلتر WMI استفاده کنیم و با آن GPO را فیلتر کنیم. یک راه خوب برای درک اهداف فیلتر WMI هم برای امتحان و هم پیاده‌سازی در دنیای واقعی بیان مثال است. Group Policy با هدف توزیع برنامه و سرویس پک قابل استفاده است قابلیتی که در فصل ۷ بحث می‌شود. ما می‌توانیم به منظور توزیع یک برنامه کاربردی یک GPO ساخته و با فیلتر WMI تعیین کنیم که policy فقط باید به کامپیوترهایی با سیستم عامل و سرویس پک مشخص به عنوان مثال ویندوز XP با سرویس پک ۳ اعمال شود. پرس و جوی WMI برای مثال بالا به شکل زیر است:

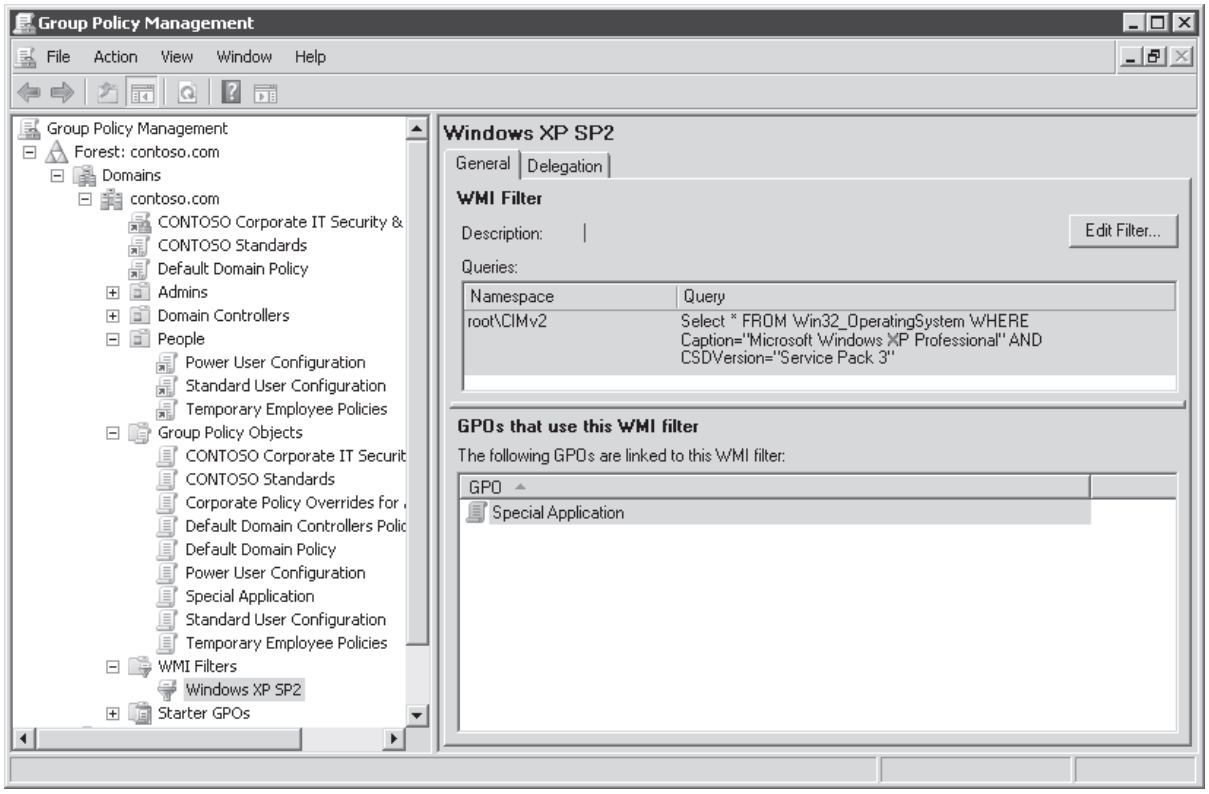
```
Select * FROM Win32_OperatingSystem WHERE Caption=”Microsoft
Windows XP Professional” AND CSDVersion=”Service Pack 3”
```

وقتی کلاینت Group Policy همه GPO هایی که دانلود کرده ارزیابی می‌کند تا تعیین کند کدام‌یک را برای پردازش باید به CSE ها تحویل دهد، یک پرس و جو روی سیستم محلی اجرا می‌کند. اگر سیستم شرایط تعیین شده در پرس و جو را احراز کند نتیجه پرس و جو True بوده و CSE ها شروع به پردازش GPO می‌کنند.

WMI فضای نام را آشکار می‌کند که در آنها کلاس‌هایی موجود است که می‌تواند مورد پرس و جو قرار بگیرند. بسیاری از کلاس‌های مفید شامل Win32_Operating System در یک کلاس با نام root\CIMv2 وجود دارند.

برای ساخت فیلتر WMI در GPME روی گره WMI Filters کلیک راست کرده و New را انتخاب می‌کنیم. نامو توضیحی را برای فیلتر تایپ کرده و دکمه Add را کلیک می‌کنیم. در کادر Namespace فضای نام پرس و جو را تایپ می‌کنیم. در کادر Query پرس و جو را وارد می‌کنیم و سپس OK می‌کنیم.

برای فیلتر کردن GPO با فیلتر WMI زبانه Scope یک GPO را باز کرده و از لیست بازشوی WMI فیلتر Wmi را انتخاب می‌کنیم. یک GPO فقط توسط یک فیلتر WMI می‌تواند فیلتر شود ولی همان فیلتر WMI می‌تواند یک پرس و جوی ترکیبی با شروط (criteria) چندگانه باشد. یک فیلتر WMI منفرد می‌تواند به یک یا چند GPO لینک شود و آنها را فیلتر کند. زبانه General فیلتر WMI همان‌گونه که در شکل ۱۵- ۶ نشان داده شده است GPO هایی را نمایش می‌دهد که از فیلتر WMI استفاده می‌کنند.



شکل ۱۵- ۶ یک فیلتر WMI

درباره فیلترهای WMI سه نکته مهم وجود دارد. اول اینکه شکل فرمان WQL مربوط به پرس و جوی WMI کمی پیچیده است. با جستجوی کلید واژه WMI filter و WMI query و توضیحی درباره پرس و جو در اینترنت می‌توانیم نمونه‌هایی از آن را پیدا کنیم.

اطلاعات بیشتر نمونه فیلتر WMI

در آدرس http://technet2.microsoft.com/windowsserver/en/library/a16cffa4-83b3-430b-b826-9bf81c0d39a71033.mspx?mfr=true می‌توانیم نمونه‌هایی از فیلترهای WMI پیدا کنیم. همچنین می‌توانیم به WMI software development kit (SDK) در آدرس http://msdn2.microsoft.com/en-us/library/aa394582.aspx مراجعه کنیم.

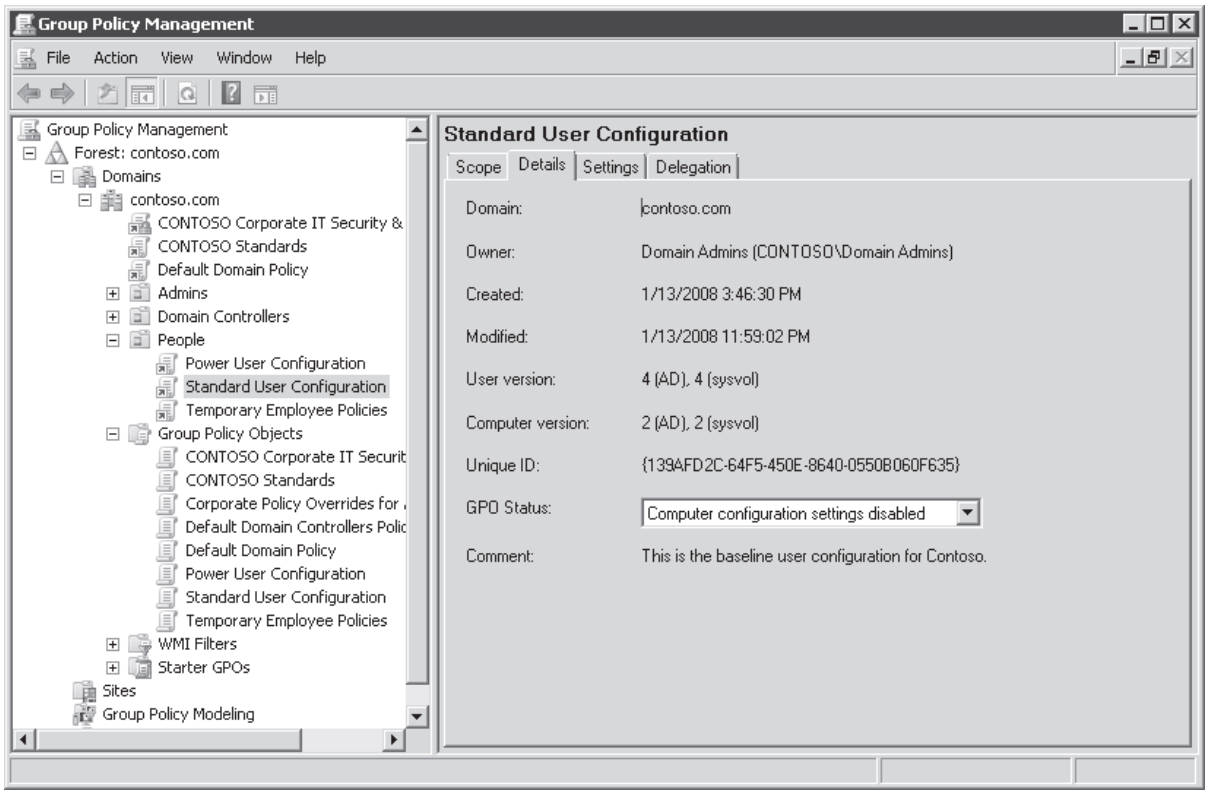
دوم اینکه فیلترهای WMI از لحاظ اجرا باری را به سیستم تحمیل می‌کند. چون کلاینت Group Policy باید پرس و جوی WMI را در بازه‌های زمانی مشخص اجرا کند هر ۹۰ تا ۱۲۰ دقیقه روی کارایی سیستم تاثیر می‌گذارد. با مشخصات سخت افزاری کامپیوترهای کنونی این تاثیر قابل ملاحظه نیست ولی باید قبل از توزیع این فیلترها آنها را آزمایش کنیم.

سوم اینکه این فیلترها توسط سیستم‌های ویندوز 2000 پردازش نمی‌شوند. اگر یک GPO با یک فیلتر WMI فیلتر شود سیستم ویندوز 2000 آنرا در نظر نمی‌گیرد و GPO را طوری پردازش می‌کند که گویی نتیجه فیلتر True می‌باشد.

فعال یا غیرفعال کردن GPO ها و گره‌های GPO

با تغییر وضعیت GPO امکان جلوگیری از پردازش تنظیمات گره‌های Computer Configuration یا User Configuration حین به روز رسانی وجود دارد. در زبانه Details مربوط به GPO که در شکل ۱۶- ۶ می‌بینیم روی لیست بازشوی GPO Status کلیک کرده و یکی از گزینه‌های زیر را انتخاب می‌کنیم:

- **Enabled** هردوی تنظیمات پیکربندی کاربر و کامپیوتر در هنگام به روز رسانی توسط CSE ها پردازش می‌شوند.
- **All Settings Disabled** CSE ها GPO ها را پردازش نمی‌کنند.
- **Computer Configuration Settings Disabled** هنگام به روز آوری policy کامپیوتر، تنظیمات پیکربندی کامپیوتر موجود در GPO اعمال می‌شود ولی GPO در زمان به روز آوری policy کاربر پردازش نمی‌شود.
- **User Configuration Settings Disabled** هنگام به روز آوری policy کاربر، تنظیمات پیکربندی کاربر موجود در GPO اعمال می‌شود ولی GPO در زمان به روز آوری policy کامپیوتر پردازش نمی‌شود.



شکل ۱۶- ۶ زبانه Details مربوط به GPO

با پیکربندی GPO Status می‌توانیم پردازش policy را بهینه کنیم. به عنوان مثال اگر یک GPO فقط مجموعه تنظیمات کاربر را در برگیرد GPO Status را در وضعیتی قرار می‌دهیم که تنظیمات کامپیوتر غیرفعال شود. در این حالت کلاینت Group Policy از پردازش GPO هنگام به روز رسانی policy کامپیوتر جلوگیری می‌کند. چون GPO هیچ تنظیمی روی کامپیوتر ندارد نیازی به پردازش GPO نیست و به این شکل می‌توانیم از اتلاف زمان پردازنده کامپیوتر جلوگیری کنیم.

نکته از GPO های غیرفعال برای زمان‌های بحرانی استفاده کنیم

ممکن است بخواهیم یک پیکربندی را در یک GPO تعریف کنیم که در موارد اضطراری مانند اشکالات امنیتی از آن بهره ببریم. بعد آن را به کاربران و کامپیوترهای مناسب لینک کنیم. سپس آنرا غیرفعال کنیم. در هنگام حادثه به راحتی آنرا فعال کرده و تنظیمات مورد نظر را اعمال کنیم.

هدفمند کردن preferences

Preferences که در ویندوز سرور 2008 گزینه جدیدی است مکانیزم تعیین حوزه‌ای با نام item-level targeting دارد. ما می‌توانیم آیتم‌های preference چندگانه را در یک GPO داشته باشیم و هر آیتم preference قابل هدفمند کردن و فیلترشدن است. بنابراین برای مثال ممکن است یک GPO منفرد با یک preference داشته باشیم که تنظیمات folder options را برای مهندسین شرکت تعریف می‌کند و آیتم دیگری برای تعیین تنظیمات folder options برای کارمندان بخش فروش داشته باشیم. با استفاده از یک گروه امنیتی یا OU می‌توانیم آیتم‌ها را هدفمند کنیم. تعداد شروط ممکن برای استفاده به دهها عدد می‌رسد که شامل خصوصیات شبکه و سخت‌افزار، ساعت و تاریخ، پرس و جوی LDAP و غیره می‌باشد.

نکته preference ها می‌توانند در یک GPO هر کدام برای جامعه هدف متفاوت پیکربندی شوند

آنچه که درباره preference جدید است این است که به جای چند GPO می توانیم چند آیتم را در یک GPO داشته باشیم. با Policy های سنتی اغلب نیاز به چند GPO داریم که برای اعمال تنظیمات مختلف روی گروه های خاص فیلتر شده اند.

item-level targeting هم مانند فیلترهای WMI برای اجرای پرس و جو نیاز به CSE دارد تا مشخص شود تنظیمات یک آیتم preference باید اعمال شود یا نه. ما باید مواظب تاثیر item-level targeting بر روی کارایی سیستم خود باشیم مخصوصا اگر از گزینه هایی نظیر پرس و جوی LDAP استفاده کنیم که زمانی را صرف پردازش و گرفتن پاسخ از DC می کند. همزمان با طراحی زیرساخت Group Policy باید تعادلی بین مزایای item-level targeting در مدیریت پیکربندی و تاثیر آن در کارایی سیستم برقرار کنیم.

پردازش Group Policy

حالا که با مفهوم، اجزاء و تعیین حوزه Group Policy آشنا شدیم می توانیم وارد جزئیات پردازش Group Policy شویم. ترتیب اعمال تنظیمات پیکربندی را یاد گرفتیم. جملات زیر جزئیات بیشتری در مورد مراحل اعمال GPO های مبتنی بر دامنه بر کاربر یا کامپیوتر ارائه می کند:

۱. کامپیوتر روشن می شود. سرویس Remote Procedure Call System Service (RPCSS) و Multiple Universal Naming Convention Provider (MUP) استارت می شود. کلاینت Group Policy استارت می شود.

۲. کلاینت Group Policy یک لیست مرتب شده از GPO های حوزه ای که کامپیوتر در آن قرار دارد دریافت می کند. ترتیب این لیست ترتیب پردازش GPO را تعیین می کند که به طور پیش فرض تنظیمات محلی، سایت، دامنه و OU است:

a. GPO های محلی. کامپیوتر دارای ویندوز سرور 2003، XP و 2000 دقیقا یک GPO دارند که روی همان سیستم ذخیره می شود. ویندوز ویستا و 2008 چندین GPO محلی دارند. اولویت GPO های محلی در بخش "GPO های محلی" در درس ۱ بحث می شود.

b. GPO های سایت. همه GPO هایی که به سایت لینک می شود در رده بعدی لیست قرار می گیرد. وقتی چند GPO به یک سایت (یا دامنه یا OU) لینک می شود خصیصه link order که در زبانه Scope پیکربندی می شود ترتیب آنرا مشخص می کند. GPO بالاتر در لیست که به عدد ۱ نزدیک تر است دارای اولویت بالاتر است و در آخر به لیست اضافه می شود. بنابراین آخر پردازش می شود و تنظیمات آن روی تنظیمات GPO هایی که زودتر اعمال شده اند می نشیند.

c. GPO های دامنه. این GPO ها به ترتیب مشخص شده در link order اضافه می شوند.

نکته policy های لینک شده به دامنه توسط دامنه های فرزند به ارث نمی رسند

policy های دامنه والد توسط دامنه های فرزند به ارث نمی رسند. هر دامنه لینک های مستقیم خود را دارد. ولی کامپیوترها در دامنه های متعدد ممکن است در حوزه یک GPO لینک شده به یک سایت قرار گیرد.

d. GPO های GPO. OU های لینک شده به OU ابتدا از بالاترین سطح در ساختار درختی Active Directory به لیست اضافه می‌شوند و بعد OU های فرزند و بقیه. درنهایت GPO های لینک شده به OU که شامل کامپیوتر می‌باشد افزوده می‌شوند. اگر policy های متعددی به یک OU لینک شود به ترتیبی که توسط link order مشخص شده افزوده می‌شوند.

e. Enforced GPOs . این نوع از GPO ها به انتهای لیست مرتب شده اضافه می‌شوند بنابراین تنظیمات آن در انتهای پردازش اعمال می‌شود و بر تنظیماتی که زودتر اعمال شده غلبه می‌کند. نکته این است که این نوع GPO ها به طور معکوس ترتیب بندی می‌شوند بعنی اول OU بعد دامنه و سپس سایت. این مطلب زمانی اهمیت پیدا می‌کند که سیاست‌های امنیتی شرکت را در قالب یک Enforced GPO به دامنه لینک کنیم. این GPO در آخر لیست مرتب شده قرار می‌گیرد و در نتیجه در آخر اعمال می‌شود و تنظیماتش در بالاترین اولویت قرار می‌گیرند.

۳. GPO ها به ترتیب مشخص شده در لیست‌های مرتب شده پردازش می‌شوند. این یعنی اینکه تنظیمات GPO محلی اول پردازش می‌گردد و بعد GPO لینک شده به سایت بعد دامنه و در آخر OU های شامل کاربر یا کامپیوتر. GPO های لینک شده به OU که کامپیوتر یا کاربر عضو مستقیم آن است آخر پردازش می‌شود و در نهایت Enforced GPO ها پردازش می‌گردند.

همان‌طوری که GPO پردازش می‌شود سیستم بر اساس وضعیت GPO برای گره کامپیوتر (فعال یا غیرفعال) مشخص می‌کند تنظیمات آن باید اعمال شود یا نه و آیا کامپیوتر مجوز Allow Group Policy دارد یا نه. اگر یک فیلتر WMI به GPO اعمال شده باشد و اگر کامپیوتر دارای سیستم عامل ویندوز XP به بعد باشد پرس و جوی WQL مشخص شده در فیلتر اجرا می‌شود.

۴. اگر قرار باشد GPO به سیستم اعمال شود CSE ها شروع پردازش تنظیمات GPO می‌کنند. تنظیمات policy در GPO از روش‌های زیر بر policy های GPO که قبلا اعمال شده غلبه می‌کند:

- اگر یک policy در یک GPO لینک شده به یک container پیکربندی شده باشد (فعال یا غیرفعال) و همان policy در GPO لینک شده به container فرزند به حالت Not Configured باشد برایند policy ها برای کاربران و کامپیوترهای container فرزند تنظیم policy والد خواهد بود. اگر container فرزند با گزینه Block Inheritance پیکربندی شده باشد تنظیم والد به ارث نمی‌رسد مگر لینک GPO با گزینه Enforced پیکربندی شده باشد.

- اگر یک تنظیم policy برای container والد پیکربندی شده باشد (فعال یا غیرفعال) و همان policy برای فرزند پیکربندی شده باشد تنظیم policy فرزند بر تنظیمات موروثی والد غلبه می‌کند. اگر لینک GPO والد با گزینه Enforced پیکربندی شده باشد تنظیم والد در اولویت قرار می‌گیرد.

- اگر policy مربوط به GPO های لینک شده به container والد به حالت Not Configured باشد و تنظیم OU فرزند نیز Not Configured باشد برایند تنظیم، تنظیمی خواهد بود که از پردازش GPO محلی به دست

می‌آید. اگر این تنظیم نیز Not Configured باشد تنظیم نهایی پیش فرض ویندوز خواهد بود.

۵. وقتی کاربر به سیستم وارد می‌شود مراحل ۲و ۳ و ۴ برای تنظیم کاربر تکرار می‌شود. کلاینت یک لیست مرتب شده از GPO های حوزه کاربر دریافت کرده به صورت متقارن GPO ها را تست کرده و GPO هایی که باید اعمال شود به CSE های مناسب به منظور پردازش تحویل داده می‌شود. اگر User Loopback Group Policy Processing فعال باشد این مرحله تغییر می‌کند. این گزینه در بخش بعدی معرفی می‌شود.

نکته تنظیمات policy در گره‌های Computer Configuration و User Configuration بسیاری از تنظیمات policy یا مختص User Configuration است یا مختص Computer Configuraion . تعداد کمی از تنظیمات در هر دو گره موجود است. اگرچه در بیشتر موارد تنظیم گره Computer Configuraion بر همان تنظیم در User Cinfiguration غلبه می‌کند بهتر است متن توضیحی درباره تنظیم policy خوانده شود تا تاثیر تنظیم را متوجه شویم.

۶. هر ۹۰ تا ۱۲۰ دقیقه یک بار بعد از بوت شدن کامپیوتر به روز رسانی policy کامپیوتر اتفاق می‌افتد و مراحل ۲و۳و۴ برای تنظیمات کامپیوتر تکرار می‌شود.

۷. هر ۹۰ تا ۱۲۰ دقیقه یک بار بعد از ورود کاربر به سیستم به روز رسانی policy کاربر اتفاق می‌افتد و مراحل ۲و۳و۴ برای تنظیمات کاربر تکرار می‌شود.

نکته تنظیمات ممکن است به سرعت اتفاق نیافتد

اگرچه بیشتر تنظیمات حین به روز رسانی اعمال می‌شوند برخی CSE ها تا راه اندازی مجدد یا ورود مجدد به سیستم اتفاق نیافتد تنظیم را اعمال نمی‌کنند. برای مثال اسکریپت‌های startup و logon که جدیدا اضافه شده‌اند تا راه اندازی مجدد یا ورود مجدد به سیستم اعمال نمی‌شود. نصب نرم‌افزار که در فصل ۷ بحث می‌شود پس از راه اندازی مجدد اتفاق می‌افتد اگر نرم‌افزار در تنظیمات کامپیوتر assign شده باشد. نمونه دیگر تغییرات policy تغییر مسیر پوشه اختصاصی کاربر می‌باشد که بعد از ورود مجدد به سیستم اتفاق می‌افتد.

پردازش policy در حالت Loopback

به طور پیش فرض تنظیمات کاربر از GPO که کاربر در حوزه آن قرار دارد نشات می‌گیرد. صرف نظر از اینکه کاربر از طریق کدام سیستم به شبکه وارد می‌شود policy های نهایی ثابت است. مواقعی ممکن است بخواهیم کاربر بر اساس کامپیوتر مورد استفاده پیکربندی‌های متفاوتی داشته باشد. برای مثال اگر بخواهیم کاربر هنگام استفاده از کامپیوترهای اتاق کنفرانس، پذیرش، کتابخانه و کلاس نتواند دسک‌تاپ خود را تغییر دهد از پردازش policy به حالت Loopback استفاده می‌کنیم. در این نوع پردازش الگوریتم پیش فرض کلاینت Group Policy برای دریافت لیست GPO هایی که باید به پیکربندی کاربر اعمال شود تغییر می‌کند. به جای اینکه پیکربندی کاربر توسط گره User Configuration که کاربر در حوزه آن قرار دارد تعریف شود توسط پیکربندی کاربر که در گره User Configuraion مربوط به GPO که شیء کامپیوتر در حوزه آن قرار می‌گیرد تعریف می‌گردد.

تنظیم User Group Policy Loopback Processing Mode که در پوشه Computer Configuraion\Policies\Administrative Templates\System\Group Policy در ابزار GPME قرار دارد مانند دیگر policy ها می‌تواند Not Configured، Enabled یا Disabled باشد. در حالت enabled تنظیم می‌تواند حالت Replace یا Merge را تعریف کند.

- **Replace** در این حالت لیست GPO برای کاربر (در مرحله ۵ بخش "پردازش Group Policy" دریافت شده) تماما با لیست GPO که قبلا برای کامپیوتر دریافت شده حین بوت شدن کامپیوتر (مرحله ۲) جایگزین می‌شود. تنظیمات policy های User Configuration مربوط به GPO کامپیوتر به کاربر اعمال می‌شود. حالت Replace در وضعیتی

مانند کلاس که کاربران بهتر است یک پیکربندی استاندارد را دریافت کنند مفید به نظر می‌رسد.

- **Merge** در این حالت لیست GPO که در هنگام بوت شدن سیستم برای کامپیوتر دریافت شده (مرحله ۲) به لیست GPO به دست آمده برای کاربر هنگام ورود به سیستم اضافه می‌شود(مرحله ۵). چون لیست GPO به دست آمده برای کامپیوتر بعدا اعمال می‌شود اگر تداخلی با تنظیمات لیست کاربر داشته باشد تنظیمات GPO ها در لیست کامپیوتر اولویت دارند. این حالت زمانی مفید خواهد بود که بخواهیم تنظیمات اضافی را به پیکربندی‌های معمولی کاربران اضافه کنیم. برای مثال ممکن است بخواهیم به کاربری اجازه دهیم هنگام ورود به کامپیوتر اتاق کنفرانس یا واحد پذیرش پیکربندی خود را دریافت کند ولی wallpaper با یک عکس استاندارد جایگزین شود و استفاده از برنامه‌ها یا دستگاههای بخصوصی غیرفعال شود.

تمرینات پیکربندی حوزه Group Policy

در این تمرینات سناریویی را دنبال می‌کنیم که بر اساس GPO که در درس ۱ ساختیم و پیکربندی کردیم ایجاد می‌شود. در هر مرحله ما تعیین حوزه Group Policy را اصلاح می‌کنیم. قبل از اجرای این تمرینات، تمرینات درس ۱ را انجام دهید.

تمرین ۱ ساخت یک GPO با یک تنظیم policy که بر تنظیم دیگری غلبه می‌کند.

فرض می‌کنیم یکی از مدیران شبکه در دامنه contoso.com هستیم. CONTOSO Standards GPO که به دامنه لینک شده است تنظیمی را پیکربندی کرده است که زمان screen saver را ۱۰ دقیقه مشخص کرده است. یکی از مهندسان شرکت گزارش می‌دهد که یک برنامه مهم و طولانی هنگام اجرای screen saver با مشکل مواجه می‌شود. او از ما می‌خواهد این تنظیم را برای اعضای تیم مهندسان شرکت که از این برنامه استفاده می‌کنند غیرفعال کنیم.

۱. با کاربر Administrator به SERVER01 وارد می‌شویم.

۲. ابزار Active Directory Users And Computers را باز کرده و یک OU سطح اول با نام People و یک OU فرزند با نام Engineers می‌سازیم.

۳. GPMC را باز می‌کنیم.

۴. روی Engineers OU کلیک راست کرده و Create A GPO In This Domain, And Link It Here را انتخاب می‌کنیم.

۵. نام Engineering Application Override را وارد و OK می‌کنیم.

۶. گره Engineers OU را باز کرده و روی GPO کلیک راست کرده و Edit را انتخاب می‌کنیم.

۷. گره User Cinfiguration\Policies\Administrative Templates\Control Panel\Display را باز می‌کنیم.

۸. روی تنظیم Screen Saver Timeout دوبار کلیک می‌کنیم.

۹. Disabled را انتخاب و OK می‌کنیم.

۱۰. GPME را می‌بندیم.

۱۱. در پنجره GPMC، Engineers OU را انتخاب کرده و زبانه Group Policy Inheritance را باز می‌کنیم.

۱۲. توجه کنید که Engineering Application Override GPO بر CONTOSO Standards GPO اولویت دارد.

تنظیمی که ما پیکربندی کردیم و screen saver را غیرفعال کرده است بر تنظیم مشابه در CONTOSO Standards GPO غلبه می‌کند.

تمرین ۲ پیکربندی گزینه Enforced

می‌خواهیم مطمئن شویم همه سیستم‌ها تغییرات Group Policy را به سرعت دریافت می‌کنند. برای این کار می‌خواهیم تنظیم Always Wait For The Network Group Policy را فعال کنیم و اجازه ندهیم هیچ مدیر شبکه‌ای این policy را مغلوب کند و این باید به همه سیستم‌ها اعمال شود.

۱. در پنجره GPMC روی دامنه contoso.com کلیک راست کرده و Create A GPO In This Domain, And Link It Here را انتخاب می‌کنیم.

۲. نام Enforced Domain Policies را وارد و OK می‌کنیم.

۳. روی GPO کلیک راست کرده و Edit را انتخاب می‌کنیم.

۴. گره Computer Configuration\Policies\Administrative Templates\System\Logon را باز می‌کنیم.

۵. روی تنظیم Always Wait For The Network At Computer Startup And Logon دوبار کلیک می‌کنیم.

۶. Enabled را انتخاب و OK می‌کنیم.

۷. GPME را می‌بندیم.

۸. روی Enforced Domain Policies GPO کلیک راست کرده Enforced را انتخاب می‌کنیم.

۹. Engineers OU را انتخاب و زبانه Group Policy Inheritance را باز می‌کنیم.

توجه داشته باشید enforced GPO دامنه حتی بر GPO لینک شده به Engineers OU غلبه می‌کند. تنظیمات یک GPO همانند Engineering Application Override نمی‌تواند تنظیماتش را به درستی اعمال کند.

تمرین ۳ پیکربندی فیلتر امنیتی

با گذشت زمان متوجه می‌شویم که تعداد کمی از کاربران باید از تنظیم screen saver مستثنی شوند. به این نتیجه می‌رسیم که استفاده از تنظیمات غالب عملی نیست. به جای آن از فیلتر امنیتی برای مدیریت حوزه GPO استفاده می‌کنیم.

۱. ابزار Active Directory Users And Computers را باز کرده و یک OU با نام Groups می‌سازیم و در آن یک گروه امنیتی global با نام GPO_CONTOSO Standards_Exceptions می‌سازیم.

۲. در GPMC سپس Group Policy Objects container را انتخاب می‌کنیم.

۳. روی Engineering Application Override GPO کلیک راست کرده و Delete را انتخاب می‌کنیم. Yes را

برای تایید کلیک می‌کنیم.

۴. CONTOSO Standards GPO را در Group Policy Objects container انتخاب می‌کنیم.

۵. زبانه Delegation را کلیک می‌کنیم.

۶. دکمه Advanced را کلیک می‌کنیم.

۷. در کادرمحاوره‌ای Security Settings دکمه Add را کلیک می‌کنیم.

۸. نام گروه را تایپ کرده و OK می‌کنیم.

۹. در لیست مجوزها نوار پیمایش را به سمت پایین می‌کشیم و مجوز Apply Group Policy را Deny می‌کنیم. سپس OK می‌کنیم.

۱۰. Yes را کلیک می‌کنیم.

۱۱. به ردیف نمایش داده شده در زبانه Delegation در ستون Allowed Permissions برای گروه GPO_CONTOSO Standards_Exceptions توجه کنید

۱۲. زبانه Scope را کلیک کرده و بخش Security Filtering را بررسی می‌کنیم.
فیلتر امنیتی پیش فرض GPO جدید به این صورت است که گروه Authenticated Users مجوز Allow Apply Group Policy را دارند بنابراین همه کاربران و کامپیوترها در حوزه لینک GPO تنظیمات آنرا اعمال می‌کنند. حالا ما یک گروه با مجوز Deny Apply Group Policy پیکربندی کرده‌ایم که بر مجوز Allow غلبه می‌کند. اگر کاربری نیاز دارد از CONTOSO Standards GPO مستثنی شود کامپیوتر را به راحتی به گروه اضافه می‌کنیم.

تمرین ۴ پردازش policy در حالت Loopback

اخیرا یکی از کارمندان فروش در شرکت Contoso کامپیوتر خود را روشن کرده تا به یکی از مشتریان مهم شرکت توضیحی ارائه دهد در حالی که صفحه دسک‌تاپ ویندوز برای این کار نامناسب به نظر می‌رسیده است. مدیریت شرکت از ما خواسته لپ‌تاپ های بخش فروش wallpaper نداشته باشند. وقتی این کارمندان به کامپیوترهای رومیزی وارد می‌شوند نیازی به مدیریت wallpaper نخواهد بود. ولی وقتی به لپ‌تاپ خود وارد می‌شوند باید روی آن کنترل داشته باشیم. برای این کار از پردازش policy در حالت loopback استفاده می‌کنیم. به علاوه اشیاء کامپیوتر برای لپ‌تاپ‌های بخش فروش در OU های مختلف پخش شده‌اند و باید از فیلتر امنیتی برای اعمال GPO به یک گروه به جای یک OU مربوط به لپ‌تاپ‌های بخش فروش استفاده کنیم.

۱. ابزار Active Directory Users And Computers را باز کرده و یک گروه امنیتی global با نام Sales Laptops در Groups OU می‌سازیم. همچنین یک OU با نام Clients برای اشیاء کامپیوتر می‌سازیم.

۲. در GPMC روی Group Policy Objects container کلیک راست کرده و New را انتخاب می‌کنیم.

۳. در کادر Name عبارت Sales Laptop Configuration را تایپ کرده و OK می‌کنیم.

۴. روی GPO کلیک راست کرده و Edit را انتخاب می‌کنیم.

۵. گره User Configuration\Policies\Administrative Templates\Desktop\Desktop را باز می‌کنیم.

۶. روی تنظیم Desktop Wallpaper دوبار کیک می‌کنیم.

۷. روی زبانه Explain کلیک کرده و متن توضیحی را مرور می‌کنیم.

۸. روی زبانه Comment کلیک کرده و تایپ می‌کنیم Corporate standard wallpaper for sales laptops

۹. زبانه Settings را کلیک می‌کنیم.

۱۰. Enabled را انتخاب می‌کنیم.

۱۱. در کادر Wallpaper Name عبارت c:\windows\web\Wallpaper\server.jpg را تایپ می‌کنیم.

۱۲. OK را کلیک می‌کنیم.

۱۳. گره Computer Configuration\Policies\Administrative Templates\System\Group Policy را باز می‌کنیم.

۱۴. روی تنظیم User Group Policy Loopback Processing Mode دوبار کلیک می‌کنیم.

۱۵. روی Enabled کلیک کرده و در لیست بازشوی Mode گزینه Merge را انتخاب می‌کنیم.

۱۶. OK کرده و GPME را می‌بندیم.

۱۷. در GPMC ، Sales Configuration GPO را در Group Policy Objects container انتخاب می‌کنیم.

۱۸. در زبانه Scope در بخش Security Filtering گروه Authenticated Users را انتخاب می‌کنیم و دکمه Remove را کلیک می‌کنیم. OK را برای تایید کلیک می‌کنیم.

۱۹. دکمه Add را در بخش Security Filtering کلیک می‌کنیم.

۲۰. نام گروه را Sales Laptops تایپ کرده و OK می‌کنیم.

۲۱. روی Clients OU کلیک راست کرده و Link An Existing GPO را انتخاب می‌کنیم.

۲۲. Sales Laptop Configuration را انتخاب کرده و روی OK کلیک می‌کنیم.

ما حالا یک GPO را طوری فیلتر کردیم که فقط روی اشیاء در گروه Sales Laptops اعمال شود. ما می‌توانیم اشیاء کامپیوتر لپ‌تاپ‌های بخش فروش را به گروه اضافه کنیم که باعث می‌شود این لپ‌تاپ‌ها در حوزه GPO قرار گیرند. GPO لپ‌تاپ‌ها را طوری پیکربندی می‌کند که پردازش policy را در حالت Merge اجرا کند. وقتی کاربری به یکی از لپ‌تاپ‌ها وارد می‌شود تنظیمات پیکربندی کاربر که کاربر در آن حوزه قرار دارد اعمال می‌شود و سپس تنظیمات پیکربندی کاربر در GPO هایی که کامپیوتر در آن حوزه قرار می‌گیرند اعمال می‌شوند که یکی از آنها Sales Laptop Configuration GPO می‌باشد.

خلاصه درس

- حوزه اولیه GPO توسط لینک‌های GPO تعیین می‌شود. یک GPO می‌تواند به یک یا چند سایت، دامنه یا OU لینک شود. حوزه GPO می‌تواند توسط فیلترهای امنیتی یا فیلترهای WMI اصلاح شود.
- CSE ها GPO ها را به ترتیب زیر اعمال می‌کنند: GPOهای محلی، GPO های لینک شده به سایت، GPO های لینک شده به دامنه و GPOهای لینک شده به OU .
- وراثت policy با پیکربندی گزینه Block Inheritance در دامنه یا OU غیرفعال می‌شود.
- لینک GPO می‌تواند در حالت Enforced قرار گیرد. تنظیمات در یک enforced GPO به کامپیوترها و کاربران در حوزه GPO اعمال می‌شود حتی اگر گزینه Block Inheritance انتخاب شده باشد. به علاوه تنظیمات در یک enforced GPO در اولویت قرار می‌گیرد بنابراین بر تنظیمات مشابه غلبه می‌کند.
- از فیلتر امنیتی برای تعیین گروهی که یک GPO به آن اعمال می‌شود یا گروههایی که باید از اعمال GPO مستثنی شوند استفاده می‌شود. فقط گروههای امنیتی global برای فیلتر کردن GPO استفاده می‌شود.
- در پردازش عادی policy در زمان به روز رسانی policy کاربر (هنگام ورود به ویندوز و بعد از آن هر ۹۰ تا ۱۲۰ دقیقه) سیستم تنظیمات کاربر را از GPO هایی که کاربر در حوزه آن قرار دارد بروی کامپیوتر اعمال می‌کند.
- پردازش policy به حالت loopback باعث می‌شود سیستم در اعمال GPO ها تغییر رویه دهد. در حالت Merge بعد از اعمال تنظیمات از GPO که کاربر در آن حوزه قرار دارد سیستم تنظیمات policy را از GPO که کامپیوتر در حوزه آن قرار دارد اعمال می‌کند. این تنظیمات بر تنظیماتی که از GPO کاربر قرار دارد غلبه می‌کند. در حالت Replace تنظیمات کاربر از GPO که کاربر در حوزه آن قرار دارد اعمال نمی‌شود. به جای آن فقط تنظیمات از GPO که کامپیوتر در حوزه آن قرار دارد اعمال می‌شود.

سئوالات پایان درس

۱. می‌خواهیم یک GPO با نام Northwind Lockdown را که پیکربندی همه کاربران شرکت Northwind Traders را اعمال می‌کند توزیع کنیم. و تنظیمات نباید به اعضاء گروه Domain Admins اعمال شود. چطور این کار را انجام می‌دهیم؟ (در صورت صحیح بودن می‌توانید همه گزینه‌ها را انتخاب کنید)

A. Northwind Lockdown GPO را به دامنه لینک می‌کنیم و روی دامنه کلیک راست کرده و Block Inheritance را انتخاب می‌کنیم.

B. Northwind Lockdown GPO را به دامنه لینک می‌کنیم و روی OU که شامل همه کاربران گروه Domain Admins است کلیک راست کرده و Block Inheritance را انتخاب می‌کنیم.

C. Northwind Lockdown GPO را به دامنه لینک می‌کنیم و مجوز Apply Group Policy را برای گروه Domain Admins ، deny می‌کنیم.

D. Northwind Lockdown GPO را به دامنه لینک می‌کنیم و فیلتر امنیتی را طوری پیکربندی می‌کنیم که GPO به Domain Users اعمال شود.

۲. می‌خواهیم کاربران هنگام ورود به سیستم در اتاق‌های کنفرانس و آموزش صفحه خاصی را روی دسک‌تاپ ببینند و امکان تغییر آنرا نداشته باشند. یک GPO با نام Public Computers Configuration با تنظیم مورد نظر در گره User Configuration می‌سازیم. چه کار دیگری باید انجام دهیم؟ (در صورت صحیح بودن می‌توانید همه گزینه‌ها را انتخاب کنید. هر جواب صحیح بخشی از کل جواب است)

A. تنظیم User Policy Loopback Processing Mode را فعال می‌کنیم.

B. GPO را به OU که دربرگیرنده حساب کاربری است لینک می‌کنیم.

C. گزینه Block Inheritance را روی OU که شامل کامپیوترهای اتاق کنفرانس و آموزش است انتخاب می‌کنیم.

D. GPO را به OU دربرگیرنده کامپیوترهای اتاق کنفرانس و آموزش لینک می‌کنیم.

درس ۳ : پشتیبانی از Group Policy

تحلیل و درک برنامه Group Policy می‌تواند بسیار پیچیده باشد در حالی که تنظیمات متعدد در GPO های متعدد با روش‌های متعدد داشته باشیم. ما باید ابزارهایی داشته باشیم که بتوانیم با آنها پیاده‌سازی Group Policy را ارزیابی و عیب‌یابی کنیم قبل از این که مشکل بروز کند. مایکروسافت در ویندوز دو ابزار را که برای پشتیبانی از Group Policy واجب هستند ارائه کرده است یکی Resultant Set of Policy (RSoP) و دیگری Group Policy Operational Logs می‌باشد. در این درس استفاده از این ابزارها را در سناریوهای پشتیبانی و رفع عیب به حالت‌های proactive و reactive یاد می‌گیریم.

بعد از این درس یاد می‌گیریم:

- مجموعه GPO ها و تنظیمات policy را که به یک کاربر یا کامپیوتر اعمال می‌شود تحلیل کنیم
- تاثیر تغییرات Group Policy یا Active Directory را در RSOP پیش‌بینی کنیم.
- گزارش وقایع را شامل وقایع مربوط به Group Policy پیدا کنیم.

زمان تقریبی : ۳۰ دقیقه

برایند مجموعه تنظیمات

در درس ۲ یاد گرفتیم که یک کاربر یا کامپیوتر می‌تواند در حوزه چند GPO قرار گیرد. وراثت Group Policy، فیلترها و استثنائات بسیار پیچیده هستند و اغلب پیش بینی تنظیمات نهایی که اعمال خواهد شد مشکل است. RSoP برایند نهایی GPO های اعمال شده به یک کاربر یا کامپیوتر، با احتساب لینک‌های GPO ، استثنائاتی نظیر Enforced و Block Inheritance و فیلترهای WMI می‌باشد. RSoP همچنین مجموعه‌ای از ابزارهایی است که ما را در ارزیابی مدل‌سازی و رفع عیب تنظیمات Group Policy کمک می‌کند. RSoP می‌تواند به یک کامپیوتر محلی یا راه دور پرس و جو ارسال کند و در جواب تنظیمات دقیقی را که به کامپیوتر یا هر کاربری که به کامپیوتر وارد شده اعمال شده گزارش کند. RSoP همچنین می‌تواند تنظیمات policy را که پیش بینی می‌شود تحت شرایطی اعمال شود مدل سازی می‌کند. نمونه آن انتقال شیء بین OU ها یا سایت‌ها یا تغییر عضویت گروه اشیاء می‌باشد. با این قابلیت‌ها RSoP به ما امکان می‌دهد تداخل تنظیمات را بهتر مدیریت کرده و رفع عیب کنیم.

ویندوز سرور 2008 ابزارهای زیر را برای اجرای تحلیل RSoP فراهم می‌کند:

- Group Policy Results Wizard
- Group Policy Modeling Wizard

- Gpresult.exe

گرفتن گزارش‌های RSoP با Group Policy Result Wizard

برای کمک به تحلیل تاثیرات نهایی GPO ها و تنظیمات policy روی یک کاربر یا کامپیوتر در سازمان کنسول GPMC ویزارد Group Policy Result را ارائه داده است. اگر بخواهیم دقیقا بدانیم کدام تنظیمات و چرا اعمال شده این ابزار به ما می‌گوید. این ویزارد قادر است روی کامپیوتر محلی یا راه دور دارای ویندوز ویستا، ویندوز XP ، سرور 2003 و سرور 2008 به WMI provider دسترسی پیدا کند.

WMI provider می‌تواند هر چیزی را درباره روش اعمال Group Policy به سیستم گزارش کند. از زمان پردازش اطلاع دارد و می‌داند کدام GPO اعمال شده ، کدام GPO اعمال نشده و چرا . خطاهای پدید آمده ، تنظیمات دقیقی که در اولویت قرار گرفته و GPO منشا آنها را نیز می‌داند.

برای اجرای این ویزارد نیازمندی‌های متعددی وجود دارد:

- باید روی کامپیوتر مقصد اعتبار مدیریتی داشته باشیم.
- سیستم عامل کامپیوتر مقصد باید ویندوز XP یا جدیدتر باشد. این ویزارد به ویندوز 2000 دسترسی ندارد.
- ما باید به WMI کامپیوتر مقصد دسترسی داشته باشیم. این بدین معنی است که باید روشن باشد به شبکه دسترسی داشته باشد و از طریق پورت ۱۳۵ , ۴۴۵ در دسترس باشد.

  نکته مدیریت از راه دور کامپیوتر کلاینت را فعال کنید

  اجرای RSoP توسط ویزارد مذکور یکی از نمونه‌های مدیریت از راه دور می‌باشد. ویندوز XP با سرویس پک ۲، ویندوز ویستا و ویندوز سرور 2008 دارای فایروالی است که از ارتباطات ورودی ناخواسته حتی اگر از طرف اعضای گروه Administrators باشد جلوگیری می‌کند. Group Policy روش ساده‌ای را برای فعال کردن مدیریت از راه دور فراهم می‌کند. در پوشه Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile تنظیمی را با نام Windows Firewall: Allow Inbound Remote Administration Exception پیدا می‌کنیم. وقتی این تنظیم را فعال می‌کنیم می‌توانیم آدرس‌های IP یا شبکه‌های مجاز برای برقراری ارتباط را هم مشخص کنیم. همانند همه تنظیمات policy متن توضیحی آن را در زبانه Explain مرور کرده و تاثیر این policy را قبل از توزیع در آزمایشگاه بررسی می‌کنیم.
- سرویس WMI باید روی کامپیوتر مقصد استارت شود.
- اگر بخواهیم RSoP را برای یک کاربر تحلیل کنیم آن کاربر باید حداقل یک بار به سیستم وارد شده باشد. هنگام تهیه گزارش نیازی نیست که کاربر مربوطه به سیستم وارد شده باشد.

بعد از تامین این نیازمندی‌ها می‌توانیم تحلیل RSoP را شروع کنیم. روی Group Policy Results در GPMC کلیک راست کرده و Group Policy Results Wizard را انتخاب می‌کنیم. ویزارد از ما می‌خواهد کامپیوتر مقصد رامشخص کنیم. بعد به WMI provider همان کامپیوتر متصل شده و لیستی از کاربرانی را که به سیستم وارد شده‌اند جمع‌آوری می‌کند. بعد می‌توانیم یکی از کاربران را انتخاب کنیم یا از برنامه خارج شویم.

ویزارد یک گزارش RSoP با جزئیات را در قالب HTML فراهم می‌کند. هر بخش از گزارش با کلیک روی لینک Hide یا Show یا اینکه با دوبار کلیک روی تیتر بخش باز و بسته می‌شود. این گزارش دارای سه زبانه می‌باشد:

- **Summary** وضعیت پردازش Group Policy را در آخرین به روز رسانی نمایش می‌دهد. در این زبانه می‌توانیم

اطلاعاتی را که درباره سیستم جمع‌آوری شده ، GPO هایی که اعمال و یا رد شده، عضویت گروهی که ممکن است تحت تاثیر فیلتر شدن GPO توسط گروههای امنیتی قرار گرفته باشد، فیلترهای WMI و وضعیت CSE ها ببینیم.

- **Settings** در این زبانه برایند مجموعه تنظیمات policy که به کاربر یا کامپیوتر اعمال شده است نمایش داده می‌شود. این زبانه دقیقا به ما نشان می‌دهد پیاده‌سازی Group Policy چه تاثیری روی کاربر داشته است. حجم عظیمی از اطلاعات در این زبانه قابل دریافت است. برخی گزارش‌ها نیز وجود ندارد مانند تنظیمات IPSec، wireless و سهمیه‌بندی دیسک

- **Policy Events** وقایع Group Policy را از کامپیوتر مقصد نمایش می‌دهد.

پس از ساخت گزارش RSoP با ویزارد می‌توانیم روی آن کلیک راست کرده و پرس و جو را دوباره اجرا کنیم، آنرا چاپ کنیم یا به عنوان یک فایل XML یا HTML ذخیره کنیم .چون این نوع فایل‌ها توسط Internet Explorer اجرا می‌شود پس گزارش RSoP را می‌توان به خارج از GPMC منتقل کرد. اگر زیر پوشه Group Policy Result در ساختار درختی روی گره گزارش کلیک راست کنیم می‌توانیم به حالت Advanced View سوئیچ کنیم. در این حالت RSoP توسط ابزار RSoP (snap-in) نمایش داده می‌شود که تمام تنظیمات اعمال شده را شامل policy های IPSec ، wireless و سهمیه بندی دیسک آشکار می‌کند.

تهیه گزارش RSoP با استفاده از Gpresult.exe

این دستور نسخه خط فرمان ویزارد Group Policy Result می‌باشد. این دستور به همان WMI provider که ویزارد دسترسی دارد دسترسی داشته و همان اطلاعات را ارائه می‌کند. در حقیقت به ما امکان تهیه همان گزارش‌های گرافیکی را می‌دهد. Gpresult روی ویندوزهای ویستا، XP، سرور 2003 و 2008 اجرا می‌شود. در ویندوز 2000 این دستور گزارشی محدود از پردازش Group Policy آماده می‌کند و دستور آن نسبت به نسخه‌های جدیدتر خیلی ساده‌تر است.

وقتی این دستور را اجرا می‌کنیم می‌توانیم از گزینه‌های زیر استفاده کنیم:

- /s computername نام یا آدرس IP کامپیوتر مقصد را مشخص می‌کند. اگر از نقطه به جای نام کامپیوتر استفاده شود یا اصلا از این گزینه استفاده نشود دستور روی کامپیوتر محلی اجرا می‌شود.

- /scope [user | computer] گزارش را برای کاربر یا کامپیوتر نمایش می‌دهد. اگر این گزینه حذف شود گزارش هم تنظیمات کاربر و هم تنظیمات کامپیوتر را شامل می‌شود.

- /user username نام کاربری را که داده RSoP برای او نمایش داده می‌شود مشخص می‌کند.

- /r خلاصه‌ای از داده RSoP را نشان می‌دهد.

- /v داده کامل RSoP را نمایش می‌دهد که دارای اطلاعات معنی‌دارتری است.

- /z داده کامل را با جزئیات درباره همه تنظیمات اعمال شده به سیستم نمایش می‌دهد. اغلب این اطلاعات بیش از میزان مورد نیاز ما می‌باشد.

- /u domain\user /p password اعتباری را که در گروه Administrators سیستم راه دور است فراهم می‌کند. بدون این اعتبار دستور Gpresult با استفاده از اعتبار موجود که به سیستم وارد شده‌ایم اجرا می‌شود.

- /x | /h] filename] گزارش را در فرمت‌های به ترتیب XML یا HTML ذخیره می‌کند. این گزینه‌ها در ویندوز ویستا سرویس پک ۱ و سرور 2008 قابل استفاده می‌باشند.

رفع مشکل Group Policy با ویزارد Group Policy Result و Gpresult.exe

به عنوان یک مدیر شبکه ما احتمالا با سناریوهایی که نیاز به رفع عیب از Group Policy دارند مواجه می‌شویم. برخی مشکلات در زیر آمده است:

- GPO ها اصلا اعمال نمی‌شوند.
- برایند مجموعه policy ها برای یک کاربر یا کامپیوتر مطابق انتظار ما نمی‌باشد.

Group Policy Results Wizard و Gpresult.exe اغلب باارزشترین اطلاعات را از پردازش Group Policy م مشکلات مربوطه می‌دهند. به خاطر داشته باشید که این ابزارها از WMI RSoP provider برای گزارش دقیق ماوقع روی سیستم استفاده می‌کند. بررسی گزارش RSoP اغلب ما را به سوی GPO هایی که حوزه آنها اشتباه تعیین شده یا خطاهای پردازش policy که از اعمال تنظیمات GPO جلوگیری کرده هدایت می‌کند.

اجرای تحلیل What-If با Group Policy Modeling Wizard

اگر یک کامپیوتر یا کاربر از یک سایت یا OU به سایت یا OU دیگر منتقل شود یا گروهش تغییر یابد در یک حوزه GPO دیگر قرار خواهد گرفت و بنابراین RSoP برای کامپیوتر یا کاربر متفاوت خواهد بود. RSoP همچنین تغییر خواهد کرد اگر سرعت لینک پایین بیاید یا پردازش loopback اتفاق بیافتد یا اگر خصوصیاتی از سیستم که مقصد فیلتر WMI است تغییر کند. قبل از اعمال چنین تغییراتی باید تاثیرات بالقوه آنرا بر RSoP کاربر یا کامپیوتر ارزیابی کنیم. Group Policy Results Wizard تحلیل RSoP را بر اساس آنچه که واقعا اتفاق افتاده اجرا می‌کند. به منظور پیش بینی آینده و اجرای تحلیل what-if می‌توانیم از Group Policy Modeling Wizard استفاده کنیم.

روی گره Group Policy Modeling در GPMC کلیک راست می‌کنیم. بعد Group Policy Modeling Wizard را انتخاب کرده و مراحل ویزارد را ادامه می‌دهیم. مدل کردن Group Policy توسط شبیه‌ساز روی DC اجرا می‌شود بنابراین ما باید دامنه‌ای را که سیستم عامل ویندوز سرور 2003 به بعد دارد مشخص کنیم. نیازی نیست که به سرور DC وارد شویم ولی درخواست مدل روی DC اجرا خواهد شد. سپس باید تنظیمات شبیه‌سازی را تعیین کنیم:

- یک شیء کاربر یا کامپیوتر و یا سایت، OU یا دامنه را برای ارزیابی انتخاب می‌کنیم.
- مشخص می‌کنیم پردازش باید با یک لینک با سرعت کم شبیه‌سازی شود یا نه.
- مشخص می‌کنیم پردازش به حالت loopback انجام شود یا نه و اگر این‌طور باشد یکی از حالت‌های Replace یا Merge را انتخاب می‌کنیم
- سایتی را برای شبیه‌سازی انتخاب می‌کنیم
- گروه‌هایی را برای کاربر و کامپیوتر انتخاب می‌کنیم
- مشخص می‌کنیم کدام فیلتر WMI در شبیه‌سازی پردازش policy کامپیوتر و کاربر اعمال گردد.

وقتی تنظیمات شبیه‌سازی مشخص شد گزارشی شبیه به گزارش Group Policy Results تولید می‌کند. زبانه Summary کلیاتی را از GPO هایی که پردازش می‌شوند نشان می‌دهد و زبانه Settings جزئیات تنظیمات policy را که به کاربر یا کامپیوتر اعمال می‌شود نمایش می‌دهد. این گزارش با کلیک راست روی آن و انتخاب Save Report ذخیره می‌شود.

بررسی گزارشات وقایع مربوط به Policy

ویندوز ویستا و سرور 2008 توانایی ما را در رفع عیب Group Policy با ثبت وقایع Group Policy بالا می‌برد. در System log می‌توانیم اطلاعات کلی مانند خطاهای ثبت شده توسط کلاینت Group Policy را که به دلیل عدم ارتباط با DC و پیدا کردن

GPO ها بروز کرده پیدا کنیم. Application log وقایعی را نشان میدهد که توسط CSE ها ثبت شده‌اند. یک log جدید به نام Goup Policy Operational Log اطلاعات جزئی را درباره پردازش Group Policy مهیا می‌کند. این گزارشات را در ابزار Event Viewer می‌توانیم پیدا کنیم. گزارش وقایع System و Application در گره Windows Logs موجود است. Group Policy Operational Log نیز در Applications And Services Logs\Microsoft\Windows\Group Policy\Operational یافت می‌شود. این گزارش زمانی در دسترس قرار می‌گیرد که از ویزارد Group Policy Modeling استفاده کنیم.

تمرینات پیکربندی حوزه Group Policy

در این تمرین سناریویی را دنبال می‌کنیم که روی GPO هایی ساخته می‌شود که در درس ۱ و ۲ ایجاد و پیکربندی شده است. ما نتایج RSoP و تحلیل از طریق مدل‌سازی را اجرا می‌کنیم و وقایع مرتبط به policy را در event logs بررسی می‌کنیم. برای اجرای این تمرینات باید تمرینات دروس ۱ و ۲ را انجام داده باشیم.

تمرین ۱ استفاده از ویزارد Group Policy Results

در این تمرین از ویزارد Group Policy Results برای بررسی RSoP روی سرور SERVER01 استفاده می‌کنیم. باید مطمئن شویم که policy های ساخته شده در دروس ۱ و ۲ اعمال شده‌اند.

۱. با اعتبار Administrator به SERVER01 وارد می‌شویم.

۲. پنجره خط فرمان را باز کرده و تایپ می‌کنیم gpupdate.exe /force /boot تا Group Policy به روز شود. منتظر می‌مانیم تا سیستم راه اندازی مجدد شود. زمان سیستم را یادداشت می‌کنیم که در تمرین ۳ به آن نیاز پیدا می‌کنیم.

۳. با ااعتبار Administrator به SERVER01 وارد شده و کنسول Group Policy Management را باز می‌کنیم.

۴. گره Forest را باز می‌کنیم.

۵. روی Group Policy Results کلیک راست کرده و Group Policy Result Wizard را انتخاب می‌کنیم.

۶. دکمه Next را کلیک می‌کنیم.

۷. در صفحه Computer Selection گزینه This Computer را انتخاب و Next می‌کنیم.

۸. در صفحه User Selection به ترتیب Display Policy Settings For، Select A Specific User و CONTOSO\Administrator را انتخاب می‌کنیم.

۹. در صفحه Summary Of Selection تنظیمات را مرور کرده و Next را می‌زنیم.

۱۰. Finish را کلیک می‌کنیم.

گزارش RSoP در پنل وسط کنسول ظاهر می‌شود.

۱۱. در زبانه Summary در بالای گزارش روی Show All Link کلیک می‌کنیم.

۱۲. نتایج Group Policy Summary را مرور می‌کنیم. برای تنظیمات کاربر و کامپیوتر زمان آخرین اعمال policy ها و لیست GPO های اعمال شده و رد شده را می‌بینیم. اجزائی که برای پردازش تنظیمات policy استفاده شده را می‌توانیم پیدا کنیم.

۱۳. زبانه Settings و بعد در بالای صفحه Show all link را کلیک می‌کنیم. تنظیماتی را که اعمال شده مرور می‌کنیم و GPO را که تنظیمات از آن بدست آمده پیدا می‌کنیم.

۱۴. زبانه Policy Events را کلیک کرده و گزارشی که واقعه به روز رسانی policy را در اثر اجرای دستور Gpupdate در مرحله ۲ تمرین نشان می‌دهد پیدا می‌کنیم.

۱۵. روی زبانه Summary کلیک می‌کنیم روی صفحه کلیک راست می‌کنیم و Save Report را انتخاب می‌کنیم. گزارش را با فرمت HTML در پوشه Documents با نام دلخواه ذخیره می‌کنیم.

۱۶. گزارش ذخیره شده RSoP را از پوشه Documents باز می‌کنیم.

تمرین ۲ استفاده از دستور Gpresult.exe

در این تمرین قرار است تحلیل RSoP را از خط فرمان با استفاده از دستور Gpresult.exe اجرا کنیم.

۱. پنجره خط فرمان را باز می‌کنیم.

۲. دستور Gpresult /r را تایپ کرده و Enter را می‌زنیم.

نتایج خلاصه RSoP نمایش داده می‌شود. اطلاعات خیلی شبیه به اطلاعات زبانه Summary گزارش RSoP فراهم شده توسط Group Policy Results Wizard می‌باشد.

۳. دستور gpresult /v را تایپ کرده و کلید Enter را می‌زنیم.

گزارشی با جزئیات بیشتر درباره RSoP تولید می‌شود. به بسیاری از تنظیمات Group Policy اعمال شده توسط کلاینت در این گزارش توجه کنید.

۴. دستور gpresult /z را وارد کرده و کلید Enter را می‌زنیم.

گزارش دقیق‌تری از RSoP ساخته می‌شود.

۵. دستور "gpresult /h::%username%\Documents\RSOP.html" را وارد کرده و کلید Enter را می‌زنیم. یک گزارش RSoP به عنوان یک فایل HTML در پوشه Documents ما ذخیره می‌شود.

۶. این فایل را از پوشه Documents باز می‌کنیم. گزارش، اطلاعات و قالب آن را با گزارش RSoP که در تمرین قبل ذخیره کردیم مقایسه می‌کنیم.

تمرین ۳ مشاهده وقایع مرتبط با Policy

هنگامی که کلاینت به روز رسانی policy را انجام می‌دهد اجزاء Group Policy مواردی را در event log ویندوز ثبت می‌کند. در این تمرین ما وقایع مربوط به Group Policy را پیدا و بررسی می‌کنیم.

۱. کنسول Event Viewer را از پوشه Administrative Tools باز می‌کنیم.

۲. گره Windows Logs\System را باز می‌کنیم

۳. وقایع مربوط به Group Policy را پیدا می‌کنیم. حتی می‌توانیم روی لینک Filter Current Log در پنل سمت راست کلیک کرده و در لیست بازشوی Event Sources گزینه Group Policy را انتخاب کنیم.

۴. اطلاعات مرتبط با وقایع Group Policy را مرور می‌کنیم.

۵. روی گره Application در ساختار درختی زیر Windows Logs کلیک می‌کنیم.

۶. گزارشات Application را بر اساس ستون Source مرتب می‌کنیم.

۷. گزارشات را مرور می‌کنیم و وقایع مرتبط با Group Policy را پیدا می‌کنیم.

کدام وقایع به برنامه Group Policy ارتباط دارد و کدام به فعالیت‌های ما برای مدیریت Group Policy مرتبط است؟

۸. در ساختار درختی کنسول گره Application And Services Logs\Microsoft\Windows\Group Policy\Operational را باز می‌کنیم.

۹. اولین واقعه مرتبط با به روز رسانی Group Policy را که در تمرین ۱ با دستور Gpupdate.exe اتفاق افتاده پیدا می‌کنیم. این واقعه و وقایع بعدی را مرور می‌کنیم.

تمرین ۴ در این تمرین قرار است مدل‌سازی Group Policy را به منظور ارزیابی تاثیرات بالقوه تنظیمات policy روی کاربرانی که به لپ‌تاپ‌های بخش فروش وارد می‌شوند انجام دهیم.

۱. ابزار Active Directory Users And Computers را باز می‌کنیم.

۲. یک حساب کاربری برای Mike Danseglio در People OU می‌سازیم.

۳. یک OU با نام Clients در دامنه می‌سازیم.

۴. یک حساب کامپیوتر در Clients OU با نام LAPTOP101 می‌سازیم.

۵. LAPTOP101 و گروه Domain Users را به گروه Sales Laptops اضافه می‌کنیم.

یک تجربه مستند می‌گوید که وقتی پردازش loopback با فیلترینگ گروه امنیتی ترکیب می‌شود برنامه تنظیمات کاربر حین به روز رسانی policy از اعتبار کامپیوتر برای تعیین GPO که به عنوان بخشی از پردازش loopback اعمال می‌شود استفاده می‌کند ولی کاربر وارد شده باید مجوز Apply Group Policy را هم داشته باشد.

۶. در کنسول Group Policy Management گره Forest را باز می‌کنیم.

۷. روی Group Policy Modeling کلیک راست کرده و Group Plicy Modeling Wizard را اجرا می‌کنیم.

۸. روی Next کلیک می‌کنیم.

۹. در صفحه Domain Controller Selection دکمه Next را می‌زنیم.

۱۰. در صفحه User And Computer Selection در بخش User Information روی دکمه User بعد Browse کلیک کرده و Mike Danseglio را انتخاب می‌کنیم.

۱۱. در بخش Computer Information روی دکمه Computer کلیک کرده و Browse را کلیک می‌کنیم و بعد LAPTOP101 را به عنوان کامپیوتر انتخاب می‌کنیم.

۱۲. دکمه Next را کلیک می‌کنیم.

۱۳. در صفحه Advanced Simulation Options کادر Loopback Processing را علامت زده و merge را انتخاب می‌کنیم.

اگرچه Sales Laptop Configuration GPO پردازش loopback را تعیین می‌کند باید برای ویزارد Group Policy Modeling آنرا مشخص کنیم تا در شبیه‌سازی آنرا در نظر بگیرد.

۱۴. دکمه Next را کلیک می‌کنیم.

۱۵. در صفحه Alternate Active Ditectory Paths روی دکمه Next کلیک می‌کنیم.

۱۶. در صفحه User Security Groups روی دکمه Next کلیک می‌کنیم.

۱۷. در صفحه Computer Security Groups روی دکمه Next کلیک می‌کنیم.

۱۸. در صفحه WMI Filters For Users روی دکمه Next کلیک می‌کنیم.

۱۹. در صفحه WMI Filters For Computers روی دکمه Next کلیک می‌کنیم.

۲۰. تنظیمات خود را در صفحه Summary Of Selection مرور می‌کنیم. روی Next کلیک کرده و Finish را می‌زنیم.

خلاصه درس

گزارشات RSoP می‌تواند در رابط کاربری ویندوز توسط Group Policy Results Wizard تولید شود. این گزارشات نتایج واقعی پردازش نهایی سیاست را نشان می‌دهد.

گزارشات RSoP از طریق خط فرمان نیز با دستور Gpresult.rxr تولید می‌شود. گزینه /scope به منظور تولید گزارش اختصاصی تنظیمات کاربر یا کامپیوتر به کار می‌رود. سوئیچ /s برای اجرای Gpresult.exe برای سیستم راه دور کاربرد دارد.

سئوالات پایان درس

۱. کاربری با بخش پشتیبانی شبکه تماس می‌گیرد و گزارش می‌دهد که مشکلی پیش آمده و ما به تنظیماتی که اخیرا روی Group Policy انجام داده‌ایم شک می‌کنیم. می‌خواهیم اطلاعات مربوط به پردازش Group Policy را روی سیستم او بررسی کنیم. کدام از ابزارها به ما در جمع آوری اطلاعات به صورت راه دود کمک می‌کند؟ (امکان انتخاب بیش از یک جواب وجود دارد.)
   a. Group Policy Modeling Wizard
   b. Group Policy Results Wizard
   c. Gpupdate.exe
   d. Gpresult.exe
   e. Msconfig.exe

۲. فرض کنید مدیر شبکه شرکت Contoso هستیم. دامنه دارای پنج GPO لینک شده به دامنه است. یکی از آنها مربوط به تنظیماتscreen saver می‌باشد. برخی کاربران گزارش می‌دهند screen saver پس از ۱۰ دقیقه اجرا نمی‌شود. از کجا متوجه می‌شویم که GPO اعمال شده است؟
   a. دستور Gpresult.exe را برای کاربران اجرا می‌کنیم.

b. دستور Gpresult.exe –computer را اجرا می‌کنیم.
c. دستور Gpresult –scope computer را اجرا می‌کنیم.
d. دستور Gpresult.exe /Target:User را اجرا می‌کنیم.

فصل ۷

تنظیمات Group Policy

Group Policy برای مدیریت پیکربندی انواع مختلف اجزاء و ویژگی‌های ویندوز استفاده می‌شود. در فصل قبل یاد گرفتیم زیرساخت یک Group Policy را پیکربندی کنیم. در این فصل یاد می‌گیریم زیرساخت را با هدف مدیریت انواع پیکربندی مرتبط با امنیت و نصب نرم‌افزار اعمال کنیم. همچنین با ابزارهایی نظیر Security Configuration Wizard آشنا می‌شویم که کمک می‌کند ساده‌تر تشخیص دهیم کدام تنظیمات بر اساس نقش سرور باید پیکربندی شود. در نهایت یاد می‌گیریم ممیزی فایل‌ها و پوشه‌ها و تغییرات AD DS را پیکربندی کنیم.

اهداف امتحانی در این فصل:

- ساخت و نگهداری اشیاء Active Directory
  - ساخت و اعمال اشیاء Group Policy (GPOs)
  - پیکربندی الگوهای GPO
  - پیکربندی policy ممیزی با استفاده از GPO ها

دروس این فصل:

- درس ۱: تفویض اختیار پشتیبانی کامپیوترها
- درس ۲: مدیریت تنظیمات امنیتی
- درس ۳: مدیریت نرم‌افزار توسط Group Policy Software Installation
- درس ۴: ممیزی

قبل از شروع

برای اجرای تمرینات این فصل باید یک DC با نام SERVER01 در دامنه contoso.com ساخته باشیم. برای اجرای این مراحل به فصل ۱ مراجعه کنید.

دنیای واقعی

دن هلم

تعجب می‌کنم بعد از ۸ سال از معرفی Group Policy بسیاری از سازمان‌ها هنوز از همه قابلیت‌های آن مخصوصا در زمینه امنیت استفاده نمی‌کنند. سه درس از چهار درس این فصل روی تعامل بین پیکربندی امنیتی و Group Policy تمرکز می‌کند.

پیکربندی‌هایی نظیر عضویت گروه Administrators و انتساب حقوق کاربری (user rights) ، حالت‌های startup سرویس‌ها و policy های ممیزی می‌تواند با Group Policy مدیریت شود. چیزی که در این فصل یاد می‌گیریم فقط برای قبولی در امتحان 70-640 کاربرد ندارد. این دانش به ما کمک می‌کند امنیت و مدیریت‌پذیری را در شبکه ارتقاء دهیم. این قابلیت شامل خود Active Directory نیز می‌شود. در تمام هشت سال گذشته دائما این سئوال را از من پرسیدند "چطور می‌توان فهمید چه تغییراتی توسط مدیران شبکه در Active Directory ایجاد شده است". حالا به لطف ممیزی جدید Directory Service Changes در ویندوز سرور 2008 می‌توانیم گزارش امنیتی را چک کنیم. حتی اگر از قبل policy برای مدیریت پیکربندی امنیتی سازمان دارید این ویژگی جدید به همراه ویزارد Security Configuration توسعه یافته قطعا قابلیت‌های مدیریت امنیت را به سطح بالاتری ارتقاء می‌دهد.

درس ۱: تفویض اختیار پشتیبانی کامپیوترها

بسیاری از سازمان‌ها وظیفه پشتیبانی از کامپیوترها را به دوش یک یا چند نفر از پرسنل می‌گذارند که به این گروه اسامی help desk، desktop support و یا support اطلاق می‌گردد (ما به این گروه تیم پشتیبانی می‌گوییم). اغلب از اعضاء تیم پشتیانی خواسته می‌شود وظایفی از قبیل عیب‌یابی، پیکربندی یا دیگر وظایف را روی کلاینت‌ها انجام دهند و این وظایف معمولا نیاز به دسترسی مدیریتی دارند. بنابراین اعتبار اعضاء این تیم باید در سطح گروه Administrators کامپیوترهای کلاینت باشد و نیازی نیست عضو گروه Domain Admins باشند بنابراین توصیه می‌شود آنها را به این گروه اضافه نکنیم. در عوض سیستم‌های کلاینت را طوری پیکربندی می‌کنیم که گروه پشتیبانی به گروه Administrators محلی کلاینت‌ها اضافه شود. Policy های گروههای محدود شده به ما اجازه این کار را می‌دهد که در این درس نحوه استفاده از آن برای افزودن اعضاء تیم پشتیبانی به گروه Administrators آموزش داده می‌شود. بعد از آن وظیفه پشتیبانی از کلاینت‌ها را به این تیم محول می‌کنیم. چنین رویکردی برای تفویض مدیریت هر حوزه‌ای از کامپیوترها به تیم مسئول همان کامپیوترها قابل استفاده است.

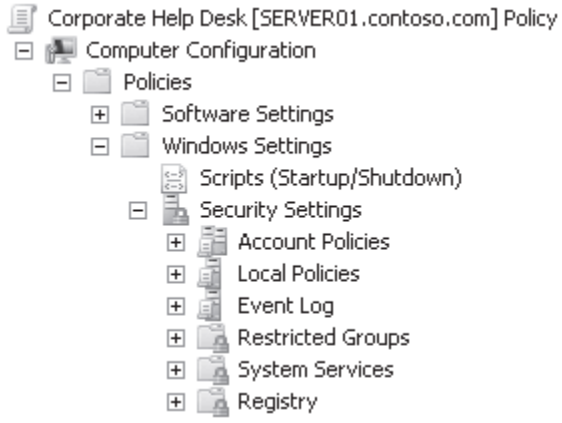
بعد از این درس یاد می‌گیریم:

- وظیفه مدیریت کامپیوترها را محول کنیم
- از Group Policy برای تغییر یا اجبار کردن عضویت گروهها استفاده کنیم.

زمان تقریبی: ۳۰ دقیقه

Policy های گروههای محدود شده

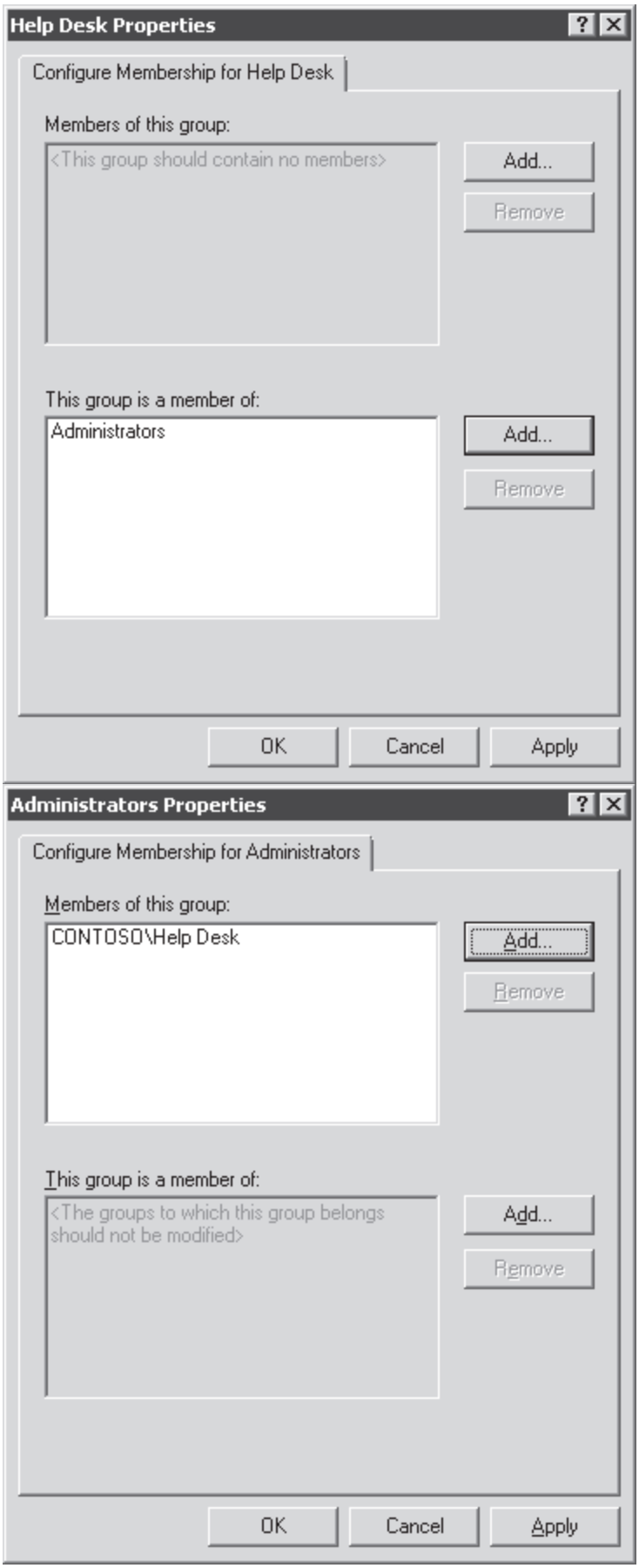
وقتی یک GPO را ویرایش می‌کنیم و گره Computer Configuration ، گره Policies ، گره Windows Settings و گره Security Settings را باز می‌کنیم همانطوری که در شکل ۱- ۷ نشان داده شده گره Restricted Groups پیدا می‌شود



شکل ۱- ۷ گره Restricted Groups از یک شیء Group Policy

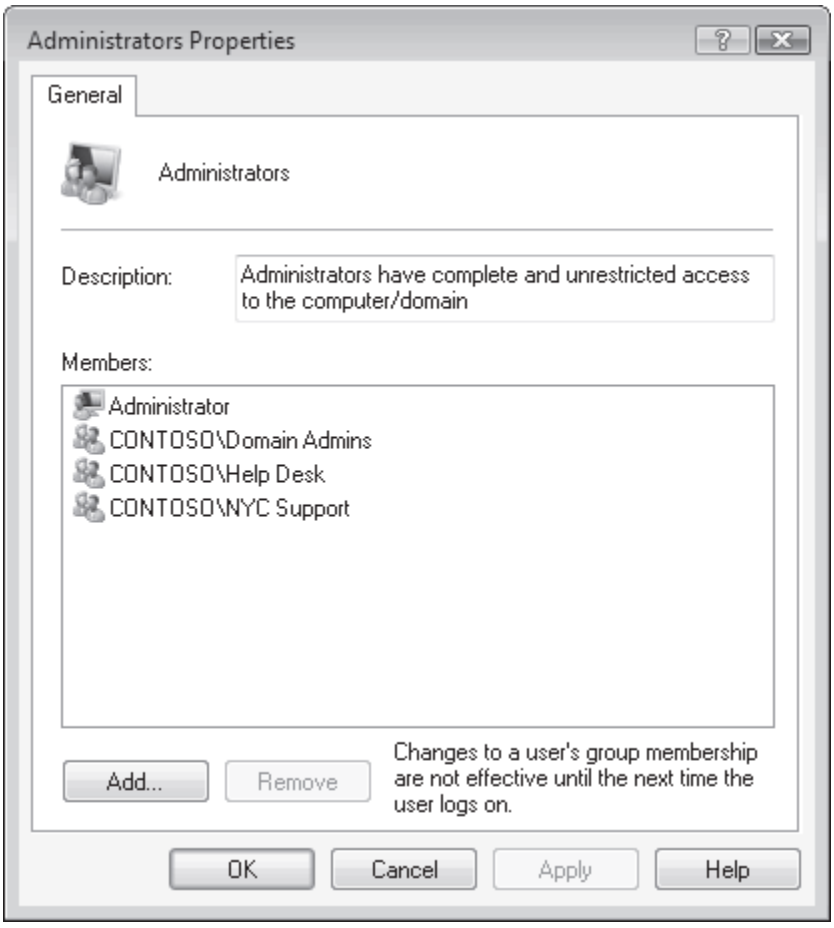
تنظیمات این policy امکان مدیریت اعضاء گروهها را فراهم می‌کند. در اینجا دو نوع تنظیم وجود دارد : This Group Is A Member Of (تنظیم Member Of) و Member Of This Group (تنظیم Members) . شکل ۲- ۷ مثال‌هایی را

نشان می‌دهد.



شکل ۲- ۷ policy های گروههای محدود شده Member Of و Members

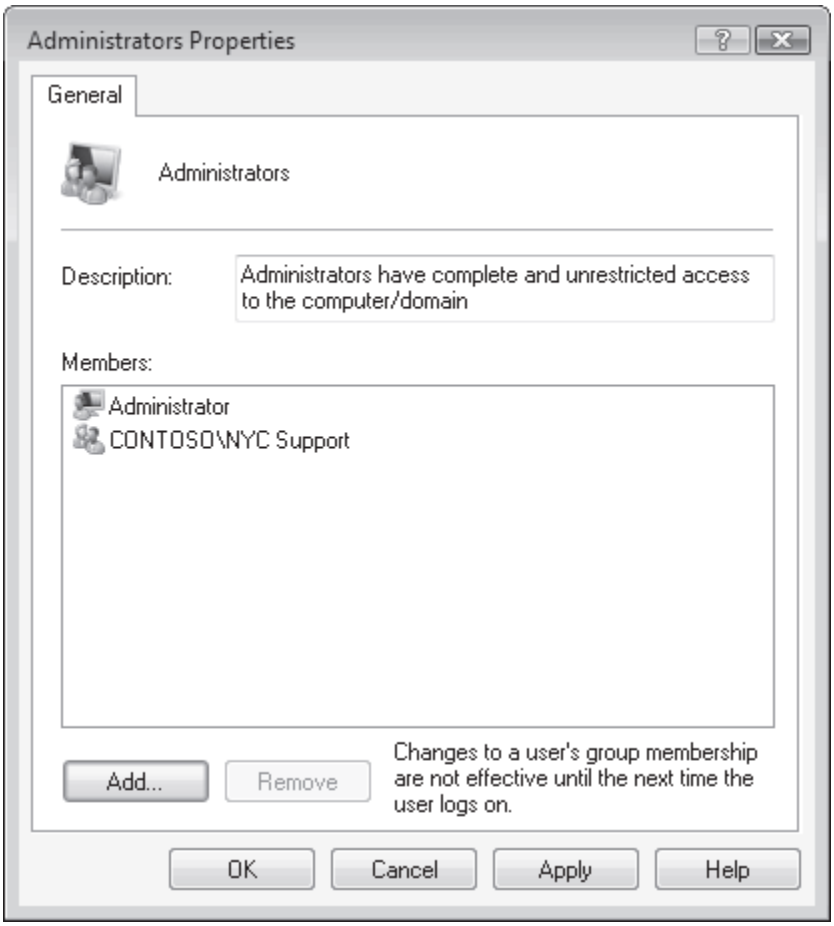
درک تفاوت بین این دو تنظیم اهمیت دارد. تنظیم A Member Of مشخص می‌کند که گروه تعیین شده در این بخش عضو گروه دیگری است. در سمت چپ شکل ۲- ۷ نمونه‌ای از آن را می‌بینیم: گروه CONTOSO\Help Desk عضو گروه Administrators است. وقتی کامپیوتری این تنظیم را اعمال می‌کند گروه Help Desk را از دامنه عضو گروه Administrators کامپیوتر خود می‌کند. اگر بیش از یک GPO با policy های گروههای محدود شده موجود باشد همه policy های Member Of اعمال می‌شود. برای مثال وقتی یک GPO لینک شده به Clients OU مشخص می‌کند که گروه CONTOSO\Help Desk عضوی از گروه Administrators است و GPO دوم لینک شده به NYC OU (یک OU فرعی از Clients OU) مشخص می‌کند که گروه CONTOSO\NYC Support نیز عضوی از گروه Administrators می‌باشد نتیجه این می‌شود که کامپیوترها در NYC OU هر دو گروه Help Desk و NYC Support را به گروه Administrators خود اضافه می‌کنند. به علاوه اینکه به طور پیش فرض گروه Domain Admins به گروه Administrators همه کامپیوترهای عضو دامنه اضافه می‌شود. این مثال در شکل ۳- ۷ شرح داده شده است. همانطوریکه می‌بینید policy های گروههای محدود شده که از تنظیم Member Of استفاده می‌کنند به صورت تجمعی عمل می‌کنند.



شکل ۳- ۷ نتیجه policy های گروههای محدود شده با استفاده از تنظیم Member Of

نوع دوم policy گروههای محدود شده تنظیم Members است که مشخص کننده کل عضویت گروه تعیین شده در policy می‌باشد. سمت راست شکل ۲- ۷ مثالی از این موضوع را نشان می‌دهد. در لیست اعضاء گروه Administrators گروه CONTOSO\Help Desk اضافه شده است. وقتی کامپیوتری این تنظیم را اعمال می‌کند تنها عضو گروه Administrators آن سیستم گروه CONTOSO\Help Desk خواهد بود. هر عضوی که در این policy اضافه نشود از گروه حذف می‌شود حتی Domain Admins . تنظیم Members یک تنظیم حکم کننده (authoritative) است یعنی لیست نهایی اعضاء همین‌جا مشخص می‌شود. اگر بیش از یک GPO با policy های گروه محدود شده موجود باشد GPO با بالاترین اولویت غلبه می‌کند. برای مثال وقتی یک GPO لینک شده به Clients OU عضویت گروه Administrators را به صورت CONTOSO\Help Desk مشخص می‌کند و GPO دیگری که به NYC OU لینک شده عضویت گروه Administrators را به صورت

CONTOSO\NYC Support تعیین کرده کامپیوترهای NYC OU فقط گروه NYC را در عضویت Administrators سیستم خواهند داشت. این مثال در شکل ۴- ۷ شرح داده شده است.



شکل ۴- ۷ policy های گروههای محدود شده با استفاده از تنظیمات Members

در شبکه سازمان خود مراقب تنظیمات گروههای محدود شده باشید که نتیجه مطلوب حاصل شود. این دو policy را با هم ترکیب نکنید و فقط از یکی از آنها استفاده کنید.

نکته امتحانی برای امتحان 70-640 باید بدانید که تنظیم Member Of تجمعی است ولی در تنظیم Members آن GPO که اولویت بالاتری دارد اعمال می‌شود.

تفویض مدیریت با استفاده از تنظیم Member Of از policy های گروههای محدود شده

یکی از راه‌های تفویض اختیار مدیریتی نسبت به کامپیوترها به صورت زیر است:

۱. در GPME گره Computer Configuration\Policies\Windows Settings\Security Settings\Restricted Groups را انتخاب می‌کنیم.

۲. روی Restricted Groups کلیک راست کرده و Add Groups را انتخاب می‌کنیم.

۳. دکمه Browse را کلیک کرده و در کادر محاوره‌ای Select Groups نام گروهی که می‌خواهیم که به گروه Administrators اضافه کنیم مثلا CONTOSO\Help Desk تایپ می‌کنیم و دکمه OK را کلیک می‌کنیم.

۴. دکمه OK را کلیک می‌کنیم تا کادر بسته شود. کادر محاوره‌ای Properties ظاهر می‌شود.

۵. دکمه Add نزدیک به بخش This Group Is A Member Of را کلیک می‌کنیم.

۶. تایپ می‌کنیم Administrators و دکمه OK را کلیک می‌کنیم. تنظیم Properties باید چیزی شبیه به سمت چپ شکل ۲- ۷ شود.

۷. دوباره OK را کلیک می‌کنیم تا کادر بسته شود.

تفویض اختیار عضویت گروه Administrators محلی به این شکل گروه مشخص شده در مرحله ۳ را به آن گروه اضافه می‌کند ولی هیچ عضوی را از این گروه حذف نمی‌کند. Group policy به سادگی به کلاینت‌ها می‌گوید این گروه را به گروه Administrators محلی خود اضافه کنند.

برای در اختیار گرفتن کنترل کامل گروه Administrators مراحل زیر را دنبال می‌کنیم:

۱. در GPMC به مسیر Computer Configuration\Windows Settings\Security Settings\Restricted Groups می‌رویم.

۲. روی Restricted Groups کلیک راست کرده و Add Groups را انتخاب می‌کنیم.

۳. Administrators را تایپ کرده و OK را کلیک می‌کنیم. کادر محاوره‌ای Properties ظاهر می‌شود.

۴. روی دکمه Add کنار بخش Members Of This Group کلیک می‌کنیم.

۵. روی دکمه Browse کلیک کرده و نام گروهی که می‌خواهیم تنها عضو گروه Administrators شود مثلا CONTOSO\Help Desk را تایپ می‌کنیم. بعد دکمه OK را کلیک می‌کنیم.

۶. دوباره OK را کلیک کرده تا کادر Add Member بسته شود. تنظیم Properties باید چیزی شبیه به سمت راست شکل ۲- ۷ شود.

۷. دوباره دکمه OK را کلیک می‌کنیم تا کادر Properties بسته شود.

وقتی تنظیم Members را از policy گروههای محدود شده استفاده می‌کنیم لیست Members عضویت قطعی گروهرا مشخص می‌کند. وقتی کامپیوتری این GPO را اعمال می‌کند همه اعضای گروه را که در لیست نیامده حذف کرده و اعضای جدید را از لیست به گروه اضافه می‌کند. فقط کاربر Administrator محلی از گروه Administratirs حذف نمی‌شود چون این کاربر عضو ثابت و غیرقابل حذف گروه Administrators است.

تمرینات تفویض اختیار عضویت با استفاده از Group Policy

در این تمرین ابتدا یک GPO با تنظیم policy گروههای محدود شده می‌سازیم که گروه Help Desk را به گروه Administrators همه کلاینت‌ها اضافه کند. سپس GPO دیگری می‌سازیم که گروه NYC Support را به گروه Administrators محلی همه کلاینت‌های NYC OU اضافه کند. بعد مشاهده می‌کنیم که هر دو گروه به گروه Administrators اضافه شده‌اند.

برای اجرای این تمرین نیاز به اشیاء زیر در دامنه contoso.com داریم:

- OU سطح اول با نام Admins با یک OU فرعی با نام Admin Groups
- یک گروه امنیتی global با نام Help Desk در Admins\Admin Groups OU
- یک گروه امنیتی global با نام NYC Support در Admins\Admin Groups

- یک OU سطح اول با نام Clients
- یک ou با نام NYC در Clients OU
- یک شیء کامپیوتر با نام DESKTOP101 در nyc ou

تمرین ۱ تفویض اختیار مدیریت همه کلاینت‌ها در دامنه

در این تمرین یک GPO با تنظیم policy گروههای محدود شده ساخته می‌شود که گروه Help Desk را به گروه Administrators همه کلاینت‌ها اضافه می‌کند.

۱. در کنسول GPMC گره Forest\Domains\contoso.com را باز می‌کنیم و Group Policy Objects container را انتخاب می‌کنیم.

۲. روی Group Policy Objects container کلیک راست کرده و New را انتخاب می‌کنیم.

۳. در کادر Name تایپ می‌کنیم Corporate Help Desk و دکمه OK را کلیک می‌کنیم.

۴. روی GPO کلیک راست کرده و Edit را انتخاب می‌کنیم.

۵. در GPME گره Computer Configuration\Policies\Windows Settings\Security Settings\Restricted Groups را انتخاب می‌کنیم.

۶. روی Restricted Groups کلیک راست کرده و Add Group را انتخاب می‌کنیم.

۷. دکمه Browse را کلیک کرده و در کادر Select Groups تایپ می‌کنیم CONTOSO\Help Desk و بعد دکمه OK را کلیک می‌کنیم.

۸. دکمه OK را کلیک می‌کنیم تا کادر بسته شود.

۹. روی دکمه Add کنار بخش This Group Is A Member Of کلیک می‌کنیم.

۱۰. تایپ می‌کنیم Administrators و بعد دکمه OK را کلیک می‌کنیم. تنظیم Properties باید چیزی شبیه به سمت چپ شکل ۲- ۷ شود.

۱۱. دوباره OK را کلیک کرده تا کادر بسته شود.

۱۲. پنجره GPMC را می‌بندیم.

۱۳. در کنسول GPMC روی Clients OU کلیک راست کرده و Link An Existing GPO را انتخاب می‌کنیم.

۱۴. Corporate Help Desk GPO را انتخاب کرده و دکمه OK را کلیک می‌کنیم.

تمرین ۲ در این تمرین ما یک GPO با یک تنظیم policy گروههای محدود شده می‌سازیم که گروه NYC Support را به گروه Administrators همه کلاینت‌های NYC OU اضافه می‌کند.

۱. در کنسول GPMC گره Forest\Domains\Contoso.com را باز می‌کنیم. Group Policy Objects

container را انتخاب می‌کنیم.

۲. روی Group Policy Objects container کلیک راست کرده و New را انتخاب می‌کنیم.

۳. در کادر Name تایپ می‌کنیم New York Support و دکمه OK را کلیک می‌کنیم.

۴. روی GPO کلیک راست کرده و Edit را انتخاب می‌کنیم.

۵. مراحل ۵-۱۲ تمرین ۱ را تکرار می‌کنیم فقط در مرحله ۷ نام گروه را CONTOSO\NYC Support وارد می‌کنیم.

۶. در کنسول GPMC روی Clients\NYC OU کلیک راست کرده و Link An Existing GPO را انتخاب می‌کنیم.

۷. New York Support GPO را انتخاب کرده و دکمه OK را کلیک می‌کنیم.

تمرین ۳ تایید تجمعی بودن Member Of Policy

اگر بخواهیم گزارشی از تنظیمات نهایی اعمال شده به یک کامپیوتر یا کاربر داشته باشیم Group Policy Modeling روش مناسبی خواهد بود. در این تمرین از این روش برای تایید اضافه شدن گروههای Help Desk و NYC Support به گروه Administrators کامپیوترهای NYC OU بهره می‌بریم.

۱. در کنسول GPMC گره Forest را باز می‌کنیم و گره Group Policy Modeling را انتخاب می‌کنیم.

۲. روی Group Policy Modeling کلیک راست کرده و Group Policy Modeling Wizard را انتخاب می‌کنیم.

۳. دکمه Next را کلیک می‌کنیم.

۴. در صفحه Domain Controller Selection روی دکمه Next کلیک می‌کنیم.

۵. در صفحه User And Computer Selection در بخش Computer Information روی دکمه Browse کلیک می‌کنیم.

۶. گره دامنه و Clients OU را باز کرده و سپس NYC OU را انتخاب می‌کنیم.

۷. روی دکمه OK کلیک می‌کنیم.

۸. کادر Skip To The Final Page Of This Wizard Without Collecting Additional Data را علامت می‌زنیم.

۹. روی دکمه Next کلیک می‌کنیم.

۱۰. در صفحه Summary Of Selections روی دکمه Next کلیک می‌کنیم.

۱۱. روی دکمه Finish کلیک می‌کنیم. گزارش Group Policy Modeling ظاهر می‌شود.

۱۲. زبانه Settings را کلیک می‌کنیم.

۱۳. روی Security Settings دوبار کلیک می‌کنیم.

۱۴. روی Restricted Groups دوبار کلیک می‌کنیم.

حالا می‌توانیم لیست گروههای Help Desk و NYC Support را ببینیم. Policy های گروههای محدود شده با استفاده از تنظیم This Group Is A Member Of به حالت تجمعی است. توجه داشته باشید که گزارش مشخص نمی‌کند که گروههای لیست شده به گروه Administrators تعلق دارد. این محدودیت ضعف این گزارش است.

تمرین ۴ (اختیاری) تایید عضویت گروه Administrators

اگر محیط تست ما کامپیوتری به نام DESKTOP101 داشته باشد که عضو دامنه contoso.com است می‌توانیم اعضاء گروه Administrators را بررسی کنیم. در این لیست باید اعضاء زیر موجود باشند:

- CONTOSO\Help desk که توسط Corporate Help Desk GPO اعمال شده است.
- CONTOSO\NYC Support که توسط New York Support GPO اعمال شده است.
- Domain Admins که هنگام join شده کامپیوتر به دامنه افزوده شده است.
- کاربر Administrator محلی که عضو پیش فرض است و قابل حذف نیست.

خلاصه درس

- برای تفویض اختیار پشتیبانی کامپیوترها در دامنه باید عضویت گروههای Administrators سیستم‌ها را مدیریت می‌کنیم.
- GPO که از تنظیم Member Of از policy های گروههای محدود شده استفاده می‌کند می‌تواند گروههای دامنه را به گروه Administrators محلی اضافه کند. تنظیمات Member Of تجمعی است بنابراین GPO ها می‌توانند گروههای خود را به گروه Administrators اضافه کنند.
- GPO که از تنظیم Members گروههای محدود شده استفاده می‌کند می‌تواند عضویت گروه Administrators را تعریف کند. تنظیم Members نهایی و حکم کننده است. اگر بیش از یک GPO به یک کامپیوتر اعمال شود فقط GPO با بالاترین اولویت عضویت گروه Administrators را مشخص می‌کند.

سئوالات پایان درس

۱. دامنه contoso.com دارای یک GPO با نام Corporate Help Desk می‌باشد که به Clients OU لینک شده است و یک GPO با نام Sydney Support که به Sydney OU لینک شده است و هر دو OU زیرمجموعه Clients OU می‌باشند. Corporate Help Desk GPO دارای یک policy گروههای محدود شده برای گروه CONTOSO\Help Desk است که This Group Is A Member Of Administrators را تعریف می‌کند. Sydney Support GPO هم دارای یک policy گروههای محدود شده برای گروه CONTOSO\Sydney Support است که This Group Is A Member Of Administrators را تعریف می‌کند. کامپیوتری با نام DESKTOP234 به دامنه join شده و در Sydney OU قرار می‌گیرد. کدام یک از جواب‌های زیر عضو گروه Administrators روی DESKTOP234 است ؟(در صورت صحیح بودن همه جواب‌ها را انتخاب کنید)

A. Administrator

B. Domain Admins

C. Sydney Support

D. Help Desk

E. Remote Desktop Users

۲. دامنه contoso.com دارای یک GPO با نام Corporate Help Desk می‌باشد که به Clients OU لینک شده است و یک GPO با نام Sydney Support که به Sydney OU لینک شده است و هر دو OU زیرمجموعه Clients OU می‌باشند. Corporate Help Desk GPO دارای یک policy گروههای محدود شده برای گروه Administrators است که تنظیم Members Of This Group را با CONTOSO\Help Desk تعریف می‌کند. Sydney Support GPO هم دارای یک policy گروههای محدود شده برای گروه Administrators است که تنظیم Members Of This Group را با CONTOSO\Sydney Support تعریف می‌کند. کامپیوتری با نام DESKTOP234 به دامنه join شده و در Sydney OU قرار می‌گیرد. کدام یک از جواب‌های زیر عضو گروه Administrators روی DESKTOP234 است ؟(در صورت صحیح بودن همه جواب‌ها را انتخاب کنید)

A. Administrator

B. Domain Admins

C. Sydney Support

D. Help Desk

E. Remote Desktop Users

۳. دامنه contoso.com دارای یک GPO با نام Corporate Help Desk می‌باشد که به Clients OU لینک شده است و یک GPO با نام Sydney Support که به Sydney OU لینک شده است و هر دو OU زیرمجموعه Clients OU می‌باشند. Corporate Help Desk GPO دارای یک policy گروههای محدود شده برای گروه Administrators است که تنظیم Members Of This Group را با CONTOSO\Help Desk تعریف می‌کند. Sydney Support GPO هم دارای یک policy گروههای محدود شده برای گروه CONTOSO\Sydney Support است که This Group Is A Member Of Administrators را تعریف می‌کند. کامپیوتری با نام DESKTOP234 به دامنه join شده و در Sydney OU قرار می‌گیرد. کدام یک از جواب‌های زیر عضو گروه Administrators روی DESKTOP234 است ؟(در صورت صحیح بودن همه جواب‌ها را انتخاب کنید)

A. Administrator

B. Domain Admins

C. Sydney Support

D. Help Desk

درس ۲: مدیریت تنظیمات امنیتی

امنیت دغدغه اصلی مدیران شبکه است. ویندوز سرور 2008 دارای تنظیمات بیشماری است که روی سرویس‌های اجرا شده، پورت‌های باز، پکت‌های شبکه که به داخل یا خارج راه پیدا می‌کنند، حقوق و مجوزهای کاربران و فعالیت‌هایی که ممیزی می‌شود تاثیر می‌گذارد. این تنظیم‌ها قابل پیکربندی بوده و متاسفانه فرمول جاویی برای اعمال بهترین پیکربندی امنیتی به سرور وجود ندارد. مناسب‌ترین پیکربندی امنیتی برای سرور بستگی به نقش‌های آن سرور، ترکیب سیستم‌های عامل در شبکه و سیاست‌های امنیتی سازمان دارد که خود اینها تابع قوانین اجباری از بیرون سازمان می‌باشد.

بنابراین ما باید تنظیمات امنیتی که سرور نیازمند آن است تعریف و پیکربندی کنیم و البته این تنظیمات باید طوری آماده شوند که پیکربندی امنیت بهینه و متمرکز باشد. ویندوز سرور 2008 مکانیزم‌های متعددی را فراهم می‌کند که با آن تنظیمات امنیتی یک یا چند سیستم را پیکربندی کنیم. در این درس ما این مکانیزم‌ها و تعامل آنها را یاد می‌گیریم.

بعد از این درس ما می‌توانیم:

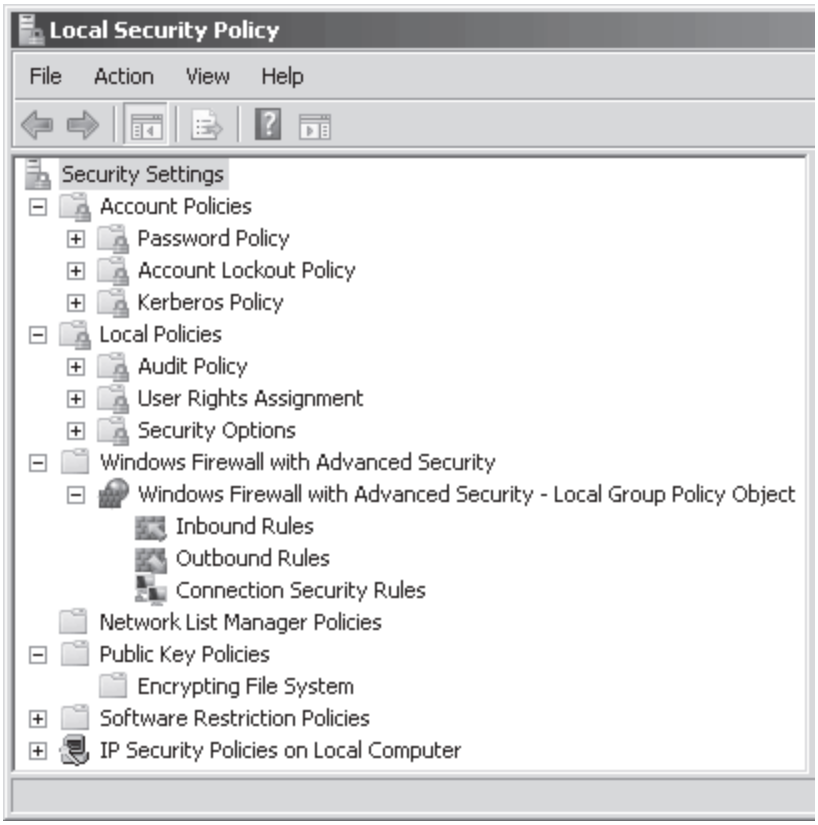
- تنظیمات امنیتی را روی یک کامپیوتر با استفاده از Local Security Policy پیکربندی کنیم.
- الگوهای امنیتی را به منظور پیکربندی امنیتی ساخته و اعمال کنیم
- پیکربندی امنیتی را براساس الگوهای امنیتی تحلیل کنیم
- Policy های امنیتی را با استفاده از Security Configuration Wizard بسازیم، ویرایش کنیم و اعمال کنیم.
- پیکربندی امنیتی را با Group Policy توزیع کنیم

زمان تقریبی: ۶۰ دقیقه

پیکربندی Local Security Policy

سیستم‌های عامل ویندوز 2008 دارای مجموعه‌ای از تنظیمات امنیتی می‌باشدکه با GPO محلی قابل مدیریت است. ما می‌توانیم GPO محلی را با استفاده از ابزار Group Policy Object Editor یا کنسول Local Security Policy پیکربندی کنیم. گروه‌بندی تنظیمات policy در شکل ۵- ۷ نمایش داده شده است.

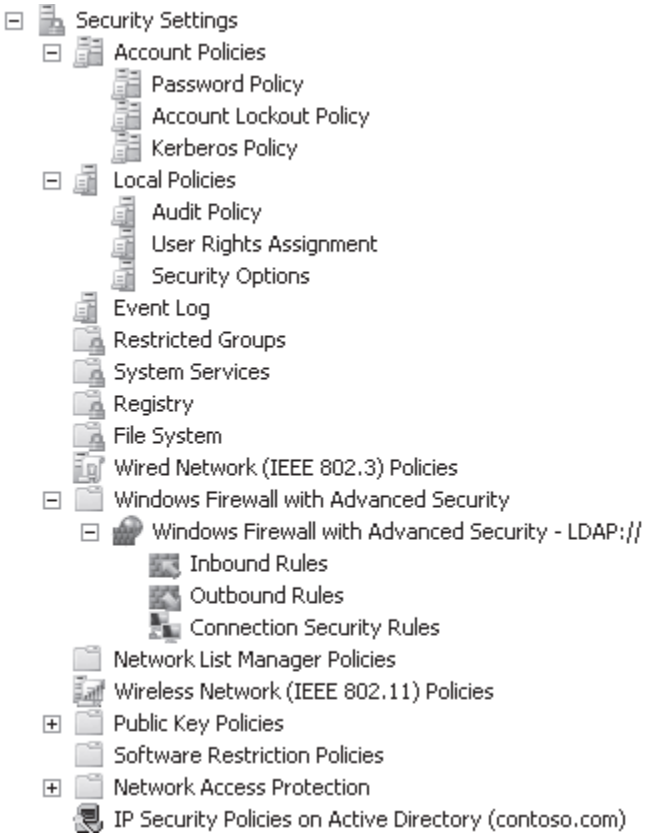
این درس به جای جزئیات خود تنظیمات روی مکانیزم‌هایی تمرکز می‌کند که با آن تنظیمات امنیتی را می‌توان مدیریت و پیکربندی کرد. بسیاری از تنظیمات نظیر account policies، audit policy و user rights assignment در جای دیگری از این کتاب بحث می‌شود.



شکل ۵- ۷ تنظیمات امنیتی موجود در GPO محلی

به دلیل اینکه DC ها حساب کاربری محلی ندارند (فقط حساب تحت دامنه دارند) policy های Account Policies container در GPO محلی روی DC ها قابل پیکربندی نیست. در عوض account policies مربوط به دامنه باید به عنوان بخشی از یک GPO لینک شده به دامنه نظیر Default Domain Policy GPO پیکربندی شود. Account policies در درس اول فصل ۸ بحث می‌شود.

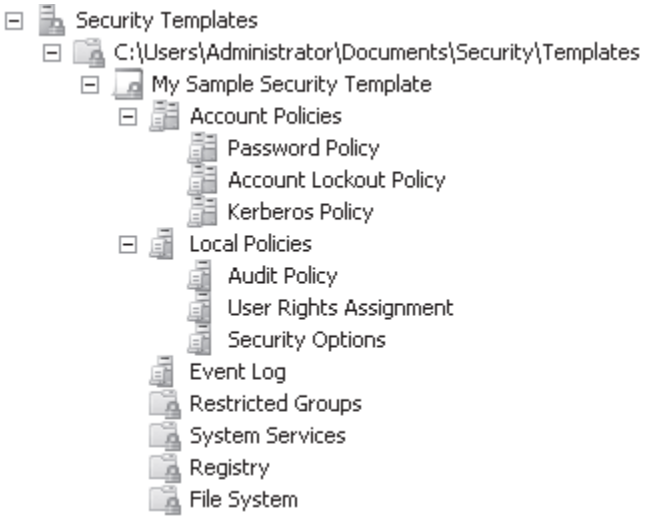
همانطور که در شکل ۶- ۷ نشان داده شده است تنظیمات local Security Settings policies مجموعه‌ای از تنظیمات است که با استفاده از Group Policy مبتنی بر دامنه پیکربندی می‌شود. همانطور که در فصل ۶ یاد گرفتیم بهترین روش مدیریت تنظیمات پیکربندی Group Policy مبتنی بر دامنه می‌باشد. Default Domain Controllers Policy GPO وقتی اولین DC برای دامنه جدید ایجاد شود ساخته می‌شود. این GPO به Domain Controllers OU لینک می‌شود و برای مدیریت تنظیمات امنیتی همه DC ها در دامنه استفاده می‌شود.



شکل ۶- ۷ تنظیمات امنیتی در یک GPO مبتنی بر دامنه

مدیریت پیکربندی امنیتی با الگوهای امنیتی

دومین مکانیزم مدیریت پیکربندی امنیتی الگوی امنیتی است. یک الگوی امنیتی مجموعه‌ای از تنظیمات است که به عنوان یک فایل متنی با پسوند .inf ذخیره می‌شود. همانطوریکه در شکل ۷- ۷ مشاهده می‌کنید یک الگوی امنیتی دارای تنظیماتی است که در GPO مبتنی بر دامنه وجود دارد و با GPO محلی کمی متفاوت است. ابزارهای مدیریت الگوهای امنیتی تنظیمات را در یک رابط کاربری ارائه می‌دهند که در آن امکان ذخیره پیکربندی را به عنوان فایل و توزیع آن فراهم است. همچنین از الگوی امنیتی برای تحلیل ک ک ک ک ک ک ک ک پیکربندی جاری کامپیوترها با پیکربندی مطلوب استفاده می‌شود.



شکل ۷- ۷ تنظیمات امنیتی در یک الگوی امنیتی

ذخیره پیکربندی امنیتی در الگوهای امنیتی مزایای متعددی دارد. برای مثال به دلیل اینکه الگوها به صورت فایل‌های متنی ساده است می‌توانیم مانند بقیه فایل‌های متنی آنها را ویرایش کنیم. به علاوه الگوها کار ذخیره پیکربندی‌های امنیتی انواع مختلف را طوری ساده می‌کنند که به آسانی می‌توان سطوح مختلف امنیتی را به کامپیوترهای با نقش‌های مختلف اعمال کرد.

الگوهای امنیتی ما را قادر می‌سازند هر کدام از انواع policy ها و تنظیمات را پیکربندی کنیم:

- Account Policies امکان تعریف محدودیت‌های کلمه عبور، account lockout policies و Kerberos policies را فراهم می‌کند.
- Local Policies ما را قادر می‌سازد audit policies، user rights assignments و security options policies را پیکربندی کنیم.
- Event Log Policies امکان پیکربندی حداکثر حجم فایل log و کککککک را فراهم می‌کند.
- Restricted Groups ما را قادر می‌سازد کاربرانی را که اجازه عضویت گروهها را دارند تعیین کنیم.
- System Services به ما امکان می‌دهد انواع startup و مجوزهای سرویس‌های سیستم را تعیین کنیم.
- Registry Permissions اعطاء مجوزهای کنترل دسترسی را نسبت به کلیدهای رجیستری خاصی امکانپذیر می‌کند.
- File System Permissions ما را قادر می‌سازد مجوزهای کنترل دسترسی به فایل‌ها و پوشه‌ها را تعیین کنیم.

توزیع الگوهای امنیتی از راههای مختلفی نظیر Active Directory Group Policy Objects، ابزار Security Configuration And Analysis یا Secedit.exe امکانپذیر است. وقتی یک الگوی امنیتی را به یک شیء Active Directory نسبت می‌دهیم تنظیمات الگو بخشی از GPO منتسب به شیء خواهد شد. نیز می‌توان یک الگوی امنیتی را مستقیما به یک کامپیوتر اعمال کرد که در این حالت تنظیمات الگو بخشی از policy های محلی کامپیوتر می‌شود. در این بخش این گزینه‌ها را یاد می‌گیریم.

استفاده از ابزار الگوهای امنیتی

برای کار با الگوهای امنیتی از ابزار Security Templates استفاده می‌کنیم. ویندوز سرور 2008 کنسولی برای کار با ابزار Security Templates ندارد بنابراین باید یا MMC آنرا بسازیم. این ابزار پوشه‌ای را به نام Security و پوشه فرعی به نام Templates در پوشه Documents ساخته و پوشه Documents\Security\Templates مسیر جستجوی الگو خواهد شد که می‌توانیم الگوها را اینجا ذخیره کنیم.

ساختن الگوی امنیتی جدید به این ترتیب است که روی گره‌ای که نمایانگر مسیر جستجوی الگوست (برای مثال C:\Users\Documents\Administrator\Security\Templates) کلیک راست کرده و New Template را انتخاب می‌کنیم. همچنین می‌توانیم الگویی بسازیم که منعکس کننده پیکربندی موجود سرور است که در بخش "ساخت الگوی امنیتی" روش آنرا یاد می‌گیریم.

تنظیمات در الگو به همان شکلی پیکربندی می‌شود که در GPO می‌شود. برای پیکربندی آن از ابزار Security Templates استفاده می‌شود. این ابزار فقط یک ویرایشگر است و هیچ نقشی در اعمال تنظیمات به سیستم ندارد. اگرچه الگو فقط یک فایل متنی است شکل آن می‌تواند گیج‌کننده باشد. استفاده از ابزار باعث می‌شود تنظیمات به شکل درستی تغییر یابد. استثنا در این قانون افزودن تنظیمات امنیتی است که قبلا در بخش Policies\Security Option از الگو لیست نشده است. هنگامی که تنظیمات امنیتی جدید شناخته می‌شوند اگر توسط یک کلید رجیستری قابل پیکربندی باشند می‌توانیم آنرا به یک الگوی امنیتی اضافه کنیم. برای این منظور آنرا به بخش Registry Values از الگو اضافه می‌کنیم.

اطلاعات بیشتر افزودن تنظیمات رجیستری سفارشی

مقاله "How to Add Custom Registry Settings to Security Configuration Editor" در آدرس http://support.microsoft.com/?kbid=214752 به ما در درک بهتر این کار کمک می‌کند

نکته تنظیمات را ذخیره کنید

با کلیک راست روی الگو و انتخاب Save از ذخیره تغییرات روی الگوی امنیتی مطمئن شوید

وقتی سروری را نصب می‌کنیم و به DC ارتقا می‌دهیم یک الگوی امنیتی توسط ویندوز اعمال می‌شود. این الگو را می‌توانیم در پوشه %SystemRoot%\Security\Templates پیدا کنیم. روی یک DC الگو DC security.inf نام دارد. این الگو به صورت مستقیم قابل ویرایش نیست و ابتدا باید آنرا به مسیر جستجوی الگو کپی کرده و ویرایش کنیم.

نکته الگوهای امنیتی در ویندوز سرور 2008 و نسخه‌های قبلی ویندوز

در نسخه‌های قبلی ویندوز تعدادی الگوی امنیتی برای تغییر و اعمال به یک کامپیوتر موجود بود که درویندوز سرور 2008 با وجود پیکربندی مبتنی بر نقش سرور و Security Cinfiguration Manager نیازی به آن احساس نمی‌شود.

توزیع الگوهای امنیتی با استفاده از اشیاء Group Policy

بدون اعمال کردن الگوهای امنیتی ساخت و ویرایش آنها به خودی خود امنیت را افزایش نمی‌دهد. برای پیکربندی تعدادی کامپیوتر در یک عملیات می‌توان یک الگوی امنیتی را به داخل GPO مربوط به یک دامنه، سایت یا OU منتقل کرد. برای این کار روی گره Security Settings کلیک راست کرده و Import Policy را انتخاب می‌کنیم. در کادر Import Policy From اگر کادر Clear This Database Before Importing را علامت بزنیم همه تنظیمات امنیتی در GPO قبل از انتقال تنظیمات الگو پاک می‌شود بنابراین تنظیمات امنیتی GPO با تنظیمات الگو همخوانی خواهد داشت. اگر این کادر را خالی بگذاریم تنظیمات امنیتی GPO باقی خواهد ماند و تنظیمات امنیتی منتقل خواهد شد. تنظیمات تعریف شده در GPO که در الگو نیز تعریف شده باشند با تنظیمات الگو پر خواهند شد.

پیکربندی امنیتی و ابزار تحلیل

از ابزار Security Configuration and Analysis به منظور اعمال الگوی امنیتی به یک کامپیوتر استفاده می‌شود. این ابزار همچنین توانایی تحلیل پیکربندی امنیتی جاری سیستم و مقایسه آن با یک الگوی امنیتی را فراهم می‌کند. این ویژگی به ما امکان می‌دهد به سرعت مشخص کنیم آیا کسی تنظیمات امنیتی یک کامپیوتر را تغییر داده است و آیا سیستم با سیاست‌های امنیتی سازمان همخوانی دارد یا نه.

این ابزار نیز در ویندوز سرور 2008 کنسول ندارد و باید ابزار را به کنسول MMC خود اضافه کنیم.

برای استفاده از این ابزار باید ابتدا یک بانک اطلاعاتی که مجموعه تنظیمات امنیتی را دربر گیرد بسازیم. بانک اطلاعاتی رابطی بین تنظیمات واقعی امنیتی روی کامپیوتر و تنظیمات ذخیره شده در الگوهای امنیتی می‌باشد. با کلیک راست روی گره Security Configuration And Analysis در ساختار درختی بانکی را ایجاد (یا بانک موجود را باز) می‌کنیم.

سپس می‌توانیم یک یا چند الگو را منتقل کنیم. اگر بیش از یک الگو را منتقل می‌کنیم باید در مورد پاک کرده بانک تصمیم بگیریم. اگر بانک پاک شود فقط تنظیمات الگوی جدید بخشی از بانک خواهد بود. اگر پاک نشود تنظیمات الگوی اضافی که تعریف می‌شود بر تنظیمات الگوهای قبلی منتقل شده غلبه می‌کند. اگر تنظیمات الگوهای منتقل شده جدید تعریف نشده باشد تنظیمات از الگوهای منتقل شده قبلی باقی می‌ماند.

نکته مهم تنظیمات بانک اطلاعاتی در مقابل تنظیمات کامپیوتر

به خاطر داشته باشید که تا زمانی که بانک اطلاعاتی برای پیکربندی کامپیوتر یا انتقال یک الگو استفاده نشده تنظیماتش تنظیمات کامپیوتر را تغییر نمی‌دهد.

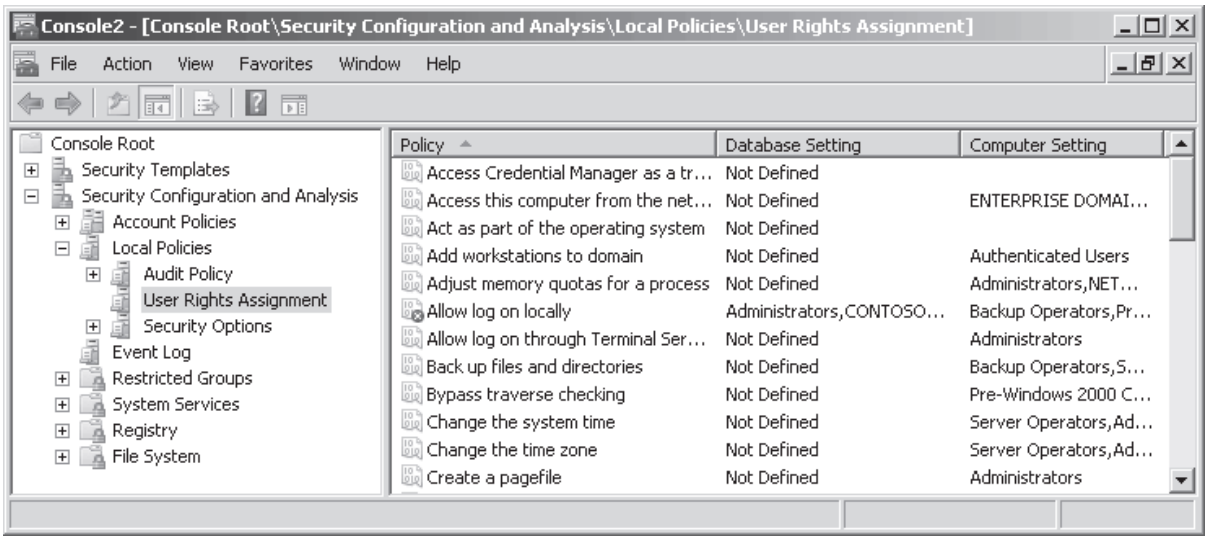
اعمال الگوهای امنیتی به یک کامپیوتر

پس از اینکه یک یا چند الگو را به منظور ساخت بانک اطلاعاتی منتقل کردیم می‌توانیم تنظیمات بانک را به کامپیوتر اعمال کنیم. برای این کار روی Security Cinfiguration And Analysis کلیک راست کرده و Cinfigure Computer Now را انتخاب می‌کنیم. پیغامی ظاهر می‌شود که مسیر فایل گزارش خطا را که درطول اجرای تنظیمات ایجاد می‌شود مشخص کنیم. پس از اعمال تنظیمات فایل گزارش خطا را مرور می‌کنیم.

تحلیل پیکربندی امنیتی یک کامپیوتر

قبل از اعمال تنظیمات امنیتی به یک کامپیوتر باید پیکربندی جاری کامپیوتر را برای تشخیص اختلافات احتمالی تحلیل کنیم. روی

Security Cinfiguration And Analysis کلیک راست کرده و Analyze Computer Now را انتخاب می‌کنیم. سیستم پیغام می‌دهد محل فایل گزارش خطا را مشخص کنیم و سپس به مقایسه تنظیمات جاری کامپیوتر و بانک اطلاعاتی ادامه می‌دهد. بعد از اتمام کار کنسول گزارشی مشابه شکل ۸- ۷ فراهم می‌کند.



شکل ۸- ۷ ابزار Security Cinfiguration and Analysis یک تحلیل پیکربندی کامپیوتر را نمایش می‌دهد.

برخلاف نمایش تنظیمات policy در ابزارهای GPME ، Group Policy Object Editor، Local Security Policy یا Security Templates گزارش برای هر policy تنظیم تعریف شده در بانک (که از الگوهایی بدست آمده که ما منتقل کردیم) و تنظیم جاری کامپیوتر را نمایش می‌دهد. دو تنظیم با هم مقایسه می‌شود و نتیجه مقایسه به عنوان یک پرچم در نام policy نشان داده می‌شود. برای مثال در شکل ۸- ۷ تنظیم Allow Log On Locally تفاوتی را بین تنظیم بانک و کامپیوتر نشان می‌دهد. معانی این پرچم‌ها به شرح زیر است:

- **حرف X در یک دایره قرمز** نشان می‌دهد که policy هم در بانک و هم در کامپیوتر تعریف شده ولی مقادیر آنها همخوانی ندارد.
- **علامت تیک سبز رنگ در یک دایره سفید** نشان می‌دهد policy در بانک و در کامپیوتر همخوانی دارند.
- **علامت سئوال در دایره سفید** نشان می‌دهد که policy در بانک تعریف نشده وبنابراین تحلیل نشده است و یا کاربر اجراکننده تحلیل مجوزهای لازم برای دسترسی به policy روی کامپیوتر ندارد
- **علامت تعجب در دایره سفید** نشان می‌دهد که policy در بانک تعریف شده ولی روی کامپیوتر وجود ندارد.
- **بدون پرچم** نشان می‌دهد که policy نه در بانک و نه در کامپیوتر تعریف نشده است.

تصحیح تفاوت‌های تنظیم امنیتی

همان‌طوری که عناصر بانک اطلاعاتی را بررسی می‌کنیم و آنرا با تنظیمات کامپیوتر مقایسه می‌کنیم ممکن است تفاوت‌هایی مشاده شود و بخواهیم یکی از طرفین را طوری تغییر دهیم که هر دو مشابه هم شوند. ما می‌توانیم روی هر policy دوبار کلیک کنیم تا کادر properties آن باز شود و مقدار آن را در بانک تغییر دهیم. پس از انجام تغییرات روی بانک می‌توان تنظیمات بانک را همان‌طور که در بخش قبلی شرح داده شد به کامپیوتر اعمال کنیم.

نکته اعمال یا انتقال تغییرات بانک اطلاعاتی

تغییر مقدار یک policy در ابزار Security Cinfiguration and Analysis فقط بانک را تغییر می‌دهد و نه تنظیمات واقعی کامپیوتر را. برای اعمال تغییرات روی کامپیوتر یا باید تنظیمات بانک را توسط دستور Configure Computer Now به کامپیوتر

اعمال کنیم یا بانک را با استفاده از دستور Secedit.exe (در بخش "Secedit.exe" بحث می‌شود) یا یک GPO به یک الگوی جدید منتقل کرده و آنرا به کامپیوتر اعمال کنیم.

به عنوان روش جایگزین ویرایش تنظیمات امنیتی کامپیوتر نیز به طور مستقیم با استفاده از کنسول Local Security Policy ، با تغییر GPO مناسب یا دستکاری فایل سیستم یا مجوزهای رجیستری امکان‌پذیر است. بعد انجام چنین تغییراتی به ابزار Security Configuration And Analysis مراجعت کرده و دستور Analyse Computer Now را انتخاب می‌کنیم تا مقایسه دوباره تنظیمات انجام شود.

ساخت یک الگوی امنیتی

با کلیک راست روی Security Configuration And Analysis و انتخاب Export Template می‌توان از بانک اطلاعاتی یک الگوی امنیتی جدید ساخت. در این صورت الگو تنظیمات بانک را دارا می‌شود که از یک یا چند الگوی امنیتی منتقل شده و ما آنرا به منظور انعکاس تنظیمات جاری کامپیوتر تحلیل شده تغییر داده‌ایم.

نکته مهم انتقال بانک به یک الگو

ویژگی Export Template باعث ساخت یک الگوی جدید از تنظیمات جاری بانک اطلاعاتی در زمان اجرای فرمان می‌شود نه از تنیظمات جاری کامپیوتر.

Secedit.exe

یک ابزار خط فرمان است که عملکردش شبیه ابزار Security Configuration And Analysis می‌باشد. مزیت این دستور در این است که می‌توان آنرا از اسکریپت‌ها و فایل‌های دسته‌ای فراخوانی کرد و توزیع الگوی امنیتی را خودکار کرد. مزیت بزرگ دیگر این دستور این است که از آن می‌توان برای اعمال فقط بخشی از الگو به کامپیوتر استفاده کرد کاری که با ابزار Security Configuration And Analysis یا GPO نمی‌توان انجام داد. برای مثال اگر بخواهیم مجوزهای سیستم فایل را از یک الگو اعمال کنیم و بقیه تنظیمات را اعمال نکنیم دستور Secedit.exe تنها راه حل است.

پارامترهای دستور به شرح زیر است:

- **Configure** همه یا بخشی از بانک اطلاعاتی را به کامپیوتر محلی اعمال می‌کند. همچنین می‌توانیم برنامه را طوری پیکربندی کنیم که قبل از اعمال تنظیمات بانک به کامپیوتر الگو را به بانک اطلاعاتی مشخق شده منتقل کند.
- **Analyze** تنظیمات امنیتی جاری کامپیوتر را با تنظیمات درون بانک اطلاعاتی مقایسه می‌کند. ما می‌توانیم برنامه را برای انتقال یک الگوی امنیتی به بانک اطلاعاتی قبل از اجرای عملیات تحلیل پیکربندی کنیم. برنامه نتایج تحلیل را در بانک مخصوصی ذخیره می‌کند که بعدا با استفاده از ابزار Security Configuration and Analysis قابل مشاهده است.
- **Import** بخشی یا همه الگوی امنیتی را به یک بانک اطلاعاتی امنیتی مشخصی منتقل می‌کند.
- **Export** همه یا بخشی از تنظیمات را از یک بانک اطلاعاتی امنیتی به یک الگوی امنیتی جدید منتقل می‌کند.
- **Validate** استفاده از شکل صحیح را توسط الگوی امنیتی بررسی می‌کند.
- **Generaterollback** الگوی امنیتی را می‌سازد که از آن برای بازیابی پیکربندی قبلی پس از اعمال الگوی جدید استفاده می‌شود.

برای مثال به منظور پیکربندی سیستمی توسط الگویی به نام BaselineSecurity از دستور زیر استفاده می‌کنیم:

```
Secedit /cinfigure /db BaselineSecurity.sdb /cfg BaseLineSecurity.inf /Log BaseLineSecurity.log
```

جهت ساخت الگوی بازیابی برای الگوی BaseLineSecurity از دستور زیر استفاده می‌شود:

```
Secedit /generaterollback /cfg BaselineSecurity.inf /rbk BaselineSecurityRollback.inf
/Log BaseLineSecurityRollback.log
```

اطلاعات بیشتر Secedit.exe

به منظور جزئیات بیشتر درباره Secedit.exe و سوئیچ‌های آن به آدرس http://technet2.microsoft.com/windowsserver/en/library/b1007de8-a11a-4d88-9370-25e2445605871033.mspx?mfr=true

ویزارد پیکربندی امنیتی

از ویزارد Security Configuraion Wizard به منظور ارتقاء امنیت یک سرور با بستن پورت‌ها و غیرفعال کردن سرویس‌های غیرضروری استفاده می‌شود. این ویزارد از صفحه اصلی Server Manager ، در بخش Security Information یا از پوشه Administrative Tools قابل اجراست. همچنین نسخه خط فرمان آن scwcmd.exe می‌باشد. در خط فرمان تایپ می‌کنیم scwcmd /? تا راهنمای دستور را ببینیم یا به آدرس http://technet2.microsoft.com/windowsserver2008/en/library/a222cb38-db08-4bf1-b9cf-6ec566c239e91033.mspx?mfr=true مراجعه می‌کنیم.

Security Cinfiguration Wizard نسل جدید ابزارهای مدیریت امنیت است. این ویزارد پیشرفته‌تر از ابزار Security Cinfiguration and Analysis و سازگاری بیشتری با پیکربندی مبتنی بر نقش در ویندوز سرور 2008 دارد. این ویزارد یک فایل تنظیمات امنیتی xml. می‌سازد که سرویس‌ها، تنظیمات امنیتی شامل قوانین فایروال، مقادیر رجیستری، سیاست‌های ممیزی و دیگر تنظیمات امنیتی را بر اساس نقش‌های یک سرور پیکربندی می‌کند. این تنظیمات قابل تغییر است و می‌توان آنرا به سرور دیگر اعمال کرد یا به یک GPO انتقال داد تا به سیستم‌های مختلف توزیع شود.

ایجاد سیاست امنیتی

برای ایجاد سیاست امنیتی ویزارد Security Cinfiguration را باز می‌کنیم. دکمه Next را کلیک کرده و Create A New Security Policy را انتخاب می‌کنیم. دکمه Next را کلیک کرده و نام سرور را وارد می‌کنیم تا ویزارد آنرا جستجو و تحلیل کند. سیاست امنیتی بر اساس نقش‌های سرور خواهد بود و ما باید روی سرور اعتبار مدیریتی داشته باشیم تا بتوانیم نقش‌های آنرا تحلیل کنیم. همچنین قبل از اجرای ویزارد باید مطمئن شویم همه برنامه‌هایی که از پورت‌های ورودی استفاده می‌کنند اجرا می‌شوند.

وقتی دکمه Next را کلیک می‌کنیم ویزارد شروع به تحلیل نقش‌های سرور منتخب می‌کند و از بانک اطلاعاتی پیکربندی امنیتی که سرویس‌ها و پورت‌های مورد نیاز هر نقش را تعریف می‌کند استفاده می‌کند. این بانک مجموعه‌ای از فایل‌های xml. است که در %SystemRoot%\Security\Msscw\Kbs نصب می‌شود.

نکته متمرکز کردن بانک اطلاعات پیکربندی امنیتی

در محیط‌های شبکه سازمانی بهتر است بانک مذکور متمرکز شود تا مدیران شبکه بتوانند از همان بانک در ویزارد Security Cinfiguration استفاده کنند. فایل‌های موجود در آدرس %SystemRoot%\Security\Msscw\Kbs را به یک مسیر شبکه‌ای کپی می‌کنیم سپس ویزارد را با دستور Scw.exe /Kb DatabaseLocation اجرا می‌کنیم. برای مثال دستور scw.exe /kb \\server01\scwkb ویزارد را با استفاده از بانک امنیتی در پوشه اشتراکی scwkb روی سرور SERVER01 باز می‌کند.

این ویزارد از بانک اطلاعات پیکربندی امنیتی برای اسکن سرور منتخب استفاده کرده و موارد زیر را بررسی می‌کند:

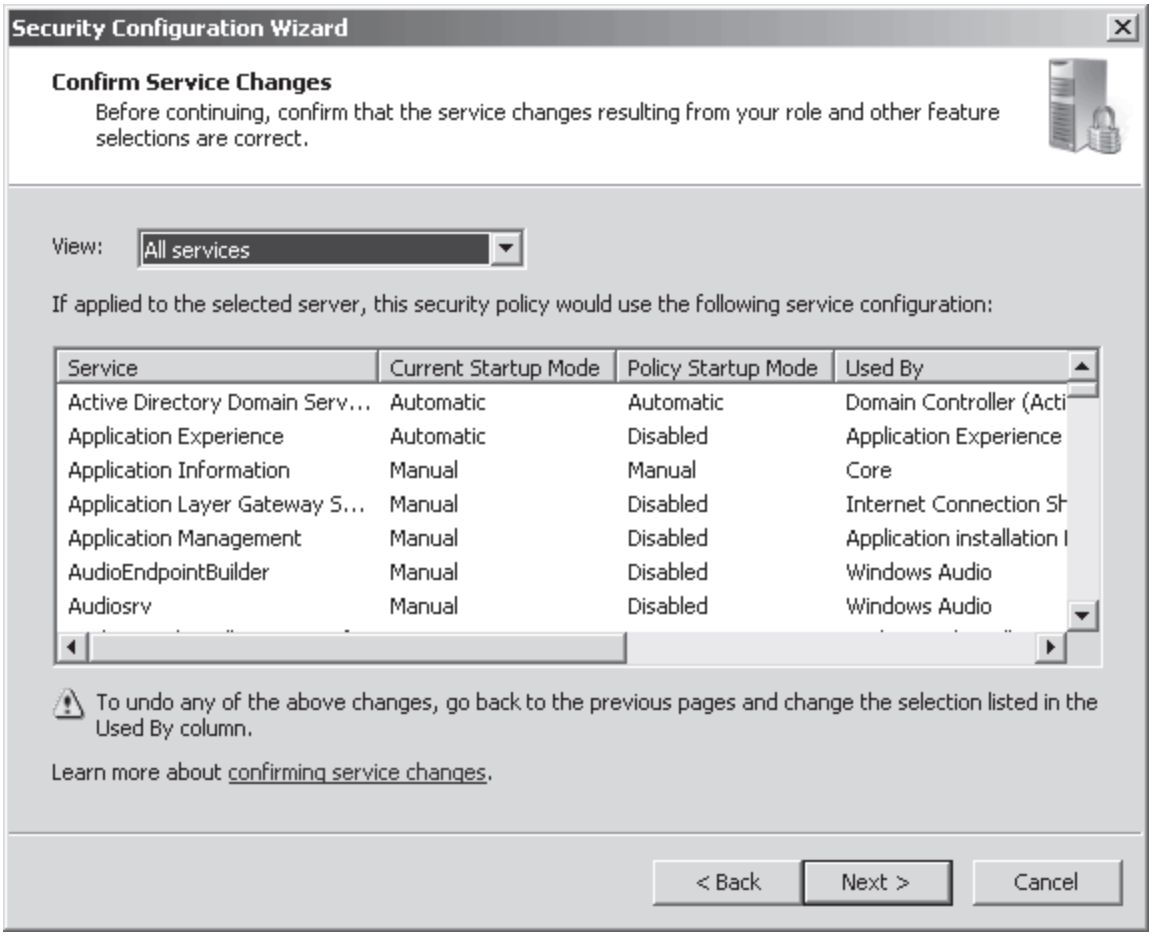
- نقش‌های نصب شده روی سرور
- نقش‌هایی که توسط سرور اجرا شده است.
- سرویس‌های نصب شده روی سرور که در بانک اطلاعاتی پیکربندی امنیتی تعریف نشده است.
- آدرس‌های IP و شماره subnet های پیکربندی شده برای سرور

اطلاعات به دست آمده درباره سرور در یک فایل با نام Main.xml ذخیره می‌شود. این فایل بانک اطلاعاتی پیکربندی (

configuration database) نامیده می‌شود که البته نباید با بانک اطلاعات پیکربندی امنیتی(security configuration database) اشتباه شود. با کلیک روی دکمه View Configuration Database در صفحه Processing Security Configuration این فایل نمایش داده می‌شود. تنظیمات اولیه در بانک اطلاعاتی پیکربندی baseline settings نامیده می‌شود. پس از اسکن سرور و ایجاد بانک اطلاعاتی پیکربندی امکان تغییر بانک اطلاعاتی وجود دارد که بعدا به منظور ایجاد سیاست‌های امنیتی استفاده می‌شود. این سیاست‌ها را می‌توان به سرور اعمال کرد. ویزارد Security Configuration هر کدام از چهار گروه سیاست امنیتی را در یک بخش ارائه می‌دهد.

- **پیکربندی سرویس مبتنی بر نقش** خروجی این بخش یک سری سیاست‌هایی است که وضعیت startup سرویس‌ها را روی سرور پیکربندی می‌کند. می‌خواهیم مطمئن شویم که فقط سرویس‌هایی استارت شوند که برای اجرای نقش سرور لازمند . برای دستیابی به این هدف ویزارد Security Configuration صفحاتی دارد که نقش‌های سروری، ویژگی‌های کلاینت، مدیریت و گزینه‌های دیگر کشف شده روی سرور را نمایش می‌دهد. در این ویزارد می‌توانیم نقش‌ها ویژگی‌ها و گزینه‌ها را اضافه یا حذف کنیم. در صفحه آخر با عنوان Confirm Service Changes که در شکل ۹- ۷ نیز نمایش داده شده تغییرات اعمال شده به سرویس‌ها بر اساس نقش‌هایی که مشخص کردیم قابل مشاهده است.

سرور نمایش داده شده در شکل ۹- ۷ یک DC است و می‌بینیم که سرویس AD DS طوری پیکربندی شده که به طور خودکار استارت شود. Policy نیز سرویس را برای استارت خودکار تنظیم کرده تا از نقش AD DS پشتیبانی کند. بهرحال صدا برای DC سرویس ضروری نیست بنابراین این سرویس با نام Audiosrv که توسط گزینه Windows Audio استفاده می‌شود توسط policy غیرفعال می‌شود.



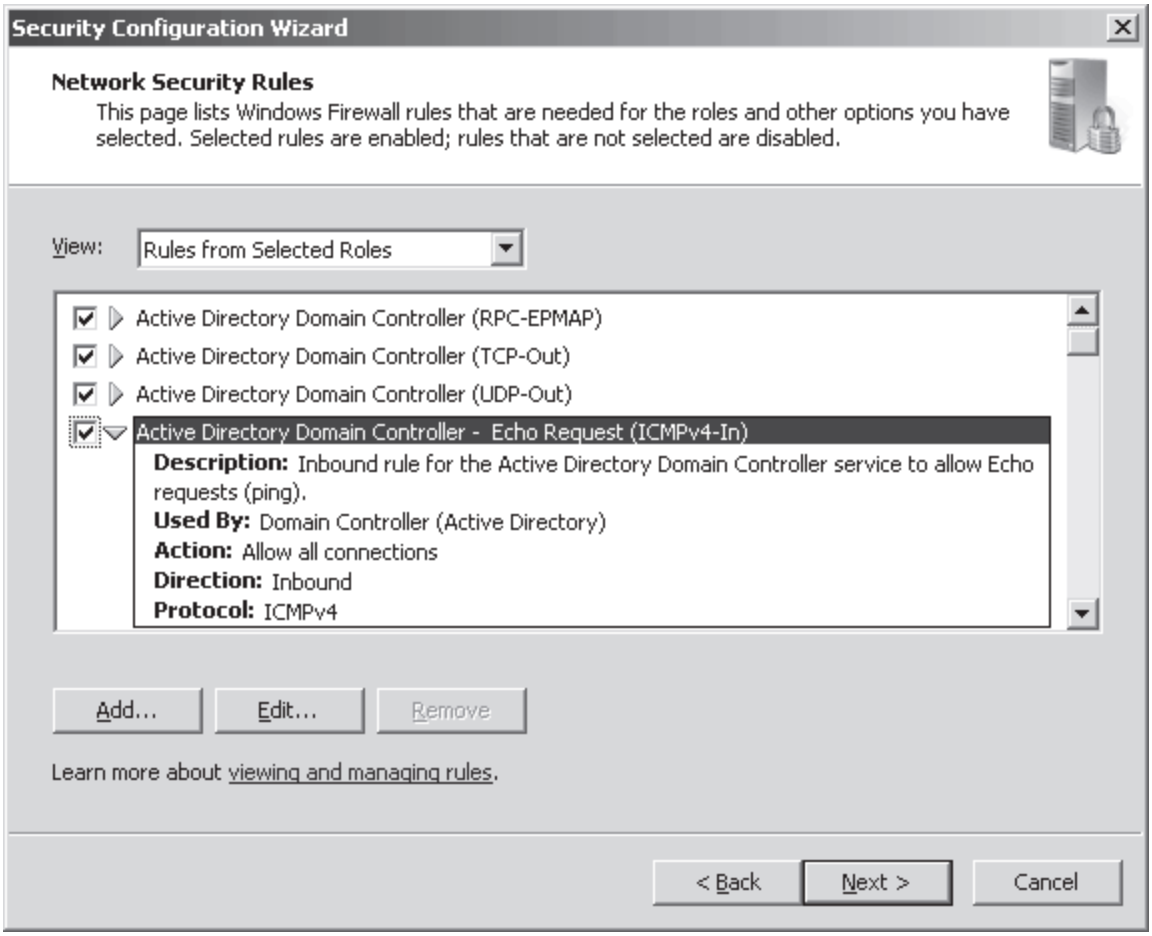
شکل ۹- ۷ صفحه Confirm Service Changes از ویزارد Security Configuration

اگر با تنظیمات نمایش داده شده در این صفحه موافق نباشیم می‌توانیم از دکمه Back استفاده کرده و آیتم‌ها را انتخاب یا از انتخاب خارج کنیم. سیاست‌های startup سرویس‌ها در صفحه Confirm Service Changes توسط نقش‌ها

سرویس‌ها و گزینه‌های انتخاب شده تعیین می‌شود. آنهایی که انتخاب نشده‌اند سیاست startup سرویس آنها غیرفعال است. این امکان وجود دارد که سروری که روی آن ویزارد Security Configuration اجرا می‌شود دارای سرویس‌هایی هستند که توسط بانک اطلاعاتی پیکربندی امنیتی ویزارد Security Configuration تعریف نشده‌اند. در صفحه Select Additional Services از ویزارد امکان افزودن سرویس‌های موجود در security policy وجود دارد به طوری که اگر سرویس‌ها روی سیستمی که policy روی آن اعمال می‌شود موجود باشد با توجه به تنظیمات startup در baseline configuration database استارت می‌شوند.

همچنین امکان دارد روی سروری که روی آن سیاست‌های امنیتی اعمال می‌شود سرویس‌هایی موجود باشد که روی سروری که از آن سیاست امنیتی ساخته شده وجود نداشته باشد. در صفحه Handling Unspecified Services می‌توانیم مشخص کنیم که چنین سرویس‌هایی غیرفعال باشند یا در حالت startup جاری خود باقی بمانند.

- **امنیت شبکه** بخش Network Security تنظیمات دیوار آتش سیاست امنیتی را فراهم می‌کند که توسط Windows Firewall with Advanced Security اعمال می‌شود. همانند بخش Role-Based Service Configuration بخش Network Security صفحه‌ای از تنظیمات نشات گرفته از تنظیمات baseline در بانک اطلاعاتی پیکربندی را نمایش می‌دهد. تنظیمات در بخش Network Security به جای حالت startup قوانین دیوار آتش است. شکل ۱۰- ۷ قانونی را نشان می‌دهد که به درخواست‌های ping ورودی به یک DC اجازه ورود می‌دهد. قوانین موجود قابل تغییر است و می‌توان قوانین مشخصی را حذف یا اضافه کرد.



شکل ۱۰- ۷ صفحه Network Security Rules از ویزارد Security Configuration

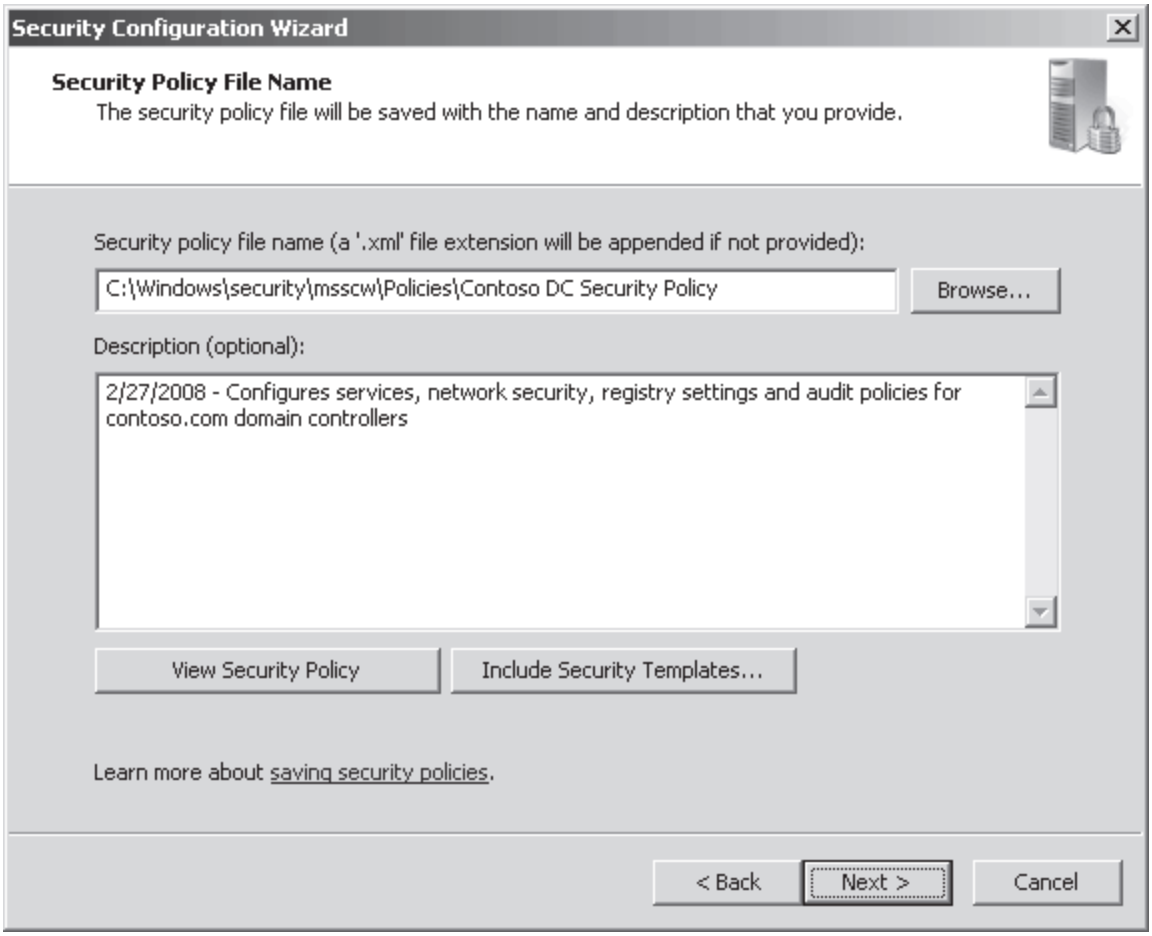
Windows Firewall with Advanced Security دیواره آتش stateful را با Internet Protocole security (IPSec) ترکیب می‌کند که همه پکت‌های Ipv4 و Ipv6 را بازرسی و فیلتر کرده و پکت‌های ناخواسته از بین می‌برد مگر قانونی در دیواره آتش ساخته شود که به ترافیک مربوط به یک پورت، برنامه یا سرویس اجازه عبور دهد. سیاست

امنیتی ایجاد شده توسط ویزارد Security Configuration قوانین دیوار آتش را مدیریت می‌کند ولی در این ویزارد پیکربندی IPSec انجام نمی‌شود.

- **تنظیمات رجیستری** بخش تنظیمات رجیستری پروتکل‌هایی را پیکربندی می‌کند که برای ارتباط با کامپیوترهای دیگر استفاده می‌شود. صفحات این ویزارد علامت‌گذاری پکت server message block (SMB) ، LDAP ، سطوح تایید هویت LAN Manager(LM) و انباره مقادیر درهم شده (hash) LM کلمات عبور را مشخص می‌کند. هر کدام از این تنظیمات در صفحه مناسب خود شرح داده شده و یک لینک در هر صفحه ما را به صفحه راهنمای ویزارد هدایت می‌کند.

- **سیاست ممیزی** این بخش تنظیماتی را ایجاد می‌کند که ممیزی موفقیت یا شکست عملیات مختلفی را مدیریت می‌کند. به علاوه این بخش به ما امکان می‌دهد یک الگوی امنیتی را با نام SCWAudit.inf به داخل سیاست امنیتی وارد کنیم. ابزار Security Templates که قبلا شرح داده شد برای امتحان تنظیمات الگو استفاده می‌شود که در آدرس %SystemRoot%\Security\Msscw\Kbs جای دارد.

در صورت عدم نیاز به هر یک از سه بخش آخر برای درج در سیاست امنیتی خود امکان گذر از کنار آنها در ویزارد وجود دارد. در آخر نام و مسیر فایل را همانند شکل ۱۱- ۷ وارد کرده و توضیحی به منظور مستندسازی درج می‌کنیم.



شکل ۱۱- ۷ صفحه Security Policy File Name از ویزارد Security Configuration

اگر روی دکمه View Security Policy کلیک کنیم تنظیمات سیاست امنیتی را می‌توانیم بررسی کنیم. البته امکان انتقال یک الگوی امنیتی به سیاست امنیتی وجود دارد. الگوهای امنیتی که قبلا معرفی شد شامل تنظیماتی است که در Managing Security Configuration with Security Templates وجود ندارد. مثال‌هایی از این تنظیمات گروههای محدود شده ، سیاست‌های event log و سیاست‌های امنیتی رجیستری و سیستم فایل می‌باشد. با درج یک الگوی امنیتی می‌توانیم مجموعه پربارتری از تنظیمات پیکربندی را در سیاست امنیتی داشته باشیم. اگر تنظیمی در الگوی امنیتی با ویزارد Security

Configuration تداخل داشته باشد تنظیم ویزارد در اولویت بالاتر قرار می‌گیرد. وقتی روی دکمه Next کلیک می‌کنیم گزینه‌های اعمال فوری الگوی امنیتی به سرور یا اعمال آن در زمان دیگر قابل انتخاب است.

ویرایش سیاست امنیتی

اجرای ویزارد Security Configuration و انتخاب Edit An Existing Security Policy ویرایش یک سیاست امنیتی ذخیره شده را امکان‌پذیر می‌کند. روی دکمه Browse کلیک می‌کنیم تا فایل سیاست امنیتی را با پسوند xml. پیدا کنیم. وقتی پیغام انتخاب سرور ظاهر شد سروری را که برای ساخت سیاست امنیتی استفاده شده است انتخاب می‌کنیم.

اعمال سیاست امنیتی

اگر بخواهیم یک سیاست امنیتی را اعمال کنیم ویزارد Security Configuration را باز می‌کنیم و در صفحه Configuration Action گزینه Apply An Existing Security Policy را انتخاب می‌کنیم. با استفاده از دکمه Browse محل فایل xml. را مشخص می‌کنیم. در صفحه Select Server سروری را که سیاست روی آن پیاده می‌شود مشخص می‌کنیم. بسیاری از تغییرات مانند افزودن قوانین جدید به دیوار آتش برای برنامه‌های در حال اجرا و غیرفعال کردن سرویس‌ها نیازمند راه‌اندازی مجدد هستند.

بی‌اثر کردن یک سیاست امنیتی اعمال شده

وقتی یک سیاست امنیتی پس از اعمال، نتایج مطلوبی به بار نمی‌آورد باید تنظیمات را به حالت اول برگردانیم. اجرای ویزارد Security Configuration و انتخاب گزینه Rollback The Last Applied Security Policy این کار را انجام می‌دهد. وقتی یک سیاست امنیتی توسط این ویزارد اعمال می‌شود فایلی به عنوان rollback ایجاد می‌شود که تنظیمات قبلی سیستم را ذخیره می‌کند. پروسه rollback این فایل را به روی سیستم اعمال می‌کند.

ویرایش تنظیمات یک سیاست امنیتی اعمال شده

وقتی یک الگوی امنیتی اعمال شده مقاصد ما را تامین نمی‌کند می‌توانیم به صورت دستی تنظیمات را توسط کنسول Local Security Policy که در آغاز این درس شرح داده شده تغییر دهیم. بنابراین با استفاده از ویزارد Security Configuration می‌توانیم به همه تنظیمات امنیتی از تنظیمات دستی گرفته تا الگوهای امنیتی و ساخت سیاست‌های امنیتی احاطه داشته باشیم.

توزیع یک سیاست امنیتی با استفاده از Group Policy

با سه روش یکی ویزارد Security Configuration دوم دستور Scwcmd.exe و سوم انتقال سیاست امنیتی به یک GPO می‌توان سیاست امنیتی ساخته شده توسط ویزارد Security Configuration را توزیع کرد. جهت انتقال یک سیاست امنیتی به یک GPO با اعتبار کاربر Administrator دامنه وارد شده و دستور Scwcmd.exe را همراه با transform به کار می‌بریم. برای مثال دستور scwcmd transform /p:"Contoso DC Security.xml" /g:"Contoso DC Security GPO" یک GPO با نام Contoso DC Security GPO ساخته و تنظیمات فایل Contoso DC Security.xml را به آن منتقل می‌کند. GPO حاصل مانند بقیه می‌تواند به یک شیء لینک شود. برای اطلاعات بیشتر درباره مراحل این کار دستور scwcmd.exe transform را تایپ می‌کنیم.

تنظیمات الگوها سیاست‌ها و GPO ها

همان‌گونه که در مقدمه درس گفته شد چند مکانیزم برای مدیریت تنظیمات امنیتی موجود است. ابزارهایی نظیر کنسول Local Security Policy می‌توانند تنظیمات یک سیستم مشخص را ویرایش کنند. از الگوهای امنیتی که از ویندوز 2000 به بعد اضافه شده برای مدیریت تنظیمات روی یک یا چند سیستم و یا مقایسه وضعیت جاری با وضعیت مطلوب تعریف شده توسط الگو استفاده می‌شود.

سیاست‌های امنیتی که توسط Security Configuration Wizard ایجاد می‌شود آخرین ابزار اضافه شده به مجموعه ابزار مدیریت پیکربندی امنیتی می‌باشد. این‌ها یک سری فایل‌های مبتنی بر نقش با پسوند xml. هستند که حالت‌های startup سرویس‌ها، قوانین دیوار آتش، سیاست‌های ممیزی و برخی تنظیمات رجیستری را تعریف می‌کنند. سیاست‌های امنیتی می‌تواند الگوهای امنیتی را ترکیب کند. الگوهای امنیتی و سیاست‌های امنیتی هردو می‌توانند با استفاده از Group Policy توزیع شوند.

تعداد زیاد ابزارهای موجود تشخیص بهترین روش مدیریت امنیتی را مشکل می‌کند. باید سعی کنیم تا حد ممکن از Group Policy برای توزیع پیکربندی امنیتی استفاده کنیم. از یک سیاست امنیتی مبتنی بر نقش که توسط ویزارد Security Configuration تهیه می‌شود می‌توانیم یک GPO بسازیم. پس از ساخت GPO می‌توانیم با ابزار Group Policy Management Editor تغییراتی را روی GPO ایجاد کنیم. تنظیماتی که با Group Policy پیکربندی نمی‌شود روی تنظیمات امنیتی GPO محلی پیکربندی می‌کنیم.

تمرینات مدیریت تنظیمات امنیتی

در این تمرینات توسط ابزارهای ارائه شده در درس تنظیمات امنیتی را مدیریت می‌کنیم. برای اجرای این تمرینات باید اشیاء زیر در دامنه contoso.com موجود باشد.

- OU سطح اول با نام Admins
- OU با نام Admin Groups در Admins OU
- یک گروه امنیتی global با نام SYS_DC Remote Desktop در Admins\Admin Groups OU . گروه باید عضو گروه Remote Desktop Users باشد. این عضویت به گروه SYS_DC Remote Desktop مجوز لازم برای ارتباط با پروتکل RDP-Tcp را فراهم می‌کند.

به جای این کار می‌توانیم با استفاده از کنسول Terminal Service Configuration این گروه را به ACL مربوط به ارتباط RDP-Tcp اضافه کنیم. روی RDP-Tcp کلیک راست کرده و Properties را انتخاب می‌کنیم. سپس روی زبانه Security کلیک می‌کنیم و دکمه Add را کلیک کرده و تایپ می‌کنیم SYS_DC Remote Desktop . دوبار روی OK کلیک می‌کنیم با کادر بسته شود.

تمرین ۱ پیکربندی Local Security Policy

در این تمرین local security policy را به منظور اعطاء مجوز به یک گروه برای ورود به یک DC به نام SERVER01 با استفاده از Remote Desktop به کار می‌گیریم. Local security policy مربوط به یک DC روی همان DC تاثیر می‌گذارد و بین DC ها تکثیر نمی‌شود.

۱. با کاربر Administrator به SERVER01 وارد می‌شویم.

۲. کنسول Local Security Policy را از پوشه Administrative Tools باز می‌کنیم.

۳. گره Security Settings\Local Policies\User Rights Assignments را باز می‌کنیم.

۴. در پنل وسط روی Allow Log On Through Terminal Services دوبار کلیک می‌کنیم.

۵. روی Add User Or Group کلیک می‌کنیم.

۶. تایپ می‌کنیم CONTOSO\SYS_DC Remore Desktop و دکمه OK را کلیک می‌کنیم.

۷. دوباره روی OK کلیک می‌کنیم.

اگر بخواهیم نتیجه این تمرین را ببینیم با کاربر عضو گروه SYS_DC Remote Desktop و از طریق Remote Desktop به DC وارد می‌شویم و حساب کاربری ساخته و آنرا به گروه اضافه می‌کنیم. مطمئن می‌شویم که گروه عضو گروه Remote Desktop Users است و مجوز ارتباط با استفاده از RDP-Tcp را دارد.

حالا تنظیم را حذف می‌کنیم چون در تمرینات بعدی با ابزارهای دیگری این تنظیم را پیکربندی می‌کنیم.

۸. روی Allow Log On Through Terminal Services دوبار کلیک می‌کنیم.

۹. CONTOSO\SYS_DC Remote Desktop را انتخاب می‌کنیم.

۱۰. روی Remove کلیک می‌کنیم.

۱۱. روی OK کلیک می‌کنیم.

تمرین ۲ ساخت الگوی امنیتی

در این تمرین یک الگوی امنیتی ساخته می‌شود که به گروه SYS_DC Remote Desktop حق ورود با استفاده از Remote Desktop را می‌دهد.

۱. با کاربر Administrator به SERVER01 وارد می‌شویم.

۲. پنجره Run را باز می‌کنیم.

۳. تایپ می‌کنیم mmc و کلید Enter را می‌زنیم.

۴. از منوی File گزینه Add/Remove Snap-in را انتخاب می‌کنیم.

۵. از لیست Available Snap-ins گزینه Security Templates را انتخاب و روی دکمه Add کلیک کرده و OK را می‌زنیم.

۶. از منوی File گزینه Save را انتخاب و کنسول را روی دسک‌تاپ با نام Security Management ذخیره می‌کنیم.

۷. روی C:\Users\Administrator\Documents\Security\Templates کلیک راست کرده و New Template را انتخاب می‌کنیم.

۸. تایپ می‌کنیم DC Remote Desktop و OK می‌کنیم.

۹. گره DC Remote Desktop\Local Policies\User Rights Assignment را باز می‌کنیم.

۱۰. در پنل وسط روی Allow Log On Through Terminal Services دوبار کلیک می‌کنیم.

۱۱. Define These Policy Settings In The Template را انتخاب می‌کنیم.

۱۲. روی Add User Or Group کلیک می‌کنیم.

۱۳. عبارت CONTOSO\SYS_DC Remote Desktop را تایپ کرده و OK می‌کنیم.

۱۴. روی OK کلیک می‌کنیم.

۱۵. روی DC Remote Desktop کلیک راست کرده و Save را انتخاب می‌کنیم.

تمرین ۳ استفاده از ابزار Security Configuration and Analysis

در این تمرین با کمک الگوی امنیتی DC Remote Desktop پیکربندی SERVER01 را تحلیل می‌کنیم و اختلاف بین

پیکربندی موجود سرور و پیکربندی مطلوب تعریف شده در الگو را تشخیص می‌دهیم. سپس الگوی امنیتی جدیدی می‌سازیم.

۱. با کاربر Administrator به SERVER01 وارد می‌شویم. کنسول Security Management که در تمرین ۲ ساختیم باز می‌کنیم.

۲. ابزار Add/Remove را از منوی File انتخاب می‌کنیم.

۳. از لیست Available Snap-ins گزینه Security Configuration And Analysis را انتخاب و دکمه Add را کلیک می‌کنیم. سپس OK را می‌زنیم.

۴. از منوی File گزینه Save را انتخاب کرده تا کنسول با تغییرات ذخیره گردد.

۵. گره Security Configuration And Analysis را انتخاب می‌کنیم.

۶. روی همان گره کلیک راست کرده و Open Database را انتخاب می‌کنیم. دستور Open Database برای ساخت بانک اطلاعاتی امنیتی جدید به کار می‌رود.

۷. تایپ می‌کنیم SERVER01 Test و روی Open کلیک می‌کنیم. کادر محاوره‌ای Import Template ظاهر می‌گردد.

۸. الگوی DC Remote Desktop را که در تمرین ۲ ساختیم انتخاب کرده و روی Open کلیک می‌کنیم.

۹. روی Security Configuration And Analysis کلیک راست کرده و Analyse Computer Now را انتخاب می‌کنیم.

۱۰. OK می‌کنیم تا مسیر پیش فرض برای ایجاد فایل گزارش خطا تایید شود.

۱۱. گره Local Policies را باز کرده و User Rights Assignment را انتخاب می‌کنیم.

۱۲. توجه کنید که Allow Log On Through Terminal Services policy با یک دایره قرمز و علامت X مشخص است. این نشان‌دهنده تفاوت بین تنظیم بانک و کامپیوتر می‌باشد.

۱۳. روی Allow Log On Through Terminal Services دوبار کلیک می‌کنیم.

۱۴. به تفاوت‌ها توجه کنید. کامپیوتر طوری پیکربندی نشده است که به گروه SYS_DC Remote Desktop Users اجازه ورود از طریق Terminal Services را بدهد.

۱۵. همچنین توجه کنید که Computer Setting اجازه ورود گروه Administrators را از طریق Terminal Services می‌دهد. این تنظیم مهمی است که باید به بانک انتقال یابد.

۱۶. کادر نزدیک Administrators زیر Database Setting را کلیک کرده و OK می‌کنیم. این کار باعث می‌شود حق ورود از طریق Terminal Services به بانک به گروه Administrators اعطاء شود. این کار تغییری در الگو ایجاد نمی‌کند و روی پیکربندی فعلی کامپیوتر تاثیر ندارد.

۱۷. روی Security Configuration And Analysis کلیک راست کرده و Save را انتخاب می‌کنیم. این کار بانک اطلاعات امنیتی را ذخیره می‌کند. اطلاعات نمایش داده شده در نوار وضعیت زمانی که دستور Save را انتخاب می‌کنیم نشان می دهند که الگو را ذخیره می‌کنیم ولی این درست نیست و ما بانک اطلاعات امنیتی را ذخیره می‌کنیم.

۱۸. روی Security Configuration And Analysis کلیک راست کرده و Export Template را انتخاب می‌کنیم.

۱۹. DC Remote Desktop را انتخاب و Save را می‌زنیم. حالا الگوی ساخته شده در تمرین ۲ با تنظیمات تعریف شده در بانک اطلاعات امنیتی در ابزار Security Configuration And Analysis جایگزین شده است.

۲۰. کنسول Security Management را بسته و باز می‌کنیم. این کار برای refresh کردن تنظیمات نمایش داده شده در ابزار Security Templates لازم است.

۲۱. گره C:\Users\Administrator\Security\Templates\DC Remote Desktop\Local Policies\User Rights Assignment را باز می‌کنیم.

۲۲. در پنل وسط روی Allow Log On Through Terminal Services دوبار کلیک می‌کنیم.

۲۳. توجه کنید که در الگوی امنیتی هم گروه Administrators و هم گروه SYS_DC Remote Desktop اجازه دارند از طریق Terminal Services ارتباط برقرار کنند.

۲۴. روی Security Cinfiguration And Analysis کلیک راست کرده و Configure Computer Now را انتخاب می‌کنیم.

۲۵. OK می‌کنیم تا مسیر فایل گزارش خطا تایید شود. تنظیمات بانک اطلاعات به سرور اعمال می‌شود. حالا تایید می‌کنیم که تغییرات حقوق کاربری اعمال شده است.

۲۶. کنسول Local Security Policy را باز می‌کنیم. اگر کنسول باز باشد کافی است روی Security Settings کلیک راست کرده و Reload را انتخاب کنیم.

۲۷. گره Security Settings\Local Policies\User Rights Assignment را باز می‌کنیم. روی Allow Log On Through Terminal Services دوبار کلیک می‌کنیم.

۲۸. بررسی می‌کنیم که هم Administrators و هم SYS_DC Remote Desktop لیست شده باشند. کنسول Local Security Policy تنظیمات جاری و واقعی سرور را نمایش می‌دهد.

تمرین ۴ استفاده از ویزارد Security Configuration

در این تمرین از ویزاردی برای تعریف یک سیاست امنیتی برای DC های دامنه contoso.com بر اساس پیکربندی SERVER01 استفاده می‌شود.

۱. به عنوان کاربر Administrator به SERVER01 وارد می‌شویم.

۲. ویزارد Security Configuration را باز می‌کنیم.

۳. Next را می‌زنیم.

۴. Create A New Security Policy را انتخاب کرده و Next را کلیک می‌کنیم.

۵. نام پیش فرض سرور را که SERVER01 است قبول کرده و Next را کلیک می‌کنیم.

۶. در صفحه Processing Security Configuration Database در صورت نیاز می‌توانیم روی View Configuration Database کلیک کرده و پیکربندی به دست آمده از SERVER01 را مرور کنیم.

۷. روی Next کلیک کرده و در صفحه معرفی بخش Role Based Configuration نیز Next را کلیک می‌کنیم.

۸. در صفحات Select Server Roles، Select Client Features، Select Administration And Other Options، Select Additional Services و Handling Unspecified Services می‌توانیم تنظیمات SERVER01 را بررسی کنیم ولی نمی‌توانیم آنها را تغییر دهیم.

۹. در صفحه Confirm Service Changes لیست بازشوی View را باز کرده و All Services را انتخاب می‌کنیم. تنیظمات ستون Current Startup Mode را بررسی می‌کنیم که حالت startup مربوط به SERVER01 را منعکس می‌کند و آنها را با تنظیمات ستون Policy Startup Mode مقایسه می‌کنیم. دوباره از منوی بازشوی View ، Changed Services را انتخاب می‌کنیم.

۱۰. در صفحه معرفی بخش Network Security دکمه Next را کلیک می‌کنیم.

۱۱. در صفحه Network Secuity Rules می‌توانیم قوانین دیواره آتش برگرفته از پیکربندی SERVER01 را بررسی کنیم. هیچ تنظیمی را تغییر نمی‌دهیم و روی Next کلیک می‌کنیم.

۱۲. در صفحه معرفی بخش Registry Settings روی Next کلیک می‌کنیم.

۱۳. در صفحات این بخش تنظیمات را بررسی می‌کنیم ولی چیزی را تغییر نمی‌دهیم. در صفحه Registry Settings Summary تنظیمات را بررسی کرده و دکمه Next را می‌زنیم.

۱۴. در صفحه معرفی بخش Audit Policy روی Next کلیک می‌کنیم.

۱۵. در صفحه System Audit Policy تنظیمات را بررسی کرده ولی هیچ چیز را تغییر نمی‌دهیم. روی Next کلیک می‌کنیم.

۱۶. در صفحه Audit Policy Summary تنظیمات ستون Current Setting and Policy Setting را بررسی کرده و روی Next کلیک می‌کنیم.

۱۷. در صفحه معرفی بخش Save Security Policy روی Next کلیک می‌کنیم.

۱۸. در کادر متنی Security Policy File Name عبارت DC Security Policy را تایپ می‌کنیم.

۱۹. روی Include Security Templates کلیک می‌کنیم.

۲۰. روی دکمه Add کلیک می‌کنیم.

۲۱. با استفاده از دکمه Browse مسیر الگوی DC Remote Desktop را که در تمرین ۳ ساختیم مشخص کرده و دکمه Open را می‌زنیم.

۲۲. روی OK کلیک می‌کنیم تا کادر بسته شود.

۲۳. روی View Security Policy کلیک می‌کنیم تا تنظیمات سیاست امنیتی را ببینیم. در پیغام مربوط به تایید استفاده از ActiveX control دکمه Yes را کلیک می‌کنیم. پس از بررسی پنجره را می‌بندیم و در پنجره Security Configuration Wizard روی Next کلیک می‌کنیم.

۲۴. تنظیم Apply Later را قبول کرده و روی Next کلیک می‌کنیم.

۲۵. روی Finished کلیک می‌کنیم.

تمرین ۵ انتقال سیاست امنیتی ساخته شده توسط ویزارد Security Configuration به یک Group Policy

در این تمرین سیاست امنیتی ساخته شده در تمرین ۴ را به GPO تبدیل می‌کنیم تا بتوانیم توسط Group Policy به کامپیوترها اعمال کنیم:

۱. با کاربر Administrator به SERVER01 وارد می‌شویم.

۲. پنجره خط فرمان را باز می‌کنیم.

۳. دستور cd c:\windows\security\msscw\policies را تایپ کرده و Enter را می‌زنیم.

۴. عبارت scwcmd transform /? را تایپ کرده و Enter را می‌زنیم.

۵. دستور scwcmd transform /p:"DC Security Policy.xml" /g:"DC Security Policy را تایپ کرده و کلید Enter را می‌زنیم.

۶. کنسول Group Policy Management را باز می‌کنیم.

۷. گره‌های Forest، Domains، contoso.com و Group Policy Objects را باز می‌کنیم.

۸. DC Security Policy را انتخاب می‌کنیم. این GPO توسط دستور Scwcmd.exe ساخته شده است.

۹. روی زبانه Settings کلیک می‌کنیم و تنظیمات GPO را بررسی می‌کنیم

۱۰. نزدیک Security Settings دکمه Show Link کلیک می‌کنیم.

۱۱. نزدیک Local Policies/ User Rights Assignment دکمه Show link را کلیک می‌کنیم.

۱۲. مطمئن می‌شویم که گروه‌های BUILTIN\Administrators و CONTOSO\SYS_DC Remote Desktop حق Allow Log On Through Terminal Services را دارند. GPO هنوز به DC ها اعمال نشده زیرا به Domain Controllers OU لینک نشده است. در این تمرین GPO را به هیچ شیء لینک نمی‌کنیم.

خلاصه درس

- تنظیمات امنیتی را می‌توانیم از طریق GPO محلی روی یک کامپیوتر خاص پیکربندی کنیم. این نوع GPO با استفاده از ابزار Group Policy Object Editor یا کنسول Local Security Policy قابل ویرایش است.
- تنظیمات امنیتی در یک الگوی امنیتی با استفاده از ابزار Security Templates قابل تعریف است. الگوهای امنیتی می‌تواند تعداد زیادی تنظیم مرتبط با امنیت را تعریف کند.
- الگوهای امنیتی توسط ابزار Security Configuration and Analysis برای ساخت بانک اطلاعاتی قابل استفاده است. سپس ابزار می‌تواند پیکربندی سیستم را از بابت تفاوت‌های بین تنظیمات جاری کامپیوتر و بانک اطلاعاتی تحلیل کند. همچنین ابزار قادر است تنظیمات بانک را به کامپیوتر اعمال کند یا تنظیمات بانک را به یک الگوی امنیتی منتقل کند.
- Secedit.exe ابزار خط فرمانی است که عملکرد ابزار Security Configuration and Analysis را اجرا کرده و توسعه می‌دهد.
- سیاست‌های امنیتی مجموعه‌هایی از تنظیمات هستند که توسط ویزارد Security Configuration ساخته می‌شوند و حالت‌های startup سرویس‌ها، قوانین دیوار آتش، تنظیمات مشخص رجیستری و سیاست‌های ممیزی را تعریف می‌کنند. ویزارد Security Configuration سیاست‌های امنیتی را مبتنی بر نقش‌های سرور می‌سازد.
- یک سیاست امنیتی می‌تواند تنظیمات را در الگوی امنیتی ثبت کند. در حالتی که تنظیمات تداخل داشته باشند تنظیمات سیاست امنیتی اولویت دارند.
- Scwcmd.exe ابزار خط فرمانی است که عملکرد ویزارد Security Configuration را اجرا کرده وتوسعه می‌دهد.
- می‌توانیم یک الگوی امنیتی را به یک GPO منتقل کنیم.
- می‌توانیم از دستور Scwcmd.exe transform برای تبدیل سیاست امنیتی به یک GPO بهره ببریم.

سئوالات پایان درس

۱. می‌خواهیم تنظیمات امنیتی را از طریق Group Policy به سرورها اعمال کنیم. تنظیمات باید حقوق کاربری را که روی یک سرور در محیط تست پیکربندی شده اعمال کند. از کدام ابزار باید استفاده می‌شود؟

A. Local Security Policy
B. Security Configuration And Analysis
C. Security Configuration Wizard
D. Security Templates

۲. می‌خواهیم تنظیمات امنیتی را از طریق Group Policy به سرورها اعمال کنیم. تنظیمات باید سرویس‌ها، قوانین دیوار آتش و سیاست‌های ممیزی مناسب برای سرورهای شبکه را که به عنوان سرورهای فایل و چاپ عمل می‌کنند پیکربندی کند. کدام ابزار این کار را بهتر انجام می‌دهد؟

A. Local Security Policy

B. Security Configuration And Analysis

C. Security Configuration Wizard

D. Security Templates

۳. توسط ویزارد Security Configuration یک سیاست امنیتی ساخته‌ایم. حالا می‌خواهیم تنظیمات آنرا به سرورهای Servers OU اعمال کنیم. کدام مرحله از مراحل زیر ضروری است؟ (دو گزینه را انتخاب کنید که هر کدام بخشی از جواب هستند.)

A. از دستور Scwcmd.exe /transform استفاده می‌کنیم.

B. یک شیء Group Policy در Group Policy Objects container می‌سازیم.

C. روی گره Security Settings از یک GPO کلیک راست کرده و Import را انتخاب می‌کنیم.

D. GPO را به Servers OU لینک می‌دهیم.

E.

درس ۳: مدیریت نرم‌افزار با Group Policy Software Installation

ممکن است با ابزارهای متعددی که به منظور توزیع نرم‌افزار در سازمان استفاده می‌شود نظیر Microsoft System Center Configuration Manager (Configuration Manager) و نسخه‌های قدیمی آن Microsoft System Management Server (SMS) آشنا باشید . اگرچه این ابزارها توانایی‌های زیادی دارند می‌توانیم بسیاری از نرم‌افزارها را بدون این ابزارها توسط سرویس نصب نرم‌افزار Group Policy یا (GPSI) توزیع کنیم.

بعد از این درس می‌توانیم:

- نرم‌افزارها را با استفاده از GPSI روی کامپیوترها و کاربران توزیع کنیم.
- نرم‌افزار نصب شده با GPSI را حذف کنیم.

زمان تقریبی: ۴۵ دقیقه

مفهوم نصب نرم‌افزار با Group Policy

GPSI برای ساخت یک محیط نرم‌افزاری طراحی شده استفاده می‌شود که ویژگی‌های زیر را دارد:

- کاربران به برنامه‌هایی که برای کارشان نیاز دارند دسترسی دارند صرف نظر از این که ازکدام کامپیوتر به شبکه وارد می‌شوند.
- کامپیوترها برنامه‌های مورد نیاز را خواهند داشت بدون اینکه تیم پشتیبانی دخالتی در این کار داشته باشند.
- برنامه‌ها برای تامین نیازهای سازمان می‌توانند به روز، نگهداری و حذف شوند.

Extention مربوط به نصب نرم‌افزار یکی از extention های سمت کلاینت است (CSEها) که با استفاده از Group Policy از مدیریت پیکربندی و تغییر پشتیبانی می‌کند. CSE ها در فصل ۶ بررسی شدند. Extention به ما اجازه می‌دهد توزیع اولیه، ارتقا و حذف متمرکز نرم‌افزار را مدیریت کنیم. همه پیکربندی‌های توزیع نرم‌افزار در یک GPO با استفاده از روندهایی که جزئیات آن در

همین درس شرح داده می‌شود مدیریت می‌شود.

Windows Installer Packages

GPSI از سرویس Windows Installer برای نصب نگهداری و حذف نرم‌افزار استفاده می‌کند.سرویس Windows Installer نرم‌افزارها را با استفاده از اطلاعات موجود در پکیج Windows Installer مربوط به نرم‌افزار مدیریت می‌کند. پکیج Windows Installer در فایلی با پسوند msi. قرار دارد که وضعیت نصب برنامه را مشخص می‌کند. Package ،دربرگیرنده دستورات صریح راجع به نصب و حذف یک برنامه می‌باشد. این امکان وجود دارد که package ها را با استفاده از یکی از انواع فایل زیر سفارشی کنیم:

- فایل‌های Transform با پسوند mst. این فایل‌ها وسیله‌ای برای سفارشی کردن نصب یک برنامه محسوب می‌شوند. برخی از برنامه‌ها ویزاردها یا الگوهایی را فراهم می‌کنند که به کاربر اجازه ساخت transform را می‌دهد. برای مثال شرکت Adobe ابزار توزیع شبکه‌ای برای برنامه Adobe Acrobat Reader ارائه داده که یک transform تولید می‌کند. بسیاری از سازمان‌ها از transform ها برای پیکربندی تایید مجوز کاربر (end user license agreement) و یا غیرفعال کردن ویژگی‌های خاصی از برنامه مانند به روز رسانی خودکار که از طریق اینترنت انجام می‌شود استفاده می‌کنند.

- فایل‌های Patch با پسوند msp. این فایل‌ها برای به روز رسانی یک فایل msi. برای دریافت آپدیت‌های امنیتی، bug fix ها و سرویس پک ها استفاده می‌شود. فایل msp. دستورالعمل‌هایی درباره اعمال فایل‌های به روز رسانی و کلیدهای رجیستری در پچ‌های نرم‌افزاری، سرویس پک یا آپدیت‌های نرم‌افزاری دارد. برای مثال آفیس 2003 و نسخه‌های جدیدتر با فایل‌های msp. ارائه می‌شوند.

نکته نصب فایل‌های msp. و mst.

فایل‌های فوق را به تنهایی نمی‌توان توزیع کرد. این فایل‌ها باید به یک پکیج Windowds Installer اعمال گردد.

GPSI از فایل‌های برنامه‌های non-MSI (zap.) به صورت محدود استفاده می‌کند. به این نوع فایل‌ها پکیج‌های برنامه سطح پایین نیز می‌گویند که محل توزیع نرم‌افزار (SDP) و دستور setup را مشخص می‌کند. برای جزئیات بیشتر مقاله شماره 231747 را در آدرس http://support.microsoft.com/?kbid=231747 مشاهده کنید. بسیاری از سازمان‌ها از فایل‌های zap. استفاده نمی‌کنند چون برای نصب برنامه کاربر باید دسترسی مدیریتی به سیستم داشته باشد. وقتی GPSI یک برنامه را با استفاده از پکیج Winsows Installer نصب می‌کند کاربر نیاز به دسترسی مدیریتی ندارد و در سازمان‌های با امنیت بالا قابل پیاده سازی است.

نکته GPSI و پکیج Windows Installer

GPSI تنها در صورتی می‌تواند برنامه‌ها را به طور کامل مدیریت کند که برنامه‌ها با استفاده از پکیج Windows Installer نصب شوند. ابزارهای دیگری نظیر Configuration Manager و SMS می‌توانند برنامه‌هایی که از مکانیزم‌های توزیع دیگر استفاده می‌کنند مدیریت کنند.

فایل msi. ، transform و دیگر فایل‌ها که برای نصب یک برنامه مورد نیاز است در یک SDP به اشتراک گذاشته شده ذخیره می‌شوند.

گزینه‌های توزیع نرم‌افزار

ما می‌توانیم از طریق assign کردن برنامه‌ها به کاربران یا کامپیوترها یا با publish کردن برنامه‌ها برای کاربران نرم‌افزارها را توزیع کنیم. روش assign زمانی به کار می‌آید که برنامه اجباری باشد و زمانی که کاربران تشخیص می‌دهند برنامه برایشان مفید است یا نه از publish استفاده می‌کنیم.

نکته امتحانی تفاوت بین assign کردن و publish کردن برنامه‌ها را باید یاد بگیرید.

Assign کردن برنامه وقتی برنامه‌ای به کاربری assign می‌شود تنظیمات رجیستری برنامه شامل پسوندهای نام فایل به روز شده و میانبرهای آن در منوی استارت یا دسک‌تاپ ایجاد می‌شود. برنامه در اولین بار که کاربر برنامه را روی کامپیوتر اجرا می‌کند نصب می‌شود یا با انتخاب برنامه در منوی استارت یا با باز کردن یک سند که به برنامه associate شده است. زمانی که یک برنامه به

کامپیوتر assign می‌شود هنگام بوت شدن ویندوز برنامه نصب می‌شود.

Publish کردن برنامه وقتی برنامه‌ای برای کاربری publish می‌شود حتی اگر روی کامپیوتر کاربر نصب شده باشد ظاهر نمی‌شود. در عوض برنامه به عنوان برنامه در دسترس کاربر برای نصب توسط اپلت Add Or Remove Programs در کنترل پنل در ویندوز XP یا در Programs And Features در ویندوز سرور 2008 و ویستا ظاهر می‌شود. به علاوه برنامه می‌تواند هنگامی که کاربر یک فایل associate به برنامه را باز می‌کند نصب شود. برای مثال اگر Acrobat Reader برای کاربر publish شده باشد وقتی کاربر یک فایل مرتبط را باز می‌کند برنامه شروع به نصب می‌کند.

برنامه‌ها می‌توانند به کاربران یا کامپیوترها assign یا publish شود و ما می‌توانیم یک ترکیب مناسب برای دستیابی به اهداف مدیریتی نرم‌افزاری ایجاد کنیم. جدول ۱- ۷ جزئیات مختلف گزینه‌های توزیع نرم‌افزار را شرح می‌دهد.

جدول ۱- ۷ گزینه‌های توزیع نرم‌افزار

	Publish (فقط کاربر)	Assign (کاربر)	Assign (کامپیوتر)
پس از توزیع GPO نرم‌افزار برای نصب آماده است	دفعه بعد که کاربر وارد می‌شود	دفعه بعد که کاربر وارد می‌شود	دفعه بعد که کامپیوتر بوت می‌شود
کاربر برنامه را نصب می‌کند از	کنترل پنل – Add Or Remove Programs در ویندوز XP یا Programs And Features در ویندوز 2008 و ویستا	منوی استارت یا میانبر دسک‌تاپ. برنامه می‌تواند طوری پیکربندی شود که به طور خودکار هنگام ورود نصب گردد.	برنامه به طور خودکار هنگام بوت کامپیوتر نصب می‌شود
نرم‌افزار نصب نمی‌شود و کاربر فایلی را باز می‌کند که به برنامه associate شده آیا برنامه نصب می‌گردد؟	بلی اگر auto-install فعال باشد	بلی	برنامه قبلا نصب شده است
آیا کاربر می‌تواند برنامه را با استفاده ازکنترل پنل حذف کند؟	بلی و کاربر می‌تواند دوباره از کنترل پنل آنرا نصب کند	بلی و نرم‌افزار برای نصب مجدد از میانبرهای منوی استارت یا association های فایل در دستری است	خیر فقط کاربر مدیر محلی می‌تواند برنامه را حذف کند و کاربر می‌تواند پروسه تعمیر نرم‌افزار را اجرا کند
فایل‌های نصب مورد پشتیبانی	پکیج‌های Windows Installer (فایل‌های msi.) و فایل‌های zap	پکیج‌های Windows Installer (فایل‌های msi.)	پکیج‌های Windows Installer (فایل‌های msi.)

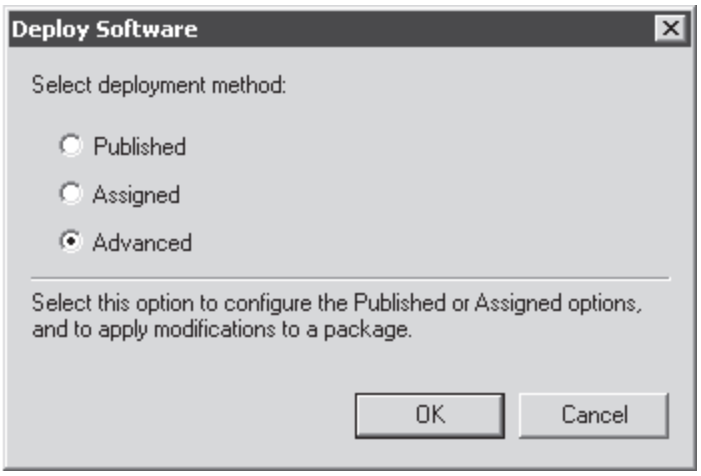
آماده سازی SDP

حال که GPSI را در سطح بالا یاد گرفتیم می‌توانیم SDP را آماده کنیم. SDP یک پوشه به اشتراک گذاشته شده است که کاربران و کامپوترها می‌توانند از روی آن برنامه‌ها را نصب کنند. پوشه‌ای را به اشتراک گذاشته و داخل آن پوشه‌های دیگری برای برنامه‌های مختلف ایجاد می‌کنیم. سپس پکیج برنامه و فایل‌های مورد نیاز را به پوشه‌ها کپی می‌کنیم. مجوز Read And Execute برای کاربران و کامپیوترها روی پوشه‌ها اعطاء می‌کنیم که کمترین مجوز مورد نیاز برای نصب برنامه از SDP می‌باشد. مدیران SDP باید بتوانند فایل‌ها را تغییر دهند یا حذف کنند.

ساخت GPO توزیع نرم‌افزار

برای این کار ابتدا از کنسول Group Policy Management برای ساخت یک GPO جدید یا انتخاب GPO موجود استفاده می‌شود. GPO را با ابزار GPME ویرایش می‌کنیم. گره‌های User Configration\Policies\Software Settings\Software Installation را باز می‌کنیم. یا به جای آن می‌توانیم گره Software Installation را در شاخه

Computer Configration باز کنیم. روی Software Installation کلیک راست کرده و New و بعد Package را انتخاب می‌کنیم. از دکمه Browse برای محل‌یابی فایل msi. مربوط به برنامه استفاده می‌کنیم. روی Open کلیک می‌کنیم. کادر محاوره‌ای Deploy Software همانند شکل ۱۲- ۷ ظاهر می‌شود. Published ، Assigned یا Advanced را انتخاب می‌کنیم. امکان publish کرده یک برنامه به کامپیوتر وجود ندارد بنابراین وقتی پکیج در گره Software Installation در Computer Configuration ایجاد می‌شود این گزینه‌ها در دسترس نیستند.



شکل ۱۲- ۷ کادر محاوره‌ای Deploy Software

گزینه Advanced ما را قادر می‌سازد مشخص کنیم برنامه publish شود یا assign و همچنین به ما اجازه می‌دهد خصوصیات پیشرفته پکیج برنامه را پیکربندی کنیم. بنابراین پیشنهاد می‌گردد از این گزینه استفاده شود. کادر محاوره‌ای Package Properties ظاهر می‌شود. از بین خصوصیات مهم چند مورد در زیر توضیح داده می‌شود:

- **Deployment Type** در زبانه Deployment بوده که یکی از موارد Published یا Assigned مشخص می‌شود.
- **Deployment Options** بر اساس انتخاب نوع توزیع ،گزینه‌های مختلفی در بخش Deployment Options ظاهر می‌شود. این گزینه‌ها همراه دیگر تنظیمات زبانه Deployment رفتار نصب برنامه را مدیریت می‌کنند.
- **Uninstall This Application When It Falls Out Of The Scope Of Management** اگر این گزینه انتخاب شود هنگامی که دیگر GPO روی کاربر یا کامپوتر اعمال نشود برنامه به طور خودکار حذف می‌شود.
- **Upgrades** در زبانه Upgrades می‌توانیم برنامه‌ای را که این پکیج ارتقاء می‌دهد مشخص می‌کنیم. ارتقاء در بخش بعدی همین درس شرح داده می‌شود.
- **Categories** در این زبانه می‌توانیم پکیج را به یک یا چند دسته (category) associate کنیم. دسته‌ها زمانی استفاده می‌شوند که یک برنامه به یک کاربر publish می‌شود. وقتی کاربر به کنترل پنل وارد می‌شود تا برنامه را نصب کند برنامه‌هایی که با GPSI ، publish شده‌اند در گروههایی بر اساس این دسته‌ها حضور دارند. برای ایجاد دسته‌هایی که برای associate کردن با پکیج‌ها استفاده می‌شوند روی Software Installation کلیک راست کرده و Properties را انتخاب می‌کنیم سپس زبانه Categories را باز می‌کنیم.
- **Modifications** وقتی یک فایل transform (.mst) داریم که پکیج را سفارشی می‌کند دکمه

Add را کلیک می‌کنیم تا فایل transform را با پکیج associate کنیم. بیشتر زبانه‌ها در کادر محاوره‌ای Properties پکیج برای تغییر تنظیمات در هر زمان در دسترس است. بهرحال زبانه Modification فقط زمانی که پکیج جدید ساخته می‌شود و گزینه Advanced همانند شکل ۱۲- ۷ انتخاب می‌شود در دسترس قرار می‌گیرد.

مدیریت حوزه GPO توزیع نرم‌افزار

پس از ساخت GPO توزیع نرم‌افزار می‌توانیم حوزه GPO را مشخص کنیم که برنامه روی کامپیوترها یا کاربران مشخصی توزیع شود. در بسیاری از سناریوهای مدیریت نرم‌افزار برنامه‌ها باید به کامپیوترها assign شود تا کاربران. این به این دلیل است که بیشتر مجوزهای نرم‌افزار به برنامه اجازه می‌دهد که فقط روی یک کامپیوتر نصب شود و اگر برنامه به کاربر assign شود روی هر کامپیوتری که کاربر وارد شود برنامه نصب می‌شود.

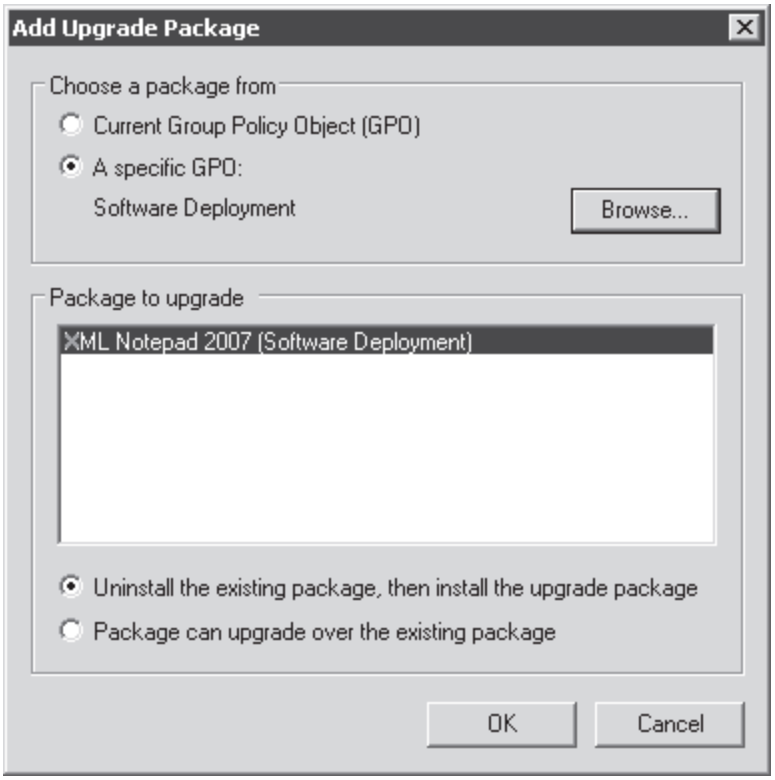
همانطوریکه در فصل ۶ یاد گرفتیم می‌توانیم حوزه یک GPO را با لینک کردن آن به یک OU یا با فیلتر کردن آن تعیین کنیم به طوری که فقط روی یک گروه امنیتی global اعمال گردد. بسیاری از سازمان‌ها عقیده دارند مدیریت نرم‌افزار توسط لینک کردن GPO برنامه به دامنه و فیلتر کردن آن با یک گروه امنیتی global که کاربران و کامپوترهای مورد نظر را در بر می‌گیرند ساده‌تر است. به عنوان مثال GPO که ابزار XML Notepad (از طریق سایت دانلود مایکروسافت قابل دانلود است) را توزیع می‌کند می‌تواند به دامنه لینک شده و با یک گروه شامل برنامه‌نویسان که به برنامه نیاز دارند فیلتر شود.

بهتر است گروه نام توصیفی داشته باشد که مشخص کننده منظور ایجاد آن باشد مانند APP_XML Notepad.

نگهداری برنامه‌های توزیع شده توسط Group Policy

پس از نصب برنامه توسط کامپیوتر با استفاده از پکیج Windows Installer مشخص شده توسط GPO ، کامپیوتر برای نصب دوباره برنامه در هر به روز رسانی Group Policy تلاشی نمی‌کند. ممکن است شرایطی به وجود آید که بخواهیم سیستم را مجبور کنیم برنامه را دوباره نصب کند. برای مثال وقتی تغییر کوچکی در پکیج Windows Installer ایجاد می‌شود نمونه‌ای از این شرایط است. برای توزیع دوباره یک برنامه که با Group Policy توزیع شده روی پکیج در GPO کلیک راست کرده All Tasks را انتخاب و سپس Redeploy Application را انتخاب می‌کنیم.

همچنین امکان ارتقاء یک برنامه توزیع شده با GPSI وجود دارد. برای نسخه جدید برنامه در گره Software Installation از GPO پکیجی ایجاد می‌کنیم. پکیج می‌تواند هم در همان GPO باشد که پکیج مربوط به نسخه قبلی وجود دارد و هم در GPO دیگر باشد. روی پکیج کلیک راست کرده و Properties را انتخاب می‌کنیم. زبانه Upgrades را باز کرده و روی دکمه Add کلیک می‌کنیم. کادر محاوره‌ای Add Upgrade Package همانند شکل ۱۳- ۷ ظاهر می‌شود.



شکل ۱۳- ۷ کادر محاوره‌ای Add Upgrade Package

مشخص می‌کنیم که پکیج نسخه قبلی برنامه در همین GPO است یا GPO دیگر. اگر در GPO دیگری باشد با دکمه Browse آنرا انتخاب می‌کنیم. سپس از لیست Package To Upgrade پکیج مورد نظر را انتخاب می‌کنیم. براساس رفتار ارتقاء برنامه یکی از گزینه‌های ارتقاء نشان داده شده در انتهای شکل ۱۳- ۷ را انتخاب کرده و OK را می‌زنیم.

همچنین می‌توانیم یک برنامه را که با GPSI توزیع شده حذف کنیم. برای این کار روی پکیج کلیک راست کرده و All Tasks و بعد Remove را انتخاب می‌کنیم. درکادر محاوره‌ای Remove Software یکی از دو گزینه زیر را انتخاب می‌کنیم:

- Immidiately Uninstall The Software From Users And Computers این گزینه که به آن forced removal نیز می‌گویند باعث می‌شود کامپیوترها برنامه را حذف کنند. اگر برنامه با یک پکیج در بخش Computer Configuration مربوط به GPO توزیع شده باشد Extention نصب برنامه هنگام بوت شدن کامپیوتر برنامه را حذف می‌کند. اگر پکیج در بخش User Configuration باشد برنامه در زمان ورود بعدی کاربر حذف می‌شود.

- Allow Users To Continue To Use The Software, But Prevent New Installations این تنظیم که به آن optional removal نیز می‌گویند باعث می‌شود extention نصب برنامه از افزودن پکیج به سیستم‌هایی که هنوز پکیج روی آنها نصب نشده جلوگیری کند. کامپیوترهایی که برنامه را نصب کرده‌اند مجبور به حذف برنامه نیستند.

اگر از یکی از این دو گزینه برای حذف برنامه از طریق GPSI استفاده کنیم مهم است که قبل از اقدام به حذف، غیرفعال کردن یا برداشتن لینک GPO به تنظیمات GPO اجازه تکثیر روی همه کامپیوترهای حوزه GPO را بدهیم. کلاینت‌ها باید این تنظیم را که مشخص کننده forced removal یا optional removal است دریافت کنند. اگر قبل از اینکه همه کلاینت‌ها این تنظیم را دریافت کنند GPO حذف شود یا دیگر به حوزه اعمال نشود برنامه حذف نمی‌شود. این مسئله در شبکه‌های با کاربران سیار دارای لپ‌تاپ که ممکن است برای مدتی به شبکه متصل نشوند خیلی مهم است.

هنگام ساخت پکیج نرم‌افزار اگر گزینه Uninstall This Application When It Falls Out Of The Scope Of Management انتخاب شود به راحتی می‌توان GPO را حذف کرد غیرفعال کرد یا لینک را برداشت و در نتیجه برنامه اجبارا از

روی کامپیوترهایی که پکیج را با تنظیم فوق نصب کرده‌اند حذف می‌شود.

GPSI و لینک‌های ضعیف

وقتی یک کلاینت Group policy به روز می‌شود سرعت شبکه را تست می‌کند. همه extention های سمت کلاینت یا به منظور پردازش Group Policy یا جهت بی‌اثرکرده تنظیمات به دلیل وجود لینک ضعیف پیکربندی می‌شوند. GPSI به طور پیش‌فرض روی لینک‌های ضعیف تنظیمات Group Policy را پردازش نمی‌کند چراکه نصب نرم‌افزار روی این گونه لینک‌ها کندی زیاد سیستم را در بر خواهد داشت.

