

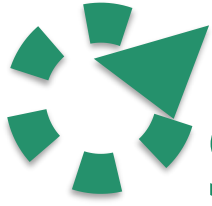
# Server Administration

## Directory Systemen - OpenLDAP



# Schema en DIT

- **Schema**
  - Definieert de mogelijke inhoud van de Directory Information Tree
    - Alle object klassen
    - Alle mogelijke attributen die objecten kunnen en/of moeten bevatten
  - Definieert de structuur van de Directory Information Tree
- **DIT - Directory Information Tree**
  - De inhoud van de Directory met zijn boomstructuur



# Schema elementen en termen

- **Attribuut:** Soort gegeven gebruikt om objecten te beschrijven  
Voorbeelden: Uid, Given-Name, User-Password, Printer-Name
- **Klasse:** Definieert een soort object en zijn attributen
- **Object:** Een data item in de Directory Service met een unieke Object Identifier (OID) – een instantie van een object



# Active Directory klassen/objecten

Bepaalde klassen/objecten in Active Directory liggen voor de hand:

- Gebruikers
- Computers
- Groepen

Andere niet:

- Organisational Units (OU's)
- Sites
- Shares
- Klasse definities
- Attribuut definities
- ...

# ACTIVE DIRECTORY – FYSISCH OPBOUW

# Fysische opbouw

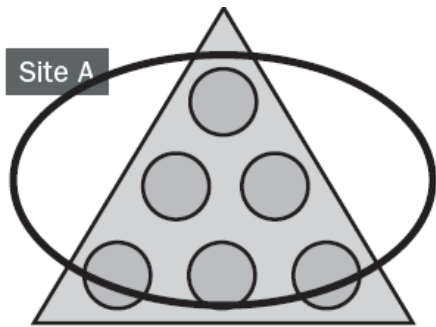
- De AD servers staan ook in een netwerk (met beperkingen)
- 2 fysische delen:
  - Sites
  - Subnets
- Gebruikt om replicatie te beheersen
- Gebruikt om frequentie en tijd van replicaties te beheren

# Sites

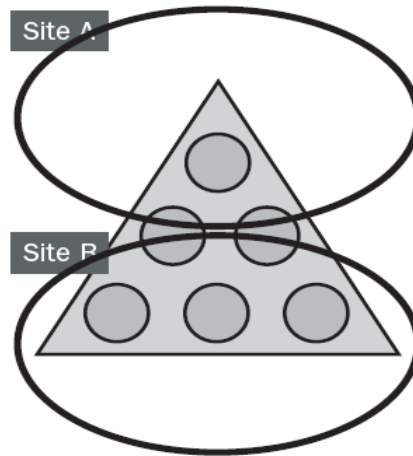
- **verschillende geografische locaties** verbonden door WAN-links noemen we “sites”
- Fysische opsplitsingen binnen een site door verschillende IP-subnets te gebruiken (ook tussen sites onderling)
- Op sites ook Grouppolicies mogelijk  
bv eenzelfde instelling voor één locatie, onafhankelijk van de bovenliggende (logische) Active Directory-structuur

# Sites

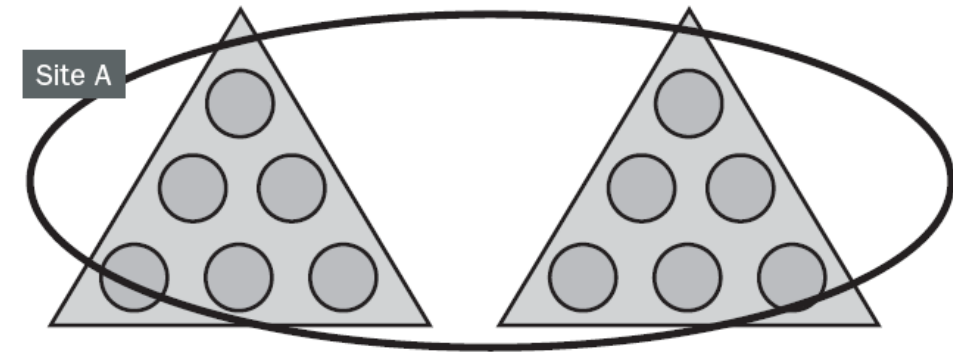
Een enkel domein op één site



Een enkel domein op meerdere sites



Meerdere domeinen op één site



En uiteraard zijn er ook ingewikkeldere combinaties mogelijk



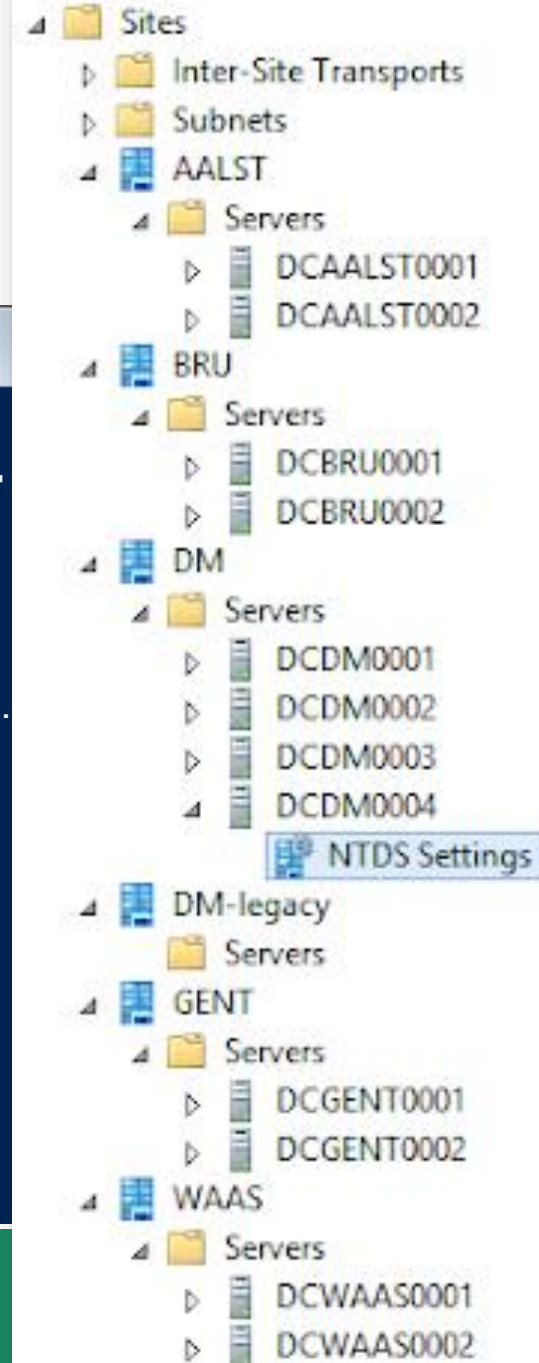
# hubkaho.be

Windows PowerShell

```
PS C:\> [System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest().Sites
```

```
Name                : GENT
Domains              : {}
Subnets             : {10.129.0.0/16, 10.130.0.0/16, 10.132.0.0/16, 10.138.128.0/18...}
Servers              : {DCGENT0001.hubkaho.be, DCGENT0002.hubkaho.be}
AdjacentSites        : {}
SiteLinks            : {DEFAULTIPSITELINK}
InterSiteTopologyGenerator : 
Options              : None
Location             : 
BridgeheadServers    : {DCGENT0001.hubkaho.be, DCGENT0002.hubkaho.be}
PreferredSntpBridgeheadServers : {}
PreferredRpcBridgeheadServers : {}
IntraSiteReplicationSchedule : 
System.DirectoryServices.ActiveDirectory.ActiveDirectorySchedule
```

