کنترل دسترسی پویا و Group Policy چه نقشی در ویندوز سرور 2019 بازی می‌کنند؟

ویندوز سرور 2019 مجموعه‌ای غنی از ابزارهای مدیریتی در اختیار کارشناسان شبکه قرار داده است. ابزارهایی که هر یک از آن‌ها در جای خود روند انجام کارها را تسهیل بخشیده و مدیریت مجموعه‌ای گسترده از کامپیوترها، سرورها و حساب‌های کاربری را ساده می‌کنند. تاکنون با ابزارهای مختلفی در این زمینه آشنا شدید و در ادامه با ابزارهای دیگری آشنا خواهید شد.

برای مطالعه قسمت قبل **آموزش رایگان ویندوز سرور 2019** اینجا کلیک کنید.

Dynamic Access Control

در کنار قابلیت‌های شاخصی که در ارتباط با اکتیو دایرکتوری به آن‌ها اشاره کردیم، مرکز مدیریت اکتیو دایرکتوری یکسری عملکردهای جدید در اختیار ما قرار داده است که ابزارهای کلاسیک موجود فاقد چنین قابلیت‌هایی هستند. اگر ابزار فوق را باز کرده و به درخت سمت چپ ابزار فوق نگاهی بیندازید، گزینه‌ای به نام کنترل دسترسی پویا (DAC) سرنام Dynamic Access Control را مشاهده می‌کنید. کنترل دسترسی پویا، فناوری است که ماژول‌های امنیتی لازم برای نظارت بر فایل‌ها و محافظت از داده‌های حساس سازمانی را در اختیارتان قرار می‌دهد تا اجازه ندهید افراد غیرمجاز به داده‌ها دسترسی پیدا کرده یا آن‌ها را ویرایش کنند. DAC به شما این امکان می‌دهد تا به برچسب‌گذاری فایل‌ها پرداخته و بر مبنای برچسب‌ها به طبقه‌بندی فایل‌ها بپردازید. در ادامه می‌توانید خط‌مشی‌های کنترل دسترسی را ایجاد کرده و به افراد اجازه دهید بر مبنای برچسب‌هایی که تعیین کرده‌اید به فایل‌های مشخصی دسترسی داشته باشند. یکی دیگر از ویژگی‌های قدرتمند کنترل دسترسی پویا، قابلیت گزارش‌دهی است. هنگامی که DAC در محیط شبکه ایجاد و اجرا شد، در ادامه می‌توانید گزارش‌هایی در ارتباط با فایل‌های خود ایجاد کنید و به‌طور مثال فهرستی از افرادی که اخیراً به یک سند طبقه‌بندی شده دسترسی داشته‌اند را پیدا کنید.

DAC همچنین می‌تواند برای تغییر مجوزهای کاربران بر اساس نوع دستگاهی که در حال حاضر از آن استفاده می‌کنند، به‌کارگرفته شود. به‌طور مثال، اگر کاربر بخش مدیریت منابع انسانی با دسکتاپ شرکت به شبکه وارد می‌شود، باید به پرونده‌های حساس منابع انسانی دسترسی داشته باشد و در مقابل اگر از لپ‌تاپ شخصی خود در محیط کار برای اتصال به شبکه استفاده می‌کند، نباید اجازه دسترسی به فایل‌ها را پیدا کند. این نوع تمایزها را می‌توان با استفاده از خط مشی‌های کنترل دسترسی پویا مدیریت کرد.

کنترل‌کننده دامنه فقط خواندنی

ما نمی‌توانیم بدون پرداختن به جزییات کنترل‌کننده دامنه فقط خواندنی (RODC) سرنام Read-Only Domain

