OS Advanced

Inhoud

- DNS concepten en werking
- Active Directory
  - Concept: directory services
  - Architecture
  - LDAP protocol
  - DNS & AD integration
  - Global Catalog
  - Access control
  - Group policy
- Email services
- VPN SSL SSH

Les 2: 19/02/20

DNS

Slide 31: vergeet client niet te laten wijzen naar DNS server

Slide 32: Je kan 2 DNS servers instellen: één voor intern, één voor extern

➔ Met DNS forwarding kan je een request van de ene DNS doorsturen naar de andere DNS als het niet binnen de zone van de eerste DNS valt.

Slide 37: forwarding zegt niks over authoritative of non-authoritative

Forward zone: naam in IP vertalen

Slide 39: je moet toestemming geven op de secundaire zone om hier een copy van te maken.

Slide 40: eenmaal dat de gebruiker de IP van de webserver weet, gaat het rechtstreeks met deze server verbinden. Dus dan is er een extra pijl nodig van ClientcPC -> WEB server 1

IPv6 is de “prefferd protocol”, daarna naar IPv4

Slide 42: eerst zone aanmaken, dan kan je het pas delegeren. Data van web.mycompany.com wordt op zijn eigen DNS bewaard. Dit is dan voor deze zone de primaire DNS.

Slide 44: alles op een Windows server is verdeeld is rollen.

Slides 59 en 60 zijn niet aan bod gekomen.

Active Directory

Slide 3: eenmaal inloggen, daarna krijg je een token die aangeeft waar je toegang tot krijgt.

Authenticatie is niet hetzelfde als autorisatie

Slide 5: niet van buiten leren

➔ Ntdis.dat file niet deleten

Slide 9: alle domain controllers zijn gelijk.

Slide 9: OU organisatie onderverdeling (Organisational Unit)

Slide 10: alles verbonden in driehoek met policies.

Slide 14: enkel “global catalog” als het internetverbinding goed is. Bij slechte verbinding wil je dit niet en zal het dataverkeer beperkt worden.

Slide 15: “domain controller” kan je vinden door DNS

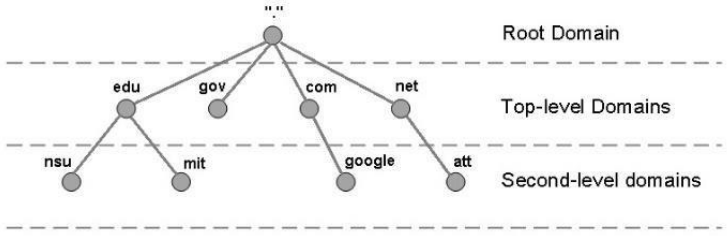
Slide 16: hiërarchische structuur van domeinen

Les 3: 26/02/2020

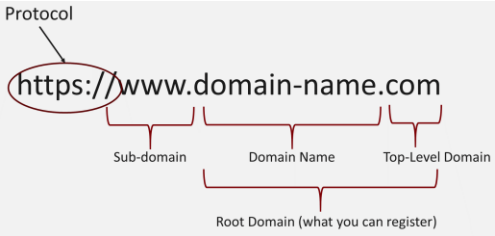
Niet aanwezig

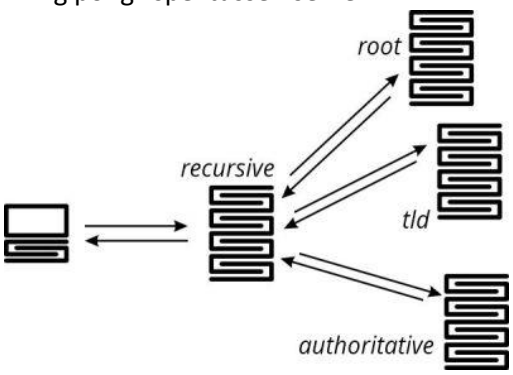
Hoofdstuk 1: DNS

- Domain Name System
- Niet wanneer DNS is ontworpen
- Naam van iets vertalen naar een IP adres van een server
    - Makkelijker namen onthouden
- **Request-response** principe
- **Hiërarchische structuur**



    - Root DNS servers
        - 13 fysieke server
        - Managed by ICANN organization
        - Verwijzen door naar TLD servers
    - Top-Level-Domain (TLD) DNS servers (.com, .org,…)
    - Sub-domain DNS servers (second-level and lower)
        - somecompany.com, google.com, …
- Van achter naar voor lezen, **boomstructuur**



- Wat zijn zones in een DNS?
    - Een zone is een deel van een domain in de DNS waar de administratieve verantwoordelijkheid is overgedragen aan een persoon of bedrijf.
        - Vb.: In de root DNS staan verschillende zones (.com, .be, …). Deze zone worden beheerd door de TLD beheerders. Deze hebben dan weer verschillende zones zoals reactr, google, …
- Concept van root servers
- **Verschil tussen authoritative en non-authoritative**
    - Authorative name servers
        - Can only reply with an IP address
    - Non-authoritive name servers
        - Refer to other name servers, per domain
- Was is **name resolution**
    - Vertalen van naam naar IP adres
        - Van URL naam naar IP
        - Van server naar IP bij het zoeken naar een netwerk toestel (WINSERVER-1)
    - **DNS resolver** is deel van besturingssyteem, deze is als eerste gevraagd
        - Caching en **hosts file (zowel op unix, linux als windows**)
- **Recursive resolution**
    - Geef eens een voorbeeld, wat is het
    - Door de schaal van het internet kan de name resolution niet worden gedaan door één server
    - Uitleg
        - Dns server nodig want zit niet in cache en hosts file
        - Netwerk instellingen van adapter
        - DNS van netwerk provider
        - Root nameserver
        - …
        - Tenzij er in de cache onderweg al iets gevonden worden
        - “Ping pong” spel tussen server
        - 