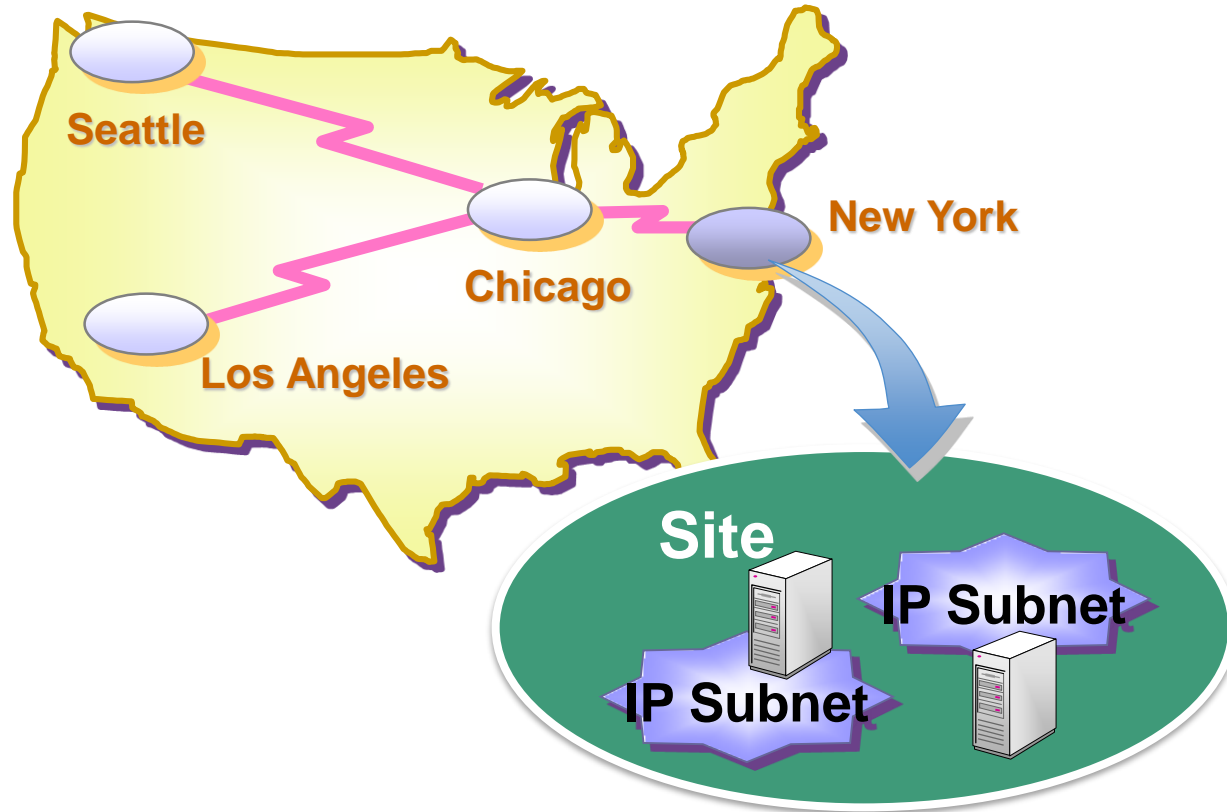
Active Directory Sites and Services [DCDM0002.hubkaho.be]



# Bandbreedte

- Verschillende factoren bepalen de nodige bandbreedte tussen de sites
  - Bv een organisatie met 1 miljoen objecten en een streng wachtwoordbeleid en hoge werknemersverplaatsing zal niet voldoende hebben aan een 10Mbps-lijn
  - Een organisatie met enkele 100 objecten en weinig veranderingen zal voldoende hebben aan een 128kbps ISDN-lijn
- We beschouwen alle verbindingen van 512kbps en lager als trage links. In dat geval gaan we zeker sites opzetten om replicatie te beheersen
- Sites aanmaken is niet moeilijk, denkwerk werd vooraf tijdens de ontwerpfase van het netwerk gemaakt (*zie cursus Introduction to Data networks, Routing and switching essentials*)

# Subnets



Binnen 1 site kunnen natuurlijk nog altijd verschillende ip-subnets gebruikt worden

# AD gegevens replicatie

**Replicatie** = proces dat informatie automatisch “kopieert” van een systeem naar een ander

- Bij Windows DC's zal replicatie zéér belangrijk zijn
- Veranderingen aan de inhoud van de AD kunnen op eender welke DC gebeuren
- De inhoud van de Active Directory samen met zijn Global Catalogs zullen continu gerepliceerd worden

# Multimaster replication

- Windows Server 2000/2003/2008 (R2)/2012 (R2)/2016 gebruikt “multimaster replication”
- Dit betekent dat alle domeincontrollers zich evenwaardig gedragen als “peers”
- Hierdoor kunnen veranderingen gebeuren op elke domeincontroller
- Enkel **veranderingen** worden gerepliceerd

# Wat wordt gerepliceerd?

- **Schema informatie:**
  - Effectieve **structuur** van de Active Directory database
  - Alle domeincontrollers in alle domeinen moeten hetzelfde schema bevatten
  - Wordt vanuit de schema-master gerepliceerd naar alle DC's in de forest.
- **Configuratie informatie:**
  - **Algemene ontwerp** van de volledige enterprise  
Omvat de domeinen en hun plaats in de hiërarchie alsook de replicatie topologie
  - Wordt gerepliceerd naar alle DC's in de forest
- **Domein-data:**
  - de informatie bewaard over de **objecten** in je domein.
  - Replicatie van alle data naar andere domeincontrollers in het domein en/of replicatie van data naar andere GC's (users, computers,....)

# ACTIVE DIRECTORY BEHEREN

# Beheer van objecten

Bij de taken van een administrator zal het beheren van objecten in de Active Directory een van de grootste zijn

==> **Aanmaken, bewerken, verwijderen, ....** van objecten

- De belangrijkste objecten zijn **gebruikers- en computeraccounts**, nodig voor:
  - Authenticatie vd identiteit van de gebruiker of PC
  - Authorisatie of toegang weigeren tot domeinbronnen
  - Andere beveiligingsconcepten beheren
  - Het “loggen” van acties van gebruikers en computers



# Computer Accounts

- Computeraccounts worden ongeveer op dezelfde manier behandeld als gebruikers
- Iedere W2003/XP/Vista/Win7/Win8/Win10 kan toegevoegd worden aan het domein

=> deze zullen zich telkens authenticeren bij het aanmelden

=> de server kan activiteiten loggen en beheer ervan doen van op centrale locatie

# Computers beheren

Een computeraccount kan op 2 manieren toegevoegd worden:

- **Vanop de client**

Nadelen:

