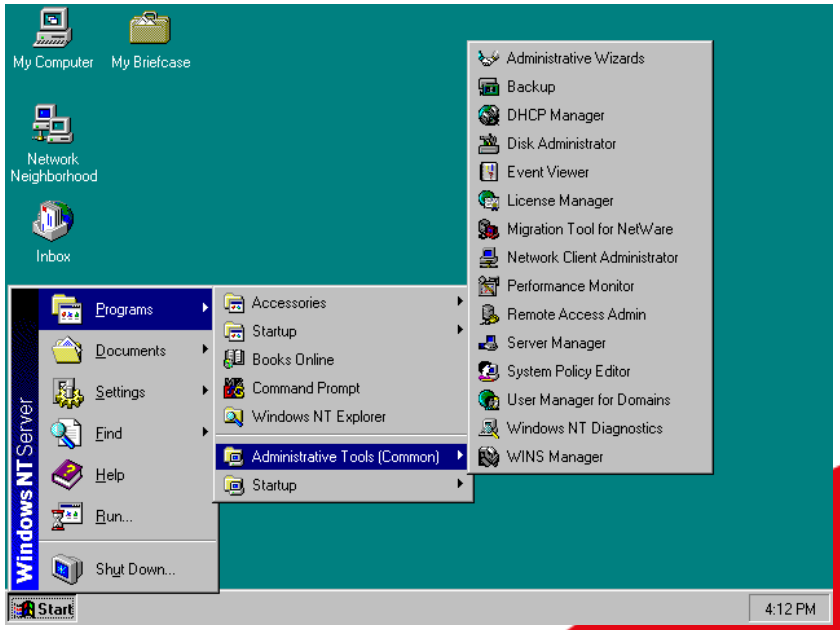
# 3. Active Directory (AD) configuratie

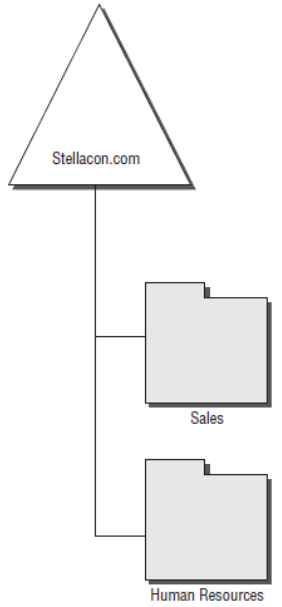
Server OS

# Windows NT4 domain model: LIMIETEN

- Slechte schaalbaarheid.
- Management van trusts (vertrouwensrelaties) is moeilijk.
- Grote bandbreedte nodig voor synchronisatie van objecten (accounts).
- Flat directory namespace (geen hiërarchieën mogelijk).
- Geen nesting van groepen.
- …



# Active Directory Definitie

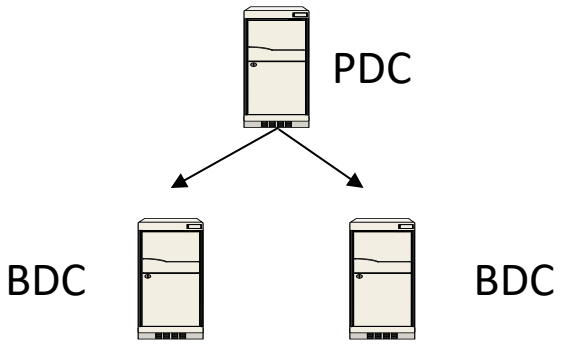



- Het “Active Directory” tijdperk
  - Boomstructuur
  - Logische en fysieke hiërarchie opbouw

  → typisch zoals bedrijvenstructuur
  - Integratie met DNS voor name resolution
- Wat is Active Directory?
  - Is een Directory Service: Definiëren, managen, voorzien van toegang en beveiligen van netwerk resources (printers, bestanden, applicaties, …)

# AD in het Windows NT tijdperk

- PDC en BDC principe (primary en backup domain controller)
  - PDC is de “master database” met R/W kopie.
  - Er kan maar 1 PDC zijn.
  - BDC’s (1 of meerdere) bevatten readonly kopie van de database (voor Load Balancing en High Availability).
  - Bij eventuele problemen BDC ‘promoveren’ naar PDC.
- Dikwijls multiple domain topology
  - 1 of meerdere domeinen en resource domeinen (met andere objecten zoals printers, shares, …).
  - Trust relaties tussen deze domeinen.
  - Niet schaalbaar. Administratieve kater.



