5. Group Policy Objects (GPO)

Server OS

Group policy

= manier om bepaalde instellingen over netwerk te verspreiden.

= gecentraliseerd beheer.

- Ondersteuning vanaf Windows 2000.
- Bij elke nieuwe versie van een Windows OS, steeds meer instellingen mogelijk.
- Wanneer toegepast?
  - @logon/logoff time (user settings)
  - @startup/shutdown time (computer settings)
- Typisch 2 stappen in Group Policy implementatie
  - Aanmaken van de GPO (Group Policy Object), deze bevat instellingen
  - Linken van de GPO aan containers (bv. aan OU)

Wat kunnen we instellen via Group Policy?

- Registry-based policies
- Software Installation policies
- Folder redirection
- Offline file storage
- Scripts
- Windows Deployment Services (WDS)
- Edge settings / browser settings
- Security settings
- …

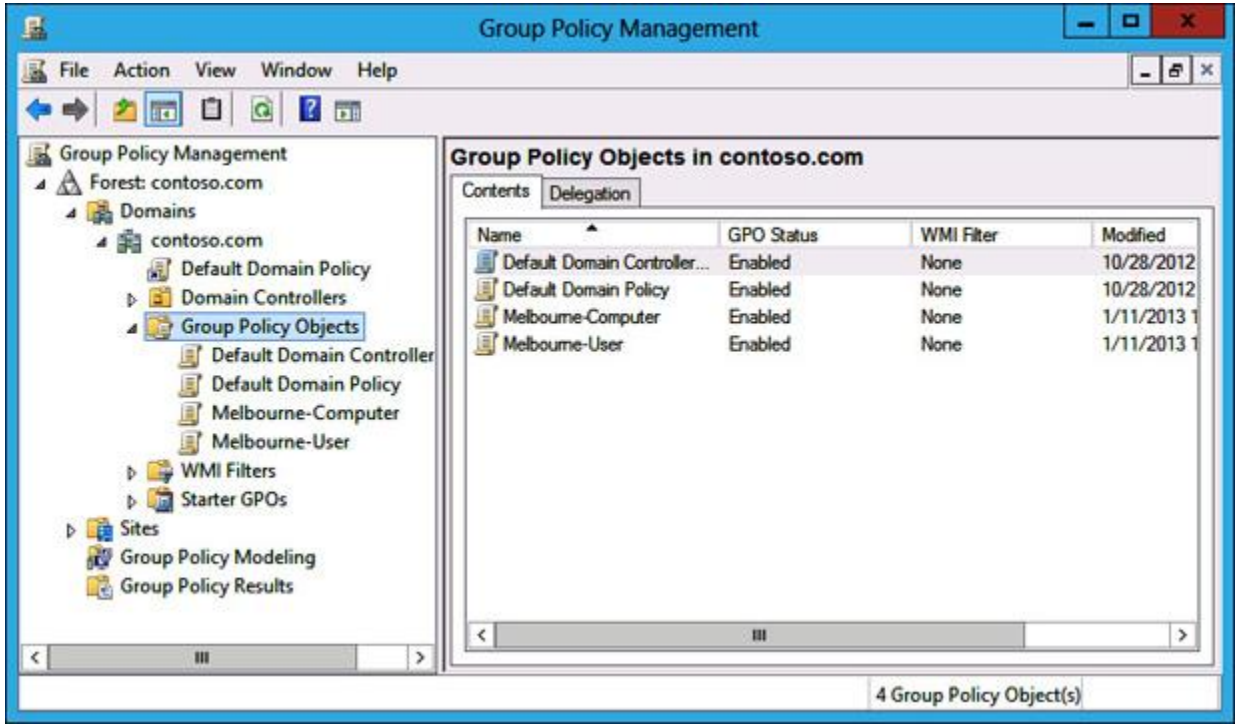
Gecentraliseerd beheer

2 belangrijke drijfveren

- ROI (Return On Investment)
  - Verhoogde productiviteit van gebruikers
  - Minder tijd steken in management van pc’s
  - Zo hoog mogelijk houden
- TCO (Total Cost of Ownership)
  - Bv. kost netwerk = kost aankoop + implementatie + upgrades + management + …
  - Zo laag mogelijk houden

Group policy management console

- Zit standaard in Windows 2008 server en hoger
- GPOs worden opgeslagen in Group Policy container
- GPOs worden nadien gelinkt aan OU, Site, Domein
- GPO-instellingen soms erg moeilijk te vinden
- Google
- Group policy xls-sheets van Microsoft (zie Canvas)