- Netwerk instellingen
- Caching is berperkt in tijd

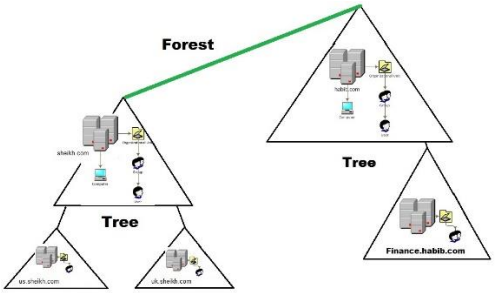
    - niet voor eeuwig
    - Time to live
    - Versnelt wel het process en zorgt voor minder verkeer op het internet
- Wat is een reverse lookup? Waarom gebruiken we die?
    - Vertalen van IP naar naam
    - Gebruikt in:
        - Spam filters: domeinnamen blokkeren
        - Bij het loggen is het makkelijker om met naam te werken
        - White listing
- Waar zitten de bestanden?
    - In een database bestaande uit records
        - Types:
            - **A**: IPv4
            - **AAAA**: IPv6
            - **NS**: name server
                - Geeft de authoritative nameserver voor een specifieke zone
                - Moet altijd samengaan met een A of AAAA record
            - **SOA**: start of authority
                - Identificeert de primaire DNS server voor een zone
            - **MX**: mail exchange
            - **SRV**: service record, vb.: active directory
            - **PRT**: pointer, gebruikt bij reverse DNS
- Wat is een host record?
    - A records of host record
- Name server record
    - Welke nameserver is authorative voor die zone?
- SOA: start of authority
    - Drie traps verhaal
        - SOA -> NS
        - NS -> A record
        - A record -> IP
- MX en SRV: gaat over services
    - DNS ook voor bepaalde services
    - Active directory service
    - Mx: voor het email domain
    - PTR en TXT zijn minder belangrijk
- **DNS forwarding**
    - Voorbeeld mag je aanhalen: slide 35
    - Doorgeven naar andere DNS als het niet binnen het domein ligt
    - Voor alles wat ik niet in mijn database vindt, verwijs ik door
    - Kan ook conditioneel (voor bepaalde name, …)
- DNS zone types
    - Primaire zone → geeft authoritative antwoord
    - Secundaire zone (read only, one way)
        - Copy van primaire zone
        - Indien de primaire DNS faalt
    - **Zone transfer**

        - Regelmatig copy van primaire naar secundaire
        - Full transfer: alle records worden gekopieerd
        - Incremental transfer: enkel de gewijzigde records worden gekopieerd
- **Zone delegation**: een deel van uw werk verdelen (delegeren) naar een andere server
    - Is beter voor load balancing van grote domeinen
    - Is makkelijker als branch offices hun eigen zone kunnen beheren
    - Zone data (DNS records) for the delegated zone can only be edited on the server to which the zone was delegated
        - Is the authorative server for the delegated zone
- DNSBL (detail, bijvragen)
    - DNS Blacklisting
    - DNS bevat lijst met IP adressen
- DDNS
    - Dynamic DNS
    - IP adressen veranderen regelmatig → DNS records moeten worden aangepast
- Domain registrars
    - Informatie over van wie het domein is
- Gevaren
    - DDos: Distributed Denial of Service
        - "bombard" DNS server with requests, trying to get it down
    - Address spoofing, Cache poisoning
        - Replacing an authentic address by a fake address
        - Purpose: redirect traffic to a malignent website (fake online-banking site or webshop)
- Slide 60 niet kennen

Hoofdstuk 2

- Waarom AD?
    - Centralisatie (recources, users en policies, …)
    - SSO
- Wat is het (SSO)?
    - Single Sign-On
    - Eenmaal inloggen, daarna krijg je een token die aangeeft waar je toegang tot krijgt
    - Authenticatie is niet hetzelfde als authorisatie
- Achtergrond van het verleden niet kennen (slide 7)
- Domains
- Domain controller
    - Bevat een database met AD objecten
    - **Multi master replication**
        - Meerde machine zijn beheerders over de data
        - Je kan het op eender welke DC beheren
        - Maar niet alles kan op alle DC
            - Zoals schema beheer
            - Inhoud van de DB kan je op elke DC doen
- Global catalog (zie verder)
- Authentication
    - Gebruikers moeten inloggen in domein

- **Forest**: groepering van domains die elkaar kunnen vertrouwen
    - Kan ook naast elkaar
    - Automatisch trust tussen domain in forest (two-way trust)
        - Does not imply authorization
    - Alle domeinen in een forest delen het AD schema
    - hiërarchische structuur van domeinen



- **Schema**: definitie van de object, zegt welke velden er zijn, blauwdruk voor een object, structuur van een object
    - Mag je dat zomaar bewerken?
        - Ja, alleen op de schema master
    - Een veld in een schema noemt men ook een **attribuut**
- **Domain functional level**
    - Bij gebruik van verschillende oudere servers in een forest
    - Forest beperken tot degene met de minste mogelijkheden
    - Zwakste wint
- DNS deligation in kader van AD niet kennen
- Elke server heeft een unieke SID
- Sysprep details niet kennen (slide 48)
- Replicatie: binnen één site, gaat die replicatie heel snel gebeuren
    - Kan je ook forceren
    - Kan je ook filteren
- Auditing
    - Event log
    - Alles kan worden gelogd
- Organisatorische structuur met OU en sites
    - Functionele kijk
        - Domains and OU's are functional views of the organization
            - Domains and OU's can contain resources from different physical locations
            - One physical location can contain resources from different domains or OU's
        - They contain resources that belong together from an administrative or even security standpoint
    - Fysieke kijk (**subnets**, kantoren op verschillende locaties, …)
        - **Sites**
            - This represents a physical location
            - Intended to let AD know where the resource is located
            - For authentication and replication purposes
    - Wat is een OU?

        - Organizational Units
        - Laat toe dat er fijnere controle is over objecten dan in een heel domein
        - Veel flexibeler dan een domein: makkelijk OU's verwijderen of toevoegen
        - Kunnen in elkaar worden gezet
        - Je kan de controle over een OU deligeren aan een group of user (remote team)
- Replicatie tussen DC
    - Domains are managed via Domain Controllers in a multi-master replication scheme
        - Any change on any DC is replicated to the other DCs
        - Between DCs in the same site (default), this replication is done asap (within 1 minute) upon any change
        - This is not desirable when there is a slower network connection between DCs → andere schedule met meer tijd tussen de replicaties
            - **Cost**
                - Slower links get a high cost
                - The links with a lower cost are used by preference
                - This way, redundant links can be set up

Les 4: 4/03/2020

- Group policies is een van de krachtigste elementen van active directory
- Wat is een group policy?
    - Een verzameling van user en computer configuraties
    - Group policies op zich doen niks, je moet het ergens op toe passen -> link maken
    - Kan je centraal beheren
    - Vb.: password policy -> wachtwoord moet minstens 10 karakters hebben
    - Vb.: welke applicaties er kunnen gebruikt worden
- Slide 10: **examen**!!!!
    - Computer: onafhankelijk van de gebruiker
        - Wordt toegepast als de computer opstart
    - User: onafhankelijk van de computer
        - Wordt toegepast als de gebruiker inlogt
- Hiërarchie
    - Software settings
        - Policies voor het installeren van software, updaten …
        - Aangeven welke programma mogen worden gebruikt
    - Windows settings
        - Instellingen voor het Windows OS
        - Uitvoeren van scripts
        - Security instellingen
            - wachtwoordinstellingen
    - Administrative templates
        - hiermee kan je registers forceren
        - Vb.: instellingen van FireFox beheren
- Slide 19: weten wat het is, maar zelf niet gebruiken
- Slide 20: niet van buiten leren
- Slide 22: gewoon bekijken

