

# Server Administration

## Directory Systemen



# Directory Service

- Software voor het bijhouden, beheren en toegankelijk maken van informatie in een 'Direcotory'
- Bij ons meer concreet:  
gebruiker- en computer accounts, groepen, printers en andere gedeelde bronnen in ons netwerk

Doel: beheren wie wat mag doen op het netwerk

Oplossing:

- Elke server regelt dit zelf voor zichzelf
- Nadelen:
  - Elke gebruiker had gebruikersnaam + wachtwoord per server
  - Moeilijk te beheren door administrators



- Verzameling van standaarden ontworpen door ISO/ITU
- **Model voor protocollen en informatie in een directory service die onafhankelijk is van een applicatie of netwerkplatform**
- Oorspronkelijk uit 1988
- Nadien verschillende aanpassingen/uitbreidingen (=verbeteringen)
- Definieert specificaties voor gedistribueerde directory gebaseerd op hiërarchie
- Men noemt het geheel een **DIT** (Directory Information Tree)



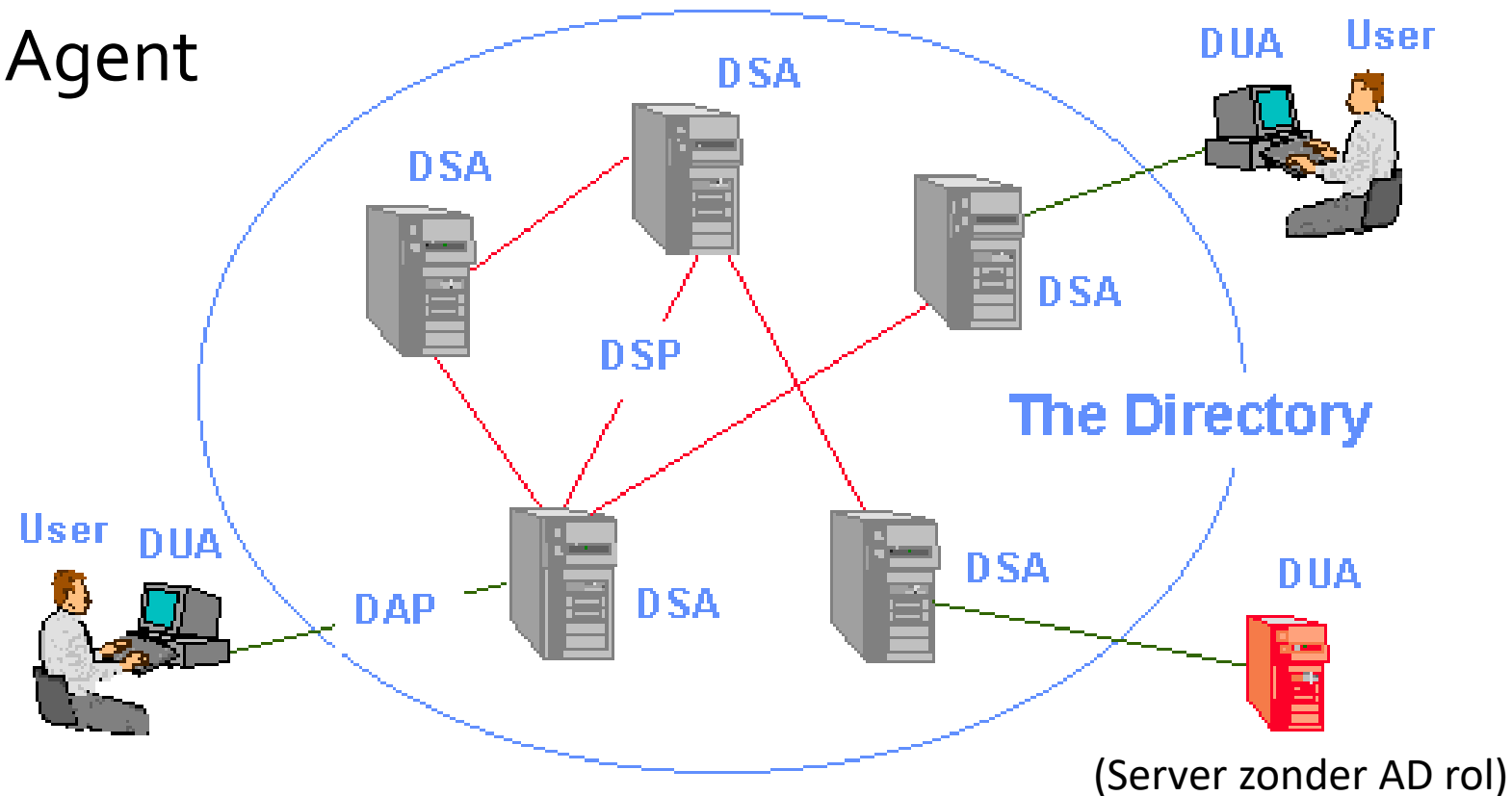
- Gebruikt model voor Directory Server Agents (DSA's)
- DSA's bewaren elk een stuk van de "Directory Information Base" (DIB)
- DSA's werken samen => transparantie voor gebruikers
- X.500 bepaalt:
  - **Hoe** informatie opgeslagen wordt in DS
  - De nodige **protocollen** om data op te vragen (door de clients)
- In X.500 1988 vooral aandacht voor protocollen voor gedistribueerde DS

2 belangrijke protocollen:

- **DAP** (Directory Access Protocol): laat toe dat gebruikers en applicaties **de DS** kunnen **bevragen**
- **DSP** (Directory Service Protocol): zorgt voor **doorgeven** van **aanvragen** aan andere DSA's (indien geen antwoord gevonden wordt op de lokal DSA)

# DSA en DUA

- DSA = Directory Server Agent
- DUA = Directory User Agent





## Lightweight Directory Access Protocol

- Is een standaard gepubliceerd door IETF (Internet Engineering Task Force)
- LDAP v2 en v3
- Is een open standaard voor DS
- Ideaal voor client-applications en (web)-servers vanwege LDAP over TCP/IP
- Bedoeling: **clients in DS laten zoeken**
- Gemaakt voor DS, gebaseerd op X.500
- Is dus zéér aantrekkelijk alternatief voor DAP



# LDAP

- Communicatie tussen clients en servers
- Vraag gestuurd vanuit de clients (server kan antwoorden)
- Geen exacte mapping met DAP
- Mogelijke operaties: zoeken, wijzigen, toevoegen, verwijderen, ...
- Uitbreidbaar
- Authenticatie

# Vergelijking AD met databank

<i><b>User ID</b></i>	<i><b>Logon</b></i>	<i><b>First Name</b></i>	<i><b>Last Name</b></i>	<i><b>Domain</b></i>
S-2882-234-23	WILL	Mark	Willems	Odisee
S-2322-321-99	BEKA	Joke	Bekaert	Odisee
S-2332-233-23	ROTT	Koert	Rottiers	Odisee

- Primary key: User-id, een intern nummer voor het systeem om gebruikers te identificeren voor beveiligingsdoeleinden. (GUID's) = Globally Unique Identifiers
- Naast GUID worden logon, voornaam, familienaam en domein gebruikt om de entiteit (*hier persoon*) te beschrijven. Lijst=tabel en kolommen=attributen
- In Active Directory definieert dit een klasse van een object
- Eerst worden attributen aangemaakt, daarna klassen op basis van beschikbare attributen
- Naast een klasse voor gebruikers kunnen ook klassen aangemaakt worden voor printers, mappen, etc...