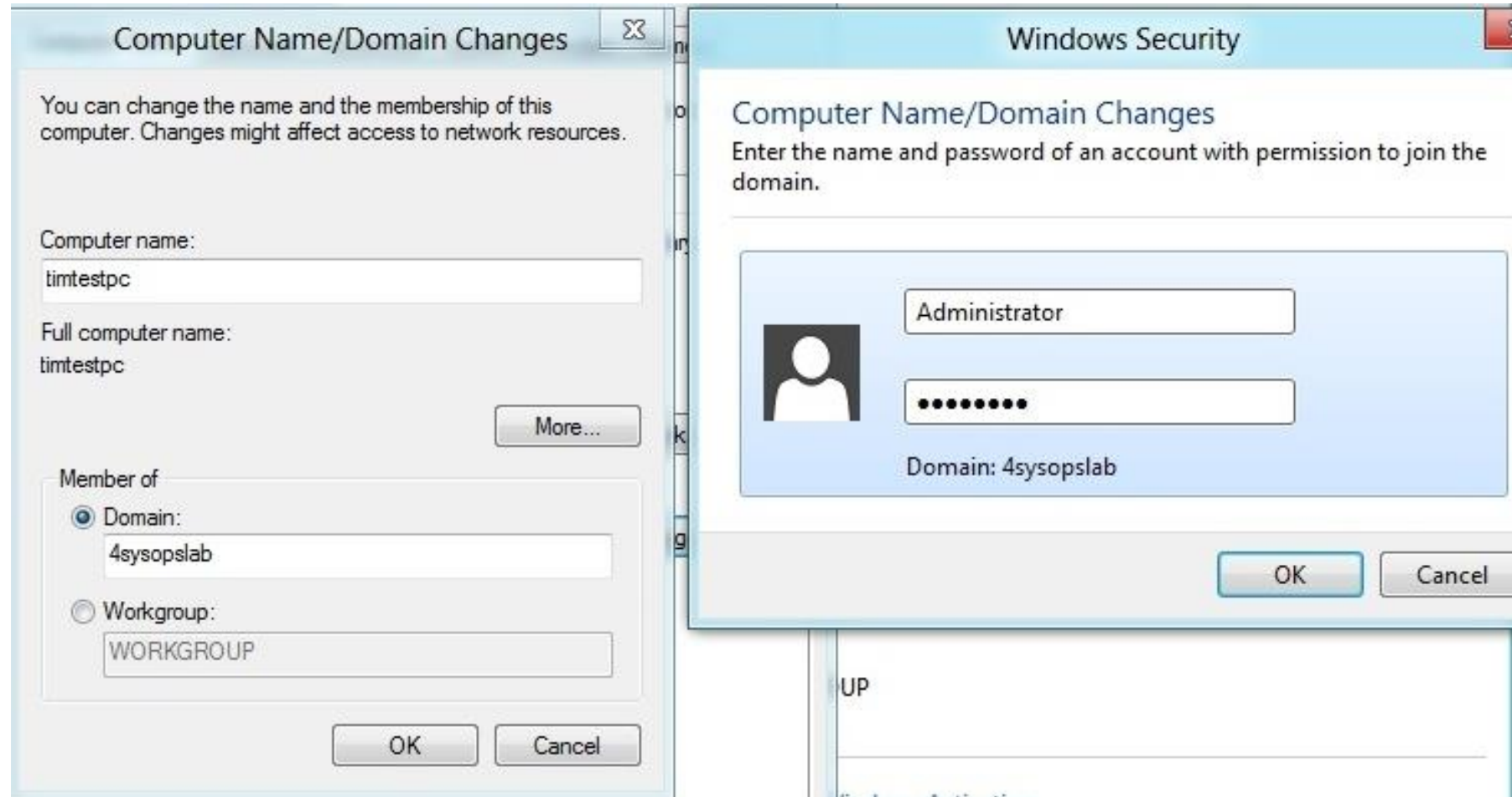
- Domein Administrator nodig om toe te voegen
- Account wordt gecreëerd in standaard OU "computers"

- **Manueel op de server:** In de Active Directory worden de accounts aangemaakt, bv onder een OU. Daar wordt de computernaam ingegeven (zal passen in de DNS-namespace)

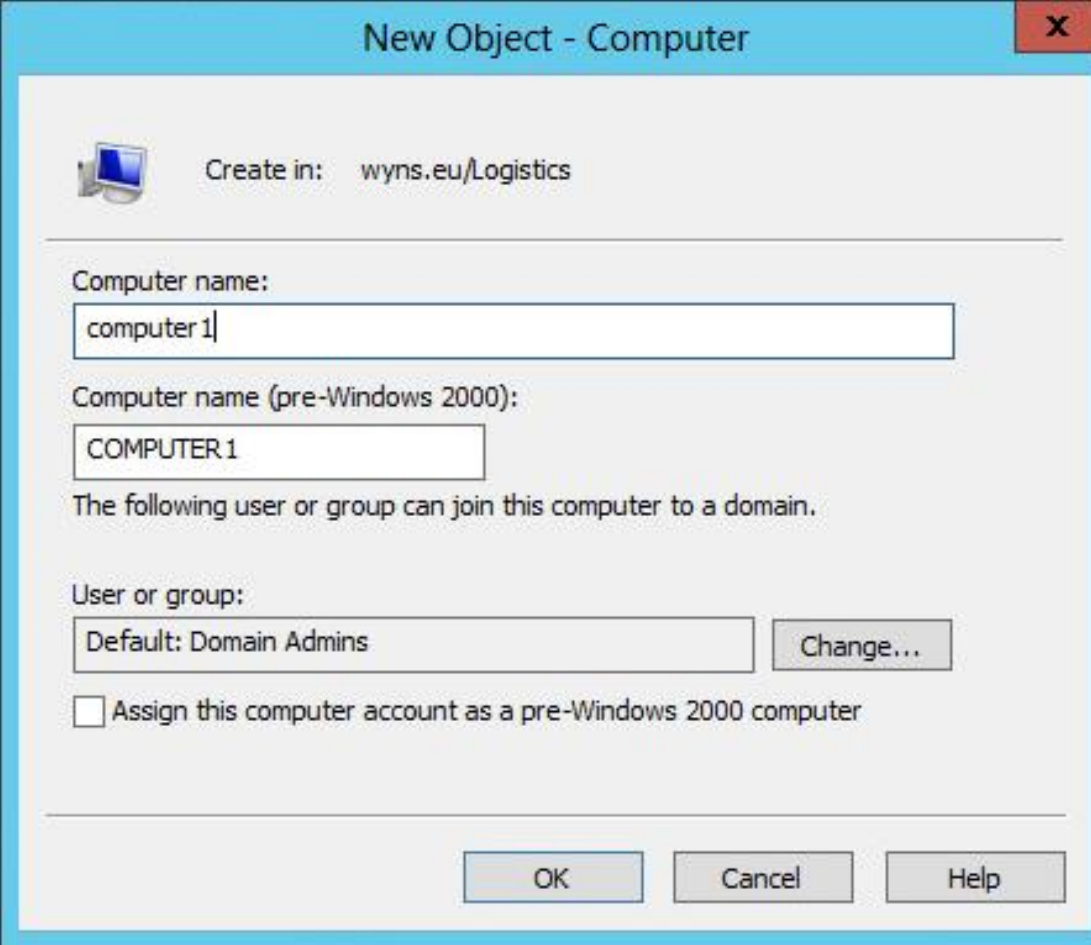
Voordelen:

- Direct in de correcte OU
- Na het aanmaken en effectief toevoegen kunnen de verschillende eigenschappen bekeken worden zoals OS, van welke groepen lid, beveiliging,...

# Vanop de client



# Vanuit de server



The screenshot shows a Windows-style dialog box titled "New Object - Computer". It has a light blue title bar with a red close button (X) in the top right corner. The main area is light gray. At the top left, there is a computer icon and the text "Create in: wyns.eu/Logistics". Below this is a horizontal line. The first section is labeled "Computer name:" and contains a text box with "computer1". The second section is labeled "Computer name (pre-Windows 2000):" and contains a text box with "COMPUTER1". Below these is the text "The following user or group can join this computer to a domain." followed by a section labeled "User or group:" containing a text box with "Default: Domain Admins" and a "Change..." button. At the bottom of the main area is a checkbox labeled "Assign this computer account as a pre-Windows 2000 computer", which is currently unchecked. At the very bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

New Object - Computer

Create in: wyns.eu/Logistics

Computer name:  
computer1

Computer name (pre-Windows 2000):  
COMPUTER1

The following user or group can join this computer to a domain.

User or group:  
Default: Domain Admins    Change...

☐ Assign this computer account as a pre-Windows 2000 computer

OK    Cancel    Help

# Verwijderen en resetten

## Verwijderen van objecten!!!

- Bij verwijderen van een account in de AD (bv computer of gebruiker) wordt het object en zijn SID verwijderd!
- Onomkeerbaar!!!
- Nieuw object met dezelfde naam => andere SID!! = probleem!

Bij crash en herinstallatie van clientPC is het voldoende om de account in de Active Directory te resetten.