Belangrijk: verschil tussen computer en user configuration

- GPO: group policy object
    - Doen opzich niets zonder link
    - Wordt toegepast op alle onderliggende objecten
- Hoe dichter bij de gebruiker (specifieker), hoe meer de voorrang
    - Site -> domain -> OU
    - Je kan dit controleren met RSoP (Resultant set of policies)
- Hierarchy
    - Eerst lokaal
    - Dan bij aanmelden op AD nemen die policies het over

Belangrijk: hiërarchie en overerving

- Hoe lager in de hiërarchie (hoe specifieker), hoe meer voorkeur
- "last writer wins"
- Overerving kan worden geblokkeerd of worden geforceerd
- LSDOU
    - Local
    - Site
    - Domain
    - OU
- WMI: filter op computer
    - Kan beperken op welke toestellen de GPO's moeten worden toegepast afhankelijk van de eigenschappen van de computer (OS, CPU, …)
    - Vb.: enkel toepassen op toestellen met een bepaald besturingssysteem
- Security filter: filter op gebruiker
    - Aangeven op welke gebruikers de GPO moet worden toegepast
    - **Deny wint van Permit** omdat het beter is als de GPO wel wordt toegepast
- Policy wordt niet direct toegepast bij een wijziging
    - Enkel bij opnieuw opstart
    - Of om de zoveel minuten
    - Dit kan je ook forceren met een cmd commando

Les 5: 11/03/2020

Laatste stuk van vorig hoofdstuk (vanaf slide 89)

- OU is een onderverdeling van Domains
- OU kan je makkelijk hernoemen, Domains is veel moeilijker
- Fysieke locatie kan je inbrengen met *sites* en *recources*
    - Vb als een gebruiker inlogt in Japan, zal het eerst op zoek gaan naar een domain controller in Japan (je wil een domain controller die fysiek dicht bij staat)
- Recources koppelen aan bepaalde sites met subnets
    - Bepaalde ip bereiken zullen gelinkt zijn aan bepaalde sites
- Alle domain controller zijn gelijkwaardig: multi-master
    - De meeste wijzigingen kan je op eender welk DC doen en zullen worden gerepliceerd op de andere controllers (er zijn enkele uitzonderingen)
    - Repliceren gaat heel snel

- Repliceren tussen verschillende sites willen we vaak niet: inter-site replication
- Cost: de voorkeur voor de lijn bepalen; hoe lager de kost, hoe meer de voordeel

Verder met vorige les over group policies (vanaf slide 44)

- GPO eerst maken, maar daarna nog linken met domain controller
- GPO bestaat uit twee stukken: gebruiker en groep instellingen
- Uitzondering op OU (vb.: IT team moet 20 karakter wachtwoord hebben maar de andere gebruikers maar 15)
    - aparte GPO voor die OU
    - filter maken op GPO (speciale filter voor IT team)
- Bij conflicten met GPO's zal de strengste winnen (deny wint van allow)
- Je kan software op verschillende PC's installeren
    - msi-bestand te delen
    - GPO aanmaken -> software settings
    - GPO linken en user configuaration settings disbled
        - Hierdoor zal het niet door de user settings lopen
        - Gaat veel sneller als er veel gebruikers zijn
- **Loopback processing**: als een gebruiker andere instellingen wil als het op een andere computer werkt
    - Computer instellingen zijn per gebruiker
    - Wat als je voor een gebruiker op een bepaalde computer andere instellingen wil?

➔ Loopback processing

- Vb.: achtergrond voor een bepaalde gebruiker als het met een bepaalde computer werkt (slide 63 – 67)
- User instellingen worden toegepast op een computer alsof het computerinstellingen zijn.
- Loopback processing modes
    - Replace
        - Er wordt niet gekeken naar de user instellingen
    - Merge
        - Beiden worden bekeken
        - Indien conflict worden de computerinstellingen gebruikt

- GPO processing sequence: hoe dichter bij de gebruiker, hoe belangrijker
    - Computer
        - Local
        - Site
        - Domain
        - OU
    - Scripts
    - Loopback
    - User
    - scripts
        - Local
        - Site
        - Domain
        - OU
- **Overerving werkt niet tussen domein en subdomeinen**
- Local Group Policy

    - 3 levels:
        - Local computer policy
        - Administrators and non-administrators local group policy
            - In deze lag kunnen geen computerinstellingen worden gedaan
        - User-specific local group policy
            - In deze lag kunnen geen computerinstellingen worden gedaan

Les 6: 18/03/2020 (online)

- Slide 88: wat onthouden
    - hoe dat groep policies werken op een bepaald niveau
    - User account (Dave) blijft altijd op de California site, zelfs als hij inlogt in New York
    - Computer instellingen zullen wel locatie afhankelijk te zijn

