Labo 2: Group Policy Objects

We hebben nu een computer aan de Active Directory gekoppeld, en een gecentraliseerde gebruiker gebruikt om aan te melden. Active Directory biedt echter nog een heleboel meer mogelijkheden, en een heel belangrijke daarvan is het definiërnen van configuraties voor PC's, gebruikers, ...

Zo'n configuraties noemen we Group Policy settings. Een Group Policy Setting laat ons een heleboel opties, bijvoorbeeld bepaalde software installeren, beveiligingsopties aanpassen, folder redirection, en het aanpassen van de Windows Registry. Een aantal Group Policy Settings (regels) vormen samen een Group Policy Object, een set regels die samenhoren.

Hieronder staat de basis over GPO's kort samengevat, maar natuurlijk heeft Microsoft hier zijn eigen documentatie over. Dit artikel omschrijft de essentie van GPO's, en is zeker een interessant als je iets meer detail wilt. Bekijk daarnaast ook gerust dit filmpje.

Soorten GPO's

We onderscheiden 3 soorten Group Policy Objects (GPO's):

1. Local Group Policy Objects: Dit zijn Group Policy Objects die van toepassing zijn op 1 enkele lokale pc en de gebruikers die hierop aanmelden. Deze bestaan standaard op iedere PC's, al dan niet geïdentificeerd in een domein.

2. Non-local Group Policy Objects: Group Policy Objects die van toepassing zijn op meerdere PC's. Een GPO is van het type Non-Local, zodra deze open een Active Directory Server toegepast worden. Non-local Group Policy Objects overschrijven altijd Local Group Policy Objects.

3. Starter Group Policy Objects: Dit zijn templates, waarvan je kan starten met het aanmaken van GPO's.

Voordelen van GPO's

- Efficiënter beheer van IT-omgevingen
- Password policy enforcement
- Folder redirection

Nadelen van GPO's

Natuurlijk is het niet allemaal rozengeur en maneschijn. Er zijn een paar valkuilen als het aankomt op GPO's.

Eerst en vooral worden GPO's standaard iedere 90-120 minuten vernieuwd. Dit betekent concreet dat je iedere keer dat je een aanpassing doet ook zolang moet wachten. Je kan de update rate wel manueel instellen, met 0 minuten als minimum en 64800 minuten als maximum, maar als je voor 0 kiest, zal de PC om de 7 seconden proberen de GPO's te vernieuwen. Hoewel dit heel leuk en efficiënt klinkt, zal je netwerkinfrastructuur daar iets anders over denken, zeker als je met honderd(en) pc's zit. Daarnaast is het ook belangrijk om te onthouden dat GPO's sequentieel worden uitgevoerd bij de opstart van een machine. Dit wil zeggen dat als je veel GPO's hebt, dat je ook heel lang zal moeten wachten tot de PC is opgestart.

Verwerking van GPO's

GPO's worden in een bepalde volgorde verwerkt.

1. Local
2. Site
3. Domain
4. Organizational Unit

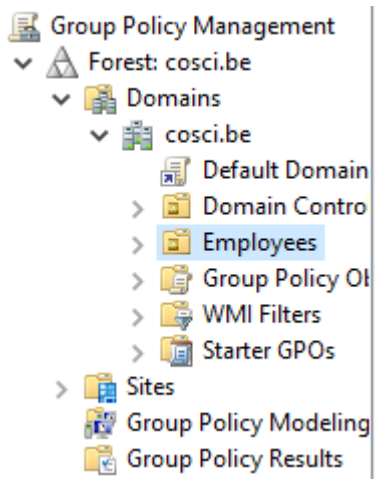
Dit wilt concreet zeggen dat een GPO die local geconfigureerd is overschreven wordt als diezelfde GPO gekoppeld aan het domein anders geconfigureerd is.

