فصل پنجم

طراحی، پیکربندی و مدیریت Group Policy

مباحث این فصل در دو قسمت "مقدماتی" و "حرفه‌ای‌تر شوید" ارائه شده است. در ابتدای هر فصل به بررسی مطالب ساده‌تری پرداخته شده که در استاندارد 70-410 وجود دارد و در قسمت "حرفه‌ای‌تر شوید" مباحث تخصصی‌تری که در استانداردهای 70-411 و 70-412 وجود دارد پرداخته شده است. لذا توصیه می‌شود ابتدا قسمت مباحث ابتدایی را مطالعه کرده و در صورتی‌که به مطالب تسلط پیدا کردید قسمت "حرفه‌ای‌تر شوید" را مطالعه نمایید.

نصب نرم‌افزار یکی از بزرگ‌ترین درخواست‌هایی است که مدیران ازطرف کاربران با آن روبه‌رو می‌شوند. این مشکل از آنجایی بدتر می‌شود که کاربران عمدتاً قادر به ایجاد تغییراتی در تنظیمات سیستم می‌باشند.

به‌عنوان مثال فرض کنید که یک کاربر برای کپی‌کردن یک فایل، فضای ذخیره‌سازی لازم را برروی سیستم خود ندارد و به‌جای این‌که از مسئول کمکی مدیر شبکه کمک بگیرد، خودش مقداری فایل از سیستم را پاک می‌کند که متأسفانه این پاک‌سازی ممکن است منجربه حذف فایل‌های سیستمی شود و یا افرادی را فرض کنید که تغییراتی در تنظیمات سیستم به‌وجود می‌آورند و ممکن است انجام این‌گونه تغییرات باعث بروز مشکلاتی در پایداری سیستم‌عامل شود.

اعمال محدودیت به کاربران شبکه می‌تواند یکی از راه‌حل‌های مناسب برای مقابله با این‌گونه مشکلات باشد که این محدودیت‌ها توسط مدیرشبکه تعیین و به کاربران اعمال می‌شود.

یکی از مهم‌ترین قابلیت‌هایی که در ویندوزسرور2012 و AD وجود دارد، Group Policy است. درحقیقت با استفاده از کنسول مدیریتی Group Policy می‌توان یک‌سری Group Policy Objects یا GPO ایجاد کرد که این GPOها مدیران را قادر می‌سازند تا به‌راحتی بتوانند برای کاربران محدودیت‌هایی را اعمال کنند. درادامه بهتراست تا با این ویژگی (Group Policy) بیشتر آشنا شوید.

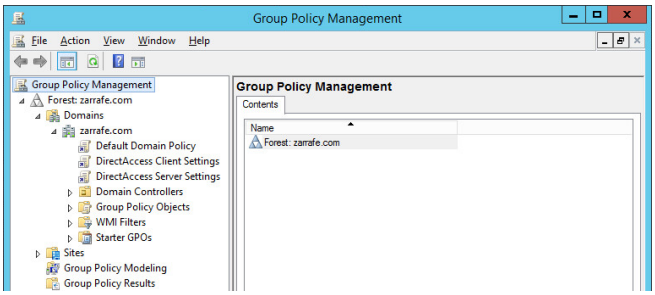
معرفی Group Policy

یکی از ویژگی‌های اصلی سیستم‌عامل ویندوز، انعطاف‌پذیری در انجام تنظیمات می‌باشد به‌این معنی که می‌توان کوچکترین جزئیات را با استفاده از Group Policy کنترل کرد. به‌همین خاطر می‌توان متناسب با نیازهای کاربران محدودیت‌هایی را درنظر گرفت تا کاربران نتوانند تغییراتی را در سیستم انجام دهند که باعث بروز مشکلاتی شود.

از این‌رو می‌توان گفت که یکی از اهداف اصلی در طراحی Group Policy اعمال محدودیت برروی مجموعه کارهایی است که کاربر می‌تواند با کامپیوتر انجام دهد.

☑ داشتن یک طرح و برنامه مدون برای استفاده از Group Policy در سازمان امری مهم و ضروری است، چراکه درصورت نیاز برای انجام تغییرات در محدودیت‌های اعمال شده باید کلیه جوانب و محدودیت‌های فعلی درنظر گرفته شود.