رفتار پردازش policy روی لینک‌های ضعیف در extention سمت کلاینت با استفاده از تنظیم موجود در Computer Configuration\Policies\Administrative Templates\System\Group Policy قابل تغییر است. برای مثال امکان تغییر رفتار extention نصب برنامه طوری که روی لینک ضعیف پردازش انجام شود وجود دارد.

همچنین می‌توانیم آستانه سرعت ارتباط را که به لینک ضعیف تعبیر می‌شود تغییر دهیم. با پیکربندی آستانه در سطح پایین می‌توانیم extension سمت کلاینت را متقاعد کنیم لینک موجود ضعیف نیست در حالی که واقعا هست. Group Policy Slow Link Detection تنظیمات مجزایی برای پردازش policy کامپیوتر و کاربر دارد. تنظیمات در پوشه Administrative Templates\System\Group Policy در Computer Configuration و User Configuration قرار دارد.

تمرینات مدیریت نرم‌افزار با برنامه نصب Group Policy

در این تمرین با استفاده از GPSI برنامه را نصب می‌کنیم، ارتقاء می‌دهیم و حذف می‌کنیم. مدیریت نرم‌افزار با استفاده از یک ویرایشگر XML ساده که از سایت مایکروسافت قابل دانلود است به نام XML Notepad انجام می‌شود. برای اجرای این تمرین مراحل مقدماتی زیر را باید انجام دهیم:

۱. یک OU سطح اول به نام Groups ساخته و در آن OU دیگری با نام Applications می‌سازیم.

۲. در Application OU یک گروه امنیتی global با نام APP_XML Notepad برای کاربران و کامپیوترهایی که XML Notepad روی آنها توزیع می‌شود می‌سازیم.

۳. پوشه‌ای با نام Software در درایو C روی SERVER01 می‌سازیم. در این پوشه پوشه دیگری به نام XML Notepad می‌سازیم. سپس به گروه APP_XML Notepad نسبت به این پوشه مجوز Read And Execute می‌دهیم. پوشه Software را به اشتراک می‌گذاریم و به گروه Everyone مجوز Allow Full Control می‌دهیم.

۴. XML Notepad را دانلود کرده و در پوشه Software\ XML Notepad ذخیره می‌کنیم. نسخه دانلود شده را یادداشت می‌کنیم. در زمان نوشتن کتاب نسخه 2007 موجود بوده است.

تمرین۱ ساخت GPO توزیع نرم‌افزار

در این تمرین یک GPO برای توزیع XML Notepad روی کامپیوتر برنامه‌نویسان شرکت می‌سازیم.

۱. با کاربر Administrator به SERVER01 وارد می‌شویم.

۲. کنسول GPMC را باز می‌کنیم.

۳. روی Group Policy Objects container کلیک راست کرده و New را انتخاب می‌کنیم.

۴. در کادر Name نام برنامه را تایپ می‌کنیم. برای مثال XML Notepad و سپس OK می‌کنیم.

۵. روی XML Notepad GPO کلیک راست کرده و Edit را انتخاب می‌کنیم.

۶. گره User Configuration\Policies\Software Settings را باز می‌کنیم.

۷. روی Software Installation کلیک راست کرده و New و سپس Package را انتخاب می‌کنیم.

۸. در کادر متنی File Name مسیر شبکه‌ای پوشه توزیع برنامه را تایپ می‌کنیم. برای مثال \\server01\software . سپس پکیج Windows Installer را انتخاب می‌کنیم. مثلا XmlNotepad.msi و سپس روی Open کلیک می‌کنیم.

۹. در کادر محاوره‌ای Deploy Software ابتدا Advanced را انتخاب و سپس OK می‌کنیم.

۱۰. در زبانه General توجه کنید که نام پکیج شامل نسخه نیز می‌باشد مثلا XML Notepad 2007 .

۱۱. روی زبانه Deployment کلیک می‌کنیم.

۱۲. روی Assigned کلیک می‌کنیم

۱۳. کادر Install This Application At Logon را علامت می‌زنیم.

۱۴. گزینه Uninstall This Application When It Falls Out The Scope Of Management را انتخاب می‌کنیم.

۱۵. دکمه OK را کلیک می‌کنیم.

۱۶. GPME را می‌بندیم.

۱۷. در کنسول Group Policy Management در Group Policy container ، XML Notepad GPO را انتخاب می‌کنیم.

۱۸. زبانه Scope را باز می‌کنیم.

۱۹. در بخش Security Filtering ، Authenticated Users را انتخاب و Remove را کلیک می‌کنیم. برای تایید عملیات OK می‌کنیم.

۲۰. روی Add button کلیک می‌کنیم.

۲۱. نام گروهی را که نمایانگر کاربران و کامپیوترهایی است که برنامه باید روی آنها توزیع شود وارد می‌کنیم مثلا APP_XML Notepad.

۲۲. دکمه OK را کلیک می‌کنیم. حالا GPO برای اعمال روی فقط گروه APP_XML Notepad فیلتر شده است. بهرحال تنظیمات GPO اعمال نمی‌شود تا به OU لینک نشود.

۲۳. روی دامنه contoso.com کلیک راست کرده و Link An Existing GPO را انتخاب می‌کنیم.

۲۴. از لیست Group Policy Objects ، XML Notepad را انتخاب کرده و OK می‌کنیم. برای تست GPO

می‌توانیم کاربر Administrator را به گروه APP_XML Notepad اضافه کنیم. از ویندوز خارج و دوباره وارد می‌شویم. هنگام ورود XML Notepad نصب می‌شود.

تمرین۲ ارتقاء یک برنامه

در این تمرین قرار است توزیع نسخه جدید برنامه XML Notepad شبیه سازی شود.

۱. با کاربر Administrator به سرور SERVER01 وارد می‌شویم.

۲. کنسول GPMC را باز می‌کنیم.

۳. روی XML Notepad GPO در Group Policy Objects container کلیک راست کرده و Edit را انتخاب می‌کنیم.

۴. گره User Configuration\Policies\Software Settings را باز می‌کنیم.

۵. روی Software Installation کلیک راست کرده و New و بعد Package را انتخاب می‌کنیم.

۶. در کادر متنی File Name مسیر شبکه‌ای پوشه توزیع برنامه را وارد می‌کنیم مثلا . \\server01\software نام فایل msi. را انتخاب کرده و روی دکمه Open کلیک می‌کنیم. در این تمرین از فایل موجود XmlNotepad.msi به عنوان نسخه جدید XML Notepad استفاده می‌شود.

۷. روی دکمه Open کلیک می‌کنیم.

۸. در کادر محاوره‌ای Deploy Software گزینه Advanced و سپس OK را انتخاب می‌کنیم.

۹. در زبانه General نام پکیج را طوری عوض می‌کنیم که مشخص شود نسخه جدید برنامه است مثلا XML Notepad 2008 .

۱۰. زبانه Deployment را باز می‌کنیم.

۱۱. Assigned را انتخاب می‌کنیم.

۱۲. کادر Install This Application At Logon را علامت می‌زنیم.

۱۳. زبانه Upgrades را کلیک می‌کنیم.

۱۴. دکمه Add را کلیک می‌کنیم.

۱۵. گزینه Current Group Policy Object (GPO) را انتخاب می‌کنیم.

۱۶. در لیست Package To Upgrade پکیج قدیمی را مثلا XML Notepad 2007 انتخاب می‌کنیم.

۱۷. Uninstall The Existing Package و سپس Then Install The Upgrade Package را انتخاب می‌کنیم.

۱۸. روی دکمه OK کلیک می‌کنیم.

۱۹. دوباره روی OK کلیک می‌کنیم. اگر این واقعا ارتقاء واقعی باشد پکیج جدید نسخه قدیمی برنامه را همزمان با اعمال XML Notepad GPO روی کلاینت‌ها ارتقاء می‌دهد. چون این تنها شبیه‌سازی یک ارتقاء است می‌توانیم پکیج ارتقاء شبیه‌سازی شده را حذف کنیم.

۲۰. روی پکیجی که برای شبیه‌سازی ساختیم کلیک راست کرده و All Tasks و سپس Remove را انتخاب می‌کنیم.

۲۱. در کادر محاوره‌ای Remove Software گزینه Immediately Uninstall The Software From Users And Computers را انتخاب می‌کنیم.

۲۲. روی OK کلیک می‌کنیم.

خلاصه درس

- GPSI برای توزیع، نگهداری، ارتقاء و حذف نرم‌افزار قابل استفاده است.
- امکان assign کردن پکیج برنامه در بخش Computer Configuration از یک GPO وجود دارد. کلاینت‌های حوزه آن GPO هنگام بوت، برنامه را نصب خواهند کرد.
- امکان assign کردن پکیج برنامه در بخش User Configuration از یک GPO وجود دارد. هنگامی که کاربر میانبر برنامه را از منوی استارت اجرا می‌کند یا فایلی را که با این برنامه associate شده اجرا می‌کند برنامه شروع به نصب می‌کند. به جای آن می‌توانیم. در صورت نیاز می‌توانیم برنامه را به کاربر assign کنیم تا برنامه در هنگام ورود کاربر به سیستم عامل نصب شود..
- امکان publish کردن نرم‌افزار در بخش User Configuration مربوط به GPO وجود دارد. در این حالت برنامه خود را در Programs And Features در کنترل پنل (ویندوز سرور 2008 و ویستا) یا Add/Remove Programs (در ویندوز XP) نشان می‌دهد.
- فایل‌های Transform با پسوند .mst برای تغییر رفتار پکیج Windows Installer که با GPSI توزیع شده به کار می‌رود.
- برنامه‌هایی که با استفاده از GPSI مدیریت می‌شوند قابلیت توزیع دوباره یا حذف توسط extension نصب نرم‌افزار را دارند.
- یک پکیج نرم‌افزار می‌تواند به منظور ارتقاء برنامه‌های دیگر که با GPSI توزیع شده‌اند به کار رود.
- تنظیمات GPSI هنگامی که لینک ارتباطی ضعیف باشد اعمال نمی‌شود.

سئوالات پایان درس

۱. می‌خواهیم برنامه‌ای را توسط Group Policy روی کلاینت‌های شعبات شرکت توزیع کنیم. دفتر مرکزی شرکت با یک

لینک WAN با پهنای باند 364kbps به شعبات متصل می‌باشد. برای نصب نرم‌افزار چه مراحلی را باید انجام دهیم؟(دو تا از گزینه‌ها صحیح هستند. هر گزینه صحیح بخشی از جواب می‌باشد)

A. یک GPO می‌سازیم که به همه کامپیوترها در شعبات و مرکز اعمال شود. در GPO در گره User Configuration پکیج نرم‌افزاری را می‌سازیم که برنامه را assign می‌کند.

B. یک GPO می‌سازیم که به همه کامپیوترها در شعبات و مرکز اعمال شود. در GPO در گره Computer Configuration پکیج نرم‌افزاری را می‌سازیم که برنامه را assign می‌کند.

C. در یک GPO که به همه کامپیوترها اعمال می‌شود policy تشخیص لینک ضعیف را در گره User Configuration به 256 kbps تغییر می‌دهیم.

D. در یک GPO که به همه کامپیوترها در مرکز اعمال می‌شود policy تشخیص لینک ضعیف را در گره Computer Configuration به 256 kbps تغییر می‌دهیم.

E. در یک GPO که به همه کامپیوترهای مرکز اعمال می‌شود policy تشخیص لینک ضعیف را در گره Computer Configuration به 1000 kbps تغییر می‌دهیم.

۲. در دامنه ما همه کاربران عضو Employees OU می‌باشند. هر سایت یک OU دارد که در آن Sales OU اشیاء کامپیوترها را در بخش Sales از همان سایت در بر می‌گیرد. می‌خواهیم برنامه‌ای را طوری توزیع کنیم که برای همه کاربران بخش‌های Sales سازمان در دسترس باشد. از کدام روش باید استفاده کنیم؟ (در صورت صحیح بودن همه را انتخاب کنید)

A. یک GPO برای لینک به دامنه می‌سازیم. گروهی را شامل همه کاربران Sales می‌سازیم. GPO را فیلتر می‌کنیم طوری که فقط به گروه اعمال شود. در User Configuration policy مربوط به GPO پکیج نرم‌افزاری می‌سازیم که برنامه را assign کند.

B. یک GPO ساخته و به Sales OU هر سایت لینک می‌کنیم. در تنظیمات User Configuration مربوط به GPO پکیج نرم‌افزاری که برنامه را assign کند می‌سازیم.

C. یک GPO برای لینک به دامنه می‌سازیم. گروهی را شامل همه کاربران Sales می‌سازیم. GPO را فیلتر می‌کنیم طوری که فقط به گروه اعمال شود. در Computer Configuration policy مربوط به GPO پکیج نرم‌افزاری می‌سازیم که برنامه را assign کند.

D. یک GPO ساخته و به Sales OU هر سایت لینک می‌کنیم. در تنظیمات User Configuration مربوط به GPO پکیج نرم‌افزاری که برنامه را assign کند می‌سازیم. در Computer Configuration مربوط به GPO گزینه loopback policy processing را در حالت merge فعال می‌کنیم.

۳. سازمان ما از ده شعبه تشکیل شده است. در Active Directory یک OU با نام Employees به ده OU فرزند شامل کاربران هر شعبه تقسیم می‌شود. می‌خواهیم یک برنامه را به کاربران چهار شعبه توزیع کنیم. برنامه باید قبل از اینکه کاربر برای اولین بار برنامه را اجرا کند به طور کامل نصب شده باشد. چه کاری باید انجام شود؟ (چهار گزینه را انتخاب کنید. هر

گزینه صحیح بخشی از جواب می‌باشد.)

A. یک GPO توزیع نرم‌افزار ساخته و به Employees OU لینک می‌کنیم.

B. یک پکیج در تنظیمات User Configuration می‌سازیم تا برنامه را publish کند.

C. گزینه Install This Application At Logon را انتخاب می‌کنیم.

D. یک گروه سایه می‌سازیم که شامل کاربران چهار شعبه باشد. GPO توزیع نرم‌افزار را طوری فیلتر می‌کنیم که فقط روی گروه سایه اعمال شود.

E. یک پکیج در تنظیمات User Configuration می‌سازیم که برنامه را assign کند.

F. گزینه Required Upgrade For Existing Packages را انتخاب می‌کنیم.

درس ۴: ممیزی

ممیزی جزء مهم امنیت به شمار می‌آید. ممیزی فعالیت‌های مشخصی را در شبکه در Windows Security log ثبت می‌کند که بعدا می‌توانیم آنها را مانیتور کنیم تا روی برخی موضوعات بیشتر تمرکز کنیم. ممیزی دسترسی‌های مجاز را ثبت می‌کنند تا تغییرات را مستند کند. همچنین دسترسی‌های ناموفق و تلاش برای نفوذ را ثبت می‌کند. ممیزی دارای سه ابزار مدیریتی است: سیاست‌های ممیزی، تنظیمات ممیزی روی اشیاء و ثبت وقایع امنیتی. دراین درس یاد می‌گیریم چطور ممیزی را در سناریوهای متعدد پیکربندی کنیم.

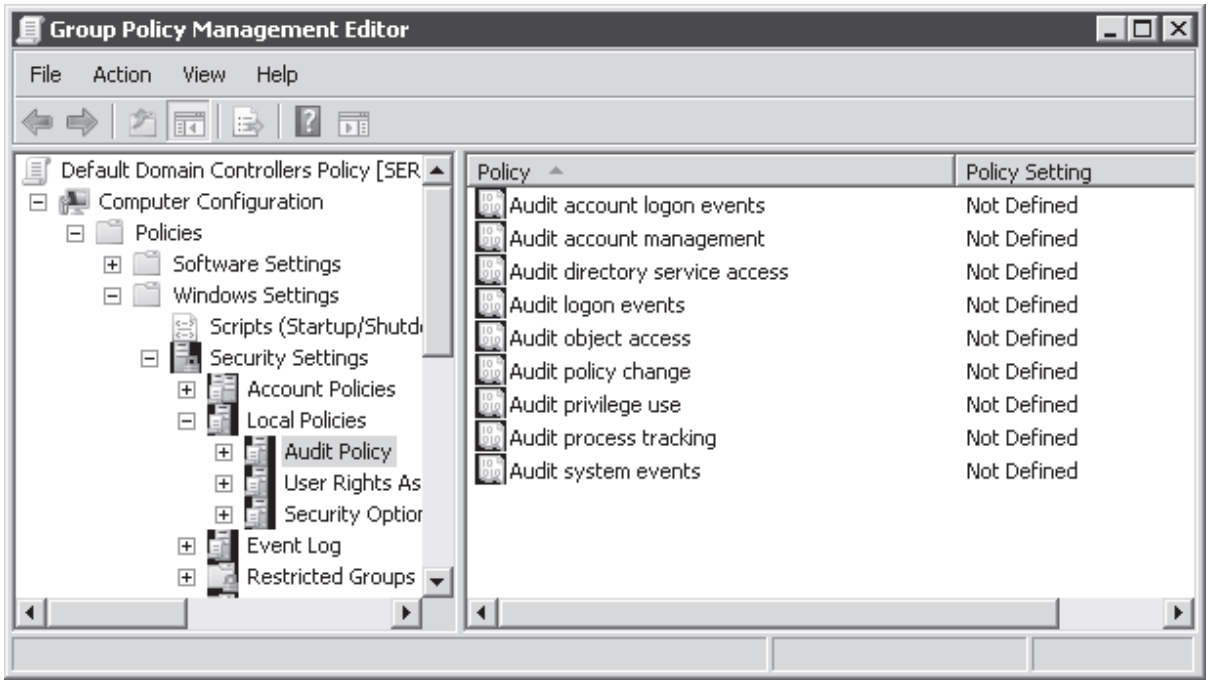
بعد از این درس می‌توانیم:

- سیاست ممیزی را پیکربندی کنیم.
- تنظیمات ممیزی را روی فایل سیستم و اشیاء سرویس دایرکتوری پیکربندی کنیم.
- ممیزی جدید Directory Service Changes را در ویندوز سرور 2008 پیاده‌سازی کنیم.
- وقایع امنیتی ثبت شده را توسط ابزار Event Viewer مشاهده کنیم.

زمان تقریبی: ۴۵ دقیقه

سیاست ممیزی

سیاست ممیزی (Audit Policy) سیستم را جهت ممیزی گروهی از فعالیت‌ها می‌تواند پیکربندی کند. اگر این سیاست فعال نباشد فعالیت‌ها ثبت نمی‌شوند. شکل ۱۴- ۷ گره Audit Policy را در یک GPO نشان می‌دهد.



شکل ۱۴- ۷ گره Audit Policy از یک GPO

برای پیکربندی ممیزی باید تنظیمات سیاست را تعریف کنیم. روی هر یک از تنظیمات دوبار کلیک می‌کنیم و کادر Define These Policy Settings را علامت می‌زنیم. سپس ممیزی را برای دسترسی‌های موفق، ناموفق و یا هردو فعال می‌کنیم. جدول ۲- ۷ همه سیاست‌های ممیزی و تنظیمات پیش فرض آنرا روی یک DC با ویندوز سرور 2008 شرح می‌دهد.

جدول ۲- ۷ سیاست‌های ممیزی

تنظیم سیاست ممیزی	شرح	تنظیم پیش فرض برای DC با ویندوز سرور 2008
Audit Account Logon Events	وقتی کاربر یا کامپیوتر برای ورود و تاییدهویت توسط Active Directory تلاش می‌کند ثبت می‌شود. مثلا وقتی یک کاربر به هر کامپیوتری در دامنه وارد می‌شود واقعه ثبت می‌شود.	ورود موفق و ناموفق حساب‌ها هر دو ثبت می‌گردد
Audit Logon Events	وقتی کاربری از روی خود سیستم یا از طریق شبکه به این کامپیوتر وارد می‌شود واقعه ثبت می‌شود. برای مثال اگر یک کلاینت و یک سرور از نظر ثبت ورود کاربران پیکربندی شوند کلاینت ورود مستقیم کاربر را به سیستم ثبت می‌کند. وقتی کاربری به پوشه اشتراکی روی سرور متصل می‌شود سرور اتصال از راه دور را ثبت می‌کند. وقتی کاربری به سیستم وارد می‌شود DC واقعه را ثبت می‌کند چون اسکریپت‌های logon و سیاست‌ها از این سرور دریافت می‌شوند.	ورود موفق و ناموفق هر دو ثبت می‌گردد
Audit Account Management	وقایعی نظیر ساخت ، حذف یا تغییر حساب کاربر، گروه یا کامپیوتر و reset کلمه عبور کاربر را ثبت می‌کند	وقایع موفق مدیریت حساب ثبت می‌شود
Audit Directory Service Access	وقایعی را که در SACL سیستم تعریف شده ثبت می‌کند که در کادر محاوره‌ای Advanced Security Settings شیء Active Properties	وقایع موفق دسترسی به سرویس دایرکتوری ثبت می‌شود ولی SACL اشیاء محدودی این

	Directory دیده می‌شود. علاوه بر تعریف سیاست ممیزی با این تنظیم همچنین می‌توان شیء یا اشیاء خاصی را با استفاده از SACL شیء یا اشیاء ممیزی کرد. این سیاست شبیه سیاست Audit Object Access می‌باشد که برای ممیزی فایل و پوشه استفاده می‌شود ولی این سیاست روی اشیاء Active Directory اعمال می‌شود.	تنظیم را دارند. برای اطلاعات بیشتر به بخش " Auditing Directory Services Changes" مراجعه کنید.
Audit Policy Change	تغییرات اعمال شده روی سیاست‌های حقوق کاربری، سیاست‌های ممیزی یا سیاست‌های trust را ثبت می‌کند.	تغییر سیاست‌ها را ثبت می‌کند
Audit Privilege Use	استفاده از حقوق کاربری را ثبت می‌کند. متن توضیحی این سیاست را در GPME مشاهده کنید.	هیچ ممیزی فعال نیست
Audit System Events	بوت مجدد، خاموش شدن یا تغییراتی که روی log امنیتی یا سیستم تاثیر می‌گذارد ثبت می‌کند.	وقایع سیستمی موفق و ناموفق هردو ثبت می‌شود
Audit Process Tracking	وقایعی نظیر فعال‌سازی برنامه و خروج از پردازه سیستم عامل را ثبت می‌کند. متن توضیحی برای این سیاست را در GPME مشاهده کنید.	وقایع موفق مربوط به پردازه‌های سیستم عامل را ثبت می‌کند.
Audit Object Access	دسترسی به اشیائی نظیر فایل‌ها، پوشه‌ها، کلیدهای رجیستری و پرینترها را که SACL خود را دارند ثبت می‌کند. علاوه بر فعال کردن این سیاست باید در SACL مربوط به شیء ممیزی را پیکربندی کنیم.	دسترسی موفق به اشیاء را ثبت می‌کند.

نکته امتحانی امتحانات مایکروسافت اغلب دانش ما را در سیاست‌های ممیزی در سطح بالا تست می‌کند. در صورت حفظ اطلاعات این جدول به این سئوالات می‌توانیم پاسخ دهیم.

همان‌طوری که می‌بینیم اهم وقایع Active Directory با فرض اینکه وقایع موفق هستند توسط DC ها ثبت می‌شود. بنابراین ساخت کاربر، ریست کردن کلمه عبور کاربر، ورود به دامنه و دریافت اسکریپت logon توسط کاربر همه ثبت می‌گردد.

ولی به طور پیش فرض همه وقایع ناموفق ثبت نمی‌شود و ما باید بر اساس سیاست‌های سازمان و نیاز خود سیاست‌های ممیزی ناموفق اضافی را پیاده‌سازی کنیم. برای مثال ثبت وقایع ورود ناموفق تلاش هکر برای ورود به دامنه با تکرار ورود کلمه عبور اشتباه را آشکار می‌کند. ثبت وقایع ناموفق مدیریت حساب مشخص می‌کند که کسی قصد دستکاری عضویت یک گروه حساس امنیتی را داشته است.

یکی از مهم‌ترین وظایفی که ما باید انجام دهیم متعادل و یکسوکردن سیاست ممیزی با سیاست‌های سازمان است. سیاست سازمان ممکن است بیان کند همه ورودهای ناموفق و تغییرات موفق در کاربران و گروههای Active Directory ثبت شود. دسترسی به این گزارشات ساده است ولی چطور باید از این اطلاعات استفاده کرد؟ اگر ندانیم و یا ابزار مناسب برای مدیریت گزارشات نداشته باشیم گزارشات طول و دراز غیرقابل استفاده هستند. برای پیاده‌سازی ممیزی باید نیازی وجود داشته باشد سیاست ممیزی مناسب پیکربندی شود و ابزارهایی داشته باشیم تا اطلاعات خروجی را مدیریت کنیم.

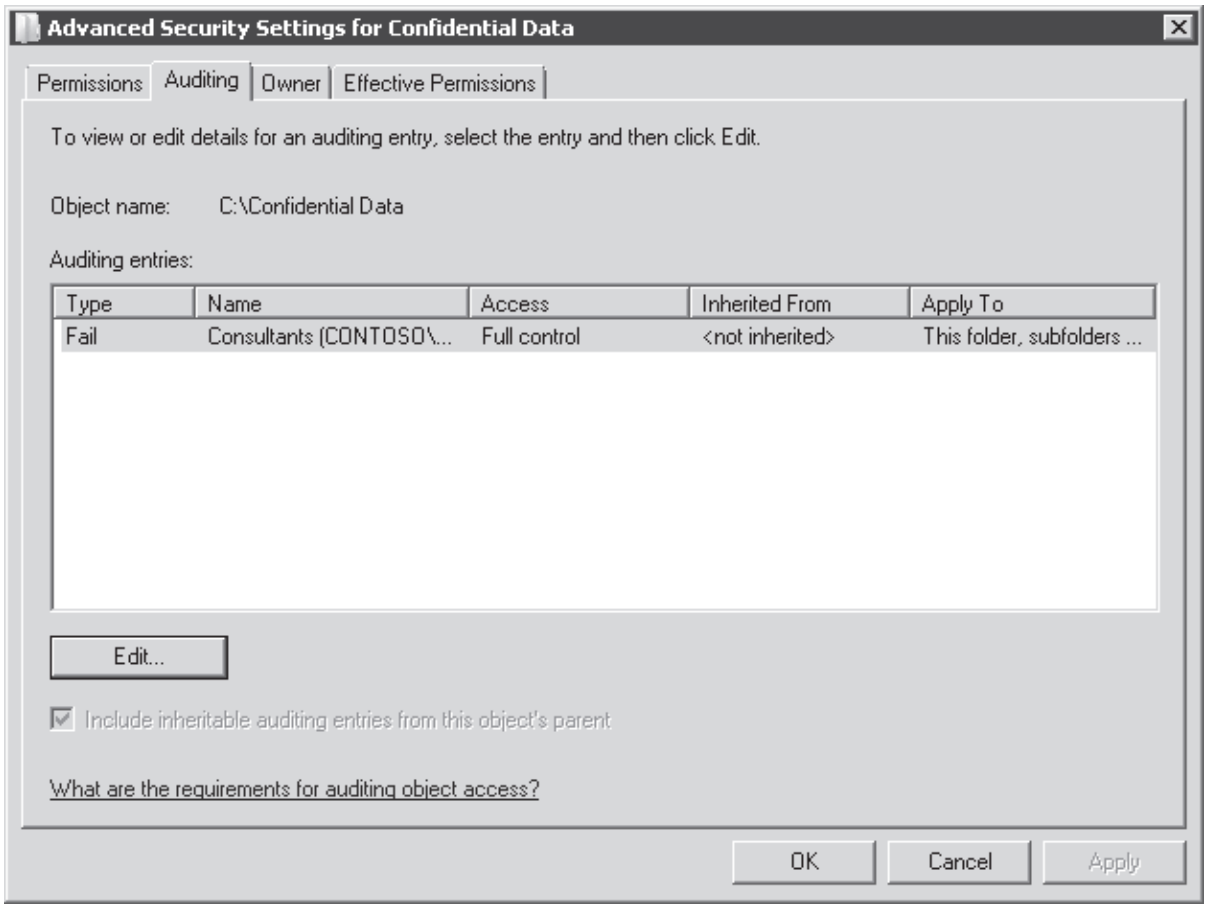
ممیزی دسترسی به فایل‌ها و پوشه‌ها

بسیاری از سازمان‌ها وقایع دسترسی به فایل را ثبت می‌کنند تا مسائل امنیتی بالقوه را کنترل کنند. ویندوز سرور 2008 از ممیزی جزئی بر اساس کاربر یا گروه و عملیات مشخص اجرا شده توسط این حساب‌ها پشتیبانی می‌کند. برای پیکربندی ممیزی باید سه کار انجام شود: مشخص کردن تنظیمات ممیزی، فعال کردن سیاست ممیزی و ارزیابی وقایع در log امنیتی.

تعیین تنظیمات ممیزی روی یک فایل یا پوشه

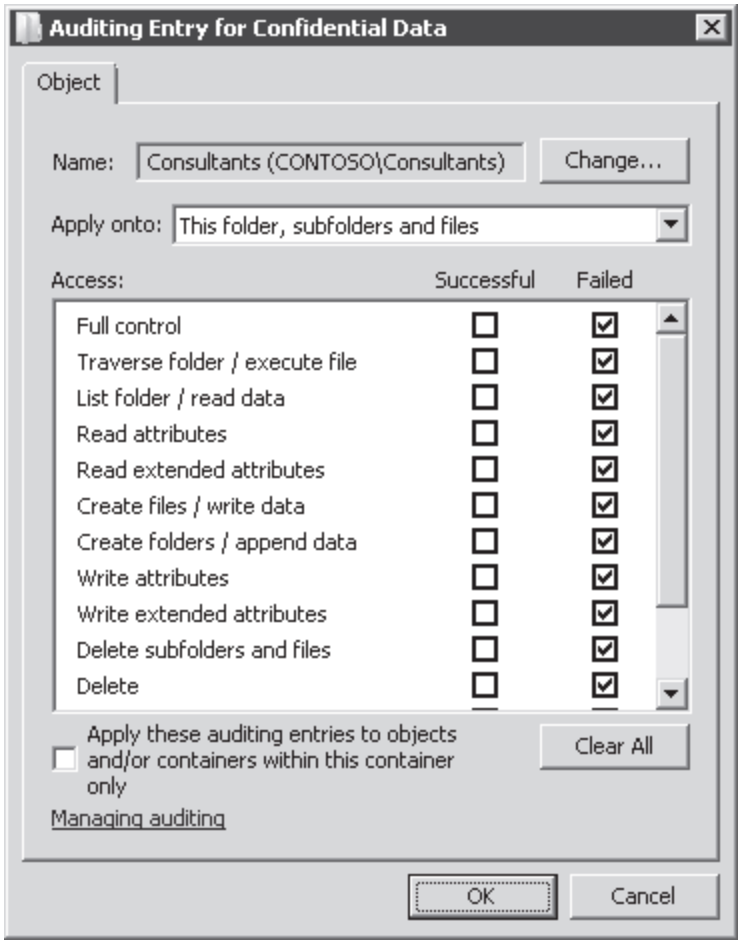
با افزودن entry به SACL می‌توانیم دسترسی به فایل و پوشه را ثبت کنیم. برای دسترسی به SACL و entry های آن کادر محاوره‌ای Properties را باز کرده و زبانه Security را کلیک می‌کنیم. سپس روی دکمه Advanced کلیک کرده و زبانه

Auditing را باز می‌کنیم. کادر محاوره‌ای Advanced Security Settings مربوط به پوشه Confidential Data در شکل ۱۵- ۷ نشان داده شده است.



شکل ۱۵- ۷ کادر محاوره‌ای Advanced Security Settings مربوط به پوشه Confidential Data

برای افزودن یک entry روی دکمه Edit کلیک می‌کنیم تا زبانه Auditing در حالت Edit باز شوند. روی دکمه Add کلیک می‌کنیم و کاربر، گروه یا کامپیوتر را برای ممیزی انتخاب می‌کنیم. سپس در کادر محاوره‌ای Auditing Entry همانطوریکه در شکل ۱۶- ۷ نشان داده شده نوع دسترسی را برای ممیزی مشخص می‌کنیم.



شکل ۱۶- ۷ کادر محاوره‌ای Auditing Entry

ما می‌توانیم وقایع موفق، ناموفق یا هردو را برای کاربر، گروه یا کامپیوتر مشخصی که برای دسترسی به منابع مشخصی تلاش می‌کند توسط یک یا چند سطح دسترسی جزئی ثبت کنیم.

وقایع موفق با اهداف زیر ثبت می‌شود:

- ثبت دسترسی به منابع برای گزارش گیری و یا تهیه صورت‌حساب
- برای مانیتور کردن دسترسی کاربرانی که بیش از نیازشان مجوز دارند و نشان‌دهنده اینست که مجوزها درست پیکربندی نشده‌اند.
- برای تشخیص دسترسی‌هایی که غیر مجاز می‌باشد.

ثبت وقایع ناموفق ما را قادر می‌سازد:

- تلاش‌های مشکوک برای دسترسی به منابعی را که در دسترس نیستند مانیتور کنیم
- تلاش‌های ناموفق برای دسترسی به یک فایل یا پوشه را که کاربر به آن نیاز دارد تشخیص دهیم. این مسئله مشخص می‌کند مجوزهای تعیین شده بر اساس نیازهای سازمان تعریف نشده‌اند.

مثال شکل ۱۵- ۷ تلاش‌های ناموفق کاربران گروه Consultants را برای دسترسی به داده پوشه Confidential Data در هر سطحی ثبت می‌کند. این کار با افزودن یک entry ممیزی برای دسترسی Full Control انجام می‌شود. دسترسی Full Control شامل همه سطوح دسترسی می‌شود بنابراین این entry همه انواع دسترسی را پوشش می‌دهد. اگر یکی از اعضاء گروه Consultant به هر شکل برای دسترسی تلاش ناموفق داشته باشد واقعه ثبت می‌شود.

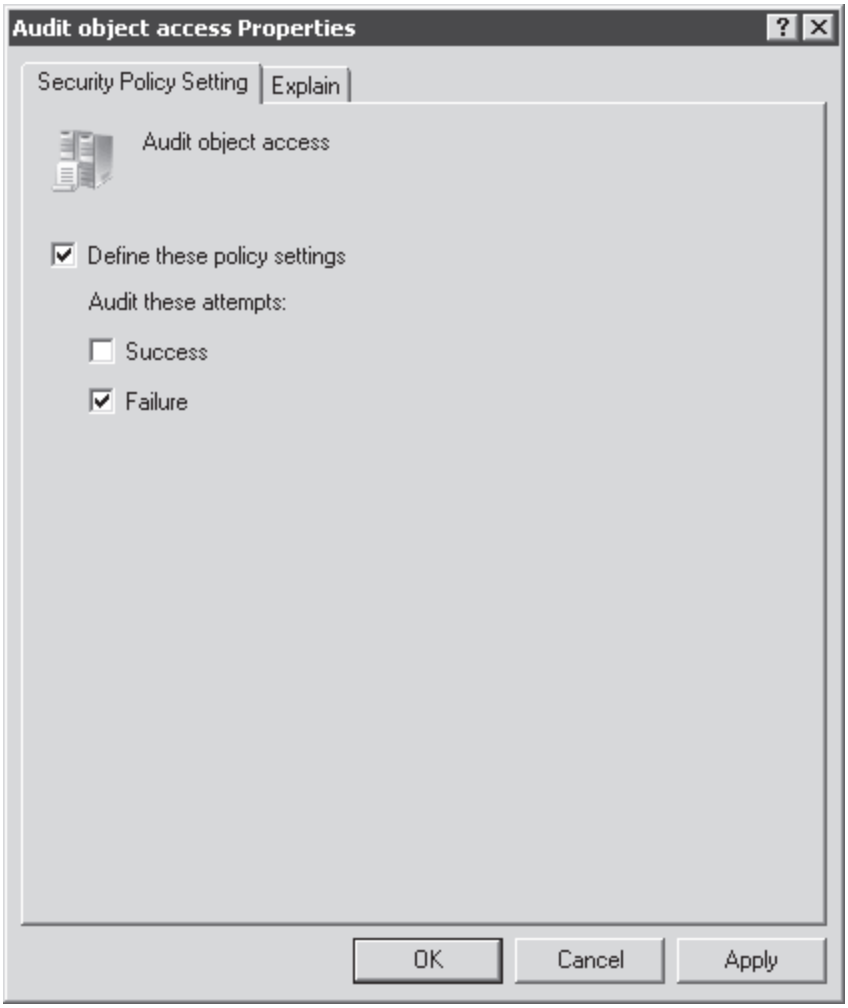
Entry های ممیزی منعکس کننده entry های شیء می‌باشد. به بیان دیگر پوشه Confidential Data طوری پیکربندی شده که از دسترسی گروه Consultants به محتویات آن جلوگیری می‌کند. سپس ما باید از ممیزی برای مانیتور کردن اعضاء این گروه که با این وجود برای دسترسی به این پوشه تلاش کرده‌اند استفاده کنیم. به خاطر داشته باشید که اعضاء این گروه ممکن است از طریق عضویت در گروه دیگری توانایی دسترسی به این منابع را به دست آورند. بدین ترتیب چون دسترسی موفق می‌باشد گزارشی ثبت نمی‌شود. بنابراین اگر دغدغه عدم دسترسی کاربران به یک پوشه را داریم باید تلاش‌های ناموفق دسترسی را مانیتور کنیم و دسترسی‌های موفق را به منظور پیدا کردن کاربرانی که از طریق گروههای دیگر به این منابع دسترسی پیدا کرده‌اند ثبت کنیم.

نکته از ممیزی بیش از حد استفاده نکنید

به دلیل اینکه ممیزی باعث افت کارایی سیستم می‌شود بهتر است تا حد ممکن از حداقل ممیزی مورد نیاز استفاده کنیم. تعیین ممیزی برای ثبت وقایع موفق و ناموفق روی یک پوشه فعال برای گروه Everyone با مجوز Full Control (همه مجوزها) گزارش بسیار طولانی ایجاد کرده و باعث افت کارایی سیستم می‌گردد.

فعال کردن سیاست ممیزی

پیکربندی entry های ممیزی در بخش امنیتی فایل و پوشه به تنهایی کافی نیست. همان‌طوری که در شکل ۱۷- ۷ نشان داده شده است ممیزی باید توسط تنظیم Audit Object Access فعال شود. پس از فعال کردن ممیزی زیرسیستم امنیتی طبق تنظیمات ممیزی شروع به ثبت وقایع می‌کند.



شکل ۱۷- ۷ تنظیم Audit Object Access

تنظیم باید به سروری که دارای شیء مورد ممیزی می‌باشد اعمال شود. هم امکان پیکربندی تنظیم در GPO محلی سرور وجود دارد و هم GPO ای که سرور در حوزه آن قرار دارد.

سپس ما می‌توانیم ممیزی را بر حسب وقایع Success ، Failure و یا هردو تعریف کنیم. تنظیم (شکل ۱۷- ۷) باید مشخص

کننده ممیزی وقایع Success یا Failure باشد. برای مثال برای ثبت تلاش ناموفق توسط یکی از اعضاء گروه Consultants برای دسترسی به پوشه Confidential Data باید تنظیم Audit Object Access را برای ممیزی وقایع ناموفق پیکربندی کنیم و SACL پوشه Confidential Data را برای ثبت وقایع ناموفق پیکربندی کنیم. اگر تنظیم فقط وقایع موفق را ثبت کند هیچ ثبتی برای وقایع ناموفق اتفاق نخواهد افتاد.

نکته Audit Policy باید با entry های ممیزی اشیاء همخوانی داشته باشد

به خاطر داشته باشید دسترسی‌هایی که ممیزی می‌شود ترکیبی از entry های ممیزی فایل‌ها یا پوشه‌های مشخص و تنظیمات Audit Policy هستند. اگر entry های ممیزی بر حسب وقایع ناموفق پیکربندی شده باشند و در تنظیم سیاست ممیزی فقط وقایع موفق مشخص شده باشد هیچ ثبتی انجام نمی‌شود.

ارزیابی وقایع در Log امنیتی

ما می‌توانیم نتیجه وقایع را در log امنیتی سرور مشاهده کنیم. کنسول Event Viewer از Administrative Tools را باز می‌کنیم و گره Windows Logs\Security را باز می‌کنیم. محل log اینجاست.

ممیزی تغییرات سرویس دایرکتوری

همانگونه که سیاست Audit Object Access تلاش‌های دسترسی به اشیائی نظیر فایل‌ها و پوشه‌ها را ثبت می‌کند سیاست Audit Directory Service Access ما را قادر می‌سازد تلاش‌های دسترسی به اشیاء در Active Directory را ثبت کنیم. همان قواعد اینجا هم پابرجاست. تنظیم را برای ثبت وقایع موفق و ناموفق پیکربندی می‌کنیم. سپس SACL مربوط به شیء Active Directory را به منظور تعیین انواع دسترسی مورد نظر پیکربندی می‌کنیم.

به عنوان مثال اگر بخواهیم تغییرات عضویت یک گروه حساس امنیتی نظیر Domain Admins را مانیتور کنیم باید تنظیم Audit Directory Service Access را برای ثبت وقایع موفق فعال کنیم. سپس می‌توانیم SACL گروه Domain Admins را باز کرده و یک entry ممیزی برای تغییرات موفق خصوصیت member گروه پیکربندی کنیم. ما این کار را در تمرینات همین درس انجام می‌دهیم.

در ویندوز سرور 2003 و 2000 می‌توانیم دسترسی به سرویس دایرکتوری را ممیزی کرده و متوجه تغییرات یک شیء یا خصوصیات آن شویم ولی نمی‌توانیم مقادیر قدیمی و جدید آن را ببینیم. برای مثال واقعه‌ای مشخص می‌کند که یک کاربر خاص خصلت member گروه Domain Admins را تغییر داده ولی نمی‌توانیم بفهمیم چه چیزی تغییر کرده است.

ویندوز سرور 2008 یک دسته خاص از ممیزی را به نام Directory Service Changes اضافه کرده است. تفاوت مهم Directory Service Changes و Directory Service Access این است که با ممیزی Directory Service Changes می‌توانیم مقدار فعلی و قبلی خصیصه تغییر یافته را ببینیم.

Directiry Service Changes در ویندوز سرور 2008 به طور پیش فرض فعال نیست. در عوض Directory Service Access برای پشتیبانی از ممیزی نسخه‌های قدیمی ویندوز فعال است.

برای فعال کردن ممیزی روی تغییرات موفق Directory Service Changes پنجره خط فرمان را در یک سرور DC باز کرده و دستور زیر را تایپ کنید:

```
Auditpol /set /subcategory:"directory service changes" /success:enable
```

نکته امتحانی دستور auditpol برای فعال کردن ممیزی Directory service changes به کار می‌رود.

ولی این کافی نیست و ما باید SACL شیء را تغییر دهیم تا مشخص شود کدام خصیصه یا خصیصه‌ها باید ممیزی شود. اگرچه در آزمایشگاه از این دستور برای ثبت تغییرات استفاده می‌کنیم ولی انجام این کار در محیط دامنه واقعی توصیه نمی‌شود حداقل تا خواندن مستندات این دستور در آدرس زیر:

http://technet2.microsoft.com/windowsserver2008/en/library/a9c25483-89e2-4202-881c-ea8e02b4b2a51033.mspx.

وقتی ممیزی Directory Service Changes فعال است و SACL شیء نیز پیکربندی شده است گزارشات در Security Log به وضوح خصایص تغییر یافته و زمان وقوع را نشان می‌دهد. در بیشتر موارد entry ها مقادیر فعلی و قبلی خصیصه را نمایش می‌دهند.

تمرینات ممیزی

در این تمرینات قرار است تنیظمات ممیزی پیکربندی شود، تنظیمات ممیزی برای دسترسی به شیء فعال شود و وقایع مشخصی در Security Log فیلتر شود. هدف مانیتور کردن یک پوشه محتوی دادهست که باید توسط کاربران گروه Consultants استفاده شود. همچنین ممیزی تغییرات عضویت گروه Domian Admins را پیکربندی می‌کنیم. برای انجام این تمرینات باید :

- پوشه‌ای با نام Confidential Data در درایو C بسازیم.
- یک گروه امنیتی global با نام Consultants بسازیم.
- گروه Consultants را به عضویت گروه Print Operators در می‌آوریم. این کار میانبری است که به کاربر گروه Consultants اجازه می‌دهد به سرور SERVER01 که در این تمرین DC است وارد شوند.
- کاربری با نام James Fine ایجاد کرده و به گروه Consultants اضافه می‌کنیم.

تمرین ۱ پیکربندی مجوزها و تنظیمات ممیزی

در این تمرین مجوزهای پوشه Confidential Data پیکربندی می‌کنیم تا از دسترسی گروه Consulatants به پوشه جلوگیری شود. سپس ممیزی فعال می‌شود تا تلاش‌های گروه مذکور برای دسترسی به پوشه ثبت شود.

۱. با کاربر Administrator به سرور SERVER01 وارد می‌شویم.
۲. پنجره properties پوشه C:\Confidential Data را باز کرده و زبانه Security را کلیک می‌کنیم.
۳. روی دکمه Edit کلیک می‌کنیم.
۴. روی دکمه Add کلیک می‌کنیم.
۵. تایپ می‌کنیم Consultants و OK می‌کنیم.
۶. کادر Deny برای مجوز Full Control را علامت می‌زنیم.
۷. روی Apply کلیک می‌کنیم.
۸. روی OK کلیک می‌کنیم تا کادر محاوره‌ای Permissions بسته شود.
۹. روی Advanced کلیک می‌کنیم.
۱۰. زبانه Auditing را کلیک می‌کنیم.
۱۱. روی Edit کلیک می‌کنیم.
۱۲. روی Add کلیک می‌کنیم.
۱۳. تایپ می‌کنیم Consultants و OK می‌کنیم.
۱۴. در کادر محاوره‌ای Auditing Entry کادر زیر Failed نزدیک Full Control را انتخاب می‌کنیم.

۱۵. روی دکمه OK کلیک کرده تا همه کادرها بسته شود.

تمرین ۲ فعال کردن Audit Policy

چون SERVER01 یک DC است برای فعال کردن ممیزی از Domain Controller Security Policy GPO استفاده می‌کنیم. روی یک سرور standalone باید ممیزی را با استفاده از Local Security Policy یا یک GPO که سرور در حوزه آن قرار دارد فعال کنیم.

۱. کنسول Group Policy Management را باز کرده و Group Policy Objects container را انتخاب می‌کنیم.

۲. روی Domain Controller Security Policy کلیک راست کرده و Edit را انتخاب می‌کنیم.

۳. گره Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy را باز می‌کنیم.

۴. روی Audit Object Access دوبار کلیک می‌کنیم.

۵. Define These Policy Settings را انتخاب می‌کنیم.

۶. کادر Failure را علامت می‌زنیم.

۷. روی دکمه OK کلیک می‌کنیم و کنسول را می‌بندیم.

۸. برای به روز رسانی policy و اطمینان از اعمال تغییرات در خط فرمان دستور gpupdate را تایپ می‌کنیم.

تمرین ۳ ساخت Audit Events

حالا باید به عنوان یکی از اعضاء گروه Consultants برای دسترسی به پوشه Confidential Data تلاش کنیم.

۱. با کاربر James Fine به SERVER01 وارد می‌شویم.

۲. My Computer را باز کرده و به مسیر C:\Confidential Data وارد می‌شویم. سعی می‌کنیم پوشه را باز کنیم.

۳. یک فایل متنی روی دسک‌تاپ ایجاد کرده و سعی می‌کنیم آنرا به پوشه کپی کنیم.

تمرین ۴ تست Security Log

حالا می‌توانیم تلاش‌های کاربر را برای دسترسی به پوشه ببینیم .

۱. با کاربر Administrator به SERVER01 وارد می‌شویم.

۲. کنسول Event Viewer را از پوشه Administrative Tools باز می‌کنیم.

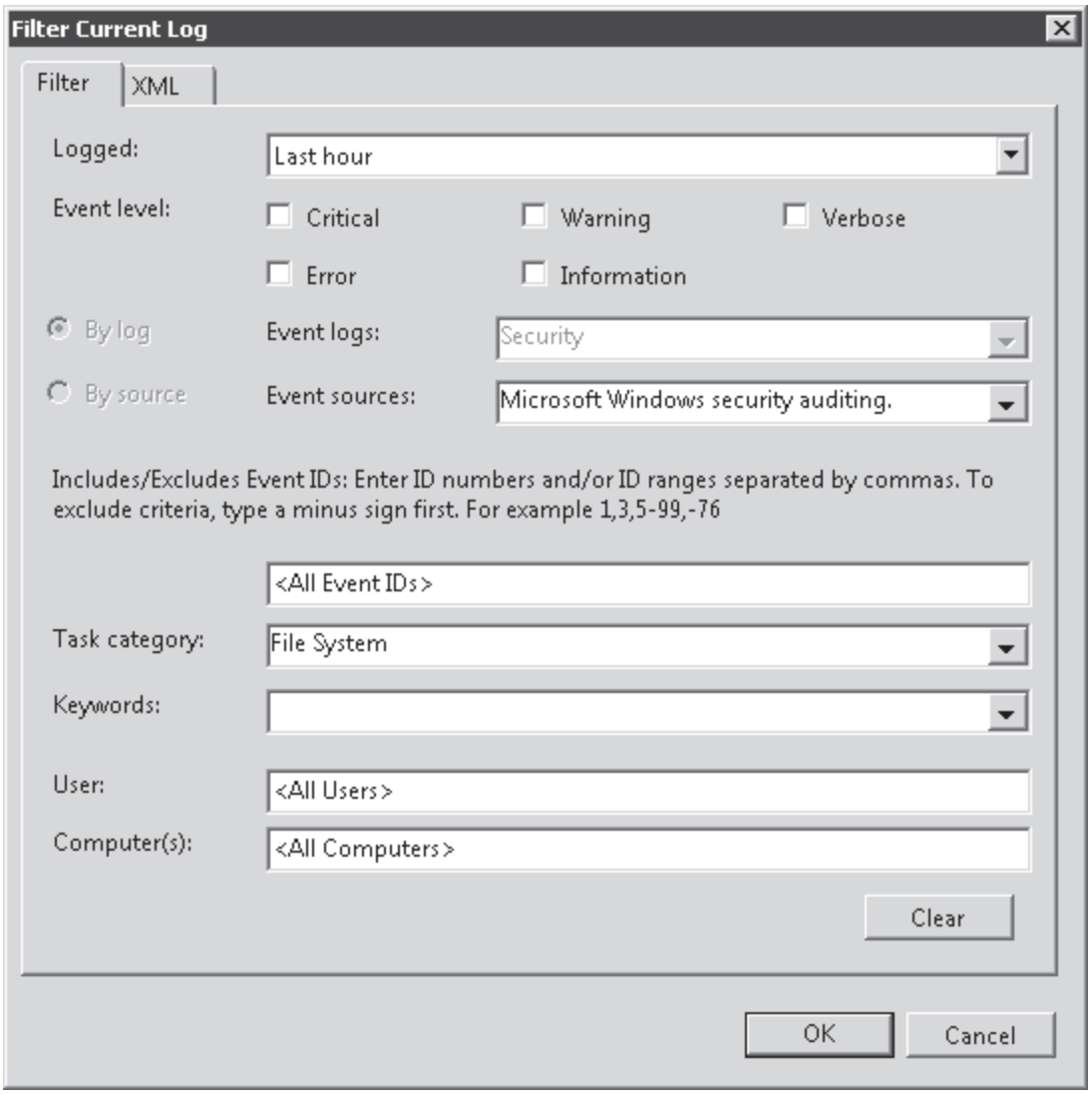
۳. گره Windows Logs\Security را باز می‌کنیم.

۴. چه وقایعی را در اینجا می‌توان یافت؟ به خاطر داشته باشید سیاست‌ها می‌توانند ممیزی را برای وقایع امنیتی بیشماری شامل دسترسی به اشیاء دایرکتوری، مدیریت حساب‌ها، ورود به ویندوز و غیره فعال کنند. توجه کنید منبع حوادث نشان داده شده در ستون Source ، Microsoft Windows security auditing می‌باشد.

۵. برای فیلتر کردن گزارش و محدود کردن جستجو روی لینک Filter Current Log در پنل راست کلیک می‌کنیم.

۶. فیلتر را طوری پیکربندی می‌کنیم که نتایج محدود شود. از واقعه مورد نظر خود چه می‌دانیم؟ ما می‌دانیم این واقعه در یک ساعت اخیر اتفاق افتاده است که منبع آن Microsoft Windows security auditing بوده و یک واقعه File System است.

۷. نتیجه کار را با مراجعه به شکل ۱۸- ۷ مرور می‌کنیم.



شکل ۱۸- ۷ فیلتر کردن Security Log برای وقایع اخیر File System

۸. روی OK کلیک می‌کنیم. اگر بخواهیم همه وقایع اتفاق افتاده روی یک پوشه را ببینیم باید فایل را به یک ابزار تحلیل log یا حتی یک فایل متنی منتقل کنیم.

۹. روی Save Filter Log File As Link در پنل راست کلیک می‌کنیم.

۱۰. در کادر محاوره‌ای Save As روی لینک Desktop در پنل Favorite Links کلیک می‌کنیم.

۱۱. روی لیست بازشوی Save As Type کلیک کرده و Text را انتخاب می‌کنیم.

۱۲. در کادر متنی File Name تایپ می‌کنیم Audit Log Export

۱۳. روی Save کلیک می‌کنیم.

۱۴. فایل متنی به دست آمده را در Notepad باز کرده و عبارت C:\Confidential Data را جستجو می‌کنیم.

تمرین ۵ استفاده از ممیزی تغییرات سرویس دایرکتوری

در این تمرین ممیزی Directory Service Access را می‌بینیم که به طور پیش فرض در ویندوز سرور 2008 و 2003 فعال است. سپس ممیزی جدید Directory Services Changes ویندوز سرور 2008 را پیاده‌سازی می‌کنیم تا تغییرات گروه Domain Admins را ببینیم.

۱. ابزار Active Directory Users And Computers را باز می‌کنیم.

۲. منوی View را باز کرده و Advanced Features را انتخاب می‌کنیم.

۳. Users container را انتخاب می‌کنیم.

۴. روی Domain Admins کلیک راست کرده و Properties را انتخاب می‌کنیم.

۵. زبانه Security را باز کرده و روی Advanced کلیک می‌کنیم.

۶. زبانه Auditing را باز کرده و روی Add کلیک می‌کنیم.

۷. تایپ می‌کنیم Everyone و OK می‌کنیم.

۸. در کادر محاوره‌ای Auditing Entry روی زبانه Properties کلیک می‌کنیم.

۹. کادر زیر Successful و نزدیک Write Members را علامت می‌زنیم.

۱۰. روی OK کلیک می‌کنیم.

۱۱. روی OK کلیک می‌کنیم تا کادر بسته شود. تا این جا تعیین کرده‌ایم هر تغییری در خصیصه member گروه Domain Admins به وجود بیاید ثبت شود. حالا دو تغییر در این عضویت این گروه ایجاد می‌کنیم.

۱۲. زبانه Members را باز می‌کنیم.

۱۳. کاربر James Fine را اضافه کرده و Apply را می‌زنیم.

۱۴. James Fine را انتخاب کرده، Remove و سپس Apply را کلیک می‌کنیم.

۱۵. روی OK کلیک می‌کنیم تا کادر محاوره‌ای Domain Admins Properties بسته شود.

۱۶. Security Log را باز کرده و وقایعی را که هنگام افزودن و حذف کاربر James Fine ایجاد شده پیدا می‌کنیم. Event ID مربوطه ۴۶۶۲ می‌باشد. اطلاعات زبانه General را مرور کنید. می‌توانیم تشخیص دهیم که یک کاربر (Administrator) به شیء (Domain Admins) دسترسی پیدا کرده و تغییری ایجاد کرده است. خود خصیصه به

عنوان یک GUID نمایش داده می‌شود. به راحتی نمی‌توان تشخیص داد که خصیصه member تغییر کرده است. همچنین جزئیات تغییر نیز نشان داده نمی‌شود. ما ممیزی Directory Service Changes را که یک ویژگی جدید در ویندوز سرور 2008 است فعال می‌کنیم.

۱۷. پنجره خط فرمان را باز کرده و تایپ می‌کنیم :

```
Auditpol /set /subcategory:"directory service changes" /success:enable
```

۱۸. پنجره properties مربوط به Domain Admins را باز کرده و کاربر James Fine را به گروه اضافه می‌کنیم.

۱۹. دوباره به ابزار Event viewer برگشته و Security Log را مشاهده می‌کنیم. ما باید هم واقعه Directory Service Access (شماره ۵۱۳۶) و هم Directory Service Changes (شماره ۵۱۳۶) را ببینیم. اگر واقعه Directory Service Changes را نمی‌بینیم باید چند لحظه صبر کنیم و پنجره را به روز آوری کنیم. ثبت وقایع سرویس دایرکتوری چند ثانیه طول می‌کشد.

۲۰. اطلاعات واقعه Directory Service Changes را مرور می‌کنیم. اطلاعات زبانهم General به وضوح نشان می‌دهند که یک کاربر (Admimistrator) روی یک شیء دایرکتوری (Domain Admins)تغییری ایجاد کرده است و آن تغییر افزودن کاربر James Fine به گروه است.

خلاصه درس

- سیاست‌های ممیزی تعیین می‌کند که وقایع موفق یا ناموفق ثبت گردد. تعدادی سیاست ممیزی مربوط به انواع مشخصی از فعالیت‌ها نظیر ورود به سیستم، دسترسی به شیء و تغییرات سرویس دایرکتوری وجود دارد.
- برای ممیزی دسترسی به فایل سیستم باید entry های ممیزی را به SACL فایل یا پوشه اضافه کنیم. همچنین باید تنظیم سیاست دسترسی به شیء را تعیین کرده و نتایج ممیزی را در Security Log ارزیابی کنیم.
- ویندوز سرور 2008 جزئیات بیشتری از ممیزی تغییرات اشیاء در Active Directory را نشان می‌دهد. ما می‌توانیم از دستور Auditpol.exe برای فعال کردن این ویژگی جدید بهره ببریم. خصیصه تغییر یافته نمایش داده می‌شود و به وضوح مشخص می‌کند چه نوع تغییری ایجاد شده و مقدار قبلی و جاری خصیصه را مشخص می‌کند.

سئوالات پایان درس

۱. کاربری تلاش می‌کند از طریق کاربر معتبر دامنه و کلمات عبور تصادفی به کامپیوترهای شبکه دسترسی پیدا کند. کدام نوع سیاست ممیزی باید پیکربندی شود؟

A. Logon Event failures
B. Derectory Service Access failures
C. Privilege Use successes
D. Account Logon Event failures
E. Account Management failures

۲. می‌خواهیم تغییرات خصیصه‌های حساب کاربری را که توسط مدیران شبکه استفاده می‌شود ثبت کنیم. وقتی تغییری اعمال می‌شود باید مقادیر قبلی و فعلی را ببینیم. چه کار باید انجام دهیم؟

A. سیاست ممیزی Account Management تعریف کنیم.

B. از دستور Auditpol.exe استفاده کنیم.

C. ممیزی Privilege Use را فعال کنیم.

D. سیاست ممیزی Directory Service Access را تعریف کنیم.

۳. سازمان شما دارای ۱۰ سرور فایل می‌باشد که هر کدام یک حساب کامپیوتری در Servers OU دامنه دارند. یک GPO با نام Server Configuration به این OU لینک شده است. روی پنج عدد از این سرورها پوشه‌ای با نام Confidential Data قرار دارد. شرکت گروهی مشاور برای یک پروژه استخدام کرده و شما می‌خواهید آنها به این پوشه دسترسی نداشته باشند. شما مجوزهای لازم را روی پوشه پیکربندی می‌کنید تا این دسترسی را ببندید و همچنین می‌خواهید هر تلاشی را برای دسترسی به این پوشه و دستکاری آن ثبت کنید. کدام از یک روشهای زیر راه حل این کار است؟ (سه جواب را انتخاب کنید. هر جواب بخشی از راه حل است)

A. Entry های ممیزی را به پوشه Confidential Data برای ممیزی دسترسی‌های موفق و حالت Full Control اضافه می‌کنیم.

B. Entry های Security log را روی DC ها ارزیابی می‌کنیم.

C. سیاست Audit Directory Access را در Server Configuration GPO تعریف می‌کنیم.

D. سیاست Audit Object Access را در Default Domain Controllers GPO تعریف می‌کنیم.

E. سیاست Audit Object Access را در Server Configuration GPO تعریف می‌کنیم.

F. Entry های Security log را روی هر سرور فایل ارزیابی می‌کنیم.

G. Entry های ممیزی را در پوشه Confidential Data به منظور ممیزی دسترسی ناموفق در حالت Full Control اضافه می‌کنیم.

فصل ۸

تایید هویت

وقتی کاربری به AD DS وارد می‌شود نام کاربری و کلمه عبور خود را وارد می‌کند و کلاینت از این اعتبار برای تایید هویت (Authentication) کاربر استفاده می‌کند. یعنی هویت کاربر را با توجه به حساب Active Directory ارزیابی می‌کند. در فصل ۳ یاد گرفتیم چطور حساب کاربری بسازیم و خصوصیات آن را از جمله کلمه عبور پیکربندی کنیم. در این فصل اجزاء سمت دامنه مربوط به پروسه تایید هویت را شامل سیاست‌هایی که نیازمندیهای کلمه عبور و ممیزی فعالیت‌های مرتبط با تایید هویت می‌باشد بررسی

می‌کنیم. همچنین دو گزینه جدید یعنی اشیاء تنظیمات کلمه عبور(password settings objects) یا (PSO) و DC های فقط خواندنی (read-only domain controllers)یا (RODC) تشریح می‌شود.

اهداف امتحانی در این فصل عبارت‌است از:

- ساخت و نگهداری اشیاء Active Directory
  - پیکربندی سیاست‌های حساب
  - پیکربندی سیاست ممیزی توسط GPO ها
- پیکربندی زیرساخت Active Directory
  - پیکربندی تکثیر Active Directory
- پیکربندی Additional Active Directory Server Roles
  - پیکربندی DC های فقط خواندنی (RODC)

دروس این فصل:

- درس ۱: پیکربندی سیاست‌های کلمه عبور و قفل کردن حساب
- درس ۲: ممیزی تایید هویت
- درس ۳: پیکربندی DC های فقط خواندنی

قبل از شروع

برای مطالعه این فصل باید یک DC با نام SERVER01 در دامنه contoso.com نصب کرده باشیم.

دنیای واقعی

دن هلم

هنگام پیاده‌سازی AD DS باید بین نیازهای تجاری کلاینت‌ها و امنیت تعادلی را برقرار کنیم. در نسخه‌های قبل از ویندوز سرور 2008 دو سناریو را به طور دائم مورد استفاده قرار می‌دادم که اجرای آن با مشکلاتی همراه بود. اول اینکه دسترسی سطح بالای کاربران چالش‌های امنیتی را به دنبال داشت. چنین حساب‌هایی برای نفوذگران خیلی جذاب است بنابراین باید دارای کلمات عبور طولانی و پیچیده باشند. در نسخه‌های قدیمی ویندوز فقط یک سیاست کلمه عبور می‌توانست به همه حساب‌های دامنه اعمال شود. بنابراین باید یک سیاست کلمه عبور خیلی پیچیده برای همه کاربران دامنه اعمال کنم که هرگز راه حل مناسبی نیست و یا از مدیران شبکه بخواهم از سیاست محدودکننده تری پیروی کنند. ویندوز سرور 2008 سیاست کلمه عیوری موسوم به fine-grained را معرفی می‌کند که به منظور اعمال کلمات عبور با محدودیت بیشتر یا کمتر نسبت به نیازمندی‌های گروهها و کاربران دامنه استفاده می‌شود.

شعبات سازمان نیز به نوبه خود دردسرساز هستند چون مجبور هستیم تعادلی بین نیازهای کاربران جهت تایید هویت و خواست‌های شعبات به منظور متمرکز کردن کنترل روی امنیت فیزیکی DC ها برقرار کنیم. قرار دادن یک DC در یک شعبه باعث بالا رفتن سرعت در آن شعبه می‌شود ولی امنیت را نسبت به حالتی که سرور در مرکز داده قرار دارد کاهش می‌دهد. برای حل این مشکل ویندوز سرور 2008 می‌تواند به عنوان DC فقط خواندنی عمل کند و کاربران را در شعبات بدون ذخیره کردن همه اعتبارهای دامنه تایید اعتبار کند که این کار باعث کاهش خطر در زمان ربوده شدن سرور DC می‌شود.

اگر با Active Directory کار کرده باشید حتما سیاست‌های کلمه عبور fine-grained و DC های فقط خواندنی را ستوده‌اید.

اگر تازه با Active Directory آشنا شده‌اید از کار کردن با این ویژگی‌های جدید لذت خواهید برد.

درس ۱: پیکربندی سیاست‌های کلمه عبور و قفل کردن حساب

در یک دامنه ویندوز سرور 2008 کاربران هر ۴۲ روز یک باز نیاز به تغییر کلمات عبورشان دارند و کلمه عبور باید حداقل ۷ کاراکتر طول داشته باشد و پیچیده باشد. تعریف کلمه عبور پیچیده به این ترتیب است که از چهار نوع کاراکتر زیر دارای حداقل سه نوع کاراکتر باشد: حروف بزرگ، حروف کوچک، اعداد و علامت. سه سیاست کلمه عبور یعنی طول عمر کلمه عبور، طول کلمه عبور و پیچیدگی کلمه عبور اولین سیاست‌های کلمه عبور است که مدیران شبکه به آن توجه می‌کنند. تنظیمات پیش فرض این بخش به ندرت پیش می‌آید که با نیازمندی‌های سازمان هماهنگی داشته باشد. ممکن است نیاز باشد در سازمان طول کلمه عبور عوض شود. در این درس یاد می‌گیریم چطور سیاست‌های کلمه عبور و قفل کردن حساب را با استفاده از شیء Default Domain Policy Group Policy (GPO)پیاده‌سازی کنیم.

هر قانونی استثنا دارد و احتمالا برای این سیاست‌های کلمه عبور نیز مجبور شویم استثنا قایل شویم. برای ارتقاء امنیت در دامنه بهتر است برای کلمات عبور کاربران مدیر شبکه، حساب‌های مربوط به سرویس‌ها نظیر MS SQL یا تهیه پشتیبان شرایط سخت‌تری در نظر بگیریم. در نسخه‌های قبلی ویندوز این کار امکان‌پذیر نبود و یک سیاست کلمه عبور به همه حساب‌ها در دامنه اعمال می‌شد. در این درس یاد می‌گیریم سیاست‌های کلمه عبور fine-grained را پیکربندی کنیم ویژگی جدیدی که به ما امکان می‌دهد سیاست‌های متفاوتی را برای کاربران و گروههای دامنه پیکربندی کنیم.

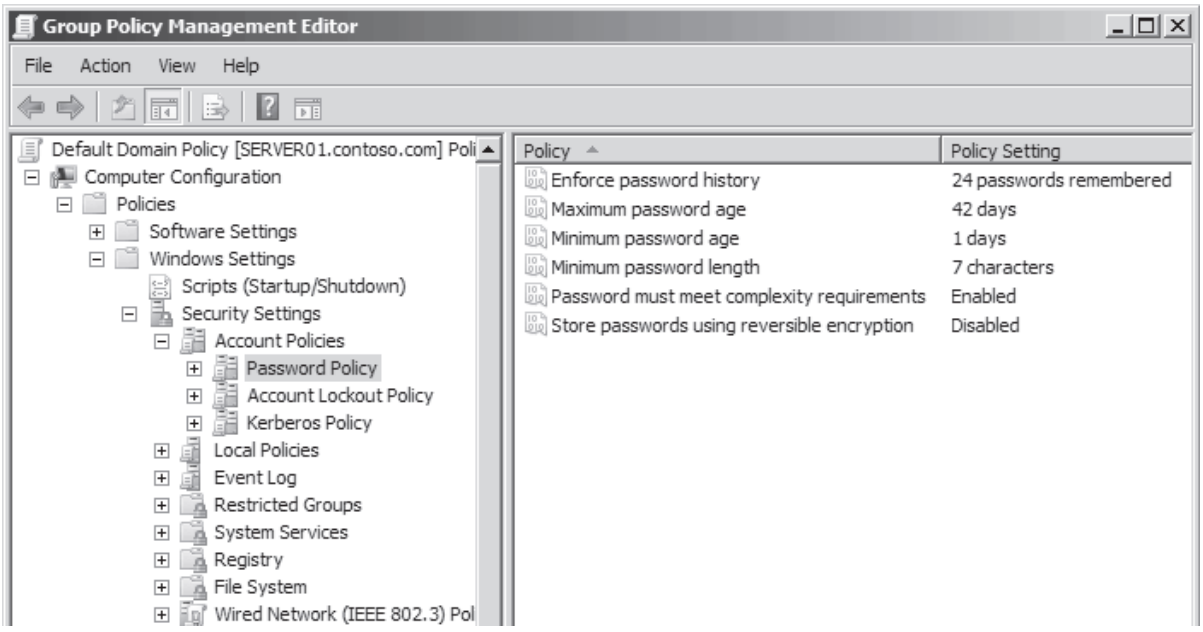
بعد از این درس می‌توانیم:

- سیاست کلمه عبور دامنه خود را پیاده‌سازی کنیم.
- سیاست‌های کلمه عبور fine-grained را تعیین و پیکربندی کنیم.

زمان تقریبی: ۴۵ دقیقه

مفهوم سیاست‌های کلمه عبور

سیاست کلمه عبور دامنه توسط یک GPO که دامنه در حوزه آن قرار دارد پیکربندی می‌شود. در GPO در بخش Computer Configuration\Policies\Windows Settings\Account Policies\Password Policy می‌توانیم تنظیمات سیاست را که نیازمندی‌های کلمه عبور را تعیین می‌کند پیکربندی کنیم. گره Password Policy در شکل ۱- ۸ نشان داده شده است.



شکل ۱- ۸ گره Password Policy مربوط به یک GPO

ما با دانستن چرخه عمر کلمه عبور کاربر می‌توانیم تاثیرات سیاست‌ها را درک کنیم. کاربر باید کلمه عبور خود را پس از گذراندن

زمان مشخص که در تنظیم سیاست Maximum Password Age مشخص می‌شود تغییر دهد. هنگامی که کاربر کلمه عبور جدید را وارد می‌کند طول کلمه عبور جدید با تعداد کاراکترهای مشخص شده در تنظیم Minimum Password Length مقایسه می‌شود. طول این کلمه عبور باید مساوی یا بیشتر از مقدار مشخص شده در تنظیم باشد. اگر تنظیم Password Must Meet Complexity Requirements فعال باشد کلمه عبور باید شامل حداقل سه تا از چهار نوع کاراکتر زیر باشد:

- حروف بزرگ برای مثال A – Z
- حروف کوچک برای مثال a – z
- اعداد برای مثال 0 – 9
- علائم مانند ! - # - % - &

اگر کلمه عبور جدید مطابق با این شرایط باشد Active Directory کلمه عبور را با استفاده از یک الگوریتم ریاضی به صورت یک hash code ذخیره می‌کند. این کد منحصر به فرد است و الگوریتم مورد استفاده تابع یکطرفه (one-way function) نام دارد و با عملیات معکوس کلمه عبور به دست نمی‌آید. این نوع ذخیره‌سازی باعث افزایش امنیت حساب کاربری می‌شود.

گاهگاهی برنامه‌های کاربردی باید بتوانند کلمه عبور کاربر را بخوانند. البته این کار امکانپذیر نیست زیرا به طور پیش فرض فقط hash code در Active Directory ذخیره می‌شود. برای این منظور می‌توانیم سیاست Store Passwords Using Reversible Encryption را فعال کنیم. این تنظیم به طور پیش فرض فعال نیست. البته این کار باعث کاهش امنیت شبکه می‌شود بنابراین بهتر است این برنامه‌ها از روی سیستم پاک شوند.

به علاوه Active Directory می‌تواند کلمات عبور قبلی کاربر را نگه دارد که کلمه عبور جدید با کلمه عبور قدیمی نباید یکسان باشد. تعداد کلمات عبور قبلی که با کلمه عبور جدید مقایسه می‌شود توسط سیاست Enforce Password History تعیین می‌شود. به طور پیش فرض ویندوز تا ۲۴ کلمه عبور را نگه می‌دارد.

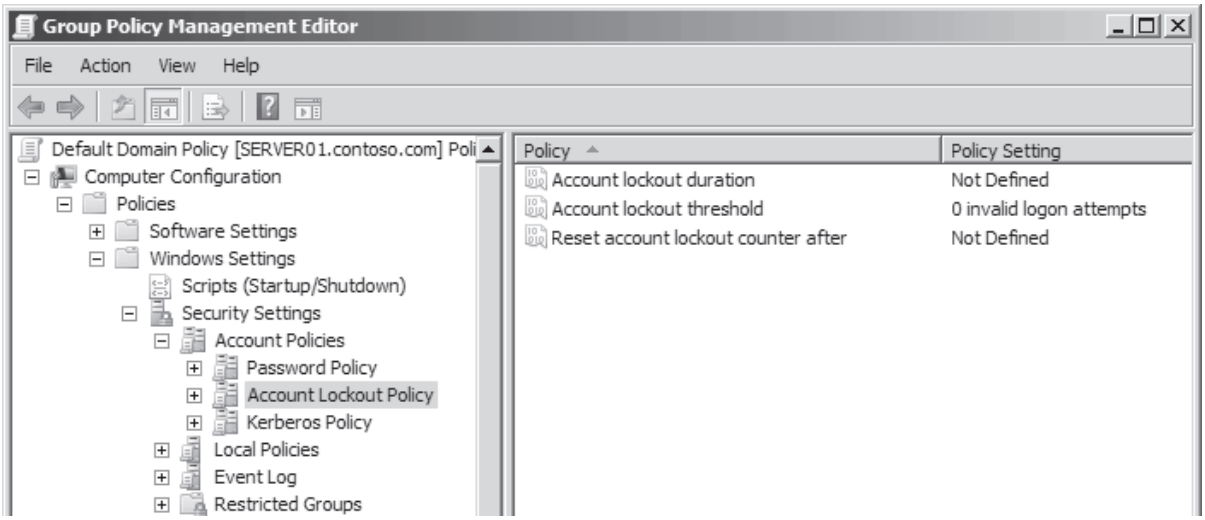
وقتی این تنظیم اعمال می‌شود پس از سررسید اعتبار زمانی کلمه عبور کاربر می‌تواند پشت سرهم کلمات عبور خود را تغییر دهد تا مثلا پس از ۲۵ بار دوباره کلمه عبور اول را به عنوان کلمه عبور خود تعیین کند و این به معنی بی‌اثر کردن تنظیم Enforce Password History می‌باشد. برای جلوگیری از این کار تنظیم Minimum Password Age مدت زمان لازم بین دو تغییر کلمه عبور را تعیین می‌کند. به طور پیش فرض این زمان یک روز است.

هرکدام از این تنظیم‌ها روی کاربری که کلمه عبور خود را تغییر می‌دهد موثر است. این تنظیمات روی کاربر مدیر شبکه که با استفاده از دستور Reset Password کلمه عبور کاربر را ریست می‌کند تاثیری ندارد.

درک سیاست‌های قفل کردن حساب

نفوذگر با پیدا کردن یک نام کاربری و کلمه عبور معتبر به منابع شبکه دسترسی پیدا می‌کند. پیدا کردن نام کاربری کار سختی نیست چرا که اکثرا از ترکیب نام و نام خانوادگی کاربر یا شماره کارمندی و امثالهم به دست می‌آید. وقتی نام کاربری کشف شد نفوذگر به دنبال کلمه عبور می‌گردد. این کار با حدث زدن یا با ترکیب کردن کاراکترها و کلمات تا ورود موفق ادامه پیدا می‌کند.

این نوع حمله با محدود کردن تعداد دفعات ورود اشتباه کلمه عبور قابل خنثی شدن می‌باشد. سیاست‌های قفل کردن حساب این موارد را مدیریت می‌کند. این سیاست‌ها در گره GPO زیر Password Policy قرار دارد. گره Account Lockout Policy در شکل ۲- ۸ نشان داده شده است.



شکل ۲- ۸ گره Account Lockout Policy مربوط به یک GPO

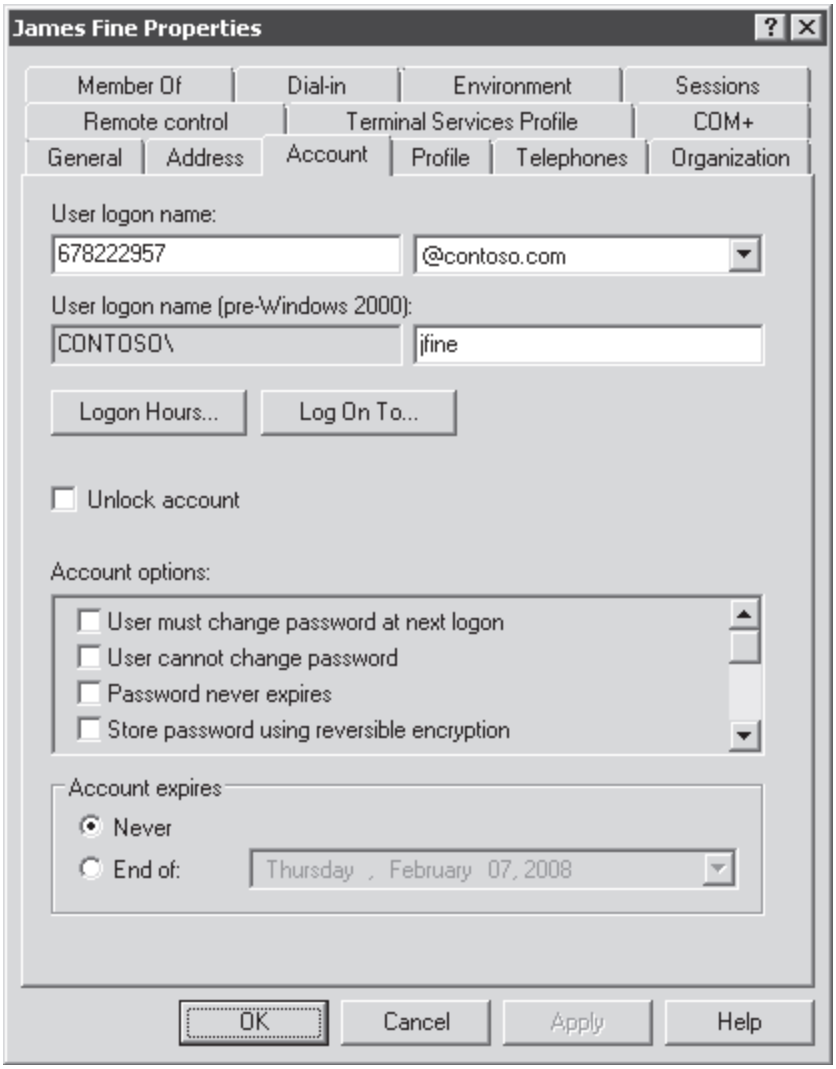
سه تنظیم در این ارتباط موجود است. اول Account Lockout Threshold است که تعداد تلاش‌های ناموفق مجاز را در زمان مشخص شده توسط سیاست Account Lockout Duration تعیین می‌کند. اگر در اثر یک حمله تعداد تلاش‌های ناموفق برای ورود در یک بازه زمانی بیش از میزان مجاز باشد حساب قفل می‌شود. وقتی حسابی قفل می‌شود Active Directory از ورود کاربر به شبکه ممانعت می‌کند حتی اگر کلمه عبور صحیح وارد شود.

کاربر Administrator می‌تواند قفل حساب کاربری را طبق مراحل شرح داده شده در فصل ۳ باز کند. همچنین می‌توانیم Active Directory را طوری پیکربندی کنیم که پس از مدت مشخص تعیین شده توسط سیاست Reset Account Lockout Counter After قفل خود بخود باز شود.

پیکربندی سیاست‌های کلمه عبور دامنه و قفل کردن حساب

Active Directory از یک سری سیاست‌های کلمه عبور و قفل کردن حساب در دامنه پشتیبانی می‌کند. این سیاست‌ها در یک GPO که دامنه در حوزه آن قرار دارد پیکربندی می‌شود. یک دامنه جدید دارای یک GPO با نام Default Domain Policy می‌باشد که به دامنه لینک شده و شامل تنظیمات سیاست‌های پیش فرض نشان داده شده در شکل ۱- ۸ و ۲- ۸ می‌باشد. این تنظیمات با ویرایش Default Domain Policy قابل تغییر است.

تنظیمات کلمه عبور پیکربندی شده در Default Domain Policy روی همه حساب‌ها در دامنه تاثیر می‌گذارد. اگر تنظیمات مربوط به کلمه عبور برای کاربر یا کاربرانی به طور اختصاصی پیکربندی شود این تنظیمات بر تنظیمات پیش فرض غلبه می‌کند. در زبانه Account مربوط به کادر Properties کاربر می‌توانیم تنظیماتی نظیر Password Never Expires و Store Passwords Using Reversible Encryption را پیکربندی کنیم. برای مثال اگر ۵ کاربر از برنامه‌ای استفاده می‌کنند که نیاز به دسترسی به کلمات عبور آنها را دارد می‌توانیم حساب کاربری آنها را طوری پیکربندی کنیم که کلمات عبورشان با استفاده از رمزگذاری قابل برگشت (Reversible Encryption) ذخیره شود.



شکل ۳- ۸ خصوصیات مرتبط با کلمه عبور در یک حساب کاربری

کلمه عبور Fine-Grained و سیاست قفل کردن حساب

یکی دیگر از راههای غلبه بر سیاست کلمه عبور و قفل کردن حساب در دامنه استفاده از ویژگی جدید ویندوز سرور 2008 با نام Fine-Grained Password and Lockout Policy می‌باشد. که نام کوتاه آن نیز Fine-Grained Password Policy است. این نوع کلمه عبور ما را قادر می‌سازد سیاستی را پیکربندی کنیم که به یک یا چند گروه یا کاربر دامنه اعمال می‌شود. برای استفاده از این قابلیت سطح عملیاتی دامنه باید Windows Server 2008 باشد که در فصل ۱۲ شرح داده می‌شود.

این ویژگی یک ویژگی برجسته در Active Directory می‌باشد. سناریوهای متعددی وجود دارد که در آنها سیاست کلمه عبور Fine-Grained در افزایش امنیت دامنه تاثیر مثبت دارد. حساب‌های مورد استفاده توسط مدیران شبکه دارای مجوزهای بالایی در دامنه می‌باشند بنابراین اگر نفوذگر این نوع کلمه عبور را کشف کند نسبت به کلمه عبور کاربر استاندارد می‌تواند خسارت بیشتری به شبکه وارد کند. به همین دلیل شرایط سخت تری را باید برای این کلمات عبور در نظر بگیریم. برای مثال حداقل طول مجاز کلمات عبور را بالا برده و فاصله بین دو تغییر کلمه عبور را کم کنیم.

حساب‌های مورد استفاده سرویس‌هایی نظیر SQL Server همچنین نیاز به وضعیت مخصوصی در دامنه هستند. سرویس‌ها وظایف خود را با اعتباری مانند اعتبار کاربران انجام می‌دهند. بهرحال بیشتر سرویس‌ها توانایی تغییر کلمه عبور خود را ندارند و مدیران شبکه کلمه عبور این حساب‌ها را به طور دائمی (Password Never Expires) پیکربندی می‌کنند. وقتی کلمه عبور یک حساب تغییر نمی‌کند باید کلمه عبور مطمئنی برای آن انتخاب کرد که به راحتی کشف نشود. برای تعیین یک حداقل طول با کاراکترهای زیاد کلمه عبور و بدون انقضاء از کلمه عبور Fine-Grained استفاده می‌شود.

اشیاء تنظیمات کلمه عبور

تنظیماتی که توسط سیاست کلمه عبور Fine-Grained مدیریت می‌شود مشابه همانهایی هستند که در گره های Password Policy و Account Policy یک GPO وجود دارند. بهرحال سیاست‌های کلمه عبور Fine-Grained به عنوان بخشی از Group Policy پیاده‌سازی نمی‌شود و به عنوان بخشی از یک GPO نیز اعمال نمی‌گردد. در عوض یک کلاس شیء مجزا در Active Directory موجود است که سیاست تنظیمات کلمه عبور Fine-Grained را نگهداری می‌کند و نام آن password settings object (PSO) می‌باشد.

نکته امتحانی فقط و فقط یک سیاست کلمه عبور و قفل کردن حساب به صورت Authoritative وجود دارد که به همه کاربران در دامنه اعمال می‌شود که همان تنظیمات موجود در Default Domain Policy GPO می‌باشد. سیاست‌های کلمه عبور Fine-Grained که به گروهها یا کاربران دامنه اعمال می‌شود با استفاده از PSO ها پیاده سازی می‌شوند.

بیشتر اشیاء Active Directory با رابط گرافیکی کاربرپسندی نظیر ابزار Active Directory Users and Computers مدیریت می‌شوند. برای مدیریت PSO ها می‌توان از ابزارهای سطح پایین مانند ADSI Edit استفاده کرد.

امکان ساخت یک یا چند PSO در دامنه موجود است. هر PSO محتوی یک سری کامل تنظیمات سیاست کلمه عبور و قفل کردن حساب است. یک PSO با لینک شدن به یک یا چند کاربر یا گروه امنیتی global اعمال می‌شود. برای مثال برای پیکربندی سیاست کلمه عبور سخت برای مدیران شبکه یک گروه امنیتی global ساخته و حساب کاربری سرویس را به عنوان عضو اضافه کرده و یک PSO را به گروه لینک می‌کنیم. اعمال سیاست‌های کلمه عبور Fine-Grained به یک گروه به این شکل منطقی تر از اعمال آنها به حساب‌های کاربری به طور مجزاست. اگر یک حساب سرویس جدید بسازیم و به گروه اضافه کنیم حساب جدید توسط PSO مدیریت می‌شود.

تقدم PSO و PSO نهایی

PSO ها می‌توانند به بیش از یک گروه یا کاربر لینک شوند و به گروه یا کاربر مشخص می‌تواند بیش از یک PSO لینک شود و کاربر نیز می‌تواند به چند گروه تعلق داشته باشد. پس کدام تنظیم کلمه عبور و قفل کردن Fine-Grained به کاربر اعمال می‌شود؟ فقط وفقط یک PSO تنظیم مورد نظر را برای کاربر تعریف می‌کند و آن PSO نهایی است. هر PSO یک خصیصه دارد که تعیین کننده تقدم PSO است. مقدار این تقدم عددی است بین صفر و یک. وقتی چند PSO به یک کاربر اعمال می‌شود PSO با بالاترین تقدم (نزدیکتر به ۱) اعمال می‌شود. قوانینی که تقدم را مشخص می‌کند به شرح زیر است:

- اگر بیش از یک PSO به گروههایی که کاربر عضو آن است اعمال شود PSO با بالاترین اولویت غلبه می‌کند.
- اگر یک یا چند PSO به طور مستقیم به کاربر لینک شده باشد PSO های لینک شده به گروهها صرف نظر از تقدم‌شان بی‌اثر می‌شود. PSO لینک شده به کاربر با بالاترین تقدم غلبه می‌کند.
- اگر یک یا چند PSO مقدار تقدم مشابه داشته باشند Active Directory از بین آنها یکی را انتخاب می‌کند و آن PSO ای است که کمترین مقدار GUID را دارد. GUID ها برای اشیاء Active Directory به مثابه شماره سریال است. هیچ دو شیء نمی‌توانند GUID مشابه داشته باشند. GUID ها معنی خاصی ندارند و فقط یک شناسه هستند بنابراین انتخاب PSO با کمترین مقدار GUID یک تصمیم تصادفی است. برای جلوگیری از چنین سناریوهایی PSO را با مقادیر مشخص و منحصر به فرد پیکربندی می‌کنیم.

این قوانین تعیین کننده PSO نهایی هستند. Active Directory در یک خصیصه شیء کاربر PSO نهایی را مشخص می‌کند. می‌توانیم این خصیصه را در یکی از تمرینات آخر این درس تست کنیم. PSO ها در بر گیرنده همه تنظیمات مربوط به کلمات عبور و قفل کردن حساب می‌باشد بنابراین هیچ وراثت یا ترکیبی از تنظیمات مشاهده نمی‌شود. PSO نهایی قطعی (Authoritative) خواهد بود.

PSO ها و OU ها

PSO ها می‌توانند به گروههای امنیتی Global یا کاربران لینک شوند. آنها نمی‌توانند به OU ها لینک شوند. اگر بخواهیم

سیاست کلمه عبور و قفل کردن حساب را روی کاربران یک OU اعمال کنیم باید یک گروه امنیتی global بسازیم که شامل همه کاربران آن OU باشد. این نوع گروه را گروه سایه (shadow group) می‌نامند.

گروههای سایه اشیاء مفهومی هستند نه تکنیکال. ما به سادگی یک گروه می‌سازیم و کاربران متعلق به OU را به آن اضافه می‌کنیم. اگر عضویت OU تغییر کند باید عضویت گروه را تغییر دهیم.

تمرینات پیکربندی سیاست‌های کلمه عبور و قفل کردن حساب

در این تمرینات از Group Policy به منظور پیکربندی سیاست‌های کلمه عبور و قفل کردن حساب در سطح دامنه contoso.com استفاده می‌شود. سپس حساب‌های مدیریتی با استفاده از پیکربندی محدودتر و سیاست‌های کلمه عبور و قفل کردن حساب Fine-Grained حساب‌های مدیریتی امن می‌گردد.

تمرین ۱ پیکربندی سیاست‌های کلمه عبور و قفل کردن حساب در دامنه

در این تمرین GPO Default Domain Policy به منظور پیاده‌سازی سیاست کلمه عبور و قفل کردن حساب برای کاربران در دامنه contoso.com ویرایش می‌گردد.

۱. با کاربر Administrator به SERVER01 وارد می‌شویم.

۲. کنسول GPMC را باز می‌کنیم.

۳. گره‌های Forest، Domains و سپس contoso.com را باز می‌کنیم.

۴. روی Default Domain Policy زیر دامنه contoso.com کلیک راست کرده و Edit را انتخاب می‌کنیم. پیغامی مبنی بر تغییر تنظیمات GPO ظاهر می‌شود.

۵. روی OK کلیک می‌کنیم. پنجره GPME باز می‌شود.

۶. گره Computer Configuration\Policies\Security Settings\Account Policies را باز کرده و Password Policy را انتخاب می‌کنیم.

۷. روی تنظیمات سیاست زیر دوبار کلیک کرده و تنظیمات را پیکربندی می‌کنیم:

- Maximum Password Age : 90 Days
- Minimum Password Length : 10 characters

۸. Account Lockout Policy را در کنسول انتخاب می‌کنیم.

۹. روی تنظیم Account Lockout Threshold دوبار کلیک کرده و مقدار ۵ بار تلاش ناموفق را پیکربندی کرده و OK می‌کنیم.

۱۰. پنجره Suggested Value Changes ظاهر می‌شود. روی OK کلیک می‌کنیم. مقدار Account Lockout Duration و Reset Account Lockout Counter After به طور خودکار روی ۳۰ دقیقه تنظیم می‌شود.

۱۱. پنجره GPME را می‌بندیم.

تمرین ۲ ساخت شیء تنظیم کلمه عبور

در این تمرین یک PSO ساخته می‌شود که سیاست کلمه عبور محدود کننده و Fine-Grained روی کاربران گروه Domain

Admins اعمال می‌کند. قبل از شروع این تمرین گروه مذکور در Users container باید ساخته شده باشد.

۱. از پوشه Administrative Tools ابزار ADSI Edit را باز می‌کنیم.

۲. روی آن کلیک راست کرده و Connect To را انتخاب می‌کنیم.

۳. در کادر Name عبارت contoso.com را تایپ کرده و OK می‌کنیم.

۴. گره contoso.com را باز کرده و DC=contoso,DC=com را انتخاب می‌کنیم.

۵. گره DC=contoso.com,DC=com را باز کرده و CN=System را انتخاب می‌کنیم.

۶. گره CN=System را باز کرده و CN=Password Settings Container را انتخاب می‌کنیم. همه PSO ها در Password Settings Container (PSC) ساخته و ذخیره می‌شود.

۷. روی PSC کلیک راست کرده New و سپس Object را انتخاب می‌کنیم. کادر محاوره‌ای Create Object ظاهر می‌شود. پیغامی مبنی بر انتخاب نوع شیء برای ساختن ظاهر می‌شود. فقط یک انتخاب ممکن است: msDS-PasswordSettings نام تکنیکال برای کلاس شیء ارجاع شده به یک PSO می‌باشد.

۸. روی Next کلیک می‌کنیم. پیغامی برای ورود مقدار هر خصیصه PSO ظاهر می‌شود. این خصیصه‌ها مشابه خصیصه‌های GPO تمرین ۱ می‌باشد.

۹. همه خصیصه‌ها را مطابق لیست زیر پیکربندی می‌کنیم. پس از ورود هر خصیصه Next را کلیک می‌کنیم.

- Common Name : **My Domain Admins PSO** . این نام با مسمی برای PSO است.
- msDS-PasswordSettingsPrecedence : **1** . این PSO بالاترین تقدم ممکن خواهد شد.
- msDS-PasswordReversibleEncryptionEnabled : **False** . کلمه عبور با استفاده از رمزنگاری قابل برگشت ذخیره نمی‌شود.
- msDS-PasswordHistoryLength : **30** . کاربر نمی‌تواند تا سی کلمه عبور قبلی خود را انتخاب کند.
- msDS-PasswordComplexityEnabled : **true** . قوانین مربوط به پیچیدگی کلمه عبور اعمال می‌گردد.
- msDS-MinimumPasswordLength : **15** . کلمه عبور باید حداقل ۱۵ کاراکتر داشته باشد.
- msDS-MinimumPasswordAge : **1:00:00:00** . کاربر نمی‌تواند کلمه عبورش را دوبار در روز عوض کند. فرمت آن به صورت d:hh:mm:ss (به ترتیب روز، ساعت، دقیقه و ثانیه می‌باشد)
- MaximumPasswordAge : **45:00:00:00** . کلمه عبور باید هر ۴۵ روز یکبار عوض شود.
- msDS-LockoutThreshold : **5** . ۵ بار تلاش ناموفق در بازه زمانی مشخص شده در خصیصه بعدی باعث

قفل شدن حساب می‌شود.

- **0:01:00:00** : msDS-LockoutObservationWindow . ۵ بار تلاش ناموفق (مشخص شده در خصیصه قبلی) در بازه زمانی ۱ ساعت باعث قفل شدن حساب می‌شود.
- **1:00:00:00** : msDS-LockoutDuration . وقتی حسابی قفل می‌شود برای مدت ۱ ساعت به همان حالت می‌ماند و پس از آن به طور خودکار قفل باز می‌شود. مقدار صفر باعث می‌شود حساب قفل باقی بماند تا کاربر Administrator آنرا باز کند.

پیکربندی خصیصه‌های فوق ضروری است. پس از کلیک روی Next در صفحه msDS-LockoutDuration می‌توانیم خصیصه‌های بعدی را که اجباری نیستند پیکربندی کنیم.

۱۰. روی دکمه More Attributes کلیک می‌کنیم.

۱۱. در کادر Edit Attributes تایپ می‌کنیم CN=DomainAdmins,CN=Users,DC=contoso,DC=com و روی OK کلیک می‌کنیم. روی Finish کلیک می‌کنیم.

تمرین ۳ تعیین PSO نهایی کاربر

در این تمرین PSO ای که سیاست‌های کلمه عبور را برای کاربر کنترل می‌کند مشخص می‌شود.

۱. ابزار Active Directory Users And Computers را باز می‌کنیم.

۲. منوی View را باز می‌کنیم و گزینه Advanced Features را علامت می‌زنیم.

۳. گره contoso.com را باز کرده و روی Users container کلیک می‌کنیم.

۴. روی حساب Administrator کلیک راست کرده و Properties را انتخاب می‌کنیم.

۵. روی زبانه Attribute Editor کلیک می‌کنیم.

۶. روی دکمه Filter کلیک کرده و Constructed را علامت می‌زنیم. خصیصه‌ای که در بخش بعدی می‌بینیم خصیصه constructed می‌باشد این بدین معنی است که PSO نهایی با محاسبه PSO های لینک شده به کاربر به دست می‌آید.

۷. در لیست Attributes محل msDS-ResultantPSO را پیدا می‌کنیم.

۸. PSO ای را که روی کاربر تاثیر می‌گذارد پیدا می‌کنیم.

My Domain Admins PSO که در تمرین ۲ ساخته شد PSO نهایی حساب Administrator می‌باشد.

تمرین ۴ حذف یک PSO

در این تمرین PSO ای که در تمرین ۲ ساخته شد حذف می‌شود به طوری که تنظیمات آن در تمرینات بعدی تاثیری ندارد.

۱. مراحل ۱ تا ۶ تمرین ۲ را برای انتخاب Password Settings container در ADSI Edit تکرار می‌کنیم.

۲. در پنل سمت چپ کنسول، CN=My Domain Admins PSO را انتخاب می‌کنیم.

۳. کلید Delete را می‌زنیم.

۴. دکمه Yes را کلیک می‌کنیم.

خلاصه درس

- تنظیمات سیاست کلمه عبور تعیین می‌کند چه موقع کلمه عبور باید یا می‌تواند تغییر یابد و کلمه عبور جدید چه ویژگی‌هایی باید داشته باشد.
- تنظیمات Account Lockout باعث می‌شود اگر تعداد معینی تلاش ناموفق برای ورود به سیستم در یک بازه زمانی مشخص اتفاق بیافتد حساب قفل شود. این تنظیم از تلاش نفوذگر برای ورود غیرقانونی به سیستم جلوگیری می‌کند.
- در دامنه فقط یک سری سیاست کلمه عبور و قفل کردن حساب موجود است که روی همه کاربران تاثیر می‌گذارد. این سیاست‌ها توسط Group Policy تعریف می‌شود. این تنظیمات در Default Domain Policy GPO قابل تغییر است.
- ویندوز سرور 2008 امکان تعیین سیاست متفاوت کلمه عبور و قفل کردن حساب را برای گروههای امنیتیglobal و کاربران دامنه فراهم می‌کند. سیاست‌های کلمه عبور Fine-Grained نه با Group Policy بلکه با اشیاء تنظیمات کلمه عبور توزیع می‌شود.
- اگر بیش از یک PSO به یک کاربر یا گروههایی که کاربر عضو آن است اعمال شود یکی از آنها به عنوان PSO نهایی سیاست‌های کلمه عبور کاربر را تعیین می‌کند. PSO با بالاترین اولویت (نزدیک به یک) بر دیگران غلبه خواهد کرد. اگر یک یا چند PSO مستقیما به کاربر لینک شود به جای اینکه به گروه لینک شود PSO های لینک شده به گروه به حساب نمی‌آیند و PSO لینک شده به کاربر با بالاترین اولویت غلبه خواهدکرد.

سئوالات پایان درس

۱. فرض کنید مدیر شبکه شرکت Tailspain Toys هستید. دامنه شما حاوی یک OU با نام Service Accounts می‌باشد که همه کاربران را دربر می‌گیرد. به دلیل اینکه حساب های سرویس با کلمات عبور بدون انقضاء پیکربندی شده است باید سیاست کلمه عبوری پیکربندی شود که حداقل کاراکتر کلمه عبور را ۴۰ تعیین کند. کدام یک از جوابهای زیر این کار را انجام می‌دهد؟ (همه گزینه‌ها در صورت صحت انتخاب شود. هر گزینه صحیح بخش از جواب است)

A. سیاست Minimum Password Length را در Default Domain Policy GPO پیکربندی می‌کنیم.

B. یک PSO را به Service Accounts OU لینک می‌کنیم.

C. گروهی با نام Service Accounts می‌سازیم.

D. یک PSO به گروه Service Accounts لینک می‌کنیم.

E. همه سرویس‌ها را به عنوان اعضاء گروه Service Accounts اضافه می‌کنیم.

۲. می‌خواهیم سیاست قفل کردن حساب را طوری پیکربندی کنیم که یک حساب قفل شده به طور خودکار باز نشود و فقط کاربر Administrator آنرا باز کند. کدام جواب صحیح است؟

A. سیاست Account Lockout Duration را روی ۱۰۰ تنظیم می‌کنیم.

B. سیاست Account Lockout Duration را روی ۱ تنظیم می‌کنیم.

C. Account Lockout Threshold را روی صفر تنظیم می‌کنیم.

D. سیاست Account Lockout Duration را روی صفر تنظیم می‌کنیم.

۳. هنگامی که اشیاء تنظیمات کلمه عبور را در دامنه خود ارزیابی می‌کنیم یک PSO با نام PSO1 با اولویت ۱ که به گروهی با نام Help Desk لینک شده است پیدا می‌کنیم. PSO دیگری با نام PSO2 با اولویت ۹۹ به گروهی با نام Support لینک شده است. Mike Danseglio عضو هر دو گروه می‌باشد. ما متوجه می‌شویم که دو PSO مستقیما به Mike لینک شده اند. PSO3 مقدار اولویت ۵۰ دارد و PSO4 ۲۰۰ . کدام PSO برای کاربر Mike نهایی است؟

A. PSO1

B. PSO2

C. PSO3

D. PSO4

درس ۲ : ممیزی تایید هویت

در فصل ۷ یاد گرفتیم که چطور برای انواع فعالیت‌ها ممیزی را فعال کنیم. ویندوز سرور 2008 همچنین به ما امکان می‌دهد ورود کاربران را به دامنه ممیزی کند. با ممیزی ورود موفق به شبکه متوجه کاربرانی می‌شویم که به دفعات و از محل‌های غیرمتعارف به شبکه وارد شده‌اند که می‌تواند نشان‌دهنده تلاش نفوذگر باشد. در این درس پیکربندی ممیزی ورود را یاد می‌گیریم.

بعد از این درس می‌توانیم:

- ممیزی فعالیت‌های مرتبط با تایید هویت را پیکربندی کنیم.
- بین account logon و logon event تفاوت قایل شوبم.
- وقایع مرتبط با تایید هویت را در Security Log تشخیص دهیم.

زمان تقریبی : ۳۰ دقیقه

در تنظیمات سیاست امنیتی دو عبارت شبیه به هم وجود دارد : یکی Audit Account Logon Events و دیگری Audit Logon Events.

وقتی کاربری به کامپیوتری در دامنه با استفاده از حساب کاربری خود وارد می‌شود DC این عملیات را تایید هویت می‌کند. این کار باعث ثبت یک واقعه account logon در DC می‌شود.

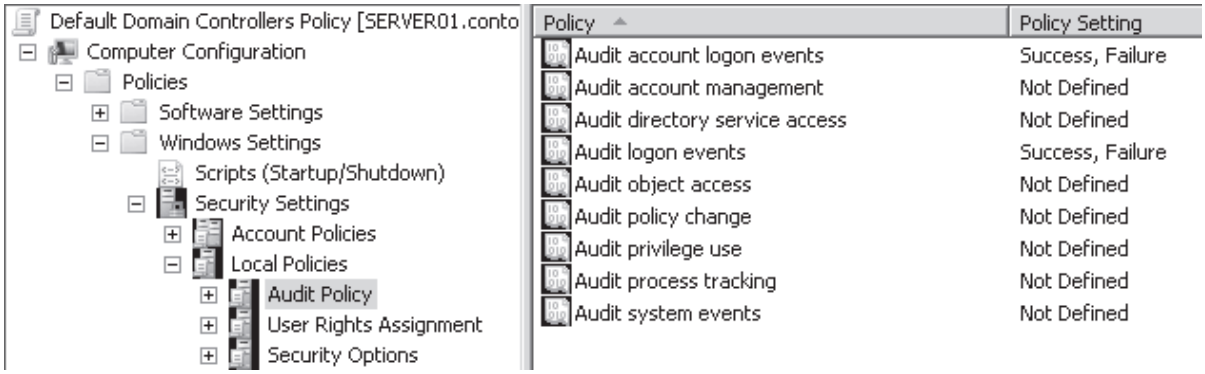
کامپیوتری که کاربر به آن وارد می‌شود یک واقعه logon event را ثبت می‌کند. کامپیوتر کاربر را تایید هویت نمی‌کند و هویت کاربر را به DC برای بررسی می‌فرستد. در صورت تایید DC کامپیوتر به کاربر اجازه ورود می‌دهد. بنابراین واقعه logon event ثبت می‌شود.

وقتی کاربری به یک پوشه روی سرور در دامنه متصل می‌شود آن سرور کاربر را به عنوان کاربر شبکه و ورود را به عنوان network logon در نظر می‌گیرد. سرور دوباره کاربر را تایید هویت نمی‌کند بلکه با همان بلیط (ticket) که DC به کاربر داده است به کاربر اجازه ورود می‌دهد. ولی ارتباط کاربر یک واقعه logon event روی سرور می‌سازد.

نکته امتحانی برای یادگیری سریع‌تر بهتر است بگوییم واقعه Account Logon Event جایی اتفاق می‌افتد که حساب کاربر آنجا قرار دارد. یعنی DC که کاربران را تایید هویت می‌کند. Logon event زمانی اتفاق می‌افتد که کاربر به کامپیوتر وارد می‌شود چه مستقیم چه از راه دور.

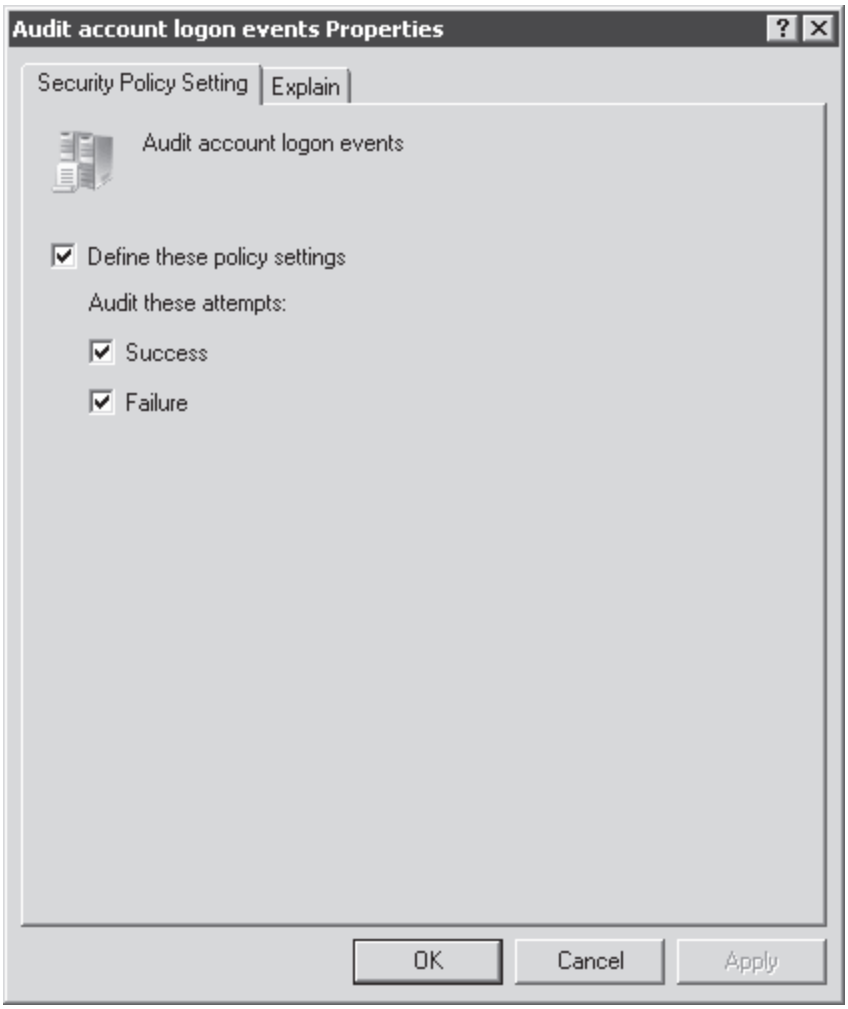
پیکربندی سیاست‌های ممیزی مرتبط با تایید هویت

وقایع account logon و logon در ویندوز سرور 2008 قابل ممیزی است. تنظیماتی که ممیزی را مدیریت می‌کند در یک GPO در مسیر Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy واقع شده است. گره Audit Policy و دو تنظیم آن در شکل ۴- ۸ نشان داده شده است.



شکل ۴- ۸ تنظیمات سیاست مرتبط با تایید هویت

برای پیکربندی یک سیاست ممیزی روی سیاست دوبار کلیک می‌کنیم تا کادر محاوره‌ای Properties باز شود. این کادر در شکل ۵- ۸ قابل مشاهده است.



شکل ۵- ۸ کادر محاوره‌ای Audit Account Logon Events Properties

تنظیم سیاست به یکی از چهار حالت زیر قابل پیکربندی است:

- **Not defined** اگر علامت کادر Define These Policy Settings را برداریم سیاست تعریف نشده خواهد شد. در این حالت سرور ممیزی را بر اساس تنظیمات پیش فرض یا تنظیمات مشخص شده در GPO دیگر انجام می‌دهد.
- **Defined for no auditing** اگر کادر Define These Policy Settings علامت داشته باشد ولی کادرهای Success و Failure بدون علامت باشند سرور وقایع را ممیزی نمی‌کند.
- **Audit successful events** اگر کادرهای Success و Define These Policy Settings علامت داشته باشند سرور وقایع موفق را در Security log ثبت می‌کند.
- **Audit failed to events** اگر کادرهای Failure و Define These Policy Settings علامت داشته باشند سرور وقایع ناموفق را در Security log ثبت می‌کند.

تعیین حوزه سیاست‌های ممیزی

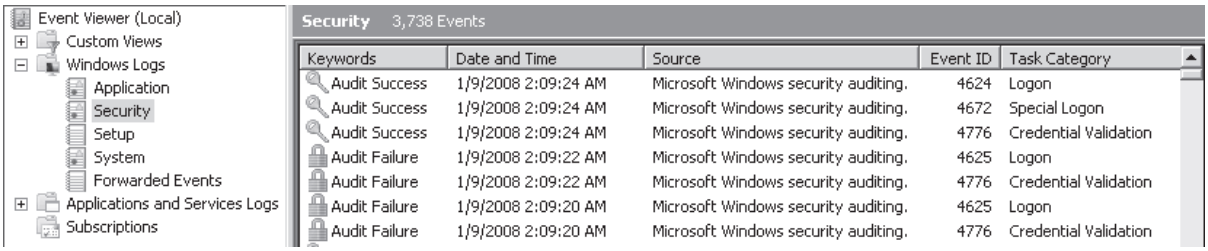
در تنظیم سیاست‌ها باید دقت شود تا سیاست به کامپیوترهای مورد نظر اعمال شود. برای مثال اگر بخواهیم تلاش‌های کاربران را برای اتصال به سرور فایل شبکه ممیزی کنیم باید ممیزی logon event را در یک GPO که به OU دربر گیرنده فایل سرور لینک شده پیکربندی کنیم. ولی اگر بخواهیم ورود کاربران را به سیستم‌های بخش منابع سازمانی شرکت ممیزی کنیم باید ممیزی logon event را روی یک GPO که به OU در بر گیرنده اشیاء کامپیوتر منابع انسانی لینک شده است پیکربندی کنیم. به خاطر داشته باشید که کاربران دامنه که به یک کلاینت شبکه وارد می‌شوند با به یک سرور متصل می‌شوند یک واقعه logon ثبت می‌شود نه account logon .

فقط DC ها واقعه account logon را برای کاربر دامنه ثبت می‌کنند. به خاطر داشته باشید که یک واقعه account logon روی DC ثبت می‌شود که کاربر دامنه را تایید هویت می‌کند صرف نظر از اینکه کاربر از کجا به شبکه وارد می‌شود. اگر بخواهیم حساب‌های دامنه را ممیزی کنیم حوزه ممیزی account logon را فقط DC در نظر می‌گیریم. در حقیقت Default Domain Controllers GPO که هنگام نصب اولین DC ساخته می‌شود یک GPO ایده‌ال برای پیکربندی سیاست‌های ممیزی account logon می‌باشد.

در بخش قبل یاد گرفتیم اگر سیاست ممیزی یک واقعه تعریف نشود سیستم بر اساس تنظیمات GPO های دیگر یا تنظیمات پیش فرض ممیزی را انجام می‌دهد. در ویندوز سرور 2008 تنظیم پیش فرض ممیزی وقایع موفق account logon و logon می‌باشد. اگر بخواهیم وقایع ناموفق را ممیزی کنیم یا ممیزی را غیرفعال کنیم باید تنظیم مناسب را در audit policy تعریف کنیم.

مشاهده وقایع Logon

وقایع مربوط به ورود کاربران در security log سیستم قابل مشاهده است. شکل ۶- ۸ مثالی در این ارتباط نشان می‌دهد. بنابراین اگر ورود کاربران را به کامپیوتر در واحد منابع انسانی ممیزی می‌کنیم وقایع در security log هر کامپیوتر جداگانه ثبت می‌شود. به طور مشابه اگر تلاش ناموفق برای account logon را ممیزی کنیم تا نفوذها را تشخیص دهیم وقایع در security log مربوط به هر DC ثبت می‌شود. این بدین معنی است که به طور پیش فرض مجبور هستیم security log همه DC ها را بررسی کنیم تا تصویری کامل از وقایع account logon در دامنه داشته باشیم.



شکل ۶- ۸ وقایع تایید هویت در security log

می‌توانید تصور کنید که در یک شبکه پیچیده با DC های متعدد و کاربران بیشمار ممیزی وقایع مربوط به ورود کاربران منجر به ثبت تعداد بیشماری واقعه خواهد شد و پیدا کردن وقایع مشکل‌دار که نیاز به بررسی بیشتر دارند خیلی سخت خواهد بود. بنابراین باید بین تعداد وقایع ثبت شده و منابع موجود برای تحلیل وقایع تعادل برقرار کنیم.

تمرینات ممیزی تایید هویت

در این تمرینات از Group Policy برای فعال کردن ممیزی فعالیت‌های ورود به سیستم در دامنه contoso.com بهره می‌گیریم. سپس logon events تولید شده را در event logs مشاهده می‌کنیم.

تمرین ۱ پیکربندی ممیزی Account Logon Events

در این تمرین قرار است Default Domian Controllers Policy GPO را ویرایش کنیم تا ممیزی ورود موفق و ناموفق کاربران را در دامنه پیاده سازی کنیم.

۱. کنسول GPMC را باز می‌کنیم.

۲. گره Forest\Domains\Contoso.com\Domain Controllers را باز می‌کنیم.

۳. روی Default Domain Controllers Policy کلیک راست کرده و Edit را انتخاب می‌کنیم. پنجره GPME باز می‌شود.

۴. گره Computer Configuration\Policies\Windows at Settings\Security Settings\Local Policies را باز کرده و Audit Policy را انتخاب می‌کنیم.

۵. روی Audit Account Logon Events دوبار کلیک می‌کنیم.

۶. کادر Define These Policy Settings را علامت می‌زنیم.

۷. کادرهای Success و Failure را علامت زده و OK می‌کنیم.

۸. روی Audit Logon Events دوبار کلیک می‌کنیم.

۹. کادر Define These Policy Settings را علامت می‌زنیم.

۱۰. کادرهای Success و Failure را علامت زده و OK می‌کنیم.

۱۱. GPME را می‌بندیم.

۱۲. منوی استارت را باز کرده و پنجره Command Prompt را باز می‌کنیم.

۱۳. تایپ می‌کنیم gpupdate.exe /force . این دستور باعث می‌شودPolicy های SERVER01 به روز شود.

تمرین ۲ تولید Account Logon Events

در این تمرین وقایع account logon از طریق ورود کلمه عبور صحیح و اشتباه تولید می‌شود.

۱. از SERVER01 خارج می‌شویم.

۲. سعی می‌کنیم با کاربر Administrator و کلمه عبور اشتباه به سیستم وارد شویم. این کار را یکی دوبار تکرار می‌کنیم.

۳. سپس با کلمه عبور صحیح به SERVER01 وارد می‌شویم.

تمرین ۳ بررسی وقایع Account Logon

در این تمرین وقایع تولید شده در اثر فعالیت‌های ورود کاربران در تمرین ۲ قابل مشاهده است.

۱. پنجره Event Viewer را از پوشه Administrative Tools باز می‌کنیم.

۲. گره Windows Logs را باز کرده و Security را انتخاب می‌کنیم.

۳. وقایع موفق و ناموفق را پیدا می‌کنیم.

خلاصه درس

- وقایع Account Logon در یک DC هنگام تایید هویت کاربران در هر کجای دامنه اتفاق می‌افتد.
- وقایع Logon روی سیستم‌هایی اتفاق می‌افتد که کاربر وارد می‌شود. برای مثال ورود به لپ تاپ و همچنین اتصال به یک فایل سرور منجر ثبت واقعه می‌شود.
- به طور پیش فرض سیستم‌های ویندوز سرور 2008 وقایع موفق logon و account logon را ممیزی می‌کند.
- برای بررسی وقایع account logon در دامنه باید به event log همان DC مراجعه کنیم.

سئوالات پایان درس

۱. می‌خواهیم یک log به دست آوریم که به ما کمک کند زمان‌های قفل شدن حساب کاربر را در اثر ورود ناموفق جدا کنیم. کدام سیاست باید پیکربندی شود؟

A. سیاست Audit Account Logon Events را برای وقایع موفق در Default Domain Policy GPO تعریف کنیم.

B. سیاست Audit Account Logon Events را برای وقایع ناموفق در Default Domain Policy GPO تعریف کنیم.

C. سیاست Audit Logon Events را برای وقایع موفق در Default Domain Policy GPO تعریف کنیم.

D. سیاست Audit Logon Events را برای وقایع ناموفق در Default Domain Policy GPO تعریف کنیم.

۲. می‌خواهیم زمان ورود کاربران را به کامپیوترها در بخش منابع انسانی در شرکت Adventure Works بررسی کنیم. کدام یک از روش‌های زیر به در به دست آوردن این اطلاعات کمک می‌کند؟

A. سیاستی را پیکربندی می‌کنیم که وقایع موفق account logon را در Default Domain Controllers GPO ممیزی کند. سپس event log اولین DC دامنه را بررسی می‌کنیم.

B. سیاستی را پیکربندی می‌کنیم که وقایع موفق logon را در GPO لینک شده به OU دربرگیرنده حساب کاربری کارکنان بخش منابع انسانی را ممیزی کند. سپس event logs همه کامپیوترهای بخش منابع انسانی را بررسی می‌کنیم.

C. سیاستی را پیکربندی می‌کنیم که وقایع موفق logon را در GPO لینک شده به OU دربرگیرنده حساب کامپیوتر کارکنان بخش منابع انسانی را ممیزی کند. سپس event logs همه کامپیوترهای بخش منابع انسانی را بررسی می‌کنیم.

D. سیاستی را پیکربندی می‌کنیم که وقایع موفق account logon را در GPO لینک شده به OU دربرگیرنده حساب کامپیوتر کارکنان بخش منابع انسانی را ممیزی کند. سپس event logs همه DC ها را بررسی می‌کنیم.

درس ۳: پیکربندی DC فقط خواندنی (Read-Only Domain Controllers)

دفاتر شرکت برای کارکنان بخش IT سازمان همیشه یک چالش به همراه دارند. وقتی یکی از دفاتر فرعی با دفتر اصلی با یک لینک WAN ارتباط دارد آیا درست است یک سرور DC در آنجا پیکربندی شود؟ در نسخه‌های قبلی ویندوز جواب دادن به این سوال ساده نبود. ولی ویندوز سرور 2008 نوع جدیدی از سرور DC را معرفی کرده که به آن سرور فقط خواندنی گویند(RODC). این سرور مشکل فوق را برطرف می‌سازد. در این درس مباحث مربوط به تایید هویت دفاتر فرعی سازمان و جایگزینی DC مطرح می‌شود و یاد می‌گیریم که یک سرور RODC را پیاده سازی و نگهداری کنیم.

بعد از این درس یاد می‌گیریم:

- نیازمندی‌های تجاری RODC را تشخیص دهیم.
- یک سرور RODC نصب کنیم.
- سیاست تکثیر کلمه عبور را پیکربندی کنیم.
- عملیات مربوط به cache کردن اعتبار را روی RODC را مانیتور کنیم.

زمان تقریبی: ۶۰ دقیقه

تایید هویت و جاگذاری DC در دفاتر فرعی شرکت

سناریویی را در نظر می‌گیریم که در آن یک سازمان دارای یک دفتر مرکزی و چند دفتر فرعی است. دفاتر فرعی از طریق لینک WAN که گران، کند و غیرمطمئن هستند به دفتر مرکزی متصل می‌باشند. کاربران در شاخه‌ها باید توسط Active Directory تایید هویت شوند. آیا باید یک سرور DC در آنجا قرار دهیم؟

در سناریوهای اینچنینی بسیاری از سرویس‌های شبکه در دفتر مرکزی تجمیع می‌شوند. دفتر مرکزی دقیقا توسط تیم IT کنترل می‌شود و دارای سرویس‌های امن می‌باشد. دفاتر فرعی معمولا از لحاظ امنیتی کامل نیستند و تیم فنی برای نگهداری سرور ندارند. وقتی در دفتر فرعی شرکت سرور DC موجود نباشد تایید هویت و فعالیت‌های مربوط به service ticket از طریق لینک WAN به سمت دفتر مرکزی هدایت می‌شود. تایید هویت زمانی اتفاق می‌افتد که کاربر به کامپیوتر وارد می‌شود. Service ticket ها جزئی از مکانیزیم تایید هویت Kerberos هستند که توسط دامنه ویندوز سرور 2008 استفاده می‌شوند. Service ticket را می‌توان کلیدی فرض کرد که توسط DC برای کاربر صادر می‌شود. کلید به کاربر اجازه می‌دهد به سرویس‌هایی نظیر سرویس File and

Print روی سرور فایل متصل شود. وقتی کاربر برای دسترسی به یک سرویس خاص اقدام می‌کند کلاینت کاربر درخواست دریافت service ticket را به DC می‌فرستد. چون کاربران معمولا در طول روز از سرویس‌های متعدد استفاده می‌کنند این پروسه چند بار تکرار می‌شود. عملیات تایید هویت و service ticket بین دفتر مرکزی و فرعی روی لینک WAN به کندی صورت می‌گیرد. به همین دلیل اگر یک سرور DC در دفتر فرعی قرار گیرد تایید هویت با کارایی بیشتری انجام می‌شود ولی خطراتی نیز به همراه دارد. سرور DC یک کپی از همه خصلت‌های همه اشیاء را مانند کلمات عبور کاربران نگه می‌دارد. اگر کسی به DC دست پیدا کند و یا دزدیده شود یک هکر می‌تواند نام‌های کاربری و کلمات عبور را به دست آورد. حداقل این است که مجبور می‌شویم کلمه عبور همه کاربران را تغییر دهیم. چون امنیت سرور در دفاتر فرعی معمولا از حالت نرمال پایین تر است سرور DC با خطرات اینچنینی مواجه است.

نگرانی دوم اینست که تغییرات در بانک اطلاعاتی Active Directory در DC دفتر فرعی روی همه دفاتر دیگر و دفتر مرکزی تکثیر می‌شود. بنابراین خرابی سرور یک دفتر باعث خرابی کل شبکه سازمان خواهد شد. مثلا اگر مدیر شبکه یکی از دفاتر به اشتباه فایل پشتیبان قدیمی سرور DC را بازیابی کند کل شبکه با مشکل مواجه می‌شود.

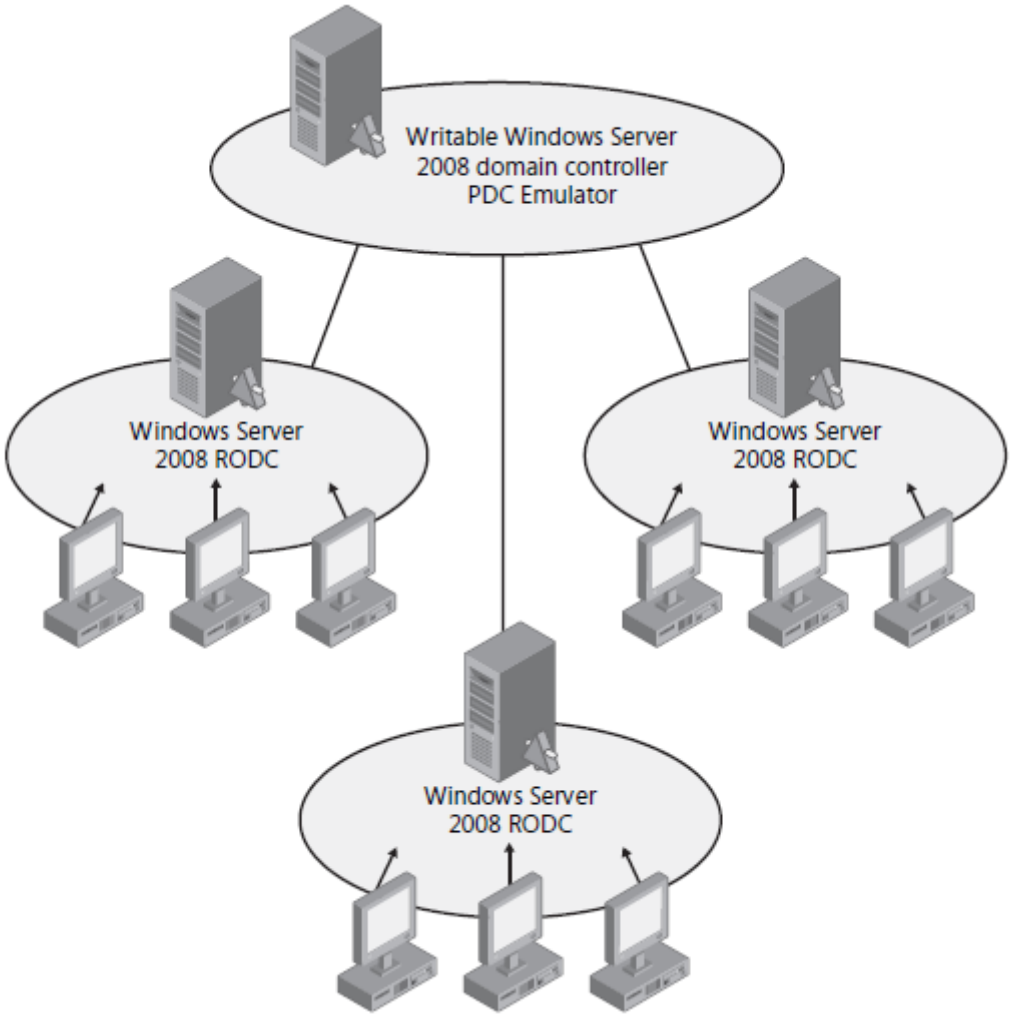
نگرانی سوم مدیریت شبکه می‌باشد. یک DC دفتر فرعی به نگهداری نیاز دارد. برای اجرای عملیات نگهداری روی DC باید با کاربر عضو گروه Administrators به آن وارد شویم. شاید مناسب نباشد که ما به تیم پشتیبانی در دفاتر فرعی چنین سطحی از توانایی را اعطاء کنیم.

DC فقط خواندنی (RODC)

مشکلات ذکر شده در بخش قبلی توسط RODC قابل حل است. RODC یک سرور DC است که در دفاتر فرعی سازمان قرار می‌گیرد و یک کپی از همه اشیاء دامنه و خصلت‌ها را غیر از موارد امنیتی مانند خصلت‌های مرتبط با کلمه عبور نگه می‌دارد. وقتی کاربری در این دفاتر وارد سیستم می‌شود RODC درخواست را دریافت کرده و آنرا جهت تایید هویت به سمت DC دفتر مرکزی ارسال می‌کند.

امکان این وجود دارد که یک سیاست تکثیر کلمه عبور (PRP) برای RODC پیکربندی کنیم که مشخص شود RODC مجاز به ذخیره چه حساب‌های کاربری می‌باشد. اگر کاربری که وارد سیستم می‌شود در PRP قرار داشته باشد RODC اعتبار آن کاربر را ذخیره می‌کند بنابراین دفعه بعد تایید هویت در محل و توسط خود RODC انجام می‌شود. این مفهوم در شکل ۷- ۸ شرح داده شده است.

چون RODC فقط گروهی از کاربران را نگهداری می‌کند وقتی به سرقت رود از لحاظ امنیتی خسارت محدود است و فقط کاربرانی که در RODC ذخیره شده‌اند باید کلمات عبورشان را تعویض کنند. DC های قابل تغییر (Writable) لیستی از همه حساب‌های ذخیره شده روی RODC های خاص را نگه می‌دارند. وقتی حساب سرور RODC به سرقت رفته را از Active Directory پاک می‌کنیم این امکان را خواهیم داشت که کلمات عبور همه کاربرانی که در RODC ذخیره شده‌اند ریست کنیم. RODC تغییرات اعمال شده روی Active Directory دفتر مرکزی را تکثیر می‌کند. تکثیر یک عمل یک طرفه از سمت DC قابل تغییر به سمت RODC است. تغییری که روی RODC ایجاد می‌شود به هیچ DC تکثیر نمی‌شود. این کار از تکثیر خطاهای ایجاد شده در DC دفاتر فرعی روی بقیه DC ها جلوگیری می‌کند. RODC ها برخلاف DC های قابل تغییر یک گروه Administrators محلی دارند. ما می‌توانیم به یک یا چند نفر از اعضاء تیم پشتیبانی (آنها را عضو این گروه کنیم) اجازه نگهداری سرور را به طور کامل اعطاء کنیم بدون این که عضو گروه Administrators دامنه باشند.



شکل ۷- ۸ سناریوی دفتر فرعی دارای RODC

توزیع RODC

مراحل کلی نصب یک سرور RODC به شرح زیر است:

۱. سطح عملیاتی forest باید ویندوز سرور 2003 یا بالاتر باشد.

۲. اگر forest دارای DC ویندوز سرور 2003 باشد دستور Adprep / rodcprep را اجرا می‌کنیم.

۳. باید حداقل یکی از DC های قابل تغییر ویندوز سرور 2008 باشد.

۴. RODC را نصب می‌کنیم.

هر کدام از این مراحل در بخش‌های زیر تشریح می‌شود.

تعیین و پیکربندی سطح عملیاتی forest ویندوز سرور 2003 یا بالاتر

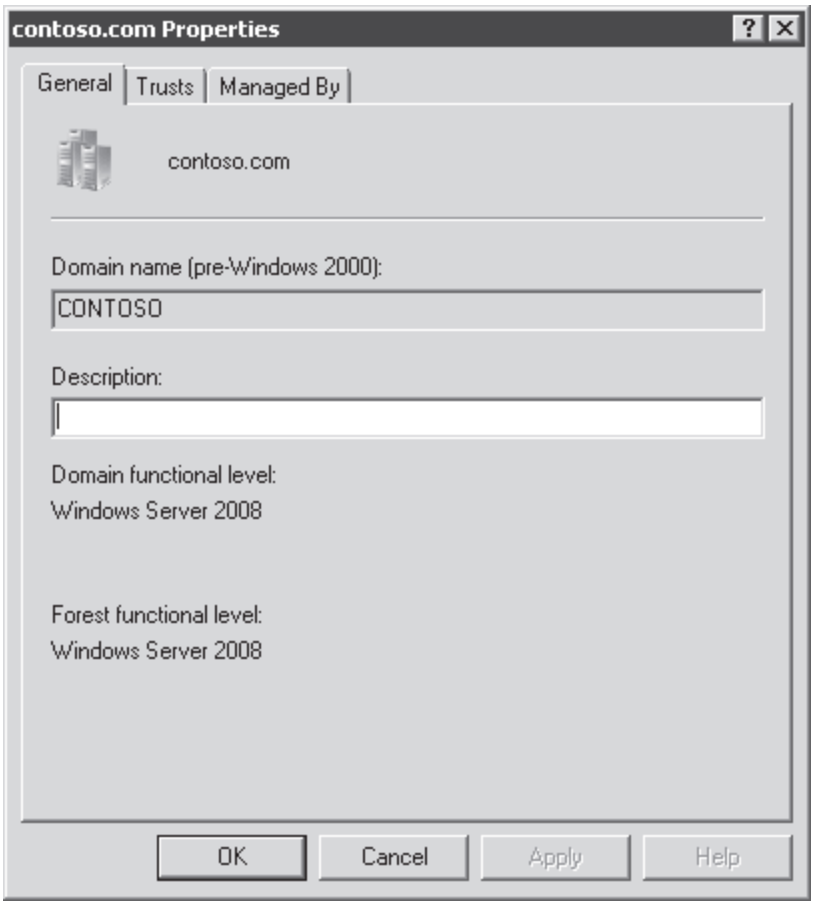
سطوح عملیاتی (Functional Levels) ویژگی‌های منحصر به یک نسخه ویندوز را فعال می‌کند و بنابراین به نسخه ویندوزی که روی DC نصب است وابستگی دارد. اگر همه DC ها ویندوز سرور 2003 یا بالاتر باشند سطح عملیاتی دامنه می‌تواند ویندوز سرور 2003 باشد. اگر همه دامنه‌ها دارای سطح عملیاتی دامنه ویندوز سرور 2003 باشند سطح عملیاتی forest می‌تواند ویندوز سرور 2003 باشد. سطح عملیاتی دامنه و forest در فصل ۱۲ شرح داده می‌شود.

RODC ها نیاز دارند سطح عملیاتی forest ویندوز سرور 2003 یا بالاتر باشد. یعنی همه DC ها در کل forest باید سرور 2003 یا بالاتر باشند. برای تعیین سطح عملیاتی forest ابزار Active Directory Domains And Trusts را باز کرده و

روی نام forest کلیک راست کرده Properties را انتخاب می‌کنیم. مانند شکل ۸- ۸ می‌توانیم سطح عملیاتی forest را تعیین کنیم.

اگر سطح عملیاتی forest حداقل ویندوز سرور 2003 نباشد properties همه دامنه‌ها را بررسی می‌کنیم تا ببینیم درکدام دامنه سطح عملیاتی از ویندوز سرور 2003 پایین‌تر است. وقتی چنین دامنه‌ای را پیدا کردیم باید مطمئن شویم همه DC ها در این دامنه ویندوز سرور 2003 دارند. سپس در Active Directory Domains And Trusts روی دامنه کلیک راست کرده و Raise Domain Functional Level را انتخاب می‌کنیم. در لیست بازشوی Select An Available Forest Functional Level ویندوز سرور 2003 را انتخاب کرده و روی دکمه Raise کلیک می‌کنیم. برای این کار باید administrator دامنه باشیم.

برای بالا بردن سطح عملیاتی forest باید یا عضو گروه Domain Admins در دامنه ریشه forest باشیم یا عضو گروه Enterprise Admins باشیم.



شکل ۸- ۸ کادر محاوره‌ای Properties مربوط به forest

اجرای دستور Adprep /rodcprep

اگر در حال ارتقاء forest با افزودن DC ویندوز سرور 2008 هستیم باید از این دستور استفاده کنیم. این دستور مجوزهایی را پیکربندی می‌کند که RODC ها بتوانند پارتیشن‌های دایرکتوری برنامه DNS را تکثیر کنند. این بحث در فصل ۹ ارائه می‌شود. اگر در حال ساخت یک forest جدید باشیم و فقط DC ویندوز سرور 2008 داشته باشیم نیازی به اجرای دستور Adprep /rodcprep نداریم.

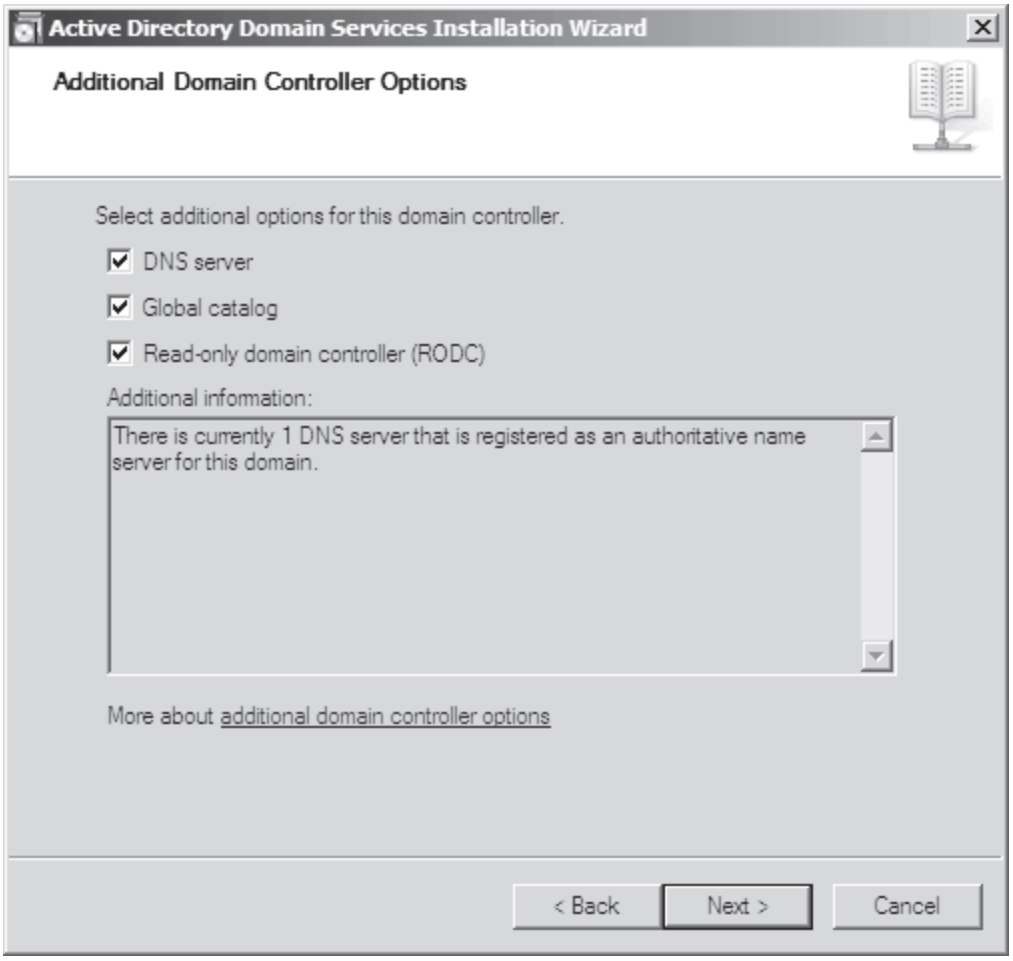
این دستور را می‌توانیم در پوشه cdrom\Sources\Adprep در DVD نصب سرور 2008 پیدا کنیم. پوشه را به DC که به عنوان schema master عمل می‌کند کپی می‌کنیم. نقش schema master در فصل ۱۰ شرح داده می‌شود. با کاربری که عضو گروه Enterprise Admins به schema master وارد می‌شویم و پنجره خط فرمان را باز می‌کنیم و مسیر را به پوشه Adprep تغییر می‌دهیم و تایپ می‌کنیم adprep /rodcprep

استقرار یک DC ویندوز سرور 2008 قابل تغییر

یک RODC باید تغییرات دامنه را از یک DC قابل تغییر دارای ویندوز سرور 2008 کپی کند. این خیلی حیاتی است که یک RODC بتواند با این DC ارتباط برقرار کند. در بهترین حالت این DC در نزدیک‌ترین سایت و دفتر مرکزی قرار دارد. در فصل ۱۱ درباره تکثیر Active Directory، سایت و لینک‌های سایت یاد می‌گیریم. اگر بخواهیم RODC به عنوان سرور DNS کار کند DC ویندوز سرور 2008 قابل تغییر باید میزبان DNS domain zone نیز باشد.

نصب RODC

پس از تکمیل مراحل ابتدایی می‌توانیم RODC را نصب کنیم. RODC می‌تواند به طور کامل یا Server Core نصب شود. با نصب کامل ویندوز سرور 2008 می‌توانیم برای نصب RODC از ویزارد Active Directory Domain Services Installation Wizard بهره بگیریم. برای این کار به سادگی همانند شکل ۹- ۸ در صفحه Additional Domain Controllers Options کادر Read-Only Domain Controller(RODC) را علامت می‌زنیم.



شکل ۹- ۸ ساخت یک RODC با ویزارد Active Directory Domain Services Installtion Wizard

به جای آن برای ساخت RODC می‌توان از دستور Dcpromo.exe با سوئیچ /Unattend استفاده کرد. در حالت نصب Server Core ویندوز سرور 2008 باید از این دستور و سوئیچ استفاده کنیم.

همچنین امکان اعطای اختیار نصب RODC ممکن است که کاربر غیر administrator را قادر می‌سازد از طریق افزودن یک سرور جدید در دفتر فرعی و اجرای دستور RODC Dcpromo.exe نصب کند. برای اعطای اختیار نصب RODC در Domain Controllers OU حساب کامپیوتر برای RODC می‌سازیم و اعتباری که برای افزودن RODC به دامنه مورد استفاده قرار می‌گیرد را مشخص می‌کنیم. این کاربر سپس می‌تواند یک سرور ویندوز 2008 را به حساب RODC attach کند. هنگام نصب RODC با استفاده از اختیار نصب، سرور باید عضو شبکه workgroup باشد.

سیاست تکثیر کلمه عبور

سیاست تکثیر کلمه عبور (PRP) تعیین می‌کند اعتبار کدام کاربر می‌تواند روی RODC ذخیره شود. اگر PRP به RODC اجازه ذخیره اعتبار کاربر را بدهد پروسه تایید هویت و service ticket آن کاربر توسط RODC پردازش می‌گردد. اگر اعتبار کاربری در RODC ذخیره نشود پروسه تایید هویت و service ticket توسط RODC به یک DC قابل تغییر ارجاع می‌شود.

PRP یک RODC توسط دو خصلت چند مقداره حساب کامپیوتر RODC تعیین می‌شود. این خصلت‌ها عبارتند از Allowed List و Denied List . اگر حساب کاربر در Allowed List باشد اعتبار کاربر ذخیره می‌شود. ما می‌توانیم به Allowed List گروه اضافه کنیم که در این حالت اعتبار همه کاربرانی که به گروه تعلق دارند در RODC ذخیره می‌شود. اگر کاربر هم در Allowed List باشد و هم در Denied List اعتبار کاربر ذخیره نمی‌شود.

پیکربندی سیاست تکثیر کلمه عبور در سطح دامنه

برای تسهیل مدیریت PRP ویندوز سرور 2008 دو گروه امنیتی domain local در Users container می‌سازد. گروه اول با نام Allowed RODC Password Replication Group به Allowed List همه RODC های جدید اضافه می‌شود. به طور پیش فرض گروه عضوی ندارد. بنابراین RODC جدید اعتبار هیچ کاربری را ذخیره نمی‌کند. اگر بخواهیم اعتبار کاربری در RODC ذخیره شود آنرا به گروه فوق اضافه می‌کنیم.

گروه دوم Denied RODC Password Replication Group نام دارد و به Denied List همه RODC های جدید اضافه می‌شود. اگر بخواهیم اعتبار کاربری هیچ گاه روی RODC ذخیره نشود آنرا به این گروه اضافه می‌کنیم. به طور پیش فرض حساب‌های کاربری امنیتی عضو این گروه هستند مانند Domain Admins، Enterprise Admins و Group Policy Creator Owners .

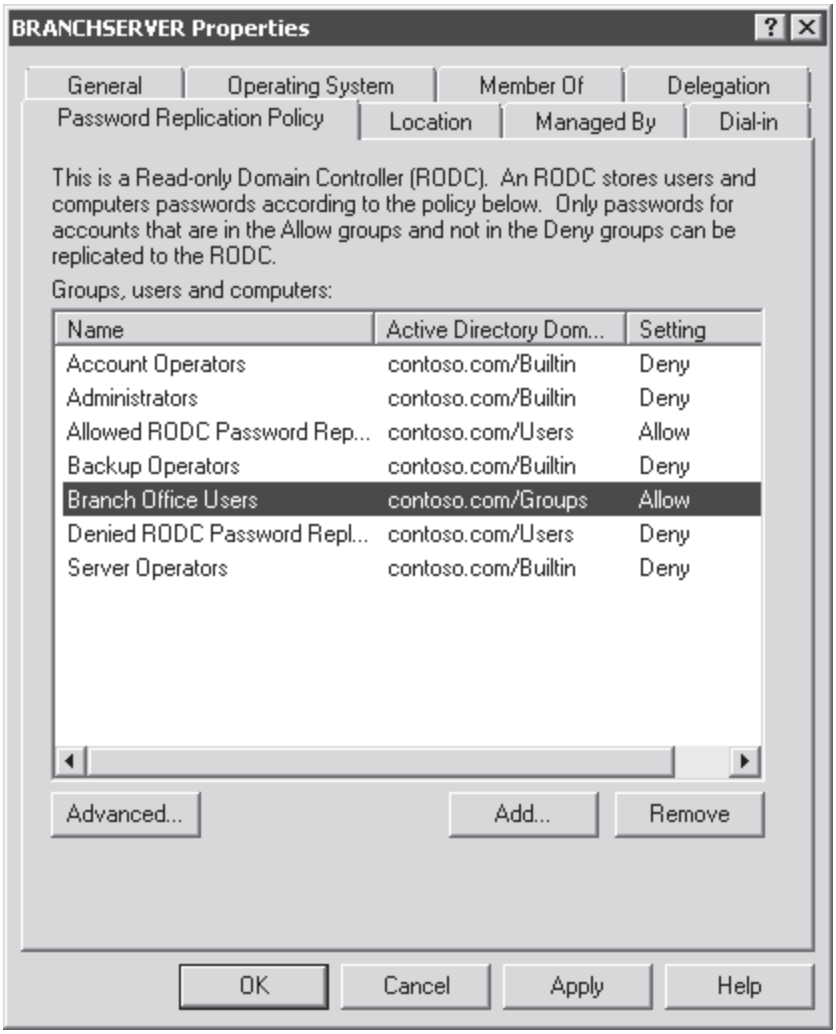
نکته رفتار کامپیوترها نیز مانند کاربران است

به خاطر داشته باشید فقط کاربران نیستند که پروسه نایید هویت و service ticket دارند. کامپیوترها نیز چنین پروسه ای را دارند. برای ارتقاء کارایی سیستم در دفتر فرعی به RODC اجازه ذخیره اعتبار کامپیوتر را نیز بدهید.

پیکربندی سیاست تکثیر کلمه عبور برحسب RODC خاص

دو گروه شرح داده شده در بخش قبل روشی را ارائه می‌دهند که بتوانیم PRP را روی همه RODC ها مدیریت کنیم. بهرحال برای پشتیبانی موثر از سناریوی دفاتر فرعی باید به RODC ها در دفاتر مختلف اجازه دهیم اعتبار کاربری و کامپیوتر را در محل‌های مشخصی ذخیره کنند. بنابراین باید Allowed List و Denied List همه RODC ها را پیکربندی کنیم.

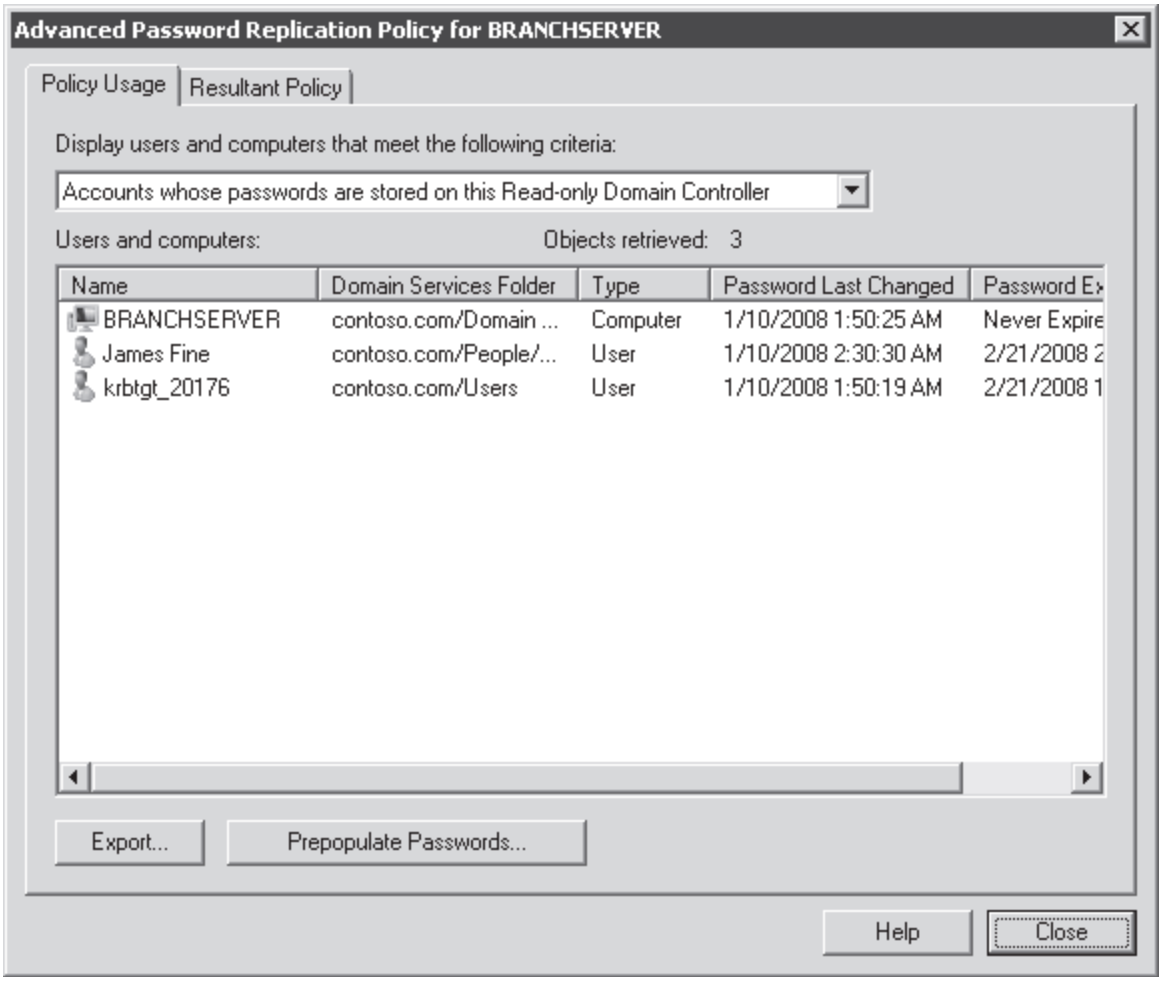
برای پیکربندی RODC PRP پنجره properties حساب کامپیوتر RODC را در Domain Controllers OU باز می‌کنیم. در زبانه Password Replication Policy که در شکل ۱۰- ۸ نشان داده شده است می‌توانیم تنظیمات PRP فعلی را مشاهده کرده و کاربر یا گروه مورد نظر را به PRP افزوده یا از آن حذف کنیم.



شکل ۱۰- ۸ زبانه Password Replication Policy یک RODC

مدیریت ذخیره سازی اعتبار در RODC

وقتی در زبانه Password Replication Policy مانند شکل ۱۰- ۸ دکمه Advanced را کلیک می‌کنیم کادر محاوره‌ای Advanced Password Replication Policy ظاهر می‌شود. مثالی از آن در شکل ۱۱- ۸ قابل مشاهده می‌باشد.



شکل ۱۱- ۸ کادر محاوره‌ای Advanced Password Replication Policy

لیست بازشوی بالای زبانه Policy Usage ما را قادر می‌سازد یکی از دو گزارش را برای RODC انتخاب کنیم:

- **Accounts Whose Passwords Are Stored On This Read-Only Domain Controller**

  لیستی از اعتبارات کاربران و کامپیوترها را نشان می‌دهد که در RODC ذخیره شده‌اند.با این لیست می‌توان تعیین کرد آیا اعتباراتی که ذخیره شده‌اند آنهایی هستند که باید ذخیره شوند یا نه.

- **Accounts That Have Been Authenticated To This Read-Only Domain Controller**

  لیستی از اعتبارات کاربران و کامپیوترها را نشان می‌دهد که برای تایید هویت به سرور DC قابل تغییر هدایت شده‌اند. از این لیست برای تشخیص کاربران یا کامپیوترهایی که برای تایید هویت روی RODC اقدام کرده‌اند استفاده کرد. اگر حسابی از این حساب‌ها ذخیره نشده‌اند آنها را به RODC اضافه می‌کنیم

در همان کادر زبانه Resultant Policy به ما امکان می‌دهد سیاست ذخیره‌سازی نهایی را برای یک کاربر یا کامپیوتر خاص ارزیابی کنیم. روی دکمه Add کلیک می‌کنیم تا حساب کاربر یا کامپیوتر برای ارزیابی انتخاب شود.

همچنین می‌توان از کادر محاوره‌ای Advanced Password Replication Policy برای ..... اعتبارات در RODC استفاده کرد. اگر کاربر یا کامپیوتری در allow list یک RODC باشد اعتبار آن می‌تواند روی RODC ذخیره شود ولی تا زمانی که تایید هویت یا service ticket اتفاق نیافتد و اعتبارها از یک سرور DC قابل تغییر RODC تکثیر نشود ذخیره نمی‌شود. با ..... اعتبارات در انباره RODC می‌توانیم مطمئن شویم روند تایید هویت حتی وقتی کاربر یا کامپیوتر برای اولین بار تایید هویت شود به صورت محلی روی سرور RODC انجام می‌شود. برای ..... اعتبارات روی دکمه Prepopulate Passwords کلیک کرده و کاربران و کامپیوترهای مورد نظر را انتخاب می‌کنیم.

مدیریت تفکیک نقش‌ها

RODC ها در دفاتر فرعی سازمان نیاز به عملیات نگهداری از قبیل نصب درایور سخت افزاری دارند. به علاوه دفاتر کوچک می‌توانند RODC را با نقش فایل سرور روی یک سیستم منفرد ترکیب کنند که در این حالت تهیه نسخه پشتیبان امری ضروری می‌باشد.
RODC ها توسط ویژگی با نام administrative role separation از مدیریت محلی پشتیبانی می‌کنند. هر RODC یک بانک اطلاعاتی شامل گروههایی برای اهداف مدیریتی خاص دارد. ما می‌توانیم کاربران دامنه را برای پشتیبانی از یک RODC خاص به این نقش‌های محلی اضافه کنیم.
ما می‌توانیم توسط دستور Dsmgmt.exe تفکیک نقش مدیریتی را پیکربندی کنیم. برای افزودن نقش Administrators به کاربر روی یک RODC مراحل زیر را دنبال می‌کنیم:

۱. پنجره خط فرمان را روی RODC باز می‌کنیم.

۲. دستور dsmgmt را تایپ کرده و کلید Enter را می‌زنیم.

۳. تایپ می‌کنیم local roles و کلید Enter را می‌زنیم. در خط فرمان با تایپ کاراکتر ؟ و زدن کلید Enter لیستی از دستورات نمایش داده می‌شود. همچنین می‌توانیم عبارت list roles را تایپ کرده و کلید Enter را بزنیم تا لیستی از نقش‌های محلی به نمایش درآید.

۴. تایپ می‌کنیم add username administrators که جای username نام pre-windows 2000 کاربر دامنه را تایپ کرده و کلید Enter را می‌زنیم.

برای افزودن کاربران دیگر می‌توانیم این مراحل را تکرار کنیم.

تمرینات پیکربندی RODC

در این تمرینات در یک محیط شبیه‌سازی شده دفتر فرعی یک RODC پیاده‌سازی می‌کنیم. یک RODC نصب کرده و سیاست تکثیر کلمه عبور را پیکربندی کرده ذخیره‌سازی اعتبارات را مانیتور کرده و اعتبارات را روی RODC ..... می‌کنیم. برای اجرای این تمرینات باید موارد زیر را تکمیل کنیم:

- یک سرور ثانوی ویندوز سرور 2008 نصب کنیم. نام سرور را BRANCH-SERVER قرار دهیم. پیکربندی پروتکل IP را به ترتیب زیر تنظیم می‌کنیم:
  - آدرس IP : 10.0.0.12
  - Subnet Mask : 255.255.255.0
  - Default Gateway : 10.0.0.1
  - DNS Server: 10.0.0.11 (آدرس SERVER01)
- اشیاء Active Directory زیر را ایجاد کنیم:
  - یک گروه امنیتی global با نام Branch Office Users
  - یک کاربر با نام James Fine که عضو گروه Branch Office Users باشد
  - یک کاربر با نام Adam Carter که عضو گروه Branch Office Users باشد.

- یک کاربر با نام Mike Danseglio که عضو گروه Branch Office Users نباشد.

- گروه Domain Users را عضو گروه Print Operators سازیم.

تمرین ۱ نصب RODC

در این تمرین سرور BRANCH SERVER را به عنوان یک RODC در دامنه contoso.com معرفی می‌کنیم.

۱. با کاربر Administrator به BRANCH SERVER وارد می‌شویم.

۲. منوی استارت را باز کرده و روی Run کلیک می‌کنیم.

۳. تایپ می‌کنیم dcpromo و OK می‌کنیم. پنجره‌ای برای مبنی بر نصب Active Directory Domain Services binaries باز می‌شود. وقتی نصب تمام شد ویزارد Active Directory Domain Services Installation ظاهر می‌شود.

۴. روی Next کلیک می‌کنیم.

۵. در صفحه Operating System Compatibility روی Next کلیک می‌کنیم.

۶. در صفحه Choose A Deployment Configuration گزینه Existing Forest را انتخاب کرده و سپس Add A Domain Controller To An Existing Domain را انتخاب می‌کنیم.

۷. در صفحه Network Credentials تایپ می‌کنیم contoso.com

۸. روی دکمه Set کلیک می‌کنیم.

۹. در کادر User Name تایپ می‌کنیم Administrator

۱۰. در کادر Password کلمه عبور Administrator دامنه را تایپ کرده و OK می‌کنیم.

۱۱. روی Next کلیک می‌کنیم

۱۲. در صفحه Select A Domain گزینه contoso.com را انتخاب کرده و Next را می‌زنیم.

۱۳. در صفحه Select A Site ، Default-First-Site-Name را انتخاب و Next می‌کنیم. در محیط شبکه واقعی سایت دفتر فرعی شرکت که در آن RODC نصب شده انتخاب می‌شود. سایت‌ها در فصل ۱۱ بررسی می‌شوند.

۱۴. در صفحه Additional Domain Controller Options گزینه Read-Only Domain Controller(RODC) را انتخاب می‌کنیم. همچنین مطمئن می‌شویم DNS Server و Global Catalog انتخاب شده‌اند. سپس روی Next کلیک می‌کنیم.

۱۵. در صفحه Delegation Of RODC Installation And Administration روی Next کلیک می‌کنیم.

۱۶. در صفحه Location For Database,Log Files,And SYSVOL روی Next کلیک می‌کنیم.

۱۷. در صفحه Directory Services Restore Mode Administrator Password کلمه عبوری را در کادرهای Password و Confirm Password تایپ کرده و دکمه Next را می‌زنیم.

۱۸. در صفحه Summary روی Next کلیک می‌کنیم.

۱۹. در پنجره بعد کادر Reboot On Completion را علامت می‌زنیم.

تمرین ۲ پیکربندی سیاست تکثیر کلمه عبور

در این تمرین PRP را در سطح دامنه و برای یک RODC مشخص پیکربندی می‌کنیم. PRP تعیین می‌کند اعتبار کاربر یا کامپیوتر روی RODC ذخیره شود یا نه.

۱. با کاربر Administrator به SERVER01 وارد می‌شویم.

۲. ابزار Active Directory Users And Computers را باز می‌کنیم.

۳. گره دامنه را باز کرده و Users container را انتخاب می‌کنیم.

۴. عضویت پیش فرض گروه Allowed RODC Password Replication را بررسی می‌کنیم.

۵. پنجره properties گروه Denied RODC Password Replication را باز می‌کنیم.

۶. گروه DNS Admins را به گروه Denied RODC Password Replication اضافه می‌کنیم.

۷. Domain Controllers OU را انتخاب می‌کنیم.

۸. پنجره properties مربوط به BRANCHSERVER را باز می‌کنیم.

۹. روی زبانه Password Replication policy کلیک می‌کنیم.

۱۰. تنظیمات PRP هر دو گروه را (Allowed RODC Password Replication – Denied RODC Password Replication) چک می‌کنیم.

۱۱. روی دکمه Add کلیک می‌کنیم.

۱۲. گزینه Allow Passwords For The Account To Replicate To This RODC را انتخاب کرده و OK می‌کنیم.

۱۳. در کادر محاوره‌ای Select Users,Computers,Or Groups تایپ می‌کنیم Branch Office Users و OK می‌کنیم.

۱۴. دوباره OK را کلیک می‌کنیم.

تمرین ۳ مانیتور کردن ذخیره سازی اعتبار

در این تمرین قرار است ورود کاربران متعدد به سرور دفتر فرعی شرکت را مانیتور کنیم. سپس می‌توانیم ذخیره شدن اعتبارات را روی سرور ارزیابی کنیم.

۱. با کاربر James Fine به سرور BRANCHSERVER وارد شده و خارج می‌شویم.

۲. با کاربر Mike Danseglio به سرور BRANCHSERVER وارد شده و خارج می‌شویم.

۳. با کاربر Administrator به سرور SERVER01 وارد شده و ابزار Active Directory Users And Computers را باز می‌کنیم.

۴. پنجره properties سرور BRANCHSERVER را در Domain Controllers OU باز می‌کنیم.

۵. روی زبانه Password Replication Policy کلیک می‌کنیم.

۶. روی دکمه Advanced کلیک می‌کنیم.

۷. در زبانه Policy Usage در لیست بازشوی Display Users And Computers That Meet The Following Criteria گزینه Accounts Whose Passwords Are Stored On This Read-Only Domain Controller را انتخاب می‌کنیم.

۸. entry مربوط به james Fine را پیدا می‌کنیم.

۹. در لیست بازشوی صفحه گزینه Accounts That Have Been Authenticated To This Read-Only Domain Controller را انتخاب می‌کنیم.

۱۰. entry مربوط به کاربر James Fine و Mike Danseglio را پیدا می‌کنیم.

۱۱. روی Close و سپس OK کلیک می‌کنیم.

تمرین ۴ Cache کردن اعتبارات

در این تمرین می‌خواهیم ذخیره RODC را با اعتبار کاربر cache کنیم.

۱. با کاربر Administrator به SERVER01 وارد شده و ابزار Active Directory Users And Computers را باز می‌کنیم.

۲. در Domain Controllers OU پنجره properties مربوط به BRANCHSERVER را باز می‌کنیم.

۳. زبانه Password Replication Policy را باز می‌کنیم.

۴. روی دکمه Advanced کلیک می‌کنیم.

۵. روی دکمه Prepopulate Passwords کلیک می‌کنیم.

۶. تایپ می‌کنیم Adam Carter و OK می‌کنیم.

۷. روی Yes کلیک می‌کنیم تا ارسال اعتبار به RODC تایید گردد.

۸. در زبانه Policy Usage گزینه Accounts Whose Passwords Are Stored On This Read-Only Domain Controller را انتخاب می‌کنیم.

۹. entry مربوط به Adam Carter را پیدا می‌کنیم. اعتبار Adam الان روی RODC ذخیره شده است.

۱۰. روی دکمه OK کلیک می‌کنیم.

خلاصه درس

- RODC شامل یک کپی فقط خواندنی از بانک اطلاعاتی Active Directory می‌باشد.
- یک RODC تغییرات را از یک سرور DC قابل تغییر با استفاده از روش تکثیر inbound-only به روز می‌کند.
- سیاست تکثیر کلمات عبور تعیین می‌کند اعتبار یک کاربر یا کامپیوتر روی RODC ذخیره شود یا نه. دو گروه Allowed RODC Password Replication و Denied RODC Password Replication به ترتیب در Allowed List و Denied List یا در هر RODC جدید قرار دارند. بنابراین از دو گروه برای مدیریت یک سیاست تکثیر کلمه عبور در سطح دامنه بهره می‌بریم. به علاوه می‌توانیم برای هر DC یک PRP مخصوص پیکربندی کنیم.
- با پیکربندی تفکیک نقش‌های مدیریتی شبکه می‌توانیم یک یا چندکاربر را موظف به پشتیبانی از RODC کنیم بدون اینکه مجوز سطح بالای شبکه را به آنها اعطاء کنیم. دستور Dsmgmt.exe کار تفکیک نقش‌های مدیریتی را انجام می‌دهد.
- یک RODC نیاز به یک DC ویندوز سرور 2008 قابل تغییر در همان دامنه دارد. به علاوه سطح عملیاتی forest نیز باید حداقل ویندوز سرور 2003 باشد و دستور Adprep /rodcprep باید قبل از نصب اولین RODC اجرا شود.

سئوالات پایان درس

۱. دامنه شما شامل ۵ DC می‌باشد که یکی از آنها ویندوز سرور 2008 نصب دارد. سیستم عامل همه DC های دیگر ویندوز سرور 2003 است. برای نصب RODC چه باید بکنیم؟

A. همه DC را به ویندوز سرور 2008 ارتقا دهیم.

B. دستور Adprep /rodcprep را اجرا کنیم.

C. دستور Dsmgmt ار اجرا کنیم.

D. دستور Dcpromo /unattend را اجرا کنیم.

۲. فرض کنید در طول یک سرقت که اخیرا در یکی از دفاتر فرعی شرکت Tailspin Toys اتفاق افتاده است RODC به سرقت رفته است. از کجا متوجه می‌شویم اعتبار کدام کاربر در RODC ذخیره شده بوده است؟

A. به زبانه Policy Usage مراجعه می‌کنیم.

B. به عضویت گروه Allowed RODC Password Replication توجه می‌کنیم.

C. به عضویت گروه Denied RODC Password Replication توجه می‌کنیم.

D. به زبانه Resultant Policy مراجعه می‌کنیم.

۳. هفته آینده ۵ نفر از اعضای شرکت Litware, Inc به یکی از ده دفتر فرعی شرکت منتقل می‌شوند. هر دفتر فرعی یک RODC دارد. می‌خواهیم مطمئن شویم وقتی کاربران برای اولین بار وارد شبکه می‌شوند مشکلی با تایید اعتبار از طریق لینک WAN با Data Center ندارند. کدام یک از موارد زیر باید اجرا شود؟ (در صورت صحت همه را انتخاب می‌کنیم.)

A. هر ۵ کاربر را به گروه Allowed RODC Password Replication اضافه می‌کنیم.

B. هر ۵ کاربر را به زبانه Password Replication Policy مربوط به RODC دفتر فرعی اضافه می‌کنیم.

C. هر ۵ کاربر را به سیاست امنیتی Log On Locally مربوط به Default Domain Controllers Policy GPO اضافه می‌کنیم.

D. روی Prepopulate Passwords کلیک می‌کنیم.

فصل ۹

عجین کردن Domain Name System با AD DS

بدون سیستم تحلیل نام دامنه (DNS) استفاده از اینترنت آسان نخواهد بود. ما همچنان از اینترنت استفاده می‌کنیم چون بستر فن‌آوری آن TCP/IP است ولی رسیدن به مقصد http://207.46.198.248 کاملا شبیه http://Technet.microsoft.com نیست مخصوصا وقتی آدرس را در مرورگر خود تایپ می‌کنیم. وقتی در Windows Live Search عبارت Windows Server 2008 را جستجو می‌کنیم و مجموعه‌ای از آدرس‌های IP را که میزبان اطلاعات مورد نظر ما هستند دریافت می‌کنیم هیچ شناختی نسبت به این سایت‌ها نمی‌توانیم داشته باشیم. آدرس‌های IP به اندازه نام دامنه برای ما معنی ندارند.

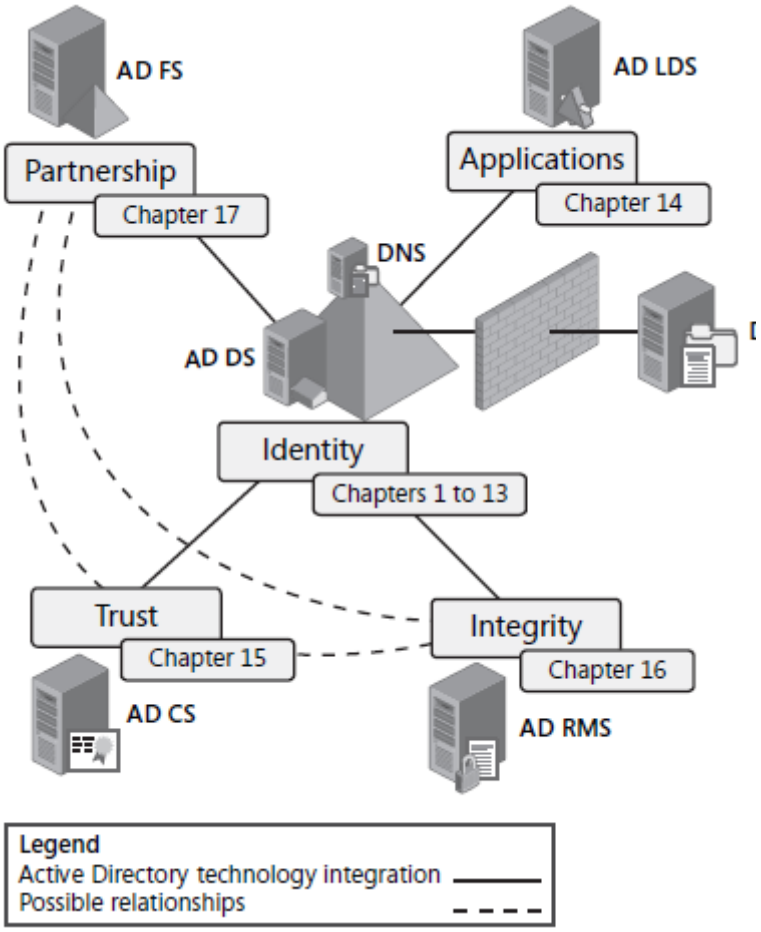
دلیل اینکه ما به DNS متکی هستیم اینست که آدرس IP را به واژه‌های آشنا یا نام دامنه ترجمه می‌کند که انسان آنها را درک می‌کند. در حقیقت DNS در مرکز پروتکل TCP/IP قرار دارد چه در نسخه IP4 سنتی با شمای آدرس ۳۲ بیت و چه در IPv6 جدید با شمای آدرس دهی ۱۲۸ بیت که در ویندوز سرور 2008 نهادینه شده است. هر زمان که سیستمی را در شبکه راه‌اندازی می‌کنیم با آدرس یا آدرس‌های IP شناخته می‌شود. در شبکه ویندوز سرور 2008 با سرویس AD DS همه دستگاههایی که به دایرکتوری لینک شده‌اند به سیستم تحلیل نام DNS نیز لینک می‌شوند و برای استفاده از همه سرویس‌های مورد نیاز به آن متکی هستند.

برای مثال وقتی کامپیوتری راه‌اندازی می‌شود که در دامنه واقع است یک پروسه مشخص اتفاق می‌افتد. شروع این پروسه با تشخیص service location record (SRV) از سرور DNS می‌باشد که برای پیدا کردن نزدیک‌ترین DC استفاده می‌شود. پس از اتمام کار DNS پروسه تایید هویت بین کامپیوتر و DC آغاز می‌شود. بهرحال بدون تحلیل نام برای SRV توسط DNS تایید هویت کامپیوتر عضو دامنه برای AD DS مشکل خواهد بود.

به دلیل اینکه این سرویس کار تبدیل آدرس IP را به نام انجام می‌دهد تبیین استانداردهای برنامه‌نویسی را به واسطه وجود نام در برنامه ممکن می‌کند. وقتی برنامه‌نویسان می‌دانند که به یک پروسه نیاز دارند که کار کشف یک سرویس مشخص را دارد از نام رایج برای آن

سرویس استفاده می‌کنند. پس وقتی مشتری نرم‌افزار همراه برنامه جدید سرویس DNS راه‌اندازی می‌کند DNS نام کامپیوتر میزبان سرویس را به آدرس IP تبدیل می‌کند.

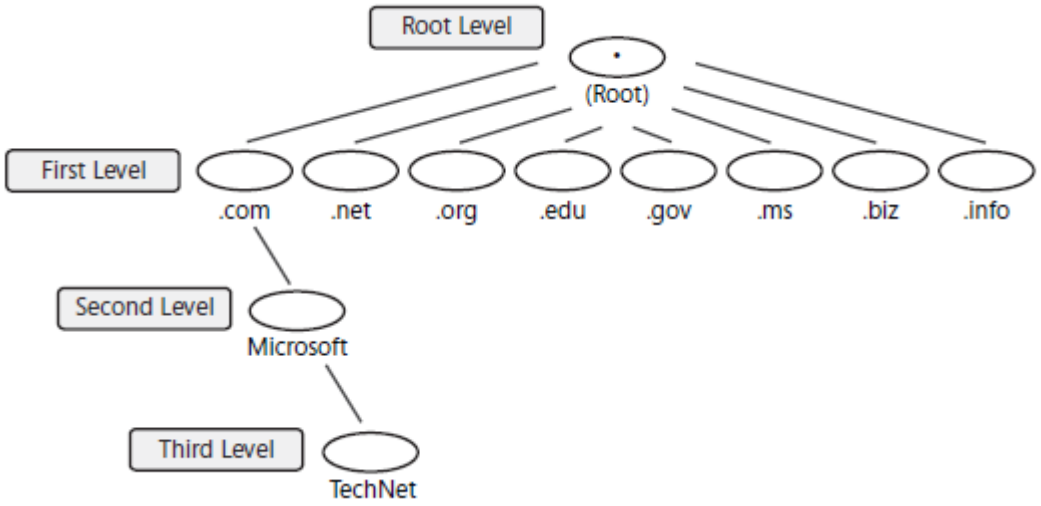
به علاوه چون این فن‌آوری برای مدیریت نام در اینترنت طراحی شده یکی از فن‌آوری‌های ارائه شده در ویندوز سرور 2008 است که قدرت ما را در شبکه به سمت اینترنت افزایش می‌دهد. DNS همانند AD CS، AD RMS ، AD LDS و AD FS با AD DS عجین شده ولی به صورت مستقل نیز می‌تواند در شبکه DMZ یا Perimeter و یا حتی پشت آن پیاده‌سازی شود. (شکل ۱- ۹ را ملاحظه کنید) وقتی این اتفاق می‌افتد به دیگران امکان می‌دهد ما را در هر جای دنیا پیدا کنند. وقتی ما را پیدا می‌کنند می‌توانند با ما یا برنامه‌های به اشتراک گذاشته شده ارتباط برقرار کنند.



شکل ۱- ۹ DNS قدرت ما را تا آنسوی مرزهای شبکه خودمان توسعه می‌دهد.

DNS صرف نظر از اینکه در شبکه محلی استفاده شود یا اینترنت از پورت TCP/IP 53 استفاده می‌کند. همه کلاینت‌ها و سرورها برای دستیابی به اطلاعات نام کامپیوترهای مورد نیازشان از این پورت استفاده می‌کنند.

ساختار نام مورد استفاده در DNS سلسله مراتبی است. نام‌ها با یک ریشه شروع می‌شوند و وقتی به این ساختار ردیفی اضافه می‌شود توسعه می‌یابند. ریشه واقعی ساختار سلسله مراتبی DNS خود نقطه (.) است. هر چند در نام‌های اینترنت استفاده نمی‌شود. به طور عادی نام‌های ریشه استاندارد در اینترنت ثبت می‌شود و شامل نام‌های .com, .biz, .net, .info, .name, .ms, .edu, .gov, .org و غیره می‌باشد. سازمان‌ها از طریق اتصال (bind) یک نام رایج با نام ریشه به اینترنت متصل می‌شوند برای مثال همان‌طوری که در شکل ۲- ۹ می‌بینید Microsoft.com از نام ریشه دو سطح پایین‌تر است و از ریشه واقعی DNS سه سطح پایین‌تر است. Technet.microsoft.com از نام ریشه سه سطح و ریشه DNS چهار سطح پایین‌تر است و به همین ترتیب. AD DS برای ایجاد ساختار دامنه یک forest به این سلسله مراتب نیاز دارد.



شکل ۲- ۹ سلسله مراتب DNS در اینترنت

DNS و IPv6

در ویندوز سرور 2008 ، DNS برای عجین شدن با IPv6 به روز شده است. برخلاف IPv4 که از چهار octet ۸ بیتی برای آدرس تشکیل شده بود IPv6 از ۸ قطعه ۱۶ بیتی تشکیل شده که IP ۱۲۸ بیتی را می‌سازد که اغلب در قالب هگزادسیمال نمایش داده می‌شود. برای مثال FE80:: به آدرس اتوماتیک link-local نسخه IPv6 ویندوز ویستا یا سرور 2008 اشاره می‌کند. یک دستگاه زمانی این آدرس را می‌گیرد که برای دریافت IP از سرور DHCP پیکربندی شده باشد ولی هیچ سروری در دسترس نباشد. این آدرس مشابه آدرس APIPA در IPv4 می‌باشد.

در IPv6 هر زمان یک قطعه آدرس ۱۶ بیتی تماما دارای صفر است می‌توانیم آدرس را خلاصه کنیم و با دو کولن (::) آنرا نمایش دهیم. این علامت نمایانگر چند بخش ۱۶ بیت است که از صفر تشکیل شده و پشت سرهم می‌باشد. این کار نوشتن آدرس‌های IPv6 را ساده می‌کند.

IPv6 همانند IPv4 انواع متعددی دارد:

- **Link-local** آدرس‌هایی هستند که از طریق آن همسایگان مستقیم با هم ارتباط برقرار می‌کنند . هر کامپیوتری در یک بخش از شبکه با هر کامپیوتر درهمان بخش از این طریق می‌تواند ارتباط برقرار کند. این آدرس به طور پیش فرض وقتی اختصاص می‌یابد که IPv6 فعال است ولی از آدرس ثابت استفاده نمی‌کند و با سرور DHCP نیز نمی‌تواند ارتباط برقرار کند. این آدرس‌ها شبیه به آدرس‌های 169.254.0.0/16 هستند که توسط پروسه APIPA استفاده می‌شوند.

- **Site-local** آدرس‌هایی private هستند که قابل مسیریابی بوده ولی در فضای اینترنت قابل استفاده نیستند. در IPv4 آدرس‌های معادل عبارتند از : 10.0.0./8 و 172.16.0.0/12 و 192.168.0.0/16 .

- **Global unicast** آدرس‌هایی هستند که به طور کل منحصر بفرد بوده و در فضای اینترنت قابل استفاده هستند. این آدرس‌ها در اینترنت قابل مسیریابی بوده و با بقیه سیستم‌ها ارتباط مستقیم دارند. معادل این آدرس‌ها در IPv4 آدرس‌های معتبر اینترنتی فعلی می‌باشند.

مزیت IPv6 در تعداد زیاد آدرس‌های آن است. با انفجار جمعیت جهان، تعداد سرویس‌ها دستگاههایی که به آدرس IP نیاز دارند و کاهش تعداد رو به کاهش آدرس‌های IPv4 آزاد زمان آن رسیده است که زیرساخت IP اینترنت به مرحله جدیدی وارد شود. IPv6 با فراهم کردن ۳۴۰ میلیارد میلیارد یا 2^{128} آدرس برای مدت طولانی اینترنت را از لحاظ تعداد آدرس بیمه می‌کند. این تعداد در مقایسه با تعداد آدرس IPv4 که ۴ میلیارد آدرس دارد بسیار بیشتر است.

جدول ۱- ۹ انواع معمول آدرس IPv6

نوع آدرس	قالب	شرح
نامشخص	::	بدون آدرس معادل آدرس 0.0.0.0 در IPv4
Loopback	::1	آدرس Loopback را نشان می‌دهد. امکان ارسال پکت به خود سیستم را می‌دهد. معادل آن در IPv4 ، 127.0.0.1 می‌باشد.
Link-Local	FE80::	فقط برای ارتباط با آدرس محلی استفاده می‌شود. با آدرس APIPA یا 169.254.0.0/16 در IPv4 مقایسه می‌شود. در IPv6 قابل مسیریابی نیست.
Site-Local	FEC0::	قابل مسیریابی است ولی نه در اینترنت. با آدرس‌های 10.0.0.0/8 و 172.16.0.0/12 و 192.168.0.0/16 در IPv4 قابل مقایسه است.
Global Unicast	مابقی	آدرس‌های منحصر که به یک میزبان اختصاص می‌یابد.

DNS برای سازگاری با استانداردهای اینترنت و پشتیبانی از گذر به سوی IPv6 در ویندوز سرور 2008 از آدرس‌های طولانی IPv6 پشتیبانی می‌کند. IPv6 به صورت پیش فرض هم در ویندوز ویستا و هم سرور 2008 نصب و فعال می‌شود. این بدین معنی است که ما می‌توانیم با کمترین ریسک از این فن‌آوری استفاده کنیم. روزی فرا می‌رسد که برای ورود به اینترنت قبل از مقدماتی نظیر Intrusion Detection System ، فایروال ، فیلترینگ ضد اسپم و غیره باید از آدرس IPv6 که امن‌تر از IPv4 است استفاده کنیم.

اطلاعات بیشتر IPv6

برای اطلاعات بیشتر درباره IPv6 به آدرس http://www.microsoft.com/technet/network/ipv6/ipv6rfc.mspx مراجعه کنید.

پروتکل Peer Name Resolution Protocol

ویندوز ویستا و سرور 2008 برای پشتیبانی کامل از IPv6 یک سیستم تحلیل نام عادی نیز به نام Peer Name Resolution Protocol (PNRP) دارند. برخلاف DNS که بر اساس ساختار نام سلسله مراتبی کار می‌کند این پروتکل از سیستم یک سطحی برای تحلیل نام استفاده می‌کند. اساسا PNRP یک سیستم ارجاعی است که جستجو را بر اساس داده موجود انجام می‌دهد. برای مثال اگر بخواهیم کامپیوتر A را پیدا کنیم و خودمان نزدیک کامپیوترهای B و C باشیم سیستم ما از کامپیوتر B سوال می‌کند که آیا کامپیوتر A را می‌شناسد. اگر جواب کامپیوتر B بله بود ارتباط ما را با کامپیوتر A فراهم می‌کند. وگرنه سیستم ما از کامپیوتر C همان سوال را می‌پرسد. و به همین ترتیب ادامه می‌یابد تا کامپیوتر A پیدا شود.

PNRP دارای ویژگی‌هایی است که آنرا از سرویس DNS متمایز می‌کند:

- این یک سیستم تحلیل نام توزیع شده بوده و متکی به یک سرور مرکزی نیست. عمدتا بدون سرور کار می‌کند ولی در بعضی موارد از سرور برای ارتقاء تحلیل نام استفاده می‌شود. ویندوز سرور 2008 از سرور PNRP به عنوان یک ویژگی add-on پشتیبانی می‌کند.

- برخلاف DNS که تعداد کمی نام را میزبانی می‌کند و برای بیش از آن به سرورهای DNS دیگر متکی است و به آنها احاطه ندارد مقیاس PNRP تا میلیاردها نام را پشتیبانی می‌کند.

- چون توزیع شده است و به اندازه سرور به کلاینت‌ها نیز متکی است تحمل خرابی (fault tolerant) دارد. کامپیوترهای متعددی می‌توانند نام‌های مشابه را میزبانی کنند و در صورت عدم دسترسی به یکی دیگری کار تحلیل نام را انجام می‌دهد.

- انتشار نام فوری و آزاد است و مانند DNS نیازی به دخالت مدیریتی ندارد.

- برخلاف DNS نام‌ها در لحظه به روز می‌شوند و cache کردن به شدت به کارایی کمک می‌کند. به همین دلیل PNRP مانند DNS مخصوصا از نوع سرور غیرپویا آدرس‌های قدیمی را برنمی‌گرداند.

- PNRP همچنین از نام‌گذاری سرویس‌ها مانند کامپیوترها پشتیبانی می‌کند چون نام PNRP (PNRP Name) شامل آدرس، پورت و یک potentioal payload نظیر عملکرد یک سرویس می‌باشد.

- نام‌های PNRP از طریق امضای دیجیتال قابل محافظت هستند. حفاظت نام در این روش از جابجایی و تقلب از طرف کاربران بداندیش جلوگیری می‌کند.

PNRP برای فراهم کردن سرویس‌های تحلیل نام از مفهوم ابر استفاده می‌کند. دو نوع ابر متفاوت وجود دارند. اول ابر global که همه آدرس‌های IPv6 و در نتیجه کل اینترنت را دربر می‌گیرد. دوم ابر link-local است که بر حوزه آدرس‌های IPv6 منطبق است. لینک‌های محلی اغلب یک شبکه واحد را نمایندگی می‌کنند. تعداد زیادی از این ابرها می‌تواند وجود داشته باشد ولی ابر global فقط یکی است.
همانطوریکه در دنیای واقعی کاملا به IPv6 نرسیده‌ایم PNRP نیز همه‌گیر نشده و هنوز شبکه‌ها به DNS متکی هستند. بهرحال PNRP یک فن‌آوری مهم جدید است که با حرکت به سمت IPv6 تاثیر آن روی اینترنت بیشتر و بیشتر می‌شود.

اطلاعات بیشتر PNRP

برای اطلاعات بیشتر درباره PNRP به آدرس http://technet.microsoft.com/en-us/library/bb726971.aspx مراجعه کنید.

ساختار DNS

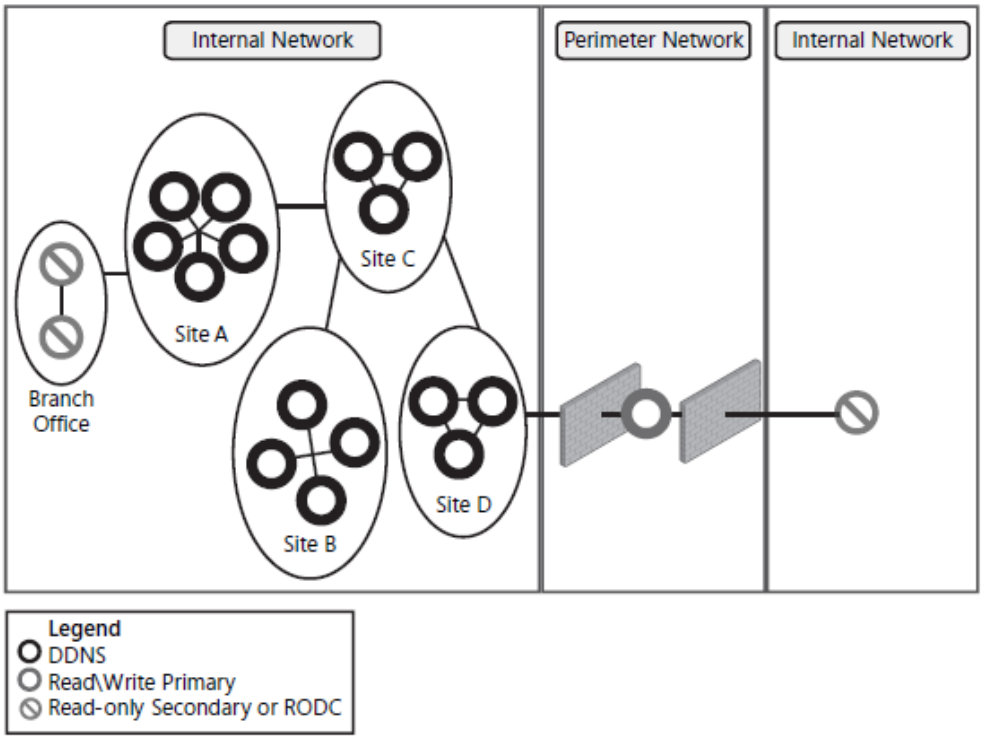
DNS همراه اینترنت و با آن توسعه پیدا کرد. به همین خاطر این سرویس در ویندوز سرور 2008 چند نقش را ایفا می‌کند. سه نوع سرور DNS موجود است:

- **Dynamic DNS server**یا سرور DNS پویا. سرورهایی که برای ثبت نام حجم وسیعی از دستگاهها از طریق به روز رسانی پویا طراحی شده‌اند DDNS نام می‌گیرند. این سرورها برای این طراحی شده‌اند که کلاینت‌ها و سرورها نام و IP خود را در آن ثبت کنند تا بقیه بتوانند آنها را پیدا کنند. وقتی سرویس DNS روی DC اجرا و با سرویس دایرکتوری عجین می‌شود در حالت DDNS قرار می‌گیرد و کامپیوترها را قادر می‌سازد که از DHCP برای ثبت نام‌شان به طور خودکار استفاده کنند. این کار AD DS را قادر می‌سازد هنگام ارسال اطلاعات مدیریتی نظیر GPO کلاینت را پیدا کند. سرورهای DDNS سرورهای خواندنی نوشتنی هستند ولی ثبت‌نام‌ها را فقط از رکوردهای شناخته شده قبول می‌کند.

- **Read-Write DNS Servers** به آن سرورهای DNS خواندنی نوشتنی می‌گویند. سرورهای DNS قدیمی که در حالت پویا کار نمی‌کنند ولی تغییرات را از منابع شناخته شده قبول می‌کنند سرورهای DNS خواندنی نوشتنی نام دارند. رایج‌ترین نوع آن سرور DNS اولیه (Primary) می‌باشد. این سرورها معمولا در شبکه‌های DMZ یا Perimeter توزیع شده و با AD DS عجین (integrate) نمی‌شوند.

- **Read-only DNS Servers** یا سرورهای DNS فقط خواندنی یک کپی فقط خواندنی از اطلاعات DNS را نگه می‌دارد که از محل دیگری دریافت کرده است. در ویندوز سرور 2008 دو نوع از این سرویس وجود دارد. اول سرور DNS ثانویه (Secondary DNS Server) است که به سرورهای DNS اولیه لینک می‌شوند و اطلاعات DNS فراهم شده توسط سرور والد اولیه را قبول و میزبانی می‌کند. این سرورها اطلاعات را به صورت محلی در دسترس قرار می‌دهند ولی نمی‌توانند اطلاعات را تغییر دهند چراکه از تکثیر یک‌طرفه از سمت سرور اولیه پشتیبانی می‌کنند. نوع دوم سرور DNS ای است که روی RODC اجرا می‌شود. این سرورها در زمان عجین شدن با RODC زون‌های فقط خواندنی اولیه (Primary Read-Only Zones)را اجرا می‌کنند.

با این سه نوع سرور DNS ما می‌توانیم استراتژی تحلیل نام را که نیازمندی‌های سازمان را مرتفع کند پایه‌ریزی کنیم. (شکل ۳- ۹)
برای مثال می‌توان سرور DDNS را با هر DC در شبکه همراه کنیم چون اطلاعات DNS معمولا با انباره دایرکتوری عجین می‌شود. اطلاعات DNS به دلیل اینکه در انباره دایرکتوری قرار دارد به همه DC های دامنه و گاهی forest با همان مکانیزمی که ترافیک دایرکتوری تکثیر می‌شود منتشر می‌شود. نتیجه این است که همه DC ها یک کپی از اطلاعات DNS را به صورت محلی در اختیار خواهد داشت. نصب سرویس DNS روی DC به طور خودکار دسترسی محلی به اطلاعات DNS را امکانپذیر می‌کند و از افزایش بار روی لینک‌های WAN شبکه جلوگیری می‌کند. به علاوه در محیط‌های ناامن می‌توانیم از سرویس RODC DNS در حالت فقط خواندنی استفاده کنیم یعنی محل‌هایی که سرویس‌های محلی ارائه می‌شود ولی مدیر شبکه حضور ندارد. همچنین می‌توانیم از سرویس DNS اولیه منفرد (Standalone Primary DNS Service) در ناحیه DMZ شبکه خود بهره ببریم. این سرورها رکوردهای کمی را در بر می‌گیرند ولی دسترسی به هر برنامه‌ای یا سرویسی را که در این ناحیه قرار دارد فراهم می‌کنند. در نهایت از سرورهای DNS ثانویه فقط خواندنی در محیط‌های ناامن که به سمت اینترنت هستند استفاده می‌کنیم.



شکل ۳- ۹ جایگاه سرور DNS در شبکه مبتنی بر ویندوز سرور 2008 : DDNS از DC ها پیروی می‌کند ، سرورهای اولیه محافظت شده‌اند و RODC ها در داخل شبکه قرار دارند در حالی که سرورهای ثانویه در خارج قرار دارند.

اطلاعات بیشتر Domain Name System

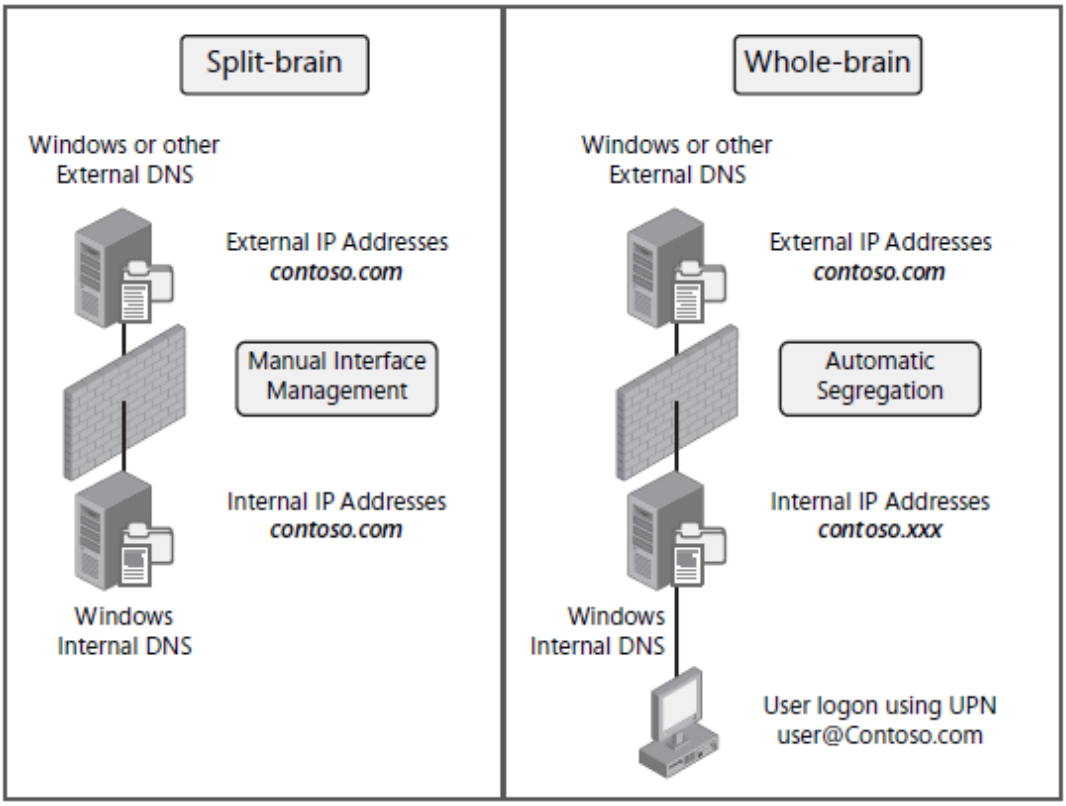
برای اطلاعات بیشتر درباره DNS به آدرس
http://technet2.microsoft.com/windowsserver2008/en/servermanager/dnsserver.mspx مراجعه کنید.

سندرم Split-Brain

یکی از اصول شبکه‌ها جداسازی شبکه داخلی از اینترنت است. سازمان‌های کوچک همانند سازمان‌های بزرگ تلاش می‌کنند شبکه داخلی خود را با استفاده از سیستم‌ها و تکنولوژهای مختلف ایمن کنند. رایج‌ترین مکانیزم حفاظت دیواره آتش است که از ورود ترافیک ناخواسته از طریق کنترل پورت‌های TCP/IP جلوگیری می‌کند. پورت‌های مورد نیاز باز و بقیه پورت‌ها بسته می‌شوند. به همین سادگی.