Aan de slag

Group Policy Management

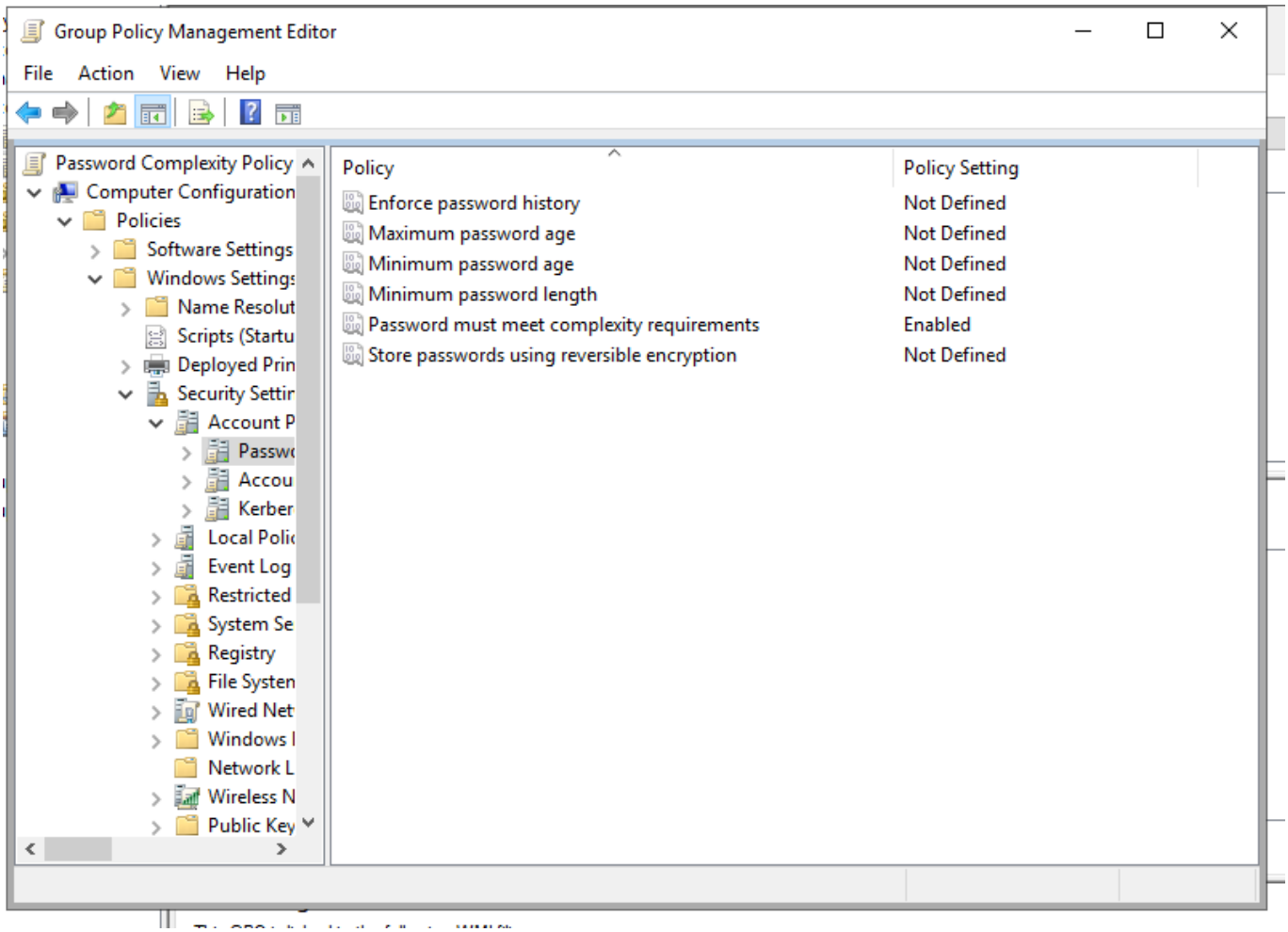
Op Windows Server krijg je wanneer je Active Directory geïnstalleerd hebt een tool "Group Policy Management". Het merendeel vandit labo zal zich wellicht hier afspelen.