# Voordelen van AD

- Integratie met DNS
- Schaalbaarheid
- Centraal management
- Delegatie
- Interactie tussen domeinen

# Wat is een Domain Controller?

- Installatie Active Directory
- Kopie Active Directory
  - R/W vanaf Windows 2000
  - Vanaf Windows Server 2008 ook read-only DC mogelijk
- Veranderingen aanbrengen aan Directory Services
- Synchroniseren naar andere DC's
- User logon service, authenticatie, directory zoekfuncties
- Elke server binnen een domein die geen domaincontroller is wordt een member-server genoemd

# Logische structuur van Active Directory

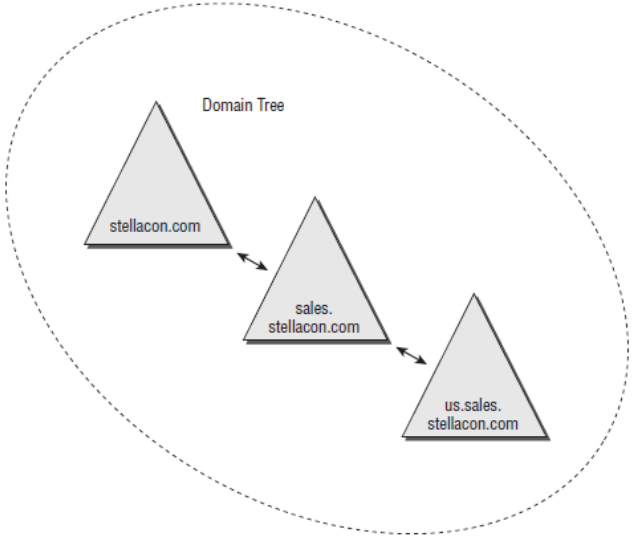
- Domein
  - Logische entiteit om je netwerk mee te beheren.
  - Logische security boundary waarbinnen gerelateerde netwerkresources gemaakt, gewijzigd en verwijderd kunnen worden.
  - Een partitie/container in een Active Directory Forest.
  - Administratief afgebakend geheel.
  - Datareplicatie.

