

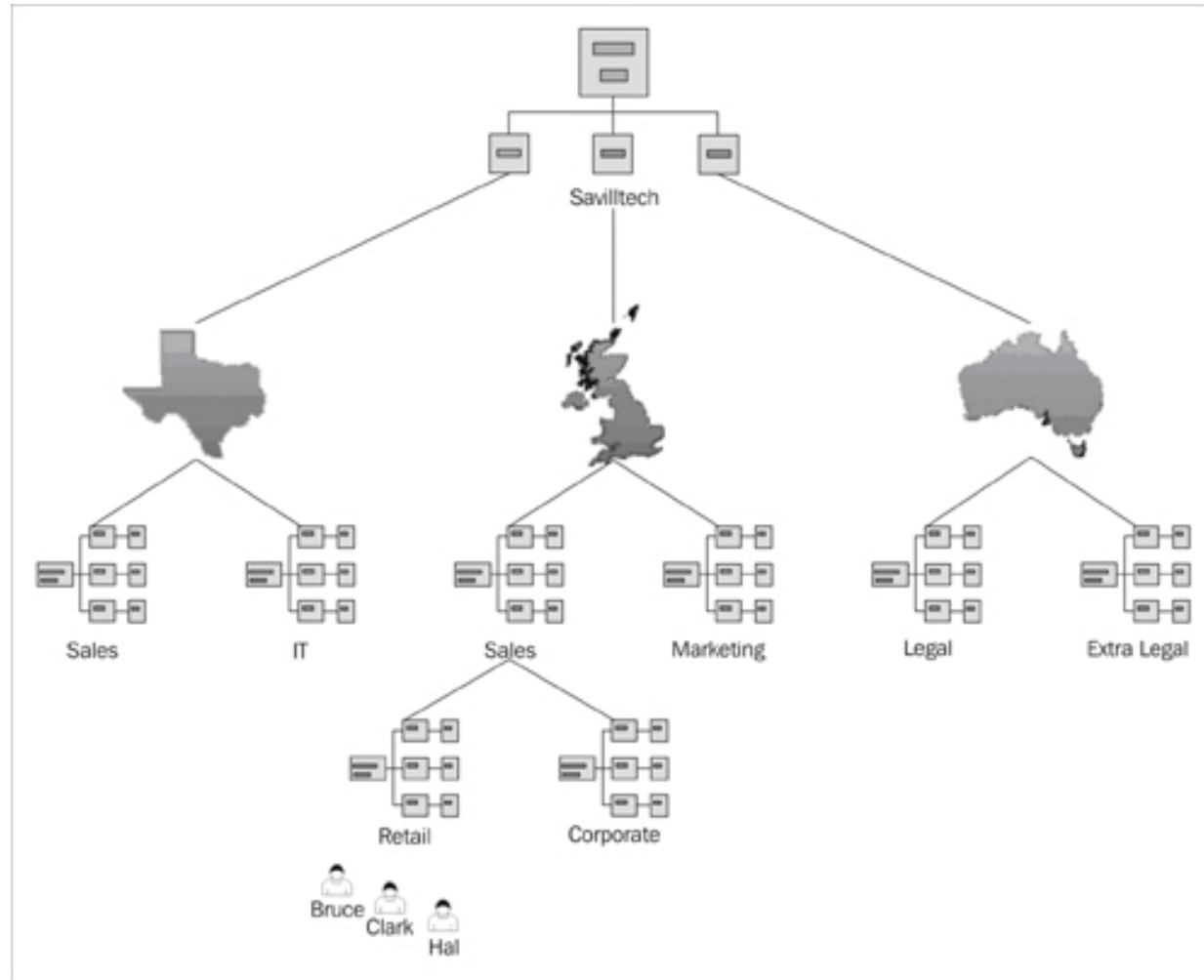
# 4. Active Directory (AD) beheer

Server OS

# Organizational Units

- Zelfs in single domein omgeving kunnen miljoenen objecten zitten
  - Organisatie wordt moeilijk ☹️
  - Oplossing: OU's 😊
- OU's zijn containers (~ directories in verkenner)
- 2 belangrijke functies
  - Delegeren van administratieve rechten (niveau 1)
  - Groeperen van objecten (niveau 2)
    - Group policies (zie later)
    - Objecten die samen horen qua departement/functie

# Organizational Units



# Organizational Units

- Mogelijke invalshoeken:
  - Functie
    - Enkel in kleinere bedrijven (moeilijk te groeperen in grote)
  - Organisatie
    - Dikwijls moeilijk met oog op delegatie
  - Locatie
    - Interessant bij gedecentraliseerd beheer
  - Hybride

# User Accounts

- Wordt gebruikt om gebruiker te authenticeren
- Belangrijkste object in Active Directory
- Eigenschappen
  - Naam, familienaam, logon name, wachtwoord instellingen
  - ...
- Veel gebruikers aanmaken?
  - Gebruik maken van scripts met csv-bestanden (via powershell)

# User Accounts

- Gebruiker kopiëren
  - Enkele template accounts maken met default instellingen
  - Tijdsbesparend
  - Wat wordt er gekopieerd?

