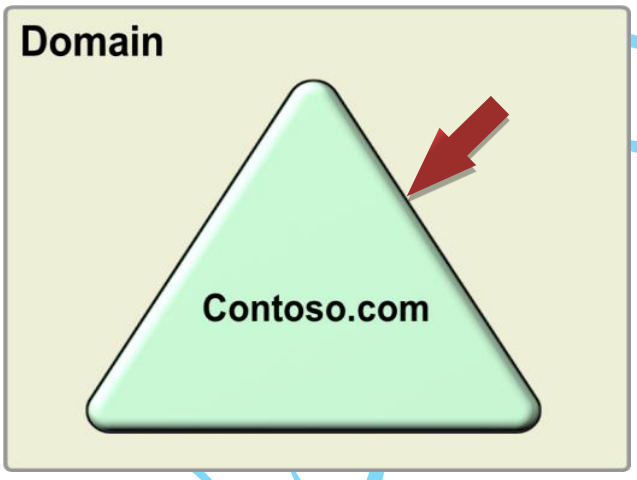
آشنایی با سازمان Active Directory

به طور کلی Active Directory یک DataBase مرکزی می‌باشد که حاوی اطلاعات موجود در شبکه Domain است این اطلاعات شامل اطلاعات کاربران – کامپیوترها و تنظیمات امنیتی می‌باشد.

توجه داشته باشید که برای نمایش شبکه‌های Domain به صورتی گرافیکی این نوع شبکه را با یک مثلث مشخص می‌نمایند که در شکل ۲-۱ می‌توانید مشاهده نمایید.



شکل ۲-۱

معرفی اجرای تشکیل‌دهنده ساختار Domain

مهمترین جز در راه‌اندازی یک شبکه Domain کامپیوتری می‌باشد که بتوانید Domain را برروی آن ایجاد نمایید. در اصطلاح به کامپیوتری که سرویس Active Directory برروی آن نصب می‌گردد DC یا Domain Controller گویند که در لغت به معنای کنترل‌کننده Domain می‌باشد. اجزای دیگری که یک شبکه Domain را تشکیل می‌دهند کامپیوترهایی می‌باشند که باید به DC متصل شوند و در داخل محدوده مدیریتی آن قرار گیرند. این گونه کامپیوترها در اصطلاح Member of Domain نامیده می‌شوند که به معنای عضوی از دامین می‌باشد.

قبل از راه‌اندازی شبکه‌ای از نوع دامین به تمام کامپیوترهای موجود Satnd alone گویند. منظور کامپیوترهایی می‌باشد که به تنهایی عمل می‌کنند و به یک شبکه دامین متصل نمی‌باشند.

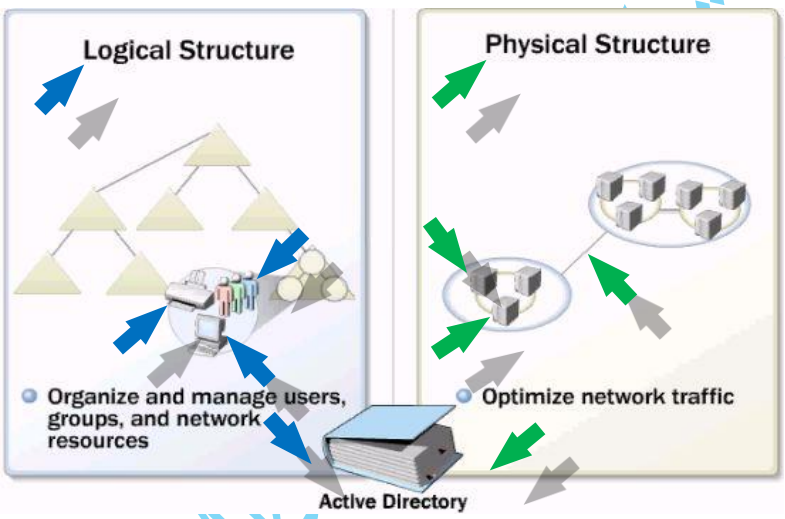
نویسنده: هادی مشکانی فراهانی
http://danesh-ac.ir
https://telegram.me/daneshacademy
https://www.instagram.com/daneshacademy

به پروسه و مراحل عضو کردن یک کامپیوتر با سیستم‌عامل ویندوزی مایکروسافت در شبکه Domain در اصطلاح Join to Domain گویند.

