Group Policy Objects

We hebben nu een netwerk met 2 domain controllers die Active Directory en een gecentraliseerde aanmeldingspunt voorzien met fouttolerantie. Active Directory biedt echter nog een heleboel meer mogelijkheden en één heel belangrijke mogelijkheid is het definiëren van configuraties of afspraken voor PC's/gebruiker(s) binnen het domein.

Zo'n configuraties noemen we **Group Policy Settings**. Een Group Policy setting maakt het mogelijk om een heleboel configuraties door te voeren, bijvoorbeeld bepaalde software installeren, beveiligingsopties aanpassen, folder redirection, en het aanpassen van de Windows Registry, meer hierover wordt wel duidelijk tijdens het labo. Een aantal Group Policy Settings (regels) kunnen samen een Group Policy Object vormen, een set van regels die jij als beheerder van het domein logischerwijs vindt 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 meer details wilt. Bekijk daarnaast ook gerust dit filmpje. Een GPO omvat beleidsregels, nl. **policies** of voorkeuren nl. **preferences** die ingesteld of toegepast moeten worden voor bepaalde gebruiker(s) en/of computer(s).

> De beveiliging van "bronnen" (printers, netwerkschijven,...) worden niet afgedwongen d.m.v. group policies maar groepen (global, domein lokaal, ...).

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, al dan niet opgenomen 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 op een Active Directory Server geïnstalleerd worden. Non-local Group Policy Objects overschrijven altijd Local Group Policy Objects.
3. **Starter Group Policy Objects**: Dit zijn templates, waarvan je kan starten bij 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 aan een GPO doet ook zolang moet wachten totdat de betrokken PC de aanpassing "oppikt". Je kan de updatefrequentie wel manueel instellen. Daarnaast is het ook belangrijk om te weten dat GPO's sequentieel worden uitgevoerd bij de opstart van de PC. Dit wil zeggen dat als je veel GPO's hebt, dat je ook heel lang zal moeten wachten totdat de PC opgestart is.

Verwerking van GPO's

GPO's worden in een bepaalde volgorde verwerkt.

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

Dit wil concreet zeggen dat een setting in een GPO die local geconfigureerd is overschreven wordt als diezelfde setting opgenomen in een GPO gekoppeld aan het domein, anders geconfigureerd is.

Het tijdstip waarop GPO-instellingen effectief worden, is niet altijd hetzelfde. Bijvoorbeeld:

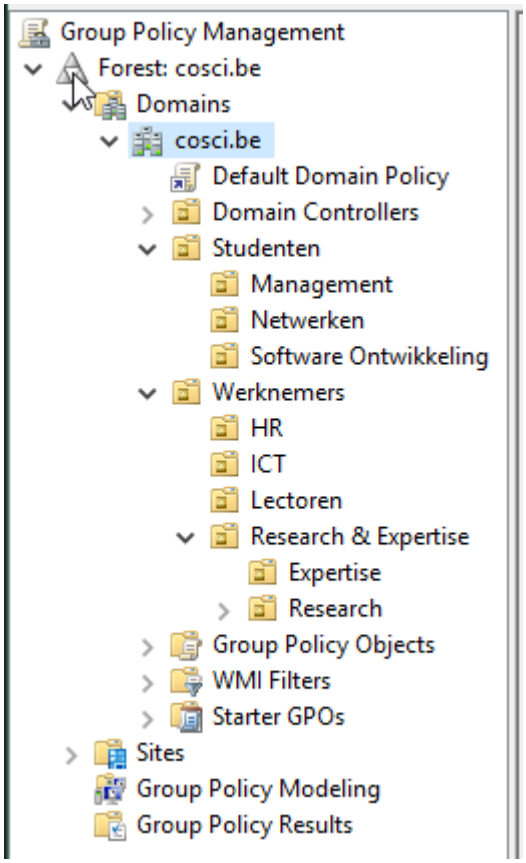
- Instellingen van computer configuration worden toegepast als de computer opnieuw opstart
- Instellingen van user configuration worden toegepast als de gebruiker opnieuw inlogt

Aan de slag

Group Policy Management

Bij de installatie van Active Directory wordt de tool "Group Policy Management" mee geïnstalleerd. Deze is te vinden in Server Manager > Tools.

