VDAB
TRAINING & OPLEIDING

Samen sterk voor werk

Windows Server Administration

Gebruikersomgeving

Inhoud

1 DE GEBRUIKERSOMGEVING

In het onderdeel File server heb je geleerd hoe je bedrijfsdata kan delen over het netwerk. Deze data moeten toegankelijk zijn voor alle of een aantal medewerkers. Er is echter ook een deel van de data dat enkel toegankelijk moet zijn voor één enkel individu. We hebben het dan over de data en gebruikersinstellingen die standaard gestockeerd worden op het lokale toestel van de gebruiker.

Lokale data en gebruikersinstellingen:

- De folder *Documents*: bevat de persoonlijke bestanden van de gebruiker
- De *desktop*: bevat documenten en shortcuts van de gebruiker
- *Favorieten*: de favorieten uit Internet Explorer of andere browsers
- De folder *Appdata*: bevat applicatie instellingen en configuratie bestanden
- *Ntuser.dat*: de registry hive die instellingen bevat van de gebruiker

De gebruiker stelt hoge eisen aan de toegankelijkheid van zijn data. Zo wil hij dat zijn data aanspreekbaar zijn niet enkel vanop zijn vast toestel, maar ook vanop een toestel uit eender welke vergaderzaal of vanop eender welk bedrijfstoestel in het gebouw of op verplaatsing vanop de laptop, zonder daarbij met een usb stick in de weer te zijn om de data te kopiëren van het ene naar het andere toestel.

Deze data zijn in vele gevallen zeer belangrijke data voor de gebruiker, wat wil zeggen dat er een systeem dient ingebouwd te worden om de data te beschermen tegen:

- beschadiging door bijvoorbeeld een hardware probleem
- het per ongeluk verwijderen van gegevens
- het in handen vallen van andere gebruikers

Oplossing:

- Centraal aanspreekbaar maken. De data zullen niet langer bewaard worden op het lokale toestel van de gebruiker maar wel op een netwerk locatie[1]. Op die manier zijn de data vanop eender welke locatie aanspreekbaar. Laptopgebruikers kunnen via offline files de data lokaal opslaan.
- Security voorzien. Zowel lokaal als op de netwerklocatie zal de ACL enkel de gebruiker rechten geven om zijn data aan te spreken.
- Backup. Door de data te bewaren op een netwerklocatie worden de data mee opgenomen in de backuputility van de server.

[1] En bij uitbreiding de cloud. Daarop wordt in deze module niet verder ingegaan.

Naast eigen data moet de gebruiker eender waar in het netwerk op eender welk toestel zijn gedeelde mappen kunnen aanspreken, zonder dat de gebruiker iedere keer opnieuw mappings moet leggen. Ervan uitgaande dat niet iedere gebruiker weet hoe hij een mapping moet leggen kan dit een tijdrovende bezigheid worden voor de netwerkbeheerder. Scripts kunnen daar een uitkomst bieden.

Naast de data van de gebruiker zijn ook de bureaubladinstellingen, favorieten, templates en voorkeursinstellingen van groot belang. Kort samengevat: het profiel van de gebruiker. Om het computergebruik van de gebruiker zo aangenaam en efficiënt mogelijk te maken wordt ervoor gezorgd dat zijn profiel op eender welk toestel binnen de organisatie aanwezig is. Roaming profiles en folder redirection bieden hier een oplossing.

Homedirectories, roaming profiles, scripts en folder redirection bieden samen met group policies tools om de omgeving centraal in te stellen en beheren.

In het eerste hoofdstuk komen homedirectories, roaming profiles en logon scripts aan bod. Dit zijn de oudere manieren om een gebruikersomgeving te organiseren. Vandaag zijn er ook group policies die analoge resultaten opleveren. Die komen in de volgende hoofdstukken aan bod.

2 HOMEDIRECTORIES, ZWERVENDE PROFIELEN EN LOGONSCRIPTS

2.1 Persoonlijke documenten overal beschikbaar maken

Persoonlijke documenten worden beter niet opgeslagen op de lokale computer, maar op een bepaalde plaats op een server. Voordelen zijn dat gebruikers altijd aan hun persoonlijke documenten kunnen, ook als ze op een andere client aanmelden en dat bij het maken van backups meteen ook een backup kan gemaakt worden van de persoonlijke documenten van alle gebruikers en dit zonder al te veel extra moeite.

De kans is groot dat gebruikers hun bestanden wegschrijven in de folder Documents. Deze folder wordt standaard opgeslagen op de lokale computer van een gebruiker.

Dit probleem kan op 2 manieren opgelost worden:

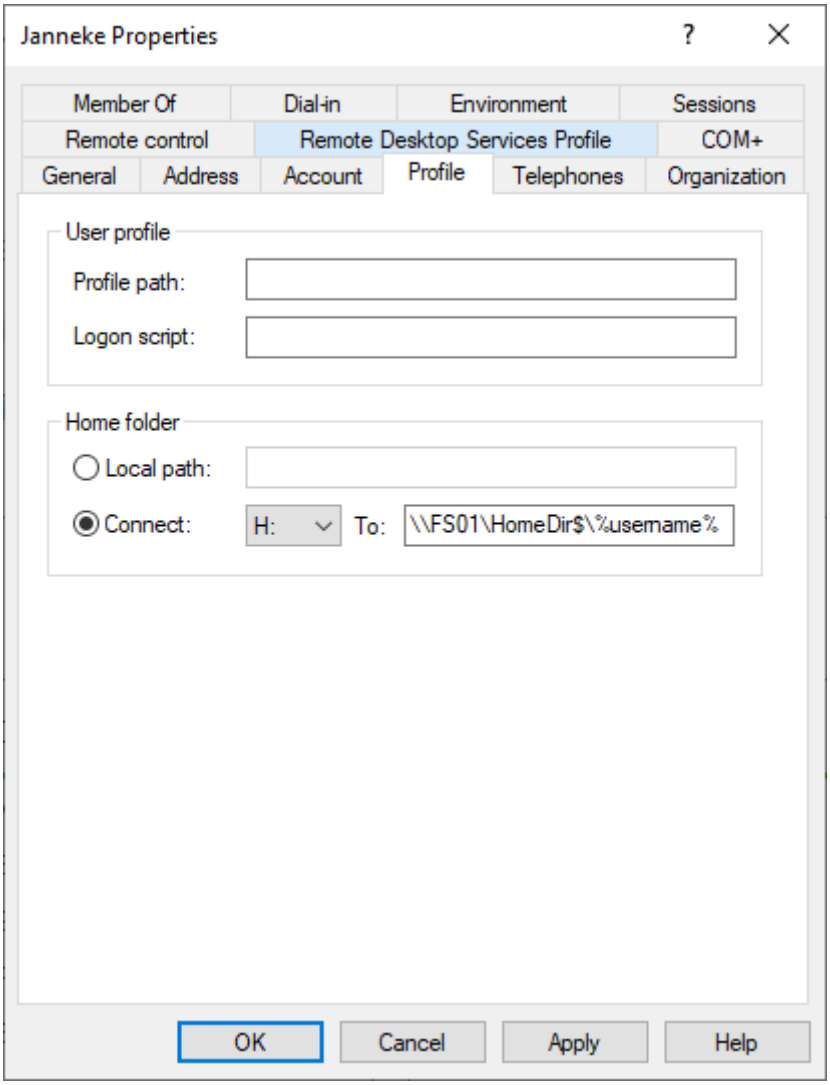
1. Via Homedirectories
2. Via Folder Redirection

Een Home directory is een plaats op een server die toegekend wordt aan een bepaalde user. Home directories worden niet gekopieerd tijdens het aanmelden, waardoor het aanmelden minder tijd in beslag neemt.

Folder redirection verplaatst de inhoud van de systeemmap Documents naar een bepaalde locatie op een server. Dit komt aan bod in het hoofdstuk Group policies.

Werkwijze voor het maken van homedirectories:

- Maak een map aan op de data schijf van een server waar de homedirectories zullen bewaard worden. In de verdere uitleg wordt ervan uitgegaan dat je de map HomeDir aanmaakt op de dataschijf van FS01.
- Deel de map homedir. Doe dit best met een verborgen share bv HomeDir$.
- Pas de toegangsrechten bij Sharing zo aan dat Everyone Full Control krijgt en verwijder bij Security de groep Users. Het resultaat is dat tot deze map Administrators, Creator owner en System toegang hebben.
- Ga via de Server manager naar Active Directory Users and Computers.
- Dubbelklik op de account en selecteer de tab **Profile**.
- Activeer de optie **connect**, kies een letter in de lijst die nog niet gebruikt wordt voor één of andere mapping en vul de server, sharenaam en de te gebruiken directory in de share, maw \\<servernaam>\HomeDir$\%username%.



Dit heeft drie gevolgen:

- In de map HomeDir op de server wordt automatisch een homedirectory aangemaakt voor de gebruiker.
- Er worden toegangsrechten op die homedirectory ingesteld, zodat alleen de administrators, de creator owner, het systeem en de gebruiker toegang hebben tot de map.
- Als de gebruiker zich aanmeldt op een client toestel krijgt hij meteen een mapping naar zijn homedirectory.

Opmerkingen:

- Het is gebruikelijk de letter H: te kiezen voor een homedirectory (op voorwaarde dat die nog niet in gebruik is). Dit is zeker geen verplichting
- %username% is een systeemvariabele die verwijst naar de gebruikersnaam.

Tip: je kan voor meerdere users tegelijk de homedirectory instellen door alle users in de OU te selecteren en in het snelmenu van de selectie properties te kiezen. Via het tabblad profile stel je dan de locatie van de Home folder in met de variabele %username%.

Voorbeeld

- Geef de gebruiker Janneke een homedirectory.
- Stel vast dat er onmiddellijk in de map HomeDir een map met de naam van de account wordt aangemaakt en bekijk de toegangsrechten tot de map.
- Meld daarna aan met de account Janneke op het clienttoestel en stel vast dat Janneke een mapping naar haar homedirectory gekregen heeft.

2.2 Profielen

2.2.1 Wat is een profiel?

Een profiel is een verzameling gebruikersinstellingen, waaronder bureaubladkenmerken, zoals lettertypen, achtergronden en kleurenschema's, evenals printer- en netwerkverbindingen.

Het profiel heeft als doel een vertrouwde werkomgeving te creëren voor een gebruiker. Zodra gebruikers zich aanmelden bij een toestel verwachten ze bv. de vertrouwde achtergrond, pictogrammen op hun vaste plaats op het bureaublad en favoriete websites in hun browser terug te vinden

Alle configuratie instellingen die een gebruiker maakt worden weggeschreven in zijn persoonlijk profiel.

2.2.2 Lokale gebruikersprofielen

Zonder verdere configuratie wordt een lokaal profiel aangemaakt de eerste keer een gebruiker zich aanmeldt op een toestel.

Je vindt de lokale profielen terug onder %systemdrive%\Users\%username%

Bekijk de lokale profielen op de client computer.

Lokale profielen zorgen er bijvoorbeeld voor dat als een gebruiker een bepaalde achtergrond instelt, die gebruiker de volgende keer dat hij/zij zich aanmeldt op diezelfde computer, opnieuw de aangepaste achtergrond krijgt.

Alle aanpassingen aan hun werkomgeving die gebruikers uitvoeren worden bij het afloggen weggeschreven naar hun persoonlijk profiel.

Lokale profielen treden in werking als gebruikers zich niet op het domein aanmelden of zolang er nog geen zwervende profielen zijn ingesteld.

In de Users Folder tref je twee bijzondere gebruikers folders aan: Default (verborgen) en Public.

Default

Bij het aanmaken van een nieuw profiel wordt er vertrokken van het default user profiel dat terug te vinden is op het lokale toestel of in de NETLOGON share van de domain controller. Hierover later meer.

Public

Documenten, muziek, video's,… bestanden die door alle gebruikers van de computer met elkaar gedeeld worden, worden opgeslagen in de Public Folder. Dit profiel wordt net zoals het All Users profiel nooit geladen als een actief profiel.

- Ga op zoek naar het lokale profiel op de client van Janneke en bekijk de inhoud.

2.2.3 Zwervende profielen/roaming profiles

Voor het comfort van gebruikers kan het van belang zijn dat hun profiel hen volgt bij gebruik van een andere computer in het domein. Dit wordt bereikt met zwervende profielen.

De instellingen van gebruikers die een zwervend profiel hebben worden de eerste keer dat ze zich aanmelden nog altijd lokaal weggeschreven (zoals beschreven in de vorige paragraaf). Zodra gebruikers met een zwervend profiel zich afmelden, worden de wijzigingen automatisch op een opgegeven locatie op een server opgeslagen. Bij een volgende aanmelding op hetzelfde toestel of op een ander toestel, worden de instellingen van de server gekopieerd en lokaal gebruikt totdat de gebruiker zich afmeldt. Op dat ogenblik wordt het profiel opnieuw naar de server geschreven.

Om met zwervende profielen te werken, maak je een gedeelde directory op een server waarin profielen van gebruikers kunnen opgeslagen worden. Daarna pas je de gebruikersaccounts zo aan dat ze het profiel ophalen uit deze gedeelde directory.

Zwervende profielen gebruiken:

- Maak een map aan op het datavolume van een server. De profielen zullen in die map bewaard worden. We kiezen voor het vervolg van de uitleg een map profielen op de dataschijf van FS01.
- Deel deze map. Je doet dit best met een verborgen share b.v. profielen$.

Voor een goede werking van de zwervende profielen is het belangrijk dat de toegangsrechten tot de map correct ingesteld zijn.

- Geef bij Sharing Everyone het recht Full Control op de map profielen.

- Schakel de inheritance van rechten uit en geef via **Security** > **Advanced** de rechten **List Folder / Read data** en **Create Folders / Append data** aan de groep Users op **This folder only**.
- Ga via de Server manager naar Active Directory Users and Computers.
- Dubbelklik op een account en klik op de tab **Profile**.
- Geef in het tekstvak **Profile Path** de server, sharenaam en de te gebruiken directory op. Via de %username% variabele wordt steeds de usernaam gebruikt om het profiel te bewaren.
  in ons voorbeeld wordt dat: \\FS01\profielen$\%username%
- Klik op OK

Opmerking: in dit voorbeeld wordt enkel voor 1 user een zwervend profiel ingesteld. Je kan ook voor meerdere personen tegelijk het profiel aanmaken. Selecteer daarvoor in de OU alle users die je een profiel wenst te geven en klik dan met de rechtermuisknop in de selectie. Kies **properties** uit het snelmenu. Via het tabblad **Profile** kan je het **profile Path** opgeven met \\servernaam\profielen$\%username%. %username% wordt dan herleidt naar de usernaam. Iedere user krijgt een folder met zijn naam in de share profielen$.

Een voorbeeld

Geef Janneke een zwervend profiel.

- Meld aan op het client toestel met Janneke. Doe een paar aanpassingen aan de desktop en meld opnieuw af.
- Bekijk op de server de inhoud van de share profielen$. Daarin is nu voor Janneke een folder aangemaakt. Ten gevolge van de rechten (enkel de user heeft rechten op zijn profiel) zal je als administrator dit profiel niet kunnen inkijken. Later meer hierover.

Opmerking: Gebruikersprofielen aangemaakt met verschillende versies van de Windows client zijn niet compatibel. Een profielmap aangemaakt met een Windows 10 client herken je aan de karakters V5, V6... achteraan. Een profiel aangemaakt via een Windows 7 client krijgt dan weer V2 achteraan. Als dezelfde gebruiker verschillende versies van het besturingssysteem gebruikt vanop verschillende toestellen, dan wordt automatisch het aangepaste profiel geladen.

Bij gebruik van zwervende profielen, heeft een gebruiker dus met ten minste twee profielen te maken: één dat lokaal op het toestel staat en één dat op de server staat. Het lokale profiel is nuttig als het netwerk niet beschikbaar is. Het profiel op de server kan van op eender welk toestel gebruikt worden, een nadeel is dan weer dat bij het aanmelden het profiel volledig gekopieerd wordt van de server naar het lokale toestel en dat dit enige tijd in beslag kan nemen.

Als er een verschil ontstaat tussen het lokale profiel en het profiel dat op de server bewaard wordt zal het systeem vragen welk profiel gebruikt moet worden.

2.2.4 Administrators kunnen niet bij profielen

Wanneer een gebruiker zich voor de eerste keer aanmeldt en een zwervend profiel wordt gecreëerd, worden de beveiligingen niet geërfd van een hoger niveau maar krijgen alleen het systeem en de gebruiker toegang. Een administrator kan dus ook niet bij het profiel van een andere gebruiker. Een policy lost dit probleem, indien nodig, op.

Pas de Default Policy ter hoogte van het domein als volgt aan:

Computer Configuration > **Administrative Templates** > **System** > **User Profiles**

De policy die je zoekt is **'Add the Administrators security group to roaming user profiles'**.

Opmerking: Group policies zijn nog niet aanbod gekomen, maar worden besproken in hoofdstuk 3 Group Policies/groepsbeleid, de theorie en in hoofdstuk 4 Computerbeheer en Userbeheer met GPO's, de praktijk.

2.3 Loginscripts

Loginscripts zijn een beproefde manier om de gebruikersomgeving te configureren. Ze vinden hun oorsprong in het pre-microsoft tijdperk.

Deze scripts kunnen drive mappings maken naar shares op de server, lokale poorten doorsturen om printers toe te wijzen, de systeemklok gelijk zetten, enz....

Een logonscript kan gekoppeld worden aan een gebruiker via de properties van de gebruikersaccount, tabblad Profile of via group policies.

In dit eerste hoofdstuk wordt een loginscript gekoppeld aan de properties van de gebruikersaccount. In het volgende hoofdstuk komen de scripts in combinatie met Group policies aan bod.

2.3.1 Bat/cmd files

De Bat/cmd files dateren al van in het Windows NT tijdperk. Iedere netwerkbeheerder kent ze wel. Als voorbeeld een script om drives te mappen. Aan de command prompt gebeurt dit met de opdracht **net use**.

De syntaxt van dit commando ziet er als volgt uit:

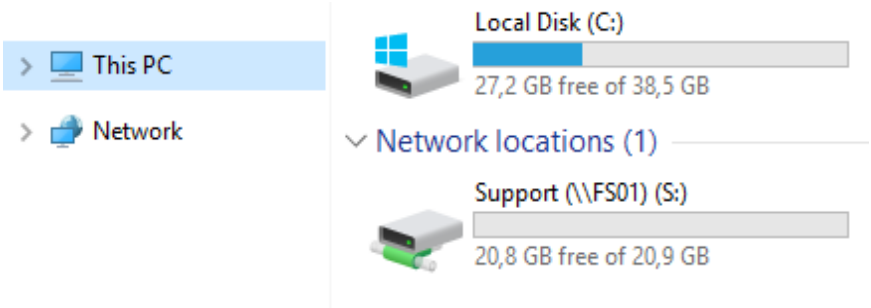
net use [{DEVICE | *}] [\\COMPUTER\SHARE[\VOL]] [{PASSWORD | *}]] [/USER:[DOMAIN\]USER] [/USER:[DOTTEDDOMAIN\]USER] [/USER:[USER@DOTTEDDOMAIN] [/SAVECRED] [/SMARTCARD] [{/DELETE | /PERSISTENT:{yes | no}}]

Werkwijze:

- Open **Notepad**
- Gebruik het net use commando voor iedere drive die je wenst te mappen.

Voorbeeld:

- Maak een map Trajecten op de dataschijf van **FS01.**
- Maak daaronder een map Support en deel die.
- Maak (op de domeincontroller) een .bat script om de map te mappen naar de letter S:
  Net use S: \\FS01\Support
- Bewaar het script in de map
  c:**windows\sysvol\sysvol\<domeinnaam>\scripts**
  met als extensie bat. Bijvoorbeeld: logon.bat.
  Opmerking: zowel de locatie als de extensie zijn van belang!
- Koppel vervolgens het script aan een gebruiker, b.v. Janneke:
  Ga via de Server manager naar **Active Directory Users and Computers**. Rechtermuisklik op de user, kies voor properties en ga naar het tabblad **Profile**. Voer de naam van het script in bij **Logon script**. Dit gebeurt zonder path aanduiding, vandaar het belang om het script op de juiste locatie op te slaan.
- Test uit! Log op het werkstation in met de useraccount. Ga naar **This PC**. Als alles goed is verlopen zie je nu de gemapte drive onder **Network Locations**.



2.3.2 Vbscripts

De manier van werken is vergelijkbaar met deze voor de BAT files. Het enige verschil is het script zelf.

Een VBscript om een map met sharenaam Infrastructuur te mappen kan zijn:

```
DIM WSHNetwork
```

```
Set WSHNetwork = CreateObject("Wscript.network")

WSHNetwork.Mapnetworkdrive "I:", "\\FS01\Infrastructuur", true
```

Dit script mapt een folder met **sharenaam Infrastructuur** op de **server FS01** naar de **driveletter I:**.

Het Vbscript wordt eveneens bewaard op de domeincontroller in de folder c:\windows\sysvol\sysvol\<domeinnaam>\scripts. Het script krijgt als extensie vbs. Bijvoorbeeld infrastructuur.vbs.

- Maak onder de map Trajecten op FS01 een map Infrastructuur en deel die.
- Map ze voor de gebruiker Jip via een .vbs logonscript.
- Opm.1: Indien je de code van hierboven copieert naar het script op je server, dan kan het zijn dat je daar de aanhalingstekens (“) moet vervangen.
- Opm.2: Indien bovenstaande commando’s een tweede keer uitgevoerd worden, zal je een foutmelding krijgen dat de mapping al bestaat (“The local device name is already in use”). Wil je dat vermijden, dan moet je deze oplossing eens bekijken.

2.3.3 PowerShell

Bij het deel logonscripts met group policies bekijken we ook eens hoe je een mapping kunt maken naar een gedeelde map met een PowerShell script.

3 GROUP POLICIES/GROEPSBELEID, DE THEORIE

3.1 Overzicht

Een belangrijk aspect bij de informatisering van een bedrijf is de totale kost van die informatisering. De voornaamste kosten zijn niet de aankoop van de computers maar de vele uren werk die naar het onderhoud en beheer gaan.

De mogelijkheid om een computerpark centraal te beheren kan een belangrijke besparing van kosten en tijd betekenen. Group policies bieden de mogelijkheid om clienttoestellen centraal te configureren. Zo kan je bijvoorbeeld de inhoud van de desktop en het startmenu bepalen, software installeren, browser instellingen meegeven, folders hermappen, mappings leggen, toegang verlenen of afnemen van bepaalde programma's, enz… en dat allemaal vanuit AD.

3.2 Instellingen beheren via GPO's?

De interface om GPO's te beheren open je via Server Manager > Tools > Group Policy Management.

Onder de node "Group Policy Objects" vind je twee policies die tijdens de installatie werden aangemaakt: de **Default Domain Policy** en de **Default Domain Controllers Policy**.

- Klik in het context **menu** van de Default Domain Policy op **Edit** om de group policy editor te openen.

De instellingen in GPO's zijn onderverdeeld in twee grote groepen:

1. **Computerinstellingen** worden doorgevoerd bij het opstarten van de computer en zijn dus van toepassing voor eender welke gebruiker die zich aanmeldt aan het toestel.
2. **Gebruikerinstellingen** worden doorgevoerd op het ogenblik dat een gebruiker zich aanmeldt.

Hieronder een kort overzicht van de instellingen die via group policies kunnen gegeven worden. Klik de nodes open om de bijbehorende instellingen terug te vinden.

Configuratie optie	Werking
Software installatie en beheer	Software kan centraal van op de server op clients geïnstalleerd en verwijderd worden, dit geldt zowel voor applicaties als voor patches en upgrades.
Scripts	Naast logonscripts kan je via policies ook logoff, start up en shutdown scripts laten uitvoeren. In

	een script kunnen opdrachten opgenomen worden voor de command prompt. Een script kan ook geschreven worden in vbscript of jscript en wordt in dat geval uitgevoerd via de Windows scripting host. Een PowerShell script behoort ook tot de mogelijkheden.
Folder redirection	Het aanmaken van homedirectories op de server kan vervangen worden door het verwijzen van de map My Documents naar de server. Het opslaan van profielen op de server kan dan weer door het start menu, de desktop of de application data te verwijzen naar de server. Dit alles gebeurt transparant voor de gebruiker.
Beveiligingsinstellingen	Beveiligingsinstellingen configureren kan ook via grouppolicies. Sommige instellingen, zoals de eigenschappen van wachtwoorden en accounts, moeten ter hoogte van het domein ingesteld worden. Andere instellingen zoal firewall instellingen, kunnen ter hoogte van elke OU gekoppeld worden.
Administrative Templates	Worden gebruikt om registry waarden in te stellen die b.v. wijzigingen die gebruikers kunnen doorvoeren op de configuratie van hun computer beperken.
Instellingen voor Internet Explorer	Via de GPO's beheer je de menu's, taakbalken, verbindingen, favorieten, beveiligingsinstellingen en standaard internet instellingen.
Preferences	Preferences bieden de mogelijkheid om een groot aantal opties van de Windows settings en Control panel settings te beheren, zoals: drive mappings, omgevingsvariabelen, netwerk shares, lokale users en groepen, services, devices enzo…
Printers	Met GPO's kunnen administrators de installatie van printerdrivers delegeren naar andere gebruikers.
Blocking Device Installation	Je kan vanaf een centraal punt de installatie van devices binnen je netwerk blokkeren zoals bijvoorbeeld, USB drives, CD-RW drives , DVD-RW drives en andere verwijderbare media.

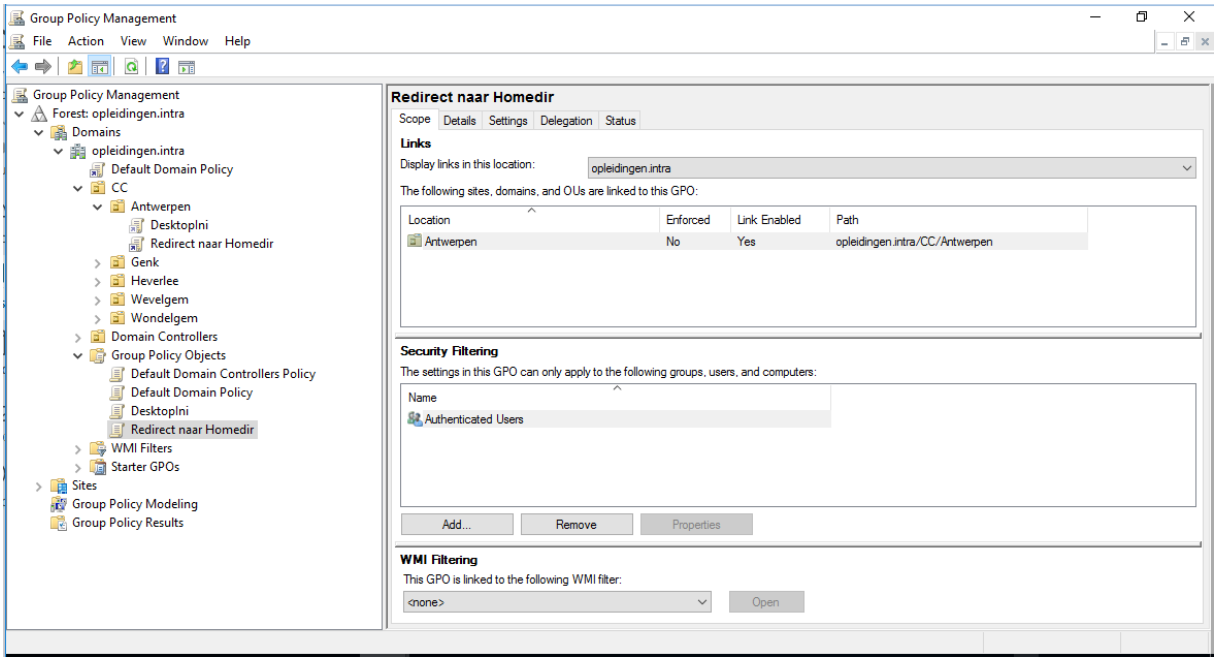
Power management settings	Power management is zeer kost besparend en kan dan ook via GPO's geactiveerd worden.