توجه داشته باشید که ساختار یک شبکه متشکل از دو بخش است که به شرح زیر می‌باشد:

- ساختار منطقی (Logical structure)
- ساختار فیزیکی (phsysicall)

در شکل ۲-۲ می‌توانید این ساختار را به صورت تفکیک شده مشاهده نمایید.



شکل ۲-۲

در این کتاب فقط با ساختار منطقی (Logical Structure) آشنا خواهیم شد.

Active Directory اطلاعات مرتبط به ساختار منطقی را در داخل DataBase خود نگهداری می‌نماید.

ساختار منطقی متشکل از مواردی به شرح زیر می‌باشد:

Domain

Object

Organization unit (OU)

Generic Container s

Tree & Forest

نویسنده: هادی مشکانی فراهانی

http://danesh-ac.ir

https://telegram.me/daneshacademy

https://www.instagram.com/daneshacademy

Domain Controller

Site and Subnets….

برای درک ساختار و سازمان Active Directory باید با موارد زیر آشنا لازم را داشته باشید.

قبل استفاده از ویندوز سرور نیاز به آشنایی با یک سری اصطلاحات می‌باشد که به شرح زیر است:

Object:

Object به‌عنوان اساسی‌ترین جز از ساختار منطقی Active Directory محسوب می‌گردد و ارائه کننده Userها و منابع موجود در شبکه می‌باشد.

هر آن چیزی را که در شبکه ایجاد می‌نمایید یک Object محسوب می‌گردد. نمونه Objectهایی که می‌توان ایجاد کرد به شرح زیر می‌باشد.

►User Account

ساده‌ترین Object در ساختار سلسله مراتبی Active Directory که قابل ایجاد کردن است را User گویند که دارای یک سری صفت خاص خود می‌باشد.

►Computer Account

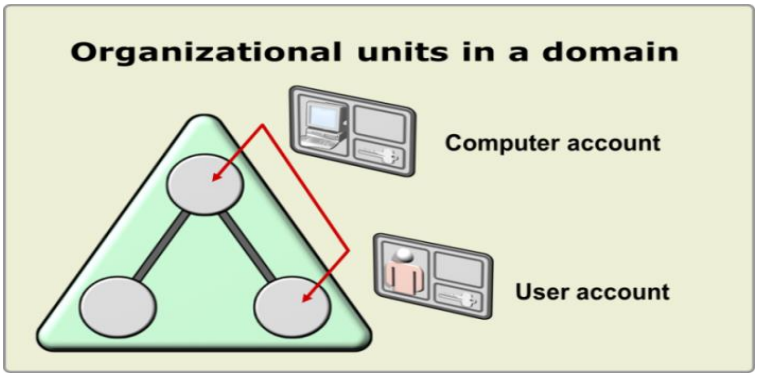
►Group Account

►Share Folder

در ساده‌ترین تعریف می‌توان این گونه بیان نمود که پوشه‌ای می‌باشد که اطلاعات آن توسط یکی از کاربران در شبکه برای قابل دسترس بودن دیگر کاربران برروی یک از کامپیوترها به اشتراک گذاشته می‌شود.

►OU(Organization Units)

در واقع نگه دارنده Objectهای موجود در شبکه و سازماندهی نمودن آنها را برعهده دارد که به آن OU گویند که در شکل ۲-۳ مشاهده می‌نمایید.



شکل ۲-۳

در شکل مشاهده می‌نمایید که یک Domain به OUهای مختلف تقسیم‌بندی شده است و Objectهای مربوط به هر یک را در داخل همان OU قرار داده شده است. تقسیم‌بندی Objectها در داخل OU باعث می‌شود مدیریت بهتری در سطح شبکه داشته باشید.