# Logische structuur van Active Directory

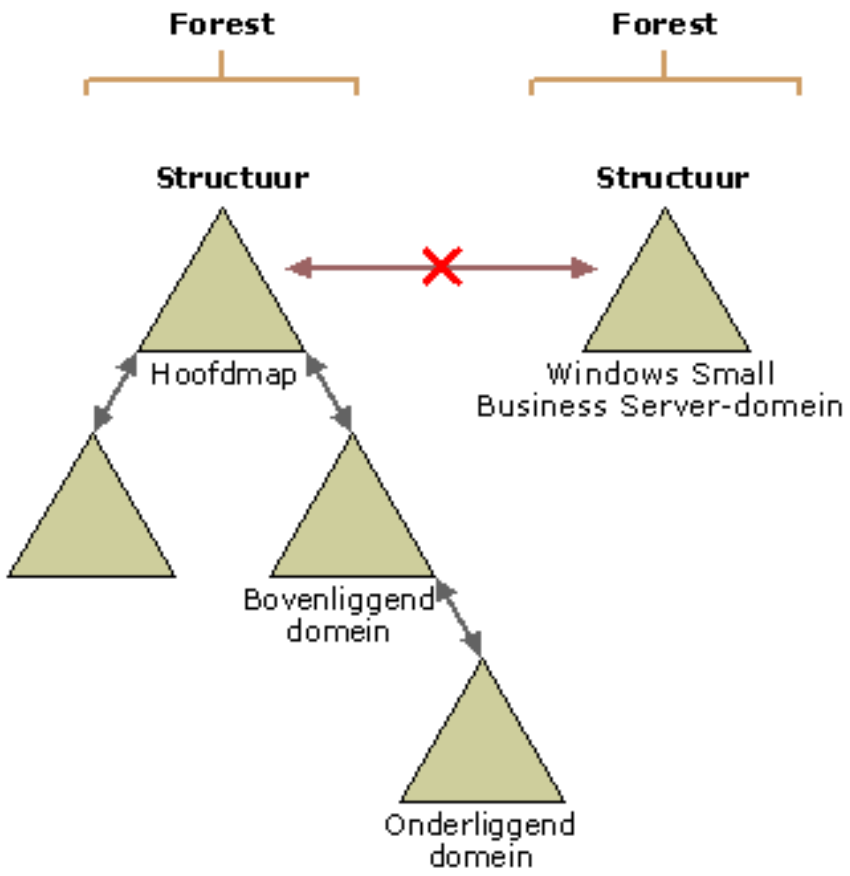
- Forest
  - Meerdere domeinen kunnen in domain trees geordend worden.
  - Domain trees zijn hiërarchische verzamelingen van één of meerdere domeinen.
  - Parent/Child domain.
  - Root domain is het hoogste domein in de hiërarchie.
  - Trust relaties worden automatisch aangemaakt tussen parent en child domains.
  - Contiguous namespace.

# Logische structuur van Active Directory

- Meerdere domeinen kunnen grotere structuren vormen
  - Hiërarchische structuren
  - Analogie: wijk is een domein, stad is een forest, het forest bestaat uit meerdere domeinen.
  - Beheer van het netwerk kan gecentraliseerd of gedecentraliseerd.
- 1 of meerdere trees maken een forest
  - Non-contiguous namespace.



# Logische structuur van Active Directory

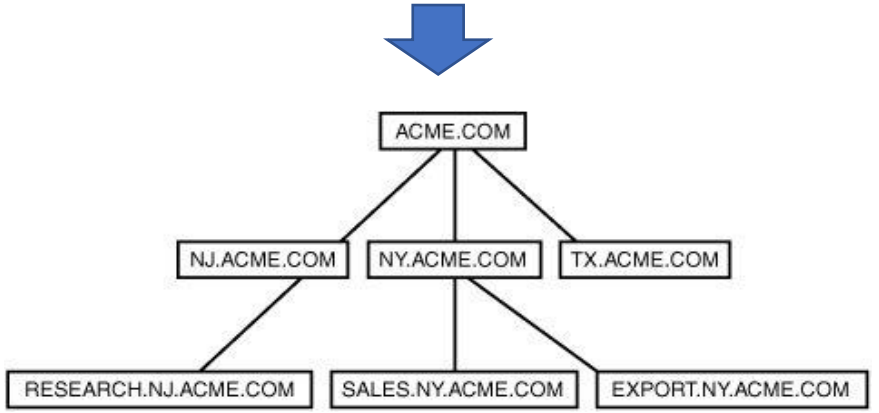



Elke driehoek vertegenwoordigt een Active Directory-domein.
Elke dubbele pijl vertegenwoordigt een vertrouwensrelatie.