Controllers تمامی جزئیات مرتبط با مولفه‌ها و ابزارهای مهم اکتیو دایرکتوری را بررسی کنیم. به‌طور معمول، هنگام نصب کنترل‌کننده دامنه جدید روی یک شبکه، شما نقشی به کنترل‌کننده دامنه اضافه می‌کنید که اجازه می‌دهد، فرآیند نوشتن و انجام کارهای مختلف روی آن امکان‌پذیر باشد تا به این شکل کنترل‌کننده دامنه از تمامی نقش‌های AD DS برای مدیریت هرچه بهتر سرورها استفاده کند. اما در برخی موارد، مجبور هستید یک کنترل‌کننده دامنه فقط خواندنی (RODC) را ایجاد کنید. یک دامنه فقط خواندنی یک نقش جداگانه نیست، بلکه به پیکربندی متفاوت AD DS اشاره دارد که در زمان تنظیم کنترل‌کننده دامنه باید آن‌را اضافه کنید. ما در آموزش ایجاد و پیکربندی کنترل‌کننده دامنه به این موضوع اشاره کردیم. یک RODC یک کنترلر دامنه تخصصی است که شما نمی‌توانید داده‌های جدیدی به آن بنویسید. این مدل کنترل‌کننده‌های دامنه یک نسخه ذخیره شده، فقط خواندنی از بخش‌های خاص یک پوشه را نگه‌داری می‌کند. شما می‌توانید به RODC بگویید که یک کپی از تمامی اعتبارنامه‌های دامنه‌تان را نگه دارد یا حتا می‌توانید به آن بگویید که فقط فهرستی از اعتبارهای انتخابی را نگه دارد. اما دلیل استفاده از RODC چیست؟ شعب مختلف یک شرکت و DMZها (زیرشبکه‌های منطقی یا فیزیکی) رایج‌ترین مثال‌هایی هستند که می‌توان به آن‌ها اشاره کرد. اگر شرکت شما شعبه کوچکی با کارمندان محدود دارد، ممکن است اضافه کردن یک کنترل‌کننده دامنه محلی برای انجام کارهای آن شعبه راهگشا باشد تا فرآیند ورود به شکل سریع‌تر و کارآمدتری انجام شود، اما به دلیل این‌که شما در مورد امنیت آن محیط اطمینان خاطر ندارید، تمایل دارید اطلاعات به شکل مستقیم از طریق شعبه محلی ویرایش نشوند. در چنین شرایطی به‌کارگیری یک RODC راه‌حل مشکل است. مورد دیگر استفاده از یک RODC در ارتباط با یک شبکه ایمن DMZ است. شبکه‌های فوق به محیط‌هایی اشاره دارند که معمولا دسترسی بسیار محدود را ارائه می‌کنند، زیرا به اینترنت عمومی متصل هستند. برخی از سرورها و خدمات که درون یک شبکه DMZ قرار دارند، ممکن است به اکتیودایرکتوری نیاز داشته باشند، اما شما نمی‌خواهید یک کانال ارتباطی را از DMZ به یک کنترل کننده دامنه در شبکه خود باز کنید. در این حالت، می‌توانید RODC را درون DMZ مستقر کنید تا اطلاعاتی را که برای سرویس‌دهی به آن سرورهای خاص در DMZ نیاز است در کنترل‌کننده دامنه فقط خواندنی ذخیره شود و به این شکل یک دامنه یا یک محیط فرعی بسیار ایمن درون شبکه DMZ ایجاد کنید.