# Schema

- Definieert de **inhoud** van de Directory Service
  - Alle object **klassen**
  - Alle mogelijke **attributen** die objecten kunnen en/of moeten bevatten
- Definieert de **structuur** van de Directory Service

# Schema elementen en termen

- **Attribuut:** Soort gegeven gebruikt om objecten (die instanties zijn van klassen) te beschrijven
- **Klasse:** Definieert een soort object en zijn attributen
- **Object:** Een data item in de Directory Service met een unieke Object Identifier (OID)
- **DIT - Directory Information Tree:** De inhoud van de Directory met zijn boomstructuur

# Attributen

Eigenschappen van een klasse

Aan een klasse definitie kunnen we altijd een attribuut toevoegen

- Op die manier kunnen we de DS naar wens aanpassen
- Bv: een “nieuw veld” met het aantal afgedrukte pagina’s van een gebruiker binnen het bedrijf.

→ Active Directory = “Extensible Architecture”

# Klassen

Voorbeelden: Gebruiker, Print-wachtrij, Groep

3 soorten klassen

- Structural Classes
  - Enkel hiervan kunnen objecten gemaakt worden
- Abstract Classes
  - Template voor andere klassen (overerving)
- Auxiliary Classes
  - Wordt toegevoegd aan een andere klasse om attributen toe te voegen

# Global Catalog

Een globale lijst met (bepaalde) **gegevens** van **elk object** van **elk domein** in het Active Directory Domain Services forest

- Wordt bijgehouden op Global Catalog Domain Controllers
- Ieder domein binnen de “*enterprise*” zal exact hetzelfde ***schema*** hebben (replicatie)
- Wordt beheerd door de ***Schema Master***  
(**één enkele server** bevat write-enabled kopie van het **Directory Schema**)
- De eerste domein controller is altijd een Global Catalog server
- DNS bevat gegevens van de Global Catalog servers

# Global Catalog

Alle attributen bijhouden van alle domeinen op alle servers is onmogelijk (miljoenen)...

Oplossing:

- We markeren welke attributen we wensen door te geven aan de andere domeinen (gegevens die frequent opgevraagd worden)
- Deze worden gekopieerd naar de Global Catalog(s) van ieder domein
- Je kan dus zelf bepalen hoeveel data er tussen de domeinen getransporteerd wordt



# Meerdere domeinen

**single-domein** structuur werkt voor **kleine bedrijven**

problemen stellen zich bij **grotere bedrijven, meerdere domeinen**

(Servers moesten gebruikers authenticeren op andere domeincontrollers via trust relation ships)

- Eerste oplossing: DS vergroten zodat **1 domein volstaat**. (bij overgang van NT naar win2k is dit het geval, van ca 1000 naar ca 1 miljoen) (SAM: ca 40MB, Active Directory: 70TB)
- Maar nood voor verschillende gescheiden domeinen blijft (domein is beveiligings- en replicatiegrens)

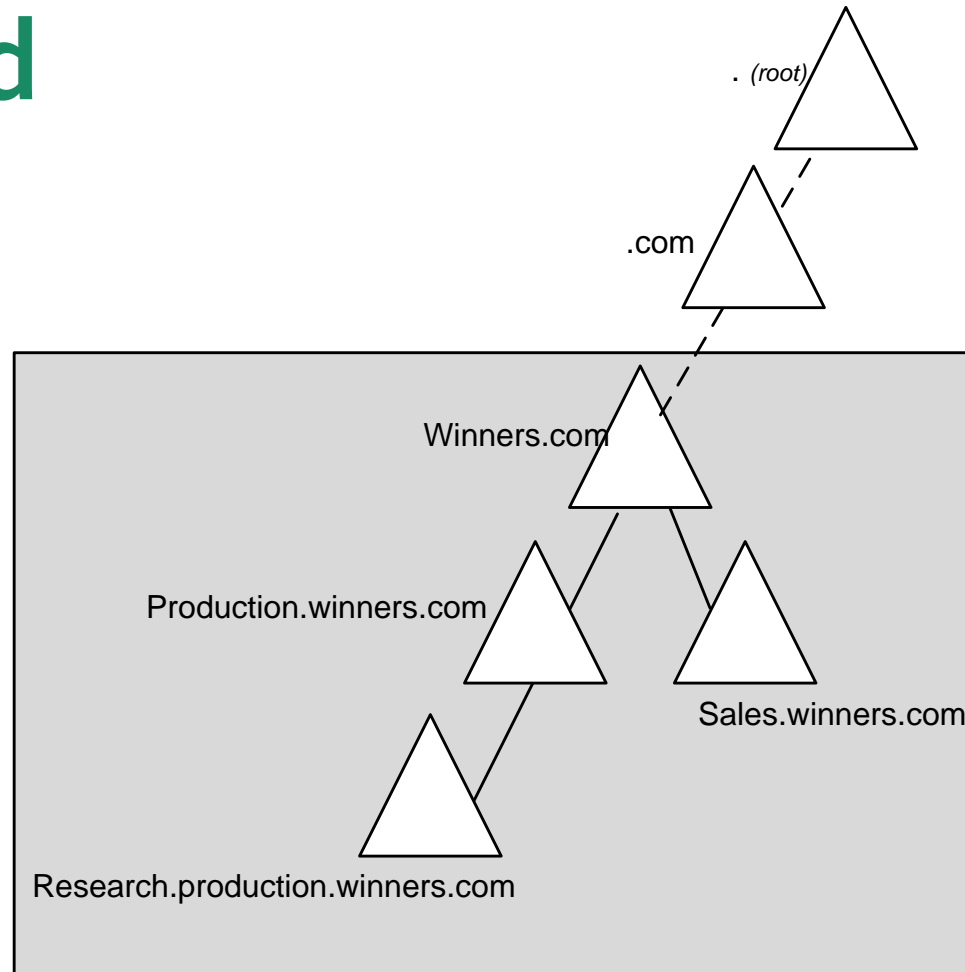
OPLOSSING:

