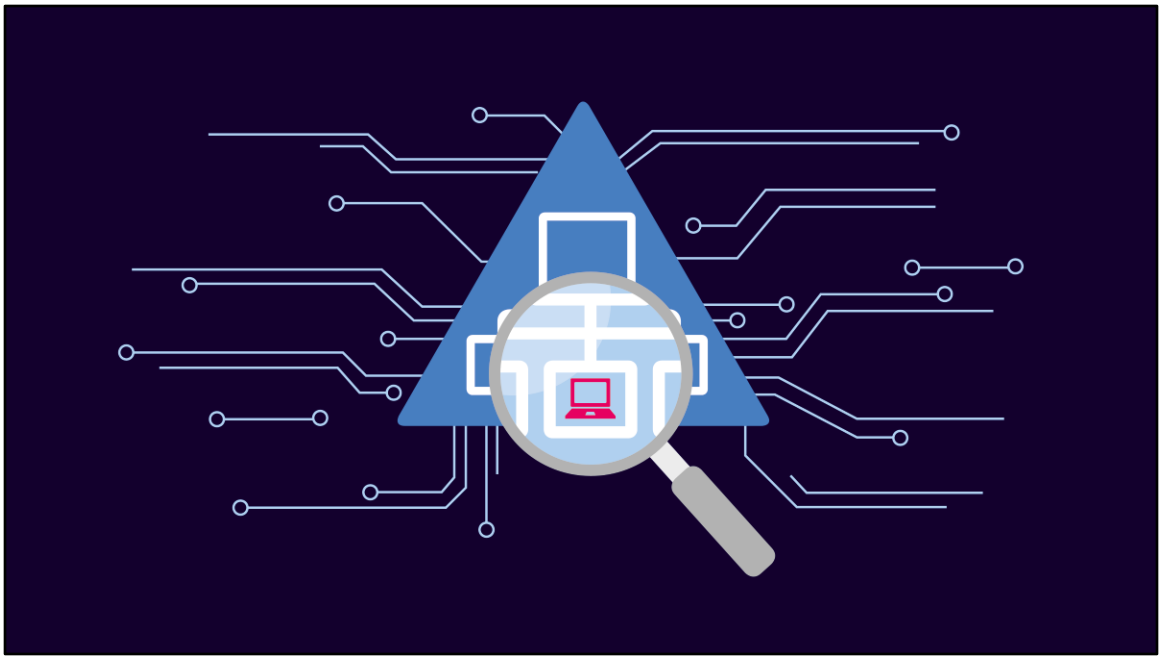
Windows Server I

5. Active Directory

HO
GENT



5. Active Directory

HO
GENT

5.1 Waarom Active Directory?

HO
GENT

5.1 Waarom Active Directory?

Peer-to-Peer vs. Client-Server

Peer-to-Peer
Decentralized
Werklast verdeelt
Geen SPOF

Client-Server
Centralized
Centraal beheer
Stabiel en veilig

HO GENT

Peer-to-Peer vs. Client-Server

Binnen computernetwerken worden vaak bronnen en applicaties beschikbaar gesteld aan andere toestellen in het netwerk. Traditioneel kan dit op twee manieren gebeuren: via een Peer-to-peer netwerk of via een client-server model. Een toestel dat diensten aanbiedt wordt vaak een *server* genoemd, terwijl een toestel dat diensten gebruikt een *client* genoemd wordt. Een *server* kan meerdere *clients* gelijktijdig bedienen, en een *client* kan tegelijk meerdere diensten gebruiken van meerdere *servers*.

In een typisch Peer-to-Peer netwerk is er geen duidelijk onderscheid tussen *servers* en *clients*. Elk toestel in het netwerk kan immers bepaalde diensten aanbieden en tegelijkertijd diensten gebruiken van andere toestellen in het netwerk. Zo kan een toestel in het netwerk bijvoorbeeld een printer delen die verbonden is met USB (= print server), maar de bestanden om te printen worden opgehaald van een ander toestel in het netwerk dat dienst doet als file server. Een toestel in het netwerk kan dus met andere woorden tegelijk *server* en *client* zijn.

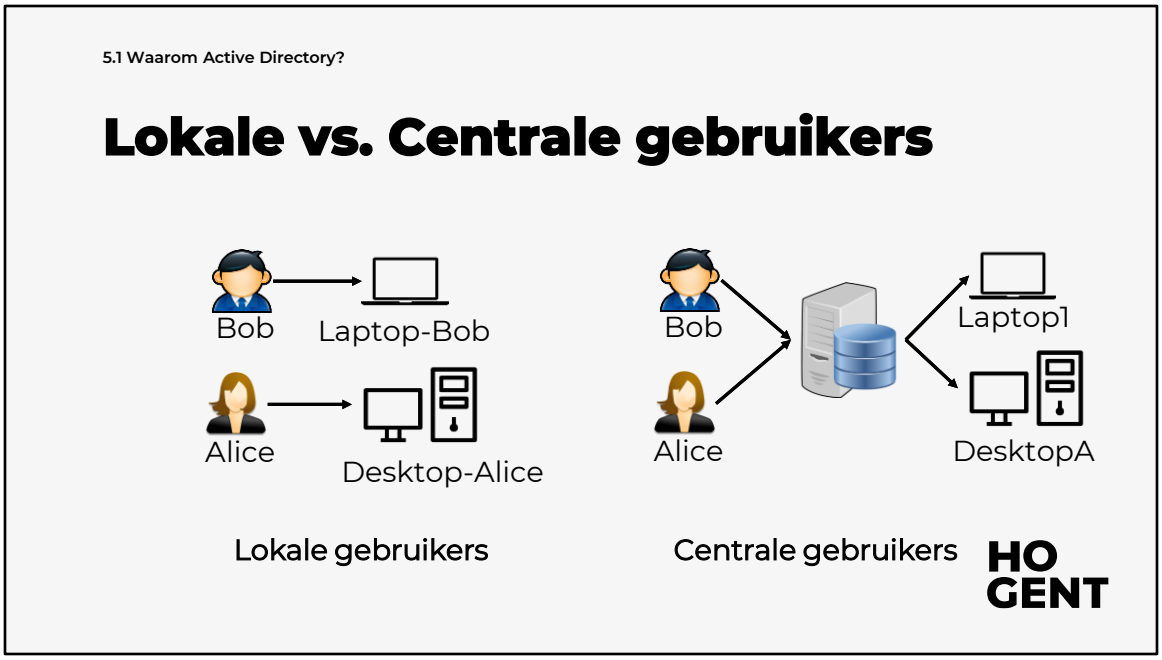
In een typisch Client-Server netwerk is er echter één centrale server, die bepaalde