Tabblad	Kopiëren?
Address	Alles, behalve street address
Account	Alles, behalve Logon Name
Profile	Alles, behalve Profile Path en Home Folder (automatisch aangepast)
Organization	Alles, behalve Title
Member Of	Alles

# Computer Accounts

- Voor elke computer in het domein is er een account
- 2 opties
  - Bij toevoegen nieuwe computer (join)
    - Computer account komt onder “Computers” container
    - Achteraf account verplaatsen naar juiste OU
  - Pre-staging: op voorhand computer account aanmaken
    - Computer komt onmiddellijk in juiste OU

# Groepen

- Gebruikers tegelijk bepaalde rechten geven
- Administratieve hulp 😊
- Access token
  - Wordt aangemaakt bij aanloggen gebruiker
  - = soort lidkaart
  - Let op
    - Wijziging in lidmaatschap is pas merkbaar na opnieuw aanloggen!





# Groepen

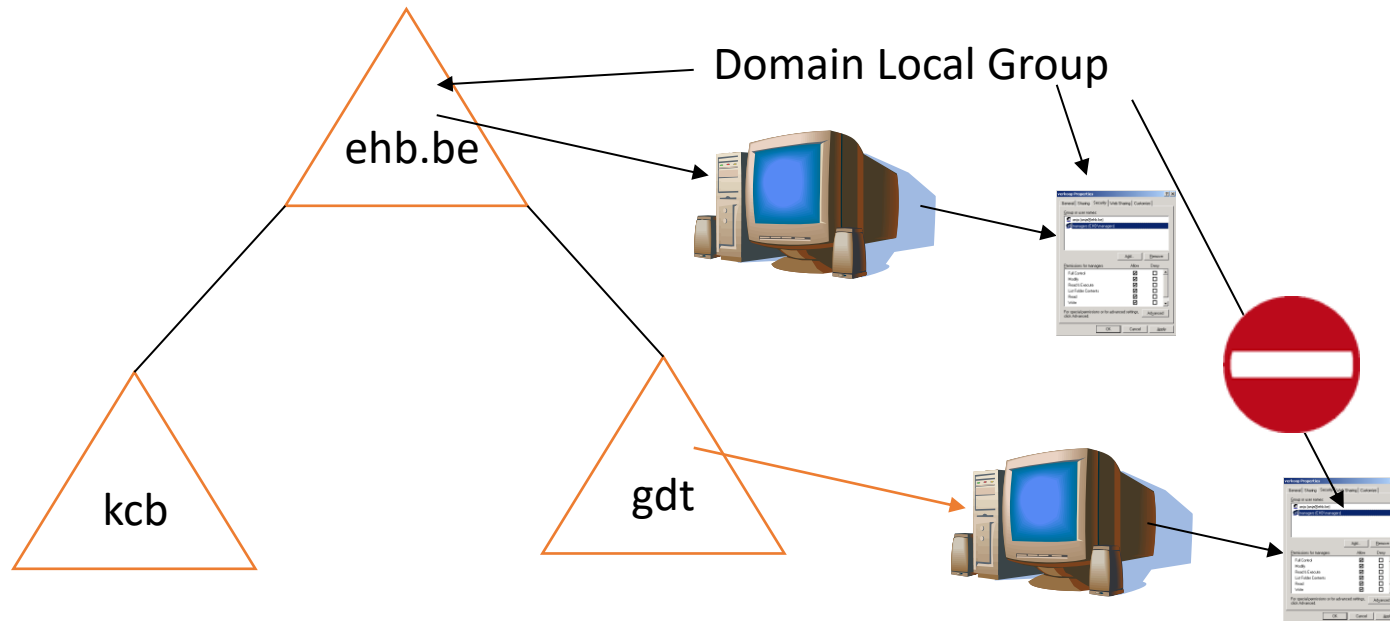
- Groep type
  - Distribution
  - Security
- Groep scope
  - Domain Local
  - Global
  - Universal

# Groepen

- Domain Local Group
  - Kan leden van heel het forest bevatten
  - Kan enkel op ACLs van het eigen domein gezet worden
- Global Group
  - Kan enkel leden van eigen domein bevatten
  - ~~• Kan op ACLs van hele forest gezet worden~~
- Universal Group
  - Kan leden van heel het forest bevatten
  - Kan op ACLs van heel het forest gezet worden
  - => enkel gebruiken voor het bundelen van Global Groups uit verschillende domeinen