توسط OU می توانید Computerها و Userهایی که نیازمندی‌های مشترکی را دارند را دسته‌بندی کرده و مدیریت هر OU را به مدیر همان بخش واگذار کرده تا تنظیمات مختص به آنها را اعمال نماید.

توجه داشته باشید که OU دارای چندین سطح مختلف می‌باشد که به شرح زیر است:

۱. Parent OU یا First Level

۲. Child OU یا Second Level

علاوه بر این یک OU می‌تواند در زیر شاخه خود چندین OU دیگری را داشته باشد که به در این حالت بـه OUهایی که در زیر شاخه یک OU ایجاد می‌شوند Leaf Object گویند.

►printer

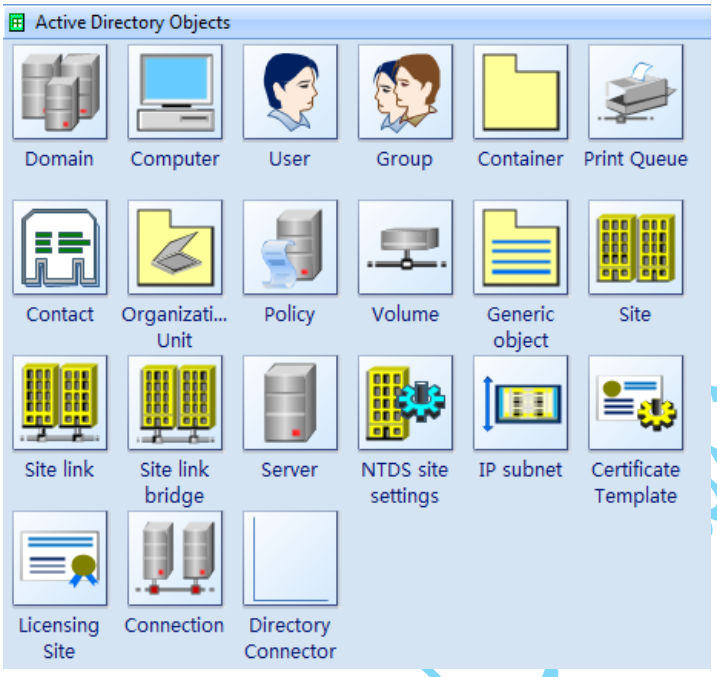
در شکل ۲-۴ می‌توانید نمونه‌ای از Objectها را به‌صورت گرافیکی مشاهده نمایید.

نویسنده: هادی مشکانی فراهانی

http://danesh-ac.ir

https://telegram.me/daneshacademy

https://www.instagram.com/daneshacademy



شکل ۲-۴

GUID:

Globally Unique Identifier (GUID) یک شناسه 128 bit می‌باشد که در ساختار Active Directory به هر Object داده می‌شود. این GUID در ساختار هر Forest انحصاری می‌باشد و ساختارش به‌صورت در مبنای hex به‌صورت xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx می‌باشد به‌طور مثال e99e82d5-deed-11d2-b15c-00c04f5cb503 یک GUID در ساختار اکتیو می‌باشد.

زمانی‌که شما یک Object را از ساختار Active Directory حذف می‌نمایید در پشت پرده GUID اختصاص داده شده به آن حذف می‌شود. توجه نمایید تمامی تنظیماتی که در ساختار Active Directory به هر Object اعمال می‌نمایید براساس GUID آن بر او اعمال می‌شود. بر همین اساس توصیه می‌شود که یک Object همانند User را تاحد امکان Disable نمایید. چنانچه شما این Object را پاک نمایید و مجدداً یک Object با همان مشخصات ایجاد نمایید دیگر GUID که از قبل به این Object داده شده است تغییر می‌کند.

Attribute:

توجه داشته باشید که هر Object توسط یک سری صفات و مقادیر که به آنها Attribute می‌گویند ایجاد می‌گردد. به طور مثال در زمان ایجاد یک Object همانند User باید اطلاعات و مقادیری به شرح زیر برای آن تعریف نمایید.

Firest Name

Last Name

Department

Account Expires

توجه داشته باشید که هر Object با توجه به Object Classesهای مختص به خود ایجاد می‌گردد.