User profiles

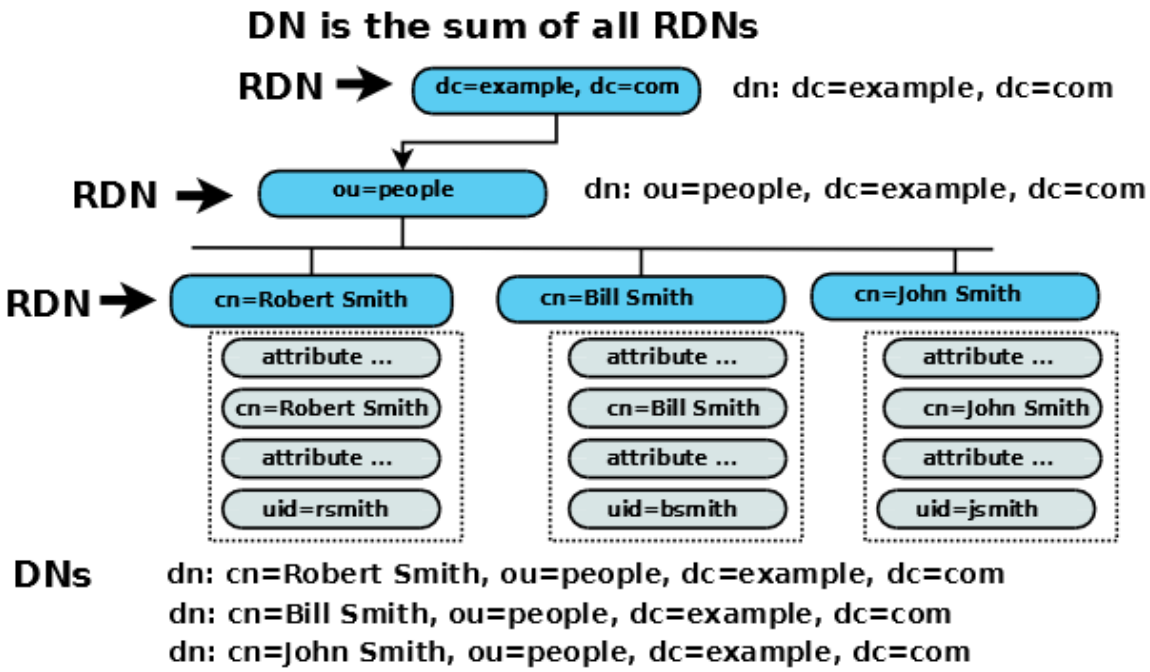
- Je kan zelf instellingen doe aan je computer
- Je kan er voor zorgen dat je gebruikersinstellingen je volgen
- Als je ergens anders inlogt, worden deze instellingen teruggezet
- Slide 113: voorbeelden (niet van buiten leren)
- Types
    - Local user profile
        - Eerste keer bij het aanmelden krijg je een scherm dat hij instellingen is aan het aanmaken
        - Gelden enkel op de gebruikte computer
    - Roaming user profile
        - Betekent “rondreizen”
        - Lokale profiel wordt gesynchroniseerd op laptop
        - Werkt nu binnen een domein
    - Mandatory user profile
        - Als administrator kan je bepaalde instellingen vastleggen die voorrang gaat krijgen
    - Temporary user profile
        - Dit is een tijdelijk profiel
        - Alle veranderingen gaan verloren bij het afmelden van die account
- Voordelen
    - Instellingen volgen je
    - Je kan niet de instellingen van anderen veranderen
- Waar kan je deze instellingen vinden?
    - Instellingen -> systeem -> about -> system properties -> user profile settings
    - Dit kan je afschermen via group policies

Kennen: linken, wat het is, hoe gebruiken, wat voorrang krijgt op wat, wat de types zijn, …

Hoofdstuk: Active Directory – LDAP

- Wat gebeurt er achter de schermen
- LDAP: **lightweight directory access protocol**
- Dit is een protocol dat ook met andere systemen goed kan samenwerken omdat Microsoft dit protocol gewoon heeft overgenomen zonder aan te passen

- **Protocol als basis voor AD dat beschrijft hoe gegevens uit AD benaderd kunnen worden**
- Het is een directory service
    - Directory: een inventaris
    - je kan er dingen van opvragen en wijzigen (query)
- heeft ook een **hiërarchie**:
    - root directory
        - organization
            - Ou …
- LDAP Directory
    - = database
    - LDAP kan op verschillende server worden gezet
    - Bij domains staat alle data op elke server, bij forest moet dat niet altijd zo zijn
    - LDAP directory server = **Directory System Agent** (DSA)
    - Als een DSA een query niet vind, zal het deze query doorsturen naar een andere DSA (zoals DNS)
- LDAP directory bevatten objecten
    - Attributen: naam, voornaam, …
    - Elk object heeft een unique identifier
        - **Distinguished Name** (DN)
            - Hoofdletter ongevoelig
        - **Relative Distinguished Name** (RDN)
- Slide 6: je zou dit ook kunnen zetten als JohnDoe@example.com
    - Lijst van domain components van bodem naar top
    - Binnen example.com is er maar één John Doe
    - Er kunnen er wel meerdere zijn, maar niet op example.com
    - RDN: John Doe is relatief t.o.v. example.com
    - DN specifieert een object
- Een hele directory in LDAP = directory information tree



AD schema

- Beschrijft een object (net zoal in LDAP)
    - Attributen (=velden)
    - Nieuwe velden kunnen worden toegevoegd
        - Alle objecten van het schema zullen de nieuwe velden krijgen
        - Niet iedereen kan het schema aanpassen, kan enkel op de schema master
- Beschrijft de definitie van de objecten (een lege formulier), uit welke eigenschappen bestaan de objecten, de template, wat zit er in een object, …
    - Vb.: de gebruiker heeft als velden voornaam, achternaam, adres, …
    - De objecten zelf worden in een database (tabel) bewaard
- LDAP: hiermee kan je gegevens opvragen en opslaan
    - Beschrijft een hele directory en waar alles zich bevindt
    - Alle objecten hebben een unieke naam (DN en RDN)
    - RDN = een unieke naam binnen een bepaald niveau
        - Slide 12: Jane Doe is uniek op Domain_name/Users/Sales/Managers/
        - Attributen:

Distinguished name attribute	Meaning
C=	Country/region
CN=	Common name
DC=	Domain component
L=	Location
O=	Organization
OU=	Organizational unit

- Elke object in AD heeft verschillende identifiers (slide 16)
    - **Security principal name** (slide 17)
        - Security principal is een object, iets waar je security op kan definiëren
        - Krijgt in de achtergrond een unieke **SID** (security ID)
        - Security principal name = naam die een unieke gebruiker, computer of groep kan identificeren binnen één domein
        - Security principal moet geauthenticeerd worden op een DC (domain controller) om toegang te bepaalde recources te verlenen
        - Deze naam kan worden gewijzigd
    - **Security identifier** (SID)
        - Kunnen nooit worden gewijzigd
            - Anders de uniekheid in gedrang brengen
        - Bij het verwijderen van een gebruiker en daarna de gebruiker weer toevoegen, zal de SID verschillend zijn
            - Voor als er nog ergens een link was naar de oude ID …
    - **Relative identifier** (RID)
        - Laatste stuk van SID van een object
            - Object SID = Domain SID + Object RID
        - Moet uniek zijn binnen het domain
        - SID moet uniek zijn binnen heel de Active Directory
        - Parallel trekken met LDAP (DN en RDN)
        - **Access control entry** (ACE)
            - Elke AD object is beschermd door één of meerdere ACE’s