تمامی تنظیمات GP ازطریق کنسول مدیریتی (Group Policy Management Consol) یـا GPMC کـه در Administrative Tools قرار دارد، قابل دستیابی می‌باشند.



شکل 5- 1

قبل شروع به بررسی بیشتر بهتراست تا با چند تعریف اولیه در Group Policy آشنا شوید.

Policy: سیاستی بوده که برای دستیابی به یک هدف در سازمان پیاده می‌شود.

Group Policy: به مجموعه‌ای از سیاست‌ها (یا Policyها) گفته می‌شود.

Group Policy Object: یک شئ شامل مجموعه‌ای از Policyها بوده کـه مـی‌تـوان آن را بـه اشـیاء موجود در دامنه اعمال کرد. یک GPO را می‌توان به Site، Domain و OU اعمال کرد.

Scope: به محدوده‌ای از کامپیوترها و کاربران که یک GPO برروی آن‌ها اعمال می‌شـود Scope آن GPO گفته می‌شود. درحالت استاندارد Scope می‌تواند Local، OU، Domain و یا Site باشد.

Local: هرکامپیوتر به‌صورت محلی دارای یک GPO است که در خودش ذخیره‌شده اسـت و ایـن GPO هم برای کاربر و هم کامپیوتر مورداستفاده قرار می‌گیرد.

Organizational Unit: دراین سطح جزئی‌ترین تنظیمات GPO صورت می‌پذیرد که می‌توان یـک-سری قوانین را برای بخشی از اشیاء یک دامنه که در زیرمجموعه یک OU قرار دارند، تعیین نمود.

Domains: دراین‌سطح تنظیمات GPO در دامنه قرارگرفته و به‌کل اشیاء Userها و کامپیوترهایی کـه در دامنه وجود دارند، اعمال می‌گردند.

Sites: در این سطح مدیران سیسـتم مـی‌تواننـد GPOهـا را بـه‌کـل یـک سـایت در AD اعمـال و پیکربندی کنند که این تنظیمات به‌کل دامنه‌ها و سـرورهایی کـه عضـو سـایت مـی‌باشـند، اعمـال می‌شوند.

آشنایی با تنظیمات Group Policy

همان‌گونه که می‌دانید اکثر تنظیمات مربوط به سیستم‌عامل ویـنـدوز در قسـمت Registery ذخیـره

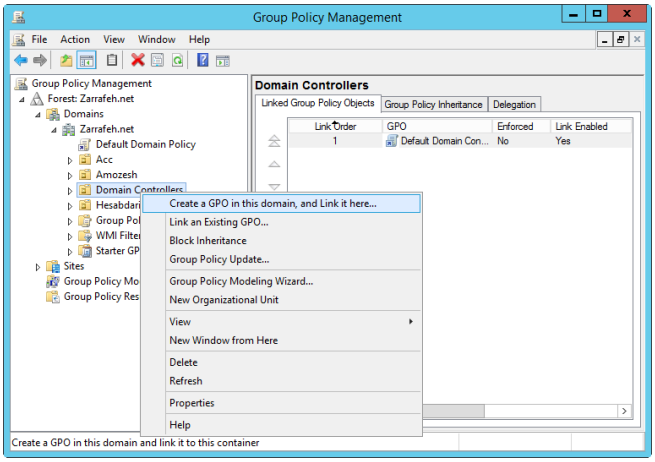
می‌شود. حال برای این‌که بتوان تنظیمات ویندوز را تغییر داد باید توسط Registery اقدام کرد؛ این همان کاری است که Group Policy انجام می‌دهد. در Group Policy یک‌سری قالب‌های مدیریتی (Administrative Templates) ازپیش‌تعریف شده وجود دارد که با استفاده از قالب‌ها می‌توان تنظیماتی را به کلاینت‌ها اعمال کرد. به‌عنوان مثال فرض کنید که یک کاربر یا کامپیوتر باید دارای تنظیمات Desktop مشخص باشد که از طریق GP این تغییرات در Registry مربوط به کاربر یا کامپیوتر اعمال و ذخیره می‌گردد.

