Samenvatting Server OS Advanced – Windows

# Algemeen

Hyper-V is een virtualisatieplatform dat je besturingssysteem virtualiseert. Een V-Switch is een virtuele switch tussen VM’s en/of fysieke netwerkadapters. Een interne switch kan je aan je VM’s koppelen. Een externe switch kan je aan het netwerkkaart koppelen (ook je interne switch).

# Active Directory

Een AD is een DB die alle gegevens bevat van het domein (incl. users, computers, policies etc.). Samengevat is deze AD voor met klassen en objecten. Elk object is uniek. Objecten kunnen gelinkt worden aan elkaar door policies (Vaste achtergrond, beperkte inloguren, etc.). Policies kunnen gekoppeld worden aan een computer en/of een user.

Active directory koppelt een adres aan een computernaam (Client wordt ingesteld als Client.pxlit.local)

# Tree – Forest

Een tree bevat 1 of meerdere ADDB’s. Elke DB is binnen hetzelfde domein identiek. Een parent domain of root domain is het eerste domain. Dit domain kan meerdere servers bevatten, maar wordt over meerdere servers gerepliceerd (duplicaat). Eén user kan enkel in 1 active directory database zitten. Tree heeft 1 domainnaam en kan daaronder nog andere domeinnamen hebben. Tree heeft een basisdomeinnaam, heeft een AD-DB.

Oplossing van een te volle AD-DB = nieuwe 2de AD-DB aan maken (AD splitsing). = Child-domain maken. vb.: student en docent zijn children en erven over van pxl.be (hoofd AD). Childs kunnen ook nog childs hebben. Voordeel structuur: elk account van eender welke child kan ingelogd worden op eender welke child. (indien geen beperkingen ingesteld). Parent is altijd de baas van zijn children.

Door een extra configuratie tussen beide trees wordt een vertrouwensrelatie gelegd (trust). Eenmaal beide root domains een trust hebben, wordt het een forest.

Om beperkingen te kunnen zetten op gebruikers, hebben we organizational units nodig (OU), in het Nederlands ‘afdelingen’ genoemd.

# Policies

Er zijn 2 soorten policies:

* User policies (user zelf en bij het inloggen van de user)
* Computer policies (computer zelf en is bij het opstarten van de computer)

Policies kunnen gebruikt worden om software updates te regelen, of computernamen toewijzen of dingen herconfigureren. OU bevat users, usergroups en computers (meestal wordt er een OU Users en een OU computers gemaakt). In een groter bedrijf met meerdere departementen is het misschien handig om OU te maken via type van computer (subdivisies Apple, HP etc.).

# AGDLP (Account – Global Groep – Domain Local Groep – Permissions)

AGDLP dient voor bestandsbeheer.

Er zijn 2 soorten groepen:

* Global group -> gebruiken in heel het forest (PXL kan inloggen op UCLL en visa versa)
* Domain local group -> alleen lokaal in het domein beschikbaar (UCLL en PXL kunnen niet bij elkaar inloggen)

Risico van een global group -> overal zichtbaar, kwetsbaar. Accounts steken in global groups, global groups steken in domain local groups en op DLG passen we permissies toe. Distribution group type is gemaakt voor voornamelijk email toepassingen.

## Fileserver

Een fileserver is een folder die toegankelijk is voor users via het netwerk. De fileserver is meestal beveiligd en enkel toegankelijk voor specifieke gebruikersgroepen.

Standaard zal een fileserver volledig toegankelijk zijn via de share, maar is de permissie beperkt via het tabblad “beveiliging” (security). Security geldt lokaal altijd. Sharing geldt alleen via het netwerk.

ROOT MAP ALTIJD BEVEILIGEN!

# Policies

Policies zijn beperkingen op user of computer niveau. Policies gelden op OU’s maar ENKEL op users of computers, niet op groepen. Policies zijn afhankelijk van besturingssysteem.

User policies:

* Worden uitgevoerd na het aanloggen van de user
* Beperkingen op user niveau
* Login en loguit script behoren altijd tot user niveau
* Beperking geldt op elk toestel waar de user aanmeld

Computer policies:

* Uitgevoerd tijdens opstarten van de computer
* Blijven gelden bij elke user die aanmeld op dezelfde pc
* Beperking geldt enkel op dat toestel maar voor alle user die daar op aanloggen

## Groepsbeleidbeheer (Policy Manager)

Policy op user niveau of computer niveau.  
Elke afzonderlijke OU kan worden één of meerdere policies hebben.  
Policies staan onder map groepsbeleidsopjecten (policy objects).  
Bestaande policies link je vanuit een OU naar de policy objects.  
Starter policies zijn policies die letterlijk gekopieerd worden van waaruit je verder kan werken.  
Beperk 1 policy tot 1 functionaliteit  
Policies worden overgeërfd m.a.w. plaats een policy op één OU en deze geldt voor alle OU’s binnen deze OU (dus ook voor alle users/computers die daarin zitten).  
Policies kunnen geblokkeerd worden per OU -> blokkeert alle policies voor die OU

gpupdate /force om alle policies te verversen! Voor computer policies moet je REBOOTEN!