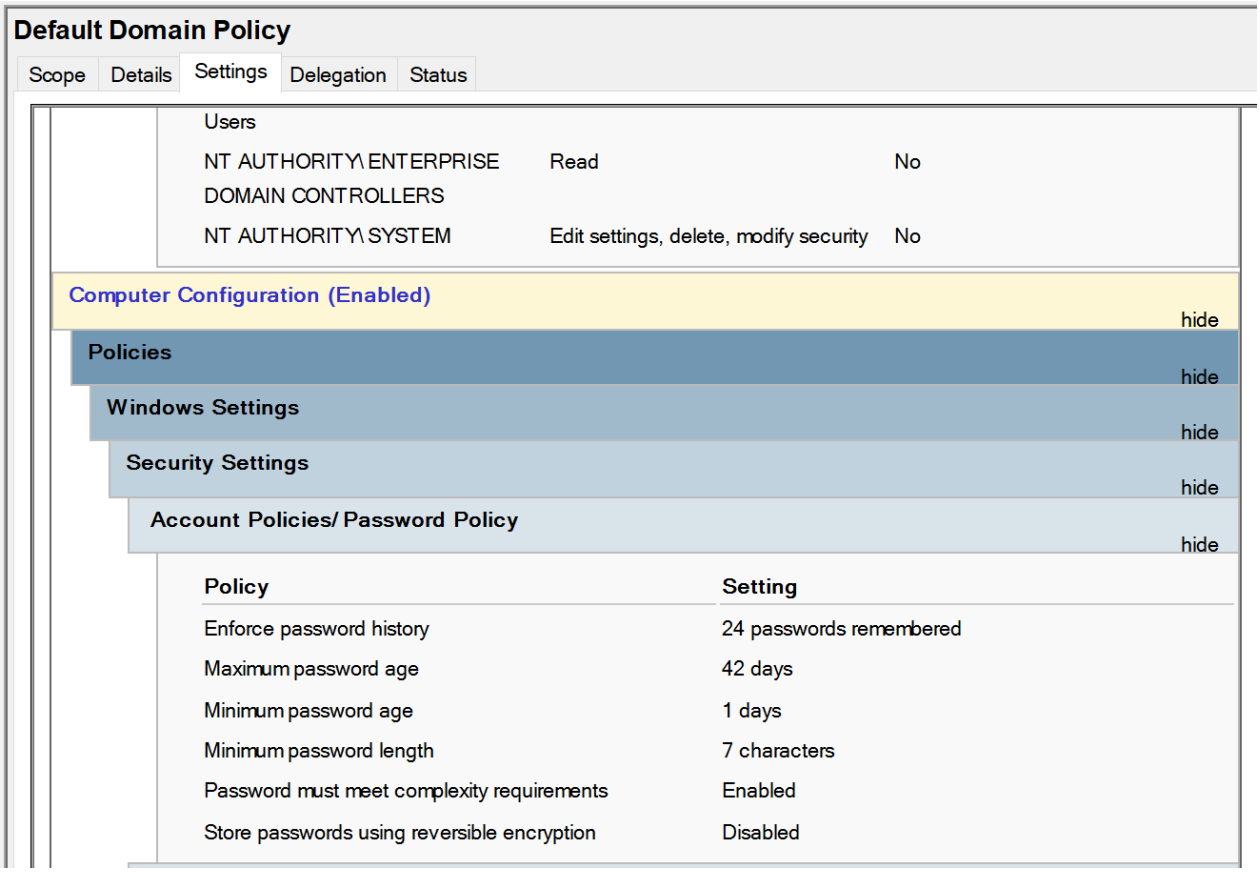
Het merendeel van dit labo zal zich hier afspelen. Als je het vorige labo goed hebt afgerond, zie je in de balk aan de linkerzijkant iets zoals hieronder:



> Indien je een paar OU's te veel hebt gemaakt en je krijgt 'access denied' bij het verwijderen, kan je volgende stappen volgen om deze op te ruimen:

