آشنایی با زیرساخت‌های Active Directory در Windows Server 2003

تهیه و تنظیم: آناهیتا سنندجی

1— مقدمه

چکیده

یک دایرکتوری (Directory) مجموعه‌ای ذخیره‌شده از اطلاعات درباره‌ی اشیایی است که به نوعی با یکدیگر مرتبطند. یک سرویس دایرکتوری (Directory Service) تمامي‌اطلاعاتی را که برای استفاده و مدیریت این اشیا لازم است، در یک محل متمرکز ذخیره نموده و بدین ترتیب نحوه‌ي یافتن و مدیریت این منابع را تسهیل مي‌بخشد. یک Directory Service زمینه‌اي را فراهم مي‌آورد تا دسترسی به منابع در سطح شبکه به بهترین نحو ممکن سازمان یابد . کاربران و مدیران ممکن است که نام دقیق یک شئ مورد نیاز را ندانند، اما با دانستن یک یا چند ویژگی از یک شئ و با استفاده از Directory Service مي‌توانند لیستی از اشیا با ویژگی مورد نظر خود را جستجو کنند.

در این بخش به معرفی سرویس Active Directory در Windows Server 2003 پرداخته و به صورت مقدماتی با خصوصیات، اشیا موجود و اجزای آن (فیزیکی و منطقی) آشنا مي‌شویم.

کلمات کلیدی: Active Directory، Domain یا دامنه، Tree یا درخت، Forest یا جنگل، Organizational Units یا واحدهای سازمانی، Domain Controller، و سایت.

آشنایی با سرویس دایرکتوری موجود در ویندوز سرور 2003 (Active Directory)

Active Directory یک سرویس دایرکتوری بوده که در Windows Server 2003 قرار داده شده است. Active Directory شامل یک دایرکتوری بوده که اطلاعات مربوط به شبکه را ذخیره مي‌کند، علاوه بر آن دارای تمامي سرویس‌هایی است که اطلاعات را قابل استفاده کرده و در دسترس قرار مي‌دهد.

Active Directory ویژگی‌هاي زیر را ارائه مي‌کند:

- ذخیره‌ي متمرکز داده (Centralized data store)
- مقیاس پذیری (Scalability)
- قابلیت توسعه (Extensibility)
- قابلیت مدیریت (Manageability)
- استفاده و تمرکز بر سیستم نام‌گذاری دامنه (Integration with Domain Name System)
- مدیریت تنظیمات سرویس گیرنده (Client configuration management)
- مدیریت بر مبنای سیاست (Policy-based administration)
- تکرار اطلاعات (Replication of information)

- شناسایی ایمن و انعطاف پذیر (Flexible, secure authentication and authorization)
- برنامه‌ها و زیرساختارهای مبتنی بر دایرکتوری

(Directory-enable applications and infrastructures)

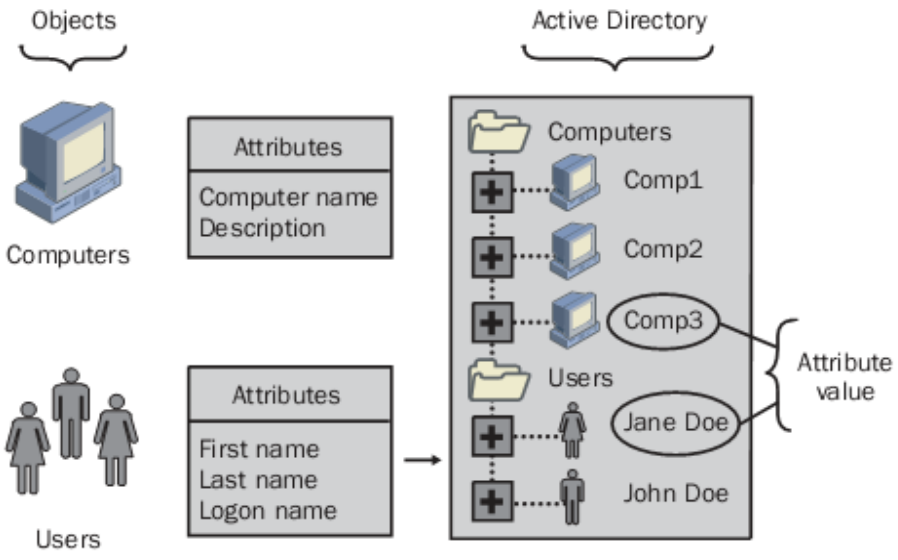
- تطبیق با سایر سرویس‌هاي دایرکتوری

(Interoperability with other directory services)

- ترافیک رمزگذاري شده و امضا شده LDAP (Signed and encrypted LDAP traffic)

اشیای موجود در Active Directory

هر داده‌اي که در Active Directory ذخیره مي‌شود، به صورت اشیایی (Objects) متفاوت سازمان مي‌یابد. یک شئ مجموعه مجزایی از صفات است که منابع شبکه را مشخص مي‌کند. صفات (Attributes)، خصوصیات اشیای موجود در یک دایرکتوری را شامل مي‌شود. به عنوان نمونه صفات یک User account (حساب کاربر) مي‌تواند شامل نام، نام خانوادگی و نام Log on برای آن کاربر باشد. در حالی که صفات یک computer account ممکن است که شامل نام و مشخصات آن شئ باشد.
بعضی از اشیا ، که از آن‌ها به نام Container یاد مي‌شود ، خود دربردارنده اشیایی دیگرند. به عنوان مثال یک domain، خود یک container است که مي‌تواند شامل اشیایی مانند حساب کاربران و کامپیوترها باشد. در شکل 1 پوشه‌ي کاربران، یکcontainer بوده که دارای اشیای مربوط به حساب کاربران است.



