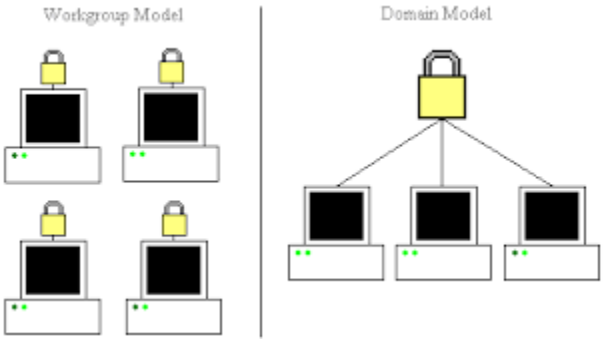
Windows Server

1. Introductie / herhaling

1.1 Domein

Een computer kan lid zijn van een workgroup (werkgroep) of een domain (domein). Beiden hebben hun voordelen en nadelen.



Figuur 18 Workgroup - domain

Een workgroup bestaat uit gelijke clients (computers voor end-users), waarbij elke client zijn eigen functionaliteit beheert. Een workgroup bestaat met andere woorden uit clients die beheerd worden door de lokale administrator van het toestel.
Indien je deze clients een beperking wil geven (policy), ben je verplicht dit voor elk toestel apart te configureren.

Een domein bestaat uit één of meerdere servers die alle onderliggende clients beheren. Elke client kan door een domein administrator beheerd worden vanop afstand, en beperkingen (policies) kunnen centraal door één domein administrator aangemaakt worden en verdeeld worden naar eender welke client. De clients worden met andere woorden beheerd door één of meerdere domein administrators vanop afstand.

In een domein kan je veel specifieker elk toestel beheren en beperken, kan je veel makkelijker beveiligingen vanuit 1 centraal punt verdelen en kan je alle instellingen vanuit 1 of meerdere servers aansturen.
Het toestel of meerdere toestellen die je domein beheren noemen ze domein controllers.

Enkele voordelen van een domein tegenover een werkgroep:

- gecentraliseerd beheer tov lokaal beheer
- (domein)gebruikers bruikbaar doorheen het volledige domein tov lokale gebruikers
- integratie van gebruikeraccounts vanuit 3th party software tov geen integratie mogelijk

- gebruikersgroepen tov individuele gebruikers
- controleerbaar tov oncontroleerbaar
- automatiseerbaar tov manueel
- …

Zoals je merkt heeft een domein een veel makkelijker beheer en kan je zeer veel automatiseren. Toch heeft een domein ook enkele nadelen. Een gebruiker is namelijk geen ‘baas’ meer over eigen toestel, en de domein administrator heeft altijd alle rechten om gebruikers en toestellen te beperken. Ook is niet alleen de extra server hardware en software een extra kost, ook de domein beheerder (administrator) is een zware extra kost en kan soms niet opwegen tov de automatisatie en beveiliging dat een domein kan bieden.

Een domein krijgt altijd een domeinnaam en een domeinextensie. Deze domeinnaam wordt dan gebruikt bij het maken van de computernaam (Fully Qualified Domain Name -> zie verder in de cursus). Het domein binnen de pxl heet PXL.LOCAL.

1.2 Domein: Active Directory (AD) en LDAP

Een domein is dus een gecentraliseerd systeem dat verschillende functies creeert voor gebruikers en clients.
Gebruikers kunnen inloggen met een gebruikersnaam en wachtwoord (username en password). Die gebruikersnaam, wachtwoord en andere instellingen worden opgeslagen in een database genaamd NTDS. Deze database is een onderdeel van een geheel van databases en relaties genaamd Active Directory. Active Directory is met andere woorden het geheel dat Microsoft gebruikt om alle informatie, instellingen, beperkingen en configuraties binnen een domein op te slaan op 1 locatie. Als je dus over Active Directory praat, gaat het eigenlijk over alle instellingen binnen je domein.
Een client die lid is van het domein, wordt via deze Active Directory (AD) aangestuurd. De gebruiker die wil inloggen op deze client moet ook een account hebben binnen deze AD. Wanneer een client wil communiceren naar de domein controller (of andere toestellen die gegevens uit deze database willen halen), gebruikt hij het protocol LDAP (**Lightweight Directory Access Protocol (LDAP)**. LDAP is dus de verbinding die gevormd wordt om gegevens uit de AD databases te halen, en leest de gegevens uit vanuit de database. Deze database moet in een bepaalde vorm gecreeerd zijn zodat LDAP deze gegevens kan uitlezen/wegschrijven en kan gebruiken.

