windows 2012

* AD
* domeinnaam
* DNS
* OU met IT,Marketing,Sales
* Elk 2 users, 1 global group, 1 domain local group

Client: Windows 8

* toegevoegd aan het domein

30blz / dag

# AD DS: Active Directory Domain Services

AD DS is een netwerk directory services.

Een directory is een database die geoptimaliseerd is om geraadpleegd te worden, m.a.w. de objecten die opgeslagen worden in de database zijn bij voorkeur niet voortdurend onderhevig aan verandering.

Een directory service maakt het mogelijk de gegevens in de database te raadplegen.

AD DS heeft een hierarchische structuur, heeft objecten gemaakt op basis van object klasse die attributen hebben. Elk attribuut heeft een uniek id en een aantal eigenschappen zoals naam en de waarden die het attribuut kan aannamen. Vb Objectklasse: User, object van de klasse User: Louiza, attributen van een object van de klasse User: name, givenName, accountExpires, ...

Het instaleren van AD DS op een server maakt van de server een domeincontroller (DC).

# Forest, tree, domein, organizational unit (OU)

Een AD DS komt overeen met een forest. Een forest kan samengesteld zijn uit 1 of meerdere trees. In een tree vind je 1 of meerdere domeinen. Een domein kan dan nog verder opgedeeld worden in organizational units (OU).

**Forest**

Een AD DS hoort bij 1 forest en omgekeerd.  
Een reden voor meerdere forest is als test netwerk of voor het isoleren van erg gevoelige data.  
In elk forest vindt je minstens 1 domein.

**Trees**

Een tree is een hierarchisch gestructureerde verzameling domeinen in eenzelfde namespace.

De reden voor een 2de tree op te zetten is om een tweede namespace te maken binnen eenzelfde forest.

**Domein**

Elk domein beschikt over een eigen database met gebruikers, computers, enz. Een server waarop deze database bestaat en beheerd wordt, is een domeincontroller.  
Een domein is dus een verzameling resources en gebruikers die centraal kunnen beheerd worden aan de hand van 1 enkele database.  
Elk domein beschikt over minstens 1 domeincontroller en elke domeincontroller hoort maar bij 1 domein.

Het is beter om meerdere domeincontrollers op eenzelfde domein te maken voor fouttolerantie of om de werkdruk te spreiden.  
Een reden voor meerdere domeinen is 2 verschillende personenen die elk een domein beheren, beperking van het replicatieverkeer, beperking verkeer over een trage verbinding, beperking van de grootte van de AD Database.

**Vertrouwensrelaties**

Vertrouwensrelaties zorgen ervoor dat een gebruiker van een domein kan werken met bestanden in een gedeelde map in een ander domein binnen hetzelfde forest.

**Organizational units**

Een domein kan verder onderverdeeld worden in organizational units (OU). Dit is om het beheer van een domein te vergemakelijken.

* Objecten groeperen waarvan het beheer kan gedelegeerd worden
* Structuur brengen in de verzameling objecten van het domein
* Policies die moeten gelden voor bepaalde gebruikers en computers

**Parent vs Child**

Een domein kan uit meerdere children domeinen bestaan. Het parent domein is dan de leider over zijn children maar elk child beheerd zichzelf ook.

**replicatie van AD DS**

De database wordt in 4 partities opgedeeld:

* Schemapartitie: hier wordt de definitie van alle objecten en attributen die kunnen voorkomen in de AD DS samen met de spelregels om die objecten en attributen aan te maken en te manipulereen opgeslagen.
* Configuratiepartitie: hier wordt de logische structuur van het netwerk opgeslagen. (Welke domeinen zijn er en hoe passen die in de structuur)
* Domeinpartitie: hier worden de gegevens van gebruikers, computers, ... die deel uitmaken van het netwerk bijgehouden. Wordt naar alle domeincontrollers binnen een domein gerepliceerd.
* Applicatiepartitie: Applicaties en services maken meestal zelf een applicatiepartitie aan om er hun objecten in op te slaan. Een applicatiepartitie wordt alleen naar welbepaalde domeincontrollers gerepliceerd.

Role: een verzameling software die de server in staat stelt een primaire service aan te bieden op het netwerk.

Feature: ondersteunende functie

**DNS**

DNS is de basis voor de naamgeving van de toestellen. Het weet welk ip adres gekoppeld is aan een webadres.

Elke organisatie draait en onderhoudt haar eigen DNS-server en die beschrijft de machines in haar eigen deel van het intranet.  
Een centrale groep houdt domeinnamen en daarmee samenhangende DNS-servers bij.

Enkele types van DNS-record:

* A-records: verbindt het web adres aan het ip adres
* Cname-records: dit is een alias om verschillende namen te koppelen aan eenzelfde adres, dit wordt gebruikt voor toestellen met verschillende taken vb.: ftp en http => [ftp.whatever.be](ftp://ftp.whatever.be) en http.whatever.be zullen naar dezelfde ip wijzen.

Forward en reverse lookup zone:  
Een forward lookup zone zet namen om in IP adressen, een reverse lookup zonde zet IP adressen om in namen.

Een primary en secondary zone:  
Een primary zone is een zone die de originele records bevat. Een secondary zone bevat een kopie van een al bestaande primary zone. Je kan alleen in een primary zone records updaten. Eeen secondary is read only.

Domain: Forest, tree, child  
DC: Domain controller  
DNS  
DHCP  
NAT  
IIS  
DFS replication  
DFS namespaces, OU  
AGDLP  
Global group, Domain local group  
Roaming, mandator, local; cached, non cached profiles  
Group Policies (GPO)

* Desktop Wallpaper
* Prevent changing desktop background
* Prohibit access to Control Panel and PC settings
* Prevent access to drives from My Computer
* Folder Redirection => Documents
* Logon hour restrictions

DHCP redundant maken: backup server  
DNS redundancy: alternative DNS   
DNS fowarding  
VPN  
security rechten  
webserver  
NTFS  
Share permissions  
Forward en backup lookup zone

In ipconfig /all kan je de dns servers zien waarmee je verbonden bent om deze als forwarders op te geven bij dns.

The major point in having a secondary DNS server is as backup in the event the primary DNS server handling your domain goes down. In this case, your server would be still up, and so without having a backup, nobody could get to your server possibly costing you lots of lost customers (i.e. REAL MONEY).

A secondary DNS server is always up, and ready to serve. It can help balance the load on the network as there are now more than one authoritative place to get your information. Updates are generally performed automatically from the master DNS. Thus it is an exact clone of the master.

Generally a DNS server contains more information than just a single server, it might contain mail routing information, information for many many hosts, mail spam keys, etc. So resilancy and redundancy are of DEFINITE benefit to domain holders.