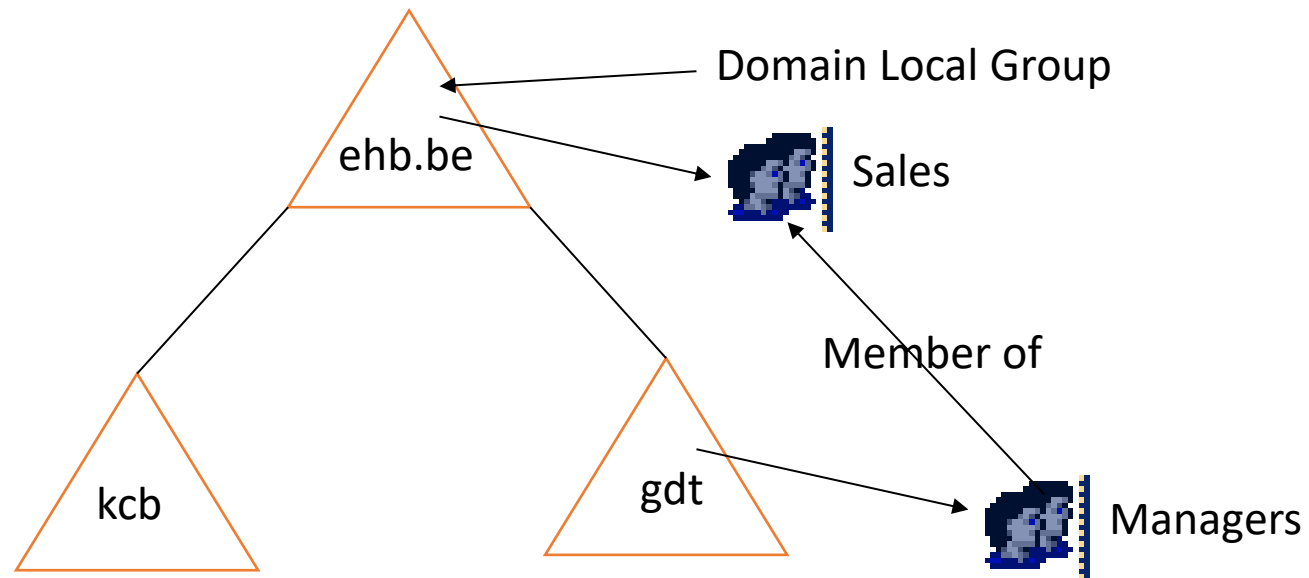
# Groepen

- Domain Local Groups
  - Enkel op ACL van eigen domein



# Groepen

- Domain Local Groups
  - Leden van hele forest



# Groepen

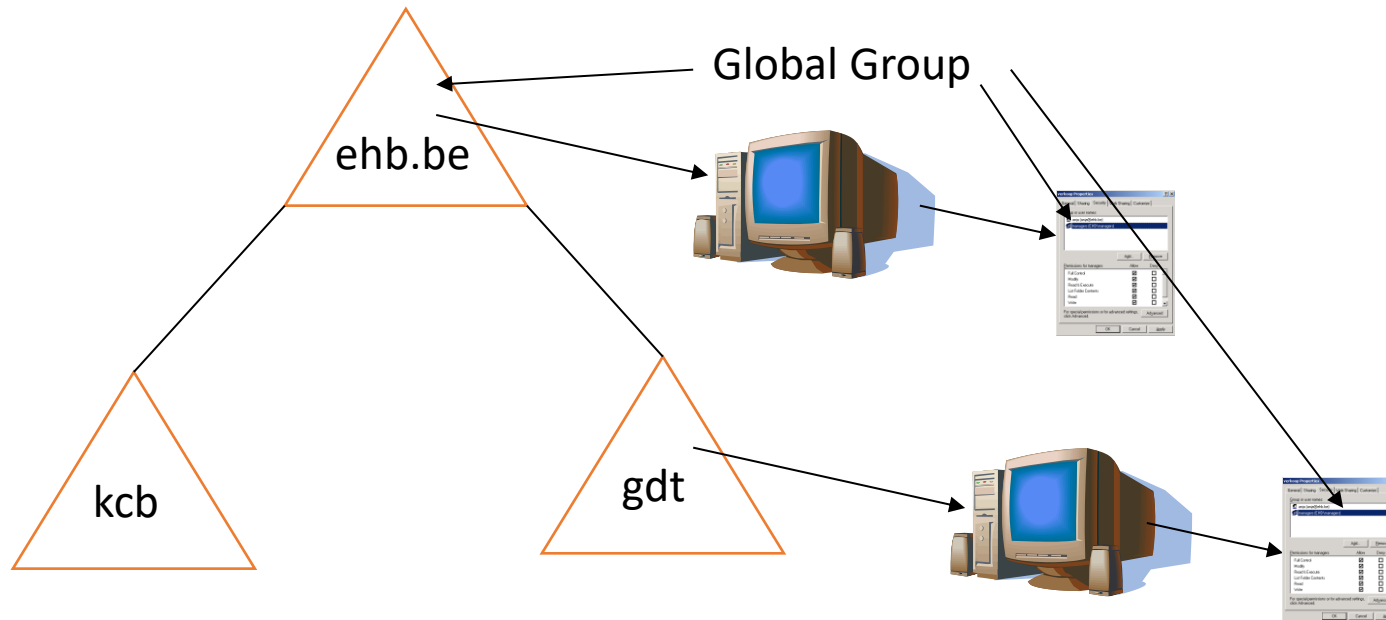
- Domain Local Groups

- Idee

- Group die een admin van een ander domein niet kan gebruiken (niet toevoegen aan ACL).
    - Members van andere domeinen kunnen toegevoegd worden indien gewenst.