Figuur 19 LDAP integratie

LDAP vind je ook dikwijls terug in andere besturingssystemen of bij andere servers/services. Een NAS storage die LDAP ondersteunt, kan met andere woorden gegevens uitlezen uit een AD database van onder andere Windows, en kan dus ervoor zorgen dat je met je Windows account automatisch rechten kunt instellen op de storage. Een WIFI-accespoint met LDAP kan met standaard Windows gebruikers het wachtwoord uitlezen uit een AD database om te zien of het wachtwoord hetzelfde is als bij de Windows server en je toegang verlenen tot het

netwerk (zie bv het PXL netwerk waarmee jij met je PXL-account jezelf kan authenticeren bij WIFI, Blackboard en andere netwerkservices).

De AD databases bevatten alle gegevens van het domein. We noemen deze gegevens objecten. Objecten kunnen zijn:

- users / usergroups (gebruikersnamen, wachtwoorden, gegevens van users)
- computers (gegevens, computernamen)
- policies (beperkingen die je vanuit het register kan instellen op users/computers)
- Organizational Units (fictieve folders die users/computers kunnen bevatten en gebruikt worden voor policies).
- Printers en andere aanstuurbare objecten

Deze AD databases bevinden zich op een server genaamd de Domain Controller (DC). Deze domain controller kan users authenticeren (via LDAP), scripts doorsturen, policies aansturen, en security instellingen uitvoeren. Deze Domain Controller (DC) beheert dus het gehele domein. Een domein controller kan bestaan uit meerdere servers, waarbij elke extra domein controller de naam 'Additional Domain Controller' (ADC) krijgt. Elke extra ADC synchroniseert zijn AD databases met de andere (A)DC's zodat elke AD database identiek is op elke domein controller binnen éénzelfde domein. Zo kan je load verdelen overheen alle domein controllers en heb je een vorm van redundancy.
Redundancy is de term waarmee je extra servers/services maakt zodat, mocht 1 toestel of service uitvallen, een ander toestel/service de functionaliteit kan overnemen.
Load balancing is de term waarbij meerdere toestellen dezelfde functionaliteit hebben, en waarbij het werk wordt verdeeld over die meerdere toestellen. Met load balancing kan je met andere woorden meerdere gebruikers tegelijkertijd laten aanloggen op verschillende domein controllers. Als dus 's morgens om half negen 3000 studenten tegelijk op het wifi netwerk willen aanloggen, zorgt load balancing overheen de verschillende AD servers dat iedereen zich op één van de verschillende servers kan aanloggen.

1. Services in domein

Elk domein heeft een aantal basisservices nodig. Deze services dienen om je domein te laten communiceren tussen hosts (clients) en services. Een aantal services zijn niet noodzakelijk, maar zouden alles wel zeer arbeidsintensief maken mochten ze niet aanwezig zijn.

1.3 DHCP (Dynamic Host Configuration Protocol)

Een DHCP service deelt ip configuraties uit aan toestellen wiens netwerk interface op automatisch (automatic) staat geconfigureerd.
In een modern netwerk gebruiken we nog amper statische (vaste) ip adressen en worden de meeste ipadressen en netwerk configuraties automatisch verdeeld. Dit kan je lokale router of lokale server doen.
Bij het opstarten vraagt een device (wiens netwerk interface als automatic staat geconfigureerd) de ip instellingen aan een DHCP service. Meestal worden volgende settings uitgedeeld:

- ipadres + subnet mask
- default gateway (default router)

- DNS
- domein naam

Figuur 20 DHCP Server

Een ipadres is nodig om elk toestel op het netwerk een uniek adres te geven, zodat alle hosts met mekaar kunnen communiceren.
Verdere uitleg over deze service krijg je bij het vak Network Essentials