شکل 1 : اشیا و صفات در Active Directory

اجزای Active Directory

برای ایجاد یک ساختار دایرکتوری، اجزای زیادی مورد نیاز است. این اجزا به دو دسته‌ي منطقی و فیزیکی تقسیم مي‌شوند.

❖ اجزای منطقی عبارتند از :

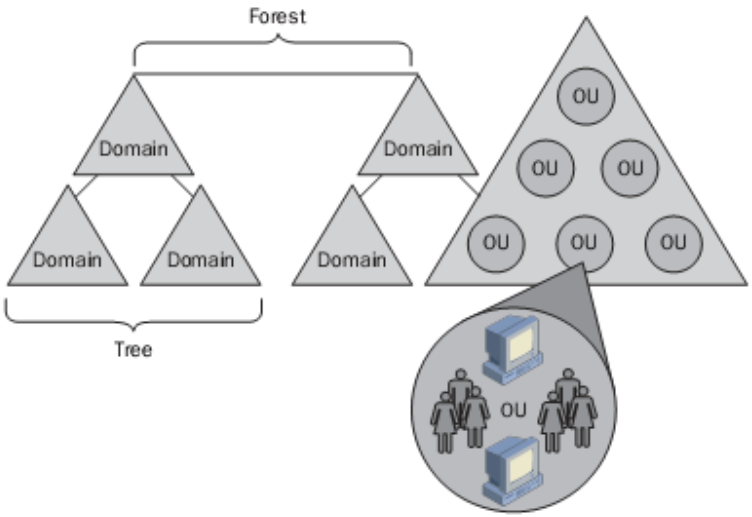
- دامنه‌ها (Domains)
- واحدهای سازمانی (Organizational Units)
- درخت‌ها (Trees)
- جنگل‌ها (Forests)

❖ اجزای فیزیکی که ساختار فیزیکی Active Directory را شکل مي‌دهند عبارتند از :

- سایت‌ها (Physical Subnets)
- Domain Controllerها (DC)

ساختار منطقی

در Active Directory، مي‌توان منابع را به صورت یک ساختار منطقی سازمان داد (ساختاری که منعکس کننده‌ي مدل‌هاي سازمانی باشد). گروه‌بندی منطقی منابع این امکان را فراهم مي‌آورد تا یک منبع با استفاده از نامش به سادگی پیدا شود و این امر ما را از یادآوری محل فیزیکی منبع بی‌نیاز مي‌سازد. در شکل 2 رابطه‌ي domainها، OUها، tree ها و forestها دیده مي‌شود.



شکل2 : رابطه میان اجزای منطقی Active Directory

حال به بررسی هر یک از اجزای منطقی در Active Directory به صورتی جداگانه مي‌پردازیم.

1. دامنه Domain

هسته‌ي اصلی ساختار منطقی در Active Directory، domain یا دامنه بوده که قادر به ذخیره‌ي میلیون‌ها شئ است. تمامي‌domainها در دو ویژگی زیر مشترکند.

- تمام اشیای شبکه در یک Domain قرار دارند و هر Domain اطلاعات مربوط به همان Domain را داراست.
- Domain یک محدوده‌ي امنیتی است. دسترسی به اشیای Domainها از طریق لیست‌هاي کنترل دسترسی یا ACL (Access Control List) میسر مي‌شود. ACLها شامل مجوزهایی هستند که مرتبط با اشیای مورد نظر است. این مجوزها بیان مي‌دارند که کدام یک از کاربران مي‌توانند به‌یک شی دسترسی داشته باشند و این دسترسی از چه نوع و در چه سطحی است. در خانواده‌ي Windows Server 2003، اشیا شامل فایل‌ها، پوشه‌ها، اشتراکات، چاپگرها و سایر اشیای Active Directory است. این نکته مي‌بایست در نظر گرفته شود که هیچ یک از تنظیمات و سیاست‌هاي امنیتی مانند اختیارات مدیریتی، سیاست‌هاي امنیتی و ACLها نمي‌توانند از یک Domain به Domain دیگر تغییر یابند. این امر بدان معنا است که‌یک مدیر در سطح یک Domain تنها دارای اختیاراتی است که وی را محدود به وضع سیاست‌ها در همان Domain مي‌کند.

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

چهار سطح عملیاتی دامنه وجود دارد:

- Windows 2000 mixed
- Windows 2000 native
- Windows 2003 interim
- Windows Server 2003

سطح عملیاتی "Windows 2000 mixed" به‌یک DC با سیستم عامل Windows Server 2003 اجازه مي‌دهد تا با سایر DCها در همان Domain که دارای سیستم عامل‌هاي Windows NT4 ، Windows 2000 و Windows server 2003 هستند ارتباط داشته باشند.

سطح عملیاتی "Windows 2000 native"، تنها امکان ارتباط DCهاي Windows 2003 با Windows 2000 را فراهم مي‌آورد.

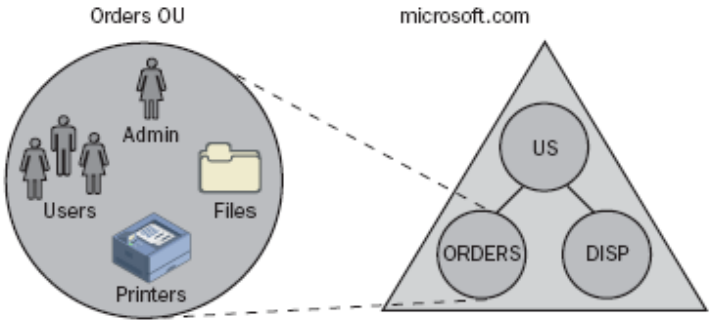
سطح عملیاتی "Windows 2003 interim" ارتباط DCهاي Windows Server 2003 با DCهاي NT4 را ممکن مي‌سازد.