در شبکه‌های Domain برای هر Object می‌توانید تعداد بسیار زیادی مشخصه تعریف نمایید و مزیتی که این کار برای شما دارد این است که در DataBase موجود در Active Directory می‌توانید یک Object را توسط مشخصه‌های آن جستجو کنید.

Object Classes

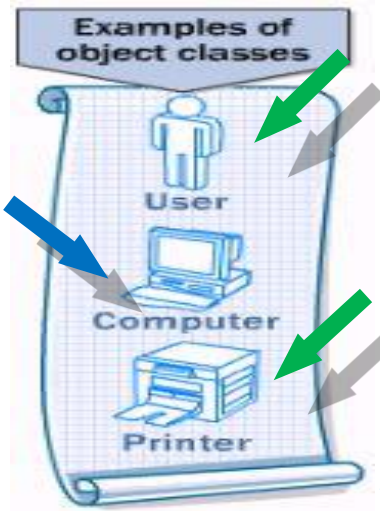
توجه داشته باشید که Object Classesها مشخص‌کننده نوع Objectهایی می‌باشد که می‌توانید در ساختار منطقی ایجاد و تعریف نمایید. در شکل ۲-۵ می‌توانید نمونه‌ای از Object Classesها را که به صورت پیش‌فرض در درون ساختار Active Directory قرار دارد مشاهده نمایید.

نویسنده: هادی مشکانی فراهانی

http://danesh-ac.ir

https://telegram.me/daneshacademy

https://www.instagram.com/daneshacademy



شکل ۲-۵

به این نکته توجه داشته باشید که باید برای ایجاد هر Object باید یک الگو در ساختار Active Directory برای آن کاربر در نظر گرفته شده باشد.

تعریف Schema

Schema به‌عنوان بانک Objectها در ساختار Active Directory محسوب می‌شود بر همین اساس هر Object که در Active Directory ایجاد می‌شود از نمونه موجود در بانک Active Directory که schema است استفاده می‌کند. برای درک بهتر این تعریف به مثال زیر توجه کنید.

در صورتی‌که شما بازی‌های استراتژیک را انجام داده باشید در طول بازی برای استفاده از هر موردی فقط یک نمونه برای شما قابل انتخاب است. به طور مثال برای تولید سرباز فقط برروی آیکون آن کلیک می‌نمایید به صورت خودکار در قبال هر یک بار کلیک برای شما یک سرباز ایجاد می‌گردد schema در ساختار Active Directory به همین ترتیب می‌باشد.

Schema در هر یک از Domain Controllerهای مایکروسافت دارای یک ورژن خاص خود می‌باشد که در ادامه اشاره شده است. اما هرچه این ورژن بالاتر باشید تعداد Objectهای بیشتری را برای ایجاد کردن در اختیار شما قرار می‌دهد.

Version 13 <-- Windows 2000 Server

نویسنده: هادی مشکانی فراهانی

Version 30 <-- Windows Server 2003 RTM, Windows Server 2003 Service Pack 1, Windows Server 2003 Service Pack 2

Version 31 <-- Windows Server 2003 R2 RTM, Windows Server 2003 R2 Service Pack 2

Version 44 <-- Windows Server 2008 RTM, Windows Server 2008 Service Pack 2

Version 47 <-- Windows Server 2008 R2 RTM, Windows Server 2008 R2 Service Pack 1

زمانی‌که شما یک Object همانند User را ایجاد می‌نمایید وظیفه ایجاد و قرار دادن این Object در ساختار سلسله مراتبی Active Directory توسط پروتکل LDAP صورت می‌پذیرد. در صورتی‌که پروتکل LDAP در ساختار Active Directory نباشد مدیریت Objectها در این ساختار بدون معنا می‌باشد.

معرفی Active Directory Schema

Schema مشخص‌کننده این می‌باشد که Objectها در داخل Active Directory به چه صورت و فرمتی نگه‌داری شوند و دارای چه خواص و Attributeهایی باشند. به بیان ساده‌تر در ساختار Active Directory به مجموعه Objectها و Attributeها Active Directory Schema گفته می‌شود.

