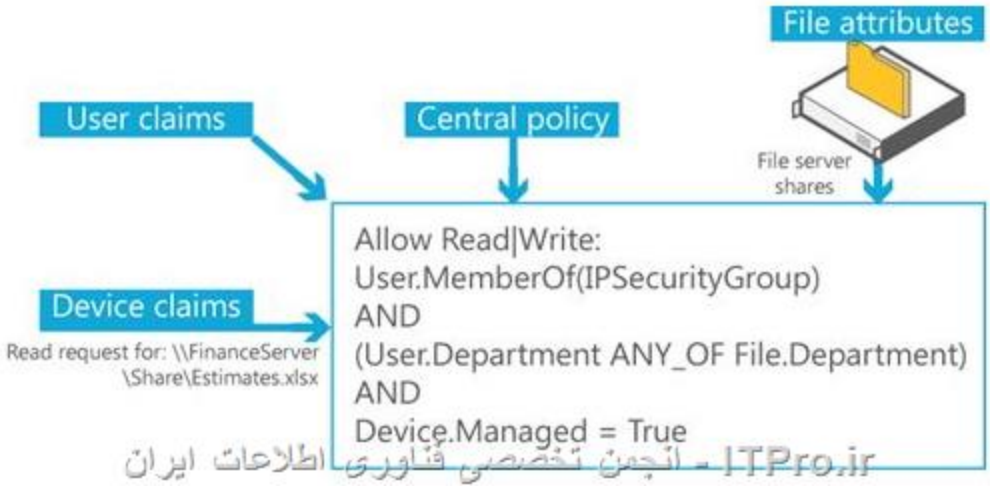
آموزش تخصصی DAC

با آموزش تخصصی DAC در سرور 2012 R2 در خدمت شما هستیم . همانطور که میدانید مدت بسیار زیادیست که به کمک ساختار فایل سیستم NTFS و استفاده از ACL انواع سطوح دسترسی و کنترلی برای استفاده از فایل ها و فولدر ها وجود دارد و پای ثابت کانفیگ ها در شبکه های کامپیوتری مخصوصا شبکه های مایکروسافتی همین ساختار ها و کانفیگ ها بوده است . در سایت آیتی پرو نیز آموزش های بسیار مناسب و کاملی برای راه اندازی و پیاده سازی این ویژگی که معروف به اعمال Permission برای فایل و فولدر ویا استفاده از قابلیت های تب security و Sharing است ، وجود دارد که به سادگی از اینجا می توانید به آنها دسترسی پیدا کنید . اما آموزشی که اکنون پیش روی شماست پا را فراتر قرار داده و قرار است تنظیمات و امکاناتی را در اختیار شما قرار دهد که بتوانی پیچیده ترین سناریو ها را برای اعمال سطوح دسترسی به کار بگیرید و در سرور 2012 از آن استفاده کنید .