diensten aanbiedt, en alle andere toestellen zijn de clients die van deze diensten gebruik maken. Het beheer van dit netwerk gebeurt centraal: er is één centrale server die de diensten aanbiedt, en typisch is deze server 24/7 online. Er bestaan bovendien ook hybride modellen (combinatie Peer-to-Peer en client-server) en variaties op bovenstaande modellen, maar deze zijn minder relevant voor dit hoofdstuk.

Het voordeel van Peer-to-Peer netwerken is dat je de werklast kan verdelen. Als er maar één toestel is in het netwerk dat diensten aanbiedt (zoals in het Client-Server model) kan dit toestel de bottleneck worden van het netwerk, en als deze server onbereikbaar is kan geen enkel toestel nog van de dienst gebruikmaken. Een andere term voor een Peer-to-Peer netwerk is een “decentralized network”: er is geen centrale server, elk toestel kan zowel server als client zijn, en het grote voordeel van peer-to-peer netwerken is dat je een hele goede performantie met hele hoge snelheden kan halen. Dit is vooral nuttig in sommige applicaties zoals het delen van bestanden over het netwerk, en torrents zijn een heel mooi voorbeeld van een toepassing die P2P gebruikt. Het grootste nadeel van Peer-to-Peer netwerken is echter dat deze moeilijker te beheren zijn, vaak kunnen veranderen (wanneer een toestel offline gaat zijn de diensten niet langer bruikbaar), en het niet altijd evident is om te achterhalen welke diensten beschikbaar zijn op het netwerk en op welke dienst op welk toestel aangeboden wordt.

Een client-server netwerk daarentegen is een “centralized network”. In het netwerk is er één server (of meerdere in geval van load balancing of een failover setup) die diensten aanbiedt, en het grote voordeel hiervan is het centraal beheer. Alle diensten worden aangeboden vanaf dit ene toestel, dus het is niet nodig om te achterhalen welk toestel welke diensten aanbiedt, maar als de centrale server offline gaat zijn de diensten wel niet langer bruikbaar door de clients. Een “centralized network” is echter wel meer stabiel en veel veiliger, aangezien dergelijk netwerk ook gemakkelijker te beveiligen is – het is immers gemakkelijk om firewall regels op te stellen voor één centrale server dan voor elk toestel in het netwerk dat mogelijks diensten aanbiedt.

Voor thuisnetwerken waarbij het aantal toestellen en aantal diensten in het netwerk vrij beperkt is, kan je perfect een Peer-to-Peer model gebruiken. Wanneer het netwerk echter groter wordt, wordt het beheer van het Peer-to-Peer netwerk veel complexer. Binnen bedrijfsnetwerken wordt dan ook vaak gebruikgemaakt van het Client-Server netwerk model, en Active Directory is een mooi voorbeeld is van een Client-Server netwerk toepassing. Maar wat precies is Active Directory?



Lokale vs. Centrale gebruikers

Bij de installatie van Windows 10 op jouw laptop heb je vermoedelijk in de laatste stap een gebruiker aangemaakt. Daarnaast heb je jouw toestel ook een naam gegeven. Dit is prima voor een persoonlijk toestel, aangezien jij vermoedelijk de enige gebruiker bent die het toestel zal gebruiken. Als nu jouw broer of zus ook van jouw laptop gebruik wil maken zal hij/zij ofwel jouw account moeten gebruiken, ofwel kan je een tweede account aanmaken op jouw laptop. Als je volgend jaar echter een nieuwe laptop koopt zal je alle gebruikers opnieuw moeten aanmaken op het nieuwe toestel. De figuur links in de slide illustreert dit concept: Bob heeft een lokale gebruikersaccount op zijn eigen laptop (Laptop-Bob) en Alice heeft een lokale account op haar desktop (Desktop-Alice), maar Bob kan niet inloggen op de desktop van Alice en vice versa.

De gebruiker die je aanmaakt bij de installatie van Windows is een lokale gebruiker: deze gebruiker bestaat **enkel** op jouw toestel, en je kan dus bv. niet met jouw gebruikersaccount inloggen op de computer van jouw buurman. Maar wat als we het client-server model van de vorige slide nu eens zouden toepassen op het beheer van gebruikers en toestellen in een netwerk?

In plaats van een lokale gebruikers aan te maken op jouw laptop zou je ook de gebruikers kunnen aanmaken op een centrale server in het netwerk. Daarnaast kan je alle toestellen in het netwerk ook registreren op deze centrale server. Op die manier is er niet langer een één-op-één relatie tussen een gebruiker en een toestel. De figuur rechts in de slide illustreert dit: Bob en Alice zijn centrale gebruikers die bewaard worden op een centrale server, en Laptop1 en DesktopA zijn twee toestellen in het netwerk. In deze configuratie kan Bob inloggen op de desktop van Alice, en kan Alice de laptop van Bob gebruiken.

In jouw thuisnetwerk is het wellicht niet nuttig om een dergelijk systeem te configureren, het aantal gebruikers en het aantal toestellen is immers vrij beperkt. In bedrijfsnetwerken zijn er echter vaak tientallen of honderden gebruikers en tientallen of honderden gebruikers, dus het zou onbegonnen werk zijn om op elk toestel in het netwerk manueel alle accounts te configureren die mogelijks moeten kunnen inloggen op het systeem. Daarom worden in dergelijke netwerken vaak centrale gebruikers aangemaakt. Dit maakt het beheer van de toestellen en gebruikers veel eenvoudiger, en bovendien kunnen extra regels en policies ingesteld worden (bv.: Wie kan wanneer op welk toestel inloggen? Wat zijn de vereisten voor het wachtwoord? Hoe vaak moet een gebruiker zijn wachtwoord wijzigen? …).