روش‌های ایجاد Group Policy

مایکروسافت به‌صورت کلی دو روش برای ایجاد Group Policy درنظر گرفته است که شامل:

- **Local Policy Computer Tool**: این ابزار در مواقعی استفاده می‌شود که نیاز باشد تنظیماتی بر-روی ویندوز به‌صورت محلی انجام پذیرد.
- **Group Policy Management Consol**: یک کنسول مدیریتی جامع و متمرکز بوده که هدف اصلی آن کنترل تمامی کلاینت‌های دامنه است و ازاین ابزار زمانی استفاده می‌شود که نیاز باشد کلاینت‌های دامنه را مدیریت کرد. درادامه سعی داریم تا با این کنسول بیشتر آشنا شوید.

برای ساخت Policy در کنسول مدیریتی در زیرشاخه نام دامنه برروی OUای که می خواهید GPO را به‌آن اعمال کنید راست‌کلیک کرده و گزینه Create a GPO in this domain and Link it here... را انتخاب کنید. سپس نامی برای GPO وارد کرده و برروی OK کلیک کنید.



شکل 5- 2

☑ توجه داشته باشید که به‌صورت پیش‌فرض یک GPO با نام Default Domain Policy وجود دارد

که شامل تنظیمات امنیتی کل دامنه بوده و بهتراست که در تنظیمات این GPO تغییری ایجاد نکنید چراکه هر تغییر ایجاد شده به کل دامنه اعمال شده و ممکن است مشکل امنیتی به‌وجود آید (تنها اگر به تنظیمات GP آشنایی دارید می‌توانید در این GPO تغییراتی را اعمال نمایید).

تمرین 5-1

عنوان: ایجاد یک GPO و اختصاص آن به OU مربوط به Hesabdari

شرح: دراین تمرین قصد برآن است تا یک GPO ایجاد کرده و آنرا به OU مربوط به حسابداری اختصاص دهید.

اهداف:

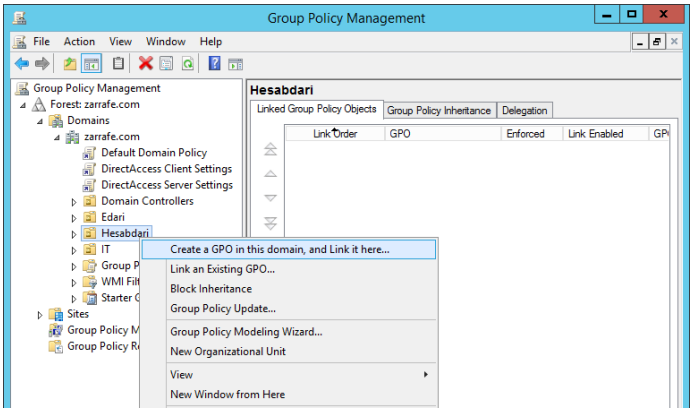
- نحوه ایجاد policy برروی یک OU
- پیکربندی Policy

تجهیزات و پیش‌نیازها:

- ویندوزسرور 2012 به‌همراه سرویس AD

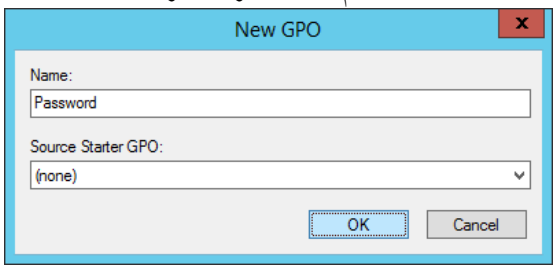
مراحل تمرین:

1. از منوی Start ← Administrative Tools را باز کنید.
2. برروی Group Policy Managment دوبار کلیک‌کرده تا کنسول مدیریتی Group Policy اجرا شود.
3. در پنجره باز شده و در زیر شاخه نام دامنه (نام دامنه در اینجا zarrafe.com است) برروی OU مربوط به Hesabdari راست‌کلیک کرده و گزینه Create a GPO in this domain and Link it here… را انتخاب کنید.



شکل 5-3

4. در پنجره باز شده در فیلدName یک نام را وارد کرده و برروی OK کلیک کنید.