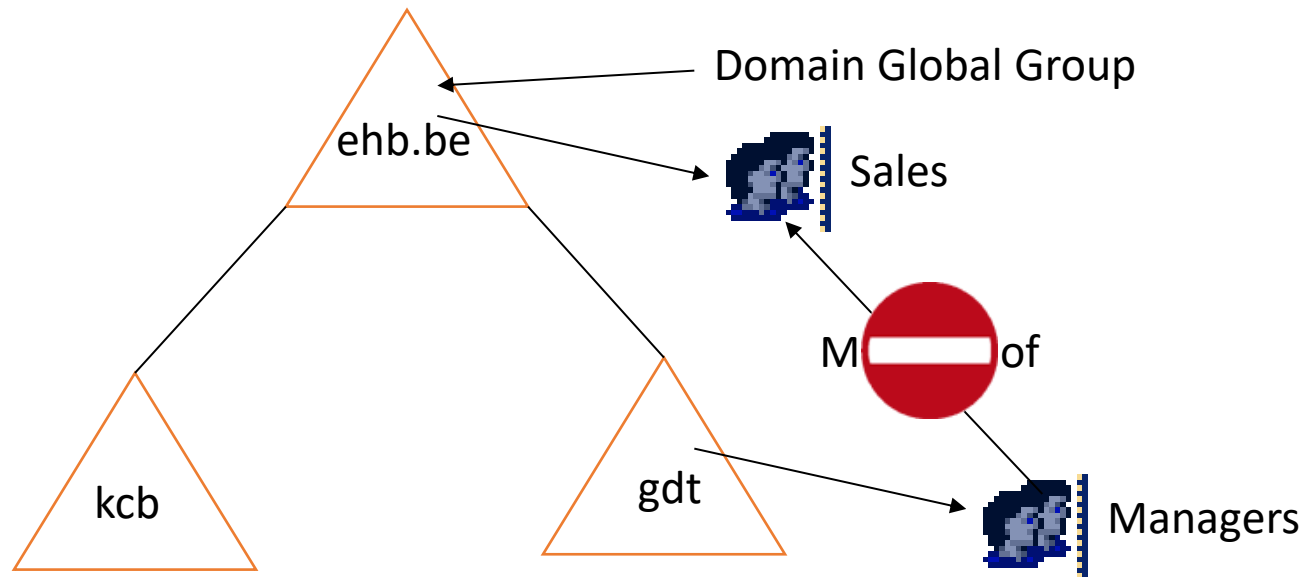
# Groepen

- Global Groups
  - Op ACL van hele forest



# Groepen

- Global Groups
  - Leden van eigen domein



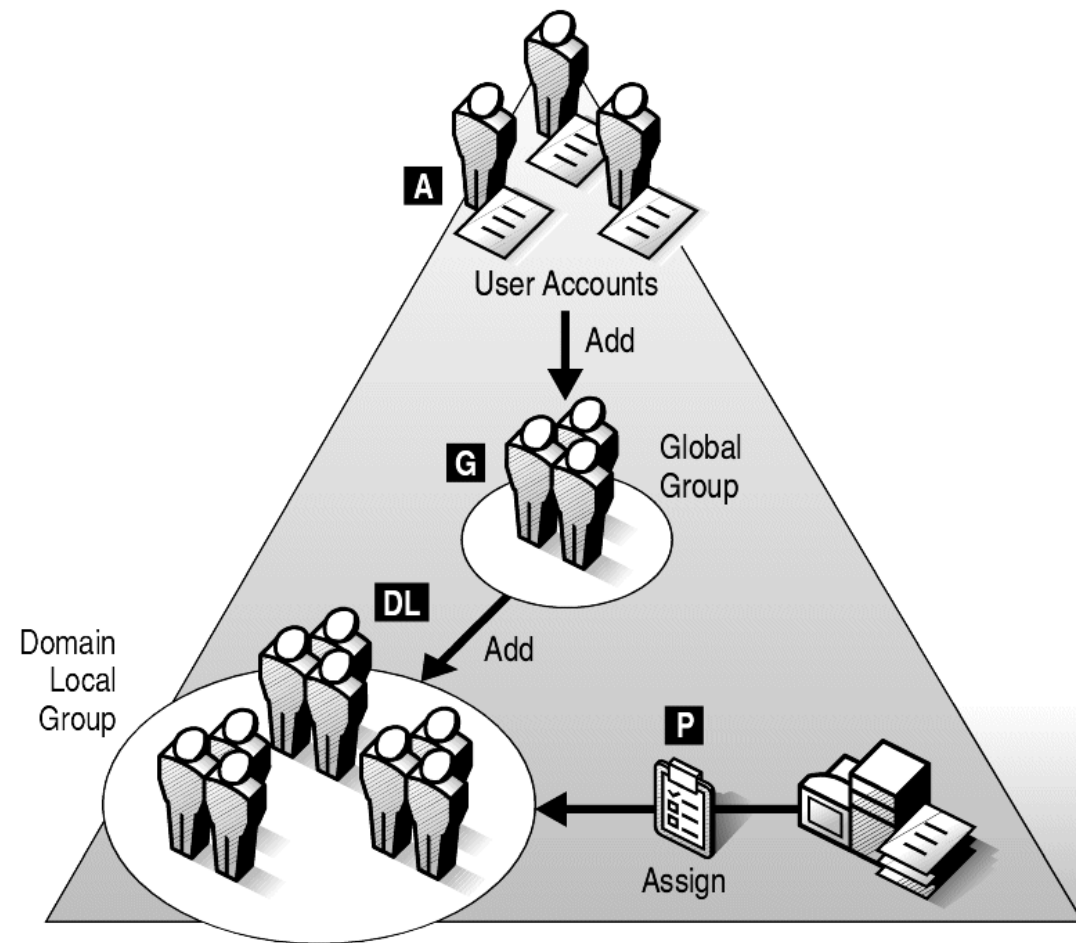
# Groepen

- Global Groups
  - Idee
    - Delegeren van permissies, zonder dat een externe admin iemand lid kan maken van deze group
    - Een group aanmaken die iedereen in het forest kan gebruiken
- Universal groups
  - Nadeel: Global Catalog meer belasten