3.3 De Group Policy Management Console

GPO's kunnen beheerd worden via de Group Policy Management Console.

Er zijn twee manieren om die op te starten.

1. Via de **Server Manager** > **Tools** > **Group Policy Management**
2. Via **Start** > **Administrative Tools** > **Group Policy Management**



De Group Policy Management Console of afgekort GPMC toont ongeveer dezelfde structuur als de Active Directory maar dan met uitbreidingen naar Group Policies toe. Zo zal je bij ieder onderdeel van de active directory kunnen zien of er een Group Policy gekoppeld is of niet. Bijvoorbeeld onder de naam van het domein wordt de Default Domein Policy getoond.

De GPMC kan ook geïnstalleerd worden op een Client PC als onderdeel van de Remote Server Administration Tools (RSAT)[2]. Niet elke gebruiker kan natuurlijk vanaf zijn client PC de GPO's beheren dat kunnen alleen de gebruikers die daar de nodige rechten toe hebben.

Selecteer je een Policy dan krijg je rechts alle instellingen van die policy te zien, verdeeld over 5 tabbladen.

[2] Na installatie van RSAT op een client beschik je over de de administrative tools op die client.

Scope	Toont de security filtering en WMI Filtering. Hier bepaal je voor welke users, computers en groups de GPO moet uitgevoerd worden. Standaard zal er altijd Authenticated Users staan. Met een WMI filter bepaal je bijvoorbeeld voor welke clienttoestellen de GPO moet uitgevoerd worden. Bijvoorbeeld wel voor Windows XP toestellen en niet voor Windows Vista toestellen.
Details	Toont onder andere de aanmaakdatum en datum waarop een GPO werd aangepast, de versie van de GPO, of de GPO al dan niet geactiveerd is. Een GPO kan je hier in- of uitschakelen.
Settings	Op dit tabblad wordt een rapport gegenereerd met alle settings die voorkomen in de GPO. Het is soms heel moeilijk om via de GPO editor te zien wat er wel of niet is geactiveerd in een GPO, dan biedt dit tabblad een snelle oplossing.
Delegation	Toont de users en groepen die rechten hebben op de GPO.
Status	Hoe zit het met de replicatie op het domein?

3.4 GPO's creëren en beheren

3.4.1 Een nieuwe GPO maken

Om een GPO aan te maken ga je als volgt te werk:

- Klik met de rechtermuisknop in **Group Policy Management** op de node **Group Policy Objects** en kies **New** in het contextmenu.
- Geef de GPO een beschrijvende naam en klik op OK.

Voorbeeld

Maak een GPO met de naam **Blokkeer Control Panel en PC Settings**

3.4.2 Een bestaande GPO linken aan een container

Alle GPO's worden verzameld in de "Group Policy Objects" Container. Een GPO zal pas effect krijgen als hij ook nog gelinkt wordt aan een Organizational unit (OU).

Dit betekent enerzijds dat eenzelfde GPO aan meerdere OU's kan gelinkt worden.

Anderzijds zorgt dit ervoor dat wijzigingen aangebracht aan een GPO meteen van invloed zijn op alle OU's waaraan de GPO gelinkt is.

Een GPO linken aan een OU:

- Klik met de rechtermuisknop op de OU en selecteer **Link an Existing GPO**
- Selecteer de te linken GPO in de lijst en klik op **OK**

Voorbeeld

- Koppel de GPO ‘Blokkeer Control Panel en PC Settings’ aan de OU Genk

Opmerking

Het is ook mogelijk een GPO bij het aanmaken meteen te linken aan een OU. Kies daartoe in het contextmenu van de container **Create a GPO in this domain, and Link it here**.

3.4.3 De instellingen gedefinieerd in een GPO aanpassen

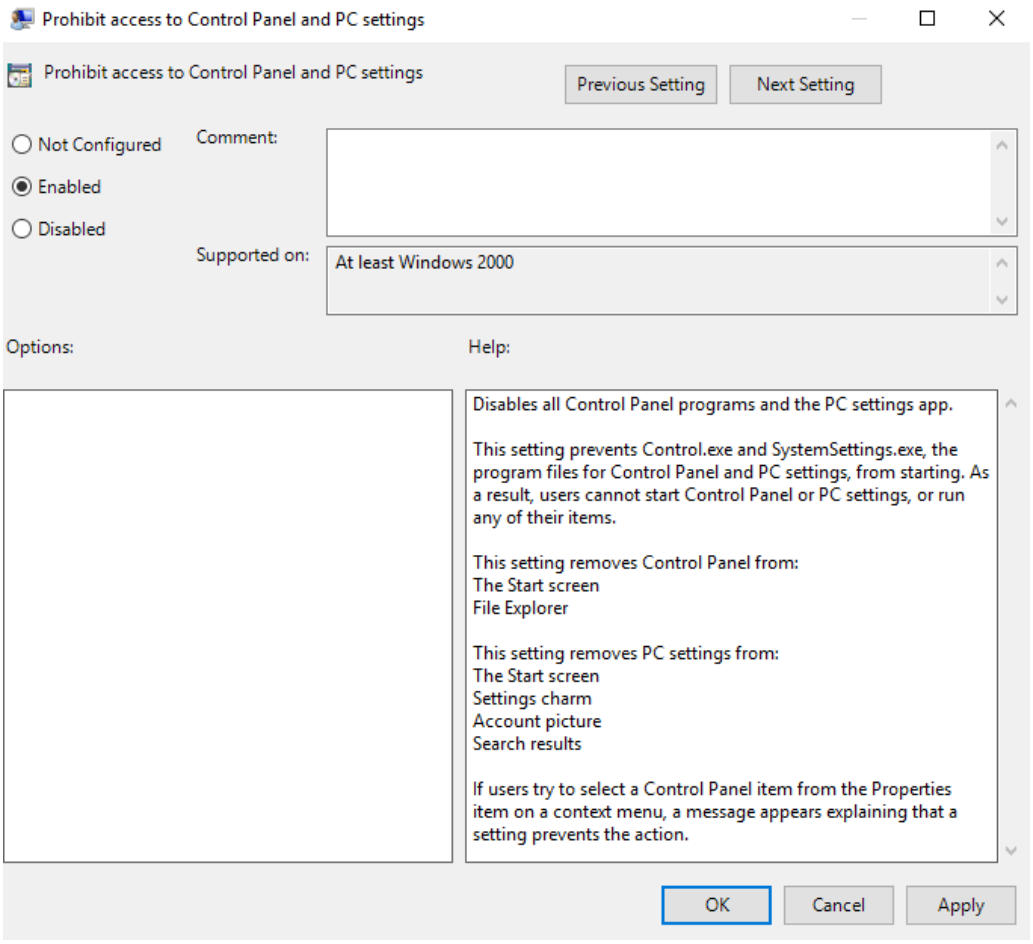
Eenmaal de GPO aangemaakt kunnen de instellingen aangepast worden.

- Kies Edit in het contextmenu van de GPO **Blokkeer Control Panel en PC Settings**. De Group Policy Editor wordt opgestart.

Zoals eerder vermeld zijn de instellingen in GPO’s onderverdeeld in 2 grote groepen: Computer Configuration en User Configuration.

Doel van de GPO **Blokkeer Control Panel en PC Settings** is het Control Panel te blokkeren voor gebruikers in de OU Genk.

- Ga naar **User Configuration** > **Policies** > **Administrative Templates** > **Control Panel**
- Dubbelklik op de Setting **Prohibit access to Control Panel and PC Settings**
- Selecteer **Enabled** en klik op **OK**



Heel wat GPO instellingen onder Administrative Templates werken met drie opties: Enabled, Disabled en Not Configured.

Enabled activeert de instelling, d.w.z. in dit voorbeeld dat gebruikers waarop de policy van toepassing is hun instellingen niet kunnen aanpassen via control panel / PC settings app.

Disabled schakelt de instelling uit. Ook als de instelling eerder op Enabled stond, dan wordt die hier op disabled gezet, in ons voorbeeld dat de gebruiker het control panel en de PC settings app kan gebruiken.

Not Configured betekent dan weer dat de policy niets wijzigt aan de toestand, ingeschakeld blijft ingeschakeld en uitgeschakeld blijft uitgeschakeld.

- 🛠 Sluit de Group Policy Management Editor.

3.4.4 De GPO testen

- 🛠 Maak een gebruiker in de OU Genk, meld aan met deze gebruiker en stel vast dat die het Control Panel niet kan openen en niet bij de opdracht Settings kan.
- 🛠 Verwijder de link met de OU Genk van de GPO

3.5 Types group policies

We onderscheiden lokale en AD Group policies.

3.5.1 Local group policy

Een local group policy bestaat op iedere computer. Deze policy wordt doorgevoerd bij het opstarten van de computer en is de enige die toegepast wordt op een computer die niet tot een domein behoort. Hij wordt ook toegepast op computers die wel tot een domein behoren maar wordt daarna meestal overschreven door de group policies gedefinieerd in de AD.

Het local Group Policy Object (GPO) wordt opgeslagen op de PC in de %systemroot%\System32\GroupPolicy folder.

Vanaf Windows Vista en hoger kan er meer dan 1 Lokale group policy ingesteld worden op één enkel toestel. Zo kan er een GPO ingesteld worden die enkel uitgevoerd wordt als een administrator aanlogt. Het omgekeerde kan ook dat een bepaalde GPO uitgevoerd wordt als er een non-administrator aanlogt of zelfs een GPO gekoppeld aan één bepaalde user. Iedere GPO bevat instellingen specifiek voor die user(s). Lokale GPO's vallen buiten het bestek van deze cursus. Meer informatie is terug te vinden in de cursus van PC beheer Windows.

3.5.2 AD group policy

AD group policies worden bewaard in de Active Directory (AD). Bij de creatie van een domein worden meteen twee default group policies gemaakt nl. de 'Default Domain Policy' en de 'Default Domain Controllers Policy'.

De Default Domain Policy regelt de account en de paswoord instellingen en kan ook gebruikt worden voor andere domeininstellingen.

De Default Domain Controllers Policy wordt gekoppeld aan de Domain Controllers OU en bevat o.a. de instellingen voor de beveiliging van de DC's.

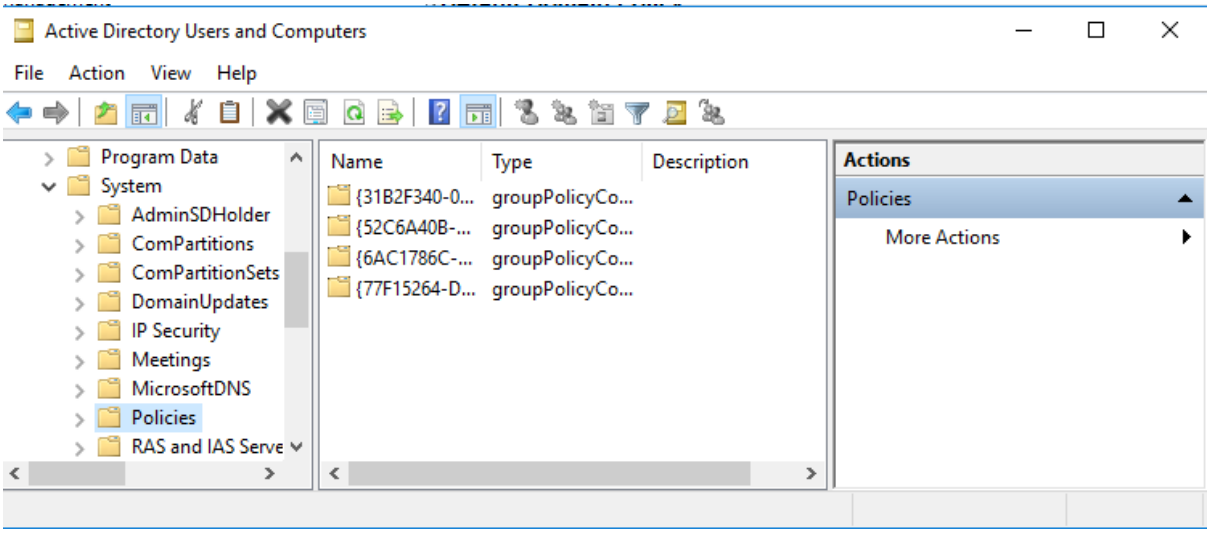
Opmerking: Let op met de default domain policy en de default domain controller policy. Dit zijn de 2 meest belangrijke GPO's. Probeer zo weinig mogelijk aan te passen in deze policies.

Daarnaast kan je nog extra GPO's creëren en die koppelen aan verschillende containers in de AD structuur, nl. aan een site, een domein of een OU in de organisatie.

Elk AD Group policy object (GPO) bestaat op zijn beurt uit twee verschillende objecten.

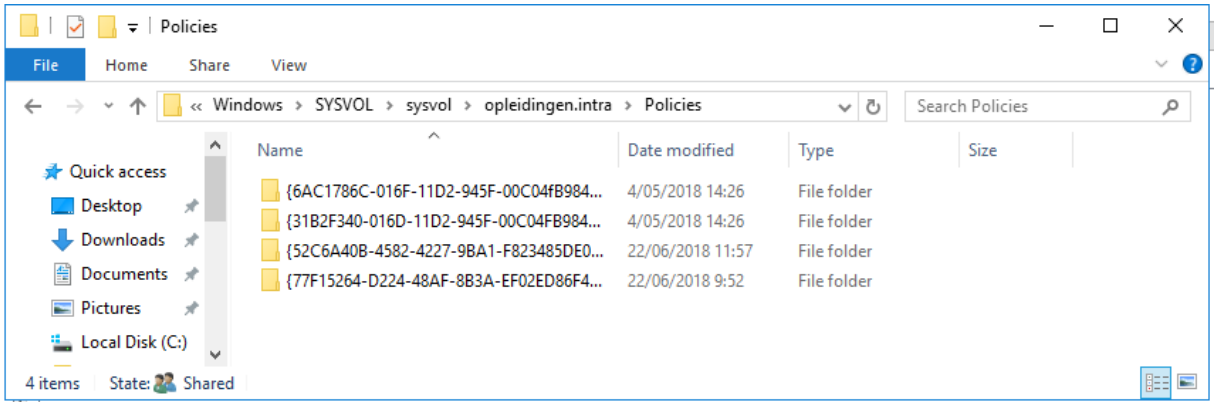
Eén ervan is de Group Policy Container (GPC). Die vind je in AD Users and Computers onder System > Policies (de System container wordt alleen getoond als View > Advanced features geactiveerd is). De GPC bevat de volgende informatie:

- **Versie informatie:** Onderhouden door zowel de GPC als de Group Policy Template om zeker te zijn dat de twee objecten gesynchroniseerd zijn.
- **Lijst van de componenten:** Lijst van de group policy instellingen die geconfigureerd zijn in deze GPO. (computer, gebruiker of beide)
- **Status informatie:** Is de GPO in of uitgeschakeld?



Opmerking: Zoals je ziet is het niet gemakkelijk om de GPC's te identificeren via de GUID's. (Globally Unique Identifiers). Via de eigenschappen van de GPC op het tabblad **Attribute Editor** vind je bij het attribuut displayName de naam van de GPO.

Het tweede object dat bij een group policy hoort, is de GPT (Group Policy Template). Die bevat het merendeel van de instellingen van de group policy en wordt bewaard in de Sysvol folder op de DC.



De inhoud van een Group Policy Template:

Folder locatie	Inhoud
Adm	Bevat de adm bestanden om de administrative templates te configureren.

Scripts	Bevat de scripts die toegewezen zijn aan de group policy.
User	Bevat alle registry instellingen die de policy toepast op de gebruiker. De instellingen worden opgeslagen in het Registry.pol bestand.
User\Applications	Bevat de applicatie scripts voor de applicaties die verspreid worden naar de gebruiker.
Machine	Bevat alle registry instellingen die de policy toepast op de computer. De settings worden opgeslagen in het Registry.pol bestand.
Machine\Applications	Bevat de applicatie scripts voor de applicaties die verspreid worden naar de computer.
{*GUID*}	Bevat het bestand, met het GPO versie nummer.

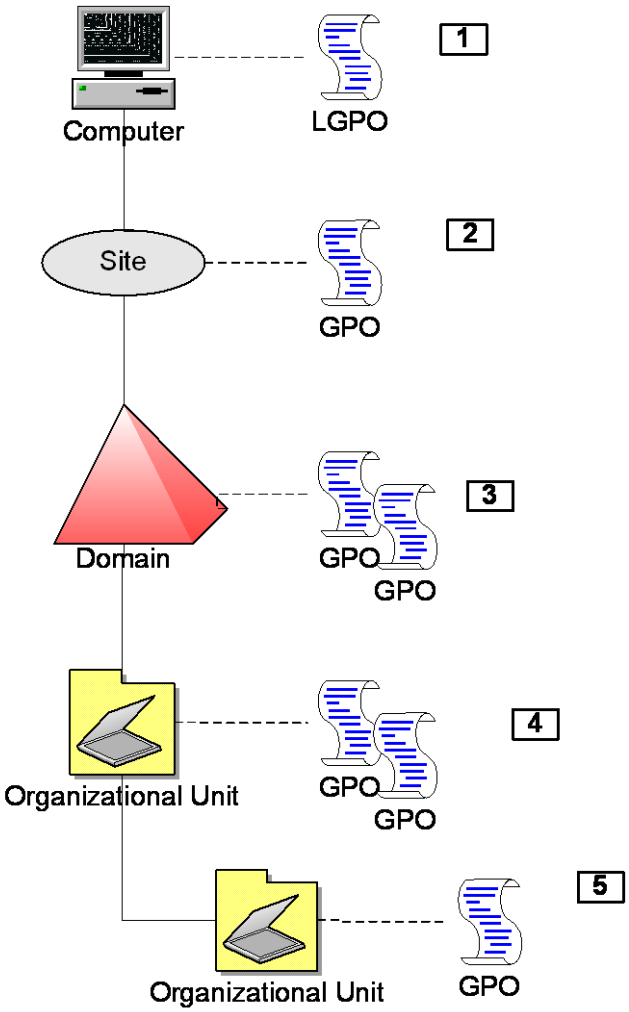
Beide GPO componenten worden gerepliceerd naar alle DC's in het domein.

Opmerking: Als je een GPO gemaakt of gewijzigd hebt, moeten de policies gerepliceerd worden naar de andere DC's in het domein. Belangrijk om weten is dat de 2 componenten van een GPO - GPC en GPT - verschilldende mechanismen gebruiken om te repliceren. De GPC repliceert als onderdeel van de Active Directory Replication. Bij GPT ligt dat iets ingewikkelder, het mechanisme is hier afhankelijk van het functional level van het domein. Als het gaat over een Windows Server 2008 functional level of hoger dan gebeurt de replicatie via de Distributed File System Replication Service (DFS-R). Bij een Windows Server 2003 of lager functional level gebeurt de replicatie via de File Replication Service (FRS).

3.6 In welke volgorde worden group policies toegepast?

Group policies werken met inheritance, d.w.z. dat group policies toegepast op een hogere container doorsijpelen naar onderliggende containers.

Alles start bij de LGPO's (Local Group Policy Objects) van de lokale computer. Die worden eerst uitgevoerd.



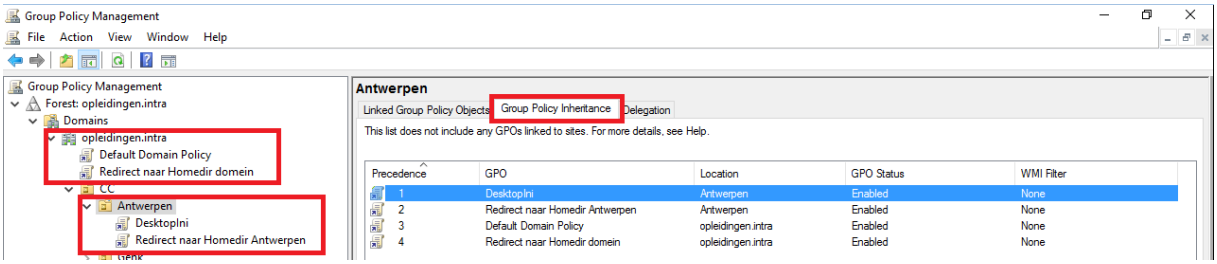
Nadien worden de GPO's op Site niveau uitgevoerd. De site GPO's worden uitgevoerd op alle users en computers binnen de domeinen en OU's van de site. Bij conflicten overschrijven de instellingen van de site GPO's die van de LGPO. Niet conflicterende instellingen worden cumulatief toegepast.

In een volgende stap worden de domain GPO's uitgevoerd op alle users en computers van het respectievelijke domein. Hier gelden dezelfde regels: niet conflicterende instellingen worden cumulatief toegepast, bij conflicten wint de laatst toegepast, nl. die van het domein.

Als laatste worden de GPO's op OU niveau uitgevoerd. Een GPO die gekoppeld is aan een bepaalde OU zal enkel effect hebben op de users en computers binnen deze specifieke OU. En opnieuw gebeurt de toepassing cumulatief en wint bij conflicten de laatst toegepaste instelling.

Als een domein meerdere levels van OU's bevat, worden de hoogste in de structuur eerst toegepast en pas daarna de lagere.

Een overzicht van overgeërfde group policies vind je terug in de Group Policy management console.



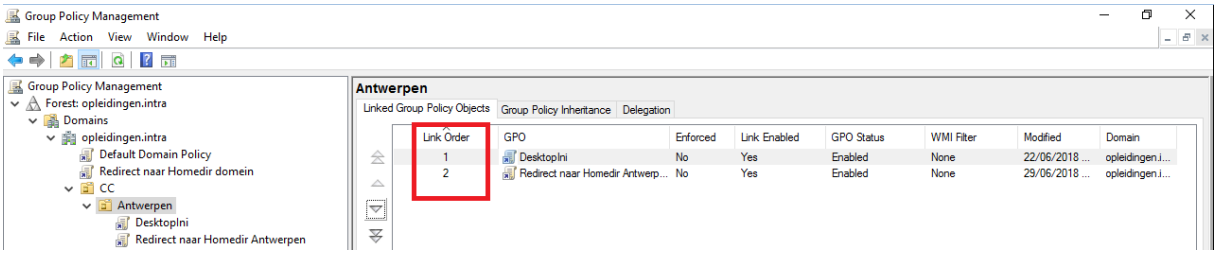
Het veld **Precedence** geeft aan in welke mate een GPO die van toepassing is op een container, prioriteit heeft. De GPO's worden uitgevoerd van onder naar boven in de lijst. Policies met een hogere waarde bij Precedence worden dus overschreven door policies met een lagere waarde.

Voorbeeld

- Maak een GPO met de naam **Verplichte screensaver** die ervoor zorgt dat een gebruiker de screensaver niet kan wijzigen (User Configuration > Policies > Administrative templates > Control Panel > Personalization > Prevent changing the screen saver
- Koppel de GPO ter hoogte van het domein
- Maak een tweede GPO die ervoor zorgt dat een gebruiker de screensaver wel kan wijzigen met de naam **Vrije screensaver**.
- Koppel die aan de OU CC
- Maak een eerste gebruiker op het domein in de container Users.
- Maak een tweede gebruiker in de container CC
- Meld aan op de client met de eerste gebruiker en stel vast dat die de screen saver niet kan instellen.
- Meld aan op de client met de tweede gebruiker en stel vast dat die de screen saver wel kan instellen.
- Verwijder de twee koppelingen.

Soms zijn er meerdere GPO's op hetzelfde niveau gekoppeld.

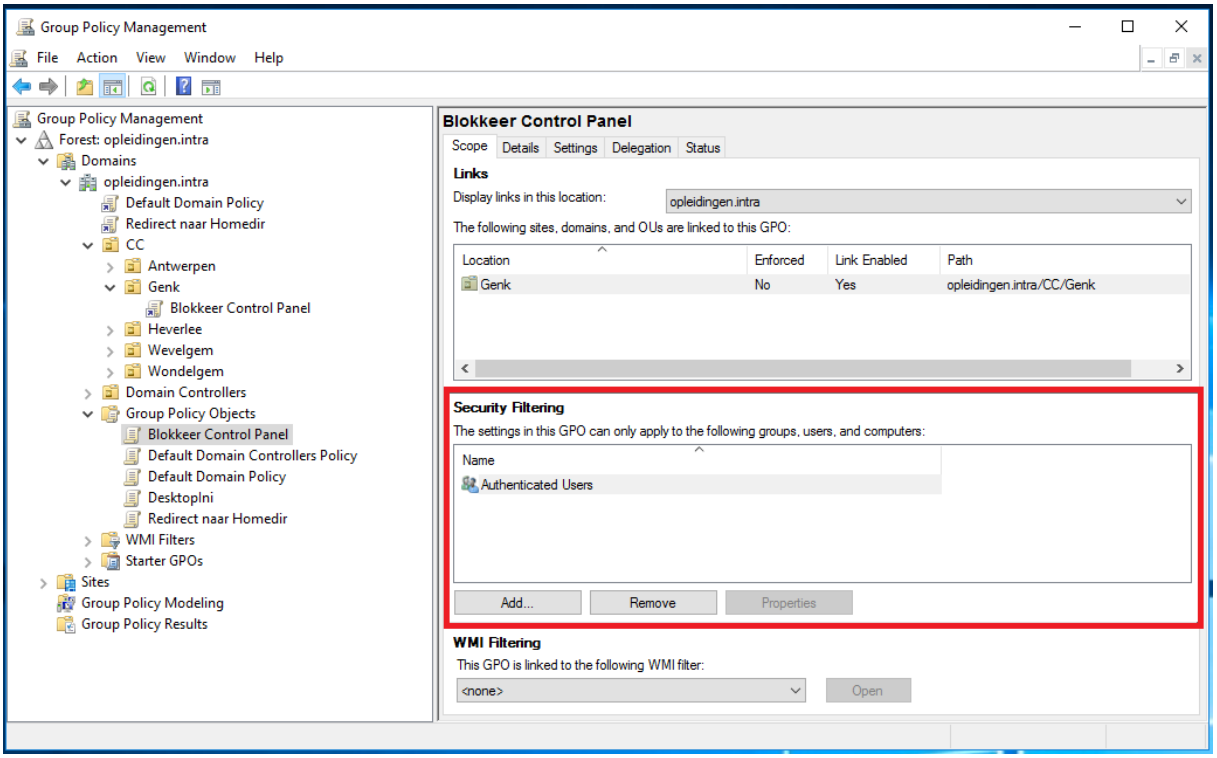
Zoals je op onderstaande afbeelding kan zien, krijgt elke GPO een link order. Uitvoering gebeurt van lage naar hoge link order. 2 wordt in dat geval als een lagere link order beschouwd dan 1, maw volgens onderstaande afbeelding wordt eerst Redirect naar Homedir Antwerpen uitgevoerd en dan desktop.ini. In geval er conflicterende instellingen staan in deze GPO's, dan winnen de instellingen van Desktop.ini.



Er zijn ook een aantal opties voorzien om af te wijken van deze standaard manier en volgorde om GPO's toe te passen: security filtering, WMI filters, block inheritance en enforced..

3.6.1 Security filtering

Security filtering gebruik je als een GPO niet mag toegepast worden op alle accounts in de container waaraan hij gelinkt is.



Onder Security filtering staat standaard de group Authenticated Users.

Dit betekent dat de groep **Authenticated users**[3] de rechten **Read** en **Apply Group Policy** heeft op de GPO, met als gevolg dat de group policy toegepast wordt op elke authenticated account in de container waaraan de GPO gelinkt is.

[3] Authenticated Users = aangemelde gebruikers + computers van het domein of van vertrouwde domeinen.