به این نکته توجه نمایید که Active Directory برای نامگذاری Objectها از سرویس DNS استفاده می‌کند.

DC (Domain Controller):

به کامپیوتری گفته می‌شود که اول از هر چیز یک سیستم‌عامل از خانواده سرور برروی آن نصب و سرویس Active Directory برروی آن فعال شده باشد و وظیفه نگهداری از DataBase مختص به Active Directory را برعهده دارد. DC وظیفه ذخیره اطلاعات و انجام Replication را برعهده دارد.

هر Domain Controller تنها می‌تواند در داخل یک Domain انجام وظیفه نماید. به این نکته هم توجه داشته باشید برای اینکه DC در تمام شرایط در دسترس باشد معمولاً برای Doman تعداد دو Damain Controller ایجاد می‌گردد تا در صورت از کار افتادن یک Domain Controller دیگری جایگزین شود.

Active Directory (NTDS Folder):

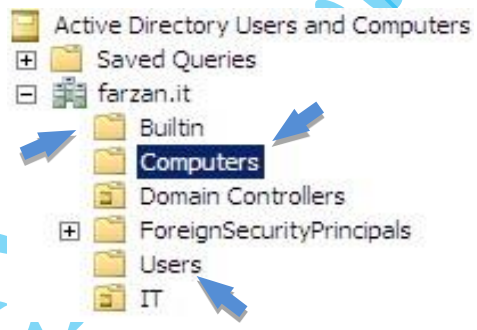
فایلی است که برروی سرور نصب شده و DataBase شبکه Domain در آن قرار دارد این سرویس را با نام NTDS مطرح می‌کنند. در واقع NTDS نام فولدری است که سرویس Active Directory در آن نصب می‌شود.

Generic Container:

Container در لغت به ظرف و جای نگه‌دارنده اطلاق می‌گردد و در ساختار شبکه از Container برای نگه داری یکسری از Objectهای پیش‌فرض در داخل Active Directory استفاده می‌گردد، نکته مهم در رابطه با یک Container به عدم توانایی قرار دادن Group Policy برروی آن بر می‌گردد به این ترتیب که Containerها قابلیت‌های بالایی همچون OUها را ندارد و بسیار محدود می‌باشند.

در هر حال امکان ساختن مجدد یک Container در داخل Active Directory نیز وجود ندارد و به جای آن می‌توانید به صورت دلخواه اقدام به ساختن OU نماید. علاوه بر این باید توجه داشته باشید که این Generic Containerها غیرقابل پاک کردن و تغییر نام هستند.

در شکل ۲-۶ می‌توانید نمایی از Containerهای پیش‌فرض را مشاهده نمایید.



شکل ۲-۶

در شکل فوق سه Container مشخص شده است که کاربرد هر یک به شرح زیر می‌باشد.

Computers Container محل پیش‌فرض ذخیره کامپیوترهایی می‌باشد که Join to Domain شده‌اند.

Users Container به صورت پیش‌فرض محل نگه‌داری از Users هایی می‌باشد که در DataBase مربوط به شبکه Domain تعریف می‌گردند.

Tree:

به مجموعه سلسله مراتبی یک Domain به همراه خانواده زیر مجموعه آن یک Tree گویند.

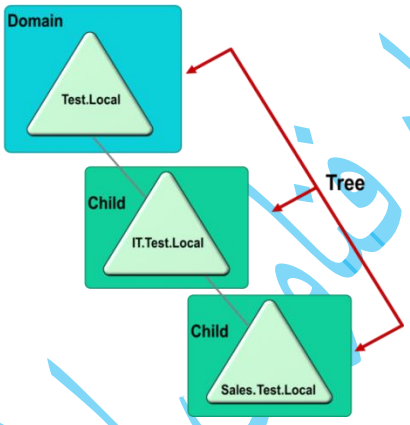
اما در ادامه تعاریف پیشرفته‌تری در مورد این اصطلاح بیان شده است.