# Groepen

- Microsoft: AGDLP
  - Accounts in Global Groups
    - Global Groups op basis van functie/job
  - Global Groups in Domain Local groups
    - Domain Local groups op basis van rechten tot map/ad object/printer/...
  - Domain Local Group permissies geven



# Groepen

- Microsoft: **AGGDL**P
  - Accounts in Global Groups
    - Global Groups op basis van functie/job
  - Global group in Global Group (indien aggregatie mogelijk)
  - Global in Domain Local groups
    - Domain Local groups op basis van rechten tot map/ad object/printer/...
  - Domain Local Group permissies geven

# Groepen

- Microsoft: **AGUDLP**
  - Accounts in Global Groups
    - Global Groups op basis van functie/job
  - Global group uit verschillende domeinen in Universal Group
  - Universal Group in Domain Local groups
    - Domain Local groups op basis van rechten tot map/ad object/printer/...
  - Domain Local Group permissies geven
- Bv.: managers van alle domeinen
  - GG managers per domein
  - UG waarin al deze GG staan
  - UG in DLG waaraan rechten wordt toegekend

# Active Directory permissies

- Elk object in AD heeft een security descriptor
  - Bepalen van toegangsrechten tot dit object
- Mogelijkheid tot groepen van objecten in OU's
  - Gebruikers rechten geven op zo'n hele OU structuur
- Elk object heeft een security-tabblad
  - Zichtbaar via View-Advanced
- Cumulatieve permissies
  - Alle rechten van de groepen waarvan je lid bent, worden opgeteld

# Active Directory permissies

- Allow
  - Toelaten van bepaald recht
- Deny
  - Weigeren van bepaald recht
  - Deny heeft altijd voorrang op allow!
  - Deny zo weinig mogelijk gebruiken!

# Active Directory permissies

- Object permissies

Object permissie	Rechten
Full Control	Permissies wijzigen, take ownership + onderstaande
Read	Attributen lezen, eigenaar en rechten bekijken
Write	Attributen veranderen
Create All Child Objects	Elk type object toevoegen aan een OU
Delete All Child Objects	Eender welk object verwijderen in een OU

# Active Directory permissies

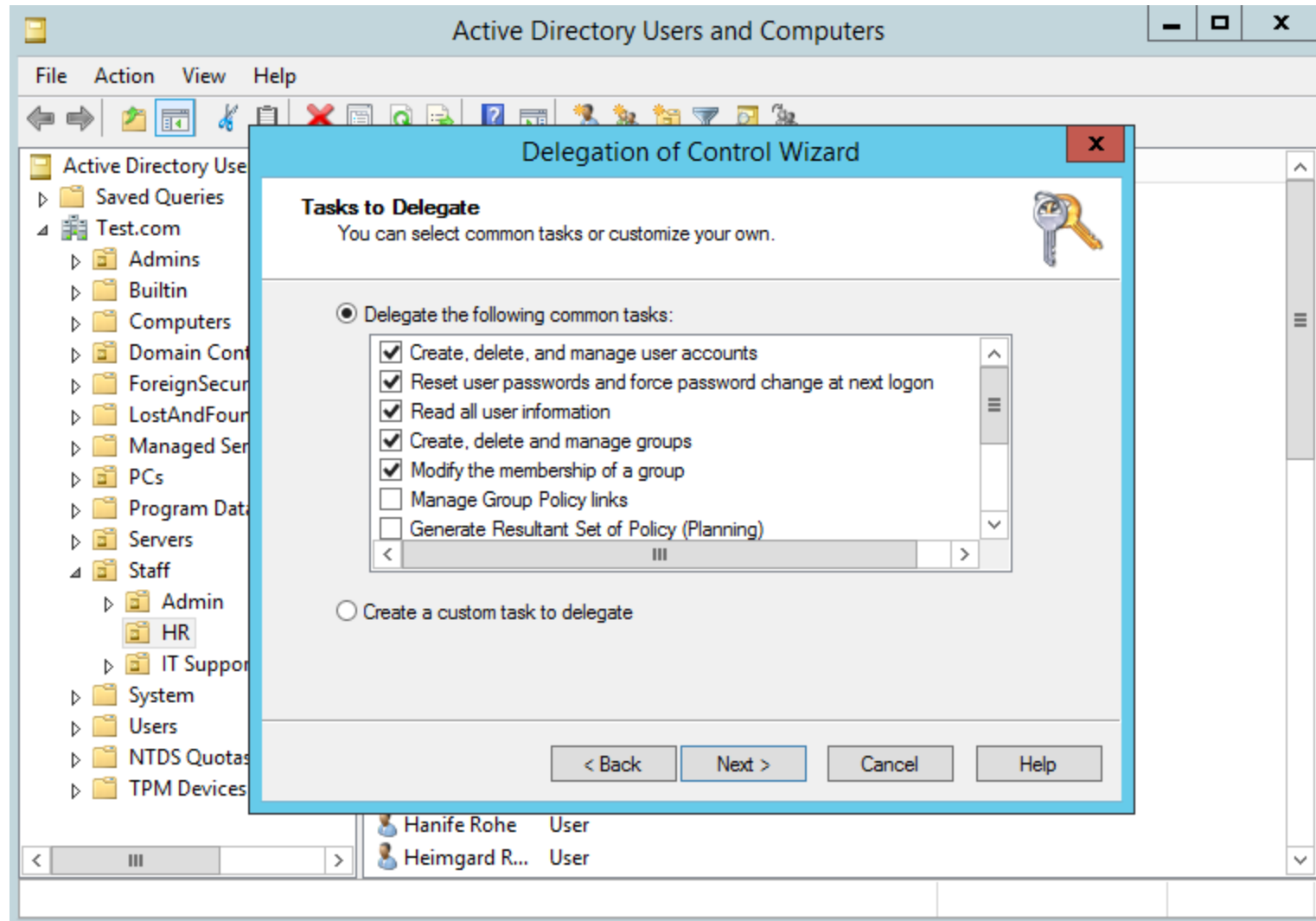
- Overerving van rechten
  - Standaard zullen child objecten de rechten van hun parent overerven
  - Dit is van toepassing in uiteenlopende situaties:
    - Mappen in Windows Explorer
    - Objecten in OU's in Active Directory
    - ...