                - De ACE bepaald wie het object mag lezen, schrijven, bewerken, …
                    - Er wordt hierbij gekeken naar de SID
                    - Verwijst achter de schermen naar SID en beschrijft wat die SID kan en niet kan
        - **LDAP name**
            - In AD wordt achter de schermen verwezen naar de LDAP name
            - Full path = DN of the object
            - Each segment of the path = RDN
            - Elke RDN is opgeslagen is een AD database
                - Elke RDN verwijst naar zijn parent
                - Elke RDN moet uniek zijn op zijn niveau
            - Canonical name
                - Dit wordt gebruikt door Windows UI i.p.v. LDAP, maar dit wordt dan omgezet naar LDAP in de achtergrond
                - vb.: example.com/sales/testuser
                    - Example moet uniek zijn in .com
                    - Sales moet uniek zijn in example.com
                    - Testuser moet uniek zijn in example.com/sales
            - LDAP URL NAMES: LDAP://server.USRegion.Orgname.com/cn=JDoe,ou=Widgets,…
                - server.USRegion.Orgname.com is machine waar systeem op gelokaliseerd is
        - **Object GUID** (Globally Unique IDentifier)
            - SID is uniek in binnen een domein
            - SID wijzigt bij het verhuizen van object van een domein naar een ander
            - Is globaal uniek, kan NOOIT wijzigen
        - **Logon names** (slide 39)
            - **User principle name** (UPN) (slide 40)
                - Verkorte naam voor LDAP naam, en gebruikersvriendelijk
            - **Security Accountmanager** (SAM)
                - Hier krijgen we nu niet meer mee te maken (oude versie van windows)
                - Niet hiërarchisch maar plat → elke naam moet volledig uniek zijn in het domein
- Voorbeeld van de verschillende noties: slide 43!!!
    - /O=internet bestaat niet in AD, maar wel in standaard LDAP

Les 7: 25/03/2020 (online)

Remote acces

- Vanop afstand verbinden met een bepaald netwerk
- Er zijn twee bestaande systemen
    - Dial up networking (DUN) (wordt als back up gebruikt, is oud)
        - Gaat via het telefoonnetwerk
            - Slechte performantie door lage bandbreedte

                - Data omgezet in geluidssignalen
                - Meerdere modems in parallel
                - Simpele seriële verbinding -> twee draden
                - Geen TCP mogelijk -> enkel met point to point protocol (PPP)(slide 5)
                - Meerde telefoonlijnen combineren om meer bandbreedte te krijgen
                - RAS = Remote Access Server (slide 6)
                    - Server met verschillende modems
        - VPN
            - Virtual private netwerk
            - Communicatie gaat via het publieke netwerk
            - Communicatie afschermen van de buitenwereld -> tunnel -> rechtstreeks tussen twee **gateways** praten
            - Is niet altijd geëncrypteerd -> is geen synoniem met VPN
            - Virtueel lijn de gateways rechtstreeks met elkaar verbonden
            - 2 soorten VPN
                - Site-to-site VPN (slide 11)
                    - 2 sites met elkaar verbinden
                    - Clients weten niks van VPN
                    - Verbinding gaat tussen de gateways
                - Remote access VPN
                    - Gateways bevind zich op de client (VPN software)
- Eenmaal verbonden, moet het volledig transparant zijn -> gateways zijn niet zichtbaar

Hoe maak je een VPN met Windows Server?

- Nieuwe rol maken
- Direct Access -> Microsoft zijn draai aan VPN
- Zowel Direct Access als VPN gebruiken
- DHCP nodig om aan de client een IP adres op het intern netwerk te geven
    - Van domain controller ook DHCP server maken
- Twee netwerk interfaces maken
    - Één op het intern netwerk 10.1.68.x
    - Één op het virtuele netwerk 192.167.68.x

➔ Netwerkinterfaces een naam geven om verschil duidelijk te maken

- DHCP heeft *scope* voor beschikbare adressen
- RAS server moet ook authenticatie kunnen doen

Tunneling protocols

- Encapsulation -> twee protocollen in elkaar gebruiken
    - TCP/IP in het buitenste protocol (extern ip adres)
    - Daarin zit een pakket voor het intern netwerk
- Slide 30 -> niet van buiten kennen

Security aspect

- **CIA** (voorbeelden geven met de echte wereld (brieven, …))
    - **C**onfidentiality (via encryption)
        - Enkel de personen die toegang hebben mogen de data lezen
    - **I**ntegrity (data)

        - Ontvangen data moet gelijk zijn aan verzonden data
    - **A**uthentication (of sender)
        - Everyone is who they claim to be
        - Gebeurt in twee richtingen
    - Non-repudiation (one's intention to fulfil their obligations)
        - Handtekening zetten als je een brief hebt gekregen
        - Je kan dat niet meer ontkennen dat je het ontvangen hebt
        - Maar wat je ontvangen hebt, is nog iets anders
- SSL
    - Layer 3: network layer
        - Standaard IP protocol is niet veilig -> IPsec
    - Applicatie onafhankelijk
    - IPsec
        - Extra security toevoeging op IP protocol
        - Voegt extra header toe
        - Zit in IPv6 geïntegreerd
        - CIA
            - Confidential
                - Is niet verbonden aan een ecryptie algoritme
                - Kan makkelijk overschakelen naar nieuw algoritme
            - Data integrity
                - Checksums: controleren of data goed is aangekomen
            - Authentication
                - Internet Key Exchange (IKE)
                - Hiervoor is het niet geschikt want makkelijk vatbaar voor spoofing

Encryptie

- **Symmetrische encryptie**
    - Zender geeft een sleutel
    - Ontvanger krijgt de sleutel om het te ontcijferen
    - Beide partijen gebruiken dezelfde sleutel
        - Hoe deze sleutel op een veilige manier doorsturen? -> zie later
        - Dit is de zwakte van deze encryptie
    - Slide 43 -> niet van buiten leren
    - Block cipher en Stream cipher
    - Nadelen
        - Doorsturen van de sleutel -> Hoe kan dit veilig?
- **Asymmetrische encryptie**
    - Privé sleutel
        - Enkel gekend door ontvanger
    - Publieke sleutel
        - Gekend door iedereen
        - Publieke sleutel is een afgeleide van de privé sleutel
        - De publieke sleutel kan afgeleid worden van de privé sleutel, maar niet omgekeerd
    - RSA is de populairste die hiervoor gebruikt wordt (Rivest – Shamir – Adleman)
        - Werkt met priemgetallen enzo…