قدرت منحصر به فرد Group Policy

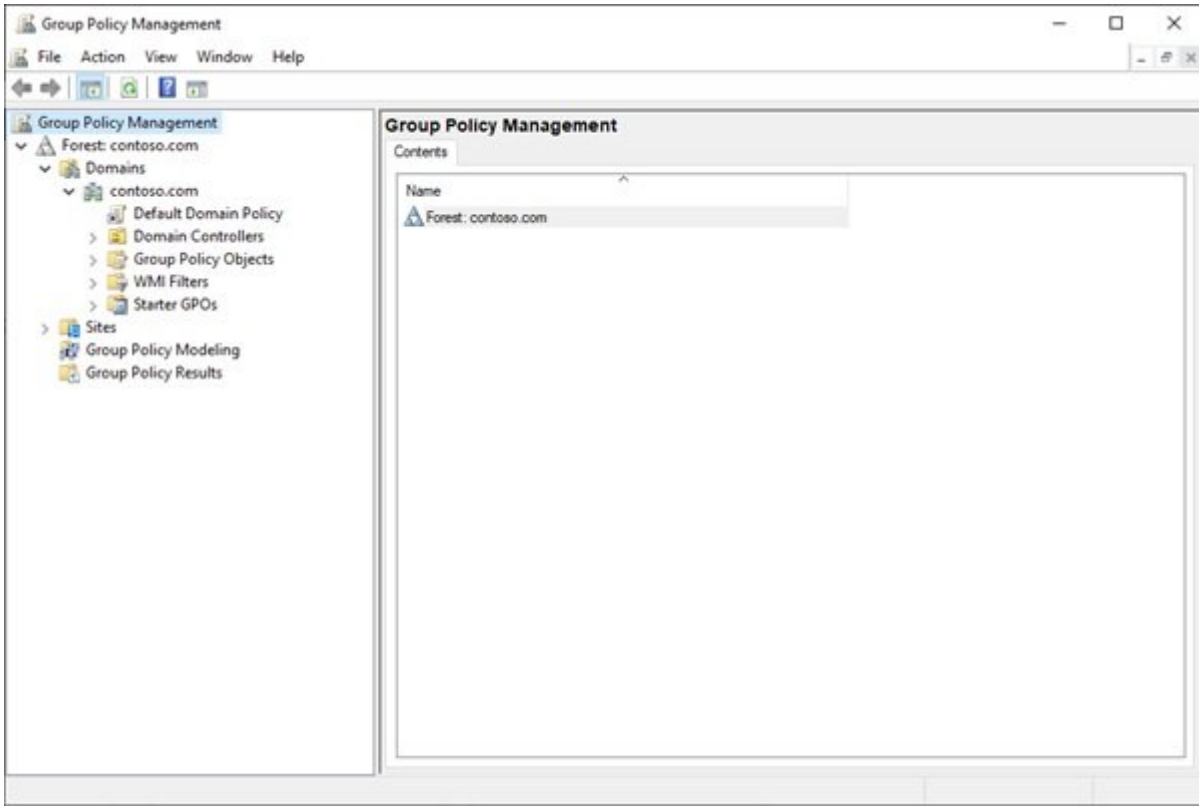
در شبکه‌ای که مبتنی بر سرورهای ویندوزی و اکتیودایرکتوری است، تقریباً مجموعه اصلی کامپیوترهای کلاینت مجهز به سیستم‌عامل ویندوز مایکروسافت هستند و همگی به یک دامنه متصل شده‌اند. مدیریت همه اشیا و ابزارها از درون اکتیودایرکتوری نه تنها از منظر سازمانی رویکرد درست و منطقی است، بلکه امکان تأیید هویت متمرکز دستگاه‌ها و برنامه‌ها را نیز امکان‌پذیر می‌کند. اما چگونه می‌توانیم خط‌مشی واحدی برای نظارت بر جنبه‌های مختلف دستگاه‌ها و کاربران پیاده‌سازی کنیم؟ این خط‌مشی‌های امنیتی چه هستند و چگونه باید آن‌ها را تنظیم کرد؟ پاسخ در ابزاری به نام Group Policy نهفته است. Group Policy این امکان را فراهم می‌کند تا خط‌مشی‌های اشیا گروه (GPO) را ایجاد کنید که شامل تنظیمات و پیکربندی‌هایی است که می‌خواهید روی کامپیوترها یا حساب‌های کاربری در دامنه اکتیو دایرکتوری اعمال کنید. هنگامی که یک GPO را با تنظیمات مختلفی ایجاد کردید، در ادامه می‌توانید این GPO را مطابق با نیازی کاری خود خط‌دهی کنید. اگر خط‌مشی خاصی دارید که قرار است روی همه سامانه‌های دسکتاپی اجرا شود، کافی است آن‌را به واحد سازمانی (OU) یا گروه امنیتی مناسب در اکتیو دایرکتوری که میزبان تمامی رایانه‌های دسکتاپ متصل به دامنه است تخصیص دهید. ممکن است یک GPO ایجاد کرده‌اید که فقط روی کامپیوترهای ویندوز 7 اعمال شود، شما می‌توانید با فیلتر کردن درست آن، کاری کنید که فقط کامپیوترهای مجهز به ویندوز 7 این خط‌مشی را دریافت کنند. جالب آن‌که تنظیمات فوق به شکل خودکار اجرایی شده و کامپیوترهای عضو دامنه این خط‌مشی را دریافت می‌کنند. به عبارت دقیق‌تر، شما نیازی ندارید تا سامانه‌های کلاینتی را مجبور کنید تا تنظیمات مربوطه را دریافت کرده و اعمال کنند. با استفاده از خط‌مشی Group Policy تقریبا می‌توانید هرگونه مولفه یا ابزاری در ویندوز را قفل کرده یا محدودیت‌های دقیقی روی آن‌ها اعمال کنید.