- We zorgen voor een structuur in de Directory Service
- Maakt het makkelijk om objecten terug te vinden in de volledige organisatie + makkelijkere replicatie
- Gerealiseerd op basis van **DNS !!!!**

# Meerdere domeinen

- DNS aanziet het volledige internet als een contiguous namespace
- Startpunt: root-domein
- Wordt verder opgesplitst in top-level en second-level domeinen (enz...)
- DNS zorgt voor hiërarchische bevraging
- DNS-structuur wordt gebruikt om de verschillende domeinen in het bedrijf aan elkaar te koppelen (trusts)
- Adhv een distinguished naam kan dan makkelijk gebruik gemaakt worden van eender welk object in de organisatie.
- Vanwege de structuur kunnen we nu makkelijk de vertrouwensrelaties beheren (de “**domain naming master**” is verantwoordelijk en controleert iedere server op correcte namespace volgens DNS bij het koppelen)

# Voorbeeld



Directory van het bedrijf Winners  
Hiërarchisch opgebouwd volgens de DNS structuur



# Active Directory Objecten

Bepaalde objecten in Active Directory liggen voor de hand:

- Gebruikers
- Computers
- Groepen

Andere niet:

- Organisational Units
- Sites
- Shares
- ....

# Objecten

Alles ( bestanden, mappen, gebruikers, printers, Active Directory onderdelen,...) kan eigenlijk aanzien worden als een object

- Maakt het eenvoudig voor het besturingssysteem om beveiliging te voorzien want 'alles' wordt op eenzelfde manier bekeken
- Objecten kunnen we bekijken als containers:  
een object bevat altijd iets
  - Bestand bevat data
  - Groep bevat andere gebruikers
  - Printers bevatten een plaats in de AD
  - Gebruikers bevatten een plaats in de AD

} Leaf objects

# DACL

Discretionary Access Control List (ook afgekort als ACL)

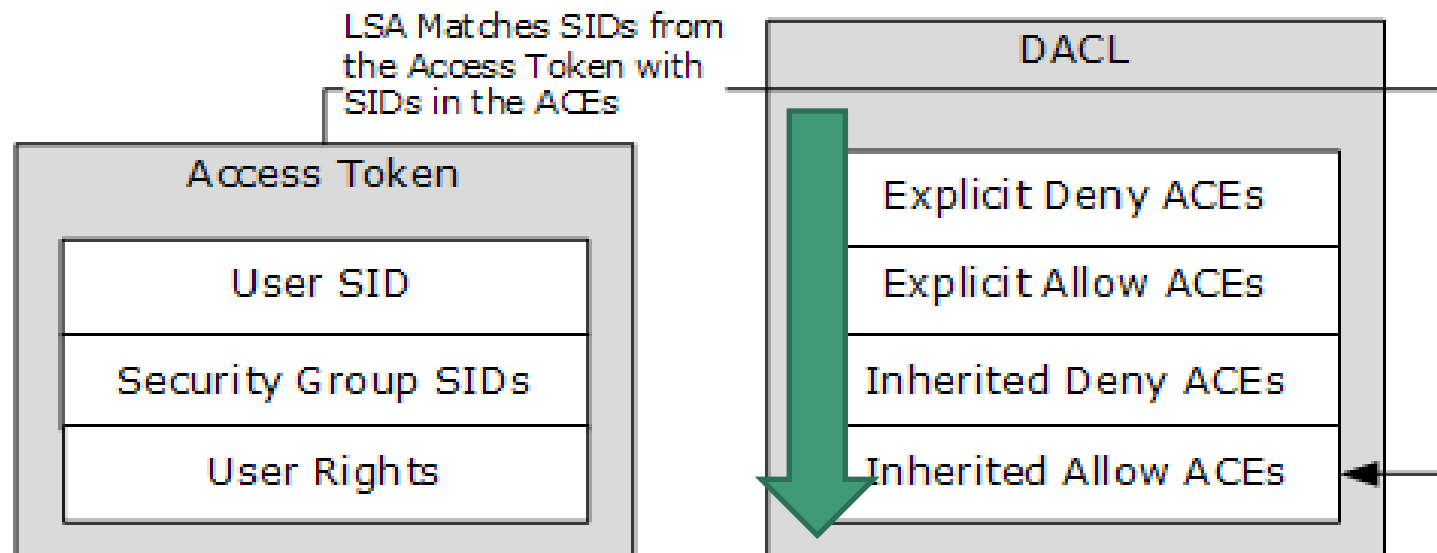
- Een sterk en toch simpel beveiligingsmodel
- Van toepassing op alle objecten:
  - Methoden: aanmaken, verwijderen, ...
  - Eigenschappen: min. een naam en een type
  - Collections: indien eigenschap of attribuut meerdere waarden bevat.
- OS benadert alles op dezelfde manier en alles heeft een DACL => beveiligingsreferentiemodel

# DACL en ACE

- DACL is lijst van Access Control Entries (ACEs)
- ACE = <account,toegangsrechten> paar
- ACE = Access Control Entry
- Maar DACL is ook meer dan dat
- Toegang toestaan of weigeren

# DACL

- Gegevens account = Acces Token
- Resource waar je toegang probeert toe te krijgen heeft DACL





Beheer in windows 2003/2008/2012:

3 belangrijke tools om delen van de Active Directory te beheren

- Active Directory Users and Computers
- Active Directory Domains and Trusts
- Active Directory Sites and Services

S1 Properties

?

x

General

Operating System


Member Of

Delegation

Location

Managed By

Dial-in

 S1

Computer name (pre-Windows 2000):

S1

DNS name:

S1.vermeulen.eu

DC Type:

Global Catalog

Site:

TCG

Description:

# Logische structuur AD

- Active Directory is gestoeld op X.500/LDAP en bepaalt hoe info intern in directory opgeslagen en aangesproken wordt
- “Daarboven” kan een eigen logische structuur gelegd worden om een volledige “enterprise” te beheren
- Dit zorgt ervoor dat AD gestructureerd en makkelijk implementeerbaar is voor grote en kleine bedrijven
- In tegenstelling tot vroegere versies van Windows die NETBIOS gebruiken om computers te vinden, is Active Directory volledig geïntegreerd met DNS en TCP/IP