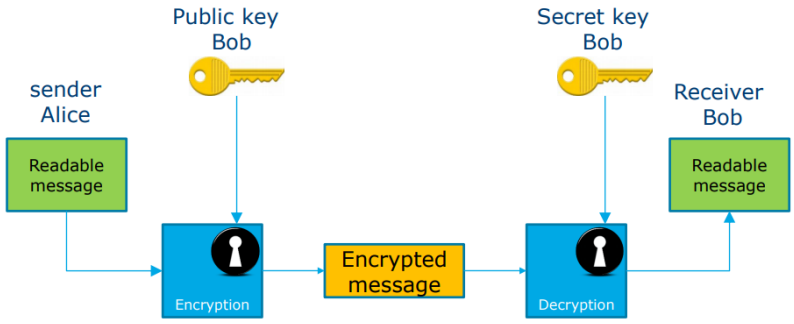
        - Probleem: door de toenemende snelheid van computers wordt dit steeds minder veilig
    - Hoe?
        - Ontvanger heeft privé sleutel
        - Ontvanger creëert publieke sleutel en geeft deze aan zender
        - Zender versleuteld data met publieke sleutel en stuurt het door
        - Ontvanger kan de data ontcijferen met de privé sleutel
    - CIA
        - Confidentiality
            - Only sender and receiver know the contents of the message
        - Authentication
            - Everyone is who they claim to be
            - Alleen ontvanger kan bericht ontsleutelen dat afkomstig is van zender met publieke sleutel

Les 8: 1/04/20 (online)

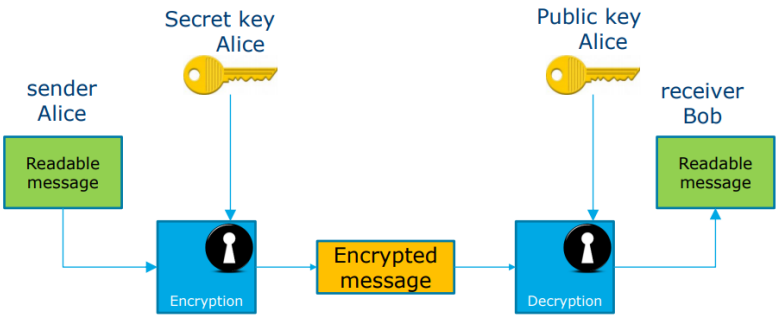
Examen: wat is asymmetrische encryptie? Wat zijn de voordelen en nadelen

- Asymmetrisch komt van het feit dat er verschillende sleutels gebruikt worden
- Er is een verband tussen de twee sleutels
- Geheime sleutel wordt nooit meegedeeld
- Publieke sleutel is afgeleid van de geheime sleutel

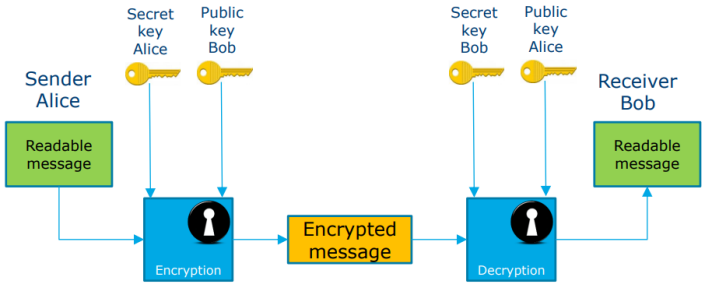
Confidentiality



Authentication



Confidentiality + **A**uthentication



- **Dubbele encryptie**
- Langs twee kanten asymmetrische encryptie
- Volgorde is belangrijk
- CIA -> I staat voor **i**ntegriteit -> checksoms
- Only sender Alice can send message encrypted with the secret key of Alice
    - **A**uthentication of Alice
    - Can be verified with public key of Alice
    - Hoe kan de ontvanger worden geauthentiseerd? → certificaat
- Only receiver Bob can decrypt message that was encrypted with the public key of Bob
    - **C**onfidentiality of the communication
- It does require that both parties know to whom the used keys belong

Certificaten

- Waarom?
    - Authentication of receiver (!)
    - Is used to exchange the public key of the receiver
- Hoe weet je of een certificaat echt is?
    - Moeten ondertekend worden (digitaal)
    - Wie doet dit?
        - Dit kan je zelf doen (self-signed)
            - Niet veilig
        - Laten doen door een derde partij: **certification authority** (CA)
            - veiliger
- Certificaat moet worden ondertekend door een derde partij
    - Die gaan bevestigen dat jouw handtekening te vertrouwen is
    - Dit gebeurt ook met een nieuwe certificaat
        - Hoe weet je dan of deze echt is?
        - Hier is een hiërarchie tot aan een **Root CA (VeriSign)**
            - Hiërarchie → PKI = PUBLIC KEY INFRASTRUCTURE
        - Root certificaat is self signed -> wordt niet meer gecontroleerd
- Slide 60: niet vanbuiten leren
- Certificaat kan ook ingetrokken worden
    - **Certificate Revocation List** (CRL)
    - Geldigheidsdatum wordt veranderd naar huidige tijd
- Bij gebruik van certificaat wordt eerst de einddatum gecontroleerd, dan kijken of deze is ingetrokken

IPSec

- Geen beveiliging in IP protocol
- Op de netwerk laag (laag 3)
- Principes van CIA toepassen
- Confidentiallity: er kunnen verschillende encryptie algothimes worden gebruikt
- Integriteit controleren met hashing
    - Als er één karakter verandert, zal de hash code ook anders zijn
- Authentication
    - PSK (Pre-Shared Key)
    - RSA (certificaten)
- IPsec gebruikt **symmetrische encryptie**
    - Symmetrische encryptie is sneller dan asymmetrische
    - Er moet een geheime sleuteloverdracht plaatsvinden
    - Dit gebeurt maar één keer voor het opzetten van de verbinding
    - **Diffie-Hellman**
        - Sleuteloverdracht gebeurt **asymmetrisch** bij het opzetten van een IPsec communicatie
- Slide 66: niet op examen, gewoon bekijken
- Anti-replay -> zorgt ook voor integriteit
    - Pakketjes kan verschillende routes vormen
    - Werking
        - Elk pakket heeft een sequence nummer
        - Wanneer een pakket aankomt moet het binnen een bepaalde window vallen
        - Wanneer een pakket met een hogere nummer dan de windows aankomt, zal de window opschuiven
        - Wanneer een pakket aankomt met een lagere nummer dan de window, dan wordt het pakketje als onveilig beschouwd; misschien is dit onderschept
    - Om een indicatie te krijgen wanneer een pakket veel later aankomt dan de rest
- Dit gebeurt in de netwerk laag

SSL VPN

- TLS gebeurd in de transport laag (laag 4)
    - Transport layer security
- TCP
    - Handshake protocol
- UDP is tegenhanger
    - Gaat gewoon pakketjes blijven sturen zonder te controleren of het aankomt: connectionless
- SSL
    - Onderling afspraken maken door handshake
    - Aantal keer over en weer praten tot er een afspraak is gemaakt
    - **Asymmetrische encryptie** voor het vastleggen van een **gemeenschappelijke sleutel (symmetrisch)**
    - Slide 72: niet alle stappen uit het hoofd leren
- Openvpn
    - Gebruikt transport layer security
    - Slide 75: niet van buiten leren
    - CIA