سطح عملیاتی "Windows Server 2003" تنها DCهاي 2003 را با یکدیگر مرتبط مي‌سازد.

تنها در زمانی مي‌توان سطح عملیاتی یک Domain را بالا برد که تمامي‌Domain Controllerها در آن Domain نسخه‌هاي مناسبی از Windows را اجرا کنند. به عنوان نمونه اگر سطح عملیاتی Domain "Windows Server 2003" باشد، در این صورت مي‌بایست که تمامي‌DCها در این Domain دارای سیستم عامل windows server 2003 باشند.

2. Organization Units (OUs) واحدهای سازمانی

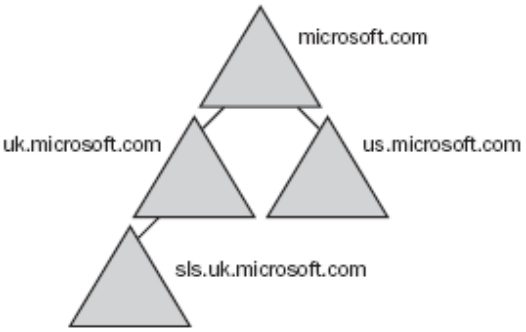
OU خود یک container بوده که اشیای یک دامنه (Domain) را در گروه‌هاي مدیریتی سازمان دهی مي‌کند. یک OU برای اعمال و اجرای وظایف مدیریتی (مانند مدیریت منابع و کاربران) به کار رفته و مي‌تواند شامل اشیایی مانند حساب‌هاي کاربران، گروه‌ها، کامپیوترها، چاپگرها، برنامه‌ها، فایل‌هاي به اشتراک گذاشته شده و حتی سایر OUها از همان domain باشد. ساختار سلسله مراتبی یک OU در یک domain مستقل از ساختار سلسله مراتبی OU در domainهاي دیگر است. مي‌توان با اضافه کردن یک OU در داخل OU دیگر (nesting)، مدیریتی سلسله مراتبی را سازمان داد. در شکل 3، domain با نام microsoft.com منعکس کننده‌ي سازمانی بوده که دارای سه OU است : US، Orders و Disp. Orders و Disp در واحد سازمانی US (OU) آشیانه‌اي شده‌اند.به صورت پیش‌فرض تمامي‌اشیای فرزند (OUهای Disp وOrder) مجوزهای خود را از والدین به ارث مي‌برند (US OU). ایجاد مجوز در سطوح بالاتر و استفاده از امکانات وراثت، وظایف مدیریتی را کاهش مي‌دهد.



شکل 3 : استفاده از OU برای به عهده گرفتن وظایف مدیریتی

3. درخت‌ها Trees

یک درخت(Tree)، سازمان دهی یا گروه‌بندی منطقی یک یا چند دامنه بوده که از طریق ایجاد یا اضافه کردن چند دامنه‌ي فرزند (Child Domain) به دامنه‌ي پدر (Parent Domain) فعلی به وجود مي‌آید. دامنه‌ها در یک درخت، دارای یک فضای اسمي(Contiguous Namespace) یا ساختار نامي سلسله مراتبی مشترک هستند. بر اساس استانداردهای DNS، نام یک دامنه‌ي فرزند، ترکیبی از نام خود دامنه‌ي فرزند به همراه نام دامنه‌ي پدر است. در شکل 4 Domain با نام microsoft.com به عنوان دامنه‌ي والد، و Domainهاي us.microsoft.com و uk.microsoft.com دامنه‌هاي فرزند آن هستند. علاوه بر آن خود دامنه‌ي uk.microsoft.com دارای یک دامنه‌ي فرزند با نام sls.uk.microsoft.com است (به روند دنباله‌وار نام دامنه‌ها دقت کنید).



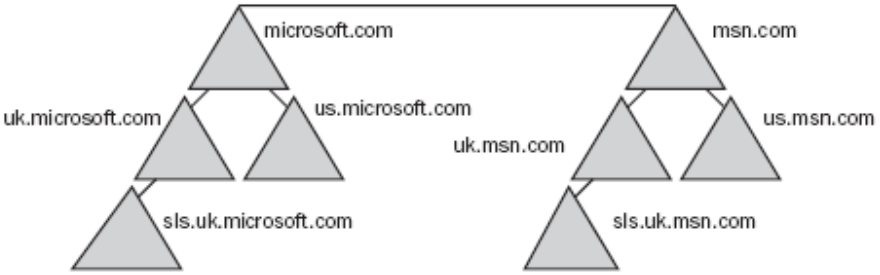
شکل 4 : A Domain Tree

4. جنگل‌ها Forests

یک جنگل (Forest) دسته‌بندی یا سازماندهی سلسله مراتبی از یک یا چند درخت (Domain Tree) کاملاً مستقل و مجزا از هم است. یک جنگل دارای ویژگی‌هایی است:

- درخت‌ها در یک جنگل با توجه به دامنه‌هایشان، دارای ساختار نامي‌متفاوت هستند.
- دامنه‌ها در یک جنگل به صورتی کاملاً مستقل از هم عمل مي‌کنند، ولی یک جنگل امکان ارتباط در تمامي‌سازمان را برقرار مي‌سازد.

در شکل 5 دو درخت microsoft.com و msn.com از یک جنگل دیده مي‌شوند. مي‌توان مشاهده کرد که فضای نامي‌در هر درخت دنباله‌وار است.



شکل5: A forest of Trees

سطح عملیاتی جنگل (Forest Functional Level)، ویژگی‌هاي خاصی را در سطح جنگل و در محیط شبکه فراهم مي‌آورد (Forest-wide Active Directory Features).