Binnen Microsoft-gebaseerde omgevingen kan Active Directory gebruikt worden voor het centrale beheer van gebruikers en toestellen in het netwerk.

Korte geschiedenis

Binnen Windows bestaat het concept van centrale gebruikers al even. Concreet werd het concept van een Windows domein voor het eerst gelanceerd in Windows NT 3.x/4, onder de naam *Windows Server Domain System*. Een domein of Windows NT-domein is een groep van computers in een netwerk die Windows draaien en centraal beheerd worden door een Windows server. De beheerder van het domein heeft volledige controle over alle computers in het domein, en domeinen zijn dus een middel voor het centrale beheer van Windows-computers. Dit is in tegenstelling tot de Windows Workgroups: Windows Workgroups kunnen ook gebruikt worden om toestellen binnen een netwerk te beheren, maar hier is er geen centrale server: elk toestel in het netwerk houdt zijn eigen security databank bij (dus elk toestel heeft onder andere zijn eigen gebruikers), en Windows Workgroups volgen dus het Peer-to-Peer netwerk model.

De beheermogelijkheden binnen Windows NT-domein waren echter nog vrij beperkt: zo kon een toestel in een domein maar 2 staten hebben: verbonden of geregistreerd. Met Windows Server 2000 werden de mogelijkheden voor het beheer van Windows domeinen echter heel wat uitgebreid, en werd de term Active Directory

geïntroduceerd. Binnen Active Directory zijn er één of meerdere servers die gebruikt kunnen worden voor het centrale beheer van toestellen en gebruikers in het netwerk, en deze servers draaien de Active Directory Domain Service (AD DS). Een dergelijke server wordt daarom een Domein Controller genoemd, en binnen Active Directory heb je dus steeds minstens één domeincontroller nodig voor een domein. De eerste versie van Active Directory was nog vrij beperkt, maar bij de introductie van Windows Server 2003 en later Windows Server 2008 werd de functionaliteit van Active Directory serieus uitgebreid met nieuwe features en mogelijkheden.

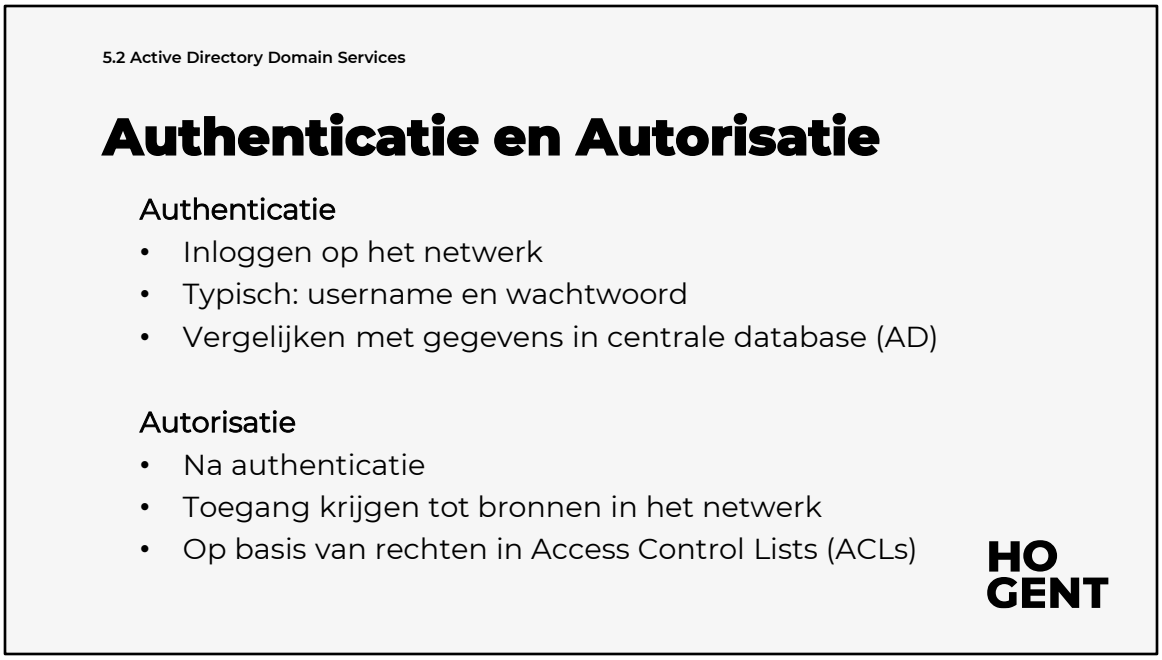
5.2 Active Directory Domain Services

HO GENT

Active Directory

Active Directory is een Directory Service, een dienst die het mogelijk maakt om toegang te krijgen tot hiërarchisch georganiseerde gegevens binnen een computernetwerk. De directory service beheert de gegevens en de relaties tussen de gegevensbronnen. Toegang tot deze gegevens gebeurt volgens het client-server principe. Een voorbeeld van informatie die opgeslagen wordt is in welke mate een gebruiker toegang heeft tot bepaalde netwerkbronnen.

Je kan Active Directory dus zien als een soort van grote database waar gegevens en objecten in zitten. Een User Account is een voorbeeld van zo een object dat opgeslagen is in Active Directory, en dit object heeft meerdere eigenschappen zoals de gebruikersnaam, het wachtwoord, de volledige naam van de gebruiker, een telefoonnummer, …



Authenticatie en Autorisatie

Active Directory biedt twee belangrijke diensten: authenticatie en autorisatie.

Authenticatie wordt gebruikt om aan te tonen wie je bent. Als een gebruiker wil aanmelden op het netwerk, dan geeft hij typisch op een Windows toestel zijn gebruikersnaam en wachtwoord in. Deze gegevens worden dan vergeleken met de gegevens in de centrale database (Active Directory) en de gebruiker krijgt dan al dan niet toegang tot het toestel en het netwerk.