**Een Active Directory-omgeving moet dus voorzien zijn van een DNS-server en deze moet de speciale SRV-records ondersteunen.**

# Domeinen

Is een basiseenheid binnen AD

Geeft je volgende voordelen:

- Domein geeft mogelijkheid om objecten te beheren binnen departement of locatie. Daarbinnen is dus alle info beschikbaar
- Domeinen bepalen beveiligingsgrens => groep beheerders heeft volledige controle over alle bronnen binnen het domein
- Eventueel groepsbeleid (zie later) op domeinniveau

# Domeinen

- Domeinobjecten kunnen beschikbaar gemaakt worden naar andere domeinen toe (publiceren in Active Directory)
  - Domeinnamen volgens DNS-structuur => laat oneindig aantal child-domeinen toe
  - Domeinen zorgen dat je replicatie kan beheersen (replicatiegrens)
- 
- Binnen het domein moet altijd **minstens één domeincontroller** staan
  - Het eerste domein dat opgezet wordt in een enterprise is het “**ROOT-domein**”. Deze server zal bijgevolg standaard alle FSMO-rollen op zich nemen (FSMO: Zie later)

# Domain functional Level:

Is een manier die aangeeft welke functionaliteiten beschikbaar zijn afhankelijk van de soorten domein controllers die moeten samenwerken in datzelfde domein

- Windows 2000 mixed (default): DC's= NT,2000 ,3,8(R2),12(R2)
- Windows 2000 native: DC's = 2000,3,8(R2),12(R2)
- Windows 2003 interim: DC's = NT en 2003
- Windows server 2003: DC's = 2003,2008(R2),2012 (R2)
- Windows server 2008 DC's = 2008(R2), 2012 (R2)
- Windows server 2008R2 DC's = 2008 R2, 2012 (R2)
- Windows server 2012 DC's = 2012 (R2)
- Windows server DC's = 2012 R2

Hoe meer eenheid in de soorten DC's, hoe meer (nieuwe) functionaliteiten

# Trees en Forests

- In domein zitten o.a. gebruikers en computers
- Om verschillende domeinen samen te nemen, organiseren we ze volgens een logische structuur:  
(DNS-structuur)
  - Domein-tree
  - Domein-forest