- SID blijft behouden
- Koppeling wordt opnieuw gelegd tussen domein en de PC
- Machinewachtwoord wordt tijdelijk weer gereset naar machinenaam+\$

# Gebruikersaccounts

- Gebruikersaccounts zorgen ervoor dat de **gebruikers** zich kunnen **aanmelden** op andere computers en op het domein. Maw authenticeren voor toegang tot bronnen
- Gebruikersaccounts zijn ook nodig als **service accounts** voor bepaalde toepassingen: IIS, Microsoft SQL of Exchange
- Windows voorziet standaard twee accounts bij installatie: **Administrator en Guest** (meestal uitgeschakeld)
- Enkele specifieke instellingen voor gebruikersaccounts bij aanmaak:
  - User must change password at next logon
  - User cannot change password
  - Password never expires
  - Account Disabled

# Gebruikersaccounts

New Object - User

Create in: wyns.eu/Logistics

First name:  Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

< Back Next > Cancel

New Object - User

Create in: wyns.eu/Logistics

Password:

Confirm password:

☐ User must change password at next logon

☒ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

# Gebruikersaccounts

Wanneer de gebruiker aangemaakt is kunnen heel wat extra instellingen beheerd worden.

The screenshot shows the 'Mario Wyns Properties' dialog box with the 'Profile' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar is a tabbed interface with the following tabs: Published Certificates, Member Of, Password Replication, Dial-in, Object, Security, Environment, Sessions, Remote control, Remote Desktop Services Profile, COM+, Attribute Editor, General, Address, Account, Profile (selected), Telephones, and Organization.

Under the 'Profile' tab, there are two main sections:

- User profile:** This section contains two text boxes. The 'Profile path:' box contains the text '\\server\profielen\mario.wyns'. The 'Logon script:' box contains the text 'logonscript.bat'.
- Home folder:** This section contains two radio buttons. The 'Local path:' radio button is unselected. The 'Connect:' radio button is selected. Next to 'Connect:' is a dropdown menu showing 'K:' and a 'To:' text box containing '\\server\homedirs\mario.wyns'.

At the bottom of the dialog are four buttons: OK, Cancel, Apply, and Help.



# Gebruikersaccounts

- **Profile Path:** voor het bewaren van het profiel van de gebruiker. Gebruiker kan op verschillende computers aanloggen en krijgt altijd zijn instellingen mee.  
Gedeelde map nodig op een server  
==> ZWERVENDE PROFIELEN
- **Logon Script:** voor meegeven van Batch-script tijdens inloggen. Wordt bewaard in `\\server\netlogon`. Wordt bv voor mappings gebruikt. (ook terug te vinden onder `\\domein\netlogon`)
- **Local Path:** verwijst naar een map als home directory, lokaal op je PC (niet handig!)
- **Connect:** maakt een verbinding naar je home-directory op een server, adhv een bepaalde letter (cfr H-schijf)

The screenshot shows the 'Mario Wyns Properties' dialog box with the 'Profile' tab selected. The 'User profile' section contains two text boxes: 'Profile path' with the value '\\server\profielen\mario.wyns' and 'Logon script' with the value 'logonscript.bat'. The 'Home folder' section has two radio buttons: 'Local path' (unselected) and 'Connect' (selected). The 'Connect' option shows a drive letter 'K:' in a dropdown menu and a path '\\server\homedirs\mario.wyns' in a text box. At the bottom of the dialog are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

# Gebruikersaccounts

- Bij zowel het “profile path” als “connect” kan er een variabele gebruikt worden voor de gebruikersnaam (%Username%)  
vb: \\server1\homedir\%username%
- Om werk te besparen kunnen ook templates aangemaakt worden. Dit gebeurt op basis van een nieuwe uitgeschakelde account (dummy) die dan telkens gekopieerd wordt.

The screenshot shows the 'Mario Wyns Properties' dialog box with the 'Profile' tab selected. The 'User profile' section contains two text boxes: 'Profile path' with the value '\\server\profielen\mario.wyns' and 'Logon script' with the value 'logonscript.bat'. The 'Home folder' section has two radio buttons: 'Local path' (unselected) and 'Connect' (selected). The 'Connect' option has a dropdown menu showing 'K:' and a 'To:' text box with the value '\\server\homedirs\mario.wyns'. At the bottom of the dialog are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

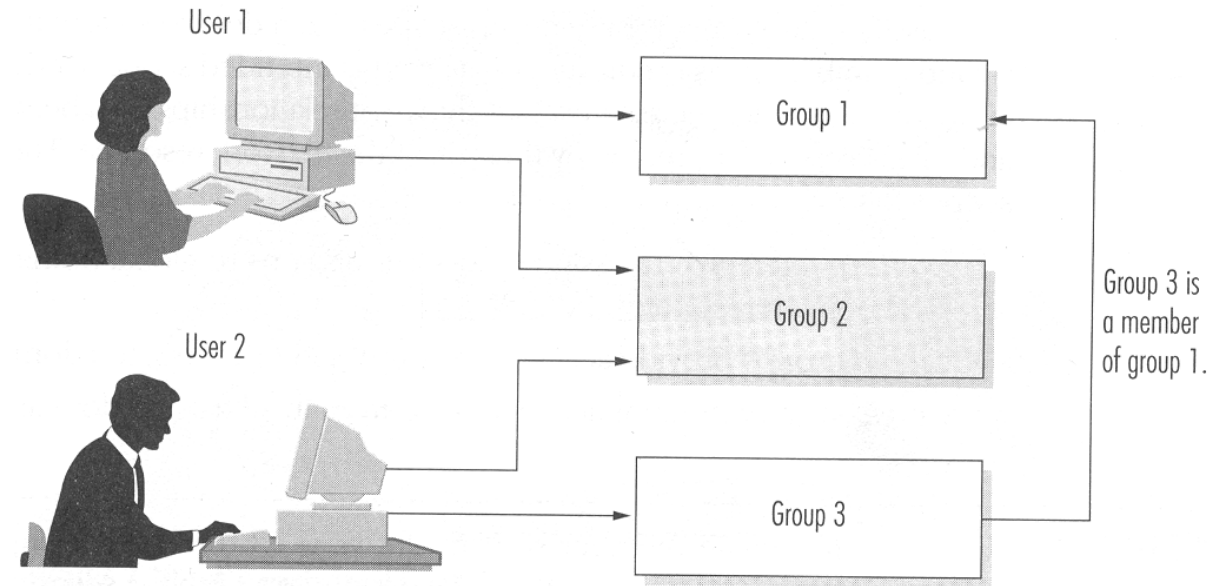
# Groepen

- 1000 accounts beheren kan niet individueel
- ==> gebruikers, computers,... in groepen plaatsen
- Twee grote types:
  - **Distributiegroepen**: exclusief voor **email**, er kan geen beveiliging op toegepast worden
  - **Beveiligingsgroepen**: gebruikt om gebruikers samen te beheren of om **permissies** op bronnen in te stellen. Kan ook voor email gebruikt worden.