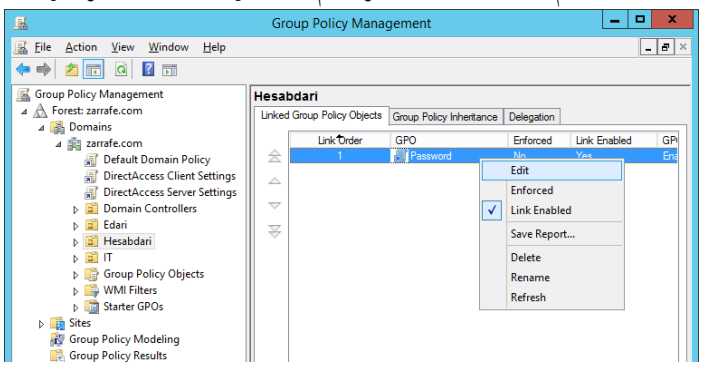


شکل 5- 4

5. بعد از کلیک برروی دکمه OK یک GPO یا Group policy object ساخته خواهد شد که مختص به OU مربوط به Hesabdari بوده و به تمام اشیاء موجود درآن اعمال خواهد شد.

پیکربندی GPO

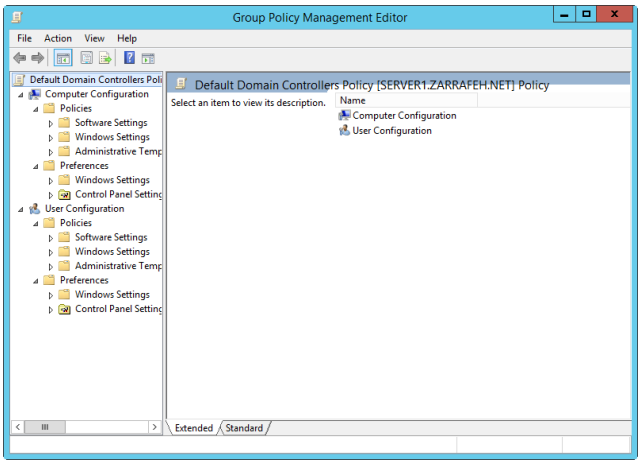
برای پیکربندی GPO در کنسول مدیریتی GPMC، برروی OUای که قصد دارید تا تنظیمات GPO را در آن انجام دهید کلیک کنید (به‌عنوان مثال برروی OU مربوط به Hesabdari) و در قسمت سمت راست برروی GPOای که قبلاً ساخته‌اید راست‌کلیک کرده و Edit را انتخاب کنید (در تمرین 5-1 یک GPO با نام Password ایجاد کرده‌ایم)تا کنسول GPME ظاهر شود.



شکل 5- 5

کنسول مدیریتی GPME

کنسول Group Policy Management Editor که با نام GPME شناخته می‌شود. برای پیکربندی و تغییرات policyها از این کنسول استفاده می‌شود. که در ادامه به بررسی کنسول GPME خواهیم پرداخت.



شکل 5- 6

همان‌گونه که در قسمت سمت چپ شکل 5- 6 مشاهده می‌کنید، تنظیمات هرGPO که به‌وسیله کنسول GPME باز شده است به دو قسمت تقسیم می‌شوند:

1. **User Configuration**: دراین قسمت Policyهایی (سیاست‌هایی) را می‌توان تنظیم کرد که تنها برروی کاربران دامنه تأثیر می‌گذارد. درواقع کلیه محدودیت‌های تعیین شده دراین قسمت مختص به کاربران خواهد بود.
2. **Computer Configuration**: دراین قسمت Policyهایی را می‌توان تنظیم کرد که روی کامپیوترهای عضو دامنه تأثیر می‌گذارد. درواقع کلیه تنظیمات مربوط به کامپیوترها ازاین‌جا در دسترس است.

تنظیمات اصلی که می‌توان در GP برای Computerها و Userها انجام داد به سه دسته زیر تقسیم می‌شوند (به شکل 5- 6 توجه کنید).

- **Software Setting**: این نوع از تنظیمات برروی برنامه‌های مشخص و یا نصب‌شده اعمال می‌گردند.
- **Windows Setting**: این نوع تنظیمات در جهت اعمال تغییرات در نحوه عملکرد ویندوز به‌کار

برده می‌شوند.

• **Administrative Templates**: دارای یک‌سری قالب‌های پیش‌فرض است که برای اعمال تغییرات در Computerها و Userها استفاده می‌شوند. علاوه بر این قالب‌ها، مدیران می‌توانند قالب‌های خود را نیز ایجاد و استفاده کنند.

به‌طور پیش‌فرض ویندوزسرور دارای یک‌سری قالب‌های مدیریتی بوده که برای مدیریت تنظیمات رایج به‌کار برده می‌شوند.