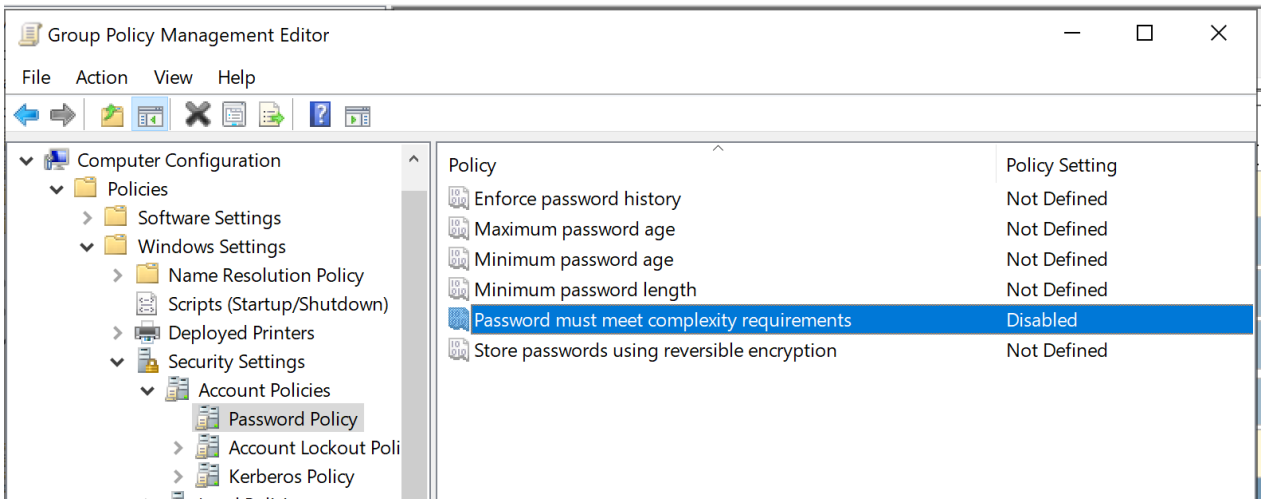
- Open `Active Directory Users and Computers`
- Onder `View` activeer je `Advanced Features`
- Ga naar je OU's Properties > Object
- Zet `Protect object from accidental deletion` uit
- Onder `View` zet je `Advanced Features` terug uit
- Verwijder je OU

Alvorens nieuwe GPO's aan te maken, is het belangrijk om te beseffen dat er reeds twee GPO's aangemaakt zijn, nl. Default Domain Controllers Policy en Default Domain Policy. De eerste GPO is bedoeld om de domain controllers te beveiligen en de tweede GPO stelt standaard beleidsregels in voor het domein. Enkele instellen zijn hieronder te zien:



In OU=HR gaan we onze eerste GPO aanmaken. Met de rechtermuisknop klik je op de OU=HR en maak je een nieuwe GPO aan. Je geeft de GPO de naam "labo-GPO-nr1". De GPO zal automatisch verschijnen onder de container OU=HR. Deze is nu nog leeg, dus we willen hem aanpassen, rechtermuisknop>Edit.

Hier krijgen we twee opties: Computer Configuration & User Configuration. Navigeer in beide categorieën naar Policies, Administrative Templates, en kijk welke regels je zoal kan instellen. Je merkt dat het aantal beleidsregels enorm is. Elke regel kan **ingeschakeld**, **uitgeschakeld** of **niet geconfigureerd** zijn. Voor het afdwingen van de Password Policy navigeren we naar Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policiy. Wanneer we dit venster open hebben zien we een aantal opties. Open 'Password must meet complexity requirements' en selecteer *Disabled*. Als je dit gedaan hebt zou je het volgende moeten zien.



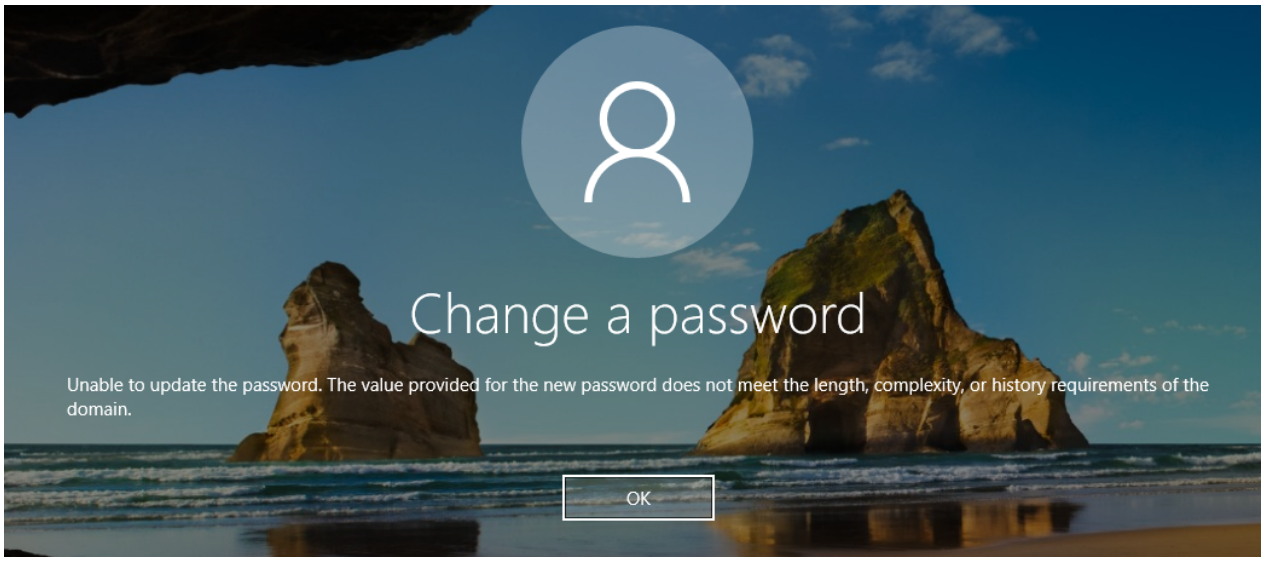
Zorg nu dat de laatste 5 wachtwoorden worden onthouden, een wachtwoord minstens 1 dag oud moet zijn voor het veranderd kan worden, na een jaar veranderd moet worden, het minstens 3 tekens heeft, dat het niet opgeslagen wordt met een terugkeerbare encryptie en behoudt de complexitiy requirements zoals hierboven. Kijk ook zeker naar de standaardwaarden van de configuratie, die je vindt onder "Explain" als je een configuratie opent.