Om te filteren op gebruikers volstond het om de groep Authenticated Users te vervangen door een andere groep om de toepassing van de GPO te beperken tot de gebruikeraccounts in de container die ook lid zijn van de groep.

Hotfix MS16-072/KB3159398 uitgebracht in 2016 vereist echter dat niet alleen de gebruikersaccount leesrecht heeft op de GPO, maar ook de computeraccount. Meer uitleg kan je vinden in deze blog : https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/who-broke-my-user-gpos/ba-p/258781

Het gevolg is dat na installatie van de hotfix op een client computer group policies met standaardinstellingen of die alleen gelden voor computers, blijven werken, maar GPO's waarin onder Security filtering de groep Authenticated users verwijderd is, niet meer het gewenste resultaat leveren.

Om het probleem op te lossen volstaat het Read permissions te geven aan de groep Domain computers.

Opmerkingen: Je kunt wel groepen gebruiken om de toepassing van de GPO te filteren, maar je kunt geen GPO toepassen op een groep zelf. De leden van de groep moeten ook in de container aanwezig zijn waaraan de GPO gekoppeld is.

Voorbeeld

- Maak een globale groep met de naam **ggMetControlPanel**
- Maak een globale groep met de naam **ggZonderControlPanel**
- Koppel de policy **Blokkeer Control Panel en PC Settings** aan de OU Antwerpen
- Maak twee gebruikers in de OU Antwerpen en maak de ene gebruiker lid van **ggMetControlPanel** en de andere van **ggZonderControlPanel**
- Filter de policy op **ggZonderControlPanel**
- Meld met beide gebruikers aan op de client en ga na of ze zoals verwacht al dan niet bij het Control Panel kunnen.
- Verwijder de koppeling zonder de GPO zelf te verwijderen.

3.6.2 WMI filters

Security filters filteren gebruikers. WMI (Windows Management Instrumentation) filters kunnen gebruikt worden om op attributen van computers te filteren. Attributen van een computer zijn b.v. de versie van het besturingssysteem, de architectuur van de processor (32bit / 64 bit), geïnstalleerde rollen, registry-instellingen, enz.

Een WMI filter werkt met een WMI query. Levert de query de waarde true op voor een computer, dan wordt de policy toegepast en anders niet.

Alle software en hardware componenten die via een WMI filter kunnen benaderd worden, corresponderen met een klasse. Enkele voorbeelden van klassen zijn Win32_LogicalDisk (logische schijven), Win32_PhysicalMemory (het geheugen van de computer), Win32_Share (lijst van gedeelde mappen)....

Een voorbeeld van een WMI query die de hoeveelheid vrije schijfruimte opvraagt van de harde schijf:

select FreeSpace from Win32_LogicalDisk where DeviceID = "C:" and Description = "Local Fixed Disk"

Enkele andere voorbeelden van een WMI query:

Bekijken of het OS een Windows Server is:

*select * from Win32_OperatingSystem where Caption like "%Windows Server%"*

Is het OS Windows 10:

*select * from Win32_OperatingSystem where Caption like "%Windows 10 %"*

Is het OS Windows 11:

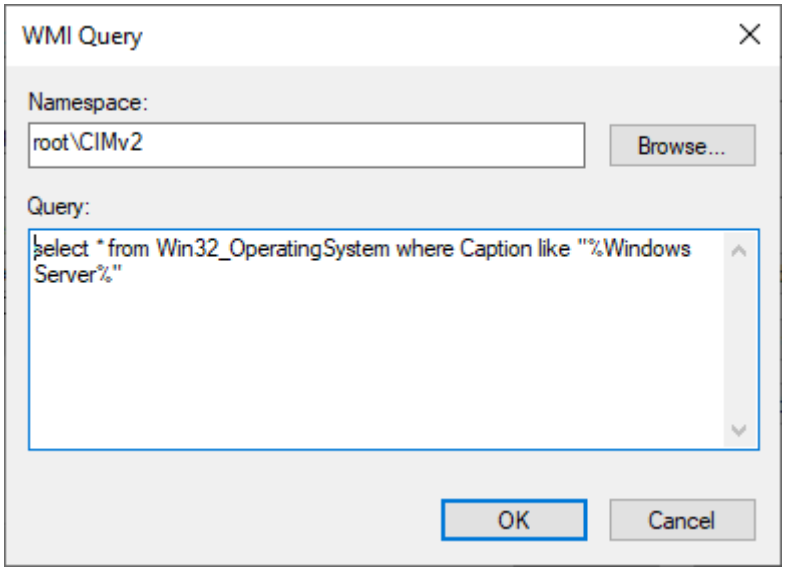
*select * from Win32_OperatingSystem where Caption like "%Windows 11 %"*

Voorbeeld

Doel is de policy **Don't display last signed-in** alleen toe te passen als de gebruiker probeert aan te melden op een server.

Eerst maak je een WMI filter.

- Klik rechts op de WMI Filter Container in de GPMC en kies **New**. Het New WMI Filter dialoogvenster wordt geopend.
- Geef de Filter een **Naam** (b.v. EnkelServers) en klik op **Add** om een Query toe te voegen.
- In het WMI Query venster tik je onderstaande Query in (tussen Windows en Server staat er 1 spatie), klik daarna op **OK**.



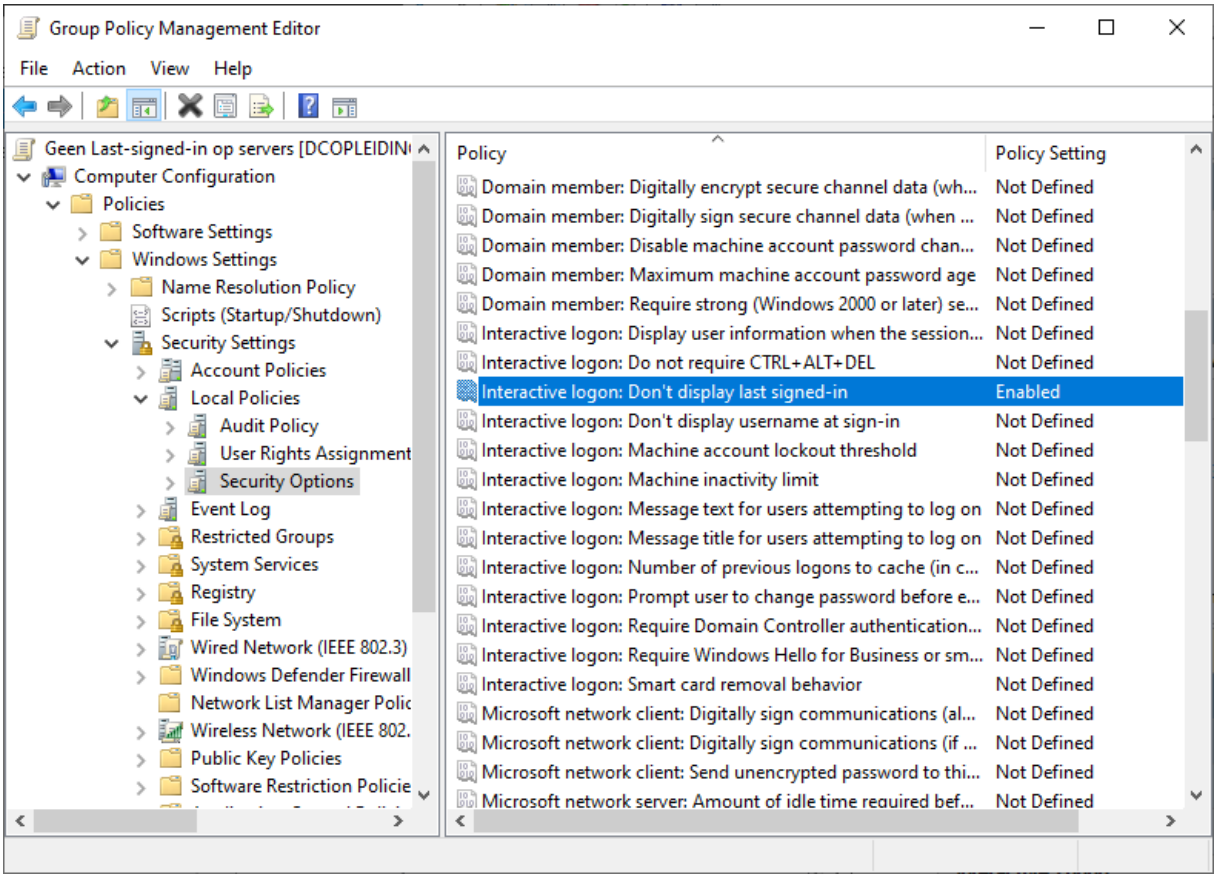
De query wordt toegevoegd aan de WMI Filter.

Klik op **Save**.

De WMI Filter is nu opgenomen in de container met de WMI-filters.

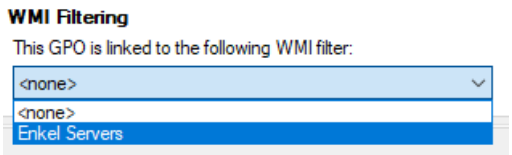
Daarna kan je de filter koppelen aan een GPO.

Maak een nieuwe GPO aan “Geen Last signed-in op servers” met de instelling zoals onderstaand scherm.



De GPO mag enkel uitgevoerd worden op toestellen met Windows Server als OS.

- Koppel de policy aan het domein.
- Laat bij Security filtering “Authentticated Users” staan.
- Klap bij WMI filtering de lijst open en selecteer de gewenste WMI Filter.



- Je krijgt een boodschap met de vraag of de WMI Filter mag aangepast worden naar de geselecteerde WMI Filter. Klik op **Yes**.
- Herstart je client-toestel en merk op de laatste gebruiker nog staat ingevuld staat als je wenst aan te melden.
- Herstart nu je ook je server. Je zal merken dat je hier wel de gebruikersnaam opnieuw moet invullen.

3.6.3 Block Inheritance

Een GPO gekoppeld aan een OU geldt ook voor de geneste OU's (=inheritance). Soms moet er voor één van de geneste OU's een uitzondering gemaakt worden.

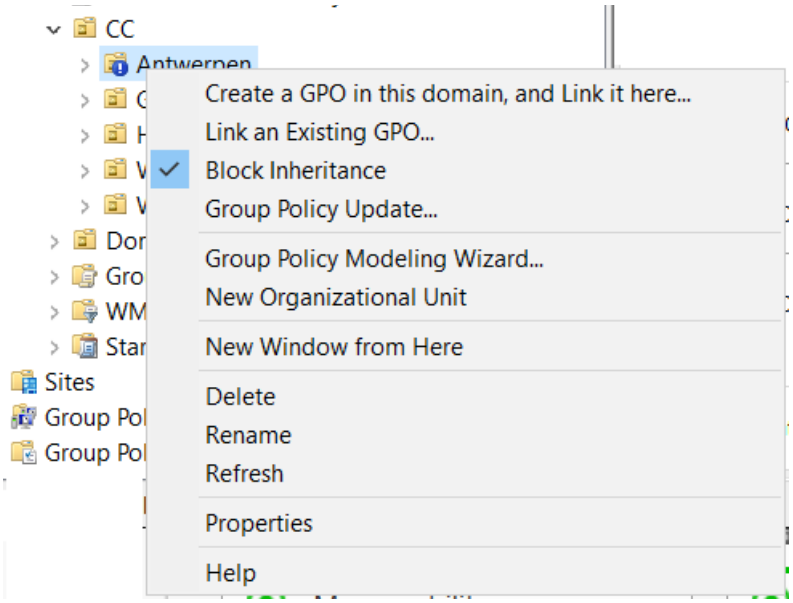
Optie 1: je creëert nog een GPO die de instellingen van de hogerop toegepaste GPO overschrijft.
Nadeel: er moeten nu twee GPO's uitgevoerd worden, één om de instellingen toe te passen en een volgende om de toegepaste instellingen teniet te doen; dit vraagt tijd en resources.

Alternatief: Block Inheritance

Aandachtspunt: het is een alles of niets verhaal, **Block Inheritance** geldt voor alle GPO's die overgeërfd worden.

De praktijk:

- Klik rechts op de OU Antwerpen
- Selecteer **Block Inheritance**



- Koppel de GPO Blokkeer Control Panel en PC Settings aan de OU CC
- Meld aan met een gebruiker uit Antwerpen en met een gebruiker uit een ander centrum en stel vast dat de eerste wel instellingen kan wijzigen via het configuratiescherm of via Settings en de tweede niet.

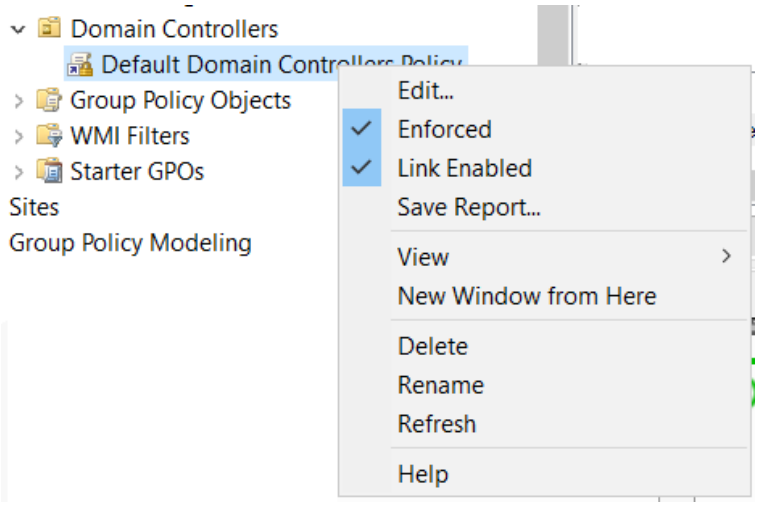
3.6.4 Enforced

Met Enforced kunnen GPO's op een lager niveau de instellingen niet overschrijven van een hogerop gekoppelde GPO waarvoor enforced geactiveerd is. Als

verschillende links op hetzelfde niveau op Enforced staan, moet je ze volgens gewenste prioriteit plaatsen.

Praktijk

- Klik rechts op de GPO die op alle lagere niveaus moet toegepast worden
- Selecteer **Enforced**



De Enforced wordt gekoppeld aan de link, niet aan de GPO zelf. Eenzelfde GPO kan dus op twee plaatsen toegepast worden, één keer met Enforced en één keer zonder.

Opmerking: GPO's met Enforced aangevinkt kunnen niet geblokt worden met block inheritance.

Voorbeeld

- Schakel Enforced in op de link met CC van de GPO Blokkeer Control panel en PC Settings.
- Meld aan met een gebruiker van de OU Antwerpen en stel vast dat die de GPO toch de toegang tot het Control Panel en de PC Settings blokkeert.
- Verwijder de koppeling van de GPO aan CC en schakel Block Inheritance ter hoogte van Antwerpen uit.

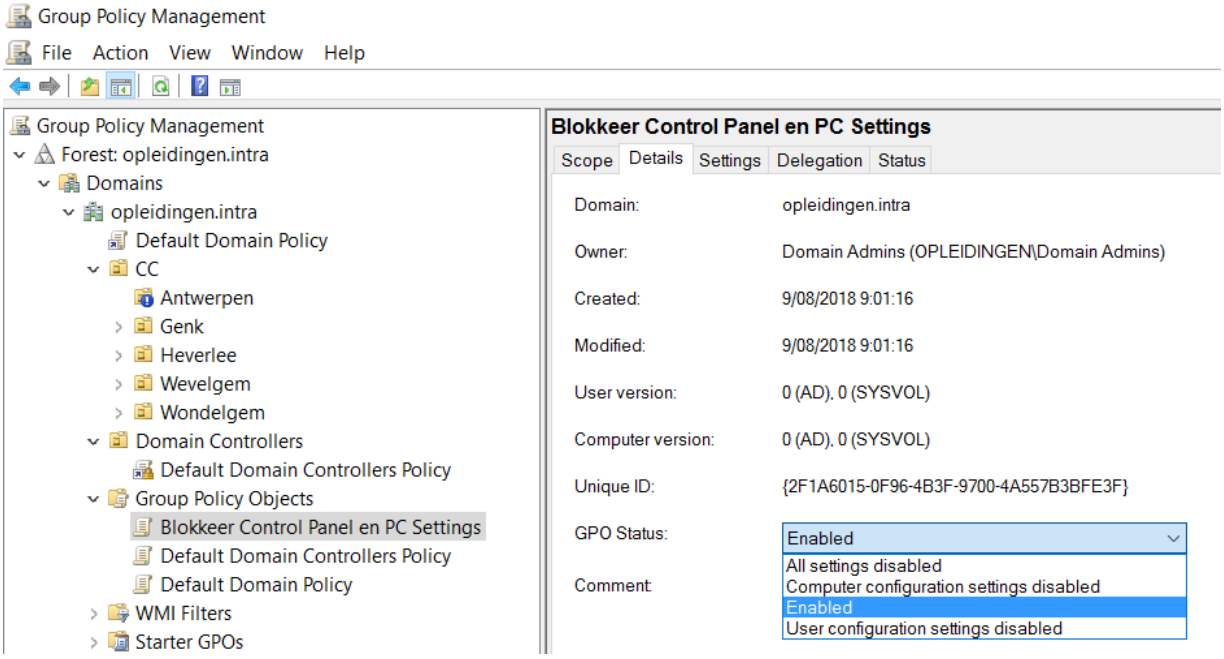
3.6.5 Group Policies uitschakelen

Op het **Details** tabblad van de GPO kan je een Group Policy uitschakelen via de GPO status.

Er zijn 4 mogelijkheden:

- **Enabled**: de GPO is actief
- **All settings disabled**: de volledige GPO wordt uitgeschakeld

- **Computer Configuration Settings disabled**: enkel de computer configuratie wordt uitgeschakeld, de user configuratie settings worden wel uitgevoerd.
- **User configuration settings disabled**: enkel de user configuatie wordt uitgeschakeld, de computer configuratie settings worden wel nog uitgevoerd.

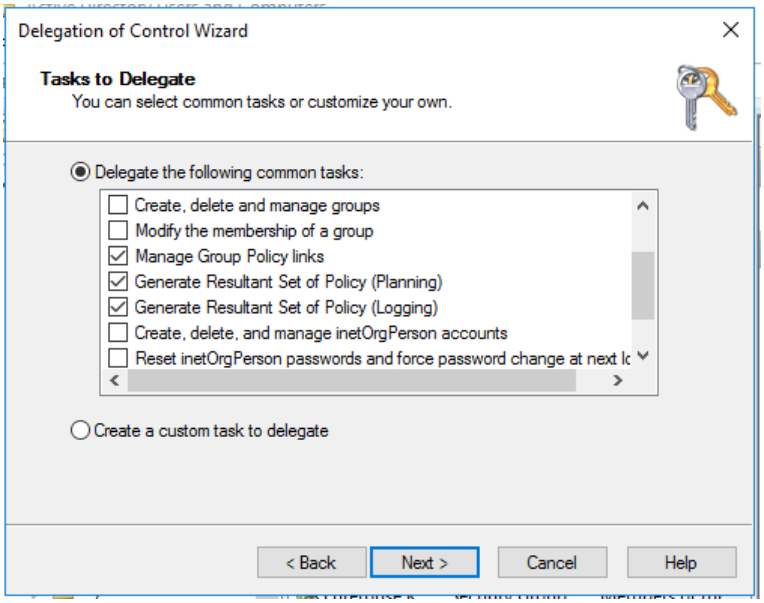


3.7 Delegatie van het beheer van GPOs

Net als de delegatie van het beheer van de administratieve taken in de AD, kan je ook het beheer van de GPO's delegeren.

Er zijn 3 mogelijkheden:

- Je kunt de permissies om GPO's te **maken**, te **verwijderen** en te **wijzigen** delegeren. Default hebben alleen Domain Admins en Group Policy Creator Owners dit recht. Als je dit recht ook nog aan andere gebruikers wilt geven voeg ze dan toe aan één van deze groepen. Je kunt ook het recht om GPO's te maken of te verwijderen geven aan andere groepen, maar het is iets ingewikkelder dan dat. Die gebruikers moeten ook nog het recht hebben om te schrijven in de map %systemroot%\sysvol\sysvol\domainname\policies. Je kunt ze ook nog rechten voor Read en Write geven op de GPO in de AD.
- Je kunt het beheer van GPO's ook delegeren door het recht om group policy **koppelingen** te **beheren** te delegeren. Met deze permissie kunnen de gedelegeerden geen GPO's wijzigen, maar ze kunnen GPO's toevoegen of verwijderen op een container. De gemakkelijkste methode is met de Delegation Of Control Wizard. In de Active Directory Users And Computers tool klik je rechts op het betreffende object en je kiest voor Delegate Control. Eén van de mogelijke delegaties is de permissie Manage Group Policy Links.



- De derde mogelijkheid ten slotte om te delegeren is de gebruikers het recht geven om de Resultant Set of Policy (RSoP) informatie te genereren. Met dezelfde wizard als hierboven kan je dat recht toekennen. Je kunt deze permissies ook toekennen door de ACL op een object aan te passen. Geef de gebruiker de Write permissie op het gPLink attribuut. Als je de permissies geeft op de gPOptions dan kan de gebruiker het blokkeren van inheritance instellen op het container level.

Via het tabblad **Delegation** binnen de GPO (in de GPMC) kan je zien wie er allemaal rechten heeft op de Group Policy. Met de knoppen **Add** en **Remove** kunnen groepen toegevoegd en verwijderd worden.

3.8 Group Policy Ontwerp

Enerzijds zal een groot aantal GPO's het opstarten en aanmelden vertragen. Dit pleit voor zo weinig mogelijk Group policies.

Anderzijds maken slechts een beperkt aantal GPO's die een groot aantal instellingen bepalen, het beheer en het documenteren dan weer ingewikkeld.

De beste oplossing is zoals zo dikwijls de gulden middenweg.

Single policy

Per verzameling instellingen wordt een aparte GPO gemaakt. Deze manier van werken is geschikt voor bedrijven waar het beheer verspreid is over een groot aantal medewerkers.

Multiple policy

Zoveel mogelijk instellingen worden in een enkele GPO gegroepeerd. Dit is geschikt voor bedrijven waar het beheer volledig centraal gebeurt.

Dedicated policy

De instellingen die met de gebruikers te maken hebben zijn gegroepeerd in één GPO, de instellingen die met de computer te maken hebben in een andere. Deze manier van werken kan het aanmelden vertragen, maar maakt het verhelpen van problemen gemakkelijker.

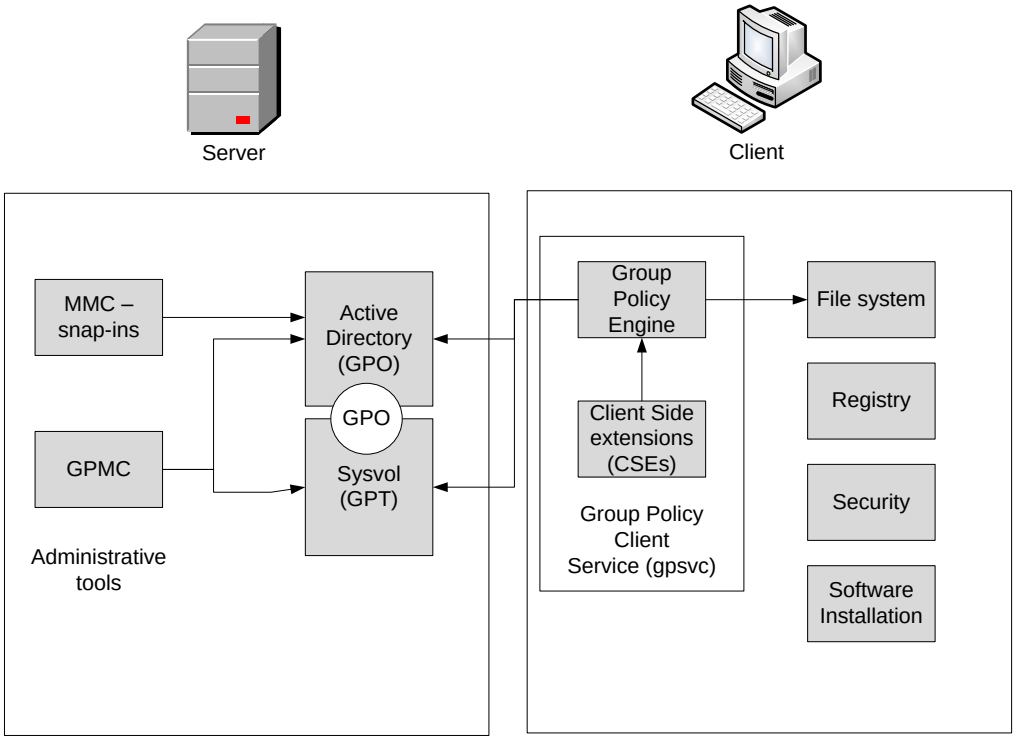
3.9 Hoe worden group policies uitgevoerd?

https://www.grouppolicy.biz/2012/04/whats-change-with-the-group-policy-client-service-in-windows-8/

Onderstaande figuur illustreert de werking van het groepsbeleid.

Aan de Server kant worden de Group policies beheerd en geconfigureerd door de administrative tools. Daaronder verstaan we de MMC snap-ins en de Group Policy Management Console (GPMC). De GPO's nestelen zich in de Active directory en de sysvol Folder.

Aan de Client kant worden de GPO's geïnterpreteerd en uitgevoerd door de Client Side extensions.



3.9.1 De Group Policy Client Service

De group policy client service is verantwoordelijk voor de uitvoering van de GPO's.

3.9.2 Het initieel GPO proces

Wanneer een nieuwe GPO gemaakt of aangepast wordt, zullen de policy settings pas doorgevoerd worden naar de client als deze client daar specifiek om vraagt. Hoe frequent en wanneer een client naar een update van GPO's vraagt hangt af van verschillende voorwaarden:

- Het type van besturingssysteem
- Is de computer lid van het domain?
- De locatie van de computer in de active directory
- De kwaliteit en het type van netwerk connectie
- De refresh instellingen. Standaard refresh voor DC's is 5 minuten, voor clients 90 minuten met een interval van 30 minuten.

Group policy instellingen voor users en computers worden op verschillende tijdstippen aangevraagd en uitgevoerd.

- Bij het opstarten van de computer worden de computer policy settings uitgevoerd.
- Bij het aanloggen van een user worden de user policy settings uitgevoerd.

3.9.3 Synchronous en asynchronous Group Policy Processing

Het toepassen van Group Policies kan synchroon of asynchroon verlopen.

Het asynchroon toepassen van de Group policies, ook wel de Fast Logon Optimization feature genoemd, is de huidige standaard.
Dit houdt in dat tijdens het opstarten van de computer en het aanloggen van de user de GPO's op de achtergrond worden uitgevoerd. Daardoor verloopt het opstarten en aanmelden sneller, de gebruiker hoeft immers niet te wachten totdat alle GPO's zijn uitgevoerd.

Let wel, Folder redirection en de installatie van software wordt enkel toegepast in synchrone modus. Wanneer dit zou uitgevoerd worden op de achtergrond bij asynchrone modus zou dit kunnen leiden tot verlies van data en onvolledige installatie van software.
Dit geldt ook voor users die gebruik maken van roaming profiles, home directories en/of user logon scripts.
Bij synchrone modus moeten de Computer Policy Settings eerst uitgevoerd worden voordat een user kan aanmelden. Idem voor de User Policy Settings: deze moeten eerst uitgevoerd worden voordat de desktop van de gebruiker verschijnt.

De Group Policy processing Mode kan via een Group Policy aangepast worden. Deze is terug te vinden onder **Computer Configuration\Policies\Administrative**

templates\System\logon. Daar enable je **Always wait for the network at computer startup and logon** wanneer je wil overschakelen naar synchrone modus.