**A forest is a non-contiguous namespace**

**-**

**A domain tree is a contiguous namespace**



# Active Directory Schema

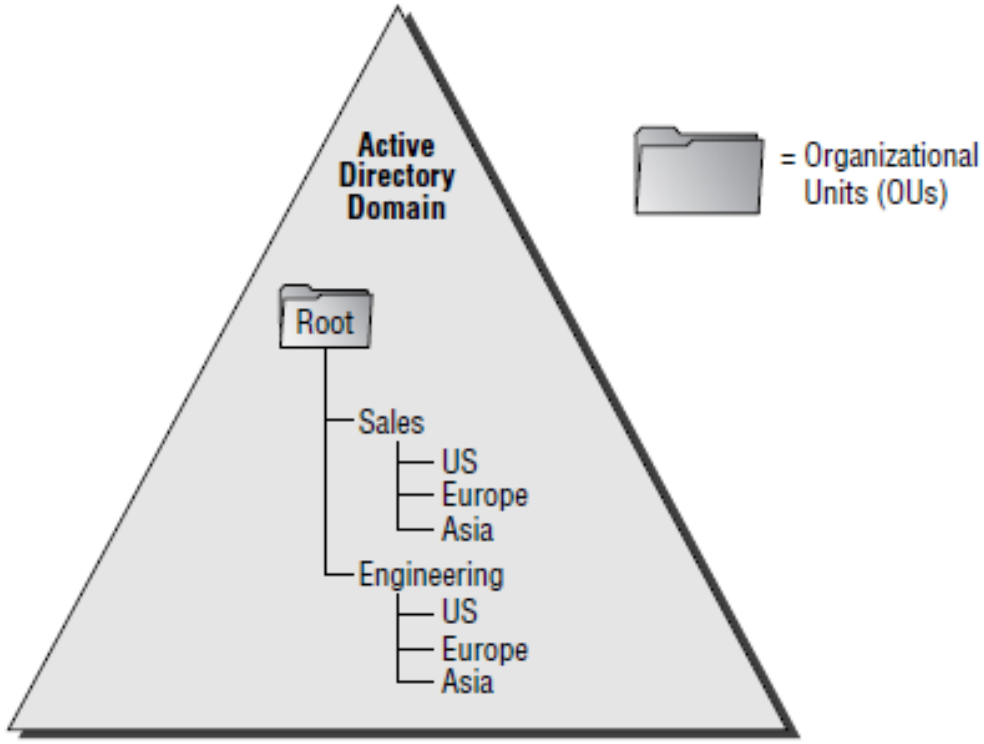
- Bevat de definities van alle objecten (users, computers, printers, …).
- 1 schema per forest. Alle objecten voldoen aan dezelfde regels.
- Veranderingen aan het schema worden gerepliceerd naar alle DC's.
- Schema updaten? Lid van de schema administrators.
- Twee types van objecten:
  - *Attribute*: stukje informatie dat bewaard wordt in AD. Bijvoorbeeld voornaam, familienaam, functie, …
  - *Classes*: collection of attributes. Bijvoorbeeld Employee (bevat voornaam en naam).
  - Verschillende classes kunnen dezelfde attributes gebruiken.
    Ze werken onafhankelijk van elkaar.
  - Default bestaan er verschillende, maar ze kunnen uitgebreid worden.

# Active Directory Objecten

- Representeren een enkele en unieke database entry in Active Directory.
- Elk object heeft een **Security Identifier (SID)**.
  - Uniek per object.
  - Alle rechten worden op de SID geplaatst en niet op de naam.
- Elk object heeft ook een **Distinguished Name (DN)**.
  - Unieke naam per object.
  - De lange naam voor een object is de DN en is eigenlijk het volledige pad.
  - Voorbeeld: `ehb.local/EHB/IWT/Users/Studenten/Janssens, Jan`
  - Of in een LDAP connectionstring:
    `“LDAP://dt-srv-dc01.ehb.local/OU=Studenten,OU=Users,OU=IWT,OU=EHB,DC=ehb,DC=local”`
- SID zal nooit veranderen. Object verwijderen en opnieuw aanmaken = nieuw SID.
- DN kan veranderen bij wijzigingen in de AD-structuur.

# Active Directory Organizational Units

- Wordt gebruikt om alles hiërarchisch onder te verdelen.
- Groeperen van Objecten.