# Groepen

Groepen hebben twee belangrijke functies:

- Gebruikers in bepaalde eenheden samenbrengen
- Worden gebruikt om rechten op bronnen of objecten in te stellen



We kunnen de groepen opdelen volgens hun scope:

- Computer local: lokale groepen op de PC (niet domein-gerelateerd)
- Global
- Domain Local
- Universal

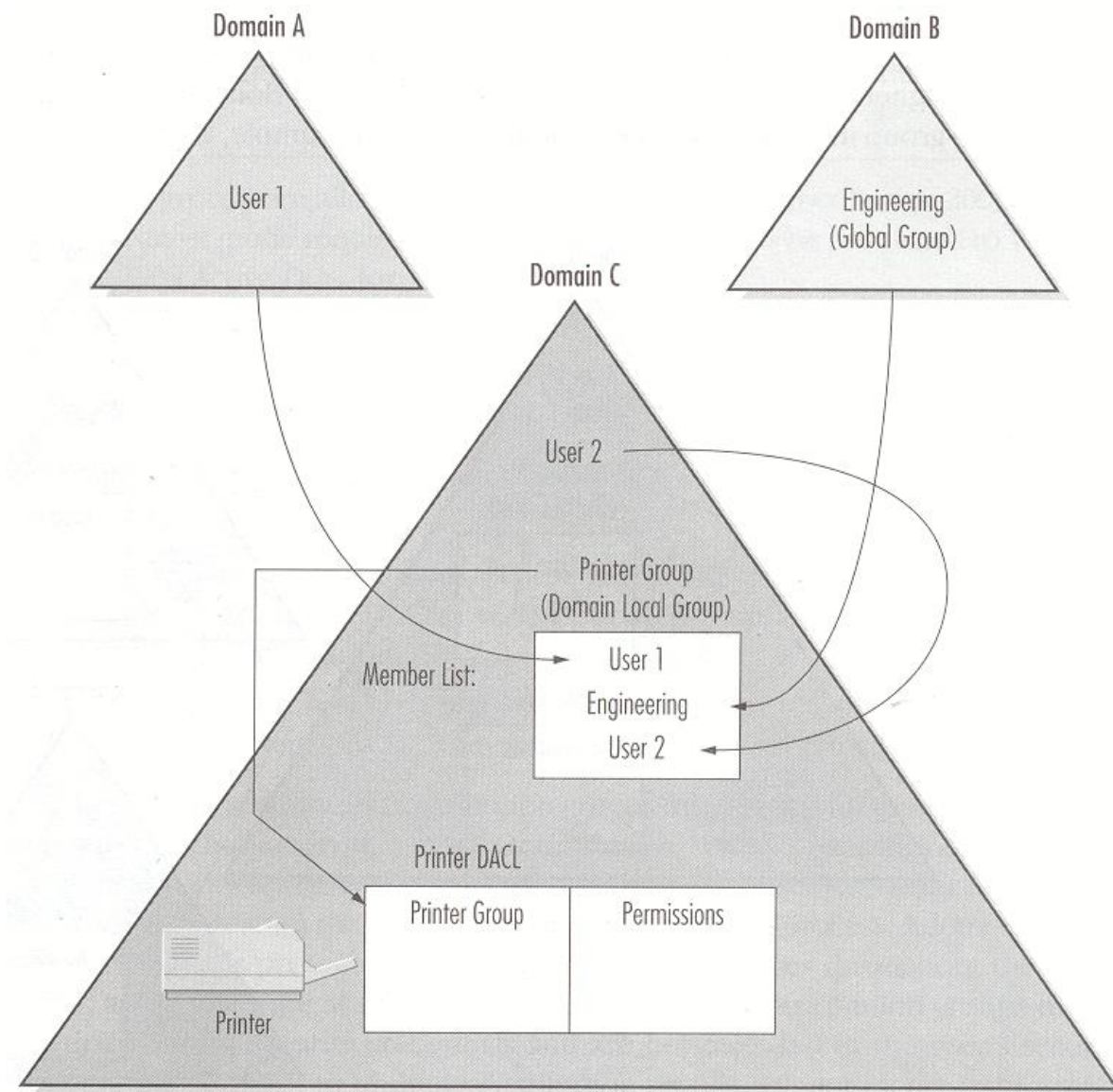
# Computer lokale groepen

- Groep op één lokaal toestel
- Deze groepen kunnen enkel en alleen gebruikt worden om rechten toe te kennen aan bronnen van de lokale computer
- In deze groep kunnen wel accounts en groepen zitten uit het domein
- Voor het domein en andere computers zijn deze groepen en gebruikers dus niet zichtbaar en dus ook niet bruikbaar.

# Domein Lokale Groepen

- Wordt gebruikt om permissies in te stellen op **bronnen binnen het domein**
- De **leden** (gebruikers) van deze groep kunnen **uit elk domein** komen of kunnen globale groepen zijn van andere domeinen
- De Domein Lokale Groepen zijn **beschikbaar binnen het volledige domein**
- “Lokale groepen” bestaan niet meer op DC’s, wel nog op lidservers en werkstations. (Vandaar dat men niet meer lokaal kan aanmelden op een DC, maar altijd als een gebruiker van het domein!!!)

# Domein Lokale Groepen

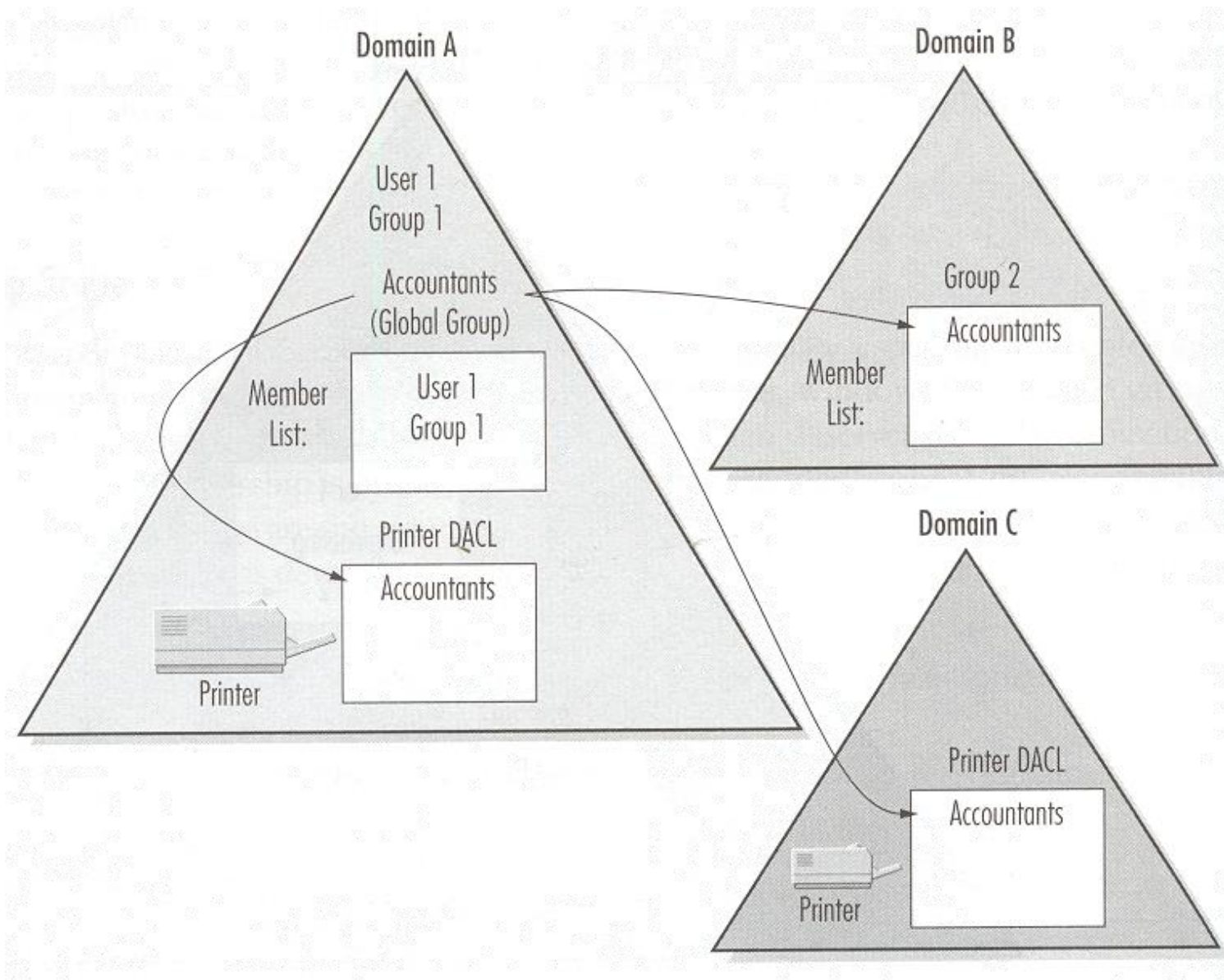


# Domein Globale Groepen

- Wordt meestal enkel gebruikt om gebruikers en computers in onder te brengen, dus niet voor permissies toe te kennen
- De gebruikers krijgen dan permissies via de domein lokale groepen waarvan de globale lid zijn
- Globale groepen kunnen **enkel leden** bevatten **van hun eigen lokale domein**
- Deze groepen staan wel **ter beschikking** (kunnen toegepast worden op) van het **lokale domein en externe domeinen** van de tree/forest