ممکن است به نقش‌های موجود در ویندوز سرور 2019 خود نگاهی داشته باشید و نقشی به نام Group Policy را مشاهده نکنید. بله درست است، چنین نقشی وجود ندارد. در حقیقت اگر شما همگام با ما این آموزش را دنبال کرده باشید، Group Policy را به‌طور کامل روی شبکه خود دارید. هر آن‌چه که Group Policy برای انجام کار خود به آن نیاز دارد، بخشی از Directory Domain Services است. بنابراین، اگر یک کنترل‌کننده دامنه در شبکه خود دارید، روی همان کنترل‌کننده دامنه Group Policy را در اختیار دارید، زیرا تمام اطلاعات مربوط به Group Policy داخل دایرکتوری ذخیره می‌شود. از آن‌جایی که نصب نقش AD DS همه آن چیزی است که شما برای استفاده از Group Policy به آن نیاز دارید و ما قبلا روی کنترل‌کننده در اختیار داریم، مستقیما به سراغ آن می‌رویم تا Group Policy را بهتر بشناسید. در طی این سال‌ها با بسیاری از مشاغل کوچک کار کرده‌ام که از سرور ویندوز استفاده می‌کردند و

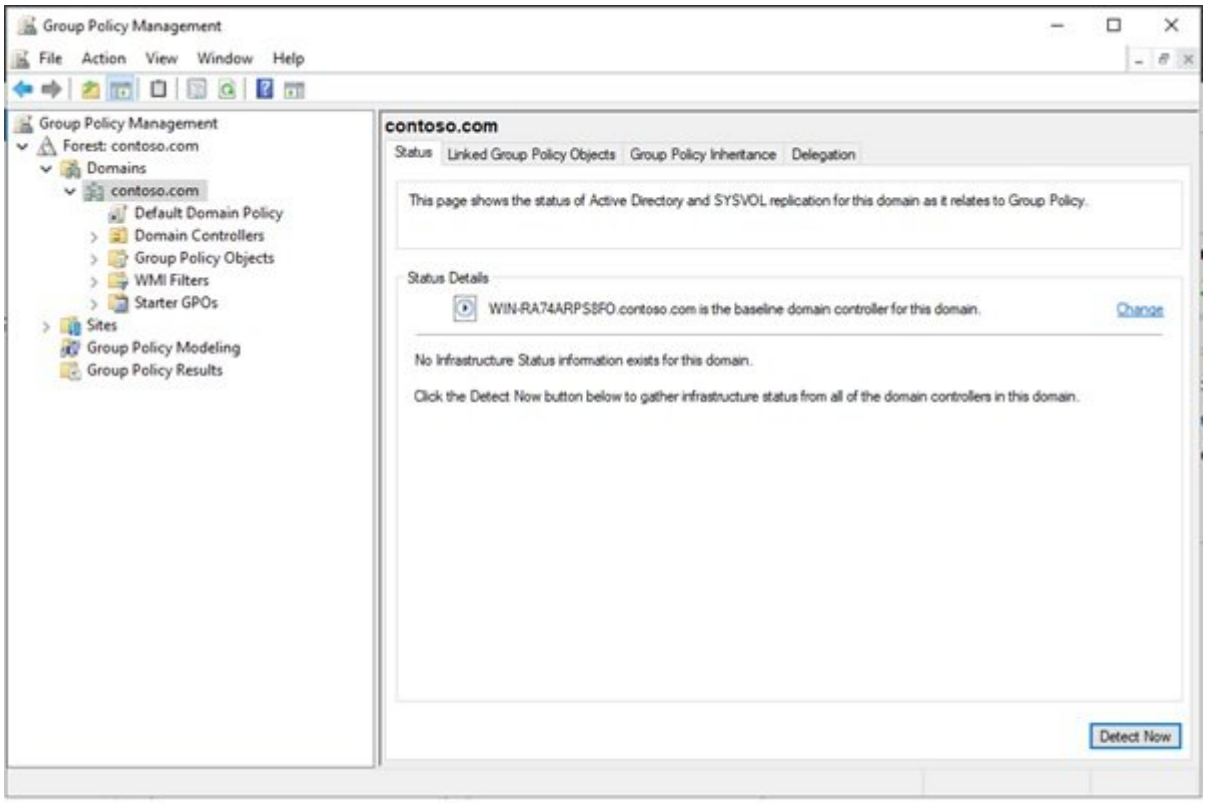
برخی از آن‌ها هیچ‌گاه به سراغ GPO نرفتند. به عبارت دیگر، شرکت‌ها ابزار قدرتمندی در جعبه ابزار خود داشتند که هیچ‌گاه از آن استفاده نکردند تا عمر مفید آن به پایان رسید! پس اجازه دهید نگاه دقیق‌تری به GPO داشته باشیم تا قدرت واقعی آن را بهتر درک کنیم.