وقتی با ویندوز سرور 2008 مخصوصا AD DS کار می‌کنیم باید با دو فضای نام (Namespace) کار کنیم. چون دایرکتوری‌های AD DS بر اساس سیستم تحلیل نام سلسله مراتبی طراحی شده برای تحلیل نام forest و دامنه‌های آن باید از یک قالب نام DNS مناسب استفاده کنیم که FQDN (Fully Quilified Domain Name) نام دارد. سازمان‌ها اغلب از همان نامی استفاده می‌کنند

که در اینترنت خود را معرفی می‌کنند. برای مثال این کتاب از نام‌های غیرواقعی نظیر contoso.com یا woodgrovebank.com استفاده کرده است. این اسامی بهترین نیستند ولی به این دلیل آورده شده‌اند که انتشارات مایکروسافت اجازه درج آنها را داده است.
بهرحال استفاده از نام‌های مشابه برای ساختار دایرکتوری AD DS به این معنی است که باید سرویس Split-Brain DNS را پیاده‌سازی کنیم. دلیل آن اینست که نیاز به نگهداری دو فضای نام برای دو هدف داریم. مفهوم پیچیده نیست . کاربران ما باید بتوانند هم منابع داخلی شبکه و هم خارجی را پیدا کنند که بر اساس یک نام طراحی شده‌اند. اگر شرکت Contoso از نام contoso.com برای هردو فضا استفاده می‌کرد مدیر سرویس DNS مجبور بود به صورت دستی مکانیزم‌های تحلیل نام داخلی و خارجی را تفکیک کند.
بهرحال اگر شرکت Contoso منحصرا برای فضای نام خارجی از نام contoso.com استفاده کند و نام مشابه با پسوند .net را برای فضای نام AD DS خود در نظر بگیرد دیگر نیازی به دخالت مدیر شبکه برای جداسازی فضاها وجود ندارد. در این دو فضا به طور خودکار از ریشه‌های متفاوت برای جداسازی نام‌ها و دو سرویس DNS برای پشتیبانی از این دو استفاده می‌شود. تنها چیزی که باید از دیواره آتش عبور کند مرجع نام استانداردی است که ما از آن برای هر نامی که در شبکه موجود نیست استفاده می‌کنیم. به علاوه برای شرکت Contoso خرید و نگهداری همه ترکیب‌های نام اینترنتی شامل پسوندهای .com ، .net ، .info ، .ms ، .ws و غیره کار ساده‌ای است. از این طریق شرکت می‌تواند از هر کدام از نام‌ها برای پیاده‌سازی، تولید، تست، توسعه یا نمایش forest یا برای اهداف دیگر استفاده کند و مطمئن باشد با هیچ چیز تداخل ندارد حتی اگر با ترکیب یا تفکیک بخشی از سازمان مواجه شود.
مسئله‌ای که معمولا در این مورد بروز می‌کند مالکیت سرویس DNS است. قبلا مجریان شبکه مالک سرویس DNS بودند و اغلب این سرویس‌ها در محیطی غیر مایکروسافتی نگهداری می‌شد. ویندوز و مخصوصا AD DS برای سرویس ویندوزی DNS طراحی شده‌اند. اگرچه امکان استفاده از ویندوز با سرورهای DNS غیرویندوزی وجود دارد توصیه نمی‌شود زیرا بار کاری را مدیر شبکه را افزایش می‌دهد. وقتی از سرویس DNS ویندوز استفاده می‌کنیم و آنرا با سرویس AD DS عجین می‌کنیم همه چیز خودکار انجام می‌شود. اگر این کار را نکنیم همه چیز دستی انجام می‌شود و اغلب بعضی اجزاء کار نمی‌کنند و علت می‌تواند این باشد که پیکربندی دستی توسط مدیر سیستم غیرمایکروسافتی کامل یا درست انجام نشده است.
اگر در چنین وضعیتی هستید و باید دو فن‌آوری DNS را اجرا کنید بهترین و ایده‌آل‌ترین پیکربندی شبکه رویکرد whole-brain می‌باشد که متکی بر دو فضای نام متفاوت است. از طرفی فضای نام داخلی را با سرورهای DNS ویندوز که روی DC اجرا می‌شوند عجین می‌کند و از طرف دیگر از طریق مکانیزم‌های تحلیل نام DNS استاندارد به سادگی لینک دو فضای نام را برقرار می‌سازد. این روش سربار مدیریتی را کاهش می‌دهد و تضمین می‌کند سرویس‌ها همیشه درست کار کنند.(شکل ۴- ۹)



شکل ۴- ۹ ساختار split-brain در مقایسه با whole-brain

دیگر نیازی نیست نگران کاربران باشید. اگر از یک فضای نام متفاوت در داخل شبکه استفاده می‌کنید و می‌خواهید آنها بتوانند از یک شبکه بیرونی مانند contoso.com وارد شوند فقط کافی است آنرا به عنوان preferred user principal name (UPN) suffix در دایرکتوری خود اضافه کنید. با این کار مدیریت DNS ساده‌تر انجام می‌شود شبکه داخلی از دسترسی بیرونی محافظت می‌شود و کاربران این تغییر را احساس نمی‌کنند.

اهداف امتحانی در این فصل:

- پیکربندی DNS برای Active Directory
  - پیکربندی زون‌ها (Zones)
  - پیکربندی تنظیمات سرور DNS
  - پیکربندی تکثیر (replication) و انتقال (transfer) زون‌ها

دروس این فصل:

- درس ۱: درک و نصب سیستم تحلیل نام دامنه (Domian Name system) یا DNS
- درس ۲: پیکربندی و استفاده از DNS

قبل از شروع

برای ادامه این فصل باید موارد زیر انجام شده باشد:

- ویندوز سرور 2008 روی یک کامپیوتر فیزیکی یا مجازی نصب شده باشد که نامش SERVER10 بوده سرور منفرد (standalone) باشد. این کامپیوتر میزبان سرویس DNS و DC است و باید طبق تمرینات این فصل نصب شود. یک آدرس

IP نسخه ۴ از یک رنج خصوصی (private range) برای مثال 192.168.x.x به سرور اختصاص یافته باشد و آدرس سرور DNS به خودش برگردد. (127.0.0.1)

- ویندوز سرور 2008 روی یک کامپیوتر فیزیکی یا مجازی نصب شده باشد که نامش SERVER20 بوده سرور منفرد (standalone) باشد. این کامپیوتر میزبان سرویس DNS و DC است و باید طبق تمرینات این فصل نصب شود. یک آدرس IP نسخه ۴ از یک رنج خصوصی (private range) برای مثال 192.168.x.x به سرور اختصاص یافته باشد و آدرس سرور DNS را IP اختصاص داده شده به SERVER10 تعیین شود.

- ویندوز سرور 2008 روی یک کامپیوتر فیزیکی یا مجازی نصب شده باشد که نامش SERVER30 بوده سرور منفرد (standalone) باشد. این کامپیوتر میزبان سرویس DNS و DC است و باید طبق تمرینات این فصل نصب شود. یک آدرس IP نسخه ۴ از یک رنج خصوصی (private range) برای مثال 192.168.x.x به سرور اختصاص یافته باشد و آدرس سرور DNS را IP اختصاص داده شده به SERVER10 تعیین شود.

اکیدا توصیه می‌شود از ماشین مجازی برای انجام تمرینات استفاده شود. نقش‌های سرور DC و DNS برای مجازی‌سازی از طریق هم Microsoft Virtual Server 2005 R2 و هم Windows Server 2008 Hyper-V ایده‌آل می‌باشد.

درس ۱: درک و نصب DNS

تحلیل نام دامنه یک روند پیچیده است که متکی بر یک ساختار سلسله‌مراتبی نام به منظور تبدیل نام به آدرس IP می‌باشد. سیستم تحلیل نام DNS محل سرویس‌ها را نیز مشخص می‌کند. به این ترتیب پروسه ورود کاربر در AD DS به درستی کار می‌کند. در حقیقت DNS نقشی ضروری در این پروسه دارد و به همین دلیل ارائه سرویس‌های AD DS بدون DNS به سادگی امکانپذیر نبودند.

برای این کار سرویس DNS به رکوردهای نام متکی است. رکوردها می‌توانند دستی ثبت شوند مثلا در یک سرور DNS اولیه که سرویس خواندنی نوشتنی را فراهم می‌کند. بهرحال عمل ثبت فقط توسط مدیر شبکه یا به صورت خودکار انجام می‌شود مانند سرورهای DNS پویا که اجازه ثبت رکورد را به سیستم‌ها می‌دهند. سیستم‌های هوشمند مانند کامپیوترها با سیستم عامل ویندوز 2000 ، XP ، 2003 ، ویستا و سرور 2008 می‌توانند نام خود را در یک سرور DDNS ثبت کنند ولی کامپیوترهای دارای سیستم عامل قدیمی مانند ویندوز NT نمی‌توانند این کار را انجام دهند. سیستم‌های قدیمی‌تر برای ثبت نام خود به سرویس DHCP متکی هستند. بهرحال این یک پیاده‌سازی زیرساخت DDNS با امنیت پایین‌تر است.

DNS دارای انواع رکورد است که برای تحلیل نام انواع سرویس یا کامپیوتر به کار می‌رود. به علاوه این رکوردها در زون‌های DNS ذخیره می‌شوند. زون‌ها مکان‌های مشخصی برای عملیات تحلیل نام یک فضای نام خاص را فراهم می‌کنند.

درک اجزاء مختلف سرویس DNS ویندوز سرور 2008 برای درک نحوه کارکرد و استفاده از آن بسیار حیاتی است.

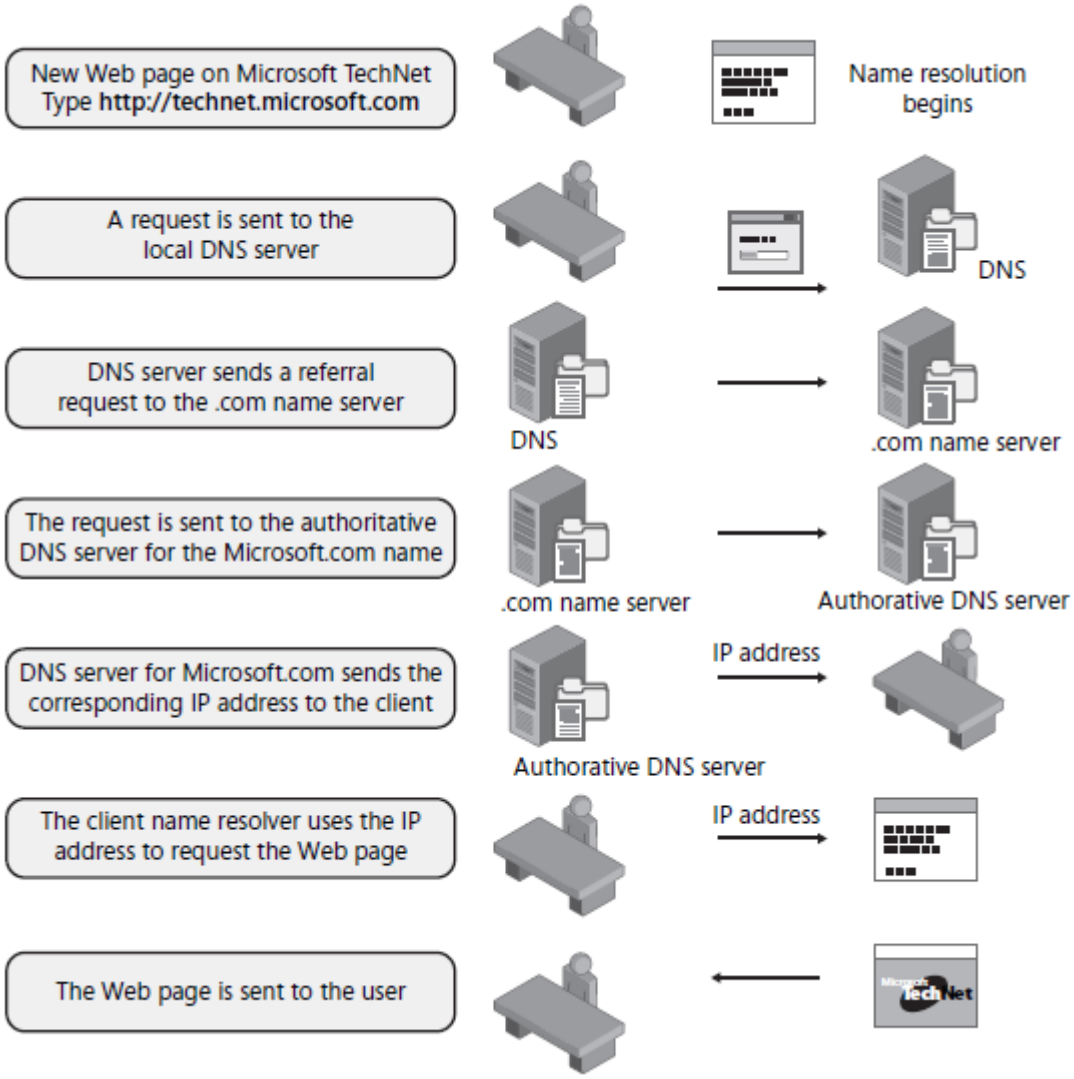
بعد از این درس ما می‌توانیم:

- یاد بگیریم که چه زمانی از DNS استفاده کنیم.
- DNS را نصب کنیم.
- DNS را محل‌یابی کرده و بررسی کنیم.

زمان تقریبی: ۷۰ دقیقه

درک DNS

اولین چیزی که هنگام کار با DNS باید یاد بگیریم این است که DNS چطور یک نام را تحلیل می‌کند. ما از قبل می‌دانستیم که DNS به سرورهای سلسله مراتبی متکی است زیرا یک سرور DNS نمی‌تواند همه رکوردهای نام موجود را در خود نگه دارد. به همین دلیل سرویس DNS برای تحلیل نام از ارجاع نام (name referral) استفاده می‌کند. (شکل ۵- ۹)



شکل ۵- ۹ پروسه تحلیل نام DNS

روند تحلیل نام به ترتیب زیر است:

۱. ما سعی می‌کنیم یک صفحه وب را از سایت Technet مایکروسافت پیدا کنیم. برای این کار در نوار آدرس مرورگر تایپ می‌کنیم : http://technet.microsoft.com و کلید Enter را می‌زنیم. از این جا تحلیل نام شروع می‌شود.

۲. کامپیوتر ما یک درخواست به سرور DNS محلی یا حداقل یکی از سرورهای لیست شده در تنظیمات پروتکل TCP/IP می‌فرستد.

۳. اگر این سرور نام مورد نظر را در بانک اطلاعات یا cache خود نداشته باشد یک درخواست ارجاعی به سرور نام می‌فرستد. چون سایت مایکروسافت با com. تمام می‌شود سرور DNS درخواست ارجاعی را به سرور نام com. ارسال می‌کند.

۴. سرور نام com. حاکم تمام نام‌های با پسوند com. می‌باشد. این سرور محل همه سرورهای DNS حاکم محلی را برای پسوند com. می‌شناسد.

۵. سرور DNS microsoft.com آدرس IP صفحه درخواست شده را به کلاینت می‌فرستد.

۶. تحلیل‌گر نام (name resolver) روی کلاینت از این آدرس IP برای ارسال درخواست صفحه از طریق سرور اینترنت استفاده می‌کند.

۷. اگر صفحه در cache محلی سرور اینترنت موجود نباشد درخواست ارسال می‌گردد.

این پروسه تحلیل نام در لحظه اتفاق می‌افتد و صفحه وب بسته به سرعت ارتباط اینترنت و حجم درخواست تقریبا همزمان با تایپ نام آن ظاهر می‌شود. این اتفاقی است که در نوار پیشرفت در پایین مرورگر مشاهده می شود . این نوار پیشرفت همچنین نشاندهنده دانلود محتوای متنی و تصاویر روی کامپیوتر می‌باشد.

DNS سیستمی است که به تنهایی نمی‌تواند کار کند و متکی به سرورهای دیگر می باشد. به علاوه سرویس DNS واژه شناسی مخصوص به خود را دارد. جدول ۲- ۹ مهم ترین واژه‌های سرویس DNS را تعریف می‌کند.

جدول ۲- ۹ واژه‌ها و مفاهیم DNS

Active Directory Integrated (ADI) zone	وقتی یک زون DNS با Active Directory عجین می‌شود روی بانک اطلاعاتی AD DS (NTDS.dit) قرار می‌گیرد و همراه اطلاعات دیگر دایرکتوری تکثیر می‌شود.
Aging	رکوردهای DNS با یک چرخه زمانی (Time To Live-TTL) ثبت می‌شود. وقتی زمان آن به سر می‌رسد این رکورد دیگر اعتبار ندارد
Application Directory Partitions	وقتی اطلاعات DNS همراه بانک دایرکتوری AD DS ذخیره می‌شود به طور پیش فرض تکثیر نیز همراه آن انجام می‌شود. بهر حال می‌توانیم یک حوزه تکثیر اختصاصی برای داده DNS تعریف کنیم. برای مثال داده DNS که به دامنه ریشه یک forest تعلق دارد باید برای کل forest قابل دسترس باشد چرا که داده DNS برای یک دامنه خاص فقط برای همان دامنه مورد نیاز است. حوزه تکثیر داده DNS به واسطه application directory partitions کنترل می‌شود.
DDNS	یک سرویس DNS است که می‌تواند توسط کلاینت‌ها به طور خودکار به روز شود. در ویندوز سرور 2008 ما وقتی بخواهیم DNS را با AD DS نصب کنیم DDNS را نصب می‌کنیم. به دلیل اینکه همه کلاینت‌ها در پیاده‌سازی DDNS حساب AD DS دارند فرض می‌شود امن بوده و دارای توانایی به روز رسانی سرور DNS با اطلاعات رکورد خود می‌باشند.
DNS Notify	سرورهای قدیمی DNS داده را در فایل‌های محلی مدیریت می‌کنند. این فایل‌ها روی سرور اولیه جای دارند. سپس از طریق مکانیزم polling and zone transfer به سرورهای ثانویه فقط خواندنی منتقل می‌شوند. بهرحال زون‌های بزرگ نیاز به به روز رسانی رکورد مکرر دارند. این مساله باعث می‌شود تعداد دکوردهای اشتباه روی سرور ثانویه زیاد باشد. برای اصلاح این وضعیت DNS از یک پروسه خبررسانی خاص استفاده

	می‌کند که سرورهای فرعی (slave) را از وجود نسخه جدید داده آگاه می‌کند که نهایتا به انتقال زون به سرورهای فقط خواندنی منجر می‌شود.
Domain DNS zone	این زونی است که رکوردهای دامنه مشخصی را دربر می‌گیرد هم ریشه و هم دامنه فرزند در ساختار AD DS forest
Forest DNS zone	زونی است که رکوردهای متعلق به کل forest را در ساختار AD DS forest در بر می‌گیرد
Forward lookup	DNS دو نوع جستجو را پشتیبانی می‌کند: forward و reverse . یک جستجوی forward حالتی است که یک کلاینت نام FQDN را به سرور می‌فرستد سپس سرور این FQDN را با IP متناظر مطابقت می‌دهد.
Forwarders	سرورهای DNS دو مکانیزم برای تحلیل نام دارند : forwarder ها و root hint ها . سرورهای DNS که سرویس تحلیل نام را برای شبکه داخلی فراهم می‌کنند اغلب برای ارسال درخواست‌هایی که روی سرور خود یا سرور خارجی مورد اطمینان نمی‌تواند تحلیل کنند به forwarder ها متکی هستند. ویندوز سرور 2008 همچنین دارای قابلیت forwarder های شرطی هستند که فقط زمانی که شرط خاصی در درخواست محقق شود استفاده می‌شوند. برای مثال اگر نام متعلق به دامنه داخلی باشد ولی نه دامنه‌ای که توسط همین سرور مدیریت می‌شود به طور خودکار درخواست را به سرور نام داخلی همان دامنه ارسال می‌کند.
GlobalNames Zones (GNZ)	نام‌های NetBIOS نام‌های یک بخشی هستند که از فرمت FQDN استفاده نمی‌کنند. این نام‌ها توسط Windows Internet Name Service (WINS) مدیریت می‌شوند. ویندوز در یک حرکت برای حذف این سرویس قدیمی از شبکه‌های مبتنی بر ویندوز GlobalNames Zones را در DNS ویندوز سرور 2008 پیاده‌سازی کرده است. GNZ ها دارای نام‌های یک بخشی بوده و جایگزین سرویس WINS در شبکه ویندوزی شده است.
Legacy DNS	سرورهای غیرپویا که به صورت دستی به روز می‌شوند سرورهای DNS قدیمی به شمار می‌آیند. ویندوز سرور 2008 با این هدف که استاندارد پروتکل DNS (RFC) را رعایت کند از سرویس‌های DNS قدیمی همانند سرویس پویای DNS مورد نیاز AD DS پشتیبانی می‌کند. سرورهای DNS قدیمی هم زون‌های اولیه و هم ثانویه را میزبانی می‌کنند.
Name Recursion	تحلیل نام می‌تواند iterative یا recursive باشد. در یک درخواست iterative هر سرور DNS فقط بخشی از جواب درخواست را دارد و برای تکمیل جواب درخواست به سرورهای

	دیگر نیاز دارد. در درخواست recursive سرور DNS جواب کامل را دارد و آنرا به درخواست کننده ارسال می‌کند. به دلیل سن رکورد خطا در جواب درخواست آدرس IP محتمل است.
Primary zones	زون‌هایی هستند که اطلاعات خواندنی-نوشتنی دامنه مشخصی را دارا هستند. زون‌های اولیه روی سرور DNS پویا یا غیرپویا ذخیره می‌شوند. زون‌های اولیه وقتی روی سرور غیرپویا ذخیره می‌شوند به صورت فایل‌های متنی بوده و به صورت دستی توسط مدیر شبکه ویرایش می‌شوند و وقتی روی سرور DDNS ذخیره می‌شوند در Active Directory ذخیره شده و هم به صورت خودکار توسط صاحب رکورد و هم دستی توسط مدیر شبکه قابل به روز رسانی هستند.
Resource records	رکوردهای نام هستند که در بانک اطلاعات DNS قرار دارند. این رکوردها معمولا یک آدرس IP را به یک FQDN لینک می‌دهند.
Reverse lookup	DNS از دو نوع جستجو پشتیبانی می‌کند: forward و reverse . جستجوی reverse رفتار کلاینتی می‌باشد که آدرس IP دارد و درخواست نام FQDN متناظر را دارد.
Reverse lookup zone	این زون شامل DNS container ها (بانک‌های اطلاعاتی یا فایل‌های متنی) می‌باشد که شامل تحلیل نام برای جستجوی reverse مربوط به یک دامنه مشخص می‌باشد.
Root hints	سرورهای DNS دو مکانیزم برای تحلیل نام دارند. Forwarder ها و root hints . سرورهای DNS که سرویس تحلیل نام را به شبکه داخلی ارائه می‌دهند ولی لینک مستقیم به اینترنت دارند برای محل‌یابی سرورهای authoritative نام‌های ریشه‌ای نظیر .com ، .org ، .net و غیره در اینترنت و فراهم کردن سرویس‌های تحلیل نام برای کلاینت‌های داخلی به root hint ها متکی هستند. به طور پیش فرض سرور DNS ویندوز سرور 2008 برای تحلیل نام خارجی بر اساس root hint ها عمل می‌کند. این hint ها به طور مرتب از طریق Microsoft Windows Update به روز می‌شوند. Root hint ها در یک فایل مشخص با نام Cache.dns ذخیره می‌شوند که برای ریست کردن root hint ها در مواقعی که پروسه تحلیل نام خارجی با مشکل مواجه می‌شود به کار می‌رود.
Round robin	سرویس‌های DNS به منظور فراهم کردن برخی انواع دسترسی سطح بالا به کار می‌رود. این کار با ساخت رکوردهای چندگانه برای یک منبع خاص هرکدام با آدرس IP متفاوت امکانپذیر است. سرور DNS هنگام دریافت درخواست، اولین آدرس بعد دومین و به همین ترتیب بقیه آدرس‌ها را ارسال می‌کند. هدف

	این است که بین سرورهای چندگانه که میزبان یک سرویس هستند تقسیم بار صورت گیرد. برای مثال Microsoft Exchange Server 2007 Edge Transport Server (سروری که به سمت اینترنت بوده و پست الکترونیک داخلی را قبول کرده و ارسال می‌کند) برای تقسیم بار به پروسه round robin متکی است.
Secondary zone	یک زون فقط خواندنی است که از یک سرور DNS اولیه به دست می‌آید. زون‌های ثانویه تحلیل نام DNS محلی را در شبکه‌های توزیع شده انجام می‌دهند
Server scavenging	ویژگی که به همراه سرویس DNS پویا زمان ارائه ویندوز سرور 2000 معرفی شد. به دلیل اینکه رکوردها طول عمر دارند ممکن است تاریخ مصرفشان بگذرد. این ویژگی بانک اطلاعاتی DNS را از وجود این رکوردها پاک می‌کند.
Single-Lable names	نام‌های NetBIOS هستند که از قالب FQDN پیروی نمی‌کنند. این نام‌ها دارای ۱۶ کاراکتر بوده و از کاراکترهای ویژه مانند نقطه استفاده نمی‌کنند. ۱۵ کاراکتر اول قابل استفاده است چراکه شانزدهمین کاراکتر برای تکمیل نام توسط سیستم رزرو می‌شود. به طور سنتی این نام‌ها توسط WINS مدیریت می‌شوند. در ویندوز سرور 2008 به جای WINS می‌توانیم از GNZ استفاده کنیم.
Start of Authority (SOA) record	یک رکورد خاص DNS است که اطلاعات دامنه را نظیر جدول به روز رسانی رکوردها، فواصل زمانی که سرورهای دیگر باید آپدیت‌ها را بررسی کنند و روز و ساعت آخرین به روز رسانی را به همراه دیگر اطلاعات را به طور خلاصه ذخیره می‌کند. در یک فایل زون مشخص فقط یک رکورد SOA وجود دارد. هر فایل زون باید دارای یک رکورد SOA مشخص باشد.
Stub zone	یک نوع زون مخصوص می‌باشد که شامل رکوردهای سرور DNS دیگر است که خود شامل زون حقیقی می‌باشد. این نوع زون باعث افزایش سرعت تحلیل نام و کاهش احتمال خطا می‌شود چراکه این زون‌ها به عنوان مرجع دیگران استفاده می‌شوند.
TTL	همه رکوردهای DNS یک مقدار TTL دارند. این مقدار نشان‌دهنده طول عمر رکورد است. وقتی به پایان رسد رکورد با استفاده از scavenging حذف می‌شود. اگر عمر رکورد به پایان نرسیده باشد می‌توانیم آنرا تجدید کنیم و بنابراین مقدار TTL نیز تجدید می‌شود.
Zone Delegations	اعطاء اختیار با هدف کمک به مدیریت بهتر بخش‌های فضای نام مختلف انجام می‌شود. برای مثال مایکروسافت ممکن است بخواهد بخش‌های مختلف فضای نام خود را تفویض اختیار کند مثلا MSDN یا TechNet که مدیریت آنها با بخش‌های

	دیگر انجام شود. هنگام مدیریت فضای نام DNS در AD DS باید اختیار زون‌های مبتنی بر دامنه را هنگام ساخت دامنه اعطاء کنید. در غیر اینصورت زون در سطح forest مدیریت می‌شود و نه در سطح دامنه. در ویندوز سرور 2003 این تفویض اختیار باید به صورت دستی قبل از ساخت دامنه انجام شود. در ویندوز سرور 2008 ویزارد Active Directory Domain Services Installation Wizard کار تفویض اختیار را به صورت خودکار هنگام ساخت دامنه فرزند انجام می‌دهد.
Zone scavenging	سرور DNS را از رکوردهای تاریخ مصرف گذشته پاک می‌کند. زمانی اعمال می‌شود که به یک زون منفرد .....
Zone Transfers	تعاملاتی هستند که سرورهای DNS از آن برای تکثیر اطلاعات از یک سرور به دیگری استفاده می‌کنند. انتقال کامل زون‌ها تمام محتوای یک زون را شامل می‌شود. انتقال افزایشی (Incremental) فقط بخشی از داده را تکثیر می‌کند. قبلا انتقال کامل به نام Asynchronous Full Transfer (AXFR) و انتقال افزایشی به نام Incremental Zone Transfer (IXFR) شناخته می‌شد. ویندوز سرور 2008 نیز از انتقال امن زون‌ها پشتیبانی می‌کند که از طریق تکثیر AD DS multimaster انجام می‌شود.

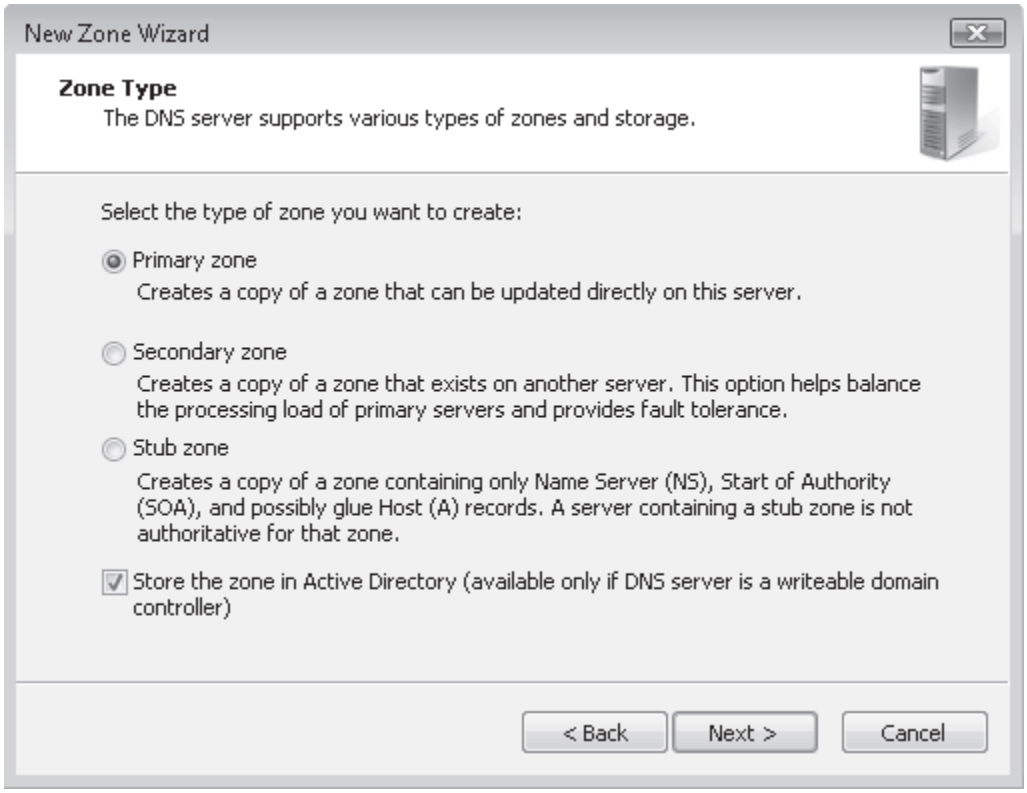
سرویس DNS ویندوز سرور 2008طبق شکل ۶- ۹ دارای سه نوع زون می‌باشد.

- **Primary Zone** یا زون‌های اولیه زون‌هایی هستند که می‌توانند با AD DS عجین شوند یا از نوع استاندارد قبلی می‌باشند. این زون‌ها برای فضای نام خودشان Authoritative هستند. زون‌های اولیه بجز زمانی که روی RODC قرار دارند خواندنی نوشتنی هستند.

- **Secondary Zone** یا زون‌های ثانویه از نوع استاندارد قدیمی‌تر بوده و فقط یک Replica از دادهی هستند که در سرورهای Authoritative برای یک فضای نام قرار دارند. وقتی زون ثانویه می‌سازیم باید آدرس زون اولیه یا منبع داده زون را برای DNS مشخص کنیم.

- **Stub Zone** زون‌هایی هستند که فقط به سرورهای دیگر که برای فضای نام خودشان Authoritative هستند اشاره می‌کنند. وقتی یک زون stub می‌سازیم باید لیست سرورهایی که برای فضای نام Authoritative هستند مشخص کنیم.

زون‌ها می‌توانند هم در یک فایل متنی و هم در پارتیشن ذخیره سازی دایرکتوری Active Directory ذخیره شود.



شکل ۶- ۹ ویزارد New Zone Wizard ما را قادر می سازد هر یک از سه زون را ایجاد کنیم.

زون ها container هایی هستند که حاوی اطلاعات اشیاء تحت مدیریت خود می باشند. این اطلاعات به فرم رکورد می باشد. DNS می تواند انواع مختلف رکورد داشته باشد. جدول ۳- ۹ مهم ترین انواع رکورد مورد استفاده در ویندوز سرور 2008 را خلاصه می کند.

جدول ۳- ۹ انواع رکورد DNS در ویندوز سرور 2008

نوع رکورد	مورد استفاده
Alias (CNAME)	به منظور ساخت یک رکورد جایگزین یا نام DNS از نوع alias برای یک نام که قبلا به عنوان یک رکورد دیگر در یک زون خاص مشخص شده است به کار می رود. همچنین به عنوان یک نام canonical یا CNAME نیز به شناخته می شود. برای مثال وقتی می خواهیم یک رکورد مانند intranet.contoso.com ایجاد کنیم تا به یک سرور یا سرور فارم میزبان سرور Microsoft Office SharePoint اشاره کند باید آنرا به عنوان یک رکورد از نوع alias ایجاد کنیم. با این کار به جای نام سرور از یک نام کاربردی تر استفاده می کنیم.
Host (A or AAA) record	رایج ترین نوع رکورد در DNS است. در واقع نمایانگر اشیاء کامپیوتر در فضای نام بوده و برای تحلیل نام یک آدرس IP یا دستگاه خاص استفاده می شود.
Mail Exchanger (MX)	e-mail ها را به یک فضای نام مشخص آدرس دهی می کند. برای مثال رکورد MX برای contoso.com مشخص می کند که همه e-mail ها ارسال شده به سمت contoso.com باید از میزبان یا میزبان‌های مشخص شده توسط این رکورد بگذرد.
Pointer (PTR)	به یک محل خاص در فضای نام اشاره می‌کند. رکوردهای

	PTR معمولا برای فراهم کردن قابلیت‌های جستجوی معکوس (reverse lookup) در فضای نام استفاده می‌شوند.
Service Location (SRV)	محل یک سرویس خاص TCP/IP را مشخص می‌کند. برای مثال اگر بخواهیم از Microsoft Office Communications Server استفاده کنیم باید یک رکورد محل سرویس از نوع session initiation protocol (SIP) بسازیم تا دستگاههایی را که به این سرویس نیاز دارند به همه نشان دهیم. به طور مشابه AD DS در پشتیبانی از پروسه ورود به سیستم یا توزیع Group Policy رکوردهای محل سرویس متعددی می‌سازد. رکورد محل سرویس معمولا شامل آدرس IP برای سرور و پورت TCP/IP که سرویس روی آن ارائه می‌شود می‌باشد.

رکوردهای جدول فوق عملکرد اصلی DNS را در پیاده‌سازی ویندوز سرور 2008 بیان می‌کند.

ویژگی‌های DNS ویندوز سرور

سرور DNS ویندوز سرور 2008 به طور کامل با RFC ارائه شده توسط Internet Engineering Task Force (IETF) برای استانداردهای فن‌آوری اینترنت همخوانی دارد و همچنین یک سری قابلیت‌هایی دارد که برای پشتیبانی از ویژگی‌های سیستم‌های عامل شبکه‌ای (NOS) در ارتباط با AD DS طراحی شده است. سرور DNS در ویندوز سرور 2008 همچنین می‌تواند با سرورهای DNS غیرمایکروسافتی کار کند چون با همه RFC های مرتبط با سرویس DNS مطابقت دارد.

وقتی سرویس DNS با AD DS عجین می‌شود می‌توانیم داده DNS را در محل دیگری در بانک اطلاعاتی دایرکتوری ذخیره کنیم. داده DNS می‌تواند در پارتیشن دامنه دایرکتوری ذخیره شود. این گزینه برای داده‌ی که انتخاب می‌شود که به خود دامنه برمی‌گردد. برای مثال یک دامنه فرزند در یک forest باید داده خود را در پارتیشن دامنه خود ذخیره کند تا داده برای همه سرورهای DNS در دامنه قابل دسترس باشد. همچنین می‌توانیم این داده را در پارتیشن‌های دایرکتوری برنامه (application directory partition) ذخیره کنیم. برخلاف پارتیشن‌های دامنه ، پارتیشن‌های دایرکتوری دامنه حوزه تکثیر قابل کنترل دارند. برای مثال داده DNS مربوط به Forest در یک پارتیشن دایرکتوری برنامه ذخیره می‌شود که در کل forest گسترش می‌یابد تا داده در دسترس همه سرورهای DNS در forest قرار گیرد. به طور پیش فرض DNS ویندوز سرور دو پارتیشن دایرکتوری برنامه می‌سازد که میزبان داده DNS در هر forest شود. این پارتیشن‌ها به ترتیب عبارتند از: ForestDnsZones و DomainDnsZones .

به علاوه سرویس DNS در ویندوز سرور 2008 به منظور پشتیبانی از background zone loading ارتقا پیدا کرده است. وقتی سرور DNS تعداد زیادی زون و رکوردها دارد زمان زیادی طول می‌کشد سرور راه اندازی شود زیرا همه داده زون‌ها باید قبل از درخواست‌ها بارگذاری شوند. سرویس DNS با استفاده از background loading در طول بارگذاری داده زون در پشت صحنه پس از استارت کامپیوتر و شروع شدن پروسه ورود به سیستم خیلی سریع شروع به پاسخگویی به درخواست‌ها می‌کند.

DNS برای پشتیبانی از نقش جدید DC فقط خواندنی داده DNS فقط خواندنی برای زون‌های اولیه روی RODC ارائه می‌دهد. این کار باعث بالا رفتن امنیت می‌شود به طوری که کسی نمی‌تواند روی سرور رکورد جعلی بسازد.

مایکروسافت در حالی که تصمیم دارد از نام‌های یک بخشی پشتیبانی کند نقش سرویس WINS را کمرنگ کرده است به طوری که DNS را با GNZ مجهز کرده است. این زون می‌تواند تعداد اندکی نام را با آدرس IP ثابت داشته باشد.

DNS در تلاش برای جلوگیری از جعل رکورد از افزونه global query block lists استفاده می‌کند. وقتی کلاینت‌ها از پروتکل‌هایی نظیر Web Proxy Automatic Discovery Protocol (WPAD) یا Intra-site Automatic Tunnel Addressing Protocol (ISATAP) استفاده می‌کنند و برای تحلیل نام از DNS بهره می‌گیرند نسبت به کاربران بدخواه که از به روز رسانی پویا برای ثبت کامپیوترها غیرواقعی استفاده می‌کنند آسیب‌پذیر می‌شوند.

WPAD در حالت عادی پروتکلی است که مرورگرهای وب از آن برای کشف تنظیمات سرورهای پراکسی شبکه استفاده می‌کنند. جعل این آدرس می‌تواند کاربران را به سمت سرورهای هکرها سوق دهد که جایگزین سرورهای حقیقی شده و شبکه را در وضعیت خطرناک قرار دهند ISATAP یک پروتکل حد واسط است که ارتباط شبکه‌های مبتنی بر نسخه های ۴ و ۶ IP را برقرار می‌کند. این کار با کپسوله کردن پکت‌های Ipv6 در قالب Ipv4 برای عبور از مسیریاب‌ها انجام می‌دهد. ولی از مکانیزم کشف پویای مسیریاب (dynamic router discovery) پشتیبانی نمی‌کند. به جای آن از لیست مسیریاب‌های بالقوه برای تعیین مسیریاب‌های ISATAP بالقوه استفاده می‌کنند. اگر این لیست کشف شود پکت‌های Ipv6 می‌تواند به سمت مسیریاب‌های هکرها آدرس‌دهی شوند.

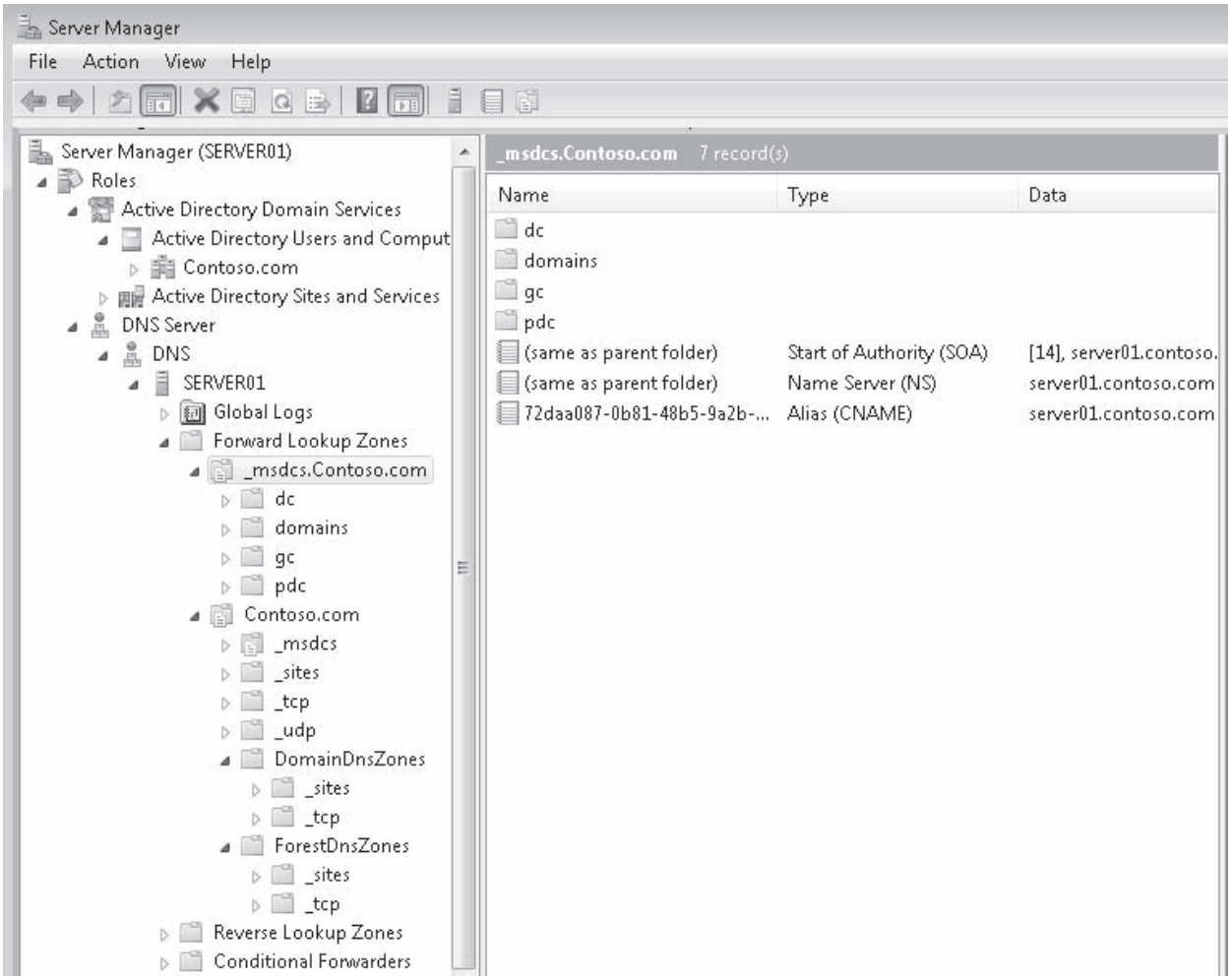
با استفاده از global query block lists که محدوده آدرس مشخصی را بلوکه می‌کند امکان کاهش احتمال خطر وجود دارد. فقط منتهی الیه سمت چپ FQDN در لیست global query block lists قرار می‌گیرد. وقتی سرور DNS درخواستی دریافت می‌کند که دارای این نام است پیغامی مبنی بر عدم وجود چنین رکوردی صادر می‌کند. به طور پیش فرض سرور DNS این لیست را هنگام نصب یا ارتقاء سرویس DNS موجود تولید می‌کند. اگر یکی از دو پروتکل موجود باشد بلوکه نمی‌شود. اگر هیچ کدام موجود نباشند هر دو بلوکه می‌شوند. به علاوه ما می‌توانیم نام‌های خود را که نمی‌خواهیم در شبکه قابل استفاده باشند به این لیست اضافه کنیم.

به طور خلاصه سرویس DNS در ویندوز سرور 2008 نه تنها به طور کامل از ویژگی‌های استاندارد مورد انتظار در یک سرور DNS پشتیبانی می‌کند بلکه دارای ویژگی‌های انحصاری ویندوزی نیز می‌باشد.

عجین سازی با AD DS

سرور DNS ویندوز به دلیل ویژگی‌های خاص خودش همیشه هنگام توزیع AD DS بهتر است توزیع گردد. امکان استفاده از سرور DNS غیرمایکروسافتی نیز با هدف فراهم کردن سرویس تحلیل نام برای پشتیبانی از AD DS وجود دارد ولی راه‌اندازی و آماده سازی این سرور DNS نسبت به سرویس مایکروسافتی کار بیشتری می‌طلبد. وقتی از سرور DNS ویندوز به همراه AD DS استفاده می‌کنیم همه محتوای DNS به طور پیش فرض پیکربندی می‌شود. به همین دلیل است که نصب DNS با ویزارد نصب DC همراه می‌شود. نصب DNS به همراه AD DS مراحل زیادی دارد که معمولا تمام آن با اجرای ویزارد از دید مدیر شبکه مخفی می‌ماند. این عملیات فقط هنگام ساخت forest ، tree در داخل forest یا دامنه جدید در forest جدید اتفاق می‌افتد.

اگر توزیع AD DS برای دامنه ریشه یک forest باشد DNS جایگاه‌هایی را برای Forward Lookup Zones (FLZ) ، Reverse Lookup Zones (RLZ) و Conditioal Forwarders (CF) می‌سازد. سپس دو زون جدید در FLZ ایجاد می‌کند. اولی جایگاه کل forest برای فضای نام ساخته شده هنگام نصب AD DS می‌باشد. این زون معمولا با نام _msdcs.domainname ایجاد می‌شود. برای مثال برای دامنه contoso.com این زون _msdcs.contoso.com نام دارد. به علاوه یک زون در FLZ برای خود دامنه ریشه همانند شکل ۷- ۹ ایجاد می‌کند.

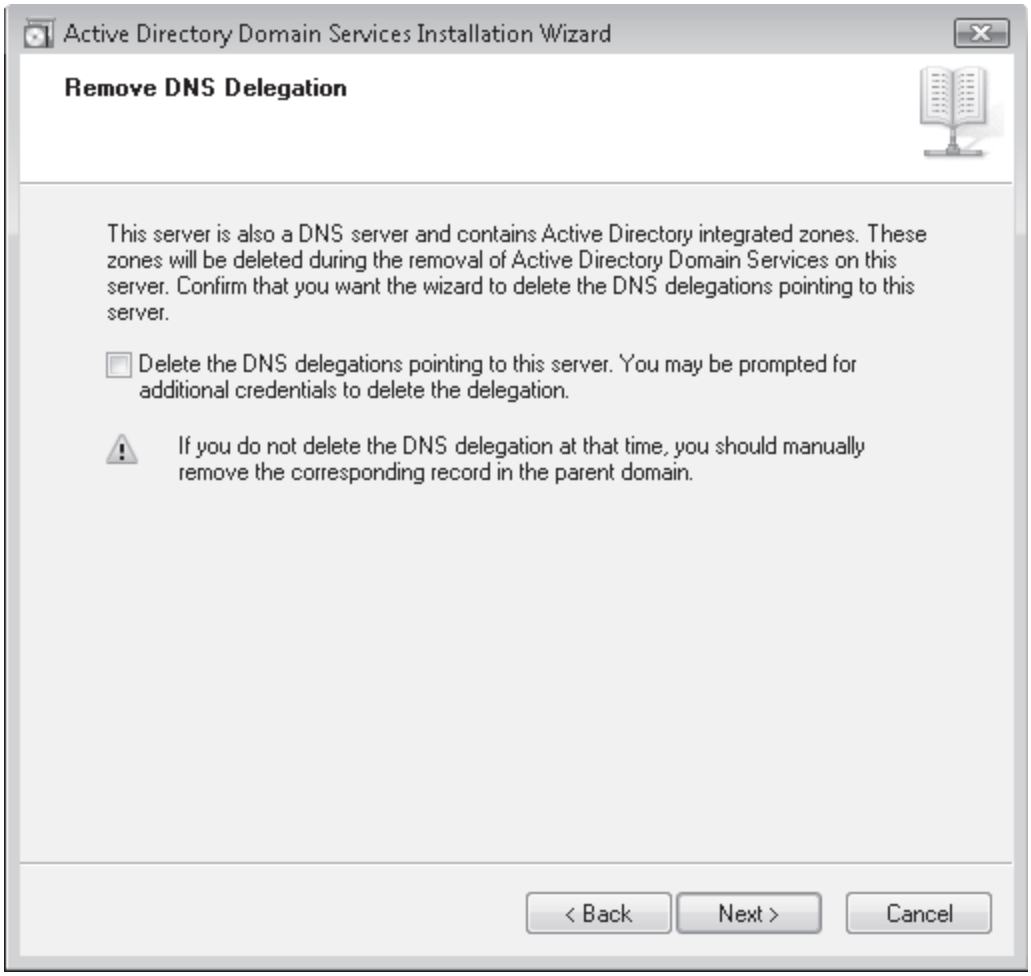


شکل ۷- ۹ Forward Lookup Zones برای forest contoso.com

وقتی در پروسه نصب سرویس AD DS یک Domain tree در forest موجود می سازیم نیاز به تفویض اختیار دستی قبل از ساخت Domain tree داریم. چون نام Domian tree متفاوت از نام دامنه ریشه است به عبارتی باید متفاوت باشد چون تعریف یک tree در یک forest می باشد ویزارد نمی تواند روی خودش تفویض اختیار کند. وقتی دو فضای نام DNS متفاوت باشند هیچ کدام روی دیگری اختیار تفویض اطلاعات ندارند از این رو تفویض اختیار باید دستی صورت گیرد. سپس ویزارد نصب AD DS فضای نام DNS را ساخته و در پارتیشن جدید دامنه جدید Domain tree ذخیره می کند.

وقتی پروسه AD DS یک دامنه فرزند در یک forest موجود می سازد به طور خودکار در سطح اول دامنه ریشه تفویض اختیار کرده و داده DNS را برای دامنه فرزند در پارتیشن دامنه فرزند ذخیره می کند.

برای حذف یک دامنه باید ویزارد Active Directory Domain Services Installation Wizard را یک بار دیگر اجرا کنیم تا نقش DC پاک شود و سپس نقش AD DS را بتوانیم پاک کنیم. به دلیل اینکه جایی برای دسترسی به ویزارد وجود ندارد باید در کادر جستجوی منوی استارت دستور Dcpromo.exe را تایپ کنیم. وقتی نقش DC حذف می شود داده DNS ساخته شده برای دامنه اگر آخرین DC دامنه باشد پاک می شود. همچنین اگر DC سرور global catalog (GC) باشد هشداری ظاهر می شود چون GC کار جستجو در AD DS را انجام می دهد. در طول حذف نقش DC با پیغام حذف تفویض اختیار DNS همانند شکل ۸- ۹ مواجه می شویم. اگر دامنه سطح اول نظیر forest یا دامنه ریشه باشد علامت این گزینه را پاک می کنیم. در غیر اینصورت با پیغام خطا مواجه می شویم و ویزارد از ما می خواهد اعتبار مناسب برای حذف تفویض اختیار را وارد کنیم. چون اعتبارات سطح ریشه را ما نداریم (برای نام هایی مانند .com ، .net ، .org و غیره) نمی توانیم این کار را انجام دهیم و بنابراین نمی توانیم تفویض اختیار سطح ریشه را ساخته یا حذف کنیم. به هر حال اگر یک دامنه فرزند باشد می توانیم تفویض اختیار را پاک کنیم.



شکل ۸- ۹ حذف تفویض اختیار DNS با ویزارد نصب AD DS

تمرینات نصب سرویس DNS

تمرین ۱ نصب یک سرور DNS اولیه

دراین تمرین ما باید از یک کامپیوتر منفرد برای نصب سرویس DNS استفاده کنیم و ببینیم که در حالت غیرپویا چطور کار می کند. این تمرین روی سرور SERVER10 انجام می شود.

۱. با کاربر Administrator محلی به سرور SERVER10 وارد می شویم.

۲. در Server Manager روی گره Roles کلیک راست کرده و Add Roles را انتخاب می کنیم.

۳. صفحه Before You Begin را مرور کرده و دکمه Next را کلیک می کنیم.

۴. در صفحه Select Server Roles از ویزارد Add Roles گزینه DNS Server را انتخاب کرده و دکمه Next را کلیک می کنیم.

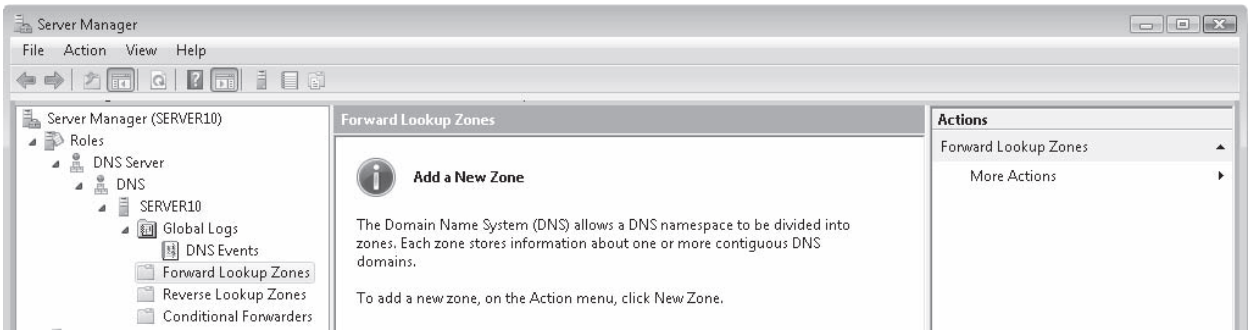
۵. اطلاعات صفحه DNS Server را مرور کرده و دکمه Next را کلیک می کنیم.

۶. انتخاب های خود را مرور کرده و دکمه Install را کلیک می کنیم.

۷. نتایج نصب را بررسی کرده و روی دکمه Close کلیک می کنیم. نصب کامل می شود.

۸. به گره DNS Server در Server Manager وارد شده و همه بخش ها را باز می کنیم. شاید نیاز باشد صفحه Server Manager را باز و بسته کنیم تا گره ها Refresh شوند. همانطوری که مشخص است نصب DNS همه container های موردنیاز اجرای سرویس DNS را در ویندوز سرور 2008 ایجاد می کند ولی به دلیل اینکه این مراحل در حالت معمول برای نصب سرور DNS قدیمی استفاده می شود هیچ اطلاعاتی در ساختار DNS container ایجاد نمی شود. (شکل ۹- ۹) . سرورهای DNS قدیمی نیاز به ورود دستی برای ساخت اطلاعات زون دارند. ما می توانیم پروسه ورود اطلاعات را ماشینی کنیم ولی به دلیل اینکه ویندوز تشخیص نمی دهد چرا از سرور DNS استفاده می کنیم دادهی برای آن ایجاد نمی کند.

۹. ساختار DNS Server container را قبل از ورود به تمرین ۲ مرور می کنیم.



شکل ۹- ۹ مشاهده DNS server container پیش فرض

تمرین ۲ نصب AD DS و ساخت یک forest جدید

۱. با کاربر Administrator به SERVER10 وارد می شویم.

۲. در پنجره Server Manager روی گره Roles کلیک راست کرده و Add Roles را انتخاب می کنیم.

۳. صفحه Before You Begin را مرور کرده و روی دکمه Next کلیک می کنیم.

۴. در صفحه Select Server Roles از ویزارد Add Roles گزینه Active Directory Domain Services را انتخاب کرده و Next را می زنیم.

۵. اطلاعات صفحه Active Directory Domain Services را مرور کرده و روی Next کلیک می کنیم.

۶. انتخاب ها را تایید کرده و روی Install کلیک می کنیم.

۷. نتایج نصب را بررسی کرده و روی دکمه Close کلیک می کنیم. حالا نصب کامل شده است.

۸. بعد روی گره Active Directory Domain Services در Server Manager کلیک می کنیم.

۹. روی Run The Active Directory Domain Services Installation Wizard در پنل وسط کلیک می کنیم.

۱۰. روی Next کلیک می کنیم.

۱۱. اطلاعات صفحه Operating System Compatibility را مرور کرده و روی Next کلیک می کنیم.

۱۲. در صفحه Choose A Deployment Configuration گزینه Create A New Domain In A New Forest را انتخاب کرده و روی Next کلیک می کنیم.

۱۳. در صفحه Name The Forest Root Domain تایپ می کنیم treyresearch.net و روی Next کلیک می کنیم. از نامی با پسوند .Net استفاد می کنیم چون نمی خواهیم از مدل split-brain DNS استفاده کنیم. شرکت Trey Research از یک نام عمومی با پسوند .com روی اینترنت و یک نام با پسوند .net در داخل شبکه استفاده می کند. شرکت هر دو نام دامنه را خریداری کرده و کسی نمی تواند از این نام ها برای ساختار AD DS خود استفاده کند. اگر شرکت با ادغام و یا تفکیک مواجه شود ترکیب این دو خیلی ساده انجام می شود.

۱۴. در صفحه Set Forest Functional Level ویندوز سرور 2008 را از لیست بازشو انتخاب کرده و دکمه Next را کلیک می کنیم.

۱۵. در صفحه Additional Domain Controller Options چک می کنیم که سرور DNS و GC هر دو انتخاب شده باشند. سپس روی Next کلیک می کنیم. توجه کنید که سرویس DNS قبلا روی سرور نصب شده است.

۱۶. اگر آدرس IP ثابت به سرور اختصاص داده نشده باشد توسط ویزارد پیغامی ظاهر می شود. روی گزینه Yes کلیک می کنیم.

۱۷. ویزارد نصب AD DS هشدار می دهد که نمی تواند یک تفویض اختیار برای این سرور بسازد. سپس روی Yes کلیک میکنیم. این خطا به دو علت ایجاد میشود. اول به دلیل اینکه آدرس IP سرور DNS خود آدرس سرور بوده و بنابراین نمیتوانیم به سرور DNS مناسب برای تفویض اختیار دست پیدا کنیم. ثانیا حتی اگر به یک سرور DNS مناسب دسترسی پیدا کنیم از یک روش مبتنی بر نام روی یک نام ریشه سطح اول (.Net) استفاده میکنیم و اعتبار لازم برای ایجاد تفویض اختیار در سرور میزبان آدرس‌های ریشه آن پسوند را نداریم.

۱۸. در صفحه Location For Database, Log Files And SYSVOL محل‌های پیش فرض را قبول و روی Next کلیک می‌کنیم.

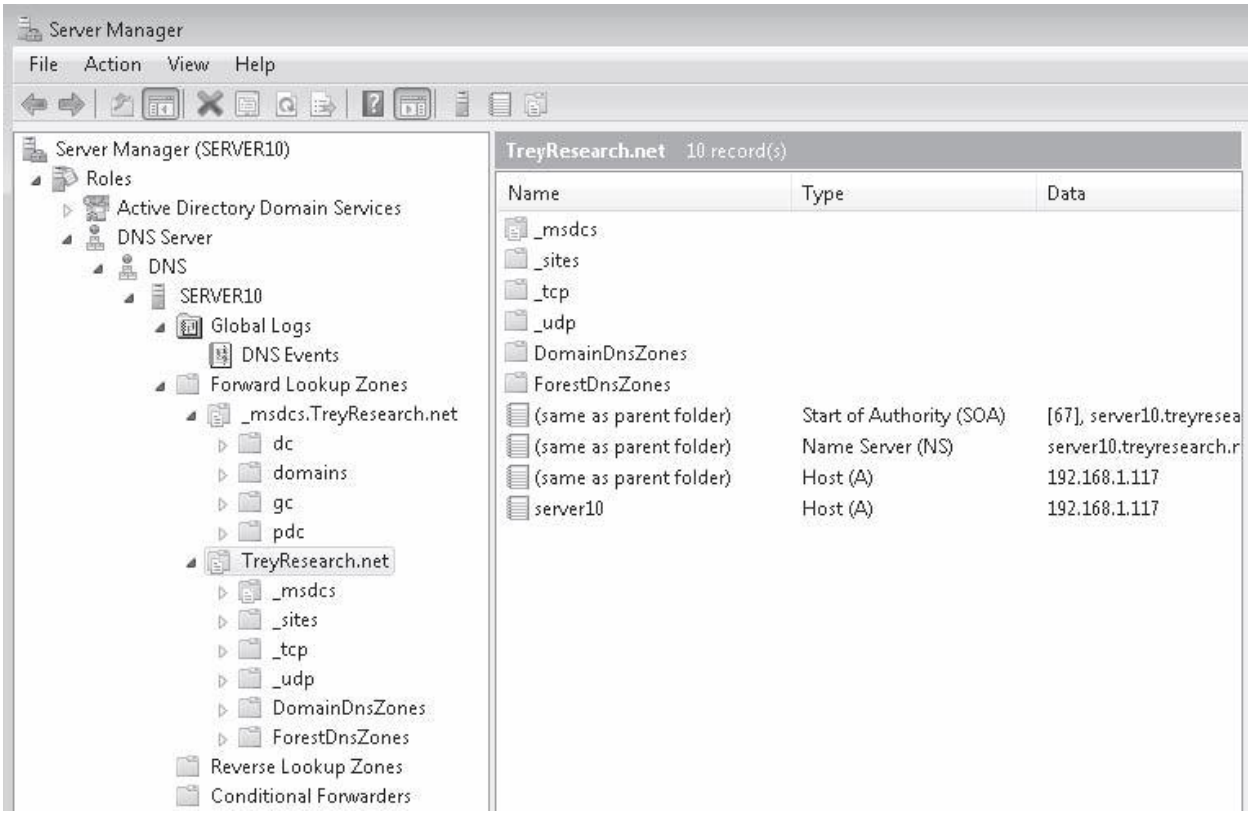
۱۹. در صفحه Directory Services Restore Mode Administrator Password یک کلمه عبور پیچیده تایپ کرده و Next را کلیک می‌کنیم.

۲۰. تنظیمات صفحه Summary را تایید کرده و Next را کلیک می‌کنیم.

۲۱. کادر Reboot On Comletion را علامت زده و منتظر تکمیل پروسه می‌مانیم.

۲۲. بعد از اینکه کامپیوتر دوباره راه‌اندازی شد با اعتبار دامنه‌ای تازه ایجاد شده (TreyResearch\Administrator) وارد شده و گره DNS Server را در Server Manager باز می‌کنیم.

۲۳. تغییرات ایجاد شده در forward lookup zones مربوط به forest جدید را به واسطه راه‌اندازی AD DS مرور می‌کنیم. توجه کنید که داده DNS به دو بخش تقسیم می‌شود یکی از آنها روی کل forest و دیگری روی دامنه ریشه تاثیر می‌گذارد.(شکل ۱۰- ۹)



شکل ۱۰-۹ Active Directory Domain Services entries برای یک forest جدید

تمرین ۳ ساخت یک Zone Delegation به صورت دستی

۱. با کاربر Administrator دامنه به Server10 وارد می‌شویم.

۲. در Server Manager گره DNS Server را باز کرده و روی گره Forward Lookup Zones کلیک می‌کنیم.

۳. روی Forward Lookup Zones کلیک راست کرده و New Zone را انتخاب می‌کنیم. این کار ویزارد New Zone را اجرا می‌کند.

۴. روی Next کلیک می‌کنیم.

۵. در صفحه Zone Type گزینه Primary Zone را انتخاب کرده و مطمئن می‌شویم که کادر Store The Zone In Active Directory علامت دارد و بعد دکمه Next را کلیک می‌کنیم.

۶. در صفحه Active Directory Zone Replication Scope گزینه To All DNS Servers In This Domain:treyresearch.net را انتخاب و دکمه Next را کلیک می‌کنیم. این کار داده DNS را در پارتیشن دایرکتوری برنامه DomainDnsZones برای treyresearch.net جای می‌دهد.

۷. در صفحه Zone Name عبارت northwindtraders.com را تایپ و روی Next کلیک می‌کنیم.

نکته استفاده از پسوندهای غیر از .com

به طور معمول ما از پسوندهای غیر از .com استفاده می‌کنیم تا شبکه داخلی از تداخل نام احتمالی و ابتلا به سندرم split-brain جلوگیری کنیم ولی برای آموزش از این پسوند استفاده می‌کنیم.

۸. در صفحه Dynamic Update گزینه Allow Only Secure Dynamic Updates (برای Active Directory پیشنهاد می‌گردد) انتخاب شده و دکمه Next را کلیک می‌کنیم.

۹. روی Finish کلیک می‌کنیم تا زون ساخته شود.

۱۰. به زون northwindtraders.com رفته و آنرا انتخاب می‌کنیم.

۱۱. روی زون کلیک راست کرده و New Delegation را انتخاب می‌کنیم.

۱۲. روی Next کلیک می کنیم.

۱۳. در صفحه Delegated Domain Name تایپ می‌کنیم SERVER20 که عبارت SERVER20.northwindtraders.com به عنوان نام FQDN لیست می‌شود. بعد روی Next کلیک می‌کنیم.س

۱۴. در صفحه Name Server روی Add کلیک کرده و نام FQDN سروری که می‌خواهیم برای این زون بسازیم تایپ می‌کنیم. اینجا نام آن SERVER20.northwindtraders.com است.

۱۵. به بخش IP Addresses Of This NS Record از کادر محاوره‌ای رفته و روی عبارت Click Here To Add An IP Address کلیک می‌کنیم و سپس آدرس IP که به SERVER20 اختصاص داده‌ایم را تایپ می‌کنیم. سپس دکمه OK را کلیک می کنیم.

۱۶. روی Next کلیک کرده و Finish را می‌زنیم تا تفویض صورت گیرد.

تمرین ۴ نصب AD DS و ساخت Domain Tree جدید

۱. با کاربر Administrator محلی به SERVER20 وارد می‌شویم.

۲. در Server Manager روی Roles کلیک راست کرده و Add Roles را انتخاب می‌کنیم.

۳. صفحه Before You Begin را مرور کرده و روی Next کلیک می‌کنیم.

۴. در صفحه Select Server Roles از ویزارد Add Roles گزینه Active Directory Domain Services را انتخاب کرده و روی Next کلیک می‌کنیم.

۵. اطلاعات صفحه Active Directory Domain Services را مرور کرده و دکمه Next را کلیک می‌کنیم.

۶. تنظیمات انتخابی را تایید کرده و Install را کلیک می‌کنیم.

۷. نتایج نصب را بررسی کرده و روی Close کلیک می‌کنیم. نصب کامل شده است.

۸. بعد روی گره Active Directory Domain Services در Server Manager کلیک می‌کنیم.

۹. روی Run The Active Directory Domain Services Installation در پنل وسط کلیک می‌کنیم.

۱۰. کادر Use Advanced Mode Installation را انتخاب کرده و روی Next کلیک می‌کنیم.

۱۱. اطلاعات صفحه Operating System Compatibility را مرور کرده و روی Next کلیک می‌کنیم.

۱۲. در صفحه Choose A Deployment Configuraion گزینه Existing Forest و بعد Create New Domain In An Existing Forest و سپس Create A New Domain Tree Root Instead Of A New Child Domain را انتخاب کرده و دکمه Next را کلیک می‌کنیم.

۱۳. در صفحه Network Credentials تایپ می‌کنیم treyresearch.net و بعد روی Set کلیک می‌کنیم تا بتوانیم اعتبار جایگزین را وارد کنیم. تایپ می‌کنیم treyresearch.net\administrator یا نام کاربری و کلمه عبور معادل آن را وارد می‌کنیم. روی OK و سپس Next کلیک می‌کنیم.

۱۴. در صفحه Name The New Domain Tree Root تایپ می‌کنیم northwindtraders.com و روی Next کلیک می‌کنیم.

۱۵. در صفحه Domain NetBIOS Name نام پیشنهادی را قبول می‌کنیم و روی Next کلیک می‌کنیم.

۱۶. در صفحه Select A Site مقدار پیش فرض را قبول کرده و روی Next کلیک می‌کنیم. نمایش این صفحه همچنین ادامه می‌یابد چون ویزارد در حالت پیشرفته اجرا می‌شود.

۱۷. در صفحه Additional Domain Controller Options چک می‌کنیم که کادر سرور DNS علامت داشته باشد. کادر Global Catalog را نیز علامت زده و روی Next کلیک می‌کنیم.

۱۸. اگر آدرس IP ثابت به سرور اختصاص نداده باشیم ویزارد پیغام هشداری تولید می‌کند .

۱۹. No, Do Not Create The DNS Delegation را انتخاب و روی Next کلیک می‌کنیم.

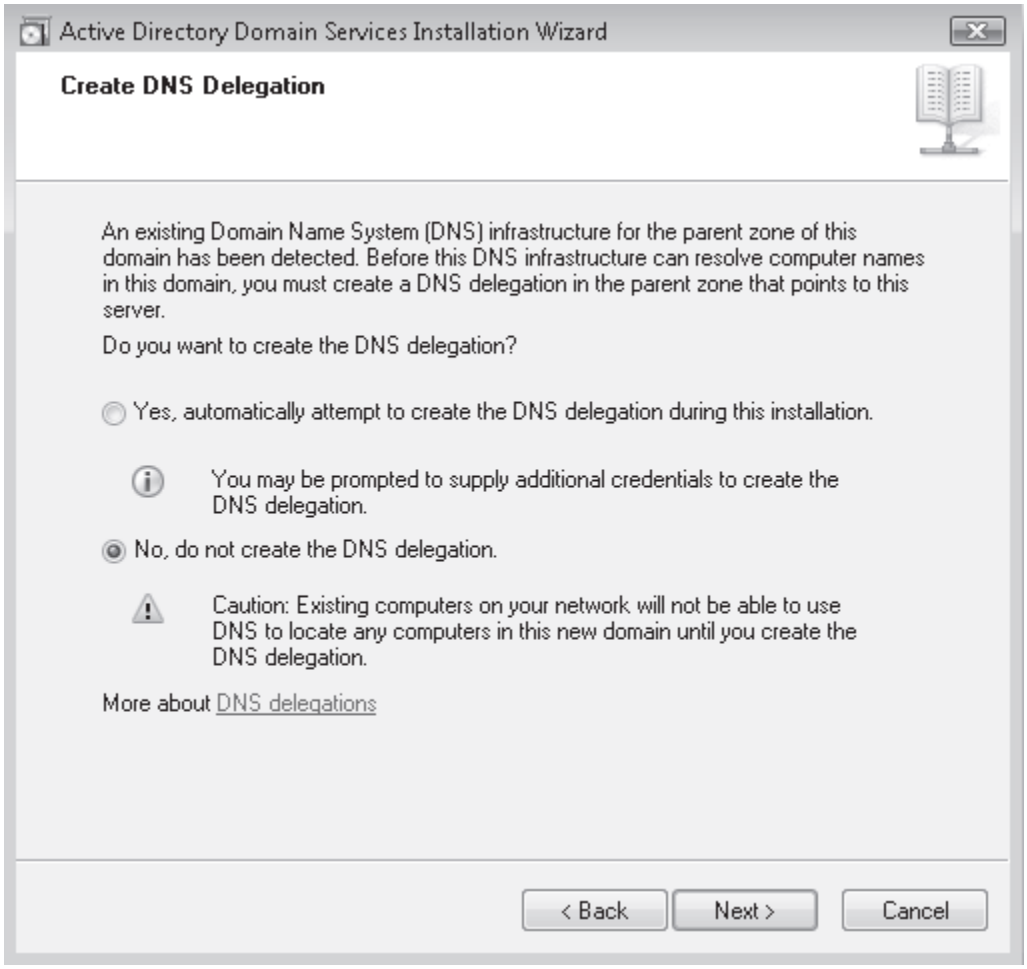
۲۰. در صفحه Source Domain Controller چک می‌کنیم که Let The Wizard Choose An Appropriate Domain Controller انتخاب شده و روی Next کلیک می‌کنیم.

۲۱. در صفحه Location For Database, Log Files And SYSVOL محل‌های پیش فرض را قبول و روی Next کلیک می‌کنیم.

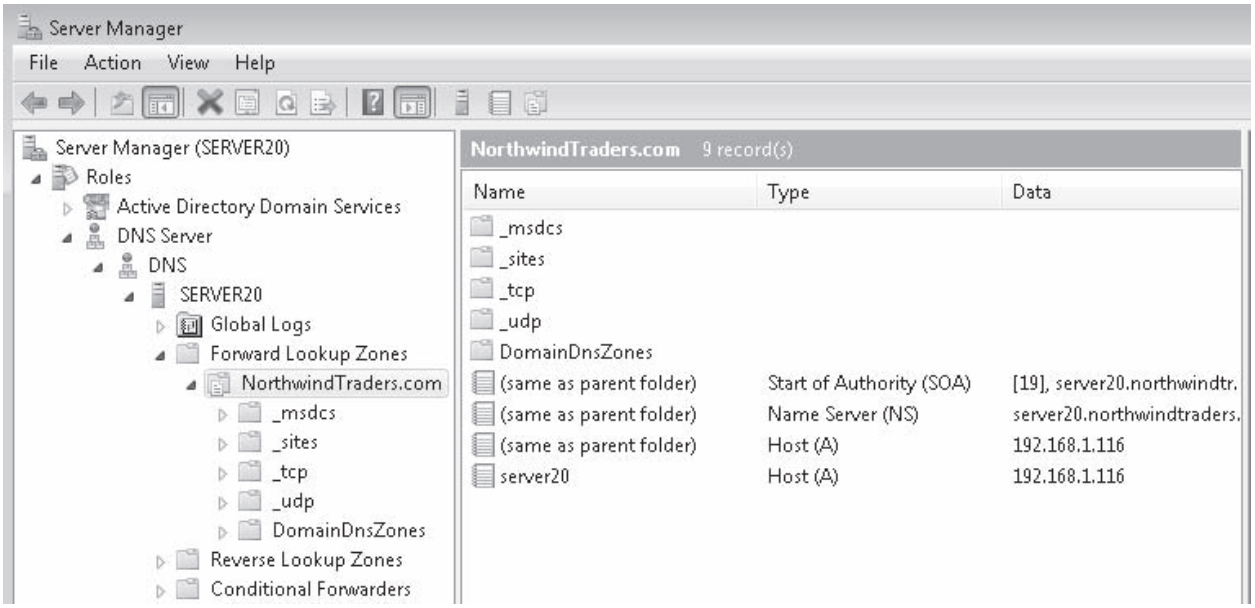
۲۲. در صفحه Directory Services Restore Mode Administrator Password یک کلمه عبور پیچیده تایپ کرده و آنرا تایید می‌کنیم.

۲۳. در صفحه Summary تنظیمات را تایید کرده و روی Next کلیک می‌کنیم. کادر Reboot On Completion را علامت زده و منتظر تکمیل عملیات می‌مانیم.

۲۴. وقتی کامپیوتر راه اندازی مجدد شد با اعتبار دامنه جدید (North-windTraders\Administrator) وارد می‌شویم و به گره DNS Server در Server Manager می‌رویم. تغییرات ایجاد شده در FLZ های Tree جدید را هنگام راه اندازی AD DS مرور می‌کنیم.



شکل ۱۱- ۹ صفحه Create DNS Delegation



شکل ۱۲- ۹ Active Directory Domain Services entries برای Tree در یک forest موجود

تمرین ۵ نصب AD DS و ساخت دامنه فرزند

۱. با کاربر Administrator به SERVER30 وارد می‌شویم

۲. در Server Manager روی گره Roles کلیک راست کرده و Add Roles را انتخاب می‌کنیم

۳. صفحه Before You Begin را مرور کرده و روی Next کلیک می‌کنیم.

۴. در صفحه Select Server Roles از ویزارد Add Roles گزینه Active Directory Domian Services را انتخاب کرده و روی Next کلیک می‌کنیم.

۵. اطلاعات صفحه AD DS را مرور کرده و روی Next کلیک می‌کنیم.

۶. انتخاب‌های خود را تایید کرده و روی Install کلیک می‌کنیم.

۷. نتایج نصب را بررسی کرده و روی Close کلیک می‌کنیم

۸. روی گره Active Directory Domain Services در Server Manager کلیک می‌کنیم.

۹. در پنل وسط روی Run The Active Directory Domain Services Installation Wizard کلیک می‌کنیم.

۱۰. روی Next کلیک می‌کنیم.

۱۱. اطلاعات صفحه Operating System Compatibikity را مرور کرده و روی Next کلیک می‌کنیم.

۱۲. در صفحه Choose Deployment Configuration گزینه Existing Forest And Create A New Domain In An Existing Forest را انتخاب کرده و روی Next کلیک می‌کنیم.

۱۳. در صفحه Network Credential عبارت treyresearch.net را تایپ کرده و روی Set کلیک می‌کنیم و اعتبار مناسب را وارد می‌کنیم.

۱۴. در کادر محاوره ای Network Credentials عبارت treyresearch\administrator یا اعتبار مشابه را تایپ کرده سپس کلمه عبور را تایپ می‌کنیم و دکمه OK و سپس Next را کلیک می‌کنیم.

۱۵. در صفحه Name The New Domain عبارت treyresearch.net را به عنوان نام FQDN دامنه والد و intranet را در فیلد child domain تایپ کرده و روی Next کلیک می‌کنیم. نام FQDN به صورت intranet.treyresearch.net خواهد شد.

۱۶. در صفحه Select A Site از تنظیمات پیش فرض استفاده کرده و روی Next کلیک می‌کنیم.

۱۷. در صفحه Additional Domain Controller Options کادر DNS Server و Global Catalog را علامت زده و روی Next کلیک می‌کنیم.

۱۸. روی Yes, The Computer Will Use A Dynamically Assigned IP Address (Not Recommanded) کلیک می‌کنیم.

۱۹. در صفحه Location For Database, Log Files And SYSVOL محلهای پیش فرض را قبول کرده و روی Next کلیک می‌کنیم.

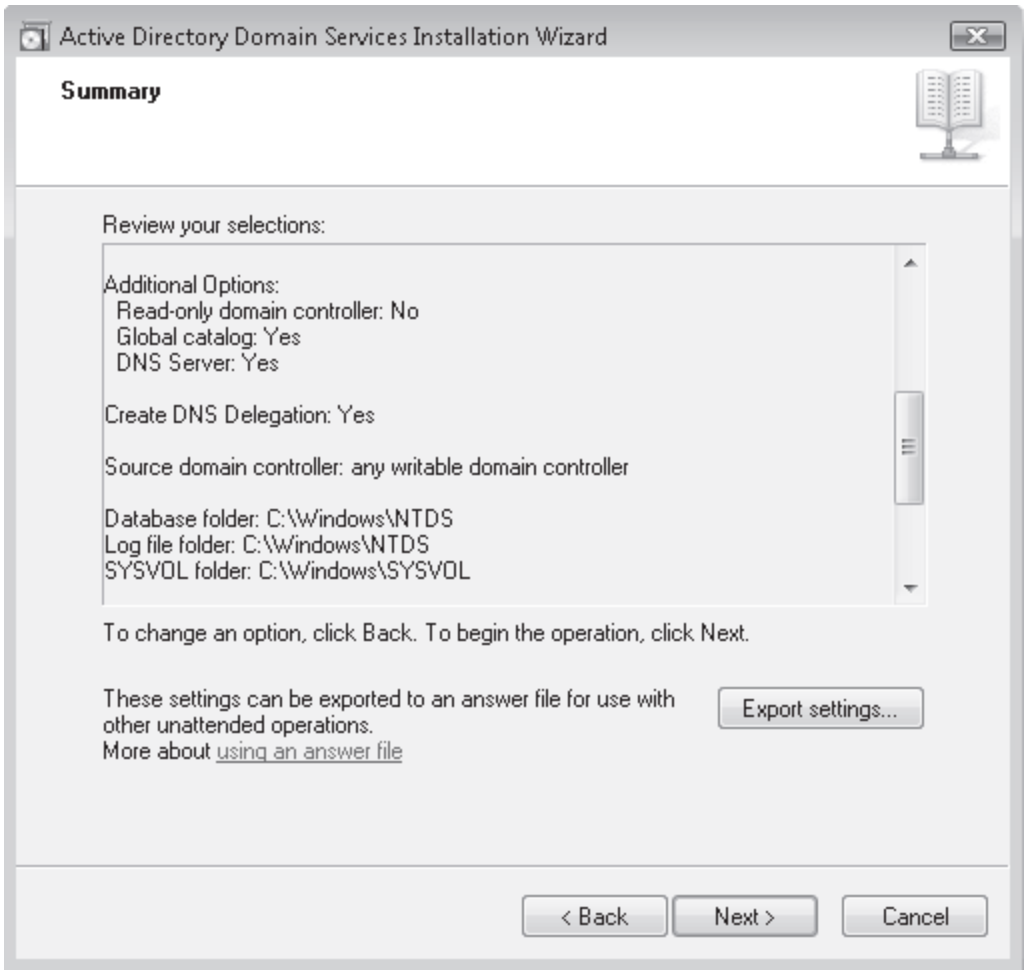
۲۰. در صفحه Directory Services Restore Mode Administrator Password کلمه عبور پیچیده تایپ کرده و پس از تایید روی Next کلیک می‌کنیم.

۲۱. تنظیمات را در صفحه Summary تایید کرده و روی Next کلیک می‌کنیم.

۲۲. کادر Reboot On Completion را علامت زده و منتظر پایان عملیات می‌مانیم.

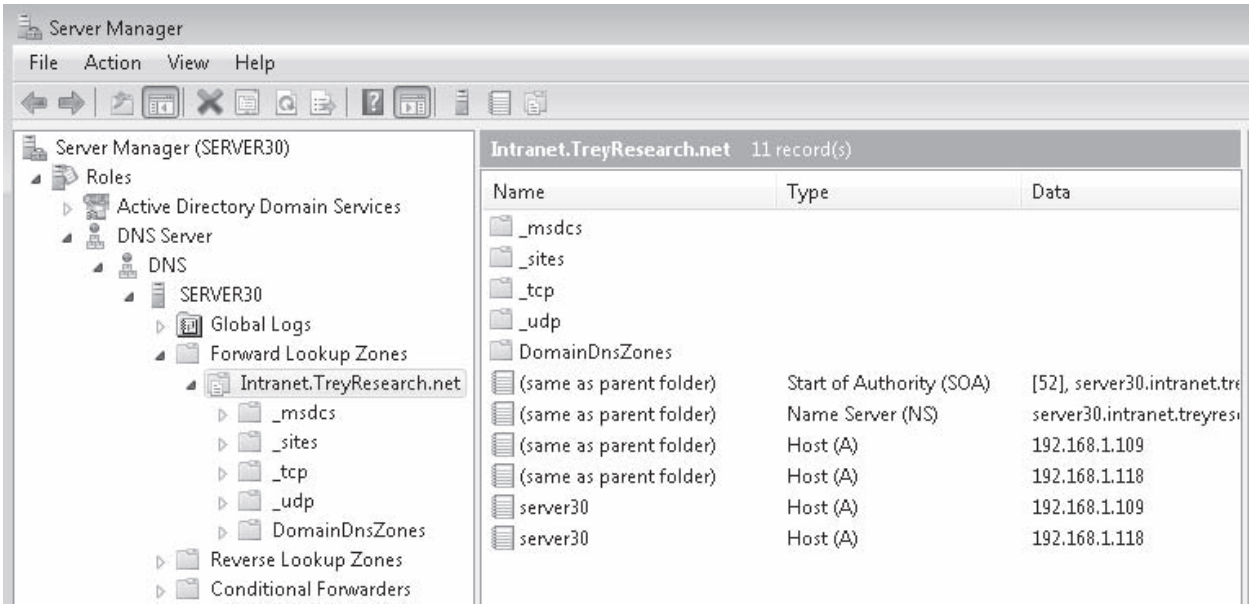
۲۳. وقتی کامپیوتر راه‌اندازی مجدد شد با کاربر دامنه جدید (Intranet\Administrator یا چیزی معادل آن) وارد می‌شویم و گره DNS Server را در Server Manager باز می‌کنیم.

۲۴. تغییرات ایجاد شده در FLZ این دامنه جدید را که هنگام نصب AD DS ساخته شده مرور می‌کنیم. توجه داشته باشید که همانند شکل ۱۴- ۹ داده DNS فقط در یک بخش که روی این دامنه خاص تاثیرگذار است موجود می‌باشد. همچنین اگر به SERVER10 برگردیم خواهیم دید که تفویض DNS جدید (آیکن خاکستری به جای زرد) برای این دامنه فرزند در FLZ treyresearch.net ساخته شده است.



۲۵.

شکل ۱۳- ۹ صفحه Active Directory Domain Services Installation Summary



شکل ۱۴- ۹ Active Directory Domain Services entries برای یک دامنه فرزند جدید در یک forest موجود

خلاصه درس

- DNS یک سیستم تحلیل نام است که بر اساس یک ساختار نام‌گذاری سلسله مراتبی کار می‌کند و آدرسهای IP را به نام FQDN نگاشت (map) می‌کند که به شکل object.namespace.rootname است.
- AD DS همچنین به ساختار سلسله مراتبی متکی است. در حقیقت ساختار AD DS forest کاملا بر اساس ساختار سلسله مراتبی موجود DNS کار می‌کند.
- چون ویندوز سرور 2008 به منظور پشتیبانی از Ipv6 ارتقا پیدا کرده است و این پروتکل به طور پیش فرض با آدرسهای link-local نصب میشود ، سرور DNS در ویندوز سرور 2008 از قالب آدرسهای ۱۲۸ بیت مورد استفاده از Ipv6 پشتیبانی می‌کند.
- DNS Server سه نوع زون می‌تواند داشته باشد. زونهای اولیه که خواندنی نوشتنی هستند و حاوی داده تحلیل نام برای فضای نام مشخص می‌باشند. زونهای ثانویه که فقط خواندنی هستند حاوی یک کپی از زون اولیه می‌باشند. زونهای stub که اشاره‌گرهایی هستند که به سرورهای DNS دیگر اشاره می‌کنند و دارای لیست سرورهای authoritative برای فضای نام مورد اشاره می‌باشند. همه انواع زونها می‌توانند با AD DS برای ذخیره‌سازی در بانک دایرکتوری عجین شوند.

سئوالات پایان درس

۱. فرض کنید مدیر شبکه شرکت Contoso, Ltd هستید. شرکت تصمیم می‌گیرد به ویندوز سرور 2008 ارتقا پیدا کند و به دلیل تجربه قبلی شما تصمیم می‌گیرید به جای ارتقا ساختار موجود یک ویندوز سرور جدید نصب کنید. پس از نصب ساختار جدید همه داده (حساب‌ها، تنظیمات دایرکتوری و غیره) را به forest جدید که با ویندوز سرور 2008 پیاده‌سازی شده است منتقل می‌کنید. از شما خواسته می‌شود ساختار اولیه forest را بسازید. این forest حاوی یک دامنه ریشه، یک global child production domain و یک domain tree می‌باشد. forest دارای پسوند .net بوده و domain tree از پسوند .ms استفاده می‌کند تا production forest متمایز باشد. شما دامنه ریشه forest و دامنه فرزند را می‌سازید ولی هنگام رفتن به سراغ domain tree متوجه می‌شوید که گزینه domain tree پیدا نمی‌شود. مشکل از کجا ناشی می‌شود؟

A. در ویزارد Active Directory Domain Services Installation Wizard نمی‌توان domain tree ساخت. شما باید از دستور Dcpromo.exe استفاده کنید.

B. با کاربر مناسب وارد نشده‌اید.

C. باید به صفحه Welcome ویزارد برگردید و با حالت Advanced ادامه دهید.

D. سروری که شما استفاده می‌کنید عضو دامنه ریشه forest نیست.

۲. فرض کنید مدیر شبکه شرکت Contoso, Ltd هستید. شرکت تصمیم می‌گیرد به ویندوز سرور 2008 ارتقا پیدا کند و به دلیل تجربه قبلی شما تصمیم می‌گیرید به جای ارتقا ساختار موجود یک ویندوز سرور جدید نصب کنید. پس از نصب ساختار جدید همه داده (حساب‌ها، تنظیمات دایرکتوری و غیره) را به forest جدید که با ویندوز سرور 2008 پیاده‌سازی شده است منتقل می‌کنید. از شما خواسته می‌شود ساختار اولیه forest را بسازید. این forest حاوی یک دامنه ریشه، یک global child production domain و یک domain tree می‌باشد. forest دارای پسوند .net بوده و domain tree از پسوند .ms استفاده می‌کند تا production forest متمایز باشد. شما دامنه ریشه forest و دامنه فرزند را می‌سازید ولی هنگام رفتن به سراغ domain tree متوجه می‌شوید که نمی‌توانید تفویض اختیار بسازید. این کار با تعویض کاربر یا گزینه‌ها نیز امکان‌پذیر نمی‌شود. مشکل از کجا ناشی می‌شود؟ (در صورت صحیح بودن همه را نیز می‌توانید انتخاب کنید.)

A. باید حالت advanced ویزارد را برای ساخت تفویض اختیار انتخاب کنیم.

B. باید قبل از ساخت domain tree تفویض دستی بسازیم.

C. در زمان ساخت domain tree و فراهم کردن اعتبار مناسب باید به ویزارد باید بگوییم که تفویض اختیار را بسازد.

D. در زمان ساخت domain tree باید به ویزارد بگوییم که ساخت تفویض را حذف کند.

E. پس از ساخت domain tree باید تفویض را به صورت دستی بسازیم.

درس ۲: پیکربندی و استفاده از DNS

وقتی نقش سرور DNS را به همراه AD DS نصب می‌کنیم به کمی پیکربندی نیاز داریم. FLZ ها به طور خودکار ایجاد می‌شوند. عملیات تکثیر به طور خودکار پیکربندی می‌شود زیرا روی سیستم تکثیر AD DS multimaster سوار می‌شود. و ما حتی نیاز به افزودن رکورد نداریم چون همه کامپیوترهای با سیستم عامل ویندوز 2000 به بعد رکورد خود را در DNS AD DS پویا ثبت و به روز می‌کنند.

ولی برخی عملیات به طور خودکار اجرا نمی‌شوند. برای مثال سرور DNS به طور پیش فرض دارای FLZ نیست. افزودن آنها برای پشتیبانی از جستجوی معکوس فکر خوبی است. به علاوه سرور DNS نیاز به تکمیل پیکربندی دارد. برای مثال باید آنرا برای پاک کردن خودکار رکوردهای تاریخ مصرف گذشته پیکربندی کنیم.

همچنین مرور همه اجزاء سرور DNS برای آشنایی با آن و بررسی منطبق بودن آن با نیاز ما فکر خوبی است.

بعد از این درس یاد می‌گیریم:

- پیکربندی سرور DNS را تکمیل کنیم.
- سرورهای DNS و تکثیر DNS را مدیریت کنیم.
- زمان تقریبی : ۴۰ دقیقه

پیکربندی DNS

پیکربندی DNS شامل عملیات متعددی است که عبارتند از:

- اهمیت دادن به امنیت سرورهای DNS به منظور کاهش سطح نفوذپذیری (attack surface)
- پیکربندی تنظیمات scavenging برای سرور
- تکمیل پیکربندی FLZ ها
- ساخت FLZ ها
- افزودن رکوردهای رایج به FLZ ها برای سرویس‌ها و منابع خاص

همچنین لازم است از اجرای مناسب عملیات تکثیر DNS اطمینان حاصل کنیم.

تمهیدات امنیتی برای نقش سرور DNS

سرورهای DNS که در اینترنت در دسترس هستند یک هدف ایده‌آل برای نفوذگران به حساب می‌آیند. رایج‌ترین حمله denial-of-service یا به اختصار DoS می‌باشد. مکانیزم حمله به این شکل است که درخواست‌های متعددی برای سرور ارسال می‌شود و سرور دیگر قادر به پاسخ‌گویی نیست. نوع دیگر حمله به دست آوردن اطلاعات سرور DNS به قصد شناسایی اشیاء شبکه است. نام این روش footprinting the network است. حمله دیگر تلاش برای دست‌کاری سرور DNS به منظور تغییر مسیر درخواست کاربران از سرور معتبر به سرور نامعتبر که تحت کنترل نفوذگر است می‌باشد. نوع دیگر تغییر داده DNS در DNS cache می‌باشد. به خاطر داشته باشید که DNS از روش in-memory caching برای افزایش سرعت پاسخ‌گویی به درخواست‌های DNS استفاده می‌کند. وقتی این داده خراب شود کاربران پاسخ‌های غیر معتبر دریافت می‌کنند.

این موارد دلیل اهمیت امنیت در پیاده‌سازی DNS می‌باشد. وقتی از رویکرد مناسب برای پیکربندی DNS استفاده می‌کنیم و برپایه عجین شدن DNS با AD DS در شبکه کار می‌کنیم سرور DNS داخلی کمتر در معرض حمله قرار می‌گیرد زیرا آنها فضای نام را با دنیای بیرون به اشتراک نمی‌گذارند و بنابراین به واسطه وجود دیواره آتش از دسترسی بیرونی به سرور DNS داخلی جلوگیری به عمل می‌آید. معنی این جمله عدم نیاز به حفاظت در سرورهای DNS داخلی نیست. هرگاه کاربر نامطمئنی به شبکه متصل شود چه با ارتباط کابلی و چه بیسیم ساختار شبکه در معرض خطر قرار می‌گیرد. به همین دلیل است که extensive screening روش مناسبی برای برقراری ارتباط یک کاربر ناشناس با شبکه می‌باشد. نمی‌توان گفت چون ما در آنسوی دیوار آتش هستیم و همه چیز در آنجا به طور پیش فرض محافظت شده است دیگر مشکل امنیتی نداریم.

رویکرد دیگری در ارتباط با سرورهای داخلی و خارجی DNS مطرح است. وقتی سرورها در یک شبکه داخلی یا DMZ قرار دارند باید از امنیت بالایی برخوردار باشند. یک روش محافظتی خوب استفاده از سرور ثانویه یا فرعی است فقط وقتی که سرور در معرض دنیای بیرون است. سپس می‌توانیم به روز رسانی زون‌ها را پیکربندی کنیم تا فقط از منابع شناخته شده که در خود DNS مشخص شده‌اند به روز رسانی را قبول کنند.

یک شبکه داخلی نقش سرور DNS را با نقش DC پیوند می‌زنند و تضمین می‌کنند که فقط از به روز رسانی پویای امن پشتیبانی می‌کنند. این کار به حفاظت آنها از دریافت یا انتقال داده غلط کمک می‌کند. صحت داده DNS را در فواصل زمانی مشخص بررسی می‌کنیم و event log مربوط به DNS را مانیتور می‌کنیم تا مشکلات امنیتی بالقوه را شناسایی کنیم.

کار با تنظیمات سرور DNS

سرور DNS رکوردهای نام را در بازه زمانی مشخص ذخیره می‌کند. هر رکورد نام مقدار TTL دارد. وقتی این زمان منقضی می‌شود رکورد برای ممانعت از اشتباه باید حذف شود. خوشبختانه سرور DNS در ویندوز سرور 2008 این کار را به طور خودکار از طریق پروسه scavenging انجام می‌دهد. وقتی این پروسه روی سرور اعمال شود همه زون‌های فعال پاک می‌شوند و وقتی روی زون مشخصی اعمال شود فقط رکوردهای همان زون پاک می‌شوند.

پیکربندی Scavenging برای همه زون‌ها

برای تنظیم scavenging برای کل سرور باید از منوی action سرور اقدام کنیم.

۱. روی نام سرور در گره DNS مربوط به Server Manager کلیک راست کرده و گزینه Set Aging/Scavenging For All Zones را انتخاب میکنیم.

۲. کادر Scavenge Stale Resource Records را علامت میزنیم. عبارت No-Refresh Interval به زمان بین به روز رسانی اخیر stamp یک رکورد و لحظهای که سیستم به timestamp اجازه به روز رسانی میدهد برمیگردد. بازه زمانی به روز رسانی به نزدیکترین زمانی که یک رکورد ممکن است به روز شود گویند. مقدار پیش فرض هفت روز است که برای اکثر شبکهها کافی است.

۳. مقادیر پیش فرض را OK میکنیم.

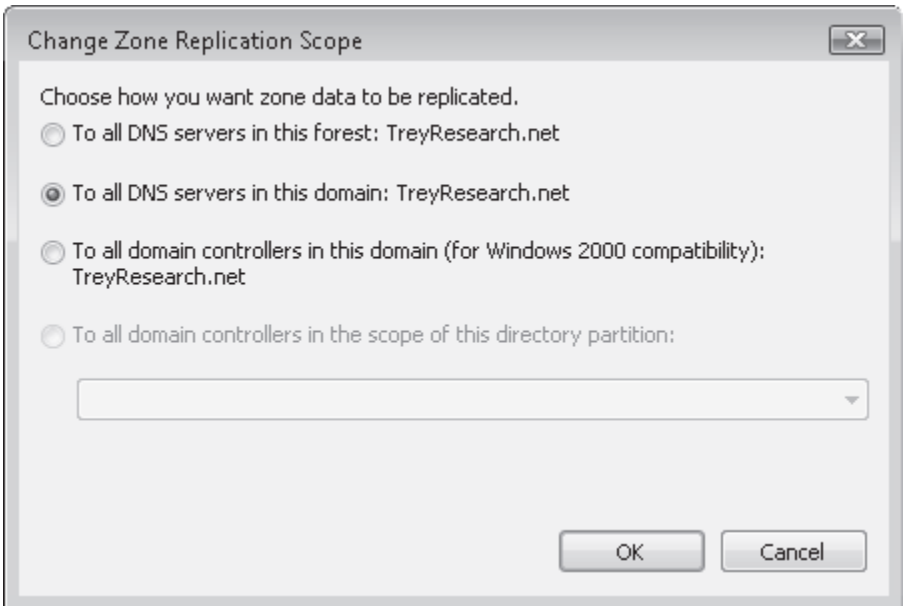
۴. به دلیل اینکه مقادیر زونهای موجود را تنظیم میکنیم DNS به ما امکان میدهد بعدا زونهای جدید را تنظیم کنیم که از آن جمله زونهای عجین شده Active Directory میباشد. کادر Apply These Settings To The Existing Active Directory-Integrated Zones را علامت زده و OK میکنیم.

زونهای DNS برای حذف رکوردهای کهنه تنظیم میشود. این تنظیمات را به همه سرورهای DNS اعمال کنید. این بخش را به عنوان پیکربندی پیش فرض سرورهای DNS تعریف کنید. اگر نیاز به تغییر تنظیمات یک زون تنها داشته باشیم باید از کادر محاورهای Properties همان زون استفاده کنیم. پاکسازی زون توسط زبانه General و کلیک روی دکمه Aging اجرا میشود.
توجه داشته باشید که با کلیک راست روی سرور میتوانیم روی Scavenging Stale Resource Records کلیک کرده و پاکسازی را پیکربندی کنیم.
برای از بین بردن رکوردهای کهنه از دستور Clear Cache منوی کلیک راست سرور استفاده میشود. به دلیل اینکه سرور DNS به شدت به کش in-memory وابسته است باید رکوردهای کهنه را از بانک پاک کنیم.

تکمیل پیکربندی FLZ وقتی کادر محاورهای Properties یک FLZ را باز میکنیم گزینههای زیادی را در رابطه با هر زون میبینیم که بهترین راه حل هر کدام را معرفی میکنیم:

- در زبانه General مطمئن میشویم که همه زون DNS داخلی با Active Directory عجین شده باشد، از حوزه تکثیر مناسب برخوردار باشد و از به روز رسانی پویای امن پشتیبانی کند.
  - زونهای DNS مبتنی بر دامنه باید به همه سرورهای DNS در دامنه تکثیر شود. همه DC هایی که نقش DNS هم دارند باید زون را داشته باشند.
  - زونهای forest DNS باید به همه سرورهای DNS در forest تکثیر شوند.
  - اگر در شبکه DC ویندوز سرور 2000 داریم باید از گزینه To All Domain Controllers In This Domain (For Windows 2000 Compatibility) استفاده کنیم زیرا ویندوز سرور 2000 از پارتیشنهای دایرکتوری برنامه پشتیبانی نمیکند.

- میتوانیم برای پارتیشنهای دایرکتوری برنامه خاص برنامه تکثیر تعیین کنیم ولی ابتدا باید پارتیشن بسازیم.

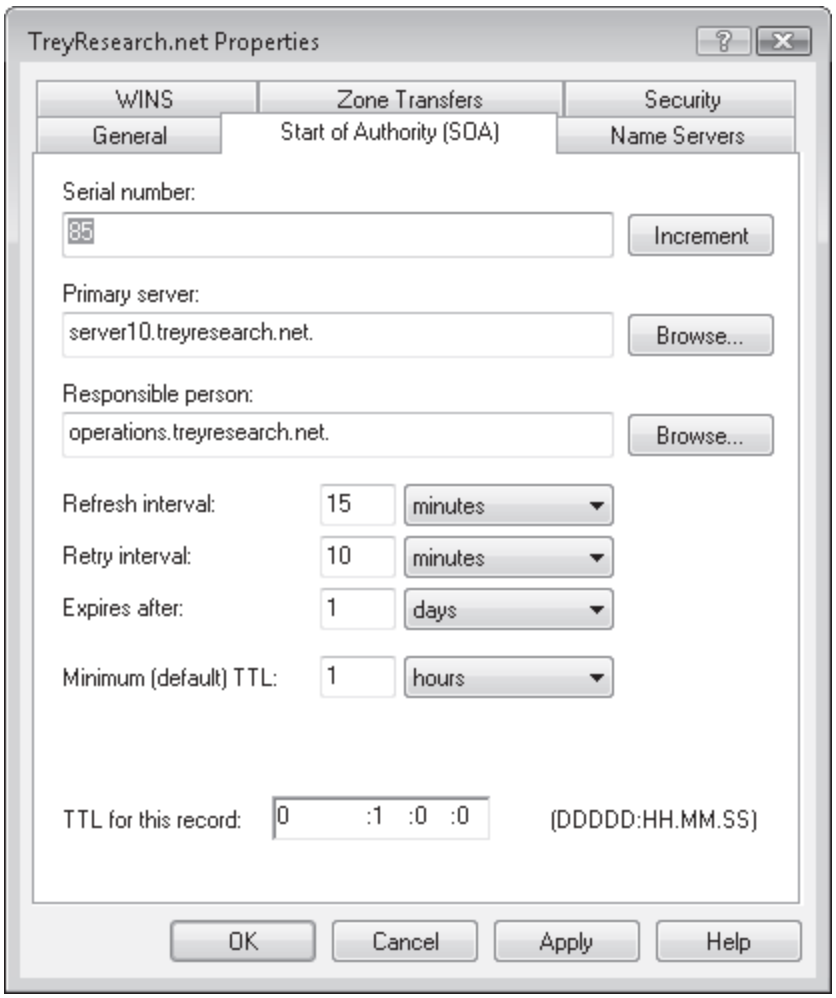


- در زبانه Name Server چک میکنیم که همه زونهای DNS حاوی حداقل دو سرور نام باشد. همانطوریکه ما حداقل برای هر دامنه دو عدد DC در نظر میگیریم دو سرور DNS هم برای هر زون در نظر میگیریم.
- در زبانه WINS اگر از GNZ نمیتوانیم استفاده کنیم و بخواهیم سرویس WINS را توزیع کنیم WINS lookup پیکربندی میکنیم. در این درس مدیریت نامهای تک بخشی بحث خواهد شد.
- در زبانه Zone Transfers سرورهای نام را که می‌خواهیم به آنها اجازه دهیم این زون‌ها را منتقل کنند مشخص می‌کنیم. اگر این زون با Active Directory عجین شده باشد نیازی به انتقال زون نیست. این زبانه بیشتر برای نصب سرور DNS قدیمی استفاده می‌شود.
- در زبانه Security تنظیمات امنیتی پیش فرض را بررسی می‌کنیم. برای بیشتر شبکه‌ها این تنظیمات مناسب است ولی در شرایط امنیتی بالا نیاز به ویرایش دارند.
- زبانه آخر SOA است. رکورد SOA زون و اطلاعات وابسته را نظیر owner، update schedules و غیره را تعریف می‌کند. این رکوردها حاوی اطلاعات زیر هستند:
  - شماره سریال که هنگام ساخت زون ایجاد می‌شوند. امکان افزایش این شماره وجود دارد.
  - سرور اولیه سرور اصلی برای این زون می‌باشد که معمولا همان جایی است که برای اولین بار زون ساخته می‌شود.
  - شخص مسئول (Responsible Person) باید نام کاربر این سرور را لیست کند. به طور پیش فرض ویندوز سرور 2008 این فرد hostmaster.dnszonename است به طوری که dnszonename نام FQDN زون مربوطه می‌باشد. این کاربران مبتنی بر رکوردهای Responsible Person است. این

رکوردها به طور پیش‌فرض ساخته نمی‌شوند بنابراین باید رکوردهای مناسب برای هر زون یا حداقل برای هر سرور DNS اصلی ساخته شده و آنرا به این مقدار نسبت دهیم.

- SOA تنظیمات مبتنی بر زمان را برای رکورد لیست می‌کند. این تنظیمات شامل Refresh Interval، Retry Interval، تنظیم Expires After و Minimum (Default) TTL برای هر رکورد می‌باشد. مقادیر پیش‌فرض برای اکثر انواع رکورد قابل قبول است.

- آخرین مقدار SOA ، TTL For This Record است. توجه داشته باشید مقدار آن مساوی مقداری است که Minimum TTL در بالای آن در کادر محاوره‌ای مشخص می‌کند.



این تنظیمات را برای هر زون که می‌خواهیم روی سرور DNS مدیریت کنیم نهایی می‌کنیم.

ساخت رکورد Responsible Person

همان‌طوریکه قبلا اشاره شد باید به هر زون یک Responsible Person (RP) نسبت دهیم. این یعنی ما حداقل به یک رکورد RP در پیکربندی DNS خود نیاز داریم. از منوی کلیک راست برا ی ساخت رکورد ، روی زونی که می‌خواهیم میزبان این رکورد باشد کلیک راست می‌کنیم. آیتم‌های مختلفی برای این کار مورد نیاز است که در زیر شرح داده می‌شود:

- **A Common Group Name** این نام در رکورد نمایش داده می‌شود.

- **A Group Mailbox In The Directory** بهترین راه این است که از یک صندوق پستی گروهی (group mailbox) استفاده کنیم.

- **A Text Record To Include With The Responsible Person Record** رکورد متنی می‌تواند اطلاعات مربوط به سازمان و سیاست‌های مدیریت DNS خود را نشان دهد.

برای ساخت رکورد RP مراحل زیر را دنبال می‌کنیم. با رکورد متنی شروع می‌کنیم.

۱. روی نام زون کلیک راست کرده و Other New Records را انتخاب می‌کنیم.

۲. در لیست Select A Resource Record Type گزینه Text (TXT) را انتخاب کرده و روی Create Record کلیک می‌کنیم.

۳. در کادر محاوره‌ای New Resource Record نام رکورد را تایپ کرده (مثلا Disclaimer) و به کادر Text می‌رویم.

۴. پیغام خود را تایپ می‌کنیم. روی OK کلیک می‌کنیم تا رکورد ساخته شود. این کار ما را به کادر محاوره‌ای Resource Record Type می‌برد.

۵. در لیست Select A Resource Record Type گزینه Responsible Person (RP) را انتخاب کرده و روی Create Record کلیک می‌کنیم.

۶. در کادر محاوره‌ای New Resource Record نام رکورد را در کادر متنی Host Or Domain وارد می‌کنیم. مثلا Operation و سپس روی Browse کلیک می‌کنیم تا صندوق پستی RP را پیدا کنیم. همچنین اگر آدرس آن را بدانیم آنرا تایپ می‌کنیم.

۷. روی Browse کلیک می‌کنیم و رکورد متنی جدید را پیدا می‌کنیم. برای پیدا کردن رکورد متنی به زونی که با آن کار می‌کنیم رفته و آنرا انتخاب کرده و روی OK کلیک می‌کنیم.

۸. روی OK کلیک می‌کنیم تا رکورد ساخته شود. روی Done کلیک کرده تا کادر بسته شود.

۹. به کادر محاوره‌ای Properties زون برگشته یا روی رکورد Start Of Authority دوبار کلیک می‌کنیم تا رکورد RP را به رکورد SOA نسبت دهیم.

برای همه زون‌ها این عملیات را انجام می‌دهیم. همیشه پیکربندی زون به طور کامل قبل از بروز مشکل بهترین راه حل است.

ساخت زون‌های Reverse Lookup

شبکه‌های کوچک با تعداد کامپیوترهای کم مثلا کمتر از ۵۰۰ دستگاه ممکن است نیاز به RLZ نداشته باشند. این زون‌ها کار تحلیل یک آدرس IP را به یک نام انجام می‌دهند. این نوع زون‌ها بیشتر توسط برنامه‌های کاربردی مورد استفاده قرار می‌گیرند. برای مثال یک برنامه کاربردی تحت وب امن از این نوع زون برای بررسی صحت هویت کامپیوتری که با آن در ارتباط است استفاده می‌کند. اگر چنین برنامه‌ای در سازمان وجود ندارد نیازی به این زون نمی‌باشد

بهرحال کلاینت‌هایی که توانایی به روز رسانی رکورد DNS خود را به صورت پویا دارند رکورد PTR هم می‌سازند. رکورد PTR رکوردی است که آدرس IP را به نام نگاشت می‌کند. سپس سعی می‌کنند آنرا در RLZ که با RLZ میزبان رکورد نام خود در ارتباط است ذخیره کنند. اگر هیچ RLZ موجود نباشد این رکوردها هرگز تولید نمی‌شوند.

اگر به RLZ نیاز دارید آن را برای FLZ های متناظر بسازید. برای هر FLZ یک زون می‌سازیم. در پیاده سازی DNS عجین شده با Active Directory باید برای هر زون DNS دامنه یک RLZ بسازیم. در Forest با چند دامنه باید شامل دامنه ریشه، تمامی دامنه‌های فرزند و همه domain tree ها باشد. برای اجرا از مراحل زیر پیروی می‌کنیم:

۱. به بخش Reverse Lookup Zone از گره DNS در Server Manager وارد می‌شویم.

۲. روی Reverse Lookup Zone کلیک راست کرده و New Zone را انتخاب می‌کنیم.

۳. اطلاعات صفحه Welcome را مرور کرده و روی Next کلیک می‌کنیم.

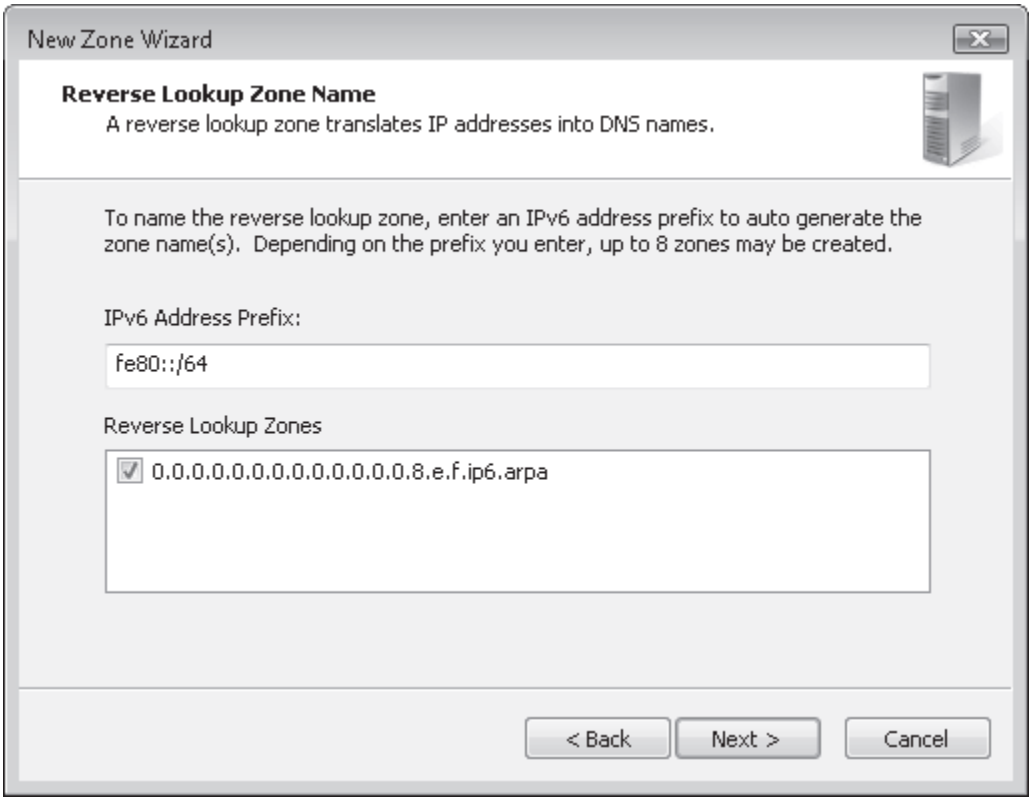
۴. Primary Zone را انتخاب کرده و کادر The Zone In Active Directory را علامت زده و روی Next کلیک می‌کنیم.

۵. به دلیل اینکه RLZ ها به یک نام دامنه وابستگی دارند گزینه To All DNS Servers In This Domain را فعال کرده و روی Next کلیک می‌کنیم.

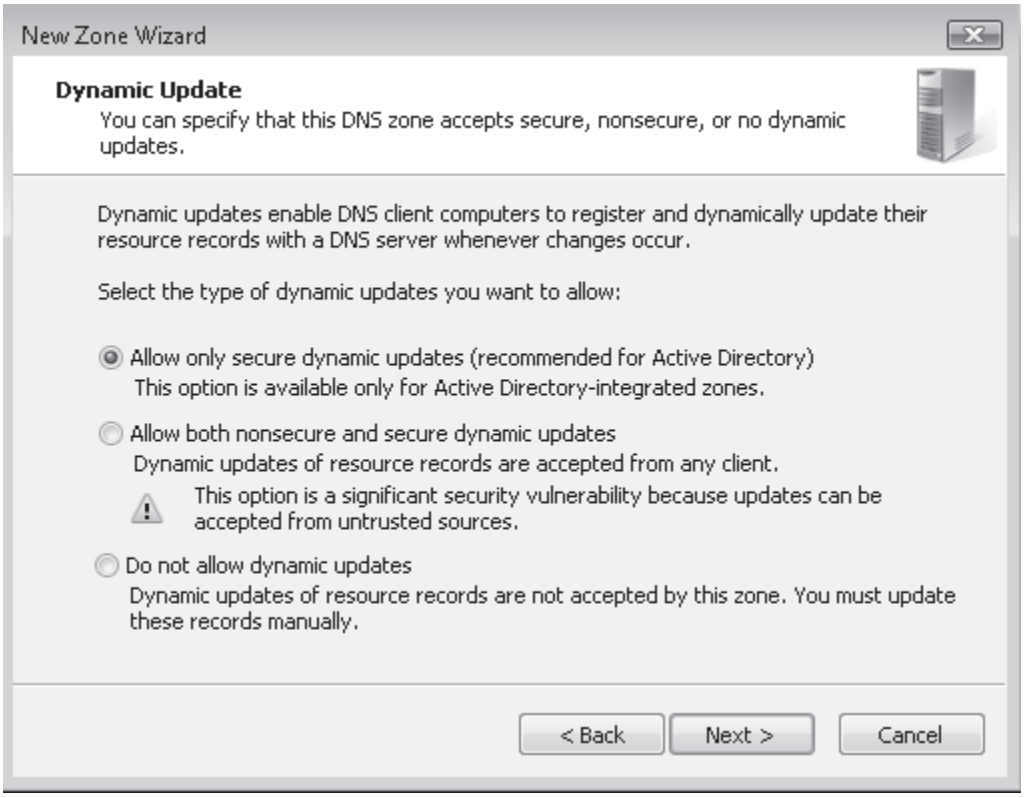
۶. در صفحه Reverse Lookup Zone Name یا Ipv4 و یا Ipv6 را انتخاب کرده و روی Next کلیک می‌کنیم.

۷. اگر از Ipv4 استفاده می‌کنیم برای زون یک ID شبکه در نظر می‌گیریم.

۸. روی Next کلیک می‌کنیم.



۹. در صفحه بعد مشخص می‌کنیم به کدام نوع از انواع به روز رسانی پویا نیاز داریم. در بیشتر موارد Allow Only Secure Dynamic Updates انتخاب می‌شود. روی Next کلیک می‌کنیم. روی Finish کلیک می‌کنیم تا زون ساخته شود.



به محض اینکه زون‌ها ساخته شدند هنگام به روز رسانی پویای بعدی روی سیستم‌های کلاینت شروع به پشتیبانی از رکوردها می‌کنند.

ساخت رکوردهای سفارشی

آخرین مرحله از پیکربندی سرور DNS ساخت رکوردهای سفارشی برای FLZ می‌باشد. رکوردهای سفارشی به صورت دستی ساخته می‌شوند و سرویس‌های متعددی را در شبکه شامل می‌شوند. برای مثال چند نمونه از این رکوردها شرح داده می‌شوند:

- یک رکورد MX برای اشاره به سرور e-mail
- یک رکورد alias نظیر intranet.domainname برای اشاره به Office SharePoint Server server farm به منظور ارتقا سطح همکاری در شبکه
- رکوردهای SRV برای سرویس‌های متعدد در شبکه. برای مثال به منظور توزیع Microsoft Office Communication Server باید رکورد SIP بسازیم.

به مرور زمان درمی‌یابیم که کدام رکورد سفارشی را نیاز داریم. در یک شبکه داخلی رکوردهای دستی باید کم باشند.

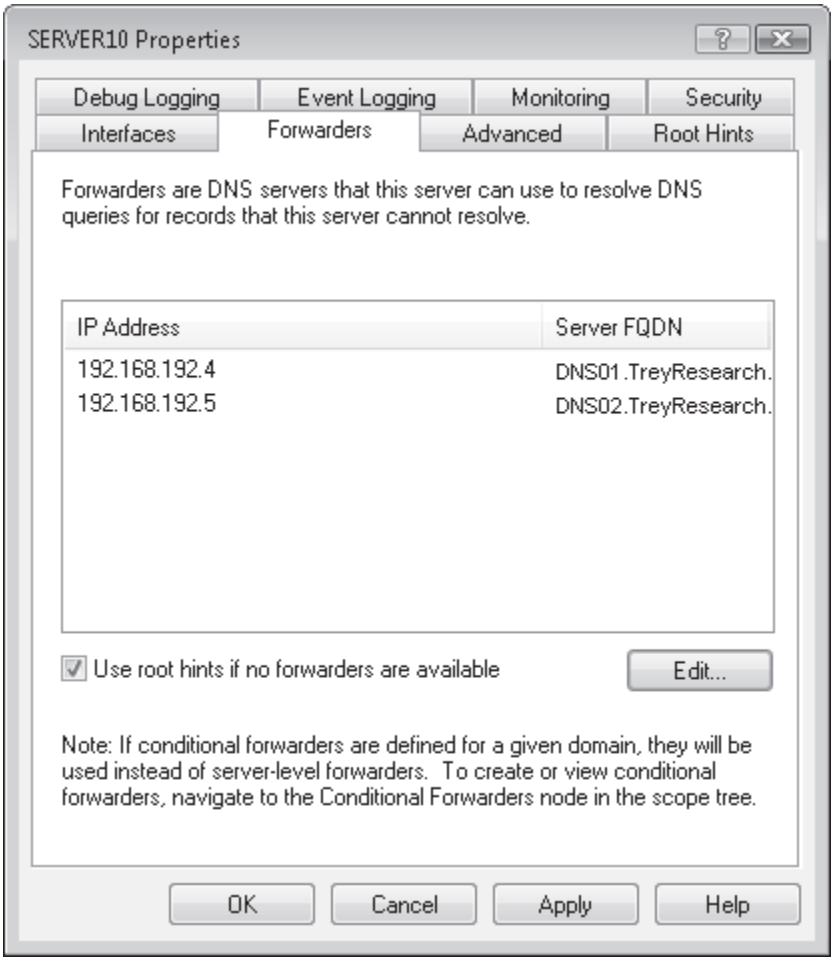
Forwarder ها در مقابل Root Hints

تحلیل نام توسط رو روش اصلی انجام می‌شود. سرورهای DNS هم حاوی root Hint می‌باشد که به آنها امکان می‌دهد سرورهای Authoritative DNS را برای نام‌های ریشه محل‌یابی کنند و هم برای ارتباط با سرورهای دیگری که کار جستجوی نام را برای آنها انجام می‌دهد به forwarder ها نیازمند هستند.

به طور پیش‌فرض سرور DNS ویندوز برای اجرای عملیات جستجوی نام به root hint ها متکی می‌باشد. یعنی اگر کاربران به جستجو در اینترنت نیاز داشته باشند سرور DNS شبکه ما با سرورهای نام ارتباط برقرار می‌کند. در سازمان‌های کوچک این کار قابل قبول است زیرا حتی اگر سرور DNS با اینترنت به طور مستقیم ارتباط داشته باشد شروع کننده ارتباط است. سیستم‌های خارجی فقط به درخواست سرور پاسخ می‌دهند و نمی‌توانند شروع کننده ارتباط باشند.

به هر جهت در شبکه‌های با نیاز امنیتی بالا ممکن است ترجیح دهیم از forwarder ها به جای root hint ها استفاده کنیم. برای مثال می‌توانیم دو دستگاه سرور منفرد DNS را در ناحیه DMZ قرار دهیم و سرورهای DNS داخلی را از طریق forwarder ها به

آنها لینک دهیم. هرگاه سرورهای داخلی نیاز به تحلیل نام اینترنتی داشته باشند به یک از سرورهای ناحیه DMZ لینک می‌شوند و درخواست تحلیل نام را ارسال می‌کند. از این طریق فقط سرورهای امن ناحیه DMZ با شبکه بیرونی ارتباط برقرار می‌کنند.
Forwarder ها به عنوان بخشی از خصوصیات سرور DNS پیکربندی می‌شوند و از زبانه Forwarders ها در کادر محاوره‌ای properties سرور DNS قابل دسترسی است. (شکل ۱۵-۹) اگر forwarder ها با اهداف امنیتی صورت می‌گیرد بهتر است در صورتی که هیچ forwarder وجود ندارد علامت کادر Use Root Hints برداشته شود. در غیر اینصورت در شرایطی که سرورهای ناحیه DMZ در دسترس نباشند سرورهای DNS داخلی به طور مستقیم با اینترنت ارتباط برقرار می‌کنند.



شکل ۱۵- ۹ پیکربندی forwarder ها در DNS

یکی دیگر از امکانات پیکربندی DNS نوعی forwarder به نام forwarder شرطی (conditional forwarder) می‌باشد که برای ارسال درخواست‌های DN در صورتی محقق شدن شرطی معین استفاده می‌شود. برای مثال اگر بخواهیم هنگام درخواست نام‌های خاصی دو فضای نام را به هم لینک دهیم از این نوع forwarder استفاده می‌کنیم.
مثلا فرض می‌کنیم دو forest در شبکه داریم. اولی forest اصلی می‌باشد که حاوی همه حساب‌های کاربران است. دوم یک forest خاص است که برای تست عجین شدن AD DS یک برنامه غیرمایکروسافتی با AD DS forest schema قبل از توزیع در forest اصلی به کار می‌رود. به دلیل تغییرات schema ما نمی‌خواهیم بین forest ها trust برقرار کنیم. بنابراین در همه forest ها از forwarder های شرطی استفاده می‌کنیم به طوری که کاربران در دامنه اصلی عمدتا برنامه‌نویسان و متخصصین IT بتوانند از دامنه اصلی به دامنه دیگر لینک برقرار کنند.
Forwarder های شرطی در سرور DNS دارای container های خود می‌باشند.

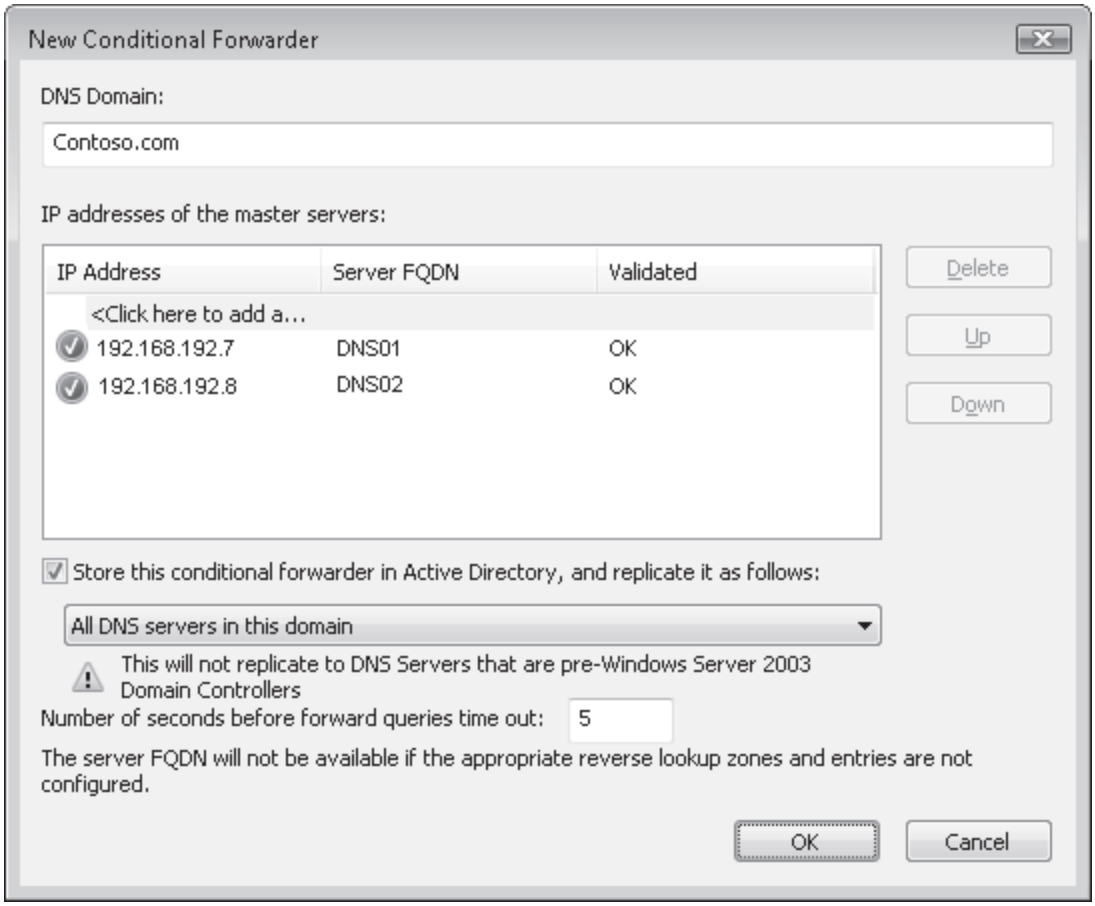
۱. برای ساخت یک forwarder شرطی روی گره Conditional Forwarders کلیک راست کرده و New Conditional Forwarder را انتخاب می‌کنیم.

۲. نام دامنه DNS را که می‌خواهیم به آن فوروارد کنیم تایپ می‌کنیم.

۳. روی <Click Here To Add An IP Address Or DNS Name> کلیک کرده و آدرس IP سرور را تایپ می‌کنیم.

۴. حداقل دو سرور را به لیست اضافه می‌کنیم.

۵. بهتر است conditional forwarder در Active Directory ذخیره شود و مشخص شود کدام حوزه تکثیر به forwarder اعمال شود.



در مثال قبلی می‌توانستیم داده را فقط روی دامنه اصلی تکثیر کنیم چون نیازی به تکثیر آن به کل forest نداریم. در موارد دیگر ممکن است نیاز باشد روی کل forest تکثیر شود.

توجه داشته باشید که وقتی conditional forwarder ساخته می‌شود یک container جدید برای دامنه‌ای که درخواست به آن ارسال می‌شود در زیر گره Conditional Forwarders قرار دارد ساخته می‌شود. از این به بعد هر زمان کاربران درخواست تحلیل نام داشته باشند که حاوی نام دامنه مذکور باشد سرور DNS به طور خودکار آنرا به سرورهای DNS که در لیست مشخص شده است ارسال می‌کند.

مدیریت نام تک بخشی (Single Lable)

اگر بخواهیم نام‌های تک بخشی را مدیریت کنیم نیاز به ساخت دستی GNZ داریم . همه forest ها به یک GNZ منفرد نیاز دارند. پروسه ساخت GNZ ۵ مرحله دارد ولی روی هر سرور DNS در forest یک عملیات اجرا می‌کند. اگر سرور DNS با AD DS عجین شده باشد و همه DC ها دارای سرویس DNS نیز باشند باید این عملیات را روی همه DC ها نیز اجرا کنیم. بنابراین نیاز به اعتبار مدیریتی برای انجام عملیات داریم.

- GlobalNames FLZ را می‌سازیم.
- حوزه تکثیر آنرا به همه سرورهای DNS در forest تعمیم می‌دهیم.

- به روز رسانی پویا را برای این زون فعال نمی‌کنیم.
- پشتیبانی GNZ را روی همه سرورهای DNS در forest فعال می‌کنیم.
- نام‌های تک بخشی را به زون DNS اضافه می‌کنیم.

پیکربندی از طریق خط فرمان اجرا می‌شود چون هیچ رابط گرافیکی برای دسترسی به این قابلیت وجود ندارد. بهرحال می‌توان از طریق Server Manager نیز GNZ را ساخت ولی فعال کردن پشتیبانی GNZ در سرور DNS نیاز به دستکاری رجیستری ویندوز دارد.
این تغییر با دستور Dnscmd.exe انجام شده و از قالب زیر استفاده می‌کند:
Dnscmd /config /enableglobalnamessupport 1
این دستور باید روی همه سرورهای DNS در forest اجرا شود. اگر نیاز به پشتیبانی از نام‌های تک بخشی باشد و نخواهیم از WINS استفاده کنیم می‌توانیم این دستور را به عنوان بخشی ازمراحل نصب و پیکربندی سرور DNS استاندارد استفاده کنیم. وقتی دستور اجرا شد باید سرویس DNS راه اندازی مجدد شود.
پس از فعال شدن پشتیبانی از GNZ می‌توانیم کار افزودن رکوردها را شروع کنیم. نام‌های GNZ مستعار هستند زیرا همه اشیاء در شبکه قبلا در DNS دارای نام هستند. ما یک نام مستعار می‌سازیم و آنرا به نام FQDN شیء متناظر اشاره می‌دهیم. نام‌های مستعار GNZ مانند نام‌های WINS نمی‌توانند بیش از ۱۵ کاراکتر داشته باشند. اگر بخواهیم نام‌ها را از طریق فایل دستور اضافه کنیم قالب دستور زیر را برای هر نام رعایت می‌کنیم:
Dnscmd dnsservername /recordadd globalnames singlelabelname cname Correspondingdnsname
به جای dnsservername نام سرور DNS را که نام را به آن اضافه می‌کنیم ، به جای singlelabelname نام ۱۵ کاراکتری و به جای correspondingdnsname نام FQDN شیء را وارد می‌کنیم.

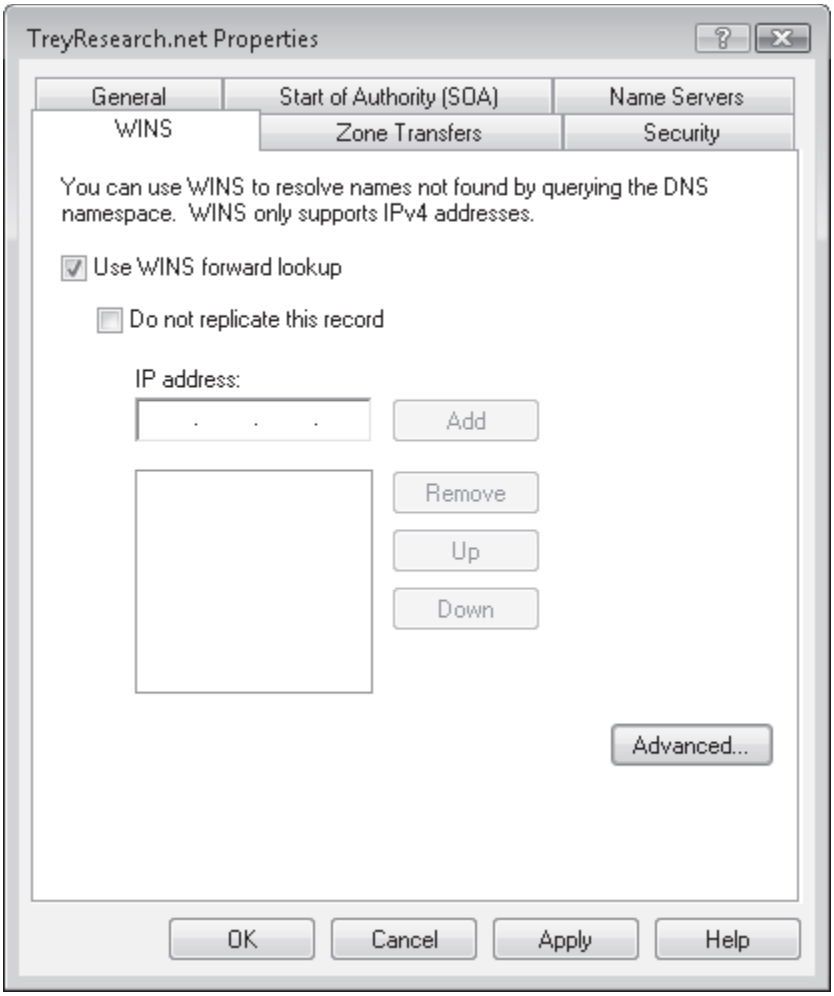
DNS و WINS

وقتی در شبکه نیاز به تعداد زیادی نام تک بخشی داریم و به علت حجم بالا از طریق GNZ این نیاز قابل رفع نیست راه حل نصب سرویس WINS روی حداقل دو سرور در شبکه است. این سرویس به طور خودکار برای هر شیء شبکه، اسمی تولید کرده و مدیریت می‌کند. به خاطر داشته باشید که سرویس WINS یک ویژگی ویندوز سرور 2008 است نه نقش و این یک فناوری منسوخ است که از زمان ظهور در ویندوز سرور 2003 هیچ تغییری نکرده است.
هنگام توزیع سرویس WINS به خاطر داشته باشید :

- WINS در پنجره Server Manager دیده نمی‌شود. برای مدیریت این سرویس باید از کنسول WINS در Administrative Tools استفاده کنیم.
- این سرویس فقط از آدرس‌های Ipv4 پشتیبانی می‌کند و برای پشتیبانی از Ipv6 قابل ارتقا نیست.
- برای فراهم کردن تحمل خرابی (fault tolerance) در رابطه با نام‌های تک بخشی در شبکه نیاز به حداقل دو سرور WINS می‌باشد. این دو سرور باید با هدف یکسان سازی ارسال/ دریافت (push/pull synchronization) پیکربندی شود تا هر دو بانک اطلاعاتی نام همیشه یکسان باشند.
- مشخصات سرویس WINS باید در تنظیمات DHCP وارد گردد. دو تنظیم مورد نیاز است. اولی سرورهای نام را لیست می‌کند و دومی مشخص می‌کند هر کلاینت با کدام نوع گره کار کند.
  - 044 WINS/NBNS Servers مشخص می‌کند کدام سرورها میزبان سرویس WINS هستند.

- 046 WINS/NBT Node مشخص می‌کند گره‌ها چطور با WINS تعامل داشته باشند. این مسئله باعث کاهش ترافیک broadcast در شبکه می‌گردد.

- با تغییر properties مربوط به یک FLZ امکان عجین شدن WINS و DNS وجود دارد. در صفحه properties زبانه‌ای با نام WINS موجود است که در صورت وجود سرور WINS در شبکه قابل استفاده است. (شکل ۱۶- ۹) این ویژگی در شبکه‌هایی مفید است که در آن کلاینت‌های زیادی به سرویس WINS وابسته هستند و ممکن است برخی نام‌ها در DNS ثبت نشوند. به هر حال همه سیستم عامل‌های ویندوزی از ویندوز 2000 به بعد می‌توانند در زیرساخت پویای DNS شرکت کنند. شبکه‌های دارای ویندوزهای قدیمی‌تر از ویندوز 2000 بسیار نادر هستند.



شکل ۱۶- ۹ لینک کردن DNS با WINS جهت تحلیل نام FQDN و نام‌های تک بخشی

ملاحظات در سرویس‌های DNS و DHCP

وقتی با سرویس DNS پویا کار می‌کنیم و آنرا با AD DS عجین می‌کنیم باید رویکرد سنتی مدیران شبکه را در مورد پیکربندی تنظیمات DHCP تغییر دهیم.

به طور سنتی مدیران شبکه دو سرور DNS مرکزی را در server options از تنظیمات DHCP در نظر می‌گرفتند. این کار باعث می‌شد همه کلاینت‌ها برای تحلیل نام داخلی و خارجی دو آدرس DNS داشته باشند ولی به دلیل اینکه سرورها در مرکز قرار می‌گرفتند کلاینتی که از راه دور متصل می‌شد می‌بایست از طریق لینک WAN درخواست DNS ارسال می‌کرد.

به هر حال با عجین شدن DNS خصوصا داده DNS با انباره دایرکتوری، هر جا که DC موجود است داده DNS نیز وجود دارد و هر جا که کلاینت‌ها حضور دارند DC ها به منظور ارائه سرویس تایید هویت در شبکه توزیع می‌شوند. در بعضی سازمان‌ها در صورت وجود بیش از ۲۰ کلاینت DC پیکربندی می‌شود. با ظهور مجازی سازی سرور از طریق Hyper-V، DC ها بیش از پیش در شبکه‌ها رایج

شده‌اند. این بدین معنی است که داده DNS حتی داده DNS فقط خواندنی در همه سایت‌ها یا دفاتر فرعی استفاده می‌شوند و کلاینت‌ها می‌توانند برای اجرای جستجوی FQDN در سایت خود از این سرورها استفاده کنند.
بهرحال برای اجرای جستجو به صورت محلی کلاینت‌ها باید از وجود سرور DNS محلی مطلع باشند. سناریوهای زیر را تصور کنید:

- کلاینتی در سایت راه دور از آدرس IP پویا از طریق سرویس DHCP بهره می‌برد.
- دو DC در سایت راه دور موجود است.
- DNS با دایرکتوری عجین شده و با پارتیشن دامنه تکثیر می‌شود.
- DHCP مقادیر دو سرور DNS را در سایت مرکزی توزیع می‌کند
- وقتی کلاینت‌ها هر روز صبح راه اندازی می‌شوند به دنبال نزدیک‌ترین DNS می‌گردند تا به شبکه وارد شوند.
- از یکی از دو DC مرکزی برای درخواست تحلیل نام جستجوی DNS روی لینک WAN انجام می‌شود.
- سرورهای DNS مرکزی سایت کلاینت‌ها جستجو کرده و متوجه می‌شود که دو DC محلی موجود است.
- سرور DNS محل نزدیک‌ترین DC به کلاینت را بر روی لینک WAN برمی‌گرداند.
- کلاینت با DC محلی خود برای ورود ارتباط برقرار می‌کند.

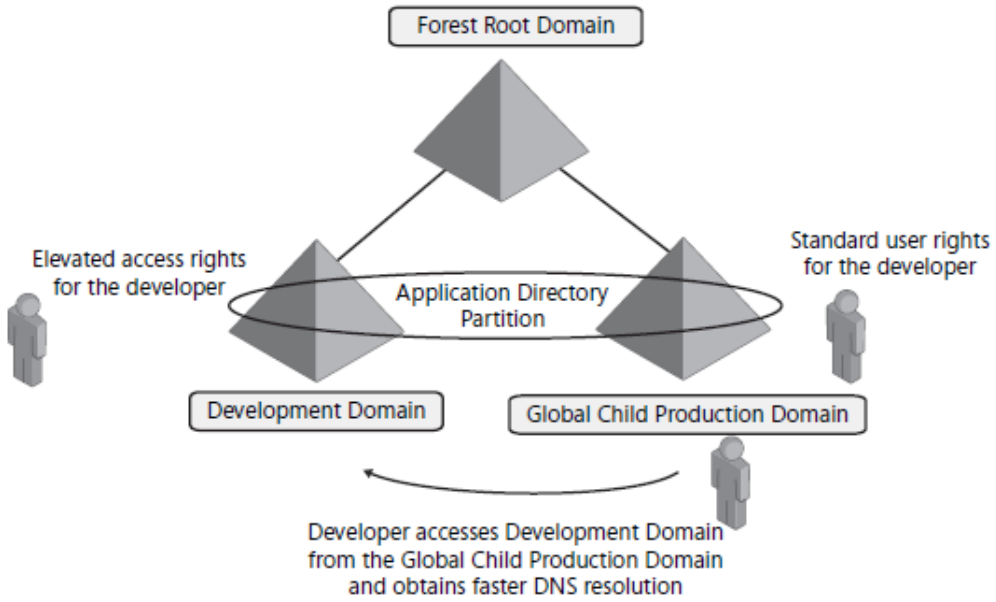
در این سناریو اگر ارتباط WAN موجود نباشد حتی اگر داده DNS به صورت محلی در دو DC ذخیره شده باشد کلاینت قادر به ورود نیست.
به همین دلیل گزینه‌های DHCP باید به صورت زیر تغییر یابد:

- حوزه سرور باید دارای حداقل دو آدرس برای سرورهای DNS محلی باشد. اگر DC محلی از دسترس خارج شد کلاینت‌ها ولو از طریق لینک WAN بتوانند به شبکه وارد شوند.
- هر حوزه آدرس اختصاصی باید دارای گزینه‌های سرورهای تحلیل نام بوده و این رکوردها باید به DC های محلی سایت منسوب به حوزه اشاره کند. یعنی به همه حوزه‌های منحصر در DHCP مقدار 006 DNS Servers اضافه شود.
- همه DC ها باید نقش سرور DNS را نیز داشته باشند. اگر یک زون DNS در انباره دایرکتوری AD DS ذخیره شود درست پس از نصب نقش سروری DNS روی DC برای سرویس DNS قابل دسترس خواهد بود. تنها چیزی که برای پیکربندی باقی می‌ماند سرور global DNS می‌باشد.

کار با پارتیشن‌های دایرکتوری برنامه

در پاره‌ای شرایط ممکن است بخواهیم پارتیشن‌های دایرکتوری برنامه سفارشی بسازیم تا از تکثیر داده DNS پشتیبانی کنیم. به خاطر داشته باشید که این پارتیشن‌ها حوزه تکثیر داده خود را کنترل می‌کنند. سرور DNS وقتی با AD DS در یک forest نصب می‌شود دو پارتیشن دایرکتوری برنامه می‌سازد. یکی برای داده forest و دیگری برای داده دامنه در هر دامنه ولی در برخی شرایط این دو حوزه ممکن است مناسب نباشند مخصوصا در forest های پیچیده.
سناریوی زیر را در نظر بگیرید. Forest ما دارای سه دامنه است: ریشه forest ، یک دامنه اصلی فرزند global و یک دامنه development. دامنه development ایجاد می‌شود برای اینکه برنامه‌نویسان سازمان نیازهای دسترسی مشخصی دارند و ما نمی‌خواهیم به آنها اجازه دهیم این دسترسی را روی دامنه اصلی به آنها بدهیم. همه کاربران دامنه اصلی به جز مدیران سیستم

دسترسی استاندارد دارند. در دامنه development می‌توانیم به برنامه‌نویسان شرکت دسترسی‌های بالاتری هم در نظر بگیریم مانند حق ساخت، تغییر یا حذف شیء چرا که این دامنه روی عملیات اصلی شبکه تاثیری ندارد.
به علاوه ما برای هر برنامه‌نویس یک حساب منفرد می‌سازیم. این حساب در دامنه اصلی فرزند global قرار دارد و دسترسی کاربری استاندارد دارد ولی از طریق transitive trust به ارث رسیده در هر forest برنامه‌نویسان می‌توانند از حساب‌شان در دامنه اصلی برای دسترسی به اشیاء دامنه development استفاده کنند در جایی که حساب‌های دامنه اصلی حقوق دسترسی بالاتری دارند.
به طور پیش فرض تحلیل نام بین دو دامنه فرزند از دامنه ریشه forest می‌گذرد. برنامه‌نویسان به طور روزمره به این دامنه دسترسی دارند بنابراین برای تحلیل نام سریع تر یک پارتیشن دایرکتوری برنامه می‌سازیم که رکوردهای DNS را بین دامنه‌های اصلی و development به اشتراک گذشته شود. به این دلیل که داده در پارتیشن در دسترس است سرورهای DNS اصلی برای تحلیل نام‌های دامنه development نیازی به عبور از دامنه ریشه forest ندارند. (شکل ۱۷- ۹)



شکل ۱۷- ۹ اتکا به پارتیشن‌های دایرکتوری برنامه برای به اشتراک گذاری داده DNS بین دو دامنه فرزند

ساخت و نسبت دادن پارتیشن‌های دایرکتوری برنامه

پارتیشن‌های دایرکتوری برنامه سفارشی از طریق خط فرمان با دستور Dnscmd.exe ساخته می‌شوند. رابط کاربری برای ساخت این پارتیشن‌ها وجود ندارد. بهرحال پس از ساخت می‌توانند از طریق رابط گرافیکی نسبت داده شوند. همه مراحل را می‌توان از طریق خط فرمان انجام داد. این سه کار باید انجام شود:

- پارتیشن ساخته شود
- سرورهای DNS در پارتیشن باید لیست شوند
- به زون‌هایی نسبت داده شوند که می‌خواهیم حوزه تکثیرشان به پارتیشن تازه ساخته شده تغییر یابد.

برای ساخت یک پارتیشن دایرکتوری برنامه باید عضو گروه Enterprise Admins باشیم زیرا باید به forest دسترسی کامل داشته باشیم.

۱. با حساب کاربری عضو گروه Enterprise Admins به سرور DNS وارد می‌شویم.
۲. خط فرمان elevated را اجرا می‌کنیم.
۳. دستور زیر را تایپ می‌کنیم:

Dnscmd dnsservername /createdirectorypartition partitionfqdn

به جای dnsservername نام fqdn سرور DNS یا آدرس IP آنرا می‌نویسیم و به جای partitionfqdn ، fqdn مربوط به پارتیشن مورد نظر برای ساخت را تایپ می‌کنیم.

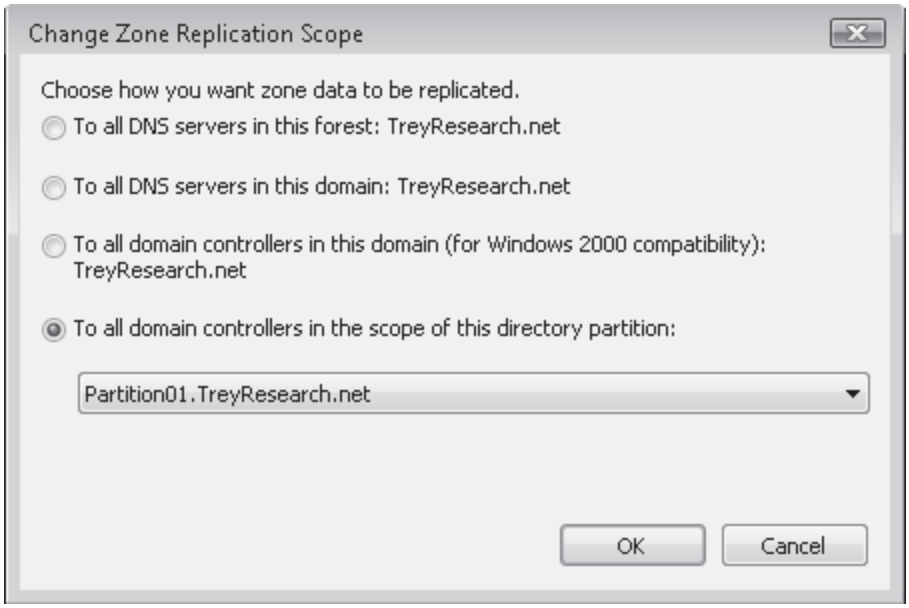
۴. سرور را در پارتیشن لیست می‌کنیم. دوباره از دستور Dnscmd.exe استفاده می‌کنیم.

Dnscmd dnsservername /enlistdirectorypartition partitionfqdn

۵. به گره DNS در Server Manager برمی‌گردیم و روی نام زون که می‌خواهیم تغییر دهیم کلیک راست کرده و properties را انتخاب می‌کنیم.

۶. در زبانه General روی دکمه Change کلیک می‌کنیم تا حوزه تکثیر را عوض کنیم.

۷. در کادر محاوره‌ای Change Zone Replication Scope گزینه To All Domain Controllers In The Scope Of This Directory Partition را انتخاب کرده و از لیست بازشو پارتیشن جدید را انتخاب می‌کنیم و دوبار روی OK کلیک می‌کنیم.



وقتی با پارتیشن‌های دایرکتوری برنامه کار می‌کنیم باید مراقب باشیم چون بسیاری از دستورات دستی وارد می‌شوند. اگر به اشتباه وارد شوند ممکن است حوزه تکثیر را خراب کنن و بنابراین تحلیل نام مختل شود.

مدیریت سرور DNS

در جدول زیر با ابزارهای مختلفی برای اجرای عملیات پشتیبانی و مدیریت DNS آشنا می‌شویم.

جدول ۴- ۹ ابزارهای رایج مدیریت DNS

ابزار	وظیفه	محل
DNS Manager	پیکربندی اولیه سرور جدید را انجام می‌دهد به یک سرور DNS محلی متصل شده و آنرا مدیریت می‌کند زون‌های جستجوی مستقیم و معکوس ایجاد و پاک می‌کند رکوردهای منابع را در زون‌ها ساخته حذف و به روز رسانی می‌کند طریقه ذخیره سازی و تکثیر بین سرورها را تغییر می‌دهد طریقه پردازش پرس و جوها و کارکردن با تغییرات پویا را توسط سرور تغییر می‌دهد.	Administrative Tools or Server Manager

	امنیت زون‌ها یا رکوردهای منابع خاصی را تغییر می‌دهد کار پشتیبانی را هم انجام می‌دهد محتویات حافظه نهانی سرور را مانیتور می‌کند گزینه‌های پیشرفته سرور را تنظیم می‌کند مکانیزم پاک کردن رکوردهای کهنه را پیکربندی و اجرا می‌کند	
Dnscmd	همه جنبه‌های سرورهای DNS را مدیریت می‌کند. این قدرتمندترین ابزار خط فرمان برای مدیریت DNS است. سوئیچ‌های مهم عبارتند از: • /info برای دریافت اطلاعات سرور • /config برای تغییر پارامترهای پیکربندی سرور • /statistics برای دریافت آمار عملکردی یک سرور • /clearcache برای پاک کردن حافظه نهانی • /startscavenging برای شروع یک عملیات پاک‌سازی • /directorypartitioninfo برای اطلاعات پارتیشن • /exportsettings برای ساخت یک فایل پشتیبان از تنظیمات سرور	خط فرمان
Dnslint	مشکلات رایج تحلیل نام DNS را تشخیص می‌دهد. سوئیچ‌های مهم عبارتند از: • /d برای درخواست تست تحلیل نام دامنه • /ql برای بررسی تست پرس و جوی DNS از یک لیست • /ad برای بررسی رکوردهای با ارتباط ویژه با Active Directory	خط فرمان
Enent Viewer	دو گزینه برای مانیتور کردن سرور DNS وجود دارد: • ثبت وقایع سرور DNS در DNS Server log به صورت پیش فرض • گزینه‌های debug برای ثبت وقایع به یک فایل متنی.	Server Manager
Ipconfig	نمایش و تغییر جزئیات پیکربندی IP. سوئیچ‌های مهم عبارتند از : • /all برای نمایش همه تنظیمات پیکربندی شبکه روی یک سیستم • /renew برای درخواست یک آدرس IP نسخه ۴ جدید از DHCP • /renew6 برای درخواست یک آدرس IP نسخه ۶ از DHCP • /release برای آزاد کردن یک آدرس Ipv4 • /release6 برای آزاد کردن یک آدرس Ipv6	خط فرمان

	• /flushdns برای پاک کردن حافظه نهانی کلاینت DNS • /registerdns برای ثبت پویای یک سیستم در DNS	
Nslookup	برای تست درخواست تحلیل نام فضای نام دامنه DNS استفاده میشود. برای خروج از دستور عبارت Exit را تایپ می‌کنیم.	خط فرمان
System Monitor	از روند کارکرد سرور نمودار تهیه می‌کند.	Server Manager, Diagnostics, Reliability, and Performance

تمرینات تکمیل پیکربندی سرور DNS

تمرین ۱ مدیریت نام‌های تک بخشی

در این تمرین قرار است یک GNZ برای forest ، treyresearch.net بسازیم. این عملیات دستی بوده و نیاز به اعتبار administrator دامنه دارد چراکه سرورهای DNS روی DC نصب شده‌اند. در این تمرین به SERVER10، SERVER20 و SERVER30 نیاز داریم.

۱. با اعتبار treyresearch\administrator به SERVER10 وارد می‌شویم.

۲. در Server Manager گره Forward Lookup Zones را در نقش DNS انتخاب می‌کنیم.

۳. روی Forward Lookup Zone کلیک راست کرده و از منوی کلیک راست New Zone را انتخاب می‌کنیم.

۴. اطلاعات صفحه welcome را مرور کرده و Next را می‌زنیم.

۵. Primary Zone را انتخاب کرده و کادر Store The Zone In Active Directory را علامت می‌زنیم. سپس روی دکمه Next کلیک می‌کنیم.

۶. در صفحه بعد گزینه To All DNS Servers In This Forest:TreyResearch.net را انتخاب کرده و Next می‌زنیم.

۷. در صفحه Zone Name عبارت GlobalNames را تایپ کرده و Next می‌زنیم.

۸. در صفحه Dynamic Update گزینه Do Not Allow Dynamic Updates را انتخاب کرده و دکمه Next را می‌زنیم. ما اجازه به روز آوری پویای این زون را نمی‌دهیم به دلیل اینکه همه نام‌های تک بخشی به صورت دستی در DNS ساخته می‌شود.

۹. روی Finish کلیک می‌کنیم تا زون ساخته شود.

۱۰. از منوی استارت روی Command Prompt کلیک راست کرده و Run As Administrator را انتخاب می‌کنیم.

۱۱. دستور زیر را تایپ می‌کنیم:

```
Dnscmd /config /enableglobalnamessupport 1
```

۱۲. پنجره خط فرمان را بسته و به پنجره Server Manager برمی‌گردیم. روی SERVER10 زیر گره DNS کلیک راست کرده و All Tasks و بعد Restart را انتخاب می‌کنیم.

۱۳. مراحل ۱۰ تا ۱۲ را روی سرورهای SERVER20 و SERVER30 تکرار می‌کنیم.

۱۴. به سرور SERVER10 برمی‌گردیم تا نام‌های تک بخشی را اضافه کنیم.

تمرین ۲ ساخت نام‌های تک بخشی

در این تمرین نام‌های تک بخشی در GNZ روی سرور SERVER10 خواهیم ساخت. این عملیات دستی است و نیاز به اعتبار مدیریتی دارد چون سرورهای DNS روی DC نصب شده‌اند. ما باید برای هر سه سرور رکورد نام تک بخشی بسازیم.

۱. با اعتبار treyresearch\administrator به SERVER10 وارد می‌شویم.

۲. در Server Manager گره GlobalNames GLZ را در نقش DNS انتخاب می‌کنیم.

۳. روی GlobalNames کلیک راست کرده و از منوی کلیک راست New Alias (CNAME) را انتخاب می‌کنیم.

۴. در فیلد Alias Name تایپ می‌کنیم SERVER10 و در فیلد Fully Qualified Domain Name (FQDN) for Target Host تایپ می‌کنیم SERVER10.treyresearch.net .

۵. گزینه Allow Any Authenticated User To Update All DNS Records With The Same Name را انتخاب نمی‌کنیم.

۶. روی OK کلیک می‌کنیم تا نام تک بخشی ساخته شود.

۷. از منوی استارت روی Command Prompt کلیک راست کرده و Run As Administrator را انتخاب می‌کنیم.

۸. دستور زیر را تایپ می‌کنیم:

```
Dnscmd server10.treyresearch.net /recordadd globalnames server20 cname
server20.northwindtraders.com
Dnscmd server10.treyresearch.net /recordadd globalnames server30 cname
server30.intranet.treyresearch.net
```

۹. پنجره خط فرمان را بسته و به GNZ در پنجره Server Manager برمی‌گردیم تا رکوردهای جدید را ببینیم. اگر تعداد نام‌ها خیلی زیاد باشد از اسکریپت برای افزودن آنها استفاده می‌کنیم.

تمرین ۳ تغییر Global Query Block List

در این تمرین قرار است یک global query block list را روی سرور SERVER10 ویرایش کنیم. این عملیات دستی است و نیاز به اعتبار مدیریتی دارد چون سرورهای DNS روی DC نصب شده‌اند. ما باید یک نام خاص DNS مانند manufacturing به لیست بدهیم تا تحلیل نام را برای همه اشیایی که از این نام استفاده می‌کنند بلوکه کنیم

۱. با اعتبار treyresearch\administrator به SERVER10 وارد می‌شویم.

۲. از پنجره خط فرمان برای ویرایش لیست بلوکه استفاده می‌کنیم. از منوی استارت روی Command Prompt کلیک راست کرده و Run As Administrator را انتخاب می‌کنیم.

۳. دستورات زیر را تایپ می‌کنیم:

```
Dnscmd /config /globalqueryblocklist wpad isatap manufacturing
```

۴. پنجره را می‌بندیم. حالا لیست آماده می‌باشد.

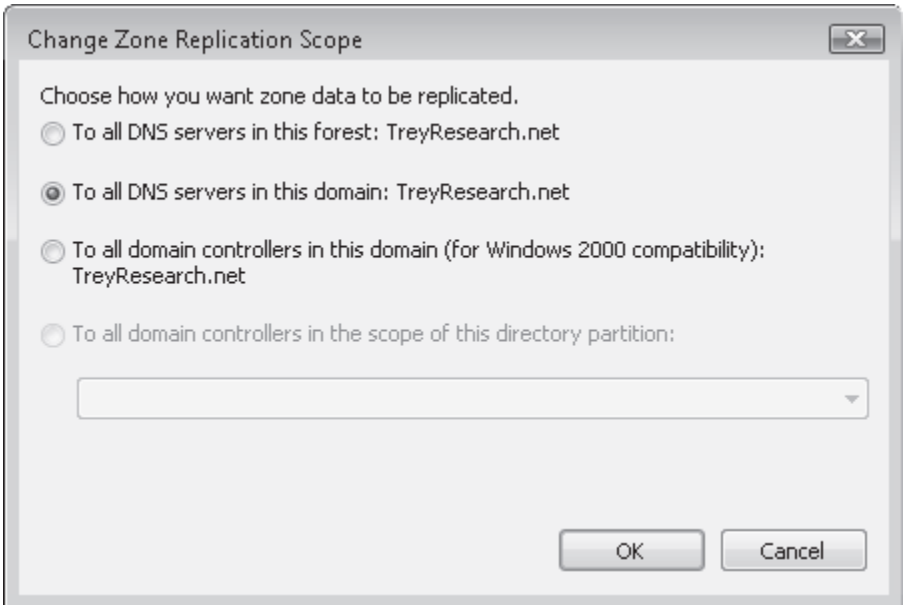
خلاصه درس

- پس از نصب سرور DNS پیکربندی آن انجام می‌شود. پیکربندی تنظیمات DNS حاوی پارامترهای امنیتی، پیکربندی حوزه و ساخت RLZ ممکن است.
- همه forward lookup zone ها و stub zone ها دارای یک رکورد SOA هستند.
- به طور پیش فرض سرورهای DNS برای تحلیل نام از root hint ها استفاده می‌کنند. همچنین امکان استفاده از forwarder ها وجود دارد که سرورهای DNS را مستقیما به سرورهای DNS دیگر تحت شرایطی متصل می‌کند.

سئوالات پایان درس

۱. فرض کنید مدیر سرویس DNSداخلی FLZشبکه contoso.com هستیم. از ما درخواست می‌شود پیکربندی این زون را انجام دهیم. چه باید بکنیم؟ (امکان انتخاب همه گزینه‌ها وجود دارد.)
   a. Scavenging را برای زون پیکربندی می‌کنیم.
   b. حوزه تکثیر را برای زون اعتبار سنجی می‌کنیم.
   c. رکوردهای سفارشی برای زون می‌سازیم.
   d. رکورد متنی (TXT) برای زون می‌سازیم.
   e. آدرس e-mail به این زون اختصاص می‌دهیم.
   f. رکوردهای بلااستفاده را از زون پاک می‌کنیم.
   g. برای زون RLZ می‌سازیم.

۲. فرض کنید مدیری شبکه دامنه treyresrarch.net هستیم. سازمان تصمیم می‌گیرد برای بخش توسعه نرم‌افزار یک دامنه دیگر اختصاص دهد. کاربران دامنه اصلی غیر از کارکنان یک بخش باید دارای دسترسی استاندارد باشند. این یعنی کارشناسان نرم‌افزار باید دسترسی به جز دسترسی آنان به دامنه اصلی داشته باشند. ولی به دلیل اینکه کارشناسان نرم‌افزار از دامنه جدید به طور مرتب استفاده می‌کنند باید پارتیشن دایرکتوری برنامه جدیدی ساخته شود. همه FLZ ها زون‌های عجین شده با Active Directory می‌باشند. ما باید این پارتیشن جدید را به FLZ نسبت دهیم. ولی وقتی می‌خواهیم این کار را انجام دهیم در دسترس نمی‌باشد. مشکل چیست؟ (امکان انتخاب همه گزینه‌ها وجود دارد.)



a. باید با اعتبار مدیر دامنه وارد شویم.
b. باید سروری را که درپارتیشن از آن استفاده می‌کنیم ثبت نام کنیم.
c. باید با کاربر enterprise administrator وارد شویم.
d. باید از خط فرمان برای تخصیص زون به پارتیشن استفاده کنیم.
e. ما نمی‌توانیم حوزه تکثیر یک FLZ را بعد از ساخت تغییر دهیم.

فصل ۱۰

Domain Controller ها

DC ها سرویس دایرکتوری را میزبانی می‌کنند و سرویس‌هایی را اجرا می‌کنند که مدیریت identity and access را در شبکه ویندوزی پشتیبانی می‌کند. در این کتاب مدیریت اجزاء یک زیرساخت AD DS را یاد می‌گیریم. این اجزاء عبارتند از : کاربران ، گروهها ، کامپیوترها و Group Policy . همه این اجزاء در بانک اطلاعاتی دایرکتوری و روی SYSVOL در DC ذخیره می‌شوند.

اهداف امتحانی در این فصل:

- پیکربندی یک forest و دامنه
- پیکربندی تکثیر Active Directory

- پیکربندی operations masters

دروس این فصل:

- درس ۱: نصب DC
- درس ۲: پیکربندی Operations Masters
- درس ۳: پیکربندی تکثیر DFS مربوط به SYSVOL

قبل از شروع

برای انجام تمرینات این فصل باید یک DC با نام SERVER01 در یک دامنه با نام contoso.com ساخته و یک member server با نصب کامل آماده کرده که به دامنه SERVER02 ، join شده باشد. برای اجرای موارد فوق از مطالب فصل ۱ می‌توانیم استفاده کنیم.

درس ۱: نصب Domain Controller

در فصل ۱ از ویزارد Add Roles Wizard در Server Manager برای نصب AD DS استفاده کردیم. سپس از ویزارد Active Directory Domain Services Installation Wizard برای ساخت اولین DC در contoso.com forest بهره بردیم. به دلیل اینکه DC برای تایید هویت در شبکه خیلی حیاتی است اکیدا توصیه می‌شود حداقل دو دستگاه سرور DC در هر دامنه داشته باشیم تا ظرفیت تحمل خرابی به میزان ۱ را فراهم کنیم. ممکن است نیاز باشد تا DC ها را به سایت های راه دور اضافه کنیم یا دامنه و tree جدید بسازیم. در این درس روش‌های نصب DC از طریق رابط گرافیکی خط فرمان و روش غیرحضوری بررسی می‌شود.
بعد از این درس یاد می‌گیریم:

- با استفاده از رابط گرافیکی، پارامترهای دستور Dcpromo.exe یا فایل پاسخ DC را نصب کنیم.
- DC ویندوز سرور 2008 را به دامنه یا forest ویندوز سرور 2003 و 2000 اضافه کنیم.
- دامنه یا tree جدید بسازیم.
- نصب سرور RODC را به صورت staged انجام دهیم.
- DC را از طریق مدیای نصب انجام دهیم تا بار شبکه کاهش یابد.
- DC را حذف کنیم.

زمان تقریبی : ۶۰ دقیقه

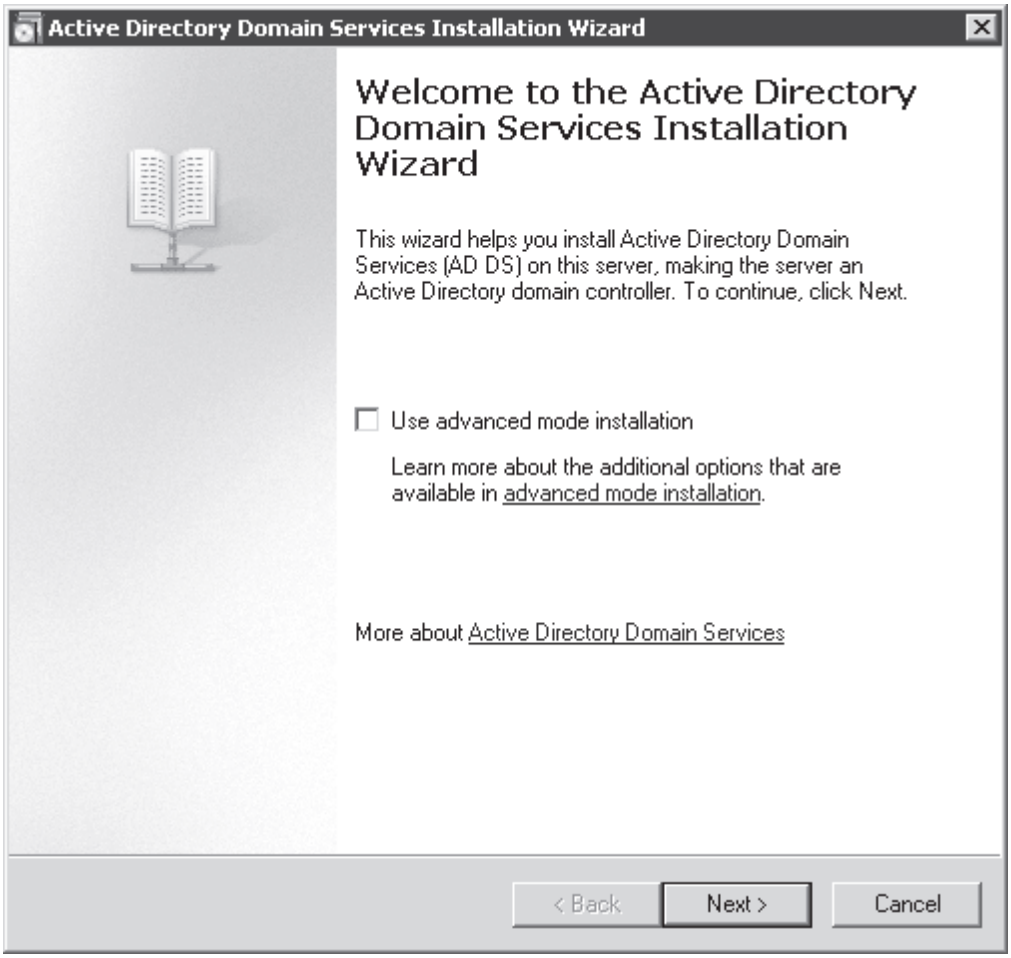
نصب DC توسط رابط ویندوزی

برای نصب یک DC توسط رابط ویندوزی دو روش اصلی وجود دارد. اول باید نقش AD DS را نصب کنیم که در فصل ۱ یاد گرفتیم. بعد با یکی از روش‌های زیر با اجرای ویزارد Active Directory Domain Services Installation Wizard کار پیکربندی AD DS را انجام می‌دهیم:

- از منوی استارت در کادر Start Search تایپ می‌کنیم dcpromo و OK می‌کنیم.
- وقتی ویزارد تمام شد روی لینک ظاهر شده کلیک می‌کنیم تا ویزارد Active Directory Domain Services Installation اجرا شود.

- پس از افزودن نقش AD DS لینک‌هایی در پنجره Server Manager ظاهر می‌شود که اجرای Active Directory Domain Services Installation را یادآوری می‌کند. روی یکی از آنها کلیک می‌کنیم.

ویزارد طبق شکل ۱- ۱۰ ظاهر می‌شود.



شکل ۱- ۱۰ ویزارد Active Directory Domain Services Installation

نکته یک ویزارد برای دو سرویس

مایکروسافت در ویندوزسرور 2008 روی مدل مبتنی بر نقش تکیه می‌کند بنابراین توصیه می‌کند ابتدا نقش AD DS را اضافه کرده و سپس دستور Dcpromo.exe را اجرا کنیم ولی در هر صورت می‌توانیم با یک دستور Dcpromo.exe بسادگی هر دو را با هم انجام دهیم.

گزینه‌های نصب غیرحضوری (Unattended Installation) و فایل‌های پاسخ (Answer File)

روش دیگر اضافه یا حذف یک DC استفاده از نصب غیرحضوری در خط فرمان می‌باشد که Dcpromo.exe در ویندوز سرور 2008 از آن پشتیبانی می‌کند. گزینه‌های نصب غیرحضوری مقادیری را به ویزارد نصب Active Directory اضافه می‌کند. برای مثال گزینه NewDomianDNSName نام FQDN دامنه را مشخص می‌کند.

در حالت عادی گزینه‌های نصب از طریق خط فرمان با تایپ دستور dcpromo /unattendoption:value برای مثال dcpromo/newdomaindnsname:contoso.com پیکربندی می‌شود. به جای آن می‌توانیم از فایل پاسخ نصب غیرحضوری استفاده کنیم. فایل پاسخ یک فایل متنی است که دارای بخش تیتر با نام DCINSTALL بوده و بعد از آن گزینه‌ها و مقادیر آنها به شکل option=value می‌آید. به عنوان مثال فایل زیر گزینه NewDomianDNSName را مقداردهی می‌کند.

```
[DCINSTALL]
NewDomianDNSName=contoso.com
```

فایل پاسخ با افزودن مسیر به پارامتر unattend فراخوانی می‌شود مانند:

Dcpromo /unattend:"path to answer file"

گزینه‌های فایل پاسخ ممکن است با پارامترهای خط فرمان بی‌اثر شود. برای مثال اگر گزینه NewDomainDNSName در فایل پاسخ مشخص شده باشد و همان گزینه در پارامتر خط فرمان نیز مقداردهی شده باشد مقدار خط فرمان در اولویت قرار می‌گیرد. اگر گزینه‌ای در هیچ جایی مشخص نشده باشد ویزارد هنگام اجرا مقدار آنرا درخواست می‌کند.

این ویزارد با دستور Dcpromo.exe در خط فرمان در Server Core اجرا نمی‌شود و باعث بروز خطا می‌گردد.

برای دریافت لیست کامل پارامترهای نصب غیرحضوری پنجره خط فرمان elevated را باز کرده و دستور زیر را تایپ می‌کنیم:

Dcpromo /?[:operation]

در حالی که به جای operation یکی از عبارات زیر را تایپ می‌کنیم:

- **Promotion** همه پارامترهایی را که هنگام ساخت یک DC استفاده می‌کنیم برمی‌گرداند.
- **CreateDCAccount** همه پارامترهایی را که هنگام ساخت یک حساب prestaged برای یک RODC استفاده می‌شود برمی‌گرداند.
- **UseExistingAccount** همه پارامترهایی را که برای attach کردن یک DC به یک حساب prestaged RODC استفاده می‌شود برمی‌گرداند.
- **Demotion** همه پارامترهایی که هنگام حذف یک DC استفاده می‌شود برمی‌گرداند.

نکته ساخت یک فایل پاسخ

وقتی از رابط ویندوزی برای ساخت یک DC استفاده می‌کنیم ویزارد Active Directory Domain Services Installation در صفحه Summary گزینه‌ای را در اختیار ما قرار می‌دهد که بتوانیم تنظیمات را به یک فایل پاسخ منتقل کنیم. اگر بخواهیم فایل پاسخ بسازیم تا از آن درخط فرمان استفاده کنیم مثلا در نسخه Server Core می‌توانیم از این میانبر برای ساخت فایل استفاده کنیم.

نصب یک forest جدید در ویندوز سرور 2008

در فصل یک نصب اولین DC ویندوز سرور 2008 در forest جدید از طریق رابط ویندوزی بررسی شد. تمرین ۳ و ۴ از درس ۱ در همان فصل مراحل افزودن نقش AD DS به یک سرور را با استفاده از Server Manager و بعد اجرای دستور Dcpromo.exe شرح می‌داد. هنگام ساخت یک دامنه ریشه forest جدید باید نام DNS ریشه forest، نام NetBIOS و سطوح عملیاتی دامنه و forest را مشخص کنیم. اولین DC نمی‌تواند فقط خواندنی باشد و باید سرور GC باشد. اگر ویزارد نیاز به نصب یا پیکربندی DNS را تشخیص دهد به طور خودکار این کار را انجام می‌دهد.

همچنین استفاده از فایل پاسخ با تایپ عبارت dcpromo /unattend:"path to answer file" امکان‌پذیر است. مثال زیر حداقل پارامترهای نصب غیرحضوری یک DC جدید در یک forest جدید را در نشان می‌دهد:

```
[DCINSTALL]
ReplicaOrNewDomain=domain
NewDomain=forest
NewDomainDNSName=fully qualified DNS name
DomainNetBiosName=domain NetBIOS name
ForestLevel={0=Windows 2000 Server Native;
2=Windows Server 2003 Native;
3=Windows Server 2008}
DomainLevel={0=Windows Server 2000 Native;
2=Windows Server 2003 Native;
3=Windows Server 2008}
InstallDNS=yes
DatabasePath="path to folder on a local volume"
LogPath="path to folder on a local volume"
```

SYSVOLPath=”path to folder on a local volume”
SafeModeAdminPassword=password
RebootOnCompletion=yes

همچنین می‌توانیم یک یا چند پارامتر و مقادیر نصب غیرحضوری را در خط فرمان مشخص کنیم. برای مثال وقتی نمی‌خواهیم کلمه عبور Directory Services Restore Mode در فایل پاسخ باشد مقدارش خالی گذاشته و هنگام اجرای Dcpromo.exe پارامتر آنرا به شکل /SafeModeAdminPassword:password مشخص می‌کنیم.

همچنین می‌توانیم همه گزینه‌ها را در خط فرمان وارد کنیم. مثال زیر اولین DC را در forest جدید می‌سازد. در این forest هیچ ویندوز سرور 2003 به عنوان DC موجود نیست.

Dcpromo /unattend /installDNS:yes /dnsOnNetwork:yes /replicaOrNewDomain:domain /newDomain:forest /newDomainDnsName:contoso.com /DomainNetbiosName:contoso /databasePath:”ntds” /logPath:”f:\ntdslogs” /sysvolpath:”g:\sysvol” /safeModeAdminPassword:password /forestLevel:3 /domainLevel:3 /rebootOnCompletion:yes

نصب Additional Domain Controller در دامنه

وقتی دامنه‌ای دارای حداقل یک DC ویندوز سرور 2000 ، 2003 یا 2008 باشد برای این دامنه می‌توان additional DC پیکربندی کرد. این سرور به منظور توزیع تایید هویت به کار می‌رود که باعث ایجاد تحمل خرابی بوده یا تایید هویت را برای سایت‌های راه دور فراهم می‌کند.

نصب اولین DC ویندوز سرور 2008 در یک دامنه یا forest موجود

اگر forest ما دارای DC های ویندوز سرور 2003 یا 2000 باشد باید قبل از ساخت اولین DC ویندوز سرور 2008 آنها را آماده کنیم. دلیل آن اینست که ویندوز سرور 2008 یک سری اشیاء و خصیصه‌ها به دایرکتوری اضافه می‌کند که نسخه‌های قبلی ویندوز آنها را تشخیص نمی‌دهند. بنابراین schema باید به روز شود. Schema تعریف کلاس‌های خصیصه و اشیائی است که در دامنه موجود است. این مانند یک کاتالوگی از چیزی است که در پارتیشن‌های دایرکتوری دیگر ساخته می‌شود. برای آماده سازی schema برای ویندوز سرور 2008 مراحل زیر را دنبال می‌کنیم:

۱. با کاربر عضو یکی از گروههای Enterprise Admins ، Schema Admins یا Domain Admins به schema master وارد می‌شویم.

۲. محتویات پوشه Sources\Adprep\ را از DVD ویندوز سرور 2008 به یک پوشه دلخواه در schema master کپی می‌کنیم.

۳. پنجره خط فرمان را باز کرده و به مسیر پوشه Adprep می‌رویم.

۴. دستور adprep /forestprep را اجرا می‌کنیم.

۵. اگر قرار است یک RODC روی دامنه نصب کنیم دستور adprep /rodcprep را اجرا می‌کنیم.

مدت زمانی طول می‌کشد که عملیات پایان یابد. وقتی تغییرات در کل forest منتشر شد می‌توانیم دامنه‌ها را برای ویندوز سرور 2008 آماده کنیم. برای آماده‌سازی دامنه ویندوز سرور 2000 یا 2003 برای ویندوز سرور 2008 مراحل زیر را انجام می‌دهیم:

۱. با کاربر عضو Domain Admins به operations master وارد می‌شویم. در درس ۲ یاد می‌گیریم operations master را پیدا کنیم.

۲. محتویات پوشه Sources\Adprep\ را از DVD ویندوز سرور 2008 به یک پوشه دلخواه در infrastructure master کپی می‌کنیم.

۳. پنجره خط فرمان را باز کرده و به مسیر پوشه Adprep می‌رویم.

۴. دستور adprep /domainprep /gpprep را اجرا می‌کنیم. در ویندوز سرور 2003 ممکن است پیغامی مبنی بر عدم نیاز به به روزآوری دریافت کنیم که پیغام را ignore می‌کنیم.

قبل از نصب DC ویندوز سرور 2008 اجازه می‌دهیم تغییرات به کل forest منتشر شود.

نصب Additional Domain Controller

افزودن یک Additional DC توسط نصب AD DS و اجرای ویزارد Active Directory Domain Services Installation انجام می‌شود. برخی از مراحل شبیه نصب اولین DC می‌باشد مانند پیکربندی محل فایل‌ها و کلمه عبور Directory Services Restore Mode .

اگر شبکه ما دارای یک DC باشد و در ویزارد نصب DC کادر Use Advanced Mode Installation را علامت بزنیم قادر به پیکربندی گزینه‌های پیشرفته زیر خواهیم بود:

- **Install From Media** به طور پیش‌فرض DC جدید همه داده همه پارتیشن‌های دایرکتوری را که میزبانش است از DC های دیگر کپی می‌کند. برای بالا بردن کارایی نصب مخصوصا روی لینک‌های کند می‌توان از رسانه نصب ساخته شده توسط DC های موجود استفاده کرد. رسانه نصب نوعی پشتیبان است. DC جدید داده را از رسانه نصب به طور مستقیم خوانده و سپس فقط آپدیت‌ها را از DC های دیگر دریافت می‌کند. نصب از روی رسانه (IFM) در بخش Installing AD DS from Media بحث می‌شود.

- Source Domain Controller اگر بخواهیم مشخص کنیم که از روی کدام DC داده به DC جدید تکثیر شود روی Use This Specific Domain Controller کلیک می‌کنیم.

نکته دستور Dcpromo /adv هنوز پشتیبانی می‌شود.

در ویندوز سرور 2003 این دستور برای مشخص کردن گزینه‌های نصب پیشرفته استفاده می‌شد. پارامتر adv هنوز هم پشتیبانی می‌شود.

برای استفاده از دستور Dcpromo.exe با پارامترهای مشخص کننده گزینه‌های نصب غیرحضوری می‌توانیم از پارامترهای حداقل زیر استفاده کنیم:

```
Dcpromo /unattend /replicaOrNewDomain:replica /replicaDomainDNSName:contoso.com
/installDNS:yes /confirmGC:yes /databasePath:”e:\ntds” /logPath:”f:\ntdslogs”
/sysvolpath:”g:\sysvol” /safeModeAdminPassword:password /rebootOnCompletion:yes
```

اگر با اعتبار کاربر دامنه به سرور وارد نشده‌ایم باید درکنار پارامتر userdomain username را نیز مشخص کنیم. یک فایل پاسخ حداقلی برای additional DC در یک دامنه موجود به شکل زیر است:

```
[DCINSTALL]
ReplicaOrNewDomain=replica
ReplicaDomainDNSName=FQDN of domain to join
UserDomain=FQDN of domain of user account
UserName=DOMAIN\username (in Administrators group of the domain)
Password=password for user specified by UserName (* to prompt)
InstallDNS=yes
ConfirmGC=yes
DatabasePath=”path to folder on a local volume”
LogPath=”path to folder on a local volume”
SYSVOLPath=”path to folder on a local volume”
SafeModeAdminPassword=password
```

RebootOnCompletion=yes

نصب یک دامنه فرزند جدید (Child Domain) روی ویندوز سرور 2008

اگر شبکه دارای دامنه باشد می‌توانیم یک دامنه فرزند بسازیم. قبل از شروع باید دستور Adprep /forestprep را طبق شرایط توصیف شده در بخش‌های قبلی اجرا کنیم. سپس AD DS را نصب کرده و ویزارد نصب را اجرا می‌کنیم. در صفحه Choose A Deployment Configuration روی Existing Forest و Create A New Domain In An Existing Forest کلیک می‌کنیم. در اینجا باید سطح عملیاتی دامنه را نیز مشخص کنیم. چون این اولین DC در دامنه است نمی‌تواند RODC باشد یا از روی مدیا نصب شود. اگر در صفحه Welcome کادر Advanced Mode Installation را علامت بزنیم ویزارد صفحه Source Domain Controller را فراهم می‌کند تا DC مبدا را برای تکثیر پیکربندی و پارتیشن‌های schema مشخص کنیم.

با استفاده از دستور Dcpromo.exe می‌توانیم یک دامنه فرزند با حداقل گزینه مانند دستورات زیر بسازیم:

```
Dcpromo /unattend /installDNS:yes
/replicaOrNewDomain:domain /newDomain:child
/ParentDomianDNSName:contoso.com
/newDomainDNSName:subsidiary.contoso.com /childName:subsidiary
/DomainNetbiosName:subsidiary
/databasePath:”e:\ntds” /logPath:”f:\ntdslogs” /sysvolpath:”g:\sysvol”
/safeModeAdminPassword:password /forestLevel:3 /domainLevel:3
/rebootOnCompletion:yes
```

فایل پاسخ زیر همان پارامترهای حداقلی را منعکس می‌کند:

```
[DCINSTALL]
ReplicaOrNewDomain=domain
NewDomain=child
ParentDomianDNSName:FQDN of parent domain
UserDomain=FQDN of user specified by UserName
UserName=DOMAIN\username (in Administrators group of ParentDomainDNSName)
Password=password for user specified by UserName or * for prompt
ChildName=single-label prefix for domian (child domain FQDN will be
ChildName.ParentDomainDNSName)
/DomainNetbiosName: Domain NetBIOS name
DomainLevel=domain functional level (not lower than current forest level)
InstallDNS=yes
CreateDNSDelegation=yes
DNSDelegationUserName=DOMAIN\username with permissions to create DNS delegation,
if different than UserName, above
DNSDelegationPassword=passord for DNSDelegationUserName or * for prompt
DatabasePath=”path to folder on a local volume”
LogPath=”path to folder on a local volume”
SYSVOLPath=”path to folder on a local volume”
SafeModeAdminPassword=password
RebootOnCompletion=yes
```

نصب یک Domain Tree جدید

در فصل یک آموختیم که در یک forest منظور از tree ترکیب یک یا چند دامنه که در فضای نام پشت سرهم قرار می‌گیرند می‌باشد. بنابراین برای مثال دامنه‌های contoso.com و subsidiary.contoso.com در یک tree قرار می‌گیرند. Tree های بعدی دامنه‌هایی هستند که در فضای نام دیگری قرار دارند. برای مثال اگر شرکت Contoso,Ltd. شرکت Tailspin Toys را بخرد دامنه tailspintoys.com در یک tree مجزا قرار خواهد گرفت. بین دامنه فرزند و دامنه در یک tree دیگر تفاوت کوچکی چه از لحاظ عملکردی و چه مراحل نصب وجود دارد.

ابتدا باید دستور Adprep /forestprep را اجرا کرده و سپس AD DS را نصب و ویزارد نصب DC را اجرا کنیم. در صفحه Choose A Deployment Configuration روی Existing Forest کلیک کرده و گزینه Create A New Domain In An Existing Forest و سپس Create A New Domain Tree Root Instead Of A New Child Domain را انتخاب می‌کنیم. بقیه مراحل مشابه نصب یک دامنه فرزند جدید است.

گزینه‌های زیر به عنوان پارامترهای دستور Dcpromo.exe برای ساخت tree جدید برای دامنه tailspintoys.com در contoso.com forest به کار می‌رود:

```
Dcpromo /unattend /installDNS:yes
/replicaOrNewDomain:domain /newDomain:tree
/newDomainDNSName:tailspintoys.com /DomainNetbiosName:tailspintoys
/databasePath:”e:\ntds” /logPath:”f:\ntdslogs” /sysvolpath:”g:\sysvol”
/safeModeAdminPassword:password /domainLevel:2
/rebootOnCompletion:yes
```

سطح عملیاتی دامنه عدد ۲ (ویندوز سرور 2003) خواهد بود بنابراین در دامنه می‌توان از DC با سیستم عامل 2003 استفاده کرد.

یک فایل پاسخ غیرحضوری که همان tree جدید را می‌سازد در زیر آمده است:

```
[DCINSTALL]
ReplicaOrNewDomain=domain
NewDomain=tree
NewDomainDNSName=FQDN of new domain
DomainNetBiosName=NetBIOS name of new domain
UserDomain=FQDN of user specified by UserName
UserName=DOMAIN\username (in Administrators group of ParentDomainDNSName)
Password=password for user specified by UserName or * for  prompt
DomainLevel=domain functional level (not lower than current forest level)
InstallDNS=yes
ConfirmGC=yes
CreateDNSDelegation=yes
DNSDelegationUserName=account with permissions to create DNS delegation, required only
if different than UserName, above
DNSDelegationPassword=passord for DNSDelegationUserName or * for prompt
DatabasePath=”path to folder on a local volume”
LogPath=”path to folder on a local volume”
SYSVOLPath=”path to folder on a local volume”
SafeModeAdminPassword=password
RebootOnCompletion=yes
```

نصب RODC به روش Staging

همانطور که در فصل ۸ دیدیم RODC برای فراهم کردن تایید هویت در شعبات شرکت طراحی شده است. در بسیاری از موارد هیچ کارشناس فنی در محل شعبه حضور ندارد. پس چطور باید یک DC در آنجا پیکربندی کنیم؟

برای پاسخ به این سئوال ویندوز سرور 2008 به ما اجازه می‌دهد نصب را به صورت Staging یا تفویض اختیار انجام دهیم. این کار دو مرحله دارد:

- **ساخت یک حساب برای RODC** کاربر عضو گروه Domain Admins باید یک حساب برای RODC در Active Directory بسازد. پارامترهای مرتبط با RODC در این مرحله مشخص می‌شوند. مانند نام، سایتی که RODC در آن ساخته می‌شود و به طور اختیاری کاربر یا گروهی که می‌تواند مرحله بعدی نصب را انجام دهد.

- **Attach کردن سرور با حساب RODC** پس از ساخت حساب AD DS نصب شده و RODC به دامنه attach می‌شود. این مراحل می‌تواند هنگام ساخت حساب RODC توسط کاربران یا گروهها مشخص شود. این کاربران

نیازی به عضویت در گروهی خاص را ندارند. کاربر عضو Domain Admins یا Enterprise Admins می‌تواند سرور را attach کند ولی توانایی تفویض اختیار این مرحله به کاربر عادی توزیع RODC را در شعبات ساده می‌سازد. DC داده خود را از یک DC قابل تغییر در دامنه تکثیر می‌کند یا می‌توان از روش IFM که در بخش‌های بعدی شرح داده می‌شود استفاده کرد.

ساخت حساب برای RODC به روش Prestaged

برای ساخت حساب برای RODC با استفاده از ابزار Active Directory Users and Computers روی Domain Controllers OU کلیک راست کرده و Pre-Create Read-Only Domain Controller Account را انتخاب می‌کنیم. ویزاردی ظاهر می‌شود که خیلی شبیه به ویزارد نصب DC می‌باشد. ویزارد از ما نام RODC و سایت را می‌پرسد. ما همچنین قادر به پیکربندی سیاست تکثیر کلمه عبور طبق جزئیات فصل ۸ خواهیم بود.

در صفحه Delegation Of RODC Installation And Administration می‌توانیم یک واحد امنیتی مانند کاربر یا گروه را مشخص کنیم که بتواند سرور را به حساب RODC که می‌سازیم attach کند. کاربر یا گروه دسترسی مدیریتی محلی را نیز روی RODC خواهد داشت. پیشنهاد می‌گردد که این حق به یک گروه تفویض شود تا کاربر. اگر کاربر یا گروهی مشخص نگردد فقط کاربران عضو گروه Domain Admins یا Enterprise Admins قادر به انجام این کار خواهند بود.

Attach کردن سرور به حساب RODC

پس از ایجاد حساب به روش prestaged سرور را به آن attach می‌کنیم. ویزارد Active Directory Domain Services Installation به راحتی اجرا نمی‌شود. این کار با اجرای دستور dcpromo /useexistingaccount:attach انجام می‌شود. ویزارد اعتبار شبکه‌ای مناسب را طلب می‌کند و سپس حساب RODC را که در اعتبار قید شده در دامنه پیدا می‌کند. بقیه مراحل شبیه به مراحل نصب DC می‌باشد.

به منظور استفاده از فایل پاسخ گزینه‌ها و مقادیر زیر را وارد می‌کنیم:

```
[DCINSTALL]
ReplicaDomainDNSName=FQDN of domain to join
UserDomain=FQDN of user specified by UserName
UserName=DOMAIN\username (in Administrators group of the domain)
Password=password for user specified by UserName
InstallDNS=yes
ConfirmGC=yes
DatabasePath=”path to folder on a local volume”
LogPath=”path to folder on a local volume”
SYSVOLPath=”path to folder on a local volume”
SafeModeAdminPassword=password
RebootOnCompletion=yes
```

دستور Dcpromo را با گزینه‌های unattend:”answer file path” و UseExistingAccount:Attach مانند مثال زیر اجرا می‌کنیم:

```
Dcpromo /useexistingaccount:attach /unattend:”c:\rodcanswer.txt”
```

همه گزینه‌ها در فایل پاسخ یا از طریق خط فرمان به طور مستقیم می‌توانند مشخص شوند. فقط کافی است دستوری مشابه دستور زیر را اجرا کنیم:

```
Dcpromo /unattend /UseExistingAccount:Attach /ReplicaDomainDNSName:contoso.com
/UserDomain:contoso.com /UserName:contoso\dan /password:* /databasePath:”e:\ntds”
/logPath:”f:\ntdslogs” /sysvolpath:”g:\sysvol” /safeModeAdminPassword:password
/rebootOnCompletion:yes
```

نصب AD DS از روی رسانه نصب

وقتی DC به forest اضافه می‌شود داده از پارتیشن‌های دایرکتوری به روی DC جدید تکثیر می‌شود. در شبکه‌های با دایرکتوری حجیم یا محیط‌هایی که پهنای باند بین DC جدید و DC قبلی کم است نصب AD DS باگزینه IFM بسیار کاراتر انجام می‌شود. رسانه یک نسخه از Active Directory است که توسط ویزارد نصب DC به عنوان منبع داده برای ساخت دایرکتوری روی DC جدید استفاده می‌شود. سپس DC جدید فقط آپدیت‌ها را از DC دیگر دریافت می‌کند بنابراین اگر رسانه نصب جدید باشد تکثیر روی DC جدید سریعتر انجام می‌شود چون داده کمتری منتقل می‌شود.

به خاطر داشته باشید که نه تنها دایرکتوری بلکه SYSVOL هم به روی DC جدید تکثیر می‌شود. وقتی رسانه نصب خود را می‌سازیم باید مشخص کنیم که SYSVOL را هم شامل شود یا نه.

استفاده از IFM این امکان را به ما می‌دهد که تاثیرات را روی پهنای باند شبکه کنترل کنیم. برای مثال می‌توانیم رسانه نصب را ساخته و در ساعات غیراداری آنرا به سایت راه دور منتقل کنیم. سپس در ساعات اداری DC را نصب کنیم. به دلیل اینکه رسانه نصب در سایت محلی است تاثیر روی شبکه کاهش می‌یابد و فقط آپدیت‌ها از روی لینک راه دور تکثیر می‌شود.

برای ساخت رسانه نصب پنجره خط فرمان را روی DC قابل تغییر که سیستم عامل ویندوز سرور 2008 دارد باز می‌کنیم. رسانه نصب روی پلتفرم‌های مختلف سازگار است. دستور Ntdsutil.exe را اجرا کرده و سپس دستور activate instance ntds را و بعد ifm را اجرا می‌کنیم. در جلوی خط فرمان با عبارت ifm: بر اساس نوع رسانه نصب مورد نظر یکی از دستورات زیر را تایپ می‌کنیم.

- **Create sysvol full** path رسانه نصب را به همراه SYSVOL برای DC قابل تغییر در پوشه مشخص شده در دستور می‌سازد.
- **Create full** path رسانه نصب را بدون SYSVOL برای DC قابل تغییر یا یک AD LDS در پوشه مشخص شده در دستور می‌سازد.
- **Create sysvol rodc** path رسانه نصب را به همراه SYSVOL برای DC فقط خواندنی در پوشه مشخص شده در دستور می‌سازد.
- **Create rodc** path رسانه نصب را بدون SYSVOL برای DC فقط خواندنی در پوشه مشخص شده در دستور می‌سازد.

وقتی ویزارد نصب DC را اجرا می‌کنیم کادر Use Advanced Mode Installation را علامت می‌زنیم و در صفحه بعد نصب از طریق رسانه پیشنهاد می‌گردد. گزینه Replicate Data From Media At The Following Location را انتخاب می‌کنیم. از گزینه نصب ReplicationSourcePath هم در فایل پاسخ و هم در خط فرمان با دستور Dcpromo.exe می‌توانیم استفاده کنیم.

حذف DC

دستور Dcpromo.exe برای حذف یک DC نیز به کار می‌رود. این کار هم با ویزارد و هم از طریق خط فرمان با تعیین پارامترها در خط فرمان یا در فایل پاسخ انجام می‌شود. وقتی یک DC حذف می‌شود در حالی که با دامنه ارتباط دارد متاداده forest را به روز می‌کند به طوری که دایرکتوری متوجه حذف DC شود.

وقتی ارتباط DC با دامنه قطع است باید از گزینه forceremoval در دستور Dcpromo.exe استفاده کنیم. دستور dcpromo /forceremoval را اجرا می‌کنیم. پیغام‌هایی مبنی بر امکان وجود نقش‌هایی روی سرور DC دریافت می‌کنیم. همه پیغام‌ها را خوانده و پس از تایید روی دکمه Yes کلیک می‌کنیم. با استفاده از گزینه demotefsmo:yes از دستور Dcpromo.exe می‌توان این پیغام‌ها را خنثی کرد. بعد از اینکه DC حذف شد باید متاداده forest را دستی پاک کنیم.

تمرینات نصب DC

در این تمرینات اقدامات لازم برای نصب یک additional DC در دامنه contoso.com انجام می شود. به کمک Active Directory Domain Services Installation Wizard ، AD DS نصب و یک additional DC پیکربندی می شود. به جای یک نصب کامل ، تنظیمات در یک فایل پاسخ ذخیره خواهند شد و با استفاده از دستور Dcpromo.exe و گزینه های نصب ، از آن فایل در فرآیند نصب غیر حضوری استفاده خواهد شد.

برای انجام این تمرینات نیاز به سرور دیگری می باشد که بر روی آن Windows Server 2008 نصب شده باشد. این سرور که نام آن SERVER02 می‌باشد باید عضو دامنه contoso.com باشد. تنظیمات این سرور به شرح زیر خواهد بود:

نام کامپیوتر: SERVER02

عضویت دامنه: contoso.com

آدرس Ipv4 : 10.0.0.12

Subnet Mask: 255.255.255.0

Default Gateway: 10.0.0.1

سرور DNS : 10.0.0.11

تمرین یک : ساخت یک Additional DC با استفاده از Active Directory Domain Services Installation Wizard

در این تمرین از Active Directory Domain Services Installation Wizard یا همان Dcpromo.exe برای ساخت یک additional DC در دامنه contoso.com استفاده می شود که البته فرآیند نصب کامل انجام نمی شود چرا که تنظیمات به صورت یک فایل پاسخ (answer file) ذخیره شده که در تمرین بعدی استفاده خواهد شد.

۱- با کاربر CONTOSO\Administrator به SERVER02 وارد می‌شویم.

۲- روی استارت کلیک کرده ، run را انتخاب می کنیم و بعد از تایپ Dcpromo.exe ،دکمه Enter را می زنیم

۳- گزینه Next را کلیک می کنیم

۴- درصفحه Operating System Compatibility ،هشدارهای مربوط به تنظیمات امنیتی پیش فرض برای DC های دارای سیستم عامل ویندوز سرور 2008 را مرور کرده و بعد بر روی Next کلیک می کنیم

۵- در صفحه Choose A Deployment Configuration ،ابتدا Existing Forest را انتخاب کرده و سپس گزینه Add A Domain Controller To An Existing Domain را انتخاب می کنیم و روی Next کلیک می کنیم

۶- در صفحه Network Credentials عبارت contoso.com را درکادر متنی تایپ کرده و گزینه My Current Logged On Credentials را انتخاب و Next را کلیک می کنیم

۷- در صفحه Select A Domain دامنه contoso.com را انتخاب کرده و Next را کلیک می کنیم

۸- در صفحه Select A Site گزینه Default-First-Site-Name را انتخاب کرده و روی Next کلیک می کنیم . صفحه Additional Domain Controller Options ظاهر می شود که در آن به صورت پیش فرض DNS Server و Global Catalog انتخاب شده اند

۹- علامت کادرهای DNS Server و Global Catalog را برداشته و روی Next کلیک می کنیم. هشدار An Infrastructure Master Configuration Conflict ظاهر خواهد شد که در درس ۲ در مورد آن خواهیم خواند، پس از این پیام خطا می گذریم

۱۰- روی گزینه Do Not Transfer The Infrastructure Master Role To This Domain Controller. I Will Correct The Configuration Later کلیک می کنیم

۱۱- در صفحه Location For Database, Log Files, And SYSVOL آدرس های پیش فرض برای فایلهای پایگاه داده ،directory service log و SYSVOL را تغییر نداده و روی Next کلیک می کنیم. بهترین کار در محیط واقعی نگهداری این فایلها در در سه دیسک جداگانه می باشد که در روی آنها هیچ نرم افزار یا فایلی

مربوط به AD DS نباشد. این کار باعث بهبود کارایی و کاهش زمان عملیات گرفتن نسخه پشتیبان و بازگرداندن آن می شود

۱۲- در صفحه Directory Services Restore Mode Administrator Password در هر دو فیلد کلمه عبور و تایید کلمه عبور یک کلمه عبور پیچیده را تایپ کرده و سپس Next می کنیم. این کلمه عبور را همیشه به خاطر داشته باشید

۱۳- در صفحه Summary تنظیمات خود را مرور کرده و در صورت وجود اشتباه با زدن دکمه Back آنها را تصحیح می کنیم

۱۴- روی Export Settings کلیک می کنیم

۱۵- روی Browse Folders کلیک می کنیم

۱۶- Desktop را انتخاب می کنیم

۱۷- در فیلد مربوط به نام فایل عبارت Additional DC را نوشته و روی دکمه Save کلیک می کنیم. پیامی مبنی بر ذخیره سازی تنظیمات با موفقیت ظاهر می شود

۱۸- روی Ok کلیک می کنیم

۱۹- در صفحه Active Directory Domain Services Installation Wizard Summary روی Cancel کلیک می کنیم.