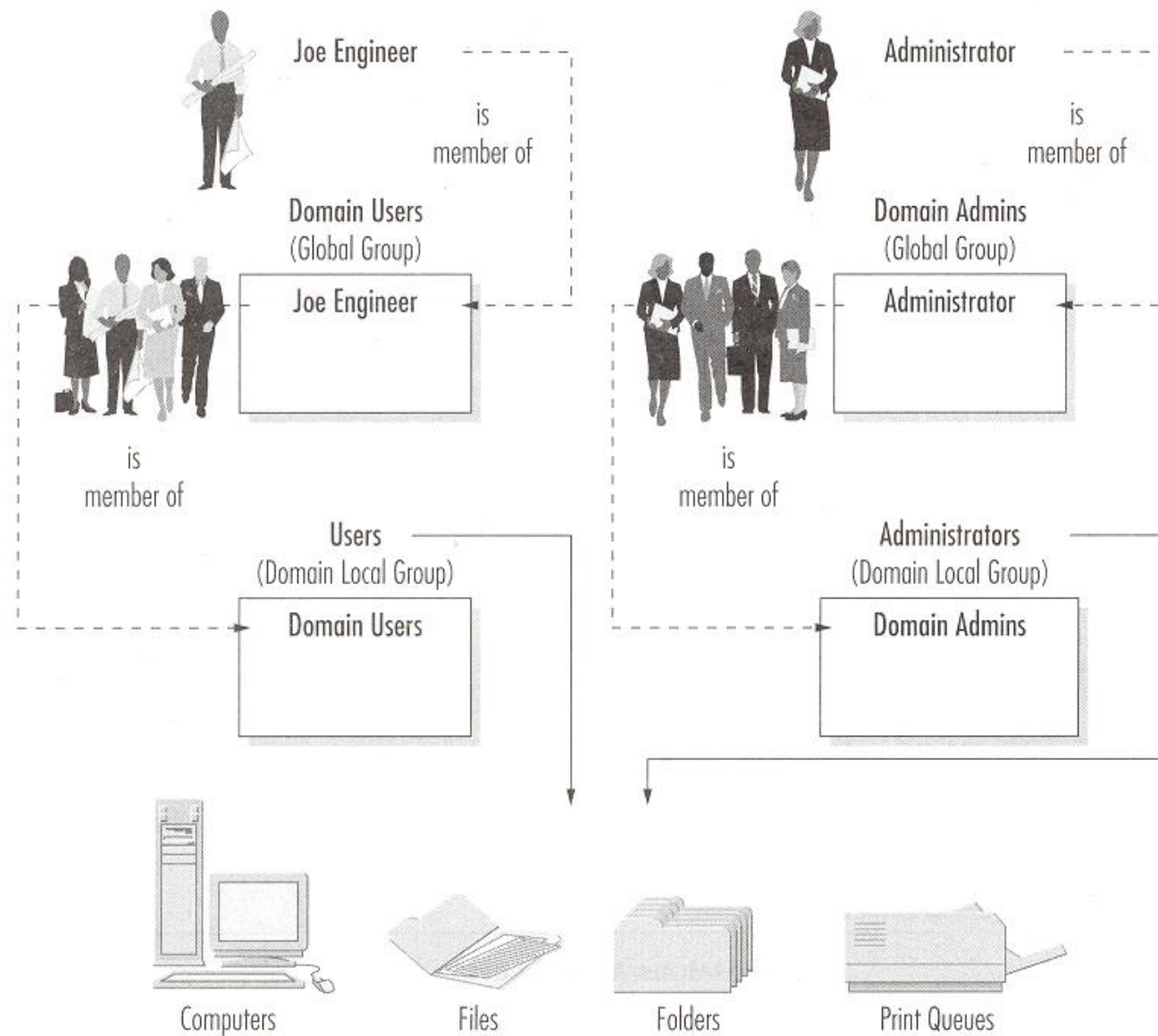
# Domain Globale Groepen



# Universele Groepen

- Deze groepen combineren de mogelijkheden van domein lokale en globale groepen
- Ze kunnen **gebruikers en groepen bevatten van elk domein**
- Ze kunnen **toegepast worden op elk domein**
- M.a.w.: er zit geen domein-begrenzing op deze groepen
- !!! Let op voor replicatieverkeer (Global Catalog)
- Enkel beschikbaar in Native Mode

# Universele Groepen



# Default groepen

Bij de installatie van de DC worden een aantal domein lokale (container "Builtin") en globale groepen (container "Users") aangemaakt.



# Domein lokale groepen

- **Account Operators:** accounts aanmaken, verwijderen, ...
- **Administrators:** volledige controle over het domein  
Domain Admins en Enterprise Admins zijn lid van deze groep
- **Users:** taken uitvoeren, printer gebruiken, ...

# Domein globale groepen

- **Domain Admins:** volledige controle over het domein
- **Domain Users:** alle gebruikers van een domein
- **Enterprise Admins:** volledige controle over de forest

# Speciale groepen

Niet terug te vinden in de mmc (management console) (Virtuele groepen)