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

Test of de GPO werkt:

- Maak een user1 aan met paswoord p@ssw0rd in OU=HR
- Log in met user1 op de Windows 10 machine en probeer het paswoord aan te passen naar ttt ... => lukt niet!

OK, waarom lukt dit niet ... wat zegt de error boodschap van Windows:



Het nieuwe paswoord kan "verkeerd" zijn volgens een van de drie redenen:

- does not meet the length => kan niet is 3 karakters lang
- does not meet the complixity => is afgezet
- does not meet the history requirements => verder onderzoeken ...

Het paswoord moet één dag oud zijn alvorens het aangepast zou kunnen worden, dan moet er onderzocht worden wanneer het paswoord "aangemaakt" werd. Hef die beleidsregel op => zet de minimum password age op 0.

> Werkt de paswoordaanpassing na de beleidsaanpassing van de "minimale password age" op 0 te zetten? Waarschijnlijk nog niet, je moet de PC of computer van de user in de juiste OU zetten, omdat het een computer policy is die je aangepast hebt. *Er is dus een duidelijk verschil tussen USER en COMPUTER policies!* Afhankelijk van de policy die je aanmaakt, moet de user en/of de PC in de juiste OU geplaatst worden.

Plaats de PC in de juiste OU=HR en probeer het paswoord nu aan te passen? Lukt het? Eindelijk! ... of toch niet.

> Volgens bovenstaande link is het **voorbeeld van password-policy een slecht voorbeeld**. Om toch te controleren of de computerpolicy wel degelijk werkt, kan je deze testen met het "Start Menu" via Computer policy => Admin. Templ. => Start Menu => full screen.

Als je wil 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 gekoppeld is. 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'.

> Note: Als meerdere GPO's na mekaar toegepast worden, dan betekent **niet geconfigureerd** dat de vorig toegepaste instelling in de GPO-hiërarchie blijft en **uitgeschakeld**, wat de vorige instelling ook was, ze wordt nu uitgeschakeld.

Policies debuggen

Wanneer er iets misloopt met het toepassen van een policy, zijn er tools om te kijken waar het probleem precies zit. Een eerste stap is kijken welke regels er nu toegepast werden. Dit kan je doen door in een console-venster het commando `gpresult /v` in te typen. Dit geeft een lijst van alle policies die toegepast worden op de huidige **gebruiker**, alsook wat extra informatie. Je kan deze informatie ook wegschrijven als een (overzichtelijker) HTML-bestand door het commando `gpresult /H bestand.html`.

Nu moet je opletten aan welk type object je juist de settings van je GPO gekoppeld hebt. Heb je settings onder User Configuration gezet, dan zal je je GPO vinden met gpresult als je ingelogd bent met de juiste user. Als je settings onder Computer Configuration hebt gezet, dan zal je moeten inloggen met een administrator account en zal je met gpresult de GPO's zien die van toepassing zijn op deze computer.

Wanneer een policy niet toegepast kan worden, gaat de Group Policy Client een foutmelding wegschrijven in het Windows event log. Je kan deze log bekijken door het programma Event Viewer op te starten en te navigeren naar Windows logs.

Zoals reeds kort aangehaald werd, komen hiërarchieën van OU’s vaak voor (dat is in feite de bedoeling). Aangezien je op elke OU bepaalde regels kan instellen, kunnen conflicten voorkomen.

Neem bijvoorbeeld het beleidsaspect “Hide my network places on desktop”. GPO's kunnen hiervoor één van de volgende waardes specificeren:

- Enabled
- Disabled
- Not configured

Door de opeenvolgende GPO’s achter elkaar te zetten/uitvoeren volgens de hiërarchieën van OU’s, krijgen we bijvoorbeeld: disabled, disabled, not configured, ..., enabled, not configured (Not configured betekent: er wordt niets veranderd aan de vorige instelling). In dit geval is enabled de definitieve instelling.