۲۰- با کلیک روی دکمه Yes لغو عملیات را تایید می کنیم

تمرین دوم اضافه کردن یک DC از طریق خط فرمان

در این تمرین از فایل پاسخی که در تمرین قبل ساختیم برای نصب یک DC از طریق خط فرمان استفاده می کنیم.

۱- فایل AdditionalDC.txt را که در تمرین اول درست کردیم باز می کنیم

۲- فایل پاسخ را مورد بررسی قرار می دهیم. نکته: خطوطی که با علامت ; شروع شده اند توضیحات می باشند

۳- یک پنجره خط فرمان باز می کنیم، از آنجا که می خواهیم بوسیله فایل پاسخ یک خط فرمان بسازیم دو پنجره Notepad و پنجره خط فرمان را طوری قرار می دهیم که هر دو قابل دیدن باشند یا اینکه از فایل پاسخ یک نسخه به عنوان مرجع پرینت می کنیم

۴- دستورات خط فرمان را برای نصب DC با استفاده از تنظیمات درون فایل پاسخ تایپ می‌کنیم. پارامترهایی که در فایل پاسخ به صورت option=value هستتند در خط فرمان به صورت /option:value در می آیند.

۵- فرمان زیر را تایپ کرده و سپس کلید Enter را می زنیم

```
dcpromo /unattend /replicaornewdomain:replica
/replicadomaindnsname:contoso.com /sitename:Default-First-Site-Name
/installDNS:No /confirmGC:No /CreateDNSDelegation:No
/databasepath:"C:\Windows\NTDS" /logpath:"C:\Windows\NTDS"
/sysvolpath:"C:\Windows\SYSVOL" /safemodeadminpassword:password
/transferimroleifnecessary:no
```

که در این فرمان کلمه عبور به صورت پیچیده خواهد بود

۶- فرآیند نصب کامل و سیستم راه اندازی مجدد می شود

تمرین سوم ساخت رسانه نصب

می توان با گزینه IFM میزان تکثیر مورد نیاز برای ساخت یک DC را کاهش داد. IFM نیازمند ساخت یک رسانه نصب است که در واقع نسخه پشتیبان اکتیو دایرکتوری می باشد. در این تمرین یک IFM خواهیم ساخت

۱- با اعتبار Administrator وارد SERVER01 می شویم

۲- command prompt را باز می کنیم
۳- عبارت ntdsuti را تایپ کرده و Enter را فشار می دهیم
۴- عبارت activate instance ntds را تایپ کرده و Enter را فشار می دهیم
۵- عبارت ifm را تایپ کرده و Enter را فشار می دهیم
۶- علامت ؟ را تایپ کرده و با فشار دادن Enter لیست دستورات موجود در حالت ifm را مشاهده می کنیم
۷- عبارت create sysvol full c:\IFM را تایپ کرده و Enter را فشار می دهیم
فایلهای رسانه نصب در آدرس C:\Ifm کپی می شوند

خلاصه درس

- سرویس AD DS را می توان با اجرای Dcpromo.exe که باعث اجرای ویزارد Active Directory Domain Services Installation می شود نصب کرد یا با گزینه نصب غیر حضوری می توان فرآیند نصب را از طریق یک فایل پاسخ انجام داد
- هنگامی که اولین DCخود را در forest موجود معرفی می کنیم باید دستور Adprep /forestprep را اجرا کنیم و قبل از آنکه اولین DC خود را در دامنه موجود معرفی می کنیم باید دستور Adprep /gpprep /domainprep را اجرا کنیم
- قبل از نصب RODC در دامنه هایی که شامل DC هایی با سیستم عامل های ویندوز سرور 2000 و 2003 هستند باید دستور Adprep /rodcprep اجرا شود
- برای انجام فرآیند نصب RODC باید یک حساب برای RODC ساخت و کاربر یا گروهی را مشخص کرد که بتواند RODCرا به آن حساب متصل کند
- برای کاهش میزان تکثیر می توان از یک رسانه نصب به عنوان منبع، در هنگام نصب DCاستفاده کرد

سئوالات پایان درس

۱- ما مدیر شبکه موسسه Trey Research هستیم. Trey Research forest دارای سه دامنه می باشد که هرکدام از آنها دارای دو DC با سیستم عامل ویندوز سرور 2003 هستند. می خواهیم یکی از این DC ها را به ویندوز سرور 2008 ارتقا دهیم. در ابتدا چه باید کرد؟

A . ارتقا سیستم عامل DCها به ویندوز سرور 2008
B . اجرای فرمان Adprep.exe /domainprep /gpprep
C . اجرای ویزارد Active Directory Domain Services Installation
D . اجرای دستور Adprep.exe /forestprep
E . اجرای دستور Adprep.exe /rodcprep

۲- ما مدیر شبکه شرکت Contoso هستیم دامنه ما از DCهایی با سیستم عامل ویندوز سرور 2008 تشکیل شده است. تصمیم داریم پروسه اعتبار سنجی در سایت راه دور خود را بوسیله راه اندازی یک RODC در آن بهبود دهیم ، همچنین تصمیم داریم چون در آن سایت هیچ کس آشنا به IT نیست ، انجام این عمل را به مدیر سایت واگذار کنیم.در ضمن نمی خواهیم که به او اعتبار Domain Administrator بدهیم کدام مراحل باید توسط ما یا آن مدیر انجام شوند؟(در صورت نیازتمام گزینه های درست را انتخاب کنید. هر پاسخ صحیح بخشی از راه حل است)

A . اجرای دستور Adprep /rodcprep
B . ساخت RODC account در OU مربوط به DCها
C . اجرای Dcpromo.exe با گزینه Use Existing Account
D . جدا کردن سرور از دامنه

۳- در نظر داریم یک سرور را به عنوان DC راه اندازی کنیم، اما نگران ترافیکی هستیم که در زمان تکثیر جابجا می شود و تاثیری که می تواند روی لینک کند بین سایت سرور و مرکز داده‌ای که بقیه سرور ها ر آن هستند، داشته باشد

به همین دلیل تصمیم می گیریم سرور را به کمک فایل پشتیبان یک DC دیگر راه اندازی کنیم. برای ساخت رسانه نصب چه باید کرد؟

A . اجرای دستور Ntbackup.exe و انتخاب System State
B . نصب Windows Server Backup
C . اجرای دستور Ntdsutil.exe در حالت IFM و استفاده از دستور Create Sysvol Full
D . کپی کردن ntds.dit و SYSVOL از یک DC که در سایت راه دور باشد

درس ۲: پیکربندی Operations Masters

در دامنه Active Directory همه DC ها معادل هم هستند. همه آنها قابلیت نوشتن روی بانک اطلاعاتی و تکثیر تغییرات روی دیگر DC ها را دارند. ولی در هر توپولوژی تکثیر multimaster عملیات خاصی فقط باید توسط یک و فقط یک سیستم انجام شود. در دامنه Active Directory ، operations masters در اصل DC هایی هستند که نقش اختصاصی را بازی می‌کنند. در این درس پنج operation masters که در Active Directory forest و دامنه موجود است معرفی می‌شود. اهداف آنها را یاد می‌گیریم و یاد می‌گیریم چطور آنرا در شبکه پیدا کنیم و تفاوت‌های مدیریت آنها و انتقال نقش‌ها را متوجه می‌شویم.

بعد از این درس یاد می‌توانیم:

- اهداف پنج master operation منفرد را در Active Directory forests تعریف کنیم.
- DC های مجری نقش‌های operations master را پیدا کنیم.
- جایگاه نقش‌های operations master را طراحی کنیم.
- نقش‌های operations master را منتقل و تصرف کنیم.

زمان تقریبی: ۴۵ دقیقه

درک Master Operations منفرد

در هر بانک اطلاعات تکثیر شده‌ای برخی تغییرات باید فقط توسط یک replica اجرا شود به این دلیل که اجرای آنها در حالت multimaster نشدنی است. Active Directory نیز از این قاعده مستثنی نیست. تعداد محدودی عملیات اجازه اجرا در جاهای مختلف و در یک زمان را ندارند و باید مسئول فقط یک DC در دامنه یا forest باشند. این عملیات و DC هایی که آنها را انجام می‌دهند به واژه‌های متعددی نامیده می‌شوند:

- operations masters
- operations masters roles
- single master roles
- operations tokens
- flexible single master operations (FSMOs)

صرف نظر از واژه‌ای که به کار می‌بریم مفهوم همه آنها یکی است. یک DC عملیات را انجام می‌دهد و تا زمانی که این سرور آنرا انجام می‌دهد هیچ DC دیگری آنرا انجام نخواهد داد.

AD DS حاوی پنج نقش operations master می‌باشد. دو نقش برای کل forest اجرا می‌شود:

- Domain naming
- Schema

سه نقش در هر دامنه اجرا می‌شود:

- Relative identifier (RID)
- Infrastructure
- PDC Emulator

همه این نقش‌ها در بخش‌های بعدی با جزئیات شرح داده می‌شوند. در یک forest با یک دامنه پنج operations masters و در forest با دو دامنه هشت operations masters موجود است زیرا سه نقش master دامنه به طور جداگانه در هر کدام از دو دامنه پیاده‌سازی می‌شود.

نقش‌های operations masters در سطح forest

Schema master و domain naming master باید در forest منحصر باشند. هر نقش در کل forest توسط فقط یک DC اجرا می‌شود.

نقش Domain Naming Master

این نقش هنگام افزودن یا حذف دامنه در forest استفاده می‌شود. هنگام افزودن یا حذف دامنه این نقش باید در دسترس باشد وگرنه عملیات با شکست مواجه می‌شود.

نقش Schema Master

DC دارای نقش schema master مسئول ایجاد هرگونه تغییر روی forest schema می‌باشد. بقیه DC ها فقط نگهدارنده replica فقط خواندنی از schema می‌باشند. اگر بخواهیم schema را ویرایش کنیم یا برنامه‌ای نصب کنیم که آنرا تغییر دهد پیشنهاد می‌گردد آنرا روی DC دارنده نقش schema master انجام دهیم. در غیر اینصورت تغییرات مورد نظر باید برای shema master به منظور ثبت در schema ارسال گردد.

نقش‌های operations master درسطح دامنه

هر دامنه دارای سه master operation منفرد می‌باشد. RID، Infrastructure و PDC Emulator . هر نقش توسط یک DC در دامنه اجرا می‌شود.

نقش RID Master

این نقش نقش اصلی ساخت SID را برای واحدهای امنیتی مانند کاربران ، گروهها و کامپیوترها بازی می‌کند. SID یک واحد امنیتی باید منحصر باشد. به دلیل اینکه هر DC می‌تواند حساب و در نتیجه SID ایجاد کند یک مکانیزم برای تولید SID های منحصر به فرد مورد نیاز است. DC ها توسط انتساب یک RID به SID دامنه SID ها را تولید می‌کنند. RID master دامنه، به همه DC های دامنه یک انباره RID منحصر اختصاص می‌دهد. بنابراین همه DC ها می‌توانند مطمئن شوند که SID که تولید می‌کنند منحصر به فرد است.

نقش Infrastructure Master

در یک محیط با چند دامنه ممکن است یک شیء به اشیاء دیگر در دامنه‌های دیگر ارجاع شود. مثلا یک گروه ممکن است دارای اعضاء از یک دامنه دیگر باشد. مقدار خصیصه member شامل DN همه اعضاء می‌باشد. اگر عضوی از دامنه دیگر منتقل شود یا نامش تغییر کند infrastructure master مربوط به دامنه گروه خصیصه member گروه را به طور مناسب به روز رسانی می‌کند.

نقش PDC Emulator

این نقش عملیاتی چندگانه و حیاتی را برای دامنه بازی می‌کند:

- **یک DC اولیه یا PDC را به منظور سازگاری با تکنولوژی‌های قدیمی شبیه‌سازی می‌کند** در زمان دامنه ویندوز NT 4.0 فقط PDC می‌توانست روی دایرکتوری تغییر ایجاد کند. ابزارها و کلاینت‌های قدیمی که برای پشتیبانی از ویندوز NT 4.0 نوشته شده از این مساله غافل هستند که همه DC ها به صورت بالقوه توانایی تغییر روی دایرکتوری را دارند. بنابراین این ابزارها برای این کار از PDC کمک می‌گیرند. DC با نقش PDC Emulator خود را به عنوان یک PDC ثبت می‌کند به طوری که برنامه‌های سطح پایین بتوانند DC قابل تغییر را محل‌یابی کنند. حالا که Active Directory ۱۰ ساله شده چنین برنامه‌هایی رواج خود را از دست داده‌اند و اگر سازمان ما دارای چنین برنامه‌هایی باشد باید آنها را به سوی سازگاری بیشتر با Active Directory سوق دهیم.

- **در پروسه به روز رسانی کلمات عبور در دامنه شرکت می‌کند** وقتی کلمه عبور کاربری تغییر می‌کند DC که تغییر روی آن ایجاد شده تغییر را به PDC emulator تکثیر می‌کند. این کار باعث می‌شود همه DC ها متوجه تغییر کلمه عبور بشوند. اگر کاربری درست پس از تغییر کلمه عبور برای ورود تلاش کند ممکن است DC دریافت کننده درخواست ورود هنوز از تغییر کلمه عبور اطلاع حاصل نکرده باشد. بنابراین قبل از اینکه درخواست را رد کند آنرا به PDC emulator ارسال می‌کند. این یعنی هر بار که کاربر کلمه عبور خود را اشتباه وارد می‌کند کار تایید هویت به PDC emulator واگذار می‌شود. بنابراین این سرور باید حتما در دسترس بوده و دارای ارتباط با پهنای باند بالا باشد.

- **آپدیت‌های Group Policy را در دامنه مدیریت می‌کند** اگر یک GPO روی دو DC تقریبا همزمان تغییر یابد بین دو نسخه تداخل پیش می‌آید. برای جلوگیری از این وضعیت PDC emulator به عنوان نقطه مرکزی برای همه تغییرات GPO عمل می‌کند. وقتی ما یک GPO را در GPME باز می‌کنیم کنسول به PDC emulator متصل می‌شود. بنابراین به طور پیش فرض همه تغییرات GPO روی PDC emulator ایجاد می‌شود.

- **یک منبع زمانی مرکزی برای دامنه فراهم می‌کند** Active Directory، Kerberos، File Replication Services (FRS) و DFS-R به برچسب زمان (timestamp) متکی هستند بنابراین یکسان سازی زمان در کل سیستم‌های دامنه یک امر حیاتی به حساب می‌آید. به طور پیش‌فرض PDC emulator در دامنه ریشه forest منبع زمان برای کل forest می‌باشد. PDC emulator در هر دامنه زمان خود را با PDC emulator ریشه forest یکسان می‌کند و DC های دیگر در دامنه ساعت‌شان را با همین PDC emulator دامنه خود یکسان می‌کنند. این ساختار سلسله مراتبی یکسان‌سازی زمان توسط سرویس Win32Time پیاده‌سازی می‌شود. Universal Time Coordinate (UTC) هماهنگ شده و زمان نمایش داده شده به کاربران بر اساس تنظیمات time zone کامپیوتر میزان می‌شود.

- **به عنوان مرورگر مرکزی دامنه عمل می‌کند** وقتی پنجره Network in Windows را باز می‌کنیم لیستی از دامنه‌ها و شبکه‌های نظیر به نظیر را می‌بینیم و وقتی یکی از آنها را باز می‌کنیم لیستی از کامپیوترها را می‌بینیم. این دو لیست که لیست مرور نام دارند توسط سرویس Browser ایجاد می‌شوند. در هر بخش (segment) شبکه مرورگر مرکزی است که این لیست را می‌سازد. مرورگر مرکزی دامنه به منظور ترکیب لیست‌های هر مرورگر مرکزی به کار می رود به طوری که کلاینت‌ها بتوانند لیست کاملی را به دست آورند.

پیدا کردن Operation Masters

وقتی دامنه ریشه forest را با اولین DC می‌سازیم همه پنج نقش operations master توسط DC اجرا می‌شود. پس از افزودن DC های جدید به دامنه می‌توانیم این نقش را به آنها محول کنیم تا بین DC ها تقسیم بار صورت گیرد یا محل master operation منفرد را بهینه کنیم. بهترین روش برای جانمایی operations master در زیر شرح داده می‌شود:

- **جانمایی schema master و domain naming master در یک محل** این دو نقش بهتر است روی یک DC منفرد که GC است قرار گیرند. این نقش‌ها به ندرت استفاده می‌شوند و DC نگهدارنده آنها باید کاملا امن باشد. نقش domain naming master باید روی GC باشد به دلیل اینکه هنگام افزودن دامنه جدید master باید مطمئن شود که هیچ شیءی از هیچ نوعی با همان نام در دامنه وجود ندارد. Partial replica مربوط به GC حاوی نام همه اشیاء forest می‌باشد. بار کاری این نقش operation master خیلی کم است مگراینکه تغییرات schema صورت بگیرد.

- **جانمایی نقش‌های RID master و PDC Emulator در یک محل** نقش‌های RID و PDC Emulator را روی یک DC منفرد قرار می‌دهیم. اگر بار کاری بالا باشد و مجبور شویم آنها را روی دو DC مجزا قرار دهیم این دو سیستم باید از لحاظ فیزیکی ارتباط خوبی داشته باشند و اشیاء ارتباطی در Active Directory مناسب باشد به طوری که این دو سیستم به طور مستقیم روی هم تکثیر شوند. همچنین باید با DC که برای operations master پشتیبان انتخاب کرده‌ایم این شرایط را داشته باشند.

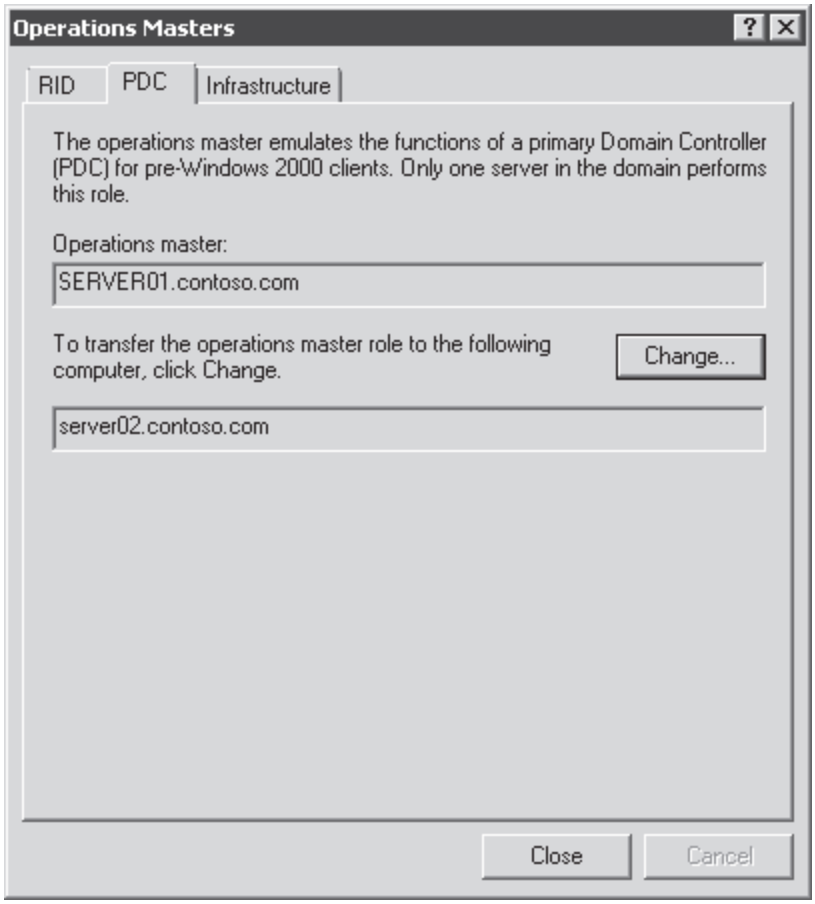
- **جانمایی Infrastructured master روی یک DC که GC نیست** باید infrastructre master روی DC نصب شود که از لحاظ فیزیکی ارتباط خوبی با سرور GC داشته باشد و اشیاء ارتباطی در Active Directory مناسب پیکربندی شده باشد به طوری که این دو به طور مستقیم روی هم تکثیر شوند و روی همان DC قرار گیرد که به عنوان RID master و PDC emulator عمل می‌کند.

- **برنامه پیش‌بینانه داشته باشیم** در بخش‌های بعدی یاد می‌گیریم نقش‌های operations master منفرد را بین DC ها منتقل کنیم که زمان زیادی این نقش‌ها از کار می‌افتند. بهتر است برای انتقال نقش‌ها برنامه‌ای را طراحی کنیم که این کار در زمان خروج یک operations master از شبکه انجام شود.

تشخیص Operations Masters

برای پیاده‌سازی طرح جانمایی نقش، باید بدانیم کدام DC ها نقش‌های master operations منفرد را بازی می‌کنند. هر نقشی در administrative tool سیستم یا ابزارهای رابط کاربری و خط فرمان قابل مشاهده است. برای تشخیص master فعلی هر نقش از ابزارهای زیر استفاده می‌کنیم:

- **PDC Emulator: ابزار Active Directory Users And Computers** روی دامنه کلیک راست کرده و Operations Masters را انتخاب می‌کنیم. زبانه PDC را باز می‌کنیم. مثالی از این دست در شکل ۲- ۱۰ مشاهده می‌شود که نشان می‌دهد SERVER01.contoso.com در حال حاضر PDC operations master می‌باشد.



شکل ۲- ۱۰ PDC Operations Master

- **RID Master**: **ابزار Active Directory Users And Computers** روی دامنه کلیک راست کرده و Operations Masters را انتخاب می‌کنیم. زبانه RID را باز می‌کنیم.
- **Infrastructure Master**: **ابزار Active Directory Users And Computers** روی دامنه کلیک راست کرده و Operations Master را انتخاب می‌کنیم. زبانه Infrastructure را باز می‌کنیم.
- **Domain Naming**: **ابزار Active Directory Domain And Trusts** روی گره ریشه کلیک راست کرده و Operations Master را انتخاب می‌کنیم.
- **Schema Master**: **ابزار Active Directory Schema** روی گره ریشه کلیک راست کرده و Operations Master را انتخاب می‌کنیم.

نکته ثبت ابزار Active Directory Schema

قبل از ساخت MMC باید ابزار را ثبت کنیم. برای این کار دستور regsrv32 schmmgmt.dll را اجرا می‌کنیم.

ابزارهای متعدد دیگری نیز هستند که برای تشخیص operations master استفاده می‌شوند که دستورات زیر نمونه آن است:

Ntdsutil
Roles
Connections
Connect to server DomainControllerFQDN:portnumber
Quit

Select operation target
List roles for connected server”
Quit
Quit
Quit
Dcdiag /test:knowsofroleholders /v
Netdom query fsmo

انتقال نقش‌های Operations Master

انتقال یک نقش operations master منفرد به سادگی صورت می‌گیرد. ما می‌توانیم نقش‌ها را به دلایل زیر منتقل کنیم:

- وقتی forest ساخته شد همه پنج نقش توسط DC اول اجرا می‌شود. زمانی که دامنه دیگری اضافه می‌کنیم همه نقش‌های دامنه توسط اولین DC دامنه اجرا می‌شود. پس از افزودن DC های دیگر می‌توانیم نقش‌ها را به منظور کاهش تمرکز توزیع کرده و کارایی را ارتقا دهیم.

- اگر بخواهیم یک DC را به صورت آفلاین داشته باشیم که دارای نقش operations master باشد قبل از خروج آن نقش مورد نظر را به DC دیگری منتقل می‌کنیم.

- اگر بخواهیم یک DC را که دارای نقش operations master است از رده خارج کنیم نقش آن را به DC دیگری واگذار می‌کنیم. ویزارد نصب DC این کار را به طور اتوماتیک انجام می‌دهد ولی باید قبلا نقش‌ها را منتقل کرده باشیم.

برای انتقال نقش operations master مراحل زیر را دنبال می‌کنیم:

۱. ابزار نمایش دهنده نقش را باز می‌کنیم.

۲. به DC که نقش منتقل خواهد شد متصل می‌شویم. این کار با کلیک راست روی گره ریشه ابزار و انتخاب Change Domain Controller یا Change Active Directory Domain Controller انجام می‌شود. (گزینه در ابزارهای مختلف متفاوت است.)

۳. کادر محاوره‌ای operations master را باز می‌کنیم. این کادر DC دارای نقش برای آن عملیات را داراست. روی دکمه Change کلیک می‌کنیم تا نقش به DC که به آن متصل شدیم منتقل شود.

هنگامی که یک نقش operations master را منتقل می‌کنیم هر دو master قبلی و جدید در دسترس خواهند بود. توکن منتقل می‌شود و master جدید فورا شروع به اجرای نقش می‌کند و master قبلی از اجرای نقش بازمی‌ایستد. این روش انتقال نقش‌های operations master بر بقیه ارجحیت دارد.
پیشنهاد می‌گردد از به روز بودن master جدید با استفاده از تکثیر از روی master قبلی قبل از انتقال نقش اطمینان حاصل نماییم. در فصل ۱۱ روش‌هایی برای تکثیر اجباری بین دو سیستم معرفی می‌شود.

تشخیص خطای operations master

برخی نقش‌های operations master ممکن مدتی غیرقابل دسترس باشند ولی غیبت آنها به چشم نیاید. نقش‌هایی هم هستند که نقش حیاتی را در عملیات روزمره شبکه دارند. بررسی Directory Service event log به ما در تشخیص مشکل operations master کمک می‌کند.
بهرحال اغلب هنگام اجرای یک عملیات تحت مدیریت master که به خطا منجر می‌شود متوجه می‌شویم که operations master با مشکل مواجه شده است. برای مثال زمانی که RID master مشکل داشته باشد نمی‌توانیم واحد امنیتی جدید بسازیم.

تصرف (Seizing) نقش‌های operations master

اگر یک DC که مجری یک نقش master منفرد است از دسترس خارج شود و توانایی برگرداندن آن نیز موجود نباشد چاره در تصرف توکن operations می‌باشد. وقتی یک نقش را تصرف می‌کنیم یعنی master جدید را بدون حذف نقش از master قبلی برمی‌گزینیم.

تصرف نقش عملی جدی است بنابراین قبل از این کار درباره نیاز به انجام آن مطمئن می‌شویم. ابتدا بررسی می‌کنیم که در چه مدت زمانی operations master در دسترس قرار خواهد گرفت. اگر operations master در مدت زمان مقتضی به شبکه برگردد بهتر است منتظر بمانیم تا اینکه نقشش را تصرف کنیم. ولی سوال این است چه مدت زمانی؟ این زمان بستگی به اهمیت آن نقش در شبکه دارد:

- خطای PDC emulator نبود این نقش بیشترین تاثیر را روی عملکرد طبیعی شبکه و کاربران خواهد داشت. خوشبختانه این نقش قابل تصرف توسط DC های دیگر بوه و در صورت برطرف شدن مشکل دوباره قابل برگشت به DC قبلی است

- خطای Infrastructure master خطای این نقش به مدیران شبکه برمی‌گردد تا کاربران. به دلیل اینکه این master مسئول به روز رسانی نام‌های اعضاء گروههای دامنه‌های دیگر است مشکل طوری بروز می‌کند مانند اینکه عضویت گروه غلط انجام شده است ولی در واقع عضویت تحت تاثیر این مشکل نیست. این نقش قابل تصرف به DC های دیگر است و پس از برطرف شدن مشکل می‌توان دوباره آنرا به DC قبلی برگرداند.

- خطای RID master این خطا سرانجام باعث می‌شود DC نتواند SID جدید بسازد و بنابراین نمی‌توانیم حساب کاربری، گروه یا کامپیوتر بسازیم. بهرحال DC ها هر بار حجم عظیمی از RID ها را از RID master دریافت می‌کنند بنابراین تا مدتی به master نیازی ندارند. تصرف این نقش توسط DC های دیگر عمل مهمی است چون DC قبلی مجری این نقش نمی‌تواند به دامنه باز گردد.

- خطای Schema master این نقش زمانی مورد نیاز است که تغییرات schema انجام می‌شود چه مستقیما توسط مدیر شبکه یا نصب برنامه عجین شده با Active Directory که باعث تغییر در schema می‌شود. در غیر این صورت به این نقش نیازی نداریم. تصرف این نقش توسط DC دیگر تصمیم مهمی است چون DC قبلی مجری این نقش نمی‌تواند به دامنه باز گردد.

- خطای Domain Naming master این نقش فقط زمانی مورد نیاز است که دامنه‌ای به forest اضافه یا از آن حذف می‌شود. تصرف این نقش توسط DC دیگر تصمیم مهمی است چون DC قبلی مجری این نقش نمی‌تواند به دامنه باز گردد.

انتقال این نقش‌ها از طریق administrative tools و تصرف آنها از طریق دستور Ntdsutil.exe صورت می‌گیرد.

برای تصرف یک نقش operations master مراحل زیر را انجام می‌دهیم:

۱. از طریق خط فرمان دستور ntdsutil را اجرا می‌کنیم.

۲. سپس roles را تایپ کرده و دکمه Enter را می‌زنیم. ارتباط با DC که می‌خواهیم نقش master operation منفرد را بازی کند برقرار می‌شود.

۳. در خط فرمان دستور connections را اجرا می‌کنیم.

۴. در خط فرمان عبارت connect to server DomainControllerFQDN را تایپ و دکمه Enter را می‌زنیم. سیستم جواب می‌دهد که ارتباط با سرور برقرار شده است.

۵. در خط فرمان دستور quit را صادر می‌کنیم.

۶. در خط فرمان دستور seize role را صادر می‌کنیم. Role یکی از نقش‌های زیر است:

a. Schema master

b. Domain naming master

c. RID master

d. PDC

e. Infrastructure master

۷. در خط فرمان دستور quit را دو بار صادر می‌کنیم.

بازگرداندن یک نقش به صاحب اصلی خود

به منظور آماده‌سازی شرایط برای خروج موقت یک DC از دامنه اگر نقش منتقل شده باشد نه تصرف امکان برگرداندن آن به صاحب قبلی وجود دارد.

اگر نقشی تصرف شده باشد و master قبلی آماده برگشت به دامنه باشد باید خیلی احتیاط کرد. نقش‌های PDC emulator و infrastructure تنها operations master هایی هستند که قابل برگشت به صاحب قبلی هستند.

نکته نقش‌های تصرف شده schema، domain naming و RID master نباید بازگردند.

DC هایی که نقش‌های schema، domain naming و RID master آنها تصرف می‌شود باید به طور کامل از شبکه حذف شوند.

وقتی نقش‌های schema، domain naming و RID master تصرف می‌شود باید نقش AD DS مربوط به DC قبلی را که نقش را از دست داده قبل از اتصال به شبکه با دستور Dcpromo /forceremoval پاک شود. همچنین باید متاداده DC را نیز به طور دستی پاک کنیم.

وقتی DC به طور کامل از روی Active Directory پاک شد می‌توانیم آنرا دوباره به دامنه join کنیم. همچنین اگر بخواهیم می‌توانیم آنرا دوباره به عنوان یک DC تعریف کنیم. اگر تصمیم بگیریم دوباره نقش operation master قبلی را بازی کند باید نقش را به آن منتقل کنیم.

نکته به دلیل حیاتی بودن نقش DC پیشنهاد می‌شود DC قبلی را از ابتدا به طور کامل نصب کنیم.

تمرینات جابجایی نقش Operations Master

در این تمرینات نقش Operations Masters در دامنه contoso.com را شناسایی کرده و برای خارج کردن operations master کنونی از دامنه جهت تعمیرات این نقش را به یک DC دیگر در دامنه انتقال می دهیم. برای انجام تمرین شماره ۲ باید تمرین درس اول را انجام داده و یک DC با نام SERVER02 در دامنه داشته باشیم.

تمرین اول: شناسایی operations masters

در این تمرین با هر دو ابزار رابط کاربر و خط فرمان جهت شناسایی operations masters در دامنه contoso.com آشنا می شویم

۱- با اعتبار Administrator وارد SERVER01 می شویم
۲- ابزار Active Directory Users And Computers را باز می کنیم
۳- روی دامنه contoso.com راست کلیک کرده و Operations Masters را انتخاب می کنیم
۴- روی زبانه مربوط به هرکدام از Operations Master ها کلیک می کنیم. زبانه ها نشان دهنده DC هایی هستند که در حال حاظر نقش Operations Master را برای هرکدام از نقشهای PDC emulator، RID master و Infrastructure master در دامنه دارند
۵- روی close کلیک کنید
۶- ابزار Active Directory Domains And Trustsرا باز می کنیم
۷- روی گره ریشه ابزار راست کلیک کرده و از با انتخاب Active Directory Domains And Trusts ، Operations Master را انتخاب می کنیم. کادر محاوره ای که باز می شود نام DCای که به عنوان domain naming master در دامنه عمل می کند را مشخص می کند
۸- روی close کلیک می کنیم.
ابزار Active Directory Schema کنسول جداگانه ای ندارد و تا زمانی که ابزار آن register نشود نمی توان آنرا به یک کنسول سفارشی اضافه کرد
۹- پنجره خط فرمان را باز کرده و عبارت regsvr32 schmmgmt.dll را در آن تایپ می کنیم. سپس Enter را فشار می دهیم
۱۰- برای بستن پنجره ای که باز می شود، روی ok کلیک می کنیم
۱۱- منوی استارت را باز کرده و در کادر جستجوی منوی استارت عبارت mmc.exe را تایپ کرده و Enter را فشار می دهیم
۱۲- از منوی فایل گزینه Add/Remove Snap-In را انتخاب می کنیم
۱۳- از لیست ابزارهای موجود، Active Directory Schema را انتخاب کرده و روی Addو بعد از آن OK کلیک می کنیم
۱۴- روی گره ریشه ابزار راست کلیک کرده و با انتخاب Active Directory Schema ، choose Operations Master را انتخاب می کنیم. پنجره ای که باز می شود مشخص کننده DC ای است که در حال حاظر نقش schema master را دارا می باشد
۱۵- روی Close کلیک می کنیم
۱۶- یک پنجره خط فرمان باز می کنیم و دستور netdom query fsmo را در آن تایپ کرده و Enter را فشار می دهیم . تمامی operations master ها لیست می شوند

تمرین دوم: انتقال یک نقش Operations Master
در این تمرین آماده می شویم تا یک Operations Master را بعد از انتقال نقشش به یک DC دیگر، از دامنه خارج کنیم سپس بصورت مجازی آن را از دامنه خارج می کنیم و مجدد آن را به دامنه متصل کرده و نقش Operations Master را به آن باز می گردانیم
۱- ابزار Active Directory Users And Computersرا باز می کنیم
۲- روی دامنه contoso.com راست کلیک کرده و گزینه Change Domain Controller را انتخاب می کنیم
۳- در لیست directory servers ، server02.contoso.com را انتخاب کرده و روی OK کلیک می کنیم. قبل از انتقال یک operations master باید DC را به دیگر DC که این نقش به آن انتقال خواهد یافت متصل کنیم. گره ریشه ابزار ، DC ای را که به آن متصل هستیم مشخص می کند: Active Directory Users And Computers [server02.contoso.com]
۴- روی دامنه contoso.com راست کلیک کرده و گزینه Operations Masters را انتخاب می کنیم

۵- روی زبانه PDC کلیک می کنیم. این زبانه نام SERVER01.contoso.com را نشان می دهد که در حال حاظر دارای این نقش است. SERVER02.contoso.com مانند شکل ۲-۱۰ ، در کادر محاوره ای دوم لیست شده است.

۶- روی دکمه Change کلیک می کنیم. کادر محاوره ای Active Directory Domain Services از ما می خواهد که انتقال را تایید کنیم

۷- روی Yes کلیک می کنیم. یک کادر محاوره ای Active Directory Domain Services تایید می کند که انتقال نقش با موفقیت انجام شد

۸- روی OK و سپس Close کلیک می کنیم

۹- با خاموش کردن SERVER01 آنرا بصورت مجازی از دامنه جدا می کنیم

۱۰- با روشن کردن SERVER01 آنرا مجددا به دامنه وصل می کنیم. باید به خاطر داشت که نمی توان یک DC را مجددا به دامنه اضافه کرد اگر که نقش های RID ، schema یا domain naming ، تصرف شده باشند. تنها در صورتی می توان این کار را انجام داد که این نقش ها منتقل شده باشند.

۱۱- مراحل ۱ تا ۸ را مجددا انجام می دهیم ، اینبار به SERVER01 متصل می شویم و نقش operations master را مجددا به SERVER01 انتقال می دهیم

خلاصه درس

- نقشهای Operations master به یک DC اختصاص داده می شوند تا یک عملیات خاص توسط آن DC انجام شود
- پنج نقش Operations master وجود دارد که دوتای آنها در سطح forest هستند: schema و domain naming . و سه نقش دیگر یعنی RID، PDC Emulator و infrastructure نیز در سطح دامنه می باشند
- DC ای که نقش infrastructure master را می پذیرد نمی تواند GC باشد مگر اینکه تمامی DCها در دامنه ، سرور GC باشند
- می توان نقشهای Operations master را از طریق ابزار ویندوز یا *Ntdsutil.exe جابجا کرد. جابجایی نقشها روش موثری در مدیریت آنها می باشد*
- می توان با استفاده از *Ntdsutil.exe یک نقش را تصرف کرد. این کار باید زمانی انجام شود که سروری که نگهدارنده این نقش است در زمان مناسب نتواند مجددا به کار ادامه دهد. تنها دو نقش* PDC Emulator و infrastructure می توانند بعد از تصرف شدن مجددا به نگهدارنده اصلی خود برگردانده شوند. سرورهایی که نقش schema ، RID یا domain naming را داشته اند بعد از تصرف کردن باید برای همیشه از رده خارج شوند

سئوالات پایان درس

۱- به عنوان مدیر شبکه در شرکت Contoso مشغول به کار هستیم. دامنه *contoso.com دارای دو سایت در دفاتر مرکزی می باشد. یک DC با نام* SERVER01 علاوه بر GC بودن دارای هر پنج نقش operations master می باشد. نام DC دوم دفاتر مرکزی SERVER02 می باشد. SERVER02 علاوه بر اینکه GC نمی باشد دارای هیچکدام از پنج نقش operations master را نیز ندارد. در یکی از شعبه های شرکت یک DC با نام SERVER03 وجود دارد که GC می باشد. چه تغییری در جایگاه نقش های operations master باید اعمال کنیم؟

A . نقش infrastructure master را به SERVER03 انتقال می دهیم

B . نقش RID master را به SERVER02 انتقال می دهیم

C . نقش schema master را به SERVER02 انتقال می دهیم

D . نقش domain naming master را به SERVER03 انتقال می دهیم

E . نقش infrastructure master را به SERVER02 انتقال می دهیم

۲- به عنوان مدیر شبکه در شرکت Contoso مشغول به کار هستیم. Forest ما دارای دو دامنه می باشد: *contoso.com و windows.contoso.com در حال حاضر* SERVER02.windows.contoso.com دارای هر

پنج نقش operations master می باشد. تصمیم داریم دامنه *windows.contoso.com را از رده خارج و تمام حساب ها را به دامنه contoso.com منتقل کنیممی خواهیم تمامی* operations master ها را به SERVER01.contoso.com منتقل کنیم. کدام یک را باید منتقل کنیم؟(در صورت نیازتمام گزینه های درست را انتخاب کنید)

A . Infrastructure master

B . PDC emulator

C . RID master

D . Schema master

E . Domain naming master

۳- عنوان مدیر شبکه در شرکت Contoso مشغول به کار هستیم. دامنه *contoso.com دارای* پنج DC می باشد می خواهیم تمام نقشهای operations master در سطح دامنه را به SERVER02.contoso.com منتقل کنیم. کدامیک را باید منتقل کنیم؟؟(در صورت نیازتمام گزینه های درست را انتخاب کنید)

A . Infrastructure master

B . PDC emulator

C . RID master

D . Schema master

E . Domain naming master

درس ۳: پیکربندی تکثیر DFS برای SYSVOL

SYSVOL فولدری به طور پیش‌فرض در مسیر %SystemRoot%\SYSVOL می‌باشد که که حاوی اسکریپت‌های زمان ورود، الگوهای group policy (GPT) و دیگر منابع حیاتی برای مدیریت دامنه می‌باشد. اگر ایده‌آل به آن نگاه کنیم بهتر است SYSVOL در DC کاملا ثابت باشد. ولی به هرحال هر لحظه اسکریپت‌ها و اشیاء group policy در حال تغییر هستند بنابراین باید اطمینان حاصل کنیم که این تغییرات به طور موثر و کارا به همه DC ها تکثیر می‌شود. در ویندوزهای قدیمی FRS برای تکثیر محتوای SYSVOL بین DC ها استفاده می‌شد. FRS هم در ظرفیت و هم کارایی محدودیت‌هایی دارد که باعث شکست ناگهانی آن می‌شود. متاسفانه عیب‌یابی و پیکربندی FRS خیلی مشکل است. در دامنه ویندوز سرور 2008 امکان استفاده از DFS-R به منظور تکثیر محتویات SYSVOL فراهم شده است. در این درس یاد می‌گیریم چطور SYSVOL را از FRS به DFS-R ارتقا دهیم.

بعد از این درس یاد می‌گیریم:

- سطح عملیاتی دامنه را بالا ببریم.
- تکثیر SYSVOL را از FRS به DFS-R ارتقا دهیم.

زمان تقریبی : ۶۰ دقیقه

بالا بردن سطح عملیاتی دامنه

در فصل ۱۲ درباره سطوح عملیاتی دامنه و forest یاد می‌گیریم. سطح عملیاتی دامنه تنظیمی است که هم سیستم عامل DC را در دامنه محدود می‌کند و هم آنرا قادر به اجرای عملیات بیشتر در Active Directory می‌کند. یک دامنه با DC ویندوز سرور 2008 در یکی از سه سطح عملیاتی زیر می‌تواند باشد: Windows 2000 Native، Windows Server 2003 Native و Windows Server 2008. در دامنه با سطح عملیاتی Windows 2000 Native یک DC می‌تواند دارای ویندوز سرور 2000 یا 2003 باشد. در دامنه با سطح عملیاتی Windows 2003

Native یک DC می‌تواند دارای ویندوز سرور 2003 باشد. در دامنه با سطح عملیاتی Windows 2008 Native همه DC ها باید دارای ویندوز سرور 2008 باشند.

با ارتقا سطح عملیاتی قابلیت‌های جدید Active Directory افزایش می‌یابد. برای مثال می‌توانیم از DFS-R برای تکثیر SYSVOL استفاده کنیم. ارتقا همه DC ها به ویندوز سرور 2008 کافی نیست و باید سطح عملیاتی دامنه را نیز ارتقا دهیم. این کار با استفاده از Active Directory Domains and Trusts انجام می‌شود. روی دامنه کلیک راست کرده و Raise Domain Functional Level را انتخاب می‌کنیم. سپس Windows Server 2008 را انتخاب کرده و روی Raise کلیک می‌کنیم. پس از تنظیم سطح عملیاتی فوق دیگر نمی‌توانیم دامنه‌های دارای سیستم عامل ویندوز سرور 2003 یا 2000 را در دامنه داشته باشیم. سطح عملیاتی فقط مربوط به سیستم عامل DC می‌شود و ربطی به سرورهای دیگر ندارد.

مراحل ارتقاء SYSVOL

به دلیل اینکه SYSVOL برای صحت و عملکرد مناسب شبکه حیاتی است ویندوز مکانیزمی برای تبدیل یکباره تکثیر SYSVOL از FRS به DFS-R ندارد. در حقیقت در مراحل ارتقاء یک ساختار موازی SYSVOL ایجاد می‌شود. وقتی این ساختار با موفقیت ایجاد شد کلاینت‌ها به سمت آن هدایت می‌شوند. بعد از اطمینان از صحت عملکرد ساختار جدید می‌توانیم FRS را حذف کنیم.

ارتقاء به DFS-R دارای چهار مرحله یا وضعیت است:

- **0 (شروع)** وضعیت پیش‌فرض DC است. فقط RFS برای تکثیر SYSVOL مورد استفاده قرار می‌گیرد.
- **1 (آماده‌سازی)** یک کپی از SYSVOL در پوشه‌ای با نام SYSVOL_DFSR تهیه و در بسته تکثیر قرار می‌گیرد. DFS-R کار تکثیر محتویات پوشه‌های SYSVOL_DFSR را روی همه DC ها شروع می‌کند. بهرحال FRS به تکثیر پوشه‌های SYSVOL اصلی نیز ادامه می‌دهد و کلاینت‌ها نیز از SYSVOL استفاده می‌کنند.
- **2 (تغییر مسیر)** محتویات SYSVOL که در اصل باید به مسیر SYSVOL\sysvol اشاره کند به مسیر SYSVOL_DFSR\sysvol اشاره می‌کند. کلاینت‌ها حالا از پوشه SYSVOL_DFSR برای دریافت اسکریپت‌های زمان ورود و الگوهای Group Policy استفاده می‌کنند.
- 3 (حذف) تکثیر پوشه SYSVOL قدیمی توسط FRS از کار می‌افتد. پوشه اصلی SYSVOL حذف نمی‌شود بنابراین باید دستی حذف گردد.

حالا DC ها را باید از طریق این مراحل و با استفاده از دستور Dfsmig.exe ارتقا دهیم. از سه انتخاب زیر به همراه دستور فوق می‌توانیم استفاده کنیم:

- **Setglobalstate state** این گزینه وضعیت ارتقاء global DFSR را پیکربندی می‌کند که روی همه DC ها اعمال می‌شود. وضعیت توسط پارامتر state مشخص می‌شود که از ۰ تا ۳ می‌تواند باشد. DC ها متوجه وضعیت جدید ارتقاء DFSR شده و وضعیت خود را به طور خودکار به آن تغییر می‌دهند.
- **Getglobalstate** این گزینه وضعیت فعلی ارتقاء DFSR را گزارش می‌دهد.

- **Getmigrationstate** این گزینه وضعیت فعلی ارتقاء هر DC را گزارش می‌دهد. به دلیل اینکه مطلع شدن DC ها از وضعیت ارتقاء global DFSR جدید زمان می‌برد و ممکن است زمانی نیز صرف ایجاد تغییر وضعیت شود یکسان‌سازی وضعیت DC ها با وضعیت global فوری انجام نمی‌شود. این گزینه ما را قادر به مانیتور کردن پیشرفت DC ها به سمت وضعیت فعلی ارتقاء golbal DFSR می‌کند.

اگر در انتقال از یک وضعیت به وضعیت اولی‌تر مشکلی پیش آید با استفاده از گزینه setglobalstate آنرا به حالت اولیه برمی‌گردانیم. بهرحال پس از استفاده از گزینه setglobalstate و پاسخ وضعیت ۳ ما نمی‌توانیم به وضعیت قبلی برگردیم.

ارتقاء تکثیر SYSVOL به DFS-R

برای ارتقاء تکثیر SYSVOL از FRS به DFS-R مراحل زیر را دنبال می‌کنیم:

۱. ابزار Active Directory Domains And Trusts را باز می‌کنیم.

۲. روی دامنه کلیک راست کرده و Raise Domain Functional Level را انتخاب می‌کنیم.

۳. اگر کادر Current Domain Functional Level عبارت Windows Server 2008 را نشان نمی‌داد این گزینه را از لیست Select An Available Domain Functional Level انتخاب می‌کنیم.

۴. روی Raise و دو بار روی OK کلیک می‌کنیم.

۵. به DC وارد شده و پنجره خط فرمان را باز می‌کنیم.

۶. دستور dfsrmig /setglobalstate 1 را اجرا می‌کنیم.

۷. دستور dfsrmig /getmigrationstate را برای دریافت میزان پیشرفت DC ها به سمت وضعیت **آماده سازی** اجرا می‌کنیم. این مرحله را تا دست یافتن همه DC ها به وضعیت تکرار می‌کنیم. این مرحله ۱۵ دقیقه تا ۱ ساعت یا حتی بیشتر طول می‌کشد.

۸. دستور dfsrmig /setglobalstate 2 را صادر می‌کنیم.

۹. دستور dfsrmig /getmigrationstate را برای دریافت میزان پیشرفت DC ها به سمت وضعیت **تغییر مسیر** اجرا می‌کنیم. این مرحله را تا دست یافتن همه DC ها به وضعیت تکرار می‌کنیم. این مرحله ۱۵ دقیقه تا ۱ ساعت یا حتی بیشتر طول می‌کشد.

۱۰. دستور dfsrmig /setglobalstate 3 را اجرا می‌کنیم. پس از شروع ارتقاء از وضعیت ۲ به ۳ همه تغییرات انجام شده روی پوشه SYSVOL باید به صورت دستی روی پوشه SYSVOL_DFSR تکثیر شود.

۱۱. دستور dfsrmig /getmigrationstate را برای دریافت میزان پیشرفت DC ها به سمت وضعیت **حذف** اجرا می‌کنیم. این مرحله را تا دست یافتن همه DC ها به وضعیت تکرار می‌کنیم. این مرحله ۱۵ دقیقه تا ۱ ساعت یا حتی بیشتر طول می‌کشد.

برای اطلاعات بیشتر درباره دستور dfsrmig.exe تایپ می‌کنیم : dfsrmig.exe /?

تمرینات پیکربندی DFS Replication of SYSVOL

در این تمرینات علاوه بر تکثیر SYSVOL مکانیسم انتقال از FRS به DFS-R را تجربه خواهیم کرد. سپس تکثیر SYSVOL به وسیله DFS-R را تایید خواهیم کرد. برای انجام دیگر تمرینهای این درس نیازمند سطح عملیاتی forest با سطح Windows Server 2008 هستیم. برای اجرای تمرینات نیاز به یک دامنه با سطح عملیاتی Windows Server 2003 داریم پس باید forest جدیدی بر مبنای سطح عملیاتی forest، Windows Server 2003 بسازیم که دارای یک دامنه با سطح عملیاتی Windows Server 2003 باشد که در آن دامنه دو DC موجود باشد. برای آماده شدن برای این تمرین ، مراحل زیر را انجام می دهیم:

- یک سرور با سیستم عامل ویندوز سرور 2008 با نام SERVER01 راه اندازی می کنیم که پیکر بندی آن به شکل زیر باشد:

  نام کامپیوتر: SERVER01

  عضویت گروه کاری: WORKGROUP

  آدرس IPv4 : 10.0.0.11

  Subnet Mask : 255.255.255.0

  Default Gateway : 10.0.0.1

  DNS Server : 10.0.0.11

- SERVER01 را به یک DC در forest جدیدی به نام contoso.com تبدیل می کنیم. سطح عملیاتی forest و سطح عملیاتی دامنه ویندوز سرور 2003 را انتخاب می کنیم، به ویزارد Active Directory Domain Services Installation اجازه می دهیم تا سرویس DNS را روی DC ما نصب کند. در صورت نیاز به راهنمایی از مراحل تمرین یکم درس اول از فصل یک کمک می گیریم. در هر صورت از انتخاب سطح عملیاتی forest و سطح عملیاتی دامنه ویندوز سرور 2003 مطمئن می شویم

- سرور دوم را با سیستم عامل ویندوز سرور 2008 و نام SERVER02 راه اندازی می کنیم. پیکربندی آن به صورت زیر خواهد بود:

  نام کامپیوتر: SERVER02

  عضویت : WORKGROUP

  آدرس IPv4 : 10.0.0.12

  Subnet Mask : 255.255.255.0

  Default Gateway : 10.0.0.1

  DNS Server : 10.0.0.11

- SERVER02 را به صورت additional DC در دامنه contoso.com راه اندازی می کنیم ، اما آنرا سرور DNS یا GC قرار نمی دهیم

تمرین اول تکثیر SYSVOL

در این تمرین تکثیر SYSVOL را بوسیله اضافه کردن یک اسکریپت به NETLOGON و مشاهده روند تکثیر در دیگر DC را تجربه خواهیم کرد

۱. با اعتبار Administrator وارد SERVER01 می شویم
۲. %SystemRoot%\Sysvol\Domain\Scripts را باز می کنیم
۳. یک فایل متنی جدید با نام **Sample Logon Script** درست می کنیم
۴. با اعتبار Administrator وارد SERVER02 می شویم
۵. %SystemRoot%\Sysvol\Domain\Scripts را باز می کنیم
۶. تکثیر فایل متنی را به پوشه Scripts از SERVER02 بررسی می کنیم

تمرین دوم آماده‌سازی برای ارتقا به DFS-R

پیش از آنکه بتوانیم تکثیر SYSVOL را به DFS-R ارتقا دهیم دامنه باید تنها شامل DCهایی از نوع ویندوز سرور 2008 باشد و سطح عملیاتی دامنه نیز به ویندوز سرور 2008 ارتقا یابد. در این تمرین تجربه خواهیم کرد که ارتقا DFS-R در دیگر سطوح عملیاتی دامنه غیر قابل انجام خواهد بود، همچنین ابزار مدیریت DFS را نیز نصب خواهیم کرد.

۱. در SERVER01 ابزار Active Directory Domains And Trusts را باز می کنیم
۲. روی دامنه contoso.com راست کلیک کرده و Raise Domain Functional Level را انتخاب می کنیم
۳. مطمئن می شویم که سطح عملیاتی دامنه کنونی در سطح ویندوز سرور 2003 است
۴. با زدن Cancel بدون ارتقا سطح عملیاتی دامنه ، کادر محاوره ای را می بندیم
۵. یک پنجره خط فرمان باز می کنیم
۶. عبارت **dfsrmig /getglobalstate را تایپ کرده و Enter را فشار می دهیم. پنجره ای ظاهر شده و به ما یاد آوری می کند که** *Dfsrmig تنها توسط دامنه هایی با سطح عملیاتی ویندوز سرور 2008 پشتیبانی می شود*
۷. ابزار Active Directory Domains And Trusts را باز می کنیم
۸. روی دامنه contoso.com راست کلیک کرده و Raise Domain Functional Level را انتخاب می کنیم
۹. سطح عملیاتی دامنه ویندوز سرور 2008 را انتخاب می کنیم
۱۰. روی دکمه Rasie کلیک کرده و برای تایید تغییرات روی OK کلیک می کنیم. پیامی مبنی بر موفقیت آمیز بودن ارتقا سطح عملیاتی دامنه ظاهر می شود
۱۱. روی OK کلیک می کنیم
۱۲. در پنجره خط فرمان عبارت **dfsrmig /getglobalstate را تایپ کرده و Enter را فشار می دهیم پنجره ای ظاهر می شود که به ما یادآوری می کند ارتقا DFSR هنوز** کامل نشده است

تمرین سوم ارتقا تکثیر **SYSVOL به DFS-R**

در این تمرین ، تکثیر **SYSVOL** را از FRS به DFS-R ارتقا می دهیم

۱. در SERVER01 ، یک پنجره خط فرمان باز می کنیم
۲. عبارت **dfsrmig /setglobalstate 0 را تایپ کرده و Enter را فشار می دهیم. پیغام زیر ظاهر می شود:**

Current DFSR global state: 'Start'
New DFSR global state: 'Start'
Invalid state change requested.

default global state در حال حاظر 0 می‌باشد پس دستور ما نامعتبر می باشد.

۳. عبارت **dfsrmig /getglobalstate را تایپ کرده و Enter** را فشار می دهیم . پیام زیر ظاهر می شود:

Current DFSR global state: 'Start' Succeeded

۴. عبارت **dfsrmig /getmigrationstate را تایپ کرده و Enter را فشار می دهیم**. پیام زیر ظاهر می شود:

All Domain Controllers have migrated successfully to Global state ('Start').
Migration has reached a consistent state on all Domain Controllers.
Succeeded.

۵. عبارت **dfsrmig /setglobalstate 1 را تایپ کرده و Enter را فشار می دهیم**. پیام زیر ظاهر می شود:

Current DFSR global state: 'Start'

New DFSR global state: 'Prepared'

Migration will proceed to 'Prepared' state. DFSR service will
copy the contents of SYSVOL to SYSVOL_DFSR
folder.

If any DC is unable to start migration then try manual polling.
OR Run with option /CreateGlobalObjects.
Migration can start anytime between 15 min to 1 hour.
Succeeded.

۶. عبارت **dfsrmig /getmigrationstate** را تایپ کرده و **Enter** را فشار می دهیم. پیغامی ظاهر می شود که روند ارتقا هر **DC** را منعکس می کند عملیات ارتقا ممکن است تا ۱۵ دقیقه طول بکشد. این مرحله را تا دریافت پیام زیر که حاکی از موفقیت آمیز بودن عملیات می باشد ادامه می دهیم:

All Domain Controllers have migrated successfully to Global state
('Prepared').
Migration has reached a consistent state on all Domain Controllers
Succeeded.

هنگامی که پیامی مشابه آنچه در بالا دیدیم را دریافت کردیم، کار را با مرحله ۷ ادامه می دهیم

ممکن است در زمان ارتقا به وضعیت 'Prepared' با یکی از پیامهای زیر مواجه شویم:

The following Domain Controllers are not in sync with Global state ('Prepared'):
Domain Controller (Local Migration State) - DC Type
==========
SERVER01 ('Start') - Primary DC
SERVER02 ('Start') - Writable DC
Migration has not yet reached a consistent state on all Domain Controllers.
State information might be stale due to AD latency.

یا

The following Domain Controllers are not in sync with Global state
('Prepared'):
Domain Controller (Local Migration State) - DC Type
==========
SERVER01 ('Start') - Primary DC
SERVER02 ('Waiting For Initial Sync') - Writable DC
Migration has not yet reached a consistent state on all Domain Controllers.
State information might be stale due to AD latency.

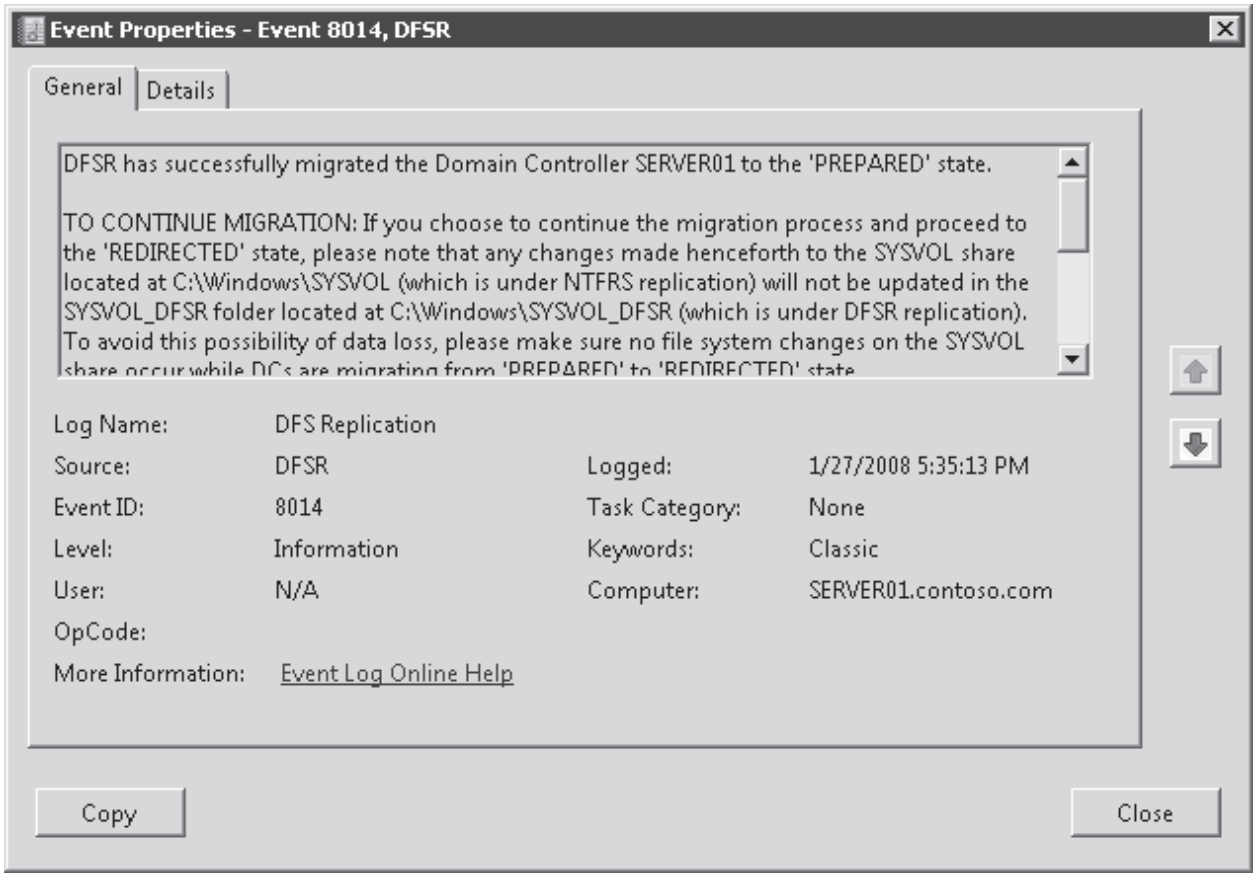
یا

The following Domain Controllers are not in sync with Global state
('Prepared'):
Domain Controller (Local Migration State) - DC Type
==========
SERVER02 ('Waiting For Initial Sync') - Writable DC
Migration has not yet reached a consistent state on all Domain Controllers.
State information might be stale due to AD latency.

۷. کنسول Event Viewer را از Administrative Tools باز می کنیم

۸. Applications And Services Logs را باز کرده و DFS Replication را انتخاب می کنیم

۹. واقعه‌ای با شماره 8014 را پیدا کرده و properties آن را باز می کنیم. جزئیاتی مانند شکل ۳-۱۰ را مشاهده خواهیم کرد



شکل ۳- ۱۰ واقعه DFS-R نشان‌دهنده ارتقاء موفقیت‌آمیز به وضعیت 'Prepared'

عبارت **dfsrmig /setglobalstate 2 را تایپ کرده و Enter را فشار می دهیم**. پیام زیر ظاهر می شود:

```
Current DFSR global state: 'Prepared'
New DFSR global state: 'Redirected'

Migration will proceed to 'Redirected' state. The SYSVOL share will be
changed to SYSVOL_DFSR folder.

If any changes have been made to the SYSVOL share during the state
transition from 'Prepared' to 'Redirected', please robocopy the changes
from SYSVOL to SYSVOL_DFSR on any replicated RWDC.
Succeeded.
```

۱۰. عبارت **dfsrmig /getmigrationstate را تایپ کرده و Enter را فشار می دهیم**. پیغامی ظاهر می شود که نشاندهنده سطح ارتقا هر کدام از DC ها می باشد. ارتقا ممکن است تا ۱۵ دقیقه هم طول بکشد این مرحله را آنقدر تکرار می کنیم تا پیام زیر که نشاندهنده ارتقا به سطح Prepared و موفقیت آمیز بودن آن می باشد، را دریافت کنیم:

```
All Domain Controllers have migrated successfully to Global state
('Redirected').
Migration has reached a consistent state on all Domain Controllers.
Succeeded.
```

هنگامی که پیام بالا را مشاهده کردیم کار را با مرحله ۱۲ ادامه می دهیم. در حین ارتقا ممکن است با پیغام زیر مواجه شویم:

```
Domain Controller (Local Migration State) - DC Type
============================================================
SERVER02 ('Prepared') - Writable DC
```

Migration has not yet reached a consistent state on all Domain Controllers.
State information might be stale due to AD latency

۱۱. عبارت **net share** را نوشته و **Enter** را فشار می دهیم

۱۲. **تایید می کنیم که** NETLOGON share به پوشه%SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts اشاره دارد

۱۳. **تایید می کنیم که** SYSVOL share به پوشه %SystemRoot%\SYSVOL_DFSR\Sysvol اشاره دارد

۱۴. **در Windows Explorer ، پوشه** %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts را باز می کنیم

۱۵. **بررسی می کنیم که فایل** Sample Logon Script به پوشه new Scripts منتقل شده است

۱۶. **یک فایل متنی جدید با نام Sample Logon Script DFSR درست می کنیم**

۱۷. **در SERVER02 ، بررسی می کنیم که فایل در پوشه** %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts **جایگزین شود**

خلاصه درس

- تا زمانی که دامنه در سطح عملیاتی دامنه ویندوز سرور 2008 نباشد نمی توان از DFS-R برای تکثیر SYSVOL استفاده کرد
- دستور Dfsrmig.exe برای مدیریت ارتقا از پوشه FRS-replicated SYSVOL به پوشه DFS-R replicated SYSVOL_DFSR استفاده می شود
- برای ارتقا چهار مرحله وجود دارد: Start ، Prepared ، Redirected و Eliminated . تا زمانی که به مرحله Eliminated نرسیده ایم میتوانیم به مرحله قبل برگردیم

سئوالات پایان درس

۱- به عنوان مدیر شبکه در موسسه Trey Research مشغول به کار هستیم. دامنه ما دارای سه DC می باشد، دوتا با سیستم عامل ویندوز سرور 2008 و یکی با سیستم عامل ویندوز سرور 2003 . دامنه ریشه forest دارای دو DC است که هر دو با سیستم عامل ویندوز سرور 2003 کار می کنند. می خواهیم در دامنه خودمان با استفاده از DFS-R ، SYSVOL را تکثیر کنیم. چه مراحلی باید انجام شود؟ ؟(در صورت نیازتمام گزینه های درست را انتخاب کنید. هر پاسخ صحیح بخشی از راه حل است)

A . ارتقا دادن DC های ریشه forest به ویندوز سرور 2008

B . تغییر سطح عملیاتی forest به ویندوز سرور 2008

C . ارتقا سیستم عامل DCدامنه خودمان از ویندوز سرور 2003 به ویندوز سرور 2008

D . ارتقا سطح عملیاتی دامنه خودمان به ویندوز سرور 2008

E . ارتقا سطح عملیاتی دامنه ریشه forest به ویندوز سرور 2008

۲- می خواهیم Active Directory را طوری پیکربندی کنیم که تکثیر logon scripts بوسیله DFS-R انجام شود. از چه دستوری استفاده می کنیم؟

A . *Dfsrmig.exe*

B . *Repadmin.exe*

C . *Dfsutil.exe*

D . *Dfscmd.exe*

فصل ۱۱

سایت و تکثیر

در فصل قبلی یاد گرفتیم که DC ها در یک دامنه ویندوز سرور 2008 نظیر هم هستند. هر کدام یک کپی از دایرکتوری را نگه می‌دارند، سرویس‌های مشابهی را به منظور تایید هویت واحدهای امنیتی ارائه می‌دهند و هر تغییری روی هر کدام از آنها روی بقیه تکثیر می‌شود. به عنوان مدیر یک شبکه مایکروسافتی یکی از وظایف ما فراهم کردن سرویس تایید هویت با کارایی بالا و تکثیر بهینه داده بین DC های شبکه است. سایت‌های AD DS جزء اصلی سرویس دایرکتوری است که اهداف بومی‌سازی سرویس و تکثیر را تامین می‌کند. در این فصل یاد می‌گیریم که چطور یک سرویس دایرکتوری توزیع‌شده بسازیم که DC ها را در بخش‌های مختلف شبکه را که با لینک‌های گران، کند یا ناپایدار از هم جدا شده‌اند پشتیبانی کند. یاد می‌گیریم که جای DC ها را تعیین کنیم و اینکه چطور عملیات تکثیر و استفاده سرویس را مدیریت کنیم. یاد می‌گیریم با پیکربندی GC و پارتیشن‌های برنامه چطور کنترل کنیم کدام داده به کدام DC تکثیر شود.

اهداف امتحانی در این فصل:

- پیکربندی زیرساخت Active Directory
  - پیکربندی global catalog (GC)
  - پیکربندی سایت‌ها
  - پیکربندی تکثیر Active Directory
- نگهداری Active Directory
  - مانیتور کردن Active Directory

دروس این فصل:

- درس ۱: پیکربندی سایت و زیرشبکه (subnet)
- درس ۲: پیکربندی Global Catalog و پارتیشن‌های دایرکتوری برنامه
- درس ۳: پیکربندی تکثیر

قبل از شروع

برای انجام تمرینات این فصل باید دو DC با نام‌های SERVER01 و SERVER02 در دامنه با نام contoso.com داشته باشیم. فصل ۱ را برای یادآوری جزئیات مرور کنید.

درس ۱: پیکربندی سایت و زیرشبکه

نماد انسان در سرویس دایرکتوری اشیاء کاربر و نماد کامپیوتر اشیاء کامپیوتر می‌باشد. نماد توپولوژی شبکه نیز اشیائی به نام سایت و زیرشبکه هستند. سایت‌ها برای مدیریت تکثیر و محلی‌سازی سرویس استفاده می‌شوند و خوشبختانه در بسیاری از شبکه‌ها پیکربندی سایت و زیرشبکه کاملا ساده و سرراست می‌باشد. در این درس مفاهیم اساسی و تکنیک‌های مورد نیاز پیکربندی و مدیریت سایت‌ها و زیرشبکه‌ها را یاد می‌گیریم.

بعد از این درس یاد می‌گیریم:

- نقش‌های سایت و زیرشبکه را مشخص تعریف کنیم.

- روندی که کلاینت DC را پیدا می‌کند شرح دهیم.
- سایت و زیرشبکه را پیکربندی کنیم.
- اشیاء سرور DC را در سایت مدیریت کنیم.

زمان تقریبی: ۴۵ دقیقه

مفهوم سایت

وقتی مدیران شبکه شبکه خود را توصیف می‌کنند اغلب به تعداد سایت‌ها اشاره می‌کنند. برای بیشتر مدیران شبکه سایت یک محل فیزیکی، یک دفتر یا شهر می‌باشد. سایت‌ها با لینک‌هایی بهم مرتبط هستند. این لینک‌ها گاهی ابتدایی مانند ارتباط dial-up و گاهی پیچیده مانند فیبر نوری است. محل فیزیکی و لینک‌ها زیرساخت شبکه را تشکیل می‌دهند.

Active Directory زیرساخت شبکه را با اشیائی به نام سایت و سایت لینک معرفی می‌کند. اگرچه واژه‌ها یکی هستند ولی معنی آنها با سایت و لینکی که مدیران شبکه می‌گویند فرق دارد. این درس روی سایت و درس ۳ روی سایت لینک تمرکز می‌کند.

دانستن نقش و خصوصیات سایت در Acive Directory ضروری است به دلیل اینکه تفاوت ظریف سایت Active Directory و سایت شبکه را انکانپذیر می‌کند. سایت در Active Directory شیئی است که در دایرکتوری موجود است و محل آن CN=Configuration,DC=forest root domain است. این اشیاء به منظور اجرای دو عملیات مدیریت سرویس به کار می‌رود.

- برای مدیریت ترافیک تکثیر
- برای تسهیل محلی کردن سرویس

ترافیک تکثیر

تکثیر یعنی انتقال تغییرات بین DC ها. برای مثال وقتی کاربری اضافه می‌شود یا کلمه عبورش تغییر می‌کند این تغییر در یکی از دایرکتوری‌ها ثبت می‌شود. این تغییر باید روی همه DC های دیگر در دامنه نیز اعمال شود.

Active Directory تایید می‌کند دو نوع شبکه در سازمان موجود است. شبکه با ارتباط قوی و ضعیف. هر نوع تغییری در Active Directory باید فورا روی DC های دیگر که با این DC ارتباط قوی دارد تکثیر شود. ولی ممکن است مایل نباشیم تغییر مذکور به سرعت روی لینک‌های کند و ضعیف به سمت سایت دیگری تکثیر شود و بخواهیم این تکثیر را مدیریت کنیم.

یک سایت Active Directory نمایانگر بخشی از شبکه می‌باشد که با شبکه سازمان ارتباط قوی دارد. وقتی سایت را تعریف می‌کنیم DC داخل سایت تغییرات را تقریبا فوری تکثیر می‌کند. تکثیر بین سایت‌ها می‌تواند زمان‌بندی شده و مدیریت شده باشد.

محلی‌سازی سرویس

Active Directory یک سرویس توزیع شده است. حداقل DC مورد نیاز دو دستگاه می‌باشد در حالی که DC های بیشماری که سرویس مشابه می‌دهند وجود دارند. اگر بیش از یک سایت شبکه داشته باشیم و در هر کدام یک DC قرار دهیم کلاینت‌ها برای سرویس تایید هویت به DC سایت خود متصل می‌شوند و این یعنی محلی‌سازی سرویس.

سایت‌ها به محلی‌سازی سرویس‌ها کمک می‌کنند که یکی از آنها سرویس‌های ارائه شده توسط DC می‌باشد. در زمان ورود به شبکه کلاینت‌ها مستقیما به DC سایت خود متصل می‌شوند. اگر DC سایت در دسترس نباشد به سمت یک DC دیگر در سایت‌های دیگر که قادر به تایید هویت است هدایت می‌شوند.

دیگر سرویس‌ها نیز امکان محلی شدن را دارند. برای مثال Distributed File System (DFS Namespaces) یک سرویس محلی است. کلاینت‌های DFS منابع تکثیرشده را از سرور با کارایی بالا بر اساس سایت Active Directory خود به دست می‌آورند. در حقیقت به دلیل اینکه کلاینت‌ها می‌دانند که در کدام سایت حضور دارند هر سرویسی می‌تواند از مزایای سایت برای محلی‌سازی خود استفاده کند.

طراحی سایت

به دلیل اینکه سایت‌ها به منظور بهینه‌سازی تکثیر و محلی‌سازی تکثیر مورد استفاده قرار می‌گیرند باید زمان کافی برای ایجاد ساختار مناسب سایت صرف کنیم. سایت‌های Active Directory ممکن است ممکن است بر سایت‌های فیزیکی شبکه منطبق نباشد.
سناریوهای زیر را در نظر بگیرید:

- دو دفتر در محل‌های مجزا داریم. یک DC را در هر محل قرار می‌دهیم. محل‌ها با لینک قوی بهم متصل هستند و برای ارتقاء کارایی تصمیم می‌گیریم برای هر دو محل فقط یک سایت در نظر بگیریم.

- شبکه سازمانی ما دارای ساختمان‌های جداست و پهنای باند بین آنها قوی است. از منظر تکثیر شبکه باید یک سایت داشته باشد. بهرحال می‌خواهیم کلاینت‌ها را مجبور کنیم از یک سرویس توزیع‌شده در محل خود استفاده کنند بنابراین برای پشتیبانی از محلی‌سازی سرویس چند سایت راه‌اندازی می‌کنیم.

بنابراین سایت Active Directory می‌تواند بیش از یک سایت فیزیکی شبکه را شامل شود یا زیر مجموعه‌ای از یک سایت فیزیکی شبکه منفرد باشد. نکته کلیدی این است که سایت‌ها هم به مدیریت تکثیر و هم به محلی‌سازی سرویس کمک می‌کنند. خصوصیات زیادی در شبکه می‌تواند ما را در انتخاب نوع سایت مورد نیاز کمک کند:

سرعت ارتباط

سایت یک واحد از شبکه است که ویژگی‌هایی از قبیل سرعت، قابلیت اعتماد و هزینه دارد. پیشنهاد می‌شود حداقل پهنای باند سایت 512 Kbps باشد. البته این مساله قطعیت ندارد و بعضی از سازمان‌ها لینک‌هایی با پهنای باند ۵۶ یا حتی ۲۸ دارند.

جایگاه سرویس

به دلیل اینکه سایت‌ها تکثیر و محلی‌سازی سرویس را مدیریت می‌کنند ساختن آنها در محلی که DC یا سرویس وابسته به DC ندارد مفید نیست.

نکته سایت‌هایی که DC ندارند

DC ها فقط یک سرویس توزیع شده در شبکه هستند. سرویس‌های دیگر مانند replicated DFS resources متکی به سایت هستند. ما ممکن است سایت‌ها را با هدف محلی‌سازی سرویس‌ها پیکربندی کنیم نه تایید هویت که در این موارد می‌توانیم سایت‌هایی بدون DC داشته باشیم.

جمعیت کاربران

کاربران نیز هر چند غیرمستقیم می‌تواند در طراحی سایت ما تاثیر داشته باشد. اگر یک محل در شبکه تعداد کاربران زیادی داشته باشد و تایید هویت با مشکل مواجه باشد قرار دادن یک DC در آن محل می‌تواند کارساز باشد. پس از اینکه DC یا سرویس دیگری در محل قرار گرفت می‌توانیم تکثیر را برای آن محل مدیریت کنیم یا با پیکربندی یک سایت سرویس را محلی کنیم.

خلاصه کردن شاخص‌های طراحی سایت

Forest حداقل دارای یک سایت است. سایت پیش‌فرض هنگام راه‌اندازی یک forest با اولین DC با نام Default-First-Site-Name ساخته می‌شود. ما هنگامی سایت‌های بعدی را ایجاد می‌کنیم که:

- بخشی از شبکه با یک لینک ضعیف جدا می‌شود.

- بخشی از شبکه دارای کاربران زیادی است.

- ترافیک درخواست ارتباط با دایرکتوری آنقدر زیاد است که ما را مجبور به نصب یک DC می‌کند.

- بخواهیم محلی‌سازی سرویس را کنترل کنیم.

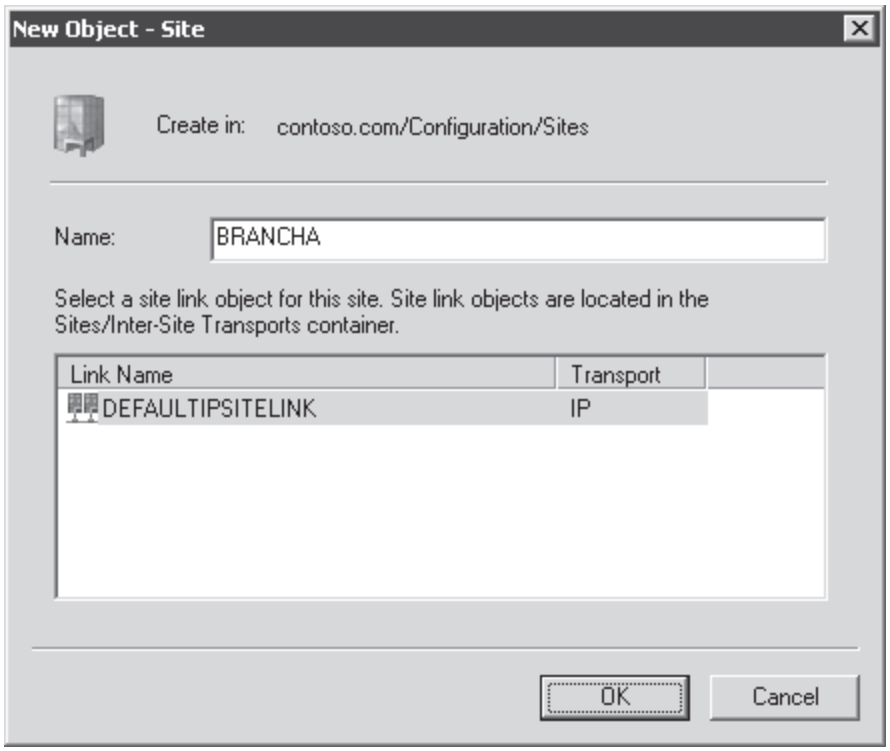
- بخواهیم تکثیر بین DC ها را کنترل کنیم.

تعریف سایت

سایت‌ها و عملیات تکثیر با استفاده از ابزار Active Directory Sites and Services مدیریت می‌شوند. برای تعریف یک سایت یک شیء از کلاس site می‌سازیم. شیء سایت یک container است که تکثیر را برای DC ها مدیریت می‌کند. همچنین یک یا چند شیء زیرشبکه می‌سازیم

شیء زیرشبکه بازه‌ای از آدرس‌های IP را تعریف می‌کند و به یک سایت لینک می‌شود. محلی‌سازی سرویس زمانی تحقق می‌یابد که آدرس IP کلاینت بتواند با سایت از طریق ارتباط بین شیء زیرشبکه و سایت عجین شود.

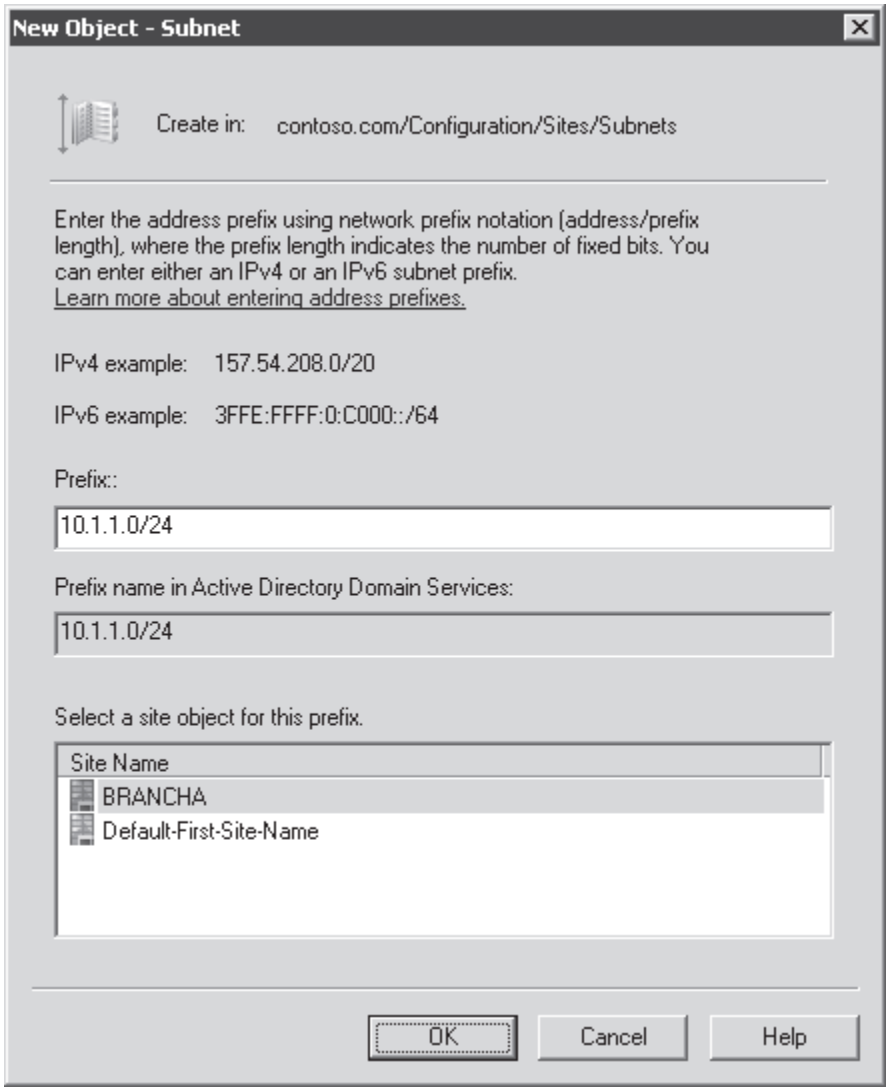
طریقه ساخت شیء سایت بدین صورت است که روی گره Sites در پنجره Active Directory Sites And Services کلیک راست کرده و New Site را انتخاب می‌کنیم. در کادر محاوره‌ای New Object – Site همانند شکل ۱- ۱۱ نام سایت را وارد کرده و یک سایت لینک را انتخاب می‌کنیم. سایت لینک پیش‌فرض DEFAULTIPSITELINK تنها سایت لینکی است که وجود دارد مگر اینکه سایت لینک‌های اضافی طبق روش‌های ارائه شده در درس ۲ همین فصل ایجاد شود.



شکل ۱- ۱۱ کادر محاوره‌ای New Object – Site

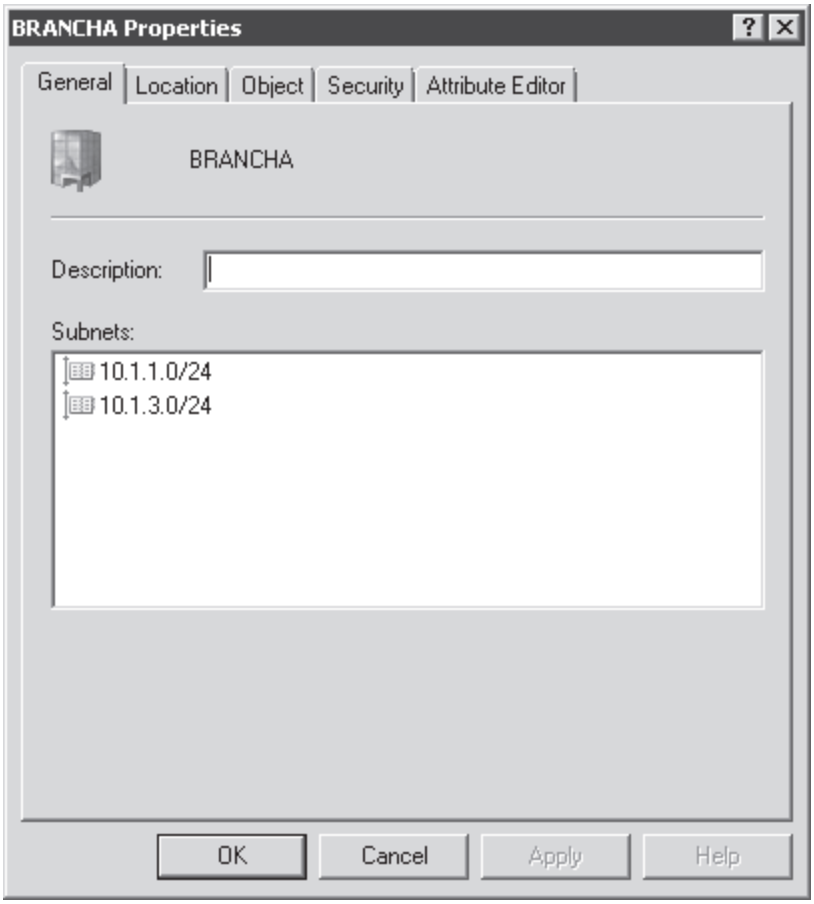
پس از ساخت سایت می‌توانیم روی آن کلیک راست کرده و با انتخاب Rename نام آنرا تغییر دهیم. پیشنهاد می‌شود نام سایت Default-First-Site-Name را به نام مناسب‌تری تغییر دهیم.

سایت زمانی می‌تواند مفید باشد که کلاینت‌ها و سرورها سایتی را که به آن تعلق دارند بشناسند. این کار با عجین شدن آدرس IP سیستم با یک سایت انجام می‌شود و اشیاء زیرشبکه این ارتباط را به دست می‌آورند. طریقه ساخت شیء زیرشبکه بدین صورت است که ابتدا روی گره Subnets در ابزار Active Directory Sites And Services کلیک راست کرده و New Subnet را انتخاب می‌کنیم. کادر محاوره‌ای New Object – Subnet همانند شکل ۲- ۱۱ ظاهر می‌شود. شیء زیرشبکه به عنوان بازه‌ای از آدرس‌ها به شکل پیشوند شبکه تعریف می‌شود. برای مثال برای ورود یک زیرشبکه نماینده آدرس‌های 10.1.1.1 تا 10.1.1.254 با ۲۴ بیت subnet mask پیشوند برابر خواهد بود با 10.1.1.0/24. برای اطلاعات بیشتر درباره ورود آدرس‌ها روی لینک Learn More About Entering Address Prefixes در کادر New Object – Subnet کلیک می‌کنیم.

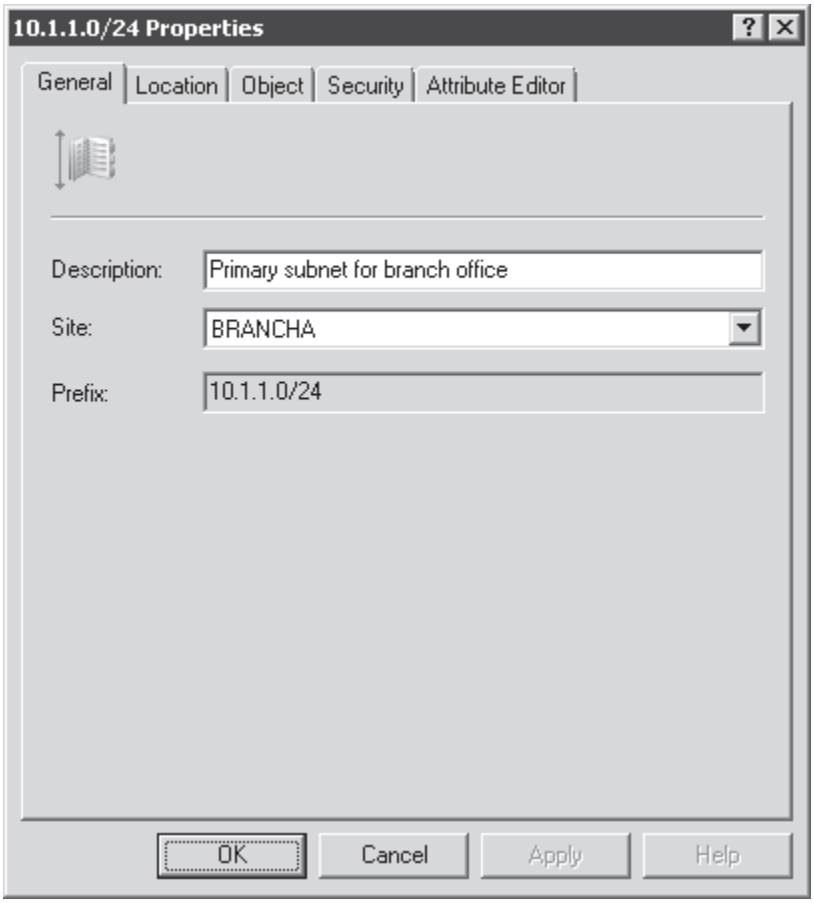


شکل ۲- ۱۱ کادر محاوره‌ای New Object – Subnet

پس از ورود پیشوند شبکه شیء سایتی را که زیرشبکه با آن عجین شده انتخاب می‌کنیم. یک زیرشبکه می‌تواند با تنها یک سایت عجین شود. ولی به یک سایت می‌تواند بیش از یک زیرشبکه لینک شود. کادر محاوره‌ای Properties یک سایت همانند شکل ۳- ۱۱ زیرشبکه‌های عجین شده با سایت را نشان می‌دهد. امکان تغییر زیرشبکه‌ها در این کادر وجود ندارد ولی می‌توان پنجره Properties زیرشبکه را باز کرده و همانند شکل ۴- ۱۱ سایتی را که زیرشبکه به آن لینک شده تغییر داد.



شکل ۳- ۱۱ کادر محاوره‌ای Properties یک سایت



شکل ۴- ۱۱ کادر محاوره‌ای Properties یک زیرشبکه

نکته تعریف تمام زیرشبکه‌های IP

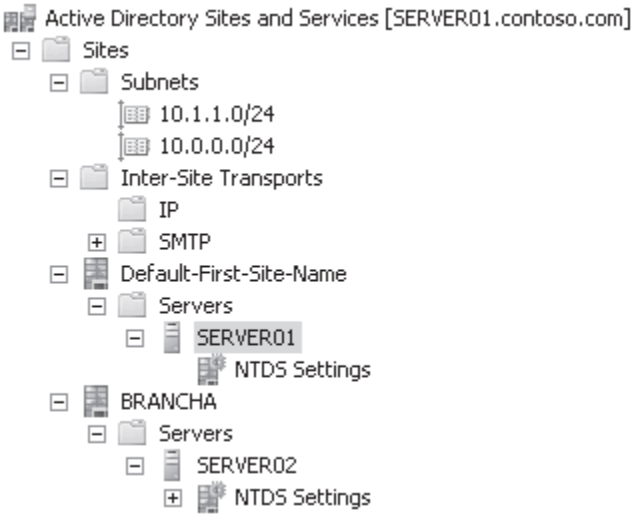
در محیط واقعی شبکه از تعریف زیرشبکه‌های IP به عنوان یک شیء زیرشبکه مطمئن می‌شویم. اگر آدرس IP یک کلاینت در هیچ محدوده زیرشبکه نباشد کلاینت نمی‌تواند تعیین کند به کدام سایت تعلق دارد. در نتیجه مشکلاتی در شبکه به وجود می‌آید.
زیرشبکه‌های Backbone و زیرشبکه‌های مورد استفاده دسترسی از راه دور مانند VPN را فراموش نکنید.

مدیریت DC ها در سایت‌ها

زمانهایی وجود دارد که نیاز به مدیریت DC ها در سایت‌های Active Directory داریم:

- وقتی سایت جدید می‌سازیم و DC موجود را به آن منتقل می‌کنیم.
- وقتی یک DC را demote می‌کنیم.
- وقتی یک DC را ایجاد می‌کنیم.

وقتی forest ایجاد می‌شود اولین DC به طور خودکار زیر شیء سایت با نام Default-First-Site-Name قرار می‌گیرد. DC با نام SERVER01.contoso.com در شکل ۵- ۱۱ قابل رویت است. Additional DC ها بر اساس آدرس‌های Ip شان به سایت‌ها اضافه می‌شوند. به عنوان مثال اگر سروری با آدرس 10.1.1.17 در شبکه نشان داده شده در شکل ۴- ۱۱ به DC ارتقا یابد به طور خودکار به سایت BRANCHA افزوده می‌شود. شکل ۵- ۱۱ SERVER02 را در سایت BRANCHA نشان می‌دهد.



شکل ۵- ۱۱ یک DC در یک سایت

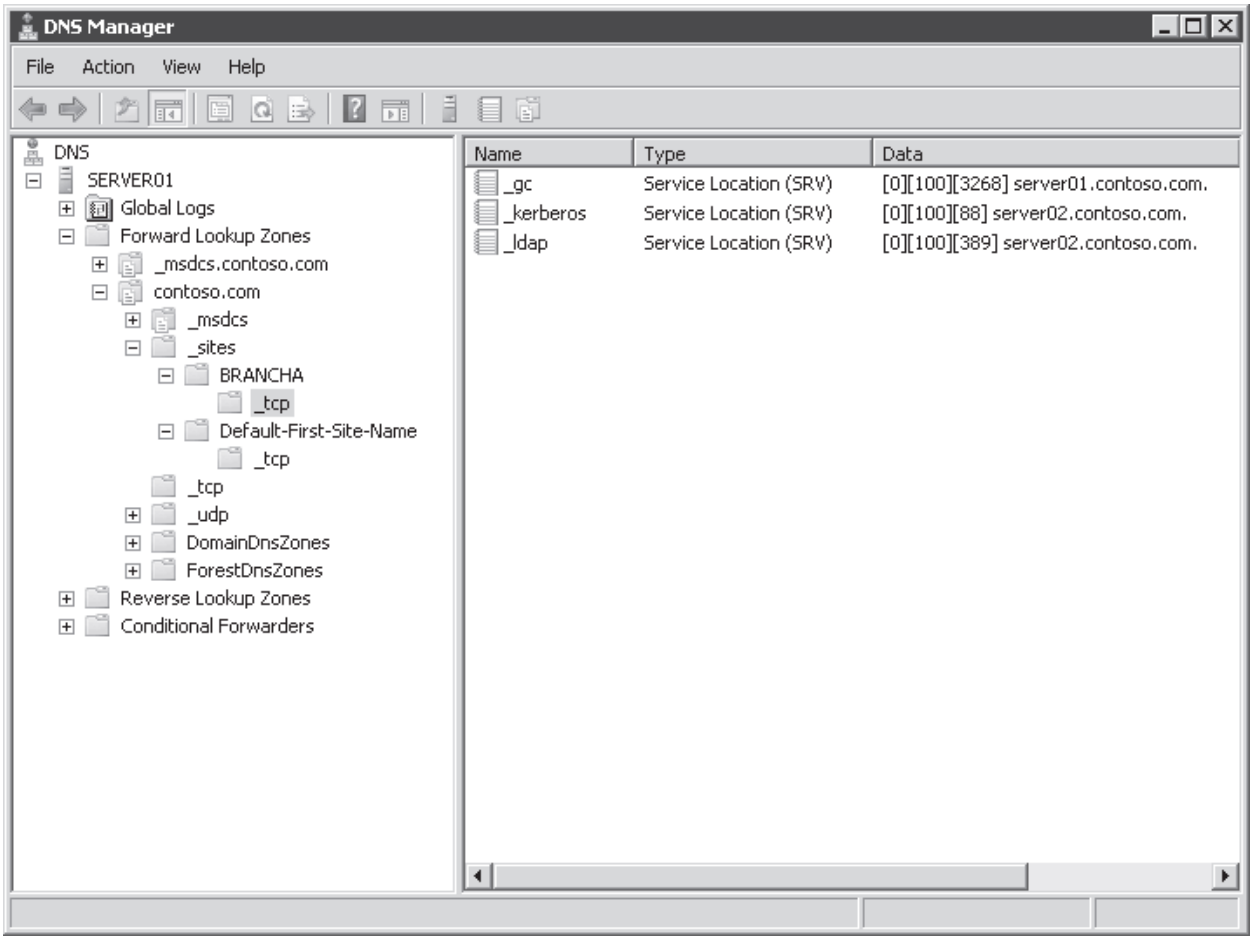
هر سایت شامل حاوی یک Servers container می‌باشد که خود آن حاوی یک شیء برای هر DC در آن سایت است. Servers container در یک سایت باید تنها DC ها را نمایش دهد نه همه سرورها را. وقتی یک DC ساخته می‌شود به طور پیش‌فرض در سایت عجین‌شده با آدرس IP خود قرار می‌گیرد. ولی ویزارد Active Directory Domain Services Installation ما را قادر می‌سازد سایت دیگری را برای این کار معرفی کنیم. همچنین می‌توانیم شیء سرور را برای DC در سایت مورد نظر از قبل ایجاد کنیم.
این کار با کلیک راست روی Servers container در سایت مورد نظر و انتخاب Server از منوی New قابل انجام است.
در نهایت پس از نصب نیز می‌توان DC را به سایت دیگری منتقل کرد. فقط کافی است روی سرور کلیک راست کرده و Move را انتخاب کنیم. بهترین کار این است که DC را در شیء سایتی قرار دهیم که با آدرس IP مربوط به DC ها عجین شده باشد. اگر DC دارای چند رابط شبکه باشد (multihomed) باز هم فقط می‌تواند به یک سایت تعلق داشته باشد. اگر سایتی DC نداشته باشد کاربران باز هم می‌توانند به دامنه وارد شوند به دلیل اینکه درخواست ورود آنها توسط DC که در سایت مجاور قرار دارد یا DC دیگری در دامنه بررسی می‌شود.
برای حذف یک شیء DC روی آن کلیک راست کرده و Delete را کلیک می‌کنیم.

مفهوم محل DC

ما این درس را با بررسی AD DS به عنوان یک سرویس توزیع شده شروع کردیم که سرویس تاییدهویت روی بیش از یک DC ارائه می‌شد. بعد یاد گرفتیم در توپولوژی شبکه جایگاه سایت‌ها و DC را تعیین کنیم. حالا آمادگی این را داریم که ببینیم دقیقا محلی‌سازی سرویس چگونه کار می‌کند و کلاینت‌ها چگونه DC را در سایت خود پیدا می‌کند. اگرچه احتمالا این جزئیات در امتحان جایی ندارد ولی در زمان رفع عیب در تایید هویت یک کامپیوتر یا کاربر به درد می‌خورد.

رکوردهای محل‌یابی سرویس (Service Locator Records)

وقتی یک DC به دامنه افزوده می‌شود سرویس‌های خود را توسط ساخت رکوردهای محل‌یابی سرویس (SRV) در DNS تبلیغ می‌کند. برخلاف رکوردهای میزبان (A records) که نام‌ها را به آدرس‌های IP نگاشت می‌کنند این رکوردها سرویس‌ها را به نام میزبان آن سرویس نگاشت می‌کنند. DC توانایی خود در فراهم کردن سرویس‌های تایید هویت و directory access با ثبت رکوردهای Kerberos و LDAP SRV تبلیغ می‌کنند. این رکوردهای SRV در پوشه‌های بسیاری در زون‌های DNS مربوط به forest افزوده می‌شوند. اولین پوشه در زون دامنه قرار می‌گیرد. نام آن _tcp بوده و حاوی رکوردهای SRV همه DC های دامنه است. پوشه دوم مختص سایتی است که در آن DC قرار دارد و در مسیر path_sites\sitename_tcp واقع شده است. در شکل ۶- ۱۱ می‌توانیم رکوردهای Kerberos و LDAP SRV را برای SERVER02.contoso.com در سایت _sites\BRANCHEA_tcp ببینیم. همچنین می‌توانیم پوشه _tcp را در اولین سطح زیر زون ببینیم.



شکل ۶- ۱۱ رکورد SRV برای SERVER02 در سایت BRANCHA

همین رکوردها در محل‌های زیادی در زون _msdcs.domainName ثبت می‌شود. نمونه آن _msdcs.contoso.com در شکل ۶- ۱۱ می‌باشد. این زون حاوی رکوردهایی برای Mictosoft Domain Cotroller Services است. کاراکتر خط زیر (_) در RFC شماره ۲۰۵۲ تعریف شده است.

رکوردهای محل‌یابی حاوی موارد زیر است:

- **نام سرویس و شماره پورت** این بخش از رکورد سرویسی را با یک پورت ثابت مشخص می‌کند. لزوما از پورت‌های شناخته‌شده نیست. رکوردهای SRV در ویندوز سرور 2008 دارای سرویس‌های LDAP با پورت ۳۸۹ ، Kerberos با پورت ۸۸ ، پروتکل Kerberos Password با پورت ۴۶۴ و سرویس‌های GC با پورت ۳۲۶۸ می‌باشد.

- **پروتکل** پروتکل لایه چهارم از مدل OSI یعنی لایه انتقال را مشخص می‌کند(TCP یا UDP). سرویس می‌تواند در رکوردهای SRV جداگانه از هر دو پروتکل استفاده کند. برای مثال رکوردهای Kerberos هم با TCP و هم با UDP ثبت می‌شوند. کلاینت‌های مایکروسافت فقط از TCP استفاده می‌کنند در حالی که کلاینت‌های لینوکس از TCP هم می‌توانند استفاده کنند.

- **نام میزبان سرویس** نامی است که به یک رکورد A برای میزبان یک سرویس برمی‌گردد. وقتی یک کلاینت درخواست سرویس را صادر می‌کند سرور DNS رکورد SRV و رکوردهای A منتسب را برمی‌گرداند بنابراین کلاینت نیازی به انتقال یک درخواست جداگانه به منظور تحلیل نام یک سرویس ندارد.

نام سرویس در رکورد SRV از استاندارد سلسله‌مراتبی DNS تبعیت می‌کند یعنی اجزاء آن با نقطه از هم مجزا می‌شوند. برای مثال سرویس Kerberos مربوط به DC به صورت زیر ثبت می‌شود :
Kerberos._tcp.sitename._sites.domainName
خواندن این رکورد از راست به چپ نظیر رکوردهای DNS به صورت زیر تعبیر می‌شود:

- DomainName : دامنه یا زون مثلا contoso.com
- _sites : همه سایت‌های ثبت شده با DNS
- siteName : سایت DC که سرویس را ثبت می‌کند.
- _tcp : هر سرویس مبتنی بر TCP در سایت
- Kerberos : یک Kerberos Key Distribution Center (KDC) با استفاده از TCP به عنوان پروتکل لایه انتقال

محل DC

کلاینت ویندوزی را تصور کنید که تازه به دامنه join شده است. راه اندازی مجدد می‌شود، یک آدرس IP جدید از DHCP می‌گیرد و آماده برای تایید هویت است. کلاینت چطور DC را پیدا می‌کند؟ به این صورت که کلاینت درخواست را از طریق پوشه _tcp که حاوی همه رکوردهای همه DC ها در دامنه است انجام می‌دهد. DNS لیستی از همه DC های متناظر برمی‌گرداند و کلاینت تلاش می‌کند با همه آنها تماس برقرار کند. اولین DC که به کلاینت پاسخ می‌دهد آدرس IP را بررسی کرده و کلاینت را از سایتی که به آن تعلق دارد آگاه می‌کند. کلاینت نام سایت را در رجیستری ذخیره می‌کند و بعد درخواست را برای DC هایی که در پوشه _tcp به تفکیک سایت موجود است ارسال می‌کند. DNS لیستی از همه DC های سایت برمی‌گرداند. کلاینت برای اتصال به همه آنها تلاش می‌کند و آن DC که اول پاسخ دهد کلاینت را تایید هویت می‌کند.
کلاینت به این DC وابستگی پیدا می‌کند و هر بار تلاش می‌کند با این DC تایید هویت شود. اگر DC در دسترس نبود کلاینت دوباره مراحل را از پوشه _tcp مربوط به سایت تکرار می‌کند و تلاش می‌کند با همه DC ها در سایت ارتباط برقرار کند. ولی اگر کلاینت یک لپ تاپ باشد چه اتفاقی می‌افتد؟ تصور کنید کامپیوتر در سایت BRANCHA تایید هویت می‌شود و سپس کاربر کامپیوتر را به سایت BRANCHB منتقل می‌کند. وقتی کامپیوتر روشن می‌شود سعی می‌کند با DC سایت BRANCHA تایید هویت شود. آن DC به آدرس IP کلاینت توجه می‌کند و متوجه می‌شود مربوط به سایت BRANCHB است. سپس کلاینت را از این موضوع آگاه می‌کند. بعد کلاینت به DNS برای DC های سایت BRANCHB درخواست ارسال می‌کند.

با ذخیره زیرشبکه و اطلاعات سایت در Active Directory توسط ثبت سرویس‌ها در DNS می‌توانیم ببینیم که چطور یک کلاینت برای استفاده از یک سرویس در سایت خودش تشویق می‌شود. این یعنی محلی‌سازی سرویس.

پوشش سایت (Site Coverage)

اگر سایتی DC نداشته باشد چه اتفاقی می‌افتد؟ سایت‌ها به منظور هدایت کاربران به سمت نسخه‌های محلی از منابع تکثیرشده نظیر پوشه‌های اشتراکی در فضای نام DFS به کار می‌رود بنابراین می‌توانیم سایتی بدون DC داشته باشیم. در این مورد نزدیک‌ترین DC رکورد SRV خود را در پروسه‌ای به نام پوشش سایت، در سایت ثبت می‌کند. بنابراین سایتی بدون DC توسط یک DC در سایت دیگری با کمترین هزینه ارتباطی پوشش داده می‌شود. درباره هزینه لینک سایت در درس بعدی یاد می‌گیریم. در صورتی که بخواهیم کنترل کاملی روی تایید هویت در سایت‌های بدون DC داشته باشیم می‌توانیم پوشش سایت و اولویت رکورد SRV را به صورت دستی پیکربندی کنیم.

تمرینات پیکربندی Site و Subnet

در این تمرینات ساختار Site و Subnet را برای دامنه contoso.com پیاده سازی می کنیم. برای انجام این تمرینات به یک دامنه نیاز داریم که دارای دو DC به نامهای SERVER01 و SERVER02 باشد.

تمرین اول پیکربندی Default Site

یک دامنه جدید حاوی سایت Default-First-Site-Name می باشد در این تمرین می خواهیم نام Site را عوض کرده و دو subnet را به آن منتسب کنیم.

۱- ابزار Active Directory Sites And Services را باز می کنیم.
۲- روی Default-First-Site-Name کلیک راست کرده و Rename را انتخاب می کنیم
۳- عبارت HEADQUARTERS را نوشته و Enter را فشار می دهیم
چون نام سایت‌ها در DNS ثبت می شود باید از یک نام سازگار با DNS برای سایت استفاده شود.
٤- روی Subnets راست کلیک کرده و New Subnet را انتخاب می کنیم
٥- در کادر Prefix عبارت 10.0.0.0/24 را تایپ می کنیم
٦- در لیست Select A Site Object For This Prefix گزینه HEADQUARTERS را انتخاب می کنیم
۷- روی OK کلیک می کنیم
۸- روی Subnets راست کلیک کرده و New Subnet را انتخاب می کنیم
۹- در کادر Prefix عبارت 10.0.1.0/24 را تایپ می کنیم
۱۰-در لیست Select A Site Object For This Prefix گزینه HEADQUARTERS را انتخاب می کنیم
۱۱-روی OK کلیک می کنیم

تمرین دوم ساخت یک سایت Additional

سایت‌ها این امکان را به ما می دهند تا ترافیک تکثیر را کنترل کرده و سرویسهایی از قبیل تایید هویت و دسترسی به دایرکتوری را متمرکز کنیم. در این تمرین یک سایت خواهیم ساخت و یک subnet به آن نسبت می‌دهیم.

۱. ابزار Active Directory Sites And Services را باز می کنیم
۲. روی sites راست کلیک کرده و New Site را انتخاب می کنیم
۳. در کادر نام عبارت BRANCHA را تایپ می کنیم
۴. DEFAULTIPSITELINK را انتخاب می کنیم
۵. روی OK کلیک میکنیم

یک کادر محاوره ای Active Directory Domain Services باز شده و مراحل تکمیل پیکربندی یک سایت را شرح می دهد

۶. روی OK کلیک میکنیم

۷. روی Subnets راست کلیک کرده و New Subnet را انتخاب می کنیم

۸. در کادر Prefix عبارت 10.1.1.0/24 را تایپ می کنیم

۹. در لیست Select A Site Object For This Prefix گزینه BRANCHA را انتخاب می کنیم

۱۰. روی OK کلیک می کنیم

۱۱. در ابزار Active Directory Sites And Services ، گره Subnets را باز می کنیم

۱۲. روی 10.1.1.0/24 کلیک راست کرده و Properties را انتخاب می کنیم

۱۳. در کادر توضیحات عبارت Primary subnet for branch office را تایپ می کنیم

۱۴. در لیست بازشوی Site ، BRANCHA را انتخاب می کنیم

۱۵. روی OK کلیک می کنیم

خلاصه درس

- سایت‌ها اشیاء Active Directory هستند که برای مدیریت تکثیر دایرکتوری و محلی‌سازی سرویس ها بکار می روند
- برای پیکربندی یک سایت باید یک شیء سایت بسازیم و یک subnet برای آن مشخص کنیم. یک سایت می تواند چندین subnetداشته باشد اما هر subnet تنها متعلق به یک سایت است
- DC ها در درون سایت‌ها به عنوان اشیاء سرور قرار می گیرند
- DC ها برای اعلام سرویس‌های تایید هویت و دسترسی به دایرکتوری خود رکورد service locator (SRV) ثبت می‌کنند. این رکوردها در گره های مخصوصی در حوزه‌های DNS برای دامنه و forest ساخته می شوند
- اعضای دامنه در حین فرایند تایید اعتبار سایت خود را شناسایی می کنند. DC ها از آدرس IP کلاینت و اطلاعات سایت و subnet دامنه برای مشخص کردن سایت مربوط به آن کلاینت استفاده می کنند و سپس این اطلاعات را برای کلاینت می فرستند

سئوالات پایان درس

۱. کلاینتهای یکی از شعبات شرکت در هنگام ورود به کندی عمل می کنند. همچنین می دانیم که سرور این رایانه ها یک DC در یک سایت راه دور می باشد. کدام یک از موارد زیر ممکن است باعث بروز این مشکل شده باشد؟

A. DC شعبه عضو برای سایت تعریف نشده است.

B. سایت شعبه به یک سایت لینک منتسب نیست.

C. بازه IP شعبه برای سایت تعریف شده نیست.

D. subnet مربوط به شعبه برای دو سایت تعریف شده است

۲. یک RODC به یکی از شعباتمان اضافه می کنیم. می خواهیم مطمئن شویم که تمام کلاینت ها در شعبه توسط RODC تایید اعتبار شوند. چه باید کرد؟ (در صورت نیاز تمام گزینه های درست را انتخاب کنید)

A . یک شیء subnet با پیشوند شبکه محدوده آدرس IP شعبه می‌سازیم.
B . یک حساب برای DC در OU مربوط به سایت می‌سازیم.
C . یک site link transport برای سایت می‌سازیم.
D . یک شیء سایت برای شعبه می‌سازیم.
E . یک شیء سرور در شیء سایت برای شعبه می‌سازیم.

درس ۲: پیکربندی Global Catalog و پارتیشن‌های دایرکتوری برنامه

وقتی بیش از یک DC در دامنه داشته باشیم باید به فکر تکثیر بانک اطلاعاتی بین DC ها باشیم. در این درس می‌بینیم که کدام پارتیشن‌های دایرکتوری روی DC تکثیر می‌شود و چطور تکثیر GC و پارتیشن‌ها را مدیریت می‌کنیم.
بعد از این درس یاد می‌گیریم:

- هدف GC را تشریح کنیم.
- DC ها را به عنوان سرورهای GC پیکربندی کنیم.
- Universal group membership caching را پیاده‌سازی کنیم.
- نقش پارتیشن‌های دایرکتوری برنامه را توضیح دهیم.

زمان تقریبی : ۴۵ دقیقه

مرور پارتیشن‌های دایرکتوری برنامه

در فصل ۱ یاد گرفتیم که AD DS حاوی یک انباره داده برای identity and management و به طور خاص بانک اطلاعاتی دایرکتوری، Ntds.dit می‌باشد. در این فایل پارتیشن‌های دایرکتوری قرار دارند. هر پارتیشن که naming context نیز نامیده می‌شود حاوی اشیاء حوزه مشخص و هدف می‌باشد. سه naming context اصلی در این کتاب بحث می‌شود:

- **Domain** naming context (NC) مربوط به دامنه حاوی همه اشیاء ذخیره شده در دامنه شامل کاربران، گروهها، کامپیوترها و Group Policy container (GPC) ها می‌باشد.
- **Configuration** پارتیشن پیکربندی حاوی اشیائی است که نمایانگر ساختار منطقی forest شامل دامنه‌ها، توپولوژی فیزیکی (سایت، زیرشبکه و سرویس‌ها) می‌باشد.
- **Schema** schema کلاس‌های شیء و خصیصه‌های آنها را برای کل دایرکتوری تعریف می‌کند.

هر DC یک کپی یا replica از naming context های مختلف نگه می‌دارد. پیکربندی همانند schema روی همه DC های forest تکثیر می‌شود. Naming context دامنه برای یک دامنه روی همه DC های دامنه نه دامنه‌های دیگر تکثیر می‌شود بنابراین هر DC حداقل سه replica دارد: NC دامنه برای دامنه خود، پیکربندی و schema.

قبلا replica ها کامل بودند. یعنی حاوی همه اشیاء یک خصیصه بودند و روی همه DC ها قابل تغییر بودند. با آمدن ویندوز سرور 2008 سرورهای RODC تصویر آنرا عوض کردند. یک RODC یک replica فقط خواندنی از همه اشیاء در پیکربندی، schema و NC دامنه برای دامنه خود نگه می‌دارد. بهرحال خصیصه‌های مشخصی وجود دارند که روی RODC تکثیر نمی‌شوند. مثلا کلمه عبور کاربران مگر اینکه سیاست کلمه عبور RODC اجازه چنین تکثیری را بدهد. همچنین خصیصه‌هایی وجود دارند که برای دامنه و forest امنیتی هستند که هیچ‌گاه روی RODC تکثیر نمی‌شوند.

مفهوم Global Catalog

یک forest را با دو دامنه تصور کنید. هر دامنه دو DC دارد. هر چهار DC یک replica از schema و پیکربندی forest را نگه می‌دارند. DC های دامنه A دارای replica های مربوط به NC دامنه برای دامنه A و DC های دامنه B دارای replica های NC دامنه برای دامنه B می‌باشند.

وقتی کاربری در دامنه B کاربر، کامپیوتر یا گروهی را در دامنه A جستجو می‌کند چه اتفاقی می‌افتد؟ DC های دامنه B هیچ اطلاعاتی درباره اشیاء دامنه A ندارند بنابراین نمی‌توانند پاسخ درخواست را بدهند.

اینجا جایی است که GC به عرصه می‌آید. GC یک پارتیشن است که اطلاعات همه اشیاء را در forest ذخیره می‌کند. وقتی کاربری در دامنه B یک شیء را در دامنه A جستجو می‌کند GC نتایج جستجو را فراهم می‌کند. جهت بهینه‌سازی کارایی، GC همه خصیصه‌های همه اشیاءforest را ذخیره نمی‌کند و زیرمجموعه‌ای از خصیصه‌هایی که برای جستجو بین دامنه‌ها مفید هستند ذخیره می‌کند. به همین دلیل GC را به نام partial attribute set (PAS) نیز می‌نامند. اگر بخواهیم بر اساس نقش GC را تعریف کنیم نوعی اندیس برای انباره داده AD DS می‌باشد.

جانمایی سرورهای GC

GC کارایی سرویس دایرکتوری را به حد زیادی افزایش می‌دهد و برای برنامه‌هایی نظیر Microsoft Exchange Server و Microsoft Office Outlook ضروری است. GC می‌تواند از یک DC سرویس بگیرد و در حالت ایده‌آل هر DC می‌تواند یک سرور GC باشد. در حقیقت بسیاری از سازمان‌ها در حال حاضر DC های خود را به عنوان سرور GC پیکربندی می‌کنند.

ایراد اینچنین پیکربندی در تکثیر مشخص می‌شود. GC پارتیشنی است که باید تکثیر شود. در یک forest با یک دامنه اگر همه DC ها به عنوان GC پیکربندی شوند بار کمی اضافه می‌شود زیرا همه DC ها قبلا مجموعه کاملی از خصیصه‌های همه اشیاء دامنه و forest را نگهداری می‌کردند. در یک forest بزرگ و با چند دامنه بار اضافی مربوط به تکثیر تغییرات PAS اشیاء در دامنه‌های دیگر است. بهرحال بسیاری از سازمان‌ها به این نتیجه رسیده‌اند که تکثیر Active Directory به اندازه کافی کارایی دارد و نگران این مساله نیستند. اگر بخواهیم همه DC ها را به عنوان GC تعریف کنیم دیگر نیاز نیست نگران جای infrastructure operation master باشیم. این نقش در شرایطی که همه DC ها سرور GC هستند زائد است.

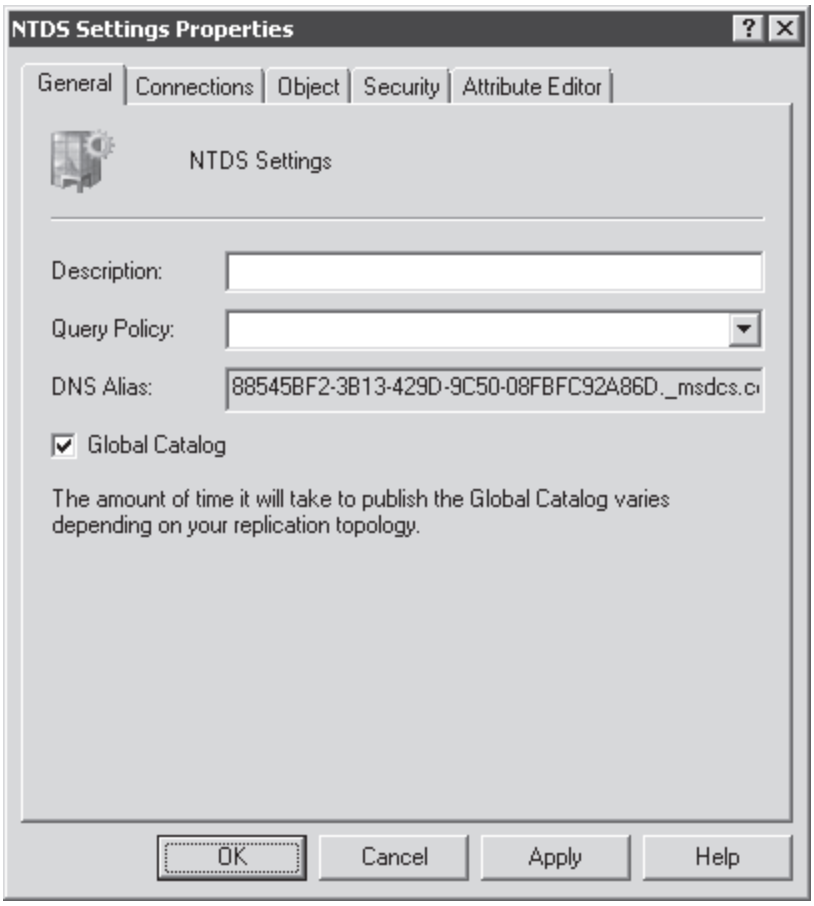
توصیه می‌شود سرور GC را روی DC در یک سایت زمانی پیکربندی کنیم که حداقل یکی از شرایط زیر حاکم باشد:

- یک برنامه پرکاربرد درخواست‌های دایرکتوری را با استفاده از پورت ۳۲۶۸ صادر کند.
- ارتباط با یک سرور GC کند یا متزلزل باشد.
- سایت حاوی سرور Exchange باشد.

پیکربندی سرور GC

وقتی اولین دامنه در forest ساخته می‌شود اولین DC به عنوان GC پیکربندی می‌شود. ما باید برای هر additional DC تصمیم بگیریم که GC باشد یا نه. هنگام نصب DC با ویزارد نصب دامنه یا دستور Dcpromo.exe امکان پیکربندی GC وجود دارد. راه دیگر حذف یا اضافه GC از DC ابزار Active Directory Sites And Services است. گره سایت و سپس Servers را در سایت

و در نهایت شیء سرور DC را باز می‌کنیم. روی گره NTDS Settings کلیک راست کرده و Properties را انتخاب می‌کنیم. در زبانه General که در شکل ۷- ۱۱ نشان داده شده است کادر Global Catalog را علامت می‌زنیم. برای حذف GC از DC همین مراحل را انجام داده و علامت کادر Global Catalog را برمی‌داریم.

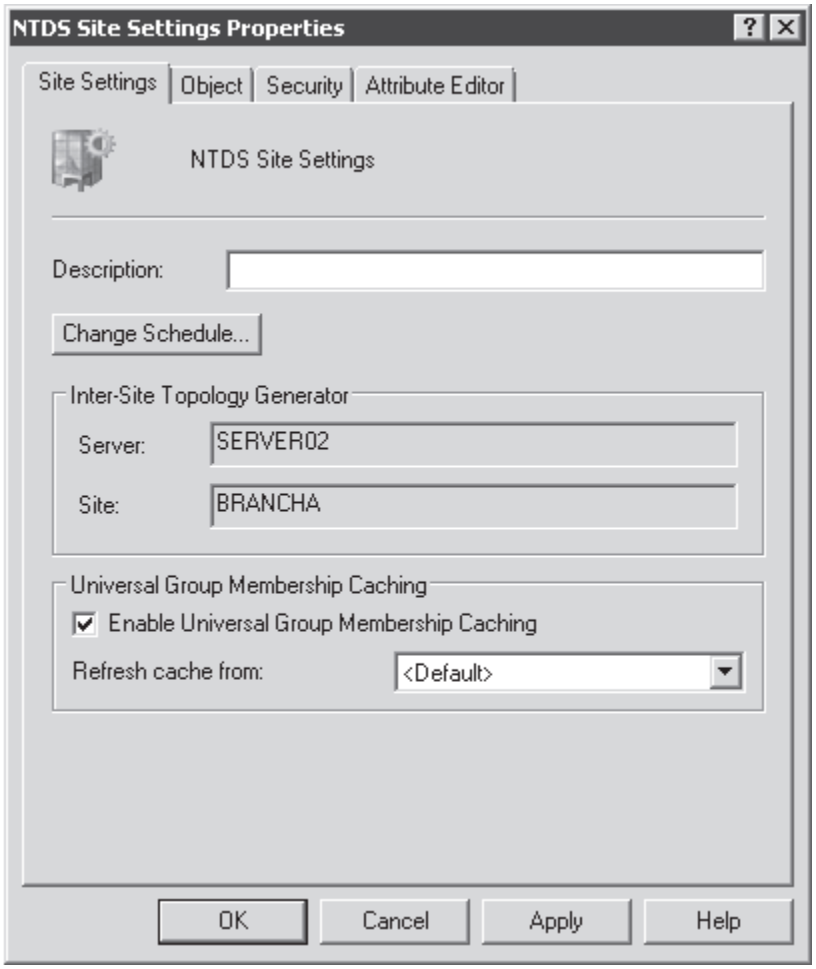


شکل ۷- ۱۱ کادر محاوره‌ای Properties مربوط به NTDS Settings که کادر علامت Global Catalog را نشان می‌دهد.

Universal Group Membership Caching

در فصل ۴ یاد گرفتیم که Active Ditectory از گروههای universal پشتیبانی می‌کند. این گروهها برای افزودن کاربران و گروههایی از دامنه‌های مختلف در forest طراحی شده است. عضویت این گروهها روی GC تکثیر می‌شود. اگر GC در دسترس نباشد گروه نیز در دسترس نخواهد بود. ممکن است گروه universal برای جلوگیری از دسترسی کاربری به منابع شبکه استفاده شود بنابراین ویندوز از تایید هویت کاربر امتناع می‌ورزد. اگر کاربر قبلا به سیستم خود وارد شده باشد با استفاده از اعتبار cache شده می‌تواند وارد شود ولی به محض اینکه تلاش کند به منابع شبکه دسترسی پیدا کند با پیغام خطا مواجه می‌شود. به عنوان خلاصه اگر یک سرور GC در دسترس نباشد کاربران نمی‌توانند به منابع شبکه دسترسی پیدا کنند.

اگر همه DC ها سرور GC هم باشند این مساله بروز نمی‌کند. اگر تکثیر معضل شبکه باشد و نخواهیم DC را به عنوان GC پیکربندی کنیم می‌توانیم ورود موفق را با universal group membership caching (UGMC) تسهیل کنیم. وقتی UGMC را روی یک DC در یک شعبه پیکربندی می‌کنیم آن DC اطلاعات عضویت گروههای universal را از یک GC برای کاربر هنگام اولین ورود کاربر در سایت دریافت می‌کند و DC این اطلاعات را cache کرده و هر ۸ ساعت یکبار این اطلاعات را به روز می‌کند. از این طریق اگر کاربری بعدا وارد شود و سرور GC در دسترس نباشد DC می‌تواند از اطلاعات cache شده برای صدور مجوز ورود کاربر استفاده کند. بنابراین پیشنهاد می‌شود که در سایت‌هایی که با سرور GC ارتباط مطمئنی ندارند روی DC ها UGMC را پیکربندی کنیم. برای پیکربندی UGMC ابزار Active Directory Sites And Services را باز کرده و سایت را در کنسول انتخاب می‌کنیم. در پنجره جزئیات روی NTDS Site Settings کلیک راست کرده و Properties را انتخاب می‌کنیم. کادر محاوره‌ای NTDS Site Settings Properties همانند شکل ۸- ۱۱ گزینه Universal Group Membership Caching را آشکار می‌کند. حالا می‌توانیم کادر را علامت بزنیم و GC را که به روز رسانی از روی آن انجام می‌شود مشخص کنیم.



شکل ۸- ۱۱ کادر محاوره‌ای NTDS Site Settings Properties با گزینه‌ای برای فعال کردن Universal Group Membership Caching

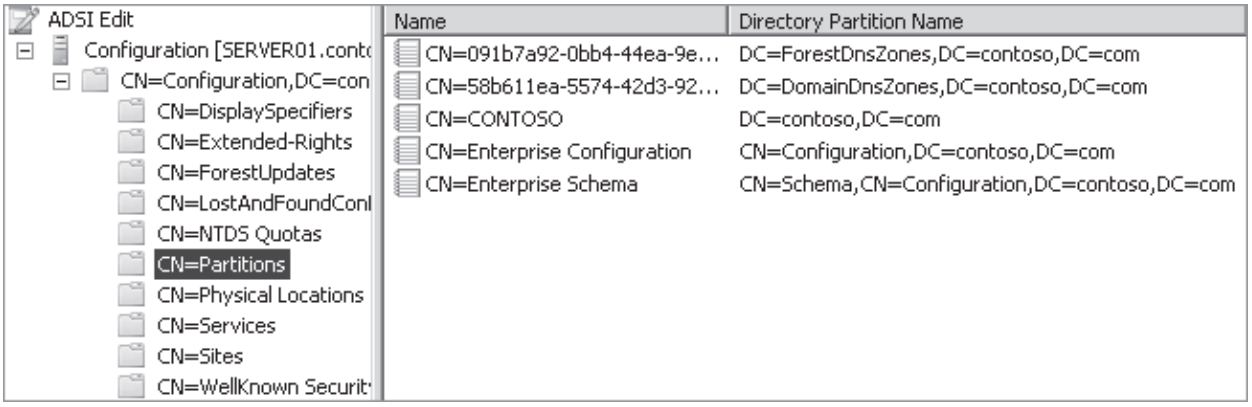
پارتیشن‌های دایرکتوری برنامه

از آنجائیکه پارتیشن‌های دامنه، پیکربندی و schema مربوط به دایرکتوری روی همه DC های دامنه تکثیر می‌شود و علاوه بر آن پیکربندی و schema روی همه DC های forest نیز تکثیر می‌شود Active Directory همچنین از پارتیشن‌های دایرکتوری برنامه پشتیبانی می‌کند. یک پارتیشن دایرکتوری برنامه بخشی از انباره دادهست که حاوی اشیاء مورد نیاز یک برنامه یا یک سرویس می‌باشد و این سرویس یا برنامه خارج از سرویس اصلی AD DS است. برخلاف دیگر پارتیشن‌ها پارتیشن‌های برنامه می‌تواند هدف تکثیر روی DC های خاصی باشد. به طور پیش‌فرض آنها روی همه DC ها تکثیر نمی‌شوند.

پارتیشن‌های دایرکتوری برنامه به منظور پشتیبانی از برنامه‌ها و سرویس‌های مرتبط با دایرکتوری طراحی شده است. آنها می‌توانند حاوی انواع اشیاء به جز واحدهای امنیتی مانند کاربران، کامپیوترها یا گروههای امنیتی باشند. به دلیل اینکه این پارتیشن‌ها فقط زمان نیاز تکثیر می‌شوند مزایایی از قبیل تحمل خرابی، دسترس پذیری و کارایی را در شرایط تکثیر بهینه به همراه دارند.

ساده‌ترین راه برای درک این نوع پارتیشن بررسی پارتیشن‌هایی است که توسط سرور DNS نگهداری می‌شود. وقتی یک زون Active Directory عجین شده می‌سازیم رکوردهای DNS با استفاده از یک پارتیشن دایرکتوری برنامه بین سرورهای DNS تکثیر می‌شوند. پارتیشن و اشیاء رکورد DNS آن روی همه DC ها تکثیر نمی‌شود و فقط روی آنهایی که به عنوان سرور DNS عمل می‌کنند تکثیر می‌شوند.

ما می‌توانیم این پارتیشن‌ها را در forest با باز کردن پنجره ADSI Edit ببینیم. روی ریشه ابزار کلیک راست کرده و Connect To را انتخاب می‌کنیم. در لیست بازشوی Select A Well Known Naming Context گزینه Configuration را انتخاب و روی OK کلیک می‌کنیم. گره Configuration و بعد پوشه‌ای که نماد پارتیشن configuration است را باز می‌کنیم و سپس در ساختار کنسول پوشه Partitions (CN=Partitions) را انتخاب می‌کنیم. در پنل وسط پارتیشن‌های انباره داده AD DS را همانند شکل ۹- ۱۱ می‌بینیم.



شکل ۹- ۱۱ پارتیشن‌ها در contoso.com forest

به دو پارتیشن شکل ۹- ۱۱ ForestDnsZones و DomainDnsZones توجه کنید. بیشتر پارتیشن‌های برنامه توسط برنامه‌های کاربردی که به آن نیاز دارند ساخته می‌شود. DNS یک نمونه از این برنامه‌هاست و Telephony Applocation Programming Interface (TAPI) نمونه دیگری است. اعضای گروه Enterprise Admins هم می‌توانند پارتیشن‌های دایرکتوری را با دستور Ntdsutil.exe به صورت دستی بسازند.

پارتیشن برنامه هر جایی از فضای نام forest که پارتیشن دامنه حضور دارد می‌تواند ظاهر شود. نام‌های DN مربوط به پارتیشن‌های DNS برای مثال DC=DomainDnsZones,DC=contoso,DC=com پارتیشن‌ها را به عنوان فرزند پارتیشن‌های دامنه DC=contoso,DC=com جای می‌دهند. یک پارتیشن برنامه همچنین می‌تواند فرزند یک پارتیشن برنامه دیگر یا یک tree جدید در forest باشد.

به زبان ساده ما از ابزار مختص برنامه برای مدیریت پارتیشن دایرکتوری برنامه، داده آن و تکثیر آن استفاده می‌کنیم. برای مثال با افزودن زون عجین شده Active Directory به یک سرور DNS باعث می‌شود به طور اتوماتیک DC برای دریافت کپی پارتیشن DomainDns پیکربندی شود. با ابزارهایی نظیر Ntdsutil.exe و Ldp.exe می‌توانیم پارتیشن‌های دایرکتوری برنامه را به طور مستقیم مدیریت کنیم.

خیلی مهم است که قبل از demote کردن DC مواظب پارتیشن‌های برنامه باشیم. اگر یک DC میزبان یک پارتیشن دایرکتوری برنامه باشد باید هدف پارتیشن را ارزیابی کنیم و ببینیم آیا مورد نیاز برنامه‌ای هست یا نه و اینکه DC میزبان آخرین کپی از پارتیشن است که در این صورت پاک کردن DC منتج به از دست رفتن دائم همه اطلاعات پارتیشن می‌شود. اگرچه ویزارد Active Directory Domain Services Installation پیغام می‌دهد که پارتیش‌های دایرکتوری برنامه را حذف کنیم ولی پیشنهاد می‌گردد این کار به صورت دستی قبل از demote کردن DC صورت گیرد.

تمرینات تکثیر و پارتیشن‌های دایرکتوری

در این تمرین تکثیر GC را پیکربندی و پارتیشن‌های دایرکتوری برنامه DNS را بررسی می کنیم. برای انجام این تمرینات لازم است تمرینات درس اول را انجام داده باشیم

تمرین اول پیکربندی یک سرور Global Catalog

اولین DC در forest به عنوان GC عمل می کند، ممکن است بخواهیم یک سرور GC دیگر برای پشتیبانی از پرس و جوهای دایرکتوری ، ورود و برنامه هایی مانند سرور Exchange اضافه کنیم. در این تمرین SERVER02 را به عنوان میزبان replica of the partial attribute set یا GC پیکربندی می کنیم.

۱- با اعتبار Administrator وارد SERVER01 می شویم
۲- ابزار Active Directory Sites And Services را باز می کنیم
۳- گره BRANCHA ، Servers و SERVER02 را باز می کنیم
٤- روی NTDS Settings در زیر SERVER02 راست کلیک کرده و Properties را انتخاب می کنیم
٥- Global Catalog را انتخاب کرده و روی OK کلیک می کنیم

تمرین دوم پیکربندی Universal Group Membership Caching

در سایت‌های بدون GC ، اگر DC نتواند با سرور GC در سایت دیگر ارتباط برقرار کند ، ورود کاربران ممکن است با مشکل مواجه شود. برای کم کردن مشکلاتی از این دست می توانیم یک سایت را طوری پیکربندی کنیم که اطلاعات عضویت گروههای universalرا در خود cache کند. در این تمرین یک سایت خواهیم ساخت و برای cache کردن اطلاعات عضویت گروههای universal آنرا پیکربندی می کنیم

۱- روی Sites راست کلیک کرده و New Site را انتخاب می کنیم
۲- در کادر نام عبارت BRANCHB را تایپ می کنیم
۳- DEFAULTIPSITELINK را انتخاب می کنیم
٤- روی OK کلیک می کنیم

در دنیای واقعی نیاز داریم که حداقل یک subnet برای این سایت درست کرده و یک DC در BRANCHB نصب کنیم

٥- BRANCHB را در کنسول انتخاب می کنیم
٦- روی NTDS Site Settings در پنجره وسط ، کلیک راست کرده و Properties را انتخاب می کنیم
۷- در زبانه Site Settings کادر Enable Universal Group Membership Caching را علامت می زنیم
۸- روی OKکلیک می کنیم

تمرین سوم بررسی پارتیشن‌های دایرکتوری برنامه

در این تمرین به جستجو در پارتیشن دایرکتوری برنامه DomainDnsZone بوسیله ADSI Edit خواهیم پرداخت

۱- ADSI Edit را از Administrative Tools باز می کنیم
۲- روی گره ریشه ابزار ADSI Edit کلیک راست کرده و گزینه Connect To را انتخاب می کنیم
۳- در لیست بازشوی Select A Well Known Naming Context ، Configuration را انتخاب و روی OK کلیک می کنیم
٤- در کنسول Configuration را انتخاب کرده و آن را باز می کنیم
٥- CN=Configuration, DC=contoso, DC=com را انتخاب کرده و آن را باز می کنیم
٦- CN=Partitions را انتخاب می کنیم
۷- نام Directory Partition برای DomainDnsZones partition را یادداشت می‌کنیم.
DC=DomainDnsZones,DC=contoso,DC=com
۸- روی ADSI Edit کلیک راست کرده و گزینه Connect To را انتخاب می کنیم
۹- گزینه Select Or Type A Distinguished Name Or Naming Context option را انتخاب می کنیم
۱۰- در کادر بازشو عبارت DC=DomainDnsZones,DC=contoso,DC=com را تایپ کرده و OKرا کلیک می کنیم
۱۱- در کنسول Default Naming Context را انتخاب کرده و آن را باز می کنیم
۱۲- گزینه DC=DomainDnsZones,DC=contoso,DC=com را انتخاب و باز می کنیم
۱۳- گزینه CN=MicrosoftDNS را انتخاب و باز می کنیم
۱٤- DC=contoso.com را انتخاب می کنیم
۱٥- اشیاء درون این container را بررسی کرده و آنها را با رکورد های DNS دامنه contoso.com مقایسه می کنیم

خلاصه درس

- global catalog (GC) شامل یک کپی از همه اشیاء در forest می‌باشد ولی فقط برخی از خصیصه‌های شیء را نگه می‌دارد. همچنین partial attribute set (PAS) نیز نامیده می شود

- سرورهای GC باعث بهبود فرآیند پرس و جوی دایرکتوری و ورود بوده و برای برنامه‌هایی مانند Exchange Server. اطلاعات فراهم می کنند
- اولین DC در forest سرور GC می باشد و ما می توانیم با استفاده از دستور *Dcpromo.exe* یا Active Directory Domain Services Installation Wizard یا ابزار Active Directory Sites And Services یک DC را به سرور GC تبدیل کنیم
- اگر سایت ما GC نداشت می توانیم با universal group membership caching (UGMC) احتمال بروز خطا در زمان در دسترس نبودن سرور GC را کاهش دهیم
- پارتیشن‌های دایرکتوری برنامه منحصربه فرد هستند زیرا می توانند به تمام DC ها در سطح forest تکیر شوند. حوزه‌های Active Directory integrated DNS در پارتیشن‌های برنامه نگهداری می شوند

سئوالات پایان درس

۱. یکی از شعبه های ما با یک خط کند و نامطمئن به مرکز داده متصل است می خواهیم مطمئن شویم که DC شعبه ما حتی زمانی که نمی تواند به سرور GC دسترسی داشته باشد، قابلیت تایید هویت کاربران را داشته باشد. کدام یک از پیکربندی های زیر باید انجام شود؟

A. Read-only domain controller
B. Application directory partition
C. Intersite replication
D. Universal group membership caching

۲. به عنوان مدیر شبکه در شرکت contoso.com مشغول به کار هستیم. Forest شرکت دارای سه دامنه می باشد که هرکدام از آنها دارای چهار DC می باشد. می خواهیم نقش DC یک سرور را در دامنه ریشه forest حذف کنیم می خواهیم مطمئن شویم که آسیب دائمی به پارتیشن‌های Active Directory نمی رسد. کدام یک از پارتیشن‌های Active Directory زیر می‌تواند تنها در آن DC موجود باشد؟ (در صورت نیاز تمام گزینه های درست را انتخاب کنید)

A. Schema
B. Configuration
C. Domain
D. Partial attribute set
E. Application directory partition

۳. می خواهیم تمام DCهای موجود در forestرا به صورت GC پیکربندی کنیم. کدام ابزار ما را در رسیدن به این هدف کمک می کند؟

A. *Dcpromo.exe*
B. Active Directory Domain Services Installation Wizard
C. ابزار Active Directory Sites and Services
D. ابزار Active Directory Users and Computers
E. Active Directory Domains and Trusts

درس ۳: تکثیر پیکربندی

در درس ۱ یاد گرفتیم که سایت و اشیاء زیرشبکه با هدف فعال کردن محلی‌سازی تایید هویت و دسترسی دایرکتوری روی Active Directory و کلاینت‌ها بسازیم. یاد گرفتیم جای DC را در شبکه تعیین کنیم. در درس ۲ سرورهای GC و پارتیشن‌های دایرکتوری برنامه را پیکربندی کردیم و تعیین کردیم چه مواردی بین DC ها تکثیر شود. در این درس یاد می‌گیریم چطور و چه زمانی عملیات تکثیر اتفاق می‌افتد. می‌بینیم که چرا پیکربندی پیش‌فرض Active Directory از تکثیر موثر پشتیبانی می‌کند و چرا باید این پیکربندی را طوری تغییر دهیم که تکثیر با همان تاثیر و کاراتر از قبل بر اساس توپولوژی شبکه انجام شود.

بعد از این درس یاد می‌گیریم:

- به منظور پیکربندی تکثیر بین دو DC اشیاء ارتباط بسازیم.
- سایت لینک‌ها و هزینه‌های آنرا پیاده‌سازی کنیم تا بتوانیم تکثیر را بین سایت‌ها مدیریت کنیم.
- سرورهای با اولویت اول bridgehead را تخصیص دهیم.
- Notification and polling را بشناسیم
- با استفاده از دستور Repadmin.exe تکثیر را آنالیز کرده و گزارش بگیریم.
- با استفاده از دستور Dcdiag.exe صحت تکثیر Active Directory را چک کنیم.

زمان تقریبی : ۹۰ دقیقه

مفهوم تکثیر Active Directory

مهم‌ترین چیزی که در دروس قبلی یاد گرفتیم این است که هر replica روی DC با replica های آن پارتیشن که روی DC های دیگر است باید یکی باشد. معنی آن این نیست که باید اطلاعات در هر لحظه روی همه DC ها دقیقا یکی باشد. بهرحال تکثیر باعث می‌شود همه تغییرات روی یک پارتیشن به همه replica های پارتیشن منتقل شود. تکثیر Active Directory بین دو آیتم صحت (integrity) و ثبات (convergence) از یک طرف و کارایی از طرف دیگر تعادلی برقرار می‌کند. از این تعادل با عنوان loose coupling یاد می‌شود.

ویژگی‌های کلیدی تکثیر Active Directory عبارتند از:

- پارتیشن‌بندی انباره داده. DC های یک دامنه فقط حاوی domain naming context برای دامنه خود می‌باشند که مخصوصا در forest هایی با چند دامنه تکثیر را به حداقل می‌رساند. دادههای دیگر شامل پارتیشن‌های دایرکتوری برنامه و GC به طور پیش‌فرض روی همه DC های شبکه تکثیر نمی‌شود.
- تولید خودکار یک توپولوژی تکثیر قوی و کارا. به طور پیش‌فرض Active Directory یک توپولوژی تکثیر دوطرفه با کارایی بالا را طوری پیکربندی می‌کند که نبود یک DC مانع تکثیر نمی‌شود. این توپولوژی هنگام افزودن، حذف یا انتقال DC به سایت دیگر به طور خودکار به روز می‌شود
- تکثیر در سطح خصیصه. وقتی خصیصه یک شیء تغییر می‌کند فقط آن خصیصه با حداقل متاداده تکثیر می‌یابد. کل شیء تکثیر نمی‌شود مگر اینکه شیء ساخته شود.
- کنترل مجزای تکثیر در یک سایت و بین سایت‌های مختلف.

- کشف تداخل و مدیریت آن. اگرچه بندرت اتفاق می‌افتد ولی ممکن است یک خصیصه روی دو DC مختلف در طول یک پنجره تکثیر تغییر کند. (منظور از پنجره تکثیر فاصله زمانی شروع و پایان تکثیر است.) در چنین وضعیتی دو تغییر باید تطبیق یابند. Active Directory دارای الگوریتم‌هایی است که تمامی این حالات را پوشش می‌دهد.

تکثیر Active Directory را با بررسی یک به یک اجزاء ساده‌تر می‌توان درک کرد. بخش‌های بعدی این اجزاء را بررسی می‌کند.

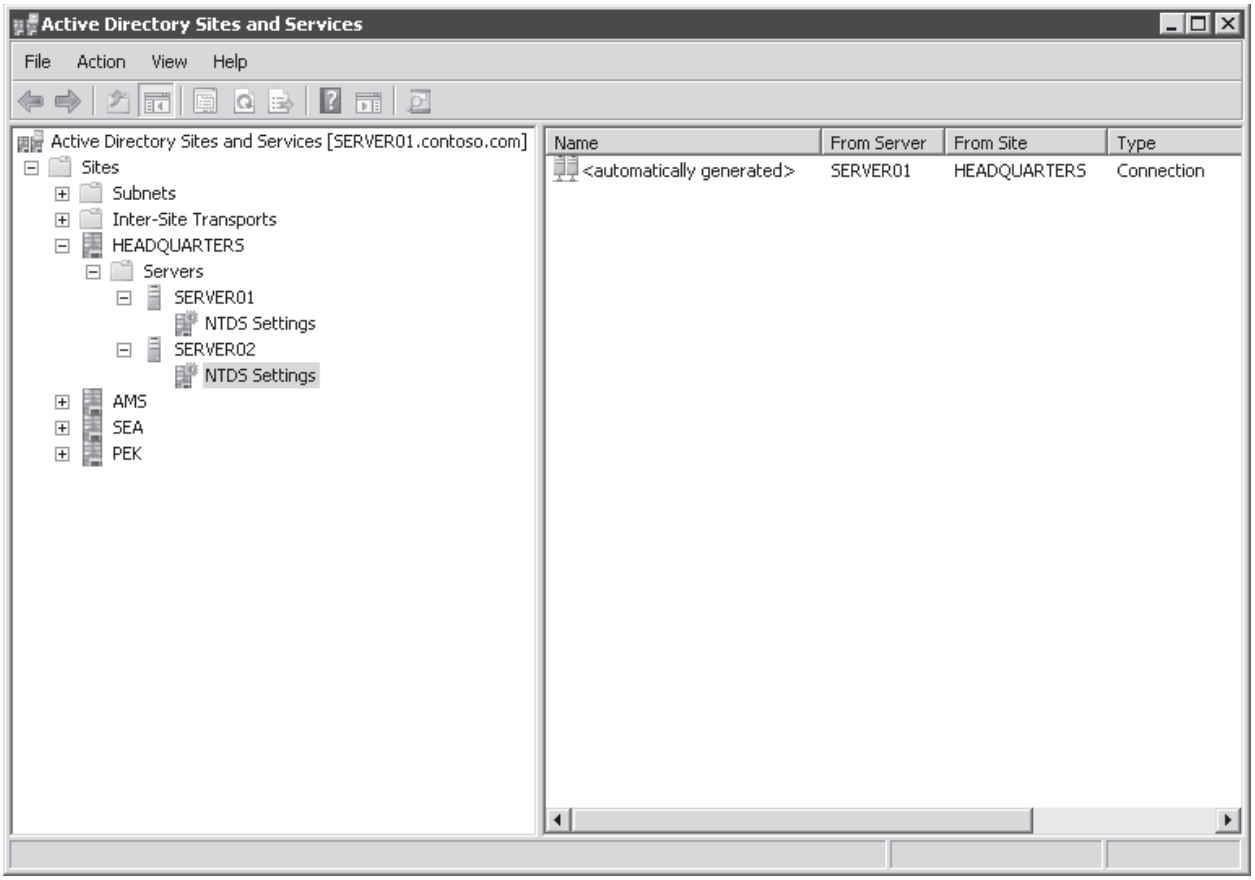
اشیاء ارتباط (Connection Objects)

یک DC با اشیاء ارتباط AD DS تغییرات را از DC های دیگر دریافت می‌کند. اشیاء ارتباط در administrative tools در ابزار Active Directory Sites and Services که محتوای NTDS Settings container مربوط به شیء سرور DC را تشکیل می‌دهند قابل رویت است. شکل ۱۰- ۱۱ مثالی را در این ارتباط نشان می‌دهد. شیء ارتباط در SERVER02 تکثیر را از SERVER01 به SERVER02 پیکربندی می‌کند. شیء ارتباط نمادی از مسیر تکثیر از یک DC به DC دیگر است.

اشیاء ارتباط یک‌طرفه بوده و نمایانگر تکثیر از بیرون به داخل است (کششی). در دامنه شکل ۱۰- ۱۱ SERVER02 تغییرات را از SERVER01 می‌کشد. SERVER02 را می‌توان در پایین و SERVER01 را در بالا تصور کرد که تغییرات از بالا به پایین جاری می‌شود.

نکته تکثیر اجباری

تکثیر بین دو DC را می‌توان با کلیک راست روی شیء ارتباط و انتخاب Replicate Now اجبار کرد. به خاطر داشته باشید تکثیر از بیرون به داخل انجام می‌شود پس برای تکثیر هر دو DC باید این عملیات را روی هر شیء ارتباط هر دو DC انجام دهیم.



شکل ۱۰- ۱۱ شیء ارتباط در ابزار Active Directory Sites and Services

Knowledge Consistency Checker

مسیرهای تکثیر ساخته شده بین DC ها توسط اشیاء ارتباط، توپولوژی تکثیر را در forest ایجاد می‌کند. خوشبختانه ما مجبور نیستیم توپولوژی را دستی بسازیم. به طور پیش‌فرض Active Directory توپولوژی را طوری ایجاد می‌کند که تکثیر موثر تحقق یابد. این

توپولوژی دوطرفه است به طوری که اگر یک DC از کار افتاد تکثیر بدون وقفه به کار خود ادامه می‌دهد. این توپولوژی همچنین تضمین می‌کند که بین دو DC حداکثر سه پرش موجود باشد.

اگر به شکل ۱۰- ۱۱ توجه کنیم متوجه می‌شویم که شیء ارتباط به طور خودکار ساخته شده است. روی هر DC یک بخش به نام knowledge consistency checker (KCC) موجود است که به ایجاد و بهینه‌سازی تکثیر خودکار بین DC های سایت کمک می‌کند. KCC کار ارزیابی DC ها را در یک سایت انجام داده و اشیاء ارتباط را به منظور ایجاد توپولوژی دوطرفه و حداکثر با سه پرش می‌سازد. وقتی DC به سایت افزوده یا حذف می‌شود یا زمانی که دیگر در دسترس نیست KCC توپولوژی را به طور پویا مرتب‌سازی می‌کند. این کار با اضافه کردن یا حذف اشیاء ارتباط برای بازسازی توپولوژی تکثیر موثر انجام می‌شود.

ما می‌توانیم اشیاء ارتباط را با هدف تعیین مسیر ایجاد کنیم. این اشیاء توسط KCC حذف نمی‌شوند. برای ساخت شیء ارتباط شیء سرور مقصد تکثیر را پیدا کرده در شیء سرور روی NTDS Settings container کلیک راست کرده و New Active Directory Domain Services Connection را انتخاب می‌کنیم. در کادر محاوره‌ای Find Active Directory Domain Controllers شیء مبدا تکثیر را انتخاب کرده و OK می‌کنیم. به شیء ارتباط جدید نامی را اختصاص داده و OK می‌کنیم. سپس پنجره properties شیء ارتباط را باز کرده و از فیلد Description برای درج هدف ساخت شیء استفاده می‌کنیم.

در یک سایت سناریوهای کمی وجود دارد که نیاز به ساخت شیء ارتباط دارد. یکی از این سناریوها standby operations masters می‌باشد. operations masters ها در فصل ۱۰ بررسی شدند. پیشنهاد می‌شود که DC ها را به عنوان standby operations masters انتخاب کنیم تا در زمان انتقال یا تصرف نقش operations master از آنها استفاده کنیم. Standby operations master باید با operations master فعلی ارتباط تکثیر مستقیم داشته باشد. بنابراین اگر یک DC با نام DC01 نقش RID master داشته باشد و DC02 سیستمی است که در زمان خروج DC01 نقش master را بازی خواهد کرد باید یک شیء ارتباط در DC02 طوری ساخته شود که تکثیر مستقیما از DC01 انجام شود.

تکثیر درون سایتی

پس از اینکه اشیاء ارتباط بین DC های سایت چه خودکار و چه دستی برقرار شد تکثیر اتفاق می‌افتد. تکثیر درون‌سایتی کار تکثیر تغییرات را در یک سایت انجام می‌دهد.

اطلاع‌رسانی (Notification)

سایت نمایش داده شده در شکل ۱۰- ۱۱ را در نظر بگیرید. وقتی SERVER01 تغییری را روی پارتیشن ایجاد می‌کند این تغییر در صف تکثیر به سرورهای دیگر قرار می‌گیرد. SERVER01 به طور پیش‌فرض به مدت ۱۵ ثانیه صبر می‌کند و بعد اولین سرور را یعنی SERVER02 را متوجه تغییر می‌کند. اطلاع‌رسانی پروسه‌ای است که توسط آن سرور مبدا تکثیر سرور مقصد را متوجه تغییر می‌کند. SERVER01 به طور پیش‌فرض ۳ ثانیه صبر می‌کند و بعد تغییر را به بقیه سرورها اطلاع می‌دهد. این تاخیرها که به ترتیب initial notification delay و subsequent notification delay نامیده می‌شوند برای ایجاد تناوب در ترافیک شبکه در اثر تکثیر درون‌سایتی طراحی شده است.

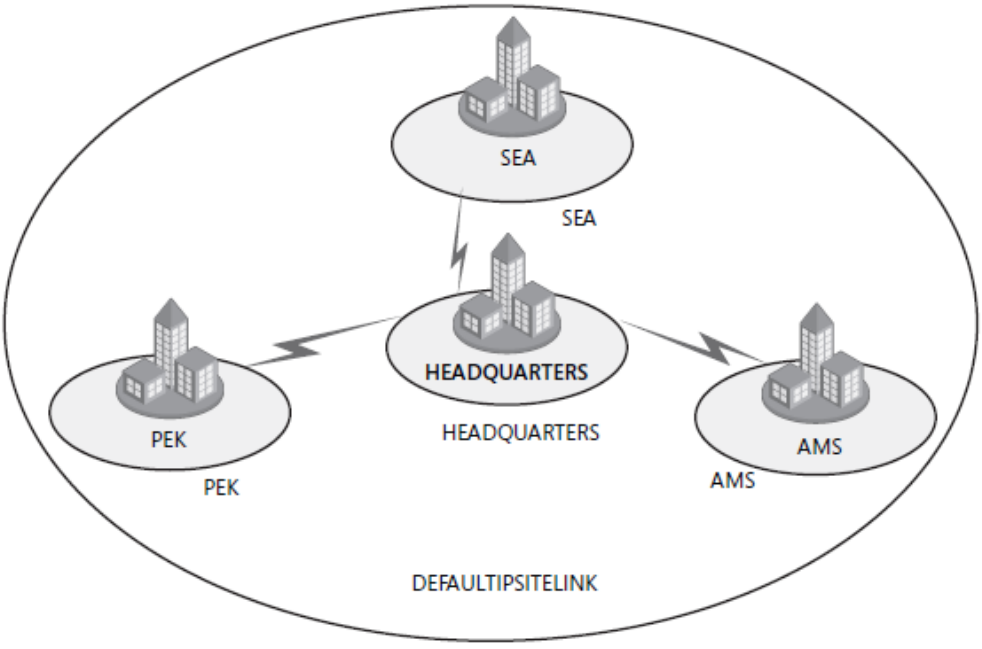
SERVER02 براساس دریافت اطلاع تغییرات را از SERVER01 درخواست می‌کند و عامل تکثیر دایرکتوری یا directory replication agent (DRA) انتقال خصیصه را از SERVER01 به SERVER02 عملی می‌کند. در این مثال SERVER01 تغییر اولیه را در Active Directory ایجاد کرده است. این سرور DC آغازین و تغییری که ایجاد می‌کند سرمنشا تغییر محسوب می‌شود. وقتی SERVER02 تغییر را دریافت می‌کند آنرا روی دایرکتوری خود اعمال می‌کند. این تغییر تکثیر نامیده نمی‌شود ولی بهرحال تغییر است. SERVER02 تغییر را به منظور تکثیر به رده‌های پایین‌تر در صف قرار می‌دهد. SERVER03 سروری است که در ساختار پایین‌تر از SERVER02 قرار دارد. پس از ۱۵ ثانیه SERVER02 به SERVER03 اطلاع می‌دهد که تغییری ایجاد شده است. SERVER03 تغییر را به دایرکتوری خود اعمال می‌کند و به زیررده‌های خود نیز اطلاع می‌دهد. تغییر تاکنون دو پرش داشته یکی از SERVER01 به SERVER02 و دیگری از SERVER02 به SERVER03. گفتیم که توپولوژی تکثیر تضمین می‌کند که حداکثر پرش تکثیر ۳ تاست پس هر پرش تقریبا ۱۵ ثانیه طول می‌کشد و بنابراین هر تغییری در حدود ۱ دقیقه طول می‌کشد تا به طور کامل در سایت تکثیر شود.

Polling

بسیار محتمل است که SERVER01 برای مدت طولانی مخصوصا در زمان تعطیلی سازمان تغییری را در replica ایجاد نکند. در این گونه موارد SERVER02 اطلاعی از SERVER01 دریافت نمی‌کند. همچنین ممکن است SERVER01 در دسترس نباشد که باز هم هیچ اطلاعی به دست SERVER02 نمی‌رسد بنابراین برای SERVER02 مهم است بداند که سرور بالایی در دسترس است و آیا تغییری ایجاد کرده است یا نه. این کار از طریق پروسه‌ای به نام polling انجام می‌شود. Polling باعث می‌شود که سرور رده پایین (از نظر تکثیر) درخواستی را به سرور بالایی ارسال کرده و تغییرات احتمالی را جهت تکثیر جویا شود. به طور پیش‌فرض فاصله زمانی بین دو polling در تکثیر درون سایتی یکبار در ساعت است که البته امکان تغییر آن وجود دارد ولی توصیه نمی‌شود.
برای این کار در پنجره properties شیء ارتباط روی Change Schedule کلیک می‌کنیم.
اگر سرور بالایی به درخواست‌های مکرر سرور پایینی جوابی ندهد سرور پایینی KCC را با هدف بررسی توپولوژی تکثیر اجرا می‌کند.
اگر سرور بالایی واقعا در دسترس نباشد توپولوژی تکثیر سایت بازسازی می‌شود.

سایت لینک‌ها

KCC فرض می‌کند همه DC ها به هم دسترسی دارند. همچنین یک توپولوژی تکثیر درون‌سایتی می‌سازد. به هر حال بین سایت‌ها می‌توانیم مسیر شبکه را که روی آن تکثیر اتفاق می‌افتد شیء سایت لینک بسازیم. یک سایت لینک حاوی دو یا چند سایت است.
ISTG به عنوان جزئی از KCC در هر سایت اشیاء ارتباط بین سرورها را می‌سازد که تکثیر بین سایتی فعال شود.
معمولا سایت لینک‌ها درست درک نمی‌شوند و نکته مهم این است که به خاطر داشته باشیم سایت لینک نمایانگر یک مسیر قابل دسترس برای تکثیر است. یک سایت لینک تنها نمی‌تواند مسیرهای شبکه مورد استفاده را کنترل کند. وقتی یک سایت لینک می‌سازیم و سایت‌ها را به آن اضافه می‌کنیم در واقع به Active Directory می‌گوییم می‌تواند بین هر کدام از این سایت‌ها تکثیر را انجام دهد.
ISTG اشیاء ارتباط می‌سازد و این اشیاء مسیر واقعی تکثیر را تعریف می‌کند. اگرچه توپولوژی تکثیر ساخته شده توسط ISTG به طور موثری Active Directory را تکثیر می‌کند ممکن است کارایی لازم را در توپولوژی شبکه ما نداشته باشد.
مثالی در این ارتباط مساله را روشن می‌کند. هنگام ایجاد forest یک شیء سایت لینک ساخته می‌شود.
DEFAULTIPSITELINK . به طور پیش‌فرض هر سایت جدیدی که اضافه می‌شود با این شیء عجین می‌شود. سازمانی را با یک مرکز داده در دفتر مرکزی و سه شعبه در نظر بگیرید. هر سه شعبه به مرکز داده با یک لینک اختصاصی متصل می‌شوند. ما برای هر شعبه یک سایت می‌سازیم. یکی Seattle (SEA)، Amsterdam (AMS) و Beijing (PEK). توپولوژی سایت و شبکه در شکل ۱۱- ۱۱ نمایش داده شده است.



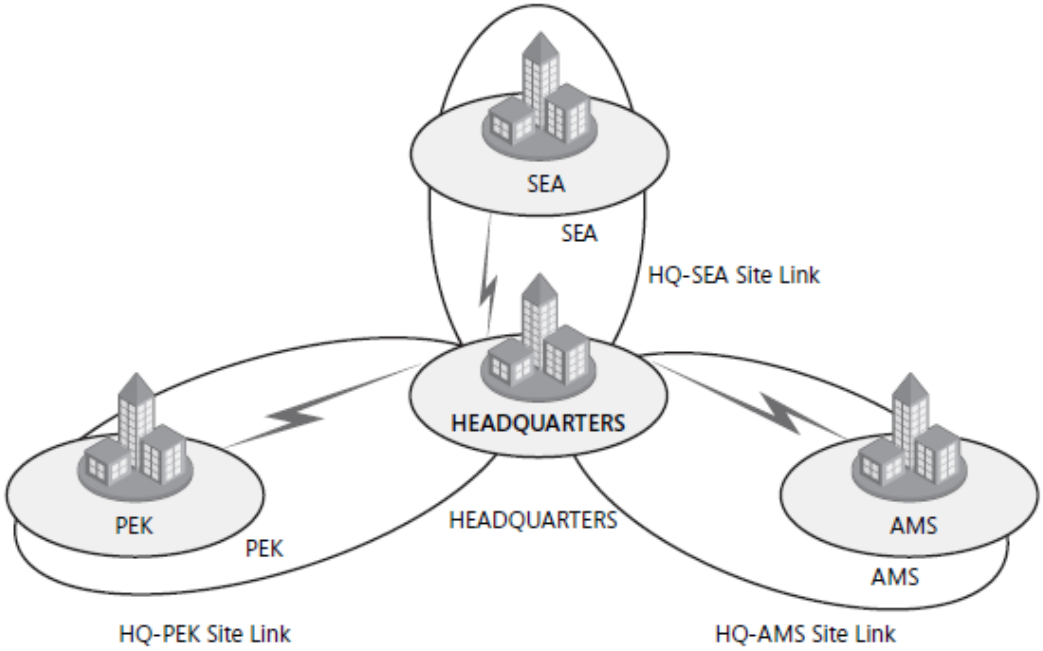
شکل ۱۱- ۱۱ توپولوژی شبکه و یک سایت لینک منفرد

به دلیل اینکه هر چهار سایت در یک سایت لینک قرار دارند Active Directory را طوری پیکربندی می‌کنیم که همه سایت‌ها بتوانند با یکدیگر تکثیر داشته باشند. یعنی امکان این وجود دارد که داده Amsterdam روی Seattle ، Beijing روی Amsterdam و دفتر مرکزی روی Beijing تکثیر شود. در بسیاری از این مسیرهای تکثیر ترافیک تکثیر از شعبه‌ای به شعبه دیگر از مسیر دفتر مرکزی می‌گذرد. با داشتن یک سایت لینک منفرد نمی‌توانیم توپولوژی تکثیر hub-and-spoke داشته باشیم حتی اگر توپولوژی شبکه ما hub-and-spoke باشد.

بنابراین پیشنهاد می‌گردد سایت لینک‌ها را که منعکس کننده توپولوژی فیزیکی شبکه است به صورت دستی بسازیم. در ادامه مثال قبلی ما سه سایت لینک می‌سازیم:

- HQ-AMS شامل سایت‌های دفتر مرکزی و آمستردام
- HQ-SEA شامل سایت‌های دفتر مرکزی و سیاتل
- HQ-PEK شامل سایت‌های دفتر مرکزی و پکن

سپس DEFAULTIPSITELINK را حذف می‌کنیم. توپولوژی نهایی به صورت شکل ۱۲- ۱۱ خواهد بود.



شکل ۱۲- ۱۱ توپولوژی شبکه با سه سایت لینک

پس از ساخت این سایت لینک‌ها ISTG از توپولوژی برای ساخت یک توپولوژی تکثیر بین‌سایتی متصل به همه سایت‌ها استفاده می‌کند. اشیاء ارتباط به منظور پیکربندی مسیرهای تکثیر بین‌سایتی ایجاد خواهد شد. این اشیاء به طور خودکار ایجاد شده ولی می‌توان آنها را به طور دستی ایجاد کرد. سناریوهای اندکی وجود دارد که نیازمند ساخت دستی اشیاء ارتباط بین‌سایتی می‌باشد.

پروتکل‌های انتقال داده تکثیرشده

در ابزار Active Directory Sites and Services می‌بینیم که سایت لینک‌ها در یک container به نام IP قرار دارند و خود IP نیز در container دیگری به نام Inter-Site Transports جای دارد. تغییرات بین DC ها توسط یکی از دو پروتکل زیر تکثیر می‌شود:

- **Directory Service Remote Procedure Call (DS-RPC)** DS-RPC در ابزار Active Directory Sites and Services با عنوان IP ظاهر می‌شود که برای کل تکثیر درون‌سایتی به کار می‌رود و به طور پیش‌فرض و ترجیحا پروتکل تکثیر بین‌سایتی است.

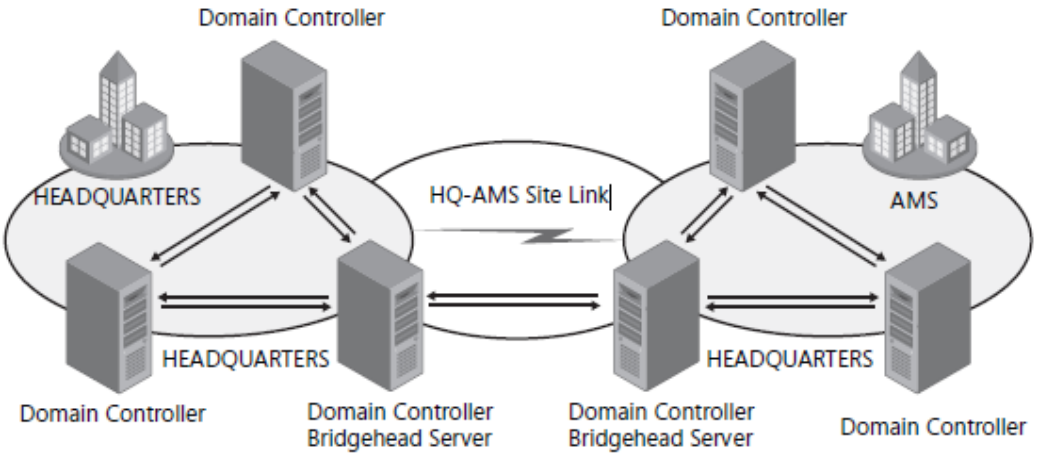
- **Inter-Site Messaging – Simple Mail Transport Protocol (ISM-SMTP)** که به طور خلاصه SMTP نیز خوانده می‌شود پروتکلی است که فقط زمانی استفاده می‌شود که ارتباط شبکه بین سایت‌ها متزلزل بوده یا همیشه برقرار نیست.

به طور کل می‌توان فرض کرد IP برای همه نوع تکثیر بین‌سایتی استفاده می‌شود. سازمان‌های محدودی از SMTP استفاده می‌کنند به دلیل اینکه بار کاری مدیر شبکه برای پیکربندی و مدیریت یک certificate authority (CA) خیلی زیاد می‌شود و تکثیر SMTP برای domain naming context پشتیبانی نمی‌شود. یعنی اگر یک سایت از SMTP برای تکثیر روی بقیه شبکه استفاده کند آن سایت باید دامنه خود باشد.

سرورهای Bridgehead

وظیفه ISTG ایجاد توپولوژی تکثیر بین سایت‌ها روی یک سایت لینک می‌باشد. برای بالا بردن کارایی تکثیر می‌توان یکی از DC ها را به عنوان سرور bridgehead انتخاب کنیم. این سرور مسئول همه تکثیرها به سمت داخل یا خارج سایت برای یک پارتیشن خاص می‌باشد. برای مثال اگر یک سایت مرکز داده دارای ۵ DC باشد یکی از آنها می‌تواند سرور bridgehead برای domain naming context باشد. همه تغییرات ایجاد شده روی پارتیشن دامنه در مرکز داده روی همه DC های سایت تکثیر خواهد شد. وقتی تغییر به سرور bridgehead برسد این تغییرات روی سرورهای bridgehead شعبات نیز تکثیر می‌شود که آنها هم تغییرات را روی DC های سایت‌های خودشان تکثیر می‌کنند. به همین منوال هر تغییری روی domain naming context در شعبات اتفاق بیافتد از سرورهای bridgehead آنجا تکثیر روی سرورهای bridgehead در مرکز داده انجام می‌شود که آنهم تغییرات را روی DC های دیگر مرکز داده تکثیر می‌کند. شکل ۱۳- ۱۱ تکثیر درون‌سایتی را در دو سایت و تکثیر بین‌سایتی را با استفاده از اشیاء ارتباط بین سرورهای bridgehead در سایت‌ها شرح می‌دهد.

به طور خلاصه سرور bridgehead سروری است که مسئول تکثیر تغییرات پارتیشن از سرورهای bridgehead سایت‌های دیگر است. روی این سرورها نیز عملیات pooling اتفاق می‌افتد.



شکل ۱۳- ۱۱ سایت‌ها، تکثیر درون‌سایتی، سرورهای bridgehead و تکثیر بین‌سایتی

سرورهای bridgehead به طور خودکار انتخاب می‌شوند و ISTG توپولوژی تکثیر درون‌سایتی را می‌سازد تا تغییرات به طور موثری بین سرورهای bridgehead دوسر سایت لینک تکثیر شود. سرورهای bridgehead برحسب پارتیشن انتخاب می‌شوند بنابراین امکان این وجود دارد که یک DC در یک سایت به عنوان bridgehead برای schema و DC دیگر برای پیکربندی انتخاب شوند. ولی معمولا می‌بینیم که یک DC سرور bridgehead برای همه پارتیشن‌های یک سایت می‌باشد مگر اینکه DC هایی در دامنه‌های دیگر یا پارتیشن‌های دایرکتوری برنامه دیگر وجود داشته باشند که در این صورت سرورهای bridgehead برای آن پارتیشن‌ها انتخاب خواهند شد.

سرورهای bridgehead با ترتیب اولویت

می‌توانیم یک یا چند سرور bridgehead با ترتیب اولویت داشته باشیم. برای نامزد کردن یک DC به عنوان سرور bridgehead با اولویت بالا پنجره properties شیء سرور را در ابزار Active Directory Sites And Services باز کرده و پروتکل transport را انتخاب کرده که تقریبا همیشه IP می‌باشد و روی Add کلیک می‌کنیم.

امکان پیکربندی بیش از یک سرور bridgehead برای یک سایت وجود دارد ولی از بین آنها فقط یکی انتخاب و به عنوان bridgehead استفاده می‌شود. اگر این سرور از شبکه خارج شود یکی از سرورهای دیگر مورد استفاده قرار خواهد گرفت.

مهم است که بدانیم اگر بیش از یک سرور را به عنوان bridgehead مشخص کنیم و هیچ‌کدام از آنها در دسترس نباشند هیچ سرور دیگری به طور خودکار انتخاب نخواهد شد و تکثیر در سایت اتفاق نخواهد افتاد. در شرایط ایده‌آل ما نباید سرورهای bridgehead با ترتیب اولویت را پیکربندی کنیم. بهرحال نگرانی از کارایی ممکن است ما را مجبور کند سروری را که دارای منابع سخت‌افزاری بهتری است به عنوان سرور bridgehead در نظر بگیریم. مسائل مربوط دیوار آتش ممکن است باعث شود یک سرور منفرد را به عنوان bridgehead انتخاب کنیم تا اینکه به Active Directory اجازه دهیم آنرا انتخاب کند که آن هم احتمالا در هر زمان یکی را انتخاب کند.

پیکربندی تکثیر بین‌سایتی

پس از ساخت سایت لینک‌ها و تولید اشیاء ارتباط توسط ISTG برای تکثیر پارتیشن‌ها بین سرورهای bridgehead دو طرف یک سایت لینک کار شبکه به اتمام رسیده است. در بسیاری از شبکه‌ها خصوصا در شبکه‌های با توپولوژی‌های straightforward سایت لینک‌ها ممکن است برای مدیریت تکثیر بین‌سایتی کافی باشند. در شبکه‌های پیچیده‌تر می‌توانیم اجزاء اضافی و ویژگی‌های تکثیر را پیکربندی کنیم.

انتقال‌پذیری سایت لینک

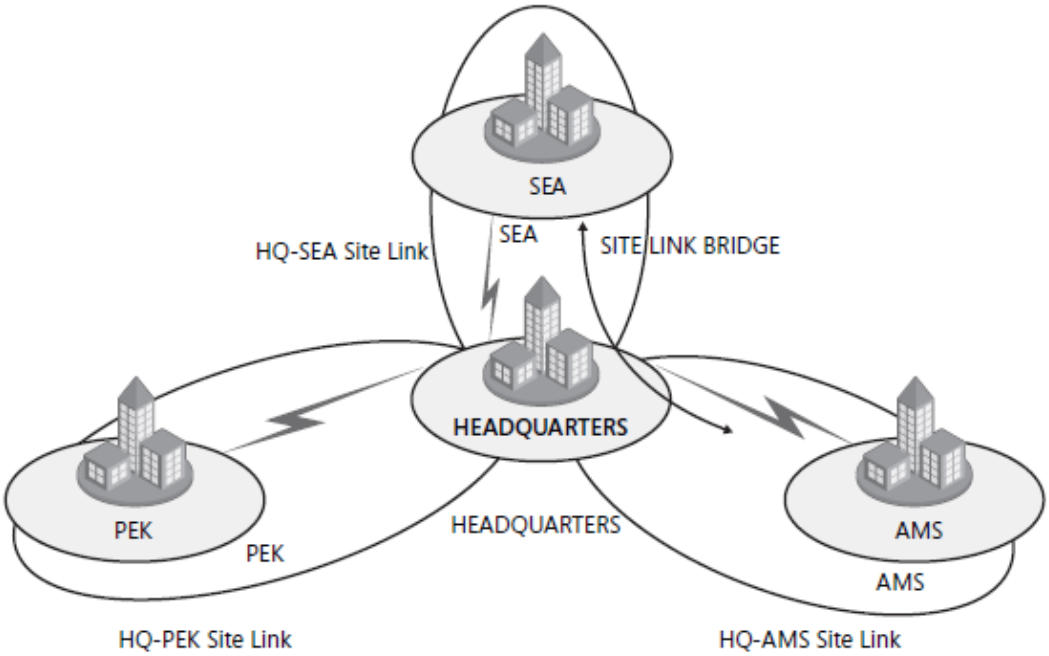
به طور پیش‌فرض سایت لینک‌ها انتقال‌پذیر هستند. یعنی در ادامه مثال قبلی اگر سایت‌های آمستردام و دفتر مرکزی به هم متصل شوند و دفتر مرکزی با سیاتل هم لینک داشته باشد پس سایت‌های آمستردام و سیاتل با هم لینک انتقال دارند. معنی آن این است که فرض بر این اساس است که ISTG می‌تواند شیء ارتباط بین سرور bridgehead در سیاتل و یک سرور bridgehead در آمستردام بسازد و باز هم همان مساله توپولوژی شبکه hub-and-spoke تکرار می‌شود.

امکان غیرفعال کردن انتقال‌پذیری سایت لینک وجود دارد به این ترتیب که پنجره properties مربوط به IP transport را در Intersite Transports container باز کرده و گزینه Bridge All Site Links را از حالت انتخاب خارج می‌کنیم. البته قبل از انجام این کار اطلاعات لازم را درباره تکثیر از آدرس http://technet.microsoft.com به دست می‌آوریم.

پل‌های سایت لینک

یک پل سایت لینک دو یا چند سایت لینک را به هم متصل می‌کند که نتیجه لینک انتقال‌پذیر خواهد بود. پل‌های سایت لینک فقط زمانی مورد نیاز هستند که گزینه Bridge All Sites Links برای پروتکل transport از حالت انتخاب خارج شده باشد. به خاطر داشته باشید که انتقال‌پذیری سایت لینک به طور پیش‌فرض فعال است و پل‌های سایت لینک اثری ندارد.

شکل ۱۴- ۱۱ استفاده از یک پل سایت لینک را در یک forest که انتقال‌پذیری در آن غیرفعال شده است شرح می‌دهد. با ساخت یک پل سایت لینک AMS-HQ-SEA که شامل سایت لینک‌های HQ-AMS و HQ-SEA می‌باشد این دو سایت لینک انتقال‌پذیر می‌شوند بنابراین یک ارتباط با هدف تکثیر بین یک DC در آمستردام و یک DC در سیاتل برقرار می‌شود.

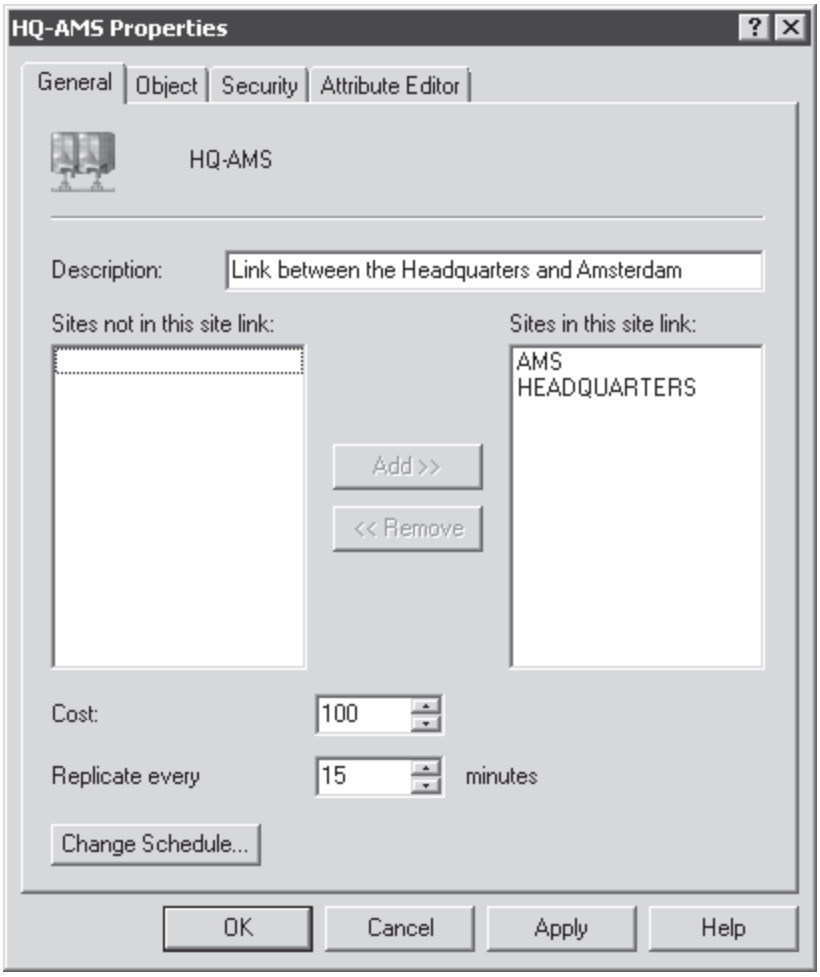


شکل ۱۴- ۱۱ پل سایت لینک که شامل دو سایت لینک HQ-AMS و HQ-SEA می‌باشد.

هزینه سایت لینک

هزینه‌های سایت لینک برای مدیریت جریان ترافیک مربوط به تکثیر، زمانی که بیش از یک مسیر برای این کار وجود دارد به کار می‌رود. ما م هزینه سایت لینک را برای این پیکربندی می‌کنیم که لینک سریع‌تر و بهتر را مشخص کنیم. لینک‌های کندتر دارای هزینه‌های بیشتر و لینک‌های سریع‌تر دارای هزینه‌های کمتر هستند. تکثیر معمولا از طریق لینک‌های با هزینه کمتر اتفاق می‌افتد.

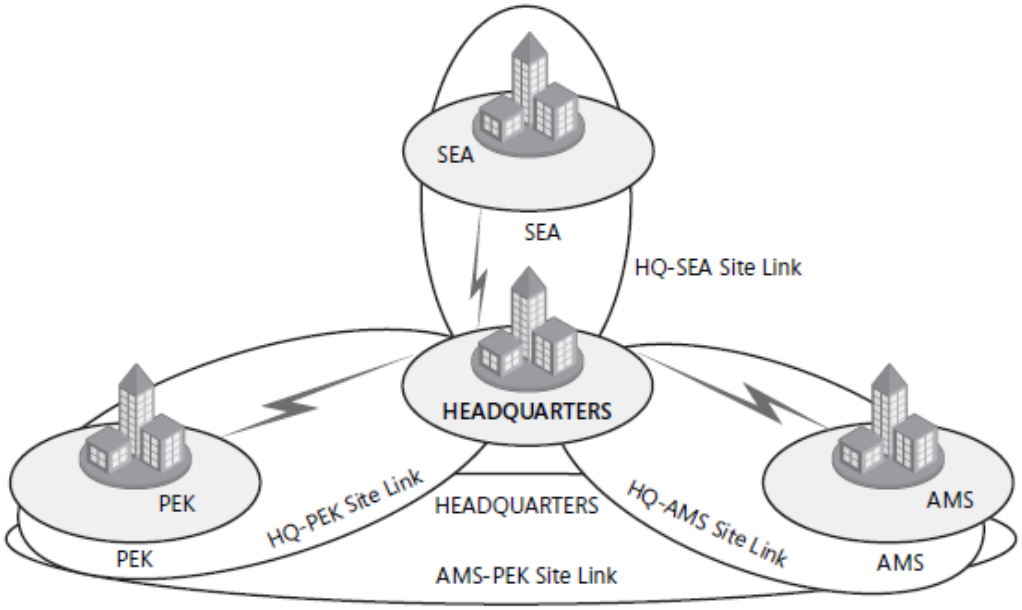
به طور پیش‌فرض همه سایت لینک‌ها با هزینه ۱۰۰ پیکربندی می‌شوند. برای تغییر هزینه سایت لینک همانند شکل ۱۵- ۱۱ پنجره Properties آنرا باز کرده و مقدار آنرا در کادر Cost عوض می‌کنیم.



شکل ۱۵- ۱۱ properties یک سایت لینک

با توجه به مثال استفاده شده در همین درس تصور کنید همانند شکل ۱۶- ۱۱ یک سایت لینک بین سایت‌های آمستردام و پکن ساخته شده است. چنین سایت لینکی می‌توانست در زمان از کار افتادن لینک‌های منتهی به دفتر مرکزی تکثیر را بین دو شعبه نام‌برده برقرار سازد و ما ممکن است جهت تحمل خرابی از چنین توپولوژی استفاده کنیم.

با مقدار هزینه ۱۰۰ انتساب داده شده به سایت لینک AMS-PEK ، Active Directory تغییرات را به طور مستقیم روی همین لینک تکثیر می‌کند. اگر این هزینه ۳۰۰ شود تغییر ابتدا از آمستردام روی دفتر مرکزی و بعد از روی دفتر مرکزی روی پکن تکثیر می‌شود. جمع این دو هزینه ۲۰۰ شده که در مقایسه با هزینه لینک مستقیم (۳۰۰) بهتر است.



شکل ۱۶- ۱۱ سایت لینک‌ها و هزینه‌ها

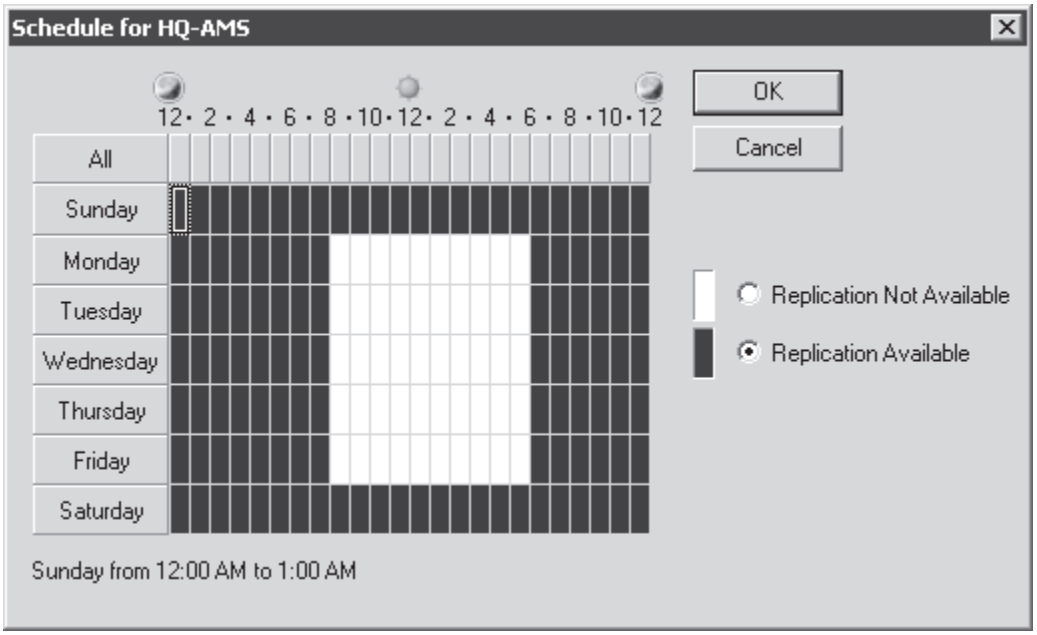
تعدد تکثیر

تکثیر بین‌سایتی فقط متکی به polling است و هیچ اطلاع‌رسانی وجود ندارد. به طور پیش‌فرض یک سرور bridgehead هر سه ساعت یکبار از سرور بالایی تغییرات را جویا می‌شود. این فاصله زمانی تکثیر برای سازمان‌هایی که نیاز به سرعت تکثیر بیشتر دارند خیلی طولانی است. ما می‌توانیم فاصله زمانی polling را برای هر سایت لینک تغییر دهیم. پنجره properties سایت لینک را مطابق ۱۵- ۱۱ باز کرده و مقدار را در کادر Replicate Every تغییر می‌دهیم.

حداقل فاصله زمانی polling ۱۵ دقیقه است. این یعنی تکثیر تغییر ایجاد شده در دایرکتوری در یک سایت با استفاده از پیکربندی پیش‌فرض تکثیر Active Directory روی DC های سایت‌های دیگر دقایقی طول می‌کشد.

زمان‌بندی تکثیر

به طور پیش‌فرض تکثیر ۲۴ ساعت شبانه روز اتفاق می‌افتد. ولی می‌توانیم تکثیر بین‌سایتی را با تغییر خصیصه زمان‌بندی سایت لینک به دفعات مشخص محدود کنیم. پنجره properties یک سایت را باز می‌کنیم و روی دکمه Change Schedule کلیک می‌کنیم. با استفاده از کادر محاوره‌ای Schedule For که در شکل ۱۷- ۱۱ نشان داده شده است می‌توانیم زمانهایی را که لینک برای تکثیر در دسترس است مشخص کنیم. لینک مشاهده شده در شکل از ۸ صبح تا ۶ بعدازظهر دوشنبه تا جمعه تکثیر نمی‌شود.



شکل ۱۷- ۱۱ زمان‌بندی سایت لینک

هنگام تعیین زمان‌بندی استفاده از لینک باید مراقب باشیم. امکان این وجود دارد که پنجره زمان‌بندی هم‌پوشانی نداشته باشد که در این نقطه تکثیر اتفاق نمی‌افتد. معمولا پیشنهاد نمی‌شود دسترسی لینک پیکربندی شود. اگر نیاز به زمان‌بندی لینک ندارید گزینه Ignore Schedules را در پنجره properties مربوط به پروتکل IP transport انتخاب کنید. این گزینه باعث می‌شود هر زمان‌بندی برای دسترسی سایت لینک چشم‌پوشی شود و ۲۴ ساعته تکثیر انجام شود.

مانیتورکردن تکثیر

پس از پیاده‌سازی پیکربندی تکثیر باید بتوانیم تکثیر را از لحاظ پیشرفت، بهینه‌سازی و عیب‌یابی مانیتور کنیم. دو ابزار مخصوصا برای گزارش‌گیری و تحلیل تکثیر مفید هستند. یکی ابزار Replication Diagnostics (Repadmin.exe) و دیگری Directory Server Diagnosis (Dcdiag.exe). در این درس این ابزارهای قدرتمند معرفی می‌شوند.

Repadmin.exe

دستوری است که به ما اجازه می‌دهد از وضعیت تکثیر روی هر DC گزارش تهیه کنیم. اطلاعات به دست آمده از این دستور به ما کمک می‌کند مشکلات را قبل از وقوع شناسایی کنیم و مشکلات به وجود آمده را در مورد تکثیر در forest عیب‌یابی کنیم. می‌توانیم سطوح مختلف جزئیات را تا متاداده تکثیر برای یک شیء یا خصیصه مشخص ببینیم. این به ما امکان می‌دهد زمان و مکان بروز تغییری که باعث مشکل شده دریابیم. حتی می‌توانیم از دستور برای ساخت توپولوژی تکثیر و اجباری کردن تکثیر بین DC ها استفاده کنیم. این دستور از تعدادی دستور که عملیات خاصی انجام می‌دهند پشتیبانی می‌کند. برای دریافت اطلاعات بیشتر درباره هر دستور تایپ می‌کنیم repadmin /?:command . بیشتر دستورات نیاز به پارامتر دارند. بسیاری از دستورات پارامتر DSA_LIST را دارند که برچسب شبکه (DNS یا نام NetBIOS یا آدرس IP) یک DC می‌باشد. برخی عملیات مانیتورینگ تکثیر با این دستور انجام می‌شود:

- **نمایش سرور مقابل تکثیر برای یک DC** برای نمایش ارتباط تکثیر یک DC دستور repadmin /showrepl DSA_LIST را تایپ می‌کنیم. به طور پیش‌فرض دستور Repadmin.exe فقط ارتباطات بین‌سایتی را نمایش می‌دهد. پارامتر repsto/ را با هدف نمایش ارتباطات بین‌سایتی اضافه می‌کنیم.

- **نمایش اشیاء ارتباط برای یک DC** برای این کار دستور repadmin /showconn DSA_LIST را تایپ می‌کنیم.

- **نمایش متاداده شیء خصیصه‌های آن و تکثیر** با بررسی یک شیء روی دو DC مختلف می‌توانیم چیزهای زیادی درباره تکثیر یاد بگیریم. می‌توانیم بفهمیم کدام خصیصه‌ها تکثیر شده اند و کدام‌ها نشده‌اند. دستور repadmin /showobjmeta DSA_LIST Object راتایپ می‌کنیم و به جای DSA_LIST ، نام DC یا DC ها را تایپ می‌کنیم. (می‌توانیم از علامت ستاره * برای تعیین تمامی DC ها استفاده کنیم.) Object یک مشخصه انحصاری برای شیء می‌باشد مثلا DN یا GUID شیء.

همچنین می‌توانیم زیرساخت تکثیر را توسط این دستور تغییر دهیم. برخی عملیات مدیریتی عبارتند از:

- **اجرای KCC** دستور repadmin /kcc را برای مجبور کردن KCC به منظور محاسبه مجدد توپولوژی تکثیر از بیرون به داخل یک سرور تایپ می‌کنیم.

- **اجباری کردن تکثیر بین دو سرور** از این دستور برای اجبار کردن تکثیر پارتیشن بین DC مبدا و مقصد استفاده می‌شود. برای این کار تایپ می‌کنیم: repadmin /replicate Destination_DSA_List Source_DSA_Name Naming_Context.

- **یکسان کردن دایرکتوری یک DC با DC های دیگر** برای هماهنگ کردن DC با DC های دیگر حتی در سایت‌های دیگر تایپ می‌کنیم repadmin /syncall DSA /A /e .

Dcdiag.exe

این دستور بررسی‌هایی روی سلامت کلی پروسه تکثیر و امنیت AD DS انجام می‌دهد. اجرای خالی دستور بررسی مختصری انجام داده و گزارش نتایج را نمایش می‌دهد. اجرای دستور به شکل Dcdiag.exe /c تقریبا تمام بررسی‌ها را انجام می‌دهد. خروجی تست را می‌توان در فایل با انواع مختلف مانند XML ذخیره کرد.

با اجرای دستور به همراه پارامتر /test:Test Name می‌توانیم تست مشخصی را انجام دهیم. تست‌هایی که مستقیما به تکثیر مربوط می‌شوند عبارتند از :

- **FrsEvent** همه خطاهای اجرا را در سیستم تکثیر فایل (FRS) گزارش می‌دهد.
- **DFSREvent** همه خطاهای اجرا را در سیستم تکثیر DFS (DFS-R) گزارش می‌دهد.
- **Intersite** خطاهایی را که منجر به توقف یا تاخیر تکثیر بین‌سایتی می‌شود بررسی می‌کند
- **KccEvent** خطاهای KCC را تشخیص می‌دهد.
- **Replications** تکثیر به موقع را بین DC ها بررسی می‌کند.
- **Topology** بررسی می‌کند که آیا توپولوژی تکثیر برای همه DSA ها کامل است یا نه
- **VerifyReplicas** بررسی می‌کند که آیا همه پارتیشن‌های دایرکتوری برنامه به طور کامل روی همه DC های میزبان replica اجرا شده است یا نه.

تمرینات پیکربندی تکثیر

در این تمرینات فرآیند تکثیر درون سایتی و بین سایتی را مدیریت خواهیم کرد. قبل از انجام این تمرینات باید تمرینهای درس دوم را انجام داده باشیم

تمرین اول ساخت یک شیء ارتباط

بین یک DC که به عنوان standby operations master و DC ای که در حال حاظر نقش operations master را دارد تکثیر مستقیم را پیکربندی می‌کنیم. سپس اگر operations master کنونی دچار مشکلی شد، سرور standby operations master با نقش operations master تا حد امکان بروز خواهد بود. در این تمرین یک شیء ارتباط بین SERVER01 و SERVER02 خواهیم ساخت که در این ارتباط SERVER02 که به عنوان standby operations master می باشد از SERVER01 که به عنوان operations master کنونی می باشد، تکثیر خواهد کرد.

۱- با اعتبار Administrator وارد SERVER01 می شویم
۲- ابزار Active Directory Sites And Services را باز می کنیم
۳- گره sites ، HEADQUARTERS ، Servers و SERVER02 را باز می کنیم
۴- گره NTDS Settings در زیر SERVER02 در کنسول را انتخاب می کنیم
۵- روی NTDS Settings راست کلیک کرده و New Active Directory Domain Services Connection را انتخاب می کنیم
۶- در کادر محاوره ای Find Active Directory Domain Controllers ، SERVER01 را انتخاب کرده و روی OK کلیک می کنیم. چون KCC قبلا یک ارتباط از SERVER01 به SERVER02 ساخته است، پیغامی ظاهر می شود که آیا می خواهید یک ارتباط دیگر بسازید.
۷- روی Yes کلیک می کنیم

۸- در کادر محاوره ای New Object – Connection نام SERVER01 – OPERATIONS MASTER را نوشته و روی OK کلیک می کنیم
۹- روی new connection object در پنجره وسط ، راست کلیک کرده و Properties را انتخاب می کنیم
۱۰- اطلاعات Properties را بدون هیچ گونه تغییر بررسی می کنیم. چه پارتیشن‌هایی از SERVER01 تکثیر می شوند؟ آیا SERVER02 یک سرور GC است؟
۱۱- برای بستن کادر محاوره ای Properties روی OK کلیک می کنیم
۱۲- چون این دامنه ساده تنها دو DC دارد و قرار است در تمرین بعد سرور را منتقل کنیم، با راست کلیک کردن روی connection object و انتخاب Delete آنرا پاک می کنیم

تمرین دوم ساخت سایت لینک

در این تمرین بین دو سایت دفتر مرکزی و یکی از شعبه ها یک سایت لینک می‌سازیم.