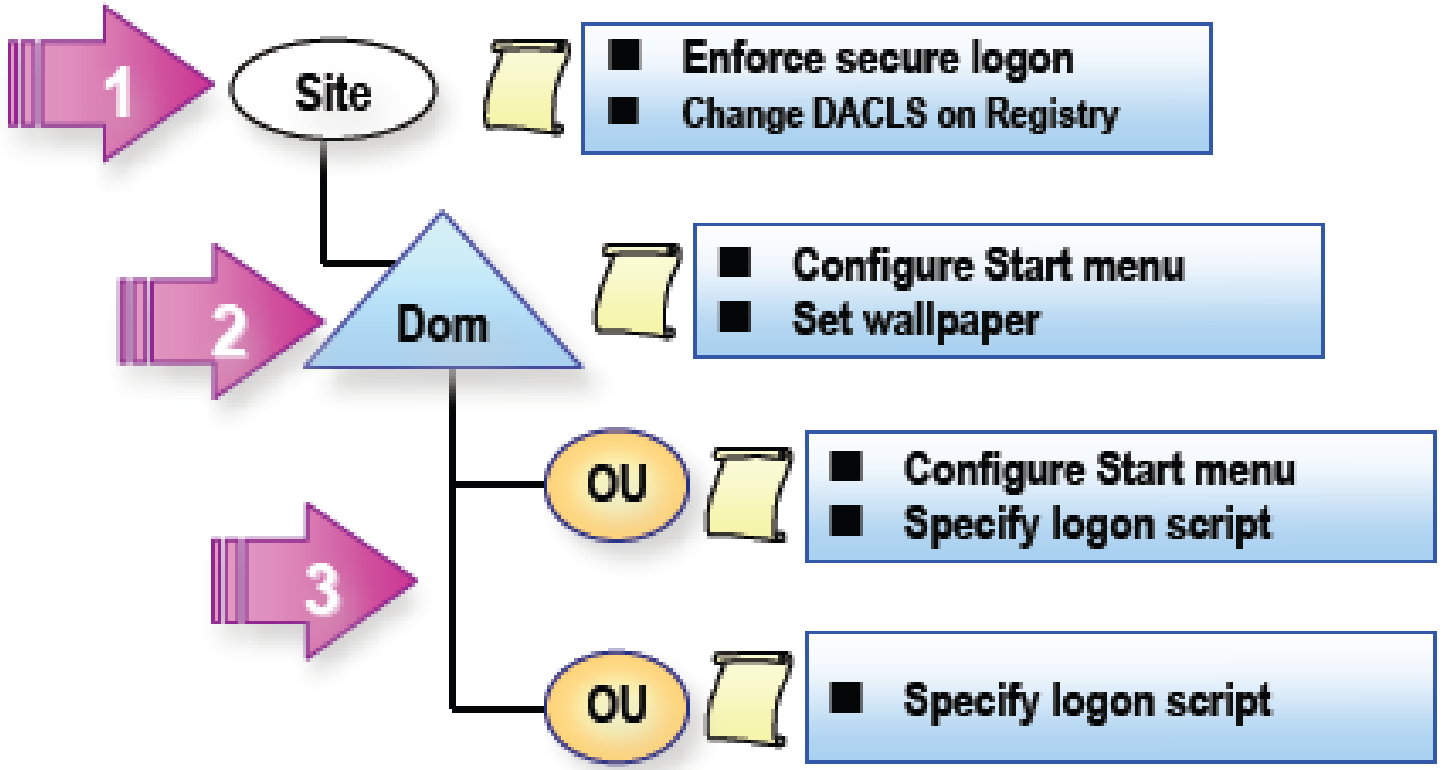


erasmus HOGESCHOOL BRUSSEL

Basisregels voor group policy

- GPO wordt steeds gelinkt aan site, domein of OU
- Instellingen hebben uitwerking op alle objecten onder deze container (en child containers)
- Volgorde van toepassing:
    1. Local group policy (gpedit.msc)
    2. Site level group policies
    3. Domain level group policies
    4. OU level group policies (hiërarchisch)
- Een GPO die later wordt toegepast, overschrijft de voorgaande

Basisregels voor group policy



Basisregels voor group policy

Processing?

1. Boot: secure link naar DC voor afhalen GPOs
2. Gedurende boot: computer configuration toepassen
3. Alles toegepast vóór logon screen
4. Startup scripts worden toegepast (timeout 10 minuten)
5. User krijgt logon scherm (Ctrl + Alt + Del)
6. User authenticeert
7. GPOs van user worden opgehaald en in volgorde toegepast.
8. Logon scripts worden toegepast

Basisregels voor group policy

Processing?