## Folder Redirection

Dit is het wijzigen van het pad van de basisprofielmappen van de gebruiker. Dit wordt meestal verplaatst naar een netwerkshare (centrale opslag). Dit heeft als voordeel dat de bestanden van de gebruiker ook op andere computers beschikbaar zijn. Deze bron wordt bij de gebruiker gecasht dus is ook offline nog beschikbaar.

## Profielen

### Local Profile

Een lokaal profiel is het standaard profiel bij elke nieuwe gebruiker. Dit profiel bevindt zich lokaal op elke computer. Gegevens blijven op 1 profiel aanwezig op elk apart toestel. Een nadeel is dat het moeilijk te back-uppen is indien er veel informatie op de computer staat.

### Roaming Profile

Een zwervend profiel is een profiel dat centraal opgeslagen is op de netwerkshare. Gebruikers halen hun profiel van de netwerkshare bij het inloggen. Gebruikers synchroniseren hun gegevens naar de netwerkshare bij het uitloggen.

Cached roaming profile: het profiel blijft behouden op het toestel na het uitloggen. Bij het opnieuw inloggen worden enkel wijzigingen binnen gehaald. Gebruiker kan nog inloggen als de server niet online is. Nadien worden bestanden bij het terug aanloggen op het domein terug gesynchroniseerd. Een nadeel is dat de bestanden aanwezig blijven: veiligheidsrisico en na een tijd is veel schijfruimte bezet.

Non-cached roaming profile is een profiel dat na het uitloggen wordt gewist van de lokale computer. Bij het inloggen moet telkens het hele profiel terug gedownload worden. Een nadeel is veel bandbreedte en de gebruiker kan niet meer inloggen als de server offline is. DIT IS EEN COMPUTER POLICY!

### Mandatory Profile

Een verplicht profiel is een non-cached roaming profile met uitzondering dat de wijzigingen nooit gesynchroniseerd worden met de server. Bij het inloggen krijgt de gebruiker telkens hetzelfde profiel te zien.

Verplichte profielen vereisen enkele extra aanpassingen aan een bestaand profiel (ntuser.dat -> ntuser.man, rechten van een default profiel gebruiken, elk Windows besturingssysteem heeft zijn eigen mandatory profile nodig (.V2, .v4; .v5; .V6).

# DNS

DNS wordt gebruikt voor het oplossen van Fully Qualified Domain Names (FQDN).

Een FQDN is een domein met extensie en een prefix. Elke computer heeft als FQDN zijn computernaam+domeinnaam+extensie. Bv Client1.PXLIT.LOCAL Zonder configuratie kan de lokale DNS enkel eigen URL’s en FQDN oplossen. Een URL is een FQDN. (prefix = www, blackboard, mail), (domain = pxl.be, google.be)

ALLE communicatie binnen een domein verloopt altijd via DNS! Indien DNS niet werkt of het toestel de DNS server niet kan contacteren kan geen enkele communicatie worden uitgevoerd.

DNS is unicast. (Vroeger was het broadcast = depracated) Voordeel DNS: minder webverkeer (lokaal) Op een client MOET het DNS IP ingesteld zijn. Op een client mag nooit het DNS IP van de ISP ingesteld zijn. ALLEEN BIJ DE DNS DOMAIN CONTROLLER (forwarding).

Origineel was DNS ontwikkeld om email op het ARPANET te ondersteunen. Nu voorziet DNS het hele internet van name resolution. DNS is gebaseerd op een hosts bestand (IP RFC 226). Dit was inefficiënt omdat men meerdere kopies moest maken. Daarna kwam gecentraliseerd management (hosts bestand downloaden). Daarna kwam DNS zoals we het nu kennen. De database is publiek, er is geen login voor nodig.

DNS.be is een vzw die in België verantwoordelijk is voor dns. Via een DNS agent huur/koop je een domeinnaam voor een periode van standaard 1 jaar. Je krijgt dan het recht deze domeinnaam te laten verwijzen naar de nameservers van jou keuze.