3. DNS (Domain Name System)

DNS is een service die Fully Qualified Domain Names (fqdn) oplost naar ip adressen. Dikwijls wordt gerefereerd dat DNS ipadressen en urls oplost, maar dit is slechts een deel van de resolving dat DNS doet.
Resolving is de Engelse term voor het oplossen van een vraag. Een DNS server lost dus maw volledige domeinnamen op naar IP adressen en omgekeerd.
Een fqdn is een domeinnaam met een prefix + domeinnaam + suffix. Een voorbeeld is www+pxl+be. Wij herkennen deze url als www.pxl.be waarbij de punt dient als afscheiding. Binnen een domein gebruiken we die DNS server ook om te kunnen communiceren tussen de hosts en de servers. Zo krijgt elke host ook een fqdn. Deze bestaat bij een host uit de computernaam+domeinnaam+domeinextensie. Indien we dus een computer lid maken van het domein PXL.LOCAL krijgt het als fqdn (bv pc201851234.PXL.LOCAL).

Meer info (buiten deze cursus) vind je op
https://www.ionos.com/digitalguide/domains/domain-administration/fqdn-fully-qualified-domain-name/

Figuur 21 DNS resolving

1.4 Domein creatie

Tree

Een domein bestaat uit een Active Directory Database die gerepliceerd (gesynchroniseerd) wordt tussen verschillende servers. Elke domeincontroller die in hetzelfde domein zit, bevat dezelfde Active Directory Database als eender welke andere domein controller. De databases zijn met andere woorden identiek. Een user kan inloggen op éénder welke domein controller, en de load wordt dus verdeeld binnen éénzelfde domein.

Die AD database kan zeer snel groeien door bijvoorbeeld enorm veel users te creeren. Hoe groter een database, hoe trager deze wordt en hoe moeilijker deze ook te beheren is. Ook kan security een issue worden en scheid je graag accounts op.
Daarom kan een bedrijf kiezen om de database te splitsen in een nieuwe kleinere database. Je maakt een child database door een child domain te creeren.

Wat is een child domain? Een child domain is een afgesplitst domein van het originele domein (de parent domain genoemd), en bevat een volledig nieuwe Active Directory. Het child domein krijgt ook gedeeltelijk dezelfde naam als het parent domain, maar krijgt een extra prefix. Bv PXL.LOCAL kan het parent domain zijn, dan wordt student.PXL.LOCAL het child domain. PXL.LOCAL heeft zijn eigen AD database, en de child student.PXL.LOCAL krijgt zelf ook een nieuwe AD database.

Eenmaal een child aangemaakt, kan je users, groepen, en andere objecten verplaatsen van de ene parent naar de child of andersom. Automatisch wordt het nieuwe child domain vertrouwd, maw een account die verplaatst wordt van de parent naar de child kan nog altijd inloggen op het parent domain, en ook andersom. We spreken dan van een trust tussen de 2 parent en child domains.

Standaard is er tussen een parent en een child een 2-way trust (de parent vertrouwt de child volledig, de child vertrouwt de parent volledig) en kunnen dus alle accounts op beide domeinen gebruik maken van alle login services. De policies die staan op de parent, kunnen mee overgenomen worden (maar is niet noodzakelijk) naar de child.
We kunnen meerdere childs maken vanuit de parent, en childs kunnen op hun beurt ook nog extra childs bevatten. De verzameling van alle parent en child domeinen noemen we een TREE.

Binnen een tree kunnen dus accounts van alle childs inloggen op alle andere childs en de parent. Zo kunnen wij op de PXL inloggen met onze studentenaccounts (lid van student.pxl.local) op de parent PXL.LOCAL (bv het wifi netwerk) en kunnen docentenaccounts (lid van PXL.LOCAL) ook inloggen op services die in de child student.pxl.local staan.

Een account kan maar in 1 database zitten, maw je studentnummer (je account name) is uniek binnen de gehele tree.