Na de authenticatie zit de gebruiker dus in het netwerk of het domein, maar kan hij nog geen diensten gebruiken of bronnen op het netwerk raadplegen. Hiervoor moet hij eerst toegang krijgen tot, dit noemen we authorisatie. Authorisatie bepaalt dus wat een gebruiker wel of niet mag doen met de bronnen op het netwerk. Typisch worden hiervoor rechten ingesteld op de verschillende netwerkbronnen aan de hand van Access Control Lists. Zo kan het zijn dat een gebruiker enkel leesrechten heeft tot een bepaald bestand op het netwerk, terwijl een andere gebruiker volledige rechten heeft. Op bestandsniveau worden deze rechten binnen Windows vaak ingesteld aan de hand van NTFS rechten.

5.2 Active Directory Domain Services

Objecten en LDAP

- AD is dus een verzameling van objecten
  - Verschillende types objecten
  - Elk object heeft bepaalde kenmerken (properties)
- Toegang tot informatie in directory via LDAP
  - Active Directory
  - OpenLDAP
- LDAP specifieke syntax om object te beschrijven
  bv.: “dn:CN=John Doe,OU=Sysadmins,DC=hogent,DC=be”
  - dn: DistinguishedName (unieke entry)
  - CN: Common Name object
  - OU: Organizational Unit
  - DC: Domain Component

} Zie verder

HO GENT

Objecten

Active Directory is dus een hele grote verzameling van objecten, en relaties tussen objecten. Er zijn verschillende types van objecten, en elk object heeft bepaalde kenmerken (properties). Je kan dit vergelijken met objecten van verschillende klassen binnen programmeren. Zo is er bijvoorbeeld een object van het type *User* met als eigenschappen onder andere *password* en *name*.

Binnen Active Directory kunnen objecten elkaar terugvinden via het Lightweight Directory Access Protocol (LDAP). LDAP wordt dus gebruikt om toegang te krijgen tot de informatie in een directory service, in dit geval over een netwerk. De 2 meest gekende directory services zijn Active Directory en OpenLDAP.

LDAP gebruikt een specifieke syntax om objecten te beschrijven. Een voorbeeld van deze syntax is “dn:CN=John Doe,OU=Sysadmins,DC=hogent,DC=be”. Hierin stelt *dn* de DistinguisedName voor (unieke identificatie van een object in de directory), CN de common name van het object, OU de Organizational Unit waartoe het object behoort (soort van folder), en DC de Domain Component (voorstelling naam van het domein).

We komen hier later nog op terug.

5.2 Active Directory Domain Services

Kerberos

- Protocol voor authenticatie
  - Gebruikt door LDAP
  - Maakt beperkte vorm van Single Sign-on mogelijk
  - Maakt gebruik van symmetrische encryptie
- Ontwikkeld door MIT
  - Gebaseerd op mythologische karakter Kerberos (driekoppige hond die toegang tot Hades bewaakte)
- Ingelogde gebruiker krijgt ticket, geldig voor sessie
  - Ticket vertrouwd door andere servers die protocol kennen
  - Bij uitloggen sessie afgebroken en is ticket niet meer geldig
- Kerberos is multi-platform
  - Unix, Linux, Windows, MacOS, ...

HO GENT

Kerberos

LDAP maakt gebruik van Kerberos, een heel veilig protocol voor authenticatie. Via Kerberos kunnen gebruikers zich dus op een veilige manier aanmelden op een netwerk, en hun identiteit bewijzen, zonder telkens opnieuw te moeten aanmelden wanneer ze een bron willen raadplegen. Kerberos maakt hiervoor gebruik van symmetrische encryptie, en maakt dus in beperkte mate Single Sign-on mogelijk (zie ook cursus Cybersecurity in de 1e bachelor).

Kerberos werd ontwikkeld door MIT en heeft zijn naam ontleend aan de driekoppige hellehond Kerberos uit de Griekse mythologie, die de toegang tot Hades bewaakte. De details van dit protocol vallen buiten de scope van deze cursus, maar in essentie krijgen gebruikers die ingelogd zijn een soort van ticket dat geldig is voor de sessie. Dit ticket kunnen ze dan gebruiken om diensten van andere servers te gebruiken, elke server die het Kerberos protocol kent kan de geldigheid van het ticket verifiëren. Wanneer een gebruiker uitlogt wordt de sessie afgebroken en is het ticket niet langer geldig.

Kerberos is beschikbaar op vrijwel alle computerplatformen, van Unix en Linux tot

Windows en MacOS. Ook andere systemen zoals het Oracle DBMS ondersteunen Kerberos voor het regelen van de toegang tot relationele databases.

5.2 Active Directory Domain Services

Kerberos

Je kan de werking van Kerberos vergelijken met een festival:

- Aan de hoofdingang koop je een ticket (authenticatie)
  Hoofdingang = Key Distribution Center (KDC) in Kerberos
- Ticket (bv. geel bandje) geeft je toegang tot alle concerten van die dag
  Ticket = Ticket Granting Ticket (TGT) in Kerberos
- Voor bijwonen concert krijg je een ander ticket, hiervoor moet je geel bandje (TGT) tonen. Dit moet je doen voor alle concerten die je wil bijwonen.
- Ticket is maar één dag geldig, morgen andere kleur
  TGT is dus maar beperkt geldig

HO GENT

Kerberos

Je kan de werking van Kerberos wat vergelijken met een festival. Als je toegang wil tot het festival koop je eerst aan de hoofdingang een algemeen ticket. Dit is de authenticatie binnen Kerberos. Aan de hoofdingang controleren ze dus of je betaald hebt en zo ja krijg je bijvoorbeeld een geel bandje dat je toegang geeft tot alle concerten van die dag. Binnen de Kerberos terminologie is de hoofdingang de Key Distribution Center (KDC) en het gele bandje is het Ticket Granting Ticket (TGT).