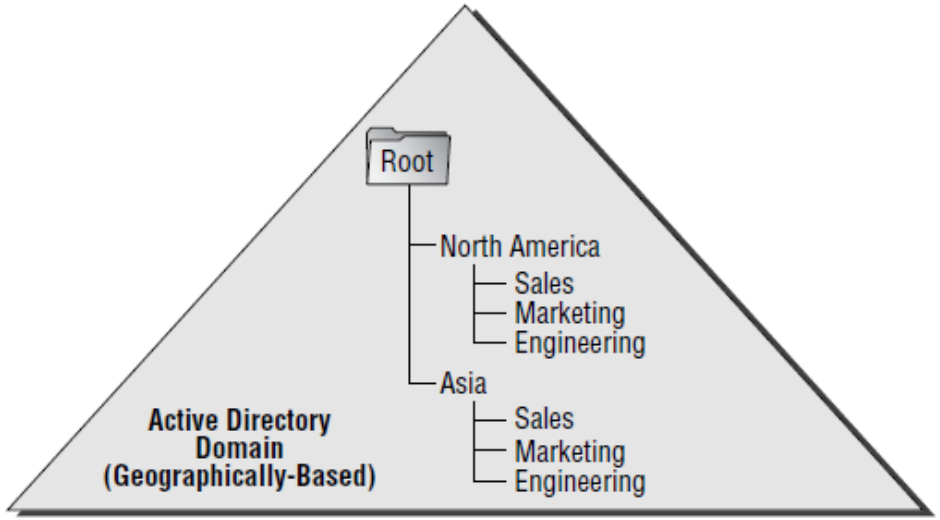


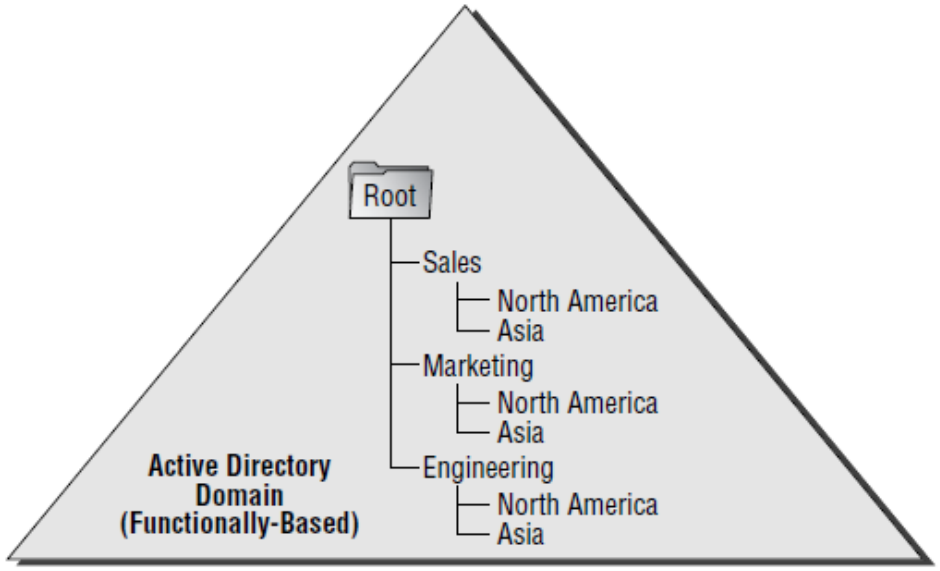
# Active Directory Organizational Units

- OU Design heeft geen impact op DNS.
- OUs kunnen genest worden.
- OUs zijn transparant voor de eindgebruiker. Merkt er niets van (tenzij er policies zijn toegepast).
- OU structuur is zeer eenvoudig aanpasbaar.
- Enkel aanmaken als je ze echt gebruikt.
- Hulpmiddel voor de administrator.

# Active Directory OU Structuur

- Kan op verschillende manieren opgebouwd worden.
  - Bijvoorbeeld geografisch, op functie of op delegatie van administratie (verschillende administrators die elk een deel managen).
- Structuur is belangrijk want op deze manier gaan we rechten, group policy's (software installaties, desktop configuratie, login scripts, …), en dergelijke toekennen.