سه سطح دسترسی جنگل وجود دارد:

- Windows 2000 (پیش فرض)
- Windows 2003 interim
- Windows Server 2003

سطح عملیاتی "Windows 2000" به یک DC با سیستم عامل Windows Server 2003 اجازه مي‌دهد تا با سایر DCها در شبکه که دارای سیستم عامل‌هاي Windows NT4 ، Windows 2000 و Windows Server 2003 هستند ارتباط داشته باشد.

سطح عملیاتی "Windows 2003 interim" ارتباط DCهاي Windows Server 2003 با DCهاي ویندوز NT4 و ویندوز سرور 2003 را ممکن مي‌سازد.

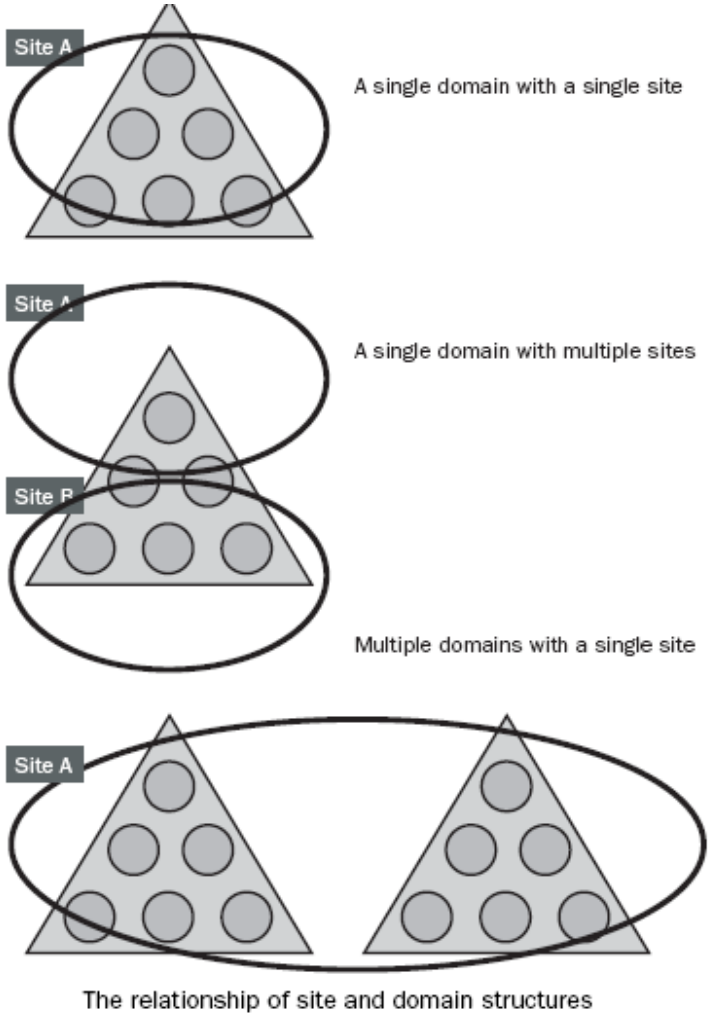
سطح عملیاتی "Windows Server 2003" تنها DCهای 2003 را با یکدیگر مرتبط مي‌سازد.

تنها در زمانی مي‌توان سطح عملیاتی یک Forest را بالا برد که تمامي‌Domain Controllerها در آن جنگل نسخه‌هاي مناسبی از Windows را اجرا کنند. به عنوان نمونه اگر سطح عملیاتی "Windows Domain Server 2003" باشد، در این صورت مي‌بایست که تمامي‌DCها در این جنگل دارای سیستم عامل windows server 2003 باشند.

ساختار فیزیکی

1. سایت‌ها (Sites)

یک سایت اجتماع یک یا چند زیر شبکه (Subnet) IP است که به وسیله‌ي یک اتصال فیزیکی مطمئن و سریع به هم مرتبط شده‌اند تا بتوان تا آنجا که ممکن است در جهت بهبود ترافیک شبکه اقدام کرد. سایت‌ها تنها شامل اشیای کامپیوتری و ارتباطی هستند که به منظور تنظیم چگونگی تکرار در سایت (Replication) به کار گرفته شده‌اند. همان گونه که در شکل 6 نشان داده شده است، یک دامنه مجزا مي‌تواند شامل یک یا بیش از یک سایت (از لحاظ جغرافیایی) باشد، و یک سایت مجزا مي‌تواند شامل حساب‌هاي کاربران و کامپیوترهایی باشد که متعلق به چندین دامنه هستند.



شکل 6 : رابطه بین سایت و دامنه

2. Domain Controller (DC)

یک Domain Controller کامپیوتری است که دارای سیستم عامل Windows Server باشد و یک نسخه از دایرکتوری دامنه (Local Domain Database) یا replica را در خود ذخیره کند. هر دامنه مي‌تواند بیش از یک Domain Controller داشته باشد. یک Domain Controller تنها مي‌تواند به‌یک دامنه سرویس دهد. یک DC

وظيفـه‌ي شنـاسـايی كـاربرانی را كـه تـلاش بـرای log on بـه دامنـه دارنـد، را بـر عهـده دارد. عـلاوه بـر آن سياست‌هاي امنيتی برای يک دامنه را نيز تنظيم و حفظ مي‌كند.

2— مقدمه (ادامه)

در ادامه‌ي مطالب بيان شده، در اين بخش با مفاهيم پايه در Active Directory آشنا مي‌شويم.