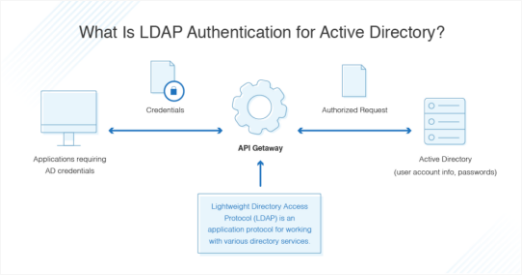
Als je dan een concert wil bijwonen (= een service gebruiken) moet je aan de ingang van het concert een ander ticket aankopen, en dit moet je doen voor elk concert. De persoon die de tickets uitdeelt voor een concert ziet jouw geel bandje en weet zo dat je recht hebt op een ticket. De TGT zorgt er hier dus voor dat je andere tickets kan krijgen, vandaar de naamgeving.

Aan het einde van dag sluit de festivalweide, en vervalt de geldigheid van jouw gele bandje (TGT). De volgende dag gebruikt het festival bijvoorbeeld een andere kleur van bandjes, en zal je dus een nieuw bandje moeten kopen aan de hoofdingang als je opnieuw toegang wil.

Merk op dat jij als gebruiker hier al het werk moest doen, door eerst een bandje te kopen en daarna dit bandje te tonen voor elk concert. Er is dus geen rechtstreekse communicatie tussen de verschillende partijen (hoofdingang en ticketverkopers van concerten).

AD en LDAP

- Active Directory = Directory Server
  - Database van objecten
- LDAP = toegang tot database
  - Manier om te communiceren met AD



HO GENT

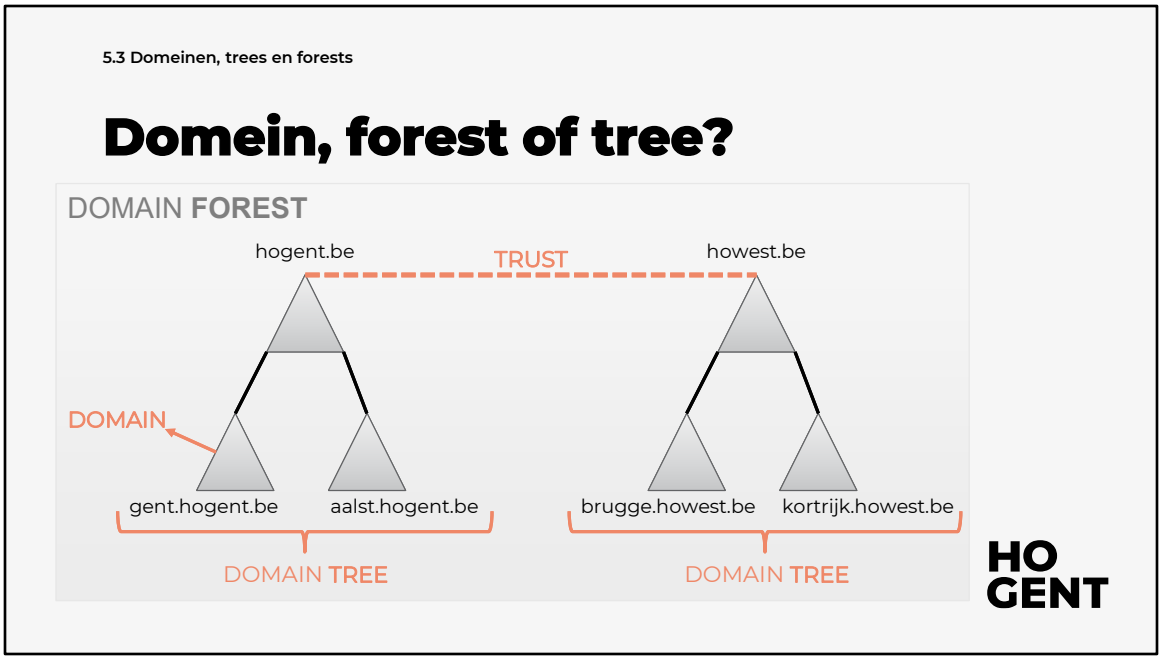
5.3 Domeinen, trees en forests

HO GENT

Domein, tree of forest?

Een domein is binnen Active Directory een logische groep van (netwerk)objecten zoals computers, gebruikers en andere toestellen die bewaard worden in dezelfde Active Directory database. Aangezien bij grote organisaties het aantal objecten snel kan oplopen kan een domein echter opgesplitst worden in verschillende subdomeinen die in aparte AD databases bewaard worden en waarbij verschillende domeincontrollers gebruikt worden voor elk subdomein. De verzameling van een domein en alle subdomeinen noemen we een tree (boom). Het opsplitsen van een domein heeft enkele voordelen: enerzijds is er de schaalbaarheid (gegevens worden verdeeld over verschillende databases die op verschillende servers bewaard worden), indien de organisatie kantoren heeft op verschillende fysieke locaties kan de AD server voor het domein lokaal geïnstalleerd worden wat de performantie ten goede komt, en binnen elk domein kunnen de rechten nauwkeurig ingesteld worden. Doordat de verschillende subdomeinen met elkaar verbonden zijn kunnen gebruikers van één subdomein diensten gebruiken binnen een ander subdomein in dezelfde tree. Alle subdomeinen moeten echter tot dezelfde namespace behoren, zo kan het domein hogent.be bijvoorbeeld opgesplits worden in twee subdomeinen aalst.hogent.be en gent.hogent.be.

Een tree (domein en subdomeinen) kan echter ook nog verbonden worden met een andere tree. Tussen beide trees wordt er dan een trust relationship gedefinieerd die vastlegt wat gebruikers van de ene tree kunnen doen met de bronnen van de andere tree. Aangezien beide trees vaak toebehoren tot andere organisaties, is dit noodzakelijk: je wil namelijk niet dat een gebruiker binnen organisatie X zomaar volledige toegang heeft tot alle bronnen van organisatie Y. De verzameling van meerdere trees (en hun trust relationships) noemen we een forest (woud). Binnen een forest heeft elke tree zijn eigen namespace (zie ook volgende slide).



Domein, tree of forest?

Deze slide illustreert een (domain) forest dat bestaat uit twee (domain) trees: hogent.be en howest.be. Beide trees zijn nog eens opgesplitst in meerdere subdomeinen (merk op dat dit niet noodzakelijk is!). De trust relationship bepaalt bijvoorbeeld tot welke bronnen binnen howest gebruikers van hogent toegang hebben.