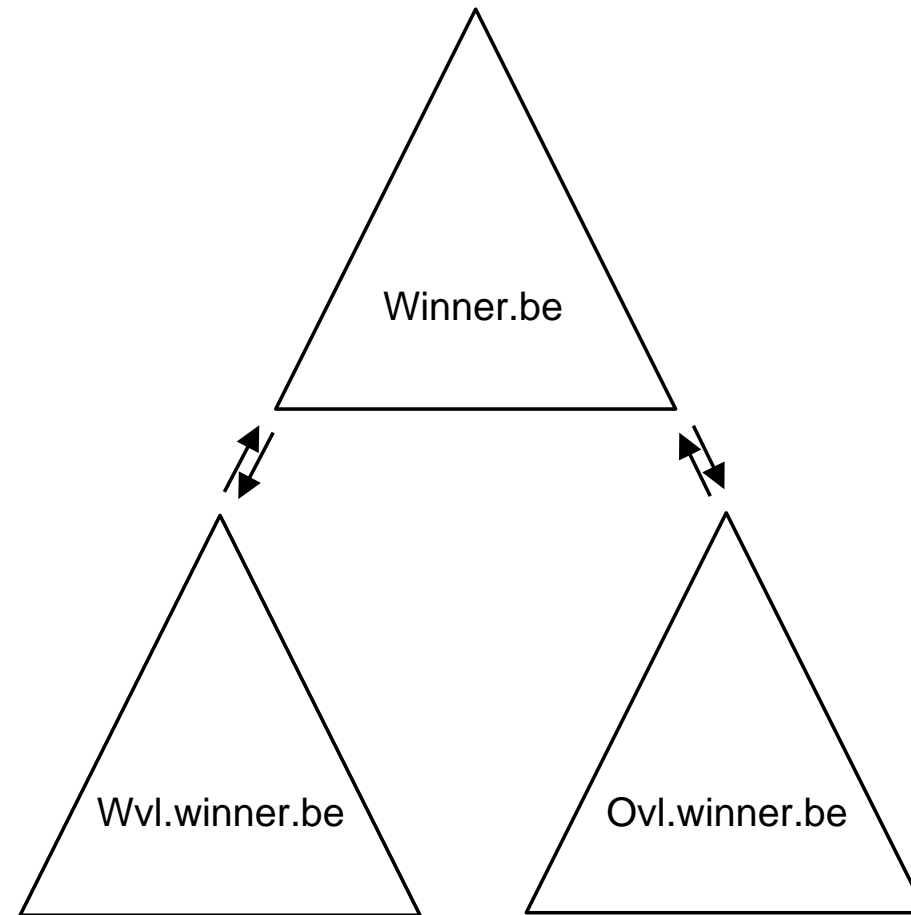
# Tree

Mogelijkheid: 1 domein met alle objecten erin

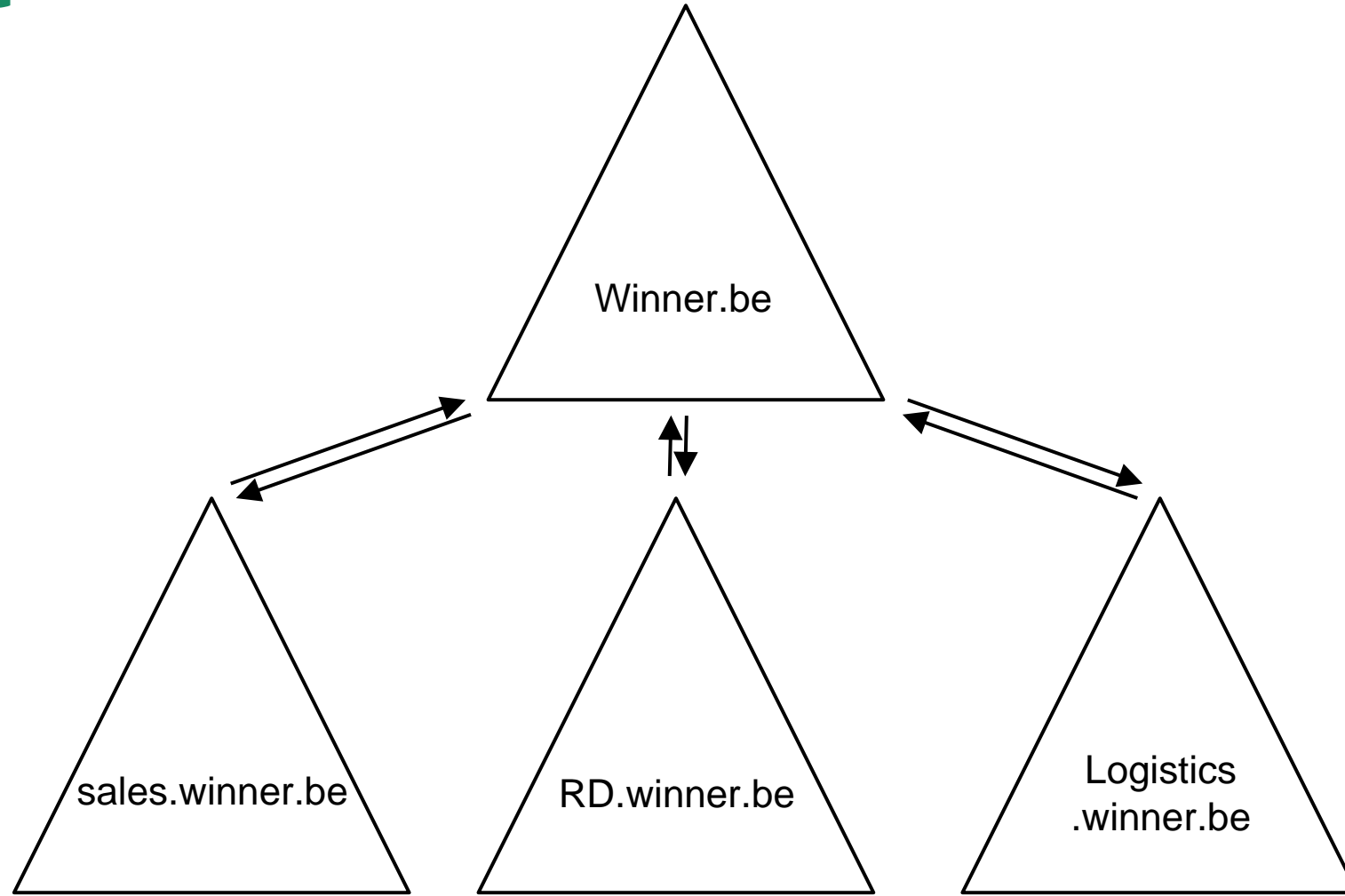
- Niet interessant indien verschillende afdelingen geografisch verspreid en onafhankelijkheid gewenst is
- In dat geval bv gescheiden domeinen (geografisch) als oplossing  
Hier is top-domein een pointer naar de verschillende sub-domeinen (*vb*)
- Eventueel splitsing volgens functies  
Hier zal de administratie en de support zich in het top-domein bevinden (*vb*)
- In beide gevallen: Alle domeinen **eenzelfde schema** en **eenzelfde GC** (in elk domein min 1 GC). Tussen de domeinen ligt een **transitieve tweewegs-relatie**
- We maken dus een tree vanaf het root-domein
- De onderliggende domeinen zijn child-domeinen



# Een eenvoudige domeinstructuur gesplitst in sub-domeinen volgens geografische ligging



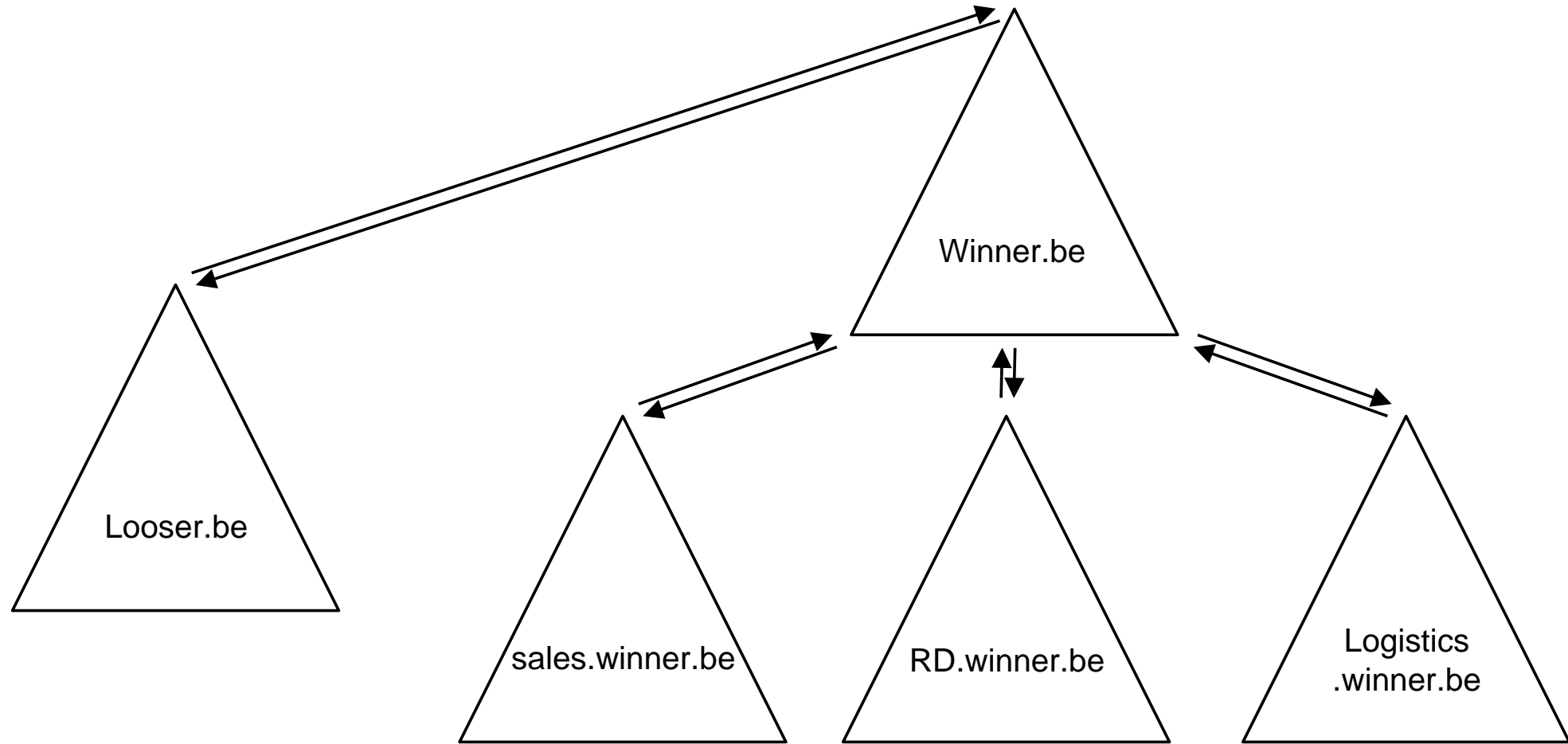
# Domein opgesplitst in subdomeinen volgens functie