نویسنده: هادی مشکانی فراهانی

به مجموعه یک یا چندین Domain که زیر نظر یک ساختار Domain Name یا DNS Name قرار دارند و بین آنها یک ارتباط منطقی یا Trust به صورت دو طرفه برقرار است و Schema آنها یکسان است و نقش Global Catalog در آنها یکسان است Tree گویند.

به عبارت دیگر می‌توان این گونه تعریف نمود چنانچه Domainهای موجود که با یکدیگر دارای ارتباط Trust (قابل اعتماد) برقرار می‌نمایند و در یک ساختار درختی در کنار یکدیگر قرار گیرند اصطلاحاً یک Tree یا ساختار درختی را ایجاد می‌نمایند.

در شکل ۲-۷ می‌توانید نمونه‌ای از ساختار یک Tree را مشاهده نمایید.



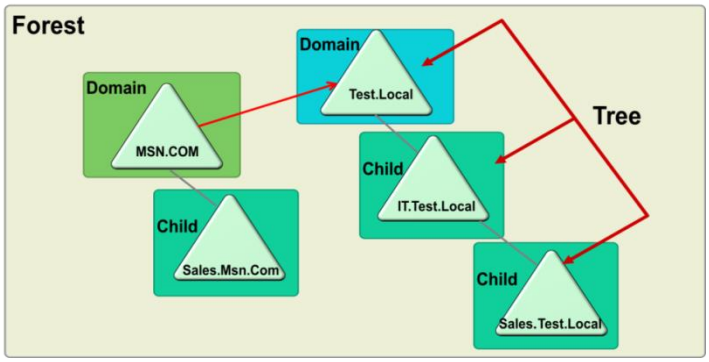
شکل ۲-۷

همان‌طور که در شکل مشاهده می‌نمایید چنانچه Domain دوم به DC اول متصل شود به DC دوم Child Domain گویند و به DC اول که Child Domain به آن متصل است Parent Domain یا دامین والد گویند.

برای تشکیل یک Child Domain نام Child Domain با نام Parent Domain ترکیب می‌گردد و یکDNS Name را تشکیل می‌دهد. نحوه ایجاد DNS Name را در شکل بالا مشاهده می‌نمایید.

Forest:

هایی را برعهده Tree گفته می‌شود و وظیفه برقراری ارتباط بین Domain Treeاین اصطلاح به مجموعه آنها متفاوت است. در شکل ۲-۸ می‌توانید این ساختار را مشاهده نمایید.Domain Name Spaceدارد که



شکل ۲-۸

اولین DC که درون یک Forest قرار می‌گیرد با عنوان Forest Root Domain معرفی می‌گردد و نام آن به‌عنوان نام کلی Forest محسوب می‌شود. یک Forest حاوی تمامی اجزای تشکیل‌دهنده Active Directory می‌باشد و به طور پیش‌فرض اطلاعات در محدوده همان Forest تبادل (Replicate) می‌گردد.

Forest Root Domain یک Top Level Domain می‌باشد و به اولین Domain تحت Active Directory گفته می‌شود.

Tree Root Domain بالاترین Level یک Domain تحت یک Tree می‌باشد.

Site:

یک اصطلاح فیزیکی می‌باشد مربوط به ایجاد چندین Subnet متفاوت از لحاظ IP Address که در یک Domain یا یک Forest قرار داشته باشند به صورتی‌که بین این siteها پهنای باند متفاوتی وجود داشته باشد.

Subnet:

به تعدادی از کامپیوترها که دارای یک NET ID مشترکی هستند و در یک کلاس IP قرار دارند Subnet گویند.

با توجه به تعریف Site وSubnet باید بدنید که از این دو برای تبادل اطلاعات Active Directory استفاده می‌شود بین یک یا چندین Location متفاوت. علاوه‌بر این به اصطلاح دیگری به نام Site Link وجود دارد که به ارتباط بین دو Site گفته می‌شود که اجازه Replication را صادر می‌کند.