۱- در ابزار Active Directory Sites And Services گره Inter-Site Transports را باز می کنیم
۲- گزینه IP را انتخاب می کنیم
۳- روی DEFAULTIPSITELINK راست کلیک کرده و Rename را انتخاب می کنیم
٤- عبارت HQ-BRANCHA را نوشته و Enter را فشار می دهیم
٥- روی HQ-BRANCHA دوبار کلیک می کنیم
٦- در لیست Sites In This Site Link ، BRANCHB را انتخاب کرده و روی Remove و بعد OK کلیک می کنیم
۷- روی IP راست کلیک کرده و New Site Link را انتخاب می کنیم
۸- در کادر نام عبارت HQ-BRANCHB را تایپ می‌کنیم.
۹- در لیست Sites Not In This Site Link ، Headquarters را انتخاب کرده و روی Add کلیک می کنیم
۱۰- در لیست Sites Not In This Site Link ، BRANCHB را انتخاب کرده و روی Add کلیک می کنیم
۱۱- روی OK کلیک می کنیم

تمرین سوم تعیین سرور Preferred Bridgehead

می توانیم برای سایت خود یک Preferred Bridgehead Server تعیین کنیم تا در فرآیند تکثیر از سایت و به سایت به ما کمک کند. این کار زمانی که می خواهیم این نقش را به یک DC در یک site با منابع سیستمی بیشتر بدهیم و یا در جایی که تنظیمات دیواره آتش نیازمند آن است که این نقش به یک DC مشخص و ثابت سپرده شود، بسیار مفید خواهد بود. در این تمرین برای سایت یک Preferred Bridgehead Server تعیین می کنیم.

۱- گره Headquarters ، Servers و SERVER02 را باز می کنیم
۲- روی SERVER02 راست کلیک کرده و Properties را انتخاب می کنیم
۳- در لیست Transports Available For Inter-Site Data Transfer ، IP را انتخاب می کنیم
٤- روی Add و سپس OK کلیک می کنیم

توصیه می شود که اگر در سایت سرورGC داریم همان سرور را به عنوان preferred bridgehead server تعیین کنیم هنگامی که Active Directory به صورت اتوماتیک bridgehead server را تعیین می کند در صورت وجود سرور GC ، آنرا به عنوان bridgehead server انتخاب می کند

تمرین چهارم پیکربندی تکثیر بین سایت ها

بعد از ساخت سایت لینک و (در صورت تمایل) تعیین bridgehead servers می توانیم کنترل و بهینه سازی تکثیر را با پیکر بندی خصوصیات سایت لینک در این تمرین ادامه دهیم. با این کار علاوه بر کاهش polling frequency تکثیر بین site ها ، هزینه سایت لینک را نیز کاهش خواهیم داد.

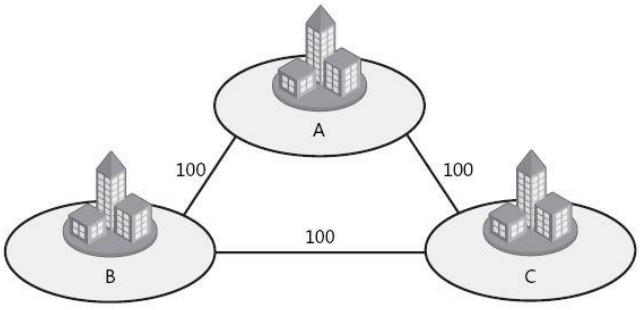
۱- گره Inter-Site Transports را باز می کنیم
۲- IP container را در کنسول انتخاب می کنیم
۳- روی سایت لینک HQ-BRANCHA دوبار کلیک می کنیم
۴- در کادر Replicate Every عدد ۱۵ را تایپ می کنیم
۵- روی سایت لینک HQ-BRANCHB دوبار کلیک می کنیم
۶- در کادر Replicate Every عدد ۱۵ را تایپ می کنیم
۷- روی دکمه Change Schedule کلیک می کنیم
۸- کادر محاوره ای Schedule For HQ-BRANCHB را بررسی می کنیم. تغیر زمانبندی را امتحان کنیم اما هنگامی که کارمان تمام شد روی Cancel کلیک می کنیم
۹- در کادر Cost عدد ۲۰۰ را تایپ می کنیم
۱۰- روی OK کلیک می کنیم

خلاصه درس

- Connection objects مسیر تکثیر بین دو DC را مشخص می کند
- سایت لینک‌ها ارتباط شبکه بین دو سایت را مشخص می کنند
- Bridgehead server در هر سایت مسئول تکثیر از، و به سایت می باشد
- The intersite topology generator (ISTG) بین Bridgehead server هایی که از یک سایت لینک مشترک استفاده می کنند ، شیء ارتباط می سازد
- اگر چندین ارتباط در دسترس باشد، فرآیند تکثیر از طریق ارتباطی که کمترین cost را دارد انجام می شود
- بصورت پیش فرض سایت لینک‌ها transitive هستند. اگر این خاصیت را با پاک کردن گزینه Bridge All Site Links در properties، intersite transport protocol غیر فعال کنیم ، ممکن است برای ساخت transitive link های بخصوص بین دو یا چند سایت نیازمند ساخت site link bridge باشیم

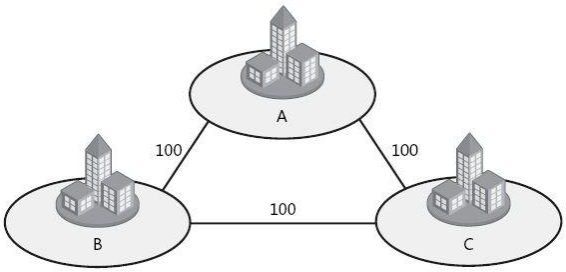
سئوالات پایان درس

۱- فرض کنید مدیر شبکه Adventure Works هستیم. Active Directory forest ما دارای سه سایت با نامهای A ، B و C می باشد. سایتA و سایتC با یک ارتباط پر سرعت به سایت B متصل هستند و بوسیله یک ارتباط کند VPN به یکدیگر متصل هستند. شیء سایت لینک و هزینه آنها در شکل نشان داده شده است. می خواهیم از تکثیر از طریق ارتباط VPN جلوگیری کنیم. چه باید بکنیم؟



A . زیاد کردن هزینه لینک A-B به ۲۵۰
B . زیاد کردن هزینه لینک C-B به ۲۵۰
C . کم کردن هزینه لینک‌های A-B و C-B به ۷۵
D . زیاد کردن هزینه لینک A-C به ۲۵۰

۲- فرض کنید به عنوان مدیر شبکه در Adventure Works کار می‌کنیم. Active Directory forest ما دارای سه سایت با نامهای A ، B و C می باشد. اشیاء سایت لینک و هزینه آنها در شکل نشان داده شده است. می خواهیم مطمئن شویم که تمام تکثیر های بین سایت A و سایت C قبل از رفتن به سایت‌های دیگر از سایت B بگذرد چه باید بکنیم؟ ؟(در صورت نیازتمام گزینه های درست را انتخاب کنید. هر پاسخ صحیح بخشی از راه حل است)



A . زیاد کردن هزینه سایت لینک A-C به ۳۰۰

B . حذف سایت لینکA-C

C . غیر فعال کردن Bridge All Site Links

D . کم کردن هزینه لینک‌های A-B وB-C به ۲۵

۳- زیرساخت شبکه در شرکت Trey Research بصورت ارتباط مستقیم IP بین مرکز داده و کشتی تحقیقاتی در دریا می باشد. برای تکثیر بین مرکز داده و کشتی چه باید کرد؟

A . ایجاد یک دامنه جدید برای کشتی در forest

B . کم کردن هزینه برای سایت لینک حاوی دفتر مرکزی و کشتی

C . پیکربندی یک DC در کشتی بصورت preferred bridgehead server

E . ساخت یک شیء ارتباط به صورت دستی بین DC کشتی و DC دفتر مرکزی

۴- می خواهیم برای اطمینان از درست انجام شدن فرآیند تکثیر بین دو DC عملیات تکثیر را بصورت دستی بین آنها انجام دهیم. از کدام ابزار می توان استفاده کرد؟ ؟(در صورت نیازتمام گزینه های درست را انتخاب کنید.)

A . ابزار Active Directory Sites And Services

B . Repadmin.exe

C . Dcdiag.exe

D . ابزار Active Directory Domains And Trusts

فصل ۱۲

دامنه و forest

در فصل ۱ یاد گرفتیم AD DS اساس یک راه حل مدیریت identity and access را فراهم می‌کند و ساخت یک زیرساخت AD DS ساده را شامل یک forest و یک دامنه یاد گرفتیم. در فصل جاری با جزئیات مدیریت AD DS آشنا می‌شویم. حالا آماده هستیم به بالاترین سطح یک زیرساخت AD DS وارد شویم و مدل و عملکرد دامنه‌ها و forest را تصور کنیم. در این فصل یاد می‌گیریم که چطور سطوح عملیاتی دامنه و forest را در شبکه بالا ببریم و چطور زیرساخت AD DS بهینه را برای سازمان طراحی کنیم. چگونه اشیاء را بین دامنه‌ها و forest ها جابجا کنیم و چطور تایید هویت و دسترسی به منابع را بین چند دامنه و forest فعال کنیم.

اهداف امتحانی در این فصل:

- پیکربندی زیرساخت Active Directory
  - پیکربندی یک forest یا دامنه
  - پیکربندی trust

دروس این فصل:

- درس ۱: مفهوم سطوح عملیاتی دامنه و forest
- درس ۲: مدیریت شبکه‌ها با چند دامنه و ارتباطات trust

قبل از شروع

برای انجام تمرینات این فصل باید دو DC با نام‌های SERVER01 و SERVER02 در دامنه contoso.com بسازیم. فصل ۱ و فصل ۱۰ را برای یادآوری جزئیات ببینید.

درس ۱: مفهوم سطوح عملیاتی دامنه و forest

با افزودن DC های ویندوز سرور 2008 به دامنه خود می‌توانیم از مزایای جدید سرویس دایرکتوری Active Directory بهره‌مند شویم. سطوح عملیاتی دامنه و forest حالت‌های اجرایی دامنه و forest هستند. سطوح عملیاتی مشخص کننده نسخه‌های ویندوزی است که به عنوان DC استفاده می‌شود و ویژگی‌های بالفعل Active Directory می‌باشد.

بعد از این درس می‌توانیم:

- سطوح عملیاتی دامنه و forest را شرح دهیم.
- سطوح عملیاتی دامنه و forest را ارتقاء دهیم.
- قابلیت‌های ایجاد شده توسط سطوح امنیتی را شرح دهیم.

زمان تقریبی : ۴۵ دقیقه

مفهوم سطوح عملیاتی

سطوح عملیاتی مانند سوئیچ‌هایی هستند که قابلیت‌های جدید ارائه شده توسط نسخه‌های ویندوز را فعال می‌کنند. ویندوز سرور 2003 ویژگی‌های متعددی را به Active Directory می‌افزاید و ویندوز سرور 2008 به تکامل AD DS ادامه می‌دهد. این ویژگی‌ها با نسخه‌های قبلی سازگار نیستند بنابراین اگر DC با سیستم عامل ویندوز سرور 2000 داشته باشیم نمی‌توانیم از ویژگی‌های ارائه شده توسط نسخه‌های بعدی ویندوز استفاده کنیم و این ویژگی غیرفعال می‌شود. به همین صورت تا زمانی که همه DC ها ویندوز سرور 2008 نداشته باشند نمی‌توانیم AD DS را ارتقاء دهیم. بالابردن سطوح عملیاتی شامل دو شرط اصلی است:

- همه DC ها باید دارای نسخه مناسب ویندوز سرور باشند.
- باید سطح عملیاتی را به صورت دستی ارتقاء دهیم به دلیل اینکه به طور خودکار انجام نمی‌شود.

سطوح عملیاتی دامنه

سطح عملیاتی دامنه روی ویژگی‌های Active Directory تاثیر داشته و نسخه‌های ویندوز مورد پشتیبانی DC ها در دامنه مشخص می‌کند. در نسخه‌های قبلی ویندوز سطوح عملیاتی دامنه و حالت‌ها از DC های ویندوز سرور NT 4.0 پشتیبانی می‌کردند. این پشتیبانی با ویندوز سرور 2008 به اتمام رسیده است و همه DC ها اکنون باید دارای سیستم عامل ویندوز سرور 2000 یا بالاتر باشند تا بتوانیم DC با ویندوز سرور 2008 به دامنه بیافزاییم. Active Directory ویندوز سرور 2008 از سه سطح عملیاتی پشتیبانی می‌کند:

- Windows 2000 Native
- Windows Server 2003
- Windows Server 2008

سطح عملیاتی Windows 2000 Native

این سطح عملیاتی پایین‌ترین سطحی است که DC ویندوز سرور 2008 پشتیبانی می‌کند. سیستم‌های عامل زیر در این سطح قابل قبول می‌باشند:

- ویندوز سرور 2000
- ویندوز سرور 2003
- ویندوز سرور 2008

اگر DC با ویندوز سرور 2000 یا 2003 در شبکه موجود باشد یا امکان افزودن این DC ها در آینده وجود دارد باید سطح دامنه را در این حد نگه داریم.

سطح عملیاتی Windows Server 2003

وقتی همه DC های ویندوز سرور 2000 را حذف کردیم یا ارتقاء دادیم سطح عملیاتی را می‌توانیم به Windows Server 2003 ارتقاء دهیم. در این سطح دامنه دیگر نمی‌تواند DC با سیستم عامل ویندوز سرور 2000 داشته باشد بنابراین همه DC ها باید یکی از ویندوزهای سرور 2003 یا 2008 را داشته باشند.

این سطح عملیاتی چند ویژگی جدید را به دامنه اضافه می‌کند که عبارتند از :

- **تغییرنام DC** ابزار مدیریت دامنه Netdom.exe جهت تغییرنام دامنه قابل استفاده است.
- **خصیصه lastLogonTimestamp** هنگام ورود کاربر یا کامپیوتر به دامنه خصیصه lastLogonTimestamp با زمان ورود به روز می‌شود. این خصیصه در دامنه تکثیر می‌شود.
- **خصیصه userPassword** واحدهای امنیتی در Active Directory شامل کاربران، کامپیوترها و گروهها است. کلاس شیء چهارم inetOrgPerson شبیه کاربر است و برای عجین شدن با سرویس دایرکتوری غیرمایکروسافتی به کار می‌رود. در سطح عملیاتی دامنه Windows Server 2003 می‌توانیم خصیصه userPassword را به عنوان کلمه عبور موثر روی اشیاء inetOrgPerson و user تنظیم کنیم.
- **تغییر مسیر container پیش‌فرض کاربر و کامپیوتر** در فصل ۵ یاد گرفتیم که از دستورات Redirusr.exe و Redircmp.exe برای تغییر مسیر container پیش‌فرض کاربر و کامپیوتر استفاده کنیم. این کار باعث می‌شود حساب جدید در یک OU دیگری غیر از container های Users و Computers ساخته شود.
- **سیاست‌های Authorization Manager** ابزاری است که اعتبارسنجی را برای برنامه‌ها فراهم می‌کند و می‌تواند سیاست‌های اعتبارسنجی را در AD DS ذخیره کند.
- **تفویض اختیار اجباری** برنامه‌ها می‌توانند از مزایای تفویض امن اعتبار کاربر به وسیله پروتکل تایید هویت Kerberos بهره‌مند شوند. تفویض را می‌توان طوری پیکربندی کرد که فقط به سرویس‌های خاصی مجوز داده شود.

- **تایید هویت انتخابی** در درس ۲ یاد می‌گیریم که چطور بین دامنه خود و دامنه‌های دیگر ارتباط trust ایجاد کنیم. تایید هویت انتخابی ما را قادر می‌سازد کاربران و گروههایی از دامنه یا forest مورد اعتماد را برای تایید هویت در forest خود مشخص کنیم.

سطح عملیاتی Windows Sever 2008

وقتی همه DC ها سیستم عامل ویندوز سرور 2008 داشته باشند و مطمئن باشیم در آینده نیز هیچ DC با سیستم عامل قبل از 2008 نخواهیم داشت می‌توانیم سطح عملیاتی دامنه را به Windows Server 2008 ارتقاء دهیم. این سطح عملیاتی از DC های با سیستم عامل ویندوز سرور 2008 پشتیبانی می‌کنند.

این سطح عملیاتی چهار ویژگی را در سطح دامنه به AD DS اضافه می‌کند:

- **DFS-R مربوط به SYSVOL** در فصل ۱۰ یاد گرفتیم SYSVOL را طوری پیکربندی کنیم که به جای FRS با DFS-R تکثیر شود. با DFS-R ، SYSVOL بسیار قوی‌تر و دقیق‌تر تکثیر می‌شود.

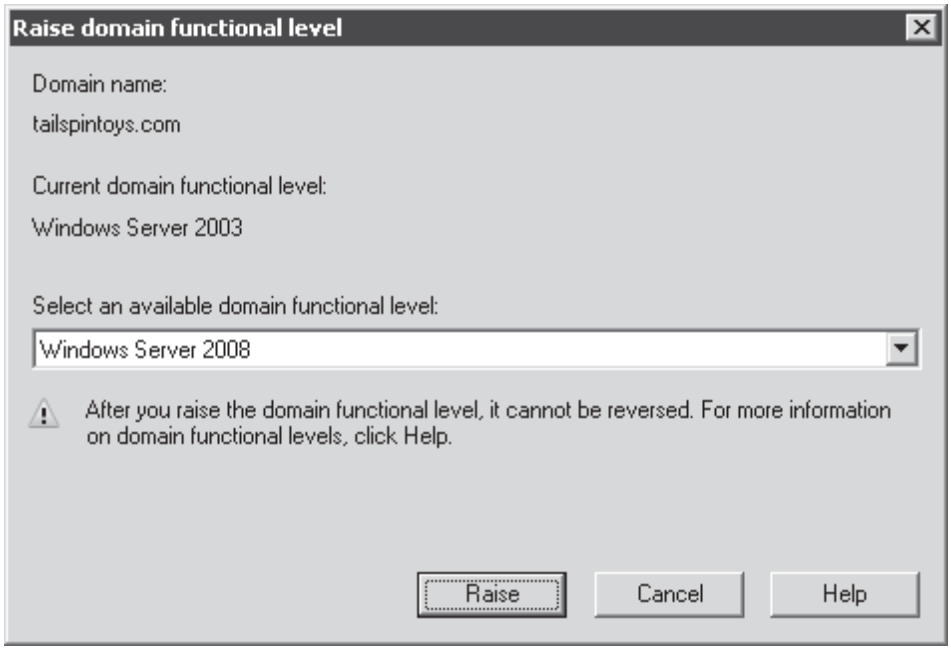
- **سرویس‌های رمزنگاری پیشرفته (AES)** امنیت تایید هویت با AES (Advanced Encryption Services 128و256) که با پروتکل Kerberos پشتیبانی می‌شود بالا می‌رود. AES جای الگوریتم رمزنگاری RC4-HMAC (Hash Message Authentication Code) را گرفته است.

- **اطلاعات آخرین ورود مستقیم به سیستم** وقتی کاربری به دامنه وارد می‌شود خصیصه‌های بسیاری از شیء کاربر مانند کامپیوتری که کاربر به آن وارد شده و تعداد دفعات تلاش ناموفق برای ورود پس از آخرین ورود موفق به روز می‌شوند.

- **سیاست‌های کلمه عبور Fine-Grained** در فصل ۸ درباره این سیاست‌ها یاد گرفتیم که ما را قادر می‌سازد سیاست‌های کلمه عبور انحصاری برای کاربران و گروهها در دامنه تعیین کنیم.

ارتقاء سطح عملیاتی دامنه

زمانی که همه DC ها نسخه مناسب ویندوز را دارا باشند و مطمئن باشیم در آینده از نسخه‌های قدیمی‌تر ویندوز برای DC ها استفاده نخواهیم کرد می‌توانیم سطح عملیاتی دامنه را ارتقاء دهیم. برای این کار ابزار Active Directory Domains And Trusts را باز کرده و روی دامنه کلیک راست کرده و Raise Domain Functional Level را انتخاب می‌کنیم. کادر محاوره‌ای مشابه شکل ۱-۱۲ امکان انتخاب سطح عملیاتی بالاتر را فراهم می‌کند.



شکل ۱- ۱۲ کادر محاوره‌ای Raise Domain Functional Level

نکته عملیات یک طرفه

ارتقاء سطح عملیاتی دامنه یک عملیات یک طرفه است. ما دیگر نمی‌توانیم سطح عملیاتی را به حالت قبلی برگردانیم.

راه دیگر ارتقاء استفاده از ابزار Active Directory Users And Computers است. روی دامنه کلیک راست کرده و Raise Domain Functional Level را انتخاب می‌کنیم. یا اینکه روی گره ریشه کلیک راست کرده و از منوی All Tasks گزینه Raise Domain Functional Level را انتخاب می‌کنیم.

سطوح عملیاتی forest

همانند سطح عملیاتی دامنه که عملکرد و سیستم‌های عامل DC را در سطح دامنه مشخص می‌کند سطح عملیاتی forest نیز عملکرد را در سطح forest مشخص می‌کند. Active Directory ویندوز سرور 2008 از سه سطح عملیاتی forest پشتیبانی می‌کند:

- Windows 2000
- Winsows Server 2003
- Windows Server 2008

این سطوح عملیاتی یک به یک شرح داده می‌شوند.

سطح عملیاتی Windows 2000

این سطح عملیاتی پایه و پیش‌فرض forest است. دامنه‌ها در این سطح عملیاتی می‌توانند هر سطح عملیاتی داشته باشند Windows 2000 Native ، Windows Server 2003 و Windows Server 2008 . ما می‌توانیم سطح عملیاتی forest را پس از اینکه همه دامنه‌ها به سطح عملیاتی معادل رسیدند ارتقاء دهیم.

سطح عملیاتی Windows Server 2003

پس از اینکه همه دامنه‌ها در forest به سطح عملیاتی Windows Server 2003 رسیدند و بدانیم در آینده هیچ DC با ویندوز سرور 2000 نخواهیم داشت می‌توانیم سطح عملیاتی forest را به Windows Server 2003 ارتقاء دهیم. در این سطح دامنه‌ها می‌توانند در یکی از سطوح زیر باشند:

- Windows Server 2003
- Windows Server 2008

در این سطح عملیاتی ویژگی‌های زیر فعال هستند:

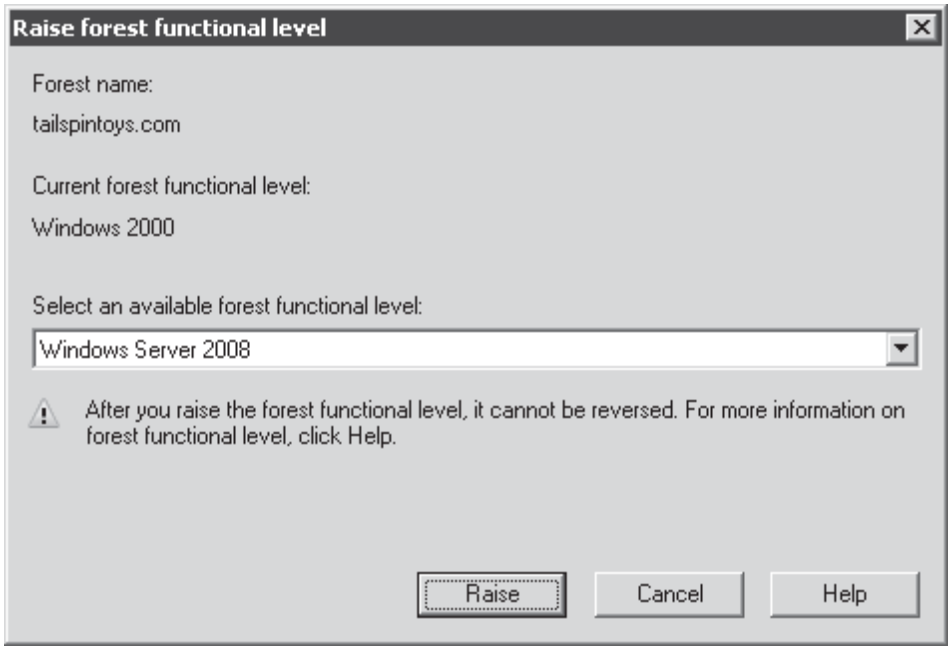
- **Forest trusts** در درس ۲ طریقه ساخت ارتباط trust بین forest ها را یاد می‌گیریم.
- **تغییر نام دامنه** می‌توانیم نام دامنه را در forest تغییر دهیم.
- **تکثیر Linked-Value** در سطح عملیاتی Windows 2000 تغییر در عضویت یک گروه منجر به تکثیر کل خصیصه چند مقداره member می‌شود. این مساله می‌تواند باعث افزایش ترافیک شبکه و هنگام تغییر همزمان آن در DC های مختلف از دست دادن اطلاعات بروز عضویت شود. همچنین محدودیت ۵۰۰۰ عضو برای یگ گروه را دارد. تکثیر linked-value در سطح عملیاتی Windows Server 2003 تغییر عضویت را منحصرا تکثیر می‌کند به جای آنکه کل خصیصه را تکثیر کند. این کار باعث می‌شود پهنای باند کمتری استفاده شود و از دست دادن اطلاعات بروز جلوگیری شود.
- **پشتیبانی از DC های فقط خواندنی** RODC ها در این سطح عملیاتی پشتیبانی می‌شوند ولی خود RODC باید دارای ویندوز سرور 2008 باشد.
- **الگوریتم‌های پیشرفته Knowledge Consistency Checker (KCC) و مقیاس‌پذیری** تولیدکننده توپولوژی بین‌سایتی (ISTG) از الگوریتم‌های پیشرفته‌ای استفاده می‌کند که AD DS را قادر به پشتیبانی از تکثیر در forest های دارای بیش از ۱۰۰ سایت می‌سازد. در سطح عملیاتی Windows Server 2000 باید برای ساخت توپولوژی تکثیر برای forest با صدها سایت باید به صورت دستی عمل کنیم. به علاوه با انتخاب ISTG از یک الگوریتم بسیار کاراتر استفاده می‌کنیم.
- **تبدیل اشیاء inetOrgPerson به اشیاء کاربر** ما می‌توانیم یک instance از شیء inetOrgPerson را که برای سازگاری با سرویس‌های غیرمایکروسافتی مشخصی استفاده می‌شود به یک instance از کلاس user تبدیل کنیم.
- **پشتیبانی از کلاس کمکی dynamicObject** این کلاس شیء توسط برنامه‌ها مورد استفاده قرار می‌گیرد.
- **پشتیبانی از گروه‌های applocation basic group و LDAP query group** این دو گروه جدید برای اعتبارسنجی مبتنی بر نقش در برنامه‌هایی که از Authorization Manager استفاده می‌کنند به کار می‌روند.
- **غیرفعال کردن و تعریف دوباره خصیصه‌ها و کلاس‌های شیء** اگرچه امکان حذف یک خصیصه یا کلاس شیء در schema در سطح عملیاتی Windows Server 2003 وجود ندارد ولی می‌توانیم آنها را غیرفعال کرده و یا دوباره تعریف کنیم.

سطح عملیاتی Windows Server 2008

این سطح عملیاتی ویژگی‌های سطح forest را افزایش نمی‌دهد. بهرحال پس از پیکربندی forest به این سطح، دامنه‌های جدید اضافه شده به forest به طور پیش‌فرض در این سطح عملیاتی کار خواهند کرد. در این سطح همه DC ها باید در سطح Windows Server 2008 باشند که یعنی همه DC ها دارای ویندوز سرور 2008 باشند.

ارتقاء سطح عملیاتی forest

از ابزار Active Directory Domains and Trusts برای ارتقاء سطح عملیاتی forest استفاده می‌شود. روی گره ریشه در ابزار Active Directory Domains And Trusts کلیک راست کرده و Raise Forest Functional Level را انتخاب می‌کنیم.



شکل ۲- ۱۲ کادر محاوره‌ای Raise Forest Functional Level

فقط زمانی سطح عملیاتی forest را ارتقاء می‌دهیم که مطمئن باشیم دامنه دیگری با سطح پایین‌تر از آن به forest افزوده نخواهد شد. پس از ارتقاء امکان برگشت وجود ندارد.

تمرینات ارتقاء سطوح عملیاتی دامنه و forest

در این تمرینات سطح عملیاتی دامنه و forest را ارتقا خواهیم داد. برای انجام این تمرینات باید حداقل یک DC در یک دامنه جدید و forest جدید با سیستم عامل ویندوز سرور 2008 داشته باشیم. این سرور که نام آن SERVERTST خواهد بود دارای پیکربندی زیر می باشد:

نام کامپیوتر : SERVERTST
آدرس IPv4 : 10.0.0.111
Subnet Mask : 255.255.255.0
Default Gateway : 10.0.0.1
DNS Server : 10.0.0.111

با اجرای Dcpromo.exe یک forest و یک دامنه جدید با نام tailspintoys.com می‌سازیم. سطح عملیاتی forest را روی Windows 2000 و سطح عملیاتی دامنه را روی Windows 2000 Native می گذاریم سرویس DNSرا روی سرور نصب می کنیم، پیام هشداری ظاهر می شود که به ما یادآوری می کند که سرور دارای IP پویاست. روی Yes کلیک می کنیم، همچنین هنگامی که به ما یادآوری می شود که DNS delegation را نمی توان انجام داد روی Yes کلیک می کنیم. در دامنه tailspintoys.com دو OU سطح اول با نامهای Clients و People می سازیم.

تمرین اول تجربه غیرفعال بودن قابلیت‌ها

در این تمرین مزیت قابلیتهایی را که سطوح عملیاتی دامنه بالاتر دارند تجربه می کنیم. در این تمرین خواهیم دید که این قابلیتها پشتیبانی نمی شوند.

۱- با اعتبار مدیر دامنه وارد SERVERTST می شویم
۲- پنجره خط فرمان را باز می کنیم
۳- عبارت redircmp.exe "ou=clients,dc=tailspintoys,dc=com" را نوشته و سپس Enter را فشار می دهیم

پنجره ای باز می شود و به ما اطلاع می دهد که فرآیند تغییر مسیر ناموفق بوده است، این به این خاطر است که باید سطح عملیاتی دامنه حداقل ویندوز سرور 2003 باشد.

٤- عبارت redirusr.exe "ou=people,dc=tailspintoys,dc=com" را نوشته و Enter را فشار می دهیم

پنجره ای باز می شود و به ما اطلاع می دهد که فرآیند تکثیر ناموفق بوده است، این به این خاطر است که باید سطح عملیاتی دامنه حداقل ویندوز سرور 2003 باشد.

٥- ابزار Active Directory Users And Computers را باز می کنیم

٦- روی منوی View کلیک کرده و Advanced Features را انتخاب می کنیم

٧- روی حساب Administrator در Users container دوبار کلیک می کنیم

٨- روی زبانه Attribute Editor کلیک می کنیم

٩- خصیصه lastLogonTimestamp را پیدا کرده و می بینیم که مقدار آن <not set> می باشد

تمرین دوم ارتقا سطح عملیاتی دامنه و forest

در این تمرین سطح عملیاتی دامنه tailspintoys.com را ارتقا خواهیم داد

١- Active Directory Domains And Trusts را باز می کنیم

٢- روی دامنه tailspintoys.com راست کلیک کرده و گزینه Raise Domain Functional Level را انتخاب می کنیم

٣- انتخاب موجود در منوی بازشو، یعنی Windows Server 2003 را تایید می کنیم

٤- روی Raise و سپس OK برای تایید تغییرات کلیک می کنیم

پیامی مبنی بر موفقیت آمیز بودن ارتقا سطح عملیاتی ظاهر می شود.

٥- روی OK کلیک می کنیم

تمرین سوم بررسی سطح عملیاتی دامنه ویندوز سرور 2003

در این تمرین خواهیم دید ویژگی هایی که قبلا به علت پایین بودن سطح عملیاتی غیر فعال بودند اکنون فعال هستند

١- از سیستم خارج شده و با اعتبار مدیر دامنه وارد می شویم

٢- یک پنجره خط فرمان باز می کنیم

٣- عبارت redircmp.exe "ou=clients,dc=tailspintoys,dc=com" را نوشته و Enter را فشار می دهیم

پیامی مبنی بر موفقیت آمیز بودن تکثیر ظاهر می شود

٤- عبارت redirusr.exe "ou=people,dc=tailspintoys,dc=com" را نوشته و Enter را فشار می دهیم

پیامی مبنی بر موفقیت آمیز بودن تکثیر ظاهر می شود

٥- ابزار Active Directory Users And Computers را باز می کنیم

٦- منوی View را باز کرده و مطمئن می شویم که Advanced Features انتخاب شده باشد

٧- روی حساب Administrator در Users container دوبار کلیک می کنیم

٨- روی زبانه Attribute Editor کلیک می کنیم

٩- خصوصیت lastLogonTimestamp را پیدا کرده و می بینیم که اینبار مقدار آن populated می باشد

١٠- در خط فرمان عبارت dfsrmig /setglobalstate 0 را نوشته و Enter را فشار می دهیم

پیامی ظاهر می شود و به ما می گوید که این عملیات فقط در سطح عملیاتی دامنه ویندوز سرور 2008 در دسترس است. در فصل دهم برای پیکربندی ارتقا DFS-R برای SYSVOL این کار را انجام داده بودیم

خلاصه درس

- سطح عملیاتی دامنه و forest مشخص می کنند که چه توانایی هایی از Active Directory ، و چه نسخه ای از ویندوز روی DCها، پشتیبانی می شوند

- سطح عملیاتی دامنه ویندوز سرور 2003 و ویندوز سرور2008 قابلیت های مهمی را امکان پذیر می کند.
- سطح عملیاتی forest ویندوز سرور 2003 تکثیر linked-value را فعال ، از RODC پشتیبانی می کند و توانایی های دیگری را فراهم می کند. سطح عملیاتی forest ویندوز سرور2008 عملکرد جدیدی را اضافه نمی کند.

سئوالات پایان درس

۱- می خواهیم سطح عملیاتی دامنه در یک دامنه در Forest با نام contoso.com را ارتقا دهیم. از کدام ابزار باید استفاده کنیم؟ (در صورت نیاز تمام گزینه های درست را انتخاب کنید.)

A . Active Directory Users And Computers
B . Active Directory Schema
C . Active Directory Sites And Services
D . Active Directory Domains And Trusts

۲- فرض کنید مدیر شبکه دامنه contoso.com هستیم. می خواهیم یک RODC به دامنه ای با یک DC با سیستم عامل ویندوز سرور 2003 و یک DC با سیستم عامل ویندوز سرور2008 اضافه کنیم.کدام یک از کارهای زیر باید قبل از اضافه کردن سرور انجام شود؟(در صورت نیازتمام گزینه های درست را انتخاب کنید. هر پاسخ صحیح بخشی از راه حل است)

A . ارتقا DC با سیستم عامل ویندوز سرور 2003 به سیستم عامل ویندوز سرور2008
B . ارتقا سطح عملیاتی دامنه به ویندوز سرور 2003
C . ارتقا سطح عملیاتی دامنه به ویندوز سرور 2008
D . ارتقا سطح عملیاتی forest به ویندوز سرور 2003
E . اجرای دستور Adprep /rodcprep
F . اجرای دستور Adprep /forestprep

۳- به تازگی کار ارتقا تمام DC های دامنه contoso.com را به ویندوز سرور 2008 تمام کرده ایم. DC های دامنه subsidiary.contoso.com نیز تا سه ماه دیگر ارتقا می یابند می خواهیم سیاستهای کلمه عبور fine-grained را برای گروهی از کاربران در دامنه contoso.com پیکربندی کنیم. در ابتدا چه باید کرد؟

A . نصب یک RODC
B . اجرای دستور Dfsrmig.exe
C . ارتقا سطح عملیاتی forest
D . نصب Group Policy Management Console (GPMC)

درس ۲ : مدیریت ارتباط دامنه و trust چندگانه

در فصل‌های قبل با پیکربندی و مدیریت یک دامنه منفرد آشنا شدیم ولی زیرساخت Active Directory شبکه ما ممکن است شامل یک forest با چند دامنه یا حتی چند forest باشد. ممکن است مجبور شویم اشیاء را بین دامنه‌ها جابجا کنیم یا ساختار دامنه را به طور کل تغییر دهیم. ممکن است مجبور شویم تایید هویت و دسترسی به منابع را بین دامنه و forest ها فعال کنیم. در این درس مهارت‌هایی را یاد می‌گیریم که برای کار با محیط چند دامنه‌ای و یا چند forest نیاز می‌باشد.

بعد از این درس یاد می‌توانیم:

- یک ساختار دامنه و tree موثر برای AD DS طراحی کنیم.
- نقش Active Directory Migration Tool و مسائل مربوط به انتقال شیء و بازسازی ساختار دامنه را تشخیص دهیم.
- ارتباطات trust را بفهمیم.

- ارتباطات امن trust را پیکربندی و مدیریت کنیم.

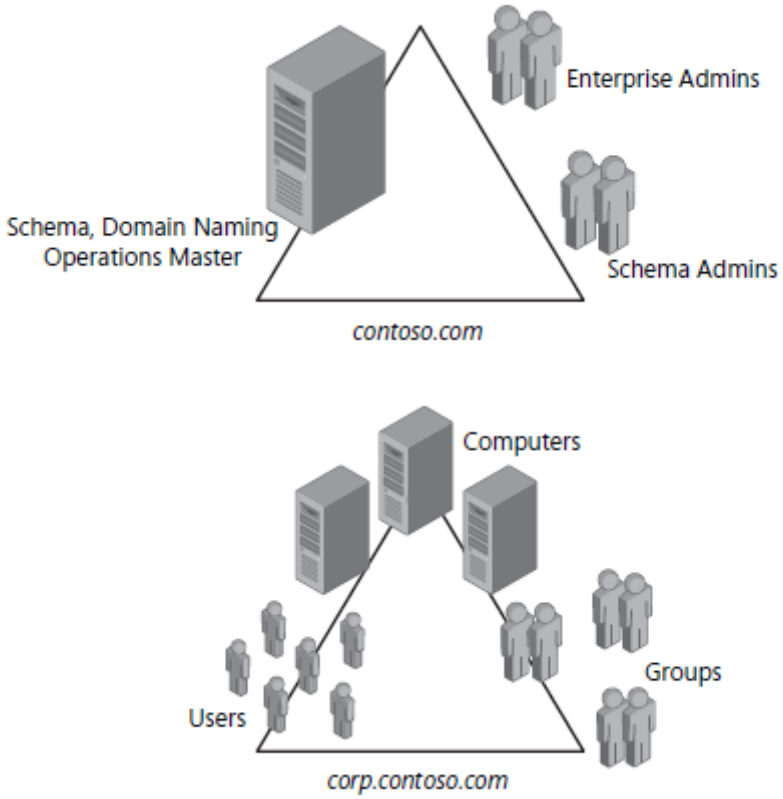
زمان تقریبی : ۶۰ دقیقه

تعریف ساختار دامنه و forest

پس از مطالعه فصل ۱۱ حالا آماده طراحی forest، tree و دامنه هستیم.

دامنه اختصاصی ریشه forest

در کاربردهای اولیه Active Directory پیشنهاد می‌شد که دامنه اختصاصی ریشه forest ساخت شود. از فصل‌های ۱ و ۱۰ آموختیم که دامنه ریشه forest اولین دامنه در forest است. هدف انحصاری دامنه اختصاصی ریشه forest مدیریت زیرساخت forest می‌باشد. این دامنه به طور پیش‌فرض حاوی master operation های منفرد برای forest است. همچنین حاوی گروههای بسیار حساس نظیر Enterprise Admins و Schema Admins است که دسترسی کاملی در forest دارند. فرض بر این است که ریشه اختصاصی forest امنیت را در محدوده این عملیات در سطح forest ارتقاء دهد. دامنه اختصاصی ریشه forest احتمال کمی دارد که منسوخ شود و انتقال مالکیت را تسهیل می‌کند. با توجه به توصیه‌های قبلی زیر ریشه اختصاصی forest یک دامنه فرزند global با همه اشیاء ممکن در دامنه قرار دارد یعنی کاربران، گروهها، کامپیوترها و غیره. ساختار چیزی شبیه به شکل ۳- ۱۲ خواهد شد.



شکل ۳- ۱۲ مثالی از دامنه ریشه forest

یک forest تک دامنه‌ای

نکته توصیه جدید forest تک‌دامنه‌ای

پیاده‌سازی یک دامنه اختصاصی ریشه forest برای بیشتر شبکه‌های سازمانی دیگر توصیه نمی‌شود. بهترین پیشنهاد طراحی می‌تواند forest تک‌دامنه‌ای باشد. هیچ طرحی را نمی‌توان برای تمامی سازمان‌ها مناسب دانست بنابراین خصوصیات شبکه باید در برابر شاخص‌های طراحی که در ادامه این درس می‌بینیم بررسی گردد.

بعد از ۹ سال حضور Active Directory در بازار کاملا شناخته شده است و پیشنهادهای قبلی و اولیه دیگر ارائه نمی‌گردد. الان برای بیشتر سازمان‌ها توصیه می‌شود یک forest با یک دامنه داشته باشیم. تجربه و علم می‌گوید:

- به طوری که در ادامه درس می‌بینیم هزینه و ریسک forest های چند دامنه‌ای زیاد است. یک دامنه منفرد روی سخت‌افزار ضعیف‌تر و ارزان‌تر کار می‌کند و ریسک کمی دارد.

- هنوز ابزارهایی که کار هرس و پیوند tree های Active Directory را انجام می‌دهند تولید نشده‌اند (تشبیه به هرس و پیوند درختان) به عبارت دیگر امکان شکستن یک دامنه از tree و کاشت آن در forest شبکه دیگر وجود ندارد. اگر این امکان موجود بود داشتن یک ریشه اختصاصی forest در هنگام انتقال دامنه‌ها از forest یا به forest عاقلانه به نظر می‌رسید.

- می‌توانیم در دامنه منفرد حداقل دسترسی امنیتی را پیاده کنیم بدین معنی که اگر امنیت آن بالاتر از forest با ریشه اختصاصی و دامنه فرزند نباشد کمتر نیست.

بنابراین هنگام طراحی دامنه باید با فرض را بر این بگذاریم که یک دامنه منفرد در forest داریم.

Forest های چند دامنه‌ای

در برخی سناریوها نیاز به forest با دامنه چندگانه داریم. نکته مهم این است که هرگز این forest به سادگی منطبق بر ساختار سازمانی نخواهد شد. یکی از دلایل این است که این ساختار یعنی واحدهای کاری، بخش‌ها و دفاتر به مرور زمان تغییر می‌کنند بنابراین ساختار منطقی سرویس دایرکتوری نباید تنها متکی به وضعیت سازمان باشد.

مدل دامنه باید از خصوصیات خود دامنه‌ها نشات گرفته شده باشد. خصوصیات مشخصی از یک دامنه روی همه اشیاء دامنه تاثیر می‌گذارد و اگر این تاثیرات ماندگار مناسب نیازهای سازمان نباشد باید دامنه‌های additional بسازیم. دامنه‌ها با عبارات زیر توصیف می‌شوند:

- **یک پارتیشن دامنه روی همه DC ها تکثیر می‌شود** domain naming context حاوی اشیاء کاربر، گروه، سیاست‌ها و دیگر منابع دامنه است و روی همه DC های دامنه تکثیر می‌شود. اگر به تکثیر پارتیشن نیاز داشته باشیم باید دامنه‌های مجزا بیاندیشیم. فرض می‌کنیم کارایی تکثیر Active Directory بینهایت بوده و می‌تواند دامنه‌های بزرگ را با حداقل پهنای باند پوشش دهد.

اگر محدودیت تکثیر داده مشخصی روی محل‌های معینی وجود دارد می‌بایست از ذخیره آن داده در پارتیشن دامنه جلوگیری کرده و یا دامنه‌های جداگانه‌ای برای برنامه‌های مجزا بسازیم. در چنین مواردی باید مطمئن شویم GC آن داده را تکثیر نمی‌کند.

- **سیاست منفرد Kerberos** تنظیمات پیش‌فرض سیاست Kerberos در AD DS برای بیشتر شبکه‌ها کافی است. ولی اگر نیاز به سیاست‌های متفاوتی باشد باید دامنه‌های مجزا داشته باشیم.

- **فضای نام منفرد DNS** دامنه Active Directory دارای یک نام دامنه DNS می‌باشد. در صورت نیاز به نام‌های دامنه چندگانه به دامنه‌های چندگانه نیز نیاز داریم. ولی قبل از مدل‌سازی دامنه‌های سرویس دایرکتوری به منظور پوشش دادن نیازهای مربوط به نام‌گذاری DNS باید به هزینه‌ها و ریسک‌های دامنه‌های چندگانه توجه جدی داشته باشیم

- در دامنه‌های دارای سطوح عملیاتی پایین‌تر از Windows Server 2008 دامنه فقط یک سیاست واحد حساب و کلمه عبور می‌تواند داشته باشد. بنابراین در این دامنه‌ها سازمانی که بخواهد سیاست‌های کلمه عبور چندگانه داشته باشد نیاز به چند دامنه دارد. در حالی که اگر سطح عملیاتی دامنه Windows Server 2008 باشد می‌توانیم از سیاست‌های کلمه عبور fine-grained استفاده کنیم.

افزودن دامنه به forest هزینه‌های سخت‌افزار و مدیریت شبکه را افزایش می‌دهد. هر دامنه توسط حداقل دو DC کنترل می‌شود که باید پشتیبان تهیه شود امن باشد و مدیریت شود. در مورد دسترسی به منابع بین دامنه‌ای در شبکه‌ای که از نظر جغرافیایی توزیع شده باشد حتی ممکن است به DC بیشتری نیاز باشد. دامنه‌های بیشتر می‌تواند به انتقال کاربران بین دامنه‌ها منجر شود که پیچیدگی آن بیشتر از انتقال کاربران بین OU ها می‌باشد. اشیاء Group Policy و تنظیمات کنترل دسترسی که در شبکه بسیار کاربرد دارند باید روی همه دامنه‌ها تکثیر شوند.

این‌ها همه فقط برخی هزینه‌های مرتبط با محیط‌های چند دامنه‌ای هستند. در این میان ریسک‌هایی نیزز موجود است. بیشتر این ریسک‌ها مربوط به این است که دامنه مرز امنیتی نیست در حالی که forest مرز امنیتی به شمار می‌آید. در یک forest مدیران سرویس شبکه ممکن است در سطح forest آسیب برسانند. انواع نفوذپذیری‌های متعددی وجود دارد که یک حساب مدیریتی شبکه لو رفته یا یک مدیر شبکه دارای غرض به وسیله آن می‌توانند حمله denial of service را انجام دهند یا اطلاعات forest را مخدوش کنند.

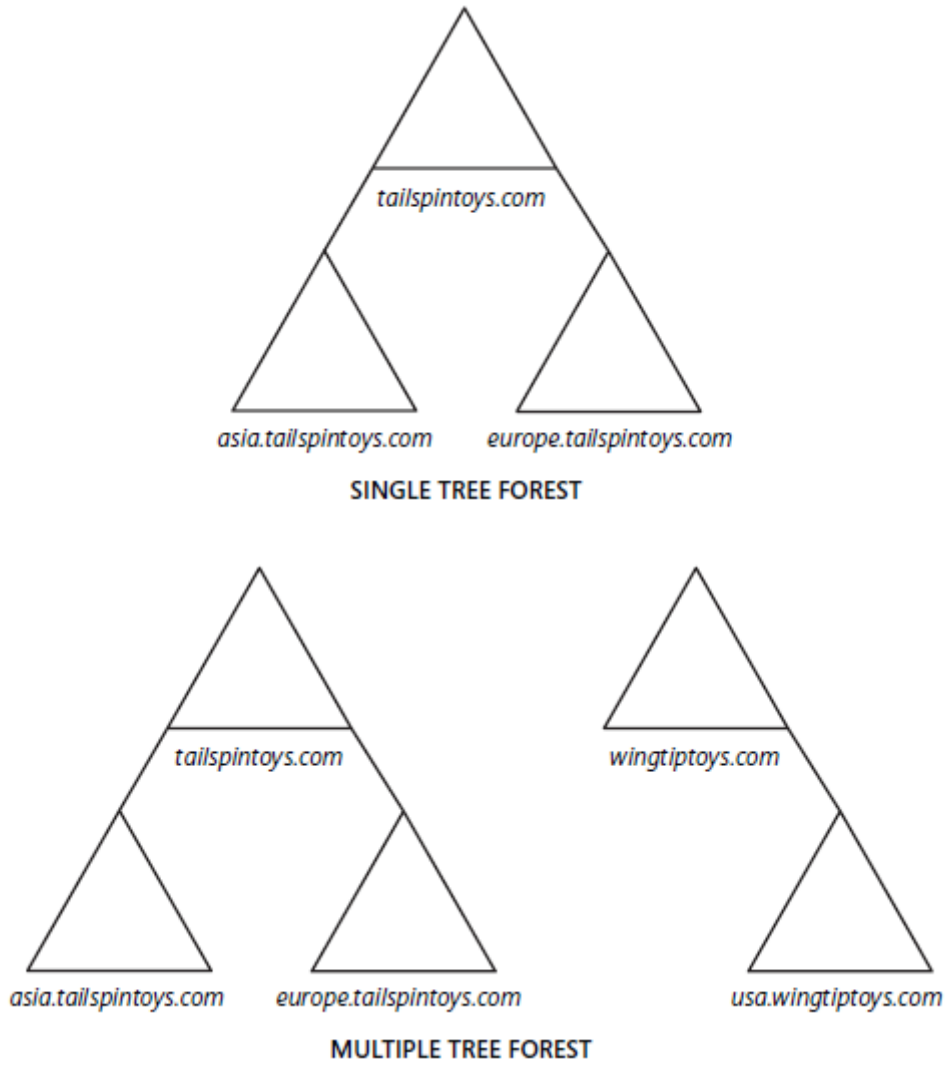
برای مثال یک مدیر شبکه در هر دامنه می‌تواند گروههای universal بسازد که عضویت آن‌ها روی GC تکثیر می‌شود. با ساخت گروههای universal متعدد و تعداد بیش از حد اعضاء در خصیصه member که منجر به تکثیر مفرط می‌شود باعث از کار افتادن سرویس‌دهی DC دامنه‌های دیگر خواهد شد. مدیرشبکه در هر دامنه می‌تواند همچنین مدیر شبکه ممکن است نسخه پشتیبان قدیمی را روی دایرکتوری بازیابی کند که باعث اخلال در forest می‌شود.

با توجه به هزینه‌ها و ریسک‌های دامنه‌های چندگانه اکیدا پیشنهاد می‌شود forest تک‌دامنه‌ای ایجاد شود. مهم‌ترین دلیل forest های چنددامنه‌ای می‌تواند نیاز جدی به تکثیر domain naming context باشد.

در forest با چند دامنه ممکن است ساخت یک دامنه اختصاصی ریشه forest به عنوان یک دامنه خالی به عنوان trust root برای forest عاقلانه به نظر می‌رسد.

Tree های چندگانه

به خاطر داریم که tree را فضای نام DNS دنباله‌دار تعریف کردیم. زمانی که بیش از یک دامنه موجود باشد باید تصمیم بگیریم که این دامنه‌ها از یک فضای نام DNS دنباله‌دار استفاده کنند و مانند شکل ۴- ۱۲یک tree واحد بسازند یا در فضای نام DNS مجزا قرار بگیرند و مانند شکل ۴- ۱۲ تشکیل tree های چندگانه را بدهند.



شکل ۴- ۱۲ forest با یک tree و tree چندگانه

Forest های چندگانه

Forest instanceای از Active Directory است. همه دامنه‌ها و DC ها در forest ، replica های schema و configuration را به اشتراک می‌گذارند. DC هایی که سرور GC هستند میزبان بخشی از خصیصه‌های همه اشیاء دامنه‌های دیگر در forest هستند. دامنه‌های forest، trust های دوطرفه و transitive را به اشتراک می‌گذارند بدین معنی که همه کاربران دامنه به گروه Authenticated Users تعلق دارند. گروههای Enterprise Admins، Schema Admins و Administrators در forest قدرت زیادی روی همه اشیاء forest دارند.

اگر هر کدام از این خصوصیات forest با نیازهای کاری سازمان در تضاد باشند forest باید به صورت چندگانه ساخته شود. در حقیقت با توجه به دغدغه‌های فعلی در مورد امنیت بسیاری از مشاوران شبکه پیشنهاد می‌کنند یا از forest تک‌دامنه‌ای استفاده شود یا از forest چندگانه (از forest با چنددامنه استفاده نشود). Trust های بین forest که در همین درس بحث می‌شود و AD FS مدیریت تایید هویت در شبکه‌های با چند forest را تسهیل می‌کند.

انتقال اشیاء بین دامنه‌ها و forest ها

در شبکه‌های چنددامنه‌ای ممکن است بخواهیم کاربران، گروهها یا کامپیوترها را بین دامنه‌ها و forest ها جابجا کنیم. ممکن است لازم باشد تعداد زیادی شیء را با هدف ایجاد ساختار جدید دامنه جابجا کنیم.

در هر کدام از این موارد ما حساب‌ها را از یک دامنه (دامنه مبدا) به دامنه دیگر (دامنه مقصد) کپی یا منتقل می‌کنیم. در حالت انتقال بین forest (inter-forest migration) اشیاء بین یک ویندوز NT 4.0 یا دامنه مبدا Active Directory و دامنه مقصد

Active Directory در یک forest مجزا و جابجا می‌شوند و در حالت انتقال درون forest (intra-forest migration) انتقال اشیاء بین دامنه‌های همان forest انجام می‌شود.

بازسازی دامنه بین forest ، حساب‌های موجود دامنه مبدا را حفظ کرده و روی دامنه مقصد نیز کپی می‌کند. این روش غیرتخریبی امکان فازبندی انتقال را میسر می‌کند. عملیات بدون وقفه ادامه پیدا می‌کند زیرا هر دو دامنه به طور موازی عمل می‌کنند. در این روش امکان برگشت نیز میسر است چون محیط قبلی بدون تغییر می‌ماند. پس از اینکه انتقال به طور کامل صورت گرفت می‌توانیم ماموریت دامنه مبدا را با انتقال باقیمانده حساب‌ها، سرورهای غیر DC و کامپیوترها به دامنه جدید به پایان برسانیم. پس از خارج کردن DC های مبدا از شبکه امکان توزیع مجدد آنها برای ایفای نقش در دامنه جدید وجود دارد.

انتقال بین forest یعنی انتقال اشیاء از دامنه مبدا به دامنه مقصد بدون اتمام ماموریت دامنه مبدا. پس از انتقال اشیاء می‌توانیم ساختار دامنه‌های خود را به منظور یکپارچه سازی عملیات و ساخت دامنه و ساختار OU که مدل مورد نظر ما را منعکس کند بازسازی کنیم. بسیاری از سازمان‌ها دامنه‌های خود را در یک دامنه تجمیع می‌کنند. این تجمیع به علت کاهش پیچیدگی مدیریت شبکه و هزینه پشتیبانی باعث کاهش هزینه و مدیریت آسان شبکه می‌شود.

ابزار انتقال Active Directory

ابزار انتقال Active Directory نسخه ۳ (ADMT v3) کار انتقال اشیاء و وظایف security translation را انجام می‌دهد. این نسخه از ADMT از آدرس http://go.microsoft.com/fwlink/?LinkID=75627 قابل دانلود است. همچنین صفحه دارای جزئیات ابزار می‌باشد.

از ADMT برای انتقال اشیاء بین دامنه مبدا و مقصد استفاده می‌شود. این انتقال می‌تواند بین دامنه‌های یک forest یا دامنه‌های forest های متفاوت اتفاق بیافتد. ADMT ویزاردهایی را فراهم می‌کند که کار انتقال و ترجمه امنیتی (security translation) را به طور اتوماتیک انجام می‌دهد. این انتقال شامل کاربران، گروهها، حساب‌های سرویس، کامپیوترها و trust می‌باشد. این کار با استفاده از کنسول ADMT یا خط فرمان می‌تواند انجام شود. فایل‌های جواب در این دستور موجود است که با مشخص کردن پارامترهای فرمان انجام مراحل کار را ساده و خودکار می‌کند. بعد توسط یک فایل متنی ساده لیست اشیائی که باید منتقل شود مشخص می‌کنیم به جای اینکه همه اشیاء را در خط فرمان وارد کنیم. این دستور رابطی نیز دارد که به ما اجازه می‌دهد با زبان‌هایی نظیر VBScript انتقال را با اسکریپت انجام دهیم. برای بررسی جزئیات کنسول ADMT را اجرا کرده و پنجره online help را باز می‌کنیم.

ADMT هنگام اجرای عملیات انتقال به ما اجازه می‌دهد کار را شبیه‌سازی کنیم به طوری که نتایج را ارزیابی کرده و خطاهای احتمالی را پیش‌بینی کنیم بدون اینکه تغییری در دامنه مقصد اتفاق بیافتد. ویزارد گزینه Test The Migration Settings And Migrate Later را در اختیار ما قرار می‌دهد. با این گزینه می‌توانیم عملیات انتقال را پیکربندی کنیم، تنظیمات را تست کنیم و فایل‌های log و گزارشات به دست آمده توسط ویزارد را مرور کنیم. پس از تشخیص و حل مشکلات می‌توانیم عملیات انتقال را اجرا کنیم. در مرحله انتقال هر یک از اشیاء کاربران، گروهها و کامپیوترها این مراحل تکرار می‌شود.

مشخصه‌های امنیتی و انتقال

دغدغه اصلی هنگام انتقال عدم ایجاد وقفه در دسترسی به منابع است. در ادامه با مفاهیمی نظیر مشخصه‌های امنیتی (SID)، token ها، ACL ها و sIDHistory آشنا می‌شویم.

SID ها مقادیری منحصربه‌فرد در سطح دامنه هستند که هنگام ایجاد به حساب‌های واحدهای امنیتی نظیر کاربران، گروهها و کامپیوترها نسبت داده می‌شوند. وقتی کاربری وارد می‌شود توکن حاوی SID اولیه حساب کاربر و SID های گروههایی که کاربر عضو آنهاست تولید می‌شود. بنابراین توکن نماینده کاربر با همه SID های منتسب به کاربر و عضویت گروههای مختلف است.

امنیت منابع با استفاده از توصیف‌کننده امنیتی (SD) تامین می‌گردد بدین صورت که SD مجوزها، مالکیت‌ها، حقوق و ممیزی منابع را توصیف می‌کند. در SD دو ACL موجود است. ACL سیستم (SACL) که ممیزی را توصیف می‌کند و discretionary ACL (DACL) که مجوزهای دسترسی به منابع را توصیف می‌کند. در بسیاری از کتاب‌ها به جای DACL از واژه ACL استفاده می‌شود. DACL مجوزهای منتسب به واحدهای امنیتی را لیست می‌کند. در لیست ACE ها مجوز خاصی را به SID یک واحد امنیتی لینک می‌کند. ACE می‌تواند مجوز دسترسی (allow) یا عدم دسترسی (deny) باشد.

وقتی کاربری برای دسترسی به منبعی تلاش می‌کند Local Security Authority Subsystem (LSASS) کار مقایسه SID های توکن کاربر را با SID های ACE ها در ACL منبع انجام می‌دهد.
وقتی حسابی را به دامنه جدید منتقل می‌کنیم حساب از دامنه مبدا به دامنه مقصد کپی می‌شود. SID های جدید برای حساب‌ها در دامنه مقصد تولید می‌شود بنابراین این SID ها با SID های قبلی متفاوت می‌باشد. یعنی حتی اگر حساب‌ها با همان نام و خصیصه‌ها منتقل شوند به دلیل تفاوت SID دیگر به منابع دامنه مبدا دسترسی نخواهند داشت. برای حل این مساله دو راه حل موجود است: sIDHistory و ترجمه امنیتی:

- **sIDHistory** در شبکه‌های سازمانی ترجیح بر این است که برای بازسازی موثر ساختار دامنه از این خصیصه استفاده شود. واحدهای امنیتی AD یک SID و یک خصیصه sIDHistory دارند که حاوی یک یا چند SID منتسب به حساب می‌باشد. وقتی حسابی به دامنه مقصد کپی می‌شود SID منحصر به فرد در دامنه مقصد برای آن حساب تولید می‌شود. خصیصه sIDHistory نیز می‌تواند مقدار SID حساب در دامنه مبدا را به خود بگیرد. وقتی کاربری به دامنه وارد می‌شود توکن کاربر مجموعه‌ای از SID و sIDHistory حساب کاربر و گروههایی که کاربر عضو آنهاست می‌باشد. LSASS از SID های خصیصه sIDHistory همانند هر SID دیگری در توکن استفاده می‌کند تا دسترسی کاربر را به منابع دامنه مبدا تامین کند.

- **ترجمه امنیتی** SD منابع را بررسی کرده و SID هایی را که به حسابی در دامنه مبدا برمی‌گردد مشخص کرده و آن SID را با SID حساب جدید در دامنه مقصد جابجا می‌کند. نام این فرایند بازسازی ACL می‌باشد. ترجمه امنیتی یا بازسازی ACL به صورت دستی حتی در شبکه‌های ساده کاری ملال‌آور و خسته‌کننده می‌باشد. ابزارهای انتقال نظیر ADMT کار ترجمه امنیتی را به صورت خودکار انجام می‌دهد. به طور مشخص ADMT می‌تواند موارد زیر را ترجمه کند:
  - مجوزهای فایل و پوشه
  - مجوزهای پرینتر
  - مجوزهای منابع به اشتراک‌گذاشته‌شده
  - مجوزهای دجیستری
  - حقوق کاربری
  - پروفایل‌های محلی
  - عضویت گروهها

عضویت گروهها

دغدغه آخر در مورد دسترسی به منابع عضویت گروههاست. گروههای golbal می‌تواند فقط حاوی اعضاء همان دامنه باشد. بنابراین اگر یک کاربر به دامنه مقصد انتقال یابد حساب کاربری جدید دیگر عضو گرههای global دامنه مبدا نخواهد بود.
برای حل این مساله در انتقال بین forest ابتدا باید گروههای global را به دامنه مقصد منتقل کنیم. این گروهها در خصیصه sIDHistory خود حاوی SID های گروههای مبدا می‌باشند. بنابراین کاربران باید منتقل شوند. ADMT هنگام انتقال کاربران عضویت حساب‌های مبدا را ارزیابی می‌کند و حساب‌های جدید را به همان گروه در دامنه مقصد اضافه می‌کند. اگر گروه در دامنه مقصد موجود نباشد آنرا به طور خودکار ایجاد می‌کند. در نهایت حساب کاربری در دامنه مقصد به گروههای global دامنه مقصد تعلق خواهد

داشت. کاربر و گروهی که کاربر عضو آن است در خصیصه‌های sIDHistory خود حاوی SID های حساب مبدا می‌باشد. بنابراین کاربر توانایی دسترسی به منابع دامنه مبدا را طبق روال گذشته خواهد داشت.

در انتقال درون forest فرایند متفاوت است. یک گروه global در دامنه مقصد به عنوان یک گروه universal ساخته می‌شود به طوری که بتواند کاربران را از دامنه مبدا و مقصد در خود جای دهد. گروه جدید SID جدیدی به خود می‌گیرد ولی sIDHistory با SID گروه global دامنه مبدا جمع شده و بدین وسیله دسترسی به منابع را برای گروه جدید فراهم می‌کند. بعد از اینکه همه کاربران از دامنه مبدا به دامنه مقصد منتقل شدند حوزه گروه به global برمی‌گردد.

مشکلات دیگر انتقال

ما در برنامه‌ریزی برای انتقال اشیاء بین دامنه‌ها و forest ها باید چند مساله را در نظر بگیریم. مهم‌ترین مسایل عبارتند از:

- **انتقال کلمه عبور** با ADMT کلمات عبور را نیز می‌توان منتقل کرد. ولی ممکن است سیاست‌های کلمه عبور در دامنه مقصد متفاوت باشد. کلمات عبور با حداقل یک کاراکتر بدون توجه به سیاست کلمه عبور دامنه مقصد منتقل خوهد شد. اگر بخواهیم هنگام انتقال شبکه قفل باشد باید ابتدا به ADMT اجازه دهیم کلمات پیچیده پیکربندی کند و یا کلمات عبور اولیه را توسط اسکریپت تولید کرده و کاربران مجبور کنیم اولین بار هنگام ورود به شبکه کلمه عبور خود را تغییر دهند.

- **حساب‌های سرویس** سرویس‌های کامپیوترهای دامنه ممکن است برای تایید هویت از حساب‌های کاربری دامنه استفاده کنند. با انتقال این حساب‌های کاربران به دامنه مقصد سرویس‌ها باید با هویت جدید حساب سرویس به روز شوند. ADMT این فرایند را به طور خودکار انجام می‌دهد.

- **اشیائی که نمی‌توان منتقل کرد** برخی اشیاء را به صورت یکپارچه نمی‌توان منتقل کرد. ADMT گروههای پیش‌فرض (buit-in) مانند Domain Admins یا گروه Administrators محلی را نمی‌تواند منتقل کند. برای رفع این محدودیت به راهنمای کاربران مراجعه کنید.

ارتباطات Trust

هرگاه در AD DS بیش از یک دامنه داشته باشیم احتمالا باید به فکر ارتباطات trust یا به اختصار trust باشیم. خیلی مهم است که اهداف، عملکرد و پیکربندی trust را بشناسیم.

Trust در یک دامنه

در فصل ۵ دیدیم هنگام join یک سرور منفرد یا کلاینت چه اتفاقی می‌افتد. در یک workgroup کامپیوتر دارای یک انباره هویت در SAM می‌باشدکه هنگام تایید هویت کاربران از روی آن انجام می‌شود. وقتی کامپیوتری عضو دامنه می‌شود یک ارتباط trust با دامنه برقرار می‌سازد. تاثیر این trust این است که کامپیوتر به کاربران اجازه می‌دهد نه به صورت محلی بلکه در دامنه تایید هویت شوند. کاربر دامنه هنچنین به منابع سیستم محلی دسترسی دارد. برای مثال گروه Domain Users به گروه Users محلی اضافه می‌شود که به آنها اجازه ورود به سیستم (log on locally) را می‌دهد. همچنین حساب‌های گروه و کاربر دامنه می‌تواند به ACL های فایل‌ها، پوشه‌ها، کلیدهای رجیستری و پرینترهای سیستم اضافه شوند. همه اعضاء دامنه trust های مشابه با دامنه دارند که باعث می‌شود دامنه به عنوان یک انباره هویت مرکزی و یک سرویس فراهم کننده تایید هویت مطرح باشد.

Trust بین دامنه‌ها

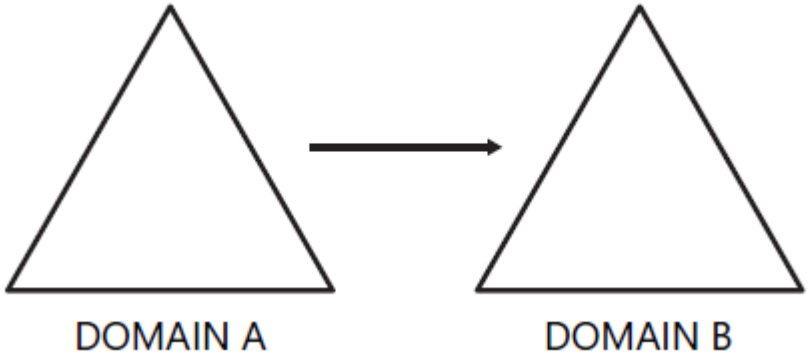
با این مفاهیم اولیه حالا می‌توانیم دانش خود را به دامنه‌های دیگر بسط دهیم. Trust بین دو دامنه باعث می‌شود یک دامنه به سرویس تایید هویت و انباره هویت دامنه دیگر اعتماد کند. در واقع trust یک لینک منطقی بین دامنه برای تایید هویت می‌باشد.

در هر ارتباط trust دو دامنه موجود است. یکی دامنه اعتماد کننده و دیگری دامنه مورد اعتماد. دامنه مورد اعتماد حاوی انباره هویت بوده و کار تایید هویت را برای کاربران انجام می‌دهد. وقتی کاربری در دایرکتوری دامنه مورد اعتماد به دامنه اعتمادکننده وارد می‌شود به دلیل عدم وجود کاربر در انباره داده، دامنه اعتمادکننده امکان تایید هویت کاربر را ندارد بنابراین تایید هویت را به DC دامنه مورد

اعتماد می‌سپارد. بنابراین می‌توان گفت دامنه اعتماد کننده به دامنه مورد اعتماد برای تایید هویت کاربر اعتماد می‌کند. دامنه اعتماد کننده سطح اعتماد را تا سرویس‌های تایید هویت و انباره هویت دامنه مورد اعتماد گسترش می‌دهد.

به دلیل اینکه دامنه اعتمادکننده به هویت‌های دامنه مورد اعتماد اعتماد می‌کند دامنه اعتمادکننده می‌تواند از هویت‌های مورداعتماد برای اعطاء دسترسی به منابع استفاده کند. کاربران دامنه مورداعتماد می‌توانند حقوق کاربری نظیر ورود به سیستم‌های دامنه اعتمادکننده داشته باشند. کاربران یا گروههای global در دامنه مورداعتماد می‌توانند به گروههای محلی دامنه اعتمادکننده اضافه شوند. کاربران و گروههای global در دامنه مورداعتماد از طریق افزودن هویت به ACL ها در دامنه اعتمادکننده می‌توانند روی پوشه‌های اشتراکی مجوز داشته باشند.

شکل ۵- ۱۲ یک شمای ساده از trust را نمایش می‌دهد. دامنه A به دامنه B اعتماد می‌کند. یعنی دامنه A دامنه اعتمادکننده و دامنه B دامنه مورداعتماد می‌باشد. اگر یک کاربر در دامنه B به کامپیوتری در دامنه A متصل شود دامنه A درخواست تایید هویت را به DC در دامنه B می‌فرستد.

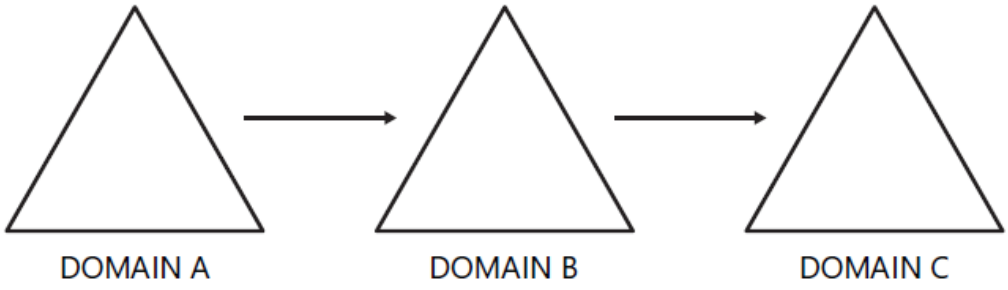


شکل ۵- ۱۲ شمای ارتباط trust ساده

خصوصیات ارتباط trust

ارتباط trust بین دامنه‌ها می‌تواند با دو خصیصه trust توصیف شود:

- **انتقال‌پذیری** برخی trust ها انتقال پذیر نیستند. در شکل ۶- ۱۲ دامنه A به دامنه B اعتماد می‌کند و دامنه B به دامنه C اعتماد می‌کند. اگر trust انتقال پذیر باشد دامنه A باید به دامنه C نیز اعتماد کند. در بیشتر موارد باید ارتباط trust سومی برقرار کنیم تا دامنه A به دامنه C اعتماد کند.



شکل ۶- ۱۲ مثالی از ارتباط trust

- **جهت** ارتباط trust می‌تواند یک‌طرفه یا دوطرفه باشد. در trust یک‌طرفه نظیر شکل ۵- ۱۲ کاربران در دامنه مورداعتماد به منابع دامنه اعتمادکننده دسترسی دارند ولی برعکس آن امکانپذیر نیست به همین دلیل در بیشتر موارد ارتباط یک‌طرفه دوم در جهت خلاف ایجاد می‌شود. برای مثال می‌توان trust دوم را طوری ساخت که دامنه B به دامنه A اعتماد کند. برخی trust ها ذاتا دوطرفه هستند. در چنین trust هر دو دامنه به هویت‌ها و سرویس تایید هویت یکدیگر اعتماد دارند.

- **خودکار یا دستی** برخی trust ها به طور خودکار ایجاد می‌شوند. برخی دیگر باید دستی ساخته شوند.

در یک forest همه دامنه‌ها به یکدیگر اعتماد دارند. به این دلیل که دامنه ریشه هر tree به دامنه ریشه forest اعتماد دارد و هر دامنه فرزند به دامنه والد خود اعتماد دارد. این trust ها که به طور خودکار ساخته می‌شود نباید حذف شوند. این trust ها انتقال‌پذیر و دوطرفه هستند. نتیجه نهایی این است که دامنه به انباره هویت و سرویس تایید هویت همه دامنه‌های دیگر forest اعتماد می‌کند. کاربران و گروههای global از هر دامنه در forest می‌تواند به گروههای محلی دامنه اضافه می‌شود، حق کاربری اعطاء شود و به ACL منابع دامنه‌های دیگر در forest افزوده شود. Trust به forest های دیگر و دامنه‌های بیرون forest باید به صورت دستی ایجاد شود. با این خلاصه حالا می‌توانیم به جزئیات trust در داخل و خارج forest بپردازیم.

پروتکل‌های تایید هویت و ارتباطات trust

Active Directory ویندوز سرور 2003 کاربران را با یکی از دو پروتکل Kerberos v5 یا NT LAN Manager (NTLM) تایید هویت می‌کند. Kerberos v5 پروتکل پیش‌فرض مورد استفاده توسط کامپیوترهای ویندوز سرور 2008 ، ویستا، سرور 2003 ، XP و سرور 2000 می‌باشد. اگر کامپیوتری از Kerberos پشتیبانی نکند پروتکل NTLM مورد استفاده قرار می‌گیرد.

تایید هویت Kerberos در دامنه

وقتی کاربری به کلاینتی وارد می‌شود که Kerberos نسخه ۵ را نصب کرده درخواست تایید هویت به DC ارسال می‌گردد. هر DC به عنوان یک مرکز توزیع کلید (KDC) که بخش مرکزی Kerberos می‌باشد عمل می‌کند. پس از تایید اعتبار هویت کاربر KDC روی DC به کاربر تایید هویت شده بلیطی تحت عنوان ticket-granting ticket (TGT) اعطاء می‌کند.

وقتی کاربر نیاز به دسترسی به منابع یک کامپیوتر در همان دامنه دارد باید ابتدا یک بلیط (session ticket) برای کامپیوتر به دست آورد. این بلیط توسط KDC یک DC فراهم می‌شود بنابراین کاربر برای درخواست بلیط به DC مراجعه می‌کند. کاربر برای اثبات اینکه تایید هویت شده است TGT ارائه می‌کند. این کار به KDC امکان می‌دهد که به درخواست بلیط کاربر بدون اجبار به تایید هویت دوباره کاربر پاسخ دهد. درخواست بلیط ، کامپیوتر و سرویسی را که کاربر می‌خواهد مشخص می‌کند. KDC بر اساس service principle name (SPN) تشخیص می‌دهد که سرویس در همان دامنه است یا نه. سپس به کاربر بلیط همان سرویس را ارائه می‌دهد.

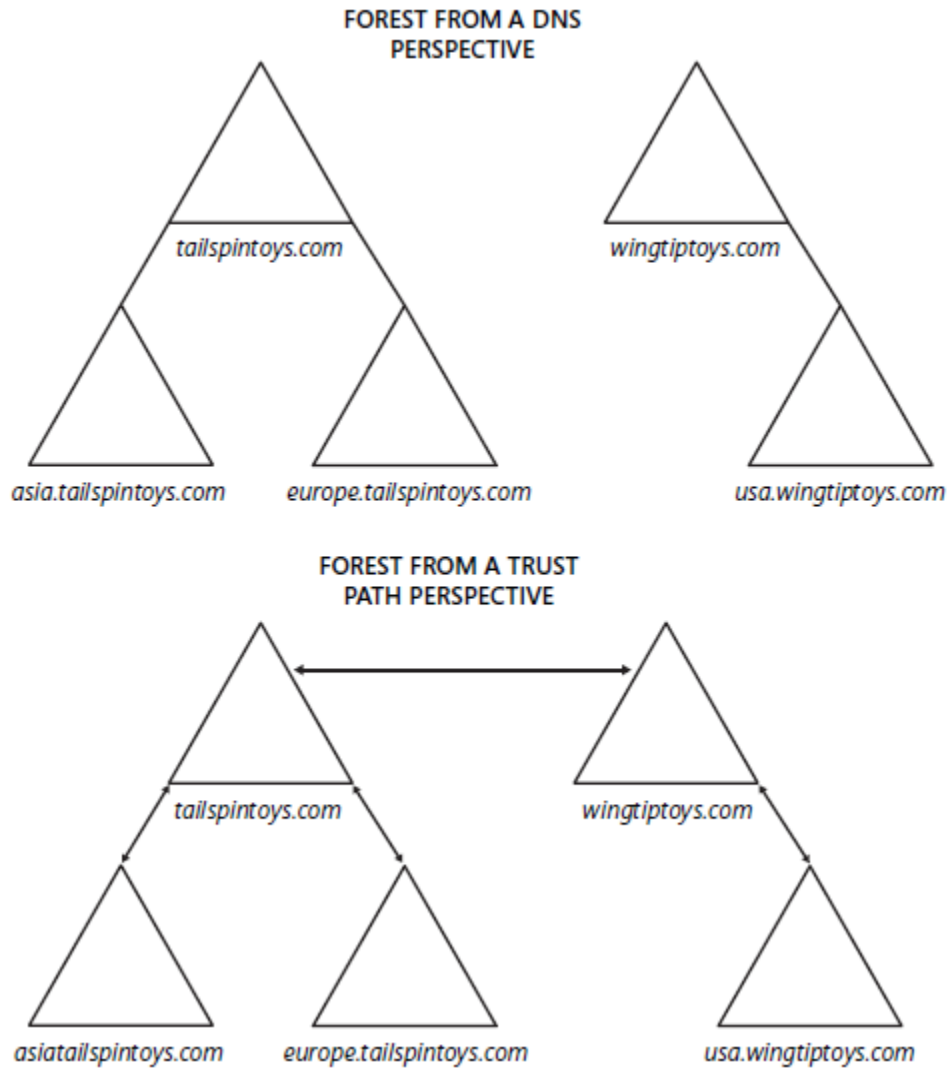
سپس کاربر به سرویس متصل شده و بلیط خود را ارائه می‌دهد. سرور نیز اعتبار بلیط را بررسی کرده و چک می‌کند که کاربر توسط دامنه تایید هویت شده است یا نه. این کار از طریق کلیدهای خصوصی (private keys) انجام می‌شود که از بحث ما خارج است. بنابراین سرور نیازی به تایید هویت کاربر ندارد و تایید هویت کاربر توسط دامنه را قبول می‌کند.

همه این تعاملات Kerberos توسط کلاینت‌ها و سرورهای ویندوز کنترل شده و از دید کاربران مخفی است.

تایید هویت Kerberos در یک forest

همه دامنه‌های فرزند به دامنه والد خود به صورت خودکار، دوطرفه و قابل انتقال اعتماد دارند که به آن parent-child trust گویند. دامنه ریشه هر tree نیز به دامنه ریشه forest به صورت خودکار، دوطرفه و قابل انتقال اعتماد دارد که به آن tree-root trust گویند.

این ارتباطات trust مفهومی به نام trust path یا trust flow را ایجاد می‌کند. trust path با یک دیاگرام همانند شکل ۷- ۱۲ قابل درک است. در این شکل Forest دارای دو tree است. یکی tailspintoys.com و دیگری wingtiptoys.com . دامنه اول دامنه ریشه forest است. در بالای شکل، forest از منظر DNS قابل مشاهده است. در پایین نیز trust path دیده می‌شود. از شکل می‌توان دریافت که دامنه ریشه tree مربوط به wingtiptoys.com به دامنه tailspintoys.com اعتماد دارد.



شکل ۷- ۱۲ یک forest از منظر DNS و منظر trust path

تایید هویت Kerberos از trust path برای فراهم کردن بلیط session یک سرویس در دامنه دیگر استفاده می‌کند. اگر کاربری در usa.wingtiptoys.com بخواهد به پوشه‌های اشتراکی سروری در euroup.tailspintoys.com دسترسی داشته باشد تعاملات زیر اتفاق می‌افتد:

۱. کاربر به کامپیوتری در usa.wingtiptoys.com وارد شده و همان طور که در بخش قبلی فرایند تایید هویت تشریح شد توسط یک DC در این دامنه تایید هویت می‌شود. کاربر یک TGT از DC تحویل می‌گیرد.

۲. کاربر به منظور درخواست یک بلیط session برای سرور واقع در euroup.tailspintoys.com با KDC مربوط به یک DC در دامنه usa.wingtiptoys.com ارتباط برقرار می‌کند.

۳. DC واقع در usa.wingtiptoys.com بر اساس SPN تشخیص می‌دهد که سرویس مورد نظر در euroup.tailspintoys.com واقع شده نه در دامنه محلی. نقش KDC واسط مورد اعتماد بین یک کلاینت و سرویس است. به دلیل اینکه سرویس در یک دامنه مورد اعتماد واقع شده نه در دامنه محلی اگر KDC نتواند بلیط session برای سرویس را فراهم کند کلاینت را به آنجا ارجاع می‌دهد. KDC برای تعیین مرحله بعدی از اگوریتم ساده‌ای استفاده می‌کند. اگر دامنه میزبان سرویس مستقیما به دامنه KDC ، trust داشته باشد KDC کلاینت‌ها را به DC دامنه میزبان سرویس

ارجاع می‌دهد و درغیراین‌صورت اگر trust قابل انتقال بین دو دامنه برقرار باشد KDC کلاینت را به دامنه بعدی در trust path ارجاع می‌دهد.

۴. دامنه usa.wingtiptoys.com با دامنه euroup.tailspintoys.com ارتباط trust ندارند ولی trust قابل انتقال بین آنها برقرار است بنابراین KDC دامنه usa.wingtiptoys.com کلاینت را به DC در دامنه بعدی در trust path یعنی wingtiptoys.com ارجاع می‌دهد.

۵. کلاینت با KDC دامنه که به آن ارجاع شده یعنی wingtiptoys.com ارتباط برقرار می‌کند.

۶. دوباره KDC مشخص می‌کند که سرویس در دامنه محلی نیست و اینکه europe.tailspintoys.com به طور مستقیم با wingtiptoys.com رابطه trust ندارد بنابراین به DC بعدی در trust path که tailspintoys.com می‌باشد ارجاع می‌دهد.

۷. کلاینت با KDC دامنه ارجاع شده یعنی tailspintoys.com ارتباط برقرار می‌کند.

۸. KDC مشخص می‌کند که سرویس در دامنه محلی نیست و اینکه europe.tailspintoys.com به طور مستقیم با wingtiptoys.com رابطه trust دارد بنابراین به DC واقع در دامنه europe.tailspinroys.com ارجاع می‌دهد.

۹. کلاینت با KDC دامنه ارجاع شده یعنی europe.tailspintoys.com ارتباط برقرار می‌کند.

۱۰. KDC واقع در europe.tailspintoys.com یک بلیط session برای سرویس مورد نظر برمی‌گرداند.

۱۱. کلاینت با سرور ارتباط برقرار کرده و بلیط session فراهم می‌کند. سرور دسترسی به پوشه‌های اشتراکی را بر اساس مجوزهای منتسب به کاربر و گروه‌ها فراهم می‌کند.

این فرایند ممکن است پیچیده به نظر برسد ولی طوری انجام می‌شود که از دید کاربر مخفی می‌ماند.
اگر یک کاربر از usa.wingtiptoys.com به کامپیوتری در دامنه europe.tailspintoys.com وارد شود عکس این فرایند انجام می‌شود. درخواست اولیه تایید هویت باید مسیر trust path را طی کند تا به یک KDC در دامنه usa.wingtiptoys.com برسد.

ایجاد trust به صورت دستی

چهار نوع trust باید به صورت دستی ساخته شود:

- میانبر (shortcut trusts)
- خارجی (external trusts)
- ناحیه‌ای (realm trusts)
- Forest trusts

همه انواع فوق در بخش‌های بعدی بحث می‌شوند.

ایجاد ارتباط trust به صورت دستی

مراحل ایجاد trust در انواع مختلف مشابه است. ما باید عضو گروه Domain Admins یا Enterprise Admins باشیم تا بتوانیم trust ایجاد کنیم.

برای ایجاد ارتباط trust مراحل زیر را انجام می‌دهیم:

۱. ابزار Active Directory Domains And Trusts را باز می‌کنیم.

۲. روی دامنه‌ای که در یک طرف ارتباط trust قرار خواهد گرفت کلیک راست کرده و properties را انتخاب می‌کنیم. این ابزار را باید با اعتبار دارنده مجوز ایجاد trust در این دامنه اجرا کنیم.

۳. روی زبانه Trusts کلیک می‌کنیم.

۴. روی دکمه New Trust کلیک می‌کنیم. ویزارد New Trust ما را به سوی ایجاد trust راهنمایی می‌کند.

۵. در صفحه Trust Name نام DNS دامنه آن سوی trust را وارد کرده و Next را می‌زنیم.

۶. اگر دامنه‌ای که وارد می‌کنیم در همان forest نباشد پیغامی مبنی بر انتخاب نوع trust ظاهر می‌شود که یکی از موارد زیر باید انتخاب شود:

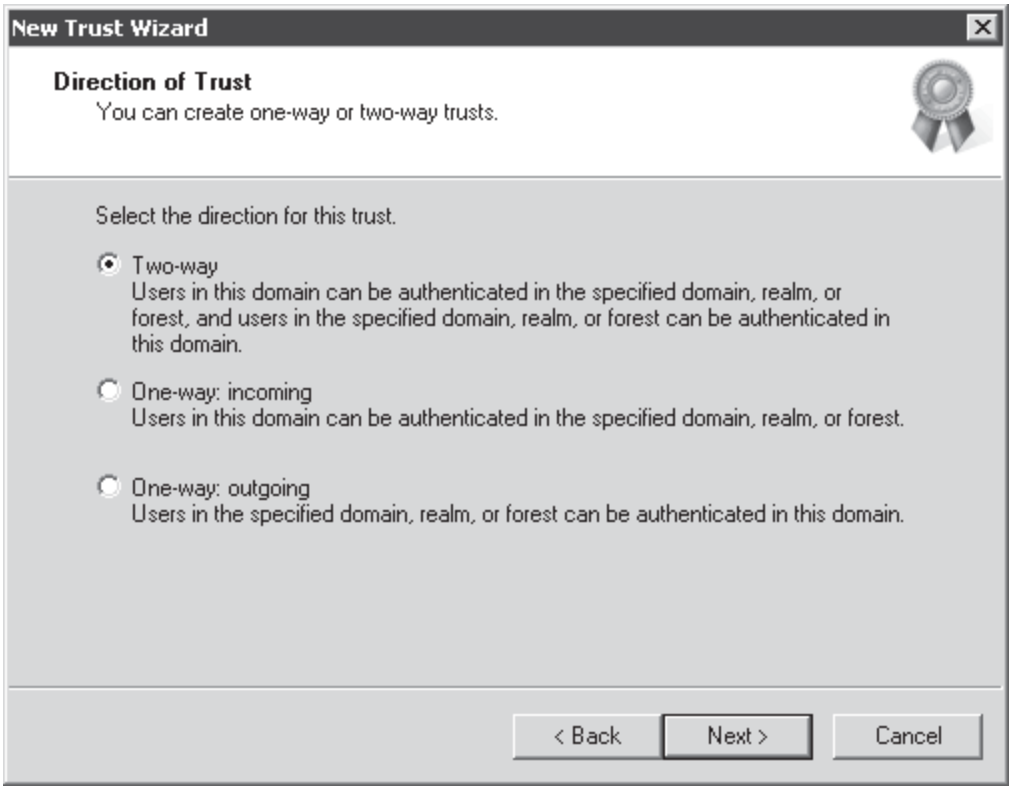
- Forest
- External
- Realm

اگر دامنه در همان forest باشد ویزارد می‌داند که منظور shortcut trust است.

۷. اگر trust از نوع realm می‌سازیم پیغامی ظاهر می‌شود که از ما می‌خواهد مشخص کنیم trust قابل انتقال باشد یا خیر.

۸. در صفحه Direction Of Trust همانند شکل ۸- ۱۲ یکی از موارد زیر را انتخاب می‌کنیم:

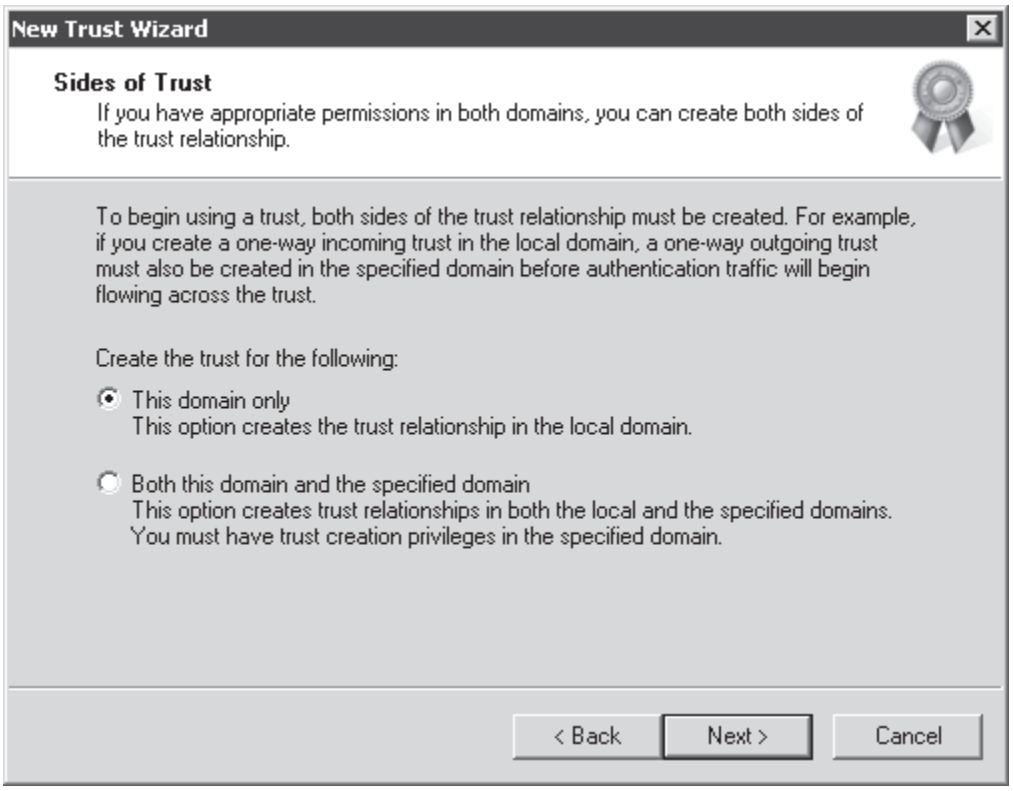
- گزینه Two-Way یک trust دوطرفه بین دامنه‌ها ایجاد می‌کند.
- گزینه One-Way:Incomming نوع trust یک‌طرفه را برقرار می‌کند که در آن دامنه انتخاب شده در مرحله ۲ دامنه مورد اعتماد و دامنه انتخاب شده در مرحله ۵ دامنه اعتمادکننده خواهد بود.
- One-Way:Outgoing یک trust یک‌طرفه برقرار می‌شود که دامنه انتخاب شده در مرحله ۲ دامنه اعتمادکننده و دامنه انتخاب شده در مرحله ۵ دامنه مورد اعتماد خواهد بود.



شکل ۸- ۱۲ صفحه Direction Of Trust

۹. روی Next کلیک می‌کنیم.

۱۰. در صفحه Sides Of Trust که در شکل ۹- ۱۲ نمایش داده شده است یکی از موارد زیر را انتخاب می‌کنیم:



شکل ۹- ۱۲ صفحه Sides Of Trust

- Both This Domain And The Specified Domain : هر دو طرف trust را برقرار می‌کند. نیازمند این است که مجوز ایجاد trust را در هر دو دامنه داشته باشیم.
- This Domain Only : ارتباط trust را در دامنه انتخاب شده در مرحله ۲ ایجاد می‌کند. یک Administrator با مجوز ایجاد trust روی دامنه‌های دیگر باید این فرایند را برای تکمیل ارتباط trust تکرار کند.

مراحل بعدی بستگی به گزینه‌هایی دارد که ما در مراحل ۸ و ۱۰ انتخاب می‌کنیم. مراحل به یکی از حالت‌های زیر ادامه می‌یابد:

- اگر گزینه Both This Domain And The Specified Domain انتخاب شود باید نام کاربری و کلمه عبور دارای مجوز ایجاد trust در دامنه تعیین شده در مرحله ۵ باشد.
- اگر گزینه This Domain Only انتخاب شود باید یک کلمه عبور trust وارد شود. کلمه عبور trust توسط یکی از اعضاء گروه Adiministrator در هر سمت trust وارد می‌شود. این کلمه عبور باید با کلمه عبور کاربر Administrator متفاوت باشد و کلمه عبور انحصاری برای ایجاد trust در نظر گرفته شود. کلمه عبور برای ایجاد trust استفاده می‌شود و دامنه فورا آنرا تغییر می‌دهد.

۱۱. اگر trust از نوع outgoing باشد پیغامی ظاهر می‌شود تا یکی از موارد زیر را انتخاب کنیم:

- Selective Authentication
- Domain-Wide Authentication یا Forest-Wide Authentication به ترتیب وقتی نوع trust خارجی یا forest باشد.

گزینه‌های Authentication در بخش‌های بعدی همین فصل بررسی می‌شوند.

۱۲. ویزارد New Trust انتخاب‌های ما را در صفحه Trust Selections Complete به طور خلاصه نمایش می‌دهد. روی Next کلیک می‌کنیم تا trust ایجاد شود.

۱۳. صفحه Trust Creation Complete ظاهر می‌شود. تنظیمات را چک کرده و روی Next کلیک می‌کنیم. حالا امکان تایید trust وجود دارد. این گزینه زمانی مفید است که هر دو سمت trust ایجاد شده باشد.

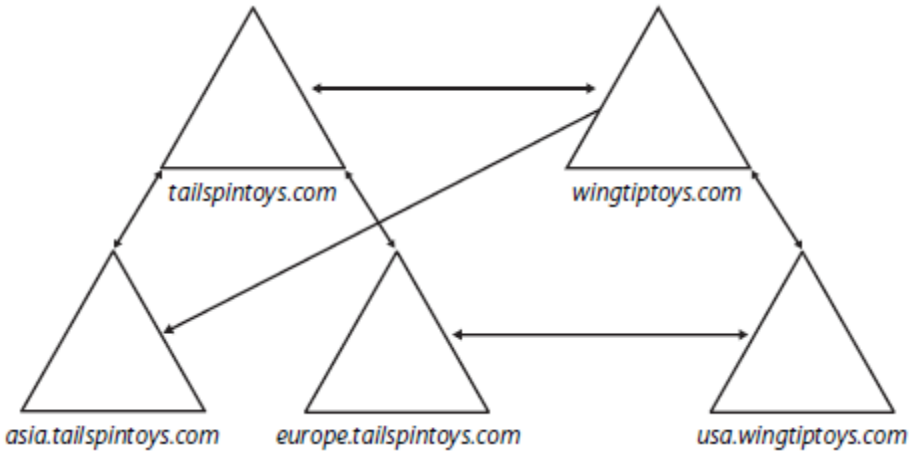
اگر در مرحله ۸ گزینه Both This Domain And The Specified Domain انتخاب شده باشد فرایند تمام شده است. ولی اگر در مرحله ۸ گزینه This Domain Only انتخاب شده باشد ارتباط trust ایجاد نمی‌شود مگر کاربر Administrator دامنه مقابل فرایند را به پایان برساند:

- اگر ارتباط trust برقرار شده یک‌طرفه و outgoing باشد مدیر شبکه دامنه مقابل باید trust یک‌طرفه و incoming بسازد.
- اگر ارتباط trust برقرار شده یک‌طرفه و incoming باشد مدیر شبکه دامنه مقابل باید trust یک‌طرفه و outgoing بسازد.
- اگر ارتباط trust برقرار شده دوطرفه باشد مدیر شبکه دامنه مقابل باید trust دوطرفه بسازد.

Trust میانبر (Shortcut Trust)

در بخش قبلی فرایند ۱۱ مرحله‌ای اعطاء بلیط session برای یک کلاینت به منظور دسترسی به منابع دامنه دیگر در یک forest را دیدیم. بسیاری از این مراحل به ارجاع کاربر به دامنه‌های مسیر trust path بین دامنه خود کاربر و دامنه دارای منبع مورد نظر ختم شد. وقتی کاربری از دامنه‌ای به کامپیوتری در دامنه دیگر متصل می‌شود درخواست تایید هویت باید trust path را طی کند. این کار روی کارایی تاثیر می‌گذارد و اگر در یک دامنه در مسیر trust path، DC موجود نباشد کلاینت نمی‌تواند تایید هویت شود یا به سرویس دسترسی یابد.

Trust های میانبر با ایجاد ارتباط Trust مستقیم بین دامنه‌های فرزند در trust path برای غلبه بر این مشکلات طراحی می‌شوند. دو Trust میانبر در شکل ۱۰- ۱۲ دیده می‌شود.



شکل ۱۰- ۱۲ Trust های میانبر

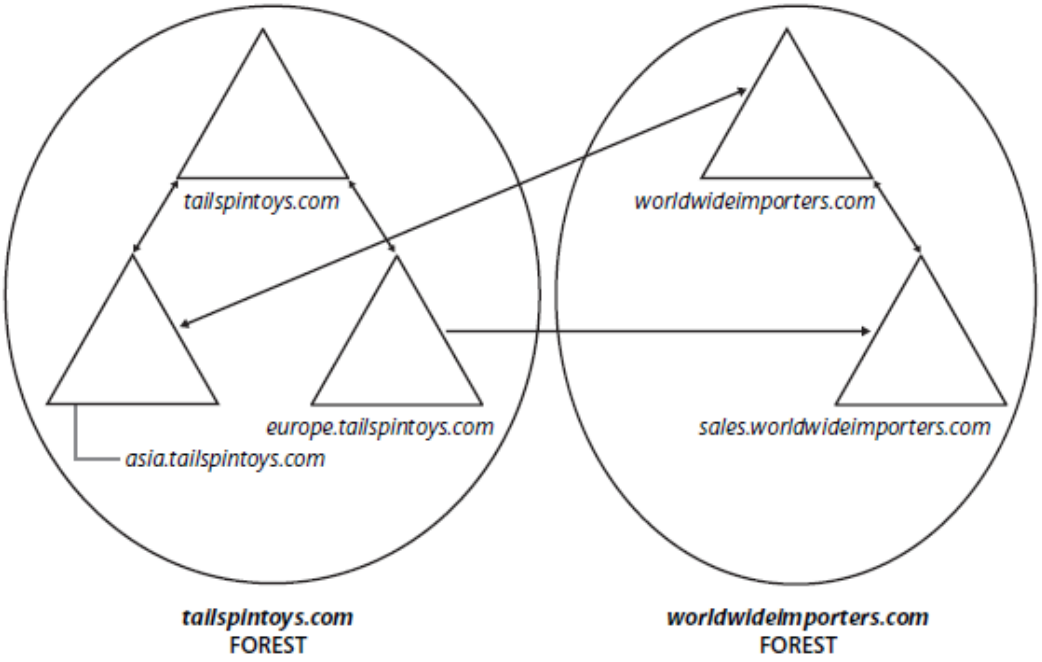
این نوع Trust ها تایید هویت و درخواست‌های بلیط session بین دامنه‌ها در یک forest چند دامنه‌ای را بهینه می‌کند. با حذف trust path زمان مورد نیاز برای طی مسیر حذف شده و در نتیجه کارایی درخواست بلیط ارتقاء می‌یابد.

Trust های میانبر می‌توانند یک‌طرفه یا دوطرفه باشند. در هر دو اینها Trust قابل انتقال است. در شکل ۱۰- ۱۲ از دامنه wingtiptoys.com به asia.tailspintoys.com یک Trust میانبر وجود دارد. وقتی کاربری از دامنه asia.tailspintoys.com به کامپیوتری در دامنه wingtiptoys.com متصل می‌شود یا منبعی را درخواست می‌کند درخواست می‌تواند مستقیما به DC در دامنه مورد اعتماد یعنی asia.tailspintoys.com ارجاع شود. ولی عکس آن صادق نیست. اگر کاربری در دامنه wingtiptoys.com به کامپیوتری در دامنه asia.tailspintoys.com متصل شود درخواست تایید هویت مسیر trust path را به سمت بالا tailspintoys.com و بعد به سمت پایین wingtiptoys.com طی می‌کند.

یک Trust میانبر دوطرفه بین usa.wingtiptoys.com و europe.tailspintoys.com ایجاد شده است. کاربران در هر دو دامنه می‌توانند تایید هویت شوند و توسط مسیر Trust میانبر به منابع یکدیگر دسترسی پیدا کنند.

Trust های خارجی (External Trust)

وقتی نیاز داریم با دامنه‌ای در خارج forest کار کنیم می‌توانیم یک Trust خارجی بسازیم. این نوعی Trust است که بین یک دامنه در forest ما و یک دامنه ویندوزی در یک forest دیگر برقرار می‌شود. نمونه‌هایی در شکل ۱۱- ۱۲ مشاهده می‌شود.



شکل ۱۱- ۱۲ یک Trust خارجی به سمت یک دامنه در forest دیگر

در شکل یک Trust یک‌طرفه بین دامنه sales.worldwideimporters.com و دامنه europe.tailspintoys.com دیده می‌شود. دامنه Europe به دامنه Sales اعتماد می‌کند بنابراین کاربران در دامنه Sales می‌توانند به کامپیوترهای دامنه Europe متصل شوند.

شکل ۱۱- ۱۲ همچنین یک Trust دوطرفه بین worldwideimporters.com و دامنه asia.tailspintoys.com را نشان می‌دهد. کاربران در دو دامنه به منابع دامنه دیگر دسترسی دارند. از لحاظ فنی همه Trust های خارجی غیرقابل انتقال و یک‌طرفه هستند. وقتی یک Trust خارجی دوطرفه ساخته می‌شود در واقع دو Trust یک‌طرفه در هر سمت ساخته شده است.

وقتی یک trust خارجی outgoing می‌سازیم Active Directory یک شیء واحد امنیتی خارجی برای هر شیء دامنه مورد اعتماد می‌سازد. از این به بعد این کاربران، گروهها و کامپیوترها می‌توانند عضو گروههای domain local شده یا به ACL منابع دامنه اعتمادکننده اضافه شوند.

برای ارتقاء امنیت ارتباط trust خارجی در صفحه Outgoing Trust Authentication Level از ویزارد New Trust گزینه Selective Authentication را انتخاب می‌کنیم. به علاوه قرنطینه دامنه که فیلترینگ SID نیز نامیده می‌شود به طور پیش‌فرض روی همه trust های خارجی فعال می‌باشد. هر دو این پیکربندی‌ها در همین فصل به تفصیل بررسی خواهد شد.

Trust های ناحیه‌ای (Realm Trust)

زمانی که از لحاظ سرویس‌های امنیتی پیاده سازی شده با Kerberos نسخه ۵ نیاز به سازگاری بین پلتفرم‌های مختلف داریم می‌توانیم یک trust ناحیه‌ای بین دامنه خود و UNIX Kerberos نسخه ۵ برقرار کنیم. این نوع trust یک‌طرفه است ولی می‌توان آنرا در هر دو طرف ایجاد کرد که در نهایت مانند این است که یک ارتباط دوطرفه داریم. به طور پیش‌فرض این trust ها غیرقابل‌انتقال هستند ولی می‌توانیم آنها را قابل انتقال کنیم.

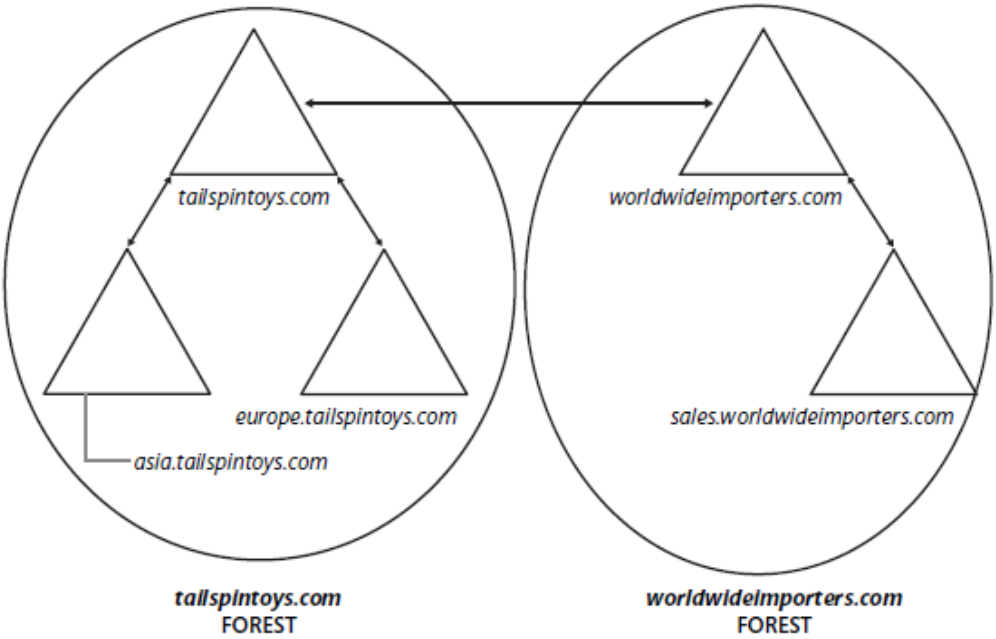
اگر یک trust ناحیه‌ای غیرویندوزی Kerberos نسخه ۵ به سمت دامنه ما موجود است همه واحدهای امنیتی دامنه ما قابل اعتماد خواهند بود. اگر دامنه ما به یک شبکه غیرویندوزی Kerberos نسخه ۵ trust داشته باشد کاربران آن به منابع دامنه ما دسترسی خواهند داشت ولی فرایند غیرمستقیم است. وقتی کاربران توسط یک شبکه غیرویندوزی تایید هویت می‌شوند بلیط‌های Kerberos حاوی همه داده مورد نیاز ویندوز نمی‌باشد. بنابراین یک سیستم نگاشت حساب وارد بازی می‌شود. واحدهای امنیتی در دامنه ویندوزی ساخته می‌شوند و به یک حساب هویت Kerberos خارجی در شبکه غیرویندوزی نگاشت می‌شود. دامنه ویندوزی فقط از این حساب‌ها برای ارزیابی دسترسی به اشیاء دامنه استفاده می‌کند. همه حساب‌های اینچنینی می‌توانند در گروهها و ACL های منابع به منظور

کنترل دسترسی در واحدهای امنیتی شبکه‌های غیرویندوزی استفاده شوند. نگاشت حساب از طریق ابزار Active Directory Users and Computers مدیریت می‌شود.

Forest Trusts

زمانی که به تعامل بین دو سازمان مجزا با دو forest نیاز داریم می‌توانیم از این نوع trust استفاده کنیم. Forest trust یک trust یک‌طرفه یا دوطرفه قابل انتقال بین دامنه‌های ریشه forest می‌باشد. شکل ۱۲- ۱۲ مثالی از این نوع را بین forest های tailspintoys.com و worldwideimporters.com نشان می‌دهد.

یک ارتباط trust از نوع forest با فرض اینکه دوطرفه باشد امکان تایید هویت کاربر را در همه دامنه‌ها فراهم می‌کند. اگر ارتباط یک‌طرفه باشد کاربران در forest مورد اعتماد توسط کامپیوترهای forest اعتمادکننده تایید هویت می‌شوند. این نوع trust از نظر برقراری، نگهداری و مدیریت ساده‌تر از ارتباط trust مجزا بین دامنه‌های forest می‌باشد.



شکل ۱۲- ۱۲ یک trust از نوع forest

هنگام ایجاد این نوع trust قرنطینه دامنه (فیلترینگ SID) به طور پیش‌فرض فعال می‌شود که در بخش‌های بعدی همین فصل بررسی می‌شود. ما می‌توانیم تعیین کنیم که ارتباط یک‌طرفه، incoming، outgoing یا دوطرفه باشد همان‌طور که قبلا اشاره شد forest trust قابل انتقال است و به همه دامنه‌های forest اعتمادکننده اجازه می‌دهد به همه دامنه‌های forest مورداعتماد اعتماد کنند. ولی forest trust به خودی خود قابل انتقال نیست. برای مثال اگر tailspintoys.com forest به worldwideimporters.com forest اعتماد کند و worldwideimporters.com forest به northwindtraders.com forest اعتماد کند این trust ها باعث نمی‌شود tailspintoys.com forest به northwindtraders.com اعتماد کند. اگر بخواهیم چنین شود باید trust اختصاصی برای آنها ایجاد کنیم.

برای برقراری forest trust پیش‌نیازهایی مورد نیاز است. سطح عملیاتی forest باید Windows Server 2003 به بعد باشد. به علاوه باید یک زیرساخت DNS مخصوص برای پشتیبانی از این نوع trust داشته باشیم.

مدیریت trust

اگر در عملکرد یک trust مشکلی مشاهده شد می‌توانیم ارتباط trust بین دو دامنه را ارزیابی کنیم. البته امکان ارزیابی این ارتباط به یک شبکه غیرویندوزی وجود ندارد. برای ارزیابی ارتباط trust مراحل زیر را دنبال می‌کنیم:

۱. ابزار Active Directory Domains And Trusts را اجرا می‌کنیم.

۲. روی دامنه حاوی trust که می‌خواهیم ارزیابی کنیم کلیک راست کرده و Properties را کلیک می‌کنیم.

۳. روی زبانه Trusts کلیک می‌کنیم.

۴. Trust را که می‌خواهیم ارزیابی کنیم انتخاب می‌کنیم.

۵. روی Properties کلیک می‌کنیم

۶. روی Validate کلیک می‌کنیم.

۷. یکی از موارد زیر را انجام می‌دهیم و روی OK کلیک می‌کنیم:

- روی Yes, Validate The Incoming Trust کلیک می‌کنیم. اعتبار عضو گروه Domain Admins یا Enterprise Admins را که در دامنه مقابل اعتبار دارد وارد می‌کنیم.
- روی No, Do Not Validate The Incoming Trust کلیک می‌کنیم. پیشنهاد می‌گردد این مراحل برای دامنه مقابل نیز تکرار شود.

از طریق خط فرمان نیز می‌توان ارزیابی را انجام داد.

```
Netdom trust TrustingDomainName /domain:TrustedDomainName /verify
```

اگر بخواهیم trust ایجاد شده به روش دستی را حذف کنیم مراحل زیر را انجام می‌دهیم:

۱. ابزار Active Directory Domains And Trusts را باز می‌کنیم.

۲. روی دامنه حاوی trust که می‌خواهیم حذف کنیم کلیک راست کرده و Properties را کلیک می‌کنیم.

۳. روی زبانه Trusts کلیک می‌کنیم.

۴. Trust را که می‌خواهیم حذف کنیم انتخاب می‌کنیم.

۵. روی Remove کلیک می‌کنیم.

۶. یکی از موارد زیر را انجام می‌دهیم و روی OK کلیک می‌کنیم:

- روی Yes, Remove The Trust From Both The Local Domain And The Other Domain کلیک می‌کنیم. اعتبار عضو گروه Domain Admins یا Enterprise Admins را که در دامنه مقابل اعتبار دارد وارد می‌کنیم.
- روی No, Do Not Remove The Trust From The Local Domain Only کلیک می‌کنیم. پیشنهاد می‌گردد این مراحل برای دامنه مقابل نیز تکرار شود.

۷. برای حذف trust ایجاد شده به روش دستی از طریق خط فرمان از دستور زیر استفاده می‌کنیم:

```
Netdom trust  TrustingDomainName  /domain:TrustedDomainName  /remove [/force]
/UserD:User /PasswordD:*
```

پارامتر UserD کاربر با اعتبار گروه Enterprise Admins یا Domain Admins دامنه مورد اعتماد است. مقدار دادن به پارامتر *:PasswordD باعث می‌شود دستور پیغامی را مبنی بر ورود کلمه عبور نمایش دهد سوئیچ /force در زمان حذف trust ناحیه‌ای مورد نیاز است.

امنیت ارتباط trust

وقتی trust بین دامنه‌ها برقرار می‌شود در واقع به کاربران دامنه مورد اعتماد اجازه استفاده از منابع دامنه اعتمادکننده را می‌دهیم. بخش‌های بعدی اجزاء مرتبط با امنیت منابع دامنه اعتمادکننده را بررسی می‌کند.

گروه Authenticated Users

خود trust هیچ‌گاه دسترسی به منابع را فراهم نمی‌کند بلکه به واسطه ACL منابع به کاربران گروه Authenticated Users دسترسی اعطاء می‌شود.

عضویت در گروههای Domain Local

همان‌طور که در فصل ۴ آموختیم بهترین راه برای مدیریت دسترسی به منابع اعطاء مجوز به گروه domain local می‌باشد. بعد ما می‌توانیم کاربران و گروهها را از دامنه خود به این گروه اضافه کنیم و به واسطه آن نسبت به منابع دسترسی بدهیم. ما می‌توانیم کاربران و گروههای global را از دامنه‌های مورد اعتماد به این گروه اضافه کنیم. بنابراین بهترین راه برای اعطاء دسترسی به کاربران دامنه مورد اعتماد اعطاء عضویت گروه domain local دامنه خود به کاربران و گروههای global آنان است.

ACL

همچنین امکان افزودن مستقیم کاربران و گروههای global از دامنه مورد اعتماد به ACL منابع دامنه اعتمادکننده وجود دارد. این رویکرد هرچند به خوبی روش قبلی نیست ولی امکان‌پذیر است.

قابلیت انتقال

وقتی یک trust ناحیه‌ای ایجاد می‌شود به طور پیش‌فرض trust قابلیت انتقال ندارد. اگر این قابلیت را ایجاد کنیم در واقع توانایی دسترسی به منابع دامنه خود را به کاربران دامنه مورد اعتماد شبکه‌های Kerberos نسخه ۵ می‌دهیم. پیشنهاد می‌گردد از trust های غیرقابل انتقال استفاده شود مگر اینکه مجبور باشیم.

قرنطینه دامنه

به طور پیش‌فرض در همه trust های خارجی و forest قرنطینه دامنه یا فیلترینگ SID فعال است. وقتی کاربری در یک دامنه مورداعتماد تایید هویت می‌شود داده اعتباری حاوی SID های حساب کاربر را در گروهها دارا می‌باشد. به علاوه داده اعتبار کاربر حاوی اطلاعات امنیتی خصیصه‌های دیگر کاربر و گروه آن است.

برخی از SID های ارائه شده از دامنه مورداعتماد توسط کاربر ممکن است در همان دامنه ساخته نشده باشد. برای مثال اگر کاربری از یک دامنه دیگر منتقل شده باشد SID جدیدی برای آن ساخته شده است. بنابراین حساب جدید دسترسی خود را به منابعی که قبلا دسترسی داشته از دست می‌دهد. برای حل این مشکل مدیر شبکه می‌تواند مشخص کند که خصیصه sIDHistory کاربر حاوی SID حساب قبلی باشد. وقتی کاربر تلاش می‌کند به منابع دسترسی داشته باشد SID اصلی در خصیصه sIDHistory دسترسی را ممکن می‌کند.

در سناریوی دامنه مورداعتماد ممکن است یک مدیرشبکه قلابی بتواند از اعتبار مدیریتی در دامنه مورداعتماد برای درج SID در خصیصه sIDHistory کاربر که مشابه SID حساب دارای دسترسی بالا در دامنه ماست استفاده کند. این کاربر از این پس دسترسی غیرمنطقی به منابع دامنه ما خواهد داشت.

قرنطینه دامنه از این مساله جلوگیری می‌کند. به این صورت که دامنه اعتمادکننده را قادر می‌سازد SID های دامنه مورداعتماد را که SID اولیه واحدهای امنیتی نیستند فیلتر کند. هر SID حاوی SID دامنه منشا می‌باشد بنابراین وقتی کاربری از دامنه مورد اعتماد لیست SID های کاربر و گروهها را ارائه می‌دهد فیلترینگ SID به دامنه اعتمادکننده دستور می‌دهد همه SID های بدون SID دامنه را از دامنه مورد اعتماد دور بیاندازد.

قرنطینه دامنه به طور پیش‌فرض برای همه trust های outgoing به دامنه‌های خارجی و forest ها فعال است. این قابلیت را زمانی غیرفعال می‌کنیم که یکی از حالات زیر اتفاق بیافتد:

- به مدیران شبکه دامنه مورد اعتماد اطمینان کامل داشته باشیم.
- برخی کاربران و گروهها به دامنه مورداعتماد با تاریخچه SID خود منتقل شده‌اند و ما می‌خواهیم به آنها مجوز دسترسی به منابع دامنه اعتمادکننده را بر اساس خصیصه sIDHistory اعطاء کنیم.

برای غیرفعال کردن قرنطینه دامنه دستورات زیر را به کار می‌گیریم:

Netdom trust TrustingDomainName /Domain:TrustedDomainName /quarantine:no

برای فعال کردن دوباره آن دستور زیر را تایپ می‌کنیم:

Netdom trust TrustingDomainName /Domain:TrustedDomainName /quarantine:yes

تایید هویت انتخابی (Selective Authentication)

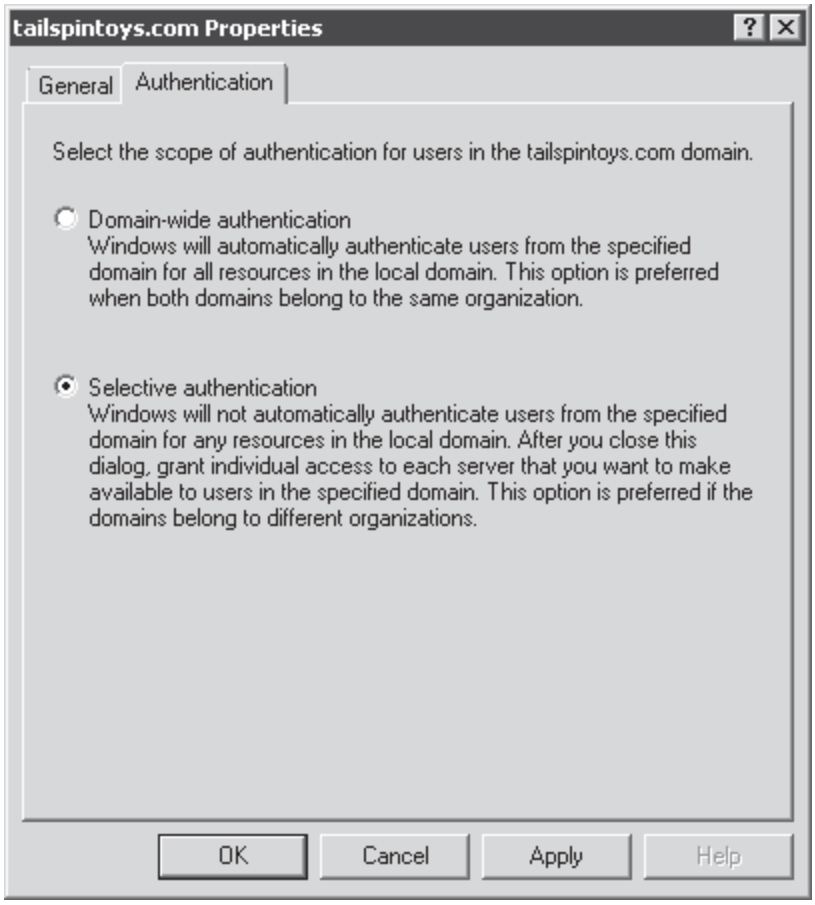
وقتی یک trust خارجی یا forest ایجاد می‌کنیم می‌توانیم حوزه تایید هویت واحدهای امنیتی مورد اعتماد را کنترل کنیم. دو حالت تایید هویت برای یک trust خارجی یا forest موجود است:

- تایید هویت انتخابی
- تایید هویت در سطح دامنه (برای یک trust خارجی) یا تایید هویت در سطح forest (برای یک forest trust)

اگر تایید هویت در سطح دامنه یا forest انتخاب شود همه کاربران دامنه مورد اعتماد برای دسترسی به سرویس‌ها روی همه کامپیوترهای دامنه اعتمادکننده تایید هویت می‌شوند. بنابراین کاربران مورداعتماد مجوز دسترسی به منابع دامنه اعتمادکننده را خواهند داشت. در این حالت از تایید هویت باید اطمینان کافی از بحث امنیت شبکه و مدیران شبکه داشته باشیم. به یاد داشته باشید کاربران دامنه مورداعتماد در دامنه اعتماد کننده به مانند کاربران گروه Authenticated Users عمل می‌کنند.

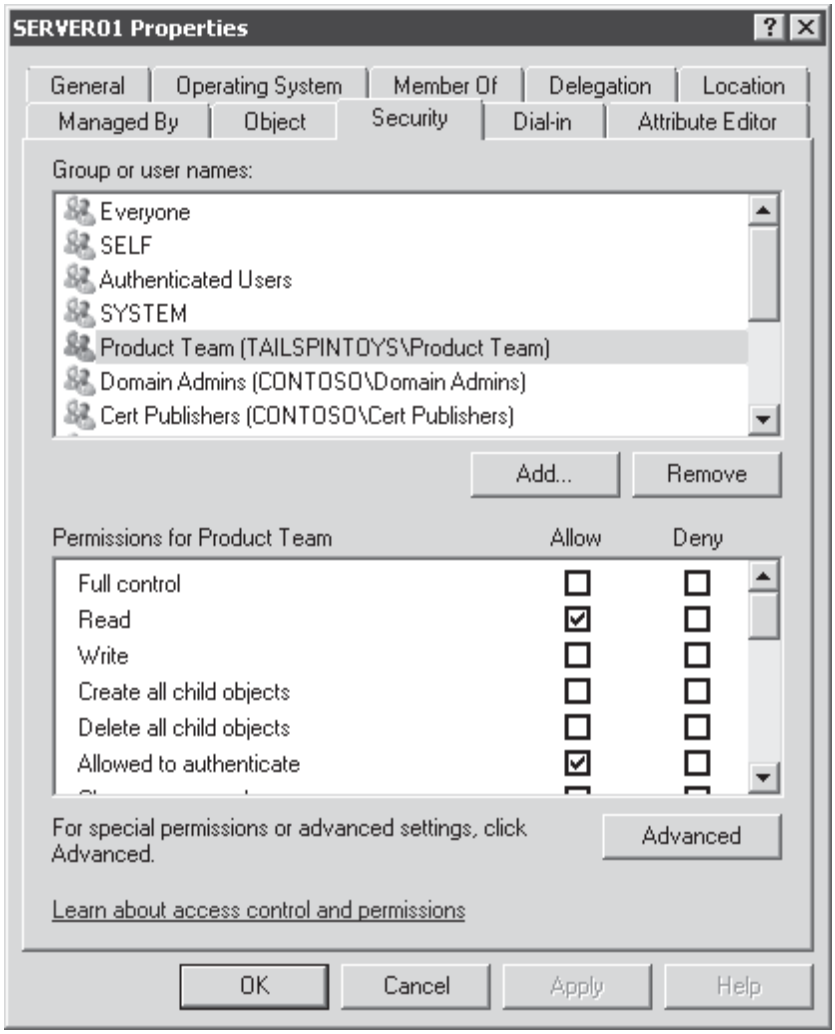
ولی اگر تایید هویت انتخابی داشته باشیم همه کاربران دامنه مورداعتماد به همه سرویس‌های دامنه اعتماد کننده دسترسی نخواهند داشت و فقط به آنهایی دسترسی دارند که ما مشخص می‌کنیم. برای مثال فرض کنید با یک دامنه سازمان دیگر trust خارجی داریم. حال می‌خواهیم فقط کاربران گروه بازاریابی آنها به پوشه‌های اشتراکی ما روی یکی از فایل سرورهای ما دسترسی داشته باشند. برای این کار تایید هویت انتخابی را برای ارتباط trust پیکربندی کرده و به کاربران مورداعتماد اجازه تایید هویت فقط برای یک فایل سرور مجوز می‌دهیم.

برای پیکربندی حالت تایید هویت برای یک trust از نوع outgoing از صفحه Outgoing Trust Authentication Level در ویزارد New Trust استفاده می‌کنیم. سطح تایید هویت را برای trust موجود پیکربندی کرده و صفحه properties دامنه اعتمادکننده را در ابزار Active Directory Domain And Trusts باز می‌کنیم. سپس ارتباط trust را انتخاب و روی Properties کلیک کرده و بعد زبانه Authentication را همانند شکل ۱۳- ۱۲ کلیک می‌کنیم.



شکل ۱۳- ۱۲ زبانه Authentication مربوط به کادر محاوره‌ای properties یک trust

پس از انتخاب Selective Authentication برای trust دیگر هیچ کاربری از دامنه مورداعتماد قادر به دسترسی به منابع دامنه اعتمادکننده نخواهد بود حتی اگر به آن کاربر مجوز داده شده باشد. همچنین باید به کاربران مجوز Allowed To Authentication روی شیء کامپیوتر دامنه داده شود. برای اعطاء این مجوز ابزار Active Directory Users And Computers را باز کرده و مطمئن می‌شویم که گزینه Advanced Features در منوی View انتخاب شده است. پنجره properties کامپیوتر میزبان سرویس را باز کرده و در زبانه Security کاربران مورداعتماد را اضافه کرده و کادر Allow مربوط به مجوز Allowed To Authenticate را همانند شکل ۱۴- ۱۲ علامت می‌زنیم.



شکل ۱۴- ۱۲ انتساب مجوز Allowed To Authentication به یک گروه مورداعتماد

تمرینات مدیریت یک رابطه Trust

در این تمرینات یک رابطه trust را بین دو دامنه contoso.com و tailspintoys.com ساخته ، ایمن و مدیریت می کنیم. در این سناریو شرکت Contoso همکار شرکت Tailspin Toys بوده و یک تیم از محققان شرکت Tailspin Toys نیازمند دسترسی به یک پوشه مشترک در دامنه contoso.com هستند. برای انجام این تمرینات باید تمرین درس یکم را انجام داده باشیم که در آن صورت دو DC خواهیم داشت ، یکی درforest و دامنه contoso.com و دیگری درforest و دامنه tailspintoys.com .

تمرین اول پیکربندی DNS

در مورد DNS مهم است که قبل از برقراری رابطه trust درست کار کند. هر دامنه باید توانایی تحلیل نام در دیگر دامنه ها را داشته باشد. در درس نهم نحوه پیکربندی تحلیل نام را یاد گرفتیم. برای برقرای تحلیل نام بین دو forest چندین راه مختلف وجود دارد. در این تمرین ما یک stub zone در دامنه contoso.com برای دامنه tailspintoys.com و یک conditional forwarder در دامنه tailspintoys.com برای تحلیل نامهای دامنه contoso.com می سازیم

۱- با کاربر مدیر شبکه وارد SERVER01.contoso.com می شویم
۲- DNS Manager را از منوی Administrative Tools باز می کنیم
۳- گره SERVER01 را باز کرده و Forward Lookup Zones را انتخاب می کنیم
٤- روی Forward Lookup Zones راست کلیک کرده و New Zone را انتخاب می کنیم
صفحه Welcome To The New Zone Wizard ظاهر می شود.
٥- روی Next کلیک می کنیم

صفحه Zone Type ظاهر می شود

٦- Stub Zone را انتخاب کرده و روی Next کلیک می کنیم

صفحه Active Directory Zone Replication Scope ظاهر می شود

۷- روی Next کلیک می کنیم

صفحه Zone Name ظاهر می شود

۸- عبارت tailspintoys.com را نوشته و روی Next کلیک می کنیم

صفحه Master DNS Servers ظاهر می شود

۹- 10.0.0.111 را تایپ کرده و کلید Tab را فشار می دهیم

۱۰-گزینه Use The Above Servers To Create A Local List Of Master Servers را علامت می زنیم ، روی Next کلیک کرده و سپس روی finish کلیک می کنیم.

۱۱-با کاربر مدیر شبکه وارد SERVERTST.tailspintoys.com می شویم

۱۲-DNS Manager را از منوی Administrative Tools باز می کنیم

۱۳-گره SERVERTST را باز می کنیم

۱٤-روی پوشه Conditional Forwarders راست کلیک کرده و New Conditional Forwarder را انتخاب می کنیم

۱٥-در کادر DNS Domain عبارت contoso.com را تایپ می کنیم

۱٦-Click Here To Add An IP را انتخاب کرده و 10.0.0.11 را تایپ می کنیم

۱۷-گزینه Store This Conditional Forwarder In Active Directory, And Replicate It As Follows را انتخاب می کنیم

۱۸-روی OKکلیک می کنیم

تمرین دوم ساخت یک رابطه trust

در این تمرین برای ایجاد فرآیند اعتبار سنجی کاربران Tailspin Toys در دامنه Contoso یک رابطه trustخواهیم ساخت

۱- کاربران tailspintoys.com نیازمند دسترسی به یک پوشه مشترک در contoso.com هستند. به سوالات زیر پاسخ دهید:

- کدام دامنه اعتمادکننده و کدام دامنه مورداعتماد می باشد؟
- کدام دامنه outgoing trust و کدام دامنه incoming trust می باشد؟

پاسخ: دامنه contoso.com ، دامنه اعتمادکننده با outgoing trust می باشد و دامنه tailspintoys.com یک دامنه trust مورد اعتماد با incoming trust است

۲- با اعتبار مدیر دامنه contoso.com وارد SERVER01 می شویم

۳- کنسول Active Directory Domains And Trusts را از Administrative Tools باز می کنیم

٤- روی contoso.com راست کلیک کرده و Properties را انتخاب می کنیم

٥- روی زبانه Trusts کلیک می کنیم

٦- روی New Trust کلیک می کنیم

صفحه Welcome To The New Trust Wizard ظاهر می شود

۷- روی Next کلیک می کنیم

صفحه Trust Name ظاهر می شود

۸- در کادر نام tailspintoys را نوشته و روی Next کلیک می کنیم

چون DNS در SERVER01 برای فرستادن پرس و جوها به tailspintoys.com پیکر بندی نشده است. باید از نام NetBIOS استفاده کنیم ولی در محیط واقعی توصیه می شود که از نام DNS استفاده کنیم.

صفحه Trust Type ظاهر می شود

۹- External Trust را انتخاب کرده و روی Next کلیک می کنیم

صفحه Direction of Trust ظاهر می شود

۱۰- One-way: Outgoing را انتخاب کرده و روی Next کلیک می کنیم

صفحه Sides Of Trust ظاهر می شود

۱۱- This Domain Only را انتخاب کرده و روی Next کلیک می کنیم

صفحه Outgoing Trust Authentication Level ظاهر می شود

۱۲- Domain-Wide Authentication را انتخاب کرده و روی Next کلیک می کنیم

صفحه Trust Password ظاهر می شود

۱۳- یک کلمه عبور پیچیده در کادرهای Trust Password و Confirm Trust Password می نویسیم.

این کلمه عبور را به یاد خواهیم داشت چون برای پیکربندی incoming trust برای دامنه tailspintoys.com به آن نیاز داریم. روی Next کلیک می کنیم

صفحه Trust Selections Completeظاهر می شود

۱۴- تنظیمات را مرور کرده و روی Next کلیک می کنیم

صفحه Trust Creation Complete ظاهر می شود

۱۵- وضعیت تغییرات را مرور کرده و روی Next کلیک می کنیم

صفحه Confirm Outgoing Trust ظاهر می شود .تا قبل از ساخت دو طرف trust نباید آنرا تایید کنیم

۱۶- روی Next کلیک می کنیم

صفحه Completing The New Trust Wizard ظاهر می شود

۱۷- روی Finish کلیک می کنیم

یک کادر محاوره ای ظاهر می شود و به ما یادآوری می کند که SID filtering به صورت پیش فرض فعال است

۱۸- روی OK کلیک می کنیم

۱۹- روی OK برای بسته شدن کادر محاوره ای Properties دامنه contoso.com ، کلیک می کنیم

ساخت incoming trust برای دامنه tailspintoys.com تمام شد.

۲۰- با اعتبار مدیر شبکه دامنه tailspintoys.com به دامنه وارد SERVERTST.tailspintoys.com می شویم

۲۱- Active Directory Domains And Trusts را از Administrative Tools باز می کنیم

۲۲- روی tailspintoys.com راست کلیک کرده و Properties را انتخاب می کنیم

۲۳- روی زبانه Trusts کلیک می کنیم

۲۴- روی New Trusts کلیک می کنیم

صفحه Welcome To The New Trust Wizard ظاهر می شود

۲۵- روی Next کلیک می کنیم

صفحه Trust Name ظاهر می شود

۲۶- در کادر نام contoso را نوشته و روی Next کلیک می کنیم

صفحه Trust Type ظاهر می شود

۲۷- External Trust را انتخاب کرده و روی Next کلیک می کنیم

صفحه Direction Of Trustظاهر می شود

۲۸- One-way: Incoming را انتخاب کرده و روی Next کلیک می کنیم

صفحه Sides Of Trust ظاهر می شود

۲۹-This Domain Only را انتخاب کرده و روی Next کلیک می کنیم
صفحه Trust Password ظاهر می شود
۳۰-کلمه عبوری که در مرحله ۱۳ وارد کردیم را در کادرهای Trust Password وConfirm Trust Password وارد می کنیم و روی Next کلیک می کنیم
صفحه Trust Selections Complete ظاهر می شود
۳۱-روی Next کلیک می کنیم
صفحه Trust Creation Complete ظاهر می شود
۳۲-وضعیت تغییرات را مرور کرده و روی Next کلیک می کنیم
صفحه Confirm Incoming Trust ظاهر می شود
۳۳-روی Next کلیک می کنیم
صفحه Completing The New Trust Wizard ظاهر می شود
۳٤-روی Finish کلیک می کنیم
۳۵-روی OK کلیک می کنیم

تمرین سوم تایید اعتبار Trust

در مرحله ۳۳ تمرین قبل این فرصت را داشتیم تا رابطه trust را تایید کنیم. همچنین می توانیم این کار را برای یک trust موجود انجام دهیم. در این تمرین trust بین contoso.com و tailspintoys.com را تایید اعتبار می کنیم

۱- با اعتبار مدیر شبکه دامنه contoso.com وارد SERVER01.contoso.com می شویم
۲- کنسول Active Directory Domains And Trusts را از Administrative Tools باز می کنیم
۳- روی contoso.com راست کلیک کرده و Properties را انتخاب می کنیم
۴- روی زبانه Trusts کلیک می کنیم
۵- *tailspintoys.com* را انتخاب و روی Properties کلیک می کنیم
۶- روی Validate کلیک می کنیم
پیامی مبنی بر معتبر و فعال بودن trust ظاهر می شود
۷- روی OK کلیک می کنیم
۸- برای بسته شدن کادر محاوره ای Properties دوبار روی OK کلیک می کنیم

تمرین چهارم فراهم کردن دسترسی برای کاربران مورد اعتماد

در این تمرین به گروه تولید شرکت Tailspin Toys به یک پوشه مشترک در دامنه contoso دسترسی می دهیم.

۱-اشیاء زیر را بسازید

- یک گروه global با نام **Product Team** در دامنه *tailspintoys.com* .
- یک گروه global با نام **Product Developers** در دامنه *contoso.com*
- یک گروه domain local با نام **ACL_Product_Access** در دامنه *contoso.com*

۲- یک پوشه با نام **Project** در درایو C از SERVER01 می سازیم
۳- به گروه ACL_Product_Access دسترسی Modify به پوشه Project می دهیم
۴- ابزار Active Directory Users And Computers را در دامنه *contoso.com باز می کنیم*
۵- Properties گروه ACL_Product_Access را باز می کنیم
۶- روی زبانه Members کلیک می کنیم
۷- روی Add کلیک می کنیم

۸- عبارت **Product Developers را نوشته و OKرا کلیک می کنیم**

۹- روی Add کلیک می کنیم

۱۰-عبارت **TAILSPINTOYS\Product Team را نوشته و OK را کلیک می کنیم**

یک پنجره امنیتی باز می شود. چون trust یک طرفه می باشد ، کاربر ما به عنوان مدیر شبکه contoso.com دسترسی به دایرکتوری دامنه tailspintoys.com را ندارد. باید حسابی در دامنه tailspintoys.com داشته باشیم تا بتوانیم دایرکتوری آن را بخوانیم. اگر این trust یک ارتباط دو طرفه بود این هشدار امنیتی ظاهر نمی شد.

۱۱- در کادر نام کاربر عبارت **TAILSPINTOYS\Administrator را می نویسیم**

۱۲-**در کادر کلمه عبور ، کلمه عبور مدیر شبکه در دامنه** *tailspintoys.com را می نویسیم*

۱۳-**روی OKکلیک می کنیم**

۱۴- **بررسی می کنیم که هر دو گروه** global عضو گروه domain local ، در دامنه contoso.com هستند و به پوشه مشترک دسترسی دارند

تمرین پنجم پیاده سازی تایید اعتبار انتخابی

در این تمرین توانایی کاربران دامنه *tailspintoys.com* را برای تایید اعتبار توسط رایانه های دامنه *contoso.com* محدود می کنیم

۱- در SERVER01.contoso.com ، Active Directory Domains And Trusts را باز می کنیم

۲- روی *contoso.com راست کلیک کرده و* Properties را انتخاب می کنیم

۳- روی زبانه Trusts کلیک می کنیم

٤- *tailspintoys.com* را انتخاب کرده و روی Properties کلیک می کنیم

٥- *روی زبانه* Authentication کلیک می کنیم

٦- *روی گزینه* Selective Authentication کلیک کرده و سپس دو بار OK را کلیک می کنیم

با فعال کردن selective authentication کاربران دامنه مورد اعتماد حتی با داشتن اجازه دسترسی به پوشه نمیتوانند برای دسترسی به رایانه های دامنه اعتماد کننده تایید اعتبار شوند. کاربران مورد اعتماد باید مجوز Allow To Authenticaion را نیز روی خود رایانه ها داشته باشند

۷- ابزار Active Directory Users And Computers در دامنه *contoso.com را باز می کنیم*

۸- *روی منوی* View کلیک کرده و مطمئن می شویم که Advanced Features انتخاب شده باشد

۹- Domain Controllers OU را در کنسول انتخاب می کنیم

۱۰- در پنجره سمت راست روی SERVER01 راست کلیک کرده و Properties را انتخاب می کنیم

۱۱-روی زبانه Security کلیک می کنیم

۱۲-روی Add کلیک می کنیم

۱۳-عبارت **TAILSPINTOYS\Product Team را نوشته و روی OKکلیک می کنیم**

یک کادر محاوره ای امنیتی ظاهر می شود . چون trust یکطرفه است حساب کاربری ما به عنوان مدیر دامنه *contoso.com اجازه خواندن دایرکتوری دامنه tailspintoys.com را ندارد. به حساب کاربری در دامنه tailspintoys.com برای خواندن دایرکتوری tailspintoys.com نیاز داریم. اگر trust دوطرفه بود این پنجره ظاهر نمی شد.*

۱٤-در کادر نام کاربر عبارت **TAILSPINTOYS\Administrator را تایپ می کنیم**

۱٥-**در کادر کلمه عبور ، کلمه عبور** حساب مدیر دامنه *tailspintoys.com را تایپ می کنیم*

۱٦-**روی OKکلیک می کنیم**

۱۷-**در لیست** Permissions For Product Team ، تیک Allow و Allowed To Authenticate را می زنیم

۱۸-**روی OK کلیک می کنیم**

اکنون تیم دامنه *tailspintoys.com می توانند برای* SERVER01 اعتبارسنجی شوند و از طریق عضویت در گروه ACL_Product_Access به پوشه مشترک دسترسی داشته باشند. این گروه به هیچ رایانه دیگری نمی توانند دسترسی داشته باشند حتی اگر اجازه دسترسی به پوشه های آن رایانه را داشته باشند. **همچنین هیچ کاربر دیگری از** *tailspintoys.com/مکان دسترسی به منابع* SERVER01.contoso.com را ندارد

خلاصه درس

- **بهترین طراحی یک** Active Directory forest این است که دارای یک دامنه باشد ، اگرچه ممکن است بعلت تکثیر domain naming context بیش از یک دامنه در یک forest نیاز باشد
- **ابزار** Active Directory Migration Tool (ADMT) برای انتقال object ها بین دامنه های بین یا درون forest بکار می رود. هنگامی که یک حساب به دامنه دیگری منتقل می شود SID جدیدی می گیرد. SID قبلی نیز با به خصوصیت *SIDHistory* **حساب اضافه می شود و به همین دلیل حساب به منابعی که به SID اصلی حساب اختصاص داده شده بودند نیز دسترسی دارد. از ADMT همچنین برای عضویت گروه می توان استفاده کرد.**
- **رابطه trust این اجازه را می دهدکه کاربران دامنه** مورد اعتماد **در دامنه اعتمادکننده اعتبارسنجی شوند و در نتیجه بتوانند عضو گروههای محلی دامنه شده یا به منابع درون دامنه دسترسی داشته باشند.**
- **در درون forest بین دامنه های فرزند و والد و بین هر دامنه ریشه** tree و دامنه ریشه forest ، **trust از نوع دو طرفه و** transitive می باشد. همچنین با برقراری shortcut trust می توان تایید هویت را بهبود داد
- **می توانیم برای دامنه های خارجی ،forestها و** Kerberos v5 realms **نیز trust بسازیم. این trustها می توانند یکطرفه یا دوطرفه باشند و در مورد** Kerberos v5 realms می توانند transitive یا nontransitive باشند. Trustهای forest همیشه transitive و trustهای خارجی همیشه nontransitive هستند
- **اعتبارسنجی انتخابی به ما این اجازه را می دهد که تعیین کنیم کدام گروه ها و کاربران دامنه** مورد اعتماد **می توانندر دامنه اعتماد کننده** اعتبارسنجی شوند
- **قرنطینه دامنه که با نام** SID filtering نیز شناخته می شود به صورت پیش فرض در trustهای خارجی و forest فعال است و از تایید هویت کاربران مورد اعتماد با SID غیر از SID دامنه اصلی آن کاربر جلوگیری می کند.

سئوالات پایان درس

۱- به عنوان مدیر شبکه در شرکت Wingtip Toys مشغول به کار هستیم. که شرکت Tailspin Toys را به تازگی خریده است . می خواهیم forest دو شرکت به صورتی باشد که تمام اشیاء در دامنه wingtiptoys.com بوده و تمام کاربران دامنه های wintiptoys.com و europe.wingtiptoys.com اجازه دسترسی به تمام رایانه های دامنه tailspintoys.com را داشته باشند. کدام یک از موارد زیر رابطه trust را که باید پیکربندی کنیم شرح می دهد؟ ؟(در صورت نیازتمام گزینه های درست را انتخاب کنید. هر پاسخ صحیح بخشی از راه حل است)

A . Incoming
B . Outgoing
C . One-way
D . Two-way
E . Realm
F . Shortcut
G . Forest
H . External

۲- به عنوان مدیر شبکه در شرکت Wingtip Toys مشغول به کار هستیم. که شرکت Tailspin Toys را به تازگی خریده است . برای دسترسی کاربران دامنه *tailspintoys.com* به *منابعی که به دامنه* *wingtiptoys.com* *منتقل شده اند* یک *trust* *یکطرفه* و outgoing **ساخته ایم .عده ای از کاربران به منابع دسترسی دارند اما تعدادی نیز نمی توانند به منابع دسترسی داشته باشند متوجه می شویم که کاربرانی که مشکل دارند هشت سال یا بیشتر برای** Tailspin Toys کار می کنند و حساب آنها از دامنه ویندوز NT 4.0 **انتقال داده شده است. برای دسترسی آنها به منابع چه باید بکنیم؟** (در صورت نیازتمام گزینه های درست را انتخاب کنید)

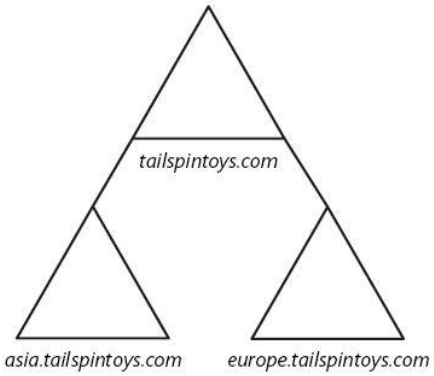
A . ساخت نام کاربری و کلمه عبور در دامنه *wingtiptoys.com* *مشابه حساب آنها در دامنه* *tailspintoys.com* .

B . ساخت مجدد دامنه ویندوز NT 4.0 **و ارتقا DC ها به ویندوز سرور 2008**

C . اجرای دستور *Netdom* trust **با پارامتر** */verify*

D . اجرای دستور *Netdom* trust **با پارامتر** */quarantine:no*

۳- **مدیر شبکه forestای هستیم که در شکل زیر نشان داده شده است DC های دامنه** *tailspintoys.com* *در لس آنجلس واقع شده اند. DCهای آسیا در بیجینگ هستند DC های اروپا نیز در استکهلم واقع شده اند.کاربران اروپا و آسیا گزارش داده اند که به پوشه های مشترک در دامنه های یکدیگر با تاخیر دسترسی دارند.کارایی در دسترسی* کاربران به اسنادشان مهم است. برای بهبود کارایی چه باید بکنیم؟



A . سیستم عامل رایانه کاربران را مجدد نصب می کنیم

B . آدرس IP را به static تغییر می دهیم

C . در DNS ، dynamic updates را غیر فعال می کنیم

D . بین اروپا و آسیا رابطه trust برقرار می کنیم

Directory Business Continuity

این بحث امروزه به یک بحث داغ تبدیل شده است مخصوصا از زمانی که سازمان‌ها در کل دنیا با مشکلاتی مواجه شده‌اند. گردبادها، زمین‌لرزه‌ها و بلایای طبیعی دیگر در مقیاس خیلی بزرگ تاثیرات منفی بسیاری روی سازمان‌ها داشته است. آمارها نشان می‌دهند که بالغ بر ۴۰ درصد سازمان‌های حدمتوسط که با این بلایا مواجه شده‌اند و برنامه business continuity نداشته‌اند شکست خورده‌اند. به همین دلیل نباید اجازه دهیم این مشکل برای ما نیز پیش بیاید و باید آمادگی لازم را در این زمینه داشته باشیم.

بلایا همیشه در مقیاس بزرگ حادث نمی‌شوند. کاربری را در نظر بگیرید که حسابش بر اثر یک اشتباه پاک شده است. این یک مشکل در مقیاس کوچک است. کاربر وقتی صبح تلاش می‌کند به شبکه وارد شود ولی موفق نمی‌شود و نمی‌داند مشکل از کجا ناشی می‌شود. به همین دلیل از برنامه‌های پیش‌گیرانه استفاده می‌کنیم که همیشه در مقابل هر مشکلی می‌توانیم به کار خود ادامه دهیم. برای این کار باید دو زمینه business continuity را داشته باشیم یکی نگهداری و محافظت از داده دایرکتوری و دیگری مدیریت کارایی دایرکتوری.

هر کدام از این زمینه‌ها یک وجه از business continuity را پوشش می‌دهد. زمینه سوم در دسترس بودن همیشگی است که در مدل اجرایی AD DS پیاده می‌شود. هر DC غیر از RODC دارای قابلیت پشتیبانی از تکثیر multi-master می‌باشد. به همین دلیل هر گاه بیش از یک DC در یک دامنه داشته باشیم سرویس با قابلیت دسترسی بالا خواهیم داشت. بنابراین قوانین ساده توزیع به فرایند قابلیت دسترسی سرویس دایرکتوری کمک می‌کند.

اهداف امتحانی در این فصل:

- نگهداری Active Directory
  - نگهداری آفلاین
  - پیکربندی پشتیبان‌گیری و بازیابی
  - مانیتور کردن Active Directory

دروس این فصل:

- درس ۱: نگهداری پیش‌گیرانه دایرکتوری و محافظت از انباره داده
- درس ۲: مدیریت کارایی دایرکتوری پیش‌گیرانه

قبل از شروع

برای ادامه کار موارد زیر باید انجام شده باشد:

- سرور ویندوز 2008 باید روی کامپیوتر فیزیکی یا مجازی با نام SERVER10 نصب شده باشد. این کامپیوتر میزبان نقش DNS و Active Directory Domain Services بوده و یک DC برای دامنه ریشه treyreasearch.net forest می‌باشد. دیسک دوم به سرور افزوده شود. حجم دیسک را به صورت پویا تا 10GB در نظر می‌گیریم و آنرا فرمت کرده و نام DATA به آن اختصاص می‌دهیم.
- سرور ویندوز 2008 باید روی کامپیوتر فیزیکی یا مجازی با نام SERVER11 نصب شده باشد. این کامپیوتر میزبان نقش DNS و Active Directory Domain Services می‌باشد که یک آدرس IP نسخه ۴ از محدوده خصوصی برای مثال 192.168.x.x به آن اختصاص می‌دهیم و آدرس سرور DNS آنرا آدرس SERVER10 تنظیم می‌کنیم.
- تمرینات فصل ۹ را باید انجام داده باشیم.

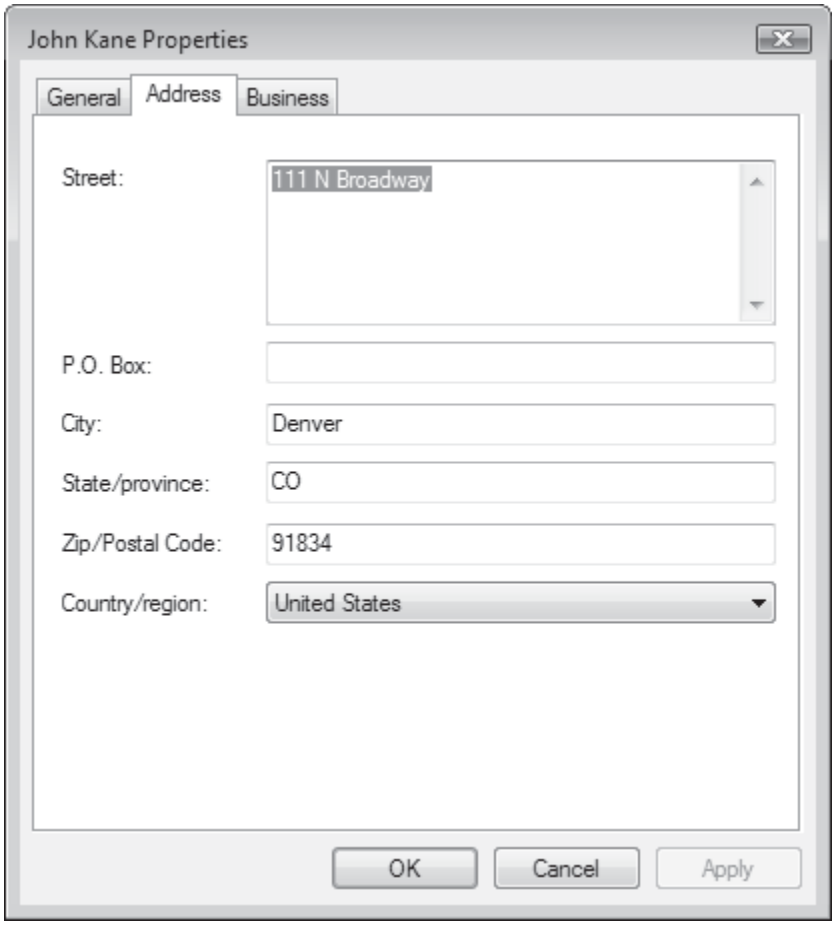
استفاده از VM در تمرینات اکیدا توصیه می‌شود. نقش‌های DC و DNS برای مجازی‌سازی از طریق Microsoft Virtual Server 2005 R2 یا Hyper-V ایده‌آل هستند.

درس ۱: نگهداری پیش‌گیرانه دایرکتوری و محافظت از انباره داده

یکی از مهم‌ترین مفاهیمی که مدیران شبکه هنگام کار با یک سرویس دایرکتوری نظیر AD DS نیاز دارند تقسیم وظایف خود می‌باشد. سرویس دایرکتوری خیلی شبیه یک سرویس وب می‌باشد. مدیران یک سرویس وب مسئول مدیریت IIS و سیستم عامل آن هستند نه مسئول نگهداری محتویات وب‌سایت.

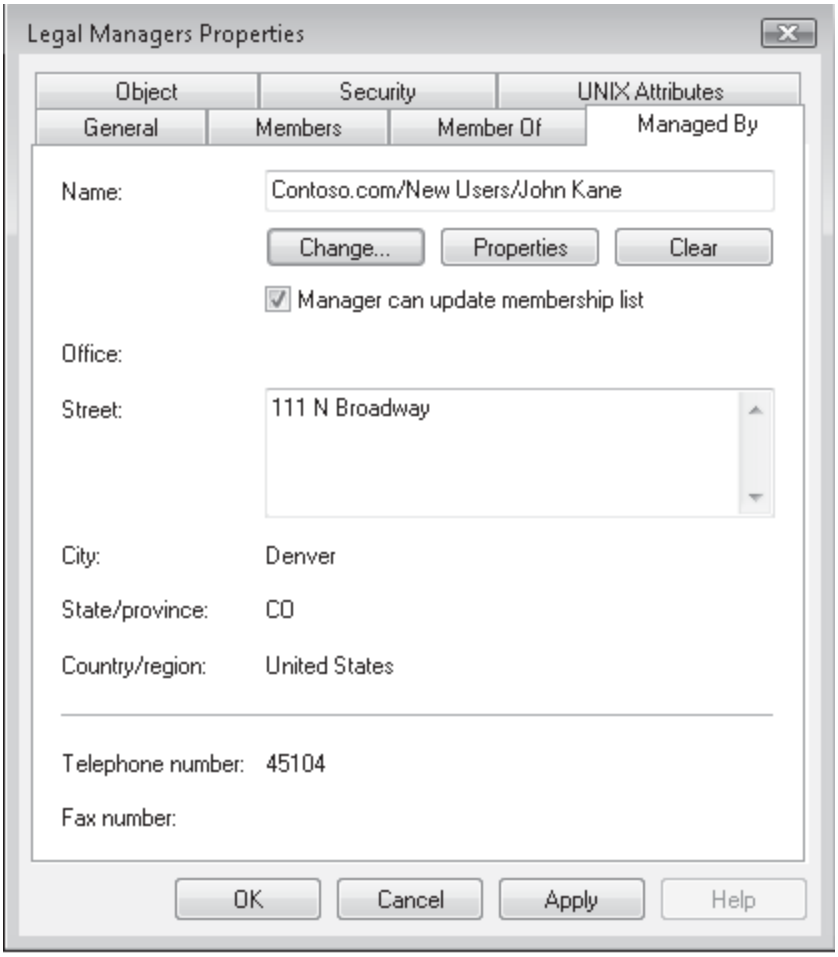
در یک سرویس وب باید مسئولیت‌ها بر اساس مدیریت داده و سرویس تقسیم شود. تیم IT مسئول مدیریت سرویس می‌باشد در حالی که کاربران مسئول مدیریت محتوا و داده هستند. همین وضعیت برای سرویس دایرکتوری نیز صادق است. AD DS بانک اطلاعاتی توزیع شده‌ای است که حاوی اطلاعات کاربران، کامپیوترها، سرورها و سرویس‌های شبکه می‌باشد از اینرو همانند LDAP جزء گروه سیستم‌های عامل شبکه‌ای (NOS) به حساب می‌آید. به همین دلیل فعالیت‌های مدیریتی شبکه بین تعداد زیادی از افراد سازمان تقسیم می‌شود:

- کاربران می‌توانند رکوردهای خود را به روز کنند. اگر یک کاربر از ویژگی Search Active Directory برای محل‌یابی



رکورد حساب خود استفاده کند اجازه خواهد یافت اطلاعاتی نظیر شماره تلفن، آدرس و بقیه موارد تغییر دهد.

- مدیران گروههای توزیع و امنیتی هنگامی که نقش AD DS نصب شود می‌توانند در صورت اعطاء حق لازم به طور خودکار محتویات گروه را مدیریت کنند. این رویکرد مناسبی برای کاهش بار کاری مدیران سیستم هنگام مدیریت سرویس دایرکتوری سیستم عامل شبکه‌ای می‌باشد. چطور متوجه می‌شویم کاربری عضو یک گروه است یا نه؟ در هر موردی وقتی مالکیت گروه تغییر می‌کند یعنی کسی این درخواست را از شما داشته و شما نیز پاسخ داده‌اید. چرا ما نباید خودمان را از چرخه خارج کنیم و مسئولیت مدیریت گروه را به خود آنان نسپاریم؟



- ریست کلمه عبور توسط گروه پشتیبانی انجام می‌شود و هر بار تیم را درگیر می‌کند.
- قابلیت دسترسی سرویس دایرکتوری و DNS مسئولیت اصلی مدیران سیستم بوده و باید در راس امور آنها قرار گیرد. در نهایت حضور مدیران سیستم به جهت پایداری سرویس‌های نام‌برده و داده دایرکتوری می‌باشد نه مدیریت خود داده.

وقتی استراتژی مدیریت پیش‌گیرانه را برنامه‌ریزی می‌کنیم روی جنبه‌های سرویس مدیریت عملیات و اعطاء مجوز مدیریت داده تا حد امکان کار می‌کنیم. قابلیت‌های تفویض اختیار AD DS این مدل را ارتقاء می‌دهد. ارتقاء این مدل با امکان اعطاء کنترل روی اشیاء به دیگران تعریف می‌شود. این رویکرد مباحث این فصل را تشکیل می‌دهد.

بعد از این درس یاد می‌گیریم:

- کدام وظایف مدیریتی برای نگهداری AD DS و DNS باید انجام شود
- تفاوت نگهداری آفلاین و آنلاین را درک کنیم
- نگهداری آفلاین انجام دهیم
- در وضعیت آنلاین بازیابی داده انجام دهیم
- در وضعیت آفلاین بازیابی داده انجام دهیم

زمان تقریبی : ۹۰ دقیقه

دوازده گروه مدیریت AD DS

مدیریت و اداره Active Directory دوازده فعالیت اصلی را پوشش می‌دهد. این فعالیت‌ها و وسعت پوشش آنها در جدول ۱- ۱۳ خلاصه شده و مشخص می‌کند کدام فعالیت روی مدیریت داده و محتوا و کدام روی مدیریت سرویس متمرکز می‌باشد.

جدول ۱- ۱۳ فعالیت‌های مدیریتی AD DS

فعالیت	شرح	سرویس	داده
مدیریت حساب کاربری و گروه	شامل ریست کلمه عبور کاربر، ساخت و غیرفعال کردن کاربر، ساخت گروه و مدیریت عضویت گروه‌ها می‌باشد. باید به تیم پشتیبانی محول شود.		√
مدیریت کلاینت	همه کامپیوترها در شبکه ویندوزی باید حساب داشته باشند. با این حساب با دایرکتوری ارتباط برقرار می‌کنند. باید به تکنسین‌های شبکه واگذار شود.		√
مدیریت سرویس‌های شبکه‌ای	شامل توزیع فایل‌های اشتراکی، پرینترها، DFS، پارتیشن‌های دایرکتوری برنامه و غیره می‌باشد. باید به مدیر هر سرویس واگذار شود.	√	√
مدیریت GPO	GPO ها قدرتمندترین مدل مدیریت اشیاء را در ویندوز سرور 2008 پیاده می‌کنند. باید به تکنسین‌های مناسب واگذار شود ولی یک GPO مرکزی باید تکثیر GPO را کنترل کند.	√	
مدیریت DNS	در حال حاضر DNS ارتباط نزدیکی با دایرکتوری دارد و عملکرد آن بستگی به کارکرد مناسب سرویس DNS دارد. به دلیل اینکه DNS با دایرکتوری عجین می‌شود مدیریت آن با مدیر آن دامنه است.	√	
توپولوژی Active Directory و مدیریت تکثیر	تکثیر یکی از مهم‌ترین عملیات سرویس دایرکتوری است. ما باید به منظور کنترل عملیات تکثیر به KCC تکیه کنیم. این کار مسئولیت مدیر دامنه است.	√	
مدیریت پیکربندی Active Directory	مدیریت پیکربندی با طراحی و پیاده سازی دامنه، forest و OU انجام می‌شود. نقش‌های FSMO، سرورهای GC و DC ها طراحی می‌شوند به دلیل اینکه این سرورها پیکربندی forest را تشکیل می‌دهند. یک فعالیت دیگری که به این مدیریت مربوط است همسان سازی زمان است. برای این منظور AD DS به PDC Emulator متکی است. این فعالیت‌ها جزء وظایف مدیران دامنه است.	√	
مدیریت Active Directory Schema	AD DS یک بانک اطلاعاتی توزیع شده حاوی schema بانک اطلاعاتی است. تغییرات schema به راحتی انجام نمی‌شوند چون اشیاء به سادگی حذف نمی‌شوند ولی می‌توانند به راحتی غیرفعال شوند یا تغییر نام دهند. این کار درحیطه وظایف مدیر forest است.	√	
مدیریت اطلاعات	این مدیریت با اطلاعات دایرکتوری حاوی اشیاء مرتبط است. اشیاء کاربر، پوشه‌های اشتراکی و اشیاء کامپیوتر دارای مالک هستند. گروهها دارای مدیر و پرینترها و کامپیوترها دارای اطلاعات محل استقرار هستند. در کنسول Active Directory Schema Management می‌توانیم محتویات GC را حذف یا اضافه کنیم و مشخص کنیم شیء index شود یا نه. همچنین می‌توان برای NTDS سهمیه در نظر گرفت که هر کس فقط در حد اختیار خود در دایرکتوری تغییر ایجاد کند. بهتر است تا حد ممکن وظیفه مدیریت اطلاعات را به دیگران تفویض کنیم.		√
مدیریت امنیت	مدیریت امنیت هر چیزی را از تنظیمات سیاست‌های حساب‌های دامنه و اعطاء حق کاربری گرفته تا مدیریت trust و ACL و ACE شامل می‌شود. این کار	√	

	وظیفه مدیر دامنه یا کاربران واجد شرایط دیگر که کار به آنها واگذار شده باشد می‌باشد.		
مدیریت بانک اطلاعاتی	مدیریت بانک اطلاعاتی نگهداری Ntds.dit و حفاظت از اشیاء AD DS و GPO می‌باشد. شامل مدیریت container های LostandFound و LostandFoundConfig می‌باشد که برای جمع‌آوری اشیاء بی نام و نشان طراحی می‌شود. همچنین حاوی بانک اطلاعاتی فشرده شده روی هر DC می‌باشد. اگرچه AD DS به طور خودکار و منظم بانک خود را فشرده می‌سازد فشرده سازی دستی نیز توصیه می‌شود. این کار وظیفه مدیر دامنه است.	√	
گزارش‌گیری از AD	از دایرکتوری گزارش تهیه می‌کنیم تا ببینیم چطور ساختاربندی شده حاوی چیست و چطور اجرا می‌شود. هیچ ابزار گزارش‌گیری متمرکز پیش‌فرضی وجود ندارد ولی می‌توانیم تحت سطوح مختلف دایرکتوری داده را منتقل کرد. همچنین امکان تولید گزارشات GPO با کنسول GPMC وجود دارد. این کار جزء وظایف مدیر دامنه و مسئول GPO است.	√	√

بسته به اندازه شبکه ما هرکدام از فعالیت‌های جدول بالا می‌تواند یک شغل ایجاد کند. به همین دلیل باید هر قسمتی از این کارها را به دیگران واگذار کنیم تا سرویس دایرکتوری همیشه در دسترس باشد. دو ابزار در این مورد به ما کمک می‌کند.

استفاده از AcctInfo.dll

برای مدیریت حساب‌های کاربری می‌توانیم از کنسول Active Directory Users and Computers استفاده کنیم. در این کنسول با دانلود و رجیستر کردن AcctInfo.dll روی سرور یا کلاینت دارای کنسول Active Directory Users and Computers می‌توانیم زبانه‌ای با نام Additional Account Info به صفحه properties شیء کاربر اضافه کنیم. این فایل و ابزار Account Lockout and Management هر دو بخشی از Resource Kit ویندوز سرور 2003 هستند.

برای نصب زبانه مذکور مراحل زیر را دنبال می‌کنیم. اگر روی کلاینت یا سرور غیر DC باشیم باید دسترسی کامل روی سیستم داشته باشیم و اگر روی سرور DC هستیم باید با کاربر administrator به سیستم وارد شویم.

۱. باید ابزار Remote Server Administration Tools (RSAT) مخصوصا ابزارهای مدیریت AD DS روی سیستم نصب شده باشد.

۲. ابزار Account Lockout And Management Tools را از سایت مایکروسافت دانلود کرده و روی پوشه Documents سیستم مورد نظر ذخیره می‌کنیم.

۳. ابزارها را از حالت فشرده خارج می‌کنیم.

۴. سپس فایل AcctInfo.dll را پیدا می‌کنیم.

۵. پنجره خط فرمان elevated را باز کرده و دستور زیر را تایپ می‌کنیم:

```
regsvr32 acctinfo.dll
```

۶. هنگام دریافت پیغام رجیستر موفق روی OK کلیک می‌کنیم و پنجره خط فرمان را می‌بندیم.

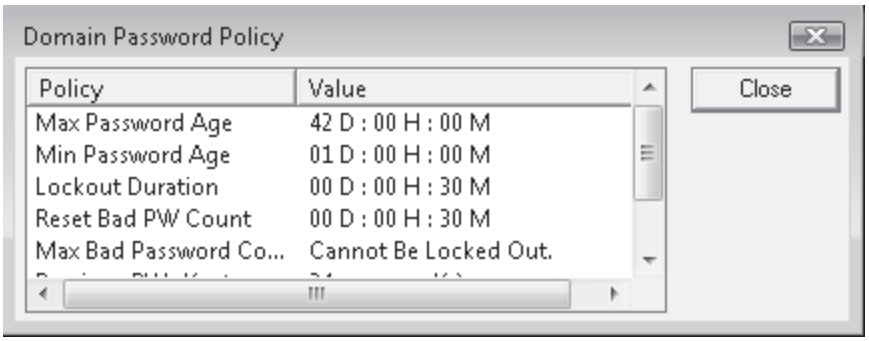
۷. کنسول Active Directory Users and Computers را باز و بسته می‌کنیم.

۸. یک حساب کاربری را انتخاب می‌کنیم.

۹. کادر محاوره‌ای properties آنرا باز می‌کنیم.

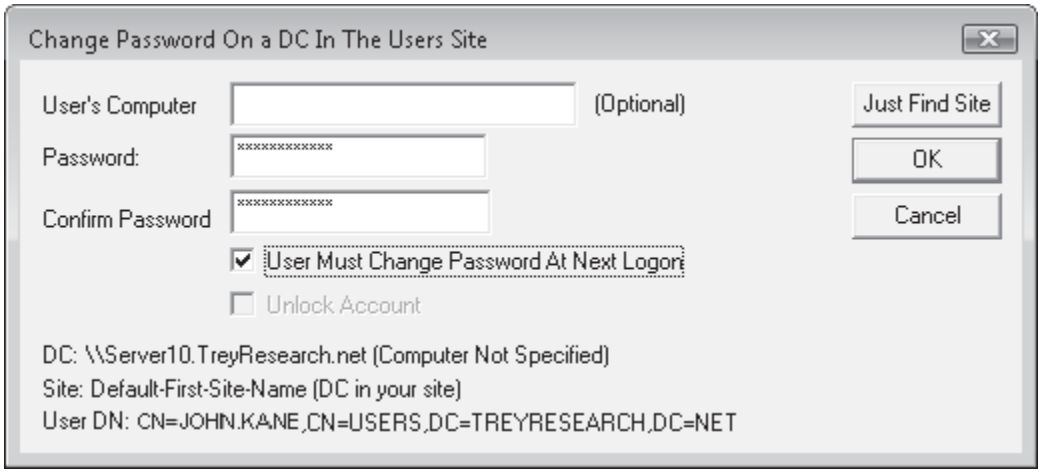
۱۰. زبانه Additional Account Info را باز می‌کنیم. به اطلاعات این صفحه توجه کنید. علاوه بر این اطلاعات موارد زیر را در این صفحه می‌بینیم:

- دکمه Domain PW Info سیاست کلمه عبور منتسب به این حساب را نمایش می‌دهد. AD DS از سیاست‌های کلمه عبور چندگانه در یک دامنه منفرد پشتیبانی می‌کند.

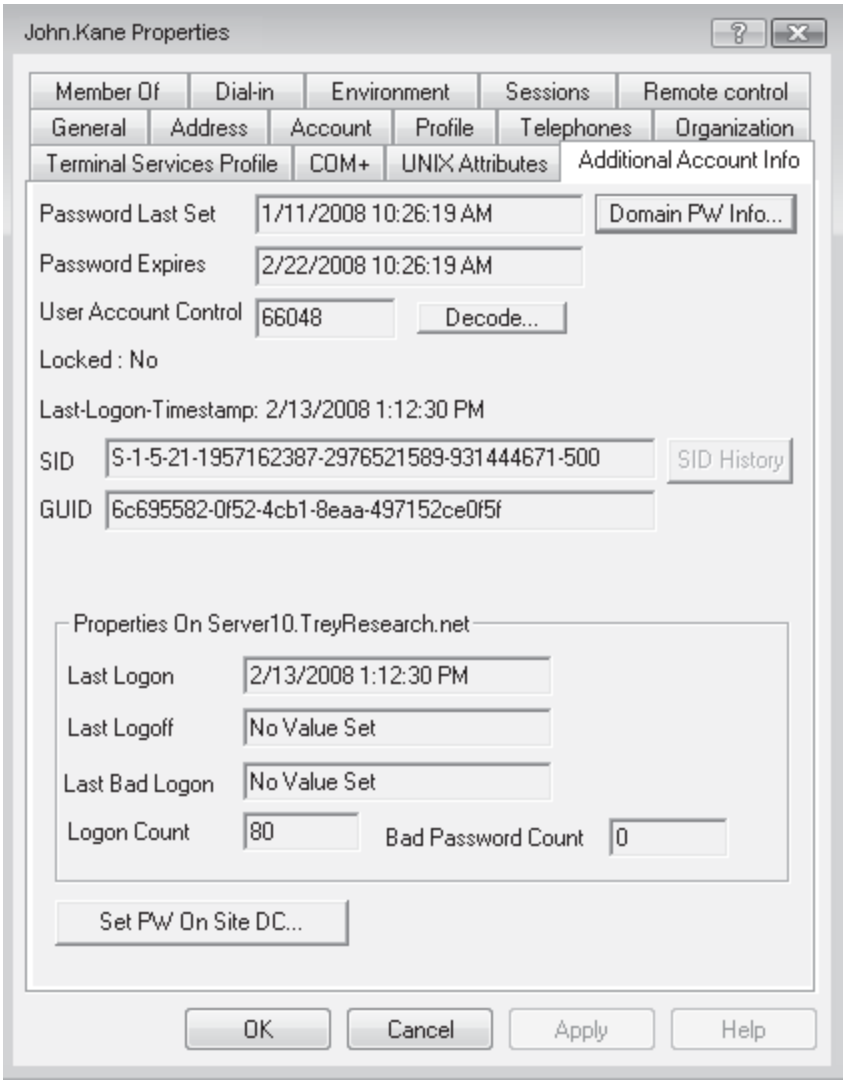


- SID History اطلاعات شناسه‌های امنیتی چندگانه را که یک حساب در زمان فعال شدن SID History در دامنه ممکن است داشته باشد نشان می‌دهد. البته این ویژگی هنگام اجرای عملیات انتقال حساب‌ها از یک دامنه به دامنه دیگر فعال می‌شود. در دامنه‌های جدید این ویژگی فعال نیست مگر اینکه انتقال صورت گیرد. برای جلوگیری از SID spoofing در دامنه بهتر است SID History پس از اتمام فرایند انتقال غیرفعال شود. اگر این ویژگی فعال باشد می‌توانیم از این دکمه برای ارزیابی انتساب SID به حساب‌ها استفاده کرد.

- گزینه PW On Site DC به ما امکان می‌دهد برای جلوگیری از تاخیر در تکثیر و اعطاء دسترسی سریع به کاربر کلمه عبور کاربر را ریست کنیم. از دکمه Just Find Site برای پیداکردن DC سایت و ریست کلمه عبور استفاده می‌کنیم.



این DLL در زمینه کمک به تیم پشتیبانی و مدیران شبکه کاملا مفید است.



شکل ۱- ۱۳ استفاده از زبانه Additional Account Info در کادر محاوره‌ای properties کاربر

استفاده از Specops Gpupdate

وقتی با اشیاء کامپیوتر کار می‌کنیم می‌توانیم روی شیء کلیک راست کرده و گزینه Manage را انتخاب کنیم تا کنسول Computer Management باز شود ولی این کار دسترسی به عملیات ساده‌ای نظیر به‌روزآوری از راه دور GPO ها یا دستورات ساده‌تر start، shut down یا restart را فراهم نمی‌کند. ولی می‌توانیم با یک add-on ساده و رایگان از Special Operations Software با نام Specops Gpupdate این کار را انجام دهیم. این add-on به عنوان مثال ارائه شده و به معنی توصیه نمی‌باشد. این ابزار به طور خودکار قابلیت‌هایی را به کنسول Active Directory Users and Computers اضافه می‌کند و امکان کنترل فعالیت‌های زیر را می‌دهد:

- به روز رسانی GPO از راه دور
- روشن کردن کامپیوتر از راه دور در صورت فعال بودن Wake-on-LAN
- روشن و خاموش کردن کامپیوتر
- گزارش‌گیری نتایج عملیات به صورت نمودار

در صورتی که اشیاء کامپیوتر را داخل OU قرار دهیم می‌توانیم عملیات بالا را روی کل OU هم اعمال کنیم. این ابزار برای مدیرانی که مایلند کامپیوترها و سرورهای خود را از راه دور مدیریت کنند مفید است.

برای پیاده‌سازی Specops Gpupdate مراحل زیر را انجام می‌دهیم. برای انجام این کار اگر روی کلاینت یا سرور غیر DC کار می‌کنیم نیاز به اعتبار مدیریتی محلی سیستم و اگر روی DC کارمی‌کنیم نیاز به اعتبار مدیریتی دامنه خواهیم داشت. همچنین برای رجیستر کردن یکباره Display Specifier در forest باید عضو گروه Enterprise Administrator باشیم.

۱. RSAT مخصوصا ابزارهای مدیریتی AD DS باید روی سیستم نصب باشد.

۲. از سایت Special Operations Software ابزار Specops Gpupdate را دانلود کرده و آنرا در پوشه Documents سیستم ذخیره می‌کنیم.

۳. آنرا از حالت فشرده خارج می‌کنیم.

۴. بعد محل فایل SpecopsGpupdate.msi را پیدا کرده و روی آن دوبار کلیک می‌کنیم.

۵. در کادر محاوره‌ای دکمه Run را کلیک می‌کنیم.

۶. در صفحه Welcome دکمه Next را کلیک می‌کنیم.

۷. مجوز را قبول کرده و Next را کلیک می‌کنیم.

۸. نام کامل و نام سازمان را تایپ کرده و کادر Anyone Who Uses This Computer را انتخاب کرده و روی Next کلیک می‌کنیم.

۹. محل نصب پیش‌فرض را قبول کرده و Next را کلیک می‌کنیم.

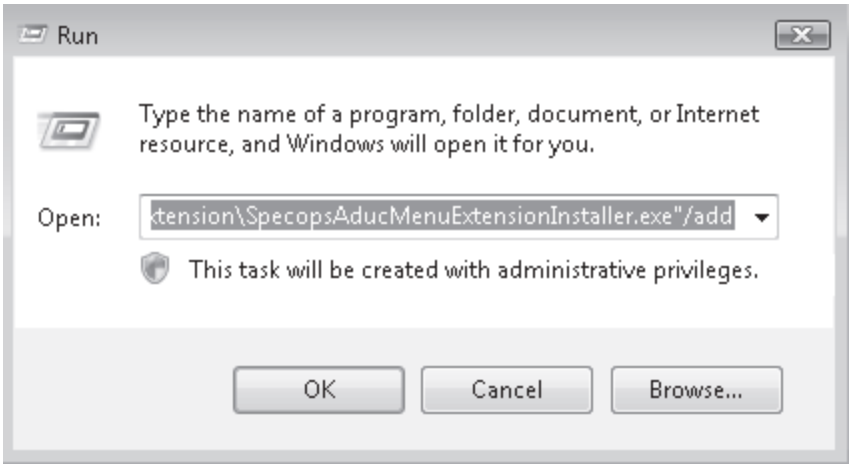
۱۰. دکمه نصب را کلیک می‌کنیم تا برنامه نصب شود و بعد روی Finish کلیک می‌کنیم. نصب تمام شده است ولی باید display specifier ها را به forest اضافه کنیم. این کار نیازمند اعتبار Enterprise Admins می‌باشد.

۱۱. پنجره Windows Explorer را باز کرده و به مسیر %ProgramFiles%\Common Files\Secopssoft\SpecopsADUC Extension می‌رویم.

۱۲. وقتی فایل‌های Specops در پنل جزئیات Windows Explorer ظاهر شد به منوی استارت رفته و روی Run کلیک می‌کنیم. کادر محاوره‌ای Run نمایش داده می‌شود.

۱۳. عبارت SpecopsAducMenuExtensionInstaller.exe را از پنجره Windows Explorer به کادر Run می‌کشیم.

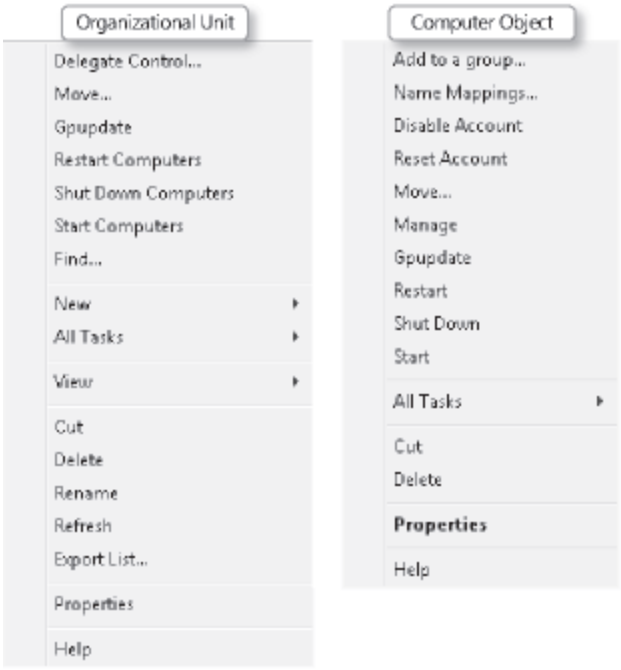
۱۴. به انتهای متن رفته و سوئیچ /add را تایپ می‌کنیم.



۱۵. کلید Enter را می‌زنیم.

۱۶. کلیدی را می‌زنیم تا پنجره بسته شود.

حالا که display specifier ها اضافه شدند می‌توانیم به راحتی فایل SpecopsGpupdate.msi را روی کامپیوتر اجرا کنیم. وقتی نیاز داریم با اشیاء کامپیوتر کار کنیم به راحتی می‌توانیم روی شیء کامپیوتر یا OU حاوی اشیاء کامپیوتر کلیک راست کرده و به ویژگی‌های جدید دسترسی پیدا کنیم. (شکل ۲- ۱۳). این ابزار رایگان بوده و برای هر سرویس دایرکتوری مفید است.



شکل ۲- ۱۳ گزینه‌های منوی کلیک راست اضافه شده توسط Specops Gpupdate

استفاده از ابزارهای مدیریتی AD DS

به منظور انجام فعالیت‌های مرتبط با مدیریت سرویس در AD DS و DNS می‌توانیم از یک سری ابزار استفاده کنیم. قبلا با بسیاری از این ابزارها آشنا شدیم ولی مرور آنها خالی از لطف نیست. جدول ۲- ۱۳ به طور خلاصه نشان می‌دهد کدام ابزار را می‌توانیم برای کدام عملیات استفاده کنیم و کجا این ابزار را پیدا می‌کنیم. در این جدول تمرکز روی سرویس است نه مدیریت داده. بسیاری از این ابزارها به دلیل اینکه بر اساس همان کد هسته AD DS هستند می‌توانند با AD LDS کار کنند.

جدول ۲- ۱۳ ابزارهای مدیریتی سرویس‌های پرکاربرد

ابزار	شرح	محل
Active Directory	Trust ها، سطوح عملیاتی دامنه و forest و پسوندهای نام کاربر را	گروه برنامه‌های

Domain and Trusts	مدیریت می‌کند.	Administrative Tools
Active Directory Schema Snap-in	Schema را برای دایرکتوری‌های AD DS یا AD LDS تغییر می‌دهد. باید دستور Regsvr32.exe را اجرا کنیم تا اول Schmmgmt.dll رجیستر شود.	MMC سفارشی
Active Directory Sites and Services	حوزه‌های تکثیر دایرکتوری AD DS و AD LDS را پیکربندی و مدیریت می‌کند	گروه برنامه‌های Administrative Tools
Active Directory Users and Computers	نقش‌های FSMO با مرکزیت دامنه و ویژگی‌های RODC را پیکربندی و مدیریت می‌کند.	گروه برنامه‌های Administrative Tools
ADSI Edit	اشیاء و خصیصه‌های آنها را نمایش داده و ویرایش می‌کند.	گروه برنامه‌های Administrative Tools
CSVDE.exe	داده را به دایرکتوری AD DS و AD LDS منتقل می‌کند	خط فرمان
DCDiag.exe	دایرکتوری‌های AD DS یا AD LDS را ارزیابی می‌کند.	خط فرمان
Dcpromo.exe	سرویس DC را اضافه یا حذف می‌کند.	منوی استارت و Search
DFSRadmin.exe	تکثیر DFS را که هنگام اجرای forest در ویندوز سرور 2008 در حالت نصب کامل مورد استفاده قرار می‌گیرد مدیریت می‌کند	خط فرمان
DNS Manager	عملیات نگهداری سرورهای DNS را انجام می‌دهد.	گروه برنامه‌های Administrative Tools یا Server Manager
Dnscmd.exe	همه جنبه‌های سرورهای DNS را مدیریت می‌کند	خط فرمان
DSACLS.exe	ACL ها را روی اشیاء دایرکتوری کنترل می‌کند.	خط فرمان
Dsadd.exe	شیء اضافه می‌کند (کاربر، گروه و کامپیوتر)	خط فرمن
Dsmain.exe	فایل‌های پشتیبان Active Directory را Mount می‌کند تا محتویات را بازیابی کند	خط فرمان
Dsbutil.exe که به همراه AD LDS و Ad DS نصب می‌شود	انباره AD DS را نگهداری می‌کند. پورت‌های AD LDS را پیکربندی می‌کند. AD LDS را نمایش می‌دهد.	خط فرمان
Dsget.exe	خصوصیات منتخب یک شیء مشخص را نمایش می‌دهد. (کاربر - کامپیوتر)	خط فرمان
Dsmgmt.exe	پارتیشن‌های برنامه و نقش‌های operation master را مدیریت می‌کند	خط فرمان
Dsmod.exe	شیء موجود را تغییر می‌دهد.	خط فرمان
Dsmove.exe	شیء را به محل جدید منتقل می‌کند. همچنین قابلیت تغییرنام شیء را دارد.	خط فرمان
Dsquery.exe	پرس و جوی دایرکتوری را برای یک نوع شیء خاص انجام می‌دهد.	خط فرمان
Dsrm.exe	یک شیء یا اشیاء را حذف می‌کند.	خط فرمان
Event Viewer	تغییرات AD DS و AD LDS را ممیزی می‌کند.	گروه برنامه‌های Administrative Tools

Gpfixup.exe	مشکلات مرتبط با نام دامنه را از بین می‌برد. همچنین اشیاء GP را بعد از عملیات تغییر نام دامنه دوباره لینک می‌کند.	خط فرمان
Group Policy Diagnostic Best Practices Analyzer	پیکربندی GPO و خطاهای مرتبط را بررسی می‌کند	دانلود از سایت مایکروسافت
Group Policy Management Console	GPO ها را می‌سازد، پشتیبان تهیه می‌کند، مدیریت و بازیابی می‌کند.	گروه برنامه‌های Administrative Tools
Ipconfig	جزئیات پیکربندی IP را نمایش داده و تغییر می‌دهد.	خط فرمان
Ksetup.exe	یک کلاینت را برای کار با Kerberos نسخه ۵ غیرمایکروسافتی پیکربندی می‌کند.	خط فرمان
Ktpass.exe	سرویس Kerberos غیرویندوزی را به عنوان یک واحد امنیتی در AD D پیکربندی می‌کند.	خط فرمان
LDIFDE.exe	داده‌ها را به AD LDS منتقل می‌کند.	خط فرمان
Ldp.exe	عملیات LDAP را روی دایرکتوری اجرا می‌کند.	منوی استارت و Search
Movetree.exe	اشیاء را بین دامنه‌ها در یک forest منتقل می‌کند	دانلود از سایت مایکروسافت
Netdom.exe	حساب‌های کامپیوتر، دامنه‌ها و ارتباط trust را مدیریت می‌کند.	خط فرمان
Nltest.exe	وضعیت تکثیر و ارتباطات trust را پرس و جو می‌کند.	خط فرمان
Nslookup.exe	اطلاعات سرورهای نام را برای بررسی مشکلات زیرساخت DNS نمایش می‌دهد.	خط فرمان
Ntdsutil.exe که همراه AD DS نصب می‌شود.	کار نگهداری بانک اطلاعاتی را روی انباره AD DS اجرا می‌کند.	خط فرمان
Repadmin.exe	تکثیر بین DC هایی را که از FRS استفاده می‌کنند بررسی و رفع عیب می‌کند.	خط فرمان
Server Manager	دامنه‌های AD DS یا AD LDS موجود را مدیریت می‌کند	گروه برنامه‌های Administrative Tools
System Monitor	نمودارهای روند کارایی سرور را ایجاد می‌کند.	Server Manager, Diagnostics,Reliability, and Performance
Ultrasound.exe	یک ابزار گرافیکی برای رفع عیب تکثیر بین DC های استفاده کننده از FRS است. برای این کار به WMI متکی است.	دانلود از سایت مایکروسافت
W32tm.exe	کار مشاهده تنظیمات، مدیریت پیکربندی و بررسی مشکلات Windows Time را انجام می‌دهد.	خط فرمان
Windows Server Backup	دایرکتوری‌های AD DS یا AD LDS و محتویات آنها را پشتیبان‌گیری یا بازیابی می‌کند.	گروه برنامه‌های Administrative Tools

اجرای عملیات پشتیبانی آنلاین

بسیاری از فعالیت‌های لیست شده در جدول ۱- ۱۳ را انجام دادیم. جدول ۳- ۱۳ فصل‌های حاوی اطلاعات درباره هر کدام از ۱۲ فعالیت را نشان می‌دهد.

جدول ۳- ۱۳ فعالیت‌های مدیریتی AD DS

وظیفه	محل (فصل‌های کتاب)
مدیریت حساب گروه و کاربر	۲-۳-۴
مدیریت کامپیوترهای کلاینت	۵
مدیریت سرویس شبکه‌ای	۴-۷-۱۰- ۱۱
مدیریت GPO	۶-۷
مدیریت سرویس نام دامنه DNS	۹
مدیریت تکثیر و توپولوژی Active Directory	۱۰-۱۱
مدیریت پیکربندی Active Directory	۱-۲-۸-۱۰-۱۱-۱۲
مدیریت Active Directory Schema	۱۴
مدیریت اطلاعات	۲-۳-۴-۵-۱۱
مدیریت امنیت	۲-۷-۸-۱۲
مدیریت بانک اطلاعاتی	۱۳
گزارش‌گیری از Active Directory	۲-۶-۷-۸-۱۰-۱۱-۱۳

اجرای عملیات پشتیبانی آفلاین

یک تغییر عمده در AD DS نسبت به نسخه‌های قبلی تبدیل نقش DC به سرویس قابل کنترل است. در نسخه‌های قبلی ویندزو سرور، نقش DC یکپارچه بود یعنی برای متوقف کردن سرویس باید کل DC را متوقف می‌کردیم. مثلا وقتی می‌خواستیم عملیات پشتیبانی روی بانک Ntds.dit انجام دهیم باید DC را خاموش می‌کردیم و سرور را در حالت Directory Service Repair راه‌اندازی می‌کردیم. به همین دلیل راهی برای خودکارسازی عملیات نگهداری بانک اطلاعاتی مورد نظر نداشتیم. برای همین مدیران شبکه تمایلی به اجرای عملیات نگهداری بانک اطلاعاتی نداشتند. و البته عدم اجرای عملیات نگهداری رویکرد مناسبی برای مدیریت سیستم نیست.

همه بانک‌ها به همین شکل کار می‌کنند. هنگامی که رکورد جدیدی اضافه می‌شود بانک فضای بیشتری را برای ذخیره اطلاعات مرتبط با آن رکورد اختصاص می‌دهد. ولی وقتی رکورد حذف شود فضای مصرفی آزاد نمی‌شود. برای آزاد کردن این فضا باید فشرده‌سازی بانک اطلاعاتی صورت گیرد. سرویس AD DS برخی از عملیات فشرده‌سازی بانک را به طور خودکار اجرا می‌کند ولی این کار باعث آزاد شدن فضای گم‌شده بانک نمی‌شود. بلکه فقط داده‌ها را در بانک طوری مرتب می‌کند که دسترسی به آنها ساده‌تر صورت گیرد. برای آزاد سازی فضای گم‌شده باید عملیات فشرده‌سازی و از بین بردن پراکندگی را در حالت آفلاین روی بانک اجرا کنیم.

ولی با وجود AD DS و ویندوز سرور 2008 ، سرویس AD DS حالا یک سرویس قابل کنترل است که همانند بقیه سرویس‌های ویندوز سرور متوقف و اجرا می‌شود. این یعنی برای اجرای عملیات نگهداری بانک اطلاعاتی دیگر نیازی به خاموش کردن DC نیست و به دلیل اینکه مانند سرویس اصلی ویندوز عمل می‌کند عملیات نگهداری را می‌توان از طریق اسکریپت و ابزارهای خط فرمان انجام داد. توجه داشته باشیدکه برای متوقف کردن سرویس AD DS، DC باید با یک DC دیگر ارتباط برقرار کند. وگرنه نمی‌توانیم سرویس را متوقف کنیم. AD DS دارای مکانیزم‌های خودکار کنترلی است که تضمین می‌کند در آن واحد حداقل یک DC در دسترس است وگرنه هیچ کسی نمی‌تواند به شبکه وارد شود.

حدود حفاظت از دایرکتوری به صورت خودکار

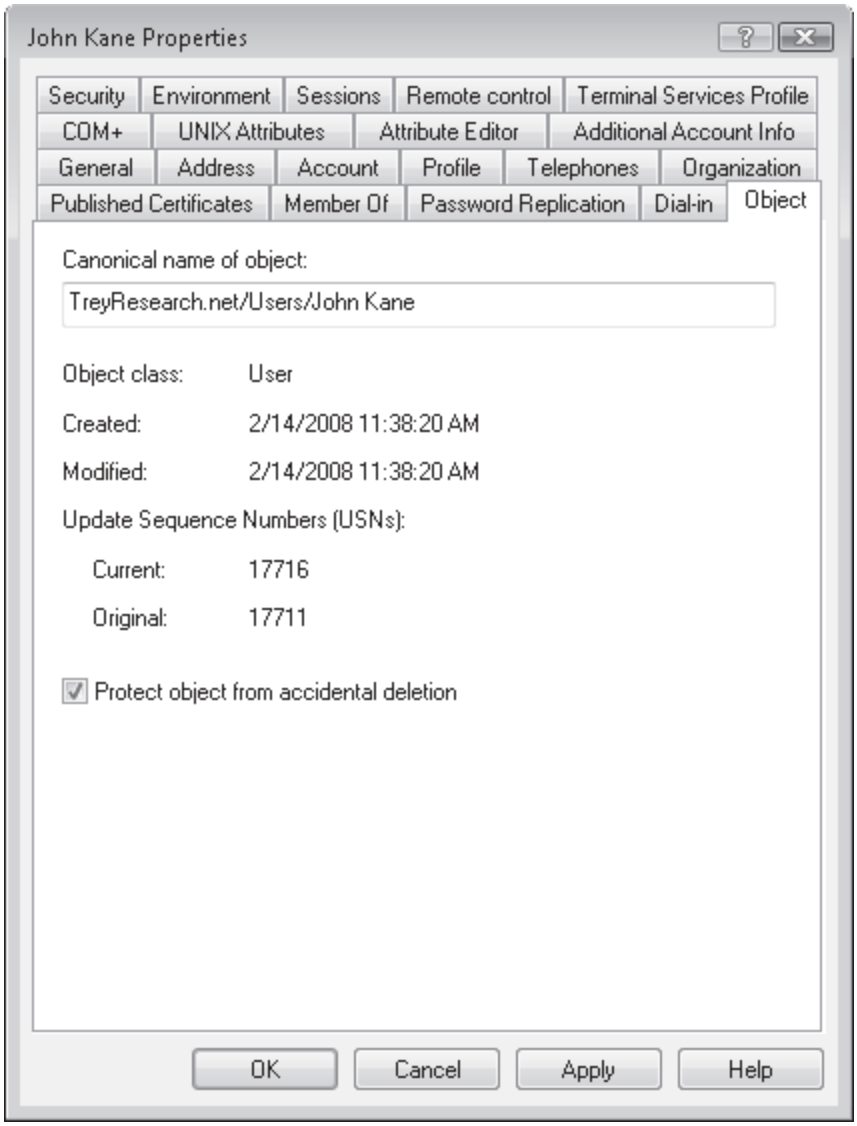
حفاظت از داده نیز یکی از مهم‌ترین جنبه‌های مدیریت پیش‌گیرانه سیستم‌ها می‌باشد و برای AD DS نیز ضروری است. همان‌طور که می‌دانید همه حساب‌های ذخیره شده در بانک AD DS منحصر به فرد هستند و به یک SID واحد و مشخص گره خورده‌اند. یعنی وقتی حسابی حذف شود ساخت دوباره آن به سادگی امکان‌پذیر نیست. اگرچه می‌توان حساب را صوری ایجاد کرد ولی این حساب جدید کاملا با شیء قبلی متفاوت خواهد بود و نمی‌تواند خصیصه‌ها و مشخصات شیء قبلی را احیاء کند. عضویت گروه، کلمه عبور، تنظیمات خصیصه و بسیاری دیگر با شیء قبلی تفاوت خواهند داشت. این دلیل خوبی برای انتساب دوباره حساب به جای ساخت دوباره آن است.

انتساب دوباره یک حساب به طور خودکار همان حقوق مالک قبلی را به کاربر جدید اعطاء می‌کند. ساخت دوباره یک حساب نیازمند انجام همه تنظیمات روی حساب جدید است که بار کاری بسیاری ایجاد می‌کند.
از دست دادن داده در دایرکتوری بسیار سخت است به این دلیل که در مدل تکثیر multimaster زمانی که تغییری در یک محل ایجاد می‌شود به طور خودکار به محل‌های دیگر سرایت می‌یابد. ولی این مدل دارای مشکلاتی نیز می‌باشد. وقتی یک شیء حذف می‌شود مخصوصا به صورت سهوی از کل دایرکتوری حذف می‌شود و در این حالت ممکن است مجبور شویم آنرا از طریق فایل پشتیبان بازیابی کنیم. AD DS دارای چهار ویژگی است که مارا قادر می‌سازد اطلاعات را بدون توسل به نسخه پشتیبان بازیابی کنیم:

- گزینه new object protection که اشیاء را از حذف شدن محافظت می‌کند.
- ویژگی جدید ممیزی AD DS Access که مقادیر جدید و قدیمی را ثبت می‌کند و باعث می‌شود بتوانیم پس از تغییر خصوصیات شیء آنرا به حالت قبلی برگردانیم.
- Conatainer موقت (tombstone). شیئی که از دایرکتوری حذف می‌شود برای مدتی در این محل ذخیره می‌گردد. پس از مقضی شدن این زمان شیء به طور کل حذف خواهد شد.
- ویژگی تهیه نسخه پشتیبان و بازیابی توسط Windows Server Backup

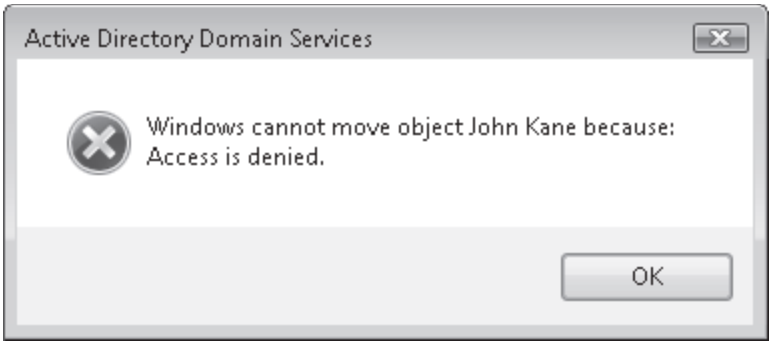
محافظت از اشیاء AD DS

به طور پیش‌فرض همه اشیاء AD DS هنگام ایجاد نسبت به حذف محافظت می‌شوند. وقتی اشیاء به صورت گروهی ایجاد یا منتقل می‌شوند این ویژگی برای آنان غیرفعال است مگر اینکه در فرایند ساخت آنرا فعال کنیم. هنگام ایجاد یک شیء به صورت interactive نیز باید این کار به صورت دستی انجام شود. محافظت از شیء در زبانه Object فعال یا غیرفعال می‌شود که فقط زمانی قابل مشاهده است که گزینه Advanced Features از منوی View در کنسول Active Directory Users And Computers فعال باشد (شکل ۳- ۱۳). توجه داشته باشید که در container هایی نظیر OU ها به طور پیش‌فرض این گزینه فعال است به دلیل اینکه بخشی از ساختار دایرکتوری می‌باشند.



شکل ۳- ۱۳ محافظت از شیء AD DS در برابر حذف شدن

پس از فعال کردن محافظت از شیء امکان حذف آن از بین می رود. حتی امکان انتقال آن نیز وجود نخواهد داشت.