# Administratieve controle delegeren

- In theorie
  - Eender welke toekenning van rechten is mogelijk
  - Is meestal té gedetailleerd
- In praktijk
  - Full control over 1 OU
  - Full control over specifieke objecten in een OU
    - Bv. enkel user objecten in een OU managen
  - Full control over specifieke objecten in een domein
  - Rechten voor bepaalde properties van objecten
  - Bv. HR mag personal information van users aanpassen

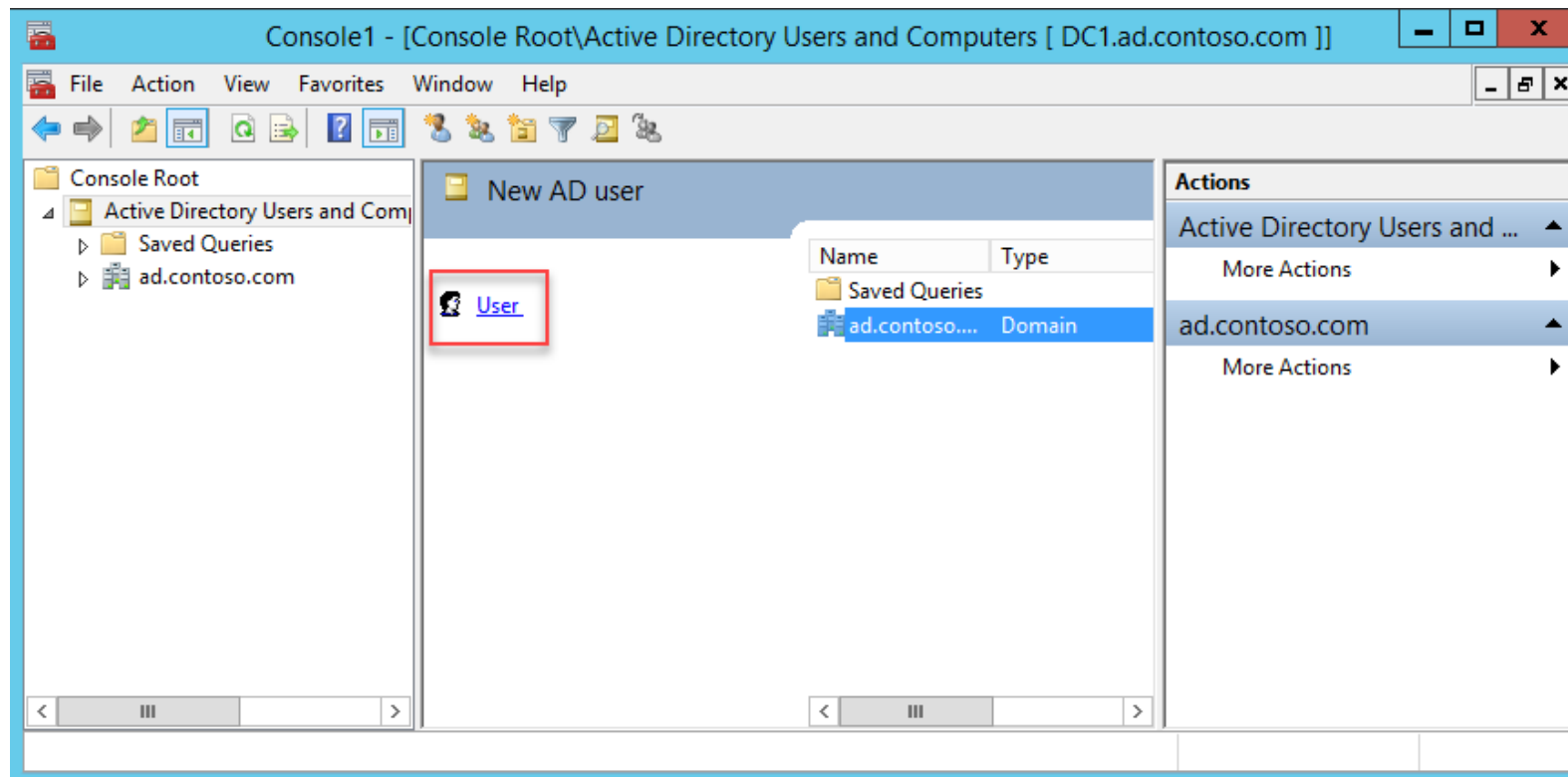


# Administratieve controle delegeren



# Administratieve controle delegeren

- Mogelijkheid tot maken van Custom MMC of Taskpad



# Administratieve controle delegeren

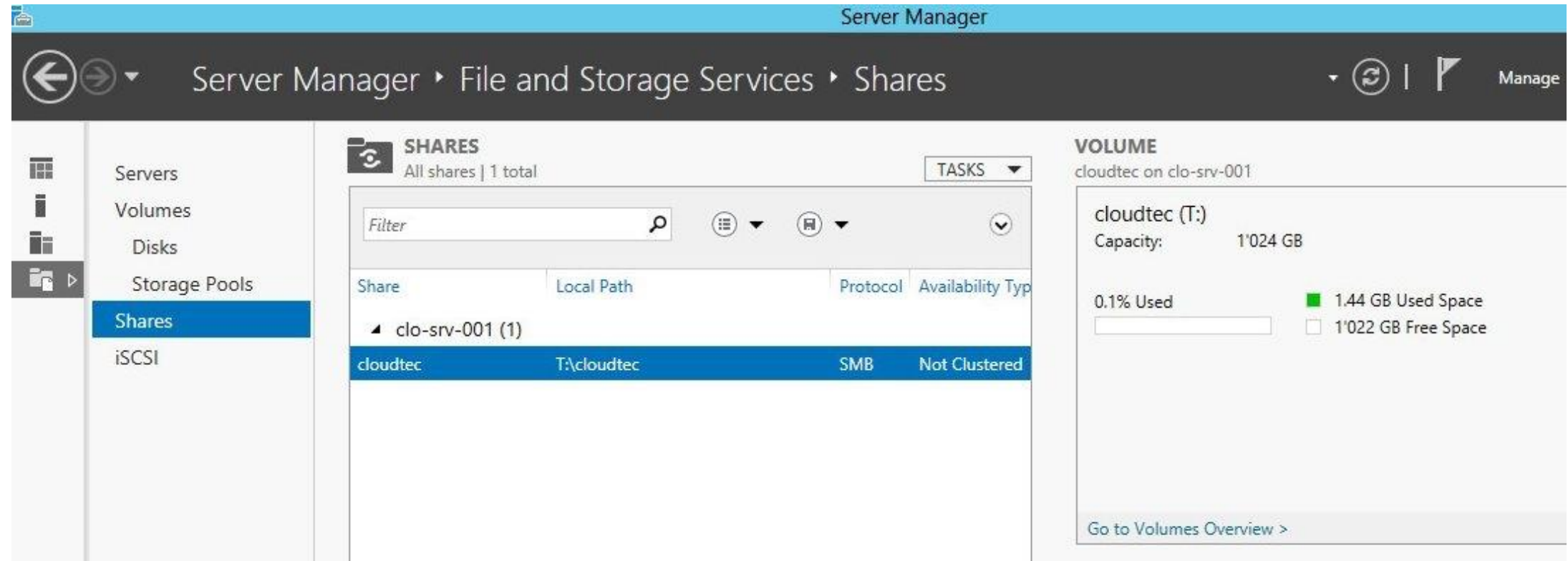
- Instelling voor groepen: “managed by”
  - Enkel informatief, geef op zich geen rechten
  - Optie “Manager can update membership list”

# File Sharing

# File Sharing

- = nog steeds een van de belangrijkste functionaliteiten in een Windows domein.
- Installatie op Domain Controller of Member Server

# File and Storage Services > Shares



Server Manager

Server Manager > File and Storage Services > Shares

**SHARES**  
All shares | 1 total

Filter

Share	Local Path	Protocol	Availability Type
▲ clo-srv-001 (1)			
cloudtec	T:\cloudtec	SMB	Not Clustered

**VOLUME**  
cloudtec on clo-srv-001

cloudtec (T:)  
Capacity: 1'024 GB

0.1% Used

1.44 GB Used Space  
1'022 GB Free Space

[Go to Volumes Overview >](#)

# Shares creëren

- Openen van bestand via console (logon)
  - Enkel NTFS-rechten spelen mee (Security tabblad)
- Openen van bestand via share
  - Zowel NTFS-rechten als Share-rechten (Share tabblad) spelen mee