Meer dan een GPO per OU

Ga naar Group Policy Management en maak onder de OU Studenten twee nieuwe GPO's aan (via "Create a GPO in this domain, and Link it here…").

- Noem de eerste **Disable Command Prompt** en zorg dat, onder User Configuration, de instelling "Toegang tot de opdrachtprompt voorkomen" (E. Prevent access to the command prompt) aan staat.
- Noem de tweede **Enable Command Prompt** en zorg dat daarin dezelfde instelling uitgeschakeld staat.

> Tip: gebruik de filter tool `View > Filter Options...`

We hebben nu twee GPO's gedefinieerd in de OU van Studenten die in conflict liggen met elkaar.

Selecteer in Group Policy Management de OU en navigeer naar het "Linked Group Policy Objects"-tabblad. Hier zie je de volgorde staan van waarin de GPO's voorrang krijgen (hoger krijgt voorrang). Zorg dat de GPO Disable Command Prompt bovenaan staat. Log op de Windows 10-machine in als iemand van de OU Studenten en probeer een opdrachtprompt te openen. Dat zou niet mogen werken. Zet nu de GPO Enable Command Prompt bovenaan, en meld je opnieuw aan op de Windows 10-machine (wijzigingen in de group policy worden pas doorgegeven wanneer men opnieuw inlogt). Probeer opnieuw om een opdrachtprompt te openen. Nu zou het wel moeten gaan.

De registry: een kennismaking

> TIP: Waarom bespreken we hier kort de registry? Met groepsbeleid kan je onder andere het register aanpassen, maar ook scripts toepassen, mappen omleiden, applicaties beheren, ...

De registry is een database waarin Windows de instellingen i.v.m. de software en de hardware bijhoudt. Via het commando `regedit` hebben we toegang tot de registry. Er zijn 5 *afdelingen* (E. hives, wat letterlijk vertaald bijenkorf betekent) die elk een categorie van instellingen bijhouden.

Via `regedit` kan men wijzigingen aanbrengen aan de registry. Dit moet evenwel uiterst omzichtig gebeuren. Wie nog in een leerfase zit, kan best alleen aan de registry prutsen op een machine waarbij het geen kwaad kan (een virtuele machine, een machine in een pc-lab, ...). Zorg alleszins dat je een backup hebt, want een foutje in de registry kan ervoor zorgen dat het Windows OS niet meer start/werkt.

Een afdeling is gestructureerd als een folder met subfolders. Een (sub)folder wordt key genoemd. Zoals een folder kan een key bestaan uit subkeys. Ook kan een key een of meerdere waardes hebben (afhankelijk van de key kan het type van de waarde zijn: unicode string, dword, bytes, ...). Een registry-afdeling wordt ook rootkey genoemd. Van de 5 afdelingen zijn er 3 echte, waar dus daadwerkelijk data in opgeslagen wordt:

- **HKEY_LOCAL_MACHINE**: bevat informatie over Windows en de geïnstalleerde applicaties die algemeen van toepassing is (d.i. voor alle gebruikers).
- **HKEY_USERS**: bevat informatie voor alle gebruikers die een profiel hebben. De gegevens staan gegroepeerd per gebruiker.
- **HKEY_CLASSES_ROOT**: bevat allerlei informatie over bestandsextensies, e.d.

De andere twee afdelingen zijn shortcuts naar bepaalde delen van één van de bovenvernoemde afdelingen:

- **HKEY_CURRENT_USER**: bevat informatie voor Windows en de applicaties die enkel van toepassing is op de huidige gebruiker. Het verwijst naar een bepaalde subkey in *HKEY_USERS*.
- **HKEY_CURRENT_CONFIG**: bevat informatie over de configuratie van de hardware. Het verwijst door naar een bepaalde subkey in HKEY_LOCAL_MACHINE.

Instellingen worden bij voorkeur gewijzigd via het configuratiescherm of via de programma's die ze in de registry gestoken hebben. Uitzonderlijk kan het nodig zijn de registry te editeren via `regedit`.