Figuur 22 Tree met child domains

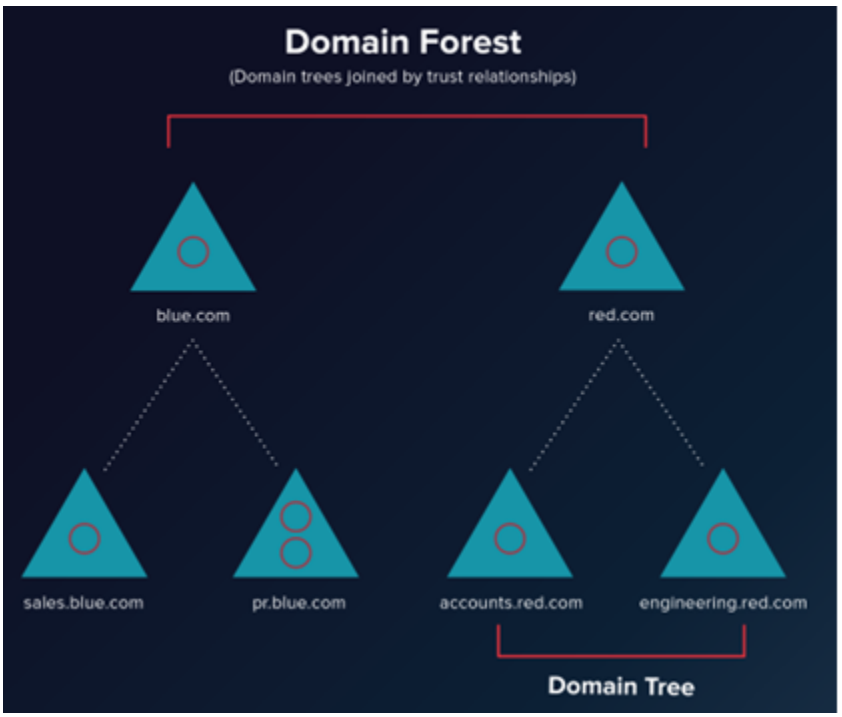
Forest

Wanneer een bedrijf wil samenwerken of fusioneren met een ander bedrijf, kan het zijn dat beide bedrijven tijdelijk dezelfde domeinstructuur willen behouden, maar toch op IT-gebied willen integreren met mekaars infrastructuur.

Beide bedrijven blijven dan dezelfde domeinstructuur houden, alle accounts blijven binnen hetzelfde domein, maar je gaat mekaars domeinen vertrouwen zodat gebruikers op beide domeinen kunnen werken.

Het koppelen van 2 aparte domeinen en dus 2 verschillende trees noemen we een Forest. Je zet een forest op door een trust verbinding op te zetten tussen beide domeinen. Je hebt 2 vormen van trusts. Ofwel bouw je een éénwegs trust op waarbij de accounts van 1 domein wel het andere domein vertrouwen, maar niet omgekeerd. Zo kan het zijn dat bedrijf A wel accounts toestaat van bedrijf B, maar dat de accounts van bedrijf A niet meer kunnen inloggen op de services van bedrijf B.
Meestal wordt een 2-wegs trust opgezet, waarbij beide bedrijven mekaars accounts vertrouwen.

Forests worden veelal opgezet bij diepere samenwerking of bij fusionering.
Stel dat de trees Syntra.local en PXL.local een 2way trust zouden opzetten.
Zo zou je met een account van het domein Syntra.local jezelf kunnen connecteren op het PXL wifi netwerk, en kunnen lectoren accounts van xxxxx@syntra.local toevoegen aan services zoals Blackboard of Epos. Syntra kan dan het omgekeerde doen, waardoor studenten van PXL zouden kunnen inloggen op het Syntra netwerk. Je kan ook fileservers bouwen waar beide domeinen toegang zouden verlenen aan gemengde groepen.



Figuur 23 Forest - Tree

Rollen - Features

Een rol is een functie dat we onze server kunnen geven. Enkele veel gebruikte rollen zijn domein controller (ADDS), file server, print server, database server, DNS server, web server, dhcp server en/of vpn/router server. Elke rol moet eerst geinstalleerd worden en kan naderhand geconfigureerd worden via Server Manager (onderdeel van Windows Server, zie verder).
Een feature is geen afgescheiden functie maar eerder een uitbreiding, een toepassing, die kan gebruikt worden door rollen of als stand alone uitbreidingsfunctie. Veel gebruikte features zijn bv .Net Framework, Bitlocker, Backup, etc…
Een rol kan vereisen dat bepaalde features mee geinstalleerd worden, deze moet je dus ook altijd accepteren bij het installeren van een bepaalde rol.
Je bent niet beperkt in het aantal rollen dat je installeert op een server, maar voor gemak worden rollen meestal verdeeld over verschillende servers zodat updates, upgrades of migraties makkelijker kunnen uitgevoerd worden.