در حقیقت این گزینه دو مجوز عدم دسترسی (deny) به گروه Everyone اعطاء می‌کند. یکی Deny Delete و دیگری Deny Delete subtree . تنها راه حذف یا انتقال شیء مذکور برداشتن علامت protection می‌باشد. این ویژگی برای سازمان‌هایی که مدیریت اشیاء را به گروه فنی واگذار می‌کنند خیلی مفید است.

ممیزی تغییرات دایرکتوری

وقتی تغییرات دایرکتوری در ویندوز سرور 2008 ممیزی می‌شود با تغییر یک شیء مقادیر جدید و قدیمی شیء تغییر یافته ثبت می‌شود. به دلیل اینکه سیاست ممیزی AD DS در ویندوز سرور 2008 چهار زیرگروه دسترسی را ثبت می‌کند می‌توانیم انتساب این سیاست را در سطوح ریزتری نسبت به نسخه‌های قدیمی ویندوز سرور انجام دهیم. یکی از زیرگروهها Directory Service

Changes می‌باشد و اگر فعال باشد عملیات ساخت، تغییر، انتقال و بازیابی را روی شیء انجام می‌دهد. هر عملیات دارای یک ID اختصاصی در Directory Services Event Log می‌باشد.

این ویژگی باعث ثبت Enent Log در یک سیستم نگهداری رکورد می‌شود. این کار ما را قادر می‌سازد رکوردهای زیادی را نگهداری کنیم. همچنین برای اصلاح تغییراتی که به خطا منجرشده مفید است.

وقتی شیئی تغییر می‌کند حداقل دو واقعه در رابطه با آن تغییر ثبت می‌شود. اول اینکه مقدار قبلی و دوم مقدار جدید ثبت می‌شود که برای اصلاح تغییر نامطلوب هر دو را نیاز داریم.

بازیابی (Undeleting) اشیاء

وقتی شیئی اشتباها حذف می‌شود می‌توانیم از دستور Ldp.exe برای بازیابی آن استفاده کنیم. برای این کار از مراحل زیر استفاده می‌کنیم. البته اعتبار مدیریتی مورد نیاز است.

۱. در خط فرمان تایپ می‌کنیم Ldp.exe

۲. از منوی Connection روی Connect کلیک می‌کنیم. نام FQDN سرور را تایپ می‌کنیم. مثلا Server10.TreyResearch.net

۳. از منوی Connection روی Bind کلیک می‌کنیم. گزینه Bind As Currently Logged On User باید انتخاب شده باشد. سپس روی OK کلیک می‌کنیم.

۴. از منوی Options روی Controls کلیک کرده از لیست بازشوی Load Predefined گزینه Return Deleted Objects را انتخاب می‌کنیم. در بخش Control Type از کادر محاوره‌ای گزینه Server باید انتخاب شده باشد. روی OK کلیک می‌کنیم.

۵. از منوی View روی گزینه Tree کلیک کرده و نام DN مربوط به container شیء حذف شده را تایپ کرده و OK می‌کنیم. مثلا container DN در TreyResearch خواهد بود cn=deleted objects, dc=TreyResearch,dc=net

۶. در پنل چپ روی container اشیاء حذف شده دوبار کلیک می‌کنیم تا گره باز شود. دستور Ldp.exe فقط ۱۰۰۰ شیء را به طور پیش‌فرض برمی‌گرداند.

۷. شیئی را که می‌خواهیم بازیابی کنیم پیدا کرده و روی آن دوبار کلیک می‌کنیم. این کار باعث می‌شود اطلاعات آن ظاهر شود. برای مثال اگر شیء کاربر باشد اطلاعات آن با cn=username شروع می‌شود.

۸. روی نام شیء کلیک راست کرده و Modify را انتخاب می‌کنیم.

۹. در کادر محاوره‌ای Modify عبارت isDeleted را در Edit Entry Attribute تایپ کرده و Delete as the Operation را انتخاب کرده وکلید Enter را می‌زنیم.

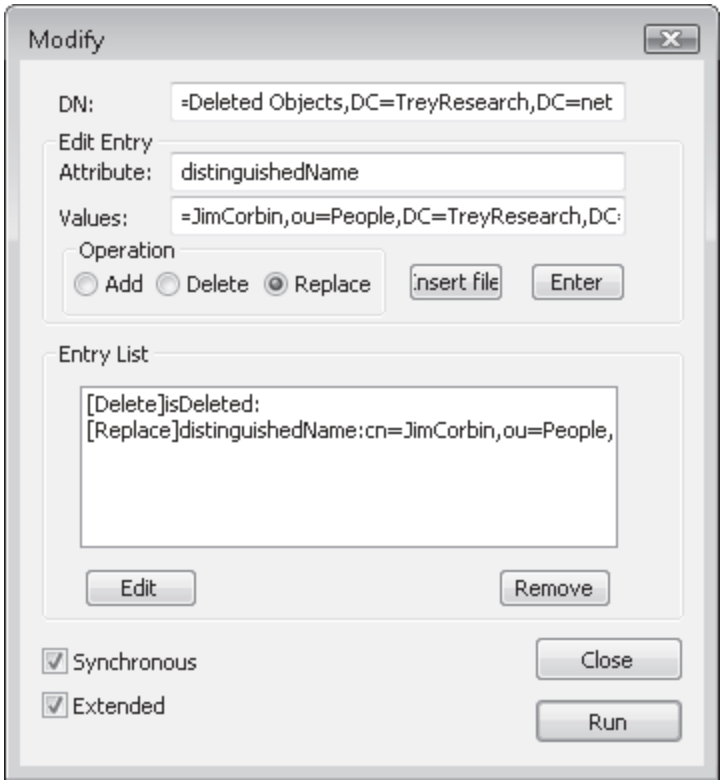
۱۰. در همین کادر در Edit Entry Attribute عبارت distinguishedName را تایپ کرده و DN جدید شیء را در Attribute تایپ کرده و Replace as the Operation را انتخاب می‌کنیم. سپس کلید Enter را می‌زنیم. مثلا برای بازیابی حساب کاربری John Kane در People container در دامنه TreyResearch ، DN را به صورت زیر وارد می‌کنیم: cn=John Kane,ou=People,dc=TreyResearch,dc=net .

۱۱. کادرهای Synchoronous و Extended در پایین سمت چپ کادر محاوره‌ای باید علامت داشته باشند. روی Run کلیک می‌کنیم. (شکل ۴- ۱۳)

۱۲. برای بررسی نتیجه عملیات به کنسول Active Directory Users And Computers مراجعه می‌کنیم.

۱۳. کلمه عبور، عضویت گروه و مقادیر دیگر مورد نیاز شیء تازه بازیابی‌شده را ریست می‌کنیم و روی Enable کلیک می‌کنیم.

حالا شیء بازیابی شده است. این فرایند SID اصلی شیء را برمی‌گرداند ولی همه عضویت گروهها را نمی‌تواند برگرداند.



شکل ۴- ۱۳ بازیابی شیء حذف شده با Ldp.exe

استفاده از نرم‌افزار Quest Object Restore برای بازیابی اشیاء دایرکتوری

همانطور که دیدیم اشیاء پس از حذف در مکانی موقت و مخفی نگهداری می‌شوند. دستیابی به این محل با ابزارهای خاصی مانند Quest Object Restore از شرکت Quest Software امکان‌پذیر است. این ابزار کنسولی را در اختیار ما قرار می‌دهد که در آن می‌توانیم شیء مورد نظر را بیابیم و بازیابی کنیم. این نرم افزار رایگان است ولی هر ۶ ماه یکبار باید پاک شده و دوباره نصب شود. این نرم‌افزار به عنوان نمونه معرفی شده و به منظور توصیه استفاده از آن نیست.

روش دانلود و نصب آن به شرح زیر است.

۱. RSAT مخصوصا ابزارهای مدیریتی AD DS باید روی سیستم نصب شده باشد.

۲. از وب‌سایت شرکت Quest Software نرم افزار را دانلود کرده و در پوشه Documents ذخیره می‌کنیم.

۳. آنرا از حالت فشرده خارج می‌کنیم.

۴. بعد فایل Quest Object Restore For Active Directory.msi را پیدا کرده و روی آن دوبار کلیک می‌کنیم.

۵. در کادر محاوره‌ای روی Run کلیک می‌کنیم.

۶. در صفحه Welcome روی Next کلیک می‌کنیم.

۷. مجوز استفاده را قبول کرده و Next می‌زنیم.

۸. نام کامل و سازمان را وارد کرده و کادر Anyone Who Uses This Computer را علامت می‌زنیم.

۹. محل پیش‌فرض نصب را قبول کرده و Next می‌زنیم.

۱۰. دوباره Next و بعد Finish را کلیک می‌کنیم. حالا نصب کامل شده است.

۱۱. برای استفاده ابتدا نرم‌افزار را اجرا می‌کنیم. نرم افزار دارای MMC مخصوص به خود است.

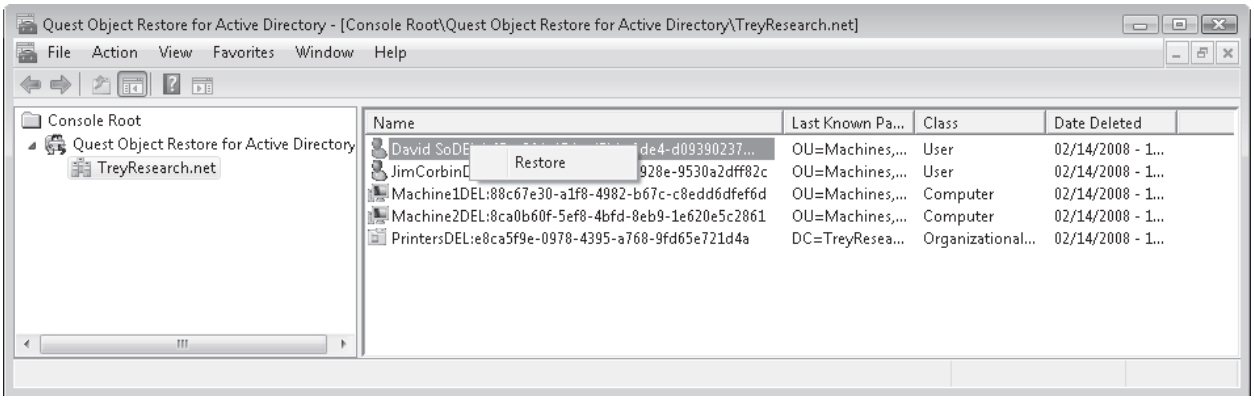
۱۲. روی Quest Object Restore For Active Directory کلیک راست کرده و Connect To را انتخاب می‌کنیم.

۱۳. نام FQDN دامنه را تایپ کرده OK را می‌زنیم.

۱۴. در پنل نام دامنه را کلیک می‌کنیم. لیست اشیاء حذف شده نمایش داده خواهد شد.

۱۵. اگر اشیاء ظاهر نشد روی Refresh کلیک می‌کنیم.

۱۶. روی نام شیء کلیک راست کرده و Restore را انتخاب می‌کنیم. (شکل ۵- ۱۳) پس از اتمام کار روی OK کلیک می‌کنیم.



شکل ۵- ۱۳ نمایی از نرم‌افزار شرکت Quest

اساسا این نرم‌افزار محل موقت ذخیره اشیاء حذف شده را در AD DS نمایان می‌کند. به دلیل اینکه مدت ذخیره در این محل ۱۸۰ روز است قبل از انقضاء این تاریخ بازیابی باید صورت گیرد. استفاده از این نرم‌افزار از دستور Ldp.exe ساده‌تر است.

استفاده از Windows Server Backup برای محافظت از دایرکتوری

اگرچه ابزارها به ما کمک می‌کنند تا به داده‌های حذف شده دسترسی داشته باشیم همیشه بهترین روش بازیابی داده نیستند. به عنوان مثال اشیایی که از مکان موقت بازیابی می‌شوند حاوی همه خصیصه‌های قبلی خود نیستند. به همین دلیل باید بدانیم چه خصیصه‌هایی را پس از بازیابی شیء باید به صورت دستی مقداردهی کنیم. ولی در بازیابی با فایل پشتیبان نیازی به این مراحل نیست چون تمامی خصیصه‌های شیء به حالت قبلی برمی‌گردد. این کار باعث کاهش زمان عملیات پس از بازیابی بوده ولی مراحل بازیابی را پیچیده‌تر می‌کند.

به علاوه بازیابی اشیاء در AD DS در نسخه‌های قبلی ویندوز سرور کم‌وبیش تصادفی بوده زیرا رویت اشیاء در داده پشتیبان تا قبل از بازیابی امکان‌پذیر نبود. همچنین بازیابی فایل‌های پشتیبان روی DC های دیگر غیرممکن بود. ویندوز سرور 2008 حاوی ابزاری با نام

AD DS Database mounting است که با آن می‌توانیم محتوای داده‌های پشتیبان را قبل از بازیابی مشاهده کرد. این ابزار هنگام به ما کمک می‌کند از صحت شیء بازیابی شونده مطمئن شویم.

وقتی با عملیات پشتیبان‌گیری و بازیابی Active Directory کار می‌کنیم می‌توانیم:

- از کل سرور به همراه سیستم عامل پشتیبان تهیه کنیم
- فقط از داده System State ، داده پیکربندی سرور یا انباره دایرکتوری Ntds.dit پشتیبان تهیه کنیم.
- داده را به صورت nonauthoritative بازیابی کنیم. یعنی داده بازیابی شده هنگام بازگشت DC به شبکه توسط تکثیر multimaster به روز شود.
- داده را به صورت authoritative بازیابی کنیم. یعنی داده بازیابی شده هنگام بازگشت DC به شبکه همه DC ها را از طریق تکثیر multimaster به روز کند.
- از روش Install From Media (IFM) استفاده کنیم. در این روش از فایل Ntds.dit مربوط به DC دیگر استفاده می‌شود تا میزان تکثیر کاهش یابد.

راههای زیادی برای کارکردن با داده‌ههای پشتیبان وجود دارد. ولی اگر با DC های نسخه‌های قبلی ویندوز آشنا باشید متوجه می‌شوید ویندوز سرور 2008 دارای عملیات متعدد متفاوتی می‌باشد.

- عمل پشتیبان‌گیری با Windows Server Backup یا فرمان Wbadmin.exe در خط فرمان اجرا می‌شود. هر دو از ویژگی‌های ویندوز سرور 2008 بوده و به طور پیش‌فرض نصب نیستند و باید به سرور افزوده شوند.
- داده‌های پشتیبان مجزا نیستند و حاوی پارتیشن‌های حیاتی سرور هستند. این پارتیشن‌ها روی DC عبارتند از:
  - پارتیشن سیستم
  - پارتیشن بوت
  - پارتیشن میزبان SYSVOL
  - پارتیشن میزبان بانک اطلاعاتی AD DS .
  - پارتیشن میزبان گزارشات وقایع AD DS .
- تهیه پشتیبان همانند نسخه‌های قبلی ویندوز هم به صورت دستی و هم به صورت خودکار انجام می‌شود.
- تهیه پشتیبان روی نوارگردان و پارتیشن‌های پویا انجام نمی‌شود در حالی که روی درایوهای شبکه، هارد درایوهای قابل حمل از نوع basic و CD یا DVD انجام می‌شود.
- امکان تهیه پشتیبان از فایل‌های خاص وجود ندارد بلکه از کل پارتیشن پشتیبان تهیه می‌شود.
- اگر بخواهیم فقط داده system state را محافظت کنیم از دستور Ntdsutil.exe استفاده می‌کنیم. برای این کار از سوئیچ جدید IFM در این دستور استفاده می‌کنیم. اگر نصب برای یک RODC باشد این ابزار به طور خودکار اطلاعات محرمانه AD DS را خالی می‌کند.

- گروه Backup operators نمی‌توانند پشتیبان گیری را زمان‌بندی کنند. این کار فقط از اعضاء گروه Administrators محلی ویندوز سرور 2008 برمی‌آید. در بیشتر موارد این یعنی عضویت در گروه Domain Admins روی DC .

- وقتی سرور از شبکه خارج است باید از نسخه محلی Windows Recovery Environment (WinRE) برای بازیابی سیستم استفاده کنیم که هم به صورت محلی نصب می‌شود و هم از روی DVD نصب ویندوز سرور 2008 قابل نصب است.

این قابلیت‌های جدید نحوه کار با DC ها را در ویندوز سرور 2008 تغییر می‌دهد. اگر بخواهیم DC ها را طوری پیکربندی کنیم که کار بازیابی ساده‌تر شود به توصیه‌های زیر عمل می‌کنیم:

- DC ها را به عنوان یک سرور تک‌منظوره پیکربندی می‌کنیم و هیچ نقش دیگری را جز سرور DNS به آن اختصاص نمی‌دهیم. بهتر است DC ها روی ماشین‌های مجازی تحت Windows Server 2008 Hyper-V اجرا شوند. DC ها بهترین گزینه برای Hyper-V می‌باشند زیرا بیش از همه به کارایی و قابلیت پردازش نیاز دارند تا بتوانند ورود کاربران را مدیریت کنند. حتی اگر دامنه ما دارای هزاران کاربر باشد و مصرف پردازشگر آن در محدوده‌های زمانی خاص مانند ابتدای صبح و بعد از نهار بسیار بالا باشد باز هم توصیه می‌شود از مجازی سازی با اختصاص منابع بیشتر به آن استفاده شود.

- هیچ داده دیگری روی DC ذخیره نکنیم اگرچه از پارتیشن مجزایی برای ذخیره بانک DC استفاده شود و اگر بانک اطلاعاتی AD DS حاوی تعداد زیادی از اشیاء بود به صورت واقعه ثبت شود.

- DVD نصب ویندوز را در یک فایل ISO ذخیره کنیم و در دسترس میزبان Hyper-V قرار می‌دهیم به طوری که هر زمان که به بازیابی DC نیاز داشتیم به آسانی به آن دسترسی پیدا کنیم. راه دیگر این است که روی همه DC ها WinRE را نصب کنیم. برای این کار نیاز به Windows Automated Installation Kit (WAIK) داریم.

- پشتیبان گیری از DC را به صورت خودکار و مستمر اجرا کنیم. این پشتیبان می‌تواند روی یک پارتیشن basic اختصاصی یا یک درایو نگاشت شبکه‌ای (mapped network drive) ذخیره شود.

- کلمه عبور Directory Services Restore Mode را با دقت نگهداری کنیم. این کلمه عبور برای بازیابی داده DC استفاده می‌شود و بسیار بااهمیت است.

کار با System State تنها

روی سرور دارای نقش AD DS داده system state شامل داده‌های زیر است:

- رجیستری
- COM+ Class Registration database
- فایل‌های بوت
- فایل‌های سیستم که تحت محافظت Windows Resource Protection هستند
- بانک اطلاعاتی AD DS
- دایرکتوری SYSVOL

وقتی نقش‌های دیگری روی سیستم نصب می‌شود system state شامل چهار شیء اول لیست شده در بالا به علاوه فایل‌های زیر خواهد بود:

- برای نقش AD CS بانک اطلاعاتی AD CS اضافه می‌شود
- برای ویژگی Failover Cluster اطلاعات سرویس کلاستر اضافه می‌شود
- برای نقش وب سرور فایل‌های پیکربندی IIS اضافه می‌شود.

اطلاعات system state خیلی اهمیت دارد. پشتیبان گیری ویندوز سرور دارای سه حالت می‌باشد:

- بازیابی کامل سرور
- بازیابی system state تنها
- بازیابی فایل یا پوشه خاص

در هر حالت می‌توان اطلاعات مورد نیاز را بازیابی کرد. به خاطر داشته باشید که فایل پشتیبان ساخته شده در هر بار پشتیبان گیری حجیم‌تر شده به دلیل اینکه اطلاعات جدید به اطلاعات قبلی افزوده می‌شود. هر بار که فایل پشتیبان ایجاد می‌شود یک فایل catalog نیز ساخته می‌شود. این فایل در پیدا کردن پشتیبان‌ها به ما کمک می‌کند.

ساخت مجموعه داده Installation From Media

در شبکه‌های بزرگ با چند DC ممکن است ترجیح دهیم از هارد قابل حمل برای ایجاد محتوای اولیه DC استفاده کنیم تا اجازه دهیم در مراحل نصب DC عمل تکثیر دایرکتوری صورت گرفته و پهنای باند را اشغال کند. برای این کار از روش Installation From Media استفاده می‌کنیم. برای ساخت این فایل از دستور Ntdsutil.exe با زیر دستور IFM استفاده می‌شود.

Ntdsutil.exe یک مفسر فرمان بوده و می‌تواند از طریق یک خط دستور با مشخص کردن تمام گزینه‌ها اجرا شود. یا با اجرای دستور بدون سوئیچ مرحله به مرحله سئوالات دستور را پاسخ دهیم. جدول ۴- ۱۳ گزینه‌های مختلف را که در زیردستور IFM موجود هستند لیست می‌کند.

جدول ۴- ۱۳ گزینه‌های زیردستور IFM دستور Ntdsutil.exe

نوع DC	گزینه	شرح
DC قابل تغییر	Create Full *destination*	برای DC نرمال یا AD LDS در یک پوشه رسانه نصب می‌سازد
RODC	Create RODC *destination*	برای RODC در پوشه مقصد رسانه نصب امن می‌سازد
DC قابل تغییر با داده SYSVOL	Create SYSVOL Full *destination*	برای DC نرمال، یک رسانه نصب به همراه کل محتویات پوشه SYSVOL در پوشه مقصد می‌سازد.
RODC با داده SYSVOL	Create SYSVOL RODC *destination*	برای RODC ، یک رسانه نصب به همراه کل محتویات پوشه SYSVOL در پوشه مقصد می‌سازد.

Ntdsutil.exe تنها ابزار ساخت رسانه نصب است. در تمرینات درس کار با این ابزار را یاد می‌گیریم.

پشتیبان‌گیری کامل سیستم

به دو صورت انجام می‌گیرد: فوری و زمان‌بندی شده. هر دو هم از طریق رابط گرافیکی و هم خط فرمان انجام می‌شوند. ما بهتر است با رابط گرافیکی شروع کنیم. Windows Server Backup یک ویژگی است و باید نصب گردد.

پشتیبان‌گیری کامل از سیستم با Windows Server Backup

با اجرای مراحل زیر می‌توان از داده‌های AD DS پشتیبان تهیه کرد. این مراحل را هم می‌توان روی نصب کامل و هم روی Server Core اجرا کرد ولی اگر روی Server Core اجرا می‌کنیم باید از راه دور کار کنیم. به این صورت که در پنل راست گزینه Connect To Another Computer را انتخاب می‌کنیم و به سرور میزبان Server Core متصل می‌شویم.

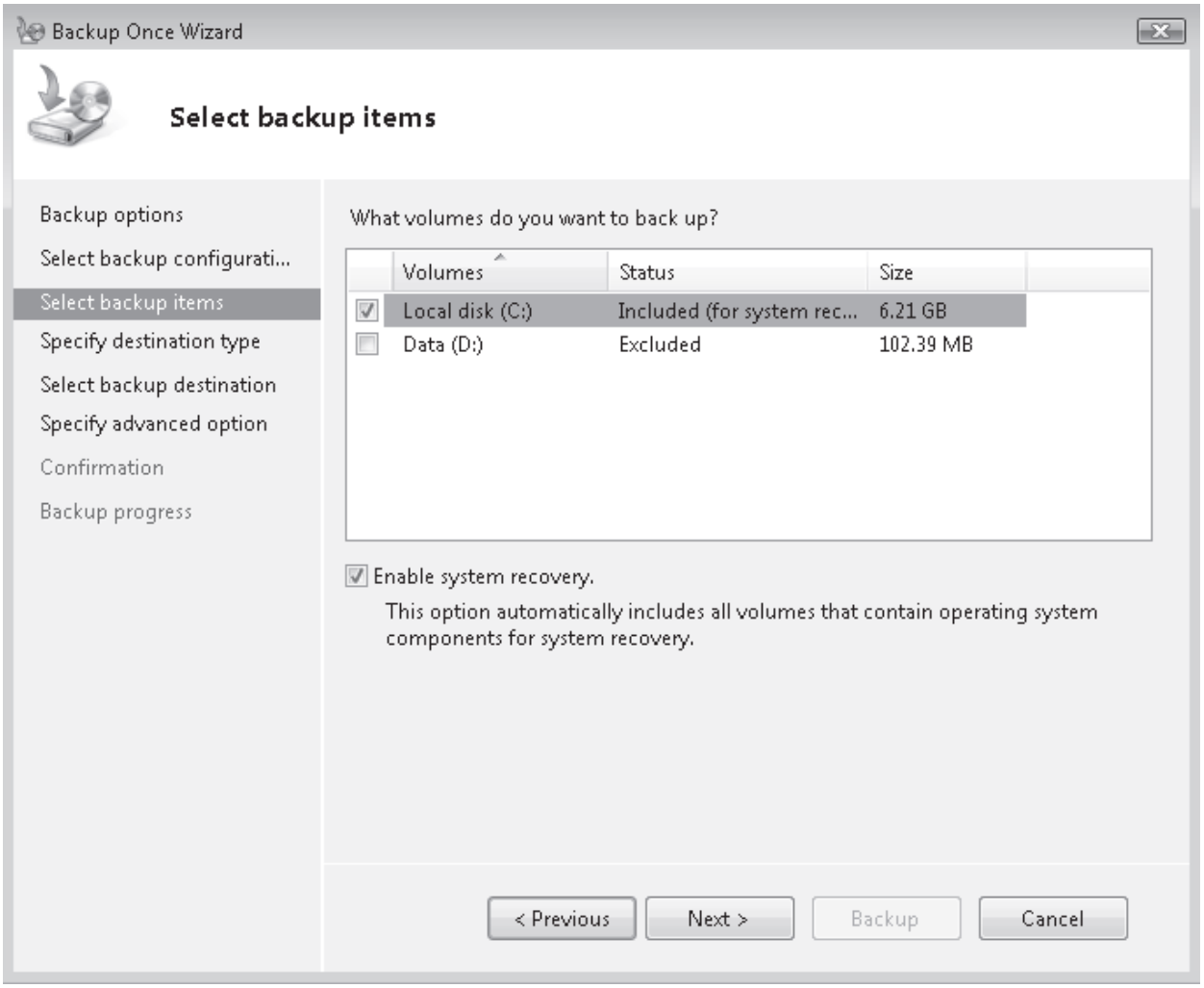
۱. با کاربر administrator دامنه به DC وارد می‌شویم و از گروه برنامه‌های Administrative Tools برنامه Windows Server Backup را اجرا می‌کنیم.

۲. اگر کادر محاوره‌ای User Account Control باز شد عملیات را تایید کرده وروی Continue کلیک می‌کنیم.

۳. روی Backup Once در پنل راست کلیک می‌کنیم. ویزارد اجرا می‌شود.

۴. اگر اولین بار است که از ویزارد Backup Once را اجرا می‌کنیم بهتر است Different Options را انتخاب کرده و Next را بزنیم. و اگر نخواهیم می‌توانیم از Same Options نیز استفاده کنیم.

۵. روی Full Server کلیک کرده و Next را می‌زنیم. توجه داشته باشید که گزینه Custom را نیز می‌توانیم انتخاب کنیم ولی نمی‌توانیم چیزی غیر از پارتیشن‌های خاص را حذف کنیم. برای مثال پوشه‌ها را نمی‌توانیم حذف کنیم. به خاطر داشته باشید که DC ها باید سرورهای تک‌منظوره باشند و بنابراین در فرایند پشتیبان‌گیری نیازی به حذف هیچ پارتیشنی نیست. ولی اگر پوشه مقصد پشتیبان دیسک محلی است باید این دیسک را از عملیات حذف کنیم. وقتی از گزینه Custom استفاده می‌کنیم گزینه‌ای به نام Enable System Recovery قابل انتخاب است که همه داده‌های مورد نیاز برای پشتیبان‌گیری کامل را جمع‌آوری می‌کند.



۶. مقصد را انتخاب می‌کنیم برای مثال درایوهای محلی و روی Next کلیک می‌کنیم.

۷. اگر درایو محلی انتخاب شود باید درایو را مشخص کنیم و از فضای کافی روی آن اطمینان حاصل کنیم.

۸. در صفحه Specify Advanced Option گزینه VSS Full Backup را انتخاب کرده و Next را کلیک می‌کنیم.

۹. روی Backup کلیک می‌کنیم تا فرایند آغاز شود.

۱۰. روی Close کلیک می‌کنیم.

نیازی نیست پنجره را باز نگه داریم چون عملیات در پس زمینه ادامه می‌یابد. ولی مشاهده پیشرفت کار می‌تواند مفید باشد.

پشتیبان‌گیری کامل سیستم با Wbadmin.exe

این روند هم روی نصب کامل و هم روی Server Core اجرا می‌شود. در نصب کامل باید از پنجره خط فرمان elevated استفاده کنیم ولی در Server Core پنجره خط فرمان همیشه elevated است. برای شروع دستور زیر را به کار می‌بریم:

```
wbadmin start backup -allcritical -backuptarget:location –quiet
```

به جای location، drive letter یا مسیر درایو مقصد را درج می‌کنیم. گزینه quiet– برای ممانعت از ظاهر شدن پیغام تایید و ورود کاراکتر Y از طرف ما استفاده می‌شود.

زمان‌بندی پشتیبان‌گیری با Windows Server Backup

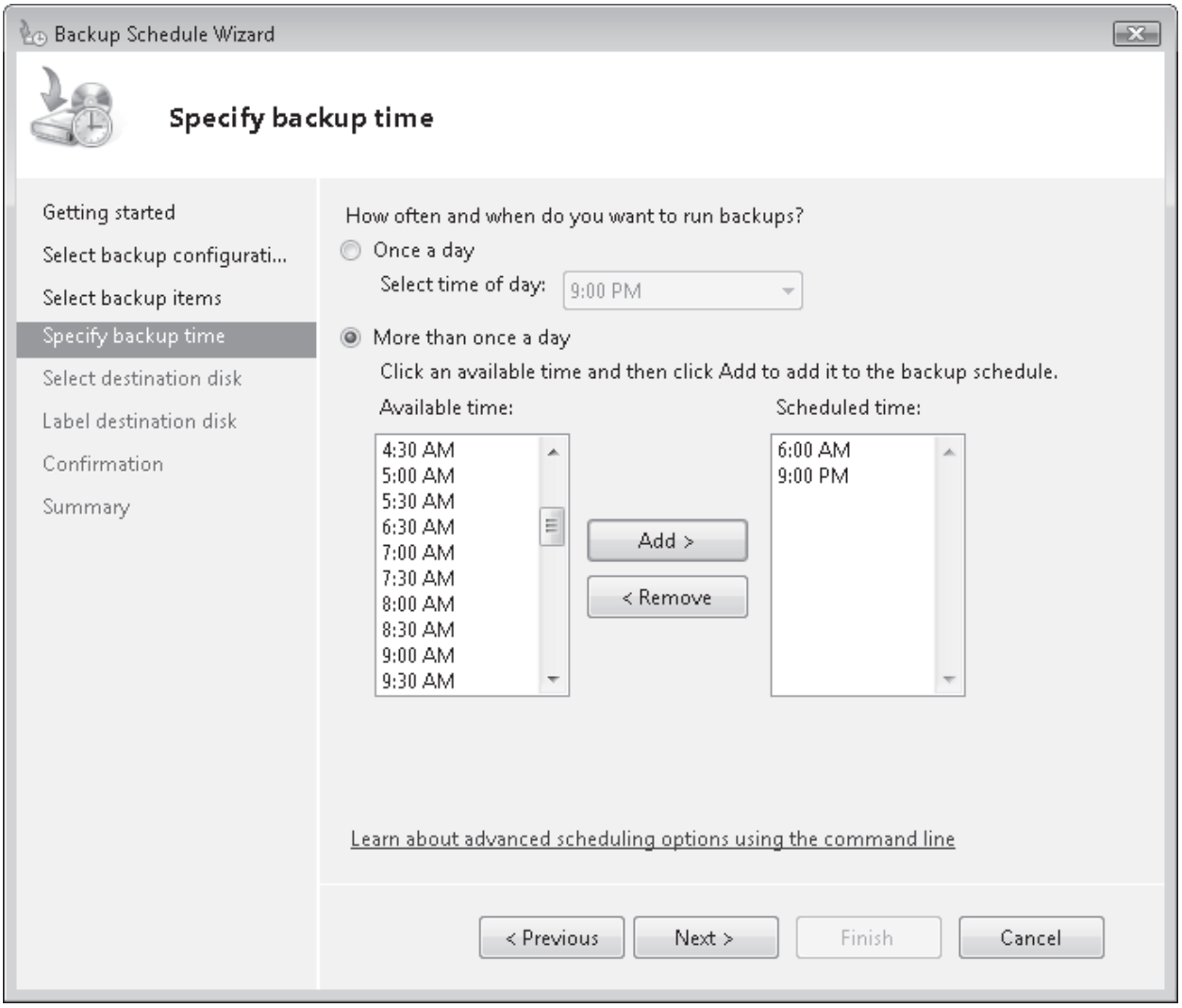
۱. با کاربر administrator دامنه به DC وارد می‌شویم و از گروه برنامه‌های Administrative Tools برنامه Windows Server Backup را اجرا می‌کنیم.

۲. اگر کادر محاوره‌ای User Account Control باز شد عملیات را تایید کرده وروی Continue کلیک می‌کنیم.

۳. روی Backup Schedule در پنل راست کلیک می‌کنیم. ویزارد اجرا می‌شود.

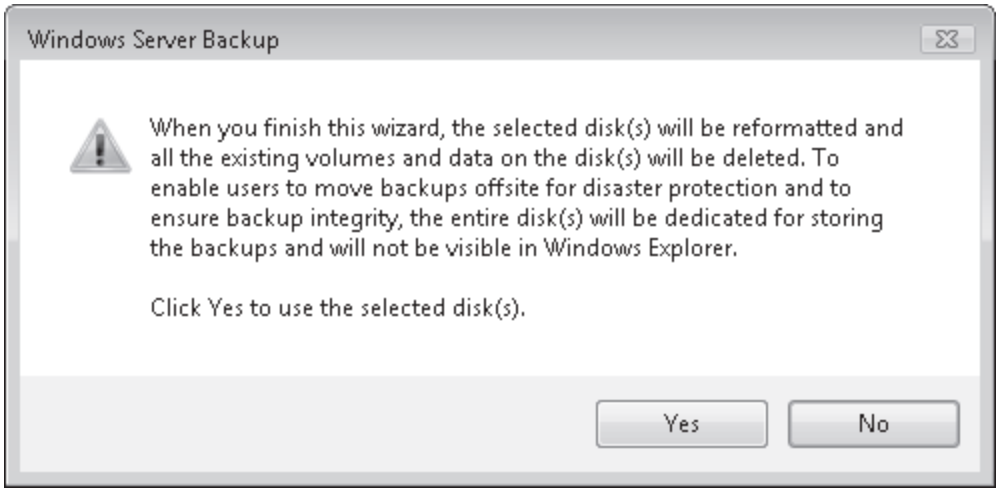
۴. روی Full Server کلیک کرده و Next را می‌زنیم. توجه داشته باشید که گزینه Custom را نیز می‌توانیم انتخاب کنیم ولی نمی‌توانیم چیزی غیر از پارتیشن‌های خاص را حذف کنیم. برای مثال پوشه‌ها را نمی‌توانیم حذف کنیم. به خاطر داشته باشید که وقتی از گزینه Custom استفاده می‌کنیم گزینه Enable System Recovery قابل انتخاب نیست.

۵. در صفحه Specify Backup Time زمان اجرا را انتخاب می‌کنیم. امکان انتخاب تعداد دفعات بیش از یک بار در روز وجود دارد.



۶. در صفحه Select Destination Disk روی Show All Available Disks کلیک کرده و یک دستگاه ذخیره سازی راه دور را انتخاب کرده و روی OK کلیک می‌کنیم. دیسک را انتخاب کرده و Next را می‌زنیم. توجه داشته باشید از درایوهای نگاشت شده شبکه‌ای در این مرحله نمی‌توان استفاده کرد.

۷. وقتی روی Next کلیک کردیم ویزارد پیغام فرمت دیسک مقصد را می‌دهد. روی Yes کلیک می‌کنیم. Windows Server Backup باید به دستگاه ذخیره‌سازی مقصد دسترسی انحصاری داشته باشد بنابراین باید هنگام پشتیبان‌گیری آنرا فرمت کند.



۸. در صفحه Label Destination Disk برچسبی برای دیسک انتخاب می‌کنیم که از دیسک‌های دیگر متمایز گردد.

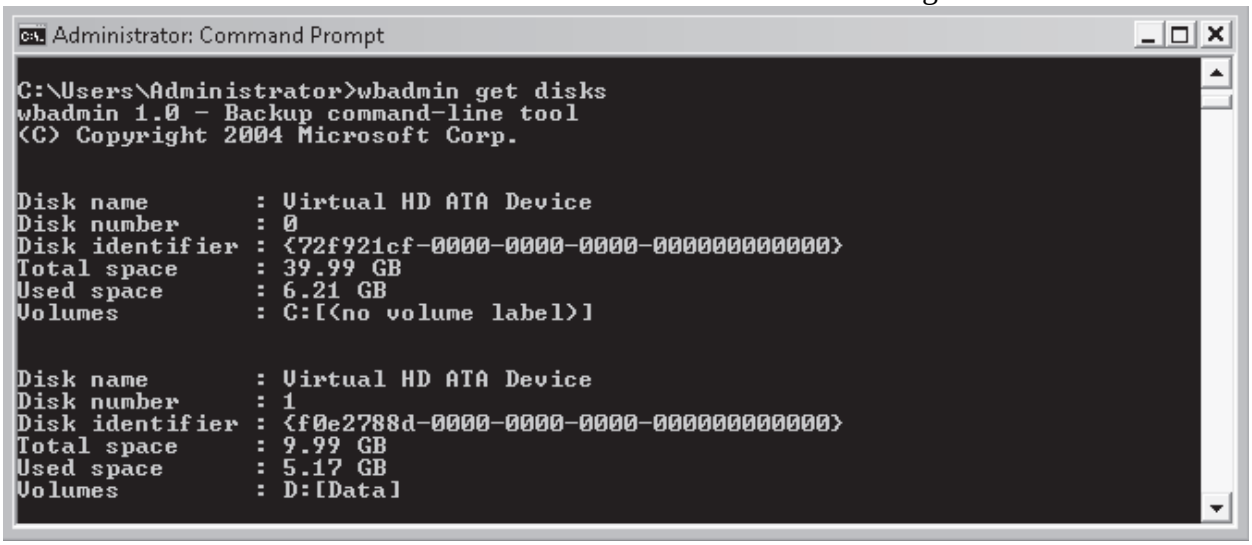
۹. گزینه‌ها را تایید کرده و روی Finish کلیک می‌کنیم.

۱۰. روی Close کلیک می‌کنیم تا زمان‌بندی تکمیل شود. دیسک مقصد فرمت شده و این وظیفه به لیست وظایف زمان‌بندی شده سیستم اضافه می‌شود.

زمان بندی پشتیبان‌گیری با Wbadmin.exe

از طریق خط فرمان نیز می‌توان پشتیبان‌گیری را انجام داد. در این مورد باید از یک پنجره خط فرمان elevated استفاده کنیم. این کار با تعیین ID دیسک مقصد شروع می‌شود:

wbadmin get disks >diskidentifers.txt



این دستور لیستی از دیسک‌های متصل شده به سیستم را در فایل Diskidentifiers.txt ذخیره می‌کند. دستور Wbadmin.exe به ID دیسک یا GUID برای پیدا کردن دیسک احتیاج دارد. برای استخراج GUID دیسک تایپ می‌کنیم:

notepad diskidentifiers.txt

ID دیسک مورد نظر را به همراه علامت [] انتخاب کرده و آنرا به clipboard کپی می‌کنیم. بعد نرم‌افزار Notepad را می‌بندیم.

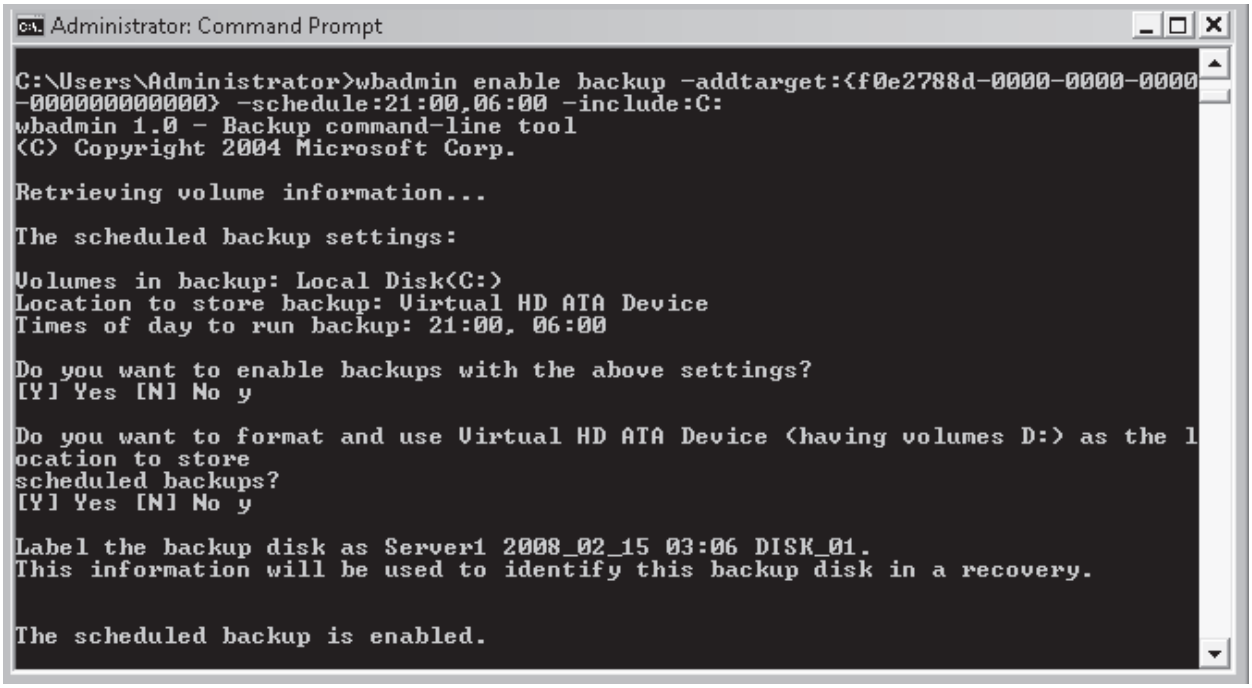
حالا آماده ساخت زمان‌بندی هستیم. دستور زیر را تایپ می‌کنیم:

wbadmin enable backup -addtarget:diskid -schedule:times -include:sourcedrives

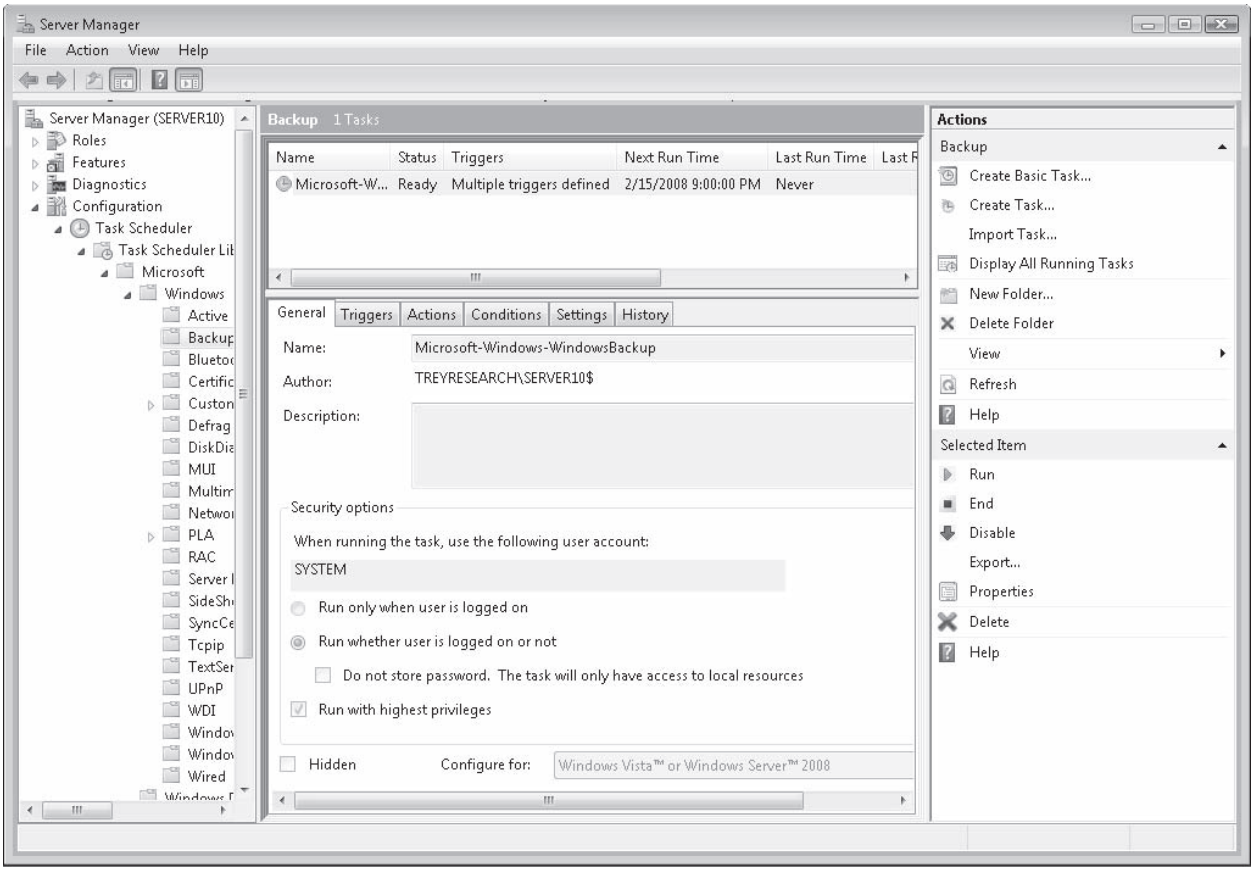
به جای diskid همان GUID را تایپ می‌کنیم. Time زمان پشتیبان‌گیری را با قالب HH:MM مشخص می‌کند. اگر بیش از یک بار مورد نظر باشد زمان‌ها را با کاما از هم جدا می‌کنیم. Sourcedrives همان drive letter درایوهای مورد نظر پشتیبان‌گیری می‌باشد. برای مثال:

wbadmin enable backup -addtarget:{f0e2788d-0000-0000-0000-000000000000} -schedule:21:00,06:00 -include:C:

دستور بالا درایو C را در ساعات ۹ عصر و ۶ صبح بر روی درایوی که GUID آن مشخص شده است برای پشتیبان‌گیری زمان‌بندی می‌کند.



نتیجه، وظیفه زمان‌بندی شده در گره Microsoft\Windows\Backup از برنامه Task Scheduler می‌باشد (شکل ۶- ۱۳)



شکل ۶- ۱۳ وظیفه زمان‌بندی شده که توسط Wbadmin.exe ایجاد شده است.

می‌توانیم این مراحل را برای ساخت یک فایل دسته‌ای مجری وظایف مورد نظر به کار بریم. ولی باید نتایج را به داخل یک فایل متنی بفرستیم در غیر این صورت وگرنه نمی‌توانیم برچسب‌های دیسک‌های قابل حمل را به دست آوریم.

توجه داشته باشید در هر بار روند پشتیبان‌گیری، درایو مقصد فرمت می‌شود. اگر نیاز به زمان‌بندی ریزتری داریم یا بخواهیم زمان‌بندی را از روزانه به هفتگی تغییر دهیم باید پس از ساخت آن توسط دستور Wbadmin.exe آنرا تغییر دهیم.

بازیابی پیش‌بینانه

مجموعه داده‌های پشتیبان به اندازه بازیابی که انجام می‌دهند اهمیت دارند. به همین دلیل تست مراحل بازیابی به منظور اطمینان از صحت عملکرد فایل‌های پشتیبان در مواجهه با اتفاقات ناخواسته ضروری است.

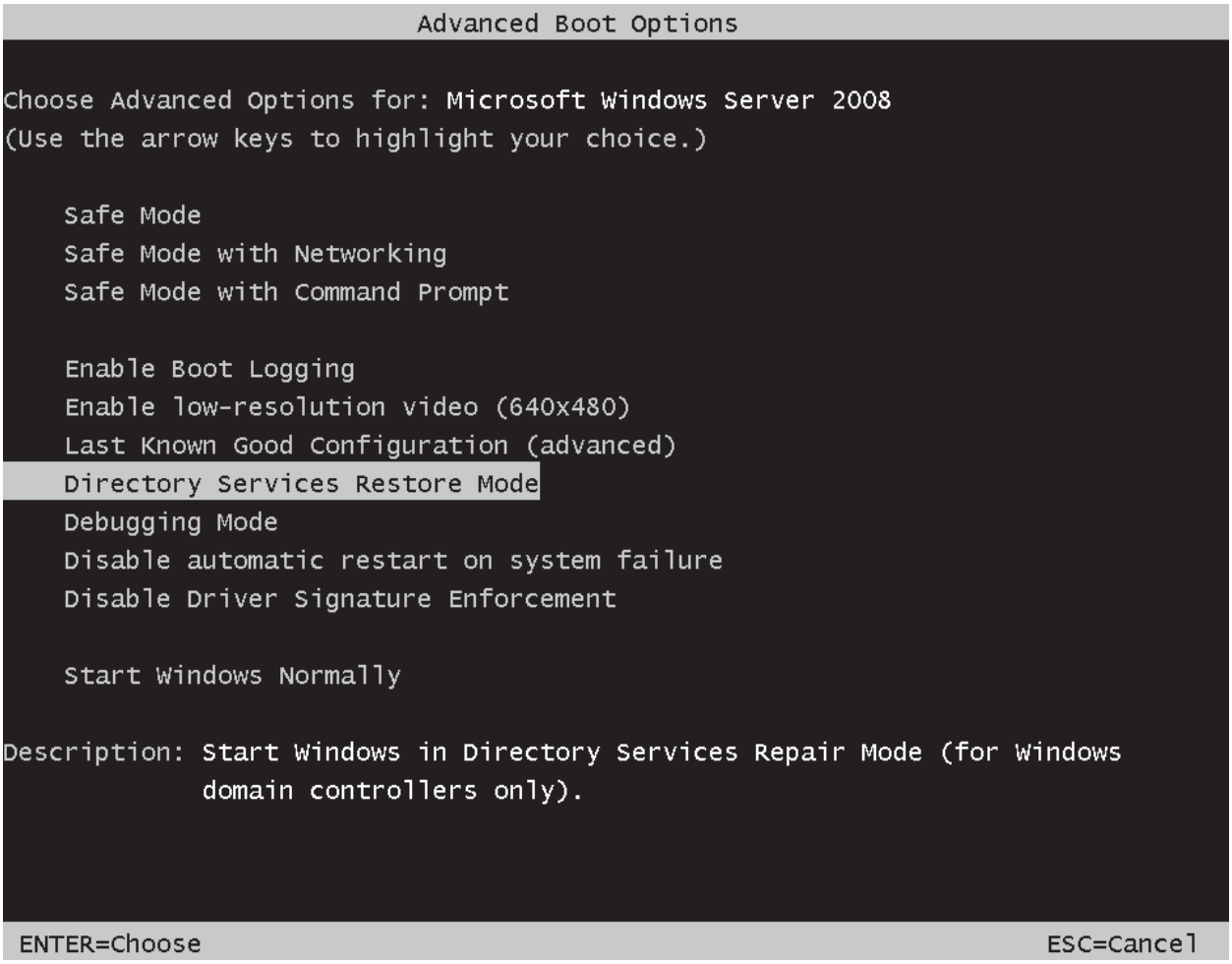
در رابطه با DC سناریوهای بازیابی متعددی وجود دارند که عبارتند از:

- بازیابی داده به صورت nonauthoritative به روی دایرکتوری برای کاهش تکثیر مورد نیاز به روز رسانی DC که مدتی از شبکه خارج بوده است.
- بازیابی داده به صورت authoritative به دلیل خرابی داده در دایرکتوری
- بازیابی کامل DC از نسخه پشتیبان

هنگام بازیابی داده روی سیستم، DC نباید در حال اجرا باشد برخلاف این واقعیت که در ویندوز سرور 2008 می‌توان سرویس AD DS را مانند بقیه سرویس‌ها کنترل کرد. در واقع باید سرور را راه‌اندازی مجدد کرده و WinRE را اجرا کنیم یا سرور را درحالت Directory Services Restor Mode (DSRM) بالا بیاوریم. مراحل اجرای هر کدام با دیگری متفاوت است. DSRM از بازیابی داده روی دایرکتوری پشتیبانی کرده و WinRE از بازیابی کل سیستم پشتیبانی می‌کند.

ورود به حالت DSRM

دو راه برای ورود به DSRM موجود است. اول راه‌اندازی مجدد سرور و فشردن کلید F8 برای ظاهر شدن منو برای انتخاب گزینه DSRM. البته برای ادامه به کلمه عبور مخصوص DSRM نیاز داریم.



همچنین می‌توانیم با تغییر ترتیب بوت در فایل مربوطه سیستم عامل سیستم را مجبور کنیم به حالت DSRM وارد شود. دستور آن Bcdedit.exe می‌باشد. برای این منظور در پنجره خط فرمان elevated دستور زیر را تایپ می‌کنیم:

bcdedit /set safeboot dsrepair

بعد از اتمام کار و نیاز به بوت نرمال این دستور را به کار می‌بریم:

bcdedit /deletevalue safeboot

اگر عملیات فقط باید یک‌بار اجرا شود بهتر است از همان کلید F8 استفاده شود.

تشخیص مجموعه داده پشتیبان مناسب

یکی از مشکلات سازمان‌های استفاده کننده از AD DS در نسخه‌های قبلی ویندوز عدم توانایی آنها در تشخیص وجود داده مورد نظر در مجموعه داده پشتیبان بود. در ویندوز سرور 2008 ابزاری برای نمایش محتویات آن قبل از بازیابی ارائه شده است.

ابزار مورد نظر با برش‌های مقطعی(snapshot) از بانک اطلاعات کار می‌کند. این برش‌ها با ابزار Ntdsutil.exe تهیه می‌شوند. برای مثال برای ایجاد برش‌های دایرکتوری به صورت منظم از دستور زیر استفاده می‌کنیم:

ntdsutil ‘activate instance NTDS’ snapshot create quit quit

این دستور یک برش روی درایو حاوی بانک اطلاعاتی می‌سازد. مراقب اجرای دستور باید باشیم به دلیل اینکه خیلی سریع دیسک میزبان بانک Ntds.dit را پر می‌کند.

برای مشاهده مجموعه داده پشتیبان یا محتویات برش مقطعی از بانک مراحل زیر را انجام می‌دهیم.

۱. پنجره خط فرمان elevated را باز می‌کنیم.

۲. با لیست برش‌های موجود شروع می‌کنیم. این برش‌ها در زمان اجرای پشتیبان یا اجرای زیردستور Ntdsutil.exe create ساخته می‌شوند. ولی برای mount کردن برش‌ها باید GUID آنرا داشته باشیم. دستور زیر برای فرستادن GUID همه برش‌ها به یک فایل متنی به کار می‌رود.

ntdsutil ‘activate instance NTDS’ snapshot ‘list all’ quit quit >snapshot.txt

۳. حالا فایل متنی را باز کرده و GUID مورد نظر را کپی می‌کنیم:

snapshot.txt notepad

۴. GUID را به همراه کاراکترهای [] به حافظه موقت سیستم کپی می‌کنیم.

۵. برش مورد نظر را mount می‌کنیم. به خاطر داشته باشید برای درج GUID کافی است روی صفحه کلیک راست کرده و Paste را انتخاب می‌کنیم.

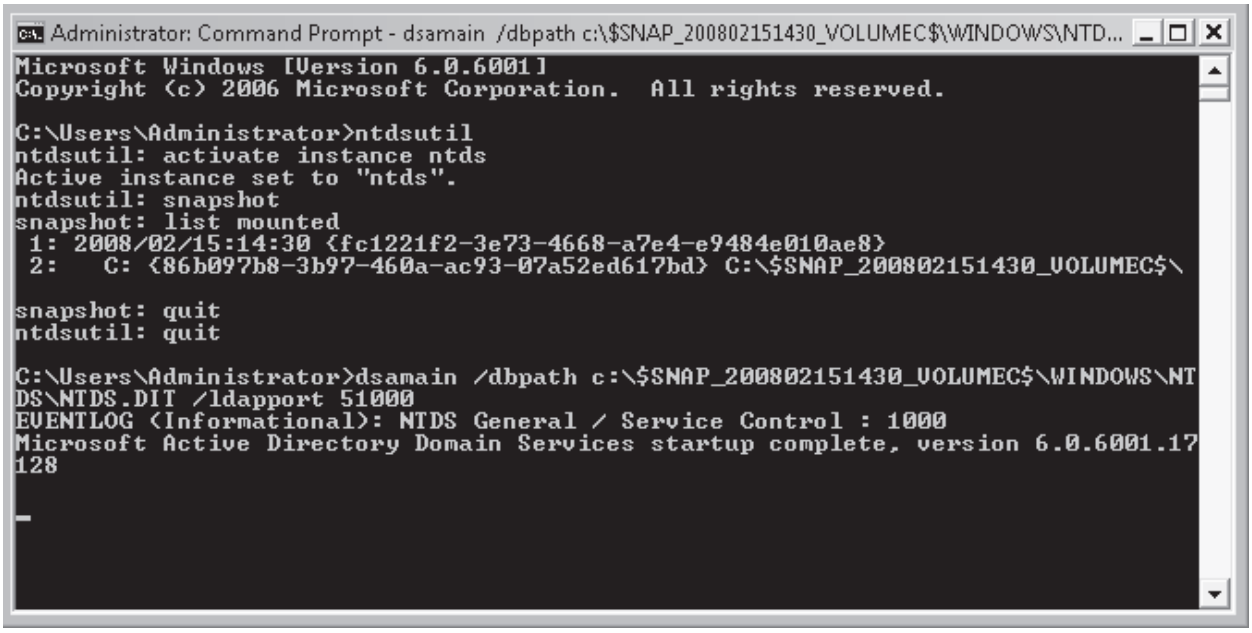
ntdsutil
activate instance NTDS
snapshot
mount guid
quit
quit

به مسیر لیست شده برای بانک mount شده دقت کنید.

۶. از ابزار mount بانک اطلاعاتی AD DS برای بارگذاری برش به عنوان سرور LDAP استفاده می‌کنیم.

dsamain -dbpath c:\$snap_datetime_volumec$\windows\ntds\ntds.dit
-ldapport portnumber

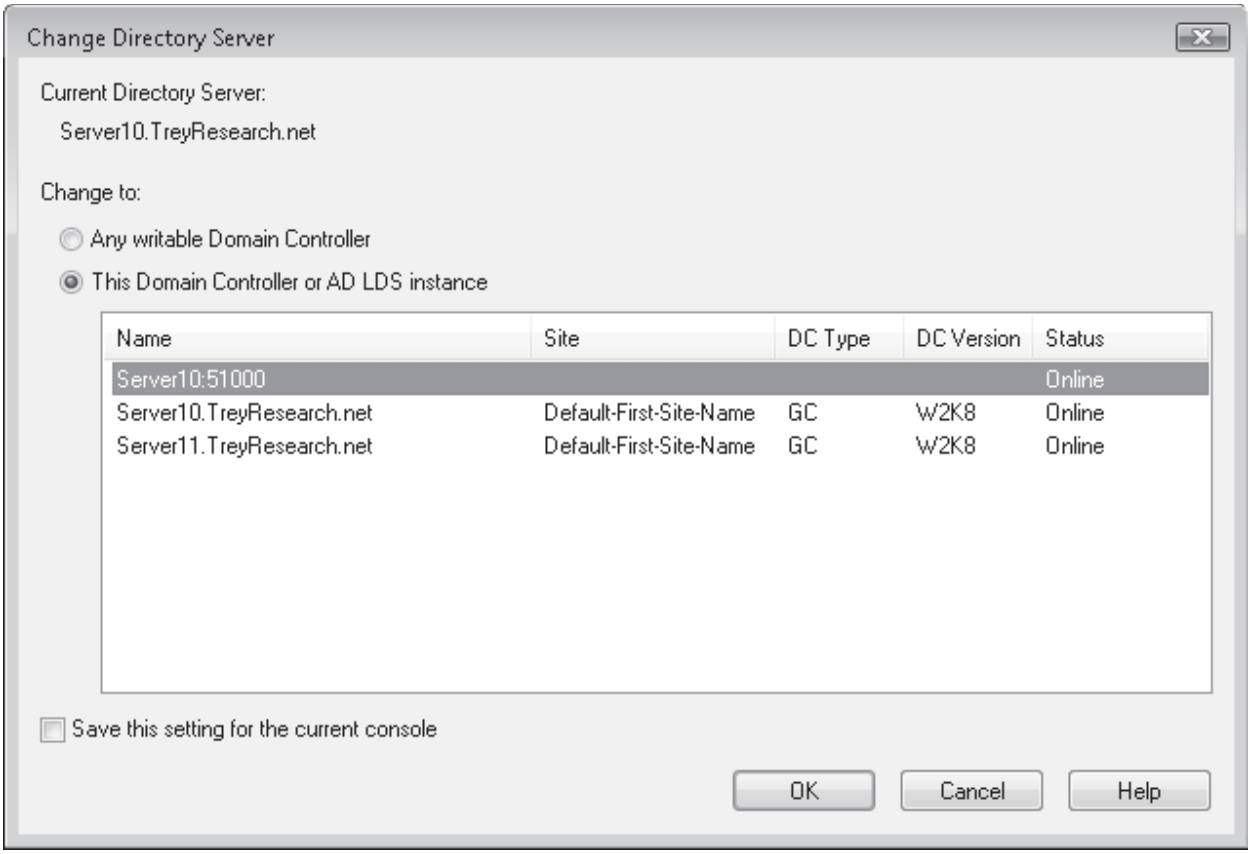
توجه داشته باشید هنگام درج مسیر به جای dbpath از حروف بزرگ استفاده کنید و شماره پورت ldapport را بالاتر از 50000 انتخاب کنید تا با AD DS تداخلی نداشته باشد. همچنین به جای علامت "-" از علامت "/" نیز می‌توانیم استفاده کنیم. بانک اطلاعاتی mount خواهد ماند تا عملیات به پایان برسد. پنجره خط فرمان را نباید ببندیم. همچنین می‌توانیم از دو پنجره خط فرمان استفاده کنیم یکی برای mount کردن برش و دیگری برای دستور Dsamin.exe . با این کار می‌توانیم برش‌های مختلفی را mount و dismount کنیم تا آنرا که حاوی اطلاعات مورد نیاز بازیابی است پیدا کنیم.



۷. حالا می‌توانیم از دستور ldp.exe یا ابزار Active Directory Users and Computers استفاده کنیم.

۸. روی Active Directory Users and Computers کلیک راست کرده و Change Domain Controller را انتخاب می‌کنیم.

۹. در کادر محاوره‌ای Change Directory Server روی <Type A Directory Server Name[:Port] Here> کلیک کرده و servername:portnumber را تایپ می‌کنیم. مثلا Server10:51000 و کلید Enter را می‌زنیم. وضعیت به online تغییر می‌کند. روی OK کلیک می‌کنیم.



۱۰. instance بازگذاری شده را برای پیدا کردن اطلاعات مورد نیاز جستجو می‌کنیم و properties آنرا مشاهده می‌کنیم. اگر همان instance مورد نظر ما باشد نام آنرا یادداشت می‌کنیم. کادر را می‌بندیم.

۱۱. به خط فرمان برمی‌گردیم و کلیدهای Ctrl+C را می‌زنیم تا دستور Dsamain.exe متوقف شود.

۱۲. برش بانک اطلاعاتی را unmount می‌کنیم. دستور زیر را اجرا می‌کنیم.

```
ntdsutil
activate instance NTDS
snapshot
unmount guid
quit
quit
```

۱۳. پنجره خط فرمان را می‌بندیم.

اگر برش بانک اطلاعاتی همانی که دنبالش هستیم نباشد مراحل را تکرار می‌کنیم. و اگر باشد ادامه می‌دهیم.

بازیابی Nonauthoritative و Authoritative

همان‌طور که قبلا اشاره شد اجرای عملیات بازیابی نیاز به ورود دایرکتوری به حالت DSRM دارد. این یعنی خاموش شدن DC. از طرف دیگر هر دو نوع بازیابی هم بر روی نصب کامل و هم Server Core قابل اجراست. روش اول زمانی به کار می‌آید که هیچ داده‌ای از بین نرفته به دلیل اینکه روی DC های دیگر موجود است. روش دوم داده‌ای را که گم شده بازیابی می‌کند و Update

Sequence Number (USN) را به روز می‌کند تا به DC های دیگر هم تکثیر شود. هر دو در ابتدا یک روند را اجرا می‌کنند. دیسک قابل‌حملی را که داده پشتیبان روی آن قرار دارد به سیستم متصل می‌کنیم.

۱. اگر نیاز باشد سرور را تعمیر کرده و بوت می‌کنیم. در حین بوت کلید F8 را می‌زنیم.

۲. گزینه Directory Services Restore Mode را انتخاب و کلید Enter را می‌زنیم.

۳. ویندوز بوت می‌شود. با کاربر و کلمه عبور مخصوص DSRM وارد می‌شویم. ما می‌توانیم داده را هم از طریق Windows Server Backup و هم از خط فرمان بازیابی کنیم. ولی وقتی می‌خواهیم داده دایرکتوری را بازیابی کنیم باید از بازیابی System State استفاده کنیم و در نتیجه از خط فرمان این کار را انجام می‌دهیم.

۴. پنجره خط فرمان elevated را باز می‌کنیم.

۵. دستور زیر را تایپ می‌کنیم:

wbadmin get versions -backuptarget:drive -machine:servername

مثلا برای مشاهده لیست فایل‌های پشتیبان موجود در درایو D روی SERVER10 تایپ می‌کنیم:

wbadmin get versions -backuptarget:d: -machine:server10

به مشخصه نسخه دقت کنید به دلیل اینکه در دستور بعدی نام دقیق آنرا نیاز داریم.

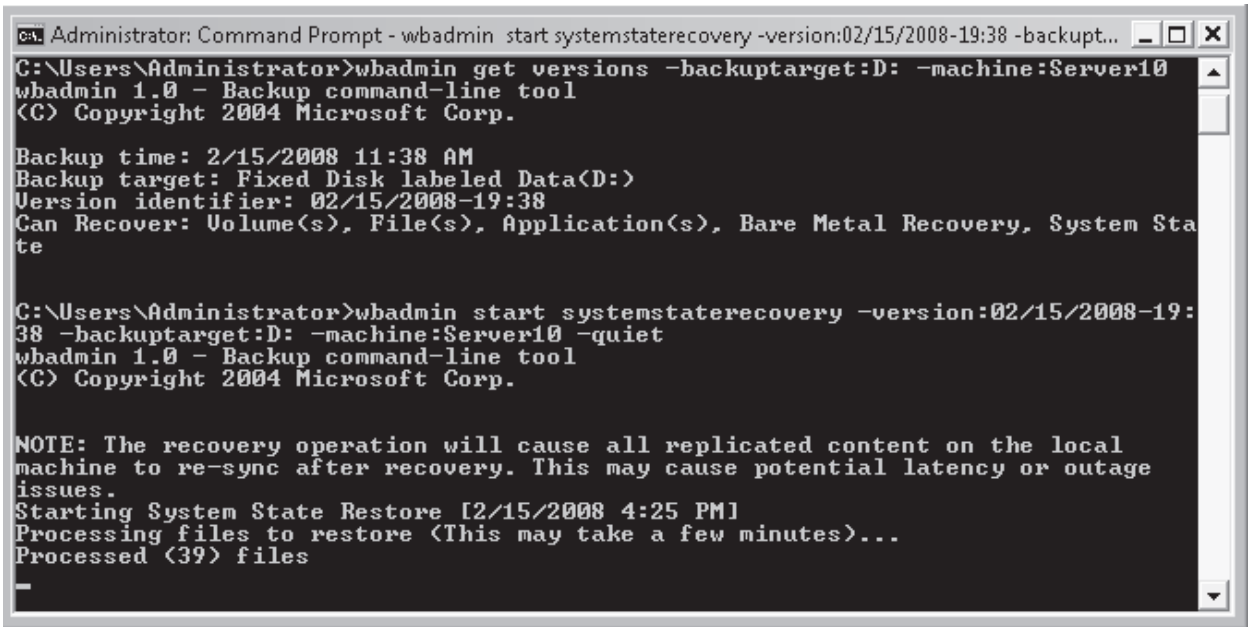
۶. برای بازیابی اطلاعات system state دستور زیر را تایپ می‌کنیم:

wbadmin start systemstaterecovery -version:datetime -backuptarget:drive -machine:servername –quiet

برای مثال برای بازیابی system state از یک پشتیبان که در تاریخ ۱۵ فوریه سال ۲۰۰۸ گرفته شده از درایو D روی SERVER10 تایپ می‌کنیم:

wbadmin start systemstaterecovery -version:02/15/2008-19:38 -backuptarget:d: -machine:server10 –quiet

از گزینه quiet– برای جلوگیری از ظاهر شدن پیغام تایید عملیات استفاده می‌شود.



۷. پنجره خط فرمان را می‌بندیم. اگر بازیابی nonauthoritative را انتخاب کرده باشیم کار تمام است.

۸. DC را به حالت نرمال راه اندازی مجدد می‌کنیم. وقتی سرور راه اندازی می‌شود AD DS به طور خودکار متوجه می‌شود از یک بازیابی برگشته و صحت بانک اطلاعاتی را چک می‌کند.

ولی اگر بازیابی authoritative انجام می‌دهیم باید داده را به عنوان authoritative علامت بزنیم. سرور را راه اندازی مجدد نمی‌کنیم و مراحل زیر را دنبال می‌کنیم.

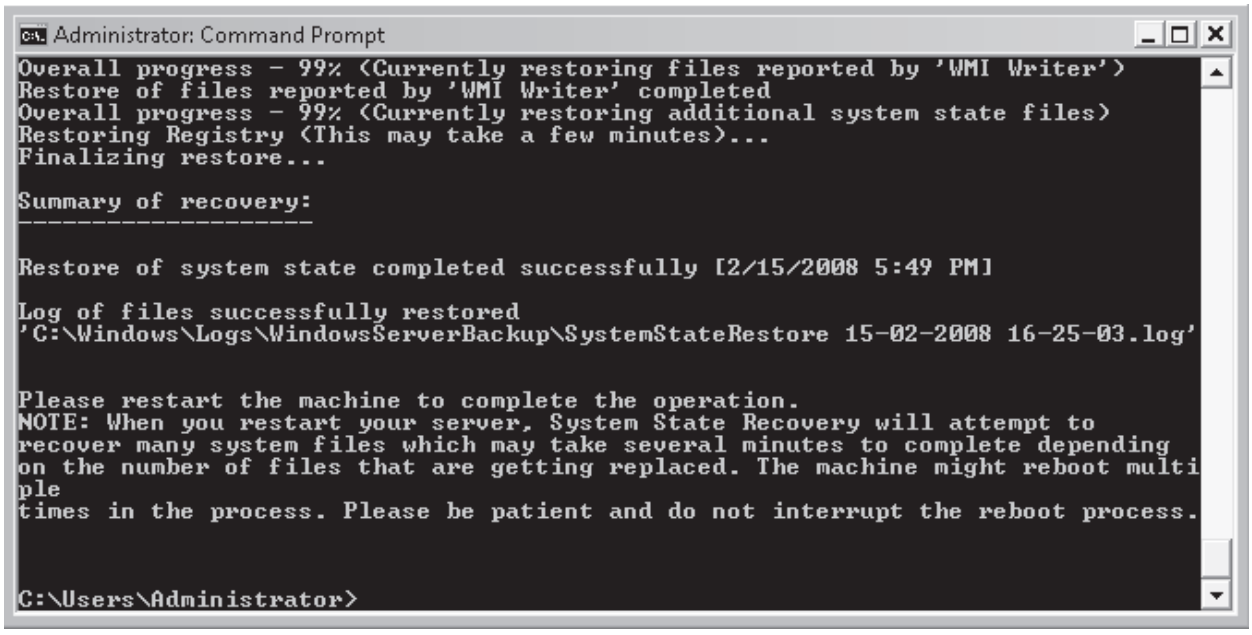
۱. دستورات زیر را تایپ می‌کنیم:

```
ntdsutil
authoritative restore
restore database
quit
quit
```

۲. سرور را در حالت نرمال راه اندازی می‌کنیم. دستور restore database همه داده‌ها را در بانک Ntds.dit همین DC به عنوان authoritative علامت می‌زند. اگر بخواهیم فقط بخشی از دایرکتوری را بازیابی کنیم از زیر دستور پایین در دستور Ntdsutil.exe استفاده می‌کنیم:

```
restore subtree ou=ouname,dc=dcname,dc=dcname
```

پس از اینکه سرور بوت شد تکثیر آغاز می‌شود و اطلاعات علامت دار به عنوان authoritative روی همه DC ها تکثیر می‌شوند. ولی ممکن است سیستم در عملیات بازیابی که فایل‌های سیستمی را به روز می‌کنند چندین بار راه اندازی مجدد شود. تکثیر AD DS پس از راه اندازی آخر باعث به روز آوری آن می‌شود چه با تکثیر از طرف این DC به DC های دیگر به دلیل بازیابی authoritative و چه برعکس آن.



بازیابی از یک نسخه پشتیبان کامل

وقتی سرور DC کاملا از کار افتاده باشد و ما نسخه پشتیبان کامل سرور را داشته باشیم می‌توانیم بازیابی کامل سیستم را انجام دهیم. اگر فایل‌های پشتیبان روی درایو قابل حمل باشند قبل از شروع بازیابی مطمئن می‌شویم به سیستم متصل است وگرنه باید سرور را راه‌اندازی مجدد کنیم. اگر فایل‌ها روی شبکه موجود باشد مسیر شبکه را یادداشت می‌کنیم. همچنین DVD نصب ویندوز ر آماده می‌کنیم.

بازیابی‌های کامل سرور هم از طریق رابط گرافیکی و هم خط فرمان امکان‌پذیر هستند.

بازیابی کامل سرور از طریق رابط گرافیکی

برای این کار مراحل زیر را دنبال می‌کنیم. (هم برای نصب کامل و هم Server Core)

۱. DVD نصب ویندوز سرور 2008 را وارد کرده و کامپیوتر را راه‌اندازی مجدد می‌کنیم وسیستم را از روی DVD بوت می‌کنیم.

۲. در صفحه ابتدایی ویندوز گزینه‌های Language ، قالب‌های Time and Currenct و Keyboard را انتخاب کرده و روی Next کلیک می‌کنیم.

۳. در پنجره Install Now روی Repair Your Computer کلیک می‌کنیم.

۴. در کادر محاوره‌ای System Recovery Options سیستم‌های عامل انتخاب شده را برای تعمیر پاک می‌کنیم.

۵. در Choose A Recovery Tool گزینه Windows Complete PC Restore را انتخاب می‌کنیم.

۶. اگر فایل‌ها روی یک سرور راه دور ذخیره شده باشند روی Cancel در پیغام هشدار کلیک می‌کنیم.

۷. Restore A Different Backup را انتخاب کرده و روی Next کلیک می‌کنیم.

۸. در صفحه Select The Location Of The Backup مراحل زیر را بسته به محل ذخیره نسخه پشتیبان به صورت محلی یا روی شبکه دنبال می‌کنیم:

a. اگر نسخه پشتیبان روی به صورت محلی ذخیره شده باشد محل آنرا انتخاب کرده و روی Next کلیک می‌کنیم.

b. اگر روی شبکه ذخیره شده باشد روی Advanced کلیک کرده و گزینه Search For A Backup On The Network را انتخاب می‌کنیم. برای تایید روی OK کلیک می‌کنیم.

c. در Network Folder مسیر شبکه‌ای فایل‌ها را تایپ کرده و OK می‌کنیم.

d. اعتبار مناسب را وارد کرده و OK می‌کنیم.

e. در صفحه Select The Location Of The Backup محل نسخه پشتیبان را انتخاب کرده و روی Next کلیک می‌کنیم.

۹. نسخه پشتیبان مورد نظر را انتخاب کرده و روی Next کلیک می‌کنیم.

۱۰. اگر بخواهیم همه داده‌های همه پارتیشن‌ها را جایگزین کنیم در صفحه Choose How To Restore The Backup گزینه Format And Repartition Disks را انتخاب می‌کنیم.

۱۱. برای جلوگیری از حذف و ساخت دوباره پارتیشن‌هایی که در بازیابی نقشی ندارند Exclude Disks را انتخاب کرده و دیسک‌های مورد نظر را انتخاب کرده و روی OK کلیک می‌کنیم.

۱۲. روی Next و بعد Finish کلیک می‌کنیم.

۱۳. I Confirm That I Want To Format The Disks And Restore The Backup را انتخاب کرده و OK می‌کنیم.

۱۴. سرور را راه‌اندازی مجدد می‌کنیم.

بازیابی کامل سرور از طریق خط فرمان

برای این کار مراحل زیر را دنبال می‌کنیم. (هم برای نصب کامل و هم Server Core)

۱. DVD نصب ویندوز سرور 2008 را وارد کرده و کامپیوتر را راه‌اندازی مجدد می‌کنیم وسیستم را از روی DVD بوت می‌کنیم.

۲. در صفحه ابتدایی ویندوز گزینه‌های Language ، قالب‌های Time and Currenct و Keyboard را انتخاب کرده و روی Next کلیک می‌کنیم.

۳. در پنجره Install Now روی Repair Your Computer کلیک می‌کنیم.

۴. در کادر محاوره‌ای System Recovery Options سیستم‌های عامل انتخاب شده را برای تعمیر پاک می‌کنیم.

۵. در Choose A Recovery Tool، Command Prompt را انتخاب می‌کنیم.

۶. دستور diskpart را صادر می‌کنیم.

۷. دستور list vol را صادر می‌کنیم. پارتیشن میزبان نسخه پشتیبان را پیدا می‌کنیم. Drive letter در WinRE لزوما با ویندوز منطبق نیست.

۸. دستور exit را تایپ کرده و کلید Enter را می‌زنیم.

۹. در کادر Sources دستور زیر را صادر می‌کنیم:

```
wbadmin get versions -backuptarget:drive -machine:servername
```

برای مثال برای لیست نسخه‌های موجود روی درایو D در SERVER10 تایپ می‌کنیم:

```
wbadmin get versions -backuptarget:D: -machine:SERVER10
```

به مشخصه نسخه دقت کنید چون در دستور بعدی به آن نیاز داریم.

۱۰. در خط فرمان دستور زیر را صادر می‌کنیم:

```
wbadmin start systemstaterecovery -version:datetime -backuptarget:drive
-machine:servername -quiet
```

برای مثال برای بازیابی system state از نسخه پشتیبان تهیه شده در تاریخ ۱۵ فوریه ۲۰۰۸ از درایو D روی SERVER10 تایپ می‌کنیم:

```
Wbadmin start sysrecovery -version:02/15/2008-19:38 -backuptarget:d:
-machine:server10 -restoreallvolumes -quiet
```

۱۱. پس از اتمام عملیات پنجره را minimize کرده و در کادر محاوره‌ای System Recovery Options روی Restart کلیک می‌کنیم. سرور راه‌اندازی شده و به صورت نرمال کار خواهد کرد.

محافظت از DC های ماشین مجازی

وقتی یک سرویس روی ماشین مجازی ارائه می‌شود در واقع چیزی جز چند فایل روی دیسک نیست. DC های میزبان سرویس AD DS و DNS گزینه مناسبی برای مجازی‌سازی هم روی Microsoft Virtual Server R2 و هم روی Hyper-V هستند. وقتی ماشین مجازی باشد محافظت، بازیابی و تغییر آن بسیار ساده‌تر است. وقتی سروری به طور کامل از کار می‌افتد کافی است به نسخه‌های قبلی ماشین مراجعه گردد. در مورد DC تکثیر multimaster به طور خودکار بقیه کار را انجام می‌دهد آن را به روز می‌کند. تا الان این قوی‌ترین سناریوی محافظت از DC ها می‌باشد.

به علاوه یک ویژگی ویندوز سرور 2008 کار محافظت از ماشین مجازی را ساده‌تر می‌کند و آن Volume Shadow Copy Service (VSS) می‌باشد. در صورت پیکربندی این سرویس به طور خودکار از محتویات دیسک در بازه‌های زمانی مشخص برش مقطعی تهیه می‌کند. اگر مشکلی در فایل‌های روی دیسک پیش بیاید به راحتی می‌توان به Previous Versions مراجعه کرد که یک زبانه در کادر محاوره‌ای properties همه فایل‌ها و پوشه‌هاست. با این کار می‌توان نسخه‌های قبلی فایل یا پوشه را به سرعت بازیابی کرد. این زبانه به طور پیش‌فرض در ویندوز سرور 2008 و ویستا فعال است.

روی یک ماشین مجازی هارد دیسک‌های مجازی هستند که بازیابی می‌شوند. در کل این کار ۵ دقیقه طول می‌کشد. هیچ روش دیگری با VSS و ماشین مجازی نمی‌تواند رقابت کند.

VSS باید روی سرورهای میزبان که ماشین‌های مجازی را نگهداری و اجرا می‌کنند فعال شود. VSS می‌تواند هم به نصب کامل و هم به Server Core افزوده شود. فعال کردن VSS روی سرور ۱۰ دقیقه طول می‌کشد ولی ما باید ساختار دیسک مناسب داشته و آماده این کار باشیم. برای مثال سیستم میزبان مجری Hyper-V باید حداقل سه دیسک داشته باشد:

- درایو C باید سیستم و بوت باشد ونیز میزبان نقش Hyper-V باشد.
- درایو D باید درایو داده باشد که میزبان ماشین‌های مجازی است. این درایو به طور نرمال به صورت منبع ذخیره‌سازی اشتراکی ذخیره می‌شود.
- درایو E باید طوری پیکربندی شود که میزبان برش‌های VSS باشد که ممکن است تعدادشان زیاد شود. هر برش VSS حجمی معادل 100MB دارد چراکه فقط اشاره‌گرها ذخیره می‌کند نه همه ساختار دیسک را. امکان ذخیره حداکثر ۵۱۲ برش در هر زمان وجود دارد. وقتی به این حد برسیم VSS به طور خودکار آخرین برش را جایگزین می‌کند. حجم این دیسک را متناسب شرایط تعیین می‌کنیم.

فعال‌سازی VSS شامل مراحل زیر است:

۱. با کاربر administrator محلی به سرور میزبان وارد می‌شویم.
۲. روی درایو D کلیک راست کرده و Properties را انتخاب می‌کنیم.
۳. زبانه Shadow Copy را باز می‌کنیم.
۴. روی دکمه Settings کلیک می‌کنیم.
۵. در کادر محاوره‌ای از لیست بازشو درایو D را انتخاب می‌کنیم. محدودیت کپی را تعیین می‌کنیم (مقدار پیش‌فرض می‌تواند مناسب باشد) و در صورت نیاز زمان‌بندی را تغییر می‌دهیم و روی OK کلیک می‌کنیم.
۶. از لیست Select Volume درایو D: را انتخاب کرده و روی Enable کلیک می‌کنیم. در کادر Enable Shadow Copies روی Yes کلیک می‌کنیم. با زمان‌بندی پیش‌فرض شروع می‌کنیم ضمن اینکه بعدا هم می‌توان آنرا تغییر داد. سرویس VSS الان فعال است.

۷. برای گرفتن اولین برش روی Create Now کلیک می‌کنیم.

۸. روی OK کلیک می‌کنیم تا کادر بسته شود.

این مراحل از طریق خط فرمان نیز قابل انجام است. اگر میزبان دارای Server Core باشد باید این عملیات را یا از راه دور انجام دهیم یا از طریق خط فرمان. روش انجام از طریق خط فرمان به صورت زیر است:

```
vssadmin add shadowstorage /for=d: /on=e: /maxsize=6000mb
vssadmin create shadow /for=d:
vssadmin list shadowstorage
vssadmin list shadows
```

اولین دستور shadow copy را با زمان‌بندی پیش‌فرض فعال می‌کند. دستور دوم اولین کپی را تهیه می‌کند. دو دستور بعدی کپی‌های موجود را لیست می‌کند.

با استفاده از دستور Schtasks.exe و یا اجرای Task Scheduler از راه دور در کنسول Computer Management می‌توانیم زمان‌بندی را تغییر دهیم.

برای دستیابی به نسخه‌های قبلی یک فایل یا پوشه پنجره Windows Explorer را باز کرده و به پوشه اشتراکی متصل شده و فایل و در صورتی که فایل پاک شده باشد پوشه آنرا پیدا می‌کنیم. روی آن کلیک راست کرده و Properties را انتخاب کرده و به زبانه Previous Versions می‌رویم و نسخه مورد نظر را انتخاب کرده و Restore را کلیک می‌کنیم. کادر محاوره‌ای Properties را می‌بندیم. همچنین می‌توانیم فایل‌ها را کپی و مقایسه کنیم.

تمرینات کار با بانک اطلاعاتی AD DS

در این تمرین با تعدادی ابزار که بانک‌های اطلاعاتی AD DS مدیریت و محافظت می‌کند کار می‌کنیم. ابتدا یک کپی از داده دایرکتوری برداشته و بعد از آن برای ساخت DC جدید استفاده می‌کنیم. این داده آفلاین برای سرعت بخشیدن به روند تکثیر به کار می‌آید. بعد با بانک اطلاعاتی AD DS کار می‌کنیم تا مراحل فشرده سازی را به طور دستی و سپس به طور خودکار انجام دهیم. در نهایت از GPMC برای محافظت از اشیاء Group Policy استفاده می‌کنیم. این تمرینات روی SERVER10 و SERVER11 انجام می‌شود که قبلا آماده کرده‌ایم.

تمرین ۱ استفاده از Ntdsutil.exe برای دریافت داده system state

۱. با کاربر مدیر دامنه به SERVER10 وارد می‌شویم.

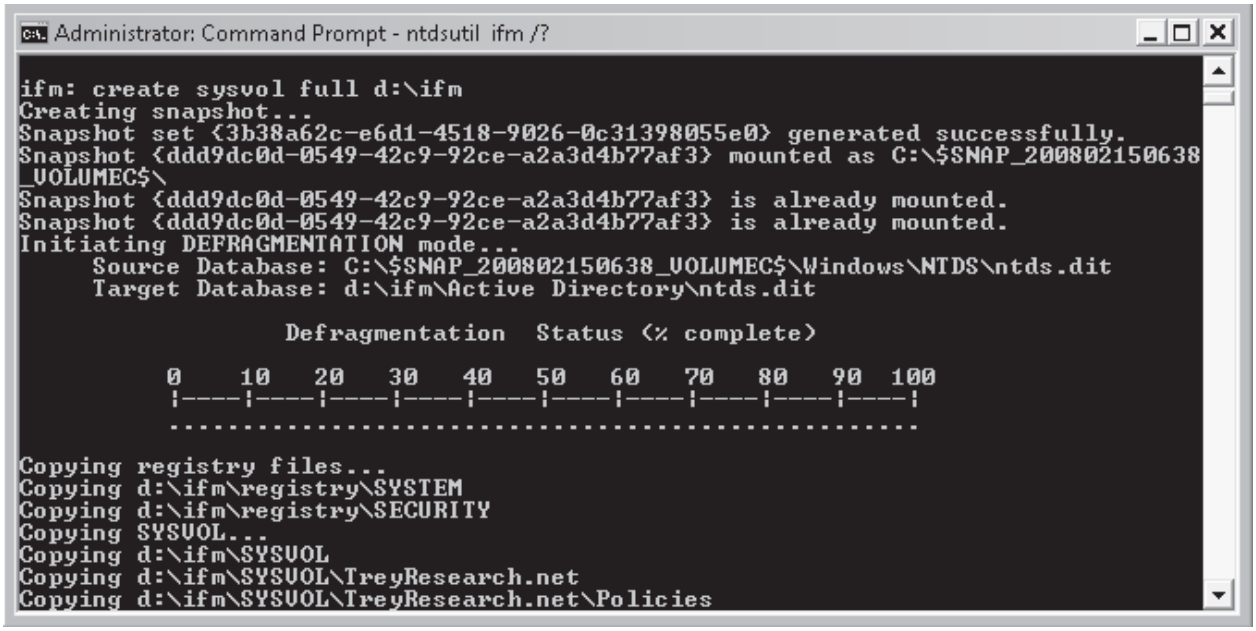
۲. بررسی می‌کنیم که این سرور حاوی درایو D بوده و یک پوشه با نام IFM روی آن می‌سازیم.

۳. پنجره خط فرمان elevated را باز می‌کنیم.

۴. دستورات زیر را تایپ می‌کنیم:

```
ntdsutil
activate instance NTDS
ifm
create sysvol full d:\ifm
```

سیستم پیغام Creating Snapshot را نمایش می‌دهد در حالی که عملیات پیش می‌رود. توجه کنید که سیستم snapshot جدید را فشرده می‌کند.



۵. دستور quit را دوبار اجرا می‌کنیم.

۶. نتایج snapshot را با استفاده از Windows Explorer مرور می‌کنیم.

۷. IFM را با کلیک راست و انتخاب Share به اشتراک می‌گذاریم.

۸. در لیست بازشو Everyone را انتخاب بعد Add و سپس نقش Contributor را در ستون Permission Level به آن اختصاص می‌دهیم.

۹. روی Share کلیک می‌کنیم.

۱۰. روی Done کلیک می‌کنیم.

داده IFM حالا آماده استفاده در DC جدید است.

تمرین ۲ ساخت DC از داده پشتیبان

۱. با کاربر مدیر محلی به SERVER11 وارد می‌شویم.

۲. Windows Explorer را اجرا کرده و یک پوشه جدید روی درایو C با نام IFM می‌سازیم.

۳. در نوار آدرس عبارت \\server10\ifm را تایپ کرده و کلید Enter را می‌زنیم.

۴. اگر کادر ورود کلمه عبور باز شد عبارت Treyresearch\Administrator یا حساب معادل آنرا تایپ کرده و کلمه عبور را وارد می‌کنیم.

۵. کل محتوا را از پوشه IFM روی SERVER10 به پوشه C:\IFM روی SERVER11 کپی می‌کنیم.

۶. مطمئن می‌شویم که همه محتویات کپی شده‌اند.

۷. نقش Active Directory Domain Services را نصب می‌کنیم. در Server Manager روی گره Roles کلیک راست کرده و Add Roles را انتخاب می‌کنیم.

۸. صفحه Before You Begin را مرور کرده و روی Next کلیک می‌کنیم.

۹. در صفحه Select Server Roles از ویزارد Add Roles ، Active Directory Domain Services را انتخاب و روی Next کلیک می‌کنیم.

۱۰. اطلاعات صفحه Active Directory Domain Services را مرور کرده وروی Next کلیک می‌کنیم.

۱۱. انتخاب‌های خود را مرور کرده و روی Install کلیک می‌کنیم.

۱۲. نتایج نصب را بررسی کرده و روی Close کلیک می‌کنیم. نصب تمام می‌شود.

۱۳. گره Active Directory Domain Services را باز می‌کنیم.

۱۴. روی Run The Active Directory Domain Services Installation Wizard در پنل وسط کلیک می‌کنیم.

۱۵. کادر Use Advanced Mode Installation را قبل از اینکه روی Next کلیک کنیم علامت می‌زنیم.

۱۶. اطلاعات صفحه Operating System Compatibility را مرور کرده و روی Next کلیک می‌کنیم.

۱۷. در صفحه Choose A Deployment Configuration گزینه Existing Forest و بعد Add A Domain Controller To An Existing Domainرا انتخاب کرده و روی Next کلیک می‌کنیم.

۱۸. در صفحه Network Credentials عبارت treyresearch.net را تایپ می‌کنیم.

۱۹. روی Set کلیک می‌کنیم. عبارت treyresearch.net\administrator یا حساب کاربری معادل آنرا تایپ کرده وکلمه عبور را وارد می‌کنیم. روی OK و بعد Next کلیک می‌کنیم.

۲۰. در صفحه Select A Domain روی treyresearch.net (دامنه ریشه forest) کلیک می‌کنیم و روی Next کلیک می‌کنیم.

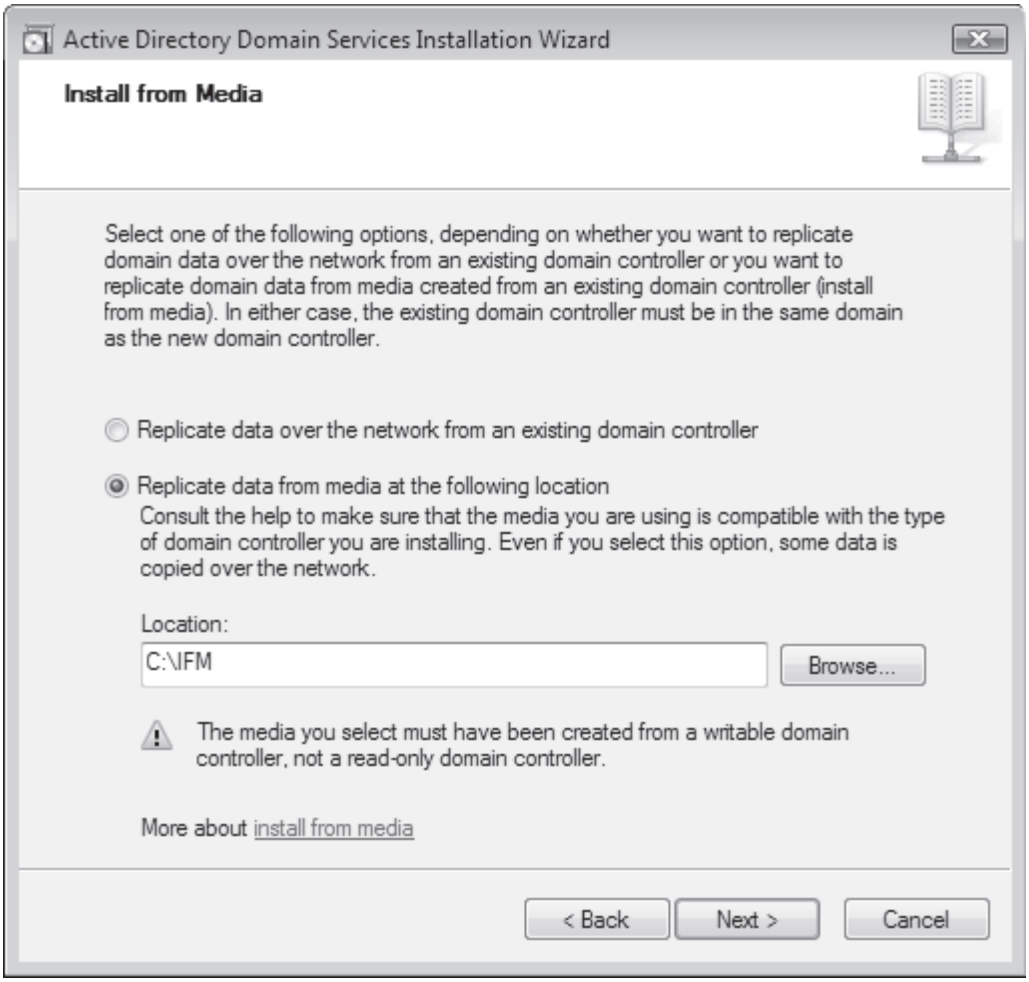
۲۱. در صفحه Select A Site مقدار پیش فرض را تایید و روی Next کلیک می‌کنیم.

۲۲. در صفحه Additional Domain Controller Options بررسی می‌کنیم تا کادرهای DNS Server و Global Catalog هر دو انتخاب شده باشند. بعد روی Next کلیک می‌کنیم.

۲۳. روی Yes, The Computer Will Use A Dynamically Assigned IP Address (Not Recommended) کلیک می‌کنیم.

۲۴. روی Yes کلیک می‌کنیم.

۲۵. در صفحه Install From Media روی Replicate Data From Media At The Following Location کلیک کرده و عبارت C:\IFM را تایپ کرده روی Next کلیک می‌کنیم.



۲۶. در صفحه Source Domain Controller مقادیر پیش فرض را قبول کرده و روی Next کلیک می‌کنیم.

۲۷. در صفحه Location For Database, Log Files And SYSVOL مقادیر پیش فرض را قبول کرده و روی Next کلیک می‌کنیم.

۲۸. کلمه عبور پیچیده وارد کرده و روی Next کلیک می‌کنیم.

۲۹. تنظیمات را تایید کرده و روی Next کلیک می‌کنیم. Reboot On Completion را انتخاب کرده و منتظر تکمیل عملیات می‌مانیم.

تمرین ۳ نگهداری بانک اطلاعاتی

در این تمرین نگهداری تعاملی بانک را انجام دهیم. این عملیات را حالا انجام می‌دهیم به دلیل اینکه دو DC در دامنه treyresearch.net داریم.

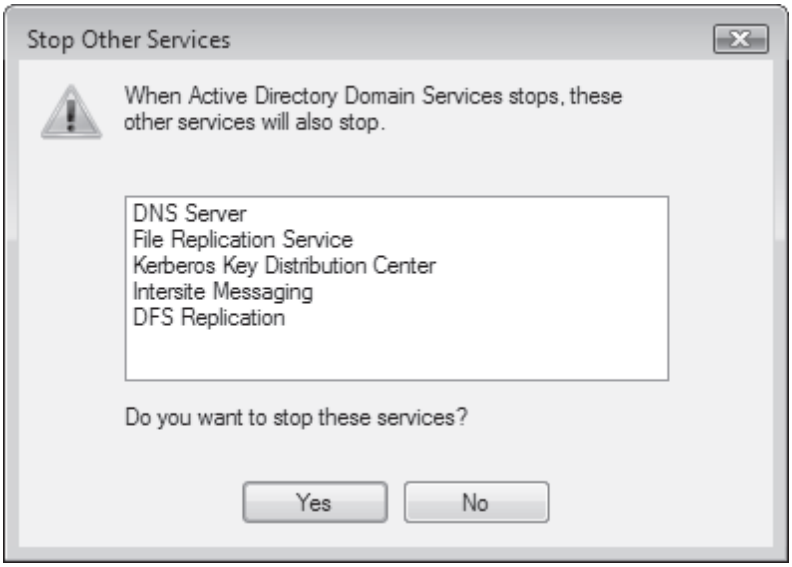
۱. با کاربر مدیر دامنه به SERVER11 وارد می‌شویم.

۲. پوشه‌هایی با نام‌های C:\Temp و C:\OriginalNTDS می‌سازیم.

۳. در Server Manager گره Configuration را باز کرده و روی Services کلیک می‌کنیم.

۴. سرویس Active Directory Domain Services را پیدا کرده و روی آن کلیک راست کرده و Stop را انتخاب می‌کنیم.

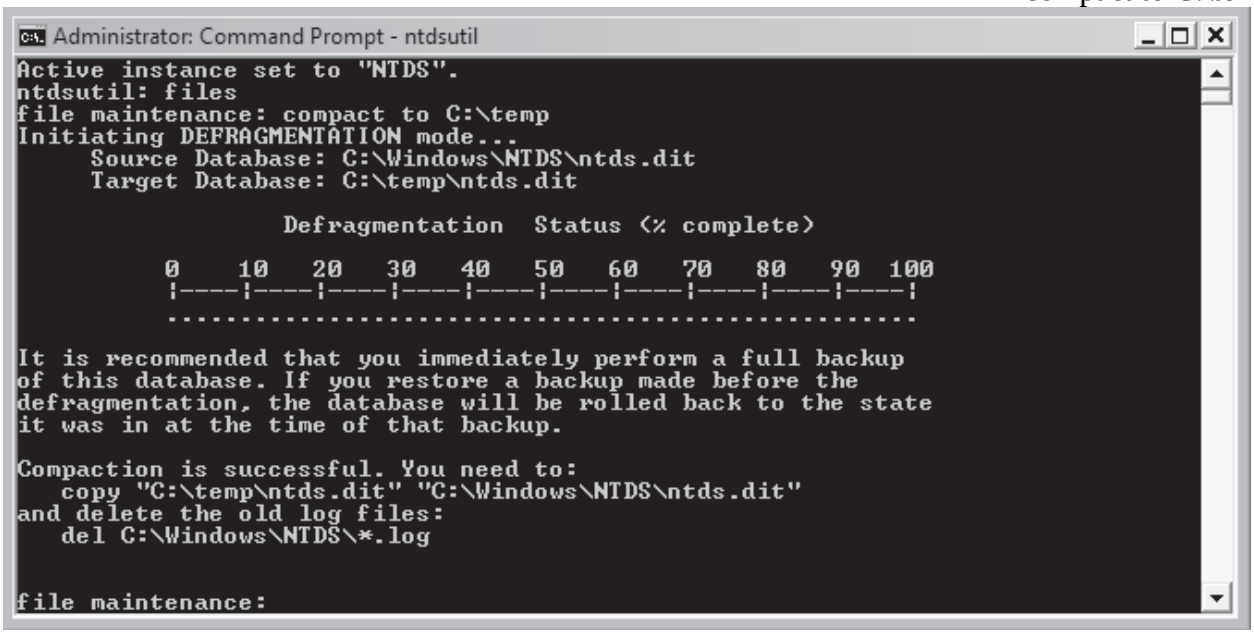
۵. در کادر محاوره‌ای Stop Other Services روی Yes کلیک می‌کنیم. سرور سرویس را متوقف می‌کند



۶. پنجره خط فرمان elevated را باز می‌کنیم.

۷. با فشرده‌سازی بانک شروع می‌کنیم. دستورات زیر را اجرا می‌کنیم:

```
ntdsutil
activate instance NTDS
files
compact to C:\temp
```



۸. پس از تکمیل عملیات فشرده‌سازی دستور quit را دو بار اجرا می‌کنیم.

۹. حالا فایل‌های log را با دستورات زیر حذف می‌کنیم:

```
cd %systemroot%\ntds
del *.log
```

۱۰. حالا از فایل Ntds.dit پشتیبان تهیه می‌کنیم. دستور زیر را اجرا می‌کنیم:

```
copy ntds.dit \originalntds
```

۱۱. بانک تازه فشرده شده را به پوشه اصلی کپی می‌کنیم. در حالی که در مسیر %SystemRoot%\NTDS هستیم دستور زیر را وارد می‌کنیم:

```
copy c:\temp\ntds.dit
Y
```

۱۲. در نهایت از صحت فایل Ntds.dit مطمئن می‌شویم. بعد با تحلیل بانک از صحت آن مطمئن می‌شویم:

```
ntdsutil
activate instance NTDS
files
integrity
quit
semantic database analysis
go fixup
quit
quit
```

۱۳. به Server Manager برمی‌گردیم و گره Configuration را باز کرده و روی Services کلیک می‌کنیم.

۱۴. سرویس Active Directory Domain Services را پیدا کرده و روی آن کلیک راست و Start را انتخاب می‌کنیم.

خلاصه درس

- برای نگهداری سرویس دایرکتوری باید از روش پیش‌گیرانه استفاده کنیم. این عملیات در ۱۲ گروه خلاصه می‌شود که بسیاری از آنها را بهتر است به دیگران واگذار کنیم. مدیران دامنه مسئول سرویس AD DS بوده و بهتر است روی عملیات اصلی دایرکتوری مانند مدیریت بانک اطلاعاتی متمرکز شوند.
- ابزارهای متعددی برای مدیریت AD DS موجود است. رایج‌ترین آنها سه کنسول اصلی Active Directory می‌باشند: Active Directory Users and Computers ، Active Directory Sites and Services و Active Directory Domains and Trusts.
- با ویندوز سرور 2008 سرویس AD DS مانند بقیه سرورها قابل مدیریت می‌باشد و بدون نیاز به راه‌اندازی مجدد و ورود به Restore Mode می‌توان متوقف و استارت کرد.

سئوالات پایان درس

۱. فرض کنید مدیری شبکه contoso.com هستیم. از ما درخواست می‌شود که بانک یکی از دو DC دامنه ریشه forest را فشرده کنیم. ولی وقتی می‌خواهیم سرویس AD DS را متوقف کنیم متوجه می‌شویم نمی‌توانیم این کار را انجام دهیم. مشکل از کجاست؟

A. ما نمی‌توانیم سرویس AD DS را روی DC ویندوز سرور 2008 متوقف کنیم.
B. مدیر دیگری روی DC دیگری در دامنه کار می‌کند.
C. باید سرور را راه‌اندازی مجدد کرده و با Restore Mode بوت کنیم.
D. باید با دستور net stop سرویس AD DS را متوقف کنیم.

۲. فرض کنید مدیر یک شبکه بزرگ هستیم. یکی از DC ها قبلا از کار ایستاده است. ما باید DC را بازیابی کنیم. پشتیبان‌های متعددی از سرور داریم که با Windows Server Backup تهیه شده‌اند. کدام یک از مراحل زیر باید اجرا شود؟ (همه گزینه‌ها می‌تواند درست باشد.)

A. سرور را با حالت Directory Services Restore Mode بوت می‌کنیم.
B. بازیابی را با دستور Ntdsutil.exe در حالت authoritative اجرا می‌کنیم.
C. ویندوز سرور 2008 را دوباره نصب می‌کنیم.

D. سرور را با WinRE راه‌اندازی مجدد می‌کنیم.

E. بازیابی را با استفاده از دستور Ntdsutil.exe به حالت nonauthoritative اجرا می‌کنیم.

F. بازیابی کامل سرور را از طریق خط فرمان اجرا می‌کنیم.

درس ۲: مدیریت پیش‌گیرانه کارایی دایرکتوری

فعالیت دوم که ما باید برای نگهداری DC انجام دهیم مدیریت کارایی است. اگر ما از روش نصب مناسب استفاده کنیم می‌توانیم مطمئن باشیم DC به درستی کار کند. به خاطر داشته باشید نقش DC الان در پنجمین ویرایش خود پس از ظهور در ویندوز NT بوده و با نسخه‌های مختلف سیستم عامل‌های سرور مایکروسافت کار می‌کند. این یعنی حالا به یک سرویس مطمئن تبدیل شده است. علیرغم این ثبات در مواردی ممکن است به مشکل برخورد کند. منشا این مشکل می‌تواند سیستم یا کاربر باشد. زمانی که بروز می‌کنند باید آماده تشخیص و اقدام سریع باشیم. وقتی مدیریت پیش‌گیرانه کارایی را اجرا می‌کنیم پیشاپیش متوجه اتفاقات ناخواسته که ممکن است اتفاق بیافتد می‌شویم. این معمای درس حاضر است.

بعد از این درس یاد می‌گیریم:

- با شاخص‌های کارایی سیستم کار کنیم
- از ابزارهای کارایی ویندوز سرور استفاده کنیم.
- از Windows System Resource Monitor استفاده کنیم
- گزارشات کارایی را تولید و مشاهده کنیم.

زمان تقریبی : ۴۵ دقیقه

مدیریت منابع سیستم

ویندوز سرور دارای ابزارهای متعددی است که به تشخیص مشکلات بالقوه منابع سیستم کمک می‌کند. وقتی سیستم به طور مناسب پیکربندی نمی‌شود و منابع سیستم مانند CPU ، RAM یا دیسک را به طور مناسب اختصاص نمی‌دهد مانیتورینگ سیستم به ما در پیدا کردن گلوگاه کمک می‌کند. وقتی گلوگاه پیدا شد منابع اضافی را به آن اختصاص می‌دهیم. اگر سیستم فیزیکی باشد این یعنی خاموش کردن سیستم، نصب منابع سخت‌افزاری جدید مثلا افزودن ماژول‌های حافظه و سپس روشن کردن سیستم. اگر سیستم مجازی باشد بر اساس موتور مجازی‌سازی که استفاده می‌کنیم ممکن است بتوانیم منابع جدید را در حالی که سیستم روشن است به آن اختصاص دهیم. وگرنه ماشین را خاموش کرده منابع جدید را اختصاص داده و آنرا روشن می‌کنیم. پس از بالا آمدن سیستم دوباره کارایی را مانیتور می‌کنیم تا از رفع مشکل مطمئن شویم.

ابزارهای تشخیص گلوگاه در ویندوز سرور 2008 عبارتند از:

- Task Manager که میزان مصرف جاری منابع را نمایش می‌دهد.
- Event Viewer که وقایع خاصی را ثبت می‌کند که وقایع مرتبط با کارایی از جمله آنهاست.
- Reliability Moniter که تغییرات سیستم را مانیتور می‌کند و به ما امکان می‌دهد تشخیص دهیم آیا تغییر سبب ایجاد گلوگاه جدید شده است.

- Performance Monitor که داده‌ها را هم در زمان حال و هم در بازه‌های زمانی مشخص برای تشخیص مشکلات بالقوه جمع‌آوری می‌کند.
- Windows System Resource Manager (WSRM) که برای تشخیص میزان منابع مورد نیاز برنامه کاربردی به کار می‌رود. همچنین برای مدیریت منابع برنامه بر اساس پروفایلی که ما می‌سازیم استفاده می‌شود.

ابزارهای دیگری نیز مانند Microsoft System Center Operations Manager وجود دارند که وضعیت سیستم را مداوم مانیتور می‌کنند و به طور خودکار مشکلات مشخصی را برطرف می‌کنند. این ابزار برای مانیتور کردن برنامه‌های مشخص به پک‌های مدیریتی سفارشی نیاز دارد.

استفاده از Task Manager

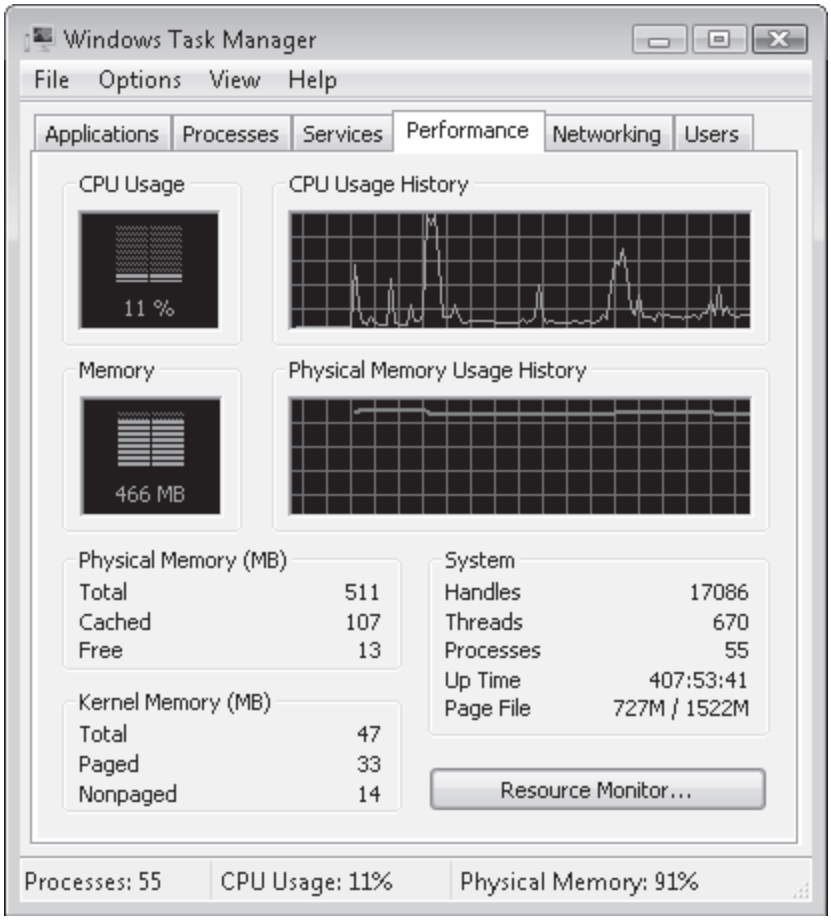
این ابزار ساده‌ترین ابزار مانیتورینگ می‌باشد. این ابزار وضعیت فعلی سیستم را نمایش می‌دهد و جنبه‌های کلیدی کارایی سیستم را پوشش می‌دهد که شامل موارد زیر است:

- برنامه‌های اجرا شده
- فرایندهای اجرا شده
- سرویس‌های اجراشده
- کارایی شامل میزان استفاده از CPU و حافظه
- شبکه شامل میزان استفاده از کارت شبکه (NIC)
- کاربران وارد شده به سیستم

راههای زیادی برای باز کردن ابزار Task Manager وجود دارد که راحت‌ترین آن کلیک راست روی نوار وظیفه و انتخاب Task Manager می‌باشد. روش دیگر استفاده همزمان از کلیدهای Ctrl+Alt+Delete می‌باشد. برای مثال از این روش در Server Core استفاده می‌شود به دلیل اینکه نوار وظیفه موجود نیست. یکی دیگر از راهها اجرای دستور Taskmgr.exe می‌باشد.

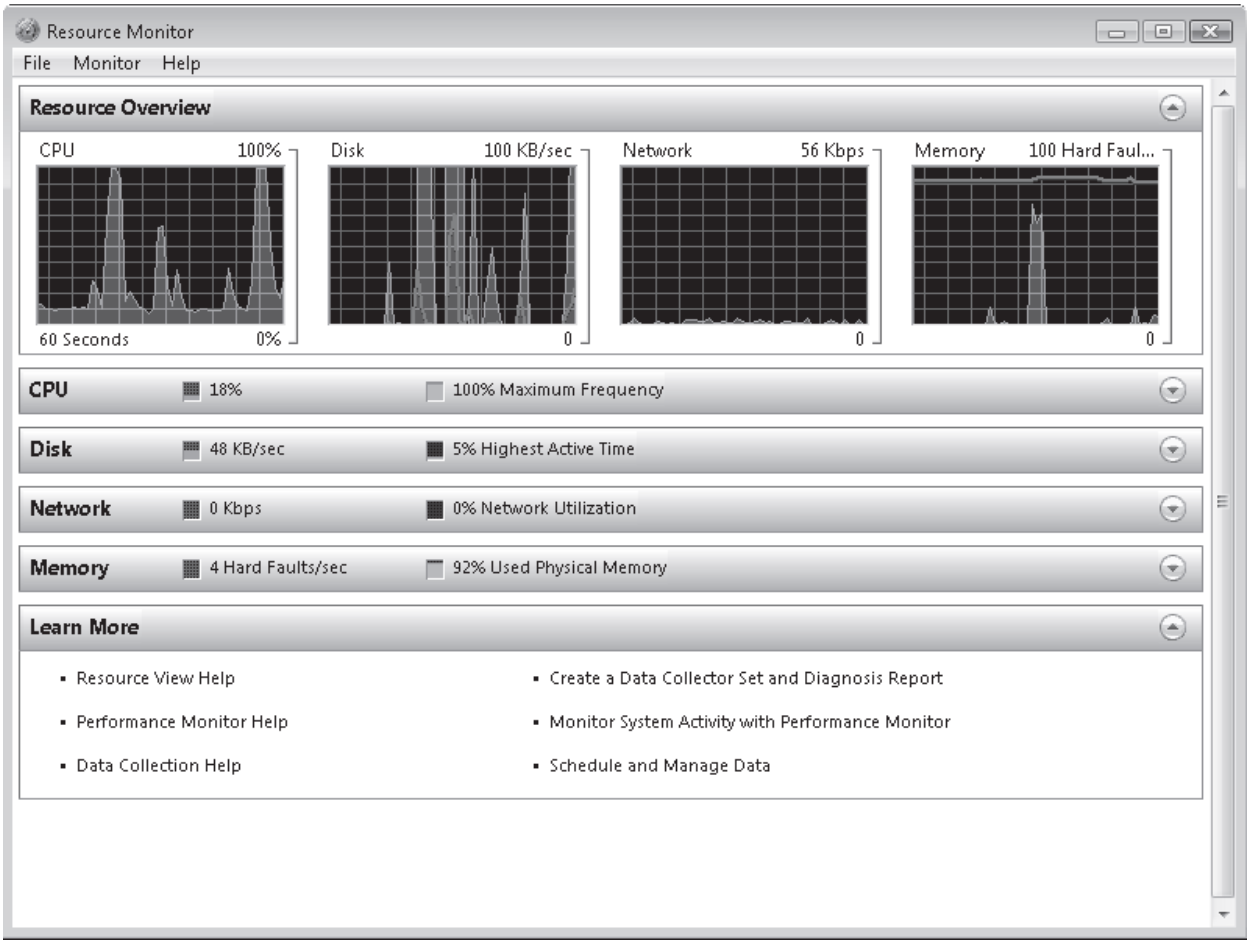
زبانه Performance مفیدترین زبانه است. (شکل ۷- ۱۳) این زبانه اطلاعات کاملی از میزان استفاده از منابع کلیدی سیستم نمایش می‌دهد. این زبانه دارای یک دکمه است که دسترسی به Resource Monitor را فراهم می‌کند. با زدن این دکمه ابزار Resource Monitor اجرا شده در حالی که پنجره Task Manager هم باز می‌ماند.

ابزار Resource Monitor یک فوق Task Manager است به این دلیل که میزان استفاده از CPU، دیسک، حافظه و شبکه را در یک نمودار واحد نمایش می‌دهد. (شکل ۸- ۱۳) به علاوه می‌توانیم جزئیات هر کامپوننت را نمایش دهیم به طوری که مشخص کنیم کدام پروسه‌ها ممکن است باعث بروز مشکل شوند. این دو ابزار برای مانیتور کردن فوری سرور مناسب هستند.



شکل ۷- ۱۳ مشاهده اطلاعات کارایی فعلی در Task Manager

برای مثال اگر سیستم حافظه کافی در اختیار نداشته باشد خواهیم دید میزان استفاده از حافظه پیوسته بالاست. در این مورد ویندوز مجبور می‌شود از حافظه مجازی روی دیسک استفاده کند و باید محتوای حافظه را بین حافظه فیزیکی و مجازی دائما جابجا کند. این جابجایی دایم یکی از مشکلات سرورهایی است که دارای حافظه کافی نیستند و اغلب با کندی سیستم تشخیص داده می‌شوند.



شکل ۸- ۱۳ مشاهده اطلاعات کارایی فعلی در Resource Manager

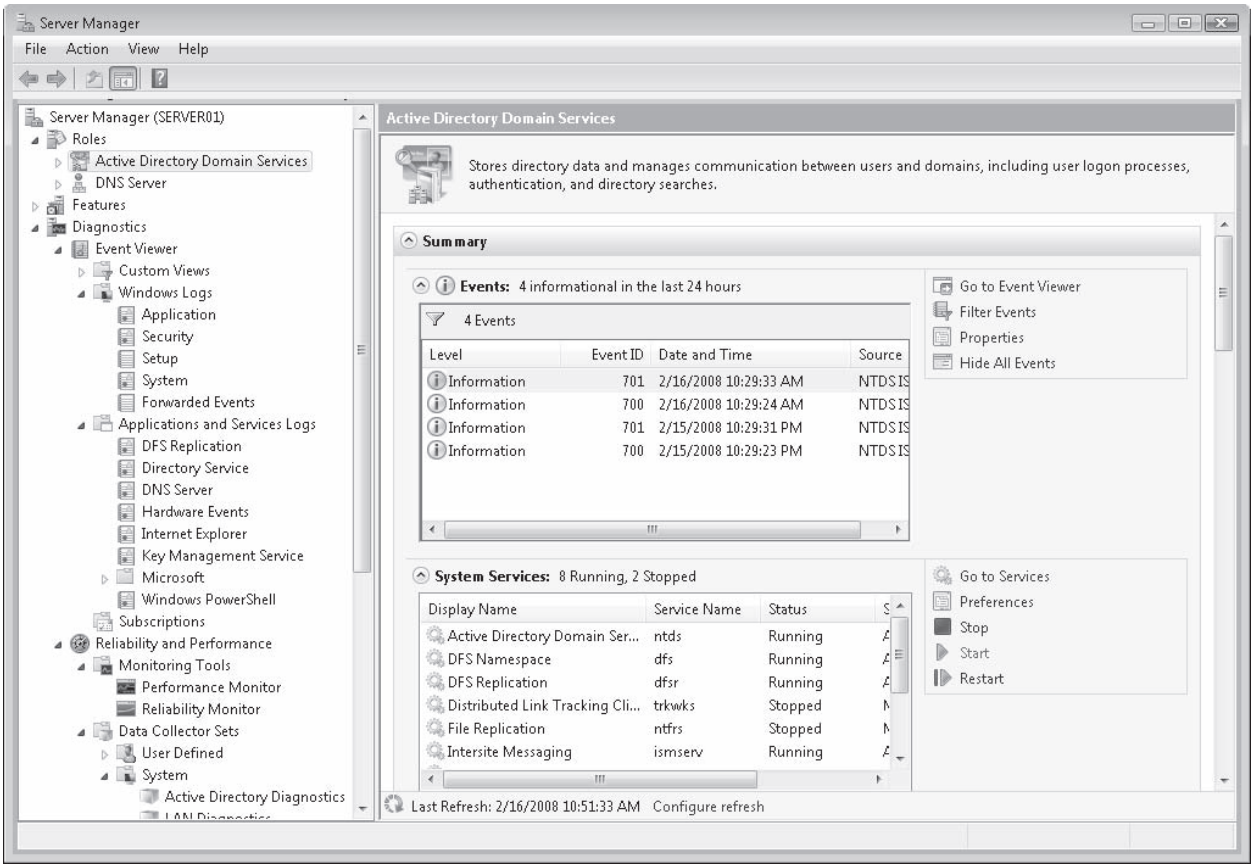
کار با Event Viewer

ابزار دیگر نمایش سلامت سیستم Windows Event Log می‌باشد. ویندوز وقایع زیادی را به منظور جمع‌آوری اطلاعات درباره سرویس‌های اجرا شده روی سرور ثبت می‌کند که به طور پیش‌فرض شامل وقایع Application، Security، Setup، System و Forwarded Events می‌باشد که همه در پوشه Windows Logs جای می‌گیرند. ولی روی DC ها وقایع بیشتری ثبت می‌شود که به عملیات AD DS مربوط هستند و در پوشه Application and Services Logs جای می‌گیرند و شامل موارد زیر هستند:

- DFS Replication که در دامنه‌ها و forest های دارای حالت عملیاتی کامل ویندوز سرور 2008 موجود است. اگر دامنه یا forest در یکی از حالت‌های قدیمی کار می‌کند وقایع برای سرویس تکثیر FRS ثبت می‌شود.
- Directory Service که روی عملیات مرتبط با AD DS متمرکز است.
- DNS Server که همه وقایع مرتبط با سرویس نام را که از عملیات AD DS پشتیبانی می‌کند لیست می‌کند.

یکی از بهترین ویژگی‌های Event Log مرتبط با Server Manager می‌باشد. به دلیل اینکه برای هر نقش ویندوز سرور 2008 به عنوان یک محل مدیریت مرکزی عمل می‌کند نمای سفارشی فراهم می‌کند که همه وقایع مرتبط با نقش خاص سرور را نشان می‌دهد. برای مثال اگر روی نقش Active Directory Domain Services کلیک کنیم Server Manager وقایع کلیدی مرتبط با این سرویس را در کنار بقیه وقایع نمایش می‌دهد. (شکل ۹- ۱۳)

Event Log سه نوع واقعه را لیست می‌کند: Information، Warning و Errors . به طور پیش‌فرض پیغام‌های Error در صفحه دارای اولویت بالا، Warining دارای اولویت متوسط و Information دارای اولویت پایین می‌باشد. بنابراین همیشه Errors در بالای صفحه ظاهر می‌شود و ما را از مشکل پیش‌آمده مطلع می‌کند. برای مشاهده جزئیات واقعه می‌توان روی واقعه دوبار کلیک کرد.



شکل ۹- ۱۳ مشاهده Summary Events برای AD DS در Server Manager

در ویندوز سرور 2008 و ویستا اطلاعات بیشتری نسبت به نسخه‌های قدیمی ویندوز می‌توان یافت. در نسخه‌های قبلی وقایع محرمانه بوده و اطلاعات محدودی را در اختیار قرار می‌داد. امروز شرح کامل یک واقعه را در Event Viewer می‌توانیم ببینیم و برای هر واقعه به بانک آنلاین مایکروسافت دراینترنت متصل شده و اطلاعات بگیریم. در کادر محاوره‌ای Properties واقعه اگر روی لینک Event Log Online Help کلیک کنیم به اطلاعات بانک در رابطه با همین واقعه دسترسی پیدا می‌کنیم. اگر بخواهیم اطلاعات خاص این واقعه را به دست آوریم پیغام ارسال اطلاعات برای مایکروسافت را تایید می‌کنیم.

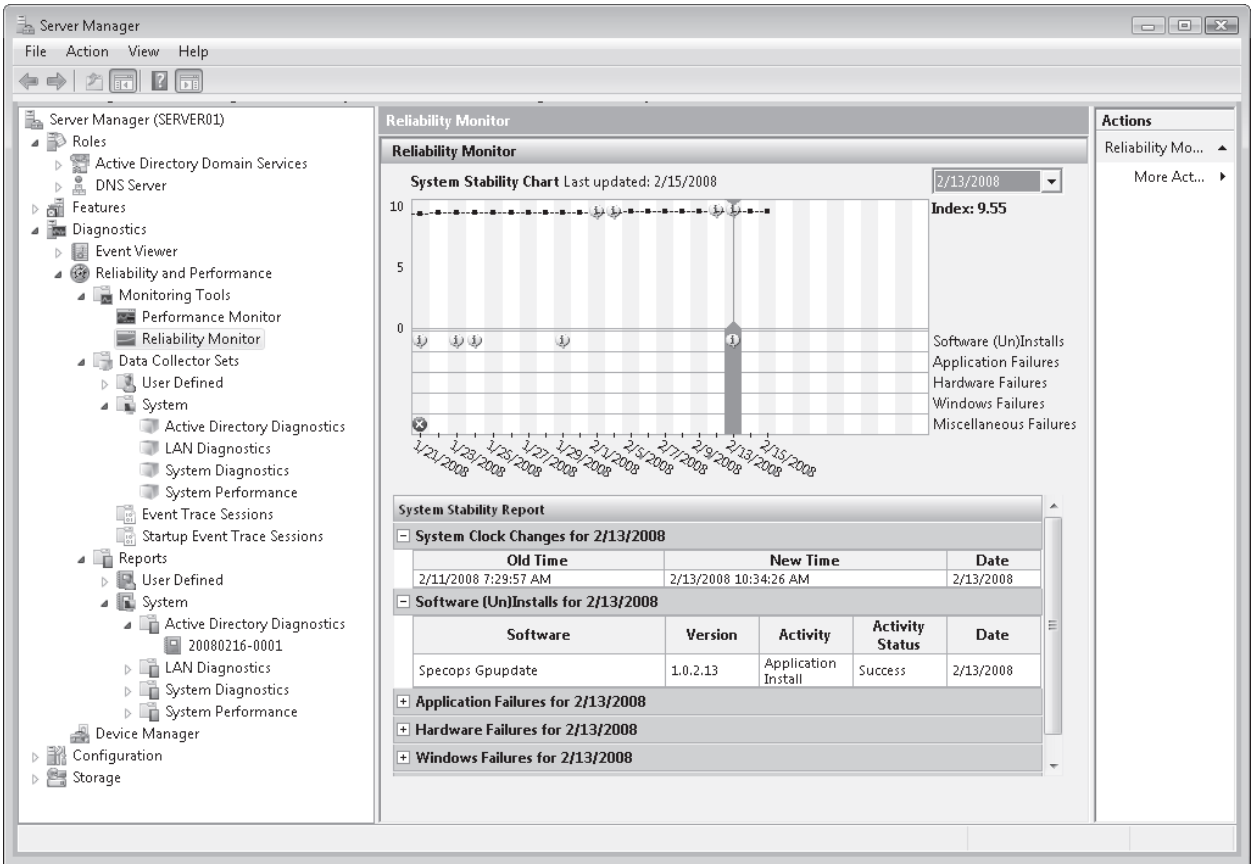
این بانک اطلاعاتی همه اطلاعات وقایع ویندوز را فراهم نمی‌کند ولی بیشتر آنها را پوشش می‌دهد. ما می‌توانیم از بانک‌های اطلاعاتی شرکت‌های دیگر برای دریافت اطلاعات استفاده کنیم.

هرچقدر اطلاعات ما درباره وقایع ویندوز بیشتر باشد برخورد با مشکل ساده‌تر می‌شود. روش‌های یاد شده به علاوه Windows Live Search در پیدا کردن اطلاعات به ما کمک می‌کنند. جستجو با event ID نتایج بیشتری را در بر خواهد داشت.

کار با Windows Reliability Monitor

ابزار مفید دیگری که به منظور تشخیص مسائل سیستم به کار می‌رود Reliability Monitor است. این ابزار زیر گره Diagnostic\Reliability and Performance\Monitoring Tools در Server Manager قرار دارد و برای دنبال کردن تغییرات سیستم طراحی شده است. هر بار که تغییری روی سیستم ایجاد می‌شود در این قسمت ثبت می‌شود. (شکل ۱۰- ۱۳) تغییرات شامل تغییرات سیستمی، نصب یا حذف نرم‌افزار، خطای برنامه کاربردی، خطای سخت‌افزاری و خطای ویندوزی می‌باشد.

وقتی مشکلی بروز می‌کند اولین جایی که باید کنترل شود Reliability Monitor می‌باشد. برای مثال اگر درایوری برای یک دستگاه نصب شده و مشکل به وجود آمده راه مناسب این است که نصب درایور را roll back کنیم و نتیجه را مشاهده کنیم. وقتی مشکلی متوجه کارایی سیستم باشد Reliability Monitor را بررسی می‌کنیم.



کار با Windows Performance Monitor

برخی مشکلات سریع قابل تشخیص نیستند و نیاز به جستجوی بیشتری دارند. در این گونه موارد Performance Monitor به ما کمک می‌کند. این ابزار زیر گره Diagnostic\ Reliability and Performance\Monitoring Tools در Server Manager قرار دارد و برای دریافت اطلاعات کارایی سیستم طراحی شده است. این ابزار برای تحت نظر گرفتن اجزاء سیستم یا به صورت آنی و یا بر اساس زمان‌بندی استفاده می‌شود.

اگر با نسخه‌های قدیمی ویندوز سرور آشنا باشید خواهید دید Performance Monitor ویندوز سرور 2008 ابزارهای مختلفی را با هم یکجا ارائه می‌دهد: Performance Logs and Alerts, Server Performance Advisor و System Monitor . Performance Monitor بخشی از Windows Reliability and Performance Monitor (WRPM) می‌باشد. جدول ۵-۱۳ هر کدام از ابزارهای WRPM را که مانیتورینگ کارایی را انجام می‌دهد و دسترسی مورد نیاز برای کار با آن را لیست می‌کند.

جدول ۵- ۱۳ ابزارهای WRPM و حقوق دسترسی

ابزار	شرح	عضویت مورد نیاز
Monitoring Tools, Performance Monitor	برای مشاهده کارایی سیستم در لحظه یا از طریق فایل‌های log قبلی به کار می‌رود. به حالت‌های نمودار یا گزارش ارائه می‌شود.	گروه Performance Log Users
Monitoring Tools, Reliability Monitor	به منظور مشاهده پایداری سیستم و وقایعی که آنرا تحت تاثیر قرار می‌دهد به کار می‌رود.	گروه Administrators محلی
Data collector sets	Data collectors را گروه‌بندی می‌کند. سه نوع آن موجود است: Performance counts، event trace data و system configuration information	گروه Local Performance Log Users با حق Log on as a batch
Reports	شامل کارایی پیکربندی شده و گزارشات تشخیصی می‌باشد. به منظور ارائه گزارش از داده‌های جمع‌آوری شده با استفاده	گروه Local Performance Log Users با حق Log on as a batch job

	از data collector set نیز استفاده می‌شود.	

ویندوز سرور 2008 دارای گروه جدید built-in به نام Performance Log Users می‌باشد که مدیران سرور را از عضویت در گروه Administrators محلی سیستم بی‌نیاز می‌کند و براحتی می‌توانند کار ثبت و مانیتورینگ کارایی سرور را انجام دهند. برای این کار حق کاربری Log On As A Batch Job مورد نیاز است که به طور پیش‌فرض به این گروه اعطاء می‌شود.

به علاوه ویندوز سرور 2008 هنگام نصب یک نقش الگوهای سفارشی Data Collector Set می‌سازد. این الگوها زیر گره System از گره Data Collector Sets از WRPM قرار دارد. برای مثال در مورد نقش AD DS چهار collector set ساخته می‌شود:

- The Active Directory Diagnostics set که داده‌ها را از کلیدهای رجیستری، شمارنده‌ها (performance counter) و بررسی وقایع مرتبط با کارایی AD DS روی DC محلی جمع می‌کند.
- LAN Diagnostics set که داده‌ها را از کارت‌های شبکه، کلیدهای رجیستری و سخت‌افزارهای دیگر سیستم با هدف تشخیص مشکلات مربوط به ترافیک شبکه روی DC محلی جمع می‌کند.
- System Diagnostic set داده‌ها را از منابع سخت‌افزاری محلی جمع‌آوری می‌کند تا به جریان مداوم بررسی کارایی سیستم روی DC کمک کند.
- System Performance set که روی وضعیت منابع سخت‌افزاری و زمان‌های پاسخ‌دهی سیستم DC محلی متمرکز است.

از بین چهار مورد اولین مفیدترین برای AD DS محسوب می‌شود. امکان ساخت data set اختصاصی خود را داریم. برای این کار جدول ۶- ۱۳ شمارنده‌های مورد نیاز در data set را لیست می‌کند.

جدول ۶- ۱۳ مانیتور کردن شمارنده‌های رایج برای AD DS

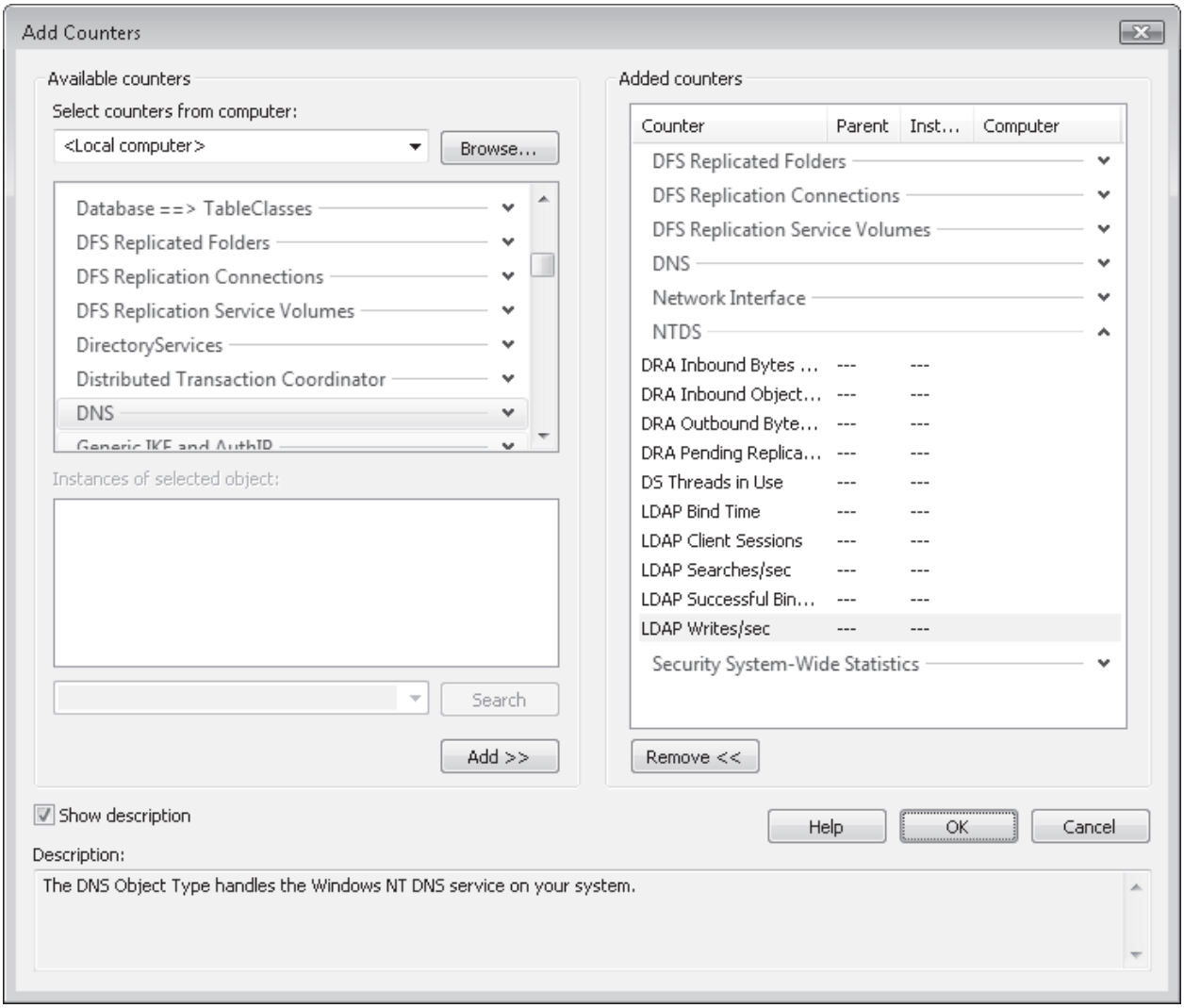
شمارنده	شرح	علت
Network Interface: Bytes Total/Sec	میزان ارسال و دریافت هر کدام از رابط‌های شبکه را نشان می‌دهد.	شبکه را به منظور تشخیص نسبت بالای استفاده از کارت شبکه پایش می‌کند. به ما می‌گوید که به بخش‌بندی شبکه یا افزایش پهنای باند نیاز داریم یا نه
Network Interface: Packets Outbound Discarded	تعداد پکت‌های خروجی که دور انداخته شده‌اند حتی اگر هیچ خطایی کشف نشود	صف‌های طولانی نشان می‌دهد که شبکه گلوگاه است.
NTDS: DRA Inbound Bytes Total/Sec	تعداد بایت‌های دریافت شده از طریق تکثیر. هم شامل داده‌های فشرده و هم غیرفشرده می‌شود.	اگر این شمارشگر حرکتی انجام ندهد نشان‌دهنده این است که شبکه تکثیر را کند کرده است.
NTDS: DRA Inbound Object Updates Remaining in Packet	تعداد اشیاء به روز شده دریافت شده از طریق تکثیر که هنوز به سرور محلی اعمال نشده	این مقدار باید کم باشد. مقادیر بالا نشان می‌دهد که سرور قابلیت کافی در استفاده از داده دریافت شده توسط تکثیر را ندارد.
NTDS: DRA Outbound Bytes Total/Sec	تعداد بایت‌های ارسال شده در ثانیه. مجموع داده‌های فشرده و غیر فشرده می‌باشد.	اگر این شمارشگر حرکتی انجام ندهد نشان‌دهنده این است که شبکه تکثیر را کند کرده است.
NTDS: DRA Pending Replication	انباشتگی تکثیر روی سرور	اگر این شمارشگر حرکتی انجام ندهد

Synchronizations		نشان‌دهنده این است که شبکه تکثیر را کند کرده است.
NTDS: DS Threads In Use	تعداد رشته‌های (thread) مورد استفاده AD DS	اگر فعالیتی مشاهده نشود ممکن است به این علت باشد که شبکه از پردازش درخواست کلاینت‌ها جلوگیری می‌کند
NTDS: LDAP Bind Time	زمان صرف شده برای تکمیل آخرین LDAP binding	مقادیر بالا هم نشان‌دهنده مشکل کارایی سخت‌افزار و هم شبکه می‌باشد.
NTDS: LDAP Client Sessions	تعداد نشست‌های (session) کلاینت LDAP که متصل شده است	اگر فعالیتی مشاهده نشود شبکه ممکن است مشکل داشته باشد.
NTDS: LDAP Searches/Sec	تعداد جستجوهای LDAP در ثانیه	اگر فعالیتی مشاهده نشود شبکه ممکن است مشکل داشته باشد.
NTDS: LDAP Successful Binds/Sec	تعداد LDAP bind ها در ثانیه	اگر فعالیتی مشاهده نشود شبکه ممکن است مشکل داشته باشد.
NTDS: LDAP Writes /Sec	تعداد تغییرات موفقیت‌آمیز LDAP در ثانیه	اگر فعالیتی مشاهده نشود شبکه ممکن است مشکل داشته باشد.
Security System-Wide Statistics: Kerberos Authentications	تعداد تایید هویت Kerberos روی سرور در ثانیه	اگر فعالیتی مشاهده نشود ممکن است به این علت باشد که شبکه از پردازش درخواست تایید هویت جلوگیری می‌کند
Security System-Wide Statistics: NTLM Authentication	تعداد تایید هویت NTLM روی سرور در ثانیه	اگر فعالیتی مشاهده نشود ممکن است به این علت باشد که شبکه از پردازش درخواست تایید هویت جلوگیری می‌کند
DFS Replicated Folders: All Counters	شمارشگر تداخل داده‌ها	اگر فعالیتی مشاهده نشود شبکه ممکن است مشکل داشته باشد.
DFS Replication Connections: All Counters	شمارشگر ارتباطات از بیرون به داخل	اگر فعالیتی مشاهده نشود شبکه ممکن است مشکل داشته باشد.
DFS Replication Service Volumes: All Counters	شمارشگر USN و پردازش بانک اطلاعاتی روی هر پارتیشن	اگر فعالیتی مشاهده نشود پردازشگر ممکن است با مشکل مواجه شده باشد.
DNS: All Counters	DNS Object Type با سرویس NT DNS روی سیستم کار می‌کند.	اگر فعالیتی مشاهده نشود ممکن است شبکه با مشکل مواجه شده باشد و کلاینت‌ها نتوانند DC را پیدا کنند.

برای افزودن شمارشگر به Performance Monitor به سادگی روی علامت (+) در نوار ابزار بالای صفحه کلیک می‌کنیم. کادر محاوره‌ای Add Counters به نمایش درمی‌آید. (شکل ۱۱- ۱۳) در برخی موارد به گروه فرعی زیر شمارشگر نیاز داریم (جدول ۶-۱۳). در برخی موارد دیگر به کل زیرگروه شمارشگر نیاز داریم. وقتی به شمارشگرفرعی نیاز داریم روی فلش رو به پایین کنار گروه کلیک می‌کنیم، شمارشگر فرعی را پیدا کرده و روی Add کلیک می‌کنیم. ولی اگر به کل شمارشگر نیاز داشته باشیم روی شمارشگر

کلیک کرده و Add را کلیک می‌کنیم. این کار باعث افزوده شدن شمارشگر با علامت ستاره زیر آن شده که معنی آن افزوده شدن همه شمارشگرهای فرعی می‌باشد.

برای دریافت اطلاعات یک شمارشگر روی Show Description کلیک می‌کنیم. سپس وقتی روی هر شمارشگری کلیک کنیم توصیف مختصری از آن در انتهای کادر محاوره‌ای ظاهر می‌شود.



شکل ۱۱-۱۳ افزودن شمارشگر به Performance Monitor

پس از افزودن شمارشگرها و کلیک کردن روی OK کار ثبت آنها شروع می‌شود. هر شمارشگر دارای یک خط با رنگ مخصوص به خود خواهد بود. برای حذف یک شمارشگر کافی است روی آن کلیک کرده و دکمه Delete را روی نوار ابزار کلیک کنیم.

ما می‌توانیم Performance Monitor را مانند برنامه media player استارت و متوقف کنیم. اگر بخواهیم نمودار شمارشگرها را ثبت کنیم روی Performance Monitor کلیک راست کرده و New را انتخاب می‌کنیم. سپس New Data Collector Set را انتخاب می‌کنیم. کار را دنبال می‌کنیم تا نمودارها ذخیره شوند که بتوانیم بعدا از آنها استفاده کنیم.

ساخت مقیاس (Baseline) برای AD DS و DNS

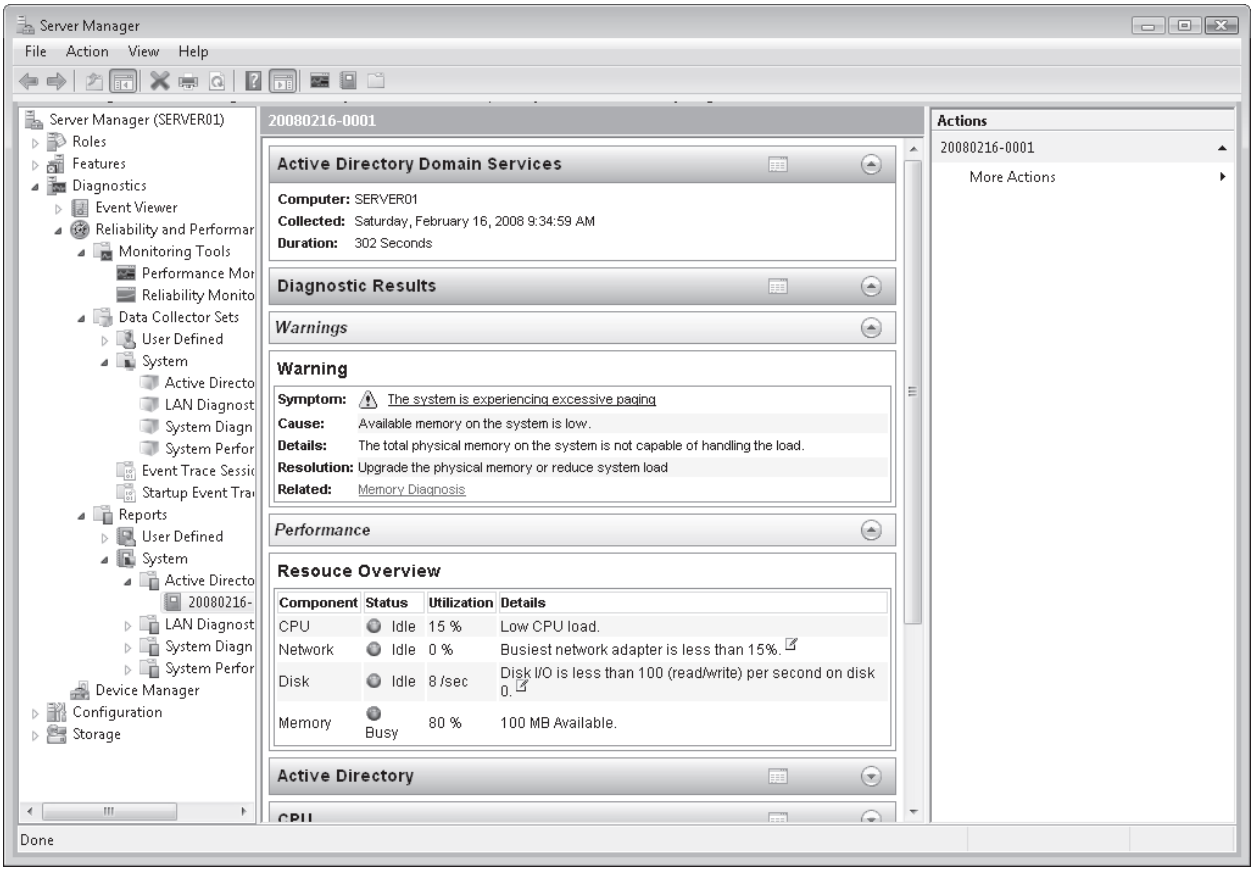
جهت مانیتورینگ بلند مدت سیستم باید data collector set بسازیم. وقتی ابتدا سیستمی را نصب می‌کنیم بهتر است مقیاسی برای کارایی سیستم بسازیم. بعد اگر بار سیستم بالا رفت بتوانیم آنرا با مقیاس مقایسه کنیم و تغییرات را بررسی می‌کنیم. این کار به ما کمک می‌کند تشخیص دهیم آیا منابع بیشتری برای سیستم مورد نیاز است یا نه. برای مثال در مورد DC بهتر است کارایی را در زمان‌های اوج و کف مصرف ثبت کنیم. زمان اوج زمانی است که صبح کاربران به شبکه وارد می‌شوند. برای ساخت مقیاس کارایی نیاز به instanceهای شمارشگر به مدت ۳۰ تا ۴۵ دقیقه آنهم در یک هفته در زمان‌های اوج و نرمال داریم. مراحل کار به صورت زیر است:

۱. تعیین منابع برای اندازه‌گیری

۲. ثبت داده‌ها در زمان‌های مشخص

۳. ذخیره داده‌های ثبت شده برای دسترسی آینده

ما می‌توانیم collector set های سفارشی بسازیم ولی در ویندوز سرور 2008 بهتر است از الگوهای پیش‌فرض که هنگام نصب نقش سرور افزوده می‌شود استفاده کنیم. برای مثال جهت ساخت مقیاس برای DC به سادگی یک collector set بر پایه الگوی Active Directory Diagnostics می‌سازیم و آنرا در بازه‌های زمانی مشخص اجرا می‌کنیم.
بعد وقتی آماده مشاهده نتایج شدیم به بخش Reports از گره Windows Reliability and Performance مراجعه می‌کنیم. روی collector set مورد نظر کلیک راست کرده و Latest Report را انتخاب می‌کنیم. این کار باعث ایجاد گزارش شده و اطلاعات مبسوطی درباره وضعیت DC ارائه می‌کند (شکل ۱۲- ۱۳)



شکل ۱۲- ۱۳ مشاهده گزارش تشخیصی Active Directory

کار با Windows System Resouce Manager

ویندوز سرور 2008 حاوی یک ابزار اضافی برای مدیریت منابع سیستم با نام WSRM است. این ابزار یک ویژگی است که از پنجره Add Features در Server Manager قابل افزودن است. WSRM به دو طریق استفاده می‌شود. اول اینکه برای تعیین پروفایل برنامه‌ها استفاده می‌شود. این یعنی به تشخیص میزان منابع مورد نیاز برنامه کمک می‌کند. WSRM وقتی در این حالت کار می‌کند وقایع برنامه را زمانی که از حد مجاز عبور می‌کند ثبت می‌کند. این کار به ما کمک می‌کند نیازمندی‌های برنامه را به خوبی بسنجیم.
حالت دوم مدیریتی است. در این حالت WSRM از سیاست‌های تخصیص منابع خود در جهت کنترل میزان منابع مصرفی توسط برنامه‌های روی سرور استفاده می‌کند. اگر برنامه‌ها بخواهند از این محدوده عبور کنند WSRM برنامه را حتی می‌تواند متوقف کند تا بقیه برنامه‌های سرور به کار خود ادامه دهند. ولی اگر مجموع منابع مصرف شده پردازشگر به ۷۰ درصد نرسد WSRM به برنامه‌ها کاری نخواهد داشت.
WSRM همچنین از Alerts and Event Monitoring پشتیبانی می‌کند. این ابزار یک ابزار قدرتمندی است که به ما در کنترل استفاده از پردازشگر و حافظه روی سرورهای با چند پردازشگر کمک می‌کند. به طور پیش‌فرض WSRM دارای چهار سیاست مدیریتی

آماده می‌باشد ولی می‌توانیم سیاست‌های متعددی نیز خودمان تعریف کنیم. اساسا WSRM تضمین می‌کند برنامه‌های با اولویت بالا همیشه دارای منابع کافی هستند که در سرورهای DC می‌تواند خیلی مفید باشد.

ابتدا WSRM را جهت ارزیابی چگونگی استفاده از برنامه‌ها به کار می‌گیریم. سپس سیاست‌های مدیریتی خود را اعمال می‌کنیم. قبل از اعمال سیاست‌های خود آنها را به طور کامل تست کنید. بعد با استفاده از WSRM Calendar تعیین می‌کنیم چه موقع کدام سیاست اعمال شود.

WSRM می‌تواند با سناریوهای زیر به کار رود:

- از سیاست‌های آماده و یا تعریف شده خود برای مدیریت منابع سیستم استفاده کنیم. منابع می‌توانند بر حسب پردازش، کاربر یا IIS application pool اختصاص یابند.
- از قواعد calendar برای اعمال سیاست‌ها در زمان‌های مختلف بهره بگیریم.
- روند انتخاب سیاست منابع را بر اساس خصوصیات، وقایع یا حتی تغییرات شمارشگرهای حافظه و پردازشگر سرور خودکار سازیم.
- اطلاعات مصرف منابع را در فایل‌های متنی جمع‌آوری کرده یا آنها را در بانک SQL ذخیره کنیم. همچنین می‌توانیم سیستم جمع‌آوری WSRM مرکزی ایجاد کنیم تا منابع مصرفی سیستم‌های متعددی را مقایسه کنیم.

جدول ۷- ۱۳ سیاست‌های WSRM و منابع سفارشی

سیاست موجود	شرح
تقسیم به نسبت پردازه	به برنامه‌ها سهم‌های مساوی از منابع اختصاص می‌دهد.
تقسیم به نسبت کاربر	پردازش‌های منتسب به کاربر را گروه‌بندی کرده و به هر گروه سهم مساوی اختصاص می‌دهد.
تقسیم به نسبت نشست (session)	به هر session به میزان مساوی منابع را اختصاص می‌دهد.
تقسیم به نسبت IIS application pool	به IIS application pool ها منابع مساوی اختصاص می‌دهد.
منبع سفارشی	شرح
Process Matching Criteria	برای انتساب یک برنامه به یک سیاست به کار می‌رود. می‌تواند توسط نام، دستور، کاربر مشخص یا گروهها انتخاب شود.
Resource Allocation Policies	برای اختصاص منابع پردازشگر و حافظه به پردازش‌هایی که شرایط مشخص شده را احراز می‌کنند به کار می‌رود.
Exclusion lists	به منظور حذف برنامه‌ها، سرویس‌ها، کاربران و گروهها از مدیریت WSRM استفاده می‌شود. همچنین می‌توان از مسیرهای خط فرمان برای این کار استفاده کرد.
Scheduling	از calendar interface برای وقایع مبتنی بر زمان به منظور اختصاص منابع استفاده می‌شود.
Conditional policy Application	بر اساس وقایعی مشخصی تعیین می‌شود که سیاست اجرا شود یا نه.

WSRM به طور کامل چگونگی اجرای برنامه‌ها را کنترل می‌کند.

تمرینات تحلیل کارایی AD DS

در این تمرین از WRPM و WSRM برای مشاهده کارایی سرورها استفاده می‌شود. ابتدا یک collector set ساخته و آنرا اجرا می‌کنیم. سپس گزارش آنرا مشاهده می‌کنیم. در تمرین ۲ WSRM را نصب می‌کنیم تا سیاست‌های آنرا ببینیم.

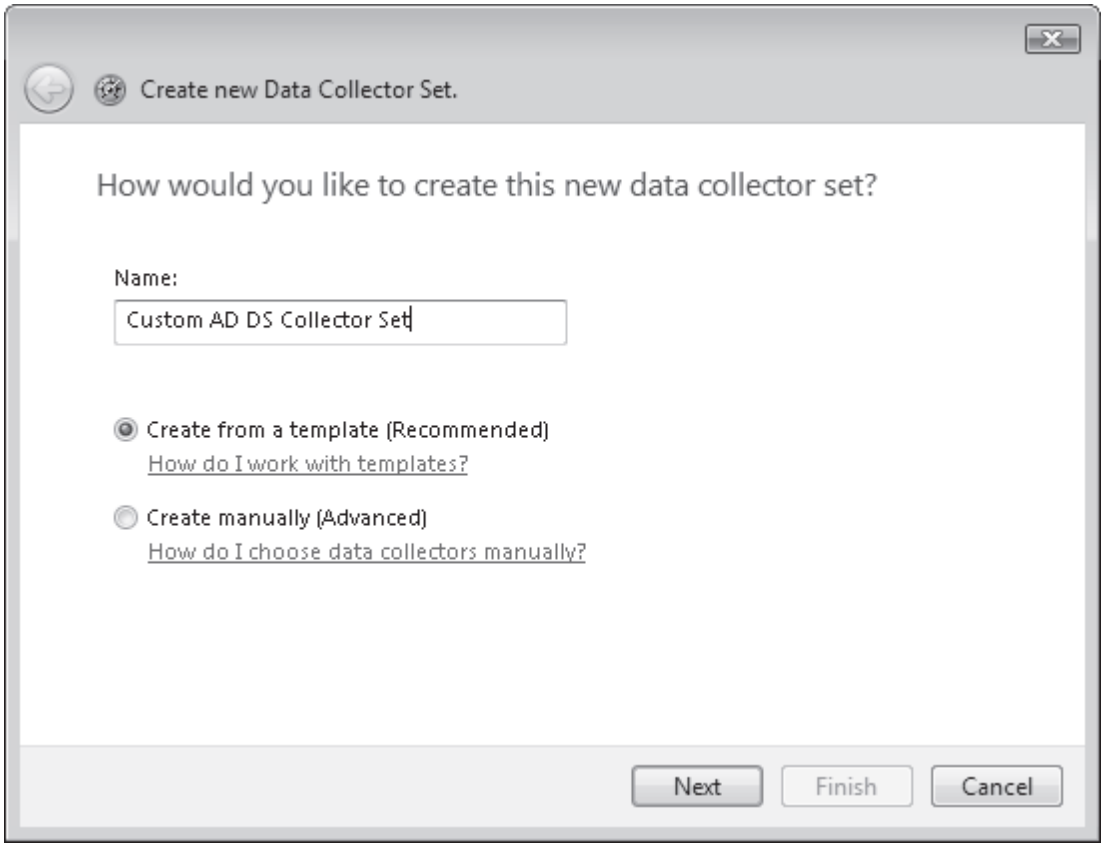
تمرین ۱ ساخت Dara Collector Set

Dara collector set هسته اصلی مانیتورینگ کارایی و گزارش گیری در WRPM می‌باشد. ما می‌توانیم ترکیبی از dara collector ها را ساخته و آنها را به عنوان dara collector set منفرد ذخیره کنیم.

۱. با کاربر Administrator دامنه به SERVER10 وارد می‌شویم.

۲. در Server Manager گره Diagnostic\Reliability and Performance\Dara Collector Sets را باز کرده و روی User Difined کلیک راست کرده و New و سپس Dara Collector Set را انتخاب می‌کنیم.

۳. در صفحه Template عبارت Custom AD DS Collector Set را تایپ کرده و Create From A Template (Recommended) را انتخاب می‌کنیم. سپس روی Next کلیک می‌کنیم.



۴. در صفحه بعد الگوی Active Directory Diagnostics را انتخاب کرده و روی Next کلیک می‌کنیم.

۵. به طور پیش‌فرض ویزارد %systemdrive%\Perflogs\Admin را به عنوان دایرکتوری ریشه انتخاب می‌کند. ولی ممکن است ترجیح دهیم collector set خود را روی درایو مجزا نگهداری کنیم.

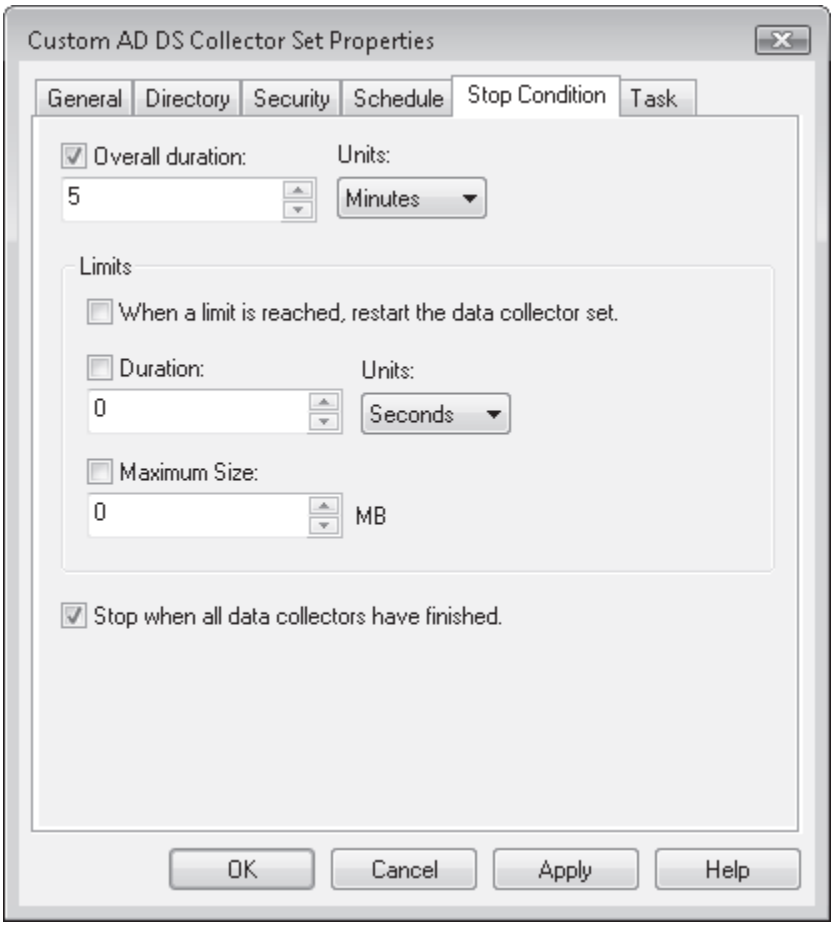
۶. در صفحه Create The Dara Collector Set در فیلد Run نام کاربری را تایپ کرده و کلمه عبور را وارد می‌کنیم تا dara collector set اجرا شود. مقادیر پیش‌فرض را حفظ کرده و روی Finish کلیک می‌کنیم.

۷. روی Custom AD DS Collector Set کلیک راست کرده و روی Properties کلیک می‌کنیم.

۸. زبانه Schedule را کلیک کرده و روی Add کلیک می‌کنیم تا تاریخ و زمان شروع را مشخص کنیم.

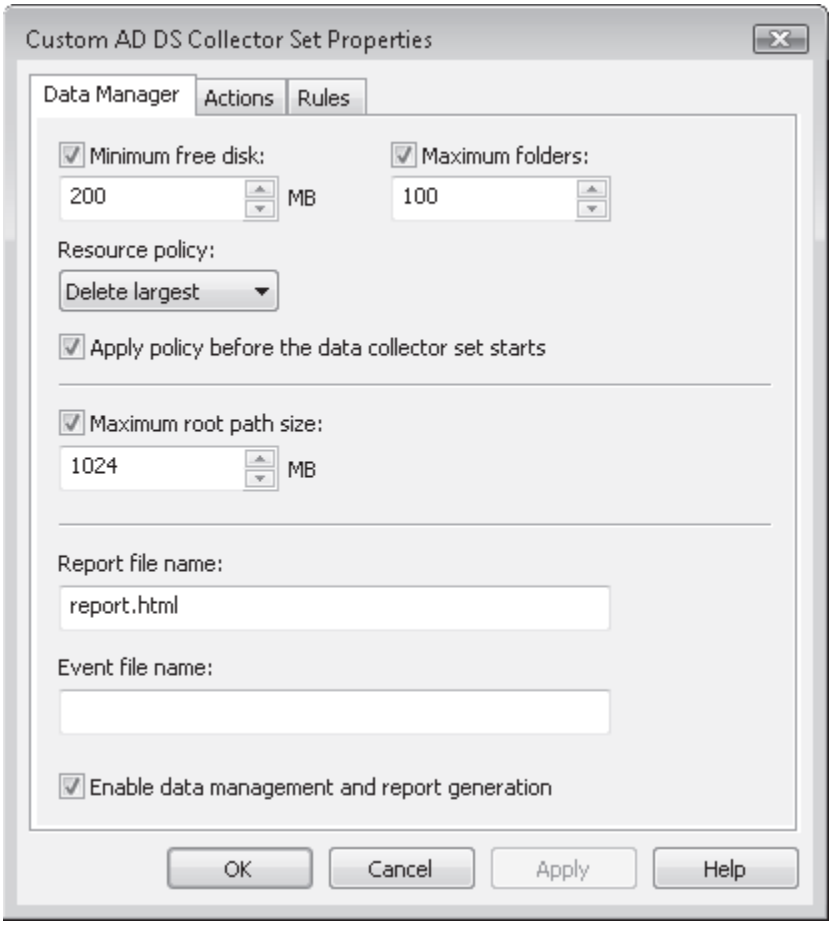
۹. در کادر محاوره‌ای Folder Action مطمئن می‌شویم تاریخ روز به عنوان تاریخ شروع مشخص شده است. کادر Expiration Date را انتخاب کرده و آنرا روی هفته تنظیم می‌کنیم. نیز مطمئن می‌شویم که زمان گزارش به تاریخ جاری تنظیم شده باشد. روی OK کلیک می‌کنیم.

۱۰. زبانه Stop Condition را باز کرده و کادر Overal Duration را انتخاب می‌کنیم. مقدار آن را روی ۵ دقیقه تنظیم می‌کنیم و کادر Stop When All Data Collector Have Finished را علامت می‌زنیم. روی OK کلیک می‌کنیم.



۱۱. روی Custom AD DS Data Collector Set کلیک راست کرده و روی Data Manager کلیک می‌کنیم.

۱۲. در زبانه Data Manager می‌توانیم مقادیر پیش‌فرض را رها کنیم یا بر حسب سیاست بازیابی داده خود تغییر دهیم. اینجا مقادیر پیش فرض را قبول می‌کنیم.

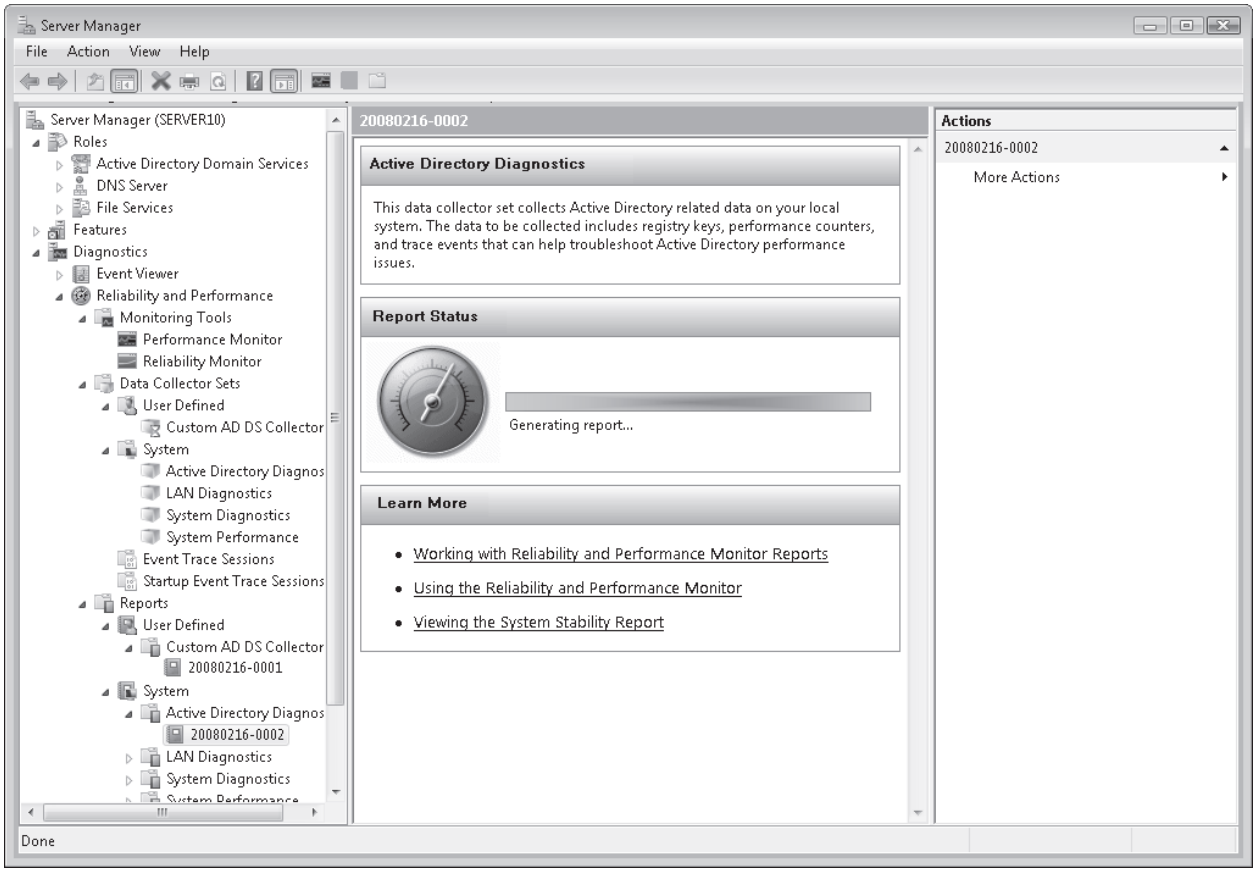


۱۳. در زبانه Actions می‌توانیم عملیات مدیریت داده خاصی را برای این Collector set تنظیم کنیم. توجه داشته باشید که سه سیاست از قبل موجود است. روی سیاست 1 Day(s) و بعد Edit کلیک می‌کنیم.

۱۴. دو بار روی OK کلیک می‌کنیم.

۱۵. روی Active Directory Diagnostic template collector set زیر Data Collector Sets, System کلیک راست کرده و روی Latest Report کلیک می‌کنیم.

۱۶. اگر گزارشی موجود نباشد و ما بخش Reports مربوط به WRPM را باز کنیم می‌بینیم که collection set گزارشی را تهیه می‌کند. روی نام گزارش کلیک می‌کنیم.

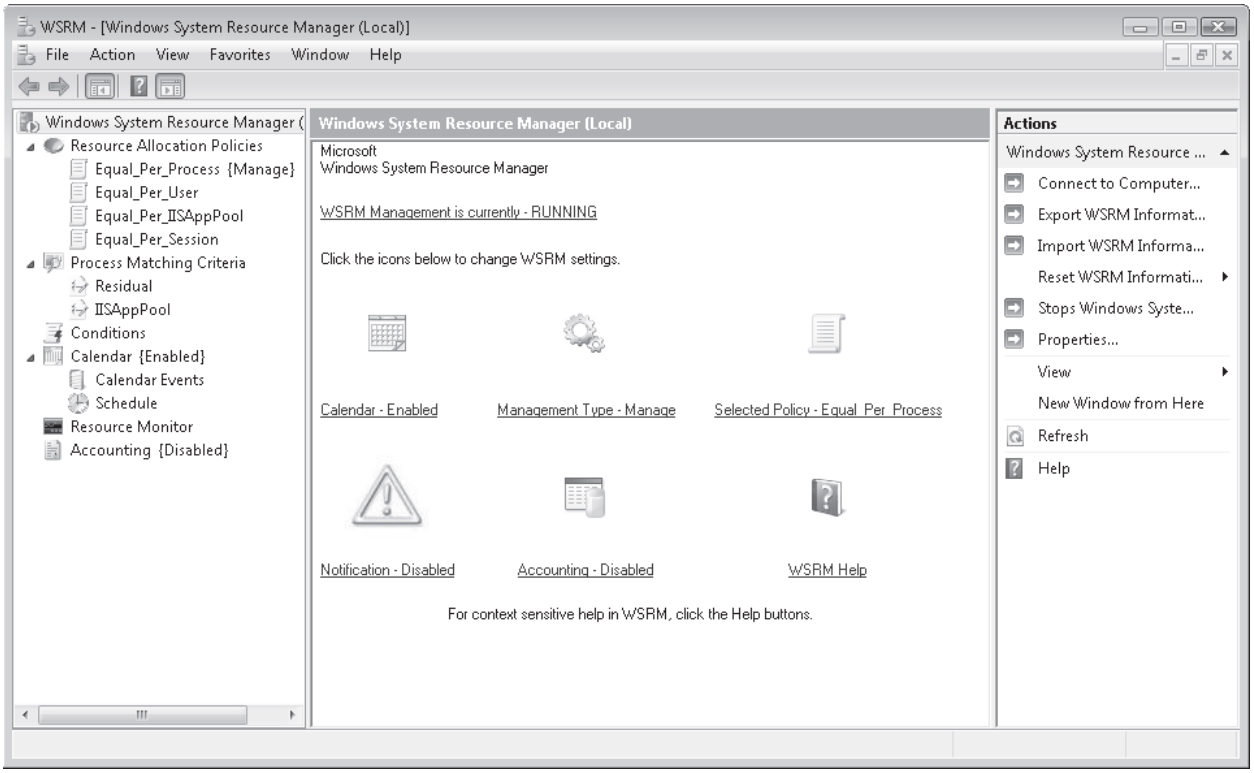


۱۷. گزارشی را که توسط collector set ما به دست آمده مشاهده می‌کنیم. روی Report Name زیر نام collector set در گزارشات System کلیک می‌کنیم.

تمرین ۲

در این تمرین سرویس WSRM را نصب کرده و چگونگی کارکرد آنرا مشاهده می‌کنیم.

۱. با کاربر مدیر دامنه به Server10 وارد می‌شویم.
۲. در Server Manager روی گره Features کلیک راست کرده و Add Features را انتخاب می‌کنیم.
۳. در صفحه Select Features از ویزارد Add Features گزینه Windows System Resource Manager را انتخاب کرده و روی Next کلیک می‌کنیم.
۴. Server Manager پیغام می‌دهد که Windows Internal Database را مشخص کنیم. روی Add Required Features کلیک می‌کنیم. روی Next کلیک می‌کنیم.
۵. اطلاعات صفحه Confirm Installation Selection را مرور کرده و روی Install کلیک می‌کنیم.
۶. نتایج نصب را بررسی کرده و روی Close کلیک می‌کنیم.
۷. حالا می‌توانیم از WSRM روی سیستم خود استفاده کنیم. WSRM یک کنسول مستقل است که در Administrative Tools قرار دارد.
۸. وقتی کنسول را باز می‌کنیم از ما می‌پرسد به کدام کامپیوتر می‌خواهیم متصل شویم. گزینه This Computer را انتخاب کرده و روی Connect کلیک می‌کنیم.



شکل ۱۳- ۱۳ استفاده از WSRM

خلاصه درس

- در ویندوز سرور 2008 از یک سری ابزار برای مدیریت و مانیتور کردن میزان مصرف منابع کامپیوتر استفاده می‌کنیم. این ابزارها شامل Task Manager، Event Logs، Reliability Monitor و Performance Monitor می‌باشد.
- Performance Monitor ابزار مستقلی است که حاوی مجموعه ابزارهای قبلی ویندوز است. این ابزارها شامل Performance Logs and Alerts، Server Performance Advisor و System Monitor می‌باشد.
- از WSRM برای کنترل چگونگی رفتار منابع به صورت منظم استفاده می‌شود. در حقیقت دو عملکرد دارد. مانیتور کردن میزان مصرف منابع برحسب زمان و فعالیت. سپس به منظور کنترل دسترسی به منابع بر اساس سیاست‌های مشخص قابل استفاده است.

سئوالات پایان درس

۱. فرض کنید مدیر سیستم دامنه contoso.com هستیم و وظیفه بررسی data collector set های روی DC که کارشناس دیگری ساخته به ما محول شده است. وقتی آنها را بررسی می‌کنیم متوجه می‌شویم که دائما در حال اجرا هستند و ظرفیت ذخیره‌سازی به پایان رسیده است. مشکل از کجا می‌تواند باشد؟ (امکان انتخاب همه گزینه ها وجود دارد)
   A. Collector set ها تاریخ انقضا ندارند.
   B. اجرای Collector set ها زمان‌بندی نشده است.
   C. Collector set ها شرایط توقف ندارند.
   D. Collector set ها به طور نامناسب زمان‌بندی شده‌اند.

۲. فرض کنید مدیر سیستم دامنه contoso.com هستیم. وقتی به DC وارد می‌شویم تا عملیات نگهداری را انجام دهیم متوجه می‌شویم که پاسخ‌دهی سرور خیلی کند است. حالا می‌خواهیم علت را پیدا کنیم. از کدام ابزار استفاده می‌کنیم؟ (امکان انتخاب همه گزینه ها وجود دارد)
   A. Reliability Monitor

B. Event Viewer
C. Task Manager
D. Performance Monitor

فصل ۱۴

Active Directory Lightweight Directory Services

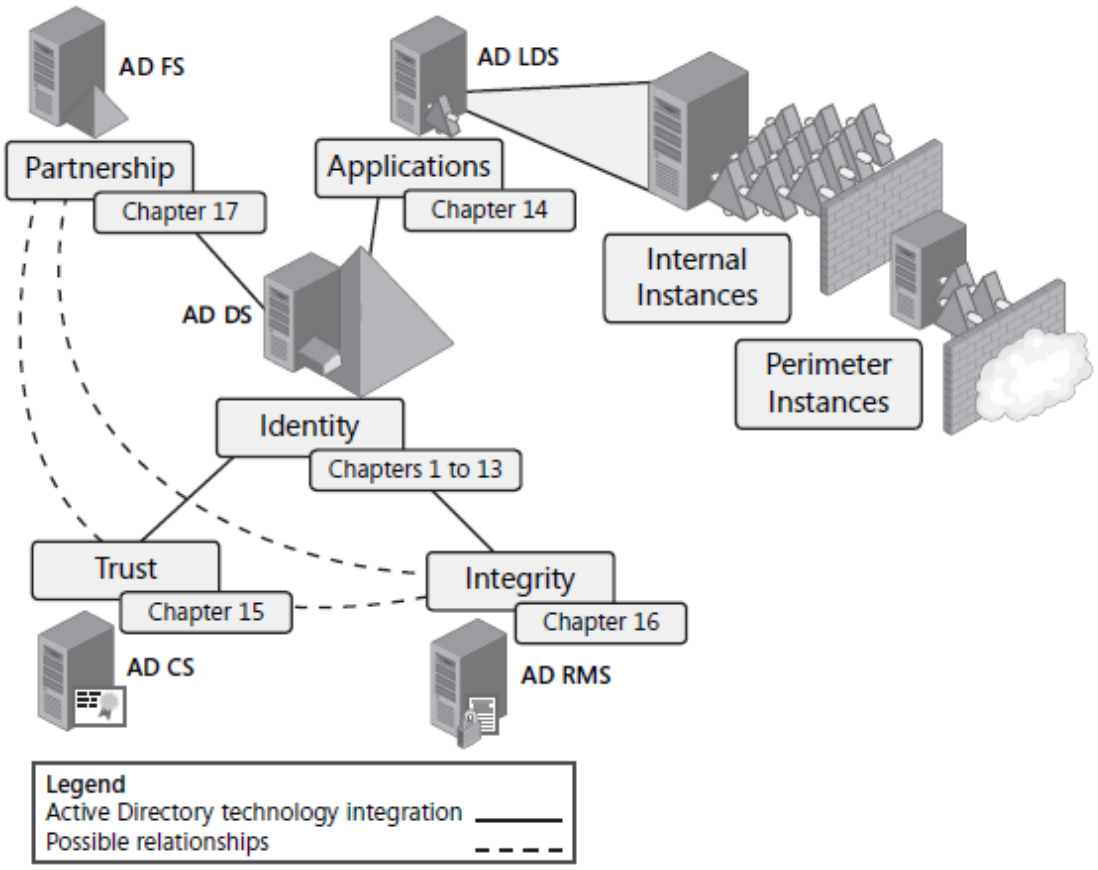
از بین ۵ فناوری موجود Active Directory در ویندوز سرور 2008 ، AD LDS از همه به AD DS شباهت بیشتری دارد. دلیل آن این است که AD LDS چیزی جز مجموعه عملکرد AD DS نیست. هر دو از یک هسته کد استفاده می‌کنند و هر دو ویژگی‌های مشابهی دارند.

AD LDS که قبلا Active Directory Application Mode (ADAM) نامیده می‌شد یک فناوری طراحی شده به منظور پشتیبانی از برنامه‌های وابسته به دایرکتوری می‌باشد. AD LDS برای مدیرانی که می‌خواهند از برنامه‌های وابسته به دایرکتوری بدون عجین شدن با دایرکتوری NOS استفاده کنند نعمت محسوب می‌شود.

AD DS نیز از برنامه‌های وابسته به دایرکتوری پشتیبانی می‌کند. نمونه بارز آن Microsoft Exchange Server 2007 است. همه اطلاعات کاربران توسط دایرکتوری فراهم می‌شود. وقتی سرور Exchange در شبکه نصب می‌شود AD DS schema از لحاظ اندازه دوبرابر می‌شود. همان طور که می‌دانید تغییرات schema به راحتی صورت نمی‌گیرد و دلیل آن این است که وقتی شیئی به آن افزوده می‌شود هیچ‌گاه حذف نمی‌شود. افزودن به schema برای یک برنامه نظیر Exchange مشکلی ندارد چون سرویس مهم شبکه یعنی e-mail را ارائه می‌دهد.

ولی وقتی صحبت برنامه‌های شرکت‌های متفرقه به میان می‌آید باید در عجین کردن آن با AD DS محتاط باشیم. به خاطر داشته باشید ساختار AD DS شبکه تا مدتهای مدید ثابت خواهد ماند. خوشایند نیست که محصولی را با دایرکتوری عجین کنیم و بعد از چند سال ببینیم شرکت منحل شده و extension های آن که به AD DS اضافه شده بلااستفاده مانده و زمان تکثیر با توجه به افزایش محتوای دایرکتوری افزایش یافته است.

برخلاف AD DS که فقط می‌تواند یک instance از دایرکتوری را روی سرور داشته باشد AD LDS می‌تواند چند instance روی سرور داشته باشد. همچنین برای کار کردن با AD LDS نیازی به عضویت گروههای Enterprise Administrators یا Schema Administrators نیست. AD LDS روی سرورهای غیر DC نصب شده و برای مدیریت فقط به دسترسی مدیریتی روی همان سیستم نیاز دارد. به همین دلیل می‌تواند به منظور فراهم کردن سرویس‌های برنامه کاربردی یا تایید هویت مبتنی بر وب در ناحیه DMZ به کار گرفته شود. AD LDS یکی از چهار فناوری Active Directory است که قدرت ما را در آن سوی دیواره آتش و داخل ابر اینترنت افزایش می‌دهد. (شکل ۱- ۱۴)



شکل ۱- ۱۴ AD LDS هم به صورت داخلی و هم خارجی از برنامه‌ها پشتیبانی می‌کند.

اهداف امتحانی در این فصل:

- پیکربندی نقش‌های سروری اضافی Active Directory
  - پیکربندی AD LDS

دروس این فصل:

- درس ۱: درک و نصب AD LDS
- درس ۲: پیکربندی و استفاده از AD LDS

قبل از شروع

برای ادامه موارد زیر باید انجام شده باشد:

- ویندوز سرور 2008 روی سیستم فیزیکی یا مجازی با نام SERVER01 نصب شده و DC دامنه contoso.com باشد.
- ویندوز سرور 2008 روی سیستم فیزیکی یا مجازی با نام SERVER03 نصب شده و عضو دامنه contoso.com باشد. این کامپیوتر میزبان AD LDS بوده که در تمرینات نصب خواهد شد. این دستگاه باید دارای درایو D باشد تا داده‌های AD LDS را ذخیره کند. فضای پیشنهادی برای این درایو 10 GB است.
- ویندوز سرور 2008 روی سیستم فیزیکی یا مجازی با نام SERVER04 نصب شده و عضو دامنه contoso.com باشد. این کامپیوتر برای پیکربندی تکثیر حوزه‌های AD LDS استفاده می‌شود. این دستگاه باید دارای درایو D باشد تا داده‌های AD LDS را ذخیره کند. فضای پیشنهادی برای این درایو 10 GB است.

درس ۱: درک و نصب AD LDS

هرچند AD LDS بر اساس همان کد AD DS طراحی شده ولی از آن خیلی ساده‌تر است. برای مثال وقتی AD LDS را روی سرور نصب می‌کنیم تغییراتی که AD DS هنگام نصب DC روی پیکربندی سرور ایجاد می‌کند ایجاد نمی‌کند. AD LDS فقط یک برنامه است و دیگر هیچ. وقتی نصب می‌شود نیازی به راه‌اندازی مجدد ندارد.

قبل از شروع باید بدانیم AD LDS از چه تشکیل شده است، چطور استفاده می‌شود و رابطه آن با دایرکتوری‌های AD DS چیست. بعد شروع به نصب سرویس کنیم.

بعد از این درس یاد می‌گیریم:

- چه موقع از AD LDS استفاده کنیم.
- آنرا روی سرور عضو دامنه نصب کنیم.
- انباره دایرکتوری AD LDS را پیدا و مشاهده کنیم.

زمان تقریبی : ۳۰ دقیقه

AD LDS چیست

همانند AD DS بر اساس پروتکل LDAP کار می‌کند و سرویس‌های بانک اطلاعاتی سلسله‌مراتبی دارد. دایرکتوری‌های LDAP برخلاف بانک‌های رابطه‌ای برای مقاصد خاصی بهینه شده‌اند و باید زمانی از آنها استفاده کنیم که نیاز به جستجوی سریع اطلاعات داریم. جدول ۱- ۱۴ تفاوت‌های اصلی بین دایرکتوری LDAP و بانک اطلاعاتی رابطه‌ای نظیر SQL Server را لیست می‌کند. این مقایسه به ما کمک می‌کند بدانیم چه موقع از دایرکتوری LDAP برای پشتیبانی از برنامه مبتنی بر بانک رابطه‌ای استفاده کنیم.

جدول ۱- ۱۴ مقایسه دایرکتوری‌های LDAP با بانک‌های رابطه‌ای

دایرکتوری LDAP	بانک‌های رابطه‌ای
خواندن و جستجوی سریع	نوشتن سریع در بانک
طراحی بانک سلسله مراتبی اغلب بر اساس DNS یا سیستم تحلیل نام X.500	طراحی داده به صورت ساخت یافته متکی به جداول دارای سطر و ستون. جداول می‌توانند به هم لینک داشته باشند.
به ساختار استاندارد schema متکی است. Schema که قابل توسعه است.	متکی به schema نیست
توزیع شده است و برای ثبات داده‌ای از تکثیر استفاده می‌کند.	داده‌ها متمرکز هستند.
امنیت در سطح شیء ارائه می‌شود.	امنیت در سطح سطر و ستون ارائه می‌شود.
به دلیل اینکه بانک توزیع‌شده است ثبات داده مطلق نیست حداقل تا زمان تکثیر.	به دلیل اینکه ورود داده تعاملی است ثبات داده‌ای مطلق است و همیشه تضمین شده است.
رکوردها قفل نمی‌شوند و دو کاربر مختلف همزمان می‌توانند روی رکوردها کار کنند. تداخل از طریق USN ها کنترل می‌شود.	رکوردها قفل می‌شوند و در آن واحد فقط توسط یک نفر قابل تغییر هستند.

این جدول راهنمای انتخاب بانک مناسب برای برنامه می‌باشد.

به علاوه AD LDS بر اساس AD DS کار می‌کند ولی همه ویژگی‌های AD DS را ندارد. جدول ۲- ۱۴ تفاوت ویژگی‌های AD LDS و AD DS را بیان می‌کند.

جدول ۲- ۱۴ مقایسه AD LDS با AD DS

ویژگی	AD	AD DS

	LDS	
حاوی بیش از یک instance روی سرور می‌تواند داشته باشد	√	
برای هر schema instance های مستقل دارد.	√	
روی کلاینت سیستم عامل نظیر ویستا یا سرور عضو دامنه 2008 اجرا می‌شود.	√	
روی DC ها اجرا می‌شود.	√	√
پارتیشن‌های دایرکتوری از X.500 برای تحلیل نام استفاده می‌کند.	√	
می‌تواند بدون راه‌اندازی مجدد نصب یا حذف شود.	√	
سرویس بدون راه‌اندازی مجدد می‌تواند متوقف یا استارت شود.	√	√
از Group Policy پشتیبانی می‌کند		√
حاوی GC می‌باشد		√
اشیائی نظیر کلاینت‌ها، سرورهای عضو دامنه و DC ها را مدیریت می‌کند		√
از trust بین دامنه‌ها و forest ها پشتیبانی می‌کند		√
با PKI ها و گواهی‌نامه‌های X.509 عجین شده و از آنها پشتیبانی می‌کند		√
از رکوردهای SRV برای پیدا کردن محل سرویس‌های دایرکتوری پشتیبانی می‌کند		√
از LDAP API پشتیبانی می‌کند	√	√
از ADSI API پشتیبانی می‌کند	√	√
از Messaging API (MAPI) پشتیبانی می‌کند		√
از امنیت سطح شیء و تفویض مدیریت پشتیبانی می‌کند	√	√
برای ثبات داده از تکثیر multimaster استفاده می‌کند	√	√
از توسعه schema و پارتیشن‌های دایرکتوری برنامه پشتیبانی می‌کند	√	√
می‌تواند از رسانه نصب قابل حمل یک replica بسازد	√	√
می‌تواند به منظور فراهم کردن دسترسی به شبکه ویندوز سرور حاوی واحدهای امنیتی باشد.		√
می‌تواند به منظور فراهم کردن دسترسی به سرویس‌های وب و برنامه، حاوی واحدهای امنیتی باشد.	√	√
با ابزارهای پشتیبان‌گیری ویندوز سرور 2008 عجین می‌شود.	√	√

همان‌طور که می‌بینید تفاوت‌ها و شباهت‌های بسیاری بین این دو وجود دارد. برای مثال دلیل آن مشخص است که چرا Exchange Server باید با AD DS عجین شود. دلیل آن این است که نیاز به دسترسی سرویس GC دارد. بدون آن کاربران e-mail نمی‌توانند دریافت‌کنندگان را پیدا کنند. چون AD LDS از GC پشتیبانی نمی‌کند سرور Exchange نمی‌تواند با آن کار کند.

در برخی موارد AD LDS عملکردی شبیه AD DS دارد. برای مثال می‌توانیم در محل‌های مختلف شبکه instanceهایی با replica های توزیع‌شده بسازیم و از تکثیر multimaster برای ثبات داده در کل شبکه استفاده کنیم. به طور خلاصه AD LDS نسخه سبک شده، قابل حمل و قابل انعطاف نسبت به سرویس دایرکتوری ارائه شده توسط AD DS است.

سناریوهای AD LDS

حالا که با ویژگی‌های AD LDS آشنا شدیم می‌توانیم سناریوهای مختلفی را با آن بررسی کنیم. وقتی خواستیم بین AD LDS و AD DS یکی را انتخاب کنیم به این سناریوها توجه می‌کنیم.

- وقتی برنامه‌های ما به دایرکتوری LDAP متکی باشند از AD LDS به جای AD DS استفاده می‌کنیم. اغلب می‌توانیم سرویس AD LDS را روی همان سرور برنامه قرار دهیم تا با سرعت بالا با داده دایرکتوری در ارتباط باشد. این کار باعث کاهش ترافیک تکثیر می‌شود. به علاوه می‌توانیم AD LDS instance را هنگام توزیع با برنامه همراه کنیم. اگر برای مثال برنامه منابع انسانی داشته باشیم و برای دسترسی کاربران به محتوای خاصی سیاست بر این باشد که کاربر دارای خصیصه خاصی باشد می‌توانیم این خصیصه‌ها را با سیاست‌ها در AD LDS ذخیره کنیم.

- استفاده از AD LDS در این سناریو داده‌های اضافی کاربر را بدون تغییر AD DS schema فراهم می‌کند. برای مثال اگر یک برنامه متمرکز داشته باشیم که تصویر همه کارمندان سازمان را نگهداری کرده و با حساب AD DS کاربر عجین کند تصاویر را می‌توانیم در AD LDS ذخیره کنیم. با این کار این تصاویر با حساب کاربران در AD DS عجین شده و به دلیل اینکه در AD LDS ذخیره می‌شوند با داده‌های دیگر AD DS تکثیر نمی‌شوند.

- استفاده از AD LDS به عنوان سرویس تایید هویت برای برنامه‌های مبتنی بر وب نظیر Microsoft SharePoint Portal Server در شبکه DMZ یا اکسترانت یکی دیگر از سناریوهای ممکن است. AD LDS می‌تواند پرس‌وجوی خود را از میان دیواره آتش به ساختار AD DS داخلی بفرستد تا اطلاعات حساب کاربری را دریافت کرده و آنرا به صورتی مطمئن در شبکه DMZ ذخیره کند. این کار ما را از توزیع AD DS یا DC در شبکه DMZ بی‌نیاز می‌کند. ناگفته نماند از AD FS نیز برای فراهم کردن این دسترسی می‌توانیم استفاده کنیم. AD FS در فصل ۱۷ شرح داده خواهد شد.

- کار یکپارچه‌سازی انباره‌های هویت مختلف را در یک انباره دایرکتوری منفرد انجام می‌دهد. با استفاده از یک سرویس متادایرکتوری قادر خواهیم بود داده‌های منابع مختلف را دریافت کرده و آنرا در AD LDS یکپارچه کنیم. Microsoft Identity Integration Server (MIIS) ، Microsoft Identity Lifecycle Manager (MILM) یا Identity Integration Feature Pack (IIFP) مثال‌هایی از سرویس متادایرکتوری می‌باشند. MIIS و MILM از تهیه داده‌ها از منابع مختلفی نظیر AD DS forest ، بانک‌های اطلاعاتی سرور SQL، سرویس‌های LDAP شرکت‌های متفرقه و دیگر منابع پشتیبانی می‌کند. IIFP نیز زیرمجموعه MIIS بوده و از عجین شدن داده‌ها بین AD DS ، AD LDS و سرور Exchange پشتیبانی می‌کند. استفاده از این راه‌حل‌ها با توجه به وجود یک مرکز داده متمرکز بار کاری مدیریتی را کاهش می‌دهد.

- از برنامه‌های مختص بخش‌های سازمانی نیز پشتیبانی می‌کند. در برخی موارد بخش‌های سازمان ممکن است به اطلاعات هویتی دیگری نیاز داشته باشند که ربطی به بخش‌های دیگر سازمان نداشته باشد. با عجین کردن این اطلاعات در AD LDS آن بخش بدون تاثیرگذاری روی سرویس دایرکتوری بخش‌های دیگر به آن دسترسی پیدا خواهد کرد.

- از برنامه‌های توزیع شده نیز پشتیبانی می‌کند. اگر برنامه توزیع‌شده باشد و نیاز به دسترسی به داده‌های محل‌های مختلف داشته باشد AD LDS قابلیت تکثیر multimaster را همانند AD DS فراهم می‌کند.

- می‌توانیم برنامه‌های دایرکتوری قدیمی را به AD LDS منتقل کنیم. اگر سازمان دارای برنامه‌های قدیمی باشد که به دایرکتوری LDAP وابسته است می‌توان داده‌ها را به AD LDS منتقل کرده و بر اساس فناوری‌های دایرکتوری Active Directory استانداردسازی کرد.

- از توسعه نرم‌افزاری محلی پشتیبانی می‌کند. به دلیل اینکه AD LDS می‌تواند روی کلاینت نصب شود می‌توانیم دایرکتوری‌های قابل حمل را در اختیار تیم توسعه نرم‌افزار قرار دهیم. مدیریت توسعه نرم‌افزاری با AD LDS خیلی ساده‌تر از AD DS است.

- در ارزیابی برنامه‌های تجاری مبتنی بر دایرکتوری به جای AD DS ترجیح ما بر وابستگی به AD LDS یا نسخه قدیمی آن ADAM است. توزیع برنامه‌های تجاری با دایرکتوری‌های قابل حمل ساده‌تر بوده و نسبت به برنامه‌هایی که schema دایرکتوری NOS ما را برای همیشه تغییر می‌دهند تاثیر کمتری روی شبکه می‌گذارند.

این سناریوها استفاده‌های ممکن از AD LDS را بیان می‌کند.
همان‌طور که می‌بینید AD LDS نسبت به AD DS قابلیت حمل و انعطاف بیشتری دارد. وقتی به تغییر schema در AD DS فکر می‌کنیم به جای آن به بهتر است به AD LDS فکر کنیم.

نصب AD LDS

AD LDS به عنوان بخشی از ویندوز سرور 2008 هم روی نصب کامل و هم Server Core نصب و پیکربندی می‌شود. به علاوه AD LDS بهترین انتخاب برای مجازی‌سازی از طریق Hyper-V ویندوز سرور 2008 است. با توجه به نیازمندی‌های کم در ماشین‌های مجازی با سیستم عامل ویندوز سرور 2008 اجرا می‌شود مگر اینکه برنامه عجین شده با آن نیازمند نصب روی ماشین فیزیکی باشد.
از طرفی تا جایی که امکان دارد از نصب آن روی DC بپرهیزید. اگرچه AD LDS همکاری خوبی با نقش DC یا حتی RODC دارد بهتر است DC به عنوان نقش خاص شبکه فقط با سرویس DNS عجین شود نه سرویس دیگر. خود DC هم گزینه مناسبی برای نصب روی ماشین مجازی می‌باشد.
پیشنهاد می‌شود AD LDS در سناریوهایی که امنیت بالایی دارند پیاده‌سازی شود. مثالی از این مورد زمانی است که به اجرای سرویس دایرکتوری تایید هویت در اکسترانت یا DMZ داریم. استفاده از نصب Server Core در این محیط به کاهش سطح نفوذپذیری سرور از بیرون منجر می‌شود.

تشخیص نیازمندی‌های AD LDS

نیازمندی‌های نصب AD LDS شامل موارد زیر است:

- سیستم عامل مناسب مانند ویندوز سرور 2008 نسخه Standard، Enterprise یا Datacenter .
- حساب با دسترسی administrator محلی

حذف AD LDS نیازمند دو عمل است:

- ابتدا از طریق Programs And Features همه instanceهای AD LDS را که پس از نصب نقش ساخته شده حذف می‌کنیم
- بعد با استفاده از Server Manager نقش AD LDS را حذف می‌کنیم.