Voorbeeld: de standaard toetsenbord layout

Wanneer er een nieuwe gebruiker aangemaakt wordt, worden een aantal standaardinstellingen gekopieerd naar zijn profiel. Zo wordt er onder andere de default layout van het toetsenbord (AZERTY, QWERTY, DVORAK, …) opgehaald uit de registry (HKEY_USERS.DEFAULT\Keyboard Layout\Preload\1). Open de registry en zoek op welke waarde er standaard gebruikt wordt. Je kan deze waarde als volgt interpreteren:

- 00000413 Dutch (Standard) – QWERTY
- 00000813 Dutch (Belgian) – AZERTY
- 0000040c French (Standard) – AZERTY
- …

Exporteren en importeren

Via `regedit` kan je ook (delen van) de registry *exporteren* naar een .reg-bestand. Dat is een bestand in tekstformaat dat de verschillende keys met bijbehorende waarden bevat. Zo kan een .reg-bestand bijvoorbeeld de volgende data bevatten:

```
------------------------------------------------
Windows Registry Editor Version 5.00

[HKEY_USERS\.DEFAULT\Keyboard Layout\Preload]
"1"="00000409"
------------------------------------------------
```

Dit bestand terug importeren in de registry kan door er eenvoudigweg op te dubbelklikken. Als de gebruiker bovenstaand bestand importeert, dan zal de standaard toetsenbord layout dus op English (United States) gezet worden.

Oefeningen

Beperk toegang tot het configuratiescherm & Command Line (voor users)

Gewone gebruikers mogen geen toegang hebben tot het configuratiepaneel en command line. Dit is enkel toegelaten voor gebruikers in de OU=ICT.

Verbied het gebruik van USB-sticks, CDs, DVDs en andere verwijderbare media (voor users)

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

Sluit het gastaccount af (voor computers)

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 (voor computers)

Windows voert automatisch een heleboel updates uit, ook device drivers updates. In de OU=ICT gebruikt men echter custom drivers die niet geüpdatet mogen worden.

Snelkoppeling (E. shortcut) cosci.be (voor users)

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

Script Logon name

Zorg dat iedere keer dat er iemand aanmeldt op een PC in het domein, de gebruikersnaam en tijd van aanmelding naar een tekstbestand op de PC worden weggeschreven.

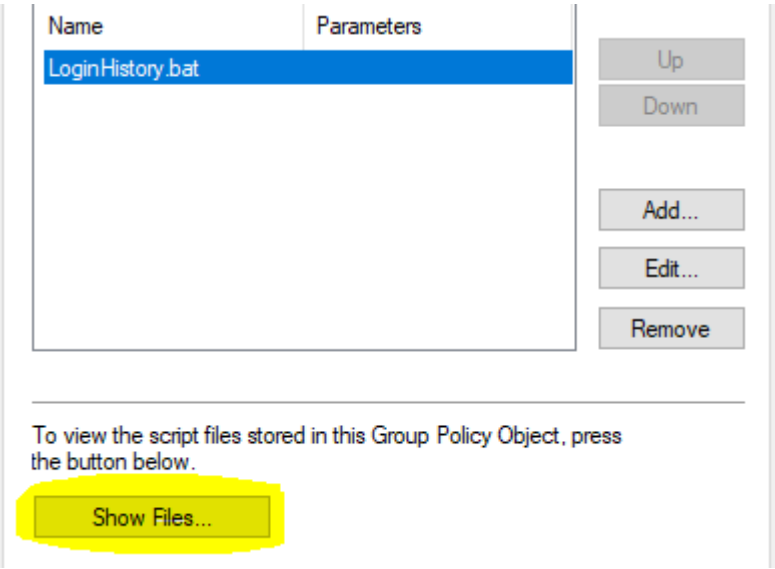
> Om een .bat file te maken in File Explorer zal je onder View de optie 'File name extensions' moeten aanzetten. Dan kan je een txt document maken en de naam wijzigen naar een .bat file. Deze file bevat uitvoerbare instructies die Windows zal uitvoeren in de achtergrond alsof je deze zou typen in CMD.

Je kan voor deze oefening het volgende .bat script gebruiken:

```
echo %username% - %date% %time% >> C:/Users/%username%/LoginHistory.txt
```

Om het script te laten uitvoeren door een gebruiker zijn er een aantal vereisten:

