**توضیح اجمالی**

این فصل با استفاده از خط مشی گروهی به توانمندی بیشتر، استفاده آسان تر و مدیریت پذیرتر کردن شبکه می پردازد. رایانه‌ها و حساب‌های کاربری صدها تنظیماتی دارند که رفتار آنها را کنترل می‌کنند، مانند اینکه چند وقت یکبار رمزهای عبور باید تغییر کنند، چه مواردی روی دسک‌تاپ ظاهر می‌شوند، تنظیمات بی‌سیم و موارد دیگر. بر اساس Active Directory، Group Policy این امکان را فراهم می‌کند که چنین چیزهایی تعریف شده و سپس در بین گروه‌هایی از رایانه‌ها و کاربران اعمال شوند، در نتیجه یک محیط سازگارتر و کنترل‌شده‌تر ایجاد می‌شود. این فصل به عنوان یک آموزش عمیق در مورد خط مشی گروه در نظر گرفته نشده است، بلکه تمرکز بر روی چند مثال عملی ساده از استفاده از آن است.

خط مشی های گروه با استفاده از کنسول مدیریت سیاست گروه ایجاد و کنترل می شوند. این یکی از ابزارهای اداری است و می توان به روش های مختلفی به آن دسترسی داشت:

روی Start > Server Manager > Tools > Group Policy Management یا روی Start > Windows Administrative Tools > Group Policy Management کلیک کنید یا gpmc.msc را در کادر جستجو در نوار وظیفه تایپ کنید و Enter را فشار دهید.

درخت را در پانل سمت چپ به طور کامل گسترش دهید تا ساختار کلی دامنه نمایش داده شود. ساختار را می توان به آن اضافه کرد، اما برای ساده نگه داشتن چیزها، همه چیز را همانطور که هستند رها می کنیم. به ورودی به نام Default Domain Policy توجه کنید. همانطور که از نام آن پیداست، این تنظیمات پیش‌فرض برای کل دامنه را پوشش می‌دهد و بنابراین هرگونه تغییر برای همه رایانه‌ها یا کاربران سیستم اعمال می‌شود. مثال های ما روی آن تمرکز خواهند کرد.

ایجاد تغییر شامل کلیک راست بر روی یک مورد - مانند Default Domain Policy - و انتخاب Edit است. هنگام انجام این کار، ممکن است اخطار زیر را دریافت کنید و ممکن است بخواهید برای جلوگیری از آن در موارد آینده، کادر "این پیام را دوباره نشان ندهد" علامت بزنید:

خط‌مشی‌ها برای پیکربندی رایانه یا پیکربندی کاربر ایجاد یا اصلاح می‌شوند، اولی همه رایانه‌ها را تحت تأثیر قرار می‌دهد و دومی همه کاربران را تحت تأثیر قرار می‌دهد. هیچ الزامی برای ذخیره تغییرات وجود ندارد، زیرا هنگام انجام تغییرات به طور خودکار اتفاق می افتد. تغییرات در خط‌مشی‌ها و تنظیمات برگزیده بلافاصله منتشر نمی‌شوند و دفعه بعد که یک کلاینت به شبکه وارد می‌شود یا زمانی که رایانه راه‌اندازی می‌شود اعمال می‌شوند. با این حال، به طور کلی می توان با آوردن یک خط فرمان در یک ایستگاه کاری و تایپ دستور gpupdate /force، مسائل را تسریع کرد.

نکته ای که باید به آن توجه داشت این است که برخی از تنظیمات Group Policy وابسته به سیستم عامل هستند. برای مثال، برخی ممکن است فقط برای مثلاً کلاینت‌های ویندوز 10 قابل اجرا باشند و مثلاً به ویندوز 7 مربوط نباشند. با این حال، اکثر آنها برای تمام نسخه های ویندوز قابل اجرا هستند.

توجه برای کاربران نسخه های قبلی ویندوز سرور: کنسول مدیریت سیاست گروهی به طور خودکار در مرحله نصب سرور نصب می شود و دیگر نیازی به اضافه شدن به عنوان یک ویژگی جداگانه نیست.

به‌طور پیش‌فرض، کلاینت‌های ویندوز 7 و بالاتر، نام آخرین فردی را که از رایانه استفاده کرده است، نمایش می‌دهند. این می تواند در محیطی که در آن افراد رایانه های مشترک را به اشتراک می گذارند، گیج کننده باشد، زیرا لازم است شخص بعدی که از آن استفاده می کند به صراحت «Logon به عنوان کاربر دیگر» را مشخص کند، که ممکن است برای برخی افراد بصری و ناخوشایند باشد. با این حال، این رفتار قابل تغییر است، به طوری که همیشه یک نام کاربری و رمز عبور خالی به کاربران ارائه می شود و این کار از طریق Group Policy انجام می شود.