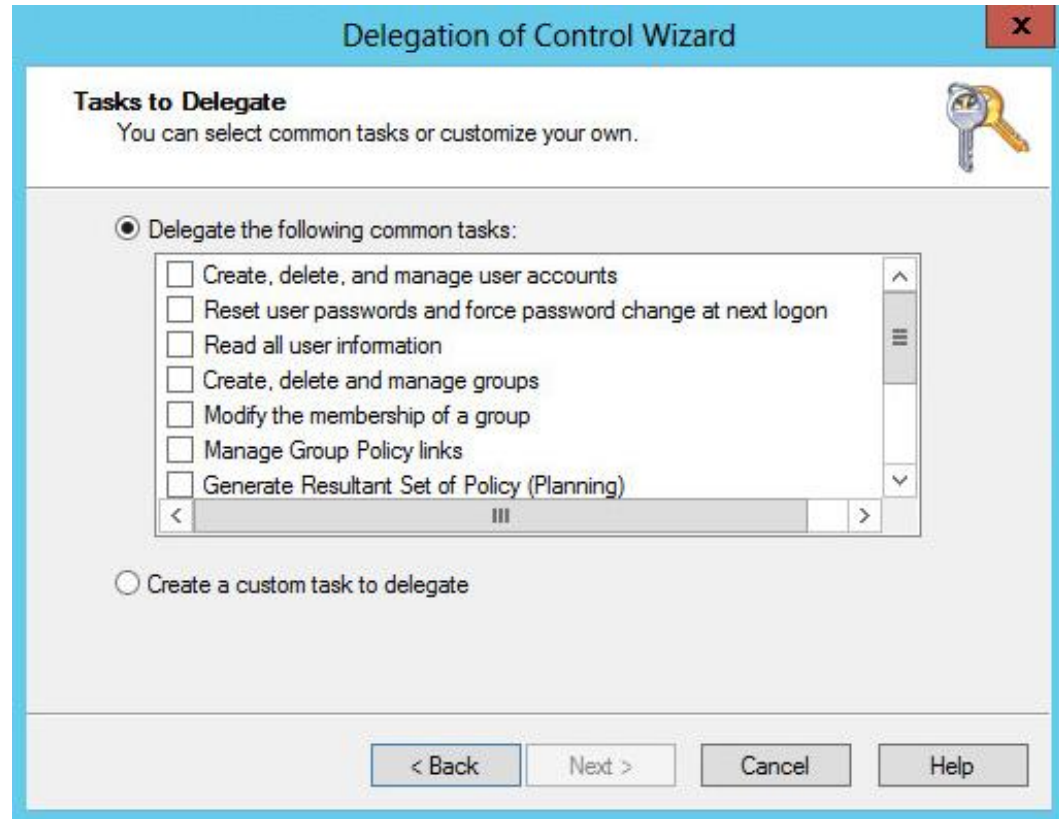
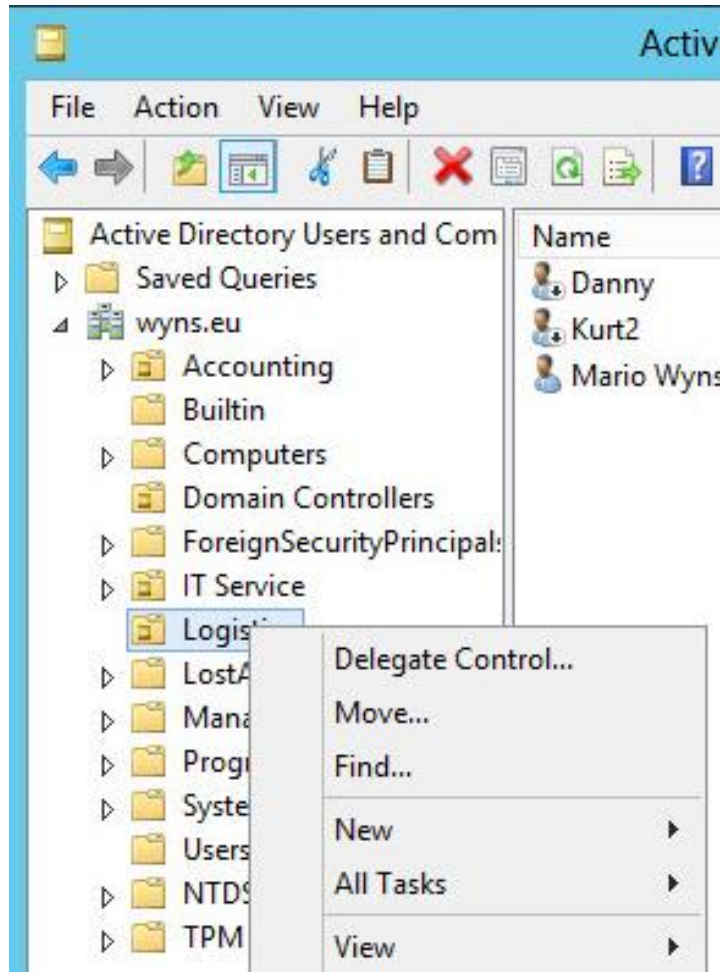
- **Everyone:** Stellen alle gebruikers voor die een verbinding maken via het netwerk of lokaal aanmelden
- **Network:** Dit is een groep die alle gebruikers bevat die een bron over het netwerk aan het gebruiken zijn
- **Interactive:** Dit zijn de gebruikers die effectief fysisch op het lokale station aangemeld zijn
- **Authenticated:** Alle gebruikers die op dit moment aangemeld en dus geauthenticeerd zijn

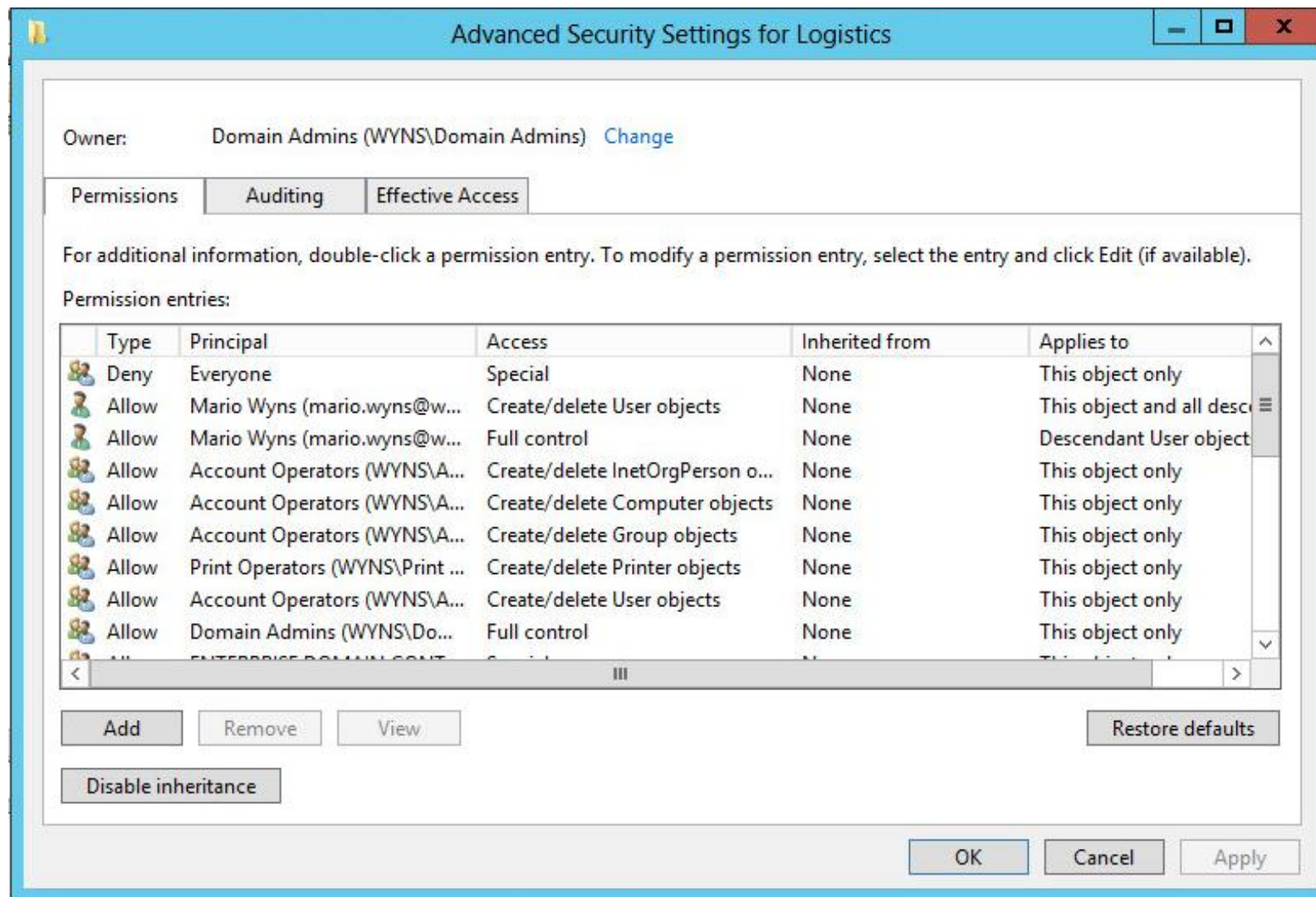
# OU's delegeren

- Zoals eerder gezien, worden OU's gebruikt om de objecten in Active Directory verder te structureren
- Maar op OU's kunnen we ook permissies plaatsen zodat hiermee kan bepaald worden wie welke rechten heeft op een OU
- *"Delegate Control"*  
is een wizard die de handmatige instelling overneemt waarmee je willekeurige gebruikers gepaste rechten kan geven (bv objecten toevoegen, verwijderen,...)