In deze cursus zullen we voorlopig werken met een forest dat bestaat uit maar één tree en deze tree bestaat uit één domein. In de bedrijfswereld zal je echter merken dat meerdere domeinen en trust relationships vaak gebruikt worden binnen grotere organisaties.

5.4 Redundantie

HO
GENT

Redundantie en FSMO

- Binnen één domein mogelijk om meerdere DCs te hebben voor redundantie
- Multi-master: aanpassingen mogelijk vanaf elke DC
  - Kan echter leiden tot conflicten
  - In geval van conflict: laatste aanpassing wint
- Single-master: één DC voor aanpassingen
  - Vroeger (NT4.0): Primary Domain Controller (PDC) rol
  - Nu: Flexible Single Master Operations (FSMO) rollen
  - Er zijn 5 FSMO rollen

HO GENT

Redundantie en FSMO

Binnen één domein kan je meerdere domeincontrollers (DCs) opzetten voor redundantie. Wanneer één domeincontroller offline gaat, kunnen gebruikers nog steeds aanmelden via een andere domeincontroller. Binnen Active Directory wordt hiervoor zowel een multi-master als een single-master model gebruikt. De domeincontrollers wisselen alle gegevens van het domein uit met elkaar via een synchronisatie (zie cursus Operating Systems).

Multi-master wil zeggen dat je bepaalde aanpassingen in de database kan uitvoeren vanaf elke domeincontroller. Dit kan echter leiden tot conflicten wanneer je bijvoorbeeld op twee domeincontrollers gelijktijdig zaken zou aanpassen. Binnen AD is het zo dat, bij conflicten, de laatste aanpassing wint. Als je op DC 1 bijvoorbeeld de naam van een gebruiker wijzigt naar X, en op DC 2 een seconde later de naam van dezelfde gebruiker wijzigt in Y, dan zal enkel de naam Y bewaard worden – alle voorgaande aanpassingen worden dus genegeerd.

Single-master wil zeggen dat AD voor bepaalde objecten de updates of aanpassingen laat uitvoeren door één domeincontroller. Vroeger (in Windows NT 4.0) noemden we

deze server de Primary Domain Controller of PDC. Deze server was toen verantwoordelijk voor alle updates binnen het domein. In recentere versies van Active Directory is deze rol echter opgesplitst in meerdere rollen, en deze kunnen verdeeld zijn over meerdere servers. Daarom spreken we nu over Flexible Single Master Operations (FSMO) rollen, en er zijn 5 FSMO rollen die op de volgende slide kort besproken worden.

FSMO rollen

De **Schema master** is de enige domeincontroller die updates kan doen aan het directory schema. Het directory schema legt de vorm en structuur vast van de objecten binnen Active Directory. Wijzigingen aan het schema worden nadien gerepliceerd naar alle andere domeincontrollers.

De **Domain Naming master** is verantwoordelijk voor de forest-wide domain name space. Dit is de enige domeincontroller die een domein kan toevoegen of verwijderen in de directory.

De **RID master** wordt gebruikt voor het verplaatsen van objecten naar een ander domein. Elk object binnen Active Directory heeft een SID (Security Identifier) dat bestaat uit de SID van het domein (dus hetzelfde voor alle objecten binnen het domein) en een RID (relative identifier) dat uniek is voor elk object binnen het domein. De RID master zorgt dus voor aanmaken van deze SID, en er is één RID master per domein binnen de forest.

De **PDC emulator** wordt hoofdzakelijk gebruikt voor time synchronization. De naam

zelf verwijst naar de oude PDC (primary domain controller) naam. De forest PDC emulator krijgt de huidige tijd via een externe bron, en per domein is er een PDC emulator die luistert naar de forest PDC emulator.

De **Infrastructure master** gaat de update doen van de SID van een object alsook de DN wanneer het object vanuit een ander domein wordt benaderd.

5.4 Redundantie

Global Catalog

- Belangrijkste rol in AD!
- Elke DC kan deze rol uitvoeren
- Global Catalog bevat alle objecten binnen forest
  - Complete kopie van objecten eigen domein
  - Gedeeltelijke kopie van alle objecten andere domeinen
- Wordt gebruikt om objecten te vinden in forest
- Voor load balancing: maak van elke DC een GC

HO GENT

Global Catalog

Naast de 5 FSMO rol bestaat er nog een rol: de Global Catalog (GC). Elke domeincontroller binnen Active Directory kan deze rol (gelijktijdig) uitvoeren, en de global catalog is de allerbelangrijkste rol binnen Active Directory.

Een domeincontroller die de GC rol heeft maakt een catalogus aan die alle objecten binnen de AD forest bevat. Deze catalogus bevat enerzijds een volledige kopie van alle objecten in het eigen domein, en een gedeeltelijke kopie van alle objecten binnen de andere domeinen in de forest.

Via de GC kunnen gebruikers en programma's objecten terugvinden in de hele forest door te zoeken naar hun attributen in de global catalog. Voor load balancing doeleinden is het aangeraden om op elke domeincontroller de Global Catalog rol toe te voegen.