تمرین 5-2

عنوان: بررسی تنظیمات مربوط به رمزعبور برای تمام کامپیوترهای موجود در OU مربوط به Hesabdari.

شرح: در این تمرین قصد برآن است تا با محدودیت‌هایی که می‌توان برای کاربران در انتخاب رمز عبور اعمال و پیاده‌سازی کرد آشنا شوید.

هدف:

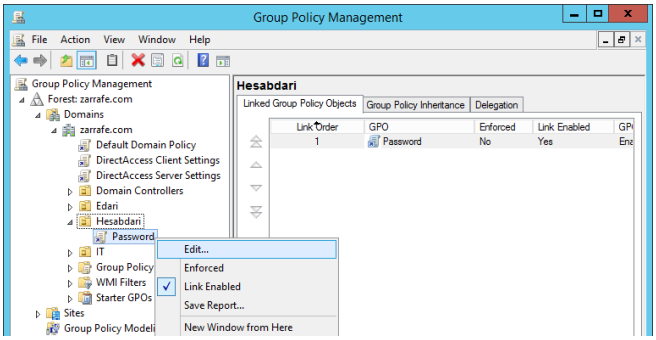
• آشنایی با سیاست‌های رمزعبور

تجهیزات و پیش نیازها:

• ویندوزسرور2012 به‌همراه سرویس AD

مراحل تمرین:

1. از منوی Start و سپس Administrative Tools ← GPMC را اجرا کنید.
2. در زیرشاخه zarrafe.com ← Hesabdari برروی GPO که در تمرین 5-1 ایجاد کرده‌اید راست کلیک کرده و گزینه Edit را انتخاب کنید.



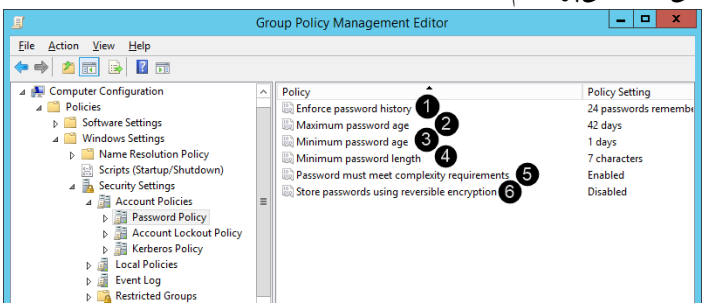
شکل 5-7

3. با استفاده از کنسول مدیریتی GPME و از قسمت چپ به مسیر زیر بروید.

Computer Configuration → Policies → Windows Settings → Security Settings

4. حال برروی Password Policies دوبار کلیک کنید.

5. در سمت راست تنظیمات امنیتی مربوط به سیاست‌های رمز عبور را مشاهده می‌کنید که در ادامه به بررسی آن‌ها می‌پردازیم.



شکل 5-8

1 با استفاده از این گزینه می‌توان تعیین کرد تا کاربر نتواند رمزهای عبوری که قبلاً استفاده کرده است را انتخاب کند. به‌صورت پیش‌فرض کاربر نمی‌تواند از 24 رمزعبور قبلی‌اش استفاده کند و باید رمزعبور جدیدی را وارد نماید.

2 با استفاده از این گزینه می‌توان زمان انقضاء رمزعبور را مشخص کرد.

3 با استفاده از این گزینه می‌توان حداقل مدت زمان استفاده از رمزعبور را مشخص کرد.

4 با استفاده از این گزینه می‌توان حداقل طول رمزعبور را تعیین کرد.

5 با استفاده از این گزینه می‌توان تعیین کرد که رمزعبور مورداستفاده باید دارای پیچیدگی یا اصطلاحاً Complex باشد. Complex بودن بدین معنی است که رمزعبور باید 3 شرط از 4 شرط زیر را داشته باشد.

- دارای حروف کوچک باشد.
- دارای حروف بزرگ باشد.
- دارای عدد باشد.
- دارای کاراکتر خاص باشد.

6 این گزینه باعث می‌شود تا رمزعبور غیرقابل بازیابی باشد؛ یعنی به‌صورت یک‌طرفه Hash شود.

در انتها هرکدام از این موارد گفته شده را به‌صورت دلخواه تغییر داده و پنجره GPME را ببندید.