Na aanloggen

- Toepassen van group policies om de 90 + [0-30] min
- Op DC toepassen om de 5 minuten
- Forceren via gpupdate /force
- Al deze refresh tijden kunnen aangepast worden (via group policy ☺)

Basisregels voor group policy

- **Inheritance is de basisregel**
  - Maar uitzonderingen zijn mogelijk
- **Block inheritance**
  - Instelbaar op container-niveau (bv. OU).
  - Alle policies die normaal gezien worden overgeërfd, worden nu niet meer toegepast (maw. “hoger gelegen” group policies worden niet toegepast).
  - Niet selectief: ineens alle bovenliggende policies niet toepassen.
- **Enforced**
  - Instelbaar op een GPO (Group Policy Object).
  - “Deze instelling kan niet meer overschreven worden op lager niveau”.
  - Wint van een block policy inheritance op lager niveau!

Basisregels voor group policy

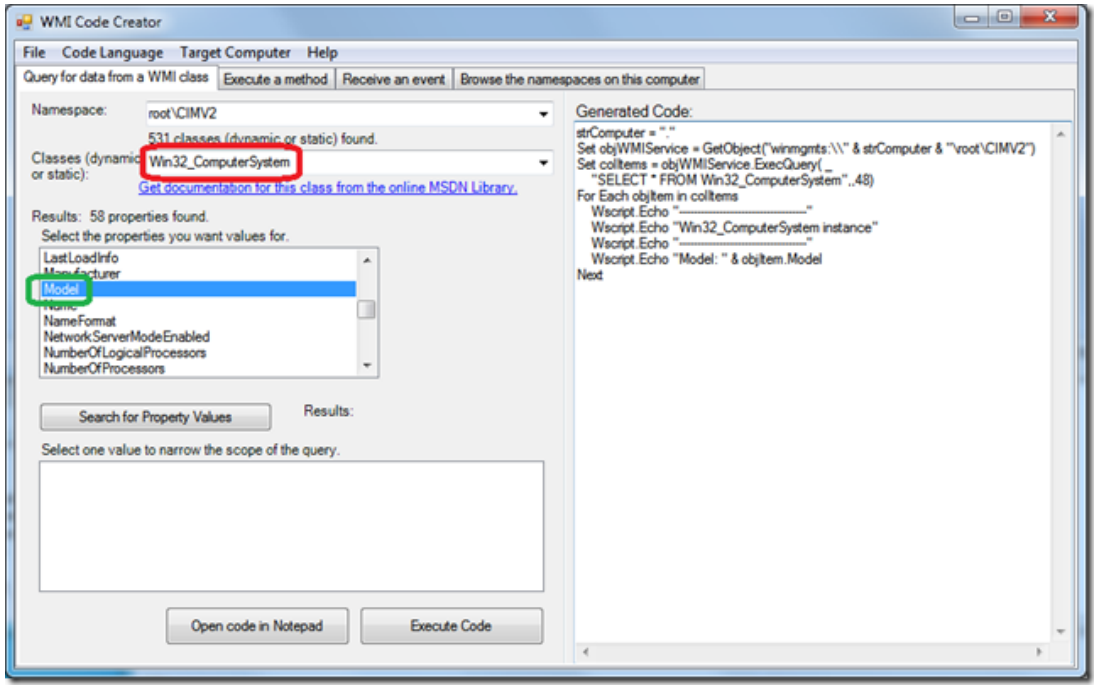
- Gebruik
  - Enforced (No override): policies die absoluut moeten worden toegepast en nooit overschreven mogen worden
    - Bv. antivirus-software installeren in heel het bedrijf
  - Block policy inheritance: OU's die eilandjes vormen
    - Bv. developers in een bedrijf: zij managen hun eigen pc
    - Bv. managers

Filtering op group membership

- Group policies worden default op alle users/computers van die container toegepast.
- Ook al staat filtering aan, nog steeds moet de user/computer in die container staan om de group policy toegepast te krijgen.
- Voorbeeld
  - Software voor alle managers over heel het domein
    - Zet policy op domein niveau, en filter op membership van managers group.
  - Administrators willen liefst niet alle domein policies toegepast krijgen
    - Deny zetten voor Domain Admins
    - Let op bij deny “Apply Group Policy”, best ook een deny “Read” want anders zal bij aanloggen toch telkens de group policy ingelezen worden en niet toegepast (☹ performantie).