در سرور، کنسول مدیریت خط مشی گروه را راه اندازی کنید. روی Default Domain Policy کلیک راست کرده و روی Edit کلیک کنید. به Configuration کامپیوتر > Policies > Windows Settings > Security Settings > Local Policies > Security Options بروید. ورود تعاملی را پیدا کنید: آخرین ورود به سیستم نمایش داده نشود. روی آن دوبار کلیک کنید، سپس روی Define this Policy setting و Enabled و سپس OK کلیک کنید.

به طور پیش فرض، ویندوز سرور 2022 یک خط مشی رمز عبور از رمزهای عبور پیچیده دارد، به این معنی که رمزهای عبور باید ترکیبی از حروف، اعداد و کاراکترهای خاص باشند. با استفاده از رمزهای عبور پیچیده، امنیت افزایش می یابد. برای مثال، بسیار بعید است که یک کاربر یا هکر غیرمجاز بتواند رمز عبوری مانند !!40#mgzjeu23!398ab را حدس بزند. با این حال، در برخی از سناریوها، چنین گذرواژه‌هایی بسیار پیچیده هستند - به عنوان مثال، در یک مدرسه یا در یک محیط کار با تعداد زیادی از کاربران معمولی - در این صورت می‌توان خط‌مشی را بر این اساس تنظیم کرد.

برای انجام این کار، به مدیریت خط مشی گروه بروید. درخت را گسترش دهید تا Default Domain Policy نمایش داده شود، روی آن راست کلیک کرده و Edit را انتخاب کنید. به موارد زیر توجه کنید: پیکربندی رایانه > سیاست ها > تنظیمات ویندوز > تنظیمات امنیتی > سیاست های حساب > خط مشی رمز عبور:

برای حذف الزامات رمزهای عبور پیچیده، تغییر رمز عبور باید الزامات پیچیدگی را به Disabled برآورده کند.

برای جلوگیری از اجبار کاربران به تغییر رمز عبور خود به طور منظم، حداکثر سن رمز عبور را به 0 و حداقل سن رمز عبور را به 0 تغییر دهید.

برای حذف حداقل طول رمز عبور، حداقل طول رمز عبور را به 0 تغییر دهید.

به طور پیش فرض، رمزهای عبور حداکثر 14 کاراکتر طول دارند. برای افزایش این، محدودیت های حداقل طول Relax را تعریف و فعال کنید.

پیش فرض های ارائه شده توسط مایکروسافت معقول هستند و برای پشتیبانی از یک محیط امن طراحی شده اند. شما آزاد هستید که آنها را همانطور که در بالا توضیح داده شد تغییر دهید و بهترین کار داشتن رمز عبور و خط مشی های قوی است.

ویندوز سرور را می‌توان طوری پیکربندی کرد که در صورت تلاش‌های ناموفق برای ورود به سیستم، به طور موقت یک حساب کاربری را قفل کند. این می‌تواند امنیت را بهبود بخشد، زیرا چندین بار ورود ناموفق ممکن است نشان‌دهنده این باشد که یک کاربر غیرمجاز در حال حدس زدن گذرواژه‌ها برای تلاش برای دسترسی است.

برای پیکربندی این، به مدیریت سیاست گروه بروید. درخت را گسترش دهید تا Default Domain Policy نمایش داده شود، روی آن راست کلیک کرده و Edit را انتخاب کنید. به موارد زیر توجه کنید: پیکربندی رایانه > سیاست ها > تنظیمات ویندوز > تنظیمات امنیتی > سیاست های حساب > خط مشی قفل حساب:

برای فعال کردن قفل حساب: روی آستانه قفل حساب دوبار کلیک کنید. کادر تنظیم این سیاست را علامت بزنید. تعداد تلاش برای ورود نامعتبر را مشخص کنید (معمولاً از مقدار 3 استفاده می شود). روی OK کلیک کنید. پیامی با مقادیر پیشنهادی 30 دقیقه برای دو مورد دیگر نمایش داده می شود که مدت زمان قفل حساب و مدت زمانی را که باید قبل از تنظیم مجدد شمارنده قفل حساب بگذرد، مشخص می کند. اگر این مقادیر قابل قبول هستند، روی OK کلیک کنید. در غیر این صورت، می توان آنها را با استفاده از مدت زمان قفل حساب و تنظیم مجدد شمارنده قفل حساب پس از ویژگی ها تغییر داد.

هدف از این کار هدایت پوشه Documents کاربر (که گاهی اوقات به عنوان My Documents نیز شناخته می شود) از رایانه به درایو خانگی آنها در شبکه است. با انجام این کار، هر فایلی که کاربر ایجاد می کند به طور خودکار در سرور ذخیره می شود و از این رو هنگام ورود از هر رایانه ای در شبکه در دسترس آنها خواهد بود، بدون اینکه به طور خاص به یاد داشته باشید که آنها را در درایو خانگی شبکه خود ذخیره کنید. مزیت تغییر مسیر پوشه اصلی این است که قابلیتی به نام پوشه های آفلاین نیز فعال است. کاربرانی که لپ تاپ دارند همچنان اسناد پوشه خانه خود را هنگام کار خارج از سایت در دسترس خواهند داشت و هر تغییری که ایجاد شده است به طور خودکار با بازگشت به دفتر همگام سازی می شود.