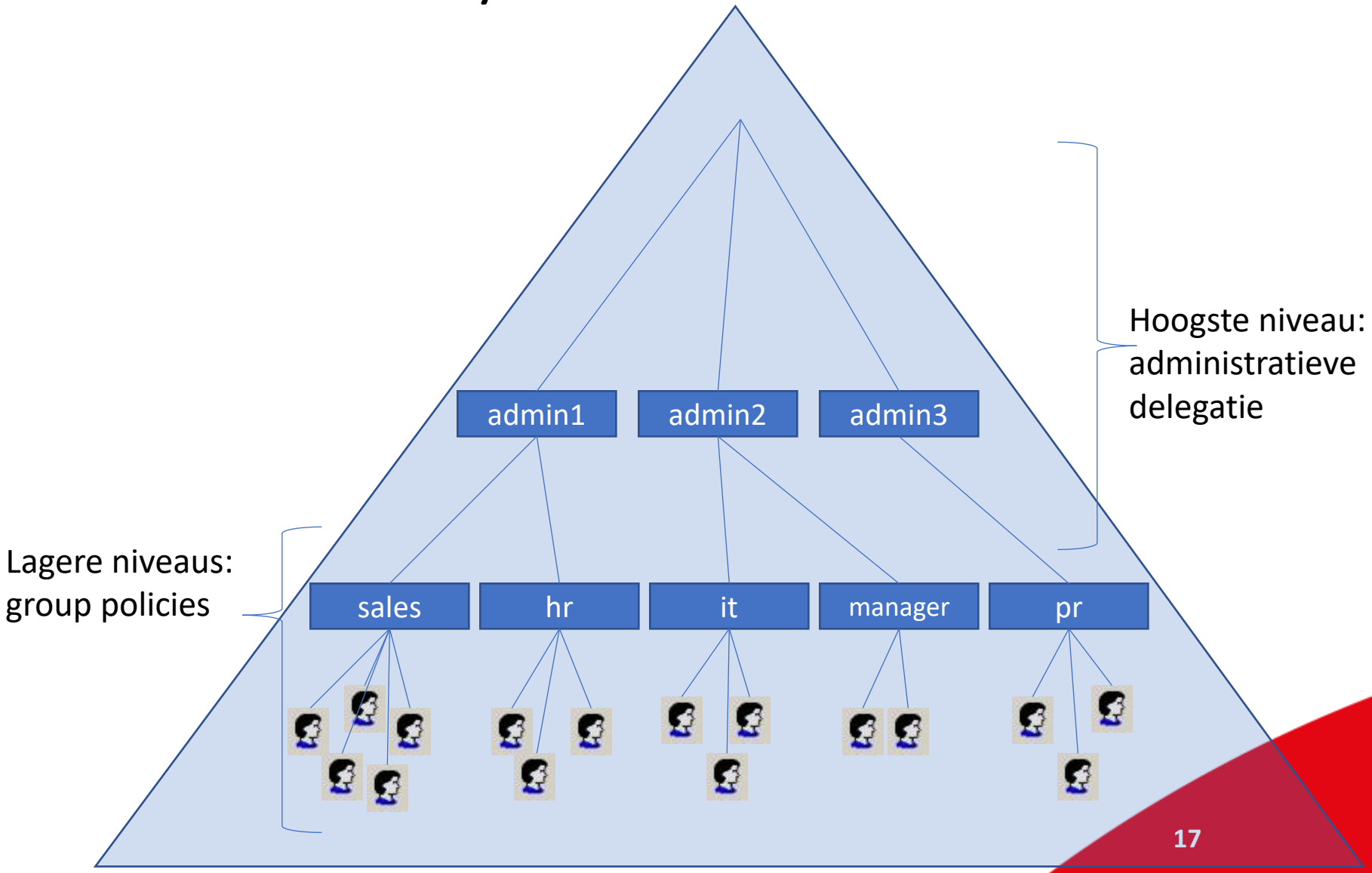


# Active Directory OU Structuur

- Hoogste niveau: best een principe volgen dat weinig zal veranderen.
- Verder kan een combinatie gebruikt worden (zie voorafgaande afbeelding).
- Men gebruikt meestal:
  - Op hoogste niveau: administratieve delegatie.
    Vb: bedrijf met 3 admins.
    - Admin 1 doet departement 1
    - Admin 2 doet departement 2, enz.
  - Op lager niveau: group policy (zie hoofdstuk Group Policy Objects).