WMI filters

- Specifiëren op welke computers een group policy moet toegepast worden
  - Bv. enkel computers met 2000 MB vrije schijfruimte
  - Bv. enkel computers met Windows 11
  - Bv. enkel computers met Intel Core i7 860
- Vrij complexe queries
  - Opstellen via WMI code creator en Technet documentatie



erasmus HOGESCHOOL BRUSSEL

Granular password policies

- In vorige versies hadden we slechts één paswoord en account lock-out policy voor het hele domein.
- Nu kunnen we verschillende fine-grained password policies aanmaken.
- Meer info:
  - https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/fine-grained-password-policies?tabs=adac

Group policy modeling vs. Group policy results

- Modeling
  - Simulatie: user X logt aan op computer Y
  - Welke policies zijn uiteindelijk van toepassing?
- Results
  - Effectief opvragen van toegepaste policies
  - User moet hiervoor eerst hebben aangelogd op bepaalde PC
  - Nodig: RPC service die op client toegankelijk is
    - Firewall!
    - Regelen via Policy! [Computer/Administrative Templates/Network/Network Connections/Windows Firewall/Domain Profile/Windows Firewall: Allow remote administration exception]

GPResult

- Command-line tool
- Bekijken van
  - Wanneer laatste keer toegepast?
  - Lijst van alle applied GPOs
  - Applied registry settings
  - Redirected Folders
  - Assigned/published applications
  - Disk quota
  - IP Security settings
  - Scripts
- Voorbeeld
  - Gpresult /user bram/v

Software deployment

Automatische…

- Installatie
- Upgrading
- Patching
- Repair
- Removal

…van software via group policy deployment

Software deployment

Gebaseerd op **Windows Installer technologie**

- Software-installation packages
  - **.msi** bestanden
  - Bevat informatie voor installatie/verwijderen van software
  - Voordeel
    - Self-healing software, mooie uninstall
- Windows installer service
  - Beheert de installatie van software op een pc
  - Gebruikt msi.dll om de msi-files te lezen
  - Kopiëren van juiste bestanden, zetten van registry keys, eventuele andere taken…

Software deployment

Maken van msi bestanden

- Dikwijls levert de fabrikant van de software de msi
  - “Native Windows Installer file”
- Indien niet geleverd: zelf msi aanmaken

1. Vertrekken vanuit “clean” installatie van target OS
2. 3rd party tool voor snapshot van OS vóór installatie
3. Installeren van software
4. Customizen van applicatie waar nodig
5. 3rd party tool voor snapshot van OS nà installatie
6. Hieruit wordt het msi bestand gegenereerd

Software deployment

Stappen voor deployment via Group Policy

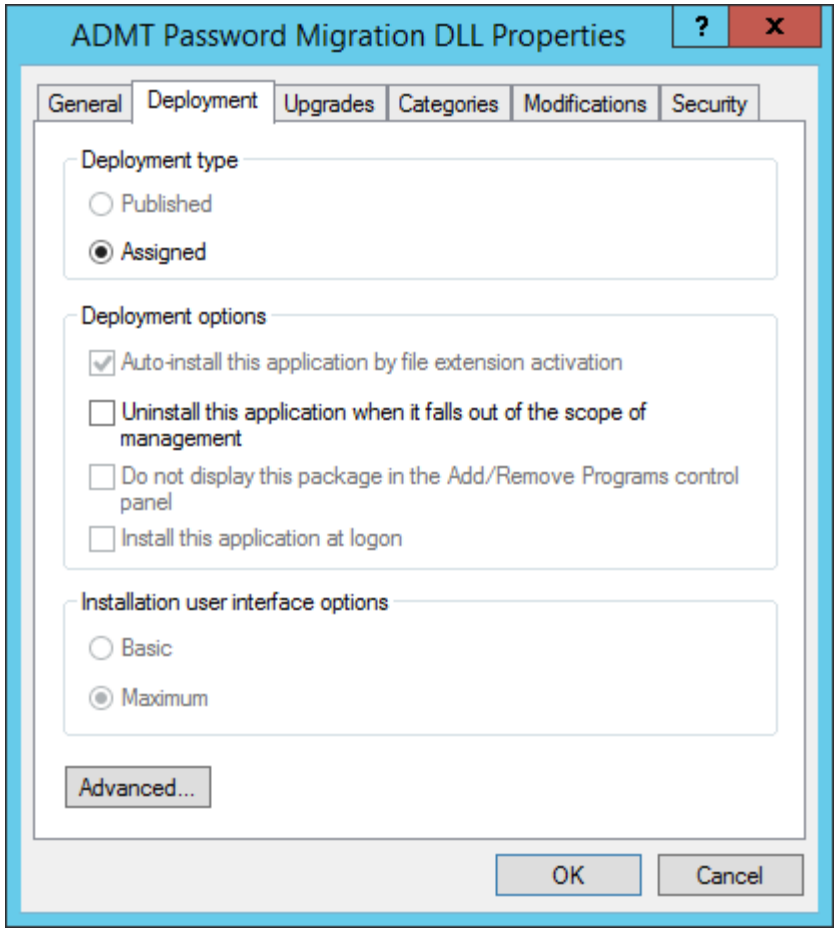
1. Aanmaken van distribution share
   - Gebruikers en computers moeten Read-rechten krijgen op NTFS niveau
   - Best subfolder maken voor elke applicatie
2. Aanmaken/wijzigen van GP
   - **Publish**: publiceer de applicatie in gedeelte software van Control Panel
   - **Assigned**: zet opstarticoon in Start menu