# Shares creëren

- Verborgen share
  - Eindigen met \$
- Speciale shares
  - ADMIN\$: Pad naar systemroot
  - NETLOGON: logon scripts voor pre-win2K clients
  - SYSVOL: informatie over policies
  - PRINT\$: remote administratie van printers

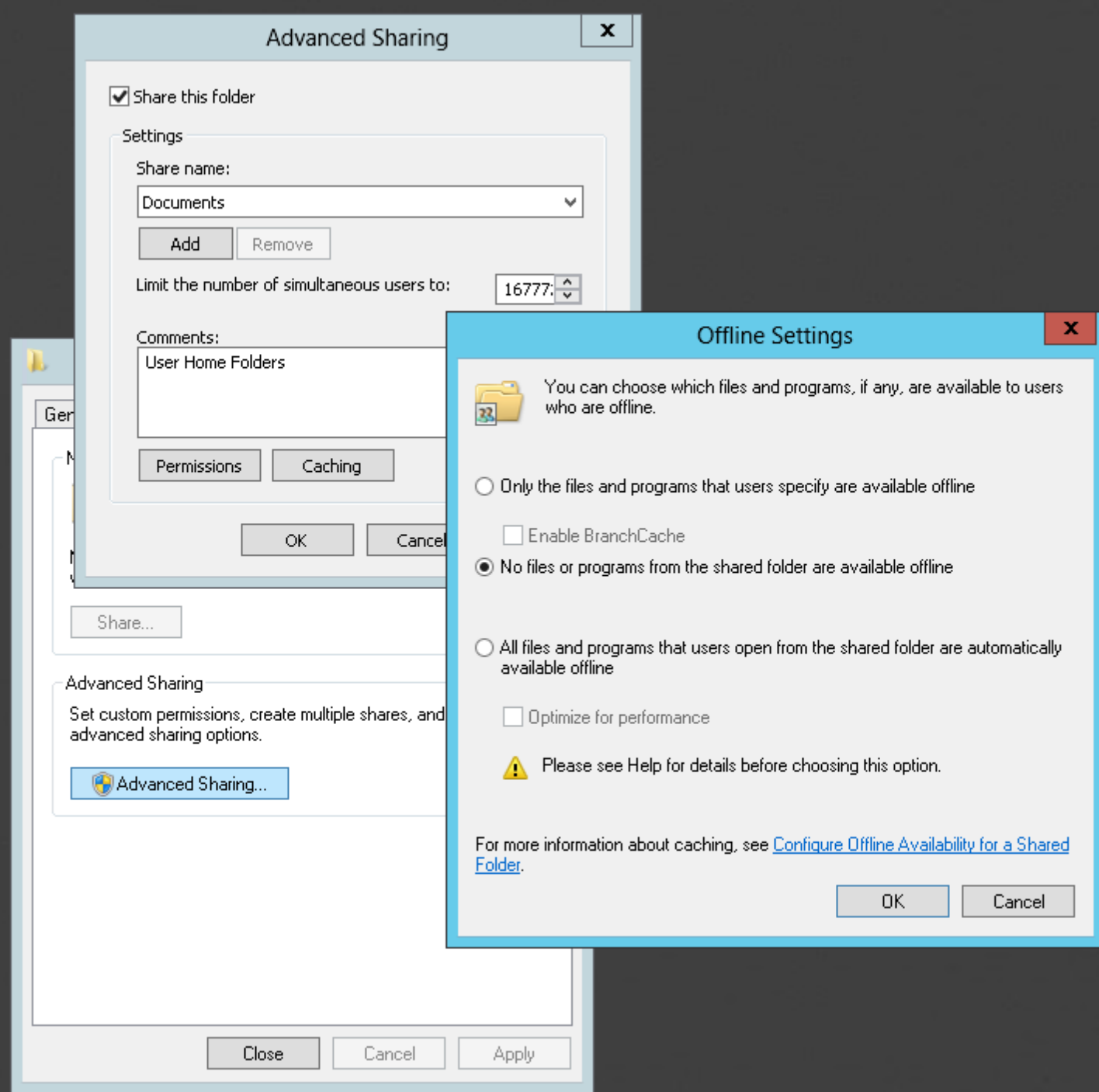


# Disk quota

- Maximale toegewezen opslagcapaciteit op harde schijf
- 2 mogelijkheden
  - Per volume: op user basis quota instellen (op volume)
  - Per map: maximumgrootte voor deze map (niet per gebruiker)
- “Add feature”
  - Remote Server Administration Tools
- “Add role service”
  - File service resource manager

# Offline files

- Bestanden beschikbaar, ook wanneer er geen netwerkverbinding is



# Share- en NTFS-permissies

- Cumulatieve permissies
  - Bij aanloggen van gebruiker wordt nagegaan (recursief) van welke groepen hij/zij lid is
  - Alle allow rechten van de groepen waarvan gebruiker lid is worden opgeteld
  - Alle deny rechten van de groepen waarvan gebruiker lid is ook.
  - Uiteindelijke rechten = ALLOW - DENY

# Share- en NTFS-permissies

- Share-permissies
  - Full Control
  - Change
  - Read
- NTFS-permissies
  - Full Control (FC)
  - Modify (W)
  - Read&Execute (R)
  - List Folder Contents
  - Read
  - Write