نویسنده: هادی مشکانی فراهانی

نکته قابل توجه این می‌باشد که Site از ساختار Domain متفاوت می‌باشد به این علت که Domain یک ساختار منطقی را فراهم می‌کند در حالی که Site یک ساختار فیزیکی می‌باشد.

Group Policy Object (GPO)

برای مشخص‌کردن چگونگی کارکرد Objectها در دامین و مدیریت آنها نیاز به ارائه سیاست‌هایی است که اصطلاحاً مجموعه این سیاست‌ها در ابزاری به‌نام Group Policy تعریف می‌گردد، از وظایف یک مدیر شبکه طراحی و اعمال Group Policy برای کامپیوترها و کاربران دامین می‌باشد.

حتی می‌توان به این صورت تعریف نمود:

با استفاده از Group Plolicy می‌توان محیط کاری کاربران را تنظیم و تغییرات را برروی کامپیوترهای آنها اعمال نمایید. با استفاده از این ابزار مدیر شبکه قادر است یک سیاست امنیتی یا Policy را طراحی و آن را برای تمامی کامپیوترهای شبکه اعمال نماید.

به طور کلی در Group Policy می‌توان تنظیمات و سیاست‌های امنیتی را به دو روش اعمال نمود.

◄ کامپیوترها (Computer Setting)

◄ کاربران (User Setting)

چنانچه یک Policy برروی یک کامپیوتری اعمال نمایید، بدون توجه به اینکه چه کاربری با چه مجوزی به آن کامپیوتر Login می‌نماید این Policy برای این کاربر اعمال می‌گردد.

همچنین با اعمال یک Policy به یک کاربر خاص این Policy بدون توجه به این که این کاربر خاص با کدام یک از کامپیوترهای عضو، به شبکه Login نماید این Policy برای آن اعمال می‌گردد.

علاوه بر این موارد باید توجه داشته باشید که در داخل Active Directory DataBase یک فایل وجود دارد به نام NTDS.dit که یک DataBase فیزیکی محسوب می‌شود که شامل تمامی شامل تمامی اطلاعات Directory می‌باشد.

این فایل به طور کلی شامل سه بخش در داخل خود می‌باشد که به شرح ذیل می‌باشد.

1-Data Table

این بخش حاوی اطلاعاتی کامل و جامع در خصوص Active Directory می‌باشد

نویسنده: هادی مشکانی فراهانی

http://danesh-ac.ir

https://telegram.me/daneshacademy

https://www.instagram.com/daneshacademy

Domain Controller از چندین بخش تشکیل شده است که به شرح زیر می‌باشد:

Domain partition:

این پارتیشن حاوی اطلاعات موجود در خصوص Object موجود در Domain می‌باشد. توجه داشته باشید که اطلاعات این پارتیشن بین DCهای درون همان Domain موجود Replicate می‌شود.

Configuration partition:

در این پارتیشن اطلاعات مربوط به کل ساختار Forest و Domainهای موجود در آن و نوع رابطه آنها را در درون خود ذخیره می‌نماید. اطلاعات موجود در این بخش بین تمامی DCهای موجود در بین یک Forest تبادل Replicate می‌گردد.

Schema partition:

در این بخش اطلاعات مربوط به Schema و ساختار Active Directory را درون خود ذخیره می‌کند. اطلاعات این بخش نیز در درون کل Forest بین DCها تبادل می‌گردد.

Application partition:

این بخش یک قسمت اضافه می‌باشد که حاوی اطلاعاتی به‌جز اطلاعات امنیتی و Security می‌باشد و توسط یک یا چند برنامه کاربردی مورد استفاده قرار می‌گیرد. اطلاعات این قسمت فقط بین DCهای خاصی درون Forest تبادل می‌گردد.

با توجه به مطالب مطرح شده از ساختار منطقی این تعریف کلی به‌دست می‌آید که به جهت سازماندهی و مدیریت کاربران، گروه‌ها و منابع به اشتراک گذاشته شده مورد استفاده قرار می‌گیرد.

توجه نمایید که آشنایی با ساختار فیزیکی Physical مربوط به کتاب طراحی زیر ساخت شبکه می‌باشد.

نویسنده: هادی مشکانی فراهانی