De Fast Logon Optimization wordt niet toegepast onder de volgende omstandigheden en resulteert dus in het synchroon uitvoeren van de GPO's:

- Wanneer een gebruiker voor de eerste keer aanlogt op een computer
- Wanneer de gebruiker is geconfigureerd met een logon script
- Wanneer de gebruiker gebruik maakt van een roaming profile en/of home directory
- Bij de installatie van software via GPO's

In bovenvernoemde gevallen zijn er twee logons nodig om de settings door te voeren. De eerste logon verloopt asynchroon en geeft aan dat de volgende logon synchroon met verlopen. De tweede logon verloopt via de synchrone modus en past de Group Policy Settings toe die synchrone modus vereisen.

3.9.4 Vernieuwen van groepsbeleid

Wanneer GPO's aangepast worden gedurende de periode dat gebruikers aangelogd zijn, zullen de aanpassingen doorgevoerd worden door middel van een background refresh interval.

Het vernieuwen van het groepsbeleid is afhankelijk van het besturingssysteem:

Bij DC's: wordt het groepsbeleid op de achtergrond om de 5 minuten vernieuwd.

Bij member servers en clients wordt het groepsbeleid op de achtergrond om de 90 minuten vernieuwd met een willekeurige afwijking van 30 minuten. Deze 30 minuten heeft als doel om te voorkomen dat alle clients tegelijkertijd om een refresh van de GPO's vragen.

Belangrijk om weten is dat het vernieuwen van de computer en user instellingen binnen een GPO afzonderlijk wordt toegepast. Via de GPMC kan je de vernieuwingstijd en de standaard afwijking zowel voor de computer als voor de user instellingen afzonderlijk aanpassen.

Volgende instellingen zijn terug te vinden in het groepsbeleid:

Set Group policy refresh interval for computers.
Locatie: Computer Configuration\Policies\Administrative Templates\System\group policy

Set Group policy refresh interval for domain controllers.
Locatie: Computer Configuration\Policies\Administrative Templates\System\group policy

Set Group policy refresh interval for users.
Locatie: User Configuration\Policies\Administrative Templates\System\group policy

3.9.5 Uitzonderingen op het vernieuwen van GPO's

Stel dat je een nieuw groepsbeleid hebt aangemaakt of een bestaand hebt aangepast en je wil dat die aanpassingen onmiddellijk worden doorgevoerd zonder te wachten op de vernieuwing van de GPO.

In dat geval kan je op de client gebruik maken van een command-line tool: *Gpupdate*.

Syntaxis:
Gpupdate [**/target:**{**computer**|**gebruiker**}] [**/force**] [**/wait:***waarde*] [**/logoff**] [**/boot**]

Parameters	
/target:{**computer**|**gebruiker**}]	Alleen de instellingen van de *computer* of de huidige *gebruiker worden verwerkt*. Standaard worden zowel de instellingen van de computer als die van de gebruiker vernieuwd.
/force	Vernieuwd alle groepsbeleid instellingen of deze nu zijn aangepast of niet.
/wait:waarde	Het aantal seconden dat wordt gewacht vooraleer het groepsbeleid wordt vernieuwd. De standaardwaarde is 600 seconden. *0* betekent 'niet wachten'; *-1* betekent 'onbepaalde tijd wachten'.
/logoff	Er wordt afgemeld nadat het vernieuwen is voltooid. Dit is vereist voor die clientextensies van Groepsbeleid waarbij verwerking niet plaatsvindt in een achtergrondvernieuwingscyclus, maar waarbij verwerking plaatsvindt wanneer de gebruiker zich aanmeldt, zoals Software-installatie en Folder redirection door een gebruiker. Deze optie heeft geen effect als er geen extensies worden aangeroepen waarbij de gebruiker zich moet afmelden.
/boot	De computer herstart nadat het vernieuwen is voltooid. Dit is vereist voor die clientextensies van Groepsbeleid waarbij verwerking niet plaatsvindt in een achtergrondvernieuwingscyclus, maar waarbij verwerking plaatsvindt wanneer de computer wordt gestart, zoals Software-installatie

	door een computer. Deze optie heeft geen effect als er geen extensies worden aangeroepen waarbij de computer opnieuw moet worden gestart.
/?	Geeft Help-informatie vanaf de opdrachtprompt.

Tip: *Gpupdate /force*

kan handig zijn in een lab-omgeving om nieuwe instellingen uit te proberen.

3.10 Starter GPO's

Een Starter GPO kan je aanzien als een template voor de instellingen onder Administrative Templates. Bij het maken van een nieuwe GPO kan je vertrekken vanaf deze template of starter GPO waardoor de GPO reeds een aantal vooraf gedefinieerde instellingen bevat.

Een toepassing van een starter GPO kan zijn meerdere OU's die voor een groot deel dezelfde instellingen moeten krijgen, maar afwijkingen voor enkele instellingen.

De gemeenschappelijke instellingen kunnen dan opgenomen worden in een Starter GPO.

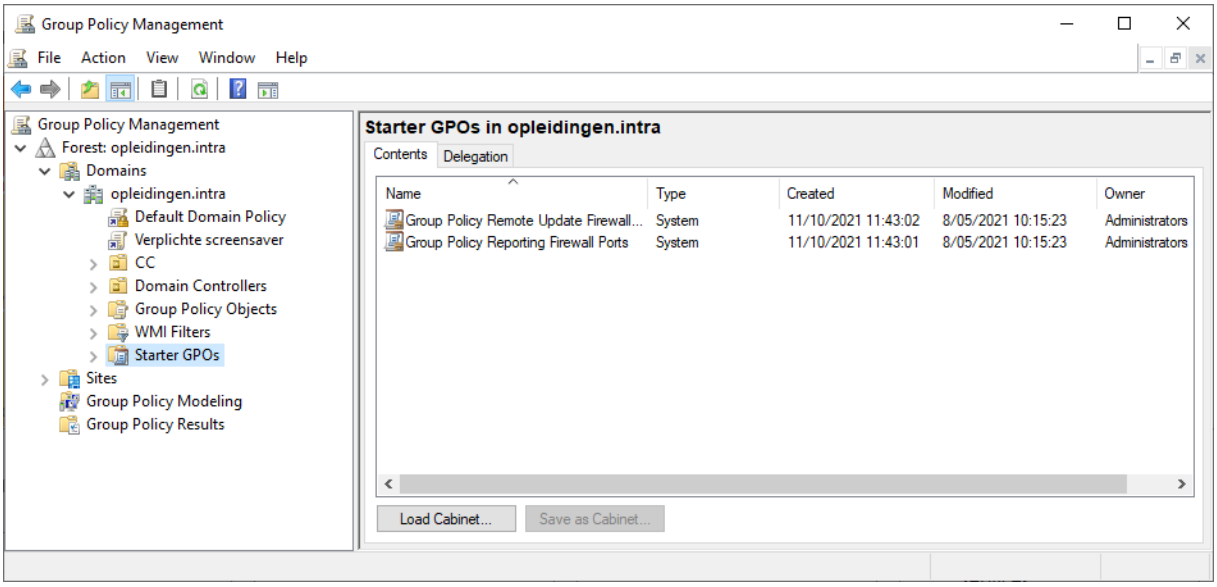
Een starter GPO kan ook van pas komen bij het uitrollen van een GPO in meer dan één forest.

3.10.1 Starter GPO's in gebruik nemen

- Open de Group Policy Management Console.
- Klap de boomstructuur van het domein open
- Onderaan vind je de Starter GPO's
- Bij het allereerste gebruik dien je de starter Folder nog te creëren. Klik op de knop **Create Starter GPO's Folder**.

De folder wordt aangemaakt en er worden een aantal al bestaande Starter GPO's aan toegevoegd.

Net zoals bij een gewone GPO kan je de naam van het groepsbeleid selecteren en via het tabblad settings de aanwezige instellingen bekijken.



3.10.2 Een nieuwe Starter GPO maken

Naast het gebruik van de vooraf gedefinieerde Starter GPO's bestaat de mogelijkheid om eigen Starter GPO's te maken.

Voorbeeld

- Klik rechts op de container **Starter GPO's** en selecteer **New**.
- Geef de Starter GPO een naam (**Geen grafieken in Rekenmachine**) en eventueel een omschrijving. Klik vervolgens op **OK**.

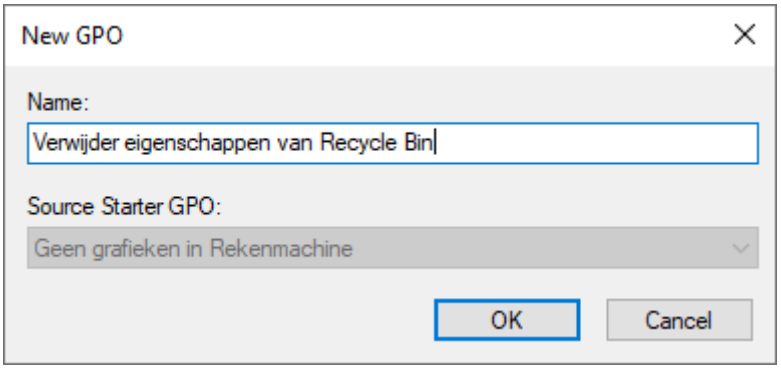
De Starter GPO wordt toegevoegd aan de lijst. Er staan echter nog geen instellingen in.

- De instelling om de grafieken niet te kunnen gebruiken bij de rekenmachine (calculator) vind je onder
  User Configuration > Administrative Templates > Windows Components > Calculator -> Allow Graphing Calculator. Activeer deze setting en zet deze op Disabled.

3.10.3 Een nieuwe GPO gebaseerd op een starter GPO

Om een nieuwe GPO te maken gebaseerd op een starter GPO ga je als volgt te werk:

- Creëer een nieuwe GPO en geef een duidelijke naam.
- Selecteer in de keuzelijst **Source Starter GPO** de juiste Starter GPO. Kies die jezelf hebt gemaakt en klik op OK.



In de nieuwe GPO zullen de instellingen van de Starter GPO overgenomen worden. Het verder configureren van de GPO doe je door rechts te klikken op de GPO en **Edit** te kiezen.

Opmerking: Veranderingen die je doorvoert op Starter GPO's zullen NIET doorgevoerd worden op reeds bestaande GPO's die gebaseerd zijn op de Starter GPO.

Voorbeeld

- Maak een nieuwe GPO gebaseerd op de hiervoor gedefinieerde starter GPO (Geen grafieken in Rekenmachine).
- Verwijder uit het contextmenu van prullenbak (Recycle Bin) de toegang tot het eigenschappenvenster. Dit via User configuration > Policies > Administrative Templates > Desktop > Remove Properties from the Recycle Bin context menu.
- Bekijk de Settings van de nieuwe GPO en stel vast dat je daar ook de setting ivm de rekenmachine terugvindt.

3.11 Group policy troubleshooting

De oorzaak van onverwachte resultaten achterhalen na het toepassen van GPO's kan ingewikkeld worden. De GPMC stelt twee tools ter beschikking om daarbij te helpen: Group Policy Modeling en Group Policy Results

3.11.1 Group Policy Results

Group Policy Results gebruik je om

- te weten te komen welke grouppolicy instellingen effectief toegepast worden voor een bepaalde computer of een bepaalde gebruiker.
- niet werkende of overschreven instellingen op te sporen.

Om een rapport te maken:

Klik met de rechtermuisknop op Group Policy Results en kies **Group Policy Results Wizard…** in het contextmenu. Group Policy Results werkt met een wizard.

Kies voor Another computer en selecteer via Browse jouw client computer.

Kies in het volgende venster Select a specific user en duid een gebruiker aan. In de lijst verschijnen uitsluitend gebruikers die al eens aangemeld hebben.

Dan volgt nog een samenvatting en wordt het rapport aangemaakt.

Om de analyse op een remote device toe te passen moeten een aantal inbound firewall rules geconfigureerd zijn, meer bepaald

- Remote Event Log Managment (NP-In)
- Remote Event Log Management (RPC)
- Remote Event Log Management (RPC-EPMAP)
- Windows Management Instrumentation (WMI-in)

Tip: Dit kan via een GPO.

Maak een Group Policy Results rapport voor één van je gebruikers.

3.11.2 Group Policy Modeling

Group Policy Modeling gebruik je om

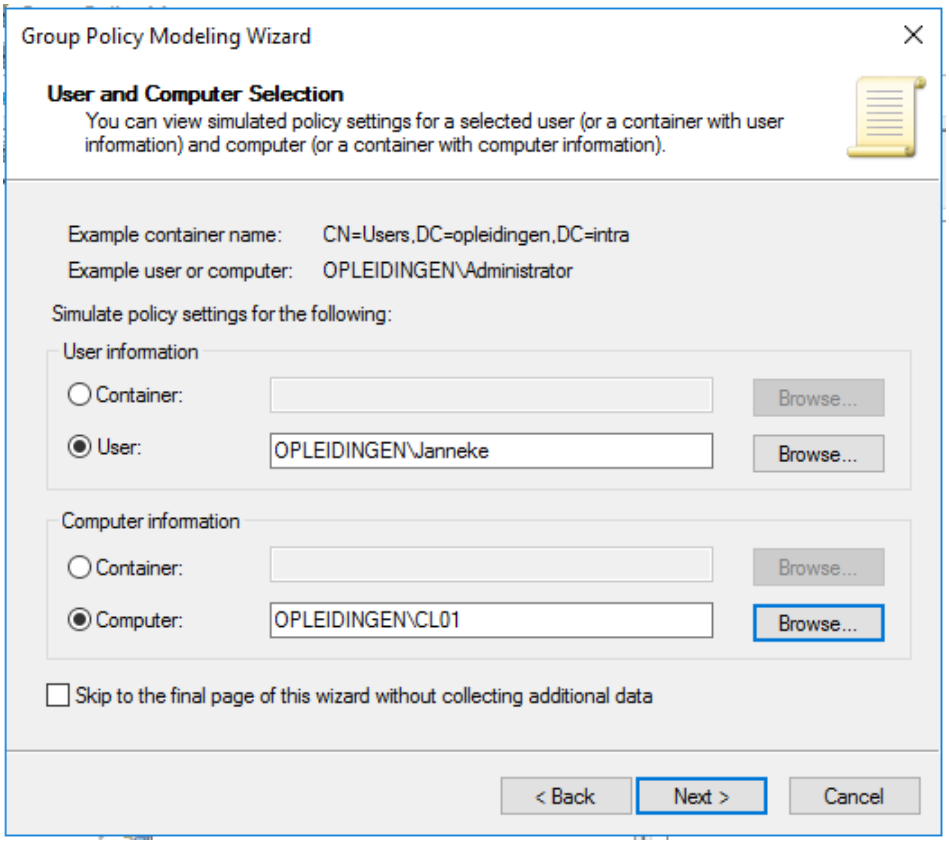
- Het effect van een bepaalde policy op een computer of gebruiker te simuleren.
- De voorrang van de GPO's te testen in volgende situaties:
    - De gebruiker en de computer zitten in verschillende security groepen
    - De gebruiker en/of de computer zitten in verschillende OU's
    - De gebruiker of de computer wordt verplaatst naar een nieuwe locatie.
- Het resultaat van een trage netwerkverbinding te simuleren.
- Een loopback situatie te creëren

Ook Group Policy Modeling werkt met een wizard

Kies in het context menu van Group Policy Modeling de **Group Policy Modeling Wizard**.

Duid in de volgende stap aan voor welk domein en op welke domein controller de simulatie moet gemaakt worden.

Definieer de computer en de gebruiker waarvoor je de simulatie wil maken. Dit kan ook voor alle gebruikers of computers in een bepaalde container zijn.



Selecteer het vinkje bij **Skip to the final page of this wizard without collecting additional data.**

Selecteer je dat vinkje niet, dan volgen nog vensters waarin je met wat gesimuleerde toestanden kan rekening houden zoals

- een trage netwerkverbinding
- loopback processing
- een bepaalde site

of

- de gebruiker wordt verplaatst naar een andere container
- de computer wordt verplaatst naar een andere container

of

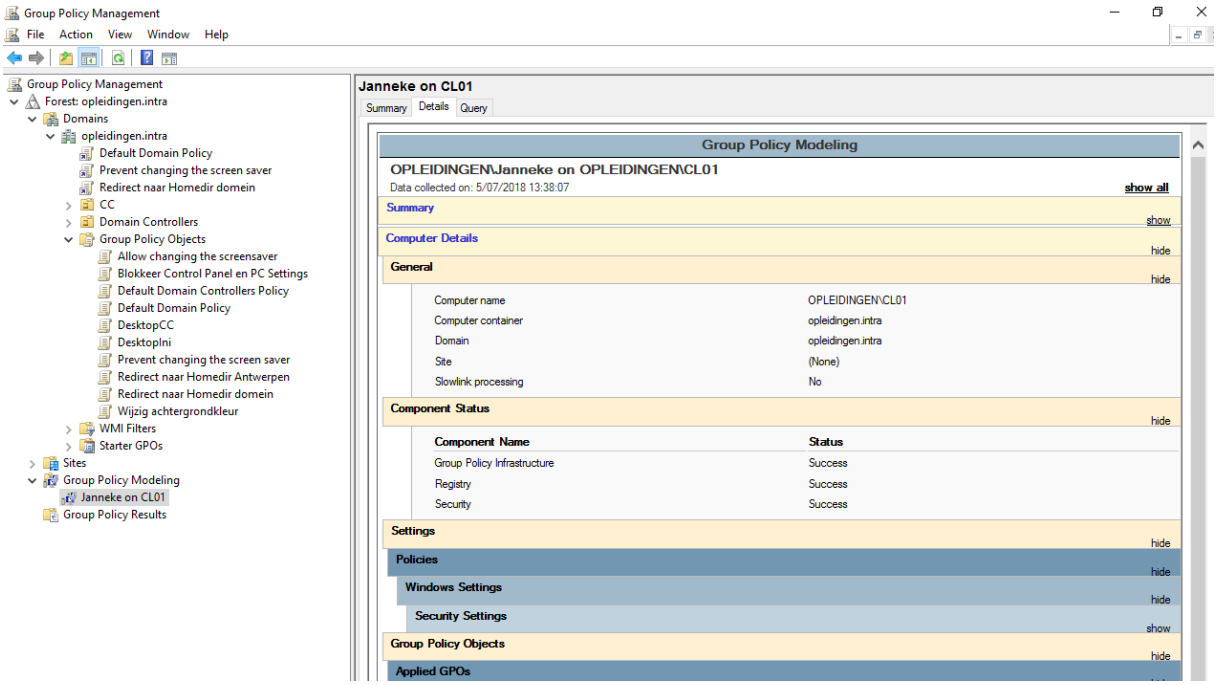
- de gebruiker wordt lid van of verwijderd uit een bepaalde groep

of

- een WMI filter wordt toegepast

🛠 Lees de samenvatting en klik ten slotte op Finish.

Het resultaat van de simulatie verschijnt in het console venster.



GPResult is een command-line tool die een deel van de functionaliteit van de RsoP tool voorziet. Als je GPResult toepast, zonder parameters, vanop de command line dan krijg je de group policy informatie voor de computer waarop je werkt en voor de gebruiker die aangelogd is.

Het commando kan ook gebruikt worden in de verbose mode. Dan krijg je alle effectieve GPO instellingen alsook de effectieve privileges die de gebruiker heeft.

Je kunt het commando ook gebruiken om de instellingen te zien van andere computers of gebruikers.

Tik gpresult /? om alle parameters te bekijken. GPResult is geïnstalleerd op alle computers vanaf versie Windows XP Professional en Windows Server 2003.

Een voorbeeld:

- 🛠 Log aan op de client PC met een domain user, b.v. Janneke.
- 🛠 Open een command prompt
- 🛠 Tik het commando: gpresult /H GPResultaat.html
  met /H wordt het resultaat weggeschreven in een html bestand.

Het resultaat is terug te vinden in de home-folder van de gebruiker (waar je terecht was gekomen toen je de command prompt opgestart hebt).

- 🛠 Ga via de file explorer naar de map van hierboven en open het html-bestand door er dubbel op te klikken.

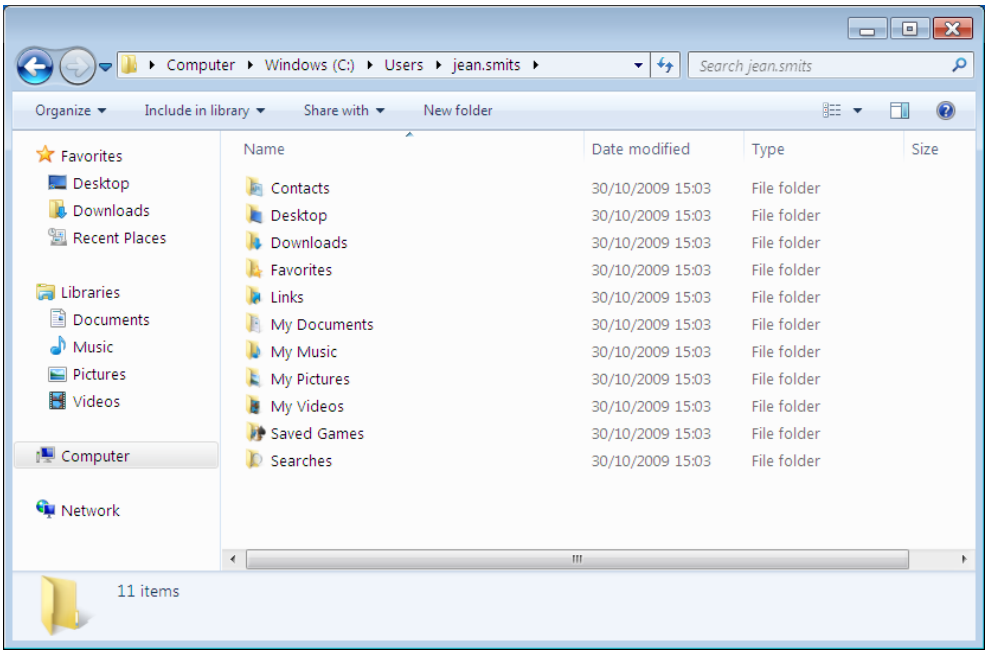
4 COMPUTERBEHEER EN USERBEHEER MET GPO'S, DE PRAKTIJK

In het vorige hoofdstuk kwam vooral aan bod hoe GPO's werken. In dit hoofdstuk wordt ingegaan op enkele concrete voorbeelden van het gebruik van GPO's om de gebruikersomgeving te beheren.

4.1 Beheer van de data en profiel instellingen van de gebruiker.

4.1.1 Beheer van de gebruikersprofielen.

Een gebruikersprofiel bevat alle configuratie informatie over de desktop van de gebruikers. Die informatie bevat dus de inhoud van de HKEY_CURRENT_USER subtree in de registry (bewaard als Ntuser.dat). Het profiel bevat ook nog folders zoals Documents, Start Menu, Desktop en Application.Data.



Bedrijven kunnen kiezen voor lokale, zwervende of verplichte profielen (zie Hoofdstuk 2Homedirectories, zwervende profielen en logonscripts).

Via GPO's kan je deze profielen beheren. Het merendeel van de instellingen hiervoor vind je onder Computer Configuration \Administrative Templates \System \User Profiles. Enkele bijkomende instellingen vind je op dezelfde locatie onder User Configuration.

Instellingen van de Gebruikersprofielen met de Group Policy Object Editor	
De voornaamste Configuratie optie	Verklaring

Do Not Check For User Ownership Of Roaming Profile Folders	Enabled betekent deze instelling dat een al bestaande profielmap zonder verder controle op de toegangsrechten in gebruik genomen wordt.
Delete Cached Copies Of Roaming Profiles	De lokale gecachte kopie van een roaming profiel wordt verwijderd als de gebruiker aflogt
Add The Administrators Security Group To Roaming User Profiles	Gebruik deze optie om de administrator toegang te geven tot de gebruikersprofielen. Standaard heeft de gebruiker full control op zijn profiel maar de administrator heeft geen toegang
Only allow local user profiles	Enkel lokale profielen worden toegepast op een bepaalde computer.
Limit Profile Size (onder User Configuration)	Hier kan je de grootte van een profiel beperken. Ook de manier van waarschuwen bij overschrijden kan je hier instellen.
Exclude Directories In Roaming Profile (onder User Configuration)	Je kunt definiëren dat bepaalde mappen niet mogen opgenomen worden in het profiel.

Een voorbeeld:

Doel: administrator rechten geven op roaming profiles van de gebruikers. Standaard kunnen enkel de gebruikers in hun eigen roaming profile. Dit geeft de nodige problemen bij het verwijderen van een profiel. De administrator dient dan een take ownership uit te voeren op deze profielen wat een tijdrovend werkje kan worden. Om dit op te lossen kan je de administrator groep toevoegen aan de ACL van de roaming profiles.

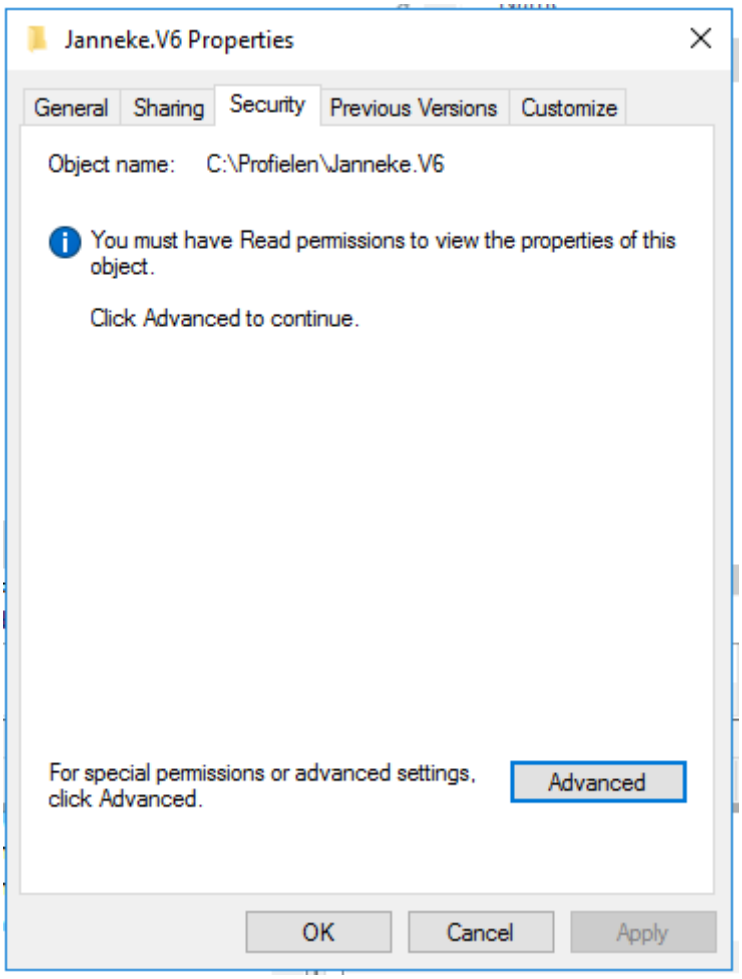
Opmerking

De GPO zal alleen invloed hebben op profielen die na het in gebruik nemen van de GPO aangemaakt worden.

In het hoofdstuk 2 heb je de gebruiker Janneke een zwervend profiel gegeven.

Bekijk de eigenschappen van de profielmap van Janneke (Janneke.V6) en ga meer bepaald naar het tabblad Security.

Omdat Administrators geen toegangsrechten hebben tot de profielen, krijg je de volgende melding



Een group policy maken om de administrators toegang te verlenen:

- Open de **Group Policy Management Console**
- Maak een nieuwe GPO aan en noem die Beheerprofielen.
- Schakel de volgende eigenschap in: Computer Configuration \ Policies \ Administrative Templates \ System \ User Profiles > Add the Administrators security Group to roaming user profiles.