## Autoriteit

Autoriteit is wanneer men van een zone de volledige controle heeft. Dit betekent inclusief alle sub zones met alle sub domeinen en hostnamen.

Elk land heeft een firma die het sub domein van dat land beheert (.be, .com) – zij bepalen welke dns records er komen.

## Delegatie

Het proces waarbij iemand autoriteit krijgt over zijn of haar zone of het bepalen wie de verdere onderverdeling mag gebruiken.

PXL heeft pxl.be als autoriteit en delegeert alle andere sub domeinen onder pxl.be

## Resolving

De resolver gaat namen omzetten naar IP-adressen.

* Resolving begint bovenaan bij . -> root name servers
* Hieruit komt informatie over com -> nam server com
* Hieruit komt informatie over contoso -> name server contoso
* Binnen de contoso zone is er bv een host www  
  -> [www.contoso.com](http://www.contoso.com).

Elke ISP heeft een rechtstreekse connectie met de root-servers. Second-level domain kan ook een dns zijn maar moet niet.

Case: ik wil naar blackboard.pxl.be

* + Stap 1: Telenet vraagt aan de root servers, wat is de dns server van .be (uit 13  
     clusters) (top-level domeinen)  
    Stap 2: Telenet vraagt aan het IP van .be waar .pxl.be is  
    Stap 3: Telenet vraagt aan het IP van .pxl.be waar blackboard.pxl.be is

DNS is ingedeeld in zones en bevat records. Een zone is een afgebakend blok informatie of een authority. Via delegatie kunnen sub domeinen aparte zones op andere servers worden (delegatie van authority) en beheerd worden door andere afdelingen. Per nieuwe DNS server wordt er een start of authority gemaakt.

## Lookup Zone

Een Forward Lookup Zone vertaald een naam naar een IP-adres. Een reverse Lookup Zone vertaald van een IP-adres naar een naam. Zo krijgen je logs ook namen van het toestel i.p.v. enkel IP-adressen.

## NSLOOKUP

Nslookup is een commando om een dns query te testen. Een reverse lookup geeft de naam weer. Het type kan ook gezet worden door “set type ‘#’” met # als opties “any, a, soa, of mx”. De server waar je je DNS query naar wilt sturen kan je instellen door “server #” met # het IP-adres van de gewenste DNS-server. Je kan de lokaal gecashte DNS records verwijderen door het commando “ipconfig/flushdns”. Je kan de records tonen met het commando “ipconfig/displaydns”.

## Mogelijke antwoorden

De client kan op een DNS query de mogelijke antwoorden geven:

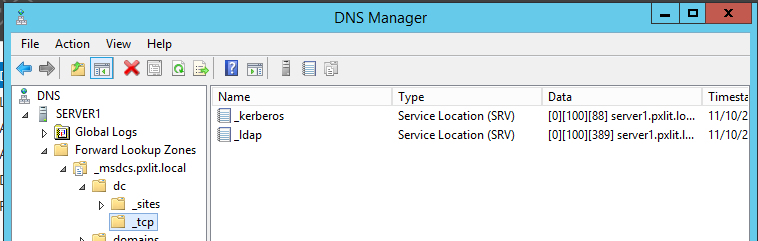
* IP
* Geen antwoord

De server kan op een DNS query de mogelijke antwoorden geven:

* IP
* Geen antwoord
* Ik weet het niet maar ga kijken bij name server X

DNS forwarding komt voor als de server geen vragen kan stellen op het internet. Dan za de vraag geforwarded worden naar een hoger liggende DNS-server die wel toegang heeft tot het internet.

Active Directory kan NIET zonder DNS. AD bevat objecten die users,computers,... voorstellen. DNS zorgt voor de koppeling van deze objecten naar IP’s en afficheren van services. Deze gegevens kan je terugvinden in je DNS van je Domaincontroller en geven de LDAP service aan. Je ziet hier ook records voor kerberos, de global catalog en bijkomende services.



Een domeinnaam heeft:

* Domeinnaamhouder (eigenaar)
* Technical Contact (technische ondersteuning)
* Registrar (agent)
* Nameservers
* Keys (dynamische updates/wijzigingen)
* Transferstatus

Split DNS is wanneer de DNS anders is wanneer hij binnen of buiten een bepaald domein zit. Afhankelijk van waar je gaat inpluggen kan de DNS reply verschillen. Zo kan je makkelijker een onderscheid maken of een user ‘intern’ of ‘extern’ is.

## Zones

Primary zone: eerste originele zone binnen je dns. Is read/write en bevat alle records van je domein. Tussen primary zones wordt continu gerepliceerd.