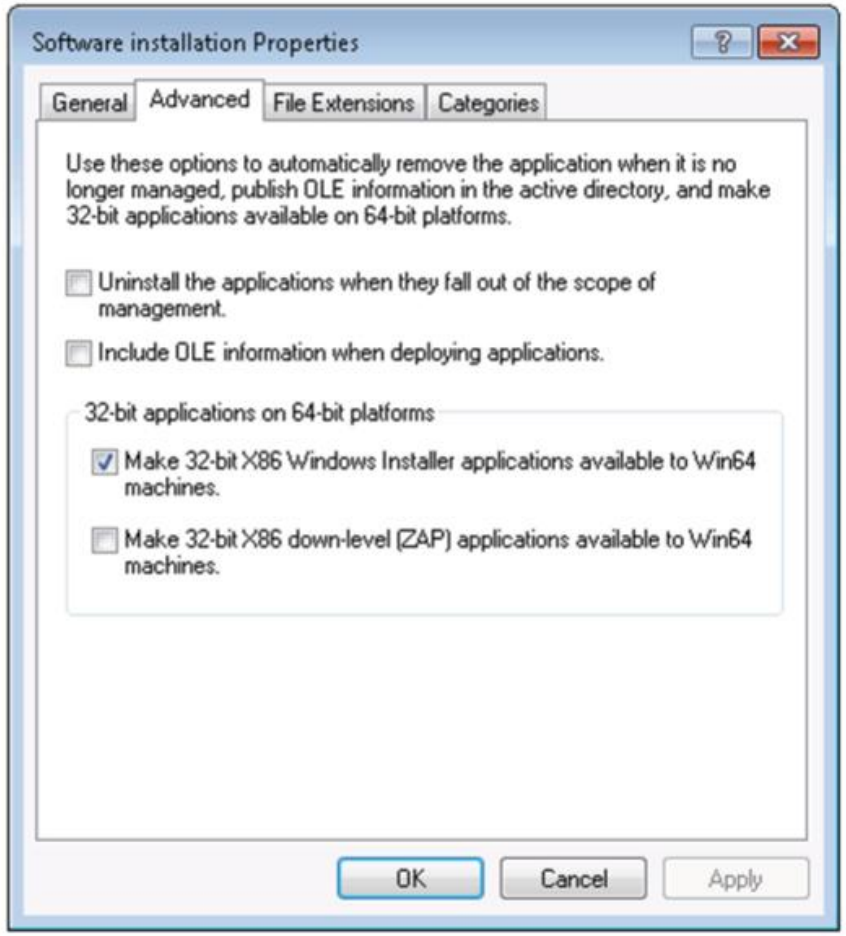
Software deployment

Stappen voor deployment via Group Policy

1. Aanmaken van distribution share
   - Gebruikers en computers moeten Read-rechten krijgen op NTFS niveau
   - Best subfolder maken voor elke applicatie
2. Aanmaken/wijzigen van GP
   - **Publish**: publiceer de applicatie in gedeelte software van Control Panel
   - **Assigned**: zet opstarticoon in Start menu

Software deployment





erasmus HOGESCHOOL BRUSSEL

Group policy design

- Theoretisch gezien
  - Alle instellingen kunnen in 1 GPO
  - Snelste bij logon
- Praktisch gezien
  - Best instellingen verspreiden over meerdere GPOs
  - Iets trager, maar overzichtelijker voor admins
  - Maakt hergebruik van GPOs mogelijk (over meerdere OU’s bijvoorbeeld)
- Best practice
  - Zo weinig mogelijk enforced, block policy, filtering, …
  - (keep it simple)