Page Break

1.5 Domain Users, User groups, security groups, AGDLP

Elke gebruiker die aangemaakt wordt binnen de domein users kan (standaard) inloggen op elk toestel dat lid is van dat domein. Dat is de grote sterkte van domeinen. Je kan tientallen computers ter beschikking stellen, waar eender welke user kan aanloggen op eender welk toestel met zijn eigen instellingen, documenten en zijn eigen profiel.

Deze domein users moeten aangemaakt worden op een Active Directory domain management tool genaamd “Active Directory Users & Computers” (zie verder).
Elke domein user kan op zijn beurt lid worden van user groups. User groups is een verzameling users die binnen deze user group samengevoegd kunnen worden en zo tegelijk dezelfde instellingen of beveiliging kunnen krijgen.
Deze user groups worden veelal gebruikt voor beveiliging van folders en toewijzen aan bv fileservers, webservers (denk aan Blackboard, gebruikers per klas of per jaar), en andere services en resources waar het gemakkelijk is om users te groeperen.
Je hoeft maar eenmalig groepen aan te maken en gebruikers lid te maken om deze overal te kunnen gebruiken. Als een user verwijderd wordt uit een groep, wordt deze doorheen de gehele structuur ook verwijderd bij elke service of resource. Zo kan je makkelijk gecentraliseerd werken.
Er zijn 2 soorten groepen: security groups en distribution groups. Een distribution group is hoofdzakelijk gebruikt om gebruikers te verzamelen in mailing groups. Zo kan je een mail sturen naar een group ipv naar een aantal aparte gebruikers (bv distribution group “alle TIN studenten” waarin je elke user van TIN toevoegt).
Security groups worden gebruikt om toe te wijzen aan resources (bv websites) of aan folders/mappen. Zo kan je één security group toegang geven tot één welbepaalde map zodat anderen er niet aan kunnen. Ook kan je security groepen gebruiken om gebruikers gezamenlijk te laten inloggen op websites.

Binnen de security groups hebben we nog een onderverdeling aan de hand van zichtbaarheid doorheen ons domain/forest.

Global groups: deze groepen zijn zichtbaar doorheen de gehele forest. Met andere woorden, bij fusies kan je deze groepen gebruiken om gebruikers van andere domeinen toegang te geven tot je eigen resources. Zo kan je bv users van Syntra toegang geven tot Blackboard van PXL (indien PXL en Syntra een forest vormen). Je voegt de global groups van Syntra toe aan Blackboard. Deze global groups kunnen enkel users bevatten van hun eigen domein (we kunnen dus geen users van Syntra toevoegen aan de global groups van PXL of andersom) maar kunnen wel de global groups, gemaakt door Syntra (met Syntra users), toevoegen aan de resources van PXL.
Meestal worden deze groepen gebruikt om gebruikers toe te wijzen, waarna we deze groepen toevoegen aan domain local groups (zie verder AGDLP).

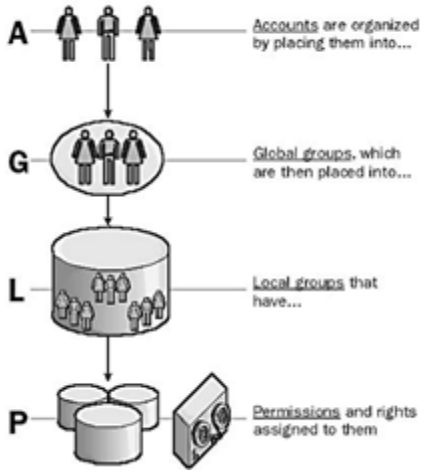
Domain local groups: deze groepen zijn enkel zichtbaar binnen het eigen domein. Deze groepen worden voornamelijk gebruikt voor security instellingen en het toevoegen aan resources. Deze groepen bevatten meestal niet rechtstreeks de gebruikers, maar wel de Global Groups (waar de gebruikers in zijn toegevoegd).