تمرین 5-3

عنوان: پیاده‌سازی چند GPO و اعمال یک‌سری محدودیت به کاربران موجود در OU مربوط به Hesabdari.

شرح: در این تمرین دسترسی کاربران بخش حسابداری به Control Panel را محدود کرده و برای اطلاع رسانی به کاربر در زمان Login شدن پیامی مبنی‌بر عدم‌دسترسی به Control Panel به کاربر نشان داده می‌شود.

اهداف:

- آشنایی و پیکربندی Policy مربوط به محدودیت Control Panel
- آشنایی و پیکربندی Policy نمایش پیام «عدم وجود دسترسی به Control Panel» در زمان ورود

تجهیزات و پیش‌نیازها:

- ویندوزسرور2012 به‌همراه سرویسAD
- وجود یک کلاینت که به دامنه Join شده باشد

مراحل تمرین:

گام 1 OUها و کاربران را با توجه به تمرین 4-3 ایجاد نمایید.

گام 2 ایجاد GPO برای نمایش پیام به کاربران در صفحه Logon

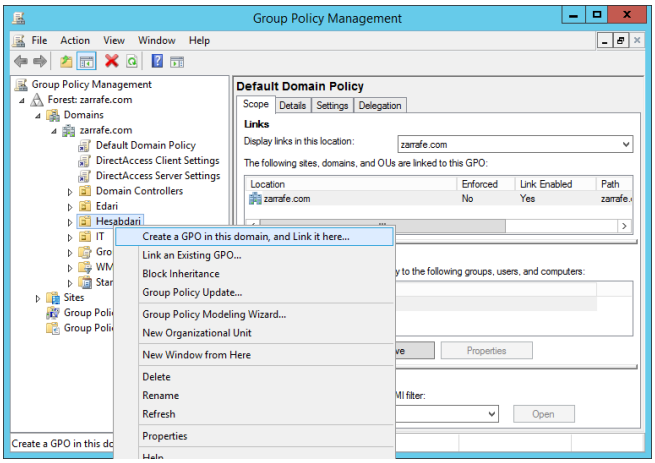
گام 3 ایجاد GPO جهت محدود کردن دسترسی به Control Panel

گام 4 Joinکردن کلاینت به دامنه

گام 5 Logon کردن به دامنه

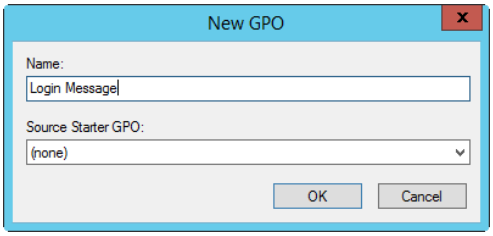
گام 2 ایجاد GPO برای نمایش پیام به کاربران در صفحه Logon

1. Administrative Tools را از منوی Start بازکرده و Group Policy Management را اجرا کنید.
2. به مسیر Forest ← Domains ← Zarrafe.com رفته و برروی OU مربوط به Hesabdari راست کلیک کرده و گزینه Create a GPO in This Domain and Link it Here… را انتخاب کنید.



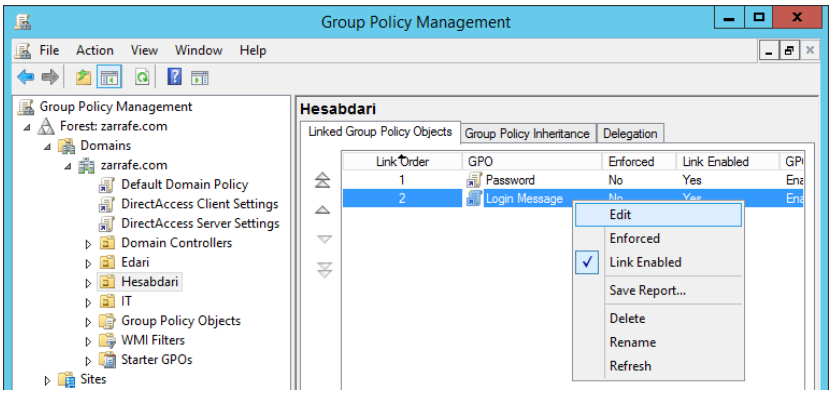
شکل 5- 9

3. هنگامی‌که پنجره محاوره‌ای New GPO باز شد، در فیلد Name عبارت Login Message را وارد کرده و برروی OK کلیک کنید.