De GPO Beheerprofielen koppelen

Het gaat over een instelling onder Computer configuration. De GPO zal bijgevolg alleen effect krijgen als hij gekoppeld wordt aan een container met computers.

Koppel de GPO aan de OU waarin de client computer zich bevindt of ter hoogte van het domein.

De GPO testen

Maak een nieuwe gebruiker Fien en geef die een zwervend profiel.

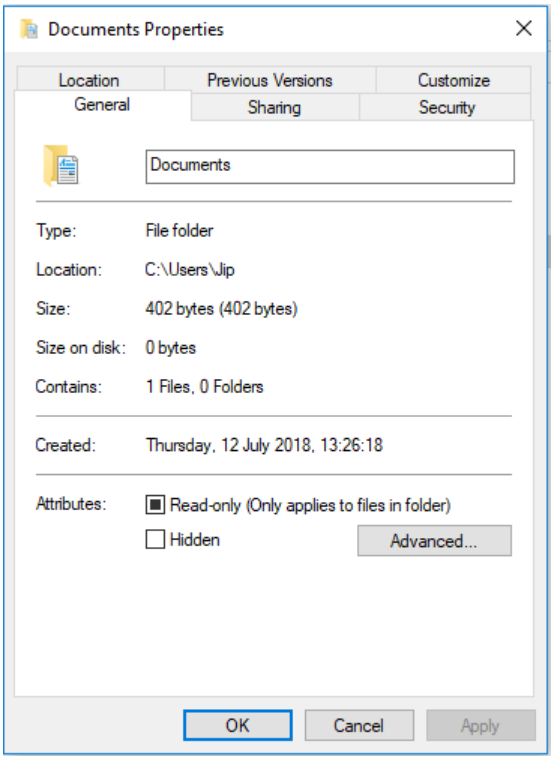
Herstart de client en meld aan met Fien.

Meld Fien af.

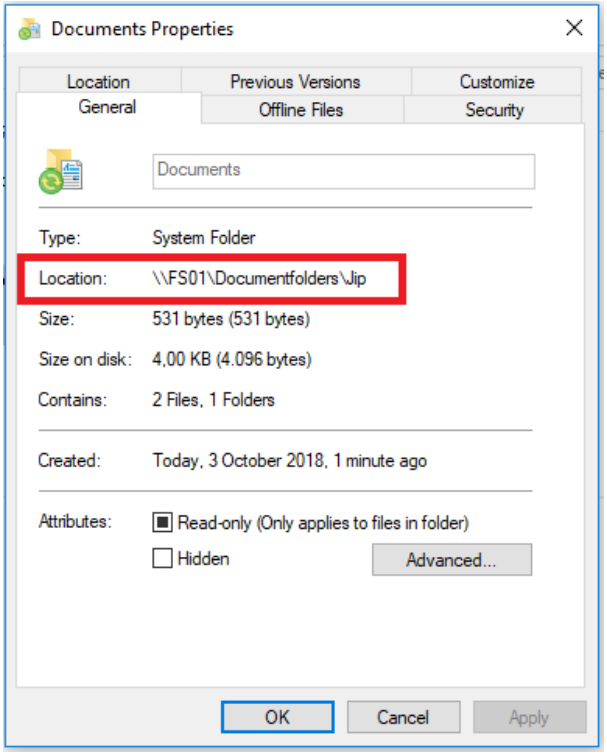
Bekijk het tabblad Security van het profiel van Fien (de map Fien.V6). Hier krijg je deze keer wel toegang toe en de Administrators hebben Full Control gekregen op de map.

4.1.2 Folder Redirection

Zoals vermeld in **2.1 Persoonlijke documenten overal beschikbaar maken** kan je home folders gebruiken om persoonlijke bestanden toch centraal op te slaan. Een Windows client systeem biedt standaard de map Documents aan om eigen bestanden weg te schrijven. Die bevindt zich echter lokaal op de client computer. Met Folder Redirection kan je die map Documents naar een server verplaatsen en dit op een voor de gebruiker transparante manier.



Zonder Folder redirection



Met Folder redirection

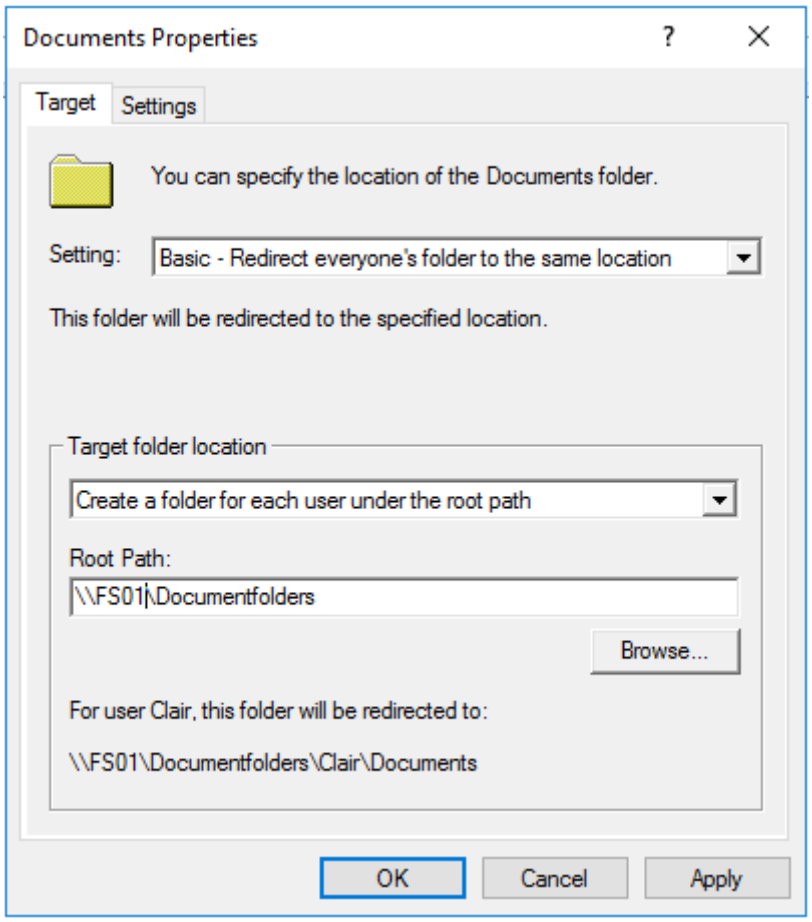
Folder redirection wordt geconfigureerd in de Group Policy Object Editor via User Configuration \ Windows Settings \ Folder Redirection.

Een voorbeeld:

Doel: Folder redirection toepassen op de Documents Folder voor de gebruikers van Wevelgem.

- 🛠 Open de **Group Policy Management Console**
- 🛠 Maak een nieuwe GPO met de naam DocumentRedirectionWevelgem.

- Gebruik de GPO editor om naar User Configuration \ Policies \ Windows Settings \ Folder Redirection te navigeren.
- Roep de eigenschappen van Documents onder Folder Redirection.



Standaard staat de instelling bij Setting op **Not Configured**. Er zijn ook nog twee andere mogelijkheden.

- Basic - Redirect Everyone's Folder To The Same Location
- Advanced - Specify Locations For Various User Groups

Opmerking

Je kunt de advanced optie niet gebruiken voor individuele gebruikers. Let er ook op dat de gebruikers die de group policy moeten ondergaan in de container moeten staan waarop de GPO van toepassing is. Een GPO werkt niet op een groep.

Ook om de doelmap / Target Folder location in te stellen zijn er meerdere mogelijkheden

- **Redirect To The User's Home Directory**: De Document folder wordt doorverwezen naar de Home Folder van de gebruiker zoals die staat ingesteld in de properties.

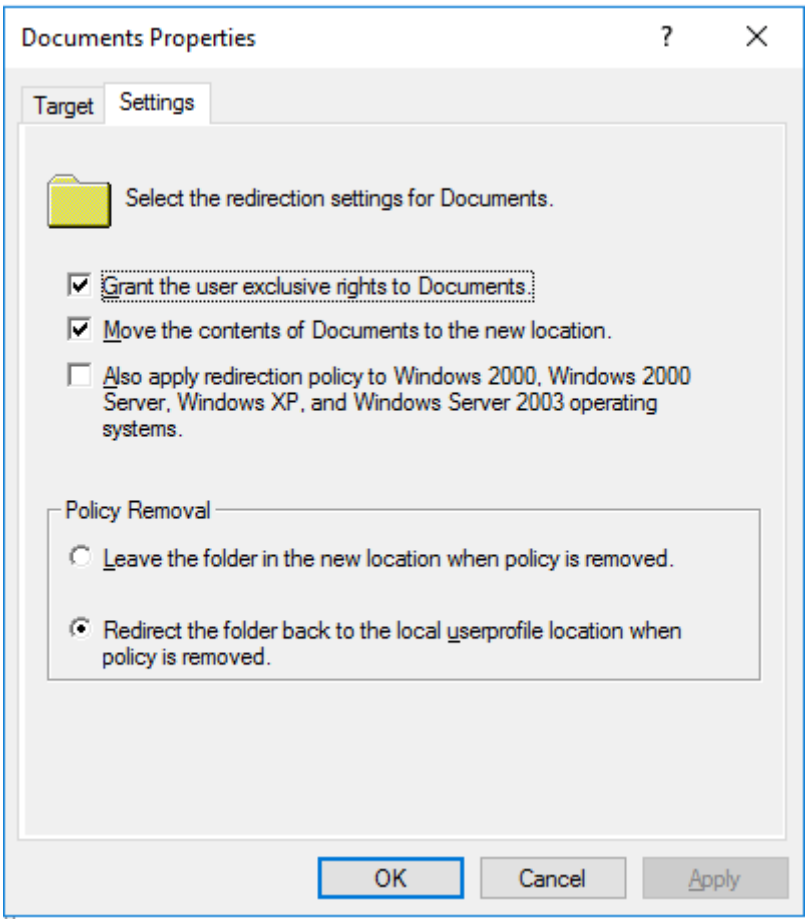
- **Create a Folder For Each User Under The Root Path**: Hier specificeer je een root path waar de folders zullen opgeslagen worden. Hier wordt voor elke gebruiker een map gemaakt.
- **Redirect To The Following Location**: Hier kan je zowel het path als de folder locatie instellen.
- **Redirect To The Local Userprofile Location** Dit is de standaard instelling als er geen policies ingeschakeld zijn. Hiervoor worden de mappen niet doorverwezen naar een netwerk share.

Kies volgende configuratie:

- **Setting**: Basic: Redirect everyone's folder to the same location
- **Target Folder location**: Create a folder for each user under the root path
- **Root Path**: \\servernaam\sharenaam in het voorbeeld: \\FS01\Documentfolders

Opmerking: dit zal enkel werken als de share Documentfolders al aanwezig is. Maak dus vooraf de share aan en zorg ervoor dat gebruikers schrijfrechten hebben in de share.

Er zijn nog extra instellingen voor de redirected folders. Klik op het **Settings** tabblad.



- **Grant the user exclusive rights to Documents**: De gebruiker krijgt volledige toegangsrechten op de folder. De administrator krijgt geen toegang. Als je dit niet aanklikt gelden de geërfde permissies.
- **Move the contents of Documents to the new location**: Deze instelling verplaatst de huidige inhoud van de doorverwezen folder naar de doelmap. Indien niet geselecteerd, zal de inhoud niet gekopieerd worden naar de doelmap.
- **Also apply redirection policy to Windows 2000, Windows 2000 Server, Windows XP, and Windows Server 2003 operating systems.** Schakelt redirection ook voor oudere systemen in.
- **Policy Removal** : Wat gebeurt er als de policy verwijderd wordt? Je kunt kiezen uit “Leave The Folder In The New Location When Policy Is Removed” of “Redirect The Folder Back To The Local Userprofile Location When Policy Is Removed”

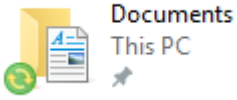
Folder Redirection is ingesteld.

Koppel de GPO aan de OU Wevelgem.

- Test de instelling uit op de Client. Log aan met een gebruiker in de OU Wevelgem.
- Bekijk de eigenschappen van Documents op de client. Deze zijn verplaatst van c:\users naar de map op de server.
- **Opmerking**: soms is het noodzakelijk om meer dan 1 keer aan te melden alvorens de wijzigingen doorgevoerd worden.
- Maak via de client een bestand aan in de folder Documents van de juist aangemelde gebruiker. Dit bestand zal weggeschreven worden naar de directory van de gebruiker op de server. Kijk dit na in de share Documentfolders op FS01.

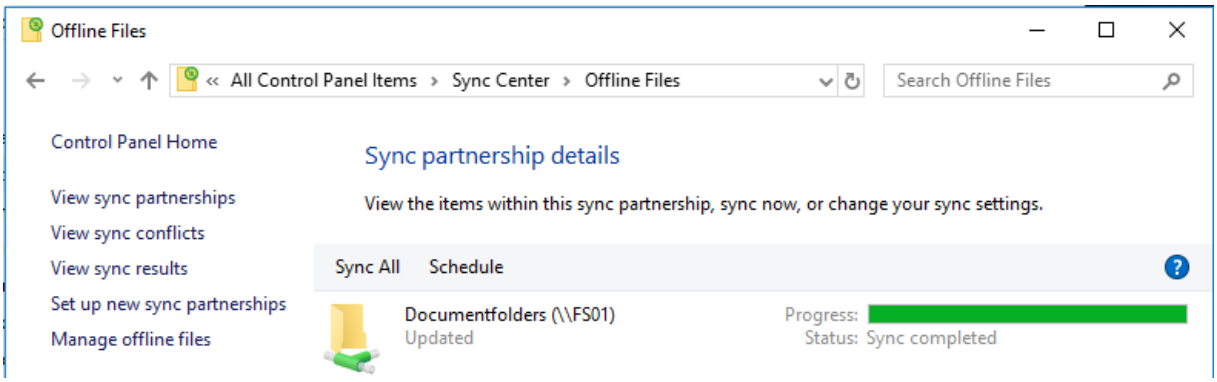
Het gebruik van offline folders bij Folder Redirection

Van zodra folder redirection is geactiveerd op een folder, zal deze folder automatisch deel uitmaken van de Offline folders.
Dit is zichtbaar door het groene symbooltje dat toegevoegd wordt aan het icoon van de folder met folder redirection. Ook in het snelmenu staat er een vinkje bij Always available offline.



- Kijk dit na op uw Client toestel

In het Sync Center is de folder ook te zien. Via deze weg kunnen instellingen aangepast worden i.v.m. de synchronisatie.



- Kijk dit na op uw Client toestel

Een bestand binnen de Folder toont via het eigenschappenvenster eveneens aanwijzigen over zijn offline status.

Het feit dat bestanden uit een redirected folder automatisch in de offline folder terecht komen, zorgt ervoor dat deze bestanden ook voorradig zijn als er geen netwerkverbinding is. Voor laptop gebruikers, die veel op verplaatsing zijn is dit een positieve zaak.

Minder interessant wordt het als een gebruiker af en toe gebruik maakt van een andere PC binnen het netwerk, denk daarbij aan computers in een vergaderzaal die

dienst doen om presentaties te geven. In dat geval heeft de gebruiker enkel nood aan die ene presentatie en is het niet echt de bedoeling dat gans zijn documents folder wordt overgebracht naar de offline folders van deze computer.
In dat geval maak je gebruik van de Group Policy setting die het automatisch offline plaatsen van de bestanden tegenhoudt.

Deze setting is terug te vinden onder:
User Configuration \ policies \ Administrative Templates \ System \ Folder Redirection \ Do not automatically make redirected folders available offline

Redirection van andere mappen zoals Desktop, Start Menu, Pictures en Downloads naar een netwerk share kunnen een zwervend profiel vervangen.

Redirection kan ook gebruikt worden om verplichte profielen (mandatory profiles) voor een groep gebruikers in te stellen. Geef die gebruikers in dat geval Read, maar geen Write permissie op eenzelfde gedeelde map waarnaar de desktop en het start menu omgeleid worden en je krijgt een standaard desktop en start menu voor deze groep.

4.1.3 Gebruik van scripts om de gebruikersomgeving aan te passen.

Via het tabblad Profile van een gebruiker kunnen alleen logon scripts meegegeven worden aan individuele gebruikers.

Group policies breiden de mogelijkheden voor scripts uit:

- **Startup** en **shutdown** scripts: met de AD kan je scripts ook toepassen bij het opstarten(startup) en afsluiten (shutdown) van de computer.
- **Logon** en **logoff** scripts: aanmelden of afmelden van een gebruiker.
- Scripts worden gekoppeld aan OU’s ipv aan individuele gebruikers.
- Ondersteuning van PowerShell scripts

Logon scripts toegekend aan individuele gebruikers op het tabblad profile worden toegepast na de computer startup scripts en de gebruikers logon scripts van de group policy.

Om scripts te configureren voor de AD, maak je eerst een script en daarna kopieer je het script naar de Domain Controller. Je kunt de scripts om het even waar opslaan op de server zolang ze toegankelijk zijn voor de clients.

Mogelijke locaties om de scripts op te slaan:

- Een algemene locatie om een script op te slaan is %systemroot%\SYSVOL\sysvol*domainname*\scripts.
  Deze map is gedeeld onder de naam NETLOGON, de standaard locatie waar de vroegere clients hun scripts zoeken. Je kunt de scripts ook opslaan in:

- %systemroot%\SYSVOL\sysvol*domainname*\Policies*GlobalPolicyGUID*\Machine\Scripts
- %systemroot%\SYSVOL\sysvol*domainname*\Policies*GlobalPolicyGUID*\User\Scripts

Na het kopiëren van de scripts naar de server, open je de GPO en localiseer je de scripts (Startup/Shutdown) onder de Computer configuration of de scripts (Logon/Logoff) map onder de User Configuration\Windows Settings map.

Een eerste voorbeeld:

Infrastructuur.vbs wordt momenteel gebruikt als logonscript voor de gebruiker Jip. Doel is dit logonscript uit te voeren voor alle gebruikers van de OU Wevelgem.

Werkwijze:

Verwijder de verwijzing naar het script bij de eigenschappen van gebruiker Jip.

- Het script infrastructuur.vbs is momenteel terug te vinden in de folder: . %systemroot%\SYSVOL\sysvol*domainname*\scripts (zie 2.3.2 De gebruikersomgeving).

Het logon script toevoegen aan de GPO:

- Open de **Group Policy Management Console**
- Ga naar de OU Wevelgem.
- Maak een nieuwe GPO met de naam MapInfrastructuur en koppel die meteen aan de OU Wevelgem.
- Navigeer naar User Configuration > Policies > Windows Settings > Scripts

Dubbelklik op **Logon**

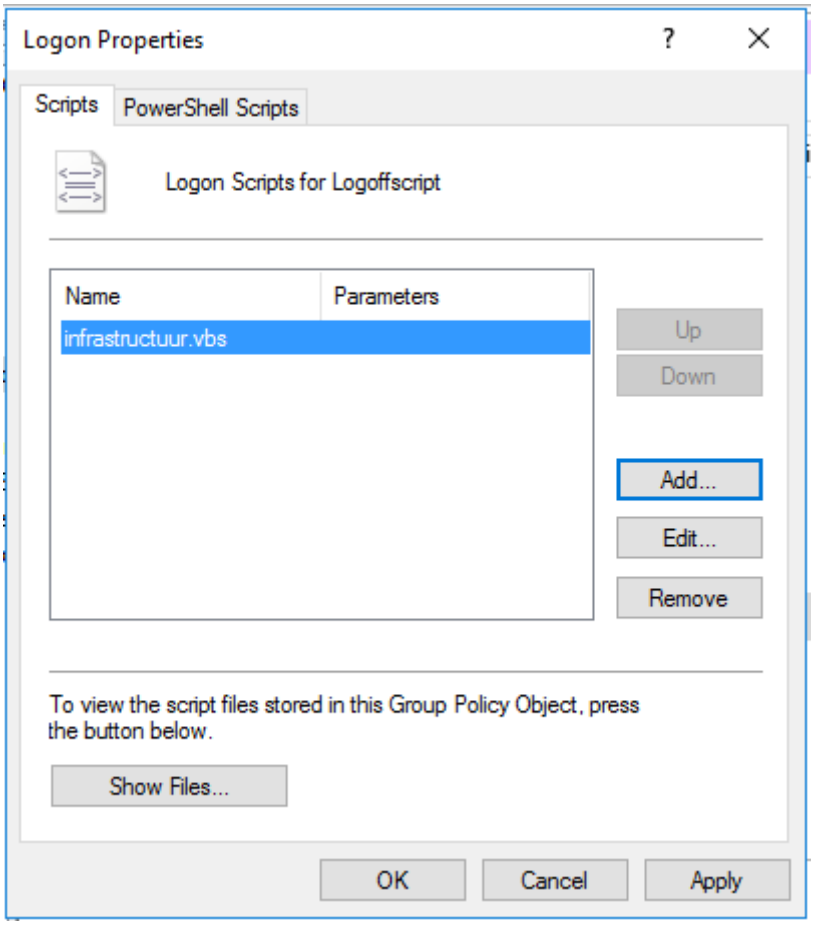
Kopieer het script naar de juiste locatie. Om die locatie te vinden klik je op de knop Show files.

Het pad naar die locatie kan eruit zien als:

\\opleidingen.intra\SysVol\opleidingen.intra\Policies\{42D06287-72EB-4647-8D51-16CC8EFF3B54}\User\Scripts\Logon

{42D06287-72EB-4647-8D51-16CC8EFF3B54} is dan de identificatie – PolicyGUID - van de policy.

- Klik vervolgens op **Add** en selecteer via de knop **Browse** het script**.**



- 🛠 Sluit beide explorer vensters.

Het script is nu gekoppeld aan de GPO

- 🛠 Test uit door op de client aan te melden met één van de gebruikers waarvoor de policy van toepassing is.

Scripts koppelen aan OU's via GPO's versus scripts gekoppeld aan gebruikerseigenschappen biedt een aantal voordelen:

- Van zodra een user toegevoegd wordt aan de OU worden automatisch de scripts toegepast op deze gebruiker, zonder eerst eigenschappen te moeten aanpassen.
- Hetzelfde geldt ook bij het verwijderen van een gebruiker uit de OU: zodra een gebruiker geen deel meer uitmaakt van de OU zullen de scripts ook niet meer uitgevoerd worden
- Er kunnen meerdere scripts gekoppeld worden. Dit kan NIET via de properties van de gebruiker, daar geldt maar één script.

Windows Server Active Directory voorziet een aantal administrative templates om de scriptverwerking te configureren op de werkstations. De meeste van deze instellingen bevinden zich in de *Computer Configuration\Policies\Administrative Templates*

System\Scripts en een paar vind je terug in *de User Configuration\Policies\ Administrative Templates\System\Scripts*. De configuratie opties zijn onder andere:

- Moeten de startup scripts asynchroon verlopen? Als je deze optie kiest dan lopen meerdere startup scripts tegelijk. Als je dit synchroon verkiest dan moeten alle startup scripts afgewerkt zijn alvorens de gebruiker de desktop te zien krijgt.
- Een maximum wachttijd instellen om alle scripts af te werken.
- Worden de scripts op de achtergrond of zichtbaar uitgevoerd.

Een tweede voorbeeld: een PowerShell script

Tot nog toe wordt in alle voorbeelden met .bat of .vbs scripts gewerkt. Uiteraard kan een script ook in PowerShell gemaakt worden.

- 🛠 Maak op de fileserver een map Devops onder Trajecten en deel die.
- 🛠 Maak in PowerShell een script om een mapping te maken naar deze gedeelde map.

  Tip: Zoek op het Internet de syntax van de cmdlet New-PSdrive (vergeet de optie *-Persist* niet)
- 🛠 Koppel het script aan de gebruikers van Wevelgem via een group policy.

  Tip: PowerShell logon scripts worden in het dialoogvenster Logon Properties gekoppeld via een apart tabblad.

Ga na of de mapping inderdaad gemaakt wordt als een gebruiker van Wevelgem aanmeldt.

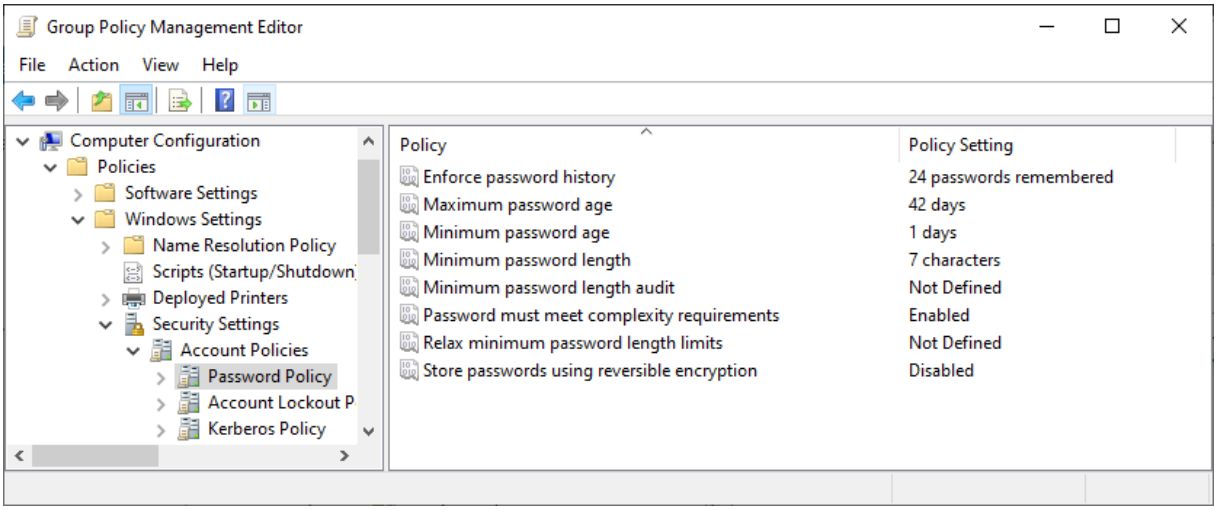
4.1.4 Nog enkele toepassingen

- 🛠 Voorzie folder redirection voor de map documents per gebruiker en dit voor alle gebruikers.
- 🛠 Geef alle gebruikers een logonscript dat een mapping maakt naar de naamruimte cursusmateriaal.

4.2 Beveiliging met Group Policies.

4.2.1 Configuratie van Domain-Level Security Policies

De Account Instellingen in Computer Configuration\Policies\Windows Settings\Security Settings worden op domeinlevel geconfigureerd en bestaan uit 3 groepen. (Password Policy, Account Lockout Policy en Kerberos Policy). Deze Instellingen (uitgez. Kerberos) gelden voor alle gebruikers in het domein.



- 🛠 Open de GPMC
- 🛠 Ga in de Default Domain policy naar Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Account Policies

Een woordje uitleg bij de belangrijkste instellingen

4.2.1.1 Password Policy

Instelling	Beschrijving	Standaard
Enforce Password History	Beschrijft hoeveel wachtwoorden uniek moeten zijn vooraleer je hetzelfde opnieuw mag gebruiken. Mogelijke waarden: *0* to *24*	*24 voor DC en domein members*
Maximum Password Age	Het aantal dagen dat een gebruiker een wachtwoord kan gebruiken voordat hij het moet veranderen (0=nooit).	*42* dagen

Minimum Password Age	Het aantal dagen dat een wachtwoord moet gebruikt worden vooraleer een gebruiker dat opnieuw mag veranderen (0=onmiddellijk).	*1 dag voor DC's en domain members*
Minimum Password Length	Minimaal aantal karakters in een wachtwoord (0=Geen wachtwoord nodig).	*7* karakters voor DC en domein members
Passwords Must Meet Complexity Requirements	Verplicht het gebruik van complexe wachtwoorden: geen enkel deel van de gebruikersnaam bevatten, minstens 6 karakters lang en die karakters komen uit 3 van 4 categorieën, nl hoofdletters, kleine letters, getallen en speciale karakters (zoals !, $, #).	Ingeschakeld voor DC's en domain members

Pas de Default Domain Policy aan als volgt:

- 🛠 Disable Password must meet complexity requirements
- 🛠 Stel een minimum wachtwoordlengte van 4 karakters in

Bekijk het resultaat van je instellingen:

- 🛠 Voer op de server een *gpupdate / force* uit om de GPO's update te forceren.
- 🛠 Herstart de client machine.
- 🛠 Reset het wachtwoord van één van de users. Een wachtwoord van 4 karakters is vanaf nu voldoende. Het wachtwoord moet niet meer voldoen aan de complexity.
- 🛠 Werkt het? Soms gebeurt het dat je de GPO wat tijd moet geven.