1.6 AGDLP

AGDLP staat voor Accounts, Global groups, Domain Local groups, Permissions
Dit is een manier van werken dat Microsoft aanraadt.
Je maakt Global groups, waar je alle gebruikers aan toevoegt per groep (bv een global group “1TINA_global” met alle studenten van die klas in).

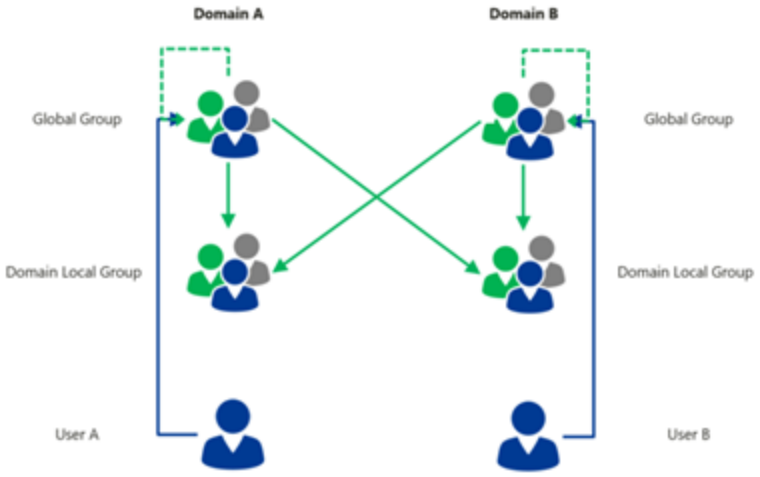
Je voegt dan deze Global Group “1TINA_global” toe aan een domain local group genaamd “1TINA_domainlocal”.

Op deze manier bevat de domain local group ook alle gebruikers van de global group, en wordt elke toegevoegde of verwijderde gebruiker uit de global group ook automatisch verwijderd uit de domain local group. Daarna gebruik je deze domain local groups om toe te wijzen aan resources (permissions).



Figuur 24 A G DL P principle

Je mag ook groupen nesten (samenvoegen of lid maken van een andere groep). Een Global group mag een andere global group bevatten (maar kan geen domain local group bevatten). Een Domain Local group kan een andere domain local group bevatten en ook andere global groupen.
De algemene werking is, we plaatsen de users in global groups, en plaatsen de global groups in (een of meerdere) domain local groups. Deze domain local groups gebruiken we dan om toe te wijzen aan onze file servers, web servers of andere resources.