كلمات كليدی: تكرار يا Replication، Replica، Partition، Global Catalog، سياست‌هاي گروهـی يـا Group Policies، و ارتباطات مطمئن يا Trust Relationships

درک مفاهيم Active Directory

در خانواده‌ي ويـنـدوز سـرور 2003، بـا مفـاهيم جديـدی در ارتبـاط بـا Active Directory روبـرو مـي‌شـويم. ايـن مفاهيم شامل موارد زير است :

- تكرار (Replication)
- ارتباطات مطمئن (Trust Relationships)
- سياست‌هاي گروهی (Group Policies)

انعكاس يا Replication

كـاربران و سـرويس‌هـا مـي‌بايسـت در هـر زمـانی و از هـر كـامپيوتری در domain، بـه اطلاعـات دايركتـوری دسترسـی داشـته باشـند. انعكـاس *(Replication)* ايـن امـر را تضـمين مـي‌نمايـد كـه هـر تغييـری در يـک domain controller در سـاير DCهـا از همـان domain نيـز مـنعكس مـي‌شـود. اطلاعـات دايركتـوری در domain controllerهاي داخل و بين سايت‌ها تكرار مي‌شود.

چه اطلاعاتی تكرار مي‌شود ؟

آنچه كه در دايركتوری ذخيره مي‌شود (در فايل Ntds.dit) به صورت منطقی به چهار دسته تقسيم مي‌شود. به هر يک از اين دسته‌هاي اطلاعاتی، لفظ *directory partition* اطلاق مي‌گردد. يـک پارتيشـن دايركتـوری را با عنوان *متن نامي (naming* context) نيز مي‌شناسند. دايركتوری دارای پارتيشن‌هاي زير است:

■ **Schema Partition :** اين پارتيشن اشيايی را مشخص مـي‌سـازد كـه مـي‌تواننـد در دايركتـوری سـاخته شوند. علاوه بر آن، اين پارتيشن ويژگی‌ها و صفات اين اشيا را نيز مشخص مي‌سازد. اين اطلاعات و داده‌ها در كل يک forest مشترک بوده و در تمامي‌DCهاي موجود در يک forest تكرار مي‌شود.

■ **Configuration Partition :** اين پارتيشن ساختار منطقی چيدمان Active Directory را بيـان مـي‌دارد و شامل داده‌هايی درباره‌ي ساختار domain و يا توپولوژی تكرار است. اين داده‌ها نيـز در تمـامي‌domainهـاي موجود در يک forest مشترک بوده و در تمامي‌DCهاي موجود در آن جنگل تكرار مي‌شوند.

■ **Domain Partition :** این پارتیشن تمامي‌اشیای موجود در یک domain را تعریف مي‌کند. این داده‌ها و اطلاعات مخصوص به‌یک domain بوده و منحصر به فرد در همان domain است و بنابراین در دیگر domainهاي موجود در یک forest تکرار نخواهد شد.

■ **Application Directory Partition :** این پارتیشن شامل اطلاعات پویای کاربردی است. ذخیره‌ي این اطلاعات در این پارتیشن موجب کنترل حوزه‌ي تکرار و محل نسخه‌هاي تکرار (replica) مي‌گردد و این امر کوچکترین تأثیر نامطلوبی در کارائی شبکه را به دنبال نخواهد داشت. این پارتیشن مي‌تواند هر نوع شی را دارا باشد (به غیر از اشیای امنیتی که شامل کاربران گروه‌ها و کامپیوترها مي‌باشد.) بدین ترتیب داده مي‌تواند به صورتی مشخص به DCهایی هدایت شود که برای کارهای مدیریتی در نظر گرفته شده‌اند و این امر ترافیک غیر ضروری تکرار (Replication) را کاهش مي‌دهد.

یک Domain Controller موارد زیر را ذخیره کرده و تکرار مي‌نماید :

- داده‌ي موجود در schema partition در سطح forest
- داده‌ي موجود در configuration partition به تمامي‌domainها در سطح یک forest
- داده‌ي موجود در domain partition (تمامي‌اشیای دایرکتوری و مشخصات آن‌ها) برای همان domain. این داده‌ها در تمامي‌domain controllerهاي اضافی موجود در آن domain تکرار خواهد شد. به منظور یافتن بهینه‌ي اطلاعات ، بخشی از نسخه‌ي تکرار (replica) که شامل صفاتی از تمام اشیایی است که به صورتی دائمي‌در domain مورد استفاده قرار مي‌گیرند، در کاتالوگ سراسری (Global Catalog) نیز تکرار مي‌گردد. کاتالوگ سراسری محلی مرکزی برای نگهداری اطلاعات در مورد اشیا در یک درخت یا جنگل است.

یک global catalog اطلاعات زیر را ذخیره و تکرار مي‌نماید :

- داده‌هاي موجود در schema partition برای یک forest
- داده‌هاي موجود در configuration partition برای تمامي‌domainها در یک forest
- بخشی از replica که شامل صفاتی از تمام اشیای دایرکتوری است که معمولا در یک forest مورد استفاده قرار مي‌گیرند (این اطلاعات تنها بین Global Catalogها تکرار مي‌شود).
- تمامي‌replica که شامل کل صفات تمام اشیای دایرکتوری در domainهایی است که کاتالوگ سراسری در آن قرار دارد.