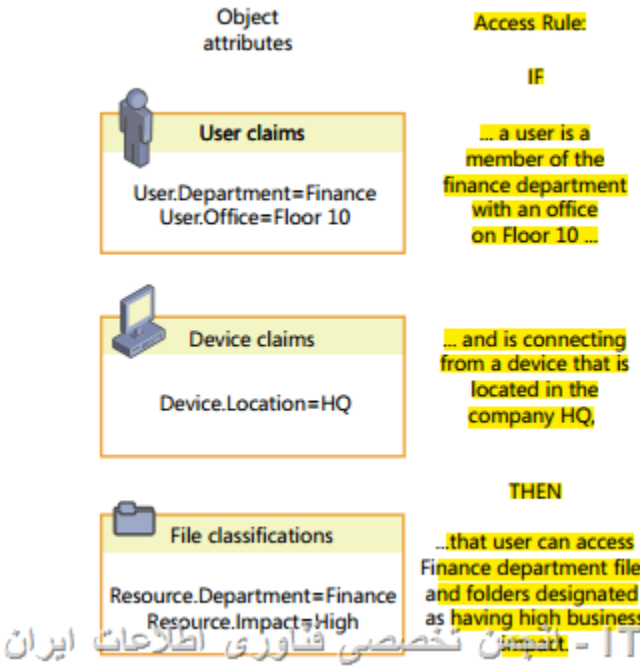
در ابتدا بهتر است کمی بیشتر با این سرویس آشنا شویم و نحوه عملکرد آن را بررسی کنیم . اگر با ساختار های اعمال Permission بر روی فایل ها و فولدر ها آنا باشید می دانید که ما می توانیم بر اساس کاربر و یا گروه کاربری برای فایل ها و فولدر های خود انواع سطوح دسترسی یا همان permission را اعمال کنیم و به طبع هر کابر با توجه به دسترسی که برای آن مشخص شده می تواند از آن فایل ها و فولدر ها استفاده کند . اکنون شرایطی را فرض کنید که شما برای یک مجموعه بسیار بزرگ و انواع گروه های کاری بخواهید این دسترسی ها را بر روی فایل سرور ها و منابع کاری خود اعمال کنید ، مسلما نیاز هست تا ابتدا به ساکن دسته بندی های خود را برای فایل های مورد نظر انجام دهید و سپس با توجه به سیاست ها و پالیسی های تنظیم شده بر روی این فولدر ها یا دیتا بیس ها کاربران مورد نظر را معرفی کنید و دسترسی ها را اعمال کنید . قطعا تا اینجای کار برای شما بسیار تکراری و شاید خسته کننده باشد ! اما خب باید کمی تحمل کنید تا به جاهای جالبش هم برسیم ! قطعا شما با تعریف گروه های کاربری میتوانید پیاده سازی خودتان را سرعت ببخشید و عملا کاری کنید که با عضو کردن یک کاربر در گروه مورد نظر و قرار دادن آن گروه در DACL یا همان لیست مجوزها بر روی یک فایل یا فولدر ، دسترسی های مورد نظر را به آن گروه و در اعضای ان اعمال کنید.شاید از خودتان سوال کنید که پس کاربر DAC در کجای این داستان است ؟ درست است که به کمک استفاده از گروه ها سرعت و دسته بندی مناسبی در اختیار ادمین های عزیز قرار گرفته اما اگر راه حل هایی راحت تر و کاملتری نیز وجود داشته باشد قطعا ایده آل تر خواهد بود .

اکنون به کمک ساختار های Dynamic Access Control ها یا همان DAC می توان به کمک استفاده از انواع Cliam ها و همینطور Classification ها شرایطی بسیار جالبی به وجود آوریم ! شاید بپرسید خب Claimچیست ؟ Classification چی میگه؟؟ یعنی الان باید ناپلئونی ره بیاریم ؟؟ !!



ببینید برای ساده تر شدن درک استفاده از DAC یک مثال را با یکدیگر بررسی میکنیم که به کمک ساختار DACبه سادگی قابل پیاده سازیست ! فرض کنید که قرار است هر کاربری که ساخته میشود و Attribute مربوط به JOB Title آن معادل Finance است بر روی فایل سروری که دارای اطلاعات مالی و حسابداریست دسترسی Read & Write داشته باشد و کاربران که مقدار Attribute مربوط به Job Title آنها معادل مثلا R&D است بر روی فایل هایی که دارای اطلاعات مالی و حسابداری هستند دسترسی خواندن یا همان Readهم نداشته باشد ! در عین حال مدیران مالی بر روی تمامی این فایل های مالی دسترسی Modify داشته باشند و این تنظیمات به صورت متمرکز و برای تمامی فایل سرور ها مجموعه قابل استفاده باشه ! در این سناریو عملا نیازی به ساختن گروه های کاری متفاوت نیست و صرفا به کمک Attribute مربوط به job Titleو ماهیت فایل های استفاده شده می توان سطوح دسترسی را ایجاد کرد و و اگر نیازی به تغییردراین متد باشد به صورت متمرکز و از یک جا این قابل انجام است .