        - **C**onfidentiality: symmetric encryption
        - Data **i**ntegrity: hashing
        - **A**uthentication: RSA, DH
    - VPN staat niet synoniem voor encryptie
    - Slide 76 is heel duidelijk
    - Encapsulatie
    - Routed adapter
        - Krijgt ip die niet in het lokale netwerk ligt (subnet)
    - Bridged adapter (tap)
        - Mee in het lokale netwerk (subnet)

SSH

- Application layer security (laag 7)
- Eerst inloggen via het onbeveiligde netwerk
- Eerste stap: verbinden maken
    - Data encryptie is symmetrisch
        - Is performanter, gaat sneller
    - Eerst sleuteluitwisseling met asymmetrische encryptie
        - Beide partijen genereren maken tijdelijke sleutels en wisselen publieke sleutels uit
- Tweede stap: authenticatie
    - Kan met sleutel
        - Publieke sleutel uploaden op server
        - Server stelt challenge message die enkel kan worden ontcijferd met de privé sleutel
- Data integriteit gebeurt met hash code
- SSH as PROXY
    - Requests omleiden door een SSH tunnel via een tussenpersoon

Proxy vs VPN

- Bij VPN wordt een tunnel gemaakt → encapsulatie van data
- Bij proxy gaat data gewoon langs server, zonder tunnel

<u>Hoofdstuk: Email</u>

- Geschiedenis
    - Eerst gewoon bestanden doorsturen van de ene server naar de andere
        - Hier is FTP uit ontstaan (File Transport Protocol)
        - Uit FTP is een mail protocol gegroeid
- Hoe werkt dat (architectuur)?
    - User agent (UA): client = user interface (Gmail, Outlook, pine, …)
    - Message Transfer Agent (MTA): gaat communiceren met één client en doorsturen van naar een andere server
        - Spooling: zegt tegen client dat bericht verzonden is en zal het bericht doorsturen naar de volgende server (dit kan traag gaan, maar voor de client lijkt dit snel te gaan door spooling); mail wordt in een wachtrij geplaatst
    - Server relay: zal mail van de ene server naar de andere doorsturen
    - SMTP protocol

        - Simple Mail Transfer Protocol

Les 9: 22/04/2020 (online)

- Message transfer agent
    - Gebruikt SMTP (simple mail transfer protocol)
- Meestal zal elke client via het netwerk verbonden is met een server
- Message access agent (mail lezen van server)
    - Gebruikt geen SMPT
        - Dit is een “push protocol”
    - Gebruikt wel “pull protocol”
        - POP3
        - IMAP4
- SMTP (outgoing mail)
    - Vroeger SMPT
        - Tekst based
        - Poorten niet van buiten kennen
        - Client – Server (TCP)
    - Nu ESMPT
        - Ook versturen van foto’s, video’s, grotere berichten, binaire file’s
    - SMPT communication
        - De client moet het IP adres kennen van de server -> DNS
            - Records toegoeven
                - MX: zoeken naar een mail service, deze gaat verwijzen naar een host record
        - Er worden commando’s gestuurd met verschillende keywords
    - Beveiliging
        - Vroeger weining beveiliging
        - Eerste beveiliging kwam van whitelisting
        - Nu is er authenticatie en beveiligingen (SSL)
- POP
    - Post office protocol
    - Pull protocol
    - Download-and-delete principle
        - Mail wordt verwijdert na het ophalen van de mail
        - Ze gingen er van uit dat deze mail maar door één apparaat wordt opgeladen
    - Command and respone zoals bij SMTP
        - Verzenden van commando’s in octets (8 bits)
    - POP3
        - Met authenticatie (gebruikersnaam en wachtwoord) in clear tekst
    - No TSL en SSL beveiliging
        - APOP
    - UIDL
        - Uniek ID van 5 karakters

    - CAPA commando
        - Geeft een lijst terug van de capabiliteit
- IMAP
    - Internet message access protocol
    - Constant verbonden
    - Meerder toestellen kunnen dezelfde mailbox lezen
    - Berichten blijven op de server
    - Hier is ook command-response communicatie
    - IMAP maakt gebruik van 'flags'
        - Vb.: read, replied, deleted, …
    - Je kan ook zelf keywords toevoegen
        - Tags
    - Nog voordelen
        - Folder toevoegen
        - Zoeken
        - Extensies toevoegen (in IMAP4)
    - Kan ook "partial fetch" waar je een preview kan krijgen van een mail
- Microsoft exchange server
    - Apart protocol om te communiceren -> MAPI
    - Heeft ook kalender, …
    - Werkte ook met de standaard protocollen
- MIME (wat is mime **EXAMEN**)
    - Multipurpose internet mail extensions
    - Email is tekst based (7 bit ascii)
        - Maar wat als je foto's wilt sturen?
    - Oplossing
        - Bitstream opdelen in binaire delen van 7 bits
        - Je moet weten waar dit begint en wanneer het stopt
    - Vb.: base64
        - 6 base nummers naar 64 mogelijke karakters
- Web-based email
    - Web server gaan mail ontvangen
    - Gebruikt IMAP zodat de mail niet wordt verwijderd en van meerdere toestellen kan worden bekeken
    - Vb.: squirrelmail
        - Gebruikt PHP
        - Heeft een "stateful connection"
            - Er wordt rekening gehouden met het verleden
                - Er moet niet voor elk commando geauthentiseerd worden
                - Gewoon eenmaal een verbinden openzetten
        - Gebruikt een IMAP proxy
            - Tussen web server en IMAP server
            - Proxy maakt verbinden met server, en jij met de proxy
                - Zo moet er niet altijd verbinden gemaakt en verbroken worden met de mailserver

Les 10: 6/05/2020 (online)

Global catalog

- Staat alle informatie in van heel het domein + van andere domeinen
    - Alle objecten binnen het eigen domein
    - Staat en beperkte hoeveelheid van andere domeinen
        - Betere performantie
        - Sneller zoeken
- Er is replicatie van deze global catalogs tussen domain controllers
- Functies
    - Objecten zoeken via LDAP
    - Valideren van referenties
        - Id van object
    - Authenticatie
        - Kijken of gebruiker in lijst van gebruikers staat
        - Voorbeeld slide 7
            - Eerst domain opzoeken op DC
            - Gebruikersnaam controleren op Global Catalog (GC)
            - Volledige naam terugsturen
            - Terugsturen welke domain controller het beste is voor de gebruiker
            - Verbinden met die DC
- Per Active directory site minstens één global catalog
- Hoe kan je zien of server GC is?
    - NTDS settings properties

Service records

- Gebruikt om domain controllers te verbinden
- Verwijst naar hosts (server)

Wat zit er in een global catalog?