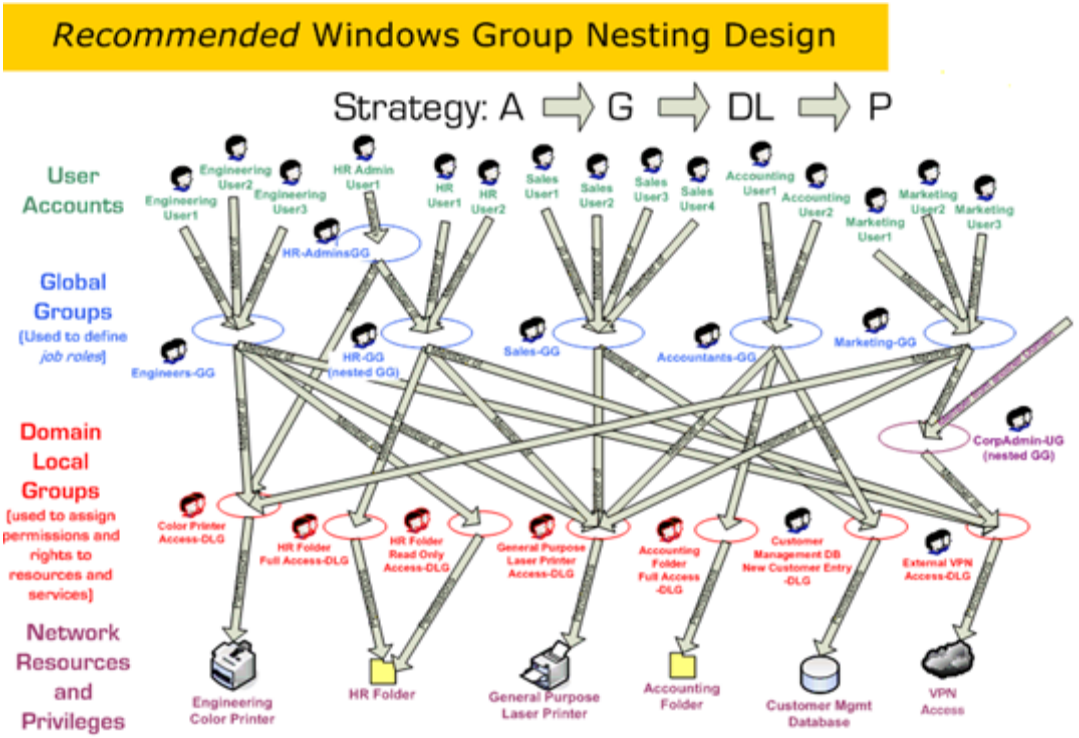


Figuur 25 Global - Domain Local groups

Voorbeeld
We maken global groups aan voor de klassen van 1TIN:

1TINA_GL, 1TINB_GL, 1TINC_GL, 1TIND_GL, 1TINE_GL, 1TINF_GL.
Deze Global groups voegen we toe aan onze Domain local groups.
1TINA_DL, 1TINB_DL, 1TINC_DL, 1TIND_DL, 1TINE_DL, 1TINF_DL.
We kunnen nu nieuwe DL (domain local) groepen aanmaken “1TIN_DL” waarin we alle Global groupen van 1TIN plaatsen. Deze groep kunnen we gebruiken om alle users van 1TIN rechten te geven, terwijl we de domain local klasgroepen kunnen gebruiken om slechts 1 klas toegang te geven tot een bepaalde resource.
Je kan hetzelfde doen voor de studenten van 2TIN en 3TIN (global groups per klas, domain local groups per klas en een domain local group voor heel 2TIN en eentje voor heel 3TIN). Daarna kan je nog een domain local group maken voor geheel TIN (TIN_DL), waarin je de domain local groups 1TIN_DL, 2TIN_DL en 3TIN_DL toevoegt.
Je kan met andere woorden binnen een domain local group andere domain local groups nesten, maar ook global groups in domain local groups nesten.
Een user die verwijderd wordt uit één global group, wordt op deze manier ook ineens ‘verwijderd’ uit elke andere groep waarin hij genest is geweest. Als je een student verwijdert van bv 1TINA_GL, wordt deze automatisch ook geen lid meer van 1TINA_DL, 1TIN_DL en TIN_DL.

Hieronder zie je een ander voorbeeld van group nesting en het toevoegen van de domain local groups aan resources.



Figuur 26 AGDLP Group nesting

1.7 Organizational Units (OU)

Een organizational Unit is een soort van map (verzameling) waarin we objecten (users, computers, printers, etc..) verzamelen, om zo beperkingen of instellingen toe te wijzen aan die OU en ook alle toegevoegde objecten (users, computers, printers, …) in die OU.
Zo kan je bv een OU “1TIN” maken, daarin alle users plaatsen van 1TIN, en daar een instelling op plaatsen (bv elke user dezelfde homepage).
Je kan ook een OU “LABfysica” maken, en daarin alle computers van dat lokaal toevoegen, en daar een instelling op plaatsen (bv geen toegang tot de C-schijf van de computer, of usb poorten uitschakelen).
Deze beperking of instellingen noemen we een policy (dit wordt pas een lab bij het vak OS Advanced 2TIN).
Het nut van deze OU’s is dus vooral om users en computers die in deze OU worden geplaatst, te beperken of in te stellen.
Als we users aanmaken, plaatsen we deze meestal in OU’s. Computers worden op hun beurt ook in deze OU’s ingedeeld. Je kan OU’s in OU’s aanmaken, waarbij inheritance optreedt. Inheritance (of overerving in het Nederlands) betekent dat een instelling (of policy) ook wordt uitgevoerd in onderliggende OU’s, en zo dus doorheen onze volledige OU structuur
De vorm van de OU structuur is heel belangrijk. Deze bepaalt namelijk ook welke objecten welke policies krijgen. De opbouw en structuur van de OU’s is leerstof voor het vak OS Advanced in 2TIN.