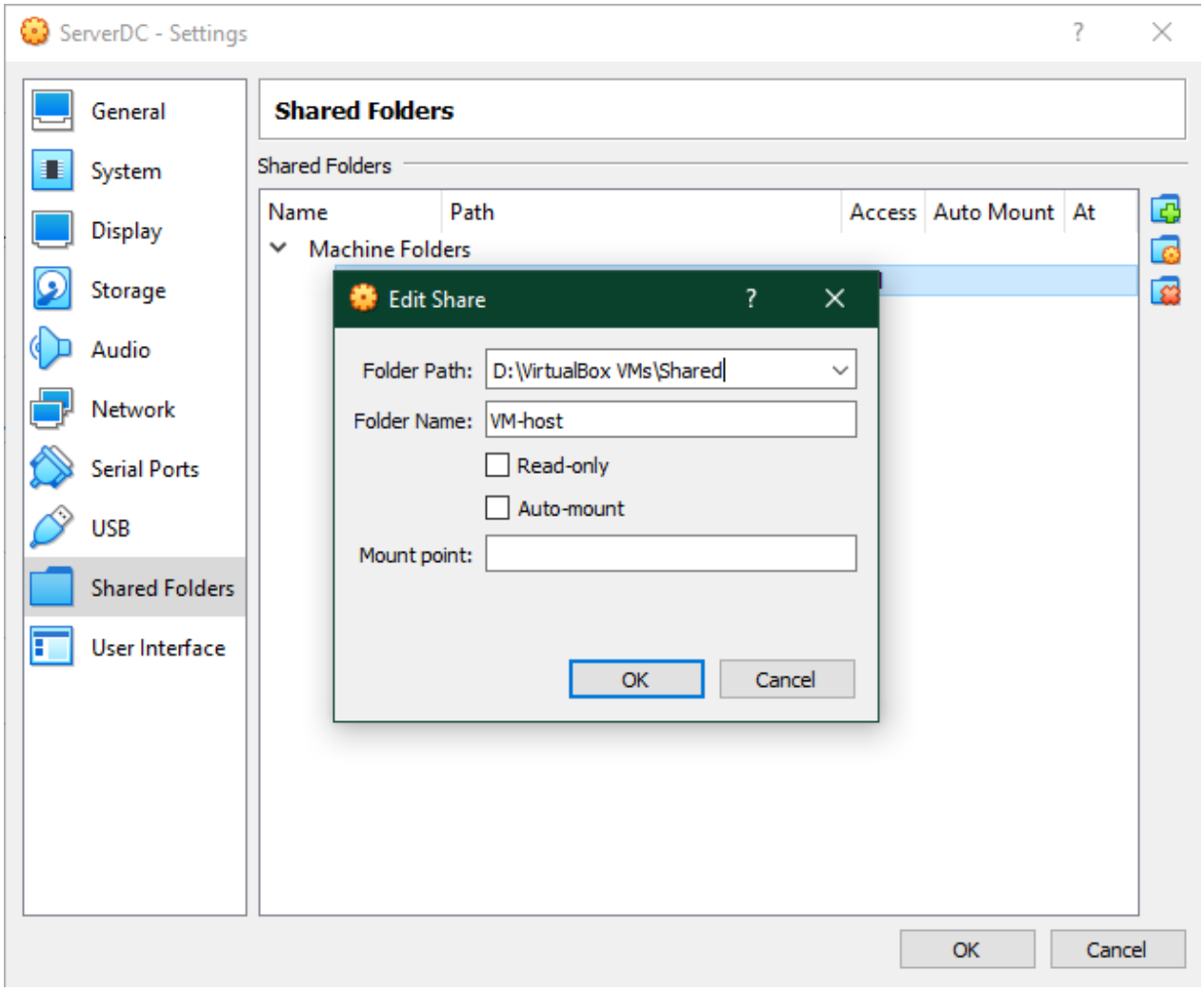
- De gebruiker moet toegang hebben tot het command prompt.
- De gebruiker moet schrijf-toegang hebben tot de folder waarnaar je de lijn schrijft. Vandaar in het script hierboven het pad `C:/Users/%username%/`. Omdat de gebruiker hier normaal gezien toegang tot heeft.
- Het script moet bereikbaar zijn voor de gebruiker over het netwerk. Dit kan je nakijken in File Explorer op je Windows 10 machine door te navigeren naar `\\COSCIDC1` en zo verder tot je aan je file geraakt. De eenvoudigste manier hiervoor is om je script te plaatsen in `Logon Scripts > Show Files ...`.



Installatie van programma's

Standaard hebben domeingebruikers geen rechten om programma's te installeren op een pc. Vaak wil men echter toch kunnen toelaten dat de gebruiker bepaalde software kan installeren, zonder hem toe te laten om eender welke software te installeren. Ook hier kunnen GPO's gebruikt worden om in te stellen welke programma's de gebruikers mag installeren op een client-pc.

Als voorbeeld nemen we de installatie van putty. Download het msi-bestand (de installer) van putty en plaats deze in een shared folder. Het gemakkelijkste hiervoor is om een shared folder in VirtualBox aan te maken en deze aan beide VM's te koppelen met als naam `VM-host`.



Om je VM's deze shared folder als een extra drive op te nemen zal je in je VM onder Devices `Insert Guest Additions CD image...` moeten activeren. Herstart je VM en je zal als D drive een folder zien met installers in. Installeer Guest additions en herstart opnieuw. Kijk na of je nu een extra drive ziet met naam `VM-host`.