# Active Directory OU Structuur




Hoogste niveau: administratieve delegatie

Lagere niveaus: group policies

# Global Catalog (GC)

- Is een database die informatie van objecten in alle domeinen in de Active Directory omgeving bijhoudt.
- Houdt slechts een gedeelte van de forest-wide AD informatie bij.
  - Niet alle attributen, enkel zogenaamde PAS (Partial Attribute Set) (naam, voornaam, logon name …).
  - Van het eigen domein worden wel alle attributen opgeslagen.
- Is een DC (aanvinken dat deze DC ook GC is).
- Meerdere GCs kunnen voorkomen.
- Waarvoor gebruikt?
  - Indexed searches.
  - Zoeken naar objecten in de forest (port 3268)
  - Verhoogde performantie voor forest-wide queries
  - Resolving van UPN (User Principal Name): Omzetten UPN naam → Username.
    Zelfs nodig in single-domain omgeving.
  - Opgelet: in een single domain bevat de global catalog altijd alle attributen.

# Operations Masters

- AD = multimaster database.
- Sommige gevoelige operaties mogen niet overal.
- Single-master ipv multi-master.
- Voor deze operaties worden FSMO rollen gemaakt.
  - Flexible: verplaatsbaar
  - Single-master: er is maar 1 DC die deze rol op zich mag nemen
  - Operation: een bepaalde operatie die niet overal kan gedaan worden
- Er bestaan 5 FSMO rollen
  - 3 rollen uniek per domein
  - 2 rollen uniek per forest

# Operations Masters

- 3 rollen, uniek per domein
  - RID (Relative Identifier) master
    - Deelt relatieve identifiers (RID) uit aan DC's in het domein.
    - RID’s die vervolgens worden gebruikt voor opbouw SID’s.
  - PDC (Primary Domain Controller) Emulator master.
    - Backwards compatibility met NT4 domeinen en down-level clients.
    - Verantwoordelijk voor password changes.
    - PDC emulator bevat altijd de laatste versie van het wachtwoord.
    - Indien wachtwoord foutief, even navragen bij PDC emulator.
    - Verantwoordelijk voor time synchronization.
      Indien klok <> 5 min dan geen vertrouwen meer.
    - Wijzigingen aan GPO’s bijhouden.
    - Wijzigen van security-sensitive info, bvb paswoord of account lockouts

# Operations Masters

- 3 rollen, uniek per domein
  - Infrastructure Master
    - Verantwoordelijk voor reference updates van het domein naar andere domeinen.
      Bvb persoon wordt lid van groep in ander domein → members updaten.
    - Bekijkt dus onder andere welk domein welke objecten bevat.
- 2 rollen, uniek per forest
  - Domain Naming Master
    - Aanmaken/verwijderen van domeinen aan forest, trees, application data partitions…
    - Zorgt voor unieke naamgeving.
  - Schema Master
    - Houdt wijzigingen aan het schema bij.
    - Heeft als enige write rechten op het schema.