4.2.1.2 Account Lockout Policy

Instelling	Verklaring	Standaard
Account Lockout Duration	De duur in minuten van de lock out. Daarna wordt de account automatisch geunlockt. Bij waarde 0 moet de administrator de account opnieuw ontgrendelen.	Geen. Komt op 30 minuten als de Threshold op 1 of meer staat.
Account Lockout Threshold	Bepaalt hoe dikwijls een gebruiker mag proberen aan te loggen alvorens zijn account gelockt wordt. 0 betekent nooit.	*0*
Reset Account Lockout Counter After	Bepaalt het aantal minuten die moeten verlopen na een mislukte logon alvorens de mislukte logonteller terug op nul wordt gezet.	Geen. Komt op 30 minuten indien de Account Lockout Threshold op 1 of meer staat.

4.2.1.3 Kerberos Policy

De Kerberos Policy bevat instellingen voor de Kerberos Ticket-Granting Ticket (TGT) en sessie ticket lifetimes en time stamp instellingen.

Instelling	Verklaring	Standaard
Enforce User Logon Restrictions	Eist dat het Key Distribution Center (KDC) iedere aanvraag voor een sessie ticket valideert t.o.v; de User Rights policy van de doelPC.	Ingeschakeld
Maximum Lifetime For Service Ticket	Bepaalt de maximum geldigheidsduur in minuten van een service ticket om toegang te hebben tot een bron.	*600* minuten
Maximum Lifetime For User Ticket	Bepaalt de maximum tijdsduur in uren dat een TGT kan gebruikt worden. Als die tijd ten einde is moet het werkstation een nieuw TGT bekomen.	*10* uren

Instelling	Verklaring	Standaard
Maximum Lifetime For User Ticket Renewal	Bepaalt de tijd in dagen dat een gebruikers TGT kan vernieuwd worden.	*7* dagen
Maximum Tolerance For Computer Clock Synchronization	Bepaalt het tijdverschil in minuten dat Kerberos zal toestaan tussen de klok van de client en de tijd op de server. Telkens de PC opstart, wordt dit teruggeplaatst naar de standaard waarde.	*5* minuten

4.2.1.4 Fine-Grained Password Policies

Account Instellingen gebeuren op het Domain Security Policy level. De instellingen gelden dan meteen voor alle gebruikers op het domein en bijgevolg krijgt elke gebruiker dezelfde password policy en account lockout policy.

Vanaf Windows Server 2008 werden “Fine-Grained Password Policies” ingevoerd. Die maken het mogelijk om specifieke password policies en account lockout settings te koppelen aan bepaalde users en/of groepen en vanaf Windows Server 2012 kan dat zelfs via een grafische interface, nl. via ADAC (Active Directory Administrative Center).

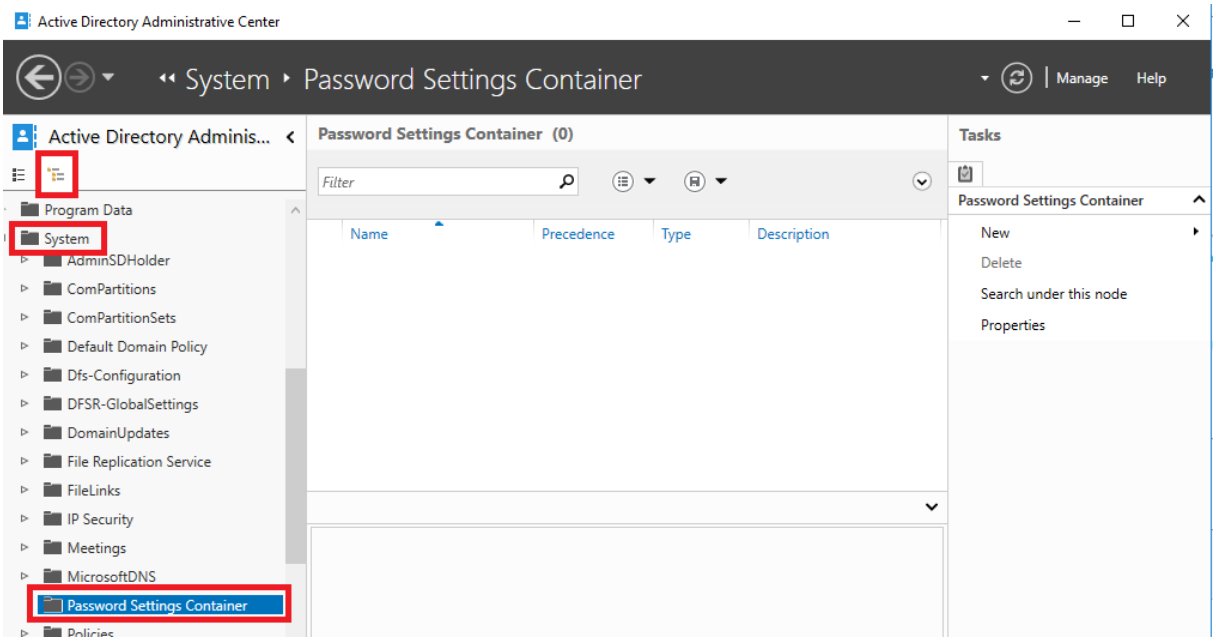
De Fine-Grained Password Policies kunnen gekoppeld worden aan users of aan security groepen, dus NIET aan OU’s.

Voorbereidend werk

- Maak in AD een security groep met de naam finegrained, leden van deze groep krijgen een van de default domain policy afwijkende password policy.
- Voeg één of meerdere gebruikers toe aan deze groep

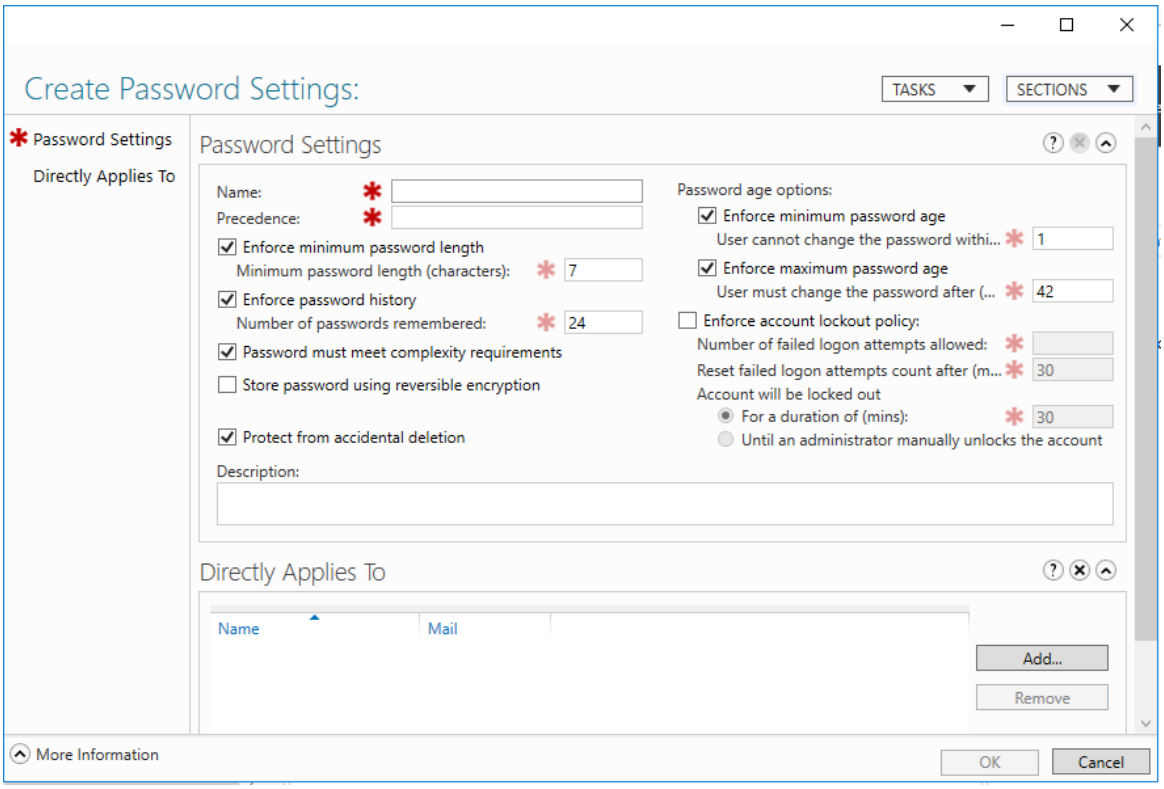
De instellingen voor de fine grained password policy bepalen

- Start ADAC, schakel naar Tree View en navigeer naar System > Password Settings Container.



- Klik met de rechtermuisknop op de Password Settings Container en selecteer New > Password Settings.

- In het venster **Create Password Settings** kan je de gewenste instellingen kwijt:

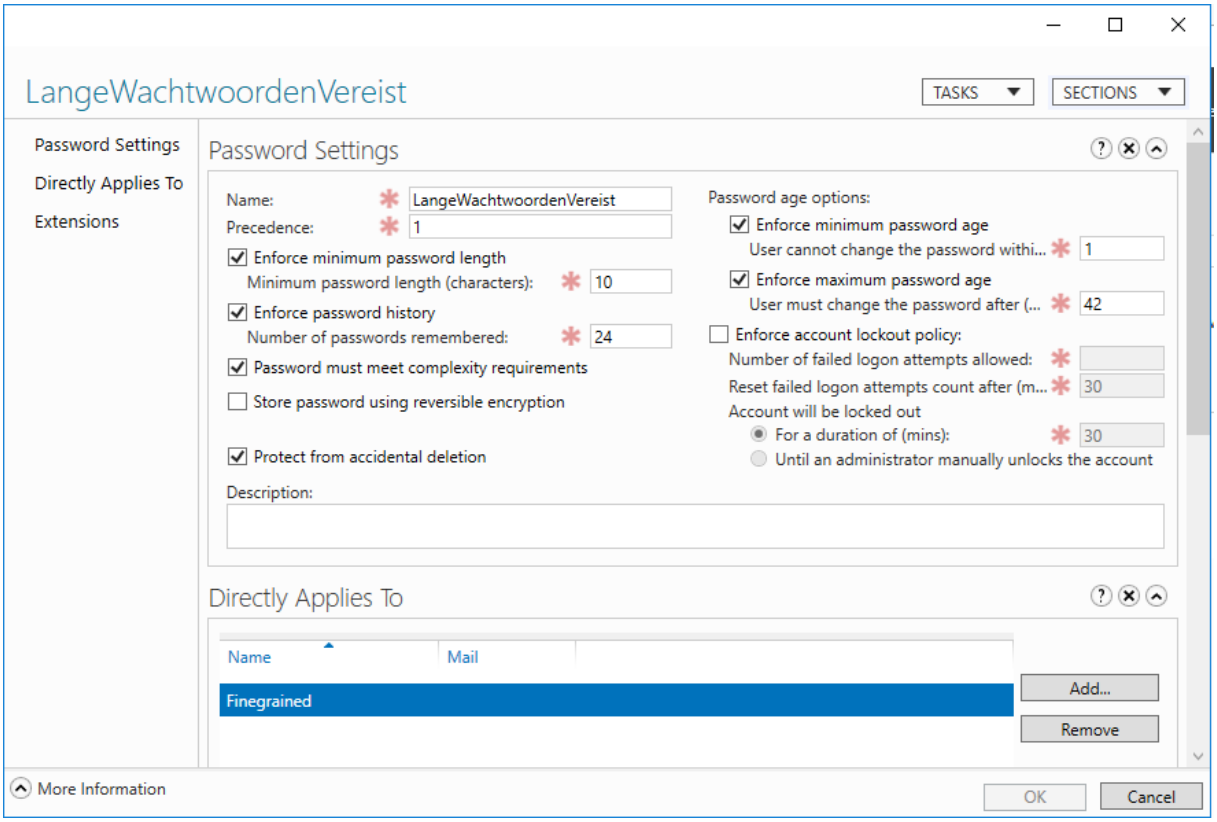


Twee velden zijn verplicht in te vullen: **Name** en **Precedence**:

- *Name*: Geef een beschrijvende naam waaruit ook blijkt met welke bedoeling de Password Policy aangemaakt wordt.
- *Precedence*: In geval meerdere fine grained password policies van toepassing zijn op eenzelfde gebruiker wint de policy met de laagste waarde bij Precedence. In geval van gelijke waarden bij Precedence wint de policy met de kleinste GUID. Vul de waarde 1 in.
- Maak de vereiste lengte van het wachtwoord groter dan de standaardwaarde, b.v. 10.
- Voeg bij **Directly Applies To** de groep *finegrained* toe.

Nagaan welke regels voor het wachtwoord van een bepaalde gebruiker gelden

- Navigeer in ADAC naar een gebruiker van de groep finegrained. Tip: Je kunt Hiervoor Global Search gebruiken
- Klik met de rechtermmuisknop op de gebruiker en kies **View resultant password settings**... ADAC toont de instellingen van de policy met de laagste precedence die van toepassing is op de gebruiker.



Nog een toepassing

Wijzig de instellingen als volgt:

- Alle gebruikers krijgen een lockout na 3 mislukte aanmeldpogingen.

- Wachtwoorden moeten minstens 8 karakters lang zijn voor cursisten en 12 voor de instructeurs.
- Het wachtwoord vervalt om de maand voor cursisten, om het jaar voor de instructeurs.

4.2.2 Andere Beveiligingsinstellingen

Naast Domain Level Security instellingen leveren GPO's nog een groot aantal security instellingen. Je vindt die terug onder **Security Settings** in **Windows Settings** van zowel de **Computer** als de **User Configuration**.

Enkele Security Settings in de Group Policies

Configuratie optie	Verklaring
Local Policies\Audit Policy	Gebruikt om de audit instellingen te configureren. Je kunt audit instellingen meegeven voor accountbeheer, logon events, policy wijzigingen en system events.
Local Policies\User Rights Assignment	Instellingen voor de rechten die de gebruikers hebben op de computer. Vb: lokaal op de computer aanloggen, toegang tot de computer krijgen via het netwerk, een backup maken en terugplaatsen van bestanden en mappen, aanloggen als een service,…
Local Policies\Security Options	Opties zoals de lokale administrator hernoemen, beheer van wie printers kan installeren, controleren of unsigned drivers kunnen geïnstalleerd worden, …
Event Log	Instellen van de maximum grootte van de event logs, instellen wie toelating heeft om de event logs te zien,…
Restricted Groups	Het lidmaatschap van lokale groepen beperken. Meestal wordt dit gebruikt om de lokale Administrators groep te configureren. Alle gebruikers of groepen die lid zijn van de lokale groep maar niet in de ledenlijst van de policy worden bij elke update van de policy verwijderd.
System Services	Je kunt deze policy gebruiken om te definiëren welke services automatisch opstarten of om services uit te schakelen.
Registry	Instellingen van veiligheid op de registry keys. Je kunt elke key van de registry toevoegen aan de policy en er specifieke beveiliging op toepassen.

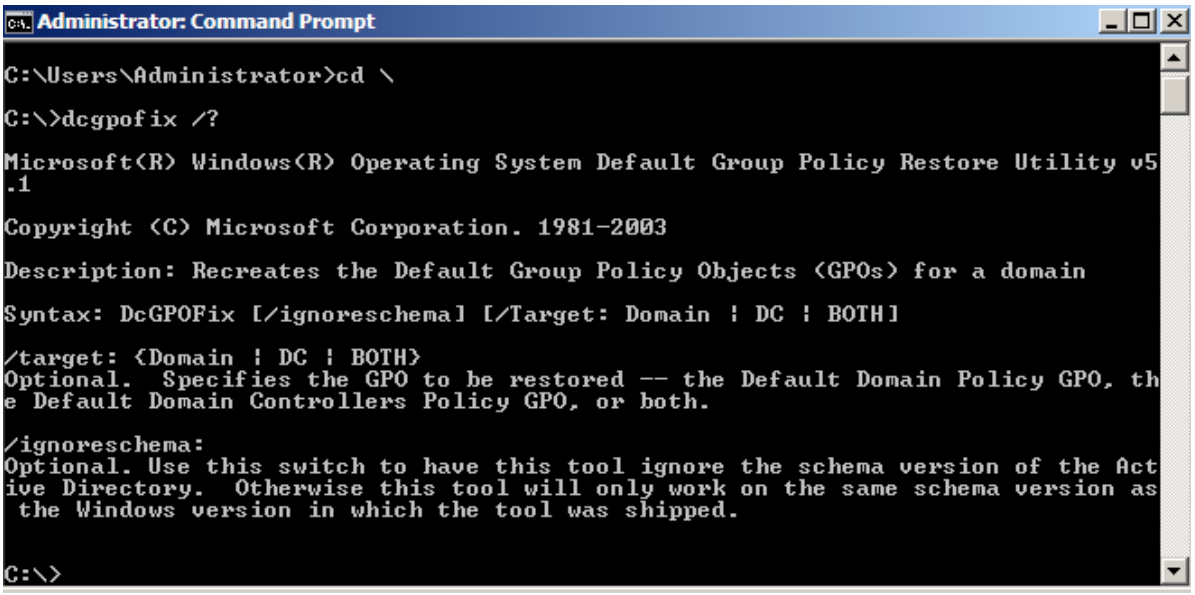
Enkele Security Settings in de Group Policies

Configuratie optie	Verklaring
File System	Instellingen van beveiliging op bestanden en mappen. Je kunt ieder bestand of map toevoegen aan de policy en er access control en auditing op toepassen.
Wireless Network (IEEE 802.11) Policies	Controle van de security voor computers met draadloze netwerkverbindingen.
Public Key Policies	Instellingen van policies die te maken hebben met digitale certificaten en certificaten beheer.
IP Security Policies On Active Directory (*domainname)*	Instellen van IP Security Policies. Je kunt policies configureren die precies definiëren welk type netwerkverkeer moet beschermd worden met IPSec.

Opmerking: Wees uiterst voorzichtig met het aanpassen van de Default Domain Policy en de Default Domain Controller policy!
Bij problemen of wanneer je terug wil keren naar de default instellingen kan je een beroep doen op de tool dcgpofix.exe. Deze tool biedt de mogelijkheid om de domain of de domain controller policy of beide te herstellen naar de beginsituatie.

de syntax voor het terugzetten van de default domain policy is:
dcgpofix /target:domain

Meer info over de tool krijg je door dcgpofix /? Te typen aan de prompt.



4.2.3 Software Restrictie GPO's

Software restriction GPO's beschermen gebruikers tegen onveilige software door te definiëren welke toepassingen wel of niet mogen gebruikt worden.

Er zijn twee benaderingen mogelijk:

- Ofwel mag alle software gebruikt worden, uitgezonderd de software die geblokkeerd wordt.
- Ofwel mag er geen software gebruikt worden uitgezonderd de software die expliciet toegelaten wordt.

Hoewel de tweede benadering het veiligst is, is die moeilijk te verwezenlijken in een bedrijf.

Wanneer je een software restriction policy maakt, kan je op vijf verschillende manieren configureren welke toepassingen beïnvloed worden door de policy.

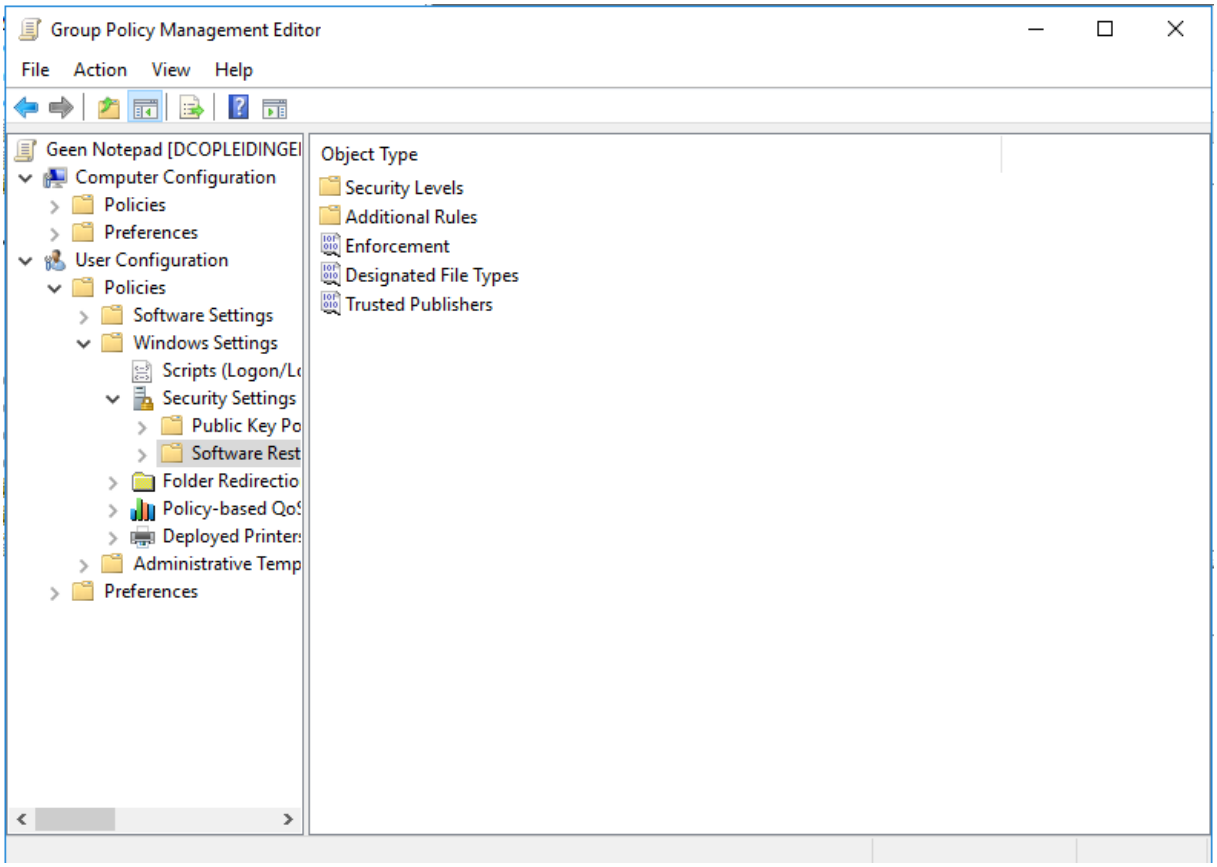
- **Certificate rules** Deze rule is gebaseerd op het certificaat van de uitgever van de software.
- **Hash rules** Een hash rule is een cryptografische herkenningssleutel die een applicatie bestand uniek identificeert, ongeacht de bestandsnaam of locatie.
- **Network zone rules** Deze rule is gebaseerd op de Network Zone van waar de software werd afgehaald: Internet, Local computer, Local intranet, Restricted sites, Trusted sites.
- **Path rules** De laatste rule is gebaseerd op het path waar het toepassingsbestand zich bevindt.

Voorbeeld :

Doel: notepad blokkeren met een hash rule

- Open de GPMC
- Selecteer een OU waarop je de restrictie wil toepassen (bijvoorbeeld de OU Antwerpen)
- Maak een nieuwe GPO en navigeer via de group policy editor naar

  User Configuration \ Policies \ Windows Settings \ Security settings \ Software Restriction Policies.
- Klik, om een policy te maken, rechts op Software Restriction Policies en kies voor **New Software Restrictions Policy**. Daardoor wordt een default policy gemaakt.



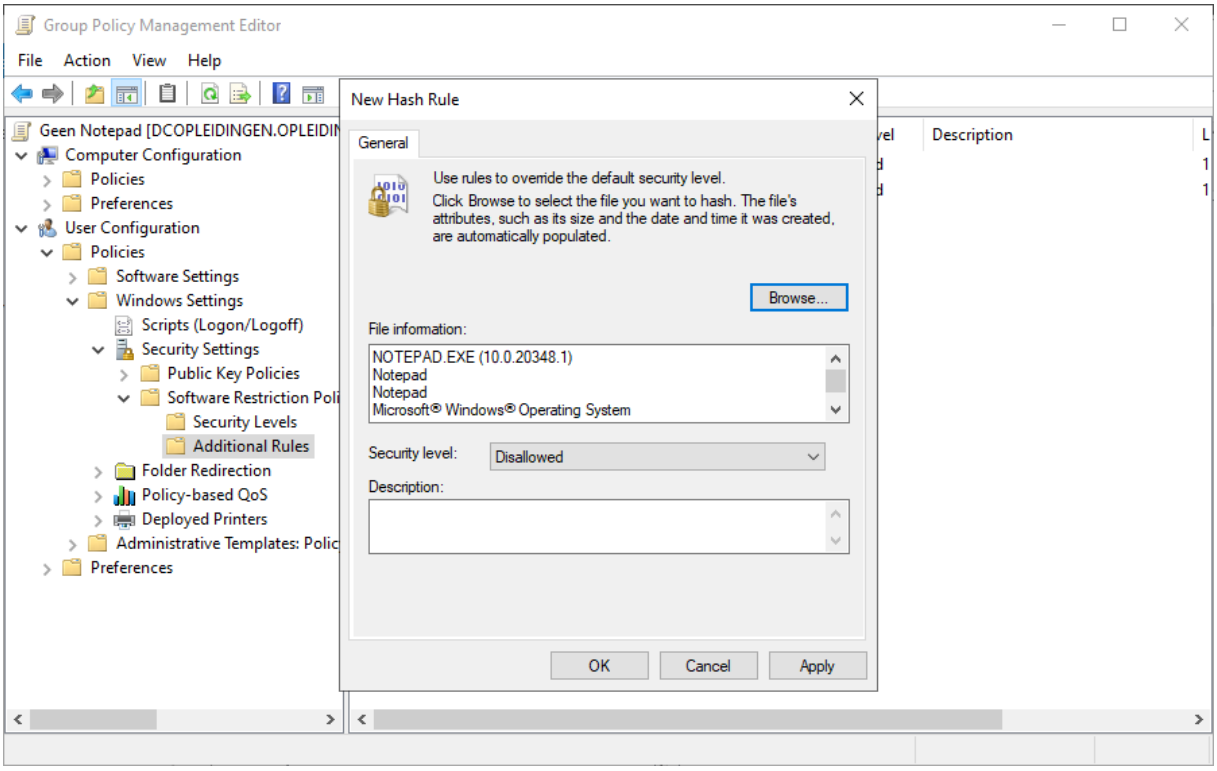
De Security Levels map wordt gebruikt om het standaard security niveau in te stellen. In de map vind je drie objecten, *Disallowed*, *Basic user* en *Unrestricted*. Standaard is Unrestricted ingeschakeld.

De Additional Rules folder wordt gebruikt om de software restrictie rules in te stellen.

- 🛠 Klik rechts op de additional Rules folder en selecteer het type rule dat je wilt. Kies hash rule.
- 🛠 Klik op Browse om het bestand te vinden dat je wilt beperken en kies voor allowed of disallowed.

LET OP: iedere versie van een programma heeft zijn eigen hash key. De versie op de server komt niet altijd overeen met die op de client.