اطلاعات چگونه منعکس مي‌شود؟

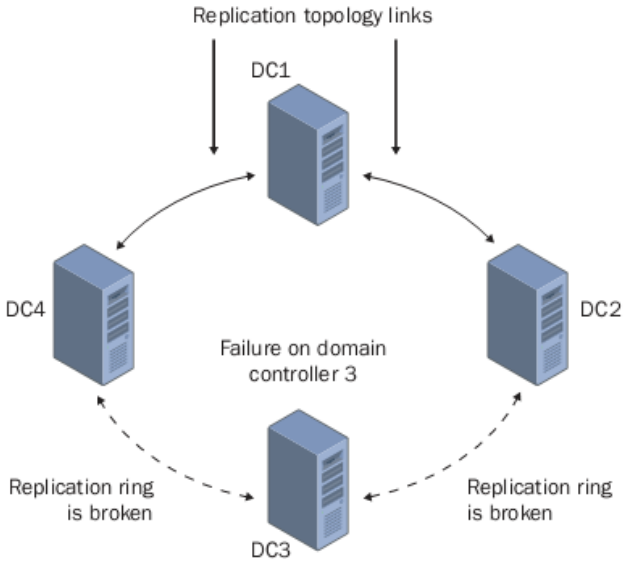
Active Directory اطلاعات را به دو صورت منعکس مي‌کند : intrasite (در داخل یک سایت) و intersite (بین سایت‌ها) .

انعکاس در داخل سایت (Intrasite Replication)

در داخل یک سایت، سرویسی از ویندوز سرور 2003 تحت عنوان Knowledge Consistency checker که به اختصار آن را KCC مي‌نامیم، به صورت خودکار یک توپولوژی برای تکرار در میان domain controllerها در همان دامنه و با استفاده از یک ساختار حلقه ایجاد مي‌کند. KCC یک پروسه‌ي خودکار است که در تمامي‌DCها اجرا مي‌شود. توپولوژی اعمال شده مسیری برای به روز رسانی‌هاي دایرکتوری فراهم مي‌آورد تا از یک DC به DC دیگر جریان یابد و این انتقال تا زمانی ادامه مي‌یابد که DCهاي موجود در یک

سایت به روزرسانی‌هاي دایرکتوری را دریافت نمایند . KCC تصمیم مي‌گیرد که کدام یک از سرورها برای انجام عمل انعکاس با یکدیگر مناسب‌تر هستند و سایر DCها را به عنوان شرکای انعکاس آن‌ها در نظر مي‌گیرد. این تصمیم‌گیری بر اساس مواردی چون نحوه‌ي اتصال، سابقه‌ي انعکاس موفق و بر مبنای تطابق با نسخه‌هاي انعکاس جزئی و یا کامل است. هر DC مي‌تواند بیش از یک شریک براي انعکاس داشته باشد. بعد از آن KCC اشیای ارتباطی را مي‌سازد که ارتباط میان شرکای انعکاس را نمایش خواهد داد.

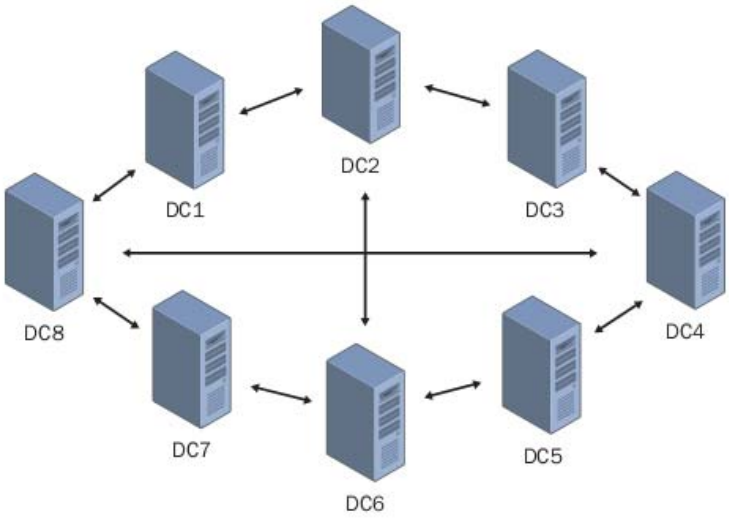
ساختار حلقه تضمین مي‌کند که حداقل دو مسیر انعکاس از یک DC به DC دیگر وجود دارد. به همین دلیل اگر یکی از DCها از کار بیفتد، عمل انعکاس (Replication) به سایر DCها ادامه خواهد یافت. شکل 7 توپولوژی انعکاس در داخل سایت را نشان مي‌دهد.



شکل 7 : Intrasite replication topology

KCC توپولوژی انعکاس در داخل سایت را هر پانزده دقیقه‌یکبار بررسی کرده و از کارکرد آن اطمینان حاصل مي‌کند. با اضافه‌یا خارج کردن یک DC از شبکه، KCC توپولوژی انعکاس را مجددا پیکربندی مي‌کند تا این تغییرات در آن منعکس شود.

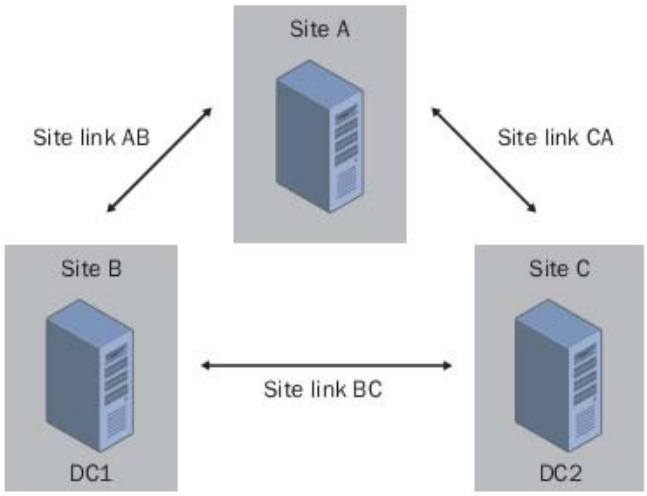
هنگامي‌که بیش از هفت Domain controller به‌یک سایت اضافه مي‌شوند، KCC اشیای ارتباط اضافی را در ساختار حلقه دخیل مي‌کند تا این اطمینان حاصل شود که اگر تغییری در هر یک از DCها ایجاد شود، هیچ یک از DCها بیش از سه Hop (گام) از DC دیگر فاصله نداشته باشند. این ارتباطات بهینه به صورت تصادفی ایجاد مي‌شوند و الزامي‌برای ساخت آنها در هر DC نیست. شکل 8 این مورد را نشان مي‌دهد.