برای پیکربندی این، Group Policy Management را راه اندازی کنید و درخت کنسول را گسترش دهید. روی Default Domain Policy کلیک راست کرده و Edit را انتخاب کنید. درخت را به User Configuration > Policies > Windows Settings > Folder Redirection > Documents گسترش دهید. روی Documents کلیک راست کرده و Properties را انتخاب کنید. در تب Target، منوی کشویی Setting را به Basic تغییر دهید - پوشه همه را به همان مکان و مکان پوشه Target را به Redirect به فهرست اصلی کاربر هدایت کنید. روی Apply کلیک کنید و برای پیام هشدار روی Yes کلیک کنید.

روی تب تنظیمات کلیک کنید و مطمئن شوید که مانند تصویر زیر به نظر می رسد. اگر نسخه های بسیار قدیمی ویندوز (XP، 2000، 2003) هنوز در حال استفاده هستند، کادر سوم را علامت بزنید. روی OK کلیک کنید. ممکن است یک پیام اخطار نمایش داده شود که با کلیک بر روی Yes می توان آن را نادیده گرفت.

سپس یک مرحله اضافی مورد نیاز است:

از درون Group Policy Management تنظیمات مربوط به Default Domain Policy را مشاهده کنید. به Computer Configuration > Policies > Administrative Templates > Network > Offline Files باز کنید. تنظیم در پانل سمت راست برای اجازه یا عدم اجازه استفاده از ویژگی Offline Files باید روی Enabled تنظیم شود. اگر از نسخه‌های قدیمی ویندوز استفاده می‌شود، تنظیمات زیرپوشه‌ها همیشه به‌صورت آفلاین در دسترس هستند، باید روی «فعال» تنظیم شود.

عیب یابی: متأسفانه، مشکلاتی در مورد فایل های آفلاین، به ویژه در نسخه های قدیمی ویندوز، غیر معمول نیست. اگر کار نمی کند، این تغییر اضافی را در Group Policy امتحان کنید. برای خط‌مشی پیش‌فرض دامنه، به Computer Configuration > Policies > Administrative Templates > System > Logon بروید. گزینه Always wait for the network at computer startup and logon را فعال کنید.

Group Policy می تواند برای ارسال تنظیمات بی سیم به کاربران درون سازمان استفاده شود. این کار استقرار وای فای را آسان‌تر می‌کند، زیرا نیازی به بازدید از هر کامپیوتر جداگانه نیست. پس از حذف این خط مشی، تنها کاری که کاربر باید انجام دهد این است که رمز عبور را وارد کند.

کنسول مدیریت سیاست گروه را راه اندازی کنید. درخت را در پانل سمت چپ باز کنید، روی ورودی Default Domain Policy کلیک راست کرده و Edit را انتخاب کنید. در پنجره جدید، درخت را گسترش دهید و به تنظیمات رایانه > سیاست ها > تنظیمات ویندوز > تنظیمات امنیتی > سیاست های شبکه بی سیم (IEEE 802.11) بروید. روی قسمت خالی در پنل سمت راست کلیک راست کرده و Create a New Wireless Policy for Windows Vista and Later Releases را انتخاب کنید:

به خط مشی جدید یک نام و یک توضیح اختیاری بدهید. روی دکمه Add کلیک کنید و Infrastructure را انتخاب کنید:

در پانل بعدی، یک نام پروفایل را مشخص کنید و نام شبکه (SSID) را تایپ کنید. هنگامی که این شبکه در محدوده است اتصال خودکار و در صورت موجود بودن گزینه اتصال به شبکه ترجیحی تر باید علامت زده شود. اگر از SSID مخفی استفاده می کنید، حتی اگر شبکه پخش نمی شود گزینه Connect را علامت بزنید. روی افزودن کلیک کنید. در تب Security، استانداردهای احراز هویت و رمزگذاری را که توسط سیستم بی‌سیم استفاده می‌شود، انتخاب کنید، سپس روی OK و سپس دوباره OK کلیک کنید:

در این مثال، ما خط مشی را برای همه رایانه های موجود در دامنه تعریف کرده ایم. با این حال، در عمل اغلب مفید است که واحدهای سازمانی (OUs) را تعریف کنیم و در صورت نیاز به کار ببریم، به عنوان مثال. یک OU برای کاربران لپ تاپ ایجاد کنید. مثال دیگر ممکن است مثلاً کسب‌وکاری باشد که در آن هر طبقه نقطه دسترسی بی‌سیم خود را دارد و شما می‌خواهید کاربران آن طبقه را فقط با آن مرتبط کنید.