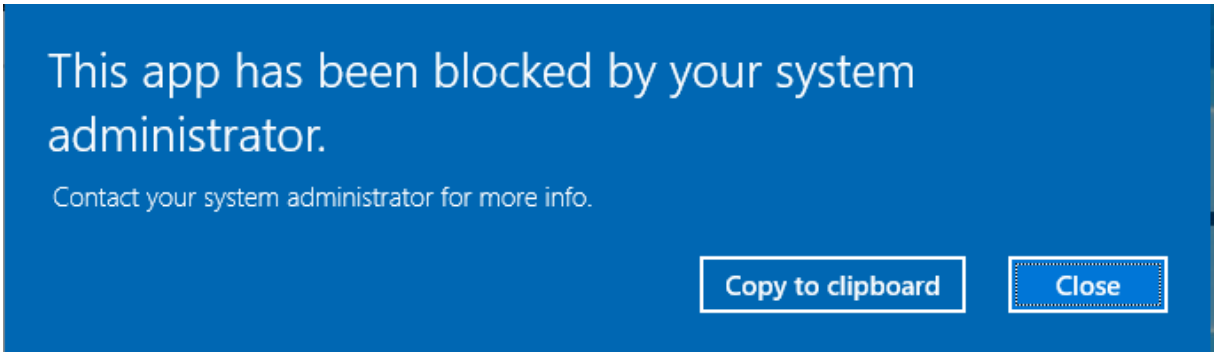
Door de versie van de client te kopiëren naar een map op de server en de hashrule toe te passen op de kopie kan je dit probleem oplossen.



- Het securitylevel stel je in op disallowed
- Klik op OK: de software restrictie is ingesteld.

Test dit uit op de client

- Log aan met een user binnen de OU waarop je de GPO hebt gemaakt
- Open het programma Notepad
- Volgende boodschap verschijnt



4.2.4 Security Templates

Zoals je reeds zult gemerkt hebben, bestaan er honderden opties voor het instellen van de security in GPO's. Gelukkig heeft Microsoft security templates voorzien om het beheren wat te vergemakkelijken.

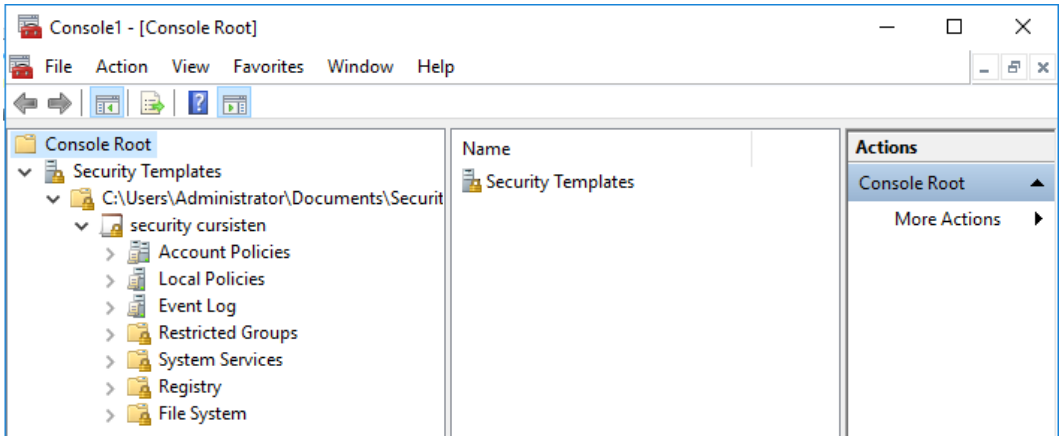
Security templates zijn voorgedefinieerde sets van security configuraties die je kunt toepassen op je computers op het netwerk.

Bijna alle security instellingen die via een group policy gebeuren, kunnen geconfigueerd worden met een security template. (uitzonderingen: IPSec en public key policies).

4.2.4.1 Een security template maken

Werkwijze:

- Open de MMC console (via start – mmc.exe)
- Ga naar **File -> add/remove snap-ins**
- Selecteer **Security Templates** in de linkse kolom en klik op **Add** en vervolgens OK
- Vouw de node onder security template open
- Op c:\users\administrators\... klik je met de rechtermuisknop -> kies **New Template**
- Geef de Template een naam en klik op OK
- Pas de security aan naar wens



- Om de template te bewaren klik je met de rechtermuisknop op de naam van de template en kies **Save As.** Bewaar de template onder c:\windows\security\templates
- De template is klaar voor gebruik

4.2.4.2 Een security template toepassen

Werkwijze:

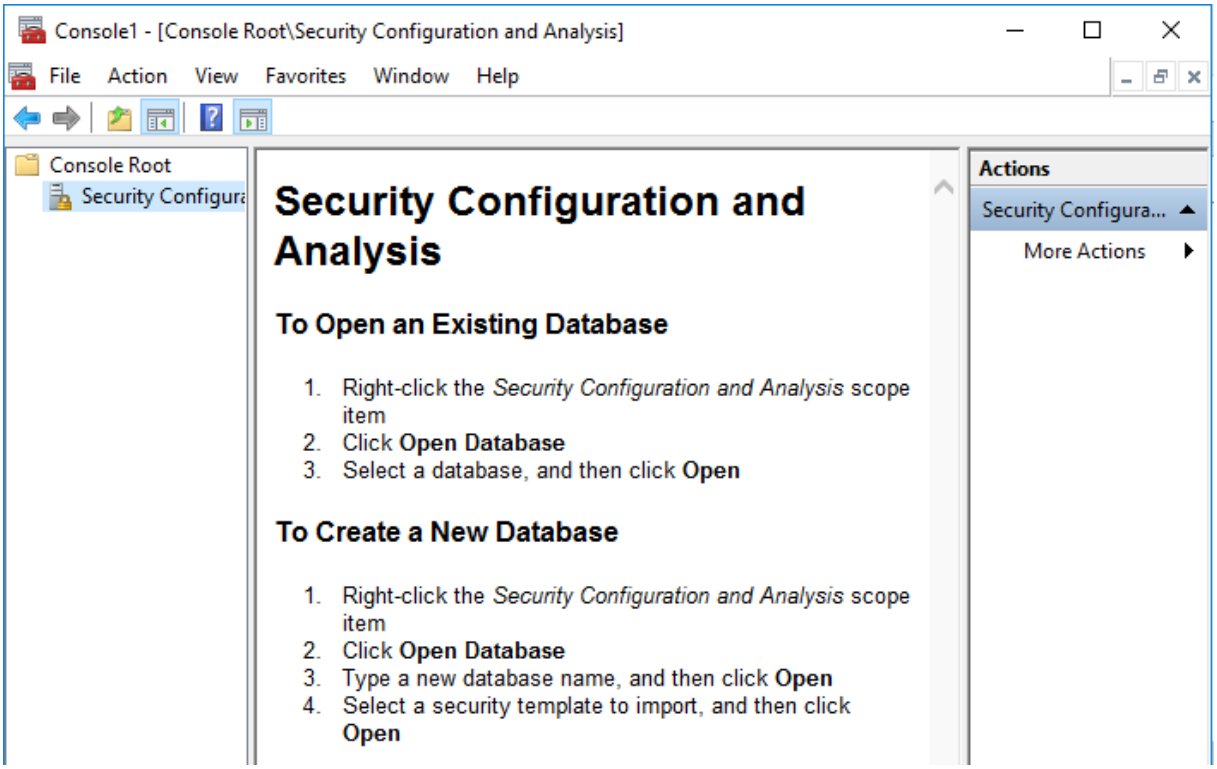
- Open de GPMC

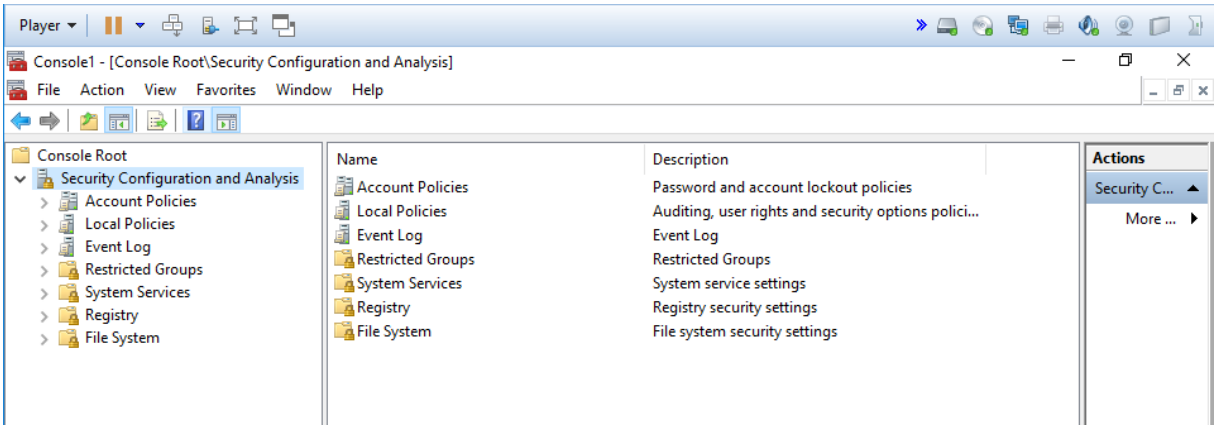
- Maak een nieuwe GPO ter hoogte van de OU waarop je de template wil toepassen.
- Editeer de GPO
- Ga naar Computer Configuration -> Policies -> Windows Settings -> Security Settings
- Klik met de rechtermuisknop op security settings en kies **Import Policy**
- Ga naar de map waar je de template hebt opgeslagen en selecteer de template die je wenst toe te passen en klik op Open.
- De template wordt nu toegepast op de GPO

4.2.4.3 Extra Security Configuratie en Analyse Tools.

Windows Server voorziet nog extra tools om de security templates te beheren en toe te passen.

<u>Security Configuration And Analysis snap-in.</u>
Deze snap-in kan je gebruiken om security templates te maken of te wijzigen. De template kan je daarna in de Security Configuration And Analysis snap-laden en gebruiken om specifieke computers te analyseren. Je kunt bijvoorbeeld een hoge security template inladen en dan een computer analyseren om te zien wat het verschil is tussen de template en de huidige computer configuratie.





Als je beslist om de high security template op de computer toe te passen, klik dan rechts op Security Configuration And Analysis en selecteer **Configure Computer Now**.

Secedit.exe
De Secedit command-line tool voorziet gelijkaardige functionaliteit. Je kunt de computer analyseren op basis van een template en daarna de instellingen toepassen. Secedit bevat een practische rollback functie.

4.3 Group Policies voor Software beheer

4.3.1 Overzicht

Het beheer van software op de clients is één van de belangrijkste taken op een netwerk. Dit is een zeer arbeidsintensieve taak als een administrator iedere desktop moet bezoeken voor elk nieuw software-pakket dat moet geïnstalleerd of ge-upgraded worden. Het gebruik van group policies biedt een oplossing voor dit probleem.

4.3.2 Windows Installer Technologie

In de meeste gevallen werkt software beheer via group policies met de Microsoft Windows Installer technologie. Windows Installer technologie wordt gebruikt om software op Windows werkstations te installeren, te beheren en te verwijderen. Zij bestaat uit 2 componenten:

- **Een software installation package bestand (.msi file)**
  Het .msi bestand bevat een database met alle instructies om de applicatie te installeren of te verwijderen.
- **De Windows Installer service (Msiexec.exe)** Deze service beheert de installatie van de software op het werkstation. De service gebruikt een dynamic link library (DLL), Msi.dll, om het .msi bestand te lezen. Gebaseerd op de inhoud, kopieert de service applicatie bestanden naar de lokale harde schijf, maakt snelkoppelingen, verandert de registry en voert alle taken uit die in het .msi bestand vermeld staan.

Het gebruik van de Windows Installer Technologie heeft een aantal voordelen. Het grootste voordeel is dat een applicatie zelf-genezend wordt. Hetzelfde bestand kan immers gebruikt worden om een applicatie die niet meer werkt te herstellen. Het .msi bestand laat ook volledige desinstallatie toe.

De meest software fabrikanten voorzien een .msi bestand. Zelf een msi bestand maken kan, mits de nodige tools. In deze cursus gaan we daar niet verder op in.

4.3.3 Software verspreiden met Group Policies

4.3.3.1 Software beschikbaar stellen voor de gebruikers

Vooraleer je een applicatie kunt verdelen naar de gebruikers, moet je eerst de software installatie bestanden, inclusief het .msi bestand, kopiëren naar een netwerk share die beschikbaar is voor alle gebruikers. Let erop dat de gebruikers voldoende rechten hebben op die share. Als je applicaties toekent aan computers, dan moeten de computer accounts Read access hebben. Als je software toekent aan gebruikers, dan moeten die gebruikers Read access hebben.

Als voorbeeld zullen we het programma Cosmo1 via een GPO verspreiden. De msi file en bijbehorende bestanden zijn terug te vinden in de map met de oefenbestanden.

- 🛠 Bij de oefenbestanden van deze cursus vind je een folder packages
- 🛠 Deel deze map
- 🛠 Zorg ervoor dat users minstens leesrechten hebben op deze map

4.3.3.2 De GPO maken

Na het maken van de netwerkshare en het kopiëren van de installatie bestanden naar de share, ben je klaar om de GPO's te implementeren die de applicatie zullen adverteren naar de clients. Je kunt een nieuwe GPO maken of een bestaande GPO aanpassen.

De keuze die je moet maken: ga je adverteren naar computers of naar gebruikers?

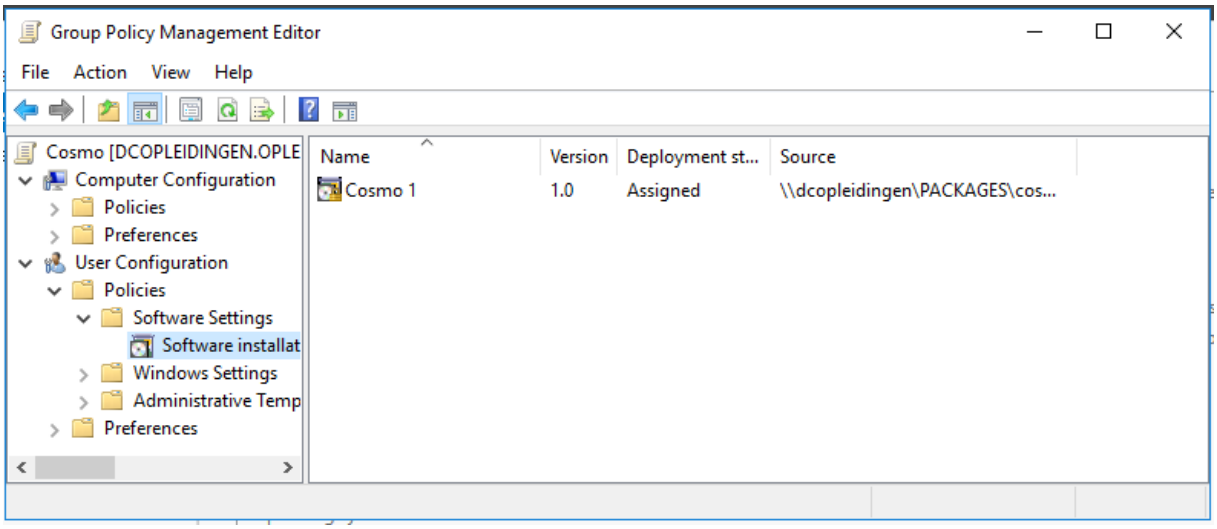
- Adverteren naar computers:
  dan gebruik je de Computer Configuration->Software Settings container in de Group Policy Object Editor en de applicatie wordt geïnstalleerd zodra het werkstation een volgende keer opstart.
- Adverteren naar gebruikers:
  dan gebruik je de User Configuration-> Software Settings container in de Group Policy Object Editor en de applicatie staat ter beschikking van de gebruikers zodra ze opnieuw aanloggen.

In ons voorbeeld:

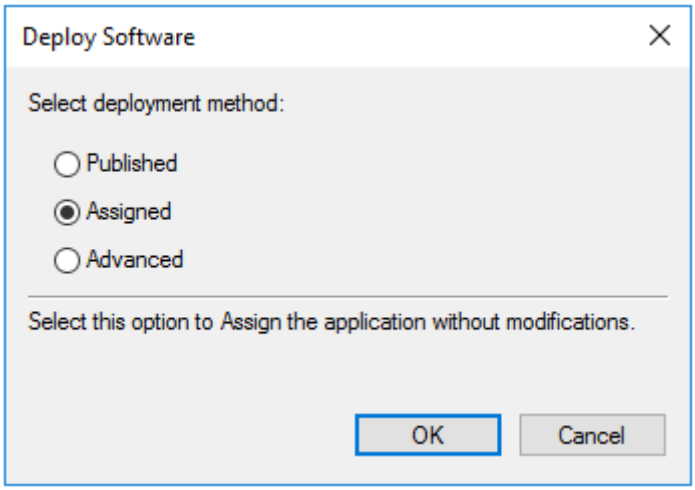
- Start de GPMC
- Selecteer een OU waarop je de GPO wenst te maken. (bv OU CC)
- Klik rechts op de OU en kies **Create a GPO in this domain and link it here**
- Geef de GPO een naam (bv: softwareinstallatie)
- Selecteer het GPO en klik op Edit
- Ga naar User configuration\policies\Software Settings\Software Installation
- Klik rechts met de rechtermuisknop en kies **New Package**
- Geef het **UNC pad** op voor het package. (het is belangrijk dat je geen lokale padaanduiding gebruikt, want dan wordt het package niet gevonden op het netwerk)
- Open de map cosmo1 en selecteer het msi bestand cosmo1.msi uit deze map
- Kies assigned (hier komen we dadelijk op terug)

De GPO is klaar.

Kijk goed na of de source weldegelijk verwijst naar een UNC pad. C:\... is GEEN verwijzing naar een UNC pad maar naar de lokale C-schijf en dat zal problemen geven bij de uitvoering van de GPO. Heb je hierbij een fout gemaakt dan kan je die enkel rechtzetten door het package opnieuw toe te voegen aan de GPO.



4.3.3.3 Assign of Publish



Hoe je de applicatie naar de client gaat adverteren is een tweede te maken keuze.

Je hebt de keuze tussen assign en publish.

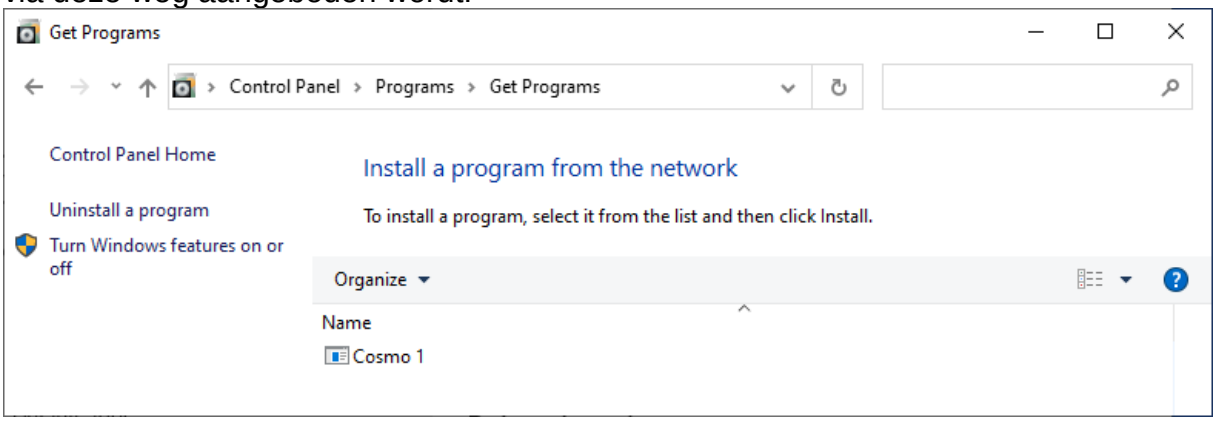
Assign:
Kan toegekend worden aan gebruikers en aan computers.
Als je een applicatie **toekent** (assign) aan een **computer**, dan is die volledig geïnstalleerd wanneer de computer de volgende keer opgestart wordt. De applicatie is beschikbaar voor alle gebruikers van de computer, de volgende keer dat ze zich aanmelden.

Als je een applicatie **toekent** (assign) aan een **gebruiker** dan wordt de applicatie beschikbaar als die gebruiker de volgende keer aanmeldt. Je kunt kiezen hoe de applicatie geadverteerd wordt, maar meestal wordt die toegevoegd aan het Start Menu. De applicatie wordt ook toegevoegd aan Programs and Features (onder Install a program from the network) in het Control Panel.
Standaard wordt die applicatie nog niet geïnstalleerd wanneer de gebruiker zich aanmeldt, maar wel wanneer de gebruiker de applicatie opstart via het Start menu of verkiest de installatie te doen via Programs and features

In ons voorbeeld:

- Log aan op de client met een user uit de OU waarop je de GPO hebt gemaakt.
- Bekijk het start menu. Cormo1 is toegevoegd. Door Cormo1 te selecteren wordt het programma geïnstalleerd en geopend.

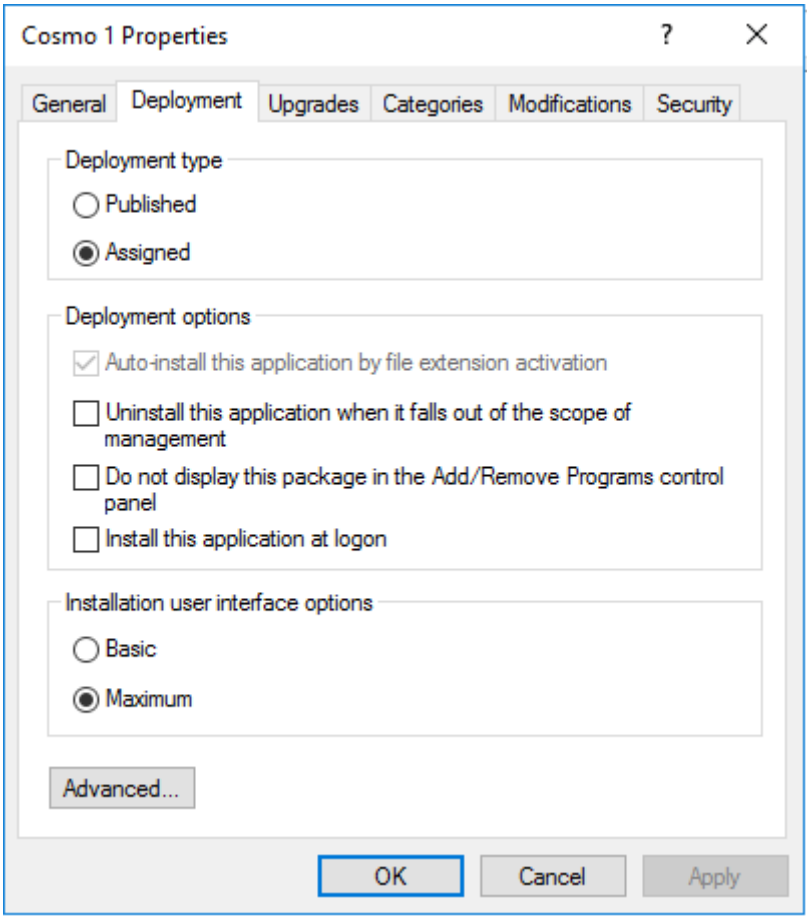
- Ga (via Search) naar Control Panel -> Programs -> Get Programs.
- Selecteer daar “Install a program from the network” en stel vast dat Cosmo1 via deze weg aangeboden wordt.



Publish:
Enkel toegekend aan gebruikers, niet mogelijk bij computers.
Als je een applicatie **publiceert** naar de **gebruiker**, dan wordt de applicatie geadverteerd de volgende keer dat de gebruiker aanmeldt op het netwerk. In dit geval wordt de applicatie ENKEL getoond in het Control Panel (onder “Install a program from the network”) en NIET in het start menu. Standaard worden gepubliceerde applicaties ook geïnstalleerd via de extensie activatie.

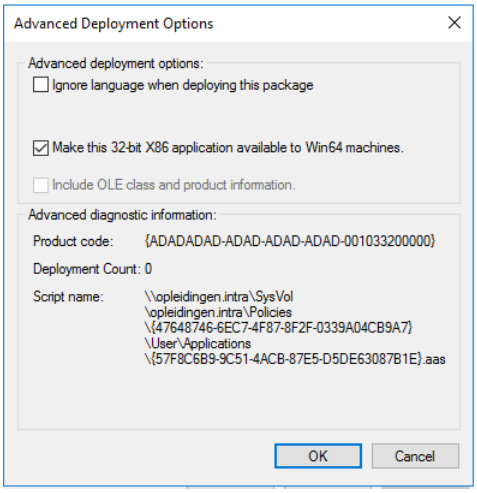
4.3.4 Configuratie van de Software Package Properties

Na het maken van een package kan je de properties aanpassen. Klik rechts op het package en kies voor **Properties**. Hieronder zie je het Deployment tabblad.



Verspreidingsopties voor een software package

Instelling	Verklaring
Deployment Type	Hoe wordt de applicatie geadverteerd?
Auto-Install This Application By File Extension Activation	Inschakelen of uitschakelen van de optie om software te installeren als de gebruiker een bestand opent met de geselecteerde extensie. Deze optie is niet beschikbaar voor de toegekende (assigned) applicaties
Uninstall This Application When It Falls Out Of The Scope Of Management	Wat gebeurt er als de group policy niet langer geldt voor de gebruiker of de computer? Als je deze optie selecteert en die slaat op een OU dan wordt de software verwijderd als de gebruiker uit de OU verwijderd wordt
Do Not Display This Package In The Add/Remove Programs Control Panel	Deze package komt niet in de Add Or Remove Programs control panel als je dit aankruist

Install This Application At Logon	Wacht niet op de gebruiker om de installatie te starten, maar doe dit reeds bij het aanloggen. Kan niet bij het publiceren
Installation User Interface Options	Wat ziet de gebruiker tijdens de installatie? Basic: alleen foutberichten en eindberichten. Maximum: alle setup schermen
Advanced 	Extra instellingen. o.a. installatie van 32 bit applicaties op 64 bit besturingssystemen, installeren zelfs als de taal niet klopt, toevoegen van COM componenten met de package zodat de client de componenten kan installeren vanuit de AD

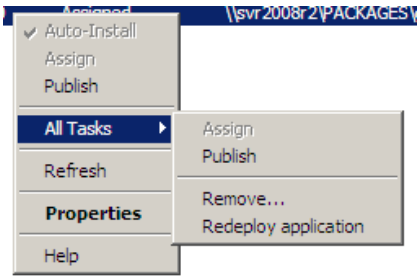
4.3.4.1 Update van een bestaand Software Pakket

Een interessant onderdeel van de installatie via de group policies is de optie om bestaande software pakketten up te daten. Er zijn twee mogelijkheden om dit te bekomen:

1. patching en installeren van een service pack op een bestaande applicatie
2. upgraden van een applicatie naar een nieuwe versie.

De twee methodes vragen verschillende procedures.

Voor het toepassen van patches of service packs op bestaande pakketten, moet je eerst het .msi bestand of het .msp bestand bekomen. Kopieer het nieuwe .msi bestand en de eventuele installatiebestanden naar de netwerk share en overschrijf de dubbele bestanden. Herverdeel nu de applicatie. Klik daarvoor rechts op het software pakket in de Group Policy Object Editor, selecteer All Tasks en selecteer Redeploy Application.



Voor een upgrade naar een nieuwere versie geldt een andere benadering. Hiervoor moet je een nieuw software pakket creëren. Daarna kan je bij de eigenschappen van het software pakket, klikken op het *Upgrades* tabblad. Gebruik de instellingen op dat tabblad om de link te leggen tussen het nieuwe pakket en het bestaande. Als je op Add klikt, kan je selecteren welk software pakket een upgrade zal krijgen. Je kunt ook instellen of het oude pakket moet verwijderd worden alvorens het nieuwe te installeren.