# Operations Masters

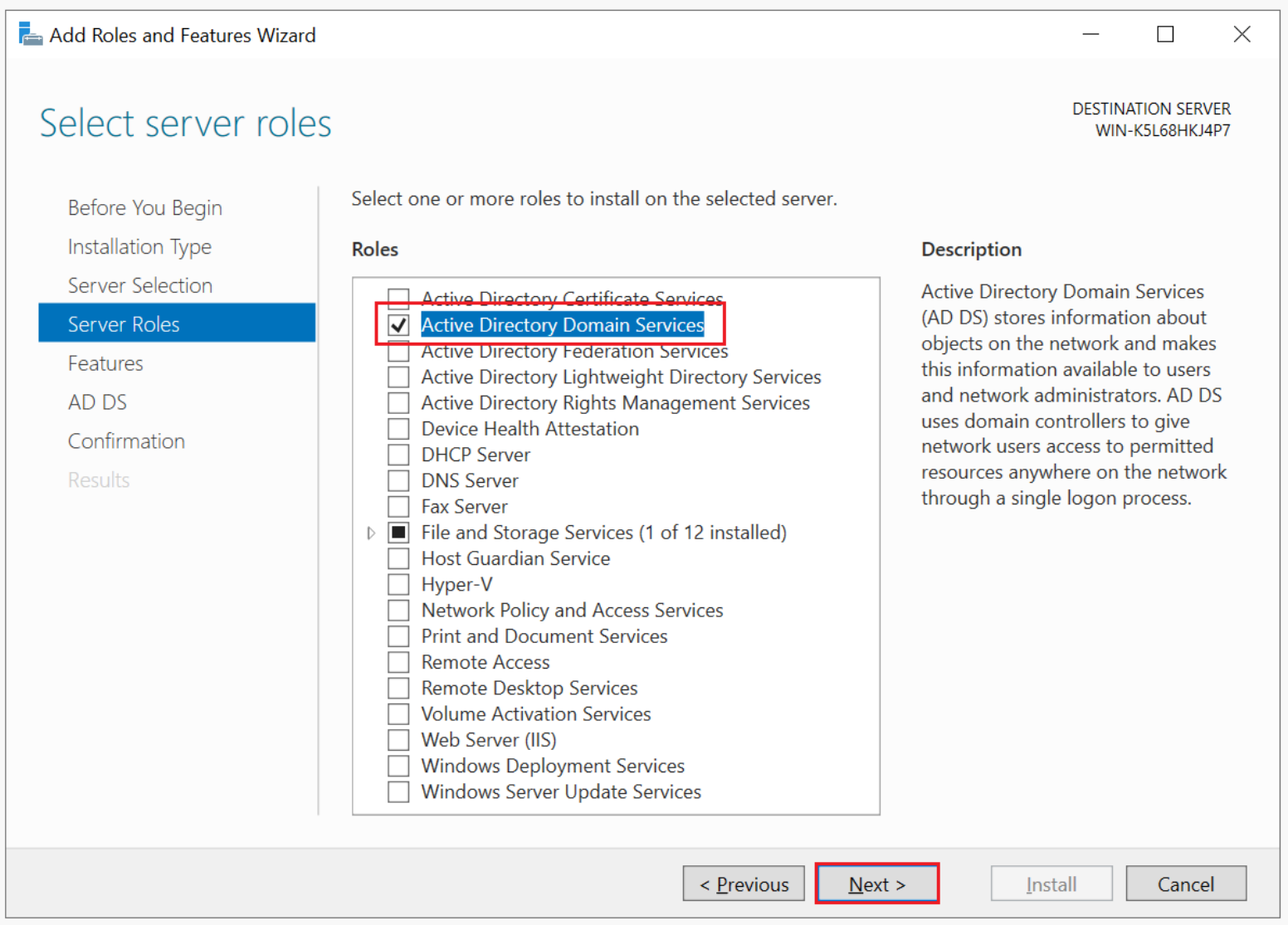
- Role Transfer
  - Verplaatsen van een rol naar een andere DC.
- Role Seizure
  - Failure van een DC die een FSMO role heeft.
  - “Forced, ungraceful transfer”.
  - Enkel doen indien je zeker weet dat de DC niet terug in gebruik genomen wordt.

# Operations Masters

- Waar zijn ze te vinden?

| FSMO Rol | MMC Module |
|---|---|
| Schema master | Active Directory Schema (regsvr32 schmmgmt.dll) |
| Domain naming master | Active Directory Domains and Trusts |
| Relative identifier master | Active Directory Users and Computers |
| PDC emulator | Active Directory Users and Computers |
| Infrastructure master | Active Directory Users and Computers |

# Installatie






erasmus HOGESCHOOL BRUSSEL

# Installatie: Decision Tree