# OU's delegeren





In het tabblad “permissions” kunnen de effectieve machtigingen op de Active Directory-objecten bekeken worden. Dit kan enkel indien men de geavanceerde weergave aanvinkt

# Gedeelde mappen

- Een gedeelde map maakt men aan om de inhoud “beschikbaar” te stellen voor netwerkgebruikers.
- Anders genoemd: share
- Shares kunnen in Active Directory gepubliceerd worden.
- Aanmaken van shares moet volgens UNC\*.
- Via GUI (verkenner) of command-line:  
NET USE K: \\server\gedeelde\_map
- Alle huidige shares kunnen bekeken worden adhv  
NET SHARE  
of via computerbeheer

\* UNC = Universal Naming Convention (<https://msdn.microsoft.com/en-us/library/gg465305.aspx>)

# Rechten op gedeelde mappen

- De uiteindelijke rechten die een gebruiker zal krijgen op een map over het netwerk, zal bepaald worden door 2 zaken:

## **NTFS-rechten én Share-rechten**

- Makkelijkste benadering: Share-rechten op Full Control, daarna alles regelen via NTFS-rechten.
- Bij conflicten zal telkens de meest beperkende permissie gelden.
- Belangrijk:

Wanneer je een map of bestand met NTFS-permissies verplaatst naar een FAT-partitie, dan vervallen alle NTFS-permissies. Bij het kopiëren erven de copies de NTFS-permissies van de map waarin ze terecht komen. Bij verplaatsen op hetzelfde volume blijven de oorspronkelijke NTFS-permissies behouden. Bij verplaatsen naar een ander volume worden de NTFS-permissies van de bestemming overgeërfd. Degene die kopieert of verplaatst wordt automatisch Eigenaar, behalve bij verplaatsen naar een ander volume.

# Andere tools voor beheer AD

- Er zijn naast de console ook andere beheersmogelijkheden voor de AD
- LDIFDE, CSVDE, ADSI en PowerShell zijn enkele technieken die standaard aanwezig zijn
- Daarnaast zijn er ook nog Third-Partyoplossingen of eigen scripts/applicaties
  - LDIFDE kan gebruikt worden om data te importeren en exporteren van of naar de AD  
vb LDIFDE -f export.txt
  - CSVDE: maakt gebruik van komma, gescheiden bestanden, ideaal voor toevoegen van nieuwe objecten adhv Excel-sheets.
  - ADSI (AD Service Interface): geeft mogelijkheid om zelf scriptjes te maken om objecten te manipuleren

# Powershell-voorbeeld

New-ADUser

```
-Name "John Smith"  
-SamAccountName "john.smith"  
-Description "Sales Manager"  
-Department "Sales"  
-EmployeeID "45896"  
-Path "ou=users,ou=sales,dc=test,dc=local"  
-Enabled $true
```

# OPENLDAP



# LDAP

## Lightweight Directory Access Protocol

- Protocol om te interageren met Directory Systemen
- Loopt over TCP/IP of andere connectie georiënteerde communicatie
- IETF - The Internet Engineering Task Force
- Vooral voor op X.500 gebaseerde Directory Systemen



# LDAP

- *How is the information referenced?*

Een unieke naam bestaande uit:

- Eigen naam (RDN - Relative Distinguished Name)
  - Opsomming van de namen van de parents (ou's + domein)
- *How is the information accessed?*
    - Vooral opzoeken van informatie (filteren + details)
    - Ook toevoegen, verwijderen en wijzigen
  - *How is the information protected from unauthorized access?*

Authenticatie

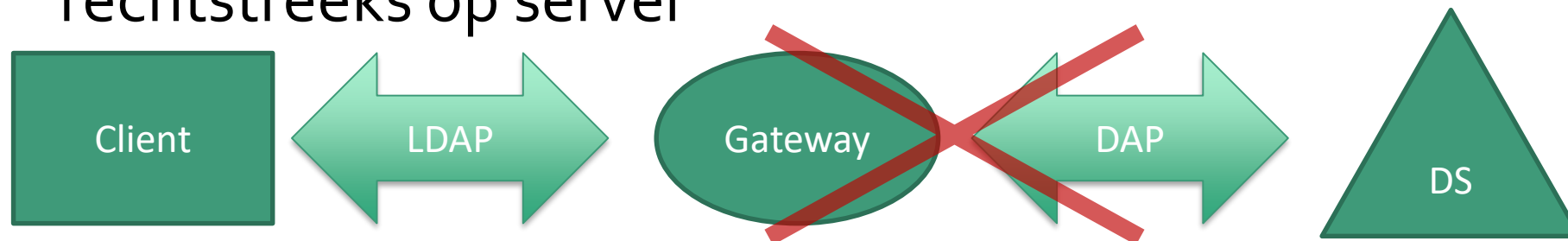
# LDAP

## Hoefdoelen/toepassingen van LDAP:

- Toestel authenticatie
- Gebruiker authenticatie
- Groepen van gebruikers en systemen
- Adres boek
- Voorstelling van de organisatie
- Telefoonboek
- Gebruikersbeheer
- Centraal beheer van instellingen van toepassingen
- ...

# LDAP structuur

- Eén of meerdere servers (die dezelfde informatie aanbieden)
- Meerdere clients
- Client-server communicatie
  - Client stelt vragen of geeft commando's
- Vroeger communicatie via gateway, nu meestal LDAP rechtstreeks op server



# LDAP

LDAP v3 ter vervanging van LDAP v2

- Sterkere authenticatie en data security via SASL
- Certificaat authenticatie en data security via TLS (SSL)
- Internationalisatie
- Uitbreidbaarheid
- LDAP v2 en LDAP v3 werken niet goed samen
- LDAP v2 zo veel mogelijk vermijden

## Open source implementation of the Lightweight Directory Access Protocol

- 3 belangrijke onderdelen:
  - Slapd: stand-alone LDAP daemon
  - Libraries: implementatie van het LDAP protocol
  - Client software: Utilities, tools, sample clients
- Sinds 1998
- LDAP v3

# slapd

stand-alone LDAP daemon

- LDAP directory server
- Ondersteunt verschillende besturingssystemen
- Beveiliging op verschillende lagen van het OSI model
- Keuze uit verschillende backends (gegevensopslag)
- API voor het toevoegen van eigen modules (=open standaard)
- Multi-threading
- Replication en caching

# Overlays

OpenLDAP bestaat uit 2 delen:

- Frontend die de vragen ontvangt
- Backend die de vragen verwerkt en toepast

Overlays zijn lagen die kunnen tussen gebracht worden

Enkele voorbeelden:

- auditlog: log server activity in a flat text file
- dyngroup: simple dynamic group support
- pcache: cache search results, mainly to improve performance for proxied servers
- rwm: rewrite module, for various alterations of LDAP data

# Replicatie

- Synchronisatie van gegevens in de directory (database)
- Master slave?
  - Single master / multi slave voor redundantie
  - Multi master mogelijk om single point of failure te vermijden
- Vorige versies server/client
- Sinds OpenLDAP2.4 provider/consumer
- *syncrepl* - LDAP Sync Replication engine (thread van slapd)  
gebruikt LDAP Content Synchronization protocol (LDAP Sync)



# Gerelateerde projecten

- JLDAP - LDAP class libraries voor Java
- JDBC-LDAP - Java JDBC - LDAP Bridge driver
- Idapc++ – LDAP class libraries voor C++
- Fortress - Role-based identity access management Java SDK
- LMDB - Memory-mapped database library

# Bronnen

- Replicatie - [https://technet.microsoft.com/en-us/library/cc737314\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc737314(v=ws.10).aspx)
- Active Directory Schema - [https://msdn.microsoft.com/en-us/library/windows/desktop/ms675087\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms675087(v=vs.85).aspx)
- Active Directory Groepen - [https://technet.microsoft.com/en-us/library/cc739393\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc739393(v=ws.10).aspx)
- LDAP - <http://www.openldap.org/doc/admin24/intro.html#What%20is%20LDAP>
- OpenLDAP - <http://www.openldap.org/doc/admin24/intro.html>
- OpenLDAP - <https://en.wikipedia.org/wiki/OpenLDAP>
- OpenLDAP replication - <http://www.openldap.org/doc/admin24/replication.html>