5.5 Promotie tot DC

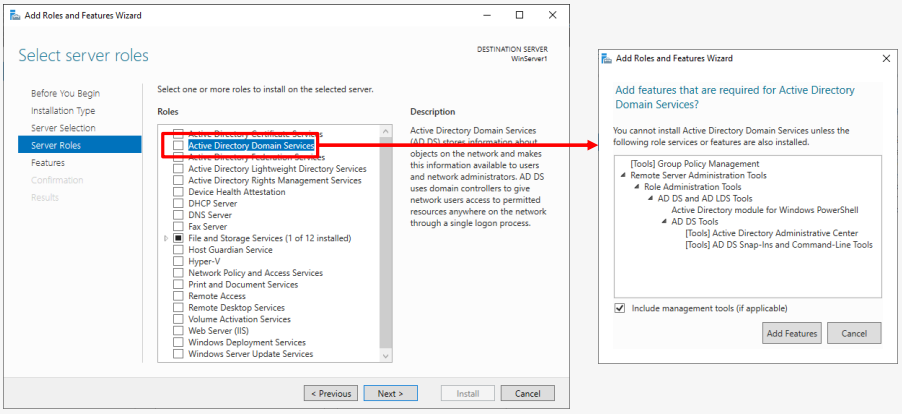
HO
GENT

Promotie tot DomeinController

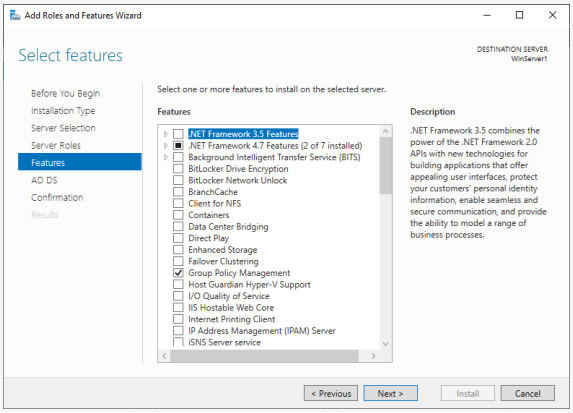
- Eerst Active Directory Domain Services installeren
  - Via Server Manager
  - Dit installeert ook DNS (indien nog niet geïnstalleerd) en de nodige management consoles
- Na installatie AD DS kan je de server promoveren tot DC
  - Indien eerste DC: aanmaken forest en domain
  - Je kan selecteren welke AD rollen je wenst toe te kennen aan de DC