- **Schema partition** (**examen!!!!**)
    - De blauwdruk voor een object
    - Definitie van de objecten, welke velden er bestaan
    - Staan op elke domain controller
    - Kan je maar wijzigen op één DC
    - Je kan schema enkel bewerken op de **schema master**
        - Enkel hierop kan je het schema aanpassen
        - Is één DC
- Configuratie partition
    - Structuur van de domain
    - Één per forest
    - Komt wel op alle andere DC

    - Er is maar één domain-naming master
- Domain partition
    - Meerdere domain partitions per forest
    - PAS
- Application partition
    - Info over applicaties
    - Andere data dat niet over active directory gaat (=varia)
- Global catalog partition
- Wat kennen op partities
    - Wat betekenen ze

AD relationships

- Relaties tussen domains in forest
    - Mekaars recources gaat herkennen
    - Als je bent geauthenticeerd op het ene domein, ben je dat ook op het andere
- kan in één richting
    - Trusted domain: kan gebruik maken van trusting domain recources
- Standaard relation in AD
    - Two-way
    - Transitive
- AD trees
- **Alle domain binnen één forest hebben automatisch two-way en tranitive**
- Tussen twee forests is er geen relatie, maar is wel mogelijk
    - Dit is eerder een uitzondering -> manueel instellen
- **Root domain**
    - Allereerste domain die je hebt toegevoegd in de forest
    - Alle relaties vertrekken vanuit het root domain
- Één van de grote voordelen: single logon
- Shortcut trust
    - Soms nodig in grote forests waar vertraging begint te komen
    - Binnenwegen maken
    - Manueel aanmaken
    - Is enkele richten, zelf tweede richting aanmaken
- AD forests
    - Slide 38!
- Trust typres
    - Parent-child trust
    - Tree-root trust
    - Shortcut trust
    - External trust
        - Voor oude domain structures
    - Realm trust
        - Voor unix, linux, …

Flexible single-master operations (FSMO) roles

- Rol die toegekend word aan een bepaalde machine
- AD is multi-master
    - Voordelen

        - Wijzigingen worden gedaan op elke DC
    - Gevaren
        - Dubbele informatie
        - Vb.: op twee plaatsen tegelijk een gebruiker aanmaken (SID)
- Forest-wide master roles
    - Slide 62
    - Schema master
    - Domain-naming master
- Domain-wide master roles
    - RID master
        - Zegt welke set van nummers elke DC mag gebruiken
        - Als deze op zijn moet de DC aan de RID master nieuwe reeks vragen
    - PDC emulator master
        - Voor communicatie met oudere DC
        - Vb.: time service -> synchronisatie van tijden
        - Vb.: account lockout processing
    - Infrastructure master
        - Voor het updaten van referenties van objecten
            - Bij het verplaatsen van objecten, zullen de ID wijzigen
                - Eerste zal het object worden verwijderd uit het ene domain
                - Dan toegevoegd bij het andere domain
- Rollen kunnen getransfereerd worden
    - Als een server wordt vervangen
- Opeisen van een rol

Hoofstuk: AD access control, groups

- User access
    - Gebruiker gaat zich aanmelden (authentication)
    - Daarna pas zeggen wat die gebruiker mag doen (authorization)
- **Principal**
    - Object waarna je kan verwijzen om toestemmingen aan te geven
        - Gebruiker
        - Machine
        - …

Authentication

- Kerberos: authenticatie waar windows voorkeur aan geeft
    - Is wederzijds (**mutual authentication**)
        - Gebruiker moet zich identificeren
        - Server moet ook identiteit kunnen bewijzen
    - Werkt met “tickets” (tokens)
    - Gebruikt drie services
    - Proces
        - Eerste aanmelden bij authenticatie server (DC)
            - TGT: ticket-granting-ticket
        - Die server geeft een “ticket” (token)

        - Met deze ticket kan je je aanmelden bij bepaalde services
            - TGS: ticket-granting-service
        - Deze controleert welke autoriteiten (rechten) de gebruiker heeft
    - Voordeel
        - Je moet maar één keer je wachtwoord door het netwerk sturen
        - Daarna wordt de token gebruikt
    - Token zal na een bepaalde tijd vervallen, of bij afmelden
    - Draait ook op DC
        - KDC: key distribution service
        - Als KDC plat ligt, werkt de AD niet meer
            - Op meerdere DC's KDC draaien
- NTLM
    - Is het oudere systeem
        - Als KDC niet meer werkt, kan je deze als back-up gebruiken voor authenticatie
    - NTLM **challenge-response**
        - Zie eerder bij encryptie

Account security

- Account lockout policies
- Password policies
    - Kunnen op verschillende niveaus worden opgelegd
        - Domain level
        - Local level
            - Wanneer je niet verbonden met het domain
- Authentication policies
    - Kerberos met als back-up NTLM

Les 11: 13/05/2020 (online)

Hoofstuk: AD access control, groups

Authorization

- Bepalen wat de gebruikers mogen doen
- Kan op objecten worden gezet, maar ook op eigenschappen
    - Kan ook op delen van een object
- Overerving van bovenliggende objecten
    - Permissies dicht bij object zal tellen
    - Als een gebruiker tot twee groepen behoort, zal de strengste worden toegepast
- Group
    - Gebruikers of computer groeperen, als één geheel beheren
    - Types
        - Simpel administration
        - Delegate administration
        - Email distribution list

    - Recources (printers/folder/…) toestemming geven aan groepen, niet aan de gebruikers zelf (bij voorkeur).
    - Scopes (soorten groepen)
        - Machine local group
            - Enkel lokaal op machine
        - Domain local
            - Enkel herkent binnen het domein zelf
        - Global
        - Universal
            - Over forests heen
    - Kunnen worden genest (slide 47)
        - Lager niveau kan niet worden toegevoegd aan een hogere groep, maar wel omgekeerd
        - AGDLP
            - Accounts
            - Global groups
            - Domain local group
            - Permissions
    - Best practice: recources -> permissions -> domain local -> global
    - Er zijn een aantal default groups
- RODC
    - Read-only copy of the AD database partition
    - Voordelen
        - Minder replicatie verkeer
        - Veiligheid: probleem wordt lokaal gehouden
    - RODC password replication policy
        - Aangeven welke user accounts worden gerepliceerd en welke niet
        - Allowed group en denied group
        - Best practice: standaard iedereen deny, uitzondering voor allow