نصب AD LDS روی Server Core

نصب AD LDS خیلی شبیه به نصب AD DS است. ابتدا باید نقش سروری را نصب کنیم. سپس instanceهای AD LDS را بسازیم. نصب AD LDS روی ویندوز 2008 با نصب کامل در تمرینات شرح داده خواهد شد. ولی نصب روی Server Core به شرح زیر است:

۱. با کاربر administrator محلی به ویندوز سرور 2008 وارد می‌شویم.
۲. نام سرویس AD LDS را با دستور زیر تعیین می‌کنیم:

```
oclist | more
```

۳. در ادامه دستور زیر را صادر می‌کنیم:

```
start /w ocsetup DirectoryServices-ADAM-ServerCore
```

نام نقش حساس به متن است. استفاده از دستور start /w باعث می‌شود خط فرمان تا پایان نصب نقش ادامه می‌یابد.
اگر دستور oclist یک بار دیگر اجرا شود می‌بینیم که نقش AD LDS به سرور افزوده شده است. نیز برای مشاهده فایل‌های جدید AD LDS به مسیر %SystemRoot%\ADAM مراجعه می‌کنیم. حالا سرور آماده است instanceهای AD LDS را میزبانی کند.

تمرینات نصب AD LDS

در این تمرینات نقش AD LDS را بر روی یک سرور که روی آن ویندوز سرور 2008 بطور کامل نصب شده ، نصب می کنیم سپس برای فهمیدن اینکه کدام فایلها نصب شده اند محتویات پوشه نصب را بررسی می کنیم.

تمرین اول نصب AD LDS

در این تمرین نقش سرور AD LDS را نصب خواهیم کرد.

۱- مطمئن می شویم که SERVER01.contoso.com ، فعال بوده و سرورهای SERVER03.contoso.com و SERVER04.contoso.com را که عضو دامنه هستند راه اندازی می کنیم

۲- با اعتبار Contoso\Administrator وارد SERVER03.contoso.com می شویم

برای کار کردن با AD LDS نیازی به داشتن حساب مدیر دامنه نیست ، چون هر نصب AD LDS مستقل از AD DS می باشد به همین دلیل برای کار کردن با آن داشتن حساب مدیر شبکه محلی کافی است اما استفاده از حساب مدیر دامنه برای اهداف این تمرین قابل قبول تر است

۳- در Server Manager ، روی گره Role راست کلیک کرده و Add Roles را انتخاب می کنیم

۴- صفحه Before You Begin را مرور کرده و روی Next کلیک می کنیم

۵- در کادر محاوره ای Select Server Roles ، گزینه Active Directory Lightweight Directory Services را انتخاب کرده و روی Next کلیک می کنیم

۶- اطلاعت پنجره Active Directory Lightweight Directory Services را مرور کرده و روی Next کلیک می کنیم

۷- انتخابمان را تایید کرده و سپس روی Install کلیک می کنیم

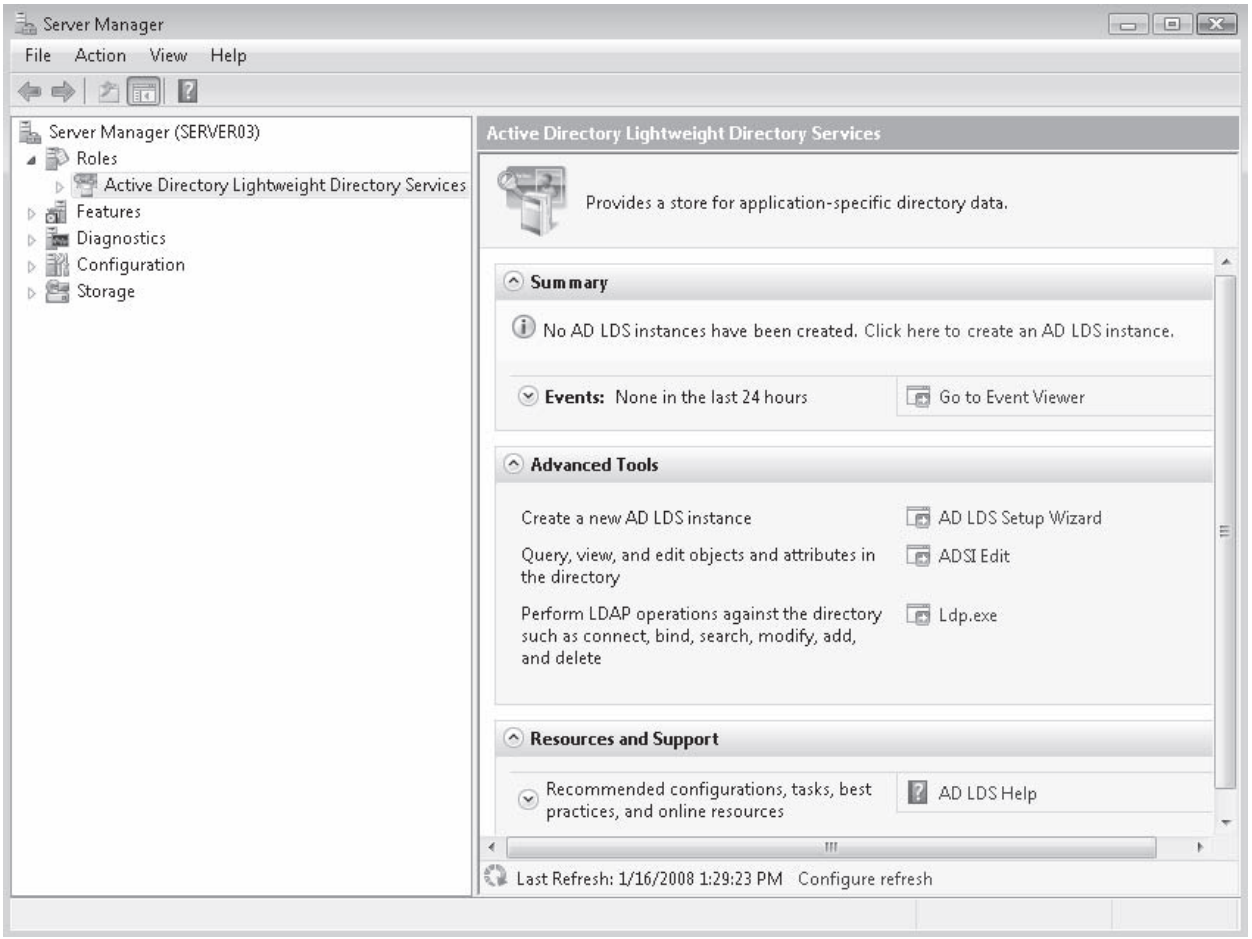
۸- نتایج نصب را مرور کرده و سپس روی Close کلیک می کنیم

۹- عملیات فوق را روی SERVER04.contoso.com تکرار می کنیم

AD LDS روی هر دو سرور نصب شده است.

با نصب AD LDS ضمن نصب خود سرویس انباره دایرکتوری با نام Adamntds.dit نیز ساخته می شود که محل آن در پوشه %SystemRoot%\Adam می باشد. همچنین برای پیکربندی و مدیریت AD LDS ابزاری در اختیار ما می گذارد.

پس از اینکه نصب تمام شد نقش در Server Manager نمایش داده می شود. (شکل ۲- ۱۴)



شکل ۲- ۱۴ نمایش نقش AD LDS در کنسول Server Manager

تمرین دوم مرور فایلهای نصب AD LDS

در این تمرین به بررسی فایلهایی که فرآیند نصب AD LDS بر روی سرور نصب کرده است می پردازیم

۱- با اعتبار Contoso\Administrator وارد SERVER03.contoso.com می شویم.

۲- از منوی Start روی Computer راست کلیک کرده و Explore را انتخاب می کنیم

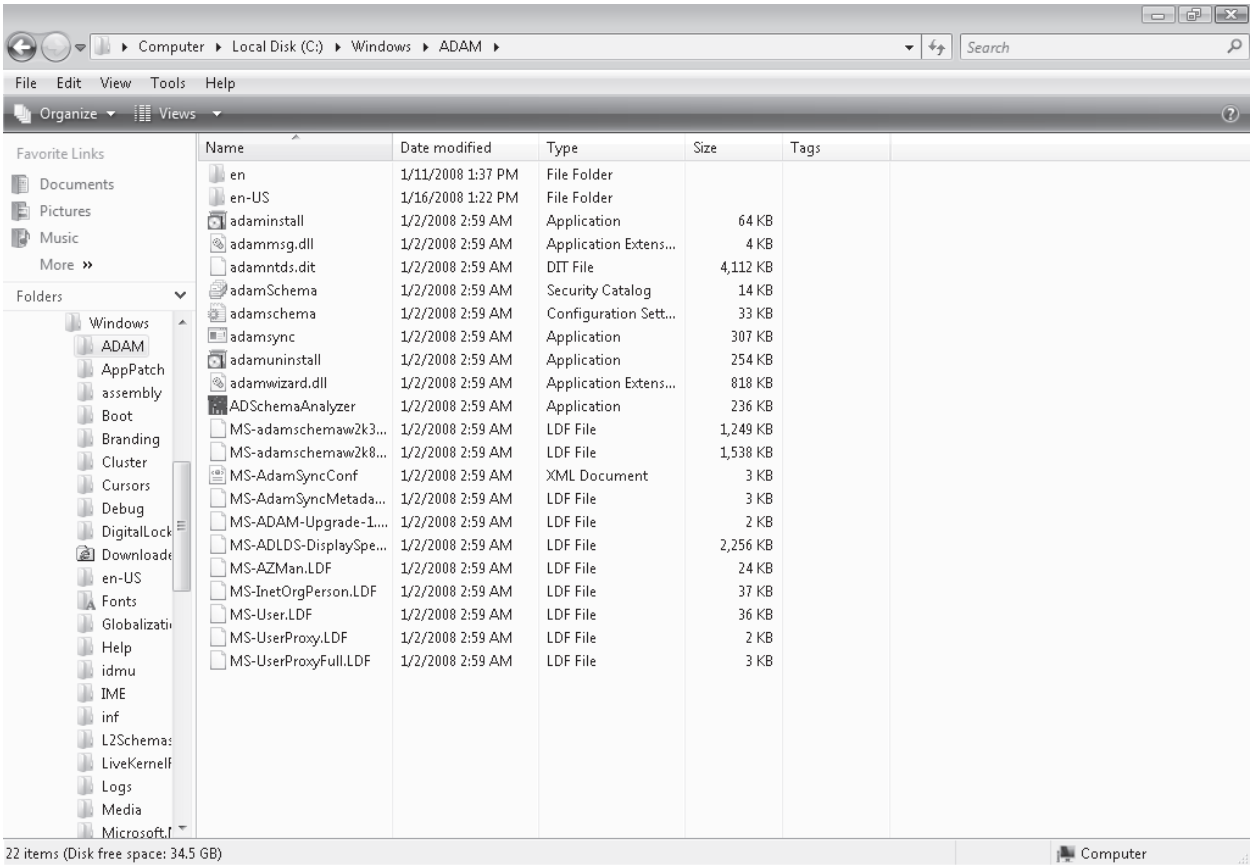
۳- وارد پوشه %SystemRoot%\ADAM می شویم.

۴- فایلهایی که توسط فرآیند نصب AD LDS ساخته شده اند را مرور می کنیم.

در یک نصب کامل ویندوز سرور 2008 ، AD LDS پوشه ADAM را با بیست فایل و دو پوشه درون آن درست می کند، این دو پوشه شامل اطلاعات محلی سازی (localization) می باشند. همانطور که در شکل ۳-۱۴ نشان داده شده است پوشه ADAM شامل فایلهای زیر می باشد:

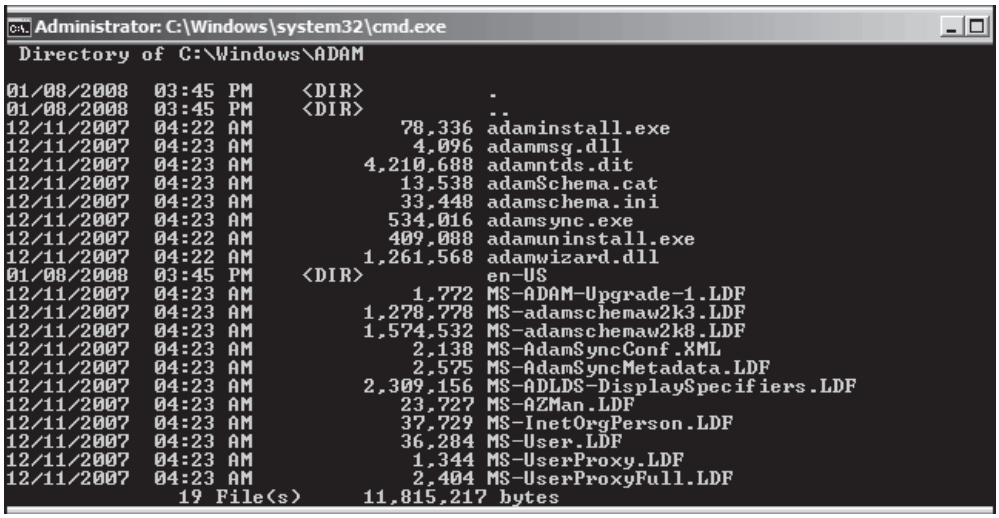
- فایلهای برنامه AD LDS شامل فایلهای .ini, .cat, .exe, .dll,و .xml
- انباره دایرکتوری AD LDS ، فایل Adamntds.dit
- فایلهای Lightweight directory format (.ldf)

در درس دوم و به هنگام پیکربندی AD LDS با این نوع فایلها کار خواهیم کرد.



شکل ۳- ۱۴ AD LDS در پوشه %Systemroot%Adam نصب شده و بانک اطلاعاتی AD LDS را می سازد.

نصب AD LDS روی Server Core شامل همان فایل‌ها و پوشه‌هایی که در نصب کامل است نمی‌باشد. Server Core فقط یک پوشه برای محلی‌سازی ساخته در حالی که نصب کامل دوتا پوشه می‌سازد. به علاوه ابزاری که در Server Coreوجود ندارد Active Directory Schema Analyzer می‌باشد. (شکل ۴- ۱۴)



شکل ۴- ۱۴ نصب AD LDS روی Server Core فقط حاوی ۱۹ فایل و یک پوشه است.

خلاصه درس

- همان‌طور که از اسم آن می‌توان حدس زد AD LDS یک نسخه سبک شده AD DS است. AD LDS از همه ویژگی‌های AD DS پشتیبانی می‌کند به جز قابلیت‌های سیستم عامل شبکه. به این ترتیب یک سرویس دایرکتوری است که با برنامه‌ها گره خورده و از نیازهای آنان برای پیکربندی سفارشی و سرویس تایید هویت در محیط‌های ناامن مانند شبکه‌های Perimeter پشتیبانی می‌کند.

- نیازمندی‌های نصب AD LDS خیلی ساده هستند. فقط به یک سرور که ویندوز سرور 2008 روی آن نصب شده باشد نیاز داریم. این سرور می‌تواند مستقل باشد یا عضو دامنه باشد حتی DC باشد هرچند توصیه می‌شود سرویس DC به تنهایی روی سرور کار کند.
- برای نصب AD LDS نقش را در ویزارد Add Roles انتخاب می‌کنیم. فرایند نصب نسبت به بقیه نقش‌ها خیلی ساده است.
- برای حذف AD LDS باید همه instance ها توسط Program And Features پاک شود بعد نقش را در Server Manager حذف کنیم.

سئوالات پایان درس

۱. فرض کنید مدیر شبکه contoso.com هستیم. امروز صبح رئیس ما دستوری جدید می‌دهد. ما باید SERVER04 را برای سرویس جدیدی آماده کنیم. این سرور در حال حاضر میزبان AD LDS Instance ها می‌باشد. ما باید این سرویس را حذف کنیم. با کاربر مدیر شبکه محلی به سرور وارد می‌شویم و پنجره خط فرمان elevated را باز می‌کنیم. دستور ocsetup را با سوئیچ uninstall/ به کار می‌بریم ولی کار نمی‌کند. کدام یک از موارد زیر برای حل مشکل استفاده می‌شو؟
   A. باید سرور را راه‌اندازی مجدد کنیم
   B. از Server Manager برای حذف همه AD LDS instance ها استفاده کنیم.
   C. ابتدا باید همه instance ها را با استفاده از Program And Features حذف کنیم و بعد دستور ocsetup /uninstall را از خط فرمان اجراکنیم.
   D. از دستور oclist برای بررسی شکل فرمان استفاده کرده و دستور ocsetup را به شکل درست اجرا می‌کنیم.

درس ۲: پیکربندی و استفاده از AD LDS

حالا که AD LDS نصب شده است می‌توانیم کار با آنرا شروع کنیم. اولین مرحله آشنایی با مجموعه ابزار AD LDS می‌باشد. بعد از اینکه یاد گرفتیم کدام ابزار برای مدیریت مناسب است شروع به ساخت اولین instance می‌کنیم. بعد از ساخت instanceها باید امنیت آنها را تامین کنیم. بعد به سراغ ساخت replica های این instanceها می‌رویم.

بعد از این درس می‌توانیم:

- AD LDS instance بسازیم.
- با ابزارهای AD LDS کار کنیم.
- با پارتیشن‌های برنامه کار کنیم.
- تکثیر بین instanceهای AD LDS را مدیریت کنیم.

زمان تقریبی: ۳۰ دقیقه

کار با ابزارهای AD LDS

برخی از ابزارها برای ما آشنا هستند چراکه برای مدیریت AD DS نیز استفاده می‌شدند. جدول ۳- ۱۴ هر کدام از این ابزارها و هدف آنها را لیست می‌کند.

جدول ۳- ۱۴ ابزارهای AD LDS و AD DS

نام ابزار	مورد استفاده	محل
ابزار Active Directory Schema	Schema را برای instanceهای AD LDS ویرایش می‌کند. باید از دستور Regsvr32.exe برای رجیستر کردن Schmmgnt.dll استفاده کنیم.	MMC سفارشی
Active Directory Sites and Services	حوزه‌های تکثیر را برای instanceهای AD LDS مدیریت و پیکربندی می‌کند.	گروه برنامه‌های Administrative Tools

AD LDS Setup	instanceهای AD LDS می‌سازد.	گروه برنامه‌های Administrative Tools
ADAMInstall.exe	ابزار خط فرمان برای ساخت AD LDS instance می‌باشد.	%SystemRoot% \ADAM
ADAMSync.exe	ابزار خط فرمان برای یکسان‌سازی داده‌های AD DS forest با AD LDS instance می‌باشد. AD LDS instance ابتدا باید AD DS schema را به روز کند.	%SystemRoot% \ADAM
ADAMUninstall.exe	ابزار خط فرمان برا ی حذف instanceهای AD LDS است.	%SystemRoot% \ADAM
ADSchemaAnalyzer.exe	ابزار خط فرمان برای کپی محتوای schema از AD DS به AD LDS یا از یک AD LDS instance به دیگری می‌باشد. از کپی‌های schema دایرکتوری شرکت‌های متفرقه نیز پشتیبانی می‌کند.	%SystemRoot% \ADAM
ADSI Edit	محتوای AD LDS را از طریق ADSI مدیریت می‌کند.	گروه برنامه‌های Administrative Tools
CSVDE.exe	داده‌ها را به instanceهای AD LDS منتقل می‌کند.	خط فرمان
DSACLS.exe	ACL های اشیاء AD LDS را کنترل می‌کند.	خط فرمان
DSAMain.exe	فایل‌های پشتیبان Active Directory (.dit) را به منظور بررسی محتویات mount می‌کند.	خط فرمان
DSDBUtil.exe	کار نگهداری بانک اطلاعاتی، پیکربندی پورت‌های AD LDS و مشاهده instanceهای موجود را انجام می‌دهد.	خط فرمان
Dcdiag.exe	instanceهای AD LDS را بررسی می‌کند. با سوئیچ /n:NamingContext باید به کار رود.	خط فرمان
DSMgmt.exe	از پارتیشن برنامه و مدیریت سیاست AD LDS پشتیبانی می‌کند.	خط فرمان
Event Viewer	برای ممیزی تغییرات AD LDS و ثبت مقادیر قدیمی و جدید اشیاء و خصیصه‌ها به کار می‌رود.	گروه برنامه‌های Administrative Tools
LDAP Data Interchange Format (LDIF) Files	نصب AD LDS به طور پویا فایل‌های LDIF (.ldp) را در طول ساخت instance منتقل می‌کند.	%SystemRoot% \ADAM
LDIFDE.exe	انتقال داده به instanceهای AD LDS	خط فرمان
LDP.exe	محتوا یا instanceهای AD LDS را از طریق LDAP ویرایش می‌کند.	خط فرمان
Ntdsutil.exe	instanceهای AD LDS را مدیریت می‌کند ولی باید AD DS نصب شده باشد. (که پیشنهاد نمی‌شود و به جای آن می‌توان از دستور DSDBUtil.exe استفاده کرد.)	خط فرمان
RepAdmin.exe	تکثیر را تحلیل می‌کند تا مشکلات بالقوه را تشخیص دهد.	خط فرمان
Server Manager	instanceهای AD LDS موجود را مدیریت می‌کند.	گروه برنامه‌های Administrative Tools
Windows Server Backup	از instanceهای AD LDS و محتوای آنها پشتیبان تهیه کرده و بازیابی می‌کند.	گروه برنامه‌های Administrative Tools

ساخت AD LDS instance

نصب نقش AD LDS خیلی شبیه AD DS است. ابتدا AD LDS binaries نصب شده و سپس instanceهای AD LDS ساخته می‌شود.

آماده‌سازی شرایط برای ساخت AD LDS instance

ویزارد Active Directory Lightweight Directory Services Setup برای ساخت AD LDS instance به کار می‌رود. ولی قبل از آن باید موارد زیر را آماده کنیم:

- یک درایو مخصوص داده برای سرور بسازیم. به دلیل اینکه این سرور میزبان انباره دایرکتوری خواهد بود آنرا روی درایوی جدا از سیستم عامل قرار می‌دهیم.
- نامی برای instance انتخاب می‌کنیم.
- پورت ارتباط با instance را مشخص می‌کنیم. AD LDS و AD DS هر دو از یک پورت برای ارتباط استفاده می‌کنند. این پورت‌های عبارتند از پورت LDAP (389) و LDAP over the Secure Sockets Layer (SSL) یا Secure LDAP (636). AD DS از از دو پورت اضافی به شماره‌های 3268 برای استفاده از LDAP برای دسترسی به GC و 3269 که از Secure LDAP برای دسترسی به GC استفاده می‌کند. تشابه پورت‌ها نیز دلیل دیگری برای عدم استفاده از یک سرور به منظور ارائه هر دو سرویس می‌باشد. وقتی ویزارد پورت‌های 389 و 636 را استفاده شده می‌بیند شماره پورت‌های 50000 و 50001 را برای هر کدام پیشنهاد کرده و از پورت 50000 برای بقیه instanceها استفاده می‌کند.
- نام پارتیشن برنامه Active Directory مورد نظر برای استفاده در instance را مشخص می‌کنیم. باید از نام DN برای ساخت پارتیشن استفاده شود. برای مثال CN=AppPartition1,DC=Contoso,DC=com . بسته به نحوه استفاده از instance ممکن است به پارتیشن برنامه نیاز پیدا کنیم. پارتیشن‌های برنامه حوزه تکثیر را برای یک انباره دایرکتوری کنترل می‌کنند. برای مثال وقتی داده DNS با دایرکتوری عجین می‌شود AD DS یک پارتیشن برنامه می‌سازد که داده DNS را در دسترس DC های مناسب قرار دهد. پارتیشن‌های برنامه از به یکی از صور زیر ساخته می‌شود. وقتی instance ساخته می‌شود، وقتی برنامه‌ای که با instance عجین شده نصب می‌شود یا وقتی پارتیشن به صورت دستی با ابزار LDP.exe ساخته می‌شود. اگر برنامه توانایی ساخت خودکار پارتیشن‌های برنامه را نداشته باشد آنرا از طریق ویزارد می‌سازیم.
- نیاز به یک حساب برای اجرای instance داریم. امکان استفاده از حساب Network Service وجود دارد ولی اگر قصد داریم چندین instance ایجاد کنیم بهتر است حساب‌های نام‌گذاری شده برای هر instance استفاده کنیم. در این مورد به راهنمای زیر توجه داشته باشید:
  - اگر در دامنه کار می‌کنیم باید یک حساب تحت دامنه بسازیم. درغیر این‌صورت از یک حساب محلی استفاده می‌کنیم.
  - همان نامی که به instance داده‌ایم به حساب نیز اختصاص می‌دهیم.
  - کلمه عبور پیچیده برای این حساب در نظر می‌گیریم.
  - کادر User Cannot Change Password را علامت می‌زنیم.
  - کادر Password Never Expires را علامت می‌زنیم.

- در Local Security Policy حق Log On As A Service User را به کامپیوتر میزبان instance اعطاء می‌کنیم.
- در Local Security Policy حق Generate Security Audits را به کامپیوتر میزبان instance اعطاء می‌کنیم.

- یک گروه که حاوی کاربران دارای حق مدیریت روی instance باشد می‌سازیم. بهترین راه برای اعطاء مجوز استفاده از گروه است حتی اگر دارای یک عضو باشد. اگر در دامنه کار می‌کنیم گروه دامنه می‌سازیم. وگرنه یک گروه محلی می‌سازیم. نام گروه را مشابه نام instance انتخاب می‌کنیم. حساب خود و حساب سرویسی را که قبلا ساختیم به گروه اضافه می‌کنیم.

- فایل‌های LDIF را در مسیر %SystemRoot%\ADAM قرار می‌دهیم. اطلاعات این فایل‌ها در حین ساخت instance منتقل می‌شود. انتقال فایل‌های LDIF، schema مربوط به instance را توسعه می‌دهد. برای مثال برای یکسان‌سازی AD DS با AD LDS می‌توانیم فایل MSAdamSyncMetadata.ldf انتقال دهیم. اگر برنامه ما نیاز به تغییرات خاص schema داشته باشد فایل LDIF را ساخته و آنرا هنگام ساخت instance منتقل می‌کنیم.البته بعد از ساخت instance نیز می‌توانیم فایل‌های LDIF را منتقل کرد. فایل‌های LDIF پیش‌فرض در جدول ۴- ۱۴ لیست شده‌اند.

جدول ۴- ۱۴ فایل‌های پیش‌فرض AD LDS LDIF

نام فایل	هدف
MS-ADAM-Upgrade-1.ldf	برای ارتقاء AD LDS schema به آخرین نسخه
MS-adamschemaw2k3.ldf	پیش‌نیاز یکسان‌سازی یک instance با Active Directory در ویندوز سرور 2003 می‌باشد.
MS-adamschemaw2k8.ldf	پیش‌نیاز یکسان‌سازی یک instance با Active Directory در ویندوز سرور 2008 می‌باشد.
MS-AdamSyncMetadata.ldf	برای یکسان‌سازی داده بین یک AD DS forest و AD LDS instance از طریق ADAMSync مورد نیاز است.
MS-ADLDS-DisplaySpecifiers.ldf	برای عملیات ابزار Active Directory Sites and Services مورد نیاز است.
MS-AZMan.ldf	برای پشتیبانی از Windows Authotization Manager مورد نیاز است.
MS-InetOrgPerson.ldf	برای ساخت کلاس و خصیصه‌های کاربر inerOrgPerson مورد نیاز است.
MS-User.ldf	برای ساخت کلاس و خصیصه‌های کاربر مورد نیاز است.
MS-UserProxy.ldf	برای ساخت یک کلاس userProxy مورد نیاز است.
MS-UserProxyFull.ldf	برای ساخت یک کلاس کامل userProxy مورد نیاز است. ابتدا باید محتوای فایل MS-UserProxy.ldf را انتقال دهیم.

با این آیتم‌ها دیگر برای ساخت instance آماده خواهیم شد. حساب کاربری که استفاده می‌کنیم باید دارای حق مدیریتی محلی داشته باشد. دو راه برای ساخت instance وجود دارد. اول از طریق Active Directory Lightweight Services Setup Wizard و دوم از طریق خط فرمان. استفاده از ویزارد در تمرینات همین درس کار می‌شود و خط فرمان نیز در بخش‌های بعدی شرح داده خواهد شد.

ساخت AD LDS instance به صورت غیرحضوری

برای مثال برای ساخت instance روی Server Core باید از این روش استفاده کنیم زیرا رابط گرافیکی برای اجرای ویزارد وجود ندارد. همچنین در مواردی که به ساخت instance برای برنامه‌های توزیع‌شده روی چندین سرور نیاز داریم ساخت غیرحضوری مفید می‌باشد.

پوشه %SystemRoot%\ADAM حاوی یک دستور دیگر است AdamInstall.exe که به منظور نصب غیرحضوری instance اجرا می‌شود. مانند دستور Dcpromo.exe این دستور نیز به فایل متنی به عنوان ورودی روند ساخت instance نیاز دارد. این دستور را می‌توان هم روی نصب کامل و هم Server Core اجرا کرد. برای شروع روش ساخت این فایل متنی را یاد می‌گیریم.

۱. برنامه Notepad را اجرا می‌کنیم.

۲. متن فایل پاسخ را تایپ می‌کنیم که حاوی آیتم‌های زیر است:

[ADAMInstall]
InstallType=Unique
InstanceName=*InstanceName*
LocalLDAPPortToListenOn=*PortNumber*
LocalSSLPortToListenOn=*PortNumber*
NewApplicationPartitionToCreate=*PartitionName*
DataFilesPath=*D:\ADAMInstances\InstanceName\Data*
LogFilesPath=*D:\ADAMInstances\InstanceName\Data*
ServiceAccount=*DomainorMachineName\AccountName*
ServicePassword=*Password*
Administrator=*DomainorMachineName\GroupName*
ImportLDIFFiles=’LDIFFilename1’ ‘LDIFFilename2’ ‘LDIFFilename3’
SourceUserName=*DomainorMachineName\AccountName*
SourcePassword=*Password*

به جای همه کلمات با خط کج (*Italic*) مقادیر مناسب درج می‌کنیم. از فایل باید محافظت کنیم به دلیل اینکه کلمه عبور در آنها درج شده و به صورت متن عادی (بدون رمز) است. به محض استفاده از فایل توسط ابزار ساخت AD LDS instance کلمه عبور پاک می‌شود.

۳. فایل را در پوشه %SystemRoot%\ADAM ذخیره می‌کنیم و نام آنرا با نام instanceای که بعدا قرار است ساخته شود یکی می‌گیریم.

۴. Notepad را می‌بندیم.

حالا آماده ساخت instance هستیم.

۱. پنجره خط فرمان elevated را باز می‌کنیم.

۲. در خط فرمان به مسیر %SystemRoot%\ADAM دستور زیر را تایپ می‌کنیم و کلید Enter را می‌زنیم.

cd windows\adam

۳. دستور زیر را تایپ می‌کنیم. اگر نام فایل دارای فاصله باشد آنرا در گیومه قرار می‌دهیم.

adaminstall /answer:filename.txt

۴. پنجره خط فرمان را می‌بندیم.

instance آماده است. بررسی می‌کنیم که فایل‌های instance در محل مقصد ساخته شده‌اند یا نه.

انتقال instance قبلی LDAP به AD LDS

ما می‌توانیم دایرکتوری‌های موجود LDAP را به AD LDS منتقل کنیم یا instanceهای ADAM را به AD LDS ارتقاء دهیم. این کار با انتقال محتویات instance قبلی به instance جدید AD LDS انجام می‌شود.

انتقال داده هم زمان ساخت instance و هم پس از آن امکان‌پذیر است. هر دو فرایند رویکردی یکسان دارند زیرا هر دو از فایل‌های LDIF با پسوند ldf. استفاده می‌کنند. اگر انتقال پس از ساخت انجام شود باید از دستور LDIFDE.exe استفاده شود. به خاطر داشته باشید ابتدا باید داده‌ها را از instance قبلی استخراج کرده و آنرا در یک فایل LDIF ذخیره کنیم بعد کار انتقال را انجام دهیم. دستور LDIFDE کار استخراج محتویات instanceهای قدیمی را انجام می‌دهد. به خاطر داشته باشید برای انجام این کارها ما به حقوق مدیریتی روی سیستم محلی و حقوق مدیریتی روی instance نیاز داریم. همچنین از پنجره‌های خط فرمان elevated استفاده کنیم. برای انجام این کار از ساختار زیر استفاده می‌کنیم:

Ldifde -f filename -s servername:portnumber -m -b username domainname password

در ساختار دستوری بالا filename نام فایلی است که باید ساخته شود (در صورت وجود فاصله در نام فایل آنرا در گیومه قرار می‌دهیم.) servername نام سروری است که میزبان instance است. Portnumber نام پورت ارتباطی است. Username, domainname و password اعتبار مدیر جهت مدیریت instance است.

به منظور انتقال داده به instance جدید دستور مشابه زیر را به کار می‌بریم:

ldifde -i -f filename -s servername:portnumber -m -b username domainname password

به یاد داشته باشید که برای انتقال کلمه عبور از instance قبلی باید از سوئیچ h– استفاده کنیم. این سوئیچ همه کلمات عبور را با استفاده از SASL رمزنگاری می‌کند.

کار با instanceهای AD LDS

از بین ابزارهای جدول ۳- ۱۴ مفیدترین آنها ابزارهای گرافیکی مانند ADSI Edit ، LDP.exe ، ابزار Schema و Active Directory Sites and Services است. این ابزارها چگونگی نمایش و ویرایش محتویات instance را کنترل می‌کنند. ابزارهای خط فرمان برای خودکارسازی فرایندها و ورود داده‌ها به instanceهای AD LDS مفید می‌باشد.

استفاده از ADSI Edit برای کار با instanceها

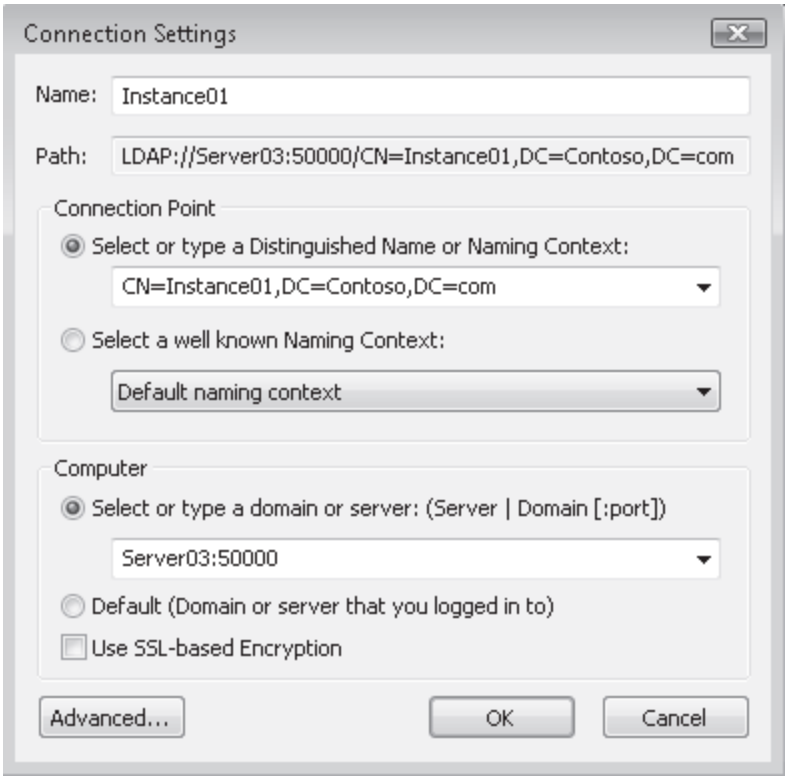
این یک ابزار مدیریت عمومی instanceهای AD LDS است. هر گاه خواسته باشیم با instanceای کار کنیم باید ابتدا به آن متصل شویم. باید روی آن instance دسترسی مدیریتی داشته باشیم تا بتوانیم روی آن کار کنیم. مراحل زیر را دنبال کنید:

۱. از گروه برنامه‌های Administrative Tools ابزار ADSI Edit را اجرا می‌کنیم.

۲. در ساختار درختی روی ADSI Edit کلیک راست می‌کنیم و Connect To را انتخاب می‌کنیم. کادر محاوره‌ای Connection Settings باز می‌شود. مقادیر زیر را همانند شکل ۵- ۱۴ تایپ می‌کنیم:

- Name : نام instance برای اتصال به آن
- Connection Point : گزینه Select Or Type A Distinguished Name Or Naming Context را انتخاب کرده و نام instance DN را وارد می‌کنیم.
- Computer: گزینه Select Or Type A Domain Or Server را انتخاب کرده و نام سرور را به همراه شماره پورت آن تایپ می‌کنیم. مثلا SERVER03:50000
- Computer: کادر Use SSL-Based Encryption را در صورتی که از یک پورت Secure LDAP استفاده می‌کنیم علامت می‌زنیم.

۳. روی OK کلیک می‌کنیم. حالا به instance متصل شده‌ایم. همه گره‌ها را باز می‌کنیم تا محتویات instance را ببینیم. منوی کلیک راست را باز می‌کنیم تا عملیات مختلف ADSI Edit را instanceهای AD LDS ببینیم.



شکل ۵- ۱۴ اتصال به AD LDS instance با ADSI Edit

حالا نوبت ساخت و مدیریت اشیاء در instance است. مراحل زیر را دنبال کنید:

۱. روی نام DN پارتیشن برنامه کلیک راست کرده و New و بعد Object را انتخاب می‌کنیم. کادر محاوره‌ای Create Object باز می‌شود که همه کلاس‌های شیء ممکن را در instance schema لیست می‌کند.

۲. با ساخت گروه کاربری شروع می‌کنیم.

۳. نام گروه را تایپ کرده برای مثال AD LDA Users و روی Next کلیک می‌کنیم.

۴. در صفحه بعد می‌توانیم روی More Attributes کلیک کنیم تا خصیصه‌های دیگر این شیء را نیز مقداردهی کنیم.

۵. روی Finish کلیک می‌کنیم تا گروه ساخته شود. به طور پیش‌فرض گروه امنیتی خواهد بود.

۶. حالا زمان ساخت کاربر است. روی DN مربوط به پارتیشن برنامه کلیک راست کرده و New و بعد Object را انتخاب می‌کنیم.

۷. شیء User را انتخاب کرده و روی Next کلیک می‌کنیم.

۸. نام کاربر را تایپ کرده و روی Next کلیک می‌کنیم.

۹. یکبار دیگر می‌توانیم روی More Attributes کلیک کنیم تا خصیصه‌های دیگر شیء جدید را مقداردهی کنیم.

۱۰. روی Finish کلیک می‌کنیم تا کاربر ساخته شود.

۱۱. حالا کاربر را به گروه اضافه می‌کنیم. گروه را در پنل وسط پیدا کرده و روی آن راست کلیک کرده و Properties را انتخاب می‌کنیم.

۱۲. در کادر Properties روی Edit کلیک می‌کنیم.

۱۳. در کادر بعدی روی Add DN کلیک می‌کنیم.

۱۴. نام DN کاربر ساخته شده را به صورت زیر تایپ می‌کنیم.

Cn=John Kane,cn=Instance01,dc=contoso,dc=com

۱۵. روی OK کلیک می‌کنیم تا عملیات تکمیل شود.

اگر پنجره properties گروه را دوباره باز کنیم می‌بینیم که کاربر به گروه اضافه شده است. افزودن کاربران و گروهها به instance به این روش کار وقت‌گیری است مگر اینکه فقط یک شیء قرار باشد به آن افزوده شود. برای افزودن تعداد بیشتر بهتر است از لیستی از آنها تهیه کرده و از دستور CSVDE.exe یا LDIFDE.exe برای افزودن آنها استفاده کنیم. برای مرور مراحل خودکارسازی ساخت کاربر به فصل ۴ مراجعه کنید.

استفاده از LDP.exe برای کار با Instance ها

کنسول LDP.exe امکان مشاهده و ویرایش محتویات Instance را فراهم می‌کند. همانند ابزار ADSI Edit باید به Instance متصل شویم تا بتوانیم با آن کار کنیم. برای این کار مراحل زیر را دنبال می‌کنیم:

۱. از طریق خط فرمان یا Server Manager، دستور LDP.exe را اجرا می‌کنیم.

۲. از منوی Connect روی Connection کلیک می‌کنیم.

۳. شماره پورت و نام سروری را که می‌خواهیم به آن متصل شویم تایپ کرده و اگر از پورت Secure LDAP استفاده می‌کنیم SSL را انتخاب می‌کنیم. روی OK کلیک می‌کنیم.

۴. از منوی Connect روی Bind کلیک می‌کنیم.

۵. اگر حساب دارای مجوزهای لازم باشد گزینه Bind As Currently Logged On User را انتخاب می‌کنیم. وگرنه Bind With Credentials را انتخاب کرده و اعتبار مناسب را

۶. از منوی View روی Tree کلیک می‌کنیم.

۷. در کادر محاوره‌ای BaseDN روی فلش پایین کلیک می‌کنیم تا لیست DN ها را نمایش داده شود و نام Instance خود را انتخاب می‌کنیم. بعد روی OK کلیک می‌کنیم.

استفاده از ابزار Schema برای کار با Instance

از ابزار Active Directory Schema برای ساخت کنسول‌های سفارشی جهت مدیریت AD LDS Instance schema استفاده می‌شود. به خاطر داشته باشید برای استفاده از این ابزار باید ابتدا آنرا روی سرور رجیستر کنیم. برای این کار از پنجره خط فرمان elevated استفاده می‌کنیم:

regsvr32 schmmgmt.dll

حالا ما آماده بارگذاری ابزار Schema و مشاهده schema مربوط به instance ها هستیم.

۱. روی Start کلیک می‌کنیم و در کادر Search عبارت mmc را تایپ می‌کنیم. سپس کلید Enter را کلیک می‌کنیم.

۲. در صفحه MMC خالی روی ابزار Add/Remove از منوی File کلیک می‌کنیم.

۳. ابزار Active Directory Schema را در لیست Available Snap-ins پیدا کرده و روی Add و سپس روی OK کلیک می‌کنیم.

۴. کنسول را با یک نام مناسب ذخیره می‌کنیم.

۵. ابزار Schema به دایرکتوری Active Directory Domain Services به طور پیش‌فرض bind می‌شود. برای bind کردن آن به یک AD LDS instance روی Active Directory Schema در پنل کلیک راست کرده و Change Active Directory Domain Controller را انتخاب می‌کنیم.

۶. در کادر محاوره‌ای Change Directory Server گزینه Domain Controller Or AD LDS Instance را انتخاب کرده و روی <Type A Directory Server Name[:Port] Here> کلیک کرده و نام سرور را به همراه شماره پورت با درج : بین آنها تایپ می‌کنیم. سپس کلید Enter را زده و روی OK کلیک می‌کنیم.

۷. درکادر بعدی روی Yes کلیک می‌کنیم تا سرورها عوض شوند.

حالا می‌توانیم schema مربوط به این instance را ببینیم. برای ذخیره تنظیمات این کنسول را دوباره ذخیره می‌کنیم. به تشابه schema در یک AD LDS instance و دایرکتوری AD DS توجه کنید.

استفاده از Active Directory Sites and Services برای کار با Instance ها

همانند دیگر ابزارهای Active Directory امکان مدیریت AD LDS instance با کنسول Active Directory Sites and Services وجود دارد. ولی قبل از اینکه این کار انجام شود باید فایل MS-ADLDS-DisplaySpecifiers.ldf را منتقل کنیم تا schema مربوط به instance به روز شود. این کار به منظور پشتیبانی از اشیاء مورد نظر انجام می‌شود. برای این کار مراحل زیر را دنبال می‌کنیم:

۱. اگر قبلا انجام نشده باشد با افزودن فایل LDIF به instance کار را شروع می‌کنیم. پنجره خط فرمان elevated را باز می‌کنیم.

۲. به مسیر %SystemRoot%\ADAM رفته و دستور cd windows\adam را تایپ می‌کنیم.

۳. محتویات فایل LDIF را به instance منتقل می‌کنیم:

```
ldifde -i -f MS-ADLDS-DisplaySpecifiers.ldf -s servername:portnumber -m -a username domainname password
```

۴. پنجره خط فرمان را می‌بندیم.

۵. از گروه برنامه‌های Administrative Tools ابزار Active Directory Sites And Services را اجرا می‌کنیم.

۶. کنسول به دایرکتوری Active Directory Domain Services به طور پیش‌فرض bind می‌شود. برای bind کردن آن به یک AD LDS instance روی Active Directory Sites and Services در پنل کلیک راست کرده و Change Domain Controller را انتخاب می‌کنیم.

۷. در کادر محاوره‌ای Change Directory Server گزینه This Domain Controller Or AD LDS Instance را انتخاب کرده و روی <Type A Directory Server Name[:Port] Here> کلیک می‌کنیم. نام سرور را به همراه شماره پورت و علامت : بین آنها تایپ کرده و کلید Enter را می‌زنیم. سپس روی OK کلیک می‌کنیم.

۸. در کادر بعدی روی Yes کلیک می‌کنیم تا سرورها عوض شوند.

تمرینات کار با AD LDS Instance

در این تمرینات اولین AD LDS instance خود را می سازیم ، سپس تکثیر بین دو instance را مدیریت می کنیم

تمرین اول ساخت AD LDS Instance

در این تمرین اولین AD LDS Instance خود را خواهیم ساخت. قبلا سرویس AD LDS را بر روی هر دو سرور خود انجام داده ایم. برای انجام این تمرین از مقادیر جدول ۵-۱۴ استفاده می کنیم

جدول ۵- ۱۴ مقادیر Instance

آیتم	مقدار
نام Instance	ADLDSInstance
پورت ها	50004 برای LDAP و 5005 برای Secure LDAP
نام پارتیشن برنامه	CN=ADLDSInstance,dc=contoso,dc=com
مسیر داده	D:\ADLDS\ADLDSInstance\Data
حساب سرویس	سرویس Network
حساب Administrator	Contoso\Administrator
فایل های LDIF برای انتقال	MS-AdamSyncMetadata.ldf MS-ADLDS-DisplaySpecifiers.ldf MS-AZMan.ldf MS-InetOrgPerson.ldf MS-User.ldf MS-UserProxy.ldf MS-UserProxyFull.ldf

بهتر است که هر زمان که می خواهیم یک instance جدید بسازیم جدولی شبیه جدول ۵-۱۴ درست کنیم، از آنجایی که هر سرور می تواند میزبان چندین AD LDS instance باشد ساختن مستند از آنها می تواند ایده خوبی باشد.

۱- از روشن بودن DC دامنه، SERVER01.contoso.com و سرورهای SERVER03.contoso.com و SERVER04.contoso.com اطمینان حاصل می کنیم

۲- با اعتبار مدیر دامنه وارد SERVER03.contoso.com می شویم

به خاطر داشته باشید برای کار کردن با AD LDS تنها نیازمند اعتبار مدیر شبکه محلی هستیم

۳- Active Directory Lightweight Directory Services Setup Wizard را از Administrative Tools اجرا می کنیم

۴- اطلاعات صفحه Welcome را مرور کرده و روی Next کلیک می کنیم

۵- در صفحه Setup Options ، A Unique Instance را انتخاب کرده و روی Next کلیک می کنیم

۶- در صفحه Instance Name عبارت ADLDSInstance را تایپ کرده و روی Next کلیک می کنیم

هنگامی که یک Instance را نامگذاری می کنیم این نام به سرویسی که آن Instance را اجرا می کند نیز داده می شود که این نام به صورت ADAM_Instancename خواهد بود ولی نام Instance به تنهایی در کنسول نمایش داده می شود

۷- در صفحه Ports پورت هایی که برای ارتباط با این Instance استفاده می شوند را مشخص می کنیم. از شماره پورت ۵۰۰۰۴ برای LDAP و ۵۰۰۰۵ برای SSL استفاده می کنیم. سپس روی Next کلیک می کنیم

۸- در صفحه Application Directory Partition نام application partition را که در این مورد CN=ADLDSInstance,dc=contoso,dc=com می باشد، مشخص کرده و روی Next کلیک می کنیم
این نام همیشه باید به صورت DN باشد
۹- در صفحه File Locations مسیر را به D:\ADLDS\ADLDSInstance\Data تغییر داده و روی Next کلیک می کنیم
چون این انباره دایرکتوری می باشد، باید در درایوی بجز درایو سیستم عامل قرار گیرد.
۱۰- در صفحه Service Account Selection ، Network Service Account را انتخاب کرده و روی Next کلیک می کنیم
ویندوز بصورت پیش فرض Network Service Account را انتخاب می کنند. این حساب یک حساب محلی محدود و محافظت شده است. در حالت عادی باید از یک حساب سرویس مناسب استفاده کنیم، اما انتخاب Network Service Account برای اهداف این تمرین کافی است
۱۱- در صفحه AD LDS Administrators ، Currently Logged On User را انتخاب کرده و روی Next کلیک می کنیم
در حالت عادی باید از یک گروه از قبل مشخص شده استفاده کنیم ولی برای اهداف این تمرین انتخاب حساب مدیر شبکه کفایت می کند
۱۲- در صفحه Importing LDIF Files ، همه فایل های لیست شده LDIF را انتخاب کرده و روی Next کلیک می کنیم
۱۳- در صفحه Ready To Install انتخابهایمان را مرور کرده و روی Next کلیک می کنیم
AD LDS یک instance جدید نصب می کند
۱۴- روی Finish کلیک می کنیم

اولین instance ما ساخته می شود. Server Manager را باز کرده و گره Roles\Active Directory Lightweight Directory Services را برای دیدن نتایج کارمان باز می کنیم. AD LDS در حین ساخت instance فایلهای گزارش واقعه می سازد. این فایلها درپوشه %SystemRoot%\Debug و با نامهای ADAMSetup.log و ADAMSetup_loader.log هستند. در صورت بروز مشکل می توان آنها را مرور کرد، همچنین در زمان نصب سرویسی برای instance نصب می شود که می توان کنسول آنرا از Administrative Tools اجرا کرد

تمرین دوم ساخت یک AD LDS Replica Instance

در این تمرین اولین AD LDS Replica Instance خود را در دومین سرور خواهیم ساخت

۱- از روشن بودن DC دامنه، SERVER01.contoso.com و سرورهای SERVER03.contoso.com و SERVER04.contoso.com مطمئن می شویم.
۲- با اعتبار مدیر دامنه وارد SERVER04.contoso.com می شویم
۳- Active Directory Lightweight Directory Services Setup Wizard را از Administrative Tools اجرا می کنیم
٤- اطلاعات صفحه Welcome را مرور کرده و روی Next کلیک می کنیم
٥- زیر Setup Options ، A Replica Of An Existing Instance را انتخاب کرده و روی Next کلیک می کنیم
٦- در صفحه Instance Name عبارت ADLDSInstance را نوشته و روی Next کلیک می کنیم
۷- در صفحه Ports پورت هایی که برای ارتباط با این Instance استفاده می شوند را مشخص می کنیم. از شماره پورت ۵۰۰۰۴ برای LDAP و ۵۰۰۰۵ برای SSL استفاده می کنیم. سپس روی Next کلیک می کنیم
۸- در صفحه Joining A Configuration Set زیر Server برای پیدا کردن Server 02 روی Browse کلیک می کنیم. عبارت SERVER03 را نوشته و روی Check Names و سپس OK کلیک می کنیم و بعد عبارت ۵۰۰۰۴ را در کادر LDAP Port نوشته و روی Next کلیک می کنیم

۹- در صفحه Administrative Credentials For The Configuration Set ، Currently Logged On User را انتخاب کرده و روی Next کلیک می کنیم

در حالت عادی باید از یک گروه استفاده کنیم ولی حساب مدیر شبکه برای اهداف این تمرین کافی است

۱۰-در صفحه Copying Application Directory Partitions، گزینه CN=ADLDSInstance,dc=contoso,dc=com partition را انتخاب کرده و روی Next کلیک می کنیم

۱۱-در صفحه File Locations مسیر را به D:\ADLDS\ADLDSInstance\Data تغییر داده و روی Next کلیک می کنیم

۱۲-در صفحه Service Account Selection ، Network Service Account را انتخاب کرده و روی Next کلیک می کنیم در حالت عادی باید از یک حساب سرویس آماده استفاده کنیم، اما انتخاب Network Service Account برای اهداف این تمرین کافی است

۱۳-در صفحه AD LDS Administrators ، Currently Logged On User را انتخاب کرده و روی Next کلیک می کنیم در حالت عادی باید از یک گروه از قبل مشخص شده استفاده کنیم ولی برای اهداف این تمرین انتخاب حساب مدیر شبکه کافی است

۱۴-در صفحه Ready to Install انتخابهایمان را مرور کرده و روی Next کلیک می کنیم

AD LDS یک instance جدید نصب می کند

۱۵-روی Finish کلیک می کنیم

Replica اکنون ساخته خواهد شد

تمرین سوم مدیریت تکثیر بین AD LDS Replica

در این تمرین پارامترهای تکثیر بین دو instance را خواهیم دید برای پشتیبانی از اشیاء Active Directory Sites and Services ها نیازی به بروزرسانی instance ها نیست زیرا در تمرین اول تمام فایلهای LDIF را وارد کردیم

۱- از روشن بودن DC دامنه، SERVER01.contoso.com و سرورهای SERVER03.contoso.com و SERVER04.contoso.com اطمینان حاصل می کنیم.

۲- با اعتبار مدیر دامنه وارد SERVER04.contoso.com می شویم

۳- Active Directory Sites And Services را از Administrative Tools اجرا می کنیم

کنسول بصورت پیش فرض با Active Directory Domain Services directory باز می شود

۴- برای bind کردن AD LDS instance روی Active Directory Sites And Services در پنل راست کلیک کرده و Change Domain Controller را انتخاب می کنیم

۵- در کادر محاوره ای Change Directory Server ، This Domain Controller یا AD LDS Instance را انتخاب می کنیم و سپس روی <Type A Directory Server Name[:Port] Here> کلیک کرده و عبارت SERVER03:50004 را نوشته و Enterرا فشار داده و روی Ok کلیک می کنیم

۶- در کادر محاوره ای برای تغییر سرور روی Yes کلیک می کنیم

۷- اکنون گره Active Directory Sites And Services را کاملا باز می کنیم. می توانیم این کار را با چند بار فشار دادن کلید ستاره (*) انجام دهیم. این صفحه ساختار تکثیر این instance را نشان می دهد.

اکنون یک سایت جدید خواهیم ساخت و یکی از اشیاء instance ها را به این سایت منتقل می کنیم

۸- در پنل روی Sites راست کلیک کرده و New Site را انتخاب می کنیم

۹- نام سایت جدید را Replication01 گذاشته، DEFAULTIPSITELINK object را انتخاب کرده و روی OK کلیک می کنیم

سایت جدید ساخته شده است (شکل ۶-۱۴)

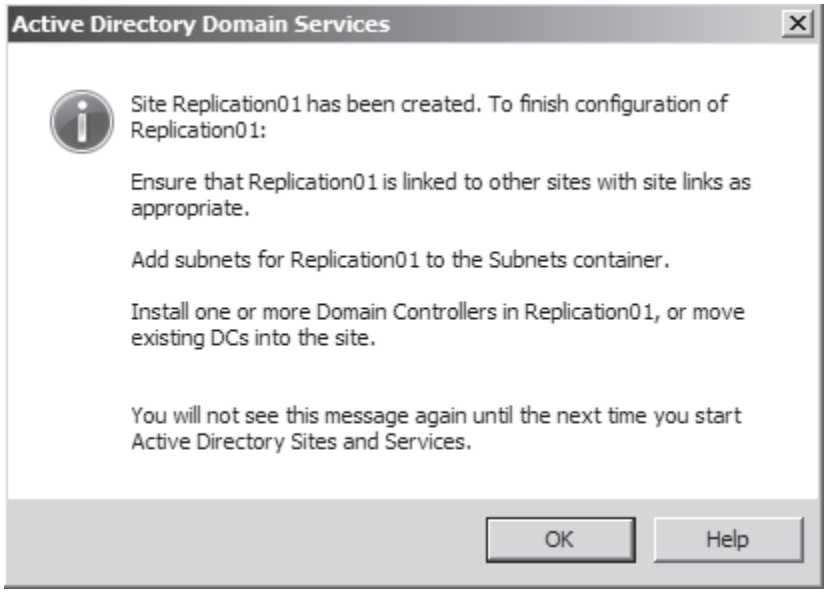
۱۰- برای بستن کادر محاوره ای روی OK کلیک می کنیم.

در این مورد خاص تنها SERVER04 را به سایت جدید منتقل خواهیم کرد

۱۱- روی SERVER04$ADLDSInstance کلیک کرده و آن را به Servers container در زیر Replication01 می کشیم

۱۲- در کادر Moving Objects ، روی Yes کلیک می کنیم. شیء اکنون در محل جدید خود می باشد

این تمرین به ما نشان می دهد که چگونه با instance ها کار کنیم و چگونه تکثیر را مدیریت کنیم. در دنیای واقعی برای درست کردن شراکت تکثیر مناسب باید تمامی مواردی که در شکل ۶-۱۴ لیست شده اندانجام دهیم.



شکل ۶-۱۴ عملیات مورد نیاز برا تکمیل شراکت تکثیر

خلاصه درس

- ابزارهایی که برای کنترل AD LDS instance بکار می روند بسیار شبیه ابزارهای کنترل AD DS هستند. برای دیدن لیست کامل ابزاری که میتواند در رابطه با AD LDS instances استفاده شود به جدول ۳-۱۴ مراجعه کنید
- می توان instance ها را هم با رابط گرافیکی از طریق ابزار نصب AD LDS و هم از طریق خط فرمان و دستور ADAMInstall.exe نصب کرد. در هر دو حالت باید برای پیش نیازها نقشه داشت. هنگامی که از ابزار *ADAMInstall.exe* استفاده می کنیم باید از قبل یک فایل پاسخ برای آن آماده کنیم
- *کار کردن با* AD LDS instance به معنی کار کردن با DN می باشد. DN ها مانند AD DS forest ها دارای ساختار سلسله مراتبی هستند
- *کار کردن با* AD LDS instance به معنی کار کردن با نام سرورها و شماره پورتها است. بهترین کار این است که نام سرور و شماره پورت هر instance که می سازیم را به یاد داشته باشیم، در واقع هر instance که درست می کنیم بهتر است از آن و همه مقادیر استفاده شده در آن لیست تهیه کنیم

سئوالات پایان درس

۱- فرض کنید مدیر سرور محلی دامنه *contoso.com* هستیم *یکی از وظایف ما مدیریت* AD LDS instance ها در SERVER03 می باشد. باید چهار instance در SERVER03 که عضو دامنه است نصب کنیم. با تنظیمات پیش فرض پورت برای هر instance کار را انجام می دهیم اکنون نیاز داریم تا تغییراتی در schema اولین instance که نصب کردیم، Instance01 ، بدهیم ابزار Active Directory Schema را در سرور register کرده و یک کنسول سفارشی Active Directory Schema درست می کنیم. اما هنگامی که سعی می کنیم به schema اولین instance متصل شویم، پیام خطا دریافت می کنیم، کدامیک از موارد زیربه احتمال زیاد مشکل دارند؟

A . Instance01 دارای schema نیست و نمی توانیم آن را تغییر دهیم

B . با ابزار Active Directory Schema نمی توان schema یک instance را تغییر داد وبرای این کار نیازمند استفاده از دستور *LDP.exe* هستیم

C . با ابزار Active Directory Schema نمی توان schema یک instance را تغییر داد و این کار را باید با وارد کردن فایلهای LDIF از طریق دستور *LDIFDE.exe انجام داد*

D . با ابزار Active Directory Schema نمی توان به instance متصل شد چون بصورت پیش فرض از همان پورتی استفاده می کند که Active Directory Domain Services directory استفاده می کند

فصل ۱۵

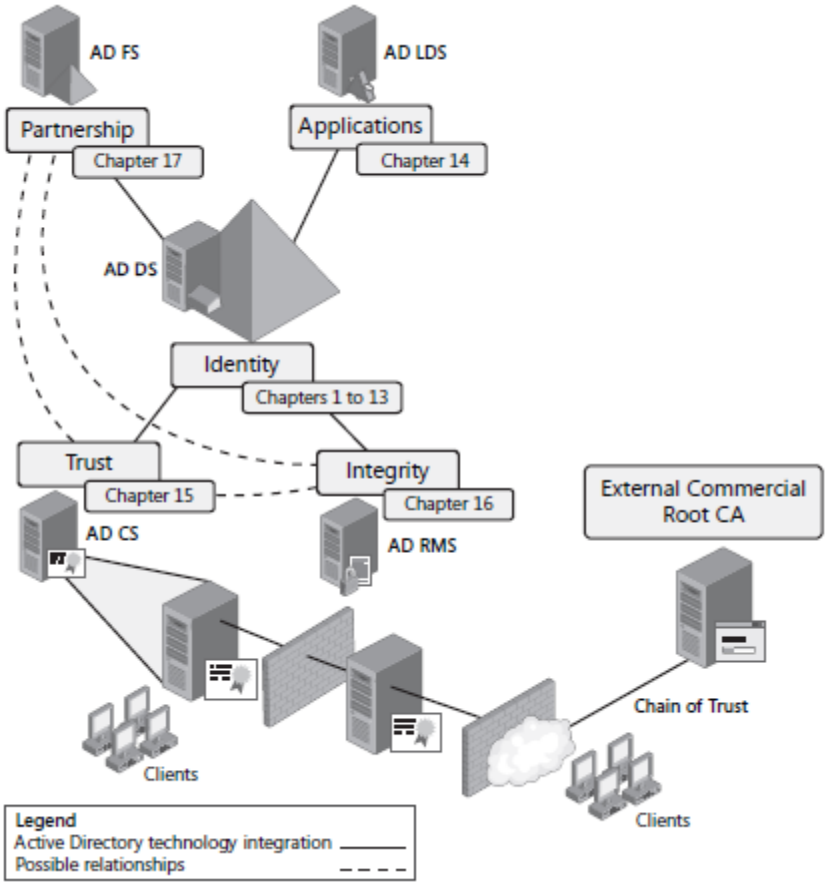
Active Directory Certificate Services و Public Key Infrastructures

Public Key Infrastructures (PKI) کم کم تبدیل به جزء اصلی زیرساخت شبکه سازمان‌ها می‌شود. تقریبا همه سازمان‌ها امروزه از این سرویس استفاده می‌کنند. از ایمن‌سازی ارتباطات بیسیم تا سرویس‌های تجاری امن وب‌سایت و SSL VPN یا حتی ثبت پست الکترونیکی همه از گواهی‌نامه‌های PKI استفاده می‌کنند.

چند سالی است که مایکروسافت قابلیت ایجاد و نگهداری PKI ها را در سیستم‌عامل‌های خود ارائه می‌دهد. در نسخه ویندوز سرور 2008 این قابلیت توسط Active Directory Certificate Services (AD CS) ارائه می‌شود که در نسخه‌های قبلی با نام Certificate Services شناخته می‌شد.

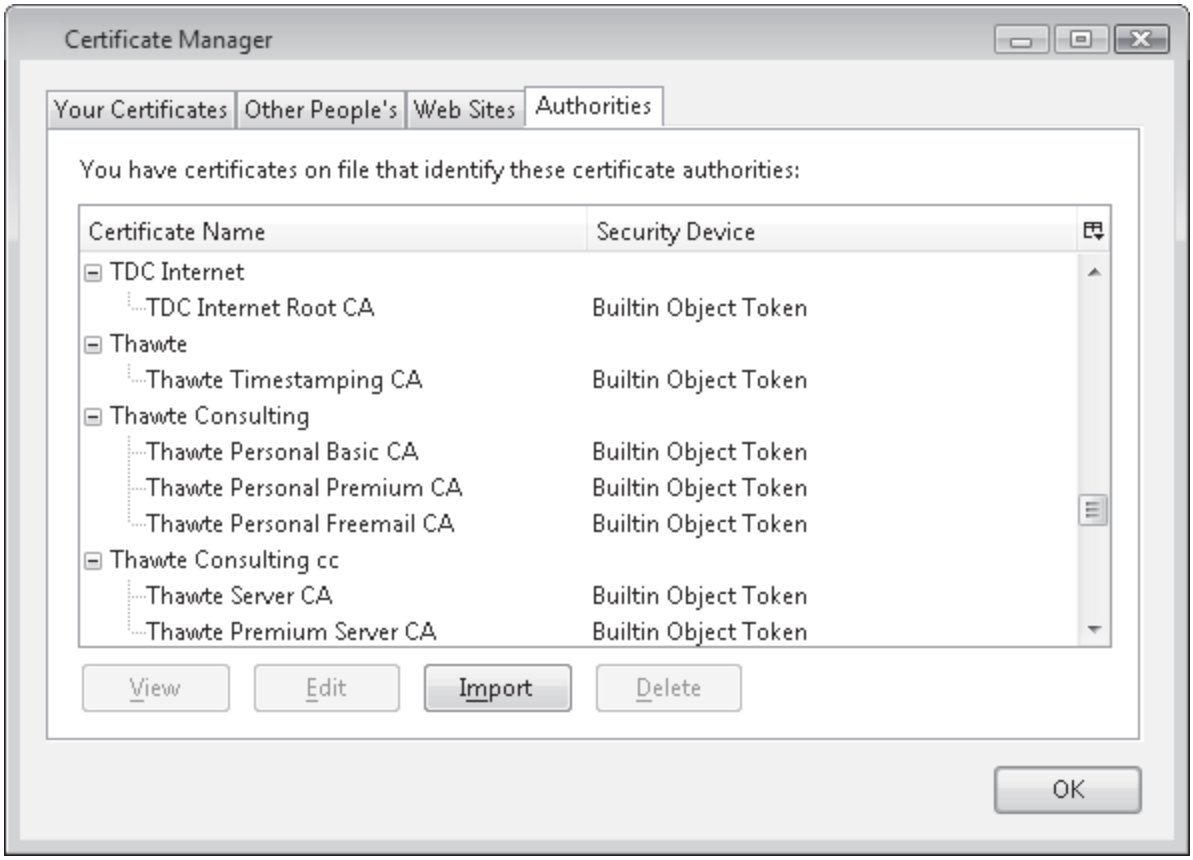
ذات PKI این است که فقط مبتنی بر نرم‌فزار نیست. به دلیل اینکه گواهی‌نامه‌های PKI برای اثبات هویت شما طراحی شده است باید فرایندی پیاده‌سازی شود که هر شخصی که گواهی دریافت می‌کند واقعا همانی باشد که ادعا می‌کند. با دادن گواهی‌نامه به افراد سازمان در واقع ابزاری در اختیار آنان قرار می‌گیرد که هویت شخص را تضمین می‌کند. PKI به منظور ساختن یک فضای مطمئن در دنیای غیرقابل اعتماد طراحی شده است.

در حقیقت PKI به منظور بسط قدرت سازمان در آن‌سوی مرزهای شبکه استفاده می‌شود. اگرچه AD DS به عنوان یک دایرکتوری NOS با هدف اولیه تایید هویت و تعیین اعتبار در داخل مرزهای شبکه طراحی شده، AD CS مانند بقیه فناوری‌های Active Directory برای فراهم کردن این سرویس‌ها برای شبکه داخل و خارج طراحی شده است. ولی وقتی حاکمیت سازمان را تا آنسوی مرزهای شبکه گسترش می‌دهیم باید از یک Certificate Authority (CA) تجاری به منظور پشتیبانی از گواهی‌نامه‌های صادره از طرف ما استفاده کنیم. (شکل ۱- ۱۵)



شکل ۱- ۱۵ AD CS سرویس‌های داخل و خارج از شبکه ما را ارائه می‌دهد.

برای مثال وقتی با استفاده از HTTPS به وب‌سایتی مراجعه می‌کنیم که دارای گواهی SSL است این گواهی‌نامه ثابت می‌کند شما جایی در سایتی هستیم که باید باشیم. اگر این گواهی‌نامه را بررسی کنیم می‌بینیم که حاوی نام سرور، سازمان و صادرکننده گواهی است. گواهی‌نامه با مرورگر ما کار می‌کند به دلیل اینکه مرورگرهای IE یا Firefox لیستی از CA های تجاری معتبر را دارد که فرایند گواهی را به صورت حرفه‌ای مدیریت می‌کند. (شکل ۲- ۱۵)

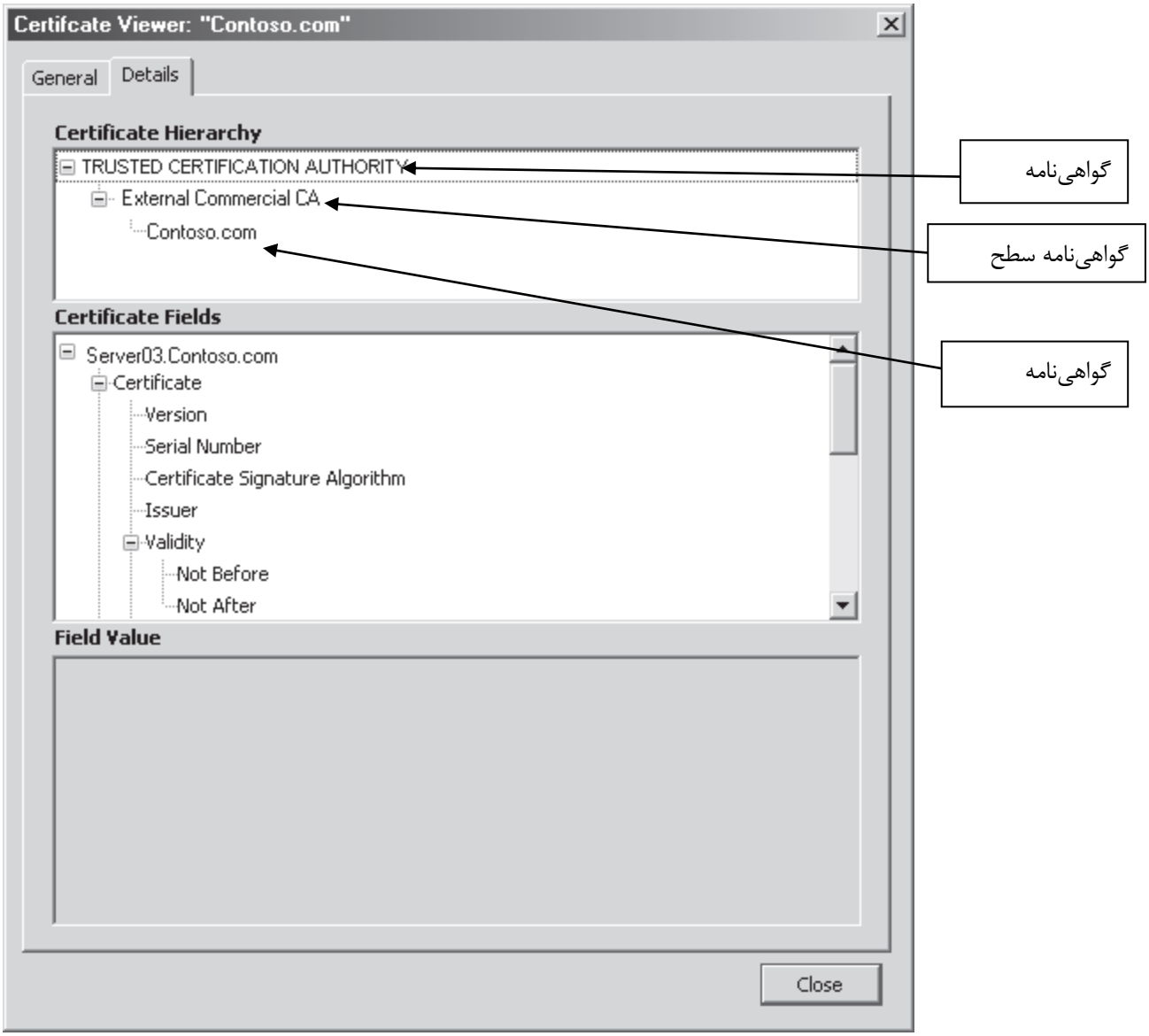


شکل ۲- ۱۵ مرورگرهایی نظیر IE و Firefox، CA های معتبر را لیست می‌کنند.

لیست CA های معتبر به طور خودکار از طریق مکانیزم‌های به روز رسانی مخصوص سیستم عامل به روز می‌شود. در ویندوز ویستا و سرور 2008 این به روز رسانی از طریق تنظیم Group Policy کنترل می‌شود که به طور پیش‌فرض فعال است. در سیستم‌های عامل ویندوز قدیمی‌تر به‌روزرسانی Trusted Root Certificate ها جزئی از ویندوز بوده که از Control Panel قابل دسترس است.

وقتی گواهی از طرف ما صادر می‌شود نه از CA خارجی باید سازمان خود را به عنوان CA معتبر روی کامپیوترهای استفاده کننده از این گواهی‌نامه‌ها معرفی کنیم. وقتی با کاربران سازمان خود طرف هستیم این کار کار ساده‌ای است به دلیل اینکه روی این کامپیوترها کنترل لازم را داریم. ولی وقتی کاربران تحت کنترل ما نیستند (کاربران اینترنتی) مشکل آغاز می‌شود. درخواست قبول این گواهی از آنان مانند این است که آنها بدون شناخت ما به ما اعتماد کنند.

لزوما همه اعضاء زیرساخت PKI با هم در یک ساختار سلسله مراتبی که به بالاترین CA منتهی می‌شود به صورت زنجیره‌ای متصل هستند. این CA نهایتا مسئول تمامی گواهی‌نامه‌های صادره از طرف کل زنجیره است. برای مثال وقتی کاربری یک گواهی از سازمان ما دریافت می‌کند و سازمان ما گواهی اصلی خود را از یک CA تجاری معتبر دریافت کرده باشد (شکل ۳- ۱۵) گواهی کاربر به طور خودکار معتبر خواهد بود چراکه همه مرورگرها به CA تجاری معتبر اعتماد دارند. همان‌طور که می‌توانید تصور کنید این CA خارجی باید برای تایید اعتبار سازمان‌ها برنامه‌های سخت‌گیرانه‌ای داشته باشد وگرنه به تدریج از اعتبار آن کم خواهد شد.



شکل ۳- ۱۵ یک زنجیره گواهی‌نامه معتبر

فناوری‌های متعددی بر اساس گواهی‌نامه‌های PKI کار می‌کنند. یک نمونه عالی Microsoft Exchange Server 2007 است. به دلیل اینکه این سرویس به نقش‌های متعددی تقسیم می‌شود (Hub Transport، Client Access، Mailbox و غیره) و به دلیل اینکه اطلاعات خصوصی افراد را روی ارتباطات TCP/IP ارسال می‌کند هر سرور به طور خودکار هنگام نصب یک گواهی برای خود صادر می‌کند. سپس از طریق استفاده از این گواهی‌نامه‌ها e-mail روی یک ارتباط امن ارسال می‌شود. این کار برای ارتباطات داخلی کارساز است ولی به محض اینکه درهای ارتباطی به بیرون باز شود مثلا ارائه سرویس Microsoft Wec Access (OWA) به کارمندان بیرون از شبکه داخلی باید گواهی‌نامه داخلی را با یک گواهی معتبر خارجی با صرف هزینه جایگزین کنیم. وگرنه کاربران نمی‌توانند از اینترنت به OWA دسترسی پیدا کنند.

اهداف امتحانی در این فصل:

- پیکربندی AD CS
  - نصب AD CS
  - پیکربندی تنظیمات سرور CA
  - مدیریت الگوهای گواهی

- مدیریت ثبت نام
- مدیریت لغو گواهی

دروس این فصل:

- درس ۱: نصب AD CS
- درس۲: پیکربندی و استفاده از AD CS

قبل از شروع

در ادامه این فصل باید موارد زیر انجام شود:

- ویندوز سرور 2008 روی کامپیوتر مجازی یا فیزیکی نصب شده باشد. نام ماشین باید SERVER01 باشد و نقش DC را در دامنه contoso.com داشته باشد.
- ویندوز سرور 2008 نسخه Enterprise باید روی کامپیوتر مجازی یا فیزیکی نصب شده باشد و نام آن SERVER03 بوده و عضو دامنه contoso.com باشد. این ماشین میزبان AD CS CA هایی است که در تمرینات باید نصب شود. بهتر است دارای درایو D بوده تا داده AD CS روی آن ذخیره شود. حجم پیشنهادی برای این درایو 10GB است.
- ویندوز سرور 2008 نسخه Enterprise باید روی کامپیوتر مجازی یا فیزیکی نصب شده باشد و نام آن SERVER04 بوده و عضو دامنه contoso.com باشد. این ماشین میزبان صادرکننده CA برای AD CS خواهد بود. که در تمرینات باید نصب شود. بهتر است دارای درایو D بوده تا داده AD CS روی آن ذخیره شود. حجم پیشنهادی برای این درایو 10GB است.

این مجموعه برای تمرین نصب و پیکربندی AD CS ابتدایی کافی است. تست همه قابلیت‌های AD CS نیاز به ۵ ماشین داشته و از بحث ما خارج است.

درس ۱: نصب AD CS

AD CS فراهم‌کننده سرویس‌های مختلفی بر اساس PKI وکاربرد گواهی به طور عام می‌باشد. با استفاده از ویندوز سرور 2008 و AD CS می‌توانیم از سناریوهای زیر پشتیبانی کنیم:

- ما می‌توانیم همه فایل‌های داده را رمزنگاری کنیم. یکی از رایج‌ترین مشکلات در IT امروزه گم شدن یا سرقت سیستم‌های قابل‌حمل است. اگر داده رمزنگاری شده باشد مشکل به حداقل می‌رسد وگرنه ممکن است روی تجارت و حرفه صاحب آن تاثیر منفی بگذارد. با ویندوز سرور 2008 و ویستا می‌توان همه فایل‌های داده کاربران را به طور خودکار از طریق اشیاء Group Policy رمزنگاری کرد و کاربران را مجبور کرد از کلمات عبور پیچیده استفاده کنند. Encryption File System(EFS) از گواهی‌نامه‌ها برای قفل و باز کردن فایل‌های رمزنگاری شده استفاده می‌کند.
- ما می‌توانیم همه ارتباطات راه دور را رمزنگاری کنیم. ویندوز سرور 2008 هم حاوی ارتباطات IPSec بوده و هم Secure Sockets Tunnelling Protocol (SSTP) VPN که اساس کارکرد هر دو برای تایید هویت دو سر ارتباط گواهی‌نامه می‌باشد.
- ما می‌توانیم پیغام‌های e-mail خود را ایمن سازیم. ویندوز سرور 2008 از پروتکل Secure Multipurpose Internet Mail Extensions (S/MIME) که پروتکل امنیتی استاندارد e-mail است پشتیبانی می‌کند. پیغام‌های امضاء شده از جعل هویت جلوگیری می‌کند و ثابت می‌کند فرستنده آنها شخص مورد نظر ماست.

- ما می‌توانیم همه ورودهای کاربران به سیستم را ایمن کنیم. با استفاده از کارت‌های هوشمند می‌توانیم از گواهی‌نامه‌ها برای پشتیبانی از فرایند ورود بهره ببریم و مطمئن باشیم همه کاربران مخصوصا مدیران شبکه همانهایی هستند که ادعا می‌کنند.

- ما می‌توانیم همه وب‌سایت‌ها را ایمن کنیم. با استفاده از ویندوز سرور 2008 و IIS نسخه ۷ می‌توانیم همه ارتباطات وب‌سایت خود را ایمن کنیم تا تعاملات کلاینت‌ها را با آن امنیت ببخشیم.

- ما می‌توانیم سرورها را ایمن کرده و اعتبار آنها را تایید کنیم. برای مثال وقتی به سرورها در زیرساخت Network Access Protection (NAP) یا در هر سرویس امن دیگری گواهینامه می‌دهیم کامپیوترهای شبکه می‌دانند که با سرورهای داخلی کار می‌کنند نه با سرورهای دیگر که خود را جای سرورهای اصلی جازده‌اند.

- ما می‌توانیم ارتباطات بیسیم خود را ایمن کنیم. با استفاده از ویندوز سرور 2008 و ویستا می‌توانیم تضمین کنیم که همه ارتباطات بیسیم از منشا معتبر می‌آید.

- ما می‌توانیم همه داده‌ها را در برابر سوء استفاده محافظت کنیم. با استفاده از Active Directory Rights Management Services (AD RMS) می‌توان از ویندوز سرور 2008 برای جلوگیری از جعل هویت یا سوء استفاده از اطلاعات بهره برد.

به علاوه بهتر است برای همه کارمندان گواهی‌نامه صادر شود تا در تعاملات با اینترنت تایید شده باشند. به خاطر داشته باشید همه گواهی‌نامه‌های خارجی باید حاوی یک CA معتبر باشد تا بتواند با مرورگرها به طور خودکار کار کند.

درک AD CS

به وسیله AD CS می‌توانیم سلسله مراتب جامع PKI بسازیم که برای صدور و مدیریت گواهنامه‌های داخل سازمان استفاده شود. AD CS دارای اجزاء متعددی است:

- **Certificate Authorities** به دلیل ساختار سلسله مراتبی ذاتی PKI ، AD CS از CA های ریشه و فرزند پشتیبانی می‌کند. CA ریشه معمولا گواهی‌نامه‌ها را برای CA های فرزند صادر می‌کند که به آنها اجازه می‌دهد برای کاربران، کامپیوترها و سرویس‌ها گواهی‌نامه صادر کنند. CA فرزند فقط زمانی می‌تواند گواهی‌نامه‌ها صادر کند که گواهی‌نامه خودش معتبر باشد. وقتی زمان گواهی‌نامه منقضی می‌شود CA فرزند باید درخواست تمدید آنرا از CA ریشه بنماید. برای همین CA های ریشه اغلب دارای زمان اعتبار خیلی بیشتری نسبت به CA های فرزند می‌باشند. در عوض CA های فرزند هم معمولا دارای مدت اعتبار بیشتری نسبت به گواهی‌نامه‌های صادره برای کاربران می‌باشند.

- **CA Web Enrollment** با استفاده از Web Enrollment کاربران می‌توانند از طریق مرورگر وب به CA متصل شده و درخواست گواهی‌نامه بدهند، ثبت نام کارت هوشمند انجام دهند یا لیست گواهی‌نامه‌های لغو شده (CRL) را دریافت کنند. CRL ها لیست گواهی‌نامه‌های نامعتبر و لغوشده توسط سازمان را به کاربران PKI ارائه می‌دهند. سیستم‌های متکی بر PKI سرورهای CA را لیست می‌کنند تا هر بار که گواهی جدیدی معرفی شد CRL ها را به دست آورند. اگر گواهی‌نامه معرفی شده به آنها در لیست باشد به طور خودکار آنرا رد می‌کند.

- **Online responder** این سرویس به منظور پاسخ دادن به درخواست‌های اعتبار سنجی گواهی مشخص از طریق پروتکل Online Certificate Status Protocole (OCSP) طراحی شده است. سیستم مبتنی بر PKI در صورتی که از online responder (OR) استفاده شود نیازی به دریافت CRL کامل ندارد و فقط درخواست بررسی اعتبار را برای یک گواهی‌نامه خاص ارسال می‌کند. OR درخواست‌های اعتبارسنجی را رمزگشایی کرده و تعیین می‌کند که گواهی معتبر است یا

نه. وقتی تعیین اعتبار گواهی‌نامه انجام شد پاسخ رمزنگاری شده برمی‌گردد. استفاده از OR باعث تسریع و کارایی بیشتر نسبت به CRL خواهد شد. AD CS سرویس OR را به عنوان یک ویژگی جدید در ویندوز سرور 2008 ارائه می‌دهد.

- **Network Device Enrollment Service** دستگاههایی که از سیستم عامل‌های سطح پایین مانند سوئیچ و مسیریاب استفاده می‌کنند نیز می‌توانند از طریق NDES در PKI شرکت کنند. پروتکل به کار رفته Simple Certificate Enrollment Protocole (SCEP) می‌باشد که توسط شرکت Cisco Systems ارائه شده است. چنین دستگاههایی معمولا در دایرکتوری AD DS شرکت نمی‌کنند بنابراین حساب AD DS نیز نخواهند داشت. ولی به واسطه NDES و SCEP آنها بخشی از سلسله مراتب PKI خواهند بود که توسط AD CS مدیریت و نگهداری می‌شوند.

اینها چهار جزء اصلی سرویس AD CS را در ویندوز سرور 2008 تشکیل می‌دهند.

CA های منفرد (Standalone) و سازمانی (Enterprise)

بزرگترین دغدغه ما هنگام آماده‌سازی توزیع AD CS چگونگی ساختاربندی چهار سرویس اصلی AD CS است. اولین دغدغه نقش اول است: CA های مورد نیاز توزیع. AD CS از دو نوع CA پشتیبانی می‌کند:

- **CA منفرد** نوعی از CA است که لزوما با سرویس دایرکتوری AD DS عجین نمی‌باشد. CA های منفرد روی سرورهای غیر DC نصب می‌شوند چه عضو دامنه باشند یا نباشند و اغلب به عنوان CA ریشه داخلی استفاده می‌شوند. اغلب به جهت تامین امنیت پس از اینکه گواهی سرورهای فرزند را صادر کردند توسط مدیر از شبکه خارج می‌شوند. صدور و تایید گواهی به صورت دستی انجام می‌شود و گواهی‌نامه‌ها مبتنی بر الگوهای استاندارد است که قابل تغییر نیست. کلاینت‌های CA منفرد می‌توانند عضو دایرکتوری AD DS باشند ولی این عضویت اجباری نیست. این نوع CA روی ویندوز سرور 2008 نسخه‌های Standard، Enterprise وDatacenter اجرا می‌شوند.

- **CA سازمانی** نوعی CA است که با سرویس دایرکتوری AD DS عجین شده است. معمولا روی سرورهای عضو دامنه نصب شده و صادرکننده گواهی می‌باشد. یعنی در ساختار سلسله‌مراتبی به عنوان CA فرزند برای کاربران گواهی صادر می‌کند. CA های صادرکننده گواهی باید همیشه در دسترس باشند. CA های سازمانی به دلیل اینکه با دایرکتوری‌های AD DS عجین هستند به طور خودکار گواهی صادر و تایید می‌کنند وقتی درخواست از طرف اعضاء دایرکتوری ارسال می‌شود. الگوهای گواهی‌نامه پیشرفته‌تر هستند و برای پوشش دادن نیازهای ویژه قابل ویرایش هستند. همه کلیدهای رمزنگاری از طریق عجین شدن با دایرکتوری محافظت می‌شوند. CA های سازمانی فقط روی ویندوز سرور 2008 نسخه Enterprise یا Datacenter اجرا می‌شوند.

شکل ۱- ۱۵ جدول ۱- ۱۵ مقایسه CA های منفرد و سازمانی

ویژگی	منفرد	سازمانی
انتشار پیکربندی CA به دایرکتوری‌های Actvie Directory Domian Services	انتخابی	اجباری
عجین شدن داده گواهی‌نامه CA با AD DS forest	انتخابی (روند دستی)	اجباری و اتوماتیک
انتشار CRL در AD DS forest	انتخابی (روند دستی)	اجباری و اتوماتیک. نیز حاوی Delta CRL ها و گواهی‌نامه‌های cross می‌باشد

انتشار AD DS forest در سطح per-remplate به عنوان یک خصیصه الگو	-	پشتیبانی می‌شود
Web Enrollment برای درخواست گواهی‌نامه و اعتبار	پشتیبانی می‌شود	پشتیبانی می‌شود
کنسول MMC گواهی‌نامه‌ها برای درخواست گواهی‌نامه و اعتبار	-	پشتیبانی می‌شود
درخواست گواهی‌نامه از طریق HTPP یا HTTPS	پشتیبانی می‌شود	پشتیبانی می‌شود
درخواست گواهی‌نامه از طریق RPC به همراه DCOM	-	در حالت پیش‌فرض
الگوهای V1 با object Identifier (OID) های سفارشی برای گواهی‌نامه‌ها	پیش‌فرض	-
الگوهای قابل تغییر V2 و V3 برای گواهی‌نامه‌ها.	-	در حالت پیش‌فرض
ورود داده توسط کاربر در حین درخواست گواهی‌نامه	دستی	از AD DS استخراج می‌شود
روش‌های ثبت نام پشتیبانی‌شده	خودکار یا معلق برای همه الگوها	خودکار یا معلق و برمبنای یک الگو اعمال می‌شود
فرایند تایید گواهی	دستی	دستی یا خودکار از طریق تایید هویت و کنترل دسترسی AD DS
انتشار گواهی‌نامه	به طور دستی برای کلاینت یا CA . فقط از طریق custom policy module روی AD DS انتشار می‌یابد.	بستگی به نوع گواهی‌نامه و تنظیمات الگو دارد ولی به طور خودکار در انباره گواهی و انتشار کلاینت در AD DS ثبت می‌شود
انتشار گواهی‌نامه و مدیریت از طریق AD DS	-	پشتیبانی می‌شود
گزینه‌های توزیع	DC ، سرور عضو دامنه یا غیرعضو	فقط DC و سرور عضو دامنه

همان‌طوری‌که در جدول مشاهده می‌شود CA های منفرد روی تحویل سرویس‌های خاص متمرکز هستند و بیشتر برای محیط‌های مجزا به کار می‌آیند که نیازمند تنظیم خودکار نیست. CA های ریشه یا CA های موجود در شبکه DMZ مثال‌های خوبی از این نوع می‌باشند که به کاربران اینترنتی سرویس می‌دهند.

CA های سازمانی بیشتر به عنوان CA صادرکننده گواهی در شبکه خصوصی به کار می‌آیند که ساختار AD DS forest دارند. این نوع از CA فرایند تخصیص گواهی را خودکار کرده و زمانی که نیاز به صدور گواهی برای دستگاههای بیسیم یا کاربران کارت‌های هوشمند می‌باشد مفید واقع می‌شوند. فرض کنید کل فرایند درخواست و تایید گواهی را وقتی برای هزاران کاربر و دستگاه به صورت دستی انجام می‌شود.

ایجاد ساختار سلسله‌مراتبی CA

دغدغه دوم در برنامه‌ریزی سلسله‌مراتب CA امنیت است. زیرا این ساختار CA مبتنی بر زنجیره گواهی بوده و هر تهدید امنیتی در سطح CA ریشه به طور خودکار به همه گواهی‌نامه‌های مبتنی بر آن اعمال می‌شود. به همین دلیل باید تا حد ممکن CA ریشه را ایمن کنیم. در واقع یک روش رایج، ساخت ساختار سلسله‌مراتبی چندسطحی CA و خروج اعضاء سطح اول از شبکه می‌باشد. وقتی سروری از شبکه خارج است منطقا بیشترین امنیت را دارد.

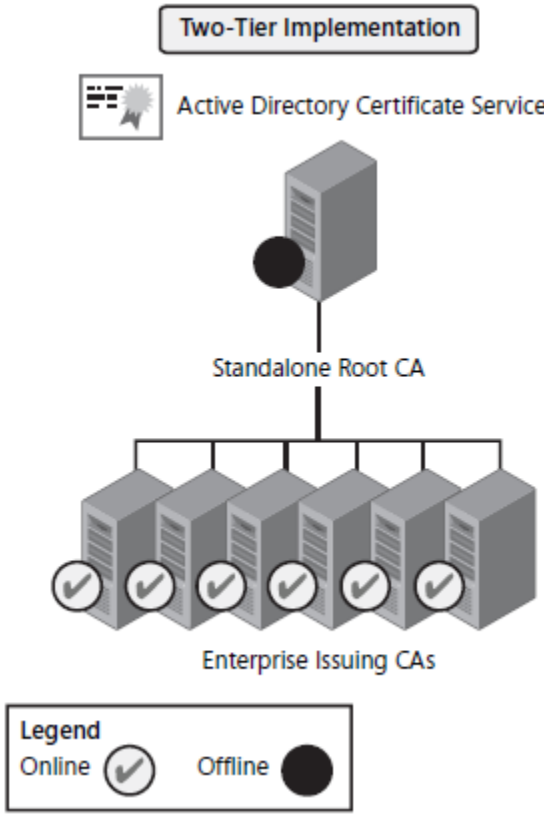
ولی تعیین تعداد گره‌های ساختار AD CS به عوامل زیادی بستگی دارد. یکی از آنها اندازه و توزیع جغرافیایی شبکه می‌باشد. ارتباطات trust بین CA ها نیز در این قضیه دخیل است. به خاطر داشته باشید که هربار یک گواهی‌نامه معرفی می‌شود باید از طریق یا CRL و یا OR اعتبارسنجی شود.

همچنین باید سناریوهایی را که قصد دارید با AD CS از آن پشتیبانی کنید درنظر آورید. مثلا آیا قرار است با افراد یا شرکاء بیرون شبکه تعامل داشته باشید؟ آیا از کارت هوشمند استفاده می‌کنید؟ آیا از شبکه‌های بیسیم استفاده می‌کنید؟ آیا از IPSec یا SSTP استفاده می‌کنید؟ اساسا هرگاه بخواهیم دستگاه، کاربر یا برنامه‌ای را گواهی کنیم باید از AD CS و مراجع خارجی گواهی‌کننده تجاری استفاده کنیم.

اگر جواب همه این سئوالات را داریم می‌توانیم با برنامه‌ریزی ساختار AD CS ادامه دهیم. موارد زیر را نیز در نظر می‌گیریم:

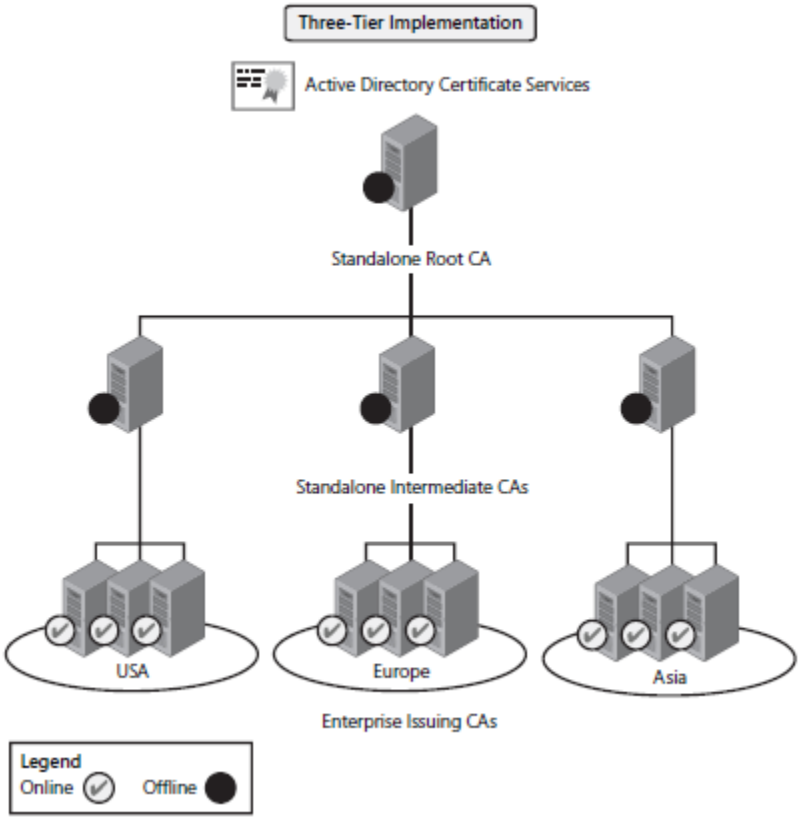
- ساخت یک ساختار یک سطحی با یک CA ریشه زمانی استفاده می‌شود که مطمئن باشیم رمز CA ریشه هیچ‌گاه کشف نمی‌شود. این اطمینات معمولا وجود ندارد.

- ساخت یک ساختار دو سطحی با CA ریشه و CA صادرکننده گواهی زمانی استفاده می‌شود که به محافظت از CA ریشه نیاز داریم ولی اندازه سازمان و ساختار سلسله‌مراتبی اجازه ساختار پیچیده را نمی‌دهد. در این مدل می‌توانیم CA ریشه را از شبکه خارج کنیم. (شکل ۴- ۱۵)



شکل ۴- ۱۵ یک ساختار سلسله‌مراتبی دو سطحی

- ساخت یک ساختار سه‌سطحی به همراه CA ریشه، CA های لایه واسط و CA های سطح آخر که صادرکننده CA می‌باشند زمانی انجام می‌شود که نیاز به سطح امنیتی و دسترس‌پذیری بالایی داریم و مدل مدیریتی، تعداد کاربران و حوزه جغرافیایی اجازه صرف هزینه اضافی لایه‌های بیشتر را می‌دهد. CA های لایه واسط چندتایی اغلب برای پشتیبانی از سیاست‌های مختلف در محیط‌های مختلف مدل استفاده می‌شود. اگر از این مدل استفاده کنیم باید هم CA های واسط و هم ریشه را همانند شکل ۵- ۱۵ از شبکه خارج کنیم.



شکل ۵- ۱۵ سلسله مراتب سه‌سطحی در یک توزیع جغرافیایی

- ساخت بیش از سه سطح فقط در محیط‌های فوق پیچیده زمانی استفاده می‌شود که به بیشترین امنیت نیازمندیم.

همان‌طور که می‌بینیم هرچه تعداد لایه‌ها بیشتر شود امنیت بالاتر و پیچیدگی مدیریتی بیشتر می‌گردد. به علاوه باید مشخص کنیم در هر لایه از چه نوع CA می‌خواهیم استفاده کنیم. جدول ۲- ۱۵ انواع CA را بر اساس مدل لایه‌ای خلاصه می‌کند.

جدول ۲- ۱۵ تعیین نوع CA بر اساس مدل لایه‌ای

نوع CA	تک‌لایه‌ای	دولایه‌ای	سه‌لایه‌ای
CA ریشه	CA سازمانی (آنلاین)	CA منفرد (آفلاین)	CA منفرد (آفلاین)
CA حدواسط			CA منفرد (آفلاین)
CA صادرکننده		CA سازمانی (آنلاین)	CA سازمانی (آنلاین)

بهترین روش‌ها برای توزیع AD DS

معماری‌هایی که از دو یا چند لایه استفاده می‌کنند رایج‌ترین نوع توزیع AD CS هستند. وقتی زیرساخت AD CS را طراحی می‌کنیم باید به موارد زیر توجه کنیم:

- از ساختارهای تک‌سطحی تا حد ممکن بپرهیزیم زیرا از لحاظ امنیتی آسیب‌پذیر هستند.

- CA های ریشه و واسط (اگر موجود باشند) پس از پیاده‌سازی ساختار سریعا باید از شبکه خارج شوند. برای همین این CA ها بهترین انتخاب‌ها برای مجازی‌سازی از طریق ویندوز سرور Hyper-V 2008 می‌باشند. برای این کار یک ماشین مجازی (VM) ساخته و نقش CA منفرد را افزوده و وضعیت ماشین را ذخیره می‌کنیم. (save state)

- پس از خروج سرور از شبکه به سرعت فایل‌های VM مربوط به CA ریشه را از روی سرور میزبان پاک می‌کنیم. VM ایمن شده را در مکانی امن قرار می‌دهیم.

- اگر از مجازی‌سازی در پشتیبانی از توزیع AD CS استفاده کنیم VM ها را تاحد ممکن ایمن می‌سازیم.
- ساخت VM های بدون کارت شبکه یا با کارت شبکه غیرفعال برای CA های واسط و ریشه را در نظر داشته باشید. این کار باعث بالاتر رفتن امنیت می‌شود. گواهی‌نامه‌ها از این سرورها بر روی دستگاههای USB و امثال آن منتقل می‌شود.
- در کنسول Local Security Policy دستگاههای قابل‌حمل روی CA های ریشه و حدواسط را توسط تنظیمات محافظتی کنترل می‌کنیم. این کار باعث بالاتر رفتن سطح امنیتی می‌شود.
- مدیران CA باید دارای شخصیت قابل‌اعتماد باشند به دلیل اینکه کل ساختار CA را کنترل می‌کنند.
- مرکز داده میزبان سرورهای CA را از لحاظ امنیتی تقویت می‌کنیم. دسترسی به مرکز را شدیدا کنترل کرده و از کارت هوشمند برای ورود مدیران شبکه استفاده می‌کنیم.
- پس از پیاده‌سازی ساختار لایه‌بندی شده CA های واسط و صادرکننده گواهی، میزان دسترس‌پذیری CA ریشه را از طریق نصب چندگانه CA تضمین می‌کنیم.
- پس از نصب سرویس AD CS نام سرور را نمی‌توانیم تغییر دهیم بنابراین سرورهای نام خود را با احتیاط نام‌گذاری می‌کنیم.
- پس از نصب AD CS سرور CA منفرد و سازمانی را نمی‌توان به یکدیگر تبدیل کرد.
- به عنوان یک تمرین عملی AD CS را روی DC نصب نمی‌کنیم. برای حفظ نقش سرور AD CS آنرا از بقیه نقش‌ها مستقل می‌کنیم به جز نقش DNS.

نیازمندی‌های دیگر طراحی

حالا تقریبا آماده شروع هستیم. همان‌طور که قبلا اشاره شد طراحی و توزیع ساختار CA فقط یک عملیات فنی نیست. باید فرایندهای مدیریتی مناسب آن را برای پشتیبانی از سرویس گواهی در شبکه داشته باشیم. سه موضوع دیگر قبل از شروع نصب AD CS لازم به توضیح است:

- باید بدانیم چطور از certificate enrollment پشتیبانی کنیم.
- باید بدانیم چطور گواهی‌ها را تجدید کنیم.
- باید یک certificate practice statement (CPS) بسازیم.

اول باید بدانیم برای پشتیبانی از درخواست‌های گواهی و توزیع چگونه برنامه‌ریزی کنیم. همان‌طور که قبلا اشاره شد یک گواهی‌نامه بیان‌کننده کامل صاحبش می‌باشد. بنابراین هویت درخواست‌کننده باید کاملا روشن باشد. ما نمی‌توانیم برای شخصی به نام John Kane گواهی صادر کنیم درحالی که مطمئن نیستیم درخواست کننده خود او باشد. مراجع صدور گواهی خارجی از انواع مختلف فرایندها برای تایید اعتبار استفاده می‌کنند. محکم‌ترین روش ملاقات نماینده رسمی مرجع CA با شخص درخواست‌کننده گواهی می‌باشد. برای حفاظت بیشتر از گواهی می‌توان آنرا روی یک سخت‌افزار نظیر کارت هوشمند ذخیره کرد و آنرا به درخواست‌کننده ارائه نمود. بعد از این مسئولیت حفظ گواهی بر عهده درخواست‌کننده می‌باشد.

ولی اگر بخواهیم از طریق CA های سازمانی automatic enrollment را پیاده‌سازی کنیم باید مطمئن شویم کاربران قبل از دسترسی به شبکه کاملا تایید اعتبار می‌شوند. برای این کار روش‌های تایید هویت رسمی مانند گذرنامه یا امثال آن مناسب می‌باشد. این کار می‌تواند در مرحله جذب نیروی انسانی شرکت انجام شود.

دغدغه دوم مربوط به زمان اعتبار گواهی‌نامه است. گواهی‌نامه‌ها معمولا حاوی دو کلید است. یکی کلید خصوصی (private) و دیگری عمومی (public). وقتی داده رمزنگاری می‌شود از کلید خصوصی برای این کار استفاده می‌شود.

دیگران داده را با کلید عمومی رمزگشایی می‌کنند. هرچه مدت استفاده از کلیدها برای یک گواهی بیشتر باشد جهت حمله یا کشف‌رمز مستعدتر است. وقتی گواهی تمدید می‌شود یک جفت کلید جدید برای گواهی تولید می‌شود. بنابراین باید زمان گواهی و تمدید را با احتیاط مشخص کنیم. باید بین زمان کلید و خطر کشف رمز تعادل برقرار کنیم.

به علاوه باید سلسله‌مراتب لایه‌ای زمان لایه‌ای نیز داشته باشد. CA های ریشه باید بیشترین زمان را داشته باشند بعد CA واسط و بعد CA صادرکننده و سپس خود گواهی صادرشده. برای مثال می‌توانیم از یک شکاف ۱۰ ساله در هر لایه استفاده کنیم. یعنی هر لایه ۱۰ سال. با این روش در معماری سه لایه CA ریشه ۳۰ سال حدواسط ۲۰ سال و صادرکننده ۱۰ سال زمان دارند. سپس می‌توانیم به گواهی‌نامه‌های صادره یک تا دو سال اعتبار اختصاص دهیم. دلیل این نوع ساختار زمانی این است که هر بار زمان گواهی‌نامه سروری منقضی می‌شود همه گواهی‌های فرزند نیز منقضی می‌شود. برای جلوگیری از این وضعیت زمان زیادی به سرور اختصاص می‌دهیم.

در نهایت باید CPS خود را طراحی و آماده کنیم. CPS ها مبتنی بر سیاست‌های گواهی‌نامه ساخته شده می‌باشد. سیاست‌ها مسئولیت‌های سازمان صادرکننده گواهی را در مدت صدور گواهی تعیین می‌کند. سازمان صادرکننده مسئول نهایی هر سوءاستفاده از گواهی صادرشده می‌باشد. برای همین از منابع انسانی و بخش امنیت سازمان برای تعیین سیاست‌های هر مناسب هر نوع گواهی‌نامه کمک می‌گیریم و سپس CPS را از آن به دست می‌آوریم. CPS باید حاوی موارد متعددی مانند مشخص کننده هویت شخص به صورت شفاف، لیست سیاست‌های گواهی، بیان کلی مراحل صدور و لغو گواهی باشد.

مورد مهم دیگر که باید در CPS گنجانده شود سیاست لغو است. لغو معمولا زمانی اتفاق می‌افتد که کاربر از سیاست تعریف شده ما در قبال یک نوع خاص از گواهی پیروی نکرده باشد. به خاطر داشته باشید لغو تنها راه از بین بردن اعتبار یک گواهی می‌باشد.

CPS باید برای کاربران CA داخلی و خارجی در دسترس باشد. این یعنی در دسترس قرار دادن آن در اینترنت و اینترانت.

نصب AD CS

نصب سرویس AD CS بسیار پیچیده‌تر از نصب AD LDS می‌باشد. دلیل آن انتخاب بین CA منفرد و سازمانی است که براساس این انتخاب انشعابات بعدی را به دنبال خواهد داشت. در بیشتر موارد حداقل ساختار دولایه نصب شده که لایه اول منفرد و دوم سازمانی می‌باشد. در سازمان‌های بزرگتر تعداد لایه‌ها بیشتر و تعداد سرورهای هر لایه به جز ریشه نیز بیشتر خواهد بود.

سرورهای میزبان نقش AD CS بهتر است با قابلیت‌های زیر پیکربندی شود چه روی سرور فیزیکی چه مجازی:

- چندپردازشگر داشته باشند تا بتوانند فرایند تخصیص گواهی را به سرعت انجام دهند
- حداقل حافظه را داشته باشند به دلیل اینکه در این فرایند به حافظه زیاد نیازی نیست. ماشین‌های مجازی می‌توانند 512MB حافظه داشته باشند.
- دیسک‌های مجزا برای انباره گواهی‌نامه داشته باشند. بهتر است حداقل یک دیسک داشته و بانک اطلاعاتی را روی آن ذخیره کنند. سرورهای صادرکننده گواهی در شرکت‌های بزرگ بهتر است یک دیسک دیگر برای فایل‌های log داشته باشند.
- طول کلید روی میزان مصرف پردازشگر و دیسک تاثیر می‌گذارد. کلیدهای کوتاه به دیسک بیشتری نیاز دارند و کلیدهای بلند روی میزان مصرف پردازشگر تاثیر دارند. بهتر است طول کلیدها را در حد متوسط نگه داریم تا بیشترین کارایی را روی سرور داشته باشیم.
- اگر از سیستم‌های فیزیکی استفاده می‌کنیم بهتر است از دیسک‌های RAID استفاده کنیم.

نسخه‌های مختلف ویندوز سرور 2008 ویژگی‌های متفاوتی از AD CS را ارائه می‌دهد. جدول ۳- ۱۵ ویژگی‌های نسخه‌ها را خلاصه می‌کند.

اجزاء و ویژگی‌ها	Web	Standard	Enterprise	Datacenter
مرجع گواهی‌نامه‌های منفرد		√	√	√
مرجع گواهی‌نامه‌های سازمانی			√	√
Network Device Enrollment Service (NDES)			√	√
سرویس OR			√	√
بایگانی کلیدها			√	√
تفکیک نقش‌ها			√	√
محدودیت Certification Manager			√	√
محدودیت Delegated enrollment agent			√	√

آماده سازی نصب AD CS

پیش‌نیازهای نصب AD CS شامل موارد زیر است:

- AD DS forest با حداقل یک دامنه ریشه forest مورد نیاز است. همچنین باید دارای یک دامنه فرزند نیز باشد.
- کامپیوترهایی جهت مراجع گواهی‌نامه در ساختار باید در نظر گرفته شوند. در ساده‌ترین نوع ساختار بندی باید دو دستگاه کامپیوتر موجود باشد یکی CA ریشه و دیگری CA صادرکننده. CA صادرکننده می‌تواند میزبان OR و NDES نیز باشد. این CA نیازمند نصب IIS بوده ولی فرایند نصب AD CS به طور خودکار این ویژگی را نصب می‌کند. هر دو کامپیوتر بهتر است عضو دامنه باشند.
  - به خاطر داشته باشید CA ریشه می‌تواند روی ویندوز سرور 2008 نسخه Standard نصب شود. به علاوه بهتر است این سرور پس از نصب CA از شبکه خارج شود.
  - CA صادرکننده نسخه سازمانی باید روی ویندوز سرور 2008 نسخه Enterprise یا Datacenter نصب شود.
  - CA ریشه به دو درایو و CA صادرکننده به سه درایو نیاز دارد تا بتواند بانک اطلاعاتی گواهی‌نامه‌ها و گزارشات آنرا ذخیره کند.
- در صورت نصب سرویس NDES ما به یک حساب کاربری خاص نیاز داریم. یک حساب کاربری ساخت و آنرا عضو گروه IIS_IUSRS روی همه سرورهای میزبان این سرویس می‌کنیم. برای مثال نام این حساب می‌تواند NDESService باشد.
- کلاینت‌های درخواست کننده گواهی‌نامه نیز دراین سیستم حضور دارند.

حالا می‌توانیم به نصب سرویس بپردازیم. برای نصب CA ریشه منفرد مراحل زیر را انجام می‌دهیم.

تمرینات نصب سلسه مراتب CA

در این تمرین یک AD CS در دو لایه سلسله مراتبی خواهیم ساخت و NDES را برای AD CS نصب خواهیم کرد. برای انجام این تمرینات به سه سرور مجازی نیاز داریم

تمرین اول نصب AD CS بصورت یک CA ریشه مستقل

در این تمرین یک CA ریشه مستقل خواهیم ساخت که به عنوان ریشه ساختار سلسه مراتبی CA استفاده می شود این تمرین روی SERVER03 انجام خواهد شد. مطمئن می شویم که DC ما یعنی SERVER01 آماده سرویس دهی و SERVER03 جزو دامنه باشد.

۱- با اعتبار مدیر دامنه وارد SERVER03 می شویم

برای این کار اعتبار مدیر محلی نیز کافی است اما برای اهداف این تمرین از اعتبارمدیر دامنه استفاده می کنیم. این سرور می تواند دارای نسخه های Enterprise Edition، Standard Edition یا Datacenter Edition ویندوز سرور 2008 باشد

۲- Server Manager را از Administrative Tools اجرا می کنیم

۳- روی گره Roles در پنل راست کلیک کرده و Add Roles را انتخاب می کنیم

٤- اطلاعات Before You Begin را مرور کرده و روی Next کلیک می کنیم

٥- در صفحه Select Server Roles ، Active Directory Certificate Services را انتخاب و روی Next کلیک می کنیم

٦- در صفحه Introduction to Active Directory Certificate Services اطلاعات مربوط به نقش انتخاب شده را مرور کرده و روی Next کلیک می کنیم

۷- در صفحه Select Role Services ، Certification Authority را انتخاب کرده و روی Next کلیک می کنیم

چون این CA ریشه ماست و بعد از صدور CA از شبکه خارج می شود هیچ سرویس یا نقش دیگری به آن نمی دهیم

۸- در صفحه Specify Setup Type ، Standalone را انتخاب کرده و روی Next کلیک می کنیم

۹- در صفحه CA Type ، Root CA را انتخاب کرده و روی Next کلیک می کنیم

۱۰- در صفحه Set Up Private Key ، Create A New Private Key را انتخاب کرده و روی Next کلیک می کنیم

چون در حال ساخت یک CA ریشه جدید هستیم به ساخت یک کلید خصوصی جدید نیاز داریم در صورتی که در حال نصب مجدد یک CA بخاطر مشکلات پیش آمده باشیم باید از از یک کلید خصوصی موجود که در زمان راه اندازی سرور CA اصلی ساخته شده است استفاده کنیم. بعلاوه اگر CA ریشه را برای اتصال به یک CA خارجی غیر مایکروسافتی استفاده می کنیم باید از گزینه آخر استفاده کنیم. برای انتخاب این گزینه باید قبل از نصب AD CS آن کلید را روی سرور نصب کنیم

۱۱- در صفحه Configure Cryptography For CA ، suggested cryptographic service provider (CSP) را انتخاب می کنیم. طول کاراکترهای کلید را 2048 و hash algorithm را sha1 انتخاب می کنیم. همچنین گزینه Use Strong Private Key Protection Features را نیز انتخاب می کنیم. در این صفحه گزینه هایی وجود دارد:

- CSP ها موتور Crypto application programming interface (API) مایکروسافت هستند که برای ساخت جفت کلید برای این CA ریشه استفاده می شوند. CSP ها هم می توانند سخت افزاری باشند و هم نرم افزاری. برای مثال RSA#Microsoft Software Key Storage Provider نرم افزاری و RSA#Microsoft Smart Card Key Storage Provider سخت افزاری هستند
- طول کاراکتر کلید مشخص کننده طول هر دو کلید است که در چهار حالت امکان پذیر است. بخاطر داشته باشید که طول بیشتر کلید نیازمند پردازش بیشتر سرور برای رمزگشایی آن است.
- الگوریتم های HASH برای تولید و اختصاص دادن مقدار hash در کلیدها بکار می رود. چون این مقادیر به کلیدها داده می شود هرگونه دستکاری کلید آنهارا تغییر داده و کلید را نامعتبر می کند. مقادیر Hash حفاظت کلید را بعهده دارند. الگوریتمی که انتخاب می کنیم به سادگی از محاسبات متفاوتی برای ساخت مقدار Hash استفاده می کنند.
- آخرین گزینه در صفحه محافظت از ریشه CA را فراهم می کند چون با استفاده از آن CA تنها با اعتبار مدیریتی قابل دسترسی خواهد بود و تنها با این سطح از دسترسی کار خواهد کرد. از این گزینه برای فراهم کردن امنیت این CA ریشه استفاده می کنیم.

۱۲- روی Next کلیک می کنیم

۱۳- در صفحه Configure CA Name عبارت **Contoso-Root-CA را تایپ کرده و** distinguished name suffix را بدون تغییر می گذاریم و روی Next کلیک می کنیم

از این نام استفاده می کنیم چون این اسم در تمام گواهی نامه هایی که در زنجیره این CA صادر می شود قرار می گیرد

۱۴-در صفحه Set Validity Period ، مقدار سال را به ۲۰ تغییر داده و روی Next کلیک می کنیم

۱۵-در صفحه Configure Certificate Database محل ذخیره سازی پایگاه داده گواهی نامه و گزارش آن را مشخص می کنیم
چون این یک CAریشه است و فقط از آن برای ساختن گواهی نامه به منظور اعطاء به CA ها استفاده می شود می توان محل هر دو را در درایو D قرار داد

۱۶-برای محل پایگاه داده روی Browse کلیک کرده و به درایو D می رویم، روی Make New Folder کلیک می کنیم و نام آن را **CertData می گذاریم. روی OK کلیک می کنیم. برای گزارش ها یک پوشه در درایو D ساخته و نام آن را CertLogs می گذاریم.**
روی Next کلیک می کنیم

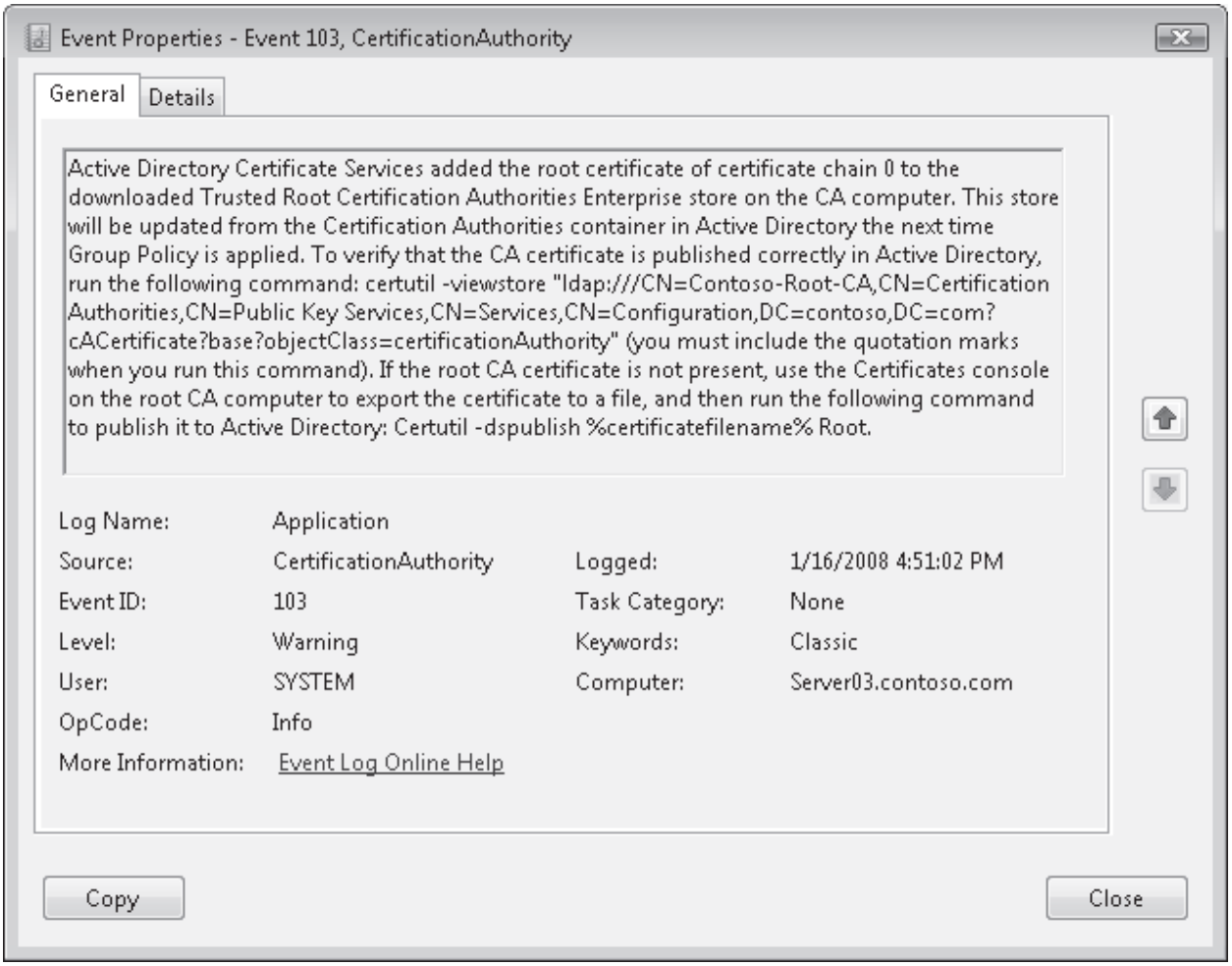
۱۷-اطلاعات صفحه AD CS را مرور کرده و روی Install کلیک می کنیم. هنگامی که نصب کامل شد نتایج نصب را مرور کرده و روی Close کلیک می کنیم

CA ریشه نصب شده است

باید بخاطر داشته باشیم که تا زمانی که AD CS را از روی سرور پاک نکنیم نمی توانیم نام سرور را عوض کنیم. این یکی از دلایلی است که از نام سرور در نام CA در مرحله ۱۲ استفاده نکردیم

به Server Manager بر می گردیم و نتایج نصب را مشاهده می کنیم برای مثال باید یک event ID 103 در صفحه summary نقش AD CS داشته باشیم (شکل ۶-۱۵) . این event نشان می دهد که نام CA در Certificate Authorities container در دامنه AD DS اضافه خواهد شد. همچنین دستوراتی را که میتوان با آنها اطلاعات دایرکتوری را بعد از اضافه شدن نام مشاهده کرد نشان می دهد.

بعد از بروز شدن چرخه Group Policy این CA را از شبکه جدا می کنیم. اکنون می توانیم اولین CA صادر کننده خود را نصب کنیم. برای بالا بردن امکان دسترسی ساختار AD CS باید بیش از یک CA صادرکننده نصب کنیم که فرآیند نصب همه آنها یکسان است



شکل ۶-۱۵ نمایش محتویات Event ID 103

تمرین دوم نصب یک **AD CS به عنوان Enterprise Issuing CA**

در این تمرین CA صادرکننده خود را نصب می کنیم. به طور معمول برای بالا بردن امکان دسترسی ساختار AD CS باید بیش از یک CA صادر کننده نصب کنیم، اما برای رسیدن به اهداف این تمرین به نصب یک CA اکتفا می کند. از کارکرد SERVER01 ، SERVER03 و SERVER04 اطمینان حاصل می کنیم.

۱- با اعتبار مدیر دامنه وارد SERVER03 می شویم

برای این کار اعتبار مدیر محلی نیز کافی است اما برای اهداف این تمرین از اعتبارمدیر دامنه استفاده می کنیم. این سرور می تواند دارای نسخه های Enterprise Edition، Standard Edition یا Datacenter Edition ویندوز سرور 20008 باشد

۲- Server Manager را از Administrative Tools اجرا می کنیم

۳- روی گره Roles در پنل راست کلیک کرده و Add Roles را انتخاب می کنیم

٤- اطلاعات Before You Begin را مرور کرده و روی Next کلیک می کنیم

٥- در صفحه Select Server Roles ، Active Directory Certificate Services را انتخاب و روی Next کلیک می کنیم

٦- در صفحه Introduction to Active Directory Certificate Services اطلاعات مربوط به نقش انتخاب شده را مرور کرده و روی Next کلیک می کنیم

۷- در صفحه Select Role Services ، Certificate Authority and Online Responder را انتخاب می کنیم

هنگامی که Online Responder را انتخاب می کنیم ویزارد از ما می خواهد که نقش Web Server را نیز اضافه کنیم روی Add Required Role Services کلیک می کنیم

۸- روی Next کلیک می کنیم

CA Web Enrollment را به این دلیل انتخاب نکردیم چون این یک enterprise CA داخلی است و Enterprise CA برای توزیع گواهی نامه از AD DS استفاده می کند. اگر این CA را در یک شبکه خارجی نصب می کردیم برای اینکه کاربران بتوانند درخواست certificate کنند باید از Web Enrollment استفاده می کردیم. به دلیل اینکه AD CS نصب همزمان CA و Network Device Enrollment Service (NDES) را پشتیبانی نمی کند در این زمان نمی توانیم NDES را نصب کنیم. در صورت نیاز به نصب NDES باید بعد از اتمام نصب CA با استفاده از Add Role Services آن را نصب کنیم

۹- در صفحه Specify Setup Type ، Enterprise را انتخاب می کنیم و روی Next کلیک می کنیم

۱۰- در صفحه Specify CA Type ، Subordinate CA را انتخاب کرده و روی Next کلیک می کنیم

۱۱- در صفحه Set Up Private Key ، Create A New Private Key را انتخاب کرده و روی Next کلیک می کنیم

۱۲- در صفحه Configure Cryptography For CA مقادیر پیش فرض را قبول کرده و روی Next کلیک می کنیم

۱۳- در صفحه Configure CA Name عبارت **Contoso-Issuing-CA01** را تایپ کرده و بدون تغییر پسوند DN ، روی Next کلیک می کنیم

باید از اعداد و شماره های معتبر استفاده کنیم چون قصد داریم برای بالا بردن تحمل خرابی CA صادر کننده های دیگری بسازیم

۱٤- در صفحه Request Certificate From A Parent CA ، Save A Certificate Request To File And Manually Send It Later را انتخاب می کنیم To A Parent CA

۱٥- Certificate Request Name را از فیلد File Name انتخاب کرده و با زدن Ctrl + C آنرا به clipboard کپی می کنیم، سپس با زدن Browse و رفتن به پوشه Documents بوسیله Ctrl + V آنرا در فیلد File Name، Paste می کنیم. Save را زده و روی Next کلیک می کنیم

۱٦- در صفحه Configure Certificate Database محل ذخیره سازی فایل پایگاه داده و گزارش را مشخص می کنیم

چون این CA جهت تست و آزمایش می باشد می توان هم فایل پایگاه داده و هم گزارش را در درایو D قرار داد اما در محیط واقعی سرور بسیار پر کار خواهد بود و این یعنی که باید پایگاه داده را در یک درایو و فایل گزارش را در یک درایو دیگر قرار دهیم.

۱۷- برای محل پایگاه داده روی Browse کلیک کرده و به درایو D می رویم روی Make New Folder کلیک می کنیم و نام آنرا **CertData** **گذاشته و روی OK کلیک می کنیم**

۱۸- **برای گزارشها یک پوشه با نام CertLogs در درایو D درست می کنیم ، سپس** روی Next کلیک می کنیم

۱۹- نصب IIS را مرور کرده و روی Next کلیک می کنیم

۲۰- در صفحه Web Server Role Services سرویسهای مورد نیاز را مرور کرده و روی Next کلیک می کنیم

۲۱- اطلاعات صفحه Confirm Installation Selections را مرور کرده و روی Install کلیک می کنیم

هنگامی که فرآیند نصب کامل شد نتایج نصب را مرور کرده و روی Close کلیک می کنیم. نصب subordinate CA تا زمان گرفتن یک گواهی از CA ریشه، غیر قابل فعال است و این گواهی برای کامل کردن نصب این subordinate CA بکار می رود.

تمرین سوم دریافت و نصب گواهی نامه از CA صادرکننده

اکنون برای کامل کردن فرآیند نصب CA صادر کننده باید گواهی نامه دریافت کنیم. در حالت عادی باید این کار خارج از شبکه روی یک دیسک قابل حمل مثل فلاپی درایو یا درایو USB فلش ، انجام داد اما برای اهداف این تمرین از یک پوشه اشتراکی استفاده می کنیم.

۱- در SERVER04 به درایو C رفته و یک پوشه جدید به نام **Temp در آن می سازیم**
۲- روی پوشه **Temp راست کلیک کرده و** Share را انتخاب می کنیم
۳- در کادر محاوره ای File Sharing در منوی بازشو Everyone را انتخاب کرده و روی Add کلیک می کنیم
۴- در ستون Permission Level از منوی بازشو نقش Contributor را به Everyone داده و روی Share کلیک می کنیم
۵- درخواست گواهی را که از پوشه Documents ساخته بودیم به پوشه Temp منتقل می کنیم
۶- در SEREVR03 کنسول Certificate Authority را از Administrative Tools اجرا می کنیم
۷- در کنسول Certification Authority روی CA ریشه کلیک راست کرده و All Tasks را انتخاب می کنیم و سپس Submit New Request را انتخاب می کنیم
۸- در کادر محاوره ای Open Request File به آدرس **\\SERVER04 \Temp رفته و هنگامی که پوشه باز شد** درخواست را انتخاب کرده و روی Open کلیک می کنیم
۹- به گره Pending Request رفته روی آن کلیک راست کرده و All Tasks را انتخاب می کنیم. سپس Issue را انتخاب می کنیم.
۱۰- در پنل به Issued Certificates رفته و در پنل سمت راست روی آن راست کلیک کرده و Open را انتخاب می کنیم
۱۱- در کادر محاوره ای Certificate زبانه Details را انتخاب کرده و در انتهای کادر محاوره ای روی Copy To File کلیک می کنیم
این کار باعث اجرای Certificate Export Wizard می شود
۱۲- روی Next کلیک می کنیم
۱۳- Cryptographic Message Syntax Standard – PKCS #7 Certificates (P7B) را انتخاب کرده و سپس Include All Certificates In The Certifications In The Certification Path If Possible را انتخاب کرده و روی Next کلیک می کنیم

چندین فرمت پشتیبانی شده وجود دارد:

- Distinguished Encoding Rules (DER) رمزگذاری شده با Binary X.509 که غالبا برای رایانه هایی با سیستم عاملی بجز ویندوز بکار می رود که فایلهای گواهی نامه با فرمت CER درست می کند
- Base-64 Encoded X.509 با پشتیبانی از S/MIME که برای جابجایی نامه الکترونیکی در اینترنت بکار می رود. در سرورها ، غالبا برای رایانه هایی با سیستم عاملی بجز ویندوز بکار می رود که فایلهای گواهی نامه با فرمت CER درست می کند
- Cryptographic Message Syntax Standard (PKCS #7) که برای جابجایی گواهی نامه ها در زنجیره رایانه ها استفاده می شود و از فایلهایی با فرمت P7B استفاده می کند
- Personal Information Exchange (PKCS #12) که این نیز برای جابجایی گواهی نامه ها از کامپیوتری به کامپیوتر دیگر استفاده می شود با این تفاوت که از انتقال کلید خصوصی درست همانند کلید عمومی پشتیبانی می کند. از این فرمت باید با احتیاط استفاده کرد چون جابجایی کلید عمومی می تواند آن را به خطر بیندازد. این فرمت از فایلهای PFX استفاده می کند
- Microsoft Serialized Certificate Store فرمت سفارشی شرکت مایکروسافت می باشد و باید زمانی استفاده شود که نیازمند جابجایی گواهی نامه ریشه از یک رایانه به دیگری هستیم. فرمت فایلهای این فرمت SST است

۱۴- در کادر محاوره ای File To Export روی Browse کلیک کرده و گواهی نامه را در آدرس \\SERVER04 \Temp با نام **Issuing-CA01.p7b ذخیره می کنیم**
۱۵- **هنگامی که به ویزارد برگشتیم** روی Next کلیک می کنیم
۱۶- تنظیمات را مرور کرده و روی Finish کلیک می کنیم
۱۷- هنگامی که پیام موفقیت بودن عملیات را مشاهده کردیم روی OK کلیک می کنیم. به SERVER04 یر می گردیم
۱۸- به Server Manager رفته و در پنل Contoso-Issuing-CA01 را انتخاب می کنیم
۱۹- روی Contoso-Issuing-CA01 راست کلیک کرده و All Tasks را انتخاب می کنیم سپس Install CA Certificate را انتخاب می کنیم
۲۰- به پوشه C:\Temp می رویم گواهی نامه را انتخاب کرده و روی Open کلیک می کنیم
۲۱- این باعث انتقال گواهی نامه و فعال شدن سرور می شود.
۲۲- روی نام سرور راست کلیک کرده و All Tasks و سپس Start Service را انتخاب می کنیم

سرور CA اکنون آماده صادر کردن گواهی نامه است. در حالت عادی در این زمان باید SERVER03 را از شبکه جدا کنیم اما چون این یک محیط آزمایشی می باشد و برای صرفه جویی در منابع آن این کار را نمی کنیم

تمرین چهارم آمادگی برای نصب NDES

۱- با اعتبار مدیر شبکه وارد SERVER01 می شویم
۲- Active Directory Users And Computers را از Administrative Tools اجرا می کنیم
۳- ساختار OU مانند روبرو می سازیم : Contoso.com\Admins\Service Identities
٤- روی Service Identities راست کلیک کرده ، اول New و بعد User را انتخاب می کنیم
٥- هم در کادر logon name و هم در کادر pre-Windows 2000 logon name نام **NDESService را وارد کرده و** روی Next کلیک می کنیم
٦- یک کلمه عبور پیچیده انتخاب وعلامت کادر User Must Change Password At Next Logon را برداشته و Password Never Expires را انتخاب می کنیم
۷- روی Next و سپس Finish برای ساخت حساب کلیک می کنیم
۸- با اعتبار مدیر شبکه دامنه وارد SERVER04 می شویم
۹- Active Directory Users And Computers را از Administrative Tools اجرا می کنیم
۱۰- به آدرس Configuration\Local Users and Groups\Groups می رویم
۱۱- روی گروه IIS_IUSRS دوبار کلیک می کنیم
۱۲- حساب NDESService را به این گروه اضافه کرده و روی OK کلیک می کنیم

تمرین پنجم نصب ویژگی NDES

اکنون برای نصب **NDES آماده هستیم**

۱- روی Active Directory Certificate Services در پنل Server Manager راست کلیک کرده و Add Role Services را انتخاب می کنیم
۲- در صفحه Select Role Services ، Network Device Enrollment Service را انتخاب می کنیم
۳- روی Add Required Role Services کلیک کرده و روی Next کلیک می کنیم
٤- در صفحه Specify User Account page روی Select User کلیک کرده و نام **NDESService را** همراه با کلمه عبورش وارد می کنیم و روی Next کلیک می کنیم
٥- در صفحه Specify Registration Authority Information نیازمند وارد کردن اطلاعاتی برای مرجعی که به منظور اعطاء و مدیریت گواهی نامه به قطعات شبکه استفاده می شود هستیم. عبارت **Contoso-MSCEP-RA01** را نوشته و از لیست کرکره ای کشورمان را انتخاب می کنیم بقیه اطلاعات را دست نخورده گذاشته و روی Next کلیک می کنیم. در حالت عادی باید تمام این اطلاعات را پر کنیم اما برای اهداف این تمرین همین قدر کفایت می کند
٦- در صفحه Configure Cryptography For Registration Authority ، بدون تغییر چیزی روی Next کلیک می کنیم
به خاطر داشته باشید که طول کلید در مصرف CPU تاثیر مستقیم دارد. بنابراین جز در موارد نیازمندی به امنیت بالا، طول کلید را ۲۰۴۸ نگه می داریم
۷- اطلاعات مربوط به نصب IIS را مرور کرده و روی Next کلیک می کنیم
۸- در صفحه Web Server Role Services سرویس های مورد نیاز را مرور کرده و روی Next کلیک می کنیم
۹- در صفحه Confirm Installation Services روی Install کلیک می کنیم
۱۰- وضعیت و روند نصب را زیر نظر می گیریم
۱۱- روی Close کلیک می کنیم
اکنون سرویس NDES نصب و آماده استفاده است

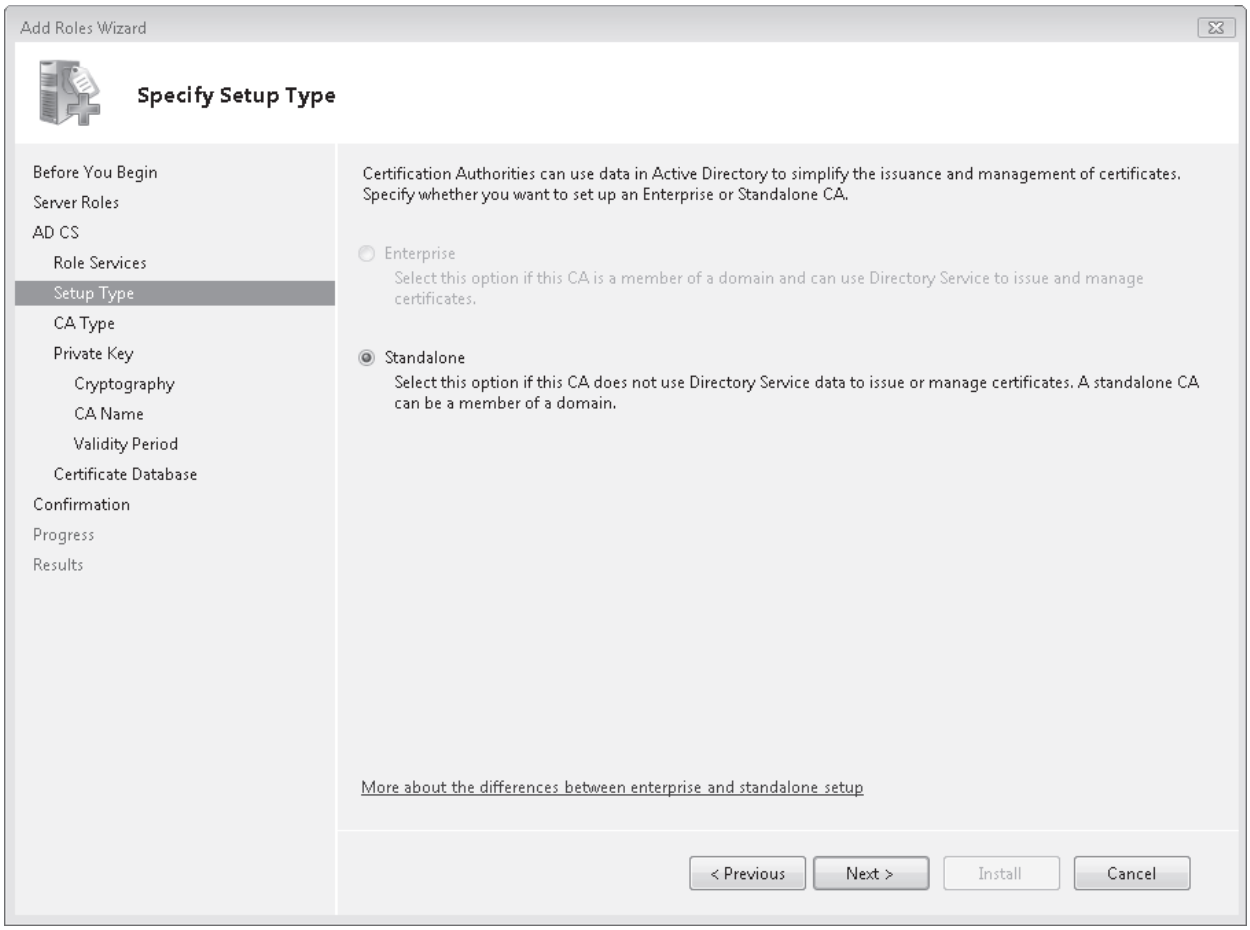
خلاصه درس

- AD CS ترکیبی از چهار رکن است : certificate authorities ، CA Web Enrollment ، online responders و Network Device Enrollment Service . اینها ارکان هر نوع توزیع AD CS هستند
- مراجع صدور گواهی نامه ها سرویس هایی هستند که برای صدور و مدیریت گواهی نامه ها بکار می روند. به خاطر ماهیت سلسله مراتبی PKI ، AD CS از هر دو نوع CA یعنی ریشه و subordinate پشتیبانی می کند. یک CA ریشه معمولا برای subordinate CA ها گواهی نامه صادر می کند که این کار به آنها این اجازه را می دهد که برای کاربران ، رایانه ها و قطعات گواهی نامه صادر کنند. subordinate CA ها تنها زمانی قادر به صدور certificate هستند که گواهی نامه خود آنها معتبر باشد، هنگامی که اعتبار گواهی نامه آنها تمام شود باید از CA ریشه درخواست تجدید گواهی نامه بدهند به همین دلیل زمان گواهی نامه ها در CA ریشه بسیار طولانی تر از subordinate CA ها می باشد. معمولا زمان اعتبار گواهی نامه در subordinate CA بیشتر از زمان گواهی نامه ای است که به کاربران ، رایانه ها و سرویس ها می دهند

- OR ها طراحی شده اند که درخواست اعتبارسنجی یک گواهی نامه مشخص با استفاده از Online Certificate Status Protocol (OCSP) را پاسخ دهند. به این وسیله سیستم با اتکا به PKI و بدون نیاز به داشتن یک CRL کامل می تواند به درخواست اعتبارسنجی یک گواهی نامه مشخص پاسخ دهد. OR درخواست اعتبارسنجی را رمزگشایی کرده و مشخص می کند که آیا گواهی نامه معتبر است یا نه. هنگامی که اعتبار گواهی نامه مشخص شد اطلاعات به صورت رمزگذاری شده به فرستنده درخواست برگردانده می شود. استفاده از OR ها بسیار سریعتر و کاربردی تر از استفاده از CRL ها می باشد. در ویندوز سرور 2008 ، AD CS حاوی ویژگی OR می باشد
- قطعاتی مانند روتر ها و سوییچها که از سیستم عامل های سطح پایین استفاده می کنند، با استفاده از SCEP که پروتکلی است که توسط شرکت سیسکو توسعه داده شده می توانند در یک PKI از طریق NDES دخالت کند. این قطعات معمولا دخالتی در دایرکتوری AD DS ندارند و بنابراین حساب AD DS هم ندارند. اگرچه از طریق NDES و SCEP ، می توانند به عنوان بخشی از ساختار سلسه مراتبی PKI در آید که با نصب AD CS مدیریت و نگهداری می شود.
- انواع سرورهای CA بسته به نوع ویندوز سرور 2008 ای است که استفاده می کنید. Standalone CA ها را می توان با نسخه های Standard Edition ، Enterprise Edition و Datacenter Edition ویندوز سرور 2008 نصب کرد. Enterprise CA ها نیز تنها با نسخه های Enterprise Edition و Datacenter Edition قابل نصب می باشد.

سئوالات پایان درس

۱- فرض کنید مدیر دامنه Contoso هستیم. رئیس شرکت تصمیم به توسعه Active Directory Certificate Services می گیرد و می خواهد که این کار امروز انجام شود. به او می گوییم که AD CS را بررسی کردیم و طبق دانش ما توسعه زیرساخت public key در یک روز امکان پذیر نمی باشد. بعد از کمی گفتگو رییس قانع می شود که باید ابتدا این نقش را در محیط آزمایشگاه نصب شود اما می خواهد در زمان نصب در محل حضور داشته باشد تا ببیند که کار چطور انجام می شود.او می خواهد که یک enterprise certificate authority نصب شود. می دانیم که سرور ما ویندوز سرور 2008 نسخه Enterprise Edition می باشد و نصب را از طریق Server Manager اجرا می کنیم. هنگامی که به صفحه Specify Setup Type می رسیم گزینه Enterprise CA غیرقابل دسترسی می باشد (شکل ۷-۱۵). مشکل چه می تواند باشد؟ (تمام گزینه های صحیح را انتخاب کنید)



شکل ۷-۱۵ صفحه Specify Setup Type مربوط به AD DS Installation Wizard

A . سرور ما نسخه Enterprise Edition ویندوز سرور 2008 نیست

B . با حسابی وارد سرور شده ایم که عضو دامنه نیست

C . سرور ما عضو دامنه AD DS نیست

D . از طریق Server Manager نمی توان یک enterprise CA نصب کرد

درس ۲: پیکربندی و استفاده از AD CS

پس از توزیع سرورها باید پیکربندی‌های مختلفی را روی آنها انجام دهیم تا بتوانند گواهی‌نامه صادر و مدیریت کنند. فعالیت‌های مختلف مورد نیاز عبارتند از:

- برای صدور و نگهداری از گواهی‌نامه‌ها باید پیکربندی CA های صادرکننده را به اتمام برسانیم.
- برای OR که بتواند به درخواست‌ها پاسخ دهد باید پیکربندی OR را تکمیل کنیم.
- برای پشتیبانی از enrollment دستگاههای شبکه باید پیکربندی NDES را روی CA صادرکننده انجام دهیم.
- پس از همه پیکربندی‌های ذکرشده باید عملکرد CA ب طور کامل بررسی شود.

پس از این درس می‌توانیم:

- پیکربندی لغو گواهی‌نامه را انجام دهیم
- با تنظیمات سرور CA کار کنیم.
- با الگوهای گواهی‌نامه کار کنیم
- CA را با هدف صدور OCSP response signing certificate پیکربندی کنیم.
- Enrollment گواهی‌نامه را مدیریت کنیم.
- لغو گواهی‌نامه را مدیریت کنیم.

زمان تقریبی : ۴۰ دقیقه

تکمیل پیکربندی CA صادرکننده گواهی

تکمیل مراحل پیکربندی CA صادرکننده به صورت زیر است:

- ابتدا پیکربندی لغو گواهی‌نامه را انجام می‌دهیم.
- الگوهای گواهی‌نامه را با توجه به عوامل زیر پیکربندی می‌کنیم:
  - اگر بخواهیم از EFS به منظور محافظت از داده‌ها استفاده کنیم باید پیکربندی لازم را انجام دهیم. در این‌صورت عامل بازیابی (recovery egent) برای آن در نظر می‌گیریم که در صورت گم شدن کلید EFS کاربر بتوانیم آنرا بازیابی کنیم.
  - اگر بخواهیم شبکه‌های بیسیم را با گواهی‌نامه محافظت کنیم باید گواهی‌نامه‌های مربوط به شبکه بیسیم را پیکربندی کنیم. این کار باعث می‌شود تایید هویت و رمزنگاری دستگاههای بیسیم خیلی قوی شود.
  - اگر بخواهیم از کارت‌های هوشمند استفاده کنیم تا تایید هویت به صورت two-factor انجام شود.

- اگر بخواهیم از وب‌سایت‌ها و تجارت الکترونیک سازمان محافظت کنیم باید گواهی‌نامه مربوط به سرور وب را نیز پیکربندی کنیم. همچنین می‌توانیم از این نوع گواهی‌نامه برای محافظت از DC ها و رمزنگاری همه ارتباطات مرتبط با آنها استفاده کنیم.

- سپس گزینه‌های ثبت نام و صدور گواهی‌نامه را پیکربندی می‌کنیم.

همه این عملیات روی CA صادرکننده به طور مستقیم یا از طریق Remote Server Administration Tools (RSAT) گواهی اتفاق می‌افتد.

پیکربندی لغو یک CA

لغو یکی از روش‌های جلوگیری از سوء استفاده از گواهی‌نامه می‌باشد. به همین دلیل قبل از صدور گواهی‌نامه باید این ویژگی پیکربندی شود.

برای انجام این کار مراحل زیر را دنبال می‌کنیم:

- نقاط توزیع CRL را مشخص می‌کنیم.

- بازه‌های زمانی هم‌پوشانی CRL و Delta CRL را پیکربندی می‌کنیم.

- انتشار CRL ها را زمان‌بندی می‌کنیم.

با نقاط توزیع CRL شروع می‌کنیم. پیکربندی لغو در کنسول مرجع گواهی‌نامه اجرا می‌شود.

۱. به سرور CA صادرکننده با کاربر دامنه که دسترسی مدیریتی محلی نیز دارد وارد می‌شویم.

۲. کنسول Certification Authority را از گروه برنامه‌های Administrative Tools اجرا می‌کنیم.

۳. روی نام CA صادرکننده کلیک راست کرده و Properties را انتخاب می‌کنیم.

۴. درکادر محاوره‌ای Properties روی زبانه Extensions کلیک کرده و در لیست بازشوی Select Extension گزینه CRL Distribution Point را انتخاب می‌کنیم. همچنین چک می‌کنیم کادرهای Publish CRLs To This Location Point و Publish Delta CRLs To This Location علامت داشته باشند.

۵. روی OK کلیک می‌کنیم. وقتی تغییری در پیکربندی CA ایجاد می‌کنیم پیغامی مبنی بر توقف و اجرای دوباره سرویس AD CS مشاهده می‌کنیم. روی Yes کلیک می‌کنیم.

حالا می‌رسیم به پیکربندی بازه زمانی هم‌پوشانی CRL و Delta CRL . این کار با دستور Certutil.exe انجام می‌شود.

۱. روی سرور CA صادرکننده پنجره خط فرمان elevated را باز کرده و دستورات زیر را اجرا می‌کنیم:

```
certutil -setreg ca\CRLOverlapUnits value
certutil -setreg ca\CRLOverlapPeriod units
certutil -setreg ca\CRLDeltaOverlapUnits value
certutil -setreg ca\CRLDeltaOverlapPeriod units
```

Value مقدار مورد نظر برای تنظیم بازه زمانی هم‌پوشانی می‌باشد و units شامل دقیقه، ساعت یا روز می‌باشد. برای مثال می‌توانیم بازه زمانی هم‌پوشانی را روی ۲۴ ساعت و بازه زمانی انتشار Delta CRL را روی ۱۲ ساعت تنظیم کنیم. برای این کار دستورات زیر را به کار می‌بریم:

```
certutil  -setreg ca\CRLOverlapUnits 24
```

certutil -setreg ca\CRLOverlapPeriod hours
certutil -setreg ca\CRLDeltaOverlapUnits 12
certutil -setreg ca\CRLDeltaOverlapPeriod hours

۲. کنسول Certification Authority را باز کرده و روی نام سرور CA صادرکننده کلیک راست کرده و سرویس را متوقف و دوباره اجرا می‌کنیم.

در نهایت انتشار CRL را پیکربندی می‌کنیم.

۱. در کنسول Certification Authority گره زیر نام سرور CA صادرکننده را باز می‌کنیم.

۲. روی Revoked Certificates کلیک راست کرده و Properties را انتخاب می‌کنیم.

۳. در زبانه CRL Publishing Parameters دوره انتشار CRL و Delta CRL را تنظیم می‌کنیم. به طور پیش‌فرض دو مقدار روی به ترتیب یک هفته و یک روز تنظیم شده‌اند. برای افزایش کارایی صدور گواهی‌نامه و دسترس‌پذیری CRL ها بهتر است هر دو مقدار را کاهش دهیم. در زبانه View CRLs می‌توانیم CRL های موجود را ببینیم.

۴. روی OK کلیک می‌کنیم.

پیکربندی لغو گواهی‌نامه به اتمام می‌رسد.

پیکربندی و سفارشی کردن الگوهای گواهی‌نامه

الگوهای گواهی‌نامه به منظور تولید گواهی استفاده می‌شود. CA های سازمانی از الگوهای نسخه ۲ و ۳ استفاده می‌کنند. این نوع الگوها به ما اجازه ویرایش را می‌دهد. الگوها را برای مقاصد مختلف آماده می‌کنیم برای این کار ابتدا باید هر الگو را به طور جداگانه پیکربندی کنیم و بعد آنرا روی CA توزیع کنیم. الگوها پس از توزیع آماده‌اند که از آنان برای صدور گواهی‌نامه استفاده کنیم. شروع کار با تعیین الگوی مورد نظر بوده و سپس کار را به شکل زیر ادامه می‌دهیم.

۱. با کاربر administrator دامنه به سرور CA صادرکننده وارد می‌شویم.

۲. کنسول Server Manager را باز می‌کنیم.

۳. گره Roles\Active Directory Certificate Services\Certificate Templates (server name) را باز می‌کنیم.

۴. توجه داشته باشید که الگوهای موجود در پنل وسط لیست شده‌اند.

۵. توجه کنید که به طور پیش‌فرض به یک DC متصل هستیم. برای کار با الگوها باید به یک سرور DC متصل باشیم به طوری که الگوها بتوانند روی AD DS انتشار یابند.

۶. اگر متصل نبودیم در پنل راست روی Connect To Another Writable Domain Controller کلیک می‌کنیم. حالا آماده ساخت الگو هستیم.

۷. الگوی منبع را انتخاب کرده روی الگو کلیک راست کرده تا Duplicate Template را انتخاب کنیم و سپس نسخه ویندوز سرور را انتخاب می‌کنیم. همیشه نسخه ویندوز سرور 2008 را انتخاب می‌کنیم مگر اینکه از ساختار PKI مختلط استفاده کنیم.

۸. نام الگو را انتخاب کرده آنرا سفارشی کرده و ذخیره می‌کنیم. بهتر است سفارشی سازی بر مبنای راهنمای زیر انجام شود:

- برای ساخت الگوی EFS الگوی Basic EFS را به عنوان منبع انتخاب کرده آنرا برای ویندوز سرور 2008 تکثیر کرده و نام آنرا تعیین می‌کنیم. بهتر است نام معتبری تعیین کنیم مثلا Basic EFS WS08 و سپس در زبانه‌های آن محتوا را ویرایش کنیم. در زبانه Request Handling به بایگانی کلید توجه کرده و مطمئن می‌شویم کادر Archive Subject Encryption Private Key علامت دارد. همچنین برای ارسال کلید به CA از رمزنگاری استفاده می‌کنیم. انباره بایگانی کلیدهای خصوصی به محافظت از آن حتی زمانی که کاربر آنرا گم می‌کند کمک

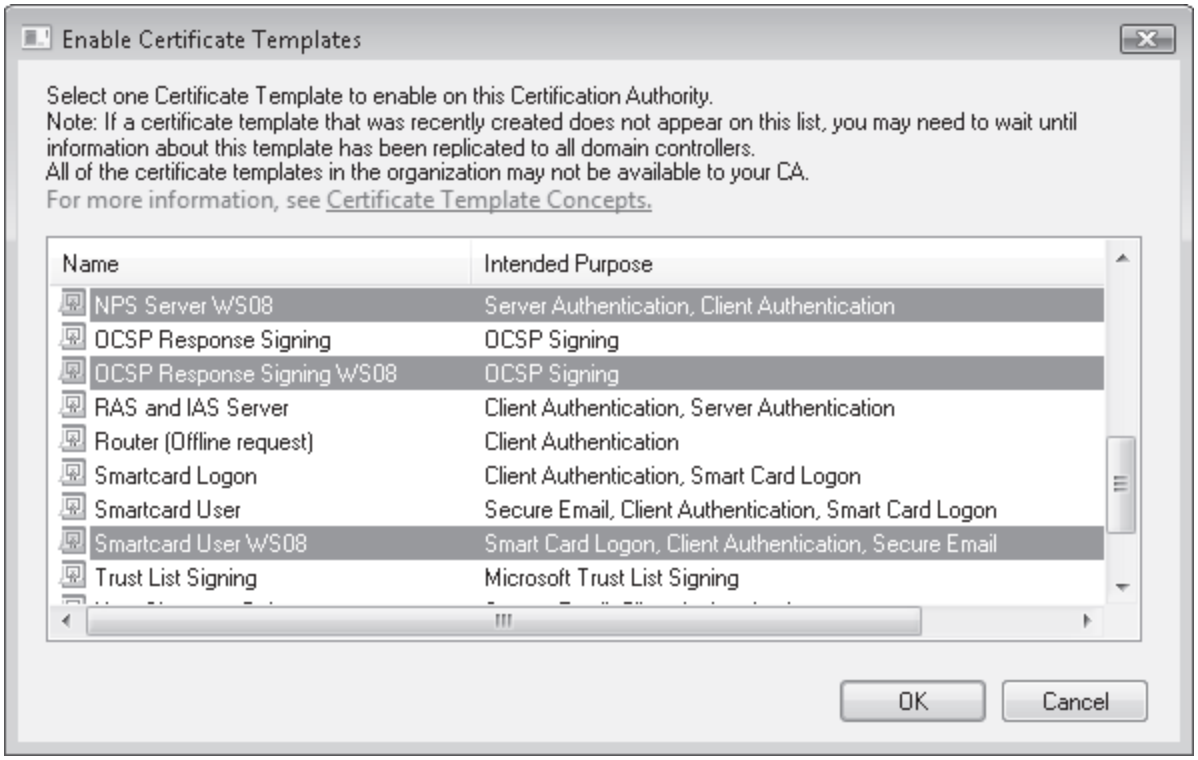
می‌کند. همچنین می‌توانیم در زبانه Subject Name اطلاعاتی نظیر مقادیر Alternate Subject Name را اضافه کنیم. روی OK کلیک می‌کنیم.

- اگر می‌خواهیم از EFS استفاده کنیم باید یک الگوی EFS Recovery Agent نیز بسازیم. آنرا برای ویندوز سرور 2008 تکثیر می‌کنیم. نام آنرا یک نام بامسمی نظیر EFS Recovery Agent WS08 می‌گذاریم. گواهی‌نامه recovery agent را در Active Directory منتشر می‌کنیم. توجه داشته باشید که دوره این گواهی از خود گواهی EFS بیشتر است. بقیه تنظیمات زبانه‌های دیگر مانند Basic EFS است.
- اگر می‌خواهیم از شبکه‌های بیسیم استفاده کنیم یک الگوی Network Policy Server (NPS) می‌سازیم. اساسا ما الگو را می‌سازیم و پیکربندی می‌کنیم تا فرایند ثبت به طور خودکار انجام شود. سپس دفعه بعد که تنظیمات Group Policy سرورهای NPS به روز شود گواهی‌نامه جدید خواهد گرفت. از الگوهای RAS و IAS Server به عنوان منبع برای الگوی جدید NPS خود استفاده می‌کنیم. بعد آنرا برای ویندوز سرور 2008 تکثیر می‌کنیم. نام مناسبی برای آن انتخاب می‌کنیم مانند NPS Server WS08 . آنرا در Active Directory منتشر می‌کنیم. به زبانه Security رفته و گروه RAS و IAS Servers را انتخاب می‌کنیم تا هم Autoenroll و هم مجوزهای Enroll را تعیین کنیم. زبانه‌های دیگر را در صورت نیاز باز کرده و در نهایت باز کرده و الگو را ذخیره می‌کنیم.
- اگر بخواهیم از کارت‌های هوشمند استفاده کنیم از الگوهای Smartcard Logon و Smartcard User کپی تهیه می‌کنیم. کپی‌ها را برای ویندوز سرور 2008 تنظیم می‌کنیم. نام آنهارا انتخاب کرده و در Actvie Directory منتشر می‌کنیم. ما برای این گواهی‌ها از ثبت خودکار استفاده نمی‌کنیم به دلیل اینکه باید از ایستگاههای ثبت‌نام کارت هوشمند برای توزیع خود کارت‌های هوشمند بین کاربران استفاده کنیم.
- اگر بخواهیم از سرورهای وب یا DC ها محافظت کنیم از الگوهای Web Server و Domain Controller Authentication کپی می‌گیریم. از الگوی Domain Controller نباید استفاده کنیم به دلیل اینکه برای نسخه‌های قبلی سیستم عامل طراحی شده‌اند. آنها را برای ویندوز سرور 2008 تکثیر می‌کنیم، در Active Directory منتشر می‌کنیم و خصوصیات دیگر آنها را بررسی می‌کنیم. حالا که الگو آماده است باید الگو را صادر کنیم تا CA بتواند کار صدور گواهی‌نامه‌ها را بر اساس این الگو انجام دهد.

۹. در Server Manager گره Roles\Active Directory Certificate Services\Issuing CA Name\Certificate Templates را باز می‌کنیم.

۱۰. برای صدور یک الگو روی Certificate Templates کلیک راست کرده و New و سپس Certificate Template To Issue را انتخاب می‌کنیم.

۱۱. در کادر محاوره‌ای Enable Certificate Templates از کلیدهای Ctrl و کلیک استفاده می‌کنیم تا همه الگوهای مورد نظر را انتخاب کنیم و سپس روی OK کلیک می‌کنیم. (شکل ۸- ۱۵)



شکل ۸- ۱۵ کادر محاوره‌ای Enable Certificate Templates

حالا می‌توانیم پیکربندی ثبت را انجام دهیم. این کار از طریق Group Policy انجام می‌شود. سیاست باید به همه اعضاء دامنه نسبت داده شود بنابراین Default Domain Policy می‌تواند بهترین انتخاب باشد یا اگر نخواهیم این سیاست را ویرایش کنیم سیاست جدیدی ساخته و آنرا به تمام دامنه نسبت می‌دهیم.

۱. به سرور DC وارد شده و از گروه برنامه‌های Administrative Tools کنسول Group Policy Management را باز می‌کنیم.
۲. سیاست مورد نظر را پیدا کرده یا می‌سازیم و روی آن کلیک راست کرده و Edit را انتخاب می‌کنیم.
۳. برای انتساب enrollment برای کامپیوترها گره Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies را باز می‌کنیم.
۴. روی Certificate Services Client-Auto-Enrollment دوبار کلیک می‌کنیم.
۵. سیاست را فعال کرده و کادر Renew Expired Certificates, Update Pending Certificates, And Remove Revoked Certificates را علامت می‌زنیم.
۶. اگر قبلا به صورت دستی گواهی‌نامه صادر کرده باشیم کادر Update Certificates That Use Certificate Templates را علامت زده و برای اعمال تنظیمات روی OK کلیک می‌کنیم.
۷. برای تنظیم ثبت خودکار برای کاربران گره User Configuration\Polices\Windows Settings\Security Settings\Public Key Policies را باز می‌کنیم.
۸. سیاست را فعال کرده و گزینه‌ها را مانند کامپیوترها انتخاب می‌کنیم.
۹. توجه داشته باشید که می‌توانیم Expiration Notification را برای کاربران فعال کنیم و مقدار مناسب به آن اختصاص دهیم. این کار باعث می‌شود به کاربران وقتی به زمان انقضاء نزدیک شوند پیغام هشدار داده شود.
۱۰. روی OK کلیک کرده تا تنظیمات اعمال شود.
۱۱. کنسول را می‌بندیم.
۱۲. به CA صادرکننده برمی‌گردیم و Server Manager را باز کرده و رفتار CA را زمان دریافت درخواست گواهی‌نامه مشخص می‌کنیم.
۱۳. روی نام سرور CA صادرکننده زیر AD CS کلیک راست کرده و Properties را انتخاب می‌کنیم.

۱۴. زبانه Policy Module را باز کرده و روی دکمه Properties کلیک می‌کنیم.
۱۵. برای صدور خودکار گواهی‌نامه گزینه Follow The Settings In The Certificate Template, If Applicable. Otherwise, Automatically Issue The Certificate را انتخاب می‌کنیم. روی OK کلیک می‌کنیم.
۱۶. یکبار دیگر روی OK کلیک می‌کنیم تا کادر بسته شود.

حالا CA صادرکننده آماده صدور گواهی خواهد بود.

تکمیل پیکربندی OR

OR می‌تواند آرایه‌ای از سیستم‌ها را به منظور پایداری سرویس ایجاد کند. یک آرایه می‌تواند از دو CA با وظیفه OR یا تعداد بیشتری سرور تشکیل شود.

برای تکمیل پیکربندی OR باید گواهی OCSP Response Signing را نصب و پیکربندی کرده و یک Authority Information Access extension برای پشتیبانی از آن پیکربندی کنیم. سپس باید یک الگو را به یک CA نسبت داده و سیستم را برای دریافت گواهی ثبت کنیم. از مراحل زیر برای پیکربندی OCSP Response Signing Certificate استفاده می‌کنیم.

۱. با کاربر عضو دامنه با دسترسی مدیریتی محلی به سرور CA صادرکننده وارد می‌شویم.
۲. در Server Manager گره Roles\Active Directory Certificate Services\Certificate Templates (servername) را باز می‌کنیم.
۳. روی الگوی OCSP Response Signing کلیک راست کرده و روی Duplicate Template کلیک می‌کنیم. یک الگوی ویندوز سرور 2008 نسخه Enterprise انتخاب و روی OK کلیک می‌کنیم.
۴. یک نام با مسمی برای الگو انتخاب می‌کنیم مانند OCSP Response Signing WS08.
۵. کادر Publish Certificate in Active Directory را علامت می‌زنیم.
۶. در زبانه Security زیر Group Or User Name روی Add بعد روی Object Types کلیک می‌کنیم تا نوع شیء Computer فعال شود و روی OK کلیک می‌کنیم.
۷. نام مورد نظر را تایپ کرده و روی Check Names کلیک می‌کنیم تا کامپیوتر میزبان OR را پیدا کنیم. روی OK کلیک می‌کنیم.
۸. روی نام کامپیوتر کلیک کرده و سپس در بخش Permissions از کادر محاوره‌ای گزینه‌های Allow:Read, Enroll, Autoenroll را انتخاب می‌کنیم.
۹. روی OK کلیک می‌کنیم تا instance از روی الگو ساخته شود.

الگوی گواهی‌نامه آماده است. حالا باید Authority Information Access (AIA) Extension را برای پشتیبانی از OR پیکربندی کنیم.

۱. با کاربر عضو دامنه با دسترسی مدیریتی محلی به سرور CA صادرکننده وارد می‌شویم.
۲. از گروه برنامه‌های Administrative Tools برنامه Server Manager را اجرا می‌کنیم.
۳. گره Roles\Active Directory Certificate Services\Issuing CA servername را باز می‌کنیم.
۴. در پنل Actions گزینه Properties را انتخاب می‌کنیم.
۵. روی زبانه Extensions و لیست بازشوی Select Extension کلیک کرده و بعد روی Authority Information Access (AIA) کلیک می‌کنیم.
۶. محل دریافت داده‌های لغو گواهی را مشخص می‌کنیم. در این موارد محل آن با HTTP:// شروع می‌شود.
۷. کادرهای Include In The AIA Extension Of Issued Certificates و Include In The Online Certificate Status Protocol (OCSP)را علامت می‌زنیم.
۸. روی OK کلیک می‌کنیم. حالا برای اعمال تغییرات باید سرویس AD CS را متوقف و دوباره اجرا کرد.
۹. در کادر محاوره‌ای روی Yes کلیک می‌کنیم.
۱۰. حال به Certificate Templates زیر نام CA صادرکننده رفته و روی آن کلیک راست کرده New را انتخاب می‌کنیم و سپس Certificate Template To Issue را انتخاب می‌کنیم.

۱۱. در کادر محاوره‌ای Enable Certificate Templates الگوی جدید OCSP Response Signing را که قبلا ساختیم انتخاب کرده و روی OK کلیک می‌کنیم.
۱۲. برای نسبت دادن الگو به سرور آنرا راه‌اندازی مجدد می‌کنیم. برای بررسی صحت کارکرد یک کنسول سفارشی برای Certificate می‌سازیم.
۱۳. منوی Start را باز کرده و در کادر جستجو mmc را تایپ می‌کنیم.
۱۴. در کنسول از منوی File ابزار Add/Remove Snap-in را انتخاب می‌کنیم. کادر محاوره‌ای باز می‌شود.
۱۵. ابزار Certificate را انتخاب کرده و روی Add کلیک می‌کنیم.
۱۶. Computer Account را انتخاب و روی Next کلیک می‌کنیم.
۱۷. Local Computer را انتخاب و روی Finish کلیک می‌کنیم.
۱۸. روی OK کلیک می‌کنیم تا کادر بسته شود.
۱۹. برای ذخیره کنسول از منوی File روی Save کلیک می‌کنیم و آنرا در پوشه Documents ذخیره می‌کنیم. نام کنسول را Comuter Certificates می‌گذاریم.
۲۰. گره Certificates\Personal\Certificates را باز کرده و بررسی می‌کنیم که آیا گواهی جدید OCSP موجود است یا نه
۲۱. اگر گواهی‌نامه موجود نباشد با کلیک راست روی Certificates زیر Personal و انتخاب All Tasks و سپس Request New Certificate آنرا نصب می‌کنیم.
۲۲. در صفحه Certificate Enrollment روی Next کلیک می‌کنیم.
۲۳. گواهی‌نامه جدید OCSP را انتخاب کرده و روی Enroll کلیک می‌کنیم.
۲۴. در صفحه بعد روی فلش روبه پایین کنار Details کلیک کرده و بعد روی View Certificate کلیک می‌کنیم. در زبانه‌های مختلف جزئیات مربوط به گواهی‌نامه را مشاهده می‌کنیم. روی OK کلیک می‌کنیم.
۲۵. روی Finish کلیک می‌کنیم تا این بخش از عملیات تمام شود.
۲۶. روی Certificate کلیک راست کرده، All Tasks و سپس Manage Private Keys را انتخاب می‌کنیم.
۲۷. در زبانه Security زیر User Group Or User Names روی Add کلیک می‌کنیم.
۲۸. در کادر محاوره‌ای Users, Computers, or Groups روی Locations کلیک کرده و نام سرور محلی را انتخاب می‌کنیم. سپس روی OK کلیک می‌کنیم.
۲۹. عبارت Network Service را تایپ کرده و روی Check Names کلیک می‌کنیم.
۳۰. روی OK کلیک می‌کنیم.
۳۱. روی Nerwork Service کلیک می‌کنیم و بعد در بخش Permissions از کادر محاوره‌ای Allow: Full Control را انتخاب می‌کنیم.
۳۲. روی OK کلیک می‌کنیم تا کادر بسته شود.

حالا OR آماده ارائه اطلاعات اعتبار گواهی است.

توجه داشته باشید که گره Online Responder در Server Manager حاوی یک گره Array Configuration می‌باشد. وقتی یک OR دیگر اضافه می‌شود می‌توانیم آنرا به این پیکربندی آرایه‌ای اضافه کنیم تا سرویس OR را پایدار سازیم. سازمان‌های با ساختار چندلایه سلسله‌مراتبی دارای آرایه‌های OR بزرگ می‌باشند که همه کاربران و دستگاههایشان به راحتی می‌توانند اعتبار گواهی‌نامه‌هایشان را بررسی کنند.

پیکربندی لغو برای یک OR

وقتی OR آماده شد یک پیکربندی لغو برای آن اضافه می‌کنیم. به دلیل اینکه CA که در آرایه OR هم هست گواهی‌نامه خود را داراست به پیکربندی لغو هم نیاز دارد. پیکربندی لغو به درخواست‌های جفت کلیدهای CA مشخص و گواهی‌نامه‌ها سرویس می‌دهد. به علاوه هر گاه که جفت کلید به روز می‌شود باید پیکربندی لغو نیز برای CA به روز شود. به منظور پیکربندی لغو مراحل زیر را دنبال می‌کنیم:

۱. با کاربر دامنه که دسترسی مدیریتی محلی دارد به CA صادرکننده وارد می‌شویم.

۲. از گروه برنامه‌های Administrative Tools کنسول Server Manager را باز می‌کنیم.
۳. گره Roles\Active Directory Certificate Services\Online Responder\Revocation Configuration را باز می‌کنیم.
۴. روی Revocation Configuration کلیک راست کرده و Add Revocation Configuration را انتخاب می‌کنیم.
۵. در صفحه Welcome روی Next کلیک می‌کنیم.
۶. در صفحه Name Revocation Configuration یک نام معتبر بامسمی می‌کنیم. به دلیل اینکه هر پیکربندی لغوی به یک CA منتسب است بهتر است نام CA را روی پیکربندی بگذاریم مثلا RCSERVER04 .
۷. روی Next کلیک می‌کنیم.
۸. در صفحه Select CA Certificate Location مشخص می‌کنیم که گواهی از کجا بارگذاری شود. گواهی می‌تواند از Active Directory، انباره گواهی محلی یا از یک فایل بارگذاری شود
۹. Select A Certificate For An Existing Enterprise CA را انتخاب و Next را کلیک می‌کنیم. حالا OR باید صادرکننده گواهی را بررسی کند که در اینجا CA ریشه است تا ببیند دارای گواهی‌نامه معتبر است یا نه.
۱۰. به دلیل اینکه CA ریشه از شبکه خارج است Active Directory را انتخاب کرده و روی Browse کلیک می‌کنیم.
۱۱. گواهی مربوط به CA ریشه را پیدا کرده و روی OK کلیک می‌کنیم. بعد از اینکه گواهی انتخاب شد ویزارد الگوهای Online Responder signing را بارگذاری می‌کند.
۱۲. روی Next کلیک می‌کنیم. به دلیل اینکه OR قبل از ارسال، پاسخ‌ها به کلاینت را علامت می‌زند در صفحه Select A Signing Certificate باید یک روش علامت‌گذاری را انتخاب کنیم یعنی یکی از سه روش زیر:
   - انتخاب خودکار از الگوی OCSP که قبلا ساخته‌ایم یک گواهی را بارگذاری می‌کند
   - یک گواهی به صورت دستی انتخاب می‌شود.
   - CA Certificate گواهی را از خودش به کار می‌گیرد.
۱۳. Automatically Select A Signing Certificate و بعد Auto-Enroll را برای یک گواهی OCSP signing انتخاب می‌کنیم.
۱۴. CA صادرکننده را انتخاب می‌کنیم. روی OK کلیک می‌کنیم. این کار به طور خودکار الگویی را که قبلا آماده کردیم انتخاب می‌کند.
۱۵. روی Next کلیک می‌کنیم. حالا ویزارد Provider لغو را راه‌اندازی می‌کند اگر به هر دلیلی آنرا پیدا نکند باید به صورت دستی Provider را اضافه کنیم.
۱۶. روی Provider و سپس Add زیر Base CRLs کلیک می‌کنیم. برای مثال http://localhost/ca.crl.
۱۷. روی OK کلیک می‌کنیم. این مراحل را برای Delta CRLs تکرار کرده و همان آدرس HTTP را استفاده می‌کنیم. روی OK کلیک می‌کنیم. به دلیل اینکه گواهی از Active Directory تهیه می‌شود آدرس Provider در قالب ldap:// بوده و به طور خودکار توسط ویزارد مشخص می‌شود. AD CS برای دریافت اطلاعات از انباره دایرکتوری AD DS از پروتکل LDAP استفاده می‌کند.
۱۸. روی Finish کلیک می‌کنیم.

حالا ما باید یک پیکربندی لغو جدید در لیست پنل وسط داشته باشیم. برای CA های دیگر هم که OR هستند همین مراحل را تکرار می‌کنیم.

ابزارهای مدیریت AD CS

سرویس‌های نقش AD CS توسط ابزارهای MMC مدیریت می‌شوند. جدول ۴- ۱۵ ابزارهایی را که تاکنون دراین فصل استفاده کرده‌ایم لیست می‌کند که بیشتر آنها از طریق Server Manager باز می‌شوند.

جدول ۴- ۱۵ ابزارهای مدیریت AD CS

ابزار	موارد استفاده	محل

Certification Authority	مدیریت یک مرجع گواهی‌نامه	Server Manager
Certificates	مدیریت گواهی‌نامه‌ها. این ابزار به طور پیش‌فرض نصب می‌شود	ابزار MMC سفارشی
Certificate Templates	مدیریت الگوهای گواهی‌نامه	Server Manager
Online Responder	مدیریت OR	Server Manager
Enterprise PKI	مدیریت کل زیرساخت PKI	Server Manager
Certutil	مدیریت عملکرد PKI از طریق خط فرمان	خط فرمان

وقتی با AD CS کار می‌کنیم می‌بینیم که حجم عظیمی از اطلاعات را به صورت گزارش Event Log می‌دهد. جدول ۵- ۱۵ رایج‌ترین وقایع مراجع گواهی AD CS را لیست می‌کند.

جدول ۵- ۱۵ Event ID های مهم مراجع گواهی‌نامه

گروه	Event ID	توضیحات
AD CS Access Control	39, 60, 92	عدم وجود مجوز مناسب
AD CS and AD DS	24, 59, 64, 91, 93, 94, 106, 107	دسترسی خواندنی و نوشتنی برای اشیاء AD DS
AD CS Certificate Request (Enrollment) Processing	3, 7, 10, 21, 22, 23, 53, 56, 57, 79, 80, 97, 108, 109, 128, 132	یکی از اجزاء مورد نیاز certificate enrollment : گواهی‌نامه CA معتبر، الگوهای گواهی با پیکربندی مناسب، حساب‌های کلاینت‌ها یا درخواست‌های گواهی
AD CS Certification Authority Certificate and Chain Validation	27, 31, 42, 48, 49, 51, 58, 64, 100, 103, 104, 105	پایداری، اعتبار و تایید اعتبار زنجیره‌ای برای یک گواهی CA
AD CS Certification Authority Upgrade	111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 125, 126	ارتقاء مرجع گواهی از نسخه قدیمی به ویندوز سرور 2008 که می‌توان گزینه‌هایا اجزاء پیکربندی را دوباره تنظیم کرد.
AD CS Cross-Certification	99, 102	گواهی‌نامه‌های از نوع cross-CA که برای ارتباط بین گواهی اصلی و ریشه به کار می‌رود.
AD CS Database Availability	17	مشکلات دسترسی به بانک CA
AD CS Exit Module Processing	45, 46	Exit module function : اطلاع رسانی از طریق پست الکترونیک یا انتشار
AD CS Key Archival and Recovery	81, 82, 83, 84, 85, 86, 87, 88, 96, 98, 127	بازیابی گواهی‌نامه‌ها از طریق recovery agent ، گواهی‌ها و کلیدهای exchange (XCHG) یا همه آنها
AD CS Performance Counters Availability	110	شاخص‌های کارایی که اجرا نمی‌شوند
AD CS Policy Module Processing	9, 43, 44, 77, 78	مشکلات policy module
AD CS Program Resource Availability	15, 16, 26, 30, 33, 34, 35, 38, 40, 61, 63, 89, 90	پایداری منابع سیستم و اجزاء سیستم عامل
AD CS Registry Settings	5, 19, 20, 28, 95	خرابی یا حذف تنظیمات پیکربندی رجیستری
AD CS Online Responder	16, 17, 18, 19, 20, 21, 22, 23, 25, 26, 27, 29, 31, 33, 34, 35	سرویس‌های وابسته به سرویس OR

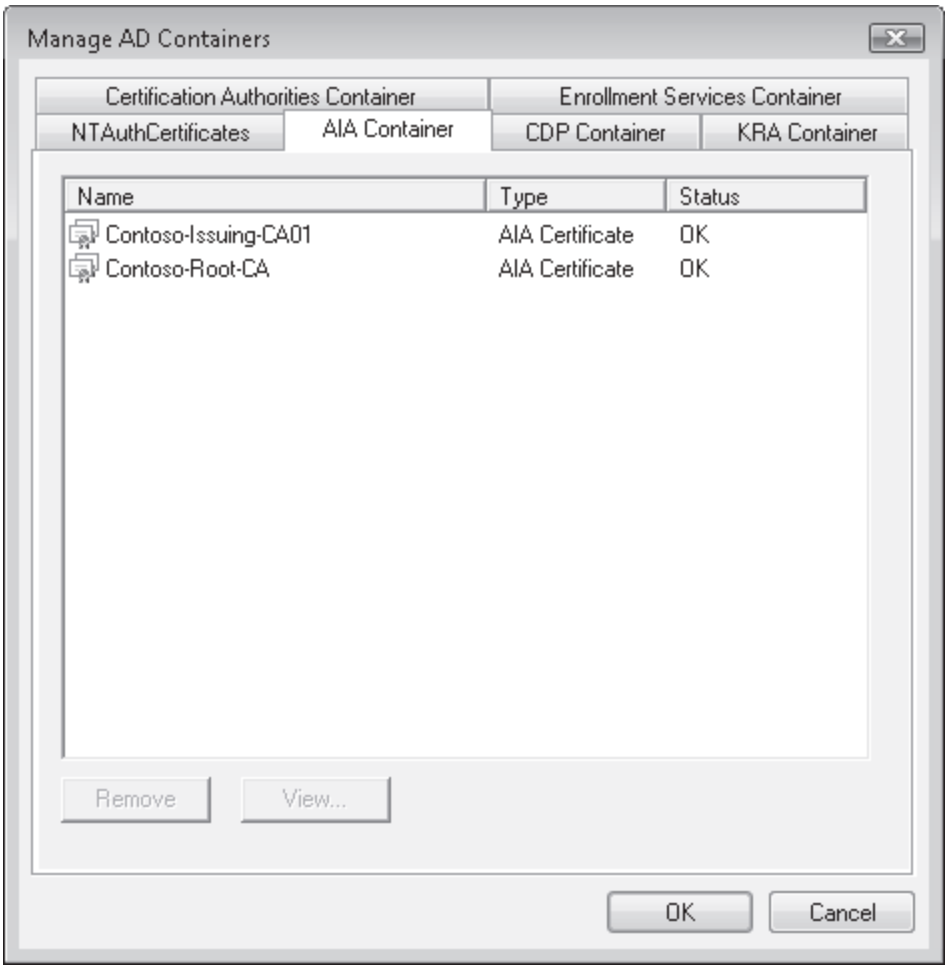
کار با Enterprise PKI

یکی از مفید ترین ابزارهای زیرساخت AD CS عبارتست از Einterprise PKI یا PKIView که در خط فرمان اجرا می‌شود. گرهی به همین نام در Server Manager زیر Active Directory Certificate Services موجود است. از آن برای مقاصد

مدیریتی متعددی در رابطه با AD CS استفاده می‌شود. اساسا Enterprise PKI نمایی از وضعیت توزیع AD CS ارائه می‌دهد و به ما امکان می‌دهد ساختار سلسله‌مراتبی کل PKI را در شبکه خود مشاهده کنیم و به طور اختصاصی یک CA را تحلیل کرده و مشکلات پیکربندی یا کارکردی زیرساخت AD CS را تشخیص دهیم.

Enterprise PKI ابزاری برای مشاهده و تست اولیه می‌باشد به دلیل اینکه اطلاعات عملی راجع به اعضاء ساختار PKI ارائه می‌دهد. ضمنا با کلیک راست روی نام CA و انتخاب Manage CA از آن برای لینک سریع به CA نیز می‌توان استفاده کرد. این کار باعث باز شدن کنسول Certification Authority می‌شود.

از پنل Actions می‌توانیم به کنسول Templates (Manage Templates) و Certificate Containers در Active Directory Domain Services (Manage AD Containers) دسترسی داشته باشیم. کنسول دوم امکان مشاهده محتویات container های دایرکتوری را که برای ذخیره گواهی‌نامه‌ها استفاده می‌شود فراهم می‌کند. (شکل ۹- ۱۵)



شکل ۹- ۱۵ مشاهده AD containers از طریق Enterprise PKI

برای بررسی سلامت سرویس AD CS به صورت تصویری گزینه مناسب Enterprise PKI می‌باشد. آیکن‌های مختلف آن امکان مشاهده اجزاء زیرساخت را فراهم می‌کند به طوری که وقتی همه چیز درست باشد رنگ سبز، وقتی مشکلات کوچکی موجود باشد رنگ زرد و زمانی که مشکلات حیاتی سرویس را تهدید می‌کند رنگ قرمز هشدار دهنده است.

محافظت از پیکربندی AD CS

همراه با چک‌های امنیتی که روی CA ریشه و واسط انجام می‌شود باید CA صادرکننده را نیز از طریق پشتیبان‌گیری مداوم محافظت کنیم. پشتیبان‌گیری از CA بسیار ساده است. در کنسول Server Manager گره Roles\Active Directory Certificate Services\CA Server Name را باز می‌کنیم. روی نام سرور کلیک راست کرده و All Tasks و سپس Backup CA را انتخاب می‌کنیم. وقتی عملیات پشتیبان‌گیری را اجرا می‌کنیم ویزارد Certification Authority Backup باز می‌شود. در ادامه موارد زیر را انجام می‌دهیم.

۱. ویزارد Certification Authority Backup را اجرا کرده و روی Next کلیک می‌کنیم.
۲. در صفحه Items To Back Up مواردی را که می‌خواهیم از آنها پشتیبان تهیه کنیم انتخاب می‌کنیم.
   - گزینه‌های Private Key و CA Certificate از گواهی‌نامه‌های همین سرور محافظت می‌کند.
   - گزینه‌های Certificate Database And Certificate Database Log از گواهی‌نامه‌هایی که این سرور مدیریت می‌کند محافظت می‌کند.
۳. محل ذخیره اطلاعات پشتیبان را مشخص می‌کنیم. به خاطر داشته باشید که اطلاعات بسیار مهم است و بهتر است روی شبکه ارسال نشود و روی یک درایو محلی ذخیره و در مرحله بعد روی یک رسانه قابل حمل کپی شود.
۴. روی Next کلیک می‌کنیم. بررسی می‌کنیم که محل ذخیره خالی باشد.
۵. یک کلمه عبور پیچیده برای پشتیبان انتخاب کرده و روی Next کلیک می‌کنیم.
۶. تنظیمات را مرور کرده و روی Finish کلیک می‌کنیم. کار پشتیبان‌گیری شروع می‌شود.

امکان اجرای پشتیبان‌گیری خودکار از طریق دستور Certutil.exe به همراه سوئیچ‌های مناسب وجود دارد.

به منظور بازیابی اطلاعات از ویزارد Certification Authority Restore استفاده می‌کنیم. برای بازیابی، روی نام سرور کلیک راست کرده All Tasks و بعد Restore CA را انتخاب می‌کنیم. ویزارد پیغامی مبنی بر توقف سرویس CA صادر می‌کند. روی OK کلیک می‌کنیم. پس از توقف سرویس صفحه Welcome ویزارد ظاهر می‌شود.

۱. روی Next کلیک می‌کنیم.
۲. موارد مورد نظر برای بازیابی را انتخاب می‌کنیم.
۳. آدرس محل فایل‌های پشتیبان را تایپ کرده یا روی Browse کلیک می‌کنیم. سپس روی Next کلیک می‌کنیم.
۴. کلمه عبور را تایپ کرده و روی Next کلیک می‌کنیم.
۵. تنظیمات را مرور کرده و روی Finish کلیک می‌کنیم. پس از اتمام عملیات ویزارد اجازه راه‌اندازی مجدد سرویس AD CS را می‌خواهد.
۶. روی Yes کلیک می‌کنیم. عملکرد CA را پس از بازیابی بررسی می‌کنیم.

تمرینات پیکربندی و استفاده از AD CS

در این تمرینات ما چهار کار مهم انجام می دهیم. در ابتدا با یک Enterprise PKI ایرادهای پیش آمده در هنگام پیاده سازی AD CS را درست می کنیم، سپس یک الگوی گواهی نامه سفارشی برای انتشار گواهی نامه خواهیم ساخت ، بعد autoenrollment را برای گواهی نامه ها فعال می کنیم تا مطمئن شویم که کاربران می توانند آنها را به صورت اتوماتیک دریافت کنند و بلاخره اطمینان حاصل می کنیم که CA به صورت اتوماتیک کار می کند.

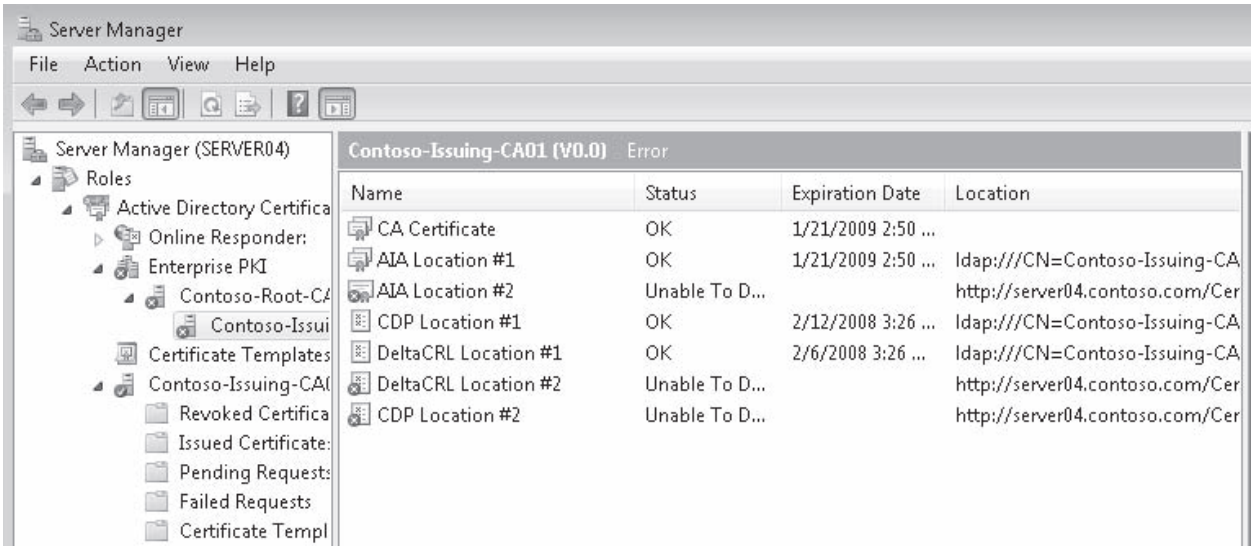
تمرین اول اصلاح پیاده سازی AD CS بوسیله Enterprise PKI

در این تمرین برای شناسایی و اصلاح مشکلات AD CS از Enterprise PKI استفاده می کنیم. این تمرین به ما کمک می کند تا به کارکرد Enterprise PKI پی ببریم

۱- اطمینان حاصل می کنیم که SERVER01 ، SERVER03 و SERVER04 در حال کارکردن هستند
۲- با اعتبار مدیر شبکه دامنه وارد SERVER04 می شویم
۳- برنامه Server Manager را از Administrative Tools اجرا می کنیم
۴- به مسیر Roles\Active Directory Certificate Services\Enterprise PKI\Contoso-Root-CA \Contoso-Issuing-CA رفته و روی Contoso-Issuing-CA کلیک کرده و خطاها را یادداشت می کنیم. (شکل ۱۰-۱۵)

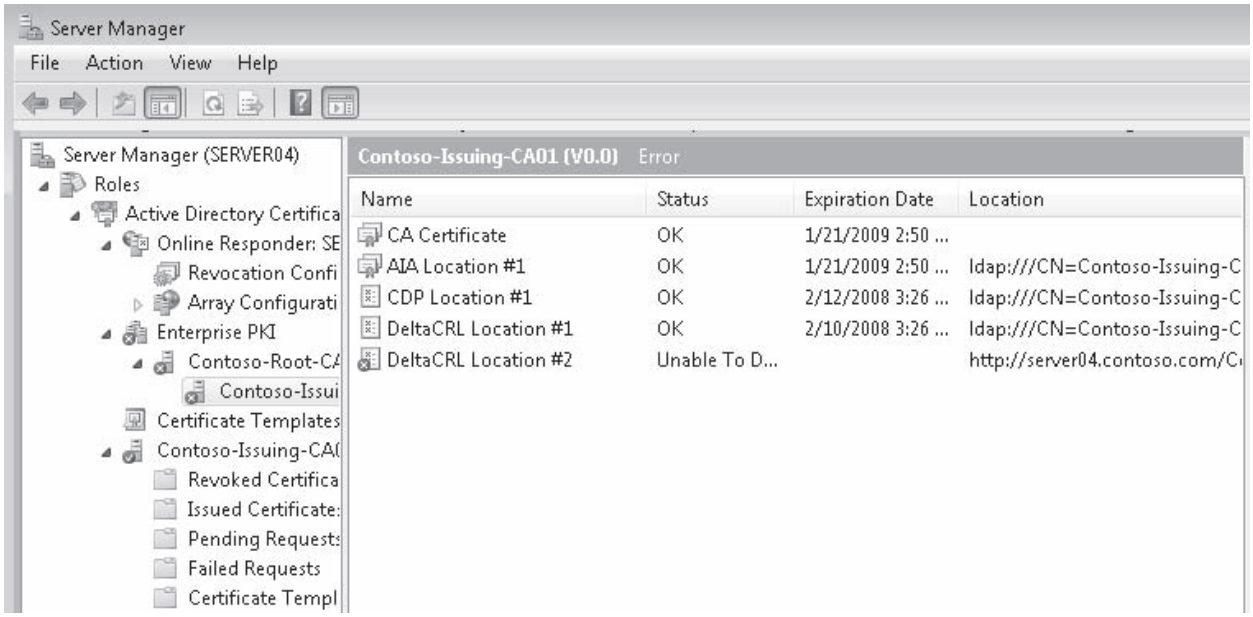
خطاهایی در پیکربندی ما وجود دارند اگر به Contoso-Root-CA برویم می بینیم که در آن خطاهایی مطابق Enterprise PKI موجود است. این خطاها به محلهای دانلود Web-based برای CRL Distribution Point و AIA اشاره دارند. این خطاها به این دلیل بوجود آمده اندکه به نقطه ای اشاره می کنند که وجود ندارد. این نقاط باید به صورت دستی در IIS ساخته شوند، هرچند که به علت نصب AD CS در درون AD DS احتیاجی به اضافه کردن محلهای دانلود Web-based نداریم حتی اگر به صورت پیش فرض در پیکر بندی AD CS شناسایی شده باشند . در یک نصب عجین شده با AD DS ، سرویس دایرکتوری مسئول توزیع AIA و CRL می باشد و چون این سرویس پایدار است نیازی به محل ثانویه نیست. در واقع این محل ثانویه تنها زمانی نیاز می شوند که بخواهیم آنها برای کاربران سیار یا خارجی که خارج از شبکه ما هستند قابل دسترسی باشند. در این صورت URL ما نیز باید از خارج از شبکه خودمان قابل دسترس باشد.

۵- روی Contoso-Root-CA در زیر گره Enterprise PKI کلیک کرده و Manage CA را انتخاب می کنیم
این کار باعث اجرای کنسول Certificate Authority standalone با تمرکز بر CA ریشه می شود به یاد داشته باشید که Server Manager تنها می تواند با سرور داخلی کار کند پس نیازمند استفاده از یک کنسول مستقل هستیم
۶- روی Contoso-Root-CA راست کلیک کرده و Properties را انتخاب می کنیم
۷- روی زبانه Extensions کلیک کرده و از انتخاب CRL Distribution Point (CDP) در منوی بازشو مطمئن می شویم.
۸- http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed> را در قسمت locations section کادر محاوره ای کلیک کرده و Include In CRLs, Clients Use This To Find Delta CRL Locations را از حالت انتخاب خارج می کنیم.
۹- از لیست بازشو Authority Information Access (AIA) را انتخاب می کنیم
۱۰- http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><Certificate Name>.crt را انتخاب کرده و Include in the AIA extension of issued certificates را از حالت انتخاب خارج می کنیم. برای اعمال تغییرات روی OK کلیک می کنیم
۱۱- چون تغییراتی در پیکربندی سرور AD CS داده ایم کنسول از ما می خواهد که AD CS را در این سرور مجددا راه اندازی کنیم. برای انجام این کار روی Yes کلیک می کنیم
۱۲- کنسول Certificate Authority را بسته و به Enterprise PKI در Server Manager برمی گردیم
۱۳- برای بروز رسانی Enterprise PKI روی دکمه Refresh در نوارابزار کلیک می کنیم. می بینیم که اگرچه دیگر از آن خطاها خبری نیست اما هنوز خطاهایی وجود دارند



شکل ۱۰-۱۵ مشاهده خطاهای پیکربندی در Enterprise PKI

اکنون آماه رفع این خطا ها هستیم
۱- روی Contoso-Issuing-CA در زیر AD CS در Server Manager راست کلیک کرده و Properties را انتخاب می کنیم.
در این مورد می توانیم از Server Manager استفاده کنیم چون Contoso-Issuing-CA همین رایانه می باشد
۲- روی زبانه Extensions کلیک کرده و مطمئن می شویم که در لیست بازشو CRL Distribution Point (CDP) انتخاب شده است
۳- http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRL Allowed>.crl را دربخش locations کادر محاوره ای انتخاب کرده و Include In CRLs را از حالت انتخاب خارج می کنیم. کلاینتها از این برای پیدا کردن محل Delta CRL و پسوند CDP استفاده می کنند.
۴- از لیست بازشو Authority Information Access (AIA) را انتخاب می کنیم
۵- http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><Certificate Name>.crt را انتخاب و Include in the AIA extension of issued certificates را از حالت انتخاب خارج می کنیم. برای اعمال تغییرات روی OK کلیک می کنیم.
۶- چون در پیکربندی سرور AD CS تغییراتی دادیم، کنسول از ما می خواهد که AD CS را در این سرور مجددا راه اندازی کنیم. روی Yes کلیک می کنیم
۷- به Enterprise PKI در Server Manager برمی گردیم
۸- برای بروزرسانی Enterprise PKI روی کلید Refresh در نوارابزار کلیک می کنیم
اکنون تنها یک خطا باقی مانده که علت آن فایل گواهی نامه ای است که در حین نصب ساخته شده است. این گواهی نامه با گواهی نامه ای که از طریق CA ریشه صادر می شود جایگزین خواهد شد. به همین دلیل باید آنرا لغو کنیم

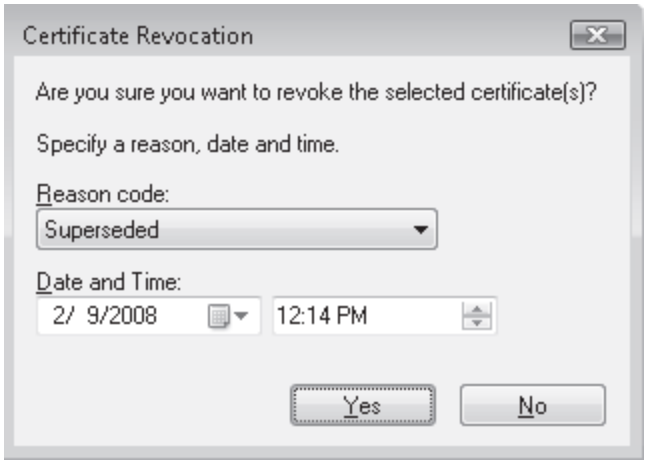


۹- برای اتمام پیکربندی، به Contoso-Issuing-CA در زیر AD CS رفته و Issued Certificates را انتخاب می کنیم
این کار باعث لیست شدن تمام گواهی نامه هایی می شود که توسط این CA صادر شده اند

۱۰- اولین گواهی نامه را پیدا می کنیم
این گواهی نامه باید از نوع CA Exchange باشد. نوع گواهی نامه در زیر ستون Certificate Template قرار دارد.