# Forest

- In bepaalde gevallen is één tree geen goede oplossing
- Bv verschillende afdelingen met totaal verschillende benamingen en de AD-structuur moet bedrijfsstructuur weerspiegelen
- In dit geval: meerdere trees samennemen (*vb*)
- **Zelfde schema, zelfde GC** en configuratie blijft belangrijk
- Eén domein zal root-domein zijn, alle andere child-domeinen
- De structuur bestaat uit meerdere trees → forest
- Onder deze trees kunnen weer nieuwe child-domeinen geplaatst worden

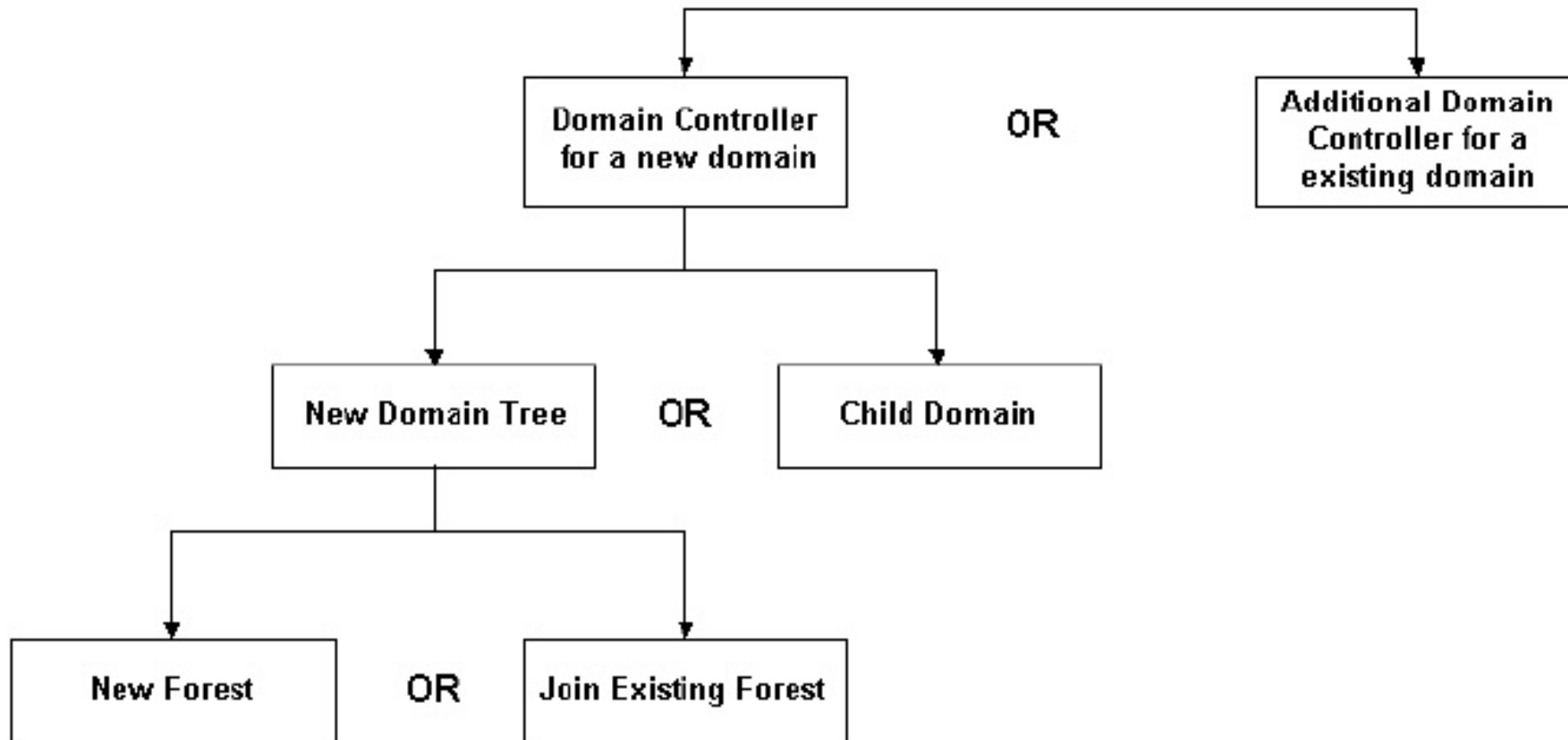
# Forest-structuur (vb 2 trees)



# Opzetten DC

- Na het opzetten van de eerste domeincontroller voor het eerste domein kunnen nieuwe servers gepromoveerd worden tot domeincontroller
- Hun functie wordt bepaald tijdens deze promovering ==>
  - Nieuwe domeincontroller in bestaand domein
  - Nieuwe domeincontroller voor child-domein
  - Nieuwe root-domeincontroller voor een nieuwe tree in een forest

# Beslissingsboom nieuwe domeincontroller



# Niveaus

- Combinatie van trees en forests geeft je bedrijf grote flexibiliteit in ontwerp van AD
- Domeinen bepalen eerste niveau van structuur in de Active Directory
- Een volgend niveau is dat van Organisational Units (OU)

# Trust relaties

Trust relaties	Definitie
One-way trust	Authenticatiebevoegdheid van het ene domein wordt door een ander domein erkend, maar niet vice-versa. Domein A zal bijvoorbeeld domein B vertrouwen, maar domein B vertrouwt domein A niet.
Two-way trust	Authenticatiebevoegdheid tussen 2 domeinen wordt wederzijds erkend. Domein A vertrouwt domein B en B vertrouwt A.
Transitive trust	Authenticatiebevoegdheid kan impliciet worden overgeërfd tussen domeinen. Zo zal wanneer A B vertrouwt en B vertrouwt C, A ook C vertrouwen.
Two-way transitive trust	Authenticatiebevoegdheid wordt in 2 richtingen overgeërfd. A vertrouwt B en alle domeinen die B vertrouwt en B vertrouwt A en alle domeinen die A vertrouwt.
Inter-forest trust	Een trustrelatie tussen verschillende forests.