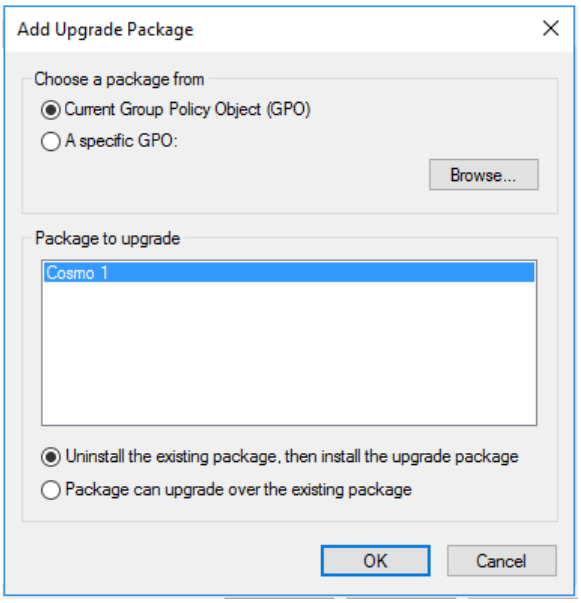
Als je de upgrade link aanmaakt, toont het upgrade tabblad de nieuwe info. Je kunt via dit tabblad ook maken dat de update verplicht is. Dan wordt alle software die verdeeld werd door de vorige GPO, automatisch ge-upgrade bij het herstarten van de computer of het aanloggen van de gebruiker.

In ons voorbeeld: Upgraden naar cosmo2

- Open de vorige GPO en navigeer naar de sofware installation.
- Voeg een nieuw package toe dmv **New -> Package**
- Open in de share packages de map **cosmo2**
- Duid het msi bestand cosmo2 aan
- Bij Deploy Software kies je **Advanced.** Het dialoogvenster Properties wordt automatisch geopend
- Ga naar het tabblad **Upgrades.**

Bedoeling is dat cosmo2 een upgrade is van cosmo1.

- Om cosmo1 toe te voegen klik je op de knop **Add**



- **Choose a package from**: Current Group Policy object waardoor cosmo1 reeds getoond wordt in de onderstaande lijst.
- Selecteer Cosmo1 bij Package to upgrade.
- Laat het bolletje staan bij Uninstall the existing package, then install the upgrade package. In dit geval is deze optie noodzakelijk omdat Cosmo2 een volwaardig nieuwe versie is van het programma, het is GEEN upgrade van Cosmo1. In dat geval had je de andere optie moeten kiezen.
- Bevestig met OK
- PC's waarbij cosmo1 nog NIET is geïnstalleerd zal dadelijk Cosmo2 geïnstalleerd worden. In ons geval is Cosmo1 reeds geïnstalleerd op de Client. Wens je deze te vervangen door Cosmo2 plaats dan op het tabblad Upgrades een vinkje bij **Required upgrade for existing packages**.
- Ga vervolgens naar het tabblad Deployment om het deployment type op Assigned te zetten.
- Klaar! Klik op OK om te bevestigen.

Aan de GPO wordt het tweede software pakket toegevoegd.

Test op de Client

- Log aan op de client met een user uit de OU waarop je de GPO hebt gemaakt.
- Bekijk het start menu. Als alles goed is verlopen zou Cosmo1 vervangen moeten zijn door Cosmo2.

4.3.4.2 Verwijderen van Software met de Group Policies.

Er zijn drie opties om software te verwijderen:

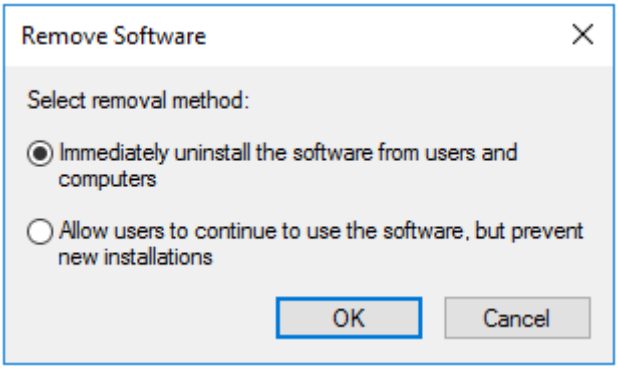
- Software verwijderen als voorbereiding op een nieuwe versie.
- Software verwijderen als de gebruiker niet meer onder het bereik van de GPO valt.
- Software verwijderen als je het software pakket verwijdert.

De eerste twee opties hebben we al eerder gezien. De derde vraagt wat meer uitleg. Als je een software pakket verwijdert, kan je kiezen om het onmiddellijk te desinstalleren. Dan wordt de software verwijderd bij een volgende aanmelding van de gebruiker of herstart van de computer.

Andere mogelijkheid is om geen nieuwe installaties meer te laten gebeuren, maar de reeds geïnstalleerde niet te verwijderen.

Werkwijze:

- Selecteer het software package dat je wenst te verwijderen
- Klik met de rechtermuisknop en kies **All tasks -> remove**
- Maak een keuze in het **remove software** venster



4.3.5 Beperkingen bij het gebruik van GPO's om de software te beheren.

Er zijn enkele beperkingen aan het gebruik van de GPO's.

- Applicaties worden pas geïnstalleerd bij opnieuw aanmelden of heropstarten.
- Er wordt geen gebruik gemaakt van de multicasting mogelijkheden.
- Er wordt niet gerapporteerd. Je weet niet of een installatie lukte of niet.

4.4 Administrative Templates

Eén van de krachtigste opties voor het beheren van desktops met GPO's zijn de Administrative Templates. Die worden gebruikt om de registry instellingen van computers en servers te configureren.

Enkele voorbeelden van Administrative Templates	
Administrative template locatie	Verklaring
Computer Configuration\Administrative Templates\System\Net Logon	Instellingen die de locatie van de clients controleert en de DNS records in een cache opslaat
Computer Configuration\Administrative Templates\System\Remote Assistance	Instellingen voor de Remote Assistance.
User Configuration\Administrative Templates\Desktop	Wat mag wel of niet getoond worden op de desktop ?
User Configuration\Administrative Templates\Network\Network Connections	Voorziet een waaier van instellingen voor het beheer van netwerkverbindingen en het beperken van de gebruikerstoegang op die verbindingen.
User Configuration\Administrative Templates\Control Panel	Instellingen voor het control panel en de mogelijkheden van de gebruiker om die instellingen te wijzigen.
User Configuration\Administrative Templates\Start Menu and Task bar	Instellingen voor het start menu en de taakbalk.

Een voorbeeld:

- Maak een nieuwe GPO.
- Ga naar **User Configuration** > **Policies** > **Administrative Templates**
- Enable volgende setting binnen de volgende item:

Desktop	Remove Recycle Bin icon from Desktop

- Koppel de GPO aan de OU Genk
- Sluit de Group Policy Management Editor.
- Schakel over naar de Windows client en log aan met een gebruiker in de OU Genk.
- Kijk na of de setting toegepast worden.
- Log aan met een andere gebruiker die geen lid is van de OU Genk. De instelling is voor deze gebruiker NIET van kracht.

4.5 Preferences

Group Policy Preferences (GPP) is een andere reeks client side extensions die bestaan vanaf Windows Server 2008 en die de mogelijkheid bieden om instellingen van het besturingssysteem en applicaties te beheren.

Veel van de instellingen die je via de Preferences kan instellen kon je voordien niet via GPO's beheren, daarvoor moest je andere methodes aanspreken zoals werken met logon scripts.

Group Policy Preferences bieden meer dan 3000 instellingen op 22 verschillende gebieden binnen een Group Policy Object waaronder bijvoorbeeld het toewijzen van schijfstations en printers en het beheer van lokale groepslidmaatschappen

4.5.1 Het verschil tussen Group Policy Preferences en Policy Settings

Group policy preferences en Group policy settings zijn twee verschillende technologieën. Ze verschillen van elkaar op gebied van Enforcement en Targeting.

Enforcement (afdwingen): Bij het configureren van Group Policy settings worden de instellingen afgedwongen. De gebruikersinterface wordt uitgeschakeld en voorkeuren worden ververst. Bij Group Policy Preferences worden voorkeuren NIET afgedwongen en kunnen maar 1 keer ververst of toegepast worden. De gebruikers interface wordt NIET uitgeschakeld. Wat wil zeggen dat de gebruiker de instellingen kan aanpassen naar eigen willekeur.

Targeting: een beperking van de Group policy settings is dat je geen filtering kan toepassen op individuele policy settings. De enige optie die je hebt is om specifieke GPO's per policy setting te creeëren en deze te laten uitvoeren gekoppeld aan een bepaalde WMI filter of security Group filtering. Group Policy preferences bieden de mogelijkheid om item level targeting toe te passen. Zo kan je bijvoorbeeld een drive mapping leggen voor twee verschillende afdelingen waarbij je één preference instelt voor de ene afdeling en een andere preference voor de andere afdeling en dat binnen dezelfde GPO.

4.5.2 Group Policy Preferences settings

Group Policy Preferences is een technologie die het Group Policy mechanisme gebruikt om instellingen door te voeren.

Enkele verschillen tussen Policies en Preferences:

- Instellingen doorgevoerd via Preferences vergrendelen de gebruikersinterface niet en dat in tegenstelling tot instellingen doorgevoerd via Policies.
- Verder worden instellingen gerealiseerd via Preferences niet verwijderd als de GPO verwijderd wordt of niet meer van toepassing is op de computer of de gebruiker.

De instellingen opgenomen in de Group Policy Preferences zijn onderverdeeld in Windows Settings en Control Panel settings.

Windows settings werden voor de invoering van Preferences ingesteld aan de hand van scripts die instellingen bevatten over drive mappings, de registry en omgevingsvariabelen.

Control panel settings zijn instellingen die voordien via het Control panel op het Client toestel werden ingesteld. Zoals Folder options, Power Options, Local Users en Groups en Start menu instellingen.

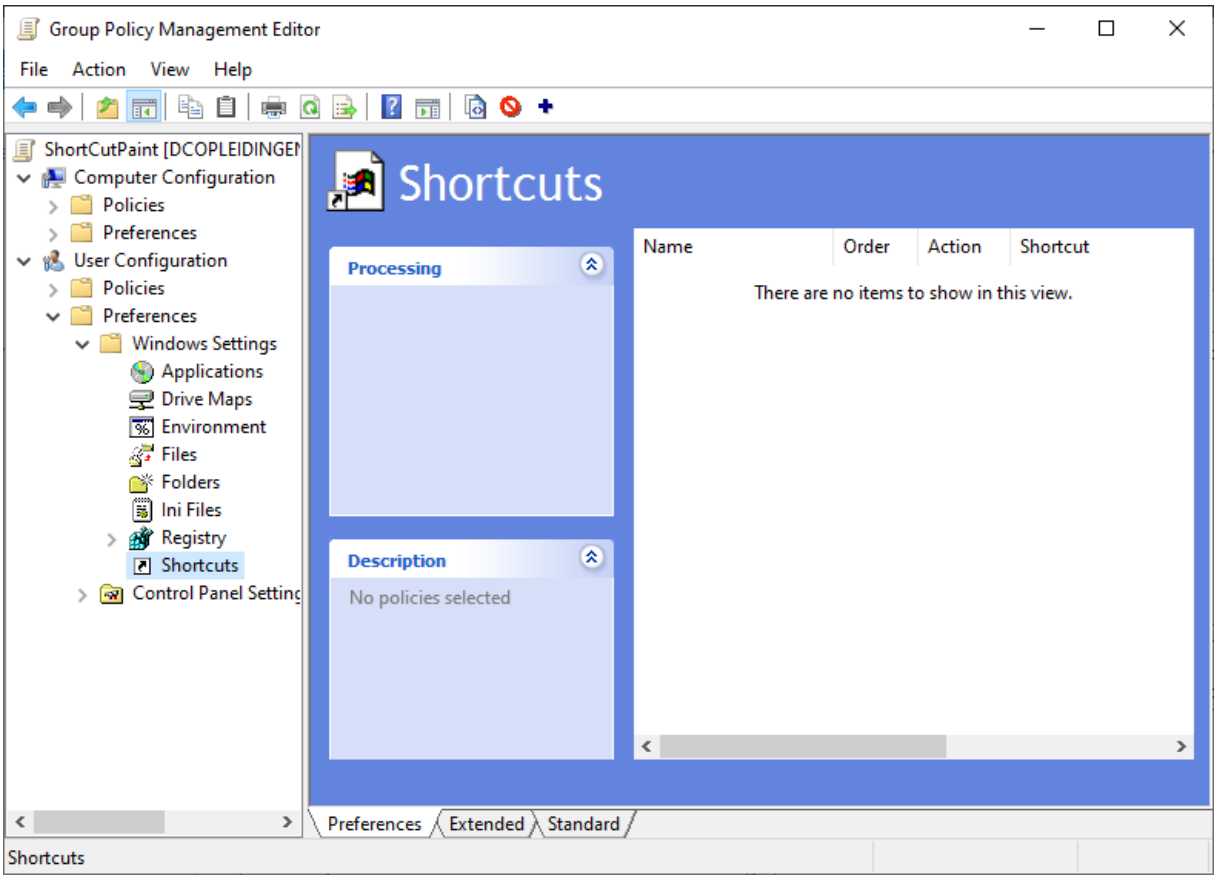
4.5.2.1 Windows Settings

Preference setting	**Omschrijving**
Environment	Biedt de mogelijkheid om gebruikers of systeem omgevingsvariabelen aan te passen.
Files	Laat toe om bestanden te kopiëren naar een andere lokatie. Bestaande bestanden of hun attributen kunnen aangepast of verwijderd worden.
Folders	Biedt de mogelijkheid om folders te maken, aan te passen of te verwijderen. Met deze preference kan je eveneens alle bestanden binnen een folder verwijderen. Bijvoorbeeld om de temp bestanden folder leeg te maken
Ini Files	Voor het aanpassen, vervangen of verwijderen van de inhoud van een .ini files. Je kan ook volledige ini files verwijderen.
Registry	Kopiëren, vervangen, maken, aanpassen of verwijderen van registry key waarden.
Network Shares (enkel onder computer configuration)	Hiermee kan je instellingen ivm Network shares maken, aanpassen of verwijderen
Shortcuts	Maken of verwijderen van shortcuts op client computers
Applications (enkel onder user configuration)	Biedt de mogelijkheid om de instellingen van applicaties te configureren.
Drive Mappings (enkel onder user configuration)	Biedt de mogelijkheid om drive mapping te maken, aan te passen of te verwijderen.

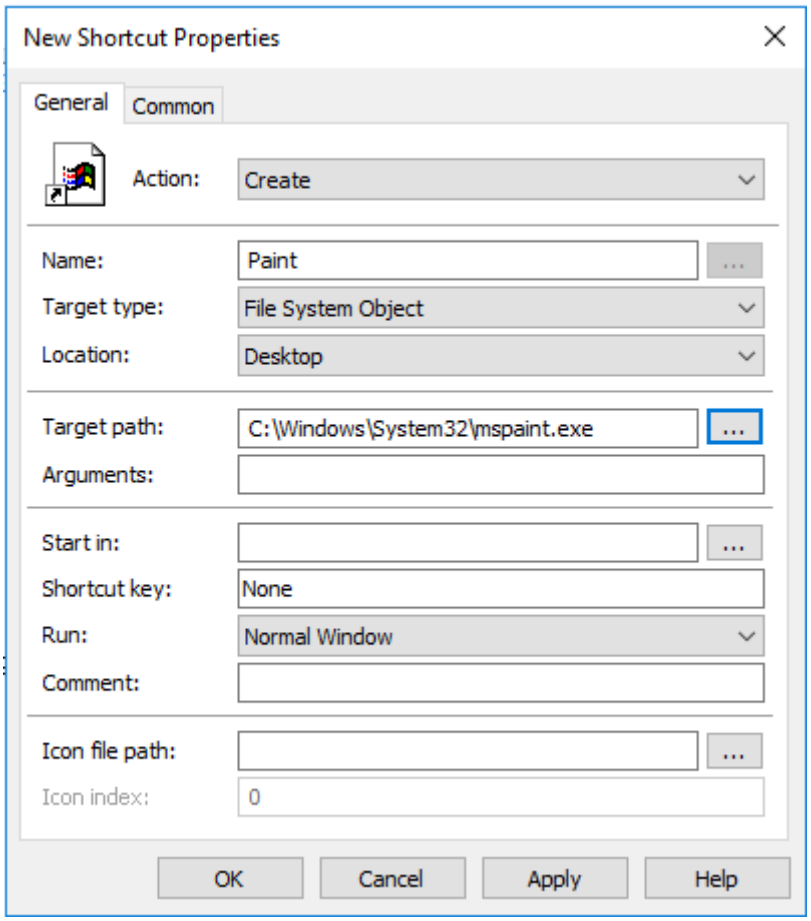
Een eerste voorbeeld

Doel: een shortcut naar het programma mspaint op de desktop van de gebruiker plaatsen

- Maak een nieuwe GPO met als naam ShortcutPaint en koppel die aan CC
- Ga naar User Configuration \ Preferences \ Windows Settings \ Shortcuts



- Klik in het witte gebied met de rechtermuisknop en kies **New -> Shortcut**
- Vul de eigenschappen in zoals op onderstaande figuur
  Het in te vullen path waar de applicatie staat verschilt afhankelijk van de versie van Windows op je toestel:
  - Windows 10: c:\Windows\System32\mspaint.exe
  - Windows 11: “C:\Program Files\WindowsApps\Microsoft.Paint_11.2311.30.0_x64__8wekyb3d8bbwe\PaintApp”



- 🛠 Klik op OK om te bevestigen

Test uit op de client.

- 🛠 Log aan met een gebruiker van CC. Verschijnt de shortcut op de desktop?

Tip:

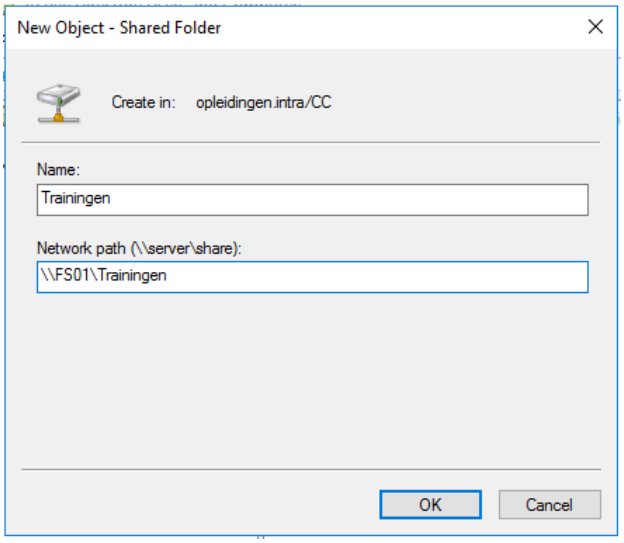
Het zou kunnen dat je meer dan 1 keer moet aanloggen.

Een tweede voorbeeld:

Doel: een drive mapping maken naar een gedeelde map (\\FS01\Trainingen)

Voorbereidend werk:

- 🛠 Maak een map Trainingen in de map Trajecten en deel die.
- 🛠 Publiceer de share *Trainingen* in active directory in de OU CC.

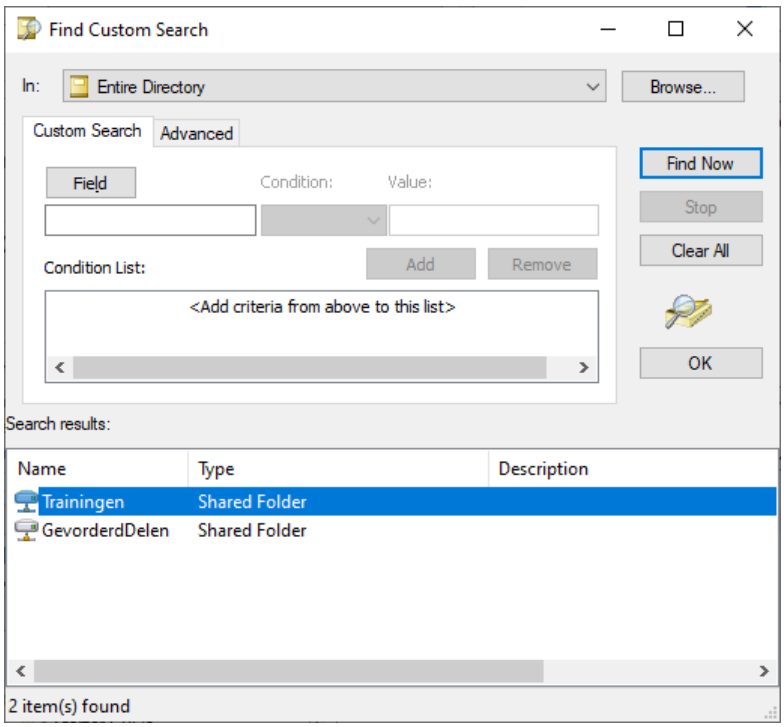


Instellen van de Preferences:

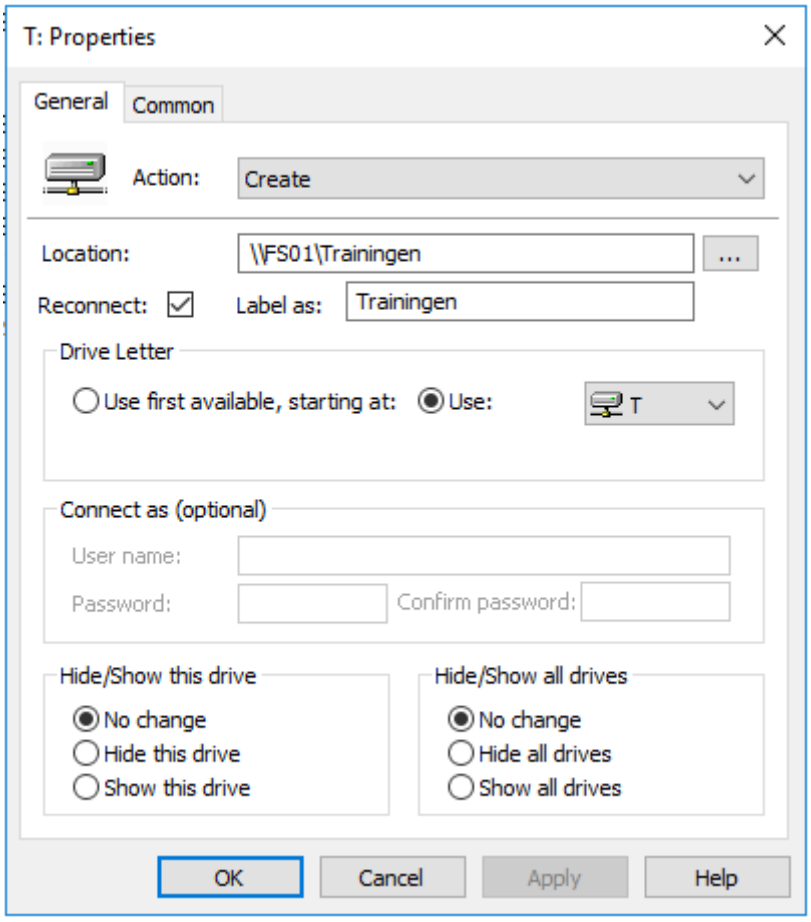
- Koppel een nieuwe GPO aan de OU CC met de naam MappingTrainingen.

Wijzig de GPOals volgt:

- **User Configuration \ Preferences \ Windows Settings \ Drive maps**
- Klik met de rechtermuisknop in het witte gebied. Kies **New -> Mapped Drive**
- Bij **Action** kies je voor **Create**
- Klik op de knop met de drie puntjes ter hoogte van **Location**
- Selecteer de map **Trainingen** en klik op OK



- In het dialoogvenster New Drive Properties zet je een vinkje bij Reconnect
- Vul een naam in bij Label As
- Kies een drive letter



- Bevestig met OK

Test op de Client

- Log aan met een gebruiker van CC en check het resultaat. Tip: het zou kunnen dat je 2 maal moet aanloggen vooraleer de mapping wordt gelegd.

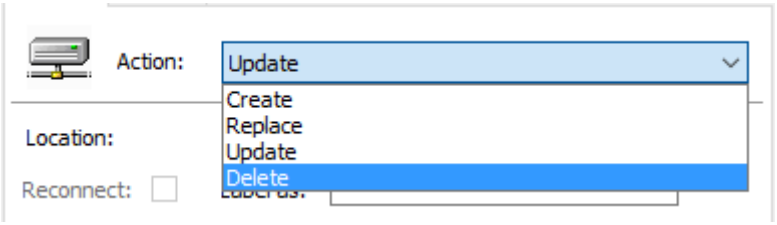
4.5.2.2 Control Panel Settings

Preference setting	Omschrijving
Data Sources	Biedt de mogelijkheid om centraal ODBC databronnen te configureren.
Devices	Hiermee kan je bepaalde types van hardware devices in- of uitschakelen. Zoals bijvoorbeeld USB poorten of floppy drives.

Preference setting	Omschrijving
Folder Options	Centraal beheer van de folder option zowel voor Windows XP als Windows Vista en latere versies.
Internet settings (user configuration)	Configuratie van de internet instellingen voor Internet Explorer
Local users and Groups	Biedt de mogelijkheid om centraal het beheer te doen van lokale users en groepen
Network Options	Hiermee kan je bijvoorbeeld VPN of Dail up connecties beheren
Power Options	Configuratie van de power options
Printers	Laat toe om lokale of netwerk printers te installeren, configureren of verwijderen
Regional Options (user configuration)	Instellingen naar getallen, kommanotaties, valuta en data zijn hier aanpasbaar
Scheduled tasks	Maken, aanpassen, beheren en verwijderen van taken
Start Menu (User Configurartion)	Biedt de mogelijkheid om het start menu te configureren
Services (Computer Configuration)	Configureren van de services

4.5.3 Group Policy Preferences Options

Volgende acties kunnen uitgevoerd worden op de Preferences



Create: een nieuw item of een nieuwe instelling wordt gemaakt en uitgevoerd

Replace: verwijdert een bestaand item en vervangt het door het nieuwe item hier ingesteld

Update: past een bestaand item aan of maakt het als het nog niet bestaat

Delete: verwijdert een bestaand item of bestaande instelling

5 NOG ENKELE TOEPASSINGEN

5.1 Selectief toepassen van GPO's

1. Maak drie .vbs bestanden

Hallo.vbs	Msgbox "hallo voor iedereen"
cursist.vbs	Msgbox "script van cursist"
instructeurs.vbs	Msgbox "script van instructeur"

2. Link de scripts via een GPO als logon scripts aan de OU CC en zorg ervoor dat de scripts als volgt uitgevoerd worden:

Hallo.vbs voor alle gebruikers in de OU CC

Cursist.vbs voor alle cursisten.

Instructeur.vbs voor alle Instructeurs.

3. Test uit door aan te melden met verschillende gebruikers op de client.

5.2 Installatie van software

1. Ga opzoek naar een installatie bestand (.msi) voor firefox. Kijk hiervoor eens op de website van Frontmotion.
2. Zorg vanop de server voor een installatie van het programma firefox voor gans het domein.
3. Gebruik de optie published.
4. Het installatiepakket mag enkel in Programs and Features van het Control panel te zien zijn wanneer een instructeur zich aanmeldt op de client.
5. Controleer door een keer aan te melden.

5.3 Software restriction

Maak een hash rule zodat instructeurs firefox wel kunnen opstarten en cursisten niet.

6 COLOFON

Sectorverantwoordelijke:	
Cursusverantwoordelijke:	Jean Smits
Didactiek:	
Lay-out:	
Medewerkers:	Vakgroep systeembeheer
Versie:	Februari 2024
Nummer dotatielijst:	