A maximum of three replication hops between domain controllers, due to the addition of connection objects by the KCC

انعکاس**بین سایت‌ها (Intersite Replication)**

به منظور اطمینان از برقراری انعکاس میان سایت‌ها، مي‌بایست که سایت‌ها به صورت دستی و از طریق ایجاد اتصالات سایتی (Site Link) به هم مرتبط شوند. اتصالات سایتی ارتباطات شبکه را نشان داده و وقوع انعکاس را ممکن مي‌سازند. یک KCC مجزا در یک سایت تمامي‌ارتباطات میان سایت‌ها را برقرار مي‌سازد. این امر در شکل 9 نشان داده شده است.

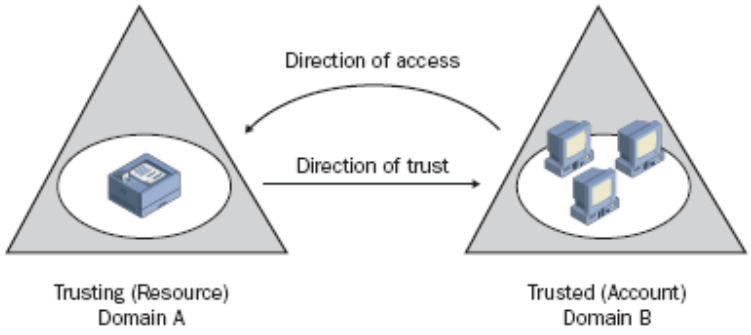


شکل 9: Intersite Replication Topology

رابطه اعتماد Trust Relationship

یک Trust، اتصالی میان دو دامنه است که در آن دامنه‌ي اعتماد کننده (trusting domain)، اطلاعات مربوط به دسترسی و شناسایی را از دامنه‌ي مورد اعتماد (trusted domain) کسب مي‌کند.دو دامنه وجود دارند

که موجب برقراری یک رابطه‌ي مطمئن و یا یک trust مي‌شوند: دامنه‌ي اعتماد کننده (trusting) و دامنه‌ي مورد اعتماد (trusted). دامنه‌ي اعتماد کننده دامنه‌اي است که منابع را در اختیار داشته و به سایر دامنه‌ها برای استفاده از این منابع اعتماد دارد. دامنه‌ي مورد اعتماد در حقیقت استفاده کننده از منابع است. این مسئله در شکل زیر بهتر نمود مي‌یابد.



Trusting and trusted domains linked with a one-way trust

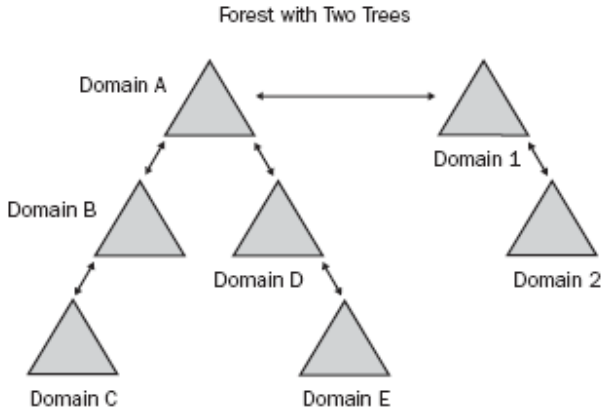
شکل 10: دامنه‌ي اطمینان کننده و دامنه‌ي مورد اعتماد قرار گرفته با یک اعتماد یک طرفه

trustها ویژگی‌هاي زیر را دارا هستند:

- **چگونگی ایجاد (Method of creation)**: trustها مي‌توانند به صورت صریح(explicitly) یا تلویحي (implicitly) ساخته شوند. هیچ trustی نمی‌تواند به هر دو صورت ساخته شود.
- **ترانهادگی (Transitivity)**: یک trust ترانهاده یعنی آنکه اگر Domain A به Domain B و Domain B به Domain C اعتماد یا trust دارد، آنگاه Domain A نیز به Domain C اعتماد مي‌کند. یک trust غیر ترانهاده یعنی آن که اگر Domain A به Domain B و Domain B به Domain C اعتماد یا trust دارد، بین Domain A و Domain C هیچ ارتباط مطمئن یا Trust برقرار نیست.
- **جهت (direction)**: trustها مي‌توانند یک طرفه(one-way) یا دو طرفه(two-way) باشند. در یک اعتماد یک طرفه Domain A به Domain B trust دارد. در یک trust دو طرفه اگر Domain A به Domain B اعتماد داشته باشد، آنگاه Domain B نیز به Domain A اعتماد دارد.
- ویندوز سرور 2003 از انواع trustهایی که در زیر آمده است پشتیبانی مي‌کند.
- Tree-root trust
- Parent-child trust
- Shortcut trust
- External trust
- Forest Trust
- Realm Trust

Parent-Child trust با ایجاد یک درخت و به صورت اتوماتیک میان تمامي‌دامنه‌هاي موجود در آن درخت به وجود مي‌آید. با اضافه شدن یک دامنه‌ي جدید به‌یک درخت، پروسه‌ي ایجاد اتوماتیک Trust صورت مي‌پذیرد. این نوع trust دو طرفه و ترانهاده است.