# Forest functional Level

Is een manier die aangeeft welke functionaliteiten beschikbaar zijn afhankelijk van de soorten domein controllers die moeten samenwerken in eenzelfde forest

- *Windows 2000 native:* *DC's = 2000,3,8(R2)*
  - *Windows server 2003:* *DC's = 2003,2008(R2),2012 (R2)*
  - *Windows server 2008:* *DC's = 2008(R2), 2012 (R2)*
  - *Windows server 2008R2:* *DC's= 2008 R2, 2012 (R2)*
  - *Windows server 2012:* *DC's= 2012 (R2)*
  - *Windows server 2012 R2:* *DC's= 2012 R2*
- Hoe meer eenheid in de soorten DC's binnen de forest, hoe meer functionaliteiten binnen die forest
  - Windows Server 2012 vereist een Windows Server 2003-forestfunctionaliteitsniveau

# Organisational Units

- OU's bepalen tweede niveau in de hiërarchie
- Met OU kan je een domein verder opdelen in logische eenheden
- OU is een container waarin gebruikers, computers en andere objecten kunnen zitten
- Met OU's is het mogelijk om bevoegdheden te delegeren naar bepaalde gebruikers of groepen. De gedelegeerde gebruikers kunnen volledig of gedeeltelijk de objecten beheren.
- OU's kunnen gebruikt worden om groepsbeleid op toe te passen.
- Binnen OU's kunnen andere OU's geplaatst worden

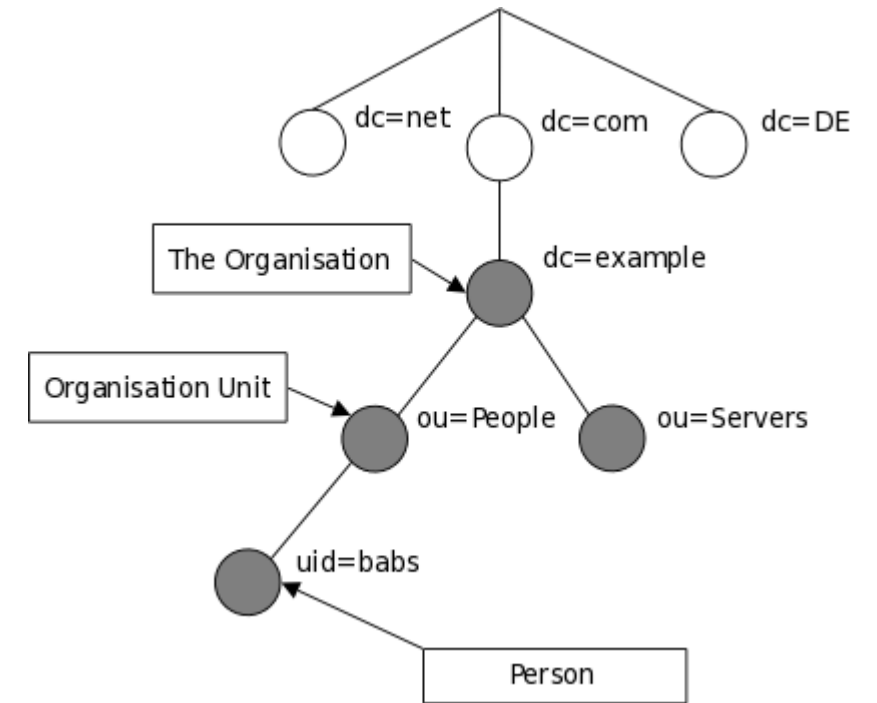
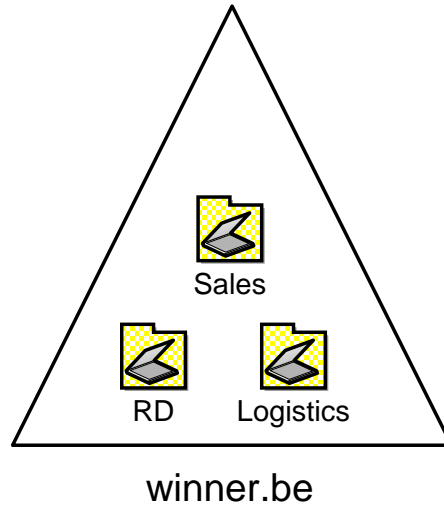
# Structuur

Er zijn dus twee mogelijkheden om gebruikers, computers en andere objecten te beheren in een gestructureerde omgeving:

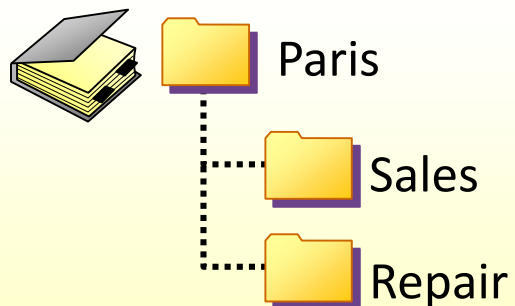
- Adhv domeinen opsplitsen (trees, forests)
- Door domein op te delen adhv OU's

# Domein met structuur adhv Organisational Units

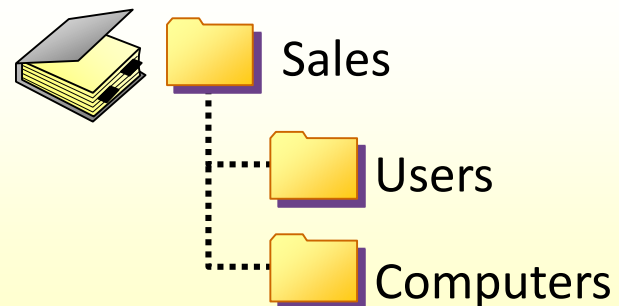
(4 vb-en)



## Organizational structure



## Network administrative model



# Keuzeregels

Wanneer splits je op in domeinen en wanneer gebruik je OU's

- Gebruik **opdeling adhv domeinen** indien bronnen moeten kunnen beheerd worden door **compleet verschillende administrators**. Administrators wensen dus volledig onafhankelijk te werken van elkaar
- Gebruik **aparte domeinen** bij netwerken waarbij delen ervan **gekoppeld zijn met trage verbindingen** (kan ook adhv sites)
- Gebruik **OU's** om de **interne structuur** van je organisatie te implementeren tot op micro-niveau (bv lokalen, doelgroepen,...)
- Gebruik **OU's** indien je **beheersrechten** wil **delegeren** naar bepaalde gebruikers, groepen
- Gebruik **OU's** als je weet dat je organisatie zal **wijzigen** in de **nabije toekomst** (fusionering van afdelingen, nieuwe afdelingen,...)

Algemeen: in de meeste gevallen zal een single domein volstaan met daarin een opdeling adhv OU's. Dit houdt het beheer overzichtelijk!