Secondary zone: kopie van de primary zone en is enkel read-only. De records worden niet weggeschreven. Ze worden ook enkel geupdate na een zone transfer.

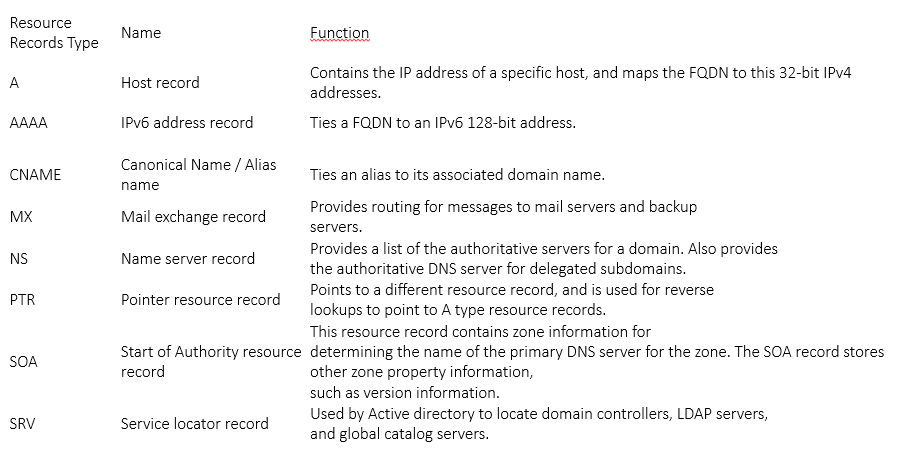
Active directory integrated zone: een DNS zone waarbinnen alle records ook naar de AD worden geschreven.

Forward lookup zone: zone waarbij de records een dns naam bevatten en het corresponderend ip wordt opgeslagen.

Reverse lookup zone: zone waarbij de records een ip adres bevatten en de corresponderende naam wordt opgeslagen.

Stub zone: bevat enkel de dns zone records zodat aangevraagde records kunnen worden doorgestuurd naar een master zone (primary zone bv).

## DNS Records



# NAT Routing

(Portbased) Network Address Translation dient om internettoegang te delen van slechts één ISP verbinding. Dit vertaalt een interne socket naar een externe socket. Dit zorgt ervoor dat meerdere toestellen van dezelfde internet toegang kunnen werken.

Een applicatie heeft een service en die werkt via een poort. Er staan meestal 100-200 poorten continu open. Data via meerdere poortnummers kunnen uiteindelijk naar slechts 1 proces gaan. Netstat -a geeft alle communicatie en de poorten waarop ze gekoppeld zijn.

Communicatie gebeurt van ip naar ip maar ook van poort naar poort. (ip:poort -> socket) -> van socket naar socket. Dit is om te weten naar welk proces je wil gaan(socket ontvanger) en die moet antwoorden op dat proces (socket verzender).

Een router kan rond de 40000 poorten tegelijk verwerken. Dynamic port based nat -> op meerdere poorten op meerdere netwerkkaarten vertalen. Een andere oplossing kan meerdere ISP’s zijn. (redundancy) Goedkopere routers hebben een beperkte NAT-tabel en hebben een kleinere buffer en zwakkere CPU. Vertaling is van een interne socket naar een externe socket (gebeurd in NAT-tabel).

DNS:  
-> aan root hint servers koppelen -> altijd naar root dus traag (meerdere query’s) -> niet aan te raden  
-> forwarden naar bvb ISP -> hebben meer cache dus sneller (1 query) -> aangeraden

Om NAT werkend te krijgen op de Windows Server 2016 kiezen we de rol ‘Remote Access’ en ‘Routing’.

# Additional Active Directory’s

De voordelen van meerdere DC’s zijn de mogelijkheid om de load te verdelen, redundancy en de services kunnen verdelen.

Gebruikt dezelfde database als de primary, de load wordt verdeeld en als de primary down gaat, kan de additional overnemen. Active Directory Replication -> data wordt gesynct. Er kunnen meerdere additional domain controllers zijn.