Als eerste, login op een niet-administrator account, start dit *msi-bestand* op de Windows 10 VM. Volg de setup wizard (laat de standaard waardes telkens ongemoeid) en blijf doorklikken tot de installatie daadwerkelijk begint. Op dat moment zal je een loginvenster krijgen waarin je je moet aanmelden als een administrator. Dit komt omdat het setup-programma aanpassingen moet maken die voor normale gebruikers niet toegelaten zijn (bijv. het kopiëren van bestanden naar C:\Program Files). Annuleer de installatie. We willen dus voorkomen dat de gebruiker als administrator moet inloggen wanneer de gebruiker dit programma installeerd.

Open nu het groepsbeleidsbeheer op de domain controller, en maak een nieuwe GPO onder de OU=ICT met de naam “Software installeren”. Bewerk de GPO en ga naar User Configuration, Policies, Software Settings, Software installation. Rechterklik, en kies New, Package. Als bestandsnaam vul je het pad naar het gedeelde bestand in (bijv. \VBoxSvr\putty-64bit-0.74-installer.msi). Klik op Open.

In het volgende scherm krijg je de keuze hoe je de software wil distribueren. Standaard staat **Published** geselecteerd, wat wil zeggen dat de gebruiker kan kiezen of hij de software wil installeren of niet. De optie **Assigned** betekent dat de gebruiker niet kan kiezen, en dat de software automatisch geïnstalleerd wordt. Kies Published en klik OK. Dit kan even duren. Als het package verschijnt, sluit de groepsbeleidsbeheer editor af.

Log in op de Windows 10-machine als een gebruiker in de OU=ICT. Ga via het Control Panel naar Programs, Programs and Features, Install a program from the network. In deze lijst zie je nu het programma putty staan en kan je het zonder probleem installeren (ook zonder beheerdersrechten).

Delegatie

Voor grote domeinen kan er veel werk zijn om alle gebruikers en instellingen te beheren. Normaal is dit de taak van de systeembeheerders, maar soms kan het zijn dat de beheerders een aantal taken willen doorgeven aan anderen (zonder die andere gebruikers daarvoor de volledige beheerdersrechten te geven). Active Directory ondersteunt dit scenario door middel van *delegatie*.

Ga naar Active Directory Users and Computers, rechtsklik de gepaste OU=HR en kies *Delegate Control…* . Voeg via de wizard de juiste groep (IT-admins) toe en laat toe dat deze groep nieuwe gebruikersaccounts kan maken, verwijderen en beheren.

Log op de Windows 10-machine in als een gebruiker in de groep IT-admins en ga via het start menu naar *Windows Administrative Tools*, Active Directory Users and Computers. Probeer een nieuwe gebruiker aan te maken onder de OU=HR; lukt dit? Waarom niet? Wat moet je doen om het wel te laten lukken? Doe dit nu en test opnieuw. Wanneer je hetzelfde probeert onder de OU=Lectoren dan zal je zien dat dit niet lukt (aangezien de gebruiker hier geen rechten voor heeft).

Overname blokkeren of niet

In een GPO kan "Block inheritance" ingesteld worden. Hierdoor worden de instellingen van een hoger niveau NIET toegepast, we beginnen weer met een “schone lei”. Hierop is evenwel één uitzondering: op een (ouder-)GPO kan ook “Enforced” gespecifieerd worden. Het gevolg is dan dat de instellingen lager in de hiërarchie (ook indien er een "Block inheritance" tussen staat) niet meer van toepassing zijn.

Maak zelf een demo-oefening om dit te testen/demonstreren. Tip: Remove Recycle Bin icon from Desktop.

Wat moet je na dit labo kennen/kunnen

- Je weet en kan uitleggen/toepassen dat GPO op verschillende niveaus toegepast kunnen worden, nl. domein, site, ou
- Binnen een OU kan je GPO's in de juiste volgorde zetten
- Binnen een domein kan je GPO(s) in de juiste volgorde zetten
- Je kan policy- en preference-regels toepassen
- Je kan uitzoeken waarom een beleidsregel (policy/preference) niet toegepast is voor een gebruiker/computer met behulp van gpresult
- Je weet en kan het verschil uitleggen tussen de twee delen waaruit een GPO bestaat *Computer Configuration* en *User Configuration*
- Je kan eenvoudige taken binnen "AD Users en Computers" delegeren naar een AD-gebruiker of een AD-groep
- Je kent het concepte "Block inheritance" bij een GPO en kan dat uitleggen