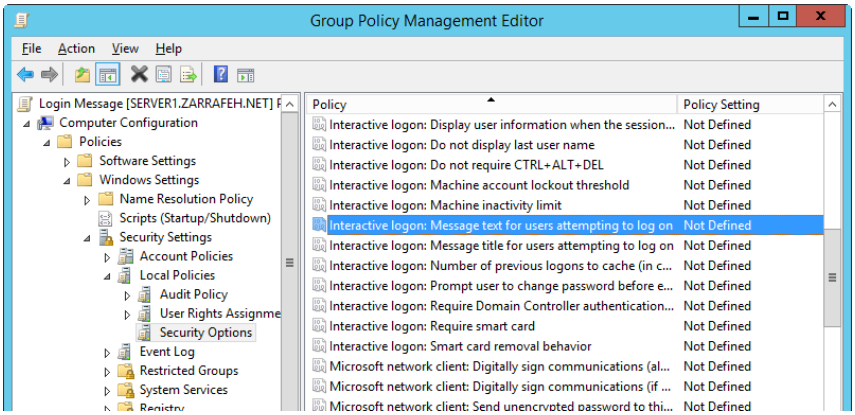
شکل 5- 10

4. در پنجره سمت راست GPO ساخته‌شده نمایش داده می‌شود. برروی آن راست‌کلیک کرده و Edit را انتخاب کنید.



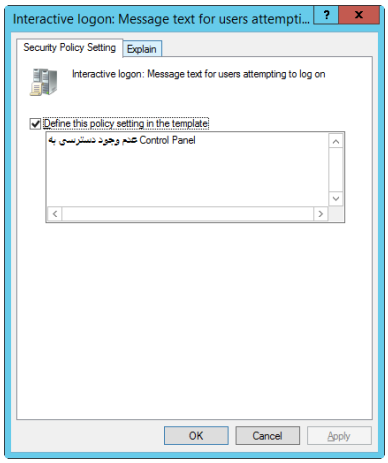
شکل 5- 11

5. در پنجره Group Policy Management Editor به مسیر Computer Configuration ← Policies ← Windows Setting ← Security Setting ← Local Policy ← Security Options بروید و در پنجره سمت راست به پایین پیمایش کرده و برروی Interactive Logon: Message Text For Users Attempting to Logon دوبار کلیک کنید.



شکل 5- 12

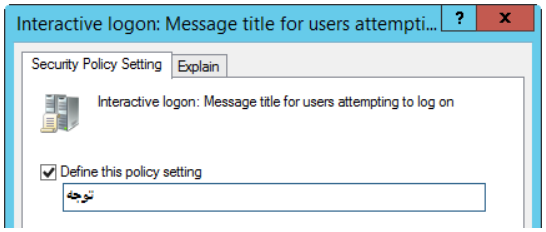
6. تیک گزینه Define This Policy Setting In The Template را زده و در جعبه متن عبارت "عدم وجود دسترسی به Control Panel"را وارد و برروی OK کلیک کنید.



شکل 5- 13

7. سپس برروی Interactive logon: Message title for Users attempting to Logon دوبار کلیک

کرده و در پنجره بازشده مطابق با شکل 5- 14 عنوان پیـام را وارد کـرده و بـرروی OK کلیـک کنید.

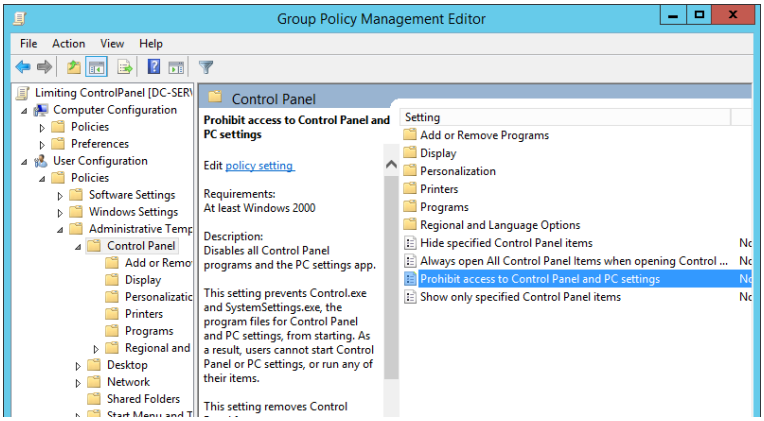


شکل 5- 14

8. پنجره GPO را بسته و به صفحه اصلی GPMC بازگردید.