Stap 1: Fatsoenlijk ip-adres binnen hetzelfde subnet (2de controller -> 192,168,1,100)  
Stap 2: DNS van de 2de server -> zelfde als server1 (nooit ISP)  
Stap 3: fatsoenlijke gateway  
Stap 4: ADDS en DNS toevoegen als rol  
Stap 5: promote this server to a Domain Controller (vlagje klikken)  
Stap 6: Additional Domain Controller in existing domain kiezen  
Stap 7: zelfde domein ingeven (pxlit.local)  
Stap 8: PXLIT.local/Administrator ingeven als gebruiker (van server1)  
Note: ADDS op interne v-switch koppelen

Troubleshooting 1: ping van server2 naar server1 (firewall’s uitzetten)  
 -> reply maar toch niet beschikbaar  
 -> DNS instellingen wss niet in orde

## DFS – Distributed File Services)

DFS -> namespace maken waar alle shares samenkomen in 1 naam. Namespace staat in het domein en verzameld meerdere netwerkshares (geïntegreerd in het domein!)

* + - Standard server editions 1 namespace  
    - Enterprise / datacenter onbeperkt aantal namespaces

Folder replication:  
 - koppel 2 verschillende shares aan mekaar en laat de gegevens continu synchroniseren  
 - ideaal voor redundancy van roaming profiles, file servers, etc…  
 - roaming profiles koppelen aan namespace geeft redundancy op logins.

Namespace mag niet dezelfde naam hebben als een netwerkshare. Zorgen dat security’s van server 1 en server 2 hetzelfde zijn. Namespace maken voor fileserver en profiles, in een replication groep op beide servers en profielpad aanpassen bij de user’s profile (geen ip maar namespacenaam).

# DHCP

DHCP (Dynamic Host Configuration Protocol) deelt automatisch ip-adressen uit. Je kan ip-adressen uit. Je kan een scope uitdelen waarbij je excluded ip-adressen er uit kunt laten om duplicate ip-adressen te voorkomen. Scopes mogen elkaar niet overlappen. De laatste van de 2 apparaten die hetzelfde IP-adres hebben, zal geen internet hebben. Door veel netwerkdomeinen te gebruiken kan men VLAN’s en ACL’s gebruiken.

Default-router: gateway = ip-adres waar alle pakketten die niet bestemd zijn voor intern netwerk naartoe worden gestuurd. De lease-time is de tijd dat je een IP-adres mag gebruiken en niemand anders dit kan opeisen. Wanneer de verbinding verbroken wordt, krijgt de DHCP server een melding dat het IP-adres niet meer gebruikt wordt.

Standaard wordt om het uur een check gedaan of het IP nog gebruikt wordt. Als je de leasetime te kort zet, valt je SaaS verbinding weg (Software as a Service) maw Google Docs en DB connecties. DHCP wordt standaard op server1 geconfigureerd (zelfde als VPN pakken). NAT + DNS zijn de favoriete theorievragen.

# VPN

VPN (Virtual Private Netwerk) is een publieke verbinding die met een lokaal netwerk gemaakt wordt. Dit zorgt ervoor dat de data geëncapsuleerd wordt. De toegang tot VPN is per gebruiker. Meestal is VPN gecombineerd met NAT.

Connectie maken naar een toestel waarbij die connectie versleuteld en privaat is. Privaat is dat de verbinding enkel tussen u en de andere kant is. Door VPN lijkt dit alsof het lokaal op het netwerk afspeelt. Dus zou je toegang hebben tot het lokale netwerk van de VPN-server.

VPN connectie maken: externe IP-adres van de VPN router invullen en verbinding maken

-> De router en de client krijgen een nieuwe virtuele adapter. Zij communiceren met elkaar voor het pakketje aangekomen is of verzonden wordt.

Eerst gaat alle data door mijn virtuele adapter naar de andere virtuele adapter -> virtueel naar virtueel. Dan gaat hij van mijn virtuele adapter via mijn fysieke adapter. Je krijgt een IP-adres van het lokale netwerk waar je inlogt.

De hele blok (OSI) data wordt toegevoegd aan de blok (OSI) van de fysieke netwerkkaart.  
Die hele blok wordt doorgestuurd naar de router van de VPN-router. Dit gaat eerst naar de fysieke netwerkkaart, terug door OSI en die data gaat naar de virtuele adapter stuurt het door naar de website die je initieel wilde bereiken. De website antwoord terug naar de VPN-router en zet dit terug naar de virtuele adapter en ingepakt naar de fysieke en over connectie naar de fysieke client en door het virtuele adapter tot de gebruiker.

VPN kan op het lokale netwerk van de router gaan kijken.

Voordeel:  
-> Je kan het hele lokale netwerk zien  
-> De data wordt versleuteld -> dit wordt op de Presentation laag gedaan (SSL)  
 -> best de fysieke versleutelen want dan is ALLE data versleuteld, bij de virtuele alleen de blok van de virtuele en niets van de fysieke  
-> ISP zou je destination niet moeten kunnen zien