Als je het vorige labo goed hebt afgerond, zie je in de balk aan de linkerzijkant iets zoals hieronder:



Van hier gaan we onze eerste GPO aanmaken. Met de rechtermuisknop klik je op cosci.be en maak je een nieuwe GPO aan. Je geeft de GPO de naam "Enforce Password Policy". De GPO zal automatisch verschijnen onder cosci.be. Deze is nu nog leeg, dus we willen hem aanpassen (rechtermuisknop>Edit).

Hier krijgen we twee opties: Computer Configuration & User Configuration. Voor het afdwingen van de Password Policy navigeren we naar Computer Configuration>Policies>Windows Policies>Security Settings>Account Policies>Password Policies. Wanneer we dit venster open hebben zien we een aantal opties. Open 'Password must meet complexity requirements' en selecteer enable. Als je dit gedaan hebt zou je het volgende moeten zien.



Zorg nu dat de laatste 10 wachtwoorden worden onthouden, een wachtwoord minstens 1 dag oud moet zijn voor het veranderd kan worden, na een jaar veranderd moet worden, het minstens 8 tekens heeft en dat het niet opgeslagen wordt met een terugkeerbare encryptie. Kijk ook zeker naar de standaardwaarden van de configuratie, die je vindt onder "Explain" als je een configuratie opent. Soms hoef je niks te veranderen.

Wanneer je klaar bent, sluit je het venster gewoon af. Je hebt nu een Group Policy Object geconfigureerd op de het domein-niveau.

Probeer nu een GPO aan te maken met een minimale lengte van 10 tekens op het niveau van de OU 'Sales'. Test daarna of deze de oorspronkelijke GPO overschrijft. (User aanmaken in OU, password proberen aan te passen, ...). Om GPO's te herladen moet je wel of te wel de client-pc herstarten, oftewel in de commandline het commando 'gpupdate /force' uitvoeren.

Als je wilt zien wat er precies is geconfigureerd in een bepaalde GPO, klik je op de GPO en selecteer je de tab 'Settings'. Hier zie je alle configuraties. Onder Scope zie je ook aan wie een GPO is gekoppeld.

Je kan ook bestaande GPO's koppelen aan meerdere containers. Dit doe je door naar een OU/Domain te gaan en te klikken op 'Link existing GPO'.

Oefeningen

Beperk toegang tot het configuratiescherm & Command Line

Gewone gebruikers mogen geen toegang hebben tot het configuratiepaneel. Dit is enkel toegelaten voor gebruikers in de ou IT.

Verbied het gebruik van USB-sticks, CDs, DVDs en andere verwijderbare media

Besmette verwijderbare media is een van de populaire manieren voor hackers om een organisatie binnen te dringen. Daarom willen we dit voor iedereen afsluiten.

Sluit het gastaccount af

Door het gastaccount kunnen gebruikers toegang krijgen tot gevoelige data. Zo'n accounts geven toegang tot een Windows-computer en vereisen geen wachtwoord. Standaard staan deze gelukkig uit, maar voor de zekerheid willen we dit toch afdwingen vanuit het domein.

Verhinder automatische driver-updates.

Windows voert automatisch een heleboel updates uit, ook aan device drivers. In de ou IT gebruikt men echter custom drivers die niet geüpdatet mogen worden.

Snelkoppeling cosci.be

Plaats bij alle gebruikers op het bureaublad een snelkoppeling naar Cosci.be

Script Logon name

Gelijkaardig aan het vorige: Zorg dat iedere keer dat er iemand aanmeldt op een PC, de naam en tijd naar een tekstbestand op de PC worden weggeschreven.

Installeer programma op alle pc's

Installeer de msi-file bij het labo op alle PC's. Hiervoor zal je een netwerk-share nodig hebben. Het gemakkelijkste hiervoor is om een shared folder te maken in VMWare en deze aan beide VM's te koppelen.