Tree-Root Trust نیز به صورت اتوماتیک و با اضافه شدن یک درخت به ساختار جنگل (a new root tree) برقرار مي‌شود شکل زیر این Trustها را نشان مي‌دهد. این نوع trust نیز دو طرفه و دارای خاصیت ترانهادگی است.



Domain structure showing tree-root and parent-child trusts

شکل 11: ساختار دامنه به همراه دو نوع Trust : parent-child و tree-root

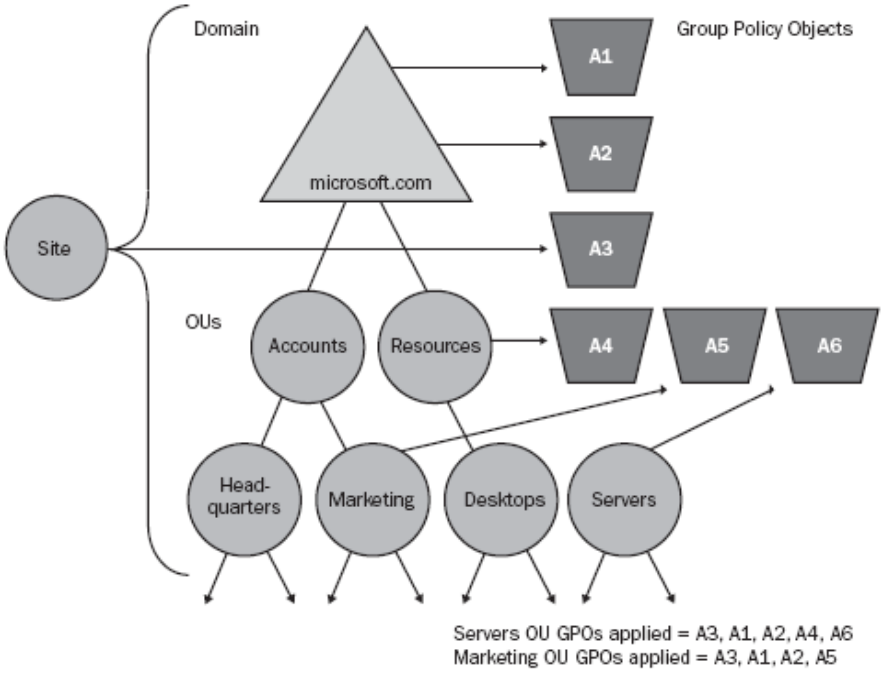
سیاست‌هاي گروهی (Group Policies)

سیاست‌هاي گروهی مجموعه‌اي از تنظیمات برای کاربران و کامپیوترهاست که مي‌تواند به کامپیوترها سایت‌ها، دامنه‌هاو OUها اعمال گردد تا بدین ترتیب عملکرد کاربران بهتر مشخص گردد. GPOها مجموعه‌اي از سیاست‌هاي گروهی تنظیم شده است. برای معلوم کردن تنظیمات desktop برای گروهی از کاربران مشخص، اشیای سیاست گروهی (Group Policy Objects or GPOs) ساخته مي‌شوند. هر کامپیوتر با سیستم عامل ویندوز دارای یک GPO داخلی بوده (Local GPO) و علاوه بر آن مي‌تواند با یک سری از سیاست‌هاي غیر محلی (مبتنی بر Active Directory) مرتبط گردد. GPOهاي غیر محلی بر GPO داخلی اولویت مي‌یابند. GPOهاي غیر محلی یا به کاربران (بدون در نظر گرفتن کامپیوتری که به آن Log on مي‌کنند) و یا به کامپیوترها (بدون در نظر گرفتن کاربری که به آن log on مي‌کنند) اعمال مي‌گردد و مربوط به اشیای خاص Active Directory (دامنه‌ها، سایت‌ها و OUها) است. این نوع از سیاست‌ها به صورت سلسله مراتبی و از گروه با کمترین محدودیت (Site) به گروه با بیشترین محدودیت (OU) اعمال مي‌شود. در حقیقت چگونگی و ترتیب اعمال به صورتی که در زیر آمده ، است:

1. **Local GPO:** هر سیستم عامل ویندوز تنها دارای یک سیاست گروهی است که به صورت محلی ذخیره شده است.
2. **GPOs linked to sites:** هر GPO که به‌یک سایت مرتبط باشد در مرحله‌ي بعد اعمال مي‌شود. این اعمال برای تمامي‌سیاست‌هاي مرتبط با یک سایت همزمان صورت مي‌گیرد و مدیر یک شبکه تعیین کننده‌ي ترتیب اعمال است.
3. **GPOs Linked to Domains:** اولویت اعمال این دسته از سیاست‌ها نسبت به دو مورد اول بیشتر است. اما اولویت اعمال چندین سیاست مربوط به‌یک دامنه را مدیر شبکه تعیین مي‌کند.

4. **GPOs linked to OUs:** GPOهایی که در بالای ساختار سلسله مراتبی یک OU قرار دارند زودتر اعمال مي‌شوند. پس از آن GPOهاي مربوط به OUهاي فرزند اعمال شده و در نهایت GPOهاي مربوط به OU شامل کاربران و کامپیوترها اعمال مي‌شود. در هر سطح از OU مي‌توان بیش از چند GPO را اعمال نمود (حتی مي‌توان هیچ GPO را اعمال نکرد).

شکل زیر چگونگی اعمال سیاست گروهی برای دو OU ی نمونه‌ي Server و marketing را نشان مي‌دهد.



مراجع :

- **Planning , Implementing and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure :** Jill Spealman, Kurt Hudson and Melissa Craft
- **Active Directory for Microsoft Windows Server 2003 :** Mike Mulcare , Stan Reimar
- **Microsoft Encyclopedia of Networking, Second Edition :** Mitch Tulloch , Ingrid Tulloch