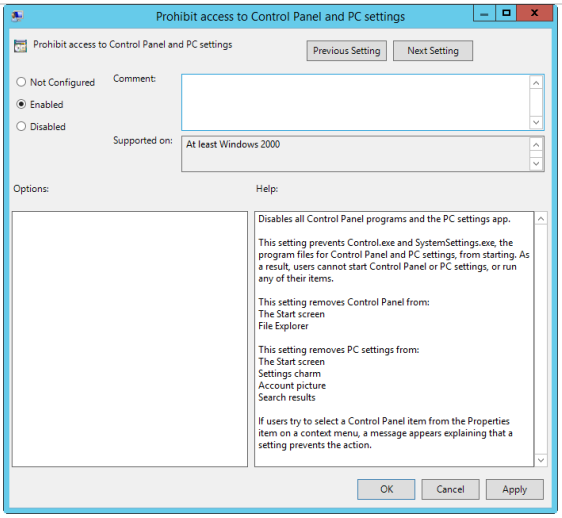
گام 3 ایجاد GPO جهت محدود کردن دسترسی به Control Panel

1. کنسول مدیریتی GPMC را بازکرده و برروی OU مربوط بـه Hesabdari راسـت‌کلیـک کـرده و گزینه Create a GPO in this Domain, and Link it Here را انتخاب و نام Limiting ControlPanel را برای نام GPO استفاده کنید.
2. برروی Limiting ControlPanel راست‌کلیک کرده و Edit را انتخاب کنید.
3. در پنجره بازشده بـه مسـیر User Configuration ← Policies ← Administrative Templates ← Control Panel رفته و در قسمت سمت راسـت پنجـره بـرروی Prohibit access to Control Panel and PC setting دوبار کلیک کنید.



شکل 5- 15

4. در پنجره بازشده گزینه Enable را انتخاب و درنهایت برروی OK کلیک کنید.



شکل 5- 16

گام 4 Join کردن به دامنه

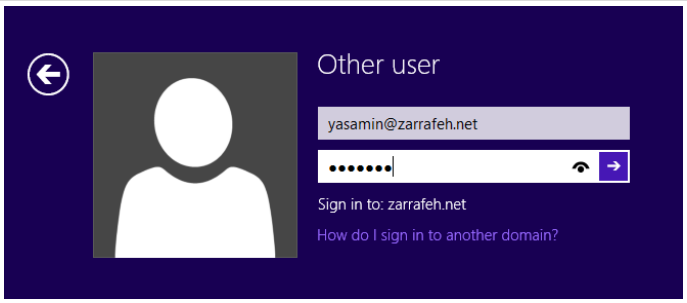
1. با استفاده از گام 2 در تمرین 3-3 (فصل 3) یک کامپیوتر را به‌دامنه Join کنید.
2. حال باید در سرورAD کامپیوتری که با آن به دامنه Logon می‌کنید را با استفاده از Active Directory به OU مربوط به Hesabdari منتقل کنید.

گام 5 Logon کردن به دامنه

1. در هنگامی‌که کلاینت تحت دامنه بالا می‌آید با صفحه زیر مواجه خواهد شد.

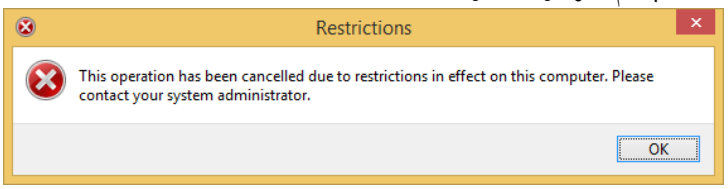
شکل 5- 17

2. با کلیک برروی OK و با واردکردن نام کاربری و رمز عبور Logon کنید.



شکل 5- 18

3. درنهایت به قسمت Control Panel بروید تا از عدم امکان دسترسی بـه Control Panel اطمینـان حاصل کنید و با پیغام زیر مواجه شوید.



شکل 5- 19