۱۱- روی این گواهی نامه راست کلیک می کنیم، All Tasks را انتخاب و روی Revoke Certificate کلیک می کنیم

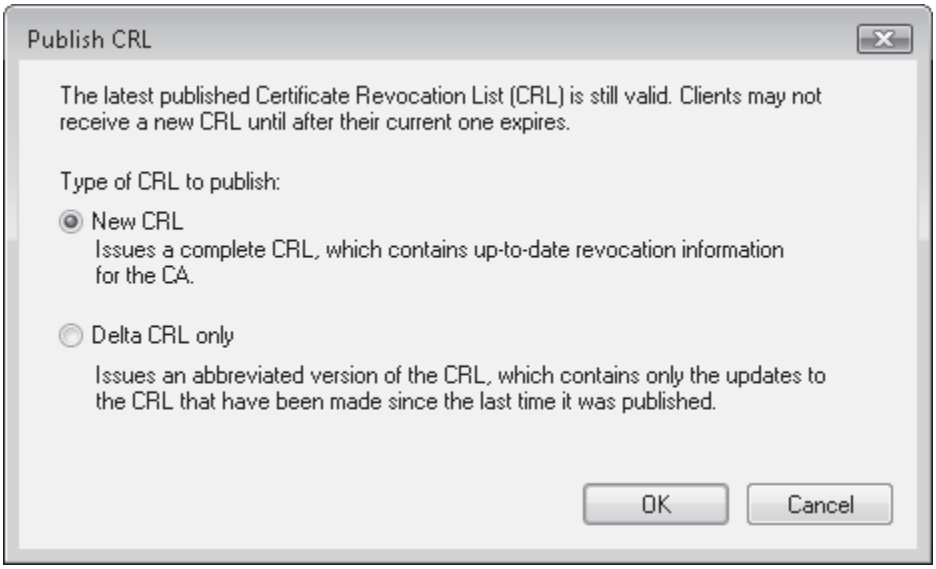
۱۲- در کادر محاوره ای Certificate Revocation از لیست بازشو Superseded را انتخاب کرده و تاریخ را چک کرده و روی OK کلیک می کنیم



هنگامی که گواهی نامه را لغو می کنیم به صورت اتوماتیک به پوشه Revoked Certificates منتقل می شود و دیگر اعتبار ندارد اما چون به تازگی یک گواهی نامه را لغو کرده ایم باید لیست لغوها را بروز رسانی کنیم

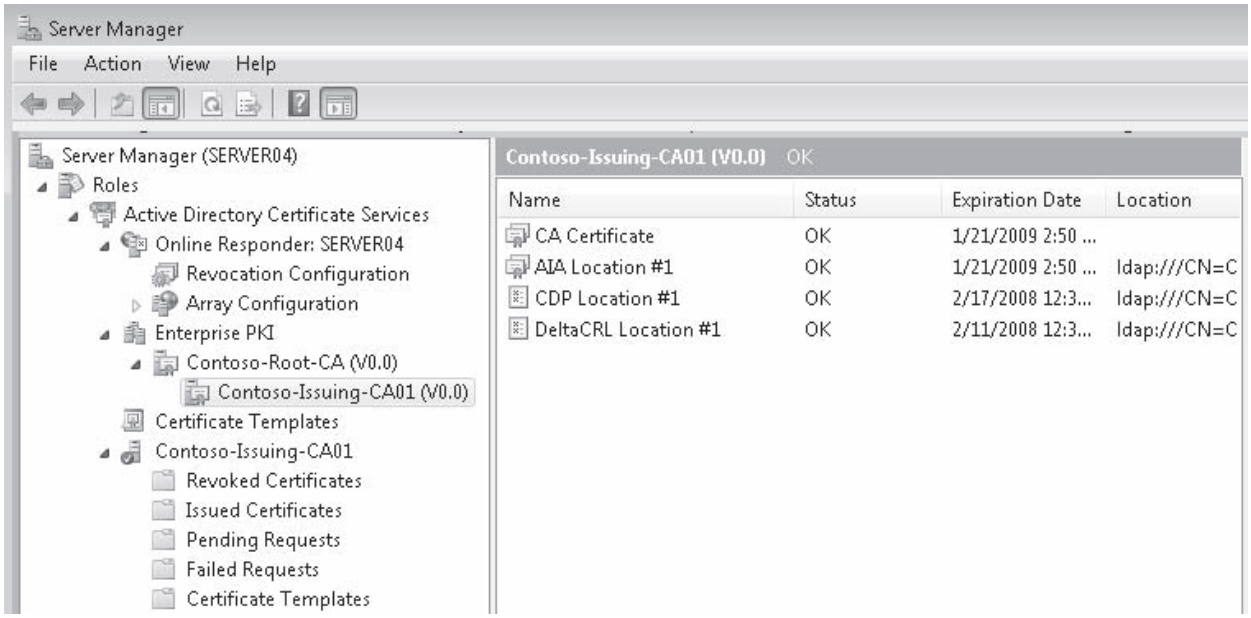
۱۳- روی گره Revoked Certificates راست کلیک می کنیم و choose All و سپس Publish را انتخاب می کنیم

۱۴- در کادر محاوره ای Publish CRL روی New CRL کلیک می کنیم و بعد روی Next کلیک می کنیم



۱۵- به Enterprise PKI برگشته و روی دکمه Refresh کلیک می کنیم

اکنون نباید دیگر خطایی وجود داشته باشد



تمرین دوم ساخت کپی الگوی گواهی نامه برای EFS

در این تمرین یک کپی الگو را برای فعال کردن EFS ، می سازیم و آنرا منتشر می کنیم تا بتواند از autoenroll استفاده کند و از EFS برای محافظت از اطلاعات سیستم استفاده می کنیم

۱- مطمئن می شویم که SERVER01 و SERVER04 هردو کار می کنند

۲- با اعتبار مدیر شبکه دامنه به SERVER04 وارد می شویم

۳- Server Manager را از Administrative Tools اجرا می کنیم

۴- به مسیر Roles\Active Directory Certificate Services\Certificate Templates (*servername*) می رویم

می بینیم که تمامی الگوهای موجود در پنجره سمت راست قابل رویت هستند و همچنین اکنون به صورت پیش فرض به DC (SERVER01) متصل هستیم. برای کار با الگوها باید به DC متصل بود تا الگوها یتوانند روی AD DS منتشر شوند. در صورتی که متصل نیستیم باید از دستور *Connect To Another Writable Domain Controller* برای این کار استفاده کنیم

۵- در پنجره سمت راست Basic EFS template را انتخاب کرده روی آن راست کلیک می کنیم و Duplicate Template را انتخاب می کنیم

۶- نوع ویندوز سرور را مشخص کرده – در این مورد ویندوز سرور 2008- و روی OK کلیک می کنیم

۷- نام قالب را **Basic EFS WS08 گذاشته و** گزینه های زیر را تنظیم می کنیم و بقیه را بدون تغییر رها می کنیم

- در زبانه Request Handling ، Archive Subject's Encryption Private Key and the Use Advanced Symmetric Algorithm To Send The Key To The CA را انتخاب می کنیم. انباره آرشیو کلید خصوصی این امکان را به ما می دهد که از آن هنگامی که کاربر آن را از دست می دهد استفاده کنیم
- در زبانه Subject Name اطلاعاتی به مقادیر Alternate Subject Name اضافه می کنیم. گزینه E-mail Name and User Principal Name (UPN) را انتخاب می کنیم

۸- روی OK کلیک می کنیم

۹- روی EFS Recovery Agent template راست کلیک کرده و Duplicate را انتخاب می کنیم

۱۰- نوع ویندوز سرور را مشخص کرده – در این مورد ویندوز سرور 2008- و روی OK کلیک می کنیم

۱۱- نام الگو را **EFS Recovery Agent WS08 گذاشته و** گزینه های زیر را تنظیم می کنیم و بقیه را بدون تغییر رها می کنیم

- در زبانه General ، Publish certificate in the Active Directory را انتخاب می کنیم

به خاطر داشته باشید که گواهی نامه عامل بازیابی برای مدت طولانی تر از خود EFS گواهی نامه معتبر است

- در زبانه Request Handling از انتخاب Archive Subject's Encryption Private Key and the Use Advanced Symmetric Algorithm To Send The Key To The CA مطمئن می شویم. . انباره آرشیو کلید خصوصی این امکان را به ما می دهد که از آن هنگامی که کاربر آن را از دست می دهد محافظت کنیم
- در زبانه Subject Name اطلاعاتی به مقادیر Alternate Subject Name اضافه می کنیم. گزینه E-mail Name and User Principal Name (UPN) را انتخاب می کنیم

۱۲- روی OK کلیک می کنیم

۱۳- در Server Manager ، گرهRoles\Active Directory Certificate Services*Issuing CA Name*\Certificate Templates را باز می کنیم.

۱۴- برای صدور الگو روی Certificate Templates راست کلیک کرده New را انتخاب می کنیم و سپس Certificate Template To Issue را انتخاب می کنیم

۱۵- در کادر محاوره ای Enable Certificate Templates از Ctrl + click برای انتخاب Basic EFS WS08 و EFS Recovery Agent WS08 با هم استفاده می کنیم و روی OK کلیک می کنیم

الگوها آماده است

تمرین سوم پیکربندی Autoenrollment

در این تمرین از Group Policy برای پیکربندی autoenrollment استفاده می کنیم. این تمرین از policy های پیش فرض دامنه استفاده می کند. اما در محیط واقعی باید از policy های سفارشی استفاده کنیم

۱- با اعتبار مدیر دامنه به SERVER01 وارد می شویم

۲- Group Policy Management را از Administrative Tools اجرا می کنیم

۳- برای پیدا کردن Default Domain policy تمام گره ها را باز می کنیم، روی آن راست کلیک کرده و Edit را انتخاب می کنیم

۴- برای انتساب autoenrollment به رایانه گره Computer Configuration\Policies \Windows Settings\Security Settings\Public Key Policies را باز می کنیم

۵- روی Certificate Services Client – Auto-Enrollment دوبار کلیک می کنیم

۶- سیاست را فعال می کنیم و Renew Expired Certificates و Update Pending Certificates را انتخاب کرده و Revoked Certificates را از حالت انتخاب خارج می کنیم

۷- Expiration Notification For Users را فعال کرده و مقدار آن را ۱۰٪ قرار می دهیم

۸- برای اعمال تغییرات روی OK کلیک می کنیم

۹- GPMC را می بندیم

سیاست ما اکنون آماده است

تمرین چهارم فعال کردن CA برای صدور گواهی نامه

اکنون نیازمند تنظیم عملکرد پیش فرض CA در برابر درخواست گواهی نامه هستیم

۱- با اعتبار مدیر شبکه دامنه به SERVER04 وارد می شویم

۲- به Server Manager می رویم

۳- روی Contoso-Issuing-CA01 در زیر AD CS راست کلیک کرده و Properties را انتخاب می کنیم

۴- روی زبانه Policy Module کلیک کرده و روی دکمه Properties کلیک می کنیم

۵- برای صدور اتوماتیک گواهی نامه ، گزینه Follow The Settings In The Certificate Template, If Applicable. Otherwise, Automatically Issue The Certificate را انتخاب کرده و روی OK کلیک می کنیم. برای بستن کادر محاوره ای Properties یکبار دیگر روی OK کلیک می کنیم

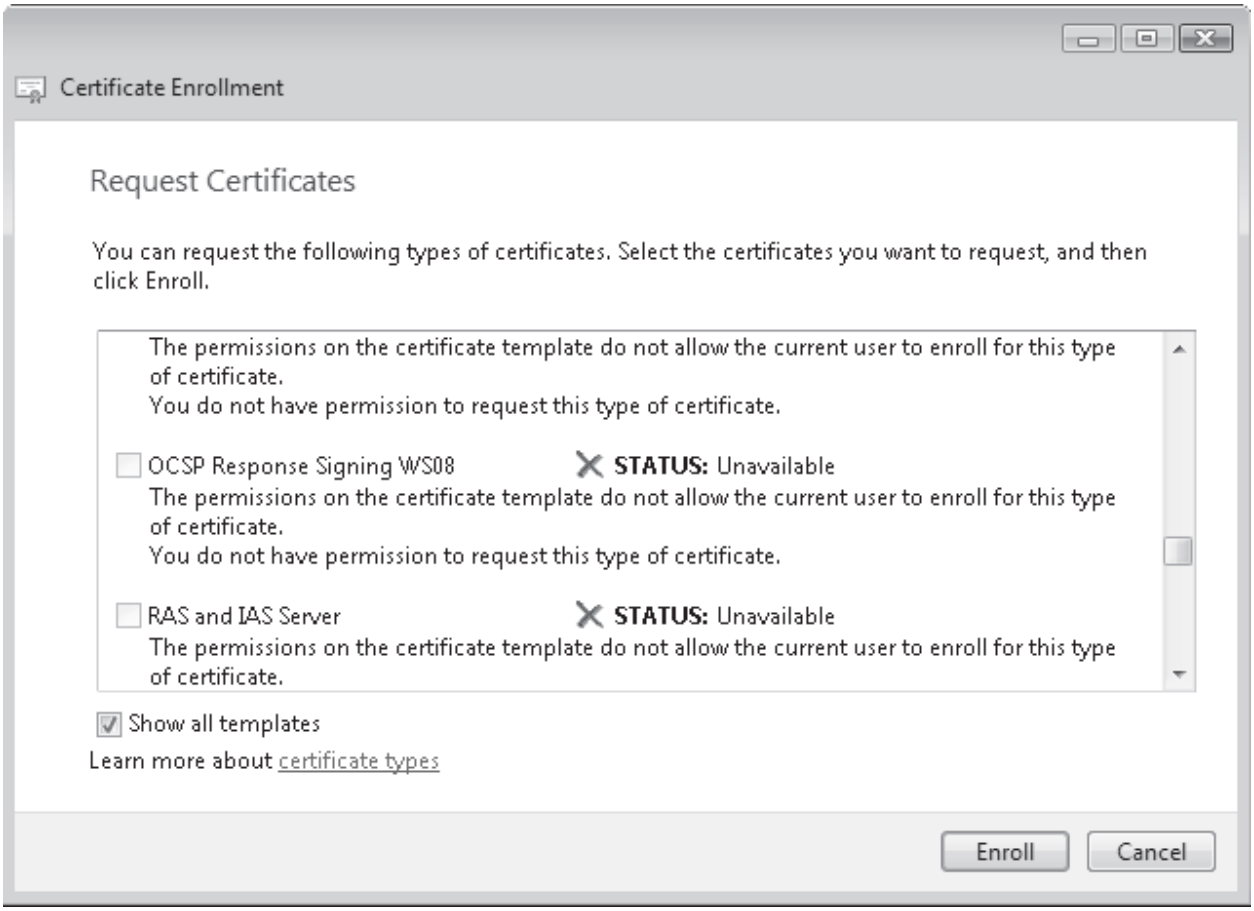
CA ما اکنون آماده صدور گواهی نامه EFS بصورت اتوماتیک می باشد

خلاصه درس

- پیکربندی لغو CA چند جزء مختلف دارد. اولین آنها نقاط توزیع Certificate Revocation List می باشد. دومی همپوشانی بین CRL و Delta CRL هایی است که به درخواست کننده فرستاده می شود. سوم زمانبندی است که برای انتشار CRL ها استفاده می کنیم
- CA ها برای داشتن توانایی پشتیبانی autoenrollment و تغییر دادن و شخصی سازی الگوهای گواهی نامه باید enterprise CA باشند
- Online responder ها با هدف پایداری سرویس آرایه ای از سیستم ها می سازند. یک آرایه می تواند عملکردی مشابه دو CA و یا بیشتر داشته باشد.
- OR ها باید به گواهی نامه های Online Certificate Status Protocol (OCSP) برای پاسخ به درخواستها استناد کنند. این گواهی نامه ها محتوای پاسخ فرستاده شده از OR را رمزنگاری می کنند
- OR ها همچنین قبل از اینکه بتوانند بطور کامل سرویس بدهند به پیکربندی Authority Information Access extension نیاز دارند. این extension به بخشی از ویژگیهای certificate authority می باشد.
- هر CA که OR می باشد باید پیکربندی لغو مخصوص بخود را داشته باشد چون هرکدام گواهی نامه مخصوص به خود را دارند. گواهی نامه هابرای اینکه در آرایه شرکت کنند باید مورد اعتماد باشند. پیکربندی لغو برای جلب اعتماد دیگر اعضای آرایه به یک CA خاص در آرایه استفاده می شود
- حفاظت از CA ها در زیرساخت ضروری است. به همین علت است که از تمام اطلاعات CA حتی گواهی نامه ها نسخه پشتیبان تهیه می شود که باید بسیار مراقب آن بود چون حاوی اطلاعات بسیار حساسی می باشد

سئوالات پایان درس

۱- فرض کنید به عنوان مدیر شبکه PKI در شرکت Contoso مشغول به کار هستیم. می خواهیم OR را پیکربندی کنیم. قبلا OCSP Response Signing certificates و Authority Information Access extension را پیکربندی کرده و سیستم را مجددا راه اندازی کرده ایم. اکنون می خواهیم مطمئن شویم که گواهی نامه بطور اتوماتیک در سرور بارگذاری شده است. یک کنسول سفارشی برای ابزار Certificates درست می کنیم اما هنگامی که می خواهیم گواهی نامه ها را در گره Personal ببینیم ، ابزار ظاهر نمی شود. تصمیم می گیریم گواهی نامه را به طور دستی وارد کنیم . اما هنگامی که از ویزارد Request New Certificate استفاده می کنیم متوجه می شویم گواهی نامه در دسترس ما نیست. مشکل چه می تواند باشد؟



A . نمی توانیم از طریق ویزارد درخواست گواهی نامه کنیم. باید این کار را با دستور *Certutil.exe انجام دهیم.*

B . الگوهای امنیتی الگوی گواهی نامه بدرستی تنظیم نشده اند

C . نمی توانیم یک OCSP Response Signing Certificate در این سرور بارگذاری کنیم

D . نیازی به وارد کردن دستی این گواهی نامه نیست چون با بروز رسانی بعدی Group Policy بصورت اتوماتیک بارگذاری می شود

فصل ۱۶

Active Directory Rights Management Services

Active Directory Rights Management Services (AD RMS) که قبلا به طور خلاصه Rights Management Services نامیده می‌شد به منظور دسترسی شبکه داخلی به دنیای بیرون طراحی شده است. ولی حالا این توسعه به مالکیت معنوی نیز تعمیم پیدا کرده است. کاربران از زمان شروع کار با کامپیوتر با Digital Rights Management (DRM) دست و پنجه نرم می‌کرده‌اند. در اولین روزهای دنیای دیجیتال تولیدکننده‌های نرم‌افزار خیلی به دنبال حفاظت از نرم افزارهایشان بودند. حتی حالا هم برخی تولیدکنندگان از کلیدهای سخت‌افزاری برای اجرای نرم‌افزارهایشان استفاده می‌کنند و برخی دیگر به رویکرد مبتنی بر وب و

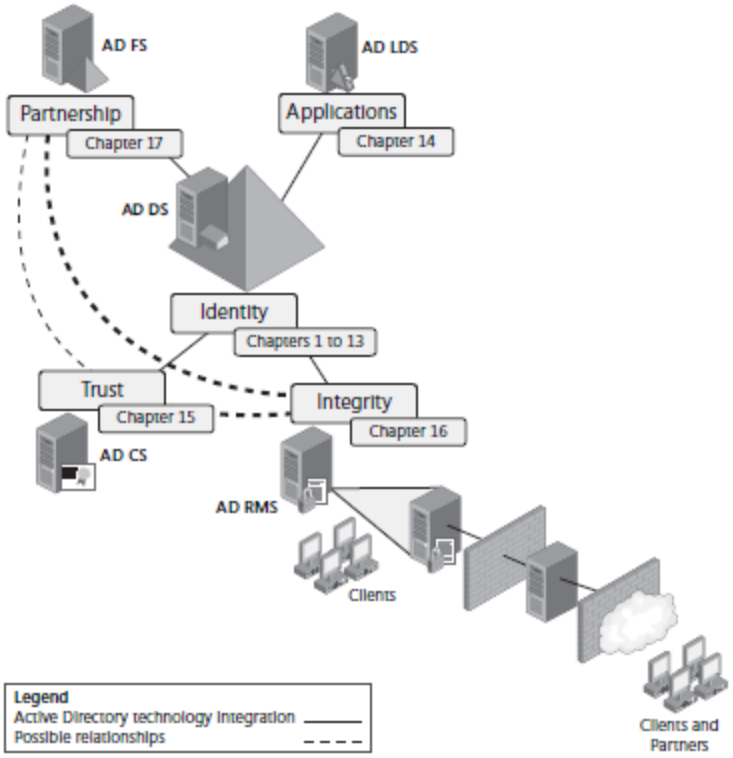
فرایند تایید اعتبار روی آورده‌اند. برای مثال هنگام عرضه ویندوز ویستا، مایکروسافت روش جدید صدور مجوز را معرفی کرد که یکی از گزینه‌ها Key Management Server (KMS) می‌باشد.

تولید نرم‌افزار تنها صنعت درگیر با مدیریت حقوق کاربری نیست. صنعت موسیقی نیز تحت تاثیر این مسئله قرار دارد تا بهترین روش برای حفاظت از موسیقی دیجیتال را پیدا کند و حتی گاهی روش‌های سئوال برانگیز نیز استفاده می‌شود. برای مثال در سال ۲۰۰۵ Mark Russionovich که حالا به استخدام مایکروسافت درآمده است فهمید که Sony BMG یک root kit در CD player هایش نصب می‌کند و هنگام اجرا روی کامپیوتر فعال می‌گردد. این root kit از طریق اینترنت اطلاعات playlist را به سرور مرکزی شرکت Sony ارسال می‌کرد. این قضیه باعث بحث و جدل‌های فراوان درباره رفتار سازندگان موسیقی در رابطه با حفاظت اطلاعات شد. حالا بسیاری تصمیم گرفته‌اند موسیقی‌شان را در قالب MP3 بدون محافظت بفروشند. وقتی ترانه‌ای را می‌خریم مسئول حفاظت از آن خواهیم بود. ولی از طریق هر دستگاه دلخواهی می‌توانیم آنرا اجرا کنیم. بهرحال این نشان می‌دهد که DRM چقدر می‌تواند پیچیده باشد.

موسیقی و نرم‌افزار تنها مواردی نیستند که احتیاج به محافظت دارند. در مراکز داده مردم به دنبال فناوری‌های جدیدی هستند که بتواند حقوق معنوی‌شان را پاسداری کند. برای مثال نکته مثبت درباره e-mail این است که به طور خودکار مذاکرات را نگهداری می‌کند. هربار که به یک پیغام پاسخ می‌دهیم پیغام اصلی در پاسخ ظاهر می‌شود. بدون DRM همه می‌توانند محتوای این پاسخ را در هر زمانی تغییر دهند. حتی بدتر از آن هر کسی می‌تواند بدون اینکه ما بدانیم مکاتبات ما را برای دیگران ارسال کند. پیاده‌سازی DRM برای محافظت از محتوای e-mail اجازه تغییر محتویات را حتی اگر به پیغام دیگری اضافه شده باشد نمی‌دهد.

همین وضعیت برای دیگر حقوق مالکیت معنوی نیز صادق است. مثلا اسناد Office. بسیاری از سازمان‌ها به ارزش مالکیت معنوی خود متکی هستند. از دست دادن این مالکیت از طریق سوء استفاده کپی غیرمجاز یا سرقت خسارات جبران ناپذیری را به سازمان وارد می‌کند. نیاز نیست ما یک سازمان بزرگ باشیم تا از منافع مدیریت حقوق مالکیت بهره‌مند شویم. هرگاه گذران زندگی ما بر پایه تولید اطلاعات باشد باید از DRM برای حفظ منافع خود استفاده کنیم.

AD RMS از طریق ترکیب ویژگی‌های متفاوتی از حقوق مالکیت معنوی حفاظت می‌کند. AD RMS به واسطه رابطه مستقیم با AD DS از AD CS و AD FS استفاده می‌کند. AD CS گواهی‌نامه‌های PKI را تولید می‌کند که AD RMS از آنها در اسناد خود بهره می‌گیرد. AD FS سیاست‌های AD RMS را به آن‌سوی دیواره آتش توسعه می‌دهد و مالکیت معنوی ما را بین شرکای تجاری حفظ می‌کند. (شکل ۱- ۱۶)



شکل ۱- ۱۶ AD RMS گستره اقتدار ما را به آن سوی مرزهای شبکه می‌کشاند.

اهداف امتحانی در این فصل:

- پیکربندی نقش دیگری از Active Directory
  - پیکربندی AD RMS

دروس این فصل:

- درس ۱: درک و نصب AD RMS
- درس ۲: پیکربندی و استفاده از AD RMS

قبل از شروع

برای ادامه دروس این فصل باید موارد زیر انجام شود:

- ویندوز سرور 2008 روی یک کامپیوتر فیزیکی یا مجازی نصب شود. نام کامپیوتر باید SERVER01 بوده و نقش DC را در دامنه contoso.com داشته باشد.
- ویندوز سرور 2008 نسخه Enterprise روی یک کامپیوتر فیزیکی یا مجازی نصب شود. نام کامپیوتر باید SERVER03 بوده و باید عضو دامنه contoso.com باشد. این کامپیوتر میزبان سرورهای سیاست AD RMS می‌باشد که نصب خواهد

شد. بهتر است دارای درایو D باشد که داده‌های AD RMS را ذخیره کند. حجم ۴۰ گیگابایت برای این تمرینات کافی است اگرچه پیشنهاد مایکروسافت ۸۰ گیگابایت می‌باشد.

- ویندوز سرور 2008 نسخه Enterprise روی یک کامپیوتر فیزیکی یا مجازی نصب شود. نام کامپیوتر باید SERVER04 بوده و باید عضو دامنه contoso.com باشد. این کامپیوتر میزبان سرورهای سیاست AD RMS می‌باشد که نصب خواهد شد. بهتر است دارای درایو D باشد که داده‌های AD RMS را ذخیره کند. حجم ۴۰ گیگابایت برای این تمرینات کافی است اگرچه پیشنهاد مایکروسافت ۸۰ گیگابایت می‌باشد.

- ویندوز سرور 2003 نسخه Enterprise روی یک کامپیوتر فیزیکی یا مجازی نصب شود. نام کامپیوتر باید SERVER05 بوده و باید عضو دامنه contoso.com باشد. این کامپیوتر میزبان سرور SQL می‌باشد که برای اجرای پیکربندی و گزارش گیری استفاده می‌شود. این کامپیوتر باید دارای یک درایو D باشد تا بتواند داده‌های SQl را ذخیره کند. پیشنهاد مایکروسافت ۱۰ گیگابایت می‌باشد.

همان طور که می‌بینیم تست AD RMS نیاز به چند کامپیوتر دارد. برای این منظور می‌توانیم از زیرساخت مجازی استفاده کنیم. بهتر است برای استفاده از AD RMS پس از توزیع، یک کلاینت ویستا و Office 2007 نیز اضافه کنیم.

درس ۱ : درک و نصب AD RMS

بسیاری از سازمان‌ها پیاده‌سازی AD RMS را در چند سطح انجام می‌دهند.

- سطح اول روی استفاده داخلی مالکیت معنوی تمرکز دارد. در این سطح پیاده‌سازی حقوق دسترسی مناسب برای اسناد خود انجام می‌شود. به این ترتیب کارکنان سازمان فقط توانایی مشاهده و مدیریت محتویات مربوط به خود را خواهند داشت. این محتویات کپی نخواهد شد مگر تحت شرایط امنیتی سخت.

- سطح دوم به اشتراک‌گذاری محتویات با شرکاست. شرکا می‌توانند اسناد را مشاهده کنند ولی امکان کپی یا به اشتراک‌گذاری آنها را ندارند.

- سطح سوم مخاطبین وسیع‌تری را تحت پوشش قرار می‌دهد. مالکیت معنوی می‌تواند در حالت محافظت شده در آنسوی مرزهای شبکه دردسترس قرار گیرد. به دلیل اینکه اسناد محافظت شده است نمی‌توان آنها را کپی یا توزیع کرد مگر اینکه اختیار لازم اعطاء گردد.

در هر کدام از سطوح بالا باید سیاست حفاظتی اسناد اعمال گردد. کارکنان باید به طور کامل آموزش ببینند و عواقب فاش شدن اطلاعات را برای افراد متفرقه درک کنند. شرکاء نیز باید سیاست سازمان را بدانند تا بتوانند از اطلاعات سازمان محافظت کنند. وقتی به

مخاطبین بیشتری سرویس می‌دهیم آنها نیز باید بدانند سیاست‌های حفاظتی ما چگونه است تا بتوانند به صورت صحیح با اطلاعات کار کنند.

هر سطح از سطوح بالا نیاز برای رعایت استراتژی‌های حفاظتی به اجزاء دیگری نیاز دارد.

بعد از این درس می‌توانیم :

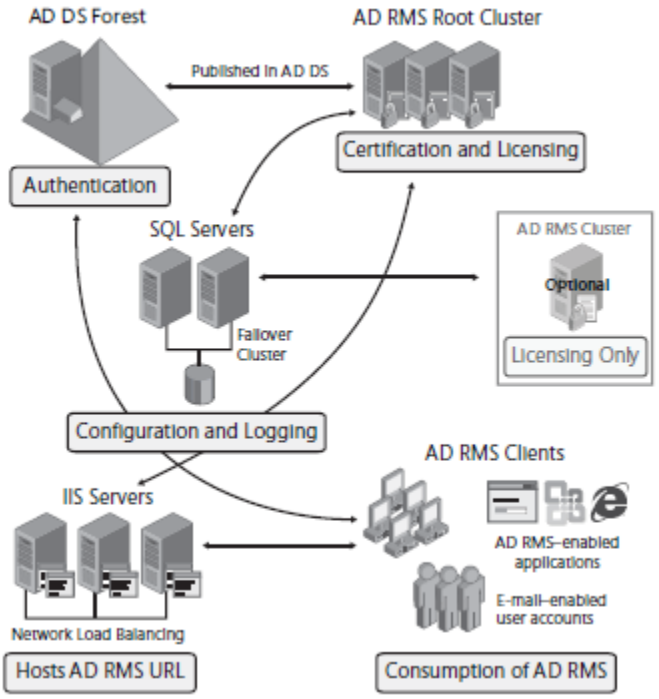
- اجزایی که سرویس AD RMS را تشکیل می‌دهند درک کنیم.
- سناریوهای مختلف توزیع AD RMS را درک کنیم.
- پیش‌نیازهای AD RMS را برای توزیع درک کنیم.
- AD RMS را در سناریوهای مختلف نصب کنیم.

زمان تقریبی : ۴۰ دقیقه

درک AD RMS

همان‌طور که اشاره شد AD RMS نسخه به روز شده Microsoft Windows Rights Management Services می‌باشد که در ویندوز سرور 2003 ارائه شد. با ارائه نسخه جدید، مایکروسافت ویژگی‌های جدید متعددی به AD RMS اضافه کرد. ولی سناریوهای توزیع AD RMS به همان شکل باقی ماند.

AD RMS برای حفاظت از اطلاعات حساس با یک کلاینت مخصوص AD RMS کار می‌کند. حفاظت توسط نقش سرور AD RMS تامین می‌شود که به منظور مدیریت اعطاء مجوز و گواهی طراحی می‌شود. اطلاعات شامل پیکربندی و گزارشات در بانک اطلاعاتی نگهداری می‌شود. در محیط‌های تست این بانک می‌تواند Windows Intenal Database (WID) باشد که در ویندوز سرور 2008 موجود است ولی در محیط‌های بزرگ‌تر به یک موتور بانک اطلاعاتی رسمی مانند SQL Server 2005 یا 2008 روی سرور مجزا نیاز داریم. این کار باعث تقسیم بار AD RMS روی سرورهای اجراکننده این نقش می‌شود. WID از ارتباطات راه دور پشتیبانی نمی‌کند بنابراین فقط یک سرور می‌تواند از آن استفاده کند. IIS 7.0 سرویس‌های وبی را برای AD RMS فراهم می‌کند و سرویس Microsoft Message Queuing هماهنگی را در محیط‌های توزیع شده به عهده دارد. کلاینت AD RMS دسترسی به ویژگی‌های AD RMS را فراهم می‌کند. به علاوه دایرکتوری AD DS تاییدهویت ومدیریت ترکیبی را ممکن می‌سازد. به این ترتیب که AD RMS برای تایید هویت کاربران و بررسی مجوز استفاده از سرویس AD DS استفاده می‌کند. این موارد زیرساخت AD RMS را تشکیل می‌دهند. (شکل ۲- ۱۶)



شکل ۲- ۱۶ زیرساخت AD RMS پایدار

وقتی سرور AD RMS را نصب می‌کنیم به صورت پیش‌فرض یک کلاستر ریشه ایجاد می‌شود. این کلاستر به منظور کار با درخواست‌های مجوز و گواهی طراحی شده است. در هر AD DS forest یک کلاستر ریشه موجود است. همچنین می‌توانیم سرور licensing-only داشته باشیم که به طور خودکار یک کلاستر licensing ایجاد می‌شود. کلاستر زمانی ایجاد می‌شود که بانک AD RMS روی یک سرور مجزا توزیع شود. هرگاه سرور AD RMS جدیدی با نقش ریشه یا licensing افزوده شود به طور خودکار در کلاستر موجود مرتبط قرار می‌گیرد. به دو دلیل مایکروسافت توصیه می‌کند از نقش ریشه استفاده شود تا نقش licensing-only :

- کلاسترهای ریشه با همه عملیات AD RMS کار می‌کنند بنابراین چندمنظوره هستند.
- کلاسترهای ریشه و licensing-only مستقل هستند یعنی روی یکدیگر تقسیم بار ندارند. ولی اگر همه سرورها به عنوان ریشه نصب شوند به طور خودکار روی یکدیگر تقسیم بار می‌کنند.

پس از اینکه زیرساخت آماده شد می‌توانیم برنامه‌های کاربردی تولیدکننده اطلاعات را مانند بسته Office، کلاینت e-mail و نرم‌فزارهای سازمانی اجرا کنیم و مطمئن باشیم AD RMS از این اطلاعات محافظت می‌کند. وقتی کاربران اطلاعات را تولید می‌کنند نیز مشخص می‌کنند چه کسی می‌تواند آنها را بخواند، تغییر دهد، چاپ کند، منتقل کند و یا دستکاری کند. به علاوه می‌توانیم الگوهایی را از سیاست بسازیم که هنگام ایجاد اسناد به آنها اعمال شود.

حقوق دسترسی به اسناد در خود آنها ثبت می‌شود بنابراین حتی اگر اطلاعات از حوزه شبکه ما نیز خارج شود حفاظت‌شده باقی خواهند ماند. AD RMS یک سری سرویس‌های وبی را ارائه می‌دهد که می‌توانیم قابلیت‌های آنرا در برنامه‌های خود به کار گیریم. به دلیل اینکه این سرویس‌ها مبتنی بر وب هستند در شبکه‌های غیرمایکروسافتی نیز قابل استفاده هستند.

ویژگی‌های جدید AD RMS

ویژگی‌های جدید AD RMS به ترتیب زیر است:

- در حال حاضر این سرویس یکی از نقش‌های ویندوز سرور 2008 است. در نسخه‌های قدیمی ویژگی‌های AD RMS در بسته‌های نرم‌افزاری قابل دانلود بود. به علاوه Server Manager همه سرویس‌های وابسته و اجزاء مورد نیاز سرویس را فراهم می‌کند. همچنین در زمان نصب اگر هیچ بانک اطلاعاتی معرفی نشود به طور خودکار WID نصب می‌شود.

- AD RMS همانند بقیه نقش‌های سروری از طریق کنسول MMC مدیریت می‌شود. نسخه‌های قدیمی از رابط وب برای مدیریت استفاده می‌کرد.

- AD RMS حالا با AD FS ارتباط مستقیم دارد که به ما امکان می‌دهد سیاست‌های مدیریت حقوق دسترسی را به آن‌سوی دیواره آتش به سمت شرکاء تجاری خود توسعه دهیم. یعنی شرکاء ما نیازی به زیرساخت AD RMS ندارند و از طریق AD FS می‌توانند به ویژگی‌های آن دسترسی پیدا کنند. در نسخه‌های قبلی برای توسعه سرویس به آنسوی مرزهای شبکه خود می‌بایست از Windows Live ID استفاده می‌کردیم. با ترکیب دو سرویس AD RMS و AD FS دیگر نیازی به محصولات غیرمایکروسافتی برای حفاظت از اطلاعات نداریم. برای استفاده از این ویژگی (federation) قبل از نصب AD RMS و ترکیب آن با AD FS باید یک trust برقرار شود. و همچنین باید جدیدترین کلاینت RMS مثل ویستا یا سرویس پک ۲ نسخه‌های قبلی ویندوز را به کار ببریم. اطلاعات بیشتر در فصل ۱۷ ارائه می‌شود.

- سرورهای AD RMS هنگام ساخت نام خود را ثبت می‌کنند. این ثبت نام باعث تولید یک Server Lincense Certificate (SLC) می‌شود که به سرور اجازه شرکت در ساختار AD RMS را اعطاء می‌کند. در نسخه‌های قبلی نیاز به دسترسی به Microsoft Enrollment Center از طریق اینترنت بود تا SLC صادر شود. به همین دلیل می‌توانیم AD RMS را در شبکه‌های مجزا بدون دسترسی به اینترنت پیاده‌سازی کنیم.

- در نهایت AD RMS نقش‌های مدیریتی جدیدی را داراست به طوری که می‌توان به جای اعطاء حقوق بیش از حد مدیریتی اجازه اجرای وظایف خاص را روی سرور اعطاء کرد. چهار نقش مدیریتی عبارتند از :

  - AD RMS Enterprise Administrators که می‌تواند همه جنبه‌های AD RMS را مدیریت کند. این گروه شامل کاربر نصب کننده نقش و گروه Administrators محلی است.

  - AD RMS Template Administrators این گروه توانایی خواندن اطلاعات از زیرساخت AD RMS و ساخت، ویرایش و انتقال الگوهای سیاست دسترسی را دارد.

- AD RMS Auditors اعضاء این گروه می‌توانند گزارشات و وقایع را مدیریت کنند. این گروه به اطلاعات زیرساخت AD RMS دسترسی فقط خواندنی دارند.
- AD RMS Service شامل حساب‌های سرویس AD RMS می‌باشد که در هنگام نصب تعیین می‌شود.

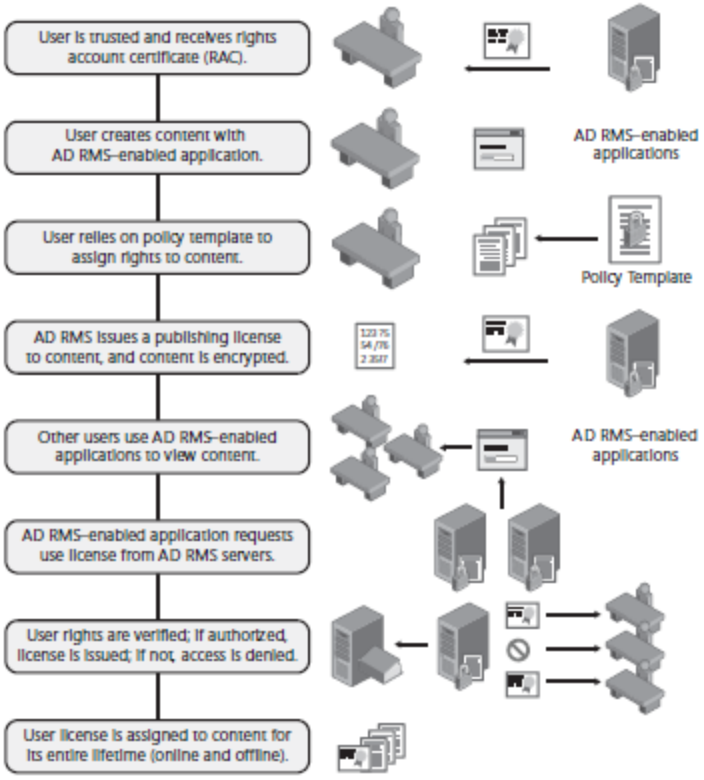
به دلیل اینکه این گروهها محلی هستند بهتر است گروههای مشابه در دایرکتوری AD DS ساخته شده و این گروهها را به گروههای محلی روی سرورهای AD RMS اضافه کنیم. سپس زمانی که بخواهیم مجوز مدیریتی روی نقش سرور اعطاء کنیم کافی است کاربر را به گروه مناسب در AD DS اضافه کنیم.

اساسا حفاظت از اطلاعات از طریق AD RMS با صدور گواهی‌نامه از روی سرور انجام می‌شود. این گواهی‌نامه‌ها کاربران، گروهها، کامپیوترها، برنامه‌های کاربردی یا سرویس‌ها را شناسایی می‌کند تا به آنها اجازه ساخت و انتشار محتوا را بدهد. بعد از اینکه انتشاردهنده محتوا مورداطمینان قرار گرفت می‌تواند به محتوای خود دسترسی داده و شرایط تعیین کند. هربار که کاربر یک سیاست حفاظتی روی یک سند تعیین می‌کند AD RMS مجوز انتشار برای آن صادر می‌کند. با عجین شدن این مجوز با محتوا دیگر نیازی به سرور AD RMS برای حفاظت محتوا وجود ندارد.

محتوا با کلیدهای مخصوص رمزنگاری به رمز در می‌آید چیزی شبیه به کلیدهایی که در AD CS ساخته می‌شود. کاربران برای مشاهده داده باید از طریق یک مرورگر یا برنامه‌ای که می‌تواند با AD RMS کار کند اقدام کنند. اگر برنامه نتواند با AD RMS کار کند کاربران نیز نمی‌توانند اطلاعات را ویرایش کنند زیرا برنامه نمی‌تواند سیاست حفاظتی را خوانده و داده را رمزگشایی کند.

وقتی کاربران دیگر بخواهند به محتوا دسترسی پیدا کنند کلاینت‌های AD RMS درخواست مجوز استفاده را به سمت سرور صادر می‌کنند. اگر کاربر یک هویت مورد اعتماد باشد سرور این مجوز را صادر می‌کند. مجوز استفاده، مجوز حفاظت این سند را خوانده و این حقوق دسترسی را برای تمام عمر روی سند اعمال می‌کند.

کاربران مورداعتماد برای تسهیل در فرایند انتشار می‌توانند از الگوهای از پیش تعریف شده مجوزهای حفاظتی بسازند. این الگوها می‌توانند از طریق ابزارهای مشهوری مانند پردازشگرهای متن و غیره اعمال شوند. همانند شکل ۳- ۱۶ هر الگو یک سیاست استفاده از پیش تعریف شده را اعمال می‌کند.



شکل ۳- ۱۶ فرایند انتشار AD RMS

انواع نصب AD RMS

هر سازمانی از لحاظ حفاظتی دارای نیازمندی‌های خاص خود می‌باشد. به همین دلیل AD RMS دارای توزیع‌های متنوعی به شرح زیر است:

- توزیع تک‌سروری در این توزیع AD RMS روی یک سرور و برای پشتیبانی از بانک اطلاعاتی WID نصب می‌شود. به دلیل اینکه همه اجزاء محلی هستند دسترس‌پذیری سرویس آنها زیاد نیست. در محیط‌های تست نصب می‌شود اگر بخواهیم از این نوع در آنسوی دیواره آتش استفاده کنیم باید استثنائات AD RMS را به شکل مناسب اضافه کنیم.

- توزیع داخلی در این حالت نصب روی چند سرور انجام می‌شود که با دایرکتوری AD DS عجین شده‌اند. ما باید یک سرور مجزا برای بانک AD RMS در نظر بگیریم وگرنه نقش AD RMS قابلیت تقسیم بار نخواهد داشت.

- توزیع اکسترانت وقتی کاربران سیار باشند و از محدوده شبکه خارج شوند باید از این نوع توزیع استفاده کنیم. در این مدل باید استثنائات دیواره آتش را به طور مناسبی پیکربندی کنیم و URL اکسترانت مخصوصی را روی سرور وب به سمت شبکه بیرونی اضافه کنیم تا کلاینت‌های خارجی اجازه ارتباط داشته باشند.

- توزیع multifoerst این نوع توزیع را زمانی به کار می‌بریم که شرکاء بر اساس AD DS forest trust با هم ارتباط دارند. در این حالت باید روی هر forest یک سرور AD RMS نصب کنیم. بعد به هر وب‌سایت که میزبان

کلاسترهای AD RMS می‌باشد یک گواهی SSL اعطاء می‌کنیم. همچنین باید AD DS forest schema را توسعه دهیم تا اشیاء AD RMS را شامل شود. اگر در هر forest یک سرور Exchange موجود باشد نیازی به توسعه نیست. در نهایت حساب سرویس AD RMS که سرویس را اجرا می‌کند باید برای همه forest ها مورد اعتماد باشد.

- AD RMS با توزیع AD FS همچنین امکان توسعه کلاستر ریشه به forest های دیگر از طریق AD FS وجود دارد. برای این کار باید شرایط را به شکل زیر آماده کنیم:

۱. یک گواهی SSL به وب سایت میزبان کلاستر ریشه AD RMS در نظر بگیریم. این کار باعث تضمین ارتباط امن بین کلاستر و سرور AD FS resource می‌شود.

۲. کلاستر ریشه نصب شود.

۳. قبل از نصب نقش Identity Federation Support مربوط به AD RMS ارتباط federated trust را آماده کنیم.

۴. روی سرور AD FS resource partner یک برنامه claims-aware برای popline های مجوز و گواهی بسازیم.

۵. حق کاربری Generate Security Audits را به حساب سرویس AD RMS اعطاء می‌کنیم.

۶. URL کلاستر اکسترانت را در AD RMS تعریف می‌کنیم و بعد سرویس نقش AD RMS Identity Federation Support را از طریق Server Manager نصب می‌کنیم. در حین نصب به federation URL نیاز داریم.

- توزیع سرور در حالت Licensing-Only در شبکه‌های پیچیده گاهی نیاز است علاوه بر کلاستر ریشه یک کلاستر licensing-only AS RMS داشته باشیم. در این گونه موارد باید ابتدا یک گواهی‌نامه SSL به وب سایت میزبان کلاستر ریشه AD RMS داده و سپس کلاستر ریشه را نصب کنیم. بعد از آماده‌سازی موارد فوق می‌توانیم سرور lincensing-only را نصب کنیم.

- ارتقاء Windows RMS به AD RMS جهت ارتقاء سرور موارد زیر را باید انجام می‌دهیم:

۱. سیستم‌های RMS باید دارای سرویس پک ۱ باشند.

۲. بهتر است از همه سرورها و بانک اطلاعاتی پیکربندی پشتیبان تهیه کنیم.

۳. اگر از ثبت‌نام آفلاین برای Windows RMS استفاده می‌کنیم باید از تکمیل ثبت‌نام مطمئن شویم.

۴. اگر در سرویس دایرکتوری service connection point داشته باشیم باید از همان URL برای ارتقاء استفاده کنیم.

۵. اگر بانک اطلاعاتی Windows RMS روی MSDE قرار دارد باید به نسخه SQL Server ارتقا یابد.

۶. صف RMS Message Queuing را خالی کرده تا همه پیغام‌ها روی بانک RMS logging نوشته شود.

۷. قبل از ارتقاء سرور licensing-only کلاستر ریشه را ارتقاء می‌دهیم. این کار باعث می‌شود هنگام ارتقاء سرور licensing ، self-signed SLC کلاستر ریشه در دسترس باشد.

۸. همه سرورهای دیگر را در کلاستر RMS ارتقاء می‌دهیم.

این سناریوها مهم‌ترین ساختارهای توزیع AD RMS است.

نصب AD RMS

نصب کامل AD RMS کاملا پیچیده است. به خاطر داشته باشید که در یک AD DS forest باید یک کلاستر وجود داشته باشد و همه پیش‌نیازها نیز قبلا آماده شده باشد. در طول این فرایند آماده‌سازی باید تصمیم بگیریم سیستم‌های AD RMS را چگونه توزیع کنیم. آیا فقط از اعضاء کلاستر ریشه استفاده می‌شود یا وظایف بین کلاسترهای ریشه و licensing تقسیم می‌شود؟ آیا تعاملی با خارج از شبکه داریم؟ آیا توزیع فقط داخلی است؟ جواب هر کدام از این سئوال‌ها معماری توزیع و پیاده‌سازی AD RMS را شکل می‌دهد. پس از این مقدمات آماده نصب هستیم. این کار عملیات چندمرحله‌ای بوده و به مراقبت و توجه نیاز دارد.

آماده‌سازی مقدمات نصب AD RMS

نصب AD RMS دارای پیش‌نیازهای بسیاری است. اگر هدف تست باشد موارد کمتر خواهد بود ولی اگر در محیط واقعی پیاده‌سازی شود باید در منتهای دقت کار انجام شود. بنابراین محیط تست را تا حد ممکن شبیه محیط واقعی طراحی می‌کنیم تا در حین کار در محیط واقعی به مشکل جدیدی برخورد نکنیم.

با پیش‌نیازها شروع می‌کنیم. جدول ۱- ۱۶ نیازمندی‌های اساسی دیگر نصب AD RMS را خلاصه می‌کند.

جدول ۱- ۱۶ نیازمندی‌های سیستم RMS

سخت‌افزار / نرم‌افزار	نیازمندی‌ها	پیشنهادات

پردازشگر	یک پردازشگر Pentium 4.3 GHz یا بالاتر	دو پردازشگر Pentium 4.3 GHz یا بالاتر
حافظه	512 MB	1024 MB
فضای دیسک	40 GB	80 GB
سیستم عامل	هر کدام از نسخه‌های ویندوز سرور 2008 به غیر از Web Edition و سیستم‌های Itanium-based	ویندوز سرور نسخه Enterprise یا Datacenter
فایل سیستم	FAT32 یا NTFS	NTFS
Messaging	Message Queuing	
سرویس‌های وب	IIS با ASP.NET	

جدول ۲- ۱۶ ملاحظات AD RMS

کامپوننت	ملاحظات
URL سرور وب	URL هایی را که تغییر نمی‌کنند رزرو می‌کنیم و نام کامپیوتر را در آن دخیل نمی‌کنیم. از localhost نیز استفاده نمی‌کنیم. برای ارتباطات داخلی و خارجی از URL های متفاوت استفاده می‌کنیم.
Active Directory Domain Services	از دامنه AD DS ویندوز سرور 2000 با سرویس پک ۳ یا ویندوز سرور 2003 و یا 2008 استفاده می‌کنیم. در صورت امکان دامنه دیگری در ویندوز سرور 2008 ایجاد می‌کنیم.
محل نصب	AD RMS را روی همان دامنه‌ای که کاربران آن حضور دارند نصب می‌کنیم. در صورت امکان یک forest با چند دامنه نصب می‌کنیم و AD RMS را در دامنه اصلی فرزند نصب می‌کنیم.
حساب دامنه	از آدرس‌های E-mail پیکربندی شده در AD DS استفاده می‌کنیم.
حساب سرویس	از حساب‌های کاربری دامنه استاندارد که عضو گروه Administrators محلی هستند استفاده می‌کنیم. حساب‌های سرویس مبتنی بر دامنه که حق کاربری Genetate Security Audits دارند مناسب هستند.

حساب نصب	از یک حساب دامنه استفاده می‌کنیم. این حساب نباید روی کارت هوشمند باشد. باید دارای دسترسی مدیریتی محلی داشته باشد. برای تولید connection point باید عضو گروه Enterprise Admins باشد. برای استفاده از بانک اطلاعاتی خارجی باید عضو نقش System Administrators روی سرور DB باشد.
سرور بانک اطلاعاتی	از WID یا سرور SQL 2005 با سرویس پک ۲ به بعد استفاده می‌شود که حاوی stored procedute باشد. برای تحمل خرابی از سرور SQL 2005 با سرویس پک ۲ نصب شده روی کامپیوتر دیگر استفاده می‌شود.
Database instance	Instance بانک اطلاعاتی AD RMS را ساخته و نام‌گذاری می‌کنیم. سپس سرویس SQL Server Browser را قبل از نصب استارت می‌کنیم.
گواهی‌نامه نصب	یک گواهی SSL برای کلاستر AD RMS دریافت می‌کنیم. از گواهی‌نامه‌ها فقط در محیط‌های تست استفاده می‌کنیم. یک گواهی‌نامه مورد اعتماد از یک CA تجاری خارجی دریافت کرده و گواهی را قبل از نصب AD RMS نصب می‌کنیم.
محافظت از کلید کلاستر	کلید کلاستر را در بانک اطلاعاتی پیکربندی AD RMS ذخیره می‌کنیم. در صورت امکان از دستگاه محافظ سخت‌افزار برای ذخیره کلید استفاده می‌کنیم و آنرا روی همه سرورها نصب می‌کنیم
پیکربندی DNS	رکوردهای CNAME سفارشی مجزا برای URL کلاستر ریشه و سرور بانک اطلاعاتی می‌سازیم
نام سرور صادرکننده گواهی	قبل از نصب یک نام رسمی انتخاب می‌کنیم. مثلا نام سازمان خود
کلاینت AD RMS	از مرورگر یا برنامه‌ای که بتواند با AD RMS کار کند استفاده می‌کنیم.(Word، Outlook، PowerPoint)
استفاده از کارت هوشمند	می‌تواند با AD RMS عجین شود ولی نه برای راه‌اندازی. از کارت هوشمند برای حساب مخصوص نصب استفاده نمی‌کنیم چون کار نمی‌کند.
سیستم عامل کلاینت	ویندوز ویستا به صورت پیش‌فرض حاوی کلاینت AD RMS است. ولی ویندوز XP به کلاینت RMS با سرویس پک ۲ نیاز دارد.

همان‌طور که می‌بینیم نصب AD RMS در محیط واقعی کار ساده‌ای نیست.

درک گواهی‌نامه‌های AD RMS

AD RMS به دلیل اینکه داده‌ها را رمزنگاری می‌کند همانند AD CS از گواهی‌نامه‌ها استفاده می‌کند و این گواهی‌نامه‌ها را در زیرساخت AD RMS به کاربران مختلفی اعطاء می‌کند. همچنین از مجوزها در قالب Extensible Rights Markup Language (XrML) بهره می‌برد. به دلیل اینکه این مجوزها در محتوای تولید شده توسط کاربر درج می‌شوند از جهتی گواهی نیز محسوب می‌شوند. همانند AD CS ، AD RMS زنجیره‌ای از trust را تشکیل می‌دهد که بتواند گواهی یا مجوز را اعتبارسنجی کند. جدول ۳- ۱۶ گواهی‌نامه‌های مختلف مورد نیاز زیرساخت AD RMS را خلاصه می‌کند.

جدول ۳- ۱۶ گواهی‌نامه‌های AD RMS

گواهی‌نامه	محتوا
گواهی Server licensor (SLC)	گواهی‌نامه خودکار می‌باشد که در طول راه‌اندازی AD RMS اولین سرور در کلاستر ریشه تولید می‌شود. اعضاء دیگر کلاستر ریشه این SLC را به اشتراک می‌گذارند. اگر کلاستر licensing-only پیکربندی شود خود SLC ساخته و آنرا با اعضاء کلاستر خود به اشتراک می‌گذارد. طول عمر هر SLC ۲۵۰ سال است.
گواهی‌نامه Right account (RAC)	RAC ها برای کاربران مورد اعتماد که حساب email-enabled در AD DS دارند صادر می‌شود. RAC ها وقتی کاربر برای اولین بار سعی می‌کند محتوای محافظت شده را باز کند ساخته می‌شوند. RAC های استاندارد کاربران را به همراه کامپیوترشان تشخیص می‌دهد و طول عمر ۳۶۵ روز دارند. RAC های موقت کاربر را به کامپیوتر مشخصی نسبت نمی‌دهند و برای ۱۵ دقیقه اعتبار دارند. RAC حاوی کلید عمومی و خصوصی کاربر است. کلید خصوصی با کلید خصوصی کامپیوتر رمزنگاری می‌شود. (به گواهی‌نامه Machine در همین جدول مراجعه شود.)
گواهی‌نامه Client licensor (CLC)	پس از اینکه کاربر RAC دریافت کرد و برنامه AD RMS-enabled را اجرا کرد برنامه به طور خودکار یک درخواست CLC به کلاستر AD RMS ارسال می‌کند. برای این کار کامپیوتر کلاینت باید در شبکه باشد ولی بعد از دریافت CLC می‌تواند از شبکه خارج شود. به دلیل اینکه CLC با RAC مربوط به کلاینت عجین است اگر RAC لغو شود CLC نیز بی اعتبار خواهد شد. CLC حاوی کلید عمومی licensor کلاینت، کلید خصوصی licensor کلاینت که توسط کلید عمومی کاربر رمزنگاری می‌شود و کلید عمومی کلاستر AD RMS می‌باشد. کلید خصوصی CLC برای رمزنگاری محتوا استفاده می‌شود.
گواهی‌نامه Machine	وقتی برای اولین بار برنامه AD RMS-enabled استفاده می‌شود این گواهی ساخته می‌شود.

	کلاینت AD RMS در ویندوز به طور خودکار این فرایند را مدیریت می‌کند. این گواهی‌نامه container امنی را روی کامپیوتر ایجاد می‌کند که گواهی‌نامه machine با پروفایل کاربر مرتبط شود. این گواهی‌نامه حاوی کلید عمومی برای کامپیوتر فعال شده است. کلید خصوصی در آن container قرار می‌گیرد.
مجوز انتشار	این مجوز زمانی ساخته می‌شود که کاربر محتوا را به حالت محافظت شده ذخیره کند. این مجوز مشخص می‌کند کدام کاربران و تحت چه شرایطی می‌توانند از محتوا استفاده کنند و چه حقوقی در مورد محتوا دارند. این مجوز برای رمزگشایی محتوا از کلید محتوای متقارن و کلید عمومی کلاستر بهره می‌برد.
مجوز استفاده	مجوز استفاده به کاربری که محتوای محافظت شده را باز می‌کند تعلق می‌گیرد. با RAC کاربر عجین شده و حقوق دسترسی کاربر روی محتوا را لیست می‌کند. اگر RAC در دسترس نباشد کاربر نمی‌تواند با محتوای محافظت شده کار کند. حاوی کلید متقارن برای رمزگشایی محتواست. این کلید با کلید عمومی کاربر رمزنگاری می‌شود.

مراحل نصب

حالا که نیازمندی‌های نصب را متوجه شدیم آماده نصب می‌شویم. قبل از شروع باید مقدمات لیست شده در جدول ۱- ۱۶ را آماده کنیم.

نصب AD RMS

۱. با کاربر Enterprise Administrator به سرور عضو دامنه دارای ویندوز سرور 2008 نسخه Standard یا Enterprise و یا Datacenter وارد می‌شویم.

۲. کنسول Server Manager را باز می‌کنیم.

۳. روی گره Roles کلیک راست کرده و Add Roles را انتخاب می‌کنیم.

۴. اطلاعات Before You Begin را مرور کرده و Next می‌زنیم.

۵. در صفحه Select Server Roles ، Active Directory Rights Management Services را انتخاب کرده و روی Next کلیک می‌کنیم. ویزارد Add Role از ما می‌خواهد که نقش Web Server (IIS) را با ویژگی‌های مورد نیاز، Windows Process Activation Services (WPAS) و Message Queuing را اضافه کنیم.

۶. اگر این سرویس‌ها نصب نباشند روی Add Required Role Services کلیک می‌کنیم. روی Next کلیک می‌کنیم.

۷. در صفحه Active Directory Rights Management Services اطلاعات نقش انتخاب شده را مرور کرده و روی Next کلیک می‌کنیم.

۸. در صفحه Select Role Services علامت کادر Active Directory Rights Management Server را زده و روی Next کلیک می‌کنیم. گزینه Identity Federation Support را در این مرحله انتخاب نمی‌کنیم. این گزینه را تا بعد از ساخت ارتباط AD FS federation نمی‌توانیم نصب کنیم.

۹. در صفحه Create Or Join An AD RMS Cluster گزینه Create A New AD RMS Cluster را انتخاب کرده و روی Next کلیک می‌کنیم. اگر کلاستر قبلا ساخته شده باشد و در حال نصب سرور دوم باشیم باید Join An Existing AD RMS Cluster را انتخاب کنیم چون در هر forest فقط یک کلاستر می‌توانیم داشته باشیم.

۱۰. در صفحه Select Configuration Database ، Use A Different Database Server را انتخاب کرده و روی Next کلیک می‌کنیم. اگر بخواهیم از WID برای میزبانی بانک اطلاعاتی AD RMS استفاده کنیم مراحل ۱۱ و ۱۲ حذف می‌گردد. به خاطر داشته باشید که وقتی از WID استفاده می‌کنیم دیگر نمی‌توانیم سروری را به این کلاستر اضافه کنیم. از WID در محیط‌های تست استفاده می‌شود اگر منابع سخت‌افزاری برای سرور بانک اطلاعاتی مناسب کافی نباشد.

۱۱. برای پیدا کردن سرور میزبان بانک اطلاعاتی روی Select کلیک کرده و نام آنرا تایپ کرده و روی Check Names کلیک می‌کنیم. سپس روی OK کلیک می‌کنیم.

۱۲. در لیست بازشوی Database Instance مورد مناسب را انتخاب کرده روی Validate و سپس روی Next کلیک می‌کنیم.

۱۳. در صفحه Specify Service Account روی Specify کلیک کرده ، حساب کاربری و کلمه عبور دامنه را که برای حساب سرویس AD RMS باید استفاده شود تایپ کرده، روی OK کلیک کرده و سپس Next را می‌زنیم. این حساب باید عضو گروه Administrators محلی باشد.

۱۴. در صفحه Configure AD RMS Cluster Key Storage گزینه Use CSP Key Storage را انتخاب کرده و سپس Next را می‌زنیم. ما از روش cryptographic storage privider به منظور محافظت از کلید کلاستر AD RMS استفاده می‌کنیم به دلیل اینکه روش امن‌تری است. در این روش باید یک storage provider را انتخاب کرده و این

گواهی‌نامه را روی همه سرورهای AD RMS قبل از اینکه بتوانیم آنها را به کلاستر ریشه اضافه کنیم نصب می‌کنیم. همچنین می‌توانیم کلید را در بانک اطلاعاتی AD RMS ذخیره کنیم ولی امنیت آن نسبت به حالت قبل پایین‌تر است.

۱۵. در صفحه Specify AD RMS Cluster Key گزینه CSP را انتخاب می‌کنیم. امکان انتخاب cryptographic service provider سخت‌افزاری یا نرم‌افزاری وجود دارد. از این دو هر کدام که به سیاست‌های امنیتی ما نزدیک‌تر است انتخاب کرده و Create A New key With The Selected CSP را انتخاب می‌کنیم. روی Next کلیک می‌کنیم. همچنین می‌توانیم از کلید موجود نیز استفاده کنیم ولی زمانی این کار را انجام می‌دهیم که یک بانک اطلاعاتی پیکربندی خراب شده را بازیابی می‌کنیم.

۱۶. در صفحه Select AD RMS Cluster Web Site وب سایت مورد نظر برای نصب سرویس‌های وب AD RMS را انتخاب می‌کنیم و روی Next کلیک می‌کنیم. اگر تا آن موقع وب سایت آماده نباشد نام وب سایت Default Web Site خواهد شد.

۱۷. در صفحه Specify Cluster Address گزینه Use An SSL-Encrypted Connection (https://) را انتخاب می‌کنیم. به عنوان بهترین روش امنیتی کلاستر AD RMS بهتر است با استفاده از ارتباط رمزنگاری شده SSL کار کند. بهتر است از یک گواهی‌نامه صادر شده از CA تجاری خارجی استفاده شود به طوری که همه قابل اعتماد باشد. بهتر است این گواهی‌نامه قبلا روی یک سرور نصب شود به طوری که بتوانیم در مراحل نصب آنرا انتخاب کنیم. از ارتباطات رمزنگاری شده بپرهیزیم. وقتی قصد استفاده از Identity Fedetation برای AD RMS خود داریم نباید از ارتباطات ناامن استفاده کنیم.

۱۸. در بخش Internal Address از صفحه Specify Cluster Adderss نام FQDN کلاستر AD RMS را تایپ کرده و روی Validate کلیک می‌کنیم. اگر اعتبار تایید شد روی Next کلیک می‌کنیم. این نام باید یک نام FQDN معتبر باشد و در آینده قابل تغییر نیست. اگر بخواهیم پورت پیش‌فرض ارتباطات AD RMS را تغییر دهیم در همین صفحه می‌توانیم این کار را انجام دهیم. تغییر پورت نیز در آینده امکان‌پذیر نمی‌باشد.

۱۹. روی validate کلیک کرده و روی Next کلیک می‌کنیم.

۲۰. در صفحه Choose A Server Authentication Certificate For SSL Encryption گزینه Choose An Existing Certificate For SSL Encryption (Recommended) را انتخاب کرده و گواهی‌نامه نصب شده را انتخاب و روی Next کلیک می‌کنیم. اگر گواهی‌نامه از قبل نصب نشده باشد روی Import کلیک می‌کنیم تا گواهی را

منتقل کنیم. از گواهی self-signed نیز می‌توانیم استفاده کنیم یا اگر گواهی دریافت نشده باشد گزینه سوم را انتخاب می‌کنیم تا رمزنگاری را به بعد موکول کنیم. بهرحال اگر آخرین گزینه انتخاب شود تا این گواهی دریافت و نصب نشود نصب AD RMS کامل نمی‌شود.

۲۱. در صفحه Name The Server Licensor Certificate نام کلاستر AD RMS را تایپ کرده و روی Next کلیک می‌کنیم.

۲۲. در صفحه Register AD RMS Service Connection Point گزینه Register The AD RMS Service Connection Point Now را انتخاب و روی Next کلیک می‌کنیم. این کار باعث ثبت AD RMS service connection point (SCP) در AD DS می‌شود. اگر در حین آماده‌سازی کلاستر هستیم و نیاز به نصب اعضاء دیگر کلاستر قبل از شروع سرویس دهی به درخواست‌ها داریم گزینه Reginster The AD RMS Service Connection Point Later را انتخاب می‌کنیم.

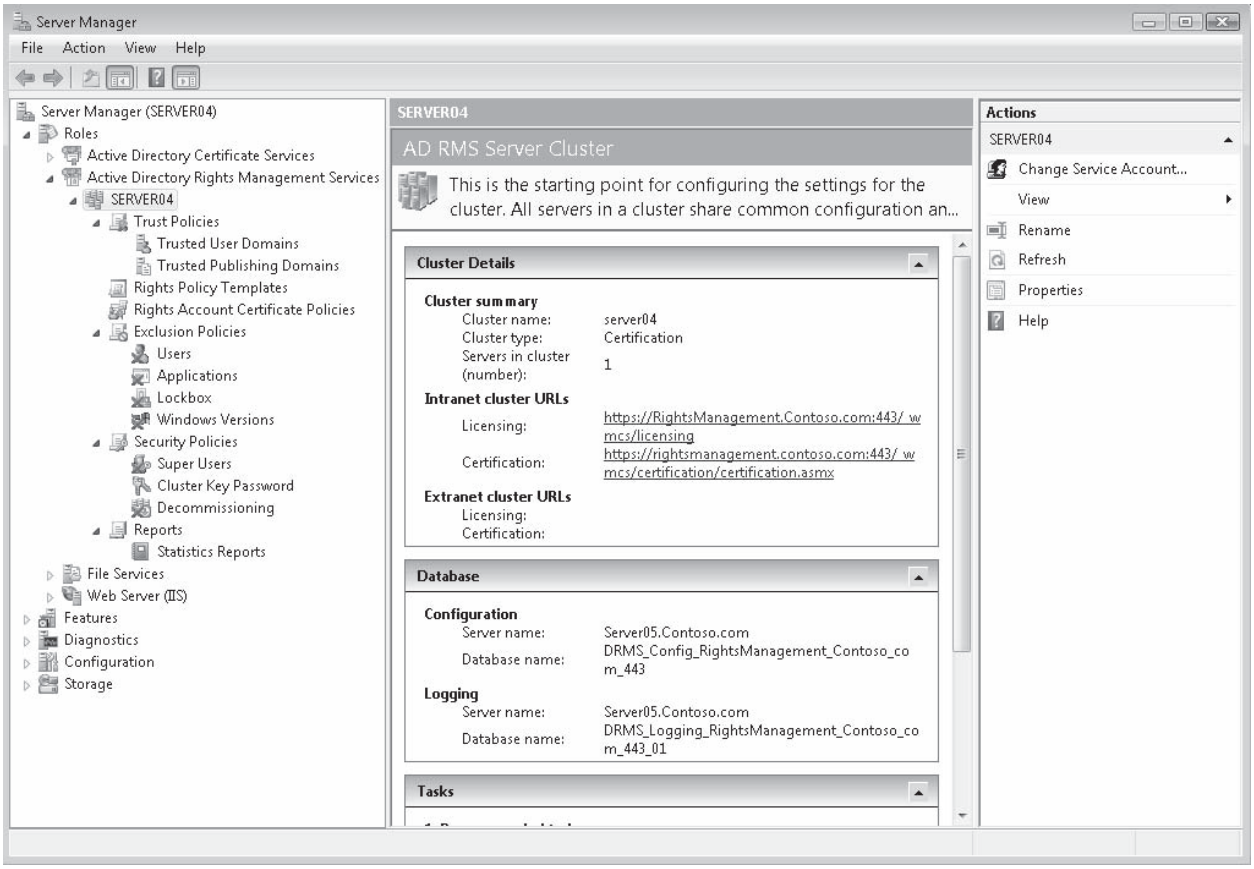
۲۳. در صفحه Web Server (IIS) اطلاعات IIS را مرور می‌کنیم و روی Next کلیک می‌کنیم. صفحات اشاره شده در مراحل ۲۳ و ۲۴ فقط در صورتی نمایش می‌یابند که قبلا IIS روی سرور نصب نشده باشد.

۲۴. در صفحه بعد انتخاب‌های پیش‌فرض سرور وب را نگه داشته و روی Next کلیک می‌کنیم.

۲۵. در صفحه Confirm Installation Selection انتخاب‌های خود را مرور کرده و روی Install کلیک می‌کنیم.

۲۶. وقتی نصب کامل شد روی Finish کلیک می‌کنیم. از ویندوز خارج و دوباره وارد می‌شویم تا مجوزهای اعطاء شده به حساب کاربری به روز گردد. حساب کاربری وارد شده وقتی نقش سروری AD RMS نصب می‌شود به طور خودکار عضو گروه AD RMS Enterprise Administrators . این کار باعث می‌شود به همه اجزاء AD RMS دسترسی پیدا کنیم.

حالا نصب کامل شده است (شکل ۴- ۱۶)



شکل ۴- ۱۶ وقتی نصب تمام شد کل ساختار درختی AD RMS در Service Manager ظاهر می‌شود.

تمرینات نصب AD RMS

در این تمرین AD RMS را در یک cluster جدید نصب می کنیم. در ابتدا باید یک رکورد DNS اضافه کنیم. در تمرین های زیر حساب سرویس و گروه های نقش AD RMS را در دایرکتوری می سازیم. گواهی‌نامه سرور وب ساخته و نصب را ادامه می‌دهیم. برای این تمرین به SERVER01 ، SERVER04 و SERVER05 نیاز داریم.

تمرین اول آماده‌سازی رکورد DNS

در این تمرین یک رکورد CNAME برای آماده کردن AD RMS cluster URL می سازیم

۱- با اعتبار مدیر دامنه وارد SERVER01 می شویم

۲- Server Manager را از Administrative Tools اجرا می کنیم

۳- به Roles\DNS Server\DNS\SERVER01\Forward Lookup Zones\contoso.com می رویم

٤- روی پنجره سمت راست کلیک کرده و New Alias (CNAME) را انتخاب می کنیم

٥- در کادر محاوره ای New Resource Record ، **RightsManagement را تایپ کرده و در بخش** Target Host آنرا به صورت Fully Qualified Domain Name (FQDN) به SERVER04.contoso.com اختصاص می دهیم و روی OK کلیک می کنیم

اکنون یک رکورد جدید برای AD RMS cluster URL ساخته ایم . با انجام دیگر تمرین ها این رکورد در دیگر سرورها بروز می شود

تمرین دوم آماده‌سازی دایرکتوری

در این تمرین چهار گروه و یک حساب سرویس برای اعطاء اختیار مدیریت AD RMS خواهیم ساخت

۱- با کاربر Administrator دامنه وارد SERVER01 می شویم

۲- Server Manager را از Administrative Tools اجرا می کنیم

۳- به Roles\Active Directory Domain Services\Active Directory Users and Computers \contoso.com رفته و ساختار OU را به شکل Admins\Service Identities می سازیم

۴- روی Service Identities راست کلیک کرده و New و سپس User را انتخاب می کنیم
۵- نام کاربر را **ADRMSService انتخاب کرده و از این نام در نام ورود به سیستم** و pre–Windows 2000 logon names استفاده کرده و روی Next کلیک می کنیم
۶- یک کلمه عبور پیچیده انتخاب می کنیم. User Must Change Password At Next Logon را از حالت انتخاب خارج کرده و Password Never Expires را انتخاب می کنیم. برای اتمام کار روی Next و سپس Finish کلیک می کنیم.
۷- اکنون ، در صورت موجود نبودن ، یک گروه مدیریتی AD RMS در Contoso.com\Admins\Admin Groups\Server Delegations می سازیم
۸- چهار گروه امنیتی global می‌سازیم. در پنجره سمت راست ، راست کلیک کرده و ابتدا New و سپس Group را انتخاب می کنیم. نام را تایپ کرده و روی OK کلیک می‌کنیم. سپس چهار گروه زیر را می‌سازیم:

- AD RMS Enterprise Administrators
- AD RMS Template Administrators
- AD RMS Auditors
- AD RMS Service Account

۹- AD RMS Service Account group را با راست کلیک کردن و انتخاب Properties باز می کنیم و روی زبانه Members کلیک می کنیم. حساب ADRMSService را به این گروه اضافه کرده و روی OK کلیک می کنیم
۱۰- با اعتبار مدیر دامنه وارد SERVER03 می شویم
۱۱- Server Manager را از Administrative Tools اجرا می کنیم
۱۲- گره Configuration\Local Users and Groups\Groups را باز می‌کنیم.
۱۳- گروه Administrators را انتخاب کرده و آن را باز می کنیم
۱۴- گروه AD RMS Service Account را به این گروه اضافه می کنیم و روی OK کلیک می کنیم

اکنون آماده برای ادامه نصب هستیم

تمرین سوم آماده کردن گواهی‌نامه سرور وب

چون AD RMS نیازمند یک ارتباط وب رمزگذاری شده با SSL می باشد باید قبل از عملیات نصب یک گواهی‌نامه وب سرور برای آن بسازیم.

۱- با اعتبار مدیر شبکه دامنه وارد SERVER04 می شویم

این کار به ما اعتبار Enterprise Administrator می دهد که برای ساختن SCP لازم است. این دسترسی برای تمرین ۴ مورد نیاز است.

۲- Server Manager را از Administrative Tools اجرا می کنیم.
۳- گره Roles\Active Directory Certificate Services\Certificate Templates (SERVER04) را باز کرده و می بینیم که تمام الگوهای موجود در این پنجره لیست شده اند
۴- الگوی Web Server را انتخاب کرده و روی آن راست کلیک کرده و Duplicate Template را انتخاب می کنیم
۵- نسخه ویندوز سرور را – در این مورد ویندوز سرور 2008 – انتخاب می کنیم و روی OK کلیک می کنیم
۶- نام الگو را **Web Server WS08 انتخاب کرده و بجز گزینه های زیر بقیه را بدون تغییر رها می‌کنیم.**

- در زبانه General ، از انتخاب Publish Certificate In Active Directory مطمئن می شویم
- در زبانه Security ، حساب کامپیوتر SERVER04 را اضافه می کنیم. روی Add و Object Types کلیک کرده و Computers را انتخاب می کنیم و روی OKکلیک می کنیم
- عبارت **SERVER04 را تایپ کرده و روی** Check Names و سپس OK کلیک می کنیم.
- به SERVER04 مجوزهای Allow:Read و Enroll را اعطاء کرده و روی OK کلیک می کنیم
- تنظیمات دیگر ار بدون تغییر رها می کنیم

۷- روی OK کلیک می کنیم

انتشار الگو در بخش کنسول Certification Authority در Server Manager اجرا می شود

۸- گره Roles\Active Directory Certificate Services\Contoso-*issuing-serve*\Certificate Templates را باز می‌کنیم.
۹- برای صدور یک الگو روی Certificate Templates راست کلیک کرده و New و سپس Certificate Template To Issue را انتخاب می کنیم

۱۰- در کادر محاوره ای Enable Certificate Templates ، Web Server WS08 را انتخاب کرده و روی OK کلیک می کنیم

تمرین چهارم نصب گواهی‌نامه سرور وب

اکنون باید درخواست گواهی‌نامه را صادر و نصب کنیم

۱- در منوی استارت در کادر جستجو عبارت **mmc را نوشته و** روی Enter کلیک می کنیم
۲- از منوی File روی Add/Remove Snap-insکلیک کرده و بعد از انتخاب Certificates snap-in روی Add کلیک می کنیم
۳- Computer Account را انتخاب کرده و روی Next کلیک می کنیم
۴- مطمئن می شویم که همین کامپیوتر انتخاب شده است، سپس روی Finish و بعد OK کلیک می کنیم
۵- از منوی File روی Save As کلیک کرده و به پوشه Documents رفته و با نام **Computer Certificates ذخیره می کنیم**
۶- گره Certificates (Local Computer)\Persona l\Certificates را باز می کنیم
۷- روی Certificates راست کلیک کرده و All Tasks و بعد Request New Certificate را انتخاب می کنیم. روی Next کلیک می کنیم
۸- Web Server WS08 certificate را انتخاب کرده و روی More Information to enroll for this certificate کلیک می کنیم
۹- در کادر محاوره ای Certificate Properties در زبانه Subject مقادیر زیر را اضافه می کنیم
- در کادر *Subject Name Value* مطمئن می شویم که Full DN انتخاب شده است و عبارت **CN=SERVER04,DC=Contoso,DC=com** را تایپ کرده و روی Add کلیک می کنیم
- روی بخش Alternative Name کلیک کرده و در منوی بازشو URL را انتخاب می کنیم و در کادر *Value عبارت* **RightsManagement.contoso.com** را نوشته و سپس روی Add کلیک می کنیم
- در زبانه General عبارت **Contoso DRM را در کادر** *Friendly Name* و عبارت **Web Server Certificate** را در کادر *Description* می نویسیم
- روی زبانه Private Key کلیک کرده و بخش Key Options را باز می کنیم و Make Private Key Exportable and Allow Private Key To Be Archived را انتخاب می کنیم

۱۰- روی OK و سپس Enroll و در آخر Finish کلیک می کنیم
۱۱- برای اطمینان از صدور گواهی‌نامه، روی Certificates کلیک کرده و در پنجره سمت راست اطلاعات را مرور می کنیم
۱۲- کنسول Certificates را می بندیم

اکنون آماده نصب AD RMS هستیم

تمرین پنجم نصب AD RMS Root Cluster

مطمئن می شویم که حداقل سیستمهای SERVER01 ، SERVER03 و SERVER05 در حال کار هستند و SQL server در SERVER05 نیز در حال کار است . SERVER03 نیز باید با انجام تمرین های فصل پانزده دارای AD CS و گواهی‌نامه باشد که در این تمرین از آنها استفاده خواهد شد.

۱- با اعتبار مدیر شبکه دامنه وارد SERVER03 می شویم. این کار به ما اعتبار Enterprise Administrator می دهد که برای ساخت SCP نیاز داریم
۲- Server Manager را از Administrative Tools اجرا می کنیم
۳- روی گره Roles در پنجره راست کلیک کرده و Add Roles را انتخاب می کنیم
۴- قبل از شروع اطلاعات را مرور کرده و روی Next کلیک می کنیم
۵- در صفحه Select Server Roles ، Active Directory Rights Management Services را انتخاب می کنیم
ویزارد از ما می خواهد که نقشهای Web Server (IIS) ، Windows Process Activation Service (WPAS) و Message Queuing را نصب کنیم
۶- قبل از نصب AD RMS روی Add Required Role Services if these services weren’t installed کلیک می کنیم و روی Next کلیک می کنیم
۷- در صفحه Active Directory Rights Management Services اطلاعات را مرور کرده و روی Next کلیک می کنیم
۸- در صفحه Select Role Services مطمئن می شویم که Active Directory Rights Management Services انتخاب شده است و روی Next کلیک می کنیم
۹- در صفحه Create Or Join An AD RMS Cluster ، Create A New AD RMS Cluster را انتخاب کرده و روی Next کلیک می کنیم
۱۰- در صفحه Select Configuration Database ، Use A Different Database Server را انتخاب می کنیم و روی Next کلیک می کنیم

اگر استفاده از Windows Internal Database جهت میزبانی بانک AD RMS به صورت سرور منفرد مد نظر باشد نیازی به انجام مراحل ۱۱ و ۱۲ نیست. در هر صورت استفاده از WID تنها در شرایط تست توصیه می شود.

۱۱- برای پیدا کردن SERVER05 روی Select کلیک می کنیم. نام سرور را نوشته و روی Check Names و سپس روی OK کلیک می کنیم

۱۲- در Database Instance ، Default instance را انتخاب کرده و روی Validate کلیک می کنیم. سپس روی Next کلیک می کنیم

۱۳- در صفحه Specify Service Account روی Specify کلیک کرده و عبارت **ADRMSService و کلمه عبور آنرا را تایپ کرده** روی OK کلیک می کنیم و سپس روی Next کلیک می کنیم

۱۴- در صفحه Configure AD RMS Cluster Key Storage ، Use AD RMS Centrally Managed Key Storage را انتخاب کرده و روی Next کلیک می کنیم

علت انتخاب سیستم حفاظتی AD RMS cluster key با استفاده از بانک اطلاعاتی سادگی آن است به اجزا دیگری نیاز ندارند.

۱۵- در صفحه Specify AD RMS Cluster Key Password یک کلمه عبور پیچیده نوشته و آنرا تایید می کنیم سپس روی Next کلیک می کنیم

۱۶- در صفحه Select AD RMS Cluster Web Site ، Default Web Site را انتخاب کرده و روی Next کلیک می کنیم

۱۷- در صفحه Specify Cluster Address ، Use An SSL-Encrypted Connection (https://) را انتخاب می کنیم

۱۸- در بخش Internal Address عبارت **RightsManagement.contoso.com را تایپ کرده و شماره** پورت را بدون تغییرمی گذاریم و روی Validate کلیک کرده و بعد از اتمام روی Next کلیک می کنیم

۱۹- در صفحه Choose A Server Authentication Certificate For SSL Encryption ، Choose An Existing Certificate For SSL Encryption (Recommended) را انتخاب کرده و سپس گواهی نامه SERVER04 را انتخاب می کنیم و روی Next کلیک می کنیم

۲۰- در صفحه Name The Server Licensor Certificate برای شناسایی AD RMS cluster نام **Contoso DRM را تایپ کرده و** روی Next کلیک می کنیم

۲۱- در صفحه Register AD RMS Service Connection Point ، Register The AD RMS Service Connection Point Now را انتخاب کرده و روی Next کلیک می کنیم

این کار AD RMS service connection point (SCP) را در AD DS رجیستر خواهد کرد

۲۲- در صفحه Web Server (IIS) اطلاعات مربوط به IIS را مرور کرده و روی Next کلیک می کنیم

۲۳- در صفحه Select Role Services تنظیمات وب سرور را بدون تغییر گذاشته و روی Next کلیک می کنیم

۲۴- در صفحه Confirm Installation Selections انتخاب هایمان را مرور کرده و روی Install کلیک می کنیم

۲۵- هنگامی که نصب کامل شد برای بستن ویزارد نصب روی close کلیک می کنیم

۲۶- برای اعمال مجوز ها به کاربر وارد شده به سیستم ، یکبار از سیستم خارج شده و مجددا وارد می شویم

هنگامی که نقش AD RMS serverنصب شده باشد حساب کاربری وارد شده به سیستم به صورت اتوماتیک عضو گروه AD RMS Enterprise Administrators می شود که به ما اجازه هرگونه فعالیتی روی AD RMS را می دهد. دیگر نصب کامل شده است.

خلاصه درس

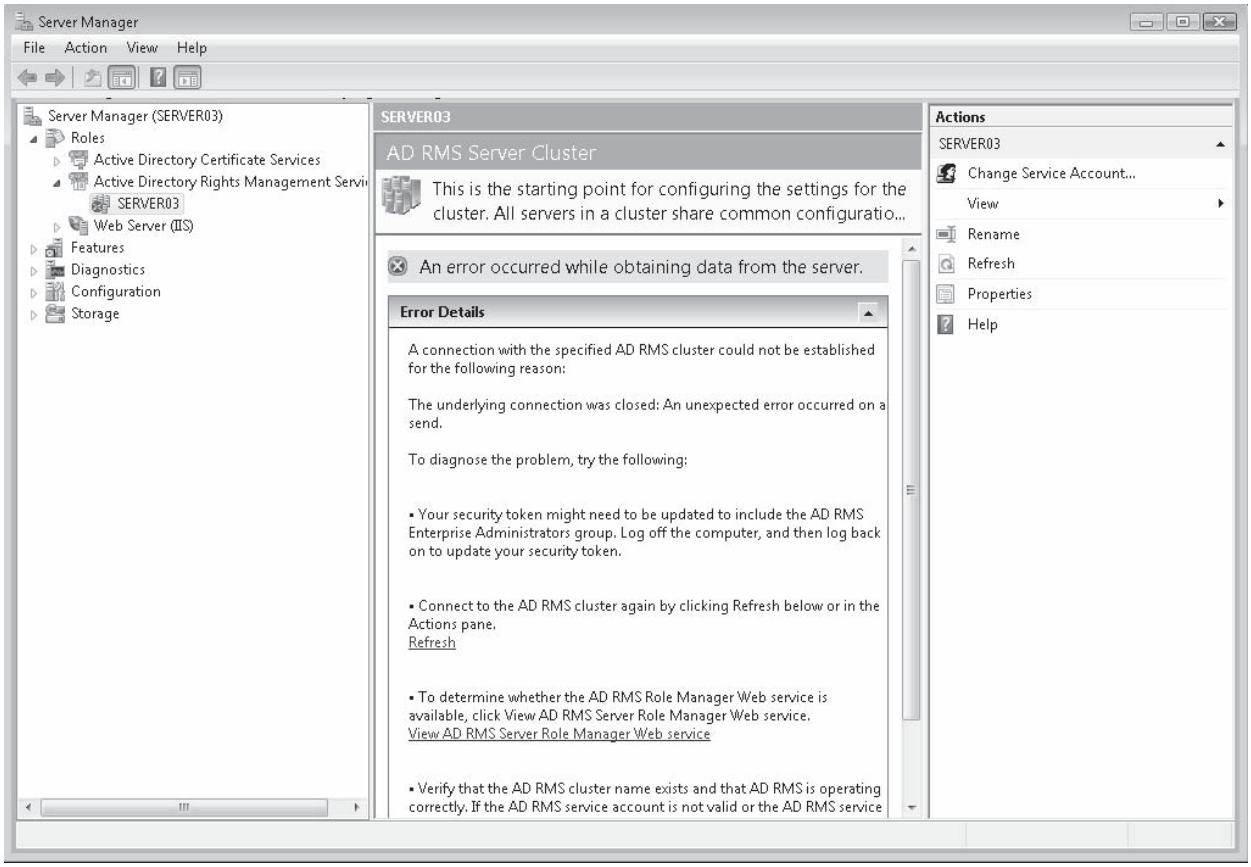
- AD RMS به منظور ارایه سرویس حفاظت از داده ها از طریق digital rights management طراحی شده است. برای انجام این کار به زیرساخت پیچیده ای اتکا می کند که به سرویس های دیگر مانند AD DS ، SQL Server و Internet Information Services و برای ارتباط بین forest ها به AD FS ، نیاز دارد
- کاربران برای استفاده از سرویس AD RMS باید در دامنه AD DS یک حساب e-mail–enabled داشته باشند
- کاربران همچنین برای محافظت از محتوا باید از برنامه های AD RMS–enabled استفاده کنند

این برنامه ها می توانند ابزارهای مفیدی مانند Office Word ، Outlook ، PowerPoint یا یک برنامه سفارشی AD RMS–enabled باشد . بدون این برنامه ها نمی توان با محتوای محافظت شده کار کرد.

- ویندوز ویستا برخلاف XP بصورت پیش فرض دارای AD RMS client می باشد. در ویندوز XP باید Windows Rights Management Client را به همراه SP2 دانلود و نصب کنیم

سئوالات پایان درس

۱- فرض کنید مدیر شبکه دامنه *contoso.com* هستیم به تازگی نصب AD RMS را تمام کرده و اکنون می خواهیم آنرا پیکربندی کنیم. نصب بدون هیچ خطایی پایان یافته است اما هنگام کار با سرور AD RMS پیام خطایی ظاهر می شود. مشکل از کجا می تواند باشد؟



A . سرور ما AD RMS ندارد.

B . گواهی‌نامه سرور نامعتبر است و به همین دلیل سرور AD RMS شروع به کار نمی کند

C . سرور عضو دامنه AD DS نیست

D . حساب کاربری دارای مجوزهای لازم برای مدیریت AD RMS را ندارد

درس ۲: پیکربندی و استفاده از AD RMS

آماده سازی نصب AD RMS فرایند پیچیده‌ای است ولی وقتی مراحل آماده‌سازی نصب به خوبی انجام شود نصب نیز بدون عیب انجام می‌شود. پس از نصب سرورها پیکربندی کلاسترهای AD RMS انجام شده و سیاست‌های استفاده مورد نظر در شبکه آماده می‌شود.

عملیات فوق شامل مراحل زیر است:

- اگر بخواهیم AD RMS بیرون از شبکه نیز در دسترس باشد باید یک URL کلاستر اکسترانت در پیکربندی بگنجانیم.
- اگر بخواهیم سرویس‌های AD RMS را با شرکاء عجین کنیم باید تنظیمات proxy را پیکربندی کنیم و Identity Federation Support را نصب کنیم. به خاطر داشته باشید که ما باید از AD FS برای افزودن این اجزاء به زیرساخت استفاده کنیم. همچنین باید سیاست‌های trust را پیکربندی کنیم تا بین کلاستر AD RMS با کلاسترهای دیگر همکاری مناسبی برقرار شود.

- باید چندین گواهی‌نامه AD RMS پیکربندی کنیم تا دوره اعتباری مورد نظر پوشش داده شود.
- اگر سازمان بخواهد سیاست‌های حفاظتی روی کل سازمان اعمال نشود و فقط گروه یا بخش‌های مخصوصی هدف این سیاست باشند باید سیاست‌های مستثنی‌کننده (exclusion) پیکربندی کنیم.
- باید حساب‌های کاربری برای عجین شدن با AD RMS آماده کنیم.
- باید الگوهای سیاست را آماده کنیم. این الگوها فرایند حفاظت دسترسی کاربران را تسهیل می‌کنند.
- باید با کلاینت‌های AD RMS مختلف آشنا باشیم تا در صورت بروز مشکل آنرا برطرف کنیم.
- AD RMS از سه بانک اطلاعاتی استفاده می‌کند. باید از این بانک‌ها اطلاع داشته باشیم و برای عملیات AD RMS آماده کنیم.

این عملیات توزیع کلاستر AD RMS را تکمیل می‌کند.

بعد از این درس می‌توانیم:

- URL های اکسترانت را پیکربندی کنیم.
- برای عجین شدن با شرکاء آماده شویم.
- با گواهی‌نامه‌های AD RMS کار کنیم.
- حساب‌های کاربری را برای AD RMS آماده کنیم.
- سیاست‌های مستثنی‌کننده را آماده کنیم.
- با الگوهای سیاست کار کنیم.
- با بانک‌های اطلاعاتی AD RMS کار کنیم.

زمان تقریبی : ۳۰ دقیقه

پیکربندی AD RMS

پیکربندی AD RMS بر خلاف Windows Rights Management Services از طریق کنسول MMC انجام می‌شود. این کنسول هم از طریق Server Manager و هم از طریق یک کنسول مجزا در Remote Server Administration Tools (RSAT) در دسترس است. همه پیکربندی‌های تکمیلی از طریق همین کنسول انجام می‌شود.

ساخت URL اکسترانت

وقتی می‌خواهیم زیرساخت AD RMS را توسعه دهیم به طوری که کاربران سیار تحت پوشش قرار گیرند باید یک URL اکسترانت پیکربندی کنیم. برای این کار باید موارد زیر را انجام دهیم:

۱. با اعتبار AD RMS Enterprise Administrators به سروری که عضو کلاستر ریشه است وارد می‌شویم.

۲. Server Manager را باز می‌کنیم.

۳. گره Roles\Active Directory Rights Management Services\servername را باز می‌کنیم.

۴. روی نام سرور کلیک راست کرده و Properties را انتخاب می‌کنیم.

۵. زبانه Cluster URLs را باز می‌کنیم.

۶. در صفحه Cluster URLs ، Extranet URLs را فعال کرده و آدرس‌های مناسب را برای Licensing و Certification وارد می‌کنیم. این URL ها باید در اکسترانت معتبر بوده و دائمی باشند. پیکربندی DNS نیز برای این URL ها باید به درستی انجام شود. از رمزنگاری SSL برای ارتباط HTTPS استفاده می‌کنیم. در نهایت دایرکتوری‌های مجازی مناسبی روی وب سایت برای میزبانی داده AD RMS می‌سازیم.

۷. روی OK کلیک می‌کنیم.

حالا URL اکسترانت آماده می‌باشد.

پیکربندی سیاست‌های Trust

تا زیرساخت AD FS در شبکه موجود نباشد نمی‌توانیم از پشتیبانی fedetation بهره‌مند شویم. AD RMS می‌تواند از چهار مدل trust پشتیبانی کند:

- دامنه‌های Trusted user باعث می‌شوند کلاستر AD RMS بتواند درخواست‌های کلاسترهای AD RMS را از AD DS forest های دیگر پردازش کند. این دامنه‌ها با انتقال گواهی‌نامه licensor سرور از کلاستر AD RMS که می‌خواهیم به کلاستر ما trust داشته باشد افزوده می‌شوند.

- دامنه‌های trusted publishing به کلاستر AD RMS ما امکان می‌دهد برای محتوای محافظت شده توسط کلاستر دیگر مجوز استفاده صادر کند. برای ساخت چنین دامنه‌ای باید SLC کلاستر publishing و کلید خصوصی آنرا به کلاستر خود منتقل کنیم.

- Windows Live ID trust کاربرانی را که دارای Windows Live ID (قبلا به آن Microsoft Passport می‌گفتند) معتبر هستند قادر می‌سازد از محتوای محافظت شده استفاده کنند ولی قادر به ساختن چنین محتوایی نیستند.

- Federated trust از طریق AD FS ایجاد می‌شود و عملکرد کلاستر AD RMS ما را تا forest هایی که trust برقرار شده گسترش می‌دهد.

هر کدام از این نوع trust اقتدار AD RMS ما را تا آن سوی محدوده forest توسعه می‌دهد.

انتقال گواهی‌نامه Licensor سرور

برای کار با دامنه‌های trusted publishing یا trusted user باید گواهی licensor سرور را از کلاستر ریشه خود یا کلاستر ریشه که قرار است با آن trust داشته باشیم منتقل کنیم. گواهی‌نامه‌ها به منظور استفاده در trust های در حال ایجاد منتقل می‌شوند. برای اجرای این فرایند باید عضو گروه AD RMS Enterprise Administrators محلی یا معادل آن باشیم.

۱. با اعتبار AD RMS Enterprise Administrators به سروری که عضو کلاستر ریشه است وارد می‌شویم.

۲. کنسول Server Manager را باز می‌کنیم.

۳. گره Roles\Active Directory Rights Management Services\servername را باز می‌کنیم.

۴. روی نام سرور کلیک راست کرده و Properties را انتخاب می‌کنیم.

۵. زبانه Server Certificate را باز کرده و روی Export Certificate کلیک می‌کنیم.

۶. در کادر محاوره‌ای Export Certificate As نام معتبری را وارد می‌کنیم. برای مثال نام کلاستر و بعد محل مناسبی را انتخاب می‌کنیم مانند پوشه Documents تا فایل .bin ساخته شود. روی Save کلیک می‌کنیم.

۷. کادر را می‌بندیم.

از این گواهی به طور کامل محافظت می‌کنیم به دلیل اینکه دسترسی به کلاستر AD RMS را کنترل می‌کنیم.

آماده‌سازی گواهی‌نامه‌های AD RMS

گواهی‌نامه‌ها به طور پیش‌فرض در حین نصب AD RMS ساخته می‌شوند. ولی ما باید دوره زمانی گواهی‌نامه را به درستی بر پایه سیاست‌های حفاظتی خود پیکربندی کنیم. از لحاظ مدیریت گواهی‌نامه چهار فعالیت قابل اجراست:

- مشخص کردن RAC
- فعال کردن ارائه گواهی برای دستگاههای سیار
- فعال کردن ارائه گواهی برای سرویس‌های سروری
- تایید هویت کلاینت‌ها از طریق کارت‌های هوشمند

مهم‌ترین این فعالیت‌ها تعیین مدت اعتبار RAC است. بقیه تنظیمات انتخابی بوده و بستگی به سیاست‌های حفاظتی ما دارد. برای تغییر مدت اعتبار RAC مراحل زیر را انجام می‌دهیم.

۱. با اعتبار AD RMS Enterprise Administrators به سروری که عضو کلاستر ریشه است وارد می‌شویم.

۲. کنسول Server Manager را باز می‌کنیم.

۳. گره Roles\Active Directory Rights Management Services\servername را باز می‌کنیم.

۴. در پنل وسط روی Change Standard RAC Validity Period کلیک می‌کنیمن.

۵. زبانه Standard RAC را باز کرده و تعداد روزهای مورد نظر را در بخش Standard RAC Validity Period وارد می‌کنیم.

۶. زبانه Temporary RAC را باز کرده و تعدا دقایق مورد نظر را در بخش Temporary RAC Validity Period وارد می‌کنیم.

۷. روی OK کلیک می‌کنیم.

RAC های استاندارد به طور پیش‌فرض برای مدت ۳۶۵ روز و RAC های موقت فقط ۱۵ دقیقه اعتبار دارند.

توجه داشته باشید که اگر از federated trust استفاده می‌کنیم باید مدت اعتبار RAC را در زیر گره Federated Identity Support تغییر دهیم نه زیر گره کلاستر ریشه.

آماده‌سازی سیاست‌های مستثنی‌کننده

سیاست مستثنی کننده برای چهار هویت ساخته می‌شود: کاربران، برنامه‌های کاربردیربا، lockbox ها و سیستم عامل ویندوز. وقتی استثنائات مشخص شود لیست آنها در مجوز استفاده برای محتوا درج می‌گردد. امکان حذف اعضاء این لیست وجود دارد ولی امکان افزودن همین عضو در مجوز استفاده وجود ندارد. به طور پیش‌فرض مجوزهای استفاده محتوای موجود شامل همه می‌شود. به همین دلیل قبل از تهیه لیست استثنائات موارد زیر را در نظر می‌گیریم:

- اعضائی را به لیست اضافه می‌کنیم که بخواهیم برای همیشه در لیست باشند.
- اگر بخواهیم عضوی را از لیست خارج کنیم باید منتظر بمانیم مجوزهای استفاده فعلی منقضی شود.
- وقتی اعتبار یکی از اعضاء مخدوش می‌شود (مثلا از شرکت اخراج شود) آنرا در لیست استثنائات قرار می‌دهیم.

وقتی تصمیم می‌گیریم لیست استثنائات بسازیم مشابه زیر عمل می‌کنیم. در این مثال کاربران را در لیست قرار می‌دهیم.

۱. با اعتبار AD RMS Enterprise Administrators به سروری که عضو کلاستر ریشه است وارد می‌شویم.
۲. کنسول Server Manager را باز می‌کنیم.
۳. گره Roles\Active Directory Rights Management Services\servername\Exclusion Policies\Users را باز می‌کنیم.
۴. در پنل Actions روی User Exclusion کلیک می‌کنیم.
۵. برای مستثنی کردن کاربران روی Exclude Users در پنل Actions کلیک می‌کنیم. ویزارد Exclude User Account اجرا می‌شود. کاربران را می‌توانیم هم از طریق آدرس e-mail یا کلید عمومی منتسب به کاربر مستثنی کنیم. روش اول برای کاربران دایرکتوری AD DS و روش دوم برای کاربران خارجی که در دایرکتوری حساب ندارند مناسب است. وقتی می‌خواهیم کاربران را از دایرکتوری AD DS مستثنی کنیم بهتر است از گروه استفاده کنیم.
۶. روش مناسب را انتخاب کرده و حساب کاربری یا string کلید عمومی را وارد می‌کنیم. سپس دکمه Next را کلیک می‌کنیم.
۷. روی Finish کلیک می‌کنیم تا ویزارد بسته شود.

آماده‌سازی حساب‌ها و حقوق دسترسی

برای اینکه کاربران بتوانند با AD RMS کارکنند باید حساب داشته باشند. این حساب‌ها در بانک اطلاعاتی ذخیره می‌شود. وقتی حسابی را حذف می‌کنیم به طور خودکار از بانک حذف نمی‌شود بلکه غیرفعال می‌شود. به همین دلیل بانک به مرور زمان حاوی

داده‌های غیرضروری می‌شود. برای جلوگیری از این مشکل هم می‌توانیم در SQL Server یک stored procedure بنویسیم که به طور خودکار این حساب‌ها را پاک کند و هم می‌توانیم اسکریپتی بنویسیم که در زمان‌های مشخص این کار را انجام دهد.

به علاوه ممکن است بخواهیم گروه Super Users داشته باشیم که کاربران با دسترسی کامل به همه محتویات محافظت شده توسط AD RMS را دربرگیرد. اعضاء این گروه خیلی شبیه recovery agent هایی هستند که برای EFS به کار می‌روند. این کاربران می‌توانند داده‌های تحت مدیریت زیرساخت AD RMS را بازیابی یا ویرایش کنند و بنابراین امکان بازیابی داده کاربرانی را که از سازمان رفته‌اند دارند.

ما معمولا بهتر است یک گروه Universal را از دایرکتوری به این نقش اختصاص دهیم. این گروه را قبل از فعال کردن Super Users در AD RMS آماده می‌کنیم. برای پیکربندی یک گروه Super User مراحل زیر را دنبال کنید.

۱. با اعتبار AD RMS Enterprise Administrators به سروری که عضو کلاستر ریشه است وارد می‌شویم.

۲. کنسول Server Manager را باز می‌کنیم.

۳. گره Roles\Active Directory Rights Management Services\servername\Security Policies را باز می‌کنیم.

۴. در پنل وسط روی Change Super Users Settings کلیک می‌کنیم.

۵. در پنل Actions روی Enable Super Users کلیک می‌کنیم.

۶. در پنل وسط روی Change Super Users Group کلیک می‌کنیم تا برگه Super User Group Property را ببینیم.

۷. آدرس e-mail گروه توزیع universal را از forest تایپ کرده یا از دکمه Browse برای پیدا کردن آن استفاده می‌کنیم.

۸. روی OK کلیک می‌کنیم تا برگه بسته شود.

اعضاء این گروه حالا به همه محتویات AD RMS دسترسی دارند. این اعضاء باید خیلی با احتیاط انتخاب شوند. ممکن است بخواهیم گروه Super Users را غیرفعال کنیم و فقط زمانی که به آن نیاز داریم آنرا فعال کنیم.

آماده‌سازی الگوهای سیاست

این الگوها در صرفه‌جویی زمان کاربران بسیار مفید هستند. ما باید کارهای متعددی را با این الگوها انجام دهیم. اول باید الگو را بسازیم. بعد باید محل الگو را مشخص کنیم.

محل الگو معمولا پوشه‌های اشتراکی در شبکه می‌باشند. در این صورت کاربران آفلاین به الگوها دسترسی ندارند و باید تنظیمات offline folder را برای این پوشه‌ها انجام دهیم. برای کسانی که به شبکه هیچ نوع دسترسی ندارند باید یک روش جایگزین برای تحویل آن در نظر بگیریم. کاربرانی که فقط به محتویات موجود دسترسی دارند نیازی به دسترسی به الگوهای سیاست ندارند.

۱. با اعتبار AD RMS Enterprise Administrators به سروری که عضو کلاستر ریشه است وارد می‌شویم.

۲. کنسول Server Manager را باز می‌کنیم.

۳. گره Roles\Active Directory Rights Management Services\servername\Rights Policy Templates را باز می‌کنیم.

۴. زیر گره AD RMS در کنسول، Rights Policy Templates (Server Manager\Roles\AD RMS\Servername) را انتخاب می‌کنیم.

۵. در پنل Actions گزینه Create Distributed Rights Policy Template را انتخاب می‌کنیم. ویزارد باز می‌شود.

۶. در صفحه Add Template Identification Information روی Add کلیک می‌کنیم.

۷. زبان را مشخص می‌کنیم نام الگو را تایپ می‌کنیم و روی Add کلیک می‌کنیم. سپس Next را می‌زنیم.

۸. در صفحه Add User Rights باید موارد زیر را انجام دهیم:

a. روی Add کلیک می‌کنیم و کاربر یا گروهی که باید به الگو دسترسی داشته باشد مشخص می‌کنیم. انتخاب Anyone باعث می‌شود همه کاربران بتوانند برای محتوا درخواست مجوز استفاده صادر کنند.

b. زیر Users And Rights باید ابتدا کاربر را انتخاب کرده و بعد در پنل Rights For User حقوق کاربر را مشخص کنیم. همچنین می‌توانیم یک حق خاص برای آن تعیین کنیم.

c. توجه داشته باشید که به طور پیش‌فرض دسترسی Grant Owner (Author) Full Control بدون زمان انقضا انتخاب خواهد شد.

d. در Rights Request URL باید URL مناسب را تایپ کنیم. این کار باعث می‌شود کاربران بتوانند درخواست‌های حقوق بیشتر را از طریق URL ارسال کنند.

۹. روی Next کلیک می‌کنیم.

۱۰. در صفحه Specify Expiration Policy یکی از سه گزینه را انتخاب کرده و مقدار را برحسب روز وارد می‌کنیم. اگر بخواهیم محتوا پس از طی زمان مشخص منقضی شود Expires After The Following Duration (Days) را انتخاب و تعداد روزها را تایپ می‌کنیم. روی Next کلیک می‌کنیم.

۱۱. در صفحه Specify Extended Policy تنظیمات زیر انجام می‌شود:

a. جهت مشاهده محتوای محافظت شده با استفاده از add-on مرورگر Enable Users را انتخاب می‌کنیم. این کار باعث می‌شود کاربرانی که برنامه سازگار با AD RMS ندارند با نصب add-on مورد نیاز بتوانند محتوای محافظت شده را مشاهده کنند.

b. اگر بخواهیم در برابر سرورهای AD RMS تایید هویت داشته باشیم Select Request A New Use License Every Time Content Is Consumed (Disable Client-Side Caching) را انتخاب می‌کنیم. توجه داشته باشید که این کار برای کاربران آفلاین کار نمی‌کند.

c. اگر بخواهیم داده‌های خاصی را به محتوای محافظت شده اضافه کنیم If You Would Like To Specify Additional Information For Your AD RMS-Enabled Applications, You Can Specify Them Here As Name-Value Pairs را انتخاب می‌کنیم. این گزینه معمولا برای برنامه‌نویسان کاربرد دارد.

۱۲. روی Next کلیک می‌کنیم. در صفحه Specify Revocation Policy می‌توانیم با انتخاب گزینه Require Revocation فرایند لغو را فعال کنیم و سپس:

a. گزینه Location Where The Revocation List Is Published (URL or UNC) را انتخاب کنیم و محل فایل لغو را مشخص کنیم. اگر از آدرس URL استفاده کنیم و کاربران داخلی و خارجی داشته باشیم URL باید هم از داخل و هم خارج شبکه در دسترس باشد.

b. گزینه Referesh Interval For Revocation List (Days) را انتخاب کرده و تعداد روزهای نگهداری لیست لغو را وارد می‌کنیم. این گزینه مشخص می‌کند چه زمانی کاربران باید لیست لغو را به روز کنند.

c. گزینه File Containing Public Key Corresponding To The Signed Revocation List را انتخاب می‌کنیم.

۱۳. روی Finish کلیک می‌کنیم.

توجه داشته باشید که وقتی فرایند لغو پیاده‌سازی می‌شود باید تنظیمات آن با احتیاط انجام شود. برای عملی شدن این فرایند باید لیست آنرا به صورت دوره‌ای منتشر کنیم.

کار با کلاینت‌های AD RMS

AD RMS برای اعطاء دسترسی به کاربران از کلاینت محلی استفاده می‌کند. دو کلاینت موجود است: کلاینت ویندوز ویستا که در ویندوز سرور 2008 نیز موجود است و کلاینتی که روی ویندوز سرور 2000 ، 2003 و ویندوز XP اجرا می‌شود. کلاینت دوم باید دانلود شده و روی همه کلاینت‌ها نصب شود. سه نسخه از این کلاینت موجود است: x86، x64 و Itanium تا همه پلتفرم‌های ویندوزی از آن پشتیبانی کنند.

کلاینت‌ها کلاستر AD RMS را از سه طریق تشخیص می‌دهند:

- از AD DS Service Connection Point ساخته شده هنگام نصب AD RMS استفاده می‌کنند.
- در توزیع‌های پیچیده و AD RMS multiforest از بازنویسی‌های رجیستری که مستقیما روی کلاینت اتفاق می‌افتد استفاده می‌کنند. مخصوصا این نوع در نسخه‌های قدیمی‌تر سیستم عامل ویندوز کاربرد دارد.
- از URL های درج شده در مجوزهای issuance برای محتوا استفاده می‌کنند.

هر کدام از این روش‌ها افزونگی را فراهم می‌کنند تا کلاینت‌ها همیشه به محتوا دسترسی داشته باشند.

مدیریت بانک اطلاعاتی

AD RMS برای کارکرد خود به سه بانک اطلاعاتی نیاز دارد. برای کنترل عملکرد بهینه کلاسترهای AD RMS باید با این سه بانک و عملکرد آنها آشنا شویم. این بانک‌ها عبارتند از:

- بانک اطلاعاتی پیکربندی که برای ذخیره همه داده‌های پیکربندی AD RMS استفاده می‌شود. این بانک توسط سرورهای AD RMS به کار گرفته می‌شوند تا سرویس‌ها و اطلاعات محافظت شده را برای کلاینت‌ها فراهم کنند.
- بانک ثبت وقایع که داده‌های مربوط به فعالیت کلاسترهای ریشه و license-only را ذخیره می‌کند. این بانک برای ممیزی وقایع AD RMS مفید است.
- بانک سرویس دایرکتوری که اطلاعات کاربران و همه داده‌های مرتبط با آنان را ذخیره می‌کند. این اطلاعات از دایرکتوری‌های AD DS قابل دسترس است و این دسترسی را LDAP فراهم می‌کند. اگر کاربری را از AD RMS حذف کنیم همان طوری که قبلا بیان شد نیاز به نگهداری مستمر بانک اطلاعاتی داریم.

به علاوه این بانک‌ها AD RMS از سرویس Message Queuing برای ارسال وقایع به بانک ثبت وقایع استفاده می‌کند. اگر دغدغه ممیزی AD RMS را داشته باشیم که باید داشته باشیم بررسی‌های لازم و مستمر را برای اطمینان از کارکرد صحیح آن انجام می‌دهیم.

علاوه بر قابلیت‌های مختلف کنسول AD RMS مایکروسافت یک ابزار RMS مخصوص ارائه داده است که حاوی یک سری ابزار برای مدیریت و اجرای AD RMS می‌باشد. توصیه می‌شود آنرا دانلود کرده و به کیت مدیریتی AD RMS اضافه کنید.

تمرینات ساخت الگوی rights policy

در این تمرین یک قالب سفارشی rights policy خواهیم ساخت. از AD RMS که در تمرین قبل نصب کردیم برای این کار استفاده می کنیم

تمرین اول ساخت الگوی جدید

الگوها کاربران را قادر می سازند تا rights policy ها را سریع و به طور استاندارد بکار ببرند. برای ساخت یک الگو باید از حقوق دسترسی AD RMS Template Administrators یا AD RMS Enterprise Administrators استفاده کنیم. برای انجام این تمرین به SERVER01 ، SERVER04 و SERVER05 نیاز داریم

۱- با اعتبار RMS Template Administrators به سروری که عضو root cluster است وارد می شویم

۲- Server Manager را از Administrative Tools اجرا می کنیم

۳- گره Roles\Active Directory Rights Management Services*servername*\Rights Policy Templates را باز می کنیم

۴- در Actions pane ، Create Distributed Rights Policy Template را انتخاب می کنیم

این کار باعث اجرای ویزارد می شود

۵- در صفحه Add Template Identification Information روی Add کلیک می کنیم

۶- زبان را مشخص کرده و عبارت **Contoso Legal Template** را برای نام و **Template to protect legal documents at Contoso Ltd را برای توضیحات اضافه می کنیم**. روی Add وسپس روی Next کلیک می کنیم

۷- در صفحه Add User Rights چند مورد را باید انجام دهیم

- برای انتخاب گروه یا کاربرانی که اجازه دسترسی به الگو را دارند روی Add کلیک می کنیم و Anyone را انتخاب می کنیم. این کار به تمام کاربران اجازه می دهد که برای کار با محتوا درخواست مجوز کنند
- در زیر Users And Rights ، Anyone را انتخاب کرده و View rights را در پنل Rights For User به آن اختصاص می دهیم
- از انتخاب Grant Owner (Author) Full Control Right With No Expiration مطمئن می شویم
- در قسمت Rights request URL آدرس **https://RightsManagement .Contoso.com را تایپ می کنیم.**

۸- روی Next کلیک می کنیم در صفحه Specify Expiration Policy ، Never Expires را انتخاب می کنیم و از عدم انتخاب Expires After The Following Duration (Days) مطمئن می شویم. روی Next کلیک می کنیم

۹- در صفحه Specify Extended Policy می توان تنظیمات زیر را اعمال کرد

- گزینه Enable Users to view protected content را انتخاب می کنیم. این به کاربه کاربران امکان می دهد حتی اگر برنامه های AD RMS–enabled ندارند باز بتوانند با نصب add-on لازم مجتوای محافظت شده را مشاهده کنند
- Request A New Use License Every Time Content Is Consumed (Disable Client-Side Caching) را انتخاب نمی کنیم
- If You Would Like To Specify Additional Information For Your AD RMS-Enabled Applications, You Can Specify Them Here As Name-Value Pairs را انتخاب نمی کنیم. این مورد به برنامه نویسان اختصاص دارد

۱۰- روی Next کلیک می کنیم. در صفحه Specify Revocation Policy ، revocation را فعال نکرده و روی Finish کلیک می کنیم

اکنون الگو ما ساخته شده و آماده توزیع می باشد

خلاصه درس

- هنگامی که با AD RMS کار می کنیم برای کامل کردن نصب نیازمند انجام چند مورد هستیم. اگر بخواهیم به کاربرانی از خارج شبکه نیز اجازه دسترسی به سیستم DRM بدهیم این موارد شامل ساخت extranet URL نیز می باشد. همچنین شامل پیکربندی سیاستهای Trust برای پشتیبانی از دسترسی خارجی می باشد

- اگر بخواهیم با زیرساخت AD RMS کار کنیم باید گواهی نامه های licensor سرورها را با یکدیگر مبادله کنیم. این به معنی صدور گواهی نامه ها از cluster مبدا و وارد کردن آنها به cluster مقصد می باشد
- اگر نیاز داریم تا کاربرانی را از دسترسی به سیستم DRM محروم کنیم باید exclusion policy بسازیم
- برای آسانی ساخت محتوای کاربر الگوهای rights policy درست می کنیم این الگوها کار را برای کاربران آسان کرده و از طریق آنها مطمئن می شویم که استراتژی DRM ما درست استفاده می شود

سئوالات پایان درس

۱. فرض کنید مدیر شبکه دامنه *contoso.com* هستیم به تازگی کار نصب AD RMS را تمام کرده ایم و اکنون می خواهیم آنرا پیکربندی کنیم. یک URL اکسترانت نیز پیکربندی کرده ایم و عملکرد آنرا از سرور AD RMS امتحان می کنیم. این URL برای ایجاد یک ارتباط امن HTTP از SSL استفاده می کند اما هنگامی که کاربران از خارج از شبکه می خواهند به AD RMS دسترسی داشته باشند نمی توانند. اشکال از چه می تواند باشد؟

A . کاربران باید از URL با فرمت HTTP:// استفاده کنند
B . گواهی نامه سرور فاقد اعتبار است و به همین دلیل کاربران به URL دسترسی ندارند
C . کاربران باید برای دسترسی به URL حساب دامنه AD DS داشته باشند
D . URL ای که به کاربران اعلام کرده ایم اشتباه است

فصل ۱۷

Active Directory Federation Services

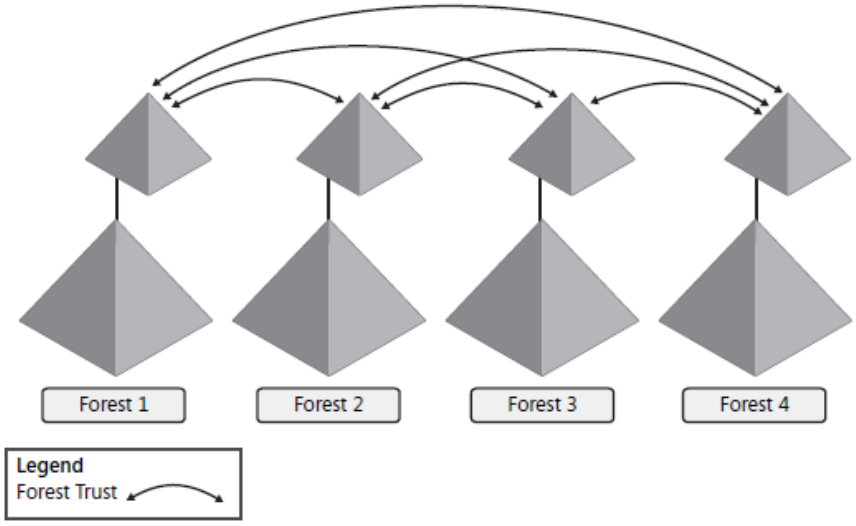
از زمان ظهور اینترنت تا حالا سازمان‌ها تلاش می‌کنند شبکه‌های خود را از سمت دنیای بیرون ایمن سازند. قاعده اساسی این است که سازمان‌هایی که بین شبکه خود و اینترنت رابط دارند ترجیح می‌دهند شبکه perimeter نیز داشته باشند. در بسیاری از موارد سازمان‌ها تلاش زیادی می‌کنند تا فناوری‌های امنیتی مخصوصی را نظیر سیستم‌های تشخیص نفوذ پیاده‌سازی کنند و تا حالا نتیجه اساسی شبکه perimeter نگهداری دیواره آتش در وضعیت امن است. ولی این کار چه تاثیری بر شرکاء خواهد داشت؟

در همان روزهای اول دامنه‌های ویندوزی در ویندوز NT مایکروسافت ویژگی trust را به منظور تعامل بین دامنه‌ها ارائه داد. با ارائه AD DS در ویندوز 2000 مایکروسافت مفهوم trust و trust های بین دامنه‌ای را پیش کشید. دامنه‌های یک forest به طور خودکار دارای transitive trust هستند و دامنه‌های forest های متفاوت زمانی که بخواهند فضای امنیتی خود را با هم به اشتراک گذارند از explicit trust استفاده می‌کنند. با ارائه ویندوز سرور 2003 مایکروسافت مفهوم transitive trust را به forest های دارای forest

trust بسط داد. شرکاء با این نوع trust می‌توانستند فضای امنیتی خود را تا forest شریک تجاری خود گسترش دهند. ولی پیاده‌سازی این نوع trust دو عیب عمده دارد:

- اول اینکه نیاز به پورت‌های باز دیواره آتش دارد تا اجازه عبور ترافیک AD DS را بدهد.
- دوم اینکه اگر شریک تجاری رشد زیادی داشته باشد مدیریت trust های چندگانه کار سختی خواهد بود. (شکل ۱- ۱۷)

استفاده از trust بهترین راه برای ارتباط شرکاء نیست.



شکل ۱- ۱۷ پیاده‌سازی trust های forest چندگانه می‌تواند خیلی پیچیده شود.

هدف دیواره آتش (Firewall)

اگرچه forest trust می‌تواند بسیار پیچیده باشد تاثیرات خوبی نیز روی مکانیزم‌های امنیتی دارند. برای مثال ترافیک AD DS از طریق LDAP روی TCP/IP با پورت ۳۸۹ یا ترجیحا secure LDAP یا LDAP/S روی پورت ۶۳۶ ارسال می‌شود. به علاوه اگر بخواهیم ترافیک GC را ارسال کنیم نیاز به پورت ۳۲۶۸ و یا ترجیحا ۳۲۶۹ روی LDAP/S داریم.

دیواره آتش برای ممانعت از عبور ترافیک نامطلوب طراحی شده است. سوراخ کردن آن برای تعداد زیادی پورت روش مناسبی نیست. شبکه‌های سنتی perimeter دو لایه محافظتی دارد. اولی شبکه perimeter را از دسترسی خارجی محافظت می‌کند و دومی شبکه داخلی را از شبکه perimeter حفظ می‌کند. شبکه perimeter خود یک سری سرویس نظیر AD CS، AD RMS و در برخی موارد AD LDS را فراهم می‌کند. AD DS منحصرا در شبکه داخلی کاربرد دارد.

دیواره آتش خارجی با پیکربندی مناسب تعدادی پورت اصلی را باز نگه می‌دارد که شامل موارد زیر است:

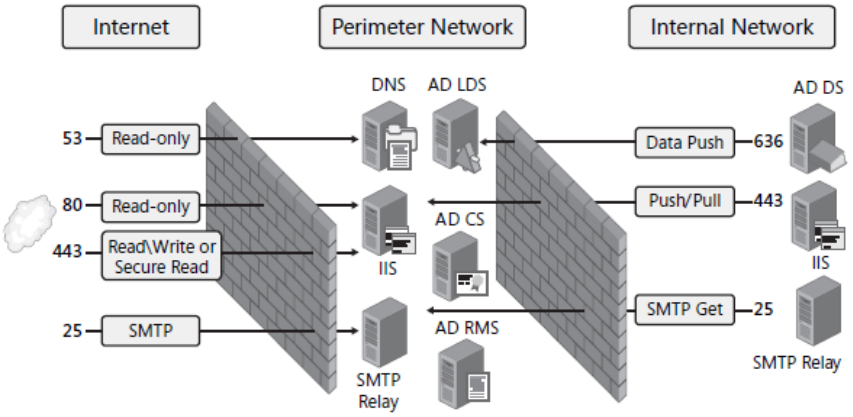
- پورت ۵۳ که برای ترافیک DNS استفاده می‌شود. ترافیک DNS معمولا به صورت فقط خواندنی است.

- پورت ۸۰ که برای داده HTTP استفاده می‌شود. پورت ۸۰ معمولا برای دسترسی فقط خواندنی به کار می‌رود به دلیل اینکه امن نیست.

- پورت ۴۴۳ برای HTTPS . ارتباطات روی این پورت به واسطه SSL یا Transport Layer Security (TSL) امن می‌باشد. این دو پروتکل از گواهی‌نامه‌های CA برای رمزنگاری داده استفاده می‌کنند به همین دلیل ارتباطات روی پورت ۴۴۳ از عملیات خواندن و نوشتن پشتیبانی می‌کند.

- پورت ۲۵ که برای SMTP به کار می‌رود. هر چند این پورت امن نیست ولی بدون آن نیز کسی نمی‌تواند به سرویس mail دسترسی داشته باشد.

بهتر است بقیه پورت‌ها بسته باشد. دیواره آتش داخلی بسته به فناوری‌هایی که در شبکه perimeter وجود دارند می‌تواند پورت‌های باز بیشتری داشته باشد. شکل (۲- ۱۷). برای مثال اگر در شبکه perimeter از سرویس تایید هویت AD LDS برای برنامه‌های مبتنی بر وب استفاده می‌کنیم ممکن است بخواهیم یکسان‌سازی یک‌طرفه از سمت دایرکتوری AD DS داخلی داشته باشیم یا اگر از IIS استفاده می‌کنیم ممکن است بخواهیم داده‌ها را به وب سایت خود در perimeter ارسال کرده یا دریافت کنیم. به علاوه نیاز داریم پیغام‌های e-mail از SMTP relay های شبکه perimeter به شبکه داخلی ارسال شود. این‌ها پایه و اساس یک طرح شبکه perimeter امن هستند.

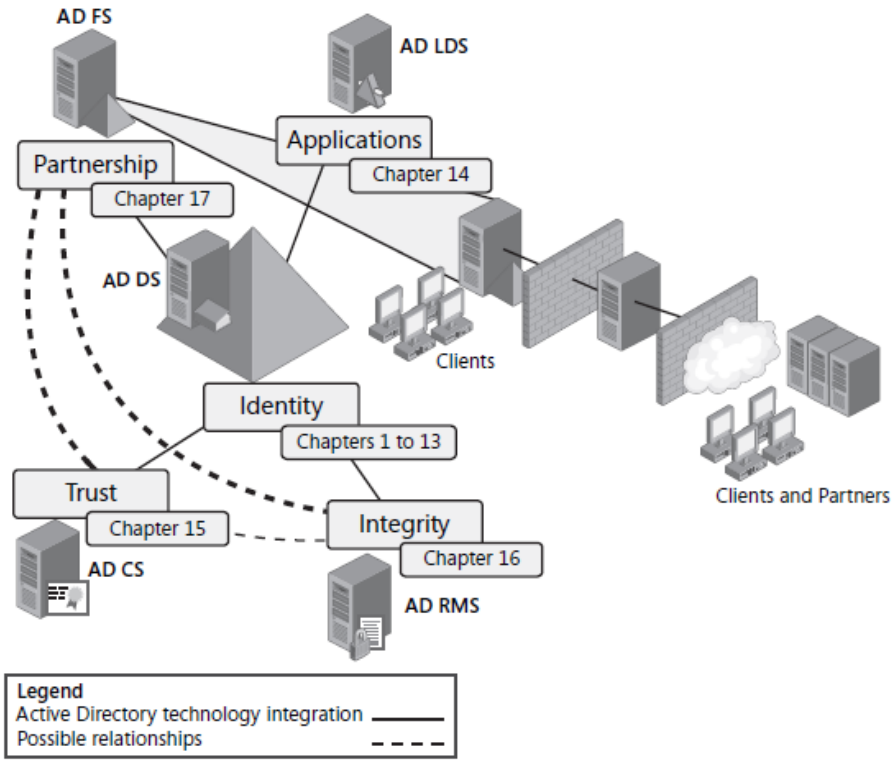


شکل ۲- ۱۷ اساس یک شبکه perimeter امن یک سری دیواره آتش امن است.

Active Directory Federation Services

AD FS به عنوان یکی از فناوری‌های Active Directory در ویندوز سرور 2008 جای گرفته است. این فناوری به منظور توسعه اقتدار شبکه داخلی به بیرون شبکه طراحی شده است. (شکل ۳- ۱۷). این سرویس با هدف فراهم کردن عملکردی شبیه به forest trust یا explicit trust طراحی شده است ولی نه از طریق پورت‌های سنتی LDAP TCP/IP بلکه از طریق پورت‌های HTTP رایج. در واقع AD FS از پورت ۴۴۳ استفاده می‌کند به دلیل اینکه همه ارتباطات trust مربوط به AD FS امن و رمزنگاری شده

هستند. به این طریق این سرویس از گواهی‌نامه‌های AD CS برای سرورهای خود در AD FS بهره می‌برد. AD FS همچنین توزیع AD RMS ما را توسعه می‌دهد و سرویس‌های federation برای مدیریت حقوق مالکیت معنوی بین شرکاء فراهم می‌کند.



شکل ۳- ۱۷ AD FS اقتدار دایرکتوری AD DS داخلی را توسعه می‌بخشد.

AD FS اقتدار شبکه را به forest های داخلی توسعه می‌دهد و به سازمان‌ها امکان می‌دهد بدون نیاز به باز کردن پورت‌های اضافی روی دیواره آتش با شرکاء تعامل داشته باشند. اساسا AD FS از دایرکتوری AD DS داخلی شرکاء برای فراهم کردن تایید هویت برای سرویس‌های اکسترانت و perimeter استفاده می‌کند. مثلا وقتی کاربری برای دسترسی به یک برنامه عجین شده با AD FS به تایید هویت نیاز دارد موتور AD FS برای تایید هویت به دایرکتوری داخلی مراجعه می‌کند. اگر کاربر به دایرکتوری داخلی دسترسی داشته باشد دسترسی به برنامه خارجی نیز به او اعطاء خواهد شد. مزیت اصلی آن این است که هر یک از سازمان‌های شریک فقط باید تایید هویت را در شبکه خود مدیریت کند و بقیه کارها توسط سرویس federation انجام می‌شود.

به طور خلاصه AD FS وقتی استفاده می‌شود که بخواهیم با سازمان دیگری رابطه شراکت داشته باشیم و آن سازمان از دایرکتوری AD DS استفاده کند. اگر بخواهیم سرویس تایید هویت را در شبکه perimeter داشته باشیم ولی کاربران یا سازمان‌های دیگر دایرکتوری AD DS نداشته باشند یا حوزه شراکت توزیع AD FS را پشتیبانی نکند باید از AD LDS استفاده کنیم.

اهداف امتحانی در این فصل:

- پیکربندی نقش‌های سروری دیگر Active Directory
  - پیکربندی AD FS

دروس این فصل:

- درس ۱ : درک AD FS
- درس ۲ : پیکربندی و استفاده از AD FS

قبل از شروع

برای تکمیل دروس این فصل باید نصب‌های زیر را در شبکه انجام دهیم. اکیدا پیشنهاد می‌گردد از ماشین‌های مجازی برای این فصل استفاده شود زیرا نیاز به دسترسی به کامپیوترهای زیادی داریم. اگر تمرینات فصل‌های قبل را انجام داده باشیم بسیاری از این کامپیوترها آماده کار هستند.

- ویندوز سرور 2008 باید روی یک ماشین فیزیکی یا مجازی نصب شده باشد. نام ماشین را SERVER01 تعریف کرده و باید در دامنه contoso.com نقش DC داشته باشد.
- ویندوز سرور 2008 نسخه Enterprise باید روی یک ماشین فیزیکی یا مجازی نصب شده باشد. نام ماشین را SERVER03 تعریف کرده و باید عضو دامنه contoso.com باشد. این کامپیوتر میزبان نقش AD FS داخلی خواهد شد.
- ویندوز سرور 2008 نسخه Enterprise باید روی یک ماشین فیزیکی یا مجازی نصب شده باشد. نام ماشین را SERVER04 تعریف کرده و باید عضو دامنه contoso.com باشد. این کامپیوتر میزبان سرور AD FS proxy داخلی خواهد شد.
- ویندوز سرور 2003 نسخه Enterprise باید روی یک ماشین فیزیکی یا مجازی نصب شده باشد. نام ماشین را SERVER05 تعریف کرده و باید عضو دامنه contoso.com باشد. این کامپیوتر میزبان سرور SQL 2005 خواهد شد که بانک اطلاعاتی پیکربندی و ثبت وقایع را برای AD RMS اجرا خواهد کرد. این کامپیوتر باید دارای درایو D بوده تا داده‌های SQL روی آن ذخیره شود. میزان فضای خالی آن بهتر است حداقل 10 GB باشد. علت استفاده از ویندوز سرور 2003 میزان حافظه مورد نیاز کمتر نسبت به ویندوز سرور 2008 است. توجه داشته باشید که این سرور برای تمرینات این فصل ضروری نیست ولی داشتن آن از خطاهای AD RMS روی SERVER04 جلوگیری می‌کند.
- ویندوز سرور 2008 نسخه Enterprise باید روی یک ماشین فیزیکی یا مجازی نصب شده باشد. نام ماشین را SERVER06 تعریف کرده و باید در دامنه woodgrovebank.com نقش DC داشته باشد. همچنین باید نقش سرور DNS را نیز داشته باشد.

- ویندوز سرور 2008 نسخه Enterprise باید روی یک ماشین فیزیکی یا مجازی نصب شده باشد. نام ماشین را SERVER07 تعریف کرده و باید عضو دامنه woodgrovebank.com باشد. این کامپیوتر میزبان نقش AD FS داخلی خواهد شد.

- ویندوز سرور 2008 نسخه Enterprise باید روی یک ماشین فیزیکی یا مجازی نصب شده باشد. نام ماشین را SERVER08 تعریف کرده و باید عضو دامنه woodgrovebank.com باشد. این کامپیوتر میزبان سرور AD FS proxy خواهد شد.

این ترکیب برای تست نصب و پیکربندی ابتدایی AD FS کافی است. تست همه قابلیت‌های AD FS نیاز به ماشین‌های کلاینت داشته و از حد توان آزمایشگاهی بیشتر خوانندگان خارج است.

توجه داشته باشید که ساخت محیط AD FS با کامپیوترهای کمتر (نصب سرویس AD FS روی DC) نیز ممکن است ولی توصیه نمی‌شود این سرویس را روی DC نصب کنیم.

درس ۱: درک AD FS

AD FS یک موتور single sign-on (SSO) می‌باشد که به کاربران خارجی برنامه‌های مبتنی بر وب اجازه می‌دهد به برنامه دسترسی داشته باشند و از طریق مرورگر تایید هویت شوند. این کار تفاوت چندانی نسبت به استفاده از انباره دایرکتوری AD LDS خارجی که با دایرکتوری داخلی لینک است ندارد. ولی ویژگی کلیدی AD FS این است که برای تایید هویت کلاینت از انباره تایید هویت داخلی دامنه خود کاربر استفاده می‌کند و انباره مخصوص به خود ندارد. همچنین از تایید هویت اصلی که کلاینت در شبکه خود اجرا می‌کند استفاده می‌کند و این تاییده را به همه برنامه‌های مبتنی بر وب که با AD FS سازگار هستند می‌فرستد.

سازمان‌ها به یک انباره تایید هویت نیاز دارند نه بیشتر. استفاده از دایرکتوری AD LDS برای تایید هویت اکسترانت بار کاری مدیر شبکه را افزایش می‌دهد به دلیل اینکه سازمان باید انباره داخلی و خارجی خود را مدیریت کند. کاربران همچنین باید کدهای دسترسی و کلمات عبور متعددی را برای ورود به هر یک از این انباره‌ها به خاطر بسپارند. کاربران با AD FS فقط کافی است یک‌بار تایید هویت شوند آنهم وقتی به شبکه وارد می‌شوند.

با استفاده از AD FS می‌توانیم شراکت B2B را با کمترین بار کاری اضافه داشته باشیم. با شراکت B2B سازمان‌ها به دو گروه کلی تقسیم می‌شوند:

- Resource Organization وقتی سازمانی تصمیم می‌گیرد منابع خود را مانند وب سایت به اشتراک بگذارد و از AD FS برای تایید هویت استفاده کند در واقع یک نوع شراکت را با دیگران تجربه می‌کند. سازمانی که این شراکت را شکل می‌دهد سازمان منبع نامیده می‌شود زیرا میزبان منابع اشتراکی در شبکه perimeter خود می‌باشد.

- Account Oraganization وقتی سازمانی با یک resource organization وارد شراکت می‌شود به آن account organization گویند زیرا آنها حساب‌های مورد استفاده دسترسی منابع اشتراکی را در طرح‌های SSO مدیریت می‌کنند.

AD FS از یک حالت تایید هویت دیگری نیز پشتیبانی می‌کند. در طرح Web SSO تایید هویت کاربران از هر جای اینترنت انجام می‌شود. پس از تایید هویت کاربر AD FS خصیصه‌های کاربر را در دایرکتوری‌های AD DS یا AD LDS بررسی می‌کند تا ببیند کاربران نسبت به برنامه‌های کاربردی چه ادعایی دارند.

برای پشتیبانی از این سرویس AD FS از چهار سرویس استفاده می‌کند.

- **Fedetation Service** این سرویس توسط سرورهایی که سیاست trust را به اشتراک می‌گذارند ارائه می‌شود. سرور federation درخواست‌های تایید هویت را به دایرکتوری منبع مناسب مسیردهی می‌کنند تا توکن‌های امنیتی برای کاربر تولید شود.

- **Fedetation Service Proxy** سرور federation برای دریافت درخواست‌های تایید هویت از کاربر از یک سرور proxy که در شبکه perimeter قرار دارد استفاده می‌کند. proxy اطلاعات تایید هویت را از مرورگر کاربر به واسطه WS-Federation Requester Profile (WS-F PRP) که یک سرویس AD FS Web می‌باشد دریافت می‌کند و آنرا به سرویس federation ارسال می‌کند.

- Claims-Aware Agent عاملی است که روی سرور وب قرار گرفته و درخواست‌های tokem claim امنیتی را به سرویس federation صادر می‌کند. هر claim برای اعطاء یا ممانعت از دسترسی به برنامه خاصی استفاده می‌شود. برنامه‌های ASP.NET که می‌تواند claim های مختلف موجود در توکن امنیتی AD FS کاربر را بررسی کند با نام برنامه claim-aware شناخته می‌شود. این برنامه‌ها برای تعیین دسترسی کاربر به برنامه از claim استفاده می‌کنند. دو مثال از این نوع برنامه‌ها AD RMS و Office SharePoint Server 2007 می‌باشد.

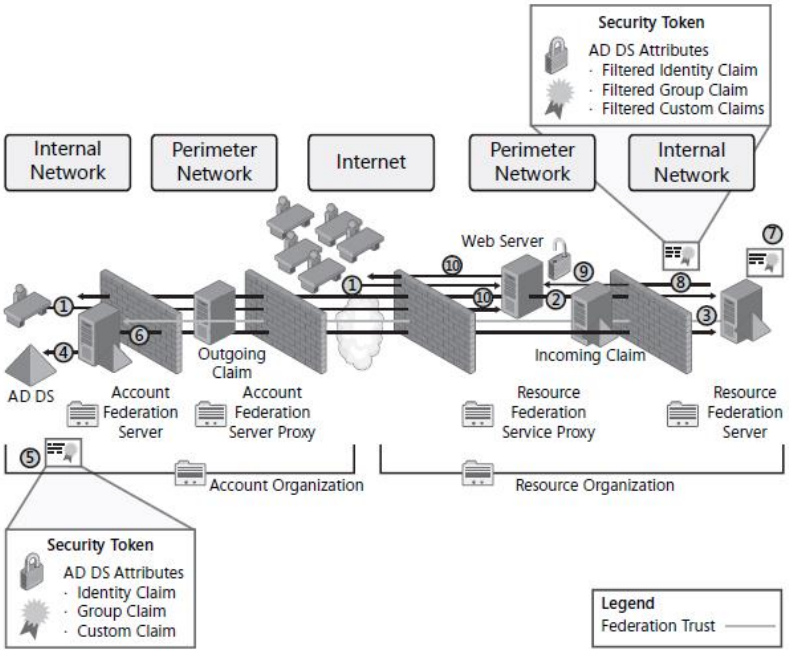
- Windows Token-Based Agent این یک عامل جایگزین محسوب شده که می‌تواند توکن امنیتی AD FS را به یک توکن دسترسی impersonation-level Windows NT برای برنامه‌هایی که از مکانیزم‌های تایید هویت ویندوز به جای تایید هویت مبتنی بر وب استفاده می‌کنند تبدیل کند.

AD FS به دلیل اینکه براساس سرویس وب استاندارد کار می‌کند برای پشتیبانی از هویت‌های federated نیازی به AD DS ندارد. هر سرویس دایرکتوری که با استاندارد WS-Federation سازگاری دارد می‌تواند در AD FS identity federation شرکت کند.

اگرچه سرویس‌های federation در ویندوز سرور 2003 R2 موجود بود AD FS در ویندوز سرور 2008 بسیار توسعه پیدا کرده است تا فرایندهای نصب و مدیریت را تسهیل کند. AD FS همچنین نسبت به نسخه‌های قدیمی از برنامه‌های تحت وب بیشتری پشتیبانی می‌کند.

فرایند تایید هویت AD FS

شراکت AD FS از چشم کاربرانی که به برنامه‌های وب خارجی وارد می‌شوند مخفی می‌ماند. در یک سناریوی AD FS معمولی وقتی کاربر به برنامه claims-aware در اکسترانت وارد می‌شود AD FS به طور خودکار اعتبار کاربر را تامین می‌کند و claim های موجود در خصیصه‌های حساب کاربر را لیست می‌کند. (شکل ۴- ۱۷)



شکل ۴- ۱۷ استفاده از AD FS به منظور فراهم کردن دسترسی به برنامه‌های تحت وب اکسترانت از طریق Federated Web SSO

۱. کاربری در یک شبکه داخلی یا اینترنت می‌خواهد به یک برنامه وب claims-aware دسترسی داشته باشد. این کاربر به یکی از account organization که عضو شراکت AD FS است تعلق دارد.

۲. عامل claims-aware روی سرور وب resource federation server (RFS) را در resource organization بررسی می‌کند تا ببیند به کلاینت دسترسی اعطاء شده است یا نه. به دلیل اینکه درخواست باید از دیواره آتش عبور کند عامل ابتدا با Federation Service Proxy (FSP) تماس می‌گیرد که آنهم با سرور federation داخلی ارتباط برقرار می‌گیرد.

۳. سرور federation در resource organization به دلیل اینکه برای کاربر حسابی ندارد و در عوض ارتباط federation با انباره دایرکتوری در account organization دارد (federation trust) حقوق دسترسی کاربر را از طریق یک account federation server (AFS) در شبکه داخلی account organization و بعد دوباره از طریق یک proxy بررسی می‌کند. این حقوق دسترسی به شکل claim لیست شده‌اند و خصیصه‌هایی محسوب می‌شوند که به شیء حساب کاربر در AD DS لینک شده‌اند.

۴. سرور federation در account organization مستقیما به AD DS داخلی سازمان لینک شده و حقوق دسترسی را از دایرکتوری از طریق پرس‌وجوی LDAP به دست می‌آورد. توجه داشته باشید که حساب کاربر می‌تواند همچنین در یک انباره دایرکتوری AD LDS قرار گیرد.

۵. سرور federation مربوط به account organization توکن امنیتی AD FS کاربر را می‌سازد. این توکن حاوی مشخصه کاربر، لیستی از claim های موجود در حساب AD DS کاربر و گواهی‌نامه دیجیتال AFS می‌باشد.

۶. AFS با توکن امنیتی که حاوی حقوق دسترسی کلاینت است یک بار دیگر از طریق سرور proxy به RFS پاسخ می‌دهد. این یک outgoing claim است.

۷. RFS توکن را رمزگشایی کرده و claim های کاربر را از incoming claim استخراج می‌کند. سپس claim ها را به claim های سازمان نگاشت می‌کند و یک سیاست فیلترینگ را برای درخواست‌های خاص برنامه تحت وب اعمال می‌کند.

۸. Claim های فیلترشده سپس در یک توکن امنیتی امضاء شده بسته‌بندی شده و به سرور وب در اکسترانت resource organization ارسال می‌گردد. این کار با پست آن به آدرس URL موجود در درخواست اصلی برنامه تحت وب انجام می‌شود. در این مورد امضاء توکن یا مبتنی بر گواهی‌نامه دیجیتال RFS یا کلید Kerberos session می‌باشد زیرا سیستم‌ها در یک شبکه هستند.

۹. سرور وب از عامل claims-aware خود برای رمزگشایی توکن امنیتی کاربر استفاده می‌کند claim های کاربر را پیدا می‌کند و سپس دسترسی به برنامه را بر مبنای claim های توکن اعطاء می‌کند.

۱۰. AD FS Web agent روی سرور وب برای پشتیبانی از single sign-on مرورگر کاربر را هدایت می‌کند تا یک کوکی تایید هویت محلی برای کاربر بنویسد به طوری که در طول همین session نیازی به جستجو و تایید هویت دوباره نداشته باشد.

پیاده‌سازی AD FS باید با احتیاط انجام شود. هر شریک می‌تواند برای اعطاء دسترسی به برنامه‌های اکسترانت از انباره‌های دایرکتوری داخلی خود استفاده کند. این کار مدیریت دسترسی را ساده می‌کند ولی برای این کار هر شریک باید federation trust را پیاده‌سازی کند. federation trust از شرکاء دارای حداقل یک سرور AD FS federation در شبکه خود استفاده می‌کند. سمت و جهت trust همیشه از resource به account است.

توجه داشته باشید که وقتی کاربر از کامپیوتر خانگی یا عمومی استفاده می‌کند که بخشی از دامنه account organization نیست فرد می‌تواند از یک صفحه وب AD FS مخصوص استفاده کند که کاربر را قادر می‌سازد بین account organization ها انتخاب کند. این صفحه وب همچنین صفحات ورود مبتنی بر فرم یا تایید هویت عجین شده ویندوز را فراهم می‌کند. این کار به کاربران خارجی امکان می‌دهد به برنامه‌های اکسترانت دسترسی داشته باشند حتی اگر از کامپیوترهای شرکت استفاده نکند.

اگر به دلایل امنیتی نخواهیم یک صفحه وب بسازیم که حاوی لیستی از account organization باشد می‌توانیم آنرا مستقیما در پرس‌وجو درج کنیم. برای این کار پرس‌وجو را به شکل زیر استفاده می‌کنیم:

https://webserver/appname/apppage.aspx?whr=urn:federation:accountpartner

در این پرس‌وجو از پارامتر whr برای تعیین account organization در شراکت federation استفاده می‌کنیم.

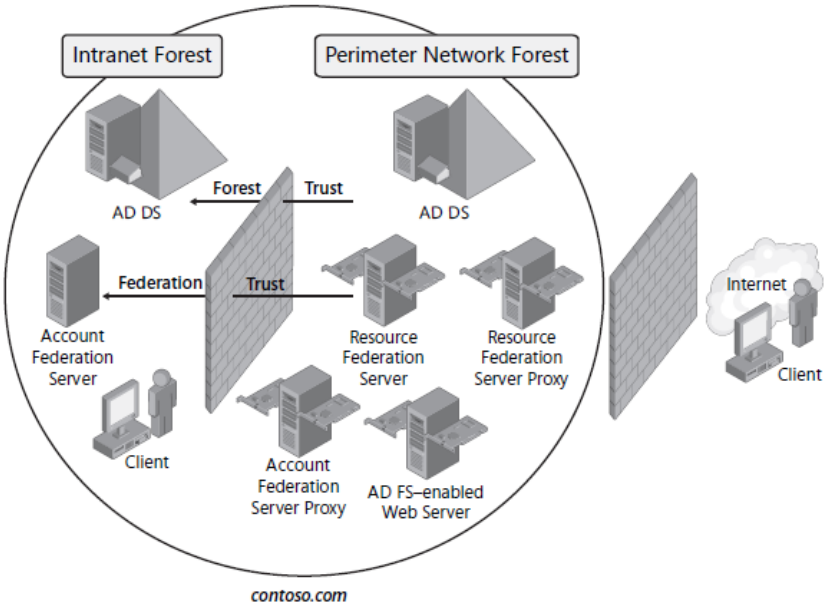
طراحی AD FS

AD FS بر اساس نوع شراکت B2B مورد نیاز از سه پیکربندی یا طراحی معماری پشتیبانی می‌کند. هر کدام دارای مشخصات مخصوص به خود بوده و از سناریوی شراکت مشخصی پشتیبانی می‌کنند.

- **Federated Web SSO** این مدل دیواره آتش متعدد را پوشش می‌دهد به دلیل اینکه برنامه‌های موجود در اکسترانت resource organization را به انباره دایرکتوری داخلی account organization لینک می‌دهد. تنها trust موجود این مدل federation است که همیشه از طرف resource organization به account organization می‌باشد. این مدل رایج‌ترین سناریوی توزیع AD FS می‌باشد.(شکل ۴- ۱۷)

- **Federated Web SSO با Forest Trust**در این مدل سازمان از دو AD DS forest استفاده می‌کند. یکی forest داخلی و دیگری خارجی که محل آن در شبکه perimeter می‌باشد. forest trust بین forest در شبکه perimeter و forest داخلی برقرار می‌شود. به علاوه federation trust بین سرور resource federation که در شبکه perimeter واقع شده و سرور account federation که در شبکه داخلی واقع شده برقرار می‌شود. در این سناریو کاربران خارجی در perimeter forest حساب داشته و کاربران داخلی در forest داخلی حساب دارند. سیستم AD FS کار federation دسترسی را از حساب‌های دو forest به برنامه‌های کاربردی شبکه perimeter انجام می‌دهد. به همین دلیل کاربران داخلی

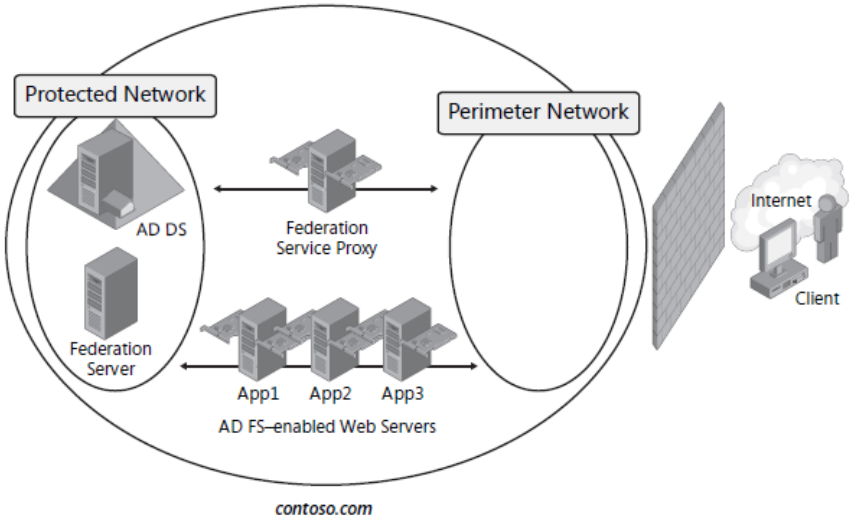
هم از شبکه داخلی و هم اینترنت به برنامه‌ها دسترسی دارند درحالی که کاربران خارجی فقط از طریق اینترنت دسترسی دارند. (شکل ۵- ۱۷)



شکل ۵- ۱۷ استفاده از forest trust و federation trust برای فراهم کردن دسترسی به برنامه‌های اکسترانت

- **Web SSO** وقتی همه کاربران برنامه اکسترانت خارجی هستند و در دامنه حساب ندارند باید Web SSO را توزیع کنیم. این مدل به کاربران اجازه می‌دهد برای دسترسی به برنامه‌های وب فقط یکبار تایید هویت شوند. ولی این مدل نیاز به سرورهای وب multihomed (با چند کارت شبکه) دارد که یکی به شبکه خارجی و دیگری به شبکه داخلی متصل می‌شود. سرورهای وب بخشی از دامنه AD DS داخلی بوده و از طریق کارت شبکه داخلی به آن متصل می‌شوند. کلاینت‌ها از طریق کارت شبکه خارجی به برنامه‌ها دسترسی پیدا می‌کنند. Federation Service Proxy نیز باید multihomed باشد تا دسترسی به شبکه‌های خارجی و داخلی را فراهم کند. (شکل ۶- ۱۷)

رایج‌ترین سناریوها اولی و آخری هستند ولی در حالت ایده‌آل همه کاربران دایرکتوری AD DS خود را دارند و به عنوان account organization برای تسهیل استراتژی توزیع عمل می‌کنند.



شکل ۶- ۱۷ استفاده از سناریوی Web SSO federation

اجزاء AD FS

به علاوه سرویس‌های مختلفی که AD FS پشتیبانی می‌کند این فناوری اجزاء متعددی نیز دارد که شامل Claim، کوکی و گواهی‌نامه است. هر کدام از این سه جزء مربوط به بخشی از فرایند AD FS می‌باشد. همچنین AD FS دارای اصطلاحات مخصوص به خود است. برای درک بهتر اجزاء نام‌برده درک این اصطلاحات ضروری است.

AD FS Claim

در ابتدایی‌ترین شکل خود عباراتی هستند که هر یک از شرکاء در ارتباط AD FS درباره کاربران خود می‌سازد. Claim دارای مقادیر متعددی است مانند نام کاربران، کلیدهای گواهی‌نامه، عضویت گروه‌ها و دسترسی‌های خاص. Claim ها اساس اعتبار AD FS ارسال شده به برنامه وب می‌باشند. Claim ها از سه طریق قابل دریافت هستند:

- سرور account federation می‌تواند از انباره دایرکتوری داخلی برای claim پرس‌وجو کرده و آنها را در دسترس یک شریک resource قرار دهد.
- Account organization می‌تواند claim ها را دراختیار یک سرور resource federation قرار دهد که پس از انجام فیلترینگ روی آنها به برنامه resource ارسال کند.
- سرویس federation از انباره دایرکتوری (AD DS یا AD LDS) برای claim ها پرس‌وجو می‌کند و پس از انجام فیلترینگ روی آنها در اختیار برنامه resource قرار دهد

AD FS از سه نوع claim پشتیبانی می‌کند:

- **نوع identity claim** هر claim که مبتنی بر هویت کاربر باشد در این گروه قرار می‌گیرد. در هر claim برای توکن‌های امنیتی باید حداقل یک عدد از این نوع claim وجود داشته باشد.

- می‌تواند شامل یک UPN باشد که نماینده هویت کاربر است. به خاطر داشته باشید که حتی اگر UPN های متعددی برای یک حساب موجود باشد فقط یکی از آنها در این نوع claim استفاده می‌شود. اگر UPN های دیگر باید در claim قرار بگیرند باید identity claim سفارشی درست کنیم. UPN وقتی به همراه انواع دیگر به کار می‌رود دارای اولویت بالاتری نسبت به دیگر identity claim هاست.
- می‌تواند یک آدرس e-mail باشد. مانند UPN فقط یک آدرس می‌تواند به عنوان نوع e-mail claim ارتباط برقرار کند. این نوع در اولویت دوم قرار دارد.
- می‌توانیم از نام رایج نیز استفاده کنیم که چیزی جز رشته‌ای از کاراکترها نیستند. توجه داشته باشید که روشی برای تضمین منحصر بودن نام رایج نیست. بنابراین در استفاده از این نوع باید محتاط بود. کمترین اولویت را دارد.

- **نوع Group claim** گروه‌هایی که کاربر به آن تعلق دارد نیز می‌تواند در یک claim استفاده شود. به دلیل اینکه یک کاربر می‌تواند به گروههای مختلف تعلق داشته باشد می‌توانیم group claim های متعددی در یک claim داشته باشیم. برای مثال کاربری می‌تواند عضو گروههای Tester، Developer و User یک برنامه کاربردی باشد.
- نوع Custom claim اگر بخواهیم اطلاعات خاصی را برای کاربر درج کنیم برای مثال یک شماره ID خاص مانند حساب بانکی می‌توانیم از این نوع استفاده کنیم.

وقتی claim ها پردازش شدند توسط سرور federation فیلتر می‌شوند. این کار باعث کاهش تعداد نهایی claim های یک سازمان می‌شود. اگر فیلترینگ انجام نشود سازمان مسئول استخراج claim های هر شریک می‌باشد. این کار باعث افزایش زیاد claim ها برای مدیریت می‌شود.

کوکی‌های AD FS

AD FS علاوه بر claim با کوکی‌ها نیز کار می‌کند که در مرورگر کاربران در طول session های وب درج می‌گردد که از طریق AD FS تایید هویت می‌شوند. سه نوع کوکی توسط AD FS استفاده می‌شوند.

- **کوکی‌های تایید هویت** به دلیل اینکه اولین instance از تایید هویت AD FS تعامل کمتری نیاز دارد AD FS یک کوکی تایید هویت تولید می‌کند تا در مرورگر کاربر قرار گرفته و برای تایید هویت‌های بعدی از SSO پشتیبانی کند. این کوکی حاوی همه claim های کاربر است. کوکی‌های تایید هویت به وسیله عامل وب AD FS و خود سرویس federation صادر می‌شوند. استفاده از عامل وب ما را از داشتن کلیدهای خصوصی و عمومی روی سرور بی‌نیاز می‌کند. وقتی عامل وب یک کوکی تایید هویت می‌سازد از توکن امنیتی موجود تولید شده توسط سرور federation استفاده می‌کند. ولی سرور

federation باید جفت کلید را داشته باشد زیرا از این کلیدها برای امضای توکن‌های امنیتی استفاده می‌کند. این کوکی‌ها امضا می‌شوند ولی رمزنگای نمی‌شوند. این دلیل دیگری است که همه ارتباطات در فرایند از طریق TLS یا SSL رمزنگاری می‌شوند. همچنین به دلیل اینکه یک کوکی session است بعد از بسته شدن session پاک می‌شود.

- **کوکی‌های Account Partner** طی فرایند تایید هویت کلاینت باید عضویت شریک حساب خود را اعلان کند. اگر این اعلان یک توکن معتبر داشته باشد فرایند AD FS یک کوکی روی کلاینت می‌نویسد طوری که دفعه بعد که کلاینت تایید هویت می‌شود از این کوکی به جای جستجو و کشف شرکاء استفاده می‌کند. این کوکی امضاء ندارد و رمزنگاری نیز نمی‌شود. این کوکی دائمی است.

- **کوکی‌های Sign-out** هر بار که سرویس federation یک توکن را انتساب می‌کند شریک resource یا سرور هدف که با توکن لینک است به کوکی sign-out افزوده می‌شود. این کوکی سپس برای تسهیل فرایند تایید هویت و عملیات پاک‌سازی برای مثال کوکی‌های cache شده در انتهای session کاربر استفاده می‌شود. این کوکی نیز امضاء ندارد و رمزنگاری نیز نمی‌شود. نوعی کوکی session است که به عنوان بخشی از عملیات پاک‌سازی حذف می‌شود.

گواهی‌نامه‌های AD FS

به منظور تضمین امنیت ارتباطات AD FS از انواع گواهی‌نامه‌ها استفاده می‌کند. در حقیقت AD FS از توزیع AD CS برای دریافت گواهی‌نامه‌های مورد نیاز خود بهره می‌برد. همه نقش سروری در توزیع AD FS از گواهی‌نامه‌ها استفاده می‌کنند. نوع گواهی‌نامه موردنیاز نقش بستگی به هدف نقش دارد.

- **سرورهای Federation** این سرورها قبل از انجام هر گونه عملیات AD FS باید هم گواهی‌نامه تاییدهویت سرور و هم گواهی امضاء توکن را داشته باشند. به علاوه سیاست trust که اصول اولیه ارتباط federation را تشکیل می‌دهد از گواهی‌نامه verification استفاده می‌کند. این آخرین گواهی‌نامه چیزی بیش از کلید عمومی گواهی‌نامه token-signing نیست.

  - گواهی‌نامه تایید هویت سرور یک گواهی تایید هویت SSL است که ترافیک وب بین سرور federation و Federation Service Proxy یا کلاینت وب را ایمن می‌سازد. گواهی‌نامه‌های SSL معمولا از طریق IIS Manager درخواست و نصب می‌شوند.

- هر بار که سرور federation یک توکن امنیتی می‌سازد باید توکن را با گواهی‌نامه token-signing خود امضای دیجیتال کند. این کار باعث ارتقاء امنیت می‌گردد. گواهی‌نامه token-signing از جفت کلیدهای خصوصی و عمومی تشکیل می‌شود.

- وقتی بیش از یک سرور federation در یک توزیع داریم فرایند تایید باید بین سرورها اتفاق بیافتد. برای این کار هر سرور باید گواهی‌نامه verification برای همه سرورهای دیگر داشته باشد. همان‌طور که قبلا اشاره شد این نوع گواهی‌نامه از کلید عمومی گواهی‌نامه token-signing برای سرور federation تشکیل می‌شود. این یعنی گواهی روی سرور مقصد بدون کلید خصوصی مرتبط نصب می‌شود.

- **پراکسی‌های سرویس Federation**پراکسی‌ها باید یک گواهی تایید هویت سرور داشته باشند تا از ارتباطات رمزنگاری شده SSL با کلاینت وب پشتیبانی کنند. همچنین به منظور تایید هویت سرور federation در حین ارتباط باید گواهی تایید هویت کلاینت را داشته باشند. این گواهی‌نامه هر نوع گواهی‌نامه تایید هویت کلاینتی می‌تواند باشد فقط باید از extended key usage (EKU) استفاده کند. کلیدهای خصوصی و عمومی برای این گواهی‌نامه روی پراکسی ذخیره می‌شوند. کلید عمومی روی سرور یا سرورهای federation در سیاست trust نیز ذخیره می‌شود. وقتی با این نوع گواهی‌نامه در کنسول AD FS کار می‌کنیم به آنها گواهی‌نامه‌های پراکسی سرویس federation گفته می‌شود.

- **عامل‌های وب AD FS** هر گونه سرور وب سازگار با AD FS میزبان عامل وب AD FS باید گواهی‌نامه تایید هویت سرور را نیز داشته باشد تا امنیت ارتباط خود را با کلاینت وب تضمین کند.

AD FS براحتی از AD CS این گواهی‌نامه‌ها را دریافت و مدیریت می‌کند. به خاطر داشته باشید که به دلیل اینکه بسیاری از نقش‌های AD FS به بیرون سرویس می‌دهند گواهی‌نامه‌های ما باید از مرجع معتبری دریافت شود. در غیر این‌صورت باید روی همه کلاینت‌های وب انباره CA معتبر را ویرایش کنیم.

اصطلاحات AD FS

AD FS به دلیل نیاز به فناوری‌های مختلف از اصطلاحات مختلفی از منابع مختلف استفاده می‌کند. برای کار کردن با این سرویس بهتر است با این اصطلاحات آشنا شویم. جدول ۱- ۱۷ رایج‌ترین واژه‌های مورد استفاده را خلاصه می‌کند. بسیاری از این واژه‌ها قبلا تعریف شده‌اند.

جدول ۱- ۱۷ اصطلاحات رایج AD FS

واژه	شرح

سرور account federation	سرور federation که در شبکه داخلی account organization قرار دارد
پراکسی سرویس account federation	FSP که در شبکه perimeter مربوط به account organization قرار دارد. به عنوان یک رله بین perimeter و سرور federation عمل می‌کند.
Account partner یا Account organization	شریکی که میزبان دایرکتوری AD DS است که حاوی حساب‌های کاربرانی است که به برنامه‌های اکسترانت دسترسی دارند.
عامل وب AD FS	یک عامل که روی سرور وب مجری IIS نصب می‌شود. عامل کار تفسیر claim ها و توکن‌های فراهم شده توسط سرور federation را انجام می‌دهد. این عامل از claim ها یا تایید هویت عجین شده ویندوز برای دسترسی به برنامه‌ها استفاده می‌کند.
Claim	عبارتی که سرور federation درباره یک کاربر یا کلاینت می‌سازد
برنامه claims-aware	یک برنامه ASP.NET که می‌تواند claim ها را برای اعطاء دسترسی به کاربر تفسیر کند.
Claim mapping	وقتی سرور federation یک claim ورودی را پردازش می‌کند و آنرا به منظور استخراج اعتبار مورد نیاز کاربر فیلتر می‌کند.
Client account parner discovery Web page	صفحه وبی که partner organization ها را لیست می‌کند و به کابران اجازه می‌دهد سازمان خود را در حین فرایند ورود تشخیص دهند.
گواهی‌نامه تایید هویت کلاینت	AD FS از تایید هویت بین سرور federation و پراکسی استفاده می‌کند. برای این کار پراکسی به گواهی‌نامه تایید هویت کلاینت نیاز دارد و سرور federation به گواهی‌نامه تایید هویت سرور.
صفحه وب ورود و خروج کلاینت	AD FS صفحات وب سفارشی برای ارسال بازخورد تصویری به کاربر استفاده می‌کند وقتی که AD FS session را باز می‌کنند یا می‌بندند.
برنامه federated	همانند برنامه claims-aware است. می‌تواند از federated identities برای تایید هویت استفاده کند.
کاربر federated	به هر کاربری که در account directory، claim های مناسب اعطاء می‌شود تا به برنامه‌های resource organization دسترسی پیدا کنند.
Federation	هر دو سازمان که بین آنها federation trust برقرار است.
Federation trust	Trust یک‌طرفه بین یک resource organization و account organization که بخواهد با آن شراکت کند.

Organization claims	همه claim هایی که در فضای نام سازمان قرار دارد.
کلاینت غیرفعال	هر مرورگر HTTP که از کوکی استفاده می‌کند. کلاینت باید از سرویس وب WS-F PRP پشتیبانی کند.
Resource account	اگر بخواهیم از تایید هویت Windows Integrated استفاده کنیم باید برای هر کاربر که باید دسترسی اعطاء کنیم resource account بسازیم. فرایند تایید هویت ویندوز NT به این حساب برای ارسال اعتبار به کاربر نیاز دارد.
سرور resource federation	سرور داخلی که برای اجرای claims mapping استفاده می‌شود و توکن‌های امنیتی دسترسی برای کاربرانی که نیاز به کار با یک برنامه را دارند صادر می‌کند. این سرور federation در شبکه داخلی resource organization قرار دارد.
resource federation service proxy	پراکسی موجود در شبکه perimeter مربوط به resource organization. کار آن اجرای account partner discovery برای کلاینت‌های اینترنت است و درخواست‌های وارد دریافت شده را به سرور federation داخلی می‌فرستد.
Resource group	در resource forest برای map کردن group claim های ورودی استفاده می‌شود. سپس برای پشتیبانی از تایید هویت ویندوز NT استفاده می‌شود.
Resrource partner یا resource organization	سازمانی که میزبان برنامه‌های federated در شبکه perimeter است.
توکن امنیتی	شیء امضاء شده دیجیتالی که حاوی claim های کاربر است. وقتی یک توکن امنیتی صادر می‌شود یعنی کاربر با موفقیت برای سرور account federation تایید هویت شده است.
سرویس توکن امنیتی STS	سرویس وب AD FS که برای صدور توکن کاربرد دارد. در AD FS سرویس federation خود یک STS است.
گواهی‌نامه تایید هویت سرور	AD FS از تایید هویت دوطرفه بین سرور federation و پراکسی استفاده می‌کند. برای این کار پراکسی به گواهی‌نامه تایید هویت کلاینت نیاز دارد و سرور federation به گواهی‌نامه تایید هویت سرور. سرورهای وب سازگار با AD FS همچنین به گواهی‌نامه‌های تایید هویت سرور برای تایید هویت خود در برابر مرورگر کلاینت‌ها نیاز دارند.
Server farm	گروهی از سرورهای federation که با هم برای پایدار کردن سرویس federation کار می‌کنند. Server farm می‌تواند به هر سرور federation ، پراکسی یا سرور وب سازگار با

	AD FS اعمال شود ولی هر farm می‌تواند حاوی فقط یک نوع سرور federation باشد.
معماری مبتنی بر سرویس (SOA)	SOA معماری مبتنی بر استاندارد و مستقل از زبان هستند که برای پشتیبانی از سرویس‌های توزیع شده در اینترنت به سرویس وب نیاز دارند.
Single sign-in (SSO)	SSO دسترسی به برنامه را تسهیل می‌کند به طوری که کاربر باید فقط یکبار اعتبار خود را وارد کند.
گواهی‌نامه token-signing	گواهی‌نامه‌ای است که برای امضاء توکن‌های امنیتی تولید شده توسط سرور resource federation استفاده می‌شود.
سیاست trust	مجموعه پارامترهایی که سرویس federation برای تشخیص شرکاء، گواهی‌نامه‌ها، انباره‌های حساب، calim ها و خصوصیات مختلف هویت‌هایی که با سرویس federation مرتبط هستند تعریف می‌کند. این سیاست در قالب فایل XML است.
Uniform resource identifier (URI)	AD FS برای تشخیص شرکاء و انباره‌های حساب به URI نیاز دارد.
گواهی‌نامه verification	کلید عمومی گواهی‌نامه token-signing که روی همه سرورهای federation در یک سازمان بارگذاری می‌شود.
سرویس‌های وب WS-*	سرویس اینترنت مبتنی بر استاندارد که بخشی از SOA را تشکیل می‌دهد. به طور خلاصه سرویس‌های وب نامیده می‌شود و حاوی Simple Object Access Protocol (SOAP) ، XML و UDDI است. سرویس‌های وب مستقل از زبان هستند به طوری که می‌توانند اطلاعات را بین زیرساخت‌های متفاوت IT منتقل کنند مانند UNIX، Linux و ویندوز.
امنیت سرویس‌های وب (WS-Security)	مشخصات SOA که چگونگی امضاء دیجیتال و رمزنگاری پیغام‌های SOAP را مشخص می‌کند.
برنامه مبتنی بر توکن ویندوز NT	برنامه مبتنی بر ویندوز که در تایید هویت ویندوز NT بوده و اعتبارسنجی را پردازش می‌کند.
WS-Federation	مشخصات سرور وب که استانداردهای مورد استفاده هنگام پیاده‌سازی federation را مشخص می‌کند
WS-Federation Passive Requestor Profile (WS-F PRP)	جزئی از WS-Federation که پروتکل استاندارد مورد استفاده هنگام دسترسی کلاینت غیرفعال را به برنامه از طریق سرویس federation مشخص می‌کند

نصب AD FS

نصب ابتدایی AD FS نیازمند چند کامپیوتر است. در حالت ایده‌آل باید دو دامنه AD DS، دو شبکه perimeter و سرورهای AD FS توزیع شده در هر شبکه داشته باشیم. account organization بهتر است میزبان AD DS و حداقل یک سرور federation داخلی و Federation Service Proxy در شبکه perimeter خود باشد. resource organization بهتر است یک AD DS و حداقل یک سرور federation داخلی داشته باشد. شبکه perimeter آن باید حاوی حداقل یک سرور وب سازگار با AD FS و یک FSP باشد. توزیع کاملی که ما طراحی می‌کنیم باید بر اساس اطلاعاتی نظیر تعداد partner organization ، نوع برنامه کاربردی به اشتراک گذاشته شده، نیازمندی‌های پایداری سرویس و تقسیم بار و موارد دیگر از این نوع باشد.

محیط تست باید با چهار کامپیوتر تجهیز شود. یک کلاینت، یک سرور وب سازگار با AD FS و دو سرور federation برای شرکت در AD FS federation بین دو سازمان. به دلیل ذات AD FS ساعت‌های کامپیوترها باید یکسان بوده یا تفاوت آنها کمتر از ۵ دقیقه باشد. در غیر این‌صورت فرایند به خوبی پیش نمی‌رود زیرا time stamp های توکن نامعتبر خواهد بود. به دلیل اینکه بسیاری از کامپیوترها بخشی از دامنه AD DS نیستند نمی‌توانیم از PDC Emulator Operations Master برای یکسان‌سازی ساعت استفاده کنیم. بهترین راه برای یکسان‌سازی Nerwork Time Protocol (NTP) است که هر سرور را به سرور ساعت خارجی لینک کرده و زمان آنها را یکسان می‌کند.

نیازمندی‌های نصب AD FS

برای نصب AD FS باید با پیش‌نیازها شروع کنیم. جدول ۲- ۱۷ نیازمندی‌های اساسی توزیع AD FS را خلاصه می‌کند. توجه داشته باشید که سرویس federation ابتدا با ویندوز سرور 2003 R2 ارائه شد. به همین دلیل می‌توانیم ارتباط بین ویندوز سرور 2003 R2 و 2008 را برقرار کنیم. جدول ۲- ۱۷ نیازمندی‌های نصب AD FS را لیست می‌کند که فقط روی ویندوز سرور 2008 اجرا می‌شود.

جدول ۲- ۱۷ نیازمندی‌های توزیع AD FS

سخت‌افزاری / نرم‌افزاری	نیاز	نکته
پردازشگر	133 MHz برای کامپیوترهای x86-based	به دلیل نیازمندی کم می‌توان به صورت ماشین مجازی پیاده کرد.
حافظه	512 MB	1GB پیشنهاد می‌شود
فضای دیسک	10 MB برای نصب AD FS	50GB پیشنهاد می‌شود.
سیستم عامل	ویندوز سرور 2008 نسخه Enterprise یا Datacenter	سرویس‌ها روی سیستم‌های عامل قدیمی اجرا نمی‌شوند.

سرویس وب	IIS با سازگاری ASP.NET Framework 2.0	از IIS 7.0 با ASP.NET 2.0 و .NET Fremework 2.0 استفاده شود.
محل نصب	محل پیش‌فرض	سرویس federation و پراکسی سرویس Federation نمی‌توانند روی یک سرور نصب شوند.
نیازمندی‌های انباره حساب AD DS و AD LDS	حداقل یک دامنه	دو forest ایده‌آل است. در بدترین حالت از یک forest و یک انباره AD LDS استفاده می‌شود.
گواهی‌نامه نصب برای TLS/SSL و امضاء توکن	دریافت یک گواهی‌نامه SSL تایید هویت سرور برای هر نقش سروری AD FS	از یک CA تجاری خارجی برای به دست آوردن یک گواهی‌نامه معتبر استفاده می‌شود.
ارتباطات شبکه TCP/IP	Ipv4 یا Ipv6 ترجیحا آدرس دستی	ارتباط شبکه باید بین کلاینت، DC و کامپیوترهای میزبان سرویس federation و عامل وب AD FS برقرار باشد.
پیکربندی DNS	ساخت رکورد CNAME سرور داخلی که سرویس federation را اجرا می‌کند.	از فایل‌های host استفاده نشود.
مرورگر وب	Microsoft IE 5 با بالاتر و Firefox Safari	Jscript و حداقل کوکی‌های معتبر باید برای سرورهای federation و برنامه‌های وب فعال باشد
سیستم عامل کلاینت	ویندوز XP یا ویستا برای کلاینت	ویندوز ویستا پیشنهاد می‌شود.

نکات ارتقاء

بسیاری از سازمان‌ها از حساب سرویس خاصی هنگام توزیع سرویس‌هایی نظیر AD FS استفاده می‌کنند. اگر بخواهیم این کار را در ویندوز سرور 2003 R2 انجام دهیم باید حساب‌ها و کلمات عبور منتسب به هر سرویس را یادداشت کنیم زیرا فرایند ارتقاء AD FS

به طور خودکار همه این سرویس‌ها را ریست می‌کند تا از حساب Nerwork Service استفاده کند. پس از ارتقاء می‌توانیم سرویس را به حالت قبل برگردانیم.

بهتر است عملیات ارتقاء را قبل از نصب در محیط شبکه واقعی در محیط آزمایش‌گاه تست کنیم.

تمرین آماده کردن توزیع AD FS

در این تمرین با تعداد زیادی کامپیوتر یک محیط پیچیده AD FS خواهیم ساخت. در جدول ۳-۱۷ نقش این رایانه ها و دامنه در توزیع AD FS خلاصه شده است

جدول ۳-۱۷ نقش های کامپیوتر AD FS

Table 17-3 AD FS Computer Roles

Domain Name	Role
contoso.com	Account Domain
woodgrovebank.com	Resource Domain
Computer Name	**Role**
SERVER01	AD DS domain controller for *contoso.com*, the account domain
SERVER03	The federation server for *contoso.com*, the account domain
SERVER04	The Federation Service Proxy for *contoso.com*, the account domain
SERVER05	The SQL Server database server for the AD RMS deployment in *contoso.com*
SERVER06	AD DS domain controller for *woodgrovebank.com*, the resource domain
SERVER07	The federation server for *woodgrovebank.com*, the resource domain
SERVER08	The Federation Service Proxy and AD FS–enabled Web server for *woodgrovebank.com*, the resource domain

ابتدا با آماده سازی نصب DNS در تمامی forest ها شروع کرده و بعد به سراغ نصب سرور federation می رویم. سپس پراکسی سرویس federation را در هر دو forest و سایت وب AD FS-enabled در resource forest نصب می کنیم.

تمرین اول پیکربندی cross-DNS references

در این تمرین سرور forest DNS ها را پیکربندی می کنیم. چون این forest ها بصورت مستقل عمل می کنند سرور های DNS در مورد هم چیزی نمی دانند و برای تبادل اطلاعات بین forest ها نیاز به پیاده سازی cross-DNS references در هر forest داریم. آسانترین راه برای انجام این کار استفاده از forwarder ها از یک دامنه به دامنه دیگر و بلعکس می باشد. ابتدا از کار کردن SERVER01 و SERVER06 مطمئن می شویم.

۱- با اعتبار مدیر شبکه دامنه وارد SERVER01 می شویم
۲- Server Manager را از Administrative Tools اجرا می کنیم
۳- گره Roles\DNS Serve\DNS\SERVER01 را باز می کنیم
۴- روی SERVER01 راست کلیک کرده و Properties را انتخاب می کنیم
۵- روی زبانه Forwarders و سپس Edit کلیک می کنیم
۶- آدرس IP مربوط به SERVER06 را تایپ کرده و دوبار روی OK کلیک می کنیم
۷- این عملیات را در مورد SERVER06 نیز انجام داده و آدرس IP مربوط به SERVER01 را به عنوان forwarder برای SERVER06 وارد می کنیم
۸- با Ping کردن هر سرور از سرور دیگر ، نتیجه را امتحان می کنیم. برای مثال از دستور زیر برای Ping کردن SERVER01 از SERVER06 استفاده می کنیم:

```
ping server01.contoso.com
```

تمرین دوم نصب سرورهای federation

در این تمرین سرورهای federation را نصب خواهیم کرد. این کار با نصب نقش سرور بعلاوه سرویسهای پشتیبان برای این نقش انجام می شود. ابتدا از کارکرد SERVER01 ، SERVER03 ، SERVER06 و SERVER07 مطمئن می شویم

۱- با اعتبار مدیر شبکه دامنه وارد SERVER07 می شویم

برای نصب و کارکردن با AD FS به اعتباری این چنین بالا نیاز نداریم اما استفاده از این سطح اعتبار انجام این تمرین را آسانتر خواهد کرد

۲- Server Manager را از Administrative Tools اجرا می کنیم

۳- روی گره Roles راست کلیک کرده و Add Roles را انتخاب می کنیم

۴- اطلاعات Before You Begin را مرور کرده و روی Next کلیک می کنیم

۵- در صفحه Select Server Roles ، Active Directory Federation Services را انتخاب کرده و روی Next کلیک می کنیم

۶- اطلاعات مربوط به نقش را مرور کرده و روی Next کلیک می کنیم

۷- در صفحه Select Role Services ، Federation Service را انتخاب می کنیم. Server Manager از ما می خواهد تا ویژگیها و سرویس های مورد نیاز نقش را نصب کنیم. روی Add Required Role Services کلیک کرده و سپس روی Next کلیک می کنیم

۸- در صفحه Choose A Server Authentication Certificate For SSL Encryption ، Create A Self-Signed Certificate For SSL Encryption را انتخاب کرده و روی Next کلیک می کنیم

در محیط واقعی نیازمند درخواست گواهی نامه از یک CA معتبر هستیم

۹- در صفحه Choose A Token-Signing Certificate ، Create A Self-Signed Token-Signing Certificate را انتخاب کرده و روی Next کلیک می کنیم

۱۰- در صفحه Select Trust Policy ، Create A New Trust Policy را انتخاب کرده و روی Next کلیک می کنیم.

آدرس این trust policy را به یادداشت می کنیم چرا که ارتباط federation ما برای کارکردن وابسته به آن می باشد

۱۱- اطلاعات صفحه Web Server (IIS) را مرور کرده و روی Next کلیک می کنیم

۱۲- در صفحه Select Role Services مقادیر پیش فرض را قبول کرده و روی Next کلیک می کنیم

۱۳- در صفحه Confirm Installation Selections ، انتخابها را مرور کرده و روی Install کلیک می کنیم

۱۴- در پایان مراحل نصب برای بستن ویزارد روی Close کلیک می کنیم

۱۵- مراحل بالا را برای SERVER03 تکرار می کنیم

چون SERVER03 خود یک CA ریشه می باشد مراحل کوتاه تر است

تمرین سوم نصب پراکسی های سرویس **Federation**

در این تمرین پراکسی های سرویس federation را نصب خواهیم کرد. این کار با نصب نقش سرور بعلاوه سرویسهای پشتیبان برای این نقش انجام می شود. ابتدا از کارکرد صحیح SERVER01 ، SERVER03 ، SERVER04 ، SERVER06 ، SERVER07 و SERVER08 مطمئن می شویم

۱- با اعتبار مدیر شبکه دامنه وارد SERVER08 می شویم

۲- Server Manager را از Administrative Tools اجرا می کنیم

۳- روی گره Roles راست کلیک کرده و Add Roles را انتخاب می کنیم

۴- اطلاعات Before You Begin را مرور کرده و روی Next کلیک می کنیم

۵- در صفحه Select Server Roles ، Active Directory Federation Services را انتخاب کرده و روی Next کلیک می کنیم

۶- اطلاعات مربوط به نقش را مرور کرده و روی Next کلیک می کنیم

۷- در صفحه Select Role Services ، Federation Service Proxy را انتخاب کرده و روی Add Required Role Services کلیک کرده و همچنین AD FS Web Agents را انتخاب می کنیم و سپس روی Next کلیک می کنیم

باید به خاطر داشته باشیم اگرچه نمی توان Federation Service Proxy را به همراه federation server روی یک سرور اجرا کرد اما می توان FSP و AD FS Web Agents را با هم ترکیب کرد

۸- در صفحه Choose A Server Authentication Certificate For SSL Encryption ، Create A Self-Signed Certificate For SSL Encryption را انتخاب کرده و روی Next کلیک می کنیم

در محیط واقعی نیازمند درخواست گواهی نامه از یک CA معتبر هستیم

۹- در صفحه Specify Federation Server عبارت server07.woodgrovebank.com را تایپ کرده و روی Validate کلیک می کنیم

اعتبارسنجی موفق نخواهد بود چون هنوز رابطه trust بین رایانه ها تعریف نشده است . این کار از طریق صدور و ورود گواهی نامه های SSL ها برای سرورها از طریق IIS انجام می شود

۱۰- روی Next کلیک می کنیم

۱۱- در صفحه Choose A Client Authentication Certificate ، Create A Self-Signed Client Authentication Certificate را انتخاب کرده و روی Next کلیک می کنیم

۱۲- اطلاعات صفحه Web Server (IIS) را مرور کرده و روی Next کلیک می کنیم

۱۳- در صفحه Select Role Services مقادیر پیش فرض را پذیرفته و روی Next کلیک می کنیم

۱۴- در صفحه Confirm Installation Selections انتخابهایمان را مرور کرده و روی Install کلیک می کنیم

۱۵- هنگامی که فرآیند نصب تمام شد برای بستن ویزارد روی Close کلیک می کنیم

۱۶- همین عملیات را برای SERVER04 در دامنه *contoso.com* تکرار می کنیم. هنگامی که از ما درخواست نام federation server شد نام **server03.contoso.com** را وارد می کنیم. در زمان نیاز از self-signed certificate ها استفاده می کنیم و AD FS Web Agents را روی SERVER04 نباید نصب کنیم. نقش SERVER04 تنها FSP می باشد چون در یک Account Organization کار می کند

خلاصه درس

- AD FS انباره تایید هویت داخلی را از طریق identity federation و federation trust به محیط خارج بسط می دهد
- یک Federation partnership همیشه از resource organization و account organization تشکیل می شود که در آن resource organization می تواند شریک چند account organization باشد اما account organization تنها می تواند با یک resource organization در ارتباط باشد
- AD FS برای یک ارتباط امن و تشخیص هویت سرور و کلاینت بر اعتبارسنجی گواهی نامه ها از طریق SSL استوار است. بنابراین تمام ارتباط ها بر مبنای پورت ۴۴۳ و HTTPS خواهند بود

سئوالات پایان درس

۱- فرض کنید مدیر سیستم شرکت Contoso هستیم. سازمان ما در حال حاضر دارای یک federation relationship با بانک Woodgrove می باشد که با استفاده از federation service ویندوز سرور 2003 R2 پیاده سازی شده است. برای بهبود امنیت federation service را با حسابهایی که سرویس را راه اندازی می کنند ، توزیع می کنیم. اکنون آماده ارتقا به AD FS هستیم اما هنگامی که اقدام به ارتقا می کنیم متوجه می شویم که حساب پاک شده است و با یک حساب Nerwork Service جایگزین شده است. چرا این اتفاق افتاده است؟

A . نمی توان از این حساب سرویس برای راه اندازی سرویس AD FS استفاده کرد

B . حساب سرویس پیش فرض که برای نصب یا ارتقا AD FS استفاده می شود Nerwork Service است

C . Woodgrove دارای سیاستهایی است که طبق آنها تمام federation service ها باید با حساب Nerwork Service راه اندازی شوند

D . مایکروسافت ترجیح می دهد برای راه اندازی federation service از حساب Network Service استفاده کند.

درس ۲: پیکربندی و استفاده از AD FS

همان‌طور که در درس ۱ دیدیم سرورها در یک ارتباط AD FS باید از گواهی‌نامه‌ها برای ساخت زنجیره trust بین هم استفاده کنند. همان‌گونه که در فصل ۱۵ بحث شد بهترین راه برای تضمین اعتبار زنجیره trust دریافت گواهی‌نامه از CA خارجی معتبر به صورت مستقیم یا با واسطه است.

این فقط یکی از جنبه‌های پیکربندی AD FS است که باید انجام شود. وقتی AD FS را توزیع می‌کنیم ممکن است بخواهیم برنامه‌های AD FS-aware، سیاست‌های trust بین partner organization و claim های کاربر یا گروهها را پیکربندی کنیم. سپس می‌توانیم کار مدیریت و اجرای AD FS را شروع کنیم.

تکمیل پیکربندی AD FS

هنگام توزیع AD FS باید عملیات مختلفی را به شرح زیر انجام دهیم.

- سرویس وب را روی همه سرورها برای استفاده از رمزنگاری SSL/TSL برای سایت وب که میزبان سرویس AD FS است پیکربندی کنیم.
- گواهی‌نامه‌ها را از همه سرورها به سرورهای دیگر که ارتباط را شکل می‌دهند منتقل کنیم. برای مثال گواهی‌نامه token-siging مربوط به سرور federation باید به عنوان گواهی validation در سرورهای دیگر با ارتباط trust نصب شود.
- IIS باید روی سرورهایی که میزبان برنامه‌های claims-aware هستند پیکربندی شود. این سرورها باید از HTTPS برای ارتباطات application-related استفاده کنند.
- ساخت و پیکربندی برنامه‌های claims-aware انجام شود
- سرورهای federation در همه partner organization ها پیکربندی شود. شامل مراحل زیر است:
  - در یک account organization سیاست trust باید پیکربندی شود claim های کاربران باید ساخته شود و در نهایت انباره حساب AD DS برای identity federation باید پیکربندی شود.
  - در resource organization سیاست trust باید پیکربندی شود claim های کاربران باید ساخته شود انباره حساب AD DS برای identity federation باید پیکربندی شود و سپس برنامه claims-aware فعال شود.
- Federation trust باید ساخته شود. این کار مراحل متعددی دارد:
  - انتقال سیاست trust از account organization به resource organization.
  - ساخت و پیکربندی یک claim mapping در resource organization.
  - انتقال سیاست partner از resource organization به account organization.

بیشتر این کار مربوط به mapping گواهی‌نامه از یک سرور به سرور دیگر است. یک عامل مهم توانایی دسترسی به ریشه یا حداقل وب سایت‌های میزبان CRL برای هر گواهی‌نامه است. همان‌طور که در فصل ۱۵ بحث شد CRL ها تنها راهی است که به اعضاء trust می‌توان گفت آیا یک گواهی‌نامه معتبر است یا نه. اگر پشتیبانی شود می‌توان از سرویس Microsoft Online Responder (OCSP) از AD CS نیز استفاده کرد.

در AD FS، CRL checking به طور پیش‌فرض فعال است. CRL checking عمدتا برای امضاءهای توکن امنیتی اجرا می‌شود ولی بهتر است برای همه امضاهای دیجیتال از آن استفاده کرد.

استفاده و مدیریت AD FS

وقتی پیکربندی identity federation به پایان می‌رسد می‌توانیم به مدیریت روتین سرویس‌های AD FS بپردازیم. برای انجام این عملیات از کنسول Active Directory Federation Services در Server Manager استفاده می‌شود. مراحل به ترتیب زیر است:

- پیکربندی سرویس federation یا federation server farm. ما می‌توانیم تا سه farm در AD FS داشته باشیم:
  - federation server farm که حاوی سرورهای متعددی است که میزبان یک نقش هستند.
  - Federation Service Proxy farm
  - Claim-aware application server farm که مجری IIS باشد.
- مدیریت سیاست trust که با سرویس federation عجین شده است این کار به صورت‌های زیر انجام می‌شود.
  - مدیریت انباره‌های حساب در AD DS یا AD LDS
  - مدیریت account partnet و resource partner یا هردو که با سازمان ما trust دارند.
  - مدیریت claim روی سرور federation
  - مدیریت گواهی‌نامه‌های مورد استفاده توسط سرورهای federation
  - مدیریت گواهی‌نامه‌ها در برنامه‌های کاربردی وب حفاظت شده توسط AD FS

به دلیل اینکه AD FS خیلی به IIS متکی است بسیاری از تنظیمات سرورهای federation که در گره Active Directory Federation Services در Server Manager پیکربندی می‌شود در فایل Web.config در دایرکتوری مجازی Federation Service مربوط به IIS ذخیره می‌شود. تنظیمات پیکربندی دیگر در فایل سیاست trust ذخیره می‌شود. همانند دیگر تنظیمات IIS فایل Web.config مستقیما قابل ویرایش است زیرا فقط یک فایل متنی است. تنظیماتی که می‌توانیم از طریق فایل Web.config کنترل کنیم شامل:

- مسیر فایل سیاست trust
- گواهی‌نامه محلی مورد استفاده برای توکن‌های امضاء
- محل صفحات وب ASP.NET که سرویس را پشتیبانی می‌کنند
- سطح debug logging برای سرویس و مسیر دایرکتوری فایل‌های log

- قابلیت کنترل نوع دسترسی برای مثال دسترسی کاربران ناشناخته به group claims که برای سازمان آماده کردیم.

هنگام ویرایش ما باید فایل Web.config را روی سرورهای نیازمند همان تنظیمات پیکربندی منتشر کنیم. پس از اینکه IIS راه‌اندازی مجدد شود پیکربندی جدید اعمال می‌شود.

ولی فایل سیاست trust به صورت دستی قابل ویرایش نیست. این فایل باید از طریق کنترل‌های کنسول AD FS یا تنظیماتی مدل شیء AD FS ویرایش شود.

برای کار با FSP از کنسول AD FS استفاده می‌کنیم.

- سرویس federation که با آن FSP کار می‌کند
- روشی که از طریق آن FSP اطلاعات اعتبار کاربر را از مرورگرها و برنامه‌های وب جمع‌آوری می‌کند

تنظیماتی که برای پراکسی‌های سرویس Federation پیکربندی می‌شود همانند تنظیمات سرور federation در فایل Web.config نیز ذخیره می‌شود. ولی به دلیل اینکه FSP حاوی یک سیاست نیست همه تنظیمات آن در فایل Web.config ذخیره می‌شود که شامل موارد زیر است:

- URL سرویس Federation
- گواهی‌نامه تایید هویت کلاینت برای استفاده توسط پراکسی سرور federation برای ارتباطات رمزنگاری شده TLS/SSl با سرویس federation.
- صفحات وب ASP.NET که از سرویس پشتیبانی می‌کند.

آماده‌سازی و پیاده‌سازی identity federation از طریق AD FS نیاز به مراقبت و برنامه‌ریزی دارد. به همین دلیل قبل از پیاده‌سازی در شبکه واقعی باید در محیط آزمایشگاه آنرا تست کنیم.

تمرینات تکمیل پیکربندی AD FS

در این تمرین نصب AD FS را تکمیل می‌کنیم. برای این تمرین از همان کامپیوترها استفاده می‌کنیم. ابتدا سرور IIS را روی همه سرورهای federation پیکربندی می‌کنیم و سپس گواهی‌نامه‌ها را از یک سرور به سرور دیگر نگاشت می‌کنیم و سرور وب را پیکربندی می‌کنیم. همچنین می‌توانیم برنامه وب را ساخته و پیکربندی کنیم. سپس سرورهای federation را برای همه سازمان‌های شریک پیکربندی می‌کنیم. در آخر federation trust را برقرار می‌سازیم.

تمرین ۱ پیکربندی SSL برای سرورهای federation و FSP ها

در این تمرین کار پیکربندی IIS را طوری انجام می‌دهیم که SSL روی وب سایت پیش فرض سرورهای federation و پراکسی‌های سرویس federation مورد نیاز باشد. در این تمرین به SERVER01، SERVER03، SERVER04 ، SERVER05، SERVER06، SERVER07 و SERVER08 نیاز داریم.

۱. با حساب مدیر دامنه به SERVER03 وارد می‌شویم.
۲. IIS Manager را اجرا می‌کنیم.
۳. گره Servername\Sites\Default \Web Site را باز می‌کنیم.

۴. در پنل وسط به بخش IIS رفته و روی SSL Settings دوبار کلیک می‌کنیم.
۵. در صفحه SSL Settings کادر Require SSL را علامت می‌زنیم.
۶. زیر Client Certificates گزینه Accept را انتخاب کرده و بعد روی Apply در پنل Actions کلیک می‌کنیم.
۷. این مراحل را روی SERVER04، SERVER07 و SERVER08 تکرار می‌کنیم.

تمرین ۲ انتقال گواهی‌نامه تایید هویت SSL به یک سرور

با SERVER03 شروع می‌کنیم.

۱. با کاربر مدیر دامنه به SERVER03 وارد می‌شویم.
۲. کنسول MMC را باز می‌کنیم.
۳. از منوی File گزینه Add/Remove Snap-in را انتخاب کرده و ابزار Certificate را انتخاب و روی Add کلیک می‌کنیم.
۴. Computer Account را انتخاب کرده و روی Next کلیک می‌کنیم. مطمئن می‌شویم که Local Computer انتخاب شده است روی Finish و بعد OK کلیک می‌کنیم.
۵. از منوی File گزینه Save As را انتخاب کرده و نام آنرا Computer Certificates می‌گذاریم.
۶. گره Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities
۷. روی Trusted Root Certification Authorities کلیک راست کرده و روی All Tasks کلیک می‌کنیم سپس روی Import کلیک می‌کنیم.
۸. در صفحه Welcome To The Certificate Import Wizard روی Next کلیک می‌کنیم.
۹. در صفحه File To Import روی Browse کلیک کرده و به مسیر C:\Temp می‌رویم.
۱۰. گواهی‌نامه SERVER04 یعنی SERVER04SSL.cer را انتخاب کرده و روی Open و Next کلیک می‌کنیم.
۱۱. در صفحه Certificate Store گزینه Place All Certificates In The Following Store را انتخاب می‌کنیم. مطمئن می‌شویم که انباره انتخاب شده Trusted Root Certification Authorities بوده و روی Next کلیک می‌کنیم.
۱۲. در صفحه Completing The Certificate Import Wizard اطلاعات را بررسی می‌کنیم و روی Finish کلیک می‌کنیم.

خلاصه درس

- به دلیل اینکه AD FS از ارتباطات امن استفاده می‌کند باید مطمئن شویم که همه سرورها در شراکت AD FS به گواهی‌نامه ریشه که برای صدور گواهی‌نامه سرورها استفاده می‌شد trust دارند. اگر از گواهی‌نامه self-signed استفاده کنیم باید همه گواهی‌نامه‌ها را به انباره trusted CA سرور منتقل کنیم.
- وقتی شراکت را پیکربندی می‌کنیم باید ابتدا برنامه‌های claims-aware ساخته و claim های مشخصی را به شرکاء اختصاص دهیم.
- پس از ساخت claim تشخیص می‌دهیم کدام انباره دایرکتوری توسط سرور federation استفاده خواهد شد.
- Federation trust بین دو شریک ساخته می‌شود. سیاست trust روی هر سرور آماده شود. سیاست trust از سرور account federation به سرور resource federation منتقل می‌شود. بعد از این سیاست trust برای انتساب claim ها به account organization استفاده می‌شود. برای تکمیل federation trust سیاست شریک را از RFS به AFS منتقل می‌کنیم. بعد از این شراکت ایجاد شده است.

سئوالات پایان درس

۱. فرض کنید مدیر دامنه contoso.com هستیم. سازمان ما تصمیم گرفته است شراکت federation با Woodgrove Bank برقرار کند به طوری که بتوانیم از identity federation برای دسترسی به یک برنامه جدید در شبکه perimeter بانک استفاده کنیم. سرورهای federation و پراکسی‌های سرویس federation از قبل حضور دارند ولی باید federation trust را پیکربندی کنیم تا identity federation فعال شود. کدام یک از موارد زیر باید انجام شود؟ (امکان انتخاب همه گزینه‌ها وجود دارد.)
   A. با خود در Woodgrove Bank تماس می‌گیریم تا مشخص کنیم چطور اطلاعات باید رد و بدل شود.
   B. سیاست شراکت را از Woodgrove Bank به Contoso منتقل می‌کنیم.
   C. سیاست شراکت را از Contoso به Woodgrove Bank منتقل می‌کنیم.
   D. سیاست trust را از Contoso به Woodgrove Bank منتقل می‌کنیم.
   E. یک claim را در Woodgrove Bank ساخته و پیکربندی می‌کنیم.
   F. سیاست trust را از Woodgrove Bank به Contoso منتقل می‌کنیم.

جدول جواب‌ها

شماره فصل	شماره درس	شماره پرسش	جواب یا جواب‌های صحیح
۱	۱	۱	A و B
		۲	D
	۲	۱	A
		۲	D
۲	۱	۱	C
	۲	۱	D
	۳	۱	A و B و D
۳	۱	۱	C
		۲	A
	۲	۱	C
		۲	D
		۳	A و B و D
	۳	۱	C
		۲	B و C
		۳	A
۴	۱	۱	B
		۲	D
		۳	C و D و E و F
	۲	۱	B و C و D
		۲	B
		۳	D
	۳	۱	D
		۲	D
		۳	B و C و D
۵	۱	۱	D
		۲	A
		۳	B
	۲	۱	C
		۲	A و D و E
	۳	۱	A
		۲	C و D و E
		۳	C
۶	۱	۱	B و D
		۲	B و D
		۳	D
	۲	۱	B و C
		۲	A و D
	۳	۱	B و D
		۲	A

۷	۱	۱	A و B و C و D
	۲		Aو C
	۳		A و C و D
	۱	۲	B
	۲		C
	۳		A و D
	۱	۳	B و D
	۲		A و D
	۳		A و C و D و E
	۱	۴	D
	۲		B
	۳		E و F و G
۸	۱	۱	C و D و E
	۲		D
	۳		C
	۱	۲	B
	۲		C
	۱	۳	B
	۲		A
	۳		B و D
۹	۱	۱	C
	۲		B و D
	۱	۲	A و B و C و D و E
	۲		A و B
۱۰	۱	۱	D
	۲		B و C و D
	۳		C
	۱	۲	E
	۲		D و E
	۳		A و B و C
	۱	۳	C و D
	۲		A
۱۱	۱	۱	C
	۲		A و D و E
	۱	۲	D
	۲		D و E
	۳		C
	۱	۳	D
	۲		B و C
	۳		A
	۴		A و B
۱۲	۱	۱	A و D

		۲	B و D و E
		۳	C
	۲	۱	A و C و G
		۲	C و D
		۳	D
۱۳	۱	۱	B
		۲	D و F
	۲	۱	C و D
		۲	A و B و C و D
۱۴	۱	۱	C
	۲	۱	D
۱۵	۱	۱	B و C
	۲	۱	B
۱۶	۱	۱	D
	۲	۱	B
۱۷	۱	۱	B
	۲	۱	A و B و D و E