# Installatie van eerste domein

Vereisten:

- Geïnstalleerde Windows 2012 R2 server
- Correct functionerende DNS-server met forward-lookup zone. Moet "Service"-records (SRV) ondersteunen en moet in staat zijn om dynamische updates toe te laten en incrementele zone transfers (kan ook samen met AD geïnstalleerd worden)
- De toekomstige domeincontroller moet een vast ip-adres krijgen. Vaste computernaam. Correcte dns-instellingen bij TCP/IP settings
- NTFS-partitie min 1GB
- Correcte tijd en tijdszone (DC zal functioneren als ntp-server voor de clients)

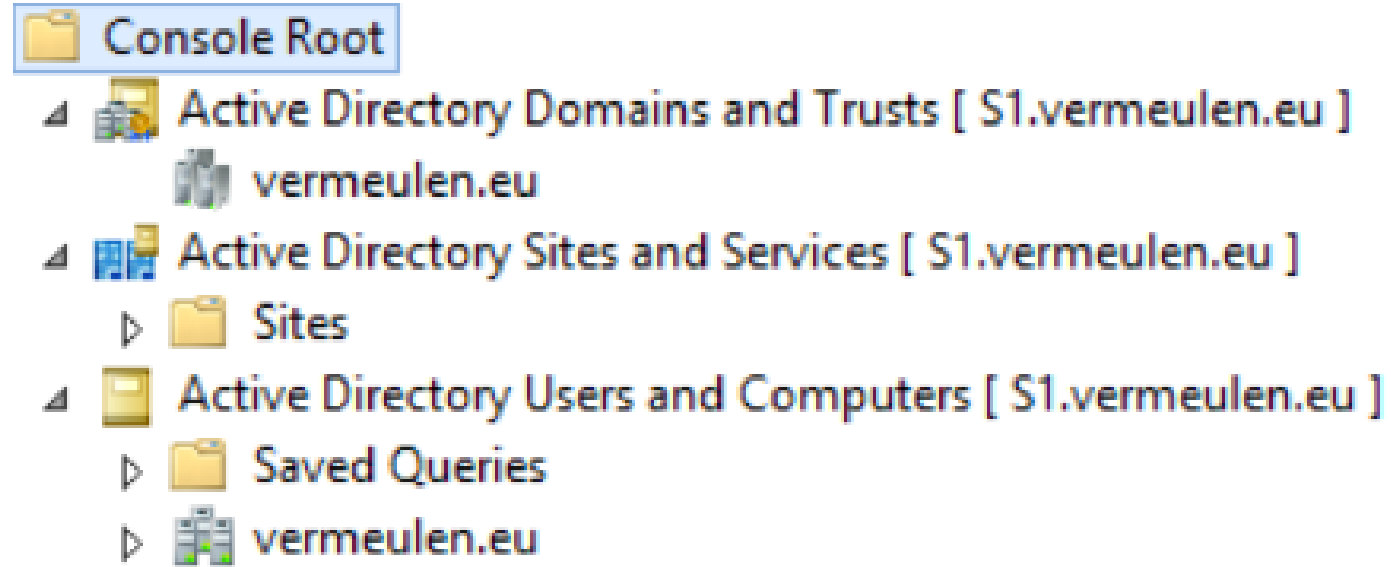
# Naam van het domein

Verschillende mogelijkheden:

- De echte internet domeinnaam: => interne en externe entiteiten zijn dezelfde. Praktisch maar risicovol (Active Directory bereikbaar door publiek netwerk indien niet beveiligd, via DNS zijn alle records te bevragen)  
vb: winner.be
- Een subdomein onder internet domeinnaam: vb AD.winner.be => maakt splitsing tussen intern en extern makkelijker <=> naamschema complexer
- Totaal andere interne naam: voorbeeld .local gebruiken (niet geregistreerd op internet) vb winner.local  
Dit garandeert veiligheid door scheiding van "echte" DNS-structuur (internet). Levert andere nadelen op...

# Installatie

Na de installatie (zie verder) is de server omgevormd tot een domeincontroller die (eventueel een deel van) de Active Directory bevat.



- **Active Directory Users en Computers:** om gebruikers, groepen, computers en OU's te beheren (ook Grouppolicies)
- **Active Directory Domains en Trusts:** om de verschillende domeinen onderling te beheren en vertrouwensrelaties in te stellen.
- **Active Directory Sites en Services:** om replicatie tussen de sites in te stellen en services (vb schema master, GC,...) die werken op de verschillende domeinen en hun controllers.



# Integratie met andere systemen

Integratie met op Unix gebaseerde systemen (Unix, Linux, Mac OS X or Java and Unix-based programs) is onder andere mogelijk met LDAP

Third party systemen:

- Fox Technologies and the product **FoxT ServerControl** (software) implements AD Bridging capabilities that allows Unix-like systems to join Active Directory and enables the use of the Kerberos for authentication of users
- **Centrify DirectControl** (Centrify) – Active Directory-compatible centralized authentication and access control
- **Centrify Express** (Centrify) – A suite of free Active Directory-compliant services for centralized authentication, monitoring, file-sharing and remote access
- **UNAB** (Computer Associates)
- **TrustBroker** (CyberSafe Limited) – An implementation of Kerberos
- **PowerBroker Identity Services**, formerly Likewise (BeyondTrust, formerly Likewise Software) – Allows a non-Windows client to join Active Directory
- **Quest Authentication Services** (Now part of Dell) (Formerly, Quest, Vintela) - AD authentication, Group Policy management, User/Group Migration tools, Auditing and Reporting
- **ADmitMac** (Thursby Software Systems)
- **Samba** – Can act as a domain controller

# Andere Directory systemen

- NIS: Network Information Service afkomstig van SUN/UNIX
- eDirectory: Novell
- Red Hat Directory Service
- Open Directory: Mac OS X Server
- OpenLDAP
- ...

# Bronnen

- LDAP - <https://tools.ietf.org/rfc/rfc4511.txt> (Inleiding)
- Global Catalog - [https://technet.microsoft.com/en-us/library/cc728188\(WS.10\).aspx](https://technet.microsoft.com/en-us/library/cc728188(WS.10).aspx)
- Active Directory - [https://en.wikipedia.org/wiki/Active\\_Directory](https://en.wikipedia.org/wiki/Active_Directory)
- DACL - <https://msdn.microsoft.com/en-us/library/cc246052.aspx>
- Functional Levels - [https://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(v=ws.10).aspx)
- Active Directory Schema Terminologie - [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)
- Soorten klassen - [https://msdn.microsoft.com/en-us/library/ms677964\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/ms677964(v=vs.85).aspx)