خط‌مشی پیش‌فرض دامنه

ابتدا باید مشخص کنیم به چه بخشی از کنترل‌کننده دامنه خود باید برویم تا بتوانیم خط‌مشی‌های اشیا گروه را ایجاد کرده و دستکاری کنیم. همانند سایر ابزارها، Server Manager یک زیرساخت مرکزی برای باز کردن کنسول‌ها در اختیارتان قرار می‌دهد. با کلیک روی منوی Tools در Server Manager قادر هستید کنسول Group Policy Management را اجرا کنید. پس از باز شدن کنسول ، نام جنگل (Forest) خود را از درخت ناوبری در سمت چپ گسترش داده، سپس دامنه را گسترش داده و نام دامنه خود را انتخاب کنید.



درون این بخش، شما اشیا نام آشنایی را مشاهده می‌کنید، فهرستی از واحدهای سازمانی که ممکن است ایجاد کرده باشید، همراه با پوشه‌هایی که به واحدهای سازمانی دیگر اشاره دارند، همگی درون این بخش قرار گرفته‌اند.



در پایین نام دامنه خود یک GPO را مشاهده می‌کنید. این GPO به‌طور پیش‌فرض هنگام نصب به اکتیو دایرکتوری متصل شده و تنظیمات آن روی هر کاربر و کامپیوتری که بخشی از پوشه دامنه است اعمال می‌شود. این GPO خط‌مشی پیش‌فرض دامنه (Default Domain Policy) نام دارد. از آن‌جایی که این GPO کاملاً فعال است و روی همه کاربران و کامپیوترها اعمال می‌شود، مکانی مشترک است که خط‌مشی‌های واحد در ارتباط با گذرواژه‌ها و قواعد امنیتی را روی همه کاربران اعمال می‌کند.

در شماره آینده آموزش رایگان **ویندوز سرور 2019** با Group Policy بیشتر آشنا خواهیم شد.

برای مطالعه تمام بخش‌های **آموزش ویندوز سرور 2019** روی لینک زیر کلیک کنید:

آموزش رایگان ویندوز سرور 2019

تاریخ انتشار:
16 مرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15878/%DA%A9%D9%86%D8%AA%D8%B1%D9%84-%D8%AF%D8%B3%D8%AA%D8%B1%D8%B3%DB%8C-%D9%BE%D9%88%DB%8C%D8%A7-%D9%88-group-policy-%DA%86%D9%87-%D9%86%D9%82%D8%B4%DB%8C-%D8%AF%D8%B1-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019-%D8%A8%D8%A7%D8%B2%DB%8C-%D9%85%DB%8C