برای آشنایی بیشتر بهتر است به این سناریو نیز یک نگاه کلی بندازید و توضیحات را با یکدیگر بررسی کنیم :



در این سناریو دسترسی به فایل های مورد نظر به شرطی قابل انجام است که کاربر مورد نظر عضو دپارتمان Financeو در طبقه دهم حضور داشته باشد) البته این Attribute ها باید برای اکانت مورد نظر از قبل پر شده باشد ، برای مثال موقع ساختن کاربر باید ذکر شود که قرار است در گروه Finance باشد یا اینکه در طبقه 10 حضور خواهد داشت (و از کامپیوتری استفاده کند که در Attribute آن کامپیوتر Location به صورت HQ (دفتر مرکزی) معرفی شده باشد یعنی آن سیستم در شعبه مرکزیست و در صورتی که فایل های مورد نظر دارای مشخصات متعلق به گروه Finance و دارای اهمیت و درجه اطلاعاتی High باشد در این صورت قابل دسترس است !! شاید هم اکنون این توضیحات و این سناریو کمی گیج کننده یا گنگ باشد اما مطمئن باشید در مجموعه اموزشی پیشرو به صورت قدم به قدم تمامی موارد را با یکدیگر بررسی خواهیم کرد و تمامی زوایای موجود در آن را به دقت انجام خواهیم داد و آن وقت خواهید دید که این سناریو و امثال آن به سادگی قابل پیاده سازی هستند !!

در واقع مقصود از Claim همان Attribute هایی است که در اکانت User و یا Computer به سادگی قابل تعریف و تغییر است شما میتوانید به کمک همین Claim ها و نوشتن Access Rule ها به اعمال دسترسی بر اساس Attribute ها و مقادیر ان بپردازید و با این کار در واقع یکجور سطح دسترسی شناور) !!! خدایی این اصطلاح باید به نام خودم ثبت کنم ، جایی هنوز مطرح نشده (D: !! ایجاد کنید . حال اگر قرار است دسترسی را به یک کاربر بدهید و یا دسترسی را از وی بگیرید دیگری نیازی به عضویت در گروه ها را تغییر دهید یا اینکه پرمیشن ها را بر روی یک فایل سرور عوض کنید ! نخواهد بود بلکه پرمیشن های مورد نظر به

صورت خودکار بروی فایل هایی که مثلا دارای محاسبات مالی هستند اعمال میشود و شما از اعمال خودکار دسترسی بر اساس Claim نهایت استفاده را خواهید برد .
در یک جمع بندی کلی میتوان مزیت های DAC را بدین صورت بررسی کرد

- مدیریت مرکزی تمامی فایل سرورها و فایل سرویس ها به طور واحد و متمرکز) استفاده از Access Ruleو اعمال آنها از طریق Group Policy به صورت متمرکز(
- کاهش چشم گیر در ساخت گروه های کاربری و سیستمی و همینطور سطوح مختلف عضویت جهت اعمال سیاست های دسترسی و کنترلی
- ساخت Access Rule ها بر اساس مدیریت مرکزی و بسیار طبقه بندی شده برای کنترل دسترسی ها آن هم به طور متمرکز و بسیار منعطف

در واقع شما بجای استفاده منحصری از ACL بر مبنای کاربران و گروه ها ، می توانید از انواع Rule ها براساس Loaction , Office,Country ,region,Telephone Number و یا خیلی موارد دیگر در کنار ACLها استفاده کنید و یک مجوعه بسیار دقیق و البته منعطف از سطوح دسترسی را بدست آوردید ، البته این امکان به معنای رد کردن و یا استفاده نکردن از ACL ها نیست بلکه در کنار آنها تکمیل کننده سطوح دسترسی خواهند بود
در واقع به طور کلی می توان گفت که در یک دامین همانطور که میدانید استفاده از Kerberos به عنوان Authentication Protocolاصلی مورد استفاده قرار میگیرد و هر یک از کاربران پس از شناسایی حتما یک Token نیز دریافت خواهند کرد که Permission های کاربر و گروه هایی که کاربر مورد نظر عضو آنها خواهد بود در آن وجود دارد) . البته هدف ما توضیح دقیق و جز به جز مراحل Authenticate شدن و دریافت TGT یا Security Ticket و Session ticket نیست و صرفا جهت آشنایی بیشتر با Claim در حال بررسی این مراحل هستیم (!!
در واقع Claim باعث بسط و گسترش این Token خواهد شد و علاوه بر اطلاعات معمول که به آنها اشاره کردیم ، Attributeهای بیشتری نیز در ساختار های DAC به مجموعه Token ما اضافه خواهد شد که در واقع همان Cliam های ما خواهد بود .
در شکل زیر می توانید این اجزا را که توسط مکانیسم DAC به Token ما اضافه شده اند روئیت کنید :