HO GENT

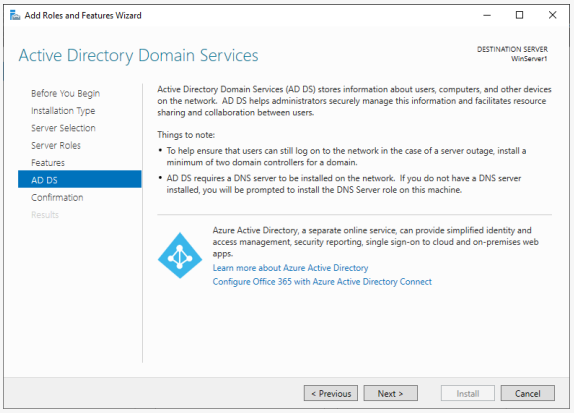
5.5 Promotie tot DC

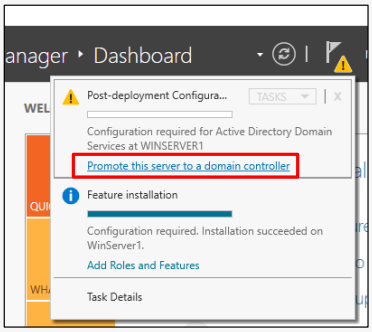


5.5 Promotie tot DC

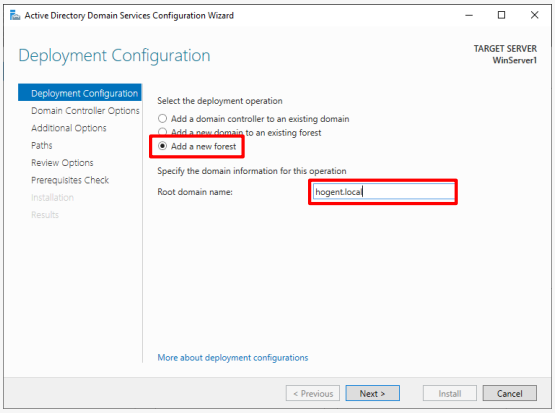


5.5 Promotie tot DC

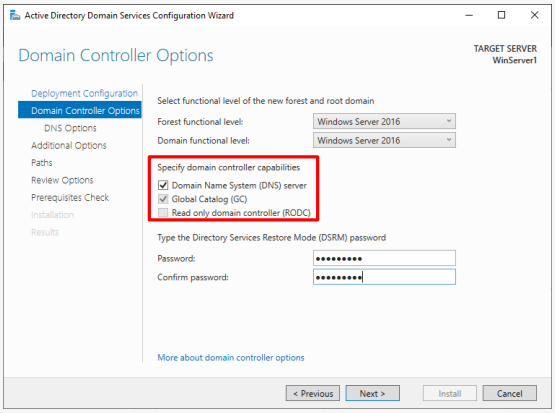


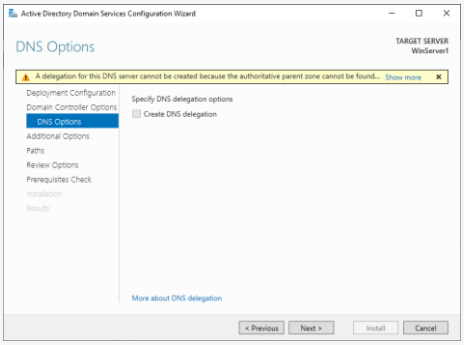


5.5 Promotie tot DC



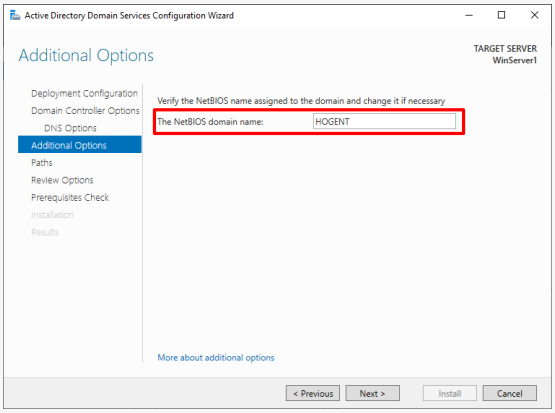
5.5 Promotie tot DC

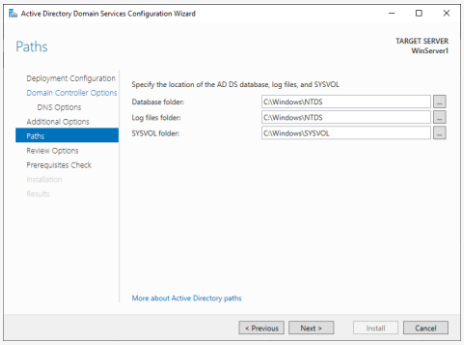




HO GENT

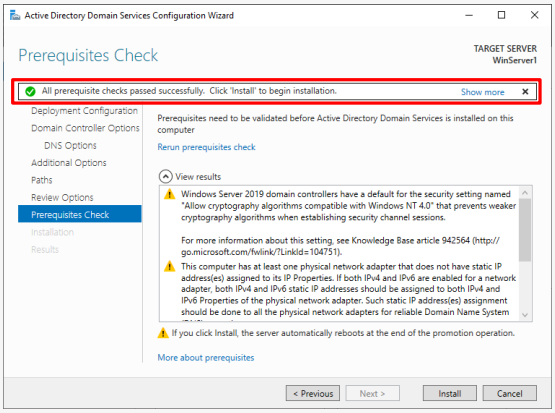
5.5 Promotie tot DC

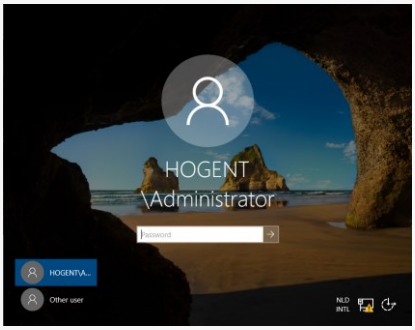




HO GENT

5.5 Promotie tot DC



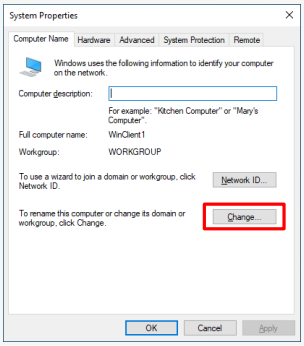


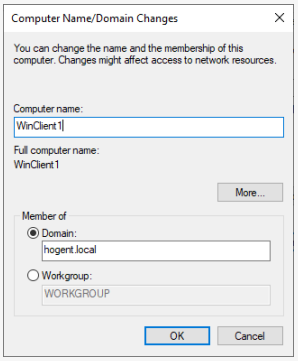
Toevoegen toestel aan domein

- Via System Properties kan je de naam wijzigen en een toestel lid maken van het domein
  - Open een Run venster (Win + R)
  - Typ **sysdm.cpl** en druk op OK om System Properties te openen
  - Klik in System Properties op Change… om de naam en/of het domein te wijzigen
- Voor toevoegen aan domein moet je account gebruiken van Domain Administrator
  - Voor onze labo's is dit HOGENT\Administrator
  - Bovendien moet de client de DC kunnen bereiken, en deze als DNS server gebruiken (controle via **ipconfig** of **ncpa.cpl** + **ping**)

HO GENT

5.5 Promotie tot DC

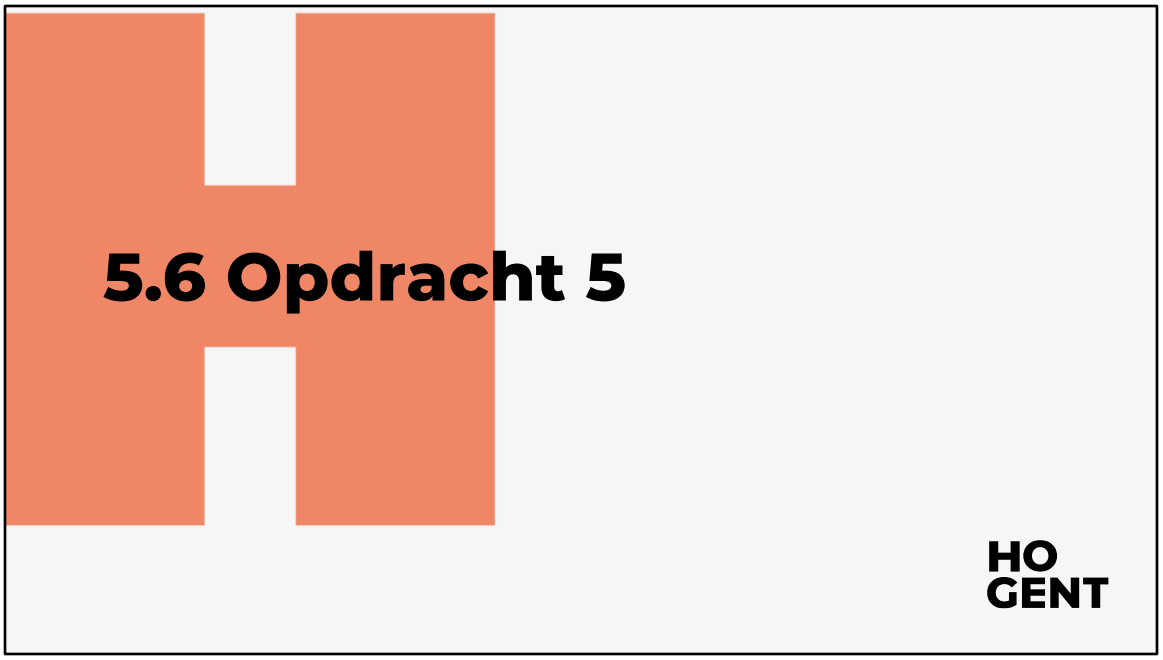




Belangrijk:

Client moet onze DC gebruiken als DNS server!

Je kan dit indien nodig wijzigen via ncpa.cpl


5.6 Opdracht 5
HO
GENT

Opdracht 5

- Installeer de AD DS rol in Windows Server 2019
- Promoveer de server tot domeincontroller
- Verken de Microsoft Management Consoles (MMCs)
- Maak de Windows 10 client VM lid van het domein
- Voeg een reverse lookup zone toe in DNS voor LAN netwerk
  - Voeg ook de nodige PTR records doe voor WinServer1 en WinClient1

Zie